Lab 4

Imaging Evidence with FTK Imager

FTK Imager creates a bit stream image in raw(.dd), Smart (.s01) and .E01 format and allows an investigator to extract registry files from a Windows computer and import them into a registry viewer fir recovering passwords and encrypted files.

FTK is not good for searching large volumes of data but it has verification features such MD5 or SHA-1 hashing calculations. The hashes can be used to show files have not been altered during imaging. It can also be used to extract files without booting the suspect's computer.

In this lab, we will delete 2 files from the EVIDENCE drive created earlier and image the drive using FTK to create an .E01 image.

Activity

1. Access the USB drive; delete the Qtr 1 Emp.xls and Online.docx files on the USB drive, and exit Explorer.
2. Open FTK Imager. Click **Yes** in the UAC message box. Click File, Create Disk Image from the menu.
3. In the Select Source dialog box, click Logical Drive option button and then click **Next**.
4. In the Select Drive dialog box, click the **EVIDENCE[NTFS]** source drive in the drop down list box and click **Finish**.
5. In the Create Image dialog box, click **Add**. In the Select Image Type dialog box, click the E01 option button and then click **Next** to continue.
6. In the Evidence Information dialog box, type **C2Proj4** in the Case Number and Evidence Number text boxes. Enter your full name in the Examiners box and type **USB image with deleted files** in the Notes text box. Click **Next** to continue.
7. In the Select Image Destination box, click Browse button and find the **Work\Labs\Evidence folder**, click **OK** and type **C2Proj4** in the Image Filename text box. Click **Finish**.
8. In the Create Image text box click **Start**. When processing finished, the results are displayed along with the MD5 and SHA-1 hashes which verify integrity. Close out of all dialog boxes that are open. The file created (C2Proj4.E01) will be used in the next lab.

Lab 5

Viewing Images using FTK Imager

FTK can be used to generate hash values, viewing file formats and to search for missing or deleted files on a disk image. The data can be viewed in its readable state as well as hexadecimal bytes written to the disk. FTK displays physical and logical blocks, including bad and unallocated blocks that can be helpful in recovering deliberately corrupted disk partitions. It also helps to figure out quickly if data has been deleted from a disk image.

In this lab, you will be able to view images for preliminary analysis, locate deleted files, and export tem for further analysis. We will use the USB image created in Lab 4

Activity

1. Open **FTK Imager** and click **File, Add Evidence Item** from the menu
2. Select Source dialog box, click the **Image File** option button and then click **Next**
3. In the Select Source dialog box, click **browse** and go to the **Work\Labs\Evidence folder**, click the **C2Proj4.E01** file and then click **Open**. Click **Finish**.
4. In the Evidence Tree Pane, expand the **C2Proj4.E01, EVIDENCE [NTFS],** and **[root]** folders and then click the [root] folder to view the files on the image drive. Notice the deleted Qtr 1 Emp.xls and Online.docx files show a red X in the File List pane. FTK was able to recover these deleted files from the USB drive even though they were not visible in File Explorer.
5. In the File List pane, Ctrl+click the **Qtr 1 Emp.xls** and **Online.docx** deleted. Right click the **Online.docx file** and click **Export Files**.
6. In the Browse for Folder dialog box navigate to and click the **Work\Lab\Evidence folder**, click **OK** to export the files and then click **OK** in the Export results dialog box.
7. In the File List pane, Ctrl+click the **Qtr 1 Emp.xls** and **Online.docx** deleted files. Right click on **online.docx** and click **Export File hash List**.
8. In the Save as dialog box, type **C2Proj4 deleted file hashes** in the File name text box and click **Save**.

Some Questions

In File Explorer, navigate to and click the WORK\Labs\Evidence folder. Find and double-click the exported **C2Proj4 deleted file hashes.csv** file to open it in Excel. Review the Excel spreadsheet listing the two deleted files and their MD5 and SHA-1 hashes. Expand the columns, if needed, to view the full hash values and exit Excel.

In File Explorer, locate the C2Proj2.dd and C2Proj2.eve images. Notice that the image size is about the same for each image type. Now look at the C2Proj4.E01 image and notice that it is much smaller. FTK creates a compressed image yet preserves the evidence.

Close any open Windows.