Guide to Computer Forensics and Investigations
Fourth Edition

Chapter 2
Understanding Computer Investigations

Objectives

- Explain how to prepare a computer investigation
- Apply a systematic approach to an investigation
- Describe procedures for corporate high-tech investigations
- Explain requirements for data recovery workstations and software
- Describe how to conduct an investigation
- Explain how to complete and critique a case

Preparing a Computer Investigation

Preparing a Computer Investigation

- Role of computer forensics professional is to gather evidence to prove that a suspect committed a crime or violated a company policy
- Collect evidence that can be offered in court or at a corporate inquiry
  - Investigate the suspect's computer
  - Preserve the evidence on a different computer

Preparing a Computer Investigation (continued)

- Follow an accepted procedure to prepare a case
- **Chain of custody**
  - Route the evidence takes from the time you find it until the case is closed or goes to court

An Overview of a Computer Crime

- Computers can contain information that helps law enforcement determine:
  - Chain of events leading to a crime
  - Evidence that can lead to a conviction
- Law enforcement officers should follow proper procedure when acquiring the evidence
  - Digital evidence can be easily altered by an overeager investigator
- Information on hard disks might be **password protected**

Examining a Computer Crime

Figure 2-1 The crime scene

An Overview of a Company Policy Violation

- Employees misusing resources can cost companies millions of dollars
- Misuse includes:
  - Surfing the Internet
  - Sending personal e-mails
  - Using company computers for personal tasks

Taking a Systematic Approach

Taking a Systematic Approach

- Steps for problem solving
  - Make an initial assessment about the type of case you are investigating
  - Determine a preliminary design or approach to the case
  - Create a detailed checklist
  - Determine the resources you need
  - Obtain and copy an evidence disk drive

Taking a Systematic Approach (continued)

- Steps for problem solving (continued)
  - Identify the risks
  - Mitigate or minimize the risks
  - Test the design
  - Analyze and recover the digital evidence
  - Investigate the data you recover
  - Complete the case report
  - Critique the case

Assessing the Case

- Systematically outline the case details
  - Situation
  - Nature of the case
  - Specifics of the case
  - Type of evidence
  - Operating system
  - Known disk format
  - Location of evidence

Assessing the Case (continued)

- Based on case details, you can determine the case requirements
  - Type of evidence
  - Computer forensics tools
  - Special operating systems

Planning Your Investigation

- A basic investigation plan should include the following activities:
  - Acquire the evidence
  - Complete an evidence form and establish a chain of custody
  - Transport the evidence to a computer forensics lab
  - Secure evidence in an **approved secure container**

Planning Your Investigation (continued)

- A basic investigation plan (continued):
  - Prepare a forensics workstation
  - Obtain the evidence from the secure container
  - Make a forensic copy of the evidence
  - Return the evidence to the secure container
  - Process the copied evidence with computer forensics tools

Planning Your Investigation (continued)

- An **evidence custody form** helps you document what has been done with the original evidence and its forensics copies

- Two types
  - **Single-evidence form**
    - Lists each piece of evidence on a separate page
  - **Multi-evidence form**

Planning Your Investigation (continued)

Corporation X		
Security Investigations		
This form is to be used for one to ten pieces of evidence		

Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

	Description of evidence:	Vendor Name	Model No./Serial No.
Item #1			
Item #2			
Item #3			
Item #4			
Item #5			
Item #6			
Item #7			
Item #8			
Item #9			
Item #10			

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Item #	Evidence Processed by	Disposition of Evidence	Date/Time
			Page __ of ___

Figure 2-2   A sample multi-evidence form used in a corporate environment

Planning Your Investigation (continued)

Metropolis Police Bureau				
High-tech Investigations Unit				
This form is to be used for only one piece of evidence.				
Fill out a separate form for each piece of evidence.				
Case No.:		Unit Number:		
Investigator:				
Nature of Case:				
Location where evidence was obtained:				

Item # ID	Description of evidence:	Vendor Name	Model No./Serial No.

		Date & Time:	
Evidence Recovered by:			
Evidence Placed in Locker:		Date & Time:	

Evidence Processed by	Disposition of Evidence	Date/Time
		Page __ of __

Figure 2-3 A single-evidence form

Securing Your Evidence

- Use **evidence bags** to secure and catalog the evidence
- Use computer safe products
  - Antistatic bags
  - Antistatic pads
- Use well padded containers
- Use evidence tape to seal all openings
  - Floppy disk or CD drives
  - Power supply electrical cord

Securing Your Evidence (continued)

- Write your initials on tape to prove that evidence has not been tampered with
- Consider computer specific temperature and humidity ranges

Procedures for Corporate High-Tech Investigations

Procedures for Corporate High-Tech Investigations

- Develop formal procedures and informal checklists
  - To cover all issues important to high-tech investigations

Employee Termination Cases

- Majority of investigative work for termination cases involves employee abuse of corporate assets

- Internet abuse investigations
  - To conduct an investigation you need:
    - Organization's Internet proxy server logs
    - Suspect computer's IP address
    - Suspect computer's disk drive
    - Your preferred computer forensics analysis tool

Employee Termination Cases (continued)

- Internet abuse investigations (continued)
  - Recommended steps
    - Use standard forensic analysis techniques and procedures
    - Use appropriate tools to extract all Web page URL information
    - Contact the network firewall administrator and request a proxy server log
    - Compare the data recovered from forensic analysis to the proxy server log
    - Continue analyzing the computer's disk drive data

Employee Termination Cases (continued)

- E-mail abuse investigations
  - To conduct an investigation you need:
    - An electronic copy of the offending e-mail that contains message header data
    - If available, e-mail server log records
    - For e-mail systems that store users' messages on a central server, access to the server
    - Access to the computer so that you can perform a forensic analysis on it
    - Your preferred computer forensics analysis tool

Employee Termination Cases (continued)

- E-mail abuse investigations (continued)
  - Recommended steps
    - Use the standard forensic analysis techniques
    - Obtain an electronic copy of the suspect's and victim's e-mail folder or data
    - For Web-based e-mail investigations, use tools such as FTK's Internet Keyword Search option to extract all related e-mail address information
    - Examine header data of all messages of interest to the investigation

Attorney-Client Privilege Investigations

- Under **attorney-client privilege (ACP)** rules for an attorney

  - You must keep all findings confidential

- Many attorneys like to have printouts of the data you have recovered

  - You need to persuade and educate many attorneys on how digital evidence can be viewed electronically

- You can also encounter problems if you find data in the form of binary files

Attorney-Client Privilege Investigations (continued)

- Steps for conducting an ACP case
  - Request a memorandum from the attorney directing you to start the investigation
  - Request a list of keywords of interest to the investigation
  - Initiate the investigation and analysis
  - For disk drive examinations, make two bit-stream images using different tools
  - Compare hash signatures on all files on the original and re-created disks

Attorney-Client Privilege Investigations (continued)

- Steps for conducting an ACP case (continued)
  - Methodically examine every portion of the disk drive and extract all data
  - Run keyword searches on allocated and unallocated disk space
  - For Windows OSs, use specialty tools to analyze and extract data from the Registry
    - AccessData Registry Viewer
  - For binary data files such as CAD drawings, locate the correct software product
  - For unallocated data recovery, use a tool that removes or replaces nonprintable data

Attorney-Client Privilege Investigations (continued)

- Steps for conducting an ACP case (continued)
  - Consolidate all recovered data from the evidence bit-stream image into folders and subfolders
- Other guidelines
  - Minimize written communications with the attorney
  - Any documentation written to the attorney must contain a header stating that it's "Privileged Legal Communication—Confidential Work Product"

Attorney-Client Privilege Investigations (continued)

- Other guidelines (continued)
  - Assist attorney and paralegal in analyzing the data
- If you have difficulty complying with the directions
  - Contact the attorney and explain the problem
- Always keep an open line of verbal communication
- If you're communicating via e-mail, use encryption

Media Leak Investigations

- In the corporate environment, controlling sensitive data can be difficult
- Consider the following for media leak investigations
  - Examine e-mail
  - Examine Internet message boards
  - Examine proxy server logs
  - Examine known suspects' workstations
  - Examine all company telephone records, looking for calls to the media

Media Leak Investigations (consider)

- Steps to take for media leaks
  - Interview management privately
    - To get a list of employees who have direct knowledge of the sensitive data
  - Identify media source that published the information
  - Review company phone records
  - Obtain a list of keywords related to the media leak
  - Perform keyword searches on proxy and e-mail servers

Media Leak Investigations (consider)

- Steps to take for media leaks (continued)
  - Discreetly conduct forensic disk acquisitions and analysis
  - From the forensic disk examinations, analyze all e-mail correspondence
    - And trace any sensitive messages to other people
  - Expand the discreet forensic disk acquisition and analysis
  - Consolidate and review your findings periodically
  - Routinely report findings to management

Industrial Espionage Investigations

- All suspected industrial espionage cases should be treated as criminal investigations

- Staff needed
  - Computing investigator who is responsible for disk forensic examinations
  - Technology specialist who is knowledgeable of the suspected compromised technical data
  - Network specialist who can perform log analysis and set up network sniffers
  - Threat assessment specialist (typically an attorney)

Industrial Espionage Investigations (continued)

- Guidelines
  - Determine whether this investigation involves a possible industrial espionage incident
  - Consult with corporate attorneys and upper management
  - Determine what information is needed to substantiate the allegation
  - Generate a list of keywords for disk forensics and sniffer monitoring
  - List and collect resources for the investigation

Industrial Espionage Investigations (continued)

- Guidelines (continued)
  - Determine goal and scope of the investigation
  - Initiate investigation after approval from management
- Planning considerations
  - Examine all e-mail of suspected employees
  - Search Internet newsgroups or message boards
  - Initiate physical surveillance
  - Examine facility physical access logs for sensitive areas

Industrial Espionage Investigations (continued)

- Planning considerations (continued)
  - Determine suspect location in relation to the vulnerable asset
  - Study the suspect's work habits
  - Collect all incoming and outgoing phone logs
- Steps
  - Gather all personnel assigned to the investigation and brief them on the plan
  - Gather resources to conduct the investigation

Industrial Espionage Investigations (continued)

- Steps (continued)
  - Place surveillance systems
  - Discreetly gather any additional evidence
  - Collect all log data from networks and e-mail servers
  - Report regularly to management and corporate attorneys
  - Review the investigation's scope with management and corporate attorneys

Interviews and Interrogations in High-Tech Investigations

- Becoming a skilled interviewer and interrogator can take many years of experience
- **Interview**
  - Usually conducted to collect information from a witness or suspect
    - About specific facts related to an investigation
- **Interrogation**
  - Trying to get a suspect to confess

Interviews and Interrogations in High-Tech Investigations (continued)

- Role as a computing investigator
  - To instruct the investigator conducting the interview on what questions to ask
    - And what the answers should be
- Ingredients for a successful interview or interrogation
  - Being patient throughout the session
  - Repeating or rephrasing questions to zero in on specific facts from a reluctant witness or suspect
  - Being tenacious

Understanding Data Recovery Workstations and Software

Understanding Data Recovery Workstations and Software

- Investigations are conducted on a computer forensics lab (or data-recovery lab)
- Computer forensics and data-recovery are related but different
- **Computer forensics workstation**
  - Specially configured personal computer
  - Loaded with additional bays and forensics software
- To avoid altering the evidence use:
  - Forensics boot floppy disk OR cd
  - Write-blocker devices

Write Blocker

- Connects a hard drive in trusted read-only mode
- There are also Linux boot CDs that mount all drives read-only, such as Helix and some Knoppix distributions

Setting Up your Computer for Computer Forensics

- Basic requirements
  - A workstation running Windows XP or Vista
  - A write-blocker device
  - Computer forensics acquisition tool
    - Like FTK Imager
  - Computer forensics analysis tool
    - Like FTK
  - Target drive to receive the source or suspect disk data
  - Spare PATA or SATA ports
  - USB ports

Setting Up your Computer for Computer Forensics (continued)

- Additional useful items
  - Network interface card (NIC)
  - Extra USB ports
  - FireWire 400/800 ports
  - SCSI card
  - Disk editor tool
  - Text editor tool
  - Graphics viewer program
  - Other specialized viewing tools

Conducting an Investigation

Conducting an Investigation

- Gather resources identified in investigation plan
- Items needed
  - Original storage media
  - Evidence custody form
  - Evidence container for the storage media
  - Bit-stream imaging tool
  - Forensic workstation to copy and examine your evidence
  - Securable evidence locker, cabinet, or safe

Gathering the Evidence

- Avoid damaging the evidence
- Steps
  - Meet the IT manager to interview him
  - Fill out the evidence form, have the IT manager sign
  - Place the evidence in a secure container
  - Complete the evidence custody form
  - Carry the evidence to the computer forensics lab
  - Create forensics copies (if possible)
  - Secure evidence by locking the container

Understanding Bit-Stream Copies

- **Bit-stream copy**
  - Bit-by-bit copy of the original storage medium
  - Exact copy of the original disk
  - Different from a simple backup copy
    - Backup software only copies known files (active data)
    - Backup software cannot copy deleted files, e-mail messages or recover file fragments
- **Bit-stream image**
  - File containing the bit-stream copy of all data on a disk or partition
  - Also known as **forensic copy**

Understanding Bit-stream Copies (continued)

- Copy image file to a target disk that matches the original disk's manufacturer, size and model
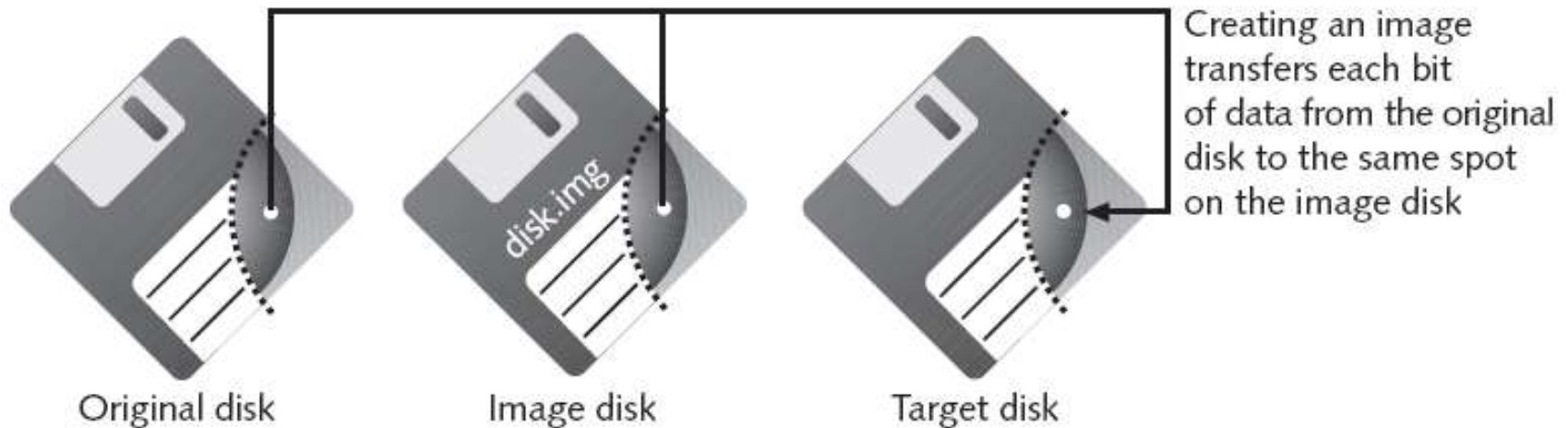

Creating an image transfers each bit of data from the original disk to the same spot on the image disk

Original disk   Image disk   Target disk

Figure 2-4 Transfer of data from original to image to target

Acquiring an Image of Evidence Media

- First rule of computer forensics
    - Preserve the original evidence
- Conduct your analysis only on a copy of the data

- We'll skip the ProDiscover section of the textbook, which is on pages 48-58

Completing the Case

Completing the Case

- You need to produce a final report
  - State what you did and what you found
- Include report generated by your forensic tool to document your work
- **Repeatable findings**
  - Repeat the steps and produce the same result, using different tools
- If required, use a report template
- Report should show conclusive evidence
  - Suspect did or did not commit a crime or violate a company policy

Critiquing the Case

- Ask yourself the following questions:
  - How could you improve your performance in the case?
  - Did you expect the results you found? Did the case develop in ways you did not expect?
  - Was the documentation as thorough as it could have been?
  - What feedback has been received from the requesting source?

Critiquing the Case (continued)

- Ask yourself the following questions (continued):
  - Did you discover any new problems? If so, what are they?
  - Did you use new techniques during the case or during research?