Chapter 1
Computer Forensics and Investigations as a Profession

Objectives

• Understand computer forensics
• Prepare for computer investigations
• Understand enforcement agency investigations
• Understand corporate investigations
• Maintain professional conduct

Understanding Computer Forensics

• Computer forensics involves obtaining and analyzing digital information for use as evidence in civil, criminal, or administrative cases
• The Fourth Amendment to the U.S. Constitution protects everyone’s rights to be secure in their person, residence, and property from search and seizure
• As case law is evolving, search warrants may not be required
Understanding Computer Forensics (continued)

• When preparing to search for evidence in a criminal case, include the suspect’s computer and its components in the search warrant.

Computer Forensics Versus Other Related Disciplines

• Involves scientifically examining and analyzing data from computer storage media so that the data can be used as evidence in court.

• Investigating computers includes:
  – Securely collecting computer data
  – Examining suspect data to determine details such as origin and content
  – Presenting computer-based information to courts
  – Applying laws to computer practice

Computer Forensics Versus Other Related Disciplines (continued)

• Network forensics uses log files to determine:
  – When users logged on or last used their logon IDs
  – Which URLs a user accessed
  – How he or she logged on to the network
  – From what location

• Computer investigations functions
  – Vulnerability assessment and risk management
  – Network intrusion detection and incident response
  – Computer investigations
Computer Forensics Versus Other Related Disciplines (continued)

• Vulnerability assessment and risk management
  – Test and verify the integrity of standalone workstations and network servers
  – Physical security of systems and the security of operating systems (OSs) and applications
  – Test for known vulnerabilities of OSs
  – Launch attacks on the network, workstations, and servers to assess vulnerabilities

Computer Forensics Versus Other Related Disciplines (continued)

• Network intrusion detection and incident response functions:
  – Detect intruder attacks using automated tools and monitoring network firewall logs manually
  – Track, locate, and identify the intruder and deny further access to the network
  – Collect evidence for civil or criminal litigation against the intruders
Computer Forensics Versus Other Related Disciplines (continued)

- Computer investigation functions
  - Manage investigations and conduct forensic analysis of systems
  - Draw on resources from those involved in vulnerability assessment, risk management, and network intrusion detection and incident response
  - Resolve or terminate all case investigations

A Brief History of Computer Forensics

- Well-known crimes—one-half cent (aka salami slicing)
- By the early 1990s, specialized tools for computer forensics were available
- ASR Data created the tool Expert Witness for the Macintosh
  - Recover deleted files and file fragments
- EnCase
- iLook

Developing Computer Forensics Resources

- Some sources of help
  - Computer Technology Investigators Network (CTIN) http://www.ctin.org
  - High Technology Crime Investigation Association (HTCIA) http://www.htcia.org
  - DOD Cyber Crime Center http://www.dc3.mil
Preparing For Computer Investigations

- Computer investigations and forensics
- Public investigations
  - Government agencies responsible for criminal investigations and prosecution

(continued)

- Private or corporate investigations
  - Criminal cases
  - Government agencies
  - Private or corporate investigations
  - Private companies
  - Non-enforcement government agencies
  - Lawyers

(continued)

- Government agencies responsible for criminal investigations and prosecution
- Private or corporate investigations
- Non-enforcement government agencies
- Lawyers
Understanding Enforcement Agency Investigations

• Understand:
  – Local city, county, state or province, and federal laws on computer-related crimes
  – Legal processes and how to build a criminal case

Understanding Enforcement Agency Investigations (continued)

• States have added specific language to their criminal codes to define crimes that involve computers
• Until 1993, laws defining computer crimes did not exist

Following the Legal Process

• A criminal case follows three stages:
  – Complaint
    • Someone files a complaint
  – Investigation
    • A specialist investigates the complaint
  – Prosecution
    • Prosecutor collects evidence and builds a case
Following the Legal Process (continued)

- Levels of law enforcement expertise:
  - Level 1 (street police officer)
    - Acquiring and seizing digital evidence
  - Level 2 (detective)
    - Managing high-tech investigations
    - Teaching the investigator what to ask for
    - Understanding computer terminology
    - What can and cannot be retrieved from digital evidence
  - Level 3: (computer forensics expert)
    - Specialist training in retrieving digital evidence

Guide to Computer Forensics and Investigations, 2e
Understanding Corporate Investigations

- Business must continue with minimal interruption from your investigation
- Corporate computer crimes:
  - E-mail harassment
  - Falsification of data
  - Gender and age discrimination
  - Embezzlement
  - Sabotage
  - Industrial espionage

Establishing Company Policies

- Company policies avoid litigation
- Policies provide:
  - Rules for using company computers and networks
  - Line of authority for internal investigations
    - Who has the legal right to initiate an investigation
    - Who can take possession of evidence
    - Who can have access to evidence

Displaying Warning Banners

- Avoid litigation by displaying a warning banner on computer screens
- A banner:
  - Informs user that the organization can inspect computer systems and network traffic at will
  - Voids right of privacy
  - Establishes authority to conduct an investigation
Displaying Warning Banners (continued)

- Types of warning banners:
  - For internal employee access (intranet Web page access)
  - External visitor accesses (Internet Web page access)

Examples of warning banners:
- Access to this system and network is restricted
- Use of this system and network is for official business only
- Systems and networks are subject to monitoring at any time by the owner
- Using this system implies consent to monitoring by the owner
- Unauthorized or illegal users of this system or network will be subject to discipline or prosecution
Displaying Warning Banners (continued)

• A for-profit organization banner
  – This system is the property of Company X
  – This system is for authorized use only
  – Unauthorized access is a violation of law and violators will be prosecuted
  – All activity, software, network traffic, and communications are subject to monitoring

Designating an Authorized Requester

• Establish a line of authority
• Specify an authorized requester who has the power to conduct investigations
• Groups who can request investigations:
  – Corporate Security Investigations
  – Corporate Ethics Office
  – Corporate Equal Employment Opportunity Office
  – Internal Auditing
  – The general counsel or legal department

Conducting Security Investigations

• Public investigations search for evidence to support criminal allegations
• Private investigations search for evidence to support allegations of abuse of a company’s assets and criminal complaints
Conducting Security Investigations (continued)

• Situations in the enterprise environment:
  – Abuse or misuse of corporate assets
  – E-mail abuse
  – Internet abuse

Conducting Security Investigations (continued)

• Employee abuse of computer privileges
  – Employee company startup
  – Porn site
  – Malicious e-mail
Distinguishing Personal and Company Property

- PDAs and personal notebook computers
- Employee hooks up his PDA device to his company computer
- Company gives PDA to employee as bonus

Maintaining Professional Conduct

- Professional conduct determines credibility
  - Ethics
  - Morals
  - Standards of behavior
  - Maintain objectivity and confidentiality
  - Enrich technical knowledge
  - Conduct with integrity

Maintaining Professional Conduct (continued)

- Maintaining objectivity
  - Sustain unbiased opinions of your cases
- Avoid making conclusions about the findings until all reasonable leads have been exhausted
- Considered all the available facts
- Ignore external biases to maintain the integrity of the fact-finding in all investigations
- Keep the case confidential
Maintaining Professional Conduct (continued)

- Stay current with the latest technical changes in computer hardware and software, networking, and forensic tools
- Learn about the latest investigation techniques that can be applied to the case
- Record fact-finding methods in a journal
  - Include dates and important details that serve as memory triggers
  - Develop a routine of regularly reviewing the journal to keep past achievements fresh

Maintaining Professional Conduct (continued)

- Attend workshops, conferences, and vendor-specific courses conducted by software manufacturers
- Monitor the latest book releases and read as much as possible about computer investigations and forensics

Summary

- Computer forensics: systematic accumulation of digital evidence in an investigation
- Differs from network forensics, data recovery, and disaster recovery in scope, technique, and objective
- Laws relating to digital evidence were established in the late 1960s
- To be successful, you must be familiar with more than one computing platform
Summary (continued)

• To supplement your knowledge, develop and maintain contact with computer, network, and investigative professionals
• Public investigations typically require a search warrant before the digital evidence is seized
• The Fourth Amendment applies to governmental searches and seizures
• During public investigations, you search for evidence to support criminal allegations

Guide to Computer Forensics and Investigations, 2e

Summary (continued)

• During private investigations, search for evidence to support allegations of abuse of a company or person’s assets and, in some cases, criminal complaints
• Silver-platter doctrine: handing the results of private investigations over to the authorities because of indications of criminal activity
• Forensics investigators must maintain an impeccable reputation to protect credibility

Guide to Computer Forensics and Investigations, 2e

Summary (continued)

• Most information is stored on hard disks, floppy disks, and CD-ROMs in a nonvolatile manner
• Peripheral components (video adapter cards, sound cards, mice, keyboards, NICs) attach to mainboard via an expansion slot or port
• All peripherals must have a unique IRQ and I/O address to communicate with the processor
• Hardware information can be gathered from computer manuals, BIOS, or other OSs

Guide to Computer Forensics and Investigations, 2e