? EASY (Q1–Q10)

Q1. Incident response primarily aims to:
A. Upgrade systems
B. Detect, respond to, and recover from incidents
C. Encrypt all data
D. Replace hardware

Q2. Which phase ensures readiness before an incident occurs?
A. Detection
B. Recovery
C. Preparation
D. Analysis

Q3. Preservation in forensics focuses on:
A. Speed of investigation
B. Preventing evidence alteration
C. Evidence deletion
D. System optimization

Q4. Which data type is lost when a system is powered off?
A. Log files
B. Registry
C. RAM data
D. Disk files

Q5. Which document records evidence access and handling?
A. Incident report
B. Chain of custody
C. Risk register
D. Audit log

Q6. Which role coordinates incident handling activities?
A. Network engineer
B. Incident manager
C. Software tester
D. Database admin

Q7. Identification phase deals with:
A. Evidence analysis
B. Locating potential evidence
C. Report writing
D. Evidence destruction

Q8. Which is an example of volatile data?
A. Emails
B. Hard disk files
C. Running processes
D. Backup archives

Q9. Which tool category captures evidence?
A. Analysis tools
B. Acquisition tools
C. Reporting tools
D. Visualization tools

Q10. The purpose of documentation is to:
A. Increase storage
B. Ensure transparency and repeatability
C. Encrypt findings
D. Speed up response

□ MEDIUM (Q11–Q25)

Q11. Why is preparation critical in incident response?
A. Reduces investigation cost
B. Enables faster and lawful response
C. Eliminates attacks
D. Prevents all incidents

Q12. Which step immediately follows identification in forensics?
A. Analysis
B. Preservation
C. Reporting
D. Recovery

Q13. Which of the following is a live system artifact?
A. Deleted files
B. Disk partitions
C. Network connections
D. Archived logs

Q14. Which incident response phase focuses on limiting damage?
A. Preparation
B. Detection
C. Containment
D. Lessons learned

Q15. Which document defines how incidents should be handled?
A. SLA
B. Incident Response Plan
C. Privacy policy
D. Network diagram

Q16. What is the primary risk of live forensics?
A. Evidence encryption
B. Evidence alteration
C. Evidence compression
D. Evidence duplication

Q17. Which team member ensures legal compliance during response?
A. Forensic analyst
B. Legal advisor
C. SOC analyst
D. Network admin

Q18. Why are write blockers used during acquisition?
A. Speed up imaging
B. Encrypt evidence
C. Prevent writing to original media
D. Compress data

Q19. Which artifact helps identify attacker IP addresses?
A. File metadata
B. Network logs
C. Registry entries
D. BIOS settings

Q20. Which phase involves extracting relevant data from evidence?
A. Collection
B. Examination
C. Identification
D. Preservation

Q21. Which activity belongs to the detection phase?
A. Imaging disk
B. Monitoring alerts
C. Writing report
D. Evidence archiving

Q22. Which document tracks evidence transfer between investigators?
A. Incident log
B. Change request
C. Chain of custody
D. Forensic report

Q23. What is the goal of containment?
A. Restore systems
B. Identify attacker
C. Stop incident spread
D. Destroy evidence

Q24. Which tool is most suitable for volatile data capture?
A. Disk imager
B. Memory acquisition tool
C. Backup software
D. Archiver

Q25. Incident response and forensics work together because:
A. Both encrypt data
B. IR limits damage, forensics preserves evidence
C. Both prevent attacks
D. IR replaces forensics

🟥 HARD (Q26–Q40)

Q26. Why must evidence be hashed immediately after acquisition?
A. To encrypt data
B. To reduce size
C. To verify integrity
D. To speed analysis

Q27. Which failure most often invalidates forensic findings?
A. Large evidence size
B. Slow response
C. Broken chain of custody
D. Weak passwords

Q28. Which scenario requires live system analysis?
A. Powered-off desktop
B. Archived server backup
C. Encrypted running server
D. Decommissioned laptop

Q29. What is the relationship between incident response and forensics?
A. Independent processes
B. Mutually exclusive
C. Complementary processes
D. Identical processes

Q30. Which response action risks destroying volatile evidence?
A. Capturing RAM
B. Disconnecting network
C. Shutting down system
D. Hash verification

Q31. Why must documentation be continuous throughout investigation?
A. For faster reporting
B. For audit and legal defensibility
C. For data compression
D. For encryption

Q32. Which artifact best supports timeline reconstruction?
A. Hash values
B. System and application logs
C. Disk geometry
D. BIOS version

Q33. Which phase focuses on restoring normal operations?
A. Detection
B. Containment
C. Recovery
D. Analysis

Q34. What is the main legal risk in incident response?
A. Slow investigation
B. Evidence tampering
C. Hardware failure
D. Tool incompatibility

Q35. Which principle ensures evidence can be verified by another examiner?
A. Confidentiality
B. Integrity
C. Repeatability
D. Availability

Q36. Which factor determines escalation to law enforcement?
A. Incident cost
B. Incident severity and legality
C. Network topology
D. Data size

Q37. Why is least-privilege important during response?
A. Faster access
B. Minimize evidence exposure
C. Encrypt evidence
D. Increase permissions

Q38. Which indicator best suggests data exfiltration?
A. High CPU usage
B. Large outbound traffic
C. Disk fragmentation
D. User login failure

Q39. What is the main objective of forensic readiness?
A. Prevent attacks
B. Enable efficient evidence collection
C. Encrypt systems
D. Replace security tools

Q40. Which mistake most affects legal admissibility?
A. Using open-source tools
B. Poor evidence handling
C. Large datasets
D. Slow hashing