

# The Nature of Digital Evidence

In this chapter, you will learn how to

- Define digital evidence and explain its role in the case of a computer security incident
- Discuss the characteristics of digital evidence and the various types of digital data
- Discuss Federal Rules of Evidence (FRE) and articulate the best evidence rule
- Summarize the international principles for computer evidence
- Differentiate between the Scientific Working Group on Digital Evidence (SWGDE) and the International Organization on Computer Evidence (IOCE)
- List the considerations for collecting digital evidence from electronic crime scenes
- Explain electronic crime and digital evidence consideration by crime category

The term *evidence* is another one of those slippery terms whose meaning depends on context, which is another way of saying that your definition of evidence may not be my definition of evidence. In this chapter, we will focus on the definition of “digital evidence” and how that evidence needs to be treated in order for it to be suitable for admission in court.

## What Is Digital Evidence?

We spent a good deal of time in the previous chapter talking about computer forensics. Early on, “computer forensics” seemed to be a good description for the application of forensic science to these particular devices (recall, too, that the definition of forensics is “presenting to a court”). As the types of devices that utilized digital communications and digital data increased, the phrase “digital forensics” became more popular, as it more precisely captured what the forensics investigator faced during an investigation. Consider that smart phones, tablets, laptops, netbooks, music players, and other devices are capable of using and generating digital data.

We represent digital data by a sequence of binary digits (a one or a zero), frequently abbreviated as bits: 8 bits are a byte; 4 bits are a nibble (seriously). These bits are only intelligible to us when we impose an agreed-upon structure (format) on that data and

we interpret data under the rules of that structure. Figure 2-1 shows a screen capture of a file containing ASCII text, with the binary values expressed in hexadecimal notation on the left and the ASCII representation on the right (hexadecimal notation is base 16, with values running from 0 to F; conveniently, a single hexadecimal character reflects 4 bits). Some of the bytes in the file don't have a printable representation, so we divide these characters into printable and nonprintable. Usually, the interpretation of digital data is done via a computer program, itself a collection of bits. Virtually anything can be represented digitally: audio, video, text, graphical images, and computer programs. Any and all of this information can be transmitted and stored as a collection of bytes, commonly referred to as a file.

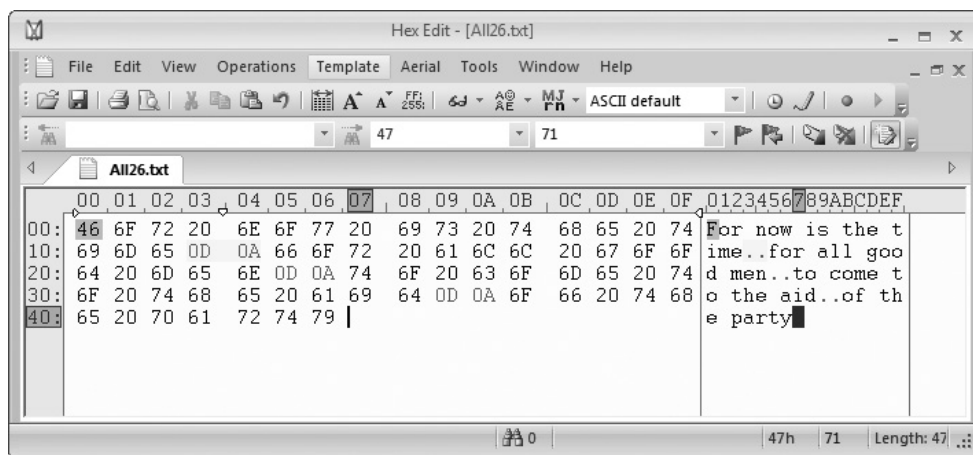
Digital data are quite different from what we are used to in the physical world. Digital data are ephemeral: They can be present one moment and gone the next. They are fragile; they are easily damaged or destroyed, but at the same time, they are very easy to copy.



**EXAM TIP** Know the characteristics of digital data, especially that they are fragile and easily damaged, but easy to copy and transmit.

Now that we have a working definition of digital data, we'll define a *digital investigation* as an effort that requires examination of a digital device because that device has been involved in a particular incident, which may be a crime. Our need to understand and explain a series of digital events motivates us to perform this investigation. We do this by developing a hypothesis regarding what might have happened and then searching for evidence that would refute that hypothesis.

*Digital evidence* is a digital object that contains reliable information that supports or refutes a hypothesis. This definition of evidence reflects its use in scientific investigations.



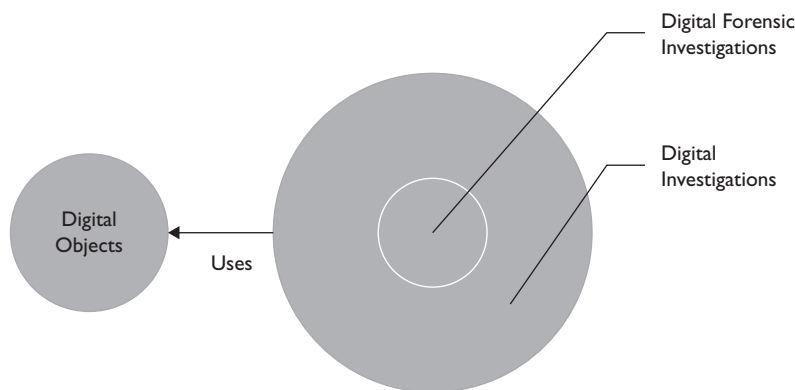
**Figure 2-1** Hexadecimal and ASCII representation

In the legal arena, digital or electronic evidence is “any probative information stored or transmitted in digital form that a party to a court case may use at trial.”<sup>1</sup> Digital forensics investigations thus are a “process that uses science and technology to analyze digital objects and that develops and tests theories which can be entered into a court of law to answer questions about events that have occurred.”<sup>2</sup>

Figure 2-2 shows the relationships between digital objects, digital investigations, and digital forensics investigations. Digital forensic investigations are a subset of digital investigations, with more constraints added by the forensic process itself. It follows that investigations and forensics investigations use digital objects, but how they use these objects will differ, depending on the type of investigation.

This helps to explain why you must take care in collecting, processing, and storing digital objects. Unless you’re very sure that the evidence you collect will not be used in court, it’s a very good idea to exercise due caution and care with the evidence such that you don’t do anything to preclude using that digital evidence in a courtroom. It’s certainly possible that an investigation that starts out as purely information gathering may turn into a criminal investigation.

What kind of digital objects might we encounter? The document “Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders”<sup>3</sup> lists 14 different crime categories and 60 different kinds of electronic crime and digital evidence. Of these 60 items, 43 of them are either digital devices or the input or output of digital devices. Financial records appear in 11 instances of criminal activities, while identity theft and prostitution are associated with 13 of the digital objects used in the commission of these crimes. Other potential sources of evidence include answering machines, audio recorders, external data storage devices, MP3 players such as the Apple iPod, multifunction machines, and pagers, among others. A quick rule of thumb is that if it’s an electronic device that can store information (even an electric alarm clock can do that), then it’s a potential source of evidence.



**Figure 2-2** Digital objects, digital investigations, and digital forensic investigations (Adapted from Carrier, B. *File System Forensic Analysis* (NJ: Pearson Education, 2005), p 4.)

## Anti-Digital Forensics

The worst mistake an investigator can make is to underestimate their adversary. Perhaps the best position to take is to assume that she is smarter than you are, has better equipment, and has more time and patience to commit the crime than you have to gather and analyze the available evidence. As in chess, don't depend on your opponent making the wrong move. But if they do, be prepared to capitalize on it.

Anti-digital forensics is a set of methods and tools that are used to destroy or obfuscate digital objects such that they cannot be used as digital evidence. We'll cover some of these techniques in future chapters, such as encryption, steganography, packing, compression, compression and encryption (in that order), the modification of file metadata (such as the MAC time—when the file is created, accessed, or modified), file erasure, and hidden file systems (such as those created by the *TrueCrypt* software). The results of using these techniques can result in no evidence that the file existed, the file existed but was erased (not just deleted), or the file exists but the content is inaccessible. Figure 2-3 shows the contents of a *TrueCrypt* file (container.dat) that has been formatted as a FAT32 file system protected by a password and has a second password-protected file system contained within it. Notice how the file appears to be random characters—exactly what you would like an investigator to see.

Take note that the previously mentioned anti-forensics techniques include techniques for ensuring privacy as well as personal information security. One provocative question is: Can you be forced to give up an encryption key? Or is it your Fifth Amendment right not to divulge this secret? In one case, the court ruled that if you had written down the password, you must reveal it, but if you had memorized the password, you did not have to reveal it.

Container.dat																
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00000000	54	FC	72	02	3D	D7	1A	F4	C8	3C	AE	C4	A8	AC	C8	07
00000016	00	3B	D0	D7	40	F8	C2	01	7D	20	35	21	6B	09	71	48
00000032	F8	E3	D4	3B	C2	E9	BF	39	85	3E	E0	D6	C7	B5	CC	27
00000048	34	09	4D	E9	26	5A	BD	19	77	76	59	2E	CE	28	ED	80
00000064	BC	CD	87	51	63	8F	F6	F2	BB	43	71	20	41	06	A3	E6
00000080	FC	91	D3	3F	C1	82	BD	9B	27	9B	FB	62	C9	0B	89	B0
00000096	32	4F	2B	5C	6C	54	75	32	EE	7E	FE	25	3B	AD	D9	00
00000112	FE	5F	BA	86	EF	42	B1	C7	BB	35	BB	83	C5	D4	96	AE
00000128	58	A3	E0	72	81	E1	DF	69	0E	47	5F	0C	94	07	57	1B
00000144	3D	62	91	E7	9F	96	C7	50	19	11	2A	EF	17	79	EF	A1
00000160	57	9E	34	2E	B4	30	EE	28	E5	EE	F9	9B	ED	7C	73	C2
00000176	25	62	17	05	EF	D7	BB	17	CA	34	BD	C8	D5	B4	96	4B
00000192	19	FC	44	7C	55	26	4A	34	68	D1	6A	8C	BB	D5	69	77
00000208	8D	DC	8B	2D	CB	21	5A	EB	3D	02	D0	86	46	01	A6	FE
00000224	F9	EB	53	5F	5C	8E	52	3B	DE	55	D1	50	30	7A	E6	CC
00000240	48	31	D5	A2	84	20	E3	73	8A	0D	C0	64	47	02	1E	4B
00000256	B5	3E	06	04	F6	D3	3C	04	66	05	77	31	69	D2	D7	35
00000272	FA	1D	65	37	B2	97	F3	84	D8	0E	77	41	D9	95	83	68
00000288	05	F3	99	CB	91	1A	48	D6	12	D0	CF	F5	1A	21	A9	49
00000304	1D	45	C2	08	BA	CA	9F	B7	4C	01	97	C9	17	CB	90	54
00000320	60	92	DB	BC	8B	6E	F7	6A	2A	11	E3	B4	F2	B5	A8	14
00000336	6E	61	D3	0B	16	C0	68	6E	52	9C	FA	48	10	AF	77	25
00000352	2F	A1	60	3B	FA	9B	E4	1F	1F	1C	C0	A4	D9	1D	2A	14
00000368	98	35	A6	35	5A	65	58	12	9E	ED	54	62	E8	30	26	3F
00000384	E7	A2	4F	0A	17	35	DC	93	39	85	E4	56	A5	0B	96	F3
00000400	2C	E9	A0	62	E7	6E	65	2E	E3	ED	8A	E2	94	50	7B	17

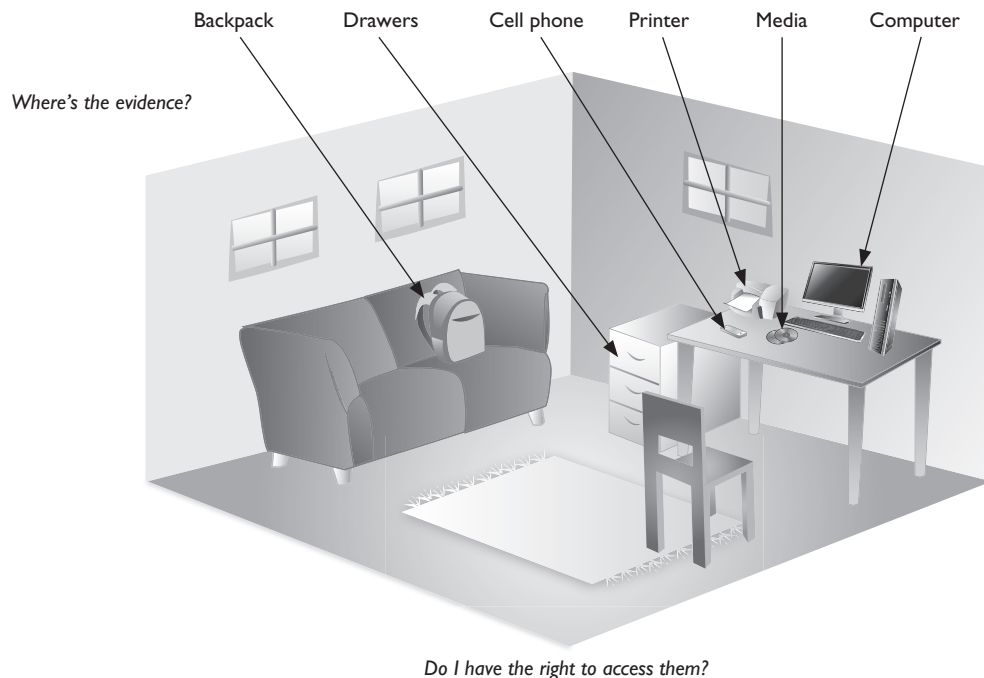
Figure 2-3 Contents of a *TrueCrypt* container

## Locard's Exchange Principle

You were introduced to Locard's exchange principle in Chapter 1: Every contact leaves a trace. How might this work in a crime scene that involves a computer? Consider this paragraph from Paul Kirk's *Crime Investigation* regarding Locard's exchange principle applied to a physical crime scene:

Wherever he steps, wherever he touches, whatever he leaves, even without consciousness, will serve as a silent witness against him his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, *it cannot be wholly absent* [my italics]. Only human failure to find it, study and understand it, can diminish its value.<sup>4</sup>

Imagine the following: We walk into a crime scene as presented in Figure 2-4. As a computer forensics investigator, we see several possible sources of digital evidence. DVDs, a printer, a desktop computer, and a cell phone. What about a network connection? Is the desktop computer powered on or powered off? Before we start collecting this evidence, we need to ensure that we don't disturb any physical evidence that is left



**Figure 2-4** Our imaginary crime scene

here, such as fingerprints, fiber evidence from a coat, or hair on the chair. And let's not forget what might be in the drawers or in the backpack on the sofa. The harder we look, the more we see potential sources for evidence that is either related to or generated by a digital device.

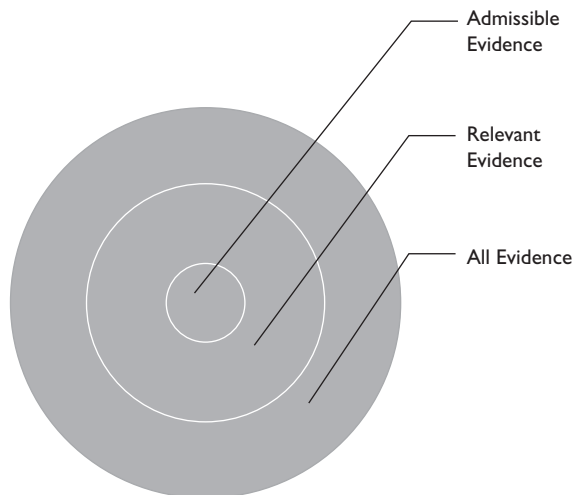
## Federal Rules of Evidence (FRE)

The Federal Rules of Evidence (FRE) are a collection of laws that determine what can or cannot be admitted into evidence in a federal courtroom. States are not required to use the same standards as presented in the FRE, but they are encouraged to do so, and many do. As always, as a digital investigator, you should know the rules of evidence for your local state or province. Copies of the FRE can be obtained from many locations; one such location is from the web site [www.uscourts.gov](http://www.uscourts.gov).

Let's assume that we've done our very best and collected all possible evidence found at our imagined crime scene as shown in Figure 2-4. We've done due diligence: We've been authorized to collect everything we've collected, we've worn gloves so as not to contaminate physical evidence, we've made a sketch, we've labeled everything appropriately, and we've photographed everything within the room. So we have everything we need, right?

Not necessarily. Figure 2-5 illustrates that only a subset of our evidence may actually be admissible, even though it's relevant, while some relevant evidence may not be admissible. One reason for this is Rule 802 from the FRE that states: "hearsay is not admissible unless any of the following provide otherwise: a federal statute, these rules; or other rules prescribed by the Supreme Court."<sup>5</sup> Hearsay is defined in Rule 801 as "a statement, that the declarant did not make while testifying at the current trial or hearing, and a party offers in evidence to prove the truth of the matter asserted in the statement."<sup>6</sup> It turns out that the declarant is not the person on the witness stand, but rather, the person who is supposed to have made the statement. Using a familiar poem

**Figure 2-5**  
Evidence, relevant  
evidence, and  
admissible  
evidence



as an example, the speaker in “’Twas the Night Before Christmas” is not the declarant, but rather Santa Claus, who exclaimed (as he drove out of sight) “Merry Christmas to all, and to all a good night.”

## Computer-Generated vs. Computer-Stored Records

When it comes to computers, it’s not possible to present the actual information stored on the computer. Instead, we need to generate some tangible output based on the information, such as a printed document or a picture. This leads us to the difference between computer-generated records and computer-stored records. According to the U.S. Department of Justice (DOJ), computer-generated records are those records produced by a running computer program, while computer-stored records are records or documents (files) containing information created by a human author.<sup>7</sup> Computer-stored records are generally considered hearsay; computer-generated records, however, are increasingly likely to be recognized as acceptable, especially if they are produced as part of “regularly conducted business activity (FRE 803(6)).” A good example of this is logging, whether it be at a system-wide level, as would be the case with a Security Information and Event Management (SIEM) installation, or on a local workstation, such as the various Windows event logs. A word of caution, however. Logging that takes place only when an event is observed or log levels are increased may not be admissible since it isn’t part of “normal business processes.” However, if increased logging is part of a standard, documented process for incident response, then the evidence may be admissible.



**EXAM TIP** Know the difference between computer-generated records and computer-stored records. Computer-generated records have been created by a running software program; computer-stored records have been

generated by a person. An easy way to remember the difference between the two is that only people go to the store.

Computer-generated records must be authentic, or identified.<sup>7</sup> The authenticity (identification) of that computer-generated record can be established by the testimony of the individual who caused that record to be created. For example, a systems administrator could testify that she had initiated packet capture on the computer’s Internet-facing network interface and had captured this information to a file on a RAID 1 storage array. Chain of custody contributes to the authenticity of these records as well. Chain of custody is a documented record of who had possession and control over a particular piece of evidence at every moment until that object is entered into evidence in the courtroom. It is critical that this chain of custody be documented by a relevant form (the chain-of-custody form). Standard formats exist for these kinds of forms. The primary details are the date and time of transfer, who provided and who received the evidence, and the purpose of the transfer (for example, Dick transferred the CD-ROM containing the log files to Jane on January 3, 2013, at 3:00 PM EST for the purpose of analysis). Chain of custody is a significant portion of the entire chain of evidence. A chain-of-evidence form includes the search and seizure of that evidence and the cataloging of that evidence, as well as the chain of custody of that evidence once it has been obtained. Figure 2-6 is an example of a chain-of-custody form. Take particular notice of

Property Record Number: \_\_\_\_\_

Anywhere Police Department  
**EVIDENCE CHAIN OF CUSTODY TRACKING FORM**

Case Number: \_\_\_\_\_ Offense: \_\_\_\_\_  
 Submitting Officer: (Name/ID#) \_\_\_\_\_  
 Victim: \_\_\_\_\_  
 Suspect: \_\_\_\_\_  
 Date/Time Seized: \_\_\_\_\_ Location of Seizure: \_\_\_\_\_

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

**Figure 2-6** Chain-of-custody form (Source: "Sample Chain of Custody Form," NIST. Retrieved from <http://www.nist.gov/oles/forensics/upload/Sample-Chain-of-Custody-Form.docx>.)



the information at the top of the form, items like property record number, case number, date and time seized, location of the seizure, and the list and item numbers of this evidence. All of this information provides us with the ability to trace a particular piece of evidence within the criminal justice system.

After all that, is our evidence reliable? That is, does the software that generated the evidence produce evidence that can be relied on? An example of that is data that are generated by a program that is part of ongoing business processes and that are utilized for other purposes within the organization. Consider an event file that records time of user login and logout, which in turn is processed to generate usage reports for particular individuals for charge-back purposes. If this event file were used as evidence, the fact that it had been used as part of normal business purposes for a second purpose would indicate that the information contained within that file was considered reliable. Proving that the program produces accurate results can also improve the chances of admission of computer-generated records that aren't usually collected as a part of normal business processing.

## Essential Data

Another characteristic of computer information is that the data that we gather and use must be essential. Essential data are digital data we can trust. Brian Carrier, in his book *File System Forensic Analysis*, uses the example of a file content address.<sup>2</sup> We can trust that data because if they were not true (accurate), then neither we nor the suspect could have accessed that digital object. Nonessential data simply are data that we can't trust because they may have been modified, or they may have never been created in the first place. Reconsidering our example of modifying MAC times on a file, we realize that these values represent nonessential data because we ultimately can't trust these values (it may be true that our adversary is clever enough that the times have been changed such that they seem plausible but completely hide the exact order of events). Nonessential data may be correct most of the time, but it's worth looking for other evidence that supports that assessment (corroborative evidence).

One last complication: We may trust a piece of essential data (a file content address) but we may not trust the data referenced by a file content address. Metadata for a deleted file may indicate that the file contents were located at file content address 3589, but the data that reside there may now be part of a different file because the file blocks associated with the address have been assigned to another file.

## Best Evidence

When presenting evidence in court, you're required to present the best evidence. FRE 1001 defines the best evidence for a computer thusly: "For electronically stored information, any 'original' means any printout—or other output readable by sight—if it accurately reflects the information."<sup>8</sup>

The best evidence rule applies when a party wants to admit as evidence the contents of a document at trial but the original document is not available. In this case, the party must provide an acceptable excuse for its absence. If the document itself is not available and

the court finds the excuse provided acceptable, then the party is allowed to use secondary evidence to prove the contents of the document and have it admissible as evidence. The best evidence rule only applies when a party seeks to prove that the contents of the document ought to be admitted as evidence.<sup>9</sup>

Think about the case when we have created a memory dump from a suspect's computer. In this case, the best evidence would be the actual contents of the computer memory at the time of capture. Failing that, however, we can use the contents of our memory dump as secondary evidence. Likewise, we can introduce a listing of network connections as evidence even though we lost the actual connections once the computer shut down. There are simply times when providing the original of the evidence is impractical, such as a rack of blade servers, or a series of disk tray cabinets in large storage array networks (SANs). Since seizing the physical devices is impractical, a forensic copy of that device must be created as a bit-for-bit forensic image, and this requirement has a specific impact on how the copy is made, as we'll see in our chapter on acquiring evidence.

## **International Principles of Computer Evidence**

As the number of PCs and workstations in use increased during the 1990s, so did the recognition that standards should be developed internationally in order to facilitate communication and sharing of information, as well as to standardize procedures. We'll focus on two organizations in this section: the International Organization on Computer Evidence (IOCE) and the Scientific Working Group on Digital Evidence (SWGDE).

### **International Organization on Computer Evidence**

The IOCE was organized in the mid-1990s in order to develop international standards regarding computer evidence. By the time the group produced the document "Guidelines of Best Practice in the Forensic Examination of Digital Technology" in 2002, the notion of computer evidence had already been replaced with the more generic category of digital evidence. The guidelines cover a range of best practices for implementing a forensics capability, and include equipment, training, and organizational needs.

### **Scientific Working Group on Digital Evidence**

The SWGDE was organized in 1999 to act as the U.S. representative of the IOCE. By the time the SWGDE came into existence, the notion of computer evidence had been subsumed by the notion of digital evidence. SWDGE published their first document in 2003 and has been active since then. They have published papers on audio forensics, cell phone forensics, and general digital forensics. Table 2-1 lists a selected set of publications that are available on their web site ([www.swdge.org](http://www.swdge.org)).

Date	Title	Purpose
02-11-2013	SWGDE Best Practices for Computer Forensics V3-0 (released for public comment)	Preferred methods for conducting the computer forensics process
02-11-2013	SWGDE Best Practices for Mobile Phone Examinations V2-0	Preferred methods for conducting forensics investigations of mobile phones
02-11-2013	SWGDE Best Practices for Vehicle Navigation and Infotainment System Examinations V1-0	Preferred methods for extracting information from navigation, information and entertainment system
02-11-2013	SWGDE Core Competencies for Mobile Phone Forensics V1-0	What mobile phone DFIs need to know to perform their duties
04-08-2013	SWGDE-SWGIT Glossary V2.7	Definitions for image, video and forensic audio analysis as well as computers
06-04-2012	SWGDE Best Practices for GPS Devices V1.0	How to examine global positioning systems (GPS) devices
09-15-2011	SWGDE Core Competencies for Forensic Audio V1.pdf	Skills and information needed by forensic audio investigators.
05-15-2010	SWGDE Technical Notes on Microsoft Windows 7	How XP, Vista, and Windows 7 differ
01-28-2008	Capture of Live Systems V1.0	How to capture live data from computers

**Table 2-1** Selected Publications (Available from SWGDE. Adapted from “Public Documents,” Scientific Working Group on Digital Evidence. Retrieved from <https://www.swgde.org/documents/Current%20Documents>.)

## Evidence Collection

We spent the beginning of this chapter discussing the nature of digital evidence and how that evidence can be admitted into a courtroom. The first thing that has to be done is that the evidence (by which I mean the sources of the evidence) must be handled in a particular way. We’ll go into the mechanisms of this in our next chapter, but for the moment, let’s consider some general rules for actually collecting the evidence.

There are two ways to acquire evidence: via a live collection or a dead collection. Live collections occur when the computer in question is running the operating system (OS) installed on that computer. This means that data collection goes on using the resources of the computer itself (memory, the network, etc.) and that the investigator is logged in to machine, either via the console or remotely using remote login software. Dead collections, on the other hand, utilize an OS that is not running on the machine in question; rather, the OS has been started from a floppy disk, or more likely these days, from a live CD-ROM or a universal serial bus (USB) thumb drive. In this case, we can access the persistent storage of the computer, but we’ve lost the volatile information such as the contents of memory, network connections, running processes, etc.

Let's add another dimension to this activity, namely the role of the forensic investigator versus the role of the incident responder. We've already learned the difference between them. In the case of incident response, we're looking for digital evidence that can help us determine the root cause of the event that concerns us.



**NOTE** I think of this as the “stop the bleeding” approach. What's of greater concern: terminating the attack or finding evidence with which to prosecute and ultimately convict the attacker? In the case of discovering an ongoing attack, the initial impulse usually would be to terminate that attack to minimize the loss to the business. And in so doing, the investigator may modify the data such that they no longer have value as forensic evidence. The first responder must weigh the cost of allowing the attack to continue versus the collection of critical evidence.

Whether you are acting as a forensic investigator or as an incident responder, your first rule is to be circumspect in what you're doing. In other words, don't make a mess at the crime scene by acting like a bull in a china shop. Understand your role as part of the forensics team that will be examining the crime scene. Be careful that you don't destroy latent evidence or contaminate the evidence by adding your own physical traces to the scene (remember, Locard's principle applies to you as well). As Eoghen Casey notes, the evidence we collect must be relevant, authentic, and integral, and must have been collected and stored in a forensically sound manner.<sup>1</sup> Evidence is relevant if it has probative value, that is, a direct bearing on the incident in question. It must be authentic: We have to ensure that it hasn't been tampered with, and integral to that, the integrity of the evidence cannot have been compromised. We do this by following specific procedures to seize and collect that evidence, documenting those efforts, and recording our efforts in chain-of-evidence forms and chain-of-custody forms. Simply speaking, a chain-of-evidence form reflects the entire history of a piece of evidence, while the chain-of-custody form documents who has had possession of the evidence at every moment since it was “bagged and tagged” until the evidence is entered into the courtroom proceedings.

## **IOCE Guidelines for Recovering Digital Forensic Evidence**

The IOCE Guidelines outline the following general principles for recovering digital forensic evidence:

1. The general principles, that have been adopted as G8<sup>9</sup> recommendations relating to digital evidence, that should be followed by forensic laboratories are as follows:
  - a. The general rules of evidence should be applied to all digital evidence.
  - b. Upon seizing digital evidence, actions taken should not change that evidence.
  - c. When it is necessary for a person to access original digital evidence that person should be suitably trained for the purpose.

- d. All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
  - e. An individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.
2. All activity relating to the seizure, examination process, and presentation of evidence access, storage, or transfer of digital evidence must be documented, preserved, and available for review.
  3. Responsibility for maintaining evidential value and provenance is a personal, not corporate issue. If an individual has acknowledged responsibility for an item by signing an access log they are responsible for all actions taken in respect of that item until such time as it is returned to storage or formally transferred to another individual.<sup>10</sup>

No surprises here.



**NOTE** G8 is the Group of Eight, an organization consisting of eight countries with the largest economies.

## The Scientific Method

Motivating the underlying principles for collecting digital evidence is a process of discovery labeled the scientific method. Remember that the scientific method is a way by which we can test out our ideas of why and how a particular event occurred. There are a number of definitions of the scientific method, and while they may vary in terminology, most definitions will include most if not all of the steps listed here.

1. Define a question/accept a question. Gather information and resources (observe). Some people consider gathering information to be a separate step.
2. Form an explanatory hypothesis.
3. Test the hypothesis by performing an experiment and collecting data in a reproducible manner.
4. Analyze the data.
5. Draw conclusions. These may support or contradict your original hypothesis. If the data and your conclusions do not support your hypothesis, go back to step 2.
6. Communicate results (report).

We will go into more depth regarding the scientific method in our chapter on the forensic investigation process and show how forensics investigations mirror the steps outlined here.

## Consider a Scenario

Consider an incident response scenario that illustrates these steps. Joe Sample has been called in to investigate a possible compromise of a critical server. The immediate question is was this server compromised, and, if so, what was the attack vector (how did the attacker gain access to the server?). Joe isolates the server from the rest of the network while still permitting network communications and begins a live analysis of the running machine, making sure to document any action that would change the state of the machine.

Joe's initial hypothesis is that access to the machine was via the network. His first action, however, is to examine the login history via the console. He notes that there are no recorded logins for the past several weeks, and he then checks to see if anyone has tampered with the logs on the server. They have not, so Joe discards the alternative hypothesis that the machine was compromised via console access.

Joe examines the list of running processes and sees nothing amiss. He continues to search the log files for login attempts (successful or unsuccessful) and discovers that an SSH (secure shell) session had been initiated three days ago from one of the internal networks that had access rights to the server. Joe is surprised to see the login name, as he knew all of the other employees who were authorized to access that server, and this individual wasn't one of them. He checks the `/etc/passwd` file (yes, the server is a Linux machine) and discovers that this user does indeed have a valid account that has been created with group membership that provides extended administrator privileges.

Joe stops for a minute to catch his breath and take stock. Given the configuration of the server, access had to come from either the console or from the network via an SSH session. No logins via the console were recorded during the period he was investigating, so the access had to be from the network. Joe has discovered that there was a suspicious login (an unauthorized user) from an internal machine.

Joe considers his options. He can turn his attention to what had occurred during that login session on the server. He could investigate the machine that was the source of the login. Or he could report back to his manager that the machine does appear to have been compromised (unauthorized access) and they should reimage the machine.

As an investigator, are you going to follow each of the previous steps in exact detail? Probably not. Remember that your investigation is in response to a question and that you are investigating a specific hypothesis (a hypothetical explanation) of what occurred. Remember our old friend 5WH.

## Exculpatory Evidence

Evidence takes on two forms: inculpatory evidence and exculpatory evidence. Inculpatory evidence is evidence that tends to show that the defendant is guilty or had criminal intent, and supports our initial hypothesis about what may have happened. On the other hand, exculpatory evidence is "evidence, such as a statement, tending to excuse, justify, or absolve the alleged fault or guilt of a defendant" ([www.law.cornell.edu/wex/exculpatory\\_evidence](http://www.law.cornell.edu/wex/exculpatory_evidence)). Applying this to our scientific method, exculpatory evidence would be evidence that disproves or fails to support our current hypothesis (although an absence of evidence doesn't necessarily mean that the hypothesis is wrong). In the

previous example, the absence of log records for a console login during a given time period disproves (fails to support) the hypothesis that the server was compromised via a console login. This isn't always easy to do in the heat of an investigation. We all tend to look for evidence that supports our current notion of what is happening or has happened (otherwise known as confirmation bias).

## Chapter Review

Digital evidence refers to digital objects that help an investigator support or disprove a hypothesis. Digital evidence is easily modified, easily copied, very volatile (consider computer RAM), and can come in many forms: images, video, audio, documents, databases, etc. Certain types of digital evidence are often associated with particular types of crime. According to the National Institute of Justice (NIJ), the most popular piece of digital evidence across all crime categories is financial records, while prostitution and identity theft utilize the most number of digital materials. It's a wired, wired world we live in!

The Federal Rules of Evidence (FRE) are a set of criteria that determine what things can be admitted as evidence in a federal court. The best evidence rule simply states that the original evidence is preferred over a copy unless a copy is specifically allowed. The international principles for computer evidence, as established by the IOCE, establish a framework for each member state to develop standard operating procedures (SOPs) for the entire digital forensics process. The Scientific Working Group on Digital Evidence (SWGDE) is the U.S. representative to the IOCE and is charged with disseminating best practices for the collection and protection of digital evidence.

When collecting digital evidence from electronic crime scenes, take care not to destroy physical evidence associated with the digital equipment, have a plan regarding which evidence should be seized, and try to preserve the digital device in the state it was found.

## Questions

1. Digital evidence is best described as:
  - A. The entire contents of the physical recording medium (disk, USB stick, floppy disk, etc.)
  - B. Any binary data file
  - C. A digital object that supports our investigation and can either support or disprove our original hypothesis
  - D. A digital object generated by systems software
2. During a security incident, digital evidence helps in determining:
  - A. How a system was compromised
  - B. What data was compromised
  - C. When the system was compromised
  - D. All of the above

3. Which is *not* an instance of digital evidence?
  - A. Audio files
  - B. Image files
  - C. System software
  - D. Microsoft Word documents
4. True or false: The presence of financial records at a crime scene means that they were used in committing the crime.
  - A. True
  - B. False
5. The best evidence rule intends to:
  - A. Eliminate all copies as possibly forged
  - B. Only allow a single piece of evidence that demonstrates the defendant's guilt or innocence
  - C. Provide the original item if at all possible
  - D. Prevent contamination of evidence while in custody
6. True or false: In the United States, the Federal Rules of Evidence are required to be used by the states.
  - A. True
  - B. False
7. Which of the following is *not* a consideration when collecting digital evidence from a crime scene?
  - A. Preservation
  - B. Documentation
  - C. Transfer
  - D. None of the above
8. What is the difference between a computer-stored record and a computer-generated record?
  - A. Computer-stored records are always readable text files.
  - B. Computer-generated records can be interpreted only by another computer program.
  - C. A computer-generated record is generated by normal business processes and not directly by a person.
  - D. Computer-stored records are created on one computer and then moved to another.



9. What is the first step of any digital investigation?
  - A. Turn all machines off that may contain digital evidence.
  - B. Plan your strategy based on the information that you've been provided concerning the case.
  - C. Assign different people responsibilities for collecting data from different digital devices.
  - D. Allow the physical forensics team to transport the digital devices to the lab to search for physical evidence.
10. What is the difference between a live investigation and a dead investigation?
  - A. Live investigations require the presence of an investigator, while dead investigations can be automated such that no investigator needs to be present.
  - B. Live investigations only consider evidence that is transient and may be destroyed when the computer is turned off.
  - C. A live investigation collects evidence from a running computer. A dead investigation collects evidence from persistent storage associated with that computer when the computer isn't running.
  - D. Live investigations require the consent of the owner; dead investigations do not.
11. John logged in to a running compromised server and began recording open files, users logged in, network connections, running processes, etc. Once he had satisfied himself that the machine was locked down and no longer under attack, he shut down the machine and rebuilt the machine from backups. What was John doing during that time?
  - A. Performing a digital forensics investigation
  - B. Performing a digital investigation
  - C. Standard system maintenance
  - D. None of the above
12. After determining that an attack was in progress, John, in accordance with the company's incident response policy, turned up the logging level on the network in order to collect extra information. Is this information admissible in court?
  - A. Yes. All log records are admissible, regardless of when or how they are collected.
  - B. No. Information collected in special circumstances that is not part of standard business activities is never admissible.
  - C. Maybe. The evidence could be admitted if the collection method was used as part of an incident response action.
  - D. Not enough information to tell.

## Answers

1. C. Digital evidence is any digital object that we can use to support our investigations.
2. D. Digital evidence could supply information leading to the determination of what data was compromised, how access was obtained, and when it happened.
3. C. System software would not be considered digital evidence, since it has no probative value with respect to a potential incident.
4. B. These financial records would have to be tied to the crime itself; the presence of such records doesn't mean that they are always related to a crime.
5. C. The intent of the best evidence rule is to provide the original item if at all possible.
6. B. In the United States, it is highly recommended, but not required, that the states use that same standard for evidence.
7. D. Preservation, documentation, and transfer are all considerations when collecting digital evidence.
8. C. Software running on a particular machine can produce computer-generated records and these records can be introduced as evidence, provided they are part of normal business processing. Computer-stored records, on the other hand, can be denied based on the rule of hearsay.
9. B. The first step in any investigation is to plan and prepare your strategy based on the information provided to you about the incident.
10. C. We perform live investigations on a running computer that is running the OS native to that given machine. Dead investigations do not utilize the OS installed on the computer, but instead use an OS that is loaded from an external data source, like a live CD, floppy disk, or USB stick.
11. B. John was performing a digital investigation, since there was no effort made to collect the information using sound forensics procedures and the machines were wiped and rebuilt immediately thereafter.
12. C. The evidence may be admissible, given that turning up the logging level on the network is part of a defined business process (the company's incident response policy).

## References

1. Casey, E., *Digital Evidence and Computer Crime*, Third Edition (MA: Academic Press, 2011).
2. Carrier, B., *File System Forensic Analysis* (NJ: Pearson Education, 2005), pp. 4–5.

3. "Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders, Second Edition," National Institute of Justice (NIJ). Retrieved from [www.nij.gov/pubs-sum/227050.htm](http://www.nij.gov/pubs-sum/227050.htm).
4. Kirk, P. L., *Crime Investigation*, Second Edition (NY: Wiley, 1974), p. 2.
5. "Rule 802: The Rule Against Hearsay," Cornell University Law School. Retrieved from [www.law.cornell.edu/rules/fre/rule\\_802](http://www.law.cornell.edu/rules/fre/rule_802).
6. "Rule 801: Definitions that Apply to this Article; Exclusions from Hearsay," Cornell University Law School. Retrieved from [www.law.cornell.edu/rules/fre/rule\\_801](http://www.law.cornell.edu/rules/fre/rule_801).
7. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Cases, Washington, DC: USDOJ, 2009), p. 192. Retrieved from <http://www.usdoj.gov/criminal/cybercrime/docs/ssmanual2009.pdf>.
8. "Require the Original," Cornell University Law School, accessed July 2013 at [www.law.cornell.edu/rules/fre/rule\\_1002](http://www.law.cornell.edu/rules/fre/rule_1002).
9. "Best Evidence Rule," Cornell University Law School. Retrieved from [www.law.cornel.edu/rules/fre/rule\\_1001](http://www.law.cornel.edu/rules/fre/rule_1001).
10. "Guidelines for Best Practices in the Forensic Examination of Digital Technology," International Organization on Computer Evidence. Retrieved from [www.ioce.org/fileadmin/user\\_upload/2002/ioce\\_bp\\_exam\\_digit\\_tech.html](http://www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_digit_tech.html).

