? EASY (Q1–Q10)

Q1. Initial assessment in digital forensics is performed to:
A. Recover deleted files
B. Determine scope and severity of incident
C. Encrypt evidence
D. Replace affected systems

Q2. Which activity is part of initial assessment?
A. Malware reverse engineering
B. Disk imaging
C. Incident type identification
D. Court testimony

Q3. An incident notification checklist ensures:
A. Faster system boot
B. Correct stakeholders are informed
C. Evidence encryption
D. Data compression

Q4. Hexadecimal number system is based on:
A. Base-2
B. Base-8
C. Base-10
D. Base-16

Q5. Which digit is valid in hexadecimal notation?
A. G
B. F
C. Z
D. H

Q6. One byte consists of:
A. 2 bits
B. 4 bits
C. 8 bits
D. 16 bits

Q7. Which unit represents 4 bits?
A. Byte
B. Word
C. Nibble
D. Sector

Q8. Hexadecimal is preferred in forensics because it:
A. Encrypts data
B. Compresses data
C. Represents binary data clearly
D. Hides evidence

Q9. File signatures are typically identified using:
A. File names
B. File extensions
C. Hex values
D. File permissions

Q10. Which security objective ensures data is accessible when required?
A. Confidentiality
B. Integrity
C. Availability
D. Authentication

□ MEDIUM (Q11–Q25)

Q11. Why is scope determination important during initial assessment?
A. To encrypt evidence
B. To decide investigation depth
C. To destroy malware
D. To reduce storage

Q12. Which stakeholder must be notified first in a major data breach?
A. Media
B. Technical response team
C. End users
D. Vendors

Q13. Which action is time-critical during incident notification?
A. Report formatting
B. Volatile data preservation
C. Archiving backups
D. Evidence disposal

Q14. Decimal number 15 is represented in hexadecimal as:
A. 0F
B. 15
C. 1F
D. FF

Q15. Why is hexadecimal more compact than binary?
A. Uses fewer symbols
B. Uses letters
C. Represents 4 bits per digit
D. Encrypts bits

Q16. Which file signature identifies a PDF file?
A. 4D 5A
B. FF D8 FF
C. 25 50 44 46
D. 50 4B 03 04

Q17. Memory dumps are usually analyzed using:
A. ASCII only
B. Hexadecimal representation
C. Decimal tables
D. Encryption tools

Q18. Which component stores data in binary at the lowest level?
A. File system
B. Application
C. Memory and disk sectors
D. User interface

Q19. Why must investigators understand bits and bytes?
A. To write code
B. To interpret raw evidence correctly
C. To design networks
D. To encrypt storage

Q20. Which decision is made during initial assessment?
A. Final verdict
B. Investigation strategy
C. Court admissibility
D. Encryption method

Q21. Incident severity is usually determined based on:
A. Disk size
B. Number of users affected
C. File extensions
D. OS version

Q22. Which data representation is closest to raw disk data?
A. ASCII
B. Hexadecimal
C. Unicode
D. Base64

Q23. Why are file headers checked during forensic analysis?
A. To compress files
B. To verify true file type
C. To encrypt content
D. To reduce size

Q24. A wrong initial assessment can result in:
A. Faster investigation
B. Loss of critical evidence
C. Better reporting
D. Reduced costs

Q25. Which artifact helps detect file tampering?
A. File name
B. File extension
C. Hex signature mismatch
D. Folder location

🔴 HARD (Q26–Q40)

Q26. Why is hexadecimal essential when analyzing disk sectors?
A. Sectors are encrypted
B. Sectors are stored in ASCII
C. Sectors are stored as binary data
D. Sectors store metadata only

Q27. Which error most often occurs due to poor initial assessment?
A. Weak hashing
B. Incomplete scope coverage
C. Tool incompatibility
D. Slow response

Q28. Why should legal teams be notified early in incidents?
A. To speed investigation
B. To ensure lawful actions
C. To compress evidence
D. To analyze malware

Q29. Decimal value 255 in hexadecimal is:
A. 0F
B. FF
C. F0
D. 1FF

Q30. Which representation is easiest for humans to read raw binary data?
A. Binary
B. Decimal
C. Hexadecimal
D. Octal

Q31. Which forensic task heavily depends on hex analysis?
A. Incident reporting
B. File signature verification
C. User interviews
D. Risk assessment

Q32. Which incident type usually demands immediate notification to regulators?
A. Malware infection
B. Policy violation
C. Personal data breach
D. System crash

Q33. Why is understanding endianess important in hex analysis?
A. Prevents encryption
B. Avoids misinterpreting byte order
C. Improves compression
D. Speeds analysis

Q34. Which scenario requires low-level data interpretation?
A. Policy drafting
B. Disk corruption analysis
C. User awareness training
D. Incident reporting

Q35. Which mistake can occur while interpreting hex data?
A. Using write blockers
B. Ignoring file offsets
C. Hash verification
D. Disk imaging

Q36. Why is hexadecimal preferred over decimal in memory analysis?
A. Decimal is encrypted
B. Hex maps directly to binary
C. Decimal is larger
D. Hex compresses memory

Q37. Which security objective is most threatened by incorrect hex interpretation?
A. Confidentiality
B. Availability
C. Integrity
D. Authentication

Q38. Why must initial assessment be documented?
A. For encryption
B. For legal accountability
C. For data recovery
D. For compression

Q39. Which forensic example best uses hex values?
A. Email content reading
B. File type identification
C. User authentication
D. Incident escalation

Q40. Failure in incident notification primarily affects:
A. Evidence size
B. Legal compliance
C. Disk performance
D. System speed