⍰ EASY (Q1–Q10)

Q1. The primary purpose of hashing in computer forensics is to:
A. Encrypt data
B. Compress files
C. Verify data integrity
D. Hide information

Q2. Which process converts data into a fixed-length value?
A. Encoding
B. Encryption
C. Hashing
D. Compression

Q3. Encoding is mainly used for:
A. Data confidentiality
B. Secure communication
C. Data representation and compatibility
D. Legal authentication

Q4. Which of the following is an example of encoding?
A. AES
B. RSA
C. Base64
D. SHA-256

Q5. A hex editor allows investigators to:
A. Encrypt files
B. View data at byte level
C. Scan networks
D. Monitor processes

Q6. Which property ensures the same input always produces the same hash?
A. Collision resistance
B. Determinism
C. Randomization
D. Encryption

Q7. MD5 produces a hash of length:
A. 64 bits
B. 128 bits
C. 256 bits
D. 512 bits

Q8. Which value is typically recorded in forensic hash logs?
A. File name only
B. Hash algorithm and hash value
C. Encryption key
D. User password

Q9. Bit rot refers to:
A. Malware infection
B. Gradual data corruption
C. File compression
D. Hash collision

Q10. Which objective does hashing primarily support in forensics?
A. Confidentiality
B. Availability
C. Integrity
D. Authentication

□ MEDIUM (Q11–Q25)

Q11. Which statement correctly differentiates encoding and encryption?
A. Encoding provides security, encryption does not
B. Encryption is reversible without keys
C. Encoding changes representation, encryption protects confidentiality
D. Both are identical processes

Q12. Why is encryption relevant in forensic investigations?
A. It prevents evidence collection
B. It hides evidence permanently
C. It protects data from unauthorized access
D. It replaces hashing

Q13. Which encoding scheme is commonly used to embed binary data in emails?
A. ASCII
B. Unicode
C. Base64
D. Hexadecimal

Q14. Which component of a file is examined first in a hex editor to identify file type?
A. Footer
B. Metadata
C. Header (signature)
D. File name

Q15. Logical files differ from physical files because logical files:
A. Exist only in memory
B. Are visible to the operating system
C. Include deleted data
D. Include slack space

Q16. Which property of a hash function makes reversing the original data infeasible?
A. Determinism
B. Fixed length
C. One-way property
D. Compression

Q17. Why is hashing performed immediately after evidence acquisition?
A. To encrypt evidence
B. To reduce file size
C. To establish baseline integrity
D. To improve performance

Q18. What is the main forensic limitation of MD5?
A. Large digest size
B. Slow computation
C. Vulnerability to collisions
D. Incompatibility with tools

Q19. Hash digest length mainly affects:
A. Encryption strength
B. Collision resistance
C. File compression
D. Data encoding

Q20. Which hashing algorithm is considered stronger for forensic purposes?
A. MD5
B. SHA-1
C. SHA-256
D. CRC32

Q21. Which artifact best helps detect file tampering?
A. File name
B. Hash mismatch
C. File extension
D. Folder structure

Q22. Bit rot is most likely detected through:
A. Antivirus scans
B. Periodic hash verification
C. Disk defragmentation
D. Encryption checks

Q23. Why are hex editors used in malware investigations?
A. To generate reports
B. To view hidden or obfuscated code
C. To capture network traffic
D. To encrypt payloads

Q24. Which forensic practice minimizes the impact of bit rot?
A. Single backup storage
B. Regular integrity checks
C. File compression
D. Encryption only

Q25. Hash logs are primarily maintained to support:
A. Data recovery
B. Chain of custody
C. Encryption management
D. File compression

● HARD (Q26–Q40)

Q26. Why is MD5 still sometimes used in forensics despite known weaknesses?
A. It is collision-free
B. It is legally mandated
C. It is fast and used alongside stronger hashes
D. It encrypts evidence

Q27. Which scenario best illustrates a hash collision risk?
A. Same file copied twice
B. Two different files producing the same hash
C. Encrypted file unreadable
D. Large file hashing slowly

Q28. Which forensic conclusion becomes questionable due to hash collision?
A. File ownership
B. Evidence integrity
C. Evidence availability
D. Evidence compression

Q29. Why are multiple hash algorithms sometimes used together?
A. To reduce hash length
B. To speed up acquisition
C. To strengthen integrity verification
D. To encrypt evidence

Q30. Which hex-level inconsistency strongly suggests file tampering?
A. Large file size
B. Matching file extension
C. Header-extension mismatch
D. Correct permissions

Q31. In forensic analysis, slack space is best examined using:
A. File explorer
B. Hex editor
C. Antivirus
D. Compression tools

Q32. Why is hashing critical during every evidence transfer?
A. To reduce storage
B. To ensure unchanged evidence state
C. To encrypt evidence
D. To increase speed

Q33. Which condition most threatens long-term digital evidence storage?
A. Encryption
B. Bit rot
C. Compression
D. Encoding

Q34. Which property differentiates cryptographic hash functions from checksums?
A. Speed
B. Collision resistance
C. File size
D. Encoding format

Q35. Why does bit rot pose legal challenges in court?
A. It encrypts evidence
B. It silently alters evidence over time
C. It compresses data
D. It improves integrity

Q36. Which forensic error most undermines integrity claims?
A. Using SHA-256
B. Missing initial hash calculation
C. Hex analysis
D. Tool validation

Q37. Which activity best ensures authenticity of digital evidence?
A. File compression
B. Repeated hashing and verification
C. Encoding
D. Encryption

Q38. Which evidence characteristic is NOT provided by hashing?
A. Integrity verification
B. Tamper detection
C. Confidentiality
D. Authenticity support

Q39. Why must hash values be included in forensic reports?
A. For file recovery
B. For legal verification of evidence integrity
C. For compression
D. For encryption key storage

Q40. Which principle is most affected if bit rot goes undetected?
A. Confidentiality
B. Availability
C. Integrity
D. Authorization