Chapter 2 Solutions

Review Questions

1. What are some initial assessments you should make for a computing investigation?

   Talk to others involved in the case and ask about the incident.

   Determine whether law enforcement or company security officers already seized the computer evidence.

   Determine whether the computer was used to commit a crime or contains evidence about the crime.

2. What are some ways to determine the resources needed for an investigation?

   Determine the OS of the suspect computer.

   List the necessary software to use for the examination.

3. List three items that should be on an evidence custody form.

   Possible answers include case number, name of the investigator assigned to the case, nature of the case, location where evidence was obtained, description of the evidence, and so on.

4. Why should you do a standard risk assessment to prepare for an investigation?

   to list problems that might happen when conducting your investigation as an aid in planning your case

5. You should always prove the allegations made by the person who hired you. True or False?

   False

6. For digital evidence, an evidence bag is typically made of antistatic material. True or False?

   True

7. Who should have access to a secure container?

   b. Only the investigators in the group

8. For employee termination cases, what types of investigations do you typically encounter?

   hostile work environment caused by inappropriate Internet use

   sending harassing e-mail messages

9. Why should your evidence media be write-protected?

   to ensure that data isn't altered

10. List three items that should be in your case report.

    Answers can include an explanation of basic computer and network processes, a narrative of what steps you took, a description of your findings, and log files generated from your analysis tools.

11. Why should you critique your case after it's finished?

    to improve your work

12. What do you call a list of people who have had physical possession of the evidence?

chain of custody

13. What two tasks is an acquisitions officer responsible for at a crime scene?

    Answers can include providing a list of all components that were seized, noting whether the computer was running at the time it was taken into evidence, making notes of the computer's state at the time it was acquired, noting the operating system if the computer is running, and photographing any open windows to document currently running programs.

14. What are some reasons that an employee might leak information to the press?

    Reasons range from disgruntled employees wanting to embarrass the company to rival organizations competing against each other.

15. When might an interview turn into an interrogation?

    Interviews are intended to collect facts about an investigation. An investigator might find that these facts warrant considering the witness to be a suspect, at which point the interview becomes an interrogation.

16. What is the most important point to remember when assigned to work on an attorney-client privilege case?

    keeping all your finding confidential

17. What are the basic guidelines when working on an attorney-client privilege case?

    Minimize written correspondence, make sure all written documentation and communication includes a label stating that it's privileged communications and confidential work product, and assisting the attorney and paralegal in analyzing data.

18. Data collected before an attorney issues a memorandum for an attorney-client privilege case is protected under the confidential work product rule. True or False?

    False. All data collected before an attorney issues notice of attorney-client privilege is subject to discovery by opposing counsel.

Hands-On Projects

Hands-On Project 2-1

Students should extract files with the Copy File feature and find two files in the image: a spreadsheet listing several accounts and their values and a life insurance policy. A text meesage is also included.

Students should write a brief statement of their findings from these two files. Reports shouldn't make any conclusions about the nature of the file contents.

Hands-On Project 2-2

Students should use the Content Search and Cluster Search tabs in the Search dialog box and enter the keyword "book." Their memos should describe the filename and cluster location of each hit. Students should find 24 hits.

Hands-On Project 2-3

This project allows students to practice keyword searches and shows that the information they seek might not be in obvious places. In this project, for example, the account number students need to locate is in the Count.gif file, so they must examine graphics files, too. Students should

also perform the same search for the keyword "book" in C2Prj03.dd as they did in Hands-On Project 2-2 with C2Prj02.eve and find similar results—that is, 24 hits on the keyword "book."

Hands-On Project 2-4

The project shows students how to extract specific data—in this case, files that haven't been deleted in an image.

Hands-On Project 2-5

Students practice selecting unallocated files and then generating a report.

Hands-On Project 2-6

Students need to apply all the skills they learned in the chapter to do this project on searching for keywords.

Case Projects

Case Project 2-1

Students need to do an assessment of what the case involves. What is the nature of the case? What challenges do they expect to encounter, and how much time do they think the investigation will take?

Case Project 2-2

After interviewing the parents, the investigator should get as much information as possible, such as names of close friends, who the girl has been talking to, and so forth. The laptop and any storage media should be bagged and tagged correctly and taken to the computer forensics lab.

Case Project 2-3

Most likely, Jonathan needs his computer to do other things in his business. Students need to acquire an image (preferably two) of the drive. Also, they should look around for clues of other storage media, and then go back to the lab and analyze the image. They should get as much detail as possible about the company and the other person.

Case Project 2-4

Students need to ask who else had access to the computer, find out whether the firm that fired her did its own investigation, and determine whether they can have access to the images. If no investigation has been done, students should state whether they can make copies now.

Case Project 2-5

Students need to find out which OS she was using and ask whether she knows the names of essential files or folders to make their search easier. Students need to formulate interview questions to determine whether she might have added new data or altered data since the file

deletion. They should understand that any file deletion recovery depends on the amount of computer activity immediately following the data loss.