EXTENDED LEARNING MODULE H

COMPUTER CRIME AND DIGITAL FORENSICS

Student Learning Outcomes

1. Define computer crime and list three types of computer crime that can be perpetrated from inside and three from outside the organization.
2. Identify the seven types of hackers and explain what motivates each group.
3. Define digital forensics and describe the two phases of a forensic investigation.
4. Describe what is meant by anti-forensics and give an example of each of the three types.
5. Describe two ways in which businesses use digital forensics.

Introduction

Computers play a big part in crime. They're used to commit crime, unfortunately. But they are also used to solve crimes. This should come as no surprise since computers are by now such an integral player in every part of our lives. Computers are involved in two ways in the commission of crime: as targets and as weapons or tools. A computer or network is a target when someone wants to bring it down or make it malfunction, as in a denial-of-service attack or a computer virus infection. Crimes that use a computer as a weapon or tool would include acts such as changing computer records to commit embezzlement, breaking into a computer system to damage information, and stealing customer lists. See Figure H.1 for examples of computer-related offenses in which computers are used as weapons/tools and targets of crime.

Some crimes are clearly what we call computer crimes, like Web defacing, denial-of-service attacks, e-mail scams, and so on. But as is the case in so many parts of our modern lives, computers are also so integrated into crime that it's hard to separate them out.

A member of a crime syndicate was sprayed with drive-by gunfire and was severely wounded. Believing that his services were no longer wanted by his crime gang, he switched sides, agreeing to become a witness for the state. The police secured an isolated intensive care unit room for him and guarded it heavily, allowing access only to medical staff and those on a very short list of visitors. Because the man was so badly wounded, there was a distinct danger of infection, and since he was allergic to penicillin, the doctor prescribed a synthetic alternative.

One evening, a nurse wheeling a medicine cart went through the police cordon and into the man's room. He injected the patient with penicillin, and the patient died shortly thereafter. An investigation started immediately and the nurse was potentially in big trouble. He insisted that when he looked at the patient's chart on the computer, there was an order there for penicillin. Subsequent examination of the computer records showed no such order. Eventually, it occurred to someone that perhaps a digital forensic expert should look at the computer angle more closely. Having retrieved the backup tapes (nightly backups are standard operating procedure in most places), the expert found evidence that exonerated the nurse. The patient chart had been changed in the computer to indicate penicillin and later changed back to its original form. Examination further revealed the point and time of access, and indicated that the medical record was changed

Figure H.1
Examples of Computer Crimes That Organizations Need to Defend Against

by someone outside the hospital. A hacker had electronically slipped into the hospital's network unnoticed, made the change, and slipped out again—twice.

Most crimes involving a computer are not as lethal as murder, but that doesn't mean they're insignificant. Organizations want to make sure their networks' defenses are strong and can prevent their computers from being used for unlawful or unethical acts. That's why so much time, money, and effort goes into security. We discussed security in Chapter 8.

This module focuses on the sort of threats that computer systems are susceptible to and the examination of electronic evidence. The latter is called *digital (or computer) forensics.*

LEARNING OUTCOME 1

Computer Crime

For our purposes, a ***computer crime*** is a crime in which a computer, or computers, play a significant part. See Figure H.2 for a list of crimes in which computers, although perhaps not essential, usually play a large part.

In this section we'll focus on crime from the organization's viewpoint. First, we'll examine some of the more high-profile types of computer crime committed against organizations that are perpetrated from the outside. Then we'll discuss the varying motivations of people who commit these acts. Lastly, we'll briefly discuss computer crime within the organization.

OUTSIDE THE ORGANIZATION

Computer security is a big issue in business. The concern is about people stealing electronic information, accessing systems without authorization, introducing viruses into networks, defacing Web sites, to name just a few of the dangers. The Computer Security Institute (CSI) together with the FBI's Computer Intrusion Squad have conducted studies every year since 1996 to assess the extent of the security problem nationwide. In their report based on the data for 2006, virus and worm attacks continued to be the cause of the largest cost financially. That problem together with unauthorized access; the theft of hardware like laptops, mobile phones, and PDAs; and the theft of information accounted for about three-quarters of the financial losses.

Figure H.2
Crimes in Which Computers Usually Play a Part

- Illegal gambling
- Forgery
- Money laundering
- Child pornography
- Hate message propagation
- Electronic stalking
- Racketeering
- Fencing stolen goods
- Loan sharking
- Drug trafficking
- Union infiltration

The good news was that the financial loss in 2006 decreased substantially compared to previous years, as did the average loss per company. Another good sign was that unauthorized access was down too. These trends are due to better security and better awareness on the part of employees. Another bit of good news was that more companies are reporting computer crime to law enforcement in greater numbers (25 percent) than they had in the previous two years. This may seem low compared to other types of crime, but companies are not keen on letting people know about security problems, especially when they are asking customers to trust them with credit card numbers and other important data. They are also concerned that competitors will use the information to their advantage and some don't realize it's of interest to law enforcement.

A large portion of attacks on computer systems are caused by ***malware,*** software designed to harm your computer or computer security.

VIRUSES Viruses are a type of malware. The term *computer virus* is a generic term for lots of different types of destructive software. A ***computer virus*** (or ***virus***) is software that was written with malicious intent to cause annoyance or damage. Two hundred new ones are developed every day.[1] There are two categories of viruses. The first category comprises benign viruses that display a message or slow down the computer but don't destroy any information.

Malignant viruses belong in the second category. These viruses do damage to your computer system. Some will scramble or delete your files. Others will shut your computer down, or make your Word software malfunction, or damage flash memory in your digital camera so that it won't store pictures anymore until you reformat it. Obviously, these are the viruses that cause IT staff (and everyone else) the most headaches.

Worms are the most prevalent type of malignant virus. A ***worm*** is a computer virus that replicates and spreads itself, not only from file to file, but from computer to computer via e-mail and other Internet traffic. Worms don't need your help to spread. They find your e-mail address book and help themselves to the addresses, sending themselves to your contacts. The first worm to attract the attention of the popular press was the Love Bug worm, and permutations of it are still out there.

THE LOVE BUG WORM Released on an unsuspecting world in 2000, the Love Bug worm caused the Massachusetts state government to shut down its e-mail, affecting 20,000 workers. It also caused problems on Capitol Hill and shut down e-mail in the British Parliament building. Companies as diverse as Ford Motor Company, H. J. Heinz, Merrill Lynch & Company, and AT&T were infected.[2] All in all, the Love Bug and its variants affected 300,000 Internet host computers and millions of individual PC users causing file damage, lost time, and high-cost emergency repairs totaling about $8.7 billion.[3,4]

A closer look at the Love Bug worm will give you a general idea of what worms do. The Love Bug arrives in your e-mail as an attachment to an e-mail message. The subject of the e-mail is "I LOVE YOU"—a very alluring message to be sure. The text says to open the attached love letter, the name of which is, appropriately, LOVE LETTER. However, what's attached is anything but love. It's a mean piece of software that is set loose in your computer system as soon as you open the attachment.

The Love Bug has three objectives: to spread itself as far and as fast as it can, to destroy your files, and to gather passwords and other information (see Figure H.3 on the next page). First, it spreads itself by mailing itself to everyone in your Outlook address book. (A previous worm of the same type named Melissa sent itself only to the first 50 people listed in Outlook's address book.) And, as if that weren't enough, it also uses your Internet chat software to spread itself to chat rooms.

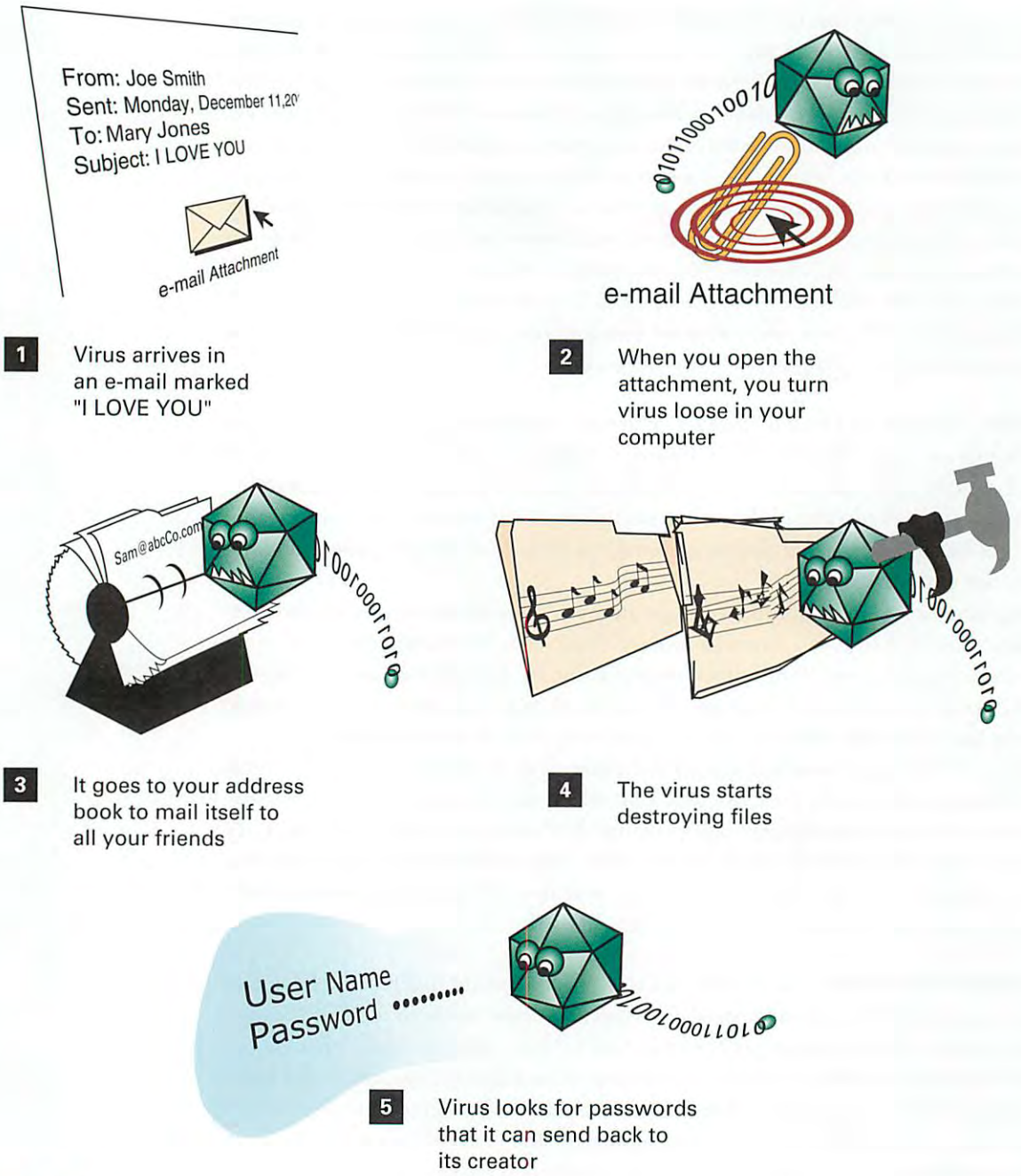


Figure H.3
The Love Bug Worm

Second, the Love Bug locates files on your computer that have certain extensions, .MP3 music files, .jpg picture files, .doc Word files, .xls Excel files, .wav sound files, .html browser files, and many others. Having found these files it wipes them out and puts itself in their place, appending .vbs to the end of the filename. For example, if you had a file called MySong.wav on your hard disk drive, the Love Bug virus would change the name to MySong.wav.vbs after it had done its dirty work.

Before it's done, the Love Bug worm changes your Internet Explorer start page and downloads a program that looks for passwords and network information, sending this information off by e-mail to the virus originator.[5]

There are at least 29 versions of the Love Bug virus. After people were warned not to open the LOVE LETTER attachment, the originators of the virus changed the name of it to something else. For example, one version is MOTHER'S DAY, and the body of the text says that the receiver has been charged hundreds of dollars for a Mother's Day "diamond special." You have to open the attachment to print the invoice, and then the virus goes into action.

The moral of the story is that you should be very careful about opening an attachment if you're not sure what it is and where it came from. That won't necessarily save you from all virus attacks, but it will certainly help a great deal.

SOBIG, SLAMMER, AND BLASTER The year 2003 was called the "worst year ever" for viruses and worms. Among the biggest, in terms of cost and name recognition, were the SoBig virus and the Slammer and Blaster worms.

There are several variations of mass-mailer viruses, but the SoBig virus is probably the best known. On Tuesday, August 19, 2003, the SoBig virus began spreading through networks generating e-mail traffic at levels never seen before. It arrived as an attachment in the victim's inbox with varying subject lines like "Your details," "Your application," and "Wicked screensaver." When the recipient opened the attachment, the virus searched through hard drives for e-mail addresses in document files, cached Web pages, and Microsoft Outlook Express databases. Then it sent out huge numbers of useless e-mail messages. At its peak, security experts estimate that 1 out of every 17 e-mail messages carried the SoBig virus, even more than the Love Bug's 1 in 20. It was estimated that SoBig sent out a mass mailing from infected computers—there were about 100,000 of those—at the rate of one every 10 minutes.

Postini Inc., an e-mail management and screening company, intercepted 1.9 million SoBig e-mails on their way to the company's customers on the first day of the virus's activation. By the next day the volume had increased to 3.5 million.

Whirlpool, a company with $11 billion a year in sales, says that about 95 percent of its sales come through the Internet and that its fast response to protect its 20,000 computers and 800 servers saved the company from suffering much damage. Others weren't so lucky. Experts say that part of the reason that SoBig was so effective was that it incorporated a line in its header that said "X-Scanner: Found to be clean," fooling a popular antivirus application that many Internet service providers use into letting the virus through.

SoBig was preprogrammed to stop replicating itself on September 10, 2003. By that time, it had infected more than 5 million e-mails. About eight times as many private computers were infected as corporate systems, since organizations moved faster to apply the patch that blocked the destruction.

Two of the many worms that hit networks in 2003 were the Slammer worm that hit in January and the Blaster worm that arrived in August. A worm looks for some flaw, or way to enter a computer, in software (often a Microsoft network operating system product) and sneaks in to do damage. Slammer kept flooding the victim server until its buffer memory was full, then it could trick that computer into sending out thousands of new copies to other servers that were vulnerable. Slammer sent out 55 million bursts of information per second onto the Internet and at that rate it took only 10 minutes for the worm to find and invade almost all the vulnerable servers. Microsoft had a patch (a way of plugging the entry point) available on its Web site, but if the network administrators didn't download and apply it, their networks remained vulnerable until they did.

The Blaster worm appeared only 26 days after Microsoft publicized the vulnerability that the worm utilized. Blaster spread like wildfire and among the thousands of companies that were affected were CSX, the third largest railroad company in North America, Amtrak, the commuter train company, and Air Canada. Passengers and freight in all three

organizations experienced delays as their network traffic ground to a halt. Commuter trains in Washington, D.C., were delayed for two hours while IT experts worked feverishly to clean out the worm's effects while Air Canada's phone-reservation system and some check-in processes were slowed down.[6,7,8,9]

STAND-ALONE VIRUSES In any given month, between 200 and 300 viruses are traveling from system to system around the world, seeking a way in to spread mayhem.[10] And they're getting more deadly. Whereas the Love Bug worm was a Visual Basic script virus (i.e., it needed Visual Basic to run), the latest worms can stand alone and run on any computer that can run Win32 programs (Windows 98 or later versions). Examples are SirCam, Nimda, and Klez. Nimda adds JavaScript to every home page on the server it infects, then passes it on to visitors to the site. Viruses of this independent type are very numerous.

The Klez virus is actually a family of worms that introduced a new kind of confusion into the virus business. They spoof e-mail addresses. ***Spoofing*** is the forging of the return address on an e-mail so that the e-mail message appears to come from someone other than the actual sender. Previous worms went to the recipient from the infected sender's computer and contained the infected person's return e-mail address. The worm found recipient addresses in the infected computer's address book.

Klez goes a step further and uses the address book to randomly find a return address as well as recipient addresses. The result is that people who are not infected with the virus get e-mail from the irate recipients and spend time looking for a virus they may not have. Even worse, some of the virus-laden e-mails look as though they came from a technical support person, leading an unsuspecting victim to open them, believing them to be safe.

TROJAN HORSE VIRUSES A type of virus that doesn't replicate is a Trojan-horse virus. A ***Trojan horse virus*** hides inside other software, usually an attachment or download. The principle of any Trojan horse software is that there's software you don't want hidden inside software you do want. For example, Trojan horse software can carry the ping-of-death program that hides in a server until the originators are ready to launch a DoS attack to crash a Web site.

Key-logger software is usually available in Trojan horse form, so that you can hide it in e-mail or other Internet traffic. ***Key logger,*** or ***key trapper, software*** is a program that, when installed on a computer, records every keystroke and mouse click. Key logger software is used to snoop on people to find out what they're doing on a particular computer. You can find out more in Chapter 8.

MISLEADING E-MAIL One type of misleading e-mail is a virus hoax. This is e-mail sent intending to frighten people about a virus threat that is, in fact, bogus. People who get such an alert will usually tell others, who react in the same way. The virus is nonexistent, but the hoax causes people to get scared and lose time and productivity. Within companies the losses can be very severe since computer professionals must spend precious time and effort looking for a nonexistent problem.

Following are some general guidelines for identifying a virus hoax.[11]

- Urges you to forward it to everyone you know, immediately.
- Describes the awful consequences of not acting immediately.
- Quotes a well-known authority in the computer industry.

These are signs that the e-mail is not meant to help but to cause harm. If you get such an e-mail, delete it immediately.

Another type of misleading e-mail is designed to get people to actually take action that results in setting a virus loose or to do something that will disrupt the functioning of their own computers. The first step is usually to make people believe that they have inadvertently e-mailed a virus to others. They get a message (maybe it purports to come from Microsoft) that they have sent out a virus and that they need to run an attached program or delete a file to fix the problem. They then do what the e-mail says believing it to be genuine, and furthermore, they e-mail everyone they sent messages to telling them about the problem. The recipients e-mail the people in their address books and so on. Be advised that Microsoft *never* sends out attachments in any official e-mail in a public mass mailing. It's possible that Microsoft may e-mail you warning you of a problem, but it will only indicate where you can download a file to take care of it. Before you delete a file from your computer, which may be an important system file without which your computer can't function, ask someone who knows or check out the various Web sites that keep up with the latest viruses, like www.symantec.com.

DENIAL-OF-SERVICE ATTACKS Many organizations have been hit with denial-of-service attacks. ***Denial-of-service (DoS) attacks*** flood a server or network with so many requests for service that it slows down or crashes. The objective is to prevent legitimate customers from getting into the site to do business. There are several types of DoS attacks. A DoS attack can come from a lone computer that tries continuously to access the target computer, or from many, perhaps even thousands, of computers simultaneously. The latter is called a distributed denial-of-service attack and is considerably more devastating.

DISTRIBUTED DENIAL-OF-SERVICE ATTACKS ***Distributed denial-of-service (DDos) attacks*** are attacks from multiple computers that flood a server or network with so many requests for service that it slows down or crashes. A common type is the Ping of Death, in which thousands of computers try to access a Web site at the same time, overloading it and shutting it down. A ping attack can also bring down the firewall server (the computer that protects the network), giving free access to the intruders. E*Trade, Amazon.com, and Yahoo!, among others, have been victims of this nasty little game. The process is actually very simple (see Figure H.4 on the next page).

The plan starts with the hackers planting a program in network servers that aren't protected well enough. Then, on a signal sent to the servers from the attackers, the program activates and each server "pings" every computer. A ping is a standard operation that networks use to check that all computers are functioning properly. It's a sort of roll call for the network computers. The server asks, "Are you there?" and each computer in turn answers, "Yes, I'm here." But the hacker ping is different in that the return address of the are-you-there? message is not the originating server, but the intended victim's server. So on a signal from the hackers, thousands of computers try to access E*Trade or Amazon.com, to say "Yes, I'm here." The flood of calls overloads the online companies' computers and they can't conduct business.

For many companies, a forced shutdown is embarrassing and costly but for others it's much more than that. For an online stockbroker, for example, denial-of-service attacks can be disastrous. It may make a huge difference whether you buy shares of stock today or tomorrow. And since stockbrokers need a high level of trust from customers to do business, the effect of having been seen to be so vulnerable is very bad for business.

MALWARE BOTS AND ROOTKITS A vital component of the increase in the spread of viruses and denial-of-service attacks is the use of bots. A ***bot*** is a computer program that runs automatically. Bots (the term comes from robot) can perform all sorts of tasks,

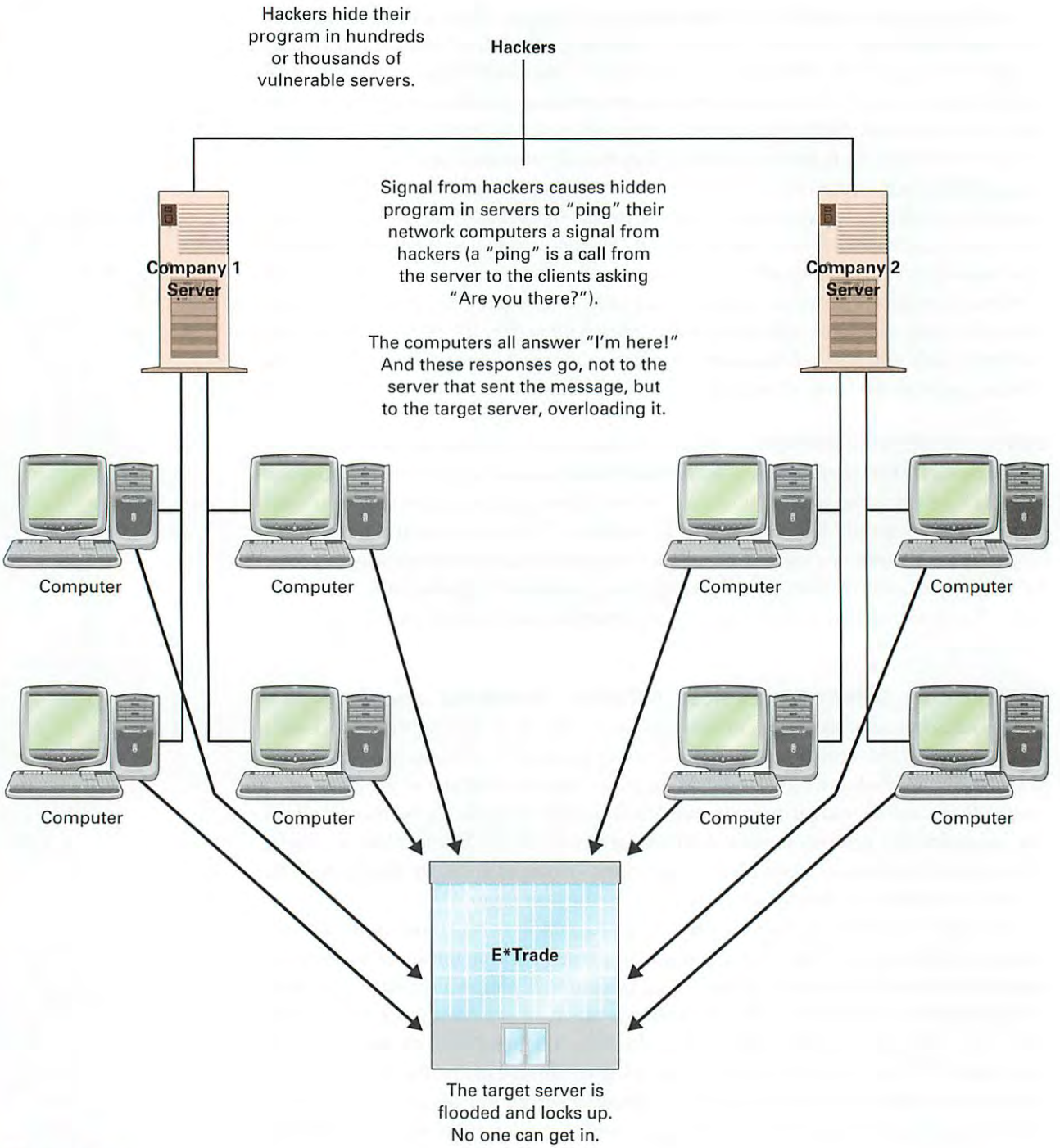


Figure H.4
Distributed Denial-of-Service Attack

both good and evil. In Chapter 4, Decision Support and Artificial Intelligence, you saw how bots take the form of intelligent agents, finding information and automatically performing computer-related tasks. Two examples are bots or intelligent agents that continuously monitor networks to find a problem before it knocks out the network and shopping bots that find products and services on the Internet for you.

However, there's another class of bots—the kind that are used for fraud or sabotage. In *Extended Learning Module E, Network Basics,* you learned that bots (software robots) can be used to break into computer systems. Having placed the unauthorized code into

a computer, attackers set up servers that are used for such things as distributing illegal copies of movies, music, and software. These compromised machines may be used to distribute kits for breaking into other computers. Malware bots are designed to be controlled by an attacker to perform unauthorized work over some period, like sending out spam or becoming part of a denial-of-service attack. Estimates are that about three-quarters of all spam mailings come from this source.

A ***malware bot*** is a bot that is used for fraud, sabotage, DoS attacks, or some other malicious purpose. It allows an unauthorized user to take control of a host computer without the victim's knowledge or permission. The term *bot* is sometimes used to mean a compromised machine, i.e., a computer that has been compromised with a bot. Bot-infected computers are also called ***zombies*** or ***drones.***

Malware bot activity has become very sophisticated over the past few years and there is a whole underground society in the bad bot business. The lowest level of the underground comprises the people who find vulnerable machines and install bad bots. The next level up are *bot herders.* Bot herders assemble battalions of bot-infected computers and sell this network of bots or botnet to people who are called fraudsters. A ***botnet*** is a network of malware-bot infected computers. Bot herders typically sell their networks for about $1 per machine, but the price can go up to $100 per system, per month, for access to a major organization that has lots of valuable information like customer and employee data. The fraudsters, in turn, use the botnet to steal this customer and employee data along with intellectual property, and anything else of value that they can get access to. Computers in organizations as varied as the Department of Defense and Colton School District in California have been compromised. Here are two other examples:

- In early November 2006, the computer of a water plant worker in Harrisburg, Pennsylvania, was invaded by a bot which then spread to the organization's server, which was hijacked into becoming part of a botnet that was then used to send out spam.[12]
- One Sunday morning in 2005, the Seattle's Northwest Hospital & Medical Center computer system was very slow and documents wouldn't print. The next day things got worse as lots of strange things started happening. The operating-room doors stopped opening, doctors' pagers wouldn't work, and computers in the intensive care unit shut down. It was all the result of a botnet attack. Three teenagers in California managed to infect a single computer with a bad bot. The code spread and soon all the computers in the network had become part of a botnet. The hospital had to wipe several hard drives clean and reinstall software at a cost of $150,000. The oldest of the teenagers, who was 19, was sentenced to 37 months in federal prison and ordered to pay compensation to the hospital.[13]

Malware bots can infect a computer in any one of a number of ways including operating system or application vulnerabilities, e-mail, instant messaging, and computer viruses. One very effective way of commandeering computers is to use a *rootkit.* It's hard to detect and even when detected, it's hard to remove. A rootkit is a Trojan-horse type program that is activated when you start your computer. It carries code that, once inside, can do whatever it was programmed to do.

A ***rootkit*** is software that gives you administrator rights to a computer or network and its purpose is to allow you to conceal processes, files, or system data from the operating system. It can be used to carry code to perform virtually any type of malicious activity. It can take full control of a system and use that computer or network for spam, denial-of-service, or spyware, and, more chillingly, create a "backdoor" into the system for the attacker, who can then commandeer the system to be part of a botnet.

An attacker exploits an operating system vulnerability to get a rootkit onto your computer. A rootkit is hard to detect since it runs while the operating system is starting and looks to the operating system like it belongs.

Probably the most widely publicized example of a rootkit was the one that Sony put into CDs and DVDs as part of a copy protection scheme in 2005. It got onto your computer when you played the disc and was then exploited by hackers. See the Industry Perspective box in Chapter 8, "Is Your Music CD Hijacking Your Computer?"

WEB DEFACING

Web defacing is a favorite sport of some of the people who break into computer systems. They replace the site with a substitute that's neither attractive nor complimentary. Or perhaps they convert the Web site to a mostly blank screen with an abusive or obscene message, or the message may just read "So-and-so was here." In essence, Web site defacing is electronic graffiti, where a computer keyboard and mouse take the place of a paint spray can. The *USA Today* Web site was once a victim. The *USA Today* Web site was attacked in July 2002, causing the newspaper to shut down the whole site for three hours to fix the problem. The hackers replaced several news stories on the site with bogus stories that were full of spelling errors. One story said that the Pope had called Christianity "a sham." The phony stories were only on the site for 15 minutes before they were spotted and the site was taken offline.[14]

LEARNING OUTCOME 2

THE PLAYERS

Who's spreading all this havoc? The answer is hackers. This is the popular name for people who break into computer systems. ***Hackers*** are knowledgeable computer users who use their knowledge to invade other people's computers. There are several categories of hackers, and their labels change over time. The important thing to note in the following discussion is that the motivation and reasons for hacking are as many and varied as the people who engage in it.

THRILL-SEEKER HACKERS ***Thrill-seeker hackers*** break into computer systems for entertainment. Sometimes, they consider themselves to be the "good guys" since they expose vulnerabilities and some even follow a "hackers' code." Although they break into computers they have no right to access, they may report the security leaks to the victims. Their thrill is in being able to get into someone else's computer. Their reward is usually the admiration of their fellow hackers. There's plenty of information on the Web for those who want to know how to hack into a system—about 2,000 sites offer free hacking tools, according to security experts.

WHITE-HAT HACKERS The thrill-seeker hackers used to be called white-hat hackers. But lately, the term *white-hat* is being increasingly used to describe the hackers who legitimately, with the knowledge of the owners of the IT system, try to break in to find and fix vulnerable areas of the system. These ***white-hat hackers,*** or ***ethical hackers*** are computer security professionals who are hired by a company to break into a computer system, so as to find security lapses. These hackers are also called counter hackers, or penetration testers.

BLACK-HAT HACKERS ***Black-hat hackers*** are cyber vandals. They exploit or destroy the information they find, steal passwords, or otherwise cause harm. They deliberately cause trouble for people just for the fun of it. They create viruses, bring down computer systems, and steal or destroy information.

A 16-year-old black-hat hacker was sentenced to detention for six months after he hacked into military and NASA networks. He caused the systems to shut down for three weeks. He intercepted more than 3,000 e-mails and stole the names and passwords of 19 defense agency employees. He also downloaded temperature and humidity control software worth $1.7 billion that helps control the environment in the international space station's living quarters.[15]

CRACKERS ***Crackers*** are hackers for hire and are the people who engage in electronic corporate espionage and other profitable ventures. This can be a pretty lucrative undertaking, paying up to $1 million per gig. Typically an espionage job will take about three weeks and may involve unpleasant tasks like dumpster diving to find passwords and other useful information and "social engineering." ***Social engineering*** is conning your way into acquiring information that you have no right to. Social engineering methods include calling someone in a company and pretending to be a technical support person and getting that person to type in a login and password, sweet talking an employee to get information, and for difficult jobs, perhaps even setting up a fake office and identity.

HACKTIVISTS ***Hacktivists*** are politically motivated hackers who use the Internet to send a political message of some kind. The message can be a call to end world hunger, or it can involve an alteration of a political party's Web site so that it touts another party's candidate. It can be a slogan for a particular cause or some sort of diatribe inserted into a Web site to mock a particular religious or national group.

Hacktivism, in the form of Web defacing, is becoming a common response to disagreements between nations. When the U.S. military plane made an emergency landing in China and a dispute arose about the return of the crew and plane, U.S. hackers started to attack Chinese Web sites, and Chinese hackers returned the favor, targeting government-related sites.

CYBERTERRORISTS Since the September 11, 2001, terrorist attacks on New York and the Pentagon, officials have become increasingly worried about the threat of *cyberterrorists.* This group of hackers, like the hacktivists, is politically motivated, but its agenda is more sinister. A ***cyberterrorist*** is one who seeks to cause harm to people or destroy critical systems or information. Possible targets of violent attacks would be air traffic control systems and nuclear power plants, and anything else that could harm the infrastructure of a nation. At a less lethal level, cyberterrorist acts would include shutting down e-mail or even part of the Internet itself, or destroying government records, say, on social security benefits or criminals.

However, the FBI and other government agencies are very much aware of the threats they face from computer-based attacks, and have taken steps to protect the infrastructure that supports cyberspace. They can enjoy a reasonable expectation of success since a computer system is a lot easier to protect than public structures like buildings and bridges.

SCRIPT KIDDIES ***Script kiddies*** or ***script bunnies*** are people who would like to be hackers but don't have much technical expertise. They download click-and-point software that automatically does the hacking for them. An example of this was the young man in Holland who found a virus toolkit on the Web and started the Kournikova worm. It was very similar to the Love Bug worm in that it sent itself to all the people in the Outlook address book. Tens of millions of people got the virus after opening the attachment hoping to see a picture of Anna Kournikova.[16]

The concern about script kiddies, according to the experts, apart from the fact that they can unleash viruses and denial-of-service attacks, is that they can be used by more sinister hackers. These people manipulate the script kiddies, egging them on in chat rooms, encouraging and helping them to be more destructive.

Digital Forensics

LEARNING OUTCOME 3

When a disturbed student at Virginia Tech went on a killing rampage in April 2007, one of the first things that law enforcement investigators did was to collect all of his information devices, like his computer system and his cell phone. They used the information they retrieved to piece together a picture of the young man and the events that preceded the tragic event.

It was not the first time electronic information was helpful in untangling criminal mysteries. Astonishingly, digital forensics solved a case that had been open for 30 years, and identified Dennis Rader as the BTK (bind, torture, kill) killer.

In 2005 Dennis Rader, a.k.a. the BTK killer, was convicted of killing 10 women over three decades. The BTK strangler had taunted police and the media over many years through letters and packages, some of which contained photos of the victims. But it was the package containing a floppy diskette that he sent to a TV station on February 16, 2005, that finally led to his capture. The TV station turned the diskette over to police, who in turn, called in digital forensics investigators. They found evidence of a deleted file that referenced the Christ Lutheran Church in Wichita. Police asked the church to allow them to examine its computer and found that Rader had used it to print out a church meeting agenda. Then they got a warrant to examine the computer in Rader's home and found evidence that he was, indeed, the BTK strangler that they had been looking for for three decades.[17]

There are many more such cases. Here is a sampling:

- The case against Thomas Murray, an English professor who killed his wife, was strengthened when, during the investigation, police found e-mails he had sent to his wife and friends. The messages showed how upset he was with the fact that his wife was divorcing him and taking their daughter to California. Digital forensics experts found that he had done Yahoo! searches for "how to make a bomb," "murder for hire," "how to hire an assassin," and "how to murder someone and not get caught." He was convicted and sentenced to 25 years in prison.
- A search that ended on March 5, 2002, uncovered 339 discarded bodies on the grounds of Tri-State Funeral home in Walker County, Georgia. Ray Brent Marsh was formally charged with multiple counts of abusing a corpse and almost two hundred counts of fraud for allegedly taking money for cremations that were not performed and for giving loved ones fake remains. Photos of the dead bodies arranged in lewd poses appeared on the Internet.
- In November 2004, Scott Peterson was convicted of killing his wife Laci and the couple's unborn son, Connor. Both bodies washed ashore separately in San Francisco Bay during April 2003. While gathering evidence to solve the crime, police had searched the hard drives of four computers in the Petersons' home. On a notebook computer they found that someone had examined maps, fishing reports, and charts of water currents in the Bay Area just before Laci disappeared. Someone at the couple's home, presumably Scott, had also done searches for keywords like divorce, silencer, and shooter.

What all these news stories have in common is the investigative technique that unearthed crucial information—the process of finding, examining, and analyzing electronic information saved on computer storage media or handheld devices like cell phones. This process is called *computer* or *digital forensics.* (Since computer forensics is no longer limited to desktop and notebook computers, the term *digital forensics* is becoming the term that is widely used.) Many digital forensics investigations involve intellectual property cases, where a company believes that an employee is secretly copying and perhaps selling proprietary information such as schematics, customer lists, financial statements, product designs, or notes on private meetings. Other investigations involve child exploitation, domestic disputes, labor relations, and employee misconduct cases.

Digital forensics is the collection, authentication, preservation, and examination of electronic information (often for presentation in court). Electronic evidence can be found on any type of computer storage media, such as hard disks, CDs, flash cards, USB devices, Pocket PCs, cell phones, and pagers.

There are two basic motivations for engaging in digital forensics. The first is to gather and preserve evidence to present in court. The second is to establish what activities have occurred on a computer, often for the purpose of dispute settlement. Evidentiary standards differ for criminal and civil cases. In criminal cases, the standard is "beyond a reasonable doubt." In civil cases, it's the "preponderance of evidence." For instance, you may find yourself in a situation that doesn't require the involvement of the legal system. Suppose you have an employee that you suspect has been using the company's computer system to gamble online. In this case your proof standard can be lower, perhaps just enough to fire the person while reducing the risk of being named in a wrongful termination lawsuit.

In a well-conducted digital forensics investigation, there are two major phases: (1) collecting, authenticating, and preserving electronic evidence; and (2) analyzing the findings.

THE COLLECTION PHASE

Step one of the collection phase is to get physical access to the computer and related items. Thus, the digital forensic team collects computers, cell phones, pocket PCs, disks, printouts, post-it notes, and so on and takes them back to the lab. This process is similar to what police do when investigating crime in the physical world, collecting hair, clothing fibers, bloodstained articles, papers, and anything else that they think might be useful. The crime investigators usually take these potential clue carriers with them and secure them under lock and key, where only authorized personnel may have access, and even they must sign in and out.

Digital forensic experts use the same kind of protocol. To conduct a thorough investigation, they first take digital photos of the surrounding environment and start developing extensive documentation. Then they start collecting anything that might store information. The hard disk is an obvious place to look, but digital forensic investigators also collect any other media where information might be stored (see Figure H.5 on the next page). If they can't take a clue source with them, they secure it and create an exact copy of the contents of the original media.

As well as electronic media, investigators collect any other potentially helpful items, especially passwords, for use in case any of the files they come across are encrypted or are otherwise difficult to access. Apparently, a favorite hiding place for passwords that people write down (which you should *not* do) is under the keyboard, so that's the first place that investigators look. Then they look in desk drawers and anywhere else that passwords might be, perhaps on post-it notes or slips of paper. Some people keep all

- Floppy disks
- CDs
- DVDs
- PDAs
- USB drives
- Flash memory cards, like an xD-Picture card, CompactFlash card, or similar storage medium for digital cameras and other devices
- Backup tapes of other media
- USB mass storage devices such as Thumb drives
- Voice mail
- Cell phones
- Electronic calendars
- MP3 players and IPods
- Scanner
- Pocket PCs
- Photocopiers
- Fax machines

Figure H.5
Where You Might Find Electronic Evidence

their passwords and PINs in the **My Documents** folder. This certainly makes life easier for digital forensics examiners—and for thieves. Passwords don't help much since, with a password cracker program like Passware, anyone can get the password in seconds. Other helpful items might be printouts and business cards of associates or contacts of the person being investigated.

Step two of the collection process is to make a forensic image copy of all the information. A ***forensic image copy*** is an exact copy or snapshot of the contents of an electronic medium. It is sometimes referred to as a bit-stream image copy. To get a forensic image copy, specialized forensic software copies every fragment of information, bit-by-bit, on every storage medium—every hard disk (if there's more than one), every floppy disk, every CD, every USB drive and flash memory card. That's usually a lot of stuff. Remember that a CD holds about a half gigabyte of information, and you can build a hard disk array (several hard disks tied together into one unit) that holds a terabyte (one trillion bytes) or more. It can take a long, long time to copy it all. And the investigator must be able to swear in court that he or she supervised the entire copying process, and that no one and nothing interfered with the evidence. This could mean sitting in the lab literally for days just copying files. Also, many experts advise that the investigator make two copies of everything in case there's a problem later with the first copy.

By the end of 2004 there were 600 cell phone networks in more than 200 countries serving more than 1.5 billion users—and that's just GSM type cell phones (the type that Cingular uses and the one that is the most popular in Europe).[18] The number of people who have personal computers is only one-third of that. Over 800,000 cell phones were sold in 2006 alone and this number is expected to keep rising. Since cell phones and other handheld devices also store important information on user activity, they're also part of the collection process.

Cell phones are simply a specialized type of computer. Since there are so many people using cell phones, it stands to reason that some of them are using the handy devices to commit crime. The list of cell phone crimes includes much of the illegal activity that's possible with computers (or without them) and some that's unique to cell phones. Some examples are:

- Illegal drug deals.
- Stealing data and storing it on a cell phone.
- Stealing the cell phone to fraudulently obtain goods and services. A variation on this theme is stealing subscriber information and using it to create duplicate accounts which are then used to purchase goods from the Internet using the original subscribers' accounts. These crimes are particularly prevalent in Europe and Japan, where people use their cell phones to buy snacks and drinks out of vending machines, pay parking tickets, make credit card payments, and engage in a host of other types of mobile commerce.
- On a vastly more serious scale, cell phones have been used by terrorists to set off explosives. This happened in Madrid in 2004 when bombs went off in commuter trains; at Hebrew University in Jerusalem in 2002, when seven people died; and in Bali outside a night club in 2002 and in the Jakarta Marriott.[19]

THE AUTHENTICATION AND PRESERVATION PROCESS To get a forensic image copy of hard disk and other media contents, investigators physically remove the hard disk from the computer. They never turn the suspect computer on, because when the PC is turned on, Windows or Vista performs hundreds of changes to files. Access dates change, and so do temporary files, and so on. So, once turned on, the hard drive is no longer exactly the same as it was when it was shut down.[20] Thus, opposing counsel could argue that this is not the same hard disk that the suspect used.

Having removed the hard disk, investigators connect it to special forensic hardware that can read files but can't write or rewrite any medium. (They prefer to remove storage devices, but if that's not possible, they copy the contents in place using cables.) Then they use forensic software like EnCase to extract a forensic image copy of the original medium without changing the files in any way.

How do we know that nothing changed on any disk during the entire investigation, from the time the computer was seized up to the present time? That's the question that opposing counsel will ask the computer forensic expert on the witness stand. So, during the collection phase and later, the analysis phase, the investigators have to make absolutely sure that evidence to be used in a trial could not have been planted, eliminated, contaminated, or altered in any way. This is a basic evidentiary rule for all court proceedings. They have to be able to document a chain of custody and be able to account for the whereabouts and protection of evidence. To help establish a complete chronology of activity, investigators also check the BIOS, which a computer uses to time and date stamp files and actions like deleting, updating, and so on.

In a digital forensic investigation, investigators use an authentication process so that they can show sometime in the future—perhaps even five or six years later—that nothing changed on the hard drive or other storage medium since seizure. They can do this with an MD5 hash value. An ***MD5 hash value*** is a mathematically generated string of 32 letters and digits that is unique for an individual storage medium at a specific point in time. The MD5 hash value is based on the contents of that medium. Any change in the content changes the MD5 hash value.

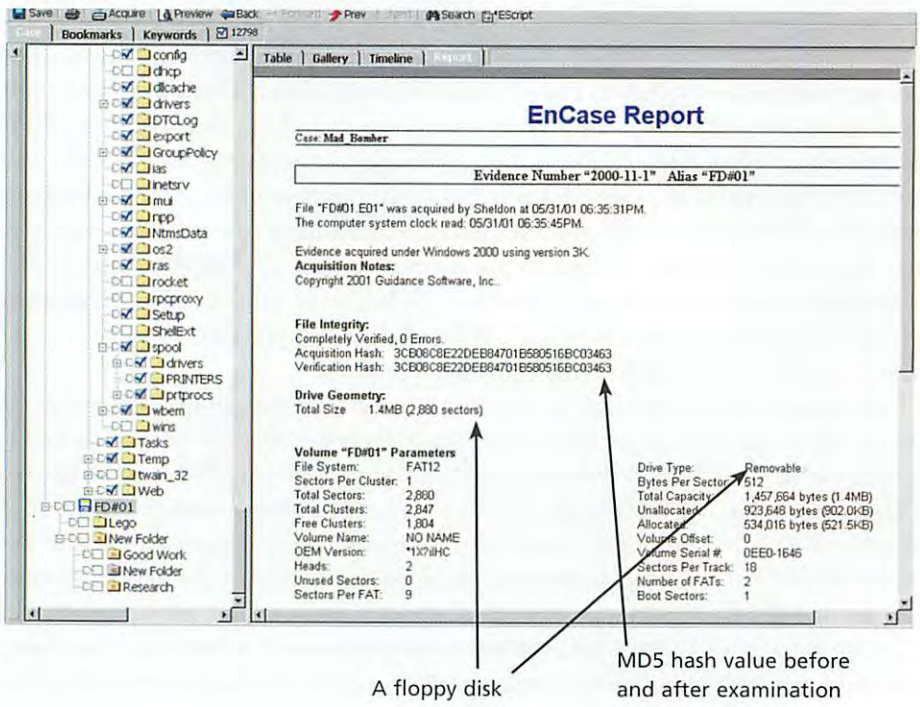
A hash value is a seemingly meaningless set of characters. It's the result of applying a mathematical algorithm to a large block of data to reduce it to a small set of characters.

For example, a hash value could be the sum of the ISBNs and the number of pages in all the books on a bookstore shelf. The result, which would be a mixture of ISBN codes and quantities of pages, would be meaningless for anything except identification. If a book, or even a page, were added to or removed from the shelf, the hash total would change, so the contents of the shelf could be shown not to be the same as they were when the hash value was originally computed. Similarly, adding so much as one space in one tiny Word document on a disk will change the MD5 hash value. See Figure H.6 for an example of an MD5 hash value generated by EnCase forensic software.

MD5 hash values are considered very reliable and have become an industry standard accepted by the FBI, the U.S. Marshall Service, and most other law enforcement authorities, as well as private professional firms, as a way of uniquely authenticating a set of contents on a particular storage medium. This confidence in MD5 hash values is based on the fact that the probability of two hard disks with different contents having the same MD5 hash value is 1 in 10 to the 38th power: that's 1 with 38 zeros behind it. This makes the MD5 hash value a sort of DNA or fingerprint for computer media contents. Actually, it's more reliable than those physiological identifiers, since the probability of two sets of hard disk contents resulting in the same MD5 hash value are less than the odds of two individuals' DNA and fingerprints being identical. As an example of this probability, consider that you would have better odds of winning the Powerball lottery 39 times in your lifetime than you would of finding two hard disks with different contents that have matching MD5 hash values.

In 2005 some researchers managed, under closely controlled circumstances and with a lot of computer power and sophisticated mathematics, to cause a collision of MD5 hash values, i.e., caused two different blocks of data to yield the same MD5 hash value. This precipitated much discussion in the digital forensics industry about the reliability of MD5. Since the chances of a collision are so very small, MD5 continues to be used. However, a new method of generating a hash value has emerged. This one is called *SHA* and it has an even lower probability of yielding the same value for two different blocks of data. Some software, such as FTK, which is another software package that digital

Figure H.6
MD5 Hash Value



forensics experts use for forensic examinations, generates SHA instead of MD5 for authentication purposes.

CELL PHONES AND OTHER HANDHELD DEVICES When it comes to cell phones and other handheld devices, the most frequently used software is Device Seizure developed by Paraban. EnCase has recently added Nutrino, which is a similar product. The procedure is to use Device Seizure to recover the data itself and then a program that uses hex dumping to get headers, footers, dates, and so on. This kind of software also finds deleted files in unallocated space. Device Seizure is often the forensic tool of choice for investigators partly because it does not allow data to be changed on the device. This is one of the strongest features of EnCase, the forensic tool used to investigate desktop and notebook computers. Since the handheld part of the industry is not as well established as the forensic examination of desktop and notebook computers, there aren't as many tools available.

Adding to the complexity is the huge range of designs in the handheld world. What kind of data and how much of it is stored on a cell phone, for example, depends on many factors such as the manufacturer, the options chosen by the user, the software it uses, and so on. Cell phones that have PDA (Personal Digital Assistant) features are becoming more widely used and these usually have flash memory cards such as an SD card. See Figure H.7 for a partial list of the types of information that can be recovered from a cell phone.

FORENSIC HARDWARE AND SOFTWARE TOOLS As we've already mentioned, digital forensic experts use special hardware and software to conduct investigations. Usually the computer system has more power than the standard computer on a desktop and much more RAM, as well as much more hard disk capacity. This is to speed up the copying and analysis process. Digital forensic experts are also very careful not to let static electricity cause any damage or changes to magnetic media (like hard disks, Zips, and floppies). Therefore they use nonconductive mats under all computer parts, and wear wristbands that connect by wire to the ground of an electrical outlet. And just in case they need a tool, such as a screwdriver, they have a special nonmagnetic set of tools nearby, too.

- Phone book
- Subscriber, equipment, and service provider identifiers
- Calendar
- To-Do list
- Phone number log and most recently dialed numbers
- E-mail
- Web activity
- Text messages and multimedia messages
- Voice mail
- Electronic documents
- Last active location and other networks encountered
- Graphics, photos and videos

Figure H.7
Recoverable Cell Phone Information

There are many kinds of software in a Digital forensics toolkit, in addition to forensic software, that can help in digital forensic investigations. Quick View Plus, used by many forensic experts, is an example. This is software that will load Word, Excel, image, and many other file formats. If it comes across a file with an .xls extension, which is actually an image and not a spreadsheet file, Quick View will show the file as an image regardless of its extension. That saves the investigator having to try it in multiple programs after loading fails in Excel. Conversions Plus is a package that does the same sort of thing. Other helpful software includes Mailbag Assistant, which reads many e-mail formats, and IrfanView, which is an image viewer that will read most picture files. Gargoyle is software that identifies encrypted files and can decrypt some of them.

Ingenium is software that does latent semantic analysis also known as concept searching. This means that it can search for your *meaning* rather than just terms that match exactly. For example, if you type in "house" as a search term, the software will search for cottage, hut, domicile, home, property, estate, holdings, manor, housing, mansion, cabin, bungalow, chalet, lodge, residence, dwelling, abode, residence, habitat, etc. It uses a neural network to find other terms that are close in meaning to your search term. You can learn more about neural networks in Chapter 4, Decision Support and Artificial Intelligence.

We have been using the EnCase forensic software for this discussion, but it's not the only package that's available. Helix and FTK are other examples of this kind of software. For investigations that might be headed toward litigation, digital forensic experts often use EnCase, since it's widely accepted as robust and reliable. EnCase has routinely been judged acceptable by courts in meeting the legal standard for producing reliable evidence.

Figure H.8

Some of the Files Recoverable from Storage Media

E-Mail Files
• E-mail messages
• Deleted e-mail messages
Program Files and Data Files
• Word (.doc) and backup (.wbk) files
• Excel files
• Deleted files of all kinds
• Files hidden in image and music files
• Encrypted files (with keys or passwords)
• Compressed files
Web Activity Files
• Web history
• Cache files
• Cookies
Network Server Files
• Backup e-mail files
• Other backup and archived files
• System history files
• Web log files

As you've already seen, the most frequently used forensic software for handheld devices is Device Seizure by Paraban, which is the equivalent of EnCase, but for cell phones and Pocket PCs. Guidence Software, the company that makes EnCase, sells Nutrino—a newcomer to the industry—for handheld devices. There are other options on the market too and they, like all forensic tools, keep improving. Since handheld device investigation is still so recent, national standards have not yet evolved in this arena.

THE ANALYSIS PHASE

The second phase of the investigation is the analysis phase when the investigator follows the trail of clues and builds the evidence into a crime story. This is the phase that really tests the skill and experience of the investigators. The analysis phase consists of the recovery and interpretation of the information that's been collected and authenticated. If all the necessary files were there in plain sight with names and extensions indicating their contents, life would be much easier for the forensic investigator, but that's seldom the case. Usually, particularly if those being investigated know that they're doing something wrong, the incriminating files will have been deleted or hidden.

Investigators can recover all of a deleted file pretty easily as long as no new information has been written to the space where the file was. But they can also recover fragments—perhaps rather large fragments—of files in parts of a disk where new files have been written, but have not completely filled the space where the old file was. With the appropriate software they can recover files or fragments of files from virtually any part of any storage medium (see Figure H.8).

Digital forensic programs can pinpoint a file's location on the disk, its creator, the date it was created, the date of last access, and sometimes the date it was deleted, as well as file formatting, and notes embedded or hidden in a document (see Figure H.9).

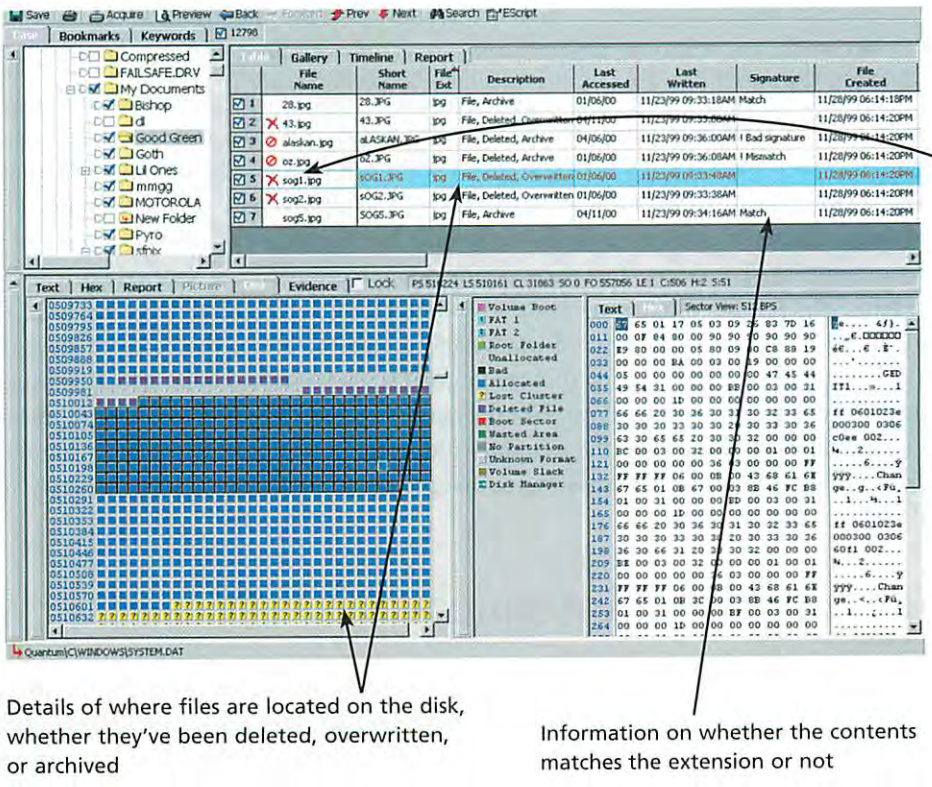


Figure H.9
History of File Activity

Also stored on the hard disk is information about where the computer user went on the Web. For example, every graphic image you view on the Internet is copied to your hard disk, usually without your knowledge. In addition, Web servers have information on which computer connected to the Web and when. The same server can also tell you the sites visited by the user of that computer, the date and time of the visits, and the actions of the user at the site. These attributes are useful if the suspect claims to have reached an inappropriate site by accident, since delving deeper into the site implies a deliberate action. And, of course, if a password was required to reach the material in question, you can rest your case.

LIVE ANALYSIS The usual digital forensic examination is conducted when the computer or computers are off. However, there are situations where this may not be possible or even the best course of action. So, the forensic team has to gather the information they need while the system is still running. For such an analysis to be acceptable there has to be a good reason for not following the more traditional procedure—an examiner won't get away with saying that it was simply too much work to do the usual type of examination. A *live analysis* is the term used to describe an examination of a system while it is still running. It may be necessary under certain circumstances such as:

- If the company hosts a Web site that takes customer orders. In this situation a complete shutdown would cost the company precious business, and a judge might consider such action as an "undue burden" on the company.
- If information is needed that is in RAM and the examiner pulls the plug that information will be lost. So in this case it would actually be better for the forensic experts to get data from a computer that's still running. For example, if someone is caught red-handed using a computer for some illicit activity it might be much better to get a memory dump from the system rather than pull the plug which would wipe out the contents of volatile RAM.
- With hard disk storage now in the terabyte range, it's simply too wasteful to copy all the data when only a small portion of it is relevant to the investigation. Under these circumstances, it may be acceptable to extract only certain well-defined portions.

In a live analysis, the examiner doesn't make a forensic image of the disk and, therefore, there's no MD5 hash value. This is a big disadvantage in making a case. All you have is a momentary snapshot of what's going on within that system. On the plus side, examiners can glean information from memory (RAM) and on processes and services that are running and also on open ports on the computer. Live analysis can also defeat on-the-fly encryption (OTFE) systems that encrypt drives when the system is shut down.

Helix, which is freeware, is one widely used tool for this type of analysis and has been endorsed by EnCase. This type of examination is still in the early stages of development and there are not yet many tools with good track records. Helix, which is Linux-based, provides a utility that allows examiners to download a PDF file, which is not easily changeable, detailing what the examiner did in the correct sequence and what tools were used. This provides some assurance that the examiner did what was necessary and followed proper procedure.

Recovery and Interpretation

As with all evidence, the analysis of the electronic clues and the assembling of the pieces into a credible and likely scenario of what happened are very important. Much of the information may come from recovered deleted files, currently unused disk space, and

deliberately hidden information or files. Some people's e-mail that was recovered to their extreme embarrassment (or worse) but arguably to society's benefit is shown in Figure H.10.

Following is a discussion, not necessarily exhaustive, of places from which digital forensic experts can recover information.

PLACES TO LOOK FOR USEFUL INFORMATION

Information is written all over a disk, not only when you save a file, but also when you create folders, print documents, repartition the disk, and so on. System and application

" . . . something could get screwed up enough . . . and then you are in a world of hurt . . . "

and

"I can only hope the folks . . . are listening . . . "

Figure H.10
Recovered E-mail Messages

Excerpts of e-mail traffic that flew back and forth only two days before the February 1, 2003, Columbia shuttle disaster, in which an engineer discussed his misgivings about the possibility of a disaster

To: David B. Duncan
Cc: Michael C. Odom@ANDERSEN WO: Richard Corgci@ANDERSEN WO
BCC:
Date: 10/16/2001 08:39 PM
From: Nancy A. Temple
Subject: Re: Press Release draft
Attachments: ATT&ICIQ: 3rd qtr press release memo.doc

Dave - Here are a few suggested comments for consideration.

- I recommend deleting reference to consultation with the legal group and deleting my name on the memo. Reference to the legal group consultation arguably is a waiver of attorney-client privileged advice and if my name is mentioned it increases the chances that I might be a witness, which I prefer to avoid.

- I suggested deleting some language that might suggest we have concluded the release is misleading.

- In light of the "non-recurring" characterization, the lack of any suggestion that this characterization is not in accordance with GAAP, and the lack of income statements in accordance with GAAP, I will consult further within the legal group as to whether we should do anything more to protect ourselves from potential Section 10A issues.

One of the "smoking gun" e-mails that helped sink Andersen Consulting and Enron

"oops I haven't beaten anyone so bad in a long time...."

From the arresting officer in the Rodney King beating

From Bill Gates in an intraoffice e-mail about a competitor in the Microsoft antitrust action

" . . . do we have a clear plan on what we want Apple to do to undermine Sun . . . ?"

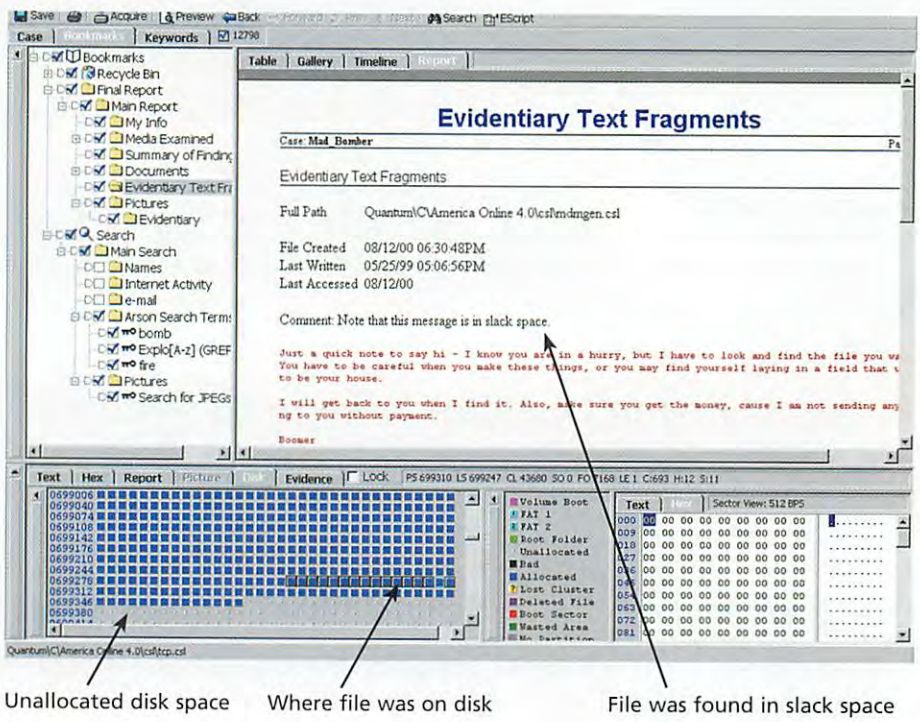
software alike continually create temporary files resulting in space and file locations being rearranged. Leftover information stays on the disk until another file writes over it, and is often recoverable with forensic software. Next, we'll examine places where files or file remnants and other indicators of user activity can be found.

DELETED FILES AND SLACK SPACE It's actually not very easy to get rid of electronically stored information completely. A surprising number of people think that if they delete a file it's gone. It's not—at least not immediately, and perhaps never. When you delete a file, all you're actually doing is marking it as deleted in the disk's directory. The actual file contents are not affected *at all* by a delete action.

If you delete a file from a hard disk you usually get a message asking you if you want it in the *Recycle Bin* and then you can recover it from there. In the case of a removable medium, like a USB flash drive, it's a little harder, but not much. The message you get asks whether you're sure you want to delete the file because it may not be recoverable. Actually that message should read "not as easily recoverable as files in the recycle bin," since you can get it back with utility programs such as Norton Utilities, and of course, forensic software.

When you mark a file as deleted, the space is freed up for use by some other file. So, another file may shortly be written to that space. However, it's not quite that straightforward. The operating system divides storage space into sectors of bytes or characters. The sectors are grouped into clusters. A file is assigned a whole number of clusters for storage, whether it completely fills the last cluster or not. This storage allocation method usually leaves unused portions of clusters. This is analogous to writing a three and one-half page report. You'd have to use the top half of the fourth page and leave the rest of the page blank. So, the fourth page is allocated to the report but not completely used. If the previously stored file (the deleted one) was bigger and used that last part of the space, then the remnants of the deleted file remain and can be recovered using the appropriate software. The space left over from the end of the file to the end of the cluster is called ***slack space,*** and information left there from previous files can be recovered by forensic software (see Figure H.11).

Figure H.11
Fragment of E-Mail Found in Slack Space by Encase



SYSTEM AND REGISTRY FILES Operating system files manage the hardware and software of your computer and let your application software access hardware without having to know how all the various types of hardware function. As one of its many functions, the operating system controls virtual memory. Virtual memory is hard disk space that is used when RAM is full. Details of virtual memory activity are stored in system files. For example, if you have several applications running and you're instant messaging someone, that exchange may be stored on the hard disk without your knowing it simply because there wasn't room for it in RAM.

The Registry is the database that Windows and Vista use to store configuration information. Registry files have information such as preferences for users of the system, settings for the hardware, system software, and installed programs. This information can be very valuable. For example, even if you uninstall a program, remnants of the install process remain in the registry file. Registry files also contain the MAC (Media Access Control) address, which is a special ID for a computer on a network. When this MAC address is contained in a file, as it is in a Word document, it links that document file to its "owner" computer.

UNALLOCATED DISK SPACE If your hard disk gets a lot of use, it's probable that each sector has had information put into it many times. The operating system is always moving files around, and if you changed a Word file and resaved it, the previous version is marked as deleted and the space becomes unallocated. ***Unallocated space*** is the set of clusters that has been marked as available to store information, but has not yet received a file, or still contains some or all of a file marked as deleted. Until the new information takes up residence, the old information remains. The bigger the hard disk, the longer it usually takes for old space to be used.

UNUSED DISK SPACE Unused space results from rearranging disk space. For example, when a hard drive is repartitioned, the new partitioning may not use all the space on the hard disk. So, again, those unused portions are not overwritten. The partition table and other operating system information are stored on their own tracks and are not visible under normal circumstances, but may have once stored a Word document. To be able to see the fragments of files tucked away in these tracks the user needs forensic software.

ERASED INFORMATION By now you may be asking whether it's possible to completely erase information from a storage medium. It is possible, but you need to know what you're doing. You can get disk-wiping programs that erase information from a disk by writing nonsense information over the previous contents. Utilities like Norton have this feature. However, erasing a disk takes a lot of time. A 10-gigabyte hard disk (not very big) would take several hours to clean. Even then you're not necessarily safe, for three reasons:

- A single overwrite may not erase the information completely. The Department of Justice recommends that government agencies write over old information seven times to be sure it's completely gone.
- Some programs keep track of what was deleted by whom, and that record is viewable if you know where to look.
- Disk-wiping programs vary greatly in which parts of the hard disk they clean. For most of them, you have to change the settings to reach certain parts of the disk. Some claim to go through the wipe process up to 35 times, but that still doesn't erase the areas that the software isn't set to erase. Also keep in mind that if you're trying to erase information because of some illicit activity, traces may still be left

of the information you're trying to discard, and unless you are very careful, you'll leave traces of your attempt to wipe the disk. At the very least, you'll most likely leave a record in the Registry that you installed the wiping program.

LEARNING OUTCOME 4

ANTI-FORENSICS

Because of high profile digital forensics cases, people nowadays understand more about how data is stored on computer storage media and how it can be accessed by forensic software. As a result, a new branch of the digital forensics industry is growing fast—the anti-forensics industry. Some of the tools now available that make it hard or impossible to trace user activity or access the data in files were not specifically intended to defeat law enforcement probes; rather they are there mainly to help computer owners to protect themselves and their data. For example, encryption is a very good way to protect the data on your notebook computer so that if it's stolen, the thief can't get the data. Another is keeping deleted files out of the Recycle Bin, so that someone can't recover your files easily. Others, however, products with names such as EvidenceEiminator, are clearly intended to keep the bad guys from getting caught.

Anti-forensic tools fall into three categories:

1. Configuration settings—included in your operating system, browser, and applications like Word and Excel.
2. Third-party tools—utility software on the market that performs specific tasks.
3. Forensic defeating software developed to remove or change the sort of data that forensics experts look for.

CONFIGURATION SETTINGS This category includes the *Shift + Delete* option that you can use instead of simple *Delete* so that the file is not listed in the Recycle Bin. However, if you use this bypass option you still leave a special signature that digital forensics experts can find. In Windows there are several options that mask user activity, like renaming the file with a different extension. This is probably the simplest, and most easily detected, way of deliberately hiding a file. Say you had an Excel file that had calculations you didn't want anyone to know about. You could name the file Space Needle.jpg. It would then appear in Windows Explorer in the list of files as an image file, with the name implying that it's just a vacation photo or something else equally innocuous. If you click on that file, Windows will try to load it with the default .jpg viewer, and of course, it won't load. What digital forensic experts usually do is load the file into a program that accommodates many file formats. This way, you save a lot of time trying to load the renamed file into lots of different types of software. Even more helpful is having a forensic tools like EnCase that actually flag files with extensions that don't match the contents and also show files in their true formats.

Another thing you can do would be to use the option that that clears out virtual memory so that any RAM data that was temporarily stored on the hard disk for use by the processor is removed when the system no longer needs it. Enabling this option, however, will make your system shutdown much slower. The *Defrag* option rearranges data on your hard disk and overwrites deleted files. *Disk Cleanup*, listed as an option in the Properties of the C:\ drive, lets you delete ActiveX controls and Java applets (little blocks of code that generate Web page content) that you downloaded automatically and without realizing it from Web sites you visit.

Internet Explorer has similar features like the option to clear temporary Internet files when you close the browser. Another one is the option to clear the history file so that your Internet surfing activity is not easy to find.

Word and Excel allow you to make your font *Hidden* so that it's not visible on the page. You could also use a very small font or make the characters the same color as the background. Plug-ins are available for Word to remove hidden data and to redact a document. ***Redacting*** means blacking out portions of the document, usually to protect confidential information, so that it cannot be recovered later. The redacted portion of the document has black bars covering the selected text and the text is no longer there.

Office lets you password protect files so that when someone tries to open the file a pop-up window asks for the password. Unless you know the password, you won't be able to read the file. Forensic software can sometimes view the contents of a file without opening the file, eliminating the effectiveness of many types of password protection. And of course there are very effective third-party password cracking programs available, although not as part of the operating system.

THIRD-PARTY TOOLS There are lots of these utility programs. For example, there are some that alter your registry—the file that logs installations of hardware and software. Another type hides Excel files inside Word documents and vice versa. This does not protect files from an experienced examiner. Others change the file properties in Windows like the creation date or the extension. Still another type can split files, password protecting and encrypting parts of the file or storing parts in different places on the storage medium.

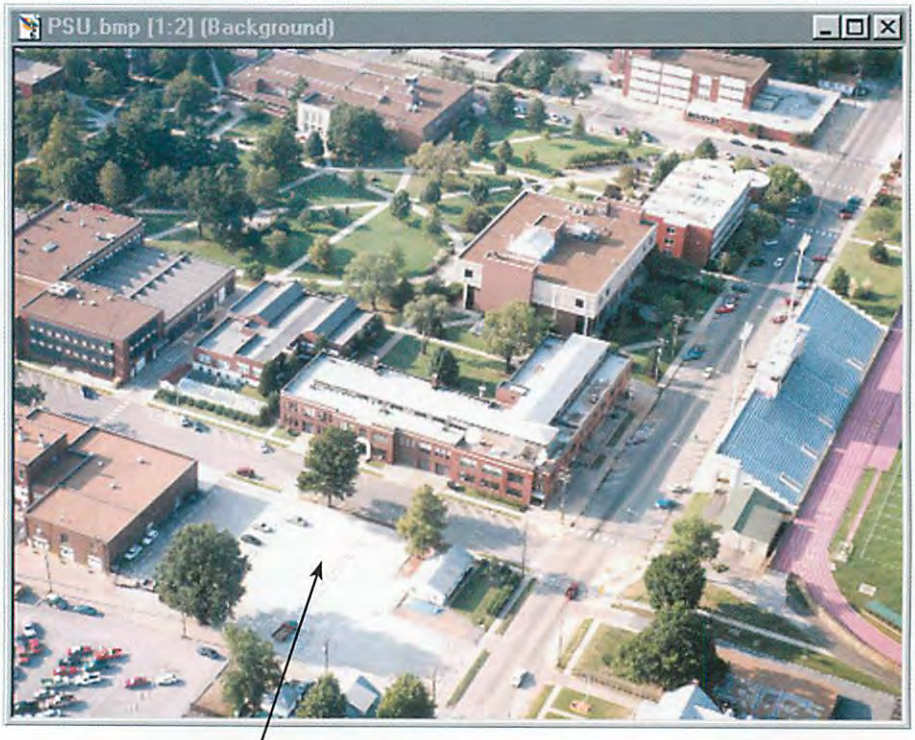
Probably the best known type of third-party tools are the wiping programs that overwrite the disk, effectively obliterating the information that was there before. They work well enough to clean a hard disk that you may be giving away to someone, but, depending on the actual software, there may be lots of fragments that digital forensics experts can still recover.

There are lots of encryption programs available that protect files so that even if someone manages to get them, it won't be any good because they're not readable without the decryption key. ***Encryption*** scrambles the contents of a file so that you can't read it without the right decryption key. Often investigators can find the decryption key in a password file or on a bit of paper somewhere around the keyboard. Password cracking programs can find passwords very easily (alarmingly easily, in fact). They have dictionaries of words from multiple languages, so whole words from any widely used language are not hard to crack. Some people put a digit or two on the front or back of a word. That doesn't fool password-cracking programs at all.

Using images to hide data is another way of protecting information. This is called steganography. ***Steganography*** (see Figure H.12 on the next page) is the hiding of information inside other information. Paper money is a good example of steganography. If you hold a dollar bill up to the light you'll see a watermark. The watermark image is hidden inside the other markings on the bill, but it can be seen if you know what to do to see it.

A very useful tool, but a hardware/software combination this time, is a ***U3 Smart drive*** which looks like and is a USB flash drive, but it stores and can launch and run software on any computer. You can have all the software and files you need on the U3 and plug it into any computer, and it can take over computer resources like the CPU, screen, and keyboard—nothing gets stored on the hard disk of the computer you're using, and you can have all your own programs—even your own wallpaper—on the screen. All cache, cookie items go to the U3 and it runs it own programs. This works because it appears to your computer to be a CD and so Windows AutoPlay feature automatically runs the U3 LaunchPad which is the U3's own user interface. It works very similarly to the Windows interface. You can get a large range of software for a U3 device.

One of the most effective ways to evade detection for someone who is doing something illicit like accessing child pornography is to use a U3 Smart device since it can be



You can't see the parts of the picture that were changed to encode the hidden message. You'll only be able to access the hidden file when you put the right password into a pop-up window.

Figure H.12
Steganography Hides a File in an Image

plugged into virtually any computer and leaves no trace of the user or the user's activity. Other methods are detailed below.

FORENSIC DEFEATING SOFTWARE In addition to the utilities that could arguably be acquired for personal privacy or protection purposes, there is software that makes no secret of its purpose to fool investigators. One type removes residual data—data left when files are deleted and the space is partially overwritten. Other software is designed to erase cache memory, cookies, internet files, Google search history, and so forth. Some programs are aimed at specific forensic software. EnCase is the usual target because of its standing as the most popular and most accepted software in the industry. Of course, if you're doing something illegal and there are records of it on your computer, for example, if you're keeping track of drug dealing, you could also use any or all of the tools provided by Windows or the utilities supplied by third parties.

Even given all these tools and more, it's not as easy as it may sound to hide your activity on a computer. First, not all programs function as advertised, or as fully as promised. Second, very few people have the knowledge and skill to completely hide their tracks. Third, the installation of third-party utilities or forensic defeating software or even operating system settings can be detected and can indicate intent to hide something.

A final note on the use of software to evade detection by law enforcement: If you find yourself in litigation and use such tools to get rid of information you believe may be incriminating and then claim that it was never there, you might be in for a rude awakening. The law says that "any product used to circumvent discovery" may be taken as consciousness of guilt. Even though the documents are not available, during the court hearing the inference may be made that you had them and that, by destroying them, you have shown yourself to be guilty. So, being able to determine that such tools have been

used is almost as good as finding the evidence itself. This line of reasoning has often been used in cases of illegal distribution of movies and music.

Who Needs Digital Forensics Investigators?

LEARNING OUTCOME 5

Digital forensics is widely used wherever and whenever the investigation of electronically stored files is warranted, such as:

- In the military, both as part of national security intelligence gathering and analysis and for internal investigations of military personnel.
- In law enforcement, when the FBI, state investigatory agencies, and local police departments need to gather electronic evidence for criminal investigations.
- Inside corporations or not-for-profit organizations, when conducting internal audits, for example, or investigating internal incidents.
- In consulting firms that specialize in providing digital forensic services to corporations and law enforcement.

Digital forensics experts work both proactively, educating and warning people about possible problems, and reactively, when they're called in to help in response to an incident. The need for such expertise is growing, especially considering that it is estimated that 93 percent of all information is generated in digital form. Since computing and investigative techniques are improving continuously, digital forensics experts need a forum to exchange ideas and information (see Figure H.13).

PROACTIVE DIGITAL FORENSICS EDUCATION FOR PROBLEM PREVENTION

Companies are increasingly providing proactive education for two reasons: first, to educate employees on what to do and not to do with computer resources and why; and

Professional organizations exist that support digital forensic experts in doing their jobs. The organizations below provide interaction between members who share information, experience, and methods. Such organizations also provide ethical guidelines and certification.

- IACIS (International Association of Computer Investigation Specialists) is open to law enforcement personnel and sets standards and guidelines for computer forensic investigations.
- ACFE (Association of Certified Fraud Examiners) focuses on serving those who investigate fraud. Members include people in law enforcement, auditors, accountants, and digital forensic experts.
- The HTCIA (High Technology Crime Investigation Association) is open to law enforcement and corporate investigators alike and facilitates the sharing of resources among its members.

A group called the Sedona Conference Working Group on Electronic Document Production published *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production.* The document, the first draft of which emerged in 2003, is a new set of standards pertaining to properly conducting a digital forensic investigation. These principles were developed by lawyers, consultants, academics, and jurists to address the many issues involved in antitrust suits, intellectual property disputes, and other types of complex litigation.

Figure H.13
Professional Organizations and Standards

second, to teach employees what to do if they suspect wrongdoing, and how not to make things worse by destroying evidence.

People who use computers every day are often not very knowledgeable about what, when, and how information is stored on computers. For example, many corporations have strict policies on how long e-mails will be kept on the system (or in the form of backups). Usually the period of time is about 60 days. You might decide to save your e-mails on your hard disk so that you'll have them indefinitely. This might not be wise since the reason that companies have this policy is that should the company find itself involved in litigation, all electronic information, including e-mail, may be discoverable. That is, the company may have to hand it over to opposing counsel. The more there is, the more it costs to collect, organize, and deliver it.

In Chapter 8 you saw the Industry Perspective box detailing Enron's e-mail situation. Lots of personal information that was not directly related to the legal case became public information and was put on the Internet.

The second reason for providing some education in computer forensics has to do with conducting internal investigations properly. Say a company wants to file a complaint with law enforcement about the suspected illegal activity of an employee. Before law enforcement can look into the situation, however, it needs to have sufficient cause to do so. It can happen that in collecting relevant information the company inadvertently contaminates or destroys the "crime scene." The result may be that law enforcement can't prosecute after all because of lack of evidence.

REACTIVE DIGITAL FORENSICS FOR INCIDENT RESPONSE

Companies need digital forensics, in a reactive mode, to track what employees have been doing with company resources. You saw in Chapter 8 that employees may be using the Internet to such an extent during working hours that their productivity is affected, and the level of personal traffic on the company network may be such that people who are actually working are slowed down. This is just one example of misuse of the company computer system. The evidence of such misappropriation of computer resources can be found on the system itself—on individual client computers and on the servers.

A second reason for reactive digital forensics is changes in laws and government regulations and new laws passed as a consequence of recent corporate crime and misbehavior, probably the most important being the Sarbanes-Oxley Act of 2002, signed into law by President Bush. Known as "Sarbanes-Oxley," the law requires companies to (1) implement extensive and detailed policies to prevent illegal activity within the company and (2) respond in a timely manner to investigate illegal activity.

In Closing Case Study 1 in Chapter 8, you saw what happened to Enron's e-mail when the government filed charges against the company.

The act expressly states that executives must certify that their financial statements are accurate. They will be held criminally liable for fraudulent reporting, removing the insulation that executives previously had of being able to say that they didn't know about misstatements. Sarbanes-Oxley also specifically requires publicly traded companies to provide anonymous hotlines so that employees and others can report suspicious activity.

The provision that suspicious activity must be investigated in a timely manner in many instances automatically requires digital forensics. In earlier litigation, courts have determined that computer-stored evidence is crucial to the proper investigation of alleged corporate fraud. Add to that the fact that delay in investigating alleged wrongdoing meets with severe penalties and that courts impose severe sanctions on those judged guilty of destroying evidence including electronic information.

A DAY IN THE LIFE

The career of a digital forensics expert can be very rewarding and satisfying. But it can also mean spending long hours carefully poring over the contents of hundreds of files looking for the clue that will unravel the mystery and show what actually happened. It also means being able to explain to lawyers, judges, juries and other noncomputer people what the evidence is and what it means. You also need to be able to keep your cool since "dispute resolution" usually means someone is aggrieved or scared and such feelings are often expressed as anger. People can even turn violent during an investigation — some have gone as far as rigging their computers with explosives to thwart an investigation.

Lanny Morrow is a digital forensics expert with the Forensic and Dispute Consulting division of BKD, LLP, one of the largest accounting firms in the United States. He's an experienced forensics expert who has all the abilities necessary to succeed as an investigator along with years of experience. He has solved many cases while working with a list of clients that includes for-profit and nonprofit organizations; litigants in civil suits; and defendants and plaintiffs in criminal proceedings. Following are two examples from his case files.

The first involves MySpace. A high-school girl posted on MySpace her account of her own molestation by her father. Her shocked friends told their parents about her plight and the parents alerted the authorities, who initiated an investigation. The girl's parents were deeply distressed and vigorously disputed the claim. They cooperated fully in the investigation, handing over family computers and cell phones to Lanny who began the process of finding the truth.

- He found multiple drafts of the text that the girl posted on MySpace describing the incident. The date stamps showed that they had been created before the rape was alleged to have taken place.
- Further examination revealed e-mails and chat logs where the girl expressed resentment at being grounded by her parents for attending a party without permission. In her communications, the girl stated her intention and explained her plan to get even.
- Lastly, Lanny found cell phone text messages and e-mails from her friends offering pledges to corroborate her story along with suggestions of details to include in the fictitious report.

As often happens, when presented with the overwhelming evidence of her lies, the girl admitted that she had made up the whole story to get revenge on her parents. She then had to explain to her teachers and peers what she had done and why. The friends who were co-conspirators in the plan were also identified and had some explaining of their own to do.

The second case involved three employees who filed a civil case against their former employer alleging wrongful termination. They had been fired on the basis of inadequate performance in their jobs and when company executives were notified of the lawsuit they hired Lanny to see if he could find evidence that the employees' performance on the job was inadequate and the termination was, therefore, justified. Since the employees' jobs all involved heavy use of the company's computer system, Lanny and his team went to work right away and what they found was very revealing

- They used EnCase's Timeline feature to generate a profile of computer usage by each of the employees. This report shows, down to the second, when a computer was being used and what it was being used to do. The analysis showed large gaps during working hours indicating that the employees had taken extended breaks.

- Furthermore, they found files that revealed that one of the employees was using the company's time and resources to run her own business on the side. It was later established that she had taken office supplies home for her private use.
- An analysis of the activity on the computer of another one of the complainants established that she had spent up to three hours a day, during business hours, surfing the Net, often participating in eBay auctions, and had routinely spent all morning e-mailing her friends and family.
- The third employee spent a large portion of his work time gambling online.

All in all, over an extended period, the three employees had spent only about one-third of their working hours doing what they were being paid to do. To cover their tracks they delegated their tasks to other employees who believed that this was standard operating procedure. After the investigation was over the office managers were also fired for allowing such conduct and because it came to light during the investigation that one of them had been having an affair with one of the fired employees. Examination of the manager's own computer confirmed the relationship.

Summary: Student Learning Outcomes Revisited

1. **Define computer crime and list three types of computer crime that can be perpetrated from inside and three from outside the organization.** ***Computer crime*** is a crime in which a computer, or computers, played a significant part in its commission. Crimes perpetrated outside the organization include
   - ***Computer viruses***
   - ***Denial-of-service (DoS) attacks***
   - ***Malware bots***
   - Web defacing
   - ***Trojan-horse virus***

   Crimes perpetrated inside the organization include
   - Fraud
   - Embezzlement
   - Harassment
2. **Identify the seven types of hackers and explain what motivates each group.** ***Hackers*** are knowledgeable computer users who use their knowledge to invade other people's computers. The seven types are
   - ***Thrill-seeker hackers,*** who are motivated by the entertainment value of breaking into computers
   - ***White-hat hackers,*** who are hired by a company to find the vulnerabilities in its network
   - ***Black-hat hackers,*** who are cyber vandals and cause damage for fun
   - ***Crackers,*** who are hackers for hire and are the people who engage in electronic corporate espionage
   - ***Hacktivists,*** who are politically motivated hackers who use the Internet to send a political message of some kind
   - ***Cyberterrorists,*** who seek to cause harm to people or destroy critical systems or information for political reasons
   - ***Script kiddies*** or ***script bunnies,*** who would like to be hackers but don't have much technical expertise
3. **Define digital forensics and describe the two phases of a forensic investigation.** ***Digital forensics*** is the collection, authentication, preservation, and examination of electronic

information for presentation in court. Electronic evidence can be found on any type of computer storage medium. A computer forensic investigation has two phases: (1) collecting, authenticating, and preserving electronic evidence; and (2) analyzing the findings. The collection phase consists of

- Getting physical access to the computer and any other items that might be helpful
- Creating a ***forensic image copy*** of all storage media
- Authenticating the forensic image copy by generating an ***MD5 hash value,*** that, when recalculated at a later date will be exactly the same number, as long as nothing at all on the storage medium has changed in any way
- Using forensic hardware that can read storage media but cannot write to them
- Using forensic software that can find deleted, hidden, and otherwise hard-to-access information

The analysis phase consists of

- Finding all the information and deducing what it means
- Assembling a crime story that fits the information that has been discovered

4. **Describe what is meant by anti-forensics and give an example of each of the three types.** Anti-forensics is a name for tools that mask or eliminate traces of user activity on a computer. The three types are:
   1. Configuration settings—included in your operating system, browser, and applications like Word and Excel. An example is Shift + Delete to bypass the Recycle Bin.
   2. Third-party tools—utility software on the market that performs specific tasks. An example is encryption software.
   3. Forensic defeating software developed to remove or change the sort of data that forensics experts look for. An example is software that changes creation and access dates on files.
5. **Describe two ways in which businesses use digital forensics.** Corporations use computer forensics for proactive education and for reactive incident response. Education serves to explain to employees what they should and should not do with computer resources and also how to conduct an internal computer forensic investigation. Incident response involves uncovering employee wrongdoing and preserving the evidence so that action can be taken.

Key Terms and Concepts

Black-hat hacker, 378
Bot, 375
Botnet, 377
Computer crime, 370
Computer virus (virus), 371
Cracker, 379
Cyberterrorist, 379
Denial-of-service (DoS) attack, 375
Digital forensics, 381
Distributed denial-of-service (DDoS) attack, 375
Drone, 377
Encryption, 393
Forensic image copy, 382
Hacker, 378
Hacktivist, 379
Key logger (key trapper) software, 374
Malware, 371
Malware bot, 377
MD5 hash value, 383
Redacting, 393
Rootkit, 377
Script bunny (script kiddie), 379
Slack space, 390
Social engineering, 379
Spoofing, 374
Steganography, 393
Thrill-seeker hacker, 378
Trojan horse virus, 374
U3 Smart drive, 393
Unallocated space, 391
White-hat hacker (ethical hacker), 378
Worm, 371
Zombie, 377

Short-Answer Questions

1. In what two ways are computers used in the commission of crimes or misdeeds?
2. What constitutes a computer crime?
3. What kind of software is a computer virus?
4. How does a denial-of-service attack work?
5. What is the effect of a virus hoax?
6. What is the difference between the Klez family of viruses and previous worms?
7. What is a white-hat hacker?
8. What do crackers do?
9. Is there a difference between a cyberterrorist and a hacktivist? If so, what is it?
10. What is digital forensics?
11. What is anti-forensics?
12. What is live analysis?

Assignments and Exercises

1. **FIND DIGITAL FORENSICS SOFTWARE** On the Web there are many sites that offer digital forensics software. Find five such software packages and for each one answer the following questions:
   - What does the software do? List five features it advertises.
   - Is the software free? If not, how much does it cost?
   - Is there any indication of the software's target market? If so, what market is it (law enforcement, home use, or something else)?
2. **WHAT EXACTLY ARE THE SEDONA PRINCIPLES?** Figure H.13 mentioned the *Sedona Principles.* These 14 principles were developed by lawyers, consultants, academics, and jurists to address the many issues involved in antitrust suits, intellectual property disputes, and other types of complex litigation.

   Write a report on the stipulations of the *Sedona Principles.* Do some research and find out exactly what the *Sedona Principles* suggest. Here's the first one to get you started:

   1. Electronic data and documents are potentially discoverable under Fed.R. Civ. P. 34 or its state law equivalents. Organizations must properly preserve electronic data and documents that can reasonably be anticipated to be relevant to litigation.

   Be sure to explain in your paper any legal terms, such as "discoverable," which appears in the 1st principle above, and "spoliation," in the 14th principle.
3. **THE INTERNATIONAL ANTI-CYBERCRIME TREATY** Find out what the provisions of the international anti-cybercrime treaty are and how they will affect the United States. One of the concerns that will have to be addressed is the issue of whether laws of one country should apply to all. For example, if certain sites are illegal in Saudi Arabia, should they be illegal for all surfers? Or if Germany has a law about hate language, should a German or a U.S. citizen be extradited to stand trial for building a neo-Nazi Web site? What do you think?
4. **DOES THE FOURTH AMENDMENT APPLY TO COMPUTER SEARCH AND SEIZURE?** The U.S. Department of Justice's Computer Crime and Intellectual Property Section has an online manual to guide digital forensics experts through the legal requirements of the search and seizure of electronic information. It's available at www.cybercrime.gov/searchmanual.htm and has a section on "Reasonable Expectation of Privacy." There are four subsections: general principles, reasonable expectation of privacy in computers as storage devices, reasonable expectation of privacy and third-party possession, and private searches. Read and summarize these four subsections.