Chapter 2 Solutions

Lab 2.1 Review Questions

1. Which statement about deleted files is true?

a. Deleted files can be rebuilt from remnants that haven’t been overwritten.

2. When a file is deleted from a storage device, only the pointer to the file location is removed. True or False?

True

3. According to NIST standards, how many wipes should be done to erase data completely?

d. Seven

4. Which of the following statements about the MFT is true?

b. The MFT is updated to indicate free space when files are deleted.

5. Secure destruction of digital data requires doing which of the following?

b. Writing 0s and 1s to the storage device to overwrite file remnants

Lab 2.2 Review Questions

1. Directory Snoop is designed to work with which of the following file systems? (Choose all that apply.)

b. NTFS

d. FAT

2. Disk images don’t include the MFT. True or False?

False

3. Which statement about Directory Snoop’s Cluster, Copy to file menu choice is true?

c. It can copy all or specific clusters of a disk drive.

4. What’s the purpose of a write-blocker?

a. Preventing any data on the original storage device from being overwritten, which would violate the chain of custody

5. What’s the purpose of disk imaging? (Choose all that apply.)

b. Giving investigators a way to analyze data without destroying potential evidence on the original medium

c. Maintaining the chain of custody

Lab 2.3 Review Questions

1. What’s the intended purpose of Directory Snoop?

b. Its primary purpose is for data recovery on disk drives.

2. Directory Snoop is capable of validating copied or compressed data. True or False?

False

3. What’s the purpose of splitting a forensic image into smaller files?

Enables storing an image on media such as CDs, DVDs, and USB drives

4. A compressed .E01 image is the same size as the total size of all evidence files on the original source. True or False?

False

5. Forensics investigators should be familiar with more than one forensics acquisition tool in case a tool fails to run on their computer. True or False?

True

Lab 2.4 Review Questions

1. FTK Imager Lite can produce all the following image formats except which one?

d. .Ext4 (Linux)

2. Which of the following features isn’t available in FTK Imager Lite?

b. Being optimized to search large volumes of data

3. FTK Imager Lite is designed to be portable. True or False?

True

4. FTK Imager Lite calculates which hash values during file imaging? (Choose all that apply.)

a. MD5

b. SHA-1

5. Why does FTK Imager Lite calculate two hash values?

b. To provide redundant verification that files haven’t been altered during imaging

Lab 2.5 Review Questions

1. How many existing Excel files were recovered in the C2Proj4.e01 image?

b. 7

2. How many deleted files were recovered in the C2Proj4.e01 image?

a. 2

3. What’s the filename of the deleted Excel file in the C2Proj4.e01 image?

c. Qtr 1 Emp.xlsx

4. What’s the name of the deleted Word file in the C2Proj4.e01 image?

b. Online.docx

5. How many SHA-1 hash files were exported to the C2Proj4 deleted file hashes.csv file?

b. Two