CHAPTER

Collecting evidence

4

"Never neglect the details ..."
—Colin Powell

INFORMATION IN THIS CHAPTER:

- Introduction to Crime Scenes
- Documenting the Scene and the Evidence
- Establishing and Maintaining the Chain of Custody
- Forensic Cloning of Evidence
- Dealing with Live Systems and Dead Systems
- Using Hashing to Verify the Integrity of Evidence
- Drafting the Examiner's Final Report

INTRODUCTION

That "smoking gun" you discovered will never get to a jury unless it's been properly collected and accounted for, starting at the scene. As important as that proper procedure is, you'll never see it done right on TV cop shows. Nothing kills the excitement faster than three solid hours of paperwork. In the real world, it's those three solid hours of paperwork that get your evidence into court. It all starts at the crime scene. Just locating the evidence can be tough, especially with stamp-sized (or smaller) memory cards and the like. Such items could be hidden in an almost limitless number of places.

At the scene, examiners could be confronted with a variety of devices and storage media. They could find one or more running computers and wireless devices like cell phones. Together, these present some unique challenges for the investigator.

Actions during the collection process must be well documented. Notes, photos, video, and sketches record our actions and refresh our recollections. As digital evidence is extremely volatile, preservation is paramount. If at all possible, a forensic image or clone is made of the suspect media. The exam is conducted on the clone (which is an exact, bit-for bit-copy) rather than the original.

CRIME SCENES AND COLLECTING EVIDENCE

From a practical standpoint, not all scenes involving digital evidence are created or treated equally. Digital evidence has been the focus of criminal, civil, and administrative proceedings. There are distinct differences in how the scene and the evidence may be handled and documented for these proceedings. Some cases, like a homicide, will require painstaking documentation. Others, like a civil dispute, will necessitate a somewhat less-intense response. While acknowledging these subtle differences, certain core principles and protocols remain consistent.

After it's deemed safe, job one at a digital crime scene, or any other, is securing the evidence. The scene and its evidence must be protected from accidental or intentional compromise. Securing a traditional crime scene entails limiting physical access by those folks who don't have a legitimate reason to be there. Nosy neighbors, the news media, and police supervisors are typical crime scene trespassers. Securing a traditional scene is accomplished by stringing crime scene tape, posting guards, or simply asking people to leave.

In contrast, a scene with digital evidence presents an entirely new dimension of access. Most computers and digital devices are connected to the Internet, cellular systems, or other kinds of networks. These connections are what permit remote access and put the evidence at risk. Computers and wireless devices must be made inaccessible as soon as you're sure that no volatile data would be lost (Association of Chief Police Officers, 2011). For computers, it may be a matter of removing the ethernet cable or unplugging a wireless modem or router. With wireless devices such as cell phones, we must take steps to isolate the phone from network signals.

REMOVABLE MEDIA

If legally permissible (such as with a warrant), we want to search anywhere that could contain a piece of storage media. Considering today's stamp-sized memory cards, such pieces of evidence could be hidden almost anywhere, such as in books, wallets, hat bands, etc.

Despite their small size, memory cards can hold a ton of potential evidence, such as child pornography or stolen credit card numbers. Let's break it down. A quick check of Amazon.com shows that you can buy a 64 gigabyte memory card for around $120. Gigabytes (GB) are pretty abstract for most of us. Instead of using a standard unit of data storage, we'll use an example that is less conventional yet more relatable.

We're going to convert the 64 GB memory card into our own unit of measure, which we will call "Potters"—Harry or "Potters." Picture a set of all seven books in the Harry Potter series. In rough numbers, each GB contains about 109 complete sets. With some simple math, we find that our 64 GB memory card can hold approximately 7,000 complete sets of books—Potters—on something about the size of

a postage stamp(Think about the amount of evidence that could be pulled from just one memory card.

Removable storage media

Removable storage media include things like DVDs, external hard drives, thumb drives, and memory cards.

We're not just interested in the devices and storage media at the scene; the surrounding area and items are also worth a look. For example, books and manuals can give investigators clues as to the skill level of the target and what kind of technology they may be up against. Perhaps the biggest payoff is an alert to the possible use of encryption. Discarded packaging in the trash could also be helpful. Any forensic examiner would tell you that avoiding encryption is definitely worth the trouble.

CELL PHONES

Almost everyone has a cell phone these days. These often contain some very valuable evidence. Text messages, e-mail, call logs, and contacts are examples of what you can recover. These items can be used to show intent, determine the last person to come in contact with a murder victim, establish alibis, determine approximate locations, and more.

As with other electronic devices, our first mandate is to make no changes to the device or its storage media. Therefore, interacting with the phone should be avoided unless absolutely necessary. Cell phones are particularly vulnerable because they can be wiped by the cell provider or even by the owners themselves. This functionality is intended to protect your data should you lose your phone or have it stolen. Apple's "Find My Phone" app is one notable example. We must address this concern by isolating or shielding the phone as soon as possible.

You have a few options to get this done:

- Turn the phone off. The concern with this approach is the same as with a PC. The phone may be password-protected. Once powered down, the code may be necessary to access the phone. If possible, it may be best to isolate the phone in a Faraday bag or arson can and leave it powered on. It can then be transported to the lab to be examined in a shielded room and otherwise treated as evidence. A Faraday bag is made of "some type of conducting material or mesh" that repels these signals. The function of the bag is based on the work of Michael Faraday, an English scientist who specialized in electromagnetism (Microsoft).
- Place the phone in a special container that shields the phone from wireless signals. Empty paint cans and Faraday bags are two of the more typical choices. Both of these items are effective at safeguarding the phone from cell signals. (See Figure 4.1.)

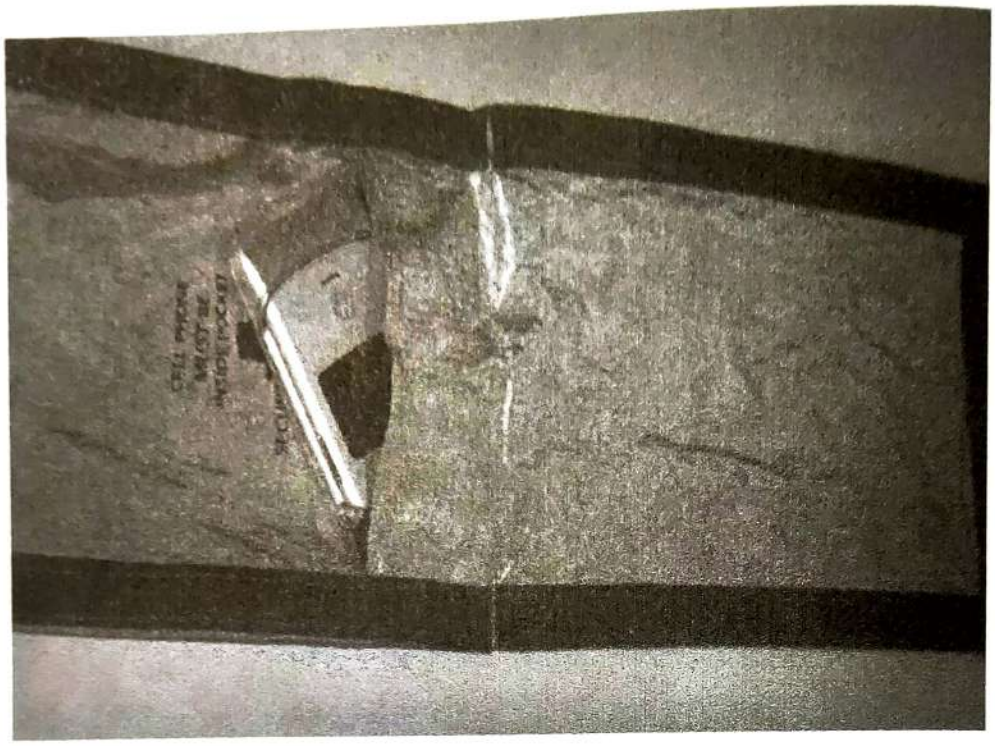

FIGURE 4.1

A Faraday bag and cell phone.

ALERT!

PROTECTING CELL PHONES FROM NETWORK SIGNALS

It's essential to isolate a live cell phone from the network. If not, it can receive calls, text messages, or even commands to delete all the data. A Faraday bag is one way to prevent a network signal from reaching the phone.

ALERT!

POWER

Power is a concern whenever you seize a cell phone. If the phone is on, it will continuously try to connect to a tower, draining the battery. If the phone is off, you should also seize the power cables. Lab personnel may very well need to recharge the device to complete their exam.

Failing to remove connectivity to these devices not only risks destruction of the evidence; it can raise serious concerns about its integrity as well. A competent attorney could successfully argue that this evidence is untrustworthy and should be excluded.

After securing the evidence, a survey of the scene will give investigators an accurate sense of what's ahead. Several questions have to be answered:

- What kinds of devices are present?
- How many devices are we dealing with?
- Are any of the devices running?
- What tools will be needed?
- Do we have the necessary expertise on hand?

Once these questions are answered, the real work begins.

ORDER OF VOLATILITY

It's a good idea to prioritize the evidence to be collected. Generally, we want to start with the most volatile evidence first. In computer parlance, this is known as the order of volatility. This descending list works from the most volatile (RAM) to the least volatile (archived data). The order of volatility is:

1. CPU, cache, and register content
2. Routing table, ARP cache, process table, kernel statistics
3. Memory
4. Temporary file system/swap space
5. Data on hard disk
6. Remotely logged data
7. Data contained on archival media
   (Henry, 2009)

DOCUMENTING THE SCENE

There is an old, tried-and-true saying in law enforcement: "If you don't write it down, it didn't happen." These are words of wisdom indeed. Regardless of the situation, any time evidence is collected, documentation is a vitally important part of the process. There are several different types of documentation. The most common in terms of digital forensics are photographs and written notes; video is also an option for documenting evidence.

This documentation process begins the moment investigators arrive at the scene. Typically, we start by noting the date and time of our arrival, along with identifying all the people at the scene. The remainder of our notes consists of detailed descriptions of the evidence we collect, its location, the names of who discovered and collected it, and how it was collected. It's also a good idea to note the condition of each item, especially if there is visible damage.

Accurately and precisely describing the evidence is of critical importance. A piece of digital evidence is described by type, make, model, serial number, or other similar descriptors. It's also important to note whether a device is on or off or if it's connected to other devices (such as printers) or a network (like the Internet). Virtually everything we see, find, and do should be documented.

While we're talking about peripheral connections, it is good practice to label each so the entire system can be reconstructed in the lab, should that become necessary.

After the scene and evidence are secure, our attention can turn to the documentation as well as identifying and collecting potential sources of evidence. Before anything else is done, it's prudent to do a walk-through to survey the scene, pinpointing the type and number of devices as well as resources that will be needed.

PHOTOGRAPHY

Next, the entire scene should be photographed. Photos should be taken of the scene before anything is disturbed, including the evidence. It's helpful to think of the photos as telling a story. Remember, at some point, you may have to walk a judge or jury through this scene weeks, months, or even years later.

Start with a broad perspective, perhaps the outside of the house or office being investigated. After the overall scene has been photographed, we can then focus on each individual piece of evidence. Long-, medium-, and close-range photos show the item in the context of its surroundings. The photos of each item should clearly show the condition of the item as it was found. We need to pay particular attention to and capture details such as identifying information like serial numbers, damage, and connections. Connection examples could include networks and peripherals such as printers and scanners. It's very important to keep in mind that this is likely to be the only chance we'll get to capture the scene so, when in doubt, shoot more, not less.

You've probably seen photos with both the evidence item and a ruler of some sort. This is done to give some perspective to the item. Comparing the item to a measurement unit of some sort gives us an idea as to the size of that particular piece of evidence. Remember, we want to record the scene before it's disturbed or altered in any way, so inserting anything into the scene with that item (like a ruler) can qualify as alteration. If it is necessary to show the size of the piece of evidence, it's a good idea to take a picture without the ruler first, then one with the ruler.

Photographs are used to depict the scene and the evidence exactly as we find them to help supplement our notes. Photos don't replace those notes. Notes capture our personal observations that won't be recorded in a photo. The notes are used to refresh our recollections when we go to court. Photos are a great aid to help us tell our story to the judge and jury. They really are worth 1,000 words.

NOTES

As we photograph the evidence, we'll also be taking detailed notes of our actions, along with any potential evidence we find. There is no set standard for note-taking. It's really up to the individual on how to document things. Chronological order is a common method. You would want to note things such as the time you arrived, who was present at the scene, who took what action, who found and collected which piece of evidence, and so on.

Never lose sight of the fact that you will be relying on these photos, notes, and reports months or years later when you prepare for court. With that in mind, you will

want more detail rather than less. Memories fade, cases run together, and details get blurry. The photos and notes should also be legible for the same reason. If cost is a concern, keep in mind that digital photos are cheap. You can fit a lot of photos on today's memory cards.

What you write in those notes matters to other people involved in the case, especially if they end up being turned over to the opposition. Under certain legal requirements, your notes could become discoverable and made available to the opposing side. This can happen if you take your notes with you to the witness stand. With that in mind, it's important not to draw conclusions or speculate based on your initial observations. You could very well end up eating those words and losing the case. It's best to keep those notes focused on what you do and observe at the scene. Saving the interpretations and conclusions until after the analysis is a much better approach.

CHAIN OF CUSTODY

Before a piece of evidence gets in front of a jury, it must first meet a series of strict legal requirements. One of those is a well-documented chain of custody. A computer taken in as evidence makes many stops on its road to trial. It's collected, logged in at the lab, stored, checked out for analysis, checked back in for storage, and so on. Each of these stops must be noted, tracking each and every time the evidence item changes hands or locations. Without this detailed accounting, the evidence will be deemed untrustworthy and inadmissible. It's this detailed trail that makes up the chain of custody (Figure 4.2).

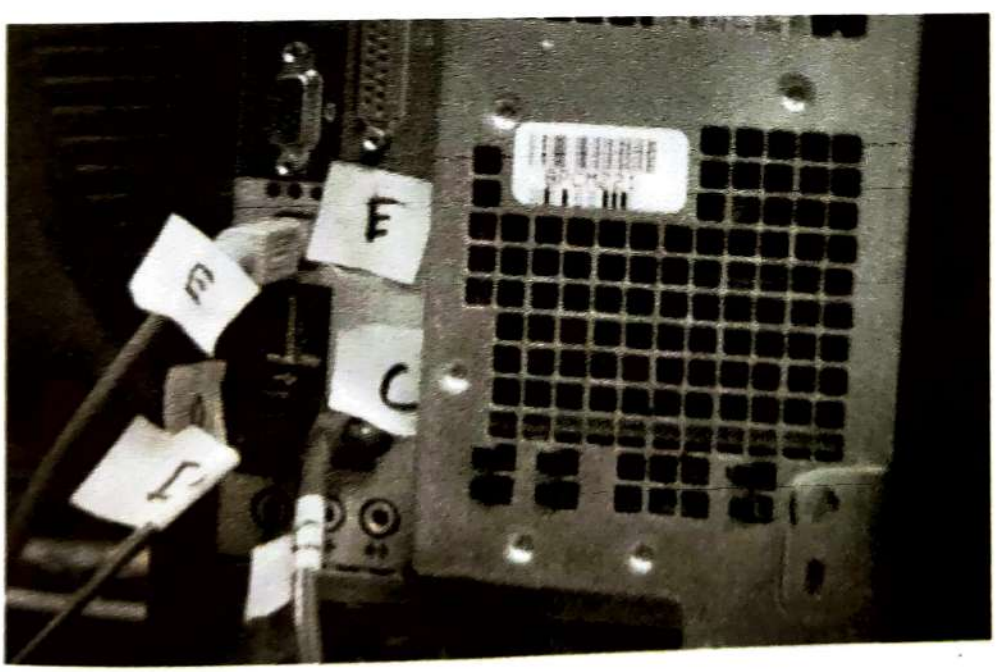

FIGURE 4.2

Marked cables from the back of a PC. Labels are placed on both ends of a cable to help document how what was connected to the PC at the time it was collected.

MARKING EVIDENCE

The first "link" in the chain of custody in any case is the person collecting the evidence. Civil cases may differ a bit in that IT staff or others may hold the distinction of being the first link. The evidence is marked as it is collected. Typically, evidence items are marked with initials, dates, and possibly case numbers. Permanent markers are the best tool for this to ensure the markings aren't smudged or removed altogether. Apart from documenting the chain of custody, these marks help authenticate the item should it be introduced in court. The person who collected the item may be asked to identify it from the witness stand. What needs to be proved is that the item presented is the same one that was collected. These marks make this identification a near sure thing. (See Figure 4.3.)

Items small enough are normally sealed in a bag with tamper-proof evidence tape. The seal is then initialed and dated. The bags are usually made of paper, plastic, or special anti-static material. The anti-static material bags are used for electronics because this material helps protect the sensitive electronics found on hard drives from being damaged by static electricity.

CLONING

A forensic clone is an exact, bit-for-bit copy of a hard drive. It's also known as a bitstream image. In other words, every bit (1 or 0) is duplicated on a separate, forensically clean piece of media, such as a hard drive. Why go to all that trouble? Why not just copy and paste the files? The reasons are significant. First, copying and pasting only gets the active data—that is, data that are accessible to the user. These are the files and folders that users interact with, such as a Microsoft Word document. Second, it does *not* get the data in the unallocated space, including deleted and partially overwritten files. Third, it doesn't capture the file system data. All of this would result in an ineffective and incomplete forensic exam.

We will want to make a forensic clone of the suspect's hard drive(s) as soon as we reasonably can. Cloning a drive can be a pretty time-consuming process and, for that reason, it usually makes more sense to do the cloning in the lab as opposed to at the scene. Cloning in the lab eliminates the need to be on scene for what could be hours. It also provides a much more stable environment, affording us better control of the process.

Before we take a computer off-premises, we must have the legal authority to do so. In a criminal case, this request and the rationale behind it should be part of the search warrant application. In civil cases, this provision can be negotiated by the parties or ordered by a judge.

Although taking the hardware back to the lab is routine in criminal cases, the cloning may have to be done at the scene in a civil case. Most civil cases with digital evidence focus on business computers. A business computer sitting in a lab isn't generating any revenue, which tends to get business folks understandably cranky. If the

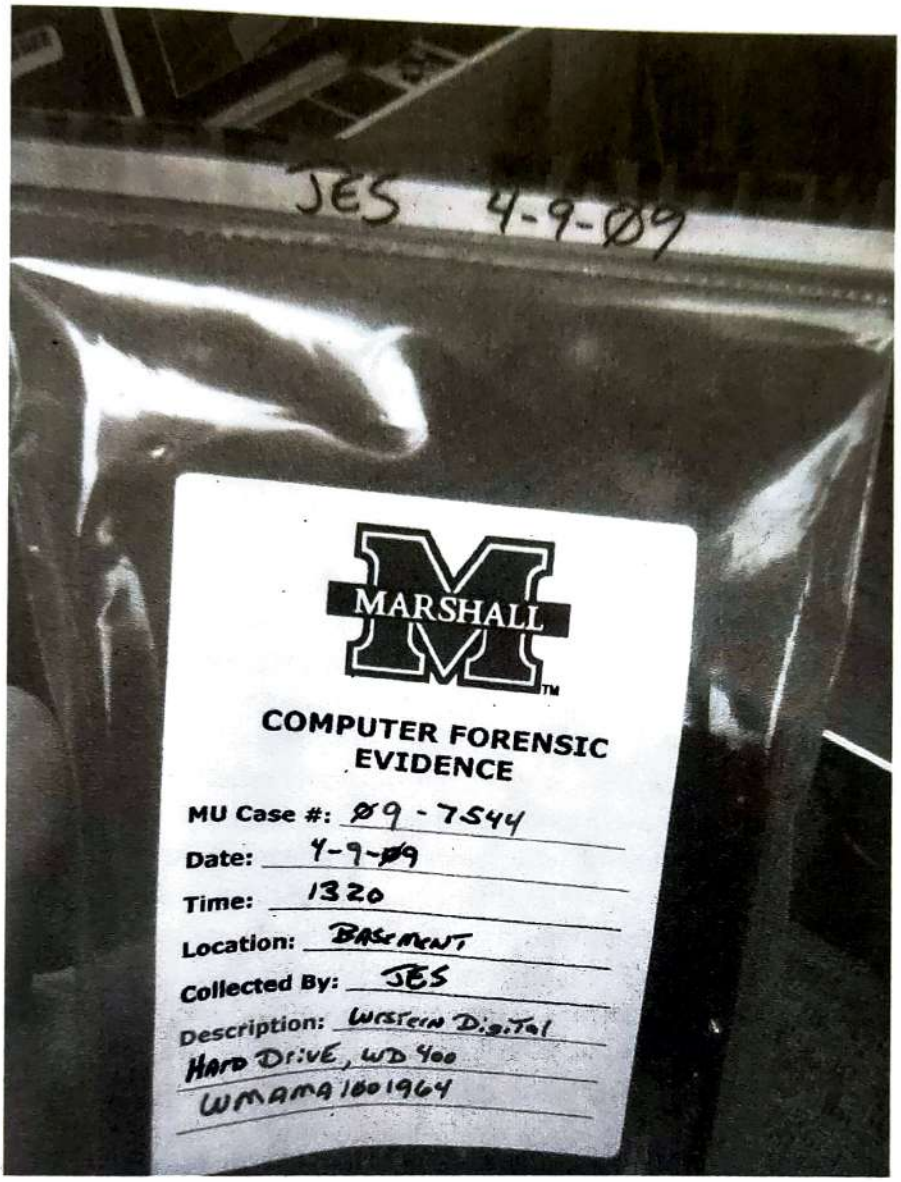

FIGURE 4.3

A marked piece of evidence, sealed in an evidence bag.

(Photo courtesy of Marshall University.)

hard drive in a business computer can't be replaced, then the machine is often cloned and put right back into service.

PURPOSE OF CLONING

We know from earlier chapters that digital evidence is extremely volatile. Thus, you never want to conduct your examination on the original evidence unless there are exigent circumstances or there is no other option available. Exigent circumstances could include situations in which a child is missing. Sometimes there are no tools or techniques available to solve the problem at hand.

Examining the clone affords us the chance at a "mulligan"—a do-over, as is said in golf—should something go wrong. If possible, the original drive should be preserved in a safe place and only brought out to reimage if needed.

Hard drives are susceptible to failure. Having two clones gives you one to examine and one to fall back on. Ideally, all examination is done on a clone as opposed to the original.

Sometimes that isn't an option, especially in a business setting when the machine and drive must be returned to service. In the eyes of the court, a properly authenticated forensic clone is as good as the original.

THE CLONING PROCESS

Cloning a hard drive should be a pretty straightforward process, at least in theory. Typically, you will clone one hard drive to another. The suspect's drive is known as the source drive and the drive you are cloning to is called the destination drive. The destination drive must be at least as large as (if not slightly larger than) our source drive. Although it is not always possible, knowing the size of the source in advance is pretty handy. Bringing the right size drive will save a lot of time and aggravation.

The drive we want to clone (the source) is normally removed from the computer. It's then connected via cable to a cloning device of some kind or to another computer. It's *critical* to have some type of write blocking in place before starting the process. A write block is a crucial piece of hardware or software that is used to safeguard the original evidence during the cloning process. The hardware write block is placed between the cloning device (PC, laptop, or standalone hardware) and the source. The write block prevents any data from being written to the original evidence drive. Using this kind of device eliminates the possibility of inadvertently compromising the evidence. Remember, the hardware write-blocking device goes in between the source drive and the cloning platform.

It takes little prep work to make a clone. The destination drive must be forensically cleaned before cloning a suspect's drive to it. Most, if not all, forensic imaging tools will generate some type of paper trail, proving that this cleaning has taken place. This paperwork becomes part of the case file.

Once the connections are made, the process starts with the press of a couple of buttons or clicks of a mouse. When complete, a short report should be generated by the tool, indicating whether the cloning was successful. Cloning is successful when the hash values (think "digital fingerprint") for the source and clone match. We'll dig deeper into hash values in just a bit.

FORENSICALLY CLEAN MEDIA

A forensically clean drive is one that can be proven to be devoid of any data at the time the clone is made. Being sterile is another way of looking at it. It is important to prove the drive is clean because comingled data is inadmissible data. Drives can be

cleaned with the same devices used to make the clones. The cleaning process overwrites the entire hard drive with a particular pattern of data such as 111111111111 (Casey, 2011).

FORENSIC IMAGE FORMATS

The end result of the cloning process is a forensic image of the source hard drive. Our finished clone can come in a few different formats. The file extension is the most visible indicator of the file format. Some of the most common forensic image formats include:

- EnCase (extension .E01)
- Raw dd (extension .001)
- AccessData Custom Content Image (extension .AD1)

There are differences in the formats, but they are all forensically sound. Some, like DD, are open source, while others, like AD1, are proprietary. Choosing one format over the other can simply be a matter of preference. Most forensic examination tools will read and write to multiple image formats.

In addition to being forensically sound, the other major consideration is that the tools to be used can read the image. The documentation with the tool should provide this information. Compatibility is a concern. This is especially true when exchanging image files between examiners.

RISKS AND CHALLENGES

The biggest risk during the cloning process is in writing to the source or evidence drive. Any writes to the evidence will compromise its integrity and jeopardize its admissibility. Getting a functioning write-blocking device or software in place will keep this from happening. Proper cloning should be pretty boring. Any time it gets exciting, you've got problems. What can ratchet up the adrenaline? Bad sectors and damaged or malfunctioning drives come to mind. A corrupt boot sector or a failing motor can also create complications.

VALUE IN eDISCOVERY

The Sedona Conference, the leading think tank on electronic discovery, defines eDiscovery as "[t]he process of identifying, preserving, collecting, preparing, reviewing, and producing electronically stored information 'ESI') in the context of the legal process" (Sedona Conference, 2010).

Forensic cloning provides some additional value in the eDiscovery process. Preservation of potentially relevant data is paramount in electronic discovery. Parties that fail to preserve evidence can face some very stiff punishment. Forensic cloning is one option available to preserve some kinds of media, such as hard drives, and removable media, such as flash drives. It serves as the gold standard of data preservation in that

There is a technique that can be used to preserve data in memory after the power is off, but it's not yet been widely adopted. (See the sidebar.)

MORE ADVANCED

PRESERVING EVIDENCE IN RAM

It's widely thought that data in RAM vanish when the power is turned off. That's not really true. Research by Princeton University has shown that data in RAM fade rather than disappear. This dissipation can be further slowed if the RAM is cooled to –58 degrees Fahrenheit (–50 Celsius). This cooling will give examiners more time to collect this volatile data. To see this technique in action, see the video here: https://citp.princeton.edu/research/memory/.

The second concern is encryption. The system or files may be unencrypted while the machine is powered on. Abruptly pulling the plug could return it to an encrypted state, potentially putting that evidence out of reach for good. Avoiding encryption is a good idea any time.

Third, a sudden loss of power could damage the data, rendering them unreadable. Fourth, some evidence may not get recorded on the drive unless and until the computer is properly shut down.

The old-school solution of pulling the plug is not the only option on the table these days. There are now tools and techniques that will capture volatile memory from a live machine in a forensically sound manner. With these advances, it's time to start recognizing the advantages of live collection.

ADVANTAGE OF LIVE COLLECTION

Until fairly recently, pulling the plug was the only real option. Capturing data in a running computer's main memory (RAM) wasn't a realistic option. The potential solutions that existed just weren't practical for use in the field. In contrast, present-day examiners do have some forensically sound alternatives. Several commercial and open source tools can be used to collect these volatile data. Unlike the older lab-bound approaches, these tools are very easy to use—so simple, in fact, that they are being marketed to nontechnical folks such as first responders. First responders could include patrol officers and IT staff, among others. While these tools do simplify the process, people still have to be trained in their proper use.

PRINCIPLES OF LIVE COLLECTION

Doing a live collection is not a rudimentary task. The following is an example of one approach.

After coming across a running computer at the scene, a couple of questions will have to be answered right from the start. Is the potential evidence to be recovered truly worth the time and effort? In some instances, the answer may be

it preserves all of the data on a piece of media, not just the active data. The down side of cloning is that it can be expensive and simply not practical in all situations.

ALERT!

SANCTIONS IN ELECTRONIC DISCOVERY

Take the case of *E.I. du Pont de Nemours v. Kolon Industries (2011).* In this case, the jury awarded $919 million to DuPont in an eye-popping verdict. Earlier in the case, the court determined that Kolon had destroyed e-mails and other potentially relevant data connecting it to the theft of trade secrets. As a result of that determination, the judge instructed the jury that Kolon (both its executives and employees) deleted important evidence even though the company had a duty to preserve it. Kolon's suffering may not end there. DuPont plans on requesting $50 million in punitive damages plus $30 million more for attorney fees (Favro, 2011).

LIVE SYSTEM VERSUS DEAD SYSTEM

Up to now, we've been talking about "dead" or powered-off machines. What happens when we come across a running computer? At the moment, there is no consensus on the answer. A growing debate exists in the digital forensics community about how to handle a "live" or running machine. The "old school" solution is simply to pull the plug, instantly removing power to the computer. Today, that approach is generating second thoughts. There are compelling reasons not to pull the power on a running computer. Next, we'll look at the reasons both for and against this somewhat controversial method.

LIVE ACQUISITION CONCERNS

On the plus side, pulling the plug eliminates the need to interact with the running machine. Interacting with a running computer, in any way, causes changes to the system. Any change to a piece of evidence is bad and can cause major problems from a legal standpoint. These alterations can call the integrity of the evidence into question. Even when a machine is just sitting there and powered on, things are changing. When a person interacts with a running machine, even more things are changing. Knowing about that change is a forensic faux pas; it's easy to see why pulling the plug is an attractive option. As a side note, these changes may have no impact on the artifacts relevant to the case. But the system is changing nonetheless.

We are now starting to second-guess this approach, recognizing that pulling the plug has some significant downsides.

For starters, yanking the plug means that any evidence in RAM will be under real threat of destruction. Data in RAM start to dissipate or fade when power is removed.

"no." In cases involving malware, RAM is vitally important. In others, such as a clear-cut possession of child pornography, RAM is likely to have little value. Second, are the necessary resources available? To successfully capture the evidence in memory will require some specialized tools and training in using them. Without these key ingredients, it could be best to punt and simply pull the plug. The risk of compromising the evidence may simply be too great. It's important to be able to recognize when you are in over your head and when you should call for help.

When interacting with a live machine, it's always best to choose the least invasive approach possible. This will require thinking before you click. Haste is not your friend in this situation. As mentioned earlier, we want to collect the most volatile information first.

ALERT!

EVIDENCE IN RAM

A computer's volatile memory (RAM) can contain some very valuable evidence, including running processes, executed console commands, passwords in clear text, unencrypted data, instant messages, Internet protocol addresses, and Trojan horse(s) (Shipley and Reeve, 2006).

CONDUCTING AND DOCUMENTING A LIVE COLLECTION

Now comes the tricky part. It's time to get focused. Once you start, you should work uninterruptedly until the process is complete. To do otherwise only invites mistakes. Before getting underway, gather everything you will need: report forms, pens, memory capture tools, and so on. Every interaction with the computer will need to be noted. You could use an action/response approach ("I did this … The computer did that.").

If the desktop isn't visible, you can move the mouse slightly to wake it up. If that fails to bring up the desktop, pressing a single key should solve the problem. You should, of course, document which key was depressed in your notes.

Now that you can see the desktop, the first thing to note is the date and time as it appears on the computer. Next, record the visible icons and running applications. You don't want to stop there. Documenting the running processes could help identify any malware that is in residence on the computer. The running processes can be documented by accessing the task manager. Why would that matter? One of the more popular defenses, especially in child pornography cases, is to claim that the contraband images were deposited by an unknown third party by way of a Trojan horse.

Now it's time to use a validated memory capture tool to collect that volatile evidence in the RAM. After this step is complete, the process ends with proper

shutdown. The proper shutdown allows any running application a chance to write any artifacts to the disk, allowing us to recover them later.

HASHING

How do we know our clone is an exact duplicate of the evidence drive? The answer comes in the form of a hash value. A hash is a unique value generated by a cryptographic hashing algorithm. Hash values (functions) are used in a variety of ways, including cryptography and evidence integrity. A hash value is commonly referred to as a "digital fingerprint" or "digital DNA." Any change to the hard drive, even by a single bit, will result in a radically different hash value. Therefore, any tampering or manipulation of the evidence is readily detectable.

TYPES OF HASHING ALGORITHMS

There are multiple types of hashing algorithms. The term "algorithm" may strike fear in the hearts of the mathematically challenged. Never fear. We won't be getting into any higher-level math here, but we will get comfortable with some of the basic concepts and terms. The most common hash functions used in digital forensics are Message Digest 5 (MD5), and Secure Hashing Algorithm (SHA) 1 and 2.

HASHING EXAMPLE

Let's hash a short phrase to demonstrate what happens with only a minor change. Apologies up front to any Baltimore or Cleveland fans. For this exercise, we'll use SHA1.

Phrase: Go Steelers!
SHA1: c924 4cac 47b3 4335 5aed 06f3 cc85 ea82 885f 9f3e

Now let's make one small alteration, changing the "S" from upper case to lower case. When we rehash, we get this:

Phrase: Go steelers!
SHA1: 1a10 ffd1 db12 c88f 88e6 b070 561f 6124 f632 26ec

Note the drastic change in the resulting hash values. Here they are stacked for an easier comparison:

c924 4cac 47b3 4335 5aed 06f3 cc85 ea82 885f 9f3e
1a10 ffd1 db12 c88f 88e6 b070 561f 6124 f632 26ec

As you can see, small changes make a big difference. If you'd like to try this yourself, it's easy to do. Go to http://www.wolframalpha.com and enter the hash function you would like to use (MD5, SHA1, etc.), followed by a space and then the phrase Go Steelers((See Figure 4.4.)

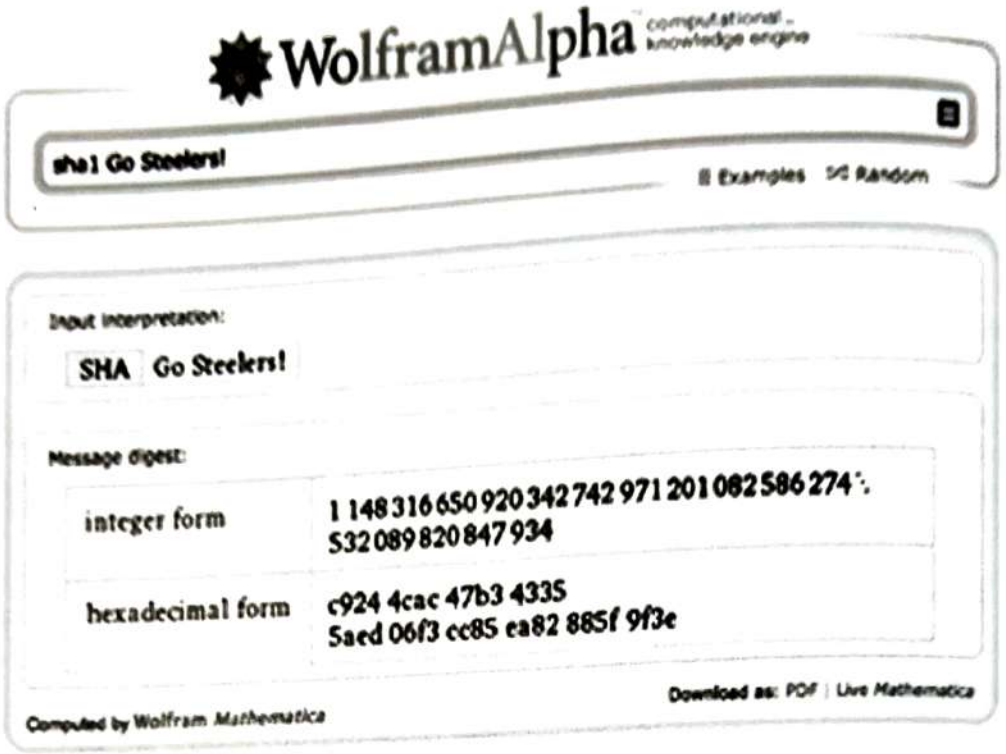

FIGURE 4.4

WolframAlpha results.

USES OF HASHING

Hash values can be used throughout the digital forensic process. They can be used after the cloning process to verify that the clone is indeed an exact duplicate. They can also be used as an integrity check at any point that one is needed. Examiners often have to exchange forensic images with the examiner on the opposing side. A hash value is sent along with the image so it can be compared with the original. This comparison verifies that the image is a bit-for-bit copy of the original. In addition, hash values can be used to identify specific files.

The relevant hash values that were generated and recorded throughout the case should be kept and included with the final report. These digital fingerprints are crucial to demonstrating the integrity of the evidence and ultimately getting that evidence before the jury.

FINAL REPORT

At the conclusion of the analysis, the examiner will generate a final report detailing what was done, what was found, and the findings. Ideally, final reports will be crafted with the intended audience in mind. In reality, far too many final reports read like the owner's manual for the space shuttle. Not only can these reports be difficult to read, they can be downright intimidating.

Because they are often filled with jargon and code, these reports aren't very useful to nontechnical reader's such as judges, attorneys, and juries. It is important to remember that these people must be able to comprehend information contained in your report. Even the best, most compelling evidence can be ignored if the jury can't understand it.

The major forensic tools, such as EnCase and FTK, have very robust reporting features, generating quite a bit of customizable information. However, as helpful as these reports are, they are just not adequate to stand on their own. They are difficult for most nontechnical readers to understand. This information should be included in the final report, but should not serve as the lone piece of documentation for the entire examination.

The best reports will consist of much more than the standard report generated with the tool alone. The final report should include a detailed narrative of all the actions taken by the examiner, starting at the scene if the examiner was there . The examination should be documented with sufficient detail for the procedure to be duplicated by another examiner.

A digital forensic report written in plain English is both much appreciated and much more effective (can I get an "Amen" from the lawyers out there?) than one that is heavy in jargon and tech talk.

SUMMARY

As we discussed in this chapter, the first step in the collection process is to secure both the scene and the evidence. If the device containing the evidence is a cell phone, you will need to isolate the phone from the network signal to prevent evidence from being destroyed.

Photographs are an excellent way to document the evidence and the scene. You will photograph the entire scene (e.g., the entire room, not just the computer on the desk). You must ensure that the chain of custody is fully documented and that the evidence is properly marked.

Preservation of the evidence is critical. Capturing a forensic image or clone eliminates the need to examine the original evidence. Examining the original could lead to the evidence being excluded.

Cloning the device will produce an exact, bit-for-bit copy of the original evidence. Hash values are used to verify that the cloned evidence is identical to the original. These hash values, such as MD5 or SHA1, are often likened to "Digital DNA" or a "Digital Fingerprint." We discussed the differences between live and dead acquisitions and the benefits and challenges of each. The final report should include detail about the scene, the collection process, the analysis, and the conclusions, if any, that were reached. It's critical that the final report be understandable to a nontechnical audience.

REFERENCES

Association of Chief Police Officers, 2011. Good Practice Guide for Computer-Based Electronic Evidence. 7Safe, Cambridge, MA.

Casey, E., 2009. Handbook of Digital Forensics and Investigation. Academic Press, Burlington, MA.

Casey, E., 2011. Digital Evidence and Computer Crime. Forensic Science, Computers, and the Internet, third ed. Academic Press, Waltham, MA.

Favro, P., 2011. Breaking News: $919 Million Verdict for DuPont in Trade Secret Theft and eDiscovery Sanctions Case. E-Discovery. Retrieved from: <www.symantec.com/connect/blogs/lessons-learned-2012-spotlighting-top-ediscovery-cases-2011> (accessed 05.01.11.).

Henry, P., 2009. Best Practices in Digital Evidence Collection. Retrieved from: <http://computer-forensics.sans.org/blog/2009/09/12/best-practices-in-digital-evidence-collection/> (accessed 11.10.11.).

Princeton University Center for Information Technology Policy, 2008. Lest We Remember: Cold Boot Attacks on Encryption Keys. Retrieved from: <https://citp.princeton.edu/research/memory/> (accessed 11.12.11.).

Sedona Conference, 2010. The Sedona Conference Glossary: E-Discovery & Digital Information Management, third ed. Retrieved from: <www.thesedonaconference.org/publications.html> (accessed 06.12.11).

Shipley, T.G., Reeve, H.R., 2006. Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community. Search Group, Incorporated, Sacramento, CA.

www.brainyquote.com/quotes/quotes/c/colinpowell144996.html.

CHAPTER

Windows system artifacts 5

"You see, but you do not observe. The distinction is clear."
—Sherlock Holmes in *A Scandal in Bohemia*

INFORMATION IN THIS CHAPTER:

- Finding Deleted Data
- Hibernation Files
- Examining the Windows Registry
- Print Spooling Evidence
- Recycle Bin Operation
- Metadata: What It Is and How It's Used
- Thumbnail Images as Evidence
- Most Recently Used Lists: How They're Created and Their Forensic Value
- Working with Restore Points and Shadow Copies
- Examining Prefetch and Link Files

INTRODUCTION

Many say that the eyes are the window to the soul, but, for the forensic examiner, Windows can be the "soul" of the computer. The odds are high that examiners will encounter the Windows operating system more times than not when conducting an investigation. The good news for us is that we can use Windows itself as a tool to recover data and track the footprints left behind by the user. Because of this, it is imperative that examiners have an extensive understanding of the Windows operating system and all of its functions.

Love it or hate it, it's a Windows world. With Windows holding about 90% of the desktop market share (Brodkin, 2011), a forensic examiner will face a Windows machine the majority of the time. Getting cozy with Windows is an absolute necessity in this line of work. In the course of using Windows and its multitude of compatible applications, users will leave artifacts or footprints scattered throughout a machine. As you can imagine, this is pretty handy from an investigative perspective. These artifacts are often located in unfamiliar or "hard to reach" places. Even savvy individuals who are bent on covering their tracks can miss some of these buried forensic treasures.

The forensic challenge is to identify, preserve, collect, and interpret this evidence correctly. In this chapter, we'll take a closer look at many of these artifacts, their purpose, and their forensic significance.

DELETED DATA

For the average user, hitting the Delete key provides a satisfying sense of security. With the click of a mouse, we think our data are forever obliterated, never again to see the light of day. Think again. We know from Chapter Two that, contrary to what many folks believe, hitting the Delete key doesn't do anything to the data itself. The file hasn't gone anywhere. "Deleting" a file only tells the computer that the space occupied by that file is available if the computer needs it. The deleted data will remain until another file is written over it. This can take quite some time, if it's done at all.

MORE ADVANCED

FILE CARVING

The unallocated space on a hard drive can contain valuable evidence. Extracting this data is no simple task. The process is known as file carving and can be done manually or with the help of a tool. As you might imagine, tools can greatly speed up the process. Files are identified in the unallocated space by certain unique characteristics. File headers and footers are common examples of these characteristics or signatures. Headers and footers can be used to identify the file as well as mark its beginning and end.

Allocated space refers to the data that the computer is using and keeping tabs on. These are all the files that we can see and open in Windows. The computer's file system monitors these files and records a variety of information about them. For example, the file system tracks and records the date and time a particular file was last modified, accessed, and created. We'll revisit this kind of information when we talk about metadata later in this chapter.

HIBERNATION FILE (HIBERFILE.SYS)

Computers sometimes need their rest and can nap just like we do. Generally, a computer can go into three different modes or states when it sleeps. Those modes are: sleep, hibernation, and hybrid sleep. (Microsoft Corporation). The different modes are intended to conserve power and can vary from laptop to desktop. Through this "cybernap" process, more potential evidence can be generated, depending on how "deeply" the PC goes to sleep. "Deep sleep" modes such as hibernation and hybrid sleep save data to the hard drive as opposed to just holding it in RAM as in "sleep." As we know, data written to the drive itself are more persistent and can be recovered. It's possible that files deleted by a suspect could still be found here. How?

Let's say that the suspect is working on an incriminating document on Monday. She has to step away for awhile to make a phone call. She puts the laptop into hibernation mode, which causes the computer to save everything she is doing to the hard drive. When she returns 45 minutes later and brings the laptop back up, everything is just as she left it, including the incriminating document.

SLEEP

Sleep mode is intended to conserve energy but is also intended to get the computer back into operation as quickly as possible. Microsoft compares this state to "pausing a DVD player" (Microsoft, 2011; TechTarget, 2011). Here, a small amount of power is continuously applied to RAM, keeping those data intact. Remember, RAM is considered volatile memory, meaning that the data disappear when power is removed. Sleep mode doesn't do much for us forensically because all the data remain in RAM.

HIBERNATION

Hibernation is also a power-saving mode but is intended for laptops rather than desktop computers. It is here that we start to see some potential investigative benefit. In this mode, all of the data in RAM are written to the hard drive, where, as we know, it is much harder to get rid of data.

HYBRID SLEEP

As the name implies, hybrid sleep is a blend of the previous two modes and is intended mainly for desktops. It keeps a minimal amount of power applied to your RAM (preserving your data and applications) and writes the data to disk.

As with a page file, suspects bent on destroying evidence can overlook these hibernation files. Pedophiles or corporate crooks will often attempt to avoid detection by deleting or destroying evidence on their hard drives as investigations close in around them. These hibernation files, unknown to most users, are often missed during these last-minute "delete-a-thons."

REGISTRY

The Windows registry plays a crucial role in the operation of a PC. Microsoft's TechNet defines the registry as "simply a database for configuration files" (TechTarget, 2011). You could also describe it as the computer's central nervous system. In that context, you can see just how critical the registry is to the Windows computer.

The registry keeps track of user and system configuration and preferences, which is no simple task. From a forensic standpoint, it can provide an abundance of potential evidence. Many of the artifacts we look for are kept in the registry. Some of the potential evidence could include search terms, programs that were run or installed,

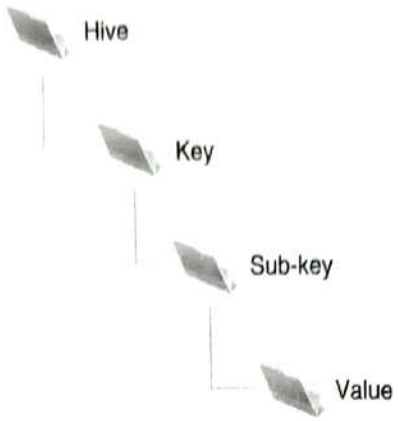

FIGURE 5.1

The Basic Structure of the Windows Registry.

web addresses, files that have been recently opened, and so on. As an added bonus, the registry can also hold the information we need to break any encrypted files we find.

REGISTRY STRUCTURE

The registry is set up in a tree structure similar to the directories, folders, and files you're used to working with in Windows. The registry is broken down into hives, keys, subkeys, and values. See Figure 5.1.

The Windows registry is comprised of five root-level keys. Each of these five bears the prefix of HKEY. Figure 5.2 shows these keys as seen through Regedit, the built-in registry editor in Windows. The five keys are classified as either derived or

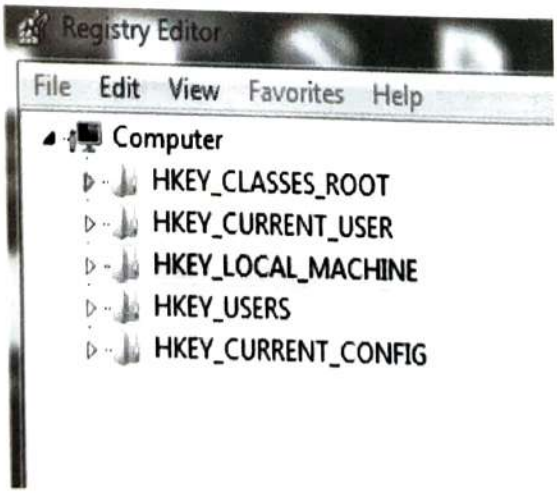

FIGURE 5.2

The Five Root-Level Keys as Seen in Regedit.

Table 5.1 The Five Root-Level Keys.

Key	Derived/Master	Brief Description
HKEY_CLASSES_ROOT	Derived	Links file types with programs (i.e., .doc file with Microsoft Word).
HKEY_CURRENT_USER	Derived	Configures the computing environment for individual users.
HKEY_CURRENT_CONFIG	Derived	Addresses the current hardware configuration.
HKEY_LOCAL_MACHINE	Master	Addresses all aspects of the computer's operation.
HKEY_USERS	Master	Computing environment settings for users that have logged on to the system.

master keys. If the key is derived, it's linked to the two master keys. Table 5.1 lists the five root-level keys along with a few details of each.

Inspecting the registry is done in nearly every forensic examination. Looking at the registry requires a tool that can translate this information into something we can understand. Two of the major multipurpose forensic tools, EnCase and FTK, do just that. FTK parses the registry for us, providing quite a bit of information. In addition, a separate application comes with FTK that is specific to the Windows registry. We can export registry files into Registry Viewer for a closer look (Figure 5.3).

As we've discussed, the registry holds quite a bit of information. Not all of it, however, will have any forensic value. A very handy feature in Registry Viewer is the ability to reduce the "noise" and show us only those areas that normally have some investigative significance. Registry Viewer calls these Common Areas and are displayed with the click of one button. Figure 5.4 shows us the software key with the Common Areas selected.

From the case files: the Windows registry

The Windows Registry helped law enforcement officials in Houston, Texas, crack a credit card case. In this case, the suspect's stolen credit card numbers were used to purchase items from the Internet. The two suspects in this case, a married couple, were arrested after a controlled drop of merchandise ordered from the Internet. Examination of their computer's NTUSER.DAT, Registry, and Protected Storage System Provider information found a listing of multiple other names, addresses, and credit card numbers that were being used online to purchase items. After further research, investigators discovered that these also were being used illegally without the owners' consent.

The information recovered from the registry was enough to obtain additional search warrants. These extra searches netted the arrest of twenty-two individuals and led to the recovery of more than (100,000 in illegally purchased merchandise. Ultimately, all of the suspects pleaded guilty to organized crime charges and were sentenced to jail time.

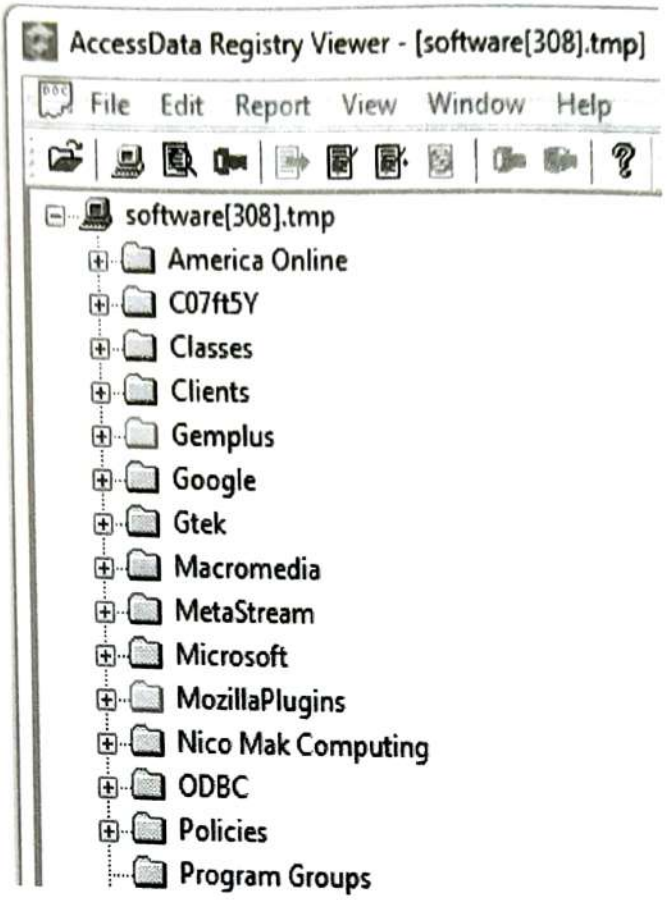

FIGURE 5.3

The Software Key in Access Data's Registry Viewer.

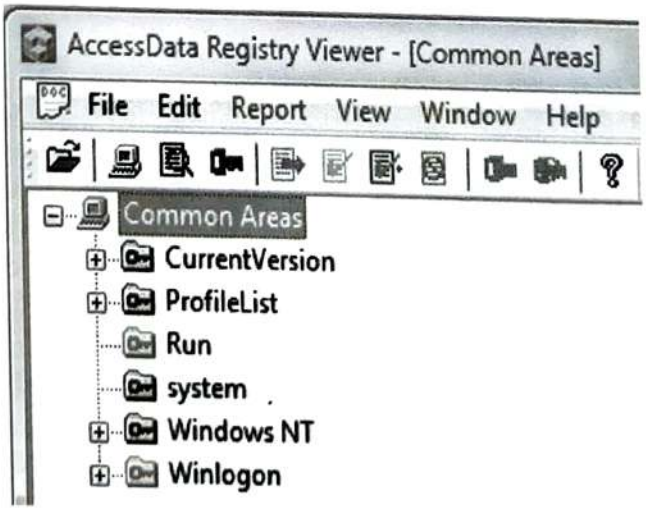

FIGURE 5.4

The Common Areas of the Software key in Access Data's Registry Viewer.

From the case files: the Windows registry and USBStor

In a small town outside Austin, Texas, guests at a local hotel called police after observing an individual at the hotel who was roaming around, mostly naked and appearing somewhat intoxicated. When the police arrived, they found the individual and determined that he was staying at the hotel. They accompanied him back to his room and were surprised by what they found. When the door opened, they discovered another individual in the room and a picture of child pornography being projected on the wall. The projector was attached to a laptop. Two external hard drives were found lying next to the laptop. The unexpected occupant said that the laptop was his but that the two external drives belonged to the other man and had never been connected to his laptop. All of the equipment was seized and sent for examination. Forensic clones were made of the laptop and both external drives. The initial examination of the external drives found both still images and movies of child pornography.

Next, examiners wanted to determine whether either of those drives had ever been connected to the laptop. The system registry file of the laptop was searched for entries in the USBStor key. Listings for external hard drives were discovered along with the hardware serial numbers from both external hard drives.

Next, examiners sought to validate their results. Using a lab computer system with a clean installation of Windows, they connected the defendants' external drives to the lab system. A write blocker was connected between the drives and the system to prevent any changes or modifications to the clones of the external drives.

The lab computer's system registry file was then examined and the USBStor keys showed the same external hard drive listings as the suspect's, with matching hardware serial numbers. These results proved that the suspect's external hard drives had, in fact, been connected to the laptop at one time. The suspect was eventually convicted of possession of child pornography.

ATTRIBUTION

Digital forensics can be used to answer many questions, such as "What terms were searched using Google?" We can find that. "Did Bob type those terms?" Houston, we've got a problem. Unfortunately, we can rarely put someone's sticky fingers on the keyboard when a particular artifact is created. We may need to uncover other evidence to connect those dots.

Tracking something back to a specific user account or identifying the registered owner of the system is a much easier task. A single PC can have multiple user accounts on the machine. In a technical sense, user accounts establish what that specific user can and can't do on the computer (Microsoft, 2011d). A PC will set up two accounts by default: the administrator and a guest account. Other accounts may be created, but they are not required. The administrator has all rights and privileges on the machine. The administrator can do anything with the machine. A guest account (which doesn't require any login) generally has less authority.

For example, a family PC could have separate accounts for Mom, Dad, and each of the kids. Each of these accounts could be password-protected.

Each account on the machine is assigned a unique number called a security identifier (SID). Many actions on the computer are associated with, and tracked by, a specific SID. It's through the SID that we can tie an account to some particular action or event.

EXTERNAL DRIVES

Information has value—sometimes substantial value. The Coca-Cola Company doesn't keep the formula for Coke under lock and key for grins. Theft of intellectual property is a huge concern. One way that would-be thieves could easily smuggle data out of an organization is by way of one of these external storage devices, such as a thumb drive. As a result, examiners are often asked to determine whether any such device has been attached to a computer.

These devices can take a variety forms, such as thumb drives or external hard drives. In addition to stealing information, these devices can also be used to inject a virus or store child pornography. Whether such a device was attached can be determined by data in the registry. The registry records this kind of information with a significant amount of detail, including both the vendor and the serial number of the device.

PRINT SPOOLING

In some investigations, a suspect's printing activities may be relevant. As you might expect, printing can also leave some tracks for us to follow. You've probably noticed that there's a bit of a delay after you click Print. This delay is an indication of a process called spooling. Essentially, spooling temporarily stores the print job until it can be printed at a time that is more convenient for the printer (TechTarget, 2011). During this spooling procedure, Windows creates a pair of complementary files. One is the Enhanced Meta File (EMF), which is an image of document to be printed. The other is the spool file, which contains information about the print job itself.

There is one of each for every print job. What kind of information can we recover from the spool file? The spool file (.spl) tells us things like the printer name, computer name, and the user account that sent the job to the printer. Either or both of these files may have evidentiary value. The problem is they don't stick around long. In fact, they are normally deleted automatically after the print job is finished. However, there are a few exceptions.

The first exception occurs if there is some kind of problem and the document didn't print. The second is that the computer that is initiating the print job may be set up to retain a copy. Some companies may find this setup appealing if they have some reason to hang onto a copy.

Spool and EMF files can be used to directly connect targets to their crimes. Copies of extortion letters, forged contracts, stolen client lists, and maps to body dump sites are but a few pieces of evidentiary gold potentially mined from their computers.

RECYCLE BIN

The trash can has been a familiar presence on computer desktops starting with the early Macintosh systems. It's a really good idea, especially from the casual user's perspective. Users may not understand sectors and bytes, but most everyone "gets" the trash can. Sometimes, though, the trash can "gets" them. This is especially true when they count on the trash can to erase their evidence. They assume that their incriminating data have disappeared into a digital "Bermuda Triangle," never again to see the light of day. Unlike Amelia Earhart, that's definitely not the case. Using forensic tools such as Forensic Toolkit and EnCase, we can quite often bring those files back in mint condition.

ALERT!

RECYCLE BIN FUNCTION

Here's a quick question. Where is a file moved when it's deleted? I bet some of you said the Recycle Bin. That would make the most sense. I mean, that's where we put the unwanted files, right? But it would also be wrong. When you delete a file, it's moved to ... wait for it ... nowhere. The file itself stays exactly where it was. It's a common notion that, when deleted, the file is actually picked up and moved to the Recycle Bin. That's not the case.

Unwanted files can be moved to the Recycle Bin a few different ways. They can be moved from a menu item or by dragging and dropping the file to the Recycle Bin. Finally, you can right-click on an item and choose Delete. The benefit of putting files into the Recycle Bin is that we can dig through it and pull files back out. I've worked in places where digging through an actual office trash can be a pretty hazardous undertaking. Fortunately, things aren't nearly as dicey on our computers. As long as our files are still "in the can," we can get them back. However, emptying the Recycle Bin (i.e., "taking out the trash") makes recovery pretty much impossible for the average user.

Not everything that's deleted passes through the Recycle Bin. A user can actually bypass the bin altogether. Bypassing can be done in a couple of ways. First, if you press Shift+Delete, the file will go straight to unallocated space without ever going through the Recycle Bin. You can also configure your machine to bypass the Recycle Bin altogether. Your deleted files won't even brush the sides of the Recycle Bin.

The Recycle Bin is obviously one of the first places where examiners look for potential evidence. The first instinct suspects have is to get rid of any and every

incriminating file on their computers. Not fully understanding how their computers work, they put all their faith in the Recycle Bin. Now you know that's a bad move. Lucky for us, many folks still don't recognize how misplaced their faith is. As a result, the Recycle Bin is a great place to look for all kinds of potentially incriminating files.

MORE ADVANCED

RECYCLE BIN BYPASS

If an examiner suspects that the system has been set to bypass the recycle bin, the first thing they would check would be the registry. The "NukeOnDelete" value would be set to "1" indicating that this function had been switched on. (See Figure 5.5.)

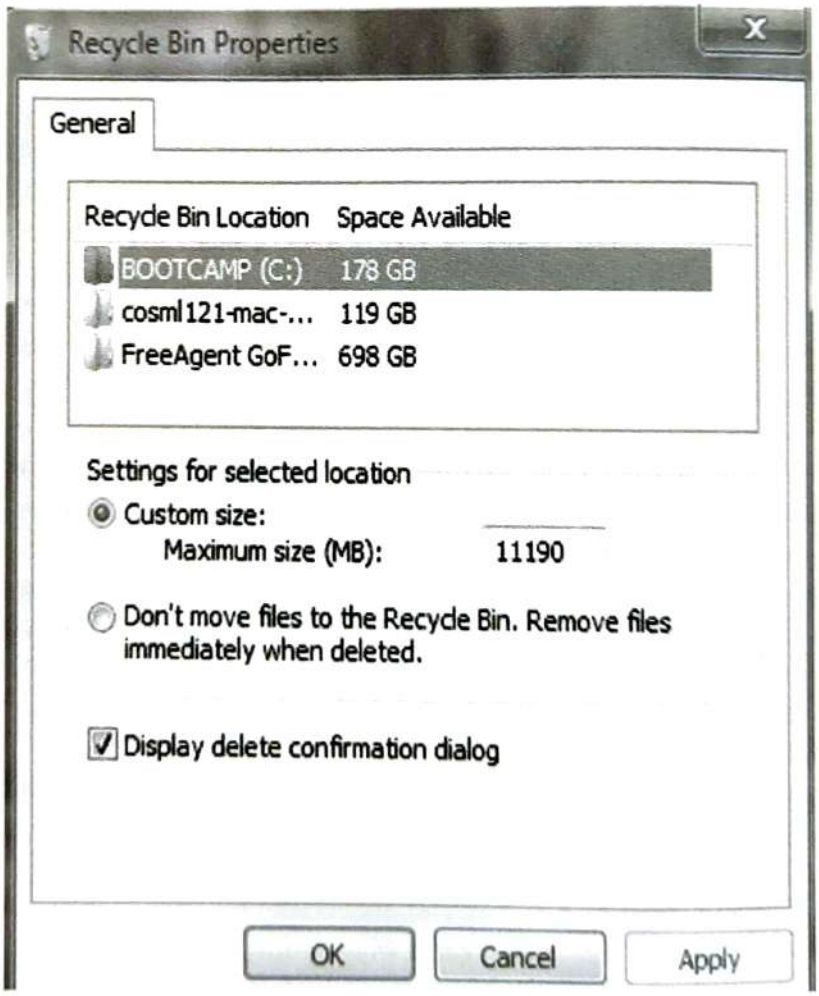

FIGURE 5.5

The recycle bin bypass option.

METADATA

Metadata is most often defined as data about data. Odds are you've come across metadata at some point, although you may not have known that's what you were looking at. There are two flavors of metadata, if you will: application and file system. Remember, the file system keeps track of our files and folders, as well as some information about them. File system metadata include the date and time a file or folder was created, accessed, or modified. If you right-click on a file and choose "Properties," you can see these date/time stamps as shown in Figure 5.6.

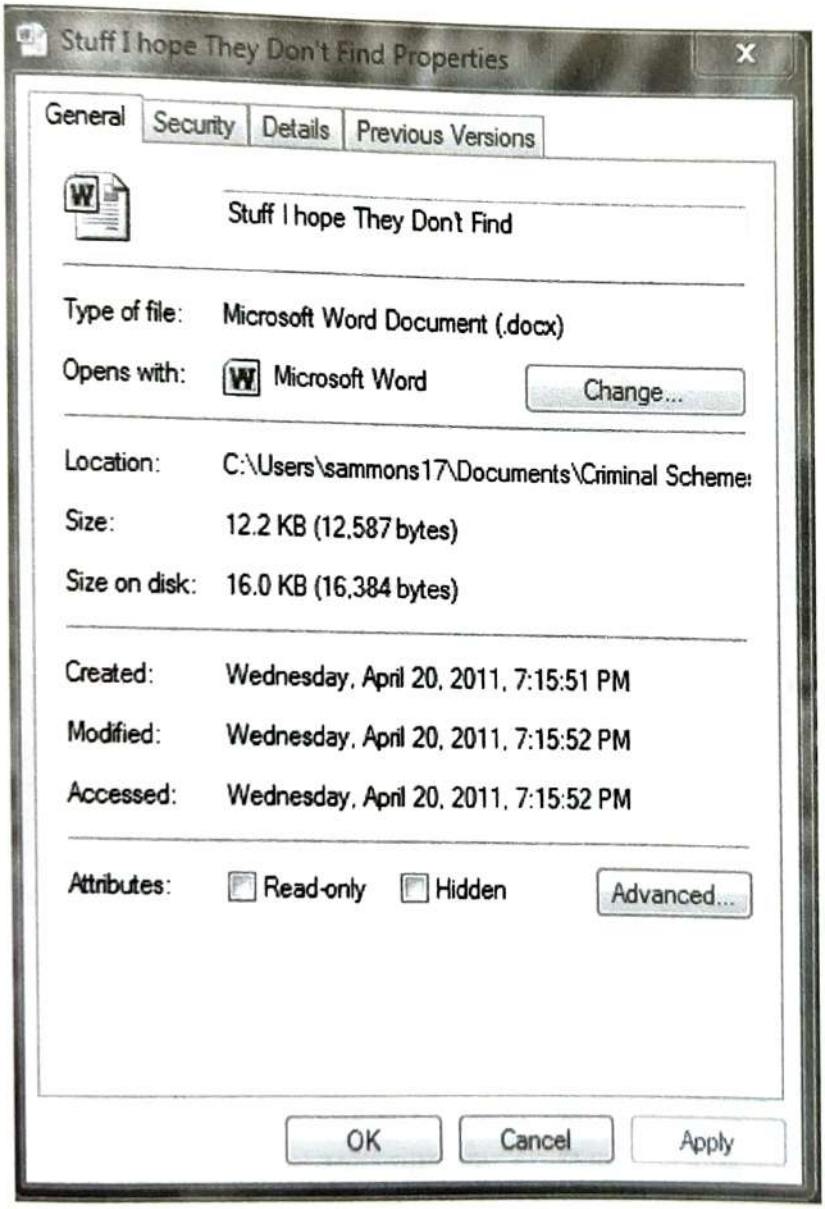

FIGURE 5.6

Metadata information as seen after right-clicking on the file and choosing "Properties." Note the created, modified, and accessed dates and times.

Although this information can prove quite valuable to an investigation, we must keep in mind that all these date/time stamps may not be what they seem. One problem is that the system's clock can be changed by the user. Time zone differences can also cause some issues. Let's take a little closer look at the created, accessed, and modified date/time stamps.

Created—The created date/time stamp frequently indicates when a file or folder was created on a particular piece of media, such as a hard drive (Casey, 2009). How the file got there makes a difference. By and large, a file can be saved, copied, cut and pasted, or dragged and dropped.

Modified—The modified date and time are set when a file is altered in any way and then saved (Casey, 2009).

Accessed—This date/time stamp is updated whenever a file is accessed by the file system. "Accessed" does not mean the same thing as "opened." You may be asking how a file can be accessed without being opened, and that's a good question. You see, the computer itself can interact with the files. Antivirus scans and other preset events are just two examples of this automated interaction.

ALERT!

DATE AND TIME STAMPS

System date and time stamps should *not* be taken simply at face value. These settings are readily accessible and can be easily changed. Determining an accurate timeline can be further complicated if the case involves more than one time zone. Just because the metadata say a file was created at a certain date and time doesn't necessarily make it so.

Applications themselves can create and store metadata as well. Like the file system, they can track the created, accessed, and modified dates and times. But it doesn't stop there. They can also track a variety of application-specific attributes as well. Examples could include the name of the author, the name of the company or organization, and the computer name, just to "name" a few (Casey, 2009).

REMOVING METADATA

Although metadata used to be one of our best-kept secrets, it's not any more. The criminals aren't the only ones taking notice. Corporations, law firms, and private citizens are just some of the folks concerned about metadata and the information contained therein. These legitimate concerns are being addressed by actually removing the metadata before sharing those files with other people. Many tools exist for just that purpose. For example, law firms routinely scrub the metadata from all of their outbound documents, like those transmitted via e-mail. For the privacy-minded individual, the newer versions of Microsoft Word have the ability to detect and remove metadata. (See Figures 5.7 and 5.8.)

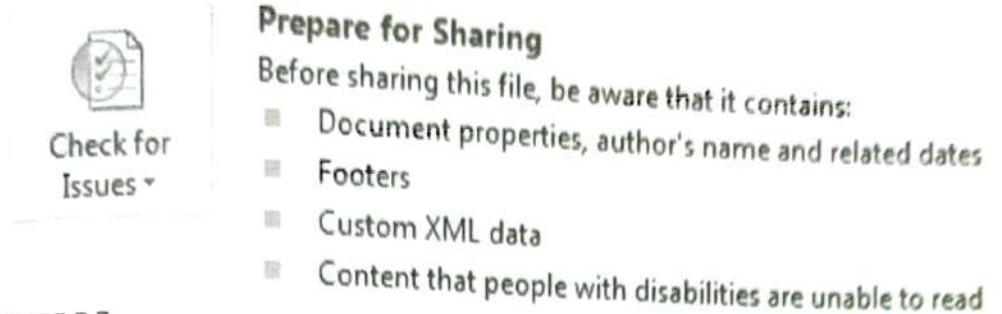

FIGURE 5.7

Menu item to choose for scrubbing inside Microsoft Word 2010.

Recovered metadata can be used to refute claims by a suspect that they had no knowledge of a file's existence. It's tough to claim you didn't know it was there when you not only opened the file but you changed or deleted the file as well. These dates and times can also be used to construct timelines in a case.

From the case files: metadata

Metadata can help investigators identify all the suspects in a case and recover more evidence. Take the case from Houston, Texas, regarding the production of counterfeit credit cards. The suspects in this case used "skimmed" card information in their card production process. Credit card skimming is when thieves grab the data from the magnetic strip on the backs of credit and debit cards. This often occurs during a legitimate transaction, such as when you use your card to pay for dinner at a restaurant.

After identifying their prime suspect, police arrested him and searched his computer. In the end, the search of the computer was disappointing. The search found one only Microsoft Word document that contained skimmed information. Furthermore, the search of the residence found no skimmer hardware and there was no skimming software on the computer. Not exactly the treasure trove they had hoped to find.

The exam didn't stop there. Further examination of the Word document hit pay dirt. A review of the metadata revealed the author of the document—a female. Further investigation found that she was the suspect's girlfriend and that she worked as a waitress in a neighboring town. This information gave investigators the probable cause needed to obtain a second search warrant for her apartment. During the second search, the skimmer (the piece of hardware used to extract the data from the

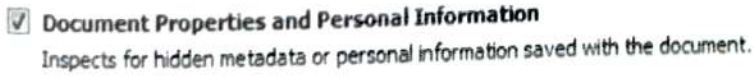

FIGURE 5.8

The option to scan for metadata in Microsoft Word 2010.

magnetic strip) was recovered. The examination of the computer found not only the skimming software, but additional lists of debit cards and related information. Fortunately, this information was seized before it could be used. Both suspects were eventually found guilty. Sammons, personal communication, 2011.

THUMBNAIL CACHE

To make it easier to browse the pictures on your computer, Windows creates smaller versions of your photos called thumbnails. Thumbnails are just miniaturized versions of their larger counterparts. These miniatures are created automatically by Windows when the user chooses "Thumbnail" view in using Windows Explorer. Windows creates a couple of different kinds of thumbnail files, depending on the version being used. Windows XP creates a file called thumbs.db. Microsoft Vista and Windows 7 create a similar file called thumbcache.db.

Most users are completely unaware that these files even exist. The cool thing about these files is that they remain even after the original images have been deleted. Even if we don't recover the original image, thumbnails can serve as the next best evidence. Their mere existence tells us that those pictures existed at one point on the system.

MOST RECENTLY USED

Windows tries to make our lives, at least on our computers, as pleasant as possible. They may not always succeed, but their hearts are in the right place. The Most Recently Used (MRU) list is one such example of Microsoft thinking of us. The MRUs are links that serve as shortcuts to applications or files that have recently been used. You can see these in action by clicking on the Windows Start button through the File menu in many applications. (See Figure 5.9.)

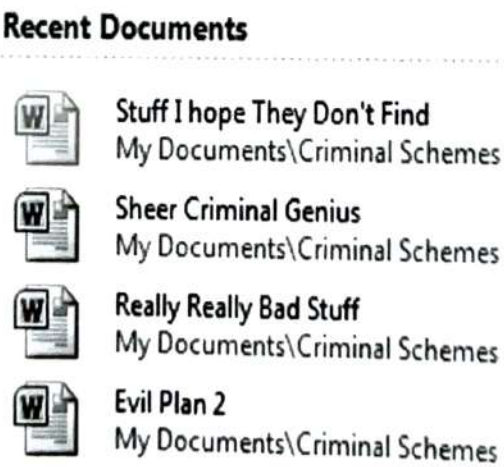

FIGURE 5.9

An MRU in Microsoft Word 2010.

RESTORE POINTS AND SHADOW COPY

Do you ever wish you could go back in time? We're not there yet, but lucky for us, Windows is. There may come a time when it's just easier (or necessary) for our computers to revert back to an earlier point in time when everything was working just fine. In Windows, these are called restore points (RPs), and they serve as time travel machines for our computers.

RESTORE POINTS

Restore points are snapshots of key system settings and configuration at a specific moment in time (Microsoft, 2011c). These snapshots can be used to return the system to working order. RPs are created in different ways. They can be created by the system automatically before major system events, such as installing software. They can be scheduled at regular intervals, such as weekly. Finally, they can be created manually by a user. The RP feature is on by default, and one snapshot is automatically produced every day.

Before you start looking around for your RPs, you should know that Microsoft has taken steps to keep them from your prying eyes. They are normally hidden from the user.

These RPs have metadata (data about the data) associated with them. This information could be valuable in determining the point in time when a snapshot was taken. If the RP contains evidence, this can tell us exactly when that data existed on the system in question.

Digging through the RPs may reveal evidentiary gems that don't exist anywhere else. For the average person trying to conceal information from investigators, RPs are likely not the first place they would start destroying evidence. Obviously, that works in our favor.

From the case files: Internet history and restore points

A defendant accused of possessing child pornography claimed that he had visited the site in question on only one occasion, and that was only by accident. To refute this claim, examiners turned to the restore points for the previous two months. Examination of each of the registry files found in the various RPs told a significantly different story. The evidence showed that not only had multiple child pornography sites been visited, but the URLs had been typed directly into the address bar of the browser, destroying his claim that the site was visited by accident. Confronted with this new evidence, the defendant quickly accepted a plea deal.

SHADOW COPIES

Shadow copies provide the source data for restore points. Like the RP, a shadow file is another artifact that could very well be worth a look. We can use shadow files to demonstrate how a particular file has been changed over time. They can likewise hold copies of files that have been deleted (Larson, 2010).

From the case files: restore points, shadow copies, and anti-forensics

Officers from the Texas Office or the Attorney General (OAG) Cyber Unit, responding to a tip, served a search warrant at a suspect's residence. The OAG Cyber Unit obtained the search warrant after being were alerted that the suspect was uploading child pornography to the Internet. When the officers served the search warrant, they found the house unoccupied. Officers called the suspect, letting him know they were in his home and that he should come home immediately and meet with them. When the suspect arrived, officers interviewed the suspect and searched his vehicle. Inside the car in which he arrived was a laptop computer.

All items seized were taken to the OAG offices for forensic examination. During the exam of the suspect's laptop, an alarming discovery was made. It appeared the suspect, on the drive home to meet the officers, used a wiping tool to get rid of not only incriminating images but the Internet history from his laptop. While the initial exam found no child pornography on the laptop, other compelling evidence was recovered.

For example, the examiner was able to recover logs from the wiping program itself, showing that it had indeed been run. That wasn't all. Since the operating system was Windows Vista, the examiner decided to check the shadow copies found on the machine. Remember, these shadow copies (or System Restore Points) are essentially snapshots of data at a given point in time.

Next, the forensic image (clone) of the suspect's laptop was loaded into a virtual environment. This enabled the examiner to see the computer system as the suspect saw it. The examiner exported out the restore points from the suspect's laptop, then imported those same files into the forensic tool. This process allowed the examiner to use his tools to extract images and other information from the suspect's system RPs. This procedure hit pay dirt. More than 3,000 images of child pornography were recovered. In addition, log files were found showing searches and downloads of those same files. When it was all said and done, the suspect pleaded guilty and is currently serving ten years in a Texas state prison.

PREFETCH

Speed kills. In the case of computers, it's the *lack* of speed that kills. Developers at Microsoft know this and work hard to squeeze every millisecond out of the system. Prefetching is one of the ways they try to speed up the system.

Prefetch files can show that an application was indeed installed and run on the system at one time. Take, for example, a wiping application such as Evidence Eliminator. Programs like this are designed to completely destroy selected data on a hard drive. Although we may not be able to recover the original evidence, the mere presence of Evidence Eliminator can prove to be almost as damning as the original files themselves. Stay tuned for more discussion on Evidence Eliminator.

LINK FILES

We all love shortcuts. They help us avoid road construction and steer clear of traffic jams. They save us time and make our travels easier, at least in theory. Microsoft Windows also likes shortcuts. It likes them a lot.

Link files are simply shortcuts. They point to other files. Link files can be created by us, or more often by the computer. You may have created a shortcut on your desktop to your favorite program or folder. The computer itself creates them in several different places. You've probably seen and used these link files before. Take Microsoft Word, for example. If you look under the File menu, you'll see an option called "Recent." The items in that list are link files, or shortcuts, created by the computer.

Link files have their own date and time stamps, showing when they were created and last used. The existence of a link file can be important. It can be used to show that someone actually opened the file in question. It can also be used to refute the assertion that a file or folder never existed. Link files can also contain full file paths, even if the storage device, such as a thumb drive, is no longer connected.

INSTALLED PROGRAMS

Software that is or has been installed on the questioned computer could also be of interest. This is especially true if the same application has been removed after some relevant point in time (i.e., when the suspect became aware of a potential investigation). There are multiple locations on the drive to look for these artifacts. The Program folder is a great place to start. Link and prefetch files are two other locations that could also bear fruit.

SUMMARY

The computer records a tremendous amount of information, unbeknownst to the vast majority of users. These artifacts come in a variety of forms and can be found throughout the system. For example, it's possible to identify external storage devices, such as thumb drives, that have been attached to the system. Items moved to the Windows Recycle Bin can tell us when they were deleted and by which account.

Even if a file has been deleted or overwritten, copies of the file could still exist on a drive in multiple forms. These often-overlooked copies are generated by print jobs and hibernation functions, as well as restore points. These files can also be found in the swap space, a specific portion of a hard drive that is used when the system is out of RAM.

One major takeaway from this chapter is that valuable evidence of specific files, actions, or events can be recorded in multiple locations. As such, truly getting rid of such material can be a highly technical process beyond the reach of most crooks.

Even deleting data and defragging your hard drive won't get rid of all data. The computer stores data in a way that permits fragments of older files to be carved out

for further analysis. The partial files removed from the slack space could contain just enough information to become a useful piece of evidence. Attribution is a major challenge in digital forensics. Saying with absolute certainty that a specific individual was responsible for a given artifact is often impossible. Identifying the account is often the best that can be done.

The system and the applications we use generate data about data. This information, known as metadata, can tell us when the file was created, accessed, modified, and deleted. Knowing what software has been installed and run could be relevant to an investigation. Drive-wiping software, for example, could be of particular interest. The Windows registry and the prefetching function are two sources of this potentially relevant information.

REFERENCES

Brodkin, J., 2011. Windows on Verge of Dropping Below 90% Market Share. Retrieved from: <http://www.networkworld.com/news/2011/011311-windows-on-verge-of-dropping.html> (accessed 11.05.11.).

Casey, E., 2009. Handbook of Digital Forensics and Investigation. Academic Press, Burlington, MA.

Doyle, A., 1891. Sherlock Holmes A Scandal in Bohemia. The Strand Magazine, United Kingdom.

Larson, T., 2010. Windows 7 Current Events in the World of Windows Forensics. Retrieved from: <http://digital-forensics.sans.org/summit.../12-larson-windows7-forensics.pdf> (accessed 11.05.11.).

Microsoft Corporation, 2011a. How the Recycle Bin Stores Files. Retrieved from: <http://support.microsoft. com/kb/136517> (accessed 11.05.11.).

Microsoft Corporation, 2011b. Sleep and Hibernation: Frequently Asked Questions. Retrieved from: <http://windows.microsoft.com/en-us/windows7/sleep-and-hibernation-frequently-asked-questions> (accessed 11.05.11.).

Microsoft Corporation, 2011c. System Restore: Frequently Asked Questions. Retrieved from: <http://windows.microsoft.com/en-us/windows/system-restore-faq#1TC=windows-7> (accessed 11.05.11.).

Microsoft Corporation, 2011d. User Accounts Overview: Microsoft Corporation. Retrieved from: <http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/usercpl_overview.mspx?mfr=true> (accessed 11.05.11.).

TechTarget, 2011. Spool: Whatis.com. Retrieved from: <http://whatis.techtarget.com/definition/0,sid9_ gci214229,00.html> (accessed 11.05.01.).

CHAPTER

Legal 7

"I am not an advocate for frequent changes in laws and constitutions, but laws and institutions must go hand in hand with the progress of the human mind ... as new discoveries are made ... institutions must advance also to keep pace with the times."

—Thomas Jefferson

INFORMATION IN THIS CHAPTER:

- The Legal Aspects of Digital Forensics
- The Fourth Amendment and Its Impact on Digital Forensics
- Electronic Discovery
- Duty to Preserve Potential Digital Evidence in Civil Cases
- Private Searches and Establishing the Need for Offsite Analysis
- Overview of the Electronic Communications Privacy Act
- Searching Digital Evidence With and Without a Search Warrant

INTRODUCTION

No discussion of digital forensic fundamentals can be complete without including the legal aspects of the discipline. The legal community has been playing a perpetual game of catch up with technology since the very beginning. With computer and other technologies becoming so intertwined in our work and private lives, it was inevitable that electronic data would find its way into the courts. It's not just about the child pornographers and identity thieves; digital evidence plays a huge role in civil litigation as well.

With these newfangled technologies came new criminal behaviors that necessitated new statutes outlawing them. Some of these are simply old crimes with a new twist. In this instance, the technology just facilitated the crime in an up-to-date, more efficient way.

Search authority is the very first step in the digital forensic process. The authority itself can take many forms, depending on which venue you're working in at the time.

Whether it be a civil or criminal case, having valid search authority is a requirement. In fact, it's the first step in the digital forensic process. In this chapter, we'll examine the fundamental legal issues in both criminal and civil litigation.

THE FOURTH AMENDMENT

The Fourth Amendment of the U.S. Constitution serves as the "litmus test" for all governmental searches and seizures. Any evidence deemed to be seized in violation of the Fourth Amendment is inadmissible in a court of law. Americans have had a long-standing distaste for governmental intrusion into their private lives. Before the American Revolution, British soldiers, operating under Writs of Assistance, routinely invaded the homes of citizens without cause. The Fourth Amendment to the Constitution was crafted with this travesty in mind. The Fourth Amendment says: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized" (FindLaw, 2011).

CRIMINAL LAW—SEARCHES WITHOUT A WARRANT

Two key questions must be answered from the beginning. First, did the government act? Second, did that action violate the individual's reasonable expectation of privacy? If the answer to the first question is "no," then the Fourth Amendment doesn't apply. It only covers searches by the government (or its agents), not ones by private citizens.

For Fourth Amendment purposes, a person becomes an agent of the government if acting at the request of law enforcement. Under that scenario, it would be no different than if a police officer conducted the search.

REASONABLE EXPECTATION OF PRIVACY

What exactly is a "reasonable expectation of privacy"? That's a great question with no easy answer. There is no clear-cut rule or test that would help us define it. Much of the interpretation centers on what society as a whole would consider as being reasonable. For example, people would reasonably have a greater expectation of privacy on their personal computers than they would at a public library. As a rule of thumb, you can consider the computer as a closed container. If the officer lacks the authority to open a desk drawer or box, the same would be true with a computer (Executive Office for United States Attorneys, 2009).

If the person has a reasonable expectation of privacy, the government must first obtain a search warrant, or the search would have to meet one of the documented exceptions to the warrant requirement.

What about individual files? Should they be seen as separate, closed containers? It seems that courts aren't sure either. Rulings have been handed down supporting both positions. In *United States v. Slanina*, the Fifth Circuit ruled that, when a proper search is conducted on a portion of a disk, defendants no longer have a reasonable expectation of privacy in regard to other files. (United States v. Slanina, 2002).

In contrast, the Tenth Circuit took the opposite stance, saying "[b]ecause computers can hold so much information touching on many different areas of a person's life, there is greater potential for the 'intermingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer" (*United States v. Walser*, 2001).

Information that an individual knowingly exposes to others is not protected by the Fourth Amendment. Examples here could include public computers such as those in a classroom or "shared drives" on a network (Executive Office for United States Attorneys, 2009).

PRIVATE SEARCHES

Private searches are not afforded Fourth Amendment protection unless the search is done at the request of the government or with its knowledge or involvement. Take the Geek Squad at Best Buy, for example. Let's say that someone gives them permission to work on a home computer and, in the process, they find child pornography images on the machine. The images found by the repair technician would be admissible as long as the technician was not searching at the request of the government, thereby acting as its agent.

E-MAIL

By and large, an individual maintains Fourth Amendment protections when an e-mail is being transmitted, but would lose those protections when it reaches its final destination. E-mail is viewed in a similar fashion as regular "snail mail." The legal interception of an individual's e-mail or other electronic communication is tightly controlled. Known as the Wiretap Act, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 prohibits unauthorized monitoring and lists the procedures needed to obtain a warrant for wiretapping (DOJ, Office of Justice Programs, 2010).

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

The purpose of the Electronic Communications Privacy Act (ECPA) was to ban a third party from intercepting and/or disclosing electronic communications without prior authorization. This federal statute was passed originally in 1968 as an amendment to the Wiretap Act of 1968. The ECPA underwent its first change in 1994, when it was amended by the Communications Assistance to Law Enforcement Act (CALEA). It was modified once again after the 9-11 attacks by the USA Patriot Act. The Patriot Act was authorized again in 2006 (TechTarget, 2005).

EXCEPTIONS TO THE SEARCH WARRANT REQUIREMENT

There are several well-known exceptions to the search warrant requirement. A warrantless search is valid with consent as long as the person giving the consent

is authorized and the consent is truly voluntary. The voluntariness of the consent is judged on the totality of the circumstances. The Supreme Court recognized age, education, intelligence, and the physical and mental condition of the person giving consent as important factors to consider. Other considerations would be whether the person was under arrest at the time of consent and whether the person had been advised of his right to refuse consent. If the validity of the search relies on consent, the burden is on the government to prove that the consent was, indeed, given voluntarily.

Consent may be revoked at any time. The search must cease immediately when the consent is withdrawn. What happens if the suspect has second thoughts after his or her computer has been collected and taken to the lab for processing? The same standard applies—almost. The search must stop when the suspects revokes consent. That said, courts have found that this does *not* apply to forensic clones. In other words, although the original must be returned, any clones that have been made do not. Defendants do not have a reasonable expectation of privacy with a forensic clone (*United States v. Megahed*, 2009). For this very reason, cloning a drive sooner rather than later is a very wise move.

The scope of a consent search is sometimes at issue in a criminal case. If the suspect gives you consent to search the house, does that include closed containers and computers? Well, that depends on the particular details of the situation. Courts will again apply the reasonableness standard in making a determination. What would a reasonable person have understood the scope to be under those conditions?

The party granting consent may set forth restrictions on the search. Should that be the case, officers must abide with this request. To do otherwise could very well result in the suppression of any evidence recovered.

MORE ADVANCED

CONSENT FORMS

In searches that hinge on consent, it often comes down to one side's word over the other. What exactly was said, how it was said, and what the suspect understood at the time could all be scrutinized. A well-crafted consent-to-search form will go a long way in countering any attack on the search. The form should include details specifically relating to digital evidence. The form should seek permission to search not just computers but any storage media, including cell phones, manuals, printers, and more. The form should ask for permission to take these items from the location for offsite examination (Executive Office for United States Attorneys, 2009).

In the end, it's important to remember that consent searches can be highly nuanced and heavily dependent on the facts or circumstances that arise during that specific incident. While searching without a warrant is sometimes a necessity, the best practice is to get a search warrant whenever possible. Your case will rest on much more solid ground with a warrant than without.

Third parties can sometimes consent to the search of private property. Roommates, spouses, and parents are just a few of the examples. Normally, if a device is

shared, all parties have the authority to provide consent to search its common areas. In this situation, none of them would have a reasonable expectation of privacy in the common areas, since the device is shared with other people. The notion of common areas is significant. Areas such as those that are password-protected would not qualify as common areas. The third party would not be likely to have the authority to consent to a search of those areas. However, if the suspect has shared the password with the third party, then this constraint no longer applies. The suspect's reasonable expectation of privacy has been greatly diminished.

It's foreseeable that, in the end, the third party in question really didn't have the authority to consent. This is not necessarily a deal breaker as far as the admissibility is concerned. Officers in the field can only do what a reasonable person would do when determining a third party's legal ability to provide consent. If the suspect is present at the scene, a third party is not permitted to grant consent.

Spouses, under normal circumstances, can consent to the search of common areas. Parents may or may not be able to provide consent to search a child's property. If the child in question is younger than eighteen years of age, parents are generally permitted to give consent. If the child is over age eighteen, it gets a bit more complicated. Factors that will affect this determination include the child's age, whether or not the child pays rent, and what steps (if any) the person has taken to restrict access.

Technicians are often in the position of uncovering evidence during the course of their work. The courts have been split when deciding if the technician has the authority to consent. Officers may recreate the technician's search or observe them retrace their steps. Officers may not, however, expand the technician's search or direct the technician to look deeper. Should a technician locate evidence, those findings are normally used as the basis for a search warrant.

Exigent circumstances arise from time to time requiring the immediate seizure and possible search of a digital device. This is generally permitted under one of these three conditions: The evidence is under imminent threat of destruction, a threat puts law enforcement or the public in general in danger, or the suspect is expected to escape before a search warrant can be acquired. This exception may apply to the seizure of an item or device, but not automatically to the search of it. Once the item has been seized (secured), the exigency may no longer exist, thus requiring a search warrant to continue.

Officers have the right to charge suspects with evidence they see if the officers are legally permitted to be where they are, and if the item is immediately apparent to be incriminating. This is known as the "plain view doctrine." This situation typically arises in a digital forensic context when an examiner is analyzing a drive for evidence of one crime and finds evidence of a completely different one. For instance, an examiner searching a hard drive for photos of stolen artwork comes across images of child pornography. At this juncture, the search should cease until a separate warrant pertaining to the possession of child pornography can be obtained.

Border searches and searches by probation and parole officers are afforded much more latitude than those conducted by police officers. From the court's perspective, individuals entering the country can be searched with probable cause or even

reasonable suspicion. The court recognizes the government's need to secure the border from contraband and like material. Those individuals on probation or parole have less of an expectation of privacy than other citizens. For example, sex offenders may be prohibited from using the Internet during their supervised release. This stipulation would permit the parole or probation officer the authority to search the offender's computer at any time to ensure compliance. There is even some case law permitting this type of search without these specific conditions in place.

Employees in the workplace may or may not possess a reasonable expectation of privacy on their work computers. This expectation will vary depending on the facts, including whether the employee is a government employee. Normally, officers can search an employee's computer without a warrant if the employer or another co-worker (with shared authority) gives permission. Government employees are looked at a bit differently. That's not to say that employers can't search the employee's system; it just means that the search must be "work-related, justified at their inception, and permissible in scope" (Executive Office for United States Attorneys, 2009).

ALERT!
CELL PHONE SEARCHES: THE SUPREME COURT WEIGHS IN

Can police officers peruse someone's text messages and photos after the person has been arrested? The U.S. Supreme Court has now answered that question, much to the disappointment of many police officers. Basic search-and-seizure law says that a warrantless search is only permissible when it falls within certain specified exceptions. One of these exceptions is a search incidental to a lawful arrest. Traditionally, if someone is lawfully arrested, police officers are permitted to search the arrestee's person and the area under the arrestee's immediate control (often described as the arrestee's "wingspan"). An arrestee's cell phone was often routinely searched based on this exception. That practice has now come to a screeching halt.

In *Riley v. California*, Riley was stopped after police observed him driving a car with expired registration tags. This traffic stop ultimately resulted in his arrest for weapons charges. Police then searched his cell phone incidental to his arrest and found other incriminating evidence. The evidence recovered from his cell phone led to further charges, as well as an enhanced sentence for gang membership.

Historically, the search of an area under a suspect's immediate control was justified for two basic reasons: officer safety and preventing evidence from being destroyed. The U.S. Supreme Court rejected both of those reasons in this case. In addressing the safety issue, the court said that "Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape" (*Riley v. California*, 2014). While the concern for the destruction of evidence is a little more realistic, it still wasn't enough to justify a search without a warrant. In rejecting this rationale, the court noted, "law enforcement currently has some technologies of its own for combatting the loss of evidence."

The court also went on to compare the intrusion of privacy represented by a search of someone's physical possessions and that of a search of the person's cell phone. A search of the items found in an arrestee's pocket constitutes a "narrow intrusion on privacy." That cell phone is a new matter entirely. Cell phones contain massive amounts of various types of data. This data represents a "digital record of nearly every aspect of their lives." The good news for law enforcement is that this treasure trove of potential evidence isn't "immune from search" as the court says. Law enforcement officers will just need a warrant before the search of a phone can begin.

SEARCHING WITH A WARRANT

Absent one of the well-defined exceptions described here, police officers must have a search warrant before searching someone's private property, including a computer.

A search warrant is an order that is obtained by a law enforcement officer from a judge, granting them permission to search a specific place and seize specific persons or things.

A judge will issue the warrant when he or she believes that there is probable cause that a crime was committed and that the people or things specified in the warrant will be found at that location. The Supreme Court said that probable cause is established when there is "a fair probability that contraband or evidence of a crime will be found in a particular place" (*Illinois v. Gates*, 1983). Another way to look at this is whether the items or persons to be seized will be more likely than not to be found at that specific location. Mathematically, this would equate to a probability of 51 percent.

When applying for a warrant, it's helpful to determine the role of the computer in the crime. The computer can be considered contraband if it contains child pornography or is stolen property. The computer can also be used to store evidence, such as incriminating documents. Finally, the computer can serve as a tool or instrumentality of the crime. This is the case when the computer is used to hack into a company's network, for example.

SEIZE THE HARDWARE OR JUST THE INFORMATION?

We know from the Fourth Amendment that a search warrant must "particularly describe the place to be searched and the person or things to be seized." To effectively meet that requirement, we first need to understand precisely what we need to seize. In short, is it the hardware or the information held by the hardware? If the computer is contraband, evidence, or fruits or instrumentalities of a crime, then we need to establish probable cause to seize the hardware. Otherwise, our focus is on the information alone.

PARTICULARITY

Courts frown heavily on overly broad affidavits that lack the particularity mandated by the Fourth Amendment. Affidavits should make it clear what items can be seized

and what can't. "Particularly" describing things that you likely have never seen may seem like an impossible task. It's really not. Serial numbers and the like are not required.

Here is some sample language I recommend that could be used:

> *"Any and all personal computer(s)/computing system(s) located at the residence of (INSERT ADDRESS HERE), to include input and output devices, electronic storage media, computer tapes, scanners, disks, diskettes, optical storage devices, printers, monitors, central processing units, and all associated storage media for electronic data, together with all other computer-related operating equipment and materials."*

Describing the information can be done in a somewhat similar fashion. Although we probably don't know the file names, for example, it's quite possible that we would know the suspect's name, the time period, and the specific crime that's being investigated. The courts are looking for some type of limiting language. Asking for "any and all files" on a suspect's hard drive stands a very good chance of being deemed overly broad, resulting in the suppression of any evidence found.

ESTABLISHING NEED FOR OFFSITE ANALYSIS

The forensic analysis of a hard drive can be a very time-consuming process. For a variety of reasons, this is best done at the lab or police station. For all intents and purposes, doing this at the scene contemporaneously with the search should not be the first option. The search warrant affidavit should spell out, in clear terms, the logic and need for this practice. Reasons can include the amount of time and data involved and potential use of anti-forensic techniques, as well as the need to perform this task under the more controlled conditions (like those found in the lab). This is one way to make this point in an affidavit:

> *"Computer storage devices (like hard disks or CD-ROMs) can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search [onsite].*
>
> *"Technical requirements. Searching computer systems for criminal evidence sometimes requires highly technical processes requiring expert skill and [a] properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search processes are exacting scientific procedures designed to protect the integrity of the evidence and*

to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis" (Executive Office for United States Attorneys, 2009).

STORED COMMUNICATIONS ACT

The Stored Communications Act (SCA), enacted in 1986, provides statutory privacy protection for customers of network service providers. The SCA controls how the government can access stored account information from entities such as Internet Service Providers (ISPs). This account information typically includes e-mail, as well as subscriber and billing, information. Specifically, the SCA lays out the process that state and federal law enforcement officers must adhere to so they can force disclosure of these records by the provider.

The SCA seeks to codify the type of information sought, privacy expectations associated with it, and legal instrument required for the government to access it. The SCA breaks down service providers into two separate and distinct groups: "electronic communication service" providers and those organizations that provide "remote computing services." Understanding these differences is essential to deciphering the SCA and its legal requirements.

According to the SCA, specifically 18 U.S.C. § 2510(15), an electronic communication service (ECS) provider is "any service which provides to users thereof the ability to send or receive wire or electronic communications." ECS examples would include companies that deliver telephone and e-mail services (Executive Office for United States Attorneys, 2009). America Online comes to mind, as does Hotmail. It may surprise you to know that any company, no matter what its focus, can qualify as an ECS.

Title 18 U.S.C.§ 2711(2) defines a remote computing service (RCS) as "the provision to the public of computer storage or processing services by means of an electronic communications system." Put another way, an RCS is provided by an "[offsite] computer that stores or processes data for a customer" (Executive Office for United States Attorneys, 2009).

The SCA also addresses the variety of information these providers store. This can include basic subscriber information like name, address, and credit card number. Other potential information includes logs and opened, unopened, draft, and sent e-mails.

ELECTRONIC DISCOVERY

The Sedona Conference defines e-Discovery as "The process of collecting, preparing, reviewing, and producing electronically stored information ("ESI") in the context of the legal process" (Sedona, 2007).

Digital evidence is alive and well in civil cases. Parties involved in litigation need to review all of the potentially relevant data, as well as any data that may have to be disclosed to the opposing party. Common means of discovery include interrogatories, depositions, and requests for document production (Sedona, 2007). Electronically stored information (ESI) presents some challenges that paper records do not. For example, ESI is easily modified, volatile, and easily duplicated and dispersed. For these reasons, the rules of evidence for both state and federal courts are changing to specifically address ESI.

DUTY TO PRESERVE

Evidence that was once confined to paper memos and filing cabinets is now found in Microsoft Word documents and backup tapes. Digital evidence is significantly different from the paper-based evidence that so many lawyers were accustomed to dealing with. For example, digital evidence is far more volatile and easier to alter or destroy. Volume is another key difference. There can be such a mind-boggling amount of data in a case that it can cost millions of dollars just to produce and review them.

In December 2006, the federal courts took the first substantive step in addressing and dealing with digital evidence by changing the Rules of Civil Procedure. These rule changes mandate that opposing attorneys work together to deal with the ESI in a case very early in the process. Addressing ESI early in a case reduces costs, time, and the chance of relevant evidence being overlooked. Not all lawyers and judges have embraced these changes. Like many folks, some lawyers and judges are very uncomfortable with technology, even going as far as to have someone else check and then print out their e-mail.

Zubalake v. USB Warburg was a series of landmark electronic discovery cases. Judge Shira Scheindlin's rulings addressed many of the fundamental concerns in cases that involve ESI. Some of the concerns included the duty to preserve electronic data, a lawyer's duty to oversee a client's compliance with these guidelines, data sampling, cost shifting, and sanctions. (Zubalake v. USB Warburg, 2003).

The duty to preserve potentially relevant data begins when there is a "reasonable anticipation of litigation." Failing to recognize this trigger and take action can result inspoliation of the evidence and potentially severe sanctions to boot. Like other legal standards addressed in this chapter, defining a reasonable anticipation of litigation can be difficult; quite difficult, in fact. The duty to preserve is not caused only by the arrival of a subpoena. It's very likely that the duty kicked in well before that time. Duty to preserve is a very fact-specific determination that will vary from case to case. The firing of a disgruntled employee could be enough to trigger it; likewise, so could an accusation of sexual harassment by an employee against a supervisor.

Judge Scheindlin also addressed a lawyer's duty to oversee a client's attempts to identify, preserve, collect, and produce potentially relevant evidence. She said, in part, "Counsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched. (Zubalke v. USB Warbur, 2003)" Furthermore, she said that the attorney should draft and distribute a "litigation hold"

that directs a company and its employees to protect the relevant data and ensure they're not destroyed or compromised in any way.

Data sampling is a way to test a large collection of ESI for the "existence or frequency of relevant information" (Sedona, 2007). The volume of potentially relevant data can be staggering, especially in a large corporate environment. Data sampling is one of the best ways to save time and reduce costs during the e-Discovery process.

The costs incurred during the e-Discovery process can be massive, rising into hundreds of thousands or even millions of dollars. Typically, in traditional discovery, the producing party bears the cost of production. Under certain conditions, the costs of production may be shifted to the requesting party. In the *Zubalake* case, Judge Scheindlin addressed this concern and devised a seven-factor test to be used to determine if cost shifting is warranted. (Zubulake v. USB Warburg, 2003).

The seven factors are "(1) the extent to which the request is specifically tailored to discover relevant information; (2) the availability of such information from other sources; (3) the total cost of production compared to the amount in controversy; (4) the total cost of production compared to the resources available to each party; (5) the relative ability of each party to control costs and its incentive to do so; (6) the importance of the issue at stake in the litigation and; (7) the relative benefits to the parties of obtaining the information" (*Zubulake v. UBS Warburg*, 2003).

PRIVATE SEARCHES IN THE WORKPLACE

It's not uncommon for work computers to be the subjects of searches for criminal, civil, or administrative actions. From the private side, employers have a fair bit of latitude to search an individual's company computer. A company computer use policy that clearly spells out that work computers, e-mail, and so on are for work purposes only and that they may be searched at any time is an accepted best practice. For Fourth Amendment purposes (law enforcement or its agents), a work computer can be searched with consent of a supervisor or another employee as long as that person has common authority over the area to be searched. It is also important to note that federal privacy statutes and the Stored Communications Act may come into play as well.

In the end, consult with the prosecuting attorney or corporate/in-house counsel for guidance. Getting their input can help ensure that the case is on the strongest legal footing (Executive Office for United States Attorneys, 2009)

ALERT!
INTERNATIONAL e-DISCOVERY

With the cloud environment and data regularly flying across borders, international electronic discovery is becoming an issue. Not every country has the same views on privacy or the same legal standards and procedures for discovery. As a result, gaining access to data in a foreign country is very complex. The Sedona Conference's

Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery is an excellent introduction to the complexities involved in international e-Discovery. You can download it for free from http://www.thesedonaconference.org/.

EXPERT TESTIMONY

As a digital forensic examiner, you must be prepared to testify in court as an expert witness as to your findings and procedures. What's the difference between a witness and an expert witness? A major difference is that a qualified expert witness can give an opinion, but a "regular" witness can't.

Determining whether or not an individual is an expert is a matter for the court to decide. An expert doesn't have to have a Ph.D or other lofty credentials. FindLaw defines an expert as someone "who by virtue of special knowledge, skill, training, or experience is qualified to provide testimony to aid the factfinder in matters that exceed the common knowledge of ordinary people" (FindLaw).

Under this definition, bakers, tailors, accountants, medical doctors, and school bus drivers could be qualified as experts. Certainly credentials help, but they are not a requirement.

Two cases form the foundation for the admissibility of expert testimony. The first is a 1923 case, *United States v. Frye* (1923). The *Frye* case centered on the admissibility of new lie-detection technology. Out of this case came what became known as the "Frye Test." The test said that "the results of scientific tests or procedures are admissible as evidence only when the tests or procedures have gained general acceptance in the particular field to which they belong" (*United States v. Frye*, 1923).

Eventually, the Frye Test fell by the wayside. In *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), the U.S. Supreme Court ruled that the Federal Rules of Evidence superseded the Frye Test. Merrell Dow Pharmaceuticals Inc. was sued by plaintiffs who claimed that its drug, Bendectin, had caused significant birth defects. The lower court granted Merrell Dow's request for summary, citing that the scientific evidence presented by the plaintiff had not yet gained approval within the scientific community. The Supreme Court agreed.

In *Daubert* (1993), the court said that the admissibility should be evaluated on "whether the testimony's underlying reasoning or methodology is scientifically valid and properly can be applied to the facts at issue. Many considerations will bear on the inquiry, including whether the theory or technique in question can be (and has been) tested, whether it has been subjected to peer review and publication, its known or potential error rate and the existence and maintenance of standards controlling its operation, and whether it has attracted widespread acceptance within a relevant scientific community" (Daubert, 1993).

Understanding this groundwork will help examiner sbetter comprehend the admissibility of their testimony within the context of the law.

ADDITIONAL RESOURCES

EXPERT TESTIMONY

Fred Smith and Rebecca Bace's book on expert testimony, *A Guide to Forensic Testimony: The Art and Practice of Presenting Testimony as an Expert Technical Witness*, contains a tremendous amount of practical information. One of the best aspects of the book is that it is written for information technology experts. The book covers the topic well and is quite readable. (Smith, F. and Bace, R., 2002).

SUMMARY

Proper search authority is a necessary first step in the forensic examination process. Evidence collected without it is very likely to be excluded. The Fourth Amendment to the U.S. Constitution protects citizens from unreasonable searches and seizures. The protections afforded by the Fourth Amendment only cover actions by the government. It does not apply to private citizens acting on their own. Law enforcement can search and seize digital evidence with and without a search warrant. Searches with a warrant are always better, from a legal standpoint, than searches without one. That said, exigent circumstances can and do arise that would permit officers to do otherwise.

On the private side, supervisors and employers are likely to have broad authority to search company computers, especially if the employee read and signed a computer usage agreement clearly stating that the company computers, e-mail, and so on could be searched at any time.

Consulting with the appropriate legal counsel before searching or seizing digital evidence is never a bad idea. If you have questions or concerns, those should always be raised in advance.

REFERENCES

Daubert v. Merrell Dow Pharmaceuticals Inc., 1993. 509 U.S. 579. Retrieved from: <www.caselaw.lp.findlaw.com/scripts/getcase.p1?court=us&vol=509&invol-579.com> (accessed 09.14.11.).

Executive Office for United States Attorneys, 2009. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Office of Legal Education. United States Department of Justice, Washington, DC.

FindLaw, 2011. Fourth Amendment—Search and Seizure. Retrieved from: <http://caselaw.lp.findlaw.com/data/constitution/amendment04/> (accessed 11.10.11.).

Frye v. United States, 1923. 293 F. 1013. DC Cir. Retrieved from: <www.law.ufl.edu/_pdf/faculty/little/topic9.pdf> (accessed 11.10.11.).

Illinois v. Gates, 1983. 462 U.S. 213, 238. Retrieved from: <www.casebriefs.com/blog/law/criminal-procedure/criminalprocedure-keyed-to-isreal/arrest-search-and-seizure/illinois-v-gates-2/> (accessed 11.10.11.).

Riley v. United States, 2014. 573 US. Retrieved from: <https://supreme.justia.com/cases/federal/us/573/13-132/> (accessed 11.10.11.).

Sedona Conference, 2007. The Sedona Conference Glossary: E-Discovery & Digital Information Management, second ed. Sedona Conference, Sedona, AZ.

Smith, F., Bace, R., 2002. A Guide to Forensic Testimony. The Art and Practice of Presenting Testimony as an Expert Technical Witness Pearson Education, Boston, MA.

TechTarget, 2005. Electronic Discovery. Retrieved from: <http://searchfinancialsecurity.techtarget.com/definition/electronic-discovery> (accessed 11.11.11.).

U.S. Department of Justice, Office of Justice Programs, 2010. Privacy and Civil Liberties. Retrieved from: <http://www.justice.gov/opcl> (accessed 10.10.11.).

United States v. Megahed, 2009. WL 722481, at *3. MD Fla. Mar. 18, 2009. Retrieved from: <http://fl.findacase.com/research/wfrmDocViewer.aspx/xq/fac.20090318_0000634.MFL.htm/qx> (accessed 11.11.11.).

United States v. Slanina, 2002. 283 F.3d 670, 680. 5th Cir. Retrieved from: <http://openjurist.org/283/f3d/670/united-states-v-slanina-j> (accessed 11.11.11.).

United States v. Walser, 2001. 275 F.3d 981, 986. 10th Cir. Retrieved from: <http://leagle.com/decision/20011256275F3d981_11155.xml/U.S.%20v.%20WALSER> (accessed 11.11.11.).

www.wisdomquotes.com/authors/thomas-jefferson/.

Zubulake v. UBS Warburg, 2003. 217 F.R.D. 309. S.D.N.Y. Retrieved from: <http://www.casebriefs.com/blog/law/civil-procedure/civil-procedure-keyed-to-friedenthal/pretrial-devices-of-obtaining-information-depositions-and-discovery-civil-procedure-keyed-to-friedenthal-civil-procedure-law/zubulake-v-ubs-warburg-llc/> (accessed 11.11.11.).

CHAPTER

Labs and tools

3

"Data! Data! Data!" he cried impatiently. "I can't make bricks without clay."
—Sherlock Holmes in *The Adventure of the Copper Beeches*

INFORMATION IN THIS CHAPTER:

- The Role and Organization of Forensic Laboratories
- The Purpose of Policies and Procedures in Forensic Laboratories
- The Role of Quality Assurance in Forensics
- Digital Forensic Hardware and Software
- Accreditation versus Certification

INTRODUCTION

In this chapter, we will explore the different types of laboratory setups, as well as the hardware and software tools in common use in digital forensics. We'll also take a look at Standard Operating Procedures and Quality Assurance, two critical components of an effective digital forensic lab. Obtaining and maintaining laboratory accreditation, although time-consuming and expensive, greatly improves a lab's performance and the quality of its findings. Examiner certification ensures that the skill of a lab meets a minimum level. At the end of the day, these elements come together to ensure that only valid and reliable results are produced and that justice is served.

FORENSIC LABORATORIES

Forensic labs are scattered throughout the United States and closely follow the jurisdictional lines of law enforcement (local, county, state, and federal) (James and Nordby, 2009). The majority of these facilities are run by law enforcement agencies. The FBI's crime laboratory in Quantico, Virginia, has the distinction of being the largest forensic lab in the world (Saferstein, 2006).

Not all computer forensic examinations are conducted in what would be considered a traditional laboratory setting. Many agencies conduct them locally at their departments if they have the necessary equipment and trained personnel on hand.

Digital forensics isn't cheap, so not every agency can afford to train and equip its own examiners. One response to this ever-growing demand is the Regional Computer

Forensic Laboratory (RCFL) program started by the FBI. The RCFL program runs sixteen facilities throughout the United States. They provide digital forensic services and training to all levels of law enforcement. Each RCFL is staffed and managed by a partnership of local, state, and federal law enforcement agencies.

The RCFL program is a great success, and is making a significant dent in the backlog of digital forensic examinations across the country. During fiscal year 2010, RCFLs nationwide performed 6,564 forensic examinations and processed a whopping 3,086 terabytes of data. To put that in context, the 2010 RCFL Annual Report explains it this way: "One single terabyte is equivalent to 1,024 gigabytes or approximately 1,000 copies of the Encyclopedia Britannica." Doing the math, that's about 3,086,000 encyclopedias. The RCFLs process a wide variety of digital devices and media, including smartphones, hard drives, Global Positioning System (GPS) units, and flash drives. In 2010, RCFL examiners helped convict rapists, terrorists, and crooked politicians (FBI, 2010).

VIRTUAL LABS

Digital labs don't have to be confined to a single location. Today's technology makes it possible to run a "virtual" lab with the examiners and the central evidence repository located in geographically separate locations. This arrangement has several advantages, including cost savings, greater access to more resources (tools and storage, for example), access to diverse and greater expertise, and reduction of unnecessary duplication of resources (Craiger, 2008).

This virtual arrangement allows for distinct role-based access. For example, full access could be granted to examiners and laboratory management. Prosecutors, investigators, and defense attorneys would have restricted access. This restricted access would limit what those folks could see and what they could do (read only, etc.) (Whitcomb, 2011).

There are some considerable concerns with this approach:

1. **Security**—The security of the system must be robust enough to maintain the level of evidence integrity required by the courts. Otherwise, there could be catastrophic consequences, such as rendering evidence from multiple cases inadmissible.
2. **Performance**—For this scheme to work, connectivity must be both speedy and reliable. No connection or a slow connection will quickly affect the organization's ability to function.
3. **Cost**—Startup costs in particular are substantial and potentially beyond what many agencies can afford (Whitcomb, 2011).

LAB SECURITY

Lab security is always a major concern. Access to evidence and facilities must be strictly managed. Stringent security plays a key role in maintaining the integrity of the digital evidence that passes through the laboratory. Only authorized, vetted

personnel should have access to critical areas such as examination stations and evidence storage. Unauthorized individuals are usually kept out by using doors and other physical barriers, along with controls such as keys, swipe cards, and access codes. Digital solutions such as swipe cards and access codes offer an advantage over older methods such as keys. Electronic methods provide a ready-made audit trail that can be used in support of the chain of custody. Security is further enhanced with alarm systems and the like.

Unauthorized access isn't the only threat to the evidence. The risks of fire, flooding, and other natural disasters also must be addressed.

The chain of custody continues at the lab, as does the paperwork. In the lab, the evidence must be signed in and out of the evidence storage area for examinations and court. This log must be completed each and every time the evidence is removed or returned to the evidence room or vault. This check-out and check-in process can be done the old-fashioned way with pen and paper or electronically with scanners and bar codes.

Just like in the field, network access to evidence in the lab is also a concern. This is true for both the Internet and the lab's own computers. Best practice tells us that the machine used to perform the examination should not be connected to the Internet. Removing this connection removes the argument that the evidence was somehow compromised by someone or something (malware, for example) via the Internet. Virtual labs will have to be able to articulate how the integrity of their evidence is maintained, given the nature of their operations.

Malware (viruses, worms, and the like) could be hiding on any evidence drive brought in for examination. Connecting it in some manner to an internal network poses a major risk to not only the lab's computers but evidence from other cases as well. To mitigate the risk, these drives should be scanned for viruses by at least one antivirus tool before examination.

EVIDENCE STORAGE

When the evidence is not actively being examined, it must be stored in a secure location with limited access. One of the best solutions is a data safe. These safes come in multiple sizes and are specifically designed to protect digital evidence from theft and fire. Some types of digital media are very vulnerable to heat (tape, for example). A data safe can keep the media at an acceptable temperature long enough (ideally) for a fire to be extinguished.

Evidence storage locations must be kept locked at all times when not actively being used. A log or audit trail should also be maintained, detailing who entered, when they entered, and what they removed or returned.

Access to evidence storage and other sensitive areas can be controlled by a variety of means, including pass codes and key cards. Electronic controls have some distinct advantages over keys. One significant advantage is the ability to log each and every time an individual accesses a restricted area. This audit trail can be very helpful in monitoring and verifying the chain of custody.

POLICIES AND PROCEDURES

How the lab handles evidence, conducts examinations, keeps records, and secures its facility should not be left to chance or the whims of any one individual. These tasks should be governed by policies and Standard Operating Procedures (SOPs). SOPs are documents that detail, among other things, how common forensic examinations should be performed. The art in writing SOPs lies in finding the right balance between being too narrow or overly broad. If too specific, the SOP will lack the flexibility needed to address any unusual conditions that may arise. In digital forensics, these situations occur far more often than we'd like. If too broad, they can be ineffective in keeping information consistent and ensuring the integrity of the evidence.

There are inherent dangers in not following your organization's policies and SOPs. Odds are that questions about your organization's policies and SOPs will come up during cross-examination should the case go to court.

QUALITY ASSURANCE

In the early 1980s, the Ford Motor Company told us that "Quality is Job 1." You may not believe that today in regard to Ford, but it's most assuredly true in regard to forensic science.

Quality assurance (QA) is a bedrock principle that underpins every discipline in forensic science. As such, every lab should have a QA program. Quality assurance is defined as "a well-documented system of protocols used to assure the accuracy and reliability of analytical results" (James and Nordby, 2009). A good QA program will cover a wide array of subjects, including peer reviews of reports, evidence handling, case documentation, training of lab personnel, and more (James and Nordby, 2009).

The review process can be divided into two discrete types: a technical review and an administrative review.

- The technical review, conducted by a separate examiner, focuses on the results and conclusions. The central question in a technical review is "Are the results reported by the original examiner supported by the evidence in the case?"
- In contrast, the focus of an administrative review is ensuring that all of the paperwork is present and has been completed correctly.

An examiner's competency must be confirmed and documented on a regular basis. In the forensic community, this is known as proficiency testing. In a proficiency test, examiners must demonstrate their competence with mock evidence. There are four types of proficiency tests:

1. **Open test**—The analyst(s) and technical support personnel are aware they are being tested.
2. **Blind test**—The analyst(s) and technical support personnel are not aware they are being tested.
3. **Internal test**—The test is conducted by the agency itself.

4. **External test**— The test is conducted by an agency independent of the agency being tested (SWGDE, 2010).

These tests may be conducted in-house with other lab personnel. These results must be documented because, at some point, the analyst's skills and abilities may be called into question during a court proceeding. This documentation will be critical should that happen.

The case of Glen Woodall, although concerning DNA, is a powerful example of the need for quality assurance. On July 8, 1997, Woodall was convicted by a Cabell County, West Virginia, jury of the brutal sexual assault of two women. He was summarily sentenced to two life terms with an additional sentence of 203 to 335 years in prison (The DNA Initiative). The arrest and conviction of Woodall brought some much-needed closure to both of the victims and peace to the community as a whole. Unfortunately for the victims and community, though, the relief didn't last long.

The forensic scientist in this case was West Virginia State Police serologist Fred Zain. After an investigation into Zain's work in both West Virginia and Texas, he was charged with perjury and tampering with evidence (Chan, 1994). During the investigation, it was found that Woodall was innocent, and that he, too, was a victim. After serving four years in a West Virginia prison, Woodall was released and awarded (1 million from the state for his wrongful imprisonment.

What the panel found was extremely disturbing. They discovered that Zain "fabricated or altered evidence and lied about academic qualifications under oath." That's not all. The panel also found that his supervisors may have been culpable as well, by overlooking or hiding complaints about his performance (Chan, 1994).

In 2011, 24 years later, the real suspect was arrested and eventually convicted of the crimes of which Woodall was originally found guilty. On April 1, Donald Good was sentenced to more than 200 years in prison (WSAZ-TV, 2011). Cases like this hammer home the need for effective quality assurance programs in all forensic sciences.

TOOL VALIDATION

Our tools, be they hardware or software, must function as they are designed. Each and every tool must be validated before it's used on an actual case. A validation process clearly demonstrates that the tool is working properly, is reliable, and yields accurate results. We can't simply accept the manufacturer's word for it; assumptions aren't permitted.

The validation process is another one of those aspects of our work that has to be committed to paper. To do otherwise will put any evidence in real jeopardy of being excluded.

DOCUMENTATION

The importance of complete and accurate documentation can't be overstated. The old saying that "if you didn't write it down, it didn't happen" are truly words to live by in this industry. Different types of documentation and reports are used

throughout the entire forensic process. These should be spelled out in the labs' or agencies' SOPs and policy manuals. Submission forms, chain of custody records, examiner's notes, and the examiner's final report form the crux of the required documentation.

Normally, all the paperwork associated with a specific case is collected into a case file. The case file will contain all of the documentation pertaining to the case, including paperwork generated by the examiner and others. Usually, these include case submission forms, requests for assistance, examiners' notes, crime scene reports, case reports, copy of the search authority, chain of custody, and so on (NIJ, 2004).

Forms

Preprinted forms are widely used in both the field and the lab. They help guide personnel through the process and ensure that a high level of quality is maintained. Forms ensure that all necessary information is captured in a uniform manner. Typically, forms are used to describe the evidence in detail (make, model, serial number, etc.), document the chain of custody, request an examination, and so on.

Examiner notes

Examiner's notes cover most, if not all, of the examiner's actions and observations, along with corresponding dates. They must be detailed enough to enable another examiner to duplicate the process used during the examination. Elements typically recorded here include:

- Discussions with key players, including prosecutors and investigators.
- Irregularities found and associated actions taken.
- Operating systems, versions, and patch state(s).
- Passwords.
- Any changes made to the system by lab personnel and of law enforcement (NIJ, 2004).

If you've ever worked in the legal system, you know that the wheels of justice can turn very, very slowly. This applies to both criminal and civil cases. It can be months or even years before a case ever gets to trial. By the time you have to testify, you may only be able to recall few, if any, facts of the case. The case documentation, and your notes in particular, will prove a great tool to refresh your recollection.

Examiner's final report

The examiner's final report is the formal document that is delivered to prosecutors, investigators, opposing counsel, and so on at or near the end of an investigation. These reports typically consist of:

- Identity of the reporting agency.
- Case identification number/submission number.
- Identity of the submitting person and case investigator.
- Dates of receipt and report.

- Detailed description of the evidence items submitted, including serial numbers, makes, models, and so on.
- Identity of the examiner.
- Description of the steps taken during the examination process.
- Results and conclusions (NIJ, 2004).

When drafting the final examiner's report, it's critical to take into account the intended audience, which is primarily laypeople. The lawyers, investigators, judges, and clients will most likely have little to no technical background. All too often, these reports are filled with technical jargon and details that only serve to frustrate and confuse the majority of their intended audiences. These reports should be comprehensible to a nontechnical audience. Jargon and acronyms should be kept to an absolute minimum.

Two major sections of the examiner's report are the summary and the details of the findings. The summary is a brief description of the results of the examination. The end users of our reports find this feature useful, especially in light of the massive caseload and amount of information they are typically dealing with. The findings included here should be supported and explained in the detailed findings.

The detailed findings provide the substance of the report. They provide the details of the examination, steps taken, results, and so on. Typically, you may find details relating to:

- Files directly pertaining to the request.
- Files that support the findings.
- E-mail, web caches, chat logs, and so on.
- Keyword searches.
- Evidence of ownership of the device (NIJ, 2004).

A glossary is a helpful addition to an examiner's report. Anything we can do to help our intended audience wade through any unfamiliar jargon and acronyms is always a good thing. Conveying our findings in a way that can be understood is our responsibility as forensic professionals.

DIGITAL FORENSIC TOOLS

Digital forensic tools make our work much more efficient—or even possible. There are tools for specific purposes as well as tools with broader functionality. They can come in the form of both hardware and software. They can be commercial tools that must be purchased or they can be open source items that are freely available. There are advantages and disadvantages to all. Keep in mind that no single tool does everything or does everything exceedingly well. For that reason, it's a good practice to have multiple tools available. Using multiple tools is also a great way to validate your findings. Obtaining the same results with two different tools significantly increases the reliability of the evidence.

TOOL SELECTION

The digital forensic tool market boasts a large number of products, with more rolling out all the time. How does an examiner know which tools are reliable and which ones are not? How should these tools be validated? The National Institute of Standards and Technology (NIST) and the National Institute of Justice (NIJ) have taken a big step in helping to answer these and other questions.

NIST has launched the Computer Forensic Tool Testing Project (CFTT), which establishes a "methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware" (NIST, 2011).

Let's explore what this looks like. This is an excerpt from the NIST test of a Tableau brand hardware write-blocking device (HWB), summarizing some of the test criteria and results:

> *"An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device."*
> *"For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive."*
> *"An HWB device shall return the data requested by a read operation."*
> *"For all test cases run, the device always allowed commands to read the protected drive."*
> **(NIJ, 2009)**

Each tool, be it hardware or software, must be validated before it is used on casework as well as anytime it is modified or updated. For example, like other software you're familiar with, our forensic software gets updated on a regular basis. After each update, the tool should be validated again. Validation also proves useful in court by supporting the validity of the tool's results.

HARDWARE

Many hardware tools out there are designed and built specifically for digital forensics. Some of these tools include cloning devices, cell phone acquisition devices, write blockers, portable storage devices, adapters, cables, and more.

As you might expect, digital forensics is heavily dependent on an assortment of hardware such as PCs, servers, write blockers, cell phone kits, cables, and so on. Figure 3.1 shows a well-equipped digital forensic workstation.

Computers are the backbone of any digital forensics lab, so, as an examiner, you will need the best computer workstation you can afford. Digital forensic exams require quite a bit of computing power. These jobs can tax even the best systems and crush those that don't measure up. A good exam machine has multiple, multicore processors; as much RAM as you can get (the more the better); and large, fast hard drives. Forensic software manufacturers provide detailed lists of minimum and suggested hardware requirements. Straying below the minimums is done at your own risk. To get a better understanding, let's look at the minimum and

FIGURE 3.1

One of the workstations in the West Virginia State Police Digital Forensics Lab at the Marshall University Forensic Science Center.

Courtesy of Cpl. Bob Boggs.

recommended system requirements (as of press time) for AccessData's Forensic Tool Kit (FTK).

AccessData's FTK has four distinct components and or applications. They are:

1. Oracle Database
2. FTK Client User Interface (UI)
3. Client-side Processing Engine
4. Distributed Processing Engine

The minimums and recommended specifications will vary with each component, but suffice it to say that you can never have too much RAM or computing power. For example, on a machine running the Oracle database, the FTK user interface, and the primary processing engine, AccessData recommends the requirements shown in Table 3.1.

Some components may be installed on separate machines. The minimum and recommended requirements will change depending on which configuration is used.

Examiners frequently sift through massive amounts of data. That means digital forensics labs need the capacity to store voluminous amounts of data. Browsing the PCs for sale on bestbuy.com shows that the majority have between 500 GB and 699 GB of hard drive space. Multiterabyte drives are also available. With numbers like these and caseloads ever increasing, it's easy to see that storage is a major concern.

Table 3.1 Basic Recommended Requirement (AccessData Group, LLC, 2011)

	Minimum	Recommended
Processor	Intel® i7 or AMD equivalent	Intel® i9 Dual Quad Core Xeon, i7 Nehalem or AMD equivalent
RAM	12GB (DDR3) 8GB (DDR2)	12GB (DDR3) 8GB (DDR2)
Operating System	Vista, 2008, Windows 7 (64 bit)	Vista, 2008, Windows 7 (64 bit)

Digital forensics is no longer a "PC-centric" endeavor. Small-scale devices such as cell phones and GPS units are pouring into labs across the country. These devices require different hardware from that used on laptops and desktops. Cellebrite's UFED supports more than 3,000 phones (Cellebrite Mobile Synchronization Ltd.). Paraben Corporation, a competitor of Cellebrite, boasts support for more than 4,000 phones, PDAs, and GPS units (Paraben Corporation).

When dealing with cell phones, having the proper cable is critical. Unlike PCs, mobile devices lack much of the standardization with regard to connectors and cables. Labs need a wide selection of cables on hand to cope with the vast array of handsets that walk through the doors. Fortunately, the manufacturers of mobile phone forensic hardware provide many of the required cables.

Several companies make hardware cloning devices. If you recall, a forensic clone is a bitstream copy of a particular piece of media such as a hard drive. These tools can really speed up the process, cloning multiple drives at once. They can also provide write protection, hash authentication, drive wiping, an audit trail, and more.

Other equipment

The hardware and software we discussed earlier are not the only equipment needed. Crime scene kits are very useful outside the lab. These kits are preloaded with all of the supplies an examiner would need in the field to collect digital evidence. Kits contain standard items such as pens, digital cameras, forensically clean storage media, evidence bags, evidence tape, report forms, permanent markers, gloves, and the like.

SOFTWARE

A wide array of digital forensic software products is on the market today. Some are general tools that serve a variety of functions. Others are more focused, serving a fairly limited purpose. These applications tend to focus on a very specific type of evidence, such as e-mail or Internet use.

When selecting software, a choice must be made between going with open source tools or a commercially produced product. There are advantages and disadvantages to both. Factors such as cost, functionality, capabilities, and support are some of the criteria that can be used to make this decision.

ADDITIONAL RESOURCES

OPEN SOURCE TOOLS

Cory Altheide and Harlan Carvey's book *Digital Forensics With Open Source Tools* is an excellent reference for those practitioners using these applications.

One of the more popular open source tools is the SANS Investigative Forensic Toolkit (SIFT). The SIFT Workstation is a powerful, free, open source tool. It's built on the Linux Ubuntu operating system. This tool is capable of file carving as well as analyzing file systems, web history, recycle bins, and more. It can analyze network traffic and volatile memory. It can also generate a timeline, which can be immensely helpful during an investigation. SIFT supports the following file systems:

- Windows (MSDOS, FAT, VFAT, NTFS)
- Mac (HFS)
- Solaris (UFS)
- Linux (EXT2/3/4)

(SANS Institute)

As for commercial tools, two of the most popular general software tools are Forensic Toolkit (FTK®) from AccessData and EnCase® from Guidance Software. Both are excellent and can make exams easier and more efficient. These applications have "Swiss Army knife"-like capabilities. They perform a multitude of tasks, including:

- Searching
- E-mail analysis
- Sorting
- Reporting
- Password cracking

The search tools in these products are particularly powerful, and give examiners the capability to drill down to precisely the information they are looking for. Here is a quick list of some of the information that can be searched for:

- E-mail addresses
- Names
- Phone numbers
- Keywords
- Web addresses
- File types
- Date ranges

As helpful as these tools can be, they do have some limitations. The reality is that no single tool does it all. For that reason, budget permitting, labs need to have a variety of tools available.

More and more specialty tools are coming on the market. These tools focus on one aspect of digital evidence, such as e-mail or web-based evidence. They can bring some additional capabilities to the table that some multipurpose tools don't.

ALERT!

DEPENDENCE ON THE TOOLS

Graphical User Interface (GUI)-based forensic tools can become a crutch. "Push-button" tools can make exams much more efficient, but they don't relieve the examiner of the responsibility to understand what's going on beneath the surface. Examiners need to understand not only what the tool is doing, but also how the artifact in question is created to begin with.

Some of the forensic tools that an examiner may use are listed in Table 3.2. Many of these companies offer video tutorials or demonstrations of their products. These

Table 3.2 Some hardware and software tools that may be found in a digital forensics laboratory

Tool	Use	URL
Forensic Toolkit Access Data Group, LLC	Multipurpose tool (acquisition, verification, searching, reporting, wiping, etc.)	http://accessdata.com
EnCase Guidance Software, Inc.	Multipurpose tool (acquisition, verification, searching, reporting, wiping, etc.)	http://www.guidancesoftware.com
SMART & SMART for Linux ASR Data, Data Acquisition and Analysis, LLC	Multipurpose tool (acquisition, verification, searching, reporting, wiping, etc.)	http://www.asrdata.com/forensic-software/
X-Ways Forensics X-Ways Software Technology AG	Multipurpose tool (acquisition, verification, searching, reporting, wiping, etc.)	http://www.x-ways.net/forensics/
Helix3 Pro e-fense, Inc.	Multipurpose tool (acquisition, verification, searching, reporting, wiping, etc.)	http://www.e-fense.com/products.php
Softblock, Macquisition, Blacklight BlackBag Technologies, Inc.	Multiple Macintosh forensic tools	https://www.blackbagtech.com/forensics.html
Mac Marshall Architecture Technology Corporation	Multiple Macintosh forensic tools	http://www.macmarshal.com/
Raptor Forward Discovery, Inc.	Linux-based acquisition and preview tool	http://www.forwarddiscovery.com/Raptor
Dossier Logicube, Inc.	Hardware acquisition	http://www.logicube.com/
Forensic hardware tools Tableau	Write blockers, bridges, storage, acquisition	http://www.tableau.com/
Wiebetech	Storage, write blockers, etc.	http://www.wiebetech.com/home.php

can be a great source of additional information. They are typically available from the manufacturer's website or on YouTube. This is in no way meant as an endorsement of a specific tool. These are only a representative sampling of the many tools that are available.

ACCREDITATION

Accreditation is an endorsement of a crime lab's policies and procedures—the way it does business, if you will (James & Nordby, 2009). The American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) is recognized as a world leader in the accreditation of forensic laboratories. Despite the name, ASCLD/LAB grants accreditation to labs both inside and outside the United States, which it has been doing since 1982 (Barbera, 2011a).

Based in Garner, North Carolina, ASCLD/LAB has accredited a total of 385 crime laboratories, 17 of those being outside the United States (ASCLD/LAB, 2011a).

According to ASCLD/LAB, its accreditation process has four objectives. They are to:

1. Improve the quality of laboratory services provided to the criminal justice system.
2. Develop and maintain criteria that may be used by a laboratory to assess its level of performance and to strengthen its operation.
3. Provide an independent, impartial, and objective system by which laboratories can benefit from a total operational review.
4. Offer to the general public and to users of laboratory services a means of identifying those laboratories that have demonstrated that they meet established standards (ASCLD/LAB, 2011b).

Think of ASCLD/LAB as the "Good Housekeeping Seal of Approval" for forensic science. Earning and maintaining an ASCLD/LAB accreditation is no easy chore. It requires an unbelievable amount of time, planning, documentation, and money. Nothing is taken for granted. Every standard met must be backed up with extensive, detailed documentation.

ASCLD/LAB offers two accreditation programs. The first is the legacy program and the second is the international program. The legacy program is the first program instituted by ASCLD/LAB. As you might expect, there are differences between the two programs as well as some common ground. A major difference is the number of criteria that must be met under each program. The international program has considerably more standards to meet than the legacy program. Labs seeking accreditation under the international program are required to fulfill the relevant requirements to demonstrate conformance to the applicable requirements of both the ISO/IEC 17025:1999(E) General Requirements for the Competence of Testing and Calibration Laboratories and the ASCLD/LAB-International Supplemental Requirements for the Accreditation of Forensic Science Testing and Calibration Laboratories.

James, S., Nordby, J.J., 2009. Forensic Science: An Introduction to Scientific and Investigative Techniques, third ed. CRC Press, Boca Raton, FL.

National Institute of Justice, 2004. Forensic Examination of Digital Evidence: A Guide for Law Enforcement. U.S. Department of Justice, Washington, DC.

National Institute of Justice, 2009. Test Results for Hardware Write Block Device: T4 Forensic SCSI Bridge. (FireWire Interface).

National Institute of Justice, U.S. Department of Justice, Office of Justice Programs. National Institute of Justice, Washington, DC.

National Institute of Standards and Technology, 2011. Computer Forensics Tool Testing Project Web Site: National Institute of Standards and Technology. Retrieved from: <http://www.cftt.nist.gov/index.html> (accessed 11.06.11.).

www.nij/gov/topics/justice-system/wrongful-convictions/Pages/dna-testing.aspx.

Saferstein, R., 2006. Criminalistics: An Introduction to Forensic Science, ninth ed. (College Edition). Prentice Hall, Upper Saddle River, NJ.

Scientific Working Group on Digital Evidence, 2010. Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence. Retrieved from: <http://www.swgde.org/documents/current-documents/> (accessed 11.08.11.).

Whitcomb, C.A., n.d. Virtual Digital Forensics Lab. National Center for Forensic Science, Largo, FL.

WSAZ-TV, 2011. UPDATE: Donald Good Receives Two Life Sentences in Mall Rape Case. Retrieved from: <http://www.wsaz.com/news/headlines/UPDATE_Judge_OHanlon_Will_Preside_Over_Huntington_Mall_Rape_Case.html> (accessed 11.11.11.).

www.astm.org.

www.paraben.com.

www.sans.org.

CHAPTER

Internet and e-mail

8

"The Internet is the crime scene of the 21st Century."
— Manhattan District Attorney Cyrus Vance, Jr.

INFORMATION IN THIS CHAPTER:

- Overview of the Internet and How It Works
- How Web Browsers Work and the Evidence They Can Create
- E-Mail Function and Forensics
- Chat and Social Networking Evidence

INTRODUCTION

In the beginning, the Internet was a little-known tool used by a few academics and the military. Today, it's truly a tool for the masses. We can order pizza, pay bills, look up a phone number, and take a class. For many of us, it is hard to imagine life without it. For examiners, its use can leave significant pieces of evidence scattered around that can persist for a long, long time. Web browsing, chat, e-mail, and social networking are just some of the technologies that we must understand in terms of how they're used, how they work, and where they leave traces.

INTERNET OVERVIEW

We'll begin with a quick introduction to the technology involved in getting your favorite web page to appear on your computer screen. Perhaps the best way is to track the process from start to finish. It all begins when someone enters a web address or Uniform Resource Locator (URL) into the address bar of a browser. A URL comprises three parts: the host, the domain name, and the file name. Let's use http://www.digitalforensics.com as an example.

In our example, "http" or Hypertext Transfer Protocol (HTTP) is the protocol used on the Internet to browse and interact with websites and the like. A protocol is nothing more than an agreed-upon way for devices to communicate with one another. Next is the domain name, "digital forensics" in this instance. Last is the Top Level Domain (TLD), ".com." It's called a TLD because it is at the top of the hierarchy that makes up the Internet's domain name system. Other TLDs include .org, .edu, and .net, just to name a few.

The browser, using the HTTP protocol, sends a "get" request to the web server hosting www.digitalforensics.com. A browser is an application that is used to view and access content on the Internet. There are several browsers to choose from; the most common are Microsoft's Internet Explorer, Mozilla's Firefox, and Google's Chrome.

After hitting Enter, the first order of business is to convert the domain name into an Internet Protocol (IP) address. The Internet functions with IP addresses. It can't do anything with the domain name itself. The domain name is for us, making it easier to remember the location of a website. A Domain Name Server (DNS) is responsible for mapping domain names to specific IP addresses. After the DNS makes the conversion, the request is then sent on to the server that's hosting the website. After receiving the request, the server returns the requested web page and associated content.

A web page has several components. The first is the Hypertext Markup Language (HTML) document. This contains quite a bit of information, including directions for how the page should be rendered (displayed) by the browser, content, and more. It also contains file names for subcomponents of the web page such as images. It's important to note that HTML is not a programming language.

There are two types of web pages: static and dynamic. A static web page is one that is prebuilt. Its content, layout, etc., are predetermined. A dynamic page, however, is built "on the fly." It doesn't exist until it's called. The page is built from different pieces drawn from databases. Amazon is a great example of a dynamic website. My Amazon page will very likely be different from your page. The books and so on that appear on my page are based on my shopping and buying habits. All this information is stored in a database, along with elements like book images, descriptions, and so on. When I logon to Amazon, the server sends the items that are standard for everyone (like the Amazon logo), along with the content targeted to me.

When interacting with a website, it's important to understand where certain things are occurring. This can be especially important from a forensics perspective because it can tell you where you should be looking for a given artifact. Actions can occur on either the client side or the server side. JavaScript (no relation to the Java programming language) is a client-side technology. It's used for things such as rollovers on a navigation bar. The code that makes that work is downloaded and run on the local machine. Server-side actions are just the opposite and are used when there is a need to send information to another computer (like my custom content at Amazon).

ADDITIONAL RESOURCES

WEB TECHNOLOGY

Today's web is a complex place using many different technologies to make it run. Understanding how these work, even at a rudimentary level, will be very helpful. The w3 Schools website is a great source of introductory material on many of these technologies. The site includes reference material, lessons, quizzes, tutorials, and more: http://www.w3schools.com/.

Determining the ownership and host of a particular domain name can become relevant in a criminal or civil case. A search query known as a "whois" can help you identify some of the individuals and/or companies associated with a given domain name. A whois search can tell you the registrant, when the domain was created, the administrative contact, and the technical contact. The contact information typically provides a name, address, and phone number. Most, if not all, domain name registrars now offer private registration. Any whois search for a domain name with private registration will typically get the registrar's contact information, rather than that of the actual owner (Network Solutions, LLC, 2011). If you'd like to give this a try, visit one of the sites offering the whois service. Network Solutions is one: http://www.networksolutions.com/whois/index.jsp.

PEER-TO-PEER (P2P)

Peer-to-Peer (P2P) is used primarily as a means to share files. A major portion of the traffic on a P2P network is pirated music and movies, as well as child pornography. P2P differs from a client/server network in that computers on a P2P network can serve both roles (client and server). Gnutella is one of the major systems or architectures used in P2P networks.

MORE ADVANCED

GNUTELLA REQUESTS

On a P2P network, what stops a file request from propagating forever? There is actually a built-in mechanism in the information packets. In each packet, there is a Time To Live (TTL) value that is set to decrease by one every time it is delivered to another node on the network. Once that number hits 0, the packet is stopped.

To get started with a P2P network, users must first download and install a P2P client such as KaZaA, Frostwire, GigaTribe, or eMule. Typically, users then create a "shared" directory containing files they want to make available to others. To find files of interest to download, users normally enter search term(s) for the file or files they want. If the search is successful, the software returns a list of computers that have the requested file(s). Lastly, the files are downloaded to a directory of the user's choosing or to the default location specified by the client. P2P networks use HTTP to transfer files.

Nodes on a Gnutella fall into two categories. Nodes that have the required bandwidth as well as the uptime (time on the network) are classified as Ultrapeers. Those that don't are known as leafs. Ultrapeers perform some additional duties such as searching, indexing, and facilitating connections.

THE INDEX.DAT FILE

The INDEX.DAT is a binary, container-like file that is used by Microsoft's Internet Explorer (MSIE). The INDEX.DAT file holds quite a bit of value for forensic

examiners. There are multiple INDEX.DAT files on a system. The INDEX.DAT tracks several pieces of information regarding the URLs visited, the number of visits, and so on. These files are hidden from the user and must be viewed using a tool of some sort. Both FTK and EnCase are able to decipher INDEX.DAT files. MSIE has three directories: History, Cookies, and Temporary Internet Files. INDEX.DAT files are used to track the information and contents of each directory (Casey, 2009).

WEB BROWSERS—INTERNET EXPLORER

Web browsers are an indispensable part of the overall computing experience and serve as our "vehicles" on the "Information Superhighway" known as the World Wide Web. Although there are multiple browsers on the market, Microsoft's Internet Explorer is far and away the most widely used. Other browsers (for the PC) also getting some traction are Mozilla's Firefox and Google's Chrome. On Macintosh computers, Safari is king, with Firefox getting some use there as well. At their foundation, these applications function in much the same way. For instance, all of them use some sort of caching system. They also have mechanisms to deal with cookies, Internet history, typed URLs, bookmarks, and more. They differ in the details. Space does not permit an exhaustive look at all the browsers and the details of their inner workings. Instead, we'll focus on some of the common functions as they work in MSIE, the overwhelming market leader.

COOKIES

A cookie is a small text file that is deposited on a user's computer by a web server. Cookies can serve a variety of purposes. They can be used to track sessions and remember a user's preferences for a particular website. Amazon.com is a great example. When you return to the site, you are normally greeted with a "Hello, Susan," as well as customized recommendations based on your buying and browsing history. That level of individualization is made possible through cookies.

Cookies can provide valuable evidence and are tracked in a single INDEX.DAT file. They can contain Uniform Resource Locators (URLs), dates and times, user names, and more. Deciphering cookies can be a challenge, as they aren't normally written in the clear. Fortunately for us, tools are available to get this done. It's critical to note that the existence of a web address in a cookie is not necessarily proof that the suspect actually visited that site (Casey, 2009).

TEMPORARY INTERNET FILES, A.K.A. WEB CACHE

We are an impatient lot. As such, speed is vital to our Internet experiences. Today, web browsing is expected to be nearly indistinguishable from the applications running on our own machines. Web cache is one way that the browser makers shave some time off how long it takes to download information. Cache speeds things along

by reusing web page components like images, saving users from having to download objects more than once.

Microsoft's browser, Internet Explorer, refers to web cache as Temporary Internet Files (TIF). In Microsoft Internet Explorer, TIF is organized into subfolders bearing random eight-character names. They are organized using a collection of INDEX.DAT files. Each file in TIF has a corresponding date and time value associated with it. This includes a "last-checked" time, which is used by the browser to determine if a newer version exists on the server. If so, then it will download the newer version.

Users can view their TIF anytime using Windows Explorer. Inside the TIF folder, users will see a listing of its contents. Each item in the list will display an icon showing file type, file name, and the associated URL. It's important to understand that, in this instance, what the user sees is a virtualized representation of the content. The actual items are kept in the TIF subdirectories. The only file that is actually kept here is the INDEX.DAT that keeps tabs on where the files are located inside the various subdirectories.

Webmail evidence can also be found in TIF. Hotmail, AOL, and Yahoo! can all leave messages and/or inbox information that can prove useful. These items can be recognized by the file names. Here are some examples:

- Outlook web Access Messages—Read[#].htm
- AOL Messages—Msgview[#].htm
- Hotmail messages—getmsg[#].htm
- Yahoo!—ShowLetter[#].htm
- Outlook web Access Inbox—Main[#].htm
- AOL Inbox—Msglist[#].htm
- Hotmail Inbox—HoTMail[#].htm
- Yahoo!—ShowFolder.htm

Web cache can be used to determine both culpability and intent. Much of what's in web cache will be thumbnails (those small images) along with bits and pieces of web pages.

Image size can affect a case, particularly those involving child pornography. If the suspect images are composed entirely of small, cache-like images, then some prosecutors may be reluctant to file charges. The issue then becomes intent. Those images could have been downloaded automatically, without his consent. Images of such a small size can make for a much weaker case. Larger images—those not commonly found as part of a web page—are harder to explain away.

INTERNET HISTORY

Microsoft's Internet Explorer, the reigning king of browsers, keeps multiple historic user records. History is used to prevent a user from having to retype URLs into the address bar of the browser. The INDEX.DAT files track other details as well. For example, it tracks the number of times the site is visited, and the name of the file.

The Internet history is organized in multiple folders and INDEX.DAT files. There are three folders: Daily, Weekly, and Cumulative.

These folders use a naming convention based on a set prefix followed by a date range. For example, a folder covering the Internet history from October 1, 2011, to October 8, 2011, would look like this:

MSHist012011100120111008
MSHist01 – Folder name/prefix
2011 – Year (start)
1001 – Date (start)
2011 – Date (end)
1008 – Date (end)

People who have something to hide will often clear their histories on a frequent basis. This can be done manually by the user or automatically by the system. By default, the history is set to clear every twenty days. The user can change this to clear much faster than that. Using a tool that can read the registry, you can view this information here:

NTUSERS\Software Microsoft\Windows\CurrentVersion\Internet Settings\URL History

MORE ADVANCED

THE NTUSER.DAT FILE

The NTUSER.DAT file contains preference settings and individual information for each user profile. Browser history is part of this information. There is one NTUSER.DAT for each user profile on the system. Although technically a registry file, the NTUSER.DAT is located in the user folder. Note that we're talking about user "profiles" and not "users." Whether a specific person has been on the keyboard is a very difficult, if not impossible, determination to make. Just because a person has a profile on the machine does not mean their fingers were on the keyboard at any given moment.

If this value is set to less than the default of twenty days, this can be used to show that the defendant took proactive steps to remove potentially incriminating evidence.

INTERNET EXPLORER ARTIFACTS IN THE REGISTRY

As part of its everyday function, MSIE deposits artifacts in the registry. These items are stored particularly in the NTUSER.DAT hive. Here we can see if the browser stores passwords, along with the default search engine, the default search provider, and more.

The registry can also tell us what URLs have been typed right into the browser's address bar. These are listed from 1 to 25 with the lowest number being the most recent. Only twenty-five entries can be kept at a time. The entries are purged on a first-in/first-out basis. Figure 8.1 shows you what they look like through a forensic tool.

Here is the file path to this registry artifact:

Name	Type	Data
url1	REG_SZ	http://www.google.com/
url2	REG_SZ	http://www.fileshredder.com/
url3	REG_SZ	http://www.wikileaks.org/
url4	REG_SZ	http://hackernews.com/
url5	REG_SZ	http://www.hacker.com/
url6	REG_SZ	http://www.hacer.com/

FIGURE 8.1

Typed URLs as found in the Windows Registry. Graphic courtesy of Jonathan Sisson.

NTUSER\Software\Microsoft\Internet Explorer\Typed URLs

Remember, the registry is not human-readable in its native form. To examine it, you will need an appropriate tool. Some of these tools include Microsoft's RegEdit, Harlan Carvey's RegRipper, and AccessData's Registry Viewer.

CHAT CLIENTS

Chat applications are both popular and numerous. They are used for instant text-based communication. Popular applications include AOL Instant Messenger (AIM), Yahoo! Messenger, Windows Live Messenger, Trillian, Digsby, and many more. These clients can be used either to commit or to facilitate a variety of crimes. Pedophiles use these tools to solicit sex from minors or to distribute child pornography. Buyers and sellers use them to negotiate the sale and transfer of narcotics. The list can go on and on. Function varies from client to client as do the artifacts they leave behind. Function and residual evidence can also vary from version to version.

It's difficult to keep up with the rapid pace at which these clients change. Changes can result in artifacts moving or disappearing. Rather than get "down in the weeds" with each application and version, we'll talk in broad terms about what kind of artifacts are possible and how they can be used as evidence.

Not unlike other software, a chat client will leave artifacts of its installation. Paths and directories may vary somewhat. The presence or absence of these files and folders may help in proving or disproving that a specific client was used to communicate with a victim or accomplice.

Chat programs maintain a contact or "buddy" list. This list of screen names can be used to link individuals together, particularly if the other parties' screen names appear in the logs or on the drive. Screen names are often nonsensical, like "football-fan7878," and it can take some effort to connect them with specific people. Entering screen names as part of your keyword search can also be very helpful. To complicate matters further, users can have multiple screen names. Many times, these alternate identities assume a parent-child relationship with the primary identity.

Users can also choose to block people, preventing them from communicating with them. If this function is available, this setting should be tracked somewhere, potentially leaving relevant artifacts. Often clients will also maintain a list of recent chats.

Other preferences that are under user control include embedding the date time in the chat, selecting a custom icon or image, and enabling or disabling logging. Logging can serve as a tremendous source of evidence if it's enabled.

Normally, logging is turned off by default, requiring the user to activate that function. Logs typically record the chat conversations and/or other related information like connection details. Even if logging is turned off, the user can manually save that particular chat session if necessary. A major difference between having logging turned on and manually saving a session log is the location where the resulting file is saved. Auto-saved logs will normally go to a default location, whereas a destination will have to be selected for a manually saved log.

Another preference setting of interest involves the automatic acceptance of video calls, file transfers, real-time instant messages, and so on. By default, many of these features are disabled. This setting and the subsequent functionality can be used to prove that an image wasn't downloaded without consent. Suspects will have an uphill slog trying to get a jury to believe that they "had no idea" they were downloading child pornography through their chat clients when the settings prove that they had to agree to accept it.

Some chat/IM clients are now allowing users to associate a cell phone (or more than one) with their accounts. This allows them to have IM messages forwarded to their mobile phones. In this situation, the cell number, together with the account information, could be used to help connect that person to a particular screen name.

INTERNET RELAY CHAT

Commercial chat clients like Yahoo! and AOL are quite popular and in wide use. Two other chat clients are well worth exploring. These tools are arguably better suited for criminal activity. Internet Relay Chat (IRC) is one such tool. IRC is a large chat network that has little to no oversight as it is under the control of no one single entity. It affords its user near-total anonymity because there is no formal registration process. IRC is also free to use. The IRC network comprises many smaller networks, such as Undernet, IRCnet, and EFnet, just to name a few (Casey, 2011). IRC users create their own chat rooms or "channels." IRC attracts criminals with a wide range of interests looking to trade information or contraband. Network intrusion, identity theft, and child pornography represent some of the main criminal interests found on IRC.

IRC boasts some other features that make it attractive for criminals. Direct Client Connection (DCC) allows two users to connect directly from one machine to the other. In this mode ,the communication is totally private. This private traffic even avoids network servers, leaving no evidence for investigators to find.

"I SEEK YOU"

I Seek You (ICQ) is the second chat tool that warrants a closer look. ICQ came on the scene in 1996.

These numbers from ICQ give you an idea of just how popular this chat client is:

- More than 42 million active users
- More than 425 million downloads

- More than 1.1 billion messages sent and received every day
- Average ICQ user connected more than five hours per day
- 47% female and 53% male
- 80% of users between the ages of thirteen and twenty-nine
- Available in sixteen languages (ICQ)

Unlike IRC, ICQ does have a registration process. Users who register are assigned a User Identification Number (UIN). Communication on ICQ maintains a high level of privacy. One must be invited to be included into a conversation. ICQ does route traffic through centralized servers so some artifacts may exist there if that server can be found.

E-MAIL

Of all the potential sources of digital evidence, e-mail is one of the best. People often draft and send e-mail that they assume will never be read by anyone other than the intended recipient. These often-candid exchanges can (and have) come back to haunt the parties involved. It's also persistent, residing in multiple locations, making it harder to get rid of.

ACCESSING E-MAIL

E-mail is accessed and managed in one of two ways. The first is web-based e-mail such as Google's Gmail or Microsoft's Hotmail. These tools function through a web browser. The second is through an e-mail application (client). E-mail clients are specialized programs designed specifically for working with e-mail. Some applications also manage calendars, tasks, contacts, and more. Outlook and Windows Live Mail by Microsoft are two of the most popular e-mail clients on Windows systems. Outlook, the more robust of the two, is used primarily in the workplace or by power users. Windows Live Mail and its predecessor Outlook Express have much more limited functionality.

Outlook stores data in either a .pst or .ost file. Windows Live Mail stores individual messages as .eml files. Microsoft Outlook Express uses .dbx. Getting at the individual messages from inside these containers is a concern, but much less so now that several current tools handle these file types natively. Individual e-mail messages (.msg files) can be exported out and given to investigators or attorneys for review.

E-MAIL PROTOCOLS

E-mail uses multiple protocols to send and receive messages. Some of them are:

- Simple Mail Transfer Protocol (SMTP)—Used by e-mail clients to send e-mail and by servers to both send and receive.
- Post Office Protocol (POP)—Used by e-mail clients to receive e-mail messages.
- Internet Message Access Protocol (IMAP)—Two-way communication protocol used by clients to access e-mail on a server.

E-MAIL AS EVIDENCE

E-mail is widely used and people tend to be uninhibited in their e-mail messages, saying things they might never say otherwise. Thus, e-mail can provide us with a wealth of potential evidence. Some of those things include:

- Communications relevant to the case
- E-mail addresses
- IP addresses
- Dates and times

When investigating e-mail, it's important to realize that it could be found in a number of places. These include: the suspect's machine, any recipient's machine, a company server or backup media, a smartphone, a service provider, and any server that the message may have passed through on its way to its final destination. Like most web-based evidence, time is still a factor. Collecting that evidence sooner rather than later will give you a better chance of success.

The main components of an e-mail are the header, the body, and—potentially—attachments. Every e-mail message that's sent has a header. The header records information as the e-mail travels from the sender to the receiver. Think of it as a passport of sorts. At every stop (server) along the way, information is added to the header. The body of the e-mail is the message itself. Finally, any attachments are added. These include items such as images and user-created files such as documents, spreadsheets, and so on. Keeping the attachments connected with an associated e-mail message is very important from an evidentiary perspective.

E-MAIL—COVERING THE TRAIL

Especially savvy suspects may take steps to prevent someone from tracing a message back to them. For example, they could forge an e-mail (make it appear to be from someone else) or remove or modify the headers. Suspects could also create phony e-mail accounts.

Free software available on the Internet enables users to "spoof" an e-mail. Spoofing is the act of making an e-mail look as though it actually came from someone else or from a different location. There are services available that will remail (forward) messages, stripping out the identifying information before transmission. This is known as anonymous remailing. Many of these companies don't keep logs, further ensuring the privacy of their users.

ALERT!

SHARED E-MAIL ACCOUNTS

E-mail can be used to communicate even without being sent. This is done by creating an anonymous account, on Yahoo! for example, and sharing the login information. Users then simply create messages and deposit them in the "Drafts" folder for others to read. Once the message is read, it can be deleted. These accounts can be for one-time use, making them nearly impossible to trace or monitor. This is a popular practice

among terrorists. "One-time anonymous accounts are extremely difficult to monitor," said Richard Clarke, former U.S. counterterrorism czar (Frontline, January 25, 2005).

TRACING E-MAIL

Tracing an e-mail message is heavily reliant on logs. As we learned earlier, each server along the e-mail's path adds information to the message header. One of those bits of information is the Message ID. The message ID is a unique number assigned to the message by the e-mail server. Correlating the message ID with the server's logs is solid evidence that the message was received and sent by that particular machine. Again, the providers may purge those logs on a regular basis if they even keep them at all. Foreign providers will likely be very tough to deal with, making collection of this evidence that much harder.

READING E-MAIL HEADERS

The e-mail header provides a record of the path the message took from sender to receiver (assuming steps weren't taken to alter or remove it). E-mail headers should be read from the bottom to the top. Below is a sample e-mail header from a message I may have sent to legendary Pittsburgh Steelers linebacker Jack Lambert.

```
Delivered-To: Lambert58@gmail.com
Received: by 11.48.31.1 with SMTP1 id c2ct279nzg;
Fri, 25 Oct 2011 22:38:23 -0800 (PST)
Return-Path:
Received: from mail.emailprovider.com (mail.myisp.com
[12.34.567.890]) by mx.gmail.com with SMTP id
f27se846431anc.2011.10.25.22.38.19; Fri, 25 Oct 2011
22:38:23 -0800 (PST)
Message-ID: <20111025233819.47097.mail@mail.myisp.com>
Received: from [12.34.567.890] by mail.myisp.com via
HTTP; Fri, 25 Oct 2011 22:38:19 PST
Date: Fri, 25 Oct 2011 22:38:19 -0800 (PST)
From: John Sammons
Subject: Super Bowl
To: Jack Lambert
Delivered-To: Lambert58@gmail.com
The message recipient
Message-ID: <20111025233819.47097.mail@mail.myisp.com>
Received: from [12.34.567.890] by mail.myisp.com via HTTP;
Fri, 25 Oct 2011 22:38:19 PST
This the record of the message being sent through Jack Lambert's
email provider, mail.myisp.com.
Delivered-To: Lambert58@gmail.com
Received: by 11.48.31.1 with SMTP1 id c2ct279nzg; Fri, 25 Oct
2011 22:38:23 -0800 (PST)
Return-Path:
Received: from mail.emailprovider.com (mail.myisp.com
[12.34.567.890]) by mx.gmail.com with SMTP id f27se846431anc.
2011.10.25.22.38.19; Fri, 25 Oct 2011 22:38:23 -0800 (PST)
Finally, the message is transmitted from my email provider
to Jack's Gmail account, Lambert58@Gmail.com
```

Note the message ID, 20111025233819.47097.mail@mail.myisp.com. Remember, this is a unique number assigned by an e-mail server (Google, 2011).

SOCIAL NETWORKING SITES

E-mail and social media have at least one thing in common: There seems to be almost nothing that people won't send, post, or tweet. The fact that everyone seems to be on Facebook, Twitter, LinkedIn, or some flavor of social media is not lost on law enforcement or prospective employers for that matter. Both groups routinely look to social media to learn more about suspects and prospective employees.

Social media evidence can be found in several places, including the suspect's computer and smartphone, and the provider's network. Getting evidence from the provider will require relatively quick action, along with a subpoena or search warrant. Remember, the provider only retains this information for a certain amount of time. At some point, the data you need will be purged without some legal intervention. All things considered, collecting the evidence from the provider might yield the best results.

Recovering evidence on the local machine can be a challenge. The page file (or swap space) is one location that could bear fruit. INDEX.DAT files also hold promise. Multiple artifacts can be found here. The confirmation e-mail (sent when the account is created) is found in the History.IE5(Index.dat file. The user's Facebook profile can be found on the local machine in a file named profile[#].htm. This is located in the Content.IE5 directories. The History.IE5(Index.dat file can hold Facebook friend searches.

ADDITIONAL RESOURCES

CASEY ANTHONY TRIAL TESTIMONY

The Casey Anthony trial garnered media attention across the country. Anthony was charged with murdering her young daughter Caylee. Digital forensics played a central role in the case, particularly regarding the searches for certain keywords such as "chloroform." The trial testimony in this case by computer forensic examiner Sgt. Kevin Stenger provides some insight expert testimony on browser forensics (Firefox, in this instance): http://www.myfoxorlando.com/dpp/news/060811-kevin-stenger-testifies

SUMMARY

The Internet functions in large part due to two protocols, specifically HTTP and TCP/IP. Another very common technology in wide use is or Hyper-text Markup Language (HTML). HTML is one of the primary languages used to construct web pages. In

digital forensics, evidence can be found within this code, so it behooves us as examiners to be able navigate through it to locate any existing evidence.

We also looked at how web pages are found and sent to browsers using Uniform Resource Locators (URLs) and Domain Name Servers (DNSs).

Peer-to-Peer (P2P) networks can be used to share not only pirated music and movies, but contraband such as child pornography as well.

This chapter also looked at several artifacts generated from Internet and e-mail usage. These includes such things as INDEX.DAT records, Temporary Internet Files (TIF), the NTUSER.DAT file, cookies, and e-mail headers. Tracing an e-mail back to its origin is no easy feat, as the identifying information can be forged or removed.

Chat clients and their associated logs are worth examining if found on a computer. Remember, logging may not be turned on by default.

IRC and ICQ are two modes of Internet communication that can't be ignored. These are two of the most popular ways for criminals (and others concerned with private communication) to help cover their trails.

Social networking is used worldwide today by a massive number of people. Social networking evidence can be found locally and remotely on a provider's network.

REFERENCES

Casey, E., 2009. Handbook of Digital Forensics and Investigation. Academic Press, Burlington, MA.

Casey, E., 2011. Digital Evidence and Computer Crime: Forensic Science. Computers and the Internet Academic Press, Waltham, MA.

E.I. du Pont de Nemours and Company v. Kolon Industries Inc, 2011. U.S. Dist. LEXIS 45888. E.D. Va. Retrieved from: <http://www.ca4.uscourts.gov/Opinions/Unpublished/121260.U.pdf> (accessed 09.16.11.).

Frontline. Retrieved from: <www.pbs.org/wgbh/pages/frontline/shows/front/special/tech-sidebar.html> (accessed 09.19.11.).

Google, 2011. Reading Full Email Headers. Retrieved from: <http://mail.google.com/support/bin/answer.py?hl=en&answer=29436> (accessed 11.10.11.).

http://www.nativeintelligence.com/ni-free/itsec-quips-05.asp.

Network Solutions LLC., 2011. WHOIS Behind That Domain Name? Retrieved from: <http://www.networksolutions.com/whois/index.jsp> (accessed 11.19.31.).

w3schools, 2011. HTML Introduction. Retrieved from: <http://www.w3schools.com/html/html_intro.asp> (accessed 11.10.13.).

http://www.nist.gov/.