The field of computer forensics and investigations is still in the early stages of development. This chapter introduces you to computer forensics and investigations and discusses some problems and concerns prevalent in the industry. This book blends traditional investigation methods with classic systems analysis problem-solving techniques and applies them to computer investigations. An understanding of these disciplines combined with the use of computer forensics tools will make you a highly skilled computer forensics analyst.
Understanding Computer Forensics

Computer forensics involves obtaining and analyzing digital information for use as evidence in civil, criminal, or administrative cases. The Federal Rules of Evidence (FRE) has controlled the use of digital evidence since 1970; from 1970 to 1985, state rules of evidence, as they were adopted by each state, controlled use of this type of evidence. The FBI Computer Analysis and Response Team (CART) was formed in 1984 to handle the increasing number of cases involving digital evidence. Figure 1-1 shows the home page for the FBI CART. By the late 1990s, CART had teamed up with the Department of Defense Computer Forensics Laboratory (DCFL) for research and training. Much of the early curriculum in this field came from the DCFL.

Documents maintained on a computer are covered by different rules, depending on the nature of the documents. Many court cases in state and federal courts have developed and clarified how the rules apply to digital evidence. The Fourth Amendment to the U.S. Constitution (and each state’s constitution) protects everyone’s rights to be secure in their person, residence, and property from search and seizure, for example. Continuing development of the jurisprudence of this amendment has played a role in determining whether the search for digital evidence has established a different precedent, so separate search warrants might not be necessary. However, when preparing to search for evidence in a criminal case, many investigators still include the suspect’s computer and its components in the search warrant to avoid problems.

In a significant case, the Pennsylvania Supreme Court addressed expectations of privacy and whether evidence is admissible (see Commonwealth v. Copenhefer, 553 Pa. 285, 719 A.2d 242).
The case involved a kidnapped woman who was eventually found dead, clearly murdered. Initial investigations by the FBI, state police, and local police resulted in finding physical evidence. In addition, investigators examined a computer the victim’s husband had used and discovered hidden computer-generated notes and instructions. This evidence included drafts and amendments to the text of a phone call the husband received, a ransom note, several other notes, and a detailed plan for kidnapping the victim. The investigation eventually produced several possible suspects, including the owner of a nearby bookstore who had a history of hostile encounters with the victim and her husband. On direct appeal, the Pennsylvania Supreme Court concluded that the physical evidence, especially the computer forensics evidence, was sufficient to support the bookstore owner’s conviction.

The husband’s argument was that “...even though his computer was validly seized pursuant to a warrant, his attempted deletion of the documents in question created an expectation of privacy protected by the Fourth Amendment. Thus, he claims, under Katz v. United States, 389 U.S. 347, 357, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967), and its progeny, Agent Johnson’s retrieval of the documents, without first obtaining another search warrant, was unreasonable under the Fourth Amendment and the documents thus seized should have been suppressed.”

The Pennsylvania Supreme Court rejected this argument, stating “A defendant’s attempt to secrete evidence of a crime is not synonymous with a legally cognizable expectation of privacy. A mere hope for secrecy is not a legally protected expectation. If it were, search warrants would be required in a vast number of cases where warrants are clearly not necessary.”


Computer Forensics Versus Other Related Disciplines

According to DIBS USA, Inc., a privately owned corporation specializing in computer forensics (www.dibsusa.com), computer forensics involves scientifically examining and analyzing data from computer storage media so that the data can be used as evidence in court. You can find a similar definition on the FBI’s Web site (www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm). Typically, investigating computers includes collecting computer data securely, examining suspect data to determine details such as origin and content, presenting computer-based information to courts, and applying laws to computer practice.

In general, computer forensics investigates data that can be retrieved from a computer’s hard disk or other storage media. Like an archaeologist excavating a site, computer investigators retrieve information from a computer or its component parts. The information you retrieve might already be on the disk, but it might not be easy to find or decipher. In contrast, network forensics yields information about how a perpetrator or an attacker gained access
to a network. Network forensics investigators use log files to determine when users logged on and try to determine which URLs users accessed, how they logged on to the network, and from what location. Keep in mind, however, that network forensics also tries to determine what tracks or new files were left behind on a victim's computer or what changes were made. In Chapter 11, you explore when and how network forensics should be used in your investigation.

Computer forensics is also different from data recovery, which involves recovering information from a computer that was deleted by mistake or lost during a power surge or server crash, for example. In data recovery, typically you know what you're looking for. Computer forensics is the task of recovering data that users have hidden or deleted, with the goal of ensuring that the recovered data is valid so that it can be used as evidence. The evidence can be inculpatory (in criminal cases, the expression is “incriminating”) or exculpatory, meaning it might clear the suspect. Investigators often examine a computer disk not knowing whether it contains evidence—they must search storage media, and if they find data, they piece it together to produce evidence. Various forensics software tools can be used for most cases. In extreme cases, investigators can use electron microscopes and other sophisticated equipment to retrieve information from machines that have been damaged or purposefully reformatted. This method is usually cost prohibitive, running from US$3000 to more than US$20,000, so it's not normally used.

Like companies specializing in data recovery, companies specializing in disaster recovery use computer forensics techniques to retrieve information their clients have lost. Disaster recovery also involves preventing data loss by using backups, uninterruptible power supply (UPS) devices, and off-site monitoring.

Investigators often work as a team to make computers and networks secure in an organization. The computer investigations function is one of three in a triad that makes up computing security. In an enterprise network environment, the triad consists of the following parts (shown in Figure 1-2):

- Vulnerability assessment and risk management
- Network intrusion detection and incident response
- Computer investigations

Each side of the triad in Figure 1-2 represents a group or department responsible for performing the associated tasks. Although each function operates independently, all three groups draw from one another when a large-scale computing investigation is being conducted. By combining these three groups into a team, all aspects of a high-technology investigation are addressed without calling in outside specialists.

The term enterprise network environment refers to large corporate computing systems that might include disparate or formerly independent systems. In smaller companies, one group might perform the tasks shown in the investigations triad, or a small company might contract with other companies to perform these tasks.
When you work in the vulnerability assessment and risk management group, you test and verify the integrity of standalone workstations and network servers. This integrity check covers the physical security of systems and the security of operating systems (OSs) and applications. People who work in this group test for known vulnerabilities of OSs and applications used in the network. This group also launches attacks on the network and its workstations and servers to assess vulnerabilities. Typically, people performing this task have several years of experience in UNIX and Windows administration.

Professionals in the vulnerability assessment and risk management group also have skills in network intrusion detection and incident response. This group detects intruder attacks by using automated tools and monitoring network firewall logs manually. When an external attack is detected, the response team tracks, locates, and identifies the intrusion method and denies further access to the network. If an intruder launches an attack that causes major or potential damage, this team collects the necessary evidence, which can be used for civil or criminal litigation against the intruder. Litigation is the legal process of proving guilt or innocence in court.

If an internal user is performing illegal acts, the network intrusion detection and incident response group responds by locating the user and blocking his or her access. For example, someone at a community college sends inflammatory e-mails to other users on the network. The network team quickly realizes that the e-mails are coming from a node on the internal network and dispatches a security team to the location. Vulnerability assessment staff often contribute significantly to high-end computing investigations.

The computer investigations group manages investigations and conducts forensic analysis of systems suspected of containing evidence related to an incident or a crime. For complex casework, the computer investigations group draws on resources from those involved in vulnerability assessment, risk management, and network intrusion detection and incident response. This group resolves or terminates all case investigations.

**A Brief History of Computer Forensics**

Thirty years ago, most people didn’t imagine that computers would be an integral part of everyday life. Now computer technology is commonplace, as are crimes in which a computer is the instrument of the crime, the target of the crime, and, by its nature, the location where evidence is stored or recorded.
By the 1970s, electronic crimes were increasing, especially in the financial sector. Most computers in this era were mainframes, used by trained people with specialized skills who worked in finance, engineering, and academia. White-collar fraud began when people in these industries saw a way to make money by manipulating computer data. One of the most well-known crimes of the mainframe era is the one-half cent crime. Banks commonly tracked money in accounts to the third decimal place or more. They used and still use the “rounding up” accounting method when paying interest. If the interest applied to an account resulted in a fraction of a cent, that fraction was used in the calculation for the next account until the total resulted in a whole cent. It was assumed that sooner or later every customer would benefit. Some computer programmers corrupted this method by opening an account for themselves and writing programs that diverted all the fractional monies into their accounts. In small banks, this practice amounted to only a few hundred dollars a month. In large banks with many branch offices, however, the amount reached hundreds of thousands of dollars.

During this time, most law enforcement officers didn’t know enough about computers to ask the right questions or to preserve evidence for trial. Many began to attend the Federal Law Enforcement Training Center (FLETC) programs designed to train law enforcement in recovering digital data.

As PCs gained popularity and began to replace mainframe computers in the 1980s, many different OSs emerged. Apple released the Apple 2E in 1983 and then launched the Macintosh in 1984. Computers such as the TRS-80 and the Commodore 64 were the machines of the day. CP/M machines (the 8088 series) and Zeniths were also in demand. Disk Operating System (DOS) was available in many varieties, including PC-DOS, QDOS, DR-DOS, IBM-DOS, and MS-DOS. Forensics tools at that time were simple, and most were generated by government agencies, such as the Royal Canadian Mounted Police (RCMP) in Ottawa, which had its own investigative tools, and the U.S. Internal Revenue Service (IRS). Most tools were written in C and assembly language and weren’t used by the general public.

In the mid-1980s, a new tool, Xtree Gold, appeared on the market. It recognized file types and retrieved lost or deleted files. Norton DiskEdit soon followed and became the best tool for finding deleted files. You could use these tools on the most powerful PCs of that time; IBM-compatible computers had 10 MB hard disks and two floppy drives, as shown in Figure 1-3.

In 1987, Apple produced the Mac SE, a Macintosh with an external EasyDrive hard disk with 60 MB of storage (see Figure 1-4). At this time, the popular Commodore 64 still used standard audiotapes to record data, so the Mac SE represented an important advance in computer technology.

By the early 1990s, specialized tools for computer forensics were available. The International Association of Computer Investigative Specialists (IACIS) introduced training on software for forensics investigations, and the IRS created search-warrant programs. However, no commercial GUI software for computer forensics was available until
ASR Data created Expert Witness for the Macintosh. This software could recover deleted files and fragments of deleted files. One of the ASR Data partners later left and developed EnCase, which has become a popular computer forensics tool.

In recent years, a lawsuit was settled between the two partners, and Expert Witness reverted back to the owner of EnCase. Most software for the Macintosh is now created by vendors such as BlackBag Technologies and SubRosaSoft.
As computer technology continued to evolve, more computer forensics software was developed. The introduction of large hard disks posed new problems for investigators. Most DOS-based software didn’t recognize a hard disk larger than 8 GB. Because contemporary computers have hard disks of 40 to 400 GB and larger, changes in forensics software were needed. Later in this book, you explore the challenges of using older software and hardware.

Other software, such as iLook, which is currently maintained by the IRS Criminal Investigation Division and limited to law enforcement, can analyze and read special data files that are copies of a disk. AccessData Forensic Toolkit (FTK) has become a popular commercial product that performs similar tasks in the law enforcement and civilian markets, and you use it in several projects in this book.

As software companies become savvier about computer forensics and investigations, they are publishing more forensics tools to keep pace with technology. This book discusses as many tools as possible. You should also refer to trade publications and Web sites, such as www.ctin.org (Computer Technology Investigators Network) or www.usdoj.gov (U.S. Department of Justice), to stay current.

Understanding Case Law

The technology of computers and other digital devices is evolving at an exponential pace. Existing laws and statutes simply can’t keep up with the rate of change. Therefore, when statutes or regulations don’t exist, case law is used. Case law allows legal counsel to use previous cases similar to the current one because the laws don’t yet exist. Each new case is evaluated on its own merit and issues. The University of Rhode Island (http://dfc.cs.uri.edu) cites many cases in which problems occurred in the past. One example cited on the Web site is about an investigator viewing computer files by using a search warrant related to drug dealing. While viewing the files, he ran across images of child pornography. Instead of waiting for a new warrant, he kept searching. As a result, all evidence but the pictures was thrown out. Investigators must be familiar with recent rulings to avoid making similar mistakes. Just because a law doesn’t exist yet does not mean a ruling won’t be made.

Developing Computer Forensics Resources

To be a successful computer forensics investigator, you must be familiar with more than one computing platform. In addition to older platforms, such as DOS and Windows 9x, you should be familiar with Linux, Macintosh, and current Windows platforms. However, no one can be an expert in every aspect of computing. Likewise, you can’t know everything about the technology you’re investigating. To supplement your knowledge, you should develop and maintain contact with computing, network, and investigative professionals. Keep a log of contacts, and record the names of other professionals you’ve worked with, their area of expertise, the last few projects you worked on together, and their specific contributions.

Join as many computer user groups as you can, in both the public and private sectors. In the Pacific Northwest, for example, Computer Technology Investigators Network (CTIN) meets monthly to discuss problems that law enforcement and corporations face.
This nonprofit organization also conducts free training. You can probably locate a similar group in your area, such as the **High Technology Crime Investigation Association (HTCIA)**, an organization that exchanges information about techniques related to computer investigations and security. (For more information, visit [www.htcia.org](http://www.htcia.org).)

User groups can be especially helpful when you need information about obscure OSs. For example, a user group helped convict a child molester in Pierce County, Washington, in 1996. The suspect installed video cameras in all the rooms of his house, served alcohol to young women to intoxicate them, and secretly filmed them playing strip poker. When he was accused of molesting a child, police seized his computers and other physical evidence. The investigator discovered that the computers used CoCoDOS, an OS that had been out of use for years. The investigator contacted a local users group, which supplied the standard commands and other information needed to gain access to the system. On the suspect’s computer, the investigator found a diary detailing the suspect’s actions over the past 15 years, including the molestation of more than 400 young women. As a result, the suspect received a much longer sentence than if he had been convicted of molesting only one child.

Build a network of computer forensics experts and other professionals, and keep in touch through e-mail. Find and cultivate professional relationships with people who specialize in technical areas different from your own. If you’re a Windows expert, for example, maintain contact with experts in Linux, UNIX, and Macintosh.

Outside experts can provide detailed information you need to retrieve digital evidence. For example, in a recent murder case, a husband and wife owned a Macintosh store. When the wife was discovered dead, probably murdered, investigators found that she had wanted to leave her husband but didn’t because of her religious beliefs. The police got a search warrant and confiscated the home and office computers.

When the detective on the case examined the home Macintosh, he found that the hard disk had been compressed and erased. He contacted a Macintosh engineer, who determined the two software programs used to compress the drive. With this knowledge, the detective could retrieve information from the hard disk, including text files indicating that the husband spent $35,000 in business funds to purchase cocaine and prostitution services. This evidence proved crucial in making it possible for the prosecutor to convict the husband of premeditated murder.

Take advantage of news services devoted to computer forensics, which you can access via e-mail, or electronic mailing lists to solicit advice from experts. In one case, investigators couldn’t access the hard disk of an Intel computer containing digital evidence without the password, which was hard-coded in the motherboard. When they began to run out of options and time, they posted a description of the problem on a mailing list. A list member told them that a dongle (a mechanical device) would bypass the password problem. As a result, the investigators were able to gather evidence to convict the perpetrator.

More recent cases involve laptops with specially designed ways of physically accessing the hard drives. Sometimes the manufacturer won’t tell the average person who calls how to access a laptop’s hard drive. Several investigators have had to go through law enforcement
contacts to get this information—another example of the importance of developing good relationships with people in all aspects of the digital industry, not just other investigators.

PREPARING FOR COMPUTER INVESTIGATIONS

Computer investigations and forensics falls into two distinct categories: public investigations and private or corporate investigations (see Figure 1-5).

Public investigations involve government agencies responsible for criminal investigations and prosecution. Government agencies range from local, county, and state or provincial police departments to federal regulatory enforcement agencies. These organizations must observe legal guidelines such as Article 8 in the Charter of Rights of Canada, the Criminal
Procedures Act of the Republic of Namibia, and U.S. Fourth Amendment issues related to search and seizure rules (see Figure 1-6).

The law of search and seizure protects the rights of all people, including people suspected of crimes; as a computer investigator, you must be sure to follow these laws. The Department of Justice (DOJ) updates information on computer search and seizure regularly (see www.usdoj.gov/criminal/cybercrime/).

Public investigations usually involve criminal cases and government agencies; private or corporate investigations, however, deal with private companies, non-law-enforcement government agencies, and lawyers. These private organizations aren’t governed directly by criminal law or Fourth Amendment issues, but by internal policies that define expected employee behavior and conduct in the workplace. Private corporate investigations also involve litigation disputes. Although private investigations are usually conducted in civil cases, a civil case can escalate into a criminal case, and a criminal case can be reduced to a civil case. If you follow good forensics procedures, the evidence found in your investigations can easily make the transition between civil and criminal cases.

Understanding Law Enforcement Agency Investigations

When conducting public computer investigations, you must understand your local city, county, state or province, and federal laws on computer-related crimes, including standard legal processes and how to build a criminal case. In a criminal case, a suspect is tried for a criminal offense, such as burglary, murder, or molestation. To determine whether there was a computer crime, an investigator asks questions such as the following: What was the tool
used to commit the crime? Was it a simple trespass? Was it a theft, a burglary, or vandalism? Did the perpetrator infringe on someone else’s rights by cyberstalking or e-mail harassment?

Laws in countries other than the United States can be quite different. Throughout this book, the authors point out when items accepted in U.S. courts don’t stand up in other courts. Lately, a major issue has been European Union (EU) privacy laws as opposed to U.S. privacy laws. Another issue is international companies. Over the past decade, more companies have been consolidating into global entities. As a result, internal corporate investigations can involve the laws of multiple countries. For example, your company has a subsidiary operating in Australia. An employee at that subsidiary is suspected of fraud, and as part of your investigation, you need to seize his cell phone. Under U.S. law, you could if he used it on company property and interfaced it with the company network. Under Australian law, you cannot.

Computers and networks are only tools that can be used to commit crimes and are, therefore, no different from the lockpick a burglar uses to break into a house. For this reason, many states have added specific language to criminal codes to define crimes involving computers. For example, they have expanded the definition of laws for crimes such as burglary or theft to include taking data from a computer without the owner’s permission, so computer theft is now on a par with breaking into someone's house and stealing the silver. Other states have instituted specific criminal statutes that address computer-related crimes but typically don’t include computer-related issues in standard trespass, theft, vandalism, or burglary laws. The Computer Fraud and Abuse Act was passed in 1986, but specific state laws weren’t formulated until later. To this day, many have yet to be tested in court.

Computers are involved in many serious crimes. The most notorious are those involving child molestation. Digital images are stored on hard disks, Zip disks, floppy disks, thumb drives, and other storage media and circulated on the Internet. Other computer crimes concern missing children and adults because information about missing people is often found on computers. Drug dealers often keep information about transactions on their computers or personal digital assistants (PDAs). This information is especially useful because it helps law enforcement officers convict the person they arrested and locate drug suppliers and other dealers. In stalking cases, deleted e-mail, digital photos, and other evidence stored on a computer can help solve a case.

**Following the Legal Processes**

When conducting a computer investigation for potential criminal violations of the law, the legal processes you follow depend on local custom, legislative standards, and rules of evidence. In general, however, a criminal case follows three stages: the complaint, the investigation, and the prosecution (see Figure 1-7). Someone files a complaint, and a specialist investigates the complaint and, with the help of a prosecutor, collects evidence and builds a case. If a crime has been committed, the case is tried in court.
A criminal case begins when someone finds evidence of an illegal act or witnesses an illegal act. The witness or victim (referred to as the “complainant”) makes a complaint to the police. Based on the incident or crime, the complainant makes an allegation, an accusation or supposition of fact that a crime has been committed.

A police officer interviews the complainant and writes a report about the crime. The police department processes the report, and the department’s upper management decides to start an investigation or log the information into a police blotter. The police blotter provides a record of clues to crimes that have been committed previously. Criminals often repeat actions in their illegal activities, and these habits can be discovered by examining police blotters. This historical knowledge is useful when conducting investigations, especially in high-technology crimes.

Law enforcement is concerned with protecting the public good. As a result, not every good police officer is a computer expert. Some are computer novices; others might be trained to recognize what they can retrieve from a computer disk. To differentiate the training and experience law officers have, CTIN has established three levels of law enforcement expertise:

- **Level 1**—Acquiring and seizing digital evidence, normally performed by a street police officer.
- **Level 2**—Managing high-tech investigations, teaching investigators what to ask for, and understanding computer terminology and what can and can’t be retrieved from digital evidence. The assigned detectives usually handle the case.
- **Level 3**—Specialist training in retrieving digital evidence, normally performed by a data recovery or computer forensics expert, network forensics expert, or Internet fraud investigator. This person might also be qualified to manage a case, depending on his or her background.

If you’re an investigator assigned to a case, recognize the level of expertise of police officers and others involved in the case. You should have Level 3 training to conduct the investigation and possibly manage the case. You start by assessing the scope of the case, which includes the computer’s OS, hardware, and peripheral devices. You then determine whether resources are available to process all the evidence. Note that your job is more difficult when
information is stored on PDAs, cell phones, and other mobile devices. Determine whether you have the proper tools to collect and analyze evidence and whether you need to call on other specialists to assist in collecting and processing evidence. After you have gathered the resources you need, your role is to delegate, collect, and process the information related to the complaint.

After you build a case, the information is turned over to the prosecutor. Your job is finished when you have used all known and available methods to extract data from the digital evidence that was seized. As an investigator, you must then present the collected evidence with a report to the government’s attorney. Depending on your community and the nature of the crime, the prosecutor can be a prosecuting attorney, district attorney, state attorney, county attorney, Crown attorney, or U.S. attorney.

In a criminal or public case, if you have enough information to support a search warrant, the prosecuting attorney might direct you to submit an **affidavit**. This sworn statement of support of facts about or evidence of a crime is submitted to a judge to request a search warrant before seizing evidence. Figure 1-8 shows a typical affidavit. It’s your responsibility to write the affidavit, which must include **exhibits** (evidence) that support the allegation to justify the warrant. You must then have the affidavit **notarized** under sworn oath to verify that the information in the affidavit is true.

![Typical affidavit language](image)

{Based on actual inspection of spreadsheets, financial records, and invoices, Joe Smith, a computer forensics expert, is aware that computer equipment was used to generate, store, and print documents used in Jonathon Douglas’s tax evasion scheme. There is reason to believe that the computer system currently located on Jonathon Douglas’s premises is the same system used to produce and store the spreadsheets, financial records, and invoices, and that both the [spreadsheets, financial records, invoices] and other records relating to Jonathon Douglas’s criminal enterprise will be stored on Jonathon Douglas’s computer.


Figure 1-8 Typical affidavit language}
After a judge approves and signs a search warrant, it’s ready to be executed, meaning you can collect evidence as defined by the warrant. After you collect the evidence, you process and analyze it to determine whether a crime actually occurred. The evidence is then presented in court, after which a judge, an administrative law judge, or a jury hands down a verdict.

Understanding Corporate Investigations

Private or corporate investigations involve private companies and lawyers who address company policy violations and litigation disputes, such as wrongful termination. When conducting a computer investigation for a private company, remember that business must continue with minimal interruption from your investigation. Because businesses usually focus on continuing their usual operations and making profits, many in a private corporate environment consider your investigation and apprehension of a suspect secondary to stopping the violation and minimizing damage or loss to the business. Businesses also strive to minimize or eliminate litigation, which is an expensive way to address criminal or civil issues. Corporate computer crimes can involve e-mail harassment, falsification of data, gender and age discrimination, embezzlement, sabotage, and industrial espionage, which involves selling sensitive or confidential company information to a competitor. Anyone with access to a computer can commit these crimes.

Embezzlement is a common computer crime, particularly in small firms. Typically, the owner is busy and trusts one person, such as the office manager, to handle daily transactions. When the office manager leaves, the owner discovers that some clients were overbilled or others were not billed at all, and money is missing. Rebuilding the paper and electronic trail can be tedious. Collecting enough evidence to press charges might be beyond the owner’s capabilities.

Corporate sabotage is most often committed by a disgruntled employee. The employee decides to take a job at a competitor’s firm and collects critical files on a disk or thumb drive before leaving. This type of crime can also lead to industrial espionage, which increases every year.

Investigators will soon be able to conduct digital investigations on site without a lab and without interrupting employees’ work on a computer. Suppose that an assisted-care facility has an employee involved in an insurance scam who’s overcharging the insurance company and then funneling the monies into her own bank account. The facility’s network server keeps track of patient billing and critical information, such as medication, medical conditions, and treatments, for each patient. Taking that system offline for more than a short time could result in harm to patients. Investigators can’t seize the evidence; instead, they acquire a disk image and any other pertinent information and allow the system to go back online as quickly as possible.

Organizations can help prevent and address these crimes by creating and distributing appropriate policies, making employees aware of the policies, and enforcing the policies.
Establishing Company Policies

One way that businesses can avoid litigation is to publish and maintain policies that employees find easy to read and follow. The most important policies are those that set rules for using the company's computers and networks. Published company policies provide a line of authority for a business to conduct internal investigations. The line of authority states who has the legal right to initiate an investigation, who can take possession of evidence, and who can have access to evidence.

Well-defined policies give computer investigators and forensic examiners the authority to conduct an investigation. Policies also demonstrate that an organization intends to be fair minded and objective about how it treats employees and state that the organization will follow due process for all investigations. Due process refers to fairness under the law and is meant to protect the innocent. Without defined policies, a business risks exposing itself to litigation by current or former employees. The person or committee in charge of maintaining corporate policies must also stay current with local laws, which can vary depending on the city, state, or country.

Displaying Warning Banners

Another way a private or public organization can avoid litigation is to display a warning banner on computer screens. A warning banner usually appears when a computer starts or connects to the company intranet, network, or virtual private network (VPN) and informs end users that the organization reserves the right to inspect computer systems and network traffic at will. (An end user is a person using a computer to perform routine tasks other than systems administration.) If this right isn’t stated explicitly, employees might have an assumed right of privacy when using a company’s computer systems and network accesses. With an assumed right of privacy, employees think their transmissions at work are protected in much the same way that mail sent via the U.S. Postal Service is protected. Figure 1-9 shows a sample warning banner.

![Figure 1-9 A sample warning banner](image)

A warning banner establishes the right to conduct an investigation. By displaying a strong, well-worded warning banner, an organization doesn’t need to obtain a search warrant or
court order as required under Fourth Amendment search and seizure rules. If a company owns the computer equipment, it doesn’t need a search warrant to seize the equipment. In a company with a well-defined policy, this right to inspect or search at will applies to both criminal activity and company policy violations. Keep in mind, however, that your country’s laws might differ. For example, in some countries, even though the company has the right to seize computers at any time, if employees are suspected of a criminal act, they need to be informed at that time.

Computer system users can include employees or guests. Employees can access the intranet, and guests can typically access only the main network. Companies can use two types of warning banners: one for internal employee access (intranet Web page access) and another for external visitor access (Internet Web page access). The following lists recommend items that should be listed in all warning banners. Before applying these warnings, you should consult with the organization’s legal department for any additional required legal notices for your work area or department.

Depending on the type of organization, the following text can be used in internal warning banners:

- Access to this system and network is restricted.
- Use of this system and network is for official business only.
- Systems and networks are subject to monitoring at any time by the owner.
- Using this system implies consent to monitoring by the owner.
- Unauthorized or illegal users of this system or network will be subject to discipline or prosecution.

The DOJ document at www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm has several examples of warning banners.

An organization such as a community college might simply state that systems and networks are subject to observation and monitoring at any time because members of the local community who aren’t staff or students might use the facilities. A for-profit organization, on the other hand, could have proprietary information on its network and use all the suggested text items.

Guests, such as employees of business partners, might be allowed to use the system. The text that’s displayed when a guest attempts to log on can include warnings similar to the following:

- This system is the property of Company X.
- This system is for authorized use only; unauthorized access is a violation of law and violators will be prosecuted.
- All activity, software, network traffic, and communications are subject to monitoring.
As a corporate computer investigator, make sure a company displays a well-defined warning banner. Without a banner, your authority to inspect might conflict with the user’s expectation of privacy, and a court might have to determine the issue of authority to inspect. State laws vary on the expectation of privacy, but all states accept the concept of a waiver (of the expectation of privacy). Additionally, the EU and its member nations impose strict fines for information that crosses national boundaries without the person’s consent. So if your company is conducting an investigation in a subsidiary residing in the EU, you may or may not be able to acquire a network drive without notifying certain parties or making sure consent forms are in place.

Some might argue that written policies are all that are necessary. However, in the actual prosecution of cases, warning banners have been critical in determining that a system user didn’t have an expectation of privacy for the information stored on the system. A warning banner has the additional advantage of being easier to present in trial as an exhibit than a policy manual. Government agencies, such as the Department of Energy, Argonne National Labs, and Lawrence Livermore Labs, now require warning banners on all computer terminals on their systems. Many corporations also require warning banners as part of the logon/startup process.

Designating an Authorized Requester

As mentioned earlier, investigations must establish a line of authority. In addition to warning banners that state a company’s rights of computer ownership, businesses should specify an **authorized requester** who has the power to conduct investigations. Executive management should define this policy to avoid conflicts from competing interests between organizations or departments. In large organizations, competition for funding or management support can become so fierce that people sometimes create false allegations of misconduct to prevent a competing department from delivering a proposal for the same source of funds.

To avoid trivial or inappropriate investigations, executive management must also define and limit who is authorized to request a computer investigation and forensic analysis. Generally, the fewer groups with authority to request a computer investigation, the better. Examples of groups that should have direct authority to request computer investigations in the corporate environment include the following:

- Corporate Security Investigations
- Corporate Ethics Office
- Corporate Equal Employment Opportunity Office
- Internal Auditing
- The general counsel or Legal Department
All other groups, such as the Human Resources or Personnel departments, should coordinate their requests through the Corporate Security Investigations group. This policy separates the investigative process from the process of employee discipline.

Conducting Security Investigations

Conducting a computer investigation in the private sector is not much different from conducting one in the public sector. During public investigations, you search for evidence to support criminal allegations. During private investigations, you search for evidence to support allegations of abuse of a company's assets and, in some cases, criminal complaints. Three types of situations are common in the enterprise environment:

- Abuse or misuse of corporate assets
- E-mail abuse
- Internet abuse

Most computer investigations in the private sector involve misuse of computing assets. Typically, this misuse is referred to as employee violation of company rules. Computing abuse complaints center on e-mail and Internet misuse by employees but could involve other computing resources, such as using company software to produce a product for personal profit. The scope of an e-mail investigation ranges from excessive use of a company's e-mail system for personal use to making threats or harassing others via e-mail. Some common e-mail abuses involve transmitting offensive messages. These types of messages create a hostile work environment that can result in an employee filing a civil lawsuit against a company that does nothing to prevent it (in other words, implicitly condones the e-mail abuse).

Computer investigators also examine Internet abuse. Employees’ abuse of Internet privileges ranges from excessive use, such as spending all day Web surfing, to viewing pornographic pictures on the Web while at work. An extreme instance of Internet abuse is viewing contraband pornographic images, such as child pornography. Viewing contraband images is a criminal act in most jurisdictions, and computer investigators must handle this situation with the highest level of professionalism. By enforcing policy consistently, a company minimizes its liability exposure. The role of a computer investigator is to help management verify and correct abuse problems in an organization. (In later chapters, you learn the procedures for conducting these types of investigations.)

Be sure to distinguish between a company's abuse problems and potential criminal problems. Abuse problems violate company policy but might not be illegal if performed at home. Criminal problems involve acts such as industrial espionage, embezzlement, and murder. However, actions that appear related to internal abuse could also have criminal or civil liability. Because any civil investigation can become a criminal investigation, you must treat all evidence you collect with the highest level of security and accountability. Later in this book, you learn the Federal Rules of Evidence, processes to ensure the chain of custody, and how to apply them to computing investigations.
Similarly, your private corporate investigation might seem to involve a civil, noncriminal matter, but as you progress through your analysis, you might identify a criminal matter, too. Because of this possibility, you must always remember that your work can come under the scrutiny of the civil or criminal legal system. The Federal Rules of Evidence are the same for civil and criminal matters. By uniformly applying the rules to all investigations, you eliminate any concerns. These standards are emphasized throughout this book.

Corporations often follow the silver-platter doctrine, which is what happens when a civilian or corporate investigative agent delivers evidence to a law enforcement officer. Remember that a police officer is a law enforcement agent. A corporate investigator’s job is to minimize risk to the company. After you turn over evidence to law enforcement and begin working under their direction, you become an agent of law enforcement, subject to Fourth Amendment restrictions on search and seizure. However, an agent of the court, such as a lawyer or police officer, can’t ask you as a private citizen to obtain evidence that would require a warrant. The silver-platter doctrine doesn’t exist in all countries, so again, check the law if you’re investigating a case outside the United States.

Litigation is costly, so after you have assembled evidence, offending employees are usually disciplined or let go with a minimum of fanfare. However, when you discover that a criminal act involving a third-party victim has been committed, generally you have a legal and moral obligation to turn the information over to law enforcement. In the next section, you learn about situations in which criminal evidence must be separated from any corporate proprietary information.

**Distinguishing Personal and Company Property**

Many company policies distinguish between personal and company computer property. One area that’s difficult to distinguish involves PDAs, cell phones, and personal notebook computers. Say that an employee has purchased a PDA and hooks up the device to her company computer. As she synchronizes the information on her PDA with the information in her copy of Microsoft Outlook, she copies some data in her PDA to the company network. Because the data is now on the company network, does the information on the PDA belong to the company or the employee?

Now suppose that the company gave the employee the PDA as part of her holiday bonus. Can the company claim rights to the PDA? Similar issues come up when an employee brings in a personal notebook computer and hooks it up to the company network. What rules apply? As computers become more entrenched in daily life, you’ll encounter these issues more often. These questions are still being debated, and companies are establishing their own policies to handle them. The safe policy is to not allow any personally owned devices to be connected to company-owned resources, thereby limiting the possibility of commingling personal and company data. This policy can be counterproductive; however, the risks must be known and addressed in company policy. Other companies simply state that if you connect a personal device to the corporate network, it falls under the same rules as corporate property. At the time of this writing, this policy has yet to be tested in court.
MAINTAINING PROFESSIONAL CONDUCT

Your professional conduct as a computer investigation and forensics analyst is critical because it determines your credibility. Professional conduct, discussed in more detail in Chapters 15 and 16, includes ethics, morals, and standards of behavior. As a professional, you must exhibit the highest level of ethical behavior at all times. To do so, you must maintain objectivity and confidentiality during an investigation, enrich your technical knowledge, and conduct yourself with integrity. On any current crime drama, you can see how attorneys attack the character of witnesses, so your character should be beyond reproach.

Maintaining objectivity means you must form and sustain unbiased opinions of your cases. Avoid making conclusions about your findings until you have exhausted all reasonable leads and considered the available facts. Your ultimate responsibility is to find digital evidence to support the allegation or clear the defendant of the criminal accusation. You must ignore external biases to maintain the integrity of your fact-finding in all investigations. For example, if you’re employed by an attorney, do not allow the attorney’s agenda to dictate the outcome of your investigation. Your reputation and long-term livelihood depend on being objective in all matters.

You must also maintain an investigation’s credibility by keeping the case confidential. Discuss the case only with people who need to know about it, such as other investigators involved in the case or someone in the line of authority asking for an update. If you need advice from other professionals, discuss only the general terms and facts about the case without mentioning specifics. All investigations you conduct must be kept confidential, until you’re designated as a witness or required to release a report at the direction of the attorney or court.

In the corporate environment, confidentiality is critical, especially when dealing with employees who have been terminated because they were running home-based businesses at work on company machines and time. The agreement might have been to lay off the employee without benefits or unemployment compensation in exchange for no bad references. If you give case details and the employee’s name to others, your company could be sued for breach of contract.

In rare instances, your corporate case might become a criminal case as serious as murder. Because of the legal system, it could be years before the case gets to trial. If an investigator talked about the digital evidence with others, the case could be damaged because of pretrial publicity. When working for an attorney on an investigation, the attorney–work-product rule and attorney-client privilege apply to all communications. This means you can discuss the case only with the attorney or other members of the team working with the attorney. All communications about the case to other people requires the attorney’s approval. If you recall the concept of six degrees of separation, someone you discuss the case with might know the person being charged, so maintaining confidentiality of evidence is critical.

In addition to maintaining objectivity and confidentiality, you can enhance your professional conduct by continuing your training. The field of computer investigations and forensics is changing constantly. You should stay current with the latest technical changes in computer
hardware and software, networking, and forensic tools. You should also learn about the latest investigation techniques you can apply to your cases.

One way to enrich your knowledge of computer investigations is to record your fact-finding methods in a journal. A journal can help you remember how to perform tasks and procedures and use hardware and software tools. Be sure to include dates and important details that serve as memory triggers. Develop a routine of reviewing your journal regularly to keep your past achievements fresh in your mind.

To continue your professional training, you should attend workshops, conferences, and vendor courses. You might also need to continue your formal education. You enhance your professional standing if you have at least an undergraduate degree in a computing field. If you don’t have an advanced degree, consider graduate-level studies in a complementary area of study, such as business law or e-commerce.

Companies often supplement your education in exchange for a commitment to a certain term of employment.

In addition to education and training, membership in professional organizations adds to your credentials. These organizations often sponsor training and offer information exchanges of the latest technical improvements and trends in computer investigations. Also, monitor the latest book releases and read as much as possible about computer investigations and forensics.

As a computer investigation and forensics professional, you’re expected to achieve a high public and private standing and maintain honesty and integrity. You must conduct yourself with the highest levels of integrity in all aspects of your life. Any indiscreet actions can embarrass you and give opposing attorneys opportunities to discredit you during your testimony in court or in depositions.

CHAPTER SUMMARY

- Computer forensics applies forensics procedures to digital evidence. This process involves systematically accumulating and analyzing digital information for use as evidence in civil, criminal, or administrative cases. Computer forensics differs from network forensics, data recovery, and disaster recovery in scope, technique, and objective.
- Laws relating to digital evidence were established in the 1970s.
- To be a successful computer forensics investigator, you must be familiar with more than one computing platform. To supplement your knowledge, develop and maintain contact with computer, network, and investigative professionals.
- Public and private computer investigations differ in that public investigations typically require a search warrant before seizing digital evidence. The Fourth Amendment to the U.S. Constitution and similar legislation in other countries apply to governmental search
and seizure. During public investigations, you search for evidence to support criminal allegations. During private investigations, you search for evidence to support allegations of abuse of assets and, in some cases, criminal complaints.

- Warning banners should be used to remind employees and visitors of company policy on computer and Internet use.
- Companies should define and limit the number of authorized requesters who can start an investigation.
- The silver-platter doctrine refers to handing the results of private investigations over to law enforcement because of indications of criminal activity. It also states that an officer of the court may not coerce a private citizen into obtaining information that requires a warrant.
- Computer forensics investigators must maintain professional conduct to protect their credibility.

**Key Terms**

**affidavit** — The document, given under penalty of perjury, that investigators create detailing their findings. This document is often used to justify issuing a warrant or to deal with abuse in a corporation.

**allegation** — A charge made against someone or something before proof has been found.

**authorized requester** — In a corporate environment, the person who has the right to request an investigation, such as the chief security officer or chief intelligence officer.

**computer forensics** — Applying scientific methods to collect and analyze data and information that can be used as evidence.

**computer investigations** — Conducting forensic analysis of systems suspected of containing evidence related to an incident or a crime.

**Computer Technology Investigators Network (CTIN)** — A nonprofit group based in the Seattle–Tacoma, WA, area composed of law enforcement members, private corporation security professionals, and other security professionals whose aim is to improve the quality of high-technology investigations in the Pacific Northwest.

**criminal case** — A case in which criminal law must be applied.

**criminal law** — Statutes applicable to a jurisdiction that state offenses against the peace and dignity of the jurisdiction and the elements that define those offenses.

**data recovery** — A specialty field in which companies retrieve files that were deleted accidentally or purposefully.

**disaster recovery** — A specialty field in which companies perform real-time backups, monitoring, data recovery, and hot site operations.

**end user** — The person who uses a software product and generally has less expertise than the software designer.

**enterprise network environment** — A large corporate computing system that can include formerly independent systems.
exculpatory — Evidence that indicates the suspect is innocent of the crime.
exhibits — Items used in court to prove a case.
Fourth Amendment — The Fourth Amendment to the U.S. Constitution in the Bill of Rights dictates that the government and its agents must have probable cause for search and seizure.
High Technology Crime Investigation Association (HTCIA) — A nonprofit association for solving international computer crimes.
hostile work environment — An environment in which employees cannot perform their assigned duties because of the actions of others. In the workplace, these actions include sending threatening or demeaning e-mail or a co-worker viewing pornographic or hate sites.
inculpatory — Evidence that indicates a suspect is guilty of the crime with which he or she is charged.
industrial espionage — Selling sensitive or proprietary company information to a competitor.
International Association of Computer Investigative Specialists (IACIS) — An organization created to provide training and software for law enforcement in the computer forensics field.
line of authority — The order in which people or positions are notified of a problem; these people or positions have the legal right to initiate an investigation, take possession of evidence, and have access to evidence.
litigation — The legal process leading to a trial with the purpose of proving criminal or civil liability.\nnetwork intrusion detection and incident response — Detecting attacks from intruders by using automated tools; also includes the manual process of monitoring network firewall logs.
notarized — Having a document witnessed and a person clearly identified as the signer before a notary public.
police blotter — A log of criminal activity that law enforcement personnel can use to review the types of crimes currently being committed.
professional conduct — Behavior expected of an employee in the workplace or other professional setting.
right of privacy — The belief employees have that their transmissions at work are protected.
search and seizure — The legal act of acquiring evidence for an investigation. See Fourth Amendment.
search warrants — Legal documents that allow law enforcement to search an office, a place of business, or other locale for evidence related to an alleged crime.
silver-platter doctrine — The policy requiring an investigator who is not an agent of the court to submit evidence to law enforcement when a criminal act has been uncovered.
vulnerability assessment and risk management — The group that determines the weakest points in a system. It covers physical security and the security of OSs and applications.

warning banner — Text displayed on computer screens when people log on to a company computer; this text states the ownership of the computer and specifies appropriate use of the machine or Internet access.

**Review Questions**

1. List two organizations mentioned in the chapter that provide computer forensics training.
2. Computer forensics and data recovery refer to the same activities. True or False?
3. Police in the United States must use procedures that adhere to which of the following?
   a. the Third Amendment
   b. the Fourth Amendment
   c. the First Amendment
   d. none of the above
4. The triad of computing security includes which of the following?
   a. detection, response, and monitoring
   b. vulnerability assessment, detection, and monitoring
   c. vulnerability assessment, intrusion response, and investigation
   d. vulnerability assessment, intrusion response, and monitoring
5. List three common types of digital crime.
6. A corporate investigator must follow Fourth Amendment standards when conducting an investigation. True or False?
7. To what does the term “silver-platter doctrine” refer?
8. Policies can address rules for which of the following?
   a. when you can log on to a company network from home
   b. the Internet sites you can or cannot access
   c. the amount of personal e-mail you can send
   d. any of the above
9. List two items that should appear on an internal warning banner.
10. Warning banners are often easier to present in court than policy manuals are. True or False?
11. A corporate investigator is considered an agent of law enforcement. True or False?
12. List two types of computer investigations typically conducted in the corporate environment.

13. What is professional conduct and why is it important?

14. You can lose your job for violating a company policy, even if you don’t commit a crime. True or False?

15. What is the purpose of maintaining a professional journal?

16. iLook is maintained by ________________.

17. The U.S. ________________ maintains a manual on procedures to follow for search and seizure of computers.

18. Laws and procedures for PDAs are which of the following?
   a. well established
   b. still being debated
   c. on the law books
   d. none of the above

19. Why should companies appoint an authorized requester for computer investigations?

**Hands-On Projects**

**Hands-On Project 1-1**
Use a Web search engine, such as Google or Yahoo!, and search for companies specializing in computer forensics. Select three and write a two- to three-page paper comparing what each company does.

**Hands-On Project 1-2**
Research criminal law related to computer crime in your state or province. If laws exist, list the source and how long they have been in existence. Identify cases that have been tried using these laws.

**Hands-On Project 1-3**
Locate the computing use policies for your school or place of work. What surprises you most about the policies? Which are most effective? Which are not enforceable?
Hands-On Project 1-4
Compare Article 8 of the Charter of Rights of Canada or any country of your choice to the U.S. Fourth Amendment. How do they differ? How are they similar? Use sources such as the U.S. Department of Justice Web site to justify your conclusions in a paper at least two pages long.

Hands-On Project 1-5
Search the Internet for articles on computer crime prosecutions. Find at least two. Write one to two pages summarizing the two articles and identify any landmark decisions you find in your search.

Hands-On Project 1-6
Is there a high-tech criminal investigation unit in your community? If so, who are the participants? E-mail the person in charge and let him or her know you are taking a course in computer forensics. Ask what the unit's policies and procedures are, and then write one to two pages summarizing your findings.

Hands-On Project 1-7
Start building a professional journal for yourself. Find at least two electronic mailing lists you can join and three Web sites and read them on a regular basis. The electronic mailing lists should contain areas for OSs, software and hardware listings, people contacted or worked with, user groups, other electronic mailing lists, and the results of any research you have done thus far.

Hands-On Project 1-8
Examine and list your community, state, or country’s rules for search and seizure of criminal evidence. What concerns do you have after reading them?

Case Projects

Case Project 1-1
A lawyer in a law firm is suspected of embezzling money from a trust account. Who should conduct the investigation? If evidence is found to support the claim, what should be done? Write at least two pages explaining the steps to take, who is involved, and what items must be considered.
28 Chapter 1 Computer Forensics and Investigations as a Profession

Case Project 1-2
A private corporation suspects an employee is using password-cracking tools to gain access to other accounts. The accounts include employees in the Payroll and Human Resources departments. Write a two- to three-page paper outlining what steps to take, who should be involved, and what should be considered.

Case Project 1-3
An employee is suspected of operating his llama business using a company computer. It’s been alleged that he’s tracking the sales price of the wool and the cost of feed and upkeep on spreadsheets. What should the employer do? Write at least two pages explaining the tasks an investigator should perform.