Computer Forensics Preparation

This lesson covers Chapters 1 and 2 in *Computer Forensics JumpStart,* Second Edition.

LESSON 1

OBJECTIVES

When you complete this lesson, you'll be able to

- Discuss computer forensics and investigation as a profession
- Assess corporate and law enforcement forensic needs
- Train end users and forensic investigators on best practices
- Conduct computing investigations and form incident response teams
- Stay current with hardware, operating systems, and file systems
- Identify hardware and its types, including unauthorized hardware
- Discuss an investigator's legal rights and limitations

ASSIGNMENT 1

Read this assignment, and then read Chapter 1, "The Need for Computer Forensics," on pages 1–22 of your textbook.

Understanding Computer Forensics

This first assignment examines the underlying reasons why computer forensics is so vital, and it takes a specific look at the issues and conflicts faced in this relatively new field of investigation. By looking at this information, you should be

able to place the information in a legal and ethical context, which is of primary importance to law enforcement and corporate security offices.

Put simply, *computer forensics* is the field of obtaining and analyzing digital information from electronic devices to be used as evidence in civil, criminal, or administrative investigations. The textbook more specifically defines computer forensics as investigation and analysis techniques involving the identification, preservation, extraction, documentation, and interpretation of computer data to determine potential legal evidence. In general, forensic practice involves secure data collection, examining suspect data for salient facts regarding its origin and past usage, legal presentation, and determining relevance to existing laws.

Because digital evidence is of a different quantitative nature than physical evidence, different rules have developed for its collection and usage, although certain basic rules, such as the Fourth Amendment's protection against search and seizure, still apply. A computer forensics professional must therefore have knowledge of not only hardware, software, and operating systems, but also proper documentation, laws, and applicable guidelines, as well as up-to-date knowledge of techniques used in *e-discovery,* or the process of collecting, preparing, reviewing, and distributing electronic documents as a part of legal or governmental proceedings.

When working with digital evidence, computer forensics professionals perform several general tasks:

- Identifying digital data or artifacts that can be used as evidence
- Collecting, preserving, and documenting evidence
- Analyzing, identifying, and organizing evidence
- Rebuilding evidence or repeating a situation to verify that results can be reliably reproduced

To perform these tasks reliably and successfully, the process of collecting evidence and processing a criminal or incident scene needs to be done systematically, to ensure the greatest degree of reproducibility and confidence in the results. Due to the rise in computer crimes—a number of which can be

reviewed online through the U.S. Department of Justice at **http://www.cybercrime.gov**—understanding and practicing effective computer forensics techniques is a must for any would-be professional in the field.

Corporate and Law Enforcement Concerns

Computer forensic professionals work on two distinct types of investigations. Depending on circumstances, though, these types can easily bleed into one another. The first type, *public investigations,* in which government agencies look into criminal investigations and prosecution, is subject to legal guidelines such as the Fourth Amendment and other guidelines that depend on the locality of the crime. The other type of investigation is *private* or *corporate investigations,* which are handled by companies, lawyers, and regulatory government agencies outside normal law enforcement. These investigations are governed by corporate policies and civil laws, although they can escalate into criminal cases and vice versa. Following sound forensic procedure allows such transitions to happen with ease on the part of the investigators.

Private companies and lawyers call upon computer forensic investigators to perform corporate investigations, and these investigations generally center on company policy violations, litigation, and *incidents* (computer security breaches that can be recovered from relatively quickly). It's often considered more important to minimize business interruption and put a stop to suspected illegal acts than to catch and detain a suspect, so this consideration must be kept in mind during the investigation. Additionally, businesses generally seek to avoid costly litigation, so developing a strong case is vital for an investigator, because the business will seek to use the investigator's findings to stave off lawsuits.

In corporate investigations, forensic investigators look into data falsification or theft, embezzlement, *industrial espionage* (the selling of confidential or sensitive data to a competitor and company policy violations, such as e-mail harassment or discrimination. In recent years, corporate investigations have focused more on *intrusion detection,* or using software and

hardware components to monitor network traffic for patterns that may indicate the unauthorized access of a company's resources. To avoid troubles with authority and responsibility in investigations, companies should always take care to define clearly the rights and regulations within their stated policies, not only to enable investigators to perform their duties when needed, but also to avoid unnecessary litigation and ensure compliance with all relevant laws, especially those briefly discussed on page 11 of the textbook.

When working on public investigations, forensic professionals must be aware of all the applicable laws regarding the crime and related matters, from city ordinances up to federal guidelines, to collect evidence properly and build a solid case. For crimes that transcend national borders, other countries' laws and international treaties may also apply, so forensic professionals must be comfortable with a broad range of legal guidelines. Despite the number of rules and increasing comfort of the public with electronic data, cases often depend on witnesses to attest to the validity of electronic evidence, so professionals must also keep this in mind when preparing cases.

Given the rise in computer crimes in recent years, nascent professionals may wonder about which factors affect the prioritization cases. While many factors influence the decision, most forensic teams use the

- Amount of harm inflicted in the incident or incidents
- Jurisdiction
- Investigation probability of success
- Availability and training of personnel
- Frequency of incidents

Fortunately, a number of professional associations have sprung up to develop and strengthen the discipline. Some of these professional associations, which offer information on best practices, legal guidelines, and training opportunities, include the High Technology Crime Investigation Association (HTCIA), online at **http://www.htcia.org,** and the International Association of Computer Investigation Specialists (IACIS), at **http://www.iacis.com.**

Training

Although all computer forensic professionals need a broad knowledge base, the type of role being fulfilled has a marked effect on what aspects need greater focus. Certain types of crime, such as child pornography and identity theft, require different skill sets and specialties. In addition, computer forensics skills are used by law enforcement, legal professionals, human resource personnel, security consultants, and private investigators. These professions each have different requirements, so the role that an investigator is undertaking determines the focus.

Getting up to speed in your particular areas can be done in many ways. Many colleges and universities offer courses and programs in computer forensics and other specific areas, such as operating systems and legal procedures. In addition, the SANS Institute (**http://www.sans.org**) and the IACIS offer information on security training. Depending on your employer and role, other institutions may offer various degrees of training; for example, law schools often offer courses on e-discovery methods and rules of evidence, and police academies are increasingly offering training on how to investigate computer crimes and collect evidence.

In the corporate world, security training often is focused on individual roles. End users, for example, have different responsibilities and needs than IT personnel, who need to be aware of vulnerabilities, defensive strategies, and return on investment (ROI). Although many corporations don't see security and IT training as cost-effective, laws such as the Sarbanes-Oxley Act (SOX) require a degree of compliance and diligence in maintaining data security and protection and require organizations to be active in such efforts. The SANS Institute is one resource that corporations can utilize for assistance.

For end users, however, training is likely to be focused primarily on changing behavior that opens systems to attack. In other words, the focus is *security awareness,* or being able to identify and avoid threats before they can attack. Common threats end users need to be able to identify include *malware,* which describes many kinds of malicious code (such as

viruses, logic bombs, and worms) and *social engineering,* which exploits human nature to obtain sensitive information, such as by calling a help desk and pretending to be an employee who will be fired if he or she doesn't get access to a certain report on a server.

Security awareness programs generally focus on a few key goals:

- Evaluate compelling and relevant issues
- Know data protection laws and policies
- Examine organizational values and culture
- Define baseline knowledge standards and best practices
- Make lasting changes to organizational culture and behavior
- Create methods and approaches that are positive, not punitive

With the prevalence of state and federal regulations regarding data protection and security, not to mention the potential consequences of security breaches, all organizations that use computers need to have a security awareness and training program in place.

Organizational Needs

Once it's been decided to develop a security awareness program, it's vital to assess the organization's needs and craft a program based on those. What will be monitored? How will it be monitored? Who will be monitoring the resources? What policies will be implemented? These questions and many others must be addressed.

In general, developing security policies, particularly those on monitoring specific resources, requires professionals to

- Identify resources that may be at risk
- Set up the relevant policies and requirements of each (such as operating system and storage space)
- Create a system for logging and review of logs

Self-Check 1

At the end of each section of *Computer Forensics,* you'll be asked to pause and check your understanding of what you've just read by completing a "Self-Check" exercise. Answering these questions will help you review what you've studied so far. Please complete *Self-Check 1* now.

1. What law covers data protection for publicly held companies?

   _____

2. Which process is used to produce electronic documents for litigation?

   _____

3. Logic bombs and worms are examples of _____.

4. *True or False?* Social engineering exploits human nature to gain information.

5. *True or False?* Human resource professionals need computer forensics professionals and skills.

Check your answers with those on page 115.

ASSIGNMENT 2

Read this assignment, and then read Chapter 2, "Preparation—What to Do Before You Start," on pages 23–54 of your textbook.

Hardware

The staggering number of devices that can store data increases daily. Obvious places to look for digital evidence include computers, external hard drives, smartphones, and flash drives. However, in many cases, data can be retrieved from devices not commonly thought of as storage-capable.