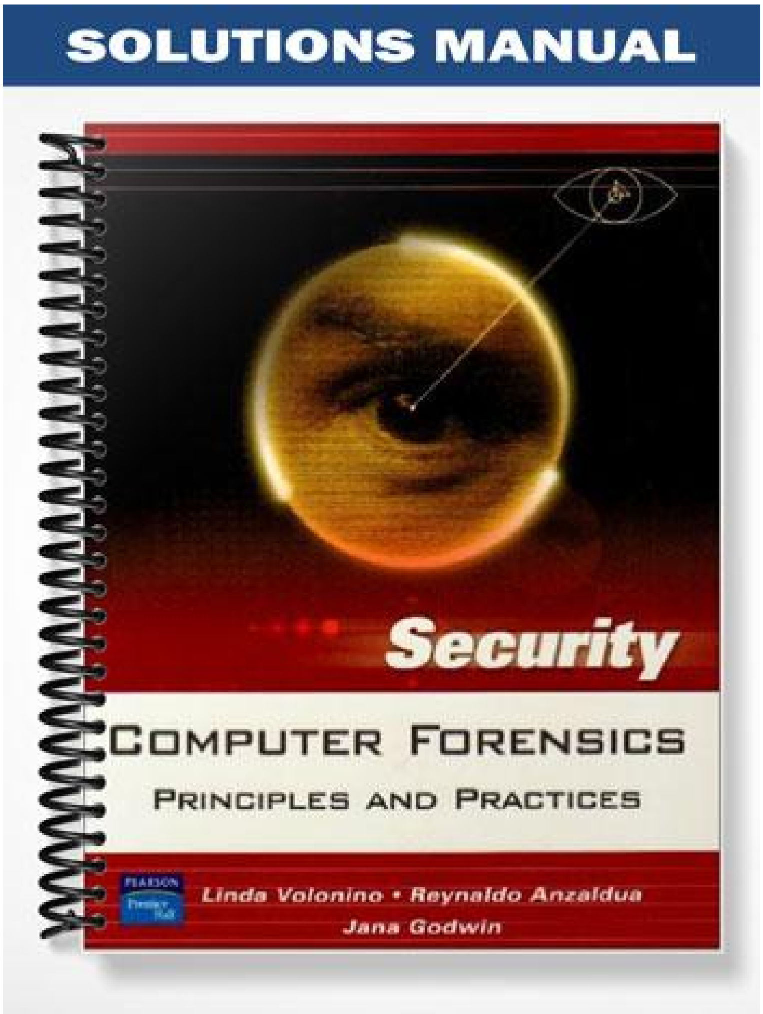

SOLUTIONS MANUAL

Security

COMPUTER FORENSICS

PRINCIPLES AND PRACTICES

PEARSON Prentice Hall

Linda Volonino • Reynaldo Anzaldua
Jana Godwin

Instructor's Manual Materials to Accompany
COMPUTER FORENSICS

CHAPTER 2
COMPUTER FORENSICS AND DIGITAL DETECTIVE WORK

CHAPTER OBJECTIVES

When students have finished reading this chapter, they will be able to:

- Recognize the role e-evidence plays in physical, or violent, and computer crimes.
- Describe the basic steps in a computer forensics investigation.
- Identify the legal and ethical issues affecting evidence search and seizure.
- Identify the types of challenges to the admissibility of e-evidence.
- Understand how criminals' motives can help in crime detection and investigation.
- Explain chain of custody.
- Explain why acceptable methods for computer forensics investigations and e-discovery are still emerging.

CHAPTER OVERVIEW

Chapter 2 introduces the generally accepted computer forensics methods and describes the technical, legal, and ethical environment in which the computer forensics investigator operates.

The major sections in this chapter are:

1. The Role of E-Evidence in Solving Physical and Computer Crimes—Gives examples of a wide variety of cases, many of them high-profile, in which e-evidence plays a key role in the prosecution.

2. Computer Forensics Science—Describes the five stages of the scientific research process as applied to computer forensics.

3. Digital Signatures and Profiling—Describes the use of digital signatures—incriminating e-evidence left by violent offenders—to construct profiles of suspects.

4. Computer Forensics and the E-Evidence Collection Process—Outlines the standard computer forensics investigative procedures and discusses the objectives computer forensic investigators must achieve.

5. Suppression, Probable Cause, and Search Warrants—Describes, using recent examples, the variety of legal challenges that may be mounted against the admissibility of e-evidence.

6. Types of Motives and Cybercrimes—Lists the variety of motivations of cybercriminals, distinguishing between crimes in which the computer is the target and those in which the computer is the instrument.

7. Forensics Rules and Evidence Issues—Describes in detail the handling of evidence and the importance of properly documenting the handling as part of the chain of custody.

8. Computer Forensics Investigator's Responsibilities—Briefly lists some of the professional responsibilities of the computer forensics investigator.

CHAPTER OUTLINE

I. Chapter Objectives

II. Introduction

III. The Role of E-Evidence in Solving Physical and Computer Crimes

A. E-Evidence Trails

B. Finding Hidden Files on a Computer

C. Knowing What to Look For

D. Answering the 5 Ws Helps in Criminal Investigations

IV. Computer Forensics Science

A. Admissibility of Evidence

B. Tradeoffs to Be Considered

V. Digital Signatures and Profiling

A. Digital Signature Left by Serial Killer

B. Digital Profiling of Crime Suspects

VI. Computer Forensics and the E-Evidence Collection Process

A. Unallocated Space and File Slack

B. Example of Standard Forensics Investigative Procedure

VII. Suppression, Probable Cause, and Search Warrants

A. Withstanding Challenges to Evidence

B. Probable Cause and Search Warrants

C. Proper Procedure and Limitations Built into the Law

D. Conclusions and Lessons

VIII. Types of Motives and Cybercrimes

A. Finding the Motive—The “Why” of the Crime

B. Computer Is the Crime Target

C. Computer Is the Crime Instrument

D. Computer Is Incidental to Traditional Crimes

E. New Crimes Generated by the Prevalence of Computers

IX. Forensics Rules and Evidence Issues

A. Chain of Custody Procedures

B. Report Procedures

X. Computer Forensics Investigator’s Responsibilities

XI. Summary

KEY TERMS

admission of evidence A judge’s acceptance of evidence in a trial.

chain of custody The process by which computer forensics specialists or other investigators preserve the crime scene and evidence throughout the life cycle of a case.

chain of custody log Documentation that evidence was handled and preserved properly and that it was never at risk of being compromised.

cluster A fixed block of data that consists of an even number of sectors, such as 1,024 bytes or 4,096 bytes.

computer forensics science The forensic discipline of acquiring, preserving, retrieving, and presenting electronic data.

file-wiping software Software that is used to delete and overwrite data.

forensic accounting The integration of accounting, auditing, and investigative skills to discover and investigate financial crimes.

indictment A grand jury charge that the defendant should stand trial.

legacy data Older data on a disk, which may indicate prior uses of the computer.

sector The smallest unit that can be accessed on a disk. A sector is 512 bytes. Computer hard drives can “grab” data only in sector-size chunks.

slack space Unused space in a cluster, which is found at the end of a file.

sniffer software A software program that monitors data traveling over a network or records keystrokes.

spoofing To trick, disguise, or deceive. A spoofed Web site is a phony site that replaces a legitimate Web site address.

suppression hearing A hearing before a criminal trial during which the judge determines whether the Fourth Amendment has been followed correctly by the police in the search and seizure of evidence.

techno-vandalism Unauthorized access to a computer that damages files or programs for the challenge or sport rather than for profit.

three C's of evidence Care, control, and chain of custody. These are legal guidelines to ensure that the evidence presented is the same as that which was seized. It requires documentation of the maintenance of evidence in its original state and preparation for civil or criminal proceedings.

wardriving Driving around with a laptop computer and antenna looking for unprotected wireless Internet connections to tap into.

TEACHING NOTES

I. The Role of E-Evidence in Solving Physical and Computer Crimes

Teaching Tips: Computers are routinely used in the commission of almost every type of crime.

Teaching Tips: Even meticulous efforts to cover one’s cybertracks will almost inevitably leave electronic evidence behind.

II. Computer Forensics Science

Teaching Tips: Computer forensics has been recognized as a scientific discipline.

Teaching Tips: The search for evidence should not be limited only to supporting evidence.

Teaching Tips: To be admissible in the courtroom, evidence must be gathered using generally accepted methods.

Teaching Tips: Without a documented chain of custody, it is impossible to prove that evidence has not been altered.

III. Digital Signatures and Profiling

Teaching Tips: E-evidence that is not strong enough to convict a suspect may still be useful for implying motive or intent.

IV. Computer Forensics and the E-Evidence Collection Process

Teaching Tips: Computer forensics investigative procedures are standardized.

V. Suppression, Probable Cause, and Search Warrants

Teaching Tips: To protect our privacy rights, the Federal Rules of Evidence and Federal Rules of Civil Procedure define allowable fact-finding procedures.

Teaching Tips: The rules on admissibility of e-evidence are still being written.

Teaching Tips: A pre-trial suppression hearing, in which the admissibility of evidence is determined, may often determine the outcome of a criminal trial.

Teaching Tips: A search warrant gives law enforcement a limited right to violate a citizen's privacy.

VI. Types of Motives and Cybercrimes

Teaching Tips: The prevalence of computers has generated new types of crime, as well as new versions of traditional crimes.

VII. Forensics Rules and Evidence Issues

Teaching Tips: Chain of custody ensures that the evidence presented at trial is the same as that which was seized.

VIII. Computer Forensics Investigator's Responsibilities

Teaching Tips: There is no rule governing how long police may keep possession of seized computers and computer equipment.

PROJECTS/EXERCISES

I. Discussion Questions

Discussion Question 1

Discuss the issues involved in admissibility of evidence, especially with reference to chain of custody. Do strict chain-of-custody requirements place an undue burden on forensics investigators, to the point that too many obviously guilty perpetrators are being set free on technicalities? Discuss the O. J. Simpson murder trial; what chain-of-custody issues were involved in the acquittal?

II. Web Projects

Web Project 1

Long before personal computers were common, the people who would later become computer hackers were hacking the phone system. The writer Ron Rosenbaum wrote a now-legendary article for *Esquire* magazine in 1971, called "Secrets of the Little Blue Box," introducing the world to Captain Crunch and the subterranean world of phone-phreaking. Search the Web for the article (it has been republished on many sites) and read this fascinating story.

Web Project 2

Read about the psychology of computer hackers at the PBS Web site: http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/psycho.html.

Web Project 3

Visit the Crime Library Web site and read the story of the O. J. Simpson trial (http://www.crimelibrary.com/notorious_murders/famous/simpson/index_1.html).

WEB RESOURCES

- http://www.247.prenhall.com—Pearson/Prentice Hall Product Support
- http://www.csoonline.com—*Chief Security Officer Magazine* Web site
- http://www.cyberscrub.com—Home page for CyberScrub Privacy Suite evidence-erasing software
- http://www.usdoj.gov—Department of Justice Web site
- http://www.securityfocus.com—*Security* Focus magazine Web site
- http://support.microsoft.com/support/kb/articles/Q223/7/90.ASP—Microsoft Knowledge Base article on Microsoft Word metadata
- http://www.usdoj.gov/criminal/cybercrime/searching.html—Federal Guidelines for Searching and Seizing Computers
- http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/psycho.html—PBS *Frontline*: "Hackers: Who Are Hackers? Studying Their Psychology."
- http://www.cybercrime.gov—Department of Justice computer crime Web site
- http://www.e-evidence.info/ccunits.html—National listing of computer forensics laboratories
- http://www.crimelibrary.com/notorious_murders/famous/simpson/index_1.html—Detailed account of the O. J. Simpson trial.

CHAPTER REVIEW/ANSWERS TO TEST YOUR SKILLS

MULTIPLE CHOICE QUESTIONS

1. What is the most significant legal issue in computer forensics?

   C

2. E-discovery of documents or data

   A

3. Federal rules regulate the fact-finding process for all of the following reasons, *except*

   D

4. Which of the following statements is true?

   B

5. In order for a law enforcement officer to search a person or his property without a search warrant, certain conditions must be met. Which of the following is *not* one of those conditions?

   A

6. Which is an example of steganography?

   A

7. "The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures shall not be violated . . ." is part of the

   B

8. Which cybercrime would be the most difficult to detect?

   A

9. What is a chain of custody?

   C

10. Traditional crimes that became easier or more widespread because of telecommunication networks and powerful PCs include all of the following *except*

    C

11. Searching for e-evidence while investigating high-profit crimes, such as drug distribution or money laundering, can be particularly challenging because criminals engaged in these crimes

    B

12. Which of the following is (are) true about crimes?

    D

13. Computer forensics tools such as MD5 create a unique value for each file. This unique value is important because

    C

14. Which of the following reporting procedures helps ensure successful investigation and prosecution of a case?

    D

15. Federal Rule of Criminal Procedure 41(c)(1) gives the police _____ after issuance of the warrant to serve it.

    C

EXERCISES

Exercise 2.1: Detecting E-Evidence from Web Site Visits

Exercise 2.1 is a practice e-evidence discovery investigation. It is meant to help students understand the types of e-evidence left by online activities by performing an actual investigation of their own activities and the trails they create/leave on their hard drives.

Exercise 2.2: E-Evidence of Corporate Crime

Exercise 2.2 is procedural. It is meant to help students identify e-evidence and recognize the challenges an investigator faces when trying to link a person to a crime as they determine whether the e-evidence is sufficient. It also gets students to think about why people leave e-evidence that could implicate them in a crime—and locations where investigators search for that e-evidence. Reasons why anyone thinks that e-records would never be revealed should relate to users' misunderstanding that "delete" does not get rid of e-evidence and that they are unaware of the use of e-evidence.

Exercise 2.3: Understanding the Meaning of Probable Cause

In this project, students become familiar with legal terminology and legal dictionaries. They relate a probable cause to the Fourth Amendment. The successful student will make some reference to the rights guaranteed by the Fourth Amendment. From the FBI Web site http://www.fbi.gov/hq/cid/civilrights/color.htm: "The Fourth Amendment of the United States Constitution guarantees the right against unreasonable searches or seizures. A law enforcement official using his authority provided under the "color of law" is allowed to stop individuals and even if necessary to search them and retain their property under certain circumstances. It is in the abuse of that discretionary power that a violation of a person's civil rights might occur. An unlawful detention or an illegal confiscation of property would be examples of such an abuse of power."

Exercise 2.4: Fourth Amendment

In Exercise2.4, students recognize that investigations can conflict with a person's right to privacy as guaranteed by the Fourth Amendment. Students should provide documented support and a logical argument for their opinions about whether the person had a legitimate expectation of privacy.

Exercise 2.5: How to Minimize Metadata in Microsoft Word Documents

This exercise is about the student’s ability to find metadata by reviewing a file’s properties. The successful student will identify five to ten types of metadata and identify those that can be deleted or removed.

PROJECTS

Project 2.1: Searching and Seizing Computers

The key to this project on search and seizure is for the student to learn more than simply the steps in an investigation. Examples of challenges would be those related to finding, collecting, transporting, or authenticating the evidence. The successful student will explain the challenges and tools that can minimize those challenges.

Project 2.2: What Motivates Hackers?

In this project, students read about hacker motivations and relate those motives to the types of e-evidence that an investigator should search for. The successful student might recognize that the motives of hackers have evolved from ego-boasting (bragging about their ability to hack into a computer) toward more financial motives or ideological motives.

Project 2.3: Global Software Piracy

In this project, students must associate crimes with the motives of the criminal who committed them. The successful student will give details about how to investigate software piracy at the university.

CASE STUDY

While students have just been introduced to many topics in the first two chapters, this case study is designed to get them thinking about how all of this has to come together to investigate electronic devices and e-evidence. Students should be able to identify what an investigator must do and not do to ensure that e-evidence is admissible. Answers should show that they have carefully considered how our activities leave evidence on computers, phones, and handheld devices.

Their answers are not expected to be detailed or completely legally accurate. Rather, answers should show that they have given consideration to all the elements of discovering and preserving admissible e-evidence.