PassQueen
a.k.a dumpsqueen.com

# Computer Hacking Forensic Investigator (CHFI-v10)

## ECCouncil 312-49v10

**Version Demo**

**Total Demo Questions: 78**

**Total Premium Questions: 784**

**Buy Premium PDF**

https://passqueen.com

support@passqueen.com

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, Computer Forensics in Today's World | 106 |
| Topic 2, Computer Forensics Investigation Process | 64 |
| Topic 3, Understanding Hard Disks and File Systems | 83 |
| Topic 4, Data Acquisition and Duplication | 57 |
| Topic 5, Defeating Anti-Forensics Techniques | 29 |
| Topic 6, Windows Forensics | 114 |
| Topic 7, Linux and Mac Forensics | 28 |
| Topic 8, Network Forensics | 103 |
| Topic 9, Investigating Web Application Attacks | 51 |
| Topic 10, Dark Web Forensics | 3 |
| Topic 11, Database Forensics | 14 |
| Topic 12, Cloud Forensics | 16 |
| Topic 13, Investigating Email Crimes | 37 |
| Topic 14, Malware Forensics | 28 |
| Topic 15, Mobile Forensics | 28 |
| Topic 16, Mix Questions | 23 |
| Total | 784 |

QUESTION NO: 1

In a forensic examination of hard drives for digital evidence, what type of user is most likely to have the most file slack to analyze?

**A.** one who has NTFS 4 or 5 partitions

**B.** one who uses dynamic swap file capability

**C.** one who uses hard disk writes on IRQ 13 and 21

**D.** one who has large allocation units (clusters)

**ANSWER: D**

**Explanation:**

The correct answer is *one who has large allocation units (clusters)*. File slack is unused space in the final allocated cluster of a file. File systems allocate disk space in whole clusters rather than allocating only the exact number of bytes that a file requires. When a file does not completely fill its final cluster, the remaining bytes are slack space. Consequently, larger cluster sizes produce a greater potential amount of unused space at the end of each stored file. A user whose volume uses large allocation units is therefore more likely to have more file slack available for forensic examination.

This matters because slack space can retain residual bytes from prior memory buffers or previous file content, potentially providing artifacts relevant to an investigation. The amount of slack is not fixed for every file: it depends on the file's length relative to the cluster boundary, but the maximum possible slack grows as the allocation-unit size grows. Microsoft documents that allocation-unit size is the cluster size used by a file system, while NIST identifies slack space as a potential source of residual digital evidence during forensic analysis. See Microsoft Disk Management documentation and NIST SP 800-86.

**QUESTION NO: 2**

Jack Smith is a forensics investigator who works for Mason Computer Investigation Services. He is investigating a computer that was infected by Ramen Virus.


He runs the netstat command on the machine to see its current connections. In the following screenshot, what do the 0.0.0.0 IP addresses signify?

**A.** Those connections are established

**B.** Those connections are in listening mode

**C.** Those connections are in closed/waiting mode

**D.** Those connections are in timed out/waiting mode

**ANSWER: B**

**Explanation:**

Those connections are in listening mode. In Windows `netstat` output, an entry using `0.0.0.0` as its local address means the socket is bound to the IPv4 wildcard address rather than to one specific local interface. In practical terms, the service will accept inbound connections addressed to any IPv4 address assigned to the computer, provided that network filtering and firewall policy permit them. When this wildcard local address appears with the TCP state `LISTENING`, it identifies a process that is waiting for a remote host to initiate a connection on the listed port; it is not evidence of an already-established session. This is particularly relevant during a forensic examination because open listening ports can identify services exposed by the host and may help an investigator correlate suspicious processes, ports, and malware behavior. Microsoft documents that `netstat` displays active TCP connections, listening ports, and related connection information. The IPv4 special-address registry also identifies `0.0.0.0/8` as the "this host on this network" block; socket implementations use the unspecified/wildcard address to represent binding across available local interfaces. See Microsoft's netstat command documentation and the IANA IPv4 Special-Purpose Address Registry.

## QUESTION NO: 3

Sheila is a forensics trainee and is searching for hidden image files on a hard disk. She used a forensic investigation tool to view the media in hexadecimal code for simplifying the search process. Which of the following hex codes should she look for to identify image files?

**A.** ff d8 ff

**B.** 25 50 44 46

**C.** d0 0f 11 e0

**D.** 50 41 03 04

## ANSWER: A

**Explanation:**

**ff d8 ff** is the correct signature to look for because it is the standard leading byte sequence, or file signature, for a JPEG image. JPEG files begin with the Start of Image marker `FF D8`; this is normally followed by another `FF` byte that introduces a JPEG marker, commonly producing the recognizable `FF D8 FF` sequence at the beginning of the file. In a forensic examination, analysts use these signatures to identify or carve files whose extensions, directory entries, or metadata may be absent, misleading, or intentionally altered. Searching raw disk data for this header can locate candidate JPEG files in unallocated space or within areas where files have been concealed. The examiner should then validate a candidate by checking its JPEG structure and, where available, its end marker (`FF D9`), rather than relying on a header match alone. The JPEG standard defines the Start of Image marker and the marker-based structure used by JPEG-coded image data. See the ITU-T T.81 JPEG specification and the Library of Congress JPEG format description.

## QUESTION NO: 4

During forensic acquisition of a powered-on computer, which of the following actions help preserve volatile evidence? (Choose three.)

**A.** Capture physical memory

**B.** Record active network connections

**C.** Document running processes

**D.** Defragment the suspect drive

**E.** Install operating-system updates

## ANSWER: A B C

**Explanation:**

Capturing **physical memory**, recording **active network connections**, and documenting **running processes** help preserve volatile evidence. These data can change rapidly when processes terminate, network sessions close, the system is powered off, or normal system activity overwrites memory. Physical memory may contain encryption keys, active malware components, command history, credentials, and network-session information that may not exist on persistent storage.

The examiner should use authorized, validated tools where possible, document each command and action, record system time, and minimize unnecessary interaction with the live system. Pulling the power cable before collecting volatile data may destroy information needed to establish the incident timeline. NIST discusses volatile-data collection and order-of-volatility considerations in SP 800-86.

## QUESTION NO: 5

Madison is on trial for allegedly breaking into her university's internal network. The police raided her dorm room and seized all of her computer equipment. Madison's lawyer is trying to convince the judge that the seizure was unfounded and baseless. Under which US Amendment is Madison's lawyer trying to prove the police violated?

**A.** The 4th Amendment

**B.** The 1st Amendment

**C.** The 10th Amendment

**D.** The 5th Amendment

## ANSWER: A

**Explanation:**

The 4th Amendment is correct because it protects people against unreasonable searches and seizures by the government. A police entry into Madison's dorm room and the taking of her computer equipment constitute a search and seizure under Fourth Amendment principles. Her lawyer's argument that the seizure was "unfounded and baseless" challenges whether law enforcement had a legally sufficient basis, such as a valid warrant supported by probable cause or a recognized exception to the warrant requirement. In a digital-forensics matter, the Fourth Amendment is especially important because computers and other electronic storage devices can contain extensive personal information. A warrant for such evidence should describe with particularity the place to be searched and the items or categories of data to be seized, helping limit an overly broad forensic acquisition. If a court finds that officers conducted an unreasonable search or seizure, evidence obtained through that constitutional violation may be subject to exclusion from the criminal case. The text and historical purpose of this protection are set out in the Fourth Amendment, Constitution Annotated. The Supreme Court has also recognized the substantial privacy interests implicated by searches of digital devices, as discussed in Riley v. California.

## QUESTION NO: 6

Recently, an Internal web app that a government agency utilizes has become unresponsive, Betty, a network engineer for the government agency, has been tasked to determine the cause of the web application's unresponsiveness. Betty launches Wlreshark and begins capturing the traffic on the local network. While analyzing the results, Betty noticed that a syn flood attack was underway. How did Betty know a syn flood attack was occurring?

**A.** Wireshark capture shows multiple ACK requests and SYN responses from single/multiple IP address(es)

**B.** Wireshark capture does not show anything unusual and the issue is related to the web application

**C.** Wireshark capture shows multiple SYN requests and RST responses from single/multiple IP address(es)

**D.** Wireshark capture shows multiple SYN requests and SYN-ACK responses from single/multiple IP address(es)

## ANSWER: D

**Explanation:**

Wireshark capture shows multiple SYN requests and SYN-ACK responses from single/multiple IP address(es) because a SYN flood abuses the TCP connection-establishment process. In a normal TCP three-way handshake, a client sends a SYN packet, the server replies with a SYN-ACK packet, and the client completes the connection by returning an ACK. An attacker conducting a SYN flood sends a very large number of SYN requests, often using spoofed source addresses. The target replies to each request with a SYN-ACK and allocates state for a half-open connection, but the expected final ACK generally never arrives. As these incomplete handshakes accumulate, the server's backlog or other connection resources can be exhausted, leaving the web application slow or unreachable for legitimate users. In a packet capture, the relevant signature is therefore repeated inbound SYNs followed by outbound SYN-ACKs, accompanied by an absence of handshake completion for many of those attempts. TCP's specified handshake behavior is described in RFC 9293. The resource-exhaustion mechanism and half-open connection pattern associated with SYN flooding are also summarized by Cloudflare's SYN flood overview.

## QUESTION NO: 7

Identify the file system that uses $BitMap file to keep track of all used and unused clusters on a volume.

**A.** NTFS

**B.** FAT

**C.** EXT

**D.** FAT32

## ANSWER: A

**Explanation:**

NTFS is correct because it stores volume allocation information in the `$Bitmap` metadata file, one of the special files maintained in the NTFS Master File Table. The bitmap contains a bit for each cluster on the volume: the bit's state records whether that cluster is allocated or available. This enables NTFS to identify free space efficiently when creating or extending files and to manage allocation without relying on the linked allocation-table approach used by older FAT-based volumes.

In forensic work, understanding `$Bitmap` is particularly valuable because it helps establish whether clusters associated with file content are presently allocated or unallocated. Investigators can correlate bitmap allocation status with file-record metadata and recovered data to assess whether content may belong to deleted files, active files, or residual data in unallocated space. Microsoft's NTFS technical documentation identifies `$Bitmap` as the file that tracks allocated and unallocated clusters on an NTFS volume. See the Microsoft Master File Table documentation and the NTFS $Bitmap file reference.

## QUESTION NO: 8

Which of the following information should be documented in the chain of custody for a seized digital device? (Choose three.)

**A.** Name of the person releasing and receiving the evidence

**B.** Date and time of each transfer

**C.** Purpose of the transfer

**D.** Investigator's opinion of the suspect's guilt

**E.** Personal social-media account of the custodian

## ANSWER: A B C

**Explanation:**

A chain of custody documents the handling of evidence from collection through final disposition. It should identify the person who collected or transferred the evidence, record the date and time of each custody event, and describe the reason or

purpose for the transfer. The evidence item should also be uniquely identified so that the examiner can demonstrate that the item analyzed is the same item originally seized.

Proper documentation supports authenticity, accountability, and admissibility by showing who possessed the evidence and how it was controlled. A chain of custody does not require the investigator to record an unverified conclusion about the suspect's guilt. NIST recommends documenting evidence collection and handling activities to preserve evidentiary integrity. See NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response.

## QUESTION NO: 9

Which of the following is NOT a physical evidence?

**A.** Removable media

**B.** Cables

**C.** Image file on a hard disk

**D.** Publications

## ANSWER: C

**Explanation:**

An image file on a hard disk is not physical evidence because it is digital data: a logical collection of bits representing the contents of a storage medium or a forensic acquisition. Although the hard disk that stores the file is a tangible physical item that may be seized, labeled, preserved, and examined, the image file itself is an intangible evidentiary artifact. Investigators acquire and validate such files using forensic processes, including cryptographic hash values, to demonstrate that the data remains unchanged from acquisition through examination. This distinction is important in CHFI practice because the handling of the physical device and the preservation, verification, and analysis of its digital contents are related but separate evidence-handling activities. NIST describes digital evidence as information of probative value that is stored or transmitted in binary form and provides guidance for integrating forensic techniques into incident-response processes. Its guidance also emphasizes preserving data integrity during collection and examination. See NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response and NIST guidance on computer-security information and records.

## QUESTION NO: 10

An investigator is reviewing packet captures for indicators of a TCP SYN scan. Which of the following observations are consistent with this type of scan? (Choose three.)

**A.** SYN packets are sent to multiple destination ports

**B.** SYN/ACK responses identify open ports

**C.** RST packets are sent instead of completing the handshake

**D.** A full TCP session is established with every scanned port

**E.** Only UDP datagrams are used for the scan

## ANSWER: A B C

**Explanation:**

A TCP SYN scan typically sends **SYN packets to multiple destination ports**, receives **SYN/ACK responses from open ports**, and generally sends an **RST packet instead of completing the TCP three-way handshake**. The scanner uses the SYN/ACK response to identify a listening service, then resets the connection rather than transmitting the final ACK that would establish a full session. Closed ports commonly return RST responses.

In packet analysis, investigators should consider the timing, source address, destination-port sequence, and response behavior to distinguish scanning from ordinary client traffic. Nmap documents SYN scanning behavior in its TCP SYN scan reference.

## QUESTION NO: 11

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 when capacity is expressed using the binary convention commonly used in disk-geometry and forensic calculations. First, calculate the total number of addressable sectors: 22,164 cylinders × 80 heads per cylinder × 63 sectors per track = 111,706,560 sectors. Each sector stores 512 bytes, so the total capacity is 111,706,560 × 512 = 57,193,758,720 bytes. Converting this byte count to binary gigabytes requires dividing by $1{,}024^3$ (1,073,741,824): 57,193,758,720 ÷ 1,073,741,824 = approximately 53.26. Thus, the drive capacity is 53.26 GB under the binary-unit convention; more precisely, this unit is now commonly called a gibibyte (GiB). Accurate geometry calculations are important in forensic work because they help validate media size, determine addressable locations, and support reliable sector-to-offset calculations. The International Electrotechnical Commission defines the binary prefix “gibi” as $2^{30}$ bytes in its binary-prefix guidance. Microsoft also documents that disk sectors are conventionally addressed in 512-byte units in its disk-partition documentation.

## QUESTION NO: 12

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 in the context of this exam question: internal penetration testing models the risk posed by an authorized user, a compromised employee account, or another actor who already has a foothold within the environment. This perspective is important because internal access can expose weaknesses that perimeter-focused testing may not reveal, such as excessive privileges, weak network segmentation, unrestricted lateral movement, and insufficient monitoring of sensitive resources. The stated percentage should be understood as a traditional training-oriented statistic rather than a universal measurement; the precise proportion of insider-related incidents changes by industry, organization, and study methodology. The key security principle remains sound: organizations need to assess controls against threats that originate after access has been obtained. NIST describes insider threat as the potential for an individual with authorized access to use that access in a way that harms an organization, reinforcing the value of evaluating internal exposure. CISA likewise identifies malicious and unintentional insider activity as a

significant organizational risk. An authorized internal test provides evidence of how effectively access controls, least privilege, logging, and segmentation contain that risk. See NIST's Insider Threat definition and CISA's Insider Threat Mitigation guidance.

## QUESTION NO: 13

Select the tool appropriate for examining the dynamically linked libraries of an application or malware.

**A.** DependencyWalker

**B.** SysAnalyzer

**C.** PEiD

**D.** ResourcesExtract

## ANSWER: A

**Explanation:**

DependencyWalker is the appropriate tool because it is designed to inspect a Windows executable's module dependencies, including the dynamically linked libraries it imports and the functions resolved from those libraries. In forensic malware examination, this provides useful static-triage information about the program's expected runtime components and capabilities. An investigator can open an executable in Dependency Walker to view its dependency tree, imported and exported functions, delay-loaded modules, and potential missing or unresolved dependencies. These details help establish how an application is constructed and which Windows APIs or third-party libraries it is intended to use, without needing to execute the suspicious file. Dependency Walker supports common Windows executable formats, including portable executable files, and presents the dependent-module relationship in a form that is useful when documenting artifacts during analysis. Its profiling capability can also observe module loading behavior for a controlled analysis environment, although static dependency inspection is the core reason it fits this task. The tool's documentation describes its purpose as scanning Windows modules for dependencies and displaying the functions imported and exported by those modules. See Dependency Walker and Microsoft's Dynamic-Link Libraries documentation.

## QUESTION NO: 14

When performing a forensics analysis, what device is used to prevent the system from recording data on an evidence disk?

**A.** a write-blocker

**B.** a protocol analyzer

**C.** a firewall

**D.** a disk editor

## ANSWER: A

**Explanation:**

A write-blocker is the appropriate device because it allows a forensic examiner to read data from an evidence disk while preventing any write commands from reaching that disk. This protection is essential to forensic soundness: connecting storage media to a computer can otherwise cause the operating system, applications, or automated processes to alter metadata, create logs, update timestamps, or write other data. A hardware write-blocker sits between the examiner's forensic workstation and the evidence drive and enforces read-only access at the interface level. Examiners can therefore acquire a forensic image and examine the source media without changing the original evidence. This helps preserve the integrity and repeatability of the examination and supports a defensible chain of custody. The U.S. National Institute of Standards and Technology describes write-blocking as preventing writes to protected media while permitting reads, and its testing program publishes requirements and test results for forensic write-blocking tools. See NIST Computer Forensics Tool Testing Program and NIST Digital Data Acquisition Tool Specification.

## QUESTION NO: 15

A small law firm located in the Midwest has possibly been breached by a computer hacker looking to obtain information on their clientele. The law firm does not have any on-site IT employees, but wants to search for evidence of the breach themselves to prevent any possible media attention. Why would this not be recommended?

**A.** Searching for evidence themselves would not have any ill effects

**B.** Searching could possibly crash the machine or device

**C.** Searching creates cache files, which would hinder the investigation

**D.** Searching can change date/time stamps

## ANSWER: D

**Explanation:**

Searching can change date/time stamps is correct because interacting with a potentially compromised system can alter the very digital evidence needed to establish what happened. Opening files, browsing folders, launching applications, logging in, or running search tools may update file-system metadata such as access times, create new operating-system artifacts, and modify logs. These changes can obscure the original sequence of events and make later forensic interpretation less reliable. A qualified incident-response or forensic professional should preserve the evidence first, document each action, and use controlled collection methods that minimize changes to the original system. This approach also supports evidence integrity and a defensible chain of custody, which are especially important when the incident may involve confidential client information, legal obligations, or later litigation. NIST guidance emphasizes preserving volatile and nonvolatile data appropriately and documenting evidence handling throughout incident response and forensic collection. See NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response and NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide.

## QUESTION NO: 16

Wireless access control attacks aim to penetrate a network by evading WLAN access control measures such as AP MAC filters and Wi-Fi port access controls. Which of the following wireless access control attacks allow the attacker to set up a rogue access point outside the corporate perimeter and then lure the employees of the organization to connect to it?

**A.** Ad hoc associations

**B.** Client mis-association

**C.** MAC spoofing

**D.** Rogue access points

## ANSWER: B

**Explanation:**

**Client mis-association** is correct because it describes an attack in which a wireless client is induced to associate with an attacker-controlled access point rather than the organization's authorized WLAN. The attacker can place the fraudulent access point outside the physical corporate boundary, advertise a convincing network name, and use a sufficiently attractive signal to entice employee devices to connect. Once a client associates, the attacker may observe or manipulate traffic, present credential-harvesting portals, or use the connection as a path for further attacks against the user or enterprise resources.

This risk exists because wireless clients can make association decisions based on remembered SSIDs, signal availability, and user interaction; a device may not reliably distinguish an authorized AP from a malicious one merely because both advertise a familiar network identity. Strong enterprise WLAN configurations reduce this exposure through mutual authentication, certificate validation, protected management practices, and monitoring for unauthorized wireless infrastructure. NIST discusses the security implications of WLAN client and access-point associations in SP 800-153, Guidelines for Securing Wireless Local Area Networks. Additional practical guidance on recognizing and managing unauthorized wireless devices is available from CISA.

## QUESTION NO: 17

Which of the following setups should a tester choose to analyze malware behavior?

**A.** A virtual system with internet connection

**B.** A normal system without internet connect

**C.** A normal system with internet connection

**D.** A virtual system with network simulation for internet connection

## ANSWER: D

**Explanation:**

A virtual system with network simulation for internet connection is the appropriate setup because it provides a controlled, repeatable malware-analysis environment while preserving the network conditions that many samples require to reveal their behavior. Malware frequently attempts domain lookups, contacts command-and-control infrastructure, downloads additional content, sends host information, or checks whether it has network access. Simulated Internet services allow the analyst to observe and record these requests without permitting unrestricted communication with real external systems.

Virtualization also supports safe experimentation through isolation, snapshots, and rapid restoration to a known-clean state. Before executing a sample, an analyst can snapshot the virtual machine; after collecting artifacts such as processes, file-system changes, registry changes, and network traffic, the machine can be reverted. A network simulator can emulate services such as DNS, HTTP, HTTPS, FTP, and SMTP, return analyst-controlled responses, and capture connection attempts for later forensic review. This approach therefore enables dynamic behavioral analysis while minimizing the risk of exposing production systems or external parties to the specimen. The Cuckoo Sandbox documentation describes isolated virtual-machine analysis and network routing considerations, while INetSim documents Internet-service simulation for malware analysis. See Cuckoo Sandbox documentation and INetSim documentation.

## QUESTION NO: 18

When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

**A.** Passive IDS

**B.** Active IDS

**C.** Progressive IDS

**D.** NIPS

## ANSWER: B

**Explanation:**

**Active IDS** is correct because it does more than observe and report suspicious activity: it can initiate a response when it detects behavior matching an attack signature, policy violation, or anomalous pattern. A vulnerability scan commonly creates a large volume of connection attempts and probe traffic, which can trigger an intrusion-detection rule. In this scenario, the defining evidence is that the system *cuts off the connection*. This is an active response, such as terminating the session, resetting a TCP connection, or dynamically applying a blocking rule against the scanning host. Active IDS capabilities are intended to provide immediate protective action in addition to detection and alerting, thereby limiting continued access or further probing after suspicious activity is identified. NIST describes intrusion prevention capabilities as those that can attempt to stop detected malicious activity, including terminating connections and blocking traffic. This distinction is central to interpreting the observed scan result: the connection loss demonstrates that an automated response mechanism was invoked rather than merely recording or notifying on the event. See NIST's Guide to Intrusion Detection and Prevention Systems (IDPS) and the MITRE ATT&CK Network Service Scanning technique for background on detection and defensive responses to scanning activity.

## QUESTION NO: 19

Event correlation is the process of finding relevance between the events that produce a final result. What type of correlation will help an organization to correlate events across a set of servers, systems, routers and network?

**A.** Same-platform correlation

**B.** Network-platform correlation

**C.** Cross-platform correlation

**D.** Multiple-platform correlation

## ANSWER: C

**Explanation:**

Cross-platform correlation is correct because it combines and analyzes events collected from disparate technologies, operating systems, devices, and applications. An organization's infrastructure commonly includes servers running different operating systems, network routers and switches, security appliances, endpoints, and business applications. Each source can record a different part of the same activity, often using different log formats, timestamps, event identifiers, and terminology. Cross-platform correlation normalizes or relates these records so an investigator or security team can identify the larger sequence of activity and establish relevance between otherwise separate events.

For example, a correlated investigation may connect an authentication event on a server, a connection record from a router or firewall, and an endpoint alert into one timeline. This broader visibility is particularly important in forensic investigations because it helps reconstruct actions across system and network boundaries, rather than considering each device's evidence in isolation. Centralized log collection and correlation are also consistent with log-management guidance that emphasizes integrating logs from multiple sources to support monitoring, incident response, and investigation. See EC-Council's CHFI certification overview and NIST's Guide to Computer Security Log Management.

## QUESTION NO: 20

Matthew has been assigned the task of analyzing a suspicious MS Office document via static analysis over an Ubuntu-based forensic machine. He wants to see what type of document It Is. whether It Is encrypted, or contains any flash objects/VBA macros. Which of the following python-based script should he run to get relevant information?

**A.** oleform.py

**B.** oleid.py

**C.** oledir.py

**D.** pdfid.py

## ANSWER: B

**Explanation:**

`oleid.py` is the appropriate initial static-triage script from the oletools suite for a suspicious Microsoft Office document. It identifies the file format and assesses whether the file is an OLE compound document, an Office Open XML file, RTF, or another supported format. It also reports indicators directly relevant to forensic examination, including whether the document is encrypted, whether it contains VBA macros, whether macros are flagged as suspicious, and whether embedded Flash objects are present. This gives an examiner a quick, non-executing overview of potentially malicious document features before performing more focused extraction or code analysis. In an Ubuntu forensic environment, oletools can be installed and run through Python, making `oleid.py` suitable for the stated workflow. The oletools documentation describes oleid as a tool intended to detect common indicators in Office documents, including encryption, VBA macros, and Flash content. See the oleid documentation and the oletools project repository for usage and supported detection features.

## QUESTION NO: 21

Which of the following are characteristics of a properly maintained forensic chain of custody? (Choose three.)

**A.** Each transfer of evidence

**B.** Identity of each person handling the evidence

**C.** Date and time of each transfer

**D.** Personal opinions regarding the suspect

**E.** Predicted outcome of the court case

**ANSWER: A B C**

**Explanation:**

A properly maintained chain of custody documents **each transfer of evidence**, **the identity of each person handling the evidence**, and **the date and time of each transfer**. These details establish an accountable history showing who possessed the evidence, when control changed, and how the item was handled from collection through presentation. The record should also identify the evidence item uniquely and note its condition, storage location, and relevant actions performed.

A chain of custody is not a technical analysis report and does not establish guilt or innocence. Its purpose is to support authenticity and demonstrate that the offered evidence is the same item collected during the investigation and has been safeguarded against unauthorized alteration. NIST discusses the importance of documenting evidence handling and preservation in SP 800-86, Guide to Integrating Forensic Techniques into Incident Response.

## QUESTION NO: 22

Amelia has got an email from a well-reputed company stating in the subject line that she has won a prize money, whereas the email body says that she has to pay a certain amount for being eligible for the contest. Which of the following acts does the email breach?

**A.** CAN-SPAM Act

**B.** HIPAA

**C.** GLBA

**D.** SOX

**ANSWER: A**

**Explanation:**

**CAN-SPAM Act** is correct because it establishes rules for commercial email messages and prohibits deceptive header information and deceptive subject lines. A subject line claiming that the recipient has “won a prize” creates a misleading impression when the message actually conditions eligibility on paying money. The subject line must accurately reflect the content of the email rather than conceal a solicitation, fee, or other material condition. The Act is enforced by the U.S. Federal Trade Commission and is intended to make commercial email more transparent, identifiable, and controllable for recipients. In addition to truthful routing and subject-line information, compliant commercial email generally must provide a valid physical postal address, clearly identify an advertisement where required, and include a functional opt-out mechanism that is honored promptly. The misleading prize representation is therefore the relevant conduct governed by the CAN-SPAM framework. The FTC’s CAN-SPAM compliance guidance explains that commercial email must not use deceptive subject lines and that the subject line must accurately reflect the message’s content: FTC: CAN-SPAM Act Compliance Guide for Business. The statutory prohibition on deceptive subject headings appears at 15 U.S.C. § 7704.

## QUESTION NO: 23

A forensic investigator is examining Windows Prefetch files from an acquired system. Which of the following information can commonly be obtained from Prefetch artifacts? (Choose three.)

**A.** Name of the executed executable

**B.** Program execution timestamps

**C.** Program run count

**D.** Complete contents of documents opened by the program

**E.** BitLocker recovery password

**ANSWER: A B C**

**Explanation:**

Windows Prefetch artifacts can provide valuable evidence of program execution. A Prefetch file is associated with an executable and can identify the executable name, retain execution-time information, and record a run count on supported Windows versions. It can also contain references to files and directories accessed during the application startup process. This information helps an investigator determine whether a program was likely executed and correlate that activity with other artifacts such as Registry entries, event logs, shortcut files, and file-system timestamps.

Prefetch files do not normally preserve the complete contents of documents that were opened by an application. Microsoft describes Prefetch as a performance feature that records information used to optimize application startup. See Microsoft documentation on Prefetch files.

## QUESTION NO: 24

While looking through the IIS log file of a web server, you find the following entries:

```
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index.asp
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /login.asp?username=if ((select user)='sa' OR (select user)='dbo')
select 1 else select 1/0
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Developments/index_02.jpg
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index_04.jpg
```

What is evident from this log file?

**A.** Web bugs

**B.** Cross site scripting

**C.** Hidden fields

**D.** SQL injection is possible

**ANSWER: D**

**Explanation:**

**SQL injection is possible** is the correct finding when IIS log entries show request parameters containing SQL-like syntax or characters intended to alter a database query, such as quotation marks, comment markers, Boolean conditions, SQL keywords, or UNION-style query construction. IIS logs record the requested URI, query string, HTTP method, status, and related request details, so they are valuable forensic evidence of attempts to pass database-control syntax through application input fields. Such input may be incorporated into an application's backend SQL statement if the application does not use parameterized queries and proper server-side validation.

From a forensic perspective, these entries should be preserved with their timestamps and correlated with web-application logs, database audit logs, affected account activity, and server responses. The log evidence establishes that SQL injection payloads were submitted or probed; it provides an important basis for investigating whether a vulnerable application endpoint was targeted and whether the requests produced unauthorized database activity. OWASP describes SQL injection and its typical payload behavior at OWASP SQL Injection. Microsoft also documents the IIS log fields that support request-level investigation at Configure Logging in IIS.

## QUESTION NO: 25

Which among the following laws emphasizes the need for each Federal agency to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets?

**A.** FISMA

**B.** HIPAA

**C.** GLBA

**D.** SOX

## ANSWER: A

**Explanation:**

FISMA is correct because the Federal Information Security Modernization Act requires U.S. federal agencies to establish, document, and implement an agency-wide information-security program. That program must protect the information and information systems that support agency operations and assets, including systems operated by agencies themselves or by contractors and other organizations on their behalf. The requirement is risk-based: agencies must assess risk, select and implement appropriate safeguards, monitor control effectiveness, and maintain security policies and procedures. FISMA also establishes the federal governance structure for information-security oversight, assigning major responsibilities to agencies, the Office of Management and Budget, the Department of Homeland Security, and the National Institute of Standards and Technology. NIST supports FISMA implementation through standards and guidance such as its Risk Management Framework, which helps organizations categorize systems, choose controls, authorize systems, and continuously monitor security. The statutory language describing the required agency-wide program appears in 44 U.S.C. § 3554, while NIST provides practical implementation resources for federal information systems. See 44 U.S.C. § 3554 and NIST Risk Management Framework.

## QUESTION NO: 26

The objective of this act was to protect consumers' personal financial information held by financial institutions and their service providers.

**A.** Gramm-Leach-Bliley Act

**B.** Sarbanes-Oxley 2002

**C.** California SB 1386

**D.** HIPAA

## ANSWER: A

**Explanation:**

The Gramm-Leach-Bliley Act is correct because it establishes requirements for financial institutions to protect customers' nonpublic personal information. Its privacy and safeguards provisions apply to organizations that offer financial products or services, as well as to service providers that handle such information on their behalf. The Act's Safeguards Rule requires covered entities to develop, implement, and maintain an information-security program appropriate to the size and complexity of the organization, the nature of its activities, and the sensitivity of the customer information involved. This program must include administrative, technical, and physical safeguards designed to protect the security and confidentiality of customer data, guard against anticipated threats or hazards, and prevent unauthorized access or use that could cause substantial harm or inconvenience to consumers. These obligations make the Gramm-Leach-Bliley Act a central U.S. financial-privacy law and directly match the stated objective of protecting personal financial information maintained by financial institutions and their service providers. The Federal Trade Commission provides an overview of the rule and its covered institutions at https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act. The statutory text is available through the U.S. Government Publishing Office at https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf.

## QUESTION NO: 27

An investigator is examining an Internet email message to reconstruct its delivery path. Which of the following header fields can assist in this examination? (Choose three.)

**A.** Received

**B.** Message-ID

**C.** Date

**D.** Sender display name alone

**E.** Font used in the message body

## ANSWER: A B C

**Explanation:**

The **Received** header fields are added by mail transfer agents as a message passes through them and can help reconstruct the message's routing path and handling times. The **Message-ID** field provides an identifier that can be used to correlate copies of the same message across mail systems, archives, and logs. The **Date** header contains the date and time stated by the message originator's client and can provide additional timeline context, although investigators should compare it with server-generated timestamps because sender-controlled fields can be inaccurate or manipulated.

The visible display name alone is not a reliable indicator of the actual sender because it can be freely chosen by the sender and may not match the originating account or address. RFC 5322 defines Internet message header fields, including Date and Message-ID. See RFC 5322: Internet Message Format.

## QUESTION NO: 28

What does Locard's Exchange Principle state?

**A.** Any information of probative value that is either stored or transmitted in a digital form

**B.** Digital evidence must have some characteristics to be disclosed in the court of law

**C.** Anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave

**D.** Forensic investigators face many challenges during forensics investigation of a digital crime, such as extracting, preserving, and analyzing the digital evidence

## ANSWER: C

**Explanation:**

Locard’s Exchange Principle states that whenever a person or object enters or interacts with a crime scene, an exchange of material occurs: they may leave something behind and take something away. In forensic practice, this principle provides the conceptual basis for seeking trace evidence that can associate a suspect, victim, object, or location with an event. Such traces can include physical materials such as hair, fibers, soil, fingerprints, DNA, glass fragments, or tool marks. The principle is commonly summarized as “every contact leaves a trace,” although the amount and recoverability of material depend on the circumstances. For computer-hacking and digital-forensics investigations, the same investigative concept supports examination for artifacts created through interaction with systems and data, including logs, metadata, browser artifacts, file-system timestamps, and network records. The examiner must identify, preserve, and document these traces in a manner that maintains their evidentiary integrity. The National Institute of Justice describes trace evidence as material that may be transferred during contact and can help establish associations relevant to an investigation. See the National Institute of Justice overview of trace evidence and the Encyclopaedia Britannica discussion of criminalistics.

## QUESTION NO: 29

An investigator is reviewing AWS CloudTrail records after a suspected cloud-account compromise. Which of the following activity can CloudTrail help record? (Choose three.)

**A.** Management API activity

**B.** S3 object-level activity when data events are enabled

**C.** Identity and source IP information for recorded events

**D.** Complete packet payloads for all EC2 network traffic

**E.** Contents of every file stored on an EBS volume

**ANSWER: A B C**

**Explanation:**

AWS CloudTrail records activity performed through AWS APIs and provides event records that can be used to investigate account and resource activity. CloudTrail management events can show control-plane actions such as creating users, changing policies, starting instances, or modifying security groups. Data events, when configured, can record high-volume object-level actions such as Amazon S3 object access and AWS Lambda function invocation. CloudTrail events also commonly include identity, time, source IP address, requested action, and affected-resource details.

CloudTrail does not capture the full packet payload of traffic traversing an Amazon EC2 network interface. That type of network visibility requires other sources, such as VPC Flow Logs, packet capture, or network security appliance telemetry. AWS documents CloudTrail event types and their use in auditing AWS account activity at Logging management events with CloudTrail and Logging data events with CloudTrail.

**QUESTION NO: 30**

Smith is an IT technician that has been appointed to his company's network vulnerability assessment team. He is the only IT employee on the team. The other team members include employees from

Accounting, Management, Shipping, and Marketing. Smith and the team members are having their first meeting to discuss how they will proceed. What is the first step they should do to create the network

vulnerability assessment plan?

**A.** Their first step is to make a hypothesis of what their final findings will be.

**B.** Their first step is to create an initial Executive report to show the management team.

**C.** Their first step is to analyze the data they have currently gathered from the company or interviews.

**D.** Their first step is the acquisition of required documents, reviewing of security policies and compliance.

**ANSWER: D**

**Explanation:**

Their first step is the acquisition of required documents, reviewing of security policies and compliance. A vulnerability-assessment plan must begin by establishing the organization’s context, authorization, boundaries, and obligations before any technical evidence gathering or testing occurs. Relevant materials typically include network diagrams, asset inventories, data-classification standards, prior assessment records, acceptable-use policies, incident-response procedures, applicable regulations, and contractual requirements. Reviewing these documents lets the cross-functional team define the assessment scope, identify systems and business processes that are critical to Accounting, Management, Shipping, and Marketing, determine data owners, and ensure that assessment activities are authorized and do not disrupt production operations. It also provides the criteria that will later be used to evaluate findings and prioritize remediation according to business impact and compliance risk. NIST’s Technical Guide to Information Security Testing and Assessment describes planning as the phase in which the assessment team develops rules of engagement, identifies targets and constraints, and obtains the information needed to conduct the work safely and effectively. This documentary and policy review creates the foundation for later collection, analysis, reporting, and remediation activities. See NIST SP 800-115: Technical Guide to Information Security Testing and Assessment and CISA cybersecurity assessment resources.

## QUESTION NO: 31

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.** Rule 804: Hearsay Exceptions—Declarant Unavailable

## ANSWER: D

**Explanation:**

**Rule 804: Hearsay Exceptions—Declarant Unavailable** is the applicable rule because a witness who cannot attend or testify due to a then-existing physical illness is considered unavailable as a declarant. Rule 804(a)(4) specifically recognizes illness or infirmity as a basis for unavailability. When that condition is established, Rule 804(b) governs whether the witness's out-of-court evidence may be admitted despite the normal hearsay restriction. For example, former testimony may be admissible when it was given under oath in a prior hearing, trial, or lawful deposition and the opposing party had an appropriate opportunity and similar motive to develop the testimony through examination. The recording should therefore preserve admissible former testimony or another statement that satisfies a Rule 804 exception; merely recording a witness's statement does not, by itself, establish admissibility. The investigator must also be able to demonstrate the witness's qualifying illness and satisfy the foundational requirements of the particular exception invoked. This approach recognizes the witness's inability to appear while maintaining the procedural safeguards required for evidence offered at trial. See Federal Rule of Evidence 804 and the United States Courts' current rules of practice and procedure.

## QUESTION NO: 32

Steve, a forensic investigator, was asked to investigate an email incident in his organization. The organization has Microsoft Exchange Server deployed for email communications. Which among the following files will Steve check to analyze message headers, message text, and standard attachments?

**A.** PUB.EDB

**B.** PRIV.EDB

**C.** PUB.STM

**D.** PRIV.STM

## ANSWER: B

**Explanation:**

**PRIV.EDB** is the correct file because it is the private information-store database used by legacy Microsoft Exchange Server deployments. This database holds the mailbox data belonging to individual users, including MAPI-formatted email items and the core properties needed during an email-forensics examination. Those properties include message metadata and headers, message bodies, recipients, timestamps, folder information, and standard attachments. An investigator examining a suspected user mailbox therefore uses the private store to recover and analyze the contents and attributes of messages relevant to the incident.

In legacy Exchange versions, the private store is distinct from the public-folder store: the private store is specifically associated with user mailboxes. Exchange databases use the Extensible Storage Engine, and forensic analysis of the private database can help establish what a user sent, received, stored, or deleted, subject to the state of the database and the available transaction logs and backups. Microsoft describes Exchange database storage and recovery concepts in its database recovery documentation. Additional Exchange forensic context, including the role of private Exchange databases in mailbox examination, is available from SysTools Exchange Server Forensics.

## QUESTION NO: 33

Brian needs to acquire data from RAID storage. Which of the following acquisition methods is recommended to retrieve only the data relevant to the investigation?

**A.** Static Acquisition

**B.** Sparse or Logical Acquisition

**C.** Bit-stream disk-to-disk Acquisition

**D.** Bit-by-bit Acquisition

## ANSWER: B

**Explanation:**

**Sparse or Logical Acquisition** is the appropriate method when the objective is to retrieve only data that is relevant to an investigation from RAID storage. A logical acquisition collects selected files, folders, file-system structures, or other specifically identified evidence rather than creating a complete forensic image of every sector on each RAID member disk. This substantially reduces the volume of data collected, the time needed to acquire it, and the storage required for the resulting evidence, which can be especially important for high-capacity RAID arrays.

In a RAID environment, the logical storage presented to the operating system may span multiple physical disks according to the array's configuration. Acquiring the relevant logical data through an authorized, documented process allows the examiner to target the material within that presented volume without unnecessarily collecting unrelated information. The examiner should record the RAID configuration, acquisition scope, tool and version used, timestamps, and cryptographic hash values for acquired evidence so the collection can be verified and its integrity supported. NIST describes logical acquisition as collection of active files and directories rather than all storage locations; its guidance on forensic handling also emphasizes preserving evidence integrity and documenting collection activities. See NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response and NIST Computer Forensics Tool Testing Program.

## QUESTION NO: 34

An investigator has extracted the device descriptor for a 1GB thumb drive that looks like: Disk&Ven_Best_Buy&Prod_Geek_Squad_U3&Rev_6.15. What does the "Geek_Squad" part represent?

**A.** Product description

**B.** Manufacturer Details

**C.** Developer description

**D.** Software or OS used

## ANSWER: A

**Explanation:**

"Product description" is correct. This device identifier follows the common Windows Plug and Play hardware-ID structure for disk devices: `Disk&Ven_<vendor>&Prod_<product>&Rev_<revision>`. In the descriptor shown, `Ven_Best_Buy` identifies the vendor string as "Best Buy," while `Prod_Geek_Squad_U3` identifies the product string reported by the USB storage device. Therefore, "Geek_Squad" is part of the product identification or description, with "U3" also included in the product field. The final component, `Rev_6.15`, is the device revision or firmware version reported by the hardware.

For forensic work, these fields can help associate an installed USB device with a particular vendor, product branding, and revision. However, the text is manufacturer-supplied device metadata, so investigators should preserve the full identifier and corroborate it with USBSTOR registry artifacts, setup logs, and device serial-number information where available. Microsoft documents that Plug and Play device identifiers contain hardware-identification components and that hardware IDs are supplied in a defined identifier format. See Microsoft's Hardware IDs documentation and Microsoft's device identification strings documentation.

## QUESTION NO: 35

Which "Standards and Criteria" under SWDGE states that "the agency must use hardware and software that are appropriate and effective for the seizure or examination procedure"?

**A.** Standards and Criteria 1.7

**B.** Standards and Criteria 1.6

**C.** Standards and Criteria 1.4

**D.** Standards and Criteria 1.5

## ANSWER: D

**Explanation:**

**Standards and Criteria 1.5** is the applicable SWGDE requirement. This criterion establishes that an agency conducting digital-evidence seizure or examination must employ hardware and software suited to the specific procedure and capable of performing it effectively. In forensic practice, this means the selected tools must be fit for purpose, used within their known capabilities, and support a process that preserves the integrity and reliability of the evidence. Tool suitability is not merely a purchasing or convenience issue: it is a core quality requirement because acquisition and examination results may later need to be reproduced, explained, and defended in legal proceedings. SWGDE's published materials provide guidance and best practices intended to promote consistent, technically sound digital-forensic work across agencies. The related NIST Computer Forensics Tool Testing program also emphasizes objective testing of forensic tools and the importance of understanding whether a tool performs its claimed functions accurately. See the SWGDE published documents repository and NIST's Computer Forensics Tool Testing Program for supporting forensic-tool guidance.

## QUESTION NO: 36

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 logging and message-tracking records are valuable forensic sources because they establish who sent or handled a message, identify the specific message, and place its transmission in a defensible timeline. The *user account that was used to send the account* represents sender-account attribution; investigators can correlate that account with authentication, mailbox, and directory records. A *unique message identifier*, such as the Internet Message-ID, supports correlation of the same message across mail clients, gateways, servers, and archived copies. The *contents of the e-mail message* can be available when the logged or retained mail record includes message data, providing evidence of communications, instructions, intent, or other relevant facts. The *date and time the message was sent* establishes chronology and can be correlated with server logs, endpoint activity, and other incident evidence. Together, these fields help an investigator attribute activity, trace message flow, and construct an accurate event timeline. Microsoft describes message tracing as a way to determine what happened to messages in an organization, including sender, recipient, and processing details: Message trace in the Exchange admin center. RFC 5322 defines key email header fields, including Date and Message-ID, used to identify and timestamp Internet messages: RFC 5322.

## QUESTION NO: 37

What is one method of bypassing a system BIOS password?

**A.** Removing the processor

**B.** Removing the CMOS battery

**C.** Remove all the system memory

**D.** Login to Windows and disable the BIOS password

**ANSWER: B**

**Explanation:**

Removing the CMOS battery is a traditional method of clearing the CMOS/RTC configuration memory that stores firmware setup settings on many desktop systems. With the machine powered off and disconnected from external power, removing the battery briefly can cause the stored configuration to reset to its factory-default state when power is restored. On systems whose BIOS or UEFI setup password is retained in that CMOS-backed configuration, this reset removes the configured password and permits access to firmware setup.

In a forensic or authorized support context, this is a physical-access technique and should be performed only with documented authority, while preserving records of the device's original state and the actions taken. The exact procedure is hardware-specific: some devices use a clear-CMOS or password-reset jumper rather than battery removal, and modern enterprise laptops may retain credentials in nonvolatile storage or require manufacturer-assisted recovery. Intel documents that clearing CMOS returns BIOS settings to defaults and may require resetting BIOS configuration afterward: Intel Support: Clear CMOS. Dell also notes that BIOS password recovery and reset behavior varies by system model and security design: Dell Support: Reset or Clear the BIOS Password.

**QUESTION NO: 38**

Which of the following data structures stores attributes of a process, as well as pointers to other attributes and data structures?

**A.** Lsproc

**B.** DumpChk

**C.** RegEdit

**D.** EProcess

**ANSWER: D**

**Explanation:**

`EPROCESS` is correct. In the Windows kernel, each active process is represented by an executive process object whose associated `EPROCESS` structure holds core process-management information. This includes process identifiers, execution and security context information, memory-management-related state, accounting details, and links or pointers to other kernel objects and supporting structures. Because it acts as the kernel's central representation of a process, forensic tools and memory-analysis workflows commonly examine `EPROCESS` structures to identify running processes and reconstruct relationships between process objects in captured memory. The structure is particularly important in Windows memory forensics because process enumeration often relies on the active-process linked list and other references maintained through process-object data. Microsoft notes that EPROCESS is an opaque kernel structure and that its fields vary between Windows versions; kernel drivers should access process details through documented kernel APIs rather than relying on internal field offsets. For forensic analysis, however, knowledge of the structure's role is essential when interpreting raw memory and process artifacts. See Microsoft's EPROCESS documentation and its overview of Windows kernel architecture.

**QUESTION NO: 39**

A forensics investigator needs to copy data from a computer to some type of removable media so he can examine the information at another location. The problem is that the data is around 42GB in size. What type of removable media could the investigator use?

**A.** Blu-Ray single-layer

**B.** HD-DVD

**C.** Blu-Ray dual-layer

**D.** DVD-18

**ANSWER: C**

**Explanation:**

Blu-Ray dual-layer is the appropriate removable medium because a dual-layer Blu-ray Disc provides up to 50 GB of storage capacity. That capacity accommodates an approximately 42 GB forensic data set on one piece of removable media, while leaving sufficient space for the complete acquisition and any necessary filesystem overhead. In forensic practice, selecting media with capacity greater than the evidence data is essential so the investigator can make a complete copy rather than splitting the data across multiple discs. A single-disc transfer also makes labeling, tracking, storage, and later verification more manageable. The copied evidence should be validated after transfer, ordinarily by calculating and comparing cryptographic hash values for the source data and the copied data. This supports evidence integrity by demonstrating that the copy examined at the other location matches the acquired data. The Blu-ray Disc Association describes Blu-ray formats and their 25 GB single-layer and 50 GB dual-layer capacities: Blu-ray Disc Association. NIST's guidance on forensic techniques also emphasizes maintaining the integrity of digital evidence through documented, repeatable handling and verification procedures: NIST SP 800-86.

## QUESTION NO: 40

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 polling and management traffic uses UDP port 161. An SNMP manager sends requests, such as GET, GETNEXT, GETBULK, and SET operations, to an SNMP agent listening on this port; the agent returns its response to the manager. Therefore, firewall rules between the central manager and devices in remote offices must permit the relevant UDP 161 traffic so the manager can query managed systems.

SNMP notifications use UDP port 162. Devices and agents send unsolicited traps to the manager or trap receiver on this port, and SNMPv2c/SNMPv3 informs are also received on this port before an acknowledgement is returned. Allowing UDP 162 enables the manager to receive important event-driven messages, such as link-state changes, authentication failures, and threshold alerts, from remote-office devices. Rules should be scoped to authorized manager and agent IP addresses rather than opened broadly, and SNMPv3 should be preferred where possible because it provides authentication and privacy protections. The IANA service-name registry identifies snmp as port 161 and snmptrap as port 162. Cisco's SNMP configuration guidance also documents the manager-agent polling and notification model: Cisco SNMP Support.

## QUESTION NO: 41

Which of the following statements is true with respect to SSDs (solid-state drives)?

**A.** Like HDDs. SSDs also have moving parts

**B.** SSDs cannot store non-volatile data

**C.** SSDs contain tracks, clusters, and sectors to store data

**D.** Faster data access, lower power usage, and higher reliability are some of the major advantages of SSDs over HDDs

## ANSWER: D

**Explanation:**

Faster data access, lower power usage, and higher reliability are some of the major advantages of SSDs over HDDs. An SSD stores information in nonvolatile flash memory and accesses that memory electronically, rather than relying on a rotating magnetic platter and a mechanical read/write head. This design substantially reduces access latency and enables high input/output performance, particularly for workloads involving many small, random reads and writes. Because an SSD has no motor or moving head assembly, it generally consumes less power and produces less heat than a conventional hard disk drive. The absence of mechanical components also improves resistance to shock and vibration, contributing to reliability in portable systems and environments where movement can occur. For forensic practitioners, the electronic, flash-based architecture is significant because SSD behavior, including controller-managed data placement and garbage collection, can affect the persistence and recoverability of deleted data. NIST identifies flash-based storage as a distinct media type with characteristics that must be considered when sanitizing or handling storage media. See NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization and Samsung Semiconductor SSD overview.

## QUESTION NO: 42

A forensic investigator is analyzing a deleted file on an ext-family Linux file system. Which of the following statements are TRUE? (Choose three.)

**A.** The directory entry can be removed or made available for reuse

**B.** The inode link count is reduced

**C.** Data blocks may remain recoverable until overwritten

**D.** The file contents are immediately overwritten with zeros

**E.** The deleted file is automatically moved to the Windows Recycle Bin

## ANSWER: A B C

**Explanation:**

When a file is deleted from an ext-family file system, the file-system directory entry is removed or marked available for reuse, and the inode link count is reduced. If the link count reaches zero and no process still holds the file open, the file system can release the inode and data blocks for reuse. Until those blocks are overwritten, portions of the former file content may remain recoverable through forensic methods.

Deletion does not normally overwrite the complete file contents immediately. Recovery prospects depend on later disk activity, filesystem behavior, journaling, trim operations on solid-state storage, and whether the released blocks have been reused. The ext4 documentation describes inode and directory structures used by the filesystem. See Linux kernel ext4 documentation.

## QUESTION NO: 43

All Blackberry email is eventually sent and received through what proprietary RIM-operated mechanism?

**A.** Blackberry Message Center

**B.** Microsoft Exchange

**C.** Blackberry WAP gateway

**D.** Blackberry WEP gateway

**ANSWER: A**

**Explanation:**

**Blackberry Message Center** is the correct answer in the terminology used by this question. BlackBerry's traditional email architecture did not ordinarily establish a direct, end-to-end connection between a handset and the organization's mail server. Whether messages originated through a BlackBerry Enterprise Server environment or a consumer-oriented BlackBerry Internet Service configuration, delivery was mediated through RIM's proprietary BlackBerry infrastructure. The BlackBerry Message Center refers to that RIM-operated intermediary mechanism responsible for relaying and coordinating BlackBerry email traffic between the relevant mail environment, wireless carrier network, and device.

This centralized architecture was a significant forensic consideration because message delivery, synchronization behavior, routing, and some service artifacts depended on the BlackBerry service infrastructure rather than solely on the mobile carrier or local mail server. In an investigation, understanding that email traversed the RIM-operated service helps identify the appropriate sources of records and clarifies why device traffic may reflect communications with BlackBerry infrastructure. BlackBerry's enterprise mobility documentation describes the role of BlackBerry infrastructure in securely connecting devices and organizational services; see BlackBerry UEM and BlackBerry Support.

**QUESTION NO: 44**

What does the bytes 0x0B-0x53 represent in the boot sector of NTFS volume on Windows 2000?

**A.** Jump instruction and the OEM ID

**B.** BIOS Parameter Block (BPB) and the OEM ID

**C.** BIOS Parameter Block (BPB) and the extended BPB

**D.** Bootstrap code and the end of the sector marker

**ANSWER: C**

**Explanation:**

**BIOS Parameter Block (BPB) and the extended BPB** is correct. In an NTFS volume boot sector, offsets 0x0B through 0x53 contain the NTFS parameter information used to describe the volume's physical and logical layout. The standard BIOS Parameter Block begins at offset 0x0B and includes foundational disk geometry and sector-related fields, such as bytes per sector and sectors per cluster. NTFS then uses an extended form of this information to store NTFS-specific parameters, including the total sector count, the logical cluster numbers for key metadata files such as the Master File Table, cluster-per-file-record values, cluster-per-index-buffer values, and the volume serial number. Together, these fields enable the operating system to locate and interpret the NTFS file-system structures during startup and volume mounting. The boot-sector jump instruction and OEM identifier occur before this range, while bootstrap code follows the BPB and extended BPB area. This offset mapping is consistent with the documented NTFS boot-sector layout. See the NTFS boot-sector field reference at NTFS.com: NTFS Partition Boot Sector and Microsoft's NTFS technical documentation at Microsoft Learn: NTFS Technical Reference.

**QUESTION NO: 45**

Which of the following malware targets Android mobile devices and installs a backdoor that remotely installs applications from an attacker-controlled server?

**A.** Felix

**B.** XcodeGhost

**C.** xHelper

**D.** Unflod

**ANSWER: C**

**Explanation:**

**xHelper** is the correct answer. It is an Android malware family identified for its persistence and its ability to communicate with command-and-control infrastructure to obtain and deploy additional payloads. Its functionality includes downloading further malicious applications from attacker-controlled locations, allowing an attacker to extend the compromise after the initial infection. This behavior effectively creates a backdoor-like mechanism: the affected Android device can receive further software selected by the operator without the user intentionally seeking out or installing those applications.

The capability to install or prompt installation of additional applications is especially significant in a mobile forensic investigation because the original xHelper component may be only the initial-stage artifact. Investigators should therefore examine installed-package records, download directories, application-installation events, network connections, and persistence-related artifacts to identify secondary payloads and reconstruct the scope of activity. Malwarebytes documented xHelper's downloader behavior and its ability to retrieve and install additional applications; Symantec also describes the threat's remote payload-download capabilities. See Malwarebytes' xHelper analysis and Broadcom/Symantec's Android.xHelper threat profile.

**QUESTION NO: 46**

Which of the following information can an examiner commonly obtain from a Windows LNK shortcut file? (Choose three.)

**A.** Target file path

**B.** Target file timestamps

**C.** Volume information associated with the target

**D.** Contents of every file in the target directory

**E.** Private key used to encrypt the target file

**ANSWER: A B C**

**Explanation:**

Windows shortcut files can contain the **target file path**, **target file timestamps**, and **volume information associated with the target**. A LNK file may preserve details about the object it referenced even after that object is deleted or the removable media containing it is no longer connected. This makes shortcut files valuable when reconstructing user activity involving documents, executables, network shares, and removable storage devices.

LNK artifacts can also include target size, machine name, working directory, command-line arguments, and link-creation or modification metadata, depending on the shortcut and operating-system version. Microsoft defines the Shell Link Binary File Format in the MS-SHLLINK specification.

**QUESTION NO: 47**

Travis, a computer forensics investigator, is finishing up a case he has been working on for over a month involving copyright infringement and embezzlement. His last task is to prepare an investigative report for the president of the company he has been working for. Travis must submit a hard copy and an electronic copy to this president. In what electronic format should Travis send this report?

**A.** TIFF-8

**B.** DOC

**C.** WPD

**D.** PDF

**ANSWER: D**

**Explanation:**

PDF is the appropriate electronic format for an investigative report because it preserves the report's intended appearance across different operating systems, devices, and office-software versions. A forensic report may include structured narrative findings, tables, exhibit references, screenshots, hashes, and conclusions; PDF provides a stable, professional, readily printable rendition of that material. This is particularly important when the electronic copy must correspond closely to the submitted hard copy and may be retained as a business or evidentiary record.

PDF also supports document-security and integrity-related features, including password protection, permissions, and digital signatures where organizational policy calls for them. A digitally signed PDF can help a recipient validate the signer and detect changes made after signing. The investigator should retain the original report, use controlled distribution, and follow the organization's evidence-handling and report-review procedures; selecting PDF does not replace those controls. NIST's guidance on digital evidence emphasizes maintaining integrity and documenting handling, principles that also apply when final investigative materials are prepared and distributed. See NIST SP 800-86 and Adobe's overview of digital IDs and signatures in PDFs.

**QUESTION NO: 48**

An investigator is examining a Windows system for evidence of program execution. Which of the following artifacts can provide evidence that an application was executed? (Choose three.)

**A.** Prefetch files

**B.** Amcache.hve

**C.** UserAssist entries

**D.** hosts file

**E.** BOOTMGR

**ANSWER: A B C**

**Explanation:**

**Prefetch files**, **Amcache.hve**, and **UserAssist entries** can provide useful evidence of program execution. Prefetch files can record executable names, execution counts, run times, and files referenced during program startup. Amcache can contain application and file inventory information that may assist in identifying executable files observed by the system. UserAssist Registry entries record user-launched GUI applications and are commonly decoded to reveal program paths and execution-related timestamps.

These artifacts should be interpreted together because each has different collection conditions and limitations. A single artifact may show that a file existed or was accessed, while corroboration across several sources produces a stronger timeline. Microsoft documents Prefetch as a performance feature and provides Registry documentation relevant to artifact examination: Microsoft Windows Registry.

**QUESTION NO: 49**

What happens when a file is deleted by a Microsoft operating system using the FAT file system?

**A.** the file's directory entry is marked deleted and its FAT cluster-chain references are released; the data remains until overwritten

**B.** the file is erased and cannot be recovered

**C.** a copy of the file is stored and the original file is erased

**D.** the file is erased but can be recovered

**ANSWER: A**

**Explanation:**

When a file is deleted from a FAT volume, the operating system normally performs a logical deletion rather than immediately overwriting the file's contents. The file's directory entry is marked as deleted, conventionally by replacing the first character of the filename with the deletion marker, and the FAT entries that recorded the file's cluster chain are released so those clusters may be allocated to another file. The underlying bytes in the data clusters usually remain on the disk until later activity overwrites them. Consequently, forensic recovery can often reconstruct a deleted file by examining the deleted directory entry and locating its former data clusters, particularly when those clusters have not been reused. This behavior is significant during evidence acquisition: the storage device should be preserved and imaged promptly to minimize the chance that normal system activity overwrites the released clusters. The FAT on-disk format and directory-entry conventions are documented in Microsoft's FAT specification. NIST also discusses the importance of preserving digital evidence before data can be altered in Guide to Integrating Forensic Techniques into Incident Response.

**QUESTION NO: 50**

Sectors in hard disks typically contain how many bytes?

**A.** 256

**B.** 512

**C.** 1024

**D.** 2048

**ANSWER: B**

**Explanation:**

512 is the correct answer because the traditional logical sector size used by hard disks is 512 bytes. In disk forensics, this value is foundational: disk offsets, partition structures, boot records, and file-system metadata have historically been described in terms of 512-byte sectors. For example, a Master Boot Record occupies the first logical sector of a disk and is conventionally 512 bytes long. Consequently, forensic tools and examination procedures commonly use 512-byte sector calculations when locating and interpreting on-disk artifacts.

Although many modern drives use Advanced Format technology with physical sectors of 4,096 bytes, they may expose 512-byte logical sectors to maintain compatibility with existing operating systems, utilities, and applications. Some newer devices use native 4,096-byte logical sectors, but this does not alter the traditional and exam-expected definition of a hard-disk sector. The investigator should nevertheless verify the device's reported logical and physical sector sizes during acquisition and analysis, since using an incorrect sector size can cause incorrect offset calculations. See the Microsoft Advanced Format disk compatibility documentation and the Seagate Advanced Format overview.

**QUESTION NO: 51**

What must an attorney do first before you are called to testify as an expert?

**A.** Qualify you as an expert witness

**B.** Read your curriculum vitae to the jury

**C.** Engage in damage control

**D.** Prove that the tools you used to conduct your examination are perfect

**ANSWER: A**

**Explanation:**

Before offering expert opinions, the attorney must establish a foundation showing that the witness is qualified to testify as an expert. “Qualify you as an expert witness” is correct because expert testimony is not admitted merely because a witness has relevant job experience or was retained for the case. Through foundational questions, counsel demonstrates the witness’s knowledge, skill, experience, training, or education in the relevant forensic discipline. The attorney may elicit information about academic credentials, professional certifications, forensic work history, prior examinations, publications, specialized training, and familiarity with the methods used in the examination. This process enables the court to determine whether the witness meets the threshold for expert testimony and whether the proposed opinions rest on reliable specialized knowledge. Under Federal Rule of Evidence 702, a qualified expert may testify when the testimony will assist the fact-finder, is based on sufficient facts or data, results from reliable principles and methods, and those methods have been reliably applied to the case facts. The court acts as the gatekeeper for this determination, so establishing the expert’s qualifications is the necessary first step before substantive expert testimony is presented. See Federal Rule of Evidence 702 and the U.S. Courts Federal Rules of Evidence.