Lab 3 – File System Forensics

Sai Sasaank Srivatsa Pallerla

University of Maryland, Baltimore County

Presented to: Gina Scaldaferri

Date: 10/01/2019

Introduction

This lab is the continuation of Lab-2, where we made an image of an evidence using FTK-Imager. FTH-Imager, also known as Forensics Toolkit Imager, is used to make an image of hard disks, USB sticks, CDs and store in one file future reference. It can also be used to recover deleted file and scan the image for strings to make sense/ search the evidence. One other tool used for the same purpose is ProDiscover. Like FTL Imager, ProDiscover can used to mage images of external/ internal storage and analyze the image at sector level without altering the meta data. It can also be used to recover deleted files examine slack space and alternate data streams.

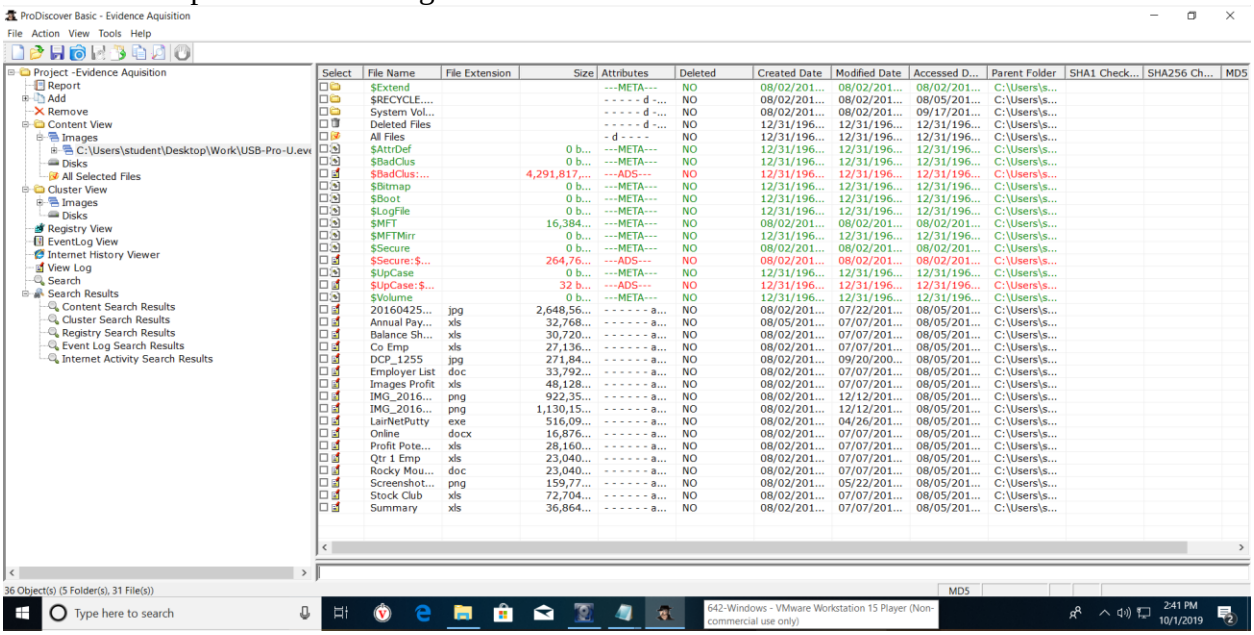
In this lab we will examine the image made in Lab-2 to check if it contains any files, deleted items and check if the deleted files can be restored and finally check the hash, to be same, to make sure the image was not altered in any manner.

Part 1

1. What is the hash of the image?

   MD5 of the image is: `2eb638cfa987fd5a0c18841f2f167573`

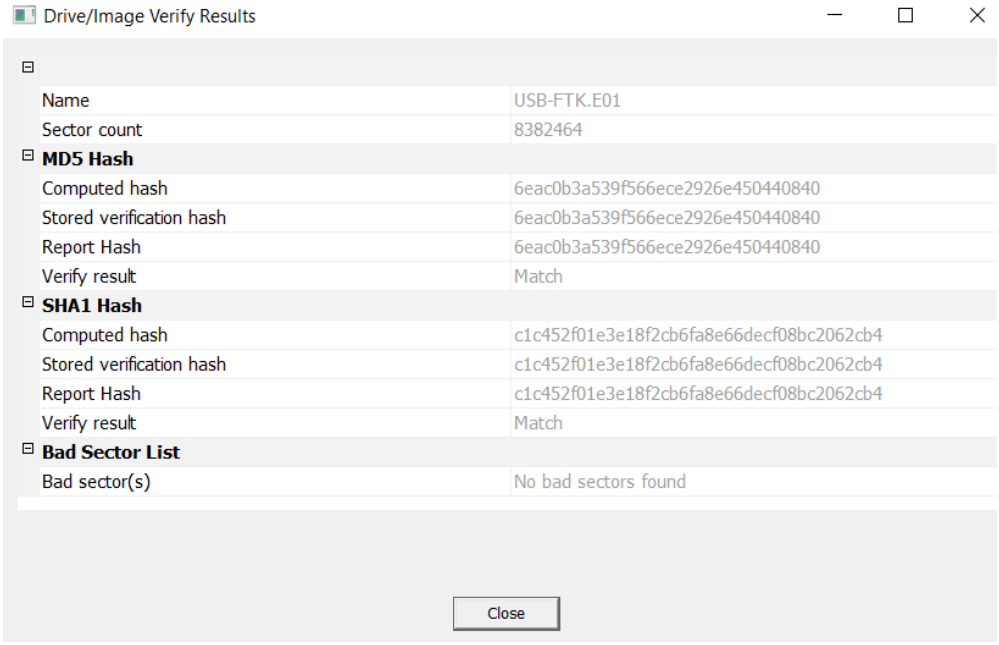
2. What files are present in the image?



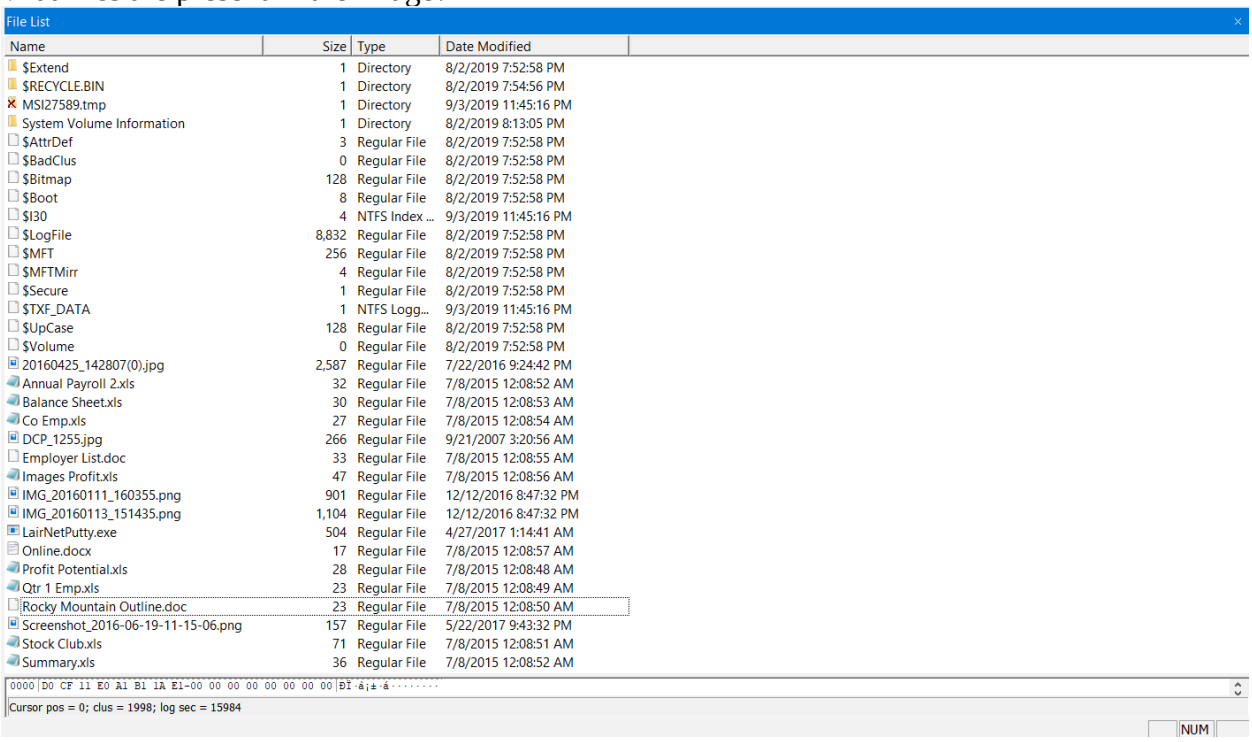
Part 2

1. What is the hash of the image?

   MD5 of the image is: 6eac0b3a539f566ece2926e450440840



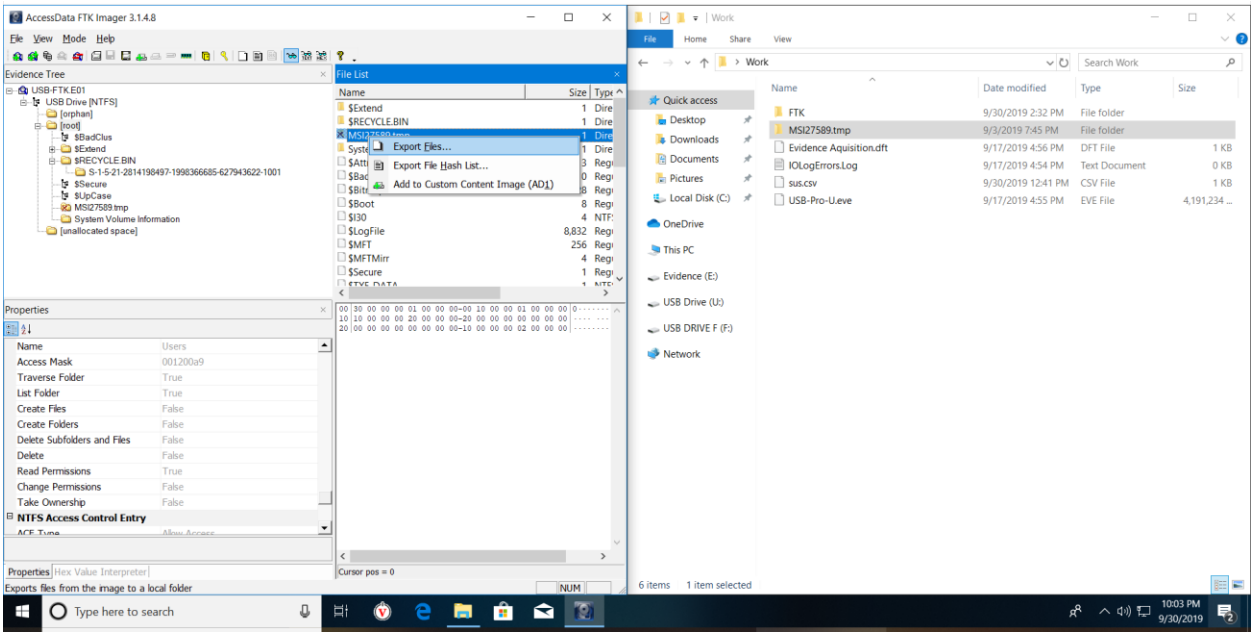
2. What files are present in the image?



3. Do you see any files that show a red X? If so, can you recover them?

Yes, MS127589.tmp

To recover this file, we simply need to right click on it and export the file at desired location.

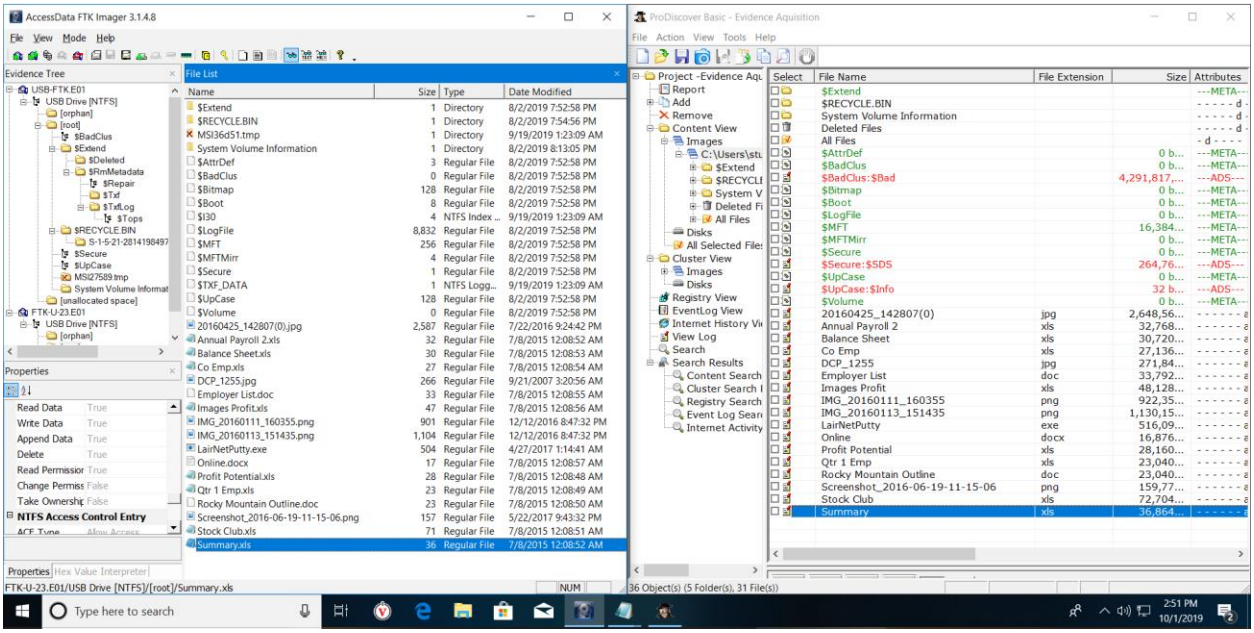


Zone Identifiers: It is generated by applications when user saves files to the local file system from a different security zone. There are 5 most commonly-encountered zone identifiers:

- 0 – Local Machine Zone, the most trusted zone for content that exists on the local computer;
- 1 – Local Intranet Zone, for content located on an organization's intranet;
- 2 – Trusted Sites Zone, for content located on Web sites that are considered more reputable or trustworthy than other sites on the Internet.
- 3 – Internet Zone, for Web sites on the Internet that do not belong to another zone;
- 4 – Restricted Sites Zone, for Web sites that contain potentially-unsafe content.

Part 3

1. Are the file system contents of each image the same?



2. Are there any files missing from an image?

   There is no difference in the files that were recovered from the USB stick, however we can notice three additional files in FTK Imager which are as follows:

   - $l30, which is an NTSF file
   - $TXF_DATA, which is also a NTSF file

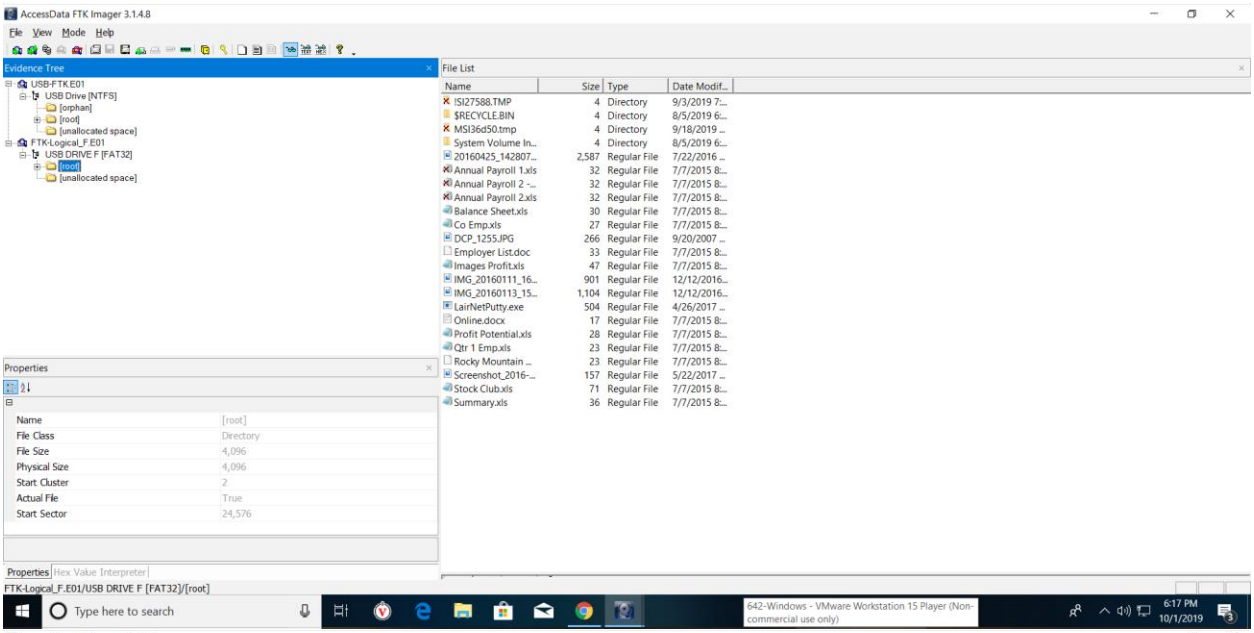
   And one additional directory that we can see in ProDiscover is ‘DeletedFiles’ which contains a folder MSI27589.tmp, it’s a temporary folder, but again FTK Imager also has this folder.

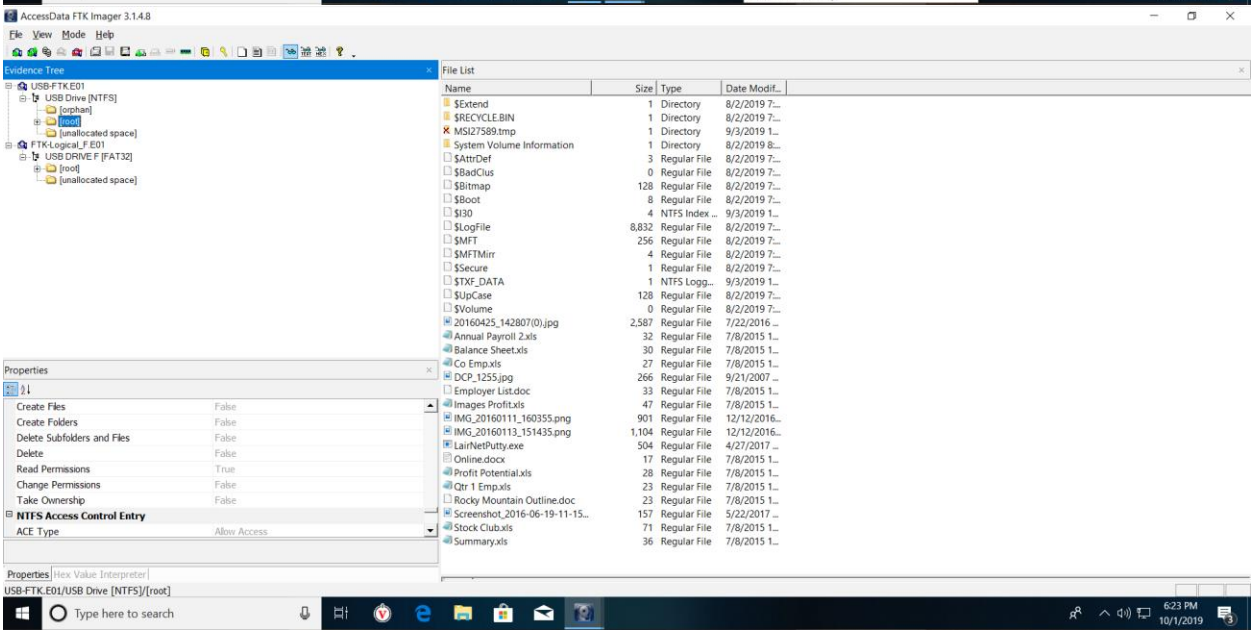
3. Which tool would you prefer to use as your main tool, and why? (There is no right or wrong answer)

   I would use FTK Imager as my main tool because it is an industry standard and, I faced many issues while using ProDiscover. The amount of information that is get out of FTK imager is more and I feel FTK Imagers interface is more convenient when compared to ProDiscover.

4. Did you notice any differences between the images of the two USB drives (F: and U:)? If so, what differences?

   The very noticeable difference between F and U drive is the number of files. We do not see files that start with '$' in F drive and we see three additional files with an 'X' mark (by the name 'Annual Payroll 1','Annual Payroll 2-copy' and 'Annual Payroll 2' which were probably deleted.





Conclusion

From this lab we can learn how to examine the image, i.e., traverse through the files recovered by the tool, recover deleted files, information about zone identifiers related to the files. Essentially, we got to explore two Evidence Acquisition Forensic Toolkit applications and the potential impact a forensic tool can make on an investigation, in the sense, if the tool can provide you with more information it might help in deducing critical situations (also the investigators comfort level with a tool).