National Forensic Sciences University
Scientific Officer (Cyber & TASI) - Gr. B (Contractual Basis)
Directorate of Forensic Science Laboratory, Home Department, State of Maharashtra
Examination type: MCQ
Revised Final Answer Key

Date: 4th May 2025

Instructions:

1. Multiple Choice Question Examination.
2. Chose the correct answer and mark in the OMR sheet with black ball pen.
3. No-negative marking and each question carry one marks.
4. Duration of the paper is 60 minutes

Q-1 Answer the following Question **[Marks: 60]**

1. In a modern computer system using a hybrid storage architecture, which combination most effectively balances speed, durability, and cost-efficiency for large-scale transactional applications?

A) RAM + HDD only B) RAM + SSD + HDD (Tiered Storage) C) SSD only

D) HDD + Tape Backup only

2. Which of the following time complexities represents the *best possible* average-case runtime for searching an element in a perfectly balanced Binary Search Tree (BST)?

A) O(1) B) O(log n) C) O(n) D) O(n log n)

3. You are tasked with designing a *priority-based task scheduling* system where the highest priority task is always processed first. Which data structure is most appropriate for achieving **O(log n)** insertion and deletion?

A) Hash Table B) Stack C) Binary Heap D) AVL Tree

4. During the booting process of an operating system, which of the following sequences **correctly** describes the order of execution?

A) Power-on Self-Test (POST) → Bootloader → BIOS → Kernel Initialization
B) BIOS → POST → Bootloader → Kernel Initialization C) POST → BIOS → Bootloader → Kernel Initialization D) Bootloader → POST → BIOS → Kernel Initialization

5. Which of the following protocols is primarily responsible for device-to-device lightweight messaging in IoT environments, especially for low-bandwidth and constrained devices?

A) HTTP B) FTP C) MQTT D) SNMP

6. In the context of SQL transactions, which ACID property ensures that **either all operations** of a transaction are completed successfully, or **none are applied**, thereby preserving database integrity?

A) Atomicity B) Consistency C) Isolation D) Durability

7. Which of the following accurately differentiates a *substitution cipher* from a *transposition cipher*?

A) Substitution cipher changes the structure of plaintext; transposition cipher changes only the values.
B) Substitution cipher retains the plaintext structure but replaces characters; transposition cipher rearranges the existing plaintext characters.
C) Both substitution and transposition ciphers change plaintext character values and structure simultaneously.
D) Substitution cipher uses matrix-based transformations while transposition cipher uses modular arithmetic exclusively.

8. In a **multi-factor authentication (MFA)** system, which of the following sets best exemplifies the principle of combining factors from *different* authentication categories?

A) Password, PIN, Security Question B) Password, Fingerprint Scan, OTP via SMS
C) RFID Card, NFC-enabled Phone, Password D) Username, Email, Password

9. Within the context of a **Public Key Infrastructure (PKI)**, which element is primarily responsible for *binding* a public key to an entity's identity through digitally signed certificates?

A) Digital Signer B) Certificate Authority (CA) C) Registration Authority (RA)
D) Key Distribution Center (KDC)

10. Which of the following statements is **TRUE** regarding the comparison of MD5, SHA-1, SHA-2, and SHA-3?

A) SHA-1 is more secure than SHA-2 but less efficient than MD5.
B) SHA-3 was developed as an improvement over the vulnerabilities discovered

in SHA-2.
C) MD5 and SHA-1 are considered cryptographically secure against collision attacks today.
D) SHA-2 and SHA-3 share the same underlying algorithmic structure and padding schemes.

11. Which of the following BEST describes the operational difference between an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS)?

A) IDS actively blocks attacks; IPS only monitors network traffic.
B) IDS monitors and alerts without acting; IPS detects and takes automated action to block threats.
C) IDS performs packet filtering at Layer 3; IPS operates at Layer 7.
D) IDS encrypts data packets; IPS decrypts incoming packets for inspection.

12. In the context of **cybercrime investigation** requiring international cooperation, what is the *primary legal distinction* between a **Mutual Legal Assistance Treaty (MLAT)** and a **Letter Rogatory**?

A) MLAT is informal; Letter Rogatory is treaty-bound.
B) MLAT operates only within EU countries; Letter Rogatory is worldwide.
C) MLAT is a formal agreement enabling faster official assistance between countries; Letter Rogatory is a slower, court-to-court formal request.
D) MLAT is used for civil matters; Letter Rogatory only for criminal matters.

13. Which of the following best represents a *core cardinal rule* of digital forensics during evidence handling?

A) Always upgrade the suspect system's software to facilitate imaging.
B) Always ensure that original evidence is altered only by authorized investigators.
C) Always access live data immediately after seizing the device.
D) Always compress the evidence before acquisition to save storage space.

14. Applying **Locard's Exchange Principle** to digital evidence implies that:

A) No interaction between a user and a digital device leaves any traces.
B) Every access or modification of a digital system leaves a trace or artifact.
C) Digital footprints can be completely eliminated using standard erasure techniques.
D) Only hardware devices like USBs leave evidence, not software interactions.

15. Which of the following statements about the use of **write-blockers** during digital evidence acquisition is MOST accurate?

A) Write-blockers allow forensic analysts to alter metadata to correct timestamps.
B) Write-blockers prevent unauthorized users from accessing the evidence.
C) Write-blockers ensure that the acquisition process does not modify the original media.
D) Write-blockers encrypt the evidence data for safe transportation.

16. In the context of maintaining a **chain-of-custody** for digital evidence, which action would MOST LIKELY invalidate the evidence in court proceedings?

A) Properly logging each transfer with signatures and timestamps.
B) Transferring the evidence to an unauthorized person without documentation.
C) Transporting the evidence in a tamper-evident bag.
D) Acquiring a forensic image using a certified tool.

17. Which key distinction separates **data recovery** from **file carving** in digital forensics?

A) Data recovery retrieves intact file systems, while file carving recovers deleted files from logical drives only.
B) Data recovery uses file headers and footers, whereas file carving uses file allocation tables.
C) Data recovery restores lost files using file system metadata, while file carving reconstructs files solely based on raw content signatures.
D) Data recovery is limited to RAID arrays, whereas file carving applies only to USB devices.

18. Whch of the following **correctly matches** a forensic tool with its **original equipment manufacturer (OEM)**?

A) FTK – Guidance Software B) EnCase – AccessData
C) Autopsy – Basis Technology D) Cellebrite UFED – Cellebrite

19. Which of the following file systems natively supports **file system journaling**, **fine-grained permissions**, and **encryption support**, making it highly suited for modern Windows forensic investigations?

A) FAT32 B) NTFS C) Ext3 D) HFS+

20. Which combination best describes the roles of **Alternate Data Streams (ADS)** and **Slack Space** in forensic analysis of NTFS volumes?

A) ADS stores deleted files; Slack space stores file metadata.
B) ADS can hide malicious data; Slack space can contain remnants of previously deleted information.
C) Slack space stores compressed files; ADS stores fragmented files.

D) ADS is visible to users; Slack space is hidden and inaccessible without administrator rights.

21. On a typical Linux file system (Ext4), what do the permission bits -rwxr-xr-- represent for a file?

A) Owner: read/write; Group: write/execute; Others: read-only
B) Owner: read/write/execute; Group: read/execute; Others: read-only
C) Owner: read-only; Group: read/write/execute; Others: execute-only
D) Owner: read/write/execute; Group: write-only; Others: no permissions

22. In Mac OS X forensic analysis, which **hidden directory** is typically crucial for investigating system startup items and persistence mechanisms used by malware?

A) /Applications B) /System/Library/StartupItems C) /Volumes
D) /Users/Shared

23. When analyzing an email header for forensic investigation, which of the following fields provides the **most accurate origin IP address** of the sender?

A) Received: from (earliest entry)
B) Return-Path
C) Message-ID
D) MIME-Version

24. Which of the following mobile acquisition techniques involves **direct reading from NAND memory**, often bypassing file-system-level restrictions but carrying a high risk of damaging the device?

A) Logical Acquisition B) File System Extraction C) Physical Acquisition
D) Cloud Backup Extraction

25. Which of the following statements best reflects the **distinction between civil and criminal justice** systems in India?

A) Civil justice focuses on punishment, whereas criminal justice focuses only on compensation.
B) Civil justice resolves disputes between individuals, whereas criminal justice addresses offenses against the society/state.
C) Civil justice is always bailable, whereas criminal justice is always non-bailable.
D) Civil justice operates under the BNSS, while criminal justice operates under the BSA.

26. In India, which of the following **is NOT an essential characteristic** of a valid FIR under procedural law?

A) It must be in writing. B) It must necessarily be given by the victim.
C) It must disclose a cognizable offense. D) It must be signed by the informant.

27. Under the **Bharatiya Nyaya Sanhita (BNS)**, which of the following BEST defines a **cognizable offense**?

A) An offense where police must obtain prior approval from the court before investigation.
B) An offense where police can arrest without a warrant and begin investigation without prior court approval.
C) An offense punishable by a fine only.
D) An offense relating solely to civil property disputes.

28. Which **amendment to the IT Act 2000** significantly introduced provisions for handling **cyber terrorism, identity theft, and sending offensive messages electronically**?

A) IT Act Amendment 2004 B) IT Act Amendment 2008
C) IT Act Amendment 2010 D) IT Act Amendment 2015

29. Under the **Digital Personal Data Protection (DPDP) Act, 2023**, which of the following principles is emphasized to ensure **accountability** of organizations handling personal data?

A) Data Sovereignty B) Purpose Limitation
C) Data Localization D) Notice and Consent Framework

30. Which of the following actions BEST exemplifies a violation of **cyber ethics** but may **not always** constitute a punishable offense under current cyber laws?

A) Cyberbullying through social media platforms. B) Hacking into government servers.
C) Child sexual abuse material dissemination. D) Intellectual property theft from a corporate database.

31. **Scenario:** An investigator arrives at a cybercrime scene and seizes a smartphone suspected of containing critical evidence. The device is powered ON, screen unlocked, and connected to Wi-Fi.

What is the MOST appropriate immediate step the investigator should take to preserve evidence integrity?

A) Turn off the device immediately to prevent remote wiping.
B) Enable Airplane mode, disable Wi-Fi, Bluetooth, and remove network SIMs if possible.
C) Pull out the battery forcefully (if accessible) to preserve volatile memory.
D) Begin forensic acquisition on-site using mobile forensic tools without isolating the device.

32. Scenario:
You encounter an Android smartphone configured with **F2FS** file system instead of the common **EXT4** during forensic analysis.

What specific forensic challenge might you face due to this file system?

A) Inability to bypass device encryption due to F2FS internal architecture.
B) Standard forensic imaging tools may not natively support parsing F2FS, risking incomplete acquisition.
C) F2FS automatically deletes call logs after 30 days, complicating evidence recovery.
D) F2FS compresses all files, making keyword searches impossible without full decryption.

33. Scenario: A forensic analyst needs to extract maximum deleted SMS, WhatsApp data, and call history from a locked iPhone running iOS 15, with no passcode available.

Which acquisition method will be the MOST effective considering device constraints?

A) Logical acquisition via iTunes backup.
B) Physical acquisition via NAND mirroring.
C) File system acquisition using jailbreak or agent-based extraction (if possible).
D) Cloud acquisition using Apple ID and password without touching the device.

34. Scenario:
During transport to the forensic lab, the mobile device under investigation unexpectedly powers down due to battery drain.

Which of the following preservation actions would have been MOST appropriate to prevent loss of volatile data?

A) Backing up data over Wi-Fi before seizure.
B) Using a Faraday bag only to block network signals.
C) Connecting the device to a portable charger without interacting with the screen or apps.
D) Removing the SIM card only before transportation.

35. Scenario: During forensic examination of an Android device, the investigator finds **both internal memory** and **external microSD card** storage.

Which type of evidence would MOST LIKELY be found only on the external microSD card, not in internal storage?

A) Application install files and system logs.
B) Encrypted WhatsApp databases (default storage).
C) Call logs and SMS databases.
D) Cached images from social media apps.

36. **Scenario:** An encrypted Android device (File-Based Encryption active) must be analyzed. The password is unknown.

Which acquisition strategy presents the MOST legally and technically acceptable first step?

A) Root the device immediately to bypass encryption.
B) Attempt cloud-based acquisition via associated Google account access.
C) Perform JTAG extraction by soldering onto the PCB.
D) Attempt brute-forcing the password without documentation.

37. **"अपराध" या शब्दाचे योग्य समानार्थी शब्द कोणते?**

a) गुन्हा

b) शिक्षण

c) चौकशी

d) न्याय

38. **"फॉरेन्सिक" या शब्दाचे शुद्धलेखन कोणते?**

a) फॉरेंन्सिक

b) फॉरेन्सीक

c) फॉरेन्सिक

d) फोरेंसिक

39. **"सत्य" या शब्दाचे विरुद्धार्थी शब्द कोणते?**

a) तिरस्कार

b) खोटे

c) अंधार

d) आरोप

40. **"डिजिटल पुरावा" या शब्दसमुहात कोणता विशेषण शब्द आहे?**

a) पुरावा

b) डिजिटल

c) साक्ष

d) गुन्हा

41. **"शंका उपस्थित करणे" - याचा योग्य अर्थ काय?**

a) निर्णय घेणे

b) माहिती मागवणे

c) संशय निर्माण करणे

d) मुद्दा स्पष्ट करणे

42. **"तपास" या क्रियापदाचे भूतकाल रूप कोणते?**

a) तपासत आहे

b) तपासेल

c) तपासला

d) तपासते

43. **"साक्षीदाराने सत्य सांगितले." या वाक्याचा काळ कोणता आहे?**

a) भविष्य

b) भूत

c) वर्तमान

d) आज्ञार्थ

44. **"पुरावे" या संज्ञेचा अनेकवचनी रूप कोणते?**

a) पुरावांचा

b) पुरावे

c) पुरावेस

d) पुरव

45. **"शंकास्पद" या शब्दात कोणता प्रत्यय आहे?**

a) क

b) स्पद

c) स

d) शक

46. **"निष्कलंक" या शब्दाचा अर्थ काय?**

a) गुन्हेगार

b) निर्दोष

c) संशयित

d) साक्षीदार

47. "अंगावर काटा उभा रहाणे" या व्याक्यप्रचाराचा अर्थ काय?

a) अंग शहारणे

b) रोमांचित होणे

c) अतिशय भिती वाटणे

d) बहरुन येणे

48. **"पुरावे गोळा करणे" - यात क्रियापद कोणते आहे?**

a) गोळा

b) करणे

c) पुरावे

d) सादर

49. "पुरावे तपासले गेले." या वाक्याचा प्रकार कोणता?

a) कर्तरी प्रयोग

b) कर्मणी प्रयोग

c) भाववाचक

d) निषेधार्थक

50. पर्यायी उत्तरांतील गटाबाहेरचा शब्द कोणता ?

a) भाकरी

b) खलबत्ता

c) डबा

d) विळी

51. "गुन्हेगार पळून गेला." - या वाक्यातील काळ कोणता आहे?

a) भविष्य

b) पूर्ण वर्तमान

c) भूत

d) आज्ञार्थ

52. **'विध्वंसक' या शब्दाचा विरोधार्थी आशय व्यक्त करणारा शब्द ओळखा.**

(अ) पुरोगामी

(ब) विधायक

(क) मवाळ

(ड) सुलक्षणी

पर्यायी उत्तरे :

a) (ब) व (ड) बरोबर

b) फक्त (ब) बरोबर

c) फक्त (क) बरोबर

d) फक्त (अ) बरोबर

53. चुकीचे वाक्य ओळखा:

a) फॉरेन्सिक तज्ज्ञांनी अहवाल दिला.

b) तपासात त्रुटी होत्या.

c) आरोपीने निर्दोष असल्याचं कबूल केलं.

d) साक्षीदाराने खोटं साक्ष दिली.

54. "पुरावे सादर करण्यात आले." या वाक्याचा प्रकार कोणता आहे?

a) आज्ञार्थ

b) भाववाचक

c) कर्मणी

d) संयुक्त

55. "आरोपीचा गुन्हा सिध्द झाला." - यात कोणते क्रियापद आहे?

a) आरोपीचा

b) गुन्हा

c) सिध्द

d) झाला

56. वाक्य पूर्ण करा:

"तपास अहवालात गंभीर ___ आढळले."

a) आरोपी

b) गुन्हेगार

c) दोष

d) पुरावे

57. "तो निरपराध आहे." - या वाक्याचा अर्थ काय?

a) दोषी आहे

b) निर्दोष आहे

c) साक्षीदार आहे

d) संशयित आहे

58. अनुच्छेद वाचनावर आधारित प्रश्न:

(डीएनए .फॉरेन्सिक विज्ञानाच्या मदतीने पोलिस गुन्ह्यांची उकल करण्यात यशस्वी ठरतात", फिंगरप्रिंट्स, तसेच सायबर पुरावे गुन्हेगार ओळखण्यासाठी उपयोगी पडतात(".

प्रश्नडीएनए व फिंगरप्रिंट्सचा उपयोग कोणासाठी होतो :?

a) आरोपीला पकडण्यासाठी

b) पुरावे नष्ट करण्यासाठी

c) खटला पुढे नेण्यासाठी

d) गुन्हेगार ओळखण्यासाठी

59. वाक्य शुध्द करा:

"त्याला न्याय मिळवायचा आहे".

a) त्याला न्याय मिळायला पाहिजे.

b) त्याला न्याय मिळवणे आहे.

c) त्याला न्याय मिळवायचं आहे.

d) त्याला न्याय मिळवायचा आहे.

60. "डिजिटल पुरावा "- या शब्दयुग्मातील संबंध ओळखा:

a) कारक संबंध

b) विशेषण विशेष्य

c) नामधातू

d) प्रयोग
