PART I

Introduction to Forensics

CHAPTER 1

Introduction to Forensics

THIS CHAPTER INTRODUCES YOU TO THE FIELD of computer forensics. That means it will cover some legal issues, the basic concepts of the forensic process, and a review of the basic computer and networking knowledge you will need.

Chapter 1 Topics

This chapter covers the following topics and concepts:

- What computer forensics is
- What you need to know about the field of digital forensics
- What you need to know for computer forensics analysis
- What the Daubert standard is
- What the relevant laws are
- What the federal guidelines are

Chapter 1 Goals

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

- Understand the basic concepts of forensics
- Maintain the chain of custody
- Understand basic hardware and networking knowledge needed for forensics
- Know the basic laws related to computer forensics

What Is Computer Forensics?

Before you can answer the question, "What is computer forensics?" you should address the question, "What is forensics?" The *American Heritage Dictionary* defines *forensics* as "the use of science and technology to investigate and establish facts in criminal or civil courts of law."

Essentially, forensics is the use of science to process evidence so you can establish the facts of a case. The individual case being examined could be criminal or civil, but the process is the same. The evidence has to be examined and processed in a consistent scientific manner. This is to ensure that the evidence is not accidentally altered and that appropriate conclusions are derived from that evidence.

You have probably seen some crime drama wherein forensic techniques were a part of the investigative process. In such dramas, a bullet is found and forensics is used to determine the gun that fired the bullet. Or, perhaps a drop of blood is found and forensics is used to match the DNA to a suspect. These are all valid aspects of forensics. However, our modern world is full of electronic devices with the capacity to store data. The extraction of that data in a consistent scientific manner is the subject of **computer forensics**.

The Computer Emergency Response Team (CERT) defines computer forensics in this manner:

> Forensics is the process of using scientific knowledge for collecting, analyzing, and presenting evidence to the courts.… Forensics deals primarily with the recovery and analysis of latent evidence. Latent evidence can take many forms, from fingerprints left on a window to DNA evidence recovered from blood stains to the files on a hard drive.

According to the website Computer Forensics World:

> Generally, computer forensics is considered to be the use of analytical and investigative techniques to identify, collect, examine and preserve evidence/information which is magnetically stored or encoded.

The objective in computer forensics is to recover, analyze, and present computer-based material in such a way that it can be used as evidence in a court of law. In computer forensics, as in any other branch of forensic science, the emphasis must be on the integrity and security of evidence. A forensic specialist must adhere to stringent guidelines and avoid taking shortcuts.

Any device that can store data is potentially the subject of computer forensics. Obviously, that includes devices such as network servers, personal computers, and laptops.

It must be noted that computer forensics has expanded. The topic now includes cell phone forensics, router forensics, global positioning system (GPS) device forensics, tablet forensics, and forensics of many other devices. The term *digital forensics* is a more encompassing term that includes all of these devices. Regardless of the term you use, the goal is the same: to apply solid scientific methodologies to a device in order to extract evidence for use in a court proceeding.

Although the subject of computer forensics, as well as the tools and techniques used, is significantly different from traditional forensics—like DNA analysis and bullet examination—the goal is the same: to obtain evidence that can be used in some legal proceeding. Computer forensics applies to all the domains of a typical IT infrastructure, from the User Domain and Remote Access Domain to the Wide Area Network (WAN) Domain and Internet Domain (see **FIGURE 1-1**).

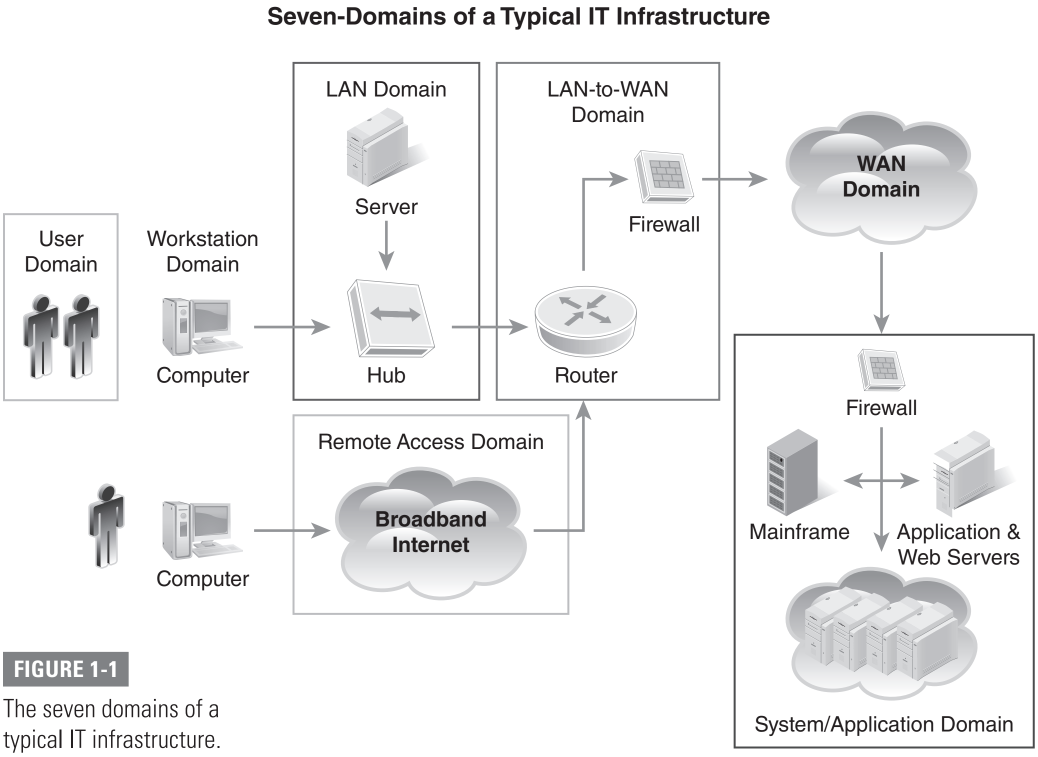


FIGURE 1-1

The seven domains of a typical IT infrastructure.

Consider some elements of the preceding definitions. In particular, let's look at this sentence: "Forensics is the process of using scientific knowledge for collecting, analyzing, and presenting evidence to the courts." Each portion of this is critical, and the following sections of this chapter examine each one individually.

Using Scientific Knowledge

First and foremost, computer forensics is a science. This is not a process based on your "gut feelings" or personal whim. It is important to understand and apply scientific methods and processes. It is also important that you have knowledge of the relevant scientific disciplines. That also means you must have scientific knowledge of the field. Computer forensics begins with a thorough understanding of computer hardware. Then you need to understand the operating system running on that device; even smartphones and routers have operating systems. You must also understand at least the basics of computer networks.

If you attempt to master forensics without this basic knowledge, you are not likely to be successful. Now if you find yourself starting in on a course and are not sure if you have the requisite knowledge, don't panic. First, you simply need a basic knowledge of computers and computer networks. If you have taken a couple of basic computer courses at a college or perhaps the CompTIA A+ certification, you have the baseline knowledge. Also, you will get a review of some basic concepts in this chapter.

However, the more you know about computers and networks, the better you will be at computer forensics. There is no such thing as "knowing too much." Even though some technical details change quickly, such as the capacity and materials of hard disks, other details change very slowly, if at all, such as the various file systems, the role of volatile and nonvolatile memory, and the fact that criminals take advantage of the advancements in computer and digital technology to improve their lives as much as the businessman, student, or homeowner. A great deal of information is stored in computers. Keep learning what is there, where it is stored, and how that information may be used by computer user and computer criminal alike.

Collecting

Before you can do any forensic analysis or examination, you have to collect the evidence. There are very specific procedures for properly collecting evidence. You will be introduced to some general guidelines later in this chapter. The important thing to realize for now is that how you collect the evidence determines if that evidence is admissible in a court.

Analyzing

This is one of the most time-consuming parts of a forensic investigation, and it can be the most challenging. Once you have collected the data, what does it mean? The real difference between a mediocre investigator and a star investigator is the analysis. The data is there, but do you know what it means? This is also related to your level of scientific knowledge. If you don't know enough, you may not see the significance of the data you have.

You also have to be able to solve puzzles. That is, in essence, what any forensic investigation is. It is solving a complex puzzle—putting together the data you have and finding out what sort of picture is revealed. You might try to approach a forensic investigation like Sherlock Holmes. Look at every detail. What does it mean? Before you jump to a conclusion, how much evidence do you have to support that conclusion? Are there alternatives and, in fact, better explanations for the data?

Presenting

Once you have finished your investigation, done your analysis, and obeyed all the rules and guidelines, you still have one more step. You will have to present that evidence in one form or another. The two most basic forms are the expert report and expert testimony. In either case, it will be your job to interpret the arcane and seemingly impenetrable technical information using plain English that paints an accurate picture for the court. You must not use jargon and technobabble. Your clear use of language, and potentially graphics and demonstrations, if needed, may be the difference between a big win and a lost case. So you should take a quick look at each of these.

⚠ **WARNING**

Court procedures vary from jurisdiction to jurisdiction, but in most cases an expert cannot directly testify about anything not in his or her expert report. That is why it is critical to be thorough and to put into the report anything you feel might be pertinent to the case. In your work as an expert witness, you will often find additional items in an investigation—items that are peripheral to the main case. If you put those in your report, however, you will be able to testify about them at trial.

The Expert Report

An **expert report** is a formal document that lists what tests you conducted, what you found, and your conclusions. It also includes your **curriculum vitae (CV)**, which is like a résumé, only much more thorough and specific to your work experience as a forensic investigator. Specific rules will vary from court to court, but as a general rule, if you don't put it in your report, you cannot testify about it at trial. So you need to make very certain that your report is thorough. Put in every single test you used, every single thing you found, and your conclusions. Expert reports tend to be rather long.

It is also important to back up your conclusions. As a general rule, it's good to have at least two to three references for every conclusion. In other words, in addition to your own opinion, you want to have a few reputable references that either agree with that conclusion or provide support for how you came to that conclusion. This way, it is not just your expert opinion, but it is supported by other reputable sources. Make sure you use reputable sources; for example, CERT, the Federal Bureau of Investigation (FBI), the Secret Service, and the Cornell University Law School are all very reputable sources.

The reason for this is that in every legal case there are two sides. The opposing side will have an attorney and perhaps its own expert. The opposing attorney will want to pick apart every opinion and conclusion you have. If there is an opposing expert, he or she will be looking for alternative interpretations of the data or flaws in your method. You have to make sure you have fully supported your conclusions.

It should be noted that the length and level of detail found in reports varies. In many cases, criminal courts won't require a formal expert report, but rather a statement from the attorney as to who you are and what topics you intend to testify about. You will need to produce a report of your forensic examination. In civil court, particularly in intellectual property cases, the expert report is far more lengthy and far more detailed. In my own experience, reports of 100, 200, or more pages are common. The largest I have seen yet was over 1500 pages long.

Although not all cases will involve a full, detailed expert report, many will, particularly intellectual property cases. There are few legal guidelines on expert report writing, but a few issues have become clear in my experience.

Expert reports generally start with the expert's qualifications. This should be a complete curriculum vitae detailing education, work history, and publications. Particular attention should be paid to elements of the expert's history that are directly related to the case at hand. Then the report moves on to the actual topic at hand. An expert report is a very thorough document. It must first detail exactly what analysis was used. How did the expert conduct his or her examination and analysis? In the case of computer forensics, the expert report should detail what tools the expert used, what the results were, and the conditions of the tests conducted. Also, any claim an expert makes in a report should be supported by extrinsic reputable sources. This is sometimes overlooked by experts because they themselves are sources who are used, or because the claim being made seems obvious to them. For example, if an expert report needs to detail how domain name service (DNS) works in order to describe a DNS poisoning attack, then there should be references to recognized authoritative works regarding the details of domain name service. If they are not included, at trial a creative attorney can often extract nontraditional meanings from even commonly understood terms.

The next issue with an expert report is its completeness. The report must cover every item the expert wishes to opine on, and in detail. Nothing can be assumed. In some jurisdictions, if an item is not in the expert report, then the expert is not allowed to discuss it during testimony. Whether or not that is the case in your jurisdiction, it is imperative that the expert report you submit is very thorough and complete. And of course, it must be error-free. Even the smallest error can give opposing counsel an opportunity to impugn the accuracy of the entire report and the expert's entire testimony. This is a document that should be carefully proofread by the expert and by the attorney retaining the expert.

Expert Testimony

As a forensic specialist, you will testify as an expert witness, that is, on the basis of scientific or technical knowledge you have that is relevant to a case, rather than on the basis of direct personal experience. Your testimony will be referred to as **expert testimony**, and there are two scenarios in which you give it: a deposition and a trial. A *deposition*—testimony taken from a witness or party to a case before a trial—is less formal, and is typically held in an attorney's office. The other side's lawyer gets to ask you questions. In fact, the lawyer can even ask some questions that would probably be disallowed by a trial judge. But do remember, this is still sworn testimony, and lying under oath is perjury, which is a felony.

U.S. Federal Rule 702, Testimony by Expert Witnesses, defines what an expert is and what expert testimony is:

> A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:
>
> a. the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
> b. the testimony is based on sufficient facts or data;
> c. the testimony is the product of reliable principles and methods; and
> d. the expert has reliably applied the principles and methods to the facts of the case.[1]

This definition is very helpful. Regardless of your credentials, did you base your conclusions on sufficient facts and data? Did you apply reliable scientific principles and methods in forming your conclusions? These questions should guide your forensic work.

During a deposition, the opposing counsel has a few goals. The first goal is to find out as much as possible about your position, methods, conclusions, and even your side's legal strategy. It is important to answer honestly but as briefly as possible. Don't volunteer information unasked. That simply allows the other side to be better prepared for trial. The second thing a lawyer is looking for during a deposition is to get you to commit to a position you may not be able to defend later. So follow a few rules:

- If you don't fully understand the question, say so. Ask for clarification before you answer.
- If you really don't know, say so. Do not ever guess.
- If you are not 100 percent certain of an answer, say so. Say "to the best of my current recollection" or something to that effect.

The other way you may testify is at trial. The first thing you absolutely must understand is that the first time you testify, you will be nervous. You'll begin to wonder if you are properly prepared. Are your conclusions correct? Did you miss anything? Don't worry; each time you do this, it gets easier. Next, remember that the opposing counsel, by definition, disagrees with you and wants to trip you up. It might be helpful to remind yourself, "The opposing counsel's default position is that I am both incompetent and a liar." Now

[1] https://www.law.cornell.edu/rules/fre/rule_702

that is a bit harsh, and probably an overstatement, but if you start from that premise you will be prepared for the opposing counsel's questions. Don't be too upset if he or she is trying to make you look bad. It is not personal.

The secret to deposition and trial testimony is simple: Be prepared. You should not only make certain your forensic process is done correctly and well documented, including liberal use of charts, diagrams, and other graphics, but also prepare before you testify. Go over your report and your notes again. Often, your attorney will prep you, particularly if you have never testified before. Try to look objectively at your own report to see if there is anything the opposing counsel might use against you. Are there alternative ways to interpret the evidence? If so, why did you reject them?

The most important things on the stand are to keep calm and tell the truth. Obviously, any lie, even a very minor one that is not directly related to your investigation, would be devastating. But becoming agitated or angry on the stand can also undermine your credibility.

In addition to U.S. Federal Rule 702, there are several other U.S. Federal Rules related to expert witness testimony at trial. They are listed and very briefly described here:

- *Rule 703, Admissibility of Facts:* An expert may base an opinion on facts or data that the expert has been made aware of or personally observed. If experts in the particular field would reasonably rely on those kinds of facts or data in forming an opinion on the subject, they need not be admissible for the opinion to be admitted. But if the facts or data would otherwise be inadmissible, the proponent of the opinion may disclose them to the jury only if their probative value in helping the jury evaluate the opinion substantially outweighs their prejudicial effect.
- *Rule 704, Opinion on Ultimate Issue:* An opinion is not objectionable just because it embraces an ultimate issue. In other words, an expert witness can, in many cases, offer an opinion as to the ultimate issue in a case.
- *Rule 705, Disclosing Underlying Facts for Opinion:* Unless the court orders otherwise, an expert may state an opinion—and give the reasons for it—without first testifying to the underlying facts or data. But the expert may be required to disclose those facts or data on cross-examination. Essentially, the expert can state his or her opinion without first giving the underlying facts, but should expect to be questioned on those facts at some point.
- *Rule 706, Court-Appointed Expert:* This rule covers the appointment of a neutral expert to advise the court. Such experts are not working for the plaintiff or the defendant, but rather for the court.
- *Rule 401, Relevance of Evidence:* Evidence is relevant if: (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action.

Understanding the Field of Digital Forensics

The field of digital forensics is changing very rapidly. First and foremost, standards are emerging. This means there are clearly defined ways of properly doing forensics. When computer forensics first began, most investigations were conducted according to the whim of the investigator rather than through a standardized methodology. But as the field has matured, it has also standardized. Today, there are clear, codified methods for conducting a forensic examination.

Another change is in who is doing forensics. At one time, all forensics, including computer forensics, was the exclusive domain of law enforcement. That is no longer the case. Today, the following entities are also involved in and actively using computer forensics:

- *The military:* The military uses digital forensics to gather intelligence information from computers captured during military actions.
- *Government agencies:* Government agencies use digital forensics to investigate crimes involving computers. These agencies include the FBI, U.S. Postal Inspection Service, Federal Trade Commission, U.S. Food and Drug Administration, and U.S. Secret Service. They also include the U.S. Department of Justice's National Institute of Justice (NIJ), the National Institute of Standards and Technology (NIST), the Office of Law Enforcement Standards (OLES), the Department of Homeland Security, and foreign government agencies, among others.
- *Law firms:* Law firms need experienced system forensics professionals to conduct investigations and testify as expert witnesses. For example, civil cases can use records found on computer systems that bear on cases involving fraud, divorce, discrimination, and harassment.
- *Criminal prosecutors:* Criminal prosecutors use digital evidence when working with incriminating documents. They try to link these documents to crimes such as drug trafficking, embezzlement, financial fraud, homicide, and child pornography.
- *Academia:* Academia is involved with forensic research and education. For example, many universities offer degrees in digital forensics and online criminal justice.
- *Data recovery firms:* Data recovery firms use digital forensics techniques to recover data after hardware or software failures and when data has been lost.
- *Corporations:* Corporations use digital forensics to assist in employee termination and prosecution. For example, corporations sometimes need to gather information concerning theft of intellectual property or trade secrets, fraud, embezzlement, sexual harassment, and network and computer intrusions. They also need to find evidence of unauthorized use of equipment, such as computers, fax machines, answering machines, voicemail systems, smartphones, and tablets.
- *Insurance companies:* Insurance companies use digital evidence of possible fraud in accident, arson, and workers' compensation cases.
- *Individuals:* Individuals sometimes hire forensic specialists in support of possible claims. These cases may include, for example, wrongful termination, sexual harassment, or age discrimination.

What Is Digital Evidence?

Information includes raw numbers, pictures, and a vast array of other data that may or may not have relevance to a particular event or incident under investigation. **Digital evidence** is information that has been processed and assembled so that it is relevant to an investigation and supports a specific finding or determination. Put another way, all the raw information is not, in and of itself, evidence. First and foremost, data has to be relevant to a case in order to be evidence.

Investigators must carefully show an unbroken chain of custody to demonstrate that evidence has been protected from tampering. The **chain of custody** is the continuity of control of evidence that makes it possible to account for all that has happened to evidence between its original collection and its appearance in court, preferably unaltered. If forensic specialists can't demonstrate that they have maintained the chain of custody, then the court may consider all their conclusions invalid.

Courts deal with four types of evidence:

- *Real:* **Real evidence** is a physical object that someone can touch, hold, or directly observe. Examples of real evidence are a laptop with a suspect's fingerprints on the keyboard, a hard drive, a universal serial bus (USB) drive, or a handwritten note.
- *Documentary:* **Documentary evidence** is data stored as written matter, on paper or in electronic files. Documentary evidence includes memory-resident data and computer files. Examples are email messages, logs, databases, photographs, and telephone call-detail records. Investigators must authenticate documentary evidence.
- *Testimonial:* **Testimonial evidence** is information that forensic specialists use to support or interpret real or documentary evidence. For example, they may employ testimonial evidence to demonstrate that the fingerprints found on a keyboard are those of a specific individual. Or system access controls might show that a particular user stored specific photographs on a desktop.
- *Demonstrative:* **Demonstrative evidence** is information that helps explain other evidence. An example is a chart that explains a technical concept to the judge and jury. Forensic specialists must often provide testimony to support the conclusions of their analyses. For example, a member of an incident response team might be required to testify that he or she identified the computer program that deleted customer records at a specified date and time. In such a case, the testimony must show how the investigator reached his or her conclusion. The testimony must also show that the specialist protected the information used in making the determination from tampering; that is, the testimony must show that the forensic investigator maintained the chain of custody. It must also show that the testifier based his or her conclusion on a reasonable, although not necessarily absolute, interpretation of the information. Further, the forensic specialist must present his or her testimony in a manner that avoids use of technical jargon and complex technical discussions and should use pictures, charts, and other graphics when helpful. Judges, juries, and lawyers aren't all technical experts. Therefore, a forensic specialist should translate technology into understandable descriptions. Pictures often communicate better than just numbers and words, so a forensic specialist may want to create charts and graphs.

Scope-Related Challenges to System Forensics

The scope of a forensic effort often presents not just an analytical challenge, but also a psychological challenge. Information systems collect and retain large volumes of data. They store this data in a dizzying array of applications, formats, and hardware components. In completing an analysis, forensic specialists face variations in the following:

- The volume of data to be analyzed
- The complexity of the computer system

- The size and character of the crime scene, which might involve a network that crosses U.S. and foreign jurisdictions
- The size of the caseload and resource limitations

Forensic specialists must be prepared to quickly complete an analysis regardless of these factors. The following sections discuss these factors in more detail.

Large Volumes of Data

Digital forensics is useful in identifying and documenting evidence. It is a disciplined approach that looks at the entire physical media, such as a hard disk drive, for all information representations. A system forensics specialist has access to all the information contained on a device—not just what the end user sees. A forensic analyst also examines *metadata*, which is data about information, such as disk partition structures and file tables. Metadata also includes file creation and modification times. Who authored a file and when it was revised or updated are also important pieces of metadata for a forensic analyst to document. An analyst also examines the often-critical unused areas of the media where information might be hidden. Examining all areas of potential data storage and examining all potential data representations generates extremely large volumes of information. A forensic specialist must analyze, store, and control all this information for the full duration of the investigation and analysis.

The total amount of information that is potentially relevant to a case offers a challenge to forensic analysts. Hard drives well in excess of 1 terabyte are quite common today. In fact, one can purchase a 4-terabyte drive for under $150 at any electronics store. While writing this chapter for the third edition of the book, I came across an advertisement from a popular electronics store for an 8-terabyte external drive for $230. When working with such large volumes, a forensic specialist must do the following:

- Ensure that his or her equipment is capable of manipulating large volumes of information quickly.
- Provide for duplicate storage so that the original media and its resident information are preserved and protected against tampering and other corruption.
- Create backups early and often to avoid losing actual information and its associated metadata.
- Document everything that is done in an investigation and maintain the chain of custody.

In addition to all these tasks, a forensic specialist must work within the forensic budget. Manipulating and controlling large volumes of information is expensive. An investigator should show how budget cost items contribute to the analysis and to maintaining the chain of custody. Resource limitations increase the potential for analysis error and may compromise the analysis. For example, a forensic analyst may need to explain how the addition of data custodians or additional hard drives can multiply costs.

System Complexity

Modern computer systems can be extremely complex. This is not just a matter of the aforementioned size of storage, but also the wide array of data and formats. Digital devices use multiple file formats, including Adobe Portable Document Format (PDF) files, Microsoft

Word (DOC and DOCX) documents, Microsoft Excel spreadsheets (XLS and XLSX), video files (AVI, MOV, etc.), and image files (JPEG, GIF, BMP, TIFF, etc.), to name just a few. This does not even take into account formats of information "in motion" such as Voice over IP (VoIP), instant messaging protocols, real-time video broadcasts, or two-way conferences. These systems connect to and share data with other systems that may be located anywhere in the world. In addition, the law may protect specific items and not others. No single forensic software application can deal with all the complexity.

Forensic specialists must use a set of software and hardware tools and supporting manual procedures. Further, a forensic specialist must build a case to support his or her interpretation of the "story" told by the information being analyzed. The specialist, therefore, must have an understanding of all digital information and its associated technology. The specialist should also be able to show corroboration that meets the traditional legal evidence tests. Specific tests of legal evidence can vary from venue to venue and from jurisdiction to jurisdiction. There are a few basic tests that apply everywhere, but the chain of custody and the Daubert standard, both of which are discussed in this chapter, are nearly universal.

Individual pieces of information may have more than one possible interpretation. To reach a conclusion and turn raw information into supportable, actionable evidence, a forensic specialist must identify and analyze corroborating information. In other words, it is often the case that a single piece of information is not conclusive. It often takes the examination and correlation of multiple individual pieces of information to reach a conclusion. It is also a common practice for a forensic investigator to use more than one tool to conduct a test. For example, if you utilize one particular tool to recover deleted files, it can be a good idea to use yet another tool to conduct the same test. If two different tools yield the same result, this is compelling evidence that the information gathered is accurate and reliable. However, if the results differ, the forensic analyst has another situation to deal with.

Distributed Crime Scenes

Because networks are geographically dispersed, crime scenes may also be geographically dispersed. This creates practical as well as jurisdictional problems. Think about how difficult it is for a U.S. investigator to get evidence out of computers in China, for instance. Criminals take advantage of jurisdictional differences. A criminal may sell fake merchandise via the Internet from a foreign country to Americans in several states. The criminal may then route his or her Internet access, and the associated electronic payments, through several other countries before they reach their final destination.

Digital crime scenes can, and increasingly do, span the globe. Depending on the type of system connectivity and the controls in place, a forensic specialist may have to deal with information stored throughout the world and often in languages other than English. This could involve thousands of devices and network logs. Networks and centralized storage also present challenges because items of interest may not be stored on the target computer.

Gathering evidence from such a geographically far-flung digital crime scene requires the cooperation of local, state, and tribal governments, sometimes multiple national governments, and international agencies in tracking down the criminals and bringing them to justice. If all the governments and agencies do not cooperate with one another, access to evidence is threatened or denied, and as a result, the investigation may fail.

Growing Caseload and Limited Resources

The number of forensic specialists today is too small to analyze every cybercrime. Regardless of the state of the economy, digital forensics specialists can be assured of two things: Their caseload will grow, and their resources will, relative to caseload, become more limited. It is a simple fact that anyone in law enforcement who works in digital crimes has a case backlog, and that backlog is increasing.

The digital forensics analysis workload is growing and will continue to grow as computers and related digital devices are used more and in different ways in the commission of crimes. Driving this growth is the increasing use of technology in all aspects of modern life, not just in support of business objectives. Criminals utilize technology not only to conduct crimes, but also, in some cases, to hide the evidence. Forensic tools can also be used by criminals to eradicate evidence as easily as they can be used by investigators to locate, analyze, and catalog evidence.

Types of Digital System Forensics Analysis

Today, digital system forensics includes a number of specialties. The following are some examples:

- *Disk forensics:* The process of acquiring and analyzing information stored on physical storage media, such as computer hard drives, smartphones, GPS systems, and removable media. **Disk forensics** includes both the recovery of hidden and deleted information and the process of identifying who created a file or message.
- *Email forensics:* The study of the source and content of email as evidence. **Email forensics** includes the process of identifying the sender, recipient, date, time, and origination location of an email message. You can use email forensics to identify harassment, discrimination, or unauthorized activities. There is also a body of laws that deals with retention and storage of emails that are specific to certain fields, such as financial and medical.
- *Network forensics:* The process of examining network traffic, including transaction logs and real-time monitoring using sniffers and tracing, is known as **network forensics**.
- *Internet forensics:* The process of piecing together where and when a user has been on the Internet. For example, you can use **Internet forensics** to determine whether inappropriate Internet content access and downloading were accidental.
- *Software forensics:* The process of examining malicious computer code is known as **software forensics**; it is also known as malware forensics.
- *Live system forensics:* The process of searching memory in real time, typically for working with compromised hosts or to identify system abuse, is **live system forensics**.
- *Cell-phone forensics:* The process of searching the contents of cell phones is called **cell-phone forensics**. A few years ago, this was just not a big issue, but with the ubiquitous nature of cell phones today, cell-phone forensics is a very important topic. A cell phone can be a treasure trove of evidence. Modern cell phones are essentially computers with processors, memory, even hard drives and operating systems, and they operate on networks. Phone forensics also includes VoIP and traditional phones, and it may involve the Foreign Intelligence Surveillance Act of 1978 (FISA), the USA Patriot Act, and the Communications Assistance for Law Enforcement Act (CALEA) in the United States.

Each of these types of forensic analysis requires specialized skills and training.

General Guidelines

Later in this chapter you will read about specific federal guidelines, but you should keep a few general principles in mind when doing any forensic work, as discussed in the following sections.

Chain of Custody

This is the most important principle in any forensic effort, digital or nondigital. The chain of physical custody must be maintained. From the time the evidence is first seized by a law enforcement officer or civilian investigator until the moment it is shown in court, the whereabouts and custody of the evidence, and how it was handled and stored and by whom, must be able to be shown at all times. Failure to maintain proper chain of custody can lead to evidence being excluded from trial.

Don't Touch the Suspect Drive

One very important principle is to touch the system as little as possible. It is possible to make changes to the system in the process of examining it, which is very undesirable. Obviously, you have to interact with the system to investigate it. The answer is to make a forensic copy and work with that copy. You can make a forensic copy with most major forensic tools such as AccessData's Forensic Toolkit, Guidance Software's EnCase, or PassMark's OSForensics. There are also open-source software products that allow copying of original source information. To be safe, make a copy and analyze the copy.

There are times, however, when you will need to interact directly with live evidence. For example, when a computer is first discovered, you will want to do an initial analysis to determine running processes and connections, before you make an image. You may also need to perform live forensics in certain situations, such as some cloud computing environments. We will discuss these as we encounter them in this book.

Document Trail

The next issue is documentation. The rule is that you document everything. Who was present when the device was seized? What was connected to the device or showing on the screen when you seized it? What specific tools and techniques did you use? Who had access to the evidence from the time of seizure until the time of trial? All of this must be documented. And when in doubt, err on the side of over documentation. It really is not possible to document too much information about an investigation.

Secure the Evidence

It is absolutely critical to the integrity of your investigation as well as to maintaining the chain of custody that you secure the evidence. It is common to have the forensic lab be a locked room with access given only to those who must enter. Then, evidence is usually secured in a safe, with access given out only on a need-to-know basis. You have to take every reasonable precaution to ensure that no one can tamper with the evidence.

Knowledge Needed for Computer Forensics Analysis

To conduct computer forensics, a certain background body of knowledge is required, just as with traditional forensics. For example, you cannot examine DNA without some basic education in blood and genetics. This applies to computer forensics as well. You must have an understanding of the systems you are examining in order to successfully examine them.

This chapter assumes that you have a basic understanding of computer hardware, software, and operating systems. This section briefly discusses the highlights of these areas that you need to know. If you find you are lacking in one or more areas, you should take some time to brush up on these topics before continuing. For many readers, these items will be a review; for others, some information may be new. If this is new information for you, bear in mind that this is the absolute minimum of knowledge. The more you know about the underlying technology, the more effective you will be.

Hardware

In general, the good digital forensics examiners begin with a working knowledge of the hardware for the devices they want to examine. For PCs and laptops, this includes knowledge equivalent to the CompTIA A+ certification or a basic PC hardware course. If you are doing phone or router forensics, you need a similar level of knowledge of the hardware on those devices.

For PCs, this means a strong understanding of hard drives, memory, motherboards, and expansion cards. What exactly is a “strong understanding”? Think about random access memory (RAM). You are probably aware that RAM is **volatile memory** and it stores the programs and data you currently have open, but only for as long as the computer has power supplied to it. However, that level of knowledge is inadequate for forensics. A forensic examiner needs to go much deeper and understand the various types of RAM, how they work, the type of information that is contained in each, and how the computer uses them.

Random Access Memory

RAM can be examined in multiple ways. One way is to look at the method whereby information is written to and read from RAM. These are presented in sequential order from older to newer technologies:

- *Extended data output dynamic random access memory (EDO DRAM):* Single-cycle EDO has the ability to carry out a complete memory transaction in one clock cycle. Otherwise, each sequential RAM access within the same page takes two clock cycles instead of three, once the page has been selected.
- *Burst EDO (BEDO) DRAM:* An evolution of the EDO, burst EDO DRAM can process four memory addresses in one burst.
- *Asynchronous dynamic random access memory (ADRAM):* ADRAM is not synchronized to the CPU clock.
- *Synchronous dynamic random access memory (SDRAM):* SDRAM is a replacement for EDO.
- *Double data rate (DDR) SDRAM:* DDR SDRAM was a later development of SDRAM. DDR2, DDR3, and DDR4 are now available.

SDRAM and, more specifically, DDR3 and DDR4, are the most common forms of RAM found in PCs and laptops.

Another way to look at RAM, one that is particularly important from a forensic point of view, is to consider the volatility of the data stored. Volatility refers to how easily the data can be changed, either intentionally or unintentionally.

- *Random access memory (RAM):* This is what most people think of when they say *memory*. It is quick to write to and read from. The memory is volatile, meaning as soon as power is discontinued, the data is gone.
- *Read-only memory (ROM):* As the name suggests, this is not at all volatile; it cannot be changed. This is usually used for instructions embedded in chips and controls how the computer, option cards, peripherals, and other devices operate.
- *Programmable ROM (PROM):* PROM can be programmed only once. Data is not lost when power is removed.
- *Erasable programmable ROM (EPROM):* Data is not lost when power is removed. Again, this is a technique for storing instructions on chips.
- *Electronically erasable programmable ROM (EEPROM):* This is how the instructions in your computer's BIOS are stored.

Hard Drives

A forensic specialist must also understand the following storage devices. The descriptions given here are for various types of connectors. The drives themselves are the same, but the method of attaching the drive, as well as the speed and efficiency of getting data to and from the drive, differ.

- *Small Computer System Interface (SCSI):* This has been around for many years, and is particularly popular in high-end servers. This standard is actually fairly old—it was established in 1986. SCSI devices must have a terminator at the end of the chain of devices to work and are limited to 16 chained devices.
- *Integrated Drive Electronics (IDE):* This is an older standard but one that was commonly used on PCs for many years. It is obvious you are dealing with an IDE or EIDE drive if you encounter a 40-pin connector on the drive.
- *Enhanced Integrated Drive Electronics (EIDE):* This is an extension/enhancement of IDE.
- *Parallel Advanced Technology Attachment (PATA):* Parallel ATA is an enhancement of IDE. It uses either a 40-pin (like IDE) or 80-pin connector.
- *Serial Advanced Technology Attachment (SATA):* This is what you are most likely to find today. These devices are commonly found in workstations and many servers. The internals of the hard drive are very similar to IDE and EIDE; it is the connectivity to the computer's motherboard that is different. Also, unlike IDE or EIDE drives, this type of drive has no jumpers to set the drive.
- *Serial SCSI:* This is an enhancement of SCSI. It supports up to 65,537 devices and does not require termination.
- *Solid-state drives (SSDs):* These are becoming more common, so it's worthwhile to discuss them in a bit more detail. Unlike the previously discussed drive types, these are not the same basic hard drive. These drives have an entirely different construction and method of

storing data. SSDs use microchips that retain data in nonvolatile memory chips and contain no moving parts. As of 2010, most SSDs use negated AND gate (NAND)-based flash memory, which retains memory even without power. Solid-state drives do not benefit from defragmentation. Any defragmentation process adds additional writes on the NAND flash, which already has a limited life cycle. High-performance flash-based SSDs generally require one-half to one-third the power of hard disk drives (HDDs); high-performance DRAM SSDs generally require as much power as HDDs, and consume power when the rest of the system is shut down.

All of these, except for solid state, refer to how the hard drive connects to the motherboard and transfers data, and do not define how information is stored on the disk. For all but solid state, the following hard drive facts apply.

HDDs record data by magnetizing ferromagnetic material directionally, to represent either a 0 or a 1 binary digit. The magnetic data is stored on platters; the platters are organized on a spindle with a read/write head reading and writing data to and from the platters. The data is organized as follows:

- A *sector* is the basic unit of data storage on a hard disk, which is usually 512 bytes. However, newer systems often use a 4096-byte sector size.
- A cluster is a logical grouping of sectors. Clusters can be 1 to 128 sectors in size. That means 512 bytes up to 64 kilobytes (KB). The minimum size a file can use is one cluster. If the file is less than the size of a cluster, the remaining space is simply unused.
- Sectors are, in turn, organized by tracks.

That is a basic description of most hard drives (with the exception of solid-state drives). Forensic examiners should know the following terms, which are used with all hard drives:

- *Drive geometry:* This term refers to the functional dimensions of a drive in terms of the number of heads, cylinders, and sectors per track.
- *Slack space:* This is the space between the end of a file and the end of the cluster, assuming the file does not occupy the entire cluster. This is space that can be used to hide data.
- *Low-level format:* This creates a structure of sectors, tracks, and clusters.
- *High-level format:* This is the process of setting up an empty file system on the disk and installing a boot sector. This is sometimes referred to as a quick format.

Software

Once you have a basic understanding of hardware, the next step is to learn about the software, and this begins with the operating system. It is imperative that you have a strong working knowledge of the operating system running on the device you want to examine.

Windows

There's a lot to know about Windows, but for now, here's a basic overview of how it works. The heart of Windows is the Windows Registry. The Windows Registry is essentially a repository of all settings, software, and parameters for Windows. If new software is installed, the Registry is updated to indicate the new software. If the background color of the desktop is changed, the Registry is updated to indicate the new color. From this Registry, you can get all kinds of information, including the password for wireless networks and the serial numbers for all USB devices that have been connected to that computer. This is really the most important part of Windows from both a technical-support and a forensic point of view.

Windows also has other interesting places to look for forensic evidence. There are certain folders and files—the index.dat file, for instance—that are great places to find evidence. Even browser cookies and history can be useful. Given that Windows is such a common operating system, it is advisable to be very familiar with Windows.

Linux

Linux is particularly interesting from a forensic point of view. Even though it is not as widely used as Windows, it is a favorite in the security and forensics community. You will find that a lot of free forensic tools come with Linux. In fact, one specific Linux distribution called Kali Linux (formerly called BackTrack) has an extensive collection of forensic, security, and hacking tools.

Linux is a UNIX clone, developed originally by Linus Torvalds. There are now well over 100 different distributions, or variations, of Linux. However, all have some commonalities. In the Linux world, work done from the command line, called the shell in Linux, is far more important than it is in Windows.

Macintosh

For many years, Apple Macintosh was a complete operating system. However, beginning with OS X, the Macintosh system has been based on FreeBSD, a UNIX clone very similar to Linux. The graphical user interface is just that, an interface. The underlying operating system is a UNIX-like system.

This means that many forensic techniques you can use on Linux can also be used on Macintosh, from the shell prompt.

Files and File Systems

Computers store discrete sets of related information in files. Any document, spreadsheet, picture, video, or even program is a file. It is a very easy thing to change the extension of a file so that it looks like some other type of file. However, that will not change the file structure itself. There are tools that allow viewing of the actual file structure and the file header. This is very important from a forensic perspective. The file header gives you an accurate understanding of the file, regardless of whether the extension has been changed. A few basic facts about files are as follows:

- File headers start at the first byte of a file. This is particularly important when you practice file carving.
- In graphics file formats, the header might give information about an image's size, resolution, number of colors, and the like.
- The Executable and Linkable Format (ELF, formerly called Extensible Linking Format) is a common standard file format for executables, object code, and shared libraries for UNIX-based systems.

- Portable Executable (PE) is used in Windows for executables and dynamic-link libraries (DLLs). PE files are derived from the earlier Common Object File Format (COFF) found on VAX/VMS, a common operating system for mainframe computers.
- Area density is the data per area of disk.
- Windows Office files have a globally unique identifier (GUID) to identify them.

Files are organized on the computer based on the file system. There are many file systems, but they can be divided into two categories. Journaling is basically the process whereby the file system keeps a record of what file transactions take place so that in the event of a hard drive crash, the files can be recovered. Journaling file systems are fault tolerant because the file system logs all changes to files, directories, or file structures. The log in which changes are recorded is referred to as the file systems journal—thus the term *journaling* file systems.

There are actually two types of journaling: physical and logical. With physical journaling, the system logs a copy of every block that is about to be written to the storage device, before it is written. The log also includes a checksum of those blocks, to make sure there is no error in writing the block. With logical journaling, only changes to file metadata are stored in the journal.

Here are some specific file systems:

- *File Allocation Table (FAT):* This is an older system, which was popular with Microsoft operating systems for many years. FAT was first implemented in Microsoft Standalone Disk BASIC. FAT stores file locations by sector in a file called the file allocation table. This table contains information about which clusters are being used by which particular files and which clusters are free to be used. The various extensions of FAT, such as FAT16 and FAT32, differ in the number of bits available for filenames.
- *New Technology File System (NTFS):* Microsoft eventually introduced a new file system to replace FAT. This file system is called New Technology File System (NTFS). This is the file system used by Windows NT 4 through Windows 10 as well as Server 2000 through Server 2016. One major improvement of NTFS over FAT was the increased volume sizes NTFS could support. The maximum NTFS volume size is 2^{64}–1 clusters. We will be discussing NTFS in more detail when we discuss Windows forensics, later in this book.
- *Extended file system:* This was the first file system created specifically for Linux. There have been many versions of EXT; the current version is 4. The EXT4 file system can support volumes with sizes up to 1 exabyte (10^{18} bytes, or 1 billion gigabytes) and files with sizes up to 16 terabytes. This is a huge file and volume size, and no current hard drives come even close to that volume size. For an administrator, one of the most exciting features of EXT4 is that it is backward compatible with EXT2 and EXT3, making it possible to mount drives that use those earlier versions of EXT.
- *ReiserFS:* This is a popular journaling file system, used primarily with Linux. ReiserFS was the first file system to be included with the standard Linux kernel, and first appeared in kernel version 2.4.1. Unlike some file systems, ReiserFS supported journaling from its inception, whereas EXT did not support journaling until version 3. ReiserFS is open source and was invented by Hans Reiser.

- *The Berkeley Fast File System:* This is also known as the UNIX file system. As its names suggest, it was developed at the University of California specifically for UNIX. Like many file systems, Berkeley uses a bitmap to track free clusters, indicating which clusters are available and which are not. Like EXT, Berkeley includes the FSCK utility. This is only one of many similarities between Berkeley and EXT. In fact, some sources consider EXT to just be a variant of the Berkeley Fast File System.

Networks

Digital forensics, like all branches of cybersecurity, breaks information into two types. There is information at rest and information in motion. Information at rest includes anything that is stored inside the computer, including in the file system or memory. Information in motion is information being transmitted between endpoints and includes the protocols and other information needed for transmission. The transmission of information across networks and the network components used are a vast, quickly changing field. The modern forensic investigator, however, should be very familiar with the components and how they work as well as the protocols and their operation if information in motion is to be considered as a part of the investigator's skill set. The modern forensic analyst who will consider information in motion must also be very familiar with the concepts and operation of both the seven-layer Open Systems Interconnection (OSI) Reference Model and the five-layer Internet Engineering Task Force (IETF) model. If you lack this knowledge, you must acquire it before proceeding any further.

Addresses

The digital forensics analyst must be aware of the way in which computer information is addressed and the proper vocabulary for discussing the different types of addresses and units of information transfer. It is also important for the digital forensics analyst to understand that not all addresses are a part of every communication. If they are present, the addresses are part of a hierarchy and are placed, one within the other, like envelopes.

Physical Ports

Physical ports are physical. You can touch them. Even a wireless physical port can be touched, although you must open the computer or other device to find the antenna first. The physical ports operate at OSI Layer 1, the Physical Layer. The units of information transfer are 1 and 0 bits grouped into fixed-length units called Layer 1 frames.

MAC Addresses

A MAC (Media Access Control) address is a 6-byte (or 48-bit) address used to identify a network interface card. The first three bytes identify the vendor; the second three identify the specific card. This can also be referred to as a computer's physical address.

A MAC address is supposed to be unique, is supposed to be tied to one and only one physical port, and is not supposed to be duplicated or reused for any reason. However, this is not always the case. Duplication of MAC addresses can occur due to bad quality control or can be done intentionally for a variety of malicious reasons. The keen forensic investigator will never be fooled by duplicate MAC addresses.

IP Addresses

Internet Protocol (IP) addresses, sometimes called logical addresses, are assigned to a computer and can be easily changed. Although IP version 6 has been available for quite some time, a majority of computers are still using IP version 4, which provides a 32-bit address. We will discuss IP version 4 and version 6 in more detail later in this book when we discuss network forensics.

Logical Port Numbers

Communication over a network depends on an IP address and a port number. You can think of the port as a channel. Here is a list of some common ports and their uses:

- *20 and 21, File Transfer Protocol (FTP):* For transferring files between computers. Port 20 is for data; port 21 is for control.
- *22, SSH (Secure Shell) and Secure FTP:* Used as secure alternates to Telnet and FTP, respectively.
- *23, Telnet:* Used to remotely log on to a system. You can then use a command prompt or shell to execute commands on that system. Popular with network administrators.
- *25, Simple Mail Transfer Protocol (SMTP):* Used to send email.
- *43, WhoIS:* A command that queries a target IP address for information.
- *53, Domain Name Service (DNS):* Translates uniform resource locators (URLs) into web addresses.
- *69, Trivial FTP (TFTP):* A barebones, unauthenticated version of FTP.
- *80, Hypertext Transfer Protocol (HTTP):* Displays webpages.
- *88, Kerberos authentication*
- *109, Post Office Protocol version 2 (POP 2):* An outdated mail protocol.
- *110, POP3:* Retrieves email.
- *137, 138, and 139, NetBIOS*
- *161 and 162, Simple Network Management Protocol (SNMP):* Used to monitor the health of network devices.
- *179, Border Gateway Protocol (BGP):* The main routing protocol for the public Internet.
- *194, Internet Relay Chat (IRC):* Chat rooms.
- *220, Internet Message Access Protocol (IMAP):* The most popular email protocol. Also can use port 143.
- *389, Lightweight Directory Access Protocol (LDAP):* How directories, the phonebooks of networks, connect and communicate.
- *443, Hypertext Transfer Protocol Secure (HTTPS):* A secure version of the web browsing protocol HTTP.
- *445: Active Directory, SMB*
- *464, Kerberos:* Used to change passwords.
- *465: SMTP over Secure Sockets Layer (SSL)*

Uniform Resource Locators (URLs)

As the Internet grew and the number of servers and their IP addresses grew, the Domain Name System (DNS) was created to allow Internet users to type a name instead of an IP address. This level of simplification is great, but it introduces a number of potential forensic issues, including changing the mapping of a website name to an IP address permanently or temporarily, and many different forms of this can be used to redirect browsers incorrectly and befuddle forensic efforts.

Addressing Review

In a complete, end-to-end Internet communication, it is most common that user information, such as email text, would be formatted as specified by the email protocol. A URL would then be used to find the actual IP address of the recipient. The message would be formatted per the Transmission Control Protocol (TCP) and sent with the proper TCP port number set to the IP addresses. The IP packet containing all of this would be put into a special envelope built per the protocol rules of Ethernet, which would make its way onto the actual wire, or go across the wireless or optical connection on its way through the cloud to its destination. At the destination, the process would be done in reverse and the email, or at least a part of it, would have gotten through to its destination.

Basic Network Utilities

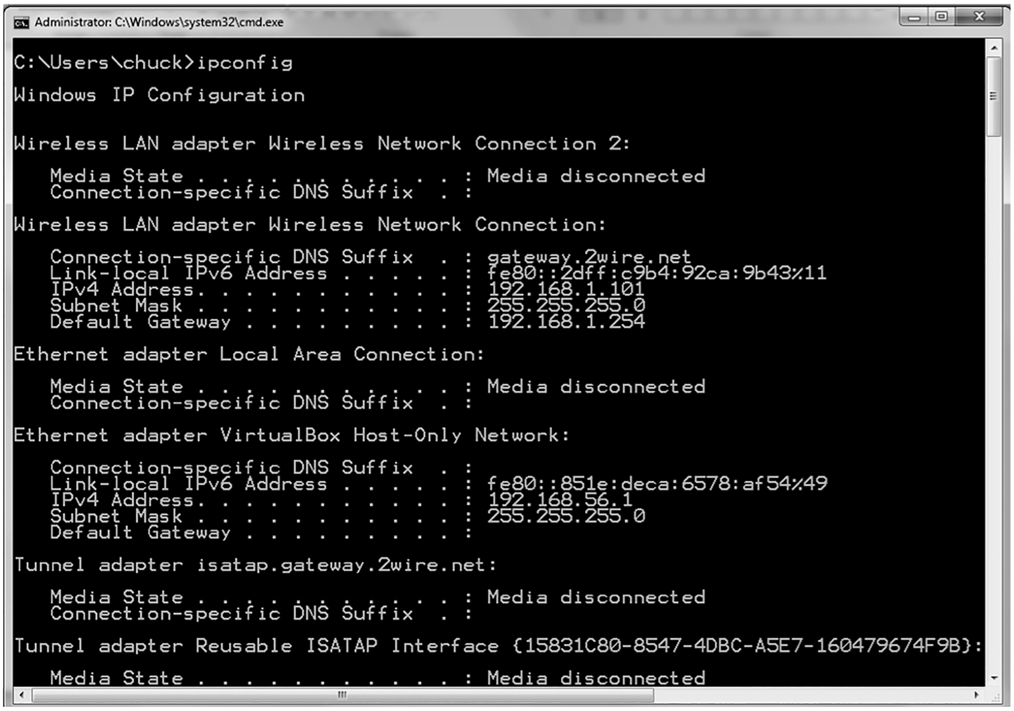
You can execute some basic network utilities from a command prompt (Windows) or from a shell (UNIX/Linux). This text's discussion executes the commands and discusses them from the Windows command-prompt perspective; however, it must be stressed that these utilities are available in all operating systems. This section covers the `ipconfig`, `ping`, and `tracert` utilities.

Working with `ipconfig`

The first thing you need to do is to get information about your own system. To accomplish this fact-finding mission, you need to get to a command prompt. In Windows XP, you do this by going to the Start menu and then selecting All Programs > Accessories > Command Prompt. For other versions of Windows, the process is identical, except the first option is called simply Programs rather than All Programs. Now you can type in `ipconfig`. You could input the same command in UNIX or Linux by typing in `ifconfig` from the shell. After typing in `ipconfig`–`ifconfig` in Linux—you should see something similar to what is shown in **FIGURE 1-2**.

This command gives you some information about your connection to a network or to the Internet. Most important, you find out your own IP address. The command also has the IP address for your default gateway, which is your connection to the outside world. Running the `ipconfig` command is a first step in determining your system's network configuration.

You can see that this option gives you much more information. For example, `ipconfig/all` gives the name of your computer, when your computer obtained its IP address, and more.



```
C:\Users\chuck>ipconfig

Windows IP Configuration


Wireless LAN adapter Wireless Network Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : gateway.2wire.net
   Link-local IPv6 Address . . . . . : fe80::2dff:c9b4:92ca:9b43%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.254

Ethernet adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::851e:deca:6578:af54%49
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.gateway.2wire.net:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Reusable ISATAP Interface {15831C80-8547-4DBC-A5E7-160479674F9B}:

   Media State . . . . . . . . . . . : Media disconnected
```

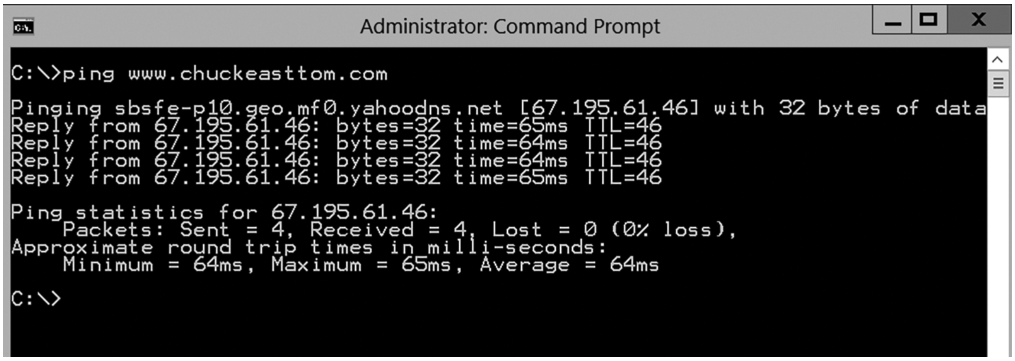
FIGURE 1-2 `ipconfig`.

Used with permission from Microsoft.

Using `ping`

Another commonly used command is `ping`, which is used to send a test packet, or echo packet, to a machine to find out if the machine is reachable and how long the packet takes to reach the machine. This useful diagnostic tool can be employed in elementary hacking techniques. The command is shown in **FIGURE 1-3**.

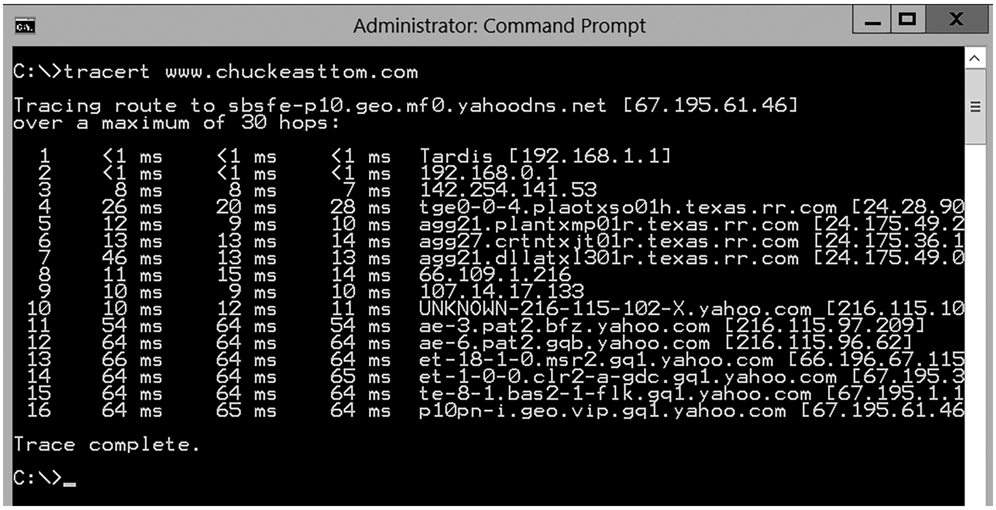
You can see in Figure 1-3 that a 32-byte echo packet was sent to the destination and returned. The TTL item means *time to live*. That time unit is how many intermediary steps, or hops, the packet should take to the destination before giving up. Remember that the Internet



```
C:\>ping www.chuckeasttom.com

Pinging sbsfe-p10.geo.mf0.yahoodns.net [67.195.61.46] with 32 bytes of data
Reply from 67.195.61.46: bytes=32 time=65ms TTL=46
Reply from 67.195.61.46: bytes=32 time=64ms TTL=46
Reply from 67.195.61.46: bytes=32 time=64ms TTL=46
Reply from 67.195.61.46: bytes=32 time=65ms TTL=46

Ping statistics for 67.195.61.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 64ms, Maximum = 65ms, Average = 64ms

C:\>
```

FIGURE 1-3 `ping`.

Used with permission from Microsoft.



```
C:\>tracert www.chuckeasttom.com

Tracing route to sbsfe-p10.geo.mf0.yahoodns.net [67.195.61.46]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  Tardis [192.168.1.1]
  2    <1 ms    <1 ms    <1 ms  192.168.0.1
  3     8 ms     8 ms     7 ms  142.254.141.53
  4    26 ms    20 ms    28 ms  tge0-0-4.plaotxso01h.texas.rr.com [24.28.90
  5    12 ms     9 ms    10 ms  agg21.plantxmp01r.texas.rr.com [24.175.49.2
  6    13 ms    13 ms    14 ms  agg27.crtntxjt01r.texas.rr.com [24.175.36.1
  7    46 ms    13 ms    13 ms  agg21.dllatxl301r.texas.rr.com [24.175.49.0
  8    11 ms    15 ms    14 ms  66.109.1.216
  9    10 ms     9 ms    10 ms  107.14.17.133
 10    10 ms    12 ms    11 ms  UNKNOWN-216-115-102-X.yahoo.com [216.115.10
 11    54 ms    64 ms    54 ms  ae-3.pat2.bfz.yahoo.com [216.115.97.209]
 12    64 ms    64 ms    64 ms  ae-6.pat2.gqb.yahoo.com [216.115.96.62]
 13    66 ms    64 ms    64 ms  et-18-1-0.msr2.gq1.yahoo.com [66.196.67.115
 14    64 ms    64 ms    65 ms  et-1-0-0.clr2-a-gdc.gq1.yahoo.com [67.195.3
 15    64 ms    64 ms    64 ms  te-8-1.bas2-1-flk.gq1.yahoo.com [67.195.1.1
 16    64 ms    65 ms    64 ms  p10pn-i.geo.vip.gq1.yahoo.com [67.195.61.46

Trace complete.

C:\>_
```

Used with permission from Microsoft.

FIGURE 1-4 `tracert`.

is a vast conglomerate of interconnected networks. Your packet probably won't go straight to its destination. It will have to take several hops to get there. As with `ipconfig`, you can type in `ping -?` to find out various ways you can refine your `ping`.

Working with `tracert`

The final command this section examines is the `tracert` command. You can see this command in **FIGURE 1-4**. Although `tracert` can be useful for some live network troubleshooting, the information reported by `tracert` is not useful or trustworthy for forensic examination. This same command can be executed in Linux or UNIX, but there it is called `traceroute` rather than `tracert`.

This section is just a brief overview of the hardware, software, and networking knowledge you should have in order to study forensics. If you find you are lacking in one or more areas, do some review in those areas before you proceed.

Obscured Information and Anti-Forensics

Two more challenges in obtaining digital evidence are obscured information and anti-forensics.

Obscured Information

Information can be obscured in a number of ways. *Obscured information* may be scrambled by encryption, hidden using steganographic software, compressed, or a proprietary format. Sometimes, cybercriminals obscure information to deter forensic examination. More often, companies use certain manipulation and storage techniques to protect business-sensitive information. Regardless of the reason for obscured data, collecting and analyzing it is difficult.

Data that has been obscured through encryption, steganography, compression, or proprietary formats can sometimes be converted with some serious detective work and the right tools. Forensic specialists often must do quite a bit of work to decrypt encrypted information. In many cases, the investigator cannot decrypt information unless the data owner provides the encryption key and algorithm. When digital evidence has been encrypted and is in use on a live system, an investigator might have to collect evidence through a live extraction process.

Anti-Forensics

Every investigation is unique. Investigations are not necessarily friendly activities. Forensic specialists may have to conduct the investigation with or without the cooperation of the information owner. And the information owner may or may not be the target of the investigation. Investigations with uncooperative information owners are difficult.

Attackers may use techniques to intentionally conceal their identities, locations, and behavior. For example, perpetrators may conceal their identities by using networked connections at a library, an Internet café, or another public computer kiosk. Or, they may use encryption or anonymous services to protect themselves. The actions that perpetrators take to conceal their locations, activities, or identities are generally termed **anti-forensics**.

Cybercriminals are becoming better at covering their tracks as their awareness of digital forensics capabilities increases. The following are examples of anti-forensics techniques:

- *Data destruction:* Methods for disposing of data vary. They can be as simple as wiping the memory buffers used by a program, or they can be as complex as repeatedly overwriting a cluster of data with patterns of 1s and 0s. Digital evidence can be destroyed easily. For example, starting a computer updates timestamps and modifies files. Attaching a hard disk or USB stick modifies file system timestamps. Powering off a machine destroys volatile memory. Suspects may delete files and folders and defrag their hard drives in an attempt to overwrite evidence.
- *Data hiding:* Suspects often store data where an investigator is unlikely to find it. They may hide data, for example, in reserved disk sectors or as logical partitions within a defined, public partition. Or they may simply change filenames and extensions.
- *Data transformation:* Suspects may process information in a way that disguises its meaning. For example, they may use encryption to scramble a message based on an algorithm. Or they may use steganography to hide a message inside a larger message.
- *File system alteration:* Suspects often corrupt data structures and files that organize data, such as a Windows NT File System (NTFS) volume.

The Daubert Standard

One legal principle that is key to forensics and is all too often overlooked in forensic books is the Daubert standard. The Cornell University Law School defines the **Daubert standard** as follows:

> Standard used by a trial judge to make a preliminary assessment of whether an expert's scientific testimony is based on reasoning or methodology that is scientifically valid and can properly be applied to the facts at issue. Under this standard, the factors that may be considered in determining whether the methodology is valid are: (1) whether the theory or technique in question can be and has been tested;

> (2) whether it has been subjected to peer review and publication; (3) its known or potential error rate; (4) the existence and maintenance of standards controlling its operation; and (5) whether it has attracted widespread acceptance within a relevant scientific community.

What this means, in layman's terms, is that any scientific evidence presented in a trial has to have been reviewed and tested by the relevant scientific community. For a computer forensics investigator, that means that any tools, techniques, or processes you utilize in your investigation should be ones that are widely accepted in the computer forensics community. You cannot simply make up new tests or procedures.

This, naturally, brings up the question, how do new techniques become widely accepted? Let's suppose you have developed a new tool that extracts forensic information from the Windows Registry. A first step might be to provide a copy of that tool to a few professors of forensics, allowing them to experiment with it. You might also publish an article describing it. After it has been tested by the forensic community and articles about it have been read (and possibly rebutted), then your tool would be usable in real forensic investigations.

It is important to remember the Daubert standard because it will affect your forensic approach. It also reminds us of an even more basic concept: The evidence you collect is important only if it is admissible in court. So you have to pay attention to the techniques and tools you use and maintain the chain of custody.

If you fail to use widely accepted techniques, to fully document your methodology, and to use only those tools and techniques you are qualified to use, the opposing attorney might issue what is commonly called a *Daubert challenge*. This is a motion to exclude all or part of your testimony due to it failing to meet the Daubert standard. Daubert challenges are quite common in civil cases, but are not common in criminal court. There has been a movement in the legal community in recent years to increase Daubert challenges in criminal court. The rationale behind this is that some people believe that "junk science" is making its way into criminal proceedings, and well-articulated Daubert challenges could reduce that.

U.S. Laws Affecting Digital Forensics

There are many laws that affect digital forensics investigation; for example, some jurisdictions have passed laws that require the investigator to be either a law enforcement officer or a licensed private investigator to extract the evidence. Of course, that does not prevent a forensic investigator from working with information someone else extracted or extracting evidence if the information owner gave his or her permission. It is important to be aware of the legal requirements in the jurisdiction in which you work.

The Federal Privacy Act of 1974

The Privacy Act of 1974 establishes a code of information-handling practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by U.S. federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.

The Privacy Protection Act of 1980

The Privacy Protection Act (PPA) of 1980 protects journalists from being required to turn over to law enforcement any work product and documentary materials, including sources, before it is disseminated to the public. Journalists who most need the protection of the PPA are those who are working on stories that are highly controversial or about criminal acts because the information gathered may also be useful to law enforcement.

The Communications Assistance for Law Enforcement Act of 1994

The Communications Assistance for Law Enforcement Act of 1994 is a federal wiretap law for traditional wired telephony. It was expanded to include wireless, voice over internet protocol (VoIP), and other forms of electronic communications, including signaling traffic and metadata.

The Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act of 1986 governs the privacy and disclosure, access, and interception of content and traffic data related to electronic communications.

The Computer Security Act of 1987

The Computer Security Act of 1987 was passed to improve the security and privacy of sensitive information in federal computer systems. The law requires the establishment of minimum acceptable security practices, creation of computer security plans, and training of system users or owners of facilities that house sensitive information.

The Foreign Intelligence Surveillance Act of 1978

The Foreign Intelligence Surveillance Act of 1978 (FISA) is a law that allows for collection of "foreign intelligence information" between foreign powers and agents of foreign powers using physical and electronic surveillance. A warrant is issued by the FISA court for actions under FISA.

The Child Protection and Sexual Predator Punishment Act of 1998

The Child Protection and Sexual Predator Punishment Act of 1998 requires service providers that become aware of the storage or transmission of child pornography to report it to law enforcement.

The Children's Online Privacy Protection Act of 1998

The Children's Online Privacy Protection Act of 1998 (COPPA) protects children 13 years of age and younger from the collection and use of their personal information by websites. It is noteworthy that COPPA replaces the Child Online Protection Act of 1988 (COPA), which was determined to be unconstitutional.

The Communications Decency Act of 1996

The Communications Decency Act of 1996 was designed to protect persons 18 years of age and younger from downloading or viewing material considered indecent. This act has been subject to court cases that subsequently changed some definitions and penalties.

The Telecommunications Act of 1996

The Telecommunications Act of 1996 includes many provisions relative to the privacy and disclosure of information in motion through and across telephony and computer networks.

The Wireless Communications and Public Safety Act of 1999

The Wireless Communications and Public Safety Act of 1999 allows for the collection and use of “empty” communications, which means nonverbal and nontext communications, such as GPS information.

The USA Patriot Act of 2001

The USA Patriot Act is the primary law under which a wide variety of Internet and communications information content and metadata is currently collected. Provisions exist within the Patriot Act to protect the identity and privacy of U.S. citizens.

The Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act of 2002 contains many provisions about recordkeeping and destruction of electronic records relating to the management and operation of publicly held companies.

18 U.S.C. § 1030: Fraud and Related Activity in Connection with Computers

This is one of the most widely used laws in hacking cases. It covers a wide range of crimes involving illicit access of any computer.

18 U.S.C. § 1020: Fraud and Related Activity in Connection with Access Devices

This is closely related to section 1030 but covers access devices (such as routers).

The Digital Millennium Copyright Act (DMCA) of 1998

This controversial law was enacted in 1998. It makes it a crime to publish methods or techniques to circumvent copyright protection. It is controversial because it has been used against legitimate researchers publishing research papers.

18 U.S.C. § 1028A: Identity Theft and Aggravated Identity Theft

As the name suggests, this law targets any crime related to identity theft. It is often applied in stolen credit card cases.

18 U.S.C. § 2251: Sexual Exploitation of Children

This law covers a range of child exploitation crimes and is often seen in child pornography cases. Related to this rather broad law are several others, such as:

- *18 U.S.C. § 2260:* Production of sexually explicit depictions of a minor for importation into the United States.
- *18 U.S.C. § 2252:* Certain activities relating to material involving the sexual exploitation of minors (possession, distribution and receipt of child pornography).
- *18 U.S.C. § 2252A:* Certain activities relating to material constituting or containing child pornography.

Warrants

According to the Supreme Court, a "seizure of property occurs when there is some meaningful interference with an individual's possessory interests in that property" (*United States v. Jacobsen*, 466 U.S. 109, 113 [1984]). The Court also characterized the interception of intangible communications as a seizure, in the case of *Berger v. New York* (388 U.S. 41, 59–60 [1967]). Now that means that law enforcement need not take property in order for it to be considered seizure. Merely interfering with an individual's access to his or her own property constitutes seizure. *Berger v. New York* extends that to communications. If law enforcement's conduct does not violate a person's "reasonable expectation of privacy," then formally it does not constitute a Fourth Amendment "search" and no warrant is required. There have been many cases where the issue of reasonable expectation of privacy has been argued. To use an example that is quite clear, if you save a message in an electronic diary, you clearly have a reasonable expectation of privacy; however, if you post such a message on a public bulletin board, you can have no expectation of privacy. In less clear cases, a general rule is that courts have held that law enforcement officers are prohibited from accessing and viewing information stored in a computer if it would be prohibited from opening a closed container and examining its contents in the same situation.

Warrants are not needed when evidence is in plain sight. For example, if a detective is talking to someone about a string of burglaries in the neighborhood, and can clearly see child pornography on that person's computer screen, no warrant is needed. Another exception to the need for a warrant is consent. If someone who is authorized to provide consent gives that consent to search, then no warrant is needed.

In computer crime cases, two consent issues arise particularly often. First, when does a search exceed the scope of consent? For example, when a person agrees to the search of a location, such as his or her apartment, does that consent authorize the retrieval of information stored in computers at the location? Second, who is the proper party to consent to a search? Can roommates, friends, and parents legally grant consent to a search of another person's computer files? These are all very critical questions that must be considered when searching a computer. In general, courts have held that only the actual owner of a property can grant consent. For example, a parent of a minor child can grant consent to search the child's living quarters and computers. However, a roommate who shares rent can grant consent to search only living quarters and computers co-owned by both parties. A roommate cannot grant consent to search the private property of the other person.

There are other cases where you don't need a warrant. One such circumstance is border crossing. Anyone going through customs in any country may have their belongings searched. This can include a complete forensic examination of laptops, cell phones, and other devices. Another such instance where a warrant is not needed is if there is imminent danger that evidence will be destroyed. In the case of *United States v. David*, the court held that "When destruction of evidence is imminent a warrantless seizure of that evidence is justified if there is probable cause to believe that the item seized constitutes evidence of criminal activity."

It is also important not to exceed the scope of a warrant. In *United States v. Schlingloff*, 2012 U.S. Dist. LEXIS 157272 (C.D. Ill. Oct. 24, 2012), Judge Shadid held that use of Forensic Toolkit's (FTK) Known File Filter (KFF) to alert on child pornography files was outside the scope of a warrant issued to look for evidence of identity theft. In this case, the owner of the device was suspected of identity theft, and a warrant was issued so that police could search for evidence of that crime. However, the investigator used the Known File Filter to search for child pornography, and indeed found illegal images on the computer in question.

Federal Guidelines

If you are setting up a forensic lab, or if you are new to forensics, a good place to start is the federal guidelines. Two agencies in particular—the FBI and the Secret Service—are particularly important.

The FBI

If an incident occurs, the FBI recommends that the first responder preserve the state of the computer at the time of the incident by making a backup copy of any logs, any damaged or altered files, and any other files modified, viewed, or left by the intruder. This last part is critical. Hackers frequently use various tools and may leave traces of their presence. Furthermore, the FBI advises that if the incident is in progress, you should activate any auditing or recording software you might have available. Collect as much data about the incident as you can. In other words, this might be a case where you do not take the machine offline, but rather analyze the attack in progress.

The FBI computer forensics guidelines stress the importance of securing any evidence. They further stress that computer evidence can come in many forms. Here are a few common forms:

- Hard drives
- System logs
- Portable storage, such as USB drives and external drives
- Router logs
- Emails

- Chat room logs
- Smartphones and tablets
- SIM cards for cell phones and smartphones
- Logs from security devices, such as firewalls and intrusion detection systems
- Databases and database logs

What you secure will be dependent upon the nature of the cybercrime. For example, in the case of child predators, online stalkers, or online fraud, email may be very important, but router logs may be irrelevant. The FBI also stresses that you should work with a copy of the hard drive, not the original.

The FBI has a cybercrimes webpage, which is a very useful resource for learning more about trends in cybercrime and in computer forensics.

The Secret Service

The U.S. Secret Service is the premier federal agency tasked with combating cybercrime. It has a website devoted to computer forensics that includes forensic courses. These courses are usually for law enforcement personnel.

FYI

Since 9/11, the U.S. Secret Service has been tasked with taking the lead in U.S. cybercrime efforts. There are electronic crime taskforce centers set up in several major cities, including Atlanta, Baltimore, Birmingham, Boston, Buffalo, Chicago, Dallas, Houston, and San Francisco. These electronic crime task force centers cooperate with other law enforcement agencies, including local police departments, in computer crime investigations.

The Secret Service also has released a guide for first responders to computer crime. The agency has listed its “golden rules” to begin the investigation. They are as follows:

- Officer safety: Secure the scene and make it safe.
- If you reasonably believe that the computer is involved in the crime you are investigating, take immediate steps to preserve the evidence.
- Determine whether you have a legal basis to seize the computer, such as plain view, search warrant, or consent.
- Do not access any computer files. If the computer is off, leave it off.
- If it is on, do not start searching through the computer. Instead, properly shut down the computer and prepare it for transport as evidence.
- If you reasonably believe that the computer is destroying evidence, immediately shut down the computer by pulling the power cord from the back of the computer.
- If a camera is available, and the computer is on, take pictures of the computer screen. If the computer is off, take pictures of the computer, the location of the computer, and any electronic media attached.

- Determine whether special legal or privacy considerations apply, such as those for doctors, attorneys, clergy, psychiatrists, newspapers, or publishers.

These are all important first steps to both preserving the chain of custody and ensuring the integrity of the investigation from the very first step.

The Regional Computer Forensics Laboratory Program

The Regional Computer Forensics Laboratory (RCFL) program is a national network of forensic laboratories and training centers. The FBI provides startup and operational funding, training, staff, and equipment to the program. State, local, and other federal law enforcement agencies assign personnel to staff RCFL facilities.

Each of the 16 RCFLs examines digital evidence in support of criminal and national security investigations. The RCFL program provides law enforcement at all levels with digital forensics expertise. It works with a wide variety of investigations, including terrorism, child pornography, fraud, and homicide.

The RCFL program conducts digital forensics training. In 2008, for example, the program trained nearly 5000 law enforcement personnel in system forensics tools and techniques. For more information, see http://www.rcfl.gov.

CHAPTER SUMMARY

This chapter explored the basics of computer forensics. You have learned general principles, such as working only with a copy of the drive you're investigating and maintaining the chain of custody. The chapter also examined the types of digital forensics done as well as the laws regarding digital forensics. You should be familiar with the Daubert standard, warrants, federal forensic guidelines, and the general forensic procedure.

KEY CONCEPTS AND TERMS

Anti-forensics
Cell-phone forensics
Chain of custody
Computer forensics
Curriculum vitae (CV)
Daubert standard
Demonstrative evidence
Digital evidence
Disk forensics
Documentary evidence
Email forensics
Expert report
Expert testimony
Internet forensics
Live system forensics
Network forensics
Real evidence
Software forensics
Testimonial evidence
Volatile memory

CHAPTER 1 ASSESSMENT

1. In a computer forensics investigation, describe the route that evidence takes from the time you find it until the case is closed or goes to court.
   A. Rules of evidence
   B. Law of probability
   C. Chain of custody
   D. Policy of separation

2. If the computer is turned on when you arrive, what does the Secret Service recommend you do?
   A. Begin your investigation immediately.
   B. Shut down according to recommended Secret Service procedure.
   C. Transport the computer with power on.
   D. Unplug the machine immediately.

3. Why should you note all cable connections for a computer you want to seize as evidence?
   A. To know what outside connections existed
   B. In case other devices were connected
   C. To know what peripheral devices existed
   D. To know what hardware existed

4. What is the essence of the Daubert standard?
   A. That only experts can testify at trial
   B. That an expert must affirm that a tool or technique is valid
   C. That only tools or techniques that have been accepted by the scientific community are admissible at trial
   D. That the chain of custody must be preserved

5. When cataloging digital evidence, the primary goal is to do what?
   A. Make bitstream images of all hard drives.
   B. Preserve evidence integrity.
   C. Keep evidence from being removed from the scene.
   D. Keep the computer from being turned off.

6. Which of the following is important to the investigator regarding logging?
   A. The logging methods
   B. Log retention
   C. Location of stored logs
   D. All of the above

7. Your roommate can give consent to search your computer.
   A. True
   B. False

8. Evidence need not be locked if it is at a police station.
   A. True
   B. False

9. You are investigating a breach of a file server that resulted in several stolen files. Which federal law is most likely to apply?
   A. 18 U.S.C. § 1028A, Identity Theft and Aggravated Identity Theft
   B. 18 U.S.C. § 1030, Fraud and Related Activity in Connection with Computers
   C. The USA Patriot Act
   D. The Telecommunications Act of 1996