Lab 01 Project (Chapter 3)

Data Acquisition

Due: 11:59 PM on Monday, September 19, 2022

**Data Acquisition in ProDiscover**

During the process of seizing a storage device, investigators use imaging tools to create a forensic copy that can safely be analyzed without the danger of damaging or deleting potential evidence. The forensic copy is an exact copy of the original evidence, including an unallocated space or bad clusters. In addition, the imaging process creates a hash signature of the original and the duplicated copy to validate the scientific imaging process and ensure that no file has been omitted or changed in any way. The two hash signatures are compared with each other, and if they match, the copy is considered legally identical to the original. The forensic copy maintains the chain of custody from the time the seized device was imaged until the end of the investigation. In addition, the information obtained by the various tools applied to the evidence will be listed in a report that can be examined during the trial by investigators and court personnel.

In this lab, you will add an image of a storage device into ProDiscover Basic.

1. Start **ProDiscover Basic** on your workstation.
2. If the Launch Dialog box appears, type **C3Lab1** 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 **C3Lab1** into the boxes as above for the New Project dialog box.
3. Click the **Action** tab and click **Add**; then in the submenu, click **Image File**.
4. In the Open dialog box, browse to the location of the **C3Proj1.dd** file, click the file, and select **Open**.
5. Expand the **Images** icon located under the **Content View** by clicking on the + symbol, and click the **C3Proj1.dd** image icon.
6. Note that the files displayed in the upper-right window represent the root directory listing of the imaged storage device. Click the + symbol to expand the Image file, and see the folder below containing all the files on the device.
7. Deleted files are represented by a red X in the icon next to the check box. Click the first three deleted files, and view the text along with the formatting structure in the lower-right window. The first deleted file is an MS Word document, and the second file is an MS Excel file. The last deleted file is a .jpg image file, and it must be viewed using a graphic image viewer.
8. Click the check box next to the first deleted file, type **Deleted file** in the Add Comment dialog box, and click **OK**. Repeat this process for the other two deleted files. You should see check marks next to each of the files.
9. Click the **Tools** tab, and select **Batch Calculate Hashing**. Click **Yes** in the ProDiscover dialog box to disregard the notification. Wait a couple minutes before proceeding.
10. Click the **View** tab, and click **Gallery View** to display the graphic images.
11. Click the **Report** icon to display the results of your initial investigation of this evidence.
    1. What is the file system used in this image? \_\_\_\_\_\_\_\_\_\_
    2. What is the time zone where this image was located? \_\_\_\_\_\_\_\_\_\_
    3. What is the total number of clusters contained in this image? \_\_\_\_\_\_\_\_\_\_
    4. How many hidden sectors are contained in this image? \_\_\_\_\_\_\_\_\_\_
    5. On what date were the three files deleted? \_\_\_\_\_\_\_\_\_\_
12. Click the **File** tab and select **Exit**. Click **No** in the ProDiscover dialog box to close ProDiscover.

**Viewing an NTFS Image in ProDiscover**

The New Technology File System (NTFS) was first available in Windows NT, and it is supported in Windows 2000, XP, Vista, 7, and so on. NTFS is the file system of choice because it supports additional file attributes such as encryption using the Encrypting File System (EFS) and compression at both the file and folder levels. In addition, it incorporates two copies of the master file table for fault tolerance. Further, when used with current versions of Windows, NTFS supports granular file permissions based on the ownership of the file, or who created it. The NTFS file system structure is more complex compared with FAT16 or FAT32, and the file attributes are particularly usable when viewed in forensic software because each file has its own associated permissions allowing investigators to see the username account that last modified each file or folder. In this lab, you will add the C3Proj2.dd image to ProDiscover to view the additional NTFS file system attributes.

1. Start **ProDiscover Basic** on your workstation.
2. If the Launch Dialog box appears, type **C3Lab2** into the Project Number and Project File Name boxes in the New Project tab. Enter **NTFS USB Device Image** in the Description area, and click **OK**. Otherwise, click the **File** tab and click **New Project** and enter the applicable data into the boxes as above for the New Project dialog box.
3. Click the **Action** tab and click **Add**; then in the submenu, click **Image File**.
4. In the Open dialog box, browse to the location of the **C3Proj2.dd** file, click the file, and select **Open**.
5. Expand the **Images** icon located under **Content View**, and click the **C3Proj2.dd** image icon.
6. Note the files displayed in the root directory listing contain a different file system structure compare with the FAT32 image analyzed in the previous lab exercise. Drag the bottom of the window down to view all the files listed at the bottom of the root directory. Notice that the deleted files are not listed in the root directory; only the remaining files are displayed. The two files listed in red support additional NTFS features. The $BadClus:$Bad file maintains a list of bad clusters encountered by the file system, and the $Secure:$SDS file contains the security attributes for EFS encryption. These are not supported in FAT16 or FAT32 file systems. Check the + symbol next to the image icon to expand it, and view the contents of the image.
7. Click the **Deleted Files** icon to display the deleted files located on this storage device.
8. Click the check box next to the first deleted file, and type **Deleted file** in the Add Comments dialog box. Click **OK**. Repeat this process for the other two deleted files.
9. Click the **$Extend** folder to display the folder structure that contains the NTFS permissions applied to parent and child files and folders. NTFS supports additional storage volume attributes that include compression, encryption, and support for disk quotas. These folders maintain the access control list and permissions available in NTFS-formatted partitions. FAT16 and FAT32 do not support these features, and their corresponding file system structures are much simpler in design.
10. Click the **Tools** tab, and click **Batch Calculate Hashing**. Click **Yes** in the ProDiscover dialog box to disregard the notification.
11. Click the **C3Proj2.dd image** icon. Click the **View** tab, and click **Gallery View** to display the graphic images.
12. Expand the + symbol next to the **Images** icon under the Cluster View, and click the **C3Proj2.dd** image icon to view the disk clusters and hex data representing the raw image displayed in the upper and lower windows, respectively. Note the NTFS file system signature listed in the lower window.
13. Click the **Report** icon to display the results of the investigation of this evidence.

f. What is the total number of clusters contained in this image? \_\_\_\_\_\_\_\_\_\_

g. What is the total size of this storage device in kilobytes? \_\_\_\_\_\_\_\_\_\_

h. How many clusters did deleted MS Word document occupy in image? \_\_\_\_\_\_\_\_\_\_

i. What time was the bank.jpg file deleted? \_\_\_\_\_\_\_\_\_\_

j. How many sectors are contained in each cluster? \_\_\_\_\_\_\_\_\_\_

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

**Viewing a FAT32 Image in FTK Imager**

Although the primary purpose of FTK Imager is to be able to duplicate digital evidence by using a bit-stream process called “imaging”, FTK Imager can also be used to preview digital files to determine whether evidentiary data exists before starting an extensive investigation. If potential forensic data is located, FTK Imager can then forensically duplicate the storage device to process the data safely. FTK Imager supports the following file systems: Microsoft FAT12, FAT16, FAT32, and NTFS; Linux/UNIX Ext2, Ext3, and Ext4; Mac HFS and HFS+. In this lab, you will add the C3Proj1.dd file to FTK Imager and perform a preliminary analysis of the imaged evidence.

1. Start **FTK Imager** 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. 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. Click the **Browse** button, navigate to the folder containing the C3Proj1.dd image file, select the **C3Proj1.dd** image file, and click **Open**. Click **Finish** in the Select File dialog box.
4. In the upper-left Evidence Tree window, click the + symbols to expand the **C3Proj1.dd** and **USBDEVICE [FAT32]** folders to display the list of directories in this device. Examine the **[unallocated space]** folder.

k. How many files of unallocated space are found in the folder? \_\_\_\_\_\_\_\_\_\_

l. Which file contains a picture of a large building (i.e., a bank)? \_\_\_\_\_\_\_\_\_\_

m. Locate the **000174** file and then select the **TEXT Eyeglass** icon on the tool bar in FTK Imager to view unformatted text found in this file. Who is this document addressed to (full name)? \_\_\_\_\_\_\_\_\_\_

1. Now examine the **[root]** folder.

n. Deleted files are shown with a red (or similar) X through the icon for the file type. How many deleted files are found in this folder? \_\_\_\_\_\_\_\_\_\_

o. What is the name of the web site that sells safes like the interior safe found at this bank? \_\_\_\_\_\_\_\_\_\_

p. What is the name of the street that the back door of the bank faces? \_\_\_\_\_\_\_\_\_\_

q. Right-click the **First Union Large Deposits** Excel file and select **Export Files…**. In the Browse For Folder dialog box, navigate to your working directory and click **OK** to export this file to that directory. Use MS Excel to open this file. What is the total amount of cash deposits made during the week ending June 15, 2009? \_\_\_\_\_\_\_\_\_\_

1. Click the **File** tab, and click **Exit** to close the FTK Imager application.

You are to submit this document, with your solutions, to the **Lab 1**dropbox on Canvas by the due date and time.