Computer Forensics and Investigations

CHAPTER 15

COMPUTER FORENSICS is the scientific process of collecting and examining data stored on, received from, or transmitted by an electronic device. It's a demanding area of study. New technologies that store data are created every day. People who choose to work in this area must constantly study these new technologies. They must learn how to collect and examine data from devices that use the new technology. Computer forensics is also a rapidly expanding profession. The U.S. Department of Labor estimates higher-than-average job growth for people in this career.[1]

This chapter introduces basic concepts about computer forensics. It also discusses the role of the computer forensic examiner. Finally, it reviews legal issues surrounding how digital evidence is gathered and used.

Chapter 15 Topics

This chapter covers the following topics and concepts:

- What computer forensics is
- What a computer forensic examiner does
- What the general rules for collecting, handling, and using digital evidence are
- What some legal issues regarding the seizure of digital evidence are

Chapter 15 Goals

When you complete this chapter, you will be able to:

- Define computer forensics
- Explain the role of a computer forensic examiner
- Explain why digital evidence must be carefully handled
- Describe why chain of custody is important
- Explain the laws that affect the collection of digital evidence
- Describe concerns regarding the admissibility of digital evidence

What Is Computer Forensics?

Computer forensics is the scientific process for examining data stored on, received, or transmitted by electronic devices. The data is examined to find evidence about an event or crime. Law enforcement uses computer forensics to investigate almost any type of crime. Consider the following:

- Illinois state prosecutors used cell phone records and data gathered by computer forensic examiners to convict a defendant of murdering two people. The defendant had used his computer to search "hire a hit man." He had also searched for directions from his home to the victims' home. The case was unique because almost no physical evidence existed to link the defendant to the murders. A judge sentenced him to life in prison.
- A Hong Kong shipping company pleaded guilty to violating U.S. pollution laws. It was fined $10 million. A ship operated by the company ran into the San Francisco Bay Bridge. It spilled more than 50,000 gallons of fuel into the San Francisco Bay. Computer forensic examiners found that someone on the ship altered its computerized navigation charts after the crash.
- A Missouri jury convicted a defendant of possessing child pornography. Digital evidence was used to convict him. Computer forensic examiners found pornographic images on his computer. A judge sentenced the defendant to 35 years in prison.

Computer forensics has many different names. It's also called system or digital forensics, computer forensic analysis, computer examination, data recovery, and inforensics (information forensics). These terms are used interchangeably. This chapter uses the term *computer forensics*.

Computer forensic examiners use specialized software and tools to collect and study data stored on various electronic devices. The evidence collected is called **digital evidence** or just electronic evidence. Computer forensics includes all the steps through which this evidence is collected, preserved, analyzed, documented, and presented.[2] The goal of computer forensics is to find evidence that helps investigators analyze an event or incident.

> **NOTE**
>
> The word *forensics* is from the Latin word *forensis*, which means "belonging to the forum." It refers to the types of arguments used in a court or public forum to prove or disprove past theories or arguments.

Computer forensic examiners study and collect electronic data for many reasons. They don't just investigate crimes. Other computer forensics uses include:

- **Individuals**—People may hire computer forensic examiners to find evidence to support tort claims. They can find digital evidence about sexual harassment or discrimination. Examiners also can uncover evidence for any type of civil litigation. They also can find evidence to support a criminal defense case.
- **Military**—The military uses computer forensics to gather intelligence information to support its operations. It also uses computer forensics to prepare for and respond to cyberattacks.
- **Organizations**—Organizations use computer forensics the same ways that individuals use it. Computer forensic examiners also can investigate employee wrongdoing. They can look for embezzlement or theft of intellectual property (IP). They also can look for unauthorized use of information technology (IT) resources. They can look into attempts to harm an organization's IT resources. An organization's incident response (IR) program can include forensic activities.
- **Colleges and universities**—Many colleges and universities offer programs in computer forensics. Some may have forensic research programs. They also use computer forensics for the institution's own IR activities.
- **Data recovery firms**—Data recovery firms use computer forensics to rescue data for their clients. They also advise clients how to keep data safe from loss.

Most electronic devices hold some type of data. Computer forensics can study any of them. Potential sources of digital evidence include:

- **Computer systems**—This includes laptop and desktop computers, and servers. It also includes the hardware and software that the system uses. This category also includes peripheral devices that can be attached to computer systems. These devices enhance the user experience. They may include keyboards, microphones, Web cameras, and memory card readers.

- **Storage devices**—This includes internal and external hard drives. It also includes removable media such as floppy disks, Zip disks, compact discs (CDs), digital versatile discs (DVDs), thumb flash drives, and memory cards.
- **Mobile devices**—This includes cell phones and smartphones. It also includes tablets, personal digital assistants (PDAs), and pagers. Global positioning system (GPS) devices hold data as well. Digital and video cameras, and audio and video multimedia devices also fall into this category.
- **Networking equipment**—This includes network hubs, routers, servers, switches, and power supplies. Networking equipment can be wired or wireless.
- **Other potential sources**—Many office devices have data storage ability. This includes copiers and fax machines, answering machines, printers, and scanners. Entertainment devices store data as well. They include digital video recorders (DVRs), digital audio recorders, and video game systems. Surveillance equipment is included in this category. This category includes any device not already mentioned that can store data.

People's dependence on electronic devices to live their lives continues to grow. As a result, computer forensics as a special area of study also grows. Computer forensic examiners aren't always experts in collecting data from every possible type of electronic device. They often focus on certain types of devices. In addition, most computer forensic examiners focus their skills in specific areas. The three main areas of computer forensics are:

- Media analysis
- Code analysis
- Network analysis

Media analysis focuses on collecting and examining data stored on physical media. This includes computer systems and storage devices. It also includes mobile devices. When people think about computer forensics, they most often think about media analysis. This type of analysis discovers normal and deleted data. It also finds encrypted, hidden, and password-protected data. This chapter focuses mostly on media analysis concepts. These concepts apply to other types of computer forensic analysis as well.

Code analysis focuses on reviewing programming code. It's also called malware forensics. This area looks for malicious code or signatures from viruses, worms, and Trojans. It looks for the signature of anything that has modified a system without permission. A signature is the executable part of a malicious code. The need for code analysis continues to grow. A 2013 report estimated that 69 new pieces of malware are created each minute.[3]

NOTE

Antivirus programs use signatures to help them detect malware on a computer system.

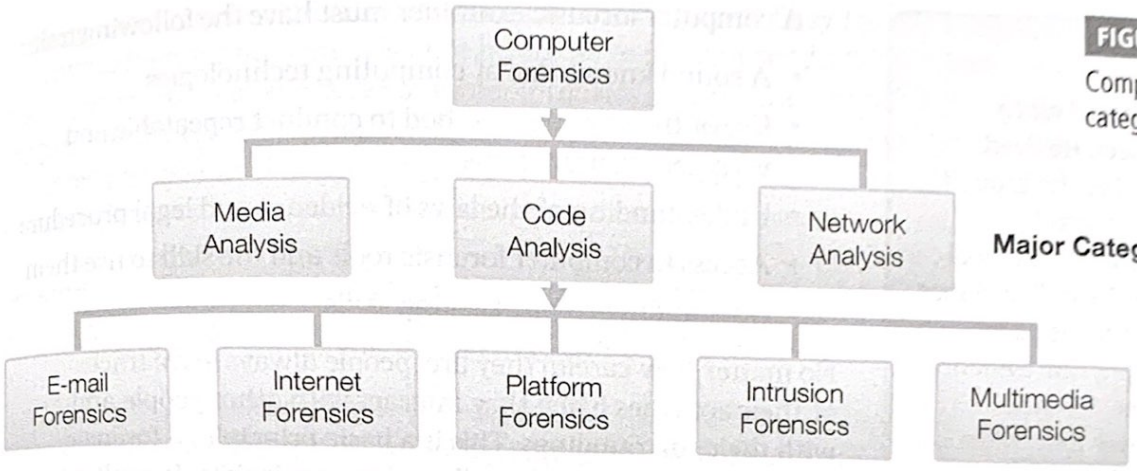

FIGURE 15-1
Computer forensic categories.

Network analysis focuses on collecting and examining network traffic. An examiner reviews transaction logs and uses real-time monitoring to find evidence. Organizations often use this type of analysis to investigate incidents.

Some computer forensic examiners also might have specialties within these three major categories. For example, some examiners might specialize in e-mail forensics. E-mail forensics includes a combination of media and network analysis. It's used to find the sender, recipient, date, time, location information, and contents of e-mail messages. As technology advances, it's not unusual to find examiners with very specialized skills. Figure 15-1 shows different computer forensic categories.

What Is the Role of a Computer Forensic Examiner?

Computer forensics is a fairly new field. It's only a few decades old. It's growing quickly. In 1984, the U.S. Federal Bureau of Investigation (FBI) began creating software programs to collect computer evidence.[4] In 1990, the International Association of Computer Investigative Specialists (IACIS) was formed. The IACIS is the oldest computer forensic professional group. It was the first group to use the phrase *computer forensics*.[5]

The first international conference on computer forensics was held in 1993. In 1995, the International Organization on Computer Evidence (IOCE) was formed. The IOCE creates guiding principles for computer forensic examiners. The IOCE is a international organization of law enforcement agencies. The U.S. arm of the IOCE is the Scientific Working Group on Digital Evidence (SWGDE).[6]

Computer forensic examiners find evidence on electronic devices. They collect it for both civil and criminal cases. They must collect this evidence in a scientific manner, regardless of the underlying case. They also must have a full understanding of various technologies, hardware, and software. An examiner helps answer who, what, where, when, why, and how.

> **NOTE**
> The scientific method is a way to answer questions in a repeatable and verifiable way. It's a formal method of investigation.

> **NOTE**
> Dr. Edmond Locard was a forensics pioneer. He lived from 1877 to 1966. He argued that scientific methods should be applied to criminal investigations. He believed that when people or objects interact, they transfer physical evidence to one another. Forensic scientists recover that evidence. They study and learn from it.

A computer forensic examiner must have the following traits:

- A sound knowledge of computing technologies
- Use of the scientific method to conduct repeatable and verifiable examinations
- Understanding of the laws of evidence and legal procedure
- Access to computer forensic tools and the skill to use them
- Outstanding record-keeping skills

No matter how careful they are, people always leave traces of their activities when they interact with other people and with their surroundings. This is a basic principle of forensic science. It's known as **Locard's exchange principle**. It applies to the digital world and the physical world. If people attempt to steal electronic information or delete incriminating files, they leave electronic traces of their activities. For example, log information can document these activities. A computer forensic examiner needs to know how to find this trace evidence material. This evidence is used to help prove a person's actions in a computer system.

Computer forensic examiners do more than turn on a computer and search through files. They must perform complex data recovery procedures. In particular, they must:

- Protect the data on any electronic device.
- Avoid deleting, damaging, or altering data in any way on any electronic device.
- Make exact copies of electronic data without altering the original device.
- Discover normal, deleted, password-protected, hidden, and encrypted files.
- Study data to create timelines of electronic activity.
- Identify files and data that may be relevant to a case.
- Fully document all evidence-collection activities.
- Provide expert testimony on the steps taken to recover digital evidence.

Computer forensic examiners must have special skills. They have skills beyond those of the traditional information security professional. The law requires that computer forensic examiners be competent at what they do. Examiners can show that they are competent by earning advanced degrees. They also can become certified. Since the profession is still new, there are many computer forensic certifications to choose from. Both independent organizations and vendors offer them.

States and courts struggle with how to make sure computer forensic examinations are done only by competent examiners. Courts rely on legal principles and trial rules to screen examiners before they testify. Sometimes states create laws that govern the activities of these examiners. Often, computer forensic examiners are governed under the broad terms of a state's private detective laws.

Many states regulate private detectives and investigators. They require a private detective to have a state-issued license before he or she can conduct investigations. These laws were created before computer forensics existed as a separate field. The broad language of these laws can pull computer forensic examiners within the scope of these regulated professions. This isn't unusual. Even the U.S. Department of Labor includes computer forensic examiners within the private detective profession.[7]

Computer Forensic Examiner Certifications

There are many independent and vendor-specific computer forensic credentials. An examiner must weigh which credential best suits his or her career path. The following are popular credentials:

- **Certified Computer Examiner (CCE)**—The International Society of Forensic Computer Examiners (ISFCE) offers the CCE. The ISFCE has offered the CCE since 2003. It's a vendor-neutral certification. CCE holders have basic knowledge of forensic examination procedures. You can learn more at *http://www.isfce.com/*.
- **Certified Computer Forensics Examiner (CCFE)**—The Information Assurance Certification Review Board (IACRB) offers the CCFE. It's also vendor neutral. CCFE candidates must take a written exam and a practical application test. There are nine subject-matter areas in the CCFE exam. You can learn more at *http://www.iacertification.org/index.htm*.
- **Certified Forensic Computer Examiner (CFCE)**—The International Association of Computer Investigative Specialists (IACIS) offers the CFCE. Only law enforcement personnel may earn it. It's vendor neutral. CFCE candidates must pass an intensive practical exam. You can learn more at *http://www.iacis.com/*.
- **GIAC Certified Forensic Analyst (GCFA)**—The Global Information Assurance Certification (GIAC) program offers the GCFA. Like the CCE and CCFE, this certification also tests practical knowledge. It's vendor neutral. You can learn about GIAC at *http://www.giac.org/*.

Some forensic software vendors offer certifications for their products. EnCase is a popular forensic tool sold by Guidance Software. It offers the EnCase Certified Examiner (EnCE) credential. The EnCE exam has a written section and a practical section. The practical section covers use of the EnCase forensics program. You can learn more at *www.guidancesoftware.com/training/Pages/ence-certification-program.aspx*.

Another software vendor that offers a certification is AccessData. AccessData offers a product known as the Forensic Toolkit. The product is better known as FTK. AccessData offers the AccessData Certified Examiner (ACE) credential. It tests knowledge of the FTK tool. The ACE exam is a multiple-choice test. You can learn more at *http://www.accessdata.com/training/ace-process*.

Some states require computer forensic examiners to have a private detective license. Examples include Illinois,[8] Michigan,[9] Oregon,[10] and Texas.[11] In Texas, the law is interpreted very broadly. It actually includes computer technicians and computer repair personnel within the scope of its law.

Some states don't include computer forensic examiners within their private detective licensing laws. North Carolina[12] and Virginia[13] are examples. North Carolina law states that any person who performs computer forensic services in order to collect evidence isn't a private investigator. The North Carolina law also excludes examiners who provide expert testimony. It also excludes any person who engages in network or system vulnerability testing.

In 2008, the American Bar Association (ABA) issued a report and resolution on computer forensic examiners. The ABA asked states to stop requiring computer forensic examiners to get a private detective license. It said that the role of private detectives is different from that of computer forensic examiners. It also stated that courts have broad discretion to make sure that digital evidence used in trials is reliable. Since the courts have that discretion, the ABA argued that there's no need to license computer forensic examiners. You can read the document at *http://www.americanbar.org/groups/science_technology/pages/forensicresolution.html*.

Collecting, Handling, and Using Digital Evidence

> **NOTE**
>
> Computer forensic examiners should always collect digital evidence in a reliable (forensically sound) manner. The nature of the underlying investigation doesn't matter. The examiner should always use a reliable and repeatable process.

Computer forensic examiners find evidence on electronic devices. They use this evidence to help reconstruct past events or activities. They use the evidence to gain a better understanding of a crime or event. It can be used to show possession and use of digital data. This section discusses how computer forensic examiners collect digital evidence. It focuses on how this evidence is collected in a criminal investigation. You need to keep in mind that almost the same process will be used in a civil investigation. An organization's IR process also will be similar.

A computer can play one of three roles in computer crime. It can be used to commit a crime, it can be used to facilitate a crime, or it can be the target of a crime. A computer, or any electronic device, can be used to commit a crime. Cyberstalking, identity theft, and phishing scams are examples of crimes facilitated by computers. The computer also can be the target of a crime. Denial of service (DoS) and distributed denial of service (DDoS) attacks, computer viruses, and communications sabotage are examples of crimes where the computer itself is the target of the crime. A computer can also play a role as witness to a crime. In every case, the computer or electronic device will hold information about the underlying crime or event. If the computer forensic examiner knows how the computer was used, he or she will be able to tailor the examination to that use.

FYI

It's important that evidence used in a court case be admissible. A judge or jury can consider only admissible evidence when they decide cases. Evidence that is invalid for some reason is called inadmissible evidence. Inadmissible evidence can't be presented to a judge or jury. A judge or jury who accidentally hears about that evidence cannot consider it later in deliberations. Admissible evidence is good evidence. Inadmissible evidence is bad evidence.

The examiner must gather evidence in a way that makes it admissible in court. Evidence is useful only if it's admissible. To be admissible, evidence must be collected in a lawful way. It also must be collected in a scientific manner. For digital evidence, this means that a computer forensic examiner conducts a repeatable and verifiable examination of an electronic device. The examiner must use established practices and procedures. The examiner also must be able to explain the results of his or her work to a client, judge, or jury in a clear way.

The Investigative Process

Different law enforcement agencies and organizations may use different investigative processes. The process used can depend on the type of case. It also can depend on the urgency of the case. The process also can depend on the agency or organization that performs the investigation. In general, the investigative process has the following basic steps:

- Identification
- Preservation
- Collection
- Examination
- Presentation

This basic process is used by both law enforcement agencies and other organizations to identify, collect, and preserve digital evidence.

Identification

During the identification step, the computer forensic examiner learns about the crime, event, or activity that is being investigated. He or she must identify the types of electronic devices that may be involved. The examiner must prepare to conduct the investigation. The examiner must make sure that he or she has all the tools needed to conduct the investigation.

A computer forensic examiner's approach to a case may depend heavily on its facts and circumstances. For example, the examiner may have to collect evidence on-site if seizing the devices and taking them back to a lab isn't possible. This might happen in cases where evidence is located on an organization's business computers.

Seizing the computers may not be possible if the computers are instrumental to the organization's business. This might be the case if the computers belong to a witness and not to a criminal suspect.

Preservation

During the preservation step, computer forensic examiners must secure the crime scene and any electronic devices. This means that they must make sure that no one tampers with the scene or electronic devices. This is to make sure that suspects and witnesses don't have a chance to access, destroy, or modify digital evidence. Examiners also must make sure that no one can access electronic devices remotely once they are seized.

Can a Person Be Compelled to Provide His or Her Encryption Key or Password?

Many information security professionals advise their clients to encrypt data. This helps protect the data in the event that the client experiences a security breach. In cases where the electronic devices are seized for evidence, encryption can be a problem for a computer forensic examiner. Can the government compel a data owner to provide an encryption key or password? What happens if the data owner is a suspect in the case? Does requiring a suspect to provide an encryption key or password violate the person's Fifth Amendment self-incrimination protections? The Fifth Amendment is best known for its "right to remain silent."

The U.S. Supreme Court has held that the Fifth Amendment protects communications that are compelled, testimonial, and incriminating in nature.[14] Testimonial communications are communications that provide facts or assertions. The heart of the issue is whether providing a password is testimonial. A defendant can potentially incriminate himself or herself if compelled to disclose a key or password to decrypt data on an electronic device.

Case law in this area is just beginning to develop. One case suggests that requiring a defendant to provide a password may not raise a self-incrimination issue. In December 2006, Sebastien Boucher entered the United States from Canada. His car was searched at the border. He had a laptop in his car, and border officers searched the laptop with Boucher's permission. The laptop contained files that appeared to be child pornography. Boucher said that he sometimes visited adult Web sites and that occasionally he downloaded adult pornography. He said those downloads sometimes include child pornography and that he always deleted it as soon as he found it. The officers arrested Boucher and seized the laptop. They turned the laptop off.

The government later got a search warrant to search the laptop. The computer forensic examiner could not examine the hard drive because it was encrypted. He could not break the encryption code. The government asked for a grand jury subpoena to force Boucher to share the password, enter it on the laptop in front of the grand jury, or produce an unencrypted copy of the hard drive.

All of these actions make sure that potential digital evidence can't be altered. This step is very important because once digital evidence is altered, it's difficult, if not impossible, to reverse the results.

Computer forensic examiners also should learn about the operation of the electronic devices they will be examining. They will want to gather information from people at the scene to learn how the devices are used. They should try to learn logon names and passwords for access to the devices. They also should try to discover the type of Internet access used by each electronic device and programs used on each device. It's also important for examiners to know whether devices are encrypted, or whether they are equipped with software that could destroy evidence.

Can a Person Be Compelled to Provide His or Her Encryption Key or Password? *continued*

Boucher argued that all of those options violated his Fifth Amendment rights. A magistrate judge said that Boucher didn't have to provide the password or unencrypted copy. The government appealed.

The U.S. District Court for the District of Vermont reversed the magistrate's ruling. He directed Boucher to provide an unencrypted version of the hard drive. The judge said that because Boucher showed unencrypted data to the border officers, the government knew that the incriminating data existed. Therefore, Boucher was not giving testimony. Since he wasn't giving testimony, he wasn't incriminating himself by providing the password or unencrypted data. The government already knew incriminating data existed and was located on the hard drive. Since Boucher had already admitted that the laptop was his, he wasn't further incriminating himself by providing the requested password or data.[15]

Another case reached a different result. This case was decided in March 2010 in the U.S. District Court for the Eastern District of Michigan. The facts are slightly different. In this case, a grand jury had indicted a defendant for receiving child pornography by computer. The government still needed to collect evidence about the crimes. The government asked for a subpoena requiring the defendant to provide all passwords to his computer. The judge in this case said that the government was seeking testimony from the defendant when it asked him for his computer passwords. In this case, it appears that the government didn't know the extent of the potentially incriminating information on the defendant's computer. Therefore, requiring the defendant to share passwords was seeking testimony from him because the government intended to use his password to gather information that would incriminate him.[16]

The case law on this issue is new. You can expect judges to continue to define the scope of the Fifth Amendment in these situations. Since this is an area of federal constitutional law, the U.S. Supreme Court has the power to make a decision on the issue.

Chain of Custody

A **chain of custody** is an important evidentiary concept. Courts and attorneys use a chain of custody document to help prove that evidence is admissible. A chain of custody document shows who obtained evidence, where and when it was obtained, who secured it, and who had control or possession of it. It's used to prove that evidence is reliable.

Evidence is reliable when it's not destroyed, changed, or altered. It can't be modified after it's originally collected. A court may find that evidence isn't admissible in court if its chain of custody is poorly documented or incomplete. A chain of custody protects the integrity of evidence.

A chain of custody documents how evidence is collected, used, and handled throughout the lifetime of a particular case. It's a journal that records every interaction that a person or object has with the evidence.

This step also includes documenting the crime scene. Examiners must record the location of all electronic devices. They also should note whether the device is on or off. They should record the condition of all devices. Examiners also should record the content of any display screens before electronic devices are moved. The crime scene can be documented using video, photos, and written notes. The documentation created at this step is important for creating a chain of custody.

Collection

The collection step also is known as the "bag and tag" step. During this step, computer forensic examiners must collect the electronic devices. These devices require special collection, packaging, and transportation in order to preserve potential evidence. For example, in most instances, a cell phone must be kept powered on in order to preserve data stored on the device. However, it must be protected from any calls or text messages that could change the data on it. The cell phone must be packaged and transported in a special evidence bag once it's collected. These special evidence bags are called Faraday bags. They keep a cell phone shielded from incoming calls or from connecting to wireless networks. This is so that data stored on it can't be changed by an incoming call or wireless network connection. A computer forensic examiner also must make sure that the collected cell phone has an additional power supply to maintain evidence that could be lost if its battery runs out. Examiners will collect electronic devices in different ways depending upon the device and its power status. They will follow different rules for devices that are on and devices that are off.

FYI

Slack space is the space between the end of a data file and the end of the disk space that is allocated to store it. Data doesn't always fill the whole space that's allocated to it. Residual information can be left over when a smaller file is written into space that used to be occupied by a larger file. This leftover data may be located in the slack space. Computer forensic examiners look at the slack space because it might contain meaningful data.

During this step, examiners must be aware of other evidence that could be on electronic devices. A keyboard or mouse could contain fingerprints or other physical evidence related to the case. Computer forensic examiners must work with other forensic technicians. They must make sure that this type of physical evidence isn't destroyed.

As a practical matter, examiners must document how all electronic devices are configured. The cables and peripheral devices that are hooked up to each computer will need to be tagged. Examiners also must collect any manuals or other materials about the electronic devices that are located near the crime scene.

Examination

During the examination step, computer forensic examiners will want to make duplicate images of any electronic storage media. This is called *imaging*. One thing to remember is that a **forensic duplicate image** is not the same as a file copy or system backup copy. It's an exact copy of the storage media. It includes deleted files, slack space, and areas of the storage media that a normal file copy would not include. A duplicate image is a bit-by-bit copy of the original storage media.

Computer forensic examiners use special tools called *write blockers* to create digital images. These tools keep examiners from altering the original storage media. Write blockers can be either hardware- or software-based. They work somewhat like a one-way flow valve in plumbing. Most examiners will make two or more duplicate images of the original storage media. One copy is a working copy that they will use to look for evidence. The other is a control copy that can be used if something goes wrong with the first copy.

A duplicate image must be verified against the original storage media. This makes sure that the duplicate image is identical to the original. It makes sure that nothing has changed on the original media or the image. Examiners verify the images using a cryptographic equation called an *algorithm*. They will apply the algorithm to the original media to create a hash. A *hash* is the value that is the result of the cryptographic equation on the image. The examiner will apply the same algorithm to the duplicate image to create another hash.

> **NOTE**
> The output of a hashing algorithm is sometimes called a *checksum*.

The examiner can prove that the duplicate image accurately represents the original media if the hashes are the same. If the hashes are different, the images are not the same. Different hashes mean that the imaging process was faulty or some sort of change took place between the original media and the duplicate image. Hashes are used to measure the integrity of the original media and the forensic duplicate. If the hashes don't match, then the data has changed somehow.

Computer forensic examiners need to know how to collect two very different types of data. **Persistent data** is stored on a hard drive or other storage media. It's preserved when an electronic device is turned off. **Volatile data** is stored in memory. Volatile data exists in registries, the cache, and random access memory (RAM). It also is the connections that one electronic device might have with another while both devices are powered on. Volatile data is lost when an electronic device is turned off. Examiners must know when this data must be collected and how to do it.

Computer forensic examiners search for relevant information on the duplicate image. They have checklists of items that they review and look for. In general, they might look at:

- File access history (when were files created, edited, and last accessed)
- File download history
- Internet browsing history
- Attempts to delete or conceal files or other data
- E-mail communications
- Instant message or Internet chat logs
- Image files
- Files containing address books or other contact information
- Documents containing financial or medical information

Examiners produce a report of files or data that might be relevant to the investigation. They must use examination procedures that are auditable. That means that an independent party can verify and repeat all of the same steps and receive the same results.

Presentation

Computer forensic examiners must be able to report on their findings. They must be able to describe how they gathered digital evidence. They often have to explain how they collected this evidence if a case goes to trial. Examiners are usually considered expert witnesses when they testify in a court case. Expert witness testimony is governed by the Federal Rules of Evidence.[17] Expert witnesses must show that their activities followed a scientific methodology. A court assesses this process to make sure that evidence offered at trial is reliable.

The test for measuring the reliability of a scientific methodology is called the Daubert test. It was first discussed in a U.S. Supreme Court case called *Daubert v. Merrell Dow Pharmaceuticals.*[18] This test is important to computer forensics. It comes into play because of the tools that examiners use to collect digital evidence. An expert witness is a person. The software tools used by examiners can't be expert witnesses. Thus, examiners must testify on behalf of the tools.

The use of a tool must satisfy the Daubert test to show that the digital evidence gathered by the tool is reliable. The Daubert test asks the following questions to determine reliability:

- Has the tool been tested?
- Is there a known error rate for the tool?
- Has the tool been peer reviewed?
- Is the tool accepted in the relevant scientific community?

The examiner will testify about how the tool works. The examiner also will testify about his or her qualifications as a computer forensic examiner. Finally, the examiner will testify about the process the examiner used to collect the digital evidence. The court will use the Daubert test to decide whether to admit the evidence collected by the examiner.

Guiding Principles for Forensic Examination

Computer forensic examiners all follow some common principles. The International Organization on Computer Evidence has created the most well-known set of principles. They were created in 1999. They are:

- Examiners should not change digital evidence after they seize it.
- If original digital evidence must be accessed, the person accessing it must be competent.
- All digital evidence handling must be fully documented and available for review.
- Each person who handles digital evidence is responsible for it while it's in his or her possession.
- Any agency that handles digital evidence must comply with these principles.[19]

The American Academy of Forensic Sciences

The American Academy of Forensic Sciences (AAFS) recognizes computer forensics as a scientific discipline. The AAFS is one of the most well-known professional organizations for forensic scientists. It has members from many different forensic disciplines. Its goals are to promote integrity and advance cooperation in the forensic sciences.

The AAFS has different sections for different areas. It created a digital and multimedia sciences section in February 2008. The digital and multimedia sciences section was the first new AAFS section in 28 years. The section started with 42 members in 2008. By 2014, it had grown to 127 members. Members must show active participation in computer forensic activities. All AAFS members have ethical rules that they must follow.

You can learn more about the AAFS at *http://www.aafs.org*.

The IOCE is an international group of law enforcement agencies. These agencies exchange information about computer forensic issues. They all agree to follow the IOCE principles.

These principles are followed in different forms by other organizations. For example, the Certified Computer Examiner (CCE) credential requires CCE holders to follow a code of ethics. That code of ethics has terms that are similar to the IOCE principles.

Legal Issues Involving Digital Evidence

There are special rules for collecting and handling digital evidence. However, the process for obtaining the electronic devices and the evidence on them in the first place must follow established legal principles. The law asks two basic questions about evidence:

- Did the person or organization that collected the evidence have the legal authority to do so?
- Is the evidence admissible in court?

Legal principles and statutes are used to address the first question. These laws focus on the situations where a private entity or the government can collect information about a person.

Court rules and case law are used to address the second question. Both the federal government and state governments have trial court rules for civil and criminal proceedings. In addition to these rules, federal and state courts have evidentiary rules. Evidentiary rules govern how parties introduce evidence at trials. This chapter uses the Federal Rules of Evidence to illustrate admissibility requirements. Many states have evidence rules based on the Federal Rules of Evidence.

One thing to keep in mind as you review this section is that there are differences between how law enforcement and private entities conduct investigations. Law enforcement agencies have very specific rules that they must follow when they collect evidence. This is because a law enforcement agency is acting on behalf of a government. They are agents of either the federal or a state government. In the United States, a government can't take some actions against its citizens without proper authority. This is part of our "checks and balances" system of government. For example, unless special circumstances exist, law enforcement must get permission from a court to monitor a person's telephone conversations.

The rules are different for private entities. Private entities are individuals and organizations that aren't related to a governmental agency. As long as a private entity is acting within the rule of law, it may take certain actions to protect its own interests. This is why an employer may monitor an employee's telephone conversations when the employee is using the employer's telephone equipment. A private entity generally has the right under the law to monitor and collect data about its own IT resources in order to protect them.

The Silver Platter Doctrine

The difference between the government's ability to collect evidence of a crime and a private entity's ability to collect evidence about that same activity is an interesting area of study. It's also a complicated area of study. The resolution of many court cases depends on these differences. Sometimes laws create special rules for law enforcement and private entities.

The Electronic Communications Privacy Act (ECPA)[20] sets out the rules for access, use, disclosure, and interception of stored electronic communications. Electronic communications include telephone, cell phones, computers, e-mail, faxes, and texting. Under the ECPA, no one may access the contents of these communications unless it's allowed somewhere else in the ECPA. The law has different rules for the government and for private entities.

The ECPA has strict rules for the government. The government can't access any stored electronic communications without a search warrant. To get a search warrant, the government must prove to a court that it has probable cause to believe that criminal activity is taking place. The stored communications must hold evidence of the criminal activity. If the government can't prove probable cause, then it can't access these communications.

The ECPA has different rules for private entities. Private entities may access stored communications within their ordinary course of business. To use this exception, the private entity must have a legitimate business interest for accessing these communications. They also must show that the access occurred on equipment provided by a communications service provider. The ECPA also allows private entities to access employee communications if the employee gives consent. The private entity must be able to prove that it provided notice of access to its employees and that the employees consented to it.

Sometimes private entities find evidence of criminal activity. The ECPA allows most types of private entities to lawfully disclose this evidence to law enforcement agencies. This evidence often is very useful to a criminal investigation. Sometimes a prosecutor will want to use this evidence at a criminal trial. The evidence rule known as the *silver platter doctrine* applies in these cases. This rule is called the silver platter doctrine because the private entity gives admissible evidence to law enforcement "on a silver platter." Law enforcement didn't need a search warrant to access the evidence because it didn't collect it or direct its collection.

The silver platter doctrine allows the admission of evidence lawfully collected by a private entity. The evidence collected by the private entity must be collected and documented properly. To take advantage of the silver platter doctrine, the government must show that the private entity isn't affiliated with law enforcement or a government (state or federal). The private entity must not be collecting the evidence under the direction of law enforcement or a government. The private entity also can't be an Internet service provider (ISP). There are special rules under the ECPA for ISPs.

Authority to Collect Evidence

There are many laws that define and limit the government's ability to monitor and collect data about individuals. The basic protections afforded to U.S. citizens stem from the Constitution. The Fourth Amendment protects citizens from an intrusive government.

Other laws further define how the government can collect and monitor data. These laws affect the activities of computer forensic examiners. The Electronic Communications Privacy Act,[21] the Wiretap Act,[22] and the Pen Register and Trap and Trace Statute[23] are discussed in this section.

The Fourth Amendment and Search Warrants

The Fourth Amendment protects people from unreasonable government search and seizure. A *search* happens when a person's reasonable expectation of privacy in a place or thing is compromised. A *seizure* happens when the government interferes with a person's property. Interference includes taking the property or using it in such a way that the person who owns it can't use it.

The Fourth Amendment states that the government may not search or seize areas and things in which a person has a reasonable expectation of privacy. If a person has a reasonable expectation of privacy in a place or item, then the government must get a search warrant before searching it or taking it. Under the Fourth Amendment, the "government" includes law enforcement. This section uses the terms government and law enforcement interchangeably.

NOTE

A search warrant is a court order. A judge issues a search warrant after the government proves that it has probable cause to believe that criminal activity is taking place. Probable cause is a burden of proof.

Several court cases have held that people have a reasonable expectation of privacy in their personal computers and mobile devices. The U.S. Court of Appeals for the Ninth Circuit has found that a person has a reasonable expectation of privacy in a personal computer. That case is called *United States v. Heckenkamp.*[24] Other courts have held that people have a reasonable expectation of privacy in data stored on personal pagers.[25] To search these devices, law enforcement must get a search warrant.

FYI

The Fourth Amendment applies to federal government actions only. Most state governments have state constitutional protections that are similar to the Fourth Amendment. The Fourth Amendment doesn't apply to private individuals or entities that conduct searches or seizures. The private individual or entity must act alone and without government direction. The Fourth Amendment may apply when a private individual or entity follows government directions in conducting a search.

To get a search warrant, law enforcement must specify the criminal activity that is being investigated. It must describe where the search will take place. It also must list the items that will be searched. Finally, law enforcement must state the evidence that they expect to find. They also must state how that evidence relates to the criminal activity that is being investigated.

If law enforcement conducts a search without a valid warrant, then any evidence that it finds isn't admissible in court. This means that a judge won't allow the government to use that evidence to prove its case. Although the rule is strict, there are some exceptions. Court-recognized exceptions to the Fourth Amendment's search warrant requirements include:

- **Consent**—Law enforcement can search places and items if the person in control of them freely consents to the search. For example, a person can allow law enforcement to search his or her home, car, or computer. A person's consent must be free and voluntary. If law enforcement finds evidence of criminal activity during a voluntary search, it's admissible in court. Cases reviewing this exception often focus on whether a person's consent really was free and voluntary.
- **Plain view doctrine**—Law enforcement doesn't need a warrant to search and seize evidence that is in an officer's "plain view." The officer must be able to see the evidence from a place where the officer has a right to be. This exception is often used to seize drugs or other contraband. For example, a police officer can seize drug paraphernalia that he or she sees in a car if the officer can plainly see the items in the car's back seat while standing on a public street.
- **Exigent circumstances**—Law enforcement is allowed to make a warrantless search and seizure in emergency circumstances. This exception applies if public safety would be harmed or evidence would be destroyed if law enforcement took the time to go to court to get a warrant. This exception also is called the "emergency" exception. Law enforcement often seizes drugs and weapons using this exception. Court cases reviewing this exception focus on whether a true emergency existed at the time the search or seizure took place.
- **Search incident to a lawful arrest**—Law enforcement doesn't need a warrant to search for weapons or contraband on the body of an arrested person. In some cases, law enforcement may make a brief visual inspection of the area where a person is arrested to make sure that no accomplices are hiding nearby. Law enforcement officers are allowed to make these warrantless searches in order to protect their own safety. They also can use this exception to make sure that critical evidence isn't destroyed during the arrest process. Courts strictly construe this exception to make sure that it's not abused. This exception also is called the *protective sweep* exception.

- **Inventory search**—Law enforcement may conduct inventory searches without a warrant when they arrest a suspect. These searches are allowed when they're made for a non-investigative purpose. For example, if a suspect has a laptop computer when he or she is arrested, law enforcement may seize the computer for safekeeping while the suspect is in custody. This helps protect law enforcement from claims that they lost or stole a suspect's property. For the exception to apply, the law enforcement agency must have standard policies and procedures for conducting inventory searches. They also must document the search. Court cases reviewing this exception focus on whether law enforcement was following a documented policy for inventory searches. They review whether the inventory search was a ploy to hide a more thorough search for evidence.

One important thing to keep in mind is that the Fourth Amendment search warrant exceptions allow for the seizure of the media containing the digital evidence. Law enforcement can seize the physical media only. If they want to conduct a forensic examination of that media, they must get a warrant to do so. The search warrant must authorize the forensic examination. Unless emergency circumstances exist, the secondary search warrant ensures that any digital evidence collected from the media will be admissible in court. Computer forensic examiners must make sure there's a valid search warrant for any electronic devices that they collect. They also must make sure that the warrant allows them to search the data on the device.

Federal Laws Regarding Electronic Data Collection

Three main federal laws govern the collection of electronic communications data. These laws cover many different communications. They include e-mail, radio and electronic communications, data transmissions, and telephone calls. Computer forensic examiners often study these communications when they investigate cases or events. An examiner must make sure that his or her actions follow the law.

> **NOTE**
> Keep in mind that states also might have laws governing the collection of electronic communications evidence. You must always review both federal and state laws when considering a legal issue.

These laws forbid the use of eavesdropping technologies. This means that the government, individuals, and private entities can't use certain technologies to snoop on electronic communications. The only time use of these technologies is allowed is when the law says it's allowed. Usually this is when the law allows an exception or if an entity has a court order. The three laws are:

- The Electronic Communications Privacy Act
- The Wiretap Act
- The Pen Register and Trap and Trace Statute