Chapter 2 Solutions

Review Questions

1. An employer can be held liable for e-mail harassment. True or False?

   True

2. Building a business case can involve which of the following?

   d. All of the above

3. The ASCLD mandates the procedures established for a digital forensics lab. True or False?

   False

4. The manager of a digital forensics lab is responsible for which of the following? (Choose all that apply.)

   a. Making necessary changes in lab procedures and software

   b. Ensuring that staff members have enough training to do the job

   c. Knowing the lab objectives

5. To determine the types of operating systems needed in your lab, list two sources of information you could use.

   Uniform Crime Report statistics for your area and a list of cases handled in your area or at your company

6. What items should your business plan include?

   Physical security items, such as evidence lockers; how many machines are needed; what OSs your lab commonly examines; why you need certain software; and how your lab will benefit the company (such as being able to quickly exonerate employees or discover whether they're guilty).

7. List two popular certification systems for digital forensics.

   IACIS, HTCN, EnCE, ISFCE

8. Why is physical security so critical for digital forensics labs?

   To maintain the chain of custody and prevent data from being lost, corrupted, or stolen

9. If a visitor to your digital forensics lab is a personal friend, it's not necessary to have him or her sign the visitor's log. True or False?

   False

10. What three items should you research before enlisting in a certification program?

    Requirements, cost, and acceptability in your chosen area of employment

11. Large digital forensics labs should have at least _____ exits.

    two

12. Typically, a(n) _____ lab has a separate storage area or room for evidence.

    regional

13. Digital forensics facilities always have windows. True or False?

    False

14. Evidence storage containers should have several master keys. True or False?

    False

15. A forensic workstation should always have a direct broadband connection to the Internet. True or False?

    False

16. Which organization provides good information on safe storage containers?

    NISPOM

17. Which organization has guidelines on how to operate a digital forensics lab?

    ASCLD

18. What name refers to labs constructed to shield EMR emissions?

    TEMPEST

Hands-On Projects

Hands-On Project 2-1

The main purpose of this project is for students to realize they must be consistent in how they handle cases. They need to state what the company does or what industry they're in. Some companies might be affected by the Sarbanes-Oxley Act and others by HIPAA requirements, but they're all affected by what stands up in court proceedings or disciplinary hearings. The U.S. DOJ has a publication on how to set things up that addresses questions such as the following: Can personal smartphones synched to the company network be searched? Who handles the evidence, and how is it collected, stored, and examined? How is an investigation started? Students can do a search on the term "digital evidence + procedures," for example, to find a lot of information.

Hands-On Project 2-2

Students' answers may vary, but they need to be skeptical about investigators touting a certification. Not all are qualified, so they should ask questions such as what experience they have, whether they're recognized in their field, and so on.

Hands-On Project 2-3

Students' answers may vary, but their reports should include a plan to monitor the lab to observe who accesses it. This project encourages an awareness of how often things are stolen from labs. The plan should include a schedule of who will monitor the lab and when it will be monitored. Make sure students mention who accesses the lab and at what times of day. Their reports should also make recommendations on how the lab can be made secure for digital forensics operations.

Hands-On Project 2-4

Students' answers may vary, but their reports should include as much information as possible on all hardware and software used in the lab. Reports should also list all available system backups currently used in the lab. Make sure students mention the minimum hardware and software needed to operate the lab. They should also list a recommended backup schedule for computers and media storage systems and a recommendation for off-site storage of backup media.

Hands-On Project 2-5

Students should begin by talking to the group that previously handled investigations to find out what equipment and software had been used. They should also talk to the firm's partners to see what worked and what didn't. They need to know, for example, how many cases a week they have to handle.

Case Projects

Case Project 2-1

Students should create a spreadsheet with the following details:

For hardware:

- Computer model
- Processor speed
- RAM
- Disk storage
- Monitor

For software, the following are possible answers:

- Windows OS
- Microsoft Office Pro
- X-Ways Forensics
- OSForensics

Case Project 2-2

Students' answers may vary, but their reports should include public release information from Microsoft on the next-generation OS with expected release dates. Make sure students mention sources of information and any available information from technology news sources and forums.

Case Project 2-3

Students' answers may vary because each state or province has its own expectations for licensing private digital forensics examiners. Students' papers should include minimum training requirements and any work experience along with the cost of licenses.