DUMPSARENA

Computer Hacking Forensic Investigator (v9)

ECCouncil 312-49v9

Version Demo

Total Demo Questions: 45

Total Premium Questions: 658

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Computer Forensics in Today's World	91
Topic 2, Computer Forensics Investigation Process	49
Topic 3, Understanding Hard Disks and File Systems	68
Topic 4, Data Acquisition and Duplication	49
Topic 5, Defeating Anti-Forensics Techniques	29
Topic 6, Windows Forensics	94
Topic 7, Linux and Mac Forensics	20
Topic 8, Network Forensics	96
Topic 9, Investigating Web Application Attacks	44
Topic 10, Database Forensics	11
Topic 11, Cloud Forensics	11
Topic 12, Investigating Email Crimes	35
Topic 13, Malware Forensics	17
Topic 14, Mobile Forensics	21
Topic 15, Mix Questions	23
Total	658

QUESTION NO: 1

When a user deletes a file, the system creates a $I file to store its details. What detail does the $I file not contain?

A. File Size

B. File origin and modification

C. Time and date of deletion

D. File Name

ANSWER: B

Explanation:

File origin and modification is the correct answer. In modern Windows Recycle Bin implementations, deletion creates a paired metadata record whose name begins with `$I`, alongside the corresponding `$R` file that contains the deleted file's content. The `$I` record is intended to preserve key deletion metadata: the original full path and file name, the logical size of the deleted file, and the date and time at which it was moved to the Recycle Bin. These values enable an examiner to identify what was deleted and when, even if the item has not yet been restored.

The record is not a complete historical file-system metadata record. In particular, it does not retain the file's original creation and last-modification history as deletion metadata. An examiner seeking those timestamps must obtain them from other artifacts where available, such as the relevant NTFS metadata, volume shadow copies, backups, journal records, or a recovered copy of the file. The Recycle Bin format's documented fields identify the original path, size, and deletion time; this makes it especially useful for establishing deletion events in a forensic timeline. See the Windows Recycle Bin format documentation and Microsoft's File Times documentation for the distinction between file timestamps and deletion-related metadata.

QUESTION NO: 2

Which of the following Windows Registry hives can contain useful evidence during an investigation? (Choose three.)

A. SAM

B. SYSTEM

C. SOFTWARE

D. BOOT.INI

E. NTLDR

ANSWER: A B C

Explanation:

SAM, **SYSTEM**, and **SOFTWARE** are correct. The SAM hive contains local account and group-related information. The SYSTEM hive contains system configuration information, including control sets, services, mounted devices, and hardware-related configuration. The SOFTWARE hive contains machine-wide application and operating-system configuration information, including installed-software traces.

These hives are normally located in the Windows system configuration directory and should be acquired from the forensic image together with their transaction logs when available. The Windows Registry is a central database for operating-system, application, hardware, and user configuration data. See Microsoft Windows Registry documentation.

QUESTION NO: 3

Ivanovich, a forensics investigator, is trying to extract complete information about running processes from a system. Where should he look apart from the RAM and virtual memory?

A. Swap space

B. Application data

C. Files and documents

D. Slack space

ANSWER: A

Explanation:

Swap space is the correct location because operating systems use it as secondary backing storage for memory pages that are moved out of physical RAM. During normal execution, portions of a process's address space, including potentially useful remnants of process memory, may be paged to the swap area. This can preserve data that is no longer resident in an acquired RAM image, such as application content, command-line fragments, network-related artifacts, credentials, or memory structures associated with a process.

For a complete process-focused forensic examination, an investigator should therefore collect and preserve the swap partition or swap file in addition to volatile-memory evidence. The swap area should be acquired carefully and correlated with the operating system, its paging configuration, and the relevant memory acquisition. This broader acquisition approach can improve reconstruction of process activity because memory pages may have transitioned between physical memory and swap over the system's uptime. NIST describes volatile data collection as a key part of incident handling and emphasizes preserving relevant system data for later analysis. Guidance on Windows paging files also confirms that paging files support virtual-memory management by storing pages moved from RAM. See NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response and Microsoft documentation on page files and virtual memory.

QUESTION NO: 4

Jason discovered a file named $RIYG6VR.doc in the C:\$Recycle.Bin\\ while analyzing a hard disk image for the deleted data. What inferences can he make from the file name?

A. It is a doc file deleted in seventh sequential order

B. RIYG6VR.doc is the name of the doc file deleted from the system

C. It is file deleted from R drive

D. It is a deleted doc file

ANSWER: D

Explanation:

It is a deleted doc file. On supported versions of Windows, the Recycle Bin stores items in a per-user directory under `C:\$Recycle.Bin\<SID>`. When a user sends a file to the Recycle Bin, Windows creates a paired set of artifacts whose names begin with `$I` and `$R`, followed by the same random-looking identifier. The `$R` file holds the recycled file's content, while its retained `.doc` extension indicates that the deleted item was a Word document in the older binary document format. Thus, finding `$RIYG6VR.doc` establishes that the file is the content artifact for a deleted document that was placed in that user's Recycle Bin. In a forensic examination, the matching `$IIYG6VR.doc` record is especially valuable because it can provide metadata such as the item's original full path, original file size, and deletion time. This lets an examiner associate the recovered content with its pre-deletion location and relevant timeline event. Microsoft documents the Recycle Bin storage location and behavior in its Recycle Bin documentation; further practical details on interpreting `$I`/`$R` artifacts are available from SANS.

QUESTION NO: 5

You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls? (Choose two.)

A. 162

B. 161

C. 163

D. 160

ANSWER: A B

Explanation:

SNMP commonly uses UDP port 161 for communications between an SNMP manager and an SNMP agent. The manager sends polling requests, such as requests for device status, interface counters, and other managed-object values, to the agent on UDP 161. Opening UDP 161 in the appropriate direction is therefore necessary for the manager to query SNMP-enabled devices at remote offices.

UDP port 162 is used for SNMP notifications, including traps and informs. An SNMP agent sends unsolicited traps to the manager's configured trap receiver on UDP 162; SNMP informs also use this notification port, although they are acknowledged. In a multi-office deployment, firewall rules must permit the relevant UDP 161 polling traffic and UDP 162 notification traffic between the manager and remote SNMP agents. Rules should be narrowly scoped to the known manager and agent IP addresses rather than exposed broadly, and SNMPv3 should be used where possible to provide authentication and encryption.

The Internet Assigned Numbers Authority lists snmp (161) and snmptrap (162) as the registered SNMP service ports.

QUESTION NO: 6

Why is it a good idea to perform a penetration test from the inside?

A. It is never a good idea to perform a penetration test from the inside

B. Because 70% of attacks are from inside the organization

C. To attack a network from a hacker's perspective

D. It is easier to hack from the inside

ANSWER: B

Explanation:

Because 70% of attacks are from inside the organization is the intended answer because an internal penetration test evaluates the risks posed by people or systems that already have access to the organization's environment. This perspective models scenarios such as a malicious insider, a compromised employee account, an infected endpoint, or an attacker who has already gained an initial foothold. Testing from within reveals whether internal network segmentation, least-privilege access, authentication controls, monitoring, and protections around sensitive data can limit lateral movement and prevent escalation of privileges. The stated percentage should be understood as a commonly cited training rationale rather than a universal, current measurement; the key security principle is that insider-originated and post-compromise activity is a significant risk that must be assessed. NIST's penetration-testing guidance recognizes testing from different perspectives and emphasizes evaluating the security of systems in realistic conditions. CISA also identifies insider threats as risks arising from individuals with authorized access. See NIST SP 800-115 and CISA Insider Threat Mitigation.

QUESTION NO: 7

Which of the following are important characteristics of a formal digital forensic report? (Choose three.)

A. Objective findings

B. A description of the methods used

C. Documented limitations

D. Unsupported opinions stated as facts

E. Omission of findings unfavorable to the client

ANSWER: A B C

Explanation:

Objective findings, **a description of the methods used**, and **documented limitations** are correct. A formal report should clearly distinguish facts, analysis, and conclusions; identify the evidence and methods used; and disclose relevant limitations, assumptions, or conditions that affect interpretation. These elements allow decision makers to understand and evaluate the examiner's work.

A forensic report should not contain unsupported opinions or omit unfavorable results. Accurate reporting is essential because the report may be reviewed by management, opposing parties, counsel, or a court. NIST identifies reporting as a key part of the forensic process and emphasizes documenting actions and findings. See NIST SP 800-86.

QUESTION NO: 8

If you discover a criminal act while investigating a corporate policy abuse, it becomes a publicsector investigation and should be referred to law enforcement?

A. true

B. false

ANSWER: A

Explanation:

true is correct. A corporate policy-abuse inquiry is ordinarily a private-sector investigation, conducted to establish whether internal rules were violated and to support an organization’s employment, disciplinary, or risk-management decisions. If the examiner identifies evidence indicating that a criminal offense may have occurred, the matter must be handled with the possibility of a public-sector, law-enforcement investigation in mind. The organization should promptly involve its legal counsel and refer or report the suspected crime to the appropriate law-enforcement authority under applicable law and organizational policy.

This referral is important because law enforcement has the statutory authority to investigate crimes, seek legal process where necessary, and pursue prosecution. The forensic examiner should preserve relevant evidence carefully, document each action taken, maintain evidence integrity, and be prepared to provide records that establish a clear chain of custody. These practices allow the evidence to be evaluated and, where appropriate, used in a criminal proceeding. The U.S. Department of Justice’s digital-evidence guidance emphasizes preserving digital evidence and documenting collection and handling, while NIST describes sound forensic processes for collecting and preserving evidence. See the U.S. Department of Justice Electronic Crime Scene Investigation guide and NIST SP 800-86.

QUESTION NO: 9

In conducting a computer abuse investigation you become aware that the suspect of the investigation is using ABC Company as his Internet Service Provider (ISP). You contact ISP and request that they provide you assistance with your investigation. What assistance can the ISP provide?

A. The ISP can investigate anyone using their service and can provide you with assistance

B. The ISP can investigate computer abuse committed by their employees, but must preserve the privacy of their customers and therefore cannot assist you without a warrant

C. The ISP can't conduct any type of investigations on anyone and therefore can't assist you

D. ISP's never maintain log files so they would be of no use to your investigation

ANSWER: B

Explanation:

The ISP can investigate computer abuse committed by their employees, but must preserve the privacy of their customers and therefore cannot assist you without a warrant is the best answer in the context of a forensic investigation. An ISP is entitled to investigate suspected misuse, misconduct, or abuse involving its own personnel, systems, network, and services. However, subscriber records, connection logs, and especially the contents of customer communications are subject to privacy protections and statutory limits on provider disclosure. Investigators should therefore use appropriate legal process before expecting an ISP to disclose customer-related evidence. In practice, the precise process can depend on the type of data sought, how long it has been stored, and the jurisdiction; investigators may also request preservation promptly while obtaining the required authority. This reflects the core forensic principle that evidence collection from a third-party service provider must be both technically sound and legally authorized. The U.S. Department of Justice's discussion of electronic evidence describes the legal processes used to obtain stored communications and related records, while the Stored Communications Act establishes restrictions and procedures for provider disclosures. See the DOJ Electronic Evidence guide and 18 U.S.C. § 2703.

QUESTION NO: 10

Where does Encase search to recover NTFS files and folders?

A. MBR

B. MFT

C. Slack space

D. HAL

ANSWER: B

Explanation:

EnCase searches the NTFS Master File Table (MFT) to recover NTFS files and folders. The MFT is NTFS's central metadata database: it contains a record for every file and directory, including names, logical sizes, timestamps, attributes, security information, and—where applicable—references to the disk clusters holding file content. When an NTFS item is deleted, its MFT record may remain available until it is reused, often retaining metadata and potentially references that permit forensic software to identify and recover the deleted item. EnCase interprets these filesystem structures during evidence processing, allowing an examiner to view allocated and deleted entries, reconstruct directory relationships, and recover data when the relevant metadata and clusters have not been overwritten. This makes the MFT a primary source for NTFS file and folder recovery, as well as for validating artefact timelines during an investigation. Microsoft's NTFS technical reference describes the MFT as the database in which NTFS stores information about every file and directory on a volume. Forensic handling should preserve the original evidence and perform such recovery against a verified forensic image. See Microsoft's Master File Table documentation and NIST's Guide to Integrating Forensic Techniques into Incident Response.

QUESTION NO: 11

companyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware.

A. Source code review

B. Reviewing the firewalls configuration

C. Data items and vulnerability scanning

D. Interviewing employees and network engineers

E. External penetration testing of the email gateway

ANSWER: E

Explanation:

External penetration testing of the email gateway is correct because the assessor is actively exercising a publicly reachable perimeter service from outside the organization's network. Crafting and transmitting a specially formatted message tests whether the gateway correctly inspects, filters, routes, quarantines, or blocks potentially malicious or malformed email content under realistic delivery conditions. This is an active security assessment rather than a review of documentation, source code, or configuration alone. The recipient's awareness and the company's authorization establish an appropriate testing arrangement, helping ensure the message can be monitored and its effects assessed without being mistaken for an unauthorized attack. A properly scoped engagement should define permitted message types, target addresses, handling of attachments or links, expected logging, escalation contacts, and evidence collection. NIST describes penetration testing as a method of testing security controls through simulated attacks, including activities that validate how systems respond in operational conditions. Its testing guidance also emphasizes authorization, defined scope, and careful coordination for potentially disruptive tests. See NIST SP 800-115, Technical Guide to Information Security Testing and Assessment and CISA guidance on penetration testing.

QUESTION NO: 12

When carrying out a forensics investigation, why should you never delete a partition on a dynamic disk?

A. All virtual memory will be deleted

B. The wrong partition may be set to active

C. This action can corrupt the disk

D. The computer will be set in a constant reboot state

ANSWER: C

Explanation:

This action can corrupt the disk is correct because a Windows dynamic disk stores its volume configuration in dynamic-disk metadata, rather than relying solely on the conventional partition-table layout used by basic disks. Removing a volume or partition-like structure is therefore a write operation that can change or remove the metadata required to identify volume membership, extents, and relationships among disks. In particular, dynamic volumes may span, stripe, or mirror data across more than one disk. Altering the configuration can make the volume inaccessible, damage the logical layout needed for reconstruction, or cause the operating system to update metadata during subsequent disk management activity. From a forensic perspective, this risks both loss of potentially relevant data and loss of the original state of evidence. Investigators should preserve the source media, acquire a verified forensic image where possible, and conduct any necessary recovery or reconstruction on a working copy using read-only procedures. Microsoft describes dynamic disks as supporting volumes that can extend across disks and notes the role of dynamic-disk configuration information in volume management. See Microsoft's Dynamic Disks and Volumes documentation. NIST's forensic guidance likewise emphasizes preserving digital evidence and avoiding actions that modify original media: NIST SP 800-86.

QUESTION NO: 13

What type of file is represented by a colon (:) with a name following it in the Master File Table of NTFS disk?

A. A compressed file

B. A Data stream file

C. An encrypted file

D. A reserved file

ANSWER: B

Explanation:

A Data stream file is correct. In NTFS, a file can contain more than one data stream. The normal, unnamed stream holds the file's primary content, while an additional named stream is identified by appending a colon and stream name to the file name, such as `document.txt:metadata`. These are commonly called NTFS alternate data streams (ADS). In forensic work, the colon notation is significant because a named stream may contain data that is not displayed through ordinary directory listings or apparent in the file's normal size. The Master File Table records the file's attributes, including data attributes associated with streams, enabling an examiner to identify and investigate named streams. A stream can be accessed using the full `filename:streamname` syntax, subject to the relevant application and operating-system behavior. Recognizing this notation helps investigators locate potentially concealed content, preserve it during collection, and assess its relationship to the host file. Microsoft documents the colon-based stream syntax and describes named streams as alternate streams associated with an NTFS file. See Microsoft: File Streams and Microsoft: Naming Files, Paths, and Namespaces.

QUESTION NO: 14

When examining a hard disk without a write-blocker, you should not start windows because Windows will write data to the:

A. Recycle Bin

B. MSDOS.sys

C. BIOS

D. Case files

ANSWER: A

Explanation:

Recycle Bin is the correct answer in the context of this forensic-handling question. Starting an installed Windows operating system from the disk under examination is an evidentiary-risk event: the operating system mounts the volume and performs routine filesystem and desktop-maintenance activity. In particular, Windows maintains per-volume Recycle Bin metadata and its associated hidden system folder, so activity involving deleted-item records can alter artifacts on the evidence drive. Any such change undermines the forensic principle of preserving the original media in an unchanged state and can affect the reliability of later findings about deleted files and filesystem metadata.

A forensic examiner should instead prevent writes at the hardware or trusted forensic-acquisition layer, normally by using a validated write-blocker before imaging or examining the drive. NIST describes the need to preserve digital evidence and to acquire it in a manner that avoids altering the original evidence. SWGDE likewise publishes guidance for validating write-blocking tools, reflecting the importance of preventing host systems from modifying attached evidence media. See NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response and SWGDE published digital-forensics documents.

QUESTION NO: 15

An investigator seizes a powered-on mobile device that may contain relevant evidence. Which of the following actions help preserve the device and its evidence? (Choose three.)

A. Photograph and document the device condition

B. Isolate the device from wireless networks

C. Maintain power when appropriate

D. Open messaging applications to review recent messages

E. Install a forensic application on the original device

ANSWER: A B C

Explanation:

Photographing and documenting the device condition, **isolating the device from wireless networks**, and **maintaining power when appropriate** are correct. Documentation preserves the device's observed state, screen display, attached items, and identifying information before handling changes occur. Wireless isolation can reduce the risk of remote wiping, synchronization, or incoming changes. Maintaining power may be necessary to avoid losing volatile data or encountering encryption protections after shutdown.

The correct handling decision depends on the device state, legal authority, safety concerns, and organizational procedure. An examiner should not browse through applications because doing so can alter evidence. NIST recommends documenting, preserving, isolating, and carefully handling mobile devices during collection. See NIST SP 800-101 Rev. 1.

QUESTION NO: 16

You should make at least how many bit-stream copies of a suspect drive?

A. 1

B. 2

C. 3

D. 4

ANSWER: B

Explanation:

2 is correct. Standard forensic acquisition practice is to create at least two verified bit-stream (forensic) images of a suspect drive. One image is retained as the protected master or evidence copy, kept unchanged so that the original acquired evidence remains available for validation, disclosure, or later re-examination. The second image is the working copy used for forensic examination, recovery attempts, keyword searches, timeline construction, and tool-based analysis. This separation protects evidentiary integrity because ordinary examination processes can create derived data, annotations, indexes, or otherwise risk unintended changes to the media being analyzed. Each acquired image should be cryptographically hashed during acquisition and verified afterward; matching hash values demonstrate that the forensic image is an exact bit-level representation of the acquired source at the time of collection. Documentation should record the acquisition method, tool and version, examiner, timestamps, hash algorithm and values, storage location, and chain-of-custody details. NIST's guidance on integrating forensic techniques emphasizes preserving data integrity and maintaining documented, repeatable processes: NIST SP 800-86. The National Institute of Justice also provides guidance on digital-evidence handling and forensic examination practices: Forensic Examination of Digital Evidence.

QUESTION NO: 17

You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the target computer, but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?

A. The registry

B. The swap file

C. The recycle bin

D. The metadata

ANSWER: B

Explanation:

The swap file is the appropriate next artifact to examine because it can retain portions of data that were held in a process's memory but never saved as a conventional user file. Operating systems use virtual memory to move memory pages between RAM and disk when needed. Consequently, the swap file may contain recoverable text, document fragments, application data, account details, cheque values, payee information, or remnants of a printing application's in-memory document content. This is particularly relevant where the suspected activity involved creating or printing unauthorized cheques without saving the document to the filesystem. A forensic examination should preserve the original image, identify the operating system's paging or swap artifacts, and search them using relevant keywords, names, account numbers, cheque numbers, and application-specific signatures. Investigators should also correlate any recovered fragments with timestamps and other available system artifacts to establish context. Microsoft documents that Windows virtual-memory paging uses page files, and notes that page-file contents may contain data that has been paged from memory. This makes such files a valuable source of residual evidence in an investigation involving unsaved work. See Microsoft's page-file overview and the NIST guide to forensic techniques.

QUESTION NO: 18

Which code does the FAT file system use to mark the file as deleted?

A. ESH

B. 5EH

C. H5E

D. E5H

ANSWER: D

Explanation:

The correct answer is **E5H** (hexadecimal `0xE5`). In a FAT file system, each file is represented by a 32-byte directory entry. When a file is deleted, FAT does not immediately erase its directory entry or overwrite the clusters that held the file's contents. Instead, it replaces the first byte of the file name field in that directory entry with the hexadecimal value `E5`. This marks the entry as available for reuse while leaving potentially recoverable metadata—such as the original starting cluster, file size, timestamps, and attributes—and the underlying data clusters intact until they are overwritten.

This behavior is significant during forensic examination because a deleted FAT file can often be reconstructed by identifying directory entries whose first filename byte is `0xE5`, restoring or inferring the original first character of the name, and following the cluster information where it remains available. The FAT specification also defines a special handling case for filenames whose real first character is `0xE5`: that character is stored as `0x05` to avoid confusion with the deletion marker. See Microsoft's FAT file-system specification and the OSDev FAT documentation for the directory-entry format and deletion-marker details.

QUESTION NO: 19

When making the preliminary investigations in a sexual harassment case, how many investigators are you recommended having?

A. One

B. Two

C. Three

D. Four

ANSWER: B

Explanation:

Two is the recommended number for preliminary investigation of a sexual-harassment allegation. Using two investigators provides a practical safeguard for the integrity of the early fact-finding process: one person can lead questioning while the other observes, takes contemporaneous notes, and identifies points requiring follow-up. This reduces reliance on a single person's recollection and helps create a clearer, more defensible record of what was reported and how the organization responded.

A two-person approach is particularly valuable in sensitive matters because the investigators can support an impartial, respectful interview process and can compare observations after meetings without treating assumptions as evidence. It also helps maintain continuity if one investigator is unavailable and supports careful handling of evidence, interview accounts, and preliminary decisions about escalation. The recommended arrangement should still preserve confidentiality as far as possible, avoid conflicts of interest, and ensure the investigators have appropriate authority and training. This approach aligns with the expectation that harassment complaints receive prompt, thorough, and impartial investigation, reflected in guidance from the U.S. Equal Employment Opportunity Commission and the UK Advisory, Conciliation and Arbitration Service.

QUESTION NO: 20

Which of the following are common indicators that a web server may have been targeted for directory traversal? (Choose two.)

A. Encoded ../ sequences in requested URLs

B. Requests for files outside the web root

C. Requests for CSS files in the public site directory

D. Successful retrieval of a public JPEG image

ANSWER: A B

Explanation:

Requests containing encoded traversal sequences and requests attempting to access operating-system files outside the web root are indicators of directory traversal activity. Attackers may use sequences such as `../` or encoded variants to attempt to move upward through the directory hierarchy and retrieve files that should not be exposed by the web application. A normal request for a stylesheet and a successful request for an image within the public web directory do not by themselves indicate traversal. OWASP describes directory traversal attacks and common encoded path-traversal patterns in its Path Traversal guidance.

QUESTION NO: 21

Netstat is a tool for collecting information regarding network connections. It provides a simple view of TCP and UDP connections, and their state and network traffic statistics. Which of the following commands shows you the TCP and UDP network connections, listening ports, and the identifiers?

A. netstat – r

B. netstat -ano

C. netstat – b

D. netstat – s

ANSWER: B

Explanation:

`netstat -ano` is the appropriate Windows command because it combines three useful Netstat switches for forensic network triage. The `-a` switch displays all active connections and all listening TCP and UDP ports, providing visibility into services that are waiting for inbound communications as well as established or pending sessions. The `-n` switch displays

addresses and port numbers numerically instead of resolving names; this avoids DNS-related delays and preserves the exact IP address and port values observed during collection. The `-o` switch adds the owning process identifier (PID) to each connection or listening-port record. That PID is particularly important in an investigation because it can be correlated with process information, such as output from Task Manager, `tasklist`, or other process-collection tools, to identify the executable associated with suspicious network activity. Microsoft documents that Netstat can display active TCP connections, listening ports, UDP endpoints, and the PID for each connection. See Microsoft Netstat command documentation and Microsoft Tasklist command documentation.

QUESTION NO: 22

The process of restarting a computer that is already turned on through the operating system is called?

A. Warm boot

B. Ice boot

C. Hot Boot

D. Cold boot

ANSWER: A

Explanation:

Warm boot is the term for restarting a computer while it is already powered on, typically by using an operating-system command such as Restart. The operating system performs an orderly restart: it closes running processes, stops services, flushes pending data where possible, and initiates the boot sequence again without requiring the user to turn off system power manually. This distinction is important in computer forensics because a restart changes the system's volatile state. Contents held only in RAM—including active processes, network connections, encryption keys, and other transient artifacts—are normally lost when the system reboots. Accordingly, forensic best practice is to assess and, where authorized, collect volatile evidence before initiating any restart or shutdown. NIST's incident-handling guidance emphasizes collecting volatile data before less volatile sources, since volatile information can disappear quickly during system-state changes. Microsoft also documents the Restart action as an operating-system power command that restarts the device. See NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response and Microsoft Support: Shut down, sleep, or hibernate your PC.

QUESTION NO: 23

In handling computer-related incidents, which IT role should be responsible for recovery, containment, and prevention to constituents?

A. Security Administrator

B. Network Administrator

C. Director of Information Technology

D. Director of Administration

ANSWER: B

Explanation:

Network Administrator is the appropriate role because this position has the operational control and technical access needed to contain an incident, restore affected network services, and implement safeguards that prevent recurrence for the organization's users and systems. During containment, the network administrator can isolate compromised hosts or network segments, modify access-control rules, block malicious traffic, and preserve the availability of unaffected services. During recovery, the role can return network connectivity and infrastructure components to an approved, secure operating state while coordinating required changes with the incident-response process. Prevention also depends on applying network hardening, segmentation, monitoring, secure configuration, and timely remediation across the environment. NIST describes

containment, eradication, and recovery as core incident-response activities and emphasizes selecting and applying containment strategies based on the incident and operational impact. These activities require the hands-on network administration capability represented by this role. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and CISA Incident Response guidance.

QUESTION NO: 24

George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity. George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network.

What filter should George use in Ethereal?

A. src port 23 and dst port 23

B. udp port 22 and host 172.16.28.1/24

C. net port 22

D. src port 22 and dst port 22

E. tcp port 22 and net 172.16.28.0/24

ANSWER: E

Explanation:

`tcp port 22 and net 172.16.28.0/24` is the appropriate Ethereal/Wireshark capture filter because SFTP is normally carried as a subsystem over an SSH connection, and SSH servers conventionally listen on TCP port 22. The `tcp port 22` portion captures packets in either direction whenever either endpoint uses port 22; this is essential because a client normally uses a temporary high-numbered source port while the server uses port 22. The `net 172.16.28.0/24` portion limits the capture to traffic involving the specified corporate subnet, rather than collecting all SSH traffic visible on the capture interface. This meets the requirement to observe relevant traffic both to and from George's network while avoiding unrelated protocols and networks. Wireshark's capture-filter documentation describes the `port` and `net` primitives and their use with protocol qualifiers: pcap-filter manual. SSH's assigned well-known service port is TCP 22, as recorded in the IANA service-name registry: IANA SSH service registration. Because SSH encrypts application payloads, this filter establishes evidence of SSH/SFTP-capable connections; proving the specific SFTP subsystem may require endpoint or session evidence.

QUESTION NO: 25

Which of the following information can be obtained from a TCP header during network forensic analysis? (Choose three.)

A. Source port

B. Destination port

C. Sequence number

D. MAC address

E. URL

ANSWER: A B C

Explanation:

Source port, **destination port**, and **sequence number** are correct. TCP uses source and destination port numbers to identify the communicating application endpoints. The sequence number supports ordered delivery and can assist an investigator in reconstructing the progression of a TCP stream.

A MAC address is contained in a data-link-layer frame header, not in the TCP header. A URL is generally part of application-layer protocol data, such as an HTTP request, rather than a TCP header field. TCP header fields and their functions are specified in RFC 9293: Transmission Control Protocol.

QUESTION NO: 26

Which of the following statements is TRUE with respect to the Registry settings in the user start-up folder HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\.

A. All the values in this subkey run when specific user logs on, as this setting is user-specific

B. The string specified in the value run executes when user logs on

C. All the values in this key are executed at system start-up

D. All values in this subkey run when specific user logs on and then the values are deleted

ANSWER: D

Explanation:

All values in this subkey run when specific user logs on and then the values are deleted is correct. The `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce` key is a per-user Windows startup location. Windows processes the commands stored as values in this key when the associated user logs on, making it useful for tasks that must occur once in that user's session, such as completing an installation or performing one-time configuration. The defining behavior of `RunOnce` is that its entries are removed after they have been processed, so they are not normally launched again at later logons. This differs from persistent startup mechanisms because the intended lifecycle is execution for one logon followed by removal of the value. From a forensic perspective, investigators should examine the value name, command data, user SID/profile associated with the hive, and surrounding registry artifacts, because malware may use RunOnce values for one-time execution or may attempt to manipulate their deletion behavior. Microsoft documents the Run and RunOnce registry keys and identifies `HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce` as a RunOnce startup location processed at user logon. See Microsoft's Run and RunOnce Registry Keys documentation and MITRE ATT&CK: Registry Run Keys / Startup Folder.

QUESTION NO: 27

An examiner is preparing a forensic image of a seized SATA hard drive. Which of the following practices help preserve evidence integrity? (Choose three.)

A. Use a validated write-blocker

B. Calculate and record hash values

C. Maintain chain-of-custody documentation

D. Boot the seized drive into its installed operating system

E. Perform analysis directly on the original drive

ANSWER: A B C

Explanation:

Using a validated write-blocker, calculating and recording cryptographic hash values, and maintaining chain-of-custody documentation are correct. A write-blocker prevents the acquisition workstation from altering the source device. Hash values allow the examiner to verify that the acquired image matches the source at acquisition and has not changed later. Chain-of-custody records document possession, transfers, storage, and handling of the evidence. Booting the seized drive into its installed operating system can modify files and metadata, while analyzing the original rather than a verified working copy unnecessarily exposes the evidence to alteration. NIST discusses preservation, acquisition, integrity verification, and documentation in NIST SP 800-86.

QUESTION NO: 28

What file structure database would you expect to find on floppy disks?

A. NTFS

B. FAT32

C. FAT16

D. FAT12

ANSWER: D

Explanation:

FAT12 is the file-system structure traditionally expected on standard floppy disks. The File Allocation Table family was designed for relatively small storage volumes, and FAT12 uses 12-bit entries in its allocation table to track clusters. This addressing capacity is well suited to the common floppy formats encountered during forensic examinations, including 1.44 MB, 1.2 MB, 720 KB, and 360 KB disks. A forensic examiner who identifies FAT12 should therefore expect familiar FAT volume structures, such as a boot sector containing the BIOS Parameter Block, one or more FAT copies, a root-directory region, and the data area. Understanding this layout supports recovery and interpretation of directory entries, deleted-file indicators, cluster chains, and volume metadata on legacy removable media. Microsoft's FAT specification describes FAT12 as the FAT variant used for small volumes and documents the boot-sector and allocation-table structures relevant to parsing such media. The OSDev Wiki also provides a practical technical overview of the FAT12 disk layout, including the reserved, FAT, root-directory, and data regions. See Microsoft FAT specification and OSDev FAT12 documentation.

QUESTION NO: 29

You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

A. Poison the DNS records with false records

B. Enumerate MX and A records from DNS

C. Establish a remote connection to the Domain Controller

D. Enumerate domain user accounts and built-in groups

ANSWER: D

Explanation:

Enumerate domain user accounts and built-in groups is correct because ldp.exe is a Microsoft LDAP client used to connect to and query directory services such as Active Directory Domain Services. LDAP commonly listens on TCP port 389 for standard, non-encrypted LDAP communications. Once connected to a domain controller with suitable credentials, an operator can browse or search the directory naming context and retrieve objects and attributes. This includes user objects, group objects, group membership attributes, organizational units, computers, and other domain information. In a forensic or penetration-testing context, directory enumeration helps establish which identities, privileged groups, and relationships exist in the domain, which can support investigation of account exposure or privilege paths. Microsoft describes Ldp.exe as a graphical LDAP client for viewing and editing LDAP directory information, and its Active Directory documentation explains that users and groups are directory objects available through LDAP queries. See Microsoft: LDAP and Active Directory and Microsoft: Ldp Overview.

QUESTION NO: 30

The newer Macintosh Operating System is based on:

A. OS/2

B. BSD Unix

C. Linux

D. Microsoft Windows

ANSWER: B

Explanation:

BSD Unix is correct. Modern macOS (formerly Mac OS X) is built on Darwin, an open-source, Unix-based operating system foundation. Darwin combines technologies derived from BSD Unix with the Mach kernel, forming the core of Apple's XNU kernel architecture. This Unix heritage is important in forensic work because macOS uses familiar Unix concepts, including POSIX-style permissions, user and group identities, processes, shells, filesystem paths, system logs, and command-line utilities. Although macOS has Apple-specific frameworks and a distinct graphical interface, its underlying operating system architecture remains certified as UNIX compliant for applicable versions. Apple describes macOS as being built on Darwin, which integrates technologies from BSD and Mach; its open-source materials also identify XNU as the kernel used by Darwin-based systems. Understanding this foundation helps an examiner apply Unix-oriented acquisition, artifact analysis, and command-line investigation techniques appropriately when handling Macintosh evidence. See Apple's Darwin open-source project information and the Apple XNU project page for the operating-system and kernel background.

QUESTION NO: 31

E-mail logs contain which of the following information to help you in your investigation? (Choose four.)

A. user account that was used to send the account

B. attachments sent with the e-mail message

C. unique message identifier

D. contents of the e-mail message

E. date and time the message was sent

ANSWER: A C D E

Explanation:

E-mail logs and associated message records are valuable forensic evidence because they preserve metadata and, depending on the mail system and logging configuration, message-level information needed to reconstruct an e-mail event. The user account that was used to send the account identifies the authenticated or submitting account associated with transmission, helping investigators attribute activity and correlate it with account, authentication, and server records. A unique message identifier supports correlation of the same message across mail servers, gateways, archives, and recipient-side records. The contents of the e-mail message may be retained in message-tracking, journaling, archival, or transport records, allowing investigators to assess what was communicated and to search for relevant terms or indicators. The date and time the message was sent establishes a timeline and enables correlation with other evidence, including login events, network connections, endpoint artifacts, and server logs. E-mail message format standards define fields such as Message-ID and date-related header information, while forensic guidance emphasizes preserving and correlating e-mail metadata and content where available. See RFC 5322: Internet Message Format and NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response.

QUESTION NO: 32

Which of the following information should be included in an evidence chain-of-custody record? (Choose three.)

A. Identity of each person handling the evidence

B. Date and time of each transfer

C. Purpose of the transfer

D. Examiner's personal opinion of the suspect

E. Unrelated corporate financial information

ANSWER: A B C

Explanation:

The identity of each person handling the evidence, the date and time of each transfer, and the purpose of the transfer are essential chain-of-custody details. These records establish who possessed the evidence, when possession changed, and why the evidence was moved or accessed. The chain of custody supports authentication by demonstrating controlled and documented handling from collection through presentation. The examiner's personal opinion about a suspect and unrelated corporate financial information do not belong in a chain-of-custody record. The U.S. Department of Justice discusses evidence possession and transfer documentation in its chain-of-custody guidance.

QUESTION NO: 33

Smith, a forensic examiner, was analyzing a hard disk image to find and acquire deleted sensitive files. He stumbled upon a $Recycle.Bin folder in the root directory of the disk. Identify the operating system in use.

A. Windows 98

B. Linux

C. Windows 8.1

D. Windows XP

ANSWER: C

Explanation:

Windows 8.1 is the correct identification because modern Windows systems store Recycle Bin contents in a protected, hidden root-level directory named `$Recycle.Bin`. This directory is created separately on each volume that supports the Recycle Bin, and it contains per-user subdirectories identified by security identifiers. During forensic examination, these folders can retain valuable evidence about deleted objects, including metadata and the renamed data files associated with Recycle Bin entries. The presence of `$Recycle.Bin` therefore indicates a Windows generation using the newer Recycle Bin directory convention, which includes Windows 8.1. This artifact is especially useful when examining an acquired image because deleted files may remain recoverable from their Recycle Bin storage location even when they no longer appear in the user's active folders. Microsoft documents the Recycle Bin as a Windows Shell component and describes its role in handling deleted filesystem objects; see Microsoft Learn: Recycle Bin. For background on Windows file-system and storage forensic artifacts, see Microsoft Learn: File Management.

QUESTION NO: 34

Which of the following fields can be obtained from an IPv4 packet header during network forensic analysis? (Choose three.)

A. Source IP address

B. Destination IP address

C. Time To Live value

D. TCP sequence number

E. TCP destination port

ANSWER: A B C

Explanation:

The source IP address, destination IP address, and Time To Live (TTL) value are fields in an IPv4 header. Source and destination addresses identify the logical endpoints represented in the packet, while TTL is decremented by routers to prevent packets from circulating indefinitely. TCP sequence numbers and TCP destination ports are found in a TCP header, not the IPv4 header. The Internet Protocol header format is specified in RFC 791.

QUESTION NO: 35

> NMAP -sn 192.168.11.200-215 The NMAP command above performs which of the following?

A. A trace sweep

B. A port scan

C. A ping scan

D. An operating system detect

ANSWER: C

Explanation:

A ping scan is correct because the `-sn` option instructs Nmap to perform host discovery without conducting a port scan. Nmap probes the target range from `192.168.11.200` through `192.168.11.215` to determine which systems are online or otherwise responsive. This type of scan is commonly called a ping scan, although Nmap's host-discovery process can use several probe types depending on privileges, network location, and target behavior, rather than relying exclusively on ICMP Echo Requests. For example, on a local Ethernet network, Nmap typically uses ARP requests; in other circumstances it may use ICMP, TCP, or other discovery probes. The key result is a list of hosts that Nmap identifies as up, with port enumeration deliberately omitted. This is useful during the reconnaissance phase of an investigation or authorized security assessment to establish the active address space before applying more targeted collection or scanning methods. Nmap documents `-sn` as "Ping Scan," noting that it disables port scanning after host discovery. See the Nmap host discovery reference and the Nmap reference guide.

QUESTION NO: 36

After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks.

What countermeasures could he take to prevent DDoS attacks?

A. Enable direct broadcasts

B. Disable direct broadcasts

C. Disable BGP

D. Enable BGP

ANSWER: B

Explanation:

Disabling direct broadcasts is an effective countermeasure because it prevents a network from being used as an amplifier in broadcast-based denial-of-service attacks, particularly Smurf-style attacks. In such an attack, an adversary sends ICMP echo requests to a subnet's directed broadcast address while spoofing the victim's source address. If routers forward directed broadcasts, every reachable host on that destination subnet may reply to the spoofed victim, multiplying the volume of traffic directed at the victim. Configuring routers not to forward directed broadcasts removes this amplification path and reduces both the organization's exposure as an unwitting attack intermediary and the likelihood that its routing infrastructure

supports this attack pattern. RFC 2644 specifically establishes that routers should not receive directed broadcasts by default, reflecting the long-standing operational security practice of disabling them to mitigate network-wide broadcast attacks. This control should be part of a layered DDoS defense program that also includes anti-spoofing filtering, traffic monitoring, rate limiting where appropriate, and upstream provider coordination. The directly relevant preventive configuration in this question is disabling direct broadcasts. See RFC 2644: Changing the Default for Directed Broadcasts in Routers and CISA: Understanding Denial-of-Service Attacks.

QUESTION NO: 37

During the trial, an investigator observes that one of the principal witnesses is severely ill and cannot be present for the hearing. He decides to record the evidence and present it to the court. Under which rule should he present such evidence?

A. Rule 1003: Admissibility of Duplicates

B. Limited admissibility

C. Locard's Principle

D. Hearsay

E. Federal Rule of Evidence 804: Hearsay Exceptions; Declarant Unavailable as a Witness

ANSWER: E

Explanation:

Federal Rule of Evidence 804: Hearsay Exceptions; Declarant Unavailable as a Witness is the applicable rule because a witness whose physical illness prevents attendance or testimony is considered unavailable. Rule 804(a)(4) specifically recognizes unavailability where a declarant cannot be present or testify because of death or a current physical or mental illness or infirmity. A recorded statement may then be offered only if it satisfies one of Rule 804's applicable hearsay exceptions. In the common situation where the recording preserves testimony given under oath at an earlier hearing or deposition, Rule 804(b)(1) permits former testimony when the opposing party had an opportunity and similar motive to cross-examine the witness. The recording should be reliably preserved, authenticated, and accompanied by sufficient information establishing the witness's illness and the applicable exception. This approach protects the evidentiary value of testimony that would otherwise be lost because the witness cannot attend, while retaining the safeguards required for evidence offered at trial. See Federal Rule of Evidence 804 and the Federal Rules of Evidence.

QUESTION NO: 38

Shane, a forensic specialist, is investigating an ongoing attack on a MySQL database server hosted on a Windows machine with SID "WIN-ABCDE12345F." Which of the following log file will help Shane in tracking all the client connections and activities performed on the database server?

A. WIN-ABCDE12345F.err

B. WIN-ABCDE12345F-bin.n

C. WIN-ABCDE12345F.pid

D. WIN-ABCDE12345F.log

ANSWER: D

Explanation:

WIN-ABCDE12345F.log is the appropriate file because it corresponds to the MySQL general query log when the server hostname is WIN-ABCDE12345F. The general query log records each client connection and disconnection, along with statements received from clients. This makes it especially valuable during an active database-server investigation: a forensic specialist can reconstruct connection activity, identify source hosts and authenticated accounts where recorded, establish a timeline, and review SQL operations issued during suspicious sessions. MySQL documents that the general query log is a

general record of what the server is doing and logs client connect and disconnect events as well as received SQL statements. The log must be enabled through the `general_log` system variable, and its filename is controlled by `general_log_file`; when a hostname-based filename is used, the `.log` extension is consistent with the general log's conventional naming. Investigators should securely preserve this file promptly because it can provide volatile, high-value evidence of ongoing activity. See the MySQL General Query Log documentation and the general_log_file system-variable reference.

QUESTION NO: 39

Which of the following are volatile data that should normally be considered for collection during a live forensic response? (Choose three.)

A. Contents of RAM

B. Active network connections

C. Running processes

D. Deleted files in unallocated space

E. Windows Registry hives stored on disk

ANSWER: A B C

Explanation:

Contents of RAM, active network connections, and running processes are volatile evidence because they can change or disappear when the system state changes, processes terminate, or the computer is powered off. Memory can contain encryption keys, injected code, credentials, and process artifacts. Network-connection information can identify current remote communications, while a process list can reveal executing programs and associated process identifiers. Deleted files and the Windows Registry are generally persistent artifacts stored on media, although they can of course be modified over time. NIST describes volatile data collection as an important consideration when performing incident response and forensic analysis; see NIST SP 800-86.

QUESTION NO: 40

What type of attack occurs when an attacker can force a router to stop forwarding packets by flooding the router with many open connections simultaneously so that all the hosts behind the router are effectively disabled?

A. digital attack

B. denial of service

C. physical attack

D. ARP redirect

ANSWER: B

Explanation:

denial of service is correct because the described activity exhausts a router's finite connection-tracking, memory, processing, or session-table resources. By creating a large number of simultaneous open connections, the attacker prevents the router from reliably processing and forwarding legitimate traffic. Consequently, systems on the network behind that router lose access to external resources even though they may remain operational themselves. This is the defining operational effect of a denial-of-service attack: reducing or eliminating the availability of a service or network resource for legitimate users. In this case, the targeted resource is the router's packet-forwarding capability and/or its ability to maintain active connection state. A SYN-flood-style event can produce this result when a stateful device allocates resources for many incomplete connection attempts. The U.S. Cybersecurity and Infrastructure Security Agency describes denial-of-service attacks as actions intended to make a machine or network resource unavailable by overwhelming it with traffic or requests.

NIST likewise identifies resource exhaustion as a key denial-of-service condition. See CISA's denial-of-service attack guidance and NIST's definition of denial of service.

QUESTION NO: 41

Steven has been given the task of designing a computer forensics lab for the company he works for. He has found documentation on all aspects of how to design a lab except the number of exits needed. How many exits should Steven include in his design for the computer forensics lab?

A. Three

B. One

C. Two

D. Four

ANSWER: B

Explanation:

One is the correct answer in the context of a computer-forensics laboratory's physical-security design. A single controlled entrance/exit creates a defined boundary for the lab and provides one point at which access can be authenticated, logged, monitored, and restricted to authorized personnel. This supports evidence integrity and chain-of-custody requirements by reducing opportunities for unrecorded removal, introduction, or handling of digital evidence. The entry point should normally be protected through measures such as access control, visitor logging, surveillance, and procedures governing evidence movement. NIST's guidance for integrating forensic techniques emphasizes preserving evidence and maintaining documentation that supports its integrity throughout handling and examination; a controlled laboratory boundary directly supports those objectives. See NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response. In a real facility, the single controlled routine exit must be designed alongside applicable fire, building, and occupational-safety requirements. Required emergency egress provisions must never be obstructed or disabled; they can be alarmed and monitored while remaining available for life safety. OSHA's overview of exit-route requirements is available at OSHA Exit Routes.

QUESTION NO: 42

Given the drive dimensions as follows and assuming a sector has 512 bytes, what is the capacity of the described hard drive?

22,164 cylinders/disk

80 heads/cylinder

63 sectors/track

A. 53.26 GB

B. 57.19 GB

C. 11.17 GB

D. 10 GB

ANSWER: A

Explanation:

53.26 GB is correct under the binary capacity convention commonly used in forensic and operating-system contexts, where "GB" is often used informally for gibibytes. First calculate the number of addressable sectors: 22,164 cylinders × 80 heads per cylinder × 63 sectors per track = 111,706,560 sectors. Multiplying by 512 bytes per sector gives a total raw capacity of 57,193,758,720 bytes. Dividing this byte total by $1,024^3$ (1,073,741,824 bytes) produces approximately 53.26 GiB, which is

the value represented by 53.26 GB in the answer set. Geometry values such as cylinders, heads, and sectors describe the logical CHS layout used for addressing sectors, and the sector size converts that sector count into a byte capacity. In forensic examinations, clearly recording both the exact byte count and the unit convention is important because storage vendors commonly use decimal gigabytes, while many tools and operating systems display binary-based values. The National Institute of Standards and Technology defines the binary prefix “gibi” as 2^{30} bytes: NIST binary prefixes. For general storage-capacity terminology and decimal-prefix usage, see NIST SI prefixes.

QUESTION NO: 43

Which of the following information should be documented when collecting digital evidence at an incident scene? (Choose three.)

A. Date and time of collection

B. Identity of the person collecting the evidence

C. Description or serial number of the item

D. Personal opinions about the suspect

E. Unverified passwords in the case report

ANSWER: A B C

Explanation:

Date and time of collection, **the identity of the person collecting the evidence**, and **a description or serial number of the item** are correct. These details identify the item, establish when it entered evidence control, and identify the person responsible for the collection event. They form part of a defensible chain-of-custody record.

The documentation should also record transfers, storage locations, acquisition methods, hash values where applicable, and relevant device condition. An investigator should never record passwords in a report merely because they are convenient; sensitive credentials must be handled under authorized procedures and protected appropriately. NIST discusses documenting collection and maintaining evidence integrity in NIST SP 800-86.

QUESTION NO: 44

What is the default IIS log location?

A. SystemDrive\inetpub\LogFiles

B. %SystemDrive%\inetpub\logs\LogFiles

C. %SystemDrive\logs\LogFiles

D. SystemDrive\logs\LogFiles

ANSWER: B

Explanation:

The default IIS logging directory is **%SystemDrive%\inetpub\logs\LogFiles**. `%SystemDrive%` is an environment variable that normally resolves to the Windows system volume, typically `C:`; therefore, a standard installation usually stores IIS logs under `C:\inetpub\logs\LogFiles`. IIS creates site-specific subdirectories beneath this path, commonly named in the form `W3SVC<site-ID>`, so that log records for individual websites can be separated. These logs are especially important in forensic work because they can record request time, client IP address, requested URI, HTTP status, user-agent, referrer, and other fields selected in the IIS logging configuration. The configured location can be changed at the server or site level in IIS Manager, but the question asks for the default installation location. Microsoft documents the default log-file directory as `%SystemDrive%\inetpub\logs\LogFiles` and describes the site-specific folders stored below it. See Microsoft IIS logging configuration documentation and Microsoft logFile configuration reference.

QUESTION NO: 45

The following excerpt is taken from a honeypot log. The log captures activities across three days.

There are several intrusion attempts; however, a few are successful.

(Note: The objective of this question is to test whether the student can read basic information from log entries and interpret the nature of attack.)

Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169

Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482

Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53

Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21

Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53

Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53

Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53

Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111

Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 -> 172.16.1.107:80

Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53

Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53

Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by (uid=0)

Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by simple(uid=506) Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080

Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.28.22.189:4558

From the options given below choose the one which best interprets the following entry: Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53

A. An IDS evasion technique

B. A buffer overflow attempt

C. A DNS zone transfer

D. Data being retrieved from 63.226.81.13

ANSWER: B

Explanation:

A buffer overflow attempt is the best interpretation because the `nops-x86` alert identifies a sequence of x86 no-operation instructions, commonly called a NOP sled. Attack payloads have historically used a NOP sled before injected shellcode to increase the likelihood that an overwritten instruction pointer lands in executable payload data. Instead of requiring control flow to jump to one exact byte, execution can land anywhere within the sled and proceed forward into the shellcode. This makes NOP patterns a well-known indicator of attempted code injection associated with memory-corruption and buffer-overflow exploitation. The source address, source port, target address, and target port identify the observed network flow, while the alert name supplies the principal forensic interpretation of the payload. In an investigation, this entry should therefore be treated as evidence that the sender transmitted content matching a common buffer-overflow exploit pattern and should prompt preservation of the related packet capture, service logs, and host-memory evidence. OWASP describes buffer overflows as memory-safety failures that can enable code execution, and MITRE's CWE entry details the underlying out-of-bounds write weakness: OWASP Buffer Overflow and CWE-120: Buffer Copy without Checking Size of Input.