National Forensic
Sciences University
Knowledge | Wisdom | Fulfilment
An Institution of National Importance
(Ministry of Home Affairs, Government of India)

Answer Key
March 30, 2025

SSA -Digital Forensics - Examination

1. Investigator A argues findings based on Tool X. Investigator B responds, "Tool X is known for being slow, so your entire analysis must be flawed." This response uses which logical fallacy?

A Appeal to Authority

B Hasty Generalization

✓ C Red Herring (attacking speed instead of accuracy/findings)

D Ad Hominem

2. Policy: "Access to the financial database requires Level 3 clearance." Fact: "Employee Raj has Level 2 clearance." Deduction: "Employee Raj should not have access to the financial database." This reasoning is an example of:

A Inductive Logic

✓ B Applying a specific rule (Deductive Logic)

C Analogical Reasoning

D Circular Reasoning

3. After observing three separate incidents where systems were compromised after visiting 'shadywebsite.net', an analyst strongly suspects the website hosts malware. This conclusion is primarily based on:

A Direct Proof

B Coincidence

✓ C Inductive Reasoning (generalizing from specific instances)

D Deductive Reasoning

4. Validating a forensic tool's accuracy is to Reliable Results as Calibrating measuring equipment is to _____?

A Faster Measurement

✓ B Accurate Measurement

C Cheaper Equipment

D Ignoring Errors

5. Statement: "The forensic analysis was conducted using standard procedures." What is a key implicit assumption that might need verification in court?

A Standard procedures are always perfect.

✓ **B** The specific examiner actually followed the standard procedures correctly in this case.

C Standard procedures are easy to understand.

D No procedures were needed.

6. Argument: "The defendant's computer contained encryption software, therefore they must have been trying to hide illicit activities." Why is this argument logically incomplete?

A Encryption software is illegal to possess.

✓ **B** Using encryption software is common for legitimate privacy reasons and doesn't automatically imply illicit activity.

C All encrypted data is automatically suspicious.

D The defendant denied using the software.

7. Having network logs showing a connection to a malicious IP address is a _____ condition for confirming a network breach occurred via that IP, but it might not be _____ if the connection was blocked by a firewall.

✓ **A** sufficient, necessary

B necessary, sufficient

C unnecessary, sufficient

D sufficient, irrelevant

8. A file server log shows timestamps in Pacific Standard Time (PST = UTC - 8:00). An incident occurred at 14:00 PST. What was the time in Coordinated Universal Time (UTC)?

A 06:00 UTC

B 14:00 UTC

C 20:00 UTC

✓ **D** 22:00 UTC

9. A 1 GB file is stored on a filesystem with a 64 KB block (cluster) size. Approximately how many blocks does this file occupy? (Assume 1 GB = 1,048,576 KB)

A 1,024 blocks

B 8,192 blocks

✓ **C** 16,384 blocks

D 65,536 blocks

10. Out of 200 logins recorded, 5 were flagged as 'anomalous'. If an auditor randomly selects one login record, what is the probability it is flagged as 'anomalous'?

A 0.05

✓ B 0.025

C 0.1

D 0.2

11. A forensic image is being transferred over a network at 500 Mbps (Megabits per second). How many Megabytes (MB) are transferred in 10 seconds? (Assume 1 Byte = 8 bits)

A 500 MB

✓ B 625 MB

C 5000 MB

D 4000 MB

12. What is the decimal equivalent of the binary number 1101?

A 11

B 12

✓ C 13

D 14

13. A memory analysis process took 45 minutes and examined 16 GB of data. What was the average analysis speed in GB per minute?

A 0.25 GB/min

✓ B Approx 0.36 GB/min

C 0.5 GB/min

D 1 GB/min

14. Log entry 1 has timestamp 08:15:55. Log entry 2 has timestamp 08:16:10. What is the time difference between these entries?

A 5 seconds

B 10 seconds

✓ C 15 seconds

D 20 seconds

15. Which sentence correctly uses the passive voice for a forensic context?

A The data recovery attempted by the software.

B Evidence by the crime scene was collected.

✓ C A forensic image was created from the original drive.

D They were examined the artifacts.

16. Choose the best conjunction: The initial scan revealed no malware, ______ a deeper analysis uncovered hidden rootkit components.

A because

B consequently

✓ C however

D unless

17. In forensic reporting, the term "exculpatory" evidence refers to evidence that tends to:

A Prove guilt

B Be irrelevant

✓ C Clear a defendant of guilt or fault

D Be inadmissible

18. Please submit ______ report detailing your findings on ______ suspect device.

A a, a

B the, the

✓ C a, the

D the, a

19. Which sentence correctly describes a past forensic action?

A The team will analyze the network traffic tomorrow.

B Network traffic is being analyzed currently.

C The team analyzes the network traffic regularly.

✓ D The team analyzed the network traffic last week.

20. A key difference between "verification" and "validation" of forensic tools is that validation typically refers to:

A Checking a hash value matches.

[✓ B] Confirming the tool works correctly for its intended purpose through testing.

C Running the tool on the actual case evidence.

D Documenting the tool's version number.

21. Slack space is the unused space within a disk cluster between the end of a file's actual data and the end of the cluster. Remnants of previously deleted files can sometimes be found in slack space. What potential forensic value does slack space hold?

A It stores the master file table.

B It guarantees recovery of full deleted files.

[✓ C] It may contain fragments of deleted data relevant to an investigation.

D It indicates physical damage to the disk.

22. The heat sinks and fans attached to CPUs and GPUs are necessary primarily to:

A Generate more electricity for the components.

[✓ B] Dissipate the waste heat produced during operation, preventing overheating.

C Make the computer run quieter.

D Protect the components from dust.

23. OLED (Organic Light Emitting Diode) displays differ from traditional LCDs in that OLED pixels:

A Use liquid crystals to block light.

B Require a separate backlight unit.

[✓ C] Emit their own light directly.

D Are much larger and less energy-efficient.

24. What is the size of MAC address?

A 32 bits

[✓ B] 48 bits

C 64 bits

D 128 bits

25. What is the size of a Bluetooth address?

A 32 bits

✓ B 48 bits

C 64 bits

D 128 bits

26. Which computer component is responsible for executing instructions and performing calculations?

A RAM (Random Access Memory)

B Hard Disk Drive (HDD)

✓ C CPU (Central Processing Unit)

D Motherboard

27. Which of the following is an example of Application Software?

A Operating System

B Linux Kernel

C Device Driver for a printer

✓ D Microsoft Excel

28. What is the primary role of RAM in a computer system?

A Long-term storage of files and programs

✓ B Temporary storage for data and programs currently being used by the CPU

C Connecting different hardware components together

D Providing power to the system

29. Which network concept provides a unique logical address to a device on an IP network?

A MAC Address

B Subnet Mask

✓ C IP Address

D Default Gateway

30. Which of the following is considered non-volatile storage, meaning it retains data even when power is turned off?

A RAM

B CPU Cache

✓ C SSD (Solid State Drive)

D System Registers

31. What fundamental function of an Operating System involves managing how multiple programs use the CPU?

A Memory Management

B File Management

✓ C Process Management (Scheduling)

D Input/Output Management

32. Which filesystem includes features like journaling, file permissions, and support for very large file sizes, commonly found on Windows systems?

A FAT16

B FAT32

✓ C NTFS (New Technology File System)

D ext2

33. What distinguishes computer Hardware from Software?

A Hardware is expensive, Software is cheap.

✓ B Hardware refers to the physical components you can touch, while Software refers to the instructions and programs that run on the hardware.

C Hardware is used for storage, Software is used for processing.

D Hardware is permanent, Software is temporary.

34. During live acquisition on a potentially compromised Windows system, an investigator observes network connections to a known malicious IP via netstat -ano. What artifact within a subsequent memory dump would be most crucial for identifying the specific process responsible for this connection?

A The MFT (Master File Table) copy in RAM.

B The list of loaded kernel drivers (modules.lst).

C The Process Environment Block (PEB) for running processes.

✓ D The network connection structures (e.g., netscan or connections output in Volatility) correlating PIDs with connection details.

35. An investigator creates a forensic image using dd and calculates a SHA-256 hash. Later, the hash of the image file is re-verified and matches. However, a hardware write blocker was NOT used during acquisition. Why might the integrity of the original source evidence still be questionable in court?

A dd cannot create bit-for-bit copies.

B SHA-256 is known to have collision vulnerabilities.

✓ C Without a write blocker, the acquisition process itself (e.g., OS automounting, metadata updates) could have inadvertently modified the source drive before or during imaging.

D The hash only verifies the image file, not the source drive's state.

36. While analyzing an NTFS volume, an investigator focuses on the $LogFile. What is the primary forensic value of this metadata file?

A It contains a backup copy of all user documents.

✓ B It records metadata transactions used for filesystem recovery, potentially revealing file operations (creations, deletions, renames) that occurred shortly before a crash or shutdown.

C It stores the encryption keys for BitLocker.

D It lists all installed applications and their version numbers.

37. You are examining a Linux system and suspect a rootkit has modified critical system binaries like /bin/ls. Which technique would be most effective in detecting this modification?

A Checking the ~/.bash_history file.

✓ B Comparing the hash values of the current system binaries against known good hashes from a trusted source or the package manager database (e.g., rpm -V or debsums).

C Analyzing the /var/log/auth.log file for unusual logins.

D Performing a keyword search across the entire disk for "rootkit".

38. Which of the following is the most secure hashing algorithm or technique as compared to the others?

A CRC

B MD5

✓ C SHA-3

D MD-6

39. During network forensic analysis of captured packets (PCAP file), you observe significant traffic to various external IPs over TCP port 443, but the payload is encrypted (TLS/SSL). What supplementary evidence source would be most helpful in potentially identifying the nature or destination hostnames of this encrypted traffic?

A Analysis of ARP cache entries on the source machine.

✓ B DNS query logs or DNS traffic captures (UDP/TCP port 53) occurring around the same time as the TLS sessions.

C System event logs from the source machine.

D The MFT from the source machine's hard drive.

40. Using the Volatility framework on a Windows memory dump, the pslist command shows running processes, while psscan reveals additional processes not found by pslist. What does this discrepancy often indicate?

A A corrupted memory dump.

B Normal operation of hidden system services.

✓ C The presence of terminated processes whose structures remain in memory or potentially hidden/unlinked processes (e.g., by malware).

D An error in the Volatility profile being used.

41. Which file timestamp on an NTFS volume typically reflects when the file's metadata (e.g., name, attributes, MFT record itself) was last modified, not necessarily the content?

A Accessed Time (A-Time)

B Modified Time (M-Time)

C Created Time / Birth Time (B/C-Time)

✓ D MFT Entry Modified Time ($FILE_NAME attribute modification time, sometimes labelled Change time or C-Time)

42. An investigator performs file carving on unallocated space and recovers numerous JPEG image fragments. However, many recovered files are corrupted or incomplete. What is a common reason for this?

A JPEG files cannot be carved reliably.

B The carving tool used an incorrect file header/footer signature.

✓ C File fragmentation: The original JPEGs' data clusters were non-contiguous on the disk, and carving relies on sequential data recovery.

D Unallocated space does not contain recoverable data.

43. Analysis of a Linux ext4 filesystem reveals a file has been deleted, but its inode number is known. What information might still be recoverable directly from the inode structure itself (even if data blocks are overwritten)?

A The full content of the file.

✓ B File metadata such as permissions, ownership, size, and potentially timestamps (though deletion time might update some).

C The user who deleted the file.

D The process name that deleted the file.

44. You find evidence of Alternate Data Streams (ADS) attached to files on an NTFS volume. What is a common malicious use of ADS relevant to forensics?

A Compressing files to save disk space.

B Storing legitimate user profile information.

✓ C Hiding malware executables or malicious scripts attached to seemingly benign files.

D Recording file access timestamps.

45. When examining macOS unified logs (log show), filtering by specific subsystems (e.g., subsystem:com.apple.securityd) is crucial because:

A The logs are always encrypted by default.

✓ B The unified log system aggregates vast amounts of data from numerous processes and subsystems, making unfiltered analysis impractical.

C Filtering is the only way to view logs older than 24 hours.

D Each subsystem log is stored in a separate physical file.

46. A key difference between MD5/SHA-1 and SHA-256/SHA-3 hashing algorithms in a forensic context is:

A MD5/SHA-1 produce much longer hash values.

B MD5/SHA-1 are significantly faster, making them preferable for large datasets.

✓ C SHA-256/SHA-3 offer much higher resistance to collision attacks, making them more trustworthy for verifying evidence integrity against deliberate tampering.

D Only SHA-256/SHA-3 can be used on non-Windows systems.

47. What specific Windows Registry hive typically contains information about USB devices that have been connected to the system, including vendor/product IDs and potentially last connection times?

A SAM

B SECURITY

C SOFTWARE

✓ D SYSTEM

48. Network flow analysis (e.g., NetFlow, sFlow) differs from full packet capture (PCAP) analysis in that flow data typically:

A Contains the full payload content of every packet.

✓ B Provides summary information about network conversations (IPs, ports, protocols, byte/packet counts) but usually lacks the actual packet content.

C Can only be collected from individual endpoint machines, not network devices.

D Is primarily used for analyzing Layer 2 (Ethernet) traffic.

49. In memory forensics, what does the term "VAD" (Virtual Address Descriptor) relate to?

A A list of validated digital signatures for kernel modules.

✓ B Metadata describing the layout and permissions of memory ranges allocated to a specific process.

C The algorithm used for compressing memory dumps.

D A hardware component responsible for memory addressing.

50. You are analyzing a photograph and suspect it might be manipulated. Examining Error Level Analysis (ELA) results reveals significantly different ELA levels around a specific object compared to its surroundings. This suggests:

A The photo was taken with a high-quality camera.

✓ B The object may have been added or altered, as different compression levels were likely introduced during manipulation.

C The photo uses lossless compression.

D The EXIF metadata is corrupted.

51. When dealing with mobile device forensics, acquiring a "Physical" image is often preferred over a "Logical" or "File System" acquisition because:

A It is always faster and requires less storage space.

B It bypasses all device passcodes and encryption automatically.

✓ **C** It captures a bit-for-bit copy of the entire flash memory, including unallocated space and potentially deleted data, which logical methods often miss.

D It only acquires user-generated data like contacts and messages.

52. The Windows artifact UsnJrnl (Update Sequence Number Journal) is primarily used for:

✓ **A** Tracking changes (file creation, deletion, renaming, etc.) made to files and directories on an NTFS volume, providing a high-level log of filesystem activity.

B Storing user credentials for network shares.

C Caching thumbnails for images viewed by the user.

D Managing system restore points.

53. Which forensic principle emphasizes the need for forensic processes and tools to produce the same result when applied to the same evidence under the same conditions?

A Admissibility

B Chain of Custody

✓ **C** Repeatability

D Volatility

54. Analysis of Linux shell history (.bash_history) shows a command rm important_file.txt. However, file recovery tools find no trace of this file in unallocated space. What is the most plausible explanation?

A The rm command on Linux always securely wipes data.

B The file system did not support journaling

✓ **C** The .bash_history file cannot be trusted.

D The file was renamed before deletion

55. In macOS Keychain analysis, what type of information is commonly sought by forensic investigators?

A System boot logs.

✓ **B** Stored passwords for websites, network shares, Wi-Fi networks, and encrypted volume keys.

C A list of all installed applications.

D CPU usage statistics.

56. Detecting Least Significant Bit (LSB) steganography in an image often involves:

- A Checking the EXIF metadata for a "HiddenData" tag.
- B Analyzing the image histogram for unusual patterns.
- ✓ C Performing statistical analysis on the pixel value LSBs to see if they deviate significantly from the expected random distribution of a normal image.
- D Comparing the image file size to its dimensions.

57. You recover a memory dump from a system suspected of running fileless malware. Which Volatility plugin would be most useful for finding injected code or reflective DLLs loaded directly into the memory of legitimate processes?

- A pslist
- B netscan
- ✓ C malfind
- D filescan

58. What is a significant challenge when performing network forensics on traffic encrypted with TLS 1.3 using Perfect Forward Secrecy (PFS)?

- A TLS 1.3 packets cannot be captured by standard tools.
- ✓ B Even if the server's private key is later compromised or obtained, it generally cannot be used to decrypt previously captured sessions due to ephemeral key exchange.
- C TLS 1.3 uses weak encryption algorithms.
- D PFS only applies to UDP traffic, not TCP.

59. The Windows Registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist is forensically significant because it can contain:

- A A list of all USB devices ever connected.
- ✓ B Encrypted records of GUI-based program executions initiated by the user.
- C The user's internet Browse history.
- D System service configuration data.

60. When comparing a forensic image creation process using dd versus using a tool like FTK Imager or EnCase, a major advantage of the dedicated forensic tools often is:

- A They produce significantly smaller image files.
- ✓ B They embed hash values (e.g., MD5, SHA1) within the image file format (like E01) and perform verification automatically during acquisition.
- C They can only image Windows systems.
- D They do not require write blockers.

61. What is the primary focus of the ISO/IEC 17025:2017 standard?

A Specifying requirements for manufacturing forensic hardware.

B Defining specific cyber laws for different countries.

✓ C Establishing general requirements for the competence, impartiality, and consistent operation of testing and calibration laboratories.

D Providing guidelines for ethical hacking practices.

62. According to ISO 17025, "impartiality" in a forensic laboratory context implies:

A Using only tools from impartial vendors.

✓ B Ensuring that objectivity is maintained and not compromised by conflicts of interest or bias.

C Processing samples from different parties at different speeds.

D Sharing preliminary results before the final report.

63. What is the main purpose of having documented Standard Operating Procedures (SoPs) in a digital forensics unit?

A To satisfy software licensing requirements.

✓ B To ensure consistency, repeatability, and quality in forensic processes and analysis.

C To increase the complexity of forensic examinations.

D To provide a basis for marketing the lab's services.

64. Which of the following is a crucial element of an SoP for handling digital evidence?

A Detailed steps for data analysis techniques.

✓ B Procedures for maintaining and documenting the Chain of Custody.

C Guidelines for writing the final forensic report.

D Instructions for validating forensic software tools.

65. The concept of an "Examiner of Electronic Evidence," often requiring government notification or certification (as hinted by regulations like India's Section 79A), primarily serves to:

A Mandate the use of specific forensic hardware device

✓ B Establish a recognized authority whose expert opinion on electronic evidence holds legal weight in court proceedings.

C Define the minimum hardware requirements for forensic workstations.

D Mandate the use of specific forensic software.

66. Cyber laws in many jurisdictions often impose penalties for unauthorized access to computer systems. This is commonly referred to as:

A Data encryption

✓ B Hacking or unauthorized access

C Steganography

D Forensic imaging

67. Intentionally introducing malware (like viruses or worms) into a computer system, causing damage, is typically covered under cyber laws related to:

A Violation of privacy

B Identity theft

✓ C Causing damage to computer systems or data

D Intermediary liability

68. Laws addressing the transmission or publication of obscene or sexually explicit material in electronic form fall under regulations concerning:

A Cyber terrorism

✓ B Content-related offenses

C Tampering with source code

D Denial of service attacks

69. What is a fundamental "best practice" regarding the use of digital forensic tools?

A Using the oldest version available for stability.

B Modifying the tool's source code for each case.

✓ C Validation: Ensuring the tool functions as expected and produces accurate, reliable results.

D Using a single, all-purpose tool for every examination.

70. Maintaining detailed case notes and documentation throughout a forensic examination is essential for:

A Making the process take longer.

✓ B Supporting the findings, ensuring transparency, enabling peer review, and withstanding legal scrutiny.

C Training junior staff members only.

D Keeping the evidence physically secure.

71. What is the primary purpose of using a write-blocker during evidence acquisition (imaging)?

- **A** To encrypt the data as it is copied.
- **B** To speed up the data transfer rate.
- ✓ **C** To prevent any modification to the original source media during the acquisition process.
- **D** To automatically generate the forensic report.

72. The Chain of Custody record is vital for demonstrating:

- **A** The technical specifications of the evidence.
- **B** The examiner's qualifications.
- ✓ **C** The chronological documentation of who handled the evidence and when, ensuring its integrity and preventing tampering allegations.
- **D** The estimated time required for analysis.

73. International guidelines, such as those published by NIST (National Institute of Standards and Technology) or the former ACPO (Association of Chief Police Officers) in the UK, typically serve as:

- **A** Legally binding international treaties on digital evidence.
- **B** Mandatory technical specifications for all forensic hardware.
- ✓ **C** Widely respected best practices and frameworks that can inform national standards and laboratory procedures.
- **D** Marketing material for forensic tool vendors.

74. A laboratory's competence, as assessed under ISO 17025, includes factors like:

- **A** The location of the laboratory building.
- ✓ **B** Personnel qualifications and training, equipment calibration, method validation, and quality assurance measures.
- **C** The price list for forensic services.
- **D** The number of computers in the lab.

75. Cyber laws often contain provisions regarding "intermediary liability." These provisions typically address:

- **A** The liability of software developers for bugs in their code.
- ✓ **B** The responsibility of service providers (like ISPs or social media platforms) for content posted or transmitted by third-party users.
- **C** The liability of hardware manufacturers for device failures.
- **D** The responsibility of end-users for securing their own devices.

76. When investigating an IoT device suspected of being part of a DDoS botnet, acquiring volatile memory (RAM) is crucial but often difficult due to non-standard OSes and lack of direct interfaces. Which alternative approach might yield information about the device's recent network activity if RAM acquisition fails?

A Analyzing the device's static firmware image only.

✓ B Capturing and analyzing network traffic (PCAP) to/from the device's IP address on the local network segment or gateway.

C Checking the device manufacturer's cloud portal for usage logs.

D Performing a factory reset on the device to see default connections.

77. Blockchain analysis tools attempting to trace Bitcoin transactions often face obfuscation techniques. Which technique involves pooling transactions from multiple users into a single large transaction, making it difficult to link specific inputs to specific outputs?

A Using Hierarchical Deterministic (HD) wallets.

✓ B Employing mixing services (tumblers) or CoinJoin implementations.

C Transferring funds to a newly generated address within the same wallet.

D Paying high transaction fees.

78. An investigator recovers a drone but finds the onboard SD card containing flight logs has been recently formatted. What other component might store redundant or partial flight telemetry data (like GPS coordinates, altitude, timestamps) that could still be forensically valuable?

A The drone's battery management system.

B The drone's camera sensor itself.

✓ C The remote controller unit used to operate the drone.

D The drone's plastic chassis material.

79. Detecting sophisticated AI-generated deepfake videos often requires moving beyond simple visual artifact analysis. Which approach focuses on analyzing inconsistencies in underlying physiological or physical models assumed by the generation process?

A Checking the video file's metadata for "AI-Generated" tags.

B Analyzing frame-by-frame pixel value distributions.

✓ C Examining inconsistencies in subtle biometric signals like heart rate reflected in micro-blushing (remote photoplethysmography - rPPG analysis) or unnatural blinking patterns.

D Verifying the video codec used for compression.

80. An investigator trying to attribute activity on a Dark Web marketplace accessed via Tor faces anonymity challenges. If the suspect made an operational security (OpSec) mistake, which type of leaked data would most directly link their Tor activity to their real-world identity?

A Using a common, easily guessable password on the marketplace.

B Posting messages using perfect grammar and spelling.

✓ C Accidentally including metadata (like GPS coordinates) in an image uploaded to the marketplace or using the same unique username on both dark and clearnet sites.

D Browse the marketplace during typical daytime hours.

81. Advanced OSINT involves correlating data from diverse sources. If investigating a suspected fake social media profile promoting disinformation, which OSINT finding would strongly suggest the profile is part of an orchestrated campaign rather than a genuine individual?

A The profile picture is a unique, never-before-seen image.

B The profile posts frequently during business hours of a specific country known for disinformation campaigns.

✓ C The profile uses the same unique profile picture or banner image across multiple unrelated accounts, all posting similar narratives simultaneously.

D The profile has very few followers.

82. Cryptocurrency tracing becomes significantly harder with privacy coins like Monero (XMR). What core technology used by Monero obscures the transaction path by including multiple other public keys (decoys) in the input signature?

A zk-SNARKs

B Mimblewimble

✓ C Ring Signatures

D Stealth Addresses

83. In cloud forensics, acquiring evidence from a multi-tenant environment poses unique challenges. What is a primary reason why a Cloud Service Provider (CSP) might be hesitant or legally restricted from providing a full physical image of a server hosting a suspect's virtual machine?

A Physical imaging technology doesn't work on cloud servers.

✓ B The physical server likely contains data from other unrelated customers (tenants), raising privacy and legal concerns.

C CSPs do not keep logs of server activity.

D Virtual machines cannot be imaged forensically.

84. Investigating the origin of "fake news" often involves technical analysis beyond just content review. Which technique might help identify if a news website is part of a coordinated network, even if domain registration details (WHOIS) are anonymized?

A Analyzing the writing style for grammatical errors.

B Checking the website's Alexa traffic ranking.

✓ C Identifying shared infrastructure identifiers like Google AdSense/Analytics IDs, unique server configuration details, or IP address blocks used across multiple suspicious sites.

D Measuring the website's loading speed.

85. Metaverse platforms allow to collect what form of evidences?

A Physical fingerprints

✓ B Digital avatars and transaction logs

C Paper documents

D Blood samples

86. When encountering an unknown embedded device with a proprietary OS, physical acquisition methods might be necessary if logical methods fail. Which technique involves connecting directly to test points on the device's PCB to access memory or debug interfaces?

A Performing a network boot (PXE).

B Using standard USB forensic imagers.

✓ C JTAG (Joint Test Action Group) or ISP (In-System Programming) techniques.

D Analyzing the device's power consumption patterns.

87. Detecting audio deepfakes is challenging. What characteristic might indicate an audio recording is synthesized rather than a genuine human voice, even if it sounds convincing superficially?

A The presence of background noise.

✓ B Consistent and overly perfect pronunciation, lacking natural disfluencies (ums, ahs) or emotional variation expected in human speech.

C The audio file being in MP3 format.

D The speaker having a foreign accent.

88. Forensic analysis of IoT device firmware might involve 'firmware unpacking'. What is the goal of this process?

A To encrypt the firmware for secure storage.

B To compress the firmware to save space.

✓ C To extract the different components (kernel, filesystem, bootloader, configuration files) from the often monolithic firmware image for individual analysis.

D To install the firmware onto a different device.

89. What is the primary purpose of a write blocker in digital forensics?

A Allows to take a copy of the data

✓ B Allows to take a forensic copy of the data

C Allows to take copy including metadata and hash of the data

D Allows to perform network communication without storing logs

90. Drones can be subject to GPS spoofing attacks. In a forensic context, how might evidence of GPS spoofing manifest in the recovered flight data?

A The GPS logs show extremely high speeds inconsistent with the drone's capabilities.

✓ B The recorded GPS path shows sudden, physically impossible jumps in location, or contradicts other sensor data (like inertial measurements or visual landmarks if video is available).

C The GPS logs are perfectly smooth and follow common flight paths.

D The drone refuses to power on after the flight.

91. Analyzing the behavior of a suspect AI model itself (e.g., a recommendation algorithm accused of bias) falls under AI Forensics. What technique might be used to understand why the model makes certain predictions or recommendations?

A Calculating the hash value of the model file.

✓ B Using interpretability techniques (like SHAP or LIME) to identify which input features most influence the model's output for specific instances.

C Re-training the model from scratch using different data.

D Measuring the model's prediction speed.

92. OSINT investigations must navigate ethical and legal boundaries. Accessing a private, password-protected social media profile without authorization using leaked credentials would generally be considered:

A A standard and acceptable OSINT technique.

✓ B Unethical and likely illegal (constituting unauthorized access), falling outside legitimate OSINT practices.

C Acceptable if the information found is relevant to the investigation.

D A necessary step for comprehensive OSINT.

93. Social media platforms increasingly use ephemeral features (e.g., stories that disappear after 24 hours). What is the primary challenge this poses for digital investigators?

A Ephemeral content uses stronger encryption.

✓ B The data may no longer exist on the platform's servers or be accessible via standard APIs by the time an investigation begins, requiring rapid preservation or alternative methods.

C Ephemeral content cannot be screenshotted.

D Only verified accounts can use ephemeral features.

94. An investigator observes that on three separate occasions involving malware infections on different systems, a specific suspicious domain badsite.example.com was contacted shortly before system compromise. The investigator concludes this domain is likely involved in malware distribution. This conclusion is primarily based on:

A Deductive reasoning (applying a general rule to specific cases).

✓ B Inductive reasoning (forming a general conclusion from specific observations).

C Hearsay evidence.

D Ignoring contradictory evidence.

95. A forensic report states: "Based on the presence of Tool X artifacts and log entries showing data exfiltration to IP address Y immediately after Tool X execution, it is highly probable that Tool X was used to steal data." This statement demonstrates which key analytical skill?

A Identifying file types.

✓ B Correlating different pieces of evidence to form a likely sequence of events.

C Performing data recovery.

D Validating forensic software.

96. When writing a digital forensic report intended for court, the language used should primarily be:

A Highly technical and filled with jargon to demonstrate expertise.

B Vague and open to interpretation.

✓ C Clear, concise, objective, and unambiguous, explaining technical concepts in a way understandable to a non-technical audience (like lawyers, judges, jury).

D Biased towards the conclusion favoured by the hiring party.

97. An investigator finds fragments of deleted emails discussing a planned fraud. Applying the principle "deleted data may still be recoverable from unallocated space or slack space" represents using:

A A specific forensic tool's feature.

✓ B Deductive reasoning (applying a general principle of digital forensics to a specific situation).

C A random guess about data location.

D A method guaranteed to recover all deleted data.

98. During expert testimony, a digital forensic examiner is asked a question they don't immediately know the answer to. What is the most appropriate response to maintain credibility?

A Guess the most likely answer.

B Refuse to answer the question.

✓ C State clearly that they do not know or cannot recall the specific detail at that moment, but offer to check their notes or provide the information later if possible.

D Blame the tools used for not providing the information.

99. An essential analytical skill in digital forensics involves reviewing large volumes of log data or file listings to identify entries that are unusual or relevant to the investigation. This skill is best described as:

✓ A Pattern recognition and anomaly detection.

B Data encryption.

C Hardware maintenance.

D Network configuration.

100. An investigator forms an initial hypothesis that an intrusion occurred via a phishing email. What analytical step should follow?

- **A** Immediately conclude the investigation based on the hypothesis.
- **B** Look only for evidence that confirms the phishing hypothesis and ignore other possibilities.
- ✓ **C** Systematically search for evidence supporting the hypothesis (e.g., email logs, browser history, malware artifacts) AND evidence that might refute it or suggest alternative intrusion vectors.
- **D** Delete all logs that don't mention phishing emails.