? EASY (Q1–Q10)

Q1. Digital evidence handling primarily focuses on:
A. Speed of analysis
B. Preserving evidence integrity
C. Data encryption
D. System optimization

Q2. An evidence checkout log is used to:
A. Encrypt evidence
B. Track evidence access and movement
C. Compress evidence
D. Delete unused evidence

Q3. Which role performs the first actions at an incident scene?
A. Legal advisor
B. First responder
C. Auditor
D. Database administrator

Q4. Forensic duplication ensures that:
A. Original evidence is modified
B. Analysis is faster
C. Original evidence remains untouched
D. Data is compressed

Q5. Which tool prevents writing to original storage media?
A. Antivirus
B. Write blocker
C. Firewall
D. IDS

Q6. Which technique verifies evidence integrity?
A. Encryption
B. Hashing
C. Compression
D. Encoding

Q7. Which document records every forensic action taken?
A. Incident policy
B. Investigation notes
C. Backup log
D. Access control list

Q8. Evidence collected while the system is ON is called:
A. Archived evidence
B. Dead evidence
C. Live evidence
D. Secondary evidence

Q9. Which of the following is a volatile artifact?
A. Hard disk file
B. RAM contents
C. Backup tape
D. Archived email

Q10. Improper evidence handling mainly leads to:
A. Faster trials
B. Evidence rejection
C. System recovery
D. Reduced storage

□ MEDIUM (Q11–Q25)

Q11. Why is evidence handling critical in computer forensics?
A. To reduce investigation cost
B. To maintain legal admissibility
C. To improve system security
D. To encrypt sensitive files

Q12. Which field is mandatory in an evidence checkout log?
A. File extension
B. Evidence ID
C. Operating system
D. Disk size

Q13. What is the main objective of first response?
A. Full analysis
B. System restoration
C. Evidence preservation
D. Data encryption

Q14. Which action should be avoided during first response?
A. Photographing the scene
B. Documenting system state
C. Booting the suspect system
D. Identifying connected devices

Q15. Logical duplication differs from physical duplication because it:
A. Copies entire disk
B. Includes slack space
C. Copies selected files only
D. Captures deleted files

Q16. Why is hashing performed before and after imaging?
A. For compression
B. For encryption
C. For integrity verification
D. For faster copying

Q17. Which activity belongs to the investigation phase?
A. Evidence labeling
B. Timeline reconstruction
C. Disk seizure
D. Evidence sealing

Q18. Interpretation in forensics involves:
A. Evidence acquisition
B. Correlating and analyzing evidence
C. Imaging disks
D. Hash generation

Q19. Which mistake directly affects chain of custody?
A. Large data size
B. Missing documentation
C. Slow analysis
D. Encrypted storage

Q20. Which artifact helps determine sequence of events?
A. File size
B. Hash value
C. Timeline data
D. Disk geometry

Q21. Evidence authentication ensures that evidence is:
A. Encrypted
B. Original and unchanged
C. Compressed
D. Archived

Q22. Which scenario represents evidence contamination?
A. Using write blockers
B. Analyzing forensic image
C. Booting original system
D. Hash verification

Q23. What is the primary purpose of documentation?
A. Improve performance
B. Establish transparency and accountability
C. Encrypt evidence
D. Reduce storage

Q24. Which data is collected first during live response?
A. Disk image
B. Volatile data
C. Backup files
D. Archived logs

Q25. Detection primarily helps investigators to:
A. Encrypt systems
B. Identify indicators of compromise
C. Recover deleted files
D. Destroy malware

🔴 HARD (Q26–Q40)

Q26. Why is physical duplication preferred for deep forensic analysis?
A. Smaller image size
B. Faster processing
C. Includes deleted and slack space
D. Requires no hashing

Q27. Which failure most compromises forensic credibility?
A. Using open-source tools
B. Incomplete chain of custody
C. Large evidence volume
D. Long investigation time

Q28. Which action best preserves volatile data?
A. Powering off system
B. Capturing RAM first
C. Removing hard disk
D. Encrypting storage

Q29. Why is first responder documentation critical?
A. Improves tool accuracy
B. Prevents legal challenges
C. Encrypts evidence
D. Speeds up investigation

Q30. Which artifact best reveals attacker persistence mechanisms?
A. File hashes
B. Cron jobs / startup entries
C. Disk partitions
D. BIOS settings

Q31. What is the forensic risk of analyzing original evidence directly?
A. Slower analysis
B. Evidence alteration
C. Larger storage usage
D. Tool incompatibility

Q32. Which evidence is most legally sensitive?
A. Public files
B. Volatile memory
C. Personal user data
D. Temporary files

Q33. Why is correlation across multiple artifacts important?
A. Reduces evidence size
B. Improves investigation speed
C. Validates findings
D. Encrypts data

Q34. Which factor most influences evidence admissibility?
A. Investigator seniority
B. Proper handling procedures
C. Tool brand
D. Data format

Q35. Why must evidence transfer be documented each time?
A. For encryption
B. For integrity and accountability
C. For compression
D. For faster analysis

Q36. Which forensic phase converts raw data into conclusions?
A. Collection
B. Preservation
C. Analysis
D. Identification

Q37. Which error commonly occurs in poorly managed investigations?
A. Over-documentation
B. Evidence contamination
C. Excessive hashing
D. Redundant imaging

Q38. Which detection artifact indicates malware communication?
A. Disk geometry
B. Network traffic logs
C. File permissions
D. BIOS version

Q39. Why is legal authorization essential before evidence collection?
A. To speed up response
B. To avoid evidence duplication
C. To ensure lawful access
D. To reduce data size

Q40. Which principle ensures another examiner can reproduce results?
A. Confidentiality
B. Availability
C. Repeatability
D. Compression