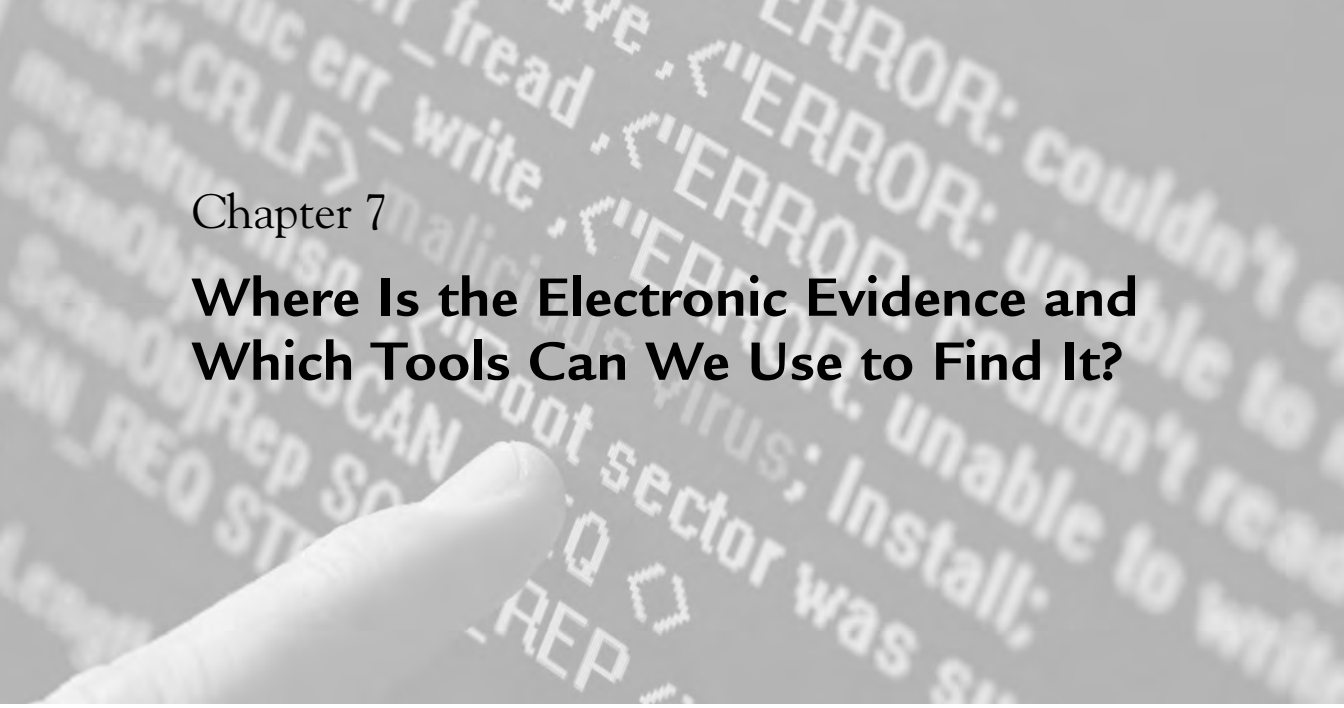

Chapter 7

Where Is the Electronic Evidence and Which Tools Can We Use to Find It?

Before we look at how to manage crime scenes and incidents (a topic that we consider in Chapter 8), we first need to explore the various hardware and software computer components, electronic devices, and media that may contain electronic evidence. The first part of this chapter explores certain hardware and software computer components and electronic devices that might be the source of evidence for computer forensics investigations. The chapter then describes the tools required to search and collect electronic evidence.

The Location of Electronic Evidence

Evidence is most commonly found on hard drives. Data within the hard drives of computers consist of volatile and nonvolatile data. **Volatile data** disappear when the computer is powered off, whereas **nonvolatile data** are stored and preserved in the hard drive when the computer is powered off. Evidence in the hard drives of computers may be found in files created by the computer user (e.g., e-mails, spreadsheets, and calendars), files protected by the computer user (e.g., encrypted and password-protected files), files created by the computer (e.g., log files, hidden files, and backup files), and other data areas (e.g., metadata).

Files Created by Computer Users

Files created by the user include document (e.g., Word; file extensions of either ".doc" or ".docx"), text, spreadsheet (e.g., Excel), image, graphics, audio and video files. These files

contain **metadata** (i.e., data about data). Metadata can provide the following kinds of information:

- The name of the author of the document and the company the document belongs to
- The owner of the computer
- The date and time the document was created
- The last time the document was saved and by whom it was saved
- Any revisions made to the document
- The date and time the document was last modified and accessed
- The last time and date the document was printed

Consider the embarrassment of the British government when the embedded metadata of a Word document on Iraqi intelligence that it published revealed that the document contained plagiarized text.[1] The identity of the BTK killer (Dennis Rader) was also revealed by embedded metadata in a deleted Word document included on a floppy disk that the suspect had sent to a TV station. Specifically, this information enabled law enforcement agents to trace the document back to a church to which Dennis Rader belonged. As these cases suggest, metadata can yield substantial evidence related to an incident or crime.

The files of the Windows operating system contain metadata that can be accessed in Windows by right-clicking on the icon of the desired file and selecting "Properties."[2] Investigators should keep in mind that whenever they access a file, they modify system metadata.

Timestamp data (i.e., the time of events recorded by computers) also may provide valuable information to an investigation. This was demonstrated in *Jackson v. Microsoft Corporation*,[3] where the timestamp data on confidential files in the defendant's possession provided evidence of intellectual property theft. Programs are available online, such as Timestomp, that try to delete or modify timestamp information. When changing timestamp information, a suspect may have one of the following aims:

- Validate a statement or testimony the suspect made
- Provide the suspect with an alibi
- Eliminate the person from consideration as a possible suspect

The use of Timestomp can frustrate computer forensics investigations if the offender has taken specific measures to conceal his or her use of this software. For instance, an investigator will be alerted to the use of this type of software if the suspect clears the timestamp of the entire system. Additionally, the dates the offender modifies must be believable and must not draw unwanted attention from authorities. For example, if an offender changes the timestamp of a Microsoft Office Publisher (".pub") document to 1980, the examiner

would consider this document to be suspicious—".pub" documents were not available in 1980. The investigator would suspect that the offender had modified timestamp information, and would proceed to look at other documents to see if their timestamps had been modified as well.

A website called "Anti-forensics," which claims to render computer investigations irrelevant, warns users that if they use Timestomp, they should take a few steps to hide their use of this software. One such step is to rename the "timestomp.exe" file (which loads the program to a user's computer) as "RUNDLL32.exe," which is a legitimate file responsible for loading dynamic link library (DLL) files to memory and running them.[4] An investigator may still be able to find this file with a simple word search because it contains strings featuring the term "timestomp." Another recommendation made by the "Anti-forensics" website is to delete the Timestomp prefetcher (".pf") file, which is stored in a directory (c:\windows\prefetch directory) when an executable file is run in Windows.[5] Regardless of the efforts the suspect takes to conceal his or her use of this software, one thing remains certain: The use of Timestomp can significantly disrupt the forensic timeline that the investigator is seeking to establish.

An investigator should also check the computer to see if the suspect has created a calendar. Calendars may hold appointment information and other data that can reveal important clues about the suspect's whereabouts on a given date and time. It can also reveal the contacts of a suspect. Questioning these contacts may provide investigators with valuable information about the case.

Additionally, investigators should examine Web browsers for any files created by the user. In particular, they may look at particular websites that a user may have bookmarked or added to his or her favorites folder in the Web browser (different versions of Internet Explorer, Mozilla Firefox, Netscape Navigator, and Chrome, to name a few). **Figure 7–1** shows the Bookmarks menu in Mozilla Firefox; **Figure 7–2** shows the Favorites menu in Internet Explorer.

Evidence can also be retrieved from e-mail accounts. For instance, address books in e-mail accounts can include the contacts of the suspect. Other pertinent information to a criminal or civil case under investigation can be retrieved from e-mails in the inbox, sent, delete, draft, and spam folders of an account, which reveal the content of communications and the persons with whom the suspect was communicating. Of particular note are the draft and spam folders.

Members of al-Qaeda have reportedly used a technique known as an electronic or virtual "dead drop" to communicate.[6] This technique involves opening up an account, creating a message, saving this message as a draft, and then transmitting the account user name and password to the intended recipient (or recipients). The receiver of this information then logs on to the account and reads the message that was saved as a draft. This technique was used by the perpetrators of the Madrid train bombings in 2004, for example. These terrorists communicated with other members of their cell by saving messages for one another in the draft folders of preselected email accounts.[7] By using this

Figure 7–1 Depicts the location of bookmarks in the Mozilla Firefox web browser.

technique, terrorists avoid the possibility that their e-mails might be intercepted by eavesdroppers. Spam folders may also need to be checked: Al-Qaeda terrorists have been known to hide their messages in spam and then send these seemingly junk e-mails to their intended recipients.[8]

Evidence retrieved from e-mail investigations is explored in more depth in Chapter 10.

Files Protected by Computer Users

There are many different ways in which a user can protect his or her files:

- An individual can modify files or folders within the computer to look like something else.
- He or she can add a password to the file or folder and/or encrypt it to ensure that no one will be able to see what is in the file or folder.
- An individual can make the file or folder invisible.

These same tactics are also used by criminals to hide evidence of their crimes.

Figure 7–2 Depicts the location of the "Favorites" button in the Internet Explorer web browser.

Renamed Files and Files with Changed Extensions

Individuals can hide files in plain sight by renaming or changing the file extensions. As an example of the former technique, a file that contains sexually explicit material involving minors might be given an innocuous label such as "Thanksgiving" or "Mom's Birthday." Using the latter technique, a file extension might be changed by a criminal to hide files that contain incriminating evidence. For instance, a drug dealer who has a spreadsheet that lists clients, their drugs of choice, telephone numbers, payment for drugs, and any money owed by clients to the dealer might change the extension of the spreadsheet from ".xls" to ".jpeg". The drug dealer would probably change the extension of the spreadsheet to that of an image file because investigators looking for information concerning the dealer's sales would most probably look for it in spreadsheet and document files.

The change of file extension corrupts the file. Such a file may be viewed only in its original format. Investigators, however, can use forensics tools (which are explored later in this chapter) to reveal the changed file's original file type. As such, this is not a very effective way to hide data from a computer forensics investigator.

Deleted Files

Evidence can be found in files deleted by a computer user, although deleted files can typically be recovered by investigators. The first thing an investigator should do when searching for a deleted file is to check the Recycle Bin. When a file is deleted, it is moved to the Recycle Bin. More often than not, the files in the Recycle Bin will have been emptied (i.e., deleted) by the offender. When this occurs, any file that has been deleted from the Recycle Bin is removed from the file allocation table.

Depending on which Windows operating systems the investigator is dealing with, the file allocation table can be in the FAT, FAT32, or NFTS format. The first two file allocation table types—**FAT** and **FAT32**—are used in Windows 3.1, 95, 98, and ME editions. **NFTS**—more formally, New Technology File System—is used in the more recent versions of Windows (NT, 2000, XP, 2003, 2008, Vista, and 7). These file allocation tables keep track of and store the names and physical locations of every file on a computer hard drive.

Once a file is removed from the file allocation table, the space where the deleted file resided is marked as free space. In particular, when a file is deleted by the user, the operating system indicates that the space occupied by that file is now available for use by another file. However, the contents of the original file remain in that space until the space is overwritten with new data. Even if a file has been deleted and partially overwritten, it is still possible to recover the file fragment that has not been overwritten. Software is commercially available that allows the user to not only delete the selected files, but also write over all of the free space that is available. This action ensures that the space where the deleted information was will be used and, therefore, that space will not contain any old information.

When a disk is wiped with a single, nonrandom bit pattern, it is possible that data may still be found by a computer forensics investigator using specialized tools. U.S. Department of Defense standards hold that files and hard drives need to be overwritten at least seven times with random binary bit patterns to ensure that the original data are completely deleted. Many software programs are available online that claim to permanently delete files and other data on hard drives and related storage devices (e.g., CDs, DVDs, flash drives). Among them are data shredders, which overwrite files on a hard drive or other storage device with a random series of binary data. This tactic ensures that the data stored on these drives or devices are obliterated beyond recognition.

Encrypted Files

To protect his or her files, an individual may use **encryption** to physically block third-party access to them, either by using a password or by rendering the file or aspects of the file unusable. How does encryption render a file unusable? Encryption basically scrambles the data and makes it unreadable. It does so by transforming plaintext into ciphertext, which is essentially gibberish. A decryption key is required to transform the ciphertext back into plaintext.

Individuals have used encryption to protect their privacy and secure the data in their computer and related electronic devices. Encryption also gives criminals a powerful tool

with which to conceal their illegal activities. In 2000, U.S. Director of Central Intelligence George Tenet testified that terrorist groups such as Hezbollah, Hamas, and al-Qaeda routinely use encryption to conceal files and communicate undetected.[9] In respect to al-Qaeda, Tenet noted that convicted terrorist Ramzi Yousef, the mastermind of the bombing of the World Trade Center in 1993, "had stored detailed plans to destroy United States airliners on encrypted files on his laptop computer."[10]

The United Kingdom has a law that grants law enforcement agencies the power to compel suspects to provide their decryption keys. Specifically, consider Part III of the **U.K. Regulation of Investigatory Powers Act of 2000** (RIPA). Section 49 (notices allowing disclosure) provides agencies with the power to monitor individuals' e-mails by allowing law enforcement authorities to serve written notice to demand that either an encryption key is handed over or a communication is decrypted when such action is deemed to be in the interests of national security, for the purpose of preventing or detecting crime, and in the interests of the economic well-being of the United Kingdom. As of October 1, 2007, Part III of RIPA was activated; now individuals using encryption technology can no longer refuse to reveal keys to U.K. law enforcement agencies if served with a notice. Failure to hand over encryption keys upon request is an offense, even if the material is completely legal. Section 53 of RIPA, which deals with failure to comply with notices to hand over encryption keys, is particularly problematic. It assumes the guilt of the accused by potentially criminalizing individuals with poor memories or reversing the burden of proof in the case of those who claimed to have forgotten (which can easily occur because these keys are normally long passwords) or lost keys to their data.[11]

The United Kingdom is not alone in demanding access to encrypted files. France has a similar law in effect, the Daily Safety Law (*Loi sur la sécurité quotidienne*), which provides the government with access to private encryption keys, restricts import and export of encryption software, and imposes strict sanctions for using cryptographic techniques when committing a crime.[12]

By contrast, the United States does not have a law that grants law enforcement agencies the power to compel suspects to provide their decryption keys. In fact, in *In re Grand Jury Subpoena to Sebastien Boucher* (hereafter *In re Boucher*), the court ruled that a hard drive could not be accessed because it was protected by **Pretty Good Privacy** (PGP).[13] PGP is software for encrypting files and messages, which provides cryptographic privacy and authentication for users, but also hampers law enforcement agencies' ability to access the content of files or communications. The *In re Boucher* ruling stated that compelling an individual to provide a password to an encrypted hard drive violated that individual's privilege against self-incrimination under the Fifth Amendment to the U.S. Constitution. An appellate court, however, reversed this decision on different grounds.

In the *In re Boucher* case, border agents had reviewed some of the contents of the defendant's encrypted Z drive that the defendant enabled them to see, which contained child pornography.[14] In *Fisher v. United States,*[15] the court had ruled that if the information the government seeks to compel the defendant to provide adds "little or nothing to the sum total of the Government's information" on the defendant, then no constitutional rights

of the defendant are touched. In line with this argument, the appellate court in the *In re Boucher* case reasoned that providing law enforcement agents with access to the Z drive "adds little or nothing to the sum total of the Government's information" about the existence and location of potentially incriminating files in the drive. Boucher was thus ordered to provide an unencrypted version of the Z drive to authorities.[16]

As matters now stand, the courts have not taken an affirmative stand on whether to grant law enforcement agents unrestricted access to encrypted files. So far, they have allowed this type of access only when the defendant has provided agents with information about the contents of the encrypted files or hard drive during questioning or border searches. If this information has not been disclosed by the defendant, then the agents cannot have access to the encrypted files. The suspect may decide to provide law enforcement agents with the password to these files. However, investigators should take care lest the offender use this opportunity to destroy evidence rather than provide authorities with it.

Some publishers of encryption programs leave backdoors in their software through which to enter their systems. If so, investigators might be able to contact the publishers to gain access to the files protected by these programs. Indeed, encryption programs contain key escrows, which enable the recovery of data in the event that a user forgets his or her passphrase.[17] When issues of national security arise, these keys must be provided to government agencies.

Password cracking software should be used cautiously, as an individual may have set up the computer to recognize unauthorized access to the system (e.g., repeated failed attempts to access the system) and created a "booby trap" to delete the data that the investigator is trying to retrieve. The suspect may have also created a kill switch—in the form of a command or the pressing of a particular key on the mouse or keyboard—to erase the data on the hard drive.

Hidden Data: Steganography

Something that needs to be protected from prying eyes can be "camouflaged in sound, pictures or other routine content in ways analogous to hiding a pebble on a shingle beach."[18] This technique is known as **steganography** (information hiding). Steganography seeks to make data and messages invisible by hiding them in various files. For example, individuals who collect and distribute child pornography may hide child pornography images and videos in files to avoid being caught by law enforcement agents. Using steganography, these individuals may store child pornography for their own personal use on their computers and send images or other files that have child pornography images or videos hidden in them to others via emails, chat rooms, discussion boards, social networking sites, peer-to-peer networks, blogs, and websites.

To determine if an image contains steganography, an investigator usually makes a visual, side-by-side comparison of the original image and the processed image to identify any differences between them. Unfortunately, computer forensics investigators may not have this luxury; they often have only the processed image available, making visual detection of steganography extremely difficult. To find it, investigators would basically need to know what they are looking for and in which type of file it is possibly hidden. With

steganography, only those individuals with the appropriate software can see the hidden information. Nevertheless, certain tools exist that can assist an investigator in determining whether steganography has been used. Specifically, investigators can use steganalysis to detect if steganography was used on a particular file—that is, to determine whether hidden data exist in the file.

Steganography software is sold commercially and can be downloaded for free over the Internet. Even the most inexperienced user can learn how to hide data using steganography. Free online tutorials that show individuals how to hide data using this technique are readily available from YouTube and websites that offer steganography software.

Files Created by the Computer

Files that are created by the computer may also have evidentiary value. Files that may assist a computer forensics specialist in his or her investigation include event logs, history files, cookies, temporary files, and spooler files.

Event Logs

Event logs automatically record events that occur within a computer to provide an audit trail that can be used to monitor, understand, and diagnose activities and problems within the system.

To find the event logs in a Windows operating system, for Windows 7,[19] click on the Start menu on the lower-left corner of the desktop and select "Control Panel." Once in the "Control Panel" page, click on "System and Security." On this page, click on "Administrative Tools" (**Figure 7–3**).

Next, select "View event logs" from the right side of the screen (see Figure 7–3). In the next screen (**Figure 7–4**), click on "Windows logs" on the upper-left corner of the screen.

Several event logs are now displayed on the screen (**Figure 7–5**), including the following:

- **Application logs.** These logs contain the events that are logged by programs and applications. Errors of these applications and programs are also recorded in this log.
- **Security logs.** These logs record all log-in attempts (both valid and invalid) and the creation, opening, or deletion of files, programs, or other objects by a computer user.

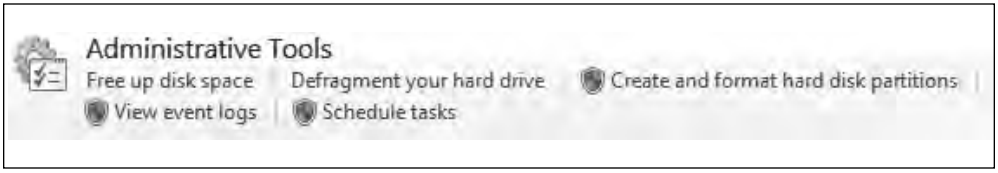

Figure 7–3

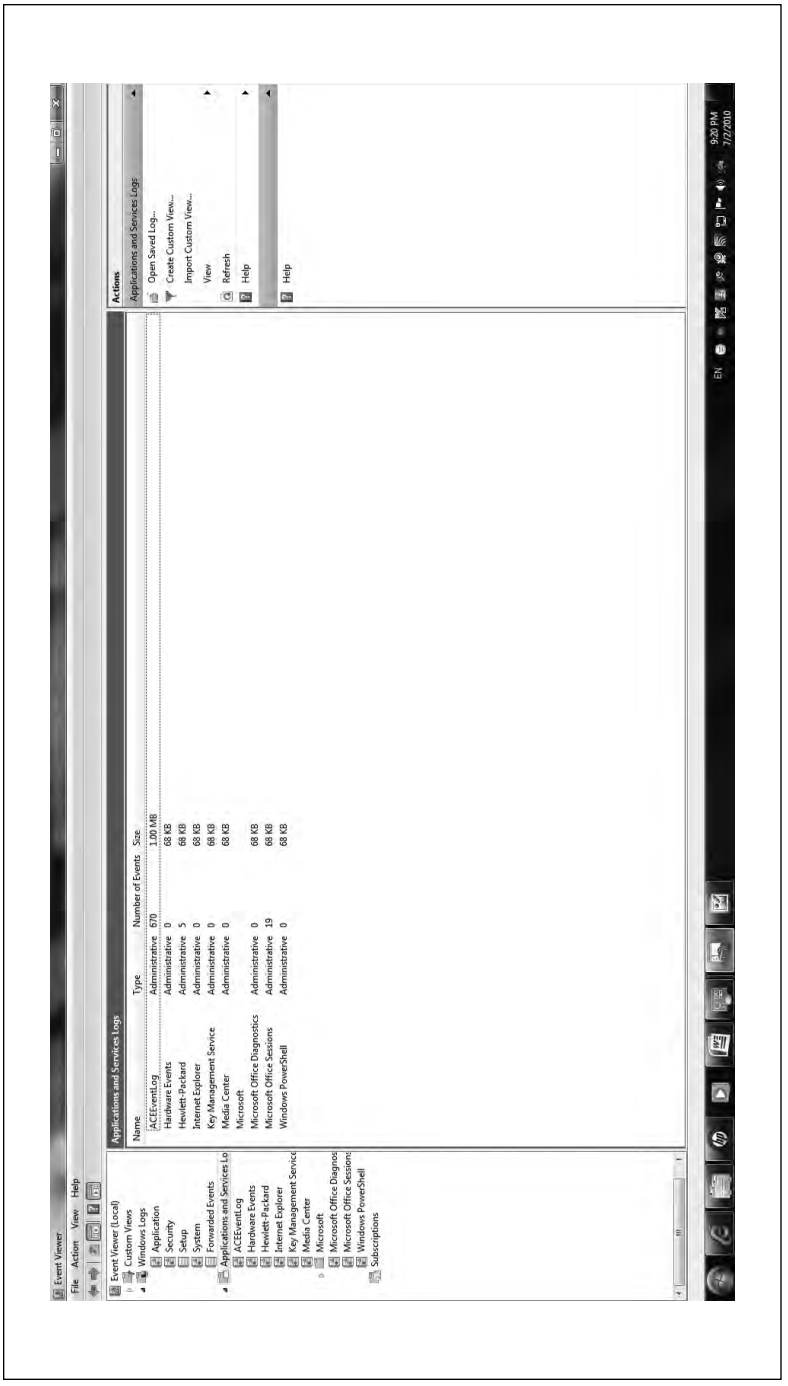

Figure 7–4

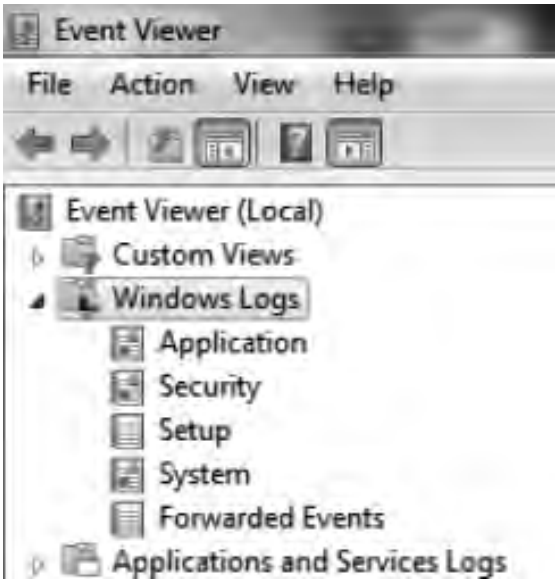

Figure 7–5

- **Setup logs.** These logs provide data on applications that are installed on a computer.
- **System logs.** These logs provide information on Windows system components. For example, they record any failure of a component to load during the startup process.
- **Applications and services logs.** These are new event logs in Windows 7. Instead of recording events that may affect the system as a whole, each log stores events from a single application or component.

Critical information and evidence of a crime may be lost if the logs are full. Depending on your settings, either new events will be added by overwriting older events or newer events will not be added at all. To fix this problem, the size of the logs should be adjusted (i.e., increased) to allow more events to be logged, the logs should be manually emptied, or the logs should be set to overwrite older events automatically.

The most important event log of those mentioned previously is the security log, which records all log-in attempts and activities of the computer user. As such, this log can indicate that malicious activity or other forms of cybercrime have been or are being

committed. For instance, numerous failed log-in attempts in the security log may indicate that someone is trying to access the computer without authorization. Moreover, this log can reveal a suspect's attempt to delete data from the computer.

History Files

The operating system also collects data about the websites visited by a user. In *United States v. Tucker*,[20] computer forensics investigators found important electronic evidence of the crime—namely, deleted Internet cache files showing that Tucker had visited child pornography websites—on the suspect's hard drive.

Internet cache files have also served as important evidence in murder cases. For example, the Web searches of Melanie McGuire provided critical evidence about the brutal murder of her husband, William.[21] McGuire shot her husband, drained his body of blood, dismembered him, placed his body parts in various garbage bags and suitcases, and later disposed of them in the Chesapeake Bay.[22] When investigators searched McGuire's home computer, the Internet search history showed that she had typed into the Google search bar, among other things, "undetected poisons," "how to commit murder," and "how to buy a gun in Pennsylvania." The results of her Internet search for weapons led investigators to the Pennsylvania store where McGuire had purchased the weapon with which she killed her husband. Investigators also found an e-mail McGuire had sent to a friend requesting information on how to buy a gun quickly. Based on the information retrieved from McGuire's home computer and the leads it produced, this defendant was found guilty of first-degree murder and other charges. Clearly, Internet history can provide invaluable information to an investigation.

The toolbars of most Web browsers save the browsing history of the computer user (**Figure 7–6** and **Figure 7–7**). While the majority of cybercriminals erase their browser history, it is important to check this location in case its contents have been overlooked by the offender. The address bar of a Web browser should also be checked, as it is often overlooked by offenders. This area does not provide information on all websites viewed, but only those whose addresses were explicitly typed or copied and pasted into the address bar by the user.

Most online chat room software temporarily stores chat session logs. It also affords users with the opportunity to permanently save logs of chat sessions. The default settings of certain chat room software (e.g., Yahoo! Messenger) are set to temporarily save messages until the user signs out of the application (**Figure 7–8**).

Users may actually set this software to save all of the messages sent or received. With these settings, the logs can provide details of the discussions the suspect had. Using these forums, individuals can forward calls; forward instant messages to their **mobile phones**; make phone calls to cell phones, landlines, or other computers; send text messages; engage in live conference calls; archive messages; and receive and save voice mails, videos, photos, and other files. Accordingly, chat room software provides a wealth of information of potential value to investigations.

Figure 7–6 Area in Internet Explorer where website history can be viewed.

Cookies

Cookies are files created by websites that are stored on a user's computer hard drive when he or she visits that particular website. As such, by viewing cookies, the investigator can determine which websites the user has visited. Certain cookies are used by websites to gather information about an individual's activities, interests, and preferences. Others are used to store credit card information, user names, and passwords. Some cookies do both. The type of information an investigator finds depends on the cookies stored on the suspect's computer.

Temporary Files

Some files are created by the computer unbeknownst to the user. Specifically, the operating system collects and hides certain information from the user. One example of this

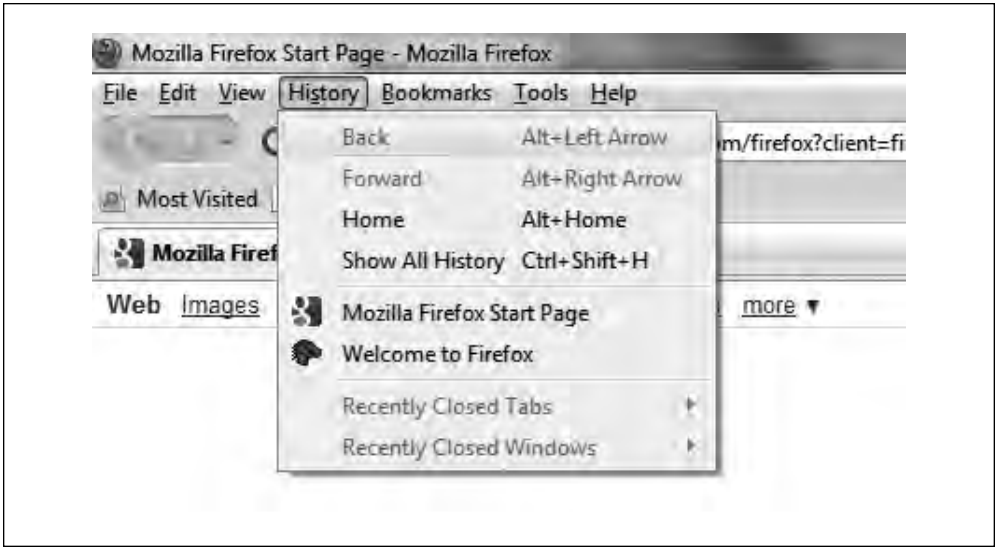

Figure 7–7 Area in Mozilla Firefox where website history can be viewed.

kind of temporary file is unsaved documents. In the case of the "Gap-Toothed Bandit," who was involved in 12 bank robberies in San Diego in 1999, unsaved Word documents including threatening demand notes used for the robberies were saved by the operating system of his computer in a temporary location.[23]

The computer also stores information about websites browsed, items searched online, user names, and passwords. This material is stored in temporary Internet files or cache. To delete this information, click on the "Start" button, and then select "Control Panel." At the upper-right corner of the screen, click on "Category" and choose "Large Icons." Then, in the "Control Panel" screen, choose "Internet Options." When the page shown in **Figure 7–9** appears on your screen, under "Browsing history," click the "Delete" button. You can then choose to delete cookies, temporary Internet files, Web browser history, items searched online, and passwords (**Figure 7–10**).

An investigator should check the temporary files because criminals may forget to delete the information that the computer stores. Some are not even aware that this information is stored. Other criminals take additional steps to delete these data (i.e., beyond those described previously and depicted in Figures 7-9 and 7-10). In particular, they may use software to delete browser cache, cookies, and other files. One such software package, Evidence Shredder Pro, claims to permanently delete this information and even provides the user with a panic button, which will close all browser windows and wipe the computer

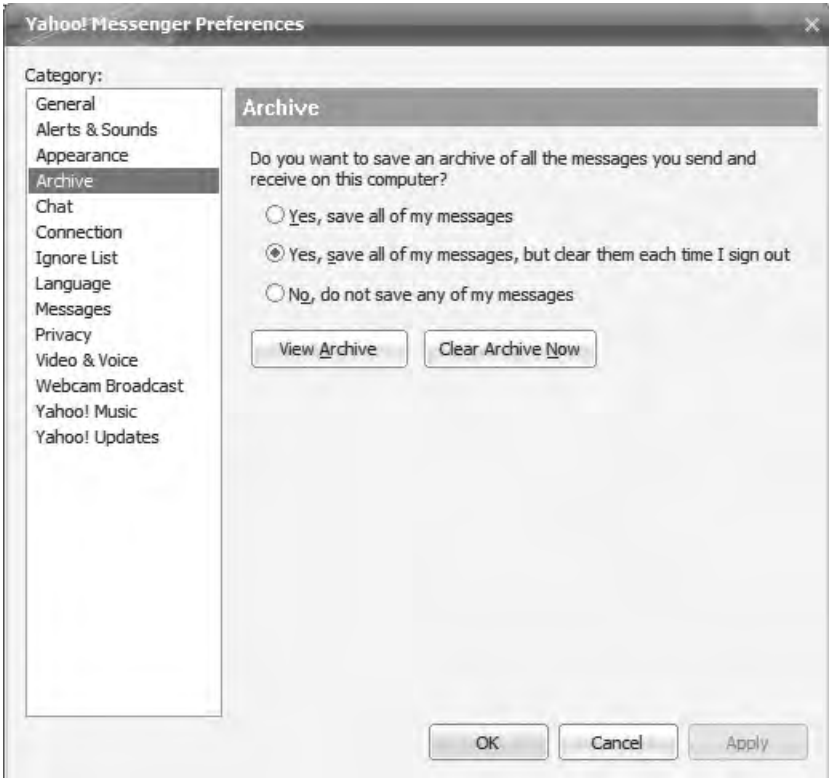

Figure 7–8

Source: Reproduced with permission of Yahoo! Inc. ©2010 Yahoo! Inc. YAHOO! and the YAHOO! logo are registered trademarks of Yahoo! Inc.

if the user clicks on it.[24] Others, such as Fixcleaner and CCleaner, offer to delete browser history, temporary files, and activity logs at the user's command.[25]

Spooler Files

As a default setting, most Microsoft Windows operating systems have print jobs "spool" to the hard drive before they are sent to the **printer**. Accordingly, a copy of the printed item is stored on the hard drive of the computer. This copy can be recovered and could provide vital evidence in the case under investigation.

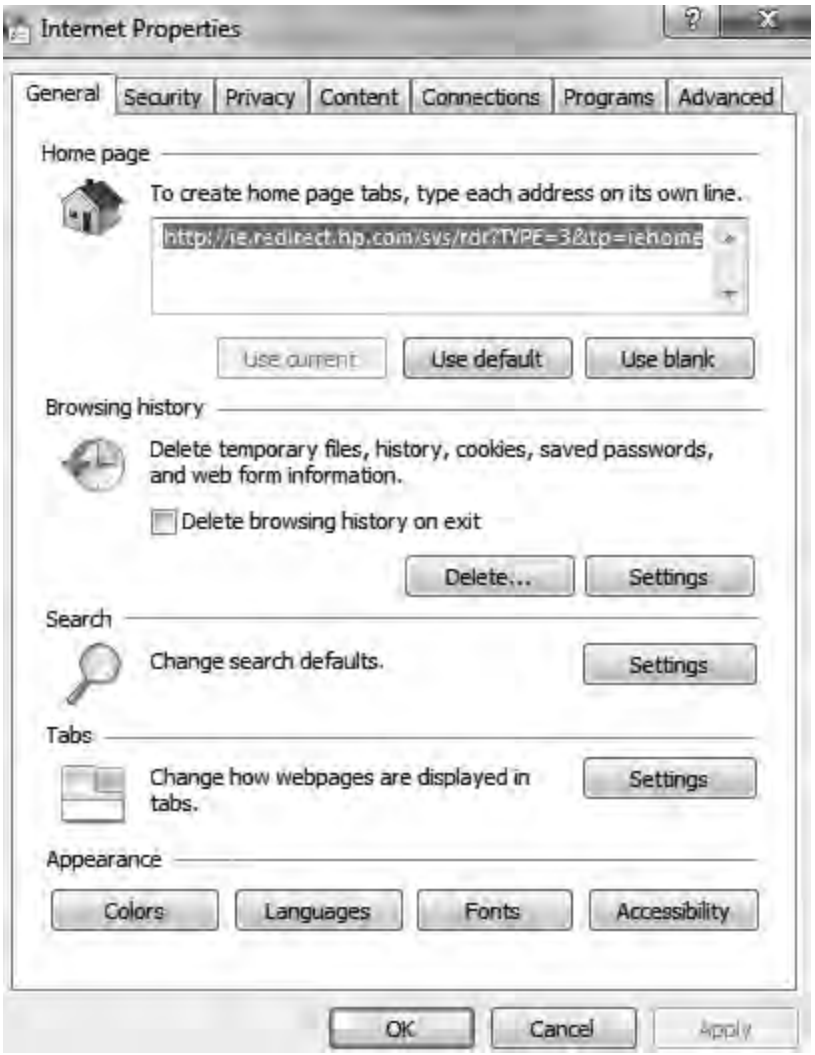

Figure 7–9

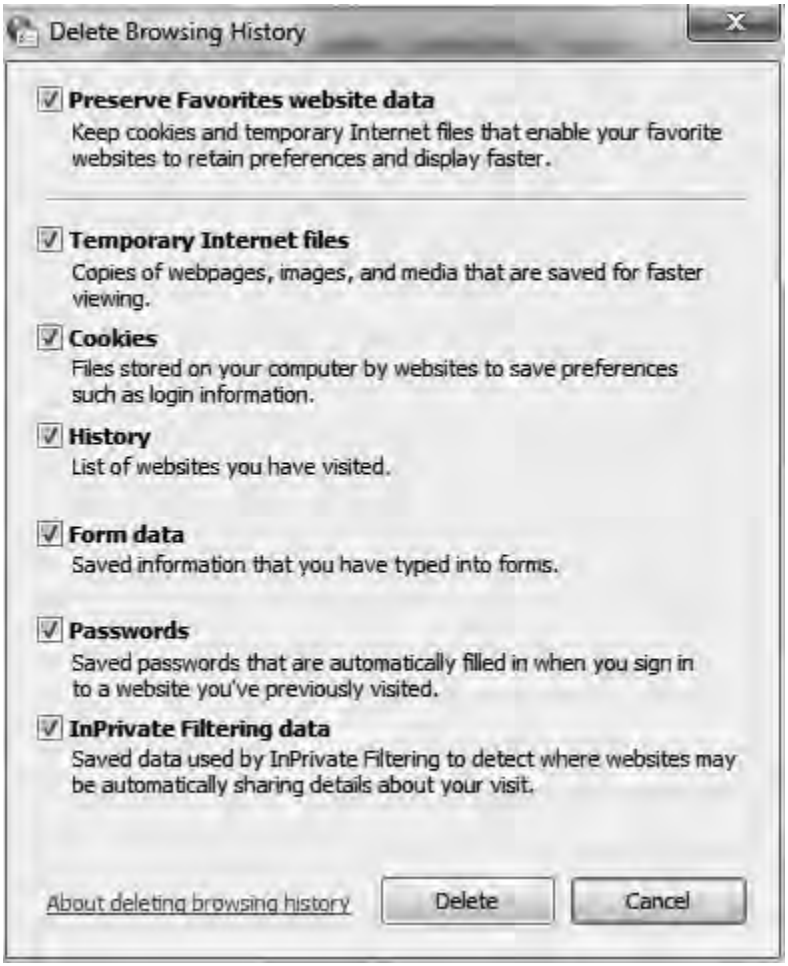

Figure 7–10

Other Data Areas on Computers

Unallocated space—space available because it was never used or because the information in it was deleted—may also contain important evidence of a crime or incident. Evidence may also be found in hidden partitions, bad clusters, and slack space.

Hidden Partitions

Individuals may choose to hide drives or files when they share computers with others, especially if these files hold confidential and sensitive data (e.g., Social Security numbers, bank information, credit card data). It is a quite simple and easy way to hide data. Criminals, however, also use the **hidden partition** technique to hide evidence of their crimes. Imagine that a member of a Russian organized crime group, Ivan, wants to hide a hard drive "G", which contains evidence of the group's money laundering transactions. To hide the drive, Ivan types in the following commands:

1. In the "Run" box on the "Start" menu, he types "cmd".
2. When the command prompt window appears on the screen, he types "cd \" (i.e., cd space backslash) and presses "Enter."
3. Ivan then types "diskpart" and presses "Enter."
4. Once Microsoft DiskPart is loaded, he types "list volume" and presses "Enter."
5. A table is displayed that contains several items, among them columns that include volumes and letters, where letters represent the letters of the drives in the computer. In this hypothetical scenario, Ivan's G drive is volume 3. Ivan then types "select volume 3" and presses "Enter."
6. To remove the drive, Ivan types "remove letter G" and presses "Enter." According to the command prompt window, the drive has been successfully removed (at times, an individual may need to reboot the computer to see this effect).

The drive has now been made invisible. To make the drive visible again, Ivan needs to go to the command prompt window, type "assign letter g", and press "Enter."

This data hiding technique can make an investigator's job extremely difficult. Windows operating systems automatically create partition gaps between each partition. Therefore, incriminating evidence can be hidden in any one of these gaps. To find the evidence, an investigator needs to search each of these gaps.

Slack Space and Bad Clusters

Certain programs (e.g., Slacker) exist that can help users hide files from computer forensics investigators in slack space. Specifically, the program breaks up the file that a user wants hidden and places parts of that file into the slack space of other files.[26]

Other areas of the computers that investigators should look at are clusters—that is, areas of the operating system where data are stored. In particular, **bad clusters**, which are

not accessed and thus overlooked by the operating systems, should be examined.[27] Criminals have been known to mark clusters as bad and hide data within them.

Peripheral Devices

Peripheral devices are devices that are not essential parts of a computer system, such as **scanners**, copiers, printers, and **fax machines**. Such devices can contain valuable information about the case being investigated. Suppose the crime being investigated is child pornography, and images of child pornography have been found on the suspect's computer. These digital images could have been generated from a variety of sources. It is possible for investigators to determine the particular device that generated the image and the make and model of the device.

For instance, the scanner may leave potential markings on scanned items that may link pictures or documents to the particular scanner. Specks or marks on the scanned item may result from dirt or scratches on the glass window where the original document was placed in and scanned. Copied documents may also be linked to a particular copy machine. Irregularly shaped characters on a copied document may be the result of imperfections on the drum in the copier that is forming the image. Similarly to scanners, if the glass window where the document is placed in is dirty or has certain imperfections, the copied document will have distinguishing markings on it that can link it to the copier.

Printers may contain logs of printer use, time and date information for printed items, and a memory card. Investigators can also determine whether a particular printer generated the image in question. For instance, banding imperfections, where some areas of a printed document look lighter or darker than other areas, constitute one way in which investigators can match a particular document to a specific printer.[28] These imperfections may or may not be visible to the naked eye. Additionally, a dot encoding mechanism, which is invisible to the naked eye, exists in many laser printers.[29] This mechanism is used by some printer companies to encode the serial number and the manufacturing code into every document that is processed by their color laser printers. A person can determine if such a mechanism exists in his or her own color laser printer by flashing a blue LED light on a printed page from the printer and viewing it under a magnifying glass.[30]

For convenience and to save space in an office or home, many individuals have bought multifunctional ("all-in-one") machines. These machines typically contain printer, scanner, and copier capabilities. In addition, these multifunction machines usually contain a hard disk that captures all of the records and images processed by the machine. This disk is of great forensics value—as long as the user or owner of the machine has not prevented the recording of such data, either by setting it not to store the data or by deleting the contents of the disk. Some devices offer users the opportunity to encrypt the data processed by the device with the installation of specific software programs.

Sometimes, multifunction machines may have fax capabilities. Fax machines may also hold important evidence. Types of data that they retain include incoming and outgoing fax numbers, documents sent and received, and transmission logs.

Evidence may also be found on peripheral storage devices such as CDs, DVDs, backup tapes, external hard drives, thumb or flash drives, and Zip drives.

Telecommunications Devices

Evidence can be retrieved from devices other than computers. **Telecommunications devices** where evidence can be found include fixed telephony, mobile phones, and answering machines.

The following types of evidence are available from **fixed telephony**:

- Calls made, received, and missed
- Voice mails
- Messages
- Favorite numbers

In mobile phones, the following types of evidence may be found:

- Names and numbers of contacts
- Calls made, received, and missed
- Date, time, and duration of calls
- Text messages—that is, **Short Message Service (SMS)** data
- Messages with a combination of text, images, videos, and sound—that is, **Multimedia Messaging Service (MMS)** data

Nowadays, mobile phones have vast storage capacities and can hold even more information than that listed above that can be used by investigators. In particular, mobile phones may be able to send e-mails, take photographs, download music, send instant messages, record and play videos, open application files (e.g., documents, spreadsheets, and presentations), and browse the Internet. Mobile phones may even store **global positioning system (GPS)** coordinates when photographs are taken, along with the time and date when the photo was created. Additionally, mobile phones may contain GPS navigation systems. Thus an investigator can pull up the GPS history and any addresses programmed into the GPS and determine which places an offender visited. Moreover, some mobile phones can link to work and home computers, thereby providing investigators with access to even more potential evidence. Further information about mobile phones and the evidence retrieved from them is provided in Chapter 12.

Finally, **answering machines** can contain, among other things, recorded voice messages (current or deleted), missed calls, caller identification information, and the last number called or dialed on the device.

Handheld Computing and Wireless Devices

Examples of handheld computing and wireless devices include **pagers** and **personal digital assistants** (PDAs). Extra care must be taken when seeking evidence from these devices

because these devices lose their evidentiary value if power is lost. The information on these devices is also easily destroyed. For instance, incoming messages can delete a pager's stored information.

Pagers may contain messages that are of interest to the investigator seeking forensic evidence. Many different kinds of pagers are available on the market, and the type of pager will determine the data that may be retrieved from it:

- A tone-only pager alerts the user that an individual has tried to contact him or her. To hear a message that an individual may have left for the user, the recipient must contact the paging service.
- Numeric pagers, as the name implies, provide data in the form of a numeric code or telephone number.
- Alphanumeric pagers can handle both text and numeric messages.
- Voice pagers actually transmit the voice messages directly to the user.

Pagers have largely fallen out of favor today, and many companies have discontinued making them. However, they are still used by some people (e.g., emergency services and medical personnel).

The procedure for handling a PDA is similar to that for handling a pager. PDAs may contain evidence of a crime or incident in its documents. Previously, these devices were limited to a single function—acting as a personal information organizer. These days PDAs can be used not only as organizers but also, among other things, to browse the Internet and send and receive text messages and e-mails; all of these actions may produce information that is pertinent to an investigation. PDA investigations are explored in further detail in Chapter 12.

Miscellaneous Electronic Devices

Another type of electronic device that may be of interest to computer forensics investigators is the **digital camera**. Evidence of images, sounds, and date and timestamps may be retrieved from the memory cards of digital cameras. Digital cameras contain a wealth of metadata in Exchangeable Image File Format (EXIF). EXIF can provide the following kinds of information:

- Date and time when a picture was taken (assuming that this capability has been set properly by the user)
- Make and model of the camera used
- Latitude, longitude, altitude, and Universal Time Coordinates (UTC) of the location where the picture was taken

The location information is obtained from the GPS capability that many cameras support. If the camera was registered after its purchase, then the manufacturer (e.g., Panasonic, Nikon, Olympus, Canon) also could have information about the consumer who purchased the camera in question.

Other Devices?

Conduct independent research and answer the following questions:

1. Which other devices might contain evidence of the crime?
2. Which types of evidence might they contain?

Tools Used to Search and Collect Electronic Evidence

Specialized tool kits are required for computer forensics investigations. A computer forensics investigator must be equipped with the appropriate kits to collect, store, preserve, and transport forensic evidence. The tools the investigator uses will depend on the operating system (e.g., Windows or BlackBerry) and type of electronic device (e.g., computer or mobile phone) to be examined. Choosing the right tools with which to examine computer system components and electronic devices for evidence is extremely important.

Before examining the evidence with the chosen forensics tool, an investigator must ask himself or herself if the chosen software is appropriate for the computer system or electronic device in question. The software used for this purpose (e.g., Encase) must be sound. To be forensically sound, a computer forensics tool must not modify the data on a computer when it is used. A **write blocker** device is used to prevent anything from being written to the hard drive or other data source. Specifically, this device blocks the wires that would communicate the data to be written to the drive.

The National Institute of Standards and Technology (NIST) has established certain requirements for computer forensics imaging tools. **Imaging** is the process by which a duplicate copy of the entire hard drive is created. Once an exact copy of a suspect's hard drive has been made, the investigator must verify that it is an exact copy. An investigator verifies this fact by computing an **MD5 hash algorithm** for both the original hard drive and the copy. If the MD5 values are exactly the same, then the copy is an exact copy of the original drive. Hashing using the MD5 or **SHA** hash algorithm has a standard of certainty even higher than that of DNA evidence. Indeed, it has been validated by many courts. For example, in *State v. Morris*,[31] prosecutors not only validated the MD5 hash process but also validated the forensic imaging process.

Once a write blocker has been set up to prevent any data from being written to a suspect's hard drive, the computer forensics investigator clones or copies the drive by writing each and every part of the drive to a blank hard drive. That is, the investigator will make a bitstream copy of the hard drive. The process by which a duplicate copy of the entire hard drive is created is known as imaging. With imaging, all data on the hard drive are copied, including metadata, system-created files, and deleted files. Sometimes, an investigator might only create a copy of an individual file; at other times, he or she might also print a hard copy of particular files. While these methods may be quick and simple, they may result in a substantial loss of information (e.g., metadata).

The integrity of an investigation is ensured by imaging an exact copy of the hard drive or other media using the proper software. In fact, in *Gates Rubber Co. v. Bando Chemical Industries, Ltd.*,[32] the court held that creating a mirror image copy of the hard drive is considered as the most complete and accurate method for processing evidence. When an investigator creates a duplicate electronic copy of the entire storage device, it prevents changes or damages to the original hard drive. By contrast, if a computer forensics investigator copies individual files on the hard drive, data on the hard drive may be unintentionally altered or destroyed. For instance, opening a file in the computer changes the time and date stamp indicating when the file was last accessed.

According to NIST, the computer forensics tools that an investigator uses must meet the following requirements:[33]

- Make a bitstream duplicate or an image of an original disk or partition
- Not alter the original disk in any way
- Log input and output errors and offer a resolution to fix such errors
- Keep correct documentation

These standards apply to software tools that copy or image hard drives. NIST has not used these standards to test other media such as mobile phones and PDAs.

When considering the use of computer forensics tools, two important questions need to be considered:

- Should examiners possess significant experience to use computer forensics tools?
- Alternatively, are computer forensics tools "idiot-proof," such that they will provide accurate information regardless of who uses them?

While some forensics tools do not require specialized training for their use, the investigator needs at least some basic level of computer expertise or at least some practice with the tool to understand how it works. As such, computer forensics investigators must have knowledge of forensics hardware and software tools and investigative methods using these tools.

The computer forensics tool that is chosen must have been successfully used in court cases. Forensics tools that meet this criterion include FTK, Encase, ILook, and e-Fense Helix and Live Response. Of these tools, the most commonly employed are FTK and Encase. In fact, the court verified this contention in *United States v. Gaynor*,[34] when it explicitly stated that FTK and Encase are the most widely used tools by computer forensics investigators.

Forensic Toolkit

Forensic Toolkit (**FTK**) is a product sold by AccessData. This software has many capabilities, including the ability to create images of hard drives, analyze the registry, scan slack space for file fragments, inspect e-mails, and identify steganography. Unlike other

computer forensics tools on the market, FTK can crack passwords. This tool can also be used to decrypt files. Indeed, FTK was used to decrypt files seized from a safe haven of a Bolivian terrorist organization that had assassinated four U.S. Marines.[35] Furthermore, this tool is quite beneficial because even if a computer crashes while using FTK software, the information will not be lost. FTK has been widely recognized by U.S. courts as a valid computer forensics tool.[36]

Encase

Encase is a computer forensics tool that is widely used by law enforcement agencies. It allows the user to create an image of a drive without altering its contents and calculates the hash value for further authentication. It can locate hidden drives or partitions within a drive, as well as other hidden files or media that some other programs would not be able to discover. Encase can search multiple file locations and devices simultaneously. In doing so, it creates an index of what is found on the computer, such as e-mails and deleted files. Overall, it is an incredibly useful tool for investigations and for law enforcement personnel.

Encase has been used by law enforcement agencies worldwide. A case in point is that of the terrorists who bombed the Indian Parliament on December 13, 2001. Investigators in India used Encase software to find evidence that the laptop of a terrorist suspect, Mohammed Afzal, was used to make the fake identification cards that were found on the dead bodies of the terrorists responsible for the bombings.[37]

The use of Encase by computer forensics investigators has been validated by U.S. courts as well.[38] For example, consider *State v. Cook*.[39] In this case, the defendant was convicted of possessing and viewing child pornography materials. Cook attempted to appeal the decision on the grounds that the forensics tool used to obtain the evidence against him (Encase) was neither valid nor reliable. The court disagreed, and upheld the validity and reliability of Encase.

ILook

ILook is another tool that is used to forensically examine computer media. Its capabilities include imaging, advanced e-mail analysis, and data salvaging (to recover files that have been deleted by the user).[40] This tool is used by the Criminal Investigation Division (CID) of the Internal Revenue Service (IRS), U.S. Department of Treasury. It is not available to the general public, but rather is provided to law enforcement agencies, government intelligence agencies, military agencies, and government, state, and other regulatory agencies with law enforcement missions.

E-fense Helix and Live Response

E-fense offers cybersecurity and computer forensics software such as Helix3Pro and Live Response. **Helix3Pro** software can be used on multiple operating systems (Windows,

Other Tools?

Numerous computer forensics tools are available on the market. Search online and find a computer forensics tool that is not mentioned in this chapter. After a forensics tool has been chosen, answer the following questions:

1. Is this tool forensically sound?
2. Why or why not?

Macintosh, and Linux). This tool is carefully designed to ensure that data are not altered during the imaging process. Local, state, and federal law enforcement agencies, along with private practitioners, have used this computer forensics tool. **Live Response** is a **Universal Serial Bus (USB)** key that is designed to be used by first responders, investigators, information technology professionals, and security professionals to collect nonvolatile and volatile data (which will be lost if the computer is shut down) from live running systems.[41]

Chapter Summary

This chapter explored evidence that may be contained in electronic devices and the tools used to collect this evidence. Electronic evidence can be found in computer systems, peripheral devices (e.g., printers, scanners, copiers, and fax machines), telecommunications devices (e.g., fixed telephony and mobile phones), handheld computing and wireless devices (e.g., PDAs and pagers), and other miscellaneous devices (e.g., digital cameras). Many hurdles arise when investigators try to extract electronic evidence, especially when criminals have employed measures to conceal evidence of their unlawful activities.

This chapter also covered the process of extracting electronic evidence from computers and the problems that investigators run into when doing so. When investigators need to examine a computer hard drive for evidence, the original disk is not used. Instead, a write blocker is used to prevent any data from being written to the drive, and then a forensics tool is used to capture a bit-by-bit image of the drive. To show the validity of the image, the original drive is hashed and then the image is hashed. If the hash values match, the copy is considered authentic.

Several computer forensics tools are commercially available that can acquire both volatile and nonvolatile data. The validity of some of these tools, such as Encase and FTK, has been upheld by U.S. courts. Some experience is required to use these tools, and the type of tool that is ultimately used depends on capabilities of the software and the operating system of the computer or electronic device that will be examined for evidence.

Practical Exercises

1. Locate a court case that either challenges a computer forensics tool or establishes its validity. Summarize the facts in this case, and briefly explain why the defendant challenged the tool used in an investigation or how the prosecution established its validity.
2. Search online for a tool or technique that criminals can use to hide evidence of their activities. Provide one example here. Include in your answer how the technique or tool works and how it makes an investigator's job more challenging.

Critical Thinking Question

Are deleted files ever really gone?

Review Questions

1. In which devices can electronic evidence be found?
2. List five types of files that may be created by the computer user.
3. What are metadata? Why is this type of data important?
4. What are event logs? Why are they important?
5. What are volatile data?
6. What is encryption?
7. What is steganography?
8. Name five types of files that are created by the computer.
9. What is imaging?
10. What is a write blocker?
11. How can an investigator validate that he or she made an exact copy of a hard drive?
12. Which computer forensics tools are widely used in the United States?

Key Terms

Answering machine
Application log
Applications and services log
Bad clusters
Cookie
Digital camera
Encase
Encryption
Event log
FAT
FAT32
Fax machine
Fixed telephony
FTK

Global positioning system (GPS)
Helix3Pro
Hidden partition
ILook
Imaging
Live Response
MD5 hash algorithm
Metadata
Mobile phone
Multimedia Messaging Service (MMS)
NFTS
Nonvolatile data
Pager
Peripheral devices
Personal digital assistant (PDA)
Pretty Good Privacy
Printer
Scanner
Security log
Setup log
SHA hash algorithm
Short Message Service (SMS)
Steganography
Systems log
Telecommunications devices
U.K. Regulation of Investigatory Powers Act of 2000
Unallocated space
Universal Serial Bus (USB)
Volatile data
Write blocker

Footnotes

[1]For further information, see http://www.casi.org.uk/ discuss/2003/msg00457.html

[2]This is the easiest way to access the file metadata of the majority of the versions of Windows. There are other ways to access "Properties." For instance, with ".doc" files, you can click on "File," then "Properties" to view metadata.

[3]211 F.R.D. 423 (W.D. Wash. 2002).

[4]Modify NTFS timestamps and cover your tracks with Timestomp.exe. (2009, March 5). Anti-Forensics. Retrieved from http://www.anti-forensics.com/modify-ntfs-timestamps-and-cover-your-tracks-with-timestomp

[5]*Ibid*. Note that the prefetcher directory can also alert users to malicious software that masks itself as legitimate ".pf" files. An example of this kind of malicious software is the "i.explore.exe.pf", which masks itself as the legitimate "IEXPLORE.EXE" (which is always in capital letters).

[6]Coll, S., & Glasser, S. B. (2005, August 7). Terrorists turn to the Web as base of operations. *Washington Post* [online], p. A01. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR2005080501138_pf.html

[7]McLean, R. (2006, April 28). Madrid suspects tied to e-mail ruse. *International Herald Tribune* [online]. Retrieved from http://www.iht.com/articles/2006/04/27/news/spain.php

[8]See, for example, spammimic.com, a website that offers such tools. Thomas, T. L. (2003). Al Qaeda and the Internet: The danger of "cyberplanning." *Parameters*, p. 115.

[9]Hezbollah is a Lebanon-based terrorist group that was founded in 1982. Hamas is a Palestinian terrorist group that was founded in 1987. Freeh, L. J. (2000, March 28). Statement for the record of . . . the Director of the Federal Bureau of Investigation on cybercrime before the Senate Committee on Judiciary Subcommittee for the Technology, Terrorism, and Government Information in Washington, D.C. U.S. Congress. Retrieved from http://www.cybercrime.gov/freeh328.htm

[10]A truck laden with explosives was driven by Ramzi Yousef and Eyad Ismoil into the garage under the North Tower of the World Trade Center in New York City on February 26, 1993. After

igniting the fuse, they fled. Six individuals died and more than 1000 people were injured. Freeh, L. J. (2000, March 28). Statement for the record of . . . the Director of the Federal Bureau of Investigation on cybercrime before the Senate Committee on Judiciary Subcommittee for the Technology, Terrorism, and Government Information in Washington, D.C. U.S. Congress. Retrieved from http://www.cybercrime.gov/freeh328.htm

[11]House of Lords, U.K. Parliament. (2007, July 17). Hansard vol. 694 col. GC5; Donohue, L. K. (2006). Criminal law: Anglo-American privacy and surveillance. *Journal of Criminal Law and Criminology*, *96*(3), 1180.

[12]See Loi n° 2001–1062 du 15 novembre 2001 relative à la sécurité quotidienne; Privacy International. (2007, December 18). PHR 2006: French Republic. Retrieved from http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559537

[13]2007 WL 4246473 (D. Vt. Nov. 29, 2007).

[14]*In re Grand Jury Subpoena to Sebastien Boucher*, 2007 WL 4246473 (D. Vt. Nov. 29, 2007), rev'd, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

[15]425 U.S. 391, 408 (1976).

[16]*In re Grand Jury Subpoena to Sebastien Boucher*, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

[17]Electronic Privacy Information Center. (1998, April 14). Key escrow. Retrieved from http://epic.org/crypto/key_escrow/

[18]Bowden, C. (2002). Closed circuit television for inside your head: Blanket traffic data retention and the emergency anti-terrorism legislation. *Computer and Telecommunications Law Review*, *8*(2), 23.

[19]The events logs of Microsoft Vista and XP can be found in a similar manner. Event logs of older versions of Windows are found more or less in the same way.

[20]150 F. Supp. 2d 1263 (D. Utah 2001).

[21]James, S. (2007, May 16). Did Melanie McGuire dismember her husband. *MSNBC* [online]. Retrieved from http://www.msnbc.msn.com/id/18688528/

[22]Culora, J. (2007, April 29). Inside cheating wife's gruesome "suitcase murder." *New York Post* [online]. Retrieved from http://www.nypost.com/p/news/regional/item_iRDscNdoDdlHoXRYMDT8tJ/0

[23]Hassell, J., & Steen. S. (December 2002/January 2003). Demystifying computer forensics. *Louisiana State Bar*, *50*, 279.

[24]For more information, see the Evidence Shredder Pro website: http://evidenceshredder.com/product_info.html

[25]For FixCleaner, see http://fixcleaner.com/; for CCleaner, see http://www.piriform.com/ccleaner

[26]Berghel, H. (2007). Hiding data, forensics, and anti-forensics. *Communications of the ACM*, *50*(4), 18.

[27]*Ibid*.

[28]Viegas, J. (2004). Computer printers can catch terrorists. *Discovery Channel News* [online]. Retrieved from http://dsc.discovery.com/news/briefs/20041011/printer.html

[29]Esguerra, R. (2008, October 24). EFF's yellow dots of mystery. Electronic Frontier Foundation. Retrieved from http://www.eff.org/deeplinks/2008/10/effs-yellow-dots-mystery-instructables

[30]Tuohey, J. (2004, November 22). Government uses color laser printer technology to track documents. *PC World* [online]. Retrieved from http://www.pcworld.com/article/118664/government_uses_color_laser_printer_technology_to_track_documents.html

[31]2005 WL 356801 (Ohio App. 9 Dist. Feb. 16, 2005).

[32]9 F.3d 823 (10th Cir. 1993).

[33]National Institute of Justice. (n.d.). Test results for disk imaging tools: dd GNU fileutils 4.0.36, provided with Red Hat Linux 7.1. US Department of Justice (NCJ 196352), p. 1. Retrieved from http://www.ncjrs.gov/pdffiles1/nij/196352.pdf

[34]2008 WL 113653.

[35]Denning, D. E., & Baugh, W. E. (1999). Hiding crimes in cyberspace. *Information Communication and Society*, *2*(3). Retrieved from http://all.net/books/iw/iwarstuff/www.infosoc.co.uk/00107/feature.htm

[36]See, for example, *Commonwealth v. Koehler*, 914 A. 2d 427 (Pa. Super. 2006); *United States v. Luken*, 515 Supp. 2d 1020 (D.S.D, August 21, 2007); *United States v. Graziano*, 558 F. Supp. 2d 304, 75 Fed. R. Evid. Serv. 1220 (E.D.N.Y., March 20, 2008); *United States v. Richardson*, 583 F. Supp. 2d 694 (W.D. Pa. October 31, 2008).

[37]Negi, S. S. (2005, August 4). Afzal to die; Shaukat gets 10-year jail term: SC acquits Geelani in Parliament attack case. *The Tribune* [online]. Retrieved from http://www.tribuneindia.com/2005/20050805/main1.htm

[38]See, for example, *Williford v. State*, 127 S.W.3d 309, 311 (Tex. App 2004); *Fridell v. State*, 2004 WL 2955227 (Tex. App. Dec. 22, 2004); *State v. Morris*, 2005 WL 356801 (Ohio App. 9 Dist. Feb. 16, 2005); *United States v. Bass*, 411 F.3d 1198 (10th Cir. 2005); *State v. Howell,* 609 S.E.2d 417,419 (N.C.App. 2005).

[39]777 N.E.2d 882 (Ohio Ct. App. 2002).

[40]See U.S. Internal Revenue Service, Criminal Investigative Division, Electronic Crimes. (n.d.). ILook investigator. Retrieved from http://www.perlustro.com/wp-content/uploads/oldwebpage.pdf

[41]See the following website for further information: http://www.e-fense.com/live-response.php