Digital Evidence and Computer Crime, Third Edition

INSTRUCTOR'S MANUAL

By Samuel Norris

CONTENTS

Chapter 1
Foundations of Digital Forensics

Objectives

On completion of this chapter, the student will

- Recognize that there will be a digital component in nearly every crime.
- Be able to list some of the ways criminals use technology.
- Recognize that increased use of technology increases evidence.
- Be able to define "digital evidence."
- Be aware of who is concerned with proper processing of digital evidence.
- Recognize how digital forensics has changed over time.
- Recognize the purpose and importance of "best practices" and accepted standards.
- Be able to define "digital forensics."
- Be aware of how Locard's Exchange Principle applies to digital forensics.
- Recognize the difference between class characteristics and individual characteristics.
- Recognize that evidence preservation is not an absolute.
- Be aware of the steps to authenticate evidentiary data.
- Recognize the need for documenting "continuity of possession."
- Be aware that hashing is an accepted method of establishing authenticity of data.
- Recognize the need for objectivity on the part of the examiner.
- Recognize that repeatability is a requirement of forensic soundness.
- Recognize that digital evidence is volatile.
- Be aware that digital data is seen through one or more layers of abstraction.
- Recognize that "evidence dynamics" will affect the state of the digital crime scene.
- Recognize the role that applied research plays in digital forensics.

Digital evidence has come to play some part in virtually every crime. It would, in fact, be difficult to describe a crime scene that does *not* have a digital element. Criminals have always found ways to use technology to their own ends, and digital technology is no different. There is an upside to this – the more digital technology is used, the more likely that there will be resulting digital evidence.

Digital forensics has undergone a number of changes from little more than looking at the hexadecimal values on floppy media to automated forensic tools that process terabytes of data in search of digital evidence.

Digital evidence is the target of the forensic examiner, who pursues those digital elements that support (or refute) a particular scenario. However, if the evidence is to be used in court, the collection and processing must adhere to strict rules of evidence. Therefore, it is important that everyone who is involved in the legal process – law enforcement, attorneys, and the judiciary – understands the concepts of digital forensics and adheres to best practices and standard procedures.

One such concept is Locard's Exchange Principle, which proposes that something is taken and something is left behind when someone enters a crime scene. This same is true with digital

media. The substance of this exchange may possess either class characteristics or individual characteristics, the latter being more specific.

The concept that digital evidence should never be changed is *desirable* but not an absolute. There will be times where necessity dictates that evidence, by being observed, has changed. This should, however, be noted in case documentation.

The above notwithstanding, every effort should be made to properly copy the evidentiary media, and then to verify or authenticate the data collected so that the examiner can state the copied data is identical to the original. The accepted method for doing this is through "hashing," which will be covered in a later chapter.

Another issue is tracking the movement of the evidentiary data through the collection, storage, and analyzing processes. It is important establish a "continuity of possession" document that records when evidence changes hands, with whom, and why.

Two other points central to forensic methodology are: objectivity and repeatability. The first, objectivity, means that the forensic examiner seeks the truth of events, not to prove that a suspect is the perpetrator. The second, repeatability, demands that, given identical media and processes, the same results should result.

Challenges to the forensic process and digital evidence include:

1. The idea that the true data (magnetic patterns) is never observed, but rather, it is observed through some level of abstraction (the hexadecimal view of a file).
2. The concept of "evidence dynamics" – changes that creep into evidence, either by accident or error, that change the data.

Digital forensics methodology is constantly in flux – the "bad guys" figure out some way to exploit a new technology and the "good guys" develop tools to capture and document the exploit. That is the way it has always been and always will be.

Multiple Choice Questions

1. A valid definition of digital evidence is:
   a. Data stored or transmitted using a computer
   b. Information of probative value
   c. Digital data of probative value
   d. Any digital evidence on a computer

2. What are the three general categories of computer systems that can contain digital evidence?
   a. Desktop, laptop, server
   b. Personal computer, Internet, mobile telephone
   c. Hardware, software, networks
   d. Open computer systems, communication systems, embedded systems

3. In terms of digital evidence, a hard drive is an example of:
   a. **Open computer systems**
   b. Communication systems
   c. Embedded computer systems
   d. None of the above

4. In terms of digital evidence, a mobile telephone is an example of:
   a. Open computer systems
   b. Communication systems
   c. Embedded computer systems
   d. None of the above

5. In terms of digital evidence, a Smart Card is an example of:
   a. Open computer systems
   b. Communication systems
   c. Embedded computer systems
   d. None of the above

6. In terms of digital evidence, the Internet is an example of:
   a. Open computer systems
   b. Communication systems
   c. Embedded computer systems
   d. None of the above

7. Computers can be involved in which of the following types of crime?
   a. Homicide and sexual assault
   b. Computer intrusions and intellectual property theft
   c. Civil disputes
   d. All of the above

8. A logon record tells us that, at a specific time:
   a. An unknown person logged into the system using the account
   b. The owner of a specific account logged into the system
   c. The account was used to log into the system
   d. None of the above

9. Cybertrails are advantageous because:
   a. They are not connected to the physical world.
   b. Nobody can be harmed by crime on the Internet.
   c. They are easy to follow.
   d. Offenders who are unaware of them leave behind more clues than they otherwise would have.

10. Private networks can be a richer source of evidence than the Internet because:
    a. They retain data for longer periods of time.
    b. Owners of private networks are more cooperative with law enforcement.
    c. Private networks contain a higher concentration of digital evidence.
    d. All of the above.

11. Due to caseload and budget constraints, often computer security professionals attempt to limit the damage and close each investigation as quickly as possible. Which of the following is NOT a significant drawback to this approach?
    a. Each unreported incident robs attorneys and law enforcement personnel of an opportunity to learn about the basics of computer-related crime.
    b. Responsibility for incident resolution frequently does not reside with the security professional, but with management.
    c. This approach results in under-reporting of criminal activity, deflating statistics that are used to allocate corporate and government spending on combating computer-related crime.
    d. Computer security professionals develop loose evidence processing habits that can make it more difficult for law enforcement personnel and attorneys to prosecute an offender.

12. The criminological principle which states that, when anyone, or anything, enters a crime scene he/she takes something of the scene with him/her, and leaves something of himself/herself behind, is:
    a. Locard's Exchange Principle
    b. Differential Association Theory
    c. Beccaria's Social Contract
    d. None of the above

13. The author of a series of threatening e-mails consistently uses "im" instead of "I'm." This is an example of:
    a. **An individual characteristic**
    b. An incidental characteristic
    c. A class characteristic
    d. An indeterminate characteristic

14. Personal computers and networks are often a valuable source of evidence. Those involved with _____ should be comfortable with this technology.
    a. Criminal investigation
    b. Prosecution
    c. Defense work
    d. All of the above

15. An argument for including computer forensic training computer security specialists is:
    a. It provides an additional credential.
    b. It provides them with the tools to conduct their own investigations.
    c. It teaches them when it is time to call in law enforcement.
    d. None of the above.

True or False Questions

1. Digital evidence is only useful in a court of law.
   a. True
   b. False

2. Attorneys and police are encountering progressively more digital evidence in their work.
   a. True
   b. False

3. Video surveillance can be a form of digital evidence.
   a. True
   b. False

4. All forensic examinations should be performed on the original digital evidence.
   a. True
   b. False

5. Digital evidence can be duplicated exactly without any changes to the original data.
   a. True
   b. False

6. Computers were involved in the investigations into both World Trade Center attacks.
   a. **True**
   b. False

7. Computer professionals who take inappropriate actions when they encounter child pornography on their employer's systems can lose their jobs or break the law.
   a. True
   b. False

8. Digital evidence is always circumstantial.
   a. True
   b. False

9. Digital evidence alone can be used to build a solid case.
   a. True
   b. False

10. Automobiles have computers that record data such as vehicle speed, brake status, and throttle position when an accident occurs.
    a. True
    b. False

11. Computers can be used by terrorists to detonate bombs.
    a. True
    b. False

12. The aim of a forensic examination is to prove with certainty what occurred.
    a. True
    b. False

13. Even digital investigations that do not result in legal action can benefit from principles of forensic science.
    a. True
    b. False

14. Forensic science is the application of science to investigation and prosecution of crime or to the just resolution of conflict.
    a. True
    b. False

15. When a file is deleted from a hard drive, it can often be recovered.
    a. True
    b. False

Essay Questions

1. When criminals use computers, what advantages does this have from an investigative standpoint?

Answer guidance: 1) Computer activities leave trails/online activities leave cybertrails, 2) these traces/trails can be linked to the associated physical world activities, and 3) some offenders have a false sense of security when they use computers and therefore expose themselves to greater risk, giving us a clearer view of them — windows to the world.

2. What are the three general categories of computer systems that can contain digital evidence? In each category, give a specific source of digital evidence that interests you and describe the type of evidence that you might find.

Answer guidance: Open systems, communication systems, and embedded systems, examples of each are provided on page 12. Note that a server on the Internet is often an open computer system but plays a role in a communications system. Therefore, the server may have information relating to the communications on the Internet such as log files of network activities.

3. Why is it important for computer security professionals to become familiar with digital evidence?

Answer guidance: So they know how to process evidence properly in preparation for a serious incident and to protect themselves and employers against liability (see p. 14).

4. At what point should computer security professionals stop handling digital evidence and contact law enforcement?

Answer guidance: This is a difficult question that requires more than a simplistic "stop and contact law enforcement whenever they detect a crime" answer. It is unrealistic to expect an organization to report every potential criminal act to law enforcement. Computer security professionals should report incident to law enforcement when their organization's policy specifies. This presumes that some organizational thought and planning has been applied to the issue. Computer security professionals should stop handling digital evidence when the task is beyond their training and experience or when they would be committing an offense by performing an action (e.g., hacking back to intruder's computer, accessing child pornography).

5. What are the main challenges of investigating computer-related crime?

Answer guidance: There are an abundance of challenges. A summary list includes:

- Abstraction
- Messy amalgam and fragmentation
- Mutability: evidence dynamics
- Attribution: linking digital to physical
- Distributed
- Transient
- Voluminous
- Anonymity
- Diversity of technologies
- Keeping up with legislation
- Shortage of trained investigators, attorneys, judges, etc.

6. What is the difference between digital evidence, electronic evidence, and computer evidence?

Answer guidance: Computer evidence and electronic evidence refer to hardware whereas digital evidence refers to the data that is contained by hardware.

7. Describe a case reported in the media or from personal experience that demonstrates how digital evidence can be useful in the investigation of a violent crime or civil dispute.

Scenario
Describe a day in your life and the associated sources of digital evidence that your actions may have created.

Chapter 2
Language of Computer Crime Investigation

Resources

The following organizations with related resources are mentioned in this chapter.

RESOURCE	SOURCE	DESCRIPTION
DFRWS	http://www.dfrws.org	Digital Forensics Research Workshop.
ENFSI	http://www.enfsi.org	European Forensic IT Working Group.
FLETC	http://www.fletc.gov	Provides computer forensic training to law enforcement personnel.
NIST	http://www.cftt.nist.gov	Conducts tests on evidence processing tools.
NW3C	http://www.nw3c.org	Provides computer forensic training to law enforcement personnel.
SEARCH	http://www.search.org	Provides computer forensic training to law enforcement personnel.
SWGDE	http://www.swgde.org	Scientific Working Group for Digital Evidence.
USDOJ	http://www.cybercrime.gov	Computer search and seizure manual.

Objectives

On completion of this chapter, the student will

- Be aware of new terms that have arisen as technology has been used for committing crimes.
- Be aware of the difficulty in defining computer crime.
- Recognize the differences between the following terms:
  - Digital forensics
  - Computer forensics
  - Network forensics
  - Mobile device forensics
  - Malware forensics
- Recognize the difference between "forensic examination" and "forensic analysis."
- Be aware of the various roles computers may play in a crime.

Chapter Guide

Since the late 1980s there have been significant advances in investigating crime involving computers. In addition to advances in tool development, there have been refinements in the law, computer crime categories, and digital investigative methods and theory. However, because it is still an emerging field, digital forensics requires additional development and refinement. Even the term digital forensics has only recently replaced computer forensics, forensic computing, and other terms that describe the field as a whole. See pages 26-38 for more details.

Although every effort is made to prevent bugs in software used in digital investigations, they do exist and can result in evidence being lost or interpreted incorrectly. Therefore, in addition to

knowing which tools are best for a given task, digital investigators must be capable of validating the results to ensure that their results are correct. Validation involves checking and documenting the results of one tool with another either by comparing the results from both tools to ensure they are in agreement, or by using one tool to verify low-level data has been interpreted correctly by another tool. For instance, two tools should recover the same deleted files from a given file system, and all tools should calculate date-time stamps correctly.

In addition to validating their own work and tools, forensic examiners can benefit from the results of the US National Institute of Standards and Testing (NIST) Computer Forensic Tool Testing (CFTT) program. This program is currently testing hardware write blockers as well as the ability of forensic tools to acquire digital evidence from storage media and recover deleted files. This testing does not include the recovery of overwritten data using more sophisticated equipment. Some forensic laboratories can recover partially overwritten data using special equipment designed for testing hard drives called "spin stand testers." Basically, this equipment enables technicians to direct the read head to read the edges of a track that may not have been overwritten by newer data that are stored in the middle of the track. Although it is theoretically possible to recover completely overwritten data using powerful microscopes, an analysis by the US National Bureau of Economic Research suggests that this is not feasible in practice:

Can Intelligence Agencies Read Overwritten Data? A Response to Gutmann,
by Daniel Feenberg, National Bureau of Economic Research,
http://www.nber.org/sys-admin/overwritten-data-guttman.html.

The role a computer plays in a crime will dictate how it and its contents are processed. Therefore, it is important for digital investigators to understand the different roles, which are clearly described in the USDOJ's "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." The following table provides examples in each category:

	Contraband	Fruits of Crime	Instrumentality	Evidence
Hardware	Cloned mobile telephones, or hardware for intercepting communications	Stolen computers, or equipment purchased with stolen credit cards	Printer used to produce counterfeit banknotes, or scanner used to produce child pornography	Mobile phone may be evidence of parole violation even if it was not used to deal drugs
Information	Digital photographs or videos of child exploitation, or strong encryption in some countries	Valuable data stolen from computers such as bank account details	Programs used to break into computers and capture passwords	A personal diary on a computer describing details of a crime, or log files showing criminal activity

Notably, a source of evidence can fall into multiple categories. For instance, a flatbed scanner used to digitize child pornography can be considered in both the hardware as instrumentality and hardware as evidence categories.

This conceptual framework helps investigators quickly identify important sources of evidence in the large amounts of information that are common in digital investigations. In addition, these categories provide a foundation for procedures. For instance, different methods, personnel, and tools are required to process hardware as contraband (e.g., mobile phone cloning equipment) versus information as evidence.

Other categorizations of the impact of technology on crime can also be useful but have their limitations (see DECC2e, pages 31-33). Another useful categorization presented by Nigel Jones in *Digital Investigation* (Volume 1, Issue 3, www.digitalinvestigation.net) is provided below:

- The target of crime, including the denial of service attacks and viruses that are distributed to bring computer systems to a halt
- An aid to crime, allowing crimes to be committed in different and easier ways than before
- A communications tool, allowing criminals more opportunities to communicate with each other with less chance of discovery than traditional communication methods
- A witness to crime, where technology in the possession of those other than victims and suspects could provide compelling evidence of criminal activity
- A storage device, containing evidence of criminal activity whether wittingly or unwittingly stored

Discussion of these categories can help students expand their understanding of computer-related crime.

Multiple Choice Questions

1. Computers can play the following roles in a crime:
    a. Target, object, and subject
    b. Evidence, instrumentality, contraband, or fruit of crime
    c. Object, evidence, and tool
    d. Symbol, instrumentality, and source of evidence

2. The first US law to address computer crime was:
    a. Computer Fraud and Abuse Act (CFAA)
    b. Florida Computer Crime Act
    c. Computer Abuse Act
    d. None of the above

3. The following specializations exist in digital investigations:
    a. First responder (a.k.a. digital crime scene technician)
    b. Forensic examiner
    c. Digital investigator
    d. All of the above

4. The first tool for making forensic copies of computer storage media was:
    a. EnCase
    b. Expert Witness
    c. dd
    d. Safeback

5. One of the most common approaches to validating forensic software is to:
    a. Examine the source code
    b. Ask others if the software is reliable
    c. Compare results of multiple tools for discrepancies
    d. Computer forensic tool testing projects

6. An instrumentality of a crime is:
    a. An instrument used to commit a crime
    b. A weapon or tool designed to commit a crime
    c. Anything that plays a significant role in a crime
    d. All of the above

7. Contraband can include:
    a. Child pornography
    b. Devices or programs for eavesdropping on communications
    c. Encryption devices or applications
    d. All of the above

8. A cloned mobile telephone is an example of:
    a. Hardware as contraband or fruits of crime
    b. Hardware as an instrumentality
    c. Information as contraband or fruits of crime
    d. Information as evidence

9. Digital photographs or videos of child exploitation is an example of:
    a. Hardware as contraband or fruits of crime
    b. Hardware as an instrumentality
    c. Hardware as evidence
    d. Information as contraband or fruits of crime

10. Stolen bank account information is an example of:
    a. Hardware as contraband or fruits of crime
    b. Information as contraband or fruits of crime
    c. Information as an instrumentality
    d. Information as evidence

11. A network sniffer program is an example of:
    a. Hardware as contraband or fruits of crime
    b. Hardware as an instrumentality
    c. Information as an instrumentality
    d. Information as evidence

12. Computer equipment purchased with stolen credit card information is an example of:
    a. Hardware as contraband or fruits of crime
    b. Hardware as an instrumentality
    c. Hardware as evidence
    d. Information as contraband or fruits of crime

13. A printer used for counterfeiting is an example of:
    a. Hardware as contraband or fruits of crime
    b. Hardware as an instrumentality
    c. Hardware as evidence
    d. Information as contraband or fruits of crime

14. Phone company records are an example of:
    a. Hardware as contraband or fruits of crime
    b. Information as contraband or fruits of crime
    c. Information as an instrumentality
    d. Information as evidence

15. In the course of conducting forensic analysis, which of the following actions are carried out?
    a. Critical thinking
    b. Fusion
    c. Validation
16. **All of the above**

True or False Questions

1. A single crime can fall into more than one of the following categories: hardware or information as evidence, instrumentality, and contraband or fruits of crime.
    a. True
    b. False

2. The American Society of Crime Laboratory Directors (ASCLD) is the only group to establish guidelines for how digital evidence is handled in crime labs.
    a. True
    b. False

3. The NIST Computer Forensic Tool Testing Project has identified all bugs in all forensic hardware and software.
    a. True
    b. False

4. A network can be an instrumentality of a crime.
    a. True
    b. False

5. There is a general agreement as to the meaning of the term "computer crime."
    a. True
    b. False

6. Contraband is property that the private citizen is not permitted to possess.
    a. True
    b. False

7. The main reason for seizing contraband or fruits of crime is to prevent and deter future crimes.
    a. True
    b. False

8. A computer can be considered instrumentality because it contained a file that detailed the growing characteristics of marijuana plants.
    a. True
    b. False

9. The US Computer Assistance Law Enforcement Act (CALEA) that took effect in 2000 compels telephone companies to keep detailed records of their customers' calls for up to three years.
    a. True
    b. False

10. When a computer contains only a few pieces of digital evidence, investigators are authorized to collect the entire computer.
    a. True
    b. False

11. When a computer is used to forge documents or break into other computers, it is the subject of the crime.
    a. True
    b. False

12. A flatbed scanner used to digitize child pornography can be considered in both the hardware as instrumentality and hardware as evidence categories.
    a. True
    b. False

13. The terms "forensic examination" and "forensic analysis" are the same, and can be used interchangeably.
    a. True
    b. False

14. The distinction between a computer as the object and subject of a crime is useful from an investigative standpoint because it relates to the intent of the offender.
    a. True
    b. False

15. Network sniffer software is illegal to possess, and therefore is considered contraband.
    a. True
    b. False

Essay Questions

1. Discuss the benefits and shortcomings of creating specializations of crime scene experts, evidence examiners, and investigators. What are the advantages and disadvantages for requiring individuals in each specialization to pass a standard competency test?

Answer guidance: Example advantages: Specialization enables professionalization, greater expertise, and higher quality. A standard competency test helps differentiate qualified individuals from unqualified ones. Such tests also ensure that individuals have basic requisite skills to perform work competently, thus increasing consistency and reducing mistakes. Regular retesting might help keep individuals updated on technological advances. Example disadvantages: Specialization increases the cost of training and staffing. Separation of task can lead to miscommunication, hindering an investigation. It may not be possible to agree upon a standard test, particularly on an international scale. In addition, standard tests might emphasize book learning over experience — a combination of both is needed. Testing might not keep pace with technology, and if the testing body does not represent all groups in the field, it could be unfair to some.

2. What term do you think best describes this field (e.g., computer forensics, forensic computing, digital forensics) and why?

Answer guidance: Digital forensics is the most fitting for this course because just referring to computers limits the scope.

3. What roles can computers play in a crime? Give an example of each role.

Answer guidance: The most effective and widely accepted categorization is provided by the US Department of Justice as discussed on pages 34-39.

Scenario

A computer crime was committed last Wednesday. Detail the trail of digits left by your activities that day that can serve as an alibi.

Chapter 3
Digital Evidence in the Courtroom

Objectives

On completing this chapter, the student will:

- Be aware of the difference between concerns of the law and scientific knowledge.
- Be aware of the concerns of the court in regard to forensic examination of digital evidence
    - The integrity of the digital investigator
    - Authenticity of the digital evidence they present
- Be aware of the US Federal Rules of Evidence and how they relate to the authenticity of evidence.
- Recognize that the duty of experts is to present objective unbiased truth in the matters before the court.
- Recognize that digital examiners have a duty to resist influences, both subtle and overt, to form an opinion on a case.
- Recognize that every case is unique and be aware of the problem of preconceived theories.
- Be aware that in the courts, theories based on scientific truth are subordinate to the legal judgment.
- Be aware of the connection between proper evidence handling and admissibility.
- Be aware of the connection between authorization to search and admissibility.
- Be aware of four considerations when searching and seizing digital evidence:
    - Does the Fourth Amendment and/or Electronic Communications Privacy Act (ECPA) apply?
    - Have Fourth Amendment and/or ECPA requirements been met?
    - How long can investigators remain at the scene?
    - What do investigators need to reenter?
- Be aware of the role of chain of custody in assuring evidence authenticity.
- Be aware of the concept of "best evidence."
- Be aware of why hearsay evidence may not be admissible.
- Recognize that there are exceptions to the hearsay rule.
- Be aware of the application of levels of certainty to digital evidence.
- Recognize that there is a difference between direct and circumstantial evidence.
- Be aware of the four criteria for evaluating scientific theories and techniques.
- Recognize that a well-written report can bolster a weak case, and that a poorly written report can undermine a strong case.
- Be aware that a digital investigator, before taking the stand, must first be recognized as an expert by the court.

The foundation of a case involving digital evidence is proper evidence handling from proper practices of seizing, storing, and accessing evidence, and verification that evidence was properly handled.

It is important to emphasize that digital investigators will be presenting their findings to a non-technical audience. Therefore, is imperative that digital investigators are able to convey complex concepts in easier to understand terms.

Multiple Choice Questions

1. Having a member of the search team trained to handle digital evidence:
    a. Can reduce the number of people who handle the evidence
    b. Can serve to streamline the presentation of the case
    c. Can reduce the opportunity for opposing counsel to impugn the integrity of the evidence
    d. All of the above

2. An attorney asking a digital investigator to find evidence supporting a particular line of inquiry is an example of:
    a. Influencing the examiner
    b. Due diligence
    c. Quid pro quo
    d. Voir dire

3. A digital investigator pursuing a line of investigation in a case because that line of investigation proved successful in two previous cases is an example of:
    a. Logical reasoning
    b. Common sense
    c. Preconceived theory
    d. Investigator's intuition

4. A scientific truth attempts to identify roles that are universally true. Legal judgment, on the other hand, has a standard of proof in criminal prosecutions of:
    a. Balance of probabilities
    b. Beyond a reasonable doubt
    c. Acquittal
    d. None of the above

5. Regarding the admissibility of evidence, which of the following is not a consideration:
    a. Relevance
    b. Authenticity
    c. Best evidence
    d. Nominally prejudicial

6. According to the text, the most common mistake that prevents evidence seized from being admitted is:
    a. Uninformed consent

b. Forcible entry
c. Obtained without authorization
d. None of the above

7. In obtaining a warrant, an investigator must convince the judge on all of the following points except:
    a. Evidence of a crime is in existence
    b. A crime has been committed
    c. The owner or resident of the place to be searched is likely to have committed the crime
    d. The evidence is likely to exist at the place to be searched

8. If, while searching a computer for evidence of a specific crime, evidence of a new, unrelated crime is discovered, the best course of action is:
    a. Abandon the original search, and pursue the new line of investigation
    b. Continue with the original search but also pursue the new inquiry
    c. Stop the search and obtain a warrant that addresses the new inquiry
    d. Continue with the original search, ignoring the new information

9. The process of documenting the seizure of digital evidence and, in particular, when that evidence changes hands, is known as:
    a. Chain of custody
    b. Field notes
    c. Interim report
    d. None of the above

10. When assessing the reliability of digital evidence, the investigator is concerned with whether the computer that generated the evidence was functioning normally, and:
    a. Whether chain of custody was maintained
    b. Whether there are indications that the actual digital evidence was tampered with
    c. Whether the evidence was properly secured in transit
    d. Whether the evidence media was compatible with forensic machines

11. The fact that with modern technology, a photocopy of a document has become acceptable in place of the original is known as:
    a. Best evidence rule
    b. Due diligence
    c. Quid pro quo

d. Voir dire

12. Evidence contained in a document provided to prove that statements made in court are true is referred to as:
    a. Inadmissible evidence
    b. Illegally obtained evidence
    c. Hearsay evidence
    d. Direct evidence

13. Business records are considered to be an exception to:
    a. Direct evidence
    b. Inadmissible evidence
    c. Illegally obtained evidence
    d. Hearsay evidence

14. Which of the following is not one of the levels of certainty associated with a particular finding?
    a. Probably
    b. Maybe
    c. Almost definitely
    d. Possibly

15. Direct evidence establishes a:
    a. Fact
    b. Assumption
    c. Error
    d. Line of inquiry

True or False Questions

1. There is no need for any specialized training in the collection of digital evidence.
    a. True
    b. False

2. It is the duty of a digital investigator to ignore influences from any source.
    a. True
    b. False

3. The application of preconceived theories to a particular case is a good method of reducing caseload.
    a. True
    b. False

4. In the United States, the prosecution must prove guilt beyond a reasonable doubt.
    a. True
    b. False

5. Chain of custody is the process of documenting who has handled evidence, where and when, as it travels from the crime scene to the courts.
    a. True
    b. False

6. Typically, a photocopy of a document is considered hearsay evidence and is not admissible in court.
    a. True
    b. False

7. Direct evidence establishes a fact.
    a. True
    b. False

8. Coerced testimony is the most common mistake that prevents evidence seized from being admitted.
    a. True
    b. False

9. Determining whether digital evidence has been tampered with is a major concern of the digital examiner.
    a. True
    b. False

10. Exceeding the scope of a warrant is not likely to affect the admissibility of the evidence collected.
    a. True
    b. False

11. Digital evidence cannot be direct evidence because of its separation from the events it represents.
    a. True
    b. False

12. When creating an expert report, digital investigators should support assertions in their reports with multiple independent sources of evidence.
    a. True
    b. False

13. Voir dire is the process of becoming accepted as an expert by the court.
    a. True
    b. False

14. During testimony, when a lawyer appears not to be tech savvy, it is a good practice to guess what the attorney is trying to ask.
    a. True
    b. False

15. A proper response to a question that you do not know the answer to is, “I don’t know.”
    a. True
    b. False

Essay Questions

Develop a procedure for systematically examining a crime scene for digital evidence.

Answer guidance: initial entrance to the crime scene, officer safety, separate the suspect from the computer, look for removable media, written passwords, evidence of networks, etc.

Develop a format for a digital examination report.

Answer guidance: readable fonts, structure that contains a summary, the details of the report, and attachments, etc.

Hold a mock court, with the instructor acting as opposing counsel, and testify under cross-examination.

Answer guidance: thoroughly know the content of the report, don't panic (or lose your temper), etc.

Scenario

You are accompanying a raid on a suspected software pirate. What would you be looking for? What precautions would you be taking? What evidence collection considerations would you be considering?

Chapter 4
Cybercrime Law: A United States Perspective

Resources

The following useful resources are related to this chapter:

RESOURCE	SOURCE	DESCRIPTION
US DOJ	http://www.cybercrime.gov/	US DOJ cybercrime resources
COE	http://www.coe.int/Files/Cybercrime	COE cybercrime resources
SAP	http://www.sentencing-guidelines.gov.uk	UK Sentencing Advisory Panel
EPIC	http://www.epic.org/	Electronic Privacy Information Center
Findlaw	http://www.findlaw.com/01topics/10cyberspace/	Cybercrime resources

Objectives

On completion of this chapter, the student will:

- Be aware of how US law deals with the major cybercrimes.
- Be aware how US law deals with digital privacy.
- Recognize that the primary source for Federal law dealing with cybercrimes is the Computer Fraud and Abuse Act
- Recognize that the Child Pornography Protection Act was adopted by Congress out of concern for the increased proliferation of child pornography.
- Be aware that copyright infringement in the form of software piracy is a crime.
- Be aware that the Lanham Act provides protection for trademarks and trade secrets.
- Recognize that state cybercrime law is often focused on crimes of access, dissemination of malware, denial of service, computer forgery, computer fraud and theft, computer extortion, and crimes against children.
- Recognize that the constitutional freedom from unreasonable searches is the Fourth Amendment.
- Be aware that wiretapping deals with several issues:
    - Content of communications
    - Traffic data
    - Technology is not in general public use
- Recognize that there are Fifth Amendment issues relating to encryption.

Chapter Guide

This chapter contains a significant amount of material that can form the foundation for more than one lesson. The ultimate aim is to have students compare the policies and laws in the US and EU, and highlight the similarities and differences between them in the following areas:

• Fraud, forgery, intrusions, and other computer abuse
• Child pornography

• Privacy
• Search and seizure
• Jurisdiction

Technology provides criminals with new opportunities, and many existing laws do not adequately address the use of computers. Prosecution of crimes such as child exploitation, theft of intellectual property, Internet fraud, and cyberstalking has yet to be resolved, for a number of reasons. One issue is jurisdiction. If an Internet fraud is conducted in one state, via an offshore ISP, against a victim in another state – who has jurisdiction? Where did the crime take place? A related issue is extradition of criminals from other countries.

Legislation covering computer misuse has matured but continues to evolve as case law and technology develop. In the US, computer fraud and abuse are defined and addressed by the CFAA at the federal level, and by state law for the remainder of smaller offenses. In the UK and EU, fraud, forgery, and computer misuse are defined slightly differently.

Another issue is the varying definitions of, and the confusion between, "pornography," "child pornography," and "obscenity." Application of the Miller test and COPA's guidelines to determine when pornography has crossed over to obscenity has been the focus of a number of court cases, and the definitions are far from being accepted.

In regard to child pornography, at present in the US, "virtual" child pornography is still protected by the First Amendment. CPPA was an unsuccessful attempt to remove this protection, the premise being that child pornography, real or digitally created, was inherently evil. However, under UK law "pseudo-photographs" are considered illegal, and the COE includes "realistic images representing a minor engaged in sexually explicit conduct" in their definition of child pornography. The rationale for making virtual child pornography illegal is that it increases the availability of such materials and thereby increases the demand. A counterargument is that law enforcement may not be able to distinguish between virtual versus real child pornography, making it more difficult to address the illegal activities. Sentencing guidelines for child pornography convictions continues to be an area of controversy, and the discussion about sentencing in the UK is provided to stimulate discussion.

Our "right to privacy" is an equally ambiguous concept. From a legal standpoint, it is 1) the right to be free from governmental intrusion (protected by the Constitution) and 2) the protection from intrusion into our private lives by others (protected by common law). Although search and seizure requirements and procedures in the US and UK are very similar, in Europe, personal data are protected by an EU directive and by associated legislation in individual countries. Historically, the EU has offered greater privacy protection than the US, making it more difficult

for entities in these two to exchange these data. However, in response to increases in international terrorism, some EU countries are considering legislation to give authorities greater access to personal data.

Intellectual property theft is based on copyright law. Alex Haley was accused of plagiarizing parts of his epic *Roots*. Napster, KaZaA, and other peer-to-peer applications engaged in the unauthorized distribution (sharing) of copyrighted music. Legal definitions are, again, behind the times. If a data thief breaks into a computer and copies confidential data, is it theft? The data is intact and still in place. Has the owner of the data been deprived of its use?

Multiple Choice Questions

1. What is one of the most complex aspects of jurisdiction when the Internet is involved?
    a. Arranging to travel to remote locations to apprehend criminals
    b. Determining which court can enforce a judgment over a defendant
    c. Finding a court that is in two states
    d. Finding a federal court that can hear a civil suit

2. In the US, to enforce a judgment over a defendant, a court must have which of the following?
    a. Subject matter and personal jurisdiction
    b. General and limited jurisdiction
    c. Diversity and long arm jurisdiction
    d. None of the above

3. Which of the following occurred most recently?
    a. Communications Decency Act (CDA)
    b. Ashcroft v. American Civil Liberties Union
    c. Child Online Protection Act (COPA)
    d. Reno v. American Civil Liberties Union

4. The Miller test takes which of the following into account when determining if pornography is obscene?
    a. It appeals to the public interest
    b. It depicts sexual conduct in a patently offensive way
    c. It lacks any monetary value
    d. All of the above

5. In the case of New York v. Ferber, in 1982, the Supreme Court defined child pornography as:
    a. Sketches from the imagination or literary descriptions of children engaged in sexual activities
    b. Visual depictions of sexual conduct by children or by persons who look younger than their actual age
    c. Works that visually depict explicit sexual conduct by children below a specified age
    d. Any public or private materials depicting children engaged in sexual activities no matter the medium

6. Which of the following rights is not explicitly mentioned in the US Constitution?
    a. Right of the people to keep and bear arms
    b. Right of personal privacy
    c. Right of the people peaceably to assemble
    d. Right to a speedy and public trial

7. Which of the following is not a consideration in determining "fair use" of copyrighted materials?
    a. The purpose and character of the use
    b. The amount and substantiality of the portion of the copyrighted work used
    c. The expense involved in creating the original material
    d. Effect on the potential market for the work

8. The definition of a "protected computer" is, according to the CFAA:
    a. A computer that is used exclusively by a financial institution or the Federal government.
    b. A computer that is used non-exclusively by a financial institution or the Federal government and the crime affects that use.
    c. A computer that is used in state or foreign commerce or communication.
    d. All of the above.

9. Under the CFAA, the provision that is used to prosecute those who create or spread viruses, worms, and other malware is:
    a. 1030(a)(5)(A)
    b. 1030(a)(5)(B)
    c. 1030(a)(5)(C)
    d. 1030(a)(5)(D)

10. Under the CFAA, it is a Federal crime to knowingly transfer, possess, or use a means of identification of another person without being authorized, with the intent to commit or to aid or abet any unlawful activity. The session that addresses this is:
    a. 1028(a)(5)
    b. 1028(a)(6)
    c. 1028(a)(7)
    d. 1028(a)(8)

11. The legislation that made the theft of trade secrets a Federal crime was
    a. The Lanham Act
    b. The Economic Espionage Act
    c. The Child Pornography Protection Act
    d. None of the above

12. Which state does not have a law prohibiting simple hacking – gaining unauthorized access to a computer?
    a. California
    b. Texas
    c. Washington
    d. None of the above

13. The term "computer contaminant" refers to:
    a. Excessive dust found inside the computer case
    b. Viruses, worms, and other malware
    c. Spam e-mails
    d. Nigerian scam e-mails

14. In those states with legislation addressing computer forgery, contraband in the form of "forgery devices" may include:
    a. Computers
    b. Computer equipment
    c. Specialized computer software
    d. All of the above

15. Compelling a suspect to reveal passwords to provide access to encrypted media is considered to fall under the:
    a. Second Amendment
    b. Fourth Amendment
    c. Fifth Amendment
    d. Seventh Amendment

True or False Questions

1. All cybercrimes can be addressed using existing laws.
   a. True
   b. False

2. The criminal justice systems in the EU and US work in essentially the same way.
   a. True
   b. False

3. Long-arm statutes enable US states to enforce their laws on out-of-state individuals or organizations.
   a. True
   b. False

4. A single photograph can be deemed acceptable in California and obscene in Tennessee.
   a. True
   b. False

5. In the US and UK, it is legal to possess child pornography but illegal to distribute it to others.
   a. True
   b. False

6. The US First Amendment protects obscenity but not child pornography.
   a. True
   b. False

7. Virtual child pornography is illegal under UK law but not US law.
   a. True
   b. False

8. Privacy is a clearly defined concept according to US law.
   a. True
   b. False

9. The US Fourth Amendment prohibits employers from unauthorized searches and seizures of their employees.

a. True
b. False

10. In the US, the government may require a warrant to search a public area.
a. True
b. False

11. In the US, the government does not require a warrant to search through garbage/rubbish bags left outside of an individual's home.
a. True
b. False

12. In the US, the government does not require a search warrant to observe an individual's home from outside its walls using "radar-based through-the-wall surveillance systems."
a. True
b. False

13. The US Electronic Communications Privacy Act prohibits employers from unauthorized searches and seizures of their employees' electronic communications.
a. True
b. False

14. Copyright law does not prohibit individuals from downloading digital copies of protected materials without paying because it is considered fair use.
a. True
b. False

15. The Fourth Amendment addresses the citizens' right to bear arms.
a. True
b. False

Essay Questions

Debate the application of Fifth Amendment protection from incrimination to the refusal to divulge passwords to encrypted data.

Discuss the difference between pornography and obscenity.

Scenario

You are asked to describe to a non-technical jury how data are stored on a hard disk drive. How would you go about describing this and what visual aids and/or analogies would you use?

Chapter 5
Cybercrime Law: A European Perspective

Objectives

On completion of this chapter, the student will:

- Be aware of differences between super-national and national legal frameworks.
- Recognize the progression of cybercrime legislation in Europe.
- Be able to list the three the computer crime categories specified in the Cybercrime Convention:
    - Computer-integrity crime
    - Computer-assisted crime
    - Content-related crime
- Be aware of other computer related offenses:
    - Copyright infringement
    - Cyberbullying
- Be aware of various forms of jurisdiction

Cybercrime is in a constant state of flux – and cybercrime investigation is likewise constantly evolving to meet new threats. The transnational aspect of Cybercrime requires international accords to facilitate mutual assistance and mitigate jurisdictional disputes. Implicit in such accords is the need for countries to constantly update legislation to meet news Cybercrime threats.

Multiple Choice Questions

1. Which of the following courts is located in France?
    a. Court of First Instance
    b. European Court of Justice
    c. Le Conseil d'État
    d. All of the above

2. In the UK, an application for a search warrant must include which of the following?
    a. Reasonable grounds for believing that a crime has been committed
    b. A specific description of the premises to be searched
    c. Which law has been broken
    d. All of the above

3. How do Europe and North America address the challenges of jurisdiction when a computer crime involves both continents?
    a. Search warrants
    b. Treaties
    c. Presidential intervention
    d. All of the above

4. The English Sentencing Advisory Panel (SAP) categorized the increasing seriousness of child pornography material into five levels. Which of the following is considered the worst, level 5?
    a. Sadism or bestiality
    b. Sexual activity between children or solo masturbation by a child
    c. Non-penetrative sexual activity between adults and children
    d. Penetrative sexual activity between adults and children

5. The EU Framework Decision makes illegal access to information systems (intentional, without right). Member states are required to ensure that this is:
    a. Handled as a civil court issue
    b. Punishable as a criminal offense
    c. The responsibility of the owner of the computer system
    d. Handled as a reprimand only

6. The Council of Europe Convention on Cybercrime introduces three categories of computer offense. The most serious category is:
    a. Computer-assisted crimes

b. Computer-related crimes
c. Computer-integrity crimes
d. Computer malfeasance crimes

7. An example of a content-related crime would be:
    a. Cyberstalking
    b. Child pornography
    c. Hacking
    d. None of the above

8. Hacking is an example of:
    a. Computer-assisted crime
    b. Computer-related crime
    c. Computer-integrity crime
    d. Computer malfeasance crime

9. Forgery is an example of:
    a. Computer assisted crime
    b. Computer-related crime
    c. Computer-integrity crime
    d. Computer malfeasance crime

10. In the UK, prosecution of child pornography falls under what Act?
    a. The Protection of Children Act of 1978
    b. The Crimes Against Children Act of 1996
    c. The Council of Europe Convention on Cybercrime
    d. None of the above

11. In Ireland, the Non-Fatal Offences Against the State Act of 1997 specifically addresses:
    a. Computerized welfare fraud
    b. Cyberbullying
    c. Nigerian scams
    d. Hacking

12. The Netherlands claims universal jurisdiction for the crime of:
    a. Attacks on the King
    b. Transnational computer crimes
    c. Terrorist network activity
    d. Malware distribution

13. Jurisdiction claims may be based on:
    a. Location of the perpetrator's computer
    b. Location of the victim's computer
    c. Location of intermediary computers
    d. All of the above

14. In the civil-law countries, such as the Netherlands, criminal law is "inquisitional" where:
    a. The judge takes an active role in "finding the truth"
    b. The judge takes a more passive role, with "truth-finding" assigned to prosecution and defense
    c. The judge and attorneys from both prosecution and defense meet in private chambers to determine guilt or innocence.
    d. The public serves as judge, with prosecution and defense presenting their case in a public forum.

15. England became the first European country to enact a law to address computer crime specifically. This law – the Computer Misuse Act – was enacted in:
    a. 1985
    b. 1990
    c. 1995
    d. 2000

True or False Questions

1. All cybercrimes can be addressed using existing laws.
    a. True
    b. False

2. The criminal justice systems in the EU and US work in essentially the same way.
    a. True
    b. False

3. In the UK, it is legal to possess child pornography but illegal to distribute it to others.
    a. True
    b. False

4. In the UK, downloading child pornography is equated with "making" illegal material according to the legal definition.
    a. True
    b. False

5. Virtual child pornography is illegal under UK law.
    a. True
    b. False

6. According to the CoE Convention on Cybercrime, it is not illegal to break into a computer provided the intruder does not cause any damage.
    a. True
    b. False

7. "Online grooming" was criminalized by the Lanzarote Convention.
    a. True
    b. False

8. Scotland has specific legislation addressing cyberbullying.
    a. True
    b. False

9. In Irish computer crime law, jurisdiction is often integrated into the legislative section setting out the offense.
    a. True

b. False

10. In England, child prostitution and pornography are scheduled offenses to the English Serious Crime Act 2007.
    a. True
    b. False

11. European law is civil-based, whereas the common-law countries are considered an adversarial system.
    a. True
    b. False

12. In the EU, crimes like illegal access, illegal interception, and data interference are categorized as computer-integrity crimes.
    a. True
    b. False

13. In the EU, computer-assisted crimes consist of those crimes which cannot be committed in the absence of computers or computer networks.
    a. True
    b. False

14. In the EU, content-related crimes relate to traditional offenses where computers are tools rather than targets but, unlike computer-assisted crimes it is the content of data rather than the result of an action that is the core of the offense.
    a. True
    b. False

15. Data interference is the intentional "serious hindering without right to the functioning of a computer system."
    a. True
    b. False

Essay Questions

Discuss the difficulties an examiner might encounter in a transnational investigation.

Answer guidance: jurisdiction, treaties, reciprocity, counterparts in other countries.

Research agencies that you would need to contact for five nations outside of Europe.

Answer guidance: Check the CIA Factbook for information on government agencies, follow up.

Scenario

You have been notified of the existence of threatening e-mails being sent to the CEO of your company. An examination of the e-mails revealed that they originated from outside of the country.

Describe the steps you would take in your investigation. In particular, address the issue of jurisdiction and locating your counterparts in the target country.

Chapter 6
Conducting Digital Investigations

Objectives

On completion of this chapter, the student will:

- Be able to discuss various digital investigation process models.
  - Physical model
  - Staircase model
  - Evidence flow model
  - Subphase model
  - Roles and responsibilities model
- Recognize that there are other activities inherent in conducting an investigation.
  - A triggering event
  - Authorization to precede
  - Threshold considerations
  - Transportation
  - Verification
  - Case management
- Recognize the application of the scientific method to digital investigations.
  - Observation
  - Hypothesis
  - Prediction
  - Experimentation/testing
  - Conclusion

Chapter Guide

Following the twelve steps described in this chapter increase the likelihood that an investigation will lead to the truth and will serve justice. More specifically, the ultimate aim of the model covered in this chapter is to help investigators ascend a sequence of steps that are generally accepted, reliable, and repeatable, and lead to logical, well-documented conclusions of high integrity. To fully appreciate the flexibility and power of this model, it is necessary to explore how it applies to different types of investigations. For instance, the Incident Handling section of the EDUCAUSE Effective Security Practices Guide (http://www.educause.edu/security/guide) outlines how this methodology is applied to computer security incidents. In addition, it is instructive to compare this model with others such as the one described in "Getting Physical with the Digital Investigation Process" by Carrier and Spafford (available online at http://www.ijde.org/docs/03_fall_carrier_Spa.pdf).

The general discussions about remaining objective, overcoming preconceived theories, and the differences between scientific and legal truths provide an important foundation for all investigations. Exercises that challenge students to question assumptions and to construct logical arguments are useful in the introductory level courses. Several other key concepts within the investigative process should be emphasized:

- Locard's Exchange Principle
- Individual versus class characteristics
- Continuity of offense
- Examination versus analysis

Locard's Exchange Principle states that anyone or anything entering a crime scene leaves something behind or takes something with him when he leaves. Although this principle was developed nearly a century ago for investigations in the physical world, it applies to crime in the digital realm. For example, a threatening e-mail creates a trail from the sender's computer, on e-mail servers that handle the message and on the recipient's computer. These exchanges of digital evidence and the resulting cybertrails enable investigators to establish the continuity of offense and link online activities to a specific computer or individual.

Notably, investigators can also inadvertently cause evidence exchange when they enter or leave a crime scene. Adherence to standard operating procedures helps minimize such spoliation of digital crime scenes, and thorough documentation helps reduce the resulting confusion.
A "class characteristic" is a general feature shared with similar items such as Kodak digital cameras that embeds the make and model names in the photographs they take. An "individual characteristic" is a unique feature specific to a particular thing, place, person, or action. For example, a scratch on a camera lens that appears in photographs it takes, a distinct monument in the background of a photograph, or the defendant's face appearing in a photograph are all individual characteristics that may help investigators associate the photograph with its source i.e., a particular camera, location, or person. See the example on page 99.

Students often think of IP addresses in e-mail headers or network packets as an individual characteristic. However, an IP address in an e-mail header is not necessarily unique to a specific computer. E-mail messages from several computers will have the same source IP address when they are connecting through a Web proxy or NAT device. Computers accessing the Internet via dial-up (PPP) connections are assigned IP addresses within a certain range using DHCP – two computers dialing in at different times may be assigned the same IP address. Denial Of Service attack tools often use randomly generated source IP addresses to make it more difficult to determine the source of the attack. Therefore, the IP address is a class characteristic that must be

combined with other class characteristics in the e-mail header (i.e., date and time) or network packet to determine which computer was involved.

The importance of class characteristics of digital evidence cannot be overstated. Digital evidence examiners use class characteristics to determine what type of data are in files, and thus what type of information they can extract from them. Examiners also use class characteristics to group like files and filter irrelevant groups to reduce the amount of data they must deal with. Ultimately, class characteristics can combine to narrow the focus of an investigation to a particular group of suspects, computers, or certain geographic regions.

As an investigation moves from one computer to another, the examiner should examine each system to establish the path that data relating to the offense took in order to reach its destination. Searching for "continuity of offense" substantiates the examiner's findings and adds weight to evidence found. See page 99 for more information.

Many people incorrectly think of examination as synonymous with analysis when in fact these are two very different processes. Examination is the process of extracting and preparing data for analysis. The examination process involves data recovery, translation, reduction, organization, and searching. A thorough examination results in all relevant data being organized and presented in a manner that facilitates detailed analysis. Analysis involves gaining an understanding of and reaching conclusions about the incident based on evidence produced during the examination process. Analysis also involves assessing key findings through experimentation, fusion, correlation, and validation.

A checklist is provided here as an example of what investigators look for when conducting a digital investigation. This type of checklist helps digital investigators document important details and contributes to case management by helping them keep track of what they have found.

Crime Scene Checklist						Case Number:		
Date:		Investigator:				Location:		
Case Description:								
COMPUTER								
Type:	□ rack/server	□ desktop	□ laptop			Make/model:		
□ PDA	□ cell phone	□ other:						
OS:	□ Linux	□ Solaris	□ Win NT/XP	□ Mac OS X	□ AIX			
	□ BSD	□ HP-UX	□ Win 95/98	□ Mac OS 8/9	□ other:			
Network interface:						SCSI interface:		
Seized by:						Authorization: □ warrant □ other:		
State when seized:	□ on	□ off	□ standby/hibernation	□ other:				
Shutdown method:	□ normal	□ cut power	□ unknown			RAM: □ KB □ MB		
S/N:						Evidence No.:		
CMOS date/time:						Photograph Exhibit No.:		
Actual date/time:						Usage/ownership history:		
INTERNAL STORAGE								
HDD 0:	Make/model:		S/N:			Connection/jumpers:		
	MD5 hash value:							
HDD 1:	Make/model:		S/N:			Connection/jumpers:		
	MD5 hash value:							
HDD 2:	Make/model:		S/N:			Connection/jumpers:		
	MD5 hash value:							
HDD 3:	Make/model:		S/N:			Connection/jumpers:		
	MD5 hash value:							
Acquisition:	□ dd	□ EnCase	□ FTK	□ ImageMaster	□ other:			
EXTERNAL STORAGE DEVICES								
Type		**Internal**	**External**			**Type**	**Internal**	**External**
3.5 Floppy		□	□			DVD read or write	□	□
Zip/Jazz		□	□			Backup tapes	□	□
CD read or write		□	□			Other:		
Notes:								
NETWORK								
LAN type:	□ none	□ Ethernet	□ 802.11	□ other:				
WAN type:	□ dial-up	□ DSL	□ cable	□ T1				
Notes:								
LOGS								
Authentication	□ RADIUS/ TACACS	□ Web	□ POP/IMAP	□ other:				
Application	□ HTTP	□ FTP	□ SMTP	□ other:				
System	□ NT Event Log	□ syslog	□ wtmp	□ other:				
Network	□ Firewall	□ IDS	□ NetFlow	□ other:				
State tables	□ Firewall	□ Switch	□ Router	□ other:				
Notes:								

Multiple Choice Questions

1. Standard operating procedures (SOPs) are important because they:
    a. Help individuals avoid common mistakes
    b. Ensure that the best available methods are used
    c. Increase the probability that two forensic examiners will reach the same conclusions when they examine the evidence
    d. All of the above

2. The goal of an investigation is to:
    a. Convict the suspect
    b. Discover the truth
    c. Find incriminating evidence
    d. All of the above

3. An investigation can be hindered by the following:
    a. Preconceived theories
    b. Improperly handled evidence
    c. Offender concealment behavior
    d. All of the above

4. When you have developed a theory, what can you do to confirm that your hypothesis is correct?
    a. Predict, based on your hypothesis, where artifacts should be located
    b. Perform experiments to test results and rule out alternate explanations
    c. Conclude, based on your findings, whether the evidence supports the hypothesis
    d. All of the above

5. Which of the following is NOT a class characteristic of files on magnetic media:
    a. Extension (e.g., .jpg, .exe)
    b. Date-time stamp (e.g., 02/28/2004 03:00 PM)
    c. Name (e.g., encase.exe)
    d. Directory structure

6. Which of the following would be considered an individual characteristic?
    a. The originating IP address in a network packet or e-mail header
    b. A scratch on the glass of a flatbed scanner or digital camera lens
    c. Date-time stamps of files on a disk or entries in a database
    d. All of the above

7. When digital photographs containing child pornography are found on a home computer, investigators can assert that:
    a. Someone in the house transferred the photographs onto the computer from a disk or the Internet.
    b. Someone in the house took the photographs with a digital camera and transferred them directly onto the computer.
    c. Someone gained unauthorized access to the computer via the Internet and transferred the photographs onto the computer.
    d. None of the above.

8. Forensic examination involves which of the following:
    a. Assessment, experimentation, fusion, correlation, and validation
    b. Seizure and preservation
    c. Recovery, harvesting, filtering, organization, and search
    d. All of the above

9. Forensic analysis involves the following:
    a. Assessment, experimentation, fusion, correlation, and validation
    b. Seizure and preservation
    c. Recovery, harvesting, filtering, organization, and search
    d. All of the above

10. The first step in applying the scientific method to a digital investigation is to:
    a. Form a theory on what may have occurred
    b. Experiment or test the available evidence to confirm or refute your prediction
    c. Make one or more observations based on events that occurred
    d. Form a conclusion based on the results of your findings

11. Which of the following should the digital investigator consider when arranging for the transportation of evidence?
    a. Should the evidence be physically in the possession of the investigator at all times?
    b. Will the evidence copies be shared with other experts at other locations?
    c. Will there be environmental factors associated with the digital media?
    d. All of the above

12. In the Staircase Model, why is case management shown spanning across all of the steps in the process model?

a. Case documents are intangible objects that can be held.
b. Case management provides stability and enables investigators to tie all relevant information together.
c. Case management documents the process function.
d. None of the above.

13. Process models have their origins in the early theories of computer forensics which defined the field in terms of a _____ process.
    a. Complicated
    b. Difficult
    c. Linear
    d. Polymorphic

14. Generating a plan of action and obtaining supporting resources and materials falls under which step in the digital investigation?
    a. Preparation
    b. Survey/identification
    c. Preservation
    d. Examination and analysis

15. The process model whose goal is to completely describe the flow of information in a digital investigation is known as:
    a. The Physical Model
    b. The Staircase Model
    c. The Evidence Flow Model
    d. The Subphase Model

True or False Questions

1. Not all incidents should be fully investigated nor do they all deserve the same priority and attention.
    a. True
    b. False

2. The scientific method uses computers to verify findings in an investigation.
    a. True
    b. False

3. The legal truth is always in agreement with the scientific truth in an investigation.
    a. True
    b. False

4. Forensic examination and forensic analysis are separate processes.
    a. True
    b. False

5. When a network is involved in a crime, investigators must seize and preserve all systems on the network.
    a. True
    b. False

6. When seizing a computer, it is always acceptable to lose the contents of RAM.
    a. True
    b. False

7. Case management is a critical part of digital investigations.
    a. True
    b. False

8. Beebe and Clark contend that most investigative process models are too low level.
    a. True
    b. False

9. The process model whose primary strength is a notion of a continuous flow of information is known as the Subphase Model.
    a. True

b. False

10. Of particular significance in the scientific method is the weight attached to finding evidence which supports a particular hypothesis.
    a. True
    b. False

11. Evidential artifacts found in the experimentation and testing process of the scientific method which are compatible with a particular hypothesis can be taken as proof of the hypothesis.
    a. True
    b. False

11. Preparation for the preservation step ensures that the best evidence can be preserved when the opportunity arises.
    a. True
    b. False

12. If alternative theories are suggested later, digital investigators have an obligation to reevaluate their findings.
    a. True
    b. False

13. Forensic examination is the process of extracting, viewing, and analyzing information from the evidence collected.
    a. True
    b. False

14. Survey/triage forensic inspection is the targeted review of all available media to determine which items contain the most useful evidence and require additional processing.
    a. True
    b. False

Essay Questions

1. Why is it important to process digital evidence properly while conducting an investigation?

Answer guidance: Proper evidence processing is essential because digital evidence is fragile and often transient (see Section 1.3) – if it is not processed using proper procedures and tools it may be damaged and deemed inadmissible. Evidence is the foundation of a case and if important evidence is excluded because of improper processing, this can make it difficult to prove a case.

Additionally, weak evidence can lead to incorrect conclusions and miscarriages of justice.

2. What is Locard's Exchange Principle? Give an example of how this principle applies to computer crime.

Answer guidance: Locard's Exchange Principle is one of the cornerstones of forensic science. The principle is that anyone, or anything, entering a crime scene takes something of the scene with them, and leaves something of themself behind when they depart from the scene. Such evidence transfer occurs in both the physical and digital realms and can be useful in Internet investigations for establishing compelling links between the offender, victim, and crime scene.

Also, investigators can inadvertently participate in the exchange of evidence, resulting in evidence dynamics. In addition to transfer between people and crime scenes, keep in mind that evidence transfer also happens between victims and offenders.

3. How are class characteristics useful in an investigation? Give an example involving digital evidence.

Answer guidance: Investigators can use class characteristics to determine what types of data are in files, and thus what type of information they can extract from them. Digital evidence examiners use class characteristics to group like files and filter irrelevant groups to reduce the amount of data they must deal with. Ultimately, class characteristics can combine to narrow the focus of an investigation to a particular group of suspects, computers, or certain geographic regions.

4. How would you search for all image files on a disk? Explain the rationale of your approach.

Answer guidance: In some cases, it may be sufficient to search for files using file extensions of common graphics formats like .jpg and .gif. Although this approach may result in sufficient incriminating evidence to proceed, it does not recover all files on the disk. Searching a disk for

class characteristics such as the file headers of common graphics formats will locate more files.

Additionally, it is necessary to examine “special” files such as Zip archives, encrypted files, etc., to determine if they contain image files. It goes without saying that you perform all of your operations on a copy or a write-protected original but I still like to hear you say it.

Chapter 7
Handling a Digital Crime Scene

Objectives

On completion of this chapter, the student will:

- Understand that crime scene investigation is the first, most crucial step in the forensic process.
- Be aware of sources for digital crime scene processing guidelines.
- Be able to list fundamental principles for digital crime scene processing.
- Be aware of the role of authorization in crime scene processing.
- Understand that a plan should be developed for processing a crime scene.
- Be aware of the steps to preserve the digital crime scene.

Chapter Guide

Although no two digital crime scenes will ever be the same, the application of accepted methods and best practices goes a long way to assuring that the scene is protected and digital evidence is preserved.

The ultimate aim of investigative models is to help digital investigation take steps that are generally accepted, reliable, and repeatable.

Application of the scientific method to crime scene processing and digital investigation provides a rigor to the processes involved. Adhering to pre-existing policies and procedures provides consistency and thoroughness, and ensures that the best available methods – the best practices – are followed.

Multiple Choice Questions

1. The following organizations have published guidelines for handling digital crime scenes:
    a. US Secret Service
    b. Association of Chief Police Officers
    c. US Department of Justice
    d. All of the above

2. When a first responder encounters technology or equipment that he is not familiar with, the recommended course of action is to:
    a. Seize the equipment as if it were a known device
    b. Seek assistance from a more experienced digital investigator
    c. Leave that particular piece of equipment at the crime scene
    d. Ask the suspect for details on the equipment

3. When preparing a questionnaire for interviewing individuals of the crime scene which of the following should NOT be requested:
    a. Passwords
    b. Encryption keys
    c. Admission of guilt
    d. Details on removable storage

4. When entering a crime scene, the initial survey should:
    a. Include user manuals
    b. Involve tracing cables
    c. Collect relevant data such as passwords and account details
    d. All of the above

5. Examples of data that should be immediately preserved include:
    a. USB drives
    b. Digital picture frames
    c. System and network information
    d. USB bracelets

6. The crime scene preservation process includes all but which of the following:
    a. Protecting against unauthorized alterations
    b. Acquiring digital evidence
    c. Confirming system date and time
    d. Controlling access to the crime scene

7. A thorough crime scene survey should include:
    a. Manuals for software applications
    b. Removable media
    c. Mobile devices
    d. All of the above

8. The challenge to controlling access to a digital crime scene is that:
    a. Information may be stored on Internet servers in different locations.
    b. The computer may be shared.
    c. The computer case may be locked.
    d. None of the above.

9. In the case where digital investigators dealing with distributed systems need to collect data from remote sites, the following procedure is recommended:
    a. Notify personnel at the remote sites to leave everything as is, and arrange for travel to the remote locations
    b. Notify personnel at the remote sites to shut down all systems and send the hard drives to the forensic lab
    c. Utilize remote forensics tools to acquire data from the remote sites' RAM as well as the hard drives
    d. None of the above

10. When presenting evidence on an organizational network, the digital investigator may require the assistance of:
    a. System administrators
    b. The CEO of the organization
    c. The CSO (Chief Security Officer)
    d. Additional forensic investigators

11. Which of the following is not a safety consideration for a first responder?
    a. Additional personnel to control those present at the crime scene
    b. Protection against ELF emanations from monitors
    c. Proper tools for disassembling and reassembling computer cases
    d. Protective gloves and eyewear

12. Digital investigators like to preserve every potential source of digital evidence; however, they are constrained by:
    a. The law

b. Resources
c. The interests of business
d. All of the above

13. During the initial survey of a crime scene, why it is necessary to photograph or videotape the area and items of potential interest in their current state?
    a. This simplifies inventorying the crime scene.
    b. Photographing items to be seized records their actual condition, and precludes damage claims when the items are returned to the offender.
    c. To record the fact that a particular item was actually found at the crime scene.
    d. None of the above.

14. Why is the first step to secure the physical crime scene by removing everyone from the immediate area?
    a. To prevent them from contaminating evidence
    b. To prevent them from asking questions about the case before they can be interviewed
    c. To give them time to fill out a personal information survey
    d. To keep them from blocking the view when photographs are being taken

15. When a piece of evidence has both a biological and a digital component, who should process it first?
    a. The crime scene technician, because biological artifacts are much more fragile
    b. The digital investigator, because processing the biological artifacts will destroy digital evidence
    c. Neither; the evidence should be preserved and transported to the lab for processing
    d. Both the crime scene technician and the digital investigator, in a cooperative effort, assuring that the biological evidence is collected in a way that does not damage the digital component

True or False Questions

1. When first entering a crime scene, the first responder should immediately focus on the computers and technology.
a. True
b. False

2. Since crime scenes are typically pretty much the same, very little planning needs to take place prior to first entering the scene.
a. True
b. False

3. On entering a crime scene, an investigator notes that a piece of equipment with antennas attached is connected to one of the target computers. Since this indicates a wireless connection, it is advisable to either disconnect or disable the piece of equipment.
a. True
b. False

4. In most situations, it is advisable to let the physical crime scene technicians, under the direction of the forensic investigator, process the scene first.
a. True
b. False

5. The likelihood of collecting notable information from a running computer is relatively small, so it is safe to shut down any running computer to preserve the data on the hard drive.
a. True
b. False

6. When shutting down a live system it is generally recommended to unplug the power from the back of the computer.
a. True
b. False

7. The proper collection of evidence at a crime scene is crucial in terms of admissibility in court.
a. True
b. False

8. When performing triage at a crime scene, an important first step is to turn on any computers that are off and immediately look for items of evidence.
a. True
b. False

9. Computer security professionals should obtain instructions and written authorization from their attorneys before gathering digital evidence relating to an investigation with an organization.
a. True
b. False

10. The Fourth Amendment, like ECPA, only applies to the government, not the private sector.
a. True
b. False

11. When an organization itself is under investigation, it is always feasible to collect all the data for every system.
a. True
b. False

12. The contents of volatile memory are becoming more and more important.
a. True
b. False

13. The decision to seize an entire computer versus create a forensic duplicate of the internal hard drive will be influenced by the role of the computer.
a. True
b. False

14. When seizing a computer, it is advisable to remove the computer's case and to unplug power cables from hard drives.
a. True
b. False

15. Capturing volatile data or specific files from a live system is a straightforward process usually handled by the first responder.
a. True
b. False

Essay Questions

1. What considerations are there when developing a crime scene plan?

Answer guidance: physical layout and access, equipment, personnel separation, connectivity issues.

2. What information would you provide when preparing a search warrant?

Answer guidance: specific details of the items to be seized, probable cause for seizing the property, location to be searched, types of evidence that will be seized, etc.

Scenario

You are participating in the pre-raid briefing of a software piracy site. Your part in the raid is to present and seize all the computers at the site.
What questions would you ask the intelligence briefer about your part in the mission?
What information and recommendations would you provide to the briefing?

Chapter 8
Investigative Reconstruction with Digital Evidence

Objectives

On completion of this chapter, the student will:

- Be aware that crime is not always committed in a straightforward manner.
- Recognize that investigative reconstruction refers to the systematic process of piecing together evidence.
- Recognize the need to conduct equivocal forensic analysis to assure that evidence is evaluated objectively.
- Be aware that the results of investigative reconstruction may need additional influences and preconceived theories.
- Recognize that evidence that is used to reconstruct crimes falls into three categories:
    a. Relational
    b. Functional
    c. Temporal
- Recognize the role of victimology in the course of an investigation.
- Recognize the connection between crime scene characteristics and modus operandi.
- Be aware that the two most common types of reports are:
    a. A threshold assessment (a preliminary summary of findings)
    b. A full investigative report

Chapter Guide

Investigatory reconstruction provides a methodology for gaining a better understanding of a crime and focusing an investigation. Objectively reviewing available evidence provides a greater understanding of the case.

As the situation dictates, the investigator may prepare a threshold assessment or a full investigative reconstruction.

Multiple Choice Questions

1. The process of evaluating available evidence objectively, independent of the interpretations of others, to determine its true meaning is referred to as:
    a. Equivocal forensic analysis
    b. Investigative reconstruction
    c. Threshold assessment
    d. Behavioral imprints

2. The words that an offender uses on the Internet, the tools that an offender uses online, and how an offender conceals his identity and criminal activity are referred to in the text as:
    a. Investigation reconstruction
    b. Threshold assessment
    c. Behavioral imprints
    d. Crime scene analysis

3. Investigative reconstruction is composed of three different forms. Which of the following is NOT one of those three forms?
    a. Functional
    b. Intentional
    c. Relational
    d. Temporal

4. Creating a histogram of times to reveal periods of high activity is an example of which form of investigative reconstruction?
    a. Functional
    b. Intentional
    c. Relational
    d. Temporal

5. The investigation and study of victim characteristics is known as:
    a. Criminal profiling
    b. Behavioral imprints
    c. Victimology
    d. Crime scene analysis

6. Why should victimology include a thorough search of the Internet for cybertrails?
    a. Because the Internet can significantly increase the victims risk.
    b. Because it is well known that even traditional criminal offenses are documented on the Internet.
    c. Because nearly everyone uses the Internet.
    d. None of the above.

7. The type of report that is a preliminary summary of findings is known as:
    a. SITREP
    b. Threshold Assessment report
    c. Full investigative report
    d. Field notes

8. According to the text, the distinguishing features of a crime scene as evidenced by the offender's behavioral decisions regarding the victim and the offense location are known as:
    a. Hard evidence
    b. Fruit of the poison tree
    c. Caveat emptor
    d. Crime scene characteristics

9. In crimes against individuals the _____ period leading up to the crime often contains the most important clues regarding the relationship between the offender and the victim.
    a. 24-hour
    b. 48- hour
    c. 60-minute
    d. 15-minute

10. One of the most important things to establish when a computer is directly involved in the commission of a crime is:
    a. Where the computer was purchased
    b. What operating system is in use
    c. Who or what was the intended victim or target
    d. None of the above

11. An example of online behavior that puts an individual at higher risk for cyberstalking is:
    a. Using your real name online
    b. Putting personal information in your profile
    c. Posting photographs on a social networking page

d. All of the above

12. In the movie *Home Alone* one of the burglars would always turn the water on in the sinks so that the house would be flooded when the owners returned. In terms of crime scene characteristics, this is an example of:
    a. Psychotic episode
    b. Signature-oriented behavior
    c. Modus operandi
    d. Vandalism

13. The totality of choices an offender makes during the commission of a crime are referred to as:
    a. The criminal's MO
    b. Crime scene characteristics
    c. Tangible evidence
    d. None of the above

14. Because seemingly minor details regarding the offender can be important, investigators should get into the habit of contemplating which of the following:
    a. What the offender brought to the crime scene
    b. What the offender took from the crime scene
    c. What the offender changed at the crime scene
    d. All of the above

15. One reason digital investigators write threshold assessments more often than full reports is because:
    a. They will be included in a final report, and so, distribute the time for final report preparation over the entire period of the investigation.
    b. They keep their supervisor aware of their productivity.
    c. They take less time to prepare and may be sufficient to close out an investigation.
    d. They serve as field notes for the investigator.

True or False Questions

1. "Investigative reconstruction" refers to the systematic process of piecing together evidence and information gathered during an investigation to gain a better understanding of what transpired between the victim and the offender during a crime.
    a. True
    b. False

2. Investigative reconstruction can be used to locate concealed evidence.
    a. True
    b. False

3. The functional form of investigative reconstruction answers the questions "Who?" "What?" and "Where?"
    a. True
    b. False

4. Minor details regarding the offender are unimportant, and can safely be ignored.
    a. True
    b. False

5. The temporal form of investigative reconstruction helps identify event sequences and patterns.
    a. True
    b. False

6. The machine with an old operating system, no patches, and many services running, located on an unprotected network, containing valuable information, and with a history of intrusions or intrusion attempts, is at low risk of being broken into.
    a. True
    b. False

7. Victimology is the investigation and study of victim characteristics.
    a. True
    b. False

8. When assessing the risk of a target computer, investigators should determine if the offender needed a high level of skill.
    a. True

b. False

9. Different offenders can use the same method of approach for control for very different reasons; however, it is possible to make reliable generations on the basis of individual crime scene characteristics.
    a. True
    b. False

10. When a computer is the target of an attack, it is also useful to determine if the system was at high or low risk of being targeted.
    a. True
    b. False

11. A threshold assessment report may have a similar structure to a full investigative report but includes more details and has firmer conclusions based on all the evidence available.
    a. True
    b. False

12. Threshold assessments have eliminated the need for digital investigators to write full reports.
    a. True
    b. False

13. Among the more informative aspects of the offender-victim relationships are victim risk and the effort than an offender was willing to make to access a specific victim.
    a. True
    b. False

14. Although it is possible that the Internet can significantly increase the victim's risk, it is not necessary for victimology to include a thorough search for cybertrails.
    a. True
    b. False

15. Forensic analysis and reconstruction only include evidence that was left at a crime scene and are intrinsically limited.
    a. True
    b. False

Essay Questions

1. Explain why it can be difficult to determine if someone took a copy of a digital file.

Answer guidance: most operating systems do not mark a file that has been copied, information may be found in log files, the system may contain information about remote storage devices that have been attached.

2. Explain why an offender's choice of weapon is significant to an investigation.

Answer guidance: The weapon is the source of control over the victim, whether it is a gun or a computer. Different offenders rely on implied or actual threats. The offender's approach shows his confidences, concerns, intents, and motives.

Scenario

Two of three Porcine brothers had their houses systematically destroyed by a large Lycan. In fear for their lives, they sought shelter with a third brother. Suspecting that his house would also come under attack, he reinforced the structure and added certain countermeasures that would come into play only if the perimeter was breached. Indeed, an attack on his house was mounted, and the perimeter was breached – resulting in the demise of the intruder.

When police arrived, the three Porcine brothers were charged with negligent homicide. The house was secured as a crime scene.

(Follow-up: all charges were dropped when the brothers cited castle doctrine and self defense.)

Prepare a threshold assessment based on the information and crime scene provided above.

Chapter 9
Modus Operandi, Motive, and Technology

On completion of this chapter, the student should:

- Be aware that introduction of any new technologies may have unintended consequences.
- Recognize that the technology is not evil – however, its application may be.
- Recognize that "modus operandi" answers the "How" part of the investigation.
- Recognize that adopting new technologies into a criminal modus operandi is not new.
- Recognize that "motive" answers the "Why" part of the investigation.
- Be aware that "offense behaviors" classify criminal acts into discrete categories:
    a. Power reassurance
    b. Power assertive
    c. Anger retaliatory
    d. Sadistic
    e. Opportunistic
    f. Profit oriented
- Recognize that using the matrix of offense behaviors, it is possible to take a specific offense and apply it to each behavior.
- Be aware of some of the current technologies, and how they are used by criminals.

The students should understand that technology, for the most part, is not inherently good or bad – it simply *is*. It is the application of that technology that is important. Criminals are quick to see how a new technology can be adapted to their purposes. The forensic examiner's job is to analyze that new technology, first of all to see how the technology was implemented, and second of all to determine if the technology has any value as a tool in a forensic investigation.

Multiple Choice Questions

1. An unintended consequence of the Advanced Research Projects Agency's development of a mechanism for ensured communication between military installations was:
    a. Mainframe computing
    b. The Internet
    c. Microwave communication
    d. The Ada programming language

2. Modus operandi (MO) is a Latin term that means:
    a. Seize the data
    b. Ways and means
    c. Operator error
    d. A method of operating

3. Motive reflects _____ the crimes were committed.
    a. How
    b. Why
    c. Where
    d. When

4. A criminal's set of learned behaviors that can evolve and develop over time are referred to as:
    a. Motivational typology
    b. Offense behaviors
    c. Modus operandi
    d. The none of the above

5. The emotional, psychological, or material need that that impels, and is satisfied by, a behavior is known as:
    a. Motive
    b. Modus operandi
    c. Offense behaviors
    d. Offender behaviors

6. Which of the following is NOT an offense behavior?
    a. Motivational typology
    b. Power reassurance
    c. Power assertive

d. Opportunistic

7. Profit-oriented offense behavior indicates that the offender's motivation was based on:
    a. Anger
    b. Revenge
    c. Restoration of self-confidence
    d. Material or personal gain

8. In power assertive offense behavior, the offenders may not take precautions that they have learned are generally unnecessary. One reason for this is because:
    a. The crimes they commit usually have minimal punishment.
    b. The offenses are usually fantasized and not really carry out.
    c. They have no respect for law enforcement.
    d. All of the above.

9. Maury Roy Travis was arrested for multiple murders based on:
    a. The fact that the police were able to link into all of his crimes prior to his capture
    b. His inadvertent cybertrail of information recovered from an online map
    c. The large number of tangible leads the police had to work on
    d. His lack of skill and poor planning

10. In the example of programs being released, an example of power assertive offense behavior would be:
    a. A terrorist releasing a virus that would shut down segments of the power grid
    b. A 13-year-old running a tool that attempts to guess phonecard PIN numbers
    c. A keylogger that is installed on the computer of anyone who visits a particular website
    d. A program that simulates the Windows Blue Screen of Death (BSOD) as a screensaver

11. The cotton gin and the Gatling gun are examples of:
    a. The role innovation played in American history
    b. New technology that had unintended social consequences
    c. Proof that inventors should be monitored by the government
    d. None of the above

12. Criminal motivation is, generally:
    a. Technology dependent

b. Technology-based
c. Technology independent
d. Technology-centric

13. The study that was taken and modify by the FBI's National Center for the Analysis of Violent Crime was:
    a. Locard's Principle
    b. The Groth rapist motivational typology
    c. Lombroso's typology
    d. Gibb's Numerical Rules

14. Which offense behavior is characterized by the belief that the victim will enjoy and eroticize the offense behavior and may subsequently fall in love with the offender?
    a. Power reassurance
    b. Power assertive
    c. Anger retaliatory
    d. Anger excitation

15. In this offense behavior, the goal is the victim's total fear and submission for the purposes of feeding the offender's sexual desires.
    a. Power reassurance
    b. Power assertive
    c. Anger retaliatory
    d. Anger excitation

True or False Questions

1. Computers and the Internet are no different from other technologies adapted by the criminal.
    a. True
    b. False

2. When the Advanced Research Projects Agency began funding a mechanism for ensured communications between military installations, they understood full well that they were developing a pervasive form of social-global connectedness.
    a. True
    b. False

3. Modus operandi is a Latin term that means "the method of operating."
    a. True
    b. False

4. An offender's MO behavior is functional by nature – one of the purposes is that it facilitates the offender's escape.
    a. True
    b. False

5. Using e-mail for anonymous harassment is an example of how technology has been used as a vehicle for criminal behavior.
    a. True
    b. False

6. As a general rule, law enforcement groupies are always engaged in some form of criminal activity.
    a. True
    b. False

7. As criminals learn about new forensic technologies and techniques being applied to their particular area of criminal behavior, they must be willing to modify their MO, if possible, to circumvent those efforts.
    a. True
    b. False

8. Power reassurance – one of the offense behaviors – intends to restore the criminal self-confidence or self-worth through the use of extremely high aggression means.
    a. True
    b. False

9. Anger retaliatory offense behavior is behavior wherein the offender obtains sexual gratification from the victim's pain and suffering.
    a. True
    b. False

10. In regard to profit-oriented offense behavior, any behavior that is not purely profit motivated, which satisfies an emotional or psychological need, should be examined with the lens of the other behavior motivational types.
    a. True
    b. False

11. The technology that proved to be the downfall of Maury Roy Travis was the online mapping service that had logged his IP address.
    a. True
    b. False

12. Maury Roy Travis, compared with other serial murderers, was foolish, impulsive, and unskilled.
    a. True
    b. False

13. The criminal's MO consists of learned behaviors that can evolve and develop over time.
    a. True
    b. False

14. A criminal's MO reflects *how* he committed his crimes.
    a. True
    b. False

15. Modus operandi and motive are considered to be the same thing.
    a. True
    b. False

Essay Questions

1. Explain the possible benefits of conducting a thorough analysis of modus operandi during an investigation.

   Answer guidance: analysis of methods may provide new investigative leads, insights into the skill level of the offender, connection to other cases.

2. You are investigating the hacking and defacing of a corporate website. Provide a motivational analysis for this incident based on each of the offense behaviors listed in the text.

   Answer guidance: The offense behaviors to consider are: compensatory, entitlement, anger, sadistic, profit oriented.

Scenario

As a security investigator, you have been asked to determine if company confidential information (intellectual property) has been copied from enterprise computers. Investigation centers on a particular computer that has shown a high volume of network traffic at unusual times. In the course of conducting your investigation you discover that large capacity removable media has been attached to the suspect computer. A preview examination reveals that software used for secure deletion had been downloaded to the desktop.

Prepare an investigative plan listing the lines of investigation that you plan to pursue.

Note that this is not an exercise to demonstrate your understanding of forensic techniques. Rather, this exercise is directed toward developing skills in the creation of planning documents. Use the example cited in the chapter to assist in your design.

Chapter 10
Violent Crime and Digital Evidence

On completion of this chapter, the student will:

- Be aware that violent crime does not occur in an evidentiary vacuum. Recognize the role of computers in violent crime and as a source of information about:
    - The victim
    - The offender
    - The use of the computer as the instrument of violent crime
- Recognize that mobile devices are a potential source of digital evidence.
- Recognize that personal computers are a potential source of digital evidence.
- Be aware that private networks usually contain a higher concentration of digital evidence.
- Recognize that it is imperative to reach out and collect all available digital evidence.
- Recognize the role of the exigent circumstances in ECPA requests.
- Recognize the importance of developing a preservation plan at a violent crime scene.
- Be aware of the importance of diagramming and clearly labeling evidence items.
- Recognize that substantial amounts of digital evidence may reside in workplace computers.
- Be aware that network administrators may not be motivated to provide access or assistance.
- Be aware that enterprise systems may be used by offenders to gain information about victims.
- Recognize that evidentiary "facts" may have more than one interpretation.
- Recognize that the study of the victims of violent crime – victimology – may provide valuable insights to the investigation.
- Recognize that, although the individual pieces of digital evidence may not be revealing, the aggregate of such digital evidence may show patterns of behavior.
- Be aware of the need to look for offender behaviors that may leave digital traces.
- Recognize the difference between the primary and secondary crime scenes.

To date, there are huge amounts of information about people's personal and professional lives stored on computers, mobile devices, corporate computers, and the Internet. This vast store of information can show where victims of violent offenders were, and what they were doing, when the attack occurred. Digital evidence may reveal investigative leads, likely suspects, previously unknown crimes, and personal information that puts the victim at risk.

Multiple Choice Questions

1. Every violent crime investigation should incorporate digital evidence because digital evidence may reveal:
    a. Investigative leads
    b. Likely suspects
    c. Previously unknown crimes
    d. All the above

2. How the offender approaches and obtains control of a victim or target is significant because it exposes the offender's:
    a. Motives
    b. Choice of weapons
    c. Modus operandi
    d. Signature behaviors

3. Crime scenes fall into two categories – primary and ____.
    a. Remote
    b. Secondary
    c. Ancillary
    d. Theoretical

4. When reconstructing evidence surrounding a violent crime, it is generally helpful to:
    a. Lay out all the evidence so it can be viewed in its entirety
    b. Work with the crime scene technicians so that a better understanding of the crime is achieved
    c. Construct a timeline of events from digital evidence
    d. Begin the process of converting field notes to a final report

5. One reason not to put too much trust into those who run the company's computers is that:
    a. There has always been an antagonism between system administrators and law enforcement.
    b. They are typically too busy to take the time to answer your questions.
    c. They are usually not authorized to answer questions.
    d. They may be the offenders.

6. Although crime scenes are typically photographed, it is a good idea to create diagrams of the crime scene because:
    a. Diagramming is a common crime scene technician's skill; however, it requires continual practice.
    b. The process of creating a diagram can result in a digital investigator noticing an important item of evidence that would otherwise have been missed.
    c. The quality of photographs taken at the crime scene is not known until the film is developed.
    d. None of the above.

7. Given the scope and consequences of violent crimes, when collecting digital evidence it is advisable to:
    a. Collect only that digital evidence that is clearly connected to the offense
    b. Focus only on the primary crime scene, as searching the offender's home and workplace requires additional authorization
    c. Seek out and preserve all available digital evidence
    d. Focus only on the offender's digital evidence, as the victim's digital evidence is usually of little value

8. When swift action is needed, law enforcement personnel may be permitted to conduct searches without a warrant. Searches of this kind are permitted under:
    a. Exigent circumstances
    b. Eminent domain
    c. Mens rea
    d. USA PATRIOT ACT

9. When processing the digital crime scene in a violent crime investigation it is important to have _____ to ensure that all digital evidence and findings can hold up under close scrutiny.
    a. A good supply of electrostatic bags for holding sensitive electronic components
    b. More than one reliable camera for photographing the crime scene
    c. Standard operating procedures for processing a digital crime scene
    d. A good supply of nitrile gloves

10. The Federal statute that has a provision allowing Internet service providers to disclose subscriber information to law enforcement in exigent circumstances is:
    a. ECPA
    b. CCPA
    c. The Privacy Act

d. FCRA

11. When reconstructing evidence surrounding a violent crime, it is generally helpful to:
    a. Diagram the crime scene
    b. Create a timeline of events from digital evidence
    c. Create a threat assessment report
    d. None of the above

12. A thief who has programmed and released a virus to roam a network looking for victim passwords used for online banking is an example of what offense behavior?
    a. Power assertive
    b. Profit oriented
    c. Power reassurance
    d. Anger retaliatory

13. The case of a Michigan bank robber requiring tellers to undress so he could photograph them is an example of:
    a. Deviant aberrant behavior
    b. Criminal humor
    c. Crime scene characteristics
    d. Investigative reconstruction

14. The assessment of the victim as they relate to the offender, the crime scene, the incident, and the criminal justice system is known as:
    a. Threat assessment methodology
    b. Signature behaviors
    c. Behavioral evidence analysis
    d. Victimology

15. Computers and mobile devices are treated as _____ crime scenes in violent crime investigations.
    a. Temporary
    b. Immediate
    c. Remote
    d. Secondary

True or False Questions

1. Victimology is the assessment of the offender as he relates to the crime scene, the incident, and the criminal justice system.
    a. True
    b. False

2. The key to any investigation is luck, which has value only when it is properly acted upon.
    a. True
    b. False

3. Digital investigators can use information gleaned from many forms of digital evidence to find likely suspects and develop leads.
    a. True
    b. False

4. Data from Internet service providers used by the victim or suspect can help determine their activities around the time of the crime.
    a. True
    b. False

5. Mobile devices may contain information about communications as well as audio or video recordings relating to an offense.
    a. True
    b. False

6. Privately owned networks are usually a poor source of information when investigating violent crimes.
    a. True
    b. False

7. Given the scope and consequences of violent crimes, it is advisable to seek out and preserve all available digital evidence.
    a. True
    b. False

8. When investigating a violent crime, it is important to obtain proper authorization to examine the primary crime scene; however, secondary crime scenes are typically covered under that authorization.

a. True
b. False

9. A Mincey warrant, which is easier to obtain, is an option when investigators really believe there is some emergency.
a. True
b. False

10. The investigator reconstruction process involves pulling all evidence together and letting it speak for itself.
a. True
b. False

11. When reconstructing evidence surrounding a violent crime, it is helpful to create a timeline of events from digital evidence.
a. True
b. False

12. It is safe to place your trust in an organization's IT staff, since forensic training is a basic requirement in most IT departments.
a. True
b. False

13. Computers and mobile devices are treated as primary crime scenes in violent crime investigations.
a. True
b. False

14. When investigating suspects of a violent crime, it is important to look for behaviors that leave digital traces.
a. True
b. False

15. What an offender does at a crime scene typically reveals little useful information to digital investigators.
a. True
b. False

Essay Questions

Prepare a sample Crime Scene Processing Procedures Field Guide, based on the information provided in this chapter. The format of this guide should facilitate use at the scene.

Answer guidance: Field guides are typically in "cookbook" format, with larger print and telegraphic prose intended to serve as reminders.

Scenario

You have just arrived at the scene of workplace violence where an individual shot his coworker. Describe, in detail, the steps that you would take to process the digital crime scene.

Things to consider: comments from coworkers, contents of computer and cell phone, other digital evidence relating to the incident.

Chapter 11
Digital Evidence as Alibi

On completion of this chapter, the student will:

- Recognize that key pieces of information in an alibi are: time and location.
- Be aware of potential sources for time and location information.
- Be aware that, when corroborating an alibi in, "the absence of evidence is not evidence of absence."
- Recognize that it is necessary to find evidence that demonstrates the lie.
- Be aware of how time can confirm or refute an alibi.
- Be aware of how location can confirm or refute an alibi.
- Recognize that time/location evidence relates to the device, not the user.

With people spending an increasing amount of time using mobile devices, computers, and networks, there are bound to be more alibis that depend on digital evidence.

Digital evidence will rarely show that someone was at a specific location at a specific time; however, it can show that the device was at that location. Through the use of other supporting evidence, such as a phone call in progress or an e-mail sent, the device can be associated with an individual.

Multiple Choice Questions

1. Investigators should not rely on one piece of digital evidence when examining an alibi – they should look for an associated _____.
    a. Cybertrail
    b. Piece of physical evidence
    c. Statement
    d. None of the above

2. Types of digital evidence that might corroborate an alibi include:
    a. Evidence of computer usage when the offense was supposed to occurred
    b. Computer records from credit cards, the telephone company, or subway ticket usage
    c. GPS information from mobile devices indicating the user's location and time
    d. All of the above

3. It is unwise to rely only on a recovered IP address because:
    a. An IP address may change many times during a session.
    b. Offenders can change their IP address.
    c. By changing the system time, the contents of log files containing IP addresses can be falsified.
    d. IP addresses only exist in system memory.

4. It is quite difficult to fabricate an alibi on a network successfully because:
    a. An offender may not have the proper access.
    b. An offender would need system administrator access level to make the necessary changes.
    c. An individual rarely has the ability to falsify digital evidence on all the computers that are involved.
    d. Creating an alibi on a network could take months of work.

5. It is important to gather as many sources of supporting evidence as possible because:
    a. The more evidence, the stronger the case.
    b. No amount of supporting evidence can prove conclusively that an individual was in a specific place at a specific time.
    c. The volume of evidence produced dictates the strength of the alibi.
    d. None of the above.

6. To demonstrate that someone is lying about an alibi, it is necessary to:

a. Find evidence that clearly demonstrates the lie
b. Require the suspect to submit to a polygraph
c. Interrogate the suspect using a number of methods
d. Show that no evidence confirming the alibi is available

7. In confirming an alibi involving an obscure piece of equipment, if no documentation is available, the manufacturer is no longer in business, or the equipment/network is so complicated that nobody fully understands how it works, you should:
a. State that the alibi is considered unproven
b. Search the Internet for any pertinent information
c. Recreate the events surrounding the alibi
d. Contact other investigators and average their opinions

True or False Questions

1. Absence of evidence refutes an alibi.
    a. True
    b. False

2. When investigating an alibi that depends on digital evidence, the first step is to assess the reliability of the information on the computers and networks involved.
    a. True
    b. False

3. It is not difficult to fabricate an alibi on a network successfully.
    a. True
    b. False

4. Investigators can rely on one piece of digital evidence when examining an alibi.
    a. True
    b. False

5. Computer networks can contain a large amount of information about times and locations.
    a. True
    b. False

6. Credit card companies are not permitted to keep records of the dates, times, and locations of all purchases.
    a. True
    b. False

7. Telephone companies keep a record of the number, the time and duration of the call, and sometimes the caller's number.
    a. True
    b. False

8. With people spending an increasing amount of time using mobile devices, computers, and networks, it is very likely that more alibis will depend on digital evidence.
    a. True
    b. False

9. It is not easy to change the time on a personal computer.
    a. True
    b. False

10. Digital evidence can rarely prove conclusively that someone was at a specific place at a specific time.
    a. True
    b. False

Essay Questions

1. Discuss the reasons why a digital investigator would confirm an alibi. Isn't that a job for the suspect's defense counsel?

Answer guidance: The digital investigator's mission is to find out the truth.

Scenario

A suspect claims that evidence artifacts found on his computer were placed there by his estranged wife out of malice. As evidence, he points out that the created dates on some the files occurred when he was on vacation.

Prepare an investigative plan on how you would confirm or refute his alibi.

Chapter 12
Sex Offenders on the Internet

On completion of this chapter, the students will:

- Be aware of the reasons why the Internet is attractive to sex offenders.
- Recognize that sexual abuse and illegal pornography existed long before the Internet.
- Recognize that computers, networks, and the Internet can be used to reveal sex offender methods.
- Be aware that the most common sex offenses on the Internet include:
    - Solicitation of minors for sex
    - Creation, possession, or distribution of child pornography
- Be aware that there are restrictions on releasing child pornography to the defense.
- Recognize that private sector security personnel can face both legal and corporate issues in carrying out their duties.
- Recognize that, with sexual predators/offenders, the Internet is an important source of evidence.
- Recognize the potential difficulty in proving the dissemination of child pornography.
- Be aware of various common defenses (Trojan defense, malware, "mouse trapping").
- Be aware of the risks when private citizens mount undercover operations.
- Recognize the value in analyzing sexual offenders.
- Recognize the value of looking for offender patterns.
- Recognize the value of victim behavioral analysis.
- Recognize the value of determining how a victim is chosen.
- Recognize the value of analyzing crime scene characteristics.
- Be aware of the methods offenders use to approach victims.
- Recognize that motivation may vary with the type of pornography.
- Recognize the importance of understanding an offender's motivation.

Forensic examiners need to be aware that they may be requested to find a particular piece of evidence, or find evidence that confirms an investigator's suspicions. That is not the examiner's job. Examiners find the truth, regardless of its convenience.

Investigators must learn to study sex offenders, so they can recognize and understand the patterns of behavior that force sex offenders to take greater risks.

Multiple Choice Questions

1. Which of the following is a reason the Internet is attractive to sex offenders?
    a. Greater access to victims.
    b. Extending their reach
    c. The vast amount of information about potential victims
    d. All of the above

2. Which of the following is an impact of sex offender peer support groups?
    a. Enabling offenders to view their behavior as socially acceptable
    b. Raising the sex offender's inhibitions to act on impulses
    c. A clearinghouse of state and Federal agencies ready to assist the sex offender
    d. Trained counselors available 24 hours a day

3. Which of the following are reasons that digital evidence may not be preserved properly or at all?
    a. Victims may destroy key evidence because they are embarrassed by it.
    b. Corporate security professionals may not be aware of proper evidence handling concepts.
    c. Poorly trained police officers may overlook important items.
    d. All of the above.

4. The reconstruction process becomes a necessity when:
    a. There is more than one victim involved
    b. There is more than one sex offender involved
    c. The victim is unknown
    d. The sex offender is unknown

5. When the offender is unknown, the reconstruction process becomes a necessary step to:
    a. Reassure the victim that progress is being made
    b. Prioritize suspects
    c. Accommodate multiple cases
    d. Open new lines of investigation

6. Detailed knowledge of an offender can help investigators:
    a. Protect past victims
    b. Warn potential victims
    c. Communicate with the offender
    d. All of the above

7. Victimology can help determine:
    a. Why the victim was selected
    b. What victim behavior caused the offense
    c. To what extent the victim was at fault
    d. The offender's modus operandi

8. Of Lanning's three general categories of sex offenders, which of the following is NOT a characteristic of the situational category?
    a. Generally more power/anger motivated
    b. Are compulsive record keepers
    c. Generally pick convenient targets
    d. None of the above

9. The process of correlating evidence through temporal, relational, and functional analysis is known as:
    a. Crime scene analysis
    b. Offense behavior analysis
    c. Investigative reconstruction
    d. Victimology

10. An offender's choice of location, tools, and actions taken are referred to as:
    a. MO
    b. Motivation
    c. Crime scene characteristics
    d. Signature behaviors

11. Failure to interpret evidence, obtain information from an unknown offender, or apprehend an unknown offender can be caused by:
    a. Excessive caseload
    b. Scrutiny of the press
    c. Negative public opinion
    d. Failure to understand the offender's motivation

12. Typically, children are not used in undercover investigations because:
    a. Children, like child actors, can be difficult to control.
    b. Parents are not comfortable with their child participating in an undercover operation.
    c. There is concern for their welfare.

d. Typically, there are no funds in the budget for undercover investigations using children.

13. One of the risks that private citizens take in luring online predators is that:
    a. If the subject of the investigation is child pornography, their efforts may cause them to have possession of child pornography and be arrested along with the offender.
    b. Should the neighbors find out, they could possibly be forced to move out of their neighborhood.
    c. One of their neighbors could be an online predator.
    d. The police consider cyber vigilantes to be a nuisance.

14. If an offender's computer reveals a large number of contacts, a good solution is:
    a. To pass the contact information to local departments and have them contact the individuals in person
    b. To draft a simple form letter summarizing the investigation and listing the suspects' online nicknames and e-mail addresses, and request assistance
    c. To reach out to each contact, using the offender's computer and online personas
    d. To determine what schools the contacts attend and have their principals call the students and their parents in for consultation

15. One way that a digital examiner can reduce the likelihood of overlooking or misinterpreting important details is:
    a. To always work in pairs, so each examiner can check the other's work
    b. Carefully apply the scientific method
    c. Videotape the entire examination process so that key areas can be reviewed
    d. Take verbal notes with a digital voice recorder

True or False Questions

1. The Internet enables sexual offenders to commit a crime without ever physically assaulting a victim.
    a. True
    b. False

2. Sex offender peer support groups can give offenders access to child pornography, children, and technical knowledge.
    a. True
    b. False

3. Generalizations regarding investigations are of particular use, even though cases tend to be unique.
    a. True
    b. False

4. It is important to stress that sexual abuse and illegal pornography did not exist before the Internet.
    a. True
    b. False

5. "Grooming" refers to the ways that a sexual offender gains control over victims.
    a. True
    b. False

6. Because sex offenders tend to be nonviolent, investigators do not need to take the same precautions when serving warrants on computer-related offenses as they would with other crimes.
    a. True
    b. False

7. When dealing with online sexual offenders, it is critically important to take advantage of the Internet as a source of evidence.
    a. True
    b. False

8. Given the potential for concealment in sex offender cases, it is important to examine all digital evidence carefully rather than simply searching for a obvious items such as images that are not hidden.
    a. True
    b. False

9. Confronting the victim with evidence of their abuse is standard practice in sex offender cases.
    a. True
    b. False

10. The initial stage of any investigation is to determine if a crime has actually occurred.
    a. True
    b. False

11. The practice of private citizens luring offenders is not recommended for reasons of safety and inadvertent violation of the law.
    a. True
    b. False

12. An accepted method of conducting undercover investigations involves using a minor, especially if the minor is the victim.
    a. True
    b. False

13. Providing information about an offender's method of approach, attack, or control may help investigators interact with an offender or provide potential victims with protective advice.
    a. True
    b. False

14. Lanning identifies three general categories of sex offenders: situational, preferential, and differential.
    a. True
    b. False

15. Sex offenders do not change over time nor do they modify their behavior, simplifying the investigative process.
    a. True

b. False

Essay Questions

1. Discuss the responsibility of the digital investigator in bringing charges of sex offense or possession of child pornography against a member of the local community.

Answer guidance: The mere accusation, even as just "a person of interest," can ruin reputations that takes years to recover.

Scenario

You, as a member of local law enforcement, were contacted by a member of a cyber vigilante group, informing you that they have been gathering information about an individual in your community who, they assert, has been downloading large amounts of child pornography. They provide samples of the types of child pornography that the sender individual has supposedly downloaded.

The local community you serve is very small, and you have known this individual most of your professional life.

The cyber vigilante group has a reputation for notifying local police and waiting a few days to hear of an arrest, and if they do not they take the information to the press and complain that they notified the police and nothing was done.

Prepare a briefing on the situation, to be given to your captain and the mayor. including a few recommendations.

Chapter 13
Computer Intrusions

On completion of this chapter the student will:

- Recognize that the value of digital data has made it the target.
- Be aware of the reasons that criminals break into computers.
- Be aware of how computer intruders operate.
- Be aware of the tactics used in computer intrusions:
    - Phishing
    - Spear phishing
    - Drive-by download
    - Cross site scripting
- Recognize that the first step in an intrusion investigation is to confirm that there actually was one.
- Be aware of the need to determine the intruder's goals.
- Recognize that an intrusion investigation requires a wide range of forensic skills.
- Recognize the difference between "intrusion investigation" and "incident response."
- Recognize that the scientific method can be applied to intrusion investigations.
- Be aware of conflicting goals of the investigators and network administrators.
- Be aware of the risks in investigating live systems.
- Recognize both the value and risk in observing the intruder.
- Be aware that intruders may have a high degree of technical knowledge and/or may employ advanced software.
- Recognize that the majority of compromised systems in an intrusion will contain malicious programs.
- Be aware that malware must be analyzed as part of the intrusion investigation.
- Recognize that intrusion investigations frequently cross jurisdictional lines.
- Recognize that the intrusion must ultimately be linked to a person.
- Recognize the importance of preserving volatile data.
- Recognize the values and risks of collecting full memory dumps.
- Be aware that remote forensics tools can collect volatile data.
- Recognize why it is important to collect all network traffic to/from a compromised system.
- Be aware of the methods used in an intrusion investigation.
- Recognize that malware and analysis strategy is given by the kind of malware and its goals.
- Recognize that intrusion crime scene analysis may reveal information about the intruders' skills and intentions.
- Recognize the value of examining the intruders' computers.

Just as a company's most valuable assets may be the data on its computers, failure to protect those assets may result in financial loss, regulatory sanctions, and reputational harm. More than one company has been forced into bankruptcy when the computer containing their company information crashed.

A common truth is that criminals tend to steal things of value. Therefore, a company's information may be a target.

Multiple Choice Questions

1. During the commission of a crime, evidence is transferred between the offender's computer and the target. This is an example of:
    a. Locard's Exchange Principle
    b. Sutherland's General Theory of Criminology
    c. Martin's Rule
    d. Parkinson's Rule of Available Space

2. Intruders who have a preferred toolkit that they have pieced together over time, with distinctive features:
    a. Usually have little experience and are relying on the kit
    b. Show little initiative – letting the tool do the work
    c. Are generally more experienced
    d. Pose less of a threat

3. In the case of a computer intrusion, the target computer is:
    a. The remote crime scene
    b. The auxiliary crime scene
    c. The virtual crime scen.
    d. The primary crime scene

4. A computer intruder's method of approach and attack can reveal a significant amount about their:
    a. Skill level
    b. Knowledge of the target
    c. Intent
    d. All of the above

5. Determining skill level can lead to:
    a. Determining the extent of the intrusion
    b. Likely hiding places for rootkits and malware
    c. Suspects
    d. Offense behaviors

6. If digital investigators find an unauthorized file, they should:
    a. Immediately move the file to removable media
    b. Check for other suspicious files in the same directory
    c. Execute the file to determine its purpose

d. Permanently delete the file

7. Remote forensic solutions can be used to access live systems, and include the ability to:
   a. Acquire and, sometimes, analyze memory
   b. Image systems without ever having to leave the lab
   c. Conduct examination and analysis without the need to image
   d. Image large systems across the Internet

8. A forensic analysis conducted on a forensic duplicate of the system in question is referred to as:
   a. Virtual analysis
   b. Clone analysis
   c. Post-mortem analysis
   d. Ex post facto analysis

9. Capturing all of the network traffic to and from the compromised system can:
   a. Allow the network administrators to participate in the investigation, establishing rapport for later interviews
   b. Reveal the source of the attack
   c. Seriously slow down the network, affecting normal work
   d. None of the above

10. A common technique that is highly useful and can be applied in a computer intrusion investigation is to simply focus on file system activities around the time of known events. This embodies a principle known as:
    a. Temporal proximity
    b. Timeline analysis
    c. File system analysis
    d. Temporal aggregation

11. The registry key **HKLM\Software\Microsoft\Windows\Current Version** is one of the most common locations for:
    a. New software entries
    b. Time and date information
    c. Trojans
    d. A list of recently run programs

12. When collecting data from a compromised computer, consideration should be given to collecting the _____ data first.
    a. CMOS

b. Most volatile
c. Magnetic
d. Optical

13. The forensic examiner needs to be aware that the process of collecting memory:
    a. Is seldom useful and not often called for
    b. Can take an extremely long period of time
    c. Is only needed for standalone systems
    d. Changes the contents of memory

14. A more thorough method of collecting specific volatile data from a computer is to:
    a. Examine the specific memory addresses live
    b. Collect the full contents of physical memory
    c. Selectively collect contents of physical memory
    d. Take screenshots.

15. Why are "non-volatile" storage locations contained in the RFC 8227 "Order of Volatility"?
    a. This is an old RFC and has not been updated.
    b. No form of data storage is permanent.
    c. An RFC is a Request for Comments – and corrections are expected.
    d. None of the above.

True or False Questions

1. Social engineering refers to any attempt to contact legitimate users of the target system and trick them into giving out information that can be used by the intruder to break into the system.
    a. True
    b. False

2. A valid profile of a computer intruder is an antisocial adolescent.
    a. True
    b. False

3. A growing number of intrusions are committed by organized criminal organizations and state-sponsored groups.
    a. True
    b. False

4. Although new exploits are published daily, it takes skill and experience to break into a computer system, commit a crime, and cover one's tracks.
    a. True
    b. False

5. A thorough understanding of the tactics and techniques used by criminals is "nice to know" but is not essential to the successful investigation of criminal behavior.
    a. True
    b. False

6. Reverse social engineering is any attempt by intruders to have someone in the target organization contact them for assistance.
    a. True
    b. False

7. The first stage of a computer intrusion is Abuse.
    a. True
    b. False

8. In a computer intrusion, the stage after Attack is Abuse.
    a. True
    b. False

9. An example of the Entrenchment phase of an intrusion would be uploading a backdoor through the remote shell.
    a. True
    b. False

10. Gathering information about a system through the use of a port scanner is considered a direct attack method.
    a. True
    b. False

11. "Spear phishing" is an intrusion technique wherein mass e-mails that appear or claim to be from a legitimate source request that the recipient follow instructions contained in the e-mail.
    a. True
    b. False

12. The first step when investigating a computer intrusion incident is to determine if there actually was one – there must be a *corpus delicti*.
    a. True
    b. False

13. Investigating computer intrusions usually involves a small amount of digital evidence from only a few sources.
    a. True
    b. False

14. Incident Response can be viewed as a subset or part of an intrusion investigation.
    a. True
    b. False

15. Examining a live system is prone to error, may change data on the system, and may even cause the system to stop functioning.
    a. True
    b. False

Essay Questions

1. Discuss why computer intrusions are among the most challenging types of cybercrimes from a digital evidence perspective.

Answer guidance: every network is different; every computer intruder is different, with different motivations.

2. Discuss the difference between automated and dynamic modus operandi, including the kinds of information to look for, and the value of conducting this kind of analysis.

Answer guidance: While automated exploits are almost generic, analysis of dynamic MO may reveal the choice of tools used in the intrusion, shedding light on a particular kind of offender behavior.

Scenario

You are participating in an intrusion investigation. The investigation has progressed to the point where a suspect has been identified. A raid is planned on the suspect's site, and you will be in attendance to collect, preserve, and examine the intruder's computer.

As part of the raid planning, you have been asked to prepare a plan detailing how you will examine the intruder's computers.

After preparing your plan, you will present it to the rest of the team in a planning meeting.

NOTES: This exercise is designed to get the student accustomed to developing planning documents, and more importantly, to be able to articulate that plan to others of the team who may not have the same level of expertise.

Chapter 14
Cyberstalking

On completion of this chapter, the student will:

- Recognize that fixation is a prominent feature of cyberstalking.
- Be aware that cyberstalking may be accompanied by more traditional, physical forms.
- Recognize that cyberstalking is based on power over the victim.
- Be aware that, although often the cyberstalker has been equated with the victim, this may not be as true with the Internet.
- Recognize the methods used by cyberstalkers to control their victims.
- Be aware of steps to take when investigating cyberstalking.
- Recognize that various interviewing techniques are needed when investigating cyberstalking.
- Be aware of victimological aspects when investigating cyberstalking.
- Recognize the risk assessment aspect of victimology.
- Be aware of the need to extend the search to the Internet.
- Recognize the various motivational typologies is may occur in a cyberstalking.

Cyberstalking is a new variation to regular stalking. The Internet has just provided another avenue.

A cyberstalking investigation requires a strong investigative methodology that includes understanding motivation. The cyberstalker's computer typically provides a rich array of digital evidence.

Multiple Choice Questions

1. The first state in the United States to enact a law to deal with cyberstalkers was:
    a. Texas
    b. Hawaii
    c. California
    d. New York

2. The first cyberstalking law in the US was passed in:
    a. 1985
    b. 1990
    c. 1995
    d. 2000

3. Stalkers want to exert power over their victims, primarily through:
    a. Fear
    b. Anxiety
    c. Autosuggestion
    d. Peer pressure

4. A stalker's ability to frighten and control a victim increases with the amount of information that he can gather, such as:
    a. Telephone numbers
    b. Addresses
    c. Personal preferences
    d. All of the above

5. Stalkers have taken to the Internet because:
    a. The cost of an Internet connection has dropped considerably.
    b. They depend heavily on information and the Internet contains vast amounts.
    c. They no longer have to go out to do their stalking.
    d. None of the above.

6. An implication from studies indicating that many stalkers had prior acquaintance with their victims is that:
    a. Part of the blame can be assigned to the victim.
    b. The offender is likely to be found in the same area as the victim.
    c. Investigators should pay particular attention to acquaintances of the victim.
    d. Investigators should always check the immediate family.

7. An excellent set of guidelines developed specifically for victims of stalking is available from:
    a. The National Center for Victims of Crime
    b. The National White Collar Crime Center
    c. The Department of Justice
    d. The National Institute of Justice

8. When a cyberstalking case is stalled, it is a good idea to interview the victim again, because:
    a. The victim might have been withholding information during the first interview.
    b. The information that investigators have gathered might help the victim recall additional details.
    c. The time between the first and second interviews has given the victim time to seek counseling.
    d. None of the above.

9. In determining how and why the offender selected a specific victim, the investigator should determine whether the cyberstalker:
    a. Knew the victim
    b. Learned about the victim through a personal web page
    c. Noticed the victim in a chat room
    d. All of the above

10. A key aspect of developing victimology is determining victim and offender _____.
    a. Hobbies
    b. Likes and dislikes
    c. Risks
    d. Roles

11. When searching for evidence of cyberstalking, it is useful to distinguish between an offender's harassing behaviors and _____ behaviors.
    a. Grooming
    b. Surreptitious monitoring
    c. Initial contact
    d. Congenial

12. That part of cyberstalking where the offender is using the Internet to find a victim is known as:

a. Profiling
b. Trolling
c. Surreptitious monitoring
d. None of the above.

13. When a cyberstalker chooses victims at random, he is said to be an:
    a. Opportunistic stalker
    b. Power assertive stalker
    c. Profit-oriented stalker
    d. None of the above

14. The initial stage in a cyberstalking investigation is to:
    a. Search for additional digital evidence
    b. Analyze crime scene characteristics
    c. Conduct victimology and risk assessments
    d. Interview the victim

15. It is extremely important for the investigator to be extremely cautious when dealing with a stalking case because:
    a. If the victim becomes offended by the investigator's methods, she is likely to go file a complaint.
    b. If the investigation is conducted too openly, the offender may stop the harassment and move on to another victim.
    c. The victim must be protected, in case the offender decides to escalate to physical violence.
    d. The victims frequently become emotionally attached to the investigator.

True or False Questions

1. Cyberstalking works in a completely different way than stalking in the physical world.
    a. True
    b. False

2. In general stalkers want to exert power over their victims in some way, primarily through fear.
    a. True
    b. False

3. Stalkers use information to impinge on their victims' lives.
    a. True
    b. False

4. The Internet contains a vast amount of personal information about people but it is relatively difficult to search for specific items.
    a. True
    b. False

5. Studies indicate that stalkers will always have prior acquaintance with their victims.
    a. True
    b. False

6. When interviewing the victim, investigators should be as tactful as possible while questioning everything, and assume nothing.
    a. True
    b. False

7. A key aspect of developing victimology is determining victim and offender risk.
    a. True
    b. False

8. The first step in a cyberstalking investigation is to conduct the victimology and risk assessment.
    a. True
    b. False

9. The victim is usually only aware of the harassing component of cyberstalking.

a. True
b. False

10. There is never correlation between the victim's Internet activities and physical surroundings or real-world activities.
    a. True
    b. False

11. When searching for evidence of cyberstalking, it is useful to distinguish between the offenders' harassing behaviors and surreptitious monitoring behaviors.
    a. True
    b. False

12. The primary aim of the motivational stage of the investigation is to understand the victim-offender relationship.
    a. True
    b. False

13. As part of the investigation, an investigator should ask why a particular stalker used the Internet.
    a. True
    b. False

14. Investigators might not be able to define the primary crime scene clearly because digital evidence is often spread all over the Internet.
    a. True
    b. False

15. As part of the interview process, the investigator should tell the victim that the stalker will cease harassing them when they're no longer giving the desired response.
    a. True
    b. False

Essay Questions

1. Regardless of the type of investigation, investigators ask "who, what, when, where, and why" questions. However, when dealing with cyberstalking victims, those questions have to be asked tactfully, and without assigning blame.

   Prepare a set of initial questions and discuss how you would ask those questions to a cyberstalking victim.

2. Discuss how you would apply the concept of crime scene characteristics to a cyberstalking case.
3. Discuss how you would explain your risk assessment findings to the victim.

Scenario

You have been contacted by a young woman complaining her ex-boyfriend is reading and blocking her e-mail. In the course of your interview with the victim, she tells you that the e-mail account is with AOL, and it is actually registered to and paid for by the ex-boyfriend. It seems that while they were together, he set up an account for her under his account.

Describe how you would proceed with the investigation at this point.

Chapter 15
Computer Basics for Digital Investigators

On completion of this chapter, the student will:

- Be aware of the process that occurs when a computer boots.
- Recognize how data is stored on a magnetic media.
- Recognize the significance of file formats.
- Be aware of how file carving affects recovered data.
- Recognize various methods that can be used to hide data on magnetic media.
- Be aware of how various file systems are implemented.
- Be aware of the various data structures that comprise a file system.
- Be aware of various methods for hiding data within a file system.
- Be aware of difficulties in dealing with passwords and encryption.
- Be aware of encryption concepts.
- Be aware of methods for detecting and dealing with encryption.

A basic understanding of how computers operate and how data is stored is a fundamental skill for forensic examiners. This includes understanding and controlling the boot process, recovering data, and analyzing data.

Most digital investigators use automated forensic tools; however, it is absolutely crucial that they understand what these tools are doing. The best way to gain that understanding is by experimentation. That would include creating a file and viewing the results, deleting the file and viewing those results, using a low level hex editor, and carving data associated with the file into a new one.

Multiple Choice Questions

1. How many bytes are in a kilobyte?
    a. 8
    b. 100
    c. 1000
    d. 1024

2. The big-endian representation of "FB 78 7A 23" is:
    a. 78 FB 23 7A
    b. 7A 23 FB 78
    c. 23 7A 78 FB
    d. FB 7A 78 23

3. The storage capacity of a hard drive with 256 heads, 63 sectors, and 1024 cylinders is:
    a. 8.4 Gbytes
    b. 7.8 Gbytes
    c. 8 Gbytes
    d. 9 Gbytes

4. What can you do to determine the number of sectors on a hard drive larger than 8GB?
    a. Use a UNIX tool like hdparm
    b. Use a Windows tools like EnCase
    c. Check the drive manufacturer's website for the specific drive
    d. All of the above

5. The first sector of a hard disk contains a:
    a. Boot sector
    b. Master boot record
    c. Volume
    d. Partition

6. The first sector of a volume contains a:
    a. Boot sector
    b. Master boot record
    c. Root Directory
    d. Partition

7. File slack space is:
    a. The space between the end of a volume and the end of a partition
    b. The sectors in a cluster that are not occupied by the file in that cluster
    c. The space on a disk that is not allocated to files
    d. The space left on a disk after a file is deleted

8. Unallocated space is:
    a. The space between the end of a volume and the end of a partition
    b. The space in a cluster that is not occupied by the file in that cluster
    c. The space on a disk that is not assigned to files
    d. The space left on a disk after a file is deleted

9. Encrypted data can be recovered using which of the following methods?
    a. Trying every possible encryption key
    b. Obtaining the passphrase used to protect the encryption key
    c. Recovering plaintext versions of data from unallocated and slack space
    d. All of the above

10. Which encryption scheme is weakest?
    a. RSA
    b. ROT13
    c. DES
    d. DSA

11. On Intel-based computers, system date and time information is maintained in:
    a. CMOS
    b. System.conf
    c. MBR
    d. Boot record

12. Solaris computers store data in:
    a. Hexadecimal
    b. Little-endian
    c. Octal
    d. Big-endian

13. Which of the following are limitations to salvaging data through data carving?
    a. File name and date-time stamps that were associated with the file are not salvaged.
    b. The size of the original file may not be known, making it necessary to guess how much data to carve out.
    c. Simple carving assumes all portions of the file were stored contiguously, and not fragmented.
    d. All of the above.

14. The boot sector in a FAT volume contains all of the following information EXCEPT:
    a. Partition table
    b. The number of file allocation tables available
    c. Cluster size
    d. Volume label

15. In NTFS, an example of a file system feature that can be used to conceal data is:
    a. Setting the Read/Only attribute on the folder you want to protect
    b. Storing data in a hidden partition

c. Using alternate data streams
d. None of the above

True or False Questions

1. The ENIAC was the first digital computer.
    a. True
    b. False

2. By default, computers will boot from a floppy disk if one is present in the system.
    a. True
    b. False

3. The CMOS RAM chip stores a computer's date and time.
    a. True
    b. False

4. Hard drive settings stored in a computer's CMOS RAM chip are always correct and accurate.
    a. True
    b. False

5. The POST verifies that all of the computer's components are functioning properly.
    a. True
    b. False

6. The BIOS can be password protected.
    a. True
    b. False

7. The Macintosh Open Firmware can be instructed to boot from a CD-ROM by holding down the "b" key.
    a. True
    b. False

8. The Sun OpenBoot PROM can be interrupted by depressing the "Stop" key.
    a. True
    b. False

9. Although storage media come in many forms, hard disks are the richest sources of digital evidence on computers.
    a. True

b. False

10. Digital forensics examiners do not need to be concerned about the distinction between little-endian and big-endian representations because automated tools make the necessary translation.
    a. True
    b. False

11. Unicode can represent more characters than ASCII.
    a. True
    b. False

12. Sectors are 557 bytes long but only 512 bytes are used to store data.
    a. True
    b. False

13. Many digital forensics laboratories have the capability to recover overwritten data from a hard drive.
    a. True
    b. False

14. A sector is composed of multiple clusters.
    a. True
    b. False

15. The number of sectors on any hard drive is calculated by multiplying its CHS values.
    a. True
    b. False

Discussion Questions

1. Describe the main steps that your computer takes during the boot process from the time you press the power switch to the first appearance of the operating system. Why is this important to a forensic examiner?
   Answer guidance: The main steps that a computer takes to boot up are: CPU reset → load first sector of book disk (MBR) into memory → BIOS & POST (compare actual configuration with CMOS settings) → load active operating system using information in partition table → locate boot disk (search order specified in CMOS).

2. What type of computer do you have and how do you interrupt the boot process to display the CMOS settings?

3. List four of the most important CMOS settings of your computer. List two CMOS settings that you do not understand or that you think are unimportant.

4. What is the ASCII representation of the binary data "01000011011011110111001001110010011001010110001101110100"?
   Answer guidance: Break this string of binary data into 8-bit segments and determine the ASCII equivalent of each 8-bit segment as shown here (it may help you to convert to hexadecimal first):
   0100 0011 = 43 = C
   0110 1111 = 6F = o
   0111 0010 = 72 = r
   0111 0010 = 72 = r
   0110 0101 = 65 = e
   0110 0011 = 63 = c
   0111 0100 = 74 = t

NOTE: WinHex has a conversion table; under the View menu, select Tables and then choose ANSI ASCII.

5. What is the ASCII representation of this hexadecimal data: "546865207375737065637427732 06E616D65206973204D69636861656C"?

Answer guidance: Determine the ASCII value associated with each hexadecimal character in this string as follows:
54 = T
68 = h
65 = e
20 = space
73 = s
75 = u
73 = s
70 = p
65 = e

63 = c
74 = t
27 = '
73 = s
20 = space
6E = n
61 = a
6D = m
65 = e
20 = space
69 = i
73 = s
20 = space
4D = M
69 = i
63 = c
68 = h
61 = a
65 = e
6C = l

6. What is the storage capacity of a hard drive with 64 heads, 63 sectors, and 787 cylinders?
Answer guidance: 64 × 63 × 787 = 3,173,184 sectors = 1,624,670,208 bytes = 1.5GB.

7. Where is the partition table located on a hard drive, and what does it contain?
Answer guidance: The partition table is located 446 bytes into the first sector of the drive and contains information about each partition on the disk, including the first and last sectors.

8. How do you remove data from a hard drive to prevent it from being recovered (e.g., delete partition table, reformat drive, delete files)?
Answer guidance: Although a low-level format effectively removes data from a drive, it can be difficult to obtain tools to perform a low-level format for all types of disks. Therefore it is more practical to "wipe" the drive by overwriting sectors several times with certain patterns. For instance, using UNIX, a drive can be effectively overwritten with zeros using the command sequence 'dd if=/dev/zero of=/dev/hdb; sync' three times. You should then verify that the wiping process was successful by looking at the first, middle, and last sectors in a hex viewer. You can also verify that the drive was wiped using the following UNIX command: 'dd if=/dev/hdb | xxd | grep –v "0000 0000 0000 0000 0000 0000 0000 0000". This command should return nothing provided the drive only contains zeros.

9. What is file slack and why is it important to digital investigators?
Answer guidance: File slack refers to the sectors in a cluster that are not occupied by the file in that cluster. This space can contain fragments of files that may contain useful digital evidence.

Scenario

You suspect that the data carving tool you are using to recover deleted files from a hard drive is not recovering all of the files that are available for recovery. How would you determine this limitation in the tool and what would you do to resolve the problem?

Chapter 16
Applying Forensic Science to Computers

On completion of this chapter the student will:

- Be able to apply those forensic methodologies discussed earlier in this book to stand-alone Computer Systems. The methodologies include:
    - Preparation
    - Survey
    - Documentation
    - Preservation
    - Examination and analysis
    - Reconstruction
    - Reporting results
- Recognize the value of data reduction.
- Be aware of the process of examining a piece of evidence.
- Recognize that data recovery procedures may need to be applied to digital evidence.
- Recognize the value of conducting functional, relational, and temporal analyses to a computer.

Computer technology continues to evolve rapidly but the fundamental components have changed little. Because processes at the top level have not changed rapidly, it is both possible and reasonable to develop SOPs to be used in the field.

Multiple Choice Questions

1. Which of the following is NOT part of the set of forensic methodologies referenced in this book?
    a. Preparation
    b. Interdiction
    c. Documentation
    d. Reconstruction

2. Preparation planning prior to processing a crime scene should include:
    a. What computer equipment to expect at the site
    b. What the systems are used for
    c. Whether a network is involved
    d. All of the above

3. The forensic crime scene processing kit should include all of the following, EXCEPT:
    a. Evidence bags, tags, and other items to label and package evidence
    b. Forensically sanitized hard drives to store acquired data
    c. Compilers for developing forensic tools on site
    d. Hardware write blockers

4. When processing the digital crime scene, one aspect of surveying for potential sources of digital evidence is:
    a. Recognizing relevant hardware such as computers, removable media, etc.
    b. Determining if electrical wiring is capable of supporting forensic machines
    c. Confirming that the operating environment is suitable for electronic equipment
    d. Making sure there is sufficient space to set up the forensic crime scene processing kit

5. The _____ documentation specifies who handled the evidence, when, where, and for what purpose.
    a. Evidence inventory
    b. Chain of custody
    c. Evidence intake
    d. Preservation notes

6. When documenting a crime scene, the computer and surrounding area should be photographed, detailed sketches should be made, and copious notes should be taken, because:

a. The more evidence collected, the stronger the case.
b. This provides a record for what to look for when you return for the second visit.
c. It is prudent to document the same evidence in several ways.
d. All of the above.

7. In regard to preservation, in a child pornography investigation, which of the following should be collected?
    a. Photographs
    b. Papers
    c. Digital cameras
    d. All of the above

8. If it is determined that some hardware should be collected, but there is no compelling need to collect everything, the most sensible approach is to employ:
    a. Nearest reach doctrine
    b. Direct connectivity doctrine
    c. Independent component doctrine
    d. Slice-the-pie doctrine

9. A crime scene investigator decides to collect the entire computer. In addition, he decides to collect all of the peripheral devices associated with that computer. What reason could he give to justify this?
    a. It is especially important to collect peripheral hardware related to the type of digital evidence one would expect to find in the computer.
    b. Since the computer is being collected, the suspect has no need for the peripherals.
    c. The presence of the peripheral devices is essential to imaging the suspect hard drive.
    d. None of the above.

10. According to the us Federal guidelines for searching and seizing computers, safe temperature ranges for most magnetic media are:
    a. 60-80 degrees Fahrenheit
    b. 50-90 degrees centigrade
    c. 50-90 degrees Fahrenheit
    d. 60-80 degrees centigrade

11. Which of the following is NOT an artifact that will be irrevocably lost if the computer is shut down?
    a. Running processes

b. Open network ports
c. Data stored in memory
d. System date and time

12. Which of the following is NOT one of the recommended approaches to preserving digital evidence?
    a. Place the evidential computers and storage media in secure storage for later processing.
    b. Preview the evidential computer, taking appropriate notes.
    c. Extract just the information needed from evidential computers and storage media.
    d. Acquire everything from evidential computer and storage media.

13. The reason UNIX "dd" is considered a de facto standard for making bitstream copies is:
    a. The majority of tools for examining digital evidence can interpret bitstream copies.
    b. "dd" stands for "digital data" and was developed for making forensic copies.
    c. "dd," although a UNIX tool, is universally able to traverse Windows file systems.
    d. The developers of "dd" have made arrangements with other forensic software companies.

14. Regarding the examination of a piece of digital evidence, which of the following is NOT one of the fundamental questions that need to be answered?
    a. What is it (identification)?
    b. What classifications distinguish it?
    c. Where did it come from?
    d. What is its value?

15. The file signature of a Microsoft Word document is an example of what type of characteristic?
    a. An individual characteristic
    b. A class characteristic
    c. An intermediate characteristic
    d. A medial characteristic

True or False Questions

1. Since computer seizures usually happen pretty much the same way, there is no real need to do any pre-planning.
    a. True
    b. False

2. If possible, prior to entering a crime scene, it is useful to try and determine what kind of computer equipment to expect.
    a. True
    b. False

3. A forensic crime scene processing kit should contain quantities of those items used to process computer equipment.
    a. True
    b. False

4. When surveying the crime scene for hardware, the investigator should focus on the computer systems since that is where most of the important evidence will be.
    a. True
    b. False

5. Chain of custody documents record who handled the evidence, when, where, and for what purpose.
    a. True
    b. False

6. It is not prudent to document the evidence more than one way.
    a. True
    b. False

7. The severity and the category of cybercrime largely determine how much digital evidence is collected.
    a. True
    b. False

8. Under independent component doctrine, if a computer system must remain in place but it is necessary to take the original hard drive, a reasonable compromise is to duplicate the

hard drive, restoring the contents onto a similar hard drive that can be placed in the computer, and to take the original into evidence.

a. True
b. False

9. At a crime scene, digital evidence will be found on the computer, on mobile devices, and on shelves, bookcases, and the area surrounding the computer. Therefore, there is no need to search the garbage for evidence.

a. True
b. False

10. When a computer is to be moved or stored, evidence tape should be put around the main components of the computer in such a way that any attempt to open the casing or use the computer will be evident.

a. True
b. False

11. The updated ACPO recommendation for seizing a running computer is to pull the electrical cord from the back of the computer.

a. True
b. False

12. A sound forensic practice is to make at least two copies of digital evidence and to confirm that at least one of the copies was successful and can be accessed on another computer.

a. True
b. False

13. Given the risks of collecting a few files only, in most cases it is advisable to preserve the full contents of the disk.

a. True
b. False

14. Computers used to store and analyze digital evidence should be connected to the Internet, so that online research can be conducted.

a. True
b. False

15. “dd” is the only way to make a bitstream copy.

a. True
b. False

Essay Questions

1. List the class and individual characteristics of each of the following:
   - A JPEG file
   - A thumb drive
   - A user manual with handwritten notes

Answer guidance: Class characteristics are generally true for a particular object. Individual characteristics are how that object has been changed by the user.

2. You have arrived at a crime scene containing one computer, one printer, connecting cables, connection to a phone line, and a shelf above the computer containing books, user manuals, and printouts.

What is your first step in processing the crime scene?

Would you seize the computer? If so, would you seize the printer?

What communication issues do you see with the above installation?

Project

Research and report on the origins and both the intended and unintended uses of the UNIX program "dd."

Chapter 17
Digital Evidence on Windows Systems

On completion of this chapter, the student will:

- Be aware that Windows-based systems will comprise the majority of cases.
- Recognize that powerful forensic tools are not a substitute for knowledge and experience and in each of the following areas:
    - File systems
    - Data recovery
    - Log files
    - Registry
    - Internet traces
    - Program analysis
- Be aware of the workings of each of the file systems covered.
- Recognize how dates and times are recorded in various Windows file systems.
- Be aware that currently there are no tools available to analyze NTFS journaling.

Chapter Guide

The Windows environment is complex and poses a number of challenges for the forensic examiner (FE). Some issues include:

- Invasive characteristics of the Windows environment (invasive because it does not mount disks read-only).
- The way Windows file system(s) are implemented.
- No facility in the Windows environment for mounting a hard drive as Read-Only.
- The location, organization, and content of Windows system log files.
- Available methods for recovering data from Windows media.
- Exploiting Windows file system traces.
- Analyzing the Windows Registry.
- Internet usage analysis in the Windows environment.
- Program effects analysis.

The forensic examiner must constantly strive to be current with new developments (such as cloud computing) in hardware and software.

File systems

Windows supports a variety of file systems. Floppy disks are formatted FAT12 (each entry in the FAT is 12 bits). Hard drives may be formatted FAT16, FAT32, or NTFS. The FE must be sufficiently familiar with all supported file systems so that inconsistencies can be recognized.

Knowing what a "normal" file structure should look like and where data can be hidden in each file system is essential to successfully examining Windows media.

For FAT-based file systems, three data structures are created during the formatting process: MBR (Master Boot Record), two FATs (File Allocation Table), and a root directory. When the OS receives a request to open a particular file, it first searches the root directory and path to locate the file name. If successful, it reads other significant information stored in the file's directory entry, namely the file size (in bytes) and starting cluster. The OS retrieves the data from the specified cluster and checks the file size parameter to see if the file is larger than one cluster. If it is, the OS checks the FAT for the next cluster number and loads the data stored at that location. This procedure continues until the last of the file data is read. The FAT and directory entry are updated when the file is changed or deleted. Data can be hidden in a variety of places including the directory structure, unused areas of the FAT, between the end of file data and the cluster boundary (file slack), and unallocated space.

NTFS uses a different method, storing file information in the Master File Table (MFT) using a B-Tree (binary tree) structure. Deleted files may be more difficult to recover because NTFS creates entries as needed and reuses entries before creating new ones, making it more likely that a new file will overwrite an existing one. The data may be intact, but the file system references may be lost.

Overview of Digital Evidence Processing Tools

Forensic-recovery activities commonly carried out include:

- Previewing a drive for relevant data (keyword search)
- Evidence media acquisition
- Validation of evidentiary data
- Evidence analysis

In those cases where a large number of drives must be examined for specific information, the results of keyword searching will indicate which drives contain relevant information. WinHex Forensic, EnCase, DiskSearch Pro, and Linux have the capability to search for keywords.

When notable data is found, then that media becomes evidence and must be "acquired" – that is, copied completely. There must be a reliable method of verifying that the original and the copies are identical. Message hashing algorithms such as MD5 and SHA-256 are accepted as reliable methods for determining whether two blocks of data (file, drive, etc.) are identical. Safeback, WinHex Forensic, EnCase, Forensic Toolkit (FTK) Snapback DataArrest, and Byte Back all employ integrity checks to assure that copies are identical to the original, to the bit level.

Media can be examined either logically (accessed through the BIOS) or physically (accessed directly). Both methods have strengths and weaknesses and the choice is dependent on the circumstances. Logical access utilizes file structures, so file data is more easily examined. However, logical access may miss some data. Physical access, on the other hand, is more likely to get all available data. However, the interpretation of findings is more difficult due to absence of file and directory markers. The FE should be knowledgeable in either format, since both methods are likely to be used at some point in an examination. WinHex Forensic and Norton Diskedit can view media in physical mode – WinHex can also view it logically. Integrated applications like WinHex Forensic, EnCase, and FTK for Windows and The Sleuth Kit for Linux/UNIX can view data physically or logically. Be aware that, unless a particular application has undergone exhaustive validation testing, the FE has no guarantee that the displayed results represent actual data. By having an arsenal of tools, the FE can apply more than one tool to the target data, and compare the results.

Data Recovery

Although automated tools exist for recovering data, the FE *must* understand the fundamental underlying principles. Knowing how to manually recover damaged FATs and directories requires a level of understanding sufficient to enable the FE to explain the relevant processes to the court.

> "Then, Your Honor, I pressed 'R' for recover…" is *not* sufficient.

Deleted directory recovery is more complex. On Windows, Encase, FTK, and WinHex/X-ways Forensics can recover files and directories for FAT and NTFS. On UNIX, SMART and The Sleuth Kit can recover files and directories for FAT and NTFS. Another method for data recovery is called "file carving" and consists of examining raw data, usually in slack space, locating the beginning and end of a file, and "carving" this block of data out to a separate file, with the proper extension. The file is then examined with the appropriate application.

Dealing with Password Protection and Encryption

FEs are often required to overcome password protection and/or encryption. Hex editors like WinHex can sometimes be used to remove a password from a file. A variety of tools are available, both validated and unvalidated, for password cracking and can be found on the Internet. Test before using on an actual case.

Passwords may be at the BIOS, OS, and individual application level. The FE should have the resources available to overcome them at any level.

Encryption is another issue the FE must deal with. There are many levels of encryption, some much more secure than others. In the case where the level of encryption is measured in millions

of years to break, other means of obtaining the data must be utilized. Some encryption applications recommend the creation of a "recovery disk" in case the password is forgotten. The recovery disk allows the data to be recovered. Therefore, where encryption is employed, first responders should collect other media as well.

Log Files

No matter how incriminating the data found on a computer, it is necessary for the FE to associate that data with a suspect. There are many instances where the defense could argue that "anyone" could have accessed the target system. Log files are used by the FE to attempt to determine *who* was responsible for creating a particular piece of evidence.

Windows 9X/ME do not maintain log files. Windows NT/2000/XP have the capability of logging a great deal of information, but have to be configured in advance to do so. Objects tracked can include login/out (both successes and failures), user activities, Internet access, significant events, and other information. Log analysis is a critical skill for the FE.

File System Traces

Windows systems create a trail of events that are very difficult to completely eliminate. It takes a thorough understanding of system events to hide all traces of a particular act. A great deal of information can be derived from these traces. Date-time stamps of objects may substantiate or destroy alibis. Metadata may provide unencrypted versions of encrypted data. Print spoolers may contain data from documents that were completely erased. Once the FE has collected all the notable data, the significance of the data must be assessed. File system traces provide a clearer picture of how a particular piece of evidence came to be.

Registry

Windows stores configuration and usage information in the Registry. **Regedit** and **Regedt32** are tools to view and modify the Windows Registry. Among other useful things to be gleaned from the Registry is the use of removable drives. If working with a live system at the crime scene, the FE would examine the Registry for references to external storage devices.

Internet Traces

Systems connected to the Internet usually contain a wide variety of relevant data. Websites visited, e-mails, Internet cache, temporary Internet files, chat room logs, newsgroups accessed, and files downloaded are all examples of the types of data that would be of interest to an FE.

- **Web Browsing**

  The date-time stamp of an Internet cache file corresponds to the date and time that the web page was viewed. Correlate this with the date-time stamp of files downloaded to

determine the origin of such files. Browsers maintain a database of sites visited that remains intact when the cache files are deleted. This database (netscape.hst for Netscape and index.dat for Internet Explorer) can be mined for a wealth of information. Tools exist to display the contents in a usable format. The ubiquitous "cookies" that websites push onto a system may also provide useful information about what sites were visited and when.

- **Usenet Access**

  Usenet readers store all the URLs that have been accessed, as well as which Usenet newsgroups have been accessed and joined. Considerable information can be derived from this data.

- **E-mail**

  E-mail contents and header information can provide the FE with a great deal of information. It is necessary to have software that can read various proprietary e-mail formats and MIME encoded message attachments. The e-mail header information is frequently "spoofed," however, and the intermediate jumps that the e-mail packets took along the way can provide the FE with useful investigative leads.

- **Other Applications**

  Internet messengers such as AOL IM, Yahoo! Pager, and others are a good source for investigative leads. Peer-to-peer file sharing programs may retain information on the hosts visited. IRC and other chat clients may retain logs but only if configured to do so.

- **Network Storage**

  Indicators of remote storage are definitely of interest to the FE. With the proliferation of wireless home networks, it is conceivable that a suspect might be using his unsuspecting neighbor's wireless network to store pornographic images. File backup sites exist on the Internet. For that matter, the suspect's ISP may provide storage space for its customers. A search for the presence of file transfer programs may provide indicators to where such storage might be located. It is advisable to obtain the requisite legal permissions before accessing remote storage sites.

Program Analysis

There are times when a controlled experiment with a malicious program may provide insights on where to look for evidence on a case system. Recreating an intrusion on a test system will provide log entries, which can then be sought on the actual system. Analysis can be accomplished by:

- analyzing the source code
- analyzing the executable code
- running the code on a test system

The processes, such as network traffic, that occur when a particular application executes may be of interest to the forensic examiner.

Multiple Choice Questions

1. Which of the following issues is NOT one that a forensic examiner faces when dealing with Windows-based media?
    a. Invasive characteristics of the Windows environment
    b. The facility in the standard Windows environment for mounting a hard drive as Read-Only
    c. The location, organization, and content of Windows system log files
    d. Available methods for recovering data from Windows media

2. Forensically acceptable alternatives to using a Windows Evidence Acquisition Boot Disk include all but which of the following?
    a. Linux boot floppy
    b. FIRE bootable CD-ROM
    c. Booting into safe mode
    d. Hardware write blockers

3. The standard Windows environment supports all of the following file systems EXCEPT _____.
    a. FAT16
    b. ext2
    c. FAT32
    d. NTFS

4. Before evidentiary media is "acquired," forensic examiners often _____ the media to make sure it contains data relevant to the investigation.
    a. Hash
    b. Preview
    c. Validate
    d. Analyze

5. Media can be accessed for examination either _____ or _____ . (Choose two)

    a. Logically

b. Sequentially
c. Randomly
d. Physically

6. 6. Which of the following software tools is NOT used for data recovery?
   a. WinHex (X-Ways) Forensic
   b. EnCase
   c. FTK
   d. Safeback

7. You find the following deleted file on a floppy disk. How many clusters does this file occupy?

Name	.Ext	ID	Size	Date	Time	Cluster	76 A R S H D V
_REENF~1	DOC	Erased	19968	5-08-03	2:34 pm	275	A - - - - -

   a. 200
   b. 78
   c. 39
   d. 21

8. Log files are used by the forensic examiner to _____.
   a. Associate system events with specific user accounts
   b. Verify the integrity of the file system
   c. Confirm login passwords
   d. Determine if a specific individual is the guilty party

9. The Windows NT Event log Appevent.evt:
   a. Contains a log of application usage
   b. Records activities that have security implications, such as logins
   c. Notes system events such as shutdowns
   d. None of the above

10. When examining the Windows registry key, the "Last Write Time" indicates:
    a. The last time RegEdit was run
    b. When a value in that Registry key was altered or added
    c. The current system time
    d. The number of allowable changes has been exceeded

11. File system traces include all of the following EXCEPT:
    a. Metadata
    b. CMOS settings
    c. Swap file contents
    d. Data object date-time stamps

12. When a file is moved within a volume, the Last Accessed Date Time:
    a. Is unchanged
    b. Changes if a file is moved to different directory
    c. Changes if a file is moved to the root
    d. Is unchanged; however, the Created Date-Time does change

13. Internet traces may be found in which of the following categories?
    a. Web browser cache
    b. Instant messenger cache
    c. Cookies
    d. All of the above

14. The Windows NT Event log Secevent.evt:
    a. Contains a log of application usage
    b. Records activities that have security implications, such as logins
    c. Notes system events such as shutdowns
    d. None of the above

15. When examining the "news.rc," you find the following entry:

    alt.binaries.hacking.utilities! 1-8905,8912,8921,8924,8926,8929,8930,8932

    What does the "!" mean?
    a. The user is subscribed to this group.
    b. The user was once subscribed, but is currently unsubscribed, to this group.
    c. The group is up to date.
    d. The last message retrieval was aborted.

True or False Questions

1. Given their widespread use and simple structure, FAT file systems are a good starting point for forensic analysts to understand file systems and recovery of deleted data.
    a. True
    b. False

2. Usenet readers store all the URLs that have been accessed, but do not record which Usenet newsgroups have been accessed and joined.
    a. True
    b. False

3. The Windows environment is invasive and poses a challenge to forensic examiners.
    a. True
    b. False

4. With the correct CMOS setting, it is possible to mount a hard drive as Read-Only in the Windows environment.
    a. True
    b. False

5. EnCase provides the means to create a Windows Evidence Acquisition Boot Disk to allow for network acquisition of an evidence drive.
    a. True
    b. False

6. Windows evidentiary media *must* be acquired and examined with Windows-based examination software.
    a. True
    b. False

7. NTFS time represents time as the number of 100-nanosecond intervals since January 1, 1601 00:00:00 UTC.
    a. True
    b. False

8. In FAT32 file systems *both* the directory and FAT entries are updated when a file is deleted.
    a. True

b. False

9. EnCase can recover deleted files but does not have the capability of recovering deleted directories.
    a. True
    b. False

10. In the Windows environment, simply opening a file to read, without writing it back to disk, can change the date-time stamp.
    a. True
    b. False

11. In NTFS, when a file is deleted from a directory, the last modified and accessed date-time stamps of the parent directory listing are updated.
    a. True
    b. False

12. The MD5 hashing algorithm is no longer considered to be a reliable method for determining whether two blocks of text are identical.
    a. True
    b. False

13. A forensic examiner would use logical access to examine media if the file and directory structures were to be analyzed.
    a. True
    b. False

14. “File carving” is an examination technique where the beginning and end of a file are located, and the block of data spanning the two locations is copied to a new file, with the appropriate extension.
    a. True
    b. False

15. Just like Windows NT, Windows 98 has event logs that record system activities.
    a. True
    b. False

Essay Questions

For each of the following questions, develop discussion notes and be prepared to discuss your findings.

1. Is it necessary for forensic examiners to understand how data is stored by various types of file systems? Explain why or why not. Support your answer with examples.

2. When examining evidence media, is it necessary to use the same operating system used on the original? Explain why or why not. Support your answer with examples.

3. Is the data-time stamp of various file system objects significant in the analysis of evidentiary media? Explain why or why not. Support your answer with examples.

Scenario

You are the digital forensic examiner at a pre-trial session with the judge and opposing counsel. You have been asked to explain the various methods that data is stored and erased in the Windows environment. Your discussion should include concepts such as slack space, unallocated space, the sequence of events that take place when a file is deleted, and any other points that you deem important. Keep in mind that you must prepare your discussion in terms that non-technical people can understand.

Chapter 18
Digital Evidence on UNIX Systems

On completion of this chapter, the student will:

- Recognize that most UNIX systems information is available for review.
- Be aware that the openness of UNIX systems presents both opportunities and challenges to digital investigation.
- Recognize the values and limitations of using UNIX-based acquisition boot disks.
- Be aware that there are many different UNIX file systems, the most common of which are:
  - UFS
  - Reiser
  - ext2
  - ext3
- Recognize that many native UNIX tools are useful to the digital examiner.
- Recognize that there are numerous open source UNIX-based forensics tools available.
- Be aware that currently there are no tools available that can analyze the ext3 journaling system.
- Be aware that UNIX does not have a file slack.
- Be aware that *some* automated forensic tools can process *some* portions of UNIX file systems.
- Recognize that deleted data on UNIX file systems can be recovered by data carving.
- Be aware of possible solutions for passwords and encrypted files on UNIX systems.
- Recognize the value of examining UNIX log files in the course of an investigation.
- Be aware of the variety of file system traces that may be found on a UNIX system.
- Recognize the value of network traces.

Chapter Guide

Various permutations of UNIX (Solaris, AIX, HP-UX) have been around for over 30 years. It is an extremely stable, powerful multi-user environment with built-in support for networking. Because some of the variants have been made available under Open Source agreements (Linux, OpenBSD, FreeBSD), startup implementation costs have been minimized. In addition, a great deal of software have also been released under Open Source agreement, providing a wide range of low cost applications, making UNIX implementations very popular, especially for e-commerce, information security, and digital forensics. Apache Webserver, which comes with most Linux distributions, is one of the most widely used web servers on the Internet.

The UNIX environment makes a large portion of system information such as configuration files and system logs readily available. This is UNIX's greatest strength and its greatest weakness.

UNIX Evidence Acquisition Boot Disk

A fundamental capability of the UNIX file system is to mount storage devices as Read-Only. However, there is still a *possibility* that it could make changes on an evidentiary device, so a hardware write-blocker can be used. (Recall that this capability is NOT supported in the standard DOS/Windows environments.) Since this capability is inherent in the UNIX environment, making an Evidence Acquisition boot disk is the straightforward process of making some media such as a bootable CD-ROM bootable in a UNIX variant and including the software tools needed for acquisition, validation, and analysis. Keep in mind that UNIX and its variants are, by nature, hardware specific. A boot disk created for Sun SPARC systems will most likely not work on an Intel-based system. Another consideration is the availability of device drivers. An Evidence Acquisition boot disk should contain drivers for various kinds of removable storage such as USB and Firewire.

File Systems

UNIX supports several file systems such as UFS (UNIX File System), ext2 and ext3 (Extended File System 2 and 3), and Reiser. They all have similar structures for managing the file system. Each UNIX partition is divided into block groups (aka "cylinder groups"). Each block group contains, among other things, an inode (index node) table. An inode table consists of entries representing either directories or files. A directory inode entry contains the names of those files and directories associated with it, and their respective inode numbers. A file inode entry contains all of the file's information except its name (i.e., owner/group ID, permissions, file type, date-time stamps, reference count, file size in bytes, data block numbers). The file block numbers point to the actual data. In addition to containing data, each block group contains duplicates of critical file system components, that is, the superblock and group descriptors to facilitate recovery if the primary copy is damaged. The superblock contains information about the file system such as block size, number of blocks per block group, the last time the file system was mounted, last time it was written to, and the sector of the root directory inode.

UNIX adds another time to the MAC (modified, accessed, created) times referenced in the chapter on Windows systems – Deleted time. If a file or directory is not deleted, the Deleted Time value is set to a default time – zero from the UNIX standpoint, as it represents time in epoch time (the number of seconds since January 1, 1970, 00:00:00 UTC).

UNIX ctime is not equivalent to NT FS creation time. In UNIX a change (ctime) alters a file's inode. A modification (mtime) alters the contents of the file.

When a file is deleted, its directory entry is hidden and the associated inode is marked as available. The directory entry and data remain on the disk until they are overwritten and, therefore, may be recoverable.

Overview of Digital Evidence Processing Tools

Linux has a number of features that make it an ideal choice for forensic examinations:

- A great many utilities useful for conducting forensic examinations come with the standard distribution (dd, md5sum, grep).
- The system pipe ("|") allows the output of one tool to be "piped" as input for another tool. A single command may move data through several tools and into a final text file.
- Linux supports a variety of file systems types, facilitating the examination of foreign file systems.
- Linux permits direct access to devices and may allow data to be recovered that would not be accessible through the file system.
- Linux is Open Source, with its inherent support base.
- There exists a large body of third-party tools suitable for conducting forensic examinations.

Data Recovery

UNIX file systems, unlike DOS/Windows, do not have slack space. The data area either contains data or is unallocated. Deleted data is treated as unallocated space. UNIX attempts to reuse existing inodes before allocating new ones, so there is an increased likelihood of losing data.

UNIX-based Tools

There are several methods available for recovering deleted files:
- Search for specific inodes and recover the data associated
- Search directories for deleted entries

Windows-based Tools

In the Windows arena, there are a few forensic examination software tools that can recover deleted UNIX files.

- EnCase can recover deleted file data, placing them all in a "Lost Files" area, however, it does not currently refer data using inode numbers or recover deleted directory entries.
- FTK can recover deleted files and directories from ext2, into an area called "[orphan]".

File Carving with UNIX

Software tools that can be used for recovering file data directly from data blocks include:
- **foremost** – this open source program from sourceforge.net can recover unfragmented files by searching for file signature headers and footers and copying the data inclusively into sequentially numbered files with the correct extension.

- **Lazarus** – a TCT (The Coroner's Toolkit) utility uses a similar, though more thorough, method for carving out file data.

Dealing with Password Protection and Encryption

Although it is possible to connect PCs into "Beowulf clusters," essentially arrays of parallel processing units, strong encryption would still require months, years, decades, or even longer to be broken. The forensic examiner seldom has the luxury of that much time.

An understanding of how encryption is typically conducted can lead to the unencrypted data. For example, if a file is encrypted, then two copies exist. If the plaintext copy is just deleted, it may be recovered.

Encrypted log-on passwords can be recovered using brute-force password guessing programs like Crack and Jack the Ripper. Booting into single user mode and modifying the password file can allow access in multiuser mode.

Log Files

Virtually every system event, including log-on and log-off, is logged somewhere in one or more system logs, depending on how the system is configured. Log analysis tools are available to correlate various log entries when reconstructing system events.

(See DECC2e, p. 311, for further information.)

File System Traces

Data remnants can be found in the data area or in swap space. Print spoolers and other applications create recoverable temporary files. As stated earlier, the deleted plaintext version of an encrypted file may be recoverable. MAC (Modify, Access, Create) and Deleted times can be recovered. The examiner uses this information to reconstruct system events, and create activity charts and a variety of other relevant information. (See pp. 311-315 for further information and examples.)

Internet Traces

UNIX is first and foremost a networking environment and there are many applications for connecting to the Internet. Although most of these applications do not create logs, they leave behind many recoverable traces.

Web Browsing

Web browsers keep track of sites visited in history and cache files. Examiners can examine this data to determine where a user has been, and when.

E-mail

Incoming e-mail is stored in "/var/spool/mail" under each user's account name. Outbound e-mails are temporarily stored in "/var/spool/mqueue/mail". In most cases e-mails are stored as plaintext, but MIME-encoded attachments require special software for decoding. Proprietary e-mail formats such as Outlook and AOL usually should be viewed in their respective applications.

Network Traces

The network-based nature of UNIX requires that forensic examiners always look for evidence of network connections. Many networked applications retain activity logs and configuration files. Evidence of shared network drives should also be sought. (See DECC2e, pp. 319-320, for further information.)

Summary

As there are a great many UNIX-based systems fielded, it is extremely likely that a forensic examiner will encounter such systems on a frequent basis. Therefore, a thorough understanding of how data is stored on UNIX-based systems is essential.

Multiple Choice Questions

1. Unlike the standard DOS/Windows environments, the UNIX environment has the capability of _____, thereby preventing the contents of evidentiary media from being changed.
    a. Encrypting all data on the media
    b. Copying the contents of the media
    c. Warning the examiner of an impending write
    d. Mounting storage media as Read-Only

2. What is the most efficient method for a forensic examiner to confirm whether a particular tool or methodology works in a forensically acceptable manner?
    a. Search the Internet for accounts of other examiners using the tool or methodology
    b. Contact the author of the tool or methodology and have them provide confirmation
    c. Test the tool under controlled conditions
    d. Contact other forensic examiners to determine if they have any experience with the tool or methodology

3. The inode table can be found in the _____.
    a. Block group
    b. Superblock table
    c. MBR
    d. Partition table

4. In a block group, file data is located in _____.
    a. The block bitmap
    b. Data blocks
    c. Inode bitmap
    d. Directory entry

5. _____, which is part of the standard Linux distribution, can be used to make a bitstream copy of evidentiary media to either image files or sterile media.
    a. grep
    b. icat
    c. dd
    d. sha1sum

6. MAC times, which are found in the _____, are an example of file system traces.
    a. Inode table
    b. MBR's partition table

c. Inode bitmap
d. Data blocks

7. Why is it important to determine the level of network connectivity on a UNIX system as soon as possible?
    a. As UNIX Systems may be configured to store critical evidence on remote systems, network connections must be determined and exploited before any evidence stored remotely is destroyed.
    b. To keep suspects and spectators from accessing the target system during the investigation.
    c. To determine if the system administrator is a suspect.
    d. None of the above.

8. The Coroner's Toolkit and The Sleuth Kit are examples of open source _____.
    a. Hard drive repair tools
    b. System administrator tools
    c. Forensic examination tools
    d. Network management tools

9. In UNIX, when a file is moved within a volume, the inode change date-time (ctime) is:
    a. Unchanged
    b. Updated
    c. Set to epoch time
    d. Set to last modified date-time

10. Deleting a file has the effect of preserving its inode until it is reused because:
    a. The inode is flagged as deleted.
    b. The inode table entry is moved to the recycle bin.
    c. Deleted inodes are not accessible to the file system.
    d. The inode number is added to a deleted files journal entry.

11. When a file is deleted on a UNIX System, the ctime of its parent directory is:
    a. Unchanged
    b. Updated
    c. Set to epoch time
    d. Set to last modified date-time

12. One of the most common web browsers on UNIX systems is:
    a. Internet Explorer

b. Safari
c. Opera
d. FireFox

13. FireFox 3 stores potentially notable information in:
    a. DBF format databases
    b. ASCII text files
    c. SQLite databases
    d. Proprietary format files

14. On UNIX systems that receive e-mail, incoming messages are held in _____, in separate files for each user account until a user accesses them.
    a. /home/<useraccount>/desktop/mail
    b. /var/spool/mqueue/mail
    c. /etc/mailbox/mail
    d. None of the above

15. The file system mount table shows local and remote file systems that are automatically mounted when the system is booted. This information is stored in:
    a. /etc/fstab
    b. /etc/mount/mtab
    c. /etc/hosts
    d. None of the above

True or False Questions

1. One of the most useful areas to search for notable data on a Linux system is in file slack.
    a. True
    b. False

2. One of the difficulties in examining UNIX systems is that the file system is extremely complex, making it difficult for the examiner to recover data.
    a. True
    b. False

3. grep is a standard Linux tool that searches a specified file or region for a specified string.
    a. True
    b. False

4. The UNIX convention of "piping" the results of one command into another is a serious limitation and is detrimental to using the UNIX platform for forensic examinations.
    a. True
    b. False

5. Most data-carving tools operate on the assumption that the operating system generally tries to save data in contiguous sectors.
    a. True
    b. False

6. Given a sufficiently powerful computer, even "strong" encryption can be broken in a short time.
    a. True
    b. False

7. As UNIX was never designed to work on networks, there are very few native utilities designed to access the Internet.
    a. True
    b. False

8. UNIX log files (or those of any operating system, for that matter) can provide a great deal of useful information to the examiner.
    a. True
    b. False

9. On UNIX systems, e-mails and all attachments are stored as plaintext in "/var/spool/mail," or "/var/mail," or in a directory under the user's account.
    a. True

b. False

10. When examining a UNIX system, searching for network traces is not usually necessary.
    a. True
    b. False

11. When requesting a search warrant, remotely connected systems cannot be considered part of the target system, so it may be necessary to obtain proper authorization before examining them.
    a. True
    b. False

12. A list of currently mounted drives, including those not listed in the file system mount table, is kept in "/etc/mtab."
    a. True
    b. False

13. When a target system is connected to other systems in remote locations, it is expedient for the digital investigator to access these systems via remote access.
    a. True
    b. False

14. The "istat" command, found in The Coroner's Toolkit, can be used to examine specific inode bitmaps.
    a. True
    b. False

15. The mainstay of acquiring digital evidence using UNIX is the "icopy" command.
    a. True
    b. False

Discussion Questions

For each of the following questions, develop discussion notes and be prepared to discuss your findings.

1. Consider the statement "Forensic examiners should have a high degree of competence in all operating systems and their respective file systems." Do you agree or disagree? Support your answer with examples.

2. Which is the more effective forensic examiner, one who can operate forensic tools in a variety of operating environments (operating system, file system, etc.) and conducts examinations in the native environment of the evidentiary media, or one who thoroughly understands a single operating environment and examines evidentiary media in that environment, regardless of the native operating environment of the media. Support your answer with examples.

Scenario

You are on-site, conducting a preliminary examination of a Linux system. The hardware suite includes a 56KB modem. What areas of search should be included in your examination? Prepare an examination plan that details what you will look for, and why.

Chapter 19
Digital Evidence on Macintosh Systems

On completion of this chapter, the student will:
- Be aware of how to HFS (and HFS Plus) manage folders and files.
- Recognize the unique features of HFS.
- Be aware of the differences between HFS and HFS Plus.
- Be aware of various data recovery methods that can be used for HFS.
- Recognize the forensic value of file carving and HFS.
- Be aware of what file system traces to expect in HFS.
- Be aware of the differences in date-time stamp behavior in HFS.
- Be aware of various methods for processing Internet traces.
- Be aware of how an e-mail is implemented in the Macintosh.

Chapter Guide

Macs represent a small but growing segment of the total number of computers and are sufficiently common to crop up frequently in digital investigations. Therefore, forensic examiners must be prepared to collect and analyze data from the Mac environment. This task can be a challenge as there are currently very few Mac tools that specifically address forensic recovery. In addition, the integration of UNIX into Mac OS X and the flexibility of the Mac file systems can create a complex digital crime scene. At the same time, as with other computer systems, there are many interesting nooks and crannies on Macs where digital dust can gather, and forensic examiners who familiarize themselves with these systems will be rewarded with useful digital evidence.

Unlike Intel-based systems, Macs do not have a BIOS per se. Instead, they use Open Firmware that can be opened using the "Command+Option+o+f" key combination at the beginning of the boot process. The current system date and time is generally visible in the opening message of newer versions of Open Firmware.

As with Windows, the Mac boot process is very invasive. To prevent altering evidentiary data, conventional wisdom dictates that the hard drives be disconnected before attempting to power up a Mac. Mac-formatted drives can be acquired in the Linux environment using dd, and likewise can be acquired in the Windows environment using tools such as EnCase or WinHex. WinHex Forensic can acquire and examine any cluster-based file system.

The Mac file systems (16-bit HFS and 32-bit HFS+) are structured similar to other file systems discussed in the text. Boot records reside at the beginning of each volume. System file structures consist of Catalog files and Extents Overflow files. Relevant to forensic examiners is how date-time stamps are recorded.

Catalog file records are organized in a balanced tree (B-tree), a storage structure optimized for searching. Each record contains a Catalog Node ID. Four types of records are supported: folders, files, folder threads, and file threads. Notable data such as folder and file names and MAC times can be found here. Data are stored in two places on the disk. Data type is determined by both extent and relevant information stored in the Catalog file. (See Section 12.1 for details.)

Deletion of a file results in it being moved to the Trash folder but it is not marked as deleted until it is removed from the there. When a file is deleted, its key length is zeroed and reference to it *may* be removed from the catalog. The net result is that the data may only be recoverable by keyword search of unallocated space.

Norton UnErase has a good likelihood of recovering erased files. Other tools, such as Disk Warrior and ProSoft Data Rescue, work well, also. Using several of the tools in combination increases the likelihood of data recovery. Alternatively, file carving tools such as EnCase and WinHex can be used to block file data and save it to a new file.

Older Macintosh systems do not keep logs but Mac OS 9 and Mac OS X have a logging capability. Of interest to examiners are the systems logs that Mac OS X keeps. Some items tracked such as external media connected to the computer, user logon/logoff activity, and system clock changes can be evident from temporal discontinuities in these logs. Macs also keep records of recently accessed applications and documents. Tools like Desktop DB Diver can provide a great deal of information about what applications have been accessed. Also of interest is how Macintosh handles file deletions – files are moved to the "Trash" folder. Examination of Desktop DB and Desktop DF may reveal the user's activities.

Mac OS 9 and X are network-aware, and keep exploitable network-related information. Also, Internet applications record activities to some degree. Netscape history files are exploitable and may contain a great deal of notable data. Internet Explorer maintains a history of browsing activities in History.html, Downloads.html, as well as .WAF cache files, and stores cookies in various locations, depending on version. The amount and quality of e-mail related data is dependent on the application – some log a great deal of information and others do not.

The single biggest obstacle to successfully exploiting Macintosh computers is limited choice in forensic tools designed with the Mac in mind. Therefore, to be effective, examiners must know where and how to look for information without the assistance of automated tools.

Multiple Choice Questions

1. Macintosh stores its partition table in:
    a. The last sector of the drive
    b. Non-volatile memory
    c. The first sector of the drive
    d. At offset 1024

2. The boot sector and additional details about the volume are stored in:
    a. The first sector of the volume
    b. At offset 0x300 from the beginning of the drive
    c. The last sector of the volume
    d. CMOS

3. HFS supports a maximum of _____ clusters.
    a. 2^8
    b. 2^{16}
    c. 2^{32}
    d. 2^{64}

4. HFS represents time as:
    a. The number of nanoseconds since January 1, 1601 00:00:00 GMT
    b. The number of milliseconds since January 1, 1980 00:00:00 GMT
    c. The number of seconds since January 1, 1601 00:00:00 GMT
    d. The number of seconds since January 1, 1904 00:00:00 GMT

5. The HFS equivalent to the NTFS MFT is:
    a. Lister file
    b. Files.db
    c. Catalog file
    d. Seeker.db

6. A difference between HFS and other file systems studied is that folders:
    a. Are listed in a separate Extents Overflow file
    b. Do not contain lists of their contents
    c. Do not show when they were last backed up
    d. Are stored in two places on the disk

7. It may not be possible to recover the file names and date-time stamps from an HFS volume with forensic tools because:
    a. That information is overwritten when a file is deleted.
    b. The inode table is deleted.
    c. That information is only held in memory.
    d. The B-tree data structure frequently rebalances.

8. The most common approach to salvaging deleted data on Macintosh systems is to:
    a. Use EnCase to recover the files.
    b. Use the Catalog utility.
    c. Use file carving techniques.
    d. There is currently no solution to recovering deleted files from a Macintosh.

9. On Mac OS X, when a file is deleted, it is copied to the:
    a. Recycler folder
    b. .Trash folder
    c. [orphans]
    d. None of the above

10. Recently accessed files and applications are listed in:
    a. ~/Library/Recent
    b. Catalog:Recent
    c. ~/Library/Preferences/com.apple.recent.items
    d. com.apple.TextEdit.plist

11. The last access times of files copied from a Mac running OS 9 onto a FAT-formatted disk are meaningless because HFS does not maintain:
    a. Access time
    b. Modified time
    c. Created time
    d. Ctime

12. The default browser used on Mac OS X is:
    a. Internet Explorer
    b. Safari
    c. Firefox
    d. Opera

13. The folder ~/Library/Mail Downloads contains:

a. Internet downloads
b. E-mails that contain attachments
c. Unread e-mails
d. E-mail attachments that have been opened

14. Keychains (~/Library/Keychains) are files that store:
a. Usernames and passwords
b. Private encryption keys
c. Favorite websites
d. Recent documents

15. When a file is deleted, its Catalog entry may be deleted as well. If this occurs,
a. A backup of the Catalog file will still contain the information.
b. All references to the data are removed from the disk.
c. The file information is moved to the Extent Overflow file.
d. The file information is moved to ".Trash," with the same name as the file, and an extent of ".info."

True or False Questions

1. There is a wide selection of forensic tools available for exploiting Macs.
   a. True
   b. False

2. Macintosh disks can only be examined on a Macintosh system.
   a. True
   b. False

3. By default, when Mac OS X boots up, it will attempt to mount an evidence disk.
   a. True
   b. False

4. HFS Plus stores file and folder names in Unicode format.
   a. True
   b. False

5. Examination of a Mac computer must be done manually – no automated tools exist.
   a. True
   b. False

6. On a Macintosh, when a file is deleted, its key length is set to zero.
   a. True
   b. False

7. Digital evidence examiners can use The Sleuth Kit on Mac OS X to examine NTFS, FAT, UFS, EXT, and HFS file systems.
   a. True
   b. False

8. Due to the design of the Macintosh Catalog file, it is easy to recover deleted files manually, using forensic tools.
   a. True
   b. False

9. Mac OS X has logging capabilities, but OS9 did not.
   a. True
   b. False

10. Internet Explorer cookies are always found in System Folder:Preferences:Explorer:Cookies.txt.
    a. True
    b. False

11. Typically, the degree of e-mail logging is dependent on the application.
    a. True
    b. False

12. By default, Eudora for Macintosh records more information than Eudora for Windows.
    a. True
    b. False

13. All ".plist" files are in plaintext.
    a. True
    b. False

14. In each volume of a Macintosh system, there is a database named "Desktop DB" that contains information about activities on the system including programs that were run and files and websites that were accessed.
    a. True
    b. False

15. One of the interesting file system traces that is created when files are saved from a Macintosh to external media formatted using FAT is a ". Spotlight" folder.
    a. True
    b. False

Discussion Questions

For each of the following questions, develop discussion notes and be prepared to discuss your findings.

1. Are Macintosh systems more or less useful than Windows systems as sources of digital evidence? Justify your answer.

2. It can be difficult to recover deleted files from HFS and HFS+ file systems manually. How can you assure yourself that automated tools used for this purpose are working correctly?

3. How does Mac OS 9 differ from Mac OS X and what significance does this have from a forensic perspective?

Scenario

You receive a Mac OS X system and are asked to summarize the applications and data on the hard drive. In addition, you are asked to report any recent system usage and any signs of encryption, external storage media, or clock tampering. What data would you look for on the hard drive, where would you find them, and what tools would you use?

Chapter 20
Digital Evidence on Mobile Devices

On completion of this chapter, the student will:

- Recognize that the use of cell phones and smart phones is an integral part of modern society.
- Recognize that mobile devices can contain vast amounts of personal information.
- Be familiar with the terminology used with mobile devices.
- Be aware that criminals will use and store information on mobile devices, providing an additional source for evidence.
- Be aware that the dynamic nature of mobile devices presents challenges to forensics examiners.
- Recognize that a major advantage of mobile devices from a forensic standpoint is that they can contain deleted information even after attempts to delete.
- Be aware that characteristics of Flash memory chips may result in the recovery of user-deleted information.
- Be aware that mobile devices have become a new target for malware developers.
- Recognize that mobile devices can connect to various networks via cellular towers, WiFi access points, and Bluetooth, and those connected networks may also contain notable data.
- Recognize that handheld devices may be synchronized to desktop applications, and notable data may be found there, as well.
- Recognize that information from mobile devices can assist the investigator in discovering the user's social network.
- Be aware that, while the same forensic principles apply to mobile devices as they do to regular computers, the dynamic, connected nature of mobile devices can present challenges.
- Be aware of the procedures for seizing mobile devices.
- Be aware of the value and benefits of first obtaining a physical acquisition of mobile devices.
- Be aware of the value of obtaining a logical acquisition of mobile devices.
- Be aware of various methods for acquiring mobile devices, such as:
    - Data cable
    - Bluetooth
- Be aware of various mobile device forensic tools currently on the market.
- Be aware of various methods of applying the forensic examination and analysis methodology to mobile devices.
- Be aware of various methods for data recovery on mobile devices.
- Be aware of the variety of formats used on mobile devices.
- Be aware of the issues involved with the acquisition and examination of SIM cards.
- Be aware of the forensic challenges relating to SIM card security.
- Recognize the value and the need to apply investigative reconstruction techniques to mobile devices.
    - Temporal analysis
    - Relational analysis
    - Functional analysis

Class Notes

The instructor should convey to the student that, because mobile devices are so pervasive and becoming more so every day, they should both expect and be prepared to deal with the ever growing variety of mobile devices. It would, in fact, be reasonable to expect to find a mobile device involved in nearly every type of case that law enforcement would counter.

Forensic examination and analysis of mobile devices presents challenges above and beyond those of traditional forensic investigations; however, the quality of the evidence obtained will make it worthwhile.

Multiple Choice Questions

1. Which of the following is NOT one of the methods mobile devices use to communicate?
    a. FDDI
    b. Telecommunication networks
    c. WiFi access points
    d. Bluetooth piconets

2. One major advantage of mobile devices from a forensic perspective is that:
    a. People very seldom delete information from mobile devices.
    b. The process for deleting information is much more complicated than for adding information, and users frequently don't delete things correctly.
    c. Flash memory is deleted block-by-block and mobile devices generally wait for a block to be full before it is deleted.
    d. Manufacturers reserve a part of memory for storing deleted items.

3. The reason that malware developers are beginning to target mobile devices is:
    a. Because available memory is much smaller and the operating system is much less sophisticated on mobile devices, it is much easier to develop malicious code.
    b. The malware market has become very crowded and developers are looking for new avenues.
    c. Since the coding is much simpler on mobile devices, many new programmers are trying at this particular platform.
    d. Since mobile devices are used more and more for online banking and making purchases, they have become prime targets for computer criminals.

4. Software designed to monitor activities on mobile devices has come to be called:
    a. Malware
    b. Spouseware
    c. Trojan defense
    d. None of the above

5. One of the dangers (from a forensic standpoint) of mobile devices is:
    a. Connected networks can contain investigatively useful information.
    b. Network service providers may provide information for comparison with data extracted from a mobile device.
    c. Connected networks can enable offenders to delete data remotely.
    d. Network service providers may provide additional historical call records.

6. One of the difficulties unique to forensic processing of mobile devices is:
    a. MD five hashes must be calculated for data recovered from mobile devices.
    b. Documentation must show continuous possession and control.
    c. An investigator must make a calculated decision to either prevent or allow the device to receive new data over wireless networks.
    d. Any issues encountered with processing the device should be documented.

7. Powering down a mobile device and removing the battery may cause problems in that:
    a. When the battery is removed from a mobile device, the information in memory is lost.
    b. Doing so may activate security measures such as lock codes and encryption.
    c. The process of removing the battering can cause a capacitive discharge, destroying the device.
    d. You now have two pieces of evidence, which have to be documented.

8. Which of the following are methods for preserving mobile devices by isolating them from the networks?
    a. Reconfigure the device to prevent communication from the network.
    b. Place the device in an RF-shielded pouch.
    c. Jam RF signaling in the immediate area.
    d. All of the above.

9. Why is it important to collect charging cables when seizing mobile devices?
    a. Mobile device batteries have a limited charge life span, and the device will need a charger to maintain the battery until the device can be processed.
    b. To reduce owner complaints about missing cables when, at some point, seized devices are returned.
    c. In those cases where evidence seized is forfeit, you want to make sure you have everything you need to operate the device.
    d. None of the above.

10. Which of the following is NOT one of the currently available methods for extracting data from mobile devices?
    a. Manual operation via user interface
    b. Logical acquisition via communication port
    c. Connecting the communication port directly to an output device such as a printer
    d. Physical acquisition via the communication port

11. Forensic examiners should be aware that a mobile device with a blank or broken display:
    a. May as well be thrown away, as no data will be recovered from it
    b. May only indicate that the screen is damaged and it may still be possible to extract data
    c. May require that the mobile device be sent out to the manufacturer for repairs
    d. None of the above

12. The IEEE standard that specifies a standardized interface for testing integrated circuits, interconnections between components, and a means of observing and modifying circuit activity during a component's operation is:
    a. RG-45
    b. FDDI
    c. WiMAX
    d. JTAG

13. A peculiarity of mobile devices is the format that they store SMS messages, which is:
    a. ASCII
    b. Unicode
    c. GSM 7-bit
    d. Baudot

14. Certain data on mobile devices, in particular phone numbers, are stored in "nibble reversed" format. In that case, the phone number 12025437078 would be displayed as:
    a. 2120457370F8
    b. 20217345870
    c. 87073452021
    d. 8F0737542021

15. The primary reason that brute-force methods are not used when trying to access an SIM card with the PIN set is:
    a. A four-digit PIN represents 10,000 possible combinations.
    b. After three failed attempts, the SIM card will become locked.
    c. PIN disclosure by the offender can be required by a court order.
    d. None of the above.

True or False Questions

1. Since mobile devices consist of a CPU, memory, storage, and software, the same as traditional computers, they are processed in exactly the same way.
    a. True
    b. False

2. Mobile devices are considered to be a type of embedded system.
    a. True
    b. False

3. Given the small amount of usable data obtainable from mobile devices, the forensic investigator needs to weigh the value of investing time examining mobile devices.
    a. True
    b. False

4. One drawback of mobile device examination is that when a user deletes data on a mobile device that data is never recoverable.
    a. True
    b. False

5. Mobile devices have become a promising new target for malware developers.
    a. True
    b. False

6. The dynamic nature of mobile device communications presents additional challenges for the forensic examiner.
    a. True
    b. False

7. Although mobile devices may connect to networks, WiFi and Bluetooth connections, and desktops synchronizing software, the forensic examiner should focus entirely on the mobile device itself.
    a. True
    b. False

8. There are currently no forensic tools available for processing mobile devices.
    a. True
    b. False

9. The forensic examiner's best option for the most complete collection of data from a mobile device is to make a physical acquisition.
    a. True

b. False

10. One of the difficulties in processing mobile devices is that the manufacturers always use proprietary storage formats.
    a. True
    b. False

11. When analyzing a GPS-enabled mobile device, it is often possible to recover location information, import it into mapping software, and display the locations on a map.
    a. True
    b. False

12. Something forensic examiners need to keep in mind when trying to brute force an SIM card that has had a PIN set is that the card will lock after the second failed attempt.
    a. True
    b. False

13. Best practices for seizing a mobile device is to power the device off and remove the battery so that no new connections are made over the network.
    a. True
    b. False

14. Certain data on mobile devices, particularly phone numbers, are stored in nibble-reversed format.
    a. True
    b. False

15. It is often possible to perform a forensic analysis of a physical duplicate of mobile devices using file system forensic tools.
    a. True
    b. False

Essay Questions

1. Discuss the preservation, examination, and analysis issues that make processing mobile devices unique.

Answer guidance: a "computer" as a communication device; full duplex communication from the network, nonstandard and proprietary data formats.

2. Discuss methodologies for processing a crime scene involving mobile devices. Take into account the special issues relating to mobile devices.

Answer guidance: search for media and SIM cards, seizing related peripherals and communication cables, charging stands, etc., how to isolate the device from the network(s), powering off issues.

Scenario

You are at a crime scene and a cell phone is discovered, powered on. Crime scene technicians have processed it for prints and turned it over to you. You are examining the interface when a text message is received. What steps will you take?

Chapter 21
Network Basics for Digital Investigators

- Be aware of the reasons that digital investigators have to have a thorough understanding of networks.
- Be aware of the hardware and protocols that constitute a network.
- Be aware of the various network technologies a digital investigator is likely to encounter.
- Be aware of the tools that assist in network investigations.

Chapter Guide

All digital investigators require some understanding of networks since most computers we encounter are connected to one. In fact, computers have become network-centered and it is no longer sufficient to only think of digital evidence on storage media. To comprehend traces of Internet activities left on personal computers and to establish continuity of offense, digital investigators require knowledge of evidence that exists on surrounding networks. These sources include server logs, network devices, and traffic on both wired and wireless networks.

This chapter provides an overview of network history, concepts, and the most common network technologies: ARCNET, Ethernet, FDDI, ATM, IEEE 801.11 (wireless), cellular, and satellite networks. Some students will be confused or intimidated by the concepts of TCP flows, network layers, log files, and remote access using applications like Telnet and SSH. Therefore, it is advisable to lead students through the reading and provide them with some hands-on exercises to ensure that the basic concepts are clear. The “Barbara the Bookie” exercise is designed to get students thinking about the different network technologies and how they might be encountered in an investigation. It is also instructive to have students connect to a remote system such as a backbone router as shown here:

> On August 15 at 11:20 EDT, Telnet was used to connect from a Windows machine to a public Internet router (see www.traceroute.org for a list of route servers).

```
C:\> telnet route-server.ip.tiscali.net

+--------------------------------------------------------------------+
|                                                                    |
|           TISCALI International Network - Route Monitor            |
|                           (AS3257)                                 |
|                                                                    |
|   This system is solely for internet operational purposes. Any     |
|   misuse is strictly prohibited. All connections to this router    |
|   are logged.                                                      |
|                                                                    |
|   This server provides a view on the TISCALI routing table that    |
|   is used in Frankfurt/Germany. If you are interested in other     |
|   regions of the backbone check out http://www.ip.tiscali.net/lg   |
|                                                                    |
|   Please report problems to noc@tiscali.com                        |
+--------------------------------------------------------------------+

route-server.ip.tiscali.net>show clock
*16:30:32.532 CEDT Sun Aug 15 2004
```



```
route-server.ip.tiscali.net>who
    Line       User       Host(s)              Idle       Location
*  2 vty 0                idle                 00:00:00
                                      pool-141-157-94-144.balt.east.verizon.net

  Interface    User               Mode         Idle     Peer Address

route-server.ip.tiscali.net>show log
Syslog logging: enabled (10 messages dropped, 4 messages rate-limited, 0 flushes
, 0 overruns, xml disabled)
    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled
    Buffer logging: disabled, xml disabled
    Logging Exception size (8192 bytes)
    Count and timestamp logging messages: enabled
    Trap logging: level debugging, 17859 message lines logged
        Logging to 213.200.88.198, 17859 message lines logged, xml disabled
```

In addition to demonstrating client-server interaction, this exercise gives routers and the Internet backbone a tangible form that students may not otherwise realize. Notably, the router's clock indicates that it is 16:30 Central European Time (GMT + 1) whereas the time according to the Windows host was 11:20 US Eastern Time (GMT – 5). Pointing out to students that router clocks often drift when they are not synchronized with a reliable source can emphasize the need for documenting the system clock on any system that they are collecting evidence from. Also, the results of the `show logging` command contain the remote syslog server (213.200.88.198 = flowscan.ip.tiscali.net) that receives logs from this router.

In addition, the Open System Interconnection (OSI) model is used in this chapter to give the reader an understanding of the different functions of networks and the types of crime and associated evidence that exist. The OSI model is comprised of seven layers summarized here:

#	Name	Summary
1	Physical	Media that carries data (e.g., network cable)
2	Data-link	Enables basic network connectivity between computers connected directly by the same network technology (e.g., Ethernet)
3	Network	Routes information to its destination using addresses (e.g., IP addresses)
4	Transport	Establishes, maintains, and terminates connections between hosts (e.g., TCP)
5	Session	Maintains connections between hosts to ensure continuity when the communication on underlying network layers disconnect or fail (e.g., RPC used by Windows and UNIX to maintain connections to network file shares)
6	Presentation	Formats and converts data to meet the conventions of the specific computer being used (e.g., ASCII versus EBCDIC)
7	Application	Creates network functionality that enables services like e-mail (e.g., SMTP)

Data in each layer are encapsulated by lower layers. For example, an e-mail message is encapsulated in an IP datagram, which in turn is encapsulated in an Ethernet frame. Notably, the OSI model does not fit

exactly with TCP/IP, the most widely use Internet protocols, but there is sufficient overlap for our purposes.

Multiple Choice Questions

1. An understanding of networks helps with which of the following:
   a. Establishing continuity of offense
   b. Tracking down offenders
   c. Understanding traces of online activities left on a PC
   d. All of the above

2. When a Windows system connects to a shared folder on another Windows machine on the Internet, which of the following protocols are used?
   a. TCP/IP
   b. SMB
   c. NetBIOS
   d. All of the above

3. Hosts that connect two or more networks are called:
   a. Routers
   b. Switches
   c. Hubs
   d. All of the above

4. Which of the following are Layer 7 protocols?
   a. Ethernet
   b. HTTP
   c. TCP
   d. All of the above

5. Which of the following is a wireless protocol?
   a. 802.11b
   b. 802.11x
   c. HyperLAN2
   d. All of the above

6. Ethernet uses which of the following technologies?
   a. CDPD
   b. CSMA/CD
   c. CDMA
   d. All of the above

7. Which of the following is a Layer 2 address?
   a. 00-02-2D-65-C9-83
   b. 192.168.9.5
   c. 121.19.7.360
   d. 1042556

8. Another name for a hub is:
   a. Switch
   b. Router
   c. Concentrator
   d. NIC

9. Currently, the most widely used Internet protocols are:
   a. TCP
   b. UDP
   c. IP
   d. All of the above

10. The OSI reference model divides Internets into seven layers. Choose the correct order, by layer.
    a. Transport, Session, Network, Presentation, Data-link, Application, Physical
    b. Presentation, Data-link, Application, Physical, Transport, Session, Network
    c. Physical, Data-link, Network, Transport, Session, Presentation, Application
    d. Data-link, Network, Session, Application, Physical, Network, Session

11. The layer that actually carries data via cables or radio signals is the:
    a. Transport layer
    b. Physical layer
    c. Network layer
    d. Data-link layer

12. A hub joins hosts at the physical level whereas a switch joins them at the _____ layer.
    a. Transport
    b. Physical
    c. Network
    d. Data-link

13. The layer responsible for managing the delivery of data is the:
    a. Application layer
    b. Presentation layer
    c. Transport layer
    d. Session layer

14. ___is a transport layer protocol.
    a. TCP
    b. IP
    c. HTTP
    d. FTP

15. Which of the following network technologies uses a fiber-optic medium?
    a. Ethernet
    b. FDDI
    c. Asynchronous Transfer Mode
    d. 802.11

True or False Questions

1. An understanding of networks is only necessary for investigating computer intrusions and Denial Of Service attacks.
    a. True
    b. False

2. It is possible to reconstruct events surrounding a crime scene using only evidence on networks when the subject's hard drive is not available.
    a. True
    b. False

3. Ethernet frames are encapsulated within IP datagrams.
    a. True
    b. False

4. A switch prevents eavesdropping on a network.
    a. True
    b. False

5. TCP connections only carry data in one direction.
    a. True
    b. False

6. Capturing network traffic at the physical layer gives investigators access to application layer data such as web pages viewed and images downloaded.
    a. True
    b. False

7. TCP is a Layer 4 protocol.
    a. True
    b. False

8. TCP addresses can be used to track down an offender.
    a. True
    b. False

9. Every mobile telephone has a unique Electronic Serial Number (ESN) and Mobile ID Number (MIN).
    a. True

b. False

10. Mobile telephones can be used to locate the person using them.
    a. True
    b. False

11. TCP/IP enables computers using different network technologies to communicate.
    a. True
    b. False

12. Air is a network (Layer 3) medium for transmitting data.
    a. True
    b. False

13. MAC addresses are uniquely associated with an NIC whereas IP addresses can be changed.
    a. True
    b. False

14. A single, prolonged NetBIOS connection can be made up of multiple TCP/IP connections.
    a. True
    b. False

15. Individuals who can access the physical layer have unlimited access to all of the data on the network unless it is encrypted.
    a. True
    b. False

Discussion Questions

1. Give an example of the type of digital evidence that can be found at each layer of the OSI model and how it can be useful to an investigation.

2. In Figure 21.13, identify each layer and describe its purpose.

Answer guidance: Ethernet = layer 2; IP = layer 3; TCP = layer 4; HTTP = layer 7; MEDIA/JPEG = data (a.k.a. payload).

3. Child pornographers are connecting to the home networks of innocent individuals via insecure wireless access points. How can this help or hinder a digital investigation?

Answer guidance: Although connecting through wireless access points can provide a level of anonymity, criminal activities may come to the attention of law enforcement when home users notice something unusual occurring. However, investigators may mistakenly attribute illegal activities to the innocent owners of the wireless access point.

4. What Internet servers do you access regularly and what activities might those systems record in log files?

Scenario

Shortly before she was killed, the victim of a homicide turned on her computer, connected to the Internet, and used both a web-based e-mail service and an Instant Messenger (IM) program before shutting her computer down.

What traces of Internet activity would you look for on the computer?
What useful digital evidence might exist on the victim's Internet service provider, and on the web-based e-mail server?
Would there be any IM data on the Internet that could be useful?

Chapter 22
Applying Forensic Science to Networks

On completion of this chapter, the student will:

- Be aware of the need to gather intelligence about the target systems prior to the actual search.
- Recognize the similarity between the intelligence gathering in preparation for seizing and conducting vulnerability assessments.
- Be aware of proper methods for preserving evidence on networked devices.
- Be aware of the need and methods for data filtering and reduction.
- Recognize the value in analyzing class and individual characteristics of network evidence.
- Recognize the value of conducting behavioral evidence analysis on network evidence.
- Recognize that the volume and complexity of evidence collected in a network investigation requires different reporting methods.

Chapter Summary

As discussed in earlier chapters, when handling digital evidence it is necessary to establish chain of custody, document the state of items in situ, and take other steps to preserve the evidence so that it can be authenticated at a later date. This chapter presents a methodology for processing digital evidence and describes key concepts and their importance, including copying all data from a disk and calculating the cryptographic hash of a disk. Students will benefit from hands-on exercises dealing with preservation of digital evidence at this stage. The guidelines in Chapter 23 provide a basis for a Standard Operating Procedure (SOP) for preserving and documenting digital evidence on computers.

Note: The practice of obtaining two separate copies of storage media using two different tools may be prohibitively expensive in investigations involving hundreds of computers. In such situations, to save time and resources, it may be necessary to make one copy and then a backup of that copy. However, some attempt should be made to verify that a complete and accurate copy of each drive has been obtained. It is not safe to assume that a forensic acquisition tool will report all errors that might be encountered which is why it is advisable to obtain a second copy of each piece of storage media using another tool.

Additionally, this chapter provides an overview of examination and analysis of digital evidence. Some digital investigators begin a forensic examination by looking for items in places where they are commonly found such as e-mail in their default location, or by searching for certain passwords such as credit card numbers. This ad hoc approach to looking for digital evidence is not effective, resulting in an incomplete examination and overlooked evidence. For instance, when e-mail is stored in a user-selected location or when credit cards are stored in compressed files, an ad hoc approach may miss them. Therefore, to uncover the truth in a way that is reliable

and repeatable, digital investigators need a methodology for the examination step of the Investigative Process presented in Chapter 4. This chapter takes concepts from forensic science and demonstrates how they apply to the examination and analysis of digital evidence. Chapter 24 demonstrates how some of the examination tasks can be implemented using common tools, providing the basics for an SOP for examining digital evidence on computers.

An effort is made to connect the applied material in this chapter with the investigative and reconstruction processes described in earlier chapters. Additionally, this chapter familiarizes students with various file types. Instructors are encouraged to explore other file types to give students the broadest possible exposure to common files and their associated metadata. For instance, the metadata within Microsoft Office documents can be explored using a hexadecimal viewer and compared with utilities such as Metadata Assistant (http://www.payneconsulting.com/). Similarly, it is instructive to teach students to view metadata within digital photographs that could be used to link images to a particular camera, and use the content of photographs to glean information about the context (e.g., who, what, where, when).

The importance of report writing is also emphasized in this chapter.

Multiple Choice Questions

1. Preservation of digital evidence can involve which of the following?
    a. Collecting computer hardware
    b. Making a forensic image of storage media
    c. Copying the files that are needed from storage media
    d. All of the above

2. A forensic image of a drive preserves which of the following?
    a. Memory contents
    b. File slack and unallocated space
    c. System date and time
    d. Screen contents

3. Examination of digital evidence includes (but is not limited to) which of the following activities?
    a. Seizure, preservation, and documentation
    b. Recovery, harvesting, and reduction
    c. Experimentation, fusion, and correlation
    d. Arrest, interviewing, and trial

4. Analysis of digital evidence includes which of the following activities?
    a. Seizure, preservation, and documentation
    b. Recovery, harvesting, and reduction
    c. Experimentation, fusion, and correlation
    d. Arrest, interviewing, and trial

5. On a Windows machine, the MD5 value of the sentence "The suspect's name is Kate" is:
    a. b5152ca3b8445d09384fed12e9089464
    b. db1a7ba15d440722cb741943f9b1538a
    c. 73654cee43a5c9acca03527afb2933f8
    d. 834b78bb23b9f9544a3a3b9267952ddd

Note: Various tools can be used for this question including WinHex.

6. Evidence can be related to its source in which of the following ways?
    a. Top, middle, bottom
    b. IP address, MD5 value, filename, date-time stamps
    c. Production, segment, alteration, location
    d. Parent, uncle, orphan

7. Different types of analysis include which of the following?
    a. Relational (e.g., link analysis) and temporal (e.g., timeline analysis)
    b. Cryptography

c. Metadata hashing
d. Digital photography

8. When a website is under investigation, before obtaining authorization to seize the systems it is necessary to:
   a. Determine where the web servers are located
   b. Inform personnel at the web server location that you'll be coming to seize the systems
   c. Conduct a reconnaissance probe of the target website
   d. None of the above

9. Which of the following is NOT an information gathering process?
   a. Scanning the system remotely
   b. Studying security audit reports
   c. Attempting to bypass logon security
   d. Examining e-mail headers

10. Unlike law enforcement, system administrators are permitted to _____ on their network when it is necessary to protect the network and the data it contains.
    a. Open unread e-mails.
    b. Monitor network traffic.
    c. Modify system logs.
    d. Divulge user personal information.

11. Although it was not designed with evidence collection in mind, _____can still be useful for examining network traffic.
    a. EnCase
    b. FTK
    c. Wireshark
    d. CHKDSK

12. Issues to be aware of when connecting to a computer over a network and collecting information include:
    a. Creating and following a set of standard operating procedures
    b. Keeping a log of actions taken during the collection process
    c. Documenting which server actually contains the data that's being collected
    d. All of the above

13. Occasionally, an intrusion detection system may trigger an alarm caused by an innocent packet that coincidentally contains intrusion class characteristics. This type of alert is called:
    a. False warning
    b. Failsafe
    c. DEF con
    d. False positive

14. Information security professionals submit samples of log files associated with certain intrusion tools to help others detect attacks on the mailing lists at:
    a. Bugtraq
    b. Sam Spade
    c. CNET
    d. Security Focus

15. Which of the following are situations where a bitstream copy may not be viable?
    a. The hard drive is too large to copy.
    b. The system cannot be shut down.
    c. The digital investigator does not have authority to copy the entire drive.
    d. All of the above.

True or False Questions

1. When a computer contains digital evidence, it is always advisable to turn it off immediately.
    a. True
    b. False

2. A forensic image of a hard disk drive preserves the partition table.
    a. True
    b. False

3. All forensic tools acquire digital evidence from storage media in the same way.
    a. True
    b. False

4. It is not necessary to sanitize/wipe a hard drive purchased directly from a manufacturer.
    a. True
    b. False

5. Chain of custody enables anyone to determine where a piece of evidence has been, who handled it when, and what was done to it since it was seized.
    a. True
    b. False

6. No two files can have the same MD5 value.
    a. True
    b. False

7. The chance of two different files having the same MD5 value is roughly one in 340 billion billion billion billion which is approximately equivalent to winning 30,000 billion billion billion first prizes in the Hong Kong Mark Six – the lotto game in Hong Kong which randomly picks 6 numbers from 1 to 47 with a one in 10,737,573 chance of winning first prize.
    a. True
    b. False

8. After the MD5 value of a piece of digital evidence has been calculated, any change in that piece of evidence can be detected.
    a. True
    b. False

9. When drawing up an affidavit for a warrant, it is important to specifically mention all desired digital evidence.
    a. True
    b. False

10. When seeking authorization to search a network and digital evidence that may exist in more than one jurisdiction it is not necessary to obtain a search warrant for each location.
    a. True
    b. False

11. Digital investigators should remember that evidence can reside in unexpected places, such as network routers.
    a. True
    b. False

12. Active monitoring is time consuming, invasive, and costly and should only be used as a last resort.
    a. True
    b. False

13. A digital evidence class characteristic is similar to toolmark analysis in the physical world.
    a. True
    b. False

14. TCP/IP network traffic never contains useful class characteristics.
    a. True
    b. False

15. It is not possible to recover deleted system or network log files.
    a. True
    b. False

Discussion Questions

1. If you are investigating a homicide and, while executing a search warrant, you find a computer in the suspect's home that appears to contain child pornography, what would you do?

Answer guidance: Ideally, your warrant would be worded to permit you to secure/seize all computer hardware at the scene. If in doubt, it is still desirable to secure the evidence to prevent destruction using an exception (e.g., plain view, consent) but this does not give you authorization to examine the contents of the computer for further evidence of child pornography creation/manufacture/distribution. Therefore, a separate warrant is required to investigate this separate offense.

2. Other than verifying the integrity of a file, how can the MD5 value of a file be useful?

Answer guidance: As a class characteristic of the file, the MD5 value can be used to search other sources of digital evidence for identical files (Chapter 9, page 220). For instance, files known to contain child pornography can be found on storage media and in network traffic by looking for files with the same MD5 value. In addition, files known to belong to an operating system or application can be found and filtered based on their MD5 values, thus reducing the number of files that a digital examiner/investigator has to deal with.

3. What are the limitations of the message digest of digital evidence?

Answer guidance: Someone could have modified digital evidence before the MD5 value was calculated. Ultimately, the trustworthiness of digital evidence comes down to the trustworthiness of the individual who collected it (see page 220).

4. What does a digital signature tell you?

Answer guidance: A digital signature tells you that a particular individual or group calculated the MD5 value of given data at a specific time. This is achieved using a signing key and associated passphrase that only the individual or group possess. The important point to note is that a group of people can possess multiple copies of a single key. Therefore, the signature tells you which key was used but not which individual used it. Additional documentation is required to determine which individual was responsible, emphasizing the importance of documenting your actions.

5. What is the difference between a class characteristic and an individualizing characteristic? Give examples of each involving digital evidence.

Answer guidance: A class characteristic is a general feature shared with similar items such as Kodak digital cameras that embed the make and model names in the photographs they take. An individual characteristic is a unique feature specific to a particular thing, place, person, or action. For example, a scratch on a camera lens that appears in photographs it takes, a distinct monument in the background of a photograph, or the defendant's face appearing in a photograph are all individual characteristics that may help investigators associate the photograph with its source, i.e., a particular camera, location, or person.

6. How would you search for all image files on a disk? Explain the rationale of your approach.

Answer guidance: This is the same question asked in Chapter 4 but the knowledge of class characteristics should have altered the way students think about media searching and file recovery.

Scenario

Suppose that your immediate area is a crime scene. What potential sources of digital evidence do you find? For two of these items, describe how you would preserve and document them.

Chapter 23
Digital Evidence on the Internet

On completion of this chapter, the student will:

- Be aware of the role of the Internet in criminal investigations.
- Recognize that Internet Services retain information about people and organizations.
- Be aware of the difficulties in connecting an Internet artifact with a person (i.e., proving that a specific e-mail was sent by a specific individual).
- Recognize the value of analyzing social networking in Internet investigations.
- Be aware of the characteristics of various synchronous chat networks.
- Be aware of the nature of peer-to-peer computer networks and some methods of gathering evidence.
- Recognize the value of analyzing various virtual world platforms.
- Recognize the value of the Internet as an investigative tool.
- Be aware of how search engines can be used in investigating an Internet crime.
- Be aware that the "invisible Web" is a valuable source of investigative information.
- Recognize the value of "whois" databases for gathering contact information on web addresses.
- Recognize that online anonymity is a necessary part of Internet investigations.

Chapter Guide

The Internet is both an attractive venue for criminal activities and a powerful investigative tool. This chapter discusses both aspects to give investigators intelligence about how criminals operate online, and to help investigators use digital evidence on the Internet to apprehend offenders. The main Internet services are covered, including the Web, e-mail, newsgroups, Internet chat, and P2P. New services are emerging that extend the capabilities of the Internet, providing criminals with new opportunities, and making digital investigations more challenging. Therefore, in addition to becoming familiar with existing Internet services, students need to learn how to explore new technologies from an evidentiary and investigative viewpoint, as well as from a criminal viewpoint. For instance, the technology used by KaZaA has been developed to provide P2P phone conversations (www.skype.com) that are encrypted and difficult to trace. Students who are familiar with the underlying functionality of the Internet (Chapters 14-17) are better equipped to deal with new Internet technology.

Many people think of the Internet as separate from the physical world. This is simply not the case and to neglect the very real and direct link between people and the online activities that involve them limits one's ability to investigate and understand crimes with an online component. The Internet effectively provides us with windows into aspects of the world that we otherwise might not know about. As discussed in Chapter 1, a trained eye can use data on computers and the Internet to learn a great deal

about an individual, providing such insight that it is like looking through a stained glass window into the individual's personal life and thoughts.

This "windows into the world" concept is important for several reasons:

- Many cybercrimes can be addressed using existing laws that were developed with physical world crime in mind.

- A crime on the Internet usually reflects a crime in the physical world, with human perpetrators and victims, and should be treated with the same gravity.

- When a crime is committed in the physical world, the Internet often contains related digital evidence and should be considered as an extension of the crime scene. This is true even when the Internet was not directly involved in the crime.

- While criminals feel safe on the Internet, they are observable and thus vulnerable. We can take this opportunity to uncover crimes in the physical world that would not be visible without the Internet.

This last point is worth reiterating and expanding. There is currently an inordinate amount of criminal activity on the Internet, providing us with a unique opportunity to learn more about criminal activities that are usually hidden. By recording offenders' activities in more detail, computers and networks can provide a window into their world, giving us a clearer view of how they operate.

Providing students with sample e-mail and Usenet messages to track, arranging online field trips on IRC and other virtual playgrounds, and having them preserve data they find can help them develop practical experience that will be useful in digital investigations.

Multiple Choice Questions

1. Who is authorized to conduct online undercover investigations when child pornography is involved?
    a. Anyone
    b. Computer security professionals
    c. Journalists
    d. Law enforcement

2. Which of the following Internet services can be used to exchange illegal materials?
    a. IRC
    b. Usenet
    c. KaZaa
    d. All of the above

3. What are two of the most useful headers for determining the origination of Usenet messages?
    a. From and Message-ID
    b. NNTP-Posting-Host and X-Trace
    c. Path and Subject
    d. RFC1036 and RFC2980

4. What information should you document when searching for evidence on the Web?
    a. Date/time of search, search engine and terms used, address of pertinent results
    b. Screenshots of significant search results
    c. Download copies of the webpages and calculate their MD5 value
    d. All of the above

5. Why is it important to hide your identity when conducting an online investigation?
    a. To reduce the risk of alerting the offender
    b. To get yourself in the mindset of covert web investigating
    c. To make it easier for you to determine the offender's location
    d. All of the above

6. When it is not possible to determine the identity of the author of a Usenet message using IP addresses in the header, what else can you do to learn more about the author?
    a. Look for unusual signature and use of language
    b. Search the Web using distinctive aspects of posts
    c. Look for similar Usenet messages posted using an alias
    d. All of the above

7. What characteristics of IRC make it attractive to criminals?
    a. IRC enables them to exchange illegal materials with other criminals.
    b. IRC provides them with some level of anonymity.
    c. IRC gives them direct, "live" access to a large pool of potential victims.
    d. All of the above.

8. Which of the following enables a user to connect to IRC and run IRC fserves without disclosing their IP address?
    a. Freenet
    b. psybnc bot
    c. Fserve
    d. All of the above

9. Which of the following applications leave traces of Internet activities on a personal computer?
    a. Internet Explorer
    b. KaZaA
    c. IRC
    d. All of the above

10. Which of the following tools can reconstruct TCP streams?
    a. Tcpdump
    b. Wireshark
    c. Snoop
    d. EnCase

11. What peer-to-peer clients use the Fast Track network?
    a. KaZaA
    b. Grokster
    c. iMesh
    d. All of the above

12. Web Whacker and Httrack are examples of tools that:
    a. Search the Web
    b. Deface websites
    c. Capture websites
    d. Launch websites

13. Metaverseink is a:
    a. Search tool (people or things) for virtual worlds
    b. Newsgroup aggregator
    c. Social networking meta-tool
    d. A file-sharing peer-to-peer network

14. Second Life is one of the better known:
    a. Research websites
    b. Archive websites
    c. Virtual worlds
    d. Web-based game shows

15. Synchronous chat networks are particularly conducive to criminal activity because of their
    a. Privacy
    b. Immediacy
    c. Impermanence
    d. All of the above

True or False Questions

1. The cybertrail is only useful for gathering information about an offender, not a victim.
    a. True
    b. False

2. The "invisible Web" can only be accessed by government employees.
    a. True
    b. False

3. When you access a web page, the content may be located on a server other than the one you accessed.
    a. True
    b. False

4. All web search engines use the same search syntax.
    a. True
    b. False

5. **Whois** databases contain contact information relating to IP addresses but not domain names.
    a. True
    b. False

6. Criminals let their guard down in chat networks because they feel protected by the perceived anonymity.
    a. True
    b. False

7. The Web archive (web.archive.org) contains a complete and accurate copy of web pages as they existed at a particular time.
    a. True
    b. False

8. E-mail Received headers can be relied on for tracking purposes because they cannot be forged.
    a. True
    b. False

9. When evidence is located on the Internet, investigators should document and preserve it immediately or it may be gone the next time they look for it.
    a. True
    b. False

10. Pseudonymous e-mail enables the sender to receive responses to messages whereas anonymous e-mail does not.
    a. True
    b. False

11. It is not possible to decrypt and view captured network traffic.
    a. True
    b. False

12. Freenet is not being widely used by criminals to exchange illegal materials because it is too difficult to use.
    a. True
    b. False

13. KaZaa has one feature that can be beneficial from an investigative standpoint – whenever possible, it obtains files from peers in the same geographical region.
    a. True
    b. False

14. Posting information online takes control of the information away from the person and such information can remain online indefinitely.
    a. True
    b. False

15. Given the wealth of information that social networks contain, digital investigators will often find useful information at these sites.
    a. True
    b. False

Discussion Questions

1. What website does http://www.paypal.com@1113781300 refer to? Explain how you got your answer.

2. What are the main approaches to searching the Internet and when are they most useful?

3. What are the pros and cons of metasearch engines like www.dogpile.com?

4. What are the advantages and disadvantages from an investigative perspective of Usenet archives like Google Groups?

5. What is the most interesting channel you can find on IRC? Note that you can answer this question by connect to IRC or searching http://searchirc.com/.

6. Describe one way that files can be exchanged on IRC.

7. Describe one way that criminals on IRC can conceal their actual IP address to make tracking them more difficult.

Scenario

1. The purpose of this scenario is to develop e-mail tracking skills. Give students an e-mail message and have them determine where it came from. Have them describe how they determined where the message came from and report what they find using the tools described in this chapter. If certain tools (e.g., Whois or finger) do not provide useful information, this should be noted in the report. It is not necessary to determine the identity of the sender. However, once students have determined where the message was sent from, have them describe the steps they would take to figure out who sent the message. You can make this assignment more challenging by selecting a forged e-mail such as those in many Unsolicited Bulk E-mail (a.k.a. SPAM) messages.

2. It can also be instructive to set up an IRC file server for students to connect to and download files. Panzer (http://arnts.tripod.com/) is a feature rich, user-friendly IRC file-serving package, and is used by criminals to exchange illegal materials. The following log gives a sense of what students will see when connecting to a Panzer server (the IP address of the computer running the server is 141.157.67.68):

```
Session Start: Wed Feb 25 10:59:24 2004
Session Ident: Fserver
[10:59] DCC Chat session
-
[10:59] Client: Fserver (141.157.67.68)
[10:59] Time: Wed Feb 25 10:59:24 2004
-
[10:59] Acknowledging chat request...
[10:59] DCC Chat connection established
-
[10:59] <Fserver> mIRC v6.12 File Server
[10:59] <Fserver> Use: cd dir ls get read help exit
[10:59] <Fserver> [\]
[10:59] <Fserver>
[10:59] <Fserver>        _____________________________
[10:59] <Fserver>            Panzer Fileserver v2.4
[10:59] <Fserver>            http://arnts.tripod.com/
[10:59] <Fserver>
[10:59] <Fserver>   Commands:
[10:59] <Fserver>     CREDIT ......... Your current credit
[10:59] <Fserver>     QUEUE .......... Shows your QUEUED files
[10:59] <Fserver>     STAT ........... Stat's this File Server


[10:59] <Fserver>     AUTO on/off .... Auto-shows credit after DIR list
[10:59] <Fserver>     XP ............. Win XP DCC problem fix
[10:59] <Fserver>     MULTIDCC ....... Shows how you can download multiple files at once
[10:59] <Fserver>
[10:59] <Fserver> Current Credit: FREE Ratio: No Ratio / Leech
[10:59] <Fserver>
[10:59] <Fserver> For usage help, type: HELP <topic>
[10:59] <Fserver> Topics: Upload - Download - Credit - Ratio - Auto
[10:59] <Fserver>
[10:59] <Student> dir
[10:59] <Fserver> [\*.*]
[10:59] <Fserver> image01.jpg       1.23 Mb
```



```
[10:59] <Fserver> End of list
[11:00] <Student> get image01.jpg
[11:00] <Fserver> Sending file IMAGE01.JPG
[11:01] <Student> credit
[11:01] <Fserver> Current Credit: FREE
[11:01] <Student> stat
[11:01] <Fserver>              _____________________________
[11:01] <Fserver>                  STAT'S FILE SERVER
[11:01] <Fserver>
[11:01] <Fserver>   Thursday February 26 2004
[11:01] <Fserver>   Total files available: unknown Size: Dirs:
[11:01] <Fserver>
[11:01] <Fserver>              DOWNLOADS             UPLOADS
[11:01] <Fserver>  Total:          167       [13.22 GB]     2      [459 KB]
[11:01] <Fserver>  This year:    167         [13.22 GB]     2      [459 KB]
[11:01] <Fserver>
[11:01] <Fserver>  This month: 167    [1.22 MB]       2      [459 KB]
[11:01] <Fserver>  Last month: 0             [0 KB]             0      [0 KB]
[11:01] <Fserver>
[11:01] <Fserver>  Today:         57  [5.57 GB]       0      [268 KB]


[11:01] <Fserver>  Yesterday:    36   [4.25 GB]       0      [134 KB]
[11:01] <Fserver>
[11:01] <Fserver>                       VISITS
[11:01] <Fserver>  Total:      102      This month: 102      Today:      46
[11:01] <Fserver>  This year:  102      Last month: 0      Yesterday:  23
[11:01] <Fserver>
[11:01] <Fserver>  Server visited by people from 0 different countries
[11:01] <Fserver>  Top country by visits: N/A
[11:01] <Fserver>
[11:05] <Fserver> Closing Idle connection in 30 seconds
-
[11:05] DCC session closed

Session Start: Wed Feb 25 11:25:41 2004
Session Ident: Fserver
[11:25] Session Ident: Fserver (Fservera@pool-141-157-67-68.balt.east.verizon.net)
[11:25] <Fserver> Upload rejected, file-type unwanted.
Session Close: Wed Feb 25 11:27:45 2004
```


Chapter 24
Digital Evidence at the Physical and Data-Link Layers

On completion of this chapter, the student will:

- Be aware of some of the tools available to exploit the physical and data-link layers of a network.
- Recognize and be able to articulate the differences in various implementations of Ethernet.
- Be aware of the value of collecting MAC addresses in addition to IP addresses.
- Recognize the role of Address Resolution Protocol (ARP) in an Ethernet network in the investigative value of capturing ARP cache.
- Be aware of various methods for documenting, collecting, and preserving evidence at the physical and data-link layers.
- Recognize the value of applying analysis and reconstruction techniques to evidence from the physical and data-link layers.

Chapter Guide

This chapter expands on the overview provided in Chapter 21, describing network technologies in more detail, focusing on Ethernet. Tools and techniques for preserving, examining, and analyzing network traffic are presented.

To begin familiarizing students with the physical and data-link layers, have them inspect a computer that is connected to an Ethernet network. Show them the physical network card and cable, and perhaps even a hub or switch connecting several computers. Also, show them the ARP table on a computer after it has connected to other systems on the local area network. For instance, the following output is from a Windows machine with IP address 192.168.0.6 that connected to two nearby computers.

```
C:\>ping 192.168.0.2
C:\>ping 192.168.0.3
C:\>arp -a

Interface: 192.168.0.6 --- 0x2
  Internet Address      Physical Address      Type
  192.168.0.1           00-30-ab-1d-cd-ef     dynamic
  192.168.0.2           00-08-74-28-8c-7d     dynamic
  192.168.0.3           00-05-02-41-3d-04     dynamic
```


The following ARP table is from a Mac OS X system with IP address 192.168.0.3 that was used to connect to two Windows machines, including the one in the previous example:

```
% arp -a
? (192.168.0.1) at 0:30:ab:1d:cd:ef
? (192.168.0.2) at 0:8:74:28:8c:7d
? (192.168.0.6) at 0:6:1b:ce:df:24
? (192.168.0.255) at ff:ff:ff:ff:ff:ff
```

Having students play around with ARP tables on a network computer provides an opportunity to discuss how ARP functions, demonstrates IP ↔ MAC address mapping, and shows that both 00-30-ab-1d-cd-ef and 0:30:ab:1d:cd:ef are valid representations of Ethernet addresses.

Capturing and examining network traffic is one of the most rewarding and most difficult endeavors a digital investigator can undertake. It is not an exaggeration to say that you can see what offenders see and say in their network traffic. Web pages viewed, e-mail sent and received, online chat, files exchanged, and any other unencrypted data can be extracted from network traffic and reconstructed for examination. From a criminal's perspective, consider how much valuable information could be obtained by monitoring wireless network traffic in a busy location such as an airport terminal where people are accessing the Internet while waiting for a plane.

Because of the significant amount of private information that exists at this layer, it can be difficult to gain authorization to eavesdrop on networks. Also, because of the distributed nature of the Internet, it can be difficult to gain access to the network that carries the relevant traffic. Extracting the few streams of useful traffic from the raging river of high-speed networks is another challenge. Provided these hurdles can be overcome, the resulting digital evidence can be the equivalent of a video recording of the crime, giving a detailed view of what occurred.

There can also be useful data on network devices at the physical and data-link layers, such as switches (some routers perform Layer 2 functions). These data include MAC addresses and records of current or past connections. Given the volatility of the data stored in the memory of these, these sources of digital evidence are rarely preserved after the fact. Nonetheless, it is important for digital investigators to be prepared to process these sources of evidence if the need and opportunity arises. Also, some computer security professionals take steps to preserve such data for tracking down problems on and misuse of their networks.

If you would like to share additional traffic data or other examples relevant to this network layer with other teachers, please submit them to decourses@digital-evidence.net and they will be posted on the book website at http://www.disclosedigital.com/downloads.html.

Multiple Choice Questions

1. What is the maximum cable length for a 10BaseT network?
    a. 10 feet
    b. 100 feet
    c. 10 meters
    d. 100 meters

2. What is the approximate theoretical maximum number of bytes that can be downloaded in one minute on a 10BaseT network?
    a. 10 Mb
    b. 75 Mb
    c. 100 Mb
    d. 175 Mb

3. Which of the following is a valid MAC address?
    a. 192.168.0.5
    b. 00:10:4b:de:fc:e9
    c. 0-0-e2-7a-c3-5b-6f
    d. 08-00-56-s7-fd-d4

4. Which of the following commands can be used to obtain the MAC address of a remote Windows computer?
    a. Netstat
    b. Ping
    c. Nbtstat
    d. Traceroute

5. What is the maximum cable length for a 10 base five segment?
    a. 100 feet
    b. 500 feet
    c. 100 m
    d. 500 m

6. ARP stands for:
    a. Address Resource Protection
    b. Advanced Retrieval Protocol
    c. Address Resolution Protocol
    d. Added Resource Processing

7. The best operating system for capturing network traffic on high-speed networks is:
    a. Microsoft DOS/Windows
    b. OpenBSD/FreeBSD
    c. Linux
    d. Solaris

8. Which of the following applications is used to capture network traffic?
    a. Snort
    b. Wireshark
    c. Tcpdump
    d. All of the above

9. How many bytes per packet does tcpdump capture by default?
    a. 10 bytes
    b. 68 bytes
    c. 128 bytes
    d. 1024 bytes

10. Which of the following tools can reconstruct TCP streams?
    a. Tcpdump
    b. Wireshark
    c. Snoop
    d. EnCase

11. The transition method in which only one computer can transmit while all the others listen is known as:
    a. Baseband
    b. Narrowband
    c. Broadband
    d. Sideband

12. Although ARP is part of TCP/IP, it is generally considered a part of the _____ layer.
    a. Physical
    b. Data-link
    c. Network
    d. Transport

13. If a criminal reconfigures his computer with someone else's IP address to conceal his identity, the local router would have an entry in its _____ showing that criminal's actual Mac address associated with somebody else's IP address.
    a. Host table
    b. BOOTP
    c. CMOS
    d. ARP table

14. The form of ARP that ATM uses to discover MAC addresses is known as:
    a. ARPATM
    b. ATMARP
    c. MACATM
    d. ATMMAC

15. Sniffers put NICs into _____, forcing them to listen in on all of the communications that are occurring on the network.
    a. Covert mode
    b. Wiretap mode
    c. Promiscuous mode
    d. None of the above

True or False Questions

1. Routers use Ethernet addresses to direct data between networks.
    a. True
    b. False

2. MAC addresses can be associated with a particular computer.
    a. True
    b. False

3. The netstat command can be used to obtain the MAC address of a remote computer.
    a. True
    b. False

4. Each network packet stored in the tcpdump file is date-time stamped.
    a. True
    b. False

5. It is necessary to physically tap a network cable to capture the traffic it carries.
    a. True
    b. False

6. A computer connected to the Internet via a dial-up modem can eavesdrop on network traffic from other computers that are dialed into the same Internet service provider.
    a. True
    b. False

7. DHCP can be configured to assign a static IP address to a particular computer every time it is connected to the network.
    a. True
    b. False

8. By default, tcpdump captures the entire contents of a packet.
    a. True
    b. False

9. It is possible to obtain file names from network traffic as well as the file contents.
    a. True
    b. False

10. The tcpdump application can be used to reconstruct TCP streams.
    a. True
    b. False

11. One of the drawbacks of copying network traffic using a SPANned port is that a SPANned port copies only valid Ethernet packets.
    a. True
    b. False

12. A common approach to collecting digital evidence from the physical layer is using a sniffer.
    a. True
    b. False

13. Unlike ARP cache, ATMARP is stored on the individual computers.
    a. True
    b. False

14. It is not possible to use a sniffer when connected to a network via a modem.
    a. True
    b. False

15. One key point about MAC addresses is that they do not go beyond the router.
    a. True
    b. False

Discussion Questions

1. Should law enforcement be given backdoors that enable them to monitor all encrypted Internet communications?

2. Describe how a computer obtains the Ethernet address of another computer that it wants to communicate with.

Answer guidance: ARP request and response.

3. Obtain the MAC address of a computer and describe how you did it.

Answer guidance: This can be performed on a local computer by various means or remotely on some Windows computers using "nbtstat –A IP_address."

4. What data is contained in an Ethernet header?

Answer guidance: See page 727.

5. What information is contained in the padding of an Ethernet frame?

Answer guidance: Generally zeros are inserted for padding but some Ethernet drivers use data from the system to pad Ethernet frames. This is considered a data disclosure vulnerability and could be useful to investigators, providing more information about the originating computer. See "Etherleak: Ethernet frame padding information leakage" by Ofir Arkin and Josh Anderson, January 2003 (http://www.sys-security.com/html/papers.html).

6. What is a "gratuitous ARP request" and why is it dangerous?

Answer guidance: It allows one computer to substitute its MAC address in the ARP cache of other computers on the local network. This can be used for man-in-the-middle attacks.

Scenario

A company learns that someone has obtained an employee's Virtual Private Network (VPN) account and is using it to connect to their network. The company asks you to monitor network traffic for only this account over a period of days to determine what the individual is doing. What hardware and software would you use to capture the network traffic, where would you place the eavesdropping equipment, how would you avoid monitoring other employees' network traffic, and how would you preserve the network traffic as evidence?

Chapter 25
Digital Evidence at the Network and Transport Layers

On completion of this chapter, the student will:

- Be aware of various network and transport layer protocols and how criminals use them.
- Be aware of the components that constitute an IP address.
- Recognize the reason for Domain Name System (DNS) tables and a correlation between a DNS listing and IP addresses.
- Be aware of various tools that facilitate collecting digital evidence at the network and transport layers.
- Be aware of how a routing utilizes the network and transport layers.
- Be aware of how TCP creates virtual circuits.
- Recognize some of the various TCP abuses that are used by criminals.
- Be aware of the process of setting up a network.
- Recognize the sources for various types of TCP/IP-related evidence.
- Be aware of the value of network log files kept by Windows and UNIX systems.

Chapter Guide

This chapter expands on the overview provided in Chapter 21, describing TCP/IP in more detail and demonstrating the usefulness of IP addresses in investigations. Because TCP/IP forms such an integral part of the Internet, information related to these layers are too numerous to describe individually. Extending the analogy on page 441, the glue that holds a network together gets stuck in many places for digital investigators to recover. Case examples are provided to improve students' familiarity with the many types of evidence that contain data relating to the transport and network layers. This chapter also sets the foundation for understanding the Internet and its use as an investigative tool and source of digital evidence. In addition to fundamental aspects of IP addresses, concepts such as routing, domain name lookups, servers and ports, and connection management are covered. TCP flows and streams are revisited and the abuses of TCP/IP that exist are described in an effort to dispel misunderstandings of IP spoofing and session hijacking.

A simplified example of setting up a network and tracking down an offender is provided in Section 21.2. Students can also be encouraged to explore the networks around them provided they do not cause any harm.

To help students become more familiar with the network and transport layers, have them inspect a computer that is connected to the Internet. Show them the nslookup, netstat, and tracert/traceroute commands available on most systems. Also, to familiarize students with TCP/IP, have them view a network capture file using Ethereal (now Wireshark) or a similar tool. Have them look at IP addresses and reconstruct TCP streams to view the interactions between clients and servers.

In addition to this class, it is to the student's advantage to "collect" skill sets in networking, computer security, and computer hardware.

Multiple Choice Questions

1. TCP is an abbreviation for:
    a. Transit Communication Protocol
    b. Transportation Cost Product
    c. Transport Control Protocol
    d. Time Communication Protocol

2. What system is used to convert IP addresses to their associated names?
    a. TCP/IP
    b. DNS
    c. ARP
    d. Routing

3. Which of the following is a Class A network?
    a. 15.0.0.0
    b. 145.19.0.0
    c. 199.54.63.0
    d. All of the above

4. What protocol does the "ping" command use?
    a. TCP
    b. IP
    c. ICMP
    d. All of the above

5. Which of the following logs record the IP addresses of computers accessing an FTP server?
    a. Wtmp
    b. Xferlog
    c. Syslog
    d. Access log

6. In addition to the IP address of the sender, SMTP e-mail server logs contain which of the following?
    a. The Message ID
    b. The time the message was received
    c. The name of the sender
    d. All of the above

7. Which of the following servers maintain logs of when users accessed their e-mail?
    a. SMTP
    b. Imapd
    c. Sendmail

d. All of the above

8. IP Address Class B addresses start with 128.0.0.0 through:
   a. 176.0.0.0
   b. 191.0.0.0
   c. 192.0.0.0
   d. 254.0.0.0

9. IP address [10.40.3.2] is a _____, _____ network address:
   a. Class A, Public
   b. Class B, Public
   c. Class A, Private
   d. Class B, Private

10. _____ is a tool for querying DNS.
   a. nslookup
   b. ping
   c. tracert
   d. nmap

11. The IP software on each _____ contains a routing table that is used to determine where to send information.
   a. Host
   b. Server
   c. Router
   d. Switch

12. It is sometimes possible to obtain a list of all machines in the DNS belonging to a specific organization by performing a _____.
   a. Web crawl
   b. Zone transfer
   c. Reverse IP
   d. IP transfer

13. To make large-scale internetworking more reliable, TCP creates what are called "TCP streams," also known as _____, to establish, maintain, and terminate connections between hosts.
   a. Virtual circuits
   b. Dedicated circuits
   c. Temporary circuits
   d. Parallel circuits

14. VNC software:
   a. Permits full remote control of a computer

b. Has legitimate uses such as remote system administration.
c. Can be used by computer intruders
d. **All of the above**

15. The creator of the first Internet worm and one of the first individuals to be prosecuted under the Computer Fraud and Abuse Act was:
    a. Captain Crunch
    b. Scott Tyree
    c. Richard Morris Jr.
    d. Kevin Mitnick

True or False Questions

1. The UDP protocol will resend packets that were not received by the destination computer.
    a. True
    b. False

2. The Internet is a packet-switched network.
    a. True
    b. False

3. TCP session hijacking can only be performed using a computer on the same network segment as the client and/or server.
    a. True
    b. False

4. The Domain Name System can be used to obtain the names of people who are responsible for a given computer.
    a. True
    b. False

5. Port 80 is generally associated with the Domain Name System.
    a. True
    b. False

6. It is sometimes possible to obtain a list of all machines in the DNS belonging to a specific organization by performing a zone transfer.
    a. True
    b. False

7. IP spoofing establishes a bi-directional TCP connection between the attacker's computer and the target.
    a. True
    b. False

8. The command 'dig' stands for 'Digital Information Groper'.
    a. True
    b. False

9. Network address translation (NAT) enables many computers to connect to the Internet using only one IP address.
    a. True
    b. False

10. An IP address can only be assigned one name in the Domain Name System.
    a. True
    b. False

11. RADIUS and TACACS authentication servers keep logs of the IP addresses that were assigned to user accounts connecting to the Internet.
    a. True
    b. False

12. All servers keep logs of the IP addresses of clients that connected to them.
    a. True
    b. False

13. "dig," which comes installed on UNIX and Windows systems, is a tool used for querying DNS.
    a. True
    b. False

14. Any host, even a personal computer in someone's home, can function as a server on the Internet.
    a. True
    b. False

15. On a packet-switched network, computers are not connected using dedicated circuits.
    a. True
    b. False

Discussion Questions

1. Should Internet service providers be required to keep log files of all their customers' Internet activities? Justify your answer.

2. When illegal activities are traced back to a particular house, how can you be sure that it is the offender's? What should you look for before obtaining a search warrant and breaking down the door of the house?

Answer guidance: Make some effort to perform surveillance on the subject network to determine if malicious activity is originating from the computer or simply being used as a platform by a remote intruder to commit offenses.

Scenario

A threatening message was sent from a web-based e-mail service. Information in the header indicates that the sender connected to the web-based e-mail server through a proxy to conceal his/her actual IP address. Describe how you would determine the sender's actual IP address? As you think about this scenario, consider the possibility that you cannot gain access to information on the proxy server itself.

Instructor Hint: Send an e-mail that contains a web bug that will provide information about the computer used to read the message.

