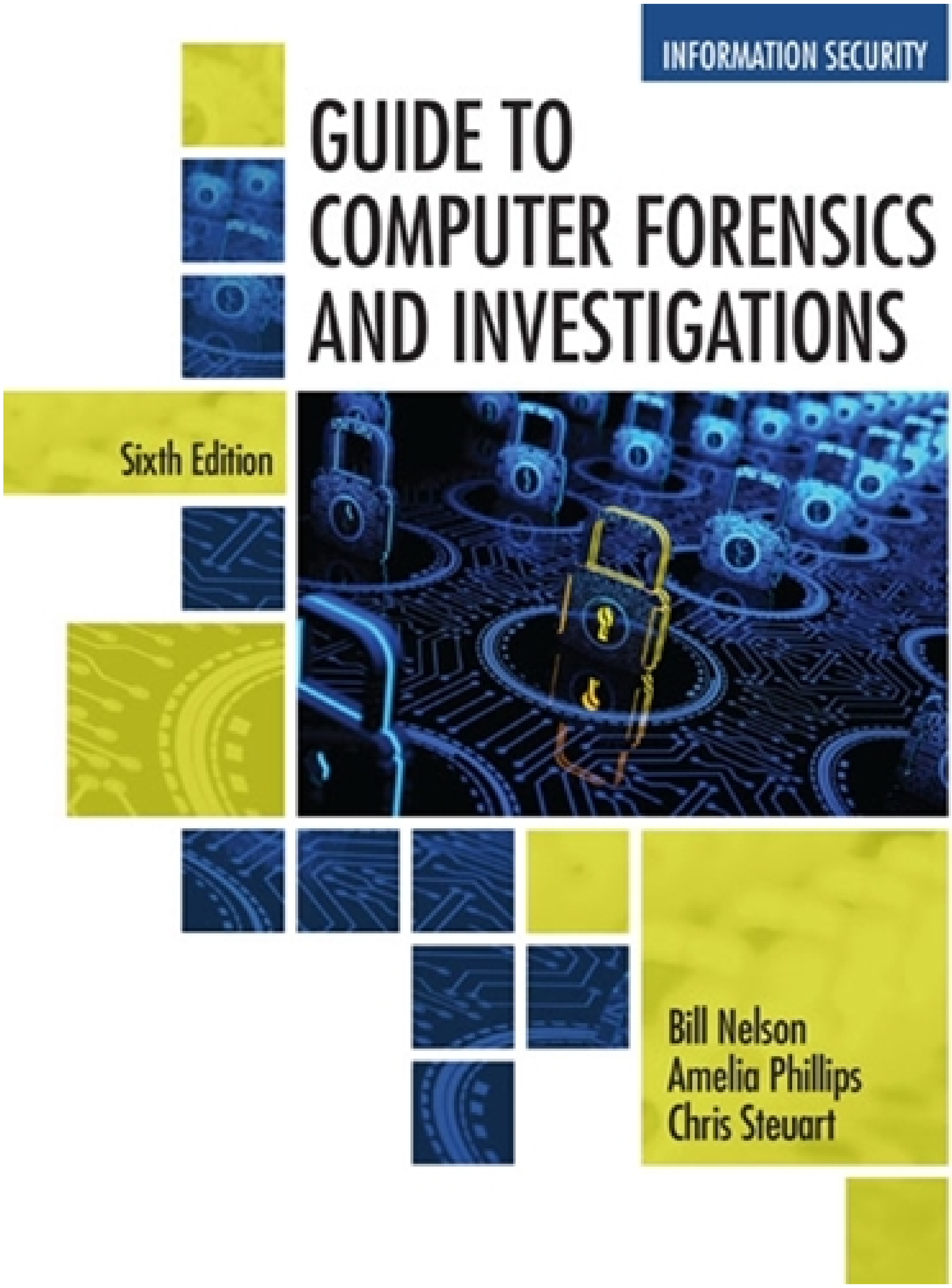
Solutions for Guide to Computer Forensics and Investigations 6th Edition by Nelson



Solutions

Chapter 1

Review Questions

1. Digital forensics and data recovery refer to the same activities. True or False?

   False

2. Police in the United States must use procedures that adhere to which of the following?

   b. Fourth Amendment

3. The triad of computing security includes which of the following?

   c. Vulnerability/threat assessment, intrusion detection and incident response, and digital investigation

4. What’s the purpose of maintaining a network of digital forensics specialists?

   To develop a list of colleagues who specialize in areas different from your own specialties in case you need help on an investigation.

5. Policies can address rules for which of the following?

   d. Any of the above

6. List two items that should appear on a warning banner.

   Statements that the organization has the right to monitor what users do, that their e-mail is not personal, and so on

7. Under normal circumstances, a private-sector investigator is considered an agent of law enforcement. True or False?

   False

8. List two types of digital investigations typically conducted in a business environment.

   Fraud, embezzlement, insider trading, espionage, and e-mail harassment

9. What is professional conduct, and why is it important?

   Professional conduct includes ethics, morals, and standards of behavior. It affects a professional’s credibility.

10. What’s the purpose of an affidavit?

    To provide facts in support of evidence of a crime to submit to a judge when requesting a search warrant

11. What are the necessary components of a search warrant?

    A search warrant must specify who, what, when, and where—that is, specifics on place, time, items being searched for, and so forth—and include any supporting materials (affidavits and exhibits, for example). In addition, a search warrant must be signed by an impartial judicial officer. In many cases, a search warrant can limit the scope of what can be seized.

12. What are some ways to determine the resources needed for an investigation?

    Determine the OS of the suspect computer and list the software needed for the examination.

13. List three items that should be on an evidence custody form.

    Answers include case number, name of the investigator assigned to the case, nature of the case, location where evidence was obtained, description of the evidence, and so on.

14. Why should you do a standard risk assessment to prepare for an investigation?

    To list problems that might happen when conducting an investigation, which can help in planning your case

15. You should always prove the allegations made by the person who hired you. True or False?

    False

16. For digital evidence, an evidence bag is typically made of antistatic material. True or False?

    True

17. Why should evidence media be write-protected?

    To make sure data isn't altered

18. List three items that should be in your case report.

    Answers can include an explanation of basic computer and network processes, a narrative of what steps you took, a description of your findings, and log files generated from your analysis tools.

19. Why should you critique your case after it's finished?

    To improve your work

20. What do you call a list of people who have had physical possession of the evidence?

    Chain of custody

21. Data collected before an attorney issues a memo for an attorney-client privilege case is protected under the confidential work product rule. True or False?

    False. All data collected before an attorney issues notice of attorney-client privilege is subject to discovery by opposing counsel.

Hands-On Projects

Hands-On Project 1-1

Students should be able to find two files of interest to this case. The first file, in Autopsy's Documents folder, is a text message pleading for help. The second file, in Autopsy's Plain Text folder, is an Excel spreadsheet containing the victim's assets and their values. Students' reports should include basic information about each file found on the USB drive.

Hands-On Project 1-2

Students should be able to find eight message files and one LibreOffice Calc spreadsheet. They should create a spreadsheet listing information about these files with Autopsy's report generator. They should also submit a short report listing the files they found in the disk image and include the Autopsy spreadsheet.

Hands-On Project 1-3

Students should be able to find three files showing a sailboat and sections of a sailboat and create an HTML Web report with links to the sailboat files, which are as follows:

```
/img_C1Prj03.E01/Pictures/Boat Building/PICT0010.JPG
2006-04-13 21:16:26 PDT
```

```
0000-00-00 00:00:00
2006-07-30 00:00:00 PDT
2006-07-30 18:04:43 PDT
415407
bdd77bb8089f147d16fb4fd11039e951

/img_C1Prj03.E01/Pictures/Boat Building/PICT0012.JPG
2006-04-13 21:16:42 PDT
0000-00-00 00:00:00
2006-07-30 00:00:00 PDT
2006-07-30 18:04:44 PDT
230593
fb6613de0ece7b5ca0e0ef7f520f2294

/img_C1Prj03.E01/Pictures/Boat Building/Boat Building/PICT0019.JPG
2006-04-14 19:15:32 PDT
0000-00-00 00:00:00
2006-07-30 00:00:00 PDT
2006-07-30 18:04:52 PDT
62676
5bf706c6309a71355a74260d1071186c
```

Hands-On Project 1-4

Student should be able to find and export two allocated files from the Images subfolder and four allocated files from the Office subfolder. The files are as follows:

```
6-Lin_tomb.jpg
16-Gettysbg.jpg
18-magnaCt.doc
19-USConst.doc
20-USDeclar.doc
22-Botany.doc
```

Hands-On Project 1-5

Students should be able to find the deleted files in the Deleted Files subfolder, tag all deleted files, and generate a spreadsheet listing the following files:

```
/img_C1Prj04.E01/Gettysburg.jpg
/img_C1Prj04.E01/THE DECLARATION OF INDEPENDENCE.doc
/img_C1Prj04.E01/Amendments to the Constitution.doc
/img_C1Prj04.E01/$CarvedFiles/f0000037.doc
/img_C1Prj04.E01/Lincoln.jpg
/img_C1Prj04.E01/Magna Carta.doc
/img_C1Prj04.E01/USAmmend.doc
/img_C1Prj04.E01/THE UNITED STATES CONSTITUTION.doc
/img_C1Prj04.E01/$CarvedFiles/f0000000.jpg
```

Hands-On Project 1-6

Students should be able to find four files and one unallocated area containing the keyword search results. When examining the unallocated area for the keyword Horatio, Autopsy’s Content Viewer defaults to the Media tab and displays a photograph of artwork for the path

/img_C1Prj06.E01//$Unalloc/Unalloc_19_29696_1474560. The keyword Horatio isn't visiblein the Media tab. To see this keyword, students need to switch to the Indexed Text tab. In addition, this file's content is visible only in the following path in the tree view: Results, Keyword Hits, Single Literal Keyword Search, HORATIO.

Students' reports should contain the following information:

```
Keyword:            ANTONIO
Path & Filename:    /img_C1Prj06.E01/The Merchant of Venice.doc
Modified date:      2004-06-23 21:25:20 PDT
Create date:        2004-06-23 22:40:23 PDT
File size:          72704
Keyword:            HORATIO
Path & Filename:    /img_C1Prj06.E01//$Unalloc/Unalloc_19_29696_1474560
Modified date:      0000-00-00 00:00:00
Create date:        0000-00-00 00:00:00
File size:          1019392

Keyword:            HORATIO
Path & Filename:    /img_C1Prj06.E01/$CarvedFiles/f0000068.doc
Modified date:      0000-00-00 00:00:00
Create date:        0000-00-00 00:00:00
File size:          90112

Keyword:            HORATIO
Path & Filename:    /img_C1Prj06.E01/The Tragedy of Hamlet.doc
Modified date:      2004-06-23 21:26:16 PDT
Create date:        2004-06-23 22:40:33 PDT
File size:          90112

Keyword:            HUGH EVANS
Path & Filename:    /img_C1Prj06.E01/The Merry Wives of Windsor.doc
Modified date:      2004-06-23 21:24:40 PDT
Create date:        2004-06-23 22:40:27 PDT
File size:          164352
```

Case Projects

Case Project 1-1

Students need to do an assessment of what the case involves. What is the nature of the case? What challenges do they expect to encounter, and how much time do they think the investigation will take?

Case Project 1-2

Most likely, Jonathan needs his computer to do other things in his business. Students need to acquire an image (preferably two) of the drive. Also, they should look around for clues of other storage media, and then go back to the lab and analyze the image. They should get as much detail as possible about the company and the other person.

Case Project 1-3

Students need to ask who else had access to the computer, find out whether the firm that fired her did its own investigation, and determine whether they can have access to the images. If no investigation has been done, students should state whether they can make copies now.

Case Project 1-4

Students need to find out which OS she was using and ask whether she knows the names of essential files or folders to make their search easier. Students should formulate interview questions to determine whether she might have added new data or altered data since the file deletion. They should understand that any file deletion recovery depends on the amount of computer activity immediately following the data loss.

Chapter 1

Understanding the Digital Forensics Profession and Investigations

At a Glance

Instructor's Manual Table of Contents

Lecture Notes

Overview

Chapter 1 introduces you to digital forensics and explains computer investigation. Students will learn how to prepare a computer investigation. Next, students will apply a systematic approach to an investigation. This chapter also describes procedures for corporate high-tech investigation. In addition, Chapter 1 explains requirements for data recovery workstations and software. Students will also learn how to conduct an investigation. Finally, Chapter 1 explains how to complete and critique a case.

Chapter Objectives

- Describe the field of digital forensics
- Explain how to prepare for computer investigations and summarize the difference between public-sector and private-sector investigations
- Explain the importance of maintaining professional conduct
- Describe how to prepare a digital forensics investigation by taking a systematic approach
- Describe procedures for private-sector digital investigations
- Explain requirements for data recovery workstations and software
- Summarize how to conduct an investigation, including critiquing a case

Teaching Tips

An Overview of Digital Forensics

1. Explain that digital forensics involves obtaining and analyzing digital information for use as evidence in civil, criminal, or administrative cases.

2. Point out that an International Organization for Standardization (ISO) standard for digital forensics was ratified in October 2012.

3. Mention that the FBI Computer Analysis and Response Team (CART) was formed in 1984 to handle the increasing number of cases involving digital evidence.

Teaching Tip	For more details about the FBI Computer Analysis and Response Team (CART), visit: https://www.fbi.gov/news/stories/piecing-together-digital-evidence.

4. Explain that 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.

Digital Forensics and Other Related Disciplines

1. Explain that digital forensics investigates data that can be retrieved from a computer's hard disk or other storage media. Network forensics yields information about how a perpetrator or an attacker gained access to a network.

Teaching Tip	Read more about digital forensics at: http://www.digitalforensicsmagazine.com/

2. Mention that data recovery involves retrieving information from a computer that was deleted by mistake or lost during a power surge or server crash. Typically, you know what you're looking for. Digital forensics is the task of recovering data that users have hidden or deleted and using it as evidence. This evidence can be inculpatory ("incriminating") or exculpatory.

3. Explain the differences between inculpatory versus exculpatory evidence.

4. Mention that investigators often work as a team to make computers and networks secure in an organization. Use Figure 1-1 to explain the investigations triad. Point out that in smaller companies, one group might perform all the tasks shown in the investigations triad.

5. Explain that when you work in the vulnerability assessment and risk management group, you test and verify the integrity of standalone workstations and network servers. Professionals in this group have skills in network intrusion detection and incident response.

6. Explain that the network intrusion detection and incident response group detects intruder attacks by using automated tools and monitoring firewall logs.

7. Define the digital investigations group as a team that manages investigations and conducts forensics analysis of systems suspected of containing evidence related to an incident or a crime.

A Brief History of Digital Forensics

1. Explain that by the 1970s, electronic crimes were increasing, especially in the financial sector. Most law enforcement officers didn't know enough about computers to ask the right questions or to preserve evidence for trial.

2. Mention that in the early 1980s, PCs gained popularity and different OSs emerged. Disk Operating System (DOS) was available in many varieties. Forensics tools were simple, and most were generated by government agencies. Use Figure 1-2 to illustrate a typical 1980s computer.

3. By the mid-1980s, Xtree Gold appeared on the market and recognized file types and retrieved lost or deleted files. Norton DiskEdit soon followed and became the best tool for finding deleted files.

4. Mention that in 1987, Apple produced the Mac SE, a Macintosh with an external EasyDrive hard disk with 60 MB of storage. Use Figure 1-3 to illustrate your explanation.

5. Explain that by the early 1990s, specialized tools for computer forensics were available. The International Association of Computer Investigative Specialists (IACIS) introduced training on software for forensics investigations and the IRS created search-warrant programs.

Teaching Tip	Read more about IACIS at: http://www.iacis.com/.

6. Mention that ExpertWitness, created by ASR Data for the Macintosh, was the first commercial GUI software for computer forensics. ExpertWitness could recover deleted files and fragments of deleted files.

7. Mention that the introduction of large hard disks posed new problems for investigators. Other software that was developed for computer forensics includes ILook and AccessData Forensic Toolkit (FTK).

Teaching Tip	AccessData Forensic Toolkit (FTK) Web site: https://accessdata.com/products-services/forensic-toolkit-ftk.

Understanding Case Law

1. Explain that since technology is evolving at an exponential pace, existing laws and statutes can't keep up with the rate of change.

2. Explain that when statutes or regulations don't exist, case law is used. Case law allows legal counsel to use previous cases similar to the current one because the laws don't yet exist. Each new case is evaluated on its own merit and issues.

Developing Digital Forensics Resources

1. Explain that you must be familiar with more than one computing platform, such as DOS, Windows 9x, Linux, Macintosh, and current Windows platforms.

2. Mention that you should join as many computer user groups as you can. The Computer Technology Investigators Network (CTIN) meets to discuss problems that digital forensics examiners encounter.

3. Point out that the High Technology Crime Investigation Association (HTCIA), International Information Systems Security Certification Consortium (ISC²), and InfraGard have local chapters open to professionals in most major cities.

4. Mention that user groups can be especially helpful when you need information about obscure OSs.

5. Explain that it is recommended that you build a network of computer forensics experts and other professionals, and keep in touch through e-mail. Outside experts can provide detailed information you need to retrieve digital evidence.

Preparing for Digital Investigations

1. Explain that digital investigations fall into two distinct categories: public-sector investigations and private-sector investigations. Use Figure 1-4 to illustrate your explanation.

2. Explain that public investigations involve government agencies responsible for criminal investigations and prosecution. These organizations must observe legal guidelines. For example, the law of search and seizure protects the rights of all people, including people suspected of crimes. Use Figure 1-5 to illustrate your explanation.

3. Explain that private or corporate investigations deal with private companies, non-law-enforcement government agencies, and lawyers. Private investigations aren't governed directly by criminal law or Fourth Amendment issues. They are governed by internal policies that define expected employee behavior and conduct in the workplace.

4. Mention that private corporate investigations also involve litigation disputes. Investigations are usually conducted in civil cases.

Understanding Law Enforcements Agency Investigations

1. Explain that in a criminal case, a suspect is tried for a criminal offense such as burglary, murder, molestation, or fraud. Computers and networks are tools that can be used to commit crimes.

2. Mention that many states have added specific language to criminal codes to define crimes involving computers.

3. Many serious crimes involve computers, smartphones, and other digital devices.

Following Legal Processes

1. Explain that the legal processes depend on local custom, legislative standards, and rules of evidence. Criminal case follows three stages: the complaint, the investigation, and the prosecution.

2. Explain that a criminal case begins when someone finds evidence of an illegal act. The complainant makes an allegation, an accusation or supposition of fact.

3. Next, a police officer interviews the complainant and writes a report about the crime. The police blotter provides a record of clues to crimes that have been committed previously. Point out that blotters now are generally electronic files. An investigator delegates, collects, and processes the information related to the complaint.

4. Discuss the difference between a Digital Evidence First Responder (DEFR) and a Digital Evidence Specialist (DES).

5. Mention that after you build a case, the information is turned over to the prosecutor.

6. Define affidavit as a sworn statement of support of facts about or evidence of a crime submitted to a judge to request a search warrant. Use Figure 1-6 to illustrate your explanation. The affidavit must be notarized under sworn oath.

7. Mention that a judge must approve and sign a search warrant before you can use it to collect evidence.

Teaching Tip	Read more about affidavits at: http://legal-dictionary.thefreedictionary.com/affidavit.

Understanding Private-Sector Investigations

1. Explain that private-sector investigations involve private companies and lawyers who address company policy violations and litigation disputes.

2. Mention that corporate computer crimes can involve:
   a. E-mail harassment
   b. Falsification of data
   c. Gender and age discrimination
   d. Embezzlement
   e. Sabotage
   f. Industrial espionage

3. Explain that one way to avoid litigation is to publish and maintain policies that employees find easy to read and follow. Published company policies provide a line of authority for a business to conduct internal investigations.

4. Mention that well-defined policies give computer investigators and forensic examiners the authority to conduct an investigation.

5. Explain that another way to avoid litigations is to display warning banners. A warning banner usually appears when a computer starts or connects to the company intranet,

network, or virtual private network. It informs end users that the organization reserves the right to inspect computer systems and network traffic at will. A warning banner establishes the right to conduct an investigation. Use Figure 1-7 to illustrate your explanation.

6. Mention that an authorized requester has the power to conduct investigations, and this policy should be defined by executive management.

7. Describe the groups that should have direct authority to request computer investigations, including:
   a. Corporate security investigations
   b. Corporate ethics office
   c. Corporate equal employment opportunity office
   d. Internal auditing
   e. The general counsel or legal department

8. Describe the most common type of situations that require conducting security investigations in a corporate environment, including:
   a. Abuse or misuse of corporate assets
   b. E-mail abuse
   c. Internet abuse

9. Mention that you should be sure to distinguish between a company's abuse problems and potential criminal problems.

10. Explain that the Federal Rules of Evidence are the same for civil and criminal matters.

11. Explain that many company policies distinguish between personal and company computer property. One area that's difficult to distinguish involves cell phones, smartphones, personal notebooks and tablet computers. Mention that some companies state that if you connect a personal device to the business network, it falls under the same rules as company property.

Maintaining Professional Conduct

1. Explain that your professional conduct as a digital investigation and forensics analyst is critical because it determines your credibility. It includes ethics, morals, and standards of behavior.

2. Explain that maintaining objectivity means you must form and sustain unbiased opinions of your cases. Maintain an investigation's credibility by keeping the case confidential. In the corporate environment, confidentiality is critical.

3. Mention that in rare instances, your corporate case might become a criminal case as serious as murder.

4. Explain that you can enhance your professional conduct by continuing your training, attending workshops, conferences, and vendor courses. Also, membership in professional organizations adds to your credentials.

5. Mention that you are expected to achieve a high public and private standing and maintain honesty and integrity.

Quick Quiz 1

1. ____ involves obtaining and analyzing digital information for use as evidence in civil, criminal, or administrative cases.
   Answer: Digital forensics

2. Evidence that is used to clear the suspect is known as _______.
   Answer: exculpatory evidence

3. A sworn statement of support of the facts about or evidence of a crime is known as a(n) _____.
   Answer: affidavit

4. ____ allows legal counsel to use previous cases similar to the current one because the laws don’t yet exist.
   Answer: Case law

5. A(n) _____ usually appears when a computer starts and informs end users that the organization reserves the right to inspect computer systems and network traffic at will.
   Answer: warning banner

Preparing a Digital Forensics Investigation

1. Explain the role of digital 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://legal-dictionary.thefreedictionary.com/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 1-8 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 Autopsy from Sleuth Kit for a digital forensics investigator, especially when dealing with intact, deleted, and hidden files.

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 during work hours

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. Known disk format
   f. Location of evidence

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. Retrieve 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 1-9 and 1-10 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 Private-Sector 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.

Internet Abuse Investigations

1. 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 digital forensics analysis tool

2. 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

E-mail Abuse Investigations

1. 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 digital forensics analysis tool

2. 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://legal-dictionary.thefreedictionary.com/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. Verify 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.

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 employee monitoring at: https://www.forensicon.com/resources/articles/worker-beware-employee-monitoring/.

4. Describe some of the planning considerations for an industrial espionage investigation, including:
   a. Examine all e-mail of suspected employees
   b. Search Internet forums or blogs
   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

Understanding Data-Recovery Workstations and Software

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

2. Compare digital forensics with data recovery.

3. Explain to the students the concept of a digital 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. In addition, strongly recommend the use of write-blocker devices when performing a forensics analysis.

Teaching Tip	Read more about write blockers at: http://www.forensicswiki.org/wiki/Write_Blockers

Setting Up your Workstation for Digital Forensics

1. Describe the basic requirements for setting up a computer forensics workstation, including:
   a. A workstation running Windows 7 or later
   b. A write-blocker device
   c. Digital forensics acquisition tool
   d. Digital 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. Carry the evidence to the computer forensics lab
   e. Complete the evidence custody form
   f. Secure evidence by locking the container

Understanding Bit-stream Copies

1. Define a bit-stream copy as a bit-by-bit copy of the original drive or 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 “image” or “image file”.

4. Explain to the students why the target disk must match the original disk. Use Figure 1-11 to illustrate your explanation.

Acquiring an Image of Evidence Media

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

Analyzing Your Digital Evidence

1. Remind your students that the job of a digital 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 1-12 through 1-14 to show the steps to load and acquire an image into Autopsy.

4. Use Figures 1-15 through 1-17 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 1-18 through 1-19 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

Some Additional Features of Autopsy

1. Use Figure 1-20 to show how to display binary (nonprintable) data in Autopsy's Content Viewer.

Completing the Case

1. Discuss the questions that need to be answered in order to write the final report.

2. 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

3. 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.

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

Autopsy's Report Generator

1. Use Figure 1-21 to explain how to prepare a report in Autopsy.

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

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

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

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

5. 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. Several Linux distributions can run entirely from a CD, DVD or even a USB drive. Discuss the possibility of using a Live distribution 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: http://www.csoonline.com/article/2118807/investigations-forensics/how-to-keep-a-digital-chain-of-custody.html

2. What is attorney client privilege?: https://www.law.cornell.edu/wex/attorney-client_privilege

3. Sniffers: What They Are and How to Protect Yourself: https://www.symantec.com/connect/articles/sniffers-what-they-are-and-how-protect-yourself

4. Write-blockers:

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

   b. No Write™ , www.mykeytech.com/nowrite.html

Key Terms

- **affidavit** — A notarized document, given under penalty of perjury, that investigators create to detail their findings. This document is often used to justify issuing a warrant or to deal with abuse in a corporation. Also called a “declaration” when the document is unnotarized.

- **allegation** — A charge made against someone or something before proof has been found.
- **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.
- **authorized requester** — In a private-sector environment, the person who has the right to request an investigation, such as the chief security officer or chief intelligence officer.
- **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 Technology Investigators Network (CTIN)** — A nonprofit group based in Seattle-Tacoma, WA, composed of law enforcement members, private corporation security professionals, and other security professionals whose aim is to improve the quality of high-technology investigations in the Pacific Northwest.
- **data recovery** — Retrieving files that were deleted accidentally or purposefully.
- **Digital Evidence First Responder (DEFR)** — A professional who secures digital evidence at the scene and ensures its viability while transporting it to the lab.
- **Digital Evidence Specialist (DES)** — An expert who analyzes digital evidence and determines whether additional specialties are needed.
- **digital forensics** — Applying investigative procedures for a legal purpose; involves the analysis of digital evidence as well as obtaining search warrants, maintaining a chain of custody, validating with mathematical hash functions, using validated tools, ensuring repeatability, reporting, and presenting evidence as an expert witness.
- **digital investigations** — The process of conducting forensic analysis of systems suspected of containing evidence related to an incident or a crime.
- **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.
- **exculpatory evidence** — Evidence that indicates the suspect is innocent of the crime.
- **exhibits** — Evidence that indicates the suspect is innocent of the crime.
- **forensics workstation** — A workstation set up to allow copying forensic evidence, whether on a hard drive, flash drive, or the cloud. It usually has software preloaded and ready to use.
- **Fourth Amendment** — The Fourth Amendment to the U.S. Constitution in the Bill of Rights dictates that the government and its agents must have probable cause for search and seizure.
- **hostile work environment** — An environment in which employees cannot perform their assigned duties because of the actions of others. In the workplace, these actions

include sending threatening or demeaning e-mail or a co-worker viewing pornographic or hate sites.

- **inculpatory evidence** — Evidence that indicates a suspect is guilty of the crime with which he or she is charged.
- **industrial espionage** — Theft of company sensitive or proprietary company information often to sell to a competitor.
- **International Association of Computer Investigative Specialists (IACIS)** — An organization created to provide training and software for law enforcement in the digital forensics field.
- **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.
- **line of authority** — The order in which people or positions are notified of a problem; these people or positions have the legal right to initiate an investigation, take possession of evidence, and have access to evidence.
- **multi-evidence form** — An evidence custody form used to list all items associated with a case. *See also* evidence custody form.
- **network intrusion detection and incident response** — Detecting attacks from intruders by using automated tools; also includes the manual process of monitoring network firewall logs.
- **professional conduct** — Behavior expected of an employee in the workplace or other professional setting.
- **repeatable findings** — Being able to obtain the same results every time from a computer forensics examination.
- **search and seizure** — The legal act of acquiring evidence for an investigation. *See also* Fourth Amendment.
- **search warrants** — Legal documents that allow law enforcement to search an office, a home, or other locale for evidence related to an alleged crime.
- **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.
- **verdict** — The decision returned by a jury.
- **vulnerability/threat assessment and risk management** — The group that determines the weakest points in a system. It covers physical security and the security of OSs and applications.
- **warning banner** — Text displayed on computer screens when people log on to a company computer; this text states ownership of the computer and specifies appropriate use of the machine or Internet access.
- **White-collar crimes** — Type of private-sector computer crimes involving falsification of data, embezzlement, and sabotage.