ANSWER KEYS

(Correct Answers are marked in bold letters)

SECTION-A

1. **Which of the following is considered pattern evidence?**
   - **a. Fingerprints**
   - b. Blood group
   - c. DNA
   - d. All of the above
2. **Which of the following is a class characteristic of firearms evidence?**
   - **a. Caliber**
   - b. Unique striation marks
   - c. Firing pin impression
   - d. Breech face marks
3. **The National Forensic Sciences University (NFSU) was formally established in India in which year?**
   - a. 2015
   - **b. 2020**
   - c. 2010
   - d. 2000
4. **Digital evidence must be authenticated using:**
   - a. Encryption keys
   - b. Passwords
   - **c. Hash values**
   - d. Firewalls
5. **Precision in forensic measurement refers to:**
   - a. Closeness to true value
   - **b. Repeatability of results**
   - c. Accuracy of instruments
   - d. Standardization
6. **The headquarters of the International Court of Justice is located at:**
   - a. Paris
   - **b. The Hague**
   - c. Geneva
   - d. New York
7. **In forensic handwriting analysis, the most common stroke pattern represents:**
   - a. Mean
   - **b. Mode**
   - c. Median
   - d. Range
8. **In forensic ballistics, the average velocity of bullets is calculated using:**
   - a. Mode
   - **b. Mean**
   - c. Median
   - d. Range
9. **In forensic DNA profiling, probability calculations are used to:**
   - **a. Determine allele frequency**
   - b. Determine Gene frequency
   - c. Determine DNA frequency
   - d. Determine STR frequency

10. **Which design feature is most commonly found on revolver cartridges to prevent them from slipping through the cylinder?**
    a. Extractor groove
    b. Rimmed case head
    c. Tapered body
    d. Rebated rim
11. **The null hypothesis in forensic hypothesis testing usually states:**
    a. Evidence is conclusive
    b. No significant difference exists
    c. Suspect is guilty
    d. Witness is reliable
12. **Bharatiya Nyaya Sanhita (BNS), 2023 replaces which earlier legislation?**
    a. Indian Penal Code, 1860
    b. Indian Evidence Act, 1872
    c. Code of Criminal Procedure, 1973
    d. Indian Contract Act, 1872
13. **Which area of the hand is considered the primary target for GSR collection because it is most likely to catch discharge gases?**
    a. The palm and the base of the wrist
    b. The fingertips and under the fingernails
    c. The web area between the thumb and index finger
    d. The knuckles and outer edge of the pinkie finger
14. **Under which section of Indian law provision have been made that the Court can form an opinion by an expert upon a point of science**
    a. Section 39 of BSA
    b. Section 47 of BSA
    c. Section 329 of BNSS
    d. Section 45 of BSA
15. **Within forensic anthropology, which limitation applies when determining cause versus manner of death?**
    a. Cannot definitively establish physiological cause of death; only skeletal trauma
    b. Can always determine homicide manner from sharp force trauma
    c. Can uniquely establish physiological cause when decomposition prevents toxicology
    d. Uses isotopic bone analysis to determine cause of death
16. **Faraday bags used for mobile devices block RF signals by:**
    a. Altering wavelength of signals
    b. Generating active jamming signals
    c. Creating conductive enclosure that cancels fields
    d. Absorbing RF waves into thermal energy
17. **When examining a crime scene for specific fibres or fluorescent powders, why is 365 nm (Longwave) typically preferred over 254 nm (Shortwave)?**
    a. Shortwave UV is too weak to cause fluorescence.
    b. Longwave UV is safer for the eyes and skin during prolonged searches.
    c. Shortwave UV only works on dark-coloured surfaces.
    d. Longwave UV penetrates deep into the substrate to find hidden blood.
18. **Which Indian institution collaborated with the ICRC to establish a humanitarian forensics initiative?**
    a. National Forensic Sciences University (NFSU)

b. All India Institute of Medical Sciences (AIIMS)
c. Central Bureau of Investigation (CBI)
d. National Crime Records Bureau (NCRB)

19. **Which parameter in a gait pattern refers to the angle formed between the "line of progression" and the "long axis of the foot"?**
a. Step Width
b. Foot Angle (or Toe-out/Toe-in angle)
c. Stride Length
d. Cadence

20. **Which ISO number is for the competence and quality assurance of forensic science laboratories (testing and calibration)?**
a. ISO/IEC 9001
b. ISO/IEC 14001
c. ISO/IEC 17025
d. ISO/IEC 27001

21. **Which Indian state has the largest coastline?**
a. Kerala
b. Gujarat
c. Andhra Pradesh
d. Maharashtra

22. **Choose the word that best completes the analogy:**
Ephemeral: Permanent: Transparent?
a. Opaque
b. Clear
c. Translucent
d. Bright

23. **Which of the following sentences contains an error?**
a. Neither of the boys is guilty.
b. Each of the players are ready.
c. Everyone has submitted the form.
d. Much has been done already.

24. **A train 180 m long crosses a pole in 9 seconds. What is its speed?**
a. 60 km/h
b. 72 km/h
c. 80 km/h
d. 90 km/h

25. **The ratio of ages of A and B is 3:5. If A is 24 years old, what is B's age?**
a. 36 years
b. 40 years
c. 30 years
d. 28 years

26. **Find the missing term: 7, 14, 28, 56,?**
a. 84
b. 112
c. 126
d. 98

27. **Assertion: Photography of the scene of crime plays a very important role in crime scene investigation.**
Reason: What a human may not be able to see can be recorded by a camera.
a. Both Assertion and Reason are false
b. Both Assertion and Reason are true

c. Assertion is true but Reason is false
d. Assertion is false but Reason is true

28. **The jury system in India was formally abolished after which landmark case exposed its weaknesses in impartiality and susceptibility to public/media influence?**
    a. K.M. Nanavati v. State of Maharashtra
    b. Kesavananda Bharati v. State of Kerala
    c. Indira Gandhi v. Raj Narain
    d. State of Uttar Pradesh v. Rajesh Talwar
29. **In a certain code, "ROAD" is written as "URDG". How is "PATH" written?**
    a. SDWK
    b. QBUJ
    c. RCUK
    d. TCVL
30. **Which global pioneer is known as the "Father of Criminalistics"?**
    a. Hans Gross
    b. Edmond Locard
    c. Alphonse Bertillon
    d. Francis Galton
31. **The acronym ISO, widely referenced in forensic laboratories and quality assurance systems, stands for:**
    a. International Security Organization
    b. International Standards Organization
    c. International Organization for Standardization
    d. International Scientific Observatory
32. **Which of the following is not a class characteristic of evidence?**
    a. Shoe size
    b. Fiber type
    c. DNA profile
    d. Caliber of firearm
33. **The chain of custody ensures:**
    a. Evidence is admissible in court
    b. Evidence is stored permanently
    c. Evidence is photographed
    d. All of the above
34. **Which fingerprint development technique is most effective on non-porous surfaces?**
    a. Ninhydrin
    b. Cyanoacrylate fuming
    c. Silver nitrate
    d. Iodine fuming
35. **Which microscope is most suitable for examining trace fibres?**
    a. Compound microscope
    b. Electron microscope
    c. Stereo microscope
    d. Phase contrast microscope

36. **If the probability of finding a specific fibre at a crime scene is 0.02, what is the probability of not finding it?**
    a. 1.00
    b. 0.98
    c. 0.20

d. 98.98

37. **The Chi-square test statistic is calculated as:**
    a. Σ(Observed – Expected)² / Expected
    b. Σ(Observed – Expected) / Expected
    c. Σ(Observed × Expected)
    d. Σ(Observed + Expected)
38. **Measurement of uncertainty is crucial in forensic science because:**
    a. It quantifies reliability of results
    b. It eliminates errors
    c. It replaces expert testimony
    d. None of the above
39. **In criminal trials, the "CSI Effect" is most accurately described as:**
    a. The tendency of forensic experts to exaggerate scientific findings in court to secure convictions.
    b. The influence of crime television shows on jurors' expectations regarding the availability and conclusiveness of forensic evidence.
    c. The psychological trauma experienced by investigators after repeated exposure to violent crime scenes.
    d. The procedural bias created when investigators rely exclusively on circumstantial evidence instead of forensic science.
40. **Arrange the changes that appear in a cadaver in sequential order.**
    a. Rigor, Marbling, Cooling, Mummification
    b. Cooling, Rigor, Mummification, Marbling
    c. Cooling, Rigor, Marbling, Mummification
    d. Rigor, Cooling, Marbling, Mummification
41. **Preservation of surface dust print of footprint cannot be done by the following:**
    a. Photography method
    b. Tracing method
    c. Electrostatic method
    d. Casting method
42. **Arrange the following steps of criminal investigation in a proper sequence:**
    I) Preservation of physical evidences
    II) Photography and sketching
    III) Protection of scene of crime
    IV) Information related to crime
    a. I, III, IV, II
    b. III, IV, II, I
    c. IV, III, II, I
    d. II, I, IV, III
43. **The Frye v. United States (1923) case introduced the "general acceptance" test. Which scientific method was being proposed?**
    a. Truth serum interview with scopolamine
    b. Acoustic spectrographic voice analysis
    c. Probability matrix for ridge identification
    d. Systolic blood pressure deception test
44. **Which forensic scientist pioneered fingerprint classification in India?**
    a. B.N. Mullick
    b. Hem Chandra Bose
    c. Lalji Singh
    d. P.C. Mahalanobis
45. **Which principle in forensic science asserts that while individuals may lie, the evidence and facts themselves remain truthful?**

a. Locard's Exchange Principle
b. Law of Individuality
c. Principle of Analysis
d. None of the above

46. **Which landmark Indian case established admissibility of expert scientific evidence?**
a. State of Maharashtra v. Damu
b. Kesavananda Bharati v. State of Kerala
c. Maneka Gandhi v. Union of India
d. None of the above

47. **Which case is recognized as the first in the world to be solved using DNA fingerprinting evidence?**
a. O.J. Simpson case (1995, USA)
b. Colin Pitchfork case (1987, UK)
c. Green River Killer case (2001, USA)
d. Josef Mengele identification (1985, Brazil)

48. **Which of the following is a non-destructive forensic analysis technique?**
a. Fourier Transform Infrared Spectroscopy (FTIR)
b. Atomic Absorption Spectroscopy (AAS)
c. Gas Chromatography – Mass Spectrometry (GC_MS)
d. Inductively Coupled Plasma-Optical Emission Spectroscopy (ICP-OES)

49. **Which of the following is a quality assurance measure in forensic laboratories?**
a. Peer review of reports
b. Destroying old evidence
c. Ignoring inconclusive results
d. Skipping calibration

50. **Which forensic discipline historically struggles most with Popperian falsifiability due to reliance on subjective interpretation?**
a. Forensic DNA Profiling
b. Forensic Toxicology
c. Bitemark Analysis
d. None of the above

SECTION-B

51. **A hard disk is formatted with MBR. What is the maximum number of primary partitions supported?**
    a. 2
    b. 4
    c. 8
    d. 16
52. **In a GUID Partition Table (GPT), where is the backup copy of the partition table stored?**
    a. At the beginning of the disk in sector 0
    b. In the volume boot record
    c. In the MBR protective partition
    d. At the end of the disk in the last 33 sectors
53. **Which of the following timestamps is typically NOT stored in NTFS MFT metadata?**
    a. File creation time ($STANDARD_INFORMATION)
    b. Last access time
    c. Last write time
    d. File print time
54. **Which of the following best describes "slack space" in digital forensics?**
    a. The unused space within the last cluster of a file
    b. Unallocated disk space between partitions
    c. Space reserved for the OS swap file
    d. Free space in the recycle bin
55. **During the boot process, which firmware standard replaces the legacy BIOS and supports GPT partitioning natively?**
    a. CMOS
    b. POST
    c. UEFI
    d. MBR
56. **In an SQL Injection attack, which of the following input payloads is most commonly used to test for vulnerability?**
    a. <script>alert(1)</script>
    b. ' OR '1'='1
    c. ../../../etc/passwd
    d. ; DROP DATABASE;
57. **Which cyber attack intercepts communication between two parties without their knowledge?**
    a. DoS attack
    b. Replay attack
    c. Man-in-the-Middle (MITM) attack
    d. Brute force attack
58. **Packet sniffing in promiscuous mode allows an attacker to:**
    a. Send forged packets to all hosts from different network
    b. Capture all packets on the network segment regardless of destination
    c. Inject malicious code into packets from a single network
    d. Block network traffic from a specific IP

59. **The purpose of a write blocker in forensic data acquisition is to:**
    a. Speed up the imaging process in the destination drive
    b. Compress the forensic image file from all devices

c. Encrypt the data before imaging
d. Prevent any write operations to the original evidence drive

60. **A forensic image that is a sector-by-sector copy of the original disk including unallocated space is called:**
a. Physical image
b. Logical image
c. Sparse image
d. Compressed image

61. **LNK (shortcut) files in Windows are forensically valuable because they can reveal:**
a. Encrypted passwords of the file, folders and emails of the user
b. The original file path, timestamps, volume serial number, and MAC address of network-accessed files
c. Browser history of the user from different browsers and application
d. Contents of deleted emails and chats

62. **On Linux systems, the file that stores the command history for a bash user session is typically:**
a. /var/log/auth.log
b. ~/.bash_history
c. /etc/passwd
d. /proc/history/bash

63. **The macOS Keychain is forensically significant because it stores:**
a. System hardware information with details of the user
b. Saved passwords, certificates, encryption keys, and Wi-Fi credentials
c. Time Machine backup logs and data retrieval methods
d. Safari browsing history

64. **Which email protocol allows an investigator to retrieve emails while keeping copies on the mail server (useful for forensic examination)?**
a. POP3
b. SMTP
c. IMAP
d. MIME

65. **Which video codec is commonly used by modern NVR systems for efficient video compression?**
a. MP3 or MP4
b. H.264 or H.265
c. MPEG-1 or MPEG-2
d. FLAC

66. **A SYN Flood attack exploits which mechanism in TCP to exhaust server resources?**
a. TCP FIN sequence
b. TCP's three-way handshake
c. TCP sliding window mechanism
d. TCP urgent pointer field

67. **Evidence collected from network routers for forensic investigation may include:**
a. Contents of user hard drives, pen drive, optical drive and other external storage devices
b. Encrypted user passwords of the files and folders
c. Routing tables, ARP tables, NAT translations, access control logs, and DHCP lease records
d. Browser history of connected devices

68. **Indicators of Compromise (IoC) in malware forensics include:**
a. Normal system event logs that are not recorded in the system and network devices
b. User's browsing preferences
c. Manufacturer's hardware serial numbers, make and model numbers

d. Suspicious file hashes, malicious IP addresses, anomalous registry keys, and unusual process names

69. **IMEI (International Mobile Equipment Identity) is a unique identifier assigned to:**
   a. The SIM card
   b. The mobile device hardware
   c. The mobile network operator
   d. The user's mobile account

70. **In mobile forensics, JTAG extraction is used when:**
   a. Standard logical extraction is unavailable
   b. The phone is in excellent working condition and logical extraction is possible
   c. The phone is connected to a Wi-Fi network connection
   d. The investigator wants to extract SIM card data only

71. **A SIM card can contain forensically significant data including:**
   a. Full email inbox and OTT application data of the user
   b. GPS location history and e-marketing data
   c. IMSI, phone book contacts, SMS messages, and last dialed numbers
   d. Application download history

72. **WEP (Wired Equivalent Privacy) is considered insecure because:**
   a. It uses 256-bit encryption which is too strong for most routers
   b. It does not support wireless networks
   c. It only works with 2.4GHz frequency bands
   d. It uses weak RC4 encryption with short static IVs and lacks proper key management

73. **The MQTT protocol used in IoT devices operates on which communication model?**
   a. Publish-subscribe messaging via a broker
   b. Client-server with HTTP
   c. Peer-to-peer encrypted tunnel
   d. UDP broadcast only

74. **In social media evidence collection, OSINT (Open Source Intelligence) direct method without login is most appropriate when:**
   a. The suspect's account is private and requires login credentials
   b. The investigator has a warrant to access private messages
   c. Publicly available information needs to be collected without creating an account
   d. API access has been denied by the platform

75. **Geolocation tracking in social media forensics can be achieved through:**
   a. EXIF metadata in uploaded photos, and geotagged posts
   b. Reviewing account creation date and time
   c. Monitoring friend list changes
   d. Analyzing text content of posts only

76. **AES (Advanced Encryption Standard) uses which block size?**
   a. 56 bits
   b. 64 bits
   c. 128 bits
   d. 256 bits

77. **Which NTFS structure is examined to determine if a file existed but has been deleted, since it maintains records even for deleted files?**
   a. File Allocation Table
   b. Master File Table
   c. Volume Boot Record
   d. Extended boot sector

78. **In Windows forensics, the UserAssist Registry key records:**
    a. Installed software license keys of the software installed in the system
    b. User account creation dates and time
    c. GUI-based program execution history including run count and last execution time (ROT13 encoded)
    d. Network adapter MAC addresses
79. **In Android forensics, rooting a device before evidence collection may:**
    a. Always improve evidence quality without any risk or damage to the data
    b. Encrypt all data on the device which cannot be used later for any purpose
    c. Potentially alter evidence and raise questions about evidence integrity in court
    d. Factory reset the device automatically
80. **In cloud forensics, API logs from cloud providers are forensically important because they:**
    a. Contain the actual content of stored data of the user
    b. Store backup copies of all user files
    c. Provide real-time monitoring of VM performance of the cloud service provider for monitoring by the investigating agency
    d. Record who performed what actions on cloud resources, when, and from which IP address
81. **In threat intelligence, a "Tactics, Techniques, and Procedures" (TTP) framework such as MITRE ATT&CK is used in forensic investigations to:**
    a. Replace traditional chain of custody procedures with the new procedure to do the investigation
    b. Map observed attacker behaviors to known adversary patterns to identify threat actors and methods
    c. Automatically decrypt ransomware-encrypted files with the key taken from the given framework
    d. Replace hash-based file verification
82. **The Windows $MFT file in NTFS contains an entry for every file and directory. When a file is deleted, what happens to its MFT entry?**
    a. The MFT entry is immediately zeroed out and everything is removed from all the location
    b. The MFT entry is marked as unallocated but retains its data until overwritten by a new file entry
    c. The MFT entry is moved to a special "deleted" section
    d. The MFT entry is encrypted and locked
83. **Web Jacking attacks differ from standard website defacement because Web Jacking involves:**
    a. Replacing a website's homepage with political messages and picture to propagate
    b. Injecting malicious scripts into web page source code
    c. Redirecting traffic to a fraudulent copy by compromising DNS records or hijacking domain registration
    d. Flooding a web server with requests from different jack servers with high data packets
84. **In the OSI model, which layer is responsible for end-to-end error detection, flow control, and reliable data delivery between applications?**
    a. Session Layer (Layer 5)
    b. Transport Layer (Layer 4)
    c. Network Layer (Layer 3)
    d. Data Link Layer (Layer 2)
85. **BGP (Border Gateway Protocol) hijacking attacks are dangerous because BGP:**
    a. BGP uses only within private enterprise networks which are situated in the remote area
    b. BGP encrypts the data by default, making attacks difficult to detect to access the user data
    c. BGP lacks built-in route authentication, allowing malicious route announcements that divert global internet traffic
    d. BGP only affects DNS resolution and deny the access
86. **Which port is used by HTTPS by default?**

a. Port 80
b. Port 443
c. Port 8080
d. Port 22

87. **In mobile forensics, the Android "ADB" (Android Debug Bridge) tool is commonly used for:**
a. Physical chip-off extraction and collects all the allocated and unallocated data
b. Logical data extraction, backup acquisition, and shell access when USB debugging is enabled
c. SIM card cloning
d. Cracking the device PIN and other password of the android device

88. **Hybrid encryption systems (used in SSL/TLS, PGP) combine symmetric and asymmetric cryptography because:**
a. Asymmetric is too slow for bulk data, so it only encrypts a symmetric session key used for efficient bulk encryption
b. Symmetric encryption is not secure enough on its own and it needs asymmetric encryption
c. Asymmetric algorithms cannot handle large data sizes
d. Regulatory requirements mandate the use of both types simultaneously

89. **In the context of email forensics, the "X-Originating-IP" header field is used to:**
a. Identify the recipient's IP address whether it a public or private
b. Identify the email encryption protocol used to know the security strength of the message
c. Specify the email server's geographic location
d. Records the IP address of the device from which the email was originally sent

90. **Which SSD wear-leveling technique distributes write operations evenly across all flash memory cells to extend device lifespan?**
a. Over-provisioning only
b. TRIM command execution
c. Dynamic and static wear leveling managed by the SSD controller's firmware
d. Bad block mapping by the OS

91. **The ext4 file system's "journal" in Linux serves which forensic purpose?**
a. It permanently stores all deleted file contents
b. Records recent file system metadata transactions, potentially enabling recovery of recently deleted file metadata
c. It encrypts all file system writes
d. It maintains user access control lists

92. **In a GPT partitioned disk, the primary purpose of the protective MBR is to:**
a. Encrypt partitions
b. Support only Windows OS
c. Prevent legacy tools from misreading the disk as empty
d. Increase disk speed

93. **Which file system is most associated with Windows modern systems?**
a. ext4
b. HFS+
c. ISO9660
d. NTFS

94. **The “order of volatility” means evidence should be collected:**
a. Alphabetically assign cases to Scientific Experts
b. From least expensive to most expensive
c. Order of Primary and Secondary Evidences

d. From most temporary to most persistent

95. **Which Windows registry hive commonly stores user profile and software settings?**
a. HKEY_LOCAL_MACHINE
b. HKEY_CURRENT_USER
c. HKEY_CLASSES_ROOT
d. HKEY_USERS

96. **Which of the following is a common sign of data tampering on a file system?**
a. Unchanged timestamps
b. Altered metadata
c. Larger monitor
d. Faster internet

97. **In Linux, which file typically stores user account information?**
a. /etc/passwd
b. /etc/shadow only
c. /var/log/auth.log
d. /home/user/.profile

98. **Which Linux log is commonly used for system-wide messages and service events?**
a. syslog
b. passwd
c. shadow
d. hosts

99. **Which browser artifact is most directly used to store login or tracking state across sessions?**
a. Cache
b. Cookies
c. Bookmark export
d. Download folder

100. **Which technique is most appropriate for acquiring data from a live running system when volatile data must be preserved?**
a. Memory dump acquisition
b. Disk defragmentation
c. File compression
d. Partition formatting

101. **Which mobile database format is widely used by apps on Android and iOS?**
a. SQLite
b. CSV
c. NTFS
d. FAT12

102. **Alternate Data Streams (ADS) in NTFS allow:**
a. Multiple partitions on a single volume
b. Multiple users to own the same file simultaneously from different locations without changing the volume
c. Encrypted data streams to be stored separately in a separate storage space
d. Hidden data to be attached to a file without changing its visible size or modifying the primary stream

103. **What does ARP poisoning primarily target?**
a. Application passwords
b. IP-to-MAC address resolution
c. File permissions
d. Email attachments

104. **What does DPI stand for in network security?**
a. Deep Packet Inspection

b. Disk Partition Imaging
c. Digital Protocol Isolation
d. Dynamic Port Injection

105. **Which malware type is especially difficult to detect because it hides its presence at the kernel or system level?**
a. Rootkit
b. Cookie
c. Cache
d. Bookmark

106. **Which term describes the smallest logical storage unit that an operating system uses to allocate space for a file on a hard disk?**
a. Track
b. Column
c. Cluster
d. Cylinder

107. **In the NTFS file system, where is the information about every file and directory on the volume stored?**
a. File Allocation Table (FAT)
b. Master File Table (MFT)
c. Registry
d. Superblock

108. **What is the smallest logical unit of storage in an SSD?**
a. Page
b. Book
c. Chapter
d. Sector

109. **Which of the following bit lengths is associated with the SHA-1 (Secure Hash Algorithm 1) digest?**
a. 128 bits
b. 160 bits
c. 224 bits
d. 512 bits

110. **In Windows systems, Google Chrome stores saved user passwords primarily in which format and location?**
a. Plain text in the Windows Registry under HKCU\Software\Google\Chrome
b. Encrypted form inside an SQLite database file named Login Data
c. As plain text in a file called Passwords.txt in the Chrome installation directory
d. Encrypted using BitLocker in the Pagefile.sys

111. **Which of the following system files is NOT primarily used as a mechanism for virtual memory or paging in Windows?**
a. Pagefile.sys
b. hiberfil.sys
c. swapfile.sys
d. ramdisk.img

112. **Which RAID level used in high-end NVRs provides block-level striping with distributed parity, requiring at least three disks?**
a. RAID 0
b. RAID 1
c. RAID 5
d. RAID 11

113. **Which network topology requires the highest number of cables and provides the best fault tolerance?**
a. Bus Topology

b. Ring Topology
c. Star Topology
d. Mesh Topology

114. **SIEM stands for:**
a. Security Information and Event Management
b. System Intrusion Event Monitor
c. Secure Internet Encryption Module
d. Safety Incident Evidence Manager

115. **Which malware analysis technique examines the code without executing it?**
a. Dynamic Analysis
b. Ultra Analysis
c. Static Analysis
d. Memory Analysis

116. **What is the full form of APK?**
a. Application Package Kit
b. Android Package Kit
c. Application Programming Kit
d. Advanced Phone Kernel

117. **What is the full form of JTAG in the context of Mobile Forensics?**
a. Java Testing and Application Group
b. Joint Technology Application Gateway
c. Junction Terminal Access Gateway
d. Joint Test Action Group

118. **The $BitMap file in NTFS keeps a record of:**
a. Metadata
b. Cluster Allocation Status
c. Bitlocker settings
d. Application settings

119. **A forensic examiner needs to identify the unique serial number and the last connection time of a specific usb drive used on a Windows 10 workstation. Which of the following artifacts is the primary source for this information?**
a. C:\Windows\Prefetch\
b. HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Enum\USBSTOR
c. C:\Windows\System32\config\SAM
d. C:\$LogFile

120. **Which Windows artifact can help determine what folders a user accessed in Explorer?**
a. Shellbags
b. Cookies
c. hiberfil.sys
d. ARP cache