Ana Haydée Di Iorio - Martín Alfredo Castellote
Bruno Constanzo - Hugo Curti - Julián Waimann - Juan Ignacio Alberdi
Pablo Adrián Cistoldi - María Fernanda Giaccaglia
Fernando Greco - Juan Ignacio Iturriaga
Sabrina Bibiana Lamperti - Luciano Nuñez - Ariel Podestá
Gonzalo M. Ruiz De Angeli - Santiago Trigo

EL RASTRO DIGITAL DEL DELITO

ASPECTOS TÉCNICOS, LEGALES Y ESTRATÉGICOS DE LA INFORMÁTICA FORENSE

UNIVERSIDAD FASTA
FACULTAD DE INGENIERÍA

Universidad FASTA Ediciones
Mar del Plata, marzo 2017

Ana Haydée Di Iorio - Martín Alfredo Castellote
Bruno Constanzo - Hugo Curti - Julián Waimann
Sabrina Bibiana Lamperti - María Fernanda Giaccaglia
Pablo Adrián Cistoldi - Ariel Podestá
Juan Ignacio Iturriaga - Fernando Greco
Juan Ignacio Alberdi - Gonzalo M. Ruiz De Angeli
Santiago Trigo - Luciano Nuñez

El rastro digital del delito

Aspectos técnicos, legales y estratégicos de la Informática Forense

InFo-Lab

Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense

Grupo de Investigación en Sistemas Operativos e Informática Forense

Facultad de Ingeniería - Universidad FASTA

Este libro es producto de proyectos de investigación desarrollados por el Grupo de Investigación en Sistemas Operativos e Informática Forense de la Universidad FASTA y por el InFo-Lab, laboratorio de investigación y desarrollo de tecnología en informática forense, en Mar del Plata, entre 2010 y 2016.

GRUPO DE INVESTIGACIÓN EN SISTEMAS OPERATIVOS
E INFORMÁTICA FORENSE
(Noviembre 2016)
Universidad FASTA

Juan Ignacio Alberdi
Nicolás Battaglia
Martin Blanco
Gabriel Cardacci
Martin Castellote
Pablo Cistoldi
Bruno Constanzo
Hugo Curti
Martín Delgado
Emanuel Gaspar
Martín Gamalero
María Fernanda Giaccaglia
Roberto Giordano Lerena
Fernando Greco
Jorge Luis Herlein
Juan Ignacio Iturriaga
Sabrina Lamperti
Sebastián Lasia
Martín Lombardo
Pablo Malaret
Carlos Mathias
Martín Matus
Mirta Mollo
Luciano Nuñez
Germán Peralta
Ariel Podestá
Ezequiel Ramírez
Gonzalo M. Ruiz De Angeli
Santiago Trigo
María Paula Vega
Julián Waimann

InFo-Lab

LABORATORIO DE INVESTIGACIÓN Y DESARROLLO DE TECNOLOGÍA EN INFORMÁTICA FORENSE
(Noviembre 2016) Universidad FASTA

Procuración de la Suprema Corte de Justicia de la Provincia de Buenos Aires

Municipalidad de General Pueyrredon

Ana Haydée Di Iorio	(Directora)
Juan Ignacio Alberdi	(Facultad de Ingeniería UFASTA)
Nicolás Battaglia	(Facultad de Ingeniería UFASTA)
Martin Blanco	(Facultad de Ingeniería UFASTA)
Gabriel Cardacci	(Facultad de Ingeniería UFASTA)
Martin Castellote	(Facultad de Ingeniería UFASTA)
Pablo Cistoldi	(Ministerio Público de la Provincia de Buenos Aires)
Bruno Constanzo	(Facultad de Ingeniería UFASTA)
Hugo Curti	(Facultad de Ingeniería UFASTA)
Martín Delgado	(Facultad de Ingeniería UFASTA)
Emanuel Gaspar	(Facultad de Ingeniería UFASTA)

María Fernanda Giaccaglia	(Facultad de Ingeniería UFASTA)
Roberto Giordano Lerena	(Facultad de Ingeniería UFASTA)
Fernando Greco	(Facultad de Ingeniería UFASTA y Ministerio Público de la Provincia de Buenos Aires)
Jorge Luis Herlein	(Facultad de Ingeniería UFASTA)
Juan Ignacio Iturriaga	(Facultad de Ingeniería UFASTA)
Sabrina Lamperti	(Ministerio Público de la Provincia de Buenos Aires)
Sebastián Lasia	(Facultad de Ingeniería UFASTA y Municipalidad de General Pueyrredon)
Martín Lombardo	(Ministerio Público de la Provincia de Buenos Aires)
Pablo Malaret	(Facultad de Ingeniería y de Ciencias Jurídicas y Sociales UFASTA)
Carlos Mathias	(Facultad de Ingeniería UFASTA)
Martin Matus	(Facultad de Ingeniería UFASTA)
Mirta Mollo	(Ministerio Público de la Provincia de Buenos Aires)
Luciano Nuñez	(Ministerio Público de la Provincia de Buenos Aires)
Germán Peralta	(Facultad de Ingeniería UFASTA)
Ariel Podestá	(Facultad de Ingeniería UFASTA y Municipalidad de General Pueyrredon)
Gonzalo M. Ruiz De Angeli	(Facultad de Ingeniería UFASTA)
Santiago Trigo	(Facultad de Ingeniería UFASTA y Ministerio Público de la Provincia de Buenos Aires)
María Paula Vega	(Facultad de Ingeniería UFASTA)
Julián Waimann	(Facultad de Ingeniería UFASTA)

Universidad FASTA - Autoridades

Gran Canciller

Fr. Dr. Aníbal Ernesto Fosbery O.P.

Rector

Dr. Juan Carlos Mena

Vicerrector Académico

Dr. Alejandro Gabriel Campos

Vicerrector de Formación

Pbro. Dr. Néstor Alejandro Ramos

Vicerrector de Asuntos Económicos

CPN. Pablo Federico Vittar Marteau

Vicerrector de Desarrollo Tecnológico,
Transferencia y Vinculación

Ing. Renato Mario Rossello

Decano de la Facultad de Ingeniería

Esp. Ing. Roberto Giordano Lerena

AUTORIDADES DE LA FACULTAD DE INGENIERÍA

Decano
Esp. Ing. Roberto Giordano Lerena

Secretaria Académica
Lic. Sandra Cirimelo

Secretaria de Investigación
Lic. Mónica Pascual

Secretario de Proyección
Esp. Ing. Pablo Miozzi

Director de Ingeniería en Informática
Ing. Roberto Sotomayor

Directora de Ingeniería Ambiental
Esp. Ing. Victoria Cosia

Coordinador de Tecnicatura en Higiene
y Seguridad en el trabajo
Esp. Ing. Marcelo Ragonese

Coordinador de Licenciatura en Higiene
y Seguridad en el trabajo
Esp. Ing. Victoria Cosia

Gestores de Asuntos Estudiantiles
Ing. Paula Fresta, Esp. Ing. Marcelo Ragonese,
Ing. Micaela Lambertini

Secretaria Administrativa
Silvina Vismara

Auxiliares Administrativas
Virginia Sebastián y Daniela Rodriguez

El rastro digital del delito

Aspectos técnicos, legales y estratégicos de la Informática Forense

Ana Haydée Di Iorio
Martín Alfredo Castellote
Bruno Constanzo
Hugo Curti
Julián Waimann
Sabrina Bibiana Lamperti
María Fernanda Giaccaglia
Pablo Adrián Cistoldi
Ariel Podestá
Juan Ignacio Iturriaga
Fernando Greco
Juan Ignacio Alberdi
Gonzalo M. Ruiz De Angeli
Santiago Trigo
Luciano Nuñez

Universidad FASTA ediciones
Mar del Plata, 2017

El rastro digital del delito : aspectos técnicos, legales y estratégicos de la informática forense / Ana Haydée Di Iorio ... [et al.]. - 1a ed . - Mar del Plata : Universidad FASTA, 2017.
Libro digital, PDF

Archivo Digital: descarga y online
ISBN 978-987-1312-81-8

1. Ciberdelitos. I. Di Iorio, Ana Haydée
CDD 658.478

Miembro de la Red de Editoriales
Privadas de la República Argentina, REUP

Responsable de Edición: Lic. José Miguel Ravasi
© Universidad FASTA Ediciones
Gascón 3145 – B7600FNK Mar del Plata, Argentina

+54 223 4990400 ✉ ingenieria@ufasta.edu.ar

El rastro digital del delito. Aspectos técnicos, legales y estratégicos de la Informática Forense. Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-Compartir Igual 4.0 Internacional.

DEDICATORIA

Dedicamos este libro a todos los investigadores judiciales, peritos informáticos, criminalistas, profesionales de la informática interesados en la actuación forense, abogados interesados en las nuevas tecnologías, y al público en general que desee incursionar en la vinculación entre la informática, el derecho y la criminalística.

Los autores

Índice

Prólogo Dra. María del Carmen Falbo.....13

Prólogo Ing. Roberto Giordano Lerena 16

Nota de los autores.....25

Agradecimientos 30

De los autores.....32

Capítulo 1. Introducción a la Informática Forense, Criminalística e Investigación Penal.....46
1. Introducción 47
2. La Criminalística 47
3. La Investigación.....59
4. Objeto, sujetos y procesos de investigación 65
5. Ciencia y Justicia.....70
6. Informática forense, evidencia y evidencia digital 78
7. Conclusiones 82

Capítulo 2. Aspectos Legales. Los Delitos Informáticos 84
1. Consideraciones Preliminares.....85
2. ¿Qué son los Delitos Informáticos? La regulación Europea y Argentina 94
3. El Convenio de cibercriminalidad de Budapest.....95
4. La regulación de los Delitos Informáticos en Argentina 101
5. Delito transnacional. Jurisdicción y competencia.....150

Capítulo 3. Investigación Criminal y Penal 159
1. Aspectos Procesales 160
2. La Investigación Penal Preparatoria.....161
3. Los desafíos de la investigación de los delitos informáticos. Las dificultades probatorias en los delitos transnacionales ...187
4. Medidas probatorias (faz de derecho procesal en la Convención de Cibercriminalidad) 202

Capítulo 4. La prueba, el rol del perito y la actuación forense 221
1. La prueba, el rol del perito y la estructura judicial 222
2. Prueba. El valor y validez de la prueba.....239
4. Perito Informático. Ley N° 13.016 de Ejercicio Profesional en la Provincia de Buenos Aires. Ética profesional.....257

Capítulo 5. PURI, Proceso Unificado de Recuperación de Información 274
1. Introducción 275
2. Antecedentes 275
3. PURI 277
4. PURI: Detalle de Fases, Actividades y Tareas 283
5. Casos Prácticos 293
6. Conclusiones 327

Capítulo 6. Aspectos Técnicos 345
1. Introducción a los Sistemas Operativos 346
3. El nivel de archivos 354
4. Gestión de memoria principal 374
6. Conclusiones 398

Capítulo 7. File y Data Carving 400
1. Introducción 401
2. Conceptos generales 402
3. File Carving 410
4. Validación de Objetos y Archivos 428
5. Data Carving 436
6. Otras consideraciones 441
7. Anexo técnico I. Hardware de Discos de Estado Sólido 448
8. Anexo técnico II. Formatos de Archivo 467

Capítulo 8. Recuperación de Datos de RAID 479
1. Forensia en entornos distribuidos 480
2. Unidades RAID 480
4. Conclusiones 514

Capítulo 9. Análisis Forense de Memoria Principal 517
1. Introducción 518
2. Pericias y Análisis Forense de Memoria 519
3. Captura del volcado de memoria 526
4. Análisis de memoria principal en Windows 531
5. Conclusiones 547

Epílogo: Un escenario desafiante 549

Prólogo Dra. María del Carmen Falbo

Procuradora General
Suprema Corte de Justicia de la Provincia de Buenos Aires,
Argentina - Agosto 2016

Por diversos motivos, me resulta grato presentar esta obra colectiva en que se abordan cuestiones de especial interés para la labor del Ministerio Público de la Provincia de Buenos Aires.

La Informática Forense es una valiosa herramienta para ser aplicada a la investigación de los casos penales; y su relevancia se extiende a la litigación. Fiscales, investigadores y peritos, entre otros, deben tener conocimientos en las áreas técnica, legal y estratégica. El libro se propone cubrir esta necesidad, brindando información específica para los diferentes operadores y adoptando un lenguaje común que facilite su comprensión, considerándose incluso otros regímenes procesales, de modo que haya una visión global, de utilidad en los casos de delitos interjurisdiccionales.

En la elaboración ha trabajado un equipo interdisciplinario. Trabajo en equipo e interdisciplina son, sin lugar a dudas, rasgos distintivos de la actividad del Ministerio Público, ya que las complejas cuestiones investigativas y probatorias que presentan muchos procesos penales sólo pueden ser abordadas en forma colaborativa e integrando los aportes provenientes de perspectivas diversas.

La actividad desplegada ha trascendido el ámbito del Ministerio Público, pues participaron profesionales de la Universidad FASTA y la Municipalidad de General Pueyrredón. Esta es una política institucional que la Procuración General se ha trazado en los últimos años, de articulación entre diferentes estamentos (judiciales,

académicos, de gobierno local), para lograr objetivos comunes.

En este sentido, el InFo-Lab -ámbito en el cual se gestó la obra- viene ejecutando diversos proyectos de interés. Y el proyecto PAIF-PURI, culminó con la Guía Integral de Actuación en Informática Forense, que fue entregada al Ministerio Público y ya cuenta con su segunda versión. Complementariamente, está preparándose una Guía para la implementación de Laboratorios de Informática Forense (proyecto GT-LIF).

No puedo dejar de mencionar además, dos proyectos orientados a la investigación y la litigación penal: INVESTIGA (un sistema integrado para el análisis y visualización de datos, de próxima implementación); y FOMO (orientado al análisis de información de teléfonos móviles). El interés despertado por ambos, está generando convenios de colaboración con otras universidades, para que estas herramientas de software se adapten progresivamente a las necesidades investigativas del Ministerio Público.

Esta iniciativa que hoy tengo el honor de prologar tuvo sus orígenes y desarrollo en Mar del Plata con proyección a toda la provincia. En este Departamento Judicial años atrás se dio la experiencia piloto de profundización del sistema acusatorio, que derivó en la oralización de los procesos de flagrancia. Y es también Mar del Plata una de las sedes descentralizadas donde se ha decidido dar gradual inicio al nuevo Cuerpo de Investigadores Judiciales.

La sociedad nos demanda con absoluta legitimidad respuestas efectivas. Esto significa que los hechos delictivos no queden impunes, para lo cual es necesario llegar a la verdad con el auxilio de la ciencia y la tecnología, con profesionales adecuadamente formados y permanentemente capacitados, en el marco de un estricto respeto a la normativa nacional e internacional de derechos humanos.

Felicitaciones a quienes hicieron realidad esta obra cuyos contenidos se encuentran disponibles en formato e-book; y que la enorme satisfacción por haber culminado exitosamente la tarea emprendida, sea el mejor estímulo para concretar otros proyectos en el futuro.

Cuentan para ello con todo nuestro apoyo.

Prólogo Ing. Roberto Giordano Lerena

"Ser digital es diferente. No se trata de una invención, sino que está aquí y ahora. Podríamos decir que es genético por naturaleza, ya que cada generación será más digital que la que la precede". Nicholas Negroponte. Being Digital. 1995.

La explosión de las tecnologías de la información y la comunicación ha transformado nuestras vidas, nuestra sociedad, nuestra cultura, "digitalizándonos". Una generación posterior a Negroponte 1995, ya nadie duda que seamos digitales, irreversiblemente digitales.

El mundo, tal como lo percibimos, sigue siendo un lugar estrictamente analógico. Desde un punto de vista macroscópico, no es digital en absoluto, sino continuo. No obstante, está cada vez más soportado por información digital.

En cientos de situaciones que vivimos a diario interactuamos de diversas maneras con la tecnología de la información y la comunicación. Nos despertamos, nos movemos, nos comunicamos, nos informamos, nos ubicamos, estudiamos, trabajamos, jugamos, viajamos, compramos, vendemos, pagamos, cobramos, compartimos y "somos", mediados por la tecnología digital. Por el solo hecho de vivir en sociedad, consumimos y producimos información digital (o provocamos su producción). Y en ese ser y vivir digital, dejamos permanentemente huellas o "rastros digitales"; información digital que habla de nosotros y de nuestras acciones. Evidencias digitales de nuestro paso por la vida.

La informática forense posibilita la detección y recuperación de la información digital que sirve de evidencia a la hora de reconstruir un hecho o sucesión de ellos. La actuación forense en informática permite recuperar y enhebrar

esos rastros digitales de nuestro paso por la vida, garantizando su valor probatorio.

La demanda de pericias informáticas (actuación forense) por parte de la justicia es cada vez mayor, y crece permanentemente, dado que los rastros digitales se multiplican y son cada vez más importantes y determinantes en la investigación. La necesidad de evidencias digitales válidas que permiten reconstruir los hechos por parte de la justicia es evidente e imperiosa, y la responsabilidad de la justicia respecto de la incorporación de estas evidencias digitales al proceso investigativo y de administrar justicia es ineludible.

La Informática Forense demanda de personal entrenado en la materia, que pueda actuar metódicamente, mantener la cadena de custodia y no contaminar la prueba, principios forenses básicos. En la actuación forense o pericia se deben obtener evidencias, a fin de reconstruir la real sucesión de los hechos estudiados. La tarea clave es la correcta recuperación de toda la información posible, tanto visible como oculta, relacionada con el hecho de estudio.

A la hora de recuperar la información, el perito informático debe trabajar con diferentes tecnologías, diversos métodos de almacenamiento, tecnologías que naturalmente eliminan evidencias, mecanismos internos de protección de la información, ausencia de herramientas específicas, herramientas que cubren sólo una parte del proceso, diferentes sistemas de criptografía, y otros obstáculos, siempre garantizando un proceso reproducible de adquisición, examinación, análisis, preservación y presentación de la evidencia para que tenga valor probatorio. Dada esta complejidad se requiere de profesionales altamente calificados desde lo técnico y respetuosos de los procedimientos que fijan los códigos procesales para la actuación forense.

La investigación aplicada y desarrollo de tecnología en la Facultad de Ingeniería de la Universidad FASTA han tenido un importante desarrollo en los últimos 12 años. En ese tiempo, los grupos de investigación permanente se han ido consolidando en las respectivas temáticas y articulando conocimientos y experiencias entre ellos.

El Grupo de Investigación en Informática y Derecho, uno de los pioneros en la Universidad, reúne a un equipo interdisciplinario de investigadores de las Facultades de Ciencias Jurídicas y Sociales y de Ingeniería en proyectos donde el derecho contribuye a regular el desarrollo de la informática y la informática contribuye al derecho en general. La Informática Forense es una disciplina que se desarrolla en este campo interdisciplinar donde la informática va en auxilio del derecho en general y de la justicia en particular. Ergo, es importante conocer tanto el marco legal como el marco técnico y lograr que “ambos mundos hablen entre sí”. En ese sentido, la experiencia del Grupo de Investigación en Informática y Derecho fue un antecedente y fortaleza fundamental para el abordaje de la Informática Forense en la Universidad FASTA, que tuvo un desarrollo sumamente interesante. Vale una breve reseña al respecto.

A fines del año 2006 la empresa Microsoft libera el código del núcleo de su sistema operativo Windows 2003/Windows XP, y en el marco de su Proyecto OZ invita a los docentes de las asignaturas de Sistemas Operativos de todas las Universidades del país a participar de este proyecto.

En la Facultad de Ingeniería de la Universidad FASTA, se conformó un grupo de estudio “Proyecto OZ”, dirigido por a Ing. Ana Di Iorio, que tuvo como objetivo principal el estudio del Administrador de Procesos, Administrador de Memoria y Administrador de Dispositivos de Entrada / Salida del núcleo del Sistema Operativo Windows 2003/XP y la producción de guías teóricas y prácticas al respecto. Dichas guías todavía forman parte del contenido práctico de la asignatura Sistemas Operativos. La investigación continuó profundizando el estudio

del Administrador de Memoria Caché, Dispositivos de Almacenamiento, Sistema de Archivos, Redes y Seguridad del núcleo del Sistema Operativo Windows 2003/XP y la producción de las guías teóricas y prácticas correspondientes.

A partir de la experiencia adquirida en la administración y alojamiento de la información de sistemas a bajo nivel, el equipo de docentes especializados comienza a realizar transferencia y asesoramiento, auxiliando a peritos informáticos de la ciudad que carecían de los conocimientos y técnicas necesarias para la eficiente recuperación de la información en sistemas informáticos.

En este contexto, y a partir de la interacción Universidad – Justicia, el equipo detecta la inexistencia de metodologías y procesos normados a efectos de la recuperación de la información con valor probatorio. Esto motivó, en el año 2008, la creación del Grupo de Investigación en Sistemas Operativos e Informática Forense a efectos de desarrollar un proceso unificado de recuperación de información. El proyecto tuvo por objeto estudiar las técnicas y herramientas disponibles en el mercado para la recuperación de la información, el diseño de propuestas de desarrollo de nuevas técnicas y herramientas y el diseño de un Proceso Unificado de Recuperación de la Información (PURI) que sirviera de asistencia a la justicia para mejorar técnicamente la recuperación de la información en pericias. La capacidad técnica, inquietud y compromiso de la Ing. Ana Di Iorio y el Ing. Fernando Greco fueron factores determinantes para la creación y desarrollo del Grupo de Investigación.

A partir de la definición y publicación del PURI, el Grupo de Investigación da inicio a otros 2 que desarrolla en forma concurrente: “Proceso Unificado de Recuperación de la Información en Entornos Distribuidos - PURI en Clúster” y “Proceso unificado de Recuperación de la Información en Smartphones”. Este último, en forma conjunta con la Universidad Autónoma de Los Andes UNIANDES, en el

marco de un acuerdo interinstitucional de cooperación. Muchos otros proyectos de investigación y de graduación en ingeniería se fueron sucediendo dentro del Grupo de Investigación. El Grupo fue creciendo, consolidándose y posicionándose como referente en la temática, con importante actividad de investigación, desarrollo, extensión, cooperación interinstitucional y transferencia, retroalimentando siempre a la docencia.

El año 2014 marca un hito en el Grupo de Investigación, con la creación del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense – InFo-Lab.

El Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense - InFo-Lab es una iniciativa conjunta de la Universidad FASTA, la Procuración General de la Suprema Corte de Justicia de la Provincia de Buenos Aires y la Municipalidad de General Pueyrredon, que nuclea en la ciudad de Mar del Plata a un equipo interdisciplinario de investigadores científicos y tecnológicos, profesionales y técnicos altamente calificados, con el objeto de desarrollar soluciones a las demandas en el campo de la informática forense y su aplicación. Es, a su vez, la sede del Grupo de Investigación en Informática Forense de la Universidad FASTA.

Surge a partir de los antecedentes de trabajo conjunto interinstitucional y el requerimiento formal de colaboración de parte de la Procuración de la Suprema Corte de Justicia de la Provincia de Buenos Aires a la Universidad FASTA en este campo.

El trabajo y experiencia del cuerpo técnico del Ministerio Público de Mar del Plata en la aplicación de la última tecnología disponible en el país en el proceso de investigación judicial, sumado a la aplicación de metodologías y herramientas diseñadas por el Grupo de Investigación, dio excelentes resultados, colaborando con la actuación judicial, y permitiendo garantizar los principios del actuar forense.

Asimismo, la Municipalidad de General Pueyrredon a partir de la sanción de la Ordenanza Municipal N° 21096 que dispone la adhesión de la Municipalidad a la Ley Nacional de Promoción de la Industria del Software N° 25.922, y a la Ley Provincial Nº 13.649 y su Decreto Reglamentario 485/07, creó el programa Municipal de “Protección y Estímulo para las Industrias de la Tecnología de la Información y la Comunicación en el Partido de General Pueyrredón”, teniendo entre sus objetivos promover o coordinar ámbitos de generación y capacitación de RRHH para la Industria TIC e impulsar la calidad e innovación tecnológica de la industria TIC loca

Con el correr del tiempo y el trabajo conjunto interinstitucional, todo esto se articula dando lugar al primer “Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense” mixto de la Argentina, con el propósito de coadyuvar a la autonomía investigativa del Ministerio Público de la Provincia de Buenos Aires, potenciando las capacidades institucionales en una problemática de fundamental importancia para la ciudad y la provincia: la seguridad.

Los proyectos de I+D que se desarrollan en el InFo-Lab se acuerdan entre las tres instituciones, que contribuyen a su cofinanciamiento, lo mismo que los correspondientes planes de trabajo. La dirección del InFo-Lab está a cargo de la Ing. Ana Di Iorio, ingeniera en informática egresada de la UFASTA, docente investigadora de la Facultad de Ingeniería y de Ciencias Jurídicas y Sociales, Instructor Informático del Ministerio Público de la Provincia de Buenos Aires y coordinadora de la Comisión Asesora de Laboratorios Forenses del Ministerio de Ciencia, Tecnología e Innovación Productiva de la Nación.

Los resultados de las investigaciones y desarrollos tecnológicos del laboratorio se aplican en primera instancia en el ámbito de la Provincia de Buenos Aires y se extienden luego a la totalidad de los Ministerios Públicos de la República

Argentina, a través del Consejo de Procuradores y del Consejo Federal de Política Criminal, dando un alcance nacional al trabajo del equipo marplatense.

Cuatro de los proyectos del InFo-Lab han sido acreditados por el Ministerio de Ciencia, Tecnología e Innovación Productiva de la Nación, y forman parte del Banco Nacional de Proyectos de Desarrollo Tecnológico y Social de la Argentina.

Hoy participan del InFo-Lab investigadores y auxiliares de las 3 instituciones (Universidad FASTA, Municipalidad de General Pueyrredon, Procuración General de la Suprema Corte de Justicia de la Provincia de Buenos Aires), conformando un equipo interdisciplinario compuesto por unos 30 ingenieros, analistas, abogados, criminalistas, psicólogos, arquitectos, médicos, técnicos y alumnos, de las diferentes unidades académicas y carreras de la Universidad, con el único fin de contribuir, desde la investigación y desarrollo a una mejor actuación judicial.

En el marco del Proyecto de Desarrollo Tecnológico Social PAIF-PURI®, el equipo del InFo-Lab desarrolló el Protocolo de Actuación Forense PAIFPURI y la Guía Integral de Empleo de la Informática Forense en el Proceso Penal®, que contempla los diversos roles que pueden desempeñar los especialistas informáticos, conforme sus diferentes niveles de experticia (entre ellos: el Rol de asesoramiento, el Rol investigativo y el Rol pericial) y las diversas responsabilidades (entre ellas: Identificación, Recolección, Adquisición, y Pericia). Además, incorpora lineamientos referidos al abordaje de los casos, la planificación y gestión de la investigación penal y la litigación.

Esta guía, formalmente adoptada y promovida en su uso por el Ministerio Público de la Provincia de Buenos Aires, es la primera en su tipo en Latinoamérica y su aplicación contribuye a una mejor administración de justicia, permitiendo la recuperación de evidencias digitales respetando los principios

forenses básicos y dando con esto las garantías necesarias para las partes. A su vez, mediante el acuerdo suscripto entre la Universidad FASTA y la Procuración de la Suprema Corte de Justicia de la Provincia de Buenos Aires, se prevé la transferencia de esta guía a otros ámbitos judiciales, a efectos de *"contribuir a mejorar la eficiencia del cuerpo de fiscales de la Provincia de Buenos Aires y de otras jurisdicciones nacionales o provinciales que así lo requieran a través de la Procuración de la Provincia de Buenos Aires y del Consejo de Procuradores y/o del Consejo Federal de Política Criminal".*

Llegado a este punto, era necesario hacer un alto en el camino de la investigación y desarrollo y documentar para compartir. Hacer público tanto conocimiento generado y tecnología desarrollada para que se conozca en todo el país y gane sentido. Por eso este libro. Un libro fundamental para profesionales de la informática que deban desempeñarse como auxiliares de la justicia, buscando los "rastros digitales" que dejamos a cada instante, por el solo hecho de vivir en este mundo digital.

Finalmente, surge este libro; mucho más que un simple libro. Es el primer libro universitario que se edita en Argentina dedicado a la problemática de la Informática Forense. Como todo libro es un gesto de generosidad de sus autores, que comparten su conocimiento y experiencia con toda la comunidad. Además, es el producto del trabajo serio, sostenido y silencioso de muchos años de un grupo humano excepcional, que investiga y desarrolla tecnología con genuina pasión por la ingeniería. Por último, es un ejemplo icónico del trabajo interdisciplinario comprometido de la Facultad de Ingeniería de la Universidad FASTA, que evidencia el efectivo compromiso institucional con la mejora de la calidad de vida de las personas, integrando saberes, ciencia y tecnología.

Mi más sincero reconocimiento y agradecimiento a los autores por esta obra; especialmente a la Ing. Ana Di Iorio, directora del Grupo de Investigación y del InFo-Lab que ha sabido conducir este y todos los proyectos, con gran

capacidad técnica, de gestión y, sobre todo, pasión ingenieril. También a la Secretaria de Investigación de la Facultad de Ingeniería, Lic. Mónica Pascual, por su apoyo y gestión. Están haciendo un aporte muy valioso a la ingeniería en particular, y a la justicia y la sociedad en general. *¡Felicitaciones!*

Esp. Ing. Roberto Giordano Lerena

Decano, Profesor e Investigador

Facultad de Ingeniería

Universidad FASTA

Nota de los autores

El presente libro está dirigido a abogados, criminalistas e informáticos interesados en la aplicación forense de las ciencias de la información en general, y en la informática forense y su integración en el ámbito penal en particular.

Se recomienda una lectura secuencial de esta obra, sin embargo, de acuerdo a las experiencias y conocimientos de cada lector, y a las motivaciones particulares, es posible abordar cada capítulo como una unidad en sí misma.

Por este motivo, y para favorecer su lectura, es que se expone un resumen de cada capítulo, a fin de que el lector seleccione los capítulos de acuerdo a su interés y afinidad.

Capítulo 1. Introducción a la Informática Forense, Criminalística e Investigación Penal

En este capítulo introductorio, a sugerencia de los autores de lectura obligada, se exponen los conceptos generales que vinculan a la ciencia, la investigación criminal y la justicia en el campo de la informática forense. Es imprescindible que los especialistas cuenten con nociones básicas acerca de diversas cuestiones fundamentales: la relación entre ciencia y justicia; las similitudes, diferencias y relaciones existentes entre el conocimiento judicial y el científico; el entorno institucional en el cual los expertos realizan su labor; las fases de un proceso judicial; los procedimientos de trabajo y los diferentes roles de cada protagonista de dicho proceso; entre otros. Es así que se exponen algunos conceptos generales para contribuir a una inserción eficaz de los especialistas en un entorno de trabajo tan particular como lo es el forense, y a la optimización y mejor aprovechamiento del aporte de la Informática en esta área.

Capítulo 2. Aspectos Legales. Los delitos Informáticos

En este capítulo se introducen algunos aspectos básicos del derecho penal que deben ser tenidos en cuenta para el análisis de los delitos informáticos. Por otra parte, se explica qué son y en qué consisten los delitos informáticos, su regulación por parte del Convenio de Cibercriminalidad de Budapest y la normativa argentina, como así también las implicaciones que tienen las cuestiones de jurisdicción y competencia. Cabe destacar que se procura realizar una redacción sencilla para que pueda ser leído tanto por abogados como por criminalistas e informáticos. No pretende realizarse un análisis exhaustivo de los tipos penales -como se acostumbra en el estudio del derecho-, dado que para ello ya existen otros artículos doctrinarios realizados por otros autores especialistas en la materia, algunos de los cuales son citados en la bibliografía de este capítulo.

Capítulo 3. Investigación Criminal y Penal

En este capítulo se abordan las cuestiones vinculadas al inicio de una investigación penal, finalidades y características principales, su interrelación con la criminalística, las funciones durante su actuación en el lugar del hecho, y lo atinente a la cadena de custodia. Por otra parte se exponen algunos de los obstáculos y desafíos con los que se enfrentan los investigadores en su labor diaria, vinculados con la investigación en entornos digitales, así como también el análisis de soluciones que aporta el derecho internacional.

Capítulo 4. La prueba, el rol del perito y la actuación forense

En este apartado se brindan algunas explicaciones sobre el entorno en el cual se lleva adelante un proceso judicial para así poder entender las obligaciones inherentes a la labor pericial, atendiendo al tipo de proceso dónde se encuentran interviniendo, el tipo de materia (civil, laboral, penal, familia) y cuáles normativas regulan -según ello- el

actuar forense. Se busca explicar la estructura judicial -usualmente difícil de comprender por quien no tiene conocimientos del campo jurídico- de una forma gráfica. Asimismo se analizan, bajo un sistema de estructura jerárquica conceptual que sea fácilmente comprensible, las cuestiones relativas a la prueba, su valor y validez; los derechos, obligaciones y deberes de los peritos y las reglas de actuación forense tanto en los procesos civiles como penales, así como también la ley de ejercicio profesional.

Capítulo 5. PURI, Proceso Unificado de Recuperación de Información

En este capítulo se expone la necesidad de contar con un actuar metódico en la realización de tareas de informática forense y antecedentes internacionales en la materia. Se describe el modelo PURI - Proceso Unificado de Recuperación de Información, su estructura y ejemplos prácticos de aplicación.

Capítulo 6. Aspectos técnicos

En este capítulo se exponen los conceptos generales que permiten al informático forense comprender y conocer las herramientas que posee el Sistema Operativo para acceder a la información contenida en la memoria principal y en las unidades de almacenamiento desde diferentes niveles de abstracción, facilitando su correcta interpretación.

Capítulo 7. File y Data Carving

En este capítulo se exponen técnicas de file carving y data carving, utilizadas para recuperar información que se considera eliminada. Se detallan los conceptos generales necesarios para entender los mecanismos que actúan en un sistema de archivos, y en los medios de almacenamiento, lo que genera un ambiente propicio para la persistencia y posterior recuperación de la información. Más adelante se profundiza en los temas de file carving, formatos de archivo, carving básico y distintas técnicas y algoritmos que permiten

obtener mejores resultados, y a más bajo nivel data carving, y la búsqueda de información con granularidad menor que un archivo.

Capítulo 8. Recuperación de RAID

En este capítulo se exponen los conceptos básicos de arreglos RAID y cómo proceder ante su presencia relacionado a las fases, actividades y tareas del modelo PURI más relevantes para estos casos. Finalmente se desarrolla una técnica para reconstrucción de arreglo de discos factible de ser utilizada como último recurso, para la cual se plantea una situación de problema ejemplo, un entorno de pruebas y la técnica propiamente dicha.

Capítulo 9. Análisis Forense de Memoria Principal

La información contenida en la memoria principal de un equipo computacional puede ser de gran relevancia y hasta un factor de éxito para una investigación de un caso penal (Burdach, 2008). Por el carácter altamente volátil de los datos contenidos en memoria, es clave realizar una captura temprana del contenido de la memoria. Para esto, es necesario entender que toda actividad que se genere en el equipo para realizar un volcado del contenido de la memoria a un archivo, debe minimizarse, dado que modifica la propia evidencia digital.

Es posible encontrar estructuras con datos que sólo se encuentran en memoria y que pueden aportar pruebas de gran relevancia en una investigación. También, el malware o software malintencionado deja rastros que sólo se pueden encontrar en memoria, lo que convierte a su análisis forense en actividad aún más importante.

Este capítulo pretende mostrar las actividades presentes en el análisis forense en memoria, los distintos formatos de volcado de memoria y sus particularidades, las estructuras que se pueden encontrar (particularmente en Microsoft Windows) y los datos que éstas pueden aportar para una

investigación judicial y para la búsqueda de presencia de malware.

Agradecimientos

Agradecer es mirar atrás, volver a andar el camino recorrido, observar desde la distancia y sentir que todas y cada una de las personas aquí nombradas debieron participar para que esta obra llegue a concretarse. Agradecer es una necesidad del alma, porque sabemos que juntos, se puede llegar mejor, se puede llegar más lejos, se aprende de la visión del otro, y, además, se disfruta del camino, como en cada una de las reuniones que tuvimos para elaborar y coordinar este libro.

Queremos agradecer especialmente:

Al Ing. Roberto Giordano Lerena, decano de la Facultad de Ingeniería de la Universidad FASTA, por haber confiado en nosotros desde el primer día cuando, por el año 2010, en un café, le mencionamos la necesidad de generar un Proceso Unificado de Recuperación de la Información.

A la Lic. Mónica Pascual, secretaria de investigación de la facultad de ingeniería de la Universidad FASTA, a la Lic. Amelia Ramírez, ex secretaria, y a la Ing. Andrea Comas, actual secretaria de investigación de la Universidad FASTA, por acompañarnos en cada uno de los pasos que dimos y apoyarnos para continuar generando conocimiento en estas áreas tan poco exploradas.

Al Dr. Juan Carlos Mena, rector de la Universidad FASTA, al Dr. Fabián Fernández Garello, Fiscal General del Ministerio Público Fiscal del Departamento Judicial Mar del Plata, al ex intendente del partido de General Pueyrredon, Cdor. Gustavo Pulti, al ex Secretario de Desarrollo Tecnológico y Mejora de la Administración, Ing. Renato Rossello y al actual intendente, Dr. Fernando Arroyo, por creer que la colaboración Universidad-Estado es posible y promover la creación del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense “InFo-Lab”, precursor de esta obra.

A la Dra. María del Carmen Falbo, Procuradora General de la Suprema Corte de Justicia de la Provincia de Buenos Aires, a la Ing. Daniela Barbera, Subsecretaria de Informática, y al Dr. Esteban Lombardo, Secretario del Departamento de Policía Judicial, quienes abrieron amablemente las puertas del Ministerio Público para que podamos interactuar y nutrirnos con las problemáticas concretas que nos permitieron entender las necesidades de los destinatarios de este libro.

A la comunidad de informáticos forenses, peritos informáticos e investigadores judiciales, que día a día nos plantean nuevos desafíos que nos motivan a seguir avanzando, a generar nuevo conocimiento, y a colaborar desde el lugar que nos toca para una mejor investigación penal, que redunda en una sociedad más justa.

A todos los investigadores del InFo-Lab, especialmente a aquellos que no participaron de este trabajo, porque cada experiencia compartida es un aporte en este apasionante camino.

A nuestras familias y amigos.

Y a Dios, junto al que todo es posible.

De los autores

Ana Haydée Di Iorio

Es Ingeniera en Informática de la Universidad FASTA y Especialista en Gestión de la Tecnología y la Innovación de la Universidad Nacional de Mar del Plata. Ha realizado y aprobado el curso de Posgrado Capacitación en Ciencias Forenses de la Universidad Nacional de La Plata y tiene pos-título de Formación Docente para Profesionales y Técnicos.

Es Instructor Informático en el Ministerio Píblico de la Provincia de Buenos Aires, docente en el Postgrado de Criminalidad Económica de la Facultad de Derecho de la Universidad de Castilla La Mancha y de la Universidad Nacional de Mar del Plata, del Postgrado de Actualización en Derecho Informático de la Universidad de Buenos Aires y del Postgrado en Forensia Digital de la Universidad Católica de Salta. También es directora y docente del Programa de Actualización Profesional en Informática Forense de la Facultad de Ingeniería de la Universidad FASTA.

Es director del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense *InFo-Lab*, integrado por la Universidad FASTA, el Ministerio Público de la Provincia de Buenos Aires y la Municipalidad de General Pueyrredón, donde dirige, además, los siguientes proyectos acreditados como Proyectos de Desarrollo Tecnológico y Social: INVESTIGA “Ambiente Integrado de Análisis y Visualización de Datos”, PAIF-PURI “Protocolo de Actuación en Informática Forense basado en PURI”, FOMO “Plataforma de Análisis Forense para Dispositivos Móviles” y GT-LIF “Guía Técnica para la Implementación de Laboratorios de Informática Forense”.

En la Universidad FASTA es Profesor Adjunto con dedicación afectada a docencia e investigación. Se desempeña como Profesor en las materias Informática y Derecho y Sistemas Operativos de la Facultad de Ingeniería, y

en la materia Derecho Informático de la Facultad de Ciencias Jurídicas y Sociales. En lo que hace a investigación, se desempeña como Directora del Grupo de Investigación en Informática Forense de la Facultad de Ingeniería de la Universidad FASTA. Actualmente dirige el proyecto "Elaboración de Indicadores para la detección de Malware" y participa del proyecto "La reconfiguración del Estado en la Sociedad en red. Experiencias democráticas de promoción de inclusión digital, participación política y transparencia en América Latina y el Caribe – ALC en la Sociedad en Red" con la Universidad Federal de Santa María de Brasil.

Trabaja e investiga en el área de informática y derecho desde hace más de diez años, habiendo participado en varios proyectos relacionados con la temática, entre ellos, el Proyecto "Ontojuris", con el I3G de Brasil y la Universidad Politécnica de Madrid y el proyecto "Diseño de un Centro de Resolución Electrónica de Conflictos" realizado en conjunto con la Universidad UNIANDES de Ecuador. Ha dirigido, entre otros, los Proyectos "Proceso Unificado de Recuperación de la Información – PURI", "PURI en Dispositivos Móviles" realizado en conjunto con la Universidad UNIANDES de Ecuador y "Análisis de Consistencia de la Legislación de Defensa del Consumidor por Métodos Formales", realizado en conjunto con el Grupo de Investigación FORMALEX de la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires.

En la Facultad de Ingeniería de la Universidad Nacional de Mar del Plata es Jefe de Trabajos Prácticos de las cátedras de Sistemas Operativos y Diseño de Sistemas Operativos.

Es integrante de la Comisión Asesora de la Red de Laboratorios Forenses del Ministerio de Ciencia, Tecnología e Innovación Productiva de la Nación, y fue integrante de la Mesa de Trabajo de la Red de Laboratorios Forenses del mismo Ministerio durante el año 2014/2015.

Ha presentado y publicado trabajos en numerosos congresos nacionales e Internacionales. Ha presidido el III Congreso Iberoamericano de Investigadores y Docentes en Derecho e Informática (2014), el Simposio de Derecho e Informática de la Jornada Argentina de Informática (2007 y 2009) y ha sido Secretaria General del Congreso Iberoamericano de Investigadores y Docentes en Derecho e Informática (2012).

Es coautora del libro Defensa del consumidor en la contratación de bienes y servicios informáticos, editado por la Universidad FASTA (2013).

Es integrante del Consejo Editorial de la Revista Argentina de Ingeniería – RADI de Argentina (ISSN 2314-0925), el Consejo Editorial de la Revista Direitos Emergentes na Sociedade Global – REDESG de la Universidad Federal de Santa María de Brasil (ISSN 2316-3054), el Comité Evaluador de la Revista Ingeniería Solidaria de la Universidad Cooperativa de Colombia (ISSN 1900-3102/e-ISSN 2357-6014), el Comité Evaluador de la Revista Democracia Digital e Governo Eletrônico de la Universidad Federal de Santa Catarina de Brasil (ISSN 2175-9391), y el Comité Científico de Arbitraje de la Revista Ventana Informática de la Universidad de Manizales.

Es integrante del Comité Técnico de Tecnología de la Información – Subcomité de Seguridad, del Instituto Argentino de Normalización y Certificación – IRAM, y Secretaria general permanente de la Red Iberoamericana de Universidades e Institutos con Investigación en Derecho e Informática - Red CIIDDI.

Martín Alfredo Castellote

Es Ingeniero en Informática de la Universidad FASTA, y está cursando el doctorado en Bioingeniería en la Facultad de Ingeniería de la Universidad Nacional de Mar del Plata.

Se desarrolla como investigador en Bioinformática en el Laboratorio de Agrobiotecnología de la Estación experimental INTA-Balcarce. También es Investigador del InFo-Lab, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense del Ministerio Público de la Provincia de Buenos Aires, Municipio de General Pueyrredón y Universidad FASTA.

Es Jefe de Trabajos Prácticos de la cátedra "Sistemas Operativos" de la carrera Ingeniería en Informática, en la Facultad de Ingeniería de la Universidad FASTA, donde también participa como investigador en el Grupo de Investigación en Sistemas Operativos e Informática Forense. Ha sido director y tutor de múltiples proyectos finales y tésis de graduación de la Universidad FASTA y otras Universidades.

Ha presentado y publicado trabajos en congresos nacionales e internacionales.

Bruno Eduardo Nicolás Constanzo

Es Ingeniero en Informática de la Universidad FASTA, y está cursando el doctorado en Ingeniería con orientación en Electrónica en la Universidad Nacional de Mar del Plata.

Es Investigador del InFo-Lab, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense del Ministerio Público de la Provincia de Buenos Aires, Municipio de General Pueyrredón y Universidad FASTA.

Participa como investigador en el Grupo de Investigación en Sistemas Operativos e Informática Forense de la Facultad de Ingeniería de la Universidad FASTA. Ha sido director y tutor de múltiples proyectos finales y tésis de graduación de la Universidad FASTA y otras Universidades.

Es Jefe de Trabajos Prácticos en la cátedra de Sistemas Operativos de la Facultad de Ingeniería de la Universidad FASTA, y Jefe de Trabajos Prácticos en la

cátedra Informática Aplicada de la Facultad de Ciencias Jurídicas y Sociales de la Universidad FASTA.

Es coautor del software “CIRA: Carving aplicado a la recuperación de archivos”, un framework de File Carving.

En el InFo-Lab ha participado de los proyectos “Desarrollo de una Guía Técnica para la implementación de un Laboratorio de Informática Forense GT--LIF”, “Proyecto: Ambiente integrado de visualización y análisis de datos de comunicaciones INVESTIGA”, “Proyecto: Forensia en Dispositivos Móviles - FOMO”, “Protocolo de Actuación en Informática Forense a partir del Proceso Unificado de Recuperación de la Información PAIF/PURI”, siendo coautor de la Guía Integral de Empleo de la Informática Forense en el Proceso Penal® de la Provincia de Buenos Aires.

Tiene una activa participación en actividades de extensión universitaria del *InFo-Lab* y del Grupo de Investigación.

Hugo Javier Curti

Es Ingeniero de Sistemas egresado de la Universidad Nacional del Centro de la Provincia de Buenos Aires, y Magíster en Ingeniería de Sistemas, otorgado por la misma Universidad. También allí es Profesor Adjunto en la Facultad de Ciencias Exactas.

Es consultor de Sistemas Informáticos.

Es Profesor Adjunto en la Facultad de Ingeniería de la Universidad FASTA, donde también participa como investigador en el Grupo de Investigación en Sistemas Operativos e Informática Forense.

Julián Waimann

Es Ingeniero en Informática de la Universidad FASTA y está cursando el doctorado en Ingeniería con orientación en Electrónica en la Universidad Nacional de Mar del Plata.

Es Investigador del InFo-Lab, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense del Ministerio Público de la Provincia de Buenos Aires, Municipio de General Pueyrredón y Universidad FASTA.

Participa como investigador en el Grupo de Investigación en Sistemas Operativos e Informática Forense de la Facultad de Ingeniería de la Universidad FASTA, donde también es Ayudante de Trabajos Prácticos en la cátedra de Sistemas Operativos.

En InFo-Lab ha participado de los proyectos “Proyecto: Ambiente integrado de visualización y análisis de datos de comunicaciones INVESTIGA”, “Proyecto: Forensia en Dispositivos Móviles - FOMO”, “Protocolo de Actuación en Informática Forense a partir del Proceso Unificado de Recuperación de la Información PAIF/PURI”, siendo coautor de la Guía Integral de Empleo de la Informática Forense en el Proceso Penal® de la Provincia de Buenos Aires. Fue Director Técnico en el proyecto final "Visor Web INVESTIGA".

Es coautor del software “CIRA: Carving aplicado a la recuperación de archivos”, un framework de File Carving.

Es desarrollador de software en la plataforma .NET en el sector privado

Ha presentado y publicado trabajos en congresos nacionales e internacionales.

Sabrina Bibiana Lamperti

Es Abogada, graduada en la Universidad Nacional de Mar del Plata (2007) y Especialista en Criminalidad Económica por la Universidad de Castilla La Mancha de España (2011-2012). Su tesis de postgrado abordó “La cuestión de la competencia en los delitos cometidos a través de medios informáticos”.

Ingresó al Poder Judicial del Departamento Judicial Mar del Plata en el año 2006 como meritorio en la Unidad Funcional de Instrucción y Juicio N° 10 de Delitos Económicos, teniendo un breve paso por el Tribunal Oral Criminal N° 1 como empleada administrativa, y regresando en 2008 al Ministerio Público Fiscal donde desarrolló su carrera profesional. Actualmente es Instructora Judicial, cumpliendo funciones en la mencionada UFI N° 10 de Delitos Económicos del Dpto. Judicial Mar del Plata, donde investiga causas relacionadas con maniobras de criminalidad organizada, así como delitos informáticos vinculados a lo económico.

Es docente en la asignatura Informática y Derecho de la Facultad de Ciencias Jurídicas y Sociales de la Universidad FASTA e investigadora del Grupo de Investigación en Sistemas Operativos e Informática Forense. Integra el staff de investigadores del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense *InFo-Lab*, conformado por la Universidad FASTA, el Ministerio Público de la Provincia de Buenos Aires y la Municipalidad de General Pueyrredón.

En el InFo-Lab ha participado de los proyectos "Desarrollo de una Guía Técnica para la implementación de un Laboratorio de Informática Forense GT--LIF", "Proyecto: Ambiente integrado de visualización y análisis de datos de comunicaciones INVESTIGA" y "Protocolo de Actuación en Informática Forense a partir del Proceso Unificado de Recuperación de la Información PAIF/PURI", siendo coautora de la Guía Integral de Empleo de la Informática Forense en el Proceso Penal® de la Provincia de Buenos Aires.

Es docente del Programa de Actualización Profesional en Informática Forense de la Universidad FASTA en el módulo de "Aspectos legales del actuar Forense".

Ha realizado cursos de postgrado en Derecho Penal, Derecho Constitucional, Criminología y Política Criminal,

Discurso Criminológico, Políticas Penales y Justicia Penal Juvenil.

Tiene una activa participación en actividades de extensión universitaria del *InFo-Lab* y del Grupo de Investigación.

María Fernanda Giaccaglia

Es abogada por la Facultad de Ciencias Jurídicas y Sociales de la Universidad FASTA (2007), y Magíster en Derecho de Internet y Nuevas Tecnologías de la Información y las Comunicaciones por el Instituto Europeo Campus Stellae de Santiago de Compostela (2016)

Se desempeña como Directora Legal y Técnica de la Universidad FASTA y Secretaria de Investigación y Extensión de la Facultad de Ciencias Jurídicas y Sociales de la misma Universidad.

Es docente de Derecho Civil - Parte General en la carrera de Martillero y Corredor Público de la Universidad FASTA desde el año 2008.

Es investigadora de las Facultades de Ciencias Jurídicas y Sociales y de Ingeniería en diversos grupos de investigación en la temática de informática y derecho desde el año 2011.

Es investigadora del InFo-Lab (Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense) del Ministerio Público de la Provincia de Buenos Aires, Municipio de General Pueyrredón y Universidad FASTA, desde el 2014.

Tiene una activa participación en actividades de extensión universitaria del *InFo-Lab* y del Grupo de Investigación.

Pablo Adrián Cistoldi

Es Abogado y Procurador por la Facultad de Derecho de la Universidad de Buenos Aires, y Especialista en Derecho Penal por la Universidad Nacional de Mar del Plata

Es Fiscal del Ministerio Público Fiscal del Departamento Judicial Mar del Plata desde el año 2003.

Es Investigador del InFo-Lab, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense del Ministerio Público de la Provincia de Buenos Aires, Municipio de General Pueyrredón y Universidad FASTA.

Fue docente de las cátedras de Derecho Penal II y Criminología en la Universidad Atlántida Argentina. Es docente del Curso de Formación de Instructores Judiciales para el Ministerio Público Fiscal.

Es coautor del libro "Justicia de Garantías, de Ejecución y Ministerio Público" (Riquert, Cistoldi, Celsi) y de la "Guía Integral de Empleo de la Informática Forense en el Proceso Penal basada en el Proceso Unificado de Recuperación de Información (PAIF-PURI)". Universidad FASTA, 2015.

Tiene una activa participación en actividades de extensión universitaria del *InFo-Lab* y del Grupo de Investigación en Sistemas Operativos e Informática Forense.

Ariel Oscar Podestá

Es Ingeniero en Informática de la Universidad FASTA.

Es Analista Desarrollador Informático en la Municipalidad del Partido General Pueyrredón.

En la Universidad FASTA es Profesor Adjunto en la cátedra "Informática Aplicada" de la carrera Licenciatura en Criminalística, en la Facultad de Ciencias Jurídicas y Sociales. En la misma Universidad es Jefe de Trabajos Prácticos de la

cátedra "Sistemas Operativos" de la carrera Ingeniería en Informática, en la Facultad de Ingeniería. En cuanto a investigación, es integrante del Grupo de Investigación de Sistemas Operativos e Informática Forense y participa como investigador de los proyectos "PURI - Proceso Unificado de Recuperación de la Información", "GT-LIF - Guía Técnica para la Implementación de un Laboratorio de Informática Forense Judicial" y "DIMA - Detección de Indicadores de Malware". Ha sido director y tutor de múltiples proyectos finales y tésis de graduación de la Universidad FASTA y otras Universidades.

En la Universidad Nacional de Mar del Plata es Ayudante de Trabajos Prácticos en la cátedra "Diseño de Sistemas Operativos" de la carrera "Ingeniería en Computación", en la Facultad de Ingeniería.

Trabaja activamente en el área de Informática desde hace quince años e investiga en el área de Informática Forense desde hace más de cinco años. Es Perito Informático de Lista y se ha desempeñado como Perito Informático de Parte. Ha presentado y publicado trabajos en congresos nacionales e internacionales.

Juan Ignacio Iturriaga

Ingeniero en Informática, egresado de la Universidad FASTA.

Es Jefe de Trabajos Prácticos de las cátedras Modelos y Simulación, y Sistemas Distribuidos de la Facultad de Ingeniería de la Universidad FASTA. Es Analista Programador de la Dirección de Informática y Tecnología de la Universidad FASTA.

Participa como investigador en el Grupo de Investigación en Informática Forense de la Facultad de Ingeniería de la Universidad FASTA.

Anteriormente participó en proyectos de investigación de la Universidad FASTA "Visual 2 Sis", para el desarrollo de una interfaz de programación gráfica de modelos en lenguaje

GPSS, y "Advance" para diseñar un protocolo de comunicación, y creación de un servidor, que permite realizar modelos de sistemas en un cliente y efectuar simulaciones en un servidor remoto. Ha presentado y publicado trabajos en congresos nacionales e internacionales.

Fernando Martín Greco

Es Ingeniero en Informática de la Universidad FASTA.

Es Instructor Informático y Perito Oficial en el Ministerio Público de la Provincia de Buenos Aires. Es Investigador del InFo-Lab, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense del Ministerio Público de la Provincia de Buenos Aires, Municipio de General Pueyrredón y Universidad FASTA.

Es Profesor Titular de la cátedra de Informática Aplicada de la Licenciatura en Criminalística, en la Facultad de Ciencias Jurídicas y Sociales, y Jefe de Trabajos Prácticos en la cátedra de Informática y Derecho, en la Facultad de Ingeniería de la Universidad FASTA. Es docente del Programa de Actualización Profesional en Informática Forense de la Universidad FASTA.

Participa como investigador en el Grupo de Investigación en Informática Forense de la Facultad de Ingeniería de la Universidad FASTA. Ha presentado y publicado trabajos en congresos nacionales e internacionales.

Gonzalo M. Ruiz De Angeli

Es Ingeniero en Informática de la Universidad FASTA.

Es Ayudante de Trabajos Prácticos de la cátedra Sistemas Operativos en la Facultad de Ingeniería de la Universidad FASTA, donde también participa como auxiliar de investigación graduado en el Grupo de Investigación en Sistemas Operativos e Informática Forense.

Es coautor del framework BIP-M, destinado al análisis forense de memoria de Windows 7 en sus arquitecturas de 32 y 64 bits.

Es analista de Servicios de Planificación, Programación e Información en Telefónica de Argentina SA.

Ha presentado y publicado trabajos en congresos nacionales e internacionales.

Juan Ignacio Alberdi

Es Ingeniero en Informática de la Universidad FASTA.

Participa como auxiliar de investigación graduado en el Grupo de Investigación en Sistemas Operativos e Informática Forense de la Facultad de Ingeniería de la Universidad FASTA.

Es coautor del framework BIP-M, destinado al análisis forense de memoria de Windows 7 en sus arquitecturas de 32 y 64 bits.

Es Coordinador del equipo de Consultoría de IT y Proyectos Complejos (Sistemas Atención de Emergencias 911, Telemetría con Centro de Adquisición de Datos, etc.) en Telefónica de Argentina SA.

Ha presentado y publicado trabajos en congresos nacionales e internacionales.

Santiago José Trigo

Es Ingeniero en Informática, graduado en la Universidad F.A.S.T.A. de Mar del Plata (2013).

Ingresó al Poder Judicial del Departamento Judicial Mar del Plata en el año 2008 en la Delegación de Informática. Actualmente es Perito Informático, cumpliendo funciones en el Laboratorio de Informática Forense Dpto. Judicial Mar del Plata.

Es CTO en TalSoft S.R.L. donde desarrolla consultoría en Seguridad Informática para empresas.

Es Ayudante de Trabajos Prácticos en la materia Seguridad Informática de 5to. Año de la Facultad de Ingeniería en Informática de la Universidad FASTA y auxiliar de investigación graduado en el Grupo de Investigación en Informática Forense de la Facultad de Ingeniería de la Universidad FASTA. Integra el staff de investigadores del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense InFo-Lab, integrado por la Universidad FASTA, el Ministerio Público de la Provincia de Buenos Aires y la Municipalidad de General Pueyrredón.

En el InFo-Lab participa de los proyectos “Proyecto: Ambiente integrado de visualización y análisis de datos de comunicaciones INVESTIGA”, “DIMA - ELABORACIÓN DE INDICADORES PARA LA DETECCIÓN DE MALWARE y como auxiliar en “Protocolo de Actuación en Informática Forense a partir del Proceso Unificado de Recuperación de la Información PAIF/PURI”.

Es docente del Programa de Actualización Profesional en Informática Forense de la Universidad FASTA en el módulo de “Forensia en Redes Informáticas”.

Luciano Núñez

Es estudiante avanzado de la carrera Licenciatura en Criminalística de la Universidad FASTA de la ciudad de Mar del Plata.

Es empleado del Ministerio Publico Fiscal, Departamento Judicial Mar del Plata e integrante desde su creación hasta el año 2016 del Cuerpo de Ayuda Técnica de Instrucción (CATI) desempeñándose en la investigación en causas penales.

Actualmente se desempeña en el Instituto de Ciencias Forenses de la ciudad de Mar del Plata, dependiente del Ministerio Publico Fiscal, en el área de Criminalística.

Es integrante del InFo-Lab, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense del Ministerio Público de la Provincia de Buenos Aires, Municipio de General Pueyrredón y Universidad FASTA colaborando en la realización del PAIF (Protocolo de Actuación de Informática Forense).

Capítulo 1. Introducción a la Informática Forense, Criminalística e Investigación Penal

Autores: Ana Haydée Di Iorio, Pablo Adrián Cistoldi y Luciano Nuñez

1. Introducción.
2. La Criminalística. 2.1 Aproximación a la Criminalística. 2.2 Criminalística y Criminología. 2.3 Principios de la Criminalística.
3. La Investigación. 3.1 La actividad investigativa en el contexto del proceso penal. 3.2 Investigación, prueba y argumentación judicial. Finalidades de la investigación penal. 3.3 Algunas precisiones terminológicas.
4. Objeto, sujetos y procesos de investigación. 4.1 Objeto de la investigación penal. 4.2 Investigación y roles procesales. 4.3 Procesos de investigación.
5. Ciencia y Justicia. 5.1 La investigación científica. 5.2 La prueba científica y los antecedentes de su uso en la Criminalística y el proceso penal. 5.3 Prueba científica y prueba pericial.
6. Informática forense, evidencia y evidencia digital. 6.1 La evidencia y sus funciones. 6.2 Informática forense y evidencia digital.
7. Conclusiones

1. Introducción

La excelencia técnica es una condición necesaria, pero no suficiente, para un eficaz desempeño de los expertos en Informática Forense. Es también imprescindible que los especialistas cuenten con nociones básicas acerca de diversas cuestiones fundamentales: la relación entre ciencia y justicia; las similitudes, diferencias y relaciones existentes entre el conocimiento judicial y el científico; el entorno institucional en el cual los expertos realizan su labor; las fases de un proceso judicial; los procedimientos de trabajo, los diferentes roles de cada protagonista en dicho proceso; etc.

En este capítulo, se brindarán algunos conceptos generales para contribuir a una inserción eficaz de los especialistas informáticos en un entorno de trabajo tan particular como lo es el forense. Una buena integración con expertos de otras disciplinas, investigadores, funcionarios y abogados es necesaria para optimizar el aporte de la Informática en este área.

Existen diversos tipos de conocimiento que nos acercan a la realidad forense en el ámbito penal. La criminalística, las metodologías de abordaje de los casos penales, las normas y conceptos jurídicos relativos a la investigación y la prueba, y los criterios dominantes acerca de la relación entre ciencia y proceso judicial, nos brindan perspectivas diferentes y complementarias. Se pretende aquí proporcionar una síntesis integrada de tales perspectivas, para facilitar esta necesaria familiarización con las variadas dimensiones de la labor forense.

2. La Criminalística

2. 1. Aproximación a la Criminalística

Desde sus orígenes, el hombre se ha encontrado con el desafío de tener que convivir con sus congéneres, relacionarse, interactuar de todas las maneras posibles

acordes a su condición humana. Para ordenar la convivencia se han ido creando reglas, y con el paso del tiempo se fueron formando leyes y códigos que establecen mandatos y prohibiciones. Desde el momento en que estas normas o leyes comenzaron a regir la vida del hombre, también fue posible transgredirlas, y es ahí donde comienza a surgir la noción de delito, entendido éste de manera simplificada como una acción u omisión que es castigada por una ley penal.

Paralelamente a la lucha por establecer normas que protejan a todos y no beneficien a unos pocos, se han ido creando instituciones encargadas de hacer cumplir la ley y solucionar controversias.

En este contexto, la Criminalística fue apareciendo como disciplina auxiliar, asistiendo a la labor policial y a la administración de justicia. En efecto, las fuerzas de seguridad necesitan información precisa para cumplir con su función, y la realización de un juicio justo requiere de pruebas consistentes. El surgimiento de esta actividad ha sido un proceso histórico en cuyo transcurso fueron incorporándose, hasta el día de hoy, los aportes de diversas disciplinas.

Si bien en Argentina la labor criminalística ha sido ejercida principalmente por las agencias policiales (a través de la denominada Policía Científica), dicha disciplina nutre además la labor de los peritos judiciales. Actualmente, y siguiendo la corriente iniciada en Córdoba, la Provincia de Buenos Aires tiene prevista la implementación del Cuerpo de Investigadores Judiciales (dependiente del Ministerio Público), que tendrá a su cargo la investigación de delitos complejos, homicidios dolosos y delitos cometidos por funcionarios públicos. Esta nueva institución también deberá acudir a la Criminalística para poder llevar a cabo investigaciones penales sólidas.

2.2. Criminalística y Criminología

Antes de incursionar en definiciones y postulados sobre la Criminalística y su nueva pero estrecha relación con la Informática Forense, es preciso hacer una breve mención a la Criminología. Tal vez por la similitud de los términos o por la repetición y propagación de errores, esta disciplina suele ser confundida con la Criminalística por abogados, magistrados, profesores, periodistas y otros actores intervinientes o relacionados directa o indirectamente a los procesos penales.

Tradicionalmente, la Criminología se ha centrado en el estudio de los móviles que conducen o provocan la delincuencia, para poder lograr su prevención y el tratamiento adecuado al delincuente. Los Criminólogos mexicanos Juan Pablo de Tavira y Jorge López Vergara la definen como la ciencia que se encarga del estudio del delito como conducta humana y social, de investigar las causas de la delincuencia, de la prevención del delito y del tratamiento del delincuente, teniendo su campo de acción en tres ramas: la administración de justicia, la penitenciaria y la prevención del delito. De esta manera, acotan su campo de acción a lo que se identifica como los móviles delictivos o también se conoce como la etiología del delito, aplicándose de manera práctica a aspectos pre delincuenciales y post delincuenciales.

Con el transcurso del tiempo, la Criminología fue ampliando sus perspectivas, comenzando así a estudiar otras problemáticas, tales como las estructuras sociales en cuyo ámbito se despliegan las conductas desviadas, la influencia de las denominadas subculturas, las reacciones sociales ante el fenómeno criminal, los procesos de etiquetamiento de personas y grupos sociales, los delitos de los ricos y poderosos, las funciones latentes del control punitivo, la selectividad en la persecución y sanción de delitos, los crímenes cometidos desde los aparatos de poder estatal, los efectos de la prisión, etc. La aparición de la victimología (que también ha ido desarrollando diferentes enfoques), el

movimiento de justicia restaurativa, los aportes de la perspectiva de género, el análisis económico del delito y la criminología actuarial (centrada en la reducción de riesgos), son otras vertientes destacables. Esta evolución ha transformado a la Criminología un campo de convergencia de disciplinas y puja de ideologías.

En general, la Criminología y la Victimología proporcionan conocimientos e ideas aplicables en instancias políticas y legislativas (especialmente en las áreas de seguridad, política criminal y derechos humanos). Enriquecen, además, las opciones de abordaje estratégico de casos penales en el ámbito judicial (priorización de casos o problemáticas, asistencia a las víctimas, alternativas al juicio, medición de la pena, etc.). En cambio, sus aportes en cuanto a procedimientos y herramientas de investigación y litigación son escasos y tangenciales.

Habiendo deslindado las contribuciones de la Criminología y la Victimología, es importante ahondar en el concepto de Criminalística, con el fin de comprender cómo ésta se conecta con la Informática Forense, formando una nueva vinculación o sociedad entre ambas.

A fin de entender no sólo el concepto moderno de Criminalística sino también sus proyecciones futuras, parece importante conocer sucintamente su evolución histórica, que muestra un proceso de continuo enriquecimiento y la incorporación de nuevos actores. Una definición tradicional de la Criminalística la brinda un referente latinoamericano en el tema, el doctor Moreno González, diciendo que es la disciplina que aplica fundamentalmente los conocimientos, métodos y técnicas de investigación de las ciencias naturales en el examen del material sensible significativo relacionado con el presunto hecho delictuoso, con el fin de determinar en auxilio de los órganos encargados de administrar justicia, su

existencia o bien reconstruirlo, o bien señalar y precisar la intervención de uno o varios sujetos en el mismo.[1]

La definición precedente ubicaba a la Criminalística entre las ciencias fácticas, es decir, aquellas cuyos objetos de estudio son materiales, objetivos; siendo su método la observación y la experimentación y, en una segunda instancia la deducción con su consiguiente verificación, confirmación o refutación para poder afirmar la veracidad de sus enunciados. Al ser una ciencia fáctica, la disciplina presenta las siguientes características:

- es analítica, yendo de lo general a lo particular
- es obligatoriamente especializada, por la particularización de los problemas y la necesidad de profundizar al máximo los conocimientos
- genera contenidos comunicables y entendibles para quien esté entrenado para su entendimiento
- los conocimientos son verificables, puesto que son reproducibles y por lo tanto comprobables
- es metódica, va siempre en la misma dirección de manera planeada, evolucionando y generando nuevos enunciados, siendo de utilidad para la aplicación práctica u operativa.

Hasta aquí, podría considerarse que el objeto de la Criminalística es el estudio de las evidencias materiales o indicios que se utilizan y que se producen en la comisión de hechos delictivos; y que la función de esta disciplina es auxiliar, con los resultados de la aplicación científica de sus conocimientos, metodología y tecnología, a los órganos que procuran y administran justicia a efectos de darles elementos

[1] Moreno González, L. R. (1976) “Manual de Introducción a las Ciencias Penales”. Cap. La Criminalística. Secretaría de Gobernación, México, D.F. p.844-845.

reconstructores, identificadores y probatorios para que conozcan la verdad técnica e histórica de los hechos que investigan[2]. Todos estos conceptos sobre la Criminalística son los que se conocen de manera tradicional. Tales nociones fueron delineadas a partir de la relación de esta ciencia con aquellas que la nutrieron histórica y permanentemente, como son la Química, la Física y la Biología, las cuales tenían por objeto el análisis de un tipo de evidencia que era solamente física, abordable en su totalidad desde estas tres materias. Sin embargo, la misma dinámica de la historia y la evolución del hombre y su tecnología fueron moldeando estos conceptos. Así surgieron nuevas realidades, como lo es la informática, con la digitalización de la información y las comunicaciones a través de sistemas telefónicos digitales y la web. Con ello, aparecieron nuevas conductas delictivas, nuevos actores, nuevas escenas del crimen y nuevas clases de evidencia. En consecuencia, la Criminalística, en su calidad de disciplina auxiliar de la justicia, se encuentra ante el desafío de dar respuesta científica a estas nuevas exigencias y demandas. Es aquí donde la definición introductoria que se viene utilizando (ceñida a la aplicación de los conocimientos, métodos y técnicas de investigación de las ciencias naturales) se presenta demasiado limitada.

El doctor Dimas Oliveros Sifontes amplía parcialmente las fronteras de la Criminalística, al definirla como el conjunto de conocimientos aplicables a la búsqueda y el estudio material del crimen para llegar a su prueba[3]. De la misma manera y con similar criterio, el doctor Rodríguez Manzanera la enuncia como el conjunto de conocimientos aplicables a la búsqueda, descubrimiento y verificación científica de un delito

[2] Montiel Sosa, J. (1994) “Manual de Criminalística 1”. Cap. 1 Resumen Histórico. Editorial Limusa, S.A. de C.V. Grupo Noriega Editores. México. p. 37-38.

[3] Oliveros Sinfonte, D. (1973) Manual de Criminalística, Monte Ávila Editores, Caracas, Venezuela. p.7.

en particular y del presunto responsable de éste[4]. Tales definiciones otorgan la posibilidad de integrar a la Informática Forense al campo de la Criminalística, ya que no se limitan sólo a las Ciencias Naturales como fuente de conocimiento, dando así lugar a otras disciplinas más recientes, como la recién mencionada.

Llegado a este punto, es posible definir a la Criminalística como la ciencia aplicada que, mediante el empleo del método científico, técnicas y conocimientos aportados por otras disciplinas, busca y estudia las evidencias materiales vinculadas con presuntos hechos delictivos, con el objeto de auxiliar a los órganos que procuran y administran justicia, brindándoles elementos reconstructores, identificadores y probatorios para que conozcan la verdad técnica e histórica de los hechos que investigan.

La digitalización de la información ha hecho que no siempre se deba o puede buscar un rastro o huella con un reactivo químico o magnético, sino con complejas herramientas informáticas que buscan ese indicio escondido en un código binario que genera complejos laberintos digitales de información. Hoy la sociedad está siendo contemporánea de ese cambio. De la pronta adaptación y capacidad de respuesta que tenga la justicia (con el auxilio imprescindible de una Criminalística dotada de conocimientos, métodos y técnicas adecuadas), dependerá en gran medida la calidad de sus respuestas frente a estos nuevos desafíos.

2.3. Principios de la Criminalística

A lo largo de la evolución de la Criminalística, se han ido formulando diversos postulados, que, al igual que otros principios científicos, permiten explicar determinados

[4] Rodríguez Manzanera, L. (1976) Manual de Introducción a las Ciencias Penales, Cap. La Criminología. Secretaria de Gobernación, México, D.F. p.389.

fenómenos y a la vez sirven para orientar la labor investigativa. En otras palabras, auxilian a los expertos ante el desafío de decidir cuáles evidencias buscar, dónde y cómo hacerlo y de qué modo analizar esas evidencias. Asimismo, otorgan respaldo a las conclusiones de los especialistas.

Cabe señalar que no debe buscarse en estos principios un camino investigativo único e infalible, dada la infinidad de variantes que presenta cada caso particular. No obstante, este conjunto de criterios orientadores puede ser empleado con sumo provecho para incrementar significativamente las posibilidades de éxito de la investigación penal, con un menor dispendio de tiempo y esfuerzos.

Teniendo en cuenta que los principios utilizados en la Criminalística han sido formulados en distintas épocas y aplicados inicialmente para cierta clase de delitos (principalmente hechos violentos), es necesario contar con una visión actualizada de los mismos. Ello posibilitará su empleo por las nuevas disciplinas forenses y extenderá su utilidad a la investigación y prueba de toda clase de delitos. En los párrafos que siguen se procura realizar una síntesis que permita satisfacer estas actuales exigencias.

Principio de intercambio o transferencia. El origen de este principio se atribuye al Dr. Edmond Locard (1877-1966). Locard fue un médico francés nacido a finales del siglo XIX que brilló en la primera mitad del siglo XX, donde logró su reconocimiento en el mundo de la Criminalística, que lo reconoce como el padre de la Medicina Forense moderna. Este médico afirmó que "*es imposible que un criminal actúe, especialmente en la tensión de la acción criminal, sin dejar rastros de su presencia*"[5]. Este enunciado derivó en lo que se conoce como *"Principio de Transferencia de Locard"*; porque a partir de este postulado, la investigación forense en la escena

[5] Locard, E. (1928) Manuel de Technique Policière. Ed. Paris Payot. Francia, Lyon.

de crimen se ordena definitivamente en busca de esos rastros que deja el autor de un delito como testigos mudos de su accionar o, también en la evolución del concepto, la evidencia que se lleva aquél tras su paso por la escena de crimen o lugar del hecho o de su contacto con la víctima. A la relación entre estos componentes (autor, víctima y escena del hecho) se la conoce como triángulo de la evidencia[6].

El principio de Locard es utilizado tradicionalmente para buscar evidencias en la investigación de hechos violentos (ej.: homicidios, abusos sexuales). Es en este contexto en el que suele hablarse del triángulo entre víctima, victimario y escena del crimen. Los contactos entre estos extremos del triángulo provocan transferencia e incorporación de materiales. Esta realidad ayuda a orientar la búsqueda de evidencias (ej.: cabellos, manchas de sangre, huellas de pisadas, rasguños en el rostro del sospechoso, etc.).

El presente postulado puede ser conceptualizado de un modo más genérico. Conforme tal reformulación, cabe afirmar que *cuando dos objetos entran en contacto, intercambian parte de su material*. Esta versión extendida del principio resulta aplicable a prácticamente cualquier investigación criminal. Es posible así analizar un cúmulo de interacciones en busca de evidencias, yendo más allá del clásico triángulo autor-víctima-escena. Por un lado, el intercambio o transferencia puede darse entre cosas muebles o inmuebles, personas, pulsos electromagnéticos, etc. Por otra parte, más de una hipótesis delictiva puede dar lugar a la formación, no de un triángulo, sino de un poliedro con muchos componentes: escenas y contactos preparatorios, escenarios múltiples, escenas e intercambios posteriores a la consumación, instrumentos del delito, espacios virtuales, productos del crimen, objetos personales de los sospechosos.

[6] Guzman, A. C. (2010) El Examen en el Escenario del Crimen. Ed. BdeF. Montevideo-Buenos Aires. p. 29.

Es posible también que estas interacciones provoquen huellas psíquicas o conductuales, o que se produzcan transferencias y/o intercambios en cadena (ej.: comunicaciones en la nube).

Más aún, el principio de intercambio o transferencia es útil para adoptar los recaudos adecuados en los procesos de búsqueda, obtención, conservación y análisis de la evidencia. La interacción de ésta con agentes físicos y/o humanos puede llegar a contaminarla, degradarla o destruirla. Los procedimientos de preservación de la escena, levantamiento de rastros, cadena de custodia, algoritmo de hash, etc., permiten neutralizar o, al menos, atenuar, los efectos de la interacción que los peritos, investigadores y terceros puedan entablar con la evidencia.

Principio de uso. Para producir cualquier cambio en el mundo exterior, los seres humanos utilizan “algo”. Esto se aplica al uso de instrumentos en la comisión de un delito (un arma para perpetrar un robo violento, un puño para propinar un golpe, un bolígrafo para falsificar una firma, un equipo informático para transferir fondos vía web, un programa de software para editar imágenes, etc.). El empleo de este principio puede extenderse bastante más allá del estudio de los tradicionales “agentes vulnerantes” o instrumentos del delito. En efecto, la utilización de instrumentos se verifica también en los actos preparatorios del ilícito, y en actos posteriores a su consumación. Incluso las personas prófugas emplean instrumentos que van dejando rastros (ej.: celulares, automóviles, tarjetas de crédito, etc.).

Este principio orienta hacia la búsqueda de posibles instrumentos de un delito, ampliando así las líneas de investigación. Su aplicación conjunta con los principios de intercambio y de correspondencia de características enriquece la búsqueda y análisis de evidencias.

También se debe tener en cuenta que un mismo instrumento puede ser utilizado de formas muy diversas, lo cual producirá resultados y rastros distintos. Además, ciertas

modalidades de uso de algunos instrumentos pueden permitir detectar un *modus operandi* particular, o trazar un perfil del sospechoso.

Principio de producción. Toda acción, física o humana genera consecuencias o resultados. Estos resultados se objetivan en evidencias, muchas de los cuales son pasibles de estudio criminalístico. Las evidencias que produce una conducta pueden ser sumamente diversas, y el método de análisis aplicable variará en función de estas diferencias (ej.: manchas de sangre, roturas, metadatos, etc.).

Al hablar de resultados, se está presuponiendo la existencia de un agente, de una acción y de un objeto sobre el cual recae dicha acción. De alguna manera, la consecuencia o resultado "habla" acerca de esos tres componentes. Aquí también es pertinente extender el alcance de este principio, ampliando el concepto de resultado. Esta noción refiere no sólo a clases de resultados previstas en una norma penal (ej.: lesión de una persona, adulteración de un documento, daño de un sistema informático, etc.), sino también a las consecuencias de cualquier acción relevante de carácter previo o posterior a un hecho presuntamente delictivo. Serán el plan de investigación y la estrategia de litigación (herramientas que se detallarán más adelante) los que ayudarán a seleccionar el material a analizar. Por ejemplo: la selección de los elementos a incautar durante un registro domiciliario, o los puntos de pericia que debe responder un perito, deberían obedecer a una planificación previa.

Principio de correspondencia de características. Este principio, en su acepción clásica, señala que la acción de un agente mecánico vulnerante, al hacer contacto con ciertos cuerpos, deja impresas sus características en la superficie de éstos. A la luz del principio, la realización de cotejos y estudios comparativos es útil para identificar e interrelacionar objetos con un hecho delictivo, o descartar su vinculación. Por ejemplo, el disparo de un proyectil testigo y su cotejo con otro que fue hallado en la escena del hecho, permite determinar si

este último fue también disparado por el arma secuestrada en poder de un sospechoso. La comparación de deformaciones de dos automóviles puede llevar a establecer si ambos participaron en una colisión, y asimismo contribuir a esclarecer la mecánica del hecho.

Tradicionalmente se explica que las huellas o marcas pueden ser producidas por diversos mecanismos, entre los que cabe mencionar: las generadas por adherencias transferidas; las marcas de compresión; las huellas por estriación; etc. En ciertos casos, puede producirse una combinación de estos mecanismos (ej.: compresión y estrías).

La aplicación integrada de los principios de producción, de uso y de correspondencia de características puede orientar la labor investigativa. Los distintos experimentos y pruebas de cotejo permiten, muchas veces, generar nueva información de carácter relevante. En el área informático forense, este principio podría ser explorado con mayor profundidad para ir estableciendo nuevas clases de “huellas”. El cotejo de datos y metadatos, o entre un mensaje remitido y su respuesta, entre un ejemplar y otro de un mismo archivo, la verificación del sitio de descarga del archivo, entre otros, son sólo algunos de los ejemplos de la utilidad de adoptar dicho principio, adaptándolo a las particularidades que presenta la evidencia digital.

Existen otros tres principios de utilidad más relativa. El denominado **principio de reconstrucción de los hechos** es, en realidad, la expresión del *propósito* de la labor investigativa y probatoria. En efecto, en un proceso se averiguan y controvierten sucesos acaecidos en el pasado o, mejor dicho, versiones encontradas acerca de hechos sucedidos en el pasado. La búsqueda, obtención y análisis de evidencias ha de contribuir al conocimiento o reconstrucción de esos hechos pasados, y a la validación o invalidación de las hipótesis planteadas por las partes.

El **principio de probabilidad** se vincula con la mayor o menor fuerza convictiva que poseen las inferencias realizadas

tras el análisis de una evidencia. Teniendo en cuenta que mediante el estudio de las evidencias se procura contribuir a la reconstrucción de un hecho pasado, el experto debe precisar el grado de aceptación que merece cada una de las conclusiones a las que arriba. En muchas ocasiones, ello exigirá que el especialista indique el grado de precisión que poseen la metodología y las herramientas utilizadas, realice una revisión de bibliografía científica y/o demuestre un adecuado manejo de estadística.

Por último, el **principio de certeza** alude a un paso metodológico previo a toda conclusión o inferencia. Se trata del estudio cuantitativo, cualitativo y/o comparativo de las evidencias, para determinar su procedencia, su composición, etc. A través de este procedimiento, se procura establecer si la evidencia se encuentra vinculada con los hechos controvertidos. De no estarlo (por ejemplo: evidencia no relacionada con ninguna de las escenas del hecho ni con sospechosos o víctimas), carece de sentido proseguir con su análisis.

Sobre la base de lo visto hasta aquí, se concluye que los principios de la Criminalística no anulan los principios y métodos propios de cada disciplina científica. Proporcionan, en cambio, orientaciones comunes para que cualquier especialista pueda desempeñarse eficazmente en el ámbito de un proceso penal. Por otra parte, la labor compartida por expertos de áreas científicas muy diversas genera un fructífero intercambio interdisciplinario, que es sumamente útil para la apreciación conjunta de toda la información que los distintos especialistas aportan al proceso.

3. La Investigación

3.1 La actividad investigativa en el contexto del proceso penal

Según el Diccionario de la Lengua Española, investigar es, en su primera acepción, "*indagar para descubrir algo.*

Investigar un hecho". De algún modo u otro, todas las personas investigan. Es más, viven investigando y lo hacen cotidianamente.

Muchas veces, se investiga "algo" por el puro placer de conocer. Esta actividad y este conocimiento plenifica y enriquece el entorno, aunque de forma difusa e impredecible. En otras ocasiones se investiga con una finalidad práctica bien definida, es decir, se necesita conocer algo para lograr un determinado propósito, por lo que la información buscada (y la actividad misma de búsqueda) es un medio para alcanzar un objetivo. Estos objetivos pueden ser personales, o bien pueden estar orientados en beneficio de otros.

Una primera aproximación a la investigación judicial lleva a ver que ésta no es una actividad puramente contemplativa y que tampoco está orientada hacia el logro de metas individuales. Su finalidad es la de brindar información relevante para la solución de una controversia.

En el Diccionario citado, la tercera acepción del término investigar es *realizar actividades intelectuales y experimentales de modo sistemático con el propósito de aumentar los conocimientos sobre una determinada materia*. Conocer con la mayor precisión posible los hechos que motivan una controversia judicial es esencial tanto para las partes como, finalmente, para los jueces. En este sentido, la actividad investigativa constituye un aporte imprescindible para la administración de justicia, vista ésta como una instancia de resolución de conflictos sociales. En esta obra se analiza la actividad investigativa en el área de la justicia penal.

3.2 Investigación, prueba y argumentación judicial. Finalidades de la investigación penal

La imagen de la justicia como una mujer con ojos vendados con una balanza en su mano izquierda y una espada en su derecha, es un símbolo que aporta datos significativos. La venda indica que la justicia no debe mirar la

condición de las partes ni dejarse llevar por favoritismos. En la balanza se pesan los argumentos de los contendientes en disputa. La espada, finalmente, muestra que un juicio produce consecuencias. En el área de la justicia penal, estas consecuencias suelen ser severas para una parte, para la otra, o para ambas. Razón de más para que cada parte se ocupe de cargar su lado de la balanza con argumentos de peso.

Los argumentos judiciales tienen tres componentes: los *hechos* invocados, la *prueba* aportada para demostrar que esos hechos existieron, y la *ley aplicable* a los hechos probados. Antes de llegar a litigar ante la justicia, la espada advierte que se debe llevar un caso sólido, en el cual *hechos*, *prueba* y *ley* estén suficientemente integrados y puedan resistir el contrapeso que opondrá la argumentación de la otra parte.

En este punto, todo parece medianamente claro. Pero, ¿cómo llegar hasta allí? ¿Cómo llegar a tener un caso para presentar? o ¿Cómo llegar a desechar un caso inviable? ¿Qué sucede en el camino? La investigación aparece como una actividad indispensable para transitar ese camino. En forma interactiva, se formula una hipótesis acerca de un *hecho*, corroborándola o rectificándola conforme los resultados que va arrojando la *investigación*, y ajustando las *calificaciones legales* que se consideran aplicables. De este modo, la investigación ayuda a *conocer* la verdad de los hechos y a aplicar una rotulación jurídica adecuada a esa realidad. Surge entonces que una primera función de la investigación es la de aportar un cuadro claro del caso a quien actúa en un proceso penal.

Muchos casos penales son inviables. En ocasiones, esto se advierte de inmediato (ej.: la denuncia de un hecho que carece de carácter delictivo), pero en otras, se requiere una actividad investigativa para arribar a esta conclusión. Por ejemplo, tal vez los resultados de la investigación muestren que los hechos denunciados no ocurrieron. En otros casos,

los indicios y evidencias obtenidos no son suficientes para saber cómo ocurrieron los sucesos. La labor de averiguación puede llevar también a advertir que alguno de los sospechados no participó en el ilícito, o desembocar en un estado de duda que no podrá ser superado. Existen varios supuestos, previstos en la ley, que justifican la desestimación de la denuncia, el archivo provisorio de una causa, o el sobreseimiento de un imputado.

El curso de la investigación puede exigir o aconsejar la adopción de *medidas que afectan derechos*. La finalidad de estas medidas puede ser variada: profundizar la investigación de los hechos, individualizar o hallar sospechosos, obtener pruebas para presentar en juicio, recuperar bienes sustraídos, evitar la fuga de un imputado o el entorpecimiento de la investigación, etc. Entre esta clase de medidas se destacan la interceptación de comunicaciones telefónicas, los allanamientos, secuestros de bienes, la detención de una persona, etc. Dichas medidas deben ser requeridas al juez. En tales casos, las evidencias recolectadas y los reportes de investigación deberán ser suficientes para sustentar estas peticiones.

En el medio del camino, quizás no se requiera controvertir ante un juez. Tal vez el Fiscal vea que es conveniente y legalmente aceptable discutir en forma directa con la contraparte, mostrando la fortaleza del caso, promoviendo acuerdos totales o parciales (salidas alternativas al juicio oral, estipulaciones probatorias acerca de puntos no controvertidos, etc.). Las evidencias y reportes producidos por la investigación servirán, en este contexto, para la labor de *persuasión* entre las partes.

Otra cauce de la actividad investigativa es la producción de medidas solicitadas por las otras partes (imputados, defensores, acusadores privados). En el ámbito bonaerense, dicha tarea está a cargo del Fiscal. Esto torna necesario distinguir los diferentes roles investigativos de los

protagonistas del proceso, que serán expuestos más adelante.

Cuando no es posible o no es legítimo arribar a acuerdos entre partes, tener un cuadro claro del caso no significa tenerlo resuelto. Más allá de lo que el litigante sepa y de las valoraciones jurídicas que realice respecto de los hechos, será un tercero quien deberá decidir si los hechos sucedieron tal como el aquél afirma, y si corresponde imponer ante ese hecho las consecuencias jurídicas que el contendiente considera adecuadas. Ese tercero (el juez o tribunal imparcial) deberá escuchar las dos campanas (la del agente fiscal y la de la parte acusada) antes de optar, total o parcialmente, por la que considere más razonable. Si en el curso de la investigación no se recogieron ni se preservaron correctamente las pruebas necesarias para demostrar exitosamente los hechos que se invocan ante el juez, el caso no está para nada resuelto. Más aún, tal vez termine siendo resuelto en forma contraria a la pretendida.

Sintetizando lo dicho más arriba, se concluye que las finalidades de la etapa de investigación son las siguientes:

1. Generar conocimientos acerca de los sucesos y de sus partícipes, posibilitando un encuadre jurídico adecuado y la toma de posteriores decisiones.
2. Justificar el pedido de medidas de injerencia, para profundizar la investigación, hallar sospechosos, obtener pruebas, restituir pertenencias, incautar bienes decomisables, evitar la fuga o entorpecimiento probatorio del imputado, etc.
3. Desechar los casos inviables, mediante el dictado de desestimaciones y archivos, o instando ante el juez el sobreseimiento de un imputado.
4. Entablar conversaciones con las otras partes para procurar acuerdos alternativos o estipulaciones probatorias.
5. Recabar información y pruebas solicitadas por otras partes.

6. Individualizar y asegurar las pruebas que se utilizarán en un juicio oral y público.

3.3 Algunas precisiones terminológicas

La etapa investigativa tiene dos nombres, de acuerdo con los distintos códigos procesales: "instrucción" e "investigación preparatoria". El primer término es asociable a un modelo de investigación secreto y escrito, que deja poco margen para la discusión y producción de prueba por parte de los contendientes. En cambio, el término "investigación preparatoria", presupone la existencia de una etapa posterior más relevante. La etapa de investigación es vista, desde este paradigma, como la preparación para el juicio oral y público, en el cual las partes producirán la prueba y debatirán ante un juez imparcial. Aunque la gran mayoría de los casos no terminan en un debate oral, la etapa de investigación proporciona una base necesaria para adoptar otro tipo de decisiones (desestimación de denuncias de hechos no delictivos, archivo de casos inviables, acuerdos alternativos al juicio, etc.).

En más de una ocasión se confunde la etapa de investigación con el legajo escrito donde se vuelcan sus resultados, al cual suele denominárselo "IPP", acrónimo de "Investigación Penal Preparatoria" o -en los ámbitos donde rigen códigos procesales más antiguos- "sumario". Se debe aclarar, entonces, que las actuaciones escritas son algo muy distinto de la etapa investigativa del proceso y de la actividad de investigación misma.

Hasta aquí, se ha planteado el tema de la investigación con un sesgo inevitable. Los procesos penales establecen una "etapa de investigación". Sin embargo, la palabra *investigación* significa *acción y efecto de investigar*. Las partes pueden seguir desplegando actividad investigativa hasta que finaliza el proceso judicial. El relevamiento de los intereses fundamentales de las partes, el análisis de las estrategias y pruebas de los contendientes, la búsqueda de precedentes

judiciales aplicables, las entrevistas previas al juicio con testigos y peritos, la “instrucción suplementaria” solicitada al ofrecer prueba, etc., son ejemplos de esta labor investigativa más amplia.

4. Objeto, sujetos y procesos de investigación

4.1 Objeto de la investigación penal

La noticia de un presunto hecho delictivo delimita inicialmente el objeto de la investigación. Esta noticia puede tener orígenes diversos: una denuncia, un procedimiento policial en la vía pública, un hallazgo casual acaecido durante un allanamiento, una nota periodística, etc., que constituyen la hipótesis fáctica de un presunto hecho que ya habría acontecido. Si los hechos de esa hipótesis son categorizables en alguna clase de conducta sancionable por la ley penal como “delito de acción pública”, los funcionarios competentes deben investigarlos. En la medida en que los sucesos son verificados, los funcionarios habilitados deben procurar individualizar y, en su caso, *perseguir* a los sospechosos de haberlos cometido.

El *objeto primario* de la investigación (qué investigar) se construye alrededor de la primera finalidad de esta actividad: el *esclarecimiento* de los hechos. Este objeto se delimita mediante una serie de preguntas relativas al presunto suceso: ¿Qué conducta se produjo? ¿Quiénes la llevaron a cabo? ¿Cuándo? ¿Dónde? ¿Cómo? ¿Con cuáles instrumentos? ¿Para qué y/o por qué? ¿A quiénes afectó? ¿Cuáles consecuencias tuvo?

La información que se va adquiriendo permite ir precisando y ajustando la hipótesis, modificando o sustituyendo la hipótesis inicial, cotejando siempre su adecuación o inadecuación a las diversas clases de delitos y formas de participación criminal previstas en la ley. Sintéticamente, se busca saber si existen suficientes motivos para sospechar que se perpetró una conducta delictiva

concreta, atribuible a personas concretas. En caso afirmativo, habrá de construirse una imputación que permita informar detalladamente al sospechoso cuál es el hecho que le atribuye (cf. art. 312 del CPPBA). Dicha imputación tiene la forma de relato, y está compuesta por diferentes afirmaciones de hecho con relevancia jurídica. Estas afirmaciones son construidas con las respuestas a cada una de las preguntas recién mencionadas.

Si el proceso sigue adelante y se pretende el enjuiciamiento del imputado, deberá efectuarse una descripción clara, precisa, circunstanciada y específica de los hechos que se le endilgan, con los fundamentos probatorios que tornan justificada la realización del juicio (art. 335 del CPPBA).

Otro objeto fundamental de la investigación lo constituyen las *pruebas de la hipótesis* trazada. En efecto, de poco le sirve a una parte saber con lujo de detalle qué ocurrió, si luego no puede probarlo ante el tribunal. Mediante la labor investigativa, se buscan y obtienen pruebas. Las tareas de preservación de esas pruebas, si bien no son actos de investigación, integran el conjunto de labores propio de la etapa investigativa.

El resultado de la labor de esclarecimiento y obtención de pruebas posibilita la selección de casos, descartando aquellos que no son viables. También aporta una base suficiente para explorar la viabilidad de acuerdos procesales con las otras partes.

Pueden también desplegarse otras tareas investigativas cuyo objeto responda a las demás posibles finalidades de la investigación. Así, puede ser pertinente averiguar si existe riesgo de fuga o de entorpecimiento probatorio por parte del imputado (para luego decidir si es necesario requerir medidas de coerción); precisar si hay bienes que podrían ser objeto de decomiso; etc.

4.2 Investigación y roles procesales

De acuerdo con el rol de cada actor en el proceso, la labor investigativa adquirirá rasgos específicos. Se abordará aquí principalmente el trabajo investigativo de la parte acusadora, prestando especial atención a la tarea del organismo que ejerce la acción penal pública (Ministerio Público Fiscal, o Fiscalía). El marco legal de referencia será el de la Provincia de Buenos Aires.

- La noticia de un hecho presuntamente delictivo pone en marcha a una pluralidad de actores. Por un lado, la *Policía* debe intervenir en las situaciones de urgencia y reunir las pruebas aptas para esclarecer el caso e individualizar a sus partícipes (dando base, sea a una acusación, sea a un pedido de sobreseimiento). Los integrantes de los organismos policiales deben actuar objetivamente, pero su labor funcional depende de las directivas que imparta el Fiscal (ver artículos 59, 268, 293 a 298 del Código Procesal Penal de la Provincia de Buenos Aires).

- En la Provincia de Buenos Aires compete al *Fiscal* dirigir la investigación (arts. 59 y 268 del CPPBA). Esta forma de organización procesal, que ha ido extendiéndose en muchas provincias, difiere del modelo establecido en el orden federal (en el cual las investigaciones son dirigidas por los denominados "jueces de instrucción", salvo en ciertos casos que son delegados al fiscal). A la orden de los fiscales trabajan *funcionarios* judiciales del Ministerio Público (ayudantes fiscales, instructores y próximamente integrantes del Cuerpo de Investigadores Judiciales), desplegando labores investigativas. Algunos de estos investigadores pueden ser *expertos* en una disciplina técnica o científica.

- En general, las medidas de investigación que implican injerencia en derechos fundamentales (allanamientos,

secuestros de bienes, interceptación de comunicaciones, etc.) deben ser solicitadas al *Juez de Garantías*.

- Los *peritos* aportan piezas de información específicas, que constituyen insumos necesarios para el esclarecimiento de los hechos, la adopción de decisiones y la litigación.

No debe ignorarse el rol de la defensa (cuya investigación es, en cierto modo, una estrategia de respuesta frente a los pasos que va dando o se prevé que dará el perseguidor), ni el lugar del particular damnificado (que coadyuva con la labor investigativa). Asistiendo a estas partes, pueden también intervenir otros expertos, como, por ejemplo, los peritos de parte.

4.3 Procesos de investigación

A esta altura, la investigación penal consiste en un conjunto de labores desplegadas por protagonistas muy diversos. Las posibles actividades de búsqueda de información son variadas y heterogéneas. Las fuentes de información pueden ser muy disímiles. Lo mismo ocurre con los canales mediante los cuales dicha información llega al fiscal (ej.: declaración de un testigo, dictamen pericial, informe de una institución, examen de evidencias, exhibición de fotos y filmaciones), y los códigos respectivos (ej.: lenguajes científicos, lenguaje vulgar, jergas, etc.). En particular, los expertos suelen verse en la necesidad de decodificar cierta información (ej.: ADN, evidencia digital), y recodificarla para su presentación ante la autoridad judicial de forma comprensible. Asimismo, suelen existir grandes diferencias en cuanto a las formas en que cada pieza de información debe ser obtenida y, eventualmente, preservada y presentada como prueba ante el tribunal.

La criminalística proporciona una visión de conjunto acerca de los aportes técnicos y científicos brindados por los

especialistas de diversas disciplinas. De esta perspectiva conjunta puede surgir nueva información relevante. A su vez, la investigación y la prueba científica se deben integrar con otros aportes investigativos y probatorios (ej.: evidencias materiales que no requieren mayor análisis, informes y documentos, testigos). Para que este conjunto de tareas pueda tener utilidad en el contexto de un caso penal, se requiere contar con un marco conceptual que las organice y les dé sentido. Ese marco es el denominado *plan de investigación.* En la Provincia de Buenos Aires es responsabilidad del Fiscal que exista una investigación planificada y que la ejecución de ese plan sea periódicamente evaluada.

A medida que se procura definir el propósito y la estrategia de intervención en un conflicto penal, se va planificando y ejecutando la búsqueda de información y de pruebas. Es así que, mediante esta búsqueda, se pretende dar respuesta a un conjunto de preguntas básicas acerca de los hechos (qué, quién, cuándo, dónde, cómo, etc.). Cada una de estas preguntas constituye una rama de la investigación, para la cual se buscará la información más pertinente y fiable.

Los tiempos e incidencias procesales influyen decisivamente en el ciclo de vida de cada pieza de información. Por ejemplo, ciertos datos o evidencias tendrán simplemente el valor de pistas para seguir avanzando en el esclarecimiento de uno o más interrogantes o para pedir medidas cautelares, mientras que otras evidencias y su decodificación técnica tendrán valor como prueba ante el tribunal.

La labor de búsqueda, obtención, transmisión y/o decodificación de cada pieza de información relevante deberá ajustarse a las necesidades estratégicas y a las exigencias legales. Cada uno de estos subprocesos específicos requerirá, entonces, particulares grados de formalización, publicidad y experticia técnica.

De esta forma es posible afirmar que varias de las preguntas básicas acerca de los hechos son también aplicables, con ciertas adaptaciones, a la labor investigativa: qué información buscar, quién lo hará, dónde, cuándo, cómo, con qué medios y con cuál finalidad.

Cabe analizar los procesos y subprocesos investigativos desde una perspectiva más amplia, complementaria de la anterior. Ciertos funcionarios y/o dependencias deben gestionar la realización de tareas vinculadas con un determinado caudal de casos. La optimización del manejo de la carga de trabajo es una exigencia derivada de la limitación de recursos.

Determinadas oficinas técnicas pueden representar un cuello de botella para una importante cantidad de casos penales. Para reducir el impacto de este problema, parece necesario adoptar un curso de acción doble. Por una parte, se debe prestar la debida atención a la planificación y a la gestión interna de la oficina técnica. Por la otra, las instancias jurídicas y estratégicas del Ministerio Público Fiscal deben delinear criterios de priorización de casos, determinar niveles de urgencia, evitar los pedidos de actividades que no requieren experticia, limitar el material a analizar y/o requerir informes preliminares, entre otros.

5. Ciencia y Justicia

5.1. La Investigación científica

Tal como se ha descripto en la sección anterior, para llegar al conocimiento de la verdad acerca de hechos, o al menos, a su aproximación, fiscales, defensores y jueces suelen necesitar del auxilio de la ciencia. En tales circunstancias se requerirá el aporte de un experto, especialista en una determinada ciencia o arte, a fin de que se

expida respecto de ciertas cuestiones vinculadas con un caso determinado[7].

En cuestiones específicas, los expertos están llamados a ser los "ojos y oídos" de las partes durante la investigación, y los "ojos y oídos del juez" en las instancias de juicio o controversia.

El especialista, conocedor de su ciencia o arte, se encuentra ante el requerimiento de hacer una "aplicación" de su conocimiento, en un ámbito judicial, y con el fin de aportar información que, de acuerdo a los principios de la criminalística, contribuyan al esclarecimiento o prueba de los hechos.

El experto interviene con una visión científica en una investigación y/o contienda penal. Pero en este ámbito se cuenta con un tiempo limitado, rigen determinadas condiciones de validez de la prueba, y actúan distintos protagonistas que hablan con su propia jerga (abogados y jueces) y son legos en materia científica. Ello demuestra que, por definición, por objetivos, por tiempos y por campo de actuación, la investigación científica difiere de la investigación penal.

> Según Hernández Sampieri *"la investigación científica es un tipo más de investigación, sólo que sigue procedimientos rigurosos y es cuidadosamente realizada. Es sistemática, controlada y crítica. Sistemática y controlada quiere decir que hay una disciplina constante para hacer investigación científica. Crítica, implica que se juzga constantemente de manera objetiva y se eliminan las preferencias personales y los juicios de valor".*[8]

7 Para profundizar estos conceptos referirse al capítulo 4 "La prueba, el rol del perito y la actuación forense".

8 Hernández Sampieri, R., Fernández Collado, C. Y Baptista, L, P.(2000) Metodología de la investigación. Mc Graw Hill. México.2da Edición.

Mario Bunge agrega que, como toda actividad humana, el trabajo de los científicos está enmarcado por las necesidades e ideas de su tiempo y espacio circundante. Es decir, el científico no es un ente abstracto y su tarea es de él y para él, sino que es un ser social por lo que es importante definir a la ciencia como una actividad social. Por lo tanto, la investigación puede realizar dos tareas fundamentales para la sociedad en la que se desarrolla: a) producir conocimiento y teorías, también conocida como *"investigación básica"* y b) resolver problemas prácticos, también conocida como *"investigación aplicada"*. Por medio de estos dos tipos de investigación la humanidad ha ido evolucionando, distanciándose de lo que algunos autores han denominado "conocimiento vulgar"[9].

La investigación científica constituye un proceso mediante el cual se va construyendo y moldeando el conocimiento. Como todo proceso, es dinámico, cambiante y continuo. A su vez, por ser una actividad investigativa, requiere unir el pensamiento riguroso con las inferencias que se puedan evocar a partir de los indicios y la imaginación.

La investigación actúa entonces como método para llegar a la verdad, como método de pensamiento crítico y como método sistemático, ya que se vale de procedimientos y resultados.

En este orden de ideas, se deduce que los elementos que colaboran con el esclarecimiento de un caso (por ejemplo, la evidencia digital) son buscados dentro de la etapa investigativa de exploración, a fin de encontrar hipótesis (líneas de investigación). A su vez, una vez halladas y/o analizadas, las evidencias podrán servir para para demostrar la validez o no de dichas hipótesis.

[9]Bunge, M. (1972) La ciencia, su método y su filosofía. Buenos Aires. Siglo XX.

En una línea de razonamiento sostenida desde la investigación científica, se podría concluir que la imputación de un hecho se realiza a partir de una "hipótesis sostenida en evidencias" donde el aporte científico tiene un gran peso.

5.2. La prueba científica y los antecedentes de su uso en la Criminalística y el proceso penal

No siempre ni en todas las culturas los litigios se han dirimido bajo los mismos procedimientos. Tampoco el concepto de prueba ha sido inmutable. Las ordalías o "juicios de Dios", por ejemplo, eran un modo de resolución de disputas utilizado en la Europa medieval, que no requería que las partes o el juez probaran hecho alguno, al menos del modo que actualmente es conocido. En el presente, la mayoría de los modelos procesales exigen que, para imponer una condena penal a alguien, se pruebe que el acusado ha cometido una conducta prevista por la ley como delito. Ello requiere desarrollar una actividad investigativa y, si el acusador encuentra motivos suficientes, un posterior juicio ante un juez imparcial. En este juicio, las partes alegan basándose en pruebas, muchas de las cuales son producidas o presentadas con el auxilio de especialistas en diversas disciplinas científicas.

Son los chinos los que poseen el primer registro en el siglo VII de la utilización de la prueba científica mediante el uso de impresiones dactilares, que aplicaban diariamente en sus negocios y empresas legales[10] y que luego fueron estudiadas en profundidad diez siglos después por Malpighi. Recién en el siglo XVI se incorpora otra de las ciencias fundacionales de la criminalística, la Medicina Legal. En el siglo XVII apareció la primera publicación específicamente de Criminalística, el Libro de Cospi, Il Giudice Criminalista,

[10] Bridges, B.C. (1942). Practical Finger-Print. Ed. Funk & Wagnalls Co. Nueva York y Londres. pp.11-12

impreso en Florencia en 1643, que era un verdadero tratado de Policía Científica, aunque con todas las omisiones, errores y preocupaciones propios de la época.[11] Hubo que esperar hasta el siglo XVIII para la irrupción de la Balística Forense de la mano del doctor Boucher.

Fue sin dudas el siglo XIX el que consolidó a la Criminalística de manera definitiva como ciencia auxiliar de la justicia, aplicando el conocimiento científico en sus investigaciones y logrando resultados resonantes, que son una referencia aún en la actualidad. Los avances en la dactiloscopía con la descripción de Purkinje de las huellas dactilares, la clasificación de los nueve grupos principales[12] y la descripción de los relieves triangulares o Deltas de Huschke, fueron conocimientos y técnicas aprovechados y utilizados en la India para la identificación de personas. También Henry Goddard en el Reino Unido hizo el primer cotejo balístico. En una de las balas que penetraron en el cuerpo de la víctima, Goddard observó una curiosa protuberancia. Con dicho proyectil, provisto de la mencionada seña particular, inició la búsqueda del asesino[13], al que descubrió gracias al hallazgo, en su vivienda, del molde para balas de plomo con un pequeño defecto, una hendidura que se ajustaba perfectamente a la protuberancia de la bala recuperada del cadáver. También el siglo XIX vio el nacimiento de la Fotografía Forense para el reconocimiento de delincuentes. Se le sumó el método antropométrico de Bertillon, al que después se le agregaría el retrato hablado. En Austria, el doctor Hanns Gross fue el primero en hablar de métodos de investigación criminal y denominarlos Criminalística en el *"Manual del Juez"*.

---

[11] De Benito, E. (1915) Manual de Policía Científica. Hijos de Reus, Ed. Madrid – España. P.22

[12] Bridges B.C. (1942). Practical Finger-Print. Ed. Funk & Wagnalls Co. Nueva York y Londres. P. 13.

[13] Tharwald, J. (1966). El siglo de la investigación criminal. Ed. Labor, S.A. México. pp. 46-47.

Argentina no estuvo ausente en este apogeo de las ciencias forenses. En 1891, Juan Vucetich inauguró la Oficina de Identificación y utilizó la Antropometría y las huellas digitales de ambas manos. Creó así la ficha decadactilar, descubriendo entre los sentenciados a siete reincidentes[14].

La breve reseña precedente permite observar que la Criminalística no es una ciencia joven. Tiene su origen en las ciencias naturales como la Biología, de la cual toma la antropología forense, la medicina legal, la citología, la hematología forense, la histología y la genética. Asimismo, recibe aportes de la Química: química analítica, bioquímica, química orgánica e inorgánica. La Física también contribuye con la mayor parte de sus ramas, como por ejemplo la óptica, la espectroscopia, la fotografía, la microscopía, la espectrofotometría y una gran cantidad de técnicas y herramientas relacionadas con la materia. Sin embargo, el gran aporte de la Física lo da sin dudas la scopometría, que es la técnica para el estudio físico de las cosas o las evidencias físicas en general, basado en la medición y la comparación no alterando la materia o el objeto de peritación.

La gran difusión que está teniendo la Criminalística a partir del fácil acceso a la información ha confundido a mucha gente, llevándola a creer que está en presencia de algo nuevo. Sin embargo, aunque tiene una estrecha relación con la tecnología y se vale de ella para avanzar y progresar, sus fundamentos teóricos poseen siglos en sus espaldas. Las ciencias de las cuales se nutre son milenarias y tienen el aprendizaje de la humanidad que las avala. Así como la medicina sigue siendo la misma ciencia pese a los enormes avances tecnológicos y la disponibilidad creciente de datos estadísticos, lo mismo sucede con la Criminalística. Ciertamente, la incorporación de nuevas disciplinas, tales

[14] Osorno Negrin, H. (1966). Los Criminales dejan siempre una tarjeta de visita. Ed. Sucesos México. p.36.

como la Genética y la Informática Forense, enriquecen y tornan aún más compleja su labor.

5.3. Prueba científica y prueba pericial

El especialista, ya sea perito o científico debe conocer y distinguir una *prueba pericial* de una *prueba científica*.

Una prueba es científica[15] cuando el procedimiento de obtención exige una experiencia particular en el abordaje que permite obtener conclusiones muy próximas a la verdad o certidumbre objetiva. El método o sistema aplicado trabaja sobre presupuestos a comprobar, y el análisis sobre la cosa o personas, puede ser racional y falible, o exacto y verificable[16]. Una prueba es científica si sigue para su obtención un método científico.

La aplicación de un método refiere a una organización lógica de las acciones a seguir. Un método científico, además, busca la sistematización de una forma de observar, definir, establecer, probar y generar conocimiento válido, utilizando para esto procedimientos e instrumentos fiables. De esta manera, se busca evitar toda subjetividad del científico con la investigación. El actuar técnico-científico realiza un aporte objetivo a la investigación.

En cambio, *una prueba pericial*, requiere la aplicación de técnicas específicas, y de rigurosidad legal propia que la distingue de una prueba científica. Una prueba pericial puede ser científica, pero no necesariamente. Las pruebas periciales son científicas siempre y cuando respeten el método científico, y será la autoridad judicial quien decida si admite o

[15] Para más información se recomienda el trabajo Prueba Científica y Verdad disponible en http://www.derecho.uba.ar/institucional/deinteres/2015-gozaini-pruebas-cientificas-y-verdad.pdf

[16] Estos conceptos serán luego ampliados en el capítulo 4, “la prueba, el rol del perito y la actuación forense”.

no este tipo de producción. En resumen, el método científico es una forma de observar, pensar y resolver problemas de una forma objetiva y sistemática, constituye un procedimiento de trabajo que permite descubrir las circunstancias en que se presentan hechos concretos y se caracteriza por ser: verificable, de observación objetiva y de razonamiento riguroso.

El método es el camino por el que se procura alcanzar un fin, y la técnica, es el medio por el cual se recorre el camino.

La verdad científica es debatida y validada por la comunidad científica, quien la hace evolucionar e, idealmente, no se reúne alrededor de intereses ajenos al saber. La verdad judicial, en cambio, es debatida por las partes litigantes y validada finalmente por un juez. Ni los litigantes ni el magistrado son pares del científico, ellos son legos en ese ámbito del saber. Por otra parte, los litigantes son portadores de intereses controvertidos, y el debate del aporte científico estará movido por esos intereses. A su vez, las partes de un litigio, buscan lograr que se imponga su versión como verdad oficial y se derive de allí una decisión que dirima la contienda en forma favorable a sus intereses (cosa juzgada). En el caso del Ministerio Público, su posición como parte en un proceso debe ser matizada mediante el deber de actuación objetiva.

Un aspecto importante del problema referido al uso de la ciencia en el proceso penal es que la ciencia normalmente representa una fuente de conocimiento y de valoración de los hechos de la causa. Es decir, las pruebas científicas son una prueba más, y pueden combinarse con las pruebas ordinarias (no científicas), para precisar el grado de veracidad de un enunciado vinculado con el hecho controvertido.

6. Informática forense, evidencia y evidencia digital

6.1. La evidencia y sus funciones

El campo principal de la labor de las diversas disciplinas forenses es el de la búsqueda, análisis y/o interpretación de *evidencia*. Aunque en Criminalística, los términos *evidencia* e *indicio* funcionan como sinónimos, es conveniente utilizar sólo el primero de ellos. Las ciencias forenses consideran evidencia o indicio a *todo objeto, marca, huella, señal, vestigio*, es decir, todo aquello que deja la realización de un delito como testigo de haber acontecido. Para la Criminalística, indicio es toda evidencia física que tiene estrecha relación con la comisión de un hecho presuntamente delictuoso, cuyo examen o estudio proporciona las bases científicas para encaminar con buenos principios la investigación y lograr fundamentalmente: a) la identificación del o los autores, b) las pruebas de la comisión del hecho y c) la reconstrucción del mecanismo del hecho[17]. Edmond Locard se refería a los indicios como los testigos mudos que no mienten[18].

Desde el ámbito jurídico procesal, en cambio, se asigna al término indicio un sentido más afín con el lenguaje común. Según el Diccionario de la Lengua Española, un indicio es un fenómeno que permite conocer o inferir la existencia de otro no percibido. Un indicio es un signo aparente y probable de que existe alguna cosa y a su vez es sinónimo de seña, muestra o indicación[19]. En el marco de un litigio, los indicios son *hechos contingentes* que permiten inferir la existencia de

[17] Montiel Sosa, J. (2003) Manual de Criminalistica. Ed. Limusa. Grupo Noriega Editores. México D.F. p.49.
[18] Moreno González, L. (1977) Manual de introducción a la Criminalística. Ed. Porrúa, S. A. México.
[19] García Pelayo y Gross, R. (1974) Pequeño Larousse Ilustrado. Ed. Larousse. México. p. 573.

los hechos principales (aquellos que constituyen el objeto de controversia).

La denominada *prueba indiciaria* posee tres elementos: un hecho comprobado (hecho indicador, de carácter contingente), una operación lógica o juicio de razonamiento y, como fruto de este razonamiento, un hecho indicado (aquél que se pretende probar y forma parte del objeto de la controversia). En el marco procesal, una evidencia requiere su adecuada presentación y/o análisis para transformarse en fuente de indicios. Son los testigos y los expertos (y posteriormente los litigantes en sus alegatos) quienes hacen "hablar" a las evidencias, dotándolas de un valor indiciario más o menos convincente.

Desde el punto de vista procesal, las evidencias pueden cumplir esencialmente dos funciones:

- Función orientadora: la evidencia proporciona una pista o hilo conductor que permite avanzar en una investigación. La pista por sí misma no necesariamente acredita un extremo del hecho investigado. Un ejemplo de ello es la obtención de una dirección IP que conduzca luego a un domicilio físico.
- Función probatoria: la evidencia puede ser invocada como prueba de los hechos que afirma una de las partes del proceso. Por ejemplo: un archivo de video que aparece captando una colisión vehicular o un intento de cohecho.

Una evidencia puede cumplir sucesivamente ambas funciones. Es relevante recordar que cuando se pretende emplear evidencia en función probatoria, deben haberse cumplido los requisitos de relevancia, suficiencia, confiabilidad y validez de esa prueba.

En este marco cabe decir que la incorporación de las tecnologías de información a la vida cotidiana ha marcado la necesidad de incluir a los medios informáticos como

elementos de carácter investigativo y/o probatorio, y, a su vez, la obtención, examinación, análisis, interpretación y presentación de esta clase de evidencia, ha requerido del auxilio de expertos en la temática.

6.2. Informática forense y evidencia digital

La Informática Forense es considerada una rama de las ciencias forenses que se encarga de adquirir, analizar, preservar y presentar datos que han sido procesados electrónicamente, y almacenados en un medio digital. Es el uso de las Tecnologías de la Información para recuperar evidencia digital.

Existen distintas fases y modalidades de actuación relacionadas con la informática forense que, a lo largo de un proceso penal, llevan a cabo expertos, investigadores y profesionales del derecho. Por ejemplo, la planificación previa, la identificación, recolección, validación, análisis, interpretación, documentación y presentación de la evidencia digital para ayudar a esclarecer y/o probar sucesos de naturaleza delictiva.

Con el desarrollo de esta disciplina se ha trabajado sobre su principal objeto de estudio: la evidencia digital. El término evidencia se suele asociar con elementos físicos, que se pueden captar con los sentidos, es así que al mencionar “evidencia”, naturalmente hace referencia a la “evidencia física”. Ello pareciera ser contrastante con el término “evidencia digital”, por cuanto, todo aquello relacionado con el término “digital” se ha asimilado al término “virtual”, es decir, como no real. Es de importancia destacar que los datos o evidencia digital siempre están almacenados en un soporte real, siendo este último de tipo físico, por lo que esta clase de evidencia podría considerarse igualmente física.

Se puede concluir entonces, que *la evidencia digital es un tipo de evidencia física construida de campos magnéticos y pulsos electrónicos, que por sus características deben ser*

recolectados y analizados con herramientas y técnicas especiales.

A modo de ejemplo, se mencionan algunos elementos que pueden convertirse en evidencia digital:

- Un archivo en un medio de almacenamiento
- Una línea de texto en un log de transacciones
- El registro de acceso a un sitio web
- Datos en el registro de auditoría de una aplicación
- Datos de una ocurrencia en los registros de eventos del sistema

La labor de los informáticos forenses gira principalmente alrededor de la *evidencia digital*, en cuanto *fuente de información de valor almacenada o transmitida en una forma binaria.*

El cometido del experto o técnico informático será, entonces, la correcta recuperación de toda la información posible, tanto visible como oculta, relacionada con el hecho de estudio, aplicando las técnicas y herramientas disponibles o desarrolladas ad hoc, y garantizando un proceso reproducible de adquisición, examen, análisis, cotejo, preservación y presentación de la evidencia, que fortalezca su valor probatorio ante los órganos jurisdiccionales.

La confiabilidad de la evidencia digital como prueba estará dada por algunos aspectos básicos: ¿Cómo se obtuvo?, ¿Cómo se conserva? y ¿Quién lo realizó?

Para el investigador judicial, el objetivo del hallazgo de la evidencia es establecer un vínculo entre la escena, la víctima y el victimario. Este esquema resulta útil aún en casos complejos (por ejemplo, con pluralidad de escenas, sospechosos y/o víctimas, etc.). En lo que hace a la informática forense, los principios de la criminalística, que se detallaron con anterioridad en este capítulo, operan bajo

modalidades sumamente variadas, incluso, la “escena del hecho” puede llegar a estar diseminada en diferentes lugares físicos, constituyendo entre todos ellos una escena virtual. No sólo el contenido visible de un documento, sino también los metadatos, registros del sistema y otras clases de evidencia digital, pueden ser relevantes para descubrir y/o probar los vínculos entre los distintos aspectos de un suceso. Ahora bien, los diversos rastros digitales que deja el contacto entre escena, víctima y victimario (intercambios en los cuales también interactúan otras variables, tales como momentos, instrumentos, objetos y consecuencias) requieren de un análisis complejo para poder reconstruir esta vinculación.

La aplicación forense de la informática proporciona los principios y técnicas aplicables para identificar, obtener, analizar e interpretar la evidencia digital durante una investigación. La evidencia se convierte luego en elemento material probatorio cuando el perito la somete a examen, pues de manera separada, evidencia, dictamen pericial y testimonio del perito, serán cada uno, elemento material probatorio. La presentación de estos en audiencia pública ante autoridad judicial y contradicción de las partes será la prueba.

7. Conclusiones

La Informática Forense, entendida como la ciencia de adquirir, analizar, preservar y presentar datos que han sido procesados electrónicamente y almacenados en un medio computacional, concepto que se profundizará más en esta publicación, es el nuevo e importante socio que tiene la Criminalística. La dinámica de la evolución humana y su avance tecnológico, han aportado un nuevo paradigma en la materia, generando nuevas escenas de crimen de características virtuales que concurren con las físicas; nuevas escrituras que no son sobre soporte papel y a las que no es posible aplicarles el método scopométrico que tan buenos resultados ha dado a la Documentología. La digitalización de la información ha hecho que ya no se deba buscar un rastro

de una huella con un reactivo químico o magnético, sino con complejas herramientas computacionales que buscan ese indicio escondido, ese rastro, en un código binario que genera complejos laberintos digitales de información. De la pronta adaptación y capacidad de respuesta que tengan los operadores judiciales a este cambio social, dependerá que en muchos procesos penales se pueda acceder a prueba de carácter crucial para la averiguación y juzgamiento de una creciente cantidad de hechos, donde los medios de almacenamiento digital actúan de testigos mudos.

Capítulo 2. Aspectos Legales. Los Delitos Informáticos

Autor: Sabrina B. Lamperti

1. Consideraciones preliminares.
2. ¿Qué son los delitos informáticos? Regulación Europea y Argentina. 2.1. El Convenio de Cibercriminalidad de Budapest. 2.2. La regulación de los Delitos Informáticos en Argentina.
3. Delito transnacional. Jurisdicción y competencia.

1. Consideraciones Preliminares

¿Cuándo un hecho es delito?

Un hecho es delito cuando es jurídicamente relevante. Esto quiere decir que un suceso cualquiera para que sea delito debe estar legislado en un Código Penal; se dirá, entonces, que el *hecho* encuadra en un *tipo penal.* A esta situación se lo conoce como *principio de legalidad* y tiene como consecuencia para el juez la prohibición de castigar aquellas conductas que no estén estrictamente contenidas en la ley penal.

Existe también otra prohibición en el derecho penal y es la proscripción de la aplicación de la analogía. La *analogía* consiste en aplicar una norma jurídica a un caso que no está incluido en el tenor literal de la norma pero que resulta muy similar a los que sí están previstos en ella, de forma que se le da el mismo tratamiento jurídico. Mientras que en otras ramas del ordenamiento jurídico la analogía es utilizada por el juez como método de integración del Derecho para completar las lagunas legales, en Derecho Penal la analogía está prohibida.

Del principio de legalidad penal solo se deduce la prohibición de la analogía cuando se use para condenar o agravar la responsabilidad penal, lo que se conoce como *"prohibición de la analogía in malam partem"*. Pero no se opone, sin embargo, al principio de legalidad el uso de la analogía favorable al reo, es decir, para excluir o atenuar su responsabilidad (*analogía in bonam partem*), pues ello no viola ninguna garantía del ciudadano.

La prohibición de la analogía incluye tanto el hecho de completar el texto legal en forma de entenderlo como prohibiendo lo que la ley no prohíbe, como el considerar antijurídico lo que la ley justifica, o reprochar lo que la ley no reprocha.

Se entiende que sólo el Estado al legislar es capaz de determinar en qué casos va a intervenir para solucionar el

conflicto con el fin de dar respuesta, penalizando a quienes realicen esas conductas para que, siéndoles reprochables, puedan ser juzgados penalmente.

Se destaca así la importancia de los temas a tratar en este capítulo, principalmente tipificación de los delitos informáticos existentes en el Código Penal argentino. La adecuación de las normas sustantivas y procedimentales en cada Estado resulta necesaria a los fines de lograr una efectiva persecución penal y la posibilidad de sanción de los autores de dichos delitos.

Resulta también importante destacar que en la legislación argentina se investigan conductas cometidas por individuos (personas físicas) y no por personas jurídicas. El derecho penal garantiza que no se sancione a las personas por lo que son o por lo que piensan, sino por acciones humanas que afecten bienes jurídicos de terceros. En consecuencia, se entiende que las personas jurídicas no son capaces de conducta y apoyan esta afirmación en normas de jerarquía constitucional (arts. 18, 19, 75, inc. 22, de la Constitución Nacional y arts.11, 2° párrafo de la Declaración Universal de los Derechos Humano; el art. 15 del Pacto Internacional de Derechos Civiles y Políticos, y el art. 9 de la Convención Americana de Derechos Humanos).

No obstante existen ciertas leyes especiales (que no integran el Código Penal) que aplican penas o sanciones a personas jurídicas por ciertos delitos, como por ejemplo la ley 19.359 de régimen penal cambiario, el código aduanero (ley 22.415), la ley de lavado de dinero 26.683, la de delitos bursátiles 26.733 y la ley 26.735 que reforma la legislación penal tributaria. Las penas que establecen no son las mismas que para una persona física. Se aplican algunas como multas, suspensión de actividades, cancelación de la personería, pérdida de beneficios estatales, etcétera.

Aunque ciertas convenciones internacionales a las cuales el país adhirió, prevén la posibilidad de aplicar

sanciones a las personas jurídicas, no exigen que éstas sean estrictamente penales, sino que admiten la posibilidad de que sean de índole administrativa o civil.[20]

Debe hacerse mención a otra cuestión de la parte general del Código Penal, y que guarda relación con el ***ejercicio de las acciones***, esto es, qué delitos pueden ser perseguidos de oficio y cuáles requieren de la intervención de la víctima.

En un lenguaje corriente el *ejercicio de las acciones* puede ser definido como el poder de poner en funcionamiento la actividad del órgano que dice el derecho (el tribunal, el juez) para lograr que se pronuncie (dicte sentencia) sobre hechos que, quien tiene ese poder, estima que son delito[21].

La acción penal es por regla general, de carácter *público y oficial.* Que tenga ***carácter público*** significa que la lleva adelante un órgano del Estado (Ministerio Público Fiscal), y que sea de ***carácter oficial*** significa que el órgano público tiene el deber de promoverla y llevarla adelante, sin que pueda abstenerse de hacerlo por razones de discrecionalidad.

El principio general de que las acciones penales son públicas está consagrado en el art. 71 del CP, que dice:

> *"Sin perjuicio de las reglas de disponibilidad de la acción penal previstas en la legislación procesal, deberán iniciarse de oficio todas las acciones penales, con excepción de las siguientes: 1°. Las que* ***dependieran de instancia privada****. 2° Las* ***acciones privadas****". Dichas excepciones están descriptas en el art 72 y 73 del C.P. e implican:*

[20] Sitio web "Pensamiento Penal". Accesible: junio 2016. Disponible en: http://www.pensamientopenal.org.ar/la-responsabilidad-penal-de-las-personas-juridicas/

[21] Zaffaroni, E. R.l (2003); *Manual de Derecho Penal. Parte general*. Edit. EDIAR. 6° edición, 3ra. reimpresión, pág. 647.

- ***Acciones dependientes de instancia privada:*** son acciones procesales públicas que se hallan sometidas a la condición de que el agraviado o su representante formule la correspondiente denuncia. En estos casos "no se procederá a formar causa sino por acusación o denuncia del agraviado o de su tutor, guardador o representantes legales. Sin embargo, se procederá de oficio cuando el delito fuere cometido contra un menor que no tenga padres, tutor ni guardador, o que lo fuere por uno de sus ascendientes, tutor o guardador.
  - El art. 72 dispone que son acciones dependientes de instancia privada las que nacen de los delitos de "abuso sexual" (art. 119 CP), "estupro" (art. 120 C.P.), y "rapto" (art. 130 C.P.) cuando no resultare la muerte de la persona ofendida o lesiones de las mencionadas en el artículo 91.
  - Las lesiones leves, sean dolosas o culposas. Sin embargo, en los casos de este inciso se procederá de oficio cuando mediaren razones de seguridad o interés público.
  - Impedimento de contacto de los hijos menores con sus padres no convivientes.
- ***Acciones privadas[22]:*** Corresponden a un grupo de delitos en que, si bien como en cualquier otro existe un interés público en que sean penados, este interés se ajusta al del damnificado expresado en forma sostenida a lo largo del proceso, en razón de que afectan una esfera muy íntima de bienes jurídicos, respecto de la que no resulta suficiente que el damnificado manifieste su voluntad de poner en movimiento la acción, sino que debe llevarla adelante, como expresión de una permanencia en ese propósito.

[22] Ídem, pág. 648.

- En todos los casos de delitos de acción privada, sólo se procede por querella del agraviado o de sus guardadores o representantes legales.
- La diferencia con los delitos dependientes de instancia privada es que en éstos -una vez hecha la denuncia, el denunciante no puede detener a la acción penal-, mientras que cuando son delitos de acción privada, en cualquier momento el damnificado puede desistir de la querella.
- Los **delitos de acción privada** están previstos en el art. 73 del C.P. y son:
  - Calumnias e injurias;
  - **Violación de secretos, salvo en los casos de los artículos 154 y 157**[23];
  - Concurrencia desleal, prevista en el artículo 159;
  - Incumplimiento de los deberes de asistencia familiar, cuando la víctima fuere el cónyuge.
  - Asimismo, son acciones privadas las que de conformidad con lo dispuesto por las leyes procesales correspondientes, surgen de la conversión de la acción pública en privada o de la prosecución de la acción penal por parte de la víctima.
  - La acción por calumnia e injuria, podrá ser ejercitada sólo por el ofendido y después de su muerte por el cónyuge, hijos, nietos o padres sobrevivientes.
  - En los demás casos, se procederá únicamente por querella del agraviado o de sus guardadores o representantes legales.

La importancia de esta cuestión sobre el *ejercicio de las acciones* radica en que algunos de los delitos que se

[23] Resaltado del autor.

explicarán a continuación -concretamente los que corresponden al Capítulo III del Código Penal ***(Violación de secretos y de la privacidad)***-, **se encuentran precisamente dentro de los enumerados por el art. 73 del C.P como delitos de acción privada**, lo que implica que no pueden ser perseguido de oficio por los poderes públicos (Policía, Jueces de Instrucción o Ministerio Público Fiscal), sino que es necesaria la intervención activa de la víctima como impulsora de la acción de la justicia y como parte en un tipo de proceso judicial que suele denominarse como *querella*.

El fundamento de ello, estiman algunos autores, corresponde a que la intervención penal debe ser mínima y que no corresponde su prosecución por parte del Estado en este tipo de casos donde el bien jurídico en juego es la privacidad, quedando reservada a la víctima el ejercicio de la acción[24].

En este sentido se ha expresado la Sala VII de la Cámara Nacional de Apelaciones en lo Criminal y Correccional[25] -citando a Palazzi- al establecer

> *"La falta de inclusión del novel tipo penal –acceso ilegítimo a un sistema o dato informático-, entonces, en las excepciones de los arts. 154 y 157, parece pauta más segura que aquella que se vincula con el título del capítulo, máxime frente a la aproximación del tipo en estudio, en algunas características, con una de las figuras del art. 153 –violación de correspondencia electrónica-, cuyo ejercicio de la acción también es privado (Palazzi, Pablo A., Los delitos informáticos*

[24] En este sentido: Riquert, M. (sf); *"Violación de secretos y de la privacidad"* en Revista Pensamiento Penal online http://www.pensamientopenal.com.ar/system/files/cpcomentado/cpc37761.pdf pág. 17/8. Accesible: julio 2016.

[25] Cámara Nacional de Apelaciones en lo Criminal y Correccional - Sala 7 - CCC 70199/2013/CA1 - "B., R. Inadmisibilidad de querella. Violación de sistema informático." Correccional 1/52. Disponible en: http://www.pensamientopenal.com.ar/system/files/2014/12/Fallos39045.pdf

en el Código Penal. Análisis de la ley 26.388, Abeledo-Perrot, Buenos Aires, 2009, p. 78).

También ha sostenido la jurisprudencia que no es posible realizar una extensión analógica de las excepciones previstas en el artículo 73 del Código Penal, ello debido a la prohibición de la analogía en contra del imputado, y de esta forma han afirmado que

> *"La circunstancia de que no se hubiera modificado el artículo 73 en oportunidad de la mencionada reforma legislativa, no puede llevar a sostener, por vía de interpretación, que el tipo penal acuñado en el artículo 157 bis se encuentre comprendido en la excepción de esa norma, esto es, asimilado a los supuestos de los artículos 154 y 157"*[26]

Además, explican que

> *"la razón por la que se exceptuó a los delitos de abuso de cargo (154) y violación de secreto oficial (157) de la regla general en virtud de la cual todos los hechos alcanzados por el Capítulo III son de acción privada, es bien la prestación de un servicio de interés público, como es el correo, o la calidad de funcionario público del sujeto activo".*

Por lo tanto, cualquier denuncia vinculada a alguno de estos delitos que sea tramitada de oficio por los organismos encargados de la persecución penal, es pasible de ser declarada nula por instancias ulteriores, como aconteció en un caso resuelto por la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal, Sala VII[27], que determinó

---

[26] Cámara Nacional de Apelaciones en lo Criminal y Correccional - Sala IV - "S.D.L., J.A. s/ Infracción art. 157 bis del C.P." - Causa n° 2.079/11 - 8/3/2012. Accesible: julio 2016. Disponible en: http://judicialdelnoa.com.ar/jurisprudencia/fallo_sldja_ccc.pdf

[27] Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal, Sala VII - "R, P.M. s/ Violación de secretos". Inst. 43/109. Accesible: julio 2016. Disponible en: http://www.pjn.gov.ar/Publicaciones/00017/00051999.Pdf

"...la violación de secretos denunciada (art. 157 bis de la ley sustantiva) imponía el ejercicio de la acción privada que establece el artículo 73, inc. 2°, ibídem -la figura aplicable escapa a las excepciones de los arts. 154 y 157 que trae la norma-, extremo que no se advierte verificado siquiera a partir del pronunciamiento del más Alto Tribunal, al dirimir el conflicto negativo de competencia suscitado en estas actuaciones. De tal suerte, sólo es posible convenir en que el vicio relativo al ejercicio de la acción penal acarrea la nulidad de lo actuado de forma oficiosa a partir de la decisión asumida por la Corte Suprema de Justicia de la Nación, que definió la significación jurídica de los hechos y, por añadidura, el carácter privado de la acción que de aquéllos se deriva"

Si bien es mayoritario este fundamento, otros autores[28] entienden que deberá diferenciarse si la acción es privada o pública de acuerdo al carácter de la información almacenada en los bancos de datos, ya que si éstos son públicos la acción debería ser de naturaleza pública y promovible de oficio.

La cuestión no ha quedado subsanada ni aclarada por el legislador en la reciente reforma del art. 73 del CP por la Ley N° 27.147, vigente desde el 26 de junio de 2015, al no haber reformulado el inciso 2°, por lo que se entiende que siguen siendo de acción privada, no pudiéndose aplicar un criterio analógico extensivo en perjuicio de persona alguna sin que la justicia pueda llenar el vacío legal que quedó latente para algunos supuestos donde intervengan funcionarios públicos o donde la información sea de una base de datos pública.

Otro de los conceptos de la parte general del derecho penal que resulta relevante explicar para luego comprender su aplicación, tiene que ver con el ***bien jurídico protegido.*** A nivel doctrinario legal, no se ha encontrado una definición única, por lo que se selecciona la del autor Von Listz, que indica

[28] Buompadre, Jorge E.; "Manual de Derecho Penal. Parte Especial", Astrea, Bs.As., 2013, pág. 382.

"...se denomina bienes jurídicos a los intereses protegidos por el Derecho. Bien jurídico es el interés jurídicamente protegido. Todos los bienes jurídicos son intereses vitales del individuo o de la comunidad. El orden jurídico no crea el interés, lo crea la vida; pero la protección del Derecho eleva el interés vital a bien jurídico"[29].

La parte especial del Código Penal argentino expone cada uno de las acciones que van a constituir delito, a esto se lo llama **"tipificación de una conducta"**. Cada una de estas descripciones se encuentra agrupada por "Títulos" bajo algún tipo de "bien jurídico protegido", es decir bajo alguno de los intereses a los que el Estado decide darle relevancia para la vida en sociedad.

Es así que, de los distintos delitos informáticos que están tipificados, algunos de ellos se encuentran amparados por el bien jurídico "integridad sexual", o "libertad", o "patrimonio", por nombrar ciertos ejemplos.

Finalmente, resulta importante mencionar definiciones que tienen que ver con la forma en que se llevan a cabo los delitos por parte de los autores, es decir, si el delito fue cometido con o sin intención, y que constituye lo que en derecho se denomina "aspecto subjetivo del tipo penal". Se clasifica entonces a los delitos en **dolosos o culposos.** Para diferenciar a ambos en un caso en concreto es relevante tener en cuenta la voluntad del autor en cometer y querer producir el resultado del delito en particular (por ej.: la *intención* de estafar, o el *querer* dañar una cosa). Esa es la diferencia con la culpa, donde el resultado puede producirse aún sin intención, sea por negligencia o imprudencia al momento de llevar a cabo la acción.

[29] VON LISZT, F. (1999) Tratado de Derecho penal, trad. de la 20a ed. alemana por Luis Jiménez de Asúa, adicionado con el Derecho penal español por Quintilliano Saldaña, t. II, 4a ed., Reus, Madrid. p. 6.

Existe un caso intermedio que es el *dolo eventual* y que puede darse cuando el autor se imagina que puede ocasionar un daño, pero actúa igual pensando que ese daño no va a acontecer. Se explica fácil con un caso de accidente de tránsito, los que usualmente son "culposos" porque se actúa con negligencia o imprudencia. Sin embargo, hay situaciones -como ocurre con las *picadas*- en que quien conduce el automotor excediendo un riesgo permitido (límite de velocidad) sabe que puede ocasionar un daño, y sin embargo confía en que si se le presenta la situación de atropellar a una persona, va a realizar una buena maniobra para evitar el resultado dañoso.

La mayoría de los delitos que se explicarán en este capítulo son *dolosos*. Sin embargo, cuando se mencione que en la ley se diga "si el hecho se cometiere por imprudencia o negligencia" hay que pensar en que el autor lo comete de forma *culposa.* También habrá casos en que se aplique el *dolo eventual.*

2. ¿Qué son los Delitos Informáticos? La regulación Europea y Argentina

Si bien existen algunas controversias doctrinarias en la definición de lo que constituyen delitos informáticos, distintos autores han brindado definiciones tales como

> *"aquel que se da con la ayuda de la informática o de técnicas anexas"; o "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de acción criminógena"; o bien: "cualquier conducta criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y, en un sentido estricto, el delito informático, es cualquier acto ilícito penal, en*

el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".[30]

El Departamento de Justicia de los Estados Unidos de América los ha definido como *"cualquier acto ilegal que requiera el conocimiento de tecnología informática para su perpetración, investigación o persecución".*[31]

En general existe consenso en reconocer una clasificación de los delitos informáticos que guarda relación con la definición más usual -o en sentido amplio- que de ella se puede dar. Se definen los delitos informáticos como *aquellas conductas que: a) atacan a las propias tecnologías de la computación y las comunicaciones; b) incluyen la utilización de tecnologías digitales en la comisión del delito; o c) incluyen la utilización incidental de las tecnologías en la comisión de otros delitos,* y, en consecuencia, la computadora pasa a ser una fuente de datos digitales probatorios.

3. El Convenio de cibercriminalidad de Budapest

Resulta de relevancia para la materia -por tratarse del más destacado acuerdo internacional desarrollado al efecto-, la mención al ***Convenio de cibercriminalidad de Budapest (Hungría)*** elaborado por el Consejo de Europa en dicha localidad el 23 de noviembre de 2001.

A través de éste, tanto países europeos como otros países adheridos establecieron el Convenio de cibercriminalidad[32], entendiendo que debían ponerse de

[30] Huilcapi Peñafiel, A. O. (2010) "El delito informático", en el que se citan autores tales como Nidia Callegari, Carlos Sarzana y María de Luz Lima; citado por Tobares Catalá, Gabriel H.-Castro Argüello, Maximiliano J.; *"Delitos Informáticos"*, Edit. Advocatus. pág. 28.

[31] Tobares Catalá, G. H. (2010) Delitos Informáticos; Edit. Advocatus. nota 23 de la página 28.

[32] Versión online disponible en: http://conventions.coe.int/Treaty/en/Treaties/html/185-SPA.htm. Accesible: junio de 2016.

acuerdo sobre algunas cuestiones básicas de la política penal de cada país participante, con miras a prevenir la criminalidad en el ciberespacio y, en particular, de hacerlo mediante la adopción de una legislación apropiada uniforme de manera que las conductas sean susceptibles de ser investigadas por cualquiera de estos Estados. Asimismo reconocieron la necesidad de una cooperación entre los Estados y la industria privada en la lucha contra la cibercriminalidad y la necesidad de proteger los intereses legítimos vinculados al desarrollo de las tecnologías de la información.

Los principales objetivos del Convenio apuntan a la introducción de conductas tipificadas (es decir, a establecer cuáles de ellas serán ilícitas) así como a establecer las medidas procesales idóneas para su esclarecimiento, y a la coordinación y cooperación entre las policías y administraciones de los países que se adhieran al mismo. En este capítulo se analizará lo atinente a las conductas tipificadas sea a nivel internacional como nacional, dejando el análisis de la faz procesal y de cooperación para el siguiente.

En primer lugar, se especificaron algunas cuestiones terminológicas vinculadas con las definiciones de *sistema informático, datos informáticos, prestador de servicio y datos de tráfico*. Luego, en cuanto a la clasificación de los delitos informáticos, se estableció la existencia de las siguientes categorías: 1) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; 2) Infracciones informáticas; 3) Delitos vinculados al contenido; 4) Delitos vinculados a violación de la propiedad intelectual y otros derechos afines.

Se detallan a continuación cuáles son las acciones contempladas en este Convenio y que resultan de importancia para su análisis ya que cualquier Estado que pretenda unirse

a él, deberá adecuar primeramente su regulación de conformidad con lo aquí establecido.[33]

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Bajo este título se Incluyen cinco tipos penales, a saber:

1. Acceso ilícito

Es el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Puede cometerse infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

2. Interceptación ilícita

Constituye la interceptación deliberada e ilegítima -por medios técnicos- de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático, o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. El delito puede cometerse con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

3. Ataques a la integridad de los datos

Es todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos, pudiendo legislarse sobre la gravedad de los daños que se ocasionen.

4. Ataques a la integridad del sistema

Consiste en la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático

[33] Cabe destacar que al presente (diciembre 2016) la República Argentina no se encuentra dentro de los Países ratificantes del Convenio de Cibercriminalidad de Budapest.

mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

5. Abuso de los dispositivos

Se trata de la comisión deliberada e ilegítima de los siguientes actos:

a) la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos antes descriptos; como también de una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos antes descriptos.

b) la posesión de alguno de los elementos contemplados precedentemente con la intención de que sean utilizados para cometer cualquiera de los delitos descriptos.

Infracciones informáticas

1. Falsificación informática

Dirigida a sancionar la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Puede exigirse una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.

2. Fraude informático

Penaliza los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: la introducción, alteración, borrado o supresión de datos informáticos; o por

cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

Delitos relacionados con el contenido

1. Delitos relacionados con la pornografía infantil

Orientada a penalizar la comisión deliberada e ilegítima de los siguientes actos:

a) La producción de pornografía infantil con la intención de difundirla a través de un sistema informático;
b) La oferta o la puesta a disposición de pornografía infantil a través de un sistema informático;
c) La difusión o la transmisión de pornografía infantil a través de un sistema informático;
d) La adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático;
e) la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

También se regula lo que se entenderá por «pornografía infantil» como todo material pornográfico que contenga la representación visual de: un menor adoptando un comportamiento sexualmente explícito; una persona que parezca un menor adoptando un comportamiento sexualmente explícito; de imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.

De igual forma se hace mención de lo que debe entenderse por «menor» como toda persona que no tiene aún 18 años de edad, que los Estados al legislar pueden reducir al límite de los 16 años.

Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

1. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Se pretende legislar las infracciones de la propiedad intelectual que defina cada Estado conforme a las obligaciones que hayan contraído por aplicación del Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor -a excepción de cualquier derecho moral otorgado por dichos Convenios-, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

También se regulan las infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas -a excepción de cualquier derecho moral conferido por dichos Convenios-, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

Finalmente, en cuanto a la legislación de fondo que se ha descripto, la Convención establece que la comisión de todos los tipos previstos por ésta, debe ser penada por los Estados miembros, no sólo con relación a su autor, sino que también se debe castigar su ayuda y su instigación. El castigo de dichos delitos se debe realizar mediante sanciones efectivas, proporcionadas y disuasivas, que pueden llegar a incluir la privación de la libertad.

Asimismo, se estipula la posible responsabilidad de las personas jurídicas para su beneficio y cuando es cometido por cualquier persona física que actúe individualmente o como parte de un órgano de la persona jurídica que tenga una posición importante en virtud de un poder de representación de ésta, o tenga facultades para tomar decisiones en su nombre o para ejercer controles dentro de ella. La responsabilidad puede ser civil, administrativa o penal, sin perjuicio de la responsabilidad penal que corresponda a las personas físicas que cometieron el delito.

4. La regulación de los Delitos Informáticos en Argentina[34]

En Argentina, el 4 de junio de 2008 se sancionó la ley 26.388 -promulgada el 24 de junio del mismo año-, por medio de la cual se realizaron reformas e incorporaciones de algunos artículos del Código Penal, denominándose a ésta como la *"ley de delitos informáticos"* siendo la de mayor avance en la temática. No obstante existen -desde antes de su puesta en marcha- otras normativas por fuera del Código Penal que regulan conductas donde la tecnología es protagonista. Asimismo, en el año 2013 se sancionó la Ley 26.904 incorporando al mencionado Código el delito de *grooming* (o acoso informático contra menores de edad).

A continuación, se describen cada una de ellas.

- ***Cuestiones terminológicas***

El primer artículo en ser reformado es el 77 del digesto, incorporando nuevas definiciones y adaptándolas a las nuevas tecnologías. De este modo, el término "documento" comprende toda representación de actos o hechos, con

[34] Sitio web *Infoleg* del Ministerio de Economia de la Nacion Argentina. Accesible: junio 2016. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

- ***Delitos contra la integridad sexual***

1. Ciberpornografia infantil

Se modifica la redacción del artículo 128 del Código Penal que reprime el ***delito de pornografía infantil***, habiendo sido sustituido por el siguiente:

> *"Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.*
>
> *Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.*
>
> *Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años."*

Se advierte la incorporación de otros verbos típicos respecto de la redacción original: a la "producción" y "publicación" de imágenes "pornográficas" se incluye a quien financie, ofrezca, comercie, facilite, divulgue o distribuya, por cualquier medio (con lo que queda incluida aquellas que se realicen a través de medios informáticos), ampliando asimismo lo atinente a las imágenes, que ya no se definen como "pornográficas" sino como *"toda representación de un*

menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales", siendo ésta acorde con la normativa internacional a la que adhirió la Argentina[35].

El segundo párrafo agregado a la redacción anterior contempla la posibilidad de perseguir a quien tenga en su poder representaciones de las descriptas, siempre que sea con *fines inequívocos de distribución o comercialización*. Tal acción es posible llevarla a cabo, por ejemplo, por medio de redes P2P o de cualquier sistema de intercambio de archivos.

Resulta importante destacar que quedan fuera de la punición los simples poseedores de imágenes pornográficas que no hagan intercambio, es decir, la sola tenencia del material sin fines de distribución o comercialización, cuestión que difiere en lo sustancial a una de las modalidades que describe la Convención de Cibercriminalidad de Budapest analizada anteriormente[36]. En lo práctico, esto implica que

---

[35] El "Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía" (dictado por la Asamblea General de las Naciones Unidas el 25-05-2000, al que adhirió la Argentina mediante la sanción de la Ley 25763) establece en su artículo 2° que: *"Por utilización de niños en la pornografía se entiende toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales."* Texto completo disponible en: http://www.unicef.org/spanish/specialsession/documentation/documents/op_se_sp.pdf

[36] El dictamen del Senado de la Nación (OD 959/2007) al momento de expedirse explica así estos cambios: "No se consideró conveniente reprimir con la misma pena a quien distribuyera representaciones de las descriptas en el párrafo anterior como a quien las tenga en su poder, ya que son ilícitos de diferente peligrosidad, y asimismo, se vigorizó la idea, en salvaguarda del principio de reserva, de requerir en forma inequívoca la finalidad por parte del autor de proceder ulteriormente a su distribución o comercialización". Ver Tobares Catalá, Op. Cit. pág. 171.

esta conducta que no es penalizada en Argentina, con lo cual no es posible su persecución penal, en cambio, sí lo es en otros países que han adherido a tal Convención.

2. Grooming (Acoso informático contra menores)

A partir del impulso dado por distintas ONG que trabajan en la temática se propulsó la sanción de una ley que penalice la conducta del ciberhostigamiento o ciberacoso. La conducta del grooming[37] la llevan adelante aquellos sujetos adultos que emprenden acciones deliberadas con el objetivo de ganarse la amistad de un menor de edad, buscando crear una conexión emocional con éste, con el fin de disminuir las inhibiciones del niño y, eventualmente, poder abusar sexualmente de él.

La sanción de la Ley 26.904 ha incorporado esta figura al ordenamiento jurídico argentino, quedando redactado de la siguiente forma:

> *'Artículo 131: Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.'*

Las acciones emprendidas por los *groomers* (o pedófilos) suele analizarse en fases. La primera es la del *contacto y acercamiento*, en la cual el abusador se vale de herramientas para engañar sobre su verdadera edad al entrar en contacto con el menor, esto implica la creación de perfiles falsos, con fotos o videos ajenos o adulterados a través de programas informáticos. Durante esta etapa se busca generar confianza y empatía. Posteriormente se despliega el *componente sexual*: el abusador consigue que el menor le envíe alguna fotografía o video con componentes íntimos,

[37] Etimológicamente "grooming" es un vocablo de habla inglesa derivado de la raiz "groom", que alude a conductas de preparación o acercamiento para un fin determinado.

sexuales o eróticos. La fase final es la del *ciberacoso*[38], en tanto si el menor no accede a sus pretensiones sexuales (le requiere envío de más material, más videos o fotografías, o peticiona un encuentro personal), el ciberacosador amenaza con difundir la imagen con mayor carga sexual que haya logrado de la víctima (o una creada a partir de otras imágenes) para su divulgación a través de Internet (plataformas de intercambio de videos, redes sociales, foros u otros) o enviarlas a los contactos personales del menor.

Rovira del Canto[39] señala las siguientes fases del acoso sexual infantil o *child grooming*, a saber: a) fase de amistad; b) toma de contacto, gustos, preferencias, confianza; c) fase de relación; d) confesiones personales e íntimas, consolidación; e) componente sexual; f) participación de actos de naturaleza sexual, fotografías, webcam; g) extorsión; h) escalada de peticiones; i) ¿agresión?

Los abusadores se valen del tiempo para fortalecer e intensificar la relación con los menores, pudiendo transcurrir muchos meses o años incluso, hasta lograr su cometido. La noción del tiempo en los menores es importante ya que permiten pensar que no se trata de un desconocido sino de alguien que se ha convertido en “amigo virtual” y con quien puede compartir su vida cotidiana. Además, los menores resultan engañados sobre “quién” se encuentra detrás del dispositivo que mediatiza la relación, confiando en que se trata de alguien de la misma edad y con intereses en común.

---

[38] A esta fase también se la conoce como “sextorsión”, ya que lo que se produce es una extorsión con material de tipo sexual.

[39] Rovira del Canto, E. (2010) Trabajo para la Primer Jornada TIC sobre Ciberdelincuencia; Disponible en: http://www.iaitg.eu/mediapool/67/671026/data/Ciberdelincuencia_intrusiva_hacking_y_grooming_Enrique_Rovira.pdf Noviembre de 2010. Accesible: junio 2016.

Desde el aspecto estrictamente legal, algunos autores cuestionan la redacción dada al delito ya que requiere una finalidad específica "...*con el propósito de cometer cualquier delito contra la integridad sexual de la misma."* ya que entienden que otras figuras existentes en el Código Penal podrían haber subsumido perfectamente esta nueva modalidad caracterizada por la intervención de las Tics., tal es el caso de lo normado en el artículo 125 del C.P.[40]

Con esta redacción la acción emprendida por el abusador se consuma cuando se establece efectivamente contacto con el menor resultando de este modo manifiesta la intención ilícita de las comunicaciones que mantuvo con éste. No obstante, en aquellas situaciones en que no se llega a concretar el abuso, por ejemplo por interceptación de los mensajes por control parental, podría quedar el delito en grado de tentativa.

Más aún, se discute también acerca de la relación que guarda esta redacción con delitos que ya estaban tipificados -pero cuya modalidad no es de contacto a través de alguna TIC- en cuanto a los niveles de penas. Se ha cuestionado que la pena sea de seis (6) meses a cuatro (4) años, por entenderla como acto preparatorio del abuso sexual infantil llevado adelante de modo tradicional, legislado en el art. 119

[40] **Art. 125 del C.P**. que regula el delito de **promoción o facilitación de la corrupción de menores establece:** *"El que promoviere o facilitare la corrupción de menores de dieciocho años, aunque mediare el consentimiento de la víctima será reprimido con reclusión o prisión de tres a diez años. La pena será de seis a quince años de reclusión o prisión cuando la víctima fuera menor de trece años. Cualquiera que fuese la edad de la víctima, la pena será de reclusión o prisión de diez a quince años, cuando mediare engaño, violencia, amenaza, abuso de autoridad o cualquier otro medio de intimidación o coerción, como también si el autor fuera ascendiente, cónyuge, hermano, tutor o persona conviviente o encargada de su educación o guarda."*

del C.P. y que tiene la misma penalidad para su acción más básica[41].

En un caso suscitado en el Departamento Judicial Necochea en una causa caratulada “F, L.N. s/ Promoción de la Corrupción de Menores agravada por la edad de la víctima y su comisión mediante engaño”[42], los jueces intervinientes resolvieron condenar por diez (10) años de prisión al autor del hecho encuadrándolo en el art. 125 del C.P. párrafo segundo y tercero.

---

[41] **Art. 119 del C.P.** que regula el **abuso sexual infantil**, establece: ***“****Será reprimido con reclusión o prisión de* ***seis meses a cuatro años*** *el que abusare sexualmente de persona de uno u otro sexo cuando, ésta fuera menor de trece años o cuando mediare violencia, amenaza, abuso coactivo o intimidatorio de una relación de dependencia, de autoridad, o de poder, o aprovechándose de que la víctima por cualquier causa no haya podido consentir libremente la acción. La pena será de* ***cuatro a diez años*** *de reclusión o prisión cuando el abuso por su duración o circunstancias de su realización, hubiere configurado un sometimiento sexual gravemente ultrajante para la víctima. La pena será de* ***seis a quince años*** *de reclusión o prisión cuando mediando las circunstancias del primer párrafo hubiere acceso carnal por cualquier vía. En los supuestos de los dos párrafos anteriores, la pena será de* ***ocho a veinte años*** *de reclusión o prisión si: a) Resultare un grave daño en la salud física o mental de la víctima; b) El hecho fuere cometido por ascendiente, descendiente, afín en línea recta, hermano, tutor, curador, ministro de algún culto reconocido o no, encargado de la educación o de la guarda; c) El autor tuviere conocimiento de ser portador de una enfermedad de transmisión sexual grave, y hubiere existido peligro de contagio; d) El hecho fuere cometido por dos o más personas, o con armas; e) El hecho fuere cometido por personal perteneciente a las fuerzas policiales o de seguridad, en ocasión de sus funciones; f) El hecho fuere cometido contra un menor de dieciocho años, aprovechando la situación de convivencia preexistente con el mismo. En el supuesto del primer párrafo, la pena será de tres a diez años de reclusión o prisión si concurren las circunstancias de los incisos a), b), d), e) o f)."*

[42] Duarte, A. (2014) *“Ley de Grooming. ¿Una nueva herramienta para el ciberacoso?”* en Revista del Ministerio Público Provincia de Buenos Aires; Año 11, N° 15, Julio 2014. Págs. 25/8. Disponible en: https://www.mpba.gov.ar/web/revista/RevistaNro15-web.pdf

En dicho caso, la agente fiscal probó y defendió esa calificación legal de corrupción de menores a través de *grooming* en el entendimiento que las nuevas posibilidades de interacción actualmente no requieren la efectiva producción de un resultado corruptor, ya que el delito es el de "promover" o "facilitar" la corrupción de un menor, invitándolo a realizar prácticas que son prematuras para su edad, ya que lo que se castiga es la interferencia en el proceso de formación de la sexualidad o en normal desarrollo de ella.

La fiscal interviniente, a partir de las pruebas colectadas, entendió que el imputado realizó una serie de actos que -analizados como una unidad de sentido bajo la figura del "grooming"- tienen suficiente entidad corruptora.

> *"En efecto, se contactaba con menores de edad utilizando redes sociales y ocultando su verdadera identidad; simulaba en este contacto ser una persona del mismo sexo y edad del menor contactado; tapaba su cámara web para evitar que su verdadera apariencia quede al descubierto, poseía gran cantidad de material de pornografía infantil en su computadora, la que luego enviaba vía correo electrónico a menores de edad, acosando, hostigando, exigiendo respuestas; y realizando proposiciones de explícito contenido sexual a sabiendas de la edad de sus víctimas y del engaño con que había obtenido su atención y/o confianza. Estos actos poseen aptitud, cuanto menos potencial, para inculcar un comportamiento sexual prematuro en una menor de ocho años de edad"*[43].

En síntesis, la autora rescata el reconocimiento del flagelo por parte de los legisladores, pero apunta a no perder de vista que el *grooming* es un medio que persigue como finalidad la de abusar de un menor de edad o la de corromperlo, acciones que ya estaban tipificadas y reprimidas con escalas penales más acordes a la verdadera tutela de los

[43] Duarte, A.; Op. Cit.; pag. 27.

intereses de los menores que resultan víctimas de estas conductas.

Finalmente, resta destacar la omisión de modificación al art. 72 del C.P.[44] que establece qué delitos son perseguibles a instancias del consentimiento de la víctima. De esta forma, mientras en los restantes delitos contra la integridad sexual es la víctima quien decide si habilita el ejercicio de la acción penal (por ejemplo, los previstos en los arts. 119, 120 y 130), en las acciones de grooming que se desplieguen en su contra queda fuera de su ámbito de decisión, pudiendo el Estado ejercer de oficio la investigación penal.

- ***Delitos contra la libertad. Violación de secretos y de la privacidad***

En cuanto a los delitos contra la libertad, se observa una modificación del título del capítulo III, el cual fue ampliado a la violación de secretos y de la privacidad.

Es importante destacar que la mayoría de los delitos que se explican a continuación -a excepción de los arts. 154 y 157-, encuadran dentro de la categoría de **delitos de acción privada** (art. 73 inc. 3° del Código Penal) lo que implica, como ya se ha explicado, que no puede ser perseguido de oficio por

[44] Art. 72 del C.P. establece que *"Son acciones dependientes de instancia privada las que nacen de los siguientes delitos: 1º) Los previstos en los artículos 119, 120 y 130 del Código Penal cuando no resultare la muerte de la persona ofendida o lesiones de las mencionadas en el artículo 91. 2º) Lesiones leves, sean dolosas o culposas. Sin embargo, en los casos de este inciso se procederá de oficio cuando mediaren razones de seguridad o interés público. 3º) Impedimento de contacto de los hijos menores con sus padres no convivientes. En los casos de este artículo, no se procederá a formar causa sino por acusación o denuncia del agraviado, de su tutor, guardador o representantes legales. Sin embargo, se procederá de oficio cuando el delito fuere cometido contra un menor que no tenga padres, tutor ni guardador, o que lo fuere por uno de sus ascendientes, tutor o guardador. Cuando existieren intereses gravemente contrapuestos entre algunos de éstos y el menor, el Fiscal podrá actuar de oficio cuando así resultare más conveniente para el interés superior de aquél"*.

los poderes públicos (Policía, Jueces de Instrucción o Ministerio Público Fiscal), sino que su acción queda reservada a la víctima bajo el proceso de querella.

1. Violación, apoderamiento y desvío de comunicación (art. 153, párrafo 1º CP).

Se sustituye el artículo 153 del Código Penal, por el siguiente:

> *"Será reprimido con prisión de quince (15) días a seis (6) meses el que **abriere o accediere indebidamente** a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se **apoderare indebidamente** de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o **indebidamente suprimiere o desviare** de su destino una correspondencia o una comunicación electrónica que no le esté dirigida (...)"*

Se observa así, la descripción de tres tipos de conducta: a) La violación o acceso indebido de una comunicación; b) El apoderamiento indebido de una comunicación; y c) El desvío o supresión de una comunicación.

Para el primer supuesto es importante destacar la utilización del término "comunicación electrónica" que importa una definición más amplia que la de correo electrónico pudiendo así circunscribir cualquier tipo de intercambio privado, por ejemplo: el acceso indebido a los mails, chats, mensajes de texto o cualquier otro objeto que encuadre en dicha acepción, además de los medios tradicionales de comunicación.

Para el segundo supuesto resulta relevante destacar la utilización del verbo típico "apoderarse indebidamente" ya que de esta forma pueden contemplarse los casos donde es posible apoderarse de un correo mediante su copia pero sin desapoderar a la víctima del original.

También se advierte que se ha hecho hincapié en que el objeto a transmitir puede encontrarse abierto o incluso no resultar necesario que esté destinado a ser transmitido.

En el tercer supuesto que se legisla, que es el de supresión o desvío indebido de correspondencia, se busca penalizar a quien desvía la correspondencia definitivamente no siendo necesaria su destrucción; desviar implica sacar la correspondencia del destino que tenía originalmente o cambiar su curso.

Finalmente, cabe destacar lo que tiene relación con casos de excepción a este encuadre -es decir en qué casos la correspondencia puede ser violada-. Si bien no están legislados en concreto, estos deben ser contemplados a la luz de otras normas existentes y/o deben ser ordenadas por autoridad judicial mediante resoluciones debidamente fundadas. Por ejemplo, en el caso del ejercicio de la patria potestad, tutela o curatela, por razones de control parental. Lo mismo en el caso en que exista acuerdo entre personas donde se haya dado consentimiento expreso para su acceso, transmisión o publicación.

Un caso que genera controversia es el de la existencia o no de privacidad en el ámbito laboral. No existe legislación alguna sobre el acceso al correo electrónico por parte de los empleadores para el monitoreo de sus dependientes como modo de control del rendimiento laboral, o cumplimiento de obligaciones asignadas o de confidencialidad de la información de la empresa que pueden llegar a manejar. Sin embargo, se estima que no encuadra en este delito aquel caso en que el empleador le haya hecho conocer -a través de la firma del contrato laboral- la forma en que debe utilizar el correo corporativo que se le asigne, para qué tipo de contenidos y demás cuestiones que se establezcan entre las partes, con expresa indicación que podrá ser monitoreado y utilizado en caso de algún tipo de uso indebido o fuera de dicho acuerdo.

Por cuestiones procedimentales es importante recordar tanto lo que prevé este artículo del Código Penal como así también el art. 18 de la Constitución Nacional que dispone *"La correspondencia de telecomunicaciones es inviolable. Su interceptación sólo procederá a requerimiento de juez competente"* ya que en el caso en que sea necesario analizar pericialmente los intercambios privados de los dispositivos que se secuestren a los imputados o que sean aportados por las partes en otros procesos judiciales, deberá contarse con el aval del juez interviniente.

2. Interceptación o captación de comunicaciones electrónicas o telecomunicaciones (art. 153, párrafo 2º CP);

   También contemplado en el artículo 153 del C.P.:

   *"En la misma pena incurrirá el que **indebidamente interceptare o captare** comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un (1) mes a un (1) año, si el autor además **comunicare a otro o publicare** el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena".*

La conducta aquí contemplada es la interceptación o captación indebida de comunicaciones. No se trata de conocer su contenido, como ocurre en la modalidad del acceso indebido, sino del despliegue de dispositivos o técnicas que permitan conocer todos los mensajes que entran y salen, o escuchar las comunicaciones de una línea intervenida o leer el tráfico de despachos telegráficos. Este delito fue pensado para perseguir a aquellos autores que realicen tareas de espionaje (gubernamental, empresarial, político, etc.), con el objeto de utilizar los datos para negociar o realizar inteligencia diversa.

Finalmente, se prevé como agravantes de todas las conductas descriptas en el art. 153 del C.P. dos acciones distintas: la de "comunicar", esto es, hacer conocer a un tercero que no participa del delito el contenido de la correspondencia, o "publicarlo", es decir, ponerlo al alcance de un número indeterminado de personas, para lo que se requiere dolo directo o, al menos, eventual. El restante agravante deviene de la calidad del autor, cual es que cualquiera de las conductas fuera realizado por un funcionario público en abuso de aquellas, caso en que se agregará como sanción conjunta la de inhabilitación especial por el doble del tiempo de condena[45].

3. Acceso a un sistema o dato informático

Seguidamente se incorpora el artículo 153 bis al Código Penal, el cual establece el delito de ***acceso indebido a un sistema o dato informático*** que reprime con prisión de quince (15) días a seis (6) meses,

> *"...si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros".*

Lo que busca proteger la norma es el mero intrusismo o acceso informático ilegítimo ya que en sí mismo importa un nivel de riesgo considerable, además de privar al titular de la información a la que se accede de su confidencialidad y exclusividad, lo que vulnera el ámbito de su intimidad como

[45] Gutiérrez, R. y otros; "Art. 153 - Violación de Secretos y de la Privacidad", en Sitio Web de Asociación Pensamiento Penal. Sección Código Penal comentado de acceso libre. Versión online disponible en: http://www.pensamientopenal.com.ar/system/files/cpcomentado/cpc37762.pdf

extensión de los atributos de la persona. En lo específico, supone vulnerar la confidencialidad de la información en sus dos aspectos: exclusividad e intimidad[46].

La acción que se penaliza es la de acceder sin autorización o excediendo la que se tiene a un sistema o dato informático de acceso restringido. Definiciones de *sistema informático*[47] y *dato informático*[48] se encuentran tanto en el Convenio de Cibercriminalidad de Budapest, como en la Ley 25.326 de Protección de Datos Personales.

Con la aclaración "acceso restringido", que establece el artículo se excluye la posibilidad de punir el acceso a redes, sistemas y contenidos de sitios públicos. La restricción podrá ser mediante una contraseña o cualquier otra modalidad limitativa que exprese que se trata de ámbito reservado por el titular. Algunos autores incluyen el acceso a dato "restringido" incluido en un sistema informático de acceso público, como podrían ser datos sensibles[49] de usuarios que se pudieran almacenar en dicho sistema. Otros, también hablan de la

[46] Sáez Capel-Velciov (2008), en su "Comentario al art. 153bis" pub. en AAVV "Código Penal", dirigido por Baigún y Zaffaroni, ed. Hammurabi, Bs.As., Tomo 5. págs. 740.

[47] Sistema informático en la Convención de Cibercriminalidad es definida como *"todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos"*.

[48] Datos informáticos en la Convención *"designa toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función".* En tanto, por *"datos informatizados"* en la Ley 25.326 son descriptos como *"Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado".*

[49] Se denomina *datos sensibles* a aquellos datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. Cfr. Ley 25.326

posibilidad de que el acceso sea total o parcial al sistema.[50] Más allá del universo de casos que podrían darse, y de las discusiones que podrían suscitarse, a nivel doctrinario legal existe cierto consenso sobre que si el sistema posee algún tipo de verificación de identidad para el sistema (identificación y/o autenticación obligatoria), ello sería suficiente para ser considerado restringido.

La modalidad presenta un agravante en aquellas situaciones en que el acceso fuere respecto de un sistema o dato informático de un organismo público estatal o un proveedor de servicios públicos[51] o de servicios financieros. La distinción aparece razonable y, en consecuencia, importa la calificación de la figura por la característica singular del sujeto pasivo.

En cuanto al requisito de que el acceso se produzca "*sin la debida autorización o excediendo la que posea"*, el legislador está previendo algunos casos en que podría haber acceso indebido a un sistema o dato informático sin que esta acción sea punible. En este sentido quedarían incluidos tanto los casos en que hubiese un consentimiento expreso, cumplimiento de un deber, testeos de seguridad informática e ingeniería inversa o reversa.

Los dos primeros mencionados no revisten mayor dificultad. En el supuesto del consentimiento expreso, se trata de la voluntad del usuario en consentir para que se acceda a

[50] Gutiérrez, R. y otros; "Art 153 bis CP - Violación de Secretos y de la Privacidad", en Sitio Web de Asociación Pensamiento Penal. Sección Código Penal comentado de acceso libre. Versión online disponible en: http://www.pensamientopenal.com.ar/system/files/cpcomentado/cpc37761.pdf

[51] Por servicio público se ha definido: *"todo aquel que se encuentre destinado a servir a la población en forma más o menos generalizada, a un número de personas indeterminado, más allá de que su prestación corra por cuenta del Estado o de particulares"*. Definición tomada de Sáez Capel-Velciov, Op. Cit.; pág. 747.

alguna información resguardada bajo contraseñas, como por ejemplo la víctima que permite el acceso a su correo electrónico en busca de evidencia digital a utilizar en un proceso penal. En tanto, el cumplimiento de un deber importa la prestación de un servicio a pedido de un tercero requirente, en tanto orden válida y fundamentada sea, como resultaría ser aquellas ocasiones en que el fiscal solicita a determinada empresa información contenida en sus sistemas informáticos para localizar los datos de alguna persona o servicio en concreto.

Es interesante rescatar el tercer supuesto de atipicidad que podría darse y que es el que llevan a cabo testeos de seguridad informática (*hacking ético* o *ethical hacking*). Se considera así a la actividad que desarrollan profesionales de la seguridad informática como servicio para empresas u organizaciones que quieran informarse acerca del estado de seguridad de sus sistemas. De esta manera, previo permiso y consentimiento del titular de los sistemas, el profesional habilitado utiliza diferentes técnicas de ataque -tal como utilizaría algún sujeto extraño que quisiera colarse por esos sistemas vulnerando la seguridad-, con el objeto de mejorar el sistema analizado y brindar soluciones de seguridad a los desarrolladores o empresas.

Aún en los casos en que no existiera un consentimiento o contrato con personas del ámbito de la seguridad informática para la realización de los testeos de penetración (*pentesting o penetration test*), autores como Palazzi[52] han entendido que cualquiera que lleve a cabo conductas de testeo de seguridad de falencias de redes informáticas en el marco de investigación académica, casera o empresaria, deben quedar fuera de la persecución.

[52] Artículo *"Análisis de la ley 26388 de reforma al Código Penal en materia de delitos informáticos"*, publicado en "Revista de Derecho Penal y Procesal Penal", dirigida por D'Alessio y Bertolino; Edit. LexisNexis; Bs.As.; N° 7/2008, pág. 1217.

Resulta de particular interés realizar una distinción lingüística en cuanto al término *hacker* puesto que suele dársele una connotación negativa al relacionarlo como un tipo de cibercriminal. Puede resumirse el término *hacker* como el de

> *"una persona experta en programación, que conoce íntimamente los sistemas y la red, que disfruta explorando sus límites, descubriendo desafíos y comprendiéndolos, cuyo fin es experimentar diferentes alternativas para vencer el sistema, sin tener intereses en la información que exista dentro del mismo (valor hacker)".*[53]

En tanto, existe por contraposición el término *cracker* que sí guarda una característica negativa ya que, por definición que proviene del término inglés *to crack* (romper, quebrar) implica una penetración en la seguridad de los sistemas con el fin de obtener información, copiarla, alterarla, modificarla, borrarla o explotarla de cualquier forma.

Por ello, haciendo una disquisición acerca del término *hacker ético* se concluye que se trata de una redundancia lingüística, toda vez que quien reviste la condición de hacker siempre lo hará con el fin de reportar una falla para su mejora, con lo cual su finalidad tiene una connotación de ética, ya que su comportamiento tiende al bien y no a causar un daño o perjuicio a un tercero.

Al respecto, se comparte la apreciación que brinda Marcelo Temperini en cuanto a la real intención del hacker y que es lo que motiva la excepción de la aplicación del tipo penal. Dice el autor:

---

[53] Temperini, M. (2011); "Delitos Informáticos: La punibilidad del Hacking y sus consecuencias"; Revista Pensamiento Penal - Edición 132 - 03/10/11. Versión online disponible en: http://media.wix.com/ugd/d4d349_064797ed43ee4042bb17d7ace2507620.pdf

"Considero de importancia la significación del valor hacker, ya que expresa el real aspecto subjetivo, que luego se deberá tener en cuenta al analizar el tipo penal. Rápidamente se observa lo dicho anteriormente con respecto a la finalidad, resumiendo la idea en que el hacker no se interesa en el final (meta lograda u objetivo, que sería la información que guarda el sistema) sino en el camino (el proceso para sortear los límites del sistema). Queda claro que la marca distintiva del valor hacker es el reto intelectual, necesitando en consecuencia dos factores. Primero una persona con verdadero y profundo conocimiento sobre alguna materia. Luego desafíos, en el sentido de aquellos planteos que supongan alguna dificultad para la persona, que incentive a resolver el enigma, a utilizar su conocimiento como base y su mente creativa como herramienta para inventar posibles soluciones"[54].

Por otra parte, este análisis resulta claro acerca de las diferencias de ambas figuras:

"A nivel objetivo, es posible observar que los hackers, al testear y comprobar vulnerabilidades de seguridad, por sus propios principios, no dañan (sentido general de no copia, no modificación, no supresión, etc.) la información contenida, siendo que en muchos casos, ni siquiera acceden a la misma. El hacker, al retirarse del sistema (si es que accedió), en la mayoría de los casos se contacta con quien tiene el sistema a cargo (administrador), para informar sobre la situación y aconsejar sobre la solución a esa grieta de seguridad. El cracker, al comprobar la vulnerabilidad existente, buscará la manera de explotarla para acceder al sistema, navegar por dicha información, normalmente copiando, modificando o suprimiendo la misma. En la mayoría de los casos, modifican o agregan información, con leyendas que hagan referencia a su paso por el sistema, con la finalidad de alimentar su ego y poder mostrarlo a sus pares (meritocracia degenerada), tal como aquel ladrón que antes de irse pinta la pared con algún mensaje alusivo. Estas diferencias son también claras a nivel

[54] Temperini, M.; Op. Cit.

subjetivo, donde el hacker tiene intenciones de mejorar sus habilidades en la programación y la comprensión de los sistemas, donde el incentivo es un desafío intelectual y no la violación de secretos ni privacidad alguna. ***Por ello es que el foco es puesto en los sistemas en sí, y no en la información que contienen.*** *En el cracker, la finalidad perseguida sí es la información resguardada detrás de alguna barrera, la vulneración de secretos. Muestra clara de ello, es la irrelevancia sobre el "cómo se accede" a la misma, que puede ser con técnicas básicas o incluso utilizando algún rootkit automatizado, denotando es lo inverso al hacker. El foco no es el sistema, sino en lo que se esconde detrás, la información."*[55]

Finalmente, Palazzi[56] señala un caso más que estaría fuera del ámbito típico de este delito y que es la denominada *ingeniería inversa o reversa*, que es la destinada a obtener información técnica a partir de un producto accesible al público (como programas de computación y componentes electrónicos), con el fin de determinar de qué está hecho, qué lo hace funcionar y cómo fue fabricado, actividad que evidentemente no se relaciona con la "privacidad" sino, a todo evento, con la protección de la propiedad intelectual.

Resta destacar que este delito -al igual que todos los que se han descripto dentro del Capítulo III (Violación de secretos y de la privacidad), a excepción de los arts. 154 y 157 (que hace referencia a empleados de correos o funcionarios públicos)-, encuadran dentro de la categoría de delitos de acción privada (art. 73 inc. 3° del Código Penal).

4. Publicación indebida de una comunicación

[55] Temperini, M.; Op. Cit.

[56] Cit. en Gutiérrez, R. y otros; "Art 153 bis CP. Violación de Secretos y de la Privacidad", en Sitio Web de Asociación Pensamiento Penal. Sección Código Penal comentado de acceso libre. Versión online disponible en: http://www.pensamientopenal.com.ar/system/files/cpcomentado/cpc37761.pdf

La sanción de la Ley 26388 también importó la sustitución del artículo 155, el cual quedó redactado de la siguiente forma:

> *"Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza,* ***no destinados a la publicidad****, los hiciere publicar indebidamente,* ***si el hecho causare o pudiere causar perjuicios a terceros****. Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público."*

Lo que prevé la norma es la sanción bajo pena de multa para quien hallándose en posesión de una comunicación de tipo privado que no esté destinado a ser público, la hiciere publicar en forma indebida (sin autorización del emisor), cuando este hecho ocasione o pudiere ocasionar perjuicios, contemplando una exención de pena ante un supuesto particular (obrar para proteger un interés público).

Dada la descripción que se ha dado al delito, se advierte que no se requiere que la comunicación que se difunde (correspondencia, comunicación electrónica, pliego cerrado, despacho telegráfico, telefónico o cualquier otro) tenga carácter de reservado, confidencial o restricción del estilo; sino que simplemente no debe estar destinada a ser pública y, a su vez, debe contar con, al menos, la posibilidad de causar perjuicios a terceros (entendido como el destinatario, el remitente u otras personas).

Se ha entendido que la divulgación por el propio remitente de una misiva que le es propia y ocasione perjuicio a terceros, no encuadra en este delito aunque pudiera ser de aplicación alguna otra modalidad cometida contra el honor,

por ejemplo.[57] También que los terceros a quienes se les causan o pueden ocasionar perjuicio, deben estar determinados o ser, al menos, determinables.

Si sucediere el caso en que otras personas distintas de aquél que difundió indebidamente la publicación indebida, también la dieran a conocer -cuestión muy factible hoy en día con la facilidad en que se utilizan los medios de comunicación, redes sociales, foros o grupos de discusión, entre otros-, se entiende que no quedarían implicadas en este delito, por posible desconocimiento de la ilegalidad de la maniobra. La conducta se consuma con la publicación inicial no siendo un nuevo delito su reiteración por otras personas distintas.

Al igual que los anteriores delitos explicados, resulta ser de acción privada.

5. Revelación de hechos, actuaciones, documentos y datos secretos

La redacción original que tenía el artículo 157 del Código Penal fue sustituido por la Ley 26.388, quedando redactado de la siguiente forma:

> *"Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que* ***revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos****."*

Aquí la ley procura proteger a los "secretos" los cuales son una faceta de la "intimidad", en particular los secretos que son conservados y que deben ser preservados por la administración pública. La diferencia con el delito de acceso indebido está dada por las características de quien administra la información. Mientras en el acceso indebido se busca perseguir a alguien que -de modo ilegal- accedió a una información determinada que no estaba destinada a ser

[57] AAVV "Código Penal de la Nación. Comentado y anotado", Andrés J. D'Alessio director, ed. La Ley, Bs.As., 2° edición, Tomo II, 2011, pág. 536.

pública, en la revelación de datos secretos quien accede a ésta es un funcionario público que tiene acceso legítimo a la información, y lo que termina siendo punible es que revele ese contenido por tener carácter de secreto.

La conducta que va a ser juzgada es precisamente la de “revelar” a terceros ajenos ese conocimiento que posee carácter de “secreto” -que lo conoce por la función que cumple dentro de la administración pública- y que es indebidamente difundido. Se trata de una acción por la que el secreto trasciende del ámbito que le es propio.

Se trata entonces de un delito especial propio, es decir, que solo puede ser cometido por el funcionario que tiene acceso a una determinada base de datos o archivo que posee esa característica de privacidad. La vinculación entre el autor y el servicio o función que le da un marco de acción para la comisión de este delito, puede ser permanente o accidental, principal o secundaria.

El término “datos” es la característica novedosa para la inclusión dentro de esta ley de delitos informáticos ya que es lo que permite hacer alusión a la información contenida en un sistema informático. Se debe tener en cuenta que esta modalidad guarda diferencia con el art. 157 bis del C.P. que particularmente se refiere a los bancos de datos, que son el acopio de datos referidos a una determinada materia, que puede ser empleado por distintos usuarios.

Por otra parte, debe contemplarse que los damnificados aquí pueden ser tanto la administración pública -en cuanto titular del secreto fijado por ley sobre hechos, documentos, actuaciones o datos-, como así también cualquier tercero que, de forma indirecta, pueda verse afectado al verse expuesta alguna cuestión privada que debería quedar en la esfera de reserva sin trascender.

Finalmente, se debe destacar que este tipo penal es de carácter subsidiario, esto implica que de existir otro más específico, queda desplazado. Y así ocurre en el caso en que

sea de aplicación el artículo 222 del C.P. que penaliza con prisión o reclusión de uno (1) a seis (6) años, al que revelare secretos políticos, industriales, tecnológicos o militares concernientes a la seguridad, a los medios de defensa o a las relaciones exteriores de la Nación.

A diferencia de otros delitos de este capítulo, este artículo, al igual que el 154, constituye una excepción a la privacidad de la acción, pudiendo ser investigado tradicionalmente por los organismos punitivos estatales, no habiendo sido tampoco modificado con la reciente sanción de la Ley 27.147 que presentó reformas al art. 73 del Código Penal.

6. Acceso a un banco de datos personales (artículo 157 bis, párrafo 1º CP); Revelación de información registrada en un banco de datos personales (artículo 157 bis, párrafo 2º CP); Inserción de datos falsos en un archivo de datos personales (artículo 157 bis, párrafo 2º CP)

Para finalizar las reformas a los delitos contra la libertad, los legisladores contemplaron la sustitución del artículo 157 bis del Código Penal por la siguiente redacción:

> *"Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:*
>
> *1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;*
>
> *2. Ilegítimamente proporcionare o revelare a otra información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.*
>
> *3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años."*

Pese a haber existido una primera regulación que trajo la sanción de la Ley de Protección de Datos Personales (año 2000) por la cual se habían incorporado al Código Penal dos nuevos tipos penales: el art. 117 bis -que preveía la *falsedad en archivos de datos personales y suministro de información falsa*- y el art. 157 bis del C.P. levemente diferente a la redacción que le dio esta reforma de la ley 26388, a través de la reformulación de este artículo se buscó darle mayor protección penal a los bancos de datos personales.

La legislación con este artículo procura resguardar a la intimidad personal, como un espacio de reserva de los individuos necesario para el desarrollo de la personalidad y que el Estado debe preservar de toda intromisión ilícita que realicen personas no autorizadas[58].

El artículo en general menciona distintos elementos cuya descripción se encuentra en la Ley de Protección de Datos Personales[59], por ejemplo:

> *— Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.*
>
> *— Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.*
>
> *— Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.*
>
> *— Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección,*

[58] Buompadre, J. E. (2013) Manual de Derecho Penal. Parte especial.; Edit. Astrea; Buenos Aires. pág. 379.
[59] Ley 25.326, art. 2.

conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

— Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

— Datos informatizados: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

— Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

— Usuario de datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

— Disociación de datos: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

En el caso del primer inciso se pena el **acceso ilegítimo a banco de datos personales**, lo que implica penetrar, ingresar o introducirse a un banco en el que ya se hayan almacenado los datos en algún sistema o soporte informático. Esto significa que una conducta previa, como sería la recolección de datos para su posterior volcado, no podría ser objeto de esta calificación legal.

En cuanto al inciso segundo, se prevén dos conductas: "ilegítimamente proporcionar" y "revelar" información que esté registrada en un archivo o en un banco de datos personales y cuyo secreto deba guardarse en función de lo dispuesto por la ley. "Revelar" implica dar a conocer, mostrar o exponer a otro la información secreta; mientras que "proporcionar" es poner a disposición una información, facilitándosela de cualquier modo a quien la solicita. Se podría considerar que en el primer

supuesto la voluntad parte del propio sujeto que tiene acceso a la base de datos y que resuelve dar a conocer una información secreta; mientras que el segundo supuesto podría aplicarse a algún caso donde la acción puede partir de un sujeto ajeno que le solicita información a quien tiene acceso a esa base de datos y éste, en connivencia y a sabiendas de su ilegitimidad, proporciona los datos requeridos. Esta facilitación o puesta a disposición puede concretarse por cualquier medio: informático, escrito, oral, en persona, entre otros.

La diferencia con el primer inciso consiste en que, en ése, el acceso lo puede realizar cualquier persona; en tanto, en este supuesto se apunta a que el sujeto debe tener un impedimento legal para revelar o proporcionar la información contenida a la base de datos a la que tiene acceso, por ser éstos de carácter secreto.

Por su parte, el tercer inciso pena la ilegítima inserción de datos en un archivo de datos personales. Inserta quien incluye datos en el archivo de datos personales, mientras que "hace insertar" quien logra que un tercero los introduzca aun cuando éste no sepa del carácter doloso de la conducta del sujeto que lo está protagonizando, lo que originaría un supuesto de autoría mediata. En cambio, si hubiere connivencia entre quien "hace insertar" y quien efectivamente inserta, podría darse también supuestos de coautoría o de instigación y participación.

Suele resaltarse que mientras se trate de datos personales carece de relevancia que sean falsos o verdaderos, que sean de terceros o del propio titular[60]. Se requiere también que la inserción tenga virtualidad suficiente para producir la lesión del bien jurídico.

En cuanto a los sujetos que pueden ser autores del delito, ya se han realizado algunas aclaraciones, sin embargo,

[60] Ibidem; pág. 381.

de modo genérico es factible concluir que tanto para el primer como el tercer inciso puede ser cualquier usuario que tenga clave de acceso a la base de datos; mientras que en el segundo inciso se requiere además que posea obligación de guardar secreto de la información por alguna disposición de la ley, es decir que posea un "rol de garante" de la privacidad[61]. En el párrafo final del artículo -que es común a todos los incisos- se redacta sobre el agravante de la inhabilitación especial para ejercer cargos públicos para el caso en que el autor sea un funcionario público.

Finalmente resta destacar que este artículo se encuentra dentro de las acciones penales de carácter privado, es decir, que su investigación queda a cargo de las partes y no de los organismos que regularmente persiguen la acción penal, ya que las únicas excepciones que prevé el artículo 73 del C.P. es la referida a los arts. 154 y 157.

- ***Delitos contra la propiedad***

1. Defraudación por uso ilícito de tarjeta de crédito o débito

En lo que respecta a los delitos contra la propiedad, el Código Penal -antes de la reforma de la ley 26.388- había incorporado mediante la sanción de la ley 25.930, el inciso 15 al artículo 173 que regula las distintas maniobras de defraudaciones especiales.

El artículo 173 inc. 15 se encuentra redactado de esta forma:

[61] Por ejemplo, el art. 10 de la Ley 25.326 define un deber de confidencialidad, al establecer: *"1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos. 2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública."*

"El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática"

Este inciso aplica para metodologías como *phishing*[62], *pharming*[63], *keylogger*[64], las cuales conllevan distintos tipos de artificios que están direccionados a obtener en forma indebida, datos personales, para así proceder con ellos a generar perjuicios económicos a quienes son titulares de los mismos[65].

---

[62] *Phishing* es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea e incluso utilizando también llamadas telefónicas.

[63] *Pharming* es la explotación de una vulnerabilidad en el software de los servidores DNS (*Domain Name System*) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (*domain name*) a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio.

[64] Un *keylogger* -derivado del inglés: *key* (tecla) y *logger* (registrador)-, es decir un registrador de teclas, es un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet. Suele usarse como malware del tipo daemon, permitiendo que otros usuarios tengan acceso a contraseñas importantes, como los números de una tarjeta de crédito, u otro tipo de información privada que se quiera obtener.

[65] Vaninetti, Hugo Alfredo; *Aspectos jurídicos de Internet*; Librería Editora Platense; La Plata, 2010; pág. 383.

También pueden ejecutarse maniobras como el clonado o copiado de la banda magnética de las tarjetas (*skimming*) y su posterior uso fraudulento en transacciones electrónicas (*carding*), aunque también se dan casos en donde se utilizan los datos contenidos en las tarjetas sin que haya un uso físico de ella (para realizar, por ejemplo, compras por Internet), lo que queda abarcado por la modalidad que el artículo establece como *uso ilegítimo de datos.*

Se detallan a continuación los distintos elementos que componen este tipo penal, comenzando por considerar al régimen específico de las tarjetas de crédito y débito que están contempladas en la Ley 25.065.

El artículo 1 de dicha ley establece lo que se entiende por *sistema de tarjeta de crédito* que es definido como el conjunto complejo y sistematizado de contratos individuales cuya finalidad es: a) Posibilitar al usuario efectuar operaciones de compra o locación de bienes o servicios u obras, obtener préstamos y anticipos de dinero del sistema, en los comercios e instituciones adheridos. b) Diferir para el titular responsable el pago o las devoluciones a fecha pactada o financiarlo conforme alguna de las modalidades establecidas en el contrato. c) Abonar a los proveedores de bienes o servicios los consumos del usuario en los términos pactados.

En tanto, el artículo 4 define a lo que se denomina como "tarjeta de crédito" y así se entiende que es el instrumento material de identificación del usuario, que puede ser magnético o de cualquier otra tecnología, emergente de una relación contractual previa entre el titular y el emisor.

El art. 2 brinda definiciones sobre otros elementos que refiere el ilícito analizado, como son:

a) Emisor: Es la entidad financiera, comercial o bancaria que emita Tarjetas de Crédito, o que haga efectivo el pago.
b) Titular de Tarjeta de Crédito: Aquel que está habilitado para el uso de la Tarjeta de Crédito y quien se hace

responsable de todos los cargos y consumos realizados personalmente o por los autorizados por el mismo.

c) Usuario, titular adicional, o beneficiario de extensiones: Aquel que está autorizado por el titular para realizar operaciones con Tarjeta de Crédito, a quien el emisor le entrega un instrumento de idénticas características que al titular.

d) Tarjeta de Compra: Aquella que las instituciones comerciales entregan a sus clientes para realizar compras exclusivas en su establecimiento o sucursales.

e) Tarjeta de Débito: Aquella que las instituciones bancarias entregan a sus clientes para que al efectuar compras o locaciones, los importes de las mismas sean debitados directamente de una cuenta de ahorro o corriente bancaria del titular.

f) Proveedor o Comercio Adherido: Aquel que en virtud del contrato celebrado con el emisor, proporciona bienes, obras o servicios al usuario aceptando percibir el importe mediante el sistema de Tarjeta de Crédito.

El uso fraudulento que se establece como ilícito se encuentra debe vincularse al origen de la tarjeta: esta tiene que ser objeto de un delito precedente, como la falsificación, la alteración de moneda, el hurto, el robo, la apropiación indebida (para el caso de utilizarse una tarjeta que se halle perdida), o de una estafa (cuando se requiere que la tarjeta que se utilice sea obtenida del emisor mediante ardid o engaño)

Como lo que se establece es el ***uso ilegítimo por parte de quien no es titular,*** queda claro que la mera tenencia de una tarjeta falsificada, adulterada, hurtada, robada, perdida u obtenida mediante fraude, no encuadra aquí, quedando subsistentes esos delitos previos que fueron enunciados en el párrafo anterior.

En el particular caso de quien obtiene la tarjeta de un legítimo emisor mediante ardid o engaño (para el cual aparenta una falsa solvencia económica con el objeto de obtener de la entidad crediticia la tarjeta de crédito o débito, y la asignación de crédito disponible), es claro que el autor lo hace con la finalidad de adquirir bienes, servicios o dinero, a sabiendas desde entonces de que no abonará los cargos que se generen y con la finalidad dirigida a perjudicar a la entidad emisora.

En este primer supuesto entonces, se tiene un caso de concurso real de delitos cuando el sujeto activo de cualquiera de las modalidades explicadas sea el mismo que previamente sustrajo la tarjeta de crédito, la falsificó o adulteró, se apropió de la misma cuando era perdida, o la obtuvo fraudulentamente de legítimo emisor. Por tanto a la imputación de la comisión del art. 173 inc. 15° del C.P. corresponderá añadir la de los delitos de *hurto* o *robo* (arts. 162, 164 y cctes. C.P.), *falsificación o alteración de moneda* (arts. 282, 283, 285 C.P), *apropiación de cosa perdida* (art. 175 inc. 1 C.P.), o *estafa genérica* (art. 172 C.P.)

> En cuanto al segundo modo de comisión que se refiere a *"quien defraudare mediante el* ***uso no autorizado de sus datos****, aunque lo hiciere por medio de una operación automática",* se da cuando el sujeto activo, sin utilizar físicamente la tarjeta, emplea los datos propios de ella, sin que haya sido autorizado por el titular, y sin que necesariamente la tarjeta le hubiere sido hurtada, robada o perdida.

En general, esta conducta se llevará a cabo por medios electrónicos (como por ejemplo las compras de objetos o de servicios por Internet, por redes sociales, o las telefónicas) y obteniendo la información a través de distintas técnicas de manipulación informática y de ingeniería social, como las descriptas al comienzo.

En relación al grado de conocimiento de la ilicitud de la maniobra por parte de quienes llevan a cabo el delito, puede

decirse que es posible aplicar la figura del dolo eventual, lo que implica que, aunque el sujeto activo tenga dudas respecto a la procedencia y calidad de la tarjeta hallada, hurtada o robada, nunca podrá aducir desconocimiento sobre la falta de autorización para su utilización, puesto que ello se presume desde que él no ha formado parte de un contrato que lo vincule con la entidad emisora y lo habilite al uso de la tarjeta. Y, en caso de que cuente con autorización para operar con dicha tarjeta, su utilización naturalmente no constituirá ningún delito[66].

En esta clase de delitos el sujeto pasivo puede ser cualquiera que se vea perjudicado patrimonialmente. No obstante ello, cabe aclarar que este tipo de delitos puede caracterizarse como una "estafa triangular", donde se produce un desdoblamiento entre el sujeto engañado, es decir, la víctima del ardid, y el sujeto perjudicado o damnificado, esto es, el que se verá afectado en su patrimonio al deber hacer frente al pago de los gastos generados[67].

El juego de roles que dispone la ley 25.065 es la que va a determinar en definitiva, quién es el damnificado o perjudicado patrimonial por el delito. Se ha entendido que puede ser tanto el comerciante, la entidad emisora o el propio titular de la tarjeta. Así, el damnificado coincidirá con el sujeto engañado, es decir, el comerciante, cuando éste haya aceptado la tarjeta extraviada, sustraída o apócrifa sin verificar la identidad de quien la presenta, o sin consultar previamente sus datos con la entidad emisora a través de los medios automáticos establecidos a tal fin. Si, en cambio, procedió a verificarlos pero la entidad emisora falló en su deber de información sobre las condiciones de vigencia y operatividad de la tarjeta, el sujeto damnificado será solo la entidad emisora. Por último, en caso de que el titular de la tarjeta sea

[66] Medina, V. Estafa con tarjeta de crédito. Versión online, disponible en: http://www.terragnijurista.com.ar/doctrina/estafa_tarjetas.htm
[67] Ibidem.

el responsable de no haber efectuado la correspondiente denuncia de extravío o sustracción ante la entidad emisora -sea que lo omitió por negligencia o porque no se percató de la sustracción o extravío-, será él quien resulte perjudicado patrimonialmente por el delito[68].

2. Defraudación informática

La ley 26.388 incorpora el inciso 16 a dicho artículo 173, penalizando de este modo la estafa informática la cual queda tipificada como:

> *"El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos".*

Al igual que el artículo precedente se busca proteger el patrimonio en un sentido amplio.

La acción es la de defraudar a otro "*mediante cualquier técnica de manipulación informática"*, lo que equivale a alterar, modificar u ocultar datos informáticos de manera que se realicen operaciones de forma incorrecta o que no se lleven a cabo, así como también modificar las instrucciones del programa con el fin de alterar el resultado que se espera obtener.

Se ha señalado que este artículo fue incorporado al Código Penal en miras de legislar sobre la modalidad de *phishing*[69] que comenzó a registrarse previo a la sanción de la ley y aún sigue siendo de los casos más denunciados. Así, se considera autores de este delito a quienes realizan maniobras de fraude mediante dicha técnica de manipulación informática -por la cual obtuvieron los datos necesarios (por ejemplo, datos de las tarjetas)-, para poder operar en las cuentas

[68] Ibidem.
[69] Phishing: ver nota 62 para su descripción.

bancarias del damnificado, efectuando transferencias ilegítimas.

La introducción de datos falsos en el ordenador (manipulación del *input*), la modificación o alteración del orden de procesamiento de datos (afectación al programa o sistema en sí mismo, es decir, del *software* o del *hardware*), o el falseamiento del resultado obtenido del ordenador (manipulación del *output*), son algunas de las posibles modalidades que puede asumir la conducta típica[70].

La alteración en la transmisión de datos puede darse en el supuesto en que al sistema se lo engañe sin una alteración concreta, lo que puede producirse al momento de recibirse la información, por ejemplo, impidiendo el funcionamiento de rutinas de chequeo o validación de datos.

La redacción es bien amplia, con lo cual las maniobras que podrían encuadrar aquí deberán ser valoradas según el caso no reduciéndose a algunos supuestos específicos. Sólo excluye el manejo o la operación que se sirve del medio tecnológico para obtener una ventaja patrimonial indebida, que no modifica su normal programación o funcionamiento.

Una crítica que suele hacerse a la redacción de este artículo pasa por el hecho de haberse establecido que la técnica de manipulación informática deba **alterar el normal funcionamiento** de un sistema informático o la transmisión de datos. La elección del término "alterar el normal funcionamiento" en algunos casos podría dejar fuera de juego a muchas maniobras de manipulación informática donde exista un perjuicio patrimonial causado pero sin que se haya alterado ningún sistema informático, que podría darse, por ejemplo, cuando la manipulación consista en el usufructo de grietas o fallas del sistema preexistentes y no provocadas.

[70] Figari, R.E. Reflexiones sobre la defraudación informática (Ley 26.388). Versión online, disponible en: http://www.rubenfigari.com.ar/reflexiones-sobre-la-defraudacion-informatica-ley-26-388-2/

Etimológicamente “alterar”, del latín *alterare,* significa modificar, cambiar la esencia o forma de algo, trastornar, perturbar. Estos conceptos se adaptan perfectamente al término referido a la manipulación que pretende alterar un sistema informático, pues aquélla consiste en justamente modificar o cambiar el funcionamiento normal de un sistema o la transmisión de datos, y por lo tanto, quien realiza esta acción queda implicado en este tipo penal[71].

Finalmente es preciso recordar que la Convención de Cibercriminalidad de Budapest define al sistema informático como “todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos”. Ello implica generar, enviar, recibir, procesar o almacenar información de cualquier forma y por cualquier medio. Mientras que la trasmisión de datos se encuentra definida, en forma general, como “toda representación de hechos, manifestaciones o conceptos en un formato que puede ser tratado por un sistema informático”[72].

3. Daño informático

También se realizaron incorporaciones y sustituciones a los delitos de daño y su figura agravada. De esta manera, el artículo 183 del Código Penal agregó un segundo párrafo de modo de tipificar la conducta de quien

> *“...alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.”*

[71] Figari, R. E.; Op. Cit.

[72] Convención de Cibercriminalidad de Budapest, art. 1. inc. a). Versión online, disponible en: https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF.

De la misma forma, sustituyó el artículo 184 por el siguiente:

> *"La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes: (...) 5. Ejecutarlo en* ***archivos, registros****, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos;* ***o en datos, documentos, programas o sistemas informáticos públicos****; 6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público".*

La redacción dada se hacía necesaria ya que la antigua que tenía el delito de daño, recaía solamente sobre cosas tangibles, y los datos o programas de un sistema son bienes intangibles. También se introduce la figura de los "virus informáticos", al preverse la tipicidad de la distribución de programas destinados a causar cualquiera de los daños descriptos anteriormente[73].

La reforma ha ampliado los objetos de protección, tutelándose especialmente al dato, al documento, a los programas y a los sistemas informáticos como banco u objeto de ataques ilegítimos, con el fin de mantener incólume su inalterabilidad. Con la protección ampliada de esta norma, la intangibilidad de una página web en internet es alcanzada por la norma en cuestión[74].

La inclusión del verbo *"alterare"* implica -desde el campo informático- la modificación de un archivo de datos o programa sin destruirlo completamente. En el contexto

[73] FIgari, Rubén E.; "Daño informático (arts. 183, 2º párr. y 184 incs. 5º y 6º del C.P. Ley 26.388)". Versión online, disponible en: http://www.rubenfigari.com.ar/dano-informatico-arts-183-2%C2%BA-parr-y-184-incs-5%C2%BA-y-6%C2%BA-del-c-p-ley-26-388/

[74] ibídem.

informático, *destruir o inutilizar* quiere decir borrar definitivamente sin posibilidad de recuperación. El hecho que exista un sistema de *back up*, en modo alguno altera el delito de daño, pues la restauración requiere un esfuerzo que ya implica reparar el daño causado[75].

Además del daño informático tradicional se agrega una nueva modalidad al penalizarse a quien *"vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños"*.

Se entiende que el uso de estos programas puede ser potencialmente dañoso. No se prohíbe la existencia de estos programas[76], sino que se penaliza a quien los venda, los distribuya o los haga circular o introduzca concretamente en un sistema informático. Por consiguiente, quien de alguna manera pone en el comercio un programa de tales características, con conocimiento del daño a producir, ayuda de esta forma a cometer el delito de daño a quien usará la herramienta[77].

En cuanto al agregado de los inc. 5° y 6° del art. 184 del C.P. se trata de agravantes de la modalidad básica que describe el artículo anterior. En el caso del inc. 5° apunta a que el daño se produzca en datos, documentos, programas o sistemas informáticos **públicos**; se agrava por la naturaleza y pertenencia de la información que se resguarda y en cuanto resultan ser "públicos", es decir cuando se ocasione en programas o sistemas informáticos públicos, pertenecientes al Estado Nacional, Provincial o Municipal, dándole de esta

[75] Palazzi, P. (2008) Análisis del proyecto de ley de delitos informáticos aprobado por el Senado de la Nación en el año 2007. En Revista de Derecho Penal y Procesal Penal, Abril-Mayo 2008, Lexis Nexis.
[76] Sería prácticamente imposible poder criminalizar a quienes producen una herramienta que puede eventualmente usarse para crear daños informáticos, sobre todo porque cualquier tecnología hoy en día que sea mal utilizada puede ocasionar un daño.
[77] Figari, R.E. Op. Cit.

forma un mayor valor a la información y a la titularidad oficial de su pertenencia o almacenamiento.

Finalmente el inciso 6° del art. 184 del C.P. se prevé un agravante cuando el daño se ejecute en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

Se contempla así al sistema informático como objeto de protección penal y a la información allí contenida, por la calidad del servicio que presta la entidad afectada, en la medida que revistan una finalidad específica y calificada por estar relacionada con la prestación de servicios de salud, comunicación, provisión, transporte de energía, medios de transporte u otros servicios públicos.

- ***Delitos contra la seguridad pública***

La ley 26.388 realizó una modificación al artículo 197 del C.P., que se lo conoce como **delito de entorpecimiento de las comunicaciones**, el cual establece:

> *"Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida"*

Este delito apunta a proteger la normalidad del servicio de telecomunicaciones y de intercambio de la información por medios electrónicos.

Contempla dos tipos penales que tienen los mismos objetos. Uno es la interrupción o entorpecimiento de la comunicación telegráfica, telefónica o de otra naturaleza, y el otro es la resistencia violenta al restablecimiento de la comunicación interrumpida. En el primero de los supuestos se amplió la terminología ya existente en este tipo penal, incluyendo "o de otra naturaleza" lo que permite dar cobertura penal a las comunicaciones electrónicas o a través de medios

informáticos como lo es Internet y los mensajes de texto o intercambio a través de equipos de telefonía celular[78].

Los casos en que puede aplicarse este delito están vinculados a los ataques masivos de *spam* de manera que obstruya un sistema informático, o los de denegación de servicios (DoS[79] / DDoS[80]) dirigidos contra una entidad u organismo.

Se ha entendido que un ataque masivo a los sistemas de información mediante la introducción ilegítima de decenas de miles de correos electrónicos de diverso contenido acompañados, en la mayoría de las ocasiones, de virus informáticos o programas *crash* de destrucción masiva, constituye una circunstancia que habría impedido la comunicación normal dentro y fuera de la empresa dedicada a la actividad publicitaria, y que la maniobra fue efectiva para privarla de, o al menos entorpecer, ese medio de comunicación, sea cual fuere la línea telefónica desde la cual se pretendiera acceder al administrador de correo y direcciones afectadas.

En un caso así un estudio pericial resulta imprescindible para determinar cuáles son los daños provocados, pudiendo detectarse[81]: 1) Demoras en la entrega y recepción de e-mails de trabajo; 2) Caídas en los servidores dedicados al envío y recepción de e-mails y del servicio en sí; 3) Corrupción en los

[78] D'Alessio, A.J. (Dir.). Código Penal de la Nación. Comentado y anotado. 2° edición actualizada y ampliada. Tomo II. Pte. especial. Edit. La Ley. Pág. 957.

[79] Ataques de denegación de servicio simples (Deny Of Service). Este tipo de ataques se caracterizan por tener un único origen desde el cual se realiza la denegación del servicio.

[80] Ataques de denegación de servicio distribuido (Distributed DOS o DDOS). En este tipo de ataques se utilizan varias fuentes coordinadas que pueden realizar un ataque progresivo, rotatorio o total.

[81] Cfr. Fallo "Marchione, Gabriel" Daño a un sistema informático - Remisión masiva de mensajes con virus (spam) - Interrupción del servicio de comunicaciones. C. Nac. Crim. y Corr. Fed., sala 2ª, 15/11/2005.

archivos de procesamiento de los servidores de mail, lo que obliga a tareas de mantenimiento y depuración adicionales en horarios de trabajo; 4) Pérdida de e-mails debido a la necesidad de recuperar backups de fechas anteriores por la corrupción mencionada en el punto anterior; 5) Interrupciones en los servicios en horarios de trabajo, por tareas de mantenimiento no programadas; 6) Tareas de depuración manual de e-mails, usuario por usuario; 7) Requerimiento de espacio adicional de almacenamiento de e-mails depurados y en proceso, con el costo aparejado por la compra del hardware necesario; 8) Inutilización por varias horas de la línea telefónica de la empresa atacada. En esa ocasión se señaló que casi todos los puntos mencionados implicaban una carga adicional de horas/hombre de trabajo, inclusive en horarios no habituales como durante la noche y fines de semana.

Por otra parte, los ataques por denegación de servicio (Dos / DDoS) -que se generan mediante la saturación de los puertos con flujo de información, haciendo que un servidor se sobrecargue y no pueda seguir prestando servicios- resulta ser una técnica usada por los *crackers* para dejar fuera de servicio a servidores objetivo.

Si bien se considera que en el ordenamiento jurídico interno el ataque de denegación de servicio está tipificado en el art. 197 del Código Penal, lo cierto es que su redacción está lejos de cubrir este delito, ya que solo contempla la intromisión en cualquier tipo de comunicación y no el provocar la baja de funciones de un sistema[82].

[82] Por este motivo se encuentra actualmente en trámite un Proyecto de Ley de la Senadora Nacional María de los Ángeles Higonet que solicita la incorporación al Código Penal del art. 197 bis, con esta redacción: *"Será reprimido con prisión de seis (6) meses a dos (2) años el que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, trasmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o*

- ***Delitos contra la Administración Pública***

El último artículo que modificó la reforma de la Ley 26.388 es el art. 255 del Código Penal relativo al delito de destrucción de objetos destinados a servir como prueba, el cual quedó redactado de esta forma:

> *"Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo. Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($750) a pesos doce mil quinientos ($ 12.500)."*

Se trata de una figura que procura la conservación o preservación de aquellos objetos que estén destinados a servir de prueba cuya custodia hubiere sido confiada a un funcionario u otra persona en el interés del servicio público. Se sanciona aquellas acciones que tiendan a impedir que los objetos cumplan el fin para el cual fueron puestos en custodia[83].

Se describen distintas formas de realización del delito de sustracción e inutilización de objetos custodiados, y se contempla también una circunstancia agravante en función de la calidad del sujeto activo. El segundo párrafo describe un tipo imprudente[84].

---

haciendo inaccesibles datos informáticos." (Expte. S. 3918/14). Puede consultarse en: http://www.senado.gov.ar/parlamentario/comisiones/verExp/3918.14/S/PL

[83] Donna, E. A.(2000) Derecho Penal. Parte Especial. Tomo III, Rubinzal-Culzoni Editores, Bs.As. pág. 202.

[84] D'Alessio, A.J. Op. Cit. pág. 1268.

La reforma incorporó el verbo “alterar” como modalidad del delito en cuestión, para poder penalizar los casos en que se produce una modificación de tipo informática a cualquiera de los objetos que puedan servir como objeto de prueba, como los registros o documentos públicos o privados en los que se haya hecho constar alguna circunstancia que interese a un servicio público.

- ***Otras normativas existentes vinculadas a delitos informáticos***

1. Alteración dolosa de registros fiscales, y alteración de sistemas y equipos electrónicos (Ley 24769 y modif. 26.735 - Ley Penal Tributaria)

El art. 12 de la Ley 24.769 (y su modificatoria, ley 26.735) previó el delito de **“alteración dolosa de registros fiscales”**, quedando contemplado de esta forma:

> *“Será reprimido con prisión de dos a seis años, el que de cualquier modo sustrajere, suprimiere, ocultare, adulterare, modificare o inutilizare los registros o soportes documentales o informáticos del fisco nacional, provincial o de la Ciudad Autónoma de Buenos Aires, relativos a las obligaciones tributarias o de recursos de la seguridad social, con el propósito de disimular la real situación fiscal de un obligado”.*

La ley 26.735 modificó la ley original (24.769) e incorporó el artículo 12 bis, cuyo texto prevé la **“alteración dolosa de sistemas informáticos o equipos electrónicos”** quedando redactado así:

> *“Será reprimido con prisión de uno (1) a cuatro (4) años, el que modificare o adulterare los sistemas informáticos o equipos electrónicos, suministrados u homologados por el fisco nacional, provincial o de la Ciudad Autónoma de Buenos Aires, siempre y cuando dicha conducta fuere susceptible de provocar perjuicio y no resulte un delito más severamente penado”.*

La norma busca proteger la actividad financiera del Estado y la recaudación de los tributos y los parámetros

imprescindibles para el cumplimiento de las pautas de la seguridad social. Se infiere, por tanto, que la simulación de cualquier otra situación o información que no sea la atinente a la fiscal de un contribuyente, no se adecuará al tipo penal descripto por cuanto no pondría en peligro aquella protección legal cubierta por el art. 12.[85]

Resulta de este modo atendible que se haya penalizado este ilícito, modalidad usual de estafa informática para quien procura alterar un registro informático cuyo contenido el sistema toma en cuenta para adoptar decisiones de pago o disposición patrimonial, con el objetivo de obtener fraudulentamente algún tipo de beneficio fiscal que, de otro modo, no correspondería.

Es un tipo de peligro abstracto, por lo que basta para su consumación la simple sustracción, supresión, ocultamiento, adulteración, modificación o inutilización, sin requerirse la producción concreta de daño alguno.

En cuanto a las modalidades delictivas se establecen la de *sustraer* que implica apoderarse con o sin violencia de una cosa; *suprimir* que implica hacer desaparecer algo o eliminar (en el caso un registro o un soporte informático, ya que el verbo no estaría dirigido a la información misma, sino al objeto que a ésta la contiene); *ocultar* que significa esconder, evitar que una cosa sea vista, disimular o encubrir; *adulterar* que es falsificar; modificar es transformar, cambiar, variar algo; y por último *inutilizar* que implica "hacer inútil, vano o nulo un objeto o una cosa, o destruirla, volviéndola ineficaz."[86]

Respecto a la figura incorporada por la modificación que legisla sobre la alteración dolosa de sistemas informáticos

[85] Riquert, M. y otro. Delitos de alteración dolosa de registros (art. 12 Ley Penal Tributaria). Versión online disponible en: http://riquert-penaltributario.blogspot.com.ar/2008/07/delito-de-alteracin-dolosa-de-registros.html

[86] Ibidem.

o equipos electrónicos, se ha buscado darle protección a los sistemas de controladores fiscales, y en general a cualquier sistema y equipo que tenga por finalidad emitir facturas y controlar operaciones de índole tributaria. Se prevé, además, que sea un delito de carácter subsidiario, es decir que su encuadre será residual en caso que no existiese otro con mayor pena.

2. Propiedad intelectual y software: la Ley Nº 25.036 (1998)

La ley 25.036 del año 1998 modificó la Ley N° 11.723 que regula a la Propiedad Intelectual y data del año 1933, brindando protección penal al software.

Se resolvió incluir a los programas de computación fuente y objeto en varios artículos, quedando de este modo de la siguiente forma

> *Artículo 1°. — A los efectos de la presente Ley, las obras científicas, literarias y artísticas comprenden los escritos de toda naturaleza y extensión, entre ellos los* ***programas de computación fuente y objeto; las compilaciones de datos o de otros materiales;*** *las obras dramáticas, composiciones musicales, dramático-musicales; las cinematográficas, coreográficas y pantomímicas; las obras de dibujo, pintura, escultura, arquitectura; modelos y obras de arte o ciencia aplicadas al comercio o a la industria; los impresos, planos y mapas; los plásticos, fotografías, grabados y fonogramas, en fin, toda producción científica, literaria, artística o didáctica sea cual fuere el procedimiento de reproducción.*
>
> *La protección del derecho de autor abarcará la expresión de ideas, procedimientos, métodos de operación y conceptos matemáticos pero no esas ideas, procedimientos, métodos y conceptos en sí.*
>
> *Art. 4°. — Son titulares del derecho de propiedad intelectual:*
>
> *a) El autor de la obra;*
>
> *b) Sus herederos o derechohabientes;*

c) Los que con permiso del autor la traducen, refunden, adaptan, modifican o transportan sobre la nueva obra intelectual resultante.

d) ***Las personas físicas o jurídicas cuyos dependientes contratados para elaborar un programa de computación hubiesen producido un programa de computación en el desempeño de sus funciones laborales, salvo estipulación en contrario.***

Art. 9°. — Nadie tiene derecho a publicar, sin permiso de los autores o de sus derechohabientes, una producción científica, literaria, artística o musical que se haya anotado o copiado durante su lectura, ejecución o exposición públicas o privadas.

Quien haya recibido de los autores o de sus derecho-habientes de un programa de computación una licencia para usarlo, podrá reproducir una única copia de salvaguardia de los ejemplares originales del mismo.

Dicha copia deberá estar debidamente identificada, con indicación del licenciado que realizó la copia y la fecha de la misma. La copia de salvaguardia no podrá ser utilizada para otra finalidad que la de reemplazar el ejemplar original del programa de computación licenciado si ese original se pierde o deviene inútil para su utilización.

Art. 55 bis — La explotación de la ***propiedad intelectual*** *sobre los* ***programas de computación*** *incluirá entre otras formas los contratos de licencia para su uso o reproducción.*

Art. 57. — En el Registro Nacional de Propiedad Intelectual deberá depositar el editor de las obras comprendidas en el artículo 1°, tres ejemplares completos de toda obra publicada, dentro de los tres meses siguientes a su aparición. Si la edición fuera de lujo o no excediera de cien ejemplares, bastará con depositar un ejemplar.

El mismo término y condiciones regirán para las obras impresas en país extranjero, que tuvieren editor en la República y se contará desde el primer día de ponerse en venta en territorio argentino.

Para las pinturas, arquitecturas, esculturas, etcétera, consistirá el depósito en un croquis o fotografía del original, con las indicaciones suplementarias que permitan identificarlas.

Para las películas cinematográficas, el depósito consistirá en una relación del argumento, diálogos, fotografías y escenarios de sus principales escenas. ***Para los programas de computación, consistirá el depósito de los elementos y documentos que determine la reglamentación.***

Cualquiera de las infracciones que se produzcan de estos artículos de la ley de Propiedad Intelectual, quedan enmarcadas dentro de la modalidad de la estafa que pena el Código Penal en su artículo 172[87], según lo definió la propia ley en sus artículos 71 y 72[88].

En el año 2007 se sumó otra reforma a la Ley de Propiedad Intelectual mediante la sanción de la ley 26.285 contemplándose en su artículo 36[89] que el uso indebido de las

[87] **Artículo 172**. del Código Penal: Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño.

[88] **Ley 11723, art. 71:** Será reprimido con la pena establecida por el artículo 172 del Código Penal, el que de cualquier manera y en cualquier forma defraude los derechos de propiedad intelectual que reconoce esta Ley. **Ley 11.723, Art. 72:** Sin perjuicio de la disposición general del artículo precedente, se consideran casos especiales de defraudación y sufrirán la pena que él establece, además del secuestro de la edición ilícita: a) El que edite, venda o reproduzca por cualquier medio o instrumento, una obra inédita o publicada sin autorización de su autor o derechohabientes; b) El que falsifique obras intelectuales, entendiéndose como tal la edición de una obra ya editada, ostentando falsamente el nombre del editor autorizado al efecto; c) El que edite, venda o reproduzca una obra suprimiendo o cambiando el nombre del autor, el título de la misma o alterando dolosamente su texto; d) El que edite o reproduzca mayor número de los ejemplares debidamente autorizados.

[89] **Ley 11.723, art. 36.** — Los autores de obras literarias, dramáticas, dramático-musicales y musicales, gozan del derecho exclusivo de autorizar:

a) La recitación, la representación y la ejecución pública de sus obras; b) La difusión pública por cualquier medio de la recitación, la representación y la ejecución de sus obras. Sin embargo, será lícita y estará exenta del pago de derechos de autor y de los intérpretes que establece el artículo 56, la representación, la ejecución y la recitación de obras literarias o artísticas ya publicadas, en actos públicos organizados por establecimientos de enseñanzas, vinculados en el cumplimiento de sus fines educativos, planes y programas de estudio, siempre que el espectáculo no sea difundido fuera del lugar donde se realice y la concurrencia y la actuación de los intérpretes sea gratuita. También gozarán de la exención del pago del derecho de autor a que se refiere el párrafo anterior, la ejecución o interpretación de piezas musicales en los conciertos, audiciones y actuaciones públicas a cargo de las orquestas, bandas, fanfarrias, coros y demás organismos musicales pertenecientes a instituciones del Estado Nacional, de las provincias o de las municipalidades, siempre que la concurrencia de público a los mismos sea gratuita. Se exime del pago de derechos de autor la reproducción y distribución de obras científicas o literarias en sistemas especiales para ciegos y personas con otras discapacidades perceptivas, siempre que la reproducción y distribución sean hechas por entidades autorizadas. Esta exención rige también para las obras que se distribuyan por vía electrónica, encriptadas o protegidas por cualquier otro sistema que impida su lectura a personas no habilitadas. Las entidades autorizadas asignarán y administrarán las claves de acceso a las obras protegidas. No se aplicará la exención a la reproducción y distribución de obras que se hubieren editado originalmente en sistemas especiales para personas con discapacidades visuales o perceptivas, y que se hallen comercialmente disponibles. A los fines de este artículo se considera que: - Discapacidades perceptivas significa: discapacidad visual severa, ampliopía, dislexia o todo otro impedimento físico o neurológico que afecte la visión, manipulación o comprensión de textos impresos en forma convencional. - Encriptadas significa: cifradas, de modo que no puedan ser leídas por personas que carezcan de una clave de acceso. El uso de esta protección, u otra similar, es considerado esencial a fin de la presente exención, dado que la difusión no protegida podría causar perjuicio injustificado a los intereses legítimos del autor, o ir en detrimento de la explotación normal de las obras. - Entidad autorizada significa: un organismo estatal o asociación sin fines de lucro con personería jurídica, cuya misión primaria sea asistir a ciegos o personas con otras discapacidades perceptivas. - Obras científicas significa: tratados, textos, libros de divulgación, artículos de revistas especializadas, y todo material relativo a la ciencia o la tecnología en sus diversas ramas. - Obras literarias significa: poesía, cuento, novela, filosofía, historia, ensayos, enciclopedias, diccionarios, textos y todos aquellos escritos en los cuales forma y fondo se combinen para expresar conocimientos e ideas de interés

reproducciones que se hagan en sistemas especiales orientados a ciegos y personas con otras discapacidades perceptivas, será reprimido con pena de prisión, conforme el artículo 172 del Código Penal.

3. Delitos tradicionales donde pueden existir componentes informáticos en su comisión

Si bien la ley argentina no adoptó más tipos penales de "delitos informáticos", existen figuras penales "tradicionales" que pueden ser cometidas a través de internet. Estos son[90]:

a) Falsificación: Como se explica al comienzo, la reforma de la ley 26.388 incorporó a las terminologías del art. 77 del Código Penal la inclusión dentro de los "documentos" a toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o

universal o nacional. - Personas no habilitadas significa: que no son ciegas ni tienen otras discapacidades perceptivas. - Sistemas especiales significa: Braille, textos digitales y grabaciones de audio, siempre que estén destinados exclusivamente a las personas a que se refiere el párrafo anterior. - Soporte físico significa: todo elemento tangible que almacene voz en registro magnetofónico o digital, o textos digitales; por ejemplo, cassettes, discos compactos (CD), discos digitales versátiles (DVD) o memorias USB. Las obras reproducidas y distribuidas en sistemas especiales deberán consignar: los datos de la entidad autorizada, la fecha de la publicación original y el nombre de la persona física o jurídica a la cual pertenezcan los derechos de autor. Asimismo, advertirán que el uso indebido de estas reproducciones será reprimido con pena de prisión, conforme el artículo 172 del Código Penal. *(**Nota Infoleg**: Por art. 1°, último párrafo de la Ley N° 20.115 B.O. 31/1/1973 se establece que ARGENTORES tendrá a su cargo las autorizaciones determinadas en el presente artículo salvo prohibición de uso expresa formulada por el autor y la protección y defensa de los derechos morales correspondientes a los autores de dichas obras.). (**Nota Infoleg**: Por arts. 1° y 2° del Decreto N° 8.478/1965 B.O. 8/10/1965 se obliga a exhibir la autorización escrita de los autores en la ejecución de música nacional o extranjera en público.).* Fuente: Sitio web Infoleg. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/texact.htm

[90] Algunos ejemplos citados por Vaninetti, H:A.; *Op. Cit.* pág. 412/4

transmisión. Además se incluyó dentro de los conceptos "firma" y "suscripción" a la firma digital, así como en los instrumentos privados queda comprendido el documento digital firmado digitalmente. Con estas ampliaciones conceptuales todas las figuras del Título XII (Delitos contra la fe pública) pueden ser cometidas por estos medios, por ejemplo, podría existir una falsificación de un documento en soporte electrónico y ser pasible, quien realiza esta conducta de la pena dispuesta en el art. 292.

b) Intimidación pública: Por internet puede infundirse un temor público o suscitarse tumultos o desórdenes, conducta recogida en el art. 211 del Código Penal. Podría efectuarse por la remisión masiva de correo electrónico, foros de discusión o desde una página web.

c) Instigación al suicidio, a cometer delitos o a la incitación a la violencia y apología del delito o de un condenado por delito. Delitos de la ley 23.592 (antidiscriminación): Estas acciones tipificadas como delitos en sus artículos 83, 209, 212 y 213 del Código Penal y art. 3 de la ley 23.592 bien pueden ser llevadas a cabo a través de internet.

d) Amenazas: Aquellas que puedan darse por cualquier medio tecnológico, con el objeto de alarmar o amedrentar a una o más personas, así como quien hace uso de amenazas con el propósito de obligar a otro a hacer, no hacer o tolerar algo contra su voluntad. En este caso la informática actúa de medio para la comisión de un delito ya contemplado en la ley (arts. 149 bis y cctes del C.P.[91]), pudiendo ser aplicado en casos por ejemplo de sextorsión[92].

[91] ARTICULO 149 bis. - Será reprimido con prisión de seis meses a dos años el que hiciere uso de amenazas para alarmar o amedrentar a una o más personas. En este caso la pena será de uno a tres años de prisión si se emplearen armas o si las amenazas fueren anónimas. Será reprimido con prisión o reclusión de dos a cuatro años el que hiciere uso de amenazas con el propósito de obligar a otro a hacer, no hacer o tolerar algo contra su voluntad.
ARTICULO 149 ter. - En el caso del último apartado del artículo anterior, la pena será: 1) De tres a seis años de prisión o reclusión si se emplearen

e) Extorsión: El tipo penal básico de la extorsión reprime con reclusión o prisión de cinco a diez años, al que con intimidación o simulando autoridad pública o falsa orden de la misma, obligue a otro a entregar, enviar, depositar o poner a su disposición o a la de un tercero, cosas, dinero o documentos que produzcan efectos jurídicos. Dentro de esta modalidad delictiva podría llegar a encuadrarse los casos de ransonware[93], un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción, y que está creciendo de manera exponencial dentro de las nuevas modalidades delictivas.

5. Delito transnacional. Jurisdicción y competencia

Las reglas de competencia tienen como objetivo determinar cuál va a ser el tribunal que va a intervenir, con preferencia o exclusión de los demás, en una controversia que ha puesto en movimiento la actividad jurisdiccional.

Dentro de las diferentes clases de competencia existentes (por cuantía, por materia, por grado y por territorio)

---

armas o si las amenazas fueren anónimas; 2) De cinco a diez años de prisión o reclusión en los siguientes casos: a) Si las amenazas tuvieren como propósito la obtención de alguna medida o concesión por parte de cualquier miembro de los poderes públicos; b) Si las amenazas tuvieren como propósito el de compeler a una persona a hacer abandono del país, de una provincia o de los lugares de su residencia habitual o de trabajo.

[92] La sextorsión (extorsión sexual) es una forma de explotación sexual en la cual una persona es chantajeada con una imagen o vídeo de sí misma desnuda o realizando actos sexuales, que generalmente ha sido previamente compartida mediante sexting. La víctima es coaccionada para tener relaciones sexuales con alguien, entregar más imágenes eróticas o pornográficas, dinero o alguna otra contrapartida, bajo la amenaza de difundir las imágenes originales si no accede a las exigencias del chantajista.

[93] *Ransomware:* del inglés *ransom,* 'rescate', y *ware*, por software.

en esta temática se tendrá especialmente en cuenta la competencia en razón del territorio.

En los casos de los delitos informáticos es importante tener en cuenta que determinados ilícitos pueden haber sido ejecutados desde distintos lugares, y tener efectos en otros tantos (delitos a distancia). La cuestión se torna más compleja aun cuando varias personas contribuyen a una acción delictiva, y/o cuando hay víctimas situadas en distintos puntos geográficos. Incluso las pruebas de la comisión de algunos ilícitos pueden estar diseminadas en distintos territorios.

Argentina tiene una estructura federal, por lo que, ante la presunta comisión de la mayoría de los delitos, interviene la justicia penal ordinaria de la provincia de que se trate. Ante ciertos casos de excepción legalmente establecidos, es ompetente la justicia nacional o federal (Ley 48).

Las controversias acerca de la ley aplicable y la determinación del juez competente (ya sea para decidir en un caso o sólo para obtener una prueba) son más problemáticas cuando involucran a diferentes países. A ello se suma la particular configuración de la nube, que es administrada por entidades privadas y sólo parcialmente regulada por los Estados.

Según el art. 1° del Código Penal de la Nación, éste es la ley aplicable ante delitos cometidos o cuyos efectos deban producirse en el territorio de la Nación Argentina, o en los lugares sometidos a su jurisdicción, y ante delitos cometidos en el extranjero por agentes o empleados de autoridades argentinas en desempeño de su cargo. De modo coincidente, para establecer el “lugar de comisión del delito” y, consecuentemente, la competencia judicial, la Corte Suprema de Justicia de la Nación ha adoptado este criterio de ubicuidad (CSJN, "Ruiz Mira". Fallos: 271:396; íd., Competencia N° 63. XXXVI, Tatarsky, Héctor Eduardo s/ denuncia, 29/08/2000, Fallos: 323:2335). El hecho se considera cometido tanto en el lugar donde se produjo la exteriorización de voluntad del autor

como donde se concretó el resultado. Para decidir si es competente el tribunal del lugar de exteriorización de la voluntad o el de producción del resultado, se aplican criterios centrados en la mejor y más pronta administración en justicia (defensa en juicio de las partes, celeridad y economía procesal).

En cuanto a la ley aplicable, el principio de territorialidad se complementa con el principio real, de defensa o de protección de intereses, por cuanto el principio territorial es insuficiente para cubrir un buen número de casos. El principio real constituye un criterio de aplicación de la ley penal que posibilita la sujeción a ésta de las infracciones contra ciertos bienes o intereses estatales cometidos fuera del territorio del país emisor de la norma jurídica penal; es decir, atiende primordialmente a la naturaleza e importancia del bien jurídico protegido agredido por el delito, sin que importe el lugar donde fue ejecutado el hecho ni la nacionalidad de sus autores (por ejemplo, un grupo de extranjeros, en un país distinto, fabrican moneda argentina falsa). Con carácter excepcional y subsidiario, se aplican los principios de la nacionalidad o de la personalidad (cuando el autor o la víctima son nacionales, en relación a un delito cometido en el extranjero, y funciona mediante tratados de extradición) y el principio universal o de justicia mundial (que se persiguen en cualquier país, porque lesionan bienes jurídicamente reconocidos por toda la comunidad internacional, como el caso de los delitos llamados de lesa humanidad).

No todos los países aplican las mismas reglas para determinar la ley aplicable y la competencia judicial. Para poder clarificar estas cuestiones es necesario establecer cuál es la normativa de derecho internacional que rige la relación con cada Estado (convenios bilaterales y tratados internacionales).

La cuestión no es fácil de resolver tampoco a nivel investigativo, lo cual será especialmente tratado en el capítulo a continuación.

Bibliografía

Buompadre, J.E. (2013). Manual de Derecho Penal. Parte Especial. Buenos Aires: Astrea.

Council of Europe. (2004). Convention on Cybercrime ETS No185. Budapest, Hungría. 01/07/2004. Recuperado 01 julio 2016, de http://conventions.coe.int/Treaty/en/Treaties/html/185¬SPA.htm

D'Alessio, A.J. & Bertolino. (2008). Análisis de la ley 26388 de reforma al Código Penal en materia de delitos informáticos. Revista de Derecho Penal y Procesal Penal, 2008(7), pág. 1217.

D'Alessio, A.J. (2011). Código Penal de la Nación Comentado y anotado. (2 nd ed.). Buenos Aires: La Ley.

Donna, E.A. (2000). Derecho Penal Parte Especial, Tomo III. Buenos Aires: Rubinzal Culzoni Editores.

Duarte, A. (Julio 2014). Ley de Grooming ¿Una nueva herramienta para el ciberacoso?. Revista del Ministerio Público Provincia de Buenos Aires, Año 11(15), 25/8. Recuperado 01 julio 2016, de https://www.mpba.gov.ar/web/revista/RevistaNro15-web.pdf

Figari, R. (2010, 26 de Julio). Daño informático (arts 183, 2º párr y 184 incs 5º y 6º del CP Ley 26388). [Weblog]. Recuperado 01 julio 2016, de http://www.rubenfigari.com.ar/dano-informatico-arts-183-2%C2%BA-parr-y-184-incs-5%C2%BA-y-6%C2%BA-del-c-p-ley-26-388/

Figari, R. (2010, 26 de Julio). Reflexiones sobre la defraudación informática (ley 26388). [Weblog]. Recuperado 01 julio 2016, de from http://www.rubenfigari.com.ar/reflexiones-sobre-la-defraudacion-informatica-ley-26-388-2/

Gutierrez, R, Radesca, L.C & Riquert, M.A. (2013). Art. 153 bis. Violación de Secretos y de la Privacidad. Revista Pensamiento Penal, Nov(14). Recuperado 01 julio 2016, de http://www.pensamientopenal.com.ar/system/files/cpcomentado/cpc37761.pdf

Gutierrez, R, Radesca, L.C & Riquert, M.A. (2013). Art. 153. Violación de Secretos y de la Privacidad. Revista Pensamiento Penal, Nov(14). Recuperado 01 julio 2016, de http://www.pensamientopenal.com.ar/system/files/cpcomentado/cpc37762.pdf

Hocsman, H.S. (2005) Negocios en internet. Buenos Aires : Astrea.

http://www.elderechoinformatico.com/publicaciones/mtemperini/JAIIO_Temperini_Marcelo_Delitos_Informaticos_Hacking.pdf

Huilcapi Peñafiel, A.O. (2010) El delito informático, en el que se citan autores tales como Nidia Callegari, Carlos Sarzana y María de Luz Lima; citado por Tobares Catalá, Gabriel H.- Castro Argüello, Maximiliano J.; Delitos Informáticos. Buenos Aires. Edit. Advocatus. pág. 28.

Medina, V. ([sd]). Estafa con tarjetas de crédito. Recuperado 01 julio 2016, de http://www.terragnijurista.com.ar/doctrina/estafa_tarjetas.htm

Ministerio de Justicia y Derechos Humanos de la Nación. Sitio web Infoleg. Recuperado 01 de julio 2016, de: http://www.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

Naciones Unidas (2000). Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía. Dictado por la Asamblea General de las Naciones Unidas el 25/-05/-2000. Recuperado 01 de julio 2016, de http://www.unicef.org/spanish/specialsession/documentation/documents/op_se_sp.pdf

Naciones Unidas (2005) A/CONF.203/14/ 11º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. Bangkok, 18 a 25 de abril de 2005.–. Recuperado 01 julio 2016, de http://www.un.org/es/conf/11thcongress/documents.html.

Palazzi, P. (2008). Análisis del proyecto de ley de delitos informáticos aprobado por el Senado de la Nación en el año 2007. Revista de Derecho Penal y Procesal Penal, Abril-Mayo (2008), Recuperado 01 de julio 2016, de http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/188231/texact.htm

República Argentina, Poder Judicial Cámara Nacional de Apelaciones en lo Criminal y Correccional - Sala 4. (2012). SDL, JA s/ Infracción art 157 bis del CP - Causa n° 2079/11 - 8/3/2012. Recuperado 01 julio 2016, de http://judicialdelnoa.com.ar/jurisprudencia/fallo_sldja_ccc.pdf

República Argentina, Poder Judicial Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala 7 - CCC 70199/2013/CA1 - B., R. Inadmisibilidad de querella. Violación de sistema informático. Correccional 1/52. 06/05/2014 Recuperado 01 julio 2016, de http://www.pensamientopenal.com.ar/system/files/2014/12/Fallos39045.pdf

República Argentina, Poder Judicial Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala 7 R. P.M. s/ Violación de secretos. Inst. 43/109. 07/05/2012. Recuperado 01 julio 2016, de: http://www.pjn.gov.ar/Publicaciones/00017/00051999.Pdf

República Argentina, Poder Judicial Cámara Nacional de Apelaciones en lo Criminal y Correccional - Sala 2a. Fallo “Marchione, Gabriel” Daño a un sistema informático - Remisión masiva de mensajes con virus (spam) Interrupción del servicio de comunicaciones. C. Nac. Crim. y Corr. Fed., sala 2a, 15/11/2005.

República Argentina. Ministerio de Justicia y Derechos Humanos y UNICEF. Sitio web Con Vos en la Web. Recuperado 01 de julio 2016, de http://www.convosenlaweb.gob.ar

República Argentina. Ministerio de Justicia y Derechos Humanos. (2016) Creación del Programa Nacional Contra la Criminalidad Informática en la órbita del Ministerio de Justicia. Resolución Ministerial 69/16. Emitida el 11 de Marzo de 2016. Boletín oficial, 18 de Marzo de 2016. Id SAIJ: NV14027.

Resolución Conjunta 866/2011 y 1500/2011 de la Jefatura de Gabinete de Ministros y el Ministerio de Justicia y Derechos Humanos de la Nación. Versión online disponible en: http://www.informaticalegal.com.ar/2011/10/05/resolucion-conjunta-8662011-y-15002011-jefatura-de-gabinete-de-ministros-y-ministerio-de-justicia-y-derechos-humanos-comision-tecnica-asesora-de-cibercrimen/

Riquert, M.A. (2008, 12 julio). Delito de alteración dolosa de registros (art 12 Ley Penal Tributaria). [Weblog]. Recuperado 01 de julio 2016, de http://riquert-penaltributario.blogspot.com.ar/2008/07/delito-de-alteracin-dolosa-de-registros.html

Riquert, M.A. Violación de secretos y de la privacidad. en Revista Pensamiento Penal online http://www.pensamientopenal.com.ar/system/files/cpcomentado/cpc37761.pdf Accesible: julio 2016.

Rovira del Canto, E. (2010). Trabajo para la Primer Jornada TIC sobre Ciberdelincuencia. Recuperado 01 de julio 2016, de http://www.iaitg.eu/mediapool/67/671026/data/Ciberdelincuencia_intrusiva_hacking_y_grooming_Enrique_Rovira.pdf

Sáez Capel-Velciov (2008) “Comentario al art. 153bis” pub. en AAVV “Código Penal”, dirigido por Baigún y Zaffaroni. Buenos Aires. Ed. Hammurabi. Tomo 5.

Sitio web “Pensamiento Penal”. Accesible: junio 2016. Disponible en: http://www.pensamientopenal.org.ar/la-responsabilidad-penal-de-las-personas-juridicas/

Temperini, M. (2011) Delitos Informáticos: La punibilidad del Hacking y sus consecuencias. Revista Pensamiento Penal - Edición 132 - 03/10/11. Versión online disponible en: http://media.wix.com/ugd/d4d349_064797ed43ee4042bb17d7ace2507620.pdf

Tobares Catalá, G. H.-Castro Argüello, M. (2010) J.; Delitos Informáticos. Buenos Aires. Edit. Advocatus.

Vaninetti, H. A. (2010) Aspectos jurídicos de Internet; Librería Editora Platense. La Plata. pág. 383.

Von Listz, F. (1999) Tratado de Derecho penal, trad. de la 20a ed. alemana por Luis Jiménez de Asúa, adicionado con el Derecho penal español por Quintiliano Saldaña, t. II, 4a ed. Reus. Madrid. p. 6.

Zaffaroni, E.R. (2003); Manual de Derecho Penal. Parte general. Edit. EDIAR. 6° edición, 3ra. reimpresión.

Capítulo 3. Investigación Criminal y Penal

Autores: Fernanda Giaccaglia, Luciano Nuñez y Sabrina Lamperti.

1. Aspectos Procesales.
2. La Investigación Penal Preparatoria.

   2.1. Denuncia. 2.2. Investigación Criminal. 2.3. Metodología de la investigación en el lugar del hecho. 2.4. El reconocimiento de la escena. La inspección ocular. Observación. 2.5. Documentación: Descripción. 2.6. Fotografías forenses. Escalas. Principios de Análisis. 2.7. La informática forense en el lugar del hecho. 2.8. Recolección de la evidencia. Cadena de Custodia.

3. Los desafíos en la investigación de los delitos informáticos.
4. Medidas Probatorias.

1. Aspectos Procesales

El profesor argentino Julio Maier define al derecho procesal penal como la rama del orden público interno del Estado, cuyas normas instituyen y organizan los órganos públicos que cumplen la función judicial penal del Estado y disciplinan los actos que integran el procedimiento necesario para imponer y actuar una sanción o medida de seguridad[94].

En términos coloquiales, los códigos procesales establecen de qué modo se llevarán a cabo las investigaciones y cómo se desarrollarán los juicios penales, y son dictados por cada legislatura provincial.

Estos códigos procesales tienen su razón de ser y están fundamentados en la Constitución Nacional y Tratados Internacionales -con jerarquía constitucional- (como derivación del artículo 75, inciso 22 del mencionado cuerpo legal) que especifican algunos de los principios que deben regir en esta materia. Entre ellos se destacan los siguientes:

- Artículo 75, inciso 12, la atribución de dictar el Código Penal.
- Artículo 18, la necesidad de contar con un juicio previo para la aplicación de penas.
- Artículo 60, ese juicio deberá estar basado en una acusación.
- Artículo 18, la garantía del juez natural.
- Artículo 120, función del Ministerio Público de promover la actuación de la justicia.
- Artículo 18, inviolabilidad de la defensa del imputado.

Todos estos principios contenidos en la Constitución Nacional, necesitan de un conjunto de normas jurídicas

[94] Maier, J. (2013). Derecho Procesal Penal. Buenos Aires: Editores del Puerto.

reglamentarias que coadyuven a la aplicabilidad real de los mismos, y a los principios jurídico-políticos que las inspiran.

Estas normas reglamentarias constituyen el contenido del Derecho Procesal Penal que se integra con las leyes de organización del Ministerio Público Fiscal y los Tribunales Penales, y con los Códigos Procesales Penales.

Teniendo como punto de partida que el *derecho penal* no puede ser aplicado sin juicio previo, el *derecho procesal penal* aparece para canalizar la pretensión penal ante la denuncia de la comisión de un delito, y garantizar que se imponga la pena que corresponda.

2. La Investigación Penal Preparatoria

El Libro Segundo del Código Procesal Penal de la Provincia de Buenos Aires que inicia con el artículo 266[95] determina explícitamente la finalidad de la *Investigación Penal Preparatoria.*

Será el Ministerio Público Fiscal quien tenga a su cargo esta etapa cuyo objetivo principal es reunir las pruebas necesarias para fundar la acusación. En este procedimiento, el juez sólo tendrá a su cargo controlar si las garantías

[95] Art. 266 CPCBA: Finalidad. La Investigación Penal Preparatoria tendrá por finalidad:

1) Comprobar, mediante las diligencias conducentes al descubrimiento de la verdad, si existe un hecho delictuoso.

2) Establecer las circunstancias que lo califiquen, agraven, atenúen, justifiquen o incidan en su punibilidad.

3) Individualizar a los autores y partícipes del hecho investigado.

4) Verificar la edad, educación, costumbres, condiciones de vida, medios de subsistencia y antecedentes del imputado; el estado y desarrollo de sus facultades mentales, las condiciones en que actuó, los motivos que han podido determinarlo a delinquir y las demás circunstancias que revelen su mayor o menor peligrosidad.

5) Comprobar a los efectos penales, la extensión del daño causado por el delito".

constitucionales fueron debidamente observadas, y su sustento probatorio. De allí que a esta función judicial se le llame "Juez de Garantías" o "Juez de Control".

En cualquier tipo de proceso judicial, ya sea en el fuero civil o laboral, generalmente es necesario que la parte actora realice una investigación previa tendiente a fijar los alcances del reclamo y reunir los elementos de prueba necesarios para fundarlo. Sin embargo, en el proceso penal, la participación de la víctima en la investigación preparatoria es opcional, y no está prevista en las leyes procesales como obligatoria. En caso de querer asumir un rol activo en la investigación, podrá constituirse como *particular damnificado*.

La mayoría de los casos que serán investigados por el Ministerio Público Fiscal corresponderán a *delitos de acción pública*. En estos supuestos determinados por el Código Penal y en los que están en juego la naturaleza de los hechos, el bien jurídico protegido o el interés público afectado, es el órgano estatal encargado de promover la persecución penal quien intervendrá en su esclarecimiento. El código procesal penal regula esta intervención en una *etapa preparatoria* que debe ocurrir obligatoriamente y es de carácter oficial. Se la conoce con el nombre de *Investigación Penal Preparatoria*, en adelante IPP.

Para el análisis del tema es preciso tomar como punto de partida que todo proceso penal tiene como principal finalidad la averiguación de la verdad material. Esto significa, aquella verdad que sea posible acreditar con las pruebas que luego se producirán en el juicio.

Esta primera *etapa preparatoria* se define como el conjunto de todas aquellas actividades de adquisición

probatoria necesarias para sostener válida y razonablemente una pretensión punitiva[96].

Es así que los objetivos principales de esta etapa de investigación dentro del sistema acusatorio previsto por la Ley 11.922 se relacionan con el análisis de la existencia del delito, y la determinación de si el presunto autor resulta o no responsable del mismo, todo ello en vistas a la *preparación* del juicio oral y público donde se juzgará al acusado en base a las pruebas reunidas en esta etapa por el hecho que le es endilgado.

Esta primera etapa presenta las siguientes finalidades:

- Actuar como filtro de juicios innecesarios. Es decir, la prueba que se obtenga en esta etapa justificará (o no) la realización del juicio.
- Intervenir de manera inmediata posibilitando la recolección de la prueba más importante, con el objeto de comprobar la existencia del hecho denunciado.
- Individualizar la participación de los posibles autores, evitando que puedan eludir la justicia.
- Precisar el objeto del juicio a llevarse a cabo, y sus posibles autores.

Caracteres

La IPP presenta los siguientes caracteres:

- Es *preparatoria del juicio*, ya que su finalidad es fundar la acusación o determinar el sobreseimiento.
- Es *escrita*, ya que todos los actos que se realicen (aunque algunos puedan ser orales, como la

[96] Vázquez Rossi, J. E. (2008) Derecho Procesal Penal. Buenos Aires: Rubinzal Culzoni.

declaración del imputado) deberán hacerse constar en actas.

- Es *contradictoria*, ya que la ley autoriza a las partes a proponer diligencias, las cuales podrán ser ordenadas por el fiscal si las considera útiles o pertinentes.
- Es *pública,* al menos para las partes, y ello deriva en el *principio de contradicción*, que supone el conocimiento por la parte acusada de todos los actos que se producen en su contra. En aquellos casos en que el Ministerio Público Fiscal deba realizar alguna actuación en pos del éxito de la investigación y para ello no deba notificar al acusado, tiene la obligación de peticionarlo al Juez de Garantías (como ocurre en los casos de pedidos de allanamientos y secuestros, por ejemplo), en aras del resguardo de las garantías constitucionales del imputado, especialmente la de inviolabilidad de la defensa en juicio.
- *Desformalizada*, como se indicará en el siguiente punto.

Desformalización

Existe una importante tendencia a la desformalización de esta etapa investigativa. Sin embargo, lo esencial será no perder de vista la importancia de la preservación y respeto de las garantías constitucionales.

Esto ha sido reafirmado por el Tribunal de Casación Penal al decir que

> *"(...) En la ley 11.922, la investigación previa no es algo totalizador y acabado, sino un ensamble provisorio, armado a la luz del criterio de oportunidad e instrumentado a la luz de la desformalización. Sólo en el debate se adquirirán y valorarán luego las pruebas que asumirán rol decisivo y en este mismo*

momento, precisamente, se corporizará la acusación fiscal (...)"[97].

La idea que subyace es que formalizar esta etapa podría traer como consecuencia el retraso innecesario del proceso. Será en la audiencia oral donde los elementos recolectados se someterán al contradictorio entre las partes. Entonces, esta primera etapa sólo estará dirigida a recoger los elementos de convicción que permitan decidir si corresponde el archivo, el sobreseimiento o la acusación.

Modalidades de inicio

Frente a la toma de conocimiento de la presunta comisión de un hecho delictivo, se pone en marcha la reacción del Estado, encaminada principalmente a otorgar certeza a dicho conocimiento. La modalidad en la que es recibida la noticia de la existencia de ese hecho determinará el modo de inicio.

Al conocerse la posible comisión de un delito de acción pública, el Ministerio Público Fiscal por sí, o por intermedio de las fuerzas policiales (en un supuesto de urgencia) son los encargados de dar inicio a la investigación penal.

Dada la inmensidad de causas penales en trámite, sería iluso pensar que el fiscal atenderá personalmente todas ellas. Por esta razón, la legislación le asigna al fiscal atribuciones para ordenar a los agentes policiales que actúen bajo su mandato supliendo así su presencia directa en todas las situaciones[98].

Sin embargo, es el Ministerio Público Fiscal quien dirigirá la actuación policial, debiendo estar informado de todo lo que hacen las fuerzas de seguridad a quienes se les pudo

[97] T.C.P.B.A., sala 1 LP, P 549 RSD-136-1, S 10/4/2001.
[98] Granillo Fernández, H. & Herbel, G. A. Código de Procedimiento Penal de la Provincia de Buenos Aires. (2° Edición Actualizada y Ampliada). Buenos Aires: La ley.

haber delegado la realización de medidas investigativas. Esta idea de subordinación de la policía al Ministerio Público refuerza la vinculación legal en el uso de la fuerza contra los ciudadanos[99], y es propia de un Estado de Derecho.

En este esquema procesal, el organismo de persecución penal tiene la responsabilidad de instar a la investigación de los delitos de acción penal pública, a fin de preparar los elementos de cargo o descargo que den base al juicio[100].

En relación a la forma de iniciación, y de acuerdo a lo establecido en el artículo 268 del CPPBA, la IPP podrá originarse en una denuncia, en la prevención policial o en cualquier forma de noticia sobre un hecho pasible de encuadrar en una norma punitiva.

En rigor de verdad, la mayor parte de las causas penales se originan en la noticia receptada por la agencia policial. Es por este motivo, y por la facultad de responder con celeridad ante estos conflictos, que la normativa procesal dota a la policía de varias atribuciones, entre ellas, detener la continuación de los hechos delictivos, individualizar a los presuntos culpables, preservar el lugar del hecho y reunir toda información que resulte útil a la investigación. Sin perjuicio de estas atribuciones, cuentan con la obligación de dar aviso inmediato al Ministerio Público Fiscal, dado que las fuerzas policiales actúan como auxiliares de la justicia.

Una vez practicadas las diligencias investigativas estimadas útiles y pertinentes para esclarecer el hecho, el Ministerio Público Fiscal deberá analizar los elementos de juicio colectados, con el objeto de alcanzar un estado de convicción que le permita definir qué trámite conviene en el caso.

---

[99] Falcone, R. - Madina, M.; El Proceso Penal en la Provincia de Buenos Aires. Edit. Ad Hoc, 2005, pág. 35/6

[100] Maier, J. (1975) La investigación penal preparatoria del Ministerio Público. Buenos Aires: Ed. Lerner.

De acuerdo al *“principio de legalidad”* si el supuesto a investigar no puede ser encuadrado dentro de una figura penal, la investigación no puede comenzar, y en consecuencia se desestima. Se trata de un principio constitucional que pregona que para comenzar una persecución penal, el hecho que la motive debe estar previsto en la ley sustantiva.

Por otra parte, si de las medidas de investigación que se hayan realizado, no surge la materialidad delictiva, es decir, no se puede acreditar lo que se denuncia, o no se ubica al autor que lo comete, el fiscal cuenta con la posibilidad de archivar las actuaciones.

En cambio, si los indicios recolectados permiten acreditar tanto la existencia del hecho denunciado como el autor que lo cometió, el fiscal debe citarlo para que brinde su versión de los hechos, y así pueda ejercer su defensa. Este acto se lo suele denominar “declaración indagatoria” o “llamado a tenor del art. 308 del CPP”, que es el artículo del Código de Procedimientos que lo regula, en la Pcia. de Buenos Aires.

Resulta de importancia mencionar que todos los actos cumplidos por el fiscal y por la policía en esta primera etapa, no podrán constituir prueba. Esto es, sólo se trata de pruebas necesarias para justificar la citación a prestar declaración del imputado, y luego para sustentar la requisitoria de elevación a juicio e identificar los elementos que luego podrán ser producidos en la etapa del juicio oral. Esto no impide que luego puedan ser incorporados como prueba al juicio, pero deberán cumplir con las formalidades legales establecidas.

Duración de la IPP

En principio, no existe plazo para realizar una denuncia. Sin embargo, existen obstáculos constitucionales para iniciar o continuar una investigación cuando transcurre desde la fecha del hecho, el plazo total de prescripción para el delito que se denuncia.

Una vez iniciada la investigación y convocado el autor a prestar su declaración de descargo (art. 308 del C.P.P.) o bien desde la detención de una persona, según lo establecido el art. 282 del Código Procesal Penal, el plazo en el que debe concluirse esta etapa preparatoria es de cuatro meses con posibilidad de ampliarse hasta seis meses más, por razones motivadas del fiscal entre las que se encuentra la gravedad o dificultad de la investigación[101].

La razonabilidad en el tiempo de duración del proceso debe estar afectada únicamente por las dificultades específicas de la causa y, en su caso, por las propias del órgano jurisdiccional, pero sin que estas últimas (...) afecten los intereses de quien, privado de su libertad, espera la definición de su situación[102].

2.1 Denuncia

La denuncia ha sido definida como una manifestación de voluntad de una persona que pone en conocimiento de la existencia de un delito de acción pública a una autoridad competente para recibirla[103].

Se trata de una facultad discrecional de las personas y su eventual obligatoriedad estará relacionada con la función que cumplan.

La denuncia podrá ser realizada por cualquier persona que pueda resultar imputable, esto es, porque será pasible de

[101] Bertolino, P. J. (2009) Código Procesal Penal de la Provincia de Buenos Aires Comentado y Anotado con jurisprudencia provincial. (9na ed. actualizada). Buenos Aires: Abeledo Perrot.
[102] Cámara Apelaciones y Garantías Morón, Sala II, causa 14.587, 15/04/2003.
[103] Vélez Mariconde, A. (1986) Derecho Procesal Penal. Buenos Aires: Editorial Astrea.

la aplicación del artículo 245[104] del Código Penal, que castiga el falso testimonio. Lo que se busca con este castigo es la seriedad de las denuncias.

Únicamente podrán ser denunciados los delitos de acción pública, ya sea que resulten perseguibles de oficio o sean dependientes de instancia privada. En este último caso, sólo podrán ser denunciados por su ofendido, tutor, curador, guardador o representante legal, y será necesaria una suerte de legitimación especial para formular denuncia por encontrarse restringida la posibilidad de efectuarla, ya que no es posible formar causa sin el consentimiento del agraviado.

En cuanto a la forma de presentación, la denuncia podrá ser realizada de manera escrita o verbal (en cuyo caso el denunciante será convocado a testimoniar a dichos efectos).

En todos los casos, el funcionario que la recibe deberá constatar la identidad del denunciante, ya que no son posibles las denuncias anónimas. Sin embargo, el llamado telefónico anónimo puede permitir la actuación policial o judicial para prevenir que los actos delictivos lleguen a consecuencias aún más graves. No obstante, ello no implica que pueda ser considerado como un elemento de convicción para realizar petición alguna, a menos que esté acompañado de otros datos que le aporten solidez[105].

Si bien al comienzo del acápite se menciona que la denuncia es una facultad “discrecional” de la persona, existen algunos supuestos en los cuales algunas personas se encuentran obligadas a denunciar.

Estos casos, detallados en el artículo 287 del CPPBA, son los siguientes:

---

[104] Artículo 245, Código Penal Argentino: “Se impondrá prisión de dos meses a un año o multa de pesos setecientos cincuenta a pesos doce mil quinientos al que denunciare falsamente un delito ante la autoridad”.
[105] Granillo Fernández, F. *Op. Cit.*

Inciso 1°: Se trata de aquellos hechos advertidos por los funcionarios o empleados públicos en ocasión o en el ejercicio de las funciones a su cargo. Quedan excluidas aquellas noticias que adquieren como simples particulares, ya que en estos supuestos la denuncia será facultativa.

Inciso 2°: Es el caso de personas que ejercen el arte de curar. Las conductas deben presentar cierta entidad y tener la característica particular de ir contra la vida y la integridad física, además de ser de acción pública.

Inciso 3°: Se dirige a aquellos que, en virtud de lo normado por el artículo 277 inciso d del Código Penal, incurran en el delito de encubrimiento por omitir la denuncia cuando estuvieren obligados a promover la persecución.

Denuncia ante el Juez

Este supuesto se encuentra reglado en el artículo 290 del CPPBA, y determina que la toma de conocimiento por parte del juez de una hipótesis delictiva no tiene otra perspectiva que su comunicación al Ministerio Público Fiscal. Esto se debe a que éste tiene “exclusividad” en el ejercicio de la acción penal pública y es quien dirige y practica la investigación penal preparatoria.

Denuncia ante el Ministerio Público Fiscal

En este supuesto, el agente fiscal deberá comunicarle de inmediato al juez de garantías. Luego de ello, el fiscal sin otra formalidad debe proceder a la pesquisa que corresponda en el caso, realizando los actos investigativos necesarios para esclarecer el hecho y determinar quién es su autor.

Denuncia ante la policía

Se trata, en definitiva, de la forma más común de recibir denuncias. En este supuesto, la policía tiene la obligación de comunicar inmediatamente al fiscal.

Los órganos policiales cuentan con las facultades que les otorga el artículo 294 del CPPBA: recibir denuncias; cuidar que los rastros materiales que hubiere dejado el delito sean

conservados y que el estado de las cosas no se modifique hasta que llegue al lugar el Ministerio Público Fiscal; disponer, en caso necesario, que ninguna de las personas que se hallare en el lugar del hecho o sus adyacencias, se aparten del sitio mientras se llevan a cabo las diligencias que correspondan; si hubiere peligro de que cualquier demora comprometa el éxito de la investigación, hacer constar el estado de las personas, de las cosas y de los lugares, mediante inspecciones, planos, fotografías, exámenes técnicos y demás operaciones que aconseje la policía científica; disponer los allanamientos del artículo 222 y las requisas urgentes, con arreglo del artículo 225, con inmediato aviso al juez o tribunal competente y al Ministerio Público Fiscal; interrogar a los testigos; aprehender a los presuntos autores y/o partícipes en los casos y formas que este código autoriza, entre otros.

En tales casos, tiene la posibilidad de realizar actuaciones de prevención comunicando luego el resultado al Ministerio Público Fiscal.

2.2 Investigación criminal

Desde el campo de la criminalística es preciso hacer referencia al concepto de *investigación criminal*, definida como la actividad encaminada a la indagación y explicación de la conducta delictiva, consiguiendo el descubrimiento de los hechos y técnicas desarrolladas por el autor del delito, y cuyo fin es aportar las pruebas necesarias a la autoridad judicial para su enjuiciamiento[106].

Ante la noticia de un hecho delictivo, el Ministerio Público Fiscal interviene asumiendo la defensa de los

[106] MPBA (2016). Manual de procedimiento para la preservación del lugar del hecho y la escena del crimen. Accesible: junio 2016. Disponible en: http://www.mpba.gov.ar/web/contenido/Lugar%20del%20hecho.pdf

intereses sociales y del respeto a los valores constitucionales y legales que se encuentren involucrados.

El principio esencial en toda investigación criminal será la protección del lugar del hecho, a fin de evitar que toda persona ajena pueda alterar las circunstancias reales, como así también, evitar que dejen sus propias improntas en los escenarios criminosos.

Al momento de iniciar una investigación criminal, la etapa preparatoria es esencial. Todo lo que se realice durante esta primera etapa de análisis permitirá fundar la acusación que lleve a juicio al posible imputado. Es aquí justamente, donde los derechos y garantías de las personas corren mayor riesgo de ser vulnerados.

Es el Estado, como instrumento de la organización social, el que establece los principios fundamentales del Derecho tendientes a garantizar los derechos de los ciudadanos, representando así las garantías constitucionales determinadas en la Constitución Nacional.

Las garantías procesales serán aquellas instituciones o procedimientos de seguridad creados para garantizar el bienestar de las personas, y brindar los medios o instrumentos que hagan efectivo el goce de sus derechos. Desde de estas garantías procesales se encuentran las relacionadas al procedimiento durante la investigación del hecho punible, donde los peritos y auxiliares juegan un rol fundamental, a través de su intervención en la producción de la prueba llevada a juicio.

2.3 Metodología de la investigación en el lugar del hecho

Muchos autores coinciden en la idea de caracterizar al *lugar de los hechos*, también conocido como *escena o escenario del crimen*, como aquel sitio o espacio físico en el cual se ha cometido un hecho que podría ser caracterizado como un delito.

En la República Argentina, con la implementación del *Protocolo de Actuación para la Preservación de la Escena del Hecho y sus Pruebas* a través del Ministerio de Seguridad de la Nación, estos conceptos han sido separados en su definición, siendo que, para ***lugar de los hechos***, se atribuye al *"espacio físico en el que se ha producido un acontecimiento susceptible de una investigación científica criminal con el propósito de establecer su naturaleza y quiénes intervinieron"*[107] diferenciándose de la ***escena de crimen*** *"cuando la naturaleza, circunstancias y características del acontecimiento permitan sospechar la comisión de un delito"*[108]*.* Es así que, el *lugar de los hechos,* pasa a ser la *escena de crimen*.

De esta manera, el **lugar del hecho** es una **potencial escena del crimen**; siendo uno u otra, una zona inviolable a la que corresponde inmediatamente su preservación para garantizar la intangibilidad de los elementos, rastros o indicios que puedan existir y evitar cualquier pérdida, alteración o contaminación. En ellas deberán estar presentes sólo los profesionales judiciales, especialistas y/o peritos, judiciales o policiales, quienes a través del estudio del caso en particular deberán analizar las posibles hipótesis a plantear en el caso[109].

Toda investigación criminal, en la mayoría de los supuestos, comienza en el lugar de los hechos. La inspección

---

[107] Protocolo de Actuación para la Preservación de la Escena del Hecho y sus pruebas. Programa Nacional de Capacitación de la Secretaría de Seguridad, del Ministerio de Justicia, Seguridad y Derechos Humanos. Tit I, Cap I. P. 4.

[108] Protocolo de Actuación para la Preservación de la Escena del Hecho y sus pruebas. Programa Nacional de Capacitación de la Secretaría de Seguridad, del Ministerio de Justicia, Seguridad y Derechos Humanos. Tit I, Cap I. P. 4

[109] *Protocolo Federal de Preservación*. Accesible: julio 2016. Disponible en: http://www.jus.gob.ar/media/183597/Protocolo%20Federal%20de%20Preservacion.pdf

criminalística que comienza a partir de este punto, tiene por objeto verificar el hecho, ubicar, evaluar y recolectar indicios o evidencias, recabar datos y testimonios vinculantes, y hacer una apreciación reconstructiva preliminar del caso. Su importancia radica en que guarda los indicios y evidencias que van a permitir el esclarecimiento de la verdad estableciendo la forma y mecanismos de los hechos[110]. Sucede entonces que, cuando no se recogen y analizan de manera correcta todos los indicios que resulten relevantes del escenario del crimen, fuente primordial de la información indiciaria, la investigación resultará más compleja.

El escenario del crimen puede estar constituido por un espacio abierto (cuando carece de límites geográficos), cerrado o mixto. Lo importante a tener en cuenta es que no sólo se deberá tener en cuenta el lugar específico donde se llevó a cabo el presunto hecho delictivo, sino que también sus alrededores, que podrán ser considerados como vías de acceso. Hoy se tiende a delimitar el escenario de un crimen con tres perímetros de protección bien diferenciados y con diferentes atributos. Un perímetro más alejado o externo, que será aquel que delimite el ingreso de curiosos y personal no indispensable en la investigación. Un segundo anillo interior o intermedio que se constituye en una zona de comando o toma de decisiones y apoyo logístico y, el tercer espacio, que es el central, constituido por la escena del crimen o lugar del hecho propiamente dicho.

No podrá perderse de vista que todas las medidas que se realicen tendrán como principal finalidad evitar el cuestionamiento respecto del levantamiento y la custodia de los indicios que se encuentren allí, y que luego serán presentados ante la autoridad jurisdiccional, por lo que se debe evitar cualquier sospecha sobre su validez legal.

[110] Guzmán, C. A. (2010) El examen en el escenario del crimen. Buenos Aires: Editorial Bdef.

Es por tal motivo que todas las evidencias localizadas en la escena del crimen, y que puedan estar relacionadas con la comisión del presunto hecho ilícito deberán ser correctamente protegidas en el lugar donde sucedieron, para luego poder entregárselas a los especialistas para que realicen los análisis que correspondan. El Dr. Hanns Gross, uno de los padres de la Criminalística moderna, decía que *"si la inspección ha de ser útil, es imprescindible que todos los objetos importantes o no que figuran en el lugar del crimen, permanezcan intactos, sin que por ninguna causa se les cambie de posición"*[111].

En el ámbito de la realidad, muchas veces, las intervenciones urgentes en la escena del crimen reducen de manera considerable el margen de planificación y control del Ministerio Público Fiscal. Lo que sucede generalmente es que los primeros en tomar contacto con la evidencia que será luego recolectada son los miembros de la policía de seguridad, que son quienes reciben la noticia del presunto hecho criminal y deberán proceder a ejecutar las medidas impostergables, con comunicación inmediata al Ministerio Público. Todo esto, respetando lo establecido en los artículos 294, 296 y 297 del CPP, y el artículo 11 de la Ley 13.482.

Resulta sumamente importante que el oficial/agente interventor que responde primariamente al llamado, proteja adecuadamente este escenario ya que la investigación completa gira sobre la base de que esa primera persona sea capaz de identificar, aislar y asegurar el lugar[112].

El funcionario policial o de la fuerza de seguridad que primero arribe al lugar del hecho será el responsable de la protección inicial del espacio físico y de los indicios o rastros que allí se encuentren. Se procurará mantener la

[111] Gross, H. (1894) Manual del Juez. Est. Tip. Viuda e Hijos de M. Telloi. Madrid, España.
[112] Guzmán,C.A. *Op. Cit.*

intangibilidad del espacio físico en el que pudieran hallarse elementos vinculados con el presunto hecho delictivo, a los fines de evitar cualquier tipo de contaminación.

Esta situación configura una ventana de riesgo en cuanto a las cuestiones de preservación de la evidencia que deberá tratar de minimizarse con la correcta capacitación de los efectivos policiales en cuestiones de manejo temprano de la escena del crimen.

En la *Guía Integral de Empleo de la Informática Forense en el Proceso Penal* elaborada por el Laboratorio de Investigación y Desarrollo en Informática Forense (InFo-Lab)[113] y aprobada por la Procuración General de Justicia de la Provincia de Buenos Aires, se recomendó la aprobación de un protocolo de actuación para el personal interviniente en las diligencias urgentes donde pueda hallarse evidencia digital.

En el mismo sentido, el Ministerio de Seguridad de la Nación ha dictado recientemente la Resolución 234/2016, de fecha 07/06/2016 que aprueba el *"Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Proceso de Recolección de Pruebas en Ciberdelitos"*[114] por el cual se reconoció el incremento de los delitos cometidos mediante las nuevas tecnologías de la información y las comunicaciones, y la necesidad de capacitar y dotar a las fuerzas de seguridad y policiales con herramientas, métodos y procedimientos a fin de mejorar su

[113] Di Iorio, Ana H. y otros.(2016) Guía integral de empleo de la informática forense en el proceso penal. 2° edición revisada, Mar del Plata, Universidad FASTA. Accesible: julio 2016. Disponible en: http://info-lab.org.ar/images/pdf/PAIF.pdf

[114] Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Proceso de Recolección de Pruebas en Ciberdelitos. Disponible en: http://www.informaticalegal.com.ar/2016/06/07/resolucion-2342016-del-ministerio-de-seguridad-protocolo-general-de-actuacion-para-las-fuerzas-policiales-y-de-seguridad-en-la-investigacion-y-proceso-de-recoleccion-de-pruebas-en-ciberdelitos/

investigación y procurar la correcta conservación de la evidencia digital.

Todo esto, en el entendimiento que la adecuada obtención, conservación y tratamiento de este tipo de evidencia constituye un elemento clave para asegurar el éxito de las investigaciones.

Una vez preservado el lugar del hecho por las fuerzas de seguridad que intervinieron en este primer momento, comienza la etapa de la investigación en sí, la cual consta de tres etapas bien diferenciadas que surgen de llevar un orden o método de abordaje para lograr la máxima eficiencia en la labor forense, a fin de poder identificar los indicios, hacer su correcto levantamiento y conservación y realizar una minuciosa documentación del lugar del hecho. Estas etapas son: el reconocimiento de la escena, la documentación de la misma y, por último, la recolección de la evidencia.

2.4 El reconocimiento de la escena: La inspección ocular. Observación

La *inspección ocular* consiste en la descripción detallada, tanto narrativa como documental, del lugar del hecho, sus indicios y todos aquellos elementos que resulten inmediatamente relacionados con la investigación del hecho delictivo del que se trate. Se trata de un proceso metódico, sistemático y lógico que necesita de la observación integral de la escena[115].

Esta etapa se caracteriza por constituirse personalmente en el lugar del hecho para realizar la observación integral del mismo. Está a cargo de un coordinador que realiza un recorrido inicial del lugar a fin de tener un conocimiento íntegro de la escena. La finalidad es registrar la situación real

[115] MPBA. Criminalística. Accesible: julio 2016. Disponible en: http://www.mpba.gov.ar/web/contenido/curso%20ayudantes%20fiscales%20la%20plata%202011.pdf

de la escena, tomando nota mediante todos los medios técnicos posibles, preservando todos los indicios que luego se someterán a su correspondiente análisis.

Una vez que se encuentra verificada la autenticidad de la denuncia de un hecho consumado, la fuerza de seguridad comunicará la novedad al Juez de Garantías, Agente Fiscal competente y al Defensor Oficial, tal lo prescripto en el artículo 296[116] del CPPBA. Serán ellos quienes dispongan la presencia del equipo multidisciplinario de peritos, convocando al personal especializado de acuerdo a la naturaleza y circunstancias del hecho que se investiga.

El equipo de trabajo pericial debe ser coordinado por un responsable encargado de dirigir las acciones del resto de los peritos. Se aplican determinados métodos para el desarrollo de sus actividades en los escenarios de los hechos[117]:

- Delimitación y Preservación del lugar de los hechos.
- Observación del lugar.
- Graficación / fijación del lugar.
- Colección de indicios.
- Suministro de indicios al laboratorio.

Una vez arribados los peritos, éstos efectúan un relevamiento del lugar de acuerdo a una metodología de trabajo. La idea de trabajo es interdisciplinaria. Previo a seguir con cualquier otra tarea se realiza un relevamiento fotográfico

[116] Artículo 296, CPPBA: "Comunicación y actuación. Los funcionarios de Policía comunicarán inmediatamente al Juez de Garantías y Agente Fiscal competentes y al Defensor Oficial en turno, con arreglo al artículo 276 último párrafo, todos los delitos de acción pública que llegaren a su conocimiento. El Ministerio Público Fiscal o la Policía Judicial deberán intervenir de inmediato, salvo imposibilidad material que lo impida, en cuyo caso lo harán a la mayor brevedad posible".

[117] MPBA. Manual de procedimiento para la preservación del lugar del hecho y la escena del crimen. Op. Cit.

para de este modo dejar constancia de la posición y del estado que tenían los objetos y personas que se encontraban en el lugar del hecho al momento de la llegada de los peritos[118].

Es importante que en esta etapa se tome nota de todos los elementos que existan en el escenario del crimen y describirlos de manera que luego puedan ser utilizados de manera correcta para la planificación de las tareas a desarrollar.

Existen numerosos métodos para sistematizar esta labor, de acuerdo a si se trata de lugares abiertos o cerrados o bien de acuerdo a lo que se está buscando, si son objetos, indicios o cadáveres, pero en general, la regla a seguir para este análisis es respetar el siguiente orden: de lo general a lo particular, de lo particular al detalle, y del detalle al mínimo detalle (minucia).

2.5 Documentación: Descripción

Consiste en la narración y descripción escrita de todo lo que se encuentra en la escena del crimen o lugar de los hechos. Es recomendable realizar esta descripción de la misma manera que se llevó a cabo la inspección ocular, esto es, de lo general a lo particular, de lo particular al detalle y del detalle al mínimo detalle.

Esta descripción debe contener una enumeración detallada de todos los indicios, ubicación geográfica, características y distribución del escenario, y la ubicación precisa de cada rastro que se encuentre y se relacione con el hecho investigado.

También es posible acompañar este acto de una videofilmación, que brinde mayores detalles y complemente a la descripción realizada.

---

[118] Ibidem.

Se formalizará en un acta, y toda persona que la lea estará en condiciones de formarse una idea clara del lugar y de la ubicación de los elementos encontrados, aunque no haya estado presente en el lugar de los hechos.

2.6 Fotografías forenses. Escalas. Principios de análisis

Se define a la fotografía forense como la disciplina que tiene por objeto la documentación gráfica de las condiciones en las que se encuentra el lugar de los hechos o de todos los indicios localizados en él[119].

Los objetivos principales de la utilización de esta disciplina son:

- Coadyuvar a la correcta conservación de la evidencia.
- Complementar las descripciones escritas.
- Constituir un elemento de prueba para el juicio.
- Reconstruir la escena del crimen todas las veces que sea necesario.

La fotografía forense constituye un punto de apoyo, y muy importante, para la descripción escrita. Es un complemento ideal y es el medio gráfico más importante con que se cuenta para fijar con precisión y detalle el lugar de los hechos o el escenario sujeto a la investigación.

En toda investigación criminal deberá obtenerse todas las fotografías necesarias que puedan resultar útiles para describir el escenario del suceso, de tal manera que todas aquellas personas que no estuvieron presentes sean capaces de percibir con detalle toda la información del lugar y sus indicios, y estar en condiciones de hacer sus apreciaciones sobre las características del caso en concreto. Es también

[119] Montiel Sosa, J. (2011) Criminalística *I*. 2° edición. Editorial Limusa.

recomendable la utilización de soporte fílmico que acompañe a las fotografías obtenidas en el lugar.

Lo aconsejable es que los peritos fotógrafos intervengan antes de que los indicios y rastros sean tocados con el fin de plasmar en gráficos la situación primitiva del lugar y todas aquellas evidencias materiales relacionadas con el caso sujeto a investigación.

La fotografía actuará como un elemento auxiliar necesario, en la faz inicial de la investigación y posteriores medidas técnicas a aplicar, a modo de ratificación de los datos vertidos en los croquis que se realicen y en las actas de inspección ocular.

La fotografía abarca:

a) Los puntos referenciales a efectos de permitir situar objetos, cadáveres y vehículos entre otros, en el lugar del hecho o escena del crimen, cuando sea de visión total o de conjunto.
b) Específicamente, aquello que es necesario resaltar, para lo cual la toma se deba efectuar con aproximación, circunscribiéndose al detalle mínimo, cuando sea visión de detalles. En estos casos siempre se debe anexar un testigo métrico o un elemento de referencia.

El fotógrafo debe considerar las siguientes premisas[120]:

a) El procedimiento debe ajustarse a la metodología de lo general a lo particular, de lo particular al detalle y del detalle al mínimo detalle.
b) La vista general se debe enfocar desde los cuatro ángulos del lugar a fin de tener una visión de conjunto de los aspectos generales del mismo lo que ayuda a la

[120] MPBA; Manual de Procedimiento para la preservación del lugar del hecho y la escena del crimen. Op. Cit.

exactitud en la descripción y ubicación de los elementos, rastros y/o indicios.

c) La vista media debe tener directa relación con objetos, elementos, rastros y/o indicios a efectos de abarcar específicamente el punto que es necesario resaltar, tomando siempre un elemento de referencia.
d) La vista de detalle deben ser tomas de aproximación que se realizan con referencias métricas. Cuando fuere posible, se deben utilizar *lentes* de macro y micro fotografía.
e) Se debe tomar registro fotográfico de todas las áreas que se consideren de relevancia, sin descalificar a priori ninguna de ellas.
f) Las fotografías deben tomarse en forma relacionada.
g) Se deben tomar fotografías desde perspectivas adicionales.
h) La información fotográfica debe completarse señalando fecha, lugar y persona que tomó las fotografías, clase de cámara utilizada, distancia de la cámara respecto de los objetos fotografiados, película utilizada y ángulo desde el cual se efectuaron las tomas y tipo de objetivo utilizado.
i) Los negativos o archivos originales deben preservarse aun cuando no se haya obtenido la calidad fotográfica deseada.
j) Se debe contar con dos testigos cuando se utilicen fotografías tomadas con luz especial para levantar rastros o indicios que por sus características así lo requieran, con el fin de que los mismos constaten dicho procedimiento.

2.7 La informática forense en el lugar del hecho

La aparición de nuevas tecnologías en los lugares del hecho ha motivado a los equipos de técnicos o peritos que participan en la recolección, a contar con una necesaria formación y capacitación para la adecuada preservación y levantamiento de la evidencia digital.

De esta forma, quienes participen en un lugar del hecho o escena de crimen producto de una habilitación judicial (como ocurre con los allanamientos, secuestros u órdenes de presentación), o por solicitud o autorización de una persona o entidad (sea la víctima o un tercero), o por un procedimiento policial urgente en la escena del crimen, deberán tener en cuenta distintas pautas elaboradas especialmente para la adecuada recolección de la evidencia digital.

La recolección debe realizarse de un modo tal que asegure la utilidad procesal de los artefactos recogidos, en sus distintos aspectos. Los principios de relevancia, suficiencia, confiabilidad y validez legal deben ser plenamente observados. En particular, el principio de confiabilidad exige garantizar la identidad e integridad de la evidencia. Eventualmente y a esos fines, será necesaria la inspección y recolección de otros objetos vinculados con los dispositivos.

Deberán atenderse en especial si existen equipos a los que deba realizarse una adquisición *in situ* de la evidencia digital, así como las cuestiones relativas al aseguramiento de la evidencia como acontece con los dispositivos móviles, procurando evitar cualquier circunstancia de destrucción que pudiera darse.

Cuestiones relativas a la inspección de la escena y de los dispositivos, de aseguramiento de las evidencias según su tipo, la forma en que deben levantarse los equipos contenedores de la evidencia digital, las recomendaciones para su clasificación, embalaje, rotulado y transporte, son consideradas especialmente en la *Guía Integral de empleo de la Informática Forense en el Proceso Penal*[121] (Fase de Recolección), cuya lectura es sugerida para un correcto abordaje del tema.

[121] Di Iorio, Ana H. y otros. (2016) Guía integral de empleo de la informática forense en el proceso penal. Op. Cit.

2.8 Recolección de la evidencia. Cadena de custodia.

La cadena de custodia está definida como el *"registro cronológico y minucioso de la manipulación adecuada de los elementos, rastros e indicios hallados en el lugar del hecho, durante todo el proceso judicial"*[122].

La cadena de custodia es una secuencia o serie de recaudos destinados a asegurar el origen, identidad e integridad de la evidencia, evitando que ésta se pierda, destruya o altere. Se aplica a todo acto de aseguramiento, identificación, obtención, traslado, almacenamiento, entrega, recepción, exhibición y análisis de la evidencia, preservando su fuerza probatoria. Permite, además, hacer transparente todo eventual cambio o alteración del material probatorio.

En otras palabras, si el proceso de la cadena de custodia no ha presentado alteraciones ni variaciones de ningún tipo durante su traslado y análisis, se dice que permite garantizar la autenticidad de la evidencia que se utilizará como prueba dentro del proceso judicial.

En la cadena de custodia intervienen todos aquellos empleados y/o funcionarios que participen durante las diferentes etapas del proceso judicial. Este proceso se inicia desde la obtención de la evidencia y finaliza cuando se dispone judicialmente sobre la misma.

Constituye el conjunto de procedimientos formales realizados dentro del proceso judicial respecto de un indicio.

---

[122] Torales, E.E. (2014) Manual de procedimiento para la preservación del lugar del hecho y la escena del crimen. Editorial Ministerio de Justicia y Derechos Humanos de la Nación. Disponible en: http://www.saij.gob.ar/manual-procedimiento-para-preservacion-lugar-hecho-escena-crimen-programa-nacional-criminalistica-autor-eloy-emiliano-torales-colaboradores-marcelino-cottier-jorge-norberto-delgado-ignacio-lombardi-ministerio-justicia-derechos-humanos-nacion-lb000061-2014-07/123456789-0abc-defg-g16-0000blsorbil

Al momento de la recolección de la evidencia se deberá describir cada uno de sus elementos de manera detallada e idéntica a la que conste en el Acta.

La recolección de indicios dependerá de la capacidad, destreza y conocimientos técnicos del perito encargado de extraer o levantar los indicios. La tarea pericial estará avalada por el acta descriptiva y de detalle de todos los indicios "levantados".

Deberá prestarse especial atención en el embalaje y el rotulado de los indicios obtenidos en la escena del crimen. Los mismos deberán ser de características tales que impidan la modificación, alteración, contaminación o destrucción.

Es imprescindible el conocimiento de los protocolos existentes en la materia por parte de los funcionarios y personas que se pongan en contacto con la evidencia de un hecho presuntamente delictivo, y que serán los responsables de velar por su aseguramiento, conservación y registro. En el ámbito de la Provincia de Buenos Aires, deberá considerarse lo previsto por el *Protocolo de Cadena de Custodia*[123] aprobado por Resolución General Nº 889/15 de la Procuración General, a fin de integrar sus disposiciones en todo cuanto sea compatible con la Guía de empleo de la Informática Forense en el Proceso Penal.

En estricta referencia a la prueba informática[124], para que pueda considerarse válida y tenga fuerza probatoria, será necesario que la misma sea garantizada respecto de su confiabilidad.

[123] Procuración General de la Suprema Corte de Justicia de la Provincia de Buenos Aires. Protocolo de Cadena de Custodia. Res. 889/15. Disponible en: http://www.mpba.gov.ar/web/Resoluciones/889-15.pdf Accesible: julio 2016.

[124] Véase en el Capítulo 4, Prueba Científica y Prueba Informática.

Es como consecuencia de las características particulares que presenta este tipo de evidencia (digital), que deberán seguirse algunos recaudos extras:

- Consultar con anterioridad a la recolección (siempre que sea posible) a un forense informático y/o Especialista en Recolección.
- Estar en conocimiento que, para cada tipo de medio digital, la preservación de la prueba será distinta, y habrá que tener en cuenta la volatilidad de los datos que almacenan.
- Impedir la manipulación de los equipos por personas que no estén capacitadas para hacerlo.
- Realizar una planilla de cadena de custodia por cada equipo secuestrado.
- Fotografiar todo lo que se encuentre, y describirlo lo más detalladamente posible.

Por otra parte, será necesario tener en cuenta todos los procedimientos de cadena de custodia previstos por la institución. Además, si hubiere copias forenses, éstas deben seguir el mismo curso que el original en cuanto a su conservación y preservación, siendo igual de relevante la realización de la cadena de custodia.

En definitiva, lo importante será aplicar los métodos correctos de acuerdo al tipo de evidencia a recolectar respetando los protocolos de levantamiento respectivos.

Será responsabilidad de todo funcionario /empleado que participe en el proceso de cadena de custodia, conocer, cumplir y ejecutar los procedimientos generales y específicos establecidos para tal fin durante el desarrollo de dicho proceso penal.

En conclusión, el proceso de cadena de custodia se basa en los principios probatorios de *protección del indicio*,

buscando que el mismo no sufra alteraciones; *legitimidad,* respetando las normas legales; *veracidad*, libre de vicios de nulidad y *de la necesidad de que los hechos sobre los cuales se basa la acusación y sentencia se encuentren acreditados.*

3. Los desafíos de la investigación de los delitos informáticos. Las dificultades probatorias en los delitos transnacionales

En el curso de una investigación penal pueden presentarse situaciones en donde la información se encuentre ubicada en el exterior, es decir, fuera de la República Argentina, planteándose en ese momento distintas dificultades que permite representan desafíos para los investigadores.

Existen convenios bilaterales y tratados de asistencia recíproca entre algunos países en lo que respecta a medidas de investigación y de prueba. El instrumento internacional más abarcativo de estas cuestiones es la Convención de Cibercriminalidad de la Unión Europea (Budapest, 2001)[125], a la que Argentina ha manifestado su intención de adherir[126] pero aún no la ha ratificado formalmente en el Congreso Nacional. No obstante, ha ido adaptando su legislación de fondo de acuerdo al texto de ese Convenio, quedando aún pendiente la adecuación de las normas procesales, cuestión que por otra parte debe ser definida por cada una de las provincias, por el territorio federal y por la Ciudad Autónoma de Buenos Aires.

[125] Convención de Cibercriminalidad de Budapest. 2001. Accesible: junio de 2016. Disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c

[126] Cfr. Resolución Conjunta 866/2011 y 1500/2011 de la Jefatura de Gabinete de Ministros y el Ministerio de Justicia y Derechos Humanos de la Nación. Versión online disponible en: http://www.informaticalegal.com.ar/2011/10/05/resolucion-conjunta-8662011-y-15002011-jefatura-de-gabinete-de-ministros-y-ministerio-de-justicia-y-derechos-humanos-comision-tecnica-asesora-de-cibercrimen/

No obstante ello, la Convención de Budapest puede ser tomada como punto de referencia para adoptar criterio en diversas problemáticas procesales y para optimizar lo relativo a la gestión de diligencias investigativas y/o probatorias.

Hay asimismo normas de cooperación entre autoridades policiales, y a ello debe añadirse la relación que cada Estado establece con los distintos ISP. Por ejemplo, con determinadas empresas globales (como Facebook, Twitter, Microsoft Corporation, Google y Apple) existen diversas guías procedimentales que los investigadores deben seguir -al pie de la letra- en miras a lograr el objetivo de conseguir la información de un usuario determinado.

Este aspecto resulta relevante ya que no siempre estas entidades tienen representación en el país -lo que no las convierte en multinacionales a las que se les pueda hacer cumplir una orden judicial argentina- siendo, por tanto, el Estado quien debe ajustarse a los cánones por ellas establecidos. E incluso ciertas compañías, aun teniendo una oficina en la República Argentina, se amparan en que su existencia sólo es empleada a los efectos comerciales, por lo cual al encontrarse la información requerida judicialmente en servidores extranjeros las peticiones que se cursen deben ajustarse a las exigencias legales del País en donde éstos se encuentren.

Otra cuestión que debe tenerse en cuenta a la hora de realizar un pedido transfronterizo es el grado de afectación de derechos fundamentales que implique cada medida (por ej.: privacidad), visto desde la perspectiva de cada Estado y/o ISP. Suelen ser éstos últimos quienes determinan en general la vía a seguir para acceder a la información que servirá de prueba necesaria en una investigación. Ello implica distintos lapsos de demora, que deben ser contemplados teniendo en cuenta el grado de relevancia y urgencia que reviste la medida en el plan de investigación del Fiscal.

En determinados casos, es además necesario coordinar con autoridades extranjeras la realización de procedimientos simultáneos, para asegurar el éxito de las medidas. Superadas estas cuestiones, resta prever el nivel de confiabilidad o valor convictivo que tendrá la prueba recibida de un Estado extranjero o de un ISP con sede en el exterior.

Básicamente estas dificultades suelen darse por el principio de soberanía nacional que subyace en los códigos procesales de cada Estado, y que está muy vinculado al principio de territorialidad de la ley[127], que es el que fija la pauta de actuación de los funcionarios encargados de ejercer la acción penal. Se trata entonces, de repensar el derecho procesal penal en función de los cambios tecnológicos, de la evolución de la sociedad de la información, y de ajustarse a las nuevas necesidades que son requeridas a nivel de la investigación para lograr un efectivo servicio de justicia.

Según informes realizados por empresas internacionales que se especializan en brindar servicios de seguridad informática, la tendencia a nivel mundial apunta a que el cibercrimen gobernará el mundo delictivo en los próximos diez años[128]. Se estima que la mayoría de los delitos va a estar relacionado con la tecnología, lo que no sólo apunta a las modalidades donde la informática es el objetivo del delito sino también donde es utilizada como medio para su comisión, donde, en todos los casos, la tecnología constituye un soporte de la evidencia a conseguir.

Este cambio de paradigma repercute en los investigadores judiciales en general. Debido a la falta de adecuación de normas procesales que definan concretamente la cuestión en análisis, estos se encuentran frente a un

[127] Art. 1° inc. 1 del C.P.: “Este código se aplicará: 1º.- Por delitos cometidos o cuyos efectos deban producirse en el territorio de la Nación Argentina, o en los lugares sometidos a su jurisdicción”

[128] https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

panorama de cierta incertidumbre, en la que impera el ingenio y la creatividad en la recolección de la evidencia que sustenta una investigación penal.

A modo de ejemplo, ante un caso en que se investiga una defraudación por el uso ilícito de una tarjeta de crédito donde los consumos se han realizado en sitios *de comercio electrónico* que en principio no son conocidos en la República Argentina ni se trata de una compañía de relevancia que pueda tener ya protocolos establecidos, se puede consultar los términos y condiciones de dicho sitio y establecer un contacto a través del correo electrónico o formulario que se indique al efecto.

Cada caso que se presenta es diferente, y lo primero a realizarse es un relevamiento por cada uno de los sitios involucrados tanto para conocer cómo funcionan, como también para establecer su sede administrativa y eventualmente el modo indicado para requerir la información de la forma más rápida y eficaz posible, dado que los mecanismos de cooperación judicial internacional podrían tornarse ineficaces si se producen demoras considerables en su tramitación.

Una serie de casos con interrogantes cotidianos y de soluciones alternativas expuestos en un informe realizado por el Dr. Marcos Salt --actual Supervisor Operativo del Comité Consultivo del Programa Nacional contra la Criminalidad Informática[129]-, resultan muy ilustrativos sobre la actualidad de la investigación penal, los que se exponen para mayor comprensión de la realidad que atraviesa la temática[130].

---

[129] Resolución 640 - E/2016 del Ministerio de Justicia y Derechos Humanos. Versión online disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/260000-264999/264577/norma.htm

[130] Salt, Marcos; "Nuevos Desafíos de la evidencia digital. El acceso transfronterizo de datos en los países de América Latina". Versión online, accesible en junio de 2016 y disponible en:

"Supuesto 1: Casos de Acceso directo por parte de las autoridades de un Estado a datos alojados en extraña jurisdicción.

Un juez dicta una orden de allanamiento para registrar y secuestrar en las oficinas de un banco toda la información disponible sobre un sospechoso x (por ejemplo, los movimientos de la cuenta bancaria correspondientes a un determinado período de tiempo). El juez ordena que la medida sea cumplimentada con colaboración de un perito informático o de expertos de una unidad especial de delitos tecnológicos pertenecientes a una fuerza de seguridad. Los peritos encuentran la información buscada, pero advierten al juez que, si bien pueden acceder desde las terminales informáticas de la sede del banco para la cual cuentan con orden de allanamiento legítimamente otorgada, la información está alojada en un servidor que está en un país extranjero o en una provincia diferente (en el caso de un país de organización política federal). Surgen un sinnúmero de interrogantes de difícil solución utilizando la normativa vigente:

- ¿Puede procederse al registro y secuestro de la información sin recurrir a los mecanismos de cooperación internacional que vinculan a ambos países? ¿Supongamos que no existe clave de acceso que deba ser "destrabada" por los investigadores ya que la información es accesible desde la terminal ubicada en el domicilio para el cual el juez libró la orden de allanamiento sin necesidad de nuevos procedimientos informáticos?

- ¿Puede obtenerse la clave mediante técnicas de "ingeniería social" o colocando programas espías especiales introducidos en la computadora del imputado para grabar las contraseñas que luego voy a utilizar para la investigación?

- ¿Si no es posible el secuestro de la información porque entendemos que ello significaría una violación al principio de territorialidad, resulta por lo menos válido proceder al copiado

---

http://delitosinformaticostest.fiscalias.gob.ar/wp-content/uploads/2013/11/Dr.-Marcos-Salt-acceso-transfronterizo.pdf

de la información sin removerlo ni alterarlo ni asegurarlo de manera alguna?

Supuesto 2: Acceso a datos a través de la cooperación del sector privado.

En estos supuestos, los órganos de persecución penal no acceden a la información de manera directa sino a través de empresas del sector privado como por ejemplo, Microsoft, Google, entidades bancarias, etc.

Supongamos, por ejemplo, que en una investigación es necesario acceder a la información contenida en una cuenta web mail (Gmail, Hotmail, Yahoo, etc.) o a los documentos contenidos en un servicio de alojamiento de datos cuyos proveedores de servicios tienen los servidores en el extranjero (por ejemplo, "Dropbox"):

- ¿Es necesario que el pedido sea realizado a través de los mecanismos de cooperación internacional (exhorto internacional) o resulta válido requerir la información a la oficina comercial de la empresa que tiene sede en el país en el que se lleva adelante la investigación?

- ¿Resulta válido obtener la evidencia a través de pedidos directos vía mail a la sede de la empresa donde se encuentra el servidor sin dar ningún tipo de información al país donde esta empresa tiene su sede?

- ¿Supongamos que por razones técnicas ni siquiera es posible conocer en un momento determinado en qué país está alojada la información que cambia de servidor constantemente?

Como el lector podrá apreciar, todos estos interrogantes son de difícil solución con el marco normativo vigente (tanto en lo que se refiere a las normas procesales sobre evidencia como a los principios de la cooperación internacional) que no previó los cambios vertiginosos que se produjeron en la tecnología informática y de las telecomunicaciones."

Frente a estos obstáculos, en los que se advierte una falta de normativa en concreto que regulen los supuestos mencionados, Salt señala -de acuerdo a un relevamiento que

realizó entre distintas dependencias y autoridades locales y extranjeras- algunas de las soluciones que se adoptan en la práctica, las que se mencionan a continuación.

Así, en casos similares a los planteados en el primer supuesto si no es necesario destrabar claves se continuará con la medida copiándose los datos que la orden de allanamiento prevé, sin que se deje constancia alguna en el acta de allanamiento. Prevalece la idea de que, al haberse ingresado a través de una terminal ubicada en el lugar físico alcanzado por la orden de allanamiento, la circunstancia de que la información esté alojada en un servidor en otro lugar es irrelevante. No se consideran casos en los que se viole el principio de territorialidad aplicándose el criterio de "ubicación física de la terminal desde la que se accede a la información"[131]. Apunta a que una única excepción se da en aquellos casos en que debe procederse a quebrar una clave de acceso a esos servicios.

En relación al segundo supuesto -del que como ya se aclaró no existe regulación alguna a nivel local-, las soluciones que se aplican son alternativas viables como las peticiones formuladas a través de los canales de contacto que establecen los distintos sitios de Internet, o bien como es el caso de las guías procedimentales ya mencionadas, que son confeccionadas por las propias compañías extranjeras estableciendo cómo realizar las peticiones legales e inclusive delineando el contenido que podrán informar, en una relación Estado-Sector Privado que excede cualquier normativa tradicional, sea de carácter nacional o internacional.

En ambos casos expuestos por Salt, el acceso transfronterizo de datos se da sin participación alguna de las autoridades del Estado donde se encuentra el servidor en el que los datos están alojados y sin rogatoria internacional

[131] Salt, Marcos; Op. Cit.

alguna en un diálogo directo entre Estado requirente – empresa privada.[132]

Otra de las cuestiones que genera un obstáculo en las investigaciones se da a partir de las peticiones que se realizan a los proveedores de servicios de internet (ISP). Los ISP son quienes brindan servicios de Internet y, por tanto, tienen la posibilidad cierta de brindar información respecto de los usuarios a los que les asigna una conexión a internet, dado que ese dato lo deben mantener -al menos un tiempo- en sus servidores por razones económicas de la empresa. La asignación de una conexión al servicio de Internet implica otorgarle al cliente que lo requirió, una dirección IP a través de un módem que fue conectado a un domicilio físico en particular. Una conexión a Internet, como mínimo, está determinada por una dirección IP pública, un nombre de usuario que realiza la conexión, nombre de la persona u organización asociada al nombre de usuario y un domicilio de instalación del módem o router que realiza dicha conexión a Internet.

Antes de seguir, se debe aclarar que hay dos tipos de direcciones IP y es fundamental que se entiendan sus diferencias y usos:

- Dirección IP pública: Es la que tiene asignada cualquier equipo o dispositivo conectado de forma directa a Internet. Algunos ejemplos son: los servidores que alojan sitios web como Google, los routers o módems que dan a acceso a Internet. Las IP públicas son siempre únicas. No se pueden repetir. Dos equipos con IP de ese tipo pueden conectarse directamente entre sí.
- Dirección IP privada: Se utiliza para identificar equipos o dispositivos dentro de una red doméstica o privada.

[132] Salt, Marcos; Op. Cit.

> Son usadas en redes que no sean la propia Internet (redes dentro de una organización generalmente) y utilicen su mismo protocolo (el mismo "idioma" de comunicación). Las direcciones IP privadas están en cierto modo aisladas de las direcciones IP públicas.

Este enfoque sólo se centrará en las direcciones IP públicas ya que son las que el ISP conoce. Las direcciones IP públicas son únicas para una fecha, hora y huso horario determinado, es decir, sólo un único dispositivo conectado a Internet tiene una dirección IP pública diferente al resto de los demás dispositivos conectados a Internet en todo el mundo para ese momento determinado. Cuando este dispositivo se desconecta de Internet, la dirección IP pública puede ser liberada y usada por otro dispositivo que necesite realizar una conexión a Internet.

Sin embargo, a la hora de requerir al ISP la información relativa al usuario y el lugar físico de su instalación, pueden darse distintas posibilidades[133], como, por ejemplo:

1) El ISP colabora y brinda la información para identificar al cliente que realizó la conexión sospechosa.

2) El ISP no tiene registro de a qué usuario asignó una dirección IP pública en un momento dado por fecha y hora (hh:mm:ss) y zona horaria (imposibilidad de identificación).

3) El ISP no colabora, argumentando que no tiene una obligación legal de guardar la información de tráfico. (Imposibilidad de identificación)

4) El ISP colabora, pero la dirección IP pública corresponde a una conexión Wifi sin contraseña (abierta), y el

[133] Problemática abordada en la presentación “El Cibercrimen y la Seguridad Informática” del Dr. Marcelo Temperini y el AIA Maximiliano Macedo en el marco del Primer Congreso Provincial de Derecho Informático, Informática Jurídica y de Peritos Informáticos de la Pcia. de Buenos Aires, Necochea, Pcia. de Buenos Aires, Mayo de 2016.

router no posee habilitado un registro de las IP privadas asignadas a los distintos dispositivos.

5) La dirección IP pública corresponde a una conexión móvil (conexión 3G o 4G desde un chip), y la empresa telefónica no posee registros de asignación de sus usuarios

6) La dirección IP pública corresponde a un ISP del extranjero, por lo que será necesaria contar con la cooperación internacional y entender la regulación interna de cada país.

De esta lista, sólo en el primer caso podrá darse con un domicilio en concreto que podrá ser allanado en la medida en que sea concedido el pedido por el Juez de Garantías, y en cuanto sea posible establecer alguna vinculación con los autores que serían los responsables del hecho investigado.

En los casos 2 y 4 no queda más nada por hacer y la identificación del usuario será totalmente imposible, lo que muchas veces deviene en un archivo de las actuaciones por imposibilidad de acreditar la materialidad del ilícito denunciado como así también de identificar a un autor en concreto.

La sexta respuesta -que suele darse en ocasiones en algunas investigaciones- deriva en una suerte de peripecia procesal para obtener la información. Aquí caben los mismos interrogantes sobre la transfronterización de los datos alojados en servidores en el exterior.

Finalmente, los casos 3 y 5 son los más conflictivos porque en ellos se detectan algunas falencias, tanto de nivel empresarial como estatal. Por un lado, las prestatarias no realizan inversiones técnicas que permitan conservar la información al menos por un plazo determinado; en otros casos, cuentan con la infraestructura pero existe una falta de voluntad en brindar colaboración a la justicia, y finalmente, el propio Estado no está dándole al poder punitivo una herramienta que permita ejercer presión sobre las empresas,

al no encontrarse regulado el servicio de conservación de los datos de tráfico de internet relativos a las comunicaciones.

En este sentido, bien puede decirse que existe la Ley N° 25.873 dictada en 2003 que modificó la Ley N° 19.758 de Telecomunicaciones, incorporando nuevos artículos al texto y, en consecuencia, estableciendo lo siguiente:

a) los prestadores de telecomunicaciones deberán disponer de los recursos humanos y tecnológicos necesarios para la captación y derivación de las comunicaciones que transmiten, para su observación remota a requerimiento del Poder Judicial o el Ministerio Público de conformidad con la legislación vigente;

b) los costos deberán ser soportados por los prestadores y el servicio deberá estar disponible en todo momento;

c) los prestadores deberán registrar y sistematizar los datos filiatorios y domiciliarios de sus usuarios y clientes y los registros de tráfico de comunicaciones para su consulta sin cargo por parte del Poder Judicial o el Ministerio Público;

d) esa información deberá ser conservada por diez años;

e) el Estado Nacional asume la responsabilidad por los eventuales daños y perjuicios que pudieran derivar para terceros de la observación y utilización de la información obtenida por el mecanismo previsto.

El Decreto 1563 (noviembre de 2004) reglamentó la ley 25873, lo que generó una polémica que finalizó tanto con el dictado del Decreto 357/2005 que suspendió la aplicación del primero, como con la declaración de inconstitucionalidad que resolvió la Justicia en el marco de la causa “CABASE s/ acción de amparo” (del Juzgado Contencioso Administrativo de Capital Federal) y el fallo dictado por la Corte Suprema de Justicia de la Nación en el “caso Halabi”.

En el primero de éstos los jueces intervinientes resolvieron que la obligación impuesta legalmente de prestar al Estado -en forma gratuita- el servicio de escucha, intercepción, derivación de comunicaciones y de contar y solventar la infraestructura necesaria a tal fin, constituyen una inconstitucional intromisión en aspectos vedados (como la privacidad), no pudiéndose habilitar la intromisión y/o registro de datos privados bajo la argumentación de una prevención o posible investigación posterior[134].

En el caso Halabi[135], la Corte Suprema afirmó que la Ley N° 25.873 que modificó la Ley N° 19.758 de Telecomunicaciones, exhibía vaguedad en sus previsiones no resultando claro en qué medida pueden las prestatarias captar el contenido de las comunicaciones sin la debida autorización judicial, así como también que, tal como está redactada la norma, existe el riesgo de que los datos sean utilizados para fines distintos que aquéllos en ella estaban previstos.

Asimismo, señalaron que las comunicaciones a las que se refiere la ley 25.873 -y todo lo que los individuos transmiten por las vías pertinentes- integran la esfera de intimidad personal y se encuentran alcanzadas por las previsiones de los artículos 18 y 19 de la Constitución Nacional, haciendo hincapié en el derecho a la intimidad y la garantía consecuente contra toda "injerencia" o "intromisión" "arbitraria" o "abusiva" en la "vida privada" de los afectados[136].

---

[134] Fallo “CABASE “Cámara Argentina de Bases de Datos y Servicios en línea c/ P.E.N. Ley 25873 Dto. 1563/04 s/ amparo Ley 16.986”, 13-05-2005. Versión online, recuperado en julio de 2016 y disponible en: http://www.hfernandezdelpech.com.ar/FALLO%20CABASE.doc

[135] Fallo “Halabi, Ernesto c/ P.E.N. - ley 25.873 dto. 1563/04 s/ amparo ley 16.986”. H. 270. XLII. CSJN - Versión online, recuperada julio 2016, disponible en: http://www.saij.gob.ar/descarga-archivo?guid=rstuvwfa-llos-comp-uest-o09000006pdf&name=09000006.pdf

[136] Cfr. art. 12 de la Declaración Universal de Derechos Humanos y art. 11, inc. 2°, de la Convención Americana sobre Derechos Humanos tratados,

El máximo Tribunal ha subrayado que

> *"...sólo la ley puede justificar la intromisión en la vida privada de una persona, siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen. Es en este marco constitucional que debe comprenderse, en el orden del proceso penal federal, la utilización del registro de comunicaciones telefónicas a los fines de la investigación penal que requiere ser emitida por un juez competente mediante auto fundado, de manera que el común de los habitantes está sometido a restricciones en esta esfera semejantes a las que existen respecto a la intervención sobre el contenido de las comunicaciones escritas o telefónicas. Esta norma concuerda con el artículo 18 de la ley 19.798 que establece que 'la correspondencia de telecomunicaciones es inviolable. Su interceptación sólo procederá a requerimiento de juez competente'"*

Finalmente agregaron -al igual que los magistrados de los tribunales intervinientes en las instancias anteriores-, que

> *"...es evidente que lo que las normas cuestionadas han establecido no es otra cosa que una restricción que afecta una de las facetas del ámbito de la autonomía individual que constituye el* ***derecho a la intimidad,*** *por cuanto sus previsiones no distinguen ni precisan de modo suficiente las oportunidades ni las situaciones en las que operarán las interceptaciones, toda vez que* ***no especifican el tratamiento del tráfico de información de Internet en cuyo contexto es indiscutible que los datos de navegación anudan a los contenidos.*** *Se añade, a ello, la circunstancia de que las normas tampoco prevén un sistema específico para la protección de las comunicaciones en relación con la acumulación y tratamiento automatizado de los datos personales." (Los resaltados pertenecen a los autores del capítulo).*

---

ambos, con jerarquía constitucional en los términos del art. 75, inc. 22, de la Constitución Nacional y en el ex-art. 1071 bis del Código Civil.

Es de hacer notar que aquello a lo que estos fallos apuntan es al *contenido* de las comunicaciones, que es lo que está protegido a nivel constitucional, y no en sí a los *datos de tráfico*. Debe, por tanto, realizarse una aclaración sobre las diferencias entre ambos conceptos[137]:

1) El almacenamiento y conservación del ***contenido*** de las comunicaciones

2) El almacenamiento y conservación de los ***datos de tráfico*** relativos a estas comunicaciones.

En relación al primer supuesto, está claro que el ***deber de confidencialidad*** es una de las principales obligaciones del transportador de un correo electrónico, quien:

- No puede revelar a terceros el contenido de los correos transmitidos;
- Debe adoptar las medidas técnicas y de seguridad necesarias para que esa confidencialidad no pueda ser violada por terceros;
- El contenido que se ha transmitido no debe ser conservado por el ISP, salvo:
- El almacenamiento automático, transitorio y necesario para llevar a cabo la transmisión;
- Cuando la ley expresamente así lo establezca y por el tiempo y modalidades establecidas en la misma;
- Cuando las partes intervinientes en la transmisión, así lo hayan solicitado;

[137] Fernández Delpech, Horacio; *"Los Datos de Tráfico en la Lucha contra los Delitos Informáticos"* - Trabajo presentado en la 3er Jornada de Derecho y Pericias Informaticas, Buenos Aires, 22.10.2009

Se trata de excepciones al principio de no conservación del almacenamiento de las comunicaciones, que garantiza el derecho constitucional a la privacidad.

Pese a las discusiones doctrinarias que se dan hoy a nivel internacional sobre si los ISP deben conservar los datos de tráfico durante algún lapso de tiempo- existe un consenso en definir a los ***datos de tráfico*** como todos los elementos que hacen a la individualización de partida y llegada, fecha, hora y demás datos de una comunicación, que no impliquen la vulneración y conocimiento del texto contenido en el mensaje.

Se han esgrimido diversos argumentos sobre la conveniencia de esta obligación de conservación de los *datos de tráfico*, entre ellas las cuestiones de seguridad nacional, las vinculadas a la posibilidad de una mejor investigación de los delitos y la de darle mayor fundamento a la prueba del correo electrónico en los regímenes procesales. En este sentido lo están haciendo en la Comunidad Europea, a través de la Directiva 2002/58/CE (relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones), facultando a los Estados a establecer excepciones a las normas de destrucción de datos de tráfico, para proteger la seguridad y la defensa nacional, y autorizándose a los Estados a retener datos de tráfico para prevenir e investigar delitos. A partir de entonces los países europeos están estudiando el dictado de normativas relativas a la retención de los datos de tráfico más allá de la finalidad de la facturación[138].

Esta materia es la que se encuentra pendiente de regulación en Argentina y que seguramente será motivo de debate próximamente, cuando el Poder Ejecutivo dé cuenta de la ineficacia de la justicia en esclarecer los hechos vinculados a la informática, derivadas, entre otras cosas, de la falta de colaboración por parte de las empresas prestatarias

[138] Fernández Delpech, H.; *Op. Cit.*

que no brindan la información o se niegan a hacerlo amparadas en cuestiones técnicas o legales.

4. Medidas probatorias (faz de derecho procesal en la Convención de Cibercriminalidad)

Como se ha mencionado anteriormente una de las carencias de los códigos procedimentales está dada por la falta de regulación de las medidas probatorias, de coerción e incautación que permitan celebrar acuerdos a nivel regional o global, con el objeto de lograr una adecuada cooperación judicial internacional.

Se detallan a continuación los aspectos procesales que contempla la Convención de Cibercriminalidad de Budapest, que es la rectora en la materia.

Conservación rápida de datos almacenados en medios informáticos

Esta medida permite la conservación rápida de determinados datos almacenados por medio de un sistema informático, en particular cuando existan razones para creer que los mismos podrían ser susceptibles de pérdida o de modificación. Podría obligarse a quien los administre a que conserve y proteja la integridad de dichos datos durante el tiempo necesario, hasta un máximo de noventa días -renovables- de manera que las autoridades competentes puedan conseguir su revelación.

Conservación y revelación parcial rápidas de datos sobre el tráfico

La posibilidad de conservar rápidamente los datos de tráfico puede realizarse con independencia de que en la transmisión de esa comunicación participen uno o varios proveedores de servicios.

Así también que la revelación rápida sea efectuada a la autoridad competente de un País -o a una persona designada

por dicha autoridad-, respecto a un volumen suficiente de datos de tráfico para que dicho País pueda identificar a los proveedores de servicio y la vía por la que se transmitió la comunicación.

Orden de presentación

Se encuentra prevista para los siguientes casos:

a) Para obligar a una persona -física o jurídica- que se encuentre en el territorio de un País, que comunique determinados datos informáticos que posea o que se encuentren bajo su control, almacenados en un sistema informático o en un medio de almacenamiento de datos informáticos; y

b) a un proveedor de servicios que ofrezca prestaciones en el territorio de ese País para que comunique los *datos* que posea o que se encuentren bajo su control *relativos a los abonados*[139] en conexión con dichos servicios.

Registro y confiscación de datos informáticos almacenados

Se prevé la posibilidad de registrar o tener acceso de una forma similar:

[139] La Convención definió a los *«datos relativos a los abonados»* como aquella información que, en forma de datos informáticos o de cualquier otra forma, posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido. Deben poder determinar: a) El tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio; b) la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios; c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios.

a) a un sistema informático o a una parte del mismo, así como a los datos informáticos almacenados en el mismo; y
b) a un medio de almacenamiento de datos informáticos en el que puedan almacenarse datos informáticos, en su territorio.

También se contempla que, si las autoridades que están llevando adelante un registro de un sistema informático específico estiman que los datos buscados están almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y dichos datos son lícitamente accesibles a través del sistema inicial o están disponibles para éste, dichas autoridades pueden ampliar rápidamente el registro o la forma de acceso similar al otro sistema.

Se faculta a las autoridades competentes a confiscar o a obtener de una forma similar los datos informáticos o un medio de almacenamiento de datos informáticos a los que se haya tenido acceso; a realizar y conservar una copia de dichos datos informáticos; a preservar la integridad de los datos informáticos almacenados de que se trate; y/o a hacer inaccesibles o suprimir dichos datos informáticos del sistema informático al que se ha tenido acceso.

Se puede ordenar a cualquier persona -física o jurídica- que conozca el funcionamiento del sistema informático a que proteja los datos informáticos contenidos en el mismo y que facilite toda la información necesaria.

Obtención en tiempo real de datos sobre el tráfico

Se prevé que se pueda obtener o grabar en tiempo real datos sobre el **tráfico asociados a comunicaciones específicas** transmitidas en su territorio por medio de un sistema informático mediante la aplicación de medios técnicos existentes en su territorio, o con la ayuda de un proveedor de servicios, dentro de los límites de su capacidad técnica, pudiendo obligarlo a tal fin.

Interceptación de datos sobre el contenido

Se prevé que se pueda obtener o grabar en tiempo real los datos sobre el **contenido** de determinadas comunicaciones en su territorio, transmitidas por medio de un sistema informático mediante la aplicación de medios técnicos existentes en su territorio, o con la ayuda de un proveedor de servicios, dentro de los límites de su capacidad técnica, pudiendo obligarlo a tal fin.

Principios definidos en el Convenio

La Convención de Cibercriminalidad establece, asimismo, los principios generales relativos a la cooperación internacional que permitirían hacer posible las medidas probatorias antes descriptas.

Éstos son:

1. Principios generales relativos a la cooperación internacional

Las Partes que resuelvan ratificar la Convención cooperarán entre sí en la mayor medida posible en la aplicación de los instrumentos internacionales relativos a la cooperación internacional en materia penal, o en acuerdos basados en legislación uniforme o recíproca y de su derecho interno, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos.

2. Principio de Extradición

Entre los Países ratificantes existirá la posibilidad de aplicar la **extradición** por la comisión de cualquiera de los delitos establecidos en el Convenio de Cibercriminalidad y que hayan sido adoptados por éstos, siempre que estén castigados en la legislación de los países implicados con una pena privativa de libertad de una duración máxima de como mínimo un año, o con una pena más grave.

La extradición estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de extradición aplicables, incluidos los motivos por los que el país requerido puede denegar la extradición.

Cuando se deniegue la extradición únicamente por razón de la nacionalidad de la persona buscada o porque el país requerido se considera competente respecto del delito, la Parte requerida deberá someter el asunto -a petición del país requirente- a sus autoridades competentes para los fines de las actuaciones penales pertinentes, e informará a su debido tiempo del resultado final al país requirente.

3. Principios generales relativos a la asistencia mutua

Se ha previsto que los países ratificantes de la Convención se concedan asistencia mutua en la mayor medida posible para los fines de las investigaciones o procedimientos relativos a delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas en formato electrónico de un delito.

En casos de urgencia, cada Parte podrá transmitir solicitudes de asistencia o comunicaciones relacionadas con las mismas por medios rápidos de comunicación, incluidos el fax y el correo electrónico, en la medida en que dichos medios ofrezcan niveles adecuados de seguridad y autenticación (incluido el cifrado, en caso necesario), con confirmación oficial posterior si el país requerido lo exige. El país requerido aceptará la solicitud y dará respuesta a la misma por cualquiera de estos medios rápidos de comunicación.

La asistencia mutua estará sujeta a las condiciones previstas en el derecho interno del país requerido o en los tratados de asistencia mutua aplicables, incluidos los motivos por los que el país requerido puede denegar la cooperación.

4. Principio de Información espontánea

Dentro de los límites de su derecho interno, y sin petición previa, un Estado podrá comunicar a otro Estado

información obtenida en el marco de sus propias investigaciones cuando considere que la revelación de dicha información podría ayudar al Estado receptor a iniciar o llevar a cabo investigaciones o procedimientos en relación con delitos previstos en el Convenio, o si podría dar lugar a una petición de cooperación por parte de dicho Estado.

Antes de comunicar dicha información, el Estado que la comunique podrá solicitar que se preserve su confidencialidad o que se utilice con sujeción a determinadas condiciones. Si el Estado receptor no puede atender esa solicitud, informará de ello al otro Estado, que deberá entonces determinar si a pesar de ello debe facilitarse la información o no. Si el país destinatario acepta la información en las condiciones establecidas, quedará vinculada por las mismas.

5. Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

Se establecen los procedimientos cuando entre los Estados requirentes y requeridos no se encuentre vigente un tratado de asistencia mutua o un acuerdo basado en legislación uniforme o recíproca.

En dichos casos, cada Estado designará una o varias autoridades centrales encargadas de enviar solicitudes de asistencia mutua y de dar respuesta a las mismas, de su ejecución y de su remisión a las autoridades competentes para su ejecución. Las autoridades centrales se comunicarán directamente entre sí.

En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Estado comunicará al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas en cumplimiento del presente apartado.

Las solicitudes de asistencia mutua en estas condiciones se ejecutarán de conformidad con los procedimientos especificados por el Estado requirente, salvo que sean incompatibles con la legislación del Estado requerido.

El Estado requerido podrá denegar la asistencia si:

a) La solicitud se refiere a un delito que el país requerido considera delito político o delito vinculado a un delito político;
b) El país requerido considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

El Estado requerido podrá posponer su actuación en respuesta a una solicitud cuando dicha actuación pudiera causar perjuicios a investigaciones o procedimientos llevados a cabo por sus autoridades.

Antes de denegar o posponer la asistencia, el Estado requerido estudiará, previa consulta cuando proceda con el Estado requirente, si puede atenderse la solicitud parcialmente o con sujeción a las condiciones que considere necesarias.

El Estado requerido informará sin demora al requirente del resultado de la ejecución de una solicitud de asistencia. Deberá motivarse cualquier denegación o aplazamiento de la asistencia solicitada. El Estado requerido informará también al requirente de cualquier motivo que haga imposible la ejecución de la solicitud o que pueda retrasarla de forma significativa.

El Estado requirente podrá solicitar al país requerido que preserve la confidencialidad de la presentación de una solicitud, salvo en la medida necesaria para su ejecución. Si el Estado requerido no puede cumplir esta petición de confidencialidad, lo comunicará inmediatamente al requirente,

que determinará entonces si pese a ello debe procederse a la ejecución de la solicitud.

En casos de **urgencia**, las solicitudes de asistencia mutua o las comunicaciones al respecto podrán ser enviadas directamente por las autoridades judiciales del Estado requirente a las autoridades correspondientes del Estado requerido. En tal caso, se enviará al mismo tiempo copia a la autoridad central del país requerido a través de la autoridad central del país requirente. Cualquier solicitud o comunicación en virtud de este apartado podrá efectuarse a través de la Organización Internacional de Policía Criminal (INTERPOL).

Si la autoridad no es competente para tramitarla, remitirá la solicitud a la autoridad nacional competente e informará directamente al Estado requirente de dicha remisión.

Las solicitudes y comunicaciones efectuadas en este carácter que no impliquen medidas coercitivas podrán ser remitidas directamente por las autoridades competentes del Estado requirente a las autoridades competentes del Estado requerido.

6. Principio de Confidencialidad y restricción de la utilización

En ausencia de un tratado de asistencia mutua o de un acuerdo basado en legislación uniforme o recíproca que esté vigente entre los Estados requirente y requerido, se prevé las siguientes posibilidades:

El Estado requerido podrá supeditar la entrega de información o material en respuesta a una solicitud a la condición de que:

a) Se preserve su confidencialidad cuando la solicitud de asistencia judicial mutua no pueda ser atendida en ausencia de esta condición, o

b) no se utilicen para investigaciones o procedimientos distintos de los indicados en la solicitud.

Si el Estado requirente no puede cumplir alguna de estas condiciones, informará de ello sin demora al otro Estado, que determinará en tal caso si pese a ello debe facilitarse la información. Cuando el Estado requirente acepte la condición, quedará vinculada por ella.

Cualquier Estado que facilite información o material con sujeción a una condición de las mencionadas podrá requerir al otro Estado que explique, en relación con dicha condición, el uso dado a dicha información o material.

7. Asistencia mutua en materia de medidas provisionales. Conservación rápida de datos digitalmente almacenados

Un Estado podrá solicitar a otro que ordene o asegure de otra forma la conservación rápida de datos almacenados por medio de un sistema informático que se encuentre en el territorio de ese otro Estado, respecto de los cuales el Estado requirente tenga la intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso de forma similar, la confiscación o la obtención de forma similar, o la revelación de los datos.

En este tipo de solicitudes de conservación se indicará:

a) La autoridad que solicita dicha conservación;
b) el delito objeto de investigación o de procedimiento penal y un breve resumen de los hechos relacionados con el mismo;
c) los datos informáticos almacenados que deben conservarse y su relación con el delito;
d) cualquier información disponible que permita identificar a la persona encargada de la custodia de los datos informáticos almacenados o la ubicación del sistema informático;
e) la necesidad de la conservación; y
f) que el Estado tiene la intención de presentar una solicitud de asistencia mutua para el registro o el

acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de los datos informáticos almacenados.

Tras recibir la solicitud de otro Estado, el país requerido tomará las medidas adecuadas para conservar rápidamente los datos especificados de conformidad con su derecho interno. A los efectos de responder a una solicitud, **no se requerirá la doble tipificación penal como condición para proceder a la conservación.**

Cuando una Parte exija la doble tipificación penal como condición para atender una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de datos almacenados, -en delitos distintos a los que tipifica la Convención- dicho Estado podrá reservarse el derecho a denegar la solicitud de conservación en los casos en que tenga motivos para creer que la condición de la doble tipificación penal no podrá cumplirse en el momento de la revelación.

Asimismo, las solicitudes de conservación únicamente podrán denegarse si:

a) La solicitud hace referencia a un delito que el Estado requerido considera delito político o delito relacionado con un delito político;
b) el Estado requerido considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

Cuando el Estado requerido considere que la conservación por sí sola no bastará para garantizar la futura disponibilidad de los datos o pondrá en peligro la confidencialidad de la investigación del Estado requirente o causará cualquier otro perjuicio a la misma, informará de ello sin demora al país requirente, el cual decidirá entonces si debe pese a ello procederse a la ejecución de la solicitud.

Las medidas de conservación adoptadas en respuesta a estas solicitudes tendrán una **duración mínima de sesenta días**, con objeto de permitir al Estado requirente presentar una solicitud de registro o de acceso de forma similar, confiscación u obtención de forma similar, o de revelación de los datos. Cuando se reciba dicha solicitud, seguirán conservándose los datos hasta que se adopte una decisión sobre la misma.

8. Principio de Revelación rápida de datos conservados sobre el tráfico

Cuando en el supuesto de ejecución de una solicitud de conservación de datos sobre el tráfico -en las condiciones descriptas anteriormente- en relación con una comunicación específica, el Estado requerido descubra que un proveedor de servicios de otro Estado participó en la transmisión de la comunicación, el país requerido revelará rápidamente al Estado requirente un volumen suficiente de datos sobre el tráfico para identificar al proveedor de servicios y la vía por la que se transmitió la comunicación.

La revelación de datos sobre el tráfico únicamente podrá denegarse si:

a) La solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político;
b) la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

9. Principio de asistencia mutua en relación con los poderes de investigación. Asistencia mutua en relación con el acceso a datos informáticos almacenados

Un Estado podrá solicitar a otro Estado que registre o acceda de forma similar, confisque u obtenga de forma similar y revele datos almacenados por medio de un sistema

informático situado en el territorio del Estado requerido, incluidos los datos informáticos conservados en forma rápida.

El Estado requerido dará respuesta a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación previstos para casos de cooperación internacional y de otras disposiciones aplicables.

Se dará respuesta lo antes posible a la solicitud cuando:

a) Existan motivos para creer que los datos pertinentes están especialmente expuestos al riesgo de pérdida o modificación; o
b) los instrumentos, acuerdos o legislación que se encuentren vigentes entre los Estados prevean la cooperación rápida.

10. Principio de acceso transfronterizo a datos almacenados, con consentimiento o cuando estén a disposición del público

Lo prevé el artículo 32 de la Convención, y establece que un Estado podrá, sin la autorización de otro Estado:

a) Tener acceso a datos informáticos almacenados que se encuentren a disposición del público (fuente abierta), con independencia de la ubicación geográfica de dichos datos; o
b) tener acceso o recibir, a través de un sistema informático situado en su territorio, datos informáticos almacenados situados en otro Estado, si el Estado obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos al Estado por medio de ese sistema informático.

11. Principio de asistencia mutua para la obtención en tiempo real de datos sobre el tráfico

Los Estados se prestarán asistencia mutua para la obtención *en* tiempo real de datos sobre el tráfico asociados a comunicaciones específicas en su territorio transmitidas por

medio de un sistema informático. Dicha asistencia se regirá por las condiciones y procedimientos establecidos en el derecho interno.

Cada Estado prestará dicha asistencia como mínimo respecto de los delitos por los que se podría conseguir la obtención en tiempo real de datos sobre el tráfico en un caso similar en su país.

12. Principio de asistencia mutua relativa a la interceptación de datos sobre el contenido

Los Estados se prestarán asistencia mutua para la obtención o grabación en tiempo real de datos sobre el contenido de comunicaciones específicas transmitidas por medio de un sistema informático en la medida en que lo permitan sus tratados y el derecho interno aplicables.

13. Red 24/7

Cada Estado designará un punto de contacto disponible las veinticuatro horas del día, siete días a la semana, con objeto de garantizar la prestación de ayuda inmediata para los fines de las investigaciones o procedimientos relacionados con delitos vinculados a sistemas y datos informáticos, o para la obtención de pruebas electrónicas de un delito. Dicha asistencia incluirá los actos tendentes a facilitar las siguientes medidas o su adopción directa, cuando lo permitan la legislación y la práctica internas:

a) El asesoramiento técnico;
b) La conservación rápida de los datos informáticos almacenados y su revelación rápida;
c) La obtención de pruebas, el suministro de información jurídica y la localización de sospechosos.

El punto de contacto de un Estado estará capacitado para mantener comunicaciones con el punto de contacto de otro Estado con carácter urgente.

Si el punto de contacto designado por un Estado no depende de la autoridad o de las autoridades de dicho Estado responsables de la asistencia mutua internacional o de la extradición, el punto de contacto velará por garantizar la coordinación con dicha autoridad o autoridades con carácter urgente.

Cada Estado garantizará la disponibilidad de personal debidamente formado y equipado con objeto de facilitar el funcionamiento de la red.

Reflexión final

La normativa procesal que impone el Convenio de Cibercriminalidad de Budapest resulta de relevancia para su aplicación en el medio local, en pos de garantizar un proceso judicial rápido, eficaz y justo, es decir, aquello que hace al *debido proceso* que regula la Constitución Nacional.

Debe destacarse principalmente la importancia de contar con un **nexo permanente** que establezca relaciones con organismos judiciales y policiales del país y del extranjero, y con proveedores de servicios de internet (ISP). Dicho nexo debería contar con información legal actualizada y con un manejo eficiente de los mecanismos de cooperación con organismos públicos y empresas privadas.

Además, podría centralizar el conocimiento de las particularidades de cada servicio de internet: tipo de servicio, tecnologías utilizadas, subcontratos con otras empresas, convenios con clientes, grado de capacitación del personal técnico asignado a las cuestiones forenses, contratos con los usuarios, sede legal de las empresas, ubicación física de la información almacenada en la nube, etc. Así, operando internamente como mesa de atención para los investigadores judiciales, permitiría agilizar la identificación de evidencia potencialmente útil, la evaluación de su relevancia y confiabilidad, prever los tiempos de demora y los riesgos de pérdida de datos (adoptando los recaudos pertinentes), y

establecer los mecanismos lícitos más rápidos y seguros para la obtención de pruebas.

Por otro lado, resulta por demás interesante la solución adoptada por la Convención de Cibercriminalidad en el artículo 32 sobre el **acceso transfronterizo a datos almacenados, con consentimiento o cuando estén a disposición del público**, al permitir la relación Estado-empresa privada en la solicitud de información aún en los casos en que ésta se encuentre fuera de los límites del Estado requirente, siempre que exista un consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos al Estado por medio de un sistema informático.

De esta manera quedarían superadas algunas barreras a la hora de investigar, sobre todo cuando debe contarse con la colaboración de empresas ubicadas en el exterior del país, que no cuentan con representación legal a nivel local e incluso cuando no se encuentra dentro de sus previsiones brindar un servicio en la República Argentina. Sobre todo apuntando a que los mecanismos tradicionales de búsqueda y obtención de esta información pueden resultar ineficaces -teniendo en cuenta la característica de la volatilidad de los datos-, como así también por no encontrarse previsto en estos medios habituales que dichos datos puedan conseguirse a través de exhortos internacionales, los cuales están pensados exclusivamente en una relación entre Estados, y no con particulares.

Bibliografía

Bertolino, P. J. (2009) Código Procesal Penal de la Provincia de Buenos Aires Comentado y Anotado con jurisprudencia provincial. (9na ed. actualizada). Buenos Aires: Abeledo Perrot.

Código Penal Ley 11.179. República Argentina. Boletín Oficial, 16 de Enero de 1985. Recuperado 01 de julio 2016, de: http://www.saij.gob.ar/documentDisplay.jsp?guid=123456789-0abc-defg-g77-62000scanyel

Council of Europe. (2004). Convention on Cybercrime ETS No185. Budapest, Hungría. 01/07/2004. Recuperado 01 julio 2016, de http://conventions.coe.int/Treaty/en/Treaties/html/185¬SPA.htm

Di Iorio, A. H. y otros (2016) Guía integral de empleo de la informática forense en el proceso penal. 2° ed. revisada, Mar del Plata, Universidad FASTA. Accesible: julio 2016. Disponible en: http://info-lab.org.ar/images/pdf/PAIF.pdf

Falcone, R. & Madina, M. (2005) El Proceso Penal en la Provincia de Buenos Aires. Edit. Ad Hoc.

Fallo "Halabi, Ernesto c/ P.E.N. - ley 25.873 dto. 1563/04 s/ amparo ley 16.986". H. 270. XLII. CSJN - Versión online, recuperada julio 2016 de: http://www.saij.gob.ar/descarga-archivo?guid=rstuvwfa-llos-comp-uest-o09000006pdf&name=09000006.pdf

Fallo CABASE "Cámara Argentina de Bases de Datos y Servicios en línea c/ P.E.N. Ley 25873 Dto. 1563/04 s/ amparo Ley 16.986, 13-05-2005. Versión online, recuperado en julio de 2016 de: http://www.hfernandezdelpech.com.ar/FALLO%20CABASE.doc

Fernández Delpech, H. (2009) Los Datos de Tráfico en la Lucha contra los Delitos Informáticos - Trabajo presentado en la 3er Jornada de Derecho y Pericias Informáticas, Buenos Aires, 22.10.2009

Granillo Fernández, H. & Herbel, G. A. Código de Procedimiento Penal de la Provincia de Buenos Aires. (2° Edición Actualizada y Ampliada). Buenos Aires: La ley.

Gross, H. (1894) Manual del Juez. Est. Tip. Viuda e Hijos de M. Telloi. Madrid, España.

Guzmán, C. A. (2010) El examen en el escenario del crimen. Buenos Aires: Editorial Bdef.

Ley 11.922 Código Procesal Penal de la Provincia de Buenos Aires. Recuperado 01 de julio 2016, de: http://www.biblioteca.jus.gov.ar/codigos.html

Maier, J. (1975) La investigación penal preparatoria del Ministerio Público. Buenos Aires: Ed. Lerner.

Maier, J. (2013). Derecho Procesal Penal. Buenos Aires: Editores del Puerto.

Montiel Sosa, J. (2011) Criminalística I. (2° edición) Editorial Limusa.

MPBA. Criminalística. Accesible: 01 de julio 2016 de: http://www.mpba.gov.ar/web/contenido/curso%20ayudantes%20fiscales%20la%20plata%202011.pdf

MPBA; Manual de procedimiento para la preservación del lugar del hecho y la escena del crimen. Accesible: junio 2016. Disponible en: http://www.mpba.gov.ar/web/contenido/Lugar%20del%20hecho.pdf

Procuración General de la Suprema Corte de Justicia de la Provincia de Buenos Aires. Protocolo de Cadena de Custodia. Res. 889/15. Disponible en: http://www.mpba.gov.ar/web/Resoluciones/889-15.pdf Accesible: julio 2016.

Protocolo de Actuación para la Preservación de la Escena del Hecho y sus pruebas. Programa Nacional de Capacitación de la Secretaría de Seguridad, del Ministerio de Justicia, Seguridad y Derechos Humanos. Tit I, Cap I. P. 4.

Protocolo Federal de Preservación. Accesible: julio 2016. Disponible en: http://www.jus.gob.ar/media/183597/Protocolo%20Federal%20de%20Preservacion.pdf

Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Proceso de Recolección de Pruebas en Ciberdelitos. Disponible en:

http://www.informaticalegal.com.ar/2016/06/07/resolucion-2342016-del-ministerio-de-seguridad-protocolo-general-de-actuacion-para-las-fuerzas-policiales-y-de-seguridad-en-la-investigacion-y-proceso-de-recoleccion-de-pruebas-en-ciberdelitos/

República Argentina, Poder Judicial Cámara Nacional de Apelaciones y Garantias Morón. Sala 2 - causa 14.587, 15/04/2003.

Resolución 640 - E/2016 del Ministerio de Justicia y Derechos Humanos. Versión online disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/260000-264999/264577/norma.htm

Resolución Conjunta 866/2011 y 1500/2011 de la Jefatura de Gabinete de Ministros y el Ministerio de Justicia y Derechos Humanos de la Nación. Versión online disponible en: http://www.informaticalegal.com.ar/2011/10/05/resolucion-conjunta-8662011-y-15002011-jefatura-de-gabinete-de-ministros-y-ministerio-de-justicia-y-derechos-humanos-comision-tecnica-asesora-de-cibercrimen/

Salt, M. (2016). Nuevos Desafíos de la evidencia digital. El acceso transfronterizo de datos en los países de América Latina. Versión online, accesible en junio de 2016 y disponible en: http://delitosinformaticostest.fiscalias.gob.ar/wp-content/uploads/2013/11/Dr.-Marcos-Salt-acceso-transfronterizo.pdf

T.C.P.B.A., sala 1 LP, P 549 RSD-136-1, S 10/4/2001.

Temperini, M. & Macedo, M. (2016) Exposición sobre El Cibercrimen y la Seguridad Informática en el marco del Primer Congreso Provincial de Derecho Informático, Informática Jurídica y de Peritos Informáticos de la Pcia. de Buenos Aires, llevado a cabo en la ciudad de Necochea, Pcia. de Buenos Aires, los días 27 y 28 de mayo de 2016.

Torales, E.E. (2014) Manual de procedimiento para la preservación del lugar del hecho y la escena del crimen.

Editorial Ministerio de Justicia y Derechos Humanos de la Nación. Disponible en: http://www.saij.gob.ar/manual-procedimiento-para-preservacion-lugar-hecho-escena-crimen-programa-nacional-criminalistica-autor-eloy-emiliano-torales-colaboradores-marcelino-cottier-jorge-norberto-delgado-ignacio-lombardi-ministerio-justicia-derechos-humanos-nacion-lb000061-2014-07/123456789-0abc-defg-g16-0000blsorbil

Vázquez Rossi, J. E. (2008) Derecho Procesal Penal. Buenos Aires: Rubinzal Culzoni.

Vélez Mariconde, A. (1986) Derecho Procesal Penal. Buenos Aires: Editorial Astrea

Capítulo 4. La prueba, el rol del perito y la actuación forense

Autor: Sabrina B. Lamperti.

1. La estructura judicial. 1.1. Justicia Federal y Justicia Provincial. 1.2. Estructura judicial: Fuero civil y fuero penal. 1.3 Órganos auxiliares: Policía Científica, Policía Judicial, Institutos de Ciencias Forenses, Asesoría Pericial. 1.3.1 Policía Científica y Policía Judicial. 1.3.2 Asesorías Periciales e Institutos de Ciencias Forenses
2. Prueba. El valor y validez de la prueba. 2.1. La prueba. 2.2. La pericia. 2.3. El perito. Perito de parte y de oficio. Perito oficial. Diferencias. Deberes y obligaciones.
3. Perito Informático. Ley N° 13.016 de Ejercicio Profesional en la Provincia de Buenos Aires. Ética profesional. 3.1 Prueba Científica. Prueba Informática.

1. La prueba, el rol del perito y la estructura judicial

1.1. Justicia Federal y Justicia Provincial

Es importante iniciar el capítulo brindando algunas explicaciones sobre el entorno en el cual se lleva adelante un proceso judicial con el fin de que los informáticos que actúen en estos sepan dónde están interviniendo, en qué tipo de materia (civil, laboral, penal, familia) y cuáles normativas regulan, según ello, el actuar forense.

En primer lugar, se debe establecer una diferencia entre lo que es **justicia federal** y **provincial.**

El Poder Judicial ejerce la función del Estado denominada "administración de justicia", "jurisdicción" o "función jurisdiccional". Es atribución del Poder Judicial el poder *impartir justicia,* y ello puede darse:

- **Entre particulares:** para dirimir litigios entre individuos o entre éstos y el Estado, y
- **Frente a la actuación del resto de los poderes**, como control de los actos del Poder Ejecutivo y Legislativo, que componen la estructura republicana.

La función jurisdiccional del Estado está en manos de los órganos judiciales federal y local (de las provincias). La competencia federal está contenida en el art. 116 de la Constitución Nacional, y es la excepción, mientras que la competencia provincial es la regla. Ello es así por lo que establece, a su vez, el artículo 121 de la Constitución Nacional, que señala:

> *"**Las provincias conservan todo el poder no delegado por esta Constitución al Gobierno Federal**, y el que expresamente se hayan reservado por pactos especiales al tiempo de su incorporación."*

La condición de federal de un país hace que divida el poder territorial en provincias y que a su vez concentre la administración en un gobierno federal, privilegiando de esta forma, la autonomía de las provincias por sobre la esfera de potestades del Gobierno Federal. De allí que la Justicia Federal sea la excepción.

A modo de síntesis esquemática:

- **Justicia Federal**
  - Es una justicia de excepción.
  - Actúa sólo en los casos que prevé el art. 116 de la Constitución Nacional, esto es:
    - Causas que versen sobre puntos regidos por la Constitución, y por las leyes de la Nación.
    - Causas que versen sobre puntos previstos en tratados con las naciones extranjeras.
    - Causas concernientes a embajadores, ministros públicos y cónsules extranjeros
    - Causas de almirantazgo y jurisdicción marítima
    - Asuntos en que la Nación sea parte.
    - Causas que se susciten entre dos o más provincias; entre una provincia y los vecinos de otra; entre los vecinos de diferentes provincias[140]; y entre una provincia o sus vecinos, contra un Estado o ciudadano extranjero
  - Aplica de acuerdo a la materia:
    - Código Procesal Penal de la Nación (CPPN)

[140] Tales causas deben versar sobre cuestiones civiles para encuadrarse en la norma. Si bien este requisito no se encuentra expresado en la C.N. el mismo se halla establecido en la ley 48, art. 2, inc. 2. Es una regla para asegurar la imparcialidad y este caso puede ser prorrogado, es decir que si se inició como caso en la justicia local puede pedirse el cambio a la justicia federal.

    - Código Procesal Civil y Comercial de la Nación (CPCCN)
    - Código Electoral Nacional
  - Cuando hay que recurrir las resoluciones interviene la Corte Suprema de Justicia de la Nación (CSJN) como órgano de Alzada, sin perjuicio de casos enunciados aquí que directamente tramitan ante la Corte, como aquellos en los que una provincia demanda a otra.

- **Justicia Provincial**
  - Es la justicia ordinaria (o local)
  - Es la que resuelve la mayoría de casos que se presentan ante la Justicia en todo aquello donde no interviene la Justicia Federal.
  - Aplica de acuerdo a la **materia** los códigos procesales de cada Provincia, por ejemplo:
    - Código Procesal Penal (CPPBA)
    - Código Procesal Civil (CPCCBA)
  - Cuando se presentan recursos extraordinarios intervienen las Cortes provinciales. Por ej.: SCBA (Suprema Corte de la Provincia de Buenos Aires)

- **Justicia Provincial Bonaerense**
  - De acuerdo a la **materia** de que se trate será el Código a aplicar.
  - Materias de derecho **civil y comercial** y de **familia**:
    - Código Civil y Comercial (Ley de fondo)
    - Código Procesal Civil y Comercial (Ley de forma)
  - Materia de derecho **laboral:**
    - Ley de Contrato de Trabajo (Ley de fondo)
    - Código Procesal Civil y Comercial (Ley de forma)
  - Materia de derecho **administrativo:**

- Normativas de competencia administrativa. (Ley de fondo)
- Ley de Procedimiento Administrativo (Ley de forma)

- Materia de derecho **penal:**
  - Código Penal (Ley de fondo)
  - Ley del Régimen Penal Juvenil (Ley de fondo)
  - Código Procesal Penal (Ley de forma)

Existen ***normas de fondo*** (leyes que regulan cada materia) y ***normas procesales (o de forma)*** que establecen los procedimientos legales para la obtención de las pruebas que se considerarán válidas en una investigación, entre otras cuestiones procedimentales que se regulan-. Existen, por tanto, tantos códigos procesales como provincias, y cada materia (civil, penal, etc.) tiene, a su vez, un código de fondo que legisla sobre cada una de ellas.

En particular, teniendo en cuenta la finalidad de este libro, se hará hincapié en los Códigos Procesales Civil y Penal de la Provincia de Buenos Aires.

1.2 Estructura judicial: Fuero civil y fuero penal

La **justicia civil** es la encargada de darle curso a las cuestiones vinculadas a las relaciones entre particulares. Juzga sobre los derechos y obligaciones que están en juego en un conflicto, que puede ser relativo a las posesiones y/o titularidades de bienes, sucesiones, ejecuciones de deudas, peticiones en torno a los nombres de las personas, cambios de identidad de género, así como la resolución de conflictos de familia.

Por su parte, la justicia laboral es la encargada de resolver los problemas de trabajo entre empleador y dependiente; mientras que la Justicia contencioso-administrativa es quien resolverá los conflictos que se den entre los particulares y el Estado.

En estos procesos intervienen las partes que se conocen como **actora** y **demandada**, quienes deben contar con un patrocinio o poder de un letrado para poder actuar judicialmente, y así accionar su petición o bien hacer defensa frente a lo que les es demandado.

Las acciones que se promueven ante los fueros civiles, familiares o laborales se conocen como **demandas**, y son presentadas ante los Juzgados Civiles y Comerciales, los Juzgados de Familia, los Tribunales Laborales o los Contencioso-Administrativos, según sea el tipo de conflicto a resolver.

De existir una resolución o sentencia que alguna de las partes considere en su contra y desee apelar -siempre que se den las circunstancias que la ley regula en cada supuesto- se recurre a un órgano superior, o Alzada, que en estos casos está dado por las Cámaras de Apelaciones, que pueden ser Civil y Comercial o Cámara Contencioso-Administrativo, de acuerdo al caso.

Nuevamente, las resoluciones o sentencias que dictan estas Cámaras pueden ser recurridas -siempre que se den los supuestos contemplados por cada código procesal- ante una instancia superior, que en este caso es el órgano máximo del Poder Judicial de cada provincia, y que en la provincia de Buenos Aires se conoce como Suprema Corte de Justicia de la Provincia de Buenos Aires (S.C.B.A.).

En este esquema, los peritos ocupan un rol de auxiliar de la justicia, ya que ayudan a las partes y a los juzgadores a resolver los conflictos que se plantean.

El cuadro siguiente procura esclarecer lo explicado:

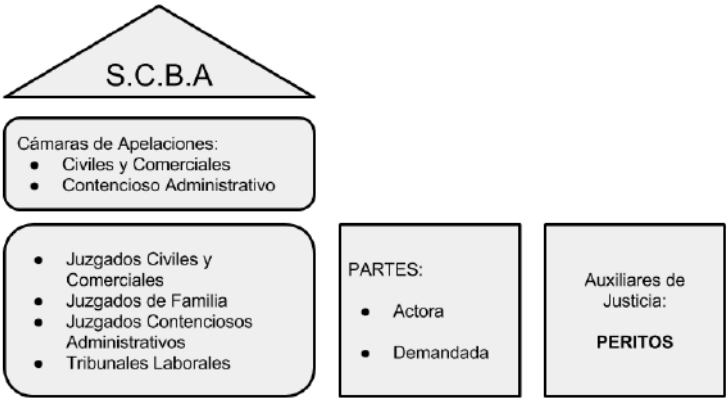


Figura 4.1: Estructura Judicial. Fueros Civil y Comercial, Laboral, Familia y Contencioso-administrativo.

Por otra parte, existe la **justicia penal** que procura dar respuesta a los conflictos originados a partir de la comisión de un ilícito que lleva a cabo una persona en perjuicio de otra, pudiendo ser esta última física o jurídica.

Los procesos penales tienen una estructura diferente a la antes señalada. Como es el Estado quien expropia el conflicto a la víctima para accionar en contra de un individuo o un grupo de éstos, el rol de la acusación lo asume el **Fiscal,** quien lleva adelante lo que se conoce como **acción penal** y que es originado a partir de una **denuncia**.

Sin embargo, y más allá de la actuación del fiscal -que es obligatoria- las víctimas pueden participar en el proceso a través del rol de **particular damnificado**, que debe ser asumido a través de un abogado matriculado.

Otra de las partes del proceso penal es la del **acusado** (o imputado) quien debe poder contar con una representación que articule su **defensa**, pudiendo ser ésta privada a través de un abogado particular, o bien provista por el Estado, dándole así paso a la **Defensa Oficial.**

La investigación de la denuncia se encuentra a cargo del Fiscal, que forma parte del Ministerio Público Fiscal, y que es quien lleva adelante este proceso con el control de los Jueces de Garantías quienes son los responsables del resguardo de garantías constitucionales.

Cuando la etapa de investigación se cierra con una requisitoria de elevación a juicio, porque se hallaron elementos que permiten acreditar tanto la materialidad del ilícito como su autoría, y el Juez de Garantías interviniente considera que a ésta debe hacerse lugar, la causa penal pasa a tramitar ante un Juzgado Correccional o un Tribunal Oral en lo Criminal, dependiendo esto de la escala penal aplicable (menor o mayor a 6 años de prisión).

En general, y siempre que se den los requisitos que contemplan los códigos procesales penales, las resoluciones que dictan cualquiera de estos organismos pueden ser apeladas ante la Cámara de Apelaciones y Garantías en lo Penal y las de éstas, a su vez, ante el Tribunal de Casación Penal. En tanto, también las sentencias definitivas de los Juzgados Correccionales y Tribunales Criminales pueden recurrirse y en ese caso tramitan ante el Tribunal de Casación Penal. El último escalafón judicial al que puede llegarse por vía de los recursos es ante la **Suprema Corte de Justicia de la Provincia de Buenos Aires (S.C.B.A.)** en los supuestos y con las condiciones que marca la normativa procesal vigente.

Por otra parte, la Procuración General de Justicia de la Provincia de Buenos Aires es la autoridad máxima del Ministerio Público, que componen tanto las Fiscalías, como las Defensorías y las Asesorías de Incapaces. El Ministerio Público Fiscal representado por los Fiscales posee un órgano superior que es la Fiscalía General; en tanto el Ministerio Público de la Defensa compuesto por las Defensorías Oficiales, tiene como superior jerárquico a la Defensoría General.

A continuación, un cuadro ilustrativo de lo expuesto.

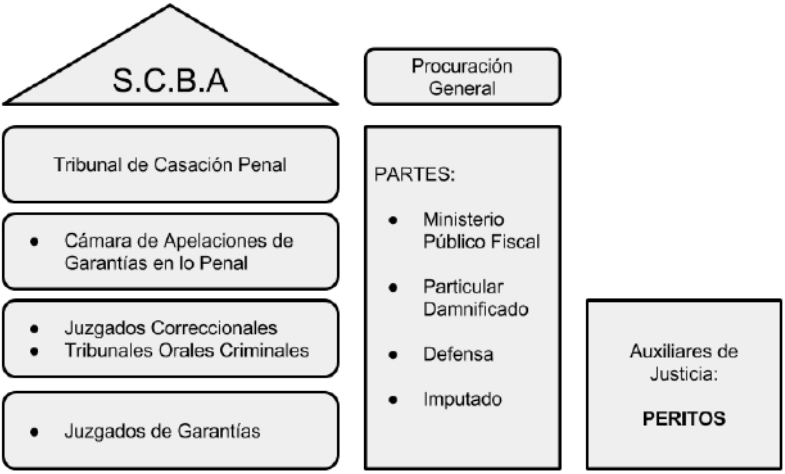


Figura 4.2: Estructura Judicial. Fuero Penal.

1.3 Órganos auxiliares: Policía Científica, Policía Judicial, Institutos de Ciencias Forenses, Asesoría Pericial

Varios son los órganos que auxilian a la Justicia en los procesos que llevan adelante y en las que se requiere de la intervención de profesionales técnicos o con alguna experticia en particular para coadyuvar en la toma de decisiones por parte de los funcionarios intervinientes, dándole -de esta forma- a sus resoluciones un fundamento técnico-científico que en definitiva se traduce en un aporte a la mejora del sistema de administración de justicia.

En tal sentido, existen órganos auxiliares dependientes de distintos estamentos del Estado que colaboran con los procesos judiciales según sea su carácter de la intervención. Así, mientras en los procesos civiles, de familia o laborales se resuelven litigios que las partes establecen como controvertidos, serán los órganos dependientes del Poder Judicial las que intervengan (por ejemplo, las Asesorías Periciales).

En cambio, en los conflictos penales a raíz de la intervención de las fuerzas de seguridad en la determinación de los hechos en los que toman conocimiento, también existirán órganos auxiliares dependientes de éstas que podrán aportar un auxilio en la función judicial, como ocurre con las Policías Científicas.

En los últimos años ha tomado auge la creación de las Policías Judiciales, dependientes de los órganos encargados de promover la persecución penal, que son los Ministerios Públicos Fiscales provinciales y el de la Ciudad Autónoma de Buenos Aires, con el objeto de lograr una efectiva división de las funciones de los poderes del Estado.

Ello tiene sustento directo en el cambio de paradigma del sistema que rige el proceso penal (de inquisitivo a acusatorio) donde ahora cobra protagonismo el Ministerio Público Fiscal, y en donde los magistrados que antes intervenían como jueces de instrucción asumen un rol diferente, de control de la investigación en procura del resguardo de garantías constitucionales. Esto se basa en el nuevo enfoque que apunta a que quien investigue no sea quien también juzgue, haciéndose hincapié en que dichas funciones deben estar divididas en un Estado de Derecho.

Siguiendo la evolución natural de los procesos de cambio, se estima conveniente que quienes tienen el rol de investigar también sean quienes asuman el desafío de la búsqueda, recopilación, análisis y estudio de elementos de evidencia o prueba así como la asistencia técnica y científica para la investigación, pues la delegación absoluta de la actividad investigativa en la policía de seguridad traería como correlato el deterioro de una atribución propia del Poder Judicial.

De allí que la existencia de la Policía Judicial encuentra su fundamento en el hecho de profesionalizar las investigaciones penales, potenciar la lucha contra el crimen organizado, el narcotráfico y las redes delictivas y dar al

Ministerio Público Fiscal herramientas autónomas para ejercer con plenitud la dirección de la investigación en el marco del esquema acusatorio que establece el Código Procesal Penal.

Se detallarán a continuación, los órganos que actualmente existen y coadyuvan al Poder Judicial en su labor diaria.

1.3.1 Policía Científica y Policía Judicial

La Dirección General de **Policía Científica en Función Judicial**[141] depende del Ministerio de Seguridad de la Provincia de Buenos Aires (es decir, del Poder Ejecutivo) y tiene como misión efectuar todos los estudios técnicos y científicos que le sean requeridos en un proceso judicial, así como desarrollar métodos científicos conducentes a descubrir todas las circunstancias del delito. Está integrada en su totalidad por personal policial con título universitario o técnico en las distintas disciplinas forenses. Realiza pericias e informes técnicos en el ámbito de la Provincia de Buenos Aires. Su desempeño es sobre las áreas de competencia de la Criminalística, la Medicina Legal y la Química Legal, en todo su espectro técnico científico. Su estructura organizativa se compone de 18 delegaciones (una por cada Departamento Judicial) que se encuentran conformadas por áreas de cada una de estas disciplinas.

Uno de los objetivos permanentes que tiene la Dirección de Policía Científica, a través de los mecanismos correspondientes, es incrementar los planteles de profesionales en las especialidades de Criminalística, de Química Legal y, en particular, de Medicina Legal descentralizando el servicio para optimizar la operatividad de

[141] Sitio web del Ministerio de Seguridad de la Provincia de Buenos Aires. Accesible julio de 2016. Dispoinible en: http://www.mseg.gba.gov.ar/migra/Policia%20Cientifica%202/cientifica.html

las delegaciones, y aumentar la calidad pericial. Esto a su vez se realiza mediante:

- Instalación de Subdelegaciones en aquellos lugares donde la distancia no hace posible la inmediatez y celeridad.
- Adquisición de instrumental de última generación.
- Perfeccionamiento de los profesionales que cumplen servicios en esta Dirección con Jornadas de actualización en las distintas materias.

Entre las disciplinas que se ocupa la Policía Científica se encuentran: accidentología vial, balística, cuerpo médico, dibujo de rostro, fotografía, laboratorio químico, levantamiento de rastros, mecánica, morgue policial, necropapiloscopía, odontología legal, patología forense, planimetría y poligráficas.

La Policía Judicial, en cambio, es un órgano auxiliar del Ministerio Público Fiscal de carácter profesional técnico-científico, que colabora con la administración de Justicia en la investigación de los delitos de acción pública. Suele denominarse también Cuerpo de Investigadores Judiciales, y su funcionamiento ya se encuentra implementado en la Provincia de Córdoba[142] y en la Ciudad Autónoma de Buenos Aires[143], encontrándose aún pendiente su implementación en la Provincia de Buenos Aires[144] y en Santa Fe[145].

[142] Sitio web del Ministerio Público Fiscal de Córdoba. Accesible: julio de 2016. Disponible en: http://www.mpfcordoba.gob.ar/policia-judicial/
[143] Sitio web del Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires. Accesible: julio de 2016. Disponible en: http://www.fiscalias.gob.ar/cij-cuerpo-de-investigacion-judicial/
[144] Sitio web de la Procuración General de la Provincia de Buenos Aires. Accesible: julio de 2016. Disponible en: https://www.mpba.gov.ar/web/cij.php
[145] Provincia de Santa Fe. Ley 13.459. Accesible: julio de 2016. Disponible en: https://www.santafe.gov.ar/boletinoficial/recursos/boletines/27-01-2015ley13459-2015.html

La misión de la Policía Judicial es, esencialmente, reunir las evidencias y pruebas útiles para que los Fiscales puedan actuar ante los Jueces reclamando una decisión basada en la verdad, desarrollando su actividad a través de un trabajo multidisciplinario de investigación técnica, científica, criminalística y operativa.

En la ley de la Provincia de Buenos Aires, sancionada y a la espera de su implementación[146], se busca que el Cuerpo de Investigadores Judiciales tenga competencia:

- En todos aquellos casos en los que, debido a la estructura organizativa de los autores que involucra, a las características propias de la comisión del hecho o la complejidad requerida para la investigación, los Agentes Fiscales dispongan su intervención.
- En la investigación de homicidios dolosos o cometidos en ocasión de otro delito doloso.
- En la investigación de ilícitos cometidos por funcionarios públicos y miembros de las fuerzas de seguridad y penitenciarias con motivo o en ocasión de sus funciones.

Sus intervenciones están dirigidas en forma exclusiva al esclarecimiento de los hechos a través de la búsqueda, recolección y análisis de elementos de prueba.

Entre sus funciones se encuentran:

- Prestar la asistencia técnica y científica necesaria para el desarrollo de las investigaciones, como así también para la búsqueda, recopilación análisis y estudio de las pruebas, u otros elementos de convicción que contribuyan al esclarecimiento de los hechos.

[146] Provincia de Buenos Aires. Ley 14.424. Accesible: julio de 2016. Disponible en: http://www.gob.gba.gov.ar/legislacion/legislacion/l-14424.html

- Aportar al desarrollo y perfeccionamiento de tecnologías que permitan mejorar las técnicas de investigación criminal.
- Aportar al estudio del delito como fenómeno social a fin de mejorar su comprensión y garantizar un mejor servicio de justicia.
- Contribuir en la elaboración de los diseños de política criminal que efectúa la Procuración General mediante la generación de insumos estadísticos, casuística y todo otro elemento de interés.
- Elaborar y actualizar protocolos de actuación para la preservación de la escena del delito; conservación de los elementos de prueba; seguridad de las víctimas y para toda otra función atinente a la competencia de este Cuerpo.

En los procesos en que se disponga su intervención, son atribuciones del Cuerpo de Investigadores Judiciales:

- Cuidar que los rastros materiales que hubiere dejado el delito sean conservados y que el estado de las cosas no se modifique hasta que así lo determine el Ministerio Público.
- Realizar en el lugar del hecho toda medida probatoria que no requiera, según lo previsto por el Código Procesal Penal de la Provincia de Buenos Aires, la presencia exclusiva del Fiscal.
- Disponer, en caso necesario, que ninguna de las personas que se hallaren en el lugar del hecho o sus adyacencias, se aparten del sitio mientras se lleven a cabo las diligencias que correspondan, de lo que deberá darse cuenta inmediatamente al Fiscal.
- Requisar a las personas demoradas, previa autorización del Fiscal, quien a su vez la solicitará al Juez de Garantías.

- Hacer constar el estado de las personas, de las cosas de los lugares, mediante inspecciones, planos, fotografías, exámenes técnicos y demás operaciones que se estimen necesarias, si hubiere peligro de que cualquier demora comprometa el éxito de la investigación.
- Requerir instrucciones al Fiscal, respecto de los objetos o instrumentos secuestrados relacionados con el delito, con el objeto de que le indique el modo de conservarlos, el envío a la Oficina de Custodia de Prueba o la remisión al Ministerio Público, según corresponda.
- Tomar declaración a los testigos, a quienes se les hará prestar juramento.
- Informar al presunto imputado y víctima sobre los derechos constitucionales que le asisten y que el Código Procesal Penal reglamenta.
- Requerir el auxilio de las autoridades administrativas y de los particulares.
- Solicitar a los agentes fiscales la asistencia de las policías y fuerzas de seguridad y de investigación, a fin de cumplimentar su tarea. Si hubiere peligro para los agentes judiciales o la de terceros, puede solicitarla en forma directa dando cuenta inmediata al Agente Fiscal. Esta asistencia no podrá significar la delegación de la tarea de investigación, ni la eximición del deber de reserva establecido por el artículo 5 de la Ley que crea el Cuerpo de Investigadores Judiciales[147].

[147] Ley 14.424 - Art. 5º. Principios. En su actuación, organización y objetivos estratégicos, el Cuerpo de Investigadores Judiciales se rige por los siguientes principios:
a) Respeto a los Derechos Humanos y a las Garantías Constitucionales. El Cuerpo de Investigadores Judiciales se rige en su actuación por lo

- Solicitar a los agentes fiscales el cese de la intervención de las policías y fuerzas de seguridad y de investigación cuando lo considere conveniente a los fines de la tarea investigativa.
- Requerir de los poderes públicos y de las personas de existencia ideal o física, la colaboración necesaria para el cumplimiento de sus funciones, pudiendo en caso de demora requerir al Juez o Tribunal, a través del Agente Fiscal, la aplicación de medidas de coerción que las normas prevean.

---

establecido en la Constitución Nacional y de la Provincia de Buenos Aires y los Tratados Internacionales de Derechos Humanos, de acuerdo a lo previsto por el artículo 75 inc. 22 de la Constitución Nacional. También rige su actuación las sentencias, recomendaciones y protocolos que establezcan los Organismos Internacionales de aplicación de dichos Tratados. Y en particular su actuación está reglada por el Código de Conducta para Funcionarios Encargados de Hacer Cumplir la Ley, aprobado por la Asamblea General de las Naciones Unidas en Resolución 34/169 del 17 de diciembre de 1979.

b) No Militarización. El Cuerpo de Investigadores Judiciales es una institución de naturaleza civil, cuyas bases doctrinarias, organizacionales y funcionales no están militarizadas. Este Cuerpo puede establecer relaciones institucionales de cooperación y coordinación con las policías y demás fuerzas de seguridad y de investigación, las que no pueden implicar dependencia funcional ni subordinación operativa.

c) Especialidad. El Cuerpo de Investigadores Judiciales tiene competencia en la búsqueda, recopilación, análisis y estudio de elementos de prueba así como en la asistencia técnica y científica para el desarrollo de las investigaciones.

d) Objetividad. El Cuerpo de Investigadores Judiciales actúa con criterio objetivo, evitando todo tipo de discriminación política, social, económica, religiosa, racial, cultural, ideológica, sexual, de género o de cualquier otra índole. Aporta elementos de convicción a todas las partes de proceso. Se considera falta grave el ocultamiento de elementos de convicción favorables a cualquiera de las partes.

e) Deber de reserva. Los integrantes del Cuerpo de Investigadores Judiciales deben guardar absoluta reserva sobre la evolución y resultado de las investigaciones que se le encomienden, así como de todas las informaciones que a través de ellas obtengan.

Desde el momento en que los integrantes del Cuerpo de Investigadores Judiciales se constituyan en el lugar del hecho pueden impartir directivas a las policías y a las demás fuerzas de seguridad e investigación que se encontrasen en el lugar con el fin de cumplir con su función.

1.3.2 Asesorías Periciales e Institutos de Ciencias Forenses

En la actualidad, el Poder Judicial de la Provincia de Buenos Aires cuenta con esquemas de **Asesorías Periciales Departamentales**, dependientes de la Suprema Corte de Justicia[148]. Éstas son las encargadas de producir los informes técnicos periciales que le sean requeridos judicialmente.

Sus dictámenes constituyen un aporte trascendente del que se nutren los magistrados a la hora de formar sus convicciones para resolver sobre las causas de su competencia y que involucran la defensa y resguardo de derechos fundamentales como la libertad, el patrimonio y el estado e integridad de las personas, cualquiera sea su fuero.

Su labor está dirigida a todos los organismos judiciales de la Administración de Justicia, el Ministerio Público y organismos administrativos de la Suprema Corte de Justicia.

Asimismo, en colaboración, responde a requerimientos de organismos públicos estatales y no estatales, como así también a pedidos que efectúan los servicios de justicia de jurisdicción federal y de otras provincias.

La Dirección General tiene a su cargo 18 Oficinas Periciales Departamentales y 18 Cuerpos Técnicos Auxiliares Departamentales con 6 Subsedes. De ella dependen más de 900 agentes, de los cuales más de 600 son profesionales.

[148] Sitio web de la Asesoría Pericial dependiente de la Suprema Corte de Justicia de la Provincia de Buenos Aires. Disponible en: http://www.scba.gov.ar/pericial/ . Accesible: julio de 2016.

Debe destacarse que en ninguno de ellos existe la especialidad de Peritos Oficiales Informáticos, por lo que este servicio no se encuentra cubierto en la actualidad por las Asesorías Periciales Departamentales.

Por otra parte, en la Provincia de Buenos Aires, y bajo la exclusiva órbita del Ministerio Público Fiscal se crearon los **Institutos de Investigación Criminal y Ciencias Forenses**[149] para dar respuesta a las cuestiones de índole pericial que no se encontraban satisfechas bajo otros esquemas de organización.

El primero de ellos fue el de Lomas de Zamora, y en base a su buena experiencia se decidió reproducir su estructura en otros departamentos judiciales, pero buscando evitar la duplicación de servicios en aras de la eficiencia.

En este sentido, se procuró darle a cada uno de estos institutos una especialización temática: el Instituto Norte (con sede en Junín) tiene como propósito investigativo fundamental la Genética Forense, mientras que el Instituto Centro (con sede San Isidro) se especializa en Toxicología y Delitos contra la Integridad Sexual. El Instituto de Ciencias Forenses Sur (con sede Mar del Plata), de reciente inauguración, se especializa en Medicina Forense, Balística y Análisis de Comunicaciones.

Los distintos esquemas actualmente existentes no contemplan la disciplina de la Informática Forense de forma integral, siendo abordada en ocasiones a través de otras oficinas con especialidades diversas que realizan algún tipo de examen pericial informático, sin cubrir todo el campo que esta nueva disciplina tiene para aportar a los procesos judiciales.

[149] Sitio web del Ministerio Público Fiscal de la Provincia de Buenos Aires. Disponible en: http://www.mpba.gov.ar/web/secpoliticacriminal.php. Accesible: julio de 2016.

Los especialistas en el manejo de la evidencia digital deberían trabajar en conjunto y de forma coordinada, bajo la forma de un Laboratorio Forense Judicial, integrando una Asesoría Pericial Departamental o bien un Instituto de Investigación Criminal y Ciencias Forenses.

2. Prueba. El valor y validez de la prueba

2.1 La Prueba

En términos generales, *prueba* es aquello que confirma o desvirtúa una hipótesis o una afirmación precedente.

La prueba es el medio más confiable para descubrir la verdad y, a la vez, la mayor garantía contra la arbitrariedad de las decisiones judiciales.

Lo que se busca con ella es la reconstrucción conceptual de los hechos que son objeto de investigación por parte del fiscal, logrando que sea comprobable y demostrable. La prueba surge de los indicios o evidencias (rastros o huellas) que los hechos pudieron haber dejado en cosas o personas, en forma de inferencias racionales, como así también de resultados de experimentaciones (por ejemplo, de pericias).

Uno de los principios del derecho penal es aquel que sostiene que nadie puede ser condenado sin un *justo* juicio previo. Ese sentido de "justicia" está dado de acuerdo a la valoración de las pruebas reunidas en el curso de una investigación que luego son presentadas ante los juzgadores en el marco de un juicio oral. La sola denuncia, sin corroboración probatoria, no es suficiente para acreditar la imputación.[150] La prueba es, por tanto, la mayor garantía frente a la arbitrariedad judicial.

[150] Cámara de Acusación de Córdoba en autos "Rodríguez" (N° 27/81) citado por Cafferata Nores, José I., et al. en "La Prueba en el Proceso Penal"; 7° edición, Abeledo Perrot, pág. 5.

El concepto de prueba está integrado por cuatro componentes: a) los elementos de prueba, b) el órgano de prueba, c) el medio de prueba y d) el objeto de la prueba.

El **elemento de prueba** es *"todo dato objetivo que se incorpora legalmente al proceso, capaz de producir un conocimiento cierto o probable acerca de los extremos de la imputación delictiva"*.[151]

Tal como se ha expuesto, esos datos se componen de rastros o huellas que el hecho pudiera haber dejado sobre personas o cosas, y las inferencias racionales que de éstas se derivan; o bien, el resultado de experimentaciones u operaciones técnicas sobre éstos, como acontece con las pericias.

Más aún, ese dato debe producir una convicción potencial o hipotética por sí mismo de acuerdo a las reglas de la lógica racional. Se requiere de la prueba que sea *objetiva, legal, relevante y pertinente* para los hechos que quieran demostrarse.

La objetividad está relacionada con que el dato provenga del *mundo externo* y que su incorporación al proceso pueda ser controlada por las partes.

La legalidad está orientada al empleo de esa prueba para que el convencimiento judicial sea válido, pudiendo ser ilegal si es irregular su obtención o su incorporación al proceso judicial.

La prueba será relevante o útil tanto cuando produzca certeza de la existencia o no del hecho que se pretende acreditar, como cuando sea empleada como fundamento de una resolución.

[151] Vélez Mariconde, A.(1981). Derecho procesal penal. Lerner, Córdoba. T. I pág. 314 y T.II pág. 201.

La pertinencia está dada por la relación entre el hecho o circunstancia que se quiere acreditar y el elemento de prueba que se pretende utilizar para ello. Debe existir una correlación entre lo que se quiere probar y la prueba elegida para este fin.

El **órgano de prueba** es el sujeto que porta un elemento de prueba y lo transmite al proceso. Resulta ser un intermediario entre la prueba y los operadores judiciales (jueces, fiscales, defensores). El dato del que es portador pudo haberlo conocido accidentalmente (por ej. un testigo) o producto de un encargo judicial (por ej. los peritos), y es la ley de forma la que va a establecer los modos de incorporación de cada uno al proceso.

El **medio de prueba** es *"el procedimiento establecido por la ley tendiente a lograr el ingreso del elemento de prueba en el proceso"*[152]. La regulación legal lo que tiende es a posibilitar que la información o dato ingrese al proceso para ser conocido por el juez y las partes.

El **objeto de la prueba** es aquello que puede ser probado, aquello sobre lo cual debe o puede recaer la prueba. Por ejemplo: hechos naturales (ej.: un fenómeno de la naturaleza), hechos humanos físicos o psíquicos, para comprobar existencia de personas (nacimiento, fallecimiento), o cosas y lugares. También se pueden probar las normas de la experiencia común (p. ej. usos y costumbres de un sector en especial o normas extranjeras).

En cambio, no resultan objeto de prueba los hechos notorios ni los evidentes -salvo que sean controvertidos razonablemente-, ni aquellos sobre los cuales las leyes prohíben hacer prueba.

---

[152] Clariá Olmedo, J: A.(1969) Tratado de derecho procesal penal; EDIAR, Buenos Aires, 1966, T. V. pág. 31. - Florián, Eugenio; "De las pruebas penales", trad. de Guerrero, Temis, Bogotá. T. I., pág. 29.

2.2 La Pericia

La pericia es el *medio probatorio* con el cual se procura la obtención de un dictamen fundado en especiales conocimientos científicos, técnicos o artísticos, útil para el descubrimiento o la valoración de un elemento de prueba. Así,

> *"La prueba pericial consiste en el informe brindado por una persona ajena al proceso, con especiales conocimientos técnicos, y/o científicos sobre la materia en litigio, que a través de un proceso deductivo (de lo general a lo particular), partiendo de sus conocimientos específicos, los aplica al caso concreto y elabora su opinión fundada con los elementos ciertos que surgen de la causa en análisis"*[153].

Se ha sostenido que la función pericial cumple con asistir al órgano jurisdiccional en áreas científicas o técnicas específicas que escapan a la formación jurídica de quienes lo componen o que, por lo menos, no tienen el deber de conocer en profundidad; siendo por tanto un ***auxiliar de la justicia***.

La jurisprudencia lo ha definido de esta forma:

> *"El perito es un técnico que auxilia al juez en la constatación de los hechos y en la determinación de sus causas y efectos, cuando media una imposibilidad física o se requieren conocimientos especiales en la materia. De allí que el mismo debe aplicar su ciencia o arte para poner de manifiesto al órgano jurisdiccional un hecho cuya existencia se niega o para apreciarlo cuando se controvierten sus caracteres."*[154]

Sin embargo, la autoridad judicial no puede renunciar a realizar una pericia aunque posea el conocimiento especializado requerido, ello en virtud del derecho de defensa

---

[153] Gilardi, M. Unzaga Domínguez, G. (2007) La Prueba Pericial en el Proceso Penal de la Provincia de Buenos Aires". Publicación en la Revista Buenos Aires La Ley. Año 14 N° 7 agosto de 2007, página 719.

[154] Cámara Civil y Comercial de La Plata en autos "Goroyeski, Nicolás y ot. c/ Sein, Sergio Fabián y ot. s/ Daños y Perjuicios". Citado por Gilardi, Marcela, op. cit.

en juicio de las partes. En este punto, resulta aplicable el principio del *contradictorio* por el cual las partes no pueden quedar excluidas de controlar el ingreso del elemento probatorio descubierto por la pericia ni de participar en su producción, ni tampoco de la valoración de su eficacia probatoria.[155]

2.3 El Perito. Perito de parte y de oficio. Perito oficial. Diferencias. Deberes y obligaciones

Los peritos son auxiliares de la justicia, y por tanto, poseen ajenidad al proceso.

Entonces, perito **de parte**, será aquél que es designado en el proceso por alguna de las partes en forma privada. Los honorarios que su actuación genere están a cargo de quien lo propuso. De todos modos, para que su participación sea válida, es deber del perito aceptar el cargo para el que es propuesto, lo cual se realiza por Secretaría de la Fiscalía, Juzgado o Tribunal interviniente.

El perito **de oficio**, por el contrario, es elegido de entre una lista de peritos registrados ante los organismos judiciales, procedimiento al que se le llama “desinsaculación”. Es elegido, en tanto y en cuanto alguna de las partes (o ambas) haya solicitado realizar una pericia donde su especialidad sea requerida, y el juez haya resuelto aceptar la realización de esa prueba.

Este perito también deberá aceptar el cargo por Secretaría previo a su actuación. Luego se ceñirá a analizar y responder sobre aquello que presentaron las partes en sus escritos iniciales (demanda y contestación de demanda), que se conocen como puntos de pericia.

El perito de oficio suele ser empleado en procesos civiles y comerciales, laborales, de familia o administrativos,

[155] Cafferata Nores, *Op. Cit.*, pág. 77.

ya que en procesos penales suelen encontrarse nombrados peritos oficiales.

El **perito oficial**, por tanto, es nombrado por una autoridad estatal (judicial o policial) encontrándose dentro de la planta permanente de alguno de los entes estatales (Asesorías Periciales u Oficinas Periciales).

Su intervención se resuelve por el fiscal o juez interviniente, cuando lo estime necesario y conveniente a los fines de acreditar los hechos bajo juzgamiento, debiendo llevar adelante su actuación a través de los puntos de pericia que establezca la autoridad judicial (que puede contemplar los que haya requerido la víctima, el particular damnificado, la defensa o el imputado).

Sea cual sea la calidad del perito y la materia en la que intervengan, todos ellos deben ajustarse a las distintas cuestiones que establece cada ley procesal para que su actuación sea válida. Se expone a continuación cuáles son estos derechos, deberes y obligaciones, a través de un sistema jerárquico conceptual de modo tal que sea fácilmente comprendido.

- **¿Cuándo interviene un perito?**
  - Código Procesal Civil y Comercial: Cuando la apreciación de los hechos controvertidos requiriere conocimientos especiales en alguna ciencia, arte, industria o actividad técnica especializada
  - Código Procesal Penal: Para conocer o apreciar algún hecho o circunstancia pertinentes a la causa en la que sean necesarios o convenientes los conocimientos especiales en alguna ciencia, técnica o arte.
- **Idoneidad del Perito**
  - Código Procesal Civil y Comercial (art. 462): Si la profesión estuviese reglamentada, los peritos

deberán tener título habilitante en la ciencia, arte, industria o actividad técnica especializada a que pertenezcan las cuestiones acerca de las cuales deban expedirse. En caso contrario, o cuando no hubiere peritos en el lugar del proceso, podrá ser nombrada cualquier persona entendida aun cuando careciere de título.

- Código Procesal Penal (art. 244): Los peritos deberán tener títulos habilitantes en la materia a la cual pertenezca el punto sobre el que han de expedirse. Si no estuviera reglamentada la profesión, no hubiere peritos diplomados o inscriptos, deberá designarse a una persona de conocimiento o de práctica reconocidas.

- **Nombramiento de los peritos en los procesos civiles**
  - Las partes:
    - Ofrecen prueba → Indicando especialización de los peritos
    - Proponen puntos de pericia
  - Juez:
    - Resuelve admitiendo prueba pericial
    - Fija audiencia (por escrito)
    - Designación de perito único o de cada parte.
    - Si no hay acuerdo o no se propone a ninguno → Nombra uno el Juez (a sorteo de la lista)

- **Aceptación del cargo (procesos civiles)**
  - Ante el Secretario, dentro de tercero día de notificado cada uno de su designación
  - Bajo juramento o bajo promesa de desempeñar fielmente el cargo, en el caso de no tener título habilitante.

- Se los citará por cédula u otro medio autorizado por este CPCC.
- Si el perito no aceptare, o no concurriere dentro del plazo fijado, el Juez nombrará otro en su reemplazo, de oficio y sin otro trámite.

- **Puntos de pericia (procesos civiles)**
  - Partes:
    - Pueden formular observaciones de los puntos de pericia
  - Juez:
    - Resuelve sobre los puntos de pericia (puede agregar o eliminar los improcedentes o superfluos)
    - Fija plazo dentro del cual deben expedirse los peritos
    - Si no se fija plazo → 30 días
- **Tarea Pericial en procesos civiles**
  - Los peritos practicarán unidos la diligencia, si no tuvieren razón especial para lo contrario.
  - Las partes y sus letrados podrán asistir a ella y hacer las observaciones que consideraren pertinentes, debiendo retirarse cuando los peritos pasen a deliberar.
  - **Dictamen inmediato**
    - Cuando el objeto de la diligencia pericial fuese de tal naturaleza que permita a los peritos expedirse inmediatamente, podrán dar su dictamen por escrito o en audiencia, en cuyo caso informará uno de ellos si existiere unanimidad.
  - **Dictamen**
    - Se presenta por escrito → con copias para las partes

- Contiene explicación detallada de las operaciones técnicas realizadas y de los principios científicos en que los peritos funden su opinión.
- Los peritos que concordaren, presentarán un único texto firmado por todos.
- Los disidentes lo harán por separado y siempre en un mismo escrito, salvo que por circunstancias especiales ello no fuere posible.
- Del dictamen → Se da traslado a las partes
- A pedido de las partes o del Juez se podrá ordenar:
- Pedido de explicaciones (en audiencia o por escrito)
- Pérdida de derecho a cobrar honorarios (total o parcialmente) si el perito no concurre o no presenta el informe ampliatorio o complementario dentro del plazo.

- **Informes científicos o técnicos en procesos civiles**
  - A petición de parte o de oficio, el Juez podrá solicitar informes a academias, corporaciones, institutos y entidades públicas o privadas de carácter científico o técnico, cuando el dictamen pericial requiriese operaciones o conocimientos de alta especialización.
  - A pedido de las entidades privadas se fijará el honorario que les corresponda percibir.

- **Fuerza probatoria en procesos civiles**
  - La fuerza probatoria del dictamen pericial será estimada por el Juez teniendo en consideración la competencia de los peritos, la uniformidad o disconformidad de sus opiniones, los principios científicos en que se fundan, la concordancia de su aplicación con las reglas de la sana crítica y demás pruebas y elementos de convicción que la causa ofrezca.

- **Recusación de Peritos**
  - La realizan las partes
  - Por justa causa
  - Hasta 5 días después de notificado
  - Los nombrados por las partes sólo serán recusables por causas sobrevinientes a la elección o cuya existencia se hubiese conocido con posterioridad.
- **Excusación de Peritos**
  - La realizan los propios peritos
- **Causales de Recusación / Excusación (Procesos civiles)**
  - Parentesco por consanguinidad dentro del cuarto grado y segundo de afinidad con alguna de las partes, sus mandatarios o letrados.
  - Tener el perito o sus consanguíneos o afines dentro del grado expresado en el inciso anterior, interés en el pleito o en otro semejante, o sociedad o comunidad con algunos de los litigantes, procuradores o abogados, salvo que la sociedad fuese anónima.
  - Tener pleito pendiente con el recusante.
  - Ser acreedor, deudor o fiador de alguna de las partes, con excepción de los bancos oficiales.
  - Ser o haber sido el perito denunciador o acusador del recusante ante los tribunales, o denunciado o acusado ante los mismos tribunales, con anterioridad a la iniciación del pleito.
  - Ser o haber sido el perito denunciado por el recusante en los términos de la ley de enjuiciamiento de magistrados, siempre que la Suprema Corte hubiere dispuesto dar curso a la denuncia.

- Haber sido el perito defensor de alguno de los litigantes o emitido opinión o dictamen o dado recomendaciones acerca del pleito, antes o después de comenzado.
- Haber recibido el perito beneficios de importancia de alguna de las partes.
- Tener el perito con alguno de los litigantes amistad que se manifieste con gran familiaridad o frecuencia de trato.
- Tener contra la parte recusante enemistad, odio o resentimiento, que se manifieste por hechos conocidos. En ningún caso procederá la recusación por ataques u ofensas inferidas al perito después que hubiese comenzado a conocer del asunto.

- **Causales de remoción (Procesos civiles)**
  - El perito que después de haber aceptado el cargo renunciare sin motivo atendible, rehusare dar su dictamen o no lo presentare oportunamente.
  - El Juez, de oficio, nombrará otro en su lugar y lo condenará a pagar los gastos de las diligencias frustradas y los daños y perjuicios ocasionados a las partes, si éstas los reclamasen. El reemplazado perderá el derecho a cobrar honorarios.
  - La negligencia de uno de los peritos no excusará a los otros, quienes deberán realizar las diligencias y presentar el dictamen dentro del plazo.

- **Parte económica del actuar forense en procesos civiles**
  - Anticipo de gastos
    - A solicitud del perito → dentro de tercero día de haber aceptado el cargo, y si correspondiere por la índole de la pericia, la o las partes que han

ofrecido la prueba deberá/n depositar la suma que el Juzgado fije para gastos de las diligencias.
    - Dicho importe deberá ser depositado dentro de quinto día de ordenado y se entregará a los peritos, sin perjuicio de lo que en definitiva se resuelva respecto de las costas y del pago de honorarios.
    - La falta de depósito dentro del plazo importará el desistimiento de la prueba.

  - Cargo de gastos y honorarios
    - A cargo de la parte que la propuso.
    - A cargo de ambas partes en el caso en que haya resultado necesaria para la solución del pleito, circunstancia ésta que se señalará en la sentencia.

- **Tarea pericial en procesos de familia**

  - Se realiza por intermedio de los profesionales integrantes del equipo técnico del Juzgado.

  - Si se tratare de una especialidad distinta que no esté dentro de este equipo técnico → se lo designará de la Asesoría Pericial Departamental.

  - SI la Asesoría no dispone de la especialidad → se lo desinsaculará de la lista respectiva.

  - Los peritos, sin perjuicio de su concurrencia a la vista de la causa, anticiparán su dictamen por escrito no menos de diez (10) días previos de la audiencia. Las partes podrán solicitar explicaciones conforme al artículo 473 del CPCC que serán dadas en la vista de la causa.

  - Audiencia vista de causa → Procurar que las partes, testigos y peritos se pronuncien con amplitud respecto de todos los hechos pertinentes controvertidos

- En todo lo demás aplica por defecto (subsidiariamente) el Código Procesal Civil y Comercial.

- **Nombramiento de los peritos en el proceso penal**
  - ¿Quiénes no pueden ser peritos? (Art. 245 CPP)
    - Los incapaces.
    - Los que deban o puedan abstenerse de declarar como testigos o que hayan sido citados como tales en la causa
    - Los condenados o inhabilitados

- **Causales de Recusación / Excusación (Proceso Penal)**
  - Si en el mismo proceso hubiere pronunciado o concurrido a pronunciar sentencia sobre puntos a decidir; si hubiere intervenido como funcionario del Ministerio Público, defensor, mandatario, denunciante, particular damnificado o querellante; si hubiera conocido el hecho investigado como testigo.
  - Si hubiere intervenido o interviniere en la causa algún pariente suyo dentro del cuarto grado de consanguinidad o segundo de afinidad.
  - Si fuere pariente, en los grados preindicados, de algún interesado, su defensor o mandatario.
  - Si él o alguno de dichos parientes tuvieren interés en el proceso.
  - Si fuere o hubiere sido tutor o curador o hubiere estado bajo tutela o curatela de alguno de los interesados.
  - Si él o sus parientes, dentro de los grados preindicados, tuvieren juicio pendiente iniciado con anterioridad, o sociedad o comunidad con alguno de los interesados, salvo la sociedad anónima.
  - Si él, su cónyuge, padres o hijos u otras personas que vivan a su cargo, fueren acreedores, deudores o

fiadores de alguno de los interesados, salvo que se tratare de bancos oficiales o constituidos por sociedades anónimas.

- Si antes de comenzar el proceso hubiese sido acusador o denunciante de alguno de los interesados, o denunciado acusado o demandado por ellos, salvo que circunstancias posteriores demostraren armonía entre ambos.
- Si antes de comenzar el proceso, alguno de los interesados le hubiere promovido juicio de destitución, y la acusación fuere admitida.
- Si hubiere dado consejos o manifestado extrajudicialmente su opinión sobre el proceso.
- Si tuviere amistad íntima o enemistad manifiesta con alguno de los interesados.
- Si él, su cónyuge, padres o hijos u otras personas que vivan a su cargo hubieren recibido o recibieren beneficios de importancia de alguno de los interesados; o si después de iniciado el proceso, reciben presentes o dádivas, aunque sean de poco valor.
- Si mediaren circunstancias que, por su gravedad, afecten su independencia e imparcialidad.

- **Designación de peritos en el Proceso Penal**
  - Fiscal:
    - Designa perito de **oficio** entre los **peritos oficiales**.
    - Si no los hubiere, entre los funcionarios públicos que, en razón de su título profesional o de su competencia, se encuentren habilitados para emitir dictamen acerca del hecho o circunstancias que se quieren establecer.

- Notifica al imputado, a los defensores y al particular damnificado **antes** de iniciadas las operaciones periciales **bajo sanción de nulidad** (art. 247 del C.P.P.B.A.). Dentro de 3 días de notificado, puede proponer cada parte -a su costa- otro perito legalmente habilitado.

- Peritos propuestos por las partes:
  - No regirán para estos últimos los artículos 245, segundo párrafo y 246. No pueden excusarse ni ser recusados

- **Obligatoriedad del cargo – Deber del perito**
  - El designado como perito tendrá el deber de aceptar y desempeñar fielmente el cargo, salvo que tuviere un grave impedimento. En tal caso deberá ponerlo en conocimiento del Agente Fiscal al ser notificado de la designación.
    - Si no acudiera a la citación, o no presentare el informe en debido tiempo, sin causa justificada, incurrirá en las responsabilidades señaladas para los testigos en los artículos 133 y 239.
    - Art. 133: Formas de citación. Conducción por la fuerza pública (ante causa no justificada). La incomparecencia injustificada, implicará abonar las costas que se causaren, sin perjuicio de la responsabilidad penal que corresponda.
    - Art. 239: Arresto en el caso de negativa.
  - Los peritos no oficiales aceptarán el cargo bajo juramento.
  - El designado como perito de parte es equiparado a funcionario público.
    - Los peritos de parte designados por resolución judicial se encuentran en la misma situación que los designados de oficio.

- Deber de guardar secreto frente a terceros ajenos al proceso.
- Deber de expresarse con veracidad sobre los puntos periciales.

- **Directivas – Puntos periciales (Proceso Penal)**
  - Fiscal:
    - Dirigirá la pericia
    - Formulará concretamente las cuestiones a elucidar
    - Fijará el plazo en que ha de expedirse el perito y si lo juzgare conveniente, asistirá a las operaciones.
    - Podrá autorizar al perito para examinar las actuaciones o asistir a determinados actos procesales.
  - Peritos:
    - Procurarán que las cosas a examinar sean en lo posible conservadas, de modo que la pericia pueda repetirse.
    - Si fuere necesario destruir o alterar los objetos analizados o hubiere discrepancia sobre el modo de operar, los peritos deberán informar al Agente Fiscal antes de proceder.

- **Tarea pericial en el Proceso Penal**
  - De existir perito de parte, practicarán unidos el examen, deliberarán en sesión secreta, a la que sólo podrá asistir el Agente Fiscal y si estuvieran de acuerdo, redactarán su informe en común.
  - En caso contrario, harán por separado sus respectivos dictámenes.
  - Si los informes discreparen fundamentalmente, se podrá nombrar otros peritos, según la importancia del caso, para que lo examinen e informen sobre su

mérito o si fuere necesario y posible, realicen otra pericia.

- **Dictamen pericial en el Proceso Penal**
  - El dictamen pericial podrá expedirse por informe escrito o hacerse constar en acta y comprenderá, en cuanto fuere posible:
    - La descripción de las personas, lugares, cosas o hechos examinados, en las condiciones en que hubieren sido hallados.
    - Una relación detallada de todas las operaciones practicadas y sus resultados.
    - Las conclusiones que formulen los peritos, conforme los principios de su ciencia, técnica o arte.
    - Lugar y fecha en que se practicaron las operaciones.
- **Parte económica del actuar forense en el Proceso Penal**
  - Honorarios
    - Los peritos nombrados de oficio tendrán derecho a cobrar honorarios, salvo que tengan sueldo por cargos oficiales desempeñados en virtud de conocimientos específicos en la ciencia, técnica o arte que el informe requiera.
    - El perito nombrado a petición de parte podrá cobrarlos siempre, directamente a ésta o al condenado en costas.
- **Actuación del perito en el Juicio Oral**
  - Los testigos, peritos o intérpretes prestarán juramento de decir verdad ante el Tribunal, bajo sanción de nulidad.
  - Serán interrogados primeramente por la parte que los propuso.

- Seguidamente quedarán sujetos a las repreguntas de las otras partes intervinientes.
- Asimismo, las partes en cada caso indicarán si han terminado con el testigo o si el mismo debe permanecer a disposición del Tribunal.
- Las evidencias que hayan sido secuestradas se presentarán, según el caso, a las partes y a los testigos a quienes se invitará a reconocerlos y a declarar lo que fuere pertinente.

- **Actuación del perito en el Juicio por Jurados**
  - Prestarán juramento de decir verdad ante el Tribunal.
  - Serán interrogados primeramente en examen directo por la parte que los propuso, la cual no podrá efectuar preguntas sugestivas ni indicativas.
  - No se admitirán preguntas engañosas, repetitivas, ambiguas o destinadas a coaccionar ilegítimamente al testigo o perito.
  - Las partes podrán objetar las preguntas inadmisibles indicando el motivo.
  - El Tribunal procurará que no se utilicen las objeciones para alterar la continuidad de los interrogatorios.
  - Cuando sea necesario para demostrar o superar contradicciones o fuere indispensable para ayudar a la memoria del testigo o perito, podrá ser confrontado con las declaraciones previas prestadas.
  - Los jueces y los jurados no podrán por ningún concepto formular preguntas a quienes comparezcan a declarar al juicio. El incumplimiento de esta prohibición constituirá falta grave.

4. Perito Informático. Ley N° 13.016 de Ejercicio Profesional en la Provincia de Buenos Aires. Ética profesional

Tanto el Código Procesal Civil y Comercial como el Procesal Penal reglamentan acerca de la idoneidad para ser perito en las causas judiciales. Ambos indican que de estar reglamentada la profesión, los peritos deberán tener título habilitante en la ciencia, arte, industria o actividad técnica especializada a que pertenezcan las cuestiones acerca de las cuales deban expedirse; y sólo en el caso en que no lo estuviera o no hubiere peritos diplomados o inscriptos, deberá designarse a una persona de conocimiento o de práctica reconocidas.

En la Provincia de Buenos Aires la profesión del informático se encuentra regulada por la Ley N° 13.016[156] que regula el ejercicio profesional en todo el ámbito provincial. De igual forma, las Provincias de Córdoba[157], Entre Ríos[158], Tucumán[159], Misiones[160], La Rioja[161] y Catamarca[162], también poseen normativa específica que legisla sobre el particular. La Provincia de Santa Fe[163] y la Ciudad Autónoma de Buenos Aires[164], tienen proyectos de ley en trámite al respecto.

---

[156] Buenos Aires. Ley N° 13.016. Disponible en: http://www.gob.gba.gov.ar/legislacion/legislacion/l-13016.html

[157] Córdoba. Ley N° 7642/87. Disponible en: http://www.cpcipc.org.ar/quienes-somos/la-ley/

[158] Entre Ríos. Ley N° 9498. Disponible en: http://www.coprocier.org.ar/archivos/9498-COPROCIER.pdf

[159] Tucumán. Ley N° 7490. Disponible en: http://rig.tucuman.gov.ar/leyes/scan/scan/L-7490-07012005.pdf

[160] Misiones. Ley N° 3752. Disponible en: http://www.diputadosmisiones.gov.ar/digesto_juridico/documentos/43.pdf

[161] La Rioja. Ley N° 6911. http://www.cpcilar.org/wp-content/uploads/2011/06/Ley_6911.pdf

[162] Catamarca. Ley N° 5169.

[163] Santa Fe. La Asociación Provincial de Profesionales en Informática nuclea a los profesionales de la informática de esta provincia quienes tienen

Debe recordarse que los colegios o consejos profesionales son asociaciones integradas por quienes ejercen una profesión liberal y que suelen estar amparados por el Estado (corporación de derecho público). Sus miembros asociados son conocidos como colegiados. Tradicionalmente la finalidad de los colegios profesionales ha sido la ordenación del ejercicio de las profesiones, la representación exclusiva de las mismas, y la defensa de los intereses profesionales de los colegiados. El colegio debe velar por el cumplimiento de una buena labor profesional, donde la práctica ética del trabajo se constituye como uno de los principios comunes que ayudan a definir los estatutos de cada corporación.

Estos estatutos, redactados en la mayoría de los colegios profesionales, aluden al desarrollo de la actividad correspondiente a cada profesión, donde se marcan pautas de actuación consideradas de manera unánime como éticas y que contribuyen al bien social de la profesión.

Las materias que suelen regularse en las leyes de ejercicio profesional tienen que ver con: a) Capacidad de las corporaciones para dictar normas de ética profesional. b) Existencia de un régimen disciplinario. c) Atribución de imponer contribuciones. d) Facultad de dictar normas administrativas. e) Existencia de Consejos Federales y locales de Supervisión.

La Ley N° 13.016 de la Provincia de Buenos Aires establece en su primer Título, las cuestiones relativas al ejercicio profesional, como quiénes pueden matricularse (títulos de pregrado, grado y posgrado en la materia) y de qué modo será considerado ejercicio profesional:

---

un estatuto vigente y un proyecto de ley presentado para convertirse en un Consejo Profesional http://www.appei.org.ar/index.php?m=ley&a=listado.

[164] Ciudad Autónoma de Buenos Aires. Estatuto del CPCI. Disponible en: http://www.cpci.org.ar/index.php/institucional/estatuto. Proyecto de ley disponible en: http://www.cpci.org.ar/index.php/proyecto

1. La publicidad ofreciendo servicios.
2. La emisión, reproducción o difusión de las palabras: Analista, Licenciado, Ingeniero, Asesor, Consultor, Computador, Experto, Auditor o similares y sus equivalencias en idiomas extranjeros, con referencia a cualesquiera de los ámbitos de las profesiones reglamentadas por esta ley.
3. El empleo de los términos Academia, Estudio, Asesoría, Consultoría, Oficina, Centro, Sociedad, Asociación, Organización u otros similares y sus equivalentes en idiomas extranjeros, con referencia a cualquiera de las profesiones reglamentadas por esta ley.

También se contempla en esta primera parte sobre las actividades que se entienden contempladas, a modo de ejemplo:

1. Relevar y analizar los procesos funcionales de una organización, con la finalidad de diseñar sus Sistemas Informáticos asociados.
2. Entender, planificar, dirigir y/o controlar el diseño y la implementación de sistemas informáticos orientados hacia el procesamiento manual o automático, mediante máquinas o equipamiento electrónico y/o electromecánico.
3. Entender, planificar y/o dirigir los estudios técnico-económico de factibilidad y/o referentes a la configuración y dimensionamiento de sistemas automatizados de procesamiento de datos.
4. Supervisar la implantación de los sistemas automatizados de procesamiento de datos y organizar y capacitar al personal afectado por dichos sistemas.
5. Organizar, dirigir y controlar Centros de Procesamientos de Datos o Centros de Cómputos, seleccionar y capacitar al personal de los mismos, preparar y capacitar al personal de todas las áreas afectadas por su servicio.
6. Asesorar, evaluar y verificar la utilización, eficiencia y confiabilidad del equipamiento electrónico o Datos o Centros de Cómputos. Desarrollar y aplicar técnicas de

seguridad en lo referente al acceso y disponibilidad de la información, como así también, los respaldos de seguridad de todos los recursos, como así también de la información procesada por los mismos.

7. Determinar, regular y administrar las pautas operativas a regir en las instalaciones de Procesamiento de operables.
8. Instrumentar y emitir toda documentación que respalde la actividad del Centro de Procesamiento de datos. También diseñar y confeccionar los manuales de procesos y los formularios requeridos para el procesamiento de la Información.
9. Crear, implantar, rever y actualizar las normas de control que hacen al funcionamiento, interno o externo, de los Centros de Procesamiento de datos.
10. Efectuar las tareas de Auditoría de los Sistemas Informáticos, de los Centros de Procesamiento, y de las redes de datos.
11. Participar en ámbitos públicos o privados, en tareas vinculadas con el desarrollo, difusión y supervisión de las actividades relacionadas con la Informática.
12. Desempeñar cargos, funciones, comisiones o empleos dependientes de organismos oficiales, privados o mixtos para cuya designación se requiera estar habilitado en Ciencias Informáticas, o para los que se requieran conocimientos propios de la profesión.
13. Realizar arbitrajes, pericias y tasaciones relacionados con los Sistemas Informáticos y todo el equipamiento para el Procesamiento de Datos. Dictaminar e informar a las Administraciones e Intervenciones Judiciales como perito en su materia, en todos los fueros.
14. Cualquier otra tarea que no estando presente en los anteriores incisos requiera de los conocimientos propios de la profesión.

De igual forma se establece que los graduados contemplados en esta ley solo podrán hacer ejercicio profesional dentro de las incumbencias fijadas por sus respectivos títulos, cuestión que es importante tener en cuenta

para el momento en ser elegido como perito en un proceso judicial, ya que *"si los puntos de pericia versan sobre temas a resolver de un ámbito ajeno a las incumbencias otorgadas por el título, el perito debe excusarse de intervenir"*.

La Ley también prevé los requisitos necesarios para matricularse en el Colegio, las cuestiones relativas a las atribuciones del Consejo Profesional -entre las que se encuentra la elaboración de un Código de Ética Profesional y su reglamento interno de funcionamiento-, la forma en que se llevarán a cabo las asambleas de los matriculados, las atribuciones del Consejo Directivo, el Tribunal de Disciplina y la forma en que se llevarán a cabo las elecciones de renovación de los cargos directivos.

La cuestión de la **ética profesional** es uno de los ejes que todo colegio profesional debe regular. En particular, el Consejo Profesional de Ciencias Informáticas de la Provincia de Buenos Aires tiene ya elaborado un código de ética[165] que es aplicado a todo profesional matriculado en él por el hecho de serlo sin importar la índole de su actividad o especialidad que cultive tanto en el ejercicio independiente o cuando actué como funcionario de una organización. Abarca también a los Profesionales de Ciencias Informáticas que ejerzan otra profesión u oficio.

La ética debe tener en primer lugar una finalidad docente, es decir debe educar las tendencias, inclinaciones y disposiciones interiores propias de las personas y secundariamente permitir la emisión de un juicio sobre un acto concreto. De esa manera se evitará entrar en un conflicto de valores negociables: por un lado el éxito profesional y por el otro los problemas de conciencia.

[165] Consejo de Profesionales de Ciencias Informáticas. Código de Ética Profesional. Versión online accesible en julio 2016: http://www.cpciba.org.ar/archivos/documentos/codigo_etica_profesional.pdf

En particular resulta de vital relevancia para la disciplina de la informática forense debido al nivel de información que puede llegar a conocer un profesional al momento de realizar una pericia en un proceso judicial, y que constituye una de las respuestas al dilema que todo profesional que se inicia en la materia realiza: *¿Hasta dónde puedo intervenir? ¿Existe un límite en la realización de la pericia?*

En el ámbito internacional los códigos de ética de profesionales en el área de informática forense, son gestionados por institutos como el *High Technology Crime Investigation Assosiation* (HTCIA) y el *American College of Forensic Examiners Institute,* entidades reconocidas a las cuales el profesional de esta disciplina debe adherirse no solamente por los aspectos técnicos sino también por a los estatutos, normas y códigos de ética que en ellas han establecido para poder desempeñarse como inspector certificado en el área[166].

Algunas normas éticas destinadas a los informáticos forenses, en las que ponen énfasis estas instituciones, están dirigidas a que no debe existir algún interés propio en el resultado de algún caso en específico ya sea por factores económicos o por alguna relación entre las personas investigadas del caso. Además el perito debe ser imparcial, limitándose a los hechos de un caso y reportando todos los detalles independientemente de los deseos de los defensores en el proceso. Esta postura ética del informático forense hace que hable con la verdad incluso cuando sus conclusiones no sean del agrado de las partes y dan como resultado una buena labor para que en la audiencia quienes intervienen

[166] Andrade, R. Códigos de ética y responsabilidad profesional en la computación forense. Disponible: https://www.linkedin.com/pulse/c%C3%B3digos-de-%C3%A9tica-y-responsabilidad-profesional-en-la-forense-andrade

puedan tomar mejores decisiones o aplicaciones para el caso[167].

En el código de ética profesional de la Provincia de Buenos Aires se presentan definiciones y directrices que marcan estas pautas de trabajo, incluso, algunas de ellas tienen implicación directa al actuar forense, como el **valor de la justicia,** que es la base de cualquier ordenamiento social justo y por lo tanto de una loable tarea profesional. El concepto romano de justicia es el de *"dar a cada uno lo que corresponde".* En relación a la justicia hay dos valores fundamentales asociados: **la veracidad**, que se fundamenta en la verdad, es decir en la adecuación del pensamiento con la realidad que es lo que la inteligencia siempre debe buscar para no caer en el error, en el engaño o el delito, y la **fidelidad a la palabra dada** que tiene que ver con cumplir con exactitud cuánto ha sido prometido.

La intervención del profesional informático, y sobre todo en un proceso judicial donde coadyuva desde su técnica a otros profesionales de áreas diferentes que resuelven sobre situaciones de terceras personas, tiene a su vez que sustentarse en otros pilares fundamentales, como la **credibilidad, la confidencialidad y la objetividad.**

Constituye un requisito ineludible que la información sea creíble, es decir que dé por verdadera una cosa cuyo conocimiento no la tiene por propia experiencia sino que le es comunicado por otro. La veracidad es el fundamento esencial de la información. De no cumplirse con ella se estaría ante una desinformación o lo que es más grave una deformación.

La confidencialidad es entendida en el sentido que el ejercicio profesional se debe llevar a cabo en un marco de estricta reserva o secreto. Se es confidencial cuando se respeta el secreto profesional.

[167] Idem; Op. Cit.

La objetividad consiste en el firme propósito de que quien lleve a cabo una actividad profesional analice los problemas tal cual son en la realidad, prescindiendo de preferencias, intereses o posturas propias. En la objetividad se encuentra finalmente la verdad.

La **Independencia de criterio** es otra de las cuestiones a tener en cuenta, ya que al momento de expresar cualquier juicio sobre un tema que le toca tratar, el profesional en informática deberá mantener un criterio libre e imparcial, sin condiciones de ningún tipo, lo que va de la mano con la objetividad.

Como deber de responsabilidad de los matriculados hacia el proveedor de recursos para el ejercicio de su labor es importante el **secreto profesional**, teniendo la obligación de guardarlo y de no revelar por ningún motivo los hechos, datos o circunstancias de que tenga conocimiento, a menos que lo autoricen los interesados. Ello es importante en el marco de un proceso judicial ya que existen sanciones penales para quien revelase información sin estar autorizado, pudiendo quedar alcanzado por los delitos vinculados a revelación de secretos profesionales en alguna de sus modalidades (art. 117 bis, 156, 157 y 157 bis del Código Penal).

3.1 Prueba Científica. Prueba Informática

Los profesionales de la informática deben realizar conclusiones sobre un tema cuando puedan demostrar que éstas tienen un fundamento basado en la ciencia que han estudiado. Se considera que una opinión es calificada cuando expresan un punto de vista en un área de su competencia.

En los procesos judiciales se busca resolver situaciones de terceras personas, ya sea sobre sus personas en sí o la de sus familiares, o sobre los bienes que poseen. Los profesionales del derecho formulan hipótesis que permiten sostener una acusación o planteo frente a quien se encuentra en la vereda opuesta, y tal premisa se ve robustecida por

aquellas pruebas que surjan de otras ciencias, en este caso, de la informática.

Sin embargo, al ser la informática -en términos generales- una disciplina nueva, su utilización en el campo judicial requiere de una interrelación con otras áreas del conocimiento que interactúan en un proceso legal, como lo son la criminalística y el derecho, involucrándose así dentro de las ciencias forenses.

La informática forense arribó al ámbito de la criminalística recién a fines del siglo XX, a partir de la detección de casos de fraudes a través de computadoras y del surgimiento de Internet[168]. A diferencias de otras disciplinas forenses, no existe una persona o institución única que haya abordado el tema por primera vez, sino que la necesidad de su estudio fue advertida desde distintos campos.

Por ejemplo, uno de los primeros estudios académicos realizados mediante la aplicación de métodos científicos fue el que realizó el jurista alemán Ulrich Sieber en 1977 bajo el título *Computerkriminalitatundstrafech*, tratándose del primer abordaje realizado desde un punto de vista legal[169].

Por su parte, en 1978 en el estado de Florida (Estados Unidos), se reconocieron los crímenes de sistemas informáticos en el "Computer Crimes Act", para los casos de sabotaje, propiedad intelectual, modificación de datos y ataques similares.

Desde el lado de la informática también comenzaron a surgir iniciativas de desarrollo de herramientas forenses, como las publicadas en 1982 por Peter Norton, *"UnErase: Norton*

[168] En 1973 en EEUU se produce un fraude de más de 30 millones de dólares por parte de la empresa EquityFunding por la manipulación de registros de los 56.000 contratos de seguros de sus clientes. Cfr. Sain, Gustavo; "¿Qué son los delitos informáticos?". Edit. Rubinzal Culzoni. RC D 875/2015. Pág. 1

[169] Idem. Op. Cit.

Utilities 1.0", la primera versión del conjunto de herramientas "Norton Utilities", entre las que destacan UnErase, una aplicación que permite recuperar archivos borrados accidentalmente. En tanto, en 1984 el FBI formó el *Magnetic Media Program,* que más tarde, en 1991, se convirtió en el *Computer Analysis and Response Team* (CART)[170].

Es a partir de la década del '70 del siglo pasado, donde comienza a haber distintas iniciativas tanto gubernamentales -a partir de legislar sobre nuevas modalidades delictivas o en la creación de agencias- como del propio ámbito de la informática al desarrollar herramientas forenses para la recuperación y análisis de información. Las primeras reformas legislativas[171] en relación a la recolección, almacenamiento y transmisión de los datos personales en computadoras y redes informáticas se dieron en Suecia en 1973, Estados Unidos en 1974 y Alemania en 1978 al incorporar figuras relativas a la protección de la privacidad en sus normativas.

Los profesionales del área comienzaron a formalizar grupos de investigación y trabajo como la *High Tech Crime Investigation Association* (HTCIA)[172] creada en 1987 en Santa Clara, EE.UU., con el fin de reunir tanto a quienes trabajaban en agencias gubernamentales como en las compañías privadas para centralizar conocimientos e impartir cursos de capacitación.

Al año siguiente se creó la International *Association of Computer Investigative Specialists* (IACIS), con el objeto de certificar los conocimientos de los profesionales de agencias

[170] Ramos, A. Historia de la Informática Forense. publicado en el sitio web "Security by Default". Disponible en: http://www.securitybydefault.com/2011/03/historia-de-la-informatica-forense.html Accesible: julio 2016.
[171] Sain, G. Op Cit. pág. 1 y 4
[172] Sitio web: High Technology Crime Investigation Association. En: https://www.htcia.org/history/

gubernamentales en el *Certified Forensic Computer Examiner* (CFCE)[173].

En ese mismo año se desarrolló el programa *Seized Computer Evidence Recovery Specialists* (SCERS), con el objetivo de comenzar a formar a profesionales en informática forense. El libro *"A forensic methodology for countering computer crime"*, de P. A. Collier y B. J. Spaul acuñó en 1992 el término *"computer forensics".* Otros libros posteriores continuaron desarrollando el término y la metodología, como: *"High-Technology Crime: Investigating Cases Involving Computers"* de Kenneth S. Rosenblatt.

En 1995, se creó la *International Organization on Computer Evidence* (IOCE), con objetivo de ser punto de encuentro entre especialistas en la evidencia electrónica y el intercambio de información; y a partir de 1996 la Interpol organiza los International *Forensic Science Symposium*, como foro para debatir los avances forenses, así como aunar esfuerzos en pos de la criminalidad informática.

Ya en este siglo, en agosto de 2001, se inició el *Digital Forensic Research Workshop* (DFRWS)[174], grupo de debate y discusión internacional que organiza conferencias sobre la temática de la informática forense en vistas de superar retos y mancomunar esfuerzos internacionales en la investigación y desarrollo de la temática.

Este relevamiento histórico sobre los múltiples orígenes y abordajes de la informática forense y su reciente incorporación dentro del campo de las ciencias forenses, permite comprender la importancia de darle un andamiaje legal y técnico que permita sostener la validez de la evidencia digital, de modo tal que quien se desempeñe en el ámbito pericial pueda sustentar cada una de las afirmaciones que se

[173] Ramos, A. Op. Cit.
[174] Sitio web: Digital Forensic Research Workshop (DFRWS). En: http://www.dfrws.org/about-us

realice apoyándose en su propia ciencia y volviéndola válida para su utilización por parte de otras disciplinas.

Es en este sentido que el experto o técnico informático tendrá, entonces, el cometido de llevar adelante la recuperación correcta de toda la información posible, tanto visible como oculta, relacionada con el hecho de estudio, aplicando las técnicas y herramientas disponibles o creándolas, y garantizando un proceso reproducible de adquisición, examen, análisis, cotejo, preservación y presentación de la evidencia, que fortalezca su valor probatorio ante los órganos jurisdiccionales.

A la hora de recuperar la información, el informático forense debe trabajar con diferentes plataformas, métodos de almacenamiento, tecnologías que naturalmente eliminan evidencias, mecanismos internos de protección de la información, ausencia de herramientas específicas, herramientas que cubren solo una parte del proceso, sistemas de criptografía, entre otros problemas.

Por ello, por la complejidad a la que puede enfrentarse un informático forense, es que se requiere de la formación de profesionales calificados desde lo técnico y respetuosos de los procedimientos que fijan los códigos procesales para la actuación forense.

Los autores de este libro son profesionales de distintas especialidades que trabajan interdisciplinariamente en informática forense, basándose en conocimientos del campo jurídico, de la criminalística y de la ingeniería en informática. Este equipo ha desarrollado un Proceso Unificado de Recuperación de la Información (PURI®) que aporta las técnicas y herramientas disponibles para la tarea forense, dándole un marco jurídico a través de la elaboración de la Guía de Empleo de la Informática Forense en el Proceso Penal que incluye un Protocolo de Actuación en Informática

Forense[175], a seguir en los procesos judiciales en que su utilización sea requerida y que fuera aprobado[176] por la Procuración General de la Provincia de Buenos Aires para su implementación en todo el ámbito provincial. En los próximos capítulos se explicarán las distintas fases, actividades, tareas, técnicas y herramientas del PURI® que da sustento científico a los requerimientos judiciales que deben llevar adelante los informáticos forenses.

Bibliografía

Andrade, R. Códigos de ética y responsabilidad profesional en la computación forense". Disponible: https://www.linkedin.com/pulse/c%C3%B3digos-de-%C3%A9tica-y-responsabilidad-profesional-en-la-forense-andrade

Buenos Aires. Ley N° 13.016. Disponible en: http://www.gob.gba.gov.ar/legislacion/legislacion/l-13016.html

Buompadre, J.E. (2013) Manual de Derecho Penal. Parte especial. Edit. Astrea; Buenos Aires.pág. 379.

Cafferata Nores, J.I., et al. en La Prueba en el Proceso Penal. 7° edición, Abeledo Perrot

Cámara Civil y Comercial de La Plata en autos "Goroyeski, Nicolás y ot. c/ Sein, Sergio Fabián y ot. s/ Daños y Perjuicios". Citado por Gilardi, Marcela, op. cit.

Catamarca. Ley N° 5169.

[175] Di Iorio, Ana H. y otros (2016) Guía integral de empleo de la informática forense en el proceso penal. 2° edición revisada, Mar del Plata, Universidad FASTA, 2016. Accesible: julio 2016. Disponible en: http://info-lab.org.ar/images/pdf/PAIF.pdf

[176] Resolución 483/16 de la Procuración de la Suprema Corte de la Provincia de Buenos Aires. Accesible: julio 2016. Disponible en: http://info-lab.org.ar/images/pdf/Res48316.PDF

Ciudad Autónoma de Buenos Aires. Estatuto del CPCI. Disponible en: http://www.cpci.org.ar/index.php/institucional/estatuto Proyecto de ley disponible en: http://www.cpci.org.ar/index.php/proyecto

Clariá Olmedo, J.A. (1966) Tratado de derecho procesal penal; EDIAR, Buenos Aires. T. V. pág. 31. - Florián, Eugenio. De las pruebas penales. trad. de Guerrero, Temis, Bogotá, 1969, T. I.

Código Penal Argentino.

Código Procesal Civil y Comercial de la Provincia de Buenos Aires.

Código Procesal Penal de la Provincia de Buenos Aires

Consejo de Profesionales de Ciencias Informáticas. Código de Ética Profesional. Versión online accesible en julio 2016: http://www.cpciba.org.ar/archivos/documentos/codigo_etica_profesional.pdf

Córdoba. Ley N° 7642/87. Disponible en: http://www.cpcipc.org.ar/quienes-somos/la-ley/

Di Iorio, A.H., Mollo, M., Cistoldi, P., Lamperti, S., Giaccaglia, M.F., Malaret, P., Vega, P., Iturriaga, J., Constanzo, B. (2016). Consideraciones para el diseño de un Laboratorio Judicial en Informática Forense". Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática (CIIDDI) 2016, Santa Fe, Universidad Nacional del Litoral (inédito).

Di Iorio, A.H. y otros. (2016) Guía integral de empleo de la informática forense en el proceso penal. 2° edición revisada, Mar del Plata, Universidad FASTA. Accesible: julio 2016. Disponible en: http://info-lab.org.ar/images/pdf/PAIF.pdf

Donna, E.A. (2000) Derecho Penal. Parte Especial.Tomo III, Rubinzal-Culzoni Editores, Bs.As. Santa Fe.

Entre Ríos. Ley N° 9498. Disponible en: http://www.coprocier.org.ar/archivos/9498-COPROCIER.pdf

Gilardi, M.; Unzaga Domínguez, G. (2007) La prueba pericial en el proceso penal de la Provincia de Buenos Aires. Publicación en la Revista Buenos Aires La Ley. Año 14 N° 7 agosto de 2007, página 719. Disponible en: http://www.scba.gov.ar/pericial/capacitacion/La%20prueba%20pericial%20en%20el%20proceso%20penal%20de%20la%20provincia%20de%20Buenos%20Aires.pdf?opcion=general

La Rioja. Ley N° 6911. http://www.cpcilar.org/wp-content/uploads/2011/06/Ley_6911.pdf

Ley 14.424. Disponible en: http://www.gob.gba.gov.ar/legislacion/legislacion/l-14424.html

Misiones. Ley N° 3752. Disponible en: http://www.diputadosmisiones.gov.ar/digesto_juridico/documentos/43.pdf

Provincia de Buenos Aires. Ley 14.424. Accesible: julio de 2016. Disponible en: http://www.gob.gba.gov.ar/legislacion/legislacion/l-14424.html

Provincia de Santa Fe. Ley 13.459. Accesible: julio de 2016. Disponible en: https://www.santafe.gov.ar/boletinoficial/recursos/boletines/27-01-2015ley13459-2015.html

Ramos, A. Historia de la ciencia forense. publicado en el sitio "Security by Default". Disponible en: http://www.securitybydefault.com/2011/02/historia-de-la-ciencia-forense.html Accesible: julio 2016.

Ramos, A. Historia de la Informática Forense. publicado en el sitio web "Security by Default". Disponible en: http://www.securitybydefault.com/2011/03/historia-de-la-informatica-forense.html Accesible: julio 2016.

Sain, G.Qué son los delitos informáticos?. Edit. Rubinzal Culzoni. RC D 875/2015

Santa Fe. La Asociación Provincial de Profesionales en Informática nuclea a los profesionales de la informática de

esta provincia quienes tienen un estatuto vigente y un proyecto de ley presentado para convertirse en un Consejo Profesional
http://www.appei.org.ar/index.php?m=ley&a=listado

Sitio web de la Asesoría Pericial dependiente de la Suprema Corte de Justicia de la Provincia de Buenos Aires. Disponible en: http://www.scba.gov.ar/pericial/ . Accesible: julio de 2016.

Sitio web del Ministerio Público Fiscal de la Provincia de Buenos Aires. Disponible en: http://www.mpba.gov.ar/web/secpoliticacriminal.php Accesible: julio de 2016.

Sitio web del Ministerio de Seguridad de la Provincia de Buenos Aires. Accesible julio de 2016. Disponible en: http://www.mseg.gba.gov.ar/migra/Policia%20Cientifica%202/cientifica.html

Sitio web del Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires. Accesible: julio de 2016. Disponible en: http://www.fiscalias.gob.ar/cij-cuerpo-de-investigacion-judicial/

Sitio web de la Procuración General de la Provincia de Buenos Aires. Accesible: julio de 2016. Disponible en: https://www.mpba.gov.ar/web/cij.php

Sitio web del Ministerio Público Fiscal de Córdoba. Accesible: julio de 2016. Disponible en: http://www.mpfcordoba.gob.ar/policia-judicial/

Sitio web: Digital Forensic Research Workshop (DFRWS). En: http://www.dfrws.org/about-us

Sitio web: High Technology Crime Investigation Association. En: https://www.htcia.org/history/

Tucumán. Ley N° 7490. Disponible en: http://rig.tucuman.gov.ar/leyes/scan/scan/L-7490-07012005.pdf

Vélez Mariconde, A. (1981) Derecho procesal penal. Lerner, Córdoba. T. I pág. 314 y T.II pág. 201.

Capítulo 5. PURI, Proceso Unificado de Recuperación de Información

Autores: Ana Haydée Di Iorio, Martín Castellote, Santiago Trigo, Juan Ignacio Iturriaga y Fernando Greco.

1. Introducción
2. Antecedentes
3. PURI. 3.1 Fases. 3.2 Actividades. 3.3 Tareas. 3.4 Técnicas y herramientas. 3.5. Niveles de actuación del Informático Forense
4. PURI: Detalle de actividades y tareas.
5. Casos. 5.1Caso I: Distribución de Pornografía Infantil. 5.2 Caso II: Defraudación Informática.
6. Conclusiones.
7. Anéxo técnico: Herramientas Complementarias.

1. Introducción

Los profesionales cuentan con capacidades y habilidades propias del ámbito del saber de su materia, sin embargo, llegado el momento de aplicar este conocimiento en una práctica forense, es necesario contar con otros conocimientos, habilidades y capacidades que no les son propios.

Es preciso entonces, que estos profesionales realicen las tareas encomendadas procurando respetar los principios forenses, que se fundan en una actuación metódica basada en un orden lógico de las tareas a realizar, en tomar los recaudos necesarios para evitar alterar el objeto original y en mantener la debida cadena de custodia.

Algunas ciencias, como las médicas, han realizado un largo camino en su aplicación forense a lo largo de los años, lo que les permite contar con protocolos de actuación, carreras de especialización y una representación en el imaginario social, que las ciencias informáticas aún no han alcanzado.

2. Antecedentes

A partir de la inserción de la tecnología en la sociedad, fue cada vez más frecuente la necesidad de recuperar información almacenada en medios digitales para su uso en el ámbito judicial.

Esto fue motivando la necesidad de elaborar guías de recomendaciones y buenas prácticas que orientaran a los profesionales en las tareas a realizar, con el fin de evitar la contaminación, es decir, la alteración del original y preservar esta información como prueba. Diversas instituciones locales y del exterior han propuesto a través de los años guías de recomendaciones y buenas prácticas, e incluso, protocolos de actuación específicos para ciertos casos.

En el año 2002 la IETF[177], formuló el RFC "*Request For Comments*" 3227, denominado "Guía para recolectar y archivar evidencia". Este documento, uno de los primeros en ser adoptados por la comunidad de informática forense, es una guía general para recolectar y almacenar información relacionada con incidentes. Propone una serie de buenas prácticas para determinar la volatilidad de los datos, decidir qué recolectar, cómo efectuar la recolección y determinar de qué manera almacenar y documentar los datos, considerando muy pocos aspectos legales, que naturalmente, son particulares del ordenamiento legal de cada país.

Durante los años 2012 al 2015, ISO[178] incorpora dentro de su línea de ISO/IEC 27000[179] una serie de normas ISO/IEC 27037:2012[180], 27041:2015[181], 27042:2015[182], 27043:2015[183] y 27050:2015[184] cuyo propósito es promover los procesos y buenas prácticas para la captura, resguardo, investigación y análisis de la evidencia digital. Estos estándares

[177] El IETF, Internet Engineering Task Force, es una organización que contribuye a la ingeniería y evolución de las tecnologías de Internet. Para obtener más información puede acceder www.ietf.org.

[178] ISO, International Standard Organization, es una organización dedicada a promover el desarrollo de normas y regulaciones internacionales para la fabricación de productos, exceptos los electrónicos.

[179] ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO e IEC (International Electrotechnical Commission) que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización.

[180] ISO/IEC 270037: Es una guía que propociona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales.

[181] ISO/IEC 27041: Es una guía para la garantizar la la idoneidad y adecuación de los métodos de investigación.

[182] ISO/IEC 27042: Es una guía con directrices para el análisis e interpretación de las evidencias digitales.

[183] ISO/IEC 27043: Desarrolla principios y procesos de investigación para la recopilación de evidencias digitales.

[184] ISO/IEC 27050: En desarrollo. Es una guía general del proceso de eDiscovery, "Descubrimiento de datos electrónicos", su adquisición, manipulación y preservación.

internacionales no pretenden contradecir ni sustituir las leyes o normativas jurisdiccionales respecto a la adquisición, tratamiento o preservación de la evidencia digital, simplemente pretenden guiar en el mejor establecimiento de estas prácticas.

Pese a constituir estándares indiscutibles, la problemática de estos documentos es que son acotados en su alcance, deben adaptarse a la normativa de un país y a la situación institucional.

3. PURI

El "Proceso Unificado de Recuperación de Información" (PURI), es el resultado de un proyecto de investigación de la facultad de ingeniería de la Universidad FASTA que comenzó en el año 2011. Su objetivo consistió en establecer una guía de las tareas a desarrollar para la prestación de un servicio de *informática forense* en un ámbito judicial o particular.

La primera versión del trabajo estuvo orientada a la recuperación de información en un equipo de escritorio. Luego fue evolucionando y transformándose de acuerdo al objeto sobre el que se realizaría su aplicación. Es así que surge una versión de PURI adaptado a Smartphones, en conjunto con la Universidad UNIANDES de Ecuador, y una versión de PURI orientada a redes y entornos distribuidos.

Estas primeras versiones de PURI se originaron bajo la definición de un proceso como un *"conjunto de fases sucesivas"*, que permiten dividir el problema, entender los objetivos de cada fase, sus particularidades y la interconexión de las mismas como un todo. De esta manera, el proceso se entiende como una serie de fases a seguir, que podría ser distinta de acuerdo al objeto origen.

Esta complejidad, llevó a elaborar una transformación de PURI en un modelo, de manera tal que el mismo pueda ser abordado en diferentes fases de acuerdo al caso origen a

resolver, y a las características del objeto sobre el que realizar las tareas forenses.

El diccionario de la real academia española define un modelo como un “esquema teórico, generalmente en forma matemática, de un sistema o de una realidad compleja que se elabora para facilitar su comprensión y el estudio de su comportamiento”. Los modelos pueden utilizarse tanto para hacer una representación fiel de un sistema existente orientado a un objeto de estudio, por ejemplo, el modelado del sistema solar; así como también para representar un sistema inexistente a fin de estudiar cómo se comportaría.

Siguiendo este lineamiento, el modelo PURI es ***un esquema[185] teórico de las tareas involucradas en la aplicación forense de las ciencias de la información***. Este esquema agrupa las tareas en actividades de mayor abstracción, y a éstas en fases. A su vez, el modelo se complementa con las técnicas para llevar a cabo cada una de esas tareas y las herramientas disponibles que ejecutan dichas técnicas.

3.1 Fases

Se entiende por **fase a cada uno de los estados sucesivos en el que puede encontrarse un proceso de recuperación de información que se ejecute sobre el modelo**.

Estas fases son sucesivas debido a que llevan un orden lógico; están compuestas por actividades, y cada una de estas actividades engloba un conjunto de tareas, las que pueden o

[185] Según el diccionario de la Real Academia Española un esquema es la representación gráfica o simbólica de cosas materiales o inmateriales. En este sentido, el modelo PURI es un esquema, dado que es una representación gráfica o simbólica de las tareas involucradas en la aplicación forense de las ciencias de la información.

no realizarse, de acuerdo al caso sobre el que trabajar y el objeto de estudio.

El modelo PURI constituye un gran conjunto de actividades y sus tareas, las que serán enhebradas en un proceso particular de acuerdo a las características del objeto origen, y el servicio a realizar.

Se presenta a continuación un gráfico explicativo de las fases que intervienen en el modelo.

Figura 5.1: Fases del modelo PURI.

Las fases iniciales de **Relevamiento** y **Recolección**, son de tipo exploratorio y es esperado que sean ejecutadas por un profesional con perfil orientado a la investigación, donde el técnico tenga un rol de asistencia y asesoramiento. En cambio, las fases subsiguientes, esto es: **Adquisición, Preparación, Extracción y Análisis**, y **Presentación**, son netamente de informática forense, y se espera que las tareas involucradas sean desarrolladas por profesionales especializados en esta temática, con la asistencia que se requiera de los "investigadores del caso".

Más allá de las preponderancias de un perfil profesional sobre otro, en cada una de las fases, se recomienda siempre el trabajo conjunto de las tres orientaciones, legal, criminalística y de informática forense, ya que, como en todo sistema, ***"el todo es más que la suma de las partes"***.

3.2 Actividades

En PURI cada fase se comprende de al menos una actividad cuyo propósito es proporcionar una guía teórica de un nivel de abstracción superior a la tarea.

Se entiende por ***actividad*** al *conjunto de tareas forenses relacionadas entre sí y agrupadas en función del objetivo que persiguen*. Las actividades, a su vez, se encuentran vinculadas de forma tal que sugieren un orden en el que podrían ser llevadas a cabo. En determinadas situaciones es posible que no sea preciso llevar a cabo todas las actividades de la fase, sino sólo algunas de ellas. A continuación se presentan algunos casos a modo de ejemplo:

- *¿Qué ocurre si una actividad de la fase no se encuadra en lo requerido? Se recurre a otra actividad dentro de la misma fase que sí corresponda realizar. Por ejemplo, en la fase de Adquisición, la actividad "Adquisición de paquetes de red" no es necesaria si sólo se debe adquirir un medio de almacenamiento de datos persistente.*

- *¿Qué ocurre si no puede realizarse una actividad? Es posible que una actividad no pueda llevarse a cabo por impedimentos legales y/o técnicos, en cuyo caso se recurre a otra actividad dentro de la misma fase que sí pueda realizarse. Por ejemplo, en la fase de adquisición, la actividad "Adquisición de datos volátiles" podría no llevarse a cabo en un allanamiento, por ejemplo, si no se contara con la correspondiente autorización judicial.*

- *¿Es preciso seguir el proceso completo? El proceso finaliza en el momento en que se obtiene el resultado esperado, en cuyo caso no hace falta continuar. Por ejemplo, en la fase de análisis se presentan tres tipos de extracciones que van aumentando en complejidad, por lo que se espera que se continúe con las tareas complejas en caso de no haberse satisfecho el requerimiento con las tareas más sencillas.*

3.3 Tareas

Una **tarea** en PURI es un *trabajo específico y atómico dentro de una actividad*. Es decir, las tareas no pueden ser divididas, y arrojan un resultado concreto. Entonces, una tarea es el eslabón más pequeño que puede ser asignado a un responsable, y sobre las que se pueden estimar todos los recursos a ser utilizados para su ejecución.

A su vez, cada tarea puede ser realizada aplicando una o varias técnicas, y estas técnicas son implementadas en distintas herramientas, las que son sugeridas en el modelo para su utilización.

Para mayor detalle se recomienda la lectura del Anexo I de este capítulo, donde se presenta el detalle de tareas y técnicas por cada fase y actividad; y el Anexo II donde se detallan algunas herramientas complementarias.

3.4 Técnicas y herramientas

En el nivel inferior del modelo, y ya a un nivel más práctico que teórico, se encuentran las técnicas y herramientas.

Conceptualmente, y desde sus orígenes, las técnicas siempre estuvieron asociadas a tareas artesanales, donde lo importante es saber “cómo” hacer algo para llegar a un objetivo, conociendo o no la explicación o fundamentación teórica de los actos.

En PURI, una técnica es un procedimiento, una serie de pasos a realizar para llevar a cabo una tarea.

En cambio, ***las herramientas son programas, aplicaciones o frameworks que implementan una o varias técnicas, y son utilizados para llevar a cabo una tarea.*** Por ejemplo, si la tarea es hacer una **imagen forense de disco**, se puede emplear la técnica de **copiar bloque por bloque** del dispositivo origen a un archivo utilizando como herramienta el **comando DD** de Debian (que implementa dicha técnica). Esto no implica que la herramienta implementa una única técnica, ni tampoco que una técnica sea exclusiva de una herramienta.

El detalle de las técnicas en el modelo tiene por objeto que el informático forense pueda discernir qué técnica utilizar para llegar a su propósito, así como, que conozca qué procedimiento sigue una determinada técnica.

Estos detalles de técnicas cobran una importancia aún mayor cuando las tareas forenses se realizan con herramientas integrales, lo que por un lado facilita la labor, pero por otro, suelen dirigir el trabajo a las técnicas que utiliza ese software en particular.

Desde PURI se procura generar una conciencia de:

- ¿Qué hacer?: se encuentra descripto en la lista de **tareas;**
- ¿Qué objetivo persiguen estas tareas?: se desprende de la agrupación lógica de las tareas en **actividades**;
- ¿En qué momento del trabajo forense se debe llevar a cabo la tarea?: está definido por la fase a la que pertenece la tarea; y por último, se procura promover el discernimiento de
- "¿Cómo hacerlo?": para el que colabora el listado de **técnicas** y las sugerencias de
- "¿Con qué hacerlo?": que son las **herramientas.**

3.5 Niveles de Actuación del Informático Forense

En la Guía Integral de Empleo de la Informática Forense en el Proceso Penal, se definen distintos niveles de conocimiento en las actuaciones informático-forenses:

- **Responsable de Identificación (RI)**: es la persona idónea para las tareas de identificación, y no necesariamente un especialista informático. Esta labor puede estar a cargo de un investigador judicial debidamente capacitado en la materia, o personal auxiliar de un Laboratorio de Inforática Forense.
- **Especialista en Recolección**: persona autorizada, entrenada y calificada para recoletar objetos físicos pasibles de tener evidencia digital. Puede necesitar el auxilio de un Especialista en Adquisición.
- **Especialista en Adquisición**: persona autorizada, entrenada y calificada para recolectar dispositivos y adquirir evidencia digital de estos, como ser imágenes de disco, volcados de memoria o red, copias lógicas, entre otros tipos de evidencia digital.
- **Especialista en Evidencia Digital**: experto que puede realizar las tareas de un Especialista en Adquisición, y además tiene conocimientos específicos, habilidades y aptitudes que le permiten manejar un amplio rango de situaciones técnicas, tales como la realización de una pericia informática.

4. PURI: Detalle de Fases, Actividades y Tareas

A continuación, se propone un recorrido teórico a través del modelo de PURI brindando una breve explicación del propósito de cada una de las seis fases junto con las actividades y tareas que las componen. En el anexo del presente capítulo, denominado *“Casos prácticos y aplicaciones del modelo PURI”*, es posible seguir este modelo

teórico con casos ejemplo que permiten trasladar el modelo a la práctica concreta de un laboratorio forense.

La ***Fase de Relevamiento*** abarca la investigación para conocer el caso e identificar los posibles objetos de interés. Esta fase puede identificarse con las labores investigativas de una investigación judicial, o con labores de "reconocimiento o exploración" en el caso de un trabajo privado no judicial.

En este sentido, debe considerarse la volatilidad de los datos y priorizar los objetos de interés. Por lo tanto, se recomienda considerar todas las situaciones y decidir en función del caso hasta qué puntos y qué tipo de dispositivos puede abarcar la Identificación/Investigación.

Las actividades que la componen son:

- **Identificación de documentación legal y técnica:** consiste en identificar toda la documentación, ya sea legal, de infraestructura, diseño, hardware, software o cualquier otra documentación relevante para conocer el caso en profundidad y poder tomar las decisiones adecuadas. Si no hay documentación sobre la cual trabajar, o no hay consideraciones legales que deban tenerse en cuenta, no es necesario profundizar en esta tarea.
- **Identificación de infraestructura IT:** consiste en identificar la infraestructura de red y/o hardware sobre la cual se va a trabajar. En investigaciones donde se involucran redes de computadoras en las que múltiples usuarios, potencialmente desde más de un dispositivo acceden a servicios, ya sea en servidores internos o externos como sistemas de computación en la nube, es muy importante identificar correctamente los objetos intervinientes para preparar adecuadamente las fases de Recolección y Adquisición. En el anexo "Casos prácticos y aplicaciones del modelo PURI" se detallan las técnicas y herramientas recomendadas de acuerdo al componente de la infraestructura a identificar.

La ***Fase de Recolección*** abarca las acciones y medidas necesarias para obtener los equipos físicos, y/o las posibles fuentes de datos, sobre los cuales se deberá trabajar posteriormente. Esto se corresponde con el acceso a la posible fuente de evidencia digital, en el caso de una investigación judicial, esto se corresponde con el "secuestro" del efecto o su "presentación espontánea" en el caso.

Las actividades que la componen son:

- **Detección de Infraestructura IT:** esta actividad se compone de tareas relacionadas con inspeccionar el lugar para detectar todos los objetos de interés para la investigación. Estas inspecciones pueden ser oculares, como también a partir del uso de técnicas y herramientas específicas, como por ejemplo, la técnica de enumeración implementada en la herramienta *nmap* para detección de servidores y dispositivos conectados a la red, el comando *dig* para la consulta de nombres de dominio, o la herramienta *Wireshark* para hacer un monitoreo de la red.
- **Recolección de objetos**: esta actividad se centra en la correcta realización de las tareas de secuestro, embalaje y transporte, a fin de garantizar la de los objetos secuestrados, así como asegurar su trazabilidad, correcta preservación y custodia. Esta actividad, denominada en el ámbito judicial "Cadena de Custodia", toma especial importancia cuando el servicio forense se realiza en un ámbito judicial, en cuyo caso se deberán seguir los protocolos, guías y/o recomendaciones vigentes.[186]

[186] Para mayor detalle respecto a los pasos a seguir en la recolección de objetos se recomienda la lectura del capítulo destinado a la "Guía integral de empleo de la informática forense en el proceso penal" que es de aplicación en el Ministerio Público de la provincia de Buenos Aires, República Argentina.

La ***Fase de Adquisición*** abarca todas las actividades en las que se obtiene la imagen forense[187] del contenido que se analizará. Esta fase puede realizarse tanto "in situ", es decir, en el lugar del hecho o durante un allanamiento, o bien en un laboratorio forense luego de haber recolectado los objetos.

Es muy importante recordar que toda la información relevante que no se tome en la fase de recolección y adquisición, tendrá que ser deducida en las fases de preparación, extracción y análisis, con un costo muy alto en lo que a tiempo y esfuerzo se refiere.

Las actividades que componen esta fase son:

- **Adquisición de datos persistentes:** consiste en realizar una imagen forense del medio de almacenamiento persistente. A modo de ejemplo se pueden mencionar: discos rígidos, CD/DVD/Blu-Ray, tarjetas de memoria y pen drive, entre otros. En el anexo que continúa este capítulo se muestra un ejemplo de su aplicación práctica. Esta actividad también contempla un paso previo a la imagen forense que es la protección contra escritura del medio de almacenamiento para evitar que los datos sean alterados en el proceso. Para garantizar esto, según disponibilidad, se pueden utilizar dispositivos que generen imágenes forenses en modo "solo lectura"; se puede utilizar el interruptor de "solo lectura" propio de los medios de almacenamiento que lo tengan incorporado o se puede hacer el bloqueo de escritura

[187] Una ***imagen forense*** es una copia exacta, sector por sector, bit a bit, de un medio de almacenamiento. De esta manera, es posible trabajar con la imagen de la misma manera que si se hiciera sobre el original. En cambio, se denomina ***copia forense*** a una copia a nivel sistema de archivos, de uno o varios archivos que constituyen la evidencia lógica, y se efectúa luego del análisis, cuando ya se ha detectado cuáles serán los datos de interés para el caso.

desde el sistema operativo antes de conectar el medio de almacenamiento.

- **Adquisición de datos volátiles:** consiste en realizar un volcado del contenido de la memoria principal en un archivo para su posterior análisis. De esta manera, se obtiene una copia del contenido de la memoria principal al momento de realizar el volcado. La importancia de esta actividad radica en que la memoria principal ofrece un panorama del estado general del dispositivo al momento de la adquisición y, además, existe información alojada en memoria principal que puede no estar replicada en otro medio de almacenamiento. Con esta adquisición se pueden llegar a obtener, por ejemplo, indicios de presencia de malware, datos de cifrado, procesos, hilos de procesos (threads), módulos, archivos, conexiones, *sockets*, entradas de registro, drivers y timers entre otros. Se considera que esta actividad puede ser realizada en paralelo con las actividades de la fase de recolección, teniendo el recaudo de no apagar el dispositivo justamente por la naturaleza volátil de estos datos.

- **Adquisición de paquetes de red:** consiste en adquirir un volcado del contenido del tráfico de red mediante la técnica de *sniffing.* La adquisición de paquetes de red se realiza generalmente en el lugar del hecho como medida de investigación, con autorización judicial, y, con frecuencia, en diferentes momentos en el tiempo. Es factible, sin embargo, que en situaciones particulares durante el análisis de un equipo se deba realizar adquisición de paquetes de red.

- **Adquisición de Smartcards:** consiste en adquirir una copia de la información contenida en algún tipo de tarjeta inteligente como por ejemplo una tarjeta SIM (subscriber identity module) comúnmente utilizada en la telefonía móvil. Esta tarea se distingue de la

adquisición de medio de almacenamiento persistente, dado que contempla técnicas y herramientas particulares, vinculadas a la o las normas de cada tipo de tarjeta inteligente.

- **Validación y resguardo:** esta actividad consiste en asignar una cadena alfanumérica como resultado de un proceso matemático conocido como *hash* (MD5, SHA-1, SHA-2, entre otros) a las imágenes forenses, y volcados de memoria capturados durante las tareas de adquisición. Ésta asegura la correspondencia entre las imágenes y los originales por medio de la teoría matemática que sustenta a las funciones de hash.

- **Transporte no supervisado:** se entiende como transporte no supervisado al acto de transportar la imagen forense sin la supervisión del "Especialista en Adquisición" o el responsable asignado. En esta situación, se recomienda el cifrado de la imagen forense previo al traslado, de manera tal de asegurar la confidencialidad del acceso a los datos.

La ***Fase de Preparación*** involucra las actividades técnicas en las que se prepara el ambiente de trabajo del informático forense, la restauración de las imágenes forenses y volcados de datos, junto con su correspondiente validación, y la selección de las herramientas y técnicas apropiadas para trabajar en la extracción y el análisis, de acuerdo al objeto origen, y a las necesidades del caso. La preparación del ambiente de trabajo adecuado es fundamental para la correcta realización de las operaciones encomendadas. Esta fase incluye las siguientes actividades:

- **Preparación de extracción:** consiste en preparar el espacio de almacenamiento en disco necesario requerido, y el entorno de trabajo para descomprimir, recomponer y validar las imágenes forenses; mapear la imagen a un dispositivo del sistema operativo, y generar las máquinas virtuales.

- **Identificación de tecnologías de la información en el objeto:** consiste en identificar la cantidad de particiones, sistemas operativos, sistemas de archivos, máquinas virtuales y medios de cifrado presentes. Una identificación correcta de estos ítems es esencial para una selección adecuada del set de técnicas y herramientas a utilizar.
- **Preparación del ambiente:** consiste en preparar en el entorno de trabajo el conjunto de técnicas y herramientas necesarias para efectuar el servicio forense encomendado.

La Fase de ***Extracción y Análisis*** comprende las tareas forenses de extracción de la información de las imágenes forenses, la selección de la potencial evidencia digital, y su análisis en relación al caso y a los puntos periciales o requerimientos de servicio forense. Con el fin de abstraer estas tareas y no vincularlas a ninguna tecnología o plataforma en particular, se separa en tres niveles teóricos: Extracción a nivel de Aplicación, Extracción a nivel de Plataforma y Extracción a bajo nivel. Esta clasificación es simple y permite separar adecuadamente las actividades específicas de acuerdo al objeto de análisis y su dependencia con técnicas y herramientas particulares.

Se distingue la ***extracción*** del ***análisis*** en la descripción del nombre de la fase, ya que son dos labores independientes que se realizan en conjunto y están íntimamente ligadas entre sí. Por un lado, está el proceso de extraer datos de las posibles fuentes de evidencia digital y por otro lado, el análisis particular de acuerdo al caso que debe realizarse sobre los datos extraídos. De esta manera, por ejemplo, una labor de extracción sería la *búsqueda y extracción de archivos de tipo imagen*, mientras que el análisis implica el estudio de cada una de ellas a fin de separar las imágenes requeridas en el caso. La extracción suele ser automatizada, e integrada por actividades netamente técnicas, mientras que el análisis

implica un proceso de interpretación de los datos extraídos en el contexto de los puntos periciales y el interés de los investigadores. Esta fase se compone de las siguientes actividades:

- **Extracción a nivel de aplicación:** consiste en la búsqueda y extracción de datos a nivel de aplicación. Esta actividad requiere un conocimiento apropiado de todas las aplicaciones instaladas en el equipo sobre el que se realiza la labor forense a fin de lograr obtener información de uso de las mismas, archivos abiertos, historiales, registros de auditoríay archivos de datos, entre otros. El objetivo es conocer la actividad de las aplicaciones con el mayor grado posible de detalle en la medida que resulte relevante para el caso. A modo de ejemplo se puede mencionar la búsqueda y extracción de mensajes en aplicaciones de mensajería instantánea, donde, más allá de las habilidades forenses típicas, es requerido el conocimiento específico de la aplicación de la cual es requerido extraer los mensajes.

- **Extracción a nivel de plataforma:** consiste en la búsqueda y extracción de información de la plataforma, lo que incluye los sistemas operativos, sistemas de archivos, y su configuración. Esta actividad es de un nivel de detalle más específico que la extracción a nivel de aplicación, y también permite un análisis más completo del entorno de uso del equipo. Las tareas incluidas en esta actividad requieren del informático forense habilidades y conocimientos particulares del sistema operativo y sistemas de archivos del equipo sobre el que se realiza el trabajo. A modo de ejemplo se puede mencionar la extracción de información del registro del sistema operativo para reconstruir la actividad de un usuario en el equipo, o la recuperación de archivos eliminados, entre otros.

- **Extracción a bajo nivel:** en esta actividad se concentran las tareas de recuperación de información lógica al nivel más bajo de abstracción, es decir, a nivel bloque de datos puro, excluyendo el sistema operativo. Incluye tareas directas sobre los bloques de datos, tales como la búsqueda de información por medio de expresiones o en bases de datos en particiones sin formato, entre otros. Toda tarea donde se esté trabajando a un nivel inferior al sistema operativo y sus mecanismos es considerada de bajo nivel.
- **Análisis de contenidos:** incluye el conjunto de tareas de alto nivel que implican un análisis del contenido, la información propiamente dicha que se almacena en los datos extraídos en las tareas anteriormente mencionadas.
- **Análisis de relaciones:** incluye el conjunto de tareas de alto nivel que implican el análisis de las relaciones entre los distintos elementos extraídos, el contenido recuperado y los elementos previos aportados, con el fin de encontrar su peso, relevancia y significancia en el caso.

Es importante destacar que las actividades de análisis de contenidos y análisis de relaciones tiene la particularidad de extenderse a lo largo de todo el proceso, y está ceñido a las habilidades intrínsecas del forense de vinculación de los datos obtenidos, características de los objetos, y particularidades que le permitan brindar una respuesta integral y objetiva a los puntos consultados.

Finalmente, la **Fase de Presentación** comprende el armado de los informes necesarios y la presentación del caso en un juicio o a los solicitantes. Las actividades involucradas son:

- **Armado del Informe:** implica la documentación de todas las actividades y tareas realizadas en un informe pericial que sea claro, preciso, concreto y redactado en un lenguaje apropiado, lo que implica, un lenguaje técnico-científico comprensible para una autoridad judicial. Se espera que en este informe se respondan los puntos solicitados con un nivel de detalle de operaciones tal que permita reproducir y replicar el proceso de análisis llevado a cabo por el cual se arriba a esa conclusión.
- **Preparación de la Información a Presentar**: consiste en la preparación de la información y la evidencia digital hallada en el caso para una eventual presentación, ya sea en juicio o a los solicitantes del servicio forense. En ocasiones es posible que el informático forense deba realizar una exposición donde explique el trabajo realizado, además del informe escrito correspondiente.

Se presenta a continuación un gráfico explicativo de las actividades incluidas en el modelo.

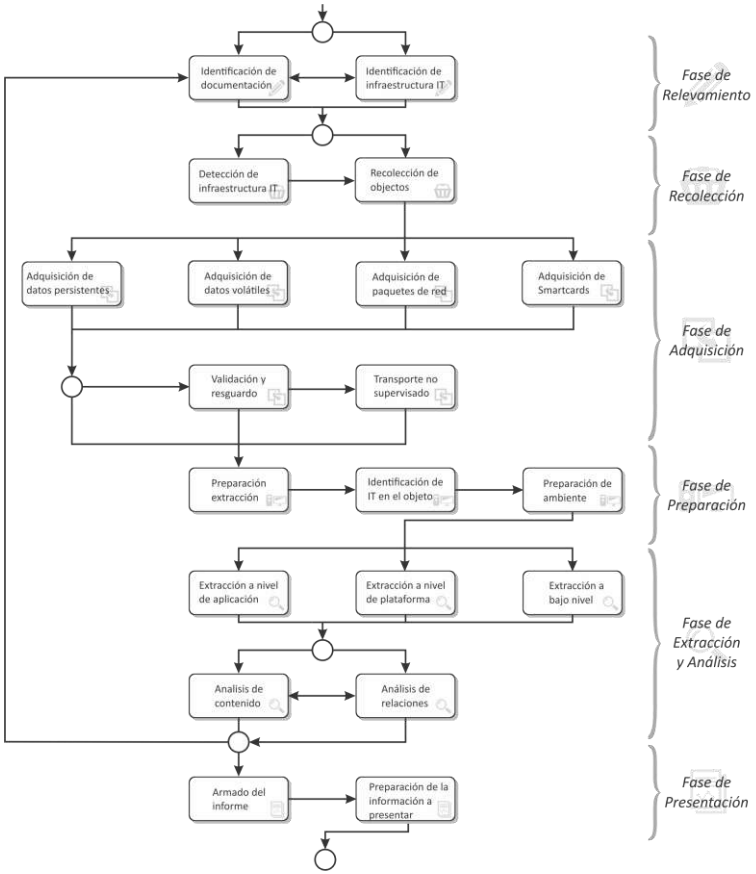


Figura 5.2: Detalle de actividades de PURI.

5. Casos Prácticos

A fin de demostrar la aplicación del modelo PURI, se presenta a continuación dos casos ilustrativos basados en hechos reales. En esta sección se describirán las fases, actividades, tareas, técnicas y herramientas del Modelo PURI de acuerdo al caso práctico a desarrollar, considerando los pasos legales que están enmarcados en la normativa procesal vigente de la Provincia de Buenos Aires, por lo que podrían

surgir algunas diferencias en el caso de aplicar una legislación distinta.

5.1 Caso I "Distribución de archivos con contenido pornográfico y explotación sexual de menores"

Generalmente este tipo de delitos parte de una investigación previa realizada por la **NCMEC**[188] quien deriva dicha investigación al país que corresponda según dónde se cometió el delito. Dicho reporte de la investigación contiene generalmente mails de los usuarios que compartieron fotos o videos a una determinada red social, como Facebook, G+, Flickr, etc.; como así también las direcciones IP[189] desde donde surgieron dichas acciones y los archivos compartidos propiamente dichos.

Fase de Relevamiento

Según el caso a estudiar en este ejemplo, es la fiscalía actuante la que determina en esta fase las actividades a realizar. Es posible que pida asistencia o asesoramiento al Perito Informático, pero son actividades exclusivas de la fiscalía. Las más importantes son:

I. <u>Identificación de Documentación Legal y Técnica</u>

Consiste en leer detenidamente los informes que la NCMEC realizó para poder determinar específicamente las acciones que deberán llevarse a cabo. Se debe prestar atención en esta actividad a los usuarios, mails, redes sociales, servidores y direcciones IP que fueron informados para luego poder establecer adecuadamente las tareas a

[188] *National Center for Missing & Exploited Children*® (Centro Nacional para Menores Desaparecidos y Explotados) se fundó en EEUU en 1984 para servir como centro de información en problemas relacionados con los menores desaparecidos y sexualmente explotados.

[189] Dirección IP: dirección de 4 bytes (32 bits) o 64 bits, que representa a un equipo en una red IP (Internet Protocol) por ej.: 194.128.12.6.

realizar en la actividad de Identificación de Infraestructura IT que se detallará a continuación.

II. Identificación de Infraestructura IT

De acuerdo a lo identificado en la actividad anterior las tareas a llevar a cabo son las siguientes:

1. Determinar el **ISP** (Proveedor de Servicios de Internet) de las direcciones IP informadas por el NCMEC. Para esto, el responsable de la causa se dirige al sitio de **LACNIC**[190] (*https://rdap.lacnic.net/rdap-web/home*) para direcciones IP pertenecientes a Latinoamérica.
2. Una vez obtenido el nombre del proveedor de la o las direcciones IP, dicho responsable, envía un oficio judicial de la fiscalía actuante al ISP para determinar el domicilio de la cuenta a la que fue asignada la/s dirección/es IP investigadas. Se debe considerar que las direcciones IP son asignadas de manera dinámica a los clientes, es decir, a demanda según sean solicitadas. Por lo tanto, un usuario no necesariamente siempre se le va a asignar la misma dirección IP al momento de conectarse a Internet. El investigador responsable, libra un oficio detallando al ISP fecha, hora y huso horario por la cual se necesita determinar el domicilio del usuario que tenía esa IP para ese momento determinado.
3. Una vez obtenido el domicilio se constata su existencia. Para eso miembros de la fiscalía, se

[190] LACNIC, el Registro de Direcciones de Internet para América Latina y Caribe, es una organización no gubernamental internacional establecida en Uruguay en el año 2002. Es responsable de la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), Números Autónomos y Resolución Inversa, entre otros recursos para la región de América Latina y el Caribe. Es uno de los 5 Registros Regionales de Internet en el mundo.

dirigen al domicilio y obtienen fotos de la fachada del inmueble constatando así su existencia, o bien pueden utilizar sistemas informáticos como **Google Street View.**

4. Por último, se solicita al Juez de Garantías que interviene en el caso, el allanamiento del domicilio para secuestrar los dispositivos electrónicos/informáticos y realizar las medidas que se consideren necesarias. Para este caso en particular, en el pedido se deben detallar las siguientes medidas:

   - Secuestro de computadoras (de escritorio o notebooks).
   - Secuestro de celulares o tabletas.
   - Secuestro de dispositivos de almacenamiento extraíble (memorias SD, Micro SD, pendrives, reproductores de tipo MP3 o MP4, etc.).
   - Secuestro de cámaras de fotos digitales. Son fundamentales para poder establecer si las imágenes que se buscarán posteriormente en la Fase de Extracción y Análisis fueron tomadas con alguna de las cámaras secuestradas.
   - Volcado de Memoria Principal. Puede ser determinante para poder establecer si al momento del allanamiento se estuvo utilizando alguno de los mails reportados por NCMEC, o la utilización de programas para compartir archivos.
   - Enumeración de dispositivos informáticos en la red mediante herramientas informáticas. Si el domicilio en el que se realizará el procedimiento judicial es una empresa o un domicilio el cual se presume que consta de muchos equipos, es posible utilizar alguna herramienta para enumerar dispositivos conectados a una red de computadoras. En la

siguiente fase, se explicará cuál es esta herramienta y el uso de la misma.

Aclaración: es de suma importancia que en la solicitud de allanamiento al Juez de Garantías se enumere detalladamente el material a secuestrar y las medidas que requieren dicha diligencia, ya que el Juez autorizará el pedido que hace la fiscalía y no agregará algún dispositivo electrónico/informático o medida netamente informática que considere faltante en el pedido. Toda medida o secuestro que en la orden de allanamiento librada por el Juez no esté determinada, no podrá llevarse a cabo.

Fase de Recolección

Cuando el ***especialista en recolección (ER)***, llega al lugar del allanamiento, debe tener pleno conocimiento de las medidas que el juez de garantías autorizó a realizar en dicha diligencia. Se debe leer muy bien el acta de allanamiento y acatarse sólo a secuestrar o llevar a cabo las actividades que estén explícitamente detalladas en ella:

I. <u>Detección de Infraestructura IT</u>

- Si se constata que el domicilio del allanamiento posee muchos dispositivos conectados a una red de computadoras y la orden autoriza la utilización de alguna herramienta informática para enumerar dichos dispositivos, es posible utilizar una herramienta muy útil que se llama **NMAP[191].** Dicha herramienta debe estar instalada en una notebook o dispositivo del ER y de ninguna manera debe ser instalada y utilizada en alguna de las computadoras que se encuentren en el

[191] Nmap ("mapeador de redes") es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales.

lugar. Los pasos para la utilización de la misma son los siguientes:

a) Como primera medida se debe conectar la notebook o dispositivo del ER a la red de computadoras del lugar. Puede ser de 2 formas:
   i. Mediante un cable de Red conectándolo a uno de los switches del lugar.
   ii. Mediante Wifi del lugar si posee. Este caso es el menos recomendable ya que si la red Wifi posee clave de acceso, debe solicitarse la misma a alguna de las personas del domicilio quedando a la buena voluntad de las mismas el acceso a la red. Además, no siempre desde la red Wifi se pueden llegar a enumerar todos los dispositivos conectados a la misma, esto dependiendo de cómo esté configurada. Es por esta razón que, en la medida de lo posible, se recomienda la conexión de la notebook o dispositivo del ER a la red mediante un cable.

b) Una vez realizado el punto anterior, el ER identifica cuál es el rango de IP que fue asignado. Para eso sólo basta ver en las propiedades del dispositivo de red que se está utilizando cuál es la IP que fue asignada. Se supone de ahora en adelante que para este caso se asignó la IP *192.168.1.15*.

c) Luego, el ER, procede a ejecutar la herramienta NMAP. El uso de la misma es muy sencillo y puede ejecutarse mediante la interfaz gráfica o mediante línea de comandos. En una consola se ejecuta el comando *nmap 192.168.1.**. Donde el "*" especifica que se enumeren todos los equipos conectados a la red de computadoras en la cual se está conectado. Como salida de dicha herramienta

se obtiene la cantidad de equipos conectados a la red de computadoras. Cabe destacar que la herramienta utilizada y de la forma que es explicada no implica una intrusión a la red que está siendo analizada. Este uso es meramente informativo y sirve para enumerar equipos, los mismos no se ven afectados de ninguna manera.

- Una vez enumerados los equipos a secuestrar mediante el uso de la herramienta antes descripta o mediante la inspección ocular, el ER procede a identificarlos y separarlos teniendo en cuenta lo especificado en la orden de allanamiento. Las tareas a realizar en este momento son:

  a) Si se debe hacer un volcado de memoria principal de uno o varios equipos del lugar, primero se identifica él o los equipos y se realizan las siguientes acciones siempre con la presencia de un testigo para que éste controle que el ER no cometa irregularidades:

     i. Una vez identificada la computadora, el ER procede a utilizar la herramienta **FTK Imager Lite** para hacer un volcado de memoria principal. Dicha herramienta se ejecuta de manera portable y debe estar en algún medio de almacenamiento masivo extraíble del ER, como un pendrive, para ser ejecutada desde allí.

        Este es un caso especial donde la *Fase de Recolección y Adquisición* están solapadas y se denomina *Fase de Adquisición in situ*.

     ii. Una vez ejecutada la herramienta, el ER se dispone a abrir el módulo de volcado de memoria principal y ejecutarlo. Es recomendable que, además, se descargue el

archivo de paginación e hibernación de la computadora para contar con más información en el momento del análisis. Se debe especificar que el archivo con el volcado de memoria principal se almacene en un medio de almacenamiento extraíble del ER, bajo ningún motivo debe almacenarse en el disco de la computadora a peritar.

iii. Detallar el tamaño y nombre del archivo y ejecutar una función de *hash*, por ejemplo MD5 o SHA-1, a fin de dejar constancia por escrito en el acta de secuestro del resultado obtenido. Esta acción permite que luego, de ser necesario, sea posible verificar el valor de *hash y* garantizar que los archivos no hayan sufrido cambio alguno. Para este ejemplo se simula la obtención de un archivo de volcado de memoria principal denominado *"dump4GB.001".* Cabe destacar que la Fase de Recolección y la Fase de Extracción y Análisis, pueden estar muy distantes en el tiempo, por lo que se deben tomar todas las medidas necesarias para garantizar el correcto resguardo de toda la evidencia secuestrada, así como su persistencia.

b) Luego se procede a desconectar todas las computadoras que se crean necesarias secuestrar. Para eso se deben tener las siguientes consideraciones:

i. Siempre realizar dicha medida mediante la presencia de un testigo.

ii. No se debe seguir el modo tradicional o de correcto apagado de la computadora si se encuentra encendida.

- Si es una computadora de escritorio se debe desconectar su cable de alimentación eléctrica.
- Si es una notebook o dispositivo portátil, se debe desconectar el cable de alimentación eléctrica, si lo posee conectado, y luego extraer su batería.

Esta tarea es fundamental ya que si se apaga correctamente una computadora se perdería información de suma importancia como es el archivo de paginación o hibernación, o se podrían disparar procesos de eliminación de información pre-configurados.

Identificar y separar los demás dispositivos electrónicos/informáticos detallados en el Acta de Allanamiento.

Es recomendable rotular cada dispositivo con un número o identificación.

II. Recolección de Objetos

Esta actividad se centra en la realización correcta de las tareas de secuestro, embalaje y transporte adecuadas, tal como se describe en el capítulo 3, sección 2.8 “Recolección de evidencia, cadena de custodia”.

Por otra parte en el acta de allanamiento que se realice en el lugar deberá hacerse constar todas y cada una de las operaciones realizadas, y así como el detalle de lo secuestrado y el correcto inicio del procedimiento de cadena de custodia, todo ello siempre en presencia de testigos hábiles tal como lo impone el Código de Procedimiento Penal.

Fase de Adquisición

Una vez finalizada la fase de Recolección, la fiscalía actuante solicita al director del laboratorio, encargado y/o al ***Especialista en Adquisición (EA)*** que determine una fecha y hora de inicio de pericia, la que se notifica a las partes intervinientes.

El día del inicio de pericia se debe comenzar el acto cuando todas las partes notificadas se encuentren presentes. Si alguna o todas las partes no concurren, se espera un lapso de tiempo no menor a 30 minutos, y se da comienzo a la diligencia, detallando en el acta las partes presentes.

Cabe destacar que de aquí en adelante, las fases, actividades y tareas descritas son realizadas dentro del laboratorio pericial excepto el caso especial de “Adquisición in situ” detallado anteriormente.

Previo a iniciar las tareas de Adquisición, se debe tomar el recaudo de identificar todos los equipos o dispositivos electrónicos/informáticos que fueron recibidos por la oficina, por lo que es preciso realizar las siguientes acciones:

1. Tomar fotos de cómo se reciben los elementos a peritar y enumerarlos de alguna manera. Por ejemplo si se recibe un gabinete de computadora, enumerarlo como *GA-1,* donde “GA” describe a la palabra “gabinete” y “1” al orden en que se va a peritar. Si hay más de un gabinete se enumerarían como *GA-1, GA-2,* y así sucesivamente. Luego identificar marca, modelo y número de serie de cada uno de estos equipos si lo poseen.
2. Como segundo paso, debe buscarse dentro de cada uno de los equipos identificados en el paso anterior, los medios de almacenamiento persistente que posean como discos rígidos, discos SSD, u otros. Enumerarlos como se hizo con los equipos en el paso 1, es decir, para cada medio de almacenamiento persistente identificarlo con un nombre seguido de un

número, marca, modelo, número de serie y capacidad de almacenamiento.

3. Repetir el paso 2 para todos aquellos dispositivos electrónicos/informáticos que se encuentren dentro de los elementos a peritar pero no contenidos en un gabinete o estructura (por ej. pendrives, tarjetas SD, reproductores MP3, cámaras digitales, etc.).

Una vez identificados debidamente los dispositivos se dispone a realizar las actividades específicas de la obtención de las imágenes forenses:

III. Adquisición de Datos de Medios de Almacenamiento Persistente

Es fundamental que cuando el EA realice este tipo de actividad, cuente con un entorno adecuadamente preparado y controlado para llevarla a cabo. Para este caso de ejemplo, se cuenta con computadoras clonadoras, que son aquellas encargadas de realizar las imágenes forenses, bajo un entorno *Debian "Jessie" Linux* y computadoras clonadoras bajo entorno *Microsoft Windows 8.1.* Para la adquisición de discos rígidos, se utilizarán las computadoras bajo entorno Debian "Jessie" y para la adquisición de medios de almacenamiento persistente extraíble se utilizarán las computadoras bajo entorno Microsoft Windows 8.1. Cabe aclarar que se utilizarán dos entornos diferentes con el fin de explicar dos formas de realizar la misma actividad, sin embargo, se aconseja adoptar un único tipo de entorno. Mientras más computadoras se asignen a esta actividad, más factible será paralelizarla y de esta manera reducir el tiempo que es un factor fundamental en el actuar del EA.

Para la adquisición de discos rígidos se supone que se cuenta con un disco rígido identificado como *"HD-1"* cuya capacidad de almacenamiento es de 500GB*.* Para esta actividad el EA realiza las siguientes tareas:

a) Conecta el disco rígido “HD-1” con la computadora clonadora apagada en algún puerto SATA/IDE, según corresponda, disponible de la misma.
b) Enciende la computadora y accede al BIOS de la misma para verificar que la computadora no intente arrancar con el sistema operativo contenido en el disco rígido a realizar la imagen forense. Si esto sucede, el disco rígido se modifica, con lo cual, se altera la evidencia.
c) El sistema debe estar configurado para no montar el dispositivo que debe peritarse automáticamente, para evitar que lo contamine en el proceso y asegurar luego el montado en modo sólo lectura.
d) Verifica qué nombre le asignó el sistema operativo al disco rígido dentro del directorio “/dev”. Para este ejemplo se utilizará el nombre “sda”.
e) Utiliza la herramienta DC3DD, que es la que realiza la copia bit a bit del disco rígido a un archivo de imagen forense. El EA abre una consola del sistema operativo y ejecuta el comando de esta manera: dc3dd if=/dev/sdb hof=/media/IMAGENES/HD-1-500GB.dd hash=sha1 hlog=/media/IMAGENES/HD-1-500GBLOG.log bfsz=10M donde:

- *if*=inputfile. En este caso sería el disco rígido a realizarle la imagen forense
- *hof*= outputfile. Directorio donde se almacenará la imagen forense con cálculo de hash.
- *hash*=función de hash a aplicar. Se utiliza SHA1
- *hlog*= archivo de log del proceso. Además este comando hace la verificación de hashes de inputfile con outputfile.
- *bfsz*= tamaño del buffer de escritura en MEGAS. Esta ventana o tamaño tiene mucho que ver con la arquitectura con la que se cuente. Para este caso, se cuenta con **puertos SATA II y el tamaño** 10Megas

es el que mejor se adapta para un óptimo rendimiento. Si se quieren copiar discos IDE el tamaño debe ser menor y si la arquitectura soporta SATA III, el tamaño debería aumentarse. Si se elige un tamaño no adecuado se ve afectado proporcionalmente el rendimiento de la herramienta.

f) Si no se utilizan las opciones *hof, hash* y *hlog* del dc3dd, o si se utiliza otra herramienta, es necesario que una vez terminada la copia, el EA verifique que el inputfile y output file tengan el mismo valor de HASH y detalla en el Acta de pericia el nombre del archivo de imagen forense y su respectivo valor de HASH.

IV. Adquisición de Datos de Medios de Almacenamiento Persistente Extraíble

Se cuenta con una tarjeta de memoria SD identificada como *"SD-1"* cuya capacidad de almacenamiento es de 4GB. Para esta actividad, el EA realiza las siguientes tareas:

a) Como primera medida, se anula en el sistema operativo, en este caso Microsoft Windows 8.1, la escritura para los medios de almacenamiento extraíbles. Esto hará que cuando conecte la tarjeta de memoria SD, no se modifique y se altere la evidencia.

b) Una vez establecido y verificado el paso anterior, se conecta la SD identificada como *"SD-1"* en el lector de tarjetas y ejecuta la herramienta **FTK Imager.** El EA selecciona la opción de crear una nueva imagen, luego selecciona el disco físico que es la tarjeta SD que se ha insertado y luego selecciona la opción de verificación de HASH. Como salida de esta operación, se obtiene una imagen forense denominada "*SD-1-4GB.001".*

c) Una vez terminada la copia, verifica que el inputfile y outputfile tengan el mismo valor de HASH y detalla en

el Acta de pericia el nombre del archivo de imagen forense y su respectivo valor de HASH.

V. Adquisición de Datos Volátiles

Esta actividad fue realizada “in situ” en la Fase de Recolección por el ER y obtuvo una imagen forense cuyo nombre fue *“dump4GB.001”* y su respectivo valor de HASH. El EA detalla esta información en el Acta Pericial.

VI. Validación y Resguardo

Esta actividad fue realizada en el mismo proceso de adquisición, ya que la herramienta utilizada (*DC3DD y FTK Imager)* permite dicho proceso solapado.

Fase de Preparación

Para esta Fase se detallarán las actividades a realizar según las imágenes forenses adquiridas en las fases anteriores. Como se dijo anteriormente, el EA obtuvo una imagen forense denominada *“HD-1-500GB.dd”* correspondiente al disco rígido; una imagen forense denominada *“SD-1-4GB.001”* correspondiente a la tarjeta SD; una imagen forense denominada *“dump4GB.001”* correspondiente al volcado de memoria principal realizado en la Fase de Recolección y la cámara digital denominada “*CAM-1”* correspondiente a la cámara digital obtenida también en la Fase de Recolección. Las actividades principales para esta fase y caso particular son las siguientes:

I. Preparación de extracción

Para las fases siguientes a la preparación es fundamental contar principalmente con 3 discos rígidos en la máquina de trabajo, donde uno es el que aloja el sistema operativo y las herramientas a utilizar posteriormente en la máquina de trabajo; el otro aloja las imágenes forenses y el

último almacena toda evidencia digital que se obtenga en la Fase de Extracción y Análisis. Se sugiere tener en cuenta ciertos aspectos técnicos en esta actividad:

- Se debe trabajar con copias de las imágenes forenses y nunca utilizar una única imagen forense para analizar. Esto es importante, a fin de preservar una copia intacta para presentación en el juicio.
- Se debe realizar la copia de la imagen forense al disco rígido de la máquina de trabajo, y luego de finalizada ésta copia, ejecutar la función de HASH a la copia para compararla con la original y así verificar que no hubo alteraciones en el proceso de copia.
- Se debe constatar que el disco que aloje la evidencia digital disponga, por lo menos, de la misma capacidad disponible que la suma de todas las imágenes forenses a analizar. Para este caso en particular en el cual se cuenta con una imagen de 500 GB, dos de 4GB, es recomendable que este disco rígido cuente con al menos 550 GB de capacidad disponible de almacenamiento.
- Los discos rígidos donde se alojarán las imágenes forenses y dónde se almacenará la evidencia digital, es conveniente que se encuentren conectados internamente en la computadora de trabajo y no de manera extraíble como discos externos, etc. Esto beneficia notablemente el tiempo que insumen las actividades de la fase de Extracción y Análisis.

II. Preparación del ambiente

Esta actividad está fuertemente relacionada con los puntos periciales que la fiscalía encomienda al Perito Informático. Los puntos periciales para este caso son los siguientes:

A. Verificar en la totalidad de los equipos incautados la existencia de archivos con representaciones de menores de edad manteniendo relaciones sexuales, llamándose tales archivos: I. xxxx.jpg, II. xxxxxx.jpg, III. xxxx.jpg
B. Determinar si en la totalidad de los elementos secuestrados se almacenan otros archivos donde se hallen imágenes o videos donde se representen menores de 18 años de edad dedicados a actividades sexuales explícitas o en toda otra representación de sus partes genitales con fines predominantemente sexuales.
C. Determinar si en las computadoras, como así también en los discos rígidos y todo otro dispositivo incautado que le permitiese, se encuentran enlaces, historiales, etc. referidos a la creación, mantenimiento y utilización de cuentas de correo de GMAIL como así también del servicio de la red social Google+ (conocida como Google Plus).
D. Llevar a cabo toda experticia técnica/informática que sea conducente para el esclarecimiento de los ilícitos que aquí se investigan.
E. Se deberá tener en cuenta que, conforme lo resuelto por el Sr. Juez de Garantías interviniente, el personal que se abocará a la tarea pericial se encuentra facultado a levantar rastros comunicacionales de índole privados.

Para el caso a tratar se utilizarán las siguientes tareas, técnicas y herramientas:

- Utilización de bases de hashes del ***"Proyecto VIC[192]".***
- Búsqueda por hashes: por un lado se intentará identificar las fotos y videos que fueron reportadas por NCMEC dentro de las imágenes forenses y por el otro se tratará de identificar todas las restantes fotos y videos que se encuentren dentro de las bases de hashes del Proyecto VIC.
- Búsqueda por palabra: se intentará buscar si existe algún indicio para determinar si los mails o usuarios informados por NCMEC se encuentran en las imágenes forenses.
- Utilización del algoritmo ***"PhotoDNA[193]"***: es fundamental el uso de este algoritmo para identificar imágenes iguales cuando, por ejemplo, las mismas son de diferente tamaño.
- Búsqueda de archivos eliminados.
- Búsqueda por metadatos de archivos.
- Búsqueda de historial web.
- Búsqueda de URLs visitadas.
- Búsqueda de imágenes y videos descargadas de redes sociales.

---

[192] Proyecto VIC (Video Image Classification Standard) tiene por objetivo crear un ecosistema de intercambio de información y datos entre organismos internacionales encargados de combatir los delitos contra los niños y su explotación sexual. Reúne empresas privadas, entes gubernamentales e instituciones que colaboran en el propósito de combatir la explotación de los niños. Mantiene bases de datos de hashes, disponibles para agencias gubernamentales, que sirven para identificar rápidamente imágenes vinculadas con delitos que afectan su integridad.

[193] PhotoDNA es un algoritmo de *hashing* visual desarrollado por Microsoft, resistente a las modificaciones visuales, que permite identificar imágenes sin necesidad de visualizarlas.

- Utilización de ***"hashmyfiles"***: Herramienta que calcula el valor HASH de un archivo. Esta herramienta se utiliza para calcular los valores hash de las imágenes y videos reportadas por NCMEC.

- Utilización de ***"Autopsy"***: Herramienta ***"de código abierto[194]"*** multiplataforma que es utilizada para el análisis de forensia digital que engloba la mayoría de las tareas antes mencionadas. En esta herramienta se deben crear las bases de datos con los valores de los hashes de las imágenes y videos reportadas por NCMEC y los valores de hashes del Proyecto VIC.

- Utilización de "***Recuva***": Herramienta gratuita para recuperar archivos borrados dentro del sistema de archivos.

- Utilización de **"bulk_extractor**": herramienta de forensia digital de código abierto multiplataforma que escanea una imagen de disco, un archivo o un directorio de archivos y extrae información útil sin necesidad de analizar las estructuras del sistema de archivos o el sistema de archivos. Es muy útil para encontrar las cadenas de mails o usuarios reportados por NCMEC.

- Utilización de ***"Volatility":*** para análisis forense de memoria principal[195].

---

[194] El software de código abierto (en inglés Open Source Software u OSS) es aquel cuyo código fuente, y otros derechos que normalmente son exclusivos para quienes poseen los derechos de autor, son publicados bajo una licencia compatible con la Open Source Definition o forman parte del dominio público. Esto permite a los usuarios utilizar, cambiar, mejorar el software y re-distribuirlo, ya sea en su forma modificada o en su forma original.

[195] Véase capítulo 9 "Análisis Forense de memoria principal" para obtener mayor información sobre estructuras contenidas en memoria.

- Utilización de ***"Photorec"***: para realizar file carving de imagen forense. La técnica de file carving es mayormente utilizada como último recurso, pero para este caso en particular, se la utiliza debido a que es necesario recolectar todo tipo de material pornográfico infantil, en busca de imágenes o videos que fueron compartidas a otros usuarios reportados por NCMEC.
- Utilización de ***"Griffeye Analyze DI":*** es una plataforma capaz de analizar grandes volúmenes de datos para la recolección, procesamiento, análisis, visualización y gestión de imágenes y vídeos. Esta herramienta implementa el algoritmo PhotoDNA. En esta herramienta se deben crear las bases de datos con los valores de los hashes de las imágenes y videos reportadas por NCMEC y los valores de hashes del Proyecto VIC.

Fase de Extracción y Análisis

A continuación, se describirán las actividades a realizar propiamente dichas para el caso de estudio.

I. Extracción a nivel de aplicación

Para esta actividad el ***Especialista en Evidencia Digital (EED)*** utiliza dos herramientas específicas que engloban diferentes tareas:

- Extracción y Análisis con Autopsy: Primeramente, se debe indicar a la herramienta las imágenes forenses a realizar la extracción y luego indicar las tareas a realizar. Las mismas son:
  - Extracción de imágenes y videos según las bases de datos de hashes descritas en la fase anterior. Con las bases de datos ya cargadas en la herramienta, ésta busca todas las imágenes y videos contenidos en las imágenes forenses que coincidan con dichas bases datos. Cuando la herramienta encuentra alguna

coincidencia, la etiqueta según la base de datos que haya sido producto de esa coincidencia.

- Extracción de metadatos de imágenes y videos.
- Extracción de URLs visitadas, historial web y todo tipo de información resultante de la navegación web: Autopsy posee técnicas para extraer dicha evidencia digital sin la necesidad de realizar la extracción manualmente.

- La otra herramienta es Griffeye Analyze DI. Esta herramienta es más potente en cuanto a rendimiento y extracción que Autopsy, ya que se enfoca únicamente en la extracción de evidencia digital referida a imágenes y videos. Al igual que con Autopsy se le debe especificar las imágenes forenses a realizar la extracción y luego indicar las tareas. Las mismas son:
  - Algoritmo PhotoDNA: utilizada para identificar evidencia digital con respecto a imágenes que visualmente sean iguales sin la necesidad de realizar una identificación manual.
  - Extracción de imágenes y videos según las bases de datos de hashes descritas en la fase anterior: con las bases de datos ya cargadas en la herramienta, ésta busca todas las imágenes y videos contenidos en las imágenes forenses que coincidan con dichas bases datos. Cuando la herramienta encuentra alguna coincidencia, la etiqueta según la base de datos que haya sido producto de esa coincidencia.
  - Extracción de metadatos de imágenes y videos.
  - Extracción de imágenes y videos provenientes desde redes sociales: es una tarea útil para poder identificar posibles víctimas del delito en cuestión. Dicha evidencia digital es etiqueta y la herramienta especifica de qué red social proviene dicha evidencia.

Es importante que toda nueva evidencia digital sea almacenada en una base de datos propia del laboratorio forense con su valor de HASH y número de causa a la cual pertenece. Será de utilidad posteriormente en la actividad de *Análisis de relaciones.*

II. Extracción a nivel plataforma

Para este caso se utiliza alguna herramienta de recuperación de archivos eliminados como puede ser ***Recuva***. La tarea principal es la extracción de archivos eliminados dentro del sistema de archivos para luego poder identificar, mediante Autopsy, si éstos representan evidencia digital que corresponda con alguna de las bases de datos de hashes antes descritas.

III. Extracción a bajo nivel

Para esta actividad se utilizan dos herramientas específicas:

- Una de las herramientas es bulk_extractor: con esta herramienta se extrae evidencia digital que demuestre el uso o existencia de los mails o usuarios reportados por NCMEC. Su uso es muy sencillo sólo basta con especificarle la imagen forense a realizar la extracción y el archivo dónde generará el reporte de dicha extracción. Por ejemplo: *bulk_extractor.exe -o <directoriodelReporte> <archivoaEscanear>* donde:
  - -o= directorio dónde se almacena el archivo de reporte;
  - <archivoaEscanear>= es la imagen forense a realizar la extracción. Para este ejemplo sería *HD-1-500GB.dd.*

  Luego con el visor del bulk_extractor se analizarán los datos extraídos.
- Photorec: su uso es muy simple, dado que es una herramienta portable. Se ejecuta, se especifica el disco

en el que se realizará el file carving y la ubicación donde se almacenarán los archivos recuperados.

V. Análisis de contenidos

Esta actividad consiste en analizar toda la evidencia digital extraída en las actividades anteriores y determinar qué evidencia digital será considerada y cuál otra será descartada:

- Se analizan todas las evidencias digitales etiquetadas en las bases de datos tanto de Autopsy como de Griffeye Analyze DI en busca de toda prueba que represente a menores explotados.
- Se comprueba que alguna o todas las imágenes y videos reportados por NCMEC se encuentran en la evidencia digital obtenida.
- Se analiza el reporte de bulk_extractor en busca de los mails o usuarios reportados por NCMEC.
- Se analiza, en base a los nombres de archivo y metadatos, si existen imágenes provenientes de redes sociales.
- Se analizan las URLs e historial web de las evidencias en busca de URLs que pueden determinar que las imágenes y videos que fueron compartidas y reportadas por NCMEC fueron subidas a la red desde los dispositivos electrónicos/informáticos secuestrados.
- La otra herramienta es ***Volatility***: con dicha herramienta se analiza la imagen forense *dump4GB.001* para poder determinar si en la memoria se encontraba alguno de los mails o usuarios reportados por NCMEC.

V. Análisis de Relaciones

Esta actividad es importante ya que en ella será posible establecer vinculaciones entre la evidencia obtenida y otras investigaciones en trámite. Las tareas fundamentales serán:

- Cruzar información entre la evidencia digital obtenida con la existente en los repositorios del laboratorio, por ejemplo, para poder determinar si las imágenes y videos encontrados en el caso actual de estudio fueron utilizadas y/o compartidas en investigaciones anteriores. Si se puede detectar algún tipo de relación, debe comunicarse a la fiscalía actuante de la causa para que determine las medidas a seguir.
- Se analizan metadatos de imágenes y videos para poder determinar si alguna de ellas fue capturada con la cámara digital CAM-1 con la cual se contaba. Si se detecta que parte de la evidencia digital fue capturada con los dispositivos incautados y representan un delito, se debe informar a la fiscalía actuante de la causa para que determine las medidas a seguir.

Fase de Presentación

Esta es la fase final de todo el modelo. En ella se realizan todos los documentos y anexos que describen la tarea pericial desarrollada. Las actividades correspondientes para este caso son:

Armado de informes necesarios

En esta actividad el Perito Informático prepara un informe con las actividades realizadas, se debe tener en cuenta que dicho informe será leído por personas que no tienen conocimientos técnicos de las actividades desarrolladas en cada fase, es por esta razón, que se recomienda aclarar todos los conceptos técnicos que se requirieron utilizar, así como también las fuentes de información con las que se contaron para la realización de la pericia informática. Los principales conceptos que deberá tener el informe son los siguientes:

- Breve Introducción del caso, partes intervinientes, número de causa y delito.

- Explicar qué es la organización NCMEC.
- Explicar qué es la organización Proyecto VIC.
- Explicar qué es la función de HASH y para qué sirve.
- Documentar por cada punto pericial, cuál fue la evidencia digital o la prueba digital[196] obtenida. Este punto es el más extenso ya que deben detallarse todos los pasos realizados para obtener la evidencia digital o prueba digital.
- Si la evidencia digital o prueba digital obtenida es muy extensa, se deben preparar anexos al informe que contengan toda la evidencia digital o prueba obtenida referenciándolos en el mismo. Es conveniente que dichos anexos sean adjuntados en algún soporte digital como CD o DVD, detallando el hash de los mismos en el informe pericial.

5.2 Caso II "Defraudación Informática" (artículo 173 inciso 16 C.P.)

En este caso ejemplo, se parte de una denuncia de la víctima, quien informa que, tras haber ingresado al HomeBanking de la entidad bancaria desde su notebook personal, detectó una transferencia ilícita y el consiguiente debito del dinero de su cuenta bancaria en favor de un tercero que no conoce.

Fase de Relevamiento y de Recolección

La fase de relevamiento en este caso la realizará la fiscalía solicitando a la entidad bancaria donde tiene la víctima su cuenta bancaria, toda la información disponible acerca de la transferencia ilícita, indicándose fecha, monto, destino del

[196] Se habla en general de evidencia digital, ya que no será el perito informático, sino la fiscalía, quienes determinen qué evidencia se presentará como prueba.

dinero, e IP desde la cual se produjo la maniobra con indicación de día, horario y huso horario exacto.

Una vez que dicha información es proporcionada por la entidad bancaria, y/o por la víctima si lo aportó en la denuncia, se deberá relevar la información bancaria de la cuenta del destinatario, en especial, si hay cámaras de vigilancia del momento en que procedió a la extracción de los fondos del dinero ilícitamente transferido a su favor (cámaras de cajas o de cajeros automáticos), así como información de la documentación presentada para la apertura de la cuenta.

Como parte de la Fase de Recolección, cabe destacar que en este caso esta medida no será a consecuencia de un procedimiento de allanamiento y secuestro ordenado judicialmente, sino que estará constituido por el aporte de la víctima del CPU y/o notebook -en caso de no haberlo formateado tras su uso- a fin de poder realizar su copia forense, en vistas a un análisis e identificación de la evidencia digital que permita determinar la presencia de un malware u otra técnica de manipulación que haya permitido a un atacante acceder al *Homebanking* robando las credenciales de acceso al mismo.

La explicación de cada fase se hará bajo el mismo ambiente de trabajo y condiciones explicadas en el caso anterior, por lo tanto, sólo se detallarán las variantes para este caso en particular, sin repetir operaciones ya mencionadas.

Fase de Adquisición

Tal como se mencionó en el caso anterior, una vez dispuesta la fecha inicio de pericia se procede a notificar a las partes.

Luego, en la fecha indicada se da inicio al acto de pericia, donde se procede a realizar las siguientes tareas:

1. Se identifica la notebook recibida con el nombre *"NB-1"* y se detalla marca, modelo y número de serie en el Acta pericial.

2. Se busca dentro del dispositivo NB-1 la existencia de algún medio de almacenamiento persistente y se lo identifica. En este caso, el EA identifica un disco rígido con el nombre *"HD-1",* luego se detalla en el Acta pericial dicho nombre, su marca, modelo, número de serie y capacidad de almacenamiento.

Para este caso en particular, sólo se realizan las actividades Adquisición de Medios de Almacenamiento Persistente y Validación y Resguardo

I Adquisición de Datos de Medios de Almacenamiento Persistente

El EA realiza la imagen forense bajo un entorno Debian Linux como es el explicado en el caso anterior (ver detalles en el Caso I)

II. Validación y Resguardo

Esta actividad fue realizada en el mismo proceso de adquisición, ya que la herramienta utilizada (*DC3DD)* realiza dicho proceso solapado con el proceso de clonación del dispositivo.

Fase de Preparación

Para esta fase se detallarán las actividades a realizar según el caso de estudio en particular para la imagen forense adquirida por el EA en la fase de adquisición. Dicha imagen forense corresponde a una notebook aportada por el denunciante/víctima cuyo nombre es *"HD-1-1TB.dd".* Las actividades principales son:

I. Preparación del Ambiente

Como se mencionó en el caso anterior, esta actividad está fuertemente relacionada con los puntos periciales ordenados por la fiscalía actuante en el caso. Se supone que los puntos periciales son los siguientes:

A. Se determine el historial de navegación accedido el día 13 de enero de 2015 y cómo se ingresó a la página falsa del Banco Francés.
B. Se determine la existencia de algún tipo de intervención de software malicioso o cualquier otra técnica de manipulación informática que pudiera haber ocasionado la maniobra.
C. Cualquier otra evidencia que permita determinar al autor de la maniobra de phishing denunciada.

Las tareas, técnicas y herramientas principales para este caso serán las siguientes:

- Virtualización de la imagen forense adquirida: es indispensable poder crear una máquina virtual que simule la notebook del denunciante/víctima utilizando la imagen forense adquirida. Esta tarea es útil para poder realizar la tarea de búsqueda de Malware. La herramienta que se utilizará es ***"Oracle VirtualBox".*** Si al iniciar la PC virtualizada, el sistema posee clave de acceso, se utilizará la herramienta ***"Offline NT"*** para resetear la clave de acceso y así poder ingresar a la misma. Cabe destacar que la virtualización se debe realizar con una copia de la imagen forense y no con la imagen forense original, debido a que la máquina virtual escribe datos de acceso y demás en dicha imagen forense, por lo tanto es modificada.

- Búsqueda de Malware: es tarea fundamental para este caso la búsqueda de algún proceso malicioso en la imagen forense que determine si hay filtración de datos hacia un servidor remoto. Para la realización de esta tarea, se deben realizar las siguientes técnicas y herramientas:

  - Volcado de memoria principal del dispositivo: se realizará con el objeto de identificar procesos

maliciosos dentro del sistema. Para esta técnica, se utilizará la herramienta ***"FTK Imager Lite".***

- Detección de malware en el volcado de memoria: Una vez realizado el volcado de memoria, se necesita poder visualizar dicho volcado. Para esta técnica se utilizará la herramienta ***"Volatility".***
- Captura de paquetes de red: para poder identificar, si existe un proceso malicioso previamente; la IP, dominio o toda información relevante de tráfico de red dónde se advirtiere la fuga de información hacia un servidor remoto. La herramienta utilizada en este caso será ***"Wireshark".***
- Búsqueda de procesos que se ejecuten automáticamente al inicio del sistema operativo: con esta técnica se podrá identificar nombre, id y toda información relevante al proceso malicioso y así poder identificarlo más fácilmente en las técnicas antes mencionadas.

- Búsqueda de indicios de ***"Phishing"[197] o "Man in the Middle (MitM)"[198]:*** Al no saber cómo fueron las características de la defraudación informática, se debe contemplar la posibilidad de estos ataques dirigidos. Para eso se deben utilizar las siguientes técnicas y herramientas:
  - Búsqueda del historial web de navegación: para poder establecer si se ingresó al sitio web real del HomeBanking o a un sitio falso.

[197] Véase en Capítulo 2 "Aspectos Legales. Delitos Informáticos".

[198] En criptografía un ataque man-in-the-middle (MitM, o intermediario, en español) consiste en vulnerar un canal de comunicación que se presume seguro, pudiendo leer, insertar o modificar mensajes del canal a voluntad. En particular, el protocolo de intercambio de claves Diffie-Hellman original es vulnerable cuando se emplea sin autenticación. La utilización de redes WiFi sin cifrar facilita la realización de este tipo de ataques.

- Búsqueda de URLs accedidas por el usuario: es posible que el ataque haya sido transparente a la víctima. Por ejemplo, si el sitio del HomeBanking posee una vulnerabilidad conocida como ***"Cross Site Scripting (XSS)***[199]***",*** el usuario o víctima no se daría cuenta del ataque, permitiendo al atacante abusar de la confianza que el usuario o víctima posee con el sitio que tiene dicha vulnerabilidad, y redirigir información, como credenciales a un servidor remoto y así poder robar información.
- Reconstrucción de la caché de navegador: esta tarea es importante para poder visualizar el sitio la cual la víctima accedió y determinar si el mismo era falso o poseía alguna vulnerabilidad antes descrita. Se utilizará la herramienta ***"ChromeCacheView", "IECacheView", "OperaCacheView" o "MZCacheView"*** de la Suite de NirSoft, según corresponda.

II. Identificación de Tecnologías de la Información en el Objeto

Para esta actividad el ***Especialista en Evidencia Digital (EED)*** deberá tener en cuenta el tipo de sistema operativo el cual posee la imagen forense adquirida. Esto es importante para la correcta creación de la máquina virtual que se generará en la siguiente etapa. Para poder observar esto, el EED monta la imagen adquirida con la herramienta FTK Imager y luego hace un recorrido por la estructura de directorios de la misma para poder identificar tipo y versión del

[199] XSS (del inglés, Cross-site scripting) es una vulnerabilidad informática típica de las aplicaciones Web, que permite a un atacante inyectar código ejecutable en páginas web comprometidas. Como vector de ataque, permite robar información delicada, secuestrar sesiones de usuario y comprometer el navegador web, subyugando la integridad del sistema.

sistema operativo. Para este caso el sistema operativo es Windows 7 64 bits.

III. Preparación de Extracción

Para esta actividad, las tareas y aspectos técnicos en cuanto al espacio de alojamiento de las imágenes forenses y evidencia digital serán los mismos que para el caso de estudio anterior, por lo tanto, no se mencionarán nuevamente. Sólo se debe tener en cuenta que como ahora se cuenta con una imagen de forense de 1 Terabyte de capacidad, el disco que aloje a la evidencia digital, deberá contar con al menos 1 Terabyte de espacio disponible. Se suma una tarea más a esta actividad que es la preparación de una máquina virtual para poder ejecutar la imagen forense adquirida. Como ya se mencionó en las actividades anteriores, el EED estableció que el sistema operativo es un Windows 7 de 64bit. Por esta razón el EED crea una máquina virtual con estas características para el correcto funcionamiento con las siguientes consideraciones:

- Como ya se mencionó, se debe trabajar con una copia de la imagen forense debido a que es posible que la misma sea modificada por la herramienta Oracle VirtualBox.
- La memoria principal para esta máquina debe ser de al menos 2GB.
- Virtual Box por defecto no acepta agregar como disco una imagen RAW como lo es la imagen adquirida HD-1-1TB.dd, por lo tanto, se debe convertir dicha imagen a un disco virtual que si lo acepte la herramienta. El EED creará un disco de tipo ***.vmdk*** debido a que dicho disco es un apuntador a la imagen RAW y no se genera un disco virtual de igual tamaño que la imagen RAW original. Esto es importante para ahorrar espacio en los discos donde se alojan las imágenes forenses y tiempo en que se tarda en la generación del disco

virtual. Para esto se utilizará la consola y se utilizará la herramienta VBoxManager que trae Virtual Box. El comando a utilizar es el siguiente: *vBoxManager.exe internalcommands createrawvmdk -filename HD-1-1TB.vmdk -rawdisk <rutaimagenforense>/HD-1-1TB.dd* dónde:

- Filename: especifica la ubicación y nombre el disco virtual generado.
- Rawdisk: especifica la ubicación de la imagen RAW original.

- La máquina virtual generada debe tener una conexión de red controlada y aislada del resto de la red del laboratorio forense. Para esto, dicha conexión, no debe tener acceso a Internet ni conexión con las demás computadoras del laboratorio. Esto es importante debido a que, si la máquina virtual posee algún tipo de malware, el mismo no se disperse e infecte a la red del laboratorio.

Fase de Extracción y Análisis

Esta fase demuestra el ciclo del modelo PURI y la no exclusividad de las actividades a una fase determinada. La Fase de extracción utilizará dos actividades descriptas en la Fase de Adquisición que son: Adquisición de Datos volátiles y Adquisición de Paquetes de Red.

I. Adquisición de Datos Volátiles

Con la máquina virtual generada y en ejecución en la Fase de Preparación, el EED se dispone a realizar un volcado de memoria principal de la misma para poder analizar posteriormente si existe algún proceso malicioso.

Para esto, se aprovechará la utilización de Oracle VirtualBox para virtualizar la computadora comprometida, y obtener directamente a través del software de virtualización

una imagen de la memoria, sin necesidad de ejecturar herramientas externas:

1. Se debe ejecutar la máquina virtual en modo debug desde la línea de comandos, utilizando los flags --dbg y --startvm, de la siguiente forma: *VirtualBox.exe --dbg --startvm VMEstafa* (asumiendo que la máquina virtual se ha creado con el nombre “VMEstafa”).
2. Una vez que la máquina virtual ha iniciado, en el menú “Debug” (o “Depurar”, si está configurado en español) se debe ejecutar la opción “Command line…” o “Línea de comandos…”.
3. En la línea de comandos, se ingresa el comando *.pgmphystofile NombreVolcado* indicando el nombre de archivo que se desea para el volcado de memoria de la máquina virtual. El volcado obtenido es un volcado de tipo RAW.

II. Adquisición de Paquetes de Red

Con la máquina virtual en ejecución el EED se dispone a realizar una captura de los paquetes de red de la misma. Para esto, se utilizará la herramienta Wireshark para la captura y su posterior análisis. A diferencia de la actividad anterior, la captura debe comenzarse con la máquina virtual en ejecución, pero ni bien la misma inicia. Luego, se deben ir ejecutando los navegadores y demás programas que se crean de interés. Es conveniente dejar a la herramienta capturando por un lapso de tiempo considerable para tener la mayor cantidad de información posible luego en la actividad de análisis. Una vez finalizado, el EED almacena el archivo de la captura de paquetes de red en un disco externo para su posterior análisis.

III. Extracción a nivel de Aplicación

La herramienta a utilizar es Autopsy. Primeramente, se debe indicar a la herramienta la imagen forense a realizar la

extracción y luego indicar las tareas a realizar. Las mismas son:

- Extracción de URLs visitadas, historial web y todo tipo de información resultante de la navegación web: como se mencionó anteriormente, Autopsy posee técnicas para extraer dicha evidencia digital sin la necesidad de realizar la extracción manualmente.

- Reconstrucción de la caché de los navegadores: el EED debe establecer la cantidad de navegadores disponible en la PC y tratar de reconstruir la caché de los navegadores. Para este caso en particular, el ED, determinó que el único navegador utilizado es Google Chrome, por lo tanto, se dispone a utilizar la herramienta ChormeCacheView de Nirsoft. Con dicha herramienta, no sólo es posible ver la caché del navegador, sino que es posible reconstruir un sitio web en particular, según los datos de la misma. Para este caso en particular, la actividad de extracción y análisis están fuertemente relacionadas, debido a que en esta parte, se debe identificar un posible sitio web accedido falso y poder reconstruirlo. Cabe destacar, que para esta actividad es preferible, el EED debe, primeramente, extraer la carpeta donde se almacena la caché del navegador. Para este caso de estudio la misma se encuentra en: *[User Profile]\Local Settings\Application Data\Google\Chrome\User Data\Default\Cache*

IV. Análisis de Contenidos

En esta actividad el ED, se enfocará en analizar toda la evidencia digital extraída en las actividades anteriores. Las tareas fundamentales son:

- Como primera medida el EED analizará con la herramienta Wireshark, todos los paquetes de red capturados en busca de direcciones IP de servidores

remotos o puertas traseras[200] existentes que filtren información en la imagen forense analizada.

- Analizar la caché extraída del navegador, historial web y URLs accedidas en busca de sitios web falsos y que en los mismos se pueda establecer algún acceso a un servidor remoto como la IP o nombre del mismo. Es importante aclarar que la reconstrucción de la caché del navegador implica una reconstrucción parcial de un sitio web, debido a que sólo es posible recuperar los accesos del lado del cliente del sitio web o no del servidor del sitio web.
- Analizar el volcado de memoria principal con la herramienta ***Volatility*** en busca de procesos maliciosos que filtren información.

Fase de Presentación

Como se dijo anteriormente, esta es la fase final de todo el modelo. En ella se realizan todos los documentos y anexos que describen la tarea pericial desarrollada. Las actividades correspondientes para este caso son:

I. Armado de informes necesarios

En esta actividad el Perito Informático prepara un informe con las actividades realizadas, se debe tener en cuenta que dicho informe será leído por personas que no tienen conocimientos técnicos de las actividades desarrolladas en cada fase, es por esta razón, que se recomienda aclarar todos los conceptos técnicos que se requirieron utilizar, así como también las fuentes de información con las que se contaron para la realización de la pericia informática. Los principales conceptos que deberá tener el informe son los siguientes:

[200] Adaptación directa del término inglés *backdoor*, que significa "puerta trasera". Son mecanismos que permiten acceder de maneras imprevistas a un sistema, y por ende representan un riesgo de seguridad.

- Breve Introducción del caso, partes intervinientes, número de causa y delito.
- Explicar concepto de máquina virtual.
- Explicar concepto de volcado de memoria principal.
- Explicar concepto de adquisición de paquetes de red.
- Explicar qué es la función de HASH y para qué sirve.
- Documentar por cada punto pericial cuál fue la evidencia digital obtenida. Este punto es el más extenso ya que deben detallarse todos los pasos realizados para obtener la evidencia digital.
- Si la evidencia digital obtenida es muy extensa, se deben preparar anexos al informe que contengan toda la evidencia digital o prueba obtenida referenciándolos en el mismo. Es conveniente que dichos anexos sean adjuntados en algún soporte digital como CD o DVD, detallando el hash de los mismos en el informe pericial.

6. Conclusiones

Se han descrito dos de las diferentes posibilidades en las que se aplica el modelo PURI con sus variantes y usos específicos. En este libro se fomenta el uso de herramientas de uso libre y/o *open source* destacando la posibilidad de conocer el funcionamiento de la herramienta observando su código, ampliándolo si se quisiere y distribuyéndolo a la comunidad sin la necesidad de gastar gran cantidad de dinero en la adquisición de licencias de software forense pago. Cabe destacar que hay un abanico muy amplio de herramientas que se adaptan a las necesidades de cada caso en particular y que las descriptas en estos casos pueden ser, también, reemplazadas y actualizadas por otras.

Anexo I: Modelo PURI - Detalle de Tareas

1. Fase Identificación

1.1 Identificación de Documentación (Legal y Técnica)

Tareas:

- Relevamiento de documentos legales (Legal).
  - Técnica: Pedido de Oficio.
  - Técnica: Exploración en Internet.
- Relevamiento de documentos técnicos (Técnico).
  - Técnica: Pedido de Oficio.
  - Técnica: Exploración en Internet.
- Relevamiento de documentos administrativos (Legal).
  - Técnica: Pedido de Oficio.
  - Técnica: Exploración en Internet.
- Relevamiento de documentos de seguridad lógica y física (Técnico).
  - Técnica: Pedido de Oficio.
  - Técnica: Exploración en Internet.

1.2 Identificación de Infraestructura IT (Técnica)

- Identificación de Servidores Internos y Externos.
  - Técnica: Para Servidores Internos y Externos – Enumeración.
    - Herramienta Recomendada: nmap.
  - Técnica: Para Servidores Externos - Consulta de Nombres de Dominio.
    - Herramienta Recomendada: Comando Dig.
- Identificación de Usuarios.
  - Técnica: Sniffing Red Lan.

        - Herramienta Recomendada: WireShark.
    - Técnica: Búsqueda de Usuarios por Internet.
        - Herramienta Recomendada: Navegadores – Mantra.

- Identificación de Dispositivo de Usuario (Equipos y Dispositivos Móviles).
    - Técnica: Enumeración.
        - Herramienta Recomendada: nmap.
    - Técnica: Sniffing Red Lan.
        - Herramienta Recomendada: WireShark.

- Identificación de Servicios Internos y Externos.
    - Técnica: Escaneo de Puertos y Servicios.
        - Herramienta Recomendada: nmap.

2. Fase recolección (Legal y Técnica)

2.1 Detección de Infraestructura IT (Técnica)

- Detección de Servidores Internos y Externos (Ej: Red Local, Cloud).
    - Técnica: Inspección ocular, seguimiento cableado de red.
    - Técnica: para Servidores Internos y Externos, Enumeración.
        - Herramienta Recomendada: nmap.
    - Técnica: para Servidores Externos, Consulta de Nombres de Dominio.
        - Herramienta Recomendada: Comando Dig.

- Detección de Dispositivos de Usuario (Ej: Equipos PC, USB, SD, SIM, CD, Dispositivos móviles, etc).
    - Técnica: Inspección ocular, seguimiento cableado de red.

- Técnica: Enumeración.
  - Herramienta Recomendada: nmap.
- Técnica: Sniffing Red Lan.
  - Herramienta Recomendada: WireShark.

2.2 Recolección de Objetos

- Secuestro.
- Embalaje.
- Transporte.

3. Fase de Adquisición (Técnica)

3.1 Adquisición de datos persistentes (Por ej: Disco, Tarjeta SD, ROM interna del Dispositivo)

- Bloqueo del medio de Almacenamiento.
  - Técnica: Bloqueo por hardware.
    - Herramienta Recomendada: Bridge USB.
    - Descripción: Consiste en utilizar dispositivos que permitan conectar el medio de almacenamiento para llevar a cabo la adquisición en modo solo lectura. De esta forma se garantiza que los datos contenidos no se modifican tanto durante la adquisición como durante el montado del mismo.
  - Técnica: Bloqueo por software.
    - Herramienta Recomendada: comandos de sistema operativos para bloqueo de dispositivos.
    - Descripción: Consiste en utilizar software o configurar el sistema operativo que se utilizará como dispositivo host para la adquisición y

montar el medio de almacenamiento en modo solo lectura.

- Búsqueda de Host Protected Areas (HPA).
  - Técnica: Comandos de interfaz Serial ATA.
    - Descripción: Consiste en la utilización de comandos definidos en la especificación ATA para la detección y acceso a las zonas protegidas que pueda tener configuradas el medio de almacenamiento.
      - Herramientas Recomendadas: TAFT, HDAT2

- Captura y resguardo de la imagen forense.
  - Técnica: Copia bit a bit del medio de almacenamiento (por SW).
    - Herramienta Recomendada: comando dd/ ddrescue/dc3dd (GNU)
  - Técnica: Copia bit a bit del medio de almacenamiento (por HW).
    - Herramienta Recomendada: Duplicador de discos, Imágen Física de Dispositivo (Ej: UFED, XRY, MobilEdit), JTag.

3.2 Adquisición de datos volátiles (Ej: RAM Equipo, RAM Dispositivos Móviles, Tablas de Ruteo)

- Captura y resguardo.
  - Técnica: CrashDump por Software (Sólo Memoria RAM).
    - Herramienta Recomendada: NotMyFault (Sysinternals).
    - Descripción: Es una técnica de adquisición de memoria principal. Consiste en generar/forzar

un malfuncionamiento del sistema operativo para que el mismo genere una copia de la memoria principal llamada CrashDump

- Técnica: Dump completo por Software (Memoria RAM y Área de Paginación - Memoria virtual).
  - Herramienta Recomendada: kntdd, dd (FAU), FTK Imager, Mandiant Memoryze.
  - Descripción: Consiste en utilizar software que realice la adquisición de memoria principal. La ventaja es que se cuenta con información de área de paginación de memoria principal.
- Técnica: Captura de memoria por Hardware.
  - Herramientas recomendadas: Tribble, Bus Firewire, PCI Express, USB.
  - Descripción: Consiste en utilizar herramientas de hardware que realice la adquisición de memoria principal. La ventaja es que se minimizan los cambios en memoria principal al momento de llevar a cabo la adquisición debido a que no hay ningún proceso ejecutándose en memoria principal que realice dicho volcado de memoria principal. Como desventaja, debe mencionarse que el equipo debe presentar puertos compatibles libres, y además algunas herramientas de clonado de memoria presentan limitaciones para copiar más de 4GB de información.
- Técnica: Comandos internos del router para las tablas de ruteo.
  - Descripción: Consiste en utilizar los comandos propios del sistema de gestión del router para

adquirir los datos volátiles contenidos en sus registros.

3.3 Adquisición de paquetes de Red

- Captura y Filtrado de Paquetes.
  - Técnica: Sniffing.
    - Herramienta recomendada: TCPDump, WireShark.
    - Descripción: Consiste en utilizar software de adquisición de paquetes de red.

3.4 Adquisición de Smartcards (Ej: SIM, Tarjetas de Crédito, Pasaportes Inteligentes)

- Lectura del medio (orientada a la norma).
  - Técnica: Hardware específico.
    - Descripción: Las Smartcards pueden tener distintos formatos y protocolos. Es por esto que esta técnica consiste en utilizar el hardware específico para cada smartcard y llevar a cabo la adquisición.

3.5 Validación y resguardo

- Compresión y división de la imagen forense.
  - Técnica: configuración en el comando de copia de la información.
    - Descripción: Consiste en utilizar los parámetros o modificadores de los comandos nativos del sistema operativo al momento de hacer la copia de la imagen forense.
  - Técnica: comandos independientes.
    - Herramientas recomendadas: GZip /bz2/ ZIP.

        - Descripción: Consiste en utilizar comandos o software específico para compresión de archivos.

- Generación de hashes.
    - Descripción: Consiste en generar un código alfanumérico que intenta representar unívocamente al archivo de la imagen forense.
    - Técnica: Generación de un hash en Original y copia.
        - Herramientas recomendadas: comando nativo del sistema operativo o hashmyfiles que implementen los algoritmos de cifrado como MD5, SHA-1.
        - Descripción: Al generar un hash en ambos archivos luego se puede validar que la copia es fiel al original.
    - Técnica: Generación de múltiples hashes, cada N bytes.
        - Herramientas recomendadas: md5deep, hashdeep, piecehash.
        - Descripción: En caso de diferir el hash entre el archivo original y su copia, generar hashes por regiones permite saber en qué regiónes del archivo hubo modificaciones y qué regiones permanecen intactas.

- Validación de hashes contra original.
    - Descripción: Es el proceso de comparar los valores de los hashes entre el original y copia.

3.6 Transporte no supervisado

- Almacenamiento protegido.

- Técnica: cifrado del medio de almacenamiento por hardware.
  - Herramientas recomendadas: discos que incorporan cifrado por dispositivo.
- Técnica: cifrado del medio de almacenamiento por software.
  - Herramientas recomendadas: Tecnología de cifrado transparente, ej: TrueCrypt, o Software ZIP o RAR con protección por contraseña y cifrado.

4. Fase preparación (Técnica)

4.1. Preparación de Extracción

- Asegurar espacio libre suficiente.
- Ensamblado y descompresión de las imágenes forenses.
- Validación del original y copia.
  - Técnica: generación de hashes.
    - Herramienta recomendada: Para estas tareas se debe utilizar las mismas herramientas que se utilizaron para la división y generación de hashes.
- Mapeo de imagen forense a dispositivo del Sistema Operativo.
  - Técnica: loopback device / Dispositivo Virtual.
    - Descripción: En sistemas operativos un loop device es un pseudo-dispositivo que hace que se pueda acceder a un fichero como un dispositivo de bloques. La idea de esta técnica es montar la imagen forense como un disco externo dentro del sistema operativo donde se

analizará la misma. De esta manera, se puede recorrer la estructura de directorios de la imagen forense tal cual figuran en el disco original de donde fue adquirida.
        - Herramientas recomendadas: comandos nativos de GNU Linux o OSFMOUNT para Windows.

- Generación de Máquina Virtual.
    - Descripción: consiste en generar una máquina virtual con la imagen forense con la que se cuenta. De esta manera se podrá emular el dispositivo del cual se obtuvo la imagen forense y tener una visión de cómo se encontraba justo antes de su secuestro.
    - Herramienta recomendada: Oracle VirtualBox.
  - Técnica: conocer sistema operativo y arquitectura del dispositivo el cual se obtuvo la imagen forense para poder crear la máquina virtual.
  - Técnica: transformar la imagen forense en disco virtual.
    - Descripción: Es necesario poder transformar la imagen forense en un disco virtual soportado por la herramienta de virtualización, en este caso VirtualBox.
    - Herramienta: VBoxManager.

4.2. Identificación de Tecnología de la Información en el objeto

- Recomposición de Volumen RAID.
  - Técnica: Reconstrucción estadística de arreglos RAID desordenados.

- Identificar cantidad de discos, particiones y tipos de filesystem.
  - Técnica: Lectura de tabla de particiones.
  - Técnica: Búsqueda de particiones por software.
    - Herramienta recomendada: fdisk, parted, cfdisk, mmls y fsstat de The Sleuth Kit.

- Identificar y quebrar medios de cifrado.
  - Técnica: Análisis estadístico y de entropía de sectores de disco.
    - Descripción: Un análisis de medidas estadísticas de los bloques del disco (promedio aritmético, varianza, entropía, por nombrar algunas) puede arrojar indicios sobre el contenido real del mismo. Dependiendo el método de cifrado que se haya utilizado, se obtendran resultados de mayor o menor utilidad.
  - Técnica: Recuperación de claves de cifrado de imagen de memoria principal.
    - Descripción: Considerando la dificultad de descifrar una clave, esta técnica consiste en buscar en memoria principal la clave sin cifrar.
  - Técnica: Ataque por fuerza bruta con infraestructura de procesamiento paralelo.
    - Herramientas recomendadas: volatility, Hashcat/oclHashcat.

- Identificar cantidad y tipo de Sistemas Operativos presentes.
  - Técnica: Análisis de tabla de particiones.

- Identificar Máquinas Virtuales presentes.
  - Técnica: Búsqueda de hypervisores.

- Identificar programas instalados en los Sistemas Operativos detectados.
  - Técnica: Búsqueda de información de aplicaciones en registro (Windows).
    - Herramientas Recomendadas: RegRipper, Registry Decoder.
  - Técnica: Búsqueda de información de paquetes (aptitude, RPM, etc).

4.3. Preparación del ambiente

- Preparación del Ambiente de Examinación.

5. Fase de extracción y análisis

5.1. Extracción a nivel de aplicación (información semántica dependiendo de la aplicación relacionada: historial web/base de datos/ registros de un sistema / cloud)

Se recomienda realizar las siguientes tareas dependiendo las necesidades del caso:

- Búsqueda de archivos recientes o frecuentes.
- Análisis de aplicaciones recientemente utilizadas.
- Análisis archivos recientes vinculados a herramientas frecuentes.
- Revisión de historiales de navegación Web (en aplicaciones de uso frecuentes).
- Análisis de almacenamiento en Cloud.
- Búsqueda de máquinas virtuales.
- Búsqueda y extracción papelera de reciclaje.
- Búsqueda y extracción archivos recientes.
- Búsqueda y extracción de archivos comprimidos.
- Búsqueda de imágenes.

- Búsqueda y extracción navegadores web.
- Búsqueda y extracción redes sociales.
- Búsqueda y extracción mensajería instantánea.
- Búsqueda y extracción correo electrónico.
- Búsqueda y extracción aplicaciones de transferencia de archivos.
- Búsqueda y extracción almacenamiento cloud.
- Búsqueda y extracción aplicaciones multimedia.
- Búsqueda y extracción archivos temporales.
- Búsqueda y extracción ofimática.
- Búsqueda y extracción juegos.
- Búsqueda y extracción aplicaciones particulares.
- Búsqueda de archivos o sectores de la imagen forense que contengan cierta cadena de caracteres.

Para evaluar cada aplicación enumerada, o aplicaciones que no se han contemplado en el listado anterior, se recomienda:

- Análisis de los archivos de configuración de la aplicación.
- Análisis de archivos de datos y bases de datos asociadas a la aplicación.
- Búsqueda del ejecutable y sus archivos asociados en una base de datos de aplicaciones.
    - Recurso: base de datos NSRL del NIST.
    - Recurso: servicio VirusTotal.
- Análisis del comportamiento de la aplicación en un entorno controlado.

- Técnica: Análisis de memoria y código dentro de un emulador.
    - Herramientas Recomendadas: QEmu, Pandas.

- Desensamblado de la aplicación para análisis de comportamiento.
    - Técnica: Ingeniería inversa sobre código.
        - Herramientas Recomendadas: bokken, radare, distorm, IDA Pro.

5.2. Extracción a nivel de plataforma

- Obtención de listado de aplicaciones más utilizadas.
    - Técnica: Análisis de sistema de precarga de aplicaciones.
    - Técnica: Análisis de las sugerencias de aplicaciones de uso frecuente.
        - Herramientas Recomendadas: Nirsoft WinPrefetchView.

- Recuperación de archivos eliminados.
    - Técnica: Recuperación en base al sistema de archivos.
        - Herramientas Recomendadas: Recuva.

- Extracción de Información a examinar por tipo de archivo.

- Extracción de metadatos del archivo en el filesystem.
    - Técnica: Acceso a información del filesystem.
        - Herramientas recomendadas: The Sleuth Kit, Autopsy.

- Extracción de archivos protegidos con contraseña.
    - Técnica: Ataque por fuerza bruta con infraestructura de procesamiento paralelo.

        - Herramientas recomendadas: Hashcat/oclHashcat.

- Detección y extracción de archivos cifrados.
  - Técnica: Análisis estadístico y de entropía de los archivos.
  - Técnica: Recuperación de claves de cifrado de imagen de memoria.
  - Técnica: Ataque por fuerza bruta con infraestructura de procesamiento paralelo.
    - Herramientas recomendadas: volatility, Hashcat/oclHashcat.

- Búsqueda de Información de Configuración.
- Búsqueda de Información de Procesos en Memoria.
  - Técnica: Análisis de memoria.
    - Herramientas recomendadas: volatility, Rekall, BIP-M.

5.3. Extracción a bajo nivel (bloques/bytes)

- Búsqueda de información en disco.
- Búsqueda de información en el área de paginado.
- Extracción de archivos en espacio no asignado.
  - Técnica: File Carving.
    - Herramientas Recomendadas: Scalpel, PhotoRec, Adroit Photo Forensics, CIRA, Autopsy, Bulk Extractor.

- Búsqueda de Bases de Datos en particiones no formateadas.

5.4. Análisis de contenido

- Búsqueda de información en el contenido.

- Búsqueda de información ofuscada u oculta en el contenido.
- Extracción de metadatos propios del archivo.

5.5. Análisis de relaciones

- Evaluación de puntos de pericia.
- Identificar relaciones entre elementos.

6. Fase de Presentación

6.1. Armado del Informe

6.2 Preparación de la Información a Presentar

Anexo II: Herramientas Complementarias

Además de las herramientas que fueron descriptas anteriormente, existe un gran abanico de herramientas para análisis forense. Aquí se describen algunas de ellas:

- OPHCRACK: es una herramienta desarrollada por Cedric Tissieres, Philippe Oechslin y Objectif Sécurité, para crackear las contraseñas de Windows, basada en las tablas Rainbow. Corre bajo Windows, Mac OS X (x86) y Linux. Link de proyecto: http://ophcrack.sourceforge.net/

- Colección de utilidades NirSoft: Web que contiene gran cantidad de herramientas y utilidades de diferente índole para análisis forense, entre otros. Las aplicaciones son todas desarrolladas por Nir Sofer y abarcan herramientas de análiis forense de bajo nivel hasta alta nivel. Link del sitio: http://www.nirsoft.net/.

  Algunas de estas utilidades son:

  - MyLastSearch: permite ver todas las búsquedas efectuadas en los navegadores que se encuentran disponibles.
  - FBCacheView: herramienta que escanea la cache de Facebook de los navegadores en busca de las imágenes que se hayan visitado.
  - MailPassView: recupera las claves de los clientes de mails más populares como Outlook Express, Outlook 2000, Windows Live Mail, entre otros. Tener especial cuidado en el uso de esta herramienta, ya que si no hay autorización para entrar al correo, se podría estar violando la privacidad del correo electrónico.
  - WebBrowserPassView: herramienta que permite visualizar las contraseñas almacenadas en los navegadores. Tener especial cuidado en el uso de

esta herramienta ya que se podría estar violando la privacidad de una persona.

- UNDBX: herramienta Open Source que permite extraer el contenido de los mails de Outlook Express (dbx). Link del sitio: https://sourceforge.net/projects/undbx/
- ExifTool: herramienta que sirve para visualizar los metadatos de gran cantidad de archivos. Está desarrollada por Phil Harvey. Link del sitio: http://www.sno.phy.queensu.ca/~phil/exiftool/
- HexEdit: editor hexadecimal de licencia freeware desarrollado por la compañía MiTec. Link del sitio: http://www.mitec.cz/hex.html
- DB Browser for SQLite: herramienta Open Source desarrollada por Mauricio Piacentini que permite visualizar, crear y editar bases de datos SQLite comúnmente utilizadas por los navegadores webs y aplicaciones de celulares, entre otras. Link del sitio: http://sqlitebrowser.org/

Capítulo 6. Aspectos Técnicos

Autores: Hugo Javier Curti, Ariel Oscar Podestá y Gonzalo Matías Ruiz De Angeli.

1. Introducción a los Sistemas Operativos. 1.1 Definición y Objetivos de un Sistema Operativo moderno. 1.2 Características esperadas de un Sistema Operativo moderno.
2. El nivel de bloques. 2.1 Características comunes de los dispositivos de bloques. 2.2 Los controladores. 2.3 Ejemplos: discos rígidos y particiones. 2.4 Ejemplo de acceso directo a nivel de bloques.
3. El nivel de archivos. 3.1 Archivo. 3.2. Sistema de Archivos. 3.3. Sistema de Archivos FAT. 3.4. Sistema de Archivos NTFS. 3.5. Sistema de Archivos EXT3.
4. Gestión de memoria principal. 4.1. La memoria principal. 4.2. Paginación. 4.3. Segmentación. 4.4. Segmentación con paginación. 4.5. Memoria Virtual. 4.6. Ejemplo práctico: Gestión de memoria principal en Windows.
5. Gestión de procesos. 5.1. Procesos. 5.2. La tabla de procesos. 5.3. Planificación de procesos. 5.4. Comunicación entre procesos. 5.5. Ejemplo práctico: análisis de procesos en Linux.
6. Conclusiones

1. Introducción a los Sistemas Operativos

Las primeras computadoras que se construyeron no tenían Sistema Operativo. Después de la puesta en marcha el programa que se deseaba ejecutar era cargado manualmente por un operador y ejecutado. Esta tarea debía realizarse introduciendo códigos binarios en un tablero, volviéndose muy tediosa y susceptible a errores.

Con la aparición de las unidades de almacenamiento de datos (lectores de tarjetas, cintas, y posteriormente discos rígidos y flexibles) el proceso de arranque pasó a ser la carga manual del programa que permitía leer estos dispositivos, para que luego se pudiera cargar en forma automática los programas que ya estaban previamente almacenados a la memoria para poder ser ejecutados.

La evolución tecnológica de este proceso devino en los primeros Sistemas Operativos: programas que permitían automatizar el arranque de la computadora. Para lograr este fin contenían los programas para leer y escribir en los dispositivos de almacenamiento y procedimientos que facilitaban al operador la carga en memoria principal y ejecución de un programa, así como también la administración de sus datos de entrada y salida.

Con la mejora de los diferentes componentes de la computadora, fundamentalmente Unidades Centrales de Procesamiento (CPU) más rápidas y memorias de más velocidad y de mayor capacidad de almacenamiento, a fin de aprovechar correctamente estos recursos, se volvió imperioso implementar la posibilidad de ejecutar más de un programa de manera simultánea, compartiendo los recursos de la computadora entre todos ellos. Este hecho forzó al Sistema Operativo a evolucionar a lo que es hoy y que se intentará describir brevemente en este capítulo.

1.1 Definición y Objetivos de un Sistema Operativo moderno

Un Sistema Operativo moderno puede definirse como un programa o conjunto de programas que tienen como objetivo principal administrar los recursos de una computadora y que para tal fin poseen privilegios especiales que lo diferencian del resto de los programas. Los objetivos generales del Sistema Operativo pueden resumirse en los citados a continuación.

- Administrar los recursos de la computadora
- Abstraer los dispositivos para facilitar la programación
- Proveer una interfaz hombre-máquina para su supervisión

Desde el mismo momento en que varios programas en ejecución, denominados *procesos*, comparten los recursos de la computadora, se vuelve necesario un mecanismo de administración para evitar que los procesos se interfieran entre sí en el uso de los recursos. El Sistema Operativo cumple esta función proveyendo mecanismos de gestión para cada recurso de la computadora. Entre los más importantes pueden citarse: gestión de memoria principal, gestión de archivos, gestión de dispositivos de entrada/salida, gestión de procesos y gestión de red de comunicaciones.

Con la evolución de las computadoras el conocimiento se fue transfiriendo progresivamente desde los circuitos (*hardware*) hacia los programas (*software*). El hardware se fue volviendo cada vez más especializado y el software cada vez más complejo. Por esta razón el reúso de software se volvió una necesidad cada vez más imperiosa. A fin de facilitar este reúso de software, el Sistema Operativo provee una serie de abstracciones sobre el hardware que permiten la construcción de aplicaciones desde un nivel de abstracción mayor, o sea en forma más general. Por ejemplo, un proceso puede solicitar que se muestre algo en la pantalla, sin necesidad de tener que conocer qué pantalla específica posee la

computadora. El proceso realiza la solicitud al Sistema Operativo mediante una *llamada al sistema*, y éste se encarga de procesarla en el hardware específico. De esta forma el software puede ser utilizado en muchas computadoras diferentes.

Finalmente, el Sistema Operativo provee una interfaz hombre-máquina que permite a los usuarios humanos (usuario final, administrador, desarrollador) supervisar su funcionamiento, hacerle solicitudes (por ejemplo, instalar o ejecutar un programa) u ordenar la información en las unidades de almacenamiento. Existen distintos tipos de interfaces orientadas a distintos tipos de uso. Las primeras interfaces que aparecieron se basaron en líneas de órdenes sobre terminales de texto. La evolución tecnológica permitió después la implementación de interfaces visuales sobre terminales gráficas. Los Sistemas Operativos modernos suelen proveer ambos tipos de interfaz, debido a que en general la interfaz gráfica se adapta mejor a los usuarios finales, mientras que la interfaz de línea de órdenes se adapta mejor a los usuarios administradores.

1.2 Características esperadas de un Sistema Operativo moderno

Todo Sistema Operativo moderno debe ofrecer como mínimo las siguientes características:

- Multitarea
- Multiusuario
- Multiprocesador

Se denomina *multitarea* a la capacidad del Sistema Operativo de gestionar la ejecución de varios programas de manera concurrente, compartiendo los recursos de la computadora entre ellos sin interferirse. Como ya se mencionó antes, esta característica es necesaria a fin de poder aprovechar correctamente los recursos de una computadora

moderna. Para compartir la Unidad Central de Procesamiento (CPU), se suele dividir el tiempo de la misma entre los diferentes procesos que se organizan en colas que definen el orden de acceso, garantizando que todos los procesos accederán en algún momento, maximizando a su vez el tiempo que la CPU está en uso. Esto se hace a gran velocidad y crea la ilusión al usuario humano de que todos los procesos se ejecutan al mismo tiempo.

Por otra parte, se espera que el Sistema Operativo provea mecanismos para que varios usuarios puedan compartir los recursos sin interferirse entre sí. Un Sistema Operativo es *multiusuario* cuando provee estos mecanismos. Como mínimo el Sistema Operativo debería *identificar* diferentes usuarios (por ejemplo, mediante el uso de cuentas de usuario), *autenticar* la identidad de los usuarios (por ejemplo, utilizando contraseñas), y proveer mecanismos de privilegios que permitan a los usuarios controlar lo que otros usuarios pueden hacer con sus recursos.

Durante las últimas décadas del siglo pasado la evolución de las CPU se basó en que éstas funcionen más rápido, mediante la progresiva miniaturización de sus componentes. Sin embargo, a principio de este siglo se alcanzó un límite tecnológico a ese respecto, y por lo tanto la evolución pasó a basarse en la idea de paralelizar tareas. Como consecuencia de esto comenzaron a aparecer las computadoras multinúcleo, que poseen más de una CPU. Naturalmente los Sistemas Operativos tuvieron que adaptarse a este cambio. Se dice que un Sistema Operativo es *multiprocesador* cuando es capaz de gestionar computadoras que poseen más de una CPU, repartiendo los procesos entre ellas maximizando su uso.

2. El nivel de bloques

El nivel de bloques es una de las abstracciones más ricas del Sistema Operativo que el analista forense puede explorar en la búsqueda de evidencia o en la recuperación de

datos. Cumple una función muy importante, junto con el nivel de archivos, en la administración de la memoria secundaria de la computadora. En esta sección se describen las características de los dispositivos de bloques, los controladores encargados de implementar la abstracción, y los discos y sus particiones como ejemplos comunes de dispositivos de bloque.

2.1 Características comunes de los dispositivos de bloques

Una abstracción por definición es una generalización. La generalización permite tratar de manera normalizada con dispositivos de distinta naturaleza, facilitando de esta forma la programación de aplicaciones. Para lograr este objetivo se extraen las características comunes de todos estos dispositivos y se genera una Interfaz de Aplicación (API) para tratar con estas características. Se citan a continuación las características comunes de los dispositivos de bloques.

1. *Almacenamiento de información en bloques contiguos de tamaño fijo*. El propósito general de un dispositivo de bloques es almacenar información. Con este fin la información se ordena en el dispositivo como una sucesión de bloques de tamaño fijo. Es responsabilidad de las aplicaciones (o de niveles de abstracción superiores, como el Sistema de Archivos) organizar la información dentro de estos bloques de forma tal que la misma sea de fácil acceso.
2. *Cantidad de bloques finita, conocida y fija*. La cantidad de bloques que posee un dispositivo, y por lo tanto también su capacidad de almacenamiento, es limitada a una cantidad conocida, que normalmente no cambia mientras el dispositivo está siendo utilizado.
3. *Acceso aleatorio de granularidad gruesa*. Los dispositivos de bloques pueden ser accedidos para

leer o escribir en ellos, pudiéndose indicar el número de bloque desde el cual comenzar la lectura o la escritura. Se denomina granularidad gruesa al hecho de que se puede acceder a un bloque en particular, y un bloque normalmente tiene un tamaño en el orden de las centenas de bytes o de los kilobytes, para distinguirlo del acceso aleatorio de granularidad fina, que permite el acceso a un byte o a un pequeño conjunto de bytes en particular, presente en la memoria principal de la computadora.

4. *Recursividad*. Uno o más dispositivos de bloques pueden estar contenidos dentro de otro dispositivo de bloques más grande, y un dispositivo de bloques puede implementarse utilizando uno o más dispositivos de bloques más pequeños como base. Esto permite la agregación de funcionalidad mediante capas de dispositivos de bloques (ver el Capítulo de RAID) y la creación de numerosos artilugios de software que pueden facilitar el trabajo del analista forense (por ejemplo, la clonación o la emulación de dispositivos, o la extracción de una copia imagen de un dispositivo para su salvaguarda o posterior análisis).

2.2. Los controladores

A fin de tratar con dispositivos físicos de naturaleza diferente, los controladores (o *drivers*) del Sistema Operativo funcionan como rutinas específicas que implementan un conjunto de funciones comunes para un dispositivo en particular. Por ejemplo, un pendrive y un disco rígido. Cada controlador debe implementar un conjunto mínimo de funcionalidades que permiten la interacción del Sistema Operativo con el dispositivo físico controlado. Las funciones que típicamente debe implementar un controlador de dispositivo de bloques son las siguientes:

- *Abrir dispositivo*. Es invocada por el Sistema Operativo para comenzar a trabajar con el dispositivo. Es responsable de inicializar el dispositivo y dejarlo preparado para realizar operaciones de entrada/salida.
- *Cerrar dispositivo*. Es invocada por el Sistema Operativo cuando deja de trabajar con el dispositivo. Es responsable de desencadenar todas las operaciones pendientes sobre el dispositivo y luego liberar todos los recursos asociados al mismo.
- *Transferir datos*. Es invocada por el Sistema Operativo para generar una transferencia de datos entre la memoria principal y el dispositivo. La transferencia puede ser tanto de entrada como de salida al dispositivo.
- *Recibir comando de control*. Es invocada por el Sistema Operativo para enviar un comando de control (*ioctl*) al dispositivo (por ejemplo: *expulsar medio*). Algunos comandos de control dependen fuertemente del dispositivo, y por lo tanto hay algunos estandarizados y otros que son propios de cada dispositivo.

2.3. Ejemplos: discos rígidos y particiones

Se describe a continuación, a modo de ejemplo, la forma que utilizan los Sistemas Operativos compatibles con UNIX para acceder a los dispositivos directamente en el nivel de bloques. Para lograr este objetivo, estos sistemas mapean cada dispositivo a un archivo especial, denominado archivo de dispositivo, que se encuentra en una ubicación conocida del sistema de archivos virtual. Esto permite a las aplicaciones tratar a los dispositivos como si fueran archivos, utilizando las mismas llamadas al sistema, haciendo en muchos casos el acceso a dispositivos intercambiable con el acceso a archivos y simplificando enormemente la programación.

En el Sistema Operativo Linux para acceder a un disco rígido directamente en el nivel de bloques se utiliza la sigla «sd» (*scsi disk*) seguido de una letra para indicar el disco al que se desea acceder, seguido de un número para indicar la partición. Si no se indica la partición, el archivo hace referencia al disco completo. A continuación se muestran algunos ejemplos:

- «/dev/sda3» hace referencia a la tercera partición del primer disco rígido.
- «/dev/sdb1» hace referencia a la primera partición del segundo disco rígido.
- «/dev/sdc» hace referencia al tercer disco rígido completo.

2.4. Ejemplo de acceso directo al nivel de bloques

Mediante el comando «dd» (*direct dump*) provisto entre las utilidades básicas en las distribuciones de GNU Linux es posible aprovechar el acceso al nivel de bloques para clonar un dispositivo, o para obtener un archivo de imagen de manera muy simple sin la necesidad de recurrir a herramientas. A modo ilustrativo se muestran algunos ejemplos a continuación:

- `dd if=/dev/sda of=/dev/sdb bs=4k` permite hacer una copia idéntica bloque a bloque del primer disco rígido en el segundo disco rígido. Para que esto sea posible el segundo disco debe tener un tamaño igual o superior al primero.
- `dd if=/dev/sdb1 of=imagen.dat bs=4k` permite generar un archivo imagen de la primera partición del segundo disco rígido.
- `dd if=imagen.dat of=/dev/sdb1 bs=4k` permite restaurar la imagen del ejemplo anterior en la primera partición del segundo disco rígido.

3. El nivel de archivos

Sobre el nivel de abstracción de bloques se halla el nivel de archivos. En este nivel la mínima unidad de tratamiento de información es justamente el “archivo” desentendiéndose de la forma en la que está compuesto (secuencia de bloques del nivel inferior). De este modo, cada operación ejecutada sobre información almacenada en un dispositivo (abrir, escribir, leer, cerrar, etc.) aplicará sobre un archivo y no sobre un bloque en particular.

Normalmente éste es el nivel a partir del cual el usuario comienza a percibir la información contenida en su equipo. La persona ve y administra sus datos siempre a través de archivos. Naturalmente estos archivos se suelen agrupar en estructuras denominadas “directorios”, pero éstos últimos también pueden contener otros directorios, llamados “subdirectorios”, conformando así una infraestructura jerárquica denominada “estructura de directorios”. Tanto para los archivos como para los directorios es necesario almacenar ciertos datos que hacen a la administración de los mismos. Por ejemplo: nombre, fecha de creación, usuario dueño, etc. Todos estos datos son lo que se conoce como “metadatos” en tanto que es información (datos) que describe los datos del usuario.

El conjunto de archivos, directorios y metadatos es lo que conforma el “Sistema de Archivos” y es todo lo que percibe el usuario cuando opera con la información almacenada en su dispositivo.

Es importante en este punto destacar que siendo que el usuario reconoce únicamente archivos y directorios, su percepción se limita a los datos que estén contenidos en el conjunto de los mismos. Pero, aun así, podría existir información valiosa para un estudio informático forense que no sea parte ni de un archivo ni de un directorio, sino que simplemente se aloje en el dispositivo, pero sin estar vinculada al Sistema de Archivos residente.

Muchas razones podrían explicar la situación previamente mencionada. Podría suscitarse por acción intencional del usuario, tratando de ocultar información, o bien podría presentarse durante el funcionamiento habitual del dispositivo.

El caso más frecuente que generaría la situación mencionada es la eliminación simple de un archivo a través de la interfaz que usualmente presenta el Sistema Operativo al usuario. Esta operación generaría al menos la desvinculación aparente de tal archivo con el Sistema de Archivos. De ese modo, con el correr del tiempo habría cada vez más probabilidad de que no quede registro alguno de su existencia y que sus bloques de contenido asociados sean sobrescritos, porque el espacio anteriormente ocupado se destina al almacenamiento de nuevos archivos. De todas maneras es posible que no todos sus bloques sean sobrescritos y que algunos de ellos aún persistan luego de un determinado tiempo. De ese modo, restos de su contenido podría hallarse aún sin ser parte del Sistema de Archivos.

Considerando lo anterior se deduce que es pertinente para el informático forense tener un dominio contundente de los conceptos que atañen a este este nivel de abstracción, el nivel de archivos. En orden a ello se profundiza a continuación en los conceptos de “archivo” y “Sistema de Archivos”.

3.1. Archivo

Cada archivo, visto naturalmente como un contenedor de información, ocupará una determinada cantidad de bloques del nivel inferior. De ese modo, el espacio reservado para tal archivo, en el dispositivo de almacenamiento persistente, será equivalente a un múltiplo del tamaño de un bloque. Desde este punto de vista el archivo puede ser visto como una secuencia de bloques que contienen sus datos.

Si bien cada archivo tendrá asignado un número entero de bloques, el mismo no necesariamente ocupará, con contenido válido, completamente todos ellos pues su tamaño

real no está vinculado al tamaño del bloque ya que se halla en un nivel de abstracción superior. El archivo debe desentenderse de las características del medio de almacenamiento en el cual se persistirá e incluso del tamaño de bloque de información que el Sistema Operativo utiliza. A continuación, se presenta una imagen ilustrativa:

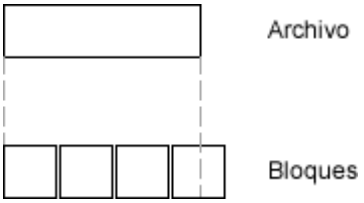


Figura 6.1: Correlación de tamaño entre archivo y bloques.

Los bloques tampoco tienen por qué encontrarse alojados físicamente en forma contigua. Cada Sistema de Archivos tiene sus propios métodos de alocación que determinan el modo en el que los bloques se almacenan en el dispositivo de almacenamiento persistente.

Cabe destacar que un bloque no puede ser utilizado por más de un archivo. El bloque se asigna única y completamente a solo uno de ellos. Frente a esto es evidente que a lo largo del dispositivo se podrán encontrar bloques ocupados parcialmente con espacio sin aprovechar, pero tampoco disponible para asignar a otro archivo. Ese espacio se conoce como “fragmentación interna” y a pesar de no poseer contenido de momento válido, es un área en donde aún podrían existir vestigios de archivos antiguos previamente almacenados con información útil para una investigación forense.

La Informática Forense debe sacar provecho de este conocimiento y contemplar los siguientes escenarios en los que independientemente de la integridad del archivo aún es posible recabar evidencia útil:

- Los bloques de un archivo no necesariamente se blanquean al eliminarlo a través del Sistema Operativo. La totalidad de su contenido aún podría persistir luego de su supresión.
- Un bloque parcialmente ocupado podría contener información útil en su espacio no utilizado.
- Los bloques de un archivo eliminado no necesariamente se sobreescriben todos al mismo tiempo con otra información. Siempre podrían hallarse fragmentos de un archivo previamente suprimido a pesar de no recuperar completamente su contenido.
- El hecho de no encontrar la información de un archivo en bloques contiguos no significa que no exista en otros distantes.

Habiendo comprendido la implicancia de la relación entre el nivel de abstracción de bloques y el de archivos se puede proseguir profundizando el concepto de archivo desde el punto de vista del Sistema de Archivos.

Formalmente un archivo puede ser definido como la "mínima unidad de representación de la información identificada unívocamente cuya administración recae en el Sistema Operativo". Partiendo de esta definición es posible extraer y ahondar en varios conceptos.

El Sistema Operativo necesita de un mecanismo para identificar los archivos unívocamente. Ya sea el nombre, la ruta de acceso sumada al nombre, un identificador oculto, etc.; pero al menos un modo de hacerlo debe tener a fin de evitar inconsistencias en la información que es el activo más importante para el usuario dentro del sistema.

Para efectuar una correcta "administración" de los archivos, el Sistema Operativo debe poder disponer de todo lo que requiera para desempeñar con eficacia dicha tarea. Esto puede comprender mecanismos e información de diversas

índoles que estarán presentes o no según el diseño del mismo. Por ejemplo, en un Sistema Operativo multiusuario es pertinente almacenar el usuario dueño de cada archivo. También corresponderá utilizar una estructura de directorios multinivel a fin de disociar lógicamente los archivos de usuarios distintos. Todo ese conjunto de convenciones que determinan el modo en el que el Sistema Operativo administra la información es lo que se conoce como Sistema de Archivos.

3.2. Sistema de Archivos

En sentido estricto un Sistema de Archivos puede definirse como el "conjunto de información organizada que habita en un volumen[201] de un dispositivo de almacenamiento.

Desde este punto de vista el Sistema de Archivos comprende datos y metadatos. Eso significa que involucra toda la información contenida en cada archivo y también todas las estructuras de datos que permiten administrarlos correctamente (por ejemplo, la estructura de directorios).

El análisis informático forense debe tener esto ciertamente presente puesto que en determinados casos la evidencia puede no hallarse en los datos sino en los metadatos de un archivo. Por ejemplo, su fecha de creación puede evidenciar el uso de un equipo en un momento indebido y sin embargo el contenido del mismo puede ser irrelevante.

Ampliando el foco de la cuestión, desde un sentido amplio el Sistema de Archivos puede definirse como el "conjunto de convenciones que se establecen en tiempo de diseño que determinan la administración de la información en un Sistema Operativo". En definitiva, es el modo que tiene un

[201] Volumen es un área de almacenamiento con un único Sistema de Archivos que típicamente reside en una única partición de un dispositivo de almacenamiento.

Sistema Operativo de administrar los datos. Conocer en profundidad estas características es menester a la hora de llevar a cabo una investigación informática forense sobre un dispositivo de almacenamiento determinado.

Actualmente existen numerosos Sistemas de Archivos pero solo algunos de ellos tienen determinado nivel de difusión que hace que estadísticamente la gran mayoría de los casos de investigación recaerá en ellos. A continuación se abordan casos particulares.

3.4. Sistema de Archivos FAT

Posiblemente uno de los Sistemas de Archivos más antiguos, pero aún en uso es FAT (o File Allocation Table). Fue diseñado en 1977 con el fin de dar soporte a los medios de almacenamiento extraíbles basados en discos flexibles (disquetes), los cuales no presentaban grandes capacidades de almacenamiento, pero a lo largo del tiempo fue extendido y utilizado sobre otros tipos de dispositivos de mayor capacidad como lo son los discos rígidos o “pen drives” habitualmente vistos hoy en día.

FAT fue y sigue siendo una solución simple y liviana de administración de archivos que requiere de una estructura significativamente menos compleja que otros esquemas como pueden ser los ejemplos que se abordarán luego (NTFS y EXT3). Por ello, es natural ver este tipo de Sistema de Archivos en medios de almacenamiento extraíbles tales como tarjetas de memoria muy frecuentemente vinculadas a dispositivos portátiles como ser teléfonos móviles o cámaras fotográficas. Frente a este escenario, para el informático forense es importante conocer también las particularidades de este Sistema de Archivos a pesar de lo antiguo que puede ser, ya que por su nivel de difusión es muy probable toparse con el mismo durante un caso de análisis.

La simpleza de FAT presenta sus ventajas y desventajas tanto desde el punto de vista de performance y

robustez para el mismo sistema como desde el de la informática forense. Si bien su esquema es relativamente fácil de interpretar, también dispone de una escasa cantidad de recursos para recuperar información eliminada. A continuación, se hará mención a cuestiones técnicas, útiles para el informático forense que se encuentre con este Sistema de Archivos.

FAT se basa en dos estructuras de datos esenciales. Una de ellas es la Tabla de Asignación de Archivos (o File Allocation Table, de allí el nombre del Sistema de Archivos) y la otra es la Entrada de Directorio (Directory Record).

El propósito de la Tabla de Asignación de Archivos es mantener la lista de bloques asignados a cada archivo. Para ello, esta tabla almacena un valor por cada bloque en todo el Sistema de Archivos. Este valor simboliza el estado del bloque y en caso de ser “asignado” representa también la referencia al bloque siguiente o bien indica que es el último bloque del archivo. Con lo cual, un registro de la Tabla de Asignación de Archivos puede tener cualquiera de los siguientes significados:

1. Bloque libre.
2. Referencia al bloque siguiente dentro del archivo.
3. Fin de archivo.

Así la Tabla de Asignación de Archivos contendrá una secuencia de bloques por cada archivo en el Sistema de Archivos.

Por otra parte, el conjunto de Entradas de Directorio sirve para mantener la estructura lógica de directorios del Sistema de Archivos. Así, en esencia, una Entrada de Directorio contendrá el nombre del archivo o directorio, su tamaño y la referencia a la secuencia de bloques plasmada en la Tabla de Asignación de archivos. A continuación se presenta una imagen ilustrativa:

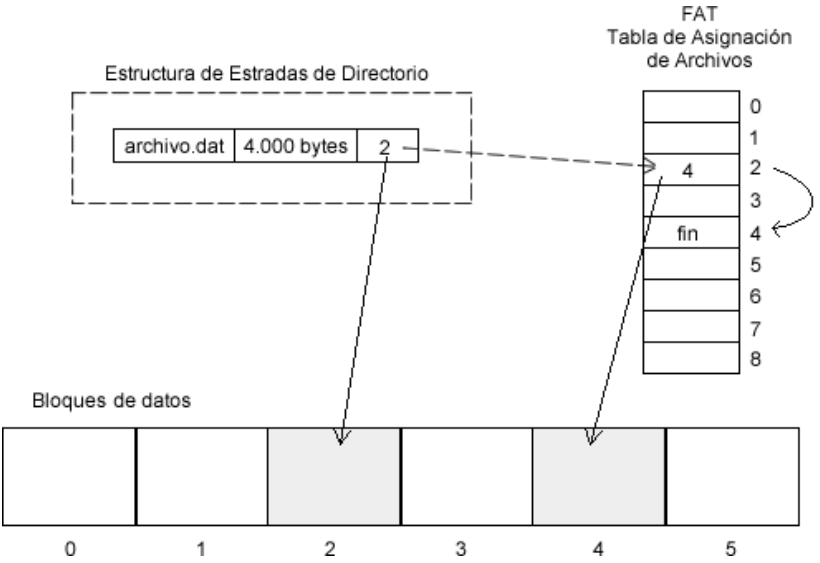


Figura 6.2: Estructura de almacenamiento en FAT para un archivo.

Como puede observarse la integridad de la cadena de bloques de cada archivo representada en la Tabla de Asignación de Archivos es imprescindible en orden a mantener la consistencia de los mismos.

Al eliminar un archivo el Sistema de Archivos recorre dicha tabla, siguiendo la secuencia asociada a tal archivo, blanqueando cada valor de la cadena, de modo que sus bloques figuren como “disponibles”. Así, la lista de bloques queda destruida pero no los bloques de datos en sí. A su vez, la entrada de directorio asociada a tal archivo se modifica indicando que la misma está disponible para ser utilizada por otro. Para ello modifica el nombre, reemplazando el primer caracter por “0xE5”.

Es lógico entonces entender que, en FAT, la información aún es recuperable luego de haber eliminado un archivo del sistema pero no siempre es un trabajo simple ya que al perder la secuencia de bloques de datos el proceso puede demandar un recorrido extenso del dispositivo de almacenamiento, en

busca de bloques no contiguos que sean parte de dicho archivo.

A nivel macro, FAT divide el volumen de almacenamiento en tres secciones físicas.

- Área reservada o de inicio
- Área de FAT
- Área de datos

El área reservada o de inicio comprende información general del Sistema de Archivos como ser las direcciones de donde comienza el área de FAT y el área de datos, la dirección del resguardo (backup) de la misma área de inicio, el nombre de la herramienta que se utilizó para crear ese Sistema de Archivos, etc…

El área de FAT contiene la Tabla de Asignación de Archivos junto a un duplicado de la misma ubicadas en forma contigua. Un aspecto ciertamente criticado ya que, ante un eventual incidente, cualquiera sea el motivo, al estar juntas es más factible que ambas queden corruptas.

Por último, el área de datos comprende todos los bloques asignables a archivos tanto de sistema como de usuario. A continuación, una imagen ilustrativa:

Figura 6.3: Distribución de áreas físicas de FAT.

Como puede verse, FAT es un esquema relativamente simple que permite una rápida interpretación pero que como contrapartida carece de estructuras que permitan una recuperación eficiente de información eliminada. A continuación, se aborda un Sistema de Archivos de mayor

complejidad que presenta distintas características en estas cuestiones (NTFS).

3.1. Sistema de Archivos NTFS

NTFS (o *New Technology File System*), visto comúnmente como el sucesor de FAT, es un Sistema de Archivos más moderno (lanzado al mercado en 1993 por primera vez), más complejo y que ofrece una significativa cantidad de mejoras basadas en las deficiencias que se fueron percibiendo sobre FAT.

Es un Sistema de Archivos que por su compleja estructura inicialmente no fue utilizado en medios de almacenamiento extraíble o dispositivos móviles, ya que mucho de lo ofrecido por NTFS solía no ser necesario ni tampoco se justificaba el espacio destinado estrictamente a estructuras administrativas propias del mismo Sistema de Archivos. A continuación, se introducen detalles técnicos de este sistema.

NTFS parte de una base completamente diferente de FAT. En él no existen divisiones estáticas del volumen. Todo el espacio de la partición es destinado para almacenar libremente tanto archivos de usuario como estructuras del propio Sistema de Archivos.

Posiblemente uno de los aspectos más distintivos de NTFS es que en él todo es un archivo, incluidas las estructuras administrativas mencionadas. Hasta la misma tabla de archivos y el sector de arranque también lo son. Siendo así, existen entonces una serie de archivos destinados exclusivamente a mantener información de toda la infraestructura necesaria. Éstos, son archivos estrictamente “de sistema” y normalmente el usuario no debería poder acceder a ellos, visualizarlos ni modificarlos. El informático forense, sin embargo, no debe dejar de tenerlos presente y acceder a ellos mediante herramientas específicas si el caso lo amerita.

A pesar de su condición especial de ser archivos estrictamente administrativos del Sistema de Archivos, no dejan de ser "archivos" y por ello deben respetar ciertos principios básicos al igual que el resto. Por ejemplo, cualquiera de ellos podría encontrarse fragmentado, cambiar de tamaño o ser ubicados en cualquier lugar el volumen. El único archivo que tiene siempre la misma ubicación y tamaño es aquel que contiene el "Registro de Arranque de Volumen" (Volume Boot Record, VBR[202]) alojado al comienzo del volumen cuyo nombre es "$Boot" (el caracter "$" indica que se trata de un archivo administrativo del *filesystem*, o meta-archivo). Esto ha sido diseñado así en orden a respetar las arquitecturas de arranque (MBR[203] y su sucesor GPT[204]) mayormente difundidas para computadores personales (PC).

Esta serie de archivos es creada inicialmente al darle formato a un volumen. Cada uno de ellos tiene un propósito específico y ocupa siempre la misma posición dentro de la tabla de archivos. Se listan a continuación:

Posición	Nombre	Propósito
0	$MFT	Es la tabla de archivos: describe todos los archivos del volumen, incluyendo los nombres,

[202] VBR es una estructura de arranque ubicada al comienzo de un volumen que contiene información descriptiva del mismo y el código necesario de inicio un Sistema Operativo alojado en dicho volumen.
[203] MBR: Es un formato de Registro de Arranque Maestro (del inglés Master Boot Record, MBR), creado por IBM y ampliamente difundido en computadoras personales (PC). Está compuesto por la tabla de particiones y el código necesario de arranque del sistema.
[204] GPT: sucesor de MBR, presenta varias mejoras, entre ellas soporta cientos de particiones, organiza mejor los tipos de particiones y permite asignar nombres y permisos a las mismas, además de permitir particiones de mayor tamaño.

		marcas de tiempo, listas de bloques asignados, índices, identificadores de seguridad, y atributos de archivo.
1	$MFTMirr	Es un duplicado de los primeros 4 registros de la tabla de archivos $MFT.
2	$LogFile	Contiene registro de transacciones de cambios en los metadatos del sistema de archivos.
3	$Volume	Contiene información sobre el volumen: el identificador del mismo, su etiqueta, la versión del Sistema de Archivos, y otros indicadores.
4	$AttrDef	Una tabla de atributos MFT que asocia identificadores numéricos con nombres.
5	.	Es el directorio raíz del Sistema de Archivos.
6	$Bitmap	Es un mapa de bits, donde cada elemento representa el estado (asignado o libre) de cada clúster del sistema de archivos.
7	$Boot	Contiene el Registro de Arranque del Volumen (Volume Boot Record).
8	$BadClus	Es un registro de bloques

		que presentan inconvenientes y no deben utilizarse.
9	$Secure	Contiene una base de datos de descriptores de seguridad (Listas de Control de Acceso) comunes a múltiples archivos con el fin de evitar su replicar dichos descriptores por cada archivo.
10	$UpCase	Contiene la versión mayúscula de cada caracter codificado en Unicode
11	$Extend	Es un directorio que contiene varios archivos de sistema opcionales tales como $Quota, $ObjId, $Reparse o $UsnJrnl, listados a continuación.
12–23	Posiciones reservadas para registros de extensión de otros listados previamente. Es requerido un registro de extensión cuando todos los atributos vinculados a un archivo no caben en un solo registro. Esto podría ocurrir cuando el archivo se encuentra demasiado fragmentado y su lista de bloques es muy numerosa, cuando tiene un nombre excesivamente largo, cuando posee un descriptor de seguridad significativamente extenso y en otras situaciones menos	

	frecuentemente vistas que hacen que todos los metadatos no quepan en el mismo registro.	
24	$Extend\$Quota	Contiene información de la cuota de espacio en disco destinada a cada usuario.
25	$Extend\$ObjId	Contiene una lista de atributos de un tipo específico empleados en el volumen.
26	$Extend\$Reparse	Guarda información administrativa del volumen tales como puntos de montaje.
27—	Comienzo de los registros de archivos de usuario.	

Tener presente este compendio de archivos de sistema es esencialmente importante cuando se realice un análisis forense sobre NTFS, ya que toda operación efectuada sobre un archivo de usuario impacta en mayor o menor medida sobre los mismos.

El escenario más habitual es la eliminación de un archivo. Cuando el usuario ordena su supresión definitiva el sistema de archivos lo marca como eliminado en su tabla de archivos $MFT, pero no blanquea ni sus datos ni sus metadatos. Simplemente marca como disponible tanto los bloques que ocupaba como su registro en la $MFT. De este modo, la información se destruirá completamente cuando un nuevo archivo ocupe su registro MFT y sus bloques sean sobrescritos.

Nótese que, a diferencia de FAT, luego de la eliminación de un archivo la lista de bloques que lo componen aún persiste. En NTFS no es necesario destruir la cadena de

bloques asociada para indicar que los mismos están disponibles ya que esto se realiza a través del uso del meta-archivo $Bitmap.

El siguiente esquema presenta el estado del Sistema de Archivos antes de eliminar un archivo de ejemplo “MiArchivo.txt”.

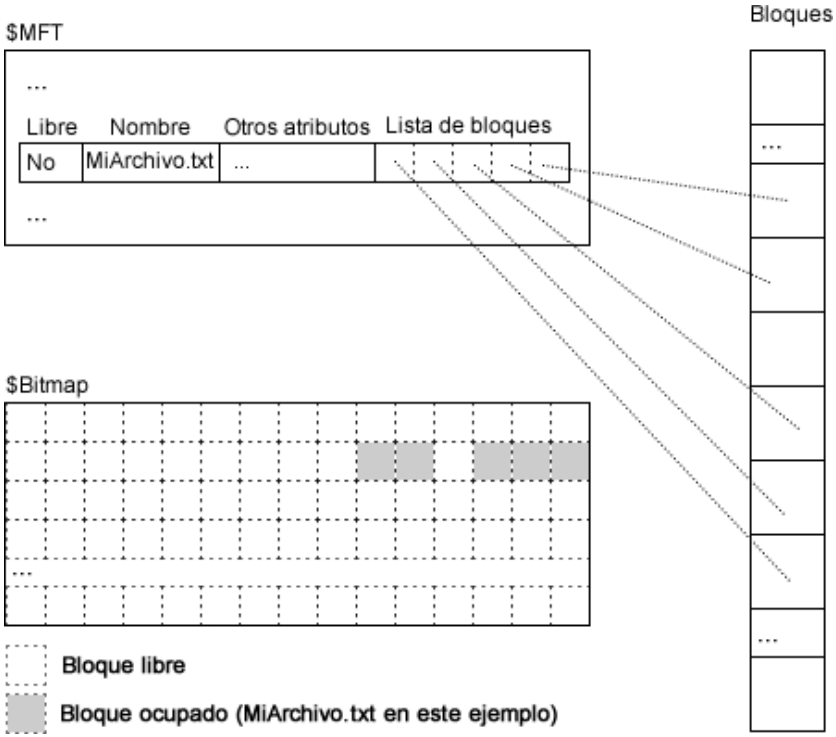


Figura 6.4: Estado de estructuras de archivos de NTFS previo a eliminar un archivo.

A continuación, se muestra el estado del Sistema de Archivos luego de la eliminación del archivo:

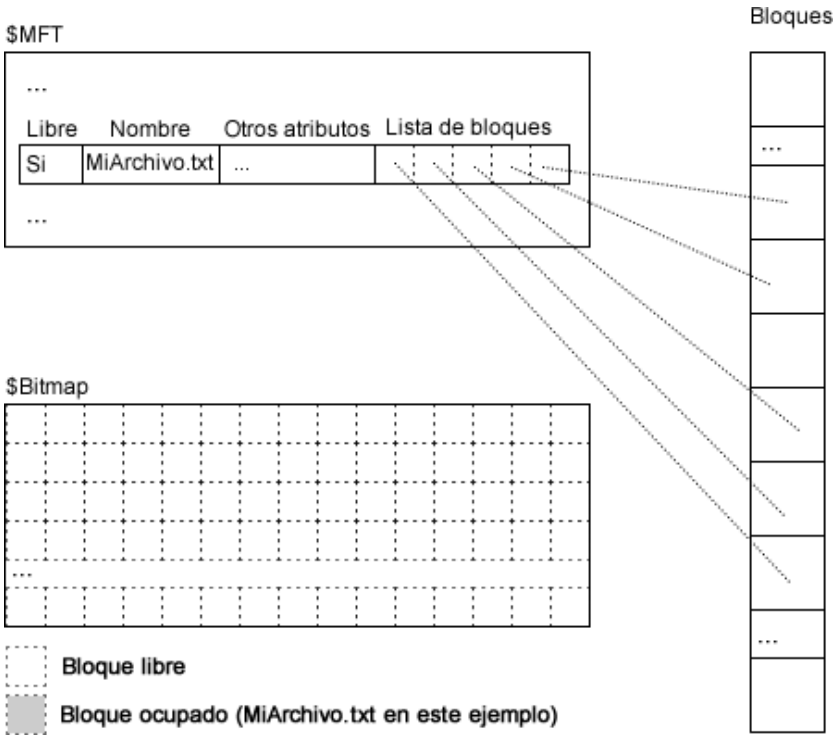


Figura 6.5: Estado de estructuras de archivos de NTFS luego de eliminar un archivo.

Véase que el cambio requerido es mínimo y dejando a un lado los beneficios de rendimiento la ventaja rescatable es que, como se observa, la totalidad de los datos y metadatos aún persisten en el dispositivo luego de la eliminación.

Otro recurso de NTFS es su registro de transacciones implementado en $LogFile, el cual almacena información de cada operación sobre los archivos y sus metadatos. Para prevenir que el mismo crezca indefinidamente con el uso prolongado del sistema, este registro tiene un tamaño máximo, y se comporta como un registro circular, en el que se reutilizan los registros iniciales una vez alcanzado el tamaño máximo.

El contenido completo de un archivo podría reconstruirse sin realizar una búsqueda extensa en todo el volumen, aún si se eliminara su entrada en la tabla $MFT, dado que la cadena de bloques aún se encuentra en el registro transaccional. Si el archivo hubiera sido completamente eliminado, aún podrían existir vestigios de su presencia a través de la secuencia de operaciones registrada por este mecanismo.

El objetivo de esta sección es solo dar una introducción al análisis de los metadatos, para ampliar en la temática se recomienda consultar la bibliografía de Brian Carrier.

3.1. Sistema de Archivos EXT3

EXT3 es el Sistema de Archivos por defecto de la mayoría de las distribuciones del Sistema Operativo Linux. Es una versión modernizada de EXT2 que agrega control de transacciones pero que aún mantiene la estructura básica original de su predecesor.

“EXT” es el acrónimo de “Extended File System” y, en este caso, “3” implica que se trata de su tercera versión. Originalmente el primero de ellos (EXT) fue diseñado en base al Sistema de Archivos UFS (Unix File System) el cual fue creado poniendo el foco en performance y seguridad. Lógicamente tales principios también se tomaron en la construcción de EXT.

En EXT existen copias de estructuras de metadatos a lo largo de todo el volumen lo cual provee los siguientes beneficios: si un conjunto de metadatos se daña cualquiera sea la razón, con este esquema, siempre habrá una réplica del mismo permitiendo así una significativa resistencia a errores. En este mismo escenario, cuando un daño físico ocurre en el dispositivo, el mismo suele abarcar bloques contiguos. Siendo así, al fraccionar y distribuir los metadatos en lugares distantes es más probable que el daño se limite a solo una parte de ellos. Por otra parte, el hecho de distribuir

los metadatos a lo largo del volumen facilita que los datos y sus metadatos se encuentren en las cercanías. De ese modo en dispositivos de almacenamiento de tipo “disco rígido” el incremento de performance es considerable ya que el lector precisa recorrer menos distancia desde los metadatos hasta los datos.

La organización de EXT comienza con una zona reservada al sector de arranque e información descriptiva del Sistema de Archivos, y el resto del volumen está dividido en secciones, que se denominan grupos de bloques. Todos los grupos de bloques, excepto el último, contienen el mismo número de bloques, que se utilizan para almacenar nombres de archivo, metadatos, y contenido de archivos. La información básica de EXT se encuentra almacenada en una estructura de metadatos ubicada al comienzo del volumen llamada “súper bloque”.

Los metadatos de cada archivo y directorio se almacenan en un registro llamado “inodo”, que tiene un tamaño fijo y se encuentra en una estructura llamada “tabla de inodos”. Hay una tabla de inodos en cada grupo de bloques.

El nombre de un archivo se almacena en una “entrada de directorio”, que es situada en los bloques asignados al directorio principal del archivo. Una entrada de directorio es una estructura de datos simple que contiene el nombre del archivo y un puntero a su registro inodo.

La relación entre la entrada de directorio, inodo y bloques puede verse en la siguiente figura:

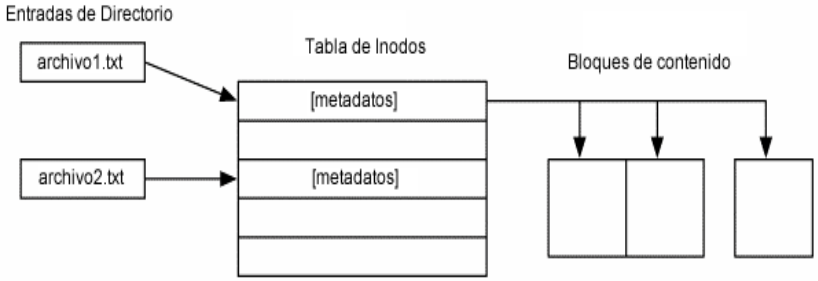


Figura 6.6: Estructura de archivos simplificada de EXT3.

Es importante tener presente este sencillo esquema ya que a simple vista puede observarse que en una situación análoga a la de NTFS, el archivo podría ser eliminado de su directorio, pero aún permanecer íntegramente en el dispositivo.

Para plantear en detalle un caso de eliminación de un archivo es necesario conocer en mayor nivel de profundidad la infraestructura de Ext3.

Como se mencionó, a nivel general la estructura de Ext3 está compuesta por un área inicial descriptiva del volumen seguida de grupos de bloques que contienen datos y metadatos de los archivos, como se muestra a continuación:

Figura 6.7: Distribución de estructuras de EXT3.

El superbloque contiene información básica del Sistema de Archivos tal como el tamaño de bloque, la cantidad de bloques por grupo de bloques y el número de bloques reservados antes del primer grupo de bloques. También contiene entre otros datos el número total de inodos y la cantidad de inodos por grupo de bloques.

Cada grupo de bloques está compuesto de la siguiente manera:

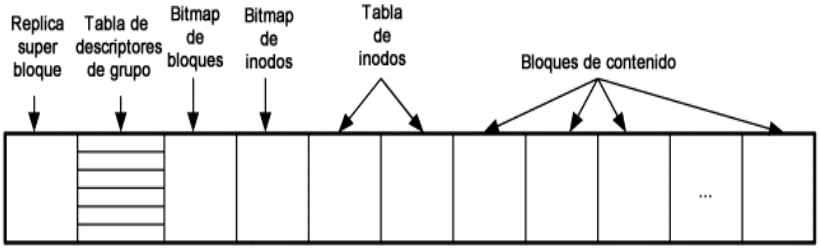


Figura 6.8: Estructura de grupo de bloques de EXT3.

Como se observa en la figura, cada grupo de bloques está compuesto por una réplica del superbloque, una tabla de descriptores de grupo que contiene la información descriptiva de cada uno de ellos, un mapa de uso de bloques (bitmap de bloques) que indica la disponibilidad de cada uno de ellos, un mapa de uso de inodos (bitmap de inodos) que es análogo al anterior, la tabla de inodos y finalmente los bloques que almacenan el contenido de los archivos.

Cuando un archivo se elimina un conjunto de operaciones sobre estas estructuras se realiza. El primer paso que efectúa el Sistema de Archivos es ubicar la entrada de directorio, procesarla y marcarla como eliminada. A través de la entrada de directorio accede al inodo del archivo y lo marca también como suprimido. Luego modifica el bit correspondiente en el mapa de inodos indicando así que ese inodo se encuentra disponible para su uso en otro archivo. Finalmente leyendo en el inodo la información de los bloques asociados indica en el bitmap de bloques que los mismos ahora están libres.

En toda esta secuencia de operaciones ni los datos ni la mayoría de los metadatos del archivo son destruidos. Aun cuando el archivo se encuentra técnicamente removido del Sistema de Archivos, la cadena de bloques se encuentra intacta hasta tanto sea sobrescrita.

4. Gestión de memoria principal

La memoria principal es uno de los recursos más importantes de la computadora. Su correcta administración es fundamental para lograr eficiencia en el aprovechamiento de todos los recursos. En esta sección se describe la memoria principal, la necesidad de su gestión y las diferentes abstracciones que se suelen emplear para implementarla. Finalmente se concluye con un ejemplo práctico.

4.1. La memoria principal

Se denomina memoria principal a una memoria de acceso aleatorio, de velocidad similar a la del procesador, conectada directamente al mismo a través del *bus interno*[205] de la computadora. Se la conoce habitualmente como memoria RAM (*Random Access Memory*) haciendo alusión a una de sus características más importantes. Debido a una limitación tecnológica histórica la memoria principal es volátil, es decir, requiere energía para mantener los datos almacenados y por lo tanto cuando la computadora se apaga los datos contenidos en la misma se pierden. Por esta razón se la utiliza normalmente para guardar temporalmente la información que los programas necesitan durante su ejecución.

La memoria principal puede verse como un gran casillero donde cada casilla puede guardar un dato de una cantidad fija de bits (normalmente ocho bits). Cada casilla está identificada con un número que comienza en 0 y se incrementa linealmente. A este número se lo conoce como dirección de memoria. Para leer un dato de la memoria el procesador debe indicar una dirección, y la memoria le devolverá el dato almacenado en la casilla indicada. Para

[205] El bus interno está formado por un conjunto de pistas o cables que transfieren bits en paralelo a una gran velocidad, comparable a la del procesador y a la de la memoria principal.

escribir un dato en la memoria el procesador debe indicar una dirección y el dato que se desea guardar, y la memoria procederá a almacenar el dato en el casillero indicado. La figura siguiente muestra un esquema representativo de la memoria principal.

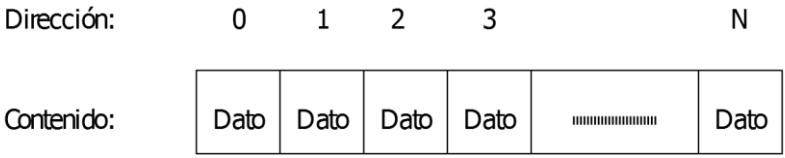


Figura 6.9: Representación esquemática de la memoria principal.

Desde el mismo momento en que muchos programas diferentes se ejecutarán en forma concurrente, la memoria principal debe gestionarse para que todos los programas puedan utilizarla sin interferirse entre sí, básicamente impidiendo que dos programas distintos utilicen la misma casilla de memoria al mismo tiempo. Las técnicas de gestión de memoria han ido evolucionando con el tiempo y los procesadores fueron incorporando características que permiten implementarla de manera muy eficiente y garantizar la protección de la misma.

4.2. Paginación

Una de las técnicas más utilizadas para gestionar la memoria principal es dividirla en casilleros de tamaño fijo (por ejemplo, grupos de 4096 casillas), denominados *páginas*, que el Sistema Operativo puede asignar a los distintos programas.

Los procesadores modernos poseen Unidades de Manejo de Memoria (MMU) que implementan la paginación utilizando el concepto de *dirección lineal* de memoria. El esquema de direcciones lineales crea una abstracción donde cada programa “cree” que dispone de toda la memoria para sí mismo. La MMU por su lado traduce cada dirección lineal en una dirección física (o real) antes de acceder a la memoria consultando a una estructura conocida como “tabla de

páginas". Cada programa tiene su propia tabla de páginas, y las mismas son administradas por el sistema operativo. La dirección lineal se divide en dos partes: la primera parte contiene el número de página, y la segunda parte, conocida como *desplazamiento*, indica la casilla dentro de la página. La figura 6.10 muestra un ejemplo sencillo de paginación. Pueden verse dos programas, cada uno de los cuales tiene 2000 direcciones asignadas. Estas direcciones lineales van para cada programa desde 0000 hasta 1999. También puede verse un ejemplo de la asignación de la memoria física, que tiene 4000 direcciones en total, junto con la tabla de páginas de cada programa que define esta asignación. En la figura se utilizan números decimales redondos para graficar el concepto (por ejemplo, 1000 casillas por página). En la práctica las computadoras utilizan números redondos en binario (por ejemplo 2^12 = 4096 casillas por página).

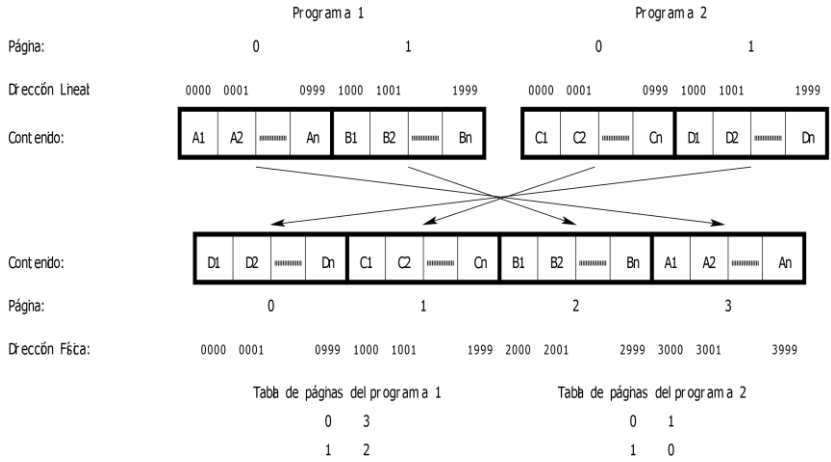


Figura 6.10: Ejemplo sencillo de un esquema de paginación

Los esquemas de paginación permiten la asignación de páginas completas a los programas. Por lo tanto si la cantidad de memoria necesitada por el programa no es múltiplo exacto del tamaño de página entonces habrá una porción de memoria que no podrá ser aprovechada ni por este programa

ni por ningún otro. A este fenómeno se lo conoce como *fragmentación interna*, y acota la cantidad de memoria desaprovechada a un máximo del tamaño de página menos una casilla de memoria por programa.

Entre las ventajas de la paginación se pueden por lo tanto nombrar:

- Desperdicio de memoria acotado.
- Alta flexibilidad a la hora de gestionar: cualquier página de memoria física puede ser asignada a cualquier programa en cualquier orden.
- El acoplamiento entre los programas es prácticamente nulo, dado que cada uno tiene su propio espacio de direcciones para administrar libremente.
- El esquema permite crear políticas de protección, (por ejemplo, haciendo que determinadas páginas sean de 'solo lectura').
- El esquema permite compartir páginas físicas entre varios programas de manera sencilla, optimizando el uso de la memoria y permitiendo implementar mecanismos seguros de comunicación entre procesos.
- El esquema permite implementar Memoria Virtual.

Entre las desventajas de la paginación se pueden nombrar:

- Requiere soporte en hardware. El esquema sería inaceptablemente lento sin este soporte.
- Un solo espacio de direcciones, si bien es natural, no ofrece ningún valor agregado al nivel superior. Queda a cargo del compilador o el intérprete la gestión total de ese espacio de direcciones.

De la primera de las desventajas se puede decir que hoy no es realmente un problema. Los procesadores modernos

vienen equipados con potentes MMU que trabajan en cooperación con el Sistema Operativo para lograr un esquema de paginación muy eficiente. Para la segunda desventaja la solución que se aplicó históricamente es el esquema de segmentación que se describe a continuación.

4.3. Segmentación

En el uso práctico un programa necesita la memoria para tres cosas diferentes:

1. *Para sus instrucciones*: El procesador lee las instrucciones de código máquina de la memoria principal, las carga y las ejecuta una por una. Por esta razón el texto (o código) del programa tiene que estar almacenado en ella antes de poder ejecutarse.
2. *Para sus datos*: Las variables alojadas estáticamente (globales) que utilizan los programas para funcionar tienen que tener un espacio reservado en la memoria principal.
3. *Para la pila*: La mayoría de los lenguajes modernos poseen variables alojadas automáticamente (locales), así como también utilizan llamados a subrutinas (para implementar funciones, procedimientos o métodos). Todas estas construcciones dependen de una estructura de pila que se guarda en memoria principal.

Un servicio que puede ofrecer el Sistema Operativo es asignar a cada programa conjuntos de celdas contiguas de diferentes tamaños. Cada conjunto, denominado en este caso *segmento*, tiene un identificador, una dirección de inicio, conocida como *base*, y una *longitud*. De esta forma el compilador o intérprete puede solicitar al sistema operativo un segmento de código, un segmento de datos y un segmento de pila, cada uno del tamaño que necesite, y de esta forma simplificar de manera sensible su implementación.

La segmentación se implementa en procesadores y sistemas operativos modernos de manera similar a como se implementa la paginación, utilizando tablas, que en este caso se llaman tablas de segmentos o tablas de descriptores (de segmento). Se citan a continuación las diferencias más importantes entre la segmentación y la paginación:

- El tamaño de las páginas es fijo y uniforme, mientras que el de los segmentos es variable. Con el correr del tiempo, y en la medida en que segmentos de diferentes tamaños son ocupados y liberados de la memoria, se van produciendo huecos de memoria libre entre la memoria ocupada. A este fenómeno se lo denomina *fragmentación externa*, y lamentablemente no tiene cota. Podría ocurrir que en algún momento se requiera un segmento que no entra en ningún hueco, pero que podría entrar en la memoria libre si ésta estuviera contigua.

- En la segmentación los programas indican la dirección de memoria como un identificador de segmento y un desplazamiento dentro de éste. En la paginación la dirección se indica como un único número.

- Es normal que los datos almacenados en un mismo segmento sean de la misma naturaleza (ej. segmento de código, o segmento de datos), por lo que implementar protección de acceso es mucho más natural y efectivo en un esquema de segmentación que en uno de paginación. Por ejemplo: el código se puede leer y ejecutar, pero no se puede escribir mientras que los datos se pueden leer y escribir, pero no se pueden ejecutar.

La conclusión final es que la segmentación es más abstracta que la paginación, y por lo tanto ofrece un mejor servicio al compilador / intérprete. Sin embargo, la segmentación es menos eficiente en el aprovechamiento del espacio que la paginación.

4.5. Segmentación con paginación

Combinando las técnicas de segmentación y paginación muchos sistemas operativos y procesadores buscan combinar sus ventajas y así ofrecer un mejor servicio. En esta combinación los programas acceden a la memoria indicando un identificador de segmento y un desplazamiento dentro de éste. A esta combinación se la suele llamar *dirección lógica*. La MMU buscará el descriptor del segmento en la tabla de descriptores de segmento. Allí obtendrá la base y la longitud del segmento. Primero verificará que el desplazamiento no supere la longitud, y luego sumará la base y el desplazamiento para obtener una dirección lineal. Esta dirección lineal será convertida en dirección física utilizando un esquema de paginación. La figura 6.11 muestra esquemáticamente estos pasos.

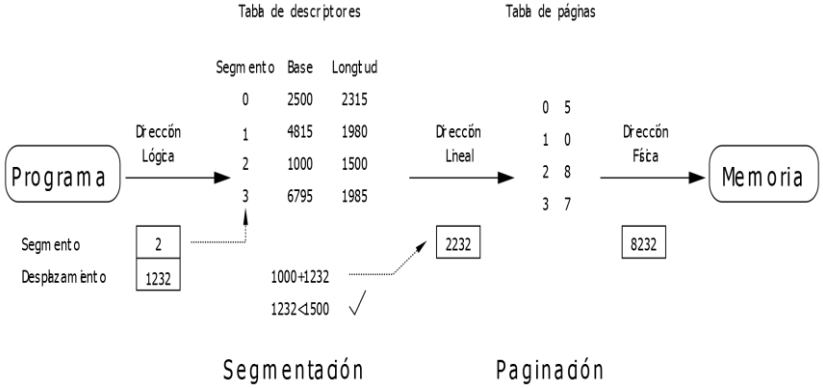


Figura 6.11: Conversión de una dirección lógica en una dirección física en un esquema de segmentación con paginación.

En resumen, la segmentación con paginación ofrece las siguientes ventajas:

- El nivel de abstracción es más adecuado para los compiladores o intérpretes.
- La protección de memoria se puede implementar con mayor nivel de precisión, por poseerse conocimiento

de la naturaleza de los datos almacenados en cada segmento.

- Los segmentos pueden crecer dinámicamente a medida que los programas lo requieran.
- La gestión del espacio es eficiente, solamente se experimenta fragmentación interna. La fragmentación externa es eliminada por el esquema de paginación.
- Se puede implementar memoria virtual en forma transparente al programa.

El esquema de segmentación con paginación está disponible en la mayoría de los procesadores y sistemas operativos modernos, aunque no siempre se utiliza en su totalidad.

4.6. Memoria Virtual

Muchos programas utilizan una gran cantidad de memoria principal, pero no la utilizan toda al mismo tiempo. Por ejemplo, si se está realizando una operación que tiene varios pasos consecutivos, se podría cargar cada paso en memoria, ejecutarse y luego descargarse, ahorrando de esta manera memoria principal. En el pasado esto era necesario en muchas aplicaciones que requerían más memoria de la que la máquina disponía. En aquel entonces los programadores debían lidiar con este problema directamente, creando los programas en partes (denominadas *overlays*) que se cargaban y descargaban consecutivamente. Hoy ya no es necesario recurrir a estas técnicas gracias a la Memoria Virtual.

Se denomina Memoria Virtual a la capacidad que tienen los sistemas operativos modernos de asignar a un programa una cantidad de memoria mayor a la presente físicamente en la máquina, y utilizar memoria secundaria (un disco rígido, por ejemplo), para almacenar el excedente. Los sistemas operativos modernos aprovechan el esquema de paginación

para hacer este trabajo de manera transparente a los programas. Cuando la memoria física se llena, entonces el sistema operativo copia varias páginas de la memoria al disco, liberando espacio. Para las páginas desalojadas de la memoria se hace una indicación en la tabla de páginas. Si la página fuera necesitada nuevamente, la MMU detecta esta marca y genera un *fallo de página*. El programa que necesitaba la página es suspendido y el sistema operativo vuelve a copiar la página a la memoria principal antes de permitirle continuar su ejecución normal.

Este mecanismo no reemplaza a la memoria física. El acceso al disco es de diez mil a un millón de veces más lento que el acceso a la memoria física. Si el sistema está funcionando con poca memoria física entonces el sistema operativo empieza a consumir su tiempo en copiar permanentemente páginas del disco a la memoria y de la memoria al disco. Este fenómeno conocido como *trashing* genera la sensación al usuario de que la máquina dejó de funcionar. En realidad la máquina está funcionando de diez mil a un millón de veces más lento, que a los fines prácticos desde el punto de vista del usuario final es la misma cosa. Para evitar este fenómeno se debe añadir memoria física a la máquina o reducir la cantidad de programas que se ejecutan de manera concurrente.

Para el analista forense el estudio de la zona del disco que el Sistema Operativo utiliza para copiar páginas de memoria desalojadas, denominada *área de intercambio*, puede ser crítico a la hora de obtener información sobre los programas que se ejecutaban cuando la máquina fue desconectada. El área de intercambio suele implementarse en particiones de disco o en archivos de ubicación conocida.

4.5. Ejemplo práctico: Gestión de memoria principal en Windows

Windows provee a cada proceso un espacio de memoria virtual privado, que representa el espacio de memoria utilizado por cada proceso.

Todas las estructuras en memoria poseen información expresada en direcciones virtuales. Por ejemplo, los procesos, almacenan en su correspondiente estructura _EPROCESS el puntero al siguiente proceso en la lista de procesos activos; también, el puntero al proceso que lo antecede en dicha lista. En ambos casos, lo que se encuentra almacenado en la estructura en memoria es una dirección virtual.

Dicho esto, resulta necesario realizar constantes traducciones de direcciones virtuales a físicas, para realizar cualquier tipo de análisis de un volcado de memoria y poder desplazarse a través del mismo.

Como se ve en la tabla 1, en Windows x86, el desplazamiento (ubicación) por defecto del *kernel* es 0x80000000, pero si se utiliza la configuración con *4-gigabyte tuning* (4GT) habilitado, el desplazamiento es 0xC0000000.

Tabla 1: *Layout* del espacio de memoria virtual en Windows x86, para cada proceso.

User Space	(0x00000000 a 0x7FFFFFFF)	2 GB
System Space	(0x80000000 a 0xFFFFFFFF)	2 GB

Windows x86

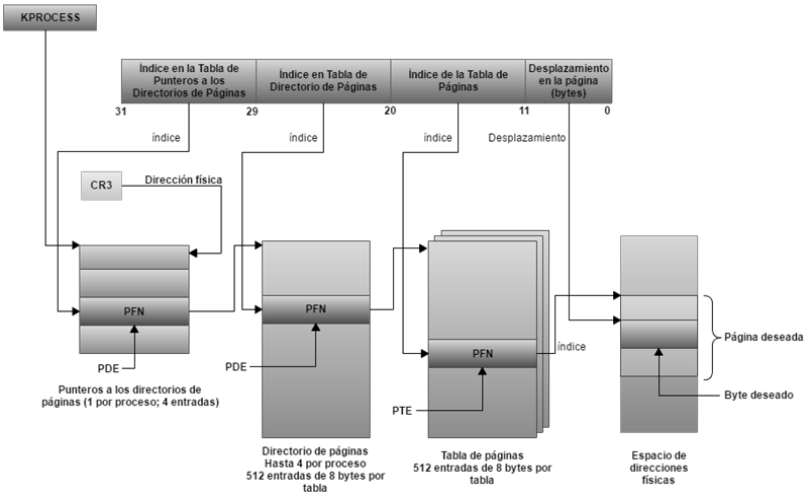


Figura 6.12: Dirección lineal en x86 (PAE habilitado)

La implementación de memoria virtual en x86 corresponde a una tabla de páginas muy grande. Por este motivo, en la traducción de direcciones lineales a físicas hay diferentes tablas involucradas. En particular, para el caso de x86 con PAE[206] (*Physical Address Extension*) habilitado, dichas tablas son:

- Page Directory Pointers Table (PDPT)
- Page Directory Table (PDT)
- Page Table (PT)

[206] *Physical Address Extension* (PAE) es una implementación que permite a sistemas operativos de 32 bits el acceso de hasta 64 GB de memoria física, cuando para procesadores Intel x86 sin PAE habilitado, el acceso es de hasta 4 GB. Esto es posible gracias a que se agrega un nuevo nivel de indirección con al existencia de la Tabla de Punteros a Directorios de Página (*Page Directory Pointers Table*) con cuatro entradas. Este capítulo se enfoca en x86 con PAE habilitado, dado que en la práctica es la implementación más utilizada en dicha arquitectura.

Como se puede ver en la figura 6.12, la dirección lineal se la puede dividir en distintas porciones donde cada una de ellas representa un índice en cada una de estas tablas según corresponda, excepto con los 12 bits menos significativos que representan el desplazamiento en bytes dentro de una página en memoria física.

Para poder comenzar con el proceso de traducción, se debe conocer la ubicación de la base de la primera tabla involucrada en la traducción*: Page Directory Pointers* Table. Esta dirección (física, por cierto) es conocida como *Directory Table Base* (DTB) y se encuentra almacenada en el registro de procesador CR3, el cual es utilizado cuando el direccionamiento virtual está habilitado, y de esta manera, contando con el valor de DTB y sumándole a éste el valor representado por los dos bits más significativos de la dirección virtual (bits 31 y 30), se obtiene la ubicación de la entrada en la PDPT donde se encuentra la dirección de la base de PDT en cuestión. Sobre esta entrada se deben descartar los últimos 12 bits (considerarlos como ceros) para tener la verdadera ubicación de la base de la PDT. Tomando como origen de referencia esta última ubicación y sumándole el valor representado por la porción de la dirección virtual entre los bits 29 al 21 inclusive, se obtiene la ubicación de la entrada a PDT en cuestión. En dicha entrada se encuentra un valor al que se le deben descartar los últimos 12 bits para calcular así la dirección de la base a la PT involucrada en la traducción. Siguiendo con el mismo mecanismo, pero utilizando ahora los bits 20 a 12 inclusive, se obtiene la dirección física de la página correspondiente. Los últimos 12 bits son los que expresan el valor del desplazamiento dentro de la página localizada, y con esto, la ubicación en el espacio de direcciones físico.

Los últimos 12 bits de la *Page Table Entry* (PTE) ofrecen información fundamental para poder realizar una traducción exitosa. En la figura 6.15 puede verse el significado de cada uno de los bits (o *flags*).

Un bit de mucha importancia para la obtención e interpretación correcta de las páginas, es el bit *Large Page*, si estuviera en 1, significa que se está en presencia de páginas más grandes que la estándar de 4KB: páginas de 2MB para arquitecturas x86 con PAE habilitado ó 4 MB para arquitecturas x86 tradicionales. Además, en el proceso de traducción se debe realizar una indirección menos cuando se trata de este tipo de páginas.

En el caso del bit *Valid*, si éste se encuentra en 1, indica que la página en cuestión es válida.

Windows x64

En una arquitectura de 64 bits, el mecanismo es similar, con la diferencia de que se agrega un nivel más de indirección y aparece una nueva tabla involucrada en la traducción llamada *Page Map Level 4* (PML4).

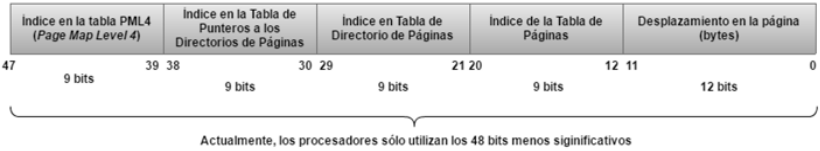


Figura 6.13: Estructura dirección lineal en x64.

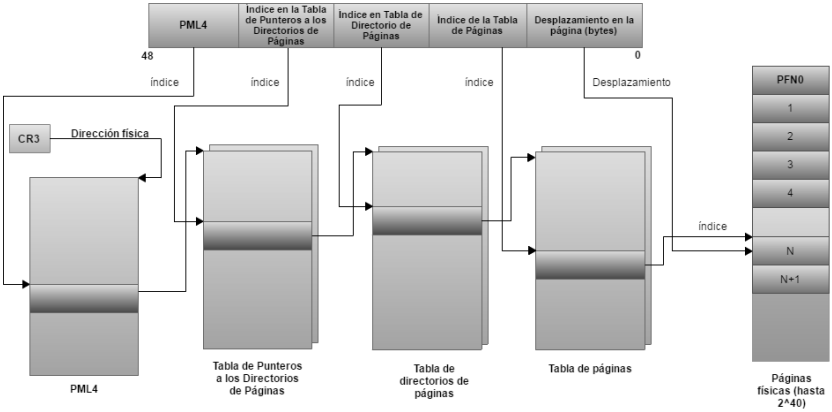


Figura 6.14: Dirección lineal en x64.

Si bien las direcciones lineales poseen 64 bits, en la práctica, sólo se utilizan los 48 bits menos significativos, como se muestra en la figura 6.13. Distintos grupos de bits de la dirección lineal, representan desplazamientos en las correspondientes tablas involucradas en la traducción de direcciones virtuales a físicas.

De manera análoga a la arquitectura x86, las entradas en las *Page Tables* (PTEs), brindan información importante para el proceso de traducción. En la figura 6.14 se muestra en detalle la estructura de una entrada en la *Page Table*:

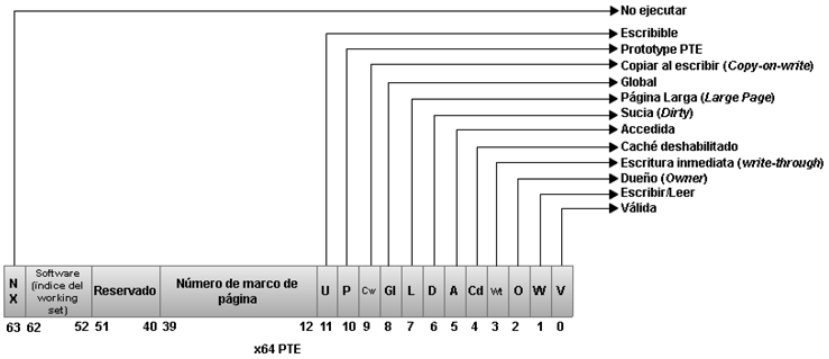


Figura 6.15: Estructura de una PTE en Windows x64.

5. Gestión de procesos

Tal como se describiera en la primera sección de este capítulo, para que los recursos de una máquina moderna puedan ser aprovechados correctamente, es necesario que el Sistema Operativo implemente la ejecución de varios programas de manera concurrente. En este capítulo se describe la abstracción propuesta por el sistema operativo para un programa en ejecución, denominada *proceso*, así como también los mecanismos utilizados para gestionarla.

Procesos

Cuando se hace referencia a un programa normalmente se piensa en un software representado en algún medio físico. El concepto de programa es inherentemente estático. Cuando se le solicita al sistema operativo que ejecute un programa, éste debe cargar su texto y sus datos a la memoria principal. Es en este momento cuando comienza la vida de un *proceso*. El proceso es un concepto inherentemente dinámico, que referencia a un programa en ejecución. El proceso vivirá dentro del sistema operativo hasta que el programa termine, ya sea naturalmente o cuando sea forzado a terminar.

Puede pensarse un proceso como un conjunto de instrucciones que se ejecuta secuencialmente, en una «CPU virtual» exclusivamente para él. En la práctica la CPU real debe conmutar entre todos los procesos del sistema operativo, repartiendo su tiempo entre ellos. Cada proceso al entrar debe encontrar la CPU exactamente en el mismo estado en que estaba cuando salió la última vez, creando de esta manera la ilusión de una CPU propia. A fin de llevar cuenta de todos los procesos el sistema operativo implementa la tabla de procesos.

5.1. La tabla de procesos

Cada proceso existente tiene durante toda su vida un lugar asignado en la tabla de procesos. La tabla de procesos es una estructura donde cada entrada representa el estado interno de un proceso. En la entrada se guarda una representación de la asignación de memoria del proceso (tabla de descriptores / tabla de páginas), el nombre del programa que está ejecutando, el estado del proceso, los archivos que el proceso tiene abierto, el estado del proceso, la prioridad del proceso, el identificador del proceso padre e información contable.

Cada proceso se identifica unívocamente por el número de entrada en la tabla de procesos. A este número se lo llama identificador de proceso.

La tabla de descriptores y la tabla de páginas se utilizan para acceder a la memoria primaria del proceso tal como se describió en la sección de gestión de memoria principal.

El estado del proceso indica si el mismo está en la CPU, o está preparado para entrar a la misma, si está en espera de entrada / salida, o si se encuentra pausado.

La prioridad del proceso hace referencia a un parámetro utilizado en la planificación, descrita más abajo.

Cada proceso normalmente es iniciado desde otro proceso, mediante una llamada al sistema. De esta manera, todo proceso tiene un proceso «padre», aquel que le dio origen. El identificador del proceso padre se guarda en la entrada de la tabla de procesos. Dependiendo del sistema operativo puede haber uno o varios procesos iniciados por el mismo sistema operativo y por lo tanto no tienen proceso padre.

Entre la información contable que se guarda el tiempo que el proceso ha estado en la CPU, la fecha y hora en que el proceso se inició, la cantidad de memoria primaria que utiliza, y la cantidad de veces que el proceso ha entrado a la CPU.

5.2. Planificación de procesos

Una de las tareas fundamentales del sistema operativo es la de repartir de una manera justa el tiempo de la CPU entre todos los procesos que están listos para entrar en ella. Se denomina Planificador de CPU al componente del sistema operativo que se encarga de esta tarea, y siguiendo diferentes estrategias busca los siguientes objetivos:

- Maximizar el tiempo que la CPU está en uso
- Maximizar la cantidad de procesos atendidos en la unidad de tiempo (*throughput*).
- Minimizar el tiempo que los procesos están en espera por la CPU (latencia).
- Evitar que un proceso nunca pueda acceder a la CPU (inanición).

Entre las estrategias clásicas de planificación se pueden mencionar las siguientes:

- *Orden de llegada o FIFO (First In First Out)*: es una sencilla estrategia que ordena los procesos listos para recibir la CPU por orden de llegada, de manera que el primero que estuvo listo es el primero que recibe la CPU. Su ventaja más importante es la simplicidad, sin embargo no es muy efectiva. No minimiza el throughput ni la latencia y un proceso largo que no requiere entrada / salida puede monopolizar la CPU, evitando que los otros procesos sean atendidos.

- *Round Robin (RR)*: es una estrategia que normalmente se combina con otras. Consiste en asignarle a cada proceso período de tiempo. Si el proceso no devuelve la CPU en el período asignado entonces es retirado de la CPU por el sistema operativo y vuelve a entrar a la cola de procesos listos. La ventaja más importante que tiene es que evita la monopolización de la CPU, y a pesar de que reduce la latencia, no consigue una solución óptima desde el punto de vista de los

procesos, porque aunque reparta el tiempo en partes iguales, no todos los procesos tienen la misma necesidad de tiempo de CPU.

- *Prioridades*: una estrategia en la que a cada proceso se le asigna una prioridad, y el proceso listo que tenga la prioridad más alta ingresa a la CPU. Existe la variante sin desalojo, que entrega la CPU al proceso listo con prioridad más alta cuando esta se desocupa, y la variante con desalojo que ni bien un proceso con prioridad más alta está listo, el proceso que está dentro de la CPU es desalojado por el sistema operativo para cederle la CPU. Normalmente la variante con desalojo se utiliza en sistemas de tiempo real, donde existen procesos que requieren tiempos de respuesta acotados. Esta estrategia en general es buena solamente si se asignan correctamente las prioridades, y puede causar inanición de los procesos con las prioridades más bajas.
- *Trabajo más corto primero (Shortest Job First, SJF)*: una estrategia que propone entregar la CPU al proceso listo que requiera menor cantidad de tiempo. Es la estrategia ideal en términos de latencia y throughput, pero es muy difícil de implementar. En la práctica se suele usar una variante que consiste en guardar información sobre el tiempo de CPU consumido por cada proceso. Se puede aproximar a SJF asumiendo que el proceso se va a seguir comportándose de la misma forma en que se comportó antes. Así, los procesos que históricamente son menos consumidores de CPU tienen más prioridad.

Los sistemas operativos reales normalmente combinan varias de estas estrategias para lograr una planificación óptima. Por ejemplo el sistema operativo Linux suele combinar una estrategia de prioridades estáticas (asignadas por el administrador) con una estrategia de prioridades dinámicas

donde el proceso va perdiendo prioridad a medida que consume CPU (aproximando de esta forma a un SJF), y utilizando *Round Robin* para evitar la monopolización de CPU.

5.3. Comunicación entre procesos

El sistema operativo debe proveer herramientas para que los procesos puedan comunicarse entre sí. Se mencionan a continuación las más comunes.

- *Memoria compartida*: Es una técnica rápida y efectiva para comunicar procesos. Consiste en asignar un segmento de memoria (o un conjunto de páginas de memoria) a dos o más procesos, de forma que todos puedan acceder a él. La ventaja de esta técnica es su velocidad. La desventaja es que los procesos que comparten la memoria deben controlar la concurrencia para evitar una falla por interferencia.

- *Cola de mensajes*: una técnica que permite a uno o más procesos escribir una serie de mensajes en una estructura (provista por el sistema operativo) y a otro conjunto de procesos leer (y consumir) los mensajes. Los mensajes se entregan en el mismo orden que se escriben. La ventaja importante de esta técnica es que administra automáticamente el balance entre producción y consumo, dado que los procesos escritores se bloquean si la memoria destinada a la cola se llena, y los procesos lectores se bloquean si la cola se vacía. En ambos casos los procesos son devueltos al estado de listos ni bien el estado cambia.

- *Líneas bidireccionales de transmisión de datos (sockets)*: Un enlace secuencial bidireccional entre dos procesos. Un proceso abrirá el *socket* en modo escucha, y así quedará hasta que otro proceso abra otro *socket* e inicie una conexión con el primero. A partir de que los dos *sockets* están conectados los procesos pueden transmitirse información a través de

ellos en ambos sentidos. La ventaja más importante de esta técnica es que, además de controlar la producción y el consumo, el *socket* es una abstracción que puede implementarse sobre diferentes canales de comunicación, permitiendo incluso utilizar la red y por lo tanto comunicar procesos que están funcionando en máquinas diferentes.

La información sobre los *sockets*, almacenada normalmente en la tabla de procesos junto con los archivos abiertos, puede resultar de mucha utilidad para el perito forense cuando investiga una máquina en funcionamiento, porque puede indicar por ejemplo origen y destino de una conexión.

5.4. Ejemplo práctico: análisis de procesos en Linux

En el sistema operativo Linux toda la información de la tabla de procesos está disponible y accesible ya sea utilizando herramientas clásicas heredadas del sistema operativo UNIX, o bien directamente a través del sistema de archivos `/proc`.

Las dos herramientas clásicas más potentes son los comandos ps y top.

El comando ps genera una lista de todas las entradas de la tabla de procesos en el momento en que es ejecutado. Mediante sus opciones se puede limitar el conjunto de procesos a mostrar, ya sea clasificando a través de alguna característica (ej. pertenecen a un usuario determinado, o poseen terminal asociada), o indicando una lista explícita. También se puede configurar a través de opciones con mucha flexibilidad los datos que se desean mostrar en cada proceso. Finalmente provee opciones para especificar un criterio de orden para la lista de procesos. La figura 6.16 muestra el resultado en pantalla del comando ps ax, que genera un listado de todos los procesos del sistema. En la figura el listado está cortado por brevedad. Con estas opciones se muestra para cada proceso el identificador (PID), la terminal asociada, el estado, el tiempo de CPU consumido y el

comando con que fue invocado, y la lista se ordena por identificador de proceso.

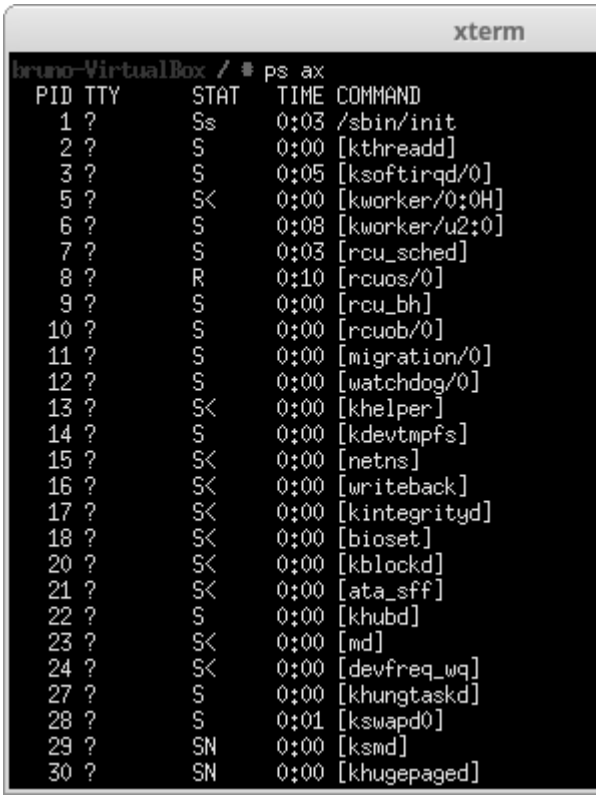


Figura 6.16: Resultado del comando ps ax, cortado por brevedad.

El comando top se puede utilizar para monitorear el sistema en general. Ofrece al administrador mucha información que puede utilizarse para determinar rápidamente la salud del sistema, y la lista de los procesos que mayor cantidad de recurso están consumiendo, en orden descendente. El recurso por el cual se ordena puede elegirse entre uso de memoria y uso de CPU, entre otros. También se puede, mediante tecla de comando, efectuar acciones sobre el sistema (por ejemplo, matar un proceso o cambiarle su

prioridad estática). La figura 6.17 muestra el resultado en pantalla del comando top.

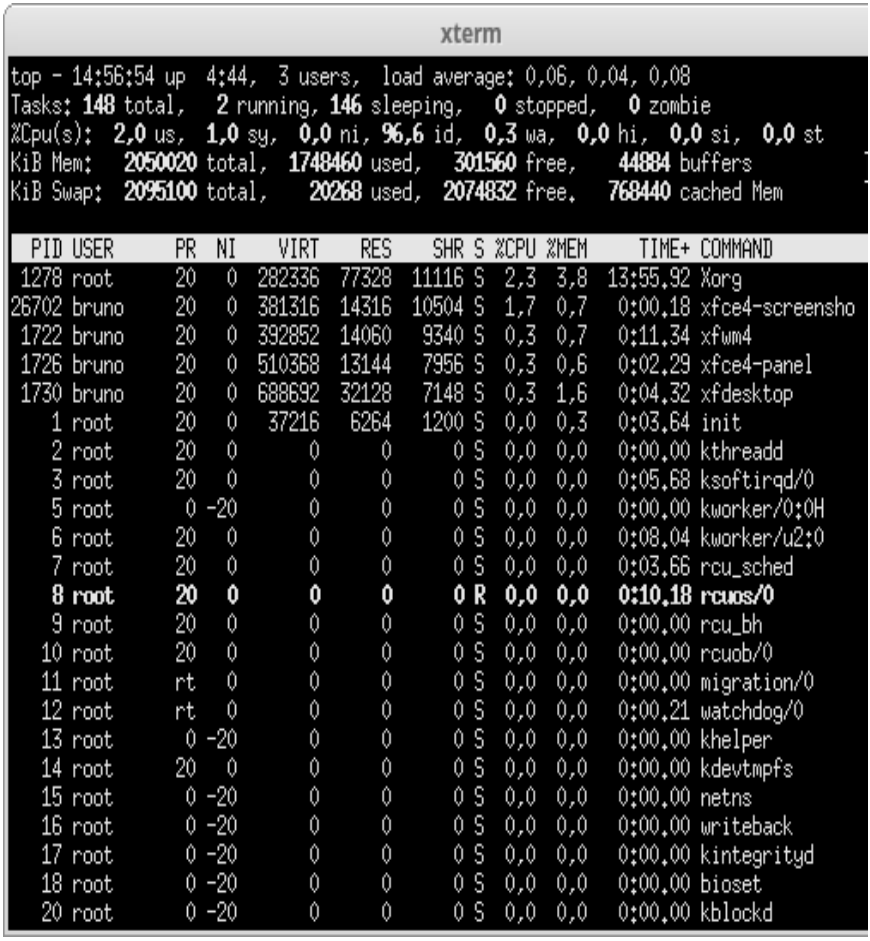


Figura 6.17: Resultado del comando top.

En la parte superior de la pantalla se muestra la hora, el tiempo que hace que el sistema está funcionando y el promedio de carga. En la segunda línea se muestra un resumen del total de procesos y un histograma ordenado por estados. En la tercera línea se muestra la distribución del

tiempo de la CPU en porcentajes entre dos muestras[207]. En la tercera y en la cuarta línea se muestra el estado de la memoria principal, memoria de intercambio y *caches* de dispositivos de entrada/salida. Luego se muestra una lista de procesos similar a la mostrada por el comando ps, ordenada en este caso en forma descendente por consumo de tiempo CPU. Para cada proceso se muestra el identificador (PID), el usuario dueño, el valor de prioridad dinámica (PR), el valor de prioridad estática (NI), el tamaño del espacio virtual de memoria ocupado (incluye páginas que no están presentes en memoria física), la cantidad de memoria residente (solo páginas presentes en memoria física), memoria compartida (páginas de memoria que están compartidas con otros procesos), estado, porcentaje de la memoria física consumido, porcentaje de tiempo de CPU consumido (entre dos muestras), tiempo total de CPU consumido y comando con que fue invocado.

Tanto el comando ps como el comando top toman la información necesaria para construir sus resultados del directorio /proc. En este directorio se encuentra montado un pseudo sistema de archivos que se genera dinámicamente con información obtenida directamente desde el núcleo del sistema operativo. Algunos de los archivos pueden ser leídos únicamente, otros pueden ser escritos para modificar dinámicamente algún parámetro del núcleo. La tabla de procesos está representada con un directorio para cada proceso nombrado por su PID. Por ejemplo, el proceso 2030 tendría su información reportada en el directorio /proc/2030. Se muestran a continuación algunos ejemplos significativos.

- El archivo /proc/2030/cwd es un enlace simbólico al directorio de trabajo del proceso.
- El archivo /proc/2030/exe es un enlace simbólico al programa invocado.

[207] Por defecto el comando `top` toma una muestra cada 3 segundos.

- El archivo /proc/2030/root es un enlace simbólico al directorio raíz del proceso.
- Los archivos que se encuentran en el directorio /proc/2030/fd son enlaces simbólicos a los archivos que el proceso tenga abiertos, incluyendo sockets.

Se pueden utilizar las herramientas clásicas heredadas de UNIX para explorar estos archivos y obtener su contenido. La figura 6.18 muestra la lista de archivos abiertos del proceso 2030 utilizando el comando ls (comando para solicitar un listado de directorio).

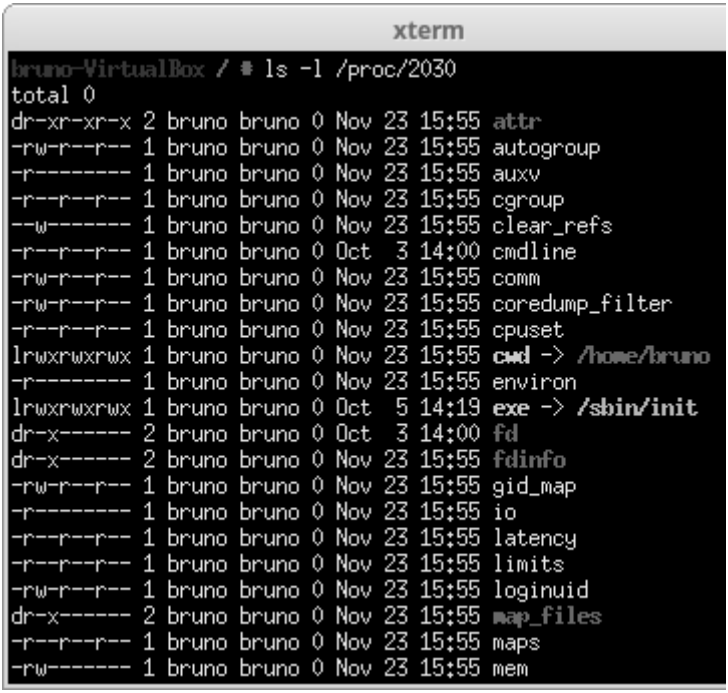


Figura 6.18: Análisis de archivos abiertos por el proceso 2030 utilizando el comando ls.

De la información mostrada en la figura anterior puede deducirse que el proceso tiene su entrada estándar (descriptor

0) anulada (conectada con /dev/null), sus salidas estándar y de error (descriptores 1 y 2) conectadas a un archivo normal (/home/.../run.log), que el descriptor 3 es un socket y el descriptor 4 está conectado al generador de números aleatorios (/dev/urandom).

6. Conclusiones

El Sistema Operativo posee herramientas que permiten acceder a la información contenida en la memoria principal o en las unidades de almacenamiento desde diferentes niveles de abstracción, facilitando su correcta interpretación. Un conocimiento profundo de estas herramientas permite al analista acceder a la información sin necesidad de recurrir a herramientas especializadas, que normalmente son propietarias y no permiten acceso a su código fuente. El hecho de utilizar directamente las abstracciones del Sistema Operativo, junto con herramientas cuyo código fuente esté disponible, permiten potencialmente armar una evidencia sin puntos oscuros o desconocidos desde la perspectiva técnica. En este capítulo se revisaron algunas de las abstracciones más importantes y se mostraron algunos ejemplos que permiten utilizarlas.

En el caso de que se disponga de herramientas privativas, este conocimiento ofrece al analista una mejor oportunidad para aprovechar la información aportada por estas herramientas.

Bibliografía

Tanenbaum, A. Modern Operating Systems, 3rd edition. Prentice Hall, 2007.

Silberschatz, A., Peter Baer Galvin, Greg Gagne. Fundamentos de Sistemas Operativos séptima edición. Mc Graw Hill España, 2006.

“The GNU C Library Reference Manual”, Free Software Foundation Inc., 2016. Disponible en: http://www.gnu.org/software/libc/manual/.

Capítulo 7. File y Data Carving

Autores: Bruno Constanzo, Julián Waimann.

1. Introducción.
2. Conceptos generales. 2.1 Hardware de discos. 2.2 Eliminación de archivos. 2.3 Archivos y representación de datos.
3. File Carving. 3.1 Métricas de Carving. 3.2 Header Footer Carving. 3.3 File Structure Based Carving. 3.4 Bifragment Gap Carving.
4. Validación de Objetos y Archivos. 4.1 Conceptos generales de validación. 4.2 CIRA File Validators.
5. Data Carving. 5.1 Data Carving en base a cadenas de texto. 5.2 Data Carving de estructuras binarias.
6. Otras Consideraciones. 6.1 Espacio no asignado y exclusión de bloques. 6.2 Identificación de archivos conocidos. 6.3 Búsqueda por hashes. 6.4 Carving sin extracción.
7. Anexo técnico I. Hardware de Discos de Estado Sólido. 7.1 Historia y evolución del almacenamiento en estado sólido. 7.2 Almacenamiento Flash y SSDs. 7.3 Consecuencias para el carving. 7.4 Tecnologías futuras.
8. Anexo técnico II. Formatos de Archivo. 8.1 Formato TXT. 8.2 Formato PPM. 8.3 Formato PNG. 8.4 Formato JPG.

1. Introducción

La información en un sistema informático tiene tendencia a persistir, más allá de los intentos de eliminación que puedan realizar los usuarios. Si no se toman medidas específicas para garantizar que efectivamente se han borrado los datos, es posible aplicar técnicas de análisis y recuperación que permiten obtener la información que se suponía eliminada. En este capítulo se verán esas técnicas, conocidas como *file carving* y *data carving*, o simplemente, *carving*.

Pese a la gran potencia que tienen estas técnicas, se debe tener en cuenta que esto viene con un costo que se debe pagar: las técnicas de *carving* pueden ser caóticas en sus resultados, y generar miles, cientos de miles o millones de resultados, que luego deben ser validados, depurados y filtrados hasta llegar a una prueba o evidencia real y válida.

En un principio, se verán conceptos generales necesarios para entender los mecanismos que actúan en un sistema de archivos, y en los medios de almacenamiento, que generan un ambiente propicio para la persistencia y posterior recuperación de la información.

Luego se pasará a los temas de *file carving* propiamente dichos, formatos de archivo, *carving* básico y distintas técnicas y algoritmos que permiten obtener mejores resultados. Luego se lleva la atención a un nivel más bajo, donde se presenta la cuestión del *data carving* y la búsqueda de información con granularidad menor que un archivo.

Finalmente, se verán algunos temas relacionados con el *carving*, que permiten trabajar con una mayor flexibilidad, o realizar un análisis distinto a la mera recuperación de archivos o datos.

2. Conceptos generales

2.1. Hardware de discos

En primer lugar, es necesario explicar a un nivel de profundidad suficiente cómo funcionan los medios de almacenamiento, desde el nivel más bajo posible. En base a estos conocimientos, se entenderá luego por qué es posible tomar medidas para la recuperación de información eliminada, y sobre qué mecanismos y situaciones se apoyan las técnicas de *carving*.

En general, a lo largo de todo el capítulo, se asume que se trabaja sobre discos de platos o *Hard Disk Drives* (HDD). Por cuestiones históricas, y por simplicidad, esta es la postura más conveniente para tomar. Al final del capítulo, en el Anexo Técnico I, se evalúa la situación presente y cómo pueden llegar a evolucionar los discos[208] de estado sólido (o SSDs, de *Solid State Drive*). También es conveniente esta postura, porque los SSD toman medidas para resultar indistinguibles de un medio de almacenamiento clásico, pese a las grandes diferencias tecnológicas que los separan.

Un HDD se compone, principalmente, de disco recubierto por un material ferromagnético, un cabezal de lectura/escritura y un motor. Estos tres componentes definen el comportamiento de los HDD como dispositivos de almacenamiento. Para realizar una operación de entrada/salida, el cabezal debe ubicarse sobre una pista determinada del plato, y esperar que el sector apropiado pase por debajo del cabezal (ver figura 7.1). Por las características de los medios magnéticos, las operaciones de lectura se realizan de forma más rápida que las operaciones de escritura

[208] Mal llamados discos, por una herencia cultural e histórica, un término más apropiado sería “dispositivos de almacenamiento de estado sólido”.

(más adelante se verán las consecuencias de esta característica).

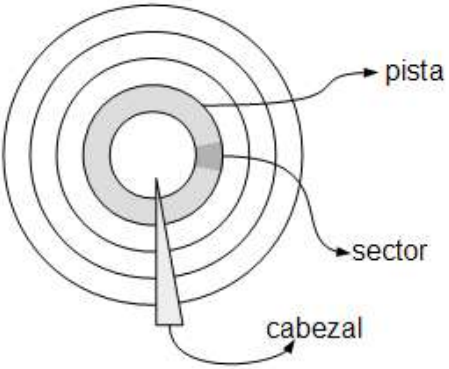


Figura 7.1: Elementos del modelo conceptual de disco rígido.

Si bien esto es un modelo conceptual simple, evita algunas cuestiones adicionales de los discos reales, que es conveniente tener en cuenta:

- En realidad, los discos pueden componerse con varios platos, y cuentan con un cabezal por plato. Dependiendo del modelo de disco, pueden encontrarse hasta 7 platos dentro de un disco.
- Usualmente se cree que los sectores de un disco almacenan una secuencia de unos y ceros, mapeando la información lógica directamente sobre el soporte físico. En realidad, la información se codifica en una señal autosincronizante, que es lo que efectivamente almacenan los campos magnéticos en el plato.
- La señal real también incorpora mecanismos de detección y corrección de errores.
- Cuando el dispositivo realiza la lectura de un sector, el firmware hace una verificación del código de errores:
  - En la medida que no haya errores, o los errores que hay puedan ser corregidos, la operación de lectura se

satisface y se envía la información por el bus de datos.

- Si hay una cantidad de errores por encima de un umbral, el sector se vuelve a escribir con la información correspondiente, generando una nueva señal con el código de corrección “restaurado”. Esto evita que la señal se continúe degradando hasta corromperse totalmente.
- Si no se pueden corregir todos los errores presentes en la señal, el código de detección permite identificar la corrupción de la información y falla la operación de lectura.

- Estrictamente, estos mecanismos utilizan una cierta capacidad de almacenamiento que está presente en el dispositivo, pero no puede ser utilizada por el usuario. Sin embargo, si no estuvieran presentes, la información almacenada se corrompería rápidamente. Efectivamente, estos mecanismos cambian capacidad de almacenamiento total por confiabilidad y robustez en el almacenamiento.

Hay una última consideración sobre el hardware de almacenamiento que es importante para este capítulo. En un capitulo anterior se definió que los dispositivos de almacenamiento, a nivel de sistema operativo, son dispositivos de bloque. A continuación, se definirán distintos niveles de granularidad de la información para ser más precisos:

- **Bit:** es la unidad mínima de información. Permite almacenar dos estados, que usualmente se asocian con valores *booleanos*, Verdadero o Falso, o con los valores numéricos 0 y 1.
- **Byte:** es una composición de 8 bits en conjunto, lo que permite representar 256 estados distintos. Suelen utilizarse para almacenar texto codificado (por ejemplo,

ASCII) o valores numéricos en el rango 0…255 o -128…127.

- **Sector:** es una secuencia ordenada de bytes, 512 por lo general[209]. Es la granularidad más fina con la que permite trabajar un dispositivo de almacenamiento.
- ***Clúster*:** es una abstracción del sistema de archivos, un nivel superior de composición que agrupa varios sectores consecutivos en una sola unidad lógica, que representa la granularidad más fina con la que el sistema de archivos asigna espacio del disco a los archivos. Es común que los *clústeres* sean de 1, 2 o 4 KiB, u otra potencia de 2.

2.2. Eliminación de Archivos

Para comprender claramente por qué funciona el *file carving*, es necesario entender los mecanismos de eliminación de los sistemas de archivos. En esta sección se mostrará como ejemplo FAT32, porque es un sistema de archivos simple en sus estructuras y funcionamiento. Si bien no es un mecanismo directamente trasladable a NTFS o ext, estos otros *sistemas de archivos* más complejos se comportan de manera suficientemente similar para que el *carving* como técnica también sea aplicable en ellos. En general, con la excepción de sistemas de archivos específicos, como pueden ser YAFFS o YAFFS2, los *sistemas de archivos* modernos eliminan los archivos en forma similar.

En el Capítulo de Aspectos Técnicos se explicó el funcionamiento de FAT. A continuación se mostrará cómo es

[209] Algunas tecnologías, como los CDs, manejan sectores de 1024 bytes, y los medios de almacenamiento moderno (tanto HDDs como SSDs) manejan sectores de 4096 bytes por cuestiones de eficiencia y performance. Estos pueden considerarse como si fueran sectores de 512 bytes, en la medida que no se use un direccionamiento basado en sectores, o se ajusten las direcciones.

el proceso de eliminación en este sistema de archivos y cómo se modifican las estructuras Directory Record y File Allocation Table. A continuación, asumiendo que se conocen estas estructuras, se verá cómo es el proceso de eliminación de un archivo en este sistema de archivos:

- En la entrada de directorio, en el campo *Short Name*, el primer byte se reemplaza por 0xE5. Este valor indica que el registro corresponde con un archivo eliminado.
- Con el valor de *First Clúster* de la entrada de directorios, se ubica la cadena de clústeres en la FAT y se recorre, reemplazando por 0 cada valor,
- Por cada *clúster* perteneciente a la cadena que forma el archivo, se reemplaza su valor (el siguiente *clúster* que compone el archivo, hasta llegar al *flag* EOF) por 0, para indicar que esos *clústeres* están disponibles para ser utilizados.

Una vez finalizado el proceso de eliminación, en el sistema de archivos siguen estando:

- El nombre del archivo casi en su totalidad (falta únicamente la primera letra), junto con su extensión.
- Los atributos del archivo junto con sus flags, su primer clúster, el tamaño y los *timestamps* de creación, último acceso y última escritura.
- El contenido real del archivo, sin ningún cambio, en los *clústeres* que ocupaban originalmente.

Es decir, la eliminación de un archivo es un proceso de eliminación lógica de la información que permite ubicar los *clústeres* que lo componen, pero no afecta al contenido. En la medida que el sistema de archivos no utilice estos *clústeres* para almacenar nuevo contenido, la información del archivo seguirá estando disponible.

Si bien la entrada de directorio provee algo de información y metadatos sobre los archivos eliminados, estos registros pueden ser reutilizados por archivos nuevos en el sistema de archivos sin que esto implique la sobre-escritura de los *clústeres* originales que componían a los archivos eliminados.

Las herramientas de recuperación de archivos, entonces, se dividen en dos grandes categorías:

- Herramientas basadas en el sistema de archivos, que son capaces de recuperar únicamente aquellos archivos eliminados de los cuales aún permanecen las entradas de directorio.
- Herramientas de carving, que trabajan en base a la estructura de los formatos de archivo que reconocen, y pueden recuperar archivos aun cuando no quedan metadatos asociados, solamente en base al contenido.

Al no depender de la información del sistema de archivos, solamente de la estructura de los formatos de archivo, las herramientas de *carving* son, efectivamente, independientes de éste y pueden trabajar sobre cualquier medio de almacenamiento, en la medida que se pueda acceder al contenido del mismo[210].

2.3. Archivos y representación de datos

Hasta ahora se han considerado a los archivos como entidades que tienen su origen e identidad en los sistemas de archivos. Sin embargo, las técnicas de *carving* no dependen del mismo, por lo que trabajan de manera independiente. Entonces queda responder a la pregunta: ¿qué es un archivo si se lo separa del *sistema de archivos*?

[210] Una situación problemática sería, por ejemplo, que el volumen del que se quieren recuperar archivos se encontrara cifrado, en cuyo caso primero deberá romperse el mecanismo de cifrado.

La definición de archivo que los caracteriza en base a su estructura y contenido, con la que se trabajará en este capítulo, es la siguiente:

> Un archivo es una secuencia ordenada de bytes, que guarda información codificada de acuerdo a un formato, y utiliza determinadas estructuras de datos y representaciones para su almacenamiento e interpretación.

Con respecto a las estructuras que componen un archivo, son idénticas a las estructuras de datos compuestas que permiten definir los lenguajes de programación, normalmente llamadas *structs* o *records*. Sin embargo, es necesario considerar una cuestión adicional: el ordenamiento de los bytes en memoria, o *endianness*, que es una cuestión interna del procesador, pero al almacenarse las estructuras en disco debe tenerse en cuenta para su correcta interpretación.

Se conoce como *Little Endian* al ordenamiento en memoria de los bytes que utilizan históricamente los procesadores Intel y como *Big Endian* al ordenamiento que utilizaban los procesadores Motorola. En la actualidad, todos los procesadores cuentan con instrucciones para llevar los datos que tienen en sus registros de una representación a otra, y soportan ambas representaciones. Al momento de analizar la estructura de un archivo, es necesario tener en cuenta el ordenamiento de los bytes ya que utilizar el formato incorrecto producirá una interpretación errónea de los mismos. El siguiente ejemplo muestra cómo se codifica el número decimal 100 con ambos sistemas:

Endianness	Short	Integer	Long
Little Endian	0x64	0x6400	0x64000000
Big Endiand	0x64	0x0064	0x00000064

Tabla 7.1: Codificación del número 100 en base 2 para *Little Endian* y *Big Endian*, asumiendo tipos short de 8 bits, integer de 16 bits y long de 32 bits.

El siguiente ejemplo muestra la interpretación de una secuencia de bytes de acuerdo a distintos tipos de datos y codificaciones. Por simplicidad, los números enteros se tomaron unsigned:

Bytes	44 61 74 6f 73 20 62 69 6e 61 72 69 6f 73 2e 00	
Tipos de Datos		
String	"Datos binarios."	
	Little Endian	Big Endian
Short	68, 97, 116, 111, 115, 32, 98, 105, 110, 97, 114, 105, 111, 115, 46, 0	68, 97, 116, 111, 115, 32, 98, 105, 110, 97, 114, 105, 111, 115, 46, 0
Integer	24900, 28532, 8307, 26978, 24942, 26994, 29551, 46	17505, 29807, 29472, 25193, 28257, 29289, 28531, 11776
Long	1869898052, 1768038515, 1769103726, 3044207	1147237487, 1931502185, 1851880041, 1869819392
Float	7.563192932183165e+28, 1.7085654520995406e+25, 1.831375918983917e+25, 4.2658425941868584e-39	901.8192749023438, 1.2706962470455845e+31, 1.7443110150429852e+28, 7.5260467974289125e+28

Tabla 7.2: Representación de bytes en distintos formatos y también de acuerdo a las representaciones de Big Endiand y Little Endian.

Como muestra la tabla 7.2, la misma secuencia de bytes puede interpretarse de múltiples formas, y una interpretación errónea, tanto en el tipo de datos como en su codificación, puede dar resultados muy dispares.

La estandarización de los tipos de datos está definida por documentación de la IEEE, ANSI y los estándares de definición de los lenguajes de programación. En general, como muchos lenguajes se construyen encima de C, o son compatibles, los tipos de datos definidos para C se encuentran disponibles en múltiples entornos y plataformas.

3. File Carving

En el Digital Forensics Research Workshop se ha definido el *file carving* de la siguiente forma:

"Es el proceso de extraer una colección de datos de un conjunto de datos más grande. Las técnicas de carving frecuentemente se utilizan en una investigación forense cuando se analiza el espacio no asignado de un sistema de archivos para extraer archivos. Las estructuras del sistema de archivos no se utilizan durante este proceso".

Sin embargo, esta definición es demasiado correcta: no menciona la utilización de las estructuras propias de los formatos de archivo, y se cierra a la posibilidad de apoyar la tarea de carving con alguna información del *sistema de archivos* (aunque menciona la exploración del espacio no asignado). La definición con la que se trabajará en este capítulo, que surge de la homogenización de varios conceptos y trabajos, es la siguiente:

File carving es el proceso de extraer archivos de un dispositivo de almacenamiento analizando el contenido de sus bloques, teniendo en cuenta características específicos de los formatos de archivo e ignorando las estructuras del sistema de archivos.

Esa definición es suficiente para comenzar a estudiar los conceptos de *carving* propiamente dichos, aunque más adelante se verá que pueden ignorarse algunas partes de la misma.

Se puede utilizar una clasificación muy simple para los algoritmos y herramientas de carving:

- **Carving básico:** se define así a los algoritmos que solamente pueden recuperar archivos contiguos en el dispositivo original y no manejan detalles de la estructura de los archivos.
- **Carving avanzado:** se define de esta manera a los algoritmos que tienen la capacidad de recuperar archivos fragmentados, aun si los fragmentos no se encuentran ordenados o no están presentes en su totalidad, apoyándose en las estructuras propias de los formatos de archivo.

Esta clasificación, que se puede derivar de múltiples trabajos sobre "algoritmos avanzados de *carving*" es tajante y deja un lugar intermedio abierto: hay algoritmos y herramientas que resuelven parcialmente el problema de la fragmentación, o que se apoyan en técnicas complementarias para resolverlo. Lo más interesante de esta categoría de "*carving* intermedio" es que consisten en herramientas reales que pueden utilizarse, y no planteos teóricos de algoritmos que no tienen implementaciones disponibles.

Las principales familias de algoritmos de *file carving* son:

- ***Header Footer Carving*:** es la técnica original y más simple de *carving*. Permite recuperar archivos, pero es muy susceptible a generar falsos positivos.
- ***File Structure Based Carving*:** son técnicas basadas en los formatos de archivo y sus estructuras. Están fuertemente relacionados con la temática de validación de archivos.

- ***Statistical Carving*:** estas técnicas apoyan las decisiones de reconstrucción de los archivos en medidas estadísticas sobre los bloques analizados y los formatos de archivo que se busca reconstruir, y de esa forma determinan el inicio y fin de los archivos, así como los bloques intermedios.
- ***Fragment Recovery Carving*:** en estos algoritmos se toma un conjunto de bloques que, de acuerdo a alguna métrica, se determina que pertenecen a un formato de archivo, y se aplican estrategias para reconstruir los archivos en base a su *pool* de bloques.
- ***Semantic Carving:*** en esta familia de algoritmos se aplica alguna medida de interpretación del contenido para vincularlo, de manera significativa y con entendimiento de la información, en búsqueda de formar archivos coherentes. El ejemplo clásico es el poder separar dos archivos de texto en distintos idiomas, pero se puede pensar de manera más amplia y aplicable a otros tipos de contenido.
- ***Graph Theoretic Carving*:** es una técnica en la que se recorre el dispositivo de almacenamiento buscando fragmentos de archivos (similar al *Fragment Recovery Carving*). Luego estos fragmentos se clasifican, y se construye un grafo sobre el cual se aplican algoritmos de múltiples caminos con múltiples puntos de inicio y final, en busca de optimizar la recuperación de archivos. Una implementación comercial de esta técnica lleva el nombre de Smart Carving™. Es una técnica compleja de implementar, y con un costo computacional grande, por lo que deben utilizarse técnicas complementarias para que funcione de forma eficiente. La calidad de los resultados es muy sensible a las medidas de similaridad que se utilicen para el pesado de los vértices cuando se construye el grafo de fragmentos.

Más adelante en el capítulo se presentarán algoritmos de *Header Footer Carving* y *File Structure Based Carving*.

3.1. Métricas de Carving

Antes de continuar con el estudio de los algoritmos en particular, es necesario presentar algunas métricas que se utilizan para poder comparar el rendimiento de los mismos entre sí. Las métricas que se utilizan son las siguientes:

- **Cantidad de archivos recuperados:** el total de archivos generados por el *carver* para un determinado proceso de extracción.
- **Cantidad de archivos no recuperados:** los archivos que se encontraban en el dispositivo de almacenamiento, pero que no se recuperaron con el proceso de *carving*. Para poder tomar esta medida es necesario conocer en profundidad la imagen analizada.
- **Cantidad de archivos válidos recuperados:** cuántos de los archivos recuperados contienen información válida. Por ejemplo, si se busca recuperar fotografías JPG, esta medida indica cuántos de los archivos recuperados muestra una imagen.
  - **Cantidad de archivos parcialmente recuperados:** se clasifica de esta forma a los archivos que mantienen la coherencia del formato de archivo hasta un punto de corte, donde el archivo se corrompe. Este punto de corrupción puede implicar las siguientes situaciones:
    - **El archivo termina abruptamente** sin llegar a encontrarse la información restante, ni las estructuras que marcan el final del archivo.
    - El archivo continúa, pero se esperaba una estructura determinada que no se encuentra. Ante

esta situación, se habla de **corrupción de la estructura de archivo**.

- El archivo continúa, y las estructuras presentes son las adecuadas, pero la información representada en los datos no es coherente. Ante esta situación, se habla de **corrupción del contenido**.

- Por definición, se dirá que son **válidos** los archivos completos que son coherentes en estructura y contenido, y se llamará **parciales** (o **parcialmente válidos**) a los archivos que presentan una parte coherente y un punto de corrupción, ya sea de estructura o contenido. Si el archivo presenta estructura válida, pero en ningún punto presenta coherencia en el contenido, se dirá que es un archivo **no válido**.

- **Precisión del *carving* (*carving precisión)*:** del total de archivos recuperados, cuántos son válidos o parciales:

$$\text{precision}_{\text{val}} = \frac{\text{recuperados}_{\text{val}}}{\text{total}_{\text{rec}}}$$

$$\text{precision}_{\text{par}} = \frac{\text{recuperados}_{\text{par}}}{\text{total}_{\text{rec}}}$$

- ***Carving recall*:** del total de archivos presentes en el dispositivo, cuántos lograron recuperarse. Esta medida también puede calcularse en base a los archivos válidos o parciales.

$$\text{recall}_{\text{val}} = \frac{\text{recuperados}_{\text{val}}}{\text{total}_{\text{reales}}}$$

$$\text{recall}_{\text{par}} = \frac{\text{recuperados}_{\text{par}}}{\text{total}_{\text{reales}}}$$

- ***Overcarving*:** es una medida que indica cuánto demás se ha extraído del dispositivo. Puede medirse tanto en cantidad de archivos, como en capacidad de almacenamiento utilizada:

$$\text{overcarving} = \frac{\text{extraidos}}{\text{reales}}$$

$$\text{overcarving}_{\text{st}} = \frac{\text{storage(extraidos)}}{\text{storage(reales)}}$$

Idealmente, se debe buscar que la precisión, el *recall* y el *overcarving* todos tiendan a 1. En condiciones reales esto resulta imposible, y se debe priorizar un comportamiento determinado, o buscar un balance entre las tres medidas que resulte razonable.

- Si se prioriza la precisión, se logra reducir la cantidad de archivos recuperados y obtener sólo archivos válidos. Sin embargo, esto implica el riesgo de perder archivos que pueden ser de interés, aunque presenten algún grado de corrupción.
- Priorizar el *recall* es más complicado, porque en teoría sería necesario un conocimiento profundo de los contenidos del disco y esto es posible sólo en casos de laboratorio. Aun así, pueden aplicarse heurísticas que tienden a mejorar esta métrica. Lo que se gana es una mayor coincidencia entre los archivos originales y los extraídos, al costo de mayor tiempo de análisis o de obtener un conjunto de resultados más reducido (en donde podría haber información de interés).

- Finalmente, reducir el *overcarving* es posible, tanto por métodos directos (utilizar tamaño máximo de archivo, o algoritmos basados en estructura, por ejemplo) como métodos indirectos (*in-place file carving* o validación de formatos pre-extracción). Se verán algunas de estas opciones más adelante.
- La validación de archivos, mediante la comparación de su estructura contra la definición formal del formato, es de suma importancia porque permite balancear las 3 medidas: logra aumentar la precisión y reducir el *overcarving*, teniendo como único costo una mayor complejidad computacional (que depende de la complejidad del formato). Sin embargo, se debe tener cuidado porque una estrategia de validación demasiado agresiva puede reducir en exceso el conjunto de resultados, y quitar resultados de interés por no ser completamente válidos.

3.2. Header Footer Carving

En general, todos los formatos de archivo respetan una estructura determinada, que permite la organización de los datos y su correcta interpretación para acceder al contenido que almacenan. Una práctica habitual es definir un *header* o "*magic number*" para los formatos de archivo, una secuencia de bytes que se ubica al principio del archivo e indica de en qué formato está almacenada la información. Además del header, muchos formatos definen un *footer*, una secuencia de bytes con la que se cierra el archivo y se indica su fin. De esta forma, todos los datos que contienen la información del archivo se encuentran entre estos dos marcadores. En la tabla 7.3 hay ejemplos de *headers* y *footers*.

Formato	Header	Largo H	Footer	Largo F
JPG	0xFFD8	2	0xFFD9	2
PNG	0x89504E470D0A 1A0A	8	0x49454E44A E426082	8
GIF	GIF87a GIF89a	6	0x003B	2
HTML	<html	5	</html>	7
XML	<xml	4	</xml>	5
SQLite3	SQLite Format 3\x00	16		
MS-OLE	0xD0CF11E0A1B1 1AE1	8		

Tabla 7.3: Varios formatos de archivo con sus *headers* y *footers*. En aquellos casos que se empieza con 0x y se utiliza letra cursiva, son caracteres binarios representados en hexadecimal, en los demás casos, es el *string* que se encuentra en el archivo.

El *Header Footer Carving*, es la técnica de *carving* mediante la cual se ubican los *headers* y *footers* de uno o varios formatos de archivo, y se recuperan archivos asumiendo que todo lo que se encuentra entre el inicio y fin de un formato de archivo determinado, es en sí mismo un archivo.

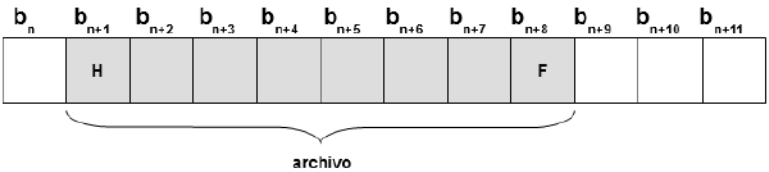


Figura 7.2: Distribución de archivo en bloques. Header y Footer.

Para dar una definición más formal, si se buscan archivos del formato X, y en el bloque b_{n+1} se encuentra el *header* del formato de archivo que se está buscando, y en el bloque b_{n+j} se encuentra el *footer*, entonces un archivo del formato X se encuentra en el disco conformado por los bloques $\{b_{n+1}, b_{n+2}, \ldots, b_{n+j}\}$.

Como suposición inicial, da un buen punto de partida para comenzar la recuperación. También históricamente fue la primera técnica de *carving* que se desarrolló. Al evaluar sus ventajas y desventajas se concluye lo siguiente:

- Conceptualmente simple, lo que permite implementarla fácilmente.
- Es una técnica rápida, ya que, al no tener procesamiento intensivo, puede correr a la velocidad de lectura secuencial del medio de almacenamiento origen (en la medida que se implementen buenas estrategias de lectura).
- También es fácil de implementar en una sola pasada sobre el dispositivo.
- No puede extraer formatos de archivo sin *footer*.
- Puede generar archivos excesivamente grandes, si un archivo de un formato se encuentra fragmentado y hay una gran separación entre sus fragmentos inicial y final.
- Si el *header* y el *footer* son muy pequeños, o cadenas relativamente frecuentes, puede generar muchos falsos positivos, o cortes prematuros en los archivos recuperados.

Una ligera mejora que se puede implementar, y que resuelve algunos de estos problemas, es imponer tamaños máximos y mínimos de archivo. Cuando se implementa a través de tamaño máximo, esta técnica se denomina *Header/Maximum-Length Carving*. Si bien no hay un nombre

para cuando se utilizan tamaños mínimos, a continuación, se da una descripción del algoritmo que lo contempla:

- Para cada formato de archivo, se definen los *headers, footers*, *min_length* (tamaño mínimo) y *max_length* (tamaño máximo).
- Se buscan todos los *headers* y *footers* de los formatos que se quiere recuperar.
- Para los formatos que tienen *footer*, se calcula la distancia entre cada par *header-footer* encontrado. Solo pasan a la etapa de extracción los pares *header-footer* cuya longitud se ubica entre el tamaño mínimo y máximo.
  - En el caso de los archivos que no llegan a tener el tamaño mínimo, no se los extrae.
  - En el caso de los archivos que superan el tamaño máximo, se trunca el contenido del mismo para que tenga un tamaño de *max_length* bytes.
- Para los formatos que no tienen *footer*, se considerará que un archivo comienza en donde se ubica un *header* del formato apropiado, y terminará *max_length* bytes más adelante.

Las ventajas y desventajas de este algoritmo son las siguientes:

- Sigue siendo un concepto simple, y se puede integrar fácilmente dentro de una herramienta que ya implemente *Header Footer Carving*.
- Consiste en operaciones de poca complejidad computacional, lo que permite llegar fácilmente a los límites de velocidad que imponga el *hardware* en el que se ejecute.
- Evita la generación de archivos excesivamente grandes.

- Si se implementa el tamaño mínimo, también evita la generación de múltiples falsos positivos demasiado pequeños para ser realmente archivos (por ejemplo, extraer como JPG la cadena `0xFFD8FFD9`).
- Permite extraer formatos sin footer.
- Aun puede generar demasiados falsos positivos si el *header* utilizado es muy corto.
- Algunos formatos, como PDF o JPG, pueden tener múltiples ocurrencias del *footer* antes de llegar efectivamente al final del archivo.

Dado que algunos formatos de archivo contienen en su encabezado de archivo[211] una variante adicional que puede hacerse es leer este campo y utilizar su información para determinar el punto de fin del archivo. Los algoritmos que implementan esta técnica se llaman Header/Embedded Length Carving, y es el punto de partida de técnicas que interpretan con mayor profundidad las estructuras y metadatos de los archivos.

Antes de evaluar la siguiente familia de algoritmos, se analizará, de forma simple, los desafíos que se enfrentan:

- **Fragmentación:** Sean a_1 y a_2 archivos que se encuentran en el dispositivo, a2 fragmenta a a1 en dos partes:

[211] No debe confundirse el encabezado de archivo, el bloque inicial con el que muchos archivos inician y que contiene metadatos de interés para la correcta interpretación del mismo, con el *header* en el sentido de *magic number*, la cadena corta con la que se indica el formato del mismo.

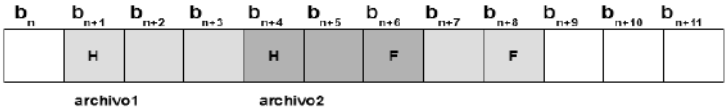


Figura 7.3: Ejemplo archivo fragmentado.

En este caso, el archivo a_2 puede recuperarse correctamente, pero a_1 se recuperará corrupto, mezclado con datos del archivo a_2.

- **Fin prematuro por tamaño máximo:** Sea a un archivo de formato X y tamaño N+M, y sea N el tamaño máximo definido para el formato X:

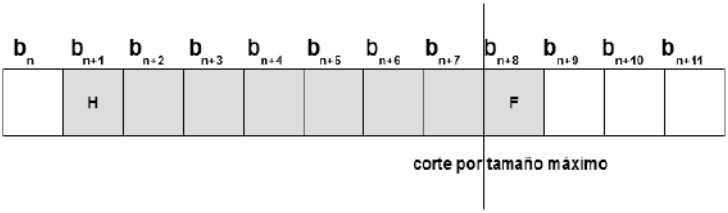


Figura 7.4: Ejemplo de archivo truncado por tamaño máximo.

En este caso el archivo se recuperará en forma parcial hasta llegar al tamaño N, y quedarán M bytes del final del archivo sin recuperar.

- **Subarchivo:** Sea a un archivo JPG con un thumbnail (a_t) embebido en su campo EXIF:

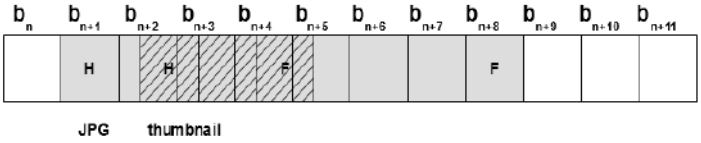


Figura 7.5: Ejemplo de archivo con subarchivo embebido.

a_t se recuperará satisfactoriamente como un archivo independiente de a, pero este se recuperará desde su *header*

hasta el *footer* de a_t, finalizando el archivo en su segmento de metadatos EXIF.

Esta situación puede presentarse en otros formatos de archivo que tienen la capacidad de contener en su interior otros archivos, el caso particular que se presenta con JPG es que un mismo archivo tiene otro archivo, de su mismo formato, en su interior y se entrelazan los marcadores de fin entre ambos archivos.

- **Fin prematuro por múltiples marcadores de fin:** Sea p un archivo en formato PDF, con N marcadores de fin de segmento, siendo Nf el último de ellos:

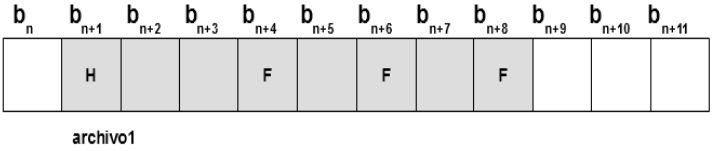


Figura 7.6: Ejemplo de archivo con múltiples marcadores de fin de archivo.

El archivo p se recuperará parcialmente hasta la ocurrencia del primer marcador de fin de segmento, quedando incompleto, con f - 1 segmentos faltantes, aún si se encuentran presentes y contiguos en el dispositivo.

3.3. File Structure Based Carving

File Structure Based Carving es la familia que agrupa los algoritmos de *carving* que trabajan en base a la definición de los formatos de archivo y sus estructuras para la determinación de los puntos de inicio y fin de los archivos que se busca recuperar. Son algoritmos más complejos que la familia de *Header Footer Carving*, porque necesitan interactuar con un decodificador o parser de cada formato de archivo con el que se quiera trabajar, o implementar la lógica necesaria para interpretar las estructuras de los mismos. Sin

embargo, esta complejidad adicional resulta en un mejor rendimiento de los algoritmos.

Para ilustrar la complejidad, se verá a continuación un ejemplo simplificado de la estructura de los archivos JPG. Al final del capítulo, en la sección Anexo Técnico: Formatos de Archivo, se muestra en mayor profundidad y detalle la estructura y las estrategias de validación aplicadas a JPG y otros formatos.

En primer lugar, los archivos JPG se organizan en segmentos que tienen una estructura definida. Todos los segmentos tienen un *tag* (etiqueta o nombre) que indica que tipo de segmento es. Los segmentos "normales" además tienen un tamaño de segmento, mientras que los segmentos de datos tienen un tamaño variable y se indica su fin con un marcador especial (similar a un *footer* de formato de archivo). Todos los *tags* de segmento JPG son de 2 bytes de longitud y comienzan con el byte `0xFF`

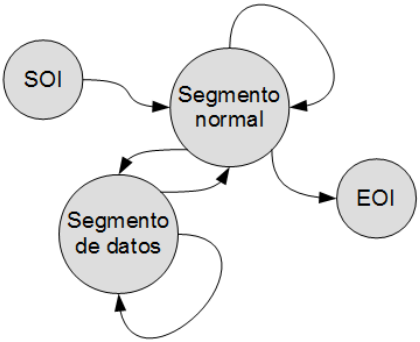


Figura 7.7: Estructura simplificada de un archivo JPG.

Entonces un archivo JPG comienza siempre con un *tag Start of Image* (SOI), cuya etiqueta es `0xFFD8` y lo sigue a continuación un segmento "normal", con metadatos sobre el

archivo y la imagen que contiene[212]. Lo siguen una cantidad variable de segmentos normales, y al menos un segmento de datos. Finalmente, se marca el final del archivo con un *tag End of Image* (EOI), cuya etiqueta es `0xFFD9`.

Una descripción general de los algoritmos de *File Structure Based Carving*, independiente de los formatos que se pretenda validar, es la siguiente:

- Se recorre el dispositivo origen en busca de puntos de interés donde podría comenzar un archivo.
  - Se suele buscar *headers* de archivo, pero podría utilizarse otra estructura para determinar un posible punto de inicio.
- Por cada punto de interés, se determinan los posibles puntos de inicio de archivo.
- A partir de cada punto de inicio, se intenta interpretar la información como si fuera un archivo válido del formato apropiado. Esto puede realizarse con parsers, decodificadores o validadores de archivo.
- Si efectivamente se trata de un archivo válido, se utiliza la información de inicio y fin del mismo para realizar la extracción.

Esta descripción general no entra en detalles sobre el proceso de verificación de la estructura de los archivos, simplemente delega la responsabilidad en un decodificador o validador adecuado. También sugiere la implementación del proceso de *carving* en dos pasadas sobre el archivo, una primera pasada en búsqueda de los puntos de interés, y la

[212] El SOI es seguido por un *tag Application*, del cual hay múltiples variantes, por lo tanto, sólo puede garantizarse que los archivos JPG comienzan con los bytes `0xFFD8FF`. El lector puede utilizar un *Header Footer Carver* para verificar cómo varía la precisión con ambos *headers*.

segunda enfocada sólo en los lugares donde podrían comenzar archivos. Implementar la técnica de esta forma permite desarrollar un *carver* de estructura sin generar un acoplamiento excesivo entre el código de *carving* y los decodificadores de archivo.

Las ventajas y desventajas de esta familia de algoritmos son:

- Tienen la capacidad de recuperar formatos complejos.
- Las verificaciones a la estructura que se realizan para poder determinar si se debe extraer o no el archivo son en sí mismos una validación de la integridad del archivo.
- Suelen producir una menor cantidad de falsos positivos y tener una mayor precisión.
  - Esto depende directamente de la calidad de los parsers o decodificadores de formato que se utilicen.
- La técnica es compleja porque se deben integrar los decodificadores, o desarrollar funciones de decodificación propias.
- Si las reglas de verificación de la estructura son muy estrictas, podría no extraerse un archivo parcialmente válido que contiene información de interés.
- Inherentemente no contempla la fragmentación, aunque se pueden utilizar técnicas complementarias para superar este problema.

3.4. Bifragment Gap Carving

En el DFRWS 2007, Simson Garfinkel presentó un trabajo llamado "*Carving Contiguous and Fragmented Files using Fast Object Validation*", donde presentó la técnica denominada *Bifragment Gap Carving*. Por su conocimiento, estudio detallado del problema y el enfoque novedoso que

tomó Garfinkel en él, este es un trabajo que aún hoy continúa vigente.

Del análisis y estudio de cientos de discos provenientes de casos reales[213], sus sistemas de archivos y los archivos propiamente dichos, Garfinkel obtuvo los siguientes resultados:

- Los *sistemas de archivos* de UNIX, al estar basados en el concepto de i-nodos, generan más fragmentación como consecuencia de su funcionamiento normal.
- Los *sistemas de archivos* de Windows (FAT y NTFS), generan menos fragmentación en los archivos, porque esta situación les genera una pérdida de rendimiento notable.
- La fragmentación es mayor en el caso de archivos grandes, aunque los sistemas de archivos pueden implementar estrategias de asignación de espacio para mitigarla.
- Obtuvo estadísticas de fragmentación de acuerdo a los formatos de archivo, muy detalladas y valiosas (ver en el original).
- La conclusión más importante a la que llegó es que **la fragmentación usualmente es en dos partes**, separadas por un espacio de bloques anómalo que no corresponde al archivo.

En base a su análisis, Garfinkel propuso un nuevo algoritmo, basado en los resultados y conclusiones de su estudio:

[213] Es decir, discos que habían visto uso por usuarios reales, y no casos de laboratorio.

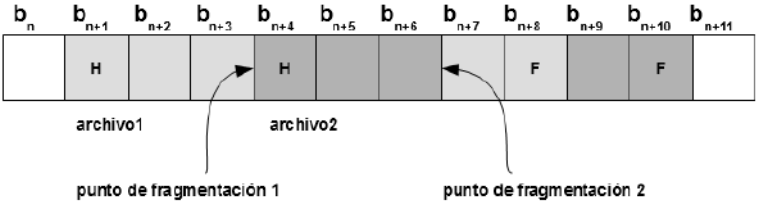


Figura 7.8: Bifragment file carving.

- En primer lugar, se ubican los *headers* y *footers* de los formatos de archivo que se busca recuperar.
- Se genera un buffer en memoria con todo el contenido entre *header* y *footer* (o a partir del *header* si se trata de un formato sin *footer*).
- Se verifica con un validador que el buffer contiene un archivo válido.
- Si se trata de un archivo válido, entonces se extrae el archivo y la técnica no es distinta de los algoritmos de la familia *File Structure Based Carving*.
- Si en cambio el validador informa que no se trata de un archivo correcto, se asume que es un archivo "bifragmentado", y por lo tanto se deben quitar los bloques extraños que se encuentran entre medio de los dos fragmentos. Este conjunto de bloques extraños es el *gap* (hueco, en inglés) del nombre del algoritmo.
  - El *gap* tiene un inicio y un final, que deben ajustarse progresivamente para probar las combinaciones posibles hasta encontrar alguna que resulte en un archivo válido.
  - Garfinkel plantea incrementar el tamaño del hueco de a 1 byte a partir del último byte válido informado por el validador, pero pueden utilizarse otras estrategias para acelerar el proceso, por ejemplo, ajustar el

tamaño de gap a los bordes de sector o clúster e incrementarlos también en base a estas unidades.

- Para el caso de archivos que no tienen indicadores de su punto de fin (tanto un *footer* como estructuras internas que permitan derivar dónde termina el archivo), Garfinkel plantea utilizar el validador en conjunto con una búsqueda binaria para determinar el menor tamaño que da como resultado un archivo válido.
- Esta estrategia de búsqueda binaria también puede aplicarse para ajustar el tamaño del *gap*.
- Otra optimización propuesta es la búsqueda de estructuras propias de formato de archivo, como podría ser un *marker* de segmento en el caso de JPG. Esto permite poner límites para el tamaño máximo que podría tener el *gap* y optimizar la reconstrucción del archivo.

En el trabajo citado, Garfinkel muestra cómo al aplicar el *Bifragment Gap Carving* sobre la imagen de prueba del DFRWS 2006 Challenge se obtienen resultados satisfactorios, y se logra la reconstrucción de los archivos fragmentados que se encuentran en dicha imagen. Sin embargo, pese al excelente planteo teórico y las pruebas de su autor, no hay herramientas que implementen *Bifragment Gap Carving* en la actualidad[214].

4. Validación de Objetos y Archivos

Además de Simson Garfinkel, Michael Cohen, Joachim Metz y otros autores presentaron trabajos sobre la utilización de funciones de validación en algoritmos de *file carving* para

[214] En el GitHub del InFoLab puede encontrarse un prototipo de investigación, Orthrus, que implementa *Bifragment Gap Carving* de forma experimental.

mejorar el desempeño de los mismos. La idea también se encuentra presente en múltiples herramientas de recuperación, no sólo programas de *carving*: dado que los archivos recuperados pueden haber sido corrompidos por otros datos, es necesario correr una verificación sobre su estructura y/o contenido para validar que se trata de información correcta.

En esta sección se presenta una perspectiva en donde se combinan los análisis de Garfinkel y Cohen, junto con la experiencia de los autores en la implementación de funciones de validación para utilizarlas en el contexto de los proyectos CIRA Framework y CIRA File Validators.

Antes de analizar los conceptos generales, es pertinente hacer una aclaración. Cohen habla de utilizar una *función de mapeo* para determinar los bloques que pertenecen a cada archivo, y luego esta selección se evalúa con un *discriminante* que es capaz de determinar si el mapeo es correcto o no. Efectivamente, Cohen está hablando de validación de formatos.

De forma análoga, Garfinkel habla de validación de objetos, y aclara que la validación de archivos es un subconjunto de ésta, pero prefiere hablar de objetos en lugar de archivos porque eso permite una granularidad más fina y la recuperación de entidades que no son archivos en sí mismos.

Es decir, tanto Cohen como Garfinkel están hablando de las técnicas que permiten verificar que un determinado objeto recuperado de un dispositivo de almacenamiento contiene las estructuras adecuadas, de forma coherente, para respetar un determinado formato de archivo y eso permite considerarlo un objeto válido.

En esta sección, se habla de validadores y de objetos, siguiendo una convención cercana a la que utiliza Garfinkel.

4.1. Conceptos generales de validación

En primer lugar, debe plantearse la cuestión de cómo se puede realizar la tarea de validación de los archivos recuperados por un *carver* (u otra herramienta de recuperación):

- Si se trata de pocos archivos, efectivamente podría intentar ver cada uno de ellos con el programa adecuado. A medida que la cantidad de archivos crece, esto se vuelve poco práctico, y es imposible para una gran cantidad de archivos.
- Además del tiempo de carga, hay que considerar que muchas veces la corrupción de datos presente en un archivo parcialmente válido o un archivo no válido es capaz de cerrar el programa que interpreta el formato de archivo, por presentar situaciones para las que no está preparado.
- Incluso si el archivo recuperado puede ser abierto, la información que muestra el programa puede ser totalmente carente de sentido.
- Algunas aplicaciones pueden ser invocadas desde la línea de comandos para ir abriendo los archivos en forma programática. El problema de este enfoque es el mismo que se mencionó antes: las aplicaciones esperan un archivo correctamente formado, y pueden reaccionar indebidamente ante los datos corruptos.
- También suele haber disponibles librerías, que pueden integrarse en un ciclo más cerrado. El problema de las librerías es que, ante una falla al abrir un archivo, en general los mensajes de error que emiten simplemente refieren a “archivo incorrecto” en lugar de indicar dónde se produjo del error.
- El caso ideal sería contar con una librería de funciones que hagan un *parsing* y decodificación del archivo,

validando el estado interno del mismo, y que mantengan información clara sobre los puntos de error si se detecta alguno.

Como se mencionó anteriormente, Garfinkel propuso un *framework* de validación, pero lo hizo de forma muy específica, acoplada con su código (prototipo, y difícil de conseguir), muy orientado a C++ y sus construcciones sintácticas. Cohen también propuso ideas con respecto a la validación de archivos, por lo que se puede combinar los conceptos que ambos proponen para sacar conclusiones generales:

- Las funciones de validación tienen que funcionar sobre cualquier objeto que pueda generar un *carver*. Es decir, tienen que ser robustas en su funcionamiento, y no pueden quedarse en *bucles* infinitos o generar excepciones.
- Las funciones de validación deben responder lo más rápidamente posible.
- Las funciones de validación tienen que proveer de medios para determinar los posibles puntos de fragmentación del objeto que analizan.
- Las funciones de validación deberían proveer medios para ubicar las estructuras importantes del tipo de objeto que analizan. Por ejemplo, identificar los segmentos JPG si se está validando un objeto en ese formato.

Como una cuestión de optimización para maximizar el rendimiento de los validadores, Garfinkel propone que se separe en distintos niveles el proceso de validación, y solo se progrese a los niveles superiores si se logra superar la etapa anterior. Los niveles de validación escalonada que propone son los siguientes:

- **Validación de *header* y *footer*:** se verifica que el objeto analizado respete el *header* y *footer* correspondientes al formato.
- **Validación de estructuras:** se verifican los punteros y referencias internas del objeto, y se valida su integridad y coherencia. Es un análisis más profundo, pero no llega a procesar la información representada en el objeto.
- **Validación por descompresión:** se procesa el objeto con una librería o programa que interpreta la información del objeto propiamente dicha. En esta etapa la *función de descompresión* verifica que, además de presentar una estructura apropiada, el objeto respeta las reglas de información que puede contener de acuerdo a su formato.
  - Por ejemplo, se verifica que un archivo HTML no tenga símbolos por fuera del conjunto ASCII-7.
- **Validación semántica:** en esta etapa se analiza el sentido de la información representada por el objeto, utilizando analizadores semánticos apropiados.
  - Por lo general cuando se habla de validación semántica o *carving* semántico se da el ejemplo de interpretación de textos, por medio de técnicas de NLP, pero también pueden aplicarse análisis semánticos sobre imágenes, audio o video.
  - La evolución de las técnicas de *Machine Learning* y *Deep Learning* resulta prometedora para la implementación de este tipo de análisis.
- **Validación humana:** más allá de todo lo que pueda realizarse en forma automática a través de algoritmos, siempre al final de la validación de objetos debería haber una persona evaluando los resultados y filtrando los eventuales falsos positivos que superen el proceso.

- El resultado de esta validación puede utilizarse para entrenar o re-entrenar sistemas de *Machine Learning* que se utilicen durante el proceso.

En su trabajo, Garfinkel opina que el nivel de validación semántica era extremadamente interesante, pero imposible de realizar con la tecnología de esa época, y que el nivel de validación humana es imposible de automatizar.

4.2. CIRA File Validators

Al finalizar el Proyecto PURI, en el año 2012, se presentaron nichos carentes con respecto a técnicas o herramientas de la Informática Forense. Uno de los proyectos que se decidió tomar fue el desarrollo de un prototipo que tratara de resolver la cuestión de validación de archivos, un área que hasta ese momento no era resuelta de manera satisfactoria por ninguna herramienta. Por lo tanto, se tomó como base la propuesta de un *framework* de validación de archivos de Garfinkel y se extendió para integrarla con otro proyecto que se encontraba en curso, CIRA Framework. El resultado fue CIRA File Validators, que surgió como un paquete de clases dentro de CIRA Framework, pero luego se lo separó en un *framework* independiente.

Además de los aportes de Garfinkel, se tomaron en cuenta las consideraciones de Cohen y se realizó un estudio propio de los formatos de archivo que se eligieron para trabajar, en base a su importancia para la investigación forense.

A la fecha, el *framework* se encuentra disponible en https://github.com/info-lab/FileValidators y cuenta con validadores para los siguientes formatos de archivo: JPG, PNG, GIF, LNK (Microsoft Shell Link), MS-OLE (Office 97-2003, thumbs.db, otros) y soporte parcial para SQLite3 y ZIP.

Las tres ideas detrás de este proyecto son:

- La validación de archivos es una técnica poderosa que complementa bien a los algoritmos de *carving* en general.
- La utilización de un lenguaje simple de entender como Python permite que se puedan hacer evaluaciones y auditorías de los algoritmos de validación. Además, Python es un lenguaje extendido en la comunidad informática forense.
- Los validadores deben permitir tanto la integración dentro de un *carver* como el funcionamiento sobre archivos de forma independiente. De esta forma se pueden utilizar en conjunto con otras herramientas ya existentes, por ejemplo, Scalpel.

Los validadores de CIRA son clases que presentan una interfaz simple:

- Una función **Validate** que recibe un descriptor de archivo o una cadena con el contenido a analizar, y lleva a cabo el proceso de validación. La función devuelve True o False dependiendo el resultado de su análisis.
- Una función **GetStatus**, que devuelve información sobre el último archivo validado: el resultado de la validación, cuál fue el último byte válido, si se llegó al fin de archivo en forma prematura y si se encontró la estructura que marca el final del archivo (dependiendo si el formato tiene una estructura de este tipo).
  - Esta es la función que provee la información necesaria para integrar los validadores dentro de un *carver*.
- Una función **GetDetails**, que devuelve información detallada y dependiente del formato de archivo sobre el último objeto validado.

- Esta función puede utilizarse para construir *parsers* de los formatos de archivo y mostrar información de interés para el analista forense.
- La información provista por esta función también puede usarse para crear reglas de validación más complejas.

Esta interfaz permite que se construyan *carvers* de estructura, con distintos grados de complejidad, o que se hagan procesos de filtrado de archivos en base a los resultados de los validadores.

Con respecto a los niveles de validación, en CIRA File Validators se utiliza un enfoque simplificado, ya que hay niveles que Garfinkel plantea como separados pero que pueden integrarse entre sí. La simplificación del esquema de validación surge como resultado de la implementación de los validadores, y el hecho que algunos formatos de archivo no necesitan de todos los niveles de validación porque integran en su formato estructuras que son capaces de garantizar su integridad. Los niveles con los que trabaja el *framework* son:

- **Validación de estructura:** comprende la validación de *header* y *footer*, la coherencia de punteros y la estructura general (ya sean segmentos, *chunks* o páginas) del archivo, sin procesar los datos que representan la información. Este análisis se caracteriza por ser muy rápido.
  - Algunos formatos, como PNG o ZIP, cuentan con estructuras internas que codificación el *checksum* de las partes del archivo. Verificando estas estructuras es posible garantizar la integridad de los archivos sin requerir de análisis adicionales.
- **Validación de datos:** comprende el análisis de las estructuras del objeto que codifican la información, y la verificación de la coherencia entre estas distintas estructuras. Es un análisis más profundo, y necesario

para resolver correctamente las situaciones en donde se presenta una estructura correcta, pero hay corrupción de la información.

  - JPG es un formato en donde es necesaria la validación de datos para detectar situaciones de corrupción de datos.

- **Validación inteligente:** comprende el análisis semántico de los archivos a través de sistemas de inteligencia computacional. Permite la interpretación del contenido propiamente dicho y tomar decisiones más complejas que los niveles de validación anteriores.

- **No se considera la validación realizada por humanos como una etapa separada,** ya que se considera que siempre debería haber una persona al final del proceso verificando las decisiones realizadas. Los validadores inteligentes se plantean con la idea de que es preferible aceptar un mayor nivel de falsos positivos con el objetivo de evitar falsos negativos.

5. Data Carving

Si bien inicialmente los términos *file carving* y *data carving* eran sinónimos, hace unos años que refieren a dos conceptos distintos: se habla de *file carving* cuando los objetos que se pretenden recuperar son archivos, es decir, bloques enteros de información, que respetan todo el formato y definición y pueden existir como entidades en sí mismas, y de *data carving* cuando se pretende recuperar fragmentos de información más pequeños. Un ejemplo ilustrativo sería la diferencia entre recuperar una base de datos (*file carving*) o recuperar registros de la misma (*data carving*).

Descender a un nivel de granularidad más fina introduce varios problemas, pero utilizando ideas y conceptos del *file carving* se puede lograr un equilibrio que resulta provechoso para el investigador.

Al utilizar *data carving*, dado que los objetos que se buscan son más pequeños, la cantidad potencial de resultados aumenta notablemente, pero la situación se equilibra al considerar que las estructuras, al ser más pequeñas, están mejor definidas y pueden evaluarse rápidamente para descartar los falsos positivos.

Las ventajas que brinda trabajar en este nivel son pocas, pero no por eso menos importantes: al buscar de esta forma, se puede encontrar información de interés en partes del sistema de archivos donde no se podría encontrar un archivo entero (por ejemplo, el *slack space* de un *clúster*) o en *sistemas de archivos* o imágenes que tienen una alta fragmentación inherente (como puede ser un *raw dump* de un SSD o la memoria flash de algunos celulares que utilizan YAFFS o YAFFS2). Es decir, el *data carving* puede dar una mejor respuesta a las situaciones más problemáticas para el *file carving*, en la medida que se puedan definir estructuras de interés con suficiente precisión como para aprovechar ésta técnica.

Los mecanismos que se utilizan son equivalentes, sino los mismos, que para el *file carving*: la búsqueda de las cadenas se puede realizar tanto con algoritmos clásicos como con expresiones regulares, y la verificación se puede hacer *casteando* los bytes sobre un *struct* y comprobando que se respeten los rangos de datos adecuados para cada uno de los campos que componen a la estructura que se está buscando.

5.1. Data Carving en base a cadenas de texto

Si la información que se busca se representa mediante cadenas de texto, entonces lo mejor es realizar una búsqueda orientada a *strings*, ya sea a través de caracteres especiales, subcadenas o expresiones regulares.

Por ejemplo, si se desea buscar direcciones de email de Gmail, Hotmail o Yahoo, podría tomarse la siguiente estrategia:

Realizar la búsqueda de las cadenas “@gmail”, “@hotmail” y “@yahoo”, y revisar los bytes alrededor de cada ocurrencia para determinar si son o no direcciones de email válidas.

Al evaluar en detalle esta estrategia, se pueden hacer las siguientes consideraciones:

- Resulta necesario ver cada uno de los posibles resultados para verificar si efectivamente es una dirección de email.
- Cada resultado debe ser evaluado por sí mismo, y se debe discernir a partir de qué punto empieza el dato de interés en cuestión.
- Es necesario verificar que la búsqueda de cadenas no sea sensible a mayúsculas y minúsculas (a través de configuraciones de la herramienta o comandos del lenguaje que se utilice).
- La búsqueda está restringida específicamente a las cadenas que se detallaron, y es necesario incorporar cada variación que pueda ser de interés.

Otra estrategia podría ser utilizar la expresión regular[215] “[\w.-_]+\@[\w-_]+(\.[\w-_]+)+”, que tiene la capacidad de detectar direcciones de email. Con respecto a la anterior estrategia, las expresiones regulares presentan las siguientes características:

- Dado que realiza la búsqueda en base a una estructura, es más amplia que una búsqueda de cadenas simple.
- Se debe tener cuidado con la complejidad y los operadores que se utilizan en la misma, porque una

[215] La expresión regular se muestra en el formato de sintaxis aceptado por Python.

expresión regular patológica puede reducir significativamente la velocidad de procesamiento.

- La arroba precedida por N grupos alfanuméricos en la expresión regular presentada más arriba es efectivamente un caso patológico para la mayoría de los motores de expresiones regulares.
- Si la expresión es muy compleja, es recomendable separarla en expresiones más fáciles de procesar y luego vincular entre si los resultados de cada expresión para componer los resultados.
- También puede complementarse la expresión regular con filtros, transformaciones y funciones de agregación de los datos para proveer de un análisis más completo.

- Ver en el Capítulo 5, en la sección de casos prácticos, Bulk Extractor.

Las expresiones regulares son herramientas muy poderosas, pero específicas a un problema: la interpretación de gramáticas regulares. Cuando la problemática presenta una complejidad mayor, su capacidad de devolver resultados precisos se reduce rápidamente. Como ejemplo ilustrativo, la cadena:

 span nro 1span nro2

Es imposible de parsear correctamente con la mayoría de los motores de expresiones regulares[216], por el anidamiento y balanceo que se requiere.

Si se necesita realizar *data carving* de estructuras que presenten este tipo de complejidad, lo mejor es utilizar las

[216] Con excepción de Perl y .NET que proveen un operador llamado *balanced matching*. De todos modos, aun pueden pensarse casos que superen las capacidades del motor de expresiones regulares.

expresiones regulares como un punto de inicio, y luego aplicar otras herramientas o funciones para resolver los casos.

5.2. Data Carving de estructuras binarias

Otra situación que puede presentarse es que se pretenda recuperar estructuras binarias que presentan un tamaño fijo. Estructuras de este tipo que pueden resultar de interés son tanto las entradas de directorios (*Directory Record*) como los registros de archivo (*File Record*) de los sistemas de archivos FAT y NTFS, respectivamente, y se tomarán como caso práctico. En sí, las técnicas para aplicar a este tipo de estructuras son la instanciación de los bytes sobre un *struct* y la validación del resultado obtenido.

El caso del *File Record* es más simple conceptualmente, y por eso se lo analizará primero. Cada *File Record* es una estructura de 1024 bytes de tamaño (o el tamaño de *clúster*, siempre múltiplo de 512 bytes) que comienza siempre con la cadena “FILE”, y toda la estructura se alinea con el comienzo de un bloque y cada 1024 bytes. Esta cadena es parte de un encabezado de registro de 48 bytes, que siempre está presente, y luego vienen los segmentos específicos, cada uno con su formato y estructura.

En general, con solo buscar en los primeros 4 bytes de cada bloque que comience con la cadena “FILE”, se tienen resultados bastante precisos. De todos modos, se pueden verificar los 44 bytes posteriores de acuerdo a algunas reglas, por ejemplo, el campo *Flags*, si bien tiene 2 bytes, nunca debería tener valores mayores a `0x0010`.

Luego del encabezado, vienen los segmentos con información de interés, desde donde se puede obtener la información de interés del archivo: *timestamps*, *hard* y *symbolic links*, nombre de archivo, jerarquía dentro del sistema de archivos, los datos del archivo o los *data runs* que lo componen, etc.

Para recuperar *Directory Records* de los sistemas de archivos FAT la situación es un poco más compleja. La estructura es más pequeña (32 bytes), no hay campos fijos que puedan servir de indicios, y la estructura se alinea con el borde de bloque y cada 32 bytes y eventualmente vuelve a alinearse con el comienzo de bloque (en el caso del primer registro de un bloque).

Además de aprovechar el alineamiento de la estructura, para recuperar estos registros es necesario realizar algunas verificaciones, a saber:

- Los primeros 11 bytes de un registro de nombre corto corresponden al nombre de archivo en formato 8.3 y solo puede utilizarse un conjunto reducido de los caracteres ASCII.
- El byte 12 son los *flags* del archivo, y sólo son válidas algunas combinaciones.
- El byte 13 siempre está en valor 0.
- El byte 14 es una cuenta de milisegundos, con un rango de 0 a 199.
- Las demás estructuras contenidas en el registro son complejas, pero podrían considerarse estrategias de validación/verificación para las mismas

Este tipo de estrategias también pueden aplicarse para la recuperación de otro tipo de estructuras, o de *headers* de tamaño fijo que preceden a estructuras de tamaño variable. Se eligió mostrar en particular el caso de las entradas de tablas de archivo (para *sistemas de archivos* FAT y NTFS) porque pueden resultar útiles para casos complejos de recuperación de archivos.

6. Otras consideraciones

Además de los temas que se han presentado hasta el momento, hay otras cuestiones vinculadas con el *carving*,

técnicas complementarias y consideraciones que son importantes y permiten realizar un análisis más específico, o realizar ajustes sobre determinados parámetros que permiten sacar provecho de características o situaciones particulares.

Los temas presentados en esta sección pueden leerse aislados, ya que no presentan una cohesión tan fuerte entre sí como los temas tratados en las secciones anteriores.

6.1. Espacio no asignado y exclusión de bloques

En la definición formal de *file carving* se dijo que la recuperación de los objetos presentes en el dispositivo de almacenamiento se realiza sin tener en cuenta las estructuras del sistema de archivos. Este es un planteo que tiene sentido desde el punto de vista teórico, pero que en la práctica resulta problemático: si se sigue ésta definición al pie de la letra, se recuperarán una enorme cantidad de archivos que se encuentran disponibles a través del mismo *sistema de archivos*, y que terminan opacando los archivos que solamente pueden recuperarse mediante *carving*.

Los archivos presentes en el *sistema de archivos* no solo molestan por la cantidad, sino que pueden generar situaciones en las que un archivo disponible a través del sistema de archivos fragmenta un archivo remanente en el dispositivo, y por lo tanto impide su correcta recuperación.

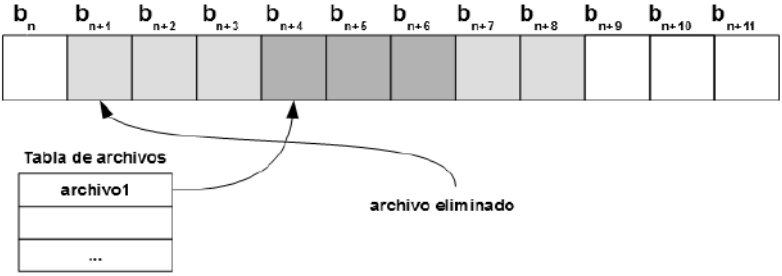


Figura 7.9: Ejemplo de fragmentación sobre un archivo eliminado producto de un archivo presente en el sistema de archivos.

Ante esta situación se hace evidente que sería útil indicar de alguna manera al *carver* los bloques sobre los que interesa trabajar y cuales se quieren excluir del análisis. Esta idea está presente en varios *carvers*, o se puede lograr realizando “extractos” de una imagen hacia otra sub-imagen. En el caso particular del espacio no asignado, se quiere separar los bloques que el sistema de archivos registra como libres, ya que en ellos se encuentra el contenido remanente de los archivos eliminados.

Trabajar sobre el espacio no asignado reduce la cantidad de archivos que se extraen, y permite concentrar el esfuerzo del perito informático sobre los archivos que realmente es necesario recuperar, ya que no se encuentran disponibles por otro medio.

En el Capítulo de Aspectos Técnicos se explicó el funcionamiento del Sistema de Archivos FAT y su tabla de clusters asignados. Si se recorre toda la tabla FAT, puede determinarse fácilmente qué *clústeres* se encuentran asignados y cuáles no. Este mismo análisis puede extenderse a otros sistemas de archivos, pero en FAT resulta más evidente y simple de explicar.

La implementación de este análisis puede realizarse tanto dentro del *carver*, o a través de herramientas desarrolladas con el propósito de analizar sistemas de archivos. Por ejemplo, The Sleuth Kit presenta una herramienta que genera automáticamente una sub-imagen en base a la imagen de una partición en donde copia únicamente los bloques no asignados, y muestra por *stderr* el mapeo de los bloques originales a los bloques de la sub-imagen.

CIRA Framework, en cambio, integra en sus clases de acceso a datos la capacidad de excluir bloques, y lo hace de forma transparente para los algoritmos de *carving*, a los que se les presenta la ilusión de una imagen continua.

PhotoRec tiene tanto la capacidad de trabajar sobre el espacio no asignado directamente, así como de generar un archivo con el espacio no asignado.

Lo más importante que debe tenerse en cuenta cuando se trabaja con exclusión de bloques, es que los *logs* de extracción se corrijan, de ser necesario, y muestren siempre las ubicaciones, o desplazamientos de los archivos recuperados en relación a la imagen original. De esta forma podrá justificarse adecuadamente el origen de un archivo recuperado.

6.2. Identificación de archivos conocidos

Una tarea que se puede realizar durante la extracción, o luego de finalizado el proceso de *carving*, es el reconocimiento de archivos conocidos. Esto permite tomar decisiones sobre estos archivos para optimizar lo que se busca obtener del proceso de recuperación.

Una decisión podría ser, por ejemplo, no extraer los archivos conocidos para evitar que se agreguen al conjunto de resultados, ahorrando tanto capacidad de almacenamiento, como tiempo del investigador que no se distrae con archivos que agregan poco a los resultados de la recuperación.

Otra decisión, por el contrario, podría ser utilizar un listado de archivos conocidos para demostrar la presencia de un determinado software en el equipo, pese a que se lo haya intentado eliminar.

Esta técnica suele implementarse con una base de datos donde se almacena información sobre el origen del archivo conocido (por ejemplo, nombre del archivo, tamaño, software al que pertenece, autor, etc.), junto con hashes MD5 y SHA-1 (u otros). El programa de *carving*, u otro programa externo, procesan los archivos extraídos y verifica los hashes contra la base de datos. Si encuentra una coincidencia, informa que el archivo procesado es un archivo conocido.

Las bases de datos de archivos conocidos pueden construirse de acuerdo a proyectos propios, en base a un caso (por ejemplo, para buscar si se ha copiado un archivo en un dispositivo de almacenamiento), o también pueden descargarse de internet.

Una base de datos muy utilizada es la *National Software Reference Library* (NSRL) que compila el *National Institute of Standards and Technology* (NIST) de Estados Unidos. Esta base de datos reúne información, metadatos y hashes de todo el software conocido (en base a sus criterios) y puede descargarse de internet. A través de esta base de datos puede detectarse una gran cantidad de software, tanto comercial, open source, sistemas operativos, y malware, entre otros.

6.3. Búsqueda por hashes

En este caso se toma el concepto de la identificación de archivos conocidos, pero se lo lleva a trabajar en una granularidad más fina. En lugar de comparar los hashes de un archivo completo, se toman los hashes de acuerdo a segmentos del archivo de interés que se busca y se busca en el dispositivo analizado la ocurrencia de estos bloques. El procedimiento es el siguiente:

- Para cada archivo que se busca en el dispositivo, se lo separa en bloques de tamaño N.
- Para cada bloque, se calcula el hash (MD5, SHA-1 u otro).
- Se recorre el dispositivo, leyendo bloques de tamaño N y calculando el hash correspondiente para cada bloque.
- Los hashes de bloque se compran con el conjunto de bloques de interés que se calculó inicialmente.

- En el caso de una coincidencia, se informa qué bloque del dispositivo coincidió con qué bloque de qué archivo.

De esta forma se puede verificar si aún quedan fragmentos de un archivo en un dispositivo, dando un indicio de que eventualmente estuvo presente en el mismo. En general es una técnica robusta, en la medida que el sistema de archivos que se analiza almacene la información alineada con los bloques o sectores. Sin embargo, esta técnica tiene problemas con los *sistemas de archivos* que almacenan los archivos desfasados dentro del bloque (por ejemplo, ReiserFS), o si los archivos de interés están contenidos dentro de otro archivo (como por ej. PDF, ZIP o RAR).

6.4. Carving sin extracción

Durante el capítulo se hicieron comentarios sobre la rapidez de los algoritmos de *carving* o su complejidad computacional, pero no se habló en detalle del problema. Hay tres factores críticos al respecto:

- El tamaño del dispositivo origen del que se quieren recuperar archivos.
- La complejidad del algoritmo utilizado y detalles de su implementación.
- La cantidad de archivos que se deben extraer, es decir, el *overcarving* – tanto en cantidad de archivos como en capacidad de almacenamiento.

De estos aspectos, sobre el tamaño del dispositivo de origen lo único que se puede hacer es decidir trabajar sobre el espacio no asignado, en la medida que esto sea posible. Con respecto a los algoritmos, si se trata de software de código abierto podría realizarse alguna optimización sobre el código si realmente se justifica, pero en general no se puede reducir la complejidad de un algoritmo.

En la práctica, la etapa que suele consumir alrededor del 70% del tiempo total de un proceso de *carving* es la extracción de los archivos del medio original hacia el medio destino, ya que esta tarea se hace a la velocidad de escritura del medio destino.

Si bien el hardware moderno es capaz de trabajar con muy buenas velocidades de lectura y escritura, una técnica que se había desarrollado en la época de los discos de platos es el *in-place file carving* o *zero-storage carving*. Estas técnicas son equivalentes entre sí, y la idea detrás de ellas es quitar la fase de extracción de un *carver* y, en lugar de copiar los resultados a un nuevo dispositivo, generar un *sistema de archivos* virtual que referencia a la imagen original. Las ventajas de este enfoque son:

- Al no generar una copia de los archivos, se ahorra tiempo en el proceso de *carving*.
- También se ahorra en capacidad de almacenamiento, ya que las estructuras y punteros del sistema de archivos virtual que se genera son mucho más pequeñas que el tamaño que ocuparían los archivos recuperados.
- También se gana en confiabilidad de la información, ya que se lee directamente del dispositivo origen (ya sea un dispositivo físico o una imagen forense).

Los desafíos que presenta es que deben crearse drivers especiales para el sistema de archivos virtual que se genera. Este enfoque es más fácil de implementar en Linux, donde se hace uso de los mecanismos de drivers FUSE.

Richard, Roussev y Marziale propusieron la utilización de esta técnica como una mejora para Scalpel, y lo presentaron junto con un driver para Linux llamado ScalpelFS. La *Dutch National Police Agency* también trabajó sobre una implementación independiente, que llamaron *zero-storage*

carving y sus componentes son la librería LibCarvPath y el sistema de archivos CarvFS.

7. Anexo técnico I. Hardware de Discos de Estado Sólido

En la introducción a los Conceptos Generales se explicó el funcionamiento de los discos de platos o HDD, y se comentó que los discos de estado sólido (*Solid State Drive*, SSD) tienen un funcionamiento totalmente distinto. Debido a que los SSD presentan una capa de compatibilidad, suelen presentarse como si fueran un HDD con una muy alta velocidad de lectura y escritura.

Sin embargo, las diferencias internas y en su forma de operación tienen consecuencias importantes y afectan la capacidad de las técnicas de *carving* para obtener resultados de estos dispositivos, de maneras que no resultan intuitivas para los expertos acostumbrados a trabajar con medios de almacenamiento ferromagnéticos.

En esta sección se presenta la tecnología detrás de los discos de estado sólido con un nivel de detalle similar al que se presentó anteriormente el hardware de los discos de platos, y se evalúan las consecuencias que tienen el hardware y su operación en el nivel físico sobre las técnicas de *carving* y la capacidad de recuperar información.

7.1. Historia y evolución del almacenamiento en estado sólido

El almacenamiento de estado sólido que se encuentra en uso masivo actualmente es un descendiente directo de las tecnologías ROM desarrolladas hace muchos años, que con su evolución llegaron a convertirse en la tecnología Flash moderna. Se verá cómo esta herencia tecnológica aún hoy afecta su rendimiento y funcionamiento, y le da características únicas, especialmente si se compara con el almacenamiento en medios ferromagnéticos.

Las memorias ROM más simples son las llamadas *Mask ROM*, nombre que se les da por el proceso de fabricación en el que se utiliza una máscara para "quemar" la información de acuerdo a un proceso físico (en los modelos iniciales, literalmente se quemaban transistores). La característica principal de estas memorias es su bajo costo, ya que se necesitan menos componentes y se utiliza menos silicio. Además, se pueden aplicar métodos de economía de escala para fabricar económicamente cientos de miles de chips con la misma información. Esto las hacía muy convenientes para almacenar *firmware* o sistemas embebidos, pero si hay algún defecto en la fabricación se debe descartar el chip como defectuoso. Otra desventaja es que tienen un ciclo de fabricación largo: si se quiere hacer un cambio, debe definirse el software, preparar la máscara de quemado y fabricar los chips – un proceso que resulta poco conveniente para hacer nuevos desarrollos o probar pequeños cambios sobre un *firmware* existente.

Una mejora sobre la ROM clásica es la *Programmable ROM* o PROM. Esta clase de dispositivos se inventó a mediados de los años 50 con el propósito de almacenar en forma más flexible y segura la información de objetivos en las computadoras de los misiles ICBM. Con esta tecnología se puede fabricar el chip, verificar su integridad y luego programarlo "en campo". El proceso de programación se podía realizar una sola vez, pero el método es mucho más flexible que en el caso de la *Mask ROM*: se podía tener muchos chips PROM en blanco, a la espera de ser programados y realizar las pruebas necesarias. Esto permitía también agilizar el desarrollo de *firmwares* embebidos, ya que permitía trabajar sobre prototipos o versiones iniciales del contenido de la ROM con PROM, y una vez terminado el proceso de desarrollo y test, tomar el contenido de la memoria como fuente para hacer una máscara y trasladar el contenido a una memoria *Mask ROM*, más barata de producir.

El siguiente escalón en el progreso del almacenamiento no volátil se dio en los años 70, en Intel, y consistió en la tecnología conocida como *Erasable Programmable ROM* (EPROM), un chip ROM que además de programarse, permite que se elimine su contenido para luego volver a programarlo. Estos chips se utilizaron mucho para almacenar los *firmwares* de BIOS durante años: son los característicos chips cucaracha con ventana de cuarzo. La ventana expone la memoria del chip, y permite, al iluminarlo con luz ultravioleta, resetear los transistores al estado original en que pueden ser escritos. La eliminación también puede hacerse con rayos X, pero luego es necesario calentar el chip a una temperatura elevada para reparar el daño estructural que le causa ese proceso. Pero incluso la utilización de luz ultravioleta, más benigna para el chip, deja depósitos de dióxido de silicio en las compuertas del chip, que se acumulan y luego de algunos miles de ciclos de re-escritura la memoria se vuelve inestable.

Hacia fines de los años 70, en Hughes Aircraft e Intel, en paralelo, se desarrollaron tecnologías de *Electrically Erasable Programmable ROM* (EEPROM), con características funcionales similares a la EPROM común, pero en las que la eliminación de los datos se realiza por medio de un proceso eléctrico. Por la forma en que se organiza la estructura de los chips, este tipo de memorias se desarrolló para permitir operaciones de lectura y escritura más rápidas que las tecnologías precedentes, ya que permiten leer y escribir múltiples bytes a la vez. Pese a las mejoras con respecto a la tecnología que le antecede, este tipo de memorias también presenta un ciclo de vida limitado a miles, cientos de miles o millones de escrituras (en el caso de los chips EEPROM modernos).

Finalmente, a principios de los 80 en Toshiba se desarrolló la tecnología Flash, que presentó varias mejoras con respecto a las memorias EEPROM. Algunas de estas mejoras fueron:

- Hay dos tecnologías Flash, una basada en compuertas NOR y otra basada en compuertas NAND. NOR es más parecida a las memorias volátiles, mientras que NAND es más parecida a los dispositivos de bloque.
- Las memorias Flash exponen el espacio de direccionamiento completo y permiten el acceso aleatorio a los datos, a nivel de bloque (NOR) o a nivel de página (NAND).
- Ambas tecnologías Flash escriben y eliminan la información más rápido que las memorias EEPROM, lo que permite una operación más rápida.
    - Esta característica permitió que las tecnologías Flash fueran competitivas con otras tecnologías de almacenamiento no volátil, como los discos de platos.
- Los componentes pueden hacerse más pequeños, lo que favoreció el aumento de densidad de almacenamiento para las tecnologías Flash.
- El proceso de eliminación de información no necesita de voltajes tan elevados como EEPROM.

Si se compara con la tecnología de HDD, el almacenamiento Flash consume menos electricidad y además es resistente a los golpes, características que la convierten en una tecnología ideal para los dispositivos móviles. También resiste bien la radiación, en la medida que se utilice en modo solo lectura.

La tecnología Flash hereda algunas características de las tecnologías ROM que deben tenerse en cuenta:

- En las celdas de información no se “escribe” la información en el mismo sentido que se escribe información en otros medios. Las celdas flash tienen la capacidad de cambiar su estado de 1 a 0, un proceso de que se conoce como “programación”, pero no pueden cambiar su estado de 0 a 1.

- Esto es análogo a programar el contenido de una ROM, y por eso se utiliza una denominación similar.

- Para volver a programar una celda, en primer lugar, se debe resetear la página, es decir, cambiar el estado de todas las celdas que componen la página a 1.
  - La página es una escala en la jerarquía en que se organizan las memorias Flash que contiene bloques y cada bloque celdas. Se verá en detalle más adelante.

- Este ciclo se denomina *program/erase* o ciclo de programación/eliminación.

- Las celdas que almacenan la información tienen una vida útil limitada y solo soportan una cantidad fija de ciclos P/E. Dependiendo de la clase, tecnología y calidad de los componentes, la vida útil de una celda se ubica entre 1.000 y 1.000.000 de ciclos.

- Los procesos de lectura y escritura de la información de las memorias deben contemplar cuestiones de los circuitos y el funcionamiento de sus componentes. No se ahondará en estos detalles por su complejidad, pero vale la pena aclarar, pero vale la pena aclarar que, al igual que la señal en los discos HDD, el almacenamiento físico que realiza una memoria Flash está codificado de una forma que es apta para el medio físico, y distinta a la representación lógica.
  - En la tecnología Flash también se utilizan algoritmos de corrección de errores que ocasionan que, ante un *dump* del contenido físico de los chips, se encuentre más información que la que informa como total el dispositivo. Los bits adicionales se utilizan para implementar algoritmos de corrección de errores y codificación de la señal física.

7.2. Almacenamiento Flash y SSDs

Dado que los objetos de este análisis son los dispositivos de almacenamiento, y estos utilizan las memorias Flash del tipo NAND, de aquí en adelante se referirá a ellas simplemente como “memorias Flash”. En el caso que se trate de otro tipo de memoria, se especificará el tipo de manera explícita.

Como se mencionó anteriormente, las memorias Flash son un tipo especial de memoria no volátil en las que el medio de almacenamiento es un circuito electrónico, que se denomina “celda”. Las celdas se organizan en páginas, estas en bloques[217], y los bloques en planos, formando una jerarquía de múltiples niveles.

En esta sección se presenta un análisis de los conceptos y mecanismos básicos que entran en funcionamiento dentro de un SSD, es decir:

- Operaciones de lectura y escritura
- *Flash Translation Layer*
- *Wear Leveling*
- *Garbage Collection*

Estos últimos tres mecanismos agregan un nivel de complejidad muy alto a la organización de la información dentro de una memoria Flash, y usualmente se encuentran presentes en los dispositivos que se llaman *Solid State Drives* (SSD), y no las formas más económicas de almacenamiento Flash, y son los encargados de prevenir el desgaste prematuro de las celdas de información en el dispositivo.

[217] No confundir los con los sectores, la unidad mínima de comunicación con un dispositivo de bloques.

Comprendiendo estos mecanismos, serán evidentes las incompatibilidades que surgen entre los supuestos iniciales que se vieron sobre *file carving*.

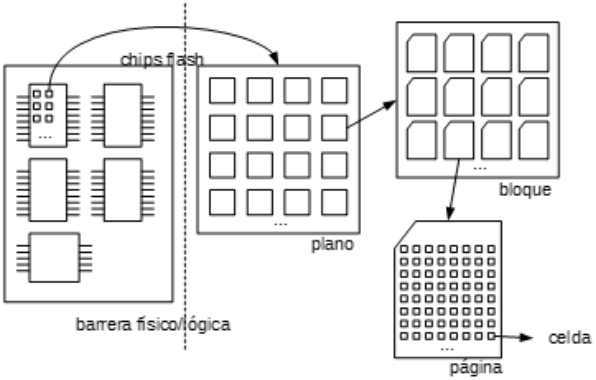


Figura 7.10: Organización de una memoria Flash en sus distintos niveles de granularidad: celda, bloque, página y plano. Las operaciones sobre la memoria trabajan en al menos uno de estos niveles.

En los dispositivos SSD la lectura se realiza en forma similar que en una memoria RAM (de hecho, el acceso en los dispositivos de almacenamiento Flash es realmente aleatorio), pero con algunas diferencias propias de la tecnología. En un dispositivo Flash hay chips de memoria que contienen planos, cada uno compuesto por múltiples bloques de páginas, las que se componen de celdas que pueden almacenar 1, 2 o 3 bits dependiendo de la tecnología de fabricación de las mismas. Para ver un detalle específico de la arquitectura a nivel de hardware, se recomienda leer el trabajo de King y Vidas citado en la bibliografía del capítulo. En general se puede asumir que el plano contiene alrededor de 1024 bloques, compuestos por 128 páginas, que contienen unas 1024 celdas (es decir, 128, 256 o 384 bytes). Luego el SSD realiza un manejo interno de la información para poder satisfacer y exponer una interfaz similar a otros dispositivos de

bloques, es decir, mostrar al resto de la computadora sectores de 512 o 4096 bytes.

Aclaración: los sectores lógicos que el dispositivo Flash expone al resto de la computadora, en realidad se encuentran distribuidos entre múltiples páginas, que pueden encontrarse en distintos bloques.

Al recibir una operación de lectura o escritura, el firmware del SSD accede a una estructura interna, la *Flash Translation Layer* (FTL), el mecanismo a través del cual el dispositivo mantiene la ilusión de ser una secuencia ordenada de bloques contiguos (como si fuera un HDD).

Cuando la memoria Flash recibe la instrucción de leer un sector, el *firmware* debe revisar la FTL y sus estructuras de datos para determinar en qué plano(s), bloque(s) y páginas se encuentra mapeado el sector, y así realizar el acceso a las celdas correspondientes para satisfacer la operación de lectura. En general, puede considerarse a la FTL como una capa de abstracción análoga a las jerarquías de memoria y esquemas de memoria virtual de los procesadores y sistemas operativos. Es decir, lo que en un HDD son direcciones físicas (el número de sector), en un SSD son direcciones lógicas que deben traducirse de acuerdo a los mapeos internos del dispositivo.

Las operaciones de escritura resultan más complicadas. Como se mencionó anteriormente, las celdas de memoria Flash no se *escriben*, sino que se *programan*. La diferencia es sutil, pero simple: el proceso de *programar* implica cambiar un bit de valor 1 a valor 0, y solamente eso. Al hablar de *escritura*, entonces también debe contemplarse la transición de 0 a 1 – es decir, la *programación* de una celda es un subconjunto de la *escritura*. Cuando se envía una orden de escritura para un sector determinado, también debe consultarse la FTL para obtener las direcciones físicas que deben modificarse. Una vez identificadas las celdas, se compara su contenido actual con el nuevo contenido. Si los

cambios que se van a realizar implican transiciones *programables*, entonces la solicitud de escritura se satisface sobre las celdas que ya se encuentran asignadas[218]. Si uno solo de los bits debe cambiarse de 0 a 1, entonces se convierte en una operación de escritura propiamente dicha y el *firmware* debe buscar una página "en blanco" para realizar la programación del contenido. Luego se actualiza la FTL para reflejar el mapeo a las nuevas direcciones físicas.

Aclaración: en general, se dirá que una página (o un bloque) está "blanqueada" cuando se resetea su contenido para que todos los bits de sus celdas se encuentren con el valor 1. El blanqueo de las celdas es el paso previo necesario para poder escribir cualquier dato en las mismas. En otras referencias se llama a este proceso "eliminación", pero se prefirió distinguirlo porque no es estrictamente un proceso de eliminación en el sentido clásico.

Tanto para las operaciones de lectura como de escritura, se mencionó la *Flash Translation Layer*, la estructura que ordena y da coherencia a los bloques físicos, que se organizan de acuerdo a los criterios del *firmware* al momento de escribir y organizar los sectores. Sin la FTL, un dispositivo Flash debería almacenar siempre los sectores en los mismos bloques físicos. Las primeras tecnologías Flash, más simples que las actuales, no contaban con FTL y era posible gastar las celdas de los bloques más utilizados hasta el punto de generar una falla prematura en el dispositivo por el desgaste que ocasionan los ciclos P/E sobre las celdas.

[218] Esta es una optimización para reducir la cantidad de ciclos P/E a los que se someten las celdas. Los sistemas de archivo orientados a dispositivos Flash almacenan metadatos aprovechando esta técnica.

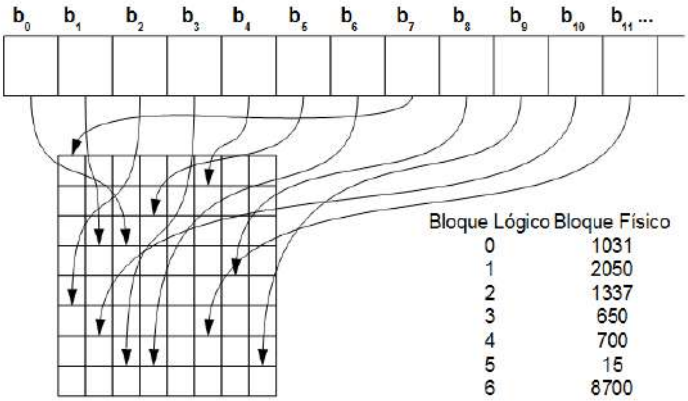


Figura 7.11: Representación de la *Flash Translation Layer*. Las implementaciones reales no son tablas, sino estructuras intermedias entre una tabla y un *log*. Esta temática se puede profundizar en la bibliografía recomendada.

La *Flash Translation Layer* es parte de los sistemas de balanceo de desgaste, o *Wear Leveling*, que se utilizan en los SSDs modernos. Otros componentes importantes de estos sistemas son los contadores de uso de los bloques, y el espacio de almacenamiento adicional (una técnica conocida como *overprovisioning*).

Los contadores de uso permiten que el *firmware* del dispositivo lleve un control y seguimiento de cuántas veces se leyó o se escribió determinada página, y al superar un umbral determinado, reasignar su contenido y actualizar la FTL para reflejar el nuevo mapeo. Tanto las lecturas repetidas como las escrituras son capaces de generar desgaste sobre las celdas y su información[219], por lo tanto, es necesario administrar los bloques para prevenir la corrupción de datos y el desgaste prematuro de las celdas. Siempre que el *firmware* busca un

[219] Aunque el desgaste que causan las operaciones de lectura es distinto al que causan las escrituras.

bloque para escribir contenido, prioriza las páginas y celdas con menor cantidad de escrituras, de forma que el desgaste sea parejo sobre el dispositivo.

Con respecto al almacenamiento adicional, u *overprivisioning*, consiste simplemente en una cierta cantidad de sectores que el dispositivo oculta cuando se expone al sistema operativo. De esta forma, el dispositivo puede contar siempre con sectores adicionales para relocalizar contenido, o contar con bloques ya blanqueados, listos para realizar nuevas escrituras. Por ejemplo, muchos dispositivos SSD que dicen ser de 240 GiB, en realidad cuentan con una capacidad real de 256 GiB, pero se reservan internamente 16 GiB para los mecanismos de *Wear Leveling* y *Garbage Collection*.

Anteriormente se mencionó que, para poder recibir cualquier escritura, se deben blanquear las páginas y las celdas, pero no se especificó que la operación de blanqueo solamente se puede realizar a nivel de bloque (es decir, de a 128 páginas a la vez).

A modo ilustrativo, se plantea la siguiente situación: en un SSD se cuenta con páginas no asignadas y no blanqueadas (es decir, páginas *dirty*), distribuidas a lo largo de todos los bloques del dispositivo, y no se cuenta con páginas en blanco listas para ser programadas. En esta situación, el dispositivo recibe una solicitud de escritura que no puede ser resuelta mediante programación sobre las páginas que componen el sector afectado. Para poder satisfacer la escritura, el *firmware* trata de relocalizar las páginas afectadas, pero al no contar con ninguna en blanco, debe empezar a recorrer los bloques en busca de alguno que se componga en su totalidad de páginas *dirty*. Cuando encuentre un bloque con esa composición, entonces deberá blanquearlo y recién ahí va a contar con páginas en blanco para acomodar el nuevo contenido y mapear estas páginas contra el sector en la *Flash Translation Layer*. Si el *firmware* no encuentra ningún bloque en esa situación, entonces debe “vaciar” un bloque, moviendo sus páginas a otros bloques (en donde pueda), y

ajustar la FTL hasta poder blanquear el bloque. Todo este proceso de búsqueda y relocalización es costoso, en tiempo y energía[220], además del tiempo que se necesita para realizar la escritura.

Al blanquear un bloque, automáticamente se blanquean muchas páginas y se resuelve una parte del problema hasta que nuevamente sea necesario relocalizar páginas para poder blanquearlas. Además, debe tenerse en cuenta que el proceso de búsqueda de páginas y bloques no es trivial, ya que el *firmware* debe tener en cuenta los contadores de desgaste de las páginas para poder elegir las más adecuadas para preservar la vida útil del dispositivo.

Si bien esta situación hipotética puede parecer forzada, sucedía en algunos modelos tempranos de SSD que no contaban con *firmwares* tan avanzados como los dispositivos modernos. Esto ocasionaba que, luego de algunos meses de uso continuo, eventualmente la velocidad de escritura del dispositivo se viera disminuida, y ante las operaciones de escritura pasará más tiempo buscando liberar páginas y reasignando contenido, que efectivamente escribiendo información.

Si bien el *overprovisioning* ayuda a paliar la situación, también se debe considerar un problema que se arrastra desde un nivel de abstracción mayor. Cuando se elimina un archivo, el sistema operativo decide que el contenido de los sectores que lo componían ya no es necesario, pero los dispositivos de almacenamiento no contaban con una forma de aprovechar esa información para así poder marcar las páginas que componen esos sectores como páginas *dirty*, disponibles para blanqueo. Durante un tiempo, algunos fabricantes implementaron soluciones propietarias en sus *firmwares* para que sus SSD pudieran analizar la *Master File*

[220] El proceso de blanqueo de un bloque necesita de un voltaje alto, comparado con los voltajes de operación usuales para un SSD.

Table de NTFS, y así poder determinar qué sectores estaban libres para poder blanquear sus páginas. Esta solución tiene dos problemas, en primer lugar, sólo servía para un sistema de archivos específico. El segundo problema es que se rompe la transparencia de capas entre dos niveles de abstracción, y desde el nivel de *firmware* se accede y se trabaja en base a información del nivel de sistema operativo.

La solución real fue dada por el comando TRIM, especificado en ATA8, que permite al sistema operativo indicarle específicamente a un dispositivo Flash que un conjunto de sectores ya no se encuentra en uso, y pueden blanquearse sus páginas.

Aun aprovechando el comando TRIM, el proceso de blanqueo demora mucho tiempo comparado con las demás operaciones, y no debería realizarse a la par de las operaciones de escritura, por lo que es necesario un mecanismo adicional para evitar la degradación de rendimiento en escrituras.

Ese mecanismo es el *Garbage Collector*, análogo a los *Garbage Collectors* de los lenguajes de programación que cada cierto tiempo intentan liberar memoria, el GC de un dispositivo Flash cada cierto tiempo intenta blanquear páginas. El objetivo del *Garbage Collector* es que siempre haya páginas blanqueadas para poder satisfacer las solicitudes de escritura con un rendimiento constante. Esto se logra manteniendo un porcentaje de páginas siempre blanqueadas. Si el porcentaje de páginas en blanco cae por debajo de un umbral determinado, en los momentos en que el dispositivo se encuentra ocioso, el *firmware* relocaliza páginas para blanquear bloques. Una vez que se activa el proceso, trata de llegar a un determinado nivel de páginas blanqueadas antes de detenerse[221].

[221] Dependiendo el mercado objetivo del dispositivo, el *Garbage Collector* puede ser más o menos agresivo, y, por lo tanto, resultar

Una característica fundamental del *Garbage Collector* es que, aunque se apoya en el comando TRIM que corresponde al nivel del sistema operativo, es inherentemente un proceso del *firmware*. Por lo tanto, siempre que el dispositivo se encuentre prendido, puede dispararse el GC y no hay forma de detenerlo desde el sistema operativo.

La utilización de un *Garbage Collector* permite al SSD que las escrituras se realicen la mayor parte del tiempo a la velocidad de programación de las celdas, sin necesitar que se realicen operaciones de blanqueo de páginas. Por supuesto, todas las operaciones de relocalizado y blanqueo que se realicen para relocalizar páginas como consecuencia del proceso de *Garbage Collection* mantienen la coherencia de la *Flash Translation Layer*.

Para la explicación de estos conceptos se tomó un compromiso entre simplicidad, claridad y rigurosidad, sin embargo, el detalle de los mecanismos reales es más complejo. Si el lector desea profundizar, se recomienda la consulta de la bibliografía al final del capítulo.

7.3. Consecuencias para el carving

Las cuestiones vinculadas con la *Flash Translation Layer*, el *overprovisioning*, *wear leveling*, blanqueo de páginas y *Garbage Collection* han inducido la noción de que “los SSD eliminan realmente la información y no es posible realizar carving”. En esta sección, se hará un análisis de la situación considerando realmente cómo funcionan e interactúan entre si los distintos mecanismos y la tecnología Flash en sí.

- En primer lugar, es cierto que al blanquear una página el contenido de los sectores contenidos en ella se elimina, y ya no es posible recuperarlo.

---

en que la información sea más o menos volátil en distintos dispositivos.

- Sin embargo, por las operaciones de la *Flash Translation Layer*, la forma en que se realizan las escrituras y los mecanismos que buscan controlar el desgaste, es probable que haya copias de una página, o de versiones anteriores.
  - En algunos dispositivos móviles que usan *sistemas de archivos* YAFFS y YAFFS2 se puede utilizar esta característica para hacer una reconstrucción de archivos eliminados.
  - Cabe destacar que YAFFS y YAFFS2 son sistemas de archivos especialmente pensados para dispositivos de almacenamiento Flash que no cuentan en su *firmware* con la lógica necesaria para administrar estas cuestiones.
- Otro punto de interés es el *Garbage Collector* y su funcionamiento. Si bien hay estudios que validan que el solo hecho de tener un SSD prendido (es decir, con energía, pero sin recibir operaciones del sistema operativo) es suficiente para que se realice el proceso de *Garbage Collection* y se elimine información, también se debe tener en cuenta los parámetros de umbral de activación y la meta de bloques libres que pretende lograr el dispositivo.
  - Para simplificar, conectar un SSD es suficiente para que el dispositivo comience a eliminar información, pero tampoco se puede garantizar que por estar conectado, el dispositivo comenzará a eliminar información.
  - Nuevamente, el comportamiento del dispositivo depende del fabricante, modelo y mercado objetivo del dispositivo.
- También hay estudios que muestran como, debido a las complejidades de los mecanismos de *wear leveling* y *Garbage Collection*, se dan situaciones en donde

sectores de archivos eliminados permanecen en el dispositivo Flash mucho tiempo después de la eliminación de un archivo.

- En los últimos años, se han implementado criterios sobre cómo puede responder el dispositivo a un comando TRIM y su comportamiento al intentar acceder a un sector que fue marcado como libre por dicho comando.
- King y Vidas realizaron un estudio muy completo y detallado sobre el funcionamiento de varios modelos de SSD para determinar la capacidad de recuperación de los dispositivos en distintos escenarios.
- En general, en la medida que el sistema operativo y el dispositivo Flash soporten el comando TRIM, se hace más probable que el mismo blanquee los sectores de los archivos eliminados y la información se pierda.

Es evidente que el panorama de recuperación y, específicamente, *carving* sobre un dispositivo Flash es complejo. Si el sistema operativo utiliza el comando TRIM (es razonable asumir que todos los sistemas operativos modernos lo hacen), las probabilidades de acceder a la información eliminada disminuyen notablemente, más aún si el dispositivo de almacenamiento utiliza alguna estrategia de *Deterministic Read After TRIM* o *Deterministic Zero After TRIM*.

A lo largo de esta sección se hicieron pocas distinciones y se habló en general de medios de almacenamiento Flash y SSDs como si fueran conceptos indistintos, cuando en realidad debe tenerse en cuenta que, por cuestiones de costos y economía, no todos los medios de almacenamiento Flash son iguales. Los SSDs representan la máxima complejidad y performance, y en ellos se encuentran toda la dificultad y los desafíos que se consideraron en este análisis. Por otra parte, las tarjetas de memoria (SD, microSD, Compact Flash, etc.) y ahora los dispositivos eMMC

pertenecen a otra categoría de almacenamiento Flash. Si bien comparten la tecnología de base, las implementaciones de los mecanismos que se explicaron en esta sección no funcionan de forma tan agresiva, ni tampoco los productos cuentan con *firmwares* e incluso *hardware* tan complejo como los SSDs – esto resulta en productos más económicos, de menor performance, y en los cuales suele haber mayores probabilidades de recuperación de información durante un análisis forense.

También se mencionaron distintos trabajos, que se encuentran citados en la Bibliografía del capítulo, donde se analiza en detalle y con rigurosidad la cuestión de recuperación sobre dispositivos Flash, y todos los estudios llegan a conclusiones similares: por lo general es más difícil, pero no imposible recuperar información de un dispositivo Flash. En la medida que la importancia de lo que se desea recuperar lo justifique, es posible hacer esfuerzos adiciones para superar estas dificultades.

Una última consideración al respecto, y que abre el panorama a la siguiente sección, es que los mecanismos que se explicaron corresponden al funcionamiento de las memorias tipo Flash, que es sólo uno de los tipos de memoria de estado sólido, aunque el más extendido en la actualidad. Hay situaciones en los que sigue siendo preferible utilizar almacenamiento HDD, y también hay tecnologías nuevas que podrían reemplazar, en el mediano a largo plazo, la tecnología Flash en el ámbito del almacenamiento en estado sólido.

7.4. Tecnologías futuras

La tecnología de almacenamiento Flash actual, si bien es una solución madura, está llegando a sus límites. A medida que las celdas reducen su tamaño, si bien aumenta la densidad de información que se puede obtener, también aumentan las complicaciones. Por ejemplo, con los procesos de fabricación de menos de 20 nanómetros, la resistencia de las celdas a los ciclos P/E disminuye notablemente, y se

calcula que las celdas de tecnología multinivel pueden resultar con vidas útiles de menos de 100 ciclos, un contraste grande comparado con las celdas de único nivel que tienen vidas útiles de 10.000 a 1.000.000 de ciclos P/E, dependiendo del proceso de fabricación.

Dado que el mercado exige las mayores densidades de datos, y también una mayor economía de fabricación, y estas ventajas se logran a través de los procesos de fabricación más pequeños, los fabricantes de memorias Flash están estudiando y desarrollando mejoras incrementales sobre la tecnología, y también tecnologías alternativas de almacenamiento en estado sólido, candidatas a suceder a la tecnología Flash en su forma actual. Se hará un breve comentario sobre tres tecnologías que han sido propuestas como posibles sucesores de Flash en cuanto al almacenamiento de información en estado sólido:

- *Phase-Change Memory* (PCM), o memorias de cambio de fase.
- *Magnetoresistive Random-Access memory* (MRAM), o memoria de acceso aleatorio magnetoresistiva.
- *Meristors*, o memoresistores.

En las *Phase-Change Memory*, la celda que almacena la información utiliza un elemento de vidrio amorfo especial, capaz de cambiar su estructura de acuerdo a los cambios en la temperatura. Estos cambios se inducen a través del paso de una corriente eléctrica, y las propiedades del vidrio permiten que se establezcan varios niveles intermedios entre los extremos de una estructura totalmente cristalina y una totalmente amorfa. El cambio de fase se produce más rápidamente, y no es necesario pasar por estados intermedios, como en las celdas Flash, lo que resulta en operaciones de escritura más rápidas comparativamente. Además, la capacidad de almacenar múltiples bits por celda sin afectar el rendimiento es una cualidad sumamente

interesante. El principal problema de este tipo de memorias es su sensibilidad a los cambios de temperatura.

Por otro lado, las memorias tipo *Magnetoresistive Random-Access Memory* son una tecnología más madura, que existe hace varias décadas, pero resultó confinada a nichos de mercado muy específicos, ya que otros tipos de memoria presentaban ventajas y permitían casos de uso más amplios. Como medio de almacenamiento no volátil, MRAM presenta varias ventajas frente a Flash: el proceso de escritura es más rápido, no se necesita resetear las celdas, tienen un consumo eléctrico menor y los procesos de escritura no generan desgaste. Sin embargo, debido a que la tecnología Flash permitió mayores densidades de datos con desarrollos tempranos, MRAM no resultó competitiva en un principio. Actualmente, de cara a los problemas que enfrenta Flash como tecnología, se evalúa a MRAM como una alternativa interesante de reemplazo.

A fines de los años 70 se describió matemáticamente un nuevo componente electrónico básico, capaz de variar su resistencia eléctrica en base a cuánta corriente fluyó a través de él. De manera muy simplificada, puede decirse que este componente “recuerda” el flujo de corriente variando su resistencia, por ende, se lo decidió llamar *memristor* (en inglés) o memoresistor.

La tecnología de memoresistores es única en muchos aspectos: tiene múltiples aplicaciones, desde memorias principales, memorias secundarias, robótica, circuitos, redes neuronales, por nombrar algunas. En particular sobre su utilización como medio de almacenamiento, se presenta como una tecnología capaz de suceder a Flash con una altísima densidad de datos (HP cita cifras de 100 TiB para dispositivos en formato de 2,5 pulgadas), mayor velocidad de operación y menor consumo eléctrico. Sin embargo, esta tecnología no es lo suficientemente madura, y los anuncios de HP y Hynix al respecto, hasta el momento, no se han cumplido.

Estas tres tecnologías que se presentaron son tres posibles sucesoras de la tecnología Flash en cuanto al almacenamiento de información en estado sólido, y las tres comparten una característica en común junto con el almacenamiento ferromagnético clásico: no es necesario eliminar la información para volver a escribir en ellas. En al menos dos de estas tecnologías incluso resultaría contraproducente, ya que el proceso de escritura es más costoso (en tiempo y energía) que el proceso de lectura. Con la adopción de estas tecnologías, volvería a ser válido el supuesto de permanencia de la información en el medio físico, que posibilitó el desarrollo del *carving* como técnica de recuperación de datos.

8. Anexo técnico II. Formatos de Archivo

En la sección dedicada a los algoritmos de *carving* de este capítulo se mencionaron tanto algoritmos que se apoyan en la estructura de los archivos, como herramientas complementarias que se utilizan para validar los resultados de un programa de *carving*. El estudio detallado de las estructuras se dejó de lado, para concentrarse en el marco teórico específico del *carving*. En esta sección, se presentan algunos formatos de archivo y estrategias para el análisis de su estructura y validación.

8.1. Formato TXT

Si bien históricamente se ha tratado a los archivos de texto como un formato de archivo simple y aislado de los formatos binarios, esto es una confusión simple. Sucede que los archivos de texto en realidad respetan un formato binario extremadamente simple, y esta separación en archivos binarios y archivos de texto proviene simplemente de la capacidad de los humanos para interpretar con relativa facilidad los archivos de texto.

En su forma más simple se puede definir un archivo de texto de la siguiente forma: es una secuencia de *tokens* que representan caracteres de un alfabeto.

Puede considerarse que un archivo de texto llega a su fin con la primera ocurrencia de un carácter no imprimible, o con la presencia de algunos caracteres especiales (por ejemplo, el carácter *End of File* o EOF).

En general, los *tokens* se representan de acuerdo a una tabla de caracteres, y cada identificador dentro del archivo de texto es una referencia a un índice dentro de esta tabla. Históricamente, si se utiliza la Tabla ASCII (ya sea ASCII-7 o la versión extendida, ASCII-8), los índices dentro de esta tabla pueden representarse con 7 u 8 bits. Con la expansión de las computadoras a nivel mundial, y el auge de la internacionalización en los últimos años, este supuesto ya no es del todo válido y es posible encontrar archivos de texto codificados de acuerdo a distintas implementaciones de Unicode. A modo de simplificar el análisis, se considerará de aquí en adelante que, al hablar de archivos de texto, se aplica la codificación ASCII o UTF-8, que resulta muy similar.

Otra cuestión importante a considerar sobre los archivos de texto es la forma de indicar el fin de línea, una cuestión simple que varía de un sistema operativo a otro:

- En Linux el fin de una línea se indica con el carácter especial *Line Feed* o LF, que se representa como \n.
- Mac en cambio marca el fin de una línea con el carácter especial *Carriage Return* o CR, que se representa como \r.
- Windows utiliza la secuencia CR-LF, es decir, dos bytes, para indicar el fin de línea.

Si se desea buscar en un dispositivo de almacenamiento los bloques que probablemente contengan datos de texto, se debe buscar secuencias de bytes cuyos rangos varíen entre el valor 32 y 127 (es decir, los rangos de la Tabla ASCII-7 que

corresponden a caracteres imprimibles). Si se quiere considerar textos en idiomas que utilizan símbolos de la Tabla ASCII Extendida, entonces deben tolerarse algunos valores por encima de 127. Esta búsqueda debería realizarse con algún algoritmo de ventana deslizante que permita analizar un rango de bytes a la vez, y determinar si dentro de la ventana se cumplen condiciones para que se considere la información como una cadena de texto. Además, con el corrimiento de la ventana se puede determinar con bastante precisión dónde termina la sección de datos de texto. Esta es una descripción general de cómo funciona el comando *strings* de Linux, aunque este comando además presenta opciones para buscar en representaciones Unicode que funcionan de acuerdo a otras heurísticas.

8.2. Formato PPM

Portable PixMap es un formato de archivo conceptualmente simple que permite guardar imágenes. Se define un encabezado compuesto por un identificador de forma, ancho y alto de la imagen y el valor máximo a representar. Todos los campos del encabezado son cadenas de texto, separados por el carácter LF. También pueden indicarse líneas del encabezado como comentarios, si comienzan con el símbolo numeral #. Luego del encabezado, siguen HxW tripletes de valores RGB (codificados en binario, o como strings ASCII dependiendo del modo de archivo). Por ejemplo, si se utiliza el identificador P6 corresponde a un archivo binario, mientras que el identificador P3 indica un archivo ASCII.

A continuación, se muestra un ejemplo de un archivo PPM muy simple y su representación gráfica:

```
P3
# Ejemplo PPM – P3 = ASCII
# 3 columnas y 3 filas
# El valor máximo es 255
3 3
255
255 0 0 0 255 0 0 0 255
255 255 0 0 255 255 255 0 255
255 255 255 0 0 0 64 128 255
```

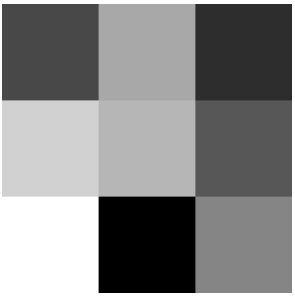


Figura 7.12: Representación gráfica del archivo PPM de ejemplo.

En el caso de un archivo en formato ASCII (P3), se pueden aplicar reglas y heurísticas similares a las del formato TXT para realizar la correcta recuperación del mismo, además del encabezado se puede determinar cuántos tripletes de información se deben recuperar para formar el archivo (pero por tratarse de representaciones en ASCII de los números, no se puede deducir la cantidad de bytes).

Por otra parte, en el caso de un archivo en formato binario (P6), si se puede derivar el tamaño en bytes en base al

alto y ancho del archivo, pero es más difícil aplicar heurísticas para detectar la corrupción con otro archivo.

8.3. Formato PNG

El formato de imágenes *Portable Network Graphics* o PNG es más interesante, más estructurado y muy prolijo. Por su capacidad para guardar imágenes sin pérdida de calidad y su capacidad de trabajar con hasta 32 bits de color en RGB + Alpha (donde el canal Alpha representa el grado de opacidad), es un formato que se ha extendido y se utiliza con bastante frecuencia, por ejemplo, para el diseño de interfaces de usuario y páginas web.

En cuanto a la estructura de los archivos resulta un formato muy regular y prolijo: toda la información se almacena en *chunks*[222] de alguno de los tipos definidos, e incluso hay reglas para que un programa pueda introducir *chunks* no estándar sin generar incompatibilidades con *encoders* y *decoders* existentes.

Cada *chunk* comienza con un encabezado de 4 bytes, luego 4 bytes más para indicar su longitud, el área y de datos, y al finalizar esta, un CRC-32 que ayuda a verificar la integridad de la información.

[222] Si bien la traducción sería “trozo” o “trama”, estas no se consideraron adecuadas para representar el sentido semántico que acompaña a la palabra *chunk*.

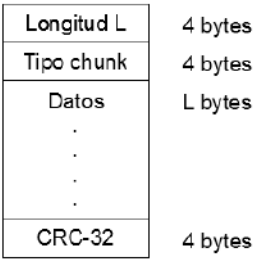


Figura 7.13: Estructura de un *chunk* PNG.

En la figura 7.13 nótese que el campo “Longitud” define solamente la Longitud del segmento de Datos del *chunk*. Es decir, que un segmento PNG, en teoría, tiene un tamaño máximo de 2^{32} + 12 bytes.

Se definen 4 tipos de *chunk* críticos en PNG, que cualquier decodificador debe poder interpretar correctamente:

- **IHDR** debe ser siempre el primer *chunk* en cualquier archivo PNG, y contiene información que define el alto, ancho, la profundidad en bits y el modo de color para la imagen.
- **PLTE** contiene la paleta de colores, en el caso que el modo de color elegido la necesite.
- **IDAT** contiene la imagen propiamente dicha. La información completa de imagen puede encontrarse dispersa entre múltiples *chunks* IDAT.
- **IEND** es el *chunk* que marca el final de un archivo PNG. Incluso este *chunk* viene acompañado por su tamaño y CRC. Dado que el tamaño del *chunk* IEND siempre es 0, el CRC también es constante y puede considerarse todo como un *footer* de 12 bytes de largo.

Además, hay otros tipos de *chunk* auxiliares, que definen distintas características: bKGD, cHRM, gAMA, hIST, iCCP, iTXT, pHYs, sBIT, sPLT, sRGB, sTER, tEXt, tIME, tRNS

y zTXt. Los detalles sobre la funcionalidad de cada uno de estos *chunks* pueden encontrarse tanto en la especificación de PNG como en artículos y trabajos que analizan el formato.

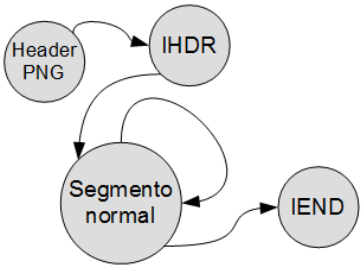


Figura 7.14: Diagrama de la estructura de un archivo PNG.

Debido a que se aceptan los *chunks* no estándar en el formato, se indicaron como "*chunks* normales" a aquellos que no son IHDR ni IEND.

Dado que las reglas para la estructura de un archivo PNG son simples, y no hay excepciones, se puede validar un archivo en este formato muy fácilmente:

- El *header* o *magic number* del archivo debe ser la secuencia `0x89504E470D0A1A0A`.
- Inmediatamente después del *header*, tiene que haber un *chunk* IHDR.
- Luego se sucede una secuencia de *chunks* de cualquier tipo.
- Una vez que se encuentra un *chunk* IEND, se puede asumir que se llegó al final del archivo.
- Todos los *chunks*, incluidos IHDR e IEND, deben tener un tamaño válido y coincidir su CRC con el CRC de sus datos.

Dado que estas reglas son tan simples, es posible construir un validador muy rápido y que, solo trabajando a

nivel de estructura del archivo, no necesite de niveles superiores, más lentos y difíciles de implementar.

8.4. Formato JPG

El formato JPG (o JPEG, por *Joint Photographics Expert Group*) es un formato de archivo diseñado desde su concepción para almacenar fotografías en forma digital. Se caracteriza por aplicar un algoritmo de compresión *lossy* (es decir, que induce pérdidas de datos, en pos de lograr una mayor tasa de compresión), basado en modelos sobre la visión y características de representación de señales. Debido a su excelente capacidad de compresión, con pocos artefactos visuales si se ajustan los parámetros adecuadamente, su uso se encuentra muy extendido: va desde páginas web, cámaras de fotos digitales, celulares, incluso como "*códec*" de compresión de video[223].

Históricamente, se desarrolló luego que TIFF (*Tagged Image File Format*), del que hereda algunos conceptos, pero antes que PNG. Dado que el estándar PNG tomó como ejemplo algunas cuestiones de JPG, hay pequeñas coincidencias entre ambos formatos.

Un archivo JPG se separa en unidades discretas o segmentos, que indican su inicio con un marcador o *marker*, seguido de un campo de longitud y finalmente los datos. Tanto el *marker* de segmento, como el campo de longitud, ocupan 2 bytes cada uno.

[223] M-JPEG, o Motion JPEG, consiste en comprimir con JPG cada fotograma de un video, usualmente con un parámetro de calidad bajo. Se desarrolló para incluir la capacidad de grabación de video en dispositivos de bajo costo sin tener que incluir *hardware* especializado para compresión de video.

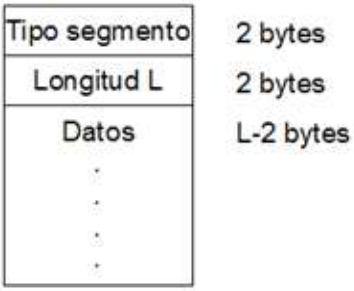


Figura 7.15: Estructura de segmento JPG. Algunos tipos de segmento no respetan esta estructura, y tienen reglas propias para la longitud de su sección de datos.

Todos los marcadores de segmento tienen que empezar con el carácter 0xFF, un carácter reservado en JPG, lo que permite un máximo de 255 tipos de segmento. Para el segundo byte, también hay algunas reglas, por ejemplo, los marcadores `0xFFE0` a `0xFFEF` corresponden a los segmentos de aplicación, y sólo deben utilizarse para el propósito de entregar información específica de aplicación a un *decoder*, pero no influir sobre el dibujado de la imagen. La definición de los tipos de segmento más comunes, y las reglas que se aplican, pueden encontrarse en la documentación del estándar.

Otra característica es que, al utilizar solamente 2 bytes para el tamaño de segmento, el tamaño máximo de un segmento es de 64 KiB. Sin embargo, varios tipos de segmento no respetan el campo Longitud, y utilizan reglas distintas:

- Los segmentos *Start of Image* (SOI) y *End of Image* (EOI), que son los indicadores de inicio y fin de un archive JPG, se componen únicamente del *marker* de segmento, sin campos Longitud ni Datos.
- Los segmentos DRI, DNL y EXP, tienen longitudes fijas de 4, 4 y 3 bytes respectivamente. Son segmentos que

se utilizan para almacenar información de parámetros especiales en modos JPG que se utilizan con poca frecuencia.

- Los segmentos *Start of Scan* (SOS) son los que almacenan la información de imagen propiamente dicha, codificada mediante Huffman o una codificación algebraica. En estos segmentos, si bien el campo Longitud se encuentra presenta, la longitud real del segmento es variable, y su sección de datos finaliza cuando se encuentra un segmento JPG válido.
  - Los *Restart Markers* no indican el fin de una zona de datos dentro de un segmento SOS.
  - Si por alguna razón se debe almacenar el byte `0xFF`, se almacena como la secuencia `0xFF00` para no generar una confusión con un *marker*.

Estas reglas especiales que se aplican dependiendo del tipo de segmento y no respetan la estructura normal de segmento introducen complejidades que dificultan la interpretación correcta, y la validación de los archivos JPG.

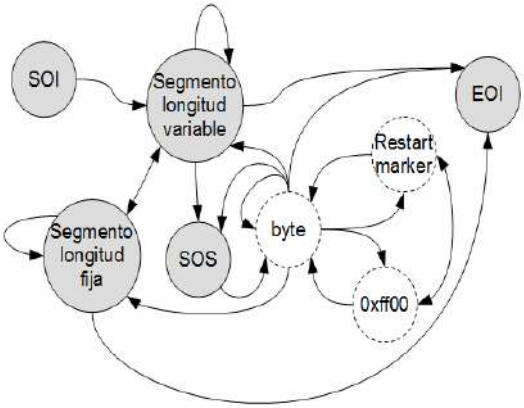


Figura 7.16: Diagrama de estructura para el formato JPG.

La estructura real del formato JPG es incluso más compleja que cómo lo muestra la figura 7.16, porque deben

respetarse algunas cuestiones de precedencia en los segmentos, pero se evitaron para mantener una cierta claridad en el diagrama.

Dado que el formato resulta complejo, su descripción detallada escapa a los alcances de esta sección. Si se quiere profundizar, se recomienda tanto la lectura del estándar JPG como de trabajos referenciados que analizan el formato a mayor profundidad.

Bibliografía

Advanced Carving Techniques – Michael Cohen

El Estado Actual de las Técnicas de File Carving y la Necesidad de Nuevas Tecnologías que Implementen Carving Inteligente – Bruno Constanzo, Julián Waimann

El framework CIRA, un aporte a las técnicas de file carving" – Ana Di Iorio, Martín Castellote, Ariel Podestá, Fernando Greco, Bruno Constanzo, Julián Waimann

Carving contiguous and fragmented files with fast object validation" – Simson Garfinkel

Empyrical analysis of solid state disk data retention when used with contemporary operating systems" – Christopher King, Timothy Vidas

Data Carving Concepts" – Antonio Merola

The Evolution of File Carving" – Anandabarata Pal, Nasir Memon

Scalpel: A frugal, high performance file carver" – Golden Richard, Vassil Roussev

In-place File Carving" – Golden Richard, Vassil Roussev, Lodovico Marziale

An Analysis of Disc Carving Techniques" - Nicholas Mikus http://cisr.nps.edu/downloads/theses/05thesis_mikus.pdf

Analysis of 2007 DFRWS Forensic Carving Challenge" – Joachim Metz, Bas Kloet, Robert-Jan Mora http://users.du.se/~hjo/cs/dt2018/readings/week1/dfrws2007_carving_challenge.pdf

Turning Android inside out – DFRWS 2011 Challenge" – Ivo Pooters, Fox-IT https://digital-forensics.sans.org/summit-archives/2011/2-taking-it-to-the-next-level.pdf

MySQL Record Carving" – Esan Wit, Leendert van Duijn, SNE University of Amsterdam and Fox-IT, http://delaat.net/rp/2013-2014/p51/presentation.pdf

SSD Forensics 2014" – Yuri Gubanov, Oleg Afonin, Belkasoft Research https://belkasoft.com/ssd-2014

SSD Forensics 2016" – Yuri Gubanov, Oleg Afonin, Belksaoft Research https://belkasoft.com/ssd-2016

Capítulo 8. Recuperación de Datos de RAID

Autores: Bruno Constanzo, Hugo Curti y Juan Ignacio Iturriaga.

1. Forensia en entornos distribuidos.
2. Unidades de RAID. 2.1 Niveles de RAID. 2.2 Niveles Anidados 2.3. Implementaciones de RAID
3. Recuperación de información. 3.1 Procedimientos recomendados. 3.2 Reconstrucción: último recurso. 3.3 Extensión de la técnica aplicada en otras situaciones.
4. Conclusiones.

1. Forensia en entornos distribuidos

En el estudio de los Sistemas Distribuidos pueden analizarse cuestiones específicas, sean servidores, máquinas virtuales o sistemas en la nube. Un aspecto de especial interés, tanto por el desafío técnico como por la necesidad de los peritos informáticos, es cómo proceder ante la presencia de arreglos de discos.

El uso de arreglos RAID (*Redundant Array of Independent Disks*), en sistemas de mediano a gran tamaño, presenta varias cuestiones a los informáticos forenses, entre los que se encuentran el no contar con la capacidad de almacenamiento para realizar una adquisición completa del volumen RAID, que la adquisición del arreglo RAID no haya seguido un procedimiento adecuado para obtener la información completa, o que exista daño físico en el sistema. Si no se siguen los procedimientos correctos el resultado puede resultar en una pila de discos (o imágenes de discos) potencialmente sin valor para la investigación judicial, por ser complicado, o imposible, acceder a la información en forma coherente y por ende resultar inútil como evidencia.

En este capítulo se van a exponer conceptos básicos de RAID y cómo proceder ante su presencia relacionado a las fases, actividades y tareas del modelo PURI más relevantes para estos casos. Finalmente se desarrolla una técnica para reconstrucción de arreglo de discos para utilizar como último recurso, para la cual se plantea una situación de problema ejemplo, un entorno de pruebas y la técnica propiamente dicha.

2. Unidades RAID

Se denomina «Unidad RAID» (*Redundant Array of Independent Disks*) a un conjunto de discos organizados y administrados de tal modo que se muestran, a los niveles superiores, como un único dispositivo. El objetivo de las unidades RAID es aprovechar la sinergia que se genera a

partir de varios discos, que trabajan juntos, para lograr una mejora en capacidad, velocidad y/o tolerancia a fallos respecto de los mismos discos trabajando cada uno por separado.

La ***capacidad*** se puede mejorar por agregación. Del conjunto de discos se puede llegar a obtener una capacidad equivalente a la suma de las capacidades de cada disco por separado, permitiendo la emulación de un dispositivo de mayor capacidad.

La ***velocidad*** se puede mejorar por paralelismo. Normalmente, debido a una propiedad conocida como «localidad espacial», los niveles superiores requieren transferir varios bloques consecutivos de información. Si estos bloques se almacenan estratégicamente en discos diferentes, la transferencia de los mismos puede ser solicitada en paralelo, ganando por lo tanto velocidad de lectura y/o escritura. En un caso óptimo, la velocidad de transferencia puede incrementarse al producto entre la velocidad de transferencia del disco individual más lento y la cantidad de discos contenida en el conjunto.

La ***tolerancia a fallos*** refiere a la capacidad del conjunto de soportar la rotura de algunos de sus componentes sin perder información. Se consigue mediante la redundancia. Por ejemplo, almacenando información redundante entre los diferentes discos se puede reconstruir la información contenida en un disco roto combinando la información contenida en los demás discos.

Una consecuencia, y tal vez fundamento, del uso de esta tecnología es la **económica**, las características mencionadas se obtienen de combinar discos reales con un costo relativamente bajo. Si se buscara un dispositivo único real con las mismas características que un arreglo de discos, en caso de existir, probablemente sería mucho más costoso.

Dependiendo la configuración de RAID que se utilice, se refuerzan en mayor o menor medida estos aspectos. Como se

verá más adelante, hay configuraciones que sacrifican la capacidad de almacenamiento por redundancia, o al revés, sacrifican la redundancia por mayor capacidad de almacenamiento. También hay configuraciones que establecen un balance entre capacidad y redundancia, a un costo de rendimiento.

Aunque históricamente RAID presentaba una forma de lograr volúmenes virtuales de gran tamaño, y aún hoy lo permite, el principal atractivo se encuentra en las mejoras de performance y tolerancia a fallos que permite con respecto a un único dispositivo físico.

2.1. Niveles de RAID

Debido a que las características mencionadas, capacidad, velocidad y tolerancia a fallos, tienen un nivel de compromiso entre sí, es decir, para mejorar una hay que sacrificar a la otra, distintas implementaciones de RAID buscan un equilibrio diferente entre las mismas dependiendo del problema que se desea resolver. Por esta razón existen 7 implementaciones o niveles estándar de RAID. Se describen brevemente a continuación los niveles de RAID que se utilizan en la actualidad.

RAID 0

El RAID de nivel 0, también conocido como volumen dividido (*striped volume*), permite mejorar la velocidad de acceso a través del paralelismo. Los bloques se dividen en grupos, denominados *chunks*, que se almacenan en forma alternada entre los diferentes discos, de forma que una lectura o escritura secuencial podrá ser procesada mediante lecturas o escrituras a varios discos del conjunto en forma simultánea. La figura 8.1 muestra la forma en que se distribuyen los grupos de bloques en un RAID 0 de dos discos.

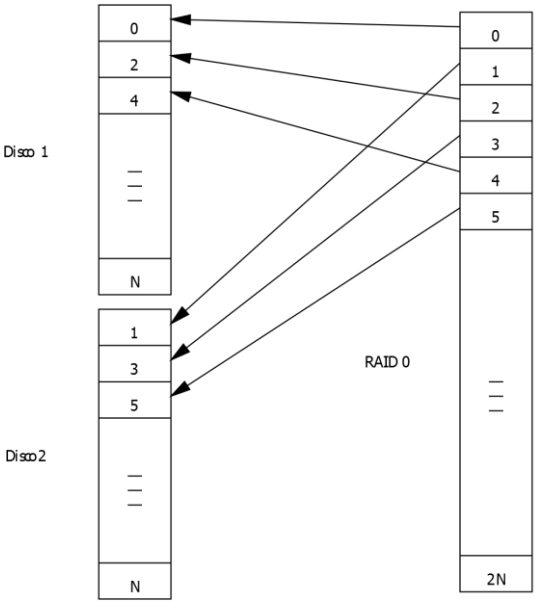


Figura 8.1: Distribución de los grupos de bloques en un RAID 0 de dos discos.

El RAID 0 provee mejora de velocidad tanto de lectura como de escritura, pero no provee tolerancia a fallos. Solamente conviene utilizarlo cuando la información que se guarda en ellos no es original (por ejemplo, para la implementación de *caches*).

RAID 1

El RAID de nivel 1, también conocido como volumen espejado (*mirrored volume*), permite mejorar la velocidad de lectura y la tolerancia a fallos mediante la copia idéntica de la información en dos o más volúmenes. La velocidad de lectura puede mejorarse de manera similar a como se hace en el RAID 0, pero la velocidad de escritura será en el mejor de los casos la misma que en un disco individual. El RAID 1 protege de la rotura de todos los discos que lo conforman menos uno, pudiéndose recuperar toda la información de la copia sana. La

figura 8.2 muestra la distribución de los grupos de bloques en un RAID 1 de dos discos.

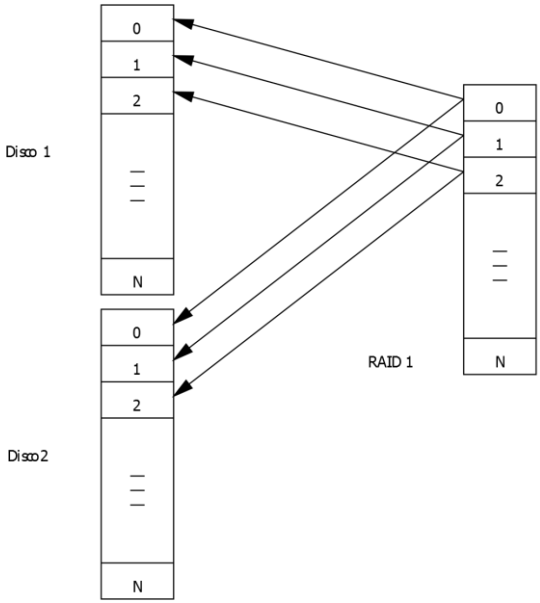


Figura 8.2: Distribución de los grupos de bloques en un RAID 1 de dos discos.

El RAID 1 con dos discos es una buena solución para guardar información original, aunque se vuelve inconveniente implementarlo con más de dos discos debido a que se aprovecha muy poco espacio.

RAID 2 y 3

Los RAID de niveles 2 y 3 se basan en paralelizar la solicitud a un bloque individual guardando los bits (en el nivel 2) y los bytes (en el nivel 3) que los componen en diferentes discos, guardando además información redundante para mejorar la tolerancia a fallos. Estos niveles no son utilizados en la actualidad, debido a que la lectura de un bloque individual requiere el acceso a todos los discos en forma simultánea, y a que para ser eficientes requieren que los

discos estén sincronizados entre sí, algo costoso y poco común en los discos modernos que traen sus controladoras incorporadas.

RAID 4

El RAID de nivel 4, también conocido como volumen dividido con paridad dedicada (*striped volume with dedicated parity*), está conformado por una configuración similar al RAID 0, pero agrega además un disco más que se utiliza para guardar información de paridad de los otros discos. Los datos contenidos en este disco son redundantes y permiten la reconstrucción total de la información contenida en el volumen si se destruye hasta un máximo de un disco del volumen. El RAID 4 ofrece un buen rendimiento en lectura, con una mejora teórica de velocidad de hasta n-1 (siendo n la cantidad de discos del volumen) y un buen rendimiento en capacidad, que también es la suma de las capacidades de todos los discos del volumen menos el de paridad. Sin embargo, el desempeño en escritura es muy pobre, debido a que cada escritura impacta en el disco de paridad y por lo tanto este se convierte en el cuello de botella del volumen. La figura 8.3 muestra una configuración de RAID 4 de 3 discos (la mínima configuración posible). Los conjuntos de bloques indicados como P guardan datos de paridad.

El RAID 4 es utilizado muy pocas veces en la actualidad, debido a su pobre desempeño en escritura. Sin embargo, en algunos casos especiales puede llegar a convenir, por ejemplo, cuando se dispone un disco mucho más rápido que los otros en el volumen, o cuando las aplicaciones realizan un número considerablemente mayor de lecturas que de escrituras.

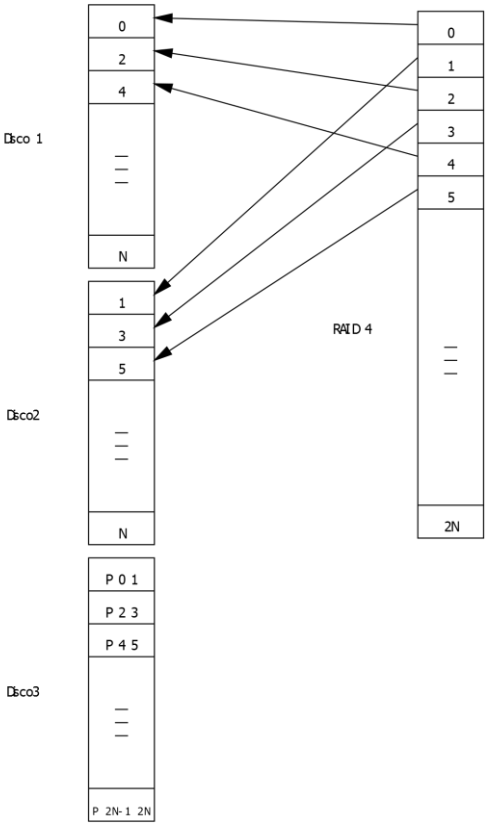


Figura 8.3: Distribución de los grupos de bloques de un RAID4

RAID 5

El RAID 5, también conocido como volumen dividido con paridad distribuida (*stripped volume with distributed parity*) parte de una configuración similar a la del RAID 4, pero distribuye los bloques utilizados para guardar el cálculo de paridad entre todos los discos, distribuyendo la penalidad de la doble escritura entre todos los discos y eliminando el cuello de botella. En lectura y capacidad el RAID 5 se desempeña similar al RAID 4, mientras que en escritura lo supera ampliamente. La figura 8.4 muestra la distribución de los

grupos de bloques en un RAID 5 de 3 discos. Los bloques indicados como P guardan datos de paridad.

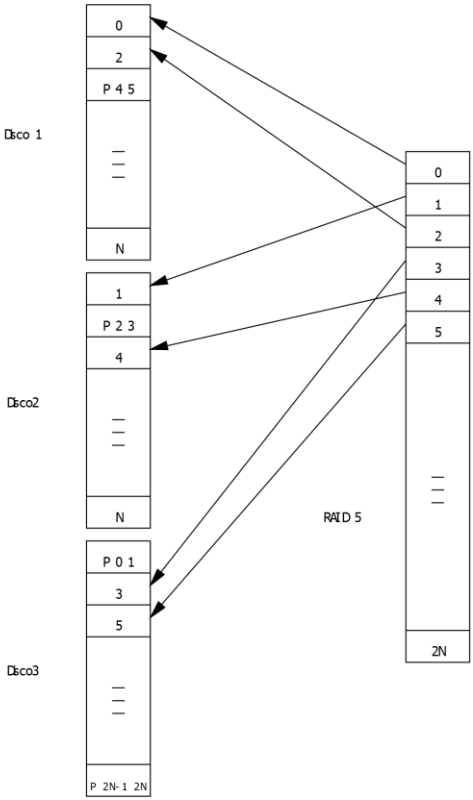


Figura 8.4: Distribución de los grupos de bloques en un RAID 5.

La configuración de RAID 5 es una de las más utilizadas en servidores para uso general, por tener un buen equilibrio de desempeño tanto en velocidad como en capacidad y tolerancia a fallos.

RAID 6

El RAID de nivel 6 también conocido como volumen dividido con doble paridad distribuida (*double distributed parity striped volume*) requiere de un mínimo de cuatro discos y lleva dos informaciones de paridad. La distribución es parecida a la

de un RAID 5, pero aprovecha la capacidad de todos los discos menos dos. El RAID 6 protege el total de la información ante la ruptura total de hasta dos discos, y se utiliza para configurar volúmenes con una cantidad importante de discos donde la probabilidad de la ruptura simultánea de dos discos no es despreciable.

2.2 Niveles Anidados

La utilización de niveles anidados (un RAID construido en base a otros RAIDs) también es muy utilizada y ofrece otros equilibrios entre capacidad, velocidad y tolerancia a fallos. Por ejemplo, la configuración conocida como RAID 10 no es en sí misma un nuevo nivel de RAID, sino que se construye configurando un RAID 0 usando como base dos RAID 1, y suele utilizarse en aplicaciones que requieren mucha actividad de entrada salida y buena tolerancia a fallos.

2.3 Implementaciones de RAID

RAID puede implementarse tanto por software como por hardware. Las **implementaciones de RAID por software** permiten flexibilidad y brinda las ventajas de los distintos niveles, usualmente a un costo de rendimiento ya que las tareas de administración de los discos y cálculo de paridades deben llevarlas a cabo el sistema operativo, introduciendo al procesador como parte del camino crítico del sistema de almacenamiento.

En el caso de un **RAID implementado por hardware** se pierde algún grado de flexibilidad, pero se gana en rendimiento: el sistema operativo delega en la controladora RAID las tareas de administración y cálculo, y se expone al *host* la controladora como uno o varios discos virtuales. Además, las controladoras RAID pueden implementar cachés de escritura y circuitos específicos para el cálculo de las funciones de paridad, que permiten acercar el arreglo al desempeño máximo teórico. Sin embargo hay que destacar que en este caso se agrega la controlador como punto único

de falla: mientras que el RAID puede soportar la rotura de un disco, si se rompe la controladora se puede perder el acceso a los datos; por este motivo es que varias soluciones de RAID incluye controladoras de respaldo.

3. Recuperación de Información

En el capítulo 5 se abordaron los principales conceptos, fases y actividades del proceso de recuperación de información propuesto en este libro. Como se vió previamente, cada fase y actividad de PURI debe ser adaptada según cada caso, tanto la tecnología involucrada como las circunstancias particulares en las que se encuentra. En los siguientes párrafos se hará un breve repaso de los conceptos presentados para luego desarrollarlos adaptados al almacenamiento distribuido, y puntualmente su aplicación RAID.

En PURI, luego de la fase de **relevamiento**, donde se identifican los posibles objetos que pueden contener la evidencia digital, el proceso de recuperación de información, propiamente dicho, suele comenzar con el contacto con un dispositivo de almacenamiento sobre el cual se debe trabajar. El contacto inicial con el dispositivo de almacenamiento permite determinar el modo de realizar dicho proceso. Usualmente se toma el dispositivo físico de la escena, a esta fase se la denomina **recolección**. Acto seguido, se establece la cadena de custodia del mismo y luego, en un ambiente controlado, se realiza la **adquisición** del mismo. Dependiendo de las necesidades, restricciones y consideraciones particulares del caso, es posible omitir la recolección del dispositivo físico y realizar directamente una adquisición in situ.

La **adquisición** tiene por objeto obtener la **imagen forense**, entendida como una copia, a nivel de bit, de toda información del dispositivo de almacenamiento, de modo que, en el momento de analizarla desde el punto de vista lógico, o sea del software, no se diferencie del dispositivo original. El

caso de la adquisición in situ requiere especial atención ya que además de las imágenes de los discos, debe tomarse toda la información relevante para su reconstrucción, como se verá más adelante.

Es importante tener presente que la información se puede encontrar en varios niveles. Por ejemplo, no limitarse a la información que pueda tener un archivo, sino también al analizar el sistema de archivos se puede extraer información de los metadatos originales del mismo. Aquí se destaca la diferencia crucial entre simplemente copiar un archivo a realizar una imágen de disco[224]. Adicionalmente disponer de la imagen del dispositivo permite obtener archivos ocultos, archivos eliminados o partes de los mismos que hayan quedado de actividad anterior en el dispositivo de almacenamiento.

Además, el trabajo con una imagen forense permite que se valide que es copia idéntica del dispositivo original, por medio de funciones *hash*. Una vez validada la copia, se puede trabajar sobre la misma sin tener contacto con el original, lo que refuerza el principio forense de preservación de la evidencia.

Las fases siguientes, **preparación** y **extracción y análisis**, se componen de actividades con tareas en las que se trabaja con las imágenes adquiridas de los dispositivos, cuyo fin de encontrar evidencia. Estas tareas se orientan de acuerdo a los que interesa recuperar, generalmente utilizando herramientas que permiten automatizar parte del análisis en busca de formatos de archivos, patrones, texto o puntos de interés.

Para el caso particular de almacenamiento distribuido, mediante RAID, existen dos cuestiones de suma importancia para la integridad y coherencia de la información, que son el

[224] Capítulo 5 – PURI. Fase de Adquisición.

orden de los discos y la configuración del arreglo. Sin esta información, cualquier recolección o adquisición realizada podría resultar prácticamente inútil, y se deberá recurrir a técnicas de reconstrucción para lograr acceder a la información del arreglo de discos. Esto puede tomarse como un principio guía para toda actividad en las fases recolección y adquisición:

> *"Toda la información relevante que no se tome en la fase de recolección y adquisición, tendrá que ser deducida en las fases de preparación, extracción y análisis"*

El resultado de una mala recolección es que se contará en el laboratorio con una "pila de discos", de los cuales se podrán realizar imágenes forenses por separado, pero no se podrá acceder directamente al disco virtual que conforman esos discos. Y consecuentemente, el resultado de una mala adquisición es un conjunto de imágenes forenses que no conforman el disco virtual correspondiente. En ambos casos, deberá intentar reconstruirse el arreglo antes de proceder con las tareas clásicas de recuperación de información. Ésta tarea adicional de reconstrucción puede realizarse con herramientas automáticas, ser guiada en forma manual por el informático forense o resultar demasiado complicada para poder realizarse, en cuyo caso tanto la recolección como la adquisición realizadas no tendrán valor ni podrá llevarse a cabo la tarea de recuperación de la información.

3.1 Procedimientos recomendados

En cuanto a los procedimientos, debe considerarse si el equipo se encuentra prendido o apagado, y si corresponde hacer recolección o adquisición. Para todos los casos es importante respetar las recomendaciones básicas a seguir durante un procedimiento, ya sea judicial, privado, un allanamiento, u otro tipo. Es decir, se tiene que garantizar que el estado del equipo no va a ser alterado a través de una red interna o externa, asegurar que no hay procesos ejecutándose en el equipo que puedan alterar o eliminar la información de

interés. En general, se asume que la integridad y seguridad de las personas, los equipos y la información está garantizada y se puede trabajar en forma tranquila, ordenada y tomando las precauciones necesarias.

A continuación, se analizará el caso de la recolección y luego la adquisición, ya que las tareas se realizan en ese orden en una experiencia real, comenzando por las situaciones más favorables hasta las de mayor complejidad junto a complicaciones que puedan surgir.

Recolección

Cuando se ha identificado para la recolección un equipo que cuenta con un arreglo de discos RAID se recomienda:

1. En lo posible, recolectar el equipo completo para asegurarse que no faltará ninguno de los discos, la controladora RAID y/o el sistema operativo con la configuración adecuada para acceder al arreglo de discos.
    a. Debe quedar en claro para los responsables del procedimiento que lo que se busca es garantizar que en las fases de Preparación y Análisis se podrá acceder a la información contenida en lo recolectado. Si es necesario trasladar el equipo completo, deben buscarse los medios para realizarlo.
2. Si no es posible recolectar el equipo completo, se recomienda:
    a. Tomar fotografías o hacer un esquema de cómo están conectados los discos al hardware del equipo.
    b. Si se trata de un RAID por software, revisar la configuración del equipo para detectar: el sistema operativo base, la herramienta a través de la cual se implementa RAID, las particiones de los discos que componen el arreglo y si está compuesto por archivos funcionando como dispositivos virtuales.

c. Si se trata de un RAID por hardware, revisar la configuración de la controladora y tomar nota de la configuración del arreglo. La controladora también debe recolectarse junto con los discos. Usualmente recolectar la controladora también implica recolectar el motherboard o contar un motherboard similar en el laboratorio. En su defecto tomar nota del modelo del mother y/o controladora.
d. Si el equipo se encuentra apagado, debe asumirse que todos los discos conectados al equipo participan de un arreglo RAID.
e. Deben recolectarse todos los discos que participan de alguna forma en el arreglo RAID. Si es necesario etiquetar los discos conforme a las notas, esquemas o fotografías tomadas.
f. Buscar, tomar o copiar cualquier documentación o nota de donde se pueda obtener información de la configuración del arreglo de discos. Algunos datos importantes a tomar en cuenta: si es RAID por software o hardware, el nivel de RAID, cantidad de discos, tamaño de grupos de bloques (*chunks*), algoritmo de paridad, etc.

Adquisición

Una vez que se tiene el acceso al dispositivo RAID, ya sea en vivo sobre el equipo o luego de realizar recolección del mismo, se debe proceder con la adquisición de la imagen, para lo que se recomienda:

1. En lo posible, si el volumen RAID está montado, realizar una adquisición clásica como si se tratara de una un dispositivo único de gran tamaño.
   a. Si bien RAID permite combinar varios dispositivos físicos para obtener un dispositivo lógico de mayor tamaño, en la actualidad hay soluciones de almacenamiento que brindan gran capacidad de

almacenamiento y pueden almacenar el contenido de un arreglo RAID.

   b. Al realizar la imagen del volumen RAID como un único dispositivo, se eliminan los problemas relacionados con la complejidad de RAID para las fases de Preparación y Análisis.

2. Si el dispositivo no está montado sobre el equipo, debe intentarse montar el disco para accederlo como volumen virtual íntegro.
   a. Para ésta tarea es importante contar con toda la información relacionada con la configuración del arreglo, es decir, el orden de los discos en el arreglo, la configuración RAID específica y, si se trataba de un RAID por hardware, la placa controladora.
   b. Si se logra montar el volumen, se debe proceder con una adquisición simple del volumen virtual, como en el caso (1).
3. En caso de no poder montar el arreglo RAID como una unidad virtual, deben tomarse imágenes individuales de cada disco y proceder con un proceso de reconstrucción del arreglo RAID.
   a. La reconstrucción del arreglo puede realizarse con herramientas automáticas, teniendo en cuenta las ventajas y desventajas para seleccionar la herramienta adecuada.
   b. También es posible realizar la reconstrucción en forma manual, o con herramientas guiadas por el experto informático forense. Este proceso suele llevar más tiempo que una herramienta automática, pero permite resolver algunos casos que las herramientas existentes no pueden manejar.

Debe quedar claro que éstas recomendaciones son para facilitar el trabajo del informático forense y evitar las tareas de reconstrucción de RAID, que demandan tiempo y esfuerzo por parte del experto. El no seguir estas recomendaciones no

implica una pérdida de la información, pero sí establece demoras, por el trabajo adicional que debe realizarse, y puntos en los cuales el informático forense deberá explicar y justificar su trabajo a una profundidad mayor que si hubiera realizado el trabajo en forma adecuada.

3.2 Reconstrucción: último recurso

En una situación judicial es mucho más simple explicar que se realizó la adquisición de la imagen completa del disco virtual, como se podía acceder en el equipo prendido, que tener que explicar y justificar un proceso de reconstrucción de RAID, con las dificultades técnicas que implica, y explicando cómo se mantienen las garantías de no contaminación de la información. Si bien la reconstrucción es casi siempre posible, pero demanda mucho más trabajo, no sólo técnico sino también procedimental y de justificación de lo realizado, debe utilizarse como opción de último recurso en la fase de preparación cuando no se tomaron los recaudos en las fases de recolección y adquisición, o bien el arreglo se encuentre deteriorado o destruido previo a la intervención del perito o especialista forense.

Para graficar el problema de reconstrucción se plantea una situación hipotética para establecer las condiciones en las que se tiene que trabajar para intentar reconstruir el arreglo:

> *Una empresa informática sufrió una falla en uno de sus servidores, y el arreglo RAID 5 de N discos se corrompió. Por malas políticas del departamento TIC, no cuentan con información sobre la configuración del arreglo de discos. Para empeorar las cosas, un intento fallido de recuperación resultó en la re-escritura de los superbloques RAID, por lo tanto tampoco se pueden utilizar para recuperar la configuración original. Es decir, se cuenta con N discos de los cuales se desconoce el orden, tamaño de grupos de bloques (chunk) y algoritmo de distribución de la paridad, de los cuales es urgente recuperar información crítica para el negocio.*

Se eligió un inconveniente no judicial para mostrar que ésta técnica es aplicable a cualquier situación de recuperación de la información. Su aplicabilidad en entornos judiciales/forenses es igualmente válida, siempre y cuando se documente el proceso para garantizar la reproducibilidad y replicabilidad del procedimiento.

Hay que destacar que puede existir una situación intermedia, entre el caso ideal que sería obtener la imagen completa del arreglo y la peor situación de tener imágenes de un arreglo desordenadas y sin ningún tipo de información de reconstrucción. Una situación intermedia podría ser tener las imágenes completas de los discos de un arreglo, en esta situación la información para su reconstrucción se encuentra en los mismos discos y muy probablemente un software para la construcción de RAID puede re-armar el arreglo sin problemas obteniendo los datos dentro de las mismas imágenes de los discos. Obviamente, lo primero que se debe intentar con las imágenes de los discos es verificar si se encuentra en esta situación y de ser así recurrir a la reconstrucción automática por software.

El caso propuesto es la peor de las situaciones, en cuanto a que está borrada la configuración del RAID de cada disco y no se dispone de la información del arreglo, pero solo que se sabe que el arreglo tenía NTFS como sistema de archivos y que la MFT ocupa al menos una cantidad de *chunks* mayor a la cantidad de discos del arreglo.

Antes de desarrollar la técnica propuesta es necesario conocer más profundamente los conceptos involucrados. En particular se revisarán las distribuciones de paridad en RAID 5, necesarias para interpretar la secuencia de los datos leídos; particiones, MBR y GPT, necesarios para conocer el licado sobre el volumen; y luego se abordarán algunos detalles específicos de NTFS sobre los que se basa de la técnica propuesta. De todos modos, si bien se trabaja sobre un caso específico, es posible extrapolar, con ingenio, la técnica a

otras situaciones las cuales se plantean en el título final de este capítulo.

Distribuciones de paridad

Los metadatos de configuración de los discos que componen un arreglo RAID se almacenan en una estructura llamada superbloque RAID, o estructura DDF según la nomenclatura del SNIA[225]. Esta estructura guarda la información relevante para determinar a qué arreglo y unidad virtual pertenece cada disco, y los parámetros de configuración, como tamaños de los *chunks* (tramas o grupos de bloques en los que se fracciona la unidad), tamaño de banda (también llamadas *stripes*), caché, entre otros.

En los niveles 5 y 6, además, es necesario además especificar cómo se van a distribuir los *chunks* de paridad y datos entre las distintas bandas. Usualmente se aplican tres algoritmos estándar[226] denominados *Left Asymmetric*, *Left Symmetric* y *Right Asymmetric*. La diferencia entre las tres radica en el modo en el que se distribuye la paridad y el orden de los *chunks* de datos en cada banda. Para profundizar en cada una de ellas se trabajará sobre RAID 5, pero los mismos conceptos pueden trasladarse a RAID 6.

La distribución de paridad ***Left Asymmetric*** comienza con la paridad de la banda 0 (cero) en el disco *N* y se desplaza hacia la izquierda a medida que se avanza en las bandas (*stripes*) del modo en que se ilustra en la figura 8.5 para un RAID 5 con 4 discos. También es la misma distribución ilustrada en la figura 8.4 en 3 discos. Además, la secuencia de *chunks* se interpreta siempre de izquierda a

[225] TANENBAUM, Andrew S. “Structured Computer Organization”, páginas 89 a 93, 5ta edición, Pearson Prentice Hall, 2006.
[226] FAY-WOLFE. (2008). “RAID Rebuilding 101”. CSC-486 Network Forensics, University of Rhode Island. Disponible en http://media.uri.edu/cs/csc486_wmv/RaidRebuilding_TOC.pdf

derecha siguiendo el orden de los discos y saltando el disco que tiene la paridad de la banda.

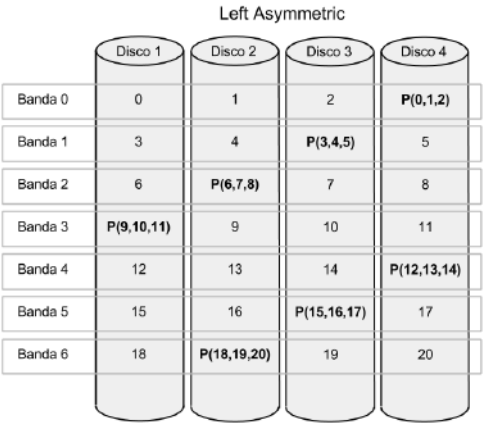


Figura 8.5: Distribución ***left asymetric*** de los *chunks* (grupos de bloques) en un RAID 5 compuesto por 4 discos.

En la distribución ***Left Symmetric***, mostrada en la figura 8.6, la paridad se ubica de igual modo que *Left Asymmetric,* La diferencia entre ambas radica en la distribución de los *chunks*, los cuales, para *left symmetric*, siempre son secuenciales respecto de los discos.

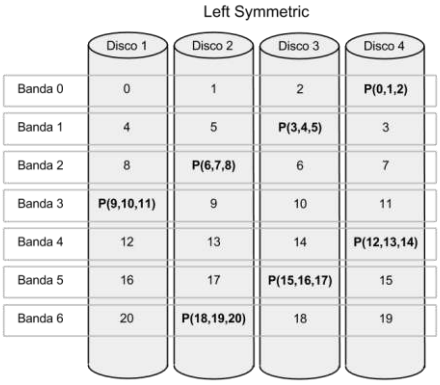


Figura 8.6: Distribución ***left symetric*** de los *chunks* (grupos de bloques) en un RAID 5 compuesto por 4 discos.

La distribución ***Right Asymmetric***, ilustrada en la figura 8.7, la paridad comienza en el primer disco y se desplaza a la derecha a medida que se avanza entre las bandas. Y la distribución de los *chunks* de datos es la misma que en *Left Asymmetric*.

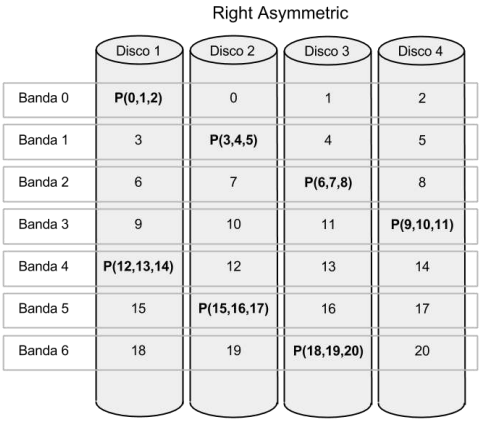


Figura 8.7: Distribución ***right asymetric*** de los *chunks* (grupos de bloques) en un RAID 5 compuesto por 4 discos.

Particiones, MBR y GPT

Los discos, tanto reales como virtuales, debe particionarse para formatear la partición con un sistema de archivos. Las particiones son exactamente eso, partes de un disco completo a las que se le asigna un sistema de archivos configurado con parámetros determinados. En la década de 1980 IBM definió el *Master Boot Record* (*MBR*) como un sector del disco en el cual guardar código del cargador de arranque (*bootloader*) e información de las particiones del disco, que permite definir 4 particiones, almacenar unos 400 bytes de código de arranque y manejar particiones de hasta 2 TiB de tamaño. Con el paso de los años se fueron haciendo extensiones y modificaciones a MBR, pero era claro que el estándar necesitaba un reemplazo.

GPT (*GUID Partition Table*), definido por Intel, reemplaza a MBR, permitiendo definir cientos de particiones, y al utilizar 64 bits para almacenar el tamaño, éstas pueden llegar a ocupar hasta 8 ZiB. Además, GPT está diseñado para ser compatible con MBR y facilitar la transición. Actualmente casi todos los sistemas informáticos modernos utilizan GPT para definir su tabla de particiones.

El concepto de particiones es importante para la reconstrucción de un RAID porque el enfoque de éste trabajo se concentra en particiones tipo NTFS. Si hay una partición NTFS presente en el arreglo RAID, es posible aplicar la técnica y deducir el orden de los discos para todo el arreglo.

Conceptos NTFS

Si bien *New Technology File System* (NTFS) fue visto en el capítulo 6 a continuación se hará un repaso para profundizar algunos aspectos a tener en cuenta en la técnica de reconstrucción propuesta. Se eligió NTFS ya que presenta características especiales que facilitan la técnica de reconstrucción de arreglos RAID planteada en este trabajo.

En NFTS todo el volumen se encuentra compuesto por bloques. El tamaño de dichos bloques es establecido al momento de la creación del sistema de archivos y siempre corresponderá a un múltiplo de dos por el tamaño del sector de disco. A su vez cada bloque puede contener información válida de un solo archivo.

Como se explicó previamente[227], una particularidad realmente distintiva de NTFS es que en él “todo es un archivo”. Toda información válida dentro del volumen se encuentra contenida en un archivo, incluso la misma tabla de archivos y el sector de arranque. Así, todos los metadatos y estructuras de administración del sistema de archivos están

[227] Capítulo 6 aspectos técnicos, Sistema de archivos NTFS

comprendidos en archivos del sistema. Probablemente el archivo de sistema más relevante es la *Master File Table* (tabla de archivos), identificada con el nombre $MFT. Esta tabla, por el hecho de encontrarse implementada como un archivo, presenta las mismas características que cualquiera de ellos. Por ejemplo, puede ubicarse en cualquier sector del volumen, crecer dinámicamente o incluso hallarse fragmentada.

La MFT cuenta con un registro por cada archivo o directorio contenido en el volumen al que pertenece. Esto no excluye a los archivos de sistema. De esta manera también existe un registro referente a la misma tabla, denominado $MFT, y un registro al archivo que contiene el sector de arranque del volumen denominado $Boot, entre otros. La MFT se implementa como una secuencia de registros de tamaño fijo (1024 bytes) que representan los metadatos de cada archivo o directorio en el sistema, lo que brinda la oportunidad de utilizarla como recurso en la reconstrucción de un arreglo de discos.

Cada registro se compone de un encabezado y una estructura dinámica de atributos opcionales. A su vez, cada atributo también se materializa mediante un encabezado y contenido dinámicos. Si la secuencia de atributos de un archivo no entra en un solo registro, se declaran “registros de extensión”, que almacenan los atributos restantes y referencian al registro original.

Para el método de reconstrucción de discos que se verá más adelante, lo que interesa de la MFT son los datos del encabezado de cada registro, y en particular el número de registro MFT. Este es un número entero de 4 bytes que crece secuencialmente con cada registro de la tabla.

Entorno de prueba

Para simular el problema propuesto, se puede trabajar en un sistema Debian Linux con la herramienta *mdadm*, que

permite realizar arreglos RAID por software. Saber cómo construir un arreglo ayuda a tener una idea clara de lo que se debe reconstruir. Es por ello que en este apartado se muestran los pasos a seguir para la construcción de una situación lo más cercana posible al problema. También es útil para realizar prácticas sobre un entorno de pruebas en el cual se puede experimentar libremente sin el riesgo de trabajar sobre una situación real.

El proceso de creación de un caso es prueba es el siguiente:

1. Se generan *N* archivos vacíos, de nombre aleatorio, que van a funcionar como discos virtuales. Cada archivo se monta como un disco a través de la interfaz de *loopback* de Linux.

   Como ejemplo, el siguiente comando genera 4 archivos con nombres aleatorios y los mapea como dispositivos loopback del /dev/loop0 al /dev/loop3

```
#for I in {0..3} ; do ARCHIVO=$(mktemp
'img.XXXXXX'); rm $ARCHIVO; dd if=/dev/zero
of=$ARCHIVO count=0 bs=1024k seek=1024; losetup
/dev/loop$I $ARCHIVO; done
```

2. Se crea el arreglo RAID 5 con *mdadm*, utilizando los *N* dispositivos loopback. El tamaño de chunk y algoritmo de distribución de paridad son datos aleatorios que no se almacenan. En la figura 8.8 se muestra como se forma el volumen virtual para 4 dispositivos.

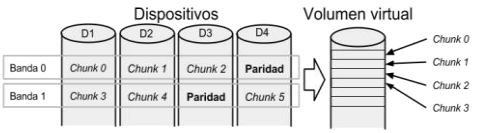


Figura 8.8: RAID 5 de 4 dispositivos (discos) con paridad *Left Asymmetric*.

Para crear el volumen tal como se ve en la figura se podría ejecutar el siguiente comando:

```
#mdadm -C /dev/md0 -l 5 -c 256 -p la -n 4 --assume-
clean /dev/loop{0..3}
```

Siguiendo el orden de las opciones del comando, lo que se está diciendo es que se cree un arreglo de discos en /dev/md0 de nivel 5 con un tamaño de *chunk* de 256 Kb y paridad *left asymetric* utilizando 4 discos que se asumen limpios tomados de /dev/loop0 a /dev/loop3 consecutivamente.

Sin embargo, para hacer más realista la prueba, en lugar de utilizar un tamaño de *chunk* de 256 Kb y paridad *left asymetric*, lo ideal sería desconocer estos datos tomando esos valores al azar. Para hacerlo así se pueden declarar 2 arreglos en la consola de comandos: uno con los posibles tamaños de *chunks* y otro con los posibles algoritmos de paridad; del siguiente modo:

```
#declare -a CHUNK=( 32 64 128 256 512)

#declare -a LAYOUTS=( ls ra la)
```

Una vez declarados los arreglos se utiliza un índice aleatorio que seleccione un elemento de cada arreglo en el momento de creación del RAID. Finalmente el comando quedaría de la siguiente manera:

```
#mdadm -C /dev/md0 -l 5 -c ${CHUNK[$RANDOM%5]} -p
${LAYOUTS[$RANDOM%3]}    -n    4    --assume-clean
/dev/loop{0..3}
```

3. Se crea en él una partición NTFS con un desplazamiento aleatorio del comienzo del disco (alineado a sector). Esto sirve para simular que la partición se encuentra en el medio del disco virtual

RAID, como si hubiera otras particiones presentes en el disco. Luego se monta el RAID para su uso.

Para realizar eso se puede ejecutar los siguientes comandos:

```
#losetup /dev/loop5 -o $(((RANDOM%10000+100)*512))
/dev/md0

#mkntfs -f /dev/loop5

#mount /dev/loop5 /mnt
```

En la figura 8.9 se ejemplifica cómo se vería si la MFT ocupase 6 *chunks* comenzando en la banda M-1 del dispositivo 3 y finalizando en el chunk de la banda M del dispositivo 4.

Figura 8.9: Ejemplo de distribución de la MFT en los dispositivos físicos y el virtual.

También se ejemplifica cómo se vería la misma MFT en el dispositivo virtual ocupando 5 *chunks* si existiera 1 *chunk* de paridad en los dispositivos físicos. Cabe destacar que para que el estudio sea posible la MFT debe ocupar una cantidad considerablemente mayor de *chunks*.

4. En la partición NTFS montada se crean 3 o 4 archivos de 1 MiB con contenido aleatorio. De estos archivos se calcula el *hash* MD5 para verificar luego que la reconstrucción ha sido exitosa.

```
#cd /mnt/
#dd if=/dev/urandom bs=1k count=1024 of=archivo1
#dd if=/dev/urandom bs=1k count=1024 of=archivo2
#dd if=/dev/urandom bs=1k count=1024 of=archivo3
#dd if=/dev/urandom bs=1k count=1024 of=archivo4
#md5SUM archivo*
```

Para guardar y verificar los *hashes* de los archivos se puede realizar lo siguiente:

```
#md5sum archivo* > SUMS
#md5sum -c SUMS
#cp SUMS /home/
```

5. Dentro de la unidad NTFS se debe crear considerable cantidad de archivos pequeños con contenido “hola”. Sin estos archivos se corre el riesgo de la MFT no sea lo suficientemente grande y no se pueda deducir la distribución de paridad. Estos archivos sirven para simular un uso normal del sistema de archivos.

   Una forma sencilla de realizarlo es nombrar a los archivos con 3 caracteres de “a” a “z” con todas sus combinaciones se logrará tener 17.536 archivos:

```
#for I in {a..z}{a..z}{a..z} ; do  echo “hola” > $I
; done
```

6. Se desmonta el volumen RAID y se desconecta de la interfaz *loopback*. Luego, se detiene el arreglo RAID con mdadm.

```
#cd ..
#umount /mnt/
#losetup -d /dev/loop5
#mdadm -S /dev/md0
```

7. Se eliminan los superbloques de cada disco con *mdadm*.

```
#mdadm --zero-superblock /dev/loop0
#mdadm --zero-superblock /dev/loop1
#mdadm --zero-superblock /dev/loop2
#mdadm --zero-superblock /dev/loop3
```

8. Finalmente se desconectan los archivos de la interfaz *loopback*.

```
#losetup -d /dev/loop{0..3}
```

En esta instancia, habiendo terminado esta serie de pasos, ya no se dispone de información de cómo está constituido el RAID. Solo se tienen los *N* archivos (4 en los ejemplos) con nombres aleatorios, como imágenes de discos, que conformaron un RAID 5 en el cual el File System utilizado fue NTFS. Si bien se dispone de los *check sums* de los archivos internos sólo a fines de poder verificar la reconstrucción, en un caso real bastaría con poder reconocer archivos bien formados.

Cabe destacar que, con esta serie de comandos propuestos para el armado del caso, es posible crear un *script* de *bash* para generar automáticamente nuevos casos de prueba con distinta cantidad de discos y configuraciones de forma fácil, para validar la técnica propuesta con múltiples pruebas.

Técnica propuesta de reconstrucción

Tal como se armó en el apartado anterior, en el punto de partida para esta la técnica propuesta de reconstrucción de RAID se tienen *N* archivos que representan los *N* dispositivos, denominados en las ilustraciones como D1, D2, D3 y D4. Si bien en los ejemplos se muestran en orden por claridad, este orden no es conocido a priori, y es justamente una de las incógnitas para descubrir.

A continuación, se describe el proceso de reensamblado:

Paso 1: Se buscan en todos los discos del arreglo las cabeceras NTFS y los registros FILE. En un sistema de archivos NTFS siempre se encuentran dos cabeceras, una al principio de la partición y otra al final. Debido a la redundancia de RAID 5 es posible que se encuentren copias de una o ambas cabeceras en el *chunk* de paridad de la banda correspondiente. Encontrar las cabeceras NTFS ayuda a establecer los posibles puntos de comienzo del sistema de archivos dentro del arreglo RAID.

Paso 2: De los registros FILE interesa el número de registro MFT, que ayuda a determinar el orden de los discos. Si un mismo conjunto de registros está presente en dos discos, ésto indica que uno de esos discos, para esa banda, contiene un *chunk* de paridad y los demás están vacíos.

Paso 3: Hay dos cuestiones para analizar con respecto al número de registro MFT:

En primer lugar, se debe analizar la longitud de los conjuntos de registros con numeración contigua por cada dispositivo. Por Ejemplo, si en el dispositivo D1 se encuentran los registros 3001, 3002, 3003, …, 4000, 7001, 7002, 7003, ... Puede apreciarse un salto en la secuencia del 4000 al 7001 y se puede deducir que el *chunk* tiene la capacidad de almacenar 1000 registros FILE de la MFT y así se determina su tamaño. La figura 8.10 muestra este concepto.

En segundo lugar, se deben ubicar los registros FILE de la MFT iniciales, y seguir la secuencia cuando salta de un disco a otro. De éste análisis se empieza a determinar el orden de los discos, aunque no alcanza para determinar cuál es el disco inicial.

El seguimiento de la secuencia de registros FILE de la MFT también permite detectar los *chunks* de paridad. En la figura 8.10 puede verse un arreglo RAID 5 con distribución *Left Asymmetric* de 4 dispositivos en orden, con los registros FILE de la MFT y la secuencia indicada con flechas. Puede apreciarse cómo la presencia de un *chunk* de paridad altera el orden común de salto de la secuencia de registros entre dispositivos, y cómo también indica la secuencia que siguen los dispositivos en el arreglo.

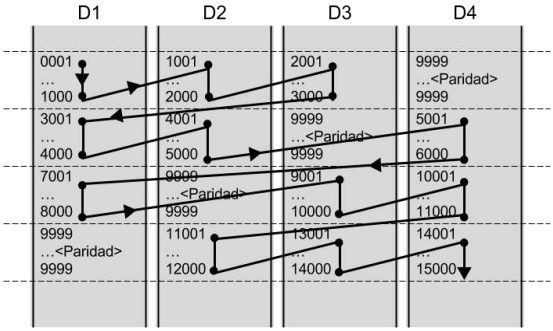


Figura 8.10: Distribución de los registros de la MFT en un arreglo RAID 5 *Left Asymmetric*. Por simplificación se representa con 1000 registros FILE de MFT por *chunk* del arreglo y se muestra el orden.

Para el caso de la distribución *Left Symmetric*, el salto de un disco a otro siempre es el mismo, pero el *chunk* de paridad introduce un salto a la siguiente banda del arreglo.

Nota: La técnica busca determinar el orden de los discos, o si eso no es posible, reducir la cantidad de combinaciones que deben intentarse para determinar el orden real. En el caso de la distribución *Left Symmetric* no se puede determinar el disco inicial, sin embargo, se logra reducir las

combinaciones posibles de *N*! a *N*. En el caso de las distribuciones *Left Asymmetric* y *Right Asymmetric*, si el tamaño de *chunk* es demasiado grande, puede no haber suficiente información para determinar el primer dispositivo del arreglo.

Paso 4: Las combinaciones posibles para reconstruir el arreglo se verifican utilizando *mdadm* en el modo en que ignora la información de los superbloques y monta el arreglo RAID con la configuración suministrada manualmente, siguiendo las deducciones previas.

Paso 5: Con el arreglo reconstruido, se monta la unidad en un directorio. Si se puede acceder a la misma, casi con seguridad se ha tenido éxito en la reconstrucción. Para verificar estrictamente el éxito de la técnica, se comparan los *hashes* MD5 de los archivos grandes con aquellos calculados previo al desarmado del arreglo RAID y la eliminación de los superbloques.

Esta técnica de reconstrucción entraría en la Fase de Preparación del modelo PURI. Por lo tanto, debe tomarse en cuenta en primera instancia en la actividad de “Preparación de extracción” disponer del espacio necesario para configurar el arreglo. Luego en marco de la actividad de “Identificación de tecnologías de la información en el objeto” reconocer que se encuentra frente a una serie de imágenes que componen una unidad RAID, verificar la presencia del NTFS. Finalmente, en la actividad de “Preparación del ambiente” entraría la instalación de las herramientas necesarias para aplicar la técnica y donde se realizaría la reconstrucción del arreglo propiamente dicho.

Cabe destacar que una vez finalizada la reconstrucción se obtiene acceso al dispositivo completo. Por lo tanto, en la fase de extracción y análisis se pueden realizar todas las actividades pertinentes para el caso de igual modo a que si se tratase de una imagen de disco común.

3.2 Extensión de la técnica aplicada en otras situaciones

Más allá de que durante el desarrollo de este capítulo se trabajó sobre el caso puntual de reconstruir un RAID 5 con NTFS, se podría generalizar que lo necesario para la reconstrucción es:

1. Reconocer el RAID y el nivel.
2. Averiguar el tamaño de los grupos de bloques o *chunk.*
3. Deducir el algoritmo de distribución de paridad, en caso de ser RAID 5 o 6.
4. Encontrar el orden de los discos.

Con esa información debería ser factible la recuperación de los datos dentro del arreglo. Debe recordarse que el objetivo de esta técnica es reducir el espacio de combinaciones posibles a intentar para la reconstrucción de un RAID, idealmente a una sola. Eventualmente es probable que esta técnica indique más de un posible orden de los discos, en cuyo caso deberá probarse las distintas alternativas hasta lograr montar satisfactoriamente una de las particiones del mismo. Cuando esto se logra, se puede decir con certeza que ese es el orden adecuado de los discos, ya que es prácticamente imposible que se construya un *filesystem* coherente con un orden incorrecto en los discos.

Por otra parte, cualquier información adicional que pueda obtenerse como pista, más allá del análisis de datos, también puede funcionar como punto de partida para realizar intentos de reconstrucción. Por ejemplo: si el RAID fue armado por hardware y se conoce la marca de la controladora, una prueba interesante sería tomar la configuración por defecto de la misma.

Reconocer el RAID y su nivel

Como se mencionó previamente, lo ideal sería reconocer el arreglo en la Fase de Recolección, y adquirir en ese momento toda la información posible. Si no se dispone de la misma, lo primero sería descartar la posibilidad de que las imágenes se corresponden a discos individuales. Asumiendo que ya se exploró esa posibilidad, lo siguiente sería agrupar las imágenes por tamaños (descomprimidas), ya que podrían tratarse de más de un arreglo. Tomando un grupo de imágenes del mismo tamaño, se podría suponer que corresponden a un arreglo (aunque podrían ser más), y asumiendo que no se puede reconocer el nivel por medio de herramientas, lo siguiente sería deducir el nivel. En cualquier caso los RAID 2, 3 y 4 quedarían prácticamente descartados debido a su escaso uso práctico. También se puede hacer un análisis rápido, para estimar el nivel basado en la cantidad de imágenes.

Por ejemplo:

- Si se dispone de 2 imágenes, necesariamente debe tratarse de un RAID 0 o 1.
- Si se encuentran 3 discos, podría ya pensarse que puede tratarse de un RAID 5, se descartan RAID 6 y RAID 10 ya que requiere al menos de 4 discos; otra posibilidad sería que sea un RAID 1 o 0 con discos de respaldo.
- Con 4 discos, lo más probable es que sea un RAID 10, o RAID 5; Ya quedarían prácticamente descartados los niveles 0 y 1: el nivel 0 si bien es posible sería extremadamente riesgoso ya que al no tener redundancia la pérdida de información queda subordinada a la rotura de uno de los discos, y por el contrario un RAID 1 con 4 discos sería un exceso redundancia. Sin embargo, con 4 discos, aunque poco probable, ya sería posible un RAID 6.

- Si se encuentran más de 4 discos, los niveles más probables serían RAID 5 o 6, o 10 con discos de respaldo. De aquí en más, cuanto mayor sea la cantidad de discos más reforzará la posibilidad del nivel 6, aunque sea más probable nivel 5.

Estas deducciones, basadas en los conceptos teóricos, constituyen sólo un análisis preliminar en la situación. El objetivo es rápidamente limitar las posibilidades, para luego con otras técnicas continuar descartando alternativas, o verificando hipótesis.

Lo más fácil de verificar en estos casos sería estar frente a un RAID 1, ya que al examinar fragmentos con el mismo desplazamiento y mismo tamaño, deberían coincidir los datos. Sin embargo, se deben tomar precauciones como, por ejemplo, si se tienen 3 discos, de los cuales en un fragmento 2 de ellos son idénticos y uno es cero, podría tratarse tanto de un RAID 1 con un disco de respaldo, como de un RAID 5 en el cual la paridad espeja el contenido. Esto último puede utilizarse como ventaja: si se tiene la sospecha de estar frente a un RAID 5, podría buscarse, en los sectores más altos, fragmentos en los cuales 2 discos tengan el mismo contenido y el resto estén en cero. Por otra parte, del mismo modo en que puede verificarse un RAID 1, También podrían verificarse un RAID 10, tomando los discos de a pares.

Averiguar el tamaño de los grupos de bloques o chunk

El tamaño de *chunk* se obtiene en base a los saltos en los indicadores de registros de la MFT. Extrapolando la idea, lo que se hace es detectar saltos cada cierta cantidad de bytes en una estructura conocida, secuencial y ordenada. Si en lugar de basarse en los registros de la MFT, se utiliza la estructura de un archivo conocido, es factible detectar discontinuidades en el mismo que permitan deducir el tamaño de *chunk* del arreglo.

Dado que un solo archivo podría no llegar a abarcar suficientes *chunks* como para indicar con suficiente grado de confiabilidad el tamaño de los mismos, puede llegar a ser necesario extender el análisis a varios archivos conocidos.

Deducir el algoritmo de distribución de paridad

Al analizar la distribución de paridad, ya se debería saber que se está trabajando sobre un RAID 5 o 6, o en alguna de sus variantes. Para el caso, del mismo modo que para averiguar el tamaño del *chunk*, para deducir el algoritmo de distribución de paridad, la técnica propuesta se basa en obtener la secuencia de los identificadores de archivos de NTFS. Por lo tanto, de no disponer de NTFS, se deberá acudir a algún dato que abarque varios discos y se pueda analizar la secuencia.

El análisis de la distribución de paridad y del orden de los discos se basa en el estudio estadístico de los saltos y discontinuidades en la estructura conocida que se eligió para guiar la reconstrucción. Por ejemplo, si la estructura salta del disco X al disco Y con mucha frecuencia, pero eventualmente del disco X al Z, este último caso está indicando que, para esa fila del arreglo, el disco Y contiene una banda de paridad.

Un caso especial son los algoritmos de distribución simétricos, en los cuales siempre se salta al mismo disco y sin bien esto determina con seguridad el orden de los mismos, no ayuda determinar cuál es el primero.

Encontrar el orden de los discos

El último paso sería encontrar el orden de los discos, en base a toda la información recauda anteriormente es posible que ya se puedan plantear propuestas o tener hipótesis de posibles secuencias. Un dato, no menor, además del orden es saber cuál es el primero de los discos. Esta tarea, podría realizarse a la vez que al deducir el algoritmo de distribución de paridad. Como se dijo previamente, de no tratarse de

NTFS, la búsqueda se debe basar en otro archivo o estructura conocida y al analizar los saltos a la vez que se detectan las paridades se puede obtener el orden de los discos.

Reconstrucción para otros niveles de RAID

A esta altura, ya se debería haber reducido sustancialmente el espacio muestral, es decir todas las combinaciones posibles de formación del arreglo. Idealmente, ese espacio muestral tendría tamaño 1; pero si no es así, y la cantidad es razonable, se debe recurrir a probar las posibles combinaciones, obviamente asegurándose de no modificar datos en el proceso o bien teniendo *backups* o *snapshots* de las imágenes.

En cuanto a la reconstrucción si el nivel es 1 sería el caso más favorable ya no requiere reconstrucción, bastaría con leer una de las imágenes, aunque no se monte la unidad si pueden aplicarse técnicas de carvin para la extracción de archivos. De tratarse de un RAID 0, habiendo deducido el desplazamiento y el tamaño del *chunk* y dada la naturaleza se podría recorrer la información alternándose entre los discos. De tratarse de una RAID 10, sería lo mismo que un RAID 0, habiendo deducido el par de discos espejados.

4. Conclusiones

El objetivo del informático forense es obtener evidencia digital, y es posible que se presente el caso de tener que buscar la misma en un entorno de almacenamiento distribuido como lo es RAID.

En este capítulo se propuso una técnica enmarcada en el modelo PURI para el caso específico de encontrarse con un equipo RAID. Lo más importante a tener en cuenta, es que lo que no se tome en las fases de recolección y adquisición, deberá ser deducido en las fases de preparación, extracción y análisis con todo lo que ello implica: mayor tiempo de análisis y menores probabilidades de éxito.

La situación más favorable, en este caso, sería poder recolectar el equipo completo, o en su defecto adquirir el volumen RAID íntegro en una única imagen. De no ser posible, adquirir imágenes individuales de los dispositivos que componen el RAID con la información adicional necesaria para la reconstrucción del volumen a partir de las mismas.

Si las imágenes de los dispositivos contienen la información de los superbloques RAID intacta, y no se dispone de información adicional, es posible la reconstrucción por medio de herramientas automáticas. Si por algún motivo esa información está dañada o no es reconocible por las herramientas automáticas, se debe realizar una reconstrucción manual, la cual requiere mucho más tiempo de análisis y depende tanto del contenido y cantidad de información del volumen como de la experiencia en el tema del analista; existiendo la posibilidad que el volumen RAID no pueda ser reconstruido para extraer la evidencia digital. Llegado este punto solo queda intentar reconstruir el arreglo con la poca información disponible.

La técnica propuesta permite reconstruir un arreglo RAID 5 contando con *N* imágenes, una por cada dispositivo del arreglo, en condiciones en las que no se conoce el orden de las mismas, el tamaño de *chunk*, ni el algoritmo de distribución de paridad. Si bien la técnica se apoya en las estructuras del sistema de archivos NTFS, es posible extenderla para su uso en otros sistemas de archivos.

Esta técnica debería utilizarse como último recurso, ya que si se procediera con las tareas de recolección y adquisición de los discos de forma ordenada y metódica no sería necesaria.

Si el arreglo es RAID 6, o si utiliza un algoritmo de distribución de paridad no estándar, la técnica tal como se expuso presenta algunas dificultades. Con un estudio detallado de RAID 6 y de los algoritmos de distribución de

paridad propietarios, la técnica puede adaptarse para funcionar en estas situaciones.

Finalmente cabe destacar que, una vez reconstruido el arreglo RAID, este es equivalente a un dispositivo de almacenamiento estándar, y por lo tanto es válido aplicar todas las demás técnicas aplicables sobre medios persistentes para obtener la información según corresponda al caso.

Capítulo 9. Análisis Forense de Memoria Principal

Autores: Juan Ignacio Alberdi, Gonzalo Matías Ruiz De Angeli.

1. Introducción.
2. Pericias y Análisis Forense de Memoria.
3. Captura del volcado de memoria.
4. Análisis de Memoria Principal en Windows. 4.1 Estructuras de memoria en Windows. 4.2 Almacenamiento de las estructuras de memoria en Windows. 4.3 Estructuras ocultas y malware en Windows.
5. Conclusiones.

1. Introducción

En los últimos años, el Análisis Forense de Memoria se ha convertido en una de las áreas de mayor interés y grandes logros en la Informática Forense. Esta rama de la disciplina tiene la capacidad de resolver situaciones complejas y brindar datos que las técnicas explicadas en los capítulos anteriores no pueden.

Se comienza el capítulo con un resumen de alto nivel de lo que permite el análisis de memoria para las pericias informáticas y su utilidad judicial.

Luego se continúa con la adquisición del volcado de memoria (también llamado *memory dump*, o *dump*), actividad de vital importancia por la volatilidad de los datos presentes en memoria, que incluso pueden cambiar durante el proceso de captura, o perderse información si se realizan otras actividades previamente. Por esta razón, la adquisición de memoria debe ser una de las tareas prioritarias al momento de realizar actuaciones en una escena.

Finalmente, se presenta un vistazo de las estructuras que se pueden encontrar en memoria, primero con una discusión general, y posteriomente, con ejemplos particulares de las estructuras de Windows 7.

El objetivo de este capítulo es quitar el velo a la memoria, y mostrar las estructuras y los datos de gran valor investigativo que se esconden en ella. En la medida que se aproveche esta fuente de información única, los peritos informáticos podrán hacer un mejor análisis en las situaciones complejas que requieren de esta disciplina.

Nota: En varias ocasiones durante el capítulo se mencionará BIP-M, un *framework* de análisis de memoria moderno desarrollado por los autores. BIP-M es una alternativa a otras herramientas de análisis de memoria (como Rekall y Volatility), que comenzó su desarrollo en un momento

donde no había certezas sobre el futuro de las herramientas de análisis de memoria. Actualmente cuenta con soporte para analizar volcados de memoria de Windows 7 en formato Crash Dump, y se está trabajando en ampliar sus capacidades.

2. Pericias y Análisis Forense de Memoria

El Análisis Forense de Memoria consiste en la adquisición y análisis de datos provenientes de la memoria principal de un sistema de computación (usualmente denominada “memoria RAM”) con el fin de obtener información relevante sobre el mismo. Usualmente se realiza sobre un volcado de memoria, que es una copia de los contenidos de la RAM al momento de realizar la adquisición, pero también algunas herramientas permiten trabajar sobre un sistema “en vivo”.

En el ámbito forense es preferible trabajar con volcados, porque así se realiza una intrusión mínima sobre el sistema, y además se garantiza la posibilidad de reproducir el análisis y obtener los mismos resultados.

Es fundamental conocer la/s herramienta/s seleccionada/s para realizar el volcado de memoria, ya que afectará al mismo: si se trata de una herramienta de *hardware*, tendrá algunas condiciones en las cuales funciona y un puerto al que debe conectarse (que la computadora objeto del análisis debe tener disponible), y si se trata de un *software*, el mismo se cargará en memoria.

Una vez obtenida la memoria para el análisis, es necesario conocer las estructuras que almacenan la información de interés: procesos, *threads*, módulos, conexiones, *sockets*, *drivers*, entradas de registro, entre otras, son estructuras propias de cada Sistema Operativo, y que además varían de acuerdo a las versiones y arquitecturas de procesador. El conocimiento de estas estructuras es

fundamental para obtener la información que se almacena en ellas, y que posiblemente sólo esté disponible en memoria.

Un aspecto fundamental que debe considerarse es que, al utilizar memoria virtual, todas las direcciones de memoria y punteros en ella son direcciones virtuales[228], y por lo tanto es necesario traducirlas a direcciones físicas (y posiblemente a direcciones en el archivo de volcado, dependiendo del formato del mismo).

En la figura 9.1, se muestra el esquema de un procedimiento punta a punta del **Análisis Forense de Memoria**.

Figura 9.1: Procedimiento punta a punta de análisis forense de memoria principal.

En el proceso pueden reconocerse las tareas del analista forense, encuadradas en gris claro, y en los recuadros gris oscuro las tareas que se realizan apoyados por herramientas de análisis de memoria.

[228] Dirección virtual equivale a dirección lineal. Véase Capítulo 6. Aspectos Técnicos: 4.6 Ejemplo práctico: Gestión de memoria principal en Windows.

El reconocimiento de estructuras consiste en identificar los distintos artefactos que pueden encontrarse dentro de la memoria explorando el *volcado de memoria* que se capturó en la etapa inicial. El paso siguiente relaciona entre sí los distintos artefactos identificados, por ejemplo, las conexiones TCP con el proceso que las abrió, y así permite establecer vínculos entre los datos recolectados que pueden brindar información útil para el analista forense. El análisis automático se realiza a partir de los datos identificados previamente, en base a reglas y condiciones predefinidas.

En base a la información que los motores de análisis de memoria pueden recuperar de manera automatizada, queda en el analista forense realizar un análisis más profundo y dar significado a la misma en el contexto del caso investigado.

Conociendo las particularidades y generalidades del análisis forense en memoria principal, resulta necesario entender en qué situaciones puede llegar a ser de mayor utilidad o no, la búsqueda de uno u otro artefacto en memoria y sus relaciones.

La búsqueda de procesos puede parecer el eje del análisis forense en memoria, pero también existen otros artefactos en memoria que pueden llegar a contener información de gran utilidad para una investigación. El análisis de la memoria principal puede ayudar a inferir el uso que se ha dado al equipo, o detectar indicios que soporten una hipótesis particular.

También puede permitir la eventual detección de un *malware* que haya tomado control del equipo, y sea el responsable de las actividades que se han llevado adelante desde esa computadora en particular. Este caso es de suma importancia, porque se podría estar investigando a una persona inocente y el verdadero culpable esconderse detrás de ella. Para estas situaciones es vital el análisis de memoria, ya que los indicios que los *malwares* dejan en otras fuentes de evidencia digital pueden ser muy difíciles de identificar.

De la memoria también pueden extraerse contraseñas y claves de cifrado que estuvieran alojadas en ella, lo que puede permitir el acceso a cuentas de usuario o información encriptada en otras imágenes forenses del caso.

A continuación, se realiza un listado de motivaciones para realizar análisis forense de la memoria principal y qué elementos serían objeto de análisis en cada caso:

- Búsqueda de información sobre el comportamiento del usuario: registro de eventos, artefactos del sistema de archivos cargados en memoria, logs, entradas de registro, conexiones y sockets, fragmentos de datos legibles.
- Búsqueda de *Malware*: procesos ocultos, librerías, conexiones, contenido cifrado, entradas de registro.

Es importante conocer los procesos críticos del sistema operativo objeto de estudio, a fin de poder identificar procesos sospechosos partiendo desde lo más básico, como puede ser la similitud en nombres de procesos con procesos de sistema. También se debe conocer el tamaño de los archivos de sistema para detectar situaciones en que coincide el nombre del proceso, pero difiere en su tamaño, siendo estos grandes candidatos a ser analizados ya que pudieron haber sido modificados.

A su vez, es fundamental tener conocimiento de otros programas de uso común como son editores de texto, herramientas de ofimática, navegadores, compresores, antivirus, entre otros, que pueden existir en equipos a fin de poner foco en procesos que resulten inusuales y sean objeto de análisis.

Basado en la búsqueda de procesos, a partir de ellos es posible descubrir muchos datos que pueden llevarnos a relacionar el mismo con actividad de interés para la investigación.

- Búsqueda del contexto de seguridad de cada proceso: puede identificarse el contexto de seguridad obtenido,

es decir, el nivel de privilegios con el cual se ejecuta el proceso (en Windows, la estructura _TOKEN), su proceso padre, y otros elementos mencionados previamente que permitan realizar un análisis y establecer conclusiones sobre la eventual presencia de *malware*.

- Búsqueda de información que no se encuentra en el disco y que se sospecha se quiso ocultar: búsqueda de contenido cifrado, búsqueda de contenido "legible" (se pueden encontrar fragmentos de texto de un archivo, un documento o un correo electrónico que ha sido leído o escrito), búsqueda de archivos.
- Búsqueda de información de conexiones y sockets: dentro de los datos de conexiones ya sean TCP, UDP o sockets, es posible vincular las mismas con los Process ID y así llegar hasta el proceso en sí mismo, pudiendo verificar si este resulta sospechoso. Esto permite relacionar procesos que resulten sospechosos con direcciones IP remotas, y eventualmente extender la investigación.
- Búsqueda de información que indique la utilización de algún dispositivo periférico en el equipo, como podrían ser *drivers* cargados en memoria.
- Búsqueda de software específico: procesos, entradas de registro, módulos.

El análisis de la memoria no se circunscribe a estas estructuras y las relaciones entre ellas, también es importante incorporar al análisis la búsqueda de datos que puedan ser relevantes y no forman parte de ninguna estructura en particular. Por ejemplo, en la figura 9.2 se puede observar parte del contenido de una página web que fue abierta en el equipo desde donde se extrajo el volcado de memoria:

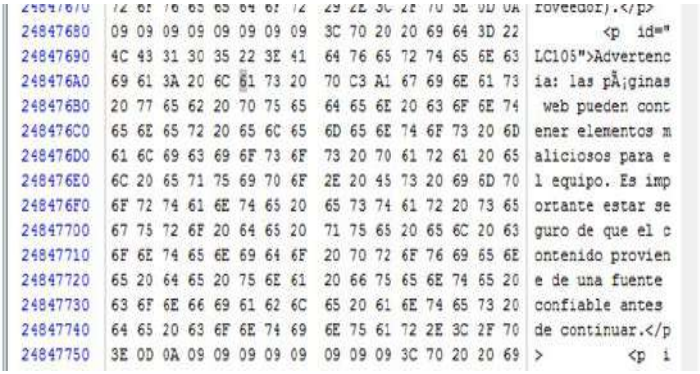


Figura 9.2: Contenido del volcado de memoria en una ubicación en particular visto con un editor hexadecimal.

Cualquiera sea la pericia a realizar, se deben considerar todos los aspectos detallados anteriormente en este capítulo. Los datos contenidos en un volcado de memoria se almacenan de diferente manera y pueden formar parte o no de distintas estructuras. Dichos datos pueden representar punteros a diferentes ubicaciones de la memoria, fechas, valores enteros o cadenas de texto. Es posible que estén almacenados en sistema *little-endian* o *big-endian*[229].

Por todo esto es necesario saber cómo interpretarlos y qué herramientas utilizar como soporte de análisis. El siguiente ejemplo, muestra cómo se vería el contenido con un editor de texto tradicional y los datos que brinda un editor hexadecimal[230]. Luego, cómo es posible realizar

[229] El término inglés *endianness* designa el formato en el que se almacenan los datos de más de un byte en un ordenador. Usando este criterio el sistema *big-endian* adoptado por Motorola entre otros, consiste en representar los bytes en el orden "natural": así el valor hexadecimal 0x4A3B2C1D se codificaría en memoria en la secuencia {4A, 3B, 2C, 1D}. En el sistema *little-endian* adoptado por Intel, entre otros, el mismo valor se codificaría como {1D, 2C, 3B, 4A}.

[230] Un editor hexadecimal, permite ver el contenido de un archivo tal cual es. Por el contrario, un editor de texto convencional, interpreta el contenido y lo representa como caracteres

interpretaciones y traducciones de esos datos en formatos legibles para el analista forense, gracias al uso de herramientas de soporte para el análisis.

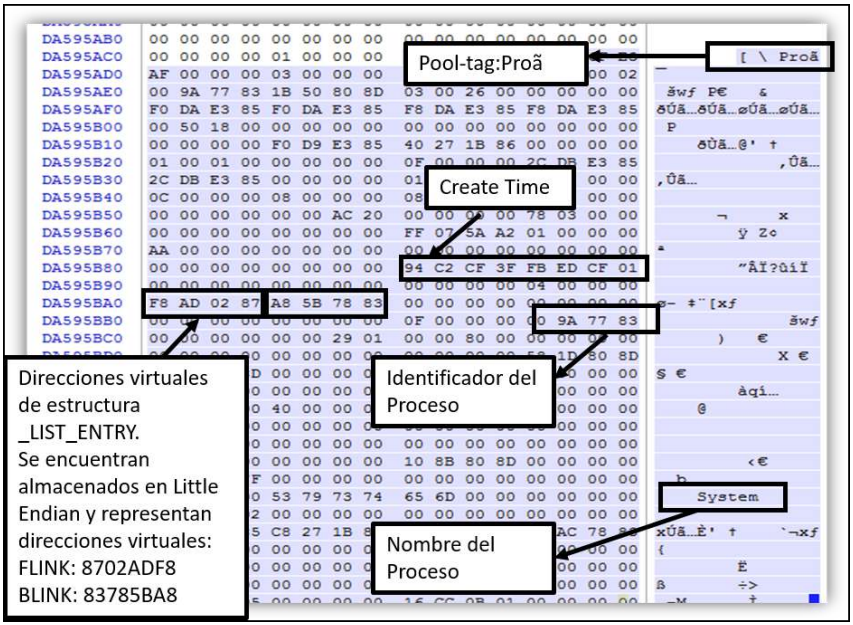


Figura 9.3: Contenido del volcado de memoria en la ubicación donde se encuentra el proceso *System*, visto con un editor hexadecimal.

Las herramientas de análisis de memoria permiten avanzar un nivel más en la interpretación y traducción de los datos en el volcado de memoria. En la figura 9.4 se muestra la salida generada por BIP-M *framework* de análisis forense cuando se le solicita la búsqueda de procesos activos en memoria. Se puede ver cómo el reporte resulta más legible, mejorando las condiciones de análisis de manera significativa:

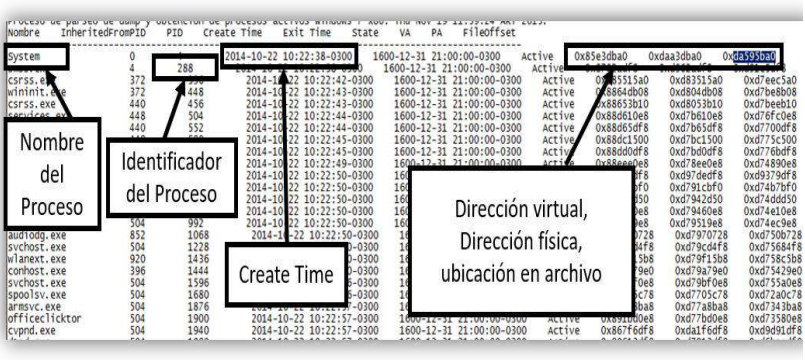


Figura 9.4: Salida de BIP-M *framework* para la búsqueda de procesos activos en un volcado de memoria.

3. Captura del volcado de memoria

La adquisición del volcado de memoria es una tarea prioritaria en las actividades a realizar *in situ*, debido a la volatilidad de los datos, y porque otras actividades a realizar en la escena (ya sean tareas de adquisición o *triage*) pueden afectar la información presente en memoria.

Si se utiliza un *software* de captura de memoria, es importante tener en cuenta:

- Cuáles son los procesos propios de la herramienta.
- El espacio que ocupan los mismos al momento de ejecución.
- El tipo de volcado que genera la herramienta: formato e información que vuelca desde la memoria al archivo (*Crash Dump*, *Raw Dump*, posibilidad de volcar el contenido del *page file*, etc).

En principio, *Raw Dump* es el volcado de memoria completo que posee directamente todo el contenido de la memoria al momento de generarlo. *Crash Dump,* sin embargo, es el volcado generado por Windows, el cual posee algunas

particularidades. La primera, es que al inicio del archivo genera un encabezado con datos que pueden ser útiles para el análisis o para la traducción de direcciones virtuales a físicas, como, por ejemplo, *DirectoryTableBase* que es la dirección física de la base de la primera tabla involucrada en la traducción de direcciones. También, *PsActiveProcessHead* que es la dirección virtual del nodo que apunta al primer proceso de la lista doblemente enlazada de procesos activos que implementa el Sistema Operativo.

La estructura de un encabezado *Crash Dump* es la siguiente:

```
Windows x86
_DMP_HEADER Tamaño total del 4096 bytes (4KB)
0x0  Signature    ['array', 4, ['unsigned char']]
0x4  ValidDump   ['array', 4, ['unsigned char']]
0x8  MajorVersion    ['unsigned long']
0xc  MinorVersion     ['unsigned long']
0x10 DirectoryTableBase   ['unsigned long']
0x14 PfnDataBase          ['unsigned long']
0x18 PsLoadedModuleList     ['unsigned long']
0x1c PsActiveProcessHead    ['unsigned long']
0x20 MachineImageType       ['unsigned long']
0x24 NumberProcessors       ['unsigned long']
0x28 BugCheckCode           ['unsigned long']
0x2c BugCheckCodeParameter ['array', 4, ['unsigned
long']]
0x3c VersionUser  ['array', 32, ['unsigned char']]
0x5c PaeEnabled               ['unsigned char']
0x5d KdSecondaryVersion       ['unsigned char']
0x5e VersionUser2     ['array', 2, ['unsigned char']]
0x60 KdDebuggerDataBlock       ['unsigned long']
0x64 PhysicalMemoryBlockBuffer
['_PHYSICAL_MEMORY_DESCRIPTOR']
0x320  ContextRecord  ['array', 1200, ['unsigned char']]
0x7d0  Exception              ['_EXCEPTION_RECORD32']
0x820  Comment        ['array', 128, ['unsigned char']]
0xf88  DumpType                 ['unsigned long']
0xf8c  MiniDumpFields           ['unsigned long']
0xf90  SecondaryDataState       ['unsigned long']
0xf94  ProductType              ['unsigned long']
0xf98  SuiteMask                ['unsigned long']
0xf9c  WriterStatus             ['unsigned long']
0xfa0  RequiredDumpSpace        ['unsigned long long']
0xfb8  SystemUpTime             ['unsigned long long']
0xfc0  SystemTime      ['unsigned long long']
0xfc8  reserved3       ['array', 56, ['unsigned char']]
```

Windows x64

```
_DMP_HEADER64 tamaño total de 8192 bytes 8 (KB)
0x0    Signature        ['array', 4, ['unsigned char']]
0x4    ValidDump        ['array', 4, ['unsigned char']]
0x8    MajorVersion     ['unsigned long']
0xc    MinorVersion         ['unsigned long']
0x10   DirectoryTableBase   ['unsigned long long']
0x18   PfnDataBase          ['unsigned long long']
0x20   PsLoadedModuleList   ['unsigned long long']
0x28   PsActiveProcessHead  ['unsigned long long']
0x30   MachineImageType            ['unsigned long']
0x34   NumberProcessors       ['unsigned long']
0x38   BugCheckCode           ['unsigned long']
0x40   BugCheckCodeParameter  ['array', 4, ['unsigned
long long']]
0x80   KdDebuggerDataBlock      ['unsigned long long']
0x88   PhysicalMemoryBlockBuffer
['_PHYSICAL_MEMORY_DESCRIPTOR']
0x348  ContextRecord     ['array', 3000, ['unsigned
char']]
0xf00  Exception             ['_EXCEPTION_RECORD64']
0xf98  DumpType              ['unsigned long']
0xfa0  RequiredDumpSpace     ['unsigned long long']
0xfa8  SystemTime            ['unsigned long long']
0xfb0  Comment         ['array', 128, ['unsigned char']]
0x1030 SystemUpTime        ['unsigned long long']
0x1038 MiniDumpFields              ['unsigned long']
0x103c SecondaryDataState          ['unsigned long']
0x1040 ProductType                 ['unsigned long']
0x1044 SuiteMask                   ['unsigned long']
0x1048 WriterStatus                ['unsigned long']
0x104c Unused1                     ['unsigned char']
0x104d KdSecondaryVersion          ['unsigned char']
0x104e Unused          ['array', 2, ['unsigned char']]
0x1050 _reserved0     ['array', 4016, ['unsigned char']]
```

Por otro lado, a diferencia de *Raw Dump*, el formato *Crash Dump* no vuelca la primera página reservada para BIOS y algunas páginas reservadas para dispositivos. La figura 9.5 muestra éstas diferencias.

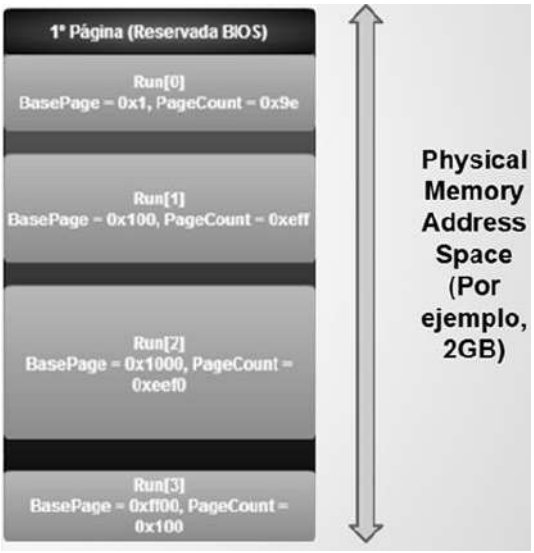


Figura 9.5: Sólo las regiones en recuadros claros se vuelcan en un archivo *Crash Dump*.

Cada porción de la memoria volcada en un *Crash Dump* posee el nombre de *Run*, y representa el contenido de una porción de la memoria en el momento de la realización del volcado, por lo que tienen asociadas una dirección física origen y una cantidad de páginas con las que se puede obtener la dirección final de la porción de memoria que representan. Es sumamente importante tener en cuenta esta característica para poder ubicar una dirección física en el desplazamiento correspondiente en el archivo. El hecho de que haya regiones de la memoria que no son volcadas, sumado a que existe un encabezado que varía su tamaño según la arquitectura, implica realizar los cálculos correspondientes para poder obtener la correspondencia entre una dirección física y la ubicación en el archivo.

Por otro lado, es importante tener presente al momento de tomar un *Crash Dump*, que este puede realizarse de acuerdo a 3 diferentes tipos: volcado de memoria completo, volcado del espacio de memoria del *kernel* o *mini dump*. El tipo de volcado debe ser configurado previamente a su toma. Esto se debe a que originalmente, el formato *Crash Dump* fue destinado para *debugging* y no para forensia. Este es un aspecto que agrega cierta desventaja al momento de optar por este formato, dado que requiere generar actividad en el equipo a analizar para verificar el tipo de volcado configurado y, de corresponder, realizar los cambios en la configuración, previo a la generación del volcado del mismo. Esto no es deseable, dado que es importante realizar la menor actividad posible en el equipo y a generar el volcado de memoria con la mayor celeridad posible, por el carácter altamente volátil de los datos en memoria. Una opción para evitar esto, es generar un *Raw Dump* con herramientas como *FTKImager*, con las que se puede realizar el volcado ejecutando dicha herramienta sin necesidad de mayor configuración previa, evitando mayor actividad en el equipo y ganando tiempo para la generación temprana del volcado de memoria.

4. Análisis de memoria principal en Windows

Los artefactos que se pueden encontrar en memoria principal son variados y, por consecuencia, también las estructuras que los representan (ver Windows Internals 5 y 6). En memoria es posible encontrar, entre otras cosas:

- Procesos: activos, terminados y ocultos
- Hilos (*Threads*)
- Módulos y DLLs
- Archivos abiertos por un proceso
- Conexiones
- *Sockets*

- Entradas de registro
- Información sobre cuentas de usuario y privilegios de acceso asociados a un proceso (*Tokens*)
- Contenido cifrado, por ejemplo, con *TrueCrypt* o *Bitlocker*
- Controladores (*Drivers*)
- Listado de usuarios conectados al equipo, local o remotamente.
- Claves asociadas a cuentas de usuario

Cada uno de estos artefactos está representado por una o varias estructura, que poseen un determinado formato, el cual puede diferir de un sistema operativo a otro y de acuerdo a la arquitectura (x86 o x64). El conocimiento y estudio de estas estructuras es el punto de partida para llevar adelante un análisis forense de los objetos que se encuentran en la memoria principal. Antes de avanzar en un análisis de estas características, es importante conocer cada uno de estos artefactos y cómo se relacionan entre sí para lograr obtener información coherente a partir de los datos identificados.

Muchas de las estructuras que se almacenan en memoria forman parte de una o más listas, y siguiendo los punteros presentes en ellas se pueden recorrer las listas, por ejemplo, para obtener del volcado de memoria el listado de procesos activos (similar a la instrucción top de Linux, o *tasklist* de Windows).

4.1 Estructuras de memoria en Windows

I. Procesos

Para profundizar en el mundo de las estructuras de memoria, se analizará la estructura _EPROCESS, presente en sistemas operativos Microsoft Windows y que representa a los procesos. En particular, se detallará a continuación la estructura para Windows 7 x64.

Como se muestra en la figura 9.6, es posible utilizar la herramienta *Windbg* para conocer la implementación de cada estructura documentada por Microsoft e identificar cuáles son sus atributos.

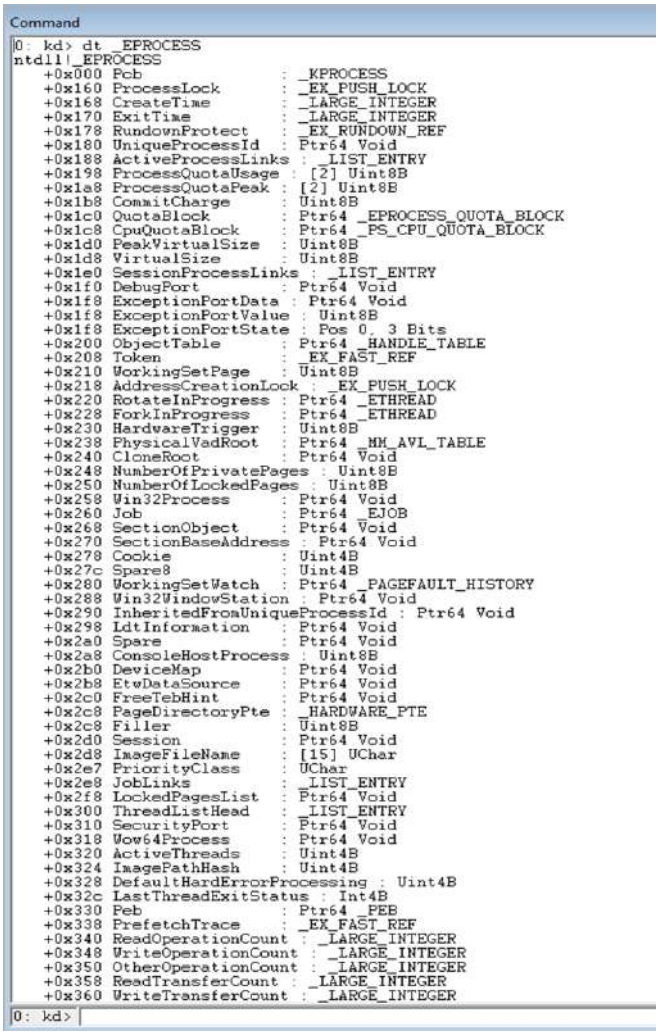


Figura 9.6: Detalle de estructura _EPROCESS de Windows 7 x64 obtenida con la herramienta Windbg.

La estructura _EPROCESS posee una importante cantidad de atributos, algunos más de los que se pueden ver en la figura anterior. Un listado reducido de algunos atributos relevantes de dicha estructura en Windows 7 x86 y x64 puede ser:

_EPROCESS

Windows 7

x86	x64		
0x000	0x000	Pcb	_KPROCESS
0x098	0x160	ProcessLock	_EX_PUSH_LOCK
0x0a0	0x168	CreateTime	_LARGE_INTEGER
0x0a8	0x170	ExitTime	_LARGE_INTEGER
0x0b0	0x178	RundownProtect	_EX_RUNDOWN_REF
0x0b4	0x180	UniqueProcessId	Ptr32Void
0x0b8	0x188	ActiveProcessLinks	_LIST_ENTRY
0x140	0x290	InheritedFromUniqueProcessId	Ptr*Void
0x16c	0x2e0	ImageFileName	[15]UChar
0x188	0x308	ThreadListHead	_LIST_ENTRY
0x198	-----	ActiveThreads	Uint4B
0x1a8	0x338	Peb	Ptr*_PEB

Nótese que el campo `ActiveThreads` no se encuentra presente en la arquitectura x64. Los punteros indicados como `Ptr*` son `Ptr32` o `Ptr64` dependiendo la arquitectura.

A su vez, se hace hincapié en algunos de ellos, ya que pueden tener mayor relevancia para el alcance que se pretende llegar:

- PCB (*Process Control Block*): este atributo es representado por una estructura que se encuentra embebida dentro del _EPROCESS. Dicha estructura

es la denominada _KPROCESS y posee atributos con datos de suma importancia, como por ejemplo, el puntero al PEB (*Procesos Environment Block*) o el puntero a la cabecera de la lista de hilos (*threads*) del proceso:

_KPROCESS

Windows 7

x86	**x64**		
0x000	0x000	Header	_DISPATCHER_HEADER
0x010	0x018	ProfileListHead	_LIST_ENTRY
0x018	0x028	DirectoryTableBase	ULONG*
0x02C	0x030	ThreadListHead	_LIST_ENTRY
0x078	0x0E0	ProcessListEntry	_LIST_ENTRY
0x088	0x0F8	KernelTime	ULONG32
0x08C	0x0FC	UserTime	ULONG32
0x094	0x15C	_PADDING0_[0x4]	UINT8

* ULONG32 o ULONG64 dependiendo la arquitectura

- *CretateTime* y *ExitTime*, son *timestamps* de creación y terminación del proceso.

Ambos atributos son de tipo UNION _LARGE_INTEGER, una estructura que representa un entero de 64 bits, pero que puede estar almacenada de dos maneras diferentes dependiendo de la arquitectura:

union LARGE_INTEGER	
0x000 LowPart	Uint4B
0x004 HighPart	int4B

union LARGE_INTEGER	
0x000 QuadPart	Uint8B

De esta manera, el entero de 64 bits, puede estar almacenado en dos partes (*LowPart* y *HighPart*) o en un solo atributo (*QuadPart*). Es importante tener en cuenta esto para la correcta interpretación del dato de acuerdo a la *endianness* del sistema.

En ambos casos el dato almacenado consiste en fechas del tipo *WindowsFileTime*[3], es decir, la cantidad de intervalos de 100 nanosegundos transcurridos desde el 1 de enero de 1601. De esta forma, se puede interpretar el dato almacenado y representar la fecha en un formato legible.

- U*niqueProcessID* e *InheritedFromUniqueProcessId* son los identificadores del proceso y de su proceso padre.
- A*ctiveProcessLinks* es el puntero a la cabecera de la lista de procesos activos.

II. Módulos

Los módulos (por ejemplo las DLLs) también se almacenan en memoria, con una estructura específica, la _LDR_DATA_TABLE_ENTRY, cuyos atributos son:

```
Windows 7
 x86   x64
0x000 0x000 InLoadOrderLinks  _LIST_ENTRY
0x008 0x010 InMemoryOrderLinks   _LIST_ENTRY
0x010 0x020 InInitializationOrderLinks
_LIST_ENTRY
0x018 0x030 DllBase           Ptr32 Void
0x01c 0x038 EntryPoint        Ptr32 Void
0x020 0x040 SizeOfImage       Uint4B
0x024 0x048 FullDllName      _UNICODE_STRING
0x02c 0x058 BaseDllName      _UNICODE_STRING
0x070 0x0d8 LoadTime         _LARGE_INTEGER
```

Los primeros tres campos son punteros a diferentes listas enlazadas de módulos cargados en memoria, de las que se hablará más adelante, por lo que nos concentraremos en los siguientes atributos de la estructura:

- *DllBase* es el puntero a la dirección de memoria donde está cargado el módulo propiamente dicho.
- *FullDllName* es el nombre del módulo completo (incluyendo su ubicación en disco) y *BaseDllName* es el nombre del módulo. Las estructuras _UNICODE_STRING tienen el siguiente formato:

```
Windows 7
 x86   x64
0x000 0x000 Length        Uint2B
0x002 0x002 MaximumLength  Uint2B
0x004 _PADDING_[0x4] Uint1B
0x004 0x008 Buffer     Ptr* Uint2B
```

III. Conexiones y Sockets

Una de las particularidades de las estructuras que representan conexiones y *sockets* es que la documentación de Microsoft sobre las mismas no es pública. Por lo tanto, es necesario un trabajo de "descubrimiento" de las mismas, y de la información que contienen. Los nombres dados a estas estructuras no son "oficiales", sino a efectos de identificarlas, y buscan ser lo suficientemente representativos de los artefactos que definen.

El detalle parcial de las estructuras para cada versión de dicho sistema operativo es:

_TCP_CONNECTION

```
Windows 7
 x86   x64
0x000 0x000 CreateTime  _LARGE_INTEGER
0x00C 0x018 AddressFamily Ptr* Uint
0x010 0x020 AddressInfo   Ptr* Uint
0x014 0x028 ListEntry     _LIST_ENTRY
0x034 0x068 State         Unit8
0x038 0x06c LocalPort     Unit16
0x03A 0x06e RemotPort     Unit16
0x178 0x238 Owner         Ptr* Uint
```

_UDP_CONNECTION

```
Windows 7
 x86   x64
0x014 0x020 AddressFamily Ptr* Uint
0x018 0x028 Owner        Ptr* Uint
0x030 0x058 CreateTime  _LARGE_INTEGER
0x038 0x060 LocalAddress  Ptr* Uint
0x048 0x080 Port          Uint16
```

_SOCKET

```
Windows 7
 x86   x64
0x00C 0x020 CreateTime  _LARGE_INTEGER
0x018 0x028 Owner         Ptr* Uint
0x034 0x058 LocalAddress  Ptr* Uint
0x038 0x060 AddressFamily Ptr* Uint
0x03E 0x06a Port          Uint16
0x050 ----- EndPoint      Ptr* Uint
```

Los campos `Ptr* Uint` son `Ptr32 Uint32` o `Ptr64 Uint64` según la arquitectura.

El análisis de la memoria en búsqueda de estas estructuras es fundamental, dado que la información sobre conexiones y *sockets* sólo está presente en memoria principal, y pueden brindar información elemental como evidencia digital, más aún en la actualidad donde la sociedad está cada vez más conectada.

4.2 Almacenamiento de las estructuras de memoria en Windows

En todos los casos, ya sea para procesos, módulos, conexiones, *sockets*, archivos, *drivers* y hasta entradas de registro, hay un factor común y este es que las estructuras se ubican en *pool* de memoria. La memoria se divide en *kernel pool* que, a su vez, se divide en bloques de memoria, dentro de los cuáles se almacenan estructuras o distintos tipos de datos. Dichos bloques son los llamados *pool* de memoria.

Un *pool* de memoria, tiene la siguiente estructura y se lo puede ver como un conjunto de capas que se apilan, algunas de las cuales, son opcionales. A esta arquitectura se la llama *Kernel Pool Layout*:

Tabla I: Kernel Pool Layout.

Estructura	Win7 x86	Win7 x64	Presencia
_POOL_HEADER	8 elementos, 0x8 bytes	9 elementos, 0x10 bytes	**Obligatorio**
_OBJECT_HEADER_PROCESS_INFO	2 elementos, 0x8 bytes	2 elementos, 0x10 bytes	**Opcionales**
_OBJECT_HEADER_QUOTA_INFO	4 elementos, 0x10 bytes	5 elementos, 0x20 bytes	
_OBJECT_HEADER_HANDLE_INFO	2 elementos, 0x8 bytes	2 elementos, 0x10 bytes	
_OBJECT_HEADER_NAME_INFO	3 elementos, 0x10 bytes	3 elementos, 0x20 bytes	
_OBJECT_HEADER_CREATOR_INFO	4 elementos, 0x10 bytes	4 elementos, 0x20 bytes	
_OBJECT_HEADER	12 elementos, 0x20 bytes	12 elementos, 0x38 bytes	**Obligatorio**
OBJECT (_EPROCESS, _FILE_OBJECT)			**Obligatorio**

Para cada estructura en particular, por ejemplo _EPROCESS, el encabezado tiene una etiqueta (*tag*) que permite identificarla y saber qué artefacto se almacena en ella:

Tabla II: Pool-tag de Estructuras en Memoria.

Estructura	**Etiqueta (tag)**
Proceso	Proã
Hiloa (Thread)	Thrä
Módulos	MmLd
Archivo (File)	Filå
SymbolicLink	Linö
Controlador (Driver)	Driö
Escritorio (Desktop)	Desö
WindowStation	Winä
TCPConnection	TcpE
TCPSocket	TcpL
UDPConnection	UdpA
RegistryEntry	CM10

Más allá que las estructuras en memoria ocupen un *pool* de memoria (o varios, como en el caso de *Big Page Pool*), en algunos casos, existe una relación lógica entre distintos artefactos. Veamos, primero, un ejemplo de búsqueda de procesos activos en un volcado del tipo *Crash* Dump con BIP-M *framework*:

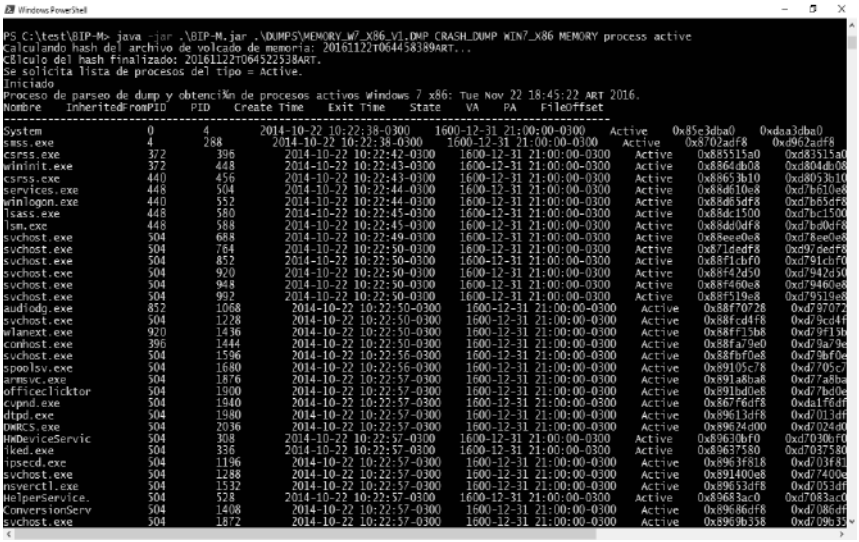


Figura 9.7: Captura de pantalla de BIP-M mostrando la información de procesos extraída de un volcado de memoria *Crash Dump*.

BIP-M *framework* obtiene este listado de procesos, recorriendo la lista circular doblemente enlazada de que implementa Windows.

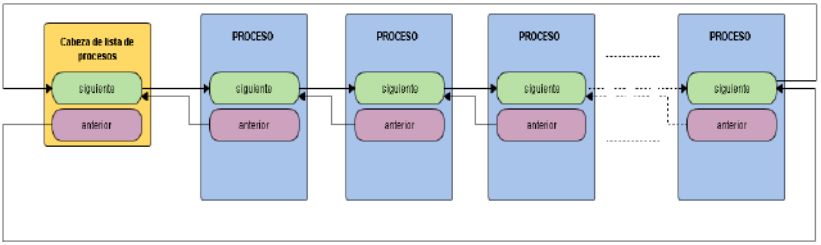


Figura 9.8: Lista doblemente enlazada de procesos activos en Microsoft Windows.

En la figura 9.8 se ilustra la lista circular doblemente enlazada de procesos activos, ésta estructura de datos permite recorrer los procesos a través de los atributos *FLINK* y *BLINK* de la estructura _EPROCESS. *PsActiveProcessHead* es la cabecera de dicha lista y se la puede encontrar como atributo del KDBG (*KernelDebugger Data Block*). Esta última

estructura contiene, además, otra información que puede ser de utilidad para poder realizar *debug* de la memoria:

```
_KDDEBUGGER_DATA64:
[0x340, {
'Header'              [0x00,
['_DBGKD_DEBUG_DATA_HEADER64']],
'PsLoadedModuleList' [0x48, ['unsigned
longlong']],
'PsActiveProcessHead'  [0x50, ['unsigned
longlong']],
...
} ]
```

```
_DBGKD_DEBUG_DATA_HEADER64:
[0x18, {
'List'          [ 0x0, ['LIST_ENTRY64']],
'OwnerTag'      [ 0x10, ['unsigned long']],
'Size'          [0x14,['unsigned long']], (832
bytes en_dump Win7x86)
}]
```

Como se puede observar, KDBG está formado con un encabezado con un *tag* específico: KDBG; seguido de esto, la estructura en sí misma con todos sus atributos.

Retomando el atributo sobre el cual veníamos hablando previamente, *PsActiveProcessHead* es una estructura del tipo _LIST_ENTRY que contiene dos atributos y permite implementar este tipo de lista:

```
Windows 7
x86   x64
0x000 0x000 Flink _LIST_ENTRY*
0x004 0x008 Blink _LIST_ENTRY*
```

Cada atributo *FLINK* apunta al atributo *FLINK* del ítem que le sigue en la lista. A la inversa sucede con el atributo *BLINK,* dado que éste apunta al atributo *FLINK* del ítem que lo precede en la lista. En este punto, es de suma importancia saber que las direcciones que poseen estos atributos, son direcciones virtuales, por lo que es fundamental traducir dichas direcciones a físicas para así poder ubicarla en memoria o, también, en un archivo de volcado de memoria. De hecho, en cualquier estructura que se encuentre, donde exista un atributo que represente a un puntero, será necesario realizar la traducción, ya que dicho puntero estará almacenado como dirección virtual.

Volviendo específicamente a la implementación de listas de estructuras, exactamente lo mismo sucede con los módulos activos cargados en memoria y, de manera análoga, se cuenta con una estructura especial del tipo _LIST_ENTRY que cumple el rol de cabecera de la lista: *PsActiveModuleList*. Existe una particularidad con los módulos y esta es que existen 3 listas circulares doblemente enlazadas que mantienen los módulos ordenados bajo 3 criterios diferentes: *InLoadMemoryOrder* (según orden en que se cargaron en memoria), *InMemoryOrderLinks* (según el orden en que se encuentran en memoria) e *InInitializationOrder* (según el orden de inicialización). En la figura 9.9 se muestra las listas doblemente enlazadas de módulos cargados en memoria:

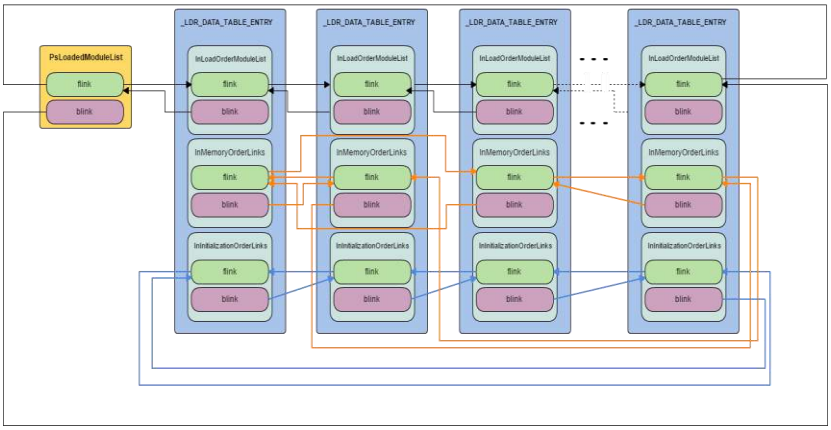


Figura 9.9: Listas doblemente enlazadas de módulos en memoria en Microsoft Windows.

4.3 Estructuras ocultas y malware en Windows

Gracias a los antes mencionados pools de memoria, es posible realizar una búsqueda de estructuras a través de una técnica llamada *pool-tag scanning* (M. H. Light, 2014). Ésta consiste en buscar en todo el volcado, las ocurrencias del *tag* de la estructura a buscar: en el caso de los procesos, la etiqueta (*tag*) es “Proã”. Una vez detectado la etiqueta, es posible construir la estructura del proceso y, así, sucesivamente con cada ocurrencia. Cada uno de estos hallazgos formará parte de una colección de potenciales procesos que, por último, se deberá comparar con la colección de procesos activos. Aquellos que no estén en esta última colección, serán los procesos sospechosos que requerirán un mayor análisis. Se debe tener en cuenta que esta técnica es susceptible de encontrar varios falsos positivos, que deberán ser manejados.

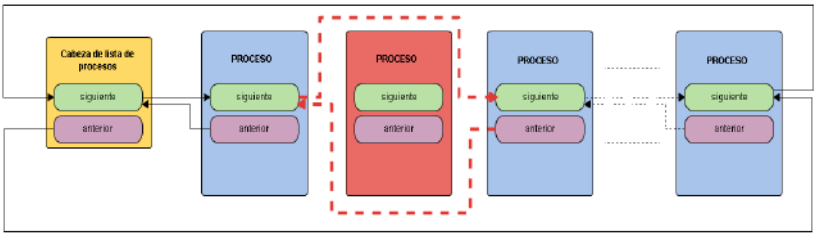


Figura 9.10: Proceso oculto, desasociado de la lista de procesos activos del sistema operativo.

Para que el *malware* se siga ejecutando una vez desvinculado de la lista de procesos, una técnica que se suele utilizar es realizar *hooks* a las llamadas al sistema (*system calls*). A través de los *hooks* se interceptan las llamadas al sistema y se realiza un salto al código malicioso, que ejecuta las acciones propias del *malware* y luego vuelve al código original continuando la ejecución en la siguiente instrucción. De esta manera, el *malware* logra ejecutarse, pero también la llamada al sistema, que devuelve la respuesta esperada, logrando así pasar desapercibido.

Existen diferentes tipos de *hooks* que se pueden realizar: IDT *Hooks* (*hooks* a la Tabla Descriptora de Interrupciones); SYSENTER *Hooks* (en sistemas modernos, la instrucción SYSENTER se utiliza en reemplazo de las interrupciones), y SSDT *Hooks* (*SystemService Dispatcher Table Hooks* (últimamente es el tipo de *hook* más utilizado).

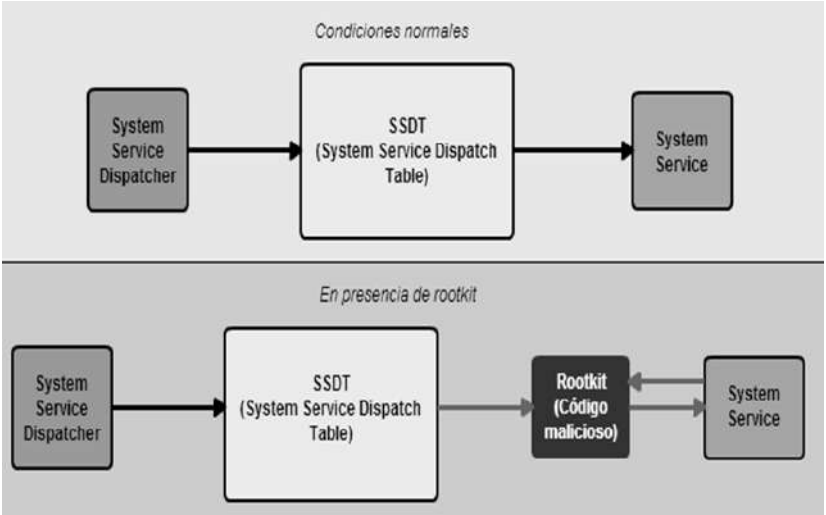


Figura 9.11: Diagrama que muestra las llamadas al sistema en condiciones normales y, en contraposición, en presencia de *rootkits* (SSDT *Hooks).*

5. Conclusiones

El análisis forense informático debe tener en cuenta el nivel de volatilidad de los datos que se pueden convertir en información relevante a partir de la evidencia digital. La adquisición del volcado de memoria para llevar adelante un análisis forense del mismo, debe realizarse en los primeros instantes en los que se tiene contacto con el equipo, dado que el contenido de la memoria cambia constantemente. La elección de la herramienta a utilizar para la adquisición del volcado de memoria es factor de éxito del posterior análisis.

En ciertas ocasiones, los objetos en memoria poseen información que sólo es posible encontrar en ella, lo que aumenta la importancia de realizar este tipo de análisis. La memoria alberga estructuras variadas, por lo que uno de los objetivos principales del analista forense debe ser la búsqueda enfocada en estructuras ocultas y el hallazgo de pruebas que indiquen la existencia de *software*

malintencionado: su presencia puede ser clave en una investigación y, en muchas ocasiones, dejan rastros exclusivamente en memoria.

6. Referencias

Burdach, M. (2008). Finding Digital Evidence In Physical Memory. *Black Hat Federal*.

Light, M. H. A. C. (2014). *The Art of Memory Forensics.*

Russinovich, M. D. S. (2009). *Windows Internals 5.*

Russinovich, M. D. S. (2012). *Windows Internals 6.*

Schuster, A.. (2006). *Searching for processes and threads in Microsoft.*

Sikorski, M. & Honig, A. (2012). *Practical Malware Analysis*.

Epílogo: Un escenario desafiante

El campo de los delitos informáticos y la prueba informática está sujeto a una evolución vertiginosa. Al compás de los avances tecnológicos y de la difusión masiva de dichos progresos, emergen incesantemente nuevos fenómenos delictivos y nuevas formas de comisión de delitos tradicionales. Asimismo, sus autores dejan rastros o vestigios antes desconocidos. Estas huellas escapan a las categorías tradicionales, y exigen un esfuerzo considerable para su efectiva búsqueda, obtención, conservación, análisis y presentación ante la autoridad judicial.

Desde la perspectiva de la justicia penal, estos cambios traen nuevas necesidades sociales que proteger, y nuevas exigencias respecto de los procedimientos y métodos de investigación y prueba.

En este contexto, la informática forense, pese a ser una disciplina joven, corre el riesgo de envejecimiento prematuro.

La visión tradicional de la informática, limitada a computadoras personales, traía aparejado un modelo de informática forense ceñido a la búsqueda de evidencia digital en dispositivos aislados. La primera revolución de internet, que extendió la influencia de la informática en múltiples dimensiones de la vida social, viene exigiendo una adaptación en el área forense. El creciente empleo de diversas modalidades de comercio electrónico y gobierno electrónico fue generando novedosas formas de relación entre las personas y las corporaciones privadas y públicas.

En medio de estos cambios, han aparecido nuevas formas de movimientos dinerarios (transacciones electrónicas, *e-banking*), y el denominado dinero electrónico.

La evolución de la red de redes dio lugar a la aparición de la denominada Web 2.0 y 3.0, donde el acceso masivo a internet se vio acompañado con nuevas funcionalidades y

modos de uso. Hoy es común utilizar plataformas de educación a distancia, software en línea, almacenamiento en la nube, así como también es usual acceder a contenidos multimedia *on demand*, interactuar con medios de periodismo digital, participar en foros, blogs, redes sociales, etc.

Paralelamente a la creciente interactividad de internet, la digitalización de las telecomunicaciones y la masificación del empleo de teléfonos móviles abrieron el camino a una progresiva convergencia tecnológica. La cada vez más íntima vinculación entre informática y telecomunicaciones es simplemente el anticipo de una nueva ola o revolución tecnológica: la denominada internet de las cosas (IdC o, en su sigla original, IoT) o internet de todo (IdT o IoE). Personas, cosas, datos, lugares y procesos se interrelacionan cada vez más intensamente. Los smartphones son, quizás, la muestra más visible de aquello que viene: una enorme diversidad de artefactos y dispositivos inteligentes, conectados o conectables, con capacidad de interactuar entre sí, ya sea en forma manual o automática. Televisores, automóviles, sistemas de monitoreo, drones, dispositivos de geolocalización, relojes, consolas de videojuegos, electrodomésticos, equipamientos médicos, drones… la lista es interminable.

Estos cambios vertiginosos están teniendo un alto impacto sobre el área de la justicia penal, en primer lugar, vienen posibilitando la aparición de fenómenos criminales antes inexistentes (por ej.: tácticas virtuales de seducción a menores de edad con fines delictivos, redes de pedofilia, ciberacoso, etc.) y además, son acompañados también por nuevas conductas de víctimas y victimarios (exposición de la intimidad, comunicación con personas desconocidas, etc.), y por consecuente la multiplicación de los rastros o huellas que ambos pueden dejar en un nuevo espacio de interacción (el ciberespacio). Este ámbito presenta una creciente complejidad, ya que se ha diversificado enormemente las posibles formas de emisión, codificación, canalización,

almacenamiento, decodificación, recepción y empleo de información; y también se han incrementado los riesgos de ruidos o interferencias. La exponencial multiplicación de datos que ingresan en el ciberespacio, si bien ofrece oportunidades para una investigación penal, también genera el peligro de extravíos y desorientación.

La conectividad de cada vez más clases de dispositivos, el consecuente incremento de aplicaciones de software, la expansión exponencial de contenidos y comunicaciones generan para el informático forense un conjunto de desafíos, a saber:

- *Peligro de obsolescencia:* La necesidad de innovación y actualización permanente es algo obvio, pero la conciencia de éste desafío debe traducirse en prácticas concretas de carácter proactive: nuevos dispositivos y aplicaciones; nuevos fenómenos y modalidades delictivas; nuevas clases de rastros digitales; nuevos métodos y técnicas forenses; entre otros.

- *Conflictos internos:* Aquellos expertos que se desempeñan en organismos judiciales deben lidiar contra una previsible resistencia al cambio al interior de esas instituciones. Tal resistencia puede presentar múltiples facetas: inadecuado diseño de puestos de trabajo; desconocimiento en materia de inversiones y gastos en equipamiento; incomprensión de cuestiones técnicas; escasa noción de los niveles de formalización requeridos para cada tipo de labor; etc.

- *Problemas que exceden la capacidad individual de abordaje:* Este desafío tiene, a su vez, varias aristas. Por un lado, la expansión de la informática obliga cada vez más a la especialización, por lo que es imposible para un solo experto dominar todo el campo de conocimientos y habilidades propios del área en forma permanentemente actualizada. Por otro lado,

frecuentemente será necesario integrar la labor con la tarea de especialistas de otras disciplinas (contabilidad, psicología, electrónica, etc.) lo que exige una especial apertura interdisciplinaria, que va más allá del campo técnico y científico, y abarca a operadores jurídicos y a investigadores judiciales. El desarrollo de habilidades de trabajo en equipo es, en éste sentido, fundamental.

- *Desafíos al eficiente funcionamiento de los laboratorios informático forenses:* El crecimiento inusitado de datos y dispositivos con presunto valor investigativo puede generar importantes niveles de saturación de las oficinas técnicas, y cuellos de botella en los procesos judiciales. Se requiere contar con una adecuada jerarquización de labores; aplicar técnicas de triage para no inundar los laboratorios con datos y dispositivos irrelevantes; administrar de modo efectivo y sustentable la capacidad de almacenamiento en función de la carga de datos acumulada; precisar la contribución del experto (para evitar la intervención en cuestiones superfluas o ajenas a la incumbencia); organizar la actualización de conocimientos y herramientas de trabajo; etc.

- *Necesidad de promover la formación de redes de colaboración informático forense e integrarse en las mismas:* En muchas ocasiones, la índole de ciertas temáticas o la carencia de herramientas técnicas adecuadas para ciertos tipos de tareas obligará a solicitar el auxilio de otro laboratorio u oficina. Pero también hay otros casos que exigen esta cooperación. El ciberespacio desdibuja las fronteras nacionales y jurisdiccionales. Muchos delitos pueden ser cometidos desde diversos lugares, o contra víctimas dispersas en distintos países, o dejar rastros en jurisdicciones diferentes. Tender puentes de cooperación técnica y establecer procedimientos de trabajo basados en

estándares comunes puede ser crucial para el éxito de esa clase de investigaciones.

- *Escasas capacidades de implementar medidas de investigación en tiempo real:* La adopción de tácticas investigativas en tiempo real (intervención y/o bloqueo de comunicaciones y transacciones electrónicas, agente encubierto informático, etc.) puede llegar a ser necesaria en casos excepcionales. Más allá de las exigencias legales, ello también requiere desplegar capacidades y herramientas adecuadas.

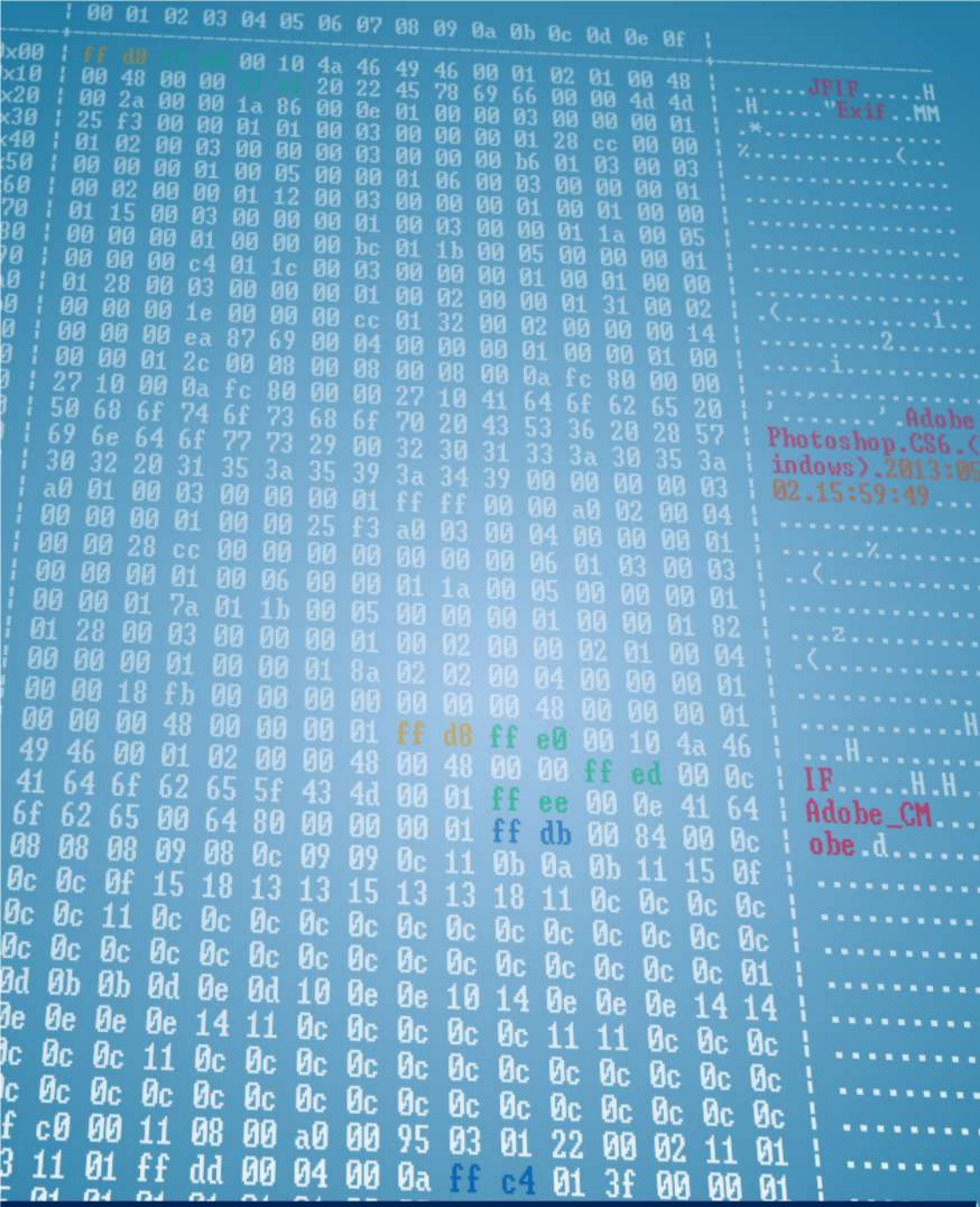
- *La necesidad de generar y emplear bases de conocimiento:* La creciente diversidad de dispositivos y aplicaciones torna más dificultosa la identificación de las herramientas empleadas para la creación, edición o transmisión de una determinada evidencia digital. Poder contar con bases de conocimiento actualizadas relativas a las estructuras de datos y a los metadatos característicos de cada herramienta puede facilitar en gran medida esta tarea.

- *El desafío de los macrodatos:* La sistematización de datos disponibles en fuentes abiertas de información (OSINT), datos de tráfico y otros metadatos, puede generar nueva información relevante para un caso penal. Para que esta tarea sea provechosa, el trabajo del informático forense debe complementarse con la labor del analista de información.

- *Las políticas y prácticas de las empresas tecnológicas:* Formalmente, el vínculo con las empresas proveedoras de hardware, software y servicios digitales está a cargo de jueces y fiscales. Sin embargo, para el eficaz acceso a datos provenientes de dichas compañías se requiere una adecuada coordinación técnica. En este aspecto, la intervención de los expertos informático forenses es clave.

- *Crecientes exigencias en materia de observancia de deberes legales:* En un caso penal, el informático forense suele tener acceso a gran cantidad de dispositivos, en un contexto de constante aumento de las capacidades de almacenamiento de muchos de estos artefactos. A ello se pueden sumar los datos proporcionados por las empresas tecnológicas, y los provenientes de fuentes abiertas. Tal circunstancia coloca al experto frente a un cúmulo de datos, muchos de los cuales no guardan relación con el caso concreto. El especialista debe preservar de toda curiosidad e indiscreción la información no pertinente (ej.: la vinculada con terceros ajenos a la investigación, los datos atinentes a las áreas de la vida del sospechado que no son objeto de investigación, las comunicaciones o contenidos confidenciales). De igual modo, también deberá adoptar recaudos para evitar la pérdida o modificación de datos.

El panorama trazado no es exhaustivo, pero permite avizorar los escenarios de trabajo de los informáticos forenses en un futuro que ya está aquí. Los motivos de inquietud son muchos, pero los desafíos son estimulantes, pues ponen a prueba la creatividad, la tenacidad y los valores de esta joven comunidad de expertos.



© 2017 CRAI
Universidad FASTA Ediciones
Mar del Plata, Argentina
ISBN: 978-987-1312-81-8

UNIVERSIDAD FASTA
FACULTAD DE INGENIERÍA