Test Bank for Practical Guide to Digital Forensics Investigations 2nd Hayes

Access Complete Test Bank for Practical Guide to Digital Forensics Investigations 2nd Hayes

Chapter 1

True/False

1. Computer forensics is the retrieval, analysis, and use of digital evidence in a civil or criminal investigation.
   True - Computer forensics is not limited to computers as the source of evidence. Any medium that can store digital files is a potential source of evidence for a computer forensics investigator. Therefore, computer forensics involves the examination of digital files.

2. The use of computer forensics is sometimes used as incriminating evidence in criminal cases and is often referred to as exculpatory evidence.
   False – Incriminating evidences is inculpatory evidence. Exculpatory evidence is evidence used to prove the innocence of a defendant.

3. Email printouts have been accepted as evidence in court.
   True – In Rombom, et al. v. Weberman et al. the judge accepted email printouts. The plaintiff testified that he had received emails from the defendant and printed them.

4. The primary purpose of a client computer is to deliver HTML documents and related resources (like images) in response to client computer requests.
   False -- A web server delivers HTML documents. The easiest way to remember what a client and a server do is to think of a client as a customer and a server as providing a service.

5. BitLocker is an encryption tool that was introduced with the Ultimate and Enterprise editions of Microsoft Windows Vista.
   True – BitLocker allows for encryption at the file, folder, or drive level.

6. The common communication Internet protocol is known as HTML.
   False – HTML is a computer language. HyperText Transport Protocol, or HTTP, is the common communication Internet protocol.

7. The FBI is the world's largest international police organization.
   False -- INTERPOL is the world's largest international police organization, representing 188 member countries.

8. Headquartered in Glynco, Georgia, the Federal Law Enforcement Training Center (FLETC) is an interagency law enforcement training organization for more than 80 federal agencies nationwide.
   True – One of the programs it provides is the Seized Computer Evidence Recovery Specialist (SCERS). FLETC also provides training in topics such as Mac forensics and network forensics.

Access Complete Test Bank for Practical Guide to Digital Forensics Investigations 2nd Hayes

9. Closed-circuit television (CCTV) refers to use of video that is transmitted to a particular location.
   True -- In the city of London, there are an estimated 500,000 CCTV cameras. These cameras have been used to investigate tourists who have been robbed of their possessions or the high-profile cases like the poisoning of former Russian spy Alexander Litvenko in 2006.

10. InfraGard is a public-private agency of the FBI that promotes the exchange of information between the private and public sectors on issues related to terrorism, intelligence, and security matters.
    True -- InfraGard has established local chapters nationally, and membership is open to all U.S. citizens, who are subject to an FBI background check.

Multiple Choice

1. The word _____ means "suitable for court."
   a. Forensics
   b. Inculpate
   c. Exculpate
   d. None of the above
   Answer: A. This definition infers that digital evidence used in an investigation needs to be retrieved, handled, and analyzed in a forensically sound manner.
2. _____ evidence is used to prove the innocence of a defendant.
   a. Inclusionary
   b. Exclusionary
   c. Exculpatory
   d. Inculpatory
   Answer: C. Evidence that is incriminating is inclupatory.

3. File _____ is information about a file and can include the creation, modified, and last access dates.
   a. Posting
   b. Metadata
   c. Processes
   d. None of the above
   Answer: B. Metadata is data about data.

4. A _____ is a device used to illegally capture the data stored on the magnetic stripe of an ATM card, credit card, or debit card.
   a. Recorder
   b. Creditor
   c. Skimmer

Access Complete Test Bank for Practical Guide to Digital Forensics Investigations 2nd Hayes

d. Striper
Answer: C. Surveillance video can be critical to the successful capture of criminals using skimmers.

5. Encryption is the process of scrambling plain text into an unreadable format using a mathematical formula known as a(n) _____.
   a. Algorithm
   b. Skimmer
   c. Heuristic
   d. None of the above
   Answer: A. With advancements in encryption and the nature of the evidence that is lost if the plug is pulled, most investigators agree that a live system should be forensically examined while it is turned on.

Short Answer

1. Dr. Edmond Locard developed a theory known as _____ of Evidence.
   Answer: Transfer. The premise is that whenever a criminal comes into contact with his environment, a cross-transference of evidence occurs.

2. _____ is defined as the concealment, destruction, alteration, or falsification of evidence.
   Answer: Endurance. It is a serious crime that carries a felony charge in many states.

3. BMP, JPEG, TIFF, and PNG are examples of _____ files.
   Answer: Picture or Image. These are the most widely used image formats.

4. The _____ Amendment of the Constitution deals with search and seizure.
   Answer: Fourth. Knowledge of the rules of search and seizure is important if a suspect's computer is located at the person's residence.

5. The Magnetic Media Program, which subsequently became known as the Computer Analysis and Response Team (CART) was established by the _____.
   Answer: FBI. The group was responsible for computer forensics examinations.

6. _____ centers are central repositories for collecting intelligence at the state and local levels with the goal of preventing terrorist attacks.
   Answer: Fusion. The project is a joint initiative between the Department of Homeland Security (DHS) and the Department of Justice (DOJ).

7. A(n) _____, is an FBI-sponsored laboratory used to train law enforcement in the use of computer forensics tools.

Access Complete Test Bank for Practical Guide to Digital Forensics Investigations 2nd Hayes

Answer: RCFL, or Regional Computer Forensics Laboratory. The laboratories are also used for law enforcement personnel from different agencies to collaborate on criminal investigations.

8. Achieving a degree in computer forensics, information technology, or even information systems can provide a strong foundation in computer forensics. A degree supplemented by _____ provides greater competencies in the field and makes a candidate even more marketable to a potential employer.
   Answer: Certifications. This is because many certification classes are taught by industry professionals and include hands-on training with professional tools.

9. A forensic _____is an individual who has an accounting background and is involved with financial investigations.
   Answer: Accountant. The American College of Forensics Examiners International provides training and assessment for the Certified Forensic Accountant (Cr.FA) certification.

10. _____, is often referred to as short-term memory or volatile memory because its contents largely disappear when the computer is powered down.
    Answer: RAM, or Random Access Memory. A user's current activity and processes, including Internet activity, are stored in RAM.

Matching

A. Chain of Custody
B. Computer security
C. eDiscovery
D. Global Positioning System
E. Spoliation of evidence
F. Tampering with evidence
G. Bit-stream imaging tool
H. Computer Analysis and Response Team
I. Computer Technology Investigators Network
J. Federal Law Enforcement Training Center

a. Documentation of each person who has been in contact with evidence, from it seizure, to its investigation, to its submission to court
b. Prevention of unauthorized access to computers and their associated resources
c. The recovery of digitally stored data
d. A device that receives communications from orbiting satellites to determine geographic location
e. Hiding, altering, or destroying evidence related to an investigation
f. The concealment, destruction, alteration, or falsification of evidence
g. A tool that produces a bit-for-bit copy of original media, including files marked for deletion

Access Complete Test Bank for Practical Guide to Digital Forensics Investigations 2nd Hayes

h. A unit within the FBI that is responsible for providing support for investigations that require skilled computer forensics examinations
i. An organization committed to the exchange of ideas and practices in computer forensics
j. An interagency law enforcement training organization for more than 80 federal agencies nationwide

Access Complete Test Bank for Practical Guide to Digital Forensics Investigations 2nd Hayes