Digital Forensics Investigation and Response 5E 5th edition Easttom Test Bank

SKU: 9781284305944-TEST-BANK

Import Settings:
Base Settings: Brownstone Default
Information Field: Complexity
Information Field: Ahead
Information Field: Subject
Information Field: Title
Information Field: Feedback
Information Field: Taxonomy
Highest Answer Letter: D
Multiple Keywords in Same Paragraph: No
NAS ISBN13: 9781284313321, add to Ahead, Title tags

Chapter: Chapter 01 - Quiz

Multiple Choice

1. Which of the following is the best definition of “forensics”?
A) Actions that perpetrators take to conceal their locations, activities, or identities
B) Testimony taken from a witness or party to a case before a trial
C) The use of science and technology to investigate and establish facts in criminal or civil courts of law
D) The process of using scientific knowledge for collecting, analyzing, and presenting digital computer evidence to the courts
Ans: C
Complexity: Moderate
Ahead: What Is Computer Forensics?
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: The American Heritage Dictionary defines forensics as “the use of science and technology to investigate and establish facts in criminal or civil courts of law.”
Taxonomy: Analyze

2. Which of the following is not true of computer forensics?
A) The objective is to recover, analyze, and present computer-based material in such a way that it can be used as evidence in a court of law.
B) The emphasis is on the volume of evidence.
C) A forensic specialist must adhere to stringent guidelines.
D) Any device that can store data is potentially the subject of computer forensics.
Ans: B
Complexity: Difficult
Ahead: What Is Computer Forensics?
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: In computer forensics, the emphasis is on the integrity and security of evidence.
Taxonomy: Understand

3. _____ is information that has been processed and assembled to be relevant to an investigation and that supports a specific finding or determination.
A) Anti-forensics
B) Expert testimony
C) Digital evidence
D) The Daubert Standard
Ans: C
Complexity: Easy
Ahead: Understanding the Field of Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: Digital evidence is information that has been processed and assembled so that it is relevant to an investigation and supports a specific finding or determination. Raw information is not, in and of itself, evidence. Data must be relevant to a case in order to be evidence.
Taxonomy: Understand

4. _____ is the continuity of control 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.
A) The chain of custody
B) Documentary evidence
C) Demonstrative evidence
D) Consistent scientific manner
Ans: A
Complexity: Moderate
Ahead: Understanding the Field of Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: The chain of custody is the continuity of control 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, the court may consider all their conclusions invalid.
Taxonomy: Understand

5. Tonya is an attorney. She is preparing evidence to be presented in a court trial. Her exhibits include several photographs, printouts of email messages, and printouts of text messages. What type of evidence is Tonya preparing?
A) Demonstrative evidence
B) Documentary evidence
C) Testimonial evidence
D) Real evidence
Ans: B
Complexity: Moderate
Ahead: Understanding the Field of Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: Documentary evidence is data stored as written matter, on paper or in electronic files. Documentary evidence can include email messages, text messages, logs, databases, photographs, telephone call-detail records, and similar items.
Taxonomy: Apply

6. Ed is an expert witness providing testimony in court. He uses a high-tech computer animation to explain a technical concept to the judge and jury. What type of evidence is Ed using?
A) Real
B) Documentary
C) Demonstrative
D) Testimonial
Ans: C
Complexity: Moderate
Ahead: Understanding the Field of Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: Demonstrative evidence is information that helps explain other evidence. An example is a chart or another type of visual that explains a technical concept to the judge and jury.
Taxonomy: Apply

7. Which of the following is the process of examining data traffic, including transaction logs and real-time monitoring using sniffers and tracing?
A) Live system forensics
B) Software forensics
C) Network forensics
D) Email forensics
Ans: C
Complexity: Moderate
Ahead: Understanding the Field of Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: Network forensics is the process of examining network traffic, including transaction logs and real-time monitoring using sniffers and tracing.
Taxonomy: Understand

8. Which of the following is the process of searching memory in real time, typically for working with compromised hosts or to identify system abuse?
A) Live system forensics
B) Internet forensics
C) Network forensics
D) Disk forensics
Ans: A
Complexity: Moderate
Ahead: Understanding the Field of Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: Live system forensics is the process of searching memory in real time, typically for working with compromised hosts or to identify system abuse.
Taxonomy: Understand

9. One must be able to show the whereabouts and custody of evidence, and how it was handled and stored and by whom, from the time the evidence is first seized by a law enforcement officer or civilian investigator until the moment it is shown in court. What standard does this refer to?
A) Consistent scientific manner
B) Chain of custody

C) Demonstrative evidence
D) Real evidence
Ans: B
Complexity: Easy
Ahead: Understanding the Field of Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: From the time evidence is first seized by a law enforcement officer or civilian investigator until the moment it is shown in court, those managing a case must be able to show the whereabouts and custody of the evidence, and how and by whom it was handled and stored, at all times. Failure to maintain proper chain of custody can lead to evidence being excluded from trial.
Taxonomy: Understand

10. Arturo is a forensic investigator. He is working on a digital forensic case that involves tracking down evidence and perpetrators in the United States, Russia, and Italy. He must coordinate with local, state, and national governments, as well as international agencies, in each country. What type of scope-related challenge is being described?
A) Large volumes of data
B) System complexity
C) Distributed crime scene
D) Growing caseload and limited resources
Ans: C
Complexity: Moderate
Ahead: Understanding the Field of Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: Digital crime scenes can span the globe. Depending on the type of system connectivity and the controls in place, a forensic specialist may have to deal with information stored throughout the world and often in languages other than English.
Taxonomy: Apply

11. Assume you run the _____ command on a computer. The command displays the computer's Internet Protocol (IP) address, the IP address for the default gateway, and more information.
A) tracert
B) ipconfig
C) ping
D) traceroute
Ans: B
Complexity: Easy
Ahead: Knowledge Needed for Computer Forensics Analysis
Subject: Chapter 1
Title: Introduction to Forensics
Feedback:
Taxonomy: Understand

12. Alice is a computer hacker. She is attempting to cover her tracks by repeatedly overwriting a cluster of data on a hard disk with patterns of 1s and 0s. What general term describes Alice's actions?
A) Obfuscation
B) Data transformation
C) Anti-forensics
D) Disk forensics

Ans: C
Complexity: Difficult
Ahead: Knowledge Needed for Computer Forensics Analysis
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: The actions that perpetrators take to conceal their locations, activities, or identities are generally termed anti-forensics.
Taxonomy: Apply

13. A computer crime suspect stores data where an investigator is unlikely to find it. What is this technique called?
A) Data hiding
B) Data destruction
C) Data transformation
D) File system alteration
Ans: A
Complexity: Moderate
Ahead: Knowledge Needed for Computer Forensics Analysis
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: Storing data where an investigator is unlikely to find it is referred to as data hiding. A suspect 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.
Taxonomy: Understand

14. _____ is the concept that any scientific evidence presented in a trial has to have been reviewed and tested by the relevant scientific community.
A) The Daubert Standard
B) Demonstrative evidence
C) Consistent scientific manner
D) Documentary evidence
Ans: A
Complexity: Moderate
Ahead: The Daubert Standard
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: The Daubert Standard requires that any scientific evidence presented in a trial has to have been reviewed and tested by the relevant scientific community. For a computer forensics investigator, that means that any tools, techniques, or processes you utilize in your investigation should be ones that are widely accepted in the computer forensics community. You cannot simply make up new tests or procedures.
Taxonomy: Understand

15. The _____ is a federal wiretap law for traditional wired telephony that was expanded to include wireless, Voice over Internet Protocol (VoIP), and other forms of electronic communications.
A) Communications Assistance for Law Enforcement Act of 1994
B) Federal Privacy Act of 1974
C) Wireless Communications and Public Safety Act of 1999
D) Telecommunications Act of 1996
Ans: A
Complexity: Easy

Ahead: U.S. Laws Affecting Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback:
Taxonomy: Remember

16. The _____ was passed to improve the security and privacy of sensitive information in federal computer systems. The law requires the establishment of minimum acceptable security practices, the creation of computer security plans, and training of system users or owners of facilities that house sensitive information.
A) Federal Privacy Act of 1974
B) Computer Security Act of 1987
C) Telecommunications Act of 1996
D) USA PATRIOT Act
Ans: B
Complexity: Easy
Ahead: U.S. Laws Affecting Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback:
Taxonomy: Remember

17. _____ is a computer's physical address.
A) A logical port number
B) An IP address
C) A MAC address
D) A physical port
Ans: C
Complexity: Moderate
Ahead: Knowledge Needed for Computer Forensics Analysis
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: A Media Access Control (MAC) address is a six-byte address used to identify a network interface card. The first three bytes identify the vendor; the second three identify the specific card. This can also be referred to as a computer's physical address.
Taxonomy: Understand

18. _____ is the default file system for Apple computers using macOS 10.XX.
A) NTFS
B) APFS
C) Ext4
D) ReiserFS
Ans: B
Complexity: Moderate
Ahead: Knowledge Needed for Computer Forensics Analysis
Subject: Chapter 1
Title: Introduction to Forensics
Feedback:
Taxonomy: Remember

19. Which of the following is not true of random access memory (RAM)?
A) It cannot be changed.
B) It is volatile memory.
C) It stores programs and data that are currently open.
D) It retains items in memory for as long as the computer has power supplied to it.
Ans: A
Complexity: Moderate
Ahead: Knowledge Needed for Computer Forensics Analysis
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: RAM is volatile memory, and it stores the programs and data you currently have open, but only for as long as the computer has power supplied to it. Read-only memory (ROM) is not volatile and cannot be changed.
Taxonomy: Analyze

20. What term describes information that forensic specialists use to support or interpret real or documentary evidence? For example, a specialist might demonstrate that a user stored specific photographs on a desktop.
A) The Daubert Standard
B) Demonstrative evidence
C) Digital evidence
D) Testimonial evidence
Ans: D
Complexity: Moderate
Ahead: Understanding the Field of Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: Testimonial evidence is information that forensic specialists use to support or interpret real or documentary evidence.
Taxonomy: Understand

True/False

1. True or False? The term “expert report” refers to testimony taken from a witness or party to a case before a trial.
Ans: False
Complexity: Easy
Ahead: What Is Computer Forensics?
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: The term “deposition” refers to testimony taken from a witness or party to a case before a trial.
Taxonomy:

2. True or False? Two ways to present evidence in a forensic case are the expert report and expert testimony.
Ans: True
Complexity: Easy

Ahead: What Is Computer Forensics?
Subject: Chapter 1
Title: Introduction to Forensics
Feedback:

3. True or False? An expert witness testifies on the basis of scientific or technical knowledge relevant to a case, rather than on the basis of direct personal experience.
Ans: True
Complexity: Moderate
Ahead: What Is Computer Forensics?
Subject: Chapter 1
Title: Introduction to Forensics
Feedback:

4. True or False? Disk forensics includes both the recovery of hidden and deleted information and the process of identifying who created a file or message.
Ans: True
Complexity: Difficult
Ahead: Understanding the Field of Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback:

5. True or False? A sector is the basic unit of data storage on a solid-state disk.
Ans: False
Complexity: Moderate
Ahead: Knowledge Needed for Computer Forensics Analysis
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: A sector is the basic unit of data storage on a hard disk drive.

6. True or False? The Windows Registry is essentially a repository of all settings, software, and parameters for Windows.
Ans: True
Complexity: Easy
Ahead: Knowledge Needed for Computer Forensics Analysis
Subject: Chapter 1
Title: Introduction to Forensics
Feedback:

7. True or False? Metadata describes data about information, such as disk partition structures and file tables.
Ans: True
Complexity: Moderate
Ahead: Understanding the Field of Digital Forensics
Subject: Chapter 1

Title: Introduction to Forensics
Feedback:

8. True or False? A warrant is not needed when evidence is in plain sight.
Ans: True
Complexity: Moderate
Ahead: U.S. Laws Affecting Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback:

9. True or False? In most cases, law enforcement may not search a mobile phone without a warrant if they do not have the owner's consent.
Ans: True
Complexity: Moderate
Ahead: U.S. Laws Affecting Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback:

10. True or False? The Electronic Communications Privacy Act of 1986 protects children 13 years old and younger from the collection and use of their personal information by websites.
Ans: False
Complexity: Difficult
Ahead: U.S. Laws Affecting Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: The Children's Online Privacy Protection Act of 1998 (COPPA) protects children 13 years of age and younger from the collection and use of their personal information by websites.

11. True or False? Raw information is always considered to be evidence.
Ans: False
Complexity: Difficult
Ahead: Understanding the Field of Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: Data has to be relevant to a case in order to be evidence.

12. True or False? If you change the extension of a file so it looks like some other type of file, you also change the file structure itself.
Ans: False
Complexity: Moderate
Ahead: Knowledge Needed for Computer Forensics Analysis
Subject: Chapter 1
Title: Introduction to Forensics

Feedback: Any document, spreadsheet, picture, video, or even program is a file. You can change the extension of a file so that it looks like some other type of file. However, that will not change the file structure itself.

13. True or False? Investigators must authenticate documentary evidence.
Ans: True
Complexity: Moderate
Ahead: Understanding the Field of Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback:

14. True or False? Internet forensics is the study of the source and content of email as evidence.
Ans: False
Complexity: Moderate
Ahead: Understanding the Field of Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: Internet forensics is the process of piecing together where and when a user has been on the internet. Email forensics is the study of the source and content of email as evidence.

15. True or False? Real evidence means physical objects that can be touched, held, or directly observed, such as a laptop with a suspect's fingerprints on it.
Ans: True
Complexity: Moderate
Ahead: Understanding the Field of Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback:

16. True or False? Volatile memory is computer memory that requires power to maintain the data it holds.
Ans: True
Complexity: Moderate
Ahead: Knowledge Needed for Computer Forensics Analysis
Subject: Chapter 1
Title: Introduction to Forensics
Feedback:

17. True or False? Disk forensics refers to the process of examining malicious computer code.
Ans: False
Complexity: Moderate
Ahead: Understanding the Field of Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: Software forensics, or malware forensics, refers to the process of examining malicious computer code.

18. True or False? To avoid changing a computer system while examining it, make a forensic copy and work with that copy.
Ans: True
Complexity: Easy
Ahead: Understanding the Field of Digital Forensics
Subject: Chapter 1
Title: Introduction to Forensics
Feedback:

19. True or False? The underlying operating system of macOS is based on Windows.
Ans: False
Complexity: Easy
Ahead: Knowledge Needed for Computer Forensics Analysis
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: The underlying operating system of macOS is based on UNIX. This means that many forensic techniques you can use on Linux can also be used on Macintosh.

20. True or False? The U.S. Secret Service is the premier federal agency tasked with combating cybercrime.
Ans: True
Complexity: Moderate
Ahead: Federal Guidelines
Subject: Chapter 1
Title: Introduction to Forensics
Feedback: