Module B4: Alternate Data Stream and Secret

Pre-requisite Knowledge and Skills:

1. Understand the basic of NTFS File Systems

Learning Objectives

1. Be familiar to Data hide techniques and alternation data stream technique.

Recommended Running Environment/Tools:

1. Windows OS
2. AccessData FTK Imager
3. Forensic Toolkit 1.8.6.exe

Material:

1. ADS Image.E01

Video Lecture:

1. N/A

Lab Assessment:

1. ADS Quiz

Lab Instructions:

Part I: (create alternate data streams and prepare a small sized clean thumb drive). If students do not have thumb drive, just let demonstrate by the instructor.

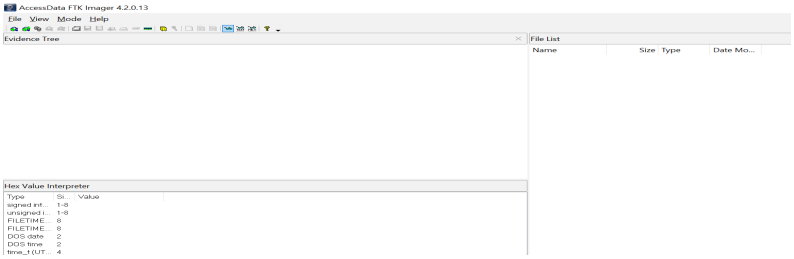
Steps:

1. Plug in the thumb drive to user's computer.
2. Make sure the thumb drive file system is NTFS. If not, please choose a free thumb drive to format the thumb drive into NTFS system (Please refer to ***Module 0 Lab*** for details).
3. Open a command line prompt (run cmd.exe at run box or other approaches).
4. On the command line prompt, type notepad testfile.txt:secret1.txt.
5. When the windows states that it cannot find the file and ask you want to create it, click *YES*
6. Inside the data stream testfile.txt:secret1.txt, add "a first secret message"
7. From the file menu, click on save and then close the file

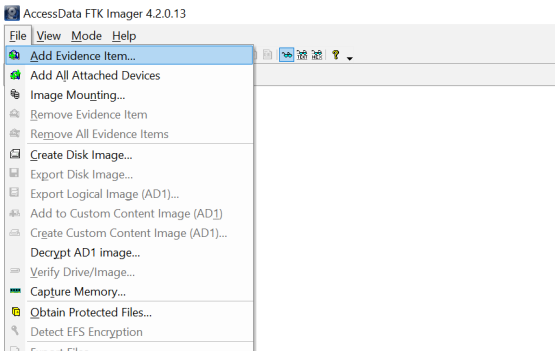
Part II: Examine the ADS file by using FTK Imager. (If students do not have thumb drive, just let demonstrate by the instructor.)

Steps:

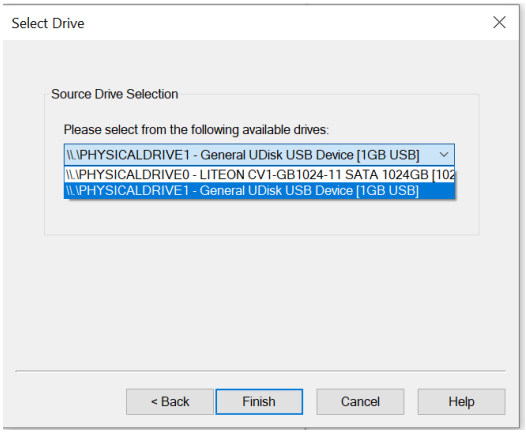
1. Run FTK Imager



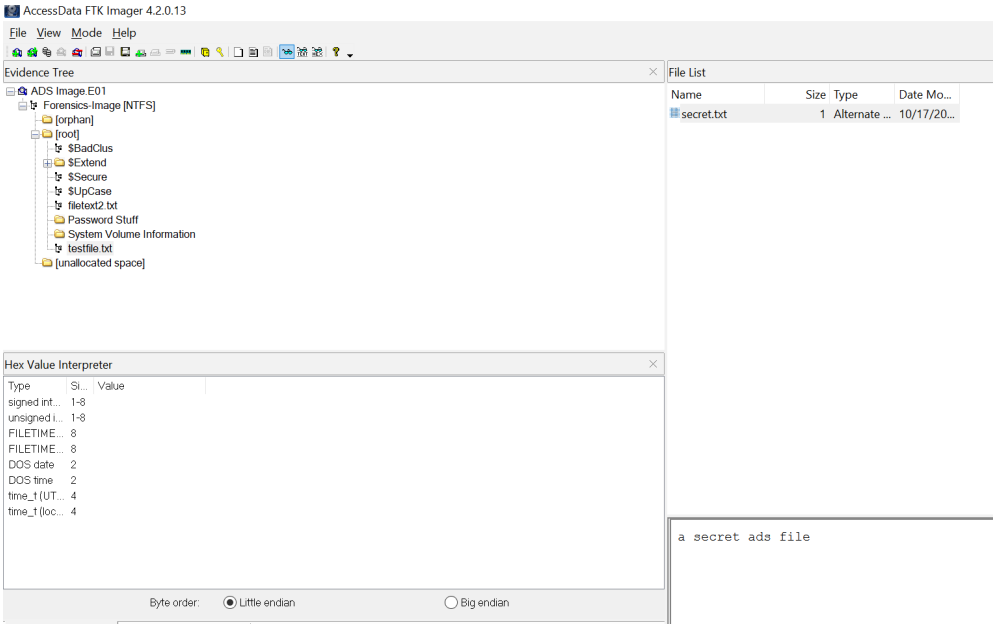
2. Click on file and select the add Evidence Item function (the 1st option)



3. Select physical drive option and click on next
4. Make sure to select the small-sized usb drive (note that your C drive usually is the default selection, please navigate the list to select the correct drive), and then click on finish



5. Click on finish. Then navigate the disk image file and its file structure to locate the ADS file and its secret.



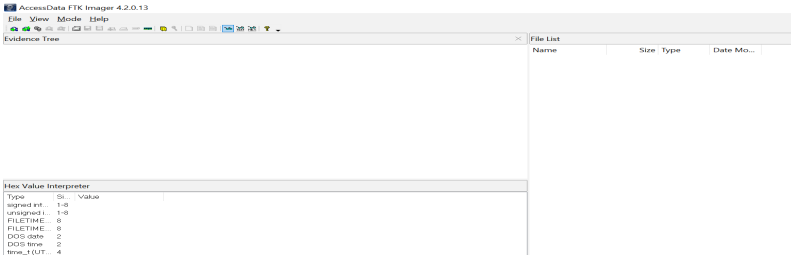
6. Click on close to close the FTK Imager.

.

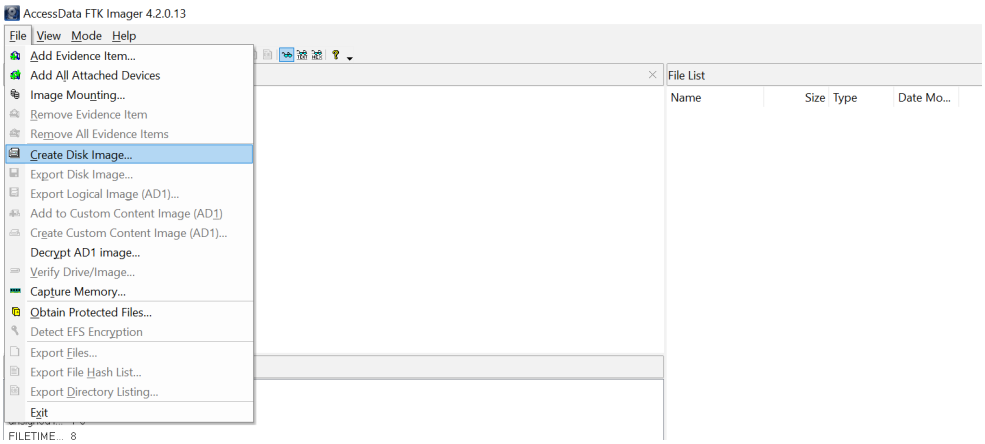
Part III: Create disk image file of the thumb drive with the ADS file by using FTK Imager. (If students do not have thumb drive, just let demonstrate by the instructor.)

Steps:

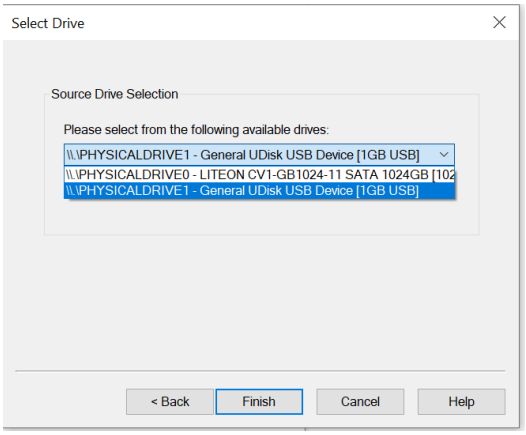
7. Run FTK Imager



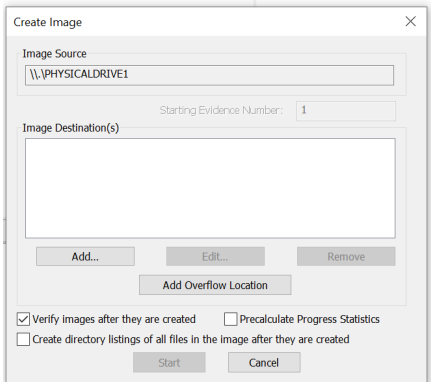
8. Click on file and select the create disk image function



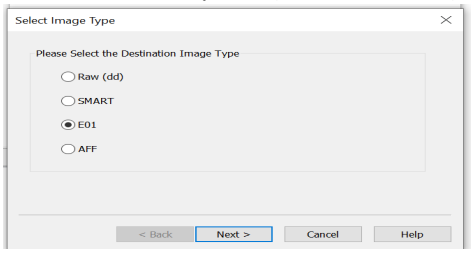
9. Select physical drive option and click on next
10. Make sure to select the small-sized usb drive (note that your C drive usually is the default selection, please navigate the list to select the correct drive), and then click on finish



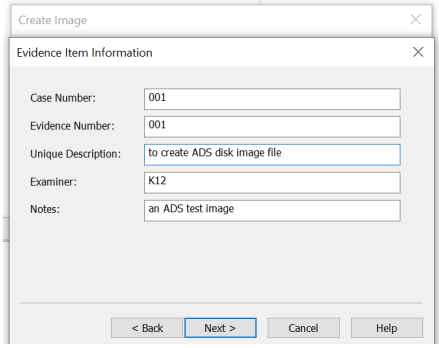
11. On the new window, please click on the add option



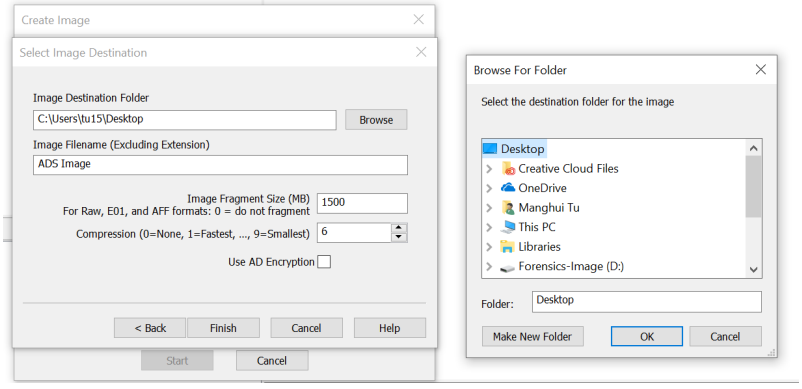
12. Select the .e01 option (Encase format), or the .dd format (raw disk image, no meta data)



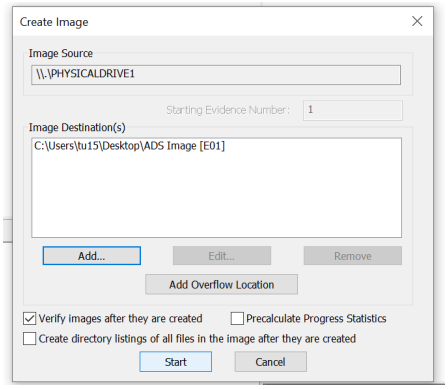
13. Click next, and then fill in the optional information, and then click next



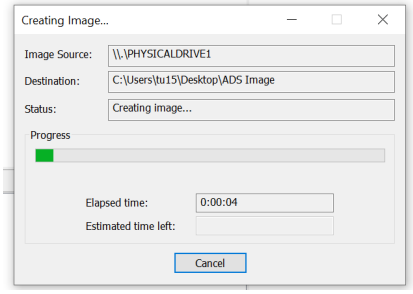
14. Choose the desired image file name (ADS Image, for example), and select the correct directory where the disk image file will be created.



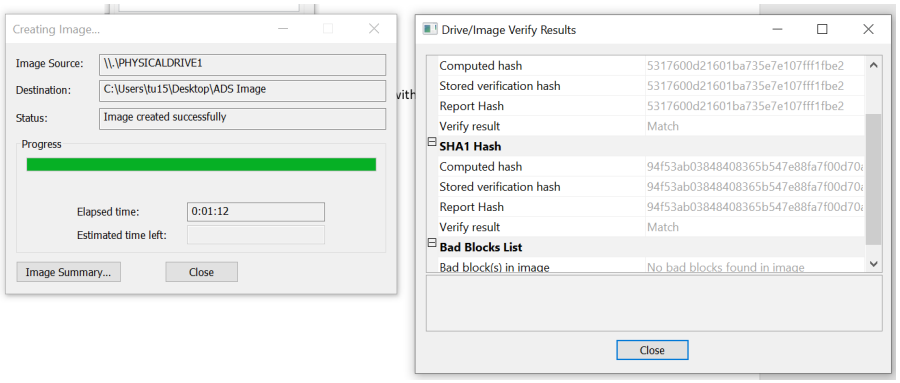
15. Click on finish



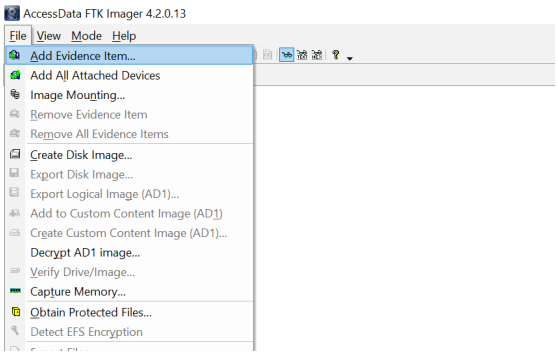
16. Click on start option, you will create a disk image with extension E01, depends on the size of the disk, it could be a few minutes to hours.



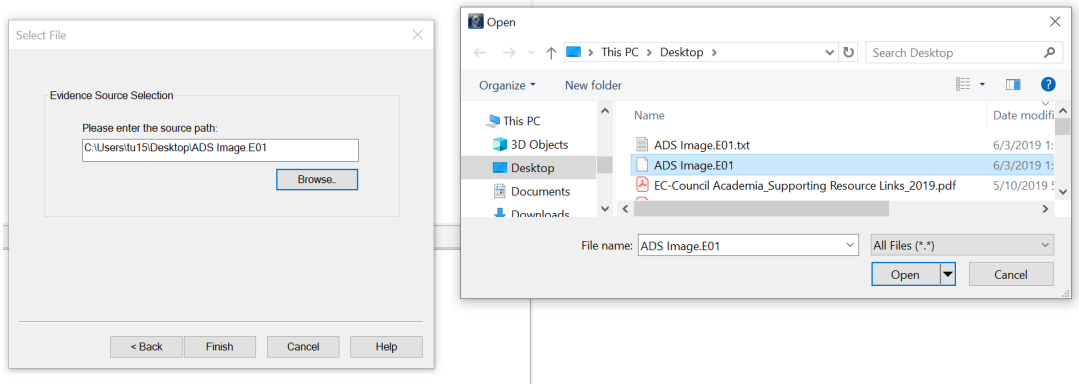
17. When finishing, it should look like what shown below. This will create disk creation report, and verify whether the hashes of the disk image and original disk are the same (if same, verified).



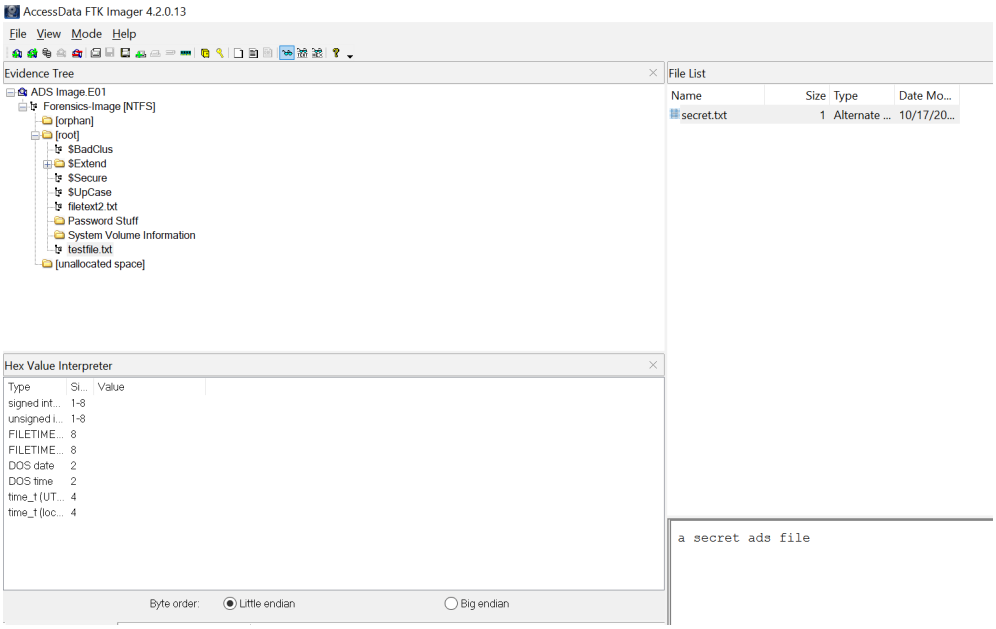
18. At the directory, you will find two files, ADS Image.e01 (disk image file) and ADS Image.E01.txt (verification file)
19. Click on close and return to the FTK imager.
20. Select the file and click the add evidence option



21. On the new pop-up window, select the image file option (not the default option), then next, and browse to the newly created ADS Image.E01 (not the txt file)

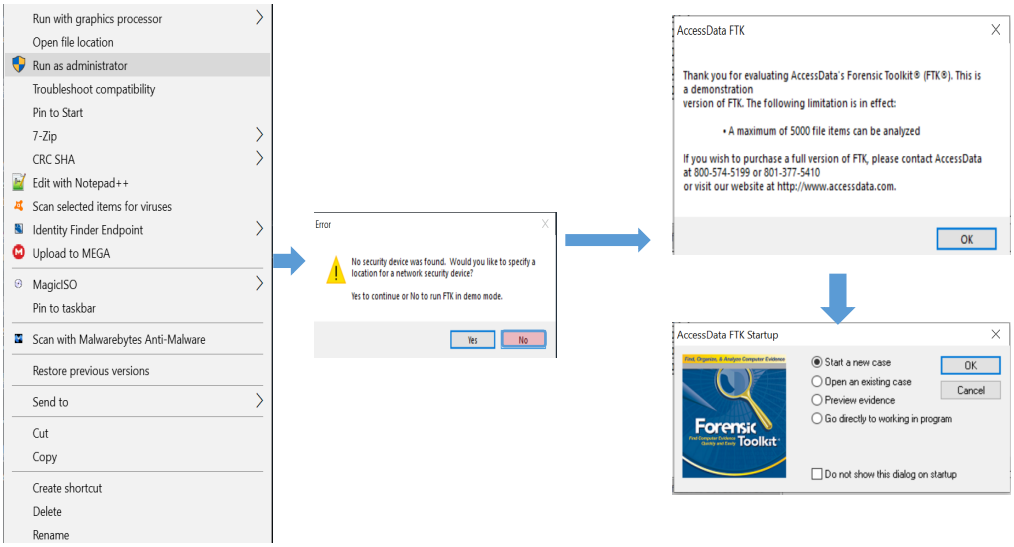


22. Then click on open and finish. Then navigate the disk image file and its file structure to locate the ADS file and its secret.



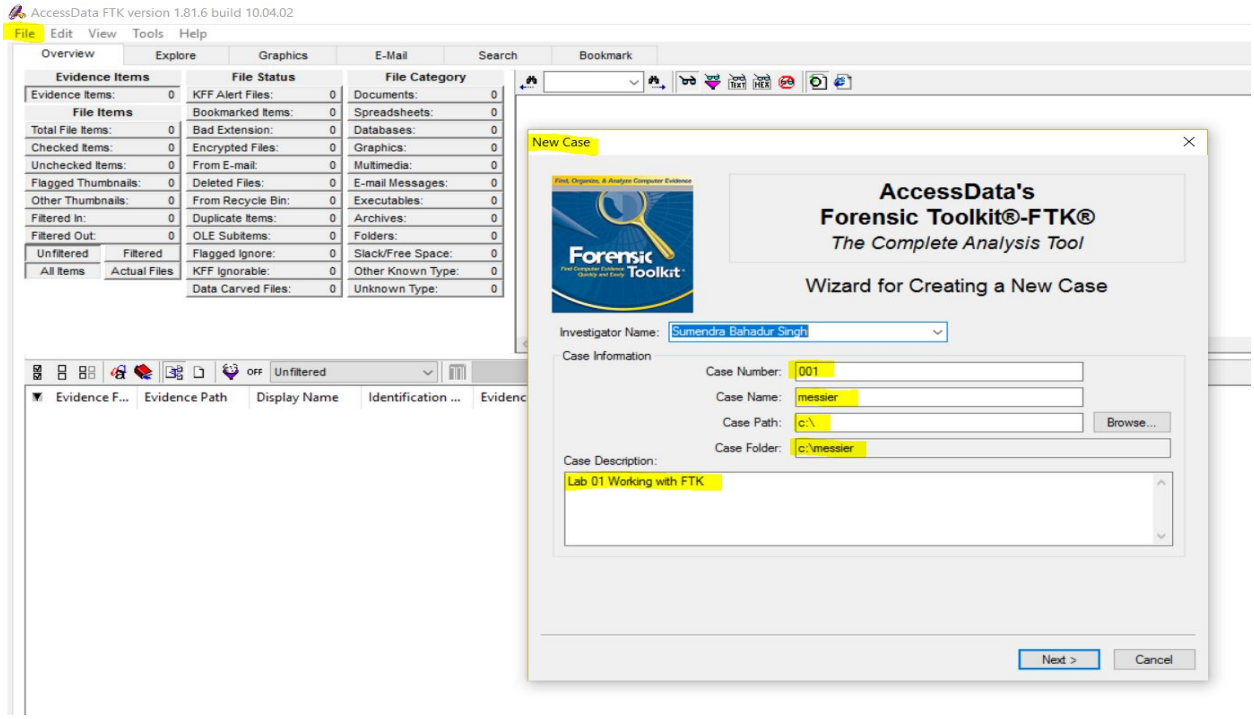
Part IV (FTK 1 ADS File Analysis by using the image file provided)
Creating a new case by using FTK 1.8.6. start by run 1.8.6 from your computer by right click the FTK1.8.6 program icon, then choose the "**run as administrator**" option. after that, select the no to run FTK in **Demo mode** (no license), click ok to accept demo mode, and then start new case.

.

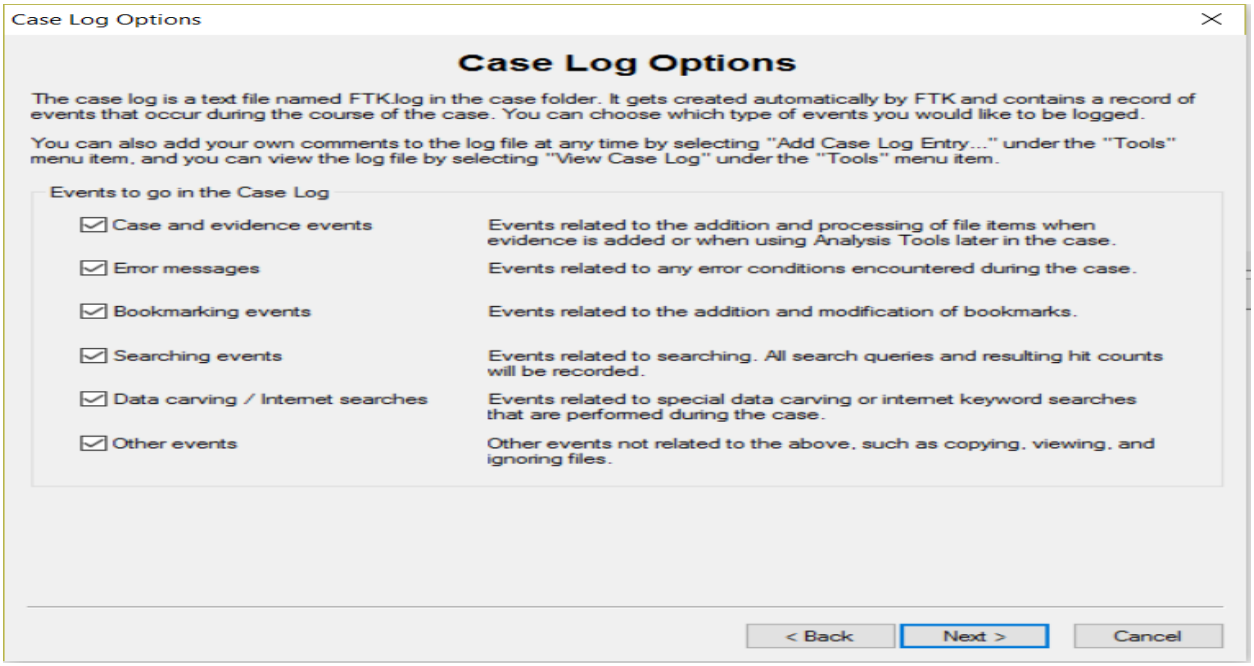


Steps:

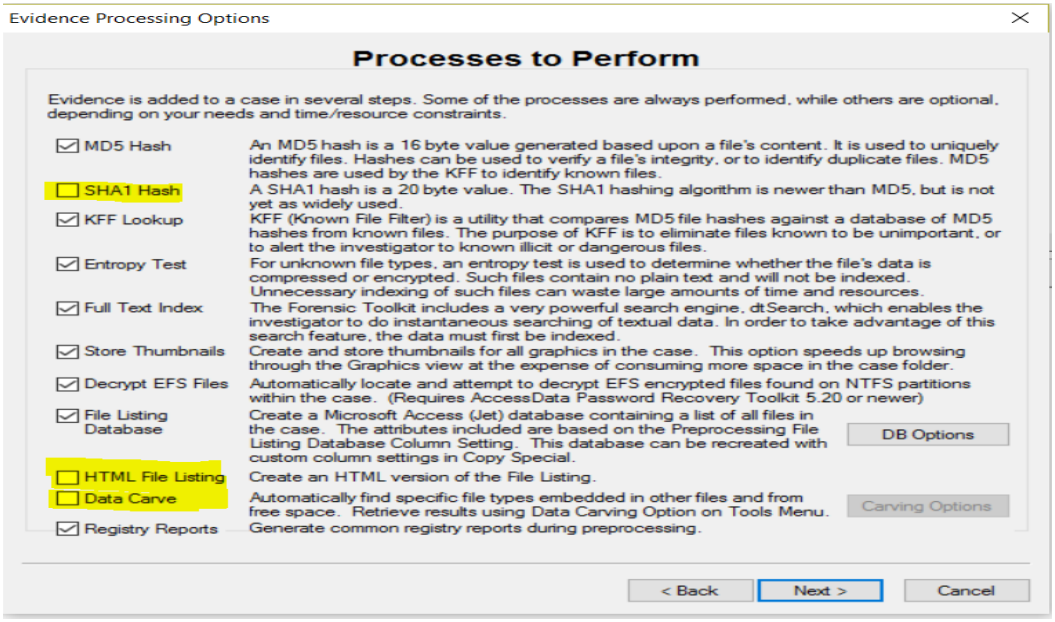
1. Create a FTK New Case



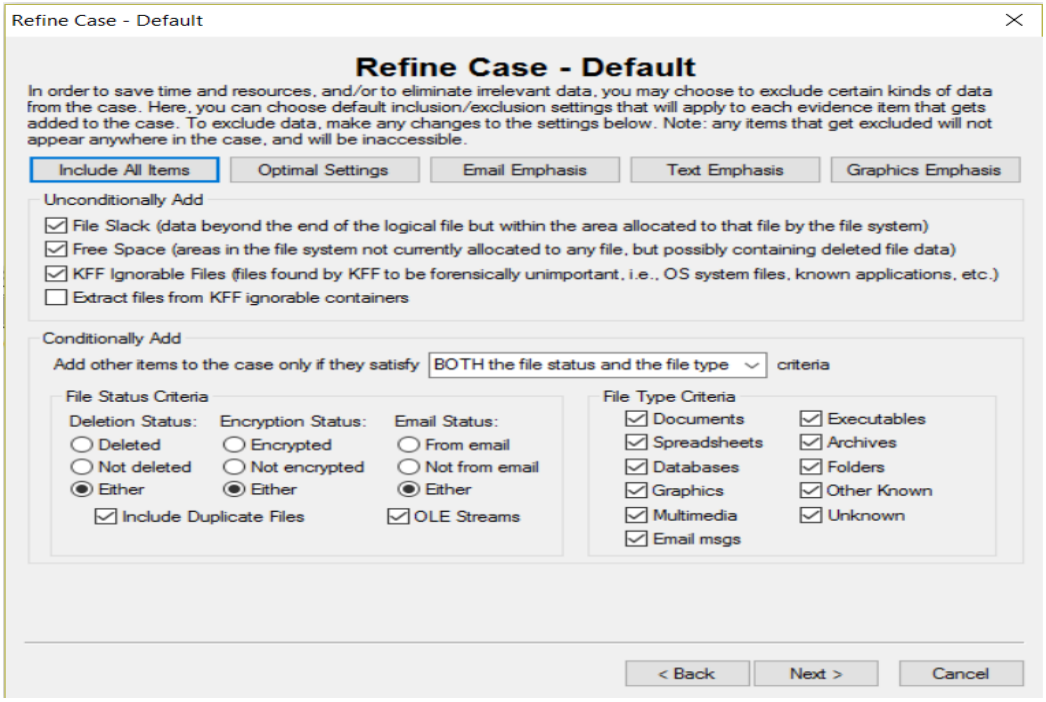
2. In the Case Log Options window, leave all options marked.

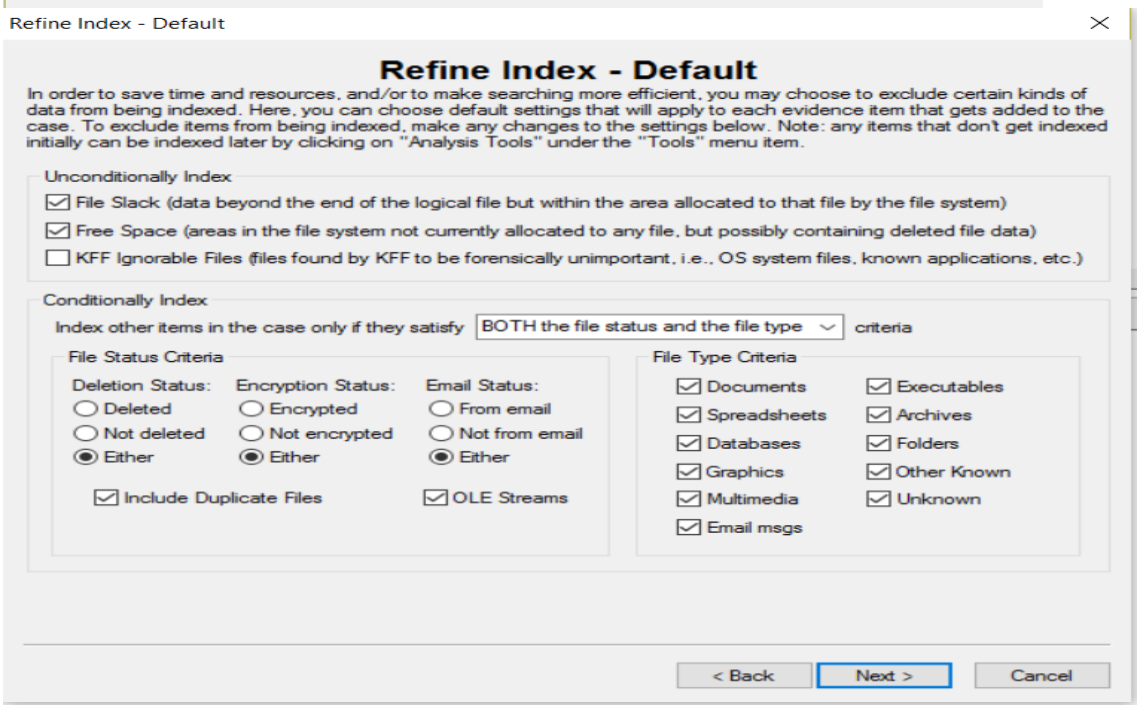


3. In the Evidence Processing Options window, mark all the options except SHAI Hash, Data Carving, and HTML File Listing.

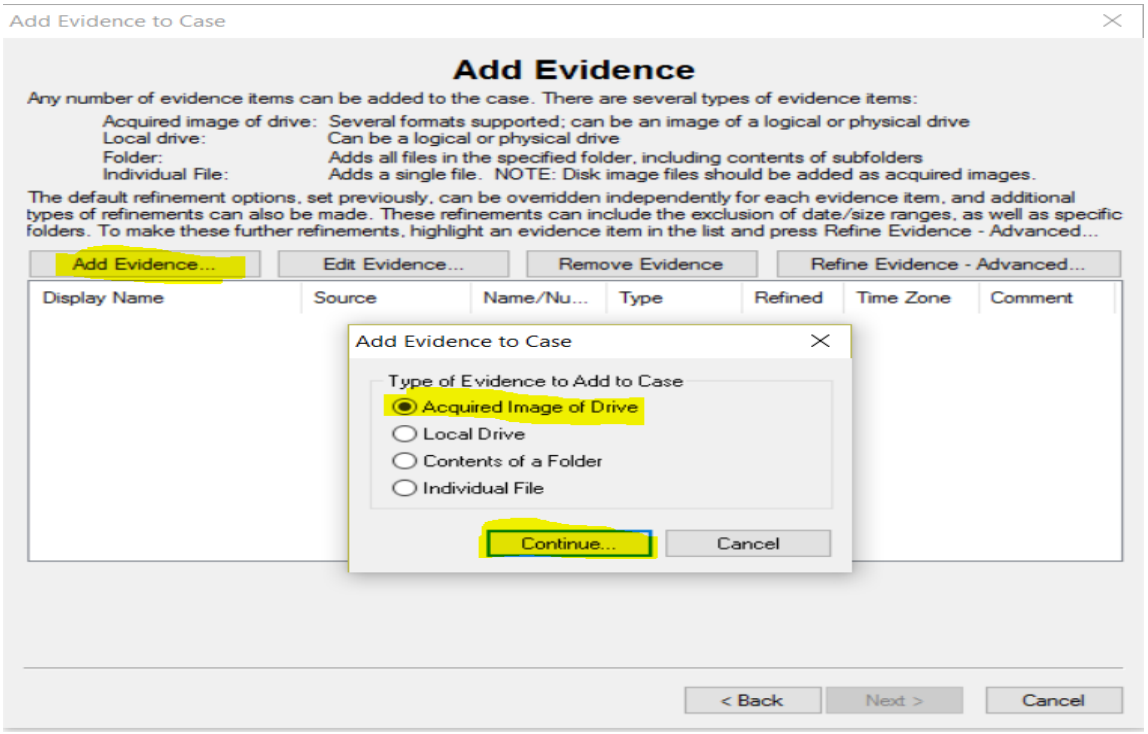


4. In the Refine Case and Refine Index default window, don't make any changes.

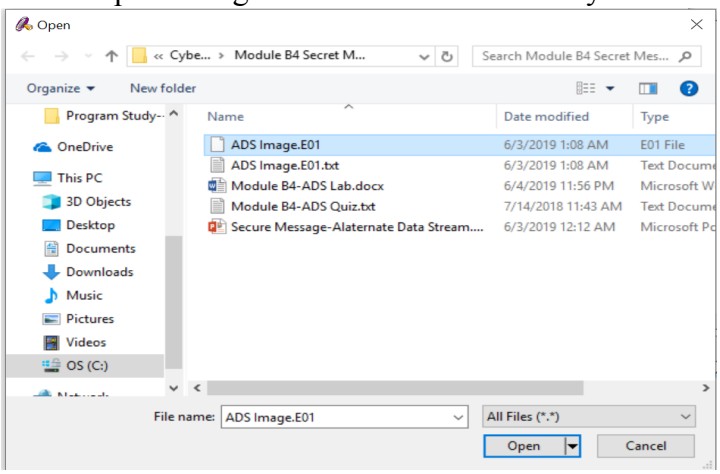




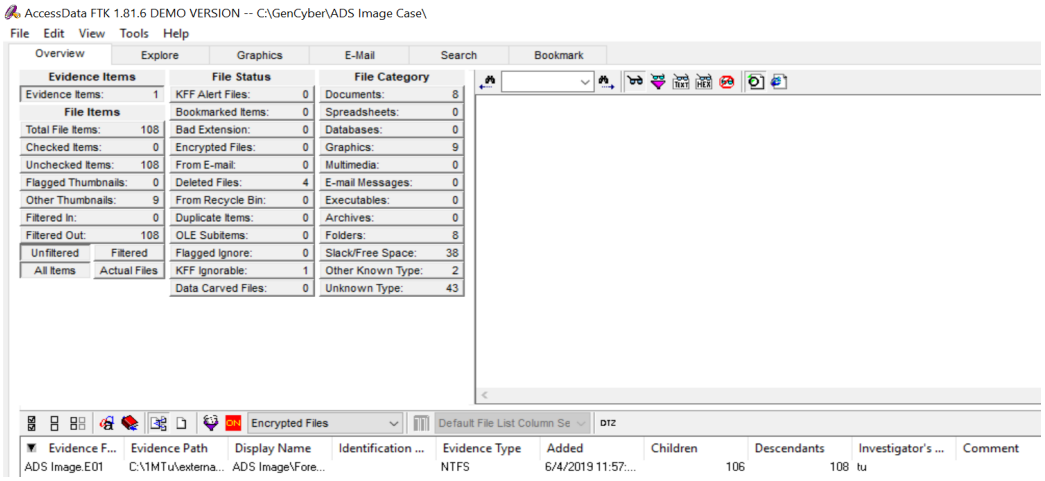
5. In the Add Evidence to Case window, click Add Evidence. Add case image from your drive with acquired image of drive option in our case. we need to download the image before we add the image file to the FTK.



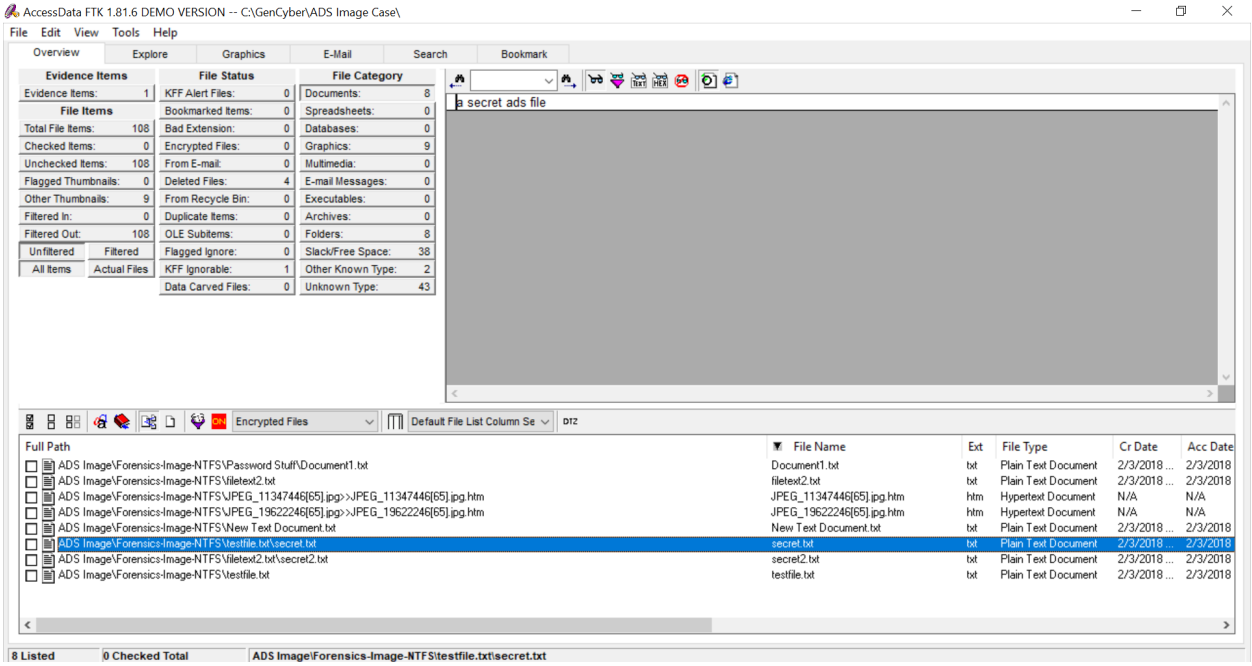
6. Select the evidence item, *ADS Image.E01*.(you can navigate to the directory following the file open dialog within the FTK tool after you click on the *continue* button)



7. The ADS Image Case will be processed as shown below.



8. Click on the ***Documents*** folder at FTK Tool's Overview Window (shown below)



9. Then navigate files and please pay attention to the two ADS files and the secret messages.