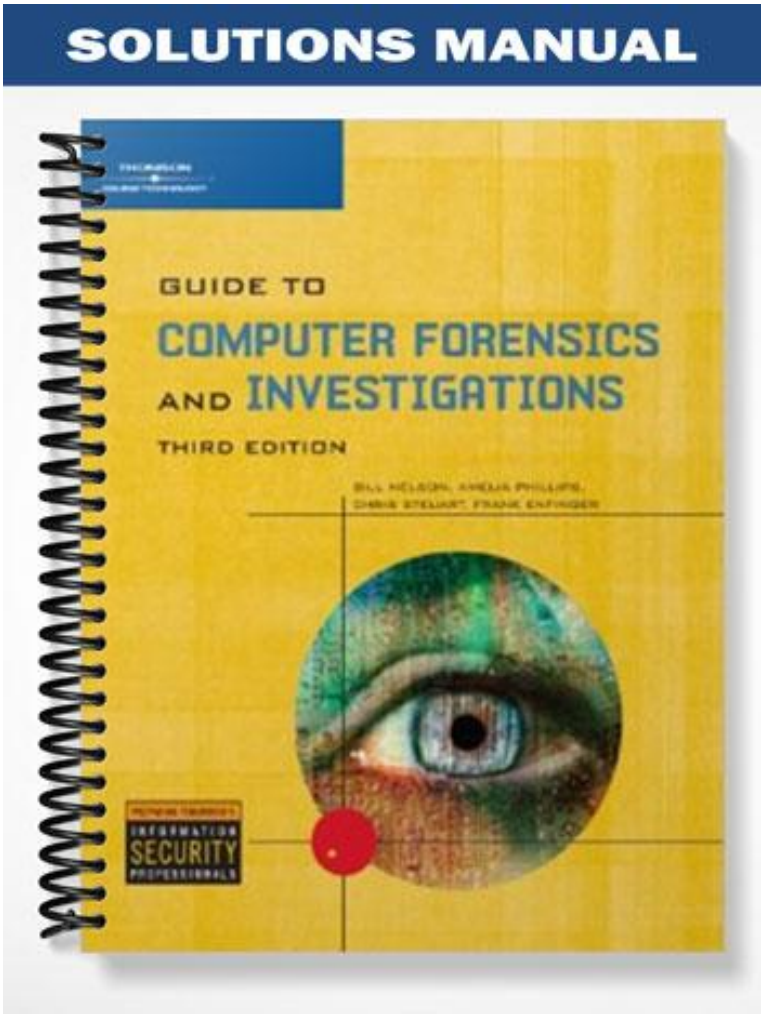
SOLUTIONS MANUAL



Chapter 2

Understanding Computer Investigations

At a Glance

Instructor's Manual Table of Contents

- Overview
- Objectives
- Teaching Tips
- Quick Quizzes
- Class Discussion Topics
- Additional Projects
- Additional Resources
- Key Terms

Lecture Notes

Overview

Chapter 2 explains computer investigation. Students will learn how to prepare a computer investigation. Next, students will apply a systematic approach to an investigation. Chapter 2 also describes procedures for corporate high-tech investigation. In addition, Chapter 2 explains requirements for data recovery workstations and software. Students will also learn how to conduct an investigation. Finally, Chapter 2 explains how to complete and critique a case.

Chapter 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

Teaching Tips

Preparing a Computer Investigation

1. Explain the role of computer forensics professionals.

2. Explain that collecting evidence that can be offered in court or at a corporate inquiry includes investigating the suspect's computer and preserving the evidence on a different computer.

3. Define chain of custody as the route the evidence takes from the time you find it until the case is closed or goes to court.

Teaching Tip	Read more about chain of custody at: http://en.wikipedia.org/wiki/Chain_of_custody.

An Overview of a Computer Crime

1. Explain to your students that information contained on a computer can help solve a case.

2. Present a case example where computer information may provide additional information to solve the crime. Use Figure 2-1 to illustrate your explanation.

3. You may need to define the roles of acquisitions officers and investigating officers.

4. Point your students to the U.S. Department of Justice (DoJ) Web page (www.usdoj.gov) for proper documentation on acquisition of digital evidence.

5. Explain the importance of tools like Digital Intelligences DriveSpy and Image, Norton DiskEdit, Guidance Softwares EnCase, and AccessData's Forensics Toolkit for a digital forensics investigator, especially when dealing with intact, deleted, and hidden files.

6. Mention that information on hard disks on computers you collect as evidence might be password protected. You might need to acquire password-cracking software or find an expert who can help you decrypt a file.

An Overview of a Company Policy Violation

1. Explain to your students that when employees misuse company resources, i.e., not following company policies, it can cost companies millions of dollars. Misuse includes:
    a. Surfing the Internet
    b. Sending personal e-mails
    c. Using company computers for personal tasks

Taking a Systematic Approach

1. Briefly explain each step to problem solving, including:
    a. Make an initial assessment about the type of case you are investigating
    b. Determine a preliminary design or approach to the case
    c. Create a detailed checklist
    d. Determine the resources you need
    e. Obtain and copy an evidence disk drive
    f. Identify the risks
    g. Mitigate or minimize the risks
    h. Test the design
    i. Analyze and recover the digital evidence
    j. Investigate the data you recover
    k. Complete the case report
    l. Critique the case

2. Do not forget to mention that the amount of time and effort for each step varies depending on the case you investigate.

Assessing the Case

1. Recall that when assessing a case, you first need to outline the case before determining the case requirements.

2. Present a list of case details. The list should include:
    a. Situation
    b. Nature of the case
    c. Specifics of the case
    d. Type of evidence
    e. Operating system
    f. Known disk format
    g. Location of evidence

3. Illustrate how case details can help you determine requirements like type of evidence, computer forensics tools, and operating systems.

Planning Your Investigation

1. Outline the basic steps when planning an investigation:
    a. Acquire the evidence
    b. Complete an evidence form and establish a chain of custody
    c. Transport the evidence to a computer forensics lab
    d. Secure evidence in an approved secure container
    e. Prepare a forensics workstation
    f. Obtain the evidence from the secure container
    g. Make a forensic copy
    h. Return the evidence to the container
    i. Process the forensic copy with appropriate tools

2. Remind your students that a broken chain of custody can throw out your case. Therefore, documenting evidence is very important during a forensics analysis.

3. Use Figures 2-2 and 2-3 to explain the use of evidence custody forms, either single-evidence or multi-evidence, and the fields typically included in these forms:
    a. Case number
    b. Investigating organization
    c. Investigator
    d. Nature of the case
    e. Location evidence was obtained
    f. Description of evidence
    g. Vendor name
    h. Model number or serial number
    i. Evidence recovered by
    j. Date and time
    k. Evidence placed in locker
    l. Item #/Evidence processed by/Disposition of evidence/Date/Time
    m. Page

Securing Your Evidence

1. Point out some of the considerations to follow when handling computer evidence:
    a. Static electricity
    b. Padding to prevent damage during transportation
    c. Sealing openings with evidence tape
    d. Writing initials on tape to prevent evidence from being altered
    e. Temperature and humidity ranges

Procedures for Corporate High-Tech Investigations

1. This section explains how to develop formal procedures and informal checklists to cover all issues important to high-tech investigations.

Employee Termination Cases

1. Mention that the majority of investigative work for termination cases involves employee abuse of corporate assets.

2. Describe what you need to conduct an Internet abuse investigation, including:
    a. The organization's Internet proxy server logs
    b. Suspect computer's IP address
    c. Suspect computer's disk drive
    d. Your preferred computer forensics analysis tool

3. Describe the steps to perform an Internet abuse investigation, including:
    a. Use standard forensic analysis techniques and procedures
    b. Use appropriate tools to extract all Web page URL information
    c. Contact the network firewall administrator and request a proxy server log
    d. Compare the data recovered from forensic analysis to the proxy server log
    e. Continue analyzing the computer's disk drive data

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

5. Describe the steps to perform an e-mail abuse investigation, including:
    a. Use the standard forensic analysis techniques and procedures
    b. Obtain an electronic copy of the suspect and victim's e-mail folder or data
    c. For Web-based e-mail investigations, use tools such as FTK's Internet Keyword Search option to extract all related e-mail address information
    d. Examine header data of all messages of interest to the investigation

Attorney-Client Privilege Investigations

1. Explain that under attorney-client privilege (ACP) rules for an attorney, you must keep all findings confidential.

Teaching Tip	Read more about attorney-client privilege at: http://en.wikipedia.org/wiki/Attorney-client_privilege.

2. Mention that many attorneys want 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 as binary files.

3. Describe the steps for conducting an ACP case, including:
    a. Request a memorandum from the attorney directing you to start the investigation
    b. Request a list of keywords of interest to the investigation
    c. Initiate the investigation and analysis
    d. For disk drive examinations, make two bit-stream images using different tools
    e. Compare hash signatures on all files on the original and re-created disks
    f. Methodically examine every portion of the disk drive and extract all data
    g. Run keyword searches on allocated and unallocated disk space
    h. For Windows OSs, use specialty tools to analyze and extract data from the Registry
    i. For binary data files such as CAD drawings, locate the correct software product
    j. For unallocated data recovery, use a tool that removes or replaces nonprintable data
    k. Consolidate all recovered data from the evidence bit-stream image into well-organized folders and subfolders

4. Describe other guidelines for conducting ACP cases, including:
    a. Minimize all written communications with the attorney
    b. Any documentation written to the attorney must contain a header stating that it's "Privileged Legal Communication—Confidential Work Product"
    c. Assist the attorney and paralegal in analyzing the data

5. If you have difficulty complying with the directions, contact the attorney and explain the problem.

6. Always keep an open line of verbal communication.

7. If you're communicating via e-mail, use encryption.

Media Leak Investigations

1. Mention that in the corporate environment, controlling sensitive data can be difficult.

2. Describe some of the considerations for media leak investigations, including:
    a. Examine e-mail
    b. Examine Internet message boards
    c. Examine proxy server logs
    d. Examine known suspects' workstations
    e. Examine all company telephone records

3. Describe the steps to take for media leaks, including:
    a. Interview management privately to get a list of employees who have direct knowledge of the sensitive data
    b. Identify the media source that published the information
    c. Review company phone records
    d. Obtain a listing of keywords related to the media leak
    e. Perform keyword searches on proxy and e-mail servers
    f. Discreetly conduct forensic disk acquisitions and analysis
    g. From the forensic disk examinations, analyze all e-mail correspondence and trace any sensitive messages to other people
    h. Expand the discreet forensic disk acquisition and analysis
    i. Consolidate and review your findings periodically
    j. Routinely report findings to management

Industrial Espionage Investigations

1. Mention that all suspected industrial espionage cases should be treated as criminal investigations.

2. Describe the staff needed for an industrial espionage investigation, including:
    a. Computing investigator who is responsible for disk forensic examinations
    b. Technology specialist who is knowledgeable of the suspected compromised technical data
    c. Network specialist who can perform log analysis and set up network sniffers
    d. Threat assessment specialist (typically an attorney)

3. Describe some of the guidelines for industrial espionage investigations, including:
    a. Determine whether this investigation involves a possible industrial espionage incident
    b. Consult with corporate attorneys and upper management
    c. Determine what information is needed to substantiate the allegation
    d. Generate a list of keywords for disk forensics and sniffer monitoring
    e. List and collect resources needed for the investigation
    f. Determine the goal and scope of the investigation
    g. Initiate the investigation after approval from management

Teaching Tip	Read more about sniffer monitoring at: http://en.wikipedia.org/wiki/Sniffer.

4. Describe some of the planning considerations for an industrial espionage investigation, including:
    a. Examine all e-mail of suspected employees
    b. Search Internet newsgroups or message boards
    c. Initiate physical surveillance
    d. Examine all facility physical access logs for sensitive areas
    e. Determine suspect location in relation to the vulnerable asset
    f. Study the suspect's work habits
    g. Collect all incoming and outgoing phone logs

5. Describe the basic steps to perform industrial espionage investigations, including:
    a. Gather all personnel assigned to the investigation and brief them on the plan
    b. Gather the resources needed to conduct the investigation
    c. Start the investigation by placing surveillance systems
    d. Discreetly gather any additional evidence
    e. Collect all log data from networks and e-mail servers
    f. Report regularly to management and corporate attorneys
    g. Review the investigation's scope with management and corporate attorneys

Interviews and Interrogations in High-Tech Investigations

1. Mention that becoming a skilled interviewer and interrogator can take many years of experience.

2. Explain that an interview is usually conducted to collect information from a witness or suspect about specific facts related to an investigation. Interrogation is the process of trying to get a suspect to confess to a specific incident or crime.

3. Explain that your role as a computing investigator is to instruct the investigator conducting the interview on what questions to ask and what the answers should be.

4. Describe the ingredients for a successful interview or interrogation, including:
    a. Being patient throughout the session
    b. Repeating or rephrasing questions to zero in on specific facts from a reluctant witness or suspect
    c. Being tenacious

Quick Quiz 1

1. The process of placing evidence in evidence bags and then labeling it with tags is called ____.
   Answer: bag and tag

2. _____ helps a computer forensics investigator to read password protected files.
   Answer: Password-cracking software

3. During the _____ step for problem solving you review the decisions you've made and the steps you have already completed
   Answer: test the design

4. A(n) ____ form, also called a chain-of-evidence form, helps you document what has and has not been done with the original evidence and forensic copies of the evidence.
   Answer: evidence custody

Understanding Data-Recovery Workstations and Software

1. Introduce your students to the concept of a computer forensics lab or data-recovery lab.

2. Compare computer forensics with data recovery.

3. Explain to the students the concept of a computer forensics workstation and its role on a forensics analysis.

4. Illustrate the different kinds of problems you may encounter when working with different operating systems and the importance of always booting with a forensics boot floppy disk. In addition, strongly recommend the use of write-blocker devices when performing a forensics analysis.

Teaching Tip	Read more about write blockers at: http://en.wikipedia.org/wiki/Write_Blocker.

Setting Up your Computer for Computer Forensics

1. Describe the basic requirements for setting up a computer forensics workstation, including:
   a. A workstation running Windows XP or Vista
   b. A write-blocker device
   c. Computer forensics acquisition tool
   d. Computer forensics analysis tool
   e. A target drive to receive the source or suspect disk data
   f. Spare PATA or SATA ports
   g. USB ports

2. Mention some additional useful items, including:
    a. Network interface card (NIC)
    b. Extra USB ports
    c. FireWire 400/800 ports
    d. SCSI card
    e. Disk editor tool
    f. Text editor tool
    g. Graphics viewer program
    h. Other specialized viewing tools

Conducting an Investigation

1. Explain that you should start by gathering the resources you identified in your investigation plan.

2. Describe the items needed for this phase, including:
    a. Original storage media
    b. Evidence custody form
    c. Evidence container for the storage media
    d. Bit-stream imaging tool
    e. Forensic workstation to copy and examine your evidence
    f. Securable evidence locker, cabinet, or safe

Gathering the Evidence

1. Explain that when you gather the evidence, you should avoid damaging the evidence.

2. Outline the steps involved in gathering the evidence, including:
    a. Meet the IT manager to interview him
    b. Fill out the evidence form, have the IT manager sign it
    c. Place the evidence in a secure container
    d. Complete the evidence custody form
    e. Carry the evidence to the computer forensics lab
    f. Create forensics copies (if possible)
    g. Secure evidence by locking the container

Understanding Bit-stream Copies

1. Define a bit-stream copy as a bit-by-bit copy of any storage medium.

2. Compare a bit-stream copy against a simple backup copy.

3. Define a bit-stream image file as the container of a bit-stream copy. A bit-stream image is also known as forensic copy.

4. Explain to the students why the target disk must match the original disk. Use Figure 2-4 to illustrate your explanation.

Acquiring an Image of Evidence Media

1. Mention that the first rule of computer forensics is to preserve the original evidence. Conduct your analysis only on a copy of the data.

2. Use Figures 2-5 through 2-8 to describe the steps to acquire a thumb drive image using ProDiscover Basic.

Teaching Tip	Learn more about ProDiscover Basic at: www.techpathways.com/DesktopDefault.aspx?tabindex=8&tabid=14.

Analyzing Your Digital Evidence

1. Remind your students that the job of a computer forensics investigator is to recover data from deleted files, files fragments, and complete files.

2. Mention that deleted files linger on the disk until new data is saved at the same physical location.

3. Use Figures 2-9 and 2-10 to show the steps to load and acquire an image into ProDiscover Basic.

4. Use Figures 2-11 and 2-12 to show how to display the contents of the acquired data.

5. Mention that data analysis can be the most time-consuming task.

6. Use Figures 2-13 through 2-16 to explain how to perform the following tasks with ProDiscover Basic:
    a. Search for keywords of interest in the case
    b. Display the results in a search results window in the work area
    c. Click each file in the search results window and examine its content in the data area
    d. Export the data to a folder of your choice
    e. Search for specific filenames
    f. Generate a report of your activities

Completing the Case

1. Give your students guides on how to write an investigation final report:
    a. State what you did and what you found
    b. Show conclusive evidence for proving a suspect guilty or innocent
    c. You can even include logs from forensic tools to support your points and show every single step you took when investigating the case

2. Stress that if by repeating the process described in a report you cannot achieve the same results, that work has no value as evidence. This characteristic is known as repeatable findings.

3. Mention to your students that the final report should be prepared accordingly to the expected readers.

Critiquing the Case

1. Describe how to make a self-evaluation of your work by answering the following questions:
    a. How could you improve your performance in the case?
    b. Did you expect the results you found? Did the case develop in ways you did not expect?
    c. Was the documentation as thorough as it could have been?
    d. What feedback has been received from the requesting source?
    e. Did you discover any new problems? If so, what are they?
    f. Did you use new techniques during the case or during research?

Quick Quiz 2

1. The secure evidence locker is located at the ____.
   Answer: data-recovery lab

2. Of all the Microsoft operating systems, ____ is the least intrusive in terms of changing data.
   Answer: MS-DOS 6.22

3. A(n) ____ is a bit-by-bit copy of the original storage medium.
   Answer: bit-stream copy

4. In any computing investigation, you should be able to repeat the steps you took and produce the same results. This capability is referred to as ____.
   Answer: repeatable findings

Class Discussion Topics

1. Discuss some of the various backup tools available in the market. What are the differences among the computer forensic tools discussed within the chapter?

2. Discuss some advantages and disadvantages of setting up a forensic workstation based on any distribution of Linux.

3. Knoppix is a Linux distribution that can run entirely from a CD or DVD. Discuss the possibility of using Knoppix (or other similar distributions) as a forensic boot disk.

Additional Projects

1. Have students practice the use of single-evidence and multi-evidence custody forms.

2. Have students investigate several computer forensics tools for use on a UNIX/Linux based workstation.

Additional Resources

1. How to Keep a Digital Chain of Custody:
   www.csoonline.com/read/120105/ht_custody.html

2. What is attorney client privilege?:
   http://co.essortment.com/attorneyclient_ritc.htm

3. Sniffers: What They Are and How to Protect Yourself:
   www.securityfocus.com/infocus/1549

4. Ethereal:
   www.ethereal.com/

5. Write-blockers:
   a. SCSI write blocker, www.paralan.com/sr14.html

   b. NoWrite™, www.techpathways.com/DesktopDefault.aspx?tabindex=4&tabid=16

   c. Forensic Examiner, www.computercop.com/examiner.html

   d. Article at SecurityFocus, www.securityfocus.com/archive/104/385537

   e. Article on a software write blocker,
   www.giac.org/practical/GCFA/Suzanne_Chevalier_GCFA.pdf

Key Terms

- **approved secure container** — A fireproof container locked by a key or combination.
- **attorney-client privilege (ACP)** — Communications between an attorney and client about legal matters is protected as confidential communications. The purpose of having confidential communications is to promote honest and open dialogue between an attorney and client. This confidential information must not be shared with unauthorized people.
- **bit-stream copy** — A bit-by-bit duplicate of data on the original storage medium. This process is usually called “acquiring an image” or “making an image.”
- **bit-stream image** — The file where the bit-stream copy is stored; usually referred to as an “image,” “image save,” or “image file.”

- **chain of custody** — The route evidence takes from the time the investigator obtains it until the case is closed or goes to court.
- **computer forensics workstation** — A workstation set up to allow copying forensic evidence, whether on a hard drive, thumb drive, CD, or Zip disk. It usually has software preloaded and ready to use.
- **evidence bags** — Nonstatic bags used to transport thumb drives, hard drives, and other computer components.
- **evidence custody form** — A printed form indicating who has signed out and been in physical possession of evidence.
- **forensic copy** — Another name for a bit-stream image.
- **interrogation** — The process of trying to get a suspect to confess to a specific incident or crime.
- **interview** — A conversation conducted to collect information from a witness or suspect about specific facts related to an investigation.
- **multi-evidence form** — An evidence custody form used to list all items associated with a case. *See also* evidence custody form.
- **password-cracking software** — Software used to match the hash patterns of passwords or to simply guess passwords by using common combinations or standard algorithms.
- **password protected** — Requiring a password to limit access to certain files and areas of storage media; this method prevents unintentional or unauthorized use.
- **repeatable findings** — Being able to obtain the same results every time from a computer forensics examination.
- **single-evidence form** — A form that dedicates a page for each item retrieved for a case. It allows investigators to add more detail about exactly what was done to the evidence each time it was taken from the storage locker. *See also* evidence custody form.