Chapter 14
Digital Forensics
Learning Objectives

- Describe the roles and responsibilities of the members of the digital forensic team
- Enumerate the key processes involved in collecting digital evidence
- Explain the difference between search and seizure in the public and private sectors
- Identify the goals of forensic analysis
Introduction

- Digital forensics: the use of sound investigation and analysis techniques to identify, collect, preserve and analyze electronic items of potential evidentiary value so that they may be admitted as evidence in a court of law or used to support administrative action.
- Applies to all modern electronic devices including computers, computer-based media, mobile phones, personal digital assistants (PDAs), portable music players, other electronic devices capable of storing digital information.
The Digital Forensic Team

- Type of digital forensic team depends on size and nature of the organization and available resources
- When setting out to plan for an organization’s commitment to forensic operations, consider the following:
  - Costs
  - Response time
  - Data sensitivity concerns
Many organizations divide the forensic functions as follows:

– First response: assess the “scene,” identifying sources of relevant digital information and preserving them for later analysis using sound processes

– Analysis and presentation: analyze collected information to identify material facts that bear on the subject of the investigation; prepare and present results of the analysis to support possible legal action
The First Response Team

- Size and makeup will vary but often includes the following roles:
  - Eyes: survey the scene and identify sources of relevant information; orchestrate team work
  - Fingers: under direction of eyes, fingers move things around, disassemble equipment, etc.
  - Scribe: produces written record of the team’s activities; maintains control of field evidence log and locker
  - Image the Geek: collects copies, or images, of digital evidence
The First Response Team (continued)

- Important part of site survey is prioritizing the sources of information

- Some considerations guiding this prioritization:
  - Value: likely usefulness of the information
  - Volatility: stability of the information over time; some types of information are lost when the power is cut, and others by default over time
  - Effort required: amount of time required to acquire a copy of the information
The Analysis Team

- Analysis and reporting phases are performed by persons specially trained in the use of forensic tools to analyze collected information and provide answers to questions that gave rise to the investigation.

- Forensic analysis function is sometimes broken into two parts:
  - Examination
  - Analysis
The Analysis Team (continued)

- Examination phase involves the use of forensic tools to recover deleted files and retrieve and characterize operating system artifacts and other relevant material.
- Analysis phase uses those materials to answer the questions that gave rise to the investigation.
- Analysis function is also responsible for reporting and presenting the investigation’s findings.
Digital Forensics Methodology

- Digital investigation begins with allegation of wrongdoing (policy violation, crime)
- Authorization then sought to begin investigation proper by collecting relevant evidence
- Public sector authorization may take the form of a search warrant; seizure of the relevant items containing the information
- Private sector authorization is specified by the organization’s policy; many use affidavit; more common to authorize the collection of images of digital information
Private organization wishing to search an employee’s computer must generally meet the following conditions:

- Employee made aware of organizational policy that search may occur
- Search must be justified at its inception
- Search must be permissible in its scope
- Organization has clear ownership over container that material was discovered in
- Search must be authorized by the responsible manager or administrator
Affidavits and Search Warrants (continued)

- Organization should have a reasonable degree of confidence in its right to search for and collect potentially evidentiary material
- Incident response policy must spell out the procedures for initiating investigative process
- Particularly critical in private sector, as private organizations do not enjoy the broad immunity accorded to law enforcement investigations
Acquiring the Evidence

- Digital evidence collection follows a four-step methodology:
  - Identify sources of evidentiary material
  - Authenticate the evidentiary material
  - Collect the evidentiary material
  - Maintain a documented chain of custody
Identifying Sources

- Data collection in suspect’s office may involve hundreds of gigabytes of data residing on:
  - Disks in a desktop or laptop computer (or both)
  - Disks in external storage enclosures
  - Memory sticks or cards
  - PDA (possibly with additional removable memory cards installed)
  - Cell phone (plus any memory cards installed in it)
  - Storage devices such as MP3 players
  - Optical storage such as CDs and DVDs
  - Networked storage
Identifying Sources (continued)

- When identifying evidence in a data center, the potential evidence sources multiply to include:
  - Disks attached to servers
  - Storage attached to a storage network such as a fibre channel or iSCSI SAN
  - Files on NAS (Network Attached Storage) devices
  - Logs on servers, routers, firewalls, or centralized logging servers
Authenticating Evidence

- One core concern is being able to demonstrate that the particular collection of bits being prepared is true and accurate copy of original
- One way to identify a particular digital item (collection of bits) is with a cryptographic hash
- When digital evidence is collected, its hash value is calculated and recorded
- At any subsequent point, the hash value can be recalculated to show that the item has not been modified since its collection
Collecting Evidence

- Many considerations and processes that surround digital evidence collection
- Investigator must decide upon:
  - Mode of acquisition
    - Live
    - Dead
  - How to package and image collected material
- Investigator must accurately and thoroughly document all activities undertaken
Live Acquisition

- Investigator cannot know what the attacker did to the system during the compromise.
- Investigator will typically use trusted set of tools from a CD (KNOPPIX-STD, F.I.R.E., Helix).
- Live acquisition typically uses scripts to automate process of running a series of tools and preserving their output.
Live Acquisition (continued)

- While usually thought of in context of a running server, the need to acquire the state of an active process arises in at least two other situations:
  - Logs
  - Active devices such as PDAs and cell phones
- “Snapshot forensics” captures a point-in-time picture of a process
- Investigator often works backwards to identify sources of evidence, making log records vital
- Critical to protect wireless devices from network accesses after seizure and during analysis
Packaging for Protection

- While any secure package will serve, use of packaging specifically designed for this purpose aids proper documentation and storage.
- Evidence envelope is preprinted with a form that collects relevant information for establishing where, by whom, and when information was collected.
- Evidence seal is designed for single use and is very difficult to remove without breaking it.
Dead Acquisition

- Computer typically powered off so its disk drives can be removed for imaging; information on the devices is static ("dead") and durable.
- While dead acquisition processes and procedures were developed for computer disks, they apply equally well to disk-like devices (thumb drives, memory cards, MP3 players, etc.).
- Forensic image of disk or device must include active files and directories as well as deleted files and file fragments.
To make sure potentially valuable information is acquired, forensic investigators use bit-stream (or sector-by-sector) copying when imaging.

Hardware tools, specialized for purpose of copying disks, are faster.

Disadvantages of hardware imaging platforms are cost and they support only certain interfaces.

Software imaging and other forensic tools are sold by many vendors and run on standard laptop or other system and support any disk interface supported by host.
The Imaging Process

- Before imaging a piece of disk media, origin and description (vendor, model, and serial number) documented in written and photographic form.

- General imaging process is:
  - Calculate and record a baseline cryptographic hash of the suspect media.
  - Perform a bit-stream image of the suspect media.
  - Calculate and record hash of target (and optional second hash to verify unmodified by imaging).
  - Compare the hashes to verify that they match.
  - Package the target media for transport.
Digital Photography

- Plays major role in documenting evidence
- Digital camera requires some preparation and sound process, as follows:
  - Sterilize digital photographic media (memory card)
  - Set camera’s clock to assure that dates/times recorded for digital photographs are accurate
  - Make photographic media “self documenting” by taking first exposure of a “Begin Digital Photography” marker
Digital Photography (continued)

- Ensure that DPM (Digital Photographic Media) number is identified in digital photography log as each photograph is taken
- At conclusion of onsite activities, make an “end of photography” exposure
- Remove card from camera, package it in static bag, and seal it in evidence envelope like any other piece of digital evidence
- Do not make hashes of digital photographs until first time evidence envelope is opened
Field Documentation

- Series of standard forms commonly used to document collection of evidence in the field
- Scene sketch: shows the general locations of items; only item that can be done in pencil
- Field activity log: documents activities of the team during evidence collection
- Field evidence log: identifies by filename number each item collected
- These forms are normally assembled into a case file; becomes permanent part of the documentary record of the investigation
The Field Forensic Kit

- As personal as the individual investigator
- The kit includes items such as: write blockers, extension cord and power strip, evidence envelopes and seals, photographic markers and scales, gloves (vinyl), security bits, tie-on labels, tool kit, assortment of screws, pens, permanent markers, ESD workstation and static strap, digital camera
Maintaining the Chain of Custody

- Legal record of where evidence was at each point in its lifetime and documentation of each and every access to it.
- Demonstrates evidence has been protected from accidental or purposeful modification at every point from its collection through analysis to presentation in court.
- Usually field investigator maintains personal custody of sealed item until logged into chain of custody book at evidence storage room.
- Each time item is removed, it is logged out.
Maintaining the Chain of Custody (continued)

- Collected evidence must be stored and handled appropriately to protect its value
- Proper storage requires protected, controlled access environment coupled with sound processes governing access to its contents
- Storage facility must maintain the proper environment for holding digital information:
  - Controlled temperature and humidity
  - Freedom from strong electrical and magnetic fields that might damage the items
  - Protection from fire and other physical hazards
Analyzing Evidence

- First step is to obtain evidence from the storage area and perform a physical authentication
- A copy of the evidence is made for analysis and the original is returned to storage
- Copy can then be authenticated by recomputing its hash and comparing it to the written record
- Disk images must be loaded into the particular forensic tool used by the organization
- Typically involves processing image into format used by the tool and performing preprocessing (undeleting files, data carving, etc.)
Analyzing Evidence (continued)

♦ Two major tools used in forensic analysis:
  – EnCase (Guidance Software)
    • Right-click menu functions
    • Supports EnScripts
  – Forensic Toolkit (Access Data)
    • Extensive preprocessing of evidence items
    • Organizes various items into a tabbed display

♦ Largely similar in function but take different approaches to the analysis task
Searching for Evidence

- Identifying relevant information is one of the more important analyst tasks
- FTK constructs an index of terms found in the image; results available under the Search tab
- FTK includes “Live Search” tab, which allows searching on user-specified terms
- Challenging to develop relevant search terms; a technique called cartwheeling can help
- EnCase offers flexible search interface; includes predefined filters for common items; as relevant items located, they are “bookmarked”
Reporting the Findings

- Findings must be reported in written and often verbal form; presentation or legal testimony
- Report must communicate findings clearly to various audiences that will use the report
- It is a temptation to prepare a series of reports
- Best to prepare a single report with an index to point parties to their particular area of interest
- Report should identify what gave rise to the investigation, sources of evidence that was analyzed, tools and processes used to analyze evidence, specific findings, and an interpretation
Interacting with Law Enforcement

- When incident violates civil or criminal law, it is the organization’s responsibility to notify the proper authorities.
- Selecting the appropriate law enforcement agency depends on type of crime committed.
- In general, if a crime crosses state lines, it becomes a federal matter.
- Local law enforcement agencies rarely have computer crimes task forces, but investigative units are capable of processing crime scenes and handling most common criminal violations.
Some advantages of involving law enforcement:

- Agencies are usually much better equipped at processing evidence than business organization.
- Company security forces may do more harm than good when attempting to extract information.
- Law enforcement agencies are prepared to handle warrants and subpoenas necessary when documenting a case.
- Agencies are adept at obtaining statements from witnesses, affidavits, and other required documents.
Some disadvantages of involving law enforcement:

– Possible loss of control of the chain of events following an incident
– Organization may not hear about case for weeks or even months because of heavy caseloads or resource shortages
– Tagging of equipment vital to business as evidence (assets removed, stored, preserved)

If organization detects criminal act, it has legal obligation to notify appropriate law enforcement
Anti-Forensics

- Forensic tools excel at retrieving information that has been deleted through normal means or resides in hidden places used by an OS.
- Recovery of deleted or hidden information can pose significant threat to privacy/confidentiality of an organization’s information assets.
- Organizations must be aware that forensic tools are available to everyone.
- Organizations must have policy and procedures to assure that discarded digital information is destroyed beyond forensic recovery.
Chapter Summary

- Computer forensics: the use of computer investigation and analysis techniques to identify, collect, preserve, and analyze electronic items of potential evidentiary value so that they may be admitted as evidence in a court of law, or used to support administrative action.

- Digital forensics applies to all modern electronic devices including mobile phones, personal digital assistants (PDAs), portable music players, and other electronic devices capable of storing digital information.
Chapter Summary (continued)

- Digital investigation begins with allegation of wrongdoing (policy violation or commission of a crime)
- Based on that allegation, authorization is sought to begin investigation by collecting relevant evidence
- Once authorization is obtained, the collection of evidence can begin
- First response digital forensics team secures and collects devices, media, or media images that are evidentiary
Analysis and reporting techniques performed by persons specially trained in use of forensic tools.

They analyze collected information and provide answers to questions that gave rise to the investigation.

To answer underlying questions that prompted the investigation, analyst must translate overall questions into series of specific questions answerable through forensic analysis and then use proper tools to determine answers to the detailed questions.
When incident violates civil or criminal law, it is organization’s responsibility to notify proper authorities and work with them throughout the investigation and resolution of the matter.

Forensic tools can be used by investigators to obtain information, even deleted information, from digital media.

This poses risks when such tools are used for non-legitimate purposes to obtain private or proprietary information from discarded digital media.