CIS4385
Assignment 2
Forensic Imaging

***Learning Objective**: Creating Forensic Images, properly utilizing forensic imaging software, and capturing memory.*

***Narrative**: Creating forensic image files is at the heart of doing digital forensic examinations. It is often the first step of the examination process, and the most important to get right. For this exercise, we will be using a USB thumb drive (recommended size between 2GB and 8GB but any size will work) as our evidence item.*

Setup

1. Install the provided forensic imaging program FTK Imager (in the **tools** folder) on your Windows computer.

2. Copy the **Target1** folder onto your thumb drive.
    a. The thumb drive need not be brand new or empty for this exercise.
    b. Copy the folder onto the root of your thumb drive.

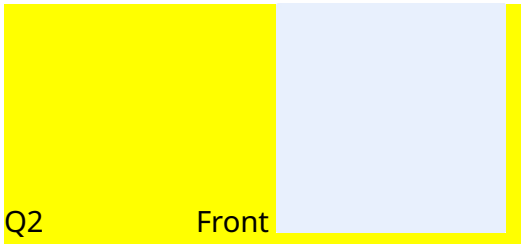
3. Eject the thumb drive – this is now your evidence.

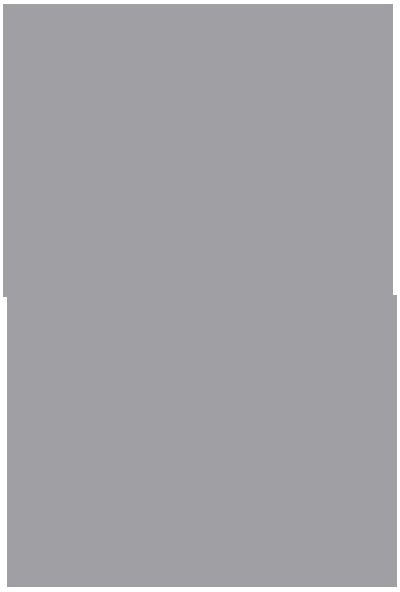
Creating Forensic Images

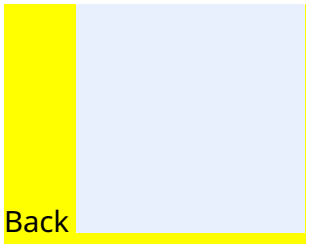
1. Before we proceed with the imaging, we need to do some documentation of our evidence. Provide the following information, if available.
    a. Make, Model, serial number, and size of the thumb drive as printed or marked on the device. (Note, serial number is not always printed on the thumb drive)

Q1 A Samsung FIT 128g Flashdrive Partitioned with instructor permission to 8gb.

b. Digital photographs of the thumb drive should be recorded. Photographs should include all visible markings on the thumb drive, front and back.

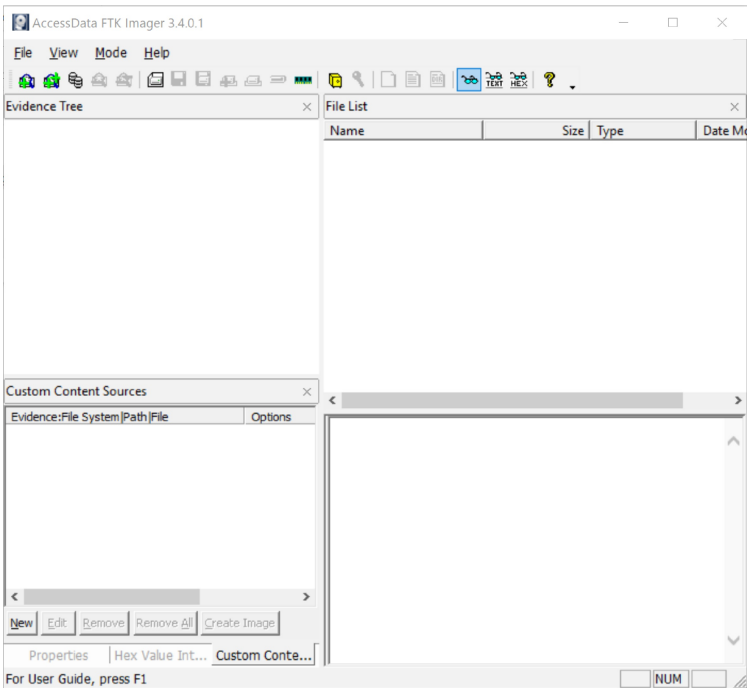






2. Plug in the USB Drive (for the purposes of this lab we will not worry about Write Blocking – more about this in a later class)

3. Run the program FTK Imager



4. Review the tool guide for FTK Imager

5. Create a forensic image with the following parameters:
    a. E01 format
    b. No fragmentation (set to 0)
    c. No compression (set to 0)
    d. File name: USB1

6. Answer the following questions about the imaging process:
    a. How many sectors are on the device?

    Q3 16,117,760

b. What is the MD5 hash value of the device?

Q4 6b8d9eaa44f48f55976fc010d5bd6db5

c. How long did the acquisition take?

Q5 1 minute and 1 second

d. How big is the image file that was created?

Q6 The same size as the drive, so roughly 7.68bg

7. Create another forensic image of the same device with the following parameters:
   a. E01 format
   b. No fragmentation (set to 0)
   c. Max compression (set to 9)
   d. File name: USB2

8. Answer the following questions about the imaging process:
   a. How many sectors are on the device?

Q7 16,117,760

   b. What is the MD5 hash value of the device?

Q8 4fc08abffc5a9ecda7690c0118c14200

   c. How long did the acquisition take?

Q9 52 seconds, compression took another 24 seconds

d. How big is the image file that was created?

Q10 62.2 MB

9. What effect does compression have on the MD5 hash value of the data contained in the forensic image?

Q11 It is a very different hash value, it is also substantially shorter than the one created prior not using compression.

10. What is the size difference between the image files created with no compression and max compression? (*USB1.E01* versus *USB2.E01*)

Q12 7.67 GB

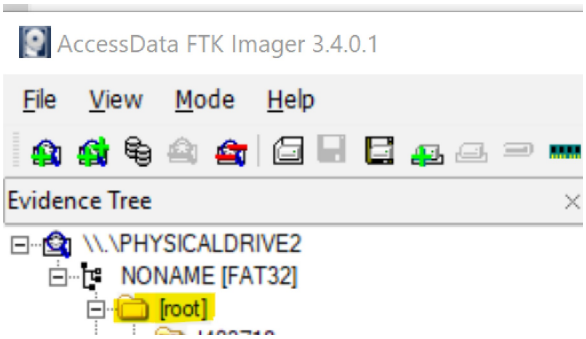
Examine Physical Drives with FTK Imager

1. Close FTK Imager, eject the thumb drive.

2. Re-insert the thumb drive and deleted the **Target1** folder.

3. Start FTK Imager again and add the thumb drive as an evidence item.

4. Using the Tree pane, navigate to the root of the thumb drive.



5. What do you notice about the “deleted” folders/files?

Q13 Within the deleted folder all of the hex values for the files are all 0. Which would make sense given that a deleted file should contain no data.

Creating Forensic Images – Part 2

1. Copy the **Target2** folder onto your thumb drive.
    a. The thumb drive need not be brand new or empty for this exercise.
    b. Copy the folder onto the root of your thumb drive.

2. Eject the thumb drive – this is now your evidence.
3. Create a forensic image with the following parameters:
    a. E01 format
    b. No fragmentation (set to 0)
    c. Compression (set to 6)
    d. File name: USB3

4. Answer the following questions about the imaging process:
    a. How many sectors are on the device?

    Q14 16,117, 760

    b. What is the MD5 hash value of the device?

    Q15 81741ad679a4d977ddbe65b92d14dba8

    c. How long did the acquisition take?

    Q16 51 seconds

    d. How big is the image file that was created?

    Q17 318 MB

Mounting Forensic Images

1. Remove all evidence items from FTK Imager.

2. Add the forensic image file provided. (USB5.E01)

3. Using the Image Mounting feature in FTK Imager, mount the forensic image as an emulated drive.
    a. What drive letter was your virtual/emulated drive assigned?

    Q18 F:

4. Using whichever anti-virus program you have installed, run a virus scan on the mounted drive.
    a. Which file was identified as malware?

    Q19 EICAR Test-NOT virus!!!

Capturing RAM

1. Unmount any mounted images and remove any evidence items from within FTK Imager.

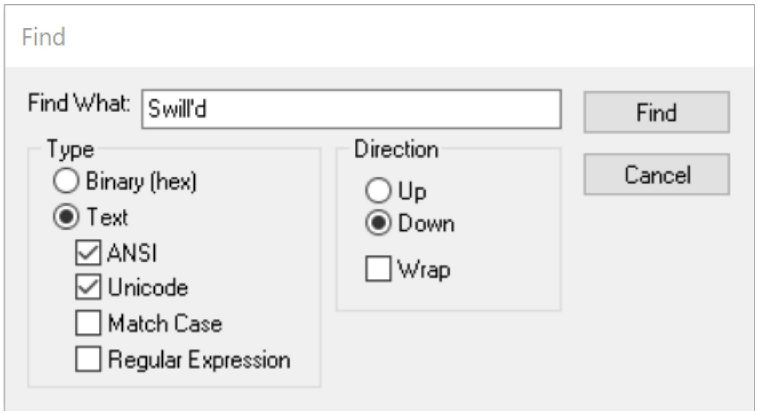
2. Locate and open the file *HenryV.txt* and leave it open. It should open in notepad, or a similar program.

3. Use the capture memory function in FTK Imager to create a RAM dump into a folder on your desktop.
    a. Keep in mind, the size of this file will be the size of your entire RAM, make sure you have enough room.

b. The default file extension is ".mem"

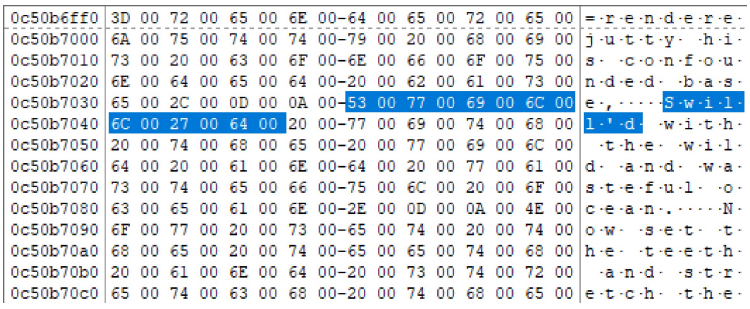
4. Once complete, open the file as though it were an Image file.

5. Using the Find command (ctrl-F or right click on the Data pane and select Find), search for the term "Swill'd" (obviously without the quotation marks)



6. Were you able to find this unique word in the memory dump? Provide a screenshot of the term highlighted.

Q20



7. Is the entire speech intact in the memory dump?

Q21 Yes, It was able to find information within the text file.

Additional requirements

In addition to this document filled out completely, you must also submit the log text files from the imaging process. They can be found in the same location as your forensic image files. They will be called, for example “USB1.E01.txt” and should only be about 2KB in size. Submit all three of these text files.