SECTION A

1. Police in the United States must use procedures that adhere to which of the following?
a. Third Amendment
b. Fourth Amendment
c. First Amendment
d. None of the above

2. The triad of computing security includes which of the following?
a. Detection, response, and monitoring
b. Vulnerability assessment, detection, and monitoring
c. Vulnerability assessment, intrusion response, and investigation
d. Vulnerability assessment, intrusion response, and monitoring

3. A corporate investigator must follow Fourth Amendment standards when conducting an investigation.

a. True b. False

4. Policies can address rules for which of the following?
a. When you can log on to a company network from home
b. The Internet sites you can or cannot access
c. The amount of personal e-mail you can send
d. Any of the above

5. Laws and procedures for PDAs are which of the following?
a. Well established
b. Still being debated
c. On the law books
d. None of the above

6. Who should have access to a secure container?
a. Only the primary investigator
b. Only the investigators in the group
c. Everyone on the floor
d. Only senior-level management
7. An employer can be held liable for e-mail harassment.

aTrue b.False

8. Building a business case can involve which of the following?
a. Procedures for gathering evidence
b. Testing software
c. Protecting trade secrets
d. All of the above

9. The ASCLD mandates the procedures established for a computer forensics lab.

a.True b.False

10. The manager of a computer forensics lab is responsible for which of the following? (Choose all that apply.)
a. Necessary changes in lab procedures and software
b. Ensuring that staff members have sufficient training to do the job
c. Knowing the lab objectives
d. None of the above

11.With remote acquisitions, what problems should you be aware of?
a. Data transfer speeds
b. Access permissions over the network
c. Antivirus, antispyware, and firewall programs
d. All of the above

12. Corporate investigations are typically easier than law enforcement investigations for which of the following reasons?
a. Most companies keep inventory databases of all hardware and software used.
b. The investigator doesn't have to get a warrant.
c. The investigator has to get a warrant.
d. Users can load whatever they want on their machines.

13. As a corporate investigator, you can become an agent of law enforcement when which of the following happens? (Choose all that apply.)
a. You begin to take orders from a police detective without a warrant or subpoena.
b. Your internal investigation has concluded, and you have filed a criminal complaint and turned over the evidence to law enforcement.
c. Your internal investigation begins.
d. None of the above.

14. If a suspect computer is located in an area that might have toxic chemicals, you must do which of the following? (Choose all that apply.)
a. Coordinate with the HAZMAT team.
b. Determine a way to obtain the suspect computer.
c. Assume the suspect computer is contaminated.
d. Do not enter alone

15. Which of the following techniques might be used in covert surveillance?
a. Key logging
b. Data sniffing
c. Network logs

16. On a Windows system, sectors typically contain how many bytes?

a. 256
b. 512
c. 1024
d. 2048

17. What is the ratio of sectors per cluster in a floppy disk?
a. 1:1
b. 2:1
c. 4:1
d. 8:1

18. What is the space on a drive called when a file is deleted? (Choose all that apply.)
a. Disk space
b. Unallocated space
c. Drive space
d. Free space

19. Windows 2000 can be configured to access which of these file formats? (Choose all that apply.)
a. FAT12
b. FAT16
c. FAT32
d. NTFS

20. Which of the following Windows XP files contains user-specific information?
a. User.dat
b. Ntuser.dat
c. System.dat
d. Sam.dat

SECTION B

1. A lawyer in a law firm is suspected of embezzling money from a trust account. Who should conduct the investigation? If evidence is found to support the claim, what should be done? Write at least two pages explaining the steps to take, who is involved, and what items must be considered.

2. Jonathan Simpson owns a construction company. One day a subcontractor calls him, saying that he needs a replacement check for the job he completed at 1437 West Maple Avenue. Jonathan looks up the job on his accounting program and agrees to reissue the check for $12,750. The subcontractor says that the original check was for only $10,750. Jonathan looks around the office but can't find the company checkbook or ledger. Only one other person has access to the accounting program. Jonathan calls you to investigate. How would you proceed? Write a one-page report detailing the steps Jonathan needs to take to gather the necessary evidence and protect his company.

3. You are the computer forensics investigator for a law firm. The firm acquired a new client, a young woman who was fired from her job for inappropriate files discovered on her computer. She swears she never accessed the files. What questions should you ask and how should you proceed? Write a one- to two-page report describing the computer the client used, who else had access to it, and any other relevant facts that should be investigated.

4. A desperate employee calls because she has accidentally deleted crucial files from her hard drive and can't retrieve them from the Recycle Bin. What are your options? Write one to two pages explaining your capabilities and listing the questions you need to ask her about her system.