THE FIELD OF SYSTEM FORENSICS is growing and evolving. Forensic tools and methods have improved access to volatile data and remote systems. They have also enhanced analysis of network traffic. Today, more than 50 different software packages assist with system forensics. Examples include Forensic Toolkit (FTK), EnCase, and Paraben’s Device Seizure.

In recent years, the world has seen a vast increase in the number of computers, networks, mobile devices, and other embedded systems, such as video games, e-readers, global positioning system (GPS) devices, and digital video recorders. The increasing attacks on those devices have resulted in an increase in the demand for system forensics professionals.

Many types of evidence can be part of an investigation. A few examples are system access information, financial data related to purchases, e-mail and postal addresses, photographs, Web pages retained in temporary storage, and logs recording network connections. This chapter discusses the difficulties related to obtaining digital evidence. It also addresses the dynamic nature of evidence, scope-related challenges, and the need for professionalization.

Chapter 3 Topics

This chapter covers the following topics and concepts:
- What the difficulties in obtaining forensic digital evidence are
- What role evidence dynamics plays in system forensics
- What the scope-related challenges to system forensics are
- Why there is a need for professionalization
Chapter 3 Goals

When you complete this chapter, you will be able to:

- Explain the factors that can make obtaining forensic evidence difficult
- Understand how easily forensic data can be destroyed
- List scope-related problems in system forensics
- Understand why professionalization would improve the field of system forensics

Difficulties in Obtaining Forensic Digital Evidence

Investigators face four basic difficulties in obtaining forensic digital evidence:

- Deciding what is and what is not evidence
- Gaining access to data
- Understanding the technical considerations related to data collection
- Obtaining obscured data and defeating anti-forensics

The following sections discuss these difficulties.

What Is Digital Evidence?

Data includes raw numbers, pictures, and other “stuff” that may or may not have relevance to a particular event or incident under investigation. Information is data that has been processed and assembled so that it is relevant to an investigation. Evidence is information that supports a specific finding or determination.

Investigators must carefully show an unbroken chain of custody to demonstrate that evidence has been protected from tampering. The chain of custody is continuity of evidence that makes it possible to account for all that has happened to evidence between its original collection and its appearance in court, preferably unaltered. If forensic specialists can’t demonstrate that they have maintained the chain of custody, then the court may consider all their conclusions invalid.

NOTE

Evidence may be conclusive and support a single finding—such as an individual’s DNA identification. Or evidence may be interpretive and support multiple findings—such as photos placed on a desktop by potentially numerous individuals.
Courts deal with four types of evidence:

- **Real**—Real evidence is a physical object that someone can touch, hold, or directly observe. Examples of real evidence are a laptop with a suspect’s fingerprints on the keyboard, a hard drive, a universal serial bus (USB) drive, and a handwritten note.

- **Documentary**—Documentary evidence is data stored as written or printed matter or using information technology. Documentary evidence includes memory-resident data and computer files. Examples are logs, databases, e-mail messages, photographs, and telephone call detail records. Investigators must authenticate documentary evidence.

- **Testimonial**—Testimonial evidence is information that forensic specialists use to support or interpret real or documentary evidence. For example, they may employ testimonial evidence to demonstrate that the fingerprints found on a keyboard are those of a specific individual. Or system access controls might show that a particular user stored specific photographs on a desktop.

- **Demonstrative**—Demonstrative evidence is information that helps explain other evidence. An example is a chart that explains a technical concept to the judge and jury.

Forensic specialists must often provide testimony to support the conclusions of their analyses. For example, a member of an incident response team might be required to testify that he or she identified the computer program that deleted customer records at a specified date and time. In such a case, the testimony must show how the investigator reached his or her conclusion. The testimony must also show that the investigator protected from tampering the data used in making the determination. That is, the testimony must show that the forensic investigator maintained the chain of custody. It must also show that the testifier based his or her conclusion on a reasonable, although not necessarily absolute, interpretation of the data. Further, the forensic specialist must present his or her testimony in a manner that avoids use of technical jargon and complex technical discussions. Judges, juries, and lawyers aren’t all technical experts. Therefore, a forensic specialist should translate technology into understandable descriptions. Pictures often communicate better than just numbers and words, so a forensic specialist may want to create charts and graphs.

**FYI**

Most incidents that forensic specialists investigate begin as rather routine investigations. They begin as investigations of system or processing anomalies or routine analysis of system logs. After analysis and evaluation, an investigation may turn into a legal action. For example, forensic analysis may show that what at first appeared to be a system failure was in fact the result of an outsider attack. Thus, all forensic investigations should be conducted using strict rules of evidence and maintain the chain of custody. Taking these measures ensures that the work of a forensic specialist will be admissible in any court proceedings.
Data Access

Gaining access to digital data is often difficult. A forensic specialist may not be able to gain access to data for a number of reasons. For example, an investigator may face physical constraints, such as the destruction or reformatting of a desktop. Or an investigator may face legal restrictions, such as the owner’s refusal to grant access to the data. Another legal restriction might involve data including information that is protected by law. Finally, an investigator may not be able to access data because of technical issues, such as encryption or data being in a nonstandard format.

Creating a Data Analysis Plan

Data access restrictions may be intentional. An attacker may try to restrict data access to prevent analysis or to prevent the use of the data to support a prosecution. On the other hand, data access restrictions may instead be an unintended consequence of an organization’s or individual’s normal business practices. Regardless of the cause, forensic specialists should plan their analyses. They can do so by creating a data analysis plan, a plan that lists the types of data to be collected and describes the expected source for the data. This plan should also list any anticipated problems as well as recommended strategies to deal with those problems.

Forensic specialists must protect data sources until they have addressed all access restrictions. While planning an investigation, they should keep this in mind. This protection may require legal actions, such as subpoenas. It may also require technical actions, such as mirroring devices to protect the original while analyzing a copy.

Besides identifying the types of data to be collected and their source, a data analysis plan should describe any anticipated problems, along with recommended actions. Table 3-1 lists some of the items that a forensic specialist might include in a data analysis plan.

Overcoming Search and Seizure Restrictions

Restrictions on search and seizure may apply in many investigations. A forensic investigator should obtain authorization to examine devices and collect data. Data collected without appropriate authorization may not be usable in an investigation.

If the equipment or data owner is not the suspect, an investigator could have the legal right to search the computer through voluntary surrender. Voluntary surrender is permission from the owner of a computer or other equipment to search and/or seize equipment as part of an investigation. An investigator would also have a right to voluntary surrender if an employee or a contractor signed a search and seizure consent as a condition of hire.
An investigator who doesn’t have permission to collect evidence can seek one of two court orders:

- **Subpoena**—A **subpoena** is a court order than requires the person or organization that owns the equipment to release it for analysis. Civil actions or court proceedings typically involve subpoenas.

- **Search warrant**—A **search warrant** is a court order that allows law enforcement personnel to collect equipment or data from that equipment. A search warrant may permit collection of the equipment or data with or without advance notice. A forensic specialist should indicate the likelihood that the data could be damaged or lost if the suspect has prior notice. Law enforcement officers typically use search warrants.
Technical Data Collection Considerations

System forensics specialists must keep in mind three main technical data collection considerations. These are understanding the life span of data, collecting data quickly, and collecting bit-level data.

Considering the Life Span of Data

In planning data collection efforts, a forensic specialist must be aware that data has a life span. The nature of the data as well as organizational policies and practices determine the data life span. For example, data regarding network traffic and the messages themselves may exist only for the time the transmission is passing through a server. This may be only milliseconds. Information stored in computer memory may have a life span of a millisecond.

As data life spans increase, the life span determinant is typically related to organizational practice. For example, an organization may establish a policy that an e-mail message may be stored within the e-mail system for only 30 days. After 30 days, any message that is not moved to alternate storage is deleted. Log files may be retained for months or years, in accordance with an organization’s audit policy. Finance and accounting information may have a multiple-year life span that corresponds with requirements established by state or federal governments.

In planning a data collection effort, forensic specialists must be aware of the life span of the data they are seeking. They must use data collection techniques appropriate to the data life span. For example, data with an extremely short life span may require the use of specialized monitoring tools to collect transmissions in process. (See Chapter 12, “Searching Memory in Real Time with Live System Forensics.”)

Collecting Data Quickly

Once the data collection effort is announced or in process, it is important to collect data as quickly as possible. Data changes easily. It is frequently not possible or practical to determine who made a change or when. In addition, the target of an investigation may try to conceal data, which further obscures changes. Networking systems also increase the potential for unauthorized data changes. The person making a change on a network does not have to be local to the device on which the data is stored.

Collecting Bit-Level Data

Data is digitally stored as a series of 1s and 0s. This is called binary representation. To be useful, data must be converted through hardware and software into text, pictures, screen displays, videos, or other human-readable formats.

Forensic specialists should be able to see data in its useful form as well as in its original format. To do so, they need to collect data at the bit level. The specialists can then analyze the layers of procedures and conversions. By using this process, they can determine
whether the data was corrupted. Investigators also look for whether unrelated data was inserted, such as trade secrets buried within other data. Forensic specialists must therefore have tools that allow manipulation and evaluation of bit-level data. Use of bit-level tools also enables an investigator to reconstruct file fragments if data files have been deleted or overwritten.

**Obscured Data and Anti-Forensics**

Two more challenges in obtaining digital evidence are obscured data and anti-forensics.

**Obscured Data**

Data can be obscured in a number of ways. Obscured data may be encrypted, compressed, or in a proprietary format. Sometimes, cybercriminals obscure data to deter forensic examination. More often, companies use data manipulation and storage techniques to protect business-sensitive data. These techniques obscure data. News outlets have reported on many data losses from unintentional and intentional security failures. Therefore, companies and individuals now widely use data protection techniques. Regardless of the reason for obscured data, collecting and analyzing it is difficult.

Data that has been obscured through compression and proprietary formats can sometimes be converted with work and the right tools. Forensic specialists often must do quite a bit of work to decrypt encrypted data. In some cases, however, the investigator cannot decrypt this type of data unless the data owner provides the encryption key and algorithm. When digital evidence has been encrypted and is in use on a live system, an investigator might have to collect evidence through a live extraction process. (Chapter 12, “Searching Memory in Real Time with Live System Forensics,” discusses live extraction in more detail.)

**Anti-Forensics**

Every investigation is unique. Investigations are not necessarily friendly activities. Forensic specialists may have to conduct them with or without the cooperation of the data provider. And the data provider may or may not be the target of the investigation. Investigations with uncooperative data providers are difficult.

An attacker may use techniques to intentionally conceal his or her identity, location, and behavior. For example, perpetrators may conceal their identity by using networked connections at a library, an Internet café, or another public computer. Or they may use encryption or anonymous services to protect themselves. The actions that perpetrators take to conceal their location, activities, or identity are generally termed anti-forensics.

Cybercriminals are becoming better at covering their tracks as their awareness of digital forensics capabilities increases. According to security consultant Scott Berinato, “For every tool forensic investigators have come to rely on to discover and prosecute electronic crimes, criminals have a corresponding tool to baffle the investigation.”
Bill Blunden, author of *The Rootkit Arsenal*, describes six types of anti-forensic activities:

- **Data destruction**—Methods for disposing of data vary. They can be as simple as wiping the memory buffers used by a program. Or they can be as complex as repeatedly overwriting a cluster of data with 1s and 0s until all that is left is random bytes of data. Digital evidence can be destroyed easily. For example, starting a computer updates timestamps and modifies files. Attaching a hard disk or USB stick modifies file system timestamps. Powering off a machine destroys volatile memory. Suspects may delete files and folders and defrag their hard drives in an attempt to overwrite evidence.

- **Data hiding**—Suspects often store data where an investigator is unlikely to find it. They may hide data, for example, in reserved disk sectors or as logical partitions within a defined, public partition. Or they may simply change filenames and extensions.

- **Data transformation**—Suspects may process information in a way that disguises its meaning. For example, they may use encryption to scramble a message based on an algorithm. Or they may use steganography to hide a message inside a larger message, often an image file.

- **Data contraception**—Suspects often store data where a forensic specialist can’t analyze it. For example, they may prevent data from being written to disk by storing it in memory. To do so, they use memory-resident rootkits.

- **Data fabrication**—Suspects often overwhelm forensic analysts with false positives and false leads. For example, they may alter as many files as possible to make it difficult to use a checksum process to identify changed files.

- **File system alteration**—Suspects often corrupt data structures and files that organize data, such as a Windows NTFS (NT File System) volume.

These anti-forensic methods and how forensic specialists combat them are discussed throughout this book. In particular, see Chapter 8, “Understanding Information-Hiding Techniques,” and Chapter 9, “Recovering Data.”

### The Role Evidence Dynamics Plays in System Forensics

Edmond Locard worked as a medical examiner during World War I. He identified causes and places of death by looking at stains or dirt left on soldiers’ uniforms. Earlier, in 1910, he opened the world’s first crime investigation lab. Through his work, he helped found a basic concept of forensic science that became known as **Locard’s exchange principle**. Locard’s principle is associated with the phrase “with contact between two items, there will be an exchange.” Locard’s principle states that when two objects come into contact, there is always transference of material from each object onto the other. In other words, every contact leaves a trace. For example, a criminal might leave fingerprints, a hair, a button, or skin cells. At the same time, the criminal might take away hair, dirt, or blood.
Locard believed that it is impossible for a criminal to act without leaving traces of his or her presence. Thus, forensic specialists focus on identifying the traces that perpetrators leave behind about their activities. Locard’s principle applies not just to traditional forensics but to system forensics as well. With systems forensics, digital evidence replaces blood, hair, fingerprints, and other physical and biological evidence.

Between the time a forensic specialist collects evidence and the time a court hears and rules on a case, evidence may change in a number of ways and for a number of reasons. As discussed elsewhere in this chapter, evidence changes very easily. Evidence dynamics is anything that changes, moves, obscures, or obliterates evidence, regardless of intent. In other words, evidence dynamics is any force that acts on evidence. For digital forensics, these forces must have a hardware or software component. Three types of forces act on evidence:

- **Human**—Human forces on digital evidence include unintentional or deliberate destruction or concealment of data. For example, a system administrator may inadvertently perform an action that obliterates patterns or adds artifacts to a crime scene. On a shared computer, an uninvolved user could use a computer after a crime and destroy or change evidence. Even forensic investigators may adversely affect evidence. Forensic specialists may cause the loss of volatile data when shutting down a live system. Or they might use other inappropriate data handling practices. For example, they might alter data when they copy a file onto a computer from another network or from removable media. Reconstructing files from a damaged hard disk can also lead to evidence corruption.

- **Natural**—Natural forces include fire, water, weather, dust, electricity, and time. Magnetic and optical media decay over time and eventually become unreadable. Therefore, hard drives, CDs, and DVDs have a data retention life expectancy. Electricity is a natural force that can change evidence. Most people recognize that standard electrical current in a home can cause damage and change evidence. However, many people don’t know that an electrostatic discharge (ESD) of only 40 volts can damage equipment. In addition, static electricity can cause data loss.

- **Incidental**—Incidental forces include equipment and software. Operating systems, applications, and forensic software tools such as disk write-blocking software are examples of software that can impact evidence.

Evidence dynamics creates challenges for forensic analysts, making it difficult to prove what actually occurred and to prove that the evidence is reliable. Forensic specialists must establish working environments that eliminate or minimize the impacts of evidence dynamics. The following are some steps they should take:

- Carefully document data received and its source.
- Establish logs and signoffs to demonstrate an unbroken chain of custody.
- Avoid contamination of evidence by placing it on systems where it can be accessed by processes or individuals not involved in the analysis.
Testing Forensic Tools: The CFReDS

An investigator should choose forensic tools and utilities with care and be well versed in their reliability. Calibrating digital forensic tools isn’t easy. The National Institute of Standards and Technology (NIST) provides the Computer Forensic Reference Data Sets (CFReDS) for testing. (See http://www.cfreds.nist.gov.) The four primary applications of CFReDS are testing forensic tools, establishing that lab equipment is functioning properly, testing proficiency in specific skills, and training laboratory staff. Each of these data sets has slightly different requirements. Courts may be more likely to accept evidence collected using tools that have been used in previous trials and that are routinely tested for reliability.

- Wear a grounding wristband and use antistatic protective mats and surfaces, when possible, to prevent ESD.
- Maintain a humidity level of 40 percent to 60 percent to reduce ESD.
- Use static-free storage bags for storing or moving equipment to reduce the potential for ESD damage.
- Use appropriate procedures to ensure that data are purged from all storage devices when no longer needed, with good documentation of the data disposal.
- Destroy data when appropriate by overwriting media with 1s and 0s.
- Test the tools used.

For more information on the steps forensic analysts should take, see Chapter 6, “Controlling a Forensic Investigation,” and Chapter 7, “Collecting, Seizing, and Protecting Evidence.”

Scope-Related Challenges to System Forensics

The scope of a forensic effort often presents not just an analytical challenge but a psychological challenge as well. Information systems collect and retain large volumes of data. They store this data in a dizzying array of applications, formats, and hardware components. In completing an analysis, forensic specialists face variations in the following:

- The volume of data to be analyzed
- The complexity of the computer system
- The size and character of the crime scene, which might involve a network that crosses U.S. and foreign jurisdictions
- The size of the caseload and resource limitations

Forensic specialists must be prepared to quickly complete an analysis regardless of these factors. The following sections discuss these factors in more detail.
Large Volumes of Data

Digital forensics is useful in identifying and documenting evidence. It is a disciplined approach that looks at the entire physical media, such as a hard disk drive, for all data representations. A system forensics specialist has access to all the data contained on a device—not just what the end user sees. A forensic analyst examines metadata, such as disk partition structures and file tables. An analyst also examines the often-critical unused areas of the media where data might be hidden. Examining all areas of potential data storage and examining all potential data representations generates extremely large volumes of data. A forensic specialist must analyze, store, and control all this data for the full duration of the investigation and analysis.
The total amount of data that is potentially relevant to a case offers a challenge to forensic analysts. Most hard drives now contain in excess of 1 million file items. It is, in fact, common for a single desktop to have 1 terabyte of data storage. When working with such large volumes of data, a forensic specialist must do the following:

- Ensure that his or her equipment is capable of manipulating large volumes of data quickly
- Provide for duplicate storage so that the original media and its resident data are preserved and protected against tampering and other corruption
- Create backups early and often to avoid losing data
- Document everything that is done in an investigation and maintain the chain of custody

In addition to all these tasks, a forensic specialist must support the forensic budget. Manipulating and controlling large volumes of data is expensive. An investigator should show how budget cost items contribute to the analysis and to maintaining the chain of custody. Resource limitations increase the potential for analysis error and compromise of the analysis. For example, a forensic analyst may need to explain how the addition of data custodians or additional hard drives can multiply costs. (For more information on budgeting for a forensics lab, see Chapter 4, “Forensics Methods and Labs.”)

**System Complexity**

Modern computer systems can be extremely complex. They use multiple file formats, including Adobe Portable Document Format (PDF) files and Tagged Image File Format (TIFF) image files. They connect to and share data with other systems that may be located anywhere in the world. In addition, the law may protect specific data items. No single forensic software application can deal with all this complexity.

Forensic specialists must use a set of software and hardware tools and supporting manual procedures. Further, a forensic specialist must build a case to support his or her interpretation of the “story” told by the data being analyzed. The specialist therefore must have an understanding of data and technology. The specialist should also be able to show corroboration that meets the traditional legal evidence tests.

The fact that individual pieces of data may have more than one possible interpretation compounds system complexity. To reach a conclusion and turn data into supportable evidence, a forensic specialist must identify and analyze corroborating information. A forensic specialist must use data to create evidence to support a conclusion provided by the data. In building a case for corroborating evidence, a forensic specialist may want to compare the results from using two different tools. By doing so, the specialist could demonstrate that two different analytical tools examining the same set of data reached the same conclusion. Conversely, the tools may reach different conclusions, showing that the data does not support the conclusion. Either case is valuable to a forensic specialist.
Distributed Crime Scenes

Digital crime scenes can span the globe. Depending on the type of system connectivity and the in-place controls, a forensic specialist may have to deal with data stored throughout the world. This could involve thousands of devices and network logs. Networks and centralized storage also present challenges because items of interest may not be stored on the target computer.

Because networks are distributed, crime scenes are also distributed. This creates practical as well as jurisdictional problems. (Think about how difficult it is for a U.S. investigator to get evidence out of computers in China.) Criminals take advantage of jurisdictional differences between governments. A criminal may sell fake merchandise from a foreign country to Americans in several states. The criminal may then route his or her Internet access through several other countries before it reaches its final destination. Stopping this type of boundary shifting requires the cooperation of state governments, federal governments, and international agencies in tracking down the criminal and bringing him or her to justice. If all the governments and agencies do not cooperate with one another, the investigation may fail.

Growing Caseload and Limited Resources

Regardless of the state of the economy, forensic specialists can be assured of two things: Their caseload will grow, and their resources will become more limited.

The forensic analysis workload is growing and will continue to grow for the foreseeable future. Driving this growth is the increasing use of technology in all aspects of modern life, not just in support of business objectives. Perpetrators have found that using technology
to commit or support a crime reduces the risk of getting caught. The number of forensic specialists today is too small to analyze every cybercrime. In addition, the “take” from an individual crime generally is too small for law enforcement to pursue every crime.

Organizations and people using technology often do not use proper control measures, which increases the number of potential targets. The number of organizations and individuals who want to prosecute perpetrators is increasing. In part, they want to catch perpetrators who stole from them. In addition, they have a legal and fiduciary duty to protect organizational assets.

Forensic specialists can take four basic actions to address the growing workload with constrained resources:

- **Continue learning**—Forensic specialists should learn how to use the new tools. They should also learn best practices and techniques developed by others and incorporate them into their analyses. This will help reduce costs by building on the work of others. It will also maximize the use of technology to reduce the costs associated with the large volumes and complexity of analyses.

- **Formalize procedures**—Establishing strict written procedures for collecting and protecting data will ultimately reduce the costs of analyses. Judges and juries are often more likely to accept a forensic specialist’s findings if the specialist can show a clear, documented process that can be independently reviewed and is repeatable.

- **Prepare a business case**—Forensic specialists compete with all other activities in an organization for a share of the funds available. Simply stating that forensic analyses can be improved by using a new tool or a new lab is not sufficient. Forensic analysts must prepare a comprehensive business case that demonstrates the need, provides reliable cost estimates, and shows how the organization will benefit from the resource investment. They should support their position on benefits by discussing past successful case analyses. Benefits derived from the investment should be stated in terms of compliance with law, improved analytical quality, and improved capability to address larger, more complex cases. They should also be stated in terms of reduced cost of performance for equivalent workloads. The business case should clearly show that the return on investment (ROI) can be favorably compared to competing requirements.

- **Prioritize workload**—To take advantage of limited resources, forensic specialists must prioritize their workloads. They should establish a formal process with defined criteria for making choices about which cases to accept, which analyses to perform, and the desired depth of analysis. A formal prioritization structure will allow those seeking forensic support to know how the process works. The information generated through the process—cases accepted, cases declined, and so on—will provide support for a business case for added resources. For example, a forensic specialist may objectively demonstrate that funds provided are used most effectively and that there is a legitimate need for a budget increase.
The field of digital forensics is still in the process of maturing. Businesses, institutions, and individuals still view digital forensics as somewhat of a “dark science” where investigators perform analysis in a black box and users accept results without question. Forensic specialists sometimes lose cases because decision makers are not familiar with the capabilities and limitations of forensics and with what constitutes appropriate documentation.

The field of digital forensics will mature as experts incorporate more rigor into analysis processes. In addition, digital forensics will become an accepted analytical approach as the forensic specialist position becomes a professionalized career. Professionalization involves establishing a body of knowledge that forensic specialists should know and against which training and testing can be directed.

Professionalization will also bring more definition to the field, including guidelines and standards for the following:

- Training and certification of forensic specialists
- How to perform forensic analyses
- Supporting forensic evidence
- Data collection that doesn’t disrupt ongoing operations
- Standards for defining digital search warrants and subpoenas
- Standards for protecting digital evidence
- Specific terminology used in describing and documenting forensic activities

A forensic specialist faces many challenges. Among them are lack of a defined career path, lack of standards, and an increasing workload with constrained resources. Resolving these challenges in a new technological discipline can be rewarding. But it requires work. Even as they address the technological challenges associated with performing an analysis, forensic specialists must also begin the process of instituting formal procedures so that the results of their work will be more readily accepted. This means that forensic specialists must not just look at their work as an opportunity to use new tools to perform interesting analyses. They must also recognize the value of maturing their industry.

Forensic specialists can focus their efforts on the following issues to help establish digital forensics as an accepted discipline:

- Training and certification
- Restrictions on search and seizure
- Standards for protecting digital evidence
- Standards for performing digital forensics
- Guidelines for presenting digital evidence
- Requirements for addressing cross-border issues between states and between countries
- Guidelines for analyzing common devices, such as PDAs, GPS devices, mobile phones, laptops, and desktops

NOTE

The National Academy of Sciences is concerned that there is currently too much variability in and uncertainty about the education, experience, and training of those practicing forensics. Professionalization would resolve this concern.
The field of system forensics faces many challenges. One of the major challenges is the difficulty of obtaining digital evidence. Data access, restrictions on search and seizure, and the ease with which digital evidence can be altered or destroyed play important roles in obtaining accurate and reliable evidence. In addition, evidence dynamics creates challenges for forensic analysts by making it more difficult to prove what actually occurred. Other challenges are related to scope. The amount of data stored on hard drives continues to increase, and this raises the cost of full disk imaging and analysis. Distributed crime scenes, especially those that cross jurisdictions, are also problematic. The great number and variety of devices that can contain digital evidence adds to the broad scope of system forensics. New software and hardware constantly become available, making it impossible for a single forensic analyst to be experienced in all operating systems, hardware platforms, devices, programs, and forensic applications and tools.

The field of system forensics is evolving. Many options for training and education are available. However, there is a need for professionalization and standards. Those involved in its early formative years will be rewarded in performing the work while helping to shape the future characteristics of the discipline.
1. Which of the following is data that has been processed and assembled so that it is relevant to an investigation?
   A. Data
   B. Forensic data
   C. Information
   D. Evidence

2. Which types of evidence are used in court?
   (Select three.)
   A. Documentary evidence
   B. Forensic evidence
   C. Real evidence
   D. Testimonial evidence
   E. Hearsay

3. A forensic specialist may not be able to gain access to data because of physical constraints, legal restrictions, or technical issues.
   A. True
   B. False

4. A _______ should identify the types of data to be collected and describe the expected source for the data. It should also list any anticipated problems as well as recommended strategies to deal with those problems.

5. Which of the following is a court order than requires a person or an organization that owns subject equipment to release it for analysis?
   A. Voluntary surrender
   B. Search warrant
   C. Arrest warrant
   D. Subpoena
   E. Trial

6. Which of the following is the name for actions that perpetrators take to conceal their location, activities, or identity?
   A. Obscured data
   B. Documentary evidence
   C. Anti-forensics
   D. Evidence dynamics
   E. Voluntary surrender

7. _______ states that when two objects come into contact, there is always transference of material from each object onto the other. In other words, every contact leaves a trace.
   A. True
   B. False

8. Evidence dynamics is anything that changes, moves, obscures, or obliterates evidence, regardless of intent.
   A. True
   B. False

9. Perpetrators have found that using technology to commit or support a crime increases the risk of getting caught.
   A. True
   B. False

10. What are some of the challenges a forensic specialist faces? (Select three.)
    A. Lack of tools
    B. Increasing workload
    C. Constrained resources
    D. Lack of professionalization
    E. Hearsay