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.)

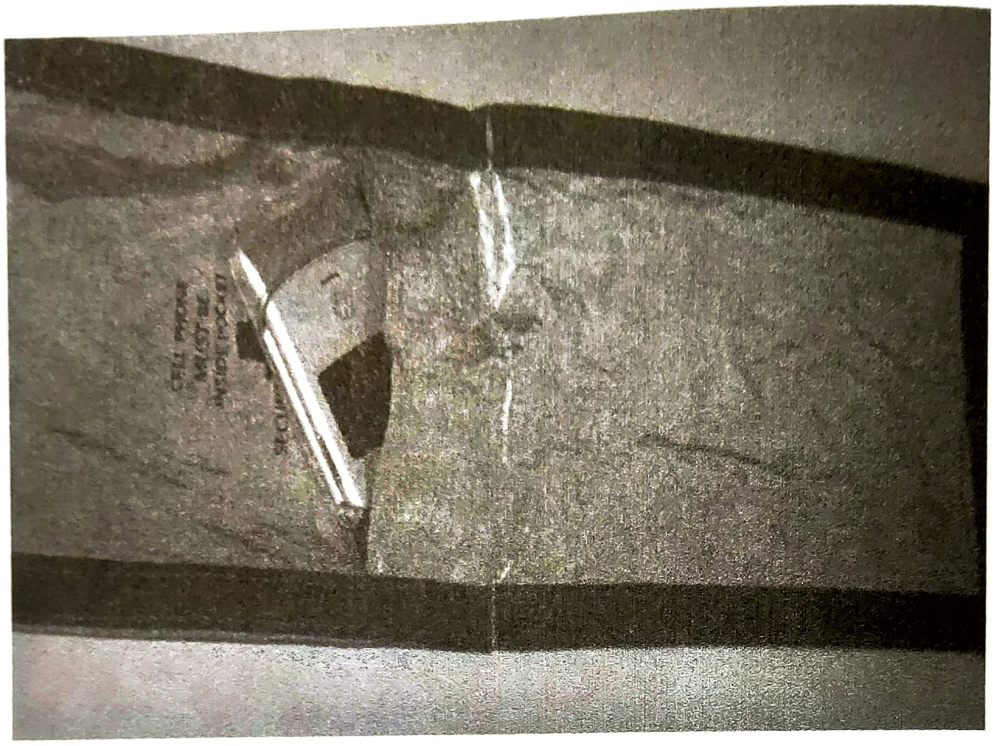

FIGURE 4.1

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).

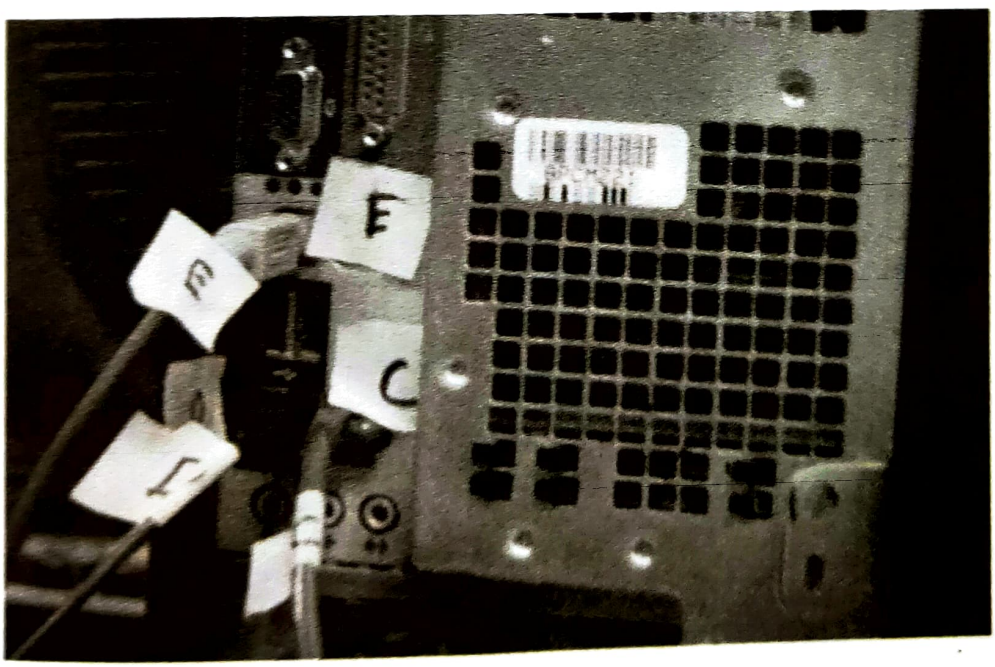

FIGURE 4.2

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

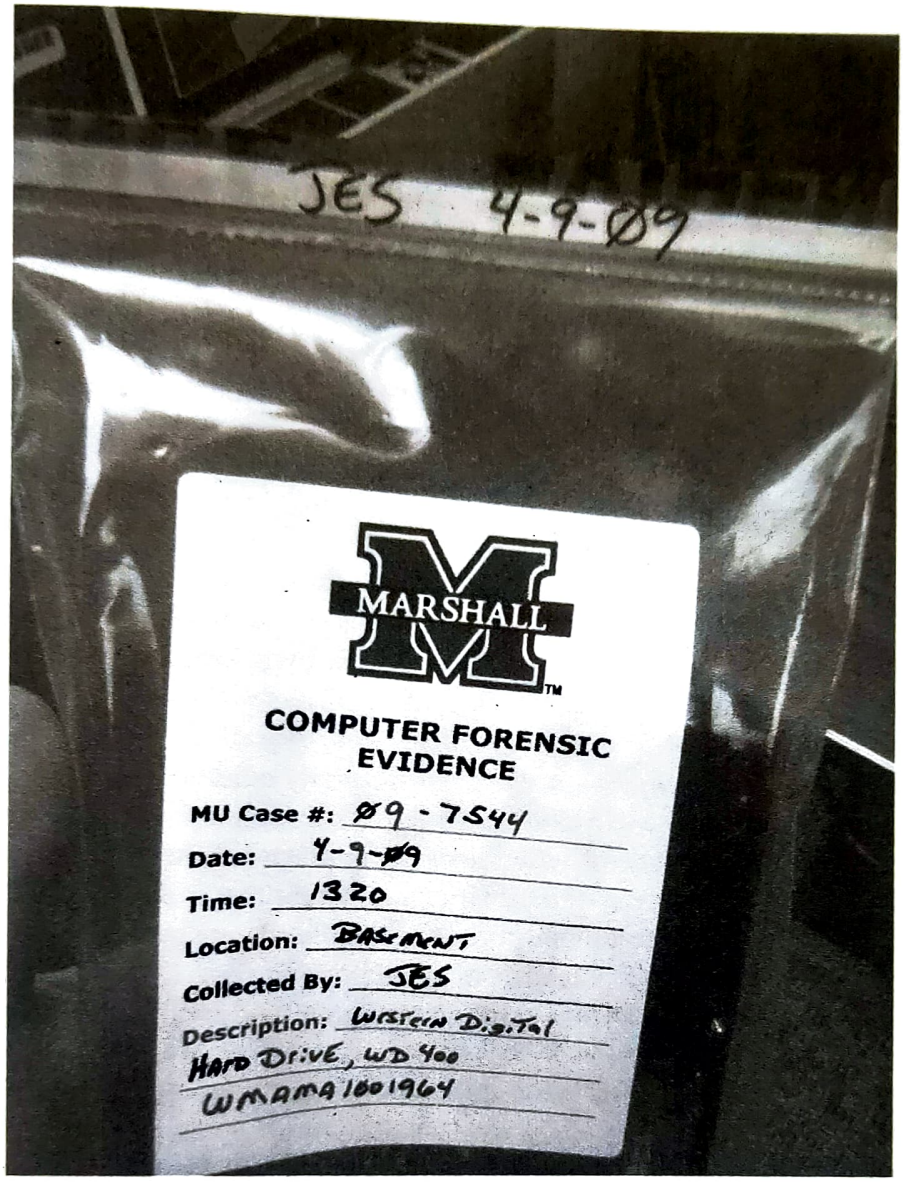

FIGURE 4.3

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.)

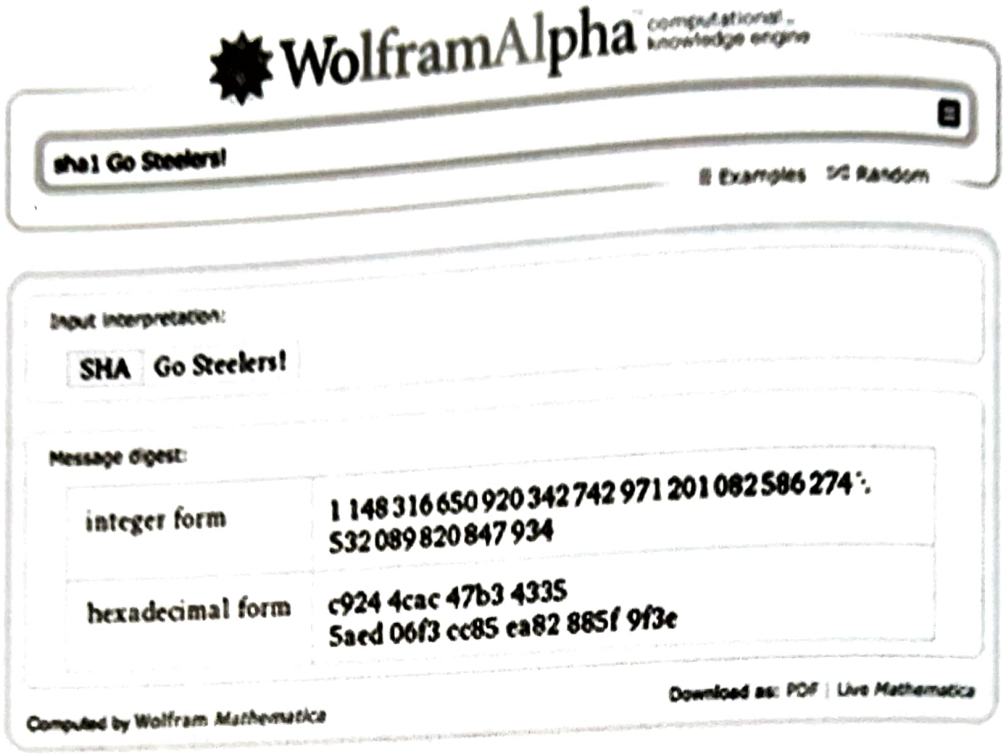

FIGURE 4.4

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.