GIAC Certified Forensic Analyst Practice Test Questions and Answers

1. What is the most critical requirement when collecting digital evidence?

A) Speed of collection
B) Maintaining chain of custody and evidence integrity
C) Using the newest software tools
D) Minimal documentation

2. Which file system maintains the most detailed logging for forensic analysis?

A) FAT32
B) NTFS with journaling enabled
C) exFAT
D) FAT16

3. What should be the first step in a digital forensics investigation?

A) Immediately power on all devices
B) Create forensically sound images of storage media
C) Install analysis software on target systems
D) Delete temporary files for clarity

4. Which technique is most effective for recovering deleted files?

A) File signature analysis and unallocated space examination
B) Registry analysis only
C) Network traffic analysis
D) Memory dump analysis exclusively

Answers: 1-B 2-B 3-B 4-A