CSCE 4555/5555 – Computer Forensics

Lab 05 Project (Chapter 8)

Student ID: 11647576

Processing Evidence Containing Graphics Images

You have been summoned to a crime scene to help recover potential evidence found on a booted computer. On initial examination of the evidence, you see several files that have suspicious file extensions, and they are not able to be viewed in Windows Explorer. Experience tells you that there may be potential evidence hidden from view, and your job is to find any usable data. The InChap8.001 image file will be added to OSForensics and processed in this lab.

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 **C8Lab1** 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 **InChap8.001** image, select the InChap8.001 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. In the left pane, click the **Create Index** button. 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, select the **Whole Drive** option, select the drive letter for the virtual disk that you just mounted in the previous step, and then click **OK**, followed by **Next**. In the Step 3 of 5 window, click **Start Indexing**. Wait until OSForensics finishes indexing (which might take several minutes). When the OSForensics – Create Index dialog box appears, click **OK** (do not worry if it indicates that there were some errors in the indexing process).

5. Once completed, click the **Search Index** button in the left pane. Without typing anything in the Enter Search Words text box, click the **Search** button.

6. Select the **Images** tab. Double-click the **old.jpg** file. The file should automatically open in Windows Photo Viewer (or whatever viewer is installed on your workstation).

   a. How many “switches” are ON in this image? **__5_____**

7. Close the viewer. Now, locate the **03x07.bmt** file. You should be able to see the image in the OSForensics application. Try double-clicking on this image. Because the extension is not correct, you should see a Windows dialog box (or similar) indicating that Windows

can't open this file. Click **Cancel** in the Windows dialog box. Now, 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.

b. What type of file is the 03x07.bmt file? **__JPEG File_____**

c. What encoding process was used for this file? __ **Baseline DCT, Huffman coding____**

d. What date was the 03x07.bmt file modified? **Saturday, january 3, 2009, 10:56:54 AM.0000000** _____ _____

8. When done, close the window to exit the Internal Viewer.

9. Select the **Files** tab. Locate the **temp.doc** file, and notice that although it "appears" to be a MS Word document, it is not. 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 question.

e. What is the true file type of this file? **__File Type,JPEG_____**

10. When done, close the window to exit the Internal Viewer.

11. Now, locate the **Test 1.txt** file. 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.

f. In the File Viewer tab, what does it say about this file?_**Unsupported File format**_____

g. Who was the file last modified by? **___Andy____**

h. Despite its .txt extension, what type of file does this appear to really be?_____**File Type,DOCX___**

12. When done, close the window to exit the Internal Viewer.

13. Click the **Deleted Files Search** button in the left pane. Without typing anything in the Enter Search Words text box, click the **Search** button. Select the applicable drive in the Disk pull-down menu for this virtual disk and click the **Search** button (without typing anything in the Filter String text box).

i. How many deleted files were found in this image? **07_____**

14. Locate the **safe deposit boxes.jpg** file. Right-click the image, and select the **File Location Information…** menu option to view its Deleted File – Raw Location dialog box.

j. What is the starting logical cluster number (LCN)? **___5145_____**

k. How many clusters are used for this file? **17_____**

15. Now click **OK** to close the Deleted File – Raw Location dialog box.

16. Click the **Mismatch File Search** button in the left pane. Click the **...** button next to the Start Folder text box and select the applicable drive for the virtual disk that you mounted in the Browse for Folder dialog box.

    l. How many mismatched files were found? **_08_____**

17. Click the **Exit** button in the left pane to close the OSForensics program.

Locating Graphics in Unreadable Partitions

Forensic evidence is often hidden by criminals using various methods on deliberately corrupted or modified partitions to make it invisible to all but the creator of the file. One of the most common methods used to hide data is to modify the file properties such as the header or file extension. For example, the file header that identifies the file type to the file system can be altered using a hex editor, rendering it unreadable by the operating system. In some cases, the file can be overlooked by forensic software unless the investigator knows how to apply special features such as data carving to rebuild corrupt file attributes. In this part of the lab, you will apply the data-carving feature to rebuild files that have been deliberately altered.

18. 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**.

19. 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 **C8Lab2** 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.

20. 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 **C8unreadable.001** image, select the C8unreadable.001 image, click **Open**, and then click **OK**, remembering the drive letter where the image was mounted. Click the **Exit** button to close the window.

21. In the left pane, click the **Create Index** button. 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, select the **Whole Drive** option, select the drive letter for the virtual disk that you just mounted in the previous step, and then click **OK**, followed by **Next**. In the Step 3 of 5 window, click **Start Indexing**. Wait until OSForensics finishes indexing (which might take several minutes). When the OSForensics – Create Index dialog box appears, click **OK** (do not worry if it indicates that there were some errors in the indexing process).

22. Once completed, click the **Search Index** button in the left pane. Without typing anything in the Enter Search Words text box, click the **Search** button.

23. Select the **Images** tab.

    m. What is the name of the file that "appears" to be damaged?___**Security bars.jpg**_____

    n. Right-click on this image, and select the **View with Internal Viewer…** menu option to view the image and its properties. Select the Hex/String Viewer tab. In place of the expected "JFIF" for JPEG files, what four printable letters are in its place? **__jped**_____

24. When done, close the window to exit the Internal Viewer.

25. Select the **Files** tab. Locate and right-click the **AC19.gpj** file, 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.

    o. In the File Viewer tab, what does it say about this file?_**Unsupported file format**_____ _____

    p. In the Hex/String Viewer tab, take a look at the header information for this file (hint: reverse the letters of the file extension). What type of file do you suppose this is? **_.jpg**_____

33. Close the window to exit the Internal Viewer. Right-click the **AC19.gpj** file again, but this time, select the **Copy File(s) to Clipboard** menu option. In Windows Explorer, navigate to your desktop (or work folder) and paste the file to that location. Using your knowledge of rebuilding headers to repair files, open this file in WinHex and repair the header, saving it as **AC19.jpg** when repaired. Now, double-click the repaired file to open in the default viewer (e.g., Windows Photo Viewer). Describe the image that you see (it is abstract, so describe the colors and what you see).

    q. **_____ Black Intersecting lines on a white background**.

26. Click the **Mismatch File Search** button in the left pane. Click the **...** button next to the Start Folder text box and select the applicable drive for the virtual disk that you mounted in the Browse for Folder dialog box.

27. You should see one file in the File List tab that is also damaged, similarly to the AC19.gpj file you found earlier. Use WinHex and apply the same technique to repair this file, saving the repaired version as **Repaired1.jpg**. Once repaired, double-click the file to open in the default viewer (e.g., Windows Photo Viewer).

    r. What two items are found in this image? **__Lock and Key**_____

    s. What word is clearly visible on one of the items in the image? **____Private**___

28. Click the **Exit** button in the left pane to close the OSForensics program.

You are to submit this document, with your solutions, to the **Lab 05** dropbox on Canvas by the due date and time.