Digital Evidence and Computer Crime, Third Edition

INSTRUCTOR'S MANUAL

By Samuel Norris

CONTENTS

PART 1 – Digital Forensics

PART 2 – Digital Investigations

PART 3 – Apprehending Offenders

PART 4 – Computers

PART 5 – Network Forensics

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.