Investigations and Evidence Recovery Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. **What characteristic qualifies as a class characteristic of a black 4th Generation iPod Classic?**

   A. It is black

   B. It has 6,240 songs

   C. It has 120GB capacity

   D. It has a cracked screen cover

2. **When a file occupying seven clusters is erased and another file of 610 bytes is saved in one cluster, how is that cluster described?**

   A. 610 bytes of data and 31,390 bytes of unallocated space.

   B. 610 bytes of data and 31,390 bytes of random zeroes and ones following the EOF marker.

   C. 610 bytes of data followed by 31,390 bytes of null space.

   D. 610 bytes of data followed by 31,390 bytes of the previous file in the slack space.

3. **Which of the following acts was passed first?**

   A. Fair Credit Reporting Act

   B. Debt Collection Practices Act

   C. The Right to Financial Privacy Act

   D. Graham Leach Billey

4. **What does the concept of present possession suggest regarding files on a subject's computer?**

   A. Files must not indicate user knowledge

   B. The subject knew the files were present

   C. Files can be moved without user awareness

   D. User has no direct access to the files

5. **What type of device is used to secure data on electronic devices to prevent unauthorized access?**

   A. Firewall

   B. Encryption software

   C. Security token

   D. Faraday bag

6. What does the term 'stateless' refer to in the context of web services?

A. A service that maintains state between requests

B. A service that does not maintain any state

C. A service requiring constant user input

D. A temporary service

7. Who originally developed the Expert Witness Format (EWF)?

A. Microsoft

B. Access Data Corporation

C. Guidance Software

D. Apple Computer

8. What is a true statement regarding a Forensic Laboratory?

A. Computer Forensic Laboratories are not subject to Accreditation.

B. All sections are subject to the same accreditation and certifications.

C. Each section of the Laboratory undergoes separate accreditations.

D. Forensic Laboratories are not accredited.

9. What are the two conditions that must be met for evidence to be considered relevant in a court of law?

A. It must be material and thought-provoking

B. It must be material and probative

C. It must be truthful and collected by an authorized official

D. It must be probative and collected legally

10. After seizing a telephone, what precaution should you take to prevent cohorts from accessing the phone remotely?

A. Put the phone in Airline Mode

B. Pull the SIM card

C. Enable call-waiting

D. Pray

Answers

1. A
2. D
3. A
4. B
5. D
6. B
7. C
8. B
9. B
10. A

Explanations

1. What characteristic qualifies as a class characteristic of a black 4th Generation iPod Classic?

A. It is black

B. It has 6,240 songs

C. It has 120GB capacity

D. It has a cracked screen cover

A class characteristic refers to a feature that is shared by a group of items rather than unique to a particular item. In this case, the fact that the iPod is black qualifies as a class characteristic because it denotes a color shared by many 4th Generation iPod Classics, not a specific feature that identifies an individual device. This characteristic helps group items into categories based on common features, which can be important in investigations where commonality among multiple objects can be analyzed. In contrast, having a specific number of songs, a unique storage capacity, or a specific physical condition like a cracked screen cover describes features that may be unique to a particular device versus shared across multiple devices of the same model. These details might be considered individual characteristics rather than class characteristics, making the color the only valid choice for class characteristics in this context.

2. When a file occupying seven clusters is erased and another file of 610 bytes is saved in one cluster, how is that cluster described?

A. 610 bytes of data and 31,390 bytes of unallocated space.

B. 610 bytes of data and 31,390 bytes of random zeroes and ones following the EOF marker.

C. 610 bytes of data followed by 31,390 bytes of null space.

D. 610 bytes of data followed by 31,390 bytes of the previous file in the slack space.

The correct answer points to the concept of slack space, which refers to the unused space in a cluster after a file is saved. When a file that occupies seven clusters is erased, its data is no longer actively referenced by the file system, yet it may still physically exist on the disk until overwritten. In this case, when a new file of 610 bytes is saved in one cluster, it does not fully utilize the entire cluster capacity. Consequently, the remaining space in that cluster (after accounting for the 610 bytes) constitutes slack space. The total size of a cluster is typically larger than the file size, and any leftover space is still a part of that cluster. Because the prior file occupied seven clusters, the cluster now holding the 610-byte file could still contain remnants of the deleted file in the slack space, which is essentially leftover data not cleared when the prior file was erased. Therefore, the correct description includes not only the current data of 610 bytes but also the residual data from the previous file that remains in the slack space, thus constituting 31,390 bytes that reflect that leftover information.

3. Which of the following acts was passed first?

A. Fair Credit Reporting Act

B. Debt Collection Practices Act

C. The Right to Financial Privacy Act

D. Graham Leach Billey

The Fair Credit Reporting Act (FCRA) was the first among the listed acts, enacted in 1970. This legislation was designed to promote the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. It established the groundwork for how consumer information can be collected, used, and shared, setting standards that protect consumers' interests regarding credit reporting. The other acts listed were passed later. The Debt Collection Practices Act came into existence in 1977, aiming to eliminate abusive practices in the debt collection industry. The Right to Financial Privacy Act was enacted in 1978, which protects the privacy of personal financial records from government authorities. Finally, the Graham-Leach-Bliley Act, which was passed in 1999, aimed to enhance consumer protections and privacy for financial information. Understanding the timeline of these acts helps clarify their significance and purpose in relation to consumer rights and protections in financial contexts.

4. What does the concept of present possession suggest regarding files on a subject's computer?

A. Files must not indicate user knowledge

B. The subject knew the files were present

C. Files can be moved without user awareness

D. User has no direct access to the files

The concept of present possession implies that the subject has actual awareness and knowledge of the files located on their computer. When it is said that the subject "knew the files were present," it suggests a level of control and acknowledgment over the files, which is significant in forensic investigations and legal matters. If a subject is in present possession of files, it often means that they can be legally accountable for the content stored on their device. This awareness is crucial during investigations, as it affects how evidence is interpreted and what implications arise regarding the subject's behavior and intentions. The other options discuss concepts that encompass lack of knowledge or non-accessibility, which do not align with the understanding that presence implies a degree of awareness and control over the files in question.

5. What type of device is used to secure data on electronic devices to prevent unauthorized access?

A. Firewall

B. Encryption software

C. Security token

D. Faraday bag

The correct choice is encryption software. This type of device or software is specifically designed to transform data into a coded format that can only be accessed or decrypted by individuals who possess the correct decryption key or password. It ensures that even if unauthorized users access the data, they cannot understand or utilize it without the proper credentials. Firewalls are primarily used to monitor and control incoming and outgoing network traffic based on predetermined security rules, but they do not inherently secure data by encoding it. Security tokens are used for authentication purposes, providing a means to verify user identities but do not protect the data itself. A Faraday bag is used to block electromagnetic fields and prevent radio frequencies from reaching electronic devices, which is useful for protecting devices from remote access or tracking but doesn't secure the data that resides on those devices. Thus, encryption software is the most effective tool for securing data against unauthorized access.

6. What does the term 'stateless' refer to in the context of web services?

A. A service that maintains state between requests

B. A service that does not maintain any state

C. A service requiring constant user input

D. A temporary service

In the context of web services, the term 'stateless' refers to a service that does not maintain any state between requests. This means that each request from a client to the server is treated as a new and independent transaction, without any knowledge or dependence on previous interactions. Stateless services do not store data about prior requests, which allows them to be more scalable and flexible, as they can handle a greater number of requests without the overhead of managing session information. This design simplifies the service architecture, as the server does not need to keep track of the individual state for each client. Clients are responsible for sending all necessary information with each request. This feature is key in many web services, such as RESTful services, where scalability and performance are often prioritized. In contrast, services that maintain state between requests create a persistence layer that can complicate the service architecture, as they need to manage client sessions and the data associated with them, which is not the case for stateless services.

7. Who originally developed the Expert Witness Format (EWF)?

A. Microsoft

B. Access Data Corporation

C. Guidance Software

D. Apple Computer

The Expert Witness Format (EWF) was originally developed by Guidance Software. This format was specifically designed to facilitate the exchange and presentation of digital evidence in a standardized manner, which is crucial in legal proceedings where clarity, integrity, and reliability of the data are paramount. Guidance Software has a long-standing reputation in the field of digital forensics, and their development of EWF reflects their commitment to providing forensic tools that help professionals manage evidence effectively. The other options, while well-known companies within the technology and software development landscape, do not have a direct connection to the creation of the Expert Witness Format. Microsoft, Access Data Corporation, and Apple Computer may produce tools or software that are utilized in digital forensics or investigative processes, but they were not involved in the development of EWF. Understanding the origin of this format is key for anyone working in investigations, as it underpins the practices used for collecting and presenting digital evidence in courtroom settings.

8. What is a true statement regarding a Forensic Laboratory?

A. Computer Forensic Laboratories are not subject to Accreditation.

B. All sections are subject to the same accreditation and certifications.

C. Each section of the Laboratory undergoes separate accreditations.

D. Forensic Laboratories are not accredited.

A true statement regarding a forensic laboratory is that all sections are subject to the same accreditation and certifications. This means that regardless of the specific area of forensic analysis being conducted—whether it be DNA analysis, toxicology, ballistics, or digital forensics—laboratories must adhere to standardized processes and be accredited to ensure reliability and accuracy in their work. Accreditation serves to validate that each section operates within established guidelines, maintains proper quality control, and employs personnel who are qualified and competent. While different sections may have distinct protocols, the overarching requirement for accreditation emphasizes consistency and quality across the board. This ensures that all forensic evidence produced is credible and can be relied upon in a legal context. In contrast, other options include assertions that either dismiss accreditation for certain types of laboratories or assert that each section is not bound by the same rigorous standards, which is not aligned with the established practice of maintaining high levels of accountability in forensic science.

9. What are the two conditions that must be met for evidence to be considered relevant in a court of law?

A. It must be material and thought-provoking

B. It must be material and probative

C. It must be truthful and collected by an authorized official

D. It must be probative and collected legally

For evidence to be considered relevant in a court of law, it must meet two essential conditions: it must be material and probative. Materiality refers to the importance of the evidence in relation to the case at hand. This means that the evidence must have a legitimate connection to the facts of the case, aiding in the determination of a fact that is at issue in the trial. Without material evidence, the evidence does not contribute to supporting or undermining a claim. Probative value, on the other hand, indicates that the evidence has the capability to prove something relevant to the case. This implies that the evidence must make a fact more or less probable than it would be without that evidence. When evidence is both material and probative, it contributes meaningfully to the judicial process by helping to establish facts, clarify issues, or support arguments made by either party. Recognizing this standard is crucial for ensuring a fair trial, as only evidence that meets these requirements should be presented to a jury or judge. The other options do not accurately represent the legal definitions and requirements for relevance in court. For instance, while truthfulness and legality are important aspects of evidence collection and admissibility, they do not define the relevance of evidence as clearly as the

10. After seizing a telephone, what precaution should you take to prevent cohorts from accessing the phone remotely?

A. Put the phone in Airline Mode

B. Pull the SIM card

C. Enable call-waiting

D. Pray

Placing the phone in Airline Mode is a crucial step in preventing remote access by others after seizing it. Airline Mode disables all wireless communication functions of the device, including cellular, Wi-Fi, and Bluetooth connections. This action ensures that the device cannot send or receive any data, calls, or messages, effectively safeguarding any potential evidence against unauthorized access or remote wiping. While removing the SIM card could help in some scenarios by disconnecting cellular service, it does not prevent access via Wi-Fi or Bluetooth if the phone is still powered on and connected. Enabling call-waiting is unrelated to securing the phone against remote access and does not affect the security of the device in this context. Lastly, praying would not provide any tangible security measures or prevent unauthorized access, making it an ineffective strategy. Taking the precaution to enable Airline Mode is a best practice in digital evidence handling, as it protects the integrity of the evidence being gathered.