CSCE 4555/5555 – Computer Forensics

Lab 06 Project (Chapter 9)

Computer Forensics Analysis and Validation

Due: 11:59 PM on Tuesday, November 8, 2022

StudentID:11647576

Searching for Hidden Partitions

The search for computer crimes often involves recovering data from hidden or deliberately modified disk partitions where the criminal might store potential evidence. In some cases, criminals hide data by formatting different file systems on a single physical disk. For example, a hard disk might have two partitions where the first partition is formatted in NTFS and the second partition is formatted in HFS or some other file system unreadable by Windows. In this situation, an examiner looking for evidence using Windows Explorer will only see the first NTFS partition and its associated files, but will not see the second partition unless the storage device is viewed using the Disk Management feature. The Disk Management utility will only identify the second partition as "Healthy" without providing any file system details. You have seen in previous labs that FTK Imager can view Windows and Macintosh file partitions and perform preliminary searches for files. In this lab, you will examine evidence gathered from a USB flash drive attached to a Windows computer to locate hidden partitions not visible in Windows.

1. Start **FTK Imager** on your workstation. If prompted to allow the program to make changes to your computer, click **OK** or **Yes**. When FTK Imager has finished loading, click the **File** tab and select the **Add Evidence Image** item.
2. Select the **Image File** radio button in the Select Source dialog box, and click **Next**.
3. In the Select File dialog box, click **Browse** and navigate to the **C9Proj1.E01** image file in the InChap9 folder, and click **Open**. Do not select the .txt file with the same name – it will be used later.
4. Click **Finish** in the Select File dialog box.
5. Click all the **+** symbols to expand the folders in the **C9Proj1.E01** icon in the upper-left evidence tree window.
   a. How many partitions are found? Do not include *Unpartitioned Space*. **__3___**
   b. What is the size of each of the partitions? **__40MB____**
6. Select the **Partition 1 [40MB]** drive icon.
   c. What is the Starting Sector for Partition 1? **__63____**

d. What is the Sector Count for Partition 1? ___**83,208**___

7. Click the **[root]** folder located in Partition 1, and note the evidence files in the upper-right File List window. Select the **Eyeglass** icon on the tool bar if necessary, and click each .jpg file to view them using the built-in file viewer in the lower-right window.

e. What is the word found embedded in the picture of the **lock.jpg** file? **_PRIVATE_____**

8. Create an **Evidence** folder on your USB flash drive or other device. Right-click the **[root]** folder, select **Export Files**, navigate to your Evidence folder, and click **OK** in the Browse for Folder dialog box to send the exported files to the Evidence folder.

f. According to the Export Results dialog box, how many folders and how many files (two different numbers) were exported successfully? **_5 folder(s) and 30 files_____**

9. Close the Exported Results dialog box by clicking **OK**. The exported files will be located in the [root] folder within the Evidence folder, although not apparently visible.

10. Click the Windows **Start** button, select **Control Panel**, select **Appearance and Personalization**, select **Folder Options**, and click on the **View** tab in the Folder Options dialog box. Now click **Show hidden files, folders, and drives**, uncheck the **Hide extensions for known file types** check box if applicable, and uncheck the **Hide protected operating systems files (Recommended)** check box. Click **Yes** in the Warning dialog box, click **Apply**, and click **OK** in the Folder Options dialog box. You can now browse the [root] folder using Windows Explorer. *Note that this step may be slightly different in Windows 10.*

g. What is the text is found in the **Test1.docx** document? **_This is a test file_____**

11. Select the **Partition 2 [40MB]** drive icon.

h. What is the Starting Sector for Partition 2? **83,286_____**

i. What is the Sector Count for Partition 2? **__83,032____**

j. Assuming contiguous sector blocks, how many sectors exist between Partition 1 and Partition 2? **15_____**

12. Click the **HFS+** folder located under the Partition 2 drive icon. Note that this HFS+ folder is one level below the HFS+ [HFS+] folder. Now right-click the **HFS+** folder, select **Export Files**, navigate to your Evidence folder, and click **OK** in the Browse for Folder dialog box to export the files and folders using the same procedure as before. Click **Close** in the Export Results dialog box and disregard any error messages.

13. Select the **Partition 3 [40MB]** drive icon.

k. What is the Starting Sector for Partition 3? **_166,320_____**

l. What is the Sector Count for Partition 3? **__82,971____**

14. Select the **Untitled 3 [HFS+]** folder located under the Partition 3 drive icon.

m. What is its Cluster Size? **_4,096_____**

15. Right-click the **Untitled 3 [HFS+]** folder, select **Export Files**, navigate to your Evidence folder, and click **OK** in the Browse for Folder dialog box. Click **Close** in the Export Results dialog box and disregard any error messages.

16. Navigate to your Evidence folder using Windows Explorer, and verify that it contains the [root], HFS+, and Untitled 3 folders containing the exported evidence files. You may close Windows Explorer.

17. Click the **C9Proj1.E01** image located at the top of the Evidence Tree in the upper-left window, and locate the Verification Hashes section in the lower-left Properties window to view the MD5 and SHA1 verification hashes.

    n. What are the first 5 hex digits of the MD5 verification hash? **__bdf78____**

    o. What are the first 5 hex digits of the SHA1 verification hash? **____d842c__**

    p. What is the Sector Count of the Drive Geometry? **__249,343____**

18. Now, open the **C9Proj1.E01.txt** file in Notepad. Compare the computed hashes in the text document with the Verification Hashes in FTK Imager. They should match, indicating that the processed image is forensically identical to the recovered image from the seized storage device.

19. Click the **File** tab in FTK Imager, and select **Exit** to close FTK Imager. Close the C9Proj1.E01.txt file.

Examining the Original Evidence with OS Forensics and ProDiscover

The USB evidence presented in this chapter contained two hidden partitions with potential evidence that might have been overlooked. Forensics investigators should become familiar with multiple discovery tools because one tool may not find all the evidence or support multiple file systems in use on storage devices. You have learned that criminals often save potential evidence in corrupt or hidden partitions to hide them from investigators assuming that only one file system is in use within a hard drive or other storage media. In this part of the lab, you will examine the original forensic image recovered at a crime scene and compare the results with the previous lab exercise results to determine how much information might have been missed if the investigator only used one forensic tool.

20. 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**.

21. 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 **C9Lab2** 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.

22. 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 **C9Proj1.E01** image, select the C9Proj1.E01 image, making note of the details in the Select a partition in image dialog box. Select **Use entire image file** option, click **Open**, and then click **OK**, remembering the drive letter where the image was mounted. Click the **Exit** button to close the window. If a Microsoft Windows dialog box displaying the message that you need to format the disk before you can use it appears, click **Cancel**.

    q. How many partitions are found in this image file? **_3_____**

    r. What is the size of Partition 1 and Partition 2 (should be same size)?**__40.5 MB_____**

    s. Which OS and file system is used for Partition 1 and Partition 2?**___MacOS X FHS_____**

23. Unfortunately, OS Forensics appears to have trouble with these Macintosh partitions, so we might have to try another forensics tool to look at this data.

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

25. Start **ProDiscover Basic** on your workstation.

26. If the Launch Dialog box appears, type **C9Lab2** into the Project Number and Project File Name boxes in the New Project tab, and click **OK**. Otherwise, click the **File** tab and click **New Project** and type **C9Lab2** into the boxes as above for the New Project dialog box.

27. Click the **Action** tab and click **Add**; then in the submenu, click **Image File**.

28. In the Open dialog box, browse to the location of the **C9Proj1.E01** file, click the file, and select **Open**.

29. Expand the **Images** icon located under the **Content View** by clicking on the **+** symbol, and then clicking the **+** symbol next to the **C9Proj1.E01** image icon. Verify that there are three partitions in this image. Now, click on the **+** symbol to expand **C:** and then select All Files to show all the regular files in the right-window.

    t. How many total regular files are found? **__8____**

30. Now, select the **D:** partition. You should notice that there is no **+** symbol to expand its contents. However, this does not mean that there is nothing found in this partition. We know, from our earlier attempt using OS Forensics that this is a Macintosh HFS partition.

31. Unfortunately, searching D: under Content View did not reveal any interesting artifacts, so expand the **Images** icon located under the **Cluster View** by clicking on the **+** symbol, and then clicking the **+** symbol next to the **C9Proj1.E01** image icon. Now, select the **D:** partition. Except for the Boot Sector & Partition Data at cluster 0, all other clusters appear to be unused (i.e., they are blue in color).

32. Go to cluster (hex) 36 either manually or by entering 36 in the selected cluster text box.

u. In the bottom-window pane, what Word document can you find evidence of that existed, at least at one time, on this partition? **_Test 2.docx_____**

v. What other file type existed, again at least at one time, on this partition?**__.jpg ____**

33. Select **Search** in the left-window pane. Click on the **Cluster Search** tab in the Search dialog box and select the **Search in Unallocated only** check box. Select the **Hex** radio button. In the **Search for the pattern() :** text box, type **6A00700067**, which is the hex pattern for jpg (with NULL characters in between each letter). Select the **D:** partition in the **Select the Disk(s) / Image(s) you want to search in :** text box and click **OK**.

w. How many clusters were found to contain this pattern? **_77_____**

34. Click the **File** tab and select **Exit**. Click **No** in the ProDiscover dialog box to close ProDiscover.

You are to submit this document, with your solutions, to the **Lab 06** dropbox on Canvas by the due date and time.