Chapter 1

Knowing What Your Digital Devices Create, Capture, and Pack Away — Until Revelation Day

In This Chapter

- Finding electronic evidence in the digital trails of our lives
- Whipping your evidence into shape
- Looking for evidence in the visible and invisible computer domain
- Looking at the life cycle of a case
- Defending your results

Think of computers, cell phones, PDAs, iPods, and other handheld devices as items with durable digital brains. Imagine that a detailed copy of every e-mail, text message, document, Internet upload or download, Google search, Facebook personal chat and posting, iPhone webChatter conversation, photo, financial transaction, and address book gets packed into electronic closets.

The amount of information left in each of these places is the basic reason that criminals are caught and found guilty and lawsuits are won or lost. When you use computer forensics tools to pick these digital brains or find skeletons in electronic closets, your case takes shape with e-evidence that's tough to refute. *Electronic evidence* (*e-evidence,* for short) can play a starring role in the civil, criminal, matrimonial, or workplace cases you investigate. It's as though people who use digital devices and social networks missed every *CSI* episode where incriminating e-mail, cell calls, and online activity became courtroom exhibits.

In this chapter, you become familiar with the locations and staying power of the all-too-accurate electronic records of actions, decisions, and indiscretions. You want to be smarter — or at least up to speed — with your opposition. For first responders to a crime scene and people planning litigation strategy, you learn how to answer your new call of duty. Methods used to hunt through hard

drives and perform digital autopsies must be generally accepted by the legal system so that your results hold up. You need to be familiar, therefore, with rules of evidence, some legal-speak, and the concept of loopholes. And, you need good report-writing skills to explain the results of your cybersleuthing in simplified detail. If the case goes to trial, so do you as an expert witness. Testifying in court is about as much fun as one person can stand.

Living and Working in a Recorded World

Ever since the World Wide Web (WWW — *the big one*) dropped into our lives in 1991, rabid growth has taken place in the personal, professional, and criminal use of computers, the Internet, e-mail, wireless tech toys, and social networks. These devices create and capture greater amounts of "digital details" that are stored in more places than most people realize. You have less chance of destroying detail-trails perfectly than of committing the perfect crime. Like the fingerprint left on the seat adjustment of a car used in a crime, a rogue digital fingerprint always lives on to tell the tale.

Once in electronic form, almost all data, documents, and other file types can be analyzed offline of the application that produced it. Computer forensics software makes this process possible by converting an entire hard drive into a single searchable file — called an *image* — that has no hiding places.

Deleting is a misnomer

A hard drive is a big place, and data or other digital content from prior years may be retrievable in pristine condition even if someone has deleted it. In this section, we discuss how a computer operating system (OS) helps a file — and your investigation — survive.

Imagine that you compose a Word document and save it on your laptop with the filename `Sand.doc`. The process of saving a file on your hard disk involves three basic events:

- An entry is made into the File Allocation Table (FAT) to indicate the space where `Sand.doc` is stored in the Data Region. Like all files, `Sand.doc` is assigned (allocated) space on the hard drive. Those spaces are *clusters.* The FAT file system is supported by virtually all existing operating systems for personal computers.
- A directory entry is made to indicate `Sand.doc` as the filename, its size, link to the FAT, and some other information.
- `Sand.doc` is written to the data region. That is, it's saved to a cluster on the hard drive. (Of course, files may occupy more than one cluster, but we're keeping it simple.)

But when you decide to delete `Sand.doc`, only two events happen:

- The FAT entry for the file is *zeroed out*. That's geek-speak for "the cluster that's storing `Sand.doc` is declared digitally vacant and available to store another file."
- The first character of the directory entry filename is changed to a special character so that the operating system knows to ignore it. In effect, it's only pretending that the file isn't there.

Like many deleted files, `Sand.doc` remains intact because nothing has been done to it. For `Sand.doc` to be totally overwritten and (almost) unrecoverable requires two events:

- The operating system must save another file (such as `Water.doc`) in the exact same cluster.
- `Water.doc` must be at least as large as `Sand.doc`.

A computer system never truly deletes files.

If, for example, `Sand.doc` filled an entire cluster and `Water.doc` file data took up less space, remnants of `Sand.doc` remain and are recoverable. The unused portion of the cluster is the *slack space*. More precisely, it's the portion of the cluster not used by the new file. Figure 1-1 shows how the Sand file wasn't dissolved (so to speak) by the Water file. Slack space cannot be seen without the specialized tools you find out about in Chapter 6.

Figure 1-1: Slack space holds the content of the former file.

When it comes to operating systems, remember these two concepts:

- You have no control over where the operating system saves files.
- The bigger the hard drive, the lower the probability that an existing deleted file will be overwritten.

Semisavvy criminals may try to outsmart the operating system by deleting the text, replacing it with non-incriminating content, and saving it with the same filename. But if they forget to account for the file size issue and compose a shorter file, remnants of the original file remain for recovery.

Online dragnet

If you're thinking that guilty parties would take action to avoid detection, follow any high-profile or murder case on CNN. Also consider the computer genius David L. Smith, who was charged with creating and unleashing the Melissa e-mail virus. Smith's claim to fame is that he was the first person prosecuted for spreading a computer virus. His Melissa creation inflicted more than $80 million in damages in 1999. He was sentenced to 20 months in the federal pen.

Smith either didn't know or didn't care that he could be identified by serial numbers in the software he created. Antivirus researchers, who tracked the activities of known virus writers, connected Smith to the online identity VicodinES. The digital fingerprints of Melissa's document serial number matched other documents on VicodinES's Web site. And, the timing of his postings gave away the region where he lived. Smith had posted the virus using a stolen America Online member's account. AOL keeps records of who calls in, and can track a person by using his Internet address.

Nothing that's digitally stored gets vaporized. Not being able to find a file that you saved just yesterday only means that you lost it. Losing a file is simply your computer's silicon sense of humor. The file is there.

Getting backed up

Workplaces have disaster-recovery and business-continuity systems that perform automatic backups. Companies are required to retain business records for audit or litigation purposes. Even if you never saved a particular file to the networked server, it might still be retained on multiple backup media somewhere. Instant, text, and voice messages exist in digital format and, therefore, are stored on the servers of your Internet service provider (ISP), cell provider, or phone company. Although text messages are more transient than e-mail, messages are stored and backed up the same way. Recipients have copies that may also be stored and backed up.

You can envision the explosion in the number of servers and hard drives that retain a copy of an e-mail message that has been CC'ed to a lot of people who then forward it on and on. Like a computer virus, e-mail evidence spreads far and wide. Your job is to find it.

E-mail is the richest source of evidence. E-mail is used as evidence of white-collar crime, fraud, trade theft, harassment, negligence, and infidelity. It is also used in violent crime cases.

Delusions of privacy danced in their headsets

You can find information relevant to almost any case on cell phones, iPods, personal digital assistants (PDAs), global positioning systems (GPS), transcripts of every word — or the letters used in place of words — in personal chats or any other forum that stores or transmit messages. Why? Because people have delusions of privacy when they're communicating with their buddies or partners in crime or friendship. E-mail and other messages share three characteristics that make them rich sources for revealing evidence. They are candid, casual, and careless.

When faced with other supporting evidence, jurors tend to believe that what is said on those devices is the honest truth.

In an IRS investigation into illegal tax shelters, eighteen accountants were indicted for tax fraud, among other charges. Exhibits that became the centerpiece of evidence in taxpayer lawsuits against their firm were e-mail messages. The case depended not on how flimsy the tax shelters were, but rather on a series of incriminating e-mails in which the accountants snickered about misleading the IRS. You can guess who got the last laugh.

Giving the Third Degree to Computers, Electronics, and the Internet

E-evidence is like a vampire lurking out of sight who can be neither destroyed nor intimidated. But this seemingly indestructible evidence can be tampered with, planted, or compromised accidentally. You don't want to be the one who accidentally compromises good evidence.

Before starting your investigation, here are a few general concepts to know:

- You must use specialized computer forensics software and toolkits according to generally accepted procedures. See Chapter 6.
- As with other types of evidence, you have to carefully handle the evidence so that it isn't compromised, and you have to keep the evidence under control at all times to be able to verify that no one has tampered with it. See Chapter 4.
- You don't get a do-over after you compromise e-evidence by mishandling it. See Chapter 5.

- Computer forensics isn't a magic or dark art. You can't make things appear that never existed. Your objective is to find what's there. See Chapter 7.

This last point is deceivingly important. Picture this: ACME Company is facing a wrongful-termination lawsuit for firing someone wrongfully. ACME management knows that they're guilty, so they need a defense (read: cover-up). An epiphany! They think, "Let's find something incriminating on his computer that we can use to whitewash our actions. To make it believable, we'll hire a computer forensics investigator and tell her we suspect that the former employee engaged in [fill-in any deviant behavior]." It's possible that the former employee had engaged in that activity, but the investigator would clearly and correctly date her activities in the report. The scheme could work. Ethical issues crop up all the time.

Be afraid — very afraid — of do-it-yourselfers. A do-it-yourselfer may try to recover lost files or find evidence of wrongdoing that he wants to use against his nemesis. A small-business owner can download a free trial version of RecoverThatFile or NoDeal, for example, and probe through the hard drive looking for proof that an employee copied and stole customer files. When that method fails, you might be called in. You cannot magically undo the damage done by the self-search so that it's usable in a legal action.

What lurks on the computer is not only content created or downloaded by the user. Computer software, like bookies who record and track gambling bets, is also making book (for example, creating logs, temporary files, and metadata) on what's going on. You need to investigate and analyze these details thoroughly for several reasons:

- To collect potentially valuable data that can support or refute other e-evidence
- To check for signs of tampering
- To avoid having to explain to the court why you didn't and then suffering the consequences

You're dealing with potential evidence. Your job is to do an intensive interrogation to learn the truth about what did or did not happen. But *Dirty Harry*-style investigative methods — however justifiable in your mind — will cause you much frustration later when the e-evidence is tossed out.

Answering the Big Questions

You need to understand the two dimensions of the digital underworld and what they hold as potential evidence. The contents of both the visible and invisible dimensions can be recovered with forensics tools. General examples of each type are shown in this list:

- **Visible**
  - Documents, spreadsheets, image files, e-mail messages
  - Files and folders
  - Programs and applications
  - Link files
  - Log files
- **Invisible**
  - Deleted documents, spreadsheets, image files, e-mail messages
  - Files and folders deliberately made invisible (hidden)
  - File system artifacts
  - Internet history
  - Print jobs
  - Random Access Memory (RAM)
  - Protected storage areas (where credit card numbers entered on Web browsers are held)
  - Storage areas outside the operating system's file system (areas that aren't readable by the operating system and that make good hiding places for files, even though computer forensics software can still find them)
  - System log files

Several of these items are created not by the user but, rather, because of what the user *does.* Visible contents can be created by either the user or the machine, and so can invisible contents. In Part III, you find out more about these sources of e-evidence.

Whereas only 1 percent of crimes involve DNA evidence, more than 50 percent of cases involve some sort of e-evidence.

What is my computer doing behind my back?

The short answer to what your computer does behind your back is "plenty." When files and messages are saved or sent, computer software (that no one ever sees) automatically generates artifacts, or *metadata*. Metadata exists in virtually every electronic document. It includes information about who created the document, the date it was created, when it was last modified, and more. Figure 1-2 shows the general metadata for a `.doc` file. Look at the

Attributes section, near the bottom of the figure. You see that the file itself isn't hidden. Even hidden files have metadata.

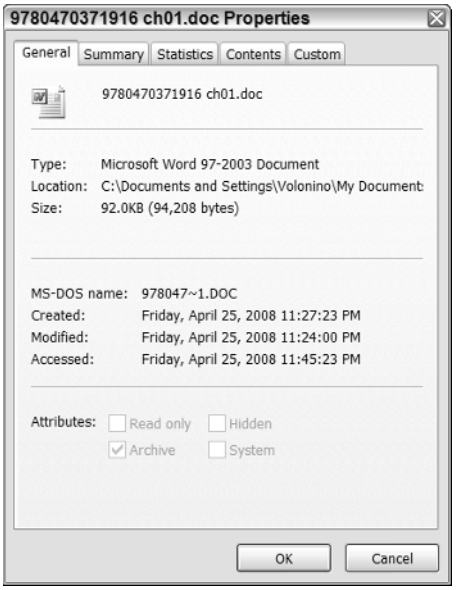

Figure 1-2: Metadata created automatically by Word software.

Unlike other forms of evidence, e-evidence tends to be more complete, can show intent or behavior patterns, and is harder to refute or deny. For example, metadata can be as revealing as a fingerprint or ballistic print. It can reveal the names of everyone who has worked on or viewed a specific document, text and comments that have been deleted, and different drafts of the document.

Can you hear me now?

Cell phones are another revealing source of data. Think about what you have stored and saved on your cell — and what you would feel if someone stole your phone. When you watch the TV show *Law and Order,* you hear a detective tell someone to "dump the phone." That person is referring to finding evidence — not to dumping Verizon for Vonage.

The 2004 Kobe Bryant case was the first high-profile U.S. criminal case involving cell phone text messages. A judge granted Bryant's attorneys access to cell phone text messages sent among three people — including the accuser — in the hours after the alleged attack. The judge ordered AT&T to produce the records of one of the accuser's friends to whom she sent text messages.

Digital communications seem anonymous, but quite the opposite is true.

Surfers Non-Anonymous

You can find out a lot about a person from the fertile trail left by her Internet activities. As e-evidence, social networks and blogs are almost too good to be true. Law enforcement can obtain text messages that were sent and received just about anywhere. People hurl information about themselves from Facebook and MySpace *and* chat about their illegal activities. A subpoena, rather than special forensics tools, might be needed to obtain this information. E-mail or chats from social networks, like other e-mail and chats, may be admissible as evidence.

Although some posting and content may not be admissible, you can use it to develop a profile of a suspect.

The unblinking eyes of search engines

In some circumstances, search engines such as Google and Yahoo! can identify the search terms used by a specific user. Internet searches have helped put many murderers in jail. The list that Google can produce shows IP addresses or cookies, not an actual list of people, unless they have provided their names when they registered. But IP addresses can be all that's needed to pick up the trail.

An IP address is like a cell phone number for your computer. Your computer, like your cell phone, is connected to a network. To communicate with the network (the Internet, for example) and devices on it (millions of computers attached to the Internet), your computer uses its unique IP address. An IP address can be private for use on a private network, or public for use on the Internet or other public network. Figure 1-3 shows the standard format of an IP address.

An IP address is made up of four bytes (think of them as four numbers) of information. Each of the four numbers in the IP address uses 8 bits of storage. Each of the four numbers, therefore, can represent any of the 256 numbers in the range between 0 (binary 00000000) and 255 (binary 11111111). A quick calculation in your head should tell you that more than 4 billion possible different IP addresses are possible — or more precisely, $256 \times 256 \times 256 \times 256 = 4{,}294{,}967{,}296$.

Find the IP address of your computer and read much more about IP addresses by visiting `http://whatismyipaddress.com`.

A *cookie* is a simple text file that can collect and store data about you on the hard drive of your own computer, such as which Web pages you've visited. Many sites use cookies as a way to track visitor information or to customize information for you.

In a long, complex case, investigators backtracked through an ISP to a hotel in the U.S. and from that were able to look at travel records and figure out which person was at the hotel at the time.

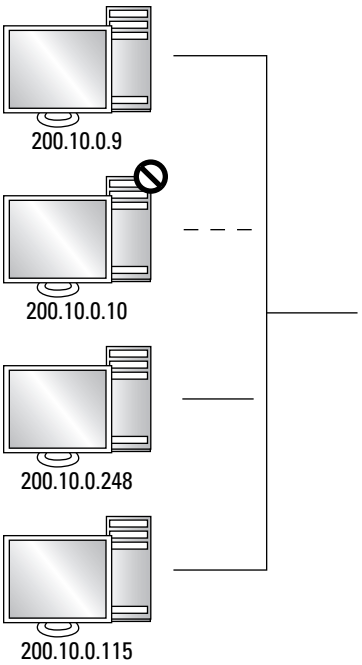

Figure 1-3: Format of an IP address used for computers to communicate over a network.

How does my data get out there?

Google, YouTube, Yahoo!, MySpace, and their competitors aren't humanitarian efforts. These profit-driven empires deal in digital currency — personal information. Their basic business model is simple: Collect it and sell it. The more they collect, the more they have to sell. Getting the picture?

People who register with almost every social network, sign up with frequent-buyer programs (Coke and Pepsi programs, for example), fill in profiles with AOL or Gmail, use chat and text messaging, play online games while sipping lattés at Internet cafés with unsecured hot spots — their data is out there. Gullible users reveal alarming amounts of information for a chance to win an i-anything.

Think about what you do that leaves a trace. You pay for every convenience with your privacy. For example, in an E-ZPass system, both car and driver are imaged with precise times, locations, and driving speeds.

Web servers contain *logs* (these are simply text files) that record visitors' activities. Server logs act like an automatic visitor sign-in sheet.

When you gain access to those logs, some of the information you can find out is

- **The Internet Protocol (IP) address of the visitor's computer:** Every computer attached to a network has a unique address, or Internet Protocol, so that the network can interact with it. An IP address is similar to a temporary phone number. A computer can be traced by its IP address. It's even possible to identify the person at the keyboard by his unique username.
- **The information in the cache:** Users may not think to clear the cache in their computers or digital devices. A cache is similar to a closet of a computer or handheld device that stores recent data. Web pages that a user visits are stored in the computer's cache. The purpose of the cache is to speed up the computer by holding on to visited Web pages to redisplay them without having to go back through the Internet to retrieve them. Even if a user wants to clear the cache, she might not know how. It's possible to find which pages were viewed, the date and time the visitor accessed each page, and images from the *referring URL* (the Web site the user came from).

Why can data be discovered and recovered easily?

Full-feature digital devices have brains and memories. Computers do too. Despite all their capabilities, computers are unable to *truly* delete a file so that that it no longer exists. Military-strength software to eradicate digital content can be applied to a hard drive, but it can't eradicate the files that were backed up or sent out to another computer.

Many computer forensics hardware and software tools have the power to acquire the contents of a hard drive or SIM card of a cell phone. Encrypted or password-protected files do not stop the tools from accomplishing their mission — at least not all of the time. Crime-supporting tools make it more difficult to recover e-evidence. But with the proper investigative tools and methods, that evidence may still be recoverable.

Aside from the technology factor, people don't expect to get caught. Consider sunbathers at the beach who rely on the fallible method of hiding keys by ingeniously stuffing them deep into the toe of a sneaker. And don't forget all those drivers caught speeding by radar. The human factor makes it easier for the technology to recover data.

Examining Investigative Methods

Your job as a computer forensics investigator involves a series of processes to find, analyze, and preserve the relevant digital files or data for use as e-evidence. You perform those functions as part of a case. Each computer forensic case has a life cycle that starts with getting permission to invade someone else's private property. You might enter into the case at a later stage in the life cycle. Taken to completion, the case ends in court where a correct verdict is made, unless something causes the case to terminate earlier.

Getting permission

Police can't arrest people without reading them their rights. And investigators can't just show up and check or confiscate a person's computer without a search warrant — usually.

When law enforcement needs to gather evidence in a criminal case, it tends to be immediate. Generally, the FBI has the power to seize information and bank accounts, issue subpoenas or search warrants, or even break down doors in exigent circumstances.

Civil cases do not include that type of authority. In civil cases, parties need to show proof that they're entitled to evidence. Meanwhile, relevant evidence can be destroyed, lost, or deleted.

Don't touch anything until you see or receive confirmation to proceed. See Chapter 3 for more on this issue.

Choosing your forensic tools

Evidence verification depends on the use of the proper software and hardware tools, equipment, and environment. A Swiss army knife for forensics hasn't been invented. No single methodology or set of tools or crystal ball exists for conducting a computer forensics investigation. Some of the many factors affecting the choice of tools are

- Type of device
- Operating system
- Software applications
- Hardware platforms

- State of the data
- Domestic and international laws that apply

Knowing what to look for and where

This area is where the deductive art of computer forensics comes into play. The importance of this thinking stage cannot be overstated. You have to think about both sides of the situation. That is, your objective is to look for the truth about what did or did not happen. But you're restricted because you don't have unlimited time or money. Strategies for focusing and refining your search are covered in Chapter 7.

In the days of paper-only discovery, lawyers asked for and received truckloads of paper documents, sometimes brought in from distant warehouses. Their strategy involved finding the "smoking gun" document that would win the case and a huge jury verdict. Trial strategies didn't change — the nature of documents did. E-evidence for a case might fill supertankers if it were in hard copy.

Gathering evidence properly

Your goal is to have e-evidence that is admissible in court. Consider evidence as the football, and court as the goal line. Keep your eye on the evidence. Preserving e-evidence and maintaining good documentation of the steps taken during the evidence processing are essential for success.

People may lie, but the e-evidence rarely does. Prepare your e-evidence with care so that it's allowed to tell the truth.

Revealing Investigation Results

Every investigative step, from acquisition to examination of the e-evidence, may someday need to be explained in court on direct examination — and then defended on cross-examination (or *cross*). During cross, the less-than-friendly opposing lawyer tries to impeach or discredit your testimony. Mistakes create loopholes that can devastate a case.

Preparing bulletproof findings

Working in the legal system carries a huge responsibility for you to perform your work with diligence, competence, honesty, and good judgment. Those qualities are your best defense in preparing your findings.

You need to admit to any possible problems and explain why they didn't compromise the evidence. Above all, always tell the truth.

Making it through trial

Most cases don't involve eyewitnesses. Even you can't see what happened without a lot of equipment. Without the benefit of direct testimony by an eyewitness, juries and judges rely on you to "connect the dots" of the circumstantial evidence. (This topic alone warrants an entire *For Dummies* book.)

Your ability to successfully make it through trial depends on your degree of preparation — and eating a good breakfast. Fortunately, the common challenges of giving testimony in open court and the stages of a trial are covered in Part IV.