WGU Digital-Forensics-in-Cybersecurity D829 Practice Questions

Shared by Reed on 30-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A cybercriminal hacked into an Apple iPad that belongs to a company's chief executive officer (CEO). The cybercriminal deleted some important files on the data volume that must be retrieved.

Which hidden folder will contain the digital evidence?

Options:

A- /Private/etc
B- /lost+found
C- /.Trashes/501
D- /etc

Answer:

C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

On Apple iOS devices, deleted files are often moved to a hidden Trash folder before permanent deletion. The directory /.Trashes/501 is a hidden folder where deleted files for user ID 501 (the first user created on macOS/iOS devices) are temporarily stored.

This folder can contain files marked for deletion and thus is a prime location for recovery attempts.

/lost+found is a directory commonly used on Unix/Linux file systems for recovered file fragments after file system corruption but is not the default trash location on iOS.

/Private/etc and /etc contain system configuration files, not deleted user files.

Apple forensic investigations per NIST and training manuals such as those from Cellebrite and BlackBag Technologies indicate that user-deleted files on iOS devices reside in .Trashes or similar hidden directories until permanently removed.

Question 2

Question Type: MultipleChoice

Which information is included in an email header?

Options:

A- Sender's MAC address
B- Number of pages
C- Content-Type
D- Message-Digest

P2P exams

Answer:

C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

An email header contains metadata about the email including sender, receiver, routing information, and content details. The Content-Type header specifies the media type of the email body (e.g., text/plain, text/html, multipart/mixed), indicating how the email content should be interpreted.

Sender's MAC address is not typically included in email headers.

Number of pages is not relevant to email metadata.

Message-Digest is a term related to cryptographic hashes but is not a standard email header field.

P2P exams

RFC 5322 and forensic email analysis references outline that email headers contain fields like Content-Type describing the format of the message content, essential for proper parsing and forensic examination.

Question 3

Question Type: MultipleChoice

Which law or guideline lists the four states a mobile device can be in when data is extracted from it?

Options:

A- Health Insurance Portability and Accountability Act (HIPAA)
B- NIST SP 800-72 Guidelines
C- Electronic Communications Privacy Act (ECPA)
D- Communications Assistance to Law Enforcement Act (CALEA)

Answer:

B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

NIST Special Publication 800-72 provides guidelines for mobile device forensics and identifies four device states during data extraction: active, idle, powered off, and locked. These states influence how data can be accessed and preserved.

Understanding these states helps forensic investigators select appropriate acquisition techniques.

NIST SP 800-72 is a key reference for mobile device forensic methodologies.

NIST SP 800-72 offers authoritative guidelines on handling mobile device data in forensic investigations.

Question 4

Question Type: MultipleChoice

An organization has identified a system breach and has collected volatile data from the system.

Which evidence type should be collected next?

Options:

A- Running processes

B- Network connections
C- Temporary data
D- File timestamps

Answer:

B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

In incident response, after collecting volatile data (such as contents of RAM), the next priority is often to collect network-related evidence such as active network connections. Network connections can reveal ongoing communications, attacker activity, command and control channels, or data exfiltration paths.

Running processes and temporary data are also volatile but typically collected simultaneously or immediately after volatile memory.

File timestamps relate to non-volatile data and are collected later after volatile data acquisition to preserve evidence integrity.

This sequence is supported by NIST SP 800-86 and SANS Incident Handler's Handbook which emphasize the volatility of evidence and recommend capturing network state immediately after memory.

Question 5

Question Type: MultipleChoice

A forensic investigator is acquiring evidence from an iPhone.

What should the investigator ensure before the iPhone is connected to the computer?

Options:

A- That the phone is in jailbreak mode
B- That the phone avoids syncing with the computer
C- That the phone is powered off
D- That the phone has root privilege

Answer:

B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Before connecting an iPhone to a forensic workstation, the investigator must ensure that the phone does not sync with the computer automatically. Automatic syncing may alter, delete, or overwrite evidence stored on the device or the computer, compromising forensic integrity.

Jailbreak mode is not necessary and can complicate forensic analysis.

Powering off the device prevents acquisition of volatile data.

Root privileges (jailbreak) may aid access but are not mandatory before connection.

NIST mobile device forensic guidelines emphasize disabling automatic sync to preserve data integrity during acquisition.

Question 6

Question Type: MultipleChoice

The chief executive officer (CEO) of a small computer company has identified a potential hacking attack from an outside competitor.

Which type of evidence should a forensics investigator use to identify the source of the hack?

Options:

A- Network transaction logs
B- Email archives
C- File system metadata
D- Browser history

Answer:

A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Network transaction logs capture records of network connections, including source and destination IP addresses, ports, and timestamps. These logs are essential in identifying the attacker's origin and understanding the nature of the intrusion.

Network logs provide traceability back to the attacker.

Forensic procedures prioritize collecting network logs to identify unauthorized access.

NIST SP 800-86 discusses the importance of network logs in digital investigations to attribute cyberattacks.

P2P exams

Question 7

Question Type: MultipleChoice

Which file system is supported by Mac?

Options:

A- NTFS
B- EXT4
C- Hierarchical File System Plus (HFS+)
D- FAT32

Answer:

C

P2P exams

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Mac systems traditionally use the Hierarchical File System Plus (HFS+), which supports features such as journaling and metadata handling suited for Mac OS environments. Newer versions use APFS but HFS+ remains relevant.

NTFS is primarily a Windows file system.

EXT4 is a Linux file system.

FAT32 is a generic cross-platform file system but lacks advanced features.

Apple and NIST documentation confirm HFS+ as a Mac-supported file system for forensic analysis.

Question 8

Question Type: MultipleChoice

Which storage format is a magnetic drive?

Options:

A- CD-ROM
B- SATA
C- Blu-ray
D- SSD

Answer:

B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

SATA (Serial ATA) refers to an interface standard commonly used for connecting magnetic hard disk drives (HDDs) and solid-state drives (SSDs) to a computer. The term SATA itself describes the connection, but most HDDs that use SATA as an interface are magnetic drives.

CD-ROM and Blu-ray are optical storage media, not magnetic.

SSD (Solid State Drive) uses flash memory, not magnetic storage.

Magnetic drives rely on spinning magnetic platters, which are typically connected via SATA or other interfaces.

This differentiation is emphasized in digital forensic training and hardware documentation, including those from NIST and forensic hardware textbooks.

Question 9

Question Type: MultipleChoice

Which Windows 7 operating system log stores events collected from remote computers?

Options:

A- System
B- Application
C- ForwardedEvents
D- Security

Answer:

C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

The ForwardedEvents log in Windows 7 is specifically designed to store events collected from remote computers via event forwarding. This log is part of the Windows Event Forwarding feature used in enterprise environments to centralize event monitoring.

The System and Application logs store local system and application events.

The Security log stores local security-related events.

ForwardedEvents collects and stores events forwarded from other machines.

Microsoft documentation and NIST SP 800-86 mention the use of ForwardedEvents for centralized event log collection in investigations.

Question 10

Question Type: MultipleChoice

Which tool can be used to make a bit-by-bit copy of a Windows Phone 8?

Options:

A- Forensic Toolkit (FTK)
B- Data Doctor

C- Pwnage
D- Wolf

Answer:

A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Forensic Toolkit (FTK) is a comprehensive forensic suite capable of acquiring bit-by-bit images from various devices, including Windows Phone 8, by supporting physical and logical extractions. FTK is widely accepted and used for mobile device forensic imaging.

Data Doctor is primarily a data recovery tool, not specialized for mobile forensic imaging.

Pwnage is related to jailbreaking iOS devices.

Wolf is not a recognized forensic imaging tool for Windows Phone 8.

NIST mobile device forensic standards cite FTK as a preferred tool for mobile device imaging.

To Get Premium Files for Digital-Forensics-in-Cybersecurity Visit

https://www.p2pexams.com/products/digital-forensics-in-cybersecurity

For More Free Questions Visit

https://www.p2pexams.com/wgu/pdf/digital-forensics-in-cybersecurity

