DATA ACQUISITION – Gathering of Evidence using FTK

Theory

In computer forensics, **data acquisition** is the task of collecting digital evidence from electronic media. A common method of collecting evidence is to acquire an image file of the suspect disk drive. An image file is a bit-stream copy *(i.e. disk-to-image file or exact duplicate)* of source files. Hence, a number of tools are available to Forensics Investigations to help them in the process of gathering of evidence.
Most imaging tools have a counterpart application that is able to read or examine files once they have been gathered using the imager. (e.g. FTK Image Files can be opened/examined using AccessData's Forensic Toolkit)

Objective

This lab will use **FTK imager** to create an image file of an entire USB flash drive (memory stick);

Tools/Software

- ✓ FTKImager software

Lab Activities

A) Pre-Tasks:

- *Install both FTK Imager on your machine or on the virtual machineif you do not have admin rights*
- *Create a Forensic folder in C drive (C:\Forensic)*
- *Have a USB flash drive handy*

B) Capturing an Image with FTK Imager

1. Start FTK Imager by navigating to Start**/All Programs/AccessData/FTK Imager/FTK Imager**
2. Insert a USB flash drive into a USB port ***(NOTE: making a bit-stream image of a thumb drive could take a long time, depending on the size of the thumb drive (memory stick))***
3. In FTK Image main window, click on **File,** and then choose **Create Disk Image** from the drop-down menu.
4. In the Select Source dialog box, select **Physical Drive** option button and then click **Next**.
5. When the Select Drive dialog box appears, click on the dropdown menu and select your USB flash drive, and then click **Finish**. ***(NOTE: do not select the "C:\" drive)***
6. When the Create Image dialog box appears, click on the **Add** button.
   Ensure that the check box for **"Verify images after they are created"** is checked.
7. When the Select Image Type dialog box appears, select **AFF (in this case SMART)** and click **Next**.
8. Fill in the Evidence Item Information; Case number ***= Lab 4***, Evidence Number = ***4.1***…
9. When the Image Destination folder appears, click the "Browse" button, navigate to "C:\Forensic" and then click "**OK**". **Create the folder if it does not exist!**
10. In the Image Filename field, type "**FTKimage**" and then click "**Finish**"
11. When the Create Image dialog box appears again, click "**Start"** and wait for the image to finish.

How long did your image copy take? What do you attribute this to?

12. After the image file has been created successfully, click the "**Close**" button

13. Open Windows Explorer and navigate to **C:\Forensic**

14. Confirm that the following three or more files have been created:

    a. *FTKimage (zip archive)*
    b. *FTKimage.001.txt (text file)*
    c. *FTKimage.002*

15. Open the **FTKimage.001.txt** file in Notepad.

    What information is contained here and how is this information relevant to computer forensic investigations?

16. You now have an FTK Image file that can be opened and examined using AccessData's Forensic Toolkit (FTK). ***Note: FTK Toolkit is a separate software tool***.

>>>>> End of Lab Exercise <<<<<