⍰ EASY (Q1–Q10)

Q1. SOP in computer forensics stands for:
A. System Operational Policy
B. Standard Operating Procedures
C. Security Operations Plan
D. Software Optimization Process

Q2. The primary purpose of SOPs is to ensure:
A. Faster investigations
B. Consistency and legal defensibility
C. Reduced storage usage
D. Automatic evidence analysis

Q3. Crime scene processing in digital forensics begins with:
A. Evidence analysis
B. Securing the scene
C. Reporting
D. Disk imaging

Q4. Which system is most commonly encountered in digital crime scenes?
A. DOS
B. UNIX only
C. Windows
D. Mainframe

Q5. Which activity is mandatory before collecting digital evidence?
A. File deletion
B. Scene documentation
C. Data encryption
D. System optimization

Q6. Which command-line environment is associated with DOS systems?
A. GUI shell
B. PowerShell
C. Text-based CLI
D. Web interface

Q7. SOP violations mainly result in:
A. Faster reporting
B. Evidence inadmissibility
C. Improved analysis
D. Reduced cost

Q8. Which artifact is commonly found on Windows systems?
A. /var/log
B. Registry
C. Cron jobs
D. Bash history

Q9. DOS systems are primarily relevant today due to:
A. Gaming
B. Legacy and embedded systems
C. Cloud computing
D. Mobile platforms

Q10. Which principle ensures evidence is not altered?
A. Confidentiality
B. Integrity
C. Availability
D. Scalability

□ MEDIUM (Q11–Q25)

Q11. Why are SOPs critical during crime scene processing?
A. They improve system speed
B. They reduce evidence size
C. They maintain procedural integrity
D. They automate analysis

Q12. Which action should be avoided at a digital crime scene?
A. Photographing the setup
B. Documenting system state
C. Booting suspect systems
D. Identifying connected devices

Q13. On-site investigation is preferred when:
A. Evidence is archived
B. Volatile data must be captured
C. Systems are decommissioned
D. Reports are prepared

Q14. Live analysis on Windows systems allows collection of:
A. Deleted files only
B. Volatile artifacts
C. Backup archives
D. Offline logs

Q15. NTFS is important in forensics because it stores:
A. Only user files
B. File metadata and timestamps
C. Encrypted backups
D. Network traffic

Q16. Which Windows component records system and security events?
A. BIOS
B. Event Logs
C. Task Manager
D. Control Panel

Q17. DOS systems pose forensic challenges mainly due to:
A. Excessive logging
B. Minimal logging and legacy formats
C. Large storage capacity
D. Strong encryption

Q18. Which forensic approach minimizes evidence contamination?
A. Working on original media
B. Using SOP-guided procedures
C. Skipping documentation
D. Live editing of files

Q19. Which activity supports chain of custody at crime scenes?
A. Tool automation
B. Proper evidence labeling
C. Faster acquisition
D. Compression

Q20. Why is documentation emphasized in SOPs?
A. To improve performance
B. To support legal accountability
C. To encrypt data
D. To reduce investigation scope

Q21. Which Windows artifact reveals USB device usage?
A. Event Viewer only
B. Registry entries
C. Task Scheduler
D. BIOS settings

Q22. DOS command-line tools are useful because they:
A. Encrypt files
B. Provide low-level access
C. Increase system load
D. Hide artifacts

Q23. Which factor determines on-site vs off-site analysis?
A. Evidence size
B. Volatility and scene constraints
C. Tool brand
D. Investigator experience

Q24. Ethical handling of crime scenes requires investigators to:
A. Modify evidence if needed
B. Remain neutral and unbiased
C. Speed up conclusions
D. Ignore privacy concerns

Q25. Which SOP failure most affects evidence admissibility?
A. Slow reporting
B. Improper evidence handling
C. Large dataset
D. Use of CLI tools

● HARD (Q26–Q40)

Q26. Why are SOPs scrutinized heavily during court proceedings?
A. They improve investigation speed
B. They demonstrate repeatability and reliability
C. They reduce evidence volume
D. They replace expert testimony

Q27. Which mistake during crime scene processing most often invalidates evidence?
A. Using open-source tools
B. Powering on suspect systems
C. Excessive documentation
D. Using CLI commands

Q28. Why is live Windows analysis legally sensitive?
A. Evidence is encrypted
B. Actions may alter evidence state
C. Storage is limited
D. Logs are unavailable

Q29. Which NTFS feature assists in timeline reconstruction?
A. Disk partitions
B. Master File Table (MFT)
C. BIOS firmware
D. Device drivers

Q30. Why must DOS forensic tools be used cautiously?
A. They are slow
B. They lack vendor support
C. They can overwrite data easily
D. They are encrypted

Q31. Which crime scene principle applies equally to physical and digital scenes?
A. Compression
B. Scene preservation
C. Automation
D. Encryption

Q32. Which scenario best illustrates SOP advantage?
A. Faster malware detection
B. Consistent handling across investigators
C. Smaller reports
D. Reduced evidence storage

Q33. Why is registry analysis critical in Windows forensics?
A. Stores encrypted backups
B. Records configuration and user activity
C. Contains malware source code
D. Manages network routing

Q34. Which SOP component defines authorized tools and methods?
A. Incident report
B. Tool usage guidelines
C. Evidence label
D. Chain of custody form

Q35. Which error is common when SOPs are ignored?
A. Redundant hashing
B. Evidence contamination
C. Over-documentation
D. Improved accuracy

Q36. Why are legacy DOS systems still relevant in investigations?
A. Used for gaming
B. Found in industrial and ATM systems
C. Preferred by users
D. Support cloud services

Q37. Which security objective is most protected by SOPs?
A. Availability
B. Confidentiality
C. Integrity
D. Performance

Q38. Which activity best ensures accountability at crime scenes?
A. Encryption
B. Evidence documentation
C. Fast analysis
D. Compression

Q39. Why must investigators follow legal authorization strictly?
A. To improve tool accuracy
B. To avoid evidence duplication
C. To ensure lawful collection
D. To reduce investigation time

Q40. Which outcome best reflects SOP-based investigations?
A. Faster but informal results
B. Legally defensible and repeatable findings
C. Minimal documentation
D. Automated conclusions