

CHAPTER 1: FORENSIC EVIDENCE AND CRIME INVESTIGATION

Multiple Choice:

1. Which of the following are required by forensic investigators?

- A. Their expertise
- B. Their objectivity
- C. Their problem-solving skills
- D. All are required

Answer: D **Reference:** Introduction

Difficulty: Moderate

2. Which of the following does NOT leave e-evidence?

- A. Instant message
- B. Word processing document file
- C. Hard copy
- D. Digital camera

Answer: C **Reference:** Introduction

Difficulty: Easy

3. Why wasn't Robert Morris sent to prison?

- A. There was no physical damage.
- B. There wasn't any e-evidence.
- C. There weren't enough computers damaged to constitute a crime.
- D. There were no laws under which they could convict him.

Answer: D **Reference:** Basics of Crimes

Difficulty: Moderate

4. Who was arrested as the author of the Lovebug virus?

- A. Francisco Antonelli
- B. Onel de Guzman
- C. Gunter Hanz
- D. Ray Chi Chen

Answer: B **Reference:** Basics of Crimes

Difficulty: Moderate

5. Criminal statutes define crimes in terms of required acts and a required state of mind, typically referred to as
- A. The person's motivation
 - B. The person's psychological makeup
 - C. The person's needs at the time
 - D. The person's intent

Answer: D **Reference:** Caution: Criminal Statutes **Difficulty:** Difficult

6. Crimes are divided into the categories of
- A. Criminal and civil crimes
 - B. Felonies and misdemeanors
 - C. Crimes against persons and crimes against property
 - D. Insider crimes and intrusion crimes

Answer: B **Reference:** Crime Categories and Sentencing Guidelines **Difficulty:** Moderate

7. Crimes against computers can include which of the following?
- A. Attacks on networks
 - B. Unauthorized access
 - C. Tampering with data
 - D. All the above

Answer: D **Reference:** Cybercrimes **Difficulty:** Easy

8. What piece of legislation makes it a crime to send e-mail using false headers?
- A. CAN-SPAM Act
 - B. CFAA
 - C. FERPA
 - D. USA PATRIOT Act

Answer: A **Reference:** Cybercrimes **Difficulty:** Moderate

9. The CFAA was significantly revised to add a civil law component in

- A. 2001
- B. 1994
- C. 1989
- D. 1990

Answer: B **Reference:** Statutes Amended to Keep Pace with Cybercrimes **Difficulty:** Moderate

10. Military planners, recognizing the need to include cyberwarfare in its defenses, have given this new field the acronym of

- A. PII
- B. C4I
- C. P2I
- D. P2M

Answer: B **Reference:** Information Warfare **Difficulty:** Moderate

11. Which of the following has the most far-reaching effect for law enforcement concerning cybercrimes?

- A. FERPA
- B. CFAA
- C. CAN-SPAM Act
- D. USA PATRIOT Act

Answer: D **Reference:** Information Warfare **Difficulty:** Moderate

12. Which of the following is NOT deemed a critical infrastructure by the Department of Homeland Security?

- A. Forestry services
- B. Energy systems
- C. Power companies
- D. Transportation departments

Answer: A **Reference:** Terrorism and Cyberterrorism **Difficulty:** Moderate

13. What federal program provides computer forensic expertise to law enforcement agencies?

- A. The RCFL
- B. The NBCD
- C. The ACHF
- D. The CDCF

Answer: A **Reference:** FBI's Computer Forensics Advisory Board **Difficulty:** Moderate

14. Which of the following is NOT one of the skills you need as a forensic investigator?

- A. Knowledge of legal issues
- B. Knowledge of proper investigative techniques
- C. Knowledge of computer technology
- D. Knowledge of the person's intent

Answer: D **Reference:** Computer Forensics Evidence and Investigations **Difficulty:** Moderate

15. The starting point for understanding all types of forensics investigations is

- A. Knowledge of all pertaining laws and regulations
- B. The investigative techniques
- C. The psychological profile of the defendant
- D. The evidence

Answer: D **Reference:** Evidence: The Starting Point for Understanding What Happened **Difficulty:** Moderate

16. Which of the following is NOT a primary type of evidence that can be used to persuade someone to believe an assertion?

- A. Electronic evidence
- B. Hearsay evidence
- C. Testimony of a witness
- D. Physical evidence

Answer: B **Reference:** Evidence: The Starting Point for Understanding What Happened **Difficulty:** Moderate

Fill in the Blank:

17. Proper collection of evidence and handling procedures must be followed to ensure the evidence is _____.

Answer: admissible **Reference:** Introduction **Difficulty:** Moderate

18. A(n) _____ is considered an offensive act against societal laws.

Answer: crime **Reference:** Definition of Crime **Difficulty:** Moderate

19. _____ laws protect the public, human life, or private property.

Answer: Criminal **Reference:** Definition of Crime **Difficulty:** Moderate

20. Criminal laws are defined in rules that are referred to as _____.

Answer: statutes **Reference:** Definition of Crime **Difficulty:** Easy

21. A(n) _____ is a lesser crime such as careless driving.

Answer: misdemeanor **Reference:** Crime Categories and Sentencing Guidelines **Difficulty:** Easy

22. _____ charges are those brought by a person or company.

Answer: Civil **Reference:** Civil vs. Criminal Charges **Difficulty:** Moderate

23. The two senses most often relied upon in testimony are sight and _____.

Answer: hearing **Reference:** Evidence: The Starting Point for Understanding What Happened **Difficulty:** Difficult

24. Based on preliminary evidence obtained at the start of an investigation, an investigator may form a(n) _____ about what happened.

Answer: theory **Reference:** Evidence Investigative Skills **Difficulty:** Moderate

25. _____ left by Internet and e-mail usage and digital devices may be the only way to collect enough evidence to solve a crime.

Answer: Cybertrails **Reference:** Cybertrails of Evidence **Difficulty:** Moderate

26. In the case of missing Washington, D.C., resident _____, e-mail and visited Web sites on a personal laptop were all the police had to go by.

Answer: Chandra Levy **Reference:** Cybertrails of Evidence **Difficulty:** Difficult

27. _____ evidence is that type that could incorrectly lead an investigator to believe the evidence is related to the crime.

Answer: Artifact **Reference:** Artifact, Inculpatory, and Exculpatory Evidence **Difficulty:** Easy

28. Only _____ evidence supports or helps confirm a given theory.

Answer: inculpatory **Reference:** Artifact, Inculpatory, and Exculpatory Evidence **Difficulty:** Easy

29. Another term for evidence that contradicts a given theory is _____ evidence.

Answer: exculpatory **Reference:** Artifact, Inculpatory, and Exculpatory Evidence **Difficulty:** Easy

30. For any item of evidence to be considered admissible, it must first be _____.

Answer: authenticated **Reference:** Admissible Evidence **Difficulty:** Moderate

31. The main reason evidence is ruled _____ is its lack of reliability.

Answer: inadmissible **Reference:** Admissible Evidence **Difficulty:** Moderate

32. _____ evidence is evidence obtained from an illegal search or seizure.

Answer: Tainted **Reference:** Admissible Evidence **Difficulty:** Moderate

33. The _____ rule states that to prove the content of a writing, recording, or photograph, you need the original writing, recording, or photograph.

Answer: “best evidence” **Reference:** Federal Rules of Evidence **Difficulty:** Difficult

Matching:

34. Match the following criminal law characteristics to their civil law counterparts.

- | | |
|--|--|
| I. Protects society’s interests | A. Deters injuries and compensates the injured |
| II. Violates a statute | B. Preponderance of the evidence |
| III. Criminal violations | C. Causes harm to an individual, group, or legal entity |
| IV. Beyond a reasonable doubt | D. Noncriminal injuries |
| V. Deters crime and punishes criminals | E. Provides an injured private party the opportunity to bring a lawsuit for the injury |

Answer: E C D B A **Reference:** Civil vs. Criminal Charges **Difficulty:** Moderate

35. Match the following to their definitions.

- | | |
|------------------------------------|--|
| I. Rules of Evidence | A. Can be gathered through a computer or via IT autopsy |
| II. Federal Rules of Evidence 1002 | B. Considered to be the “best evidence” rule |
| III. Evidence | C. The starting point of understanding all types of investigations |
| IV. E-evidence | D. How a court determines admissible evidence |

Answer: D B C A **Reference:** Terms throughout the chapter **Difficulty:** Moderate

36. Match the following to their definitions.

- | | |
|------------------------------|--|
| I. Documentary evidence | A. Testimony is inadmissible because the person saying it is not in the room to confirm it |
| II. Hearsay rule | B. Considered secondhand evidence |
| III. Circumstantial evidence | C. Used as documentary evidence |
| IV. Hearsay evidence | D. Used when direct evidence is not available |
| V. Expert witness | E. One who qualifies as a subject matter expert |

Answer: D A C B E

Reference: Terms throughout the chapter

Difficulty: Moderate

37. Match the following terms to their definitions.

- | | |
|---------------------------|--|
| I. Demonstrative evidence | A. Official request for material gathered prior to a trial |
| II. Material evidence | B. Physical evidence used to clarify facts |
| III. Discovery | C. Evidence relevant to the case |
| IV. Discovery request | D. The gathering of information in preparation for a trial |

Answer: B C D

Reference: Terms throughout the chapter

Difficulty: Moderate

38. Match the type of e-evidence to the organization that may use the evidence in litigation.

- | | |
|---------------------------------------|--------------------------|
| I. Financial fraud | A. Insurance companies |
| II. Harassment cases | B. Corporations |
| III. Investigations into arson | C. Individuals |
| IV. Misappropriation of trade secrets | D. Criminal prosecutions |
| V. Wrongful termination | E. Civil litigations |

Answer: D E A B C

Reference: Computer Forensics:
A Growing Field and Practice Area

Difficulty: Difficult

39. Match the discovery process to its definition.

- | | |
|------------------------------|--|
| I. Depositions | A. Involve the inspection of documents |
| II. Interrogatories | B. Out-of-court testimony made under oath |
| III. Requests for production | C. Intend to ascertain the validity of documents |
| IV. Requests for admission | D. Written answers made under oath |

Answer: B D A C

Reference: Discovery

Difficulty: Moderate

40. Match the following terms to their definitions.

- | | |
|------------------------------|---|
| I. Active, online data | A. Stored data not organized for retrieval of individual documents or files |
| II. Near-line data | B. Data is available for access as it is created and processed |
| III. Offline storage | C. Data tagged for deletion that may still exist on a system |
| IV. Backup tapes | D. Data is typically housed on removable media |
| V. Erased or fragmented data | E. Data on removable media that has been placed in storage |

Answer: B D E A C

Reference: Landmark Case Involving E-Discovery

Difficulty: Moderate