⍰ EASY (Q1–Q10)

Q1. Which of the following best defines computer forensics?
A. Network monitoring
B. Digital evidence analysis for legal purposes
C. Malware prevention
D. Data encryption

Q2. Which security objective ensures systems and evidence are accessible when needed?
A. Confidentiality
B. Integrity
C. Availability
D. Authentication

Q3. Which data is considered volatile?
A. Disk image
B. Archived email
C. RAM contents
D. Backup tape

Q4. Which document tracks evidence movement and access?
A. Incident report
B. SOP manual
C. Chain of custody
D. Audit policy

Q5. Which number system is base-16?
A. Binary
B. Decimal
C. Octal
D. Hexadecimal

Q6. FTK Imager is mainly used for:
A. Malware coding
B. Evidence acquisition
C. Network scanning
D. Log correlation

Q7. Which Linux directory stores system logs?
A. /etc
B. /home
C. /var/log
D. /proc

Q8. Hashing in forensics is used to ensure:
A. Confidentiality
B. Compression
C. Integrity
D. Availability

Q9. Mobile forensics primarily deals with evidence from:
A. Servers
B. Routers
C. Mobile devices
D. Firewalls

Q10. Which forensic phase comes first?
A. Analysis
B. Collection
C. Identification
D. Reporting

□ MEDIUM (Q11–Q25)

Q11. Which situation most clearly requires live forensics?
A. Powered-off laptop
B. Archived backup
C. Active ransomware attack
D. Decommissioned server

Q12. Which artifact best helps reconstruct a timeline?
A. Hash value
B. System and application logs
C. Disk size
D. File extension

Q13. Which action most risks evidence contamination?
A. Using write blockers
B. Imaging original disk
C. Booting suspect system
D. Hash verification

Q14. Which Sysinternals tool identifies startup persistence?
A. TCPView
B. Autoruns
C. PsPing
D. Handle

Q15. Which Linux artifact records user command history?
A. /etc/passwd
B. /var/log/messages
C. .bash_history
D. /proc

Q16. Why are SOPs critical in digital forensics?
A. Faster investigation
B. Evidence compression
C. Legal defensibility
D. Automation

Q17. Which encoding method is commonly used in email attachments?
A. AES
B. SHA-1
C. Base64
D. RSA

Q18. Which file signature identifies a PDF file?
A. 4D 5A
B. FF D8 FF
C. 25 50 44 46
D. 50 4B 03 04

Q19. Which forensic tool category captures disk images?
A. Analysis tools
B. Reporting tools
C. Acquisition tools
D. Visualization tools

Q20. Which factor most affects legal admissibility of evidence?
A. Tool brand
B. Evidence size
C. Handling procedure
D. Investigator speed

Q21. Which Linux mechanism is often abused for persistence?
A. Swap space
B. Cron jobs
C. File permissions
D. Disk partitions

Q22. Why is MD5 considered weak for forensics?
A. Too slow
B. Large digest
C. Collision vulnerability
D. Not deterministic

Q23. Which mobile data best indicates user movement?
A. SMS
B. Call duration
C. Location data
D. Media files

Q24. Which phase limits damage during an incident?
A. Preparation
B. Detection
C. Containment
D. Lessons learned

Q25. Hex editors are primarily used to:
A. Encrypt files
B. View raw binary data
C. Monitor traffic
D. Generate reports

HARD (Q26–Q40)

Q26. Why is physical (bit-by-bit) imaging preferred over logical imaging?
A. Faster copying
B. Smaller image
C. Includes deleted and slack space
D. No hashing required

Q27. Which failure most commonly leads to evidence rejection in court?
A. Large dataset
B. Open-source tools
C. Broken chain of custody
D. Slow analysis

Q28. Why is hashing difficult during live forensics?
A. Algorithms are slow
B. Data changes continuously
C. Tools are unavailable
D. Hashing is illegal

Q29. Which forensic implication arises from privacy violations?
A. Faster trials
B. Legal penalties and case dismissal
C. Improved evidence
D. Better documentation

Q30. Which NTFS structure is crucial for timeline reconstruction?
A. Disk partition table
B. Master File Table (MFT)
C. BIOS firmware
D. Device drivers

Q31. Why are multiple hash algorithms sometimes used together?
A. Reduce file size
B. Encrypt evidence
C. Strengthen integrity verification
D. Speed up acquisition

Q32. Which scenario best demonstrates forensic readiness?
A. Post-incident scrambling
B. No logging enabled
C. Predefined procedures and logging
D. Ad-hoc investigation

Q33. Which Linux log best shows authentication attempts?
A. /var/log/syslog
B. /var/log/auth.log
C. /etc/shadow
D. /home/user

Q34. Which mobile forensic challenge impacts cross-border cases?
A. Battery life
B. Cloud data jurisdiction
C. App size
D. Screen lock

Q35. Why must investigators avoid analyzing original evidence directly?
A. Slower processing
B. Risk of altering evidence
C. Larger storage
D. Tool incompatibility

Q36. Which principle ensures another examiner can reproduce findings?
A. Confidentiality
B. Integrity
C. Repeatability
D. Availability

Q37. Which hex-level indicator suggests file masquerading?
A. Correct extension
B. Matching header
C. Header-extension mismatch
D. Valid hash

Q38. Which ethical issue arises from management pressure?
A. Encryption failure
B. Biased reporting
C. Disk corruption
D. Tool crashes

Q39. Why is documentation required at every forensic step?
A. Improve speed
B. Reduce evidence size
C. Ensure legal accountability
D. Encrypt evidence

Q40. Which outcome best reflects a successful forensic investigation?
A. Fast recovery
B. Automated conclusions
C. Legally defensible evidence and reporting
D. Minimal documentation