Solution Manul Ch01 - Lecture notes 2

Computer forensics (EBS Rahvusvaheline ülikool)

Chapter 1

Review Questions

1. Digital forensics and data recovery refer to the same activities. True or False?

   False

2. Police in the United States must use procedures that adhere to which of the following?

   b. Fourth Amendment

3. The triad of computing security includes which of the following?

   c. Vulnerability/threat assessment, intrusion detection and incident response, and digital investigation

4. What's the purpose of maintaining a network of digital forensics specialists?

   To develop a list of colleagues who specialize in areas different from your own specialties in case you need help on an investigation.

5. Policies can address rules for which of the following?

   d. Any of the above

6. List two items that should appear on a warning banner.

   Statements that the organization has the right to monitor what users do, that their e-mail is not personal, and so on

7. Under normal circumstances, a private-sector investigator is considered an agent of law enforcement. True or False?

   False

8. List two types of digital investigations typically conducted in a business environment.

   Fraud, embezzlement, insider trading, espionage, and e-mail harassment

9. What is professional conduct, and why is it important?

   Professional conduct includes ethics, morals, and standards of behavior. It affects your credibility.

10. What's the purpose of an affidavit?

    To provide facts in support of evidence of a crime to submit to a judge when requesting a search warrant

11. What are the necessary components of a search warrant?

    A search warrant must specify who, what, when, and where—that is, specifics on place, time, items being searched for, and so forth—and include any supporting materials (affidavits and exhibits, for example). In addition, a search warrant must be signed by an impartial judicial officer. In many cases, a search warrant can limit the scope of what can be seized.

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

    Determine the OS of the suspect computer and list the software needed for the examination.

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

    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.

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

    To list problems that might happen when conducting an investigation, which can help in planning your case

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

    False

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

    True

17. Why should evidence media be write-protected?

    To make sure data isn't altered

18. 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.

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

    To improve your work

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

    Chain of custody

21. Data collected before an attorney issues a memo 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 1-1

Students should extract two files with the Copy File feature: a spreadsheet listing several accounts and a life insurance policy (`Sylvia's Assets.xls`) and a text message (`suicide1.txt`). To start the program associated with each file, students should right-click the file and click View. 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 1-2

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 approximately 24 hits.

Hands-On Project 1-3

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 `C1Prj03.dd` as they did in Hands-On Project 1-2 with `C1Prj02.eve` and find similar results—that is, more than 20 hits on the keyword "book."

Hands-On Project 1-4

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

Hands-On Project 1-5

Students practice selecting unallocated files and then generating a report.

Hands-On Project 1-6

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

Case Projects

Case Project 1-1

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 1-2

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 1-3

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 1-4

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.