CHAPTER

17

Reconstructing Digital Evidence

Eoghan Casey

Key Terms

Cybertrails; Digital evidence; Internet Protocol (IP) address

Information is flowing through wires and air all around us, from one computing device to another, frequently finding a resting place on storage media along the way. Given the ubiquity of digital data, criminal activity today often leaves digital traces stored on or transmitted using computers. Law enforcement and regulatory agencies have recognized that they cannot afford to overlook these traces and are therefore devoting resources to the collection and forensic examination of **digital evidence**. The resulting evidence provides an abundance of information that can be useful when investigating a crime. Even if digital evidence does not contain the "smoking gun," it can reveal actions, positions, origins, associations, activities, and sequences useful for reconstructing the events surrounding an offense.

Forensic examiners of computer systems are called on to answer both simple and complex questions relating to crimes. Investigators may need to know something as simple as whether a particular document can be located on a computer or when the document was created or printed. In some cases, digital evidence may provide a decisive lead, such as the floppy diskette that was sent by the Bind Torture Kill (BTK) serial killer to a television station and contained data that led investigators to a computer in the church where Dennis Rader was council president. Computers also have physical properties that can be embedded in the digital evidence they produce. The electronics in every digital camera has unique properties that specialized forensic analysts can utilize to link digital photographs to a specific device (Fridrich et al., 2005; Geradts et al., 2005). Some color printers place their serial number on pages in millimeter-sized yellow dots that are only visible under certain light frequencies, enabling investigators to associate an item with a particular printer (Tuohey, 2004). A person's Internet communications and digital documents contain verbal evidence that forensic linguists can analyze to learn more about a victim or offender (Chaski, 2005).

Information stored and created on computers can be used to answer fundamental questions relating to a crime, including what happened when (sequencing), who was responsible

DOI: 10.1016/B978-0-12-386460-4.00017-5

(attribution), and the origination of a particular item (evaluation of source). At the same time, the complexity of computer systems requires appreciation that individual pieces of digital evidence may have multiple interpretations, and corroborating information may be vital to reaching a correct conclusion. Forensic examiners need to understand, and make regular use of, the scientific method to ensure that conclusions reached are solidly based in fact. Familiarity with the limitations of forensic examinations of digital evidence will help investigators and attorneys exculpate the innocent and apprehend modern criminals.

This chapter presents the use of digital evidence to reconstruct actions taken in furtherance of a crime, providing case examples to demonstrate key concepts. The focus of this chapter is on how digital evidence can be useful in violent crime investigations. Specifically, this chapter describes how digital evidence that is handled and interpreted properly can be used to apprehend offenders, authenticate documents, assess alibis and statements, and determine intent. Other approaches to analyzing digital evidence and underlying technical details are beyond the scope of this text. For more in-depth, technical coverage of how forensic science is applied to computers and networks, see Casey (2004).

OVERVIEW OF DIGITAL EVIDENCE

Computers can be involved directly in many types of criminal activities, including terrorism, organized crime, stalking, and child exploitation. For example, sex offenders and obsessional harassers use computers to threaten and control victims, making the computer an instrument of the crime as well as the storage container of evidence relating to the crime. For forensic purposes, it is generally not computers themselves that are of primary interest but, rather, data they contain. Digital evidence is defined as any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense, such as intent or alibi (Casey, 2004). Homicide, sexual assault, and other violent crimes can involve digital evidence from a wide range of sources, including personal computers, handheld devices, servers, and the Internet, helping investigators reconstruct events and gain insight into the state of mind of individuals.

The digital footprints we leave as we move through the world create **cybertrails** that investigators can retrace to determine what we were doing, where, and when. Third parties, such as mobile telephone providers, banks, credit card companies, and electronic toll collection systems, can reveal significant information about an individual's whereabouts and activities. The computers we use at home and work contain remnants of documents, photographs, Internet communications, and other details that generally reveal a great deal about our daily life, inner thoughts, and motivations. Data that have been "deleted" often remain on a computer indefinitely, and technically savvy individuals can store data in unused areas of a hard disk. A victim's handheld device may contain entries or photographs that indicate where she was or who she met at a particular time. Records from a missing person's mobile telephone provider or car navigation system may indicate where he went. Computers could contain details about a murder plot, from a to-do list in a personal digital assistant to communications between coconspirators. A trained forensic examiner can recover and use these data to reveal evidence that a criminal sought to hide and glean a great deal about an individual and his activities.

When a large quantity of digital evidence is involved, forensic examiners employ key word searches and other data reduction techniques, as well as reconstruction tools such as timelines and link charts. Some link analysis tools can import e-mail and other digital data to help investigators identify patterns and relationships. Figure 17.1 depicts an example of how the contents of a short message service (SMS) message found on the victim's phone could lead to a suspect and how the locations of mobile telephones could be used to place the suspect at the crime scene.

Some forms of digital evidence contain additional information, called metadata, that specialists can extract to aide an investigation. Consider the following data embedded in a Microsoft Word document extracted using Metadata Assistant (www.payneconsulting.com), which reveals when the document was originally created, when it was last modified and printed, the various file names of the document, and the names of the last 10 authors:

Document Name: suicide-note.doc
Path: C:\Documents and Settings\Jane Doe\Desktop\
Document Format: Word Document
Built-in Document Properties:
Built-in Properties Containing Metadata: 3
Title: Note
Author: John Doe
Company: Personal
Document Statistics:
Document Statistics Containing Metadata: 6
Creation Date: 7/22/2005 4:31:00 PM
Last Save Time: 6/19/2005 1:58:00 PM
Time Last Printed: 6/19/2005 1:44:00 PM
Last Saved By: Jane Doe
Revision Number: 3

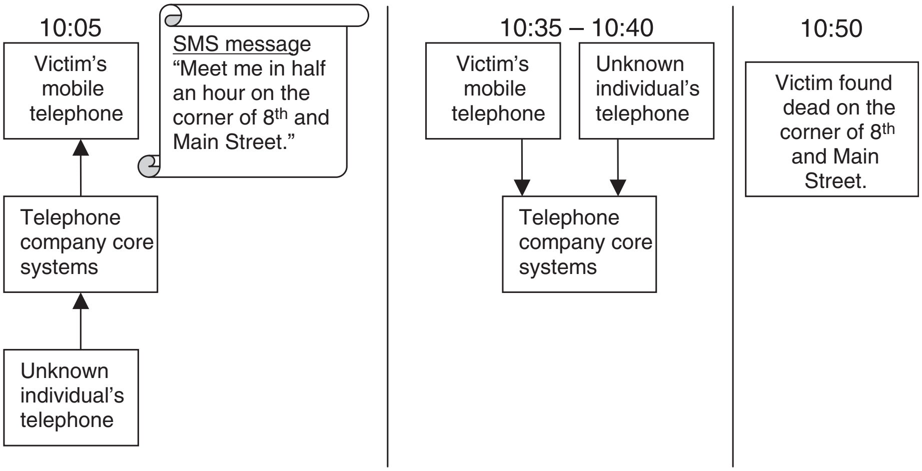

10:05
Victim's mobile telephone
SMS message
"Meet me in half an hour on the corner of 8th and Main Street."
Telephone company core systems
Unknown individual's telephone
10:35 – 10:40
Victim's mobile telephone
Unknown individual's telephone
Telephone company core systems
10:50
Victim found dead on the corner of 8th and Main Street.

FIGURE 17.1 Links between victim and suspect established using an SMS message and the location of the mobile telephone at given times.

```
Total Edit Time (Minutes): 5 Minutes
Last 10 authors:
Has Last 10 Data
Author: John Doe Path: A:\note.doc
Author: John Doe Path: C:\Documents and Settings\John Doe\Application Data\Microsoft
\Word\AutoRecovery save of note.asd
Author: John Doe Path: A:\note.doc
Author: Jane Doe Path: A:\note.doc
Author: Jane Doe Path: C:\Documents and Settings\Jane Doe\Desktop\ suicide-note.doc
Track Changes:
Tracked Changes: 1. Tracked Changes are On.
1 Type: Delete Author: Jane Doe
My husband did not kill me.
Location: Main Text
```

This type of embedded metadata can answer a variety of questions regarding a document, including its provenance and authenticity. For instance, although this document appears to have been last printed and saved on 6/19/2005, the original creation date suggests that it was not created until more than 1 month later on 7/22/2005. This date sequence is explained through examination of the last 10 authors, which reveals that the document named "note.doc" was originally created on a floppy diskette using John Doe's computer (corresponding to the "Creation Date" of 7/22/2005) and was subsequently transferred to Jane Doe's computer, where it was saved as "suicide-note.doc" and given a "Last Saved Time" on 6/19/2005, possibly because the clock on Jane Doe's computer had been backdated. Metadata also show that the line "My husband did not kill me" was deleted from the document at some time. A forensic examination of the computers and floppy diskette would likely uncover remnants of the note on the husband's computer, additional temporal information showing when the document was actually created and transferred onto the wife's computer, and other data that would help determine who wrote the note and gain insight into the author's intent.

As another example of the investigative usefulness of digital evidence, e-mail and AOL Instant Messages provided the compelling evidence to convict Sharee Miller of conspiring to kill her husband and abetting the suicide of the admitted killer (an ex-cop named Jerry Cassaday), whom she had seduced. Miller used their Internet correspondences to control Cassaday's perception of her husband, as demonstrated in the following excerpt from one of their online chat sessions (Bean, 2003).

> [Sharee Miller] twice told Cassaday she was pregnant with his babies—even though she'd had her tubes tied after her third child. In a chat session on Sept. 23, 1999, Miller wrote, "This next part will be hard—I lost my baby, Jerry."
>
> "No," Cassaday replied.
>
> "I never thought I would ever tell you that he hits. I got in trouble because I was with you," she continued. Cassaday wanted to know more.
>
> "Sharee, you can tell me now, or in person when I beat it out of him."
>
> "It made me start having bad thoughts of killing him," she wrote.
>
> "Where did he hit you?" Cassaday asked.
>
> "Jerry, I can't tell you." But Cassaday insisted.
>
> "He didn't hit me, Jerry; he raped me—I lost the baby because of the force."

In another case, the murderer's work computer revealed his intent to commit a crime, and his home computer contained a fake suicide note created after his wife's death (*State of South Dakota v. William Boyd Guthrie*, 2001). On May 14, 1999, Doctor Guthrie, a Presbyterian minister, called 911 for emergency assistance because his wife Sharon was unconscious in the bathtub. Sharon later died in the hospital. Based on the amount of temazepam and other agents in her system, a forensic pathologist determined that her death was not natural and not accidental, but from the autopsy alone he could not resolve whether it was suicide or homicide. A computer specialist examined the contents of the computer in William Guthrie's church office and found evidence of numerous Web searches on subjects related to household accidents, bathtub accidents, and prescription drugs. Some of these Internet activities occurred at approximately the same times as earlier suspicious accidents in the Guthrie household. In April 1999, 2 days after Web pages describing various drugs including temazepam were viewed on the computer in the church office, William Guthrie visited his doctor complaining of insomnia and persuaded the doctor to prescribe him temazepam. The defense argued that Sharon Guthrie had committed suicide and produced a purported suicide note that Guthrie claimed he discovered in his church office 3 weeks after Sharon drowned. The unsigned note was dated the day before Sharon's death and was addressed to her daughter. The note, replicated here with its spacing and typographical errors, was apparently created on a computer:

> May 13,1999
> Dear Suzanne,
> I am sorry I ruined your wedding, Your dad told me about your concerns of my Interfering in Jenalu's and the possibility I might ruin hers. I won't be there so Put your mind at ease. You will understand after the wedding is done. I love you all Mom.

Because there was insufficient time for experts to examine all of the fingerprints on the note, only four fingerprints were analyzed, none of which could be attributed to a specific individual. The computer specialist was called on again, this time to examine Guthrie's home computer, and he found an earlier draft of the suicide note. However, the file on the computer had been created on August 7, 1999. William Guthrie denied that he created this note but admitted to creating another note on August 11 that was found on his home computer with Sharon again as the purported author. It listed various grievances Sharon addressed to Guthrie, including one line that stated, "I'm upset that you have had an affair and have not come clean with me, I have thought of ending my life and you would have to face up to it. Believe me I known how to do it." Guthrie claimed that he wrote this note to work through the emotional trauma of Sharon's death. William Boyd Guthrie was convicted of first-degree murder for the killing of his wife.

William Guthrie was evidently unaware of the digital traces he was leaving behind. As criminals become more aware of these cybertrails, however, they are taking steps to conceal their digital footprints. This concealment behavior includes changing their computer clock to hamper reconstruction, encrypting data to restrict access, and using disk-cleaning tools to destroy digital evidence. One disk-cleaning tool, Evidence Eliminator (www.evidence-eliminator.com/product.d2w), is specifically advertised as a program that defends against digital forensic examination tools such as EnCase.

Other forms of evidence dynamics can make crime reconstruction using digital data more difficult. Digital evidence can be lost if it is not seized in a forensically sound or timely manner, as any use of a computer can overwrite existing data. Relevant network data may be similarly volatile because businesses only keep logs for a limited time. Therefore, it is critical to have digital crime scenes processed by qualified professionals to ensure that the evidence is preserved properly and examined thoroughly.

DIGITAL CRIME SCENE INVESTIGATION

Computers and networks should be considered an extension of the crime scene, even when they are not involved directly in facilitating the crime. It is useful to think of them as secondary crime scenes. Like a physical crime scene, digital crime scenes can contain many pieces of evidence, and it is necessary to apply forensic principles to preserve, document, and search the entire scene. A single computer can contain e-mail communications between the victim and the offender, evidence of intent to commit a crime, incriminating digital photographs taken by the offender as trophies, and software applications used to conceal digital evidence.

Untrained individuals commonly make the mistake of turning on a computer and looking for a particular item of evidence. The act of turning on and operating a computer is comparable to trampling a crime scene, thereby destroying useful evidence and making it more difficult to reconstruct the crime. To preserve the state of a digital crime scene, professionals make a duplicate copy of the evidence using tools that do not alter the original. At the same time, they document the context of the evidence by making notes and photographs and by calculating hash values of the evidence. A hash value is a formula that reads data comprising a piece of digital evidence and calculates a unique “fingerprint” that can be used to identify and verify the evidence. The verification process is accomplished by recalculating the hash value of the evidence at any time and ensuring that it is the same as the originally calculated value. After preserving and documenting the digital crime scene, forensic professionals perform their examination on the duplicate copy to locate relevant items, determine their provenance, and answer other questions of interest to investigators.

Only searching for a particular piece of evidence on a computer is like walking into a victim’s home just to collect a suicide note without examining the scene for signs of staging. In the United Kingdom case involving Dr. Harold Shipman, changes he made to computerized medical records on his medical office computer system were instrumental in convicting him for killing hundreds of patients. Following Shipman’s arrest, police made an exact copy of the hard drive from his computer, thus preserving a complete and accurate duplicate of the digital evidence. By analyzing the computer application Shipman used to maintain patient records, investigators found that the program kept an audit trail, recording changes made to patient records. This audit trail indicated that Shipman had lied about patients’ symptoms and made backdated modifications to records to conceal the murders. Had the investigators accepted the patient records without digging deeper into their authenticity, they would have missed this key piece of evidence about the cover-up attempt. During his trial, Shipman claimed that he was familiar with this audit trail feature and was sufficiently knowledgeable about computers to falsify the audit trail if he had actually been trying to hide these activities. However, the court was convinced that Shipman had altered the records to conceal his crimes and sentenced him to life in prison.

INTERPRETATION OF DIGITAL EVIDENCE[1]

Although computers can provide investigators with many tantalizing leads, digital evidence is not always what it seems and can be misinterpreted. At its basic level, digital evidence exists in a physical medium, such as a magnetic disk, a copper wire, or a radio signal in the air. Forensic examiners rarely scrutinize the physical medium and instead use computers to translate data into a form that humans can interpret, such as text, audio, or video. Therefore, examiners rarely see actual data but only a representation, and each layer of abstraction can lose information and introduce errors. For instance, analyzing the magnetic properties of a hard drive may reveal additional information useful for some investigations (e.g., overwritten data and the cause of damage to the disk). The risk of examining media at this low level is that the act of observing may cause changes that could destroy or undermine the evidence.

As described in the previous section, it is considered best practice to examine an exact replica of digital evidence to avoid altering the original. However, it can be difficult to obtain an exact and complete copy of a magnetic disk, Random Access Memory, a copper wire, or a radio signal. For instance, programmatic mistakes (a.k.a. bugs) have been found in tools for collecting digital evidence from hard drives, resulting in only a portion of data being copied. Bugs have also been found in tools for examining digital evidence on computers, resulting in an inaccurate representation of the underlying data, as shown in Figure 17.2.

There are many other potential sources of error in digital evidence between the time data are created by a system and the time of preservation and analysis of the evidence. For instance, system malfunction can result in erroneous or missing log entries. Also, as with other forms of evidence, poor training or lack of experience can lead forensic examiners to mishandle or

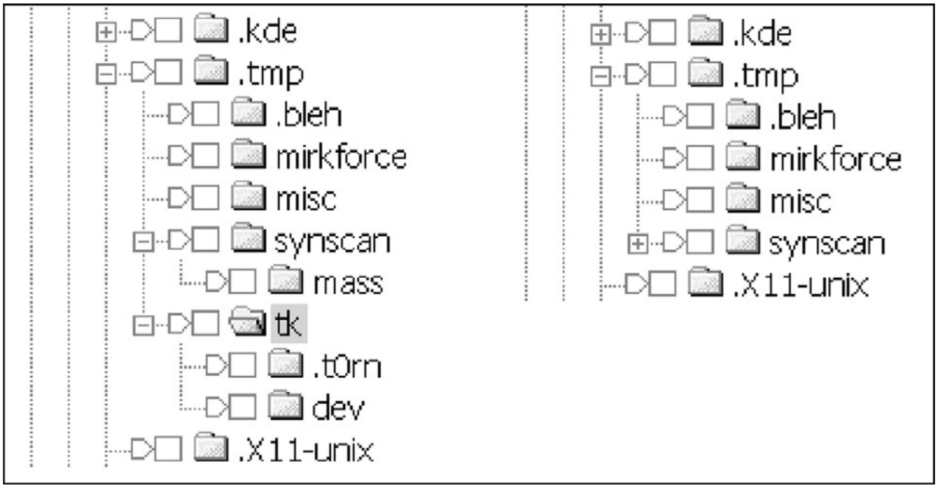


FIGURE 17.2 A folder named "tk" contained important evidence. The tk folder is visible using a newer version of a digital evidence examination tool (left) but not an older version containing a bug (right).

[1] Some examples in this section are based on Casey (2005).

interpret digital evidence incorrectly. In one case, a failure to adjust for the local time zone caused a defense expert to conclude incorrectly that police had operated the suspect's computer (Forster, 2004).

Digital evidence should always be interpreted in context. For example, the mere presence of an incriminating file on a person's computer may not be sufficient to demonstrate guilt if there is strong indicia that the file was placed on the system by a virus, intruder, or via a Web browser vulnerability without the user's knowledge. An analysis of the file, its location, security vulnerabilities, artifacts of system usage, and other contextual clues may help determine how a file came to be on a given system.

Similarly, a file with a creation date that is after its last modified date may be interpreted incorrectly as evidence that the system clock was backdated. In fact, the last written date of a file does not necessarily imply that the file was modified on the computer on which it is found. Copying a file onto a computer from removable media or another system on a network may not change the last written date, resulting in a file with a modified date prior to its creation date.

There are many other nuances to digital evidence caused by the intricacies of computer operations that can cause confusion or misinterpretation, and the same holds for networks. The **Internet Protocol** (IP)[2] address in an e-mail header may lead investigators to a particular computer, but this does not necessarily establish that the owner of that computer sent the message. Given the minor amount of effort required to conceal one's identity on the Internet, criminals usually take some action to thwart apprehension. This may be as simple as using a library computer or as sophisticated as inserting someone else's IP address into the e-mail header, requiring investigators to take additional steps to identify the culprit.

Consider a harassment case in which the offender sends the victim threatening e-mail via an intermediate server. Normally, the e-mail message would contain information about the computer used to send the message. Specifically, the e-mail header would contain the IP address of the sender's computer. However, because the harasser sent the message via an intermediate server, the e-mail header will contain the IP address of that server and conceal the actual source. For example, headers in the following e-mail sent from a Yahoo! account indicate that the message was sent from an IP address in Japan (210.249.120.210):

```
To: Count Rugen
From: "Inigo Montoya"< inigo_montoya@yahoo.com >
X-Originating-IP: 210.249.120.210
Date: Wed, 04 Jun 2003 03:51:45 -0000
Subject: Prepare to die!
```

However, the sender merely connected to Yahoo! via this computer in Japan. Therefore, additional investigation would be required to determine the actual source of the message. Log files from the intermediate computer, such as those shown next, might contain the IP address of the actual sender's computer (172.16.34.14 in this example):

```
172.16.34.14, anonymous, 6/4/03, 03:43:24, 210.249.120.210, GET, http://mailsrv.yahoo.com/login.html, 200
```

[2] Every computer on the Internet is assigned an IP address to enable delivery of data.

```
172.16.34.14, anonymous, 6/4/03, 03:44:02, 210.249.120.210, GET, http://mailsrv.yahoo.com/inigo_montoya/inbox.html, 200
172.16.34.14, anonymous, 6/4/03, 03:45:27, 210.249.120.210, GET, http://mailsrv.yahoo.com/inigo_montoya/compose.html, 200
172.16.34.14, anonymous, 6/4/03, 03:51:36, 210.249.120.210, GET, http://mailsrv.yahoo.com/inigo_montoya/sent.html, 200
```

To mitigate the risks of evidence being missed or misinterpreted, experienced forensic examiners employ a variety of techniques, including comparing the results of multiple tools, validating important findings through contextual reviews, and analyzing corroborating evidence for inconsistencies.

The scientific method provides the final bulwark against incorrect conclusions. Simply trying to validate a theory increases the chance of error—the tendency is for the analysis to be skewed in favor of the hypothesis. This is why the most effective investigators suppress their personal biases and hunches and why they seek evidence and perform experiments to disprove their working theory. Experimentation is actually a natural part of analyzing digital evidence. Given the variety and complexity of hardware and software, it is not feasible for forensic examiners to know everything about every software and hardware configuration. As a result, it is often necessary to perform controlled experiments to learn more about a given computer system or program. For instance, one approach is to pose the questions, "Was it possible to perform a given action using the subject computer, and if so, what evidence of this action is left behind on the system?" Theories about what digital evidence reveals in a particular case may be tested by restoring a duplicate copy of a subject system onto similar hardware, effectively creating a clone that can be operated to study the effects of various actions. Similarly, it may be necessary to perform experiments on a certain computer program to distinguish between actions that are automated by the program and those performed by a user action.

One useful by-product of this type of analysis is exemplars of files or other artifacts created by certain actions. Comparing an item of evidence to an exemplar can reveal investigatively useful class characteristics or even individual characteristics. In one case, the offender claimed that he could not remember the password protecting his encryption key because he had changed it recently. By experimenting with the same encryption program on a test system, the forensic examiner observed that changing the password updated the last modified date of the file containing the encryption key. An examination of the file containing the suspect's encryption key indicated that it had not been altered recently as the suspect claimed. Faced with this information, the suspect admitted that he had lied about changing the password.

In addition to presenting the facts in a case, investigators are generally expected to render an opinion about the evidence. For instance, when a program such as Evidence Eliminator is found on a suspect's computer, the forensic examiner will generally be asked if there is any evidence of its use. It is not sufficient for a forensic examiner to conclude that Evidence Eliminator was used simply because it was installed on a computer. The following is an example of how this finding might be phrased:

> Evidence Eliminator was almost definitely run on this system. The presence of a folder named "eetemp" and a detailed log file named "EElog.txt" created by Evidence Eliminator, indicate that this program was used on the subject system and was last run on 3/07/05 at 19:29. Many files referenced in the "EElog.txt" log file were altered or overwritten on 3/07/05 at 19:29, which supports the finding that Evidence Eliminator was run on the subject

system at this time. Furthermore, file slack and portions of unallocated space were overwritten with random data, which is consistent with the use of a wiping program.

Analysis of digital evidence requires interpretation that forms the basis of any conclusions reached. Investigators should assess the level of certainty underlying each conclusion in order to help the fact-finder determine what weight to attach. The C-Scale (Certainty Scale) described in Casey (2004, Chapter 7) provides a method for conveying certainty when referring to digital evidence and qualifying conclusions appropriately. Some digital investigators use a less formal system of degrees of likelihood that can be used in both the affirmative and the negative sense: (1) almost definitely, (2) most probably, (3) probably, (4) very possibly, and (5) possibly.

Whenever possible, investigators should support assertions with available sources of relevant evidence. Clearly state how and where the digital evidence was found to help fact finders interpret the findings and to enable another competent examiner to verify the results. Presenting alternative scenarios and demonstrating why they are less reasonable and less consistent with the evidence can help strengthen key conclusions. Explaining why other explanations are unlikely or impossible is a respected facet of the scientific method that can be applied to examination of digital evidence and demonstrate that a particular conclusion withstood critical scrutiny. If there is no evidence to support an alternative scenario, state whether it is more likely that relevant evidence was missed or simply not present. If digital evidence was altered after it was collected, it is crucial to mention this in the report, explaining the cause of the alterations and weighing their impact on the case (e.g., negligible or severe).

Two similar scenarios are presented here to demonstrate that apparently minor differences in the circumstances can lead to significantly different conclusions, with different levels of certainty.

EXAMPLES

Conclusion 1

At 17:57 EDT on 05/16/2005, shortly after the incriminating activities occurred on the computer, Evidence Eliminator appears to have been run. Although Jack Smith and Jane Doe were the primary users of this computer, a password was not required and it was in a location that was accessible to many people in the building. Evidence Eliminator was run at a time when both Mr. Smith and Ms. Doe were at another location and could not have accessed the computer remotely. The subject computer does not maintain a record of clock changes and there is no evidence to prove or disprove that the clock was tampered with. It is possible that Mr. Smith or Ms. Doe changed the computer clock to make it appear that Evidence Eliminator was run at a time when they would not be implicated. It is also possible that an unknown third party accessed the computer and ran Evidence Eliminator.

Conclusion 2

Although Evidence Eliminator appears to have been run on the subject computer shortly after the incriminating activities occurred on the computer at 17:57 EDT on 05/16/2005, there is evidence that the clock was tampered with. Based on temporal discontinuities in the Windows Event log, Evidence Eliminator was actually run at 11:45 that morning. Jack Smith and Jane Doe were the primary users of this computer, and they each had their own username and password. Windows Event logs show that Jane Doe's account was used to log into the computer at 11:24 on the date in question and logged out at

11:50. The computer was located in a room that required a key card to access, and the security logs show that Jane Doe's card was used to access the room at 11:20. Furthermore, security cameras show Jane Doe walking through the hall leading to the room at 11:19 and walking away from the room at 11:53. Therefore, it was almost definitely Jane Doe who committed the crime, altered the clock, and ran Evidence Eliminator on the subject computer.

ATTRIBUTION USING DIGITAL EVIDENCE

Digital evidence can play a direct role in identifying and apprehending offenders, helping investigators establish linkages between people and their online activities. This attribution process can be challenging using digital evidence alone, but when combined with traditional investigative techniques, these data can provide the necessary clues to track down criminals. For instance, a lead developed during a serial homicide investigation in St. Louis when a reporter received a letter from the killer. The letter contained a map of a specific area with a handwritten "X" to indicate where another body could be found. After investigators found a skeleton in that area, they inspected the letter more closely for ways to link it to the killer. The FBI determined that the map in the letter was from Expedia.com and immediately contacted the site to determine if there was any useful digital evidence. The Web server logs on Expedia.com showed that only one IP address (65.227.106.78) had accessed the map around May 21, the date the letter was postmarked. The ISP responsible for this IP address was able to provide the account information and telephone number that had been used to make the connection in question. Both the dial-up account and telephone number used to make this connection belonged to Maury Travis (Robinson, 2002).

In short, the act of downloading the online map included in the letter left traces on the Expedia Web server, on Travis's ISP, and on his personal computer. Investigators arrested Travis and found incriminating evidence in his home, including a torture chamber and a videotape of himself torturing and raping a number of women and apparently strangling one victim. Travis committed suicide while in custody and the full extent of his crimes may never be known.

In another case, Dartmouth professors Susanne and Half Zantop were stabbed in their homes with SOG Seal 2000 knives. Investigators tracked purchases of this type of knife through Internet sites, leading them to two local teenagers, James Parker and Robert Tulloch. A forensic examination of the boys' computers revealed that, after being interviewed by police, they contacted each other over AOL Instant Messenger and agreed to flee to California. Two knives were found in Tulloch's bedroom with blood matching the Zantops, and the boys were apprehended and confessed to the killings (CBS News, 2001).

However, attributing computer activities to a particular individual can be challenging. For instance, logs showing that a particular Internet account was used to commit a crime do not prove that the owner of that account was responsible, as someone else could have used the individual's account. Even when dealing with a specific computer and a known suspect, some investigative and forensic steps may be required to place the person at the keyboard and confirm that the activities on the computer were most likely those of the suspect. Considering the mobile telephone example at the beginning of this chapter (see Figure 17.1), it may only be possible for the forensic examiner to state that the suspect's phone was used to send the victim an SMS message at 10:05 and that the suspect's phone was in the same vicinity as the victim at the time of the murder. Other evidence would be required to establish that the suspect was in possession of his phone at these times and to place him at the crime scene.

Attributing a crime to an individual becomes even more difficult when a crime is committed via an open wireless access point or from a publicly accessible computer, such as at an Internet cafe or public library terminal. In one extortion case, investigators followed the main suspects and observed one of them use a library computer from which incriminating e-mails had been sent (Howell, 2004; Khamsi, 2005).

Using evidence from multiple independent sources to corroborate each other and develop an accurate picture of events can help develop a strong association between an individual and computer activities. This type of reconstruction can involve traditional investigative techniques, such as stakeouts. For instance, a man accused of possessing child pornography argued that all evidence found in his home should be suppressed because investigators had not provided sufficient probable cause in their search warrant to conclude that it was in fact he, and not an imposter, who was using his Internet account to traffic in child pornography (*U.S. v. Grant*, 2000). During their investigation into an online child exploitation group, investigators determined that one member of the group had connected to the Internet using a dial-up account registered to Grant. Upon further investigation, they found that Grant also had a high-speed Internet connection from his home that was used as an FTP server—the type of file-transfer server required for membership in the child exploitation group.

Coincidentally, while tapping a telephone not associated with Grant in relation to another child pornography case, investigators observed that one of the participants in a secret online chat room was connected via Grant's dial-up account. Contemporaneous surveillance of the defendant's home revealed that both his and his wife's car were parked outside their residence at the time. The court believed that there was enough corroborating evidence to establish a solid circumstantial connection between the defendant and the crime to support probable cause for the search warrant.

DIGITAL DOCUMENT AUTHENTICATION

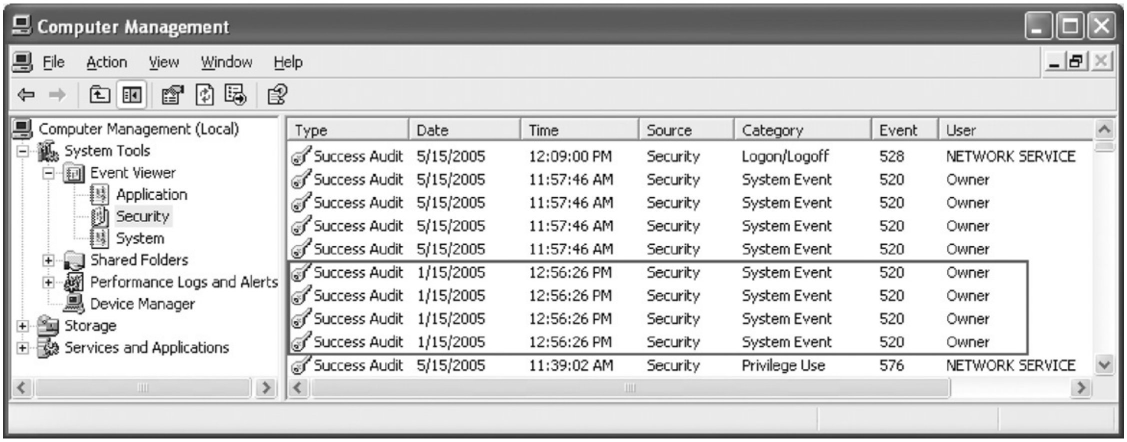
The author of a document and the date it was created can be significant, as demonstrated in the Guthrie case described at the beginning of this chapter. In that case, the offender was not technically savvy enough to change his computer's clock to an earlier date to give the impression that the document was created prior to his wife's death. Such staging can make it more difficult to determine who wrote a document and when it was created. However, there are various approaches that forensic examiners can use to authenticate a digital document.

Forensic examiners can use date stamps on files and in log files to determine the provenance of a document such as a suicide note even when the digital crime scene is staged. For instance, it is possible to detect staging and document falsification by searching for chronological inconsistencies in log files and file date stamps. Nuances in the way computers maintain different date stamps can help forensic examiners reconstruct aspects of the creation and modification of a document. In addition, certain types of files, such as Microsoft Word, contain embedded information that can be useful for authenticating a document. This embedded information may include the last printed date and the last 10 file names and authors, as shown previously.

EXAMPLE

According to Joe Smith, he created the questioned document in January 2005. However, dates associated with this document show that it was actually created in May 2005 and subsequently backdated to January. This fact is supported by dates in file slack of this document from April 2005 and by dates in a temporary copy created while the document was being edited using Microsoft Word in May 2005. Furthermore, Windows Security Event log entries from May 2005 show that the clock was backdated to January 2005 and subsequently returned to the correct date (Figure 17.3). In conclusion, the questioned document was created in May 2005 and not in January as claimed by Joe Smith.

The arrangement of data on storage media (a.k.a. digital stratigraphy) can provide supporting evidence in such forensic examinations. For instance, when a forensic examiner finds a questioned document that was purportedly created in January 2005 lying on top of a deleted document that was created in April 2005, staging should be suspected because the newer file should not be overwritten by an older one. Although the usefulness of digital stratigraphy for document authentication can be undermined by some disk optimization programs that reposition data on a hard drive, it can also be aided by the process. In one case, the suspect defragmented his hard drive prior to fabricating a document. The forensic examiner determined that the defragmentation process had been executed in 2003, causing all data on the disk to be reorganized onto a particular portion of the disk. The questioned documents that were purportedly created in 1999 were the only files on the system that were not arranged neatly in this area of the disk, which added weight to the conclusion that the questioned documents were actually created after the defragmentation process had been executed in 2003 (Friedberg, 2004).



Type	Date	Time	Source	Category	Event	User
Success Audit	5/15/2005	12:09:00 PM	Security	Logon/Logoff	528	NETWORK SERVICE
Success Audit	5/15/2005	11:57:46 AM	Security	System Event	520	Owner
Success Audit	5/15/2005	11:57:46 AM	Security	System Event	520	Owner
Success Audit	5/15/2005	11:57:46 AM	Security	System Event	520	Owner
Success Audit	5/15/2005	11:57:46 AM	Security	System Event	520	Owner
Success Audit	1/15/2005	12:56:26 PM	Security	System Event	520	Owner
Success Audit	1/15/2005	12:56:26 PM	Security	System Event	520	Owner
Success Audit	1/15/2005	12:56:26 PM	Security	System Event	520	Owner
Success Audit	1/15/2005	12:56:26 PM	Security	System Event	520	Owner
Success Audit	5/15/2005	11:39:02 AM	Security	Privilege Use	576	NETWORK SERVICE

FIGURE 17.3 Windows Security Event log from May 2005 contains entries with January date stamps, indicating that the clock was backdated.

EVALUATION OF SOURCE

Different file formats have characteristics that may be associated with their source. As shown previously, Microsoft Office documents contain embedded information, such as printer names, directory locations, names of authors, and creation/modification date–time stamps, that can be useful for determining their source. These embedded characteristics can be used to associate a piece of evidence with a specific computer. Earlier versions of Microsoft Office also embedded a unique identifier in files, called a globally unique identifier, which can be used to identify the computer that was used to create a given document (Leach and Salz, 1998). More subtle evaluations of source involve the association of data fragments with a particular originating file or determining if a given computer was used to alter a piece of evidence.

When a suspect's computer contains photographs relating to a crime, it may not be safe to assume that the suspect created those photographs. It is possible that the files were copied from another system or downloaded from the Internet. Forensic analysis of the photographs may be necessary to extract class characteristics consistent with the suspect's digital camera or flatbed scanner. The scanner may have a scratch or flaw that appears in the photographs or the files may contain information that was embedded by the digital camera, such as the make and model of the camera and the date and time the photograph was taken. This embedded metadata could be used to demonstrate that a photograph was likely taken using a suspect's camera rather than downloaded from the Internet.

If these kinds of metadata are not available in a digital photograph, it may be possible to use other characteristics of a photograph to determine its source. For instance, Europol's Excalibur system uses image recognition technology to search a database of photographs from past investigations for similarities with a given image. If two photographs contain a common component, such as a piece of fabric with a distinct design, this may indicate that they were taken in the same place, providing investigators with a lead.

If incriminating files found on a computer were downloaded from the Internet, investigators may want to locate the originating computer and search it for evidence relating to the crime. This can involve reconstructing the computer user's Internet activities to determine where the files were obtained. It may also be necessary to examine e-mail headers, logs, and other artifacts of network activity to determine where digital evidence came from.

ASSESSING ALIBIS AND STATEMENTS

Offenders, victims, and offenders may mislead investigators intentionally or inadvertently, claiming that something occurred or that they were somewhere at a particular time. By cross-referencing such information with the digital traces left behind by a person's activities, digital evidence may be found to support or refute a statement or alibi. In one homicide investigation, the prime suspect claimed that he was out of town at the time of the crime. Although his computer suffered from a Y2K bug that rendered most of the date–time stamps on his computer useless, e-mail messages sent and received by the suspect showed that he was at home when the murder occurred, contrary to his original statement. Caught in a lie, the suspect admitted to the crime.

As another example, data relating to mobile telephones were instrumental in the conviction of Ian Huntley for the murder of Holly Wells and Jessica Chapman in the United Kingdom. The last communication from Jessica's mobile phone was sent to a cell tower several miles away in Burwell rather than a local tower in Soham (BBC, 2003). The police provided a mobile telephone specialist with a map of the route they thought the girls would have taken, and the specialist determined that the only place on that route where the phone could have connected to the cell tower in Burwell was from inside or just outside Huntley's house (Summers, 2003). In addition, Huntley's alibi was that he was with his friend Maxine Carr on the night the girls went missing, but Carr's mobile phone records indicated that she was out of town at the time.

Investigators should not rely on one piece of digital evidence when examining an alibi: they should search for an associated cybertrail. On many computers, minimal skills are required to change the clock or the creation time of a file. Also, people can program a computer to perform an action, such as sending an e-mail message, at a specific time. In many cases, scheduling events does not require any programming skill—it is a simple feature of the operating system. Similarly, IP addresses can be changed and concealed, allowing individuals to pretend that they are connected to a network from another location. In addition, the location information associated with mobile telephones is not exact and does not place an individual at a specific location. As noted previously, it can also be difficult to prove who was using the mobile telephone at a specific time, particularly when telephones or subscriber identity module cards are shared among members of a group or family.

DETERMINING MOTIVATION AND INTENT

Clear evidence of intent, such as an offender's diary, may be found on a computer. Other pieces of digital data might not be useful on their own, but patterns of behavior can emerge when the pieces of digital evidence are combined with other information about a person's actions. Examples of this were observed in Shipman's modification of patient records and in Guthrie's Web searches described at the beginning of the chapter. In another case, prosecutors upgraded the charge against Robert Durall from second-degree to first-degree murder based on Internet searches found on his computer with key words including "kill + spouse," "accidental + deaths," "smothering," and "murder" (Johnson, 2000). In child exploitation cases, an offender's computer may contain evidence of soliciting and grooming victims over the Internet.

In David Westerfield's homicide trial, the prosecution claimed that Westerfield's digital pornography collection reflected his fantasies relating to kidnapping and killing 7-year-old Danielle van Dam and, in closing arguments, insinuated that the pornography motivated Westerfield to victimize the child (*California v. Westerfield*, 2002):

> Not only does he have the young girls involved in sex, but he has the anime that you saw. And we will not show them to you again. The drawings of the young girls being sexually assaulted. Raped. Digitally penetrated. Exposed. Forcibly sodomized. Why does he have those, a normal 50-year-old man? Those are his fantasies. His choice. Those are what he wants. He picked them; he collected them. Those are his fantasies. That's what gets him excited. That's what he wants in his collection. . . . When you have those fantasies, fantasies breed need. He got to the point where it was growing and growing and growing. And what else is there to collect? What else can I get excited about visually, audibly?

Forensic examinations of computers can reveal other behavior that can be very useful for determining intent. For instance, evidence of clock tampering may enable a forensic examiner to conclude that the computer owner intentionally backdated a digital document. Also, disk cleaning or encryption programs on a computer can be used to demonstrate a computer owner's conscious decision to destroy or conceal incriminating digital evidence. However, these same actions may have innocent explanations and must be considered in context before reaching a definitive conclusion.

CONCLUSION

Digital evidence can help answer many questions in an investigation, ranging from the whereabouts of a victim at a given time to the state of mind of the offender. Therefore, evidence on computers and networks should be included whenever feasible in crime reconstructions. At the same time, care must be taken when interpreting the abstracted behavioral evidence that is stored on computers. People use technology in creative ways that can complicate the reconstruction process, particularly when attempts are made to conceal digital evidence. Computers also have many subsystems that interact in ways that can complicate the reconstruction process. In all cases, given the malleability and multivalent nature of digital evidence, it is necessary to seek corroborating evidence from multiple independent sources. The risk of missing or misinterpreting important details highlights the importance of utilizing the scientific method to reach objective conclusions that are solidly based on the evidence.

SUMMARY

Digital evidence is defined as any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense, such as intent or alibi. Homicide, sexual assault, and other violent crimes can involve digital evidence from a wide range of sources, including personal computers, handheld devices, servers, and the Internet, helping investigators reconstruct events and gain insight into the state of mind of individuals. A basic knowledge of these, and how they operate, is required for a complete investigation and reconstruction.

Computers and networks should be considered an extension of the crime scene, even when they are not involved directly in facilitating the crime. It is useful to think of them as secondary crime scenes. Like a physical crime scene, digital crime scenes can contain many pieces of evidence, and it is necessary to apply forensic principles to preserve, document, and search the entire scene. A single computer can contain e-mail communications between the victim and the offender, evidence of intent to commit a crime, incriminating digital photographs taken by the offender as trophies, and software applications used to conceal digital evidence. Digital evidence that is handled and interpreted properly can be used to apprehend offenders, authenticate documents, assess alibis and statements, and determine intent.

Information stored and created on computers can be used to answer fundamental questions relating to a crime, including what happened when (sequencing), who was responsible (attribution), and the origination of a particular item (evaluation of source). At the same time, the complexity of computer systems requires appreciation that individual pieces of digital evidence may have multiple interpretations, and corroborating information may be vital to reaching a correct conclusion. Forensic examiners need to understand, and make regular use of, the scientific method to ensure that conclusions reached are based solidly in fact. Familiarity with the limitations of forensic examinations of digital evidence will help investigators and attorneys exculpate the innocent and apprehend modern criminals.

QUESTIONS

1. Define digital evidence.
2. Explain what a cybertrail is and how it is useful in reconstruction efforts.
3. Computers and networks can be thought of as __________ of crime scenes.
4. The act of turning on and operating a computer destroys useful evidence and makes it more difficult to reconstruct the crime. True or false?
5. List one source of error that may occur in digital evidence between the time data are created by a system and the time of preservation and analysis of the evidence.

ACKNOWLEDGMENTS

I thank Jessica Reust and my other colleagues at Stroz Friedberg LLC for their assistance with the development of this chapter.

References

BBC, (2003). *Soham trial: "Crucial" phone evidence*. November 6. Available at news.bbc.co.uk/1/hi/england/cambridgeshire/3246111.stm.

Bean, M. (2003). *"Mich. v. Miller: Sex, Lies and Murder,"* Court TV. Available at www.courttv.com/trials/taped/miller/background.html.

California v. Westerfield. (2002). Case No. CD165805, Superior Court of California, County of San Diego Central Division.

Casey, E. (2004). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (2nd ed.). London: Academic Press.

Casey, E. (2005). Computer crime and digital evidence. In *Encyclopedia of Forensic and Legal Medicine 1–4*. London: Elsevier.

CBS News, (2001). Teen to plead guilty in prof's death. *CBS News*, December. Available at www.cbsnews.com/stories/2001/12/03/national/main319894.shtml.

Chaski, C. (2005). Who's at the keyboard? Authorship attribution in digital evidence investigations. *International Journal Digital Evidence*, *4*(1). Available at www.ijde.org/docs/chaski_spring_05.pdf.

Forster, P. (2004). Time and date issues in forensic computing. *Journal of Digital Investigation*, *1*(1). Available at www.compseconline.com/digitalinvestigation/tableofcontents.htm.

Fridrich, J., Goljan, M., & Lukáš, J. (2005). Proceedings of the SPIE, Vol. 5685: Determining digital image origin using sensor imperfections. *Multimedia Mobile Devices Journal*, 249–260, January 16–20.

Friedberg, E. (2004). To cache a thief: How litigants and lawyers tamper with electronic evidence and why they get caught. *The American Lawyer*, January. http://www.americanlawyer.com/newcontents0104.html.

Geradts, Z., Vrijdag, D., Alberink, I., Goos, M. I., & Ruifrok, A. (2005). Questions about the integrity and authenticity of digital images. American Academy of Forensic Sciences Workshop Presentation.

Howell, B. (2004). Ambiguities in U.S. law for investigators. *Journal of Digital Investigation*, *1*(2), 106–111.

Johnson, T. (2000). Man searched Web for way to kill wife, lawyers say. *Seattle Post-Intelligencer*, June 10, 2000. Available at seattlepi.nwsource.com/local/murd21.shtml.

Khamsi, R. (2005). Dusting for digital fingerprints. *Economist Technology Quarterly*, March 12.

Leach, P., & Salz, R. (1998). *UUIDs and GUIDs*. Network Working Group. Internet draft, 1998. Available at www.webdav.org/specs/draft-leach-uuids-guids-01.txt.

Robinson, B. (2002). Taking a byte out of cybercrime. *ABC News*, July 15.

State of South Dakota v. William Boyd Guthrie. (2001). SD 61, 2001. Available at caselaw.lp.findlaw.com/scripts/getcase.pl?court=sd&vol=2001_061&invol=1.

Summers, C. (2003). Mobile phones—The new fingerprints. *BBC News Online*, December 18. Available at news.bbc.co.uk/1/hi/uk/3303637.stm.

Tuohey, J. (2004). Government uses color laser printer technology to track documents: Practice embeds hidden, traceable data in every page printed. *Medill News Service*, Monday, November 22. Available at www.pcworld.com/news/article/0,aid,118664,00.asp.

U.S. v. Grant. (2000). U.S. Court of Appeals, 1st Cir. Available at laws.lp.findlaw.com/1st/992332.html.