? EASY (Q1–Q10)

Q1. Computer forensics tools are primarily used to:
A. Prevent cyber attacks
B. Analyze and preserve digital evidence
C. Design secure networks
D. Develop software

Q2. Which category of forensic tools is used for evidence acquisition?
A. Reporting tools
B. Visualization tools
C. Imaging tools
D. Simulation tools

Q3. Sysinternals Suite is mainly used for:
A. Disk encryption
B. Live system analysis
C. Network routing
D. Database management

Q4. FTK stands for:
A. File Transfer Kit
B. Forensic Toolkit
C. Fast Tracking Kernel
D. File Tracing Key

Q5. FTK Imager is primarily used for:
A. Malware coding
B. Evidence acquisition and preview
C. Network scanning
D. Data compression

Q6. Open-source forensic tools are typically:
A. Proprietary and closed
B. Free and community-developed
C. Illegal to use
D. Hardware-based only

Q7. Hex editors display data mainly in:
A. Decimal only
B. ASCII only
C. Hexadecimal and ASCII
D. Binary only

Q8. Which feature ensures evidence has not been altered?
A. Encryption
B. Hash verification
C. Compression
D. Encoding

Q9. Sysinternals tools are most effective during:
A. Post-trial reporting
B. Live incident response
C. Evidence destruction
D. Backup restoration

Q10. Forensic tools must be used in accordance with:
A. User convenience
B. SOPs and legal requirements
C. Network topology
D. Storage capacity

□ MEDIUM (Q11–Q25)

Q11. Which factor is most important when selecting a forensic tool?
A. Graphical interface
B. Legal acceptance and validation
C. File size support
D. Tool popularity

Q12. Commercial forensic tools are preferred in courts because they:
A. Are free
B. Have vendor support and validation
C. Are open source
D. Require less documentation

Q13. Which Sysinternals utility helps identify startup persistence?
A. TCPView
B. Autoruns
C. Process Explorer
D. PsPing

Q14. Process Explorer is useful to detect:
A. Disk errors
B. Running malicious processes
C. Network routing issues
D. File system corruption

Q15. FTK processes evidence primarily by:
A. Compressing files
B. Indexing and parsing data
C. Encrypting evidence
D. Deleting duplicates

Q16. Which evidence type is supported by FTK?
A. Only text files
B. Disk images and memory dumps
C. Audio files only
D. Network packets only

Q17. FTK Imager differs from FTK because FTK Imager:
A. Performs deep analysis
B. Is mainly for acquisition
C. Is used only for reporting
D. Is network-based

Q18. Why is hash generation important during imaging with FTK Imager?
A. To reduce image size
B. To encrypt evidence
C. To verify integrity
D. To improve speed

Q19. One advantage of open-source forensic tools is:
A. Guaranteed court acceptance
B. High cost
C. Transparency of algorithms
D. Vendor-exclusive support

Q20. Hex tools are especially useful for:
A. Network monitoring
B. Viewing raw disk data
C. User training
D. Policy enforcement

Q21. Which forensic artifact is best identified using hex analysis?
A. Network sessions
B. File signatures
C. User permissions
D. Process lists

Q22. Which stage of investigation primarily uses FTK Imager?
A. Incident detection
B. Evidence acquisition
C. Court testimony
D. Policy drafting

Q23. Open-source tools are often used in investigations when:
A. Budget is limited
B. Legal compliance is not required
C. Evidence is encrypted
D. Commercial tools are banned

Q24. Why must forensic tools be validated before use?
A. To increase speed
B. To ensure reliable and repeatable results
C. To reduce data volume
D. To simplify reporting

Q25. Which output from forensic tools is most important legally?
A. Graphs
B. Logs and hash values
C. Screenshots only
D. GUI layouts

🔴 HARD (Q26–Q40)

Q26. Why is over-reliance on forensic tools risky?
A. Tools are too fast
B. Tools may produce false positives
C. Tools encrypt evidence
D. Tools reduce documentation

Q27. Which mistake can invalidate evidence despite correct tool usage?
A. Using commercial tools
B. Poor documentation
C. Large data size
D. Slow processing

Q28. Sysinternals tools are generally unsuitable for which task?
A. Live process analysis
B. Network connection review
C. Forensic disk imaging
D. Startup analysis

Q29. Why must forensic analysts understand tool internals?
A. To modify tools
B. To correctly interpret results
C. To write malware
D. To bypass SOPs

Q30. Which scenario best justifies the use of FTK over FTK Imager?
A. Previewing a USB drive
B. Creating a disk image
C. Performing large-scale evidence analysis
D. Capturing RAM

Q31. Which hex-level indicator suggests file masquerading?
A. Correct permissions
B. Header–extension mismatch
C. Large file size
D. Valid hash

Q32. Why is chain of custody relevant when using forensic tools?
A. To improve tool speed
B. To track evidence handling
C. To encrypt reports
D. To reduce storage

Q33. Which legal issue arises from using unvalidated tools?
A. Faster trials
B. Evidence admissibility challenges
C. Reduced privacy
D. Tool crashes

Q34. Why are multiple forensic tools often used in one investigation?
A. To increase complexity
B. To cross-validate findings
C. To reduce cost
D. To encrypt data

Q35. Which forensic output best supports expert testimony?
A. Raw tool output only
B. Correlated findings with documentation
C. Screenshots without context
D. Tool logs without explanation

Q36. Which limitation is common in open-source forensic tools?
A. No transparency
B. Limited official support
C. Illegal usage
D. Inability to analyze files

Q37. Why is hex analysis important in detecting steganography?
A. It encrypts data
B. It reveals hidden patterns in raw data
C. It compresses files
D. It validates passwords

Q38. Which forensic principle ensures another examiner can repeat tool results?
A. Confidentiality
B. Repeatability
C. Availability
D. Scalability

Q39. Which practice best ensures ethical use of forensic tools?
A. Using fastest tools
B. Following SOPs and legal authorization
C. Avoiding documentation
D. Tool automation

Q40. Which outcome best reflects proper forensic tool integration?
A. Automated conclusions
B. Accurate, validated, and legally defensible findings
C. Minimal human involvement
D. Tool-dependent judgments