⍰ EASY (Q1–Q10)

Q1. Live system forensics deals with systems that are:
A. Disconnected from network
B. Powered off
C. Actively running
D. Decommissioned

Q2. Which type of data is lost when a system is shut down?
A. Disk data
B. Backup data
C. Volatile data
D. Archived logs

Q3. RAM data is considered:
A. Non-volatile
B. Volatile
C. Archived
D. Static

Q4. Which operating system is commonly used in servers and cloud platforms?
A. DOS
B. Linux
C. macOS only
D. BIOS

Q5. Which directory in Linux stores system logs?
A. /bin
B. /home
C. /var/log
D. /etc

Q6. Mobile forensics focuses on evidence from:
A. Desktop computers only
B. Network devices
C. Mobile devices
D. Servers

Q7. Call logs and SMS are examples of:
A. Network evidence
B. Mobile evidence
C. Cloud evidence
D. Disk evidence

Q8. Which security objective ensures evidence is not modified?
A. Confidentiality
B. Integrity
C. Availability
D. Authentication

Q9. Live forensics is commonly used during:
A. System installation
B. Incident response
C. Software development
D. Hardware upgrade

Q10. Which mobile OS is known for strong encryption by default?
A. DOS
B. Android
C. iOS
D. Linux

□ MEDIUM (Q11–Q25)

Q11. Why is live forensics required in some investigations?
A. To reduce storage usage
B. To capture volatile artifacts
C. To compress evidence
D. To encrypt data

Q12. Which of the following is a live system artifact?
A. Deleted files
B. Disk partitions
C. Running processes
D. Backup archives

Q13. Which artifact helps identify active attacker communication?
A. File metadata
B. Network connections
C. File extensions
D. Disk geometry

Q14. Which Linux file contains user command history?
A. /etc/passwd
B. /var/log/syslog
C. .bash_history
D. /proc/meminfo

Q15. Cron jobs in Linux are mainly analyzed to detect:
A. File corruption
B. Persistence mechanisms
C. Disk failures
D. Network latency

Q16. Which Linux directory stores user personal data?
A. /etc
B. /var
C. /home
D. /boot

Q17. Timeline reconstruction in Linux forensics relies heavily on:
A. File extensions
B. Log files and timestamps
C. Disk size
D. Encryption keys

Q18. Which type of mobile data indicates user movement?
A. SMS
B. App cache
C. Location data
D. Call duration

Q19. A major challenge in mobile forensics is:
A. Lack of data
B. Strong encryption and privacy controls
C. Small storage size
D. Absence of logs

Q20. Live forensics carries higher legal risk because:
A. Evidence is compressed
B. Investigator actions may alter evidence
C. Storage is limited
D. Logs are missing

Q21. Which artifact best identifies logged-in users on a live system?
A. File hashes
B. Active sessions
C. Disk sectors
D. Backup logs

Q22. Linux forensics differs from Windows forensics mainly because Linux:
A. Uses registry
B. Uses text-based configuration and logs
C. Has no logs
D. Uses GUI only

Q23. Mobile devices are rich forensic sources because they:
A. Have large hard disks
B. Contain personal and sensor data
C. Store no logs
D. Are always offline

Q24. Which forensic practice is critical in live analysis?
A. Shutting down system
B. Minimal interaction principle
C. Deleting malware
D. Installing updates

Q25. Which data source is most volatile in mobile devices?
A. Photos
B. App databases
C. RAM data
D. SIM card

🔴 HARD (Q26–Q40)

Q26. Why is live memory acquisition prioritized before disk imaging?
A. Disk data changes faster
B. Memory contains volatile and critical evidence
C. Disk imaging is illegal
D. Memory is encrypted

Q27. Which mistake most compromises live forensic investigations?
A. Using validated tools
B. Powering off the system prematurely
C. Capturing network data
D. Documentation

Q28. Which Linux artifact best reveals unauthorized access attempts?
A. /bin
B. /var/log/auth.log
C. /home
D. /boot

Q29. Why is Linux log tampering a forensic challenge?
A. Logs are encrypted
B. Logs can be deleted or modified easily
C. Logs are stored remotely
D. Logs are binary

Q30. Which scenario most justifies live forensics?
A. Archived server
B. Powered-off workstation
C. Active ransomware infection
D. Decommissioned laptop

Q31. Which mobile forensic challenge affects cross-border investigations?
A. Disk size
B. Cloud data jurisdiction
C. Battery life
D. File extensions

Q32. Which evidence type is most sensitive to privacy concerns?
A. System logs
B. Mobile personal data
C. Network topology
D. Disk geometry

Q33. Why is hashing difficult during live forensics?
A. Hash algorithms are slow
B. Data changes continuously
C. Tools are unavailable
D. Storage is encrypted

Q34. Which Linux artifact indicates scheduled malicious execution?
A. File permissions
B. Cron jobs
C. Disk partitions
D. Swap space

Q35. Which principle is hardest to maintain in live forensics?
A. Availability
B. Confidentiality
C. Integrity
D. Authentication

Q36. Why is mobile forensics often combined with cloud forensics?
A. Mobile devices lack storage
B. Apps sync data to cloud services
C. Cloud data is unencrypted
D. Mobile devices cannot be imaged

Q37. Which live artifact best supports detection of data exfiltration?
A. File headers
B. Outbound network traffic
C. File permissions
D. Disk partitions

Q38. Which forensic limitation arises due to full-disk encryption?
A. Faster acquisition
B. Restricted access to data without keys
C. Larger storage
D. More logs

Q39. Which comparison correctly distinguishes live and dead forensics?
A. Live is safer than dead
B. Dead captures volatile data
C. Live captures volatile data
D. Dead is legally riskier

Q40. Which outcome best reflects effective live, Linux, and mobile forensics?
A. Faster system recovery
B. Comprehensive and legally defensible evidence
C. Minimal documentation
D. Tool-dependent conclusions