Digital Forensics

Answer Key

(Correct Answers are marked in bold letters)

Section -A
Forensic Aptitude

1. Which country won the 2019 Ice Hockey World Championship?
   a) Russia
   b) Finland
   c) Canada
   d) Czech Republic

2. Which Indian state shares the longest land border with Bhutan?
   a) Assam
   b) Sikkim
   c) Arunachal Pradesh
   d) West Bengal

3. Which of the following is the longest train route in the world?
   a) Moscow to Vladivostok
   b) Toronto to Vancouver
   c) Shanghai to Lhasa
   d) Sydney to Perth

4. Identify the southernmost located country amongst these
   a) Madagascar
   b) Sri Lanka
   c) New Zealand
   d) Fiji

5. India shares its land borders with how many countries.
   a) 5
   b) 7
   c) 9
   d) 4

6. I will write a letter to you tentatively _____ the dates of the program.
   a) involving
   b) urging
   c) guiding
   d) indicating

7. 2 16 112 672 3360 13440 ?

a) 3430
b) 3340
c) 40320
d) 43240

8. 40% of 210 is same as one third of?
a) 840
b) 280
c) 252
d) 84

9. QPO, NML, KJI, _____, EDC
a) HGF
b) CAB
c) JKM
d) GHD

10. Samantha is your father's mother's grandson's daughter. Therefore, Samantha is your
a) niece
b) sister
c) uncle
d) brother

11. The microscope which cannot be used for studying living cells is
a) Compound microscope
b) Electron microscope
c) Fluorescence microscope
d) Light microscope

12. What is the primary purpose of accrediting forensic labs?
a) Financial gain
b) Legal compliance
c) Quality assurance
d) Employee satisfaction

13. In which country did Sir William Herschel pioneer the use of fingerprints for identification in the 19th century?
a) United States
b) United Kingdom
c) India
d) France

14. The development of the Automated Fingerprint Identification System (AFIS) has greatly enhanced:
a) Bloodstain pattern analysis

b) Fingerprints
c) DNA profiling
d) Toxicological analysis

15. The concept of "Every contact leaves a trace" is associated with the work of:
    a) Calvin Goddard
    b) Edmond Locard
    c) Alphonse Bertillon
    d) Sir William Locard

16. Who is "Father of Forensic Entomology"?
    a) Dr. William Bass
    b) Dr. Clyde Snow
    c) Dr. Michael Baden
    d) Dr. Bernard Green Berg

17. Next number in the series 3,6,8,16,18,……is
    a) 28
    b) 36
    c) 54
    d) 34

18. If today is Wednesday, what would be the day after 121 days
    a) Wednesday
    b) Saturday
    c) Sunday
    d) Friday

19. Which is the correct spelt word
    a) Capricious
    b) Cappricious
    c) Caprisious
    d) Caprisuos

20. During electrophoresis speed of migration of ions depends on:
    a) Shape and size of molecule
    b) Magnitude of charge and shape of molecule
    c) Magnitude of charge, shape and mass of molecule
    d) Magnitude of charge and mass of molecule

21. A bullet from scene of crime is collected by means of
    a) Forceps
    b) Tongs
    c) Gloved hands
    d) Spatula

22. Chelioscopy is study of
    a) Foot
    b) Fingers
    c) Palate
    d) Lips

23. The electromagnetic spectrum's Visible region stretches from:
    (a) 380-760 nm
    (b) 500-1mm
    (c) 165-525 nm
    (d) 760-1 mm

24. Which of the following Microscope uses light as a source of illumination
    a) SEM
    b) TEM
    c) Stereo microscope
    d) Scanning probe microscope

25. What type of evidence includes tangible items such as weapons, clothing, or documents that are directly related to a crime?
    a) Circumstantial evidence
    b) Physical evidence
    c) Testimonial evidence
    d) Documentary evidence

26. A witness testifying about what they personally observed or experienced is providing:
    a) Circumstantial evidence
    b) Hearsay evidence
    c) Testimonial evidence
    d) Documentary evidence

27. Which technique involves casting three-dimensional replicas of footwear impressions found at a crime scene?
    a) Shoeprint analysis
    b) Casting
    c) Electrostatic dust print lifting
    d) Bloodstain pattern analysis

28. What is the primary purpose of creating a crime scene sketch?
    a) To replace photographs

b) To provide a visual overview of the crime scene
c) To identify suspects
d) To collect physical evidence

29. The immediate surroundings of an area where a crime has been committed is referred to as:
a) A secondary crime scene
b) A primary crime scene
c) An auxiliary crime scene
d) A contained crime scene

30. What is the primary purpose of Crime Scene Photography?
a) To document the Investigator's presence
b) To create artistic representations of the crime scene
c) To provide a visual record of the entire crime scene
d) To capture only close-up shots of evidence

31. In crime scene reconstruction, what does the term "modus operandi" refer to?
a) The suspect's motive
b) The method of operation used by the suspect
c) The victim's actions at the crime scene
d) The legal procedures followed during the investigation

32. What does the term "Integrity of the Chain of Custody" refer to?
a) Keeping the evidence in pristine condition
b) Ensuring a swift transfer of evidence
c) Allowing multiple agencies to handle the evidence
d) Sharing evidence with the media

33. Which organization is responsible for accrediting forensic laboratories in India according to ISO/IEC 17025 standards?
a) FSSAI
b) NABH
c) NABL
d) BIS

34. To identify the shape of univariate data, what type of graph would be the most useful?
a) Histogram
b) Scatter plot
c) Bar chart
d) Pie chart

35. What is the purpose of staining in gel electrophoresis?
a) To regulate temperature

b) To enhance electrical conductivity
c) To visualize separated molecules
d) To control pH

36. Sum of deviations will be zero if it is taken from
a) Mean
b) Mode
c) Medium
d) Standard Deviation

37. Find the median of the given data set: 5, 8, 12, 17, 2, 14, 6, 8, 13 and 7
a) 5
b) 2
c) 8
d) 17

38. The reducing action of developing agents for Black & White film –
a) Potassium Sulphite
b) Potassium Bromide
c) Sodium Carbonate
d) Sodium Thiosulphate

39. The Exposure Triangle refer to the three major setting that effect Exposure -
a) ISO, Aperture, Shutter Speed
b) Aperture, Shutter Speed, Focal Length
c) Quality of Camera, Aperture, Shutter Speed
d) Film, Lens & Colour

40. As per Section 8 of the Indian Evidence Act, 1872 which of the following is a relevant fact:
a) Motive
b) Preparation
c) Subsequent Conduct
d) All of the above

41. Under the PFA Act, when is the food said to be adulterated
a) if any ingredient is injurious to health
b) if it is obtained from a diseased animal
c) if spices are sold without their essence
d) all of these

42. Coca, hemp and opium are defined under:
a) The Narcotic Drugs and Psychotropic Substances Act
b) The Pharmacy Act

c) The Drugs and Cosmetics Act
d) The Poisons Act

43. Which of the following methods is non-destructive technique for ink identification
a) Solubility test
b) Thin layer chromatography
c) UV-Vis spectrophotometer
d) Videospectral analysis

44. Milk is deficient of which mineral?
a) Phosphorus
b) Sodium
c) Iron
d) Potassium

45. Preservation of footprint on snow can be done by
a) Plaster of Paris Cast
b) Sulphur casting
c) Tracing
d) Wax Casting

46. Ridge characteristics can be found in:
a) Footprint
b) Fingerprints
c) Palm prints
d) All

47. In which section of the CrPC provision for free legal aid is given:
a) 314
b) 381
c) 304
d) 334

48. The image seen through a compound microscope is-
a) Virtual
b) Real
c) False
d) Imaginary

49. Which of the following is a non-volatile memory?
a) RAM
b) Hard Disk
c) Cache
d) ROM

50. What is the full form of ALU?
    a) Arithmetic Logical Unit
    b) Arithmetic Local Unit
    c) Arithmetic Logic Unit
    d) Arithmetic Logic Unity

Section –B
Digital Forensics

51. Hard disk are organized as
    a) Cylinders only
    b) Tracks only
    c) **Cylinders and tracks**
    d) Master Boot Record

52. FDISK command is used to?
    a) **Creates partitions on a hard drive**
    b) Does fragmentation on the hard drive
    c) Fix bad sectors on hard drive
    d) Recover lost clusters on hard drive

53. The platters of a hard disk are coated with
    a) **Magnetic material**
    b) Non-magnetic material
    c) Polyvinyl coating
    d) Silica gel

54. _____has smallest storage capacity
    a) Floppy disk
    b) Zip disk
    c) Hard disk
    d) CD

55. UDF stands for
    a) Undated Disk Format
    b) Universal Data Frequency
    c) Unique Disk Format
    d) Universal Disk Format

56. What is the main directory of a disk called?
    a) Folder
    b) **Root**
    c) Sub
    d) Network

57. USB stands for
    a) **Universal Serial Bus**

b) Universal Sequential Bus
c) Uniform Serial Bus
d) United Serial Bus

58: How many pins does an IDE cable/connector have?

a) 36
b) **40**
c) 42
d) 44

59. Which of the following is a potential consequence of mishandling digital evidence?

a) Legal admissibility
b) Data authentication
c) Chain of custody violation
d) Data replication

60. Which of the following is NOT a common digital forensic technique?

a) Data obfuscation
b) File carving
c) Memory analysis
d) Hashing

61. The area that begins at the end of the last sector that contains logical data and terminates at the end of the cluster is known as:

a) File Slack
b) HDD Slack
c) ROM Slack
d) RAM Slack

62. In Digital Forensic, Hash/Hashing algorithms are used to:

a) Search malicious data
b) Verify integrity of copied data
c) Detect viruses
d) None of the above.

63.What is the full form of CDMA:

a) Code Division Multiple Access
b) Code Division Machine Access
c) Cellular Division Multiple Access
d) Code Division Multi-user Access

64. IMEI of a mobile device means:

a) International Mobile Equipment Identity
b) International Mobile Evidence Identity

c) Integrated Mobile Equipment Identity
d) International Machine Equipment Identity

65. Which of the following is NOT a potential challenge in digital forensic investigations?
a) Data corruption
b) Limited storage capacity
c) Rapid technological advancements
d) Lack of digital devices

66. Cyber Security provides security against what?
a) Against Malware
b) Against cyber-terrorists
c) Defends a device from threat.
d) All mentioned options

67. Which of the below benefits of cyber security is not true?
a) System getting slower
b) Computer lagging and crashes
c) provide privacy to users
d) Secures system against viruses

68. The process of documenting the seizure of digital evidence and, in particular, when that Evidence changes hands, is known as:
a) **Chain of custody**
b) Field notes
c) Interim report
d) None of the above

69. Which of the following pertains to network infrastructure security?
a) A competitor accesses sensitive information through an unsecured wireless network.
b) Builders accidentally cut a network cable while digging.
c) A disgruntled employee alters information in a customer database.
d) A secretary sends confidential information in a reply to an e-mail that falsely appears to come from her boss.

70. What is the name of the IT law that India is having in the Indian legislature?
a) India's Technology (IT) Act, 2000
b) India's Digital Information Technology (DIT) Act, 2000
c) **India's Information Technology (IT) Act, 2000**
d) The Technology Act, 2008

71. Which technique is used for data protection?
a) Data piracy
b) Authentication

c) Encryption
d) None of these

72. What is true about "bit time"?
a) It is the time it takes to encapsulate application data into a bit segment.
b) It is the time it takes for a NIC to move a bit from the data link layer to the Layer 1 media.
c) IEEE standards require it to be the same on all NICs.
d) It is the time it takes for a byte to traverse the copper or fiber cable

73. Even with two-factor authentication, users are vulnerable to which attacks.
a) Man-in-the-middle
b) Cross attack
c) Scripting
d) Radiant

74. Which factor uses in many applications, where two independent factors are used to identify a user?
a) Cross-site scripting
b) Cross-site request forgery
c) Two-factor authentication
d) Cross-site scoring scripting

75. Which of the below is used to analyse network flow and monitor traffic?
a) Managed detection and response
b) Cloud access security broker
c) Network traffic analysis
d) Secondary Storage Media Data Analysis

76. The term "protection from _____of source code" refers to limiting access to the source code to just authorised individuals.
a) disclosure
b) alteration
c) destruction
d) log of changes

77. _____ refers to phishing performed over smart-phone by calling.
a) Algo-based phishing
b) Email-based phishing
c) Domain Phishing
d) Vishing

78. _____ are programs or devices that capture the vital information from the target network or particular network.
a) Routers
b) Trappers

c) Wireless-crackers
d) Sniffers

79. _____ is the attack method for decoding user credentials. Using this technique an attacker can log on as a user & gain access to unauthorized data.
a) Cache Snooping
b) Cookie-jacking
c) Cookie Snooping
d) Cache-compromising

80. _____ tracks your data and displays those products as ads for promotions.
a) **Ad-based spyware**
b) System Monitors
c) Spy-trojans
d) Tracking cookies

81. Key loggers are form of
a) Spyware
b) Shoulder surfing
c) Trojan
d) Social engineering

82. SNMP stands for
a) Simple Network Message Protocol
b) Simple New Message Protocol
c) Simple Network Management Protocol
d) Simple Network Managing Protocol

83. Which attack allows the attacker to execute the scripts on the victim's browser?
a) SSL attack
b) Cookie attack
c) Banner grabbing
d) XSS attack

84. A/an _____ attack is one of the simplest processes of gaining access to any password-protected system.
a) Click jacking
b) Brute force
c) Eavesdropping
d) Waterhole

85. _____ are difficult to identify as they keep on changing their type and signature.
a) Non-resident virus
b) Boot Sector Virus
c) Polymorphic Virus

d) Multipartite Virus

86. _____ are implemented to carry out distributed DDoS attacks, steal data, send spam messages & permits the hacker to access various devices & its connection.
a) Trojan
b) Virus
c) Botnet
d) Worms

87. Which of the below is a hacking technique in which cybercriminals create fictitious web pages or domains to deceive or obtain more traffic?
a) Pharming
b) Mimicking
c) Spamming
d) Website-Duplication

88. Which of the below implemented is not a good means of safeguarding privacy?
a) Biometric verification
b) ID and password-based verification
c) 2-factor authentication
d) switching off the phone

89. The method of hiding the secret is:
a) Cryptography
b) Hashing
c) Cartography
d) Cryptanalysis

90. The_is the message after transformation.
a) cipher text
b) plain text
c) Readable Text
d) Writable Text

91. In an asymmetric-key cipher, the sender uses the_____key.
a) private
b) **public**
c) either (a) or (b)
d) neither (a) nor (b)

92. One commonly used public-key cryptography method is the__algorithm.
a) RSS
b) RAS
c) RSA
d) RAA

93. Hash functions guarantee message integrity and that the message has not been _____.
    a) Over view
    b) Replaced
    c) Violated
    d) Changed

94. SSID is abbreviated as
    a) Service Set Independent Device
    b) Service Set Identifier
    c) Secure Set Independent Device
    d) Secure Service Identifier

95. In networks protocol TCP/ IP stands for.
    a) Transaction Control Protocol
    b) **Transmission Control Protocol**
    c) Transmission Contribution Protocol
    d) None of These

96. Physical or logical arrangement of network is
    a) **Topology**
    b) Routing
    c) Networking
    d) None of the mentioned

97. Data communication system spanning states, countries, or the whole world is
    a) LAN
    b) **WAN**
    c) MAN
    d) None of the mentioned

98. Which of the following is NOT a principle of digital forensic analysis?
    a) Volatility
    b) Integrity
    c) Availability
    d) Authenticity

99. In wireless distribution system
    a) **multiple access points are inter-connected with each other**
    b) there is no access point
    c) only one access point exists
    d) none of the mentioned

100. In wireless network an extended service set is a set of
    a) **Connected basic service sets**

b) all stations
c) all access points
d) none of the mentioned

101. Mostly_____is used in wireless LAN.

a) time division multiplexing
b) **orthogonal frequency division multiplexing**
c) space division multiplexing
d) none of the mentioned

102. What is Wired Equivalent Privacy (WEP)?

a) security algorithm for ethernet
b) **security algorithm for wireless networks**
c) security algorithm for usb communication
d) none of the mentioned

103. In _____ same keys are implemented for encrypting as well as decrypting the information.

a) **Symmetric Key Encryption**
b) Asymmetric Key Encryption
c) Asymmetric Key Decryption
d) Hash-based Key Encryption

104. DES stands for _____

a) Data Encryption Security
b) Data Encrypted Standard
c) Device Encryption Standard
d) **Data Encryption Standard**

105. Packet filtering firewalls are deployed on _____

a) routers
b) switches
c) hubs
d) repeaters

106. _____ is the process or mechanism used for converting ordinary plain text into garbled non-human readable text & vice-versa.

a) Malware Analysis
b) Exploit writing
c) Reverse engineering
d) **Cryptography**

107. Cryptographic algorithms are based on mathematical algorithms where these algorithms use _____ for a secure transformation of data.
    a) **secret key**
    b) external programs
    c) add-ons
    d) secondary key

108. What is the term used to describe the process of extracting information from digital devices without altering the original data?
    a) Data replication
    b) Data extraction
    c) Data obfuscation
    d) Data corruption

109. Which of the statements are not true to classify VPN systems?
    a) Protocols used for tunnelling the traffic
    b) Whether VPNs are providing site-to-site or remote access connection
    c) **Securing the network from bots and malwares**
    d) Levels of security provided for sending and receiving data privately

110. _____ masks your IP address.
    a) Firewall
    b) Antivirus
    c) **VPN**
    d) Incognito mode

111. _____ is a type of DoS threats to overload a server as it sends a large number of requests requiring resources for handling & processing.
    a) Network Layer DoS
    b) Physical Layer DoS
    c) Transport Layer DoS
    d) **Application Layer DoS**

112. Which of the following is an application of drone?
    a) Project Monitoring
    b) Aerial Mapping
    c) Structural Health Monitoring
    d) All of the above

113. When information is read or copied by someone not authorized to do so, the result is known as _____
    a) loss of confidentiality
    b) loss of integrity
    c) loss of availability
    d) All of the above

114. The_____ layer uses data compression to reduce the number of bits to be transmitted.
    a) Presentation
    b) Network
    c) data link
    d) application

115. OSI stands for
    a) **Open System Interconnection**
    b) Operating System Interface
    c) Optical Service Implementation
    d) None of the mentioned

116**.** In Cyber Crime the attacker leaves multiple traces of their presence in:
    a) File System
    b) Registry
    c) System Logs
    d) All of the Above

117**.** _____ is a crime committed when someone uses the internet and other technologies to harass or stalk another person online.
    a) Cyber Bullying
    b) Cyber stalking
    c) Identity Theft
    d) None

118. What is the term used to describe the act of using social media to engage in romantic or sexual relationships with minors?
    a) Cyberstalking
    b) Catfishing
    c) Grooming
    d) Sexting

119. All cloud computing applications suffer from the inherent _____ that is intrinsic in their WAN connectivity.
    a) Noise
    b) Propagation
    c) Latency
    d) all of the mentioned

120. Which of the following is a potential challenge in authenticating social media evidence?

    a) Encryption
    b) Timestamp manipulation
    c) Content deletion

d) All of the above

-End of Paper-