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

Answer Key
March 29, 2025

NFSU JSO Digital Forensics Examination

1. Memory forensics relates to ___

A Forensics of Hard Disk Drives

B Forensics of TPM chips

✓ C Forensics of RAM

D All of the mentioned

2. Types of data retrieved from the Memory Forensics

A Running processes

B Network connections

C Registry keys & Loaded DLLs

✓ D All of the mentioned

3. Event logs of the Linux systems are stored at _____

✓ A /var/log

B /etc/grub.conf

C /proc/stat

D /usr/sbin

4. Which file system can be used to change certain kernel parameters at runtime using sysctl command?

A Ext3

B Sysfs

C Ext4

✓ D Procfs

5. File system for CDROM is _____

A squashfs

B ntfs

✓ C isofs

D procfs

6. What is one of the main advantage of using APFS over HFS+?

A APFS supports more file formats.

✓ B APFS is faster, especially on flash storage.

C HFS+ has better encryption capabilities than APFS.

D APFS is more compatible with older macOS versions.

7. Which of the following is true about APFS encryption?

✓ A APFS encryption is optional and can be applied to individual files or volumes.

B APFS only supports full disk encryption.

C APFS does not support any form of encryption.

D APFS encryption is only available on macOS Sierra and earlier.

8. What type of data does the macOS file system store in "System Logs" that could be useful in forensics?

A User browsing history

B Authentication logs

C Deleted files

✓ D File access and modification logs

9. Which of the following is a key feature of FileVault on macOS in the context of forensic investigations?

✓ A It encrypts the entire system disk, preventing unauthorized access to data.

B It creates secure backups of encrypted files for easy recovery

C It creates time-stamped snapshots of files for forensic examination.

D It logs every file modification to the system for auditing purposes

10. In forensic analysis, which of the following directories is crucial for retrieving deleted files in macOS?

- ✓ **A** /private/var/folders
- **B** /Library/Application Support
- **C** /System/Library
- **D** /Users/Shared

11. Which of the following is a critical log file for Windows forensic investigations?

- **A** Event logs
- **B** Anti-Virus Logs
- **C** Firewall logs
- ✓ **D** All of the mentioned

12. What type of forensic data can be found in the Windows Prefetch folder?

- ✓ **A** Recently accessed files and applications
- **B** Deleted files
- **C** Running Processes
- **D** Backup file information

13. Which method is commonly used in multimedia forensics to detect digital image tampering?

- **A** Frequency analysis
- **B** Digital watermarking
- **C** Image hashing
- ✓ **D** JPEG compression analysis

14. In videos, what does "frame interpolation" refer to?

- **A** A technique to extract audio from video
- ✓ **B** The process of modifying video frames to insert or remove elements
- **C** A method for compressing video frames
- **D** The process of detecting audio signals in video content

15. Which metadata field can help forensic investigators determine if a file was altered?

A File creation date

✓ B Last modified date

C Author

D File size

16. Which of the following is a key focus of Clause 7 of ISO 17025:2017?

A Chain of Custody procedure.

B Reconstructing the destroyed Digital evidence in perfect environment.

✓ C Laboratory operations and quality assurance.

D Handling and storage of test items.

17. What is the TCP port number for RDP?

A 4625

✓ B 3389

C 389

D 80

18. Which of the following Event ID is generated when the security log gets cleared which indicates a log tampering?

✓ A 1102

B 4625

C 4771

D 5140

19. Which DNS record type is used to implement DMARC?

✓ A TXT

B MX

C A

D CNAME

20. According to the FBI Digital Evidence Guidelines, what is one key practice for handling digital evidence?

- A All devices should be scanned for malware before analysis.
- ✓ B Evidence should be handled to maintain its integrity and chain of custody.
- C Evidence can be analyzed without concern for its integrity if a backup is available.
- D Digital evidence need to be documented before analysis.

21. Which of the following AI technique is primarily used to generate deepfakes?

- A Support Vector Machines (SVM)
- ✓ B Generative Adversarial Networks (GANs)
- C K-means clustering
- D Decision Trees

22. The Information Technology Act, 2000 provides for the legal framework of cybercrime and electronic commerce in India. Which of the following sections of this Act deals with the admissibility of electronic evidence?

- A Section 66
- ✓ B Section 65B
- C Section 77
- D Section 10A

23. What is "frame interpolation" in the context of CCTV forensics?

- A Removing frames from the video to shorten its duration
- B Increasing the resolution of individual frames
- ✓ C Creating intermediate frames between existing frames to improve motion smoothness
- D Converting video to a different format

24. Which of the following is NOT typically part of a router's log file?

- A Source and destination IP addresses
- B Timestamps of network events
- ✓ C User authentication details
- D DNS query logs

25. Which WAF feature would be useful in protecting against brute force login attacks?

- ✓ **A** Rate-limiting
- **B** IP whitelisting
- **C** HTTP header inspection
- **D** URL pattern matching

26. What does "Event ID 4720" in the Windows Security Log indicate in Active Directory forensics?

- **A** A user account was successfully logged in
- ✓ **B** A user account was created
- **C** A user password was reset
- **D** A user account was disabled

27. Which of the following would indicate that an attacker has used the "Golden Ticket" attack in Active Directory forensics?

- **A** A user account logs in multiple times from different geographic locations
- ✓ **B** The attacker uses a forged Kerberos ticket to impersonate a domain administrator
- **C** A new user account is created with administrative rights
- **D** Gaining the access of an account having weak credentials.

28. Which of the following is a popular blockchain platform for building decentralized applications (dApps)?

- ✓ **A** Ethereum
- **B** Litecoin
- **C** Dogecoin
- **D** Ripple

29. What does the term "altcoin" refer to?

- **A** A new cryptocurrency that is a clone of Bitcoin
- ✓ **B** Any cryptocurrency that is not Bitcoin
- **C** A specific cryptocurrency that is used for mining
- **D** A cryptocurrency that uses the Proof of Work consensus mechanism

30. What is the purpose of the seed phrase in a hardware wallet?

A It acts as a private key to access the hardware wallet.

✓ B It is used to generate and recover the wallet's private keys in case the device is lost or damaged

C It helps to transfer the tokens from the Hard wallet to Soft wallets.

D It helps the Wallet to store more than one Crypto currency in a single wallet.

31. Which of the following protocols is commonly used by IoT devices for communication?

A HTTP

✓ B MQTT

C FTP

D HTTPS

32. 1. Which of the following is typically found in the /data/data/ directory on an Android device?

A System files for Android's booting process

✓ B User-installed applications and app data

C Encryption keys

D Device configuration and network settings

33. What is the role of the "root" directory in iOS file system forensics?

A It stores encrypted files

✓ B It holds key system files essential for booting the device

C It contains user-created files like images and documents

D It stores application preference

34. Where would you most likely find forensic data regarding an iOS device's Wi-Fi connections?

✓ A /private/var/mobile/Library/Preferences/

B /private/var/log/

C /private/var/mobile/Library/Logs/

D /System/Library/Network/

35. Which hash function produces a 160-bit hash value?

- A MD5
- ✓ B SHA
- C SHA-256
- D CRC32

36. In Linux, which of the following tracks the execution of binaries, similar to the role of Prefetch in Windows?

- A syslog
- B lastlog
- ✓ C auditd
- D authlog

37. Which 802.11 standard operates in the 2.4 GHz band and offers a maximum data rate of 11 Mbps?

- A 802.11a
- ✓ B 802.11b
- C 802.11g
- D 802.11n

38. What is the primary purpose of a Beacon frame in Wi-Fi?

- A To establish a secure connection with a client
- ✓ B To announce the presence of a wireless network
- C To carry the data payload between devices
- D To encrypt data transmitted over the network

39. What does "zero-shot learning" mean in the context of LLMs?

- A The model cannot learn from data
- ✓ B The model is capable of performing tasks without specific task-based training
- C The model can only handle tasks it has been specifically trained on
- D The model learns tasks without human input

40. What does the "Turing Test" assess?

- A The intelligence of a machine based on its ability to perform tasks
- B Whether a machine can generate text
- ✓ C Whether a machine can exhibit intelligent behavior equivalent to, or indistinguishable from, that of a human
- D The computational power of a machine

41. Which of the following is an essential consideration when performing live forensics?

- A Shutting down the system to preserve evidence
- ✓ B Ensuring the system remains in operation while collecting evidence
- C Rebooting the system to clear any suspicious processes
- D Using a physical write blocker to prevent data changes

42. Which file system structure is primarily responsible for handling disk allocation in the HFS+ (Mac OS Extended) file system?

- A File Allocation Table (FAT)
- B Master File Table (MFT)
- ✓ C Catalog File
- D Block Map

43. What is the key characteristic of a "slack space" in the context of a file system?

- A It is the space on a hard drive that is automatically encrypted for security purposes
- ✓ B It refers to the unused space between the end of a file's logical size and the end of the allocated space
- C It is the unused space in a file system partition that is reserved for system files
- D It is the space on the hard drive where deleted files are temporarily stored before being permanently erased

44. What is the primary role of the "inode" in a UNIX-based file system like EXT4?

- A It stores file data directly
- ✓ B It stores file metadata, such as file permissions, ownership, and pointers to data blocks
- C It tracks deleted files in the system
- D It acts as the root directory for the file system

45. What is the main function of the /etc/shadow file in UNIX?

✓ **A** It stores user passwords in an encrypted format

B It stores information about user home directories

C It contains system logs and crash dumps

D It tracks the system's performance metrics

46. What is the purpose of the parity information stored in RAID 5?

A To store a copy of the data on every disk in the array

B To ensure that data is striped across disks for performance

✓ **C** To provide redundancy by allowing for the reconstruction of data from the parity information in case of a single disk failure

D To encrypt the data stored on the array

47. Which layer of the OSI model does the NetBIOS protocol operate at?

A Physical Layer

B Data Link Layer

C Network Layer

✓ **D** Session Layer

48. What does Section 66C of the Information Technology Act, 2000, address?

✓ **A** Punishment for identity theft

B Punishment for cyberstalking

C Punishment for data theft

D Punishment for sending offensive messages

49. The concept of "intermediary liability" in India, under the Information Technology Act, applies to which of the following?

A Internet Service Providers (ISPs)

B Social Media Platforms

C E-commerce websites

✓ **D** All of the mentioned

50. What is the main purpose of a hash function in a hash table?

- A To organize the table into a sorted order
- ✓ B To calculate the position in the table where the key-value pair should be stored
- C To provide direct access to the data
- D To reduce the time complexity of searching

51. Which property of a hash function ensures that it is computationally infeasible to find two different inputs that produce the same hash?

- A Pre-image resistance
- ✓ B Collision resistance
- C Avalanche effect
- D Second pre-image resistance

52. In the context of hash functions, what does the term "pre-image resistance" mean?

- A It should be impossible to find a second input that hashes to the same value as a given input
- ✓ B It should be impossible to find any input that hashes to a specific given output
- C It should be easy to find the original input given the hash
- D It refers to the uniform distribution of hash values

53. Which section of the IT Act 2000 deals with the punishment for cyber terrorism?

- ✓ A Section 66F
- B Section 420
- C Section 376
- D Section 295A

54. What is the primary purpose of iLEAPP?

- A To analyze and decrypt encrypted data on iOS devices
- ✓ B To acquire and preserve live evidence from iOS devices for forensic investigation
- C To ensure data privacy and protect the integrity of iOS device data
- D To install security patches on iOS devices.

55. In the context of cloud data security, which of the following best describes "data encryption at rest"?

- A Encrypting data only when it is being transferred between servers
- ✓ B Encrypting data that is stored in a cloud environment to protect it from unauthorized access
- C Encrypting metadata related to data stored in the cloud
- D Encrypting data while being processed by cloud services

56. What is the purpose of an initialization vector (IV) in encryption algorithms like AES?

- A To ensure the key is kept secret
- ✓ B To randomize the encryption process and ensure the same data encrypts differently each time
- C To hash the data before encryption
- D To store the encryption key securely

57. Which of the following best describes a "Zero-Day" exploit in the context of malware forensics?

- A A malware program that targets an already-known vulnerability
- B A vulnerability that is discovered after the malware is released
- ✓ C A previously unknown vulnerability that attackers exploit before a patch is released
- D A malware that becomes active on a particular date

58. Which of the following techniques is most commonly used to analyze the runtime behavior of a piece of malware in a controlled environment?

- A Fuzzing
- B Static analysis
- ✓ C Dynamic analysis in a sandbox
- D Reverse engineering

59. Which of the following information is typically stored in Shellbags?

- A User login credentials
- B File access timestamps
- ✓ C Folder view preferences and access times
- D Installed software information

60. What does the term "Web3" refer to in the context of the Metaverse?

✓ **A** The third iteration of the internet, which focuses on decentralization

B A new programming language for the Metaverse

C A social media platform within virtual reality

D The ability to view the Metaverse using a 3D web browser

61. What is the role of a write blocker during digital evidence acquisition according to international forensics standards?

A To encrypt the data before acquisition

B To block access to sensitive data

✓ **C** To prevent the modification of data during acquisition

D To compress the data being acquired

62. Which of the following should be avoided when handling digital evidence?

A Making multiple copies of the evidence

B Accessing the evidence only for investigative purposes

✓ **C** Viewing or modifying the data during the investigation

D Documenting each step of the forensic process

63. Which of the following digital forensics procedures aligns with the principle of “least intrusive analysis”?

A Using commercial forensic software to perform analysis on the original device

B Running a hash function on the device’s data and then performing full forensic analysis on it

✓ **C** Performing analysis on a forensic copy of the original evidence rather than on the original device

D Analyzing volatile data directly from a running system without any preservation of data

64. During the digital forensics process, what is the primary purpose of performing a "live acquisition" of volatile data?

✓ **A** To ensure the evidence is acquired before the device is turned off

B To capture and analyze volatile data on an encrypted device

C To analyze and catalog files for later review

D To collect data that is being transmitted across a network

65. Which of the following is the main function of IoT gateways?

- A To control and monitor sensor devices
- ✓ B To bridge communication between IoT devices and the cloud or data center
- C To store data temporarily
- D To manage user authentication for IoT networks

66. In network forensics, Packet Sniffing refers to:

- A Extracting malware from network traffic
- ✓ B Intercepting and analyzing network packets
- C Decrypting encrypted packets
- D Detecting unwanted network packets

67. What is a "Secure Enclave" in the context of Trusted Execution Environments?

- A A type of memory partition used by the operating system
- ✓ B A hardware-based isolated region where sensitive data is processed
- C A software layer used to manage encryption keys
- D A secure network used for communication between trusted devices

68. What type of indexing is primarily used by SQLite?

- A Hash Index
- B Binary Search Tree (BST)
- ✓ C B-Tree Index
- D Trie Index

69. How does SQLite handle concurrency?

- A It allows full multi-threading with multiple database connections.
- ✓ B It uses locks to allow only one process to access the database at a time.
- C It is optimized for high-concurrency and can handle thousands of simultaneous queries.
- D It allows unlimited concurrency and prevents all forms of locking.

70. What is "face encoding" in the context of facial recognition?

- ✓ A The process of generating a unique identifier from facial features
- B The process of mapping facial features.
- C The encoding of facial expressions to detect emotions
- D The process of translating facial features into an encrypted format

71. Which type of algorithm is most commonly used in facial recognition systems?

A Support Vector Machines (SVM)

B Convolutional Neural Networks (CNN)

✓ C K-means Clustering

D Linear Regression

72. Given the CIDR notation 192.168.10.0/25, how many possible IP addresses are in this network?

✓ A 128

B 254

C 256

D 512

73. Which of the following extensions are found during the imaging of a Hard Disk?

A .dmg

B .E01

C .dd

✓ D All of the mentioned

74. What does ECC stand for in the context of RAM?

✓ A Error Correction Code

B Extended Capacity Cache

C Enhanced Communication Control

D External Core Chip

75. What does SCADA stand for?

A Systematic Control and Data Analysis

✓ B Supervisory Control and Data Acquisition

C Secure Control and Data Access

D Simple Control and Data Application

76. Which of the following materials is an example of a direct bandgap semiconductor?

A Silicon

B Germanium

✓ C Gallium Arsenide

D Diamond

77. What is the solid form of carbon dioxide commonly called?

✓ **A** Dry ice

B Ice

C Graphite

D Diamond

78. If 6 men and 8 boys can do a piece of work in 10 days while 26 men and 48 boys can do the same in 2 days, the time taken by 15 men and 20 boys in doing the same type of work will be:

✓ **A** 4 days

B 5 days

C 6 days

D 7 days

79. The difference between simple and compound interests compounded annually on a certain sum of money for 2 years at 4% per annum is Re. 1. The sum (in Rs.) is:

✓ **A** 625

B 630

C 640

D 650

80. In how many ways can a committee of 3 people be formed from a group of 10 people?

A 360

B 720

✓ **C** 120

D None of the mentioned

81. What is the principle behind the operation of a LASER?

A Stimulated absorption of energy

B Spontaneous emission of radiation

✓ **C** Stimulated emission of radiation

D Reflection of light

82. Which of the following devices is most commonly degaussed?

✓ **A** Computers and hard drives

B Radios

C Microwave ovens

D Air conditioners

83. Which of the following is an example of an oxymoron?

A Bitter sweet

B Original copy

C Silent scream

✓ **D** All of the mentioned

84. Find the odd man out : 27, 64, 100, 1,125, 8, 216

A 27

✓ **B** 100

C 125

D 216

85. Two students appeared at an examination. One of them secured 9 marks more than the other and his marks was 56% of the sum of their marks. The marks obtained by them are:

A 39, 30

B 41, 32

✓ **C** 42, 33

D 43, 34

86. On 8th Feb, 2005 it was Tuesday. What was the day of the week on 8th Feb, 2004?

A Tuesday

B Monday

✓ **C** Sunday

D Wednesday

87. How many times a day do the hands of a clock coincide?

- ✓ **A** 22
- **B** 24
- **C** 20
- **D** 12

88. What does JPEG stand for?

- ✓ **A** Joint Photographic Experts Group
- **B** Joint Programming Experts Group
- **C** Java Programming Expert Group
- **D** Just Processed Encoding Graphic

89. If one-third of one-fourth of a number is 15, then three-tenth of that number is:

- **A** 35
- **B** 36
- **C** 45
- ✓ **D** 54

90. The ratio between the length and the breadth of a rectangular park is 3 : 2. If a man cycling along the boundary of the park at the speed of 12 km/hr completes one round in 8 minutes, then the area of the park (in sq. m) is:

- **A** 15360
- ✓ **B** 153600
- **C** 30720
- **D** 307200

91. Odometer is to mileage as compass is to

- **A** speed
- **B** hiking
- **C** needle
- ✓ **D** direction

92. Complete the given sentence using a suitable phrase: I arranged to meet Ram in the mall yesterday, but he didn't _____.

A Fall off

✓ B Turn up

C Move in

D Clear up

93. Sam started walking from point A towards East and walked for 6 km, then he turned to the left and walked for 8 km to reach point B. How far was he from the starting point?

A 14 km

✓ B 10 km

C 6 km

D 2 km

94. A woman introduces a man as the son of the brother of her mother. How is the man related to the woman?

A Brother

B Uncle

C Nephew

✓ D Cousin

95. Pick the odd one out from the given pair of words.

A Peace: Fight

B Rough: Smooth

✓ C Coward: Timid

D Taciturn: Talkative

96. Her _____ determination helped her achieve the impossible.

A weak

✓ B sheer

C half-hearted

D hesitant

97. What is the sum of the first 100 positive integers?

- ✓ **A** 5050
- **B** 10000
- **C** 10050
- **D** 100000

98. Choose the synonym of "Ephemeral":

- **A** Forever
- ✓ **B** Brief
- **C** Constant
- **D** Perpetual

99. If “HIM” means 936 , “CAM” means 39 . What will be the code for “MAP”?

- **A** 114
- **B** 400
- ✓ **C** 208
- **D** 98

100. Total cost of a bat and ball is $1.10 and the cost of bat is $1 more than that of ball. What is the cost of ball?

- **A** 0.1
- ✓ **B** 0.05
- **C** 0
- **D** can't say