CHAPTER ❖ 5

Computer Forensics

5.1 Computer Forensics Overview 208
5.2 The Computer Forensics Process 210
5.3 Data Destruction—When Is Data Really Gone? 219
5.4 Selecting a Computer Forensics Expert 226
5.5 When to Hire a Computer Forensics Expert 230
5.6 Defining Computer Forensics Terminology 232
5.7 Beyond Computer Forensics: Investigations and Security 236

By the end of this chapter, you will be able to:

- **Know** what it takes to successfully navigate a computer forensics matter.
- **Follow** proper forensic protocols throughout all stages of the investigation: consulting, data preservation and collection, analysis, and expert testimony and reporting.
- **Prevent** data from being destroyed as a result of overwriting, physical damage, heat exposure, and magnetization.
- **Know** which factors are important to consider when selecting a computer forensics expert, including what to look for in training and experience.
- **Find** a balance between handling a matter internally and consulting an outside expert.
- **Understand** fundamental computer forensics terminology in order to successfully participate in the investigation process.

- **Look** beyond computer forensics into other challenging issues such as forensic accounting, hostile takeovers and proxy contests, and information security.

5.1 Computer Forensics Overview

It has been reiterated many times throughout this text that computers play a pervasive role in our modern society. As a federal district court judge wrote more than two decades ago, "From the largest corporations to the smallest families, people are using computers to cut costs, improve production, enhance communication, store countless data and improve capabilities in every aspect of human and technological development." *See Bills v. Kennecott Corp.*, 108 F.R.D. 459 (C.D. Utah 1985). While this was true when it was written more than twenty years ago, it is even truer today.

It takes little imagination for lawyers to see how computers and a plethora of other high-tech gadgets are impacting criminal and civil cases across the country. While these devices purportedly simplify our daily lives, or make it possible to manage large, complex enterprises in a more efficient manner, they also make it easier to commit crimes, and in some cases—whether the user is aware of it or not—they memorialize evidence of individuals' wrong-doings. To better illustrate this point, consider some of the examples below.

- Stalkers have been known to store victims' schedules on their computer or PDA calendars, and sometimes digital pictures evidencing their stalking behavior may even be found on their cellular telephone cameras.
- Small micro-drives and solid-state memory chips (such as USB drives) make it effortless for disgruntled employees to download proprietary information, conceal the storage device, and walk out the corporation's front door.
- E-mail and instant message logs track "off-the-cuff" communications that would never be memorialized with a paper and pen or in a face-to-face conversation.

All of these high-tech transactions generate billions of electronic "footprints." Whenever data is transferred between computers, "footprints" are created. Even deleting a file creates a "footprint" that in all likelihood is not gone for good. Because of the way that most computer systems save information, when a file is deleted, it *is not actually physically removed from the storage device*. Instead, when a user deletes a file, the computer simply de-allocates the space

occupied by the file, making it available for another file to be stored in the same location. But until additional information is actually saved in the precise and entire space occupied by the deleted file it is still available to be recovered, in whole or in part, by skilled computer forensics experts. Furthermore, even if data is deleted and overwritten from the hard drive, this still does not mean it is gone for good. Documents that have been copied to other media, saved in a routine system backup, or e-mailed to anyone else may well have been copied over and over again creating numerous replicas of the "electronic footprints."

Computer forensic investigators provide insight into the digital world, telling you what computer events transpired, who was involved, and when things happened. Computer forensic protocols are investigative in nature, examining and piecing together computer-related conduct and technology use. Often, these investigations focus on a small number of hard drives or backup tapes from a single individual or a targeted group of individuals. The investigator will usually need to recover and analyze deleted information, break passwords or encryption algorithms, analyze Internet activity logs, and capture time critical digital events.

The work of a computer forensics investigator is distinct from a corporate IT professional that may be responsible for actively monitoring the company's network and reporting users' activities in "real time." Active workplace monitoring and surveillance is a common activity driven not only by the need to protect company assets, but also by the very real concern about employee productivity and liability. Employee monitoring can take many forms—from installing security cameras and access badge scanners to acquiring software that watches for suspicious keywords when employees are browsing the Internet, sending e-mails, or using instant messaging services. A majority of the computer monitoring today is performed as spot-checks rather than ongoing, around-the-clock surveillance, and most companies inform their staff members of their monitoring practices. On the other hand, computer forensics investigations are typically reactive in nature, often arising out of events occurring in the past, with the hard drive or other media holding clues to the story. Many times the investigation is being conducted to specifically implicate or exonerate claims against an individual and legal action is imminent.

Perhaps the greatest example of just how pervasive and mainstream computer forensics investigations have become is the growing practice of dedicating story lines to a computer forensics investigation in legal thriller television shows and major motion pictures. From *Law & Order* and *CSI* to *Forensics Files*, we frequently see Hollywood stars dissecting

computer hard drives, monitoring instant message conversations, tracking cell phone text messages, or digging for a deleted piece of electronic evidence.

As lawyers or legal professionals, it is important to understand that computer forensics is more than what is seen on television by our colleagues or clients. Not every case is solved in forty-eight minutes (subtracting time for commercials in your average sixty minute episode) with the "good guys" prevailing. Computer forensics is an art and a science that takes years of experience to master. Part of your responsibility as legal professionals is to help your experts do their jobs by providing technical and subject matter experience to the judge and jury. This means speaking the same language as the experts when discussing facts of the case. At the same time, you do not need to become the expert yourself. Hundreds of books now exist on this discipline, and universities and educational centers offer formal degrees in the practice of computer forensics. In 2008, the American Academy of Forensic Sciences (AAFS) recognized Digital and Multimedia Sciences as an independent forensic science. This chapter will teach you as a lawyer or legal professional everything you need to know to navigate a computer forensic matter in one of your cases, from the terminology and technology to the credentials to look for in selecting an expert.

5.2 The Computer Forensics Process

The key to any forensic investigation is to gather the data in a forensically sound manner. Forensic protocols demand the media must be copied or imaged in a way that preserves the original data and results in a complete snapshot. The imaging system utilized must be nondestructive to the data and must not alter the operating system in any way during the investigation process. This includes using procedures to collect the various files, e-mail, etc. in a manner that maintains the authenticity and admissibility in future court proceedings. Forensic accuracy and all chains of custody must be maintained, or you run the risk of losing critical data or potentially rendering the entire investigation worthless.

Figure 5.1 Computer Forensics Process

CONSULTING

The most effective place to begin a computer forensic investigation is to work with the computer forensic expert in creating a strategy for collecting, analyzing, and processing the data. The strategy should include analysis of where the critical information might reside, as well as the identification of protocols that will ensure the admissibility of the data into evidence in a court of law should it become necessary.

Counsel should convey to the computer forensic expert information about the case and the desired outcomes of the investigation. Best practices dictate that the investigator identify where key evidence is likely to be located and then piece together user and system information in order to obtain a comprehensive and thorough account of the technological landscape. Understanding where data resides, what conduct is at issue, and what output is sought should occur before any digital data is ever examined.

DATA PRESERVATION AND COLLECTION

Once the location of the relevant data is identified, it must be retrieved. Computer forensics experts can retrieve data from virtually any storage device or computer operating system, including many antiquated systems. However, electronic evidence—like other types of evidence—is fragile and often volatile. Entering data, loading software, performing routine system maintenance, or simply booting a computer can destroy certain files or metadata that are stored on the hard drive. Over time, data that may be important evidence in a case can be overwritten and destroyed through the routine use of a computer. Just as a medical examiner takes extreme caution to ensure that the body, blood evidence, fingerprints, and hair follicles are preserved in a murder case, computer forensic examiners must take extreme caution to ensure that data is not damaged, computer viruses are not introduced and a proper chain of custody is maintained. Failure to adhere to strict industry standards regarding data collection may not only result in the loss of critical data, but may also impinge upon the reliability of any data that is recovered, potentially rendering it inadmissible in a court of law.

The first task at hand is to create a complete and pristine copy of the computer media, since performing computer analysis work on original media is undesirable and can be a grave mistake in the electronic evidence industry given spoliation concerns. Instead, best practices provide for the making of an "image" whenever possible

so that the forensic examiner can work on an exact duplicate of the media rather than the original. Counsel should not assume that simply because the computer, disk drive, or other storage media is old or damaged that the data is therefore inaccessible and the media cannot be imaged. Data recovery techniques may be able to restore the media to semi-working condition—just enough to preserve a copy of the data. However, it should be remembered that where data recovery must be accomplished, questions of spoliation can arise, so good documentation and chain of custody should be a part of the process. Sometimes two copies of the original media are made. A copy of the media is made for archival purposes and a copy of the copy is made for the investigator to use in his or her recovery and analysis.

The imaging process utilizes proprietary or commercial imaging software to provide an exact duplication of the data contained on the media. The snapshot is a perfect byte-by-byte copy of the drive, including all of the unused and partially overwritten spaces—the nooks and crannies where important e-evidence may reside. The imaging process is non-destructive to the data and does not require the operating system to be turned on, thus ensuring that the system is not altered in any way during the imaging process, preserving its evidentiary value. It is not commonly understood that the mere act of booting a computer may damage critical evidence and may change metadata. Also, booting the system may cause the hard drive to be written to with startup data in a way that may overwrite information that would have remained more accessible if the boot did not occur.

There are two common methods for hard drive imaging—the software approach and the hardware approach. The tools for both these methods are designed to be used either in the expert's forensic lab or onsite at the client's location, and both approaches will render valid and complete hard drive images if used properly. Counsel will want to inquire about the imaging method used for copying the target data, and should the case proceed to trial, be prepared to examine the forensic expert under oath regarding the exact steps followed. As such, it is important to understand from a high level the main methods and steps in imaging a hard drive.

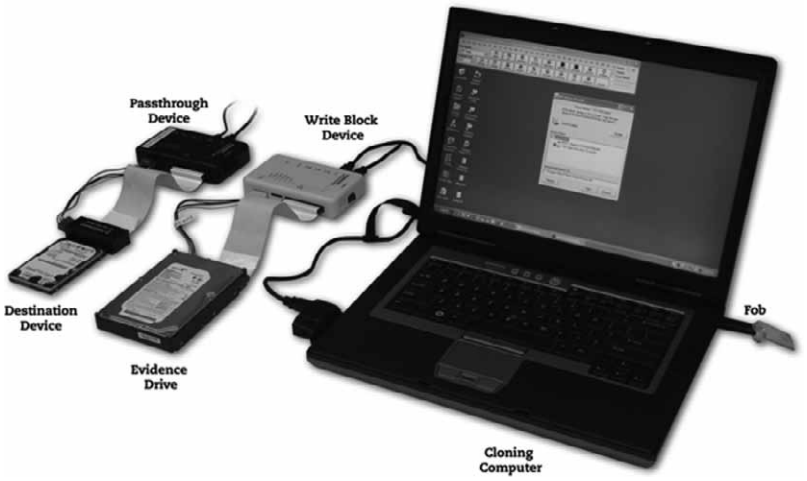
Hardware imagers (also called cloners) are specialized devices built into a small box about the size of your hand that capture a bit-by-bit copy of the hard drive. This is generally the fastest way to image a hard drive. One disadvantage of hardware imagers or cloners is that they are usually designed for one type of hard drive. Although these devices are generally very reliable, many still have difficulty

recognizing and imaging all the various brands of hard drives on the market today, and most do not effectively handle any errors that may arise in the process of imaging the original hard drive. Common hardware tools for imaging are the forensics tools made by Logicube and the ImageMASSter product suite made by Intelligent Computer Solutions.

Computer forensic investigators also can use software tools to image a drive. These products are very portable but usually slower at imaging data than some of their hardware counterparts. They also usually require more configuration than the hardware imaging tools. Common products for imaging include: Guidance Software's EnCase, Access Data's Forensic Tool Kit (FTK), New Technologies' SafeBack, SnapBack's extraction tools, and Linux "dd." Common backup software, such as Symantec Norton Ghost, should not be used for forensic imaging as they often modify the original media and/or do not copy all of the data on the original media.

Whether your investigator is using hardware imagers/cloners or a software tool to image a hard drive, it is most important to ensure that the product is specifically designed for computer forensic work. Another important step, whether using hardware or software, is to use a write-blocking device—a specially designed piece of hardware that

Figure 5.2 Hardware Imaging Setup



ensures the data on the original hard drive is not altered in any way in the imaging process—for added protection.

The final step in creating an image is to verify the accuracy of the image compared to the original hard drive. The most commonly used method for verifying that an image of a hard drive is a perfect copy is called hashing. This process involves running one of two industry standard algorithms—either the MD5 or Secure Hash Algorithm (SHA)—on the original drive and again on the working copy and then comparing the results. If the two hash values are identical, the copy is complete and accurate. If the hash values differ, the copied hard drive is not an exact match to the original. While hashing is not a mandatory process that renders the copy worthless, computer forensic investigators can diminish admissibility and credibility claims by following this proper forensic principle. It should be recognized that running hash value calculations and comparisons takes time, and can lengthen the process of capturing data.

One of the last important points at this stage in the computer forensics process is maintaining authenticity of the data. Counsel should be certain the computer forensics expert maintains a complete and documented chain of custody for all data that is collected. This means adhering to the following chain of custody procedures.

(1) Uniquely identify each item of property to be placed under chain-of-custody control. This means the investigator should be able to examine the item and be able to tell if it is the same one described on the chain of custody form. Some items will have a manufacturer's name, model number, and serial number, but others (such as tapes or removable media) may have no intrinsic unique identifier. They can be identified by marking, or by unique numbered or bar-coded labels.
(2) Document who the media was received from, who authorized its removal, the location where the media was received, and the date and time at which the investigator took control of the media. If an item is received by mail or other courier service, document this transaction as well.
(3) Keep a continuous record of custody of the item, from the time the item is acquired, until it is transferred out of the investigator's control. Chain of custody records can be paper-based with handwritten tracking methods or electronically-based with computerized tracking methods.

Figure 5.3 Talking Technology: *Standards for Handling Digital Evidence*

At the International Hi-Tech Crime and Forensics Conference in October 1999, the International Principles for Computer Evidence were promulgated by the International Organization on Computer Evidence (IOCE). Even though these guidelines were drafted almost a decade ago, they are still pertinent today and applicable to experts or consultants that handle digital evidence in any capacity. They are as follows:

- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person must be forensically competent.
- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
- Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

Implementation of these requirements requires that a computer forensic expert have in place best practices polices and procedures for preserving the evidence in its custody.

See FBI Laboratories publication Forensic Science Communications, Vol. 2 No. 2, April 2000. *See also* Forensic Examination of Digital Evidence:

A Guide for Law Enforcement, National Institute of Justice, April 2004.

There are several methods for gathering the target data through imaging depending on the specifics of the client's situation.

- **Onsite Data Collection—**Large organizations with multiple office locations, many targeted custodians, complex cases or simply implementing a precautionary measure should consider bringing the computer forensics expert onsite to collect the data.

Data collection can often be completed during non-business hours so that business operations are affected only for a limited time (if affected at all), or so that the target of an investigation is not even aware that anything has occurred. Depending on circumstances, it may be necessary to image servers, end-users' computers, or both. Consultation with the experts can help to plan the collection effort. Such planning is important to ensure that the expert will have the right equipment and sufficient storage devices to enable them to complete the project.

- **Do-It-Yourself Data Collection—**If the client has trained and experienced technical staff, the company may be able to image the drives on their own and transport them to the investigator for analysis. While imaging is relatively straightforward given the sophisticated hardware and software products available, untrained individuals should not attempt to perform this work. The risks associated with damaging or deleting data are high if proper data collection procedures are not followed. Understand that imaging must be done with forensic accuracy and must appropriately protect the images. Determine how likely the corporate personnel will be able to withstand a cross-examination on forensic practices, and be able to demonstrate that the work was done correctly.
- **Mail or Courier—**If the computer or media is not needed on a day to day basis, the client can mail or courier the original media (for example a hard drive or a laptop computer) to the expert's laboratory for imaging and analysis.

Figure 5.4 Talking Technology: *When Is Data Recovery Needed in a Forensic Investigation?*

Data recovery is not necessary in every computer forensic matter. If a hard drive has suffered physical damage (such as liquid spilled on the media or a hammer hitting the media) or logical damage (such as a computer virus or program malfunction), data recovery techniques will need to be used to try and recover the data prior to imaging. If required, a handful of computer forensic experts have access to special "clean room" facilities in which engineers can open the hard drive's protective metal casing and disassemble the drive to diagnose and remediate problems prior to beginning the computer forensics investigation. A clean room is an environment where precision parts can be assembled without contaminating sensitive components such as the physical

magnetic surface of the media (i.e., hard drive platters). Clean rooms have a rating system indicating the number of contaminating particles per cubic inch. For example, a class 100 clean room environment contains fewer than 100 particles of contaminants per cubic inch. A clean room environment should be used to minimize the risk of further damaging a hard drive when it becomes necessary to open it to repair or replace damaged internal components. Examples of this include damage to internal circuits, a damaged motor or bearings, platters that are out of alignment, fire and/or water damage. In computer forensics investigations a clean room must be used, for example, if circuit boards or cable connectors have been damaged or destroyed or if pieces of the drive need to be replaced to make it readable again.

ANALYSIS

The computer forensics analysis begins once the data collection phase is complete. The first step in the computer forensics investigation is to examine the image of the media. This commonly includes:

- *Accessing active data files*. Active files are data files that are readily available to the user upon accessing the media.
- *Accessing and recovering e-mail data*. E-mail is often a primary piece of the project and requires separate handling and processing.
- *Recovering deleted data files*. Deleted files are files and directories that were recovered after being deleted from the active data. Some files are recovered completely and are easily identifiable, while in other instances only fragments of files (i.e., those located in slack and unallocated data) may be recoverable. Factors influencing the probability of recovery of deleted files include: how the files were deleted, the amount of time passage and computer usage since deletion, the use of file deletion/destruction programs, etc.
- *Accessing password protected and encrypted files*. Most computer forensics engineers should scan data to determine if any security features have been placed on the data. They then can attempt to "break" password protection or encryption to access the contents of the file. This can be accomplished by using propriety technology tools that "work" on breaking the passwords or encryption for a specified period of time, or by human intervention using passwords that are discovered in other portions of a

data set. For example, if software is run on number of files on a hard drive, it is common to discover a pattern of password use. Those passwords can then be used to look at data files in another location, or on other media utilized by the same person. In password and encryption breaking scenarios, this issue is more often *not* whether the encryption can be broken, but how much time is reasonable to spend in the attempt. It is important to understand that computer forensics specialists cannot break all passwords. Some security software can be defeated through reverse engineering, but other systems are extremely secure and cannot realistically be defeated.

Beyond retrieving files, computer forensics investigators often can determine whether computer evidence was tampered with, altered, damaged, or removed. They examine hidden information associated with recovered files (including deleted data or data from unused storage areas on the media) and provide a historical ledger of the content contained in the files. In essence, the investigators reveal evidence of the conduct of those who had access to the drive. Computer forensics engineering analysis may include:

- Recreating a specific chain of events or user activity, including Internet activity and e-mail communication;
- Searching for key words and key dates;
- Searching for copies of previous document drafts;
- Searching for privileged information;
- Authenticating data files and the date and time stamps of those files;
- Determining whether devices like flash memory sticks have been used with a particular computer;
- Comparing and contrasting computer code to determine whether a particular program is original or copied from a similar program;
- Advising on what evidence is likely to be found on the computer media and identifying the most effective methods to search for relevant data;
- Converting data to a more user-friendly format while retaining the pertinent metadata, such as Apple® e-mail converted to Microsoft® Outlook®; and
- Evidence of data copied off to another location or piece of media.

The amount of information that is recoverable through the computer forensic recovery and analysis processes varies on a case by case

basis; however, the possible results are endless. Files that are recovered and considered key to the investigation are transmitted to counsel, usually in a native format on a CD-ROM, DVD-Rom, or hard drive for legal review. At this point, counsel can continue building his or her theory of the case and determine whether the files need to be produced to the opposing party in discovery.

EXPERT TESTIMONY AND REPORTING

Once the data analysis is complete, computer forensics engineers can help support the lawyer and client's court case by customizing reports about the data collected and produced, providing data for affidavits or other pleadings, and giving expert testimony and Rule 26 expert reports. This step in the process usually requires interaction between counsel and the investigator.

5.3 Data Destruction—When Is Data Really Gone?

Some of the most common questions litigators ask computer forensics experts are: "How much data is recoverable if my client redeployed the computer and the new user has been overwriting data that is relevant to our investigation?" "How much data is recoverable if my client reformatted, defragmented, or wiped the hard drive?" "How much data is recoverable if the hard drive was damaged due to fire, water, or other physical damage?"

Talking Technology: *Destroying Computer Evidence*

The common ways that computer data is permanently destroyed include:

- **Overwriting**—Overwriting old data with new data during everyday computer use or using overwriting software to write a pattern to every addressable location of a hard drive, essentially returning the drive to a factory (blank) condition.
- **Physical Destruction**—Shredding the hard drive platters by manually breaking them into several small pieces or utilizing a drive shredder.
- **Heat**—Exposing the media to extreme heat, usually in excess of 300 degrees Fahrenheit.
- **Magnetic Destruction**—Using a degaussing device with a magnetic field strong enough to disrupt the magnetic orientation of the data on the platters.

DESTROYING DATA BY OVERWRITING

Every time a computer is utilized, the user inevitably overwrites something. Thus when a computer is redeployed, the new user may unintentionally overwrite the old user's previously deleted data through continued use of the computer. In a simplistic view, every computer storage device contains files (used space) and free space (unused space). Each time the computer is used it may modify the metadata of the files in the used space and may overwrite previously deleted data that exists in the unused space.

- Modification of metadata of existing files. As the operating system starts up, it accesses several files during the boot process and may modify temporary cache files (e.g., Windows swap files) that may contain clues to the computer's past environment. Also, if any files are "touched" by the user, the files' "last accessed date" may change.
- Modification of free space. When the computer needs to create new files or grow existing files, it requests a new section of space (a "cluster" or "block") from the free space area of the media. Different computer systems manage free space reuse in different ways. Some may contain intelligence to use the "least recently used" free space block when requesting new blocks. In this manner, the oldest free space block will be used first, and only when all free space blocks have been used at least once, will it begin to reuse (overwrite) old free space blocks. Other file systems may respond to free space requests by writing data to the closest available free space block in an attempt to optimize the data writing process. Regardless of the file system and operating system, a risk of overwriting free space exists. The more the computer is in use or the less free space there is available on the drive, the probability of overwriting old (free space) data increases.

Standard computer maintenance and routine computer use overwrites data, often without the knowledge of the user. But there are also instances where users employ formatting, defragmenting, wiping, "Disk Cleanup" and other techniques to intentionally destroy all traces of electronic evidence. It should be noted that in some cases, a computer forensic examiner can definitively determine that deliberate destruction has occurred, and while the destroyed data is gone, the fact that the destruction occurred may be significant in and of itself, particularly if there was a duty to protect or preserve the data, or a protective order was in place.

- **Formatting**—Formatting a drive is a quick and easy housekeeping task that eliminates the document indexes and file/folder pointers on a computer hard drive. Many IT departments format a user's hard drive to give the computer a fresh start when it is deployed to a new user. In most cases, the formatting does not actually get rid of the pre-existing data on the hard drive. The contents of the documents, files, and folders still physically exist on the drive and are often fully recoverable by computer forensics experts using best practice industry standards. If a drive looks blank or the operating system looks empty upon booting, the files and folders may still be present on the drive. Shut off the computer immediately and consult a computer forensics expert to inquire as to whether data may be recoverable based on what has been done to it.
- **Defragmentation**—Defragmentation can be compared to a reorganization of the computer's filing cabinet. To make the computer run more efficiently, all of the files are condensed to the smallest space possible, reorganized, and placed at the front of the drive. This is another IT tool to keep the computer functioning at peak performance. Defragmenting a computer will not harm the active data (the data that a user can access on their own from the desktop) but may render what otherwise would have been recoverable deleted data (the data that only a forensic investigator can recover) virtually unrecoverable. This depends on the size of the drive, amount of data, and order of operations. Sometimes defragmentation can even create additional copies of computer evidence on the hard drive. A complete computer forensics investigation will help identify what is recoverable after defragmentation.
- **Wiping**—Wiping utilities are frequently used by IT staff when a computer is going to be redeployed within the company (for example after an employee leaves the company), or sold or donated outside of the company. In addition, it is our experience that individuals attempting to permanently destroy evidence of their activity, such as bad acts, committed on the computer will purchase and run wiping utilities. When a drive or portion of a drive is wiped, a software program is used to overwrite data with a specific or randomly generated pattern of data. If run properly, a wiping utility will make the data unrecoverable by commercial computer forensics experts. Depending on the software utility that was run, computer forensics experts might be able to tell the date, time, and specific program used to conduct the wiping.

While there are several tools that accomplish the task of wiping a hard drive, some are more common than others for "persons of interest" trying to destroy data. Probably one of the most popular tools, for which a whole body of case law has emerged, is called "Evidence Eliminator." For example, a Northern District of Illinois case directly on point is *Kucala Enters., Ltd. v. Auto Wax Co.*, 2003 WL 21230605 (N.D. Ill. May 27, 2003). In this patent suit, the district court ordered the inspection of the plaintiff's computer. The defendant hired a computer forensics investigator to create a forensic image of the computer hard drive and analyze the results. The computer forensics expert was able to identify that the night before the computer image was created, a wiping utility called "Evidence Eliminator" was used to delete and overwrite over 12,000 files. The expert further determined that 3,000 additional files had been deleted and overwritten three days earlier. Even though there was no clear indication that relevant evidence was among the destroyed files, the court described the Plaintiff's actions as "egregious conduct" and emphasized the Plaintiff's apparent intent to destroy evidence that it had a duty to maintain. The magistrate judge recommended to the district court that the plaintiff's case be dismissed with prejudice and that the plaintiff be ordered to pay the defendant's attorney fees and costs incurred in defending the motion.

The *Kucala* case is only one of a plethora of other cases involving the use of Evidence Eliminator or other similar products (such as Window Washer, Cyberscrub, and BC Wiping). Some additional cases involving these wiping products are summarized below.

- *Orrell v. Motorcarparts of Am., Inc.*, 2007 WL 4287750 (W.D.N.C. Dec. 5, 2007). In this sexual harassment suit, the plaintiff filed suit based on receipt of inappropriate e-mails from co-workers and customers. Before returning her work laptop to the defendant, the plaintiff utilized "Evidence Eliminator" to wipe the hard drive, allegedly to prevent any personal or confidential information from being exposed. Alleging improper destruction of evidence and incomplete compliance with discovery obligations, the defendant filed a motion to compel seeking production of the plaintiff's home and work computers and an order prohibiting further destruction of evidence. Agreeing with the defendant, the court ordered the plaintiff to produce her home computer for forensic examination. The court also ordered the plaintiff not to further destroy relevant evidence. Additionally, the court warned the plaintiff that failure to comply may result in sanctions including dismissal of the case with prejudice and payment of the defendant's attorney's fees.

- *Commc'ns Ctr., Inc. v. Hewitt*, 2005 WL 3277983 (E.D. Cal. Apr. 5, 2005). The plaintiff brought a motion for terminating sanctions against the defendant for violating a magistrate's discovery order that required the defendant to produce a compact disc containing mirror images of any responsive hard drives in the defendant's possession. Although the defendant produced three CDs, the CDs were not mirror images of the defendant's hard drives. The defendant supplemented the production with ten discs, which also failed to contain mirror images. Days after the production, the defendant ran a software wiping program called Evidence Eliminator on three of the hard drives. The defendant claimed he purchased the program only after learning the true meaning of the "mirror image" as set forth in the magistrate order. He further stated he used the program to cover up evidence of an affair and to prevent disclosure of embarrassing Web sites. The magistrate found this conduct "a stark affront to the judicial process." Noting the destroyed data was "gone forever," the magistrate awarded the plaintiff over $145,000 in costs and fees. The magistrate further recommended that a default judgment be entered for six out of the eight causes of action.
- *DirecTV, Inc. v. Borow*, 2005 WL 43261 (N.D. Ill. Jan. 6, 2005). The plaintiff brought a motion for summary judgment, claiming the defendant used the plaintiff's satellite television signal without authorization and then spoliated evidence of the unauthorized use. The court had previously awarded sanctions against the defendant for deliberately destroying evidence by using "Evidence Eliminator," a software wiping utility program, to erase electronic evidence requested by the plaintiff. The plaintiff's computer forensic expert examined the computer and recovered some of the deleted files, including programs used by satellite pirates to intercept the plaintiff's encrypted signal and files listing the name of piracy websites the defendant visited. Other files were permanently deleted. The defendant argued "somebody else" was responsible for these actions, even though he declared the computer remained in his exclusive possession. Granting the plaintiff's summary judgment motion, the court noted, "[t]he fact that [the defendant] deleted certain files on his computer only five weeks after the start of this litigation creates an inference that he destroyed evidence that would have been harmful to his defense."
- *United States v. Gordon*, 393 F.3d 1044 (9th Cir. 2004). After discovering missing stock shares, an employer suspected embezzlement and requested the defendant's laptop computer for

> examination. The employer specifically told the defendant not to delete anything from the hard drive. A computer forensic analysis revealed the defendant attempted to overwrite files on the computer by running "Evidence Eliminator" at least five times the night before he turned over the computer. The defendant was convicted of embezzlement and ordered to pay restitution, including reimbursing the employer for a portion of the investigation costs. On appeal, the defendant argued the trial court should not have awarded the employer investigation costs, including the costs of the forensic examination. The appellate court rejected this argument and affirmed the district court's award, noting the defendant "purposefully covered his tracks as he concealed his numerous acts of wrongdoing from [his employer] over a period of years. As the victim, [the employer] cannot be faulted for making a concerted effort to pick up his trail and identify all the assets he took amid everything he worked on."

Other less sophisticated ways to intentionally destroy computer data include copying or saving "garbage files" to the hard drive in attempts to fill the remaining "free space" where deleted files reside, thus removing all traces of data on the drive. A specific example of this tactic occurred in *3M v. Pribyl*, 259 F.3d 587 (7th Cir. 2001). In this case, the plaintiff brought suit against three former employees for misappropriation of trade secrets. The appellate court affirmed the trial court's negative inference instruction to the jury where the one defendant committed spoliation of evidence by downloading six gigabytes of music files onto his laptop. This act, which occurred the night before the defendant was to turn over his computer pursuant to the discovery request, destroyed numerous files sought by the plaintiff. The lesson learned from this decision is that spoliation can be found not only when a party has deleted data but also when they have simply downloaded data in what is typically thought to be the open space of a computer hard drive.

DESTROYING DATA BY PHYSICAL DAMAGE OR HEAT EXPOSURE

Some individuals will try to cause physical damage to the media or set the media on fire in attempts to destroy the data contained therein. For example, slamming a drive (sometimes still in the PC or laptop) onto a concrete floor, setting the drive on fire, submerging it in water (or other liquids), or even shooting a hole through it. In one case, a perpetrator

squirted charcoal lighter fluid into the cooling slots of a PC case and then ignited the fumes. He fried the majority of the PC, but computer forensics experts were still able to recover data from the hard drive for analysis. These attempts are typically unsuccessful because computer data is not easily destroyed in this manner. Only if the media is exposed to heat at least 300 degrees Fahrenheit, or is shred into many pieces, is the data gone for good.

Figure 5.5 In the News: *Destroying Computer Evidence*

Overwriting, physical destruction, heat, or magnetizing computer media are not the only ways to permanently destroy computer evidence. These new story excerpts below reveal the lengths some people will take to obliterate all record of computer activity. What these individuals might have forgotten is that even if the computer is gone, there might be record of the fraud contained on network shared drives or company backup tapes . . . .

Rite Aid Ex-Lawyer Said to Toss Evidence
By THE ASSOCIATED PRESS
October 2, 2003

http://www.nytimes.com/2003/10/02/business/02RITE.html?dlbk

ARRISBURG, Pa., Oct. 1 (AP)—A former chief counsel of the Rite Aid Corporation told a colleague that a computer used to create backdated letters that inflated benefits for some executives was dumped in the ocean, according to testimony Wednesday.

"He said they'll never get her computer now, it's in the Atlantic," Mr. Noonan said that Mr. Brown told him.

Head of Rove Inquiry in Hot Seat Himself:
Bloch Used Private Company, Geeks on Call, to Delete Files On His Office Computer
By JOHN R. WILKE
November 28, 2007; Page A6
http://online.wsj.com/article/SB119621772122306160.html?mod=hpp_us_whats_news

> WASHINGTON—The head of the federal agency investigating Karl Rove's White House political operation is facing allegations that he improperly deleted computer files during another probe, using a private computer-help company, Geeks on Call. Bypassing his agency's computer technicians, Mr. Bloch phoned 1-800-905-GEEKS for Geeks on Call, the mobile PC-help service.
>
> Mr. Bloch had his computer's hard disk completely cleansed using a "seven-level" wipe: a thorough scrubbing that conforms to Defense Department data-security standards. The process makes it nearly impossible for forensics experts to restore the data later. He also directed Geeks on Call to erase laptop computers that had been used by his two top political deputies, who had recently left the agency.

DESTROYING DATA BY MAGNETIZATION

Another common way to destroy computer data is by magnetization. Use of a degaussing device with a magnetic field strong enough to disrupt the magnetic orientation of the data on the platters will permanently destroy computer evidence. Holding a strong magnet up to a hard drive, however, will not erase any data. Hard disk assemblies are designed to shield the drive from disruptive magnetic fields during the normal course of a hard drive's life. It takes an extremely powerful commercial grade magnetic field to penetrate the hard drive enclosure to actually impact the platters inside. Some people may be successful in destroying computer evidence by opening the drive and placing a strong magnet next to the exposed platters.

5.4 Selecting a Computer Forensics Expert

For litigators, working with a computer forensic expert is really no different than working with any other type of expert or consultant. From arson investigators to zoology experts, computer forensic investigators are another arrow in your quiver to help you hit the bulls-eye in your case.

However, the expanded role that computer forensics plays in internal investigations and litigation today has precipitated an inevitable rise in self-proclaimed "experts" in the field of computer forensics. How can you become an expert when selecting a computer forensic

expert? As with choosing any other expert, it is crucial that counsel scrutinizes the computer forensic expert's qualifications and experiences. The expert must have the proper experience and training to successfully identify and attempt to retrieve possible evidence that may exist on a computer system.

TRAINING

Lawyers should not be alarmed if the individual has been working in the field for several years but does not have a computer forensics degree from an accredited college or university. Most computer forensic investigators have learned their skills on the job as lawyers, police officers, or computer software engineers. However, the computer forensics profession is growing. Colleges and universities are increasingly starting to offer courses, degrees, and specializations in computer forensics related areas, and in years to come, formal education in computer forensics will become the norm.

While an advanced degree in computer forensics is not imperative, computer forensic investigators must have advanced computer knowledge, with specialized data recovery and computer investigation analysis skills. Specifically, look for someone with formalized training, particularly looking for law enforcement training courses offered by large departments and agencies, and certification courses offered by recognized private sector companies. Some of the most common computer forensics and related certifications are described below.

- **EnCase Certified Examiner (EnCE)**—This program certifies both public and private sector professionals in the use of Guidance Software's EnCase computer forensic software. EnCE certification acknowledges that professionals have mastered computer investigation methodology as well as the use of EnCase during complex computer examinations. Recognized by both the law enforcement and corporate communities as a symbol of in-depth computer forensics knowledge, EnCE certification illustrates that an investigator is a skilled computer examiner.
- **Access Data Certified Examiner (ACE)**—This program certifies both public and private sector professionals in the use of Access Data's Forensic Toolkit (FTK) computer forensic software. The certification process consists of two parts: a practical based assessment and a knowledge based assessment.
- **Certified Forensic Computer Examiner (CFCE)**—This credential was the first certification demonstrating competency in computer forensics in relation to Windows based computers. The CFCE

training and certification is conducted by the International Association of Computer Investigative Specialists (IACIS), a non-profit, all volunteer organization of current and former law enforcement members.

- **Certified Electronic Evidence Collection Specialist (CEECS)**—Also sponsored by IACIS, this course is designed to instruct personnel on how to collect electronic evidence in a forensically sound manner. This course is offered only to law enforcement officers and law enforcement support personnel.
- **Certified Information System Security Professional (CISSP)**—A certification reflecting the qualifications of information systems security practitioners. The CISSP examination consists of 250 multiple choice questions, covering topics such as Access Control Systems, Cryptography, and Security Management Practices, and is administered by the International Information Systems Security Certification Consortium or ((ISC) 2).

In addition to the above certifications, several other organizations offer computer forensic training classes that are recognized in the industry.

- **National White Collar Crime Center (NWCCC or NW3C)**—This federally funded non-profit corporation offers training only to public sector (law enforcement) professionals. It does not offer certification in computer forensics but is recognized as offering good training sessions in computer forensic and investigative techniques.
- **The National Consortium for Justice Information and Statistics (SEARCH)—**This non-profit organization offers training only to public sector (law enforcement) professionals. It does not offer certification in computer forensics but is recognized as offering good training sessions in computer forensic and investigative techniques.
- **Federal Law Enforcement Training Center (FLETC)**—This is the training center for most Federal Agencies other than the FBI, which has its own training academy. FLETC offers a Seized Computer Evidence Recovery Specialist (SCERS) training course/certification but only to public sector (law enforcement) professionals. It is widely recognized as a good certification program in computer forensic and investigative techniques.
- **International Association of Computer Investigative Specialists (IACIS)**—This is an international volunteer non-profit corporation composed of law enforcement professionals dedicated

to education in the field of forensic computer science. IACIS members represent federal, state, local, and international law enforcement professionals. Regular IACIS members have been trained in the forensic science of seizing and processing computer systems.

EXPERIENCE

Seek an expert that has extensive computer forensic consulting experience as well as sufficient hardware and software tools to utilize that experience. When interviewing a potential expert, request information on how many cases he or she has worked on in the past. Determine if the expert has sufficient direct experience with the relevant electronic media and technology at issue in your case. Inquire about what hardware and software tools he or she will utilize in imaging and investigating the media. Are they using off-the-shelf tools or internally developed tools? How will they handle damaged media? Have they investigated PDAs and cell phones? Have they investigated data contained on servers? A seasoned expert will be able to determine what information is technically feasible to collect, how to best analyze that information, and how to interpret the resulting findings for you. They will deliver that information in a consultative manner—guiding you through the uncharted waters like a skilled navigator.

Additionally, request information about the processes he or she utilizes and the results typically achieved. A firm grasp of basic data handling concepts and computer forensic best practices is the first step to ensure a successful investigation. Check to see if the expert adheres to strict industry standards regarding data collection and preservation. The credibility of any recovered data is based on proper evidence handling. If a forensic analysis is done on a piece of media, an expert must make a mirror image—a bit-by-bit snapshot of the original drive—in order to preserve the integrity of the original media. Ask to see a sample of forensic reports typically issued in the course of an investigation.

Also, obtaining an admissible list of the cases in which they have provided deposition testimony and a list of the cases in which they have provided courtroom testimony is important as it provides some insight about the experts' credentials and will withstand the scrutiny of an expert disclosure. In short, acquire a complete copy of the expert's curriculum vitae, including the citations for any articles they have written and a listing all memberships in computer forensic organizations such as:

- High Technology Crime Investigation Association (HTCIA);
- International Association of Computer Investigative Specialists (IACIS);
- American Society for Industrial Security (ASIS).

Most importantly, do not assume that any computer technician is a computer forensic expert. IT staff, computer consultants, software developers, and network administrators are not computer forensic experts and should not be relied upon to issue expert opinions in court. Several cases have been won or lost because one of the attorneys in the litigation failed to hire a qualified and experienced computer forensic expert. Instead, they hired someone who seemed to know something about computers, and when the individual was deposed or placed on the stand, he/she was unable to give solid opinions about the who, what, when, where, and why of certain computer activity.

It should be noted that the American Society of Crime Laboratory Directors Laboratory Accreditation Board (ASCLD-LAB) has set standards for computer forensic laboratories and examinations. While a number of government laboratories have achieved ASCLD-LAB accreditation in computer forensics, most have not, and private sector labs are not required to be accredited. However, even where a lab does not seek accreditation—a complex and expensive process—these standards may be the basis for cross examination, and an expert who is not familiar with the standard, or how their work meets (or does not meet) the standard can be perceived as unprepared or even unqualified.

5.5 When to Hire a Computer Forensics Expert

Companies needing to conduct computer forensic analysis must find an appropriate balance between handling a matter internally and consulting an outside expert. Factors to consider include some of the following.

- **Best Practices Imaging Technology and Experience**. Computer forensic investigators need to create mirror images of target hard drives involved in an investigation or litigation. At a minimum, this requires imaging hardware or software and knowledge of its use. Both the client and its counsel can be at risk for sanctions if best practices imaging protocols are not followed. The ability to properly image the media at issue is a factor to consider when weighing whether the investigation can

proceed in-house or in-firm. The issue of actual or perceived independence should also be considered. Will an employee acting at the direction of his or her employer be perceived as performing forensic tasks in an independent and neutral manner?

- **Ability to Track Chain of Custody**. Computer forensic investigators must be able to track chain of custody on all investigated media. As discussed previously, tracking a complete chain of custody is crucial in computer forensic matters. If the investigation is conducted internally, the company or law firm should be able to definitively track the media's movement and storage as well as every individual that had access to the media.
- **Data Recovery Experience**. In addition to computer forensic imaging software and general computer forensic analysis experience, most computer forensic investigators can recover inaccessible data from damaged media or systems. This is another factor to consider when establishing whether an investigation should be outsourced to a computer forensic expert.
- **Exposure to Hostile Information**. In some cases, computer forensic investigators are exposed to hostile content, such as pornography, contained on the computer being investigated. If the investigation is being conducted in-house or in-firm, employees should be warned of this risk and how to appropriately handle the situation. Computer forensic investigators have experience handling this type of information and know how to avoid certain hostile files if irrelevant to the project. The potential for exposing in-house or in-firm employees to hostile information should be considered when determining whether to conduct a computer forensics investigation in house. It should be noted that computer forensic investigators understand that certain content (for example child pornography) is legally considered to be contraband, and outside of law enforcement may not be retained. Reputable computer forensic experts have procedures for reporting such content to law enforcement. If a corporate investigator is ordered to destroy such evidence it may represent spoliation of evidence where, for example, an investigation of sexual abuse is under way.
- **Possibility of Testifying in Court**. When an investigation is conducted internally, the employee conducting the investigation puts him or herself at risk for being called as a witness if the matter proceeds to trial. If this is the situation, the employee will likely be scrupulously questioned on his or her relevant experience and procedures used in the investigation. The potential

for bias will also likely be strongly questioned. Most external computer forensic investigators have testimony experience. Companies facing a computer forensic investigation should consider this factor most heavily when determining whether to consult an expert.

It has been our experience that given these considerations in the computer forensics arena corporate counsel are quicke to consult an external expert for a computer forensic investigation rather than utilizing in-house resources. Perhaps this is due to the sensitive nature of most of these investigations and the specified knowledge needed to bring deleted or damaged data back from the dead, or to build a timeline of behind-the-scenes computer activities.

Some large corporations with a high risk of intellectual property loss through cyber-sabotage have chosen to hire full time computer forensic investigators and bring them internal to the organization. These investigators are often aligned with the security department and are focused on preserving and analyzing hard drives of departed or current staff members and may also have active computer monitoring responsibilities. These staff members are also usually charged with the responsibility of developing protocols to protect the company's information systems, preventing loss of digital information and investigating incidents when they arise.

However an organization chooses go about it, the need for a computer forensic expert will likely arise at some point in every business's history—whether that business has five, five thousand, or fifty-thousand employees. Having a plan in place to bring in expertise—whether internal or external to the company—will ensure that the incident is handled in the best possible manner.

5.6 Defining Computer Forensics Terminology

Many industry specific terms are used within the computer forensic science. Understanding the technology lingo is half the battle in demystifying computer forensics.

Active Data—This term describes the data that is accessible to a typical user from a hard drive, backup tape, or other like media. This is the data that was accessible to the particular user working with the computer, as distinguished from recovered (deleted), unallocated, and "slack" data.

Byte—Eight bits. The byte is the basis for measurement of most computer data as multiples of the byte value. A "megabyte" is one

million bytes or eight million bits, whereas a "gigabyte" is one billion bytes or eight billion bits.

1 gigabyte = 1,024 megabytes
1 terabyte = 1,024 gigabytes

Encryption—A procedure that renders the contents of a message or file unintelligible to anyone not authorized to read it.

Fragmented data—Live data that has been broken up and stored in various locations on a single hard drive or disk.

Inactive record—Records related to closed, completed, or concluded activities, which are no longer routinely referenced, but must be retained in order to fulfill reporting requirements or for purposes of audit or analysis. Inactive records generally reside in a long-term storage format remaining accessible for purposes of business processing only with restrictions on alteration, but may be reactivated in some business circumstances.

Legacy data—Information in the development of which an organization may have invested significant resources and that has retained its importance, but which has been created or stored by the use of software and/or hardware that has been rendered outmoded or obsolete.

Metadata—Metadata is best described as data about data—the who, what, where, why, and how about a file. Most file systems, software programs, and operating systems create and store metadata, such as the last modified dates, creation dates, last access dates, size, etc., for each file. However, each program or system stores different metadata fields differently. External metadata is unique to the media that the file resides on. File system metadata falls into this category and includes fields such as the file's creation date. Internal metadata is actually a part of the file. A Microsoft word document file for example, falls into this category and includes fields such as the "Last Print Time." So the exact same Word file on your computer will have different file system metadata than the same file on another computer.

Mirror image—Bit-by-bit copy of a computer hard drive that ensures the operating system is not altered during the forensic examination, and may be used in computer forensic investigations and some electronic discovery investigations. This may also be referred to as "disc mirroring" or as a "forensic copy."

Operating system (OS)—The software that the rest of the software depends on to make the computer functional. On most PCs this is Windows or the Macintosh OS. Unix and Linux are other operating systems often found in scientific and technical environments.

RAM (Random Access Memory)—The working memory of the computer into which application programs can be loaded and executed.

Figure 5.6 System Metadata

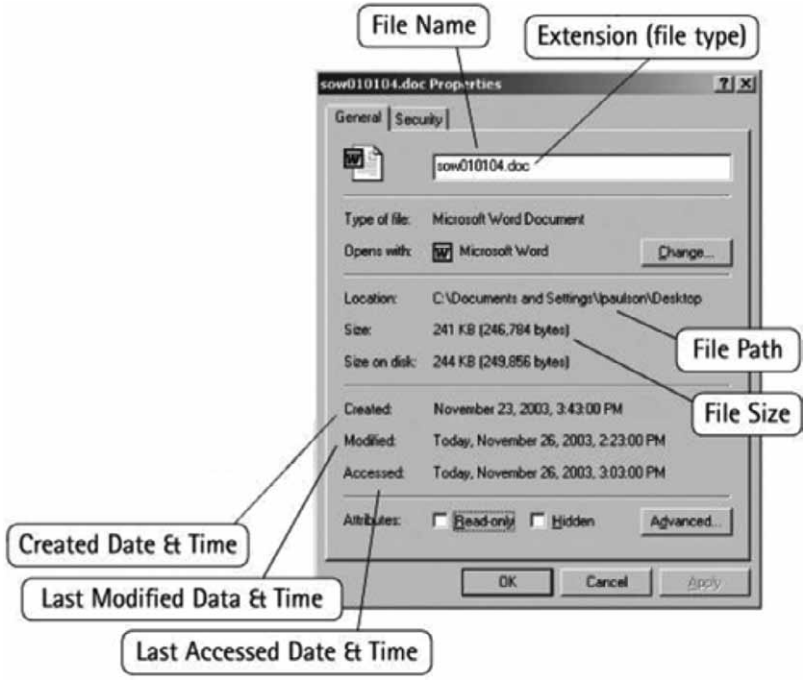
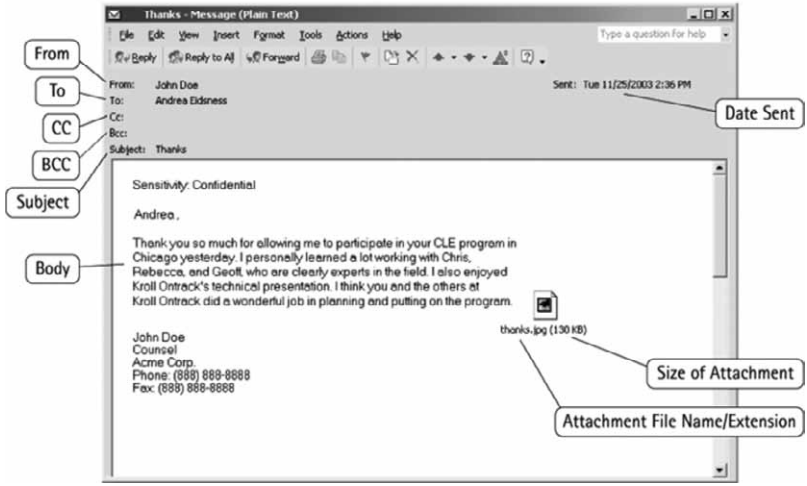


Figure 5.7 Application Metadata

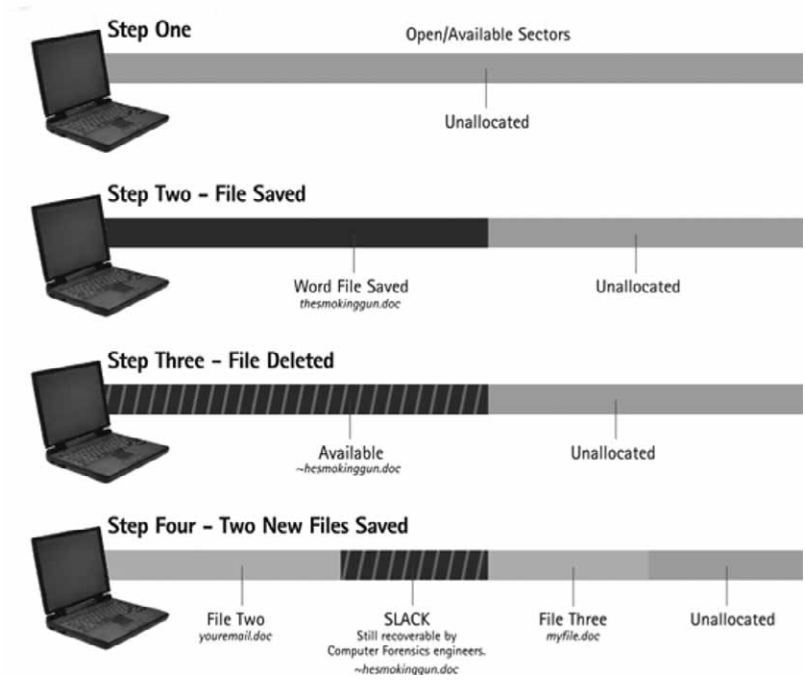


Recovered (Deleted) Data—This term refers to files and directories that were recovered after being deleted from the active data. As stated above, when a file is deleted it is merely marked as available for overwriting. If new data has not overwritten the area occupied by the previously deleted data, the deleted data can be recovered by computer forensic investigators. Due to the way computers store data, some of the files may be recovered completely and are easily identifiable, while some other data is partial and may be just fragments of the original data.

Residual data—Refers to data that is not active on a computer system. Residual data includes (1) data found on media free space, (2) data found in file slack space, and (3) data within files that has functionally been deleted, in that it is not visible using the application with which the file was created, without use of undelete or special data recovery techniques.

Slack Data—When saving a file to a drive, the computer's operating system must assign specific space on the storage device for the file. This space is allocated in fixed-size units called "clusters" or "file allocation units." Occasionally a file is exactly the size of a cluster and fills

Figure 5.8 Delete Does Not Mean Delete



it perfectly. But more often, the file is either larger or smaller than the size of a cluster. If it is larger, the operating system must assign another cluster. If the data to be written to the drive is smaller than a cluster, it is written and a special character, called an "end of file marker" is written to the drive to tell the operating system that it has reached the end of the file. Slack space is the space between the end of the file and the end of the cluster. Sometimes, when a file is marked as available for deletion and a new file is overwritten to that cluster, that new file does not overwrite all of the old file. Thus, bits and pieces of the old file reside in this "slack space" in the clusters of the drive. Computer forensic engineers search this space for remnant data when conducting computer forensic investigations. *Note: This is a simplified definition of slack data. There are additional concepts like "RAM slack" that will not be explored here.*

Unallocated Space—On a hard drive, the total storage space is divided into units called "clusters." These clusters of storage are assigned by the operating system to files as needed. A cluster that is not currently assigned to a file is said to be "unallocated." It may have been previously assigned to a file, but when the file is erased the clusters that were assigned to it are marked as being unallocated and thus available for re-use. However, when they are marked as being available, their contents are not changed, so whatever data was there when it was erased will still be there until the cluster is reused and the data is physically overwritten with new data.

5.7 Beyond Computer Forensics: Investigations and Security

Fraud, financial irregularities, and employee and commercial disputes are some of the most complex and challenging issues facing the modern business. These issues can result in severe financial damage, in addition to tarnished reputations. Investigating these issues is an important component within the realm of computer forensics. Typically, a computer forensics investigation is part of a much larger intelligence gathering exercise or e-discovery project. Below are a few common scenarios where an investigation is one part of a much larger situation.

FORENSIC ACCOUNTING

Investigations in the forensic accounting context can help unravel the true financial state of the business, as well as identify how an organization's accounting systems may have been manipulated to

cover up any wrongdoing. Forensic accountants examine and analyze relevant business records, reconstruct books, and interview involved parties. In doing so, facts are uncovered that can determine whether financial wrongdoing occurred, how long it has been in progress, how it was concealed, and the value of the impact.

An example of this practice occurred when outside counsel of a public company engaged in a team of forensic accountants to perform an independent investigation for the audit committee after a whistleblower accused certain management personnel of "inappropriately using company funds." The team first developed a work plan for evaluating the whistleblower's claims, working closely with outside counsel and a computer forensic expert. Indeed, one characteristic of the entire operation was cooperation and regular information sharing between the investigators, counsel, and the company's external auditors.

HOSTILE TAKEOVERS/PROXY CONTESTS

Another context in which an investigation may be conducted is in hostile takeovers and proxy contests. In high-profile takeover bids, information makes the difference between winning and losing. The investigator will work to gather intelligence about the opposition's strategies, intentions, vulnerabilities, and tactics. By gathering this information, you can support a bid or defense using developed facts and evidence that can be used in negotiations and litigation.

An example of this investigation context occurred when outside counsel for the board of directors of a high technology firm retained investigators in an effort to prevent the founder and two others from securing seats on the company's board of directors. The investigators' efforts were focused on identifying misleading and inaccurate statements in the trio's proxy submission. A thorough review of public filings, litigation, and media reports identified discrepancies and embellishments in the board candidates' resumes, biographies, and proxy filings. In addition, through interviews of well-positioned sources, undisclosed attempts were surfaced by the investigators that would have created conflicts for two of the candidates, should they have been elected to the board. Again, a computer forensic investigator was involved to help recover digital clues contained on hard drives involved in the matter.

INFORMATION SECURITY

Computer forensic investigators are also useful in situations where information security has been compromised. Because of the low

frequency of information security incidents, many organizations are ill-equipped and lack a practiced incident response team or protocol. Information security incidents can result in grave consequences for an organization, often resulting in extensive losses and damages. Even one breach of security can lead to catastrophic results, stressing the need to be prepared. Improper handling of these incidents can lead to high, and often unnecessary, costs to the organization.

To avoid these costs, an organization should look towards utilizing the services of an expert fraud investigator. This expert can help collect and analyze electronically stored information to show where, when, and how the incident occurred. Additionally, the expert can help interview key players and gather evidence to get to the bottom of what really happened. An expert can also implement steps to ensure evidence is properly preserved, aiding in avoiding potential negative results for the organization (such as sanctions) down the road. Finally, an expert can help implement programs aimed at preventing future security breaches. If security risks are left uncorrected, future breaches are almost inevitable leading to a loss of an organization's valuable resources, such as time and money.

The bottom line is that there may be a single computer hard drive involved in an investigation of corporate fraud, or there may be a dozen hard drives needing deleted data recovery in a discovery exercise involving hundreds of drives and tapes. Either way, it is critical that your forensics investigator and other consultants involved in the case are working together toward the end goal—helping your client or corporation navigate through the incident.