Question 1

Which of the following is a primary concern in computer forensics?

1. Detection of malware
2. Collection and preservation of digital evidence
3. Development of new software tools
4. Encryption of sensitive data

Answer 1

Which of the following is a primary concern in computer forensics?

1. Detection of malware
2. **Collection and preservation of digital evidence**
3. Development of new software tools
4. Encryption of sensitive data

Question 2

What is the key role of digital forensics in cybercrime investigations?

1. Prevention of cyberattacks
2. Identifying the attacker
3. Recovery and analysis of digital evidence
4. Development of new encryption algorithms

Answer 2

What is the key role of digital forensics in cybercrime investigations?

1. Prevention of cyberattacks
2. Identifying the attacker
3. **Recovery and analysis of digital evidence**
4. Development of new encryption algorithms

Question 3

Which phase of the digital forensics life cycle involves identifying relevant evidence?

1. Preservation
2. Identification
3. Collection
4. Reporting

Answer 3

Which phase of the digital forensics life cycle involves identifying relevant evidence?

1. Preservation
2. **Identification**
3. Collection
4. Reporting

Question 4

What is the concept of "chain of custody" in computer forensics?

1. The process of documenting the handling of evidence
2. The encryption of digital evidence to prevent tampering
3. The process of analyzing digital signatures
4. The management of secure passwords

Answer 4

What is the concept of "chain of custody" in computer forensics?

1. **The process of documenting the handling of evidence**
2. The encryption of digital evidence to prevent tampering
3. The process of analyzing digital signatures
4. The management of secure passwords

Question 5

Which one of the following is a type of file are often targeted in forensic investigations?

1. .EXE files
2. .BIN files
3. Deleted files
4. .MSI files

Answer 5

Which of the following types of files are often targeted in forensic investigations?

1. .EXE files
2. .BIN files
3. **Deleted files**
4. .MSI files

Question 6

What is the purpose of a write-blocking tool in computer forensics?

1. To block unauthorized access to the evidence
2. To prevent changes to the evidence during acquisition
3. To encrypt evidence during transportation
4. To analyze the content of evidence

Answer 6

What is the purpose of a write-blocking tool in computer forensics?

1. To block unauthorized access to the evidence
2. **To prevent changes to the evidence during acquisition**
3. To encrypt evidence during transportation
4. To analyze the content of evidence

Question 7

Dealing with Encrypted and Hidden files is a challenge in handling digital evidence!

1. True
2. False

Answer 7

Dealing with Encrypted and Hidden files is a challenge in handling digital evidence!

1. **True**
2. False

Question 8

What does "media analysis" refer to in computer forensics?

1. The analysis of file systems on a device
2. The analysis of a storage device's raw data
3. The examination of network traffic
4. The analysis of digital signatures

Answer 8

What does "media analysis" refer to in computer forensics?

1. The analysis of file systems on a device
2. **The analysis of a storage device's raw data**
3. The examination of network traffic
4. The analysis of digital signatures

Question 9

Which type of analysis involves the interpretation of data from a communication network?

1. File system analysis
2. Media analysis
3. Application analysis
4. Network analysis

Answer 9

Which type of analysis involves the interpretation of data from a communication network?

1. File system analysis
2. Media analysis
3. Application analysis
4. **Network analysis**

Question 10

Which of the following is an important guideline in evidence collection?

1. Minimize changes to the data
2. Avoid collecting volatile data first
3. Use unverified tools to speed up the process
4. Disable logging on the system

Answer 10

Which of the following is an important guideline in evidence collection?

1. **Minimize changes to the data**
2. Avoid collecting volatile data first
3. Use unverified tools to speed up the process
4. Disable logging on the system

Question 11

What is the first step in the digital forensics life cycle?

1. Analysis
2. Collection and Recording
3. Preparation and Identification
4. Testifying

Answer 11

What is the first step in the digital forensics life cycle?

1. Analysis
2. Collection and Recording
3. **Preparation and Identification**
4. Testifying

Question 12

Which of the following is not a key phase in the digital forensics life cycle?

1. Preservation
2. Reporting
3. Encryption
4. Testifying

Answer 12

Which of the following is not a key phase in the digital forensics life cycle?

1. Preservation
2. Reporting
3. **Encryption**
4. Testifying

Question 13

What is "Chain of Custody" in the context of digital forensics?

1. The process of encrypting evidence
2. The process of tracking and documenting evidence handling
3. The encryption method used in data storage
4. A forensic tool used for data preservation

Answer 13

What is "Chain of Custody" in the context of digital forensics?

1. The process of encrypting evidence
2. **The process of tracking and documenting evidence handling**
3. The encryption method used in data storage
4. A forensic tool used for data preservation

Question 14

Which digital forensic tool is used to create an image of the evidentiary media?

1. EnCase
2. BlueSniff
3. Phishing
4. MediaBlock

Answer 14

Which digital forensic tool is used to create an image of the evidentiary media?

1. **EnCase**
2. BlueSniff
3. Phishing
4. MediaBlock

Question 15

Which type of analysis involves the storage media's data without considering any file system structures?

1. Media management analysis
2. Application analysis
3. File system analysis
4. Media analysis

Answer 15

Which type of analysis involves the storage media's data without considering any file system structures?

1. Media management analysis
2. Application analysis
3. File system analysis
4. **Media analysis**

Question 16

What is the purpose of "media analysis" in digital forensics?

1. To analyze the content of files
2. To analyze storage devices without partitions or OS-specific structures
3. To analyze network traffic
4. To create backups of digital evidence

Answer 16

What is the purpose of "media analysis" in digital forensics?

1. To analyze the content of files
2. **To analyze storage devices without partitions or OS-specific structures**
3. To analyze network traffic
4. To create backups of digital evidence

Question 17

In digital forensics, which type of analysis involves understanding the content of application-specific files?

1. File system analysis
2. Media management analysis
3. Application analysis
4. Network analysis

Answer 17

In digital forensics, which type of analysis involves understanding the content of application-specific files?

1. File system analysis
2. Media management analysis
3. **Application analysis**
4. Network analysis

Question 18

Which of the following is a challenge often faced in digital forensics investigations?

1. Encryption
2. Chain of Custody
3. Reduced Data Volume
4. Lack of legal framework

Answer 18

Which of the following is a challenge often faced in digital forensics investigations?

1. **Encryption**
2. Chain of Custody
3. Reduced Data Volume
4. Lack of legal framework

Question 19

What is one of the primary challenges in digital forensics?

1. Lack of storage space
2. Encryption
3. Incomplete evidence
4. Legal hurdles

Answer 19

What is one of the primary challenges in digital forensics?

1. Lack of storage space
2. **Encryption**
3. Incomplete evidence
4. Legal hurdles

Question 20

What is a bit-stream image in the context of digital forensics?

1. A compressed version of digital evidence
2. An exact replica of the original media
3. A partial snapshot of a hard drive
4. A collection of volatile memory only

Answer 20

What is a bit-stream image in the context of digital forensics?

1. A compressed version of digital evidence
2. **An exact replica of the original media**
3. A partial snapshot of a hard drive
4. A collection of volatile memory only

Question 21

Which analysis method is used when examining data on a communications network?

1. Media analysis
2. File system analysis
3. Network analysis
4. Application analysis

Answer 21

Which analysis method is used when examining data on a communications network?

1. Media analysis
2. File system analysis
3. **Network analysis**
4. Application analysis

Question 22

What is the focus of forensic analysis of e-mail in digital forensics?

1. Investigating attachments
2. Analyzing the message body
3. Investigating the header for routing details
4. Investigating the size of the email

Answer 22

What is the focus of forensic analysis of e-mail in digital forensics?

1. Investigating attachments
2. Analyzing the message body
3. **Investigating the header for routing details**
4. Investigating the size of the email

Question 23

What does "dead analysis" refer to in digital forensics?

1. Analysis of powered-off systems
2. Analysis of encrypted data
3. Analysis of volatile memory
4. Analysis of malware

Answer 23

What does "dead analysis" refer to in digital forensics?

1. **Analysis of powered-off systems**
2. Analysis of encrypted data
3. Analysis of volatile memory
4. Analysis of malware

Question 24

Which of the following is an example of an antiforensics technique?

1. Data reduction
2. Chain of custody
3. Encryption
4. Media imaging

Answer 24

Which of the following is an example of an antiforensics technique?

1. Data reduction
2. Chain of custody
3. **Encryption**
4. Media imaging

Question 25

Which tool is commonly used to create a forensically sound duplicate of a drive?

1. BlueSniff
2. EnCase
3. Phishing
4. File scanner

Answer 25

Which tool is commonly used to create a forensically sound duplicate of a drive?

1. BlueSniff
2. **EnCase**
3. Phishing
4. File scanner