Informática Forense

Giovanni Zuccardi
Juan David Gutiérrez

Noviembre de 2006

CONTENIDO

Introducción

La informática forense está adquiriendo una gran importancia dentro del área de la información electrónica, esto debido al aumento del valor de la información y/o al uso que se le da a ésta, al desarrollo de nuevos espacios donde es usada (por Ej. El Internet), y al extenso uso de computadores por parte de las compañías de negocios tradicionales (por Ej. bancos). Es por esto que cuando se realiza un crimen, muchas veces la información queda almacenada en forma digital. Sin embargo, existe un gran problema, debido a que los computadores guardan la información de información forma tal que no puede ser recolectada o usada como prueba utilizando medios comunes, se deben utilizar mecanismos diferentes a los tradicionales. Es de aquí que surge el estudio de la computación forense como una ciencia relativamente nueva.

Resaltando su carácter científico, tiene sus fundamentos en las leyes de la física, de la electricidad y el magnetismo. Es gracias a fenómenos electromagnéticos que la información se puede almacenar, leer e incluso recuperar cuando se creía eliminada.

La informática forense, aplicando procedimientos estrictos y rigurosos puede ayudar a resolver grandes crímenes apoyándose en el método científico, aplicado a la recolección, análisis y validación de todo tipo de pruebas digitales.

¿Qué es la Informática Forense?

Según el FBI, la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional [ReEx00].

La informática forense hace entonces su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proce[Acis06].

Desde 1984, el Laboratorio del FBI y otras agencias que persiguen el cumplimiento de la ley empezaron a desarrollar programas para examinar evidencia computacional.

Dentro de lo forense encontramos varias definiciones [Acis06]:

Computación forense (computer forensics) que entendemos por disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso; o como la disciplina científica y especializada que entendiendo los elementos propios de las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos.

Forensia en redes (network forensics)
Es un escenario aún más complejo, pues es necesario comprender la manera como los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular.
Esta conjunción de palabras establece un profesional que entendiendo las operaciones de las redes de computadores, es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado para concluir su acción. A diferencia de la definición de computación forense, este contexto exige capacidad de correlación de evento, muchas veces disyuntos y aleatorios, que en equipos particulares, es poco frecuente.

Forensia digital (digital forensics)
Forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos (¿quién?, ¿cómo?, ¿dónde?, ¿cuándo?, ¿porqué?) de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática.

Importancia de la Informática Forense

"High-tech crime is one of the most important priorities of the Department of Justice"[JaRe96]. Con esta frase podemos ver cómo poco a poco los crímenes informáticos, su prevención, y procesamiento se vuelven cada vez más importantes. Esto es respaldado por estudios sobre el número de incidentes reportados por las empresas debido a crímenes relacionados con la informática. (Ver [CERT06])
Sin embargo, la importancia real de la informática forense proviene de sus objetivos.

Objetivos de la Informática Forense

La informática forense tiene 3 objetivos, a saber:

1. La compensación de los daños causados por los criminales o intrusos.
2. La persecución y procesamiento judicial de los criminales.
3. La creación y aplicación de medidas para prevenir casos similares.

Estos objetivos son logrados de varias formas, entre ellas, la principal es la recolección de evidencia.

Usos de la Informática Forense [InfFor01]

Existen varios usos de la informática forense, muchos de estos usos provienen de la vida diaria, y no tienen que estar directamente relacionados con la informática forense:

1. Prosecución Criminal: Evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.
2. Litigación Civil: Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.
3. Investigación de Seguros: La evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.
4. Temas corporativos: Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.
5. Mantenimiento de la ley: La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

Ciencia Forense

La ciencia forense nos proporciona los principios y técnicas que facilitan la investigación del delito criminal, en otras palabras: cualquier principio o técnica que puede ser aplicada para identificar, recuperar, reconstruir o

analizar la evidencia durante una investigación criminal forma parte de la ciencia forense. [ForIRT01]

Los principios científicos que hay detrás del procesamiento de una evidencia son reconocidos y usados en procedimientos como:

- Recoger y examinar huellas dactilares y ADN.
- Recuperar documentos de un dispositivo dañado.
- Hacer una copia exacta de una evidencia digital.
- Generar una huella digital con un algoritmo hash MD5 o SHA1 de un texto para asegurar que este no se ha modificado.
- Firmar digitalmente un documento para poder afirmar que es auténtico y preservar la cadena de evidencias.

Un forense aporta su entrenamiento para ayudar a los investigadores a reconstruir el crimen y encontrar pistas. Aplicando un método científico analiza las evidencias disponibles, crea hipótesis sobre lo ocurrido para crear la evidencia y realiza pruebas, controles para confirmar o contradecir esas hipótesis. Esto puede llevar a una gran cantidad de posibilidades sobre lo que pudo ocurrir, esto es debido a que un forense no puede conocer el pasado, no puede saber qué ocurrió ya que sólo dispone de una información limitada. Por esto, sólo puede presentar posibilidades basadas en la información limitada que posee.

Un principio fundamental en la ciencia forense, que usaremos continuamente para relacionar un criminal con el crimen que ha cometido, es el Principio de Intercambio o transferencia de Locard, (Edmond Locard, francés fundador del instituto de criminalistica de la universidad de Lion, podemos ver el esquema en la figura 1.

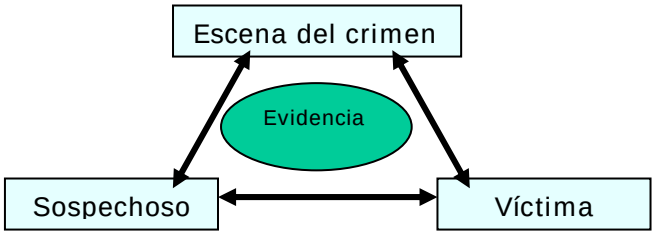

Figura 1: Principio de transferencia de Locard.

Este principio fundamental viene a decir que cualquiera o cualquier objeto que entra en la escena del crimen deja un rastro en la escena o en la víctima y vice-versa (se lleva consigo), en otras palabras: “cada contacto deja un rastro”. En el mundo real significa que si piso la escena del crimen con toda seguridad dejaré algo mío ahí, pelo, sudor, huellas, etc. Pero también me llevaré algo conmigo cuando abandone la escena del crimen, ya sea barro, olor, una fibra, etc. Con algunas de estas evidencias, los forenses podrán demostrar que hay una posibilidad muy alta de que el criminal estuviera en la escena del crimen.

En este ejemplo hemos hablado de evidencias físicas, en la ciencia forense tradicional hay varios tipos de evidencias físicas:

- **Evidencia transitoria**: como su nombre indica es temporal por naturaleza, por ejemplo un olor, la temperatura, o unas letras sobre la arena o nieve (un objeto blando o cambiante).
- **Evidencia curso o patrón**: producidas por contacto, por ejemplo la trayectoria de una bala, un patrón de rotura de un cristal, patrones de posicionamiento de muebles, etc.
- **Evidencia condicional**: causadas por una acción o un evento en la escena del crimen, por ejemplo la localización de una evidencia en relación con el cuerpo, una ventana abierta o cerrada, una radio encendida o apagada, dirección del humo, etc.
- **Evidencia transferida**: generalmente producidas por contacto entre personas, entre objetos o entre personas y objetos. Aquí descubrimos el **concepto de relación**.

En la práctica las evidencias transferidas se dividen en dos tipos, conocidas como:

- Transferencia por **rastro**: aquí entra la sangre, semen, pelo, etc.
- Transferencia por **huella**: huellas de zapato, dactilares, etc.

Aunque en la realidad, estas últimas suelen mezclarse, por ejemplo una huella de zapato sobre un charco de sangre.

El principio de intercambio de Locard se puede resumir así:

1. El sospechoso se llevará lejos algún rastro de la escena y de la víctima.
2. La víctima retendrá restos del sospechoso y puede dejar rastros de si mismo en el sospechoso.
3. El sospechoso dejará algún rastro en la escena.

El objetivo es establecer una relación entre los diferentes componentes:

- la escena del crimen
- la víctima
- la evidencia física
- el sospechoso

Para la correcta resolución del caso, todos estos componentes deben estar relacionados. Esto se conoce como el **concepto de relación**, que es lo que nos faltaba para completar el principio de intercambio de Locard.

Las evidencias pueden, a su vez, ser transferidas de dos formas distintas:

1. Transferencia directa: cuando es transferida desde su origen a otra persona u objeto de forma directa.
2. Transferencia indirecta: cuando es transferida directamente a una localización y, de nuevo, es transferida a otro lugar.

Importante resaltar que cualquier cosa y todo puede ser una evidencia.

Brevemente, la ciencia forense facilita las herramientas, técnicas y métodos sistemáticos (pero científicos) que pueden ser usados para analizar una evidencia digital y usar dicha evidencia para reconstruir qué ocurrió durante la realización del crimen con el último propósito de relacionar al autor, a la víctima y la escena del crimen.

Network Forensics

Forensia en redes, es un escenario aún más complejo, pues es necesario comprender la manera como los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular. Esta conjunción de palabras establece un profesional que entendiendo las operaciones de las redes de computadores, es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado para concluir su acción. A diferencia de la definición de computación forense, este contexto exige capacidad de correlación de evento, muchas veces disyuntos y aleatorios, que en equipos particulares, es poco frecuente [Acis06].

Es la captura, almacenamiento y análisis de los eventos de una red, para descubrir el origen de un ataque o un posible incidente.

NFTA (Network Forensic Analysis Tool)

Evidencia Digital

Casey define la evidencia de digital como "*cualquier dato que puede establecer que un crimen se ha ejecutado (commit) o puede proporcionar una enlace (link) entre un crimen y su víctima o un crimen y su autor*". [Casey04]

"Cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático" [HBIT03]

A diferencia de la documentación en papel, la evidencia computacional es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto único de la evidencia computacional es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizó una copia. [ComEvi02]. Esta situación crea problemas concernientes a la investigación del robo de secretos comerciales, como listas de clientes, material de investigación, archivos de diseño asistidos por computador, fórmulas y software propietario.
Debe tenerse en cuenta que los datos digitales adquiridos de copias no se deben alterar de los originales del disco, porque esto invalidaría la evidencia; por esto los investigadores deben revisar con frecuencia que sus copias sean exactas a las del disco del sospechoso, para esto se utilizan varias tecnologías, como por ejemplo *checksums* o *hash* MD5 [DaVa01].

Cuando ha sucedido un incidente, generalmente, las personas involucradas en el crimen intentan manipular y alterar la evidencia digital, tratando de borrar cualquier rastro que pueda dar muestras del daño. Sin embargo, este problema es mitigado con algunas características que posee la evidencia digital. [Casey04]

- La evidencia de Digital puede ser duplicada de forma exacta y se puede sacar una copia para ser examinada como si fuera la original. Esto se hace comúnmente para no manejar los originales y evitar el riesgo de dañarlos.
- Actualmente, con las herramientas existentes, se muy fácil comparar la evidencia digital con su original, y determinar si la evidencia digital ha sido alterada.

- La evidencia de Digital es muy difícil de eliminar. Aún cuando un registro es borrado del disco duro del computador, y éste ha sido formateado, es posible recuperarlo.
- Cuando los individuos involucrados en un crimen tratan de destruir la evidencia, existen copias que permanecen en otros sitios.

Clasificación de la evidencia digital

Cano clasifica la evidencia digital que contiene texto en 3 categorías [EviDig05]:

Registros generados por computador: Estos registros son aquellos, que como dice su nombre, son generados como efecto de la programación de un computador. Los registros generados por computador son inalterables por una persona. Estos registros son llamados registros de eventos de seguridad (logs) y sirven como prueba tras demostrar el correcto y adecuado funcionamiento del sistema o computador que generó el registro.

Registros no generados sino simplemente almacenados por o en computadores: Estos registros son aquellos generados por una persona, y que son almacenados en el computador, por ejemplo, un documento realizado con un procesador de palabras. En estos registros es importante lograr demostrar la identidad del generador, y probar hechos o afirmaciones contenidas en la evidencia misma. Para lo anterior se debe demostrar sucesos que muestren que las afirmaciones humanas contenidas en la evidencia son reales.

Registros híbridos que incluyen tanto registros generados por computador como almacenados en los mismos: Los registros híbridos son aquellos que combinan afirmaciones humanas y logs. Para que estos registros sirvan como prueba deben cumplir los dos requisitos anteriores.

Criterios de admisibilidad

En legislaciones modernas existen cuatro criterios que se deben tener en cuenta para analizar al momento de decidir sobre la admisibilidad de la evidencia: la autenticidad, la confiabilidad, la completitud o suficiencia, y el apego y respeto por las leyes y reglas del poder judicial [AdmEvi03].

Autenticidad: Una evidencia digital será autentica siempre y cuando se cumplan dos elementos:

- El primero, demostrar que dicha evidencia ha sido generada y registrada en el lugar de los hechos
- La segunda, la evidencia digital debe mostrar que los medios originales no han sido modificados, es decir, que la los registros corresponden efectivamente a la realidad y que son un fiel reflejo de la misma.

A diferencia de los medios no digitales, en los digitales se presenta gran volatilidad y alta capacidad de manipulación. Por esta razón es importante aclarar que es indispensable verificar la autenticidad de las pruebas presentadas en medios digitales contrario a los no digitales, en las que aplica que la autenticidad de las pruebas aportadas no será refutada, de acuerdo por lo dispuesto por el artículo 11 de la ley 446 de 1998: "*Autenticidad de documentos. En todos los procesos, los documentos privados presentados por las partes para ser incorporados a un expediente judicial con fines probatorios, se reputarán auténticos, sin necesidad de presentación personal ni autenticación. Todo ello sin perjuicio de lo dispuesto en relación con los documentos emanados de terceros*" [Ley446].

Para asegurar el cumplimiento de la autenticidad se requiere que una arquitectura exhiba mecanismos que certifiquen la integridad de los archivos y el control de cambios de los mismos.

Confiabilidad: Se dice que los registros de eventos de seguridad son confiables si provienen de fuentes que son "*creíbles y verificable*" [AdmEvi03]. Para probar esto, se debe contar con una arquitectura de computación en correcto funcionamiento, la cual demuestre que los logs que genera tiene una forma confiable de ser identificados, recolectados, almacenados y verificados.

Una prueba digital es confiable si el "*sistema que lo produjo no ha sido violado y estaba en correcto funcionamiento al momento de recibir, almacenar o generar la prueba*" [EviDig05]. La arquitectura de computación del sistema logrará tener un funcionamiento correcto siempre que tenga algún mecanismo de sincronización del registro de las acciones de los usurarios del sistema y que a posea con un registro centralizado e íntegro de los mismos registros.

Suficiencia o completitud de las pruebas: Para que una prueba esté considerada dentro del criterio de la suficiencia debe estar completa. Para asegurar esto es necesario "contar con mecanismos que proporcionen integridad, sincronización y centralización" [AdmEvi03] para lograr tener una vista completa de la situación. Para lograr lo anterior es necesario hacer una verdadera correlación de eventos, la cual puede ser manual o sistematizada.

Apogeo y respeto por las leyes y reglas del poder judicial: Este criterio se refiere a que la evidencia digital debe cumplir con los códigos de procedimientos y disposiciones legales del ordenamiento del país. Es decir, debe respetar y cumplir las normas legales vigentes en el sistema jurídico.

Manipulación de la evidencia digital

Es importante tener presente los siguientes requisitos que se deben cumplir en cuanto a la manipulación de la evidencia digital.

- Hacer uso de medios forenses estériles (para copias de información)

- Mantener y controlar la integridad del medio original. Esto significa, que a la hora de recolectar la evidencia digital, las acciones realizadas no deben cambiar nunca esta evidencia.

- Cuando sea necesario que una persona tenga acceso a evidencia digital forense, esa persona debe ser un profesional forense.

- Las copias de los datos obtenidas, deben estar correctamente marcadas, controladas y preservadas. Y al igual que los resultados de la investigación, deben estar disponibles para su revisión.

- Siempre que la evidencia digital este en poder de algún individuo, éste será responsable de todas la acciones tomadas con respecto a ella, mientras esté en su poder.

- Las agencias responsables de llevar el proceso de recolección y análisis de la evidencia digital, serán quienes deben garantizar el cumplimiento de los principios anteriores.

Gestión de la Evidencia digital

Existen gran cantidad de guías y buenas prácticas que nos muestran como llevar acabo la gestión de la evidencia digital
Las guías que se utilizan tienen como objetivo identificar evidencia digital con el fin de que pueda ser usada dentro de una investigación. Estas guías se basan en el método científico para concluir o deducir algo acerca de la información. Presentan una serie de etapas para recuperar la mayor cantidad de fuentes digitales con el fin de asistir en la reconstrucción posterior de eventos. Existen diferentes tipos de planteamientos, estos varían dependiendo del criterio de la institución y/o personas que definen la guía, como se define a continuación.

Guías Mejores Prácticas

A continuación se enuncian siete guías existentes a nivel mundial de mejores prácticas en computación forense.

RFC 3227

El "RFC 3227: Guía Para Recolectar y Archivar Evidencia" (*Guidelines for Evidence Collection and Archiving*) [GuEvCo02], escrito en febrero de 2002 por Dominique Brezinski y Tom Killalea, ingenieros del Network Working Group. Es un documento que provee una guía de alto nivel para recolectar y archivar datos relacionados con intrusiones. Muestra las mejores prácticas para determinar la volatilidad de los datos, decidir que recolectar, desarrollar la recolección y determinar como almacenar y documentar los datos. También explica algunos conceptos relacionados a la parte legal. Su estructura es:

a) Principios durante la recolección de evidencia: orden de volatilidad de los datos, cosas para evitar, consideraciones de privacidad y legales.
b) El proceso de recolección: transparencia y pasos de recolección.
c) El proceso de archivo: la cadena de custodia y donde y como archivar.

Guía de la IOCE

La IOCE [IOCE06], publico "Guía para las mejores practicas en el examen forense de tecnología digital"
(*Guidelines for the best practices in the forensic examination of digital technology*) [IOCE02]. El documento provee una serie de estándares, principios de calidad y aproximaciones para la detección prevención, recuperación, examinación y uso de la evidencia digital para fines forenses. Cubre los sistemas, procedimientos, personal, equipo y requerimientos de comodidad que se necesitan para todo el proceso forense de evidencia digital, desde examinar la escena del crimen hasta la presentación en la corte. Su estructura es:

a) Garantía de calidad (enunciados generales de roles, requisitos y pruebas de aptitud del personal, documentación, herramientas y validación de las mismas y espacio de trabajo).
b) Determinación de los requisitos de examen del caso.
c) Principios generales que se aplican a la recuperación de la evidencia digital (recomendaciones generales, documentación y responsabilidad).
d) Prácticas aplicables al examen de la evidencia de digital.
e) Localización y recuperación de la evidencia de digital en la escena: precauciones, búsqueda en la escena, recolección de la evidencia y empaquetado, etiquetando y documentación.
f) Priorización de la evidencia.
g) Examinar la evidencia: protocolos de análisis y expedientes de caso.
h) Evaluación e interpretación de la evidencia
i) Presentación de resultados (informe escrito).
j) Revisión del archivo del caso: Revisión técnica y revisión administrativa.
k) Presentación oral de la evidencia.
l) Procedimientos de seguridad y quejas.

Investigación en la Escena del Crimen Electrónico (Guía DoJ 1)

El Departamento de Justicia de los Estados Unidos de América (DoJ EEUU), publico "Investigación En La Escena Del Crimen Electrónico" (*Electronic Crime Scene Investigation: A Guide for First Responders*) [ElCr01]. Esta

guía se enfoca más que todo en identificación y recolección de evidencia. Su estructura es:

a) Dispositivos electrónicos (tipos de dispositivos se pueden encontrar y cual puede ser la posible evidencia).
b) Herramientas para investigar y equipo.
c) Asegurar y evaluar la escena.
d) Documentar la escena.
e) Recolección de evidencia.
f) Empaque, transporte y almacenamiento de la evidencia.
g) Examen forense y clasificación de delitos.
h) Anexos (glosario, listas de recursos legales, listas de recursos técnicos y listas de recursos de entrenamiento).

Examen Forense de Evidencia Digital (Guía DoJ 2)
Otra guía del DoJ EEUU, es "Examen Forense de Evidencia Digital" (*Forensic Examination of Digital Evidence: A Guide for Law Enforcement*) [FoEx04]. Esta guía esta pensada para ser usada en el momento de examinar la evidencia digital. Su estructura es:

a) Desarrollar políticas y procedimientos con el fin de darle un buen trato a la evidencia.
b) Determinar el curso de la evidencia a partir del alcance del caso.
c) Adquirir la evidencia.
d) Examinar la evidencia.
e) Documentación y reportes.
f) Anexos (casos de estudio, glosario, formatos, listas de recursos técnicos y listas de recursos
de entrenamiento).

Computación Forense - Parte 2: Mejores Prácticas (Guía Hong Kong)
El ISFS, *Information Security and Forensic Society* (Sociedad de Seguridad Informatica y Forense) creada en Hong Kong, publico "Computación Forense - Parte 2: Mejores Practicas" (*Computer Forensics – Part 2: Best Practices*) [CoFor04]. Esta guía cubre los procedimientos y otros requerimientos necesarios involucrados en el proceso forense de evidencia digital, desde el examen de la escena del crimen hasta la presentación de los reportes en la corte. Su estructura es:

a) Introducción a la computación forense.
b) Calidad en la computación forense.
c) Evidencia digital.
d) Recolección de Evidencia.
e) Consideraciones legales (orientado a la legislación de Hong Kong).
f) Anexos.

Guía De Buenas Prácticas Para Evidencia Basada En Computadores (Guía Reino Unido)
La ACPO, *Association of Chief Police Officers* (Asociación de Jefes de Policía), del Reino Unido mediante su departamento de crimen por computador, publico "Guía de Buenas Practicas para Evidencia basada en Computadores" (*Good Practice Guide For Computer Based Evidence*) [GoPra99]. La policía

creó este documento con el fin de ser usado por sus miembros como una guía de buenas prácticas para ocuparse de computadores y de otros dispositivos electrónicos que puedan ser evidencia. Su estructura es:

a) Los principios de la evidencia basada en computadores.
b) Oficiales atendiendo a la escena.
c) Oficiales investigadores.
d) Personal para la recuperación de evidencia basada en computadores.
e) Testigos de consulta externos.
f) Anexos (legislación relevante, glosario y formatos)

Guía Para El Manejo De Evidencia En IT (Guía Australia)

Standards Australia (Estándares de Australia) publico "Guía Para El Manejo De Evidencia En IT" (HB171:2003 *Handbook Guidelines for the management of IT evidence*) [HBIT03]. Esta guía no esta disponible para su libre distribución, por esto para su investigación se consultaron los artículos "Buenas Prácticas En La Administración De La Evidencia Digital" [BueAdm06] y "*New Guidelines to Combat ECrime*" [NeGu03]. Es una guía creada con el fin de asistir a las organizaciones para combatir el crimen electrónico. Establece puntos de referencia para la preservación y recolección de la evidencia digital.
Detalla el ciclo de administración de evidencia de la siguiente forma:

a) Diseño de la evidencia.
b) Producción de la evidencia.
c) Recolección de la evidencia.
d) Análisis de la evidencia.
e) Reporte y presentación.
f) Determinación de la relevancia de la evidencia.

Herramientas

Figuras

Bibliografía

[ReEx00] Michael G. Noblett. (2000) Recovering and Examining Computer Forensic Evidence. Disponible en:
http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm

[ScWo00] Scientific Working Group on Digital Evidence (SWGDE) (2000) Digital Evidence: Standards and Principles. Disponible en:
http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm

[InfFor01] Óscar López, Haver Amaya, Ricardo León. (2001) Informática forense: generalidades, aspectos técnicos y herramientas

[ForIRT01] Antonio Javier García Martínez. (2001) LA FORMACIÓN DE UN IRT (Incident Response Team) FORENSE

[ComEvi01] Computer Evidence Defined
http://www.forensics-intl.com/def3.html

[BueAdm06] Cano Martines Jeimy José. (2006) Buenas prácticas en la administración de la evidencia digital Disponible:
http://gecti.uniandes.edu.co/docs/buenas%20practica%20evidencia%20digital%20jcano.pdf [May 2006]

[DaVa01] Brian Deering. Data Validation Using The Md5 Hash
http://www.forensics-intl.com/art12.html

[JaRe96] Janet Reno, U.S. Attorney General, Oct 28, 1996

[CERT06] CERT/CC Statistics 1988-2006 Disponible en:
http://www.cert.org/stats/cert_stats.html

[HBIT03] HB171:2003 Handbook Guidelines for the management of IT evidence Disponible en:

http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf

[Casey04] CASEY, Eoghan. “Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet”. 2004

[EviDig05] Cano Martines Jeimy José, Mosquera González José Alejandro, Certain Jaramillo Andrés Felipe. Evidencia Digital: contexto, situación e implicaciones nacionales. Abril de 2005.
http://derecho.uniandes.edu.co/derecho1/export/derecho/descargas/texto/NasTecnologias6.pdf

[AdmEvi03] Cano Martines Jeimy José. Admisibilidad de la Evidencia Digital: Algunos Elementos de Revisión y Análisis. Agosto de 2003. http://www.alfa-redi.org/rdi-articulo.shtml?x=1304

[Ley446] Ley 446 de Julio de 1998, http://www.sic.gov.co/Normatividad/Leyes/Ley%20446-98.php
[ElCr01] US DEPARTMENT OF JUSTICE, Electronic Crime Scene Investigation: A Guide for First Responders, 2001

[GuEvCo02] BREZINSKI, D. y KILLALEA, T. (2002) RFC 3227: Guidelines for Evidence Collection and Archiving. Network Working Group. February. Disponible: http://www.rfceditor.org/rfc/rfc3227.txt

[IOCE02]. IOCE, Guidelines for the best practices in the forensic examination of digital technology, 2002. Disponible: http://www.ioce.org/2002/ioce_bp_exam_digit_tech.html

[IOCE06]. IOCE, International Organization of Computer Evidence. Disponible: http://www.ioce.org

[FoEx04] US DEPARTMENT OF JUSTICE, Forensic examination of digital evidence. A guide for law enforcement. Special Report, 2004

[CoFor04]. INFORMATION SECURITY AND FORENSICS. Computer forensics. Part2: Best Practices, 2004 Disponible: http://www.isfs.org.hk/publications/ComputerForensics/ComputerForensics_part2.pdf

[GoPra99]. ASSOCIATION OF CHIEF POLICE OFFICERS Good practice guide for computer based evidence, 1999. Disponible: http://www.digital-detective.co.uk/documents/acpo.pdf

[NeGu03]. GODFREY, T. New Guidelines to Combat E-Crime, 2003. Disponible:http://www.saiglobal.com/newsroom/tgs/2003-09/cyberforensics/cyberforensics.htm

[Acis06] Cano Martines Jeimy José. Introducción a la informática forense. Revista ACIS Junio de 2006 Disponible en: http://www.acis.org.co/fileadmin/Revista_96/dos.pdf