This lab is designed to allow you to practice imaging a drive and verifying it is authentic. This lab uses FTK (Forensic Tool Kit) Imager and a VHD (Virtual Hard Drive).

**Part 1: Imaging Drive**

Step 1: Launch FTK Imager as shown in Figure 1.

A screenshot of a video game

Description automatically generated

Figure 1: Launch FTK Imager

Step 2: Click on the File Menu and select Create Disk Image. See Figure 2.

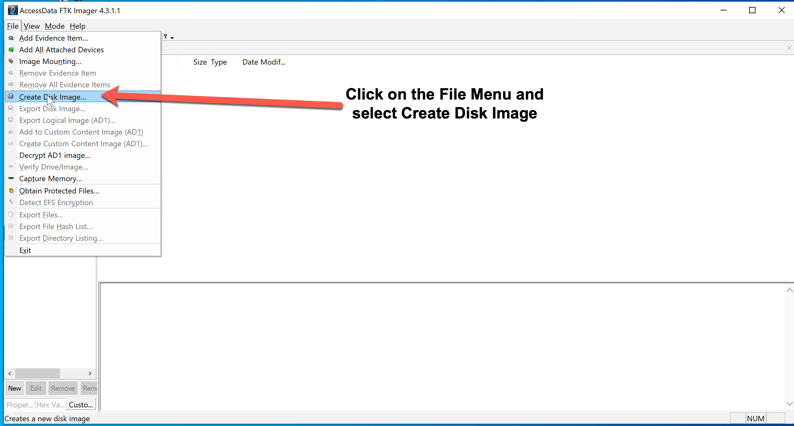


Figure 2: Start Create Disk Image

Step 3: In the Select Source Dialog, select Image File and click Next as shown in Figure 3.

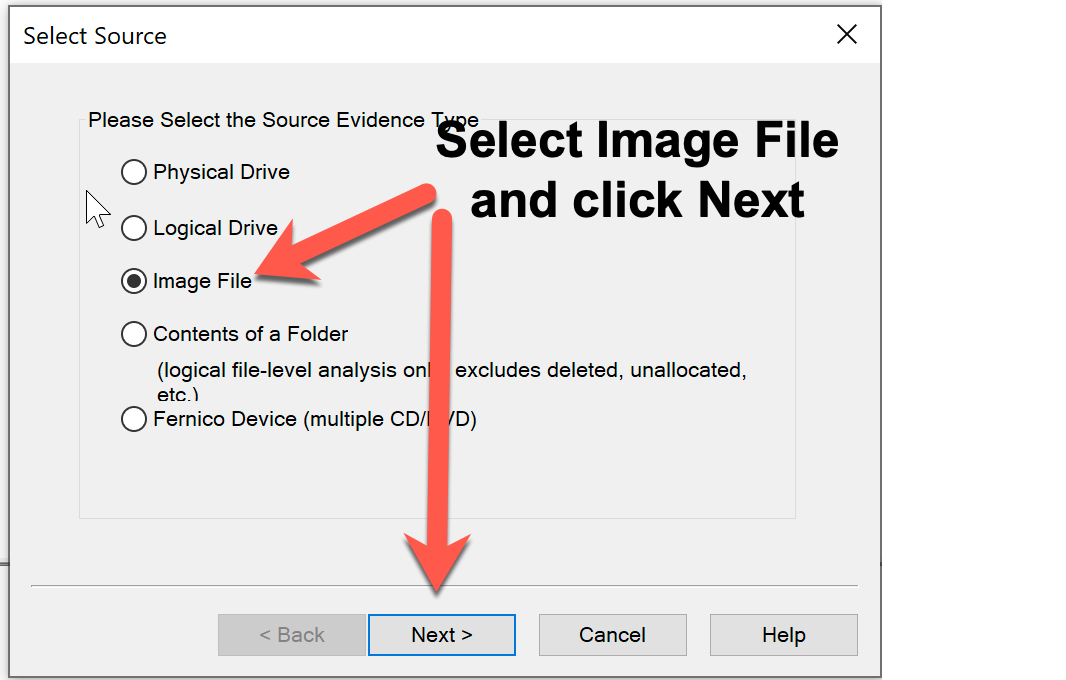


Figure 3: Select Source

Step 4: In the Select File Dialog, set the path to where the VHD (Virtual Hard Drive) is located (Desktop>Lab Data>Module5), open usb\_frive.001 and click Finish as shown in Figure 4.

Graphical user interface, text, application

Description automatically generated

Figure 4: File selection

Step 5: In the Create Image Dialog, under Image Destination(s), click Add shown in Figure 5.

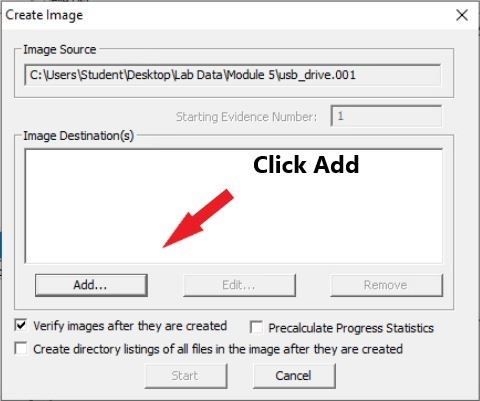


Figure 5: Image Source

Step 6: In the Select Image Type dialog, select E01 and click Next as shown in Figure 6.

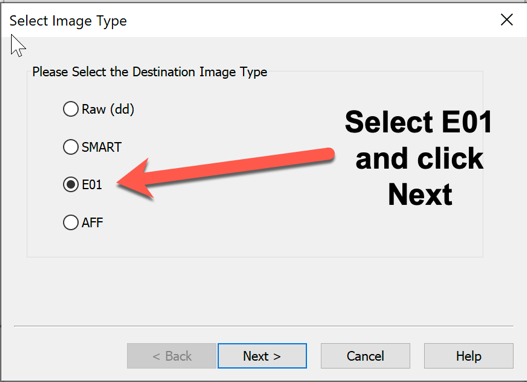


Figure 6: Select Image Type

Step 7: In the Evidence Item Information dialog, complete the following fields:

Case Number: Enter with dashes as shown in the figure of year-month-day-case number.

Evidence Number: This will increment starting at 1.

Unique Description: Enter your last name and VHD Image.

Examiner: Enter your last name

Notes: Leave notes blank

Click the Next Button

Graphical user interface, text, application, email

Description automatically generated

Figure 7: Evidence Item Information

Step 8: In the Select Image Destination dialog, set the following fields.

Image Destination Folder: set the path to the work folder on the Desktop

Image Filename (Excluding extension): enter your last name\_usb

Click the Finish Button

Graphical user interface, text, application

Description automatically generated

Figure 8: Select Image Destination

Step 9: Once back on the Create Image dialog, ensure the Image Source and Image Destination are completed and click the Start Button shown in Figure 9.

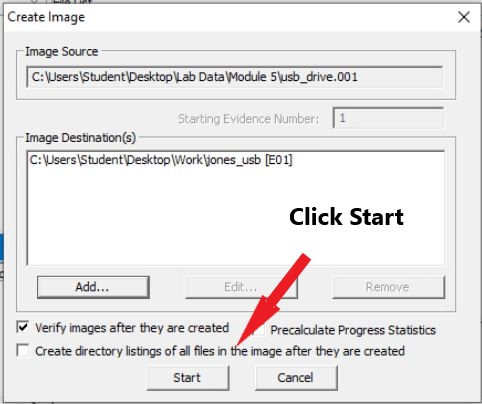


Figure 9: Create Image

Once the image starts processing, you will see dialog like shown in Figure 10.

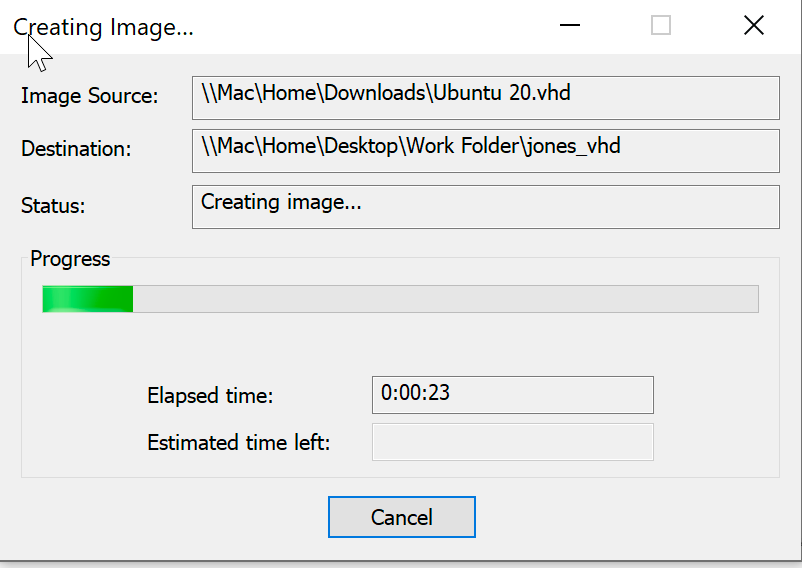


Figure 10: Creating Image

Step 10: After the drive image completes, the Drive/Image Verify Results will appear and shows the following information:

Name of the image file

Sector count

MD5 Hash data

SHA Hash data

Bad Blocks List

**Screen capture this dialog and paste below this line.** Then close the Image Summary and Creating Image dialog. After capturing the image, click close twice.

Graphical user interface, text, application

Description automatically generated

**Part 2: Using the evidence Tree, answer thee following questions.**

Step 1: In the FTK Imager interface, click on the Add Evidence Item icon as shown in Figure 11.

Graphical user interface, text, application, email

Description automatically generated

Figure 11: Add Evidence Item

Step 2: In the Select Source dialog, select Image File and click Next as shown in Figure 12.

Graphical user interface, text, application

Description automatically generated

Figure 12: Select Source

Step 3: Browse to the file you just imaged located at c:\users\student\desktop\work and click Finish as shown in Figure 13. If you get an error be sure you selected the image file and not the summary text file.

Graphical user interface, text, application

Description automatically generated

Figure 13: Source file

Step 4: This should populate the Evidence Tree. Expand the tree as shown in Figure 14 and answer the following questions.

Graphical user interface, text, application, chat or text message

Description automatically generated

Figure 14: Evidence Tree

1. How many files are there in the system volume information? List them out

a. IndexerVolumeGuid, 1KB, Regular File, 1/19/2021 7:07:10 PM

b. IndexerVolumeGuid.FileSlack, 4KB, File Slack

c. WPSettings.dat, 1KB, Regular File, 1/19/2021 7:07:06 PM

d. WPSettings.dat.FileSlack, 4KB, File Slack

1. What is the size of the Root by clicking on SECUREGUARD?
   1. 16KB
2. How many deleted files are there in root?
   1. 4
3. Based on the information in SECUREGUARD, what is the file system used?
   1. FAT16
4. Is there anything in unallocated space, if so, list it and its size?
   1. 00058, 244.240 KB