# ANSWER KEYS

**(Correct Answers are marked in Bold Letters)**

## SECTION-A

1. **If sales increase from 200 units to 260 units, calculate the percentage increase.**
   a. 20%
   b. 25%
   **c. 30%**
   d. 35%
2. **In forensic odontology, the term "Chiloscopy" refers to:**
   a. Study of palatal rugae patterns for identification
   b. Analysis of bite marks on human skin
   **c. Examination of lip print patterns for personal identification**
   d. Microscopic study of dental pulp tissues
3. **Which constitutional body among the following is incorrectly categorized as constitutional?**
   a. Election Commission of India
   b. Union Public Service Commission
   c. Finance Commission
   **d. NITI Aayog**
4. **The cerebellum is primarily associated with:**
   a. Hormonal regulation
   b. Body temperature control
   **c. Coordination of voluntary movements**
   d. Long-term memory storage
5. **Choose the correct preposition: "He is addicted _____ gambling."**
   a. with
   b. for
   **c. to**
   d. on
6. **The null hypothesis ($H_0$) generally represents:**
   a. Maximum certainty
   b. Presumption of guilt
   c. Alternative explanation
   **d. No effect or no difference**
7. **A footwear impression discovered in soft soil should be photographed:**
   a. Close-up scaled photography
   b. Long-range photography
   c. Mid-range photography
   **d. All of the above**
8. **In a positively skewed forensic dataset, the most appropriate measure of central tendency is generally the:**
   a. Mean
   b. Range
   **c. Median**
   d. Variance
9. **Which statement regarding admissibility of forensic evidence is most accurate?**

a. Forensic evidence is admissible only if collected under the Exchange Principle (Locard), regardless of chain of custody.
**b. Reports of Senior Scientific Officers (SSO) in State Forensic Science Laboratories are automatically admissible under Section 293 CrPC and Section 329 BNSS.**
c. Admissibility of forensic evidence is governed by the Best Evidence Rule and requires proper chain of custody and expert testimony.
d. Digital evidence is admissible only if accompanied by oral testimony of the investigating officer, not under Section 65B of the Indian Evidence Act

**10. Which statement regarding expert opinion under the Bharatiya Sakshya Adhiniyam is correct?**
a. Expert opinion is conclusive proof
b. Expert testimony is inadmissible
**c. Expert opinion assists the court in technical matters**
d. Courts are legally bound by expert conclusions

**11. While Calvin Goddard is popularised as the 'father of modern ballistics,' the critical instrumentation, the comparison microscope adapted specifically for comparing bullets side-by-side, was primarily engineered by which of his colleagues at the Bureau of Forensic Ballistics?**
a. Alexandre Lacassagne and Victor Balthazard
**b. Charles Waite and Philip Gravelle**
c. Albert S. Osborn and John Wigmore
d. Paul Kirk and August Vollmer

**12. Dr. E.H. Hankin served as a renowned Chemical Examiner and Bacteriologist in the late 19th and early 20th century. In which Indian city was his laboratory located, famously known for its rigorous medico-legal analysis and foundational work on cholera bacteriophages?**
**a. Agra**
b. Madras
c. Lahore
d. Bombay

**13. Grammar:Language::Formula: ?**
a. Equations
b. Calculations
**c. Mathematics**
d. Numeral

**14. Which of the following best explains the role of the sympathetic nervous system?**
a. Regulation of digestion during rest
b. Control of voluntary skeletal movements only
**c. Activation of the fight-or-flight response**
d. Long-term memory storage

**15. Under the Bharatiya Sakshya Adhiniyam (BSA), 2023, what is the evidentiary status of a video recording that is simultaneously stored on a server and broadcast live?**
a. The server recording is primary; the broadcast is secondary
**b. Both are considered primary evidence**
c. Only the server recording is admissible
d. Both are secondary evidence requiring 65B certification

**16. Bandura's Social Learning Theory emphasizes the importance of which mechanism in the acquisition of behavior?**
a. Genetic predisposition
**b. Observational learning and modeling**
c. Unconscious childhood conflicts
d. Direct reinforcement only

17. **Which constitutional amendment reduced the voting age in India from 21 years to 18 years?**
    a. 42nd Amendment
    b. 44th Amendment
    **c. 61st Amendment**
    d. 73rd Amendment
18. **The headquarters of the World Trade Organization (WTO) is situated in:**
    a. Brussels
    **b. Geneva**
    c. Paris
    d. New York
19. **Which of the following gases is NOT categorized as a greenhouse gas?**
    a. Methane
    **b. Nitrogen**
    c. Carbon dioxide
    d. Nitrous oxide
20. **If observed frequencies and expected frequencies are nearly identical, the Chi-square value will generally be:**
    a. Very high
    b. Negative
    c. Equal to one
    **d. Very low**
21. **Choose the antonym of the word "Ephemeral":**
    a. Fleeting
    b. Temporary
    c. Transient
    **d. Eternal**
22. **Which of the following correctly matches the typical magnifying powers of microscopes commonly used in forensic science?**
    a. Stereo microscope – up to 1000× magnification
    b. Compound light microscope – up to 100× magnification
    c. Comparison microscope – up to 400× magnification
    **d. Electron microscope – up to 1,000,000× magnification**
23. **Which casting material is most suitable for recovering fine tool marks from a steel surface at a crime scene?**
    a. Plaster of Paris
    b. Dental stone
    **c. Mikrosil / Silicone-based casting compound**
    d. Alginate
24. **In forensic analysis, systematic error produces:**
    a. Random fluctuations
    b. Increased objectivity
    c. Greater precision only
    **d. Consistent deviation from the true value**
25. **McNaughten's Rule is primarily associated with:**
    **a. Determination of criminal insanity and understanding of the nature of the act**
    b. Victim compensation mechanisms
    c. Witness examination procedure
    d. Police investigation methods
26. **Which search technique is generally considered most appropriate for a large outdoor crime scene with limited investigators?**
    a. Zone search

b. Spiral search
**c. Strip/Line search**
d. Wheel search

**27. The Scheimpflug principle used in forensic photography states that:**
a. The lens must shift laterally to increase focal depth
b. Lens tilt should remain orthogonal to the subject
c. Hyperfocal distance determines tilt angle
**d. Lens plane, image plane, and subject plane intersect along a common line**

**28. In forensic photogrammetry, which intrinsic camera parameter is essential for extracting accurate three-dimensional measurements?**
a. Camera XYZ coordinates
**b. Principal point and lens distortion coefficients**
c. Tripod pitch-roll-yaw angles
d. Focal plane distance to evidence marker

**29. The first practical application of fingerprinting in criminal identification in India is associated with:**
a. Lord Curzon
**b. Sir William Herschel**
c. Lord Dalhousie
d. Lord Cornwallis

**30. Adipocere formation is seen in:**
a. Dead body exposed to air
**b. Dead body buried in damp, clay soil**
c. Burial in dry hot air
d. All

**31. To accurately photograph bite marks using reflected short-wave ultraviolet radiation (254 nm), the camera lens must be manufactured from which specialized optical material?**
a. Extra-low dispersion glass
**b. Quartz or fluorite**
c. Polycarbonate-coated optics
d. Barium crown glass

**32. Which of the following is NOT recognized as a metabolite of diazepam?**
**a. Lorazepam**
b. Temazepam
c. Oxazepam
d. Desmethyldiazepam

**33. The classical confirmatory test for arsenic poisoning is known as:**
a. Marquis test
b. Mandelin's test
**c. Marsh test**
d. Vitali's test

**34. Which of the following alkaloids belongs to the Isoquinoline group?**
a. Morphine
b. Cocaine
**c. Papaverine**
d. Reserpine

**35. Which of the following compounds belongs to the class of polychlorinated hydrocarbons?**
a. Malathion
b. Parathion
**c. Endrin**
d. Diazinon

**36. Which among the following poisons is volatile in nature?**
- **a. Cyanide**
- b. Methyl parathion
- c. Brucine
- d. All of the above

**37. The Bharatiya Nyaya Sanhita primarily governs:**
- a. Civil disputes
- b. Administrative tribunals
- c. Rules of evidence
- **d. Substantive criminal law**

**38. "Who propounded the term 'White-Collar Crime'?"**
- a. Cesare Lombroso
- **b. Edwin Sutherland**
- c. Emile Durkheim
- d. Karl Marx

**39. For photographing tyre impressions at night, the best lighting technique is:**
- a. Flash directly from above
- **b. Oblique lighting at low angle from multiple sides**
- c. No light needed
- d. UV light only

**40. Within the scope of forensic anthropology and pathology, establishing the 'cause' of death is distinct from determining the 'manner' of death. Which of the following represents an accurate limitation regarding the scope of forensic anthropology in this context?**
- **a. Forensic anthropology generally cannot definitively establish the physiological cause of death; it only characterizes the skeletal trauma associated with the fatal event.**
- **b.** Forensic anthropology can definitively determine a homicide manner of death based solely on the presence of a peri-mortem sharp force trauma lesion.
- **c.** Forensic anthropology is uniquely qualified to establish the physiological cause of death when advanced decomposition prevents soft tissue toxicology.
- **d.** Forensic anthropology's primary scope is to utilize the Law of Progressive Change to determine the cause of death via isotopic bone analysis.

**41. Arrange the following cannabis preparations in ascending order of tetrahydrocannabinol (THC) concentration: Bhang, Ganja, Charas, Hashish oil.**
- **a. Bhang → Ganja → Charas → Hashish oil**
- b. Ganja → Bhang → Charas → Hashish oil
- c. Hashish oil → Charas → Bhang → Ganja
- d. Ganja → Hashish oil → Charas → Bhang

**42. Which factor is MOST important in determining the credibility of an expert witness in court?**
- a. duration of experience in relevant field
- b. Number of appearances in court
- **c. Scientific qualifications, expertise, and methodology adopted**
- d. type of evidences collected by the experts

**43. Choose the option nearest in meaning to the word 'Obfuscate':**
- a. Clarify
- b. Illuminate
- **c. Confuse intentionally**
- d. Simplify

**44. Free legal aid to ensure equal justice is provided under which Article of the Indian Constitution?**
- a. Article 21

**b. Article 39A**
c. Article 32
d. Article 36

**45. Which of the following is considered transient evidence?**
a. Fingerprints
b. Bloodstains
**c. Oduor**
d. Footwear impressions

**46. In information technology and ergonomics, "HCI" refers to:**
a. High Computer Internet
b. High Computer Interference
c. Hold Human Complex
**d. Human Computer Interaction**

**47. Which of the following is NOT recognized as a fundamental principle of forensic science?**
a. Principle of Exchange
**b. Principle of Relativity**
c. Principle of Individuality
d. Principle of Probability

**48. Which element among the following possesses the highest electron affinity?**
a. Nitrogen
b. Oxygen
c. Fluorine
**d. Chlorine**

**49. The Implicit Association Test (IAT), developed by Greenwald et al. (1998), is primarily designed to assess:**
a. Perception
b. Attention
**c. Implicit prejudice and attitudes**
d. Intelligence quotient

**50. Which chromatographic technique is most suitable for separation of non-volatile compounds?**
a. GCMS
b. Gas chromatography
c. GCHS
**d. HPLC**

# SECTION-B

**51. According to the order of volatility, which data source should be collected FIRST?**
a. Temporary files
**b. CPU registers and cache**
c. Hard disk contents
d. Backup tapes

**52. Chain of custody in digital forensics refers to:**
a. The order in which data is encrypted during acquisition to keep it safe from contamination
b. A list of witnesses presents during evidence collection from the scene of crime
**c. A documented chronological record showing the seizure, custody, control, transfer, and disposition of evidence**
d. The process of backing up evidence to cloud storage for safe custody

**53. Before writing a forensic image to a destination drive, what process should be performed to ensure no residual data remains?**
**a. Disk sanitization**
b. Formatting with FAT32
c. Quick format with NTFS
d. Running CHKDSK

**54. Which volatile evidence is captured in a memory dump that CANNOT be retrieved from the hard disk?**
a. Installed software list
**b. Running processes, and open network connections**
c. Windows Registry hives and Dwords
d. Prefetch files and eventlogs

**55. File carving is a forensic technique used to:**
a. Encrypting and decrypting files for secure transport
b. Extract metadata from file headers and footers
c. Copy selected files from a live system
**d. Recover files from unallocated disk space based on file signatures**

**56. Which of the following is NOT a standard forensic image format?**
a. EnCase (E01)
b. Raw (DD)
c. Advanced Forensics Format (AFF)
**d. ISO 9660 (I96)**

**57. The Windows pagefile (pagefile.sys) is forensically significant because:**
a. It stores backup copies of the Windows Registry and all the hives
b. It records all user login events and backup copy of all the events
**c. It can contain remnants of previously running processes, passwords, and decrypted file contents swapped from RAM**
d. It contains prefetch data for recently used applications

**58. Windows Registry hive NTUSER.DAT is associated with which of the following?**
a. System-wide hardware configuration
**b. Per-user settings and preferences stored in the user's profile**
c. Security Account Manager database with encrypted keys
d. Software and hardware installation records for all users of the system

**59. Shellbags in Windows Registry records, which forensically significant information?**
a. Recently opened documents

b. Installed browser extensions and software
c. Network connections made by the user for the last 15 days
**d. Folder browsing history including folders accessed on external drives, even after deletion**

**60. In a Recycle Bin forensic investigation on NTFS (Windows), a deleted file's metadata (original path, deletion time, file size) is stored in which file type?**
**a. $I files**
b. $R files
c. INFO2 records
d. Thumbs.db entries

**61. Which Linux log file records authentication events including successful and failed SSH logins?**
a. /var/log/syslog (RHEL/CentOS) or /var/log (Debian/Ubuntu)
**b. /var/log/auth.log (Debian/Ubuntu) or /var/log/secure (RHEL/CentOS)**
c. /var/log/kern.log (RHEL/CentOS) or /var/log/shadow (Debian/Ubuntu)
d. /etc/shadow (Debian/Ubuntu) or /etc/kern.log (RHEL/CentOS)

**62. On macOS, Property List (plist) files are used to store application settings and user preferences. In which format are modern plist files typically stored?**
a. Plain text XML only
b. JSON format exclusively (cdlist format)
c. SQLite database (dblist format)
**d. Binary plist (bplist) or XML format**

**63. An investigator wants to find which websites a suspect visited recently even after browser history was cleared. Which artifact might still contain this information?**
**a. DNS cache and browser cache files stored on disk**
b. Bookmark file and Bookmark videos
c. Browser extension list and intentions list
d. Installed plugins folder

**64. Anti-forensic techniques used by malware to evade analysis include:**
a. Using only plaintext network communications
b. Using well-known and documented exploits to cover the data from the user
c. Generating detailed logs of their activity by placing all the logs system in one place to access
**d. Code obfuscation, packing, encryption, timestamp manipulation, and detecting sandbox environments to alter behavior**

**65. In 5G network forensics, compared to 4G LTE, a key investigative challenge is:**
**a. 5G's use of network slicing, edge computing, and massive IoT connectivity creates more distributed and complex evidence trails**
b. 5G uses older encryption making it easier to intercept by the attacker to get the data
c. 5G devices do not generate any logs
d. 5G eliminates cellular towers, making location tracking impossible

**66. Firmware analysis of an IoT device is forensically valuable because:**
a. Firmware contains only manufacturer information
b. Firmware changes are impossible to detect and no information can be retrieved
c. Firmware is always encrypted and cannot be analyzed
**d. Firmware can contain hardcoded credentials, encryption keys, backdoors, and reveal the device's capabilities and vulnerabilities**

**67. The Caesar cipher is a type of:**
a. Transposition symmetric cipher
**b. Monoalphabetic substitution cipher**
c. Polyalphabetic transposition cipher
d. Asymmetric cipher

**68. RSA encryption security is based on the computational difficulty of:**

a. Solving discrete logarithm problems
b. Computing elliptic curve points
**c. Factoring large prime numbers**
d. Reversing hash functions

**69. Differential Cryptanalysis attacks work by:**
**a. Studying how differences in plaintext pairs propagate through a cipher to recover key information statistically**
b. Testing all possible keys exhaustively
c. Intercepting key exchange messages
d. Exploiting implementation bugs in cryptographic libraries present in the algorithm

**70. In cloud forensics involving social media, session tokens stored in browser cookies are forensically valuable because they:**
a. Reveal the user's encryption keys
b. Investigator can assess the token data containing all the user's message history in plaintext
**c. Investigators can authenticate as the user and access account data without needing the actual password**
d. Only contain advertising preferences

**71. Misinformation campaigns on social media can be investigated forensically by analyzing:**
a. Only the text content of posts of the user
**b. Account creation dates, shared IP addresses, and metadata of shared media**
c. Follower counts alone in different social media
d. User age and gender demographics pattern of the user along with their background colour

**72. The ElGamal signature scheme derives its security from the:**
a. Integer factorization problem
**b. Discrete logarithm problem over a finite field**
c. Elliptic curve point multiplication problem
d. Shortest vector problem in lattices

**73. Volume Shadow Copies (VSS) in Windows are forensically significant because:**
**a. They maintain snapshots of files and the registry at previous points in time**
b. They provide real-time system monitoring from the shadow file of the windows
c. They encrypt backup copies of files automatically
d. They log all user keystrokes

**74. Which standard defines the forensic examination of digital evidence?**
a. ISO 27001
b. RFC 2196
c. PCI-DSS
**d. NIST SP 800-86**

**75. In VPN forensics, what forensic artifact might reveal that a suspect used a VPN service even if VPN client logs are deleted?**
a. Installed fonts list to know which text was used
**b. Network interface configuration files, Registry entries, DNS query logs, and firewall logs showing connections to known VPN endpoints**
c. Desktop wallpaper settings, screen resolution and screen savers setting
d. Browser bookmark files

**76. In cloud storage forensics, which type of cloud log would most likely capture evidence of unauthorized file access or download?**
a. Billing and cost management logs
**b. Object-level access logs**
c. Network latency performance logs
d. Virtual machine CPU utilization logs

77. **In Android forensics, the /data/data/ directory is forensically significant because it contains:**
    a. System firmware and bootloader files
    b. Android OS core system files and the temporary file
    c. Downloaded media files visible to the user
    **d. SQLite databases, shared preferences, and cached data**
78. **Forensic analysis of a Windows system reveals the file "C:\Users\Public\evil.exe" was executed. Which artifact would most likely confirm this execution?**
    a. Browser history files
    b. Recycle Bin contents
    **c. Prefetch files**
    d. Desktop.ini file
79. **Which phenomenon occurs when two different inputs to a hash function produce the same hash output?**
    a. Pre-image attack
    **b. Hash collision**
    c. Birthday attack
    d. Avalanche effect failure
80. **Which Windows artifact stores folder view settings and browsing preferences that can reveal accessed directories even after their contents are deleted?**
    **a. Shellbags**
    b. Prefetch files
    c. Thumbs.db files
    d. Application event logs
81. **The $UsnJrnl ($J data stream) in NTFS records:**
    a. User login and logout events
    **b. A chronological record of all file system changes providing a file activity timeline**
    c. USB device connection history including the date of the USB attached
    d. Network interface configuration changes and data streaming history
82. **On a Linux system, symbolic links (symlinks) can be forensically significant because:**
    a. They always contain encrypted data in a symbolic format
    b. Symlinks prevent forensic tools from reading file contents of the system and the attacker cannot be caught
    c. Symlinks are permanent and cannot be deleted
    **d. Symlinks can be used to redirect file access to sensitive locations, revealing privilege escalation paths or data exfiltration techniques**
83. **The macOS "Spotlight" index can be forensically valuable because:**
    a. It stores decrypted versions of all encrypted files in a safe location
    b. It logs all network connections made by the system, making it easy to find the connected devices
    **c. It maintains metadata about indexed files, potentially revealing deleted file names and content snippets**
    d. It backs up all user preferences to iCloud
84. **A "fileless malware" attack is particularly difficult to detect forensically because:**
    **a. It operates in memory using legitimate tools, leaving minimal disk traces for traditional forensic analysis**
    b. It uses files with unusual extensions that tools cannot detected and traced
    c. It encrypts itself with military-grade encryption and very difficult to decrypt
    d. It only targets Linux systems which lack forensic tools
85. **In container forensics (e.g., Docker), which forensic artifact is particularly ephemeral and likely to be lost?**
    a. Container image layers stored in a registry and it will be as an image file

b. The Docker daemon's configuration file and it can be access if it is removed and reattached with the device
**c. The container's writable layer and memory state — lost when container is stopped and removed**
d. The Dockerfile used to build the image

**86. Blowfish encryption is characterized by which of the following?**
a. A 128-bit fixed block size with variable key length with symmetric key structure
**b. 64-bit block size, variable key (32–448 bits), Feistel network, expensive key setup**
c. A 256-bit block size designed for hardware implementation only
d. Use of asymmetric key pairs

**87. A forensic examination reveals that Windows Event Logs have been cleared. Which artifact can still provide evidence of system activity before the logs were cleared?**
**a. Volume Shadow Copies, Event ID 1102/104, SIEM logs, and application logs in other locations**
b. The Recycle Bin contents such as image files, doc file and exe files
c. The pagefile.sys only
d. Prefetch files only

**88. Data exfiltration via DNS tunneling works by:**
a. Overloading DNS servers with requests to steal cached records and exploiting the records to access
b. Poisoning DNS records to redirect traffic to attacker servers
c. Using DNSSEC to encrypt exfiltrated data
**d. Encoding stolen data within DNS queries/responses to an attacker-controlled domain, exploiting typically unrestricted DNS egress**

**89. Windows "Thumbs.db" and "thumbcache_*.db" files are forensically important because they:**
a. Store Windows Update installation logs including the information of data accessed
b. Store application crash dump information which make the investigator possible to retrieve the deleted files
c. Cache Windows Explorer search results
**d. Cached thumbnails of previously viewed files persisting even after originals are deleted**

**90. Which of the following describes the forensic significance of Windows "Event Tracing for Windows" (ETW)?**
a. ETW is used exclusively for game performance optimization which will also track all the events of the game
b. ETW stores all user typed passwords for recovery and used to track the changes in the password made by the user
**c. ETW is a Kernel-level tracing capturing process creation, network connections, and file access in high detail even when traditional event logs are cleared**
d. ETW is only active when Windows Defender is running

**91. In digital forensics, the term "metadata laundering" refers to:**
a. Cleaning metadata from files before sharing in social media to protect privacy of the users
**b. Deliberately manipulating/removing metadata to obscure origin, creation date, or authorship**
c. Converting metadata from one format to another during analysis and preserving it as evidence
d. The automatic metadata stripping performed by social media platforms in order to make the file lighter

**92. QR code-based attacks on mobile devices can facilitate which security threats**?
a. QR codes can directly execute code without user interaction and convert all the data to unreadable format
**b. QR codes can redirect to phishing sites, initiate payments, connect to rogue Wi-Fi, or download malicious apps**
c. QR codes can only display text and pose no security risk
d. QR codes only work with Android devices

**93. "Key escrow" in encryption systems refers to:**

a. The process of deriving encryption keys from passwords to another password
b. Automatically rotating encryption keys on a schedule
c. Using multiple keys to encrypt the same data
**d. Encryption keys held by a trusted third party for authorized access**

**94. "Volatile data" that must be captured first in a live forensic investigation includes all of the following EXCEPT:**
a. Contents of RAM
b. Network connections
**c. Data stored on optical discs**
d. Running processes

**95. In smart vehicle forensics, which data sources within a modern connected vehicle can provide evidence relevant to criminal investigations?**
**a. The vehicle's Event Data Recorder (EDR), GPS history, Bluetooth paired devices, cellular logs, infotainment artifacts, phone integration data, and telematics server data**
b. The vehicle's VIN (Vehicle Identification Number), Chassis Number, Engine Electronic Assembly Number, and Software version
c. Only the fuel level and odometer reading
d. Only the vehicle's speedometer reading at the time of seizure

**96. What does the "dd if=/dev/sda of=image.dd bs=512" command do?**
a. Encrypts disk
b. Deletes files
**c. Creates a disk image**
d. Clones partitions

**97. A forensic investigator wants to prevent remote wiping of a seized smartphone. What should be done FIRST?**
a. Reboot the phone
**b. Place the device in airplane mode or Faraday isolation**
c. Remove the SIM immediately without documentation
d. Factory reset the device

**98. Which forensic image format supports compression and metadata?**
a. .iso
b. .img
c. .raw
**d. .E01**

**99. Which log file best shows user logon and logoff events in Windows?**
a. setupact.log
b. eventlog.evxt
c. secpol.log
**d. security.evtx**

**100 During static malware analysis, which action is MOST appropriate?**
a. Executing malware on production systems
**b. Examining strings, headers, and binaries without execution**
c. Disabling antivirus permanently
d. Connecting malware to the internet

**101 In cryptocurrency forensics, what is the role of a blockchain explorer?**
a. Creates wallets
b. Anonymizes transactions identify
**c. Tracks transactions on the blockchain**
d. Mines coins

**102 What does NTFS stand for?**

a. Network Transfer File System
**b. New Technology File System**
c. Non-Transfer File System
d. Native Table File System

**103 Which attack exploits information leaked through timing, power consumption, or electromagnetic emissions?**
a. Replay attack
**b. Side-channel attack**
c. Chosen-ciphertext attack
d. SQL injection

**104 In wireless forensics, the process of capturing probe request frames can reveal:**
a. The encryption key of the connected network and other devices
b. The file transfer history over Wi-Fi
c. The web browsing history of the device
**d. The SSIDs of networks that a device has previously connected to**

**105 Which IoT communication protocol is a lightweight request-response protocol suitable for constrained devices and often used over UDP?**
**a. CoAP**
b. MQTT
c. HTTP/2
d. WebSocket

**106 A forensic analyst extracts a physical dump from a solid-state drive (SSD). When checking the hash values of two consecutive acquisitions taken 1 hour apart without any intermediate system interactions, the analyst discovers the hashes do not match. Assuming no hardware failure, what internal SSD process caused this?**
a. The NTFS $MFT table self-destructing sequence
**b. Background garbage collection and wear leveling driven by the SSD controller firmware via the TRIM command**
c. The SATA interface automatically applying random salt to prevent unauthorized duplicate dumps
d. The TPM chip resetting its public key

**107 index nodes (inodes) are used in:**
a. NTFS
b. FAT
**c. Linux file systems**
d. exFAT

**108 Bluetooth operates in which frequency band?**
a. 900 MHz
**b. 2.4 GHz**
c. 5 GHz
d. 60 GHz

**109 Which type of cookie is <u>MOST</u> commonly used for cross-site tracking and is restricted by modern browsers due to privacy concerns?**
a. Session cookies
b. First-party cookies
**c. Third-party cookies**
d. Secure cookies

**110 The forensic challenge of "data heterogeneity" in IoT investigations refers to:**
**a. Vast variety of architectures, OS, file systems, protocols, and proprietary formats requiring specialized tools per device type**
b. IoT devices producing too much data make it challenging for investigators to store in a simple workstation for investigation

c. IoT data being stored exclusively in the cloud
d. IoT devices using only wireless connections

**111 During DVR seizure, which method ensures the MOST forensically sound acquisition of volatile and non-volatile data?**
a. Powering off immediately and removing HDD
**b. Live acquisition followed by controlled shutdown**
c. Cloning HDD without documentation
d. Using screen recording only

**112 Which field in a TCP header is MOST useful for detecting packet reordering during forensic reconstruction?**
a. Window size
**b. Sequence number**
c. Checksum
d. Urgent pointer

**113 Which technique is MOST effective for detecting kernel-level rootkits that hide processes and files?**
a. File system scanning
b. Signature-based antivirus
**c. Memory forensics using trusted external tools**
d. Log file analysis

**114 Which identifier is MOST useful for tracking a subscriber across different devices in a forensic investigation?**
a. IMEI
b. MAC address
**c. IMSI**
d. IP address

**115 Which acquisition method provides the MOST complete data, including deleted artefacts?**
a. Logical acquisition
b. Manual acquisition
**c. Physical acquisition**
d. Screenshot capture

**116 What is the PRIMARY advantage of CoAP (Constrained Application Protocol) over HTTP (Hypertext Transfer Protocol) in IoT environments?**
a. Uses TCP
b. Higher latency
**c. Runs over UDP with lower overhead**
d. Supports only encryption

**117 Which method ensures the MOST legally admissible evidence collection from social media platforms?**
a. Screenshot capture
**b. API-based collection with proper chain of custody**
c. Copy-paste text
d. Manual observation with proper chain of custody

**118 OSINT techniques primarily rely on:**
a. Encrypted data only
**b. Publicly available information**
c. Deleted files
d. Internal databases

**119 Compared to RSA (Rivest-Shamir-Adleman) cryptosystem, ECC (Elliptic Curve Cryptography) achieves equivalent security with:**
a. Larger keys

b. Equal key sizes
**c. Smaller keys**
d. Variable but unpredictable key sizes

**120 Which artifact is best for confirming USB device usage?**
a. Prefetch files
b. Event logs
**c. Setupapi.dev.log**
d. Pagefile.sys