Lab 02 Project (Chapter 4)

Processing Crime and Incident Scenes

Due: 11:59 PM on Monday, September 26, 2022

Your agency received word that a bank robbery has taken place. The laptop of the suspect, John Smith, has been obtained and an image made. You have been asked to go over the evidence using the image for details about the crime that can be used in court.

**Searching for Evidence in OSForensics**

When forensics investigators process evidence during an investigation involving computer-related crimes, they often need to create a bit-stream copy of the original evidence and analyze the forensically imaged copy. In this lab, you will add a drive image to OSForensics and perform cursory analysis of image contents to determine whether the image contains any potential evidence. Storage devices can contain millions of files and other objects that can take significant time to search. Forensics investigators need to quickly examine evidence and bookmark any suspicious files or information they encounter as they prepare their case.

1. Start **OSForensics** on your workstation. If prompted to allow the program to make changes to your computer, click **OK** or **Yes**. Note that you may be prompted to enter your user ID and password. In the OSForensics message box, click **Continue Using Free Version**.
2. In the left pane, click **Manage Case**, if necessary. In the Manage Case pane on the right, click the **New Case** button. In the New Case dialog box, type **C4Lab1** in the Case Name text box and your name in the Investigator text box. For the Acquisition Type setting, click the **Investigate Disk(s) from Another Machine** option button. Click **Custom Location** for the Case Folder option. Click the **Browse** button on the lower right, navigate to and click your desired work folder, and then click **OK** twice.
3. To mount the disk image, scroll down the navigation bar on the left, and click **Mount Drive Image**. In the Mounted virtual disks window, click the **Mount new** button. In the OSFMount – Mount drive dialog box that opens, click the **...** button next to the Image file text box, navigate to the location of the **C4Proj1.dd** image, select the C4Proj1.dd image, click **Open**, and then click **OK**, remembering the drive letter where the image was mounted. Click the **Exit** button to close the window.
4. Click the **Deleted Files Search** button in the left pane. In the Disk drop-down menu in the right pane, select the appropriate volume for the image that you just mounted and click the **Search** button.
   1. How many deleted files were recovered in this image? \_\_\_\_\_\_\_
5. Right-click the deleted **Blue Chip Stock Club Investment Analysis.xls** file, select the **Save Deleted File…** menu option, and then navigate to your desired work folder. Click **OK** to save the file. Now, outside of OSForensics, navigate to your work folder and open the file in Microsoft Excel.

b. What was the name of the lowest performing stock identified in this file in both Gain/Loss and Percent Gain/Loss? \_\_\_\_\_\_\_

1. Now, right-click the deleted **Biometrics Paper.doc** file, and select the **File Location Information…** menu option to view the raw location information for the file.

c. How many clusters does this file take up? \_\_\_\_\_\_\_

1. Click the **OK** button to exit the Deleted File – Raw Location window. Again, right-click the deleted Biometrics Paper.doc file, then select the **Save Deleted File…** menu option, and then navigate to your desired work folder. Click **OK** to save the file. Now, outside of OSForensics navigate to your work folder and open the file in Microsoft Word.

d. Who is the author of the biometrics student paper? \_\_\_\_\_\_\_

e. According to experts (back in 2005), what technology will become the home user’s authentication device for e-commerce transactions? \_\_\_\_\_\_\_

1. Click the **Verify / Create Hash** button in the left pane. In the right pane, ensure that the File radio button is selected and then click the **...** button next to the File text box. Navigate to your mounted image and locate the **Walking.ppt** PowerPoint 97-2003 Presentation file. Select this file and click the **Open** button. In the Hash Function drop-down menu, select **MD5** and click on the **Calculate** button to calculate the MD5 hash value for this file. Repeat this last step for **SHA-1**.

f. What are the first five digits (in hex) of the MD5 file hash for this image? \_\_\_\_\_\_\_

g. What are the first five digits (in hex) of the SHA-1 file hash for this image? \_\_\_\_\_\_\_

1. Click the **Create Index** button in the left pane. In the Step 1 of 5 window, click the **Use Pre-defined File Types** option button, click to select all the file types listed, and click **Next**. In the Step 2 of 5 window, click the **Add** button. In the Add Start Location dialog box, verify that the **Whole Drive** option is selected, select the logical drive for your mounted image from the drop-down menu, and then click **OK**. Click **Next**, and in the Step 3 of 5 window, click **Start Indexing**. Wait until OSForensics finishes indexing (which might take several minutes) until proceeding to the next step – you should see “Finished” in the Current Action text box.

h. How many unique words were found in the image? \_\_\_\_\_\_\_

1. Click the **Search Index** button in the left pane.

i. How many “Files” were found in this image? \_\_\_\_\_\_\_

j. How many “Images” were found in this image? \_\_\_\_\_\_\_

k. Now click on the **Browse Index** tab and search through the results. How many instances of the word “Bank” were found? \_\_\_\_\_\_\_

1. Now click on the **Images** tab and find the picture of the flowers in a vase displayed in the lobby of a building. Right-click the image, and select the **View with Internal Viewer…** menu option to view the image and its properties. Search through the OSForensics Internal Viewer tabs for the answers to the following questions.

l. What is the name of this file? \_\_\_\_\_\_\_

m. What is the hexadecimal character encoding for JFIF? \_\_\_\_\_\_\_

n. What Camera Model Name was the picture taken with? \_\_\_\_\_\_\_

1. When done, close the window to exit the Internal Viewer.
2. Leave OSForensics open for the next lab.

**Searching for E-Mail Evidence Using OSForensics**

E-mail evidence is undoubtedly one of the most important aspects of computer-related crimes because each e-mail message contains accurate time stamp information that cannot be altered without detection. When an e-mail message is sent, the sending computer places a header in the outgoing message that can be used to track the message from the source to the destination. In addition, time stamps are appended to the header as e-mail messages pass through each mail handler on their way to the recipient. Each e-mail server involved in the exchange of the message will have a record with the e-mail header information and its time stamp information. This allows investigators to verify the authenticity of the e-mail message and make falsification of the e-mail message almost impossible without detection. In this lab, you will examine the e-mail records discovered in the previous lab.

1. In the Search Index pane, click on the **Emails** tab.

o. How many “Emails” were found in this image? \_\_\_\_\_\_\_

1. Find the e-mail with the subject “test” and double click the e-mail to view it (and other e-mails) in the **E-mail Viewer**. Once in the E-mail Viewer, expand the **backup.pst** icon by clicking on the **+** symbol in the upper-left window. This file contains the MS Outlook database file taken from the suspect’s hard drive.
2. Expand the **Top of Personal Folders** to view the Outlook e-mail structure. The Top of Personal Folders folder contains child folders for Deleted Items, Inbox, and Sent Items folders. Click the **Inbox** folder to view the inbound e-mail messages.

p. How many e-mail messages are contained in the Inbox mailbox? \_\_\_\_\_\_\_

1. Select the e-mail message with the time stamp for 5/31/2009 at 8:12 PM (may appear as 7:12 PM on some computers). The actual e-mail message is displayed in bottom window along with the message details. The message attachments can be viewed by double-clicking each file attachment.
2. How many attached graphic images are contained in this message? \_\_\_\_\_\_\_
3. What is the subject of this e-mail message? \_\_\_\_\_\_\_
4. Click the **Sent Items** folder to view the sent messages. Each sent e-mail message contains the next time stamps and the embedded header time stamps.
5. How many e-mail messages are contained in the Sent Items mailbox? \_\_\_\_\_\_\_
6. What is the e-mail time of the last sent e-mail message? \_\_\_\_\_\_\_
7. To whom did John Smith send the last e-mail message? \_\_\_\_\_\_\_
8. When done, close the window to exit the E-mail Viewer.
9. Leave OSForensics open for the next lab.

**Searching for Keywords in OSForensics**

Forensics investigators need to search through files to locate keywords or phrases that may be contained in documents of other files. Often keywords may be useful in searching for evidence linked to a crime. In this lab, you will search for evidence linked to a bank robbery involving two people who may have communicated using e-mail. The bank robbers were familiar with the work schedule at the bank and were not detected as they compromised a number of safe deposit boxes.

1. In the Search Index pane, type **bank** in the Enter Search Words text box and click the **Search** button.
2. In how many files was the word **bank** found? \_\_\_\_\_\_\_
3. In how many e-mails was the word **bank** found? \_\_\_\_\_\_\_
4. Now add the word **vault** to the original word **bank** in the Enter Search Words text box and click the **Search** button.
5. How many results for the words **bank vault** appear? \_\_\_\_\_\_\_
6. Double-click the first message to display the e-mail containing both **bank** and **vault** in the E-mail Viewer.
7. Who is the recipient of this e-mail message? \_\_\_\_\_\_\_
8. Who was John’s accomplice in the crime? \_\_\_\_\_\_\_
9. Which branch location is the suspect inquiring about? \_\_\_\_\_\_\_
10. Close the E-mail Viewer to get back to the Search Index pane.
11. Type **escape** in the Enter Search Words text box and click the **Search** button.
12. Where does John Smith plan to go to in his escape? \_\_\_\_\_\_\_
13. The bank robbers forced the back door open to gain access to the bank. Search for “back door” to see whether this detail was planned. Type **back door** in the Enter Search Words text box and click the **Search** button. Double-click the one file in the results to view the document in the Internal Viewer.
14. What is the name of the file containing the words **back** and **door**? \_\_\_\_\_\_\_
15. Which exit do the tellers use to leave the bank? \_\_\_\_\_\_\_
16. On what date was this document created? \_\_\_\_\_\_\_
17. What is the readable title of the document that is different from the actual name of the file? \_\_\_\_\_\_\_
18. Could this file implicate another person? And if so, what is the name of the other possible accomplice? \_\_\_\_\_\_\_

You are to submit this document, with your solutions, to the **Lab 2**dropbox on Canvas by the due date and time.