1 PART

Digital Forensics

CHAPTER 1

Foundations of Digital Forensics

Eoghan Casey

> Within the past few years, a new class of crime scenes has become more prevalent, that is, crimes committed within electronic or digital domains, particularly within cyberspace. Criminal justice agencies throughout the world are being confronted with an increased need to investigate crimes perpetrated partially or entirely over the Internet or other electronic media. Resources and procedures are needed to effectively search for, locate, and preserve all types of electronic evidence. This evidence ranges from images of child pornography to encrypted data used to further a variety of criminal activities. Even in investigations that are not primarily electronic in nature, at some point in the investigation computer files or data may be discovered and further analysis required.
>
> Lee et al. (2001)

CONTENTS

In this modern age, it is hard to imagine a crime that does not have a *digital dimension*. Criminals, violent and white-collar alike, are using technology to facilitate their offenses and avoid apprehension, creating new challenges for attorneys, judges, law enforcement agents, forensic examiners, and corporate security professionals. As a result of the large amounts of drugs, child pornography, and other illegal materials being trafficked on the Internet, the U.S. Customs Cybersmuggling Center has come to view every computer on the Internet in the United States as a port of entry. Organized criminal groups around the world are using technology to maintain records, communicate, and commit crimes. The largest robberies of our time are now being conducted via computer networks.

Terrorists are using the Internet to communicate, recruit, launder money, commit credit card theft, solicit donations, and post propaganda and training materials. Computers played a role in the planning and subsequent investigations of both World Trade Center bombings. Ramsey Yousef's laptop contained plans for the first bombing and, during the investigation into Zacarias Moussaoui's role in the second attack, over 100 hard drives were examined

Digital Evidence and Computer Crime, Third Edition

CASE EXAMPLE (MASSACHUSETTS, 2005–2010)

TJX, the parent company of T.J. Maxx, Marshalls, and other retail stores in the United States, Canada, and Europe, was the target of cyber criminals who stole over 90 million credit and debit card numbers. After gaining unauthorized access to the inner sanctum of the TJX network in 2005, the thieves spent over 2 years gathering customer information, including credit card numbers, debit card details, and drivers' license information. The resulting investigation and lawsuits cost TJX over $170 million. In 2009, a Ukrainian man named Maksym Yastremskiy was apprehended in Turkey and was convicted to 30 years in prison for trafficking in credit card numbers stolen from TJX. Digital evidence was obtained with some difficulties from computers used by Yastremskiy, ultimately leading investigators to other members of a criminal group that had stolen from TJX and other major retailers by gaining unauthorized access to their networks. In 2010, Albert Gonzalez was convicted to 20 years in prison for his involvement in breaking into and stealing from TJX. During the years that Gonzalez was breaking into the networks of major retailers, he was paid an annual salary of $75,000 by the U.S. Secret Service as an undercover informant. Others involved with Gonzalez in the theft of data, sale of credit cards, and laundering of proceeds have received lesser sentences and fines (Zetter, 2010).

(*United States v. Moussaoui; United States v. Salameh et al.; United States v. Ramsey Yousef*). Islamist extremists are going so far as to develop their own tools to avoid detection and apprehension, including a program named "Mujahideen Secrets 2" designed to encrypt e-mail and Instant Messaging communications. Their use of the Internet creates challenges for digital investigators and requires more international legal cooperation and information sharing.

Network-based attacks targeting critical infrastructure such as government, power, health, communications, financial, and emergency response services are becoming a greater concern as state-sponsored groups have become more technologically proficient. Over the past 5 years, state-sponsored intruders have gained unauthorized access to numerous government and corporate networks in the United States and Europe. To date, the purpose of these attacks has been to gather information, but they have the potential to disrupt critical infrastructure.

Violent serial offenders have used the Internet to find and lure victims. Peter Chapman used Facebook to befriend 17-year-old Ashleigh Hall and arrange a meeting to sexually assault and kill her. John E. Robinson, who referred to himself as "Slavemaster," used the Internet to con some of his victims into meeting him, at which time he sexually assaulted some and killed others. Robinson first used newspaper personal ads to attract victims and then used the Internet proactively to extend his reach (McClintock, 2001). Robinson also used the Internet reactively to conceal his identity online, often hiding behind the alias "Slavemaster." When Robinson's home was searched, five computers were seized.

Although nobody has been killed via a computer network, individuals have committed suicide after being victimized by cyberbullying. After moving from Ireland to Massachusetts, Pheobe Prince became the target of cyberbullying that pushed her to take her own life. In addition, there are violent attacks in virtual worlds such as 2nd Life, including virtual bombings and destruction of avatars, which some consider virtual murder. In one case, a Japanese woman was charged with illegal computer access after she gained unauthorized access to a coworker's online account to destroy his online avatar (Yamaguchi, 2008).

Computers are even being used to target the criminal justice system itself. In one case, offenders obtained computer information about a police officer and his family to intimidate and discourage him from confronting them. Felons have even broken into court systems to change their records and monitor internal communications.

CASE EXAMPLE (CALIFORNIA, 2003)

William Grace and 22-year-old Brandon Wilson were sentenced to 9 years in jail after pleading guilty to breaking into court systems in Riverside, California, to alter records. Wilson altered court records relating to previous charges filed against him (illegal drugs, weapons, and driving under the influence of alcohol) to indicate that the charges had been dismissed. Wilson also altered court documents relating to several friends and family members. The network intrusion began when Grace obtained a system password while working as an outside consultant to a local police department. By the time they were apprehended, they had gained unauthorized access to thousands of computers and had the ability to recall warrants, change court records, dismiss cases, and read e-mail of county employees in most departments, including the Board of Supervisors, Sheriff, and Superior Court judges. Investigators estimate that they seized and examined a total of 400 Gbytes of digital evidence (Sullivan, 2003).

There is a positive aspect to the increasing use of technology by criminals—the involvement of computers in crime has resulted in an abundance of digital evidence that can be used to apprehend and prosecute offenders. For instance, digital traces left on a floppy diskette that was sent by the Bind Torture Kill (BTK) serial killer to a television station led investigators to a computer in the church where the serial killer Dennis Lynn Rader was council president.

Realizing the increasing use of high technology by terrorists compelled the United States to enact the USA Patriot Act and motivated the European Union to recommend related measures. E-mail ransom notes sent by Islamists who kidnapped and murdered journalist Daniel Pearl were instrumental in identifying the responsible individuals in Pakistan. In this case, the "threat to life and limb" provision in the USA Patriot Act enabled Internet Service Providers (ISPs) to provide law enforcement with information quickly, without waiting for search warrants.

While paper documents relating to Enron's misdeeds were shredded, digital records persisted that helped investigators build a case. Subsequent investigations of financial firms and stock analysts have relied heavily on e-mail and other digital evidence. Realizing the value of digital evidence in such investigations, the Securities and Exchange Commission set an example in December 2002 by fining five brokerage houses a total of $8.25 million for failing to retain e-mail and other data as required by the Securities and Exchange Act of 1934 (Securities and Exchange Commission, 2002).

Digital evidence can be useful in a wide range of criminal investigations including homicides, sex offenses, missing persons, child abuse, drug dealing, fraud, and theft of personal information. Also, civil cases can hinge on digital evidence, and electronic discovery is becoming a routine part of civil disputes. Computerized records can help establish when events occurred, where victims and suspects were, and with whom they communicated, and may even show a suspects' intent to commit a crime. Robert Durall's Web browser history showed that he had searched for terms such as "kill + spouse," "accident + deaths," and "smothering" and "murder" prior to killing his wife (Johnson, 2000). These searches were used to demonstrate premeditation and increase the charge to first-degree murder. Sometimes information stored on a computer is the only clue in an investigation. In one case, e-mail messages were the only investigative link between a murderer and his victim.

CASE EXAMPLE (MARYLAND, 1996)

A Maryland woman named Sharon Lopatka told her husband that she was leaving to visit friends. However, she left a chilling note that caused her husband to inform police that she was missing. During their investigation, the police found hundreds of e-mail messages between Lopatka and a man named Robert Glass about their torture and death fantasies. The contents of these e-mails led investigators to Glass's trailer in North Carolina and they found Lopatka's shallow grave nearby. Her hands and feet had been tied and she had been strangled. Glass pleaded guilty, claiming that he killed Lopatka accidentally during sex.

Digital data are all around us and should be collected routinely in any investigation. More likely than not, someone involved in the crime operated a computer, used a mobile device, or accessed the Internet. Therefore, every corporate investigation should consider relevant information stored on computer systems used by their employees both at work and home. Every search warrant should include digital evidence to avoid the need for a second warrant and the associated lost opportunities. Even if digital data do not provide a link between a crime and its victim or a crime and its perpetrator, they can be useful in an investigation. Digital evidence can reveal how a crime was committed, provide investigative leads, disprove or support witness statements, and identify likely suspects.

This book provides the knowledge necessary to handle digital evidence in its many forms, to use this evidence to build a case, and to deal with the challenges associated with this type of evidence. This text presents approaches to handling digital evidence stored and transmitted using networks in a way that is most likely to be accepted in court. An overview of how legal frameworks in the United States and Europe address computer-related crime is provided. However, what is illegal, how evidence is handled, received, and rejected, and how searches are authorized and conducted vary from country to country. Therefore, it is important to seek legal advice from a competent attorney, particularly because the law is changing to adapt to rapid technological developments.

1.1 DIGITAL EVIDENCE

For the purposes of this text, *digital evidence* is defined *as any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi* (adapted from Chisum, 1999).

The data referred to in this definition are essentially a combination of numbers that represent information of various kinds, including text, images, audio, and video.

> Digital evidence has been previously defined as any data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator (Casey, 2000). The definition proposed by the Standard Working Group on Digital Evidence (SWGDE) is any information of probative value that is either stored or transmitted in a digital form. Another definition proposed by the International Organization of Computer Evidence (IOCE) is information stored or transmitted in binary form that may be relied upon in court. However, these definitions focus too heavily on proof and neglect data that simply further an investigation. Additionally, the term *binary* in the later definition is inexact, describing just one of many common representations of computerized data. A broader definition proposed by the Association of Chief Police Officers is information and data of investigative value that are stored on or transmitted by a computer. A more general definition proposed by Brian Carrier is digital data that support or refute a hypothesis about digital events or the state of digital data (Carrier, 2006).

Consider the types of digital data that exist and how they might be useful in an investigation. Computers are ubiquitous and digital data are being transmitted through the air around us and through wires in the ground beneath our feet. When considering the many sources of digital evidence, it is useful to categorize computer systems into three groups (Henseler, 2000):

> ***Open computer systems***: Open computer systems are what most people think of as computers—systems comprised of hard drives, keyboards, and monitors such as laptops, desktops, and servers that obey standards. These systems, with their ever increasing amounts of storage space, can be rich sources of digital evidence. A simple file can contain incriminating information and can have associated properties that are useful in an investigation. For example, details such as when a file was created, who likely created it, or that it was created on another computer can all be important.

Communication systems: Traditional telephone systems, wireless telecommunication systems, the Internet, and networks in general can be a source of digital evidence. For instance, telecommunication systems transfer SMS/MMS messages, and the Internet carries e-mail messages around the world. The time a message was sent, who likely sent it, or what the message contained can all be important in an investigation. To verify when a message was sent, it may be necessary to examine log files from intermediate servers and routers that handled a given message. Some communication systems can be configured to capture the full contents of traffic, giving digital investigators access to all communications (e.g., message text and attachments, and telephone conversations).

Embedded computer systems: Mobile devices, smart cards, and many other systems with embedded computers may contain digital evidence. Mobile devices can contain communications, digital photographs and videos, and other personal data. Navigation systems can be used to determine where a vehicle has been. Sensing and Diagnostic Modules in many vehicles hold data that can be useful for understanding accidents, including the vehicle speed, brake status, and throttle position during the last 5 s before impact. Microwave ovens are now available with embedded computers that can download information from the Internet and some home appliances allow users to program them remotely via a wireless network or the Internet. In an arson investigation, data recovered from a microwave oven can indicate that it was programmed to trigger a fire at a specific time.

To reiterate the opening sentence of this chapter, given the ubiquity of digital evidence, it is the rare crime that does not have some associated data stored and transmitted using computer systems. This evidence provides a digital dimension to any kind of investigation, and a trained eye can use these data to glean a great deal about an individual. An individual's personal computer and his/her use of network services are effectively behavioral archives, potentially retaining more information about an individual's activities and desires than even his/her family and closest friends. E-commerce sites use some of this information for direct marketing and a skilled digital investigator can delve into these behavioral archives and gain deep insight into a victim or an offender (Casey, 2011).

Despite its prevalence, few people are well versed in the evidential, technical, and legal issues related to digital evidence and as a result, digital evidence is often overlooked, collected incorrectly, or analyzed ineffectively. The goal of this text is to equip the reader with the necessary knowledge and skills to use digital evidence effectively in any kind of investigation. This text deals with the technical, investigative, and legal facets of handling and utilizing digital evidence.

1.2 INCREASING AWARENESS OF DIGITAL EVIDENCE

By now it is well known that attorneys and police are encountering progressively more digital evidence in their work. Less obviously, computer security professionals and military decision makers are concerned with digital evidence. An increasing number of organizations are faced with the necessity of collecting evidence on their networks in response to incidents such as computer intrusions, fraud, intellectual property theft, sexual harassment, and even violent crimes.

More organizations are considering legal remedies when criminals target them and are giving more attention to handling digital evidence in a way that will hold up in court. Also, by processing digital evidence properly, organizations are protecting themselves against liabilities such as invasion of privacy and unfair dismissal claims. As a result, there are rising expectations that computer security professionals will have training and knowledge related to digital evidence handling.

In addition to handling evidence properly, corporations and military operations need to respond to and recover from incidents rapidly to minimize the losses caused by an incident. Many computer security professionals deal with hundreds of petty crimes each month and there is not enough time, resources, or desire to open a full investigation for each incident. Therefore, many computer security professionals attempt to limit the damage and close each investigation as quickly as possible. There are three significant drawbacks to this approach. First, each unreported incident robs attorneys and law enforcement personnel of an opportunity to learn about the basics of computer-related crime. Instead, they are only involved when the stakes are high and the cases are complicated. Second, computer security professionals develop loose evidence processing habits that can make it more difficult for law enforcement personnel and attorneys to prosecute an offender. Third, 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.

PRACTITIONER’S TIP

System administrators who find child pornography on computers in their workplace are in a perilous position. Simply deleting the contraband material and not reporting the problem may be viewed as criminally negligent. A system administrator who did not muster his employer’s support before calling the police to report child pornography placed on a server by another employee was disavowed by his employer, had to hire his own lawyer, testify on his own time, and ultimately find a new job. Well-meaning attempts to investigate child pornography complaints have resulted in the system administrator being prosecuted for downloading and possessing illegal materials themselves. Therefore, in addition to being technically prepared for such incidents, it is important for organizations and system administrators to have clear policies and procedures for responding to these problems.

Balancing thoroughness with haste is a demanding challenge. Tools that are designed for detecting malicious activity on computer networks are rarely designed with evidence collection in mind. Some organizations are attempting to address this disparity by retrofitting their existing systems to address authentication issues that arise in court. Other organizations are implementing additional systems specifically designed to secure digital evidence, popularly called Network Forensic Analysis Tools (NFATs). Both approaches have shortcomings that are being addressed gradually as software designers become more familiar with issues relating to digital evidence.

Bearing in mind that criminals are also concerned with digital evidence and will attempt to manipulate computer systems to avoid apprehension, digital investigators cannot simply rely on what is written in this book to process digital evidence and must extend the lessons to new situations. And so, in addition to presenting specific techniques and examples, this text provides general concepts and methodologies that can be applied to new situations with some thought and research on the part of the reader.

1.3 DIGITAL FORENSICS: PAST, PRESENT, AND FUTURE

One of the most important advances in the history of digital forensics occurred on February 20, 2008, when the American Academy of Forensic Sciences (AAFS) created a new section devoted to Digital and Multimedia Sciences (DMS). The AAFS is one of the most widely recognized professional organizations for all established forensic disciplines, and this was the first new section of the AAFS in 28 years. This development advances digital forensics as a scientific discipline, and provides a common ground for the varied members of the forensic science community to share knowledge and address current challenges. Major challenges that members of the DMS section are working to address include standardization of practice and professionalization of digital forensics.

The recent development of digital forensics as a profession and scientific discipline has its roots in the efforts of law enforcement to address the growth in computer-related crime. In the late 1980s and early 1990s, law enforcement agencies in the United States began working together to develop training and build their capacity to deal with the issue. These initiatives led to law enforcement training programs at centers such as SEARCH, Federal Law Enforcement Center (FLETC), and National White Collar Crime Center (NW3C).

Subsequently, the United States and other countries established specialized groups to investigate computer-related crime on a national level. However, the demands on these groups quickly exhausted their resources and regional centers for processing digital evidence were developed. These regional centers also became overloaded, causing many local law enforcement agencies to develop their own units for handling digital evidence. Additionally, some countries have updated the training programs in their academies, realizing that the pervasiveness of computers requires every agent of law enforcement to have basic awareness of digital evidence. This rapid development has resulted in a pyramid structure of first responders with basic collection and examination skills to handle the majority of cases, supported by regional laboratories to handle more advanced cases, and national centers that assist with the most challenging cases, perform research, and develop tools that can be used at the regional and local levels.

The rapid developments in technology and computer-related crime have created a significant demand for individuals who can collect, analyze, and interpret digital evidence. Specifically, there is a growing need for qualified practitioners in the following three general areas of specialization: preservation of digital evidence, extraction of usable information from digital evidence, and interpretation of digital evidence to gain insight into key aspects of an offense. These specializations are not limited to law enforcement and have developed in the corporate world also. Even when a single individual is responsible for collecting, analyzing, and interpreting digital evidence, it is useful to consider these tasks separately. Each area of specialization requires different skills and procedures, and dealing with them separately makes it easier to define training and standards in each area.

The importance of generally accepted standards of practice and training in digital forensics cannot be overstated because they reduce the risk of mishandled evidence and of errors in analysis and interpretation. Innocent individuals may be in jail as a result of improper digital evidence handling and interpretation, allowing the guilty to remain free. Failures to collect digital evidence have undermined investigations, preventing the apprehension or prosecution of offenders and wasting valuable resources on cases abandoned due to faulty evidence. If this situation is not corrected, the field will not develop to its full potential, justice will not be served, and we risk a crisis that could discredit the field.

In addition, the lack of a generally accepted set of core competencies and standards of practice makes it more difficult to assess whether someone is qualified in digital forensics. These weaknesses in digital forensics left the door open for legislation in the United States that requires digital forensic examiners in some states to obtain a private investigator license. The lack of generally accepted core competencies was specifically stated in the National Academy of Sciences (NAS) report released on February 18, 2009:

> Digital evidence has undergone a rapid maturation process. This discipline did not start in forensic laboratories. Instead, computers taken as evidence were studied by police officers and detectives who had some

> interest or expertise in computers. Over the past 10 years, this process has become more routine and subject to the rigors and expectations of other fields of forensic science. Three holdover challenges remain: (1) the digital evidence community does not have an agreed certification program or list of qualifications for digital forensic examiners; (2) some agencies still treat the examination of digital evidence as an investigative rather than a forensic activity; and (3) there is wide variability in and uncertainty about the education, experience, and training of those practicing this discipline (Strengthening Forensic Science in the United States: A Path Forward, Committee on Identifying the Needs of the Forensic Sciences Community: Committee on Applied and Theoretical Statistics, National Research Council, National Academy of Sciences, http://www.nap.edu/catalog.php?record_id1/412589).

Even before the NAS report, the digital forensic community has been working diligently to develop standards in training and best practices. The IOCE[1] was established in the mid-1990s "to ensure the harmonization of methods and practices among nations and guarantee the ability to use digital evidence collected by one state in the courts of another state." In 2002, the Scientific Working Group for Digital Evidence (SWGDE)[2] published guidelines for training and best practices. As a result of these efforts, the American Society of Crime Laboratory Directors (ASCLD) proposed requirements for digital evidence examiners in forensic laboratories (ASCLD, 2003). There are similar efforts to develop digital evidence examination into an accredited discipline under international standards (ISO 17025; ENFSI 2003).

The development of these guidelines and requirements has emphasized the need for standards of practice for individuals in the field. To answer this need, certification and training programs are being developed to ensure that digital evidence examiners have the necessary skills to perform their work competently and to follow approved procedures. Certification provides a standard that individuals need to reach to qualify in a profession and provides an incentive to reach a certain level of knowledge. Without certification, the target and rewards of extra effort are unclear. In addition, certifications make it easier for others to assess whether an individual is qualified to perform digital forensic work. The aim of certifications in digital forensics is to create several tiers of certification, starting with a general knowledge exam that everyone must pass, including digital crime scene technicians, and then more specialized certifications for individuals who handle more complex cases in a laboratory setting.

Although there are various certifications relating to digital forensics, each has its own requirements that applicants must fulfill, including education,

[1] http://www.ioce.org.

[2] http://www.swgde.org.

training, proficiency tests, professional experience, and references. These certifications include the DFCB Digital Forensic Certified Practitioner (http://www.ncfs.org/dfcb/), ISFCE Certified Computer Examiner (http://www.isfce.com/), SANS GIAC Certified Forensic Analysts (http://forensics.sans.org/gcfa/), as well as IACIS certifications (http://www.iacis.com/certification) for law enforcement and the AFMA Certification for video, audio, and image analysts (http://www.theafma.org/). Efforts to bring the various groups together to develop consensus on the essential body of knowledge have only just begun, and these efforts are complicated by the varying needs of different specializations (e.g., Windows systems, networks, and embedded systems), contexts (e.g., corporate, criminal, and military), legal systems, languages, and the rapid rate of technological change.

Several more recent efforts are under way to better define the basic qualifications of practitioners in digital forensics. After closing the Council for the Registration of Forensic Practitioners (CRFP), the UK government shifted responsibility for professionalizing digital forensics onto the Forensic Science Regulator. This year, the Forensic Science Regulator brought together a group of specialists in digital forensics to define requirements for practitioners in the field. This group identified the following three priority areas:

1. The competence of individual experts for both the defense and prosecution.
2. The training of experts. It was suggested that this could be captured under across-the-board practitioner standards, for which there is a separate specialist group.
3. The three levels of competence in terms of electronic evidence—basic retrieval, analysis, and the interpretation of data.

In the United States, a consortium of certification organizations has been convened to form a working group called the Council of Digital Forensic Specialists (CDFS) in an effort to establish an essential body of knowledge in digital forensics. Specifically, the CDFS aims to promote the interests and protect the integrity of the digital forensic industry through standardization and self-regulation by the following:

- Uniting digital forensic specialists and industry leading organizations;
- Developing and compiling an essential body of knowledge from existing resources, to provide guidance and direction to educational and certification programs;
- Identifying minimal qualifications, standards of practice, competencies, and background requirements;
- Creating a model code of professional conduct;
- Representing the profession to federal and state regulators and other bodies.

The NAS report also highlights the need for a stronger scientific foundation in digital forensics, and includes recommendations for further research and more effective approaches to assessing uncertainty and bias of forensic findings in all forensic disciplines. The AAFS is making an effort to address these issues and increase the scientific rigor in all forensic disciplines, including digital forensics. Recommendations of a panel formed by the President of the AAFS to strengthen the scientific integrity of all forensic disciplines include the following:

- Require all public and private forensic science labs to meet the requirements set by ASCLD/LAB or an equivalent accrediting organization.
- Require all lab personnel designated by their units to testify in criminal prosecutions to be board-certified in their respective fields.
- Standardize forensic science methodologies and terminology, and make definitions of the terminology readily accessible to the public.
- Determine what research is needed to validate the forensic science practice, if any forensic discipline is found to lack sufficient scientific foundation.

Although these requirements are designed to raise the bar for forensic disciplines, they could have unintended adverse ramifications for practitioners and laboratories. Requiring practitioners in digital forensics to be board-certified may be overly restrictive, and may need to be broadened to accommodate several certifications in digital forensics. Unfairly burdening small local law enforcement and private sector laboratories with accreditation requirements designed for large government laboratories could be counterproductive, exhausting their limited resources and driving them out of business.

1.4 PRINCIPLES OF DIGITAL FORENSICS

Forensic Science provides a large body of proven investigative techniques and methods for achieving the ends that are referenced extensively in this text. By *forensic* we mean a characteristic of evidence that satisfies its suitability for admission as fact and its ability to persuade based upon proof (or high statistical confidence).

PRACTITIONER'S TIP

In Forensic Science, *certainty* is a word that is used with great care. We cannot be certain of what occurred at a crime scene when we only have a limited amount of information. Therefore, we can generally only present possibilities based on the limited amount of information.

Strictly speaking, Forensic Science is the application of science to law and is ultimately tested by use in court. For instance, the scientific study of insects has many investigative applications including the study of insects on a decaying corpse—*forensic entomology.* Entomological evidence has been accepted in courts to help determine how long a body has been exposed to fauna in a specific area. Another example of forensic science involves the preservation of shoe prints left at a crime scene to locate the source of the impressions. Forensic examiners use physical characteristics of these shoe prints to determine the type of shoe and ultimately to associate the impressions with the shoes that made them. Similarly, the systematic study of digital data becomes a forensic discipline when it relates to the investigation and prosecution of a crime.

Even when prosecution is not the goal of a digital investigation, such as a corporate investigation into a policy violation or security breach, the incident may result in legal action. For instance, terminating an employee for cause may lead to an unfair dismissal suit, and the organization must be prepared to present evidence supporting their decision to fire the individual. When data thieves gain access to an organization's computer systems and steal personally identifiable information (PII), the organization must be prepared to present evidence to fulfill their regulatory notification obligations and to apprehend and prosecute the offenders. Therefore, it is important to handle digital evidence in such cases as if it were going to be used in court. Even when a dispute or incident is handled completely within an organization, it is preferable to base major decisions on solid evidence.

Ultimately, any investigation can benefit from the influence of Forensic Science. In addition to providing scientific techniques and theories for processing individual pieces of digital evidence, Forensic Science can help reconstruct crimes and generate leads. Using the scientific method to analyze available evidence, reconstruct the crime, and test their hypotheses, digital investigators can generate strong possibilities about what occurred.

PRACTITIONER'S TIP

For the sake of the evidence and the forensic practitioner, it is important to develop and follow written policies and standard operating protocols. Following established policies and procedures increases the chances that digital evidence will be handled properly and can be relied upon by decision makers. Furthermore, following a formal process reduces the risk that the person conducting the investigation will be criticized for taking inappropriate or unauthorized actions. We have been called in to investigate IT personnel who took the law into their own hands and exceeded their authorization to pry into the activities of fellow employees and company executives. Such abuse of power is generally grounds for demotion or termination and can lead to legal action when the infraction is considered criminal.

In short, proper evidence processing is important for resolving incidents and disputes in corporate settings, as well as in criminal and civil matters. To encourage corporate digital investigators to apply the principles of Forensic Science presented in this text, a broader definition of Forensic Science will be adopted. For the purpose of this text, Forensic Science is the application of science to investigation and prosecution of crime or to the just resolution of conflict.

1.4.1 Evidence Exchange

The main goals in any investigation are to follow the trails that offenders leave during the commission of a crime and to tie perpetrators to the victims and crime scenes. Although witnesses may identify a suspect, tangible evidence of an individual's involvement is usually more compelling and reliable. Forensic analysts are employed to uncover compelling links between the offender, victim, and crime scene.

According to Locard's Exchange Principle, contact between two items will result in an exchange. This principle applies to any contact at a crime scene, including between an offender and victim, between a person with a weapon, and between people and the crime scene itself. In short, there will always be evidence of the interaction, although in some cases it may not be detected easily (note that absence of evidence is not evidence of absence). This transfer occurs in both the physical and digital realms and can provide links between them as depicted in Figure 1.1. In the physical world, an offender might inadvertently leave fingerprints or hair at the scene and take a fiber from the scene. For instance, in a homicide case the offender may attempt to misdirect investigators by creating a suicide note on the victim's computer, and in the process leave fingerprints on the keyboard. With one such piece of evidence, investigators can demonstrate the strong possibility that the offender was at the crime scene. With two pieces of evidence the link between the offender and crime scene becomes stronger and easier to demonstrate. Digital evidence can reveal communications between suspects and the victim, online activities at key times, and other information that provides a *digital dimension* to the investigation.

In computer intrusions, the attackers will leave multiple traces of their presence throughout the environment, including in the file systems, registry, system logs, and network-level logs. Furthermore, the attackers could transfer elements of the crime scene back with them, such as stolen user passwords or PII in a file or database. Such evidence can be useful to link an individual to an intrusion.

In an e-mail harassment case, the act of sending threatening messages via a Web-based e-mail service such as Hotmail can leave a number of traces. The Web browser used to send messages will store files, links, and other

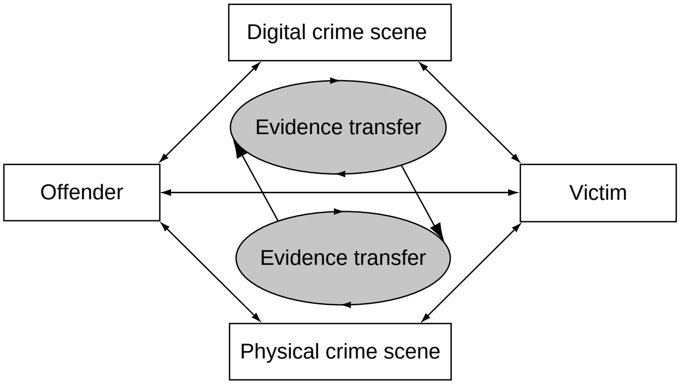


FIGURE 1.1
Evidence transfer in the physical and digital dimensions helps investigators establish connections between victims, offenders, and crime scenes.

information on the sender's hard drive along with date-time–related information. Therefore, forensic analysts may find an abundance of information relating to the sent message on the offender's hard drive, including the original message contents. Additionally, investigators may be able to obtain related information from Hotmail, including Web server access logs, IP addresses, and possibly the entire message in the sent mail folder of the offender's e-mail account.

1.4.2 Evidence Characteristics

The exchanges that occur between individual and crime scene produce trace evidence belonging to one of two general categories: (i) evidence with attributes that fit in the group called *class characteristics* and (ii) evidence with attributes that fall in the category called *individual characteristics*. As detailed in Chapter 17, class characteristics are common traits in similar items whereas individual characteristics are more unique and can be linked to a specific person or activity with greater certainty. Consider the physical world example of a shoe print left under a window at a crime scene. Forensic analysis of those impressions might only reveal the make and model of the shoe, placing it in the class of all shoes of the same make and model. Therefore, if a suspect was found to be in possession of a pair of the same make and model, a tenuous circumstantial link can be made between the suspect and the wrongdoing. If forensic analysis uncovers detailed wear patterns in the shoe prints and finds identical wear of the suspect's soles, a much stronger link is possible. The margin of error is significantly reduced by the discovery of an individual characteristic, making the link much less circumstantial and harder to refute.

In the digital realm, we move into a more virtual and less tangible space. Exchange of digital evidence often involves a copy of the data being transferred, leaving the original essentially unchanged. Furthermore, the very notion of individual identity is almost at odds with the philosophy of anonymity that exists in some communities using the Internet. Despite these issues, exchanges of evidence in the digital realm leave trace evidence with class and individual characteristics that can be used to help answer crucial questions or even solve a case.

For instance, class characteristics in a questioned Microsoft Word document may enable forensic analysts to determine that the document is fake, because it could have been created using a version of Microsoft Word that was released several years after the purported creation date of the document. When there is concern that digital evidence has been concealed or destroyed, class characteristics may reveal that a particular encryption mechanism or data destruction tool was used on the evidential computer.

The more conclusive individual characteristics are rarer but not impossible to identify through detailed forensic analysis. Certain printers mark every page with a pattern that can be uniquely associated with the device. Unique marks on a digitized photograph might be used to demonstrate that the suspect's scanner or digital camera was involved. Similarly, a specific floppy drive may make unique magnetic impressions on a floppy disk, helping to establish a link between a given floppy disk and the suspect's computer. These are examples of the more desirable category of evidence because of their strong association with an individual source. Generally, however, the amount of work required to ascertain this level of information is significant and may be for naught, especially if a proven method for its recovery has not been researched and accepted in the digital forensic community and used to establish precedent in the courts. This risk, coupled with the fact that the objects of analysis change in design and complexity at such a rapid pace, makes it difficult for applied research in digital forensics to keep pace with changes in technology.

Categorization of characteristics from various types of digital components has yet to be approached in any formal way but the value of this type of information cannot be underestimated. Class characteristics can be used collectively to determine a probability of involvement and the preponderance of this type of evidence can be a factor in reaching conclusions about guilt or innocence.

> The value of class physical evidence lies in its ability to provide corroboration of events with data that are, as nearly as possible, free of human

> error and bias. It is the thread that binds together other investigative findings that are more dependent on human judgements and, therefore, more prone to human failings.
>
> **(Saferstein, 1998)**

The more corroborating evidence that investigators can obtain, the greater weight the evidence will be given in court and the more certainty they can have in their conclusions. In this way, investigators can develop a reconstruction of the crime and determine who was involved. The classification of digital evidence as described can benefit investigators by allowing them to present the relative merits of the evidence and help them maintain the objectivity called for by the investigative process.

1.4.3 Forensic Soundness

In order to be useful in an investigation, digital evidence must be preserved and examined in a forensically sound manner. Some practitioners of digital forensics think that a method of preserving or examining digital evidence is only forensically sound if it does not alter the original evidence source in any way. This is simply not true. Traditional forensic disciplines such as DNA analysis show that the measure of forensic soundness does not require the original to be left unaltered. When samples of biological material are collected, the process generally scrapes or smears the original evidence. Forensic analysis of the evidential sample further alters the sample because DNA tests are destructive. Despite the changes that occur during preservation and processing, these methods are considered forensically sound and DNA evidence is regularly admitted as evidence.

In digital forensics, the routine task of acquiring data from a hard drive, even when using a hardware write-blocker, alters the original state of the hard drive. Such alterations can include making a hidden area of the hard drive accessible, or updating information maintained by Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T.) on modern hard drives. Furthermore, most methods of acquiring the contents of memory on live computer systems and mobile devices alter or overwrite portions of memory, but this is a generally accepted practice in digital forensics. In fact, courts are starting to compel preservation of volatile computer data in some cases, which requires digital investigators to preserve data on live systems. In Columbia Pictures Indus. v. Bunnell, for example, the court held that random access memory (RAM) on a Web server could contain relevant log data and was therefore within the scope of discoverable information in this case.

Setting an absolute standard that dictates “preserve everything but change nothing” is not only inconsistent with other forensic disciplines but is also dangerous in a legal context. Conforming to such a standard may be impossible in some circumstances and, therefore, postulating this standard as the "best practice" only opens digital evidence to criticisms that have no bearing on the issues under investigation.

PRACTITIONER'S TIP

Inadvertent errors and omissions in processing digital evidence may not invalidate the evidence. Concerns about how an item of evidence was handled may be addressed through documentation, forensic analysis, or testimony. Therefore, the best way to deal with any problems that occur is to document them thoroughly, and seek ways to mitigate the impact on the evidence. The worst thing you can do is attempt to conceal a mistake, because this could cause confusion down the road and impugn your credibility.

One of the keys to forensic soundness is documentation. A solid case is built on supporting documentation that reports on where the evidence originated and how it was handled. From a forensic standpoint, the acquisition process should change the original evidence as little as possible and any changes should be documented and assessed in the context of the final analytical results. Provided the acquisition process preserves a complete and accurate representation of the original data, and its authenticity and integrity can be validated, it is generally considered forensically sound. When preserving volatile data, digital investigators must document the date and time that data were preserved and the tools that were used, and the MD5 hash value of all outputs as discussed later in this chapter. When dealing with computers, it is critical to note the date and time of the computer and compare it to a reliable time source.

1.4.4 Authentication

Authentication of digital evidence will be covered in more detail in Chapter 3, but it is important to have a basic understanding of this concept from the outset.

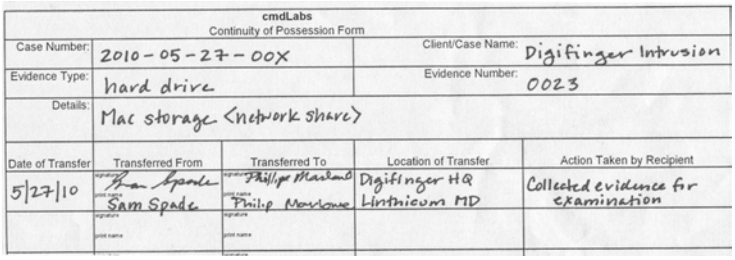
Some texts relating to digital forensics assert that authentication is the process of ensuring that the recovered evidence is the same as the originally seized data, but the concept is subtler. From a technical standpoint, it is not always possible to compare the acquired data with the original. The contents of RAM on a running computer are constantly changing. Captured memory contents are simply a snapshot in time of the running state of the computer at that moment, and there is no original to compare the copy with. Similarly, network traffic is transient and must be captured while it is in transit. Once network traffic is captured, only copies remain and the original data are not available for comparison. From a legal standpoint, authentication is the process of determining whether the evidence is worthy.

> Authentication means satisfying the court that (a) the contents of the record have remained unchanged, (b) that the information in the record does in fact originate from its purported source, whether human or machine, and (c) that extraneous information such as the apparent date of the record is accurate. As with paper records, the necessary degree of authentication may be proved through oral and circumstantial evidence, if available, or via technological features in the system or the record.
>
> **(Reed, 1990–1991)**

Authentication is actually a two-step process, with an initial examination of the evidence to determine that it is what its proponent claims and, later, a closer analysis to determine its probative value. In the initial stage, it may be sufficient for an individual who is familiar with the digital evidence to testify to its authenticity. For instance, the individual who collected the evidence can confirm that the evidence presented in court is the same as when it was collected. Similarly, a system administrator can testify that log files presented in court originated from her/his system.

1.4.5 Chain of Custody

One of the most important aspects of authentication is maintaining and documenting the chain of custody (a.k.a. continuity of possession) of evidence. Each person who handled evidence may be required to testify that the evidence presented in court is the same as when it was processed during the investigation. Although it may not be necessary to produce at trial every individual who handled the evidence, it is best to keep the number to a minimum and maintain documentation to demonstrate that digital evidence has not been altered since it was collected. A sample chain of custody form is shown in Figure 1.2, recording the transfer of evidence, when, where, and why.



cmdLabs
Continuity of Possession Form

Case Number: 2010-05-27-00X
Client/Case Name: Digifinger Intrusion
Evidence Type: hard drive
Evidence Number: 0023
Details: Mac storage <network share>

Date of Transfer	Transferred From	Transferred To	Location of Transfer	Action Taken by Recipient
5/27/10	signature Sam Spade print name Sam Spade	signature Phillip Marlowe print name Philip Marlowe	Digifinger HQ Linthicum MD	Collected evidence for examination
	signature print name	signature print name		

FIGURE 1.2
Sample chain of custody form.

Without a solid chain of custody, it could be argued that the evidence was handled improperly and may have been altered, replaced with incriminating evidence, or contaminated in some other fashion. Potential consequences of breaking the chain of custody include misidentification of evidence, contamination of evidence, and loss of evidence or pertinent elements.

1.4.6 Evidence Integrity

The purpose of integrity checks is to show that evidence has not been altered from the time it was collected, thus supporting the authentication process. In digital forensics, the process of verifying the integrity of evidence generally involves a comparison of the digital fingerprint for that evidence taken at the time of collection with the digital fingerprint of the evidence in its current state.

To understand how this verification process works, it is necessary to have a basic familiarity with message digests and cryptographic hash values. For the purposes of this text, a message digest algorithm can be thought of as a black box that accepts a digital object (e.g., a file, program, or disk) and produces a number (Figure 1.3). A message digest algorithm always produces the same number for a given input. Also, a good message digest algorithm will produce a different number for different inputs. Therefore, an exact copy will have the same message digest as the original but if a file is changed even slightly it will have a different message digest from the original.

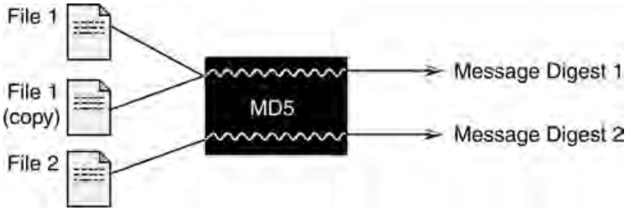


FIGURE 1.3
Black box concept of the message digest.

Currently, the most commonly used algorithms for calculating message digests in digital forensics are MD5 and SHA-1. SHA is very similar to MD5 and is currently the U.S. government's message digest algorithm of choice.

The MD5 algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally unfeasible to produce two messages having the

PRACTITIONER'S TIP

Researchers have found that two files that have the same MD5 hash value can be generated under controlled conditions. Similar weaknesses have been found in other hashing algorithms, including SHA-1. Fortunately, this type of hash collision does not invalidate the use of MD5 or SHA-1 to document the integrity of digital evidence. When the content of an item of digital evidence is altered, this will result in a different MD5 or SHA-1 hash value of the data. There have been no attempts to meet a challenge released by the Digital Forensics Research Workshop in 2006 to modify a given disk image such that it has the same MD5 and/or SHA-1 value and still has a valid file system structure (http://www.dfrws.org/hashchallenge). One approach to addressing concerns about weaknesses in any given hash algorithm is to use two independent hash algorithms. For this reason, some digital forensic tools automatically calculate both the MD5 and SHA-1 hash value of acquired digital evidence, and other tools provide multiple hashing options for the user to select.

same message digest or to produce any message having a given prespecified target message digest (RFC1321 1992).

Note the use of the word *fingerprint*. The purpose of this analogy is to emphasize the near uniqueness of a message digest calculated using the MD5 algorithm. Basically, the MD5 algorithm uses the data in a digital object to calculate a combination of 32 numbers and letters. This is actually a 16-character hexadecimal value, with each byte represented by a pair of letters and numbers. Like human fingerprints and DNA, it is highly unlikely that two items will have the same message digest unless they are duplicates.

It is conjectured that the probability of coming up with two messages having the same message digest is on the order of 264 operations and that the probability of coming up with any message having a given message digest is on the order of 2128 operations (RFC1321 1992).

This near uniqueness makes message digest algorithms like MD5 an important tool for documenting digital evidence. For instance, by computing the MD5 value of a disk prior to collection and then again after collection, it can be demonstrated that the collection process did not change the data. Similarly, the MD5 value of a file can be used to show that it has not changed since it was collected. Table 1.1 shows that changing one letter in a sentence changes the message digest of that sentence.

Table 1.1 Two Files on a Windows Machine That Differ by Only One Letter Have Significantly Different MD5 Values

Digital Input	MD5 Output
The suspect's name is John	c52f34e4a6ef3dce4a7a4c573122a039
The suspect's name is Joan	c1d99b2b4f67d5836120ba8a16bbd3c9

Keep in mind that MD5 and SHA-1 values alone do not indicate that the associated evidence is reliable, as someone could have modified the evidence before the hash value was calculated. For instance, if the person who collected the evidence altered it prior to calculating a digital fingerprint, then the alteration will not be detected by a later evaluation of the digital fingerprint. Ultimately, the trustworthiness of digital evidence comes down to the trustworthiness of individuals handling it and the strength of supporting documentation.

Message digests are also useful in digital forensics for conducting forensic analysis because the hash value of a file can be useful as a class or individual characteristic, depending on its application. For instance, the MD5 value of a common component of the Windows 2000 operating system (e.g., kernel32.dll) places a file in a group of all other similar components on all Windows 2000 installations but does not indicate that the file came from a specific machine. On the other hand, when the MD5 computation is computed for data that are or seem to be unique, such as an image containing child pornography or suspect steganographic data, the hash value becomes an individual characteristic due to the very low probability that any other data (other than an exact copy) will compute to the same hash value. Therefore, MD5 values are more trustworthy than filenames or file sizes in the comparison of data. In digital forensics, it is a common practice to use hash values when excluding known operating system files from a keyword search, and when searching storage media for a specific file such as stolen data or contraband materials—a matching MD5 value indicates that the files are identical even if the names are different.

1.4.7 Objectivity

A cornerstone of a forensic analysis is objectivity. The interpretation and presentation of evidence should be free from bias to provide decision makers with the clearest possible view of the facts. As will be discussed in Chapter 3, this can be difficult given preconceived notions and the external pressures to reach specific conclusions.

PRACTITIONER'S TIP

In some cases, particularly when dealing with child exploitation and violent crime, it may take some effort to remain objective. Just remember that any judgmental language or other expression of bias in your work could be used to raise questions about your findings. This could be harmful to the case and your reputation.

The most effective approach to remaining objective is to let the evidence speak for itself as much as possible. Every conclusion should be presented along with all of the supporting factual evidence. Another effective approach to ensuring objectivity is to have a peer review process that assesses a forensic analyst's findings for bias or any other weakness.

1.4.8 Repeatability

An important aspect of the scientific method is that any experiments or observations must be repeatable in order to be independently verifiable. This is particularly important to be able to independently verify findings in a forensic context, when a person's liberty and livelihood may be at stake. Therefore, it may become necessary for one forensic analyst to repeat some or all of the analysis performed by another forensic analyst. To enable such a verification of forensic findings, it is important to document the steps taken to find and analyze digital evidence in sufficient detail to enable others to verify the results independently. This documentation may include the location and other characteristics of the digital evidence, as well as the tools used to analyze the data.

1.5 CHALLENGING ASPECTS OF DIGITAL EVIDENCE

Digital evidence as a form of physical evidence creates several challenges for digital forensic analysts. First, it is a messy, slippery form of evidence that can be very difficult to handle. For instance, a hard drive platter contains a messy amalgam of data—pieces of information mixed together and layered on top of each other over time. Only a small portion of this amalgam might be relevant to a case, making it necessary to extract useful pieces, fit them together, and translate them into a form that can be interpreted.

Second, digital evidence is generally an abstraction of some digital object or event. When a person instructs a computer to perform a task such as sending an e-mail, the resulting activities generate data remnants that give only a partial view of what occurred (Venema & Farmer, 2000). Only certain results of the activity such as the e-mail message and server logs remain to give us a partial view of what occurred. Furthermore, using a forensic tool to recover a deleted file from storage media involves several layers of abstraction from magnetic fields on the disk to the letters and numbers that we see on the screen. So, we never see the actual data but only a representation, and each layer of abstraction can introduce errors (Carrier, 2003).

PRACTITIONER'S TIP

Forensic tools introduce an additional abstraction layer between the examiner and underlying digital evidence. As such, forensic tools can introduce errors such as incorrect or incomplete reconstruction of file systems and other data structures. Therefore, whenever feasible, it is important for digital forensic examiners to verify important results using other tools or at a low level.

This situation is similar to that of the traditional crime scene investigation. In a homicide case, there may be clues that can be used to reconstruct events, like putting a puzzle together. However, all of the puzzle pieces are not available, making it impossible to create a complete reconstruction of the crime. This book describes various sources of digital evidence and indicates how these multiple, independent sources of corroborating information can be used to develop a more complete picture of the associated crime.

Third, digital evidence is usually circumstantial, making it difficult to attribute computer activity to an individual. Therefore, digital evidence can only be one component of a solid investigation. If a case hinges upon a single form or source of digital evidence such as date-time stamps on computer files, then the case is unacceptably weak. Without additional information, it could be reasonably argued that someone else used the computer at the time. For instance, password protection mechanisms on some computers can be bypassed, and many computers do not require a password, allowing anyone to use them. Similarly, if a defendant argues that some exonerating digital evidence was not collected from one system, this would only impact a weak case that does not have supporting evidence of guilt from other sources.

CASE EXAMPLE (UNITED STATES V. GRANT, 2000)

In an investigation into the notorious online Wonderland Club, Grant argued that all evidence found in his home should be suppressed because investigators had failed to prove that he was the person associated with the illegal online activities in question. However, the prosecution presented enough corroborating evidence to prove their case.

Fourth, the fact that digital evidence can be manipulated or destroyed so easily raises new challenges for digital investigators. Digital evidence can be altered or obliterated either maliciously by offenders or accidentally during collection without leaving any obvious signs of distortion. Fortunately, digital evidence has several features that mitigate this problem.

- Digital evidence can be duplicated exactly and a copy can be examined as if it were the original. It is common practice when dealing with digital evidence to examine a copy, thus avoiding the risk of altering or damaging the original evidence.
- With the right tools, it is very easy to determine if digital evidence has been modified or tampered with by comparing it with an original copy.
- Digital evidence is difficult to destroy. Even when a file is “deleted” or a hard drive is formatted, digital evidence can be recovered.
- When criminals attempt to destroy digital evidence, copies and associated remnants can remain in places that they were not aware of.

CASE EXAMPLE (BLANTON, 1995)

When Colonel Oliver North was under investigation during the Iran Contra affair in 1986, he was careful to shred documents and delete incriminating e-mails from his computer. However, unbeknown to him, electronic messages sent using the IBM Professional Office System (PROFS) were being regularly backed up and were later retrieved from backup tapes.

The ease with which digital evidence can be altered or destroyed creates challenges in many investigations in the form of evidence dynamics.

1.5.1 Evidence Dynamics and the Introduction of Error

Investigators and digital evidence examiners will rarely have an opportunity to examine a digital crime scene in its original state and should therefore expect some evidence dynamics: any influence that changes, relocates, obscures, or obliterates evidence, regardless of intent between the time evidence is transferred and the time the case is resolved. Offenders, victims, first responders, digital evidence examiners, and anyone else who had access to digital evidence prior to its preservation can cause evidence dynamics.

Some examples of evidence dynamics encountered in past cases:

- A system administrator attempted to recover deleted files from a hard drive by installing software on an evidential computer, saving recovered files onto the same drive. This process overwrote unallocated space, rendering potentially useful deleted data unrecoverable.
- Consultants installed a pirated version of a forensic tool on the compromised server. In addition to breaking the law by using an unlicensed version of digital forensic software, the installation altered and overwrote data on the evidential computer.
- Responding to a computer intrusion, a system administrator intentionally deleted an account that the intruder had created and attempted to preserve digital evidence using the standard backup facility on the system. This backup facility was outdated and had a flaw that caused it to change the times of the files on the disk before copying them. Thus, the date-time stamps of all files on the disk were changed to the current time, making it nearly impossible to reconstruct the crime.
- During an investigation involving several machines, a first responder did not follow standard operating procedures and failed to collect important evidence. Additionally, evidence collected from several identical computer systems was not thoroughly documented, making it very difficult to determine which evidence came from which system.

Media containing digital evidence can deteriorate over time or when exposed to fire, water, jet fuel, and toxic chemicals. Errors can also be introduced during the examination and interpretation of digital evidence. Digital evidence examination tools can contain bugs that cause them to represent data incorrectly, and digital evidence examiners can misinterpret data. For instance, while a digital evidence examiner was examining several log files, transcribing relevant entries for later reference, he transcribed several dates and IP addresses incorrectly; for example, he misread 03:13 A.M. as 3:13 P.M., resulting in the wrong dial-up records being retrieved, implicating the wrong individual. Similarly, he transcribed 192.168.1.54 as 192.168.1.45 in a search warrant and implicated the wrong individual.

There are many other ways that evidence dynamics can occur.

CASE EXAMPLE (UNITED STATES V. BENEDICT)

Lawrence Benedict was accused of possessing child pornography found on a tape that he exchanged with another individual named Mikel Bolander who had been previously convicted of sexual assault of a minor and possession of child pornography. Benedict claims that he was exchanging games with many individuals and did not realize that the tape contained child pornography. Although Benedict initially pleaded guilty purportedly based on advice from his attorney, he changed his plea when problems were found in digital evidence relating to his case. A computer and disks that the defense claimed could prove Benedict's innocence were stored in a post office basement that experienced several floods. The water damage caused the computers to rust and left a filmy white substance encrusted on the disks (McCullagh, 2001). Furthermore, after Bolander's computer was seized for examination, police apparently copied child pornography from the tape allegedly exchanged by Bolander and Benedict onto Bolander's computer. Police also apparently installed software on Bolander's computer to examine its contents and files on the computer appeared to have been added, altered, and deleted while it was in police custody.

Although Bolander was found guilty, his computer was destroyed before sentencing. Additionally, a floppy disk containing evidence was mostly overwritten, presumably by accident. The evidence dynamics in this case created a significant amount of controversy.

Evidence dynamics create investigative and legal challenges, generally making it more difficult to determine what occurred and making it more difficult to prove that the evidence is authentic and reliable. Additionally, any conclusions that a forensic examiner reaches without the knowledge of how evidence was changed will be open to criticism in court, may misdirect an investigation, and may even be completely incorrect.

1.6 FOLLOWING THE CYBERTRAIL

Many people think of the Internet as separate from the physical world. This is simply not the case—crime on the Internet is closely tied to crime in the physical world. There are a couple of reasons for this cautionary note.

First, 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. 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. Auction fraud provides a simple demonstration of how a combination of evidence from the virtual and physical worlds is used to apprehend a criminal.

CASE EXAMPLE (AUCTION FRAUD, 2000)

A buyer on eBay complained to police that he sent a cashier's check to that seller but received no merchandise. Over a period of weeks, several dozen similar reports were made to the Internet Fraud Complaint Center against the same seller. To hide his identity, the seller used a Hotmail account for online communications and several mail drops to receive checks. Logs obtained from Hotmail revealed that the seller was accessing the Internet through a subsidiary of Uunet. When served with a subpoena, Uunet disclosed the suspect's MSN account and associated address, credit card, and telephone numbers. Investigators also obtained information from the suspect's bank with a subpoena to determine that the cashier's checks from the buyers had been deposited into the suspect's bank account. A subpoena to eBay for auction history and complaints and supporting evidence from each of the buyers helped corroborate the connections between the suspect and the fraudulent activities. Employees at each mail drop recognized a photograph of the suspect obtained from the Department of Motor Vehicles. A subpoena to the credit card company revealed the suspect's Social Security number and a search of real estate property in the suspect's name turned up an alternate residence where he conducted most of his fraud.

Second, while criminals feel safe on the Internet, they are observable and thus vulnerable. There is the opportunity to uncover crimes in the physical world that would not be visible without the Internet. Murderers have been identified as a result of their online actions, child pornography discovered on the Internet has exposed child abusers in the physical world, and local drug deals are being made online. By observing the online activities of offenders in our neighborhoods, jurisdictions, and companies, we can learn more about the criminal activities that exist around us in the physical world.

Third, 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. For instance, a program like Chat Monitor can be used to find individuals from a specific geographical region who are using Internet Relay Chat (IRC) networks to exchange child pornography.

The crimes of today and the future require us to become skilled at following the cybertrail and finding connections between crimes on the Internet and in the physical world. By following the cybertrail, investigators of physical world crime can find related evidence on the Internet and investigators of crime on the Internet find related evidence in the physical world. The cybertrail should be considered even when there is no obvious sign of Internet activity. Criminals are learning to conceal their Internet activities and, with the rise in wireless networks, there may not be a network cable or other obvious indication that a computer is used to access the Internet.

The Internet may contain evidence of the crime even when it was not directly involved. There are a growing number of sensors on the Internet such as cameras showing live highway traffic as shown in Figure 1.4. These sensors may inadvertently capture evidence relating to a crime. In one investigation of reckless driving that resulted in a fatal crash, the position of the victim's car and average speed were determined using position data relating to a mobile telephone in the car, enabling investigators to locate a surveillance camera at a gas station along the route. The surveillance videotape showed the offender's car tailgating the victim at high speed, supporting the theory that the offender had driven the victim off the road. A cyberstalker can access sensors over the Internet, such as a camera and microphone on a victim's home computer, to monitor his/her activities.

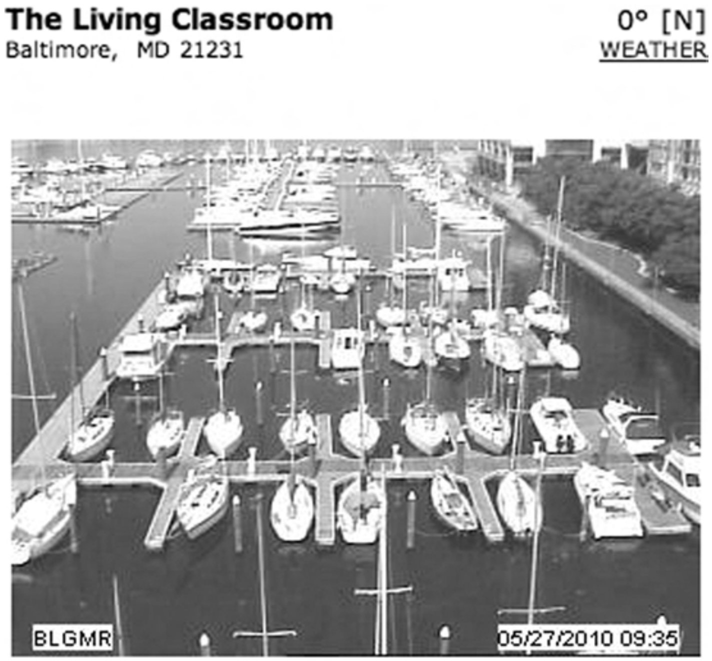


FIGURE 1.4
There are a growing number of sensors on the Internet such as cameras showing activities, cities, highways, and waterways such as the Baltimore harbor on the web.

In addition to the Internet, digital evidence may exist on commercial systems (e.g., ATMs, credit cards, and debit cards) and privately owned networks. These privately owned networks can be a richer source of information than the public Internet. In addition to having internal e-mail, chat, newsgroup, and Web servers, these networks can have databases, document management systems, time clock systems, and other networked systems that contain information about the individuals who use them. Also, private organizations often configure their networks to monitor individuals' activities more than the public Internet. Some organizations monitor which Web pages were accessed from computers on their networks. Other organizations even go so far as to analyze the raw traffic flowing through their network for signs of suspicious activity.

Furthermore, these smaller networks usually contain a higher concentration of digital information (more bits per square foot) about the individuals who use them, making it easier to find and collect relevant digital data than on the global Internet. It is conceivable that a digital investigator could determine where an individual was and what he/she was doing throughout a given day. The time an individual first logged into the network (and from where) would be recorded. E-mail sent and received by an individual throughout the day would be retrievable. The times an individual accessed certain files, databases, documents, and other shared resources might be available. The time an individual logged out of the network would be recorded. If the individual dialed in from home that evening, that would also be recorded and any e-mail sent or received may be retrievable.

1.6.1 Potholes in the Cybertrail

The dynamic and distributed nature of networks makes it difficult to find and collect all relevant digital evidence. Data can be spread over a group of adjacent buildings, several cities, states, or even countries. When dealing with cloud services such as those provided by Google, the location of data can be even more nebulous. For all but the smallest networks, it is not feasible to take a snapshot of an entire network at a given instant. Network traffic is transient and must be captured while it is in transit. Once network traffic is captured, only copies remain and the original data are not available for comparison. The amount of data lost during the collection process can be documented but the lost evidence cannot be retrieved.

Also, networks contain large amounts of data, and sifting through them for useful information can be like looking for a needle in a haystack and can stymie an investigation. Even when the vital digital evidence is obtained, networks provide a degree of anonymity that make it difficult to attribute online activities to an individual. This text provides methods of addressing these obstacles.

1.7 DIGITAL FORENSICS RESEARCH

Applied research is the lifeblood of digital forensics, enabling forensic analysts to keep pace with advances in technology and providing the techniques and tools to extract more useful information from computer systems. In 2010, the Digital Forensic Research Workshop (DFRWS) held its 10th annual conference. The DFRWS has contributed more than any other organization to the advancement of research and development in the field of digital forensics. In addition to bringing together researchers each year to tackle the emerging challenges in digital forensics, the DFRWS poses a forensic challenge each year in an effort to extend the boundaries of digital forensic analysis techniques and supporting tools. In a spirit of knowledge sharing, the DFRWS makes all past papers, presentations, and challenge submissions freely available on the Web site (www.dfrws.org). Other research-oriented groups have developed over the years, including the IFIP Working Group 11.9 on Digital Forensics (http://www.ifip119.org/).

The DFRWS gave new life to an idea proposed several years earlier—a peer-reviewed journal—leading to the creation of the online *International Journal of Digital Evidence* (www.ijde.org). This was followed closely by the publication in 2004 of the peer-reviewed journal *Digital Investigation: The International Journal of Digital Forensics and Incident Response* (http://www.digitalinvestigation.net/). Since then, other research-oriented journals relating to digital forensics have emerged, including the *Small Scale Digital Device Forensics Journal* (www.ssddfj.org/).

1.8 SUMMARY

The ultimate aim of this text is to demonstrate how digital evidence can be used to reconstruct a crime or incident, identify suspects, apprehend the guilty, defend the innocent, and understand criminal motivations.

Digital evidence exists in abundance on open computer systems, communication systems, and embedded computer systems. A hard drive can store a small library, digital cameras can store hundreds of high-resolution photographs, and a computer network can contain a vast amount of information about people and their behavior. At any given moment, private telephone conversations, financial transactions, confidential documents, and many other kinds of information are transmitted in digital form through the air and wires around us—all potential sources of digital evidence. Even crimes that were not committed with the assistance of computers can have related digital evidence (including homicide, arson, suicide, abduction, torture, and rape).

Given the widespread use of computers and the wide use of networks, it would be a grave error to overlook them as a source of evidence in *any* crime. Digital evidence should be sought in all criminal, civil, and corporate internal investigations and the cybertrail should be followed routinely. It should be remembered that privately owned networks may have more sources of digital evidence than the global Internet, detailed monitoring of individuals' activities, and a higher concentration of digital data per unit area.

There are many challenges in dealing with evidence stored on and transmitted using computers. Criminals will be especially eager to use computers and networks if they know that attorneys, forensic examiners, or computer security professionals are ill equipped to deal with digital evidence. Therefore, anyone who is involved with criminal investigation, prosecution, or defense work should be comfortable with personal computers and networks as a source of evidence. One of the major aims of this work is to educate students and professionals in the computer security, criminal justice, and forensic science communities about computers and networks as a source of digital evidence.

Education can only bring us so far. Ultimately, all of these groups must work together to build a case and bring offenders to justice. In addition to learning how to handle digital evidence, law enforcement officers must know when to seek expert assistance. Similarly, computer security professionals must know when to call law enforcement for assistance. Attorneys (both prosecution and defense) must also learn to discover digital evidence, defend it against common arguments, and determine whether it is admissible. Forensic computer examiners must continually update their skills effectively to support investigators, attorneys, and corporate security professionals in digital investigations.

REFERENCES

ASCLD. (2003). Proposed revisions to 2001 accreditation manual. Available from http://www.ascld-lab.org/pdf/aslabrevisions.pdf.

Blanton, T. (1995). The top-secret computer messages the Reagan/Bush White House tried to destroy. *National Security Archive*. Available from http://www.gwu.edu/~nsarchiv/white_house_email/.

Carrier, B. (2003). Defining digital forensic examination and analysis tool using abstraction layers. *International Journal of Digital Evidence*, 1(4), Syracuse, NY. Available from http://www.ijde.org/docs/02_winter_art2.pdf.

Carrier, B. (2006). A hypothesis-based approach to digital forensic investigations. CERIAS Tech Report 2006-06. Available from https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2006-06.pdf.

Casey, E. (2000). *Digital evidence and computer crime* (1st ed.). London: Academic Press.

Casey, E. (2011). Cyberpatterns: Criminal behavior on the Internet. In B. Turvey (Ed.), *Criminal profiling: An introduction to behavioral evidence analysis* (4th ed.). London: Academic Press.

Chisum, J. W. (1999). Crime reconstruction and evidence dynamics. *Presented at the Academy of Behavioral Profiling Annual Meeting*. Monterey, CA.

Henseler, J. (2000). Computer crime and computer forensics. In *The encyclopedia of forensic science*. London: Academic Press.

Johnson, T. (2000). Man searched web for way to kill wife, lawyers say. *Seattle Post-Intelligencer*, June 21, 2000. Available from http://seattlepi.nwsource.com/local/murd21.shtml.

Lee, H., Palmbach, T., Miller, M. (2001). *Henry Lee's crime scene handbook.* London: Academic Press.

McClintock, D. (2001). Fatal bondage, *Vanity Fair*, June.

McCullagh, D. (2002). Electronic evidence anchors porn case. Available from http://news.cnet.com/2100-1023-955961.html.

Reed, C. (1990–91). 2 CLSR 13-16 as quoted in Sommer, P. Downloads, logs and captures: Evidence from *Cyberspace Journal of Financial Crime*, October, 1997, 5JFC2 138–152.

Saferstein, R. (1998) *Criminalistics: An introduction to forensic science,* 6th Ed., Upper Saddle River, NJ: Prentice Hall.

Securities and Exchange Commission. (2002). Order instituting proceedings pursuant to Section 15(b)(4) and Section 21c of the Securities Exchange Act of 1934, making findings and imposing cease-and-desist orders, penalties, and other relief: Deutsche Bank Securities, Inc., Goldman, Sachs & Co., Morgan Stanley & Co. Incorporated, Salomon Smith Barney Inc., and U.S. Bancorp Piper Jaffray Inc. Administrative Proceeding, File No. 3-10957. Available from http://www.sec.gov/litigation/admin/34-46937.htm.

Sullivan, B. (2003). Pair who hacked court get 9 years. *MSNBC*, February 7, 2003.

Venema, W., & Farmer, D. (2000). Forensic computer analysis: an introduction. *Doctor Dobb's Journal*. Available from http://www.ddj.com/documents/s=881/ddj 0009f/0009f.htm.

Yamaguchi, M. (2008). Angry online divorcee "kills" virtual ex-hubby. Associated Press, October 23, 2008.

Zetter, K. (2010). TJX hacker gets 20 years in prison. *Wired Magazine*, March 25, 2010. Available from http://www.wired.com/threatlevel/2010/03/tjx-sentencing/.

Cases

United States v. Grant. (2000). Case No. 99-2332, US District Court, District of Maine. Available from http://laws.lp.findlaw.com/1st/992332.html.

United States v. Ramzi Yousef, Eyad Ismoil. (2003). Available from http://caselaw.findlaw.com/data/circs/2nd/98104IP.pdf.

United States v. Mohammad Salameh. (1993). S12 93 CR. 180, US District Court, Southern District of New York. Available from http://laws.findlaw.com/2nd/941312v2.html.

United States v. Zacarias Moussaoui. (2001). US District Court, Eastern District of Virginia. Available from http://notablecases.vaed.uscourts.gov/1:01-cr-00455/.