Cybercrime & Computer Forensics

SFS2. OBTAIN, EVALUATE, AND COMMUNICATE INFORMATION ON VARIOUS SCIENTIFIC TECHNIQUES TO ANALYZE PHYSICAL, TRACE, AND DIGITAL EVIDENCE.

D. ANALYZE AND INTERPRET DATA TO EVALUATE DIGITAL SOURCES OF EVIDENCE.

Computer Forensics Introduction

Computer forensics

Hardware is the physical material that creates a computer

Software are the programs and applications that carry out a set of instructions on the hardware

- The acquisition, extraction, preservation, and interpretation of computer data
- Includes many devices that are capable of storing data

Elements of Hardware

Computer Case/Chassis

- Central Processing Unit (CPU)
- Power Supply
- Motherboard
- Read Only Memory (ROM)
- Random Access Memory (RAM)
- System Bus
- Hard Disk Drive (HDD)

Input Devices

- Mouse
- Keyboard
- Scanner
- Joy Stick

Output Devices

- Monitor
- Speakers
- Printer

Data Storage and Retrieval

- Examiners must be familiar with the file system they are examining
- Evidence may be found in various computer locations and formats
- There are two categories for data-related evidence:
  - Visible data
  - Latent data
- The formatting process initializes portions of the hard drive so that it can store data, and it creates the structure of the file system

Data Storage and Retrieval

- Different operating systems map out (partition) HDDs in different manners
- RAM
- Sector – the smallest unit of data addressable by a hard disk drive, generally consisting of 512 bytes (Saferstein, 2009)
- Cluster – a group of sectors in multiples of two, typically the minimum space allocated in a file (Saferstein, 2009)

Processing the Computerized Crime Scene

- Similar to processing a traditional crime scene (i.e. warrants, documentation, investigation techniques)
- Documentation is a significant component in the computerized crime scene
    - The scene should be initially documented in as much detail as possible before any evidence is moved and examined
    - Crime scene documentation is accomplished through two actions:
        - Sketching
        - Photographing

Processing the Computerized Crime Scene

- After documentation is complete, a label should be placed on the cord of each peripheral, with a corresponding label placed on the port to which it is connected
- At a computerized crime scene most, if not all of the equipment will be seized, but before the peripherals are disconnected from the computer, a decision must be made about whether or not a live acquisition of the data is necessary (i.e. shutdown or unplug the computer)

Forensic Image Acquisition

- After the crime scene has been processed, the computer needs to be analyzed
- All electronic devices will be processed in the same manner
- The examination process that the forensic investigator uses on the computer must be intrusive
- All evidence (data) must be obtained without altering or destroying it

Forensic Image Acquisition

- Because booting a HDD to its operating system changes many files and could destroy evidentiary data, the data is generally obtained by removing the HDD from the system and placing it in a laboratory forensic computer so that a forensic image can be created
- Occasionally, in cases with specialized or unique equipment/systems the image of the HDD must be obtained by using the seized computer
- The examiner must be able to extract all forensic data/images and cause no changes to the HDD

Forensic Image Acquisition

A signature or fingerprint of the drive is taken before and after imaging

- This fingerprint is created by using a Message Digest 5 (MD5), a Secure Hash Algorithm (SHA) or a similarly validated algorithm
- Before imaging the drive the algorithm is run and a 32-character alphanumeric string is produced based on the drive’s contents
- The same algorithm is then run against the created forensic image which will result in the same alphanumeric string if none of the original content is changed

Visible Data

- Data from a computer that is openly visible and easily available to users
- Can encompass (from an evidentiary standpoint) any type of user-created data like
  - Word processing documents
  - Spreadsheets
  - Accounting records
  - Databases
  - Pictures

Visible Data

- Advances in printer technology have made high quality color printing affordable and common, which creates criminal opportunities
  - Counterfeiting
  - Check Fraud
  - Document Fraud

Visible Data

- Most criminal cases involving computers relate to financial investigations (or white collar crimes) which require any data related to personal and business finance
- Investigators must become familiar with the various computer applications that are used for criminal activities
- The ability to recognize the data produced by these applications and to display the images is essential to identifying the evidence

Temporary Files

- Can be valuable as evidence
- Can sometimes be recovered during a forensic examination including some of the data that may have been altered from a previous version
- Can be recovered when created through unsaved means (such as a computer being shut off manually)
- Most programs automatically save a temporary copy of the file in progress
- After working on a file or document, the user can save the changes, which promotes the temporary copy to a saved (or actual) file

Temporary Files

- Another type of temporary file valuable to the computer investigator is the printer spool
  - When a print job is sent to the printer a spooling process delays the sending of the data so the application can continue to work while the printing takes place in the background
  - When the print job occurs, a temporary print spool file is created
  - This file contains a copy of all of the data from the printer

Latent Data

- The areas of files and disks that are typically not apparent to the computer user (and often not to the operating system), but contain data nonetheless (Saferstein, 2009); the data which the operating system has hidden
- One of the reasons a forensic image of the media is created is because a standard copy only captures the logical data (that which the operating system is aware)
- Can be evidentiary data

Latent Data

Includes the data in the

- Swap space (used to conserve the valuable RAM within the computer system)
- RAM slack – the area from the end of the logical file to the end of the sector
- File slack – the remaining area from the end of the final sector containing data to the end of the cluster
- Unallocated space – the space on a hard drive that contains available space; the space may also contain temporary and deleted files

Defragmenting/Swap File/Swap Space

- Defragmenting a HDD involves reconnecting noncontiguous data
- The HDD has minimum space reservation requirements (i.e. a file might require 100 bytes of space, but the operating system allocates much more)
- If a file grows past the allocated amount, another cluster is required

Defragmenting/Swap File/Swap Space

- Fragmentation of numerous files can degrade the performance of an HDD, causing the read/write heads to have to traverse the platters to locate the data
- The constant read and write operations of RAM cause a constant change in the swap file or swap space

Defragmenting/Swap File/Swap Space

- If a different file occupies the next cluster, the operating system must find another place for the first file on the drive
- The file is said to be fragmented because data for the same file is contained in noncontiguous clusters
- The constant shuffling of data through deletion, defragmentation, swapping, etc., is one of the ways data is orphaned in latent areas

Deleted Files

- Another source of latent data to be examined by forensic investigators
- The actions that occur when a file is deleted vary among file systems
- When a user deletes files, the data typically remains behind
- When files in a Recycle Bin are deleted, the data remains there as well, until it is overwritten
- Data will remain in the computer even though attempts are made to delete it

The Internet

- A computer network that provides information globally (also called the “information superhighway”)
- Can be considered a series of networks
- Each computer that connects to the Internet has a unique numerical Internet Provider (IP) address and usually a name
- Includes various methods of connection
  - Wireless (Wi-Fi)
  - Wire
    - Modem
    - Cable lines or DSL telephone lines
- Affects all subjects and professions including law enforcement and security services

The World Wide Web

- The most popular area of the Internet
- Considered a depository of information stored in the computers connected to the Internet across the world
- Web browsers allow the user to search all the information available on the web and retrieve any web pages the viewer wishes to explore

The World Wide Web

- Commercial Internet service providers connect computers to the Internet while offering the user an array of options
- Keywords or phrases entered into a search engine will locate sites on the Internet that are relevant to that subject
- Several directories and indexes on the Internet, known as search engines, are available to assist the user in locating a particular topic from the hundreds of thousands of web sites located on the Internet

Electronic mail (e-mail)

- Carries messages across the world in a matter of seconds
- The service most commonly used in conjunction with the Internet

Internet Crimes

- Cybercriminals feel safe committing crimes in a “comfort zone” and often from the privacy of their own homes
- There are more cybercriminals than available law enforcement agents
- Law enforcement faces new challenges with Internet crimes
    - Internet crimes span multiple jurisdictions
    - There is a need to retrofit new crimes to existing laws
    - Most law enforcement officers are not trained in the technologies

Internet Crimes

Computers are used to commit a variety of crimes

- Computer viruses and spam
- Child pornography
- Identity theft
- Industrial espionage
- Fraud
- Gambling
- Harassment
- Piracy

Internet Crimes

There are numerous methods and techniques criminals use to hide their crimes and evidence, which include

- Using WI-FI networks and cyber cafes to cover tracks
- Password protection
- Hiding files with encryption
- Deleting files and emails
- Embedding information in unrelated files

Internet Crimes

The task of forensic investigators includes

- Tracking criminals through the digital trail — IP addresses, to ISPs, to the offender
- Restoring deleted files and emails
- Finding the hidden files through complex password encryption programs and searching techniques

Resources

- Investigator/Officer’s Personal Experience
- Introduction to Private Security: Theory Meets Practice, Cliff Roberson and Michael L. Birzer, Prentice Hall, 2009
- Forensic Science: From the Crime Scene to the Crime Lab, Richard Saferstein, Prentice Hall, 2008
- Introduction to Security, Robert J. Fischer and Gion Green, Butterworth-Heinemann, 2008