Chapter 7
Securing Information Systems

LEARNING TRACK 3: COMPUTER FORENSICS

For thirty years, a serial murderer known as the BTK killer (standing for bind, torture, and kill) remained at large in Wichita, Kansas. The BTK killer first struck in 1971 with the murder of four members of a Wichita family in their home and committed his last in this early period murder in 1991. He then resurfaced between March 2004 and February 2005, sending a letter to a local news paper and eventually a floppy disk to the city police department. The disk contained a file labeled "Test A.RTF" with the message "This is a test." Additional investigation found that the disk was opened in computers at Wichita's Christ Lutheran Church and the file was last saved by a user named "Dennis." This information led police to Dennis Rader, president of the congregation, who was proven via DNA analysis and examination of Rader's computer to be the BTK killer. Computer forensics played an important role in breaking this case.

What Is Computer Forensics?

Computer forensics is the scientific collection, examination, authentication, preservation, and analysis of digital data so that the information can be used as evidence in a court of law. Both local and federal law enforcement agencies use computer forensics to gather evidence for criminal cases or to obtain more information about a suspect. Large corporations may hire a computer forensics expert to monitor employee computer activities to make sure employees are not leaking sensitive or critical company information or using company computer resources in harmful ways.

Computer forensics can be an indispensable tool in divorce cases where one party may be trying to conceal or secretly transfer wealth, or there is suspicion of infidelity or other conduct that would constitute "fault" in divorce proceedings. The divorce discovery process will be looking for digital evidence such as names and addresses of financial institutions, fund transfers, hidden accounts, real estate holdings, debt information, account activity, and e-mail and instant message communication with other people. The party that fails to disclose an asset during the divorce process may be required to pay attorney's fees and turn over the asset to the other party or to the court in a receivership proceeding, in addition to losing credibility in the divorce proceeding as a whole.

For instance, computer forensics facilitated the discovery of records related to a family-owned business. The profit and loss statements and general ledgers for a four-year period provided by the spouse that operated the business appeared to minimize corporate assets and income. A forensic analysis of the computer system where the records were stored showed that a program designed to erase data was downloaded and used to remove items from the hard drive shortly before the computer was turned over to the forensic examiner. The forensic examiner additionally determined that the financial records that had been provided by the spouse had been generated by a program version that was not in use at the time the records were purportedly created. As a result, the court concluded that the records had been modified and imposed a sanction against the spouse that had provided the records.

Computer forensics requires specialized expertise and tools that go beyond the normal data collection preservation techniques employed by end users and information systems departments. This field also requires legal knowledge because digital evidence must adhere to the standards of evidence that are admissible in a court of law. Before performing an investigation, the examiner must make sure he or she has the legal authority to search for digital data.

Computer forensics experts perform a variety of tasks:

- Identify sources of digital or documentary evidence
- Preserve the evidence
- Analyze the evidence
- Present the findings.

Digital Evidence

Digital evidence consists of any information stored or transmitted in digital form that can be used in court for either criminal or civil cases. Digital evidence can be found in e-mail, voice mail, instant messaging, Web browsing histories, digital photographs and video, computer disk drives, CDs, DVDs, USB storage devices, iPods and MP3 players, smart phones, cell phones, pagers, photocopiers, fax machines, and Global Positioning System (GPS) tracks.

E-mail is now a primary means of communication and a major source of digital evidence. This evidence may be found in the body of the e-mail or in an attachment. E-mail data may be stored on a local hard drive, a network device, a dedicated mail server, or a removable device, and the forensic examiner will search all of these devices.

All e-mail messages generate headers attached to the messages that contain valuable information such as the time the message was sent, identities of sender and recipient, and the sender's domain name. The headers may contain "reply to" information that allow threads to be reconstructed.

The high volume of e-mail makes it difficult for an examiner to search each message. Forensic experts typically will make copies of e-mails and attachments and look for incriminating evidence using keyword searches.

Computer forensics specialists are often called in to recover data that has been deleted from a device. Many computer users do not realize that there are tools for recovering data on a computer hard drive after a file has been deleted. In addition to recovering "deleted" files, computer forensics specialists can examine local network connections to gather evidence from data transmissions or uploads of files.

Obtaining Digital Evidence

Like any other piece of evidence used in a legal case, the information obtained by a computer forensics investigation must follow the standards of admissible evidence in a court of law. Those presenting electronic evidence must be able to demonstrate the reliability of the computer equipment, the manner in which the basic data were initially entered, measures taken to ensure the accuracy of the data as entered, the method of storing the data, precautions taken to prevent its loss, and the accuracy and reliability of the computer programs used to process the data.

If the individual who generated the digital evidence has not consented to having his or her computer system examined, the computer forensics expert must make sure that he or she has the legal authority to seize, examine, and image the individual's computer devices.

The computer forensics investigator needs to document all work done to a com-

puter and all information found. An investigator who uses a faulty procedure may invalidate all the digital evidence collected. To make sure evidence is not lost, destroyed, or compromised, the following guidelines should be followed:

1. Only use tested tools and methods that have been tested and validated for accuracy and reliability.
2. Handle the original evidence as little as possible to avoid changing data.
3. Document everything done.
4. Establish and maintain a chain of custody.
5. Never exceed personal knowledge

Unless it is completely unavoidable, digital evidence should not be analyzed using the same machine from which it was collected. Instead, forensic image copies of the contents of computer storage devices (primarily hard drives) are made.

If a machine is suspected of being used for illegal communications, such as terrorist traffic, important information may not be stored on the hard drive. Several Open Source tools are available to analyze open ports, mapped drives, or open encrypted files on the live computer system. These stools can also scan RAM and Registry information to show recently accessed Web-based e-mail sites and the login/password used to access these sites or recently accessed local e-mail applications such as MS Outlook.

The Registry is a database used by the Windows operating system to store configuration information, such as settings for hardware, system software, installed programs, and user preferences. This information may help a forensic investigation by showing, for example, whether someone tried to uninstall a program.

It is possible that the expert trying to analyze a live computer system will make changes to the contents of the hard drive. During each phase of the analysis, the forensic examiner needs to identify the information that will be lost when the system powers down, balancing the need to potentially change data on the hard drive with the evidentiary value of the perishable data.

When a live analysis is being conducted, data that are most likely to be modified or damaged first must be captured first. So the examiner will first inspect data in network connections, followed by analysis of running computer programs, then the contents of RAM, which may include information on all running programs, recently run programs, passwords, encryption keys, personal information, and system and program settings. Next operating systems will be examined, including user lists, currently logged in users, system data and time, currently accessed files, and current security policies.

Finally, the hard drive will be imaged to create an exact duplicate. Forensic examiners can completely duplicate an entire hard drive using a standalone hard drive duplicator or software imaging tools such as DCFLdd or IXimager, storing the duplicate on another hard disk drive, a tape, or other media. The original drive will be moved to secure storage to prevent tampering and some type of hardware write tool will be used to ensure the original hard drive cannot be written on again. Table 1 shows some of the leading software tools used for these activities.

Careers in Computer Forensics

Computer forensics is a blossoming field, given the increasing amount of public discussion and legislation aimed controlling computer crime, identity theft, data leakage, and data protection. The FBI anticipates that nearly fifty percent of its criminal cases will involve computer forensics work in the future. The nature of crime itself is changing as criminals learn how to exploit weaknesses in computers, networks, and their

TABLE 1 DIGITAL FORENSIC SOFTWARE TOOLS

SOFTWARE TOOL	DESCRIPTION
EnCase Forensics	*Comprehensive tool capable of performing both file imaging and analysis, and analyzing and documenting multiple e-mail formats.*
DCFLdd	*Open source tool that is often used to create bit-stream image files of media as part of a forensic acquisition process. Can hash data as it is being transferred, helping to ensure data integrity, verify that a target drive is a bit-for-bit match of the specified input file or pattern, and output to multiple files or disks at the same time.*
AccessData Forensic Toolkit	*Performs imaging, decryption, and analysis, supporting many file and imaging formats.*
Mailbag Assistant	*Tools for searching, organizing, and analyzing e-mail in many different formats.*
IsoBuster	*Data recovery tool for examining CDs and DVDs. Works with multiple CD and DVD file formats and CD image files. Is capable of viewing and accessing data on CDs and DVDs from both open and closed sessions, thereby displaying data which may not be readily accessible by other forensic software tools*
IX Imager	*Linux-based digital media acquisition tool, with the ability to compress and/or encrypt image files and provide imaging accuracy in the face of damaged media, hidden geometries, and under adverse conditions. Works with devices that otherwise cannot be imaged in a Windows environment, include USB devices, server RAID systems, and tape.*
Paraban Device Seizure	*Provides deleted data recovery and full data dumps of certain cell phone models*
SMART	*Software utility that can acquire data from digital devices and clone it to any number of images and devices simultaneously. Able to recover deleted data and interpret file system metadata, and to perform an on-site or remote preview of a target system.*
Helix	*Includes more than 35 tools for incident response and forensic analysis, including tools for wiping data from disks, recovering data from slack space, and viewing the Windows Registry.*

business applications in finance and accounting.

Computer forensics professionals are referred to by many titles, including computer forensics investigator, digital forensics detectives, and digital media analysts. All these jobs deal with the investigation of digital media.

A computer forensics investigator is responsible for collecting and evaluating data stored or encrypted on digital media or for recovering data that have been deleted from a computer device. The investigator is also charged with securing the data and

ensuring they are not accidentally damaged during an investigation. Once the investigation is complete, the computer forensics investigator will write a detailed report describing the findings of the investigation. Computer forensics investigators work with law enforcement agencies, large corporations, or consulting firms or they operate on their own as freelance consultants to businesses that do not need or cannot afford a full-time computer forensics professional.

A computer forensics director is typically responsible for managing a team of computer forensics investigators in a law enforcement agency, large corporation, or computer forensics consulting firm. Computer forensics directors must have good management skills and are responsible for ensuring that all legal procedures and company policies are carefully followed. This position generally requires a bachelor's degree, usually in management, computer security, criminal justice, or computer forensics.

The salary for computer forensics professionals ranges for $85,000 to $120,000 per year, with salaries at private companies usually higher than those in law enforcement. Computer forensics directors typically earn salaries in the range of $120,000 to $160,000.

The two most common certifications for computer forensics investigators are the Certified Information Systems Security Professional (CISSP) and the Certified Computer Examiner (CCE). The CISSP is offered by the International Information Systems Security Certification Consortium, or ISC. To be certified, individuals must pass a six-hour CISSP examination. Candidates for the CISSP exam should have at least four years of professional experience in information security or a college degree and three years of experience.

The Certified Computer Examiner (CCE) certification demonstrates competency in computer forensics. The CCE credential is offered by the International Society for Computer Examiners (ISFCE). To qualify for the CCE, candidates should have at least 18 months of professional experience or documented training, pass an online examination. and perform a forensic examination on at least three "test media."

Digital Forensic Degree Programs

Many computer forensics professionals acquire expertise while on the job in law enforcement and computer security positions, but formal education is becoming more necessary as a requirement for these positions. There are computer forensics certificate programs for people who already have some career knowledge. People with no law enforcement or security background can pursue an associates' degree, a bachelors' degree or a masters degree programs in computer forensics. For positions such as forensic team leaders or bureau supervisors, a graduate degree is desirable.

All computer forensics specialists must have a solid comprehension of the law. They must understand how to properly and legally handle evidence and how to use a variety of methods for evidence discovery and retrieval. Computer forensics specialists will need knowledge of computer systems and programs and how to retrieve information from them. Computer forensic degree programs offer courses in business and criminal law along with course work in computer systems and programs and courses in technical writing and public speaking. Many of these degree programs require completion of an internship with local agencies or computer forensics professionals prior to graduation to provide real-world working experience.

The associate's degree in computer forensics is a two year study program that includes courses in cybercrime, intrusion detection systems, and legal basics, along with courses in technical writing, algebra, and public speaking.

The bachelor's degree in computer forensics is a four-year program providing computer forensics knowledge along with general education. Graduates typically take courses in criminal law, computer operating systems, and intrusion detection systems

along with courses in technical writing, economics, and statistics. A few colleges and universities, such as Utica College of Syracuse University, Keiser University, and Marymount University in Arlington, Virginia, offer bachelor's degree programs in computer forensics. Many more colleges are planning new programs in computer forensics.

Master's degree programs in computer forensics are typically pursued by law enforcement and computer security professionals who have already earned bachelor's degrees. These programs require course work in digital forensics, computer security and fraud analysis. Educational institutions offering a computer forensics master's degree include the University of Central Florida, John Jay College of Criminal Justice, Marshall University, and the University of East London.