Lab 04 Project (Chapter 7)

Linux and Macintosh File Systems

Due: 11:59 PM on Friday, October 14, 2022

Student ID:11647576

Using Forensic Tools to Examine and OS X Macintosh Image

Although FTK Imager is designed to facilitate the imaging process, it can provide useful information and allow evidence found on an HFS+ OS X partition to be exported into Forensic Toolkit (FTK) for forensic analysis. This process may be useful to forensics investigators requiring analysis of HFS+ partitions using Windows-based tools that may not directly support Macintosh file systems. The HFS+ file system is an improved version of the HFS file system supporting large disk sizes used in today's computers. The HFS+ or Mac Extended file system was introduced in the release of OS X 10.3, and it is used in the current version. In this part of the lab, you will extract the OS X image file from compressed files and export the useful information to be added to the FTK for evidentiary processing.

- 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 Item…** item.
- Select the **Image File** radio button in the Select Source dialog box, and click **Next**.
- Click the **Browse** button, navigate to the extracted OSX folder, select the **GCFI-OSX.001** image file, and click **Open**. Click **Finish** in the Select File dialog box.
- In the upper-left Evidence Tree window, click the + symbols to expand the **GCFI-OSX.001**, **Shu Systems [HFS+]**, and **Shu Systems** folders to display the list of directories located in the OS X root. Examine the folder structure, and note the differences between OS X and Windows.
    - Identify the three top-level folders in the **Shu Systems** folder beginning with a lower-case character that have names with three characters total._bin,dev,usr_______
- OS X creates a folder for each user and also creates a **Shared** folder to allow users to share files. Expand the **Users** folder.
    - What is the name of the user account specifically listed? _jimshu______
- Click the **+** symbol to expand the user account found in the previous step, and then click the **Documents** folder to view this user's documents.
    - Which two files have been downloaded?BicycleHelmetUseLaws.pdf and bikeped.zip________

____

- Locate the **02 Bike Helmet Use.pdf** file, and select the unlabeled **Eyeglass** icon on the tool bar in FTK Imager to view the **.pdf** file in the lower-right window. You can navigate throughout the document using the page select arrows inside the document viewer. Make sure the **Properties** tab is selected in the lower-left corner window.
  - What is the File Class of this file? _Regular File______
  - What is the File Size of this file? _109,159_____
  - What is the Physical Size of this file? __110,592_____

  The difference between Physical Size and File Size is due to File Slack.
  - What is the size of the File Slack? _____1433__
  - What is the Start Cluster? ___420,794____
  - When was this file last accessed? ___12/7/2006 6:41:32 PM____
  - What are the Unix permissions for this file? ___-rw-r-r--____
  - What is the UID and GID for the file? ___UID-501 and GID-501____
- Now select the **02 Bike Helmet Use.pdf.FileSlack** file.
  - What is the File Class of this file? ___File Stack____
  - What is the File Size and does it agree with your answer? _1,433-yes i agree with my answer_____
- Right-click on the **02 Bike Helmet Use.pdf.FileSlack** file and select **Export Files...** to export it to your directory or other location. Now, use word-processing software to open this file.
  - Is there any kind of real data in this file? __yes_____
  - What type of information is found in this file? (5 words)__APEX units for shutter speed_____
- Right-click the **jimshu** folder in the **Evidence Tree** and select **Export Files…** to export these files an empty work directory. You should have 431 folders and 1355 files successfully exported. Click **Close** in the Export Results dialog box. Click the **File** tab, and click **Exit** to close the FTK Imager application.
- Now, 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**.
- 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 **Specific Folder** option click the **...** button next to the right of the corresponsind text box, navigate to work folder that contains the folders exported earlier from FTK Imager, and click **OK**. Now, click **OK** in the Add Start Location dialog box followed by the **Next** button. 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).

- Click the **Search Index** button in the left pane, enter **Martha Dax** in the Enter Search Words text box, and then click the **Search** button.
- In the **Files** tab, find and double click the file titled **mbox** to view it in a new window. In the new window, select the **Text Viewer** tab to view the text from this file (actually, e-mail).
  - What competitive sensitive information regarding a new business venture is Martha Dax excited about? Manufacturing of Kayaks ________
- Close the new window (to get back to the Search Index results).
- Enter **iMac** in the Enter Search Words text box, and then click the **Search** button.
  - What type of iMac does Jim Shu have? iMac G3________
- Now, clear the Enter Search Words text box and click the **Search** button. . If needed, click **Yes** in the OSForensics – Notice dialog box to retrieve all results. In the **Files** tab, use the scroll bar to scroll down and search for and double click on the **AfterTheFlood512K.wmv** file to open it up in a new window.
  - Where (i.e., what park) is the location for this video? C:\Users\vs1135\Desktop\jimshu\.Trash\ ________
- Close the new window (to get back to the Search Index results).
- Close the E-mail Viewer window and then click the **Exit** button in the left pane to close the OSForensics program.

Using Forensic Tools to Examine an OS 9 Macintosh Image

The Macintosh OS 9 operating system is also known as Apple's "Classic" Mac OS. This operating system was introduced in 1999, and it lacked many of the modern features found in today's file systems, such as protected memory and preemptive multitasking. In 2002, Apple officially discontinued OS 9 and developed the current line of OS X operating systems. Forensics investigators may still encounter OS 9 images on older Apple computers still in use. Although the FTK does not directly support Macintosh file systems, investigators can extract potential evidence into FTK using FTK Imager. In this part of the lab, you will use the FTK Imager to extract the user account information contained in the OS 9 image files and search for potential evidence.

- 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 Item…** item.
- Select the **Image File** radio button in the Select Source dialog box, and click **Next**.

- Click the **Browse** button, navigate to the extracted OS9 folder, select the **GCFI-OS9.001** image file, and click **Open**. Click **Finish** in the Select File dialog box.
- In the upper-left Evidence Tree window, click the + symbols to expand the **GCFI-OS9.001**, the untitled **[2027MB]**, the **GCFI-OS9 DISK [HFS]**, and the **GCSI-OS9 DISK** folders to display the list of directories located in the OS 9 root. Examine the folder structure, and note the differences between OS 9, Windows, and even OS X.
- Click the **+** symbol to expand the **Documents** folder, and then click the **Documents** folder to view this user's documents. Now expand the **Mozilla**, the **Profiles**, the **default**, and finally the **d4p3o9zh.slt** folders. Select the **Cache** folder and find the file that contains a picture of an old-time bicycle. Make sure the **Properties** tab is selected in the lower-left corner window.
  - What is the name of this file? 2216E6AFd01 ________
  - What is the File Class of this file? Regular File ________
  - What is the exact File Size of this file? 57,342 ________
  - What is the exact Physical Size of this file? 65,536 ________

  The difference between Physical Size and File Size is due to File Slack.
  - What is the size of the File Slack? Confirm the size of File Slack by viewing the associated File Slack file. 8,194 ________
  - What is the Start Cluster? 1,012 ________
  - When was this file created? 1/21/2007 10:59:39 PM ________
  - What is the File Type of this file in HFS Information? TEXT [54455854] ________
  - Who is the File Creator for this file in HFS Information? MOZZ [4d4f5a5a] ________
- Right-click the **Documents** folder, select **Export Files…** to export these files to an empty work directory. You should have 21 folders and 92 files successfully exported. Click **Close** in the Export Results dialog box. Repeat this process to the same work directory for the **System Folder** folder and the **Trash** folder. Disregard any error messages, and close the error dialog boxes if they appear. Click the **File** tab, and click **Exit** to close the FTK Imager application.
- Now, 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**.
- 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 **Specific Folder** option click the **...** button next to the right of the corresponsind text box, navigate to work folder that contains the folders exported earlier from FTK Imager, and click **OK**. Now, click **OK** in the Add Start Location dialog box

followed by the **Next** button. 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).

- Click the **Search Index** button in the left pane, enter **Sebastian** in the Enter Search Words text box, and then click the **Search** button. If needed, click **Yes** in the OSForensics – Notice dialog box to retrieve all results.
  - How many files containing Sebastian were found in these exported folders?17_______
  - How many e-mails containing Sebastian were found in these exported folders?0______
- In the **Files** tab, find and double click the file titled **Re: Bicycle offer** to view it in a new window. In the new window, select the **Text Viewer** tab to view the text from this file (actually, e-mail).
  - Who is "delivering the goods"? Jim_______
  - How much is being offered for the plans? __$10,000_____
- Close the new window (to get back to the Search Index results).
- Select the **Emails** tab, find one of the e-mails with the subject **Re: Free tools** by scrolling down on the scroll bar, and double click on the e-mail to view it (and other e-mails) in the E-mail Viewer.
  - Search through the various e-mails with this subject to find the link to a web site that has freeware for his Mac? What is the link for the web site?

    http://www.pure-mac.com/database.html _______
- In the E-mail Viewer, find the e-mail from Martha Dax regarding budget constraints.
  - What is Martha Dax's role at Superior Bicycles? _CEO______
  - What percent reductions are being made to the annual budget plans? _10%______
- Close the E-mail Viewer window and then click the **Exit** button in the left pane to close the OSForensics program.

You are to submit this document with your answers through the **Lab 04** dropbox on Canvas by the due date and time.