? EASY (Q1–Q10)

Q1. Computer forensics is primarily concerned with:
A. Preventing cyber attacks
B. Designing secure networks
C. Collecting and analyzing digital evidence
D. Writing encryption algorithms

Q2. Which of the following best defines digital evidence?
A. Printed system logs
B. Any data stored or transmitted in digital form
C. Only encrypted data
D. Physical computer hardware

Q3. Which phase comes first in the forensic investigation process?
A. Analysis
B. Collection
C. Identification
D. Presentation

Q4. The main purpose of computer forensics is to ensure:
A. Faster computing
B. Legal admissibility of evidence
C. System performance
D. Network optimization

Q5. Which of the following is an example of digital evidence?
A. Paper contract
B. CCTV footage stored digitally
C. Handwritten notes
D. Fingerprints

Q6. Unauthorized access without criminal intent is classified as:
A. Computer crime
B. Cyber terrorism
C. Unauthorized activity
D. Digital fraud

Q7. The IT Act, 2000 primarily addresses:
A. Hardware manufacturing
B. Digital crimes and electronic transactions
C. Network routing
D. Software licensing only

Q8. Chain of custody refers to:
A. Encryption of evidence
B. Storage of backup data
C. Documentation of evidence handling
D. Evidence destruction

Q9. Which security principle ensures data is not altered?
A. Confidentiality
B. Availability
C. Integrity
D. Authentication

Q10. Which role is responsible for presenting forensic findings in court?
A. System administrator
B. Forensic investigator
C. Network engineer
D. Database analyst

□ MEDIUM (Q11–Q25)

Q11. Which characteristic makes digital evidence fragile?
A. Large size
B. Easy replication
C. Easy modification without trace
D. Compression

Q12. Which phase ensures evidence remains unaltered?
A. Identification
B. Preservation
C. Examination
D. Reporting

Q13. In which case is computer forensics used in civil matters?
A. Terrorism investigation
B. Insider data theft
C. Network scanning
D. Malware testing

Q14. Which of the following is a responsibility of a forensic investigator?
A. Writing malware
B. Maintaining system uptime
C. Evidence handling and documentation
D. Network configuration

Q15. Which law provides legal recognition to digital evidence in India?
A. IPC
B. CrPC
C. IT Act, 2000
D. Copyright Act

Q16. What happens if the chain of custody is broken?
A. Evidence becomes encrypted
B. Evidence is duplicated
C. Evidence may be rejected in court
D. Investigation becomes faster

Q17. Which type of case often involves computer forensics in corporations?
A. Internet routing failure
B. Employee misconduct
C. Hardware fault
D. OS upgrade

Q18. Which of the following best describes cyber law?
A. Laws for physical crimes
B. Laws governing cyberspace activities
C. Software development rules
D. Internet usage policies only

Q19. What is the role of hashing in forensics?
A. Encrypt evidence
B. Compress evidence
C. Verify integrity of evidence
D. Delete evidence

Q20. Which phase involves extracting meaningful information from evidence?
A. Preservation
B. Analysis
C. Identification
D. Collection

Q21. Which scenario represents a computer crime?
A. Accidentally accessing a folder
B. Unauthorized file deletion with intent
C. Forgetting to log out
D. Misconfigured permissions

Q22. Which digital crime involves deceiving users via messages?
A. Spoofing
B. Phishing
C. Sniffing
D. Scanning

Q23. Which forensic principle ensures repeatability of investigation?
A. Confidentiality
B. Documentation
C. Availability
D. Encryption

Q24. Which factor most affects legal admissibility of evidence?
A. Tool brand
B. Investigator experience
C. Evidence handling process
D. Data size

Q25. Which professional must remain neutral and unbiased?
A. Ethical hacker
B. Incident responder
C. Forensic investigator
D. Security auditor

HARD (Q26–Q40)

Q26. Why is bit-by-bit imaging preferred in forensic acquisition?
A. Faster copying
B. Smaller image size
C. Preservation of deleted and slack space
D. Easier compression

Q27. Which forensic phase reconstructs the sequence of events?
A. Examination
B. Collection
C. Analysis
D. Identification

Q28. Which factor differentiates computer crime from unauthorized activity most clearly?
A. Access method
B. Data size
C. Criminal intent
D. System type

Q29. Why is live system analysis risky?
A. Data is encrypted
B. Evidence may change during access
C. Storage is limited
D. Logs are unavailable

Q30. Which condition invalidates digital evidence most severely?
A. Large file size
B. Weak encryption
C. Improper documentation
D. Slow analysis

Q31. Which international framework supports cross-border cyber investigations?
A. Geneva Convention
B. Budapest Convention
C. Paris Agreement
D. WTO Agreement

Q32. Why are write blockers used during evidence acquisition?
A. Speed up copying
B. Encrypt evidence
C. Prevent modification of original media
D. Compress data

Q33. Which forensic objective aligns with ensuring evidence is accessible when needed?
A. Confidentiality
B. Integrity
C. Availability
D. Authentication

Q34. Which scenario best demonstrates forensic relevance in civil litigation?
A. Malware outbreak
B. Intellectual property theft
C. Port scanning
D. Packet loss

Q35. Why is documentation critical throughout forensic investigation?
A. Improves performance
B. Reduces storage usage
C. Establishes procedural transparency
D. Encrypts evidence

Q36. Which evidence type is most volatile?
A. Hard disk data
B. RAM contents
C. Archived emails
D. Cloud backups

Q37. Which mistake most commonly leads to evidence rejection?
A. Using open-source tools
B. Incomplete chain of custody
C. Large dataset
D. Slow reporting

Q38. Which forensic role often testifies as an expert witness?
A. System administrator
B. SOC analyst
C. Digital forensic investigator
D. Software developer

Q39. Why is integrity more critical than confidentiality in court?
A. Courts ignore privacy
B. Integrity proves evidence authenticity
C. Confidentiality delays trials
D. Integrity encrypts data

Q40. Which principle ensures digital evidence remains legally defensible?
A. Automation
B. Repeatability
C. Speed
D. Compression