Evidence Management

In this chapter you will learn:
• Proper evidence collection techniques
• How to preserve and transport evidence
• Methods for tracking evidence
• Proper storage of evidence
• Evidence access control
• How to dispose of evidence after an investigation

Evidence management is a topic that covers the details of evidence collection, chain of custody, and managing the actual investigation. Some of these topics were briefly touched upon in Chapter 2 but will be covered in more depth in this chapter. The primary theme of this chapter is maintaining the chain of custody. Chain of custody is the cornerstone of any forensic investigation.

Evidence Collection
The first step in a forensic investigation should be the collection of evidence. As discussed briefly in Chapter 2, this will begin by documenting the location and environment where the evidence is being seized. When discussing documentation of the scene, several items should be included in that documentation.

Evidence Documentation
In order to make this point clear, let us walk through a hypothetical scenario together. Assume that you are at an apartment where police allege the laptop that is on the desk in the living room has been a source for child pornography. The first thing you should document is the condition of the computer in question. When you arrived, was it running or not? Does it appear to be damaged in any way? Once you have ascertained the condition and status of the target computer, are there any other devices connected to it? For example, a printer attached to that computer would be worth noting. You will also need to take note of all other computer equipment in the residence. This will include the router, cell phones, and other computing devices. Documentation of the scene must be at least done by writing down notes; however, photographs are often useful. Figures 3-1 and 3-2 provide two photographs of a possible cybercrime scene.
Figure 3-1  Suspect computer angle 1

Now if you examine these two images, you can see they document significant information. In Figure 3-1, you can see that there is a Sony Vaio laptop in a docking station. It has several USB devices connected to it, most importantly a Passport portable USB drive. This clearly shows that external USB devices are present at the crime scene and should be examined for possible evidence. In Figure 3-2, you readily notice the Epson

Figure 3-2  
Suspect computer 
angle 2
laser printer. More advanced printers often have permanent storage that can be examined to see what documents have been printed. However, you also see a second monitor and keyboard. This would indicate that at least at some point there has been a second computer present. It would then be necessary to search the location to see if the second computer is still on site. All of these facts are documented by taking two simple photographs of the crime scene. You should also write down a description of what is at the scene to go with the photographs taken.

NOTE It is quite common for forensic investigators to document the scene using video recording. This is a good idea, with one caveat. If you are going to record video, it should be complete video. Do not stop the recording and then restart at a different angle or different portion of the crime scene. Doing so would allow the opposing counsel to question what occurred during the gap in recording. What was in the section you did not record? These questions can cast unnecessary doubt on a properly conducted investigation.

In some cases, sketching the scene may be helpful. However, sketches should only be done if required to provide context for the evidence and if personnel capable of creating a readable and helpful sketch are available. In some physical crimes, such as homicide, sketching the scene can be invaluable. However, in cybercrimes, this is less often useful. You should determine the need for a crime scene sketch on a case-by-case basis.

Once the scene has been properly documented, you should also note any environmental conditions that might affect digital evidence, such as extreme moisture or temperature. You should also note all personnel who are present. This list might include the suspect (even if he or she is removed from the scene at some point during your investigation), any other forensic personnel, any law enforcement personnel, and anyone else at the scene. The documentation should include the person’s name, role (i.e., a detective, the suspect, etc.), whether or not the person in question had access to the suspect equipment, the time they arrived, and when they left. In the case of the suspect, you should even document if they were in reach of the equipment in question.

The capture/point of transfer is generally when evidence is first seized. It can, in some cases, be the point at which a disk is imaged; however, this is less likely. Most imaging today takes place at the forensic lab. In essence, documenting the scene is the process of documenting the capture point for the evidence.

Evidence Preservation
In addition to collecting evidence, the evidence must be preserved. When collecting evidence, the investigator must protect its integrity. This involves two related tasks. Make sure that nothing is added to the evidence and that nothing is destroyed. This process is called evidence preservation.

Preserving evidence is something that must be considered throughout the process of seizing evidence, analyzing evidence, and transferring evidence. One way this is accomplished is by always working with a copy of the evidence, not directly working with
the evidence itself. This involves creating an image of any disk, drive, or other storage device. Earlier in this book we discussed how to image a hard drive manually with Linux commands. Most major forensics toolkits also provide imaging capabilities. Let us take a look at one of these tools.

**TIP** The test won’t ask you the specifics of how particular commercial tools such as EnCase and Forensic Toolkit work. However, in the field you will need to understand common forensic tools. Both EnCase and AccessData are popular with law enforcement agencies.

**AccessData’s Forensic Toolkit**

AccessData produces the Forensic Toolkit. They even provide the disk imager as a free utility you can download. Once you have installed it on your forensic computer, you begin by attaching the suspect drive and selecting Create Image from within the disk imager. This is shown in Figure 3-3.

![Figure 3-3 Choosing to create an image of a disk with Forensic Toolkit](image)

The next step is to just follow the wizard, selecting which drive to image and where to put the image. Then AccessData Disk Imager does it for you. The process is shown in Figures 3-4 through 3-6.
Chapter 3: Evidence Management

Figure 3-4  Select Source dialog box

Figure 3-5  Select Drive dialog box
When the process is done, you will have an image that you can utilize for forensic purposes. Note that you should first hash the original and the image and compare the hashes; fortunately, this utility has an option to do that for you as well.

**Guidance Software’s EnCase**
Guidance Software’s EnCase product also provides disk imaging capabilities. Their process is a bit different. Every piece of evidence must be part of a case file. So the first step is to either select an existing case or begin a new one. Beginning a new case is shown in Figure 3-7.

Then you select to add evidence to a case. As you can see in Figure 3-8, that can be a local disk, image, evidence file, and other types.

If you select a local disk, you will be presented with the screen shown in Figure 3-9. Notice that EnCase gives you the option of only working with write-protected disks. We will discuss disk write protection in detail, later in this chapter.
Chapter 3: Evidence Management

Figure 3-7  Starting a new case in EnCase

Figure 3-8  Adding evidence to the EnCase file
After you have selected a disk, the rest is just walking through the wizard, similar to how it is done in AccessData. Your next screen will give you a list of disks connected to the machine you are running EnCase on. This is shown in Figure 3-10. Note that the drives in this figure are not write-protected.

**TIP** However you image the drive, remember to make two images, hash each image and the original, and then compare the hashes of the images to the original. They must match; if they don’t, something went wrong during the copying process. Also remember that simply copying files is not adequate for forensic purposes. Complete disk imaging gets everything, bit by bit. File copying will skip hidden files, data hidden in slack space, and deleted data.
Write-Protected Storage Devices

Another of the most elementary aspects of evidence preservation is to use write-protected storage devices. This means that the suspect drive should immediately be write protected before it is imaged. The media should also be labeled to include the following:

- Investigator’s name
- The date the image was made
- Case name and number

This process is a critical step in securing evidence. Beyond the danger of simply accidentally writing some data to the drive, there is the issue of operating system writes. Many operating systems periodically write data to a drive. The NFTS file system may attempt to commit or roll back changes that occurred before the drive was seized. It is important that nothing be written to a drive that is used for evidence.

There are a variety of ways to write-protect a device. Most commonly used are write blockers that are made specifically to secure a drive for forensic purposes. These devices can be a hardware write blocker, or even a hard drive disk controller that is made specifically to disallow disk writing. These are often called forensic disk controllers, because forensic purposes are usually the only ones that require write protection. These forensic disk controllers simply interrupt any write commands sent from the operating system to prevent disk writing. Write-blocking devices are often classified by how they work: native or tailgate. A native device uses the same interface for both in and out. This is used when both ends are the same type of drive, such as SATA to SATA. A tailgate device uses one interface for one side and a different one for the other—for example, a USB to SATA write block. Some of the more widely used write blockers are listed in Table 3-1.

<table>
<thead>
<tr>
<th>Name of Write Blocker</th>
<th>Type of Write Blocker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tableau</td>
<td>Hardware devices</td>
</tr>
<tr>
<td>WiebeTech</td>
<td>Hardware devices</td>
</tr>
<tr>
<td>UltraWrite</td>
<td>USB devices</td>
</tr>
<tr>
<td>ForensicSoft</td>
<td>Software write blockers</td>
</tr>
</tbody>
</table>

There are also devices that have write-protection features on the drives themselves:

- The Kanguru USB drive has a write-protect switch that can be turned on.
- Imation also makes a USB drive with a write-protect switch.
Additional Evidence Preservation Considerations

While write-protecting the drive is a fundamental step in evidence preservation, other steps must be taken. One issue that must be addressed is preventing electronic static or other discharge from damaging or erasing data. Special evidence bags that are antistatic should be used to store digital devices. Preventing electrostatic discharge (ESD) and other electrical discharges from damaging the suspect drives is critical.

Cyber forensic labs should also block transmissions into or out of the lab. This is often done by constructing what is called a Faraday cage. The Faraday cage is named after the famous physicist Michael Faraday. A Faraday cage is a mesh of conducting material. This prevents electromagnetic energy from entering into or escaping from the cage. This prevents the device from sending data out, as well as prevents someone from the outside accessing the device via WiFi or cellular signals. There are portable bags that have a Faraday cage—these are called Faraday bags, and in some cases, colloquially referred to as black hole bags.

For mobile devices, such as smart phones, tablets, e-readers, and Google Glass, signal isolation is critical. As long as the device is remotely accessible, it is possible that someone could remotely wipe evidence. In fact, many smart phones have the option to remotely wipe them in case they are stolen. It is also possible that any device that can communicate over WiFi or cellular signal could be transmitting information. For example, if the device is infected with spyware, that spyware may continue to send information to an outside party. Whether it is electromagnetic interference (EMI) or radio frequency interference (RFI), blocking such signals is an important part of securing the evidence.

NOTE  It is becoming common for forensics labs to have terabytes of data they have trouble storing in a way that is easily accessible and searchable. One possible solution is WORM storage. WORM stands for Write Once Read Many. It automatically write-protects data as soon as it is saved to the system. Large-scale WORM implementations allow for large amounts of data to be stored in a write-protected environment.

Evidence Transport

Once evidence is collected, it must be transported to the forensic lab. And it will again need to be transported to the courthouse for trial. It is critical that the chain of custody be maintained during this transport. Therefore, the first step in transport is to maintain possession of the evidence during this time. If a person takes evidence from a crime scene, he or she should proceed immediately to the forensic lab with no stops. Not even stops for meals. Then the evidence is checked in. When transporting evidence from the lab to the courthouse, the evidence is first checked out. The person who signs for the evidence should maintain custody of the evidence until it is checked back in.

During transport, it is often a good idea to first secure evidence in some container, such as a lockable briefcase or similar portable device, and then lock that container
into the vehicle’s trunk or other storage area. Even with the double locking, it is recom-
mended that the person transporting evidence stay with the vehicle so that he or she
can maintain custody of the evidence.

NOTE While the popular television program CSI is fictional, and they do tend
to exaggerate forensics, there was a specific episode that dealt with chain of
custody that posed a realistic issue. The investigator gathered evidence from
a crime scene, but it was the end of his shift, so on the way back to the police
station, he stopped for breakfast. The evidence was in his locked vehicle for over 30 minutes,
out of his sight while he ate and chatted with colleagues. Now in reality, this might or might
not lead to the evidence being dismissed by a judge. It is not even certain that opposing
counsel would be aware of the issue and challenge the chain of custody. However, it simply is
not worth the risk. The proper thing to do is to go immediately to check in the evidence.

Evidence Tracking
In a forensic laboratory, you will have multiple cases going on simultaneously. It is
virtually impossible to mentally track where all evidence is at a given time. As we have
already discussed, the chain of custody is critical, and that includes tracking the evi-
dence. There are a variety of means for tracking evidence. The specific method you util-
ize will depend on your agency’s budget and case load. However, each major method
is described here.

Logs
The most basic form of tracking is to maintain a log of evidence. This can be as simple
as a document wherein each piece of evidence is tracked as it is removed from storage
and returned. Figure 3-11 is a sample of such a log.

<table>
<thead>
<tr>
<th>Case: CS12991</th>
<th>Item: Dell Inspiron Laptop Serial Number 12345</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Checked out</td>
<td>Time Checked out</td>
</tr>
<tr>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>1/3/2014</td>
<td>3:30 pm</td>
</tr>
</tbody>
</table>

Figure 3-11 Evidence tracking log
The log shown in Figure 3-1 is a sample—the specific formatting of the log your agency uses will probably vary somewhat from this image. However, this image shows several things that make a log useful. The first and most obvious is that the initial check-in date and time, along with who checked in that evidence, is clearly documented. Next, you should note that every time the evidence is removed from storage, the log clearly shows who removed the evidence, why they removed it, and exactly when it was checked out and when it was checked back in.

A well-maintained evidence log accomplishes two purposes. First and foremost, it aids in maintaining the chain of custody. With a complete log, you can easily show exactly where evidence was at any given time and who was accessing it. As we have discussed previously in this book, few things are more important in a forensic investigation than maintaining the chain of custody. However, the log accomplishes a second goal as well. If you should wish to examine evidence, you can go to the log and find out exactly where it is at that time. If it is currently checked out, you can talk to the person who has the evidence checked out and find out when they will be done with their testing. In addition to a log, it is common to find evidence is labeled (also discussed in this chapter), and when the investigation is complete and evidence is just waiting for trial, the evidence may be sealed.15

**Software Tracking**

A variety of software tracking packages can essentially take the place of a paper log. These packages simply make the maintaining and storing of logs more efficient. For example, these application-utilized databases will allow you to search for any item of interest, such as all entries related to a specific piece of evidence. Or perhaps you would like to know all items that have been checked out by a specific analyst in the past two weeks. You could even search for all activity in a given time frame. Several software applications are available for this purpose, including


There are many others, and it should be noted that you will need to examine specific programs to see which one is a good fit for your agency.

---

**TIP**  I highly recommend using some sort of tracking software, though I don’t recommend any specific product. If your agency’s budget allows for the purchase of such software, it is much easier to manage than paper records.
Barcode
Another process for evidence tracking that is gaining popularity is barcode tracking. This is much like logging, but it is automated. System details can vary from implementation to implementation, but in general, the system works as follows. Each piece of evidence has a barcode attached to it or to its container (such as an evidence bag). Then, each analyst has their own barcode scanner. When a piece of evidence is accessed, its barcode is scanned. Then the system knows who accessed the evidence and when. It is also possible to use systems wherein the barcode scanners themselves also record their specific location, thus adding more detail to the record.

RFID
Radio frequency ID (RFID) chips can be utilized to track evidence. These systems are implemented in much the same way as a barcode. The RFID chip is attached to the evidence or the evidence container. Then, at any given time, the system knows the exact location of a given piece of evidence.

TIP Remember that the log is the core of any evidence-tracking system. I would recommend that even if you use barcode or RFID, having each person actually sign for the evidence is a very good idea. An even better idea is to have a person responsible for the evidence, and each time it is checked out, the evidence handler and the investigator have to sign.

Evidence Storage
How and where to store evidence is an important topic. Proper storage of evidence is a significant part of maintaining the chain of custody and of evidence preservation. The evidence must be secured in a location that is safe from environmental hazards, inaccessible without proper authorization, and secure from electromagnetic interference. All of these issues must be addressed when selecting an evidence storage location.

Environmental Hazards
Environmental hazards include a variety of factors ranging from temperature control to fire suppression. Some threats from the environment include

- Fire and smoke contaminants
- Extreme cold or heat
- Utility loss (power, AC, heat)
- Water damage (broken pipes, flooding)
To protect against these environmental threats, several steps should be taken. The placement of the evidence room is a fundamental consideration. The room should be in a location not prone to flooding. It should also have adequate heat and air conditioning to prevent the temperatures from exceeding a range of approximately 50 degrees Fahrenheit to 85 degrees Fahrenheit. Colder temperatures are less likely to damage digital evidence, but some devices are susceptible to extreme heat.

**NOTE** I am personally aware of a situation wherein a city (name withheld for confidentiality reasons) was storing servers, including those that had forensic evidence, in a basement room that had water pipes along the ceiling. Eventually, a pipe did break, destroying the servers in question and their data.

Fire is a common hazard that must be guarded against. All walls, the ceiling, and the door to the evidence room must have an acceptable fire rating. UL Labs have a three-volume set of parameters by which they rate the fire resistance of walls. It is also common practice to store data in a safe within the evidence room. Most safes also have a fire rating. The following is a list of common ratings:

- Class 100 is for safes that contain digital data.
- Class 150 is the rating for microfilm and similar media.
- Class 350 is the rating for paper documents.

If your evidence room is a fire-resistant room, with equivalent walls, ceiling, and door, and your evidence is in a fire-resistant safe within that room, you have a very good chance of the evidence being undamaged in case of a fire.

**EXAM TIP** The CCFP does not ask details about fire ratings, fire extinguishers, or fire suppression. However, you will need this information in order to successfully set up a forensic lab. But you need not memorize these elements in order to take the CCFP. It should be noted that the (ISC)²’s Certified Information Systems Security Professional (CISSP) exam does ask about these specifics.

It is normal to have a fire extinguisher in or very near an evidence room. You should be aware that there are a variety of different types of fire extinguishers:

- **Carbon dioxide (CO₂)** Carbon dioxide (CO₂) foam, inert gas, and dry powder extinguishers displace oxygen to suppress a fire. CO₂ is a risk to humans because of oxygen displacement.
- **Water extinguishers** Water suppresses the temperature required to sustain a fire.
- **Halon** This substance was banned under the 1987 Montreal Protocol on Substances That Deplete the Ozone Layer. FM200 is one replacement for Halon.
Fire extinguishers are also classified into four general classes based on what types of fires they can extinguish:

- **Class A**  Ordinary combustibles such as wood or paper
- **Class B**  Flammable liquids such as grease, oil, or gasoline
- **Class C**  Electrical equipment
- **Class D**  Flammable metals

The CCFP test is going to focus on the general concept of securing the evidence storage area from environmental dangers.

### Unauthorized Access

For a room to be secure against unauthorized access takes more than simply having a good lock. To begin with, the walls must be sound. The walls must go all the way to the ceiling, rather than having a drop ceiling as many office buildings do. A drop ceiling would allow an intruder to enter an adjacent room and then simply come through the ceiling into the evidence room.

The door must be one that is not readily broken into. That indicates a door that resists forced entry and with hinges that are on the inside. A solid deadbolt lock is also necessary. Then, there should be some monitoring of who accesses the room. One way to control access is via a swipe card, with each authorized person having an individual card and the system recording who accesses the room and at what time. Ideally, such a system would have two-factor authentication, meaning that the swipe card is used in conjunction with a PIN number or password.

It is critical that the evidence room also be subjected to continuous video surveillance. That should include who enters the evidence room and the interior of the room itself. Remember that the cornerstone of evidence handling is the chain of custody. If you cannot prove that you have control of the evidence room, complete knowledge of who enters, when they enter, and what they do therein, then all of the evidence within the evidence room will be suspect.

### Electromagnetic Interference

Previously in this chapter we have discussed electromagnetic interference and radio frequency interference. We also discussed evidence bags that function as Faraday cages. It is equally important that the evidence room that will contain electronic evidence also be a Faraday cage. That is usually accomplished during the initial construction of the room. A conductive mesh is added to the walls, floor, and ceiling, thus preventing RFI and EMI. There are electronic measuring tools that will indicate the efficacy of your Faraday cage. However, you can get a quick general indication with your cell phone. Attempt to use your phone outside the evidence room and then inside it. From inside the room, you should get no connectivity whatsoever. If you can get any connectivity, even intermittent and poor connection, this indicates your Faraday cage is not implemented.
properly. One common reason for that is incomplete coverage. For example, there may be some gap in the conductive mesh.

**U.S. Army Digital Evidence Storage**

The United States Army has specific guidelines on storing digital evidence:

1. A person with digital media evidence should store such evidence in a dust-free, temperature- and humidity-controlled environment, whenever possible.

2. A person with digital media evidence will not store it near batteries, generators, electro-magnets, magnets, induction coils, unshielded microwave sources, or any material that generates static. NOTE: Vacuum cleaner motors generate small electromagnetic fields that may alter, erase, and/or destroy digital media such as tapes.

3. A person with digital media evidence should not store such evidence in the same container with electronic devices. Some electronic devices contain batteries with sufficient strength to erase digital data over extended periods.

4. The evidence custodian should make periodic checks of digital media evidence in the evidence room to determine battery life of the item(s). There is a very high risk that all evidence contained in digital storage could be lost. So you must connect the evidence with appropriate chargers that can remain connected to uninterrupted power.

5. Where possible, the evidence custodian should store digital media evidence in a fire safe designed to safeguard items in heat in excess of 120 degrees Fahrenheit.

6. Where possible, the evidence custodian should not store digital media or devices in areas with sprinkler fire protection systems. If this is not possible, the evidence custodian should cover the media with waterproof material. The media should not be completely wrapped in waterproof material, because condensation can build and destroy the evidence.

7. The evidence custodian should not store digital media and devices in the same confined area with caustic chemicals (for example, acids, solvents, industrial strength cleaners, flammables). Exposure to fumes from such materials may cause surface erosion of media and loss of data.

8. A person with items of evidence that are classified or that contain classified information or material will store such evidence in accordance with AR 380–5.

Note that items 1, 2, 5, 6, and 7 specifically deal with environmental threats. These are sound guidelines that can be used even outside the U.S. Army. Item 4 deals with the fact that digital evidence is fragile, and you must check to ensure it is still present and has not degraded. While these standards were designed for U.S. Army forensics labs, they are worth reviewing even by non-Army forensic analysts.
Evidence Access Control

You need to control who accesses evidence, when it is accessed, and how it is used. The first principle that one must bear in mind with evidence access control is who has a need to access this evidence. The principle is similar to one used in the intelligence community where they operate under the axiom of need to know. Need to know means that it does not matter how high your security clearance is or how trustworthy you are, if you do not have a need to know certain information, you are not granted access to it. A similar principle should guide access to forensic evidence. It does not matter how trustworthy the detective, agent, or technician is. It does not matter how thoroughly their background has been checked. If that person does not have an actual need to access evidence, then they should not be granted access to it.

Once you have established the principle of only providing access to those with a clear need, the next question becomes how you enforce this. We have previously discussed logs, card key access to the evidence room, and a person assigned to manage access. All of these methods can be useful in evidence access control.

Evidence Disposition

It might seem obvious that once a case is decided the evidence should be destroyed. However, it is not uncommon for cases to be appealed, thus requiring the evidence to be maintained. Furthermore, it is always possible that at some future date there will be a challenge to the outcome of the case, necessitating the review of the evidence. For this reason, it is strongly recommended that your laboratory utilize an archive system. Once a case has gone to trial or been settled, evidence is moved to archival storage.

Archival storage must meet all the security requirements that your normal evidence storage meets. That means issues of environmental security and personnel access are addressed. However, it should be easier to manage access to archival storage, given that it will be accessed with less frequency and by fewer people.

Many organizations do establish a final date by which time the evidence is actually destroyed. This is usually many years after the end of a case. It could easily be decades. Whatever your organization's policy on evidence destruction is, it is critical that all evidence be completely destroyed. In the case of disks, those disks should be broken and then burned. In the case of magnetic storage devices (like hard drives), the device should be magnetically wiped and then physically broken. It is imperative that the evidence not be recoverable from the destroyed media.

Chapter Review

In this chapter, you have learned how to properly seize, store, and transport evidence. Chain of custody, a critical concept, can only be maintained by properly documenting all phases of the investigation, beginning with the seizing of the evidence and moving on through the storage and transporting of the evidence.
Questions

1. Which of the following best describes the primary purpose of write-protecting a drive?
   A. To ensure evidence is not accidentally added to or destroyed.
   B. To ensure evidence is not accidentally destroyed.
   C. To keep the investigator from installing utilities on the drive.
   D. It is required by most forensic imaging techniques.

2. Which of the following are the two types of write protection?
   A. Fast and slow
   B. Windows and Linux
   C. Hardware and software
   D. Forensic and nonforensic

3. Which of the following best describes the term capture point?
   A. The time of the suspect’s arrest
   B. The time the suspect is booked
   C. The time of entry into the facility to seize evidence
   D. The time when evidence is first seized

4. In which of the following cases would you log that evidence has transferred from one person to another?
   A. When checking evidence in initially
   B. When checking evidence out for court
   C. When evidence is checked out for analysis
   D. All of the above

5. What is RFI?
   A. Real-time forensic investigation
   B. Radio frequency interference
   C. Radio forensic investigation
   D. Real-time forensic initialization

6. What is EMI?
   A. Electromagnetic interference
   B. Emergency mobile investigation
   C. Electromagnetic investigation
   D. Emergency mandatory investigation
7. Which of the following is not an environmental danger to digital evidence?
   A. Fire
   B. Flood
   C. Extreme heat
   D. Loud noise

**Answers**

1. A. To ensure evidence is not changed in any way, whether added to or destroyed. Write-protecting keeps you from inadvertently adding or deleting data.
2. C. Hardware and software. In this chapter, you saw examples of hardware-based write protectors and software-based write protectors.
3. D. The time when evidence is first seized.
4. D. All of the above.
5. B. Radio frequency interference.
7. D. Loud noise. It should be obvious that noise does not disturb digital media.

**References**