

SSA - Multimedia Forensics - Examination

1. In a row of 6 people, A is to the left of B but right of C. D is to the right of E who is at the extreme left. F is between A and D. Who is at the extreme right?

- ☒ A B
- ☐ B D
- ☐ C F
- ☐ D E

2. 1, 5, 17, 53, 161, ?

- ☒ A 485
- ☐ B 324
- ☐ C 231
- ☐ D 392

3. All artists are creative. Some engineers are artists. Which conclusion follows?

- ☐ A All engineers are creative.
- ☒ B Some engineers are creative.
- ☐ C No engineers are creative.
- ☐ D Creativity is limited to artists.

4. A shopkeeper marks an item at 25% above cost but gives a 10% discount. What is his profit %?

- ☐ A 0.1
- ☒ B 0.125
- ☐ C 0.15
- ☐ D 0.175

5. If 3 machines produce 60 units in 4 hours, how many units will 5 machines produce in 6 hours?

A 120

✓ B 150

C 180

D 200

6. From point A, you walk 10m east, turn left and walk 15m, then turn right and walk 5m. How far are you from A?

A 10 m

B 15 m

✓ C 20 m

D 25 m

7. Sarathi is your father's mother's grandson's daughter. Therefore, Sarathi is your

✓ A niece

B Sister

C Uncle

D Brother

8. A number is mistakenly divided by 5 instead of being multiplied by 5. The correct answer should be 500. What was the wrong result obtained?

A 20

B 25

✓ C 50

D 100

9. If $a + b = 10$ and $a^2 + b^2 = 58$, find ab .

A 15

✓ B 16

C 17

D 18

10. If $7x - 3 = 4x + 9$, what is the value of x ?

- ☐ A 2
- ☐ B 3
- ☒ C 4
- ☐ D 5

11. I will write a letter to you tentatively _____ the dates of the program.

- ☐ A involving
- ☐ B urging
- ☐ C guiding
- ☒ D indicating

12. 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

13. Components that provide internal storage to the CPU are _____

- ☒ A Registers
- ☐ B Program Counters
- ☐ C Controllers
- ☐ D Internal chips

14. Which is a characteristic of solid-state drives (SSDs) compared to traditional hard drives (HDDs)?

- ☐ A Slower read/write speeds
- ☐ B Less reliable storage
- ☐ C Uses spinning disks
- ☒ D No moving parts

15. Which of the following are not in a compressed format?

- ☐ A JPEG
- ☒ B Bitmap
- ☐ C MPEG
- ☐ D MP3

16. _____ is the computer program that would convert an assembly language to the machine language.

- ☐ A Interpreter
- ☐ B Compiler
- ☐ C Comparator
- ☒ D Assembler

17. What is the full form of Ping network command?

- ☒ A Packet Internet or Inter-Network Groper
- ☐ B Packet Intra Network Groper
- ☐ C Packet INformation Groper
- ☐ D Packet INfrastrcture Group

18. What is the primary purpose of a security incident response plan?

- ☐ A To encrypt sensitive data during transmission
- ☐ B To block malicious websites
- ☐ C To detect and remove malware from a system
- ☒ D To outline procedures for responding to and managing cybersecurity incidents

19. Which of the following is not a type of volatile evidence?

- ☐ A Routing Table
- ☐ B Running Processes
- ☒ C Log Files
- ☐ D Cached data

20. Which of the following steganography types hides the secret message in a specifically designed pattern on the document that is unclear to the average reader?

- ☒ **A** Open code steganography
- ☐ **B** Visual semagrams steganography
- ☐ **C** Text semagrams steganography
- ☐ **D** Technical steganography

21. Which of the following statements is incorrect when preserving digital evidence?

- ☐ **A** Document the actions and changes that you observe in the monitor, computer, printer, or in other peripherals
- ☐ **B** Verify if the monitor is in on, off, or in sleep mode
- ☐ **C** Remove the power cable depending on the power state of the computer i.e., in on, off, or in sleep mode
- ☒ **D** Turn on the computer and extract Windows event viewer log files

22. Which of the following statements is incorrect related to acquiring electronic evidence at crime scene?

- ☐ **A** Sample banners are used to record the system activities when used by the unauthorized user
- ☐ **B** In warning banners, organizations give clear and unequivocal notice to intruders that by signing onto the system they are expressly consenting to such monitoring
- ☐ **C** The equipment is seized which is connected to the case, knowing the role of the computer which will indicate what should be taken
- ☒ **D** At the time of seizing process, you need to shut down the computer immediately

23. Disk wiping process refers to

- ☐ **A** Carving the data from Slack Space
- ☐ **B** Investigate Unallocated Space
- ☐ **C** Defrag the disk content
- ☒ **D** Overwrite data for multiple times

24. What is the primary risk associated with deepfake technology?

- ☐ **A** Decreased bandwidth
- ☐ **B** Improved system performance
- ☒ **C** Misinformation and identity theft
- ☐ **D** Data encryption

25. In a certain code "FL4M3" is written as "IO7P6". How is "L1GH7" written in that code?

- ☐ A F1D8E
- ☐ B X8KV8
- ☒ C O4JK10
- ☐ D 2E4R4

26. BMP (Bitmap) is a standard file format for computers running the Windows OS. BMP images can range from black and white (1 bit per pixel) up to 24 bit color (16.7 million colors). Each bitmap file contains a header, the RGBQUAD array, information header, and image data. Which of the following element specifies the dimensions, compression type, and color format for the bitmap?

- ☐ A Image data
- ☐ B The RGBQUAD array
- ☒ C Information header
- ☐ D Header

27. Jack is reviewing file headers to verify the file format and hopefully find more information of the file. After a careful review of the data chunks through a hex editor; Jack finds the binary value 0xffd8ff. Based on the above information, what type of format is the file/image saved as?

- ☐ A ASCII
- ☐ B BMP
- ☐ C GIF
- ☒ D JPEG

28. Which ISO standard enables laboratories to demonstrate that they comply with quality assurance and provide valid results?

- ☒ A ISO/IEC 17025
- ☐ B ISO/IEC 18025
- ☐ C ISO/IEC 16025
- ☐ D ISO/IEC 19025

29. What is multimedia forensics primarily concerned with?

- ☐ A Creating multimedia content
- ☒ B Detecting manipulation and verifying authenticity of digital media
- ☐ C Enhancing image quality for better visualization
- ☐ D Storing multimedia files securely

30. Which of the following is a common technique used in image forensics?

- ☒ **A** Metadata analysis
- ☐ **B** Firewall protection
- ☐ **C** Data compression
- ☐ **D** Hashing algorithms

31. What does EXIF data in an image file contain?

- ☐ **A** Only the image pixels
- ☒ **B** Camera settings, timestamps, and GPS coordinates
- ☐ **C** Encryption keys
- ☐ **D** Audio waveforms

32. Which forensic method detects copy-move forgery in images?

- ☐ **A** Error Level Analysis (ELA)
- ☒ **B** Block-matching algorithms
- ☐ **C** Steganalysis
- ☐ **D** Hash verification

33. What is steganalysis used for?

- ☐ **A** Embedding hidden messages in images
- ☒ **B** Detecting steganography (hidden data) in multimedia files
- ☐ **C** Compressing video files
- ☐ **D** Enhancing audio quality

34. Which tool is commonly used for multimedia forensic analysis?

- ☐ **A** Wireshark
- ☐ **B** Autopsy
- ☒ **C** Amped Authenticate
- ☐ **D** Nmap

35. What does Error Level Analysis (ELA) help identify?

- ☒ **A** Different compression levels in an image to detect tampering
- ☐ **B** Encryption keys in a video file
- ☐ **C** Audio watermarking
- ☐ **D** Network packet analysis

36. In video forensics, what does "inter-frame forgery" refer to?

- ☒ **A** Altering individual frames within a video
- ☐ **B** Changing the audio track of a video
- ☐ **C** Compressing the video file
- ☐ **D** Adding subtitles to a video

37. Which of the following is NOT a type of multimedia forensic investigation?

- ☐ **A** Detecting deepfake videos
- ☐ **B** Identifying spliced audio recordings
- ☒ **C** Recovering deleted emails
- ☐ **D** Verifying the originality of a photograph

38. What is the role of hash values in multimedia forensics?

- ☐ **A** To enhance image brightness
- ☒ **B** To verify file integrity and detect alterations
- ☐ **C** To compress multimedia files
- ☐ **D** To encrypt multimedia files

39. An investigator needs to perform data acquisition from a storage media without altering its contents to maintain the integrity of the content. The approach adopted by the investigator relies upon the capacity of enabling read-only access to the storage media. Which tool should the investigator integrate into his/her procedures to accomplish this task?

- ☒ **A** Write blocker
- ☐ **B** Backup tool
- ☐ **C** Data duplication tool
- ☐ **D** BitLocker

40. Electric Network Frequency (ENF) analysis is used to:

- ☐ **A** Detect pitch variations in speech
- ☒ **B** Authenticate recordings based on power grid fluctuations
- ☐ **C** Remove electrical interference from audio
- ☐ **D** Enhance bass frequencies

41. Which algorithm is commonly used for non-stationary noise reduction?

- ☐ A FFT filtering
- ☐ B Wiener filter
- ☒ C Spectral subtraction
- ☐ D LMS adaptive filter

42. What forensic technique identifies recording devices through unique artifacts?

- ☐ A ENF analysis
- ☒ B Microphone signature profiling
- ☐ C Spectrogram analysis
- ☐ D Huffman coding

43. Which AI model is used for speech enhancement in noisy recordings?

- ☐ A GPT-4
- ☐ B U-Net
- ☐ C ResNet
- ☒ D WaveNet

44. Which artifact is commonly associated with JPEG compression?

- ☐ A Motion blur
- ☐ B Color banding
- ☒ C Blocking artifacts
- ☐ D Chromatic aberration

45. Photo-Response Non-Uniformity (PRNU) analysis is used to:

- ☐ A Enhance image sharpness
- ☐ B Detect image splicing
- ☒ C Identify the source camera
- ☐ D Correct color balance

46. Chromatic aberration in an image refers to:

- ☐ A Blurring due to motion
- ☒ B Misalignment of color channels
- ☐ C Overexposure of highlights
- ☐ D Underexposure of shadows

47. Which noise reduction technique is useful for forensic images?

- ☒ **A** Median filtering
- ☐ **B** JPEG compression
- ☐ **C** Pixelation
- ☐ **D** Color quantization

48. Super-resolution techniques in forensics are used to:

- ☒ **A** Increase image resolution from low-quality sources
- ☐ **B** Delete EXIF data
- ☐ **C** Add digital watermarks
- ☐ **D** Reduce file size

49. What does "noise consistency analysis" reveal in image forensics?

- ☒ **A** Whether noise patterns match across regions
- ☐ **B** The camera's shutter speed
- ☐ **C** The image's file format
- ☐ **D** Hidden text in the image

50. What is the primary purpose of crime scene photography?

- ☐ **A** To create artistic visuals
- ☒ **B** To document evidence objectively for investigations
- ☐ **C** To enhance image colors for presentations
- ☐ **D** To reduce the number of written reports

51. Why is a scale (ruler) used in close-up forensic photography?

- ☐ **A** To add professionalism
- ☒ **B** To provide size reference for evidence
- ☐ **C** To block unwanted light
- ☐ **D** To comply with social media guidelines

52. What is the "360-degree rule" in crime scene videography?

- ☒ **A** Recording a full panoramic view of the scene
- ☐ **B** Using a 360° camera only
- ☐ **C** Keeping the camera at eye level
- ☐ **D** Avoiding vertical videos

53. What does "chain of custody" documentation include for photos/videos?

- ☒ **A** Timestamps, photographer's name, and storage details
- ☐ **B** Only the camera model
- ☐ **C** Social media shares
- ☐ **D** Editing history in Photoshop

54. What is "bracketing" in crime scene photography?

- ☒ **A** Taking multiple shots at different exposures
- ☐ **B** Cropping images post-capture
- ☐ **C** Using only black-and-white mode
- ☐ **D** Deleting blurry photos

55. How should reflective surfaces (e.g., glass, metal) be photographed?

- ☒ **A** Use a polarizing filter
- ☐ **B** Direct flash only
- ☐ **C** Avoid photographing them
- ☐ **D** Shoot from a 90° angle

56. Which vocal characteristic is most unique to an individual?

- ☐ **A** Pitch
- ☐ **B** Speaking rate
- ☐ **C** Formant frequencies
- ☒ **D** All of the mentioned

57. Which feature is extracted for voice biometrics?

- ☒ **A** Mel-Frequency Cepstral Coefficients (MFCCs)
- ☐ **B** RGB pixel values
- ☐ **C** EXIF metadata
- ☐ **D** File compression ratio

58. Which database is used for training speaker ID systems?

- ☒ **A** TIMIT
- ☐ **B** MNIST
- ☐ **C** ImageNet
- ☐ **D** None of the MENTIONED

59. Bilinear transform is used for:

- ☒ **A** Analog-to-digital filter conversion
- ☐ **B** Quantization
- ☐ **C** DFT computation
- ☐ **D** Noise reduction

60. Adaptive filters are used in:

- ☐ **A** Image enhancement
- ☒ **B** Echo cancellation
- ☐ **C** Data encryption
- ☐ **D** All of the above

61. What does "stance phase" refer to in gait analysis?

- ☒ **A** Foot contact with the ground
- ☐ **B** Arm swing during walking
- ☐ **C** Head movement
- ☐ **D** Eye blinking rate

62. Which factor is critical for accurate photogrammetry?

- ☒ **A** High overlap between images
- ☐ **B** Low-resolution photos
- ☐ **C** Single camera angle
- ☐ **D** Blurry images

63. Which forensic scenario uses both gait and photogrammetry?

- ☒ **A** Suspect identification from CCTV footage
- ☐ **B** Blood spatter analysis
- ☐ **C** DNA sequencing
- ☐ **D** Voice recording

64. Which technique is used for object detection in videos?

- ☐ **A** MPEG compression
- ☐ **B** Huffman encoding
- ☒ **C** YOLO (You Only Look Once)
- ☐ **D** JPEG artifact analysis

65. What does "frame differencing" detect in video analytics?

- ☐ A Color saturation changes
- ☒ B Motion between consecutive frames
- ☐ C Audio synchronization issues
- ☐ D File format corruption

66. Which approach selects keyframes for summarization?

- ☐ A Random frame deletion
- ☐ B Increasing bitrate
- ☒ C Uniform sampling
- ☐ D Adding watermarks

67. Which industry uses video analytics for crowd monitoring?

- ☐ A Textile manufacturing
- ☐ B Food delivery
- ☐ C Pharmaceutical research
- ☒ D Surveillance and security

68. What is "anomaly detection" in video analytics?

- ☒ A Identifying unusual events
- ☐ B Measuring video brightness
- ☐ C Counting total frames
- ☐ D Converting videos to GIFs

69. What is "temporal action localization"?

- ☐ A Geotagging video files
- ☒ B Identifying start/end times of actions in videos
- ☐ C Stabilizing shaky footage
- ☐ D Detecting copyright violations

70. What does "video synopsis" achieve?

- ☐ A Converts videos to text
- ☐ B Adds subtitles automatically
- ☒ C Condenses long recordings by showing concurrent events together
- ☐ D Encrypts video content

71. Which metadata is critical for NVR forensic investigations?

- ☐ A Video brightness levels
- ☒ B Camera IP/MAC addresses
- ☐ C Speaker volume settings
- ☐ D HDMI port number

72. What does "motion-only recording" imply in DVR/NVR systems?

- ☐ A Audio is disabled
- ☐ B Frames are deleted after 24 hours
- ☐ C Encryption is automatically applied
- ☒ D Video is saved only when motion is detected

73. What is the primary difference between DVR and NVR systems?

- ☐ A DVR uses analog cameras; NVR uses IP cameras
- ☒ B DVR processes video locally; NVR streams over a network
- ☐ C NVR only works with wireless cameras
- ☐ D DVR cannot record audio

74. India's Digital Personal Data Protection Act (DPDPA) was enacted in:

- ☐ A 2003
- ☐ B 2013
- ☐ C 2020
- ☒ D 2023

75. The Examiner of Electronic Evidence is appointed under which section of IT Act?

- ☐ A Section 65B
- ☒ B Section 79A
- ☐ C Section 43A
- ☐ D Section 72A

76. Which types of digital evidence can the Examiner of Electronic Evidence analyze?

- ☐ A Only financial fraud data
- ☐ B Only social media content
- ☐ C Only encrypted data
- ☒ D All electronic records

77. Which provision replaces Section 65B of IEA?

- ☒ **A** BSA Section 63
- ☐ **B** BSA Section 90
- ☐ **C** BNS Section 176
- ☐ **D** BNSS Section 105

78. The term "Google Dorking" refers to:

- ☐ **A** Google's internal hacking team
- ☐ **B** A type of malware
- ☐ **C** Google's privacy policy
- ☒ **D** Advanced search operators to find vulnerable systems/data

79. What metadata can be extracted from a Twitter post?

- ☐ **A** User's password
- ☐ **B** IP address of all viewers
- ☐ **C** Device IMEI number
- ☒ **D** Tweet ID, timestamp, location (if enabled)

80. Instagram geolocation data is available when:

- ☒ **A** User enables "Add Location" to posts
- ☐ **B** For all posts automatically
- ☐ **C** Only to law enforcement
- ☐ **D** Never available

81. Which tool analyzes website historical data?

- ☐ **A** VirusTotal
- ☒ **B** Wayback Machine
- ☐ **C** Burp Suite
- ☐ **D** John the Ripper

82. During incident response, OSINT can identify:

- ☐ **A** Encrypted VPN traffic
- ☐ **B** BIOS passwords
- ☒ **C** Data leaks on paste sites
- ☐ **D** RAM contents

83. Which of these is NOT a type of fake news?

- ☐ A Satire
- ☐ B Misleading content
- ☒ C Peer-reviewed research
- ☐ D Fabricated content

84. Reverse image search helps investigators:

- ☐ A Encrypt evidentiary photos
- ☐ B Delete manipulated images
- ☐ C Bypass copyright laws
- ☒ D Verify original sources of viral images

85. A bot account often shows:

- ☒ A High post frequency with low engagement
- ☐ B Verified badges
- ☐ C Personal photos
- ☐ D Irregular posting times

86. Investigating avatar crimes requires analyzing:

- ☒ A Transaction logs and behavioral metadata
- ☐ B GPU specifications
- ☐ C VR headset serial numbers
- ☐ D Voice modulation

87. Which data type is MOST critical for harassment cases in VR?

- ☐ A Avatar skin color
- ☐ B Friend list count
- ☐ C Hardware specs
- ☒ D Movement coordinates and chat logs

88. AI-powered "avatar fingerprinting" analyzes:

- ☐ A Login times
- ☒ B Movement patterns and interaction styles
- ☐ C Friend requests
- ☐ D VR headset model

89. What is the FIRST step in securing a digital crime scene?

- ☐ A Reboot devices to check functionality
- ☒ B Isolate and preserve the scene
- ☐ C Immediately clone all storage media
- ☐ D Interview witnesses

90. A write-blocker is essential to:

- ☐ A Increase data transfer speed
- ☒ B Prevent modifications to original evidence
- ☐ C Bypass password protection
- ☐ D Encrypt evidence automatically

91. Timelining artifacts (e.g., \$MFT) helps establish:

- ☒ A User activity chronology
- ☐ B Hardware defects
- ☐ C Network latency
- ☐ D Software license validity

92. The Stuxnet investigation relied heavily on:

- ☐ A Instagram posts
- ☐ B Keyboard smudge patterns
- ☐ C Cloud storage metadata
- ☒ D Rootkit analysis in industrial systems

93. Which principle ensures digital evidence remains unaltered?

- ☐ A Data minimization
- ☒ B Chain of custody
- ☐ C Encryption
- ☐ D Encryption

94. Statements: All cats are dogs. All dogs are birds. Conclusion: All cats are birds. Is the conclusion:

- ☒ **A** True
- ☐ **B** False
- ☐ **C** Uncertain
- ☐ **D** None of the above

95. 'Knife' is to 'Cut' as 'Pen' is to:

- ☒ **A** Write
- ☐ **B** Ink
- ☐ **C** Paper
- ☐ **D** Pencil

96. Is X greater than Y? Statements: 1) $X + Y > 10$; 2) $X > 5$.

- ☐ **A** Statement 1 alone is sufficient.
- ☒ **B** Statement 2 alone is sufficient.
- ☐ **C** Both statements together are sufficient.
- ☐ **D** Neither statement is sufficient.

97. Which feature is unique to NTFS?

- ☐ **A** Inode-based structure
- ☐ **B** No file size limits
- ☐ **C** Case-sensitive filenames
- ☒ **D** Journaling and file compression

98. Which filesystem is designed for SSDs?

- ☒ **A** F2FS (Flash-Friendly File System)
- ☐ **B** ext3
- ☐ **C** HFS+
- ☐ **D** ReiserFS

99. NTFS alternate data streams can hide:

- ☐ A Partition tables
- ☐ B BIOS settings
- ☐ C GPU drivers
- ☒ D Malware or additional file data

100. In digital forensics, which file format is commonly associated with audio recordings?

- ☒ A .mp3
- ☐ B .avi
- ☐ C .mp4
- ☐ D .mov