Eccouncil 112-57 DFE Practice Questions

Shared by Armstrong on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following steps in forensic readiness planning provides a backup for future reference and assists in presenting evidence in a court of law?

Options:

A- Creating a process for documenting the procedure
B- Identifying the potential evidence required for an incident
C- Determining the sources of evidence
D- Keeping an incident response team ready to review the incident

Answer:

A

Explanation:

In forensic readiness planning, the goal is to ensure that when an incident occurs, the organization can collect, preserve, and present digital evidence in a manner that remains reliable, repeatable, and legally defensible. A key requirement for courtroom acceptance is clear documentation---often referred to as proper documentation and chain-of-custody support---showing what actions were taken, by whom, when, using which tools, and under what conditions. Creating a defined process for documenting procedures ensures investigators consistently record acquisition steps, handling methods, hashing/verification results, storage locations, access history, and any changes in evidence possession. This documentation becomes a ''backup'' in the sense that it preserves institutional memory of the investigation steps, allowing future reviewers (auditors, opposing experts, courts) to reconstruct and validate what occurred even long after the incident.

While identifying potential evidence (B) and determining evidence sources (C) are important readiness tasks, they do not themselves create the structured record needed to defend evidence integrity. Keeping an incident response team ready (D) supports operational response, but does not directly ensure admissibility. Therefore, the step that provides future reference and supports court presentation is Creating a process for documenting the procedure (A).

Question 2

Question Type: MultipleChoice

John, a forensic officer, was working on a criminal case. He employed imaging software to create a copy of data from the suspect device on a storage medium for further investigation. For developing an image of the original data, John used a software application that does not allow an unauthorized user to alter the image content on storage media, thereby retaining an unaltered image copy.

Identify the data acquisition step performed by John in the above scenario.

Options:

A- Enabled write protection on the evidence media
B- Validated data acquisition
C- Sanitized the target media
D- Planned for contingency

Answer:

A

Explanation:

The scenario emphasizes that John used an application (or mechanism) that prevents alteration of the acquired image content, ensuring the image remains unaltered and protected from unauthorized modification. In forensic acquisition standards, this corresponds to enabling write protection during imaging---commonly implemented using a write blocker (hardware or controlled software write-protection) to prevent any writes to the source evidence and, where applicable, to protect the integrity of the evidence copy from accidental or unauthorized changes. The purpose is to preserve evidential integrity by ensuring that neither the original media nor the forensic image is modified during handling, analysis preparation, or transfer.

''Validated data acquisition'' refers to confirming the image is an exact duplicate, typically by computing and comparing cryptographic hashes (e.g., MD5/SHA) of the source and the acquired image. While validation is essential, the question specifically highlights preventing alteration, not verifying equality. ''Sanitized the target media'' is the step of wiping/clearing the destination drive before acquisition to avoid contamination, which is not what is described. ''Planned for contingency'' relates to operational planning for unexpected issues (equipment failure, encryption, power loss), not integrity protection. Therefore, the best match is Enabled write protection on the evidence media (A).

Question 3

Question Type: MultipleChoice

Alice and John are close college friends. Alice frequently sends emails to John attaching her pics with friends. One day, Alice sent an email to John describing all the details related to the final year project without specifying the actual purpose. John missed the message as he frequently receives emails from her and did not arrive for a project seminar.

Which option best email fields could Alice have used in the above scenario to highlight the importance of the email?

Options:

A- Subject
B- Date
C- Cc
D- Bcc

Answer:

A

Explanation:

The Subject field is the primary email header element used to communicate the purpose and urgency of a message at a glance. Digital forensics training emphasizes that email messages consist of headers (routing and descriptive metadata) and a body (content). Among user-visible header fields, the Subject line is specifically intended to summarize what the email is about, helping recipients prioritize and correctly interpret the message without opening it. In the scenario, John routinely receives casual emails from Alice (often with pictures). When Alice sent a project-related email ''without specifying the actual purpose,'' John treated it like routine mail and overlooked its significance. A clear, descriptive subject such as ''Final Year Project Seminar -- Attendance Required'' would have flagged the message as time-sensitive and different from her usual emails, reducing the chance it would be missed.

The other options do not serve this purpose. Date is automatically assigned and mainly supports ordering and timeline reconstruction rather than highlighting importance. Cc and Bcc control who receives copies and can affect visibility or secrecy, but they do not summarize intent for the recipient. Therefore, the field best suited to highlight importance is Subject (A).

Question 4

Question Type: MultipleChoice

Wesley, a professional hacker, deleted a confidential file in a compromised system using the ''/bin/rm/'' command to deny access to forensic specialists.

Identify the operating system on which Don has performed the file carving act.

Options:

A- Windows
B- Android
C- Mac OS
D- Linux

Answer:

D

Explanation:

The command path /bin/rm is a hallmark of UNIX/POSIX-style operating systems, where core userland utilities are commonly stored under directories such as /bin, /sbin, and /usr/bin. The utility rm (remove) is the standard UNIX command used to delete directory entries that reference a file's data blocks on disk. This layout and command structure do not match Windows, which uses different filesystem conventions (drive letters, backslashes, and Windows-native executables) and does not provide /bin/rm as a native path. Android, while Linux-kernel-based, typically exposes shell utilities through environments like /system/bin (and newer systems may use toybox/busybox variants), not the classic /bin hierarchy expected on general-purpose UNIX systems. Between the remaining options, both Linux and macOS are UNIX-like and can include an rm command; however, in digital forensics training and examination contexts, the explicit reference to /bin/rm is most commonly used to indicate a Linux/UNIX command-line environment on a compromised host. Therefore, the best single-choice answer from the provided options is Linux (D).

Question 5

Question Type: MultipleChoice

Which of the following Windows system files is created in the system drive after OS installation to support the internal functions and system service dispatch stubs to executive functions?

Options:

A- Ntoskrnl.exe
B- Win32k.sys
C- Ntdll.dll
D- Kernel32.dll

Answer:

C

Explanation:

Ntdll.dll is the Windows user-mode system library that provides many internal NT functions (commonly exposed as ''NT Native API'' routines such as Nt*/Zw*) and, critically, contains the system service dispatch stubs used by user-mode code to transition into kernel mode for operating system services. In standard Windows architecture, most user-mode applications call higher-level APIs (for example, Win32 APIs in Kernel32.dll), which then ultimately rely on Ntdll.dll to perform the final step of invoking the kernel through these system call stubs. This is why Ntdll.dll is a core component loaded into nearly every process and is tightly associated with the boundary between user mode and the executive components of the OS.

From a forensics viewpoint, understanding Ntdll.dll matters because it is central to how processes request privileged services, and it is frequently referenced in analyses of process execution, API call chains, and certain user-mode hooking techniques used by malware or anti-forensics tools.

By contrast, Ntoskrnl.exe is the kernel image itself (core kernel/executive), Win32k.sys is a kernel-mode graphics/windowing subsystem component, and Kernel32.dll provides higher-level Win32 APIs rather than the primary system-call stub layer. Hence, Ntdll.dll (C) is the correct answer.

Question 6

Question Type: MultipleChoice

David, a cybercriminal, targeted a community and initiated anti-social campaigns online. In this process, he used a layer of the web that allowed him to maintain anonymity during the campaign.

Which option best layers of the web allowed David to hide his presence during the anti-social campaign?

Options:

A- Surface Web
B- World Wide Web
C- Dark Web
D- Deep Web

Answer:

C

Explanation:

The layer of the web most associated with maintaining anonymity for users and services is the Dark Web. In digital forensics terminology, the Dark Web refers to services hosted on overlay networks (such as Tor hidden services) that are not indexed by standard search engines and are typically accessible only through specialized software and configurations. Its core characteristic is that it is deliberately designed to reduce traceability by routing traffic through multiple relays and separating identifying information (like the user's real IP address) from the destination. This makes attribution and geolocation significantly harder using traditional network logs alone, which is why adversaries often choose it to conduct covert communications, host content, or coordinate campaigns.

By contrast, the Surface Web (the regular, indexed portion of the web) is generally reachable through normal browsers and is easier to monitor and attribute using conventional ISP, server, and platform logs. ''World Wide Web'' is a general term for web content accessed via HTTP/HTTPS and does not specifically imply anonymity. The Deep Web refers to content not indexed by search engines (e.g., webmail, databases, authenticated portals), but it is not inherently anonymizing---many deep web resources are simply private or access-controlled. Therefore, the layer enabling David to hide his presence is the Dark Web (C).

Question 7

Question Type: MultipleChoice

Sarah, a forensic investigator, is working on a criminal case. She was provided with all the suspect devices. Sarah employs an imaging software tool for duplicating the original data from the suspect devices. However, the tool she employed failed to image the data as the suspect version of the drive was very old and incompatible with imaging software. Hence, Sarah used an alternative data acquisition technique and succeeded in imaging the data.

Which option best types of data acquisition techniques did Sarah employ in the above scenario?

Options:

A- Sparse acquisition
B- Bit-stream disk-to-image-file
C- Logical acquisition
D- Bit-stream disk-to-disk

Answer:

D

Explanation:

The key detail is that Sarah's imaging software could not acquire the device because the drive was very old and incompatible with the software-based approach. In such situations, forensic practice recommends switching to an acquisition method that is less dependent on the operating system or specific imaging application compatibility, while still producing a forensic-accurate duplicate. Bit-stream disk-to-disk acquisition (also called forensic cloning) creates a sector-by-sector copy of the entire source drive directly onto another physical drive. This method is commonly performed using dedicated duplicators or hardware-assisted workflows that can interface with legacy media more reliably than certain disk-to-image software utilities.

Sparse acquisition would intentionally capture only selected portions of a disk (used to reduce time/storage), which does not fit the goal of ''succeeded in imaging the data'' after a failure due to incompatibility. Logical acquisition captures only active files/folders through the file system and is not the preferred alternative when full forensic imaging is required, especially in criminal cases. Bit-stream disk-to-image-file is still software/container dependent and is essentially what failed initially. Therefore, the most appropriate alternative that explains success with an older incompatible drive is Bit-stream disk-to-disk (D).

Question 8

Question Type: MultipleChoice

An organization decided to strengthen the security of its network by studying and analyzing the behavior of attackers. For this purpose, Steven, a security analyst, was instructed to deploy a device to bait attackers. Steven selected a solution that appears to contain very useful information to lure attackers and find their locations and techniques.

Identify the type of device deployed by Steven in the above scenario.

Options:

A- Intrusion detection system
B- Firewall

C- Honeypot
D- Router

Answer:

C

Explanation:

A honeypot is a deliberately deployed decoy system or service designed to attract attackers by appearing valuable or vulnerable, thereby enabling defenders to observe malicious behavior in a controlled manner. Digital forensics and incident response references describe honeypots as tools for threat intelligence and evidence collection, because they can record interaction details such as connection sources, exploited services, commands executed, malware dropped, and attempted privilege escalation. This directly matches the scenario: Steven deployed something that ''appears to contain very useful information'' to lure attackers and help identify their locations and techniques. Honeypots are typically instrumented with extensive logging and monitoring, making them especially useful for building timelines, extracting indicators of compromise, and understanding adversary tactics, techniques, and procedures.

The other options do not align with the ''bait attackers'' goal. An IDS primarily detects and alerts on suspicious activity but is not intended to impersonate a valuable target. A firewall enforces access control rules to block/allow traffic, not entice attackers. A router forwards packets and provides network connectivity; it is not a deception platform. Therefore, the device type described is a Honeypot (C).

Question 9

Question Type: MultipleChoice

A disk drive has 16,384 cylinders, 80 heads, and 63 sectors per track, and each sector can store 512 bytes of data.

What is the total size of the disk?

Options:

A- 42,278,584,320 bytes
B- 42,278,584,340 bytes
C- 42,279,584,320 bytes
D- 43,278,584,320 bytes

Answer:

A

Explanation:

In classic hard-disk geometry, total capacity is computed from CHS parameters (Cylinders Heads Sectors per track) multiplied by bytes per sector. Forensic examiners learn this because it helps validate whether an image acquisition size is consistent with the physical disk geometry and to spot anomalies caused by misreported device geometry or capture errors.

First compute total addressable sectors:

16,384 cylinders 80 heads = 1,310,720 tracks (because each head provides a track per cylinder).

Then multiply by sectors per track:

1,310,720 63 = 82,575,360 sectors.

Convert sectors to bytes using the sector size:

82,575,360 sectors 512 bytes/sector = 42,278,584,320 bytes.

This matches option A exactly. In practice, modern drives often use LBA and may report different logical geometries, but the forensic principle remains the same: capacity equals the number of logical blocks times the logical block size, and CHS-style values are a structured way to perform that verification.

Question 10

Question Type: MultipleChoice

Sam is working as a loan agent for a financial institution. He frequently receives a number of emails from clients providing their personal details for loan approval. As these emails contain sensitive data, Sam had set up a feature that directly downloads the emails on his device without storing a copy on the mail server. Which of the following protocols provides the above-discussed email features?

Options:

A- SHA-1
B- ICMP
C- POP3

D- SNMP

Answer:

C

Explanation:

The scenario describes an email-retrieval configuration in which messages are downloaded to a client device and not retained on the server. This behavior aligns with POP3 (Post Office Protocol v3), a legacy but widely referenced mail access protocol that retrieves email from a server mailbox to a local client. In standard POP3 operation, the client authenticates to the mail server, issues retrieval commands (e.g., to list and download messages), and may then issue a delete command so that downloaded messages are removed from the server mailbox. Digital forensics references commonly contrast POP3 with IMAP: IMAP is designed for server-side mailbox synchronization and typically leaves mail stored on the server, whereas POP3 is oriented toward client-side storage and supports workflows where server copies are not preserved after download. The other options are unrelated to email retrieval: SHA-1 is a cryptographic hash function used for integrity checks, ICMP supports network diagnostics and control messaging, and SNMP is used for network device management and monitoring. From an investigative standpoint, POP3 usage can reduce server-resident evidence and shift evidentiary value to local artifacts (mail client databases, cache, OS traces, backups), which is consistent with the intent described in the question.

Question 11

Question Type: MultipleChoice

In which of the following attacks does an attacker trick high-profile executives such as CEOs, CFOs, politicians, and celebrities to reveal critical corporate and personal information through email or website spoofing?

Options:

A- Whaling
B- Smishing
C- Identity fraud
D- Spimming

Answer:

A

Explanation:

The scenario describes a targeted social-engineering attack aimed specifically at high-profile individuals (CEOs, CFOs, politicians, celebrities) and uses email or website spoofing to deceive them into disclosing sensitive information. In digital forensics and incident response documentation, this is most accurately categorized as whaling, a specialized form of phishing that focuses on ''big targets'' (often called ''high-value targets'' or ''VIPs''). Whaling campaigns typically use highly tailored pretexts (e.g., legal subpoenas, board communications, invoice/payment requests, HR or executive directives) and may include spoofed sender domains, look-alike websites, or fraudulent login pages to harvest credentials and confidential corporate data. Because executives often have access to financial systems, strategic documents, and privileged communications, attackers concentrate effort on realism and personalization, making whaling distinct from broad, generic phishing.

By contrast, smishing is phishing conducted via SMS/text messages, spimming is spam over instant messaging platforms, and identity fraud is a broader category involving impersonation/misuse of personal data but does not specifically denote the executive-targeted spoofing technique described. Therefore, the attack type in the question is Whaling (A).

Question 12

Question Type: MultipleChoice

In which of the following malware distribution techniques does the attacker use tactics such as keyword stuffing, doorway pages, page swapping, and adding unrelated keywords to improve the search-engine ranking of their malware pages?

Options:

A- Drive-by downloads
B- Spearphishing sites
C- Black-hat search-engine optimization
D- Social-engineered clickjacking

Answer:

C

Explanation:

The technique described---keyword stuffing, doorway pages, page swapping, and inserting unrelated high-traffic keywords---matches black-hat search-engine optimization (SEO), often

called SEO poisoning in digital forensics and threat intelligence materials. In this distribution method, attackers manipulate search engine ranking algorithms so that malicious or malware-hosting pages appear near the top of search results for popular queries (breaking news, software downloads, trending events, adult content, etc.). Doorway pages are created to rank well for specific terms and then funnel victims to malicious landing pages. Page swapping (or ''bait-and-switch'') occurs when a page is optimized and indexed as benign content, but later replaced or dynamically served as malicious content once it has gained ranking and trust signals. Keyword stuffing and unrelated keyword injection further exploit ranking heuristics by artificially increasing perceived relevance.

From a forensic perspective, black-hat SEO campaigns often leave artifacts such as compromised websites with injected spam links, abnormal redirect chains, cloaking behavior (different content for crawlers vs. users), and malicious scripts or exploit kit references. The other options do not primarily rely on search ranking manipulation: drive-by downloads are about silent exploitation on visit, spearphishing relies on targeted messaging, and clickjacking tricks users into unintended clicks. Hence, Black-hat search-engine optimization (C) is correct.

Question 13

Question Type: MultipleChoice

Below are the various steps involved in an email crime investigation.

1.Acquiring the email data

2.Analyzing email headers

3.Examining email messages

4.Recovering deleted email messages

5.Seizing the computer and email accounts

6.Retrieving email headers

What is the correct sequence of steps involved in the investigation of an email crime?

Options:

A- 5-->1-->3-->6-->2-->4
B- 2-->4-->3-->6-->5-->1
C- 1-->3-->6-->4-->5-->2
D- 1-->3-->4-->2-->5-->6

Answer:

A

Explanation:

In an email crime investigation, the workflow should begin with seizing the computer and email accounts (5) to preserve evidence and prevent alteration, deletion, or continued misuse. This includes securing endpoints and ensuring account access is maintained under proper authority. Next, investigators proceed with acquiring the email data (1) using forensic methods (logical export, mailbox acquisition, or forensic imaging of local mail stores) to maintain integrity and chain of custody.

Once the data is preserved, investigators examine email messages (3) to identify relevant communications, context, attachments, and indicators of fraud, harassment, data leakage, or impersonation. After identifying emails of interest, investigators retrieve email headers (6) (full headers, not just what the mail client displays) because headers contain routing metadata required for attribution and timeline reconstruction. They then analyze email headers (2) to interpret fields such as Received lines, Message-ID, originating IP clues (where applicable), sending infrastructure, and authentication results, which helps determine spoofing, relay paths, and sender legitimacy. Finally, they recover deleted email messages (4) from mail stores, server-side retention, or unallocated space to restore missing evidence. This sequence matches option A.

To Get Premium Files for 112-57 Visit

https://www.p2pexams.com/products/112-57

For More Free Questions Visit

https://www.p2pexams.com/eccouncil/pdf/112-57