PIVOT Lab - Forensic Image Extraction

(portions of this lab are made available via sharing with CyFor Modules, NYU Polytechnic School of Engineering)

Part 1= how to image a drive

Part 2 = extracting evidence from a drive image

What is it?

A *forensic image* is an electronic copy of a drive (e.g. a hard drive, USB, etc.). It's a bit-by-bit or bitstream file that's an exact, unaltered copy of the media being duplicated.

How is it done?

Wikipedia said that the most straightforward disk imaging method is to read a disk from start to finish and write the data to a forensics image format. "This can be a time-consuming process, especially for disks with a large capacity," Wikipedia said.

To prevent write access to the disk, you can use a write blocker. It's also common to calculate a cryptographic hash of the entire disk when imaging it. "Commonly-used cryptographic hashes are MD5, SHA1 and/or SHA256," said Wikipedia. "By recalculating the integrity hash at a later time, one can determine if the data in the disk image has been changed. This by itself provides no protection against intentional tampering, but it can indicate that the data was altered, e.g. due to corruption."

Why image a disk?

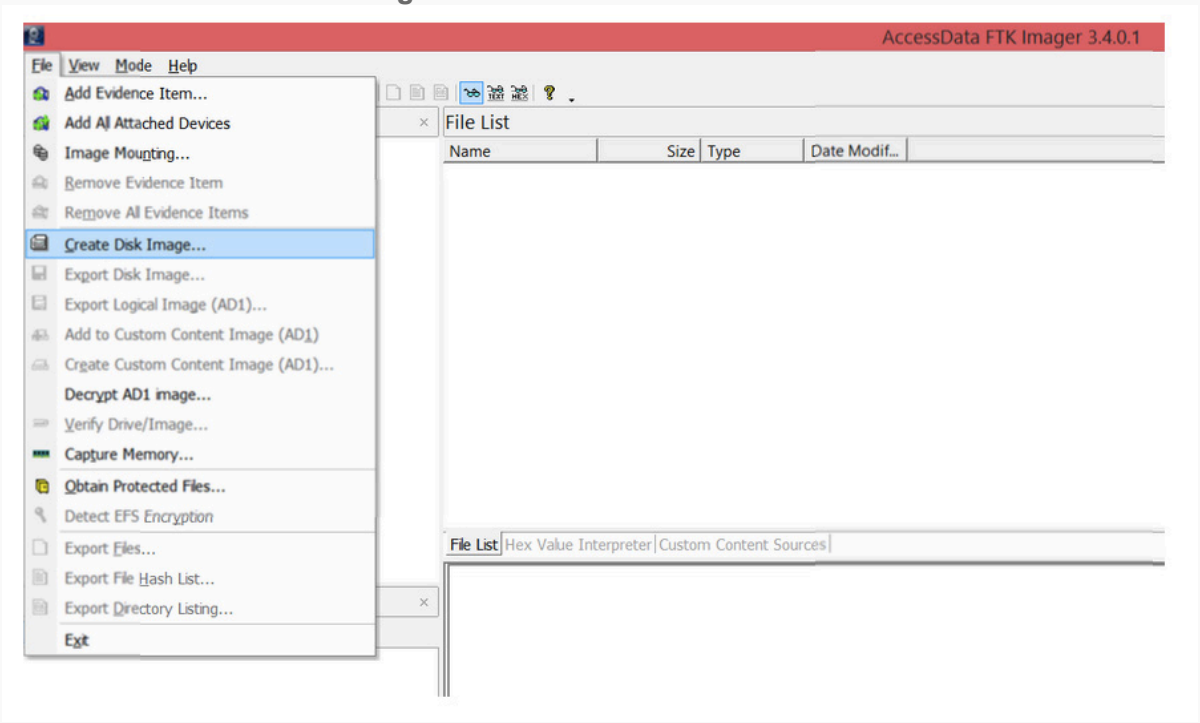
There are two reasons for Forensic imaging:

- Prevents tampering with the original data evidence
- Allows you to play around with the copy, without worrying about messing up the original

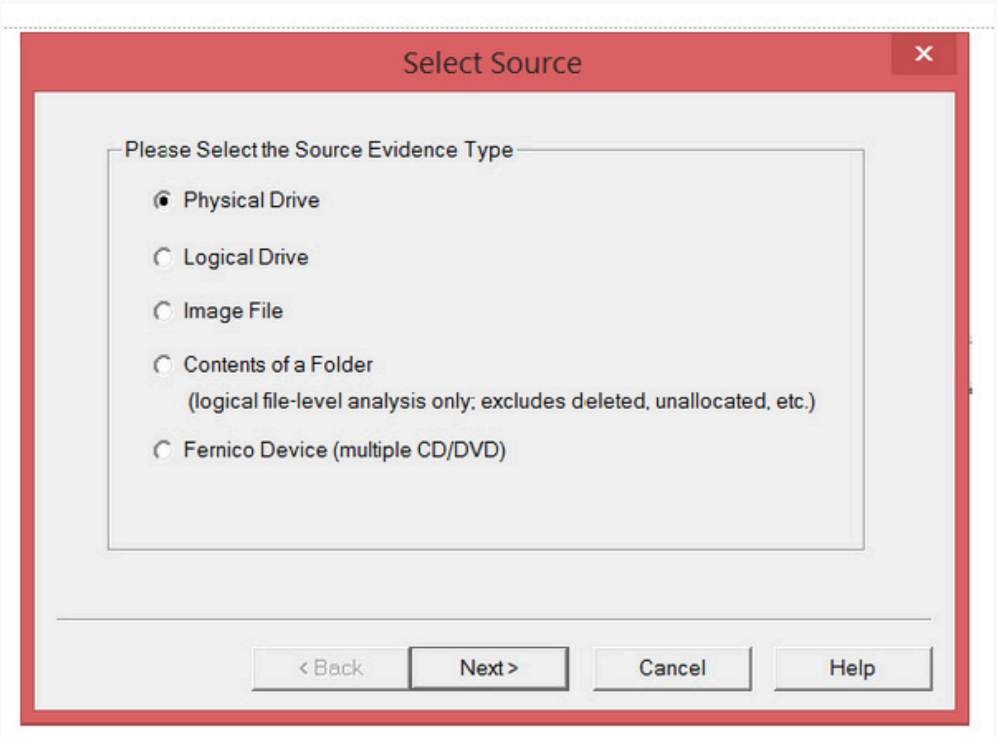
Part 1= how to image a drive

Find a USB drive and follow along with these instructions to image it. For your imaging tool, download AccessData FTK Imager. ! ! Recommend the smallest USB drive you can find - 128 MB is optimal.

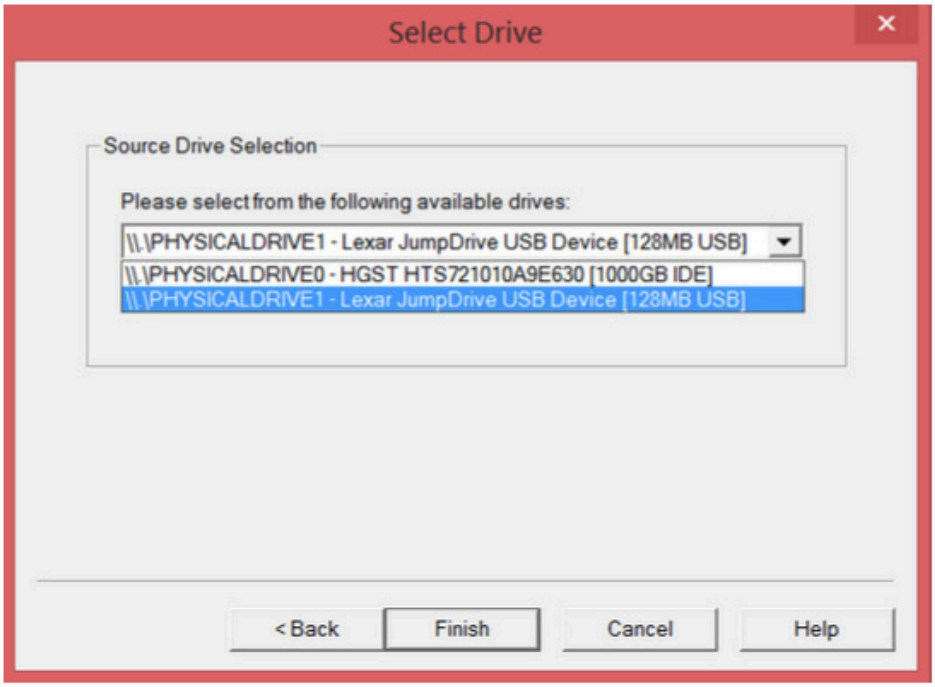
Step 1: Go to **File > Create Disk Image**.



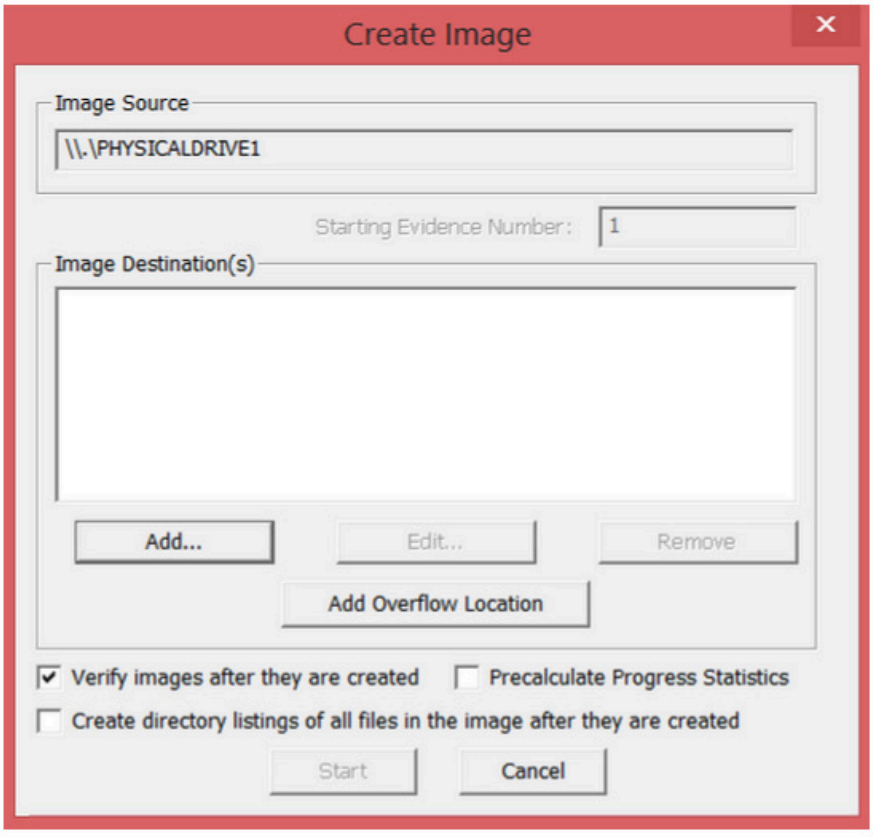
Step 2: Select **Physical Drive**, because the USB or hard drive you're imaging is a physical device or drive.



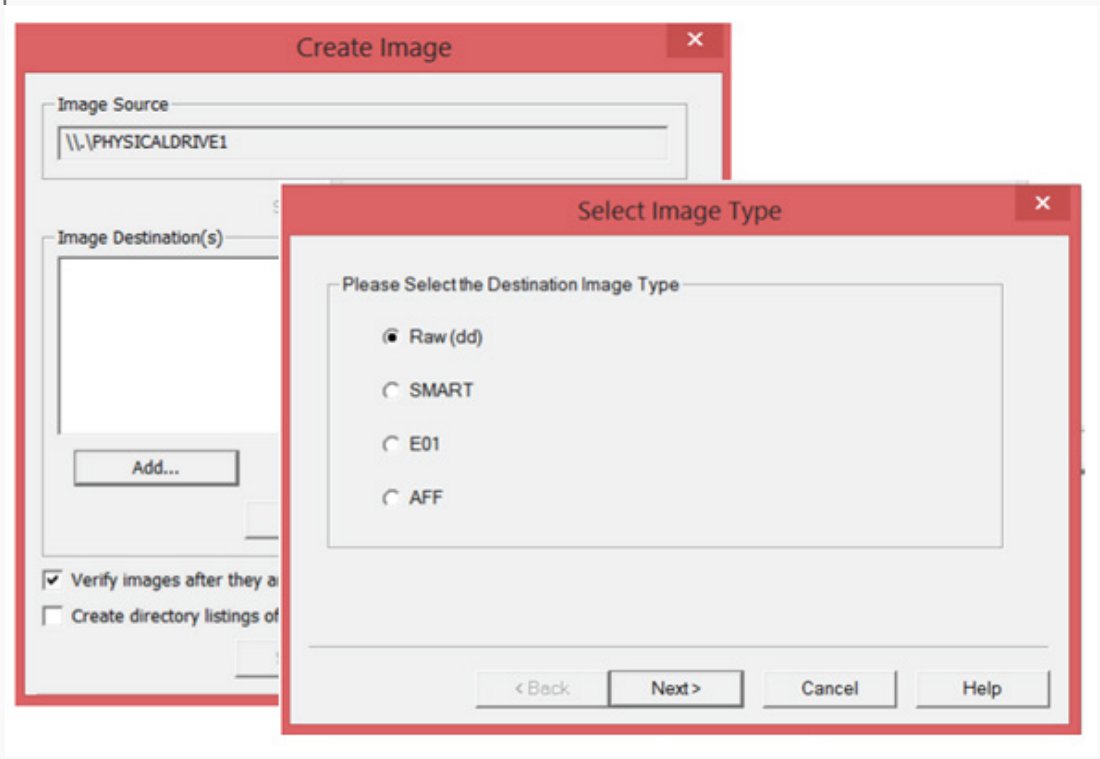
Step 3: Select the drive you're imaging. The 1000 GB is my computer hard drive; the 128 MB is the USB that I want to image.



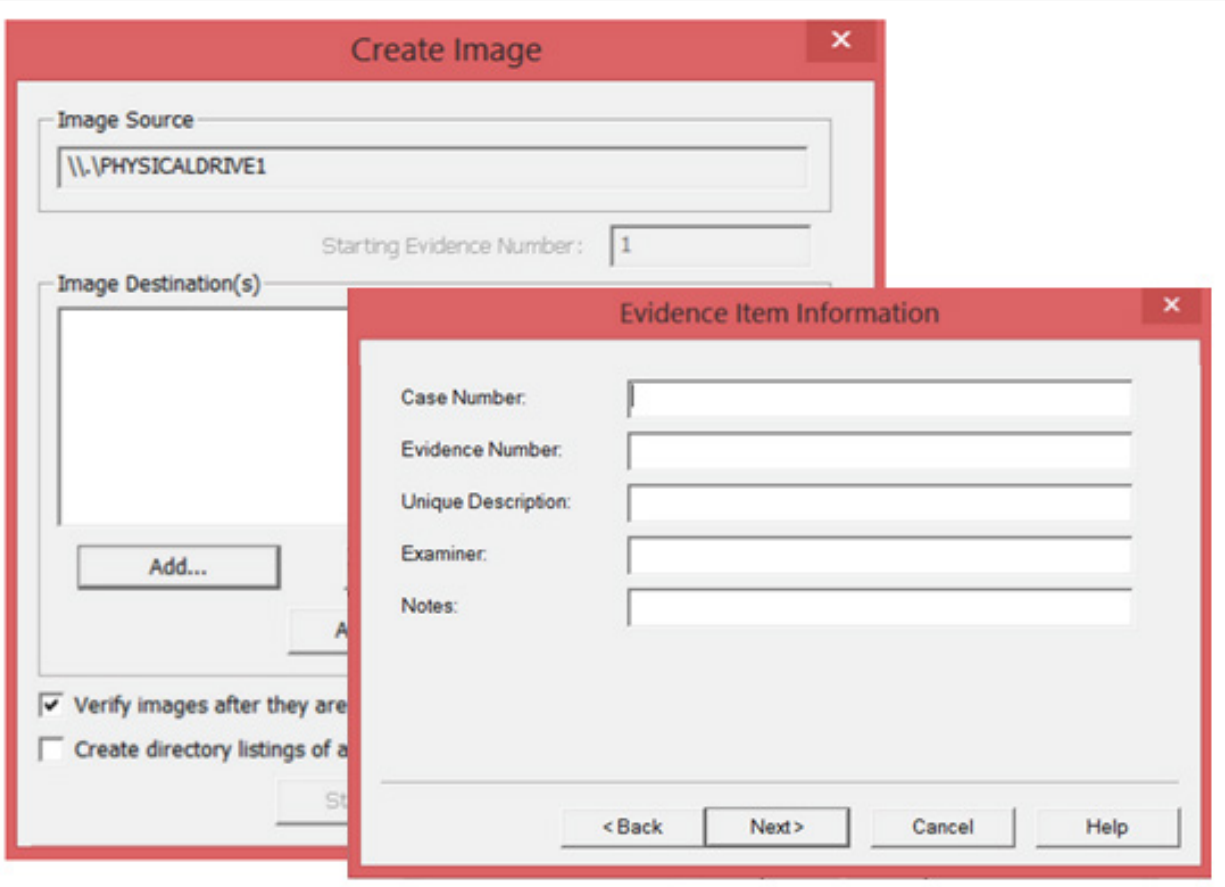
Step 4: Click **ADD** - a new dialog box will pop up



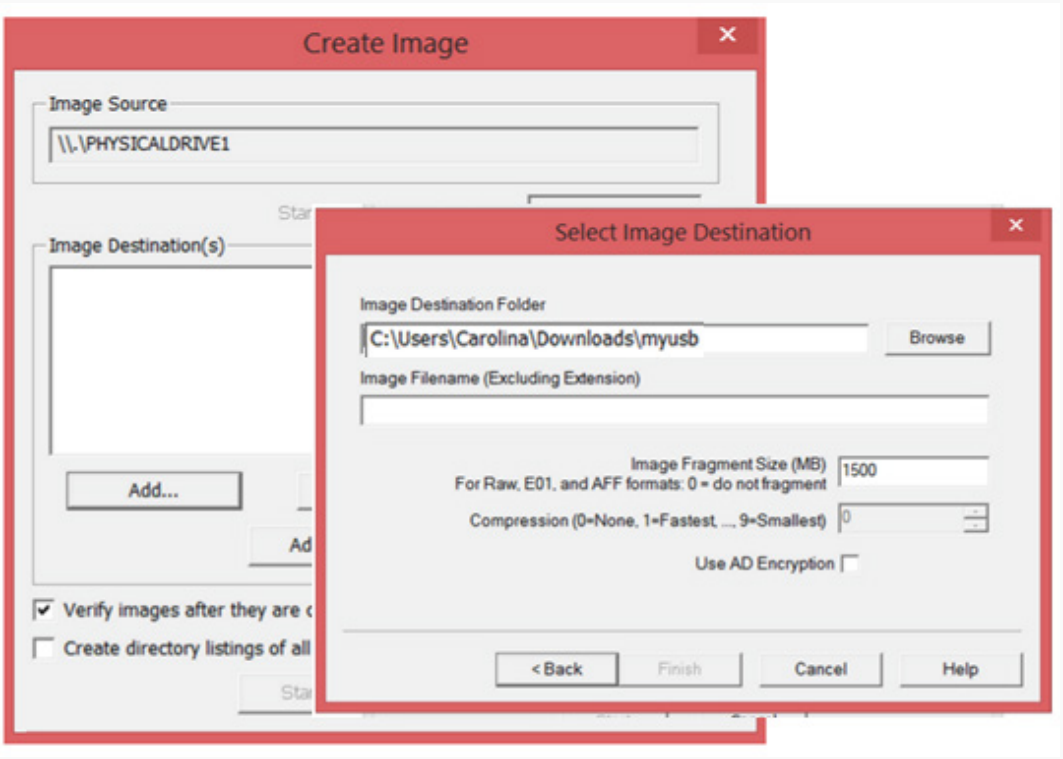
Step 5: Select whichever image type you want. Choose **Raw (dd)** if you're a beginner, since it's the most common type.



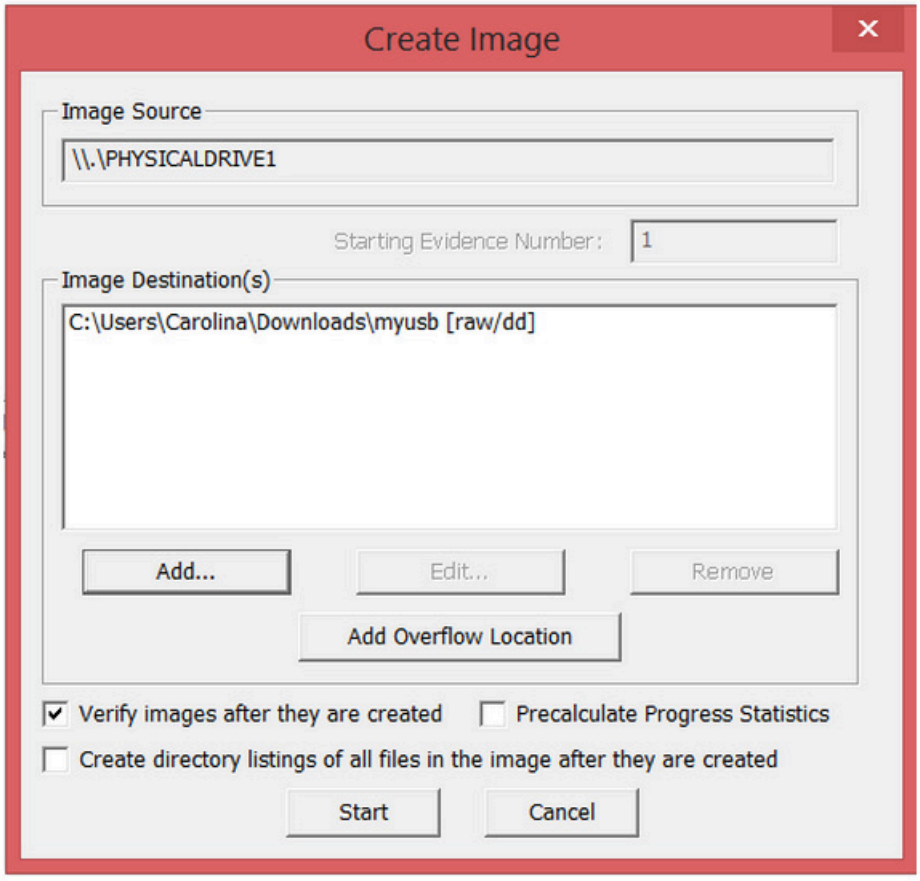
Step 6: Fill in the evidence information. (Minimum is Case Number)



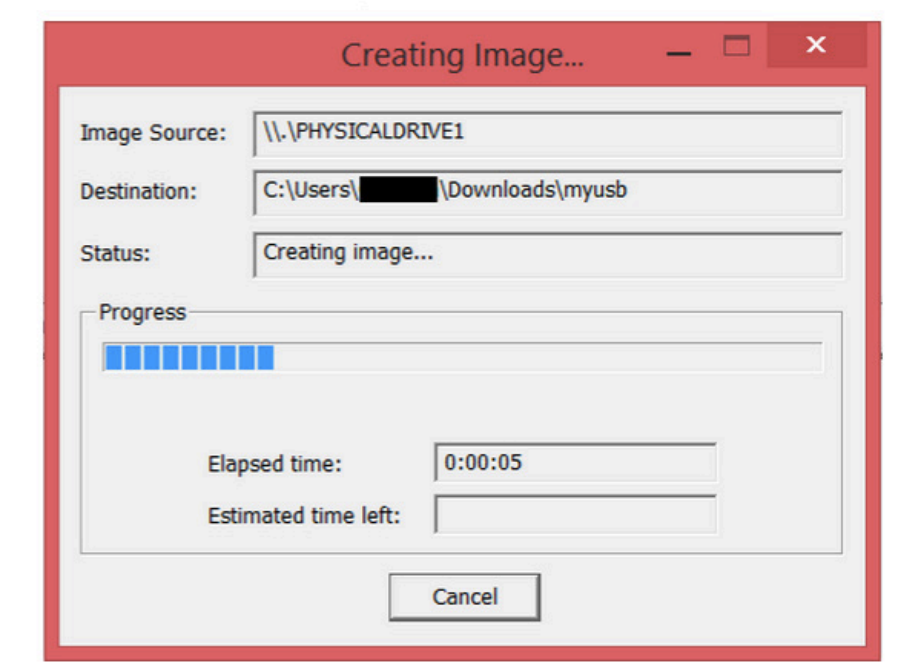
Step 7: Choose where you want to store it. Make sure the destination has enough space!



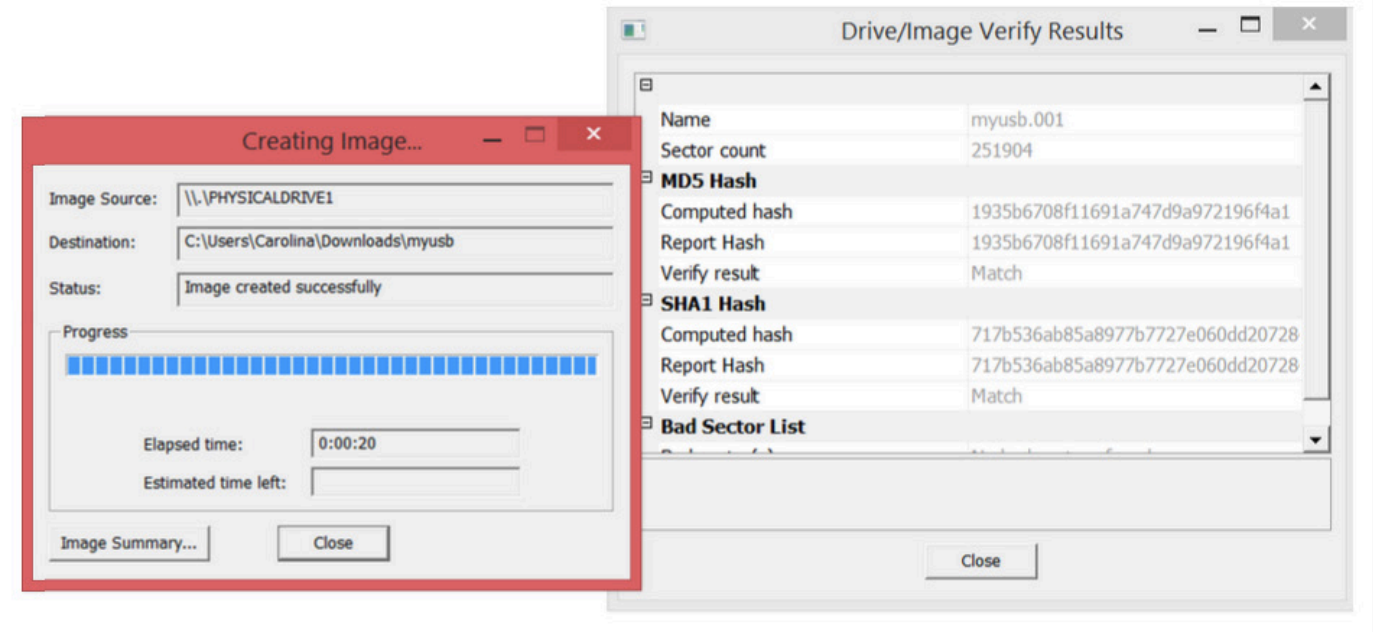
Step 8: Click START to begin creating the image.



Step 9: Wait for the image to be created



Step 10: This is the confirmation that the image creation is completed.



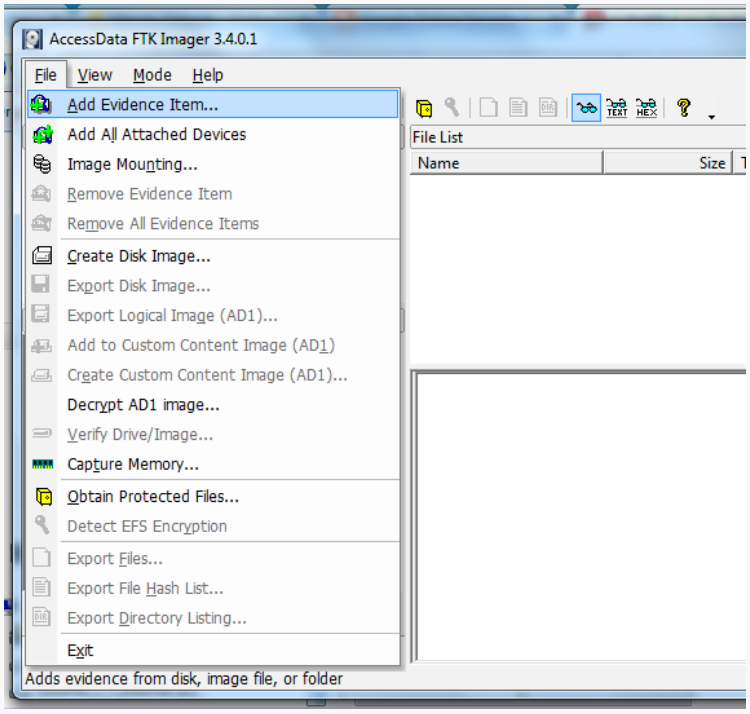
Notice the **MD5 and SHA1 Hashes.** These can be used at a future date to prove that this image is an exact duplicate of the original drive. This means that we can look for evidence on this drive and it will be treated as if we had examined the original drive directly.

Part 2= extracting evidence from a drive image

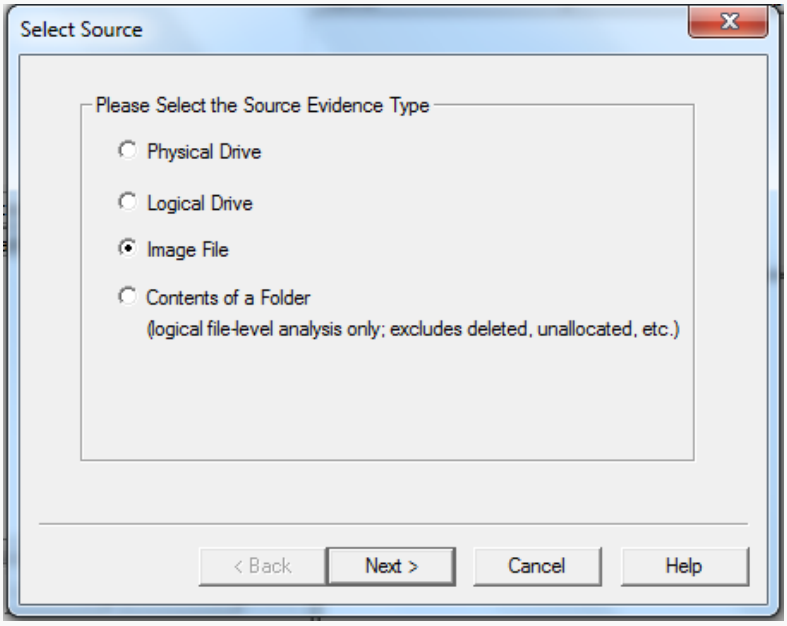
STOP - for this section we will use the two lab images:

FlashOne.001 and *FlashTwo.001 files*

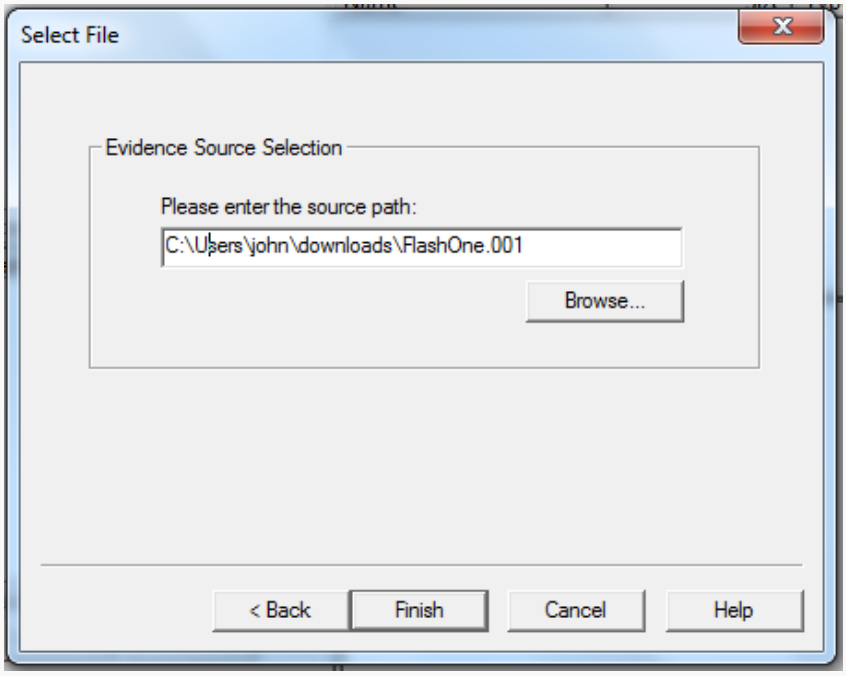
Step 1: Add the FlashOne.001 image so that you can view the contents



Step 2: This time, choose *image file*

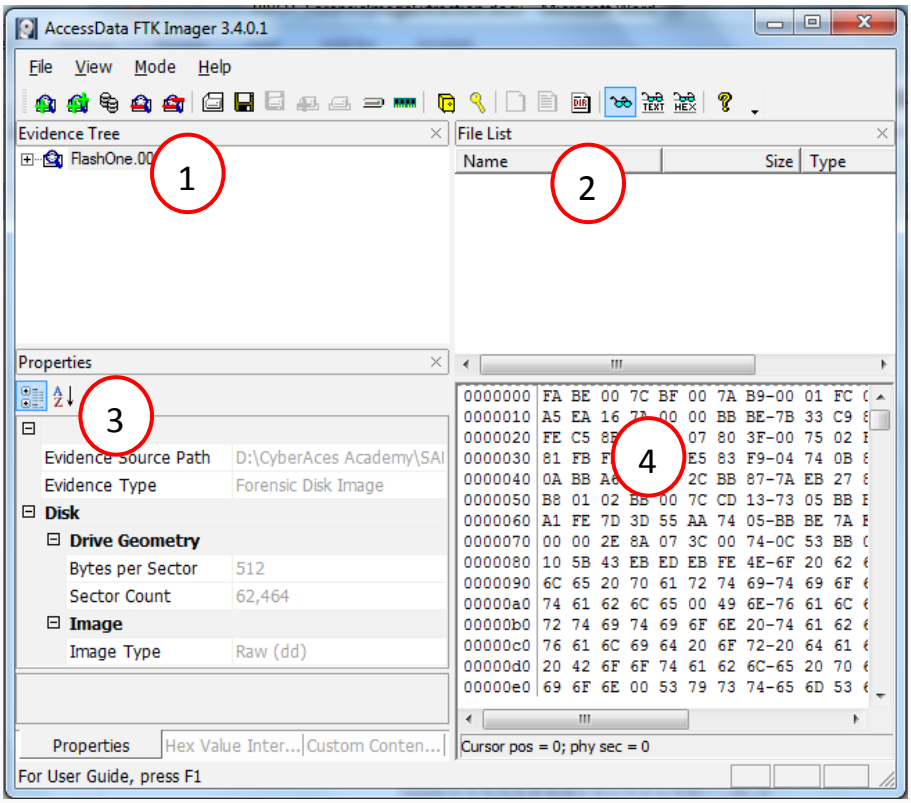


Step 3: Enter the path to the image file



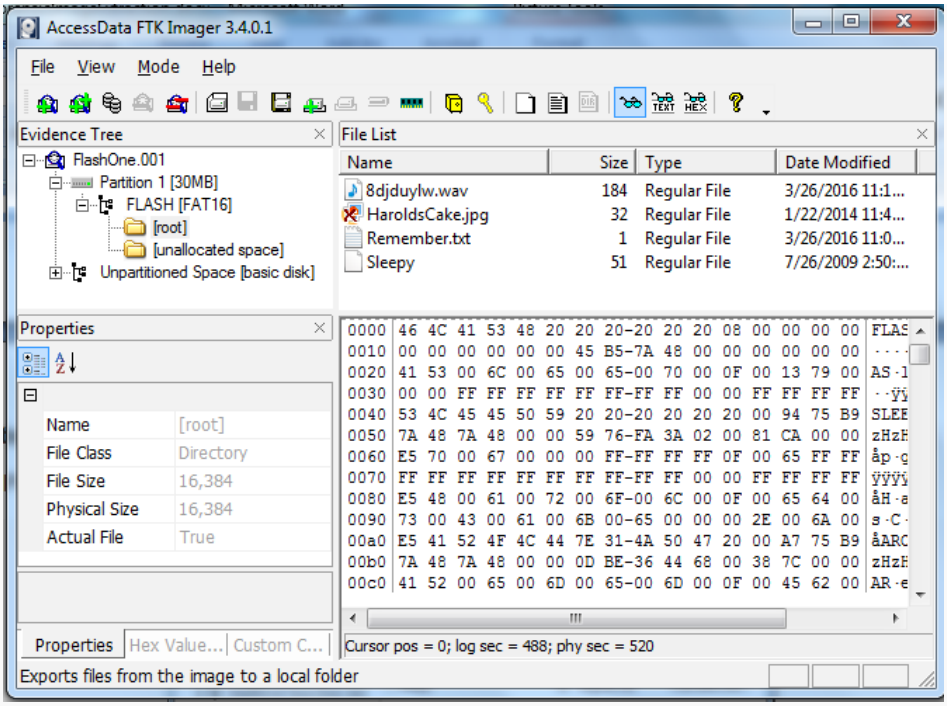
Step 4: View the image.

1. **Evidence tree** = Structure of the drive image
2. **File list** = List of all the files in the drive image folder
3. **Properties** = Properties of the file/folder being examined
4. **Hex viewer** = View of the drive/folders/files in hexadecimal

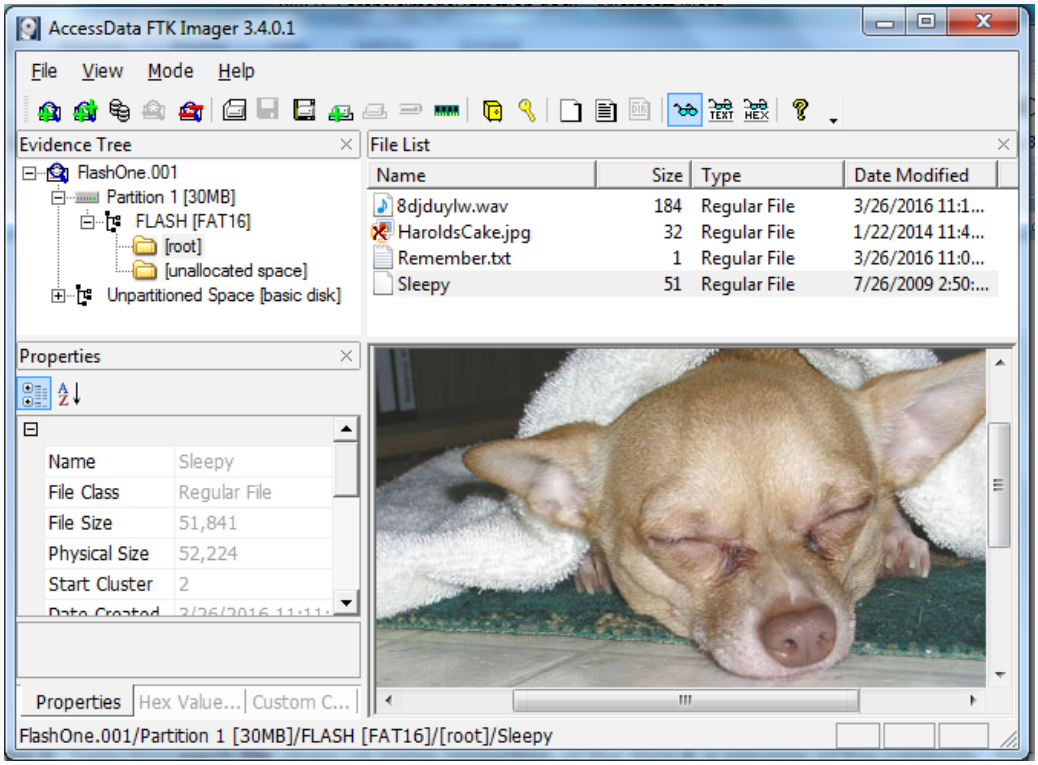


Step 5: To view files in the USB, go to

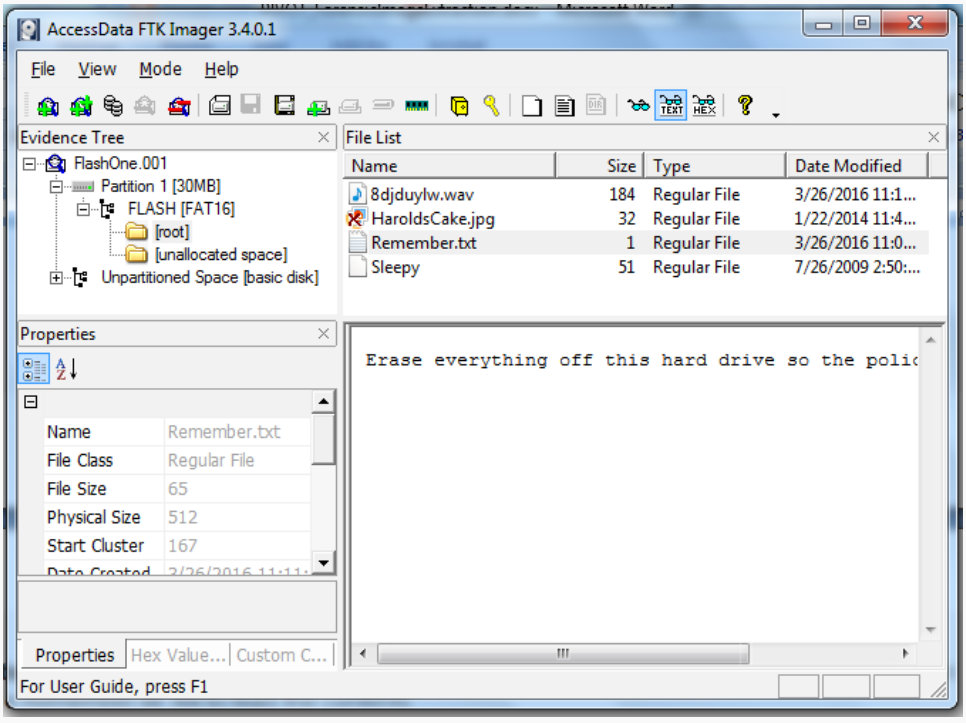
> Partition 1 > [USB name] > [root] in the Evidence Tree and look in the File List.



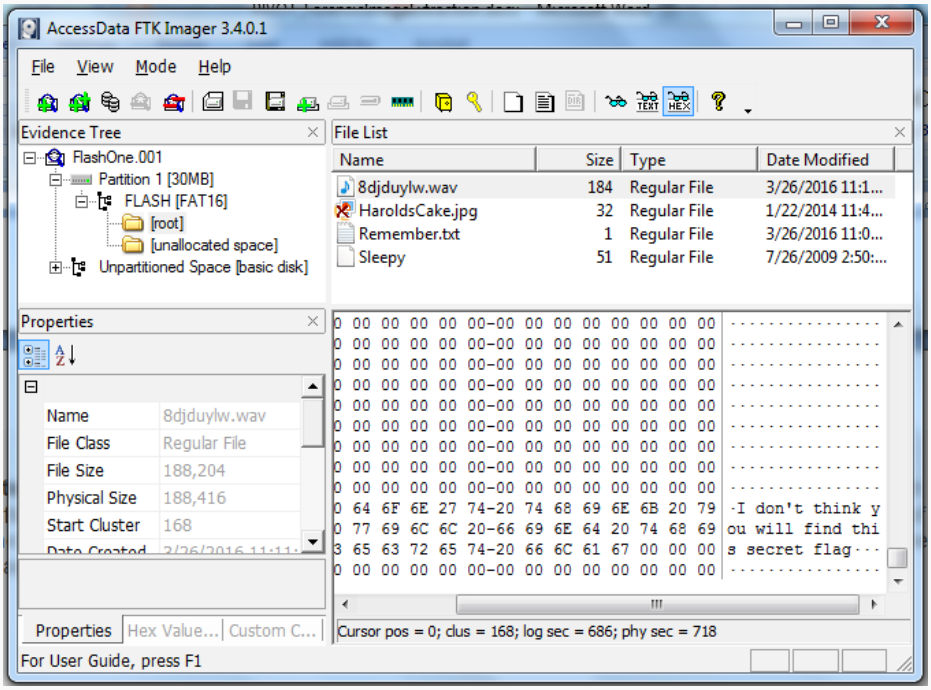
Step 6: Selecting **each file** gives us some properties of the files & a preview of the contents. For example, if we click on Sleepy we see a the image of a dog. NOTE that even though Sleepy had no file extension, AccessData FTK was able to identify that it is a jpeg and display the picture.



Step 7: Data stored in text files can be read easily in the contents section. For example, click on the *Remember.txt* file to read the contents.

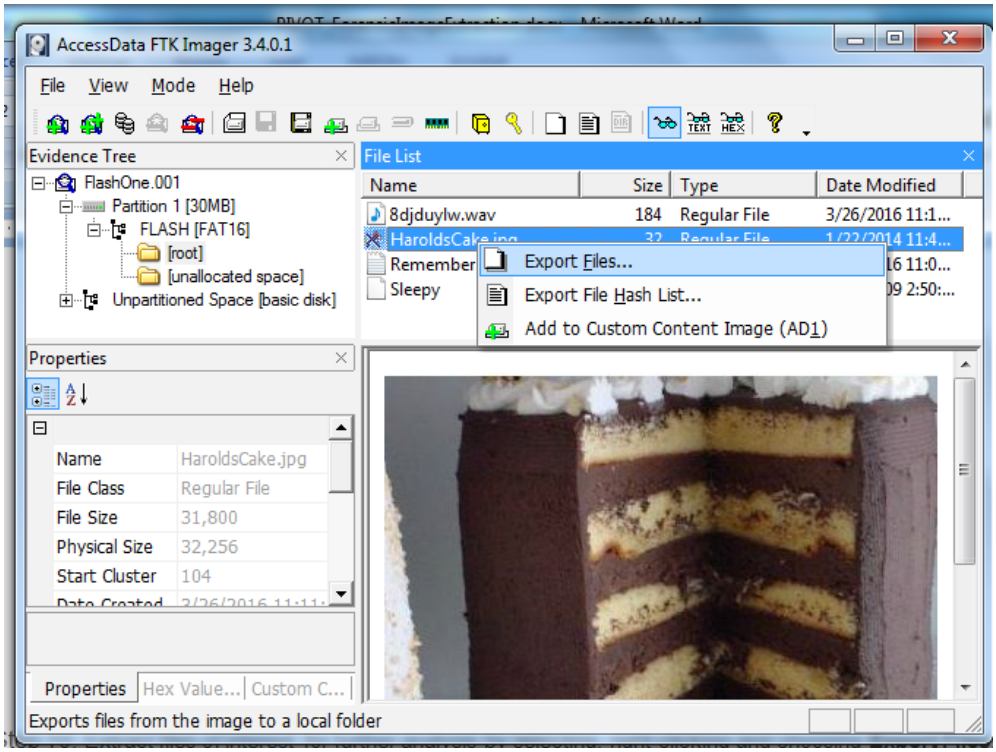


Step 8: By examining the **Hex data** for the file we may be able to find additional information about a file or even hidden data. For example, click on the *8djduylw.wav* file - you will hear a sound which is the contents of the wav file. Now click on the Hex icon on the toolbar and view the Hex information - scroll all the way down and you will see that a text message has been hidden in this area.



Step 9: Files that have been deleted on the imaged drive will be represented with a red X. However, as long as the storage area has not been overwritten with new data, the contents of deleted files will still be present on the drive. For example, click on the HaroldsCake.jpg and the picture will be displayed even though the file was deleted from the usb.

Step 10: Extract files of interest for further analysis by selecting, right-clicking and choosing **Export Files**.



Challenge: FlashTwo.001 has been provided for practice. It contains evidence of a crime. Investigate the data on the image to find the answers to the following questions:

1. There is a combination in the evidence - what is it for and what are the numbers?
2. What is the date and time to meet and what is the crime?
3. What was used as the murder weapon?
4. Who was the victim? (First and last name!)

PIVOT Lab - Forensic Image Extraction

Part 2= extracting evidence from a drive image

Answers:

1. Combination is for the safe (ToDo.txt) and the actual number is 4-55-67 (2.jpeg - in the hex)

2. This info is in Journal.doc - the crime is a robbery (this info is just in the doc text) but the Date and time are in WHITE text so the font color needs to be changed to read it. This can't be done in AccessData FTK, need to extract the document and open it with Word.
Date = 4/1/2020 Time=12 noon

3. Murder weapon is a poison can of hairspray - 4.jpg

4. Victim is Dolly Parton (one of the deleted Jpg) - if don't know name, then upload the picture to Google Images Search and it will come right up!