# Digital Forensics

## Answer Key

## (Correct Answers are marked in bold letters)

### Section - A
### Forensic Aptitude

1. Vijay Singh (Golf player) is from which country?
   a) UK
   b) USA
   c) India
   **d) Fiji**

2. Which of these is the plant important in sericulture?
   a) Cassia
   b) Legumes
   c) Pea
   **d) Mulberry**

3. Which of the following Himalayan regions is called "Shivalik's"?
   a) Upper Himalayas
   b) Lower Himalayas
   **c) Outer Himalayas**
   d) Inner Himalayas

4. United Arab Emirates is federation of how many Emirates
   a) 6
   **b) 7**
   c) 5
   d) 8

5. Who amongst the following is a winner of Ramon Magsaysay Award?
   a) Vinobha Bhave
   b) Dara Khurody
   c) Tribhuvandas patel
   **d) All of the above**

6. Cinder Cone is a type of
   a) Dress
   **b) Volcano**
   c) Human Disease
   d) None of the above

7. Who of the following is not a hockey player?
   a) Birendra Lakra

b) Dhyan Chand
c) Dhanraj Pillai
**d) Bajrang Punia**

8. There are _____ views on the issue of giving bonus to the employees
a) independent
**b) divergent**
c) modest
d) adverse

9. What is the missing letter in this series?
b e h k n ? t
**a) q**
b) r
c) s
d) u

10. There are twenty-four students in a certain class. For every nine girls there are three boys. How many girls and how many boys are there in the class?
a) 19 and 5
**b) 18 and 6**
c) 15 and 9
d) 14 and 10

11. FISH: SCHOOL
**a) wolf: pack**
b) cow: farm
c) herd: peacock
d) elephant: jungle

12. While making Crime Scene Sketch location of interest on the walls or elsewhere in the enclosed space are best shown using
a) Triangular method of sketching
b) Base line method of sketching
**c) Cross projection method of sketching**
d) Compass point method

13. Magnification range from 2X to 250000X is possible from:
a) Fluorescence microscope
b) Polarizing microscope
**c) Electron microscope**
d) Stereo zoom microscope

14. Who conducts the assessment during the accreditation process?
a) Lab technicians

b) Competent authorities
**c) External assessors**
d) Police officers

15. Which principle emphasizes the use of Scientific methods and Techniques in Forensic Analysis?
a) Frye Standard
**b) Daubert Standard**
c) Principle of Exclusion
d) Alphonse Bertillon's Principle

16. What is the full form of RTGS?
a) Ready Transaction and Gross Settlement
**b) Real Time Gross Settlement**
c) Real Transaction and General Settlement
d) Real Transaction Gross Settlement

17. The founder of the Innocence Project, an organization dedicated to using DNA evidence to exonerate wrongfully convicted individuals, is:
a) Dr. Michael Baden
b) Dr. Henry C. Lee
**c) Dr. Barry Scheck**
d) Dr. Paul L. Kirk

18. If the sum of two number is 32 and their difference is 16, the smaller number would be
a) 6
**b) 8**
c) 16
d) 18

19. In India Inquest in Dowry Death is done by
a) Police
b) Coroner
**c) Magistrate**
d) Medical examiner

20. Hands of a clock overlap/coincide in a day
a) 24 times
**b) 22 times**
c) 6 times
d) 12 times

21. How many cores and deltas are present in a whorl
**a) Two deltas and one core**
b) One delta and two cores

c) Two deltas and two cores
d) One delta and one core

22. Detection of deception means
a) Psychological profiling of a suspect
b) Examining mental condition of suspect
**c) To find out whether the suspect is misleading**
d) To elicit number of crimes committed by the suspect

23. Order for exhumation can be given by
a) District Collector
b) Additional District Magistrate
c) Sub-collector
**d) Any of the above**

24. The Electromagnetic Spectrum's Infrared region stretches from:
a) 380-740 nm
b) 500-1mm
c) 165-525 nm
**d) 760-1 mm**

25. Which of the following is used for three-dimension image?
a) Compound Microscope
b) Simple Microscope
c) Transmission Electron Microscope (TEM)
**d) Scanning Electron Microscope (SEM)**

26. Presence of a functional group in a compound can be established by using
a) Chromatography
**b) IR Spectroscopy**
c) Mass Spectroscopy
d) X-ray diffraction

27. Which of the following Microscope best for observing colorless cells
a) Bright field microscope
**b) Dark field microscope**
c) Simple microscope
d) Stereo microscope

28. A written or recorded statement made by someone who is not testifying in court is classified as:
a) Physical evidence
b) Demonstrative evidence
**c) Hearsay evidence**
d) Expert evidence

29. Which method involves searching a Crime Scene in a back-and-forth pattern, covering the area systematically?
    a) Spiral search method
    b) Strip search method
    **c) Grid search method**
    d) Quadrant search method

30. What is the purpose of using a baseline in Crime Scene sketching?
    **a) To establish a reference line for measurements**
    b) To indicate the direction of entry
    c) To mark the location of evidence
    d) To create a visual representation of the crime scene

31. What is the recommended procedure for Photographing individual pieces of evidence at a crime scene?
    a) Capture only one angle for each item
    b) Use a flash for better visibility
    **c) Photograph each item in context and from multiple angles**
    d) Avoid photographing evidence to prevent contamination

32. Which is the only nation to have won both the FIFA Football World Cup and the FIFA Women's Football World Cup?
    a) Brazil
    b) Italy
    c) Argentina
    **d) Germany**

33. These are Sketching methods in crime scene, except
    a) Rectangular co-ordinate method
    **b) Spiral co-ordinate method**
    c) Triangular co-ordinate method
    d) Polar co-ordinate method

34. In crime scene reconstruction, what does the term "trajectory analysis" refer to?
    **a) The path of a projectile through space**
    b) The sequence of events leading up to the crime
    c) The psychological profile of the suspect
    d) The time of day the crime occurred

35. ISO/IEC 17025 accreditation for forensic laboratories in India ensures:
    a) Adherence to forensic procedures only
    **b) Quality and competence in testing and calibration**
    c) Compliance with international trade regulations

d) Exemption from regulatory audits

36. Which technique is suitable for separating large DNA fragments or whole chromosomes?

a) Agarose gel electrophoresis
b) SDS-PAGE
**c) Pulse-field gel electrophoresis**
d) Capillary electrophoresis

37. What role does the loading buffer play in electrophoresis?

a) Provides mechanical support
**b) Enhances sample conductivity**
c) Separates molecules based on charge
d) Regulates temperature

38. Determine the mode of the decision received seven days in a row: 11,13,13,17,19,23,25

a) 11
**b) 13**
c) 17
d) 23

39. Chromatic aberration is also known as

**a) Colour fringing**
b) Colour filter
c) Both a &b
d) None of the above

40. In which of the following causing death a human being will be Culpable Homicide not amounting to murder:

a) Causing an injury which is likely to cause death
b) Doing something which so imminently dangerous that it will cause death in all probability
c) Injury which the offender knows that it is likely to cause death of the person to whom the harm is caused
**d) causing Injury which is sufficient in the ordinary course of nature to cause death**

41. For which offence can the Police arrest without a court order?

a) **Cognizable offences**
b) Bailable offences
c) Detention offences
d) Non-cognizable offences

42. Which of the following fibre is of mineral origin?
    a) Mohair
    b) Nylon
    **c) Asbestos**
    d) Rayon

43. Which of the following measures the spread of data?
    a) Mean
    b) Median and interquartile range
    c) First and third quartiles
    **d) Standard deviation and variance**

44. The term 'Eddy Diffusion is used in which of the following analytical techniques?
    a) Microscopy
    **b) Chromatography**
    c) Spectrophotometry d
    d) Differential thermal analysis

45. In an air crash case, the following method of survey is most useful
    a) Strip method
    b) Spiral method
    c) Zonal method
    **d) Wheel method**

46. In SEM, the incident beam is focused by means of
    a) Lens
    b) Mirrors
    **c) Electromagnets**
    d) Slits

47. In the following question, find the correctly spelt word
    a) Quintessance
    b) Quintesance
    **c) Quintessence**
    d) Quintassence

48. Which of the following is a robust tool for Analysis of adulteration of Petrol, Diesel and Kerosene
    **a) Gas chromatography**
    b) Spectrophotometry
    c) Thin layer chromatography
    d) Electrophoresis

49. Which of the following is designed to control the operations of a computer?
    a) User
    b) Application Software
    **c) System Software**
    d) Utility Software

50. Which of the following is not a characteristic of a computer?
    a) Versatility
    b) Accuracy
    c) Diligence
    **d) I.Q.**

## Section-B
## Digital Forensics

51. What is digital forensic investigation primarily concerned with?
    a) Recovering lost data
    **b) Investigating crimes involving digital devices**
    c) Enhancing computer performance
    d) Protecting digital assets

52. Which of the following is NOT a common type of digital forensic investigation?
    a) Data recovery
    b) Network security analysis
    c) Malware analysis
    **d) Financial auditing**

53. What is the primary goal of digital forensic analysis?
    a) Identifying potential suspects
    b) Recovering deleted files
    **c) Preserving evidence integrity**
    d) Enhancing data encryption

54. Which of the following is NOT a step in the digital forensic investigation process?
    a) Data analysis
    b) Evidence collection
    **c) Suspect interrogation**
    d) Report generation

55. What legal principles govern digital forensic investigations?
    a) Miranda rights
    **b) Chain of custody**
    c) Habeas corpus

d) Double jeopardy

56. Which of the following techniques can be used to acquire digital evidence?
    **a) Disk imaging**
    b) System rebooting
    c) Cloud migration
    d) Browser history clearing

57. What is the term used to describe the process of analyzing digital evidence to reconstruct events?
    a) Data recovery
    **b) Timeline analysis**
    c) Hashing
    d) Data obfuscation

58. Which of the following is a potential challenge in digital forensic investigations?
    **a) Data encryption**
    b) Lack of digital devices
    c) Limited storage capacity
    d) Absence of cybersecurity threats

59. What role does metadata play in digital forensic investigations?
    a) Identifying potential suspects
    b) Enhancing data encryption
    **c) Providing context to digital evidence**
    d) Recovering lost data

60. Which of the following is a common source of digital evidence?
    a) Physical documents
    b) Eyewitness testimony
    c) Video surveillance footage
    **d) Social media posts**

61. What is Network Forensics primarily concerned with?
    a) Recovering lost data
    b) Investigating crimes involving digital devices
    **c) Analyzing network traffic**
    d) Enhancing network performance

62. Which of the following is NOT a common type of Network Forensic investigation?
    a) Intrusion detection
    b) Packet sniffing
    **c) Data recovery**
    d) Traffic analysis

63. What is the primary goal of Network Forensics?
    a) Identifying potential suspects
    b) Recovering deleted files
    **c) Analyzing network activity**
    d) Enhancing network security

64. Which of the following is NOT a step in the Network Forensic investigation process?
    a) Evidence collection
    **b) Suspect interrogation**
    c) Data analysis
    d) Report generation

65. What legal principles govern Network Forensic investigations?
    **a) Chain of custody**
    b) Habeas corpus
    c) Double jeopardy
    d) Probable cause

66. Which of the following techniques can be used in Network Forensics to acquire evidence?
    a) Disk imaging
    b) System rebooting
    **c) Packet capture**
    d) Browser history clearing

67. What is the term used to describe the process of analyzing network traffic to identify security breaches?
    **a) Intrusion detection**
    b) Packet sniffing
    c) Traffic analysis
    d) Network scanning

68. Which of the following is a potential challenge in Network Forensic investigations?
    a) Lack of network activity
    b) Limited data storage
    c) Absence of cybersecurity threats
    **d) Data encryption**

69. What role does metadata play in Network Forensic investigations?
    **a) Providing context to digital evidence**
    b) Recovering lost data
    c) Analyzing user behavior
    d) Identifying potential suspects

70. Which of the following is a common source of digital evidence in Network Forensics?
    a) Hard drives
    b) Mobile phones
    **c) Routers and switches**
    d) Social media posts

71. What is the first step in the mobile phone forensic process?
    a) Analyzing call logs
    **b) Extracting data from the device**
    c) Examining social media accounts
    d) Checking network connections

72. Which of the following is NOT a common challenge in mobile phone forensics?
    a) Encryption of data
    **b) Lack of storage space on the device**
    c) Complicated hardware components
    d) Incompatibility with forensic tools

73. What does the term "IMEI" stand for in mobile phone forensics?
    **a) International Mobile Equipment Identity**
    b) Internal Memory Extraction Interface
    c) Integrated Mobile Encryption Interface
    d) Internet Mobile Enhancement Infrastructure

74. Which of the following techniques is used to bypass locked devices in mobile phone forensics?
    a) IMEI spoofing
    **b) Jailbreaking**
    c) Rooting
    d) SIM swapping

75. What type of data is commonly recovered from mobile phones during forensic investigations?
    a) Financial transactions
    b) DNA profiles
    c) Geographical coordinates
    **d) Browser history**

76. Which of the following techniques is commonly used to recover deleted data from mobile devices in forensic investigations?
    a) Overwriting the existing data
    b) Fragmenting the storage drive
    **c) Carving or file carving**
    d) Formatting the device

77. In mobile phone forensics, what is the purpose of the "hex dump" analysis?
    a) To analyze network traffic
    b) To extract metadata from files
    c) To recover encrypted data
    **d) To examine raw data at the binary level**

78. Which of the following file systems is commonly used in Android devices and poses challenges for forensic investigators due to its fragmentation?
    a) NTFS
    b) FAT32
    c) HFS+
    **d) Ext4**

79. What is the significance of the Secure Enclave in mobile phone forensics, particularly in iPhones?
    a) It stores user passwords
    b) It encrypts data stored in the cloud
    **c) It protects sensitive data such as biometric information**
    d) It provides access to third-party apps

80. Which of the following techniques can be used to bypass encryption on mobile devices, but is highly intrusive and may void warranties?
    a) File carving
    **b) NAND mirroring**
    c) Firmware flashing
    d) SQL injection

81. What is Social Media Forensics primarily concerned with?
    a) Identifying social media influencers
    b) **Investigating crimes committed on social media platforms**
    c) Analyzing marketing trends on social media
    d) Monitoring social media usage patterns

82. Which of the following is NOT a common type of social media crime?
    a) Cyberbullying
    b) Identity theft
    **c) Video game cheating**
    d) Financial fraud

83. What is the primary purpose of using metadata in social media forensics?
    a) To track the physical location of a user
    b) To analyze user behavior and interactions
    **c) To identify the source and authenticity of digital evidence**
    d) To determine the popularity of a social media post

84. Which of the following is NOT a step in the social media forensics process?
    a) Collection
    b) Analysis
    **c) Creation**
    d) Preservation

85. What legal challenges might arise when conducting social media forensics?
    a) Privacy concerns
    b) Copyright infringement
    c) Defamation
    **d) All of the above**

86. Which of the following techniques can be used to preserve social media evidence?
    a) Taking screenshots
    b) Recording video
    c) Logging into the user's account
    **d) All of the above**

87. What is the term used to describe the process of recovering deleted social media posts?
    a) Data mining
    b) Data scraping
    **c) Data recovery**
    d) Data extraction

88. What role do geotags play in social media forensics?
    **a) They provide information about a user's physical location**
    b) They determine a user's social media activity level
    c) They authenticate a user's identity
    d) They indicate a user's political affiliations

89. Which of the following is a limitation of using social media as evidence in court?
    a) Lack of admissibility
    b) Difficulty in obtaining consent
    **c) Inability to verify authenticity**
    d) Limited storage capacity

90. What is Cryptography primarily concerned with?
    a) Studying ancient civilizations
    **b) Securing communication and data**
    c) Predicting future events
    d) Analyzing financial markets

91. Which of the following is NOT a common goal of cryptography?
    a) Confidentiality
    b) Integrity

**c) Availability**
d) Efficiency

92. What is the primary purpose of encryption in cryptography?
**a) Hiding information**
b) Altering data
c) Deleting files
d) Accessing restricted content

93. Which of the following is NOT a cryptographic technique?
a) Caesar cipher
b) Hash function
**c) Data compression**
d) Public-key encryption

94. What is the term used to describe the process of converting plaintext into ciphertext?
a) Decryption
b) Compression
**c) Encryption**
d) Hashing

95. Which of the following is NOT a component of a cryptographic key?
a) Public key
b) Private key
**c) Hash key**
d) Session key

96. What is the purpose of a cryptographic hash function?
a) Encrypting data
b) Decrypting data
c) Creating digital signatures
**d) Protecting data integrity**

97. Which of the following is NOT a symmetric encryption algorithm?
a) AES (Advanced Encryption Standard)
**b) RSA (Rivest-Shamir-Adleman)**
c) DES (Data Encryption Standard)
d) 3DES (Triple Data Encryption Standard)

98. What is the term used to describe the process of converting ciphertext into plaintext?
**a) Decryption**
b) Encryption
c) Compression
d) Hashing

99. Which of the following is NOT a property of a secure cryptographic algorithm?
    a) Efficiency
    **b) Reversibility**
    c) Resistance to attacks
    d) Key strength

100. You are examining log files and notice several connection attempts to a hosted web server. Several attempts appear as such:
http://www.example.com/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/windows\system32\cmd.exe
What type of attack is in use?
    a) SQL injection
    b) Unicode parameter tampering
    **c) Directory traversal**
    d) Cross-site scripting

101. The accounting department of a business notices several orders that seem to have been made erroneously. In researching the concern, you discover it appears the price of items on several web orders do not match the listed price on the public site. You verify the web server and the ordering database do not seem to have been compromised. Additionally, no alerts have displayed in the Snort logs concerning a possible attack on the web application. Which of the following might explain the attack in play?
    a) **The attacker has copied the source code to his machine and altered hidden fields to modify the purchase price of the items**.
    b) The attacker has used SQL injection to update the database to reflect new prices for the items.
    c) The attacker has taken advantage of a Server Side Include that altered the price.
    d) The attacker used Metasploit to take control of the web application.

102. Which of the following would best represent a parameter-tampering attack?
    **a) http://example.com/add.asp?ItemID=513&Qty=1&Price=15**
    b) http://www.example.com/search.asp?lname=walker%27%update%20usertable%20%20set%3d%23hAxor%27
    c) http://www.example.com/../../../../../../windows\system32\cmd.exe
    d) http://www.example.com/?login=‘OR 1=1-

103. Which form of communication is a real-time, text-based communication type used between two or more people who use mostly text to communicate?
    a) Weblogs
    b) Wikis
    **c) Instant messaging**
    d) Podcasting

104. What prioritizes traffic and its characteristics to manage data?
    a) Network administration

b) Network traffic
**c) QoS strategy**
d) Network evaluation

105. Which of the following is the correct "top down" order of the OSI model?
a) Application, presentation, session, network, transport, data link, physical
**b) Application, presentation, session, transport, network, data link, physical**
c) Application, session, presentation, transport, network, data link, physical
d) Application, presentation, session, network, data link, transport, physical

106. Which of the following is a connection using Telnet?
a) File Transfer Protocol (FTP) session
b) Trivial File Transfer Protocol (TFTP) session
**c) Virtual Terminal (VTY) session**
d) Auxiliary (AUX) session

107. As security in the enterprise increases,
a) ease of use increases and functionality decreases.
b) functionality increases and ease of use decreases.
c) ease of use decreases and functionality increases.
**d) functionality decreases and ease of use decreases.**

108. You want to ensure your messages are safe from unauthorized observation, and you want to provide some means of ensuring the identities of the sender and receiver during the communications process. Which of the following best suits your goals?
a) Steganography
**b) Asymmetric encryption**
c) Hash
d) Symmetric encryption

109. You've discovered that an expired certificate is being used repeatedly to gain logon privileges. Which type of attack is this most likely to be?
a) Man-in-the-middle attack
b) Back door attack
**c) Replay attack**
d) TCP/IP hijacking

110. Your system has been acting strangely since you downloaded a file from a colleague. Upon examining your antivirus software, you notice that the virus definition file is missing. Which type of virus probably infected your system?
a) Polymorphic virus
**b) Retrovirus**
c) Worm
d) Armored virus

111. Which device stores information about destinations in a network?
a) Hub

b) Modem
c) Firewall
**d) Router**

112. Which of the following is *not* a part of an incident response?
a) Identification
b) Investigating
**c) Entrapment**
d) Repairing

113. The set of procedures, policies and guidelines that commence at the detection of an incident is the _____.
a) computer forensics
b) digital forensics
**c) incident response**
d) investigation

114. In _____ acquisition, the data acquisition method captures only specific files of interest to the case or specific types of files, such as Outlook PST files.
a) live
b) sparse
**c) logical**
d) All of these

115. PEM stands for _____.
a) Public Encryption Mail
**b) Privacy Enhanced Mail**
c) Privacy Enhanced Message
d) Public Encryption Message

116. A set of duplicate data that is stored in a temporary location to allow rapid access for computers to function more efficiently, is known as _____.
a) boot record
b) metadata
c) swap
**d) cache**

117. The Netstat command indicates that POP3 is in use on remote server. Which port is the remote server?
a) port 25
**b) port 110**
c) port 80
d) port 143

118. What are the types of scanning?

a) Port, network, and services
**b) Network, vulnerability, and port**
c) Passive, active, and interactive
d) Server, client, and network

119. In _____ acquisition, like logical acquisitions, this data acquisition method captures only specific files of interest to the case, but it also collects fragments of unallocated data.
a) Live
**b) sparse**
c) logical
d) data and information

120. What is synchronization?
a) Keeping the correct time of day on all network machines
**b) The timing mechanism devices use when transmitting data**
c) Devices processing bits to the data link layer at the same speed
d) Constant bit times throughout the network

**-End of Paper-**