Computer Forensic
Evidence Collection and Management

Chapter 6

Investigative Tools, Technical Training, and Forensic Equipment

Chapter Objectives

- Identify the specialized tools and supplies required for electronic and computer forensic investigation
- Describe the various techniques employed for identifying and collecting electronic forensic evidence
- Identify training requirements for electronic forensic investigators and examiners
- Explain the use of software in computer network administration and surveillance
- Look at resources that provide for surveillance and capture of network traffic

Introduction

- Special tools, equipment, and software are required to collect computer and electronic evidence. Advances in technology have increased the complexity of forensic investigations involving the latest devices. Different types of packaging are required fore media storage devices and wireless communication devices to preserve the evidence.
- New tools and techniques for identifying, collecting, preserving, transporting, and storing computer and electronic evidence are required.
- Hardware and software solutions are available for the identification and capture of potential electronic forensic evidence
- First responders, computer forensic examiners, and investigators must receive training involving the use of the new forensic tools and must also become adept at technology testimony in courtrooms environment.

Forensic Investigation Requirements

- A wide variety of tools, including specialized equipment, computer hardware and software, are required in investigations that involve evidence retrieved from incident scenes where electronic devices are present. These investigative tools are in addition to those that are required for any incident scene investigation.
- A number of commercial vendors provide tools that can be used in computer and electronic investigations and examinations. Product and service categories include the following:
  - Disk manipulations, formatting, partitioning
  - Data recovery specialists
  - Disk/text/hex editing
  - General purpose software: a variety of uses
  - Graphic viewers and processing
  - Hashing –CRC, SHA, MD calculations
  - Linux(*UX tools)
  - Windows administrative tools.
- Common crime-scene supplies must also be included in any first-responder kit.

Forensic Investigation Requirements (Cont.)

Tool Kit

- Specialty took kits will be required for the forensic examiner to successfully investigate a computer or electronic use. Crime-scene responders and examiners usually posses kits for collection, storage, and transportation of evidence; however, they do not fulfill the requirements for computer and electronic evidence.

Specialty tool kit might contain instruments to open a computer case to retrieve a hard drive including screwdrivers, pliers, and a flashlight.
The Black box took kits contains also every conceivable tool for accessing computer and electronic devices. Documentation aids would include cable tags, indelible felt-tip, markers, and stick-on labels.
A kit for disassembly and removal of evidence would contain the following nonmagnetic tools:

Flat blade and Phillips screwdrivers
Specialized computer case screwdrivers
Hex-nut drivers
Needle-nose pliers
Secure-bit drivers
Small tweezers
Torque drivers
Standard pliers
Star-nut drivers
Wire cutters
Bolt cutters
Hammer

The Paraben forensic tool kit might contain documentation aids, disassembly and removal tools, package and transport supplies, and miscellaneous items.

Forensic Investigation Requirements (Cont.)

- Obtaining the evidence is only the first step in the evidence procurement cycle. If the evidence is not protected, it will be useless in court proceedings. Computer and electronic components can be rendered useless by faulty handling. Packing and transportation supplies include the following items:
  - Antistatic bag
  - Faraday bags
  - Antistatic bubble wrap
  - Evidence boxes
  - Evidence tape/seals
  - Crime-scene tape
  - Packing material such as Styrofoam and Styrofoam peanuts
  - Evidence bags
  - Packing tape
  - Sturdy boxes of various size
- A collection of items that support the evidence collection effort include the following:
  - Antistatic gloves
  - Large rubber bands
  - Magnifying glass
  - Seizure disks of various capacities
  - Flashlight
  - Floppy disks
  - Printer paper
  - Hand truck
  - Power strip
  - Extension cord
- Experience will indicate the types of tools that the forensic examiner will require at the crime scene or incident site. Each investigation team would also possess a laptop computer and camera.

Forensic Investigation Requirements (Cont.)

- Obtaining the evidence is only the first step in the evidence procurement cycle. If the evidence is not protected, it will be useless in court proceedings. Computer and electronic components can be rendered useless by faulty handling. Packing and transportation supplies include the following items:
  - Antistatic bag
  - Faraday bags
  - Antistatic bubble wrap
  - Evidence boxes
  - Evidence tape/seals
  - Crime-scene tape
  - Packing material such as Styrofoam and Styrofoam peanuts
  - Evidence bags
  - Packing tape
  - Sturdy boxes of various size
- A collection of items that support the evidence collection effort include the following:
  - Antistatic gloves
  - Large rubber bands
  - Magnifying glass
  - Seizure disks of various capacities
  - Flashlight
  - Floppy disks
  - Printer paper
  - Hand truck
  - Power strip
  - Extension cord
- Experience will indicate the types of tools that the forensic examiner will require at the crime scene or incident site. Each investigation team would also possess a laptop computer and camera.

Forensic Investigation Requirements (Cont.)

Forensic Workstation

- Desktop and laptop computers can be utilized as forensic workstation. If any electronic forensic examinations are to be conducted at the incident scenes, the laptop solution will probably be required, unless the organization has a mobile forensic lab.
- Desktop computers will be the most appropriate solution for a forensic lab settings. Configurations for these workstations are almost endless and usually depend on the budge of the department. These devices must function properly with the software and hardware products that are selected for both computer and electronic forensic investigations.
- Several vendors offer software products that have been used successfully in computer forensic investigations. Additionally, a number of special interface cables are required for attaching to hard drives and other computer media storage devices.
- Software forensic tools must comply with industry and court standards, so that evidence obtained is admissible in court.

Forensic Software

Numerous software products are available for the forensic examiner. These products would usually be loaded on a laptop computer specifically dedicated to computer forensic investigation.
Number of software products and systems provide for network administration, surveillance, imaging, analyses, carving, pattern matching, and other forensic evidence.

Computer Forensic Products

- A brief description is provided for a number of acceptable forensic software products. These includes:
  - **X-waysForensic**, by X-Ways Software, is an advanced computer examination and data recovery software product that is used by computer investigative specialist in private enterprise and law enforcement.
  - **Encase**, by Guidance Software, offers an industry standard in computer forensic investigation technology. This product provides investigators with a single tool, capable of conducting large-scale and complex investigations from beginning to end.
  - **The Forensic Toolkit (FTK**), by Access Data, provides a toll for complete and thorough forensic examinations. FTK has full text indexing, advanced searching, deleted file recovery, data-carving, e-mail and graphics analysis, and other advanced features.
  - **Ilook** is an all-in-one computer forensic suite currently maintained by the Internal Revenue Services (IRS). It is available free of charge to law enforcement agencies and certain U.S government agencies. Ilook is not available to the general public. The suite consists of the Ilook External Imager, an analysis program, and a few utilities. IXimager is a Linux-based custom boot CD that produces forensic grade compressed output

Forensic Software (Cont.)

Computer and Electronic Forensic Utilities and Programs

- Digital intelligence has created several forensic software tools in-house specifically for forensic use. These tools include DriveSpy, PDBlock, and PDWipe
- DriveSpy uses familiar DOS commands (CD, DIR, etc) to navigate the system under investigation, extend the capabilities of the associated DOS commands or adds new commands as necessary, and provides a familiar DOS-like prompt during system navigation.
- DriveSpy processes operate on the following components:
  - Large hard drives (greater than 8.4 gigabytes)
  - Floppy disks and removable media
  - FAT12/16/16x/32/32x partitions
  - Hard drives without partitions (removable media)
  - Hidden DOS partitions (full functionality)
  - Non-Dos partitions (physically)
  - Long file names (fully decoded and listed)
  - File creation (Win95/98), modification (DOS), and access dates (Win95/98)
  - Erased files (with their companion long file name, if one exists)
  - Slack space
  - Unallocated space
- With operating systems becoming more and more complex, it is increasingly difficult to protect fragile computer evidence.

Computer Media Recovery

- Computer data recovery requires knowledge of the Microsoft file allocation table (FAT) file system.FAT consists of a table an operating system maintains on the hard disk. It provides a map of the clusters where a file has been stored.
- Issues concerning the FAT file system could include:
  - Events that occur when a file is deleted
  - Long file name or short file name usage
  - Time stamp (time and date) issues when a file is moved or copied
  - Differences if file properties when it is removed from one directory on a logical volume to another on the same volume versus moving it from on logical volume on a physical disk to a different logical volume on the same physical disk.
  - Physical versus logical volume details
  - File creation information and properties
  - Data that can be recovered after a file has been deleted
  - Microsoft Windows “recycle bin” usage.

MD5 Algorithm

- Message digest-5 (MD5) is a hashing algorithm that is used to verify data integrity through the creation of a 128- bit message digest from data input. This message may be of any length and is claimed to be as unique to that specific data as a fingerprint is to the specific individual
- The repeatability requirement of digital evidence relies on MD5 algorithm to prove the integrity of imaged hard-disk drives.

Computer Media Recovery (Cont.)

SHA Algorithm

- The secure hash algorithm (SHA) family is a set of related cryptographic hash functions. The most commonly used function in the family, SHA-1 is employed in a large variety of popular security applications and protocols, including TLS, SSL, PGP, SSH, S/MIME, and IPSec.
- SHA-1 creates a 256-bit message digest versus the 128-bit message digest of MD5

CRC Algorithm

- The cyclic redundancy check (CRC) is a mathematical algorithm that translates a file into a unique hexadecimal code. A DRC is a type of checksum.
- The idea is that the file changes, the checksum will change. CRC checksums are usually used to detect radon, uncorrelated changes in files; therefore, they are useful in ensuring reproducibility when imaging hard-disk drives.

Forensic Hardware Devices

- A number of hardware devices are available that are specifically designated for both proactive and reactive electronic investigations. These devices might include the proactive and reactive electronic investigations. These devices might include the ability to copy an image from a computer hard drive or collect data and information via some electronic surveillance monitor.

Imaging

- Ghost imaging is the copying of the contents of a computer's hard disk into a single compressed file or set of files (referred to as an image). This allows the contents of the hard disk, including configuration files and applications, to be copied to the hard disk of other computer or onto an optical disk fore temporary storage.
- Examinations must not be conducted on original disk media because the data cold be compromised and are therefore not useful in legal proceedings.
- The portable image can then be used to setup each hard disk in other computers. Automatically formatting and partitioning each target disk. Ghost imaging is useful where one systm is to be replicated on a number of computes in a classroom or for a team of notebook computer users who all need the same system and application.
- The forensic usage of imaging is to preserve the original disk contents without making any modifications.

Disk Imaging Devices

Surveillance Equipment

- Investigators often require surveillance or eavesdropping devices for collecting evidence to identify criminal activities or violations of corporate security policies.

Snooping

- Snooping, in a security context, is unauthorized access to another person's or company's data. The practice is similar to eavesdropping, but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing.
- Malicious hackers (crackers frequently use snooping techniques and equipment such as key loggers to monitor keystrokes, capture passwords and login information.
- Corporations sometimes snoop on employees legitimately to monitor their use of business computers and track Internet usage; governments may snoop on individual to collect information and avert crime and terrorism.

Sniffing

- In common industry usage, a sniffer is a program that monitors and analyzes network traffic, detecting bottlenecks and problems. Using this information, a network manager can keep traffic flowing efficiently.
- A sniffer can also be used legitimately or illegitimately to capture data being transmitted on a network.
- A network router also reads every packet of data passed to it, determining whether it is intended for a destination within the router's own network or whether it should be passed further along the Internet.

Surveillance Equipment (Cont.)

Probing

- In telecommunications generally, a probe is an action taken or an object used for the purpose of learning something about the state of the network. A probe is a program or other device inserted at a key juncture in a network for the purpose of monitoring or collecting data about network activity.
- Probes can be used in conjunction with network surveillance system to capture digital data. Hackers use various techniques to constantly probe networks for vulnerabilities.

Network Security Management

- A basic knowledge of computers networks is a prerequisite to understanding the principles of network security. Primarily the network configurations would include the Internet, a local area network (LAN), an intranet, and or/ an extranet.
- There are a number of threats that managers and administrators of computer networks will need to confront.
- Computer network investigation usually occur in the realm of corporate network security administrators. Most of these incidents will involve improper use of corporate network facilities and resources, violations of computer-use policies, or violation of a corporate security policy.
- With the advent of the Internet and Web-based E-0commerce, the network has become a vehicle for numerous illegal activities.
- Network management and surveillance can be accomplished by utilizing dedicated devices, by host computers on the network, by people , or by some combination of all. The network functions in order are:
  - *Monitoring*
  - *Control*
  - *Troubleshooting*
  - *Statistical reporting*
- These function assume the role of the network watchdog, boss, diagnostician, and statistician. All of these functions are closely interrelated, and often, many of them are performed on the same device.

Network Management Tools

- The primary network management surveillance systems and network management products and services available include:

NetView

- IBM Tivoli NetView ensures the availability of critical business systems and provides rapid resolution of problems. It discovers TCP/IP networks, display network topologies, correlates and manages events and SNMP traps, monitors network heath, and gathers performance data.
- Functions provided by NetView:
  - *Allow the user to quickly identify the root cause of network failures*
  - *Builds collections for management of critical business systems*
  - *Integrates with leading networking vendors*
  - *Maintains device inventory of asset management*
  - *Measures availability and provides fault isolation for problem control and management*
  - *Reports on network trends and analysis.*

OpenView

- HP OpenView is a suite of business computer management or “E-services” programs from HP
- *An HP customer’s IT professionals can use OpenView to manage applications, device availability, network conditions and status, system performance, service and program maintenance, and storage resources.*

Network Management Tools (Cont.)

SunNet Manager

- Solstice SunNet Manager is a comprehensive set of tools and services that is used to perform fundamental tasks in managing a network. SunNet Manager is also an extensible platform that allows for the development of network management applications.
- SunNet Manager provides additional tools for viewing and analyzing returned data: the Results Browser allows the user to analyze data that has been stored to a disk file, while the software allows for a graphical representation of either incoming data or stored data.

RMON

- RMON (Remote Network Monitoring) provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed LANs and interconnecting network circuits from a central site.
- RMON can be supported by hardware monitoring devices, called “probes” or through software or some combination.
- RMON collects nine kinds of information, including packets sent, bytes sent, packet dropped, statistics by host, by conversation between two sets of addresses, and certain kinds of events that have occurred.
- A network administrator can find out how much bandwidth or traffic each user is imposing on the network and what Web sites are being accessed. Alarms can be set in order to be aware of impeding problems.

Network Forensic

- Network forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents. Network forensics systems consist of active and passive systems.
- Online systems include those in which all packets passing through a network traffic point are captured and written to storage with analysis being done subsequently in batch mode. Since all traffic is recorded, much of it may be irrelevant to the investigation. This approach requires large amounts of storage, usually involving a RAID system
- Real-time systems involve those in which each packet is analyzed in a rudimentary way in memory and only certain information is saved for future analysis. This approach requires less storage but may require a faster processor to keep up with incoming traffic.
- One concern with the passive approach is one of privacy because all packets information (including user data) is captured.
- Network forensic application include the capturing and analyzing of network communications using the following techniques:
  - *Capturing and analyzing wireless communications*
  - *Building low-cost wireless forensics platforms utilizing high-powered wireless cards and open-source software*
  - *Determining whether volatile data on live systems may be of interest and how to extract that data in a forensically sound manner*
  - *Dumping the contents of RAM*
  - *Exporting metadata regarding running processes an network connections*
  - *Working with encrypted storage volumes*
  - *Creating effective reports that educate and impress*
  - *Importing data into litigation management software*

Computer Forensic Training

- The investigator must be trained in the proper use of various imaging utilities available to the computer examiner. Knowledge of verification methodologies and the testing of forensic tools is required.
- In many cases, investigators are limited by media size, purpose, scope of warrant, or consent, and cannot remove the media from the scene.

Training Requirements

- Forensic investigators and examiners must understand the concepts, techniques, and tools providing a solid foundation in concepts related to the investigation, preservation, and processing of computer-based evidence
- Specific technical training can be divided into three categories:
- **Hardware**

  PC hardware, processors, memory, motherboard, hard/floppy/removable drives, physical and logical characteristics of hard and floppy drives, IDE and SCSI channel configuration guidelines
- **Software**

  Computer data, Bits and bites, hexadecimal and binary, ASCII, Norton's DiskEdit and DriveSpy, Mater boot record, partitions and file systems, partition tables, boot records, boot-up sequence of a Dos-based computer, operating systems, FAT-13/FAT-16/FAT-32, Time and date stamps (access, modification, creation), Long/short files names, MS-SOS command line review, understanding file types and files headers.
- **Procedural**

  Computer and electronic crime fundamentals, evidence collection, packaging, and storage considerations, media imaging-copying hard drives, disks, multimedia cards, etc, cell phone evidence, recovering deleted files, keyword searching, data compression, data encryption, potential evidence in MS Windows, hidden media, creating a forensic boot floppy.

Computer Forensic Training (Cont.)

Training Providers

- Training and educational programs are available for various levels and categories of criminal justicee.
- Some provides of forensic tools also provide for compute forensic training.

Specialized Training

- First responders and investigations require special skills to successfully process any evidence that might be present at an indecent scene.
- The duties, assignments, and procedures vary from departments and agencies regarding the investigators to technicians; therefore, the job description may very depending on geographic locations.
- Most of the experience to become proficient will be gained in an on-the-job phase of employment. Most departments also offer their employees an opportunity fore peach officers standards and training. Most of the POST employee educational classes for the crime-scene investigator would be specific classes geared to crime-homicide, and death scene investigation.

Computer Forensic Training (Cont.)

Forensic Investigations Training

- The rate of identity theft, fraud, abuse, and criminal activity on computer systems is reaching alarming rates. Violations of corporate security policies and computer-use policies are commonplace.
- Specific subject relating to computer and electronic forensic investigations include:
  - *Overview of computer crime*
  - *Computer forensics training with open-source tools*
  - *Preparing sterile examination media*
  - *Acquisition, collection, and seizure of magnetic media*
  - *Issues when presenting data in court*
  - *Documenting a "chain of custody"*
  - *The marking, storage, and transmittal of evidence*
  - *Investigating data streams*
  - *File storage dates and times*
  - *File deletion/recovery*
  - *Preservation and safe handling of original media*
  - *Recovering deleted data form a cell phone*
  - *Digital camera evidence*
  - *Recovering Internet usage data*
  - *Recovering swap files/temporary files/cache files*
  - *Making bit-stream copies of original media*
  - *Others*

Support Organizations

- Organizations engaged in forensics investigations can find support from a number of agencies.
- *The mission of National White Collar Crime (NW3C) is to provide a nationwide support system for agencies involved in the prevention, investigation, and prosecution of economic and high-tech crimes and to support and partner with other appropriate entities in addressing homeland security initiatives, as they relate to economic and high-tech crimes.*
- *The Department of Justice (DOJ) and other agencies are continually working to better prevent compute crimes and enforce existing laws concerning computer crime.*