FTK Imager

A How-To Guide

What is FTK Imager?

- A piece of software (made by AccessData) able to acquire digital evidence in various ways
    - physical acquisition
    - logical acquisition
    - folder/file acquisition
- Allows the investigator to quickly, efficiently, and correctly acquire evidence from a system
- It has support for plugins and external supporting hardware such as write-blockers as well for the most forensically sound acquisition possible

Physical Acquisition

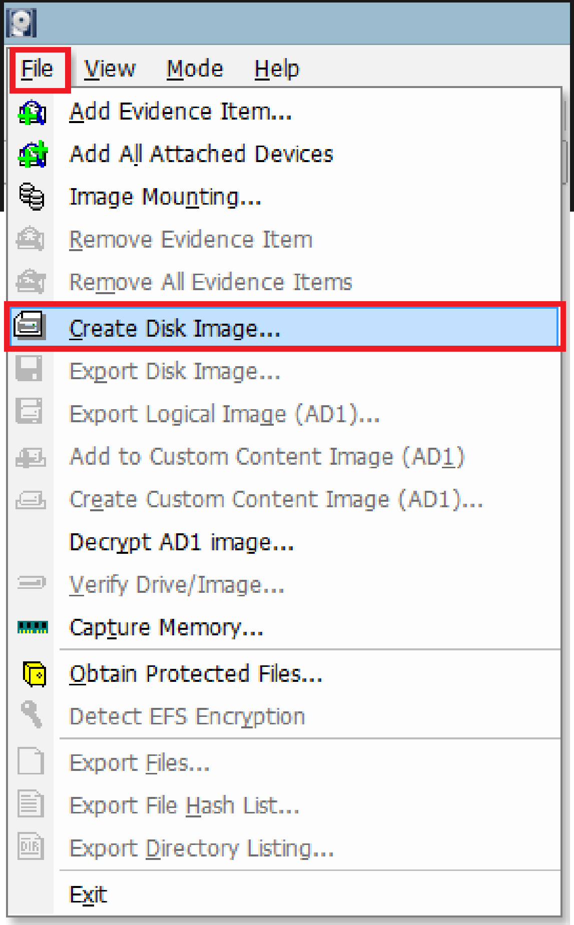
- Physical acquisition includes everything on a hard drive.
  - Unallocated space
  - Allocated space
  - Every partition on the hard drive

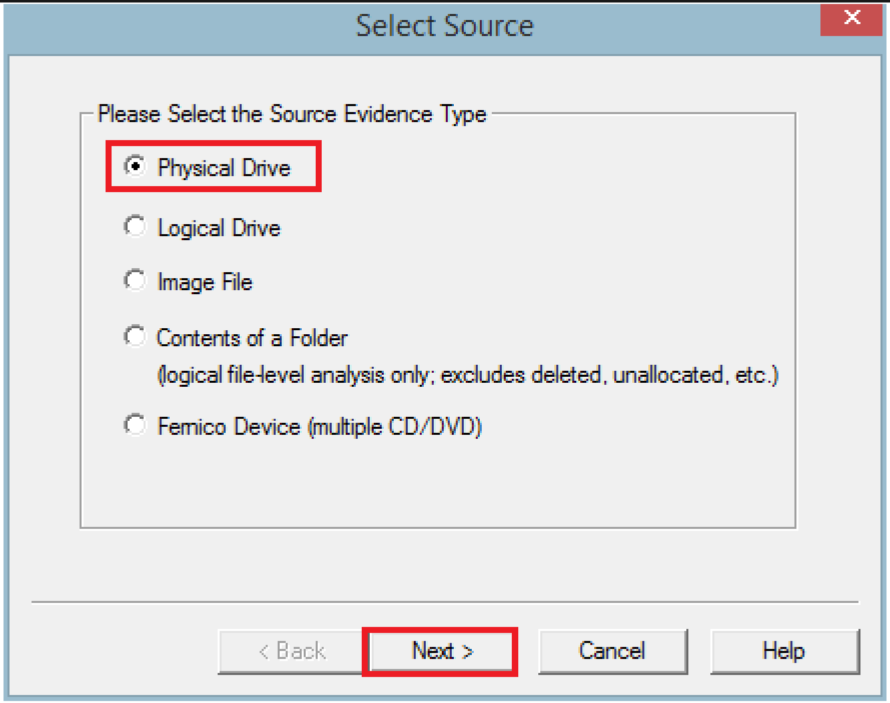
Step-By-Step

- After downloading and installing from here, open FTK Imager by right-clicking and selecting “run as administrator”
- To perform a physical acquisition, select “File” then “Create Disk Image”
- Select “Physical Drive” and click “Next”
- First make sure the drive you want to image is connected to the computer via “Disk Manager” then in FTK Select the drive you want to acquire and click “Finish”
- A new window will appear. Select “Add” and select “E01” and press “Next”
- Fill out the case information as well as a description of the evidence and press “Next”

Step-By-Step (cont.)

- Select the folder to save the Image to as well as input a Filename for the Image file.
- If you want the Image to be processed quickly make sure to put the compression at 0. However this will make the file size bigger. Keep this in mind. Also, FTK fragments files by default so if you simply want one large file set this number to 0. Otherwise, keep it at its default value.
- If you want to encrypt the file, select the box “Use AD Encryption”
- Then Select “Finish”
- Finally select “Start” to acquire the Image

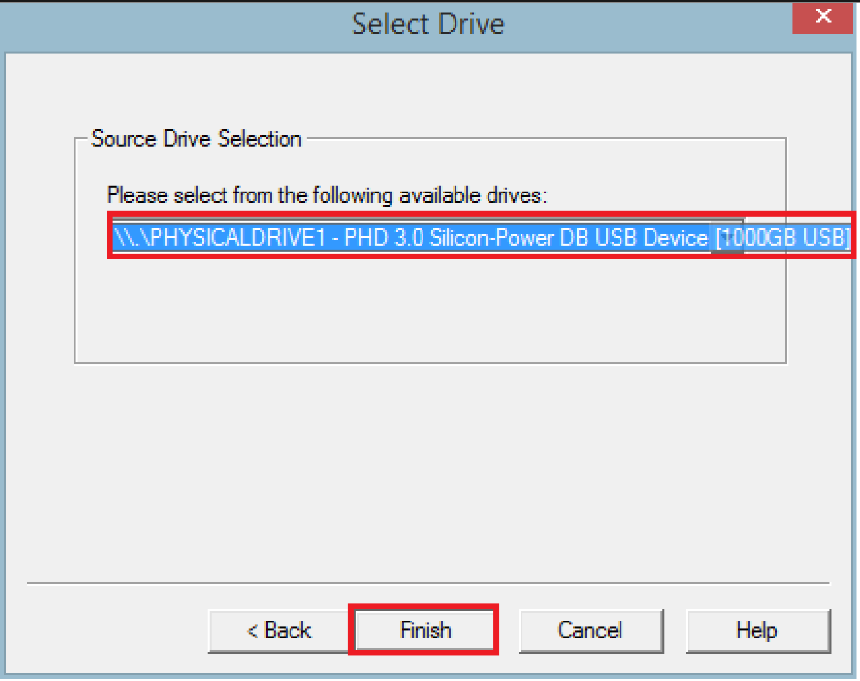



Select Source

Please Select the Source Evidence Type

- ● Physical Drive
- ○ Logical Drive
- ○ Image File
- ○ Contents of a Folder
  (logical file-level analysis only; excludes deleted, unallocated, etc.)
- ○ Femico Device (multiple CD/DVD)

[redacted]

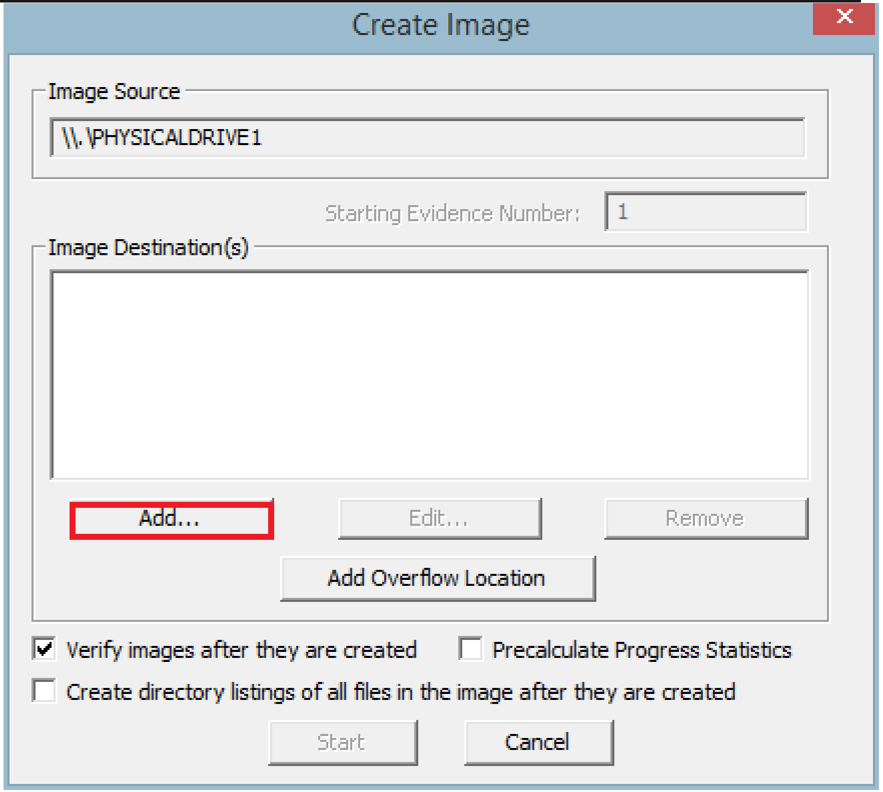


Select Drive

Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE1 - PHD 3.0 Silicon-Power DB USB Device [1000GB USB]



Create Image

Image Source

\\.\PHYSICALDRIVE1

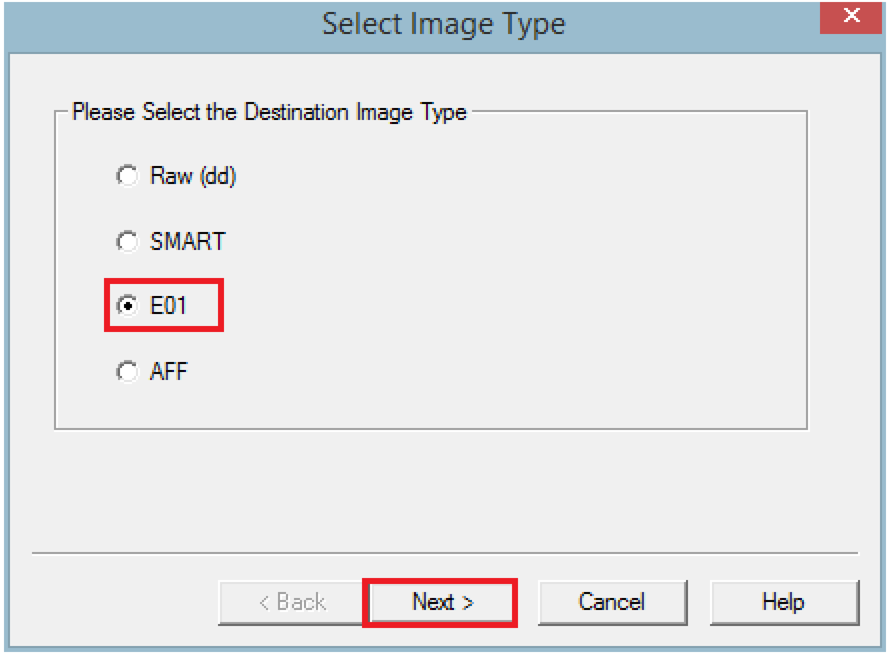
Starting Evidence Number: 1

Image Destination(s)

☑ Verify images after they are created

□ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created



Select Image Type

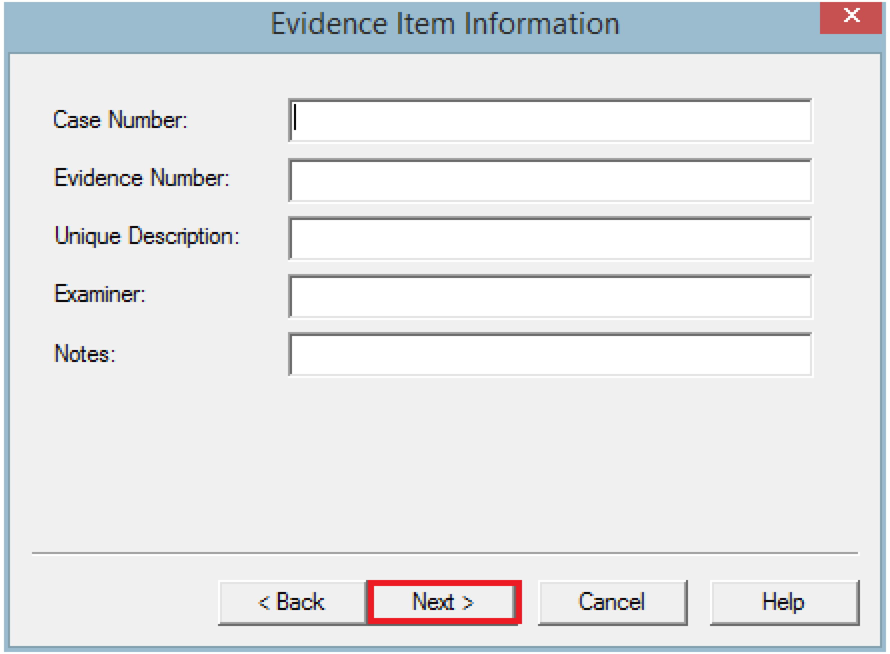
Please Select the Destination Image Type

○ Raw (dd)

○ SMART

● E01

○ AFF



Evidence Item Information

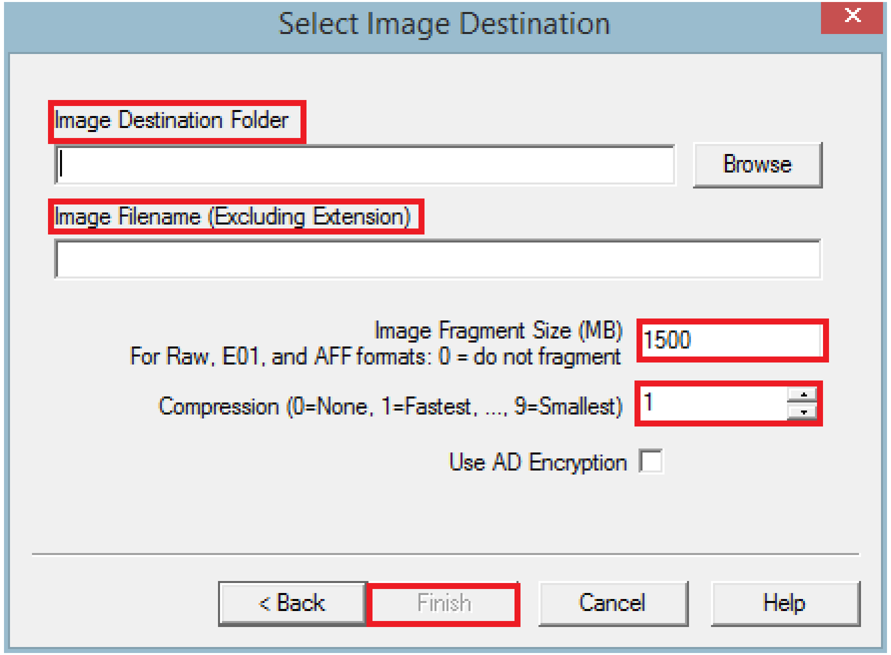
Case Number:

Evidence Number:

Unique Description:

Examiner:

Notes:



Select Image Destination

Image Destination Folder

Browse

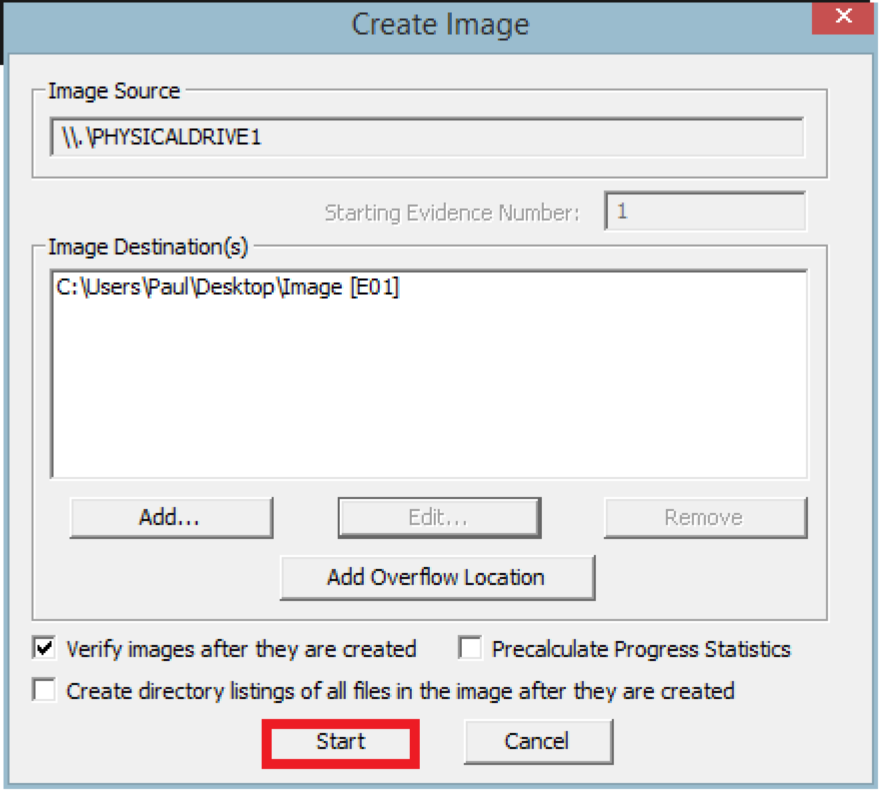
Image Filename (Excluding Extension)

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest): 1

Use AD Encryption □

< Back | Finish | Cancel | Help



Create Image

Image Source

\\.\PHYSICALDRIVE1

Starting Evidence Number: 1

Image Destination(s)

C:\Users\Paul\Desktop\Image [E01]

Add... | Edit... | Remove

Add Overflow Location

☑ Verify images after they are created

□ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created

Start | Cancel

Logical Acquisition

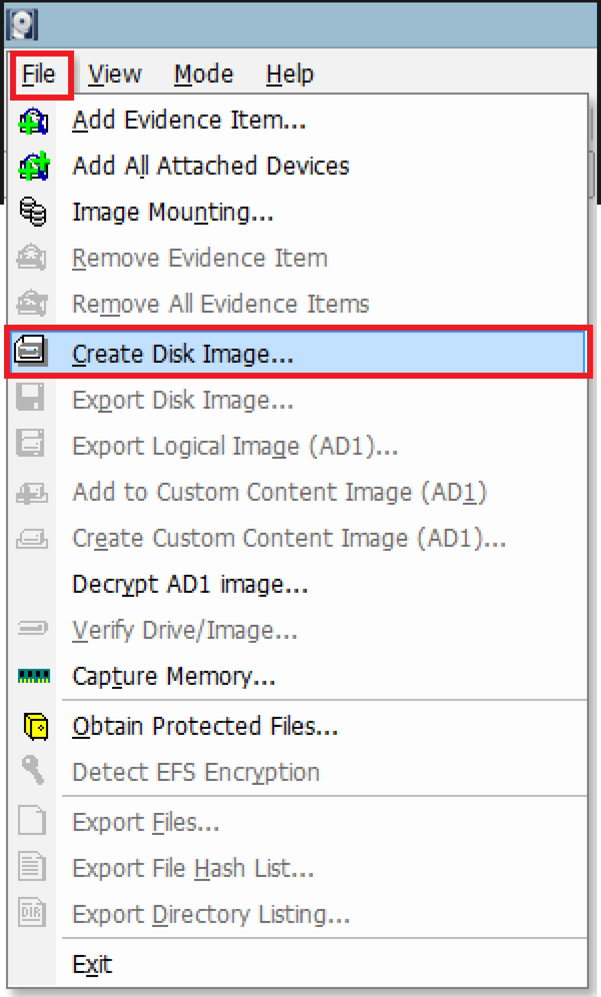
- Logical Acquisition does not include entire hard drive
- It only includes
  - Partitions
  - Files within those partitions
  - Allocated space only

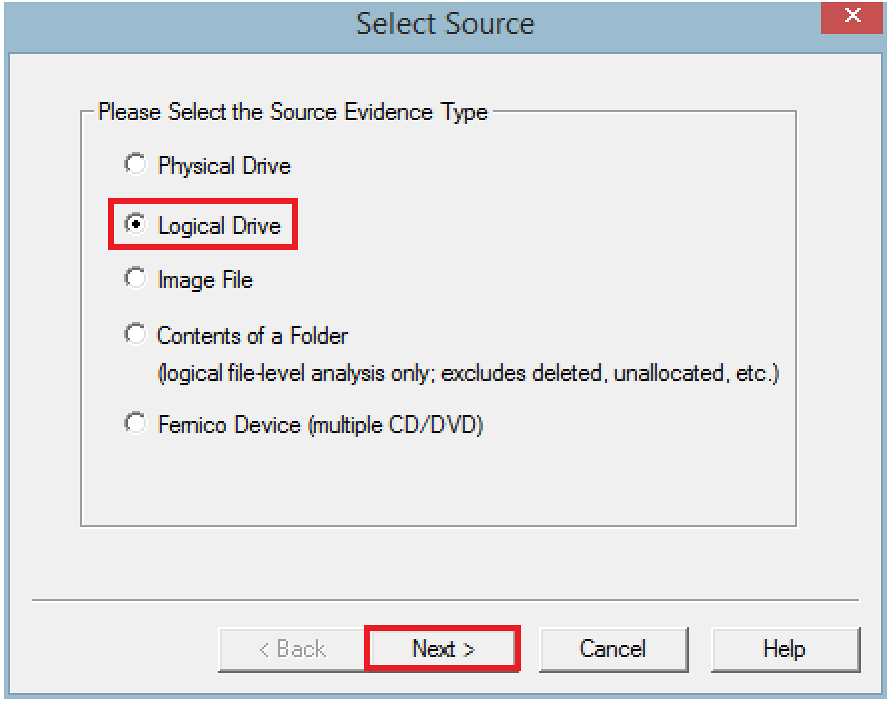
Step-By-Step

- After downloading and installing from here, open FTK Imager by right-clicking and selecting “run as administrator”
- To perform a logical acquisition, select “File” then “Create Disk Image”
- Select “Logical Drive” and click “Next”
- First make sure the drive you want to image is connected to the computer via “Disk Manager” then in FTK Select the drive you want to acquire and click “Finish”
- A new window will appear. Select “Add” and select “E01” and press “Next”
- Fill out the case information as well as a description of the evidence and press “Next”

Step-By-Step (cont.)

- Select the folder to save the Image to as well as input a Filename for the Image file.
- If you want the Image to be processed quickly make sure to put the compression at 0. However this will make the file size bigger. Keep this in mind. Also, FTK fragments files by default so if you simply want one large file set this number to 0. Otherwise, keep it at its default value.
- If you want to encrypt the file, select the box “Use AD Encryption”
- Then Select “Finish”
- Finally select “Start” to acquire the Image




Select Source

Please Select the Source Evidence Type

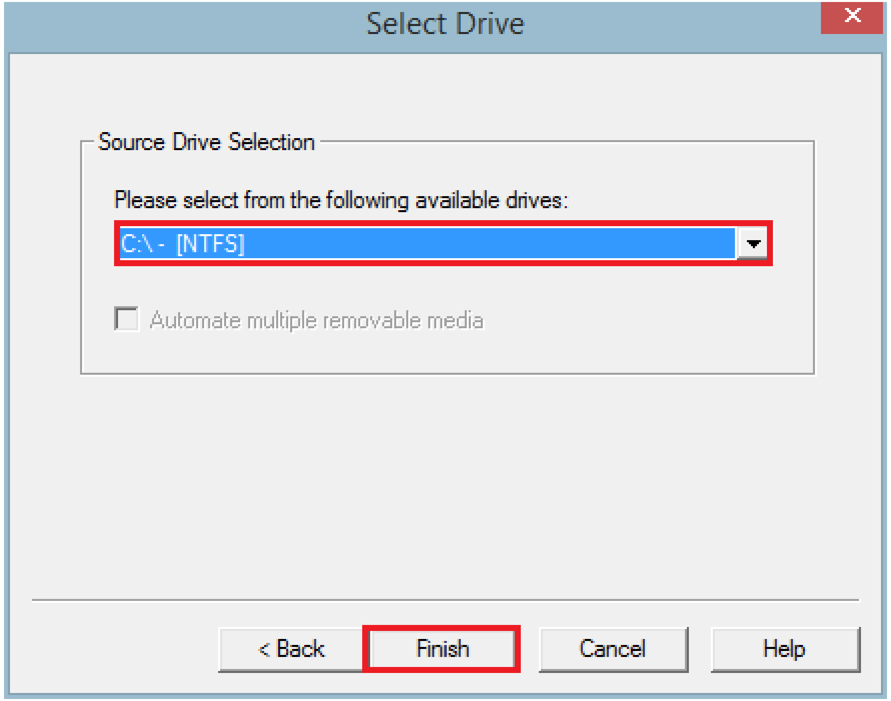
○ Physical Drive

● Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Femico Device (multiple CD/DVD)



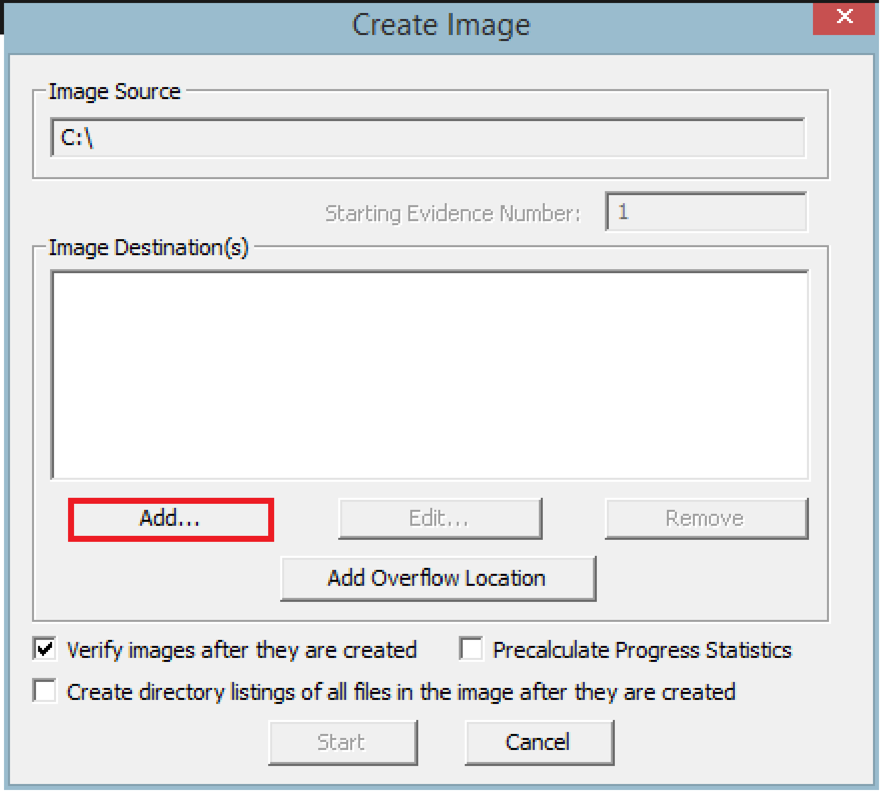
Select Drive

Source Drive Selection

Please select from the following available drives:

C:\ - [NTFS]

□ Automate multiple removable media



Create Image

Image Source

C:\

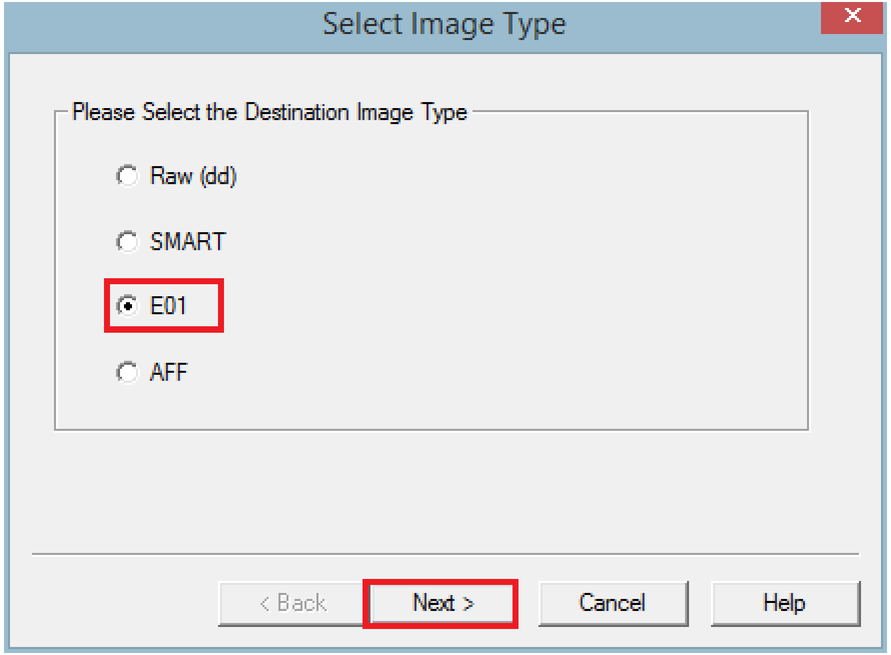
Starting Evidence Number: 1

Image Destination(s)

☑ Verify images after they are created

□ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created



Select Image Type

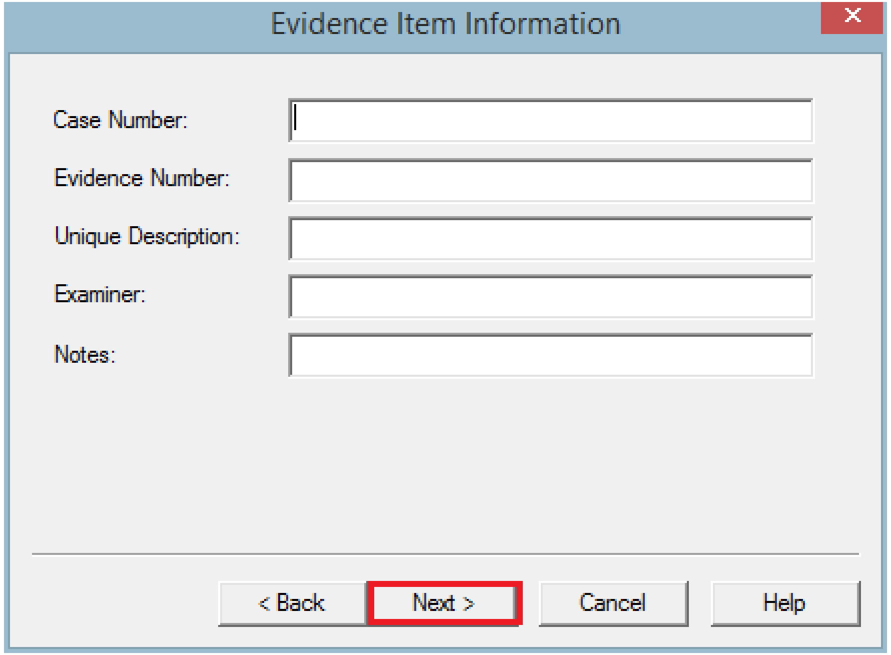
Please Select the Destination Image Type

○ Raw (dd)

○ SMART

● E01

○ AFF



Evidence Item Information

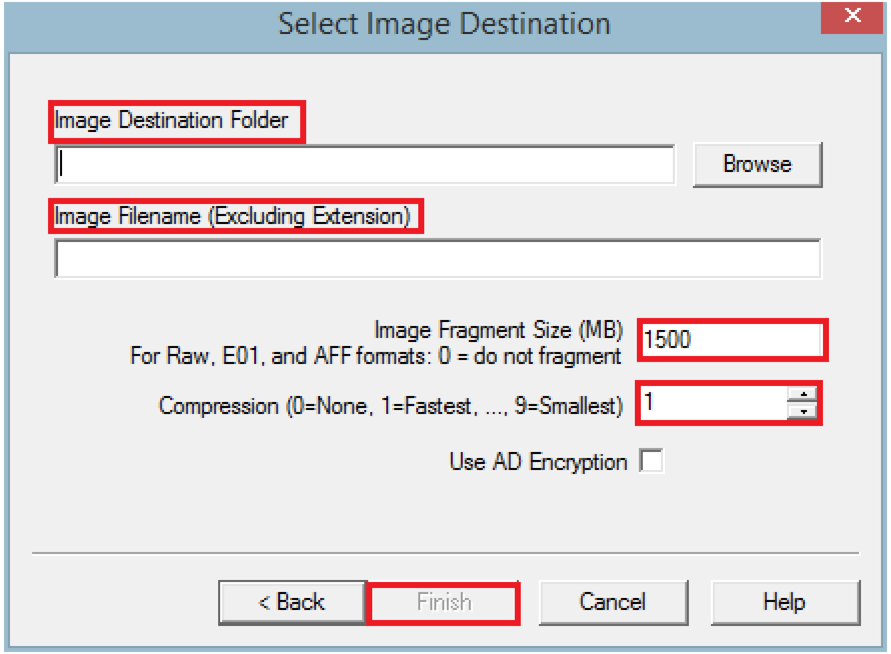
Case Number:

Evidence Number:

Unique Description:

Examiner:

Notes:



Select Image Destination

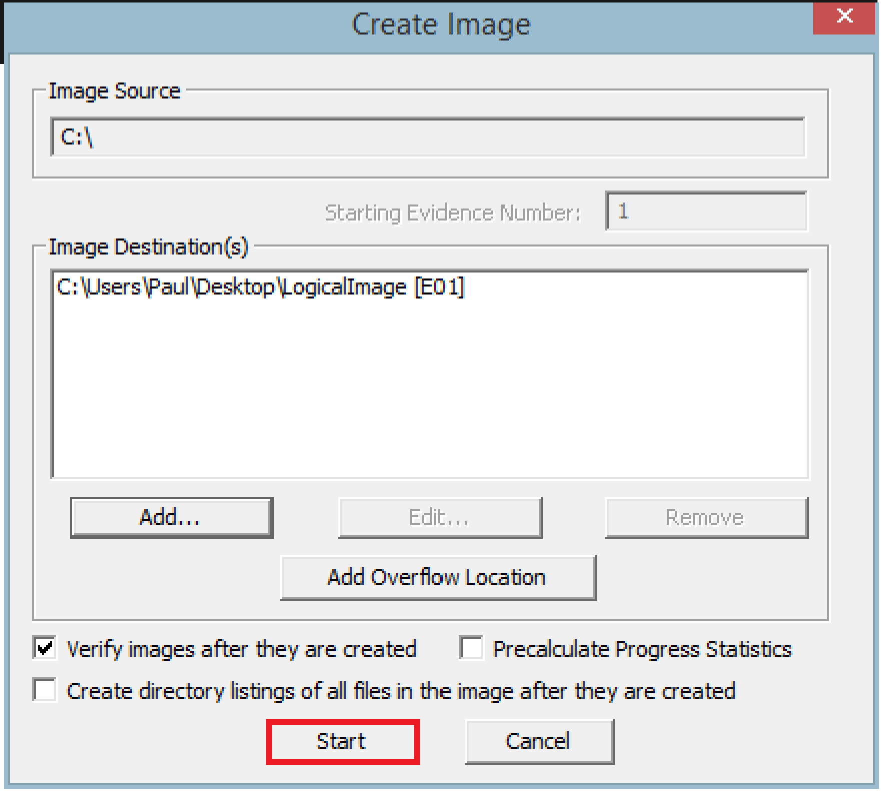
Image Destination Folder

Image Filename (Excluding Extension)

Image Fragment Size (MB) 1500
For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest) 1

Use AD Encryption □



Create Image

Image Source

C:\

Starting Evidence Number: 1

Image Destination(s)

C:\Users\Paul\Desktop\LogicalImage [E01]

☑ Verify images after they are created

□ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created

File/Folder Acquisition

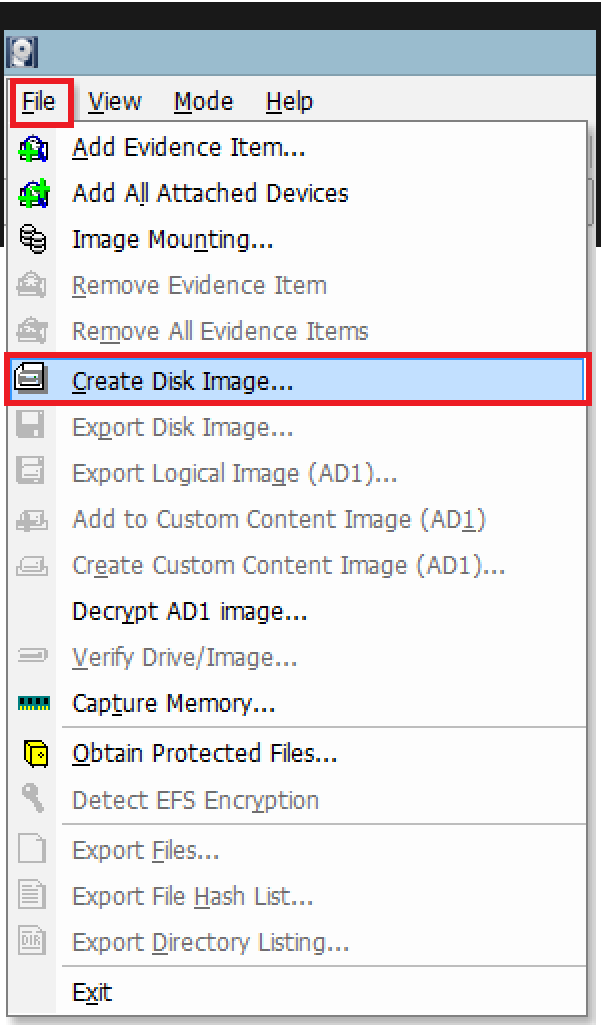
- As the name implies
    - only includes particular files or folders on a hard drive to be imaged

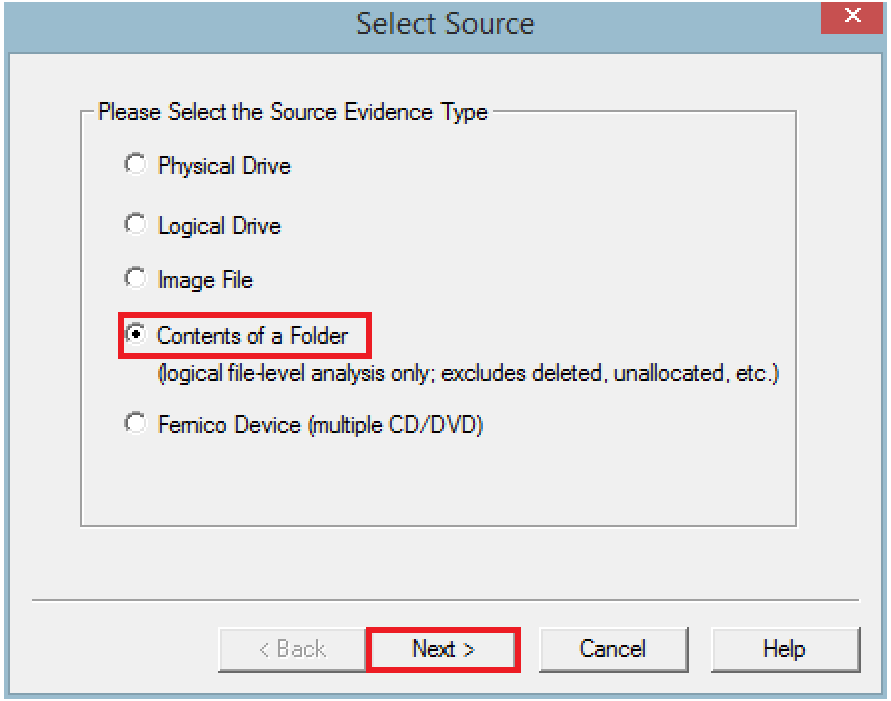
Step-By-Step

- After downloading and installing from here, open FTK Imager by right-clicking and selecting “run as administrator”
- To perform a folder acquisition, select “File” then “Create Disk Image”
- Select “Contents of a Folder” and click “Next”
- A Window will appear that explains some of the problems with Folder only acquisitions. Simply press “Yes” to continue
- Next choose the Folder you would like to image. Then press “Finish”
- A new window will appear. Select “Add”
- Fill out the case information as well as a description of the evidence and press “Next”

Step-By-Step (cont.)

- Select the folder to save the Image to as well as input a Filename for the Image file.
- If you want the Image to be processed quickly make sure to put the compression at 0. However this will make the file size bigger. Keep this in mind. Also, FTK fragments files by default so if you simply want one large file set this number to 0. Otherwise, keep it at its default value.
- If you want to encrypt the file, select the box “Use AD Encryption”
- Then Select “Finish”
- Finally select “Start” to acquire the Image





Select Source

Please Select the Source Evidence Type

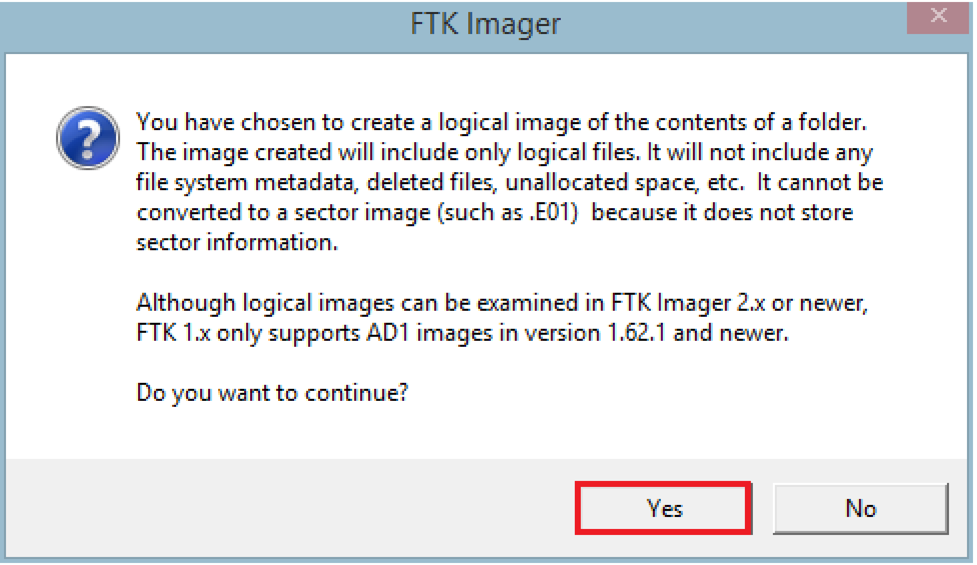
○ Physical Drive

○ Logical Drive

○ Image File

● Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Femico Device (multiple CD/DVD)

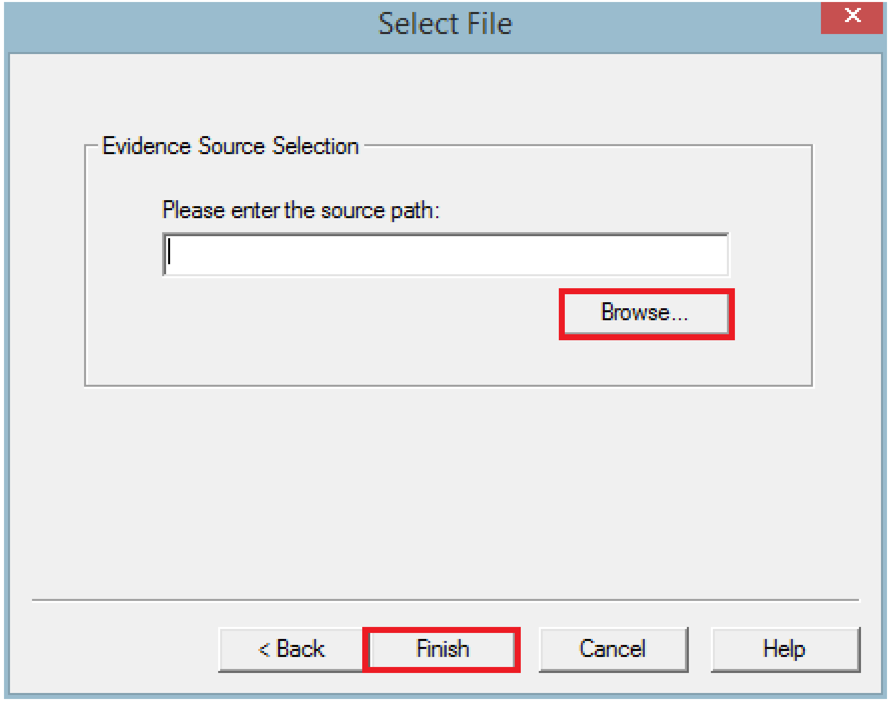


FTK Imager

You have chosen to create a logical image of the contents of a folder. The image created will include only logical files. It will not include any file system metadata, deleted files, unallocated space, etc. It cannot be converted to a sector image (such as .E01) because it does not store sector information.

Although logical images can be examined in FTK Imager 2.x or newer, FTK 1.x only supports AD1 images in version 1.62.1 and newer.

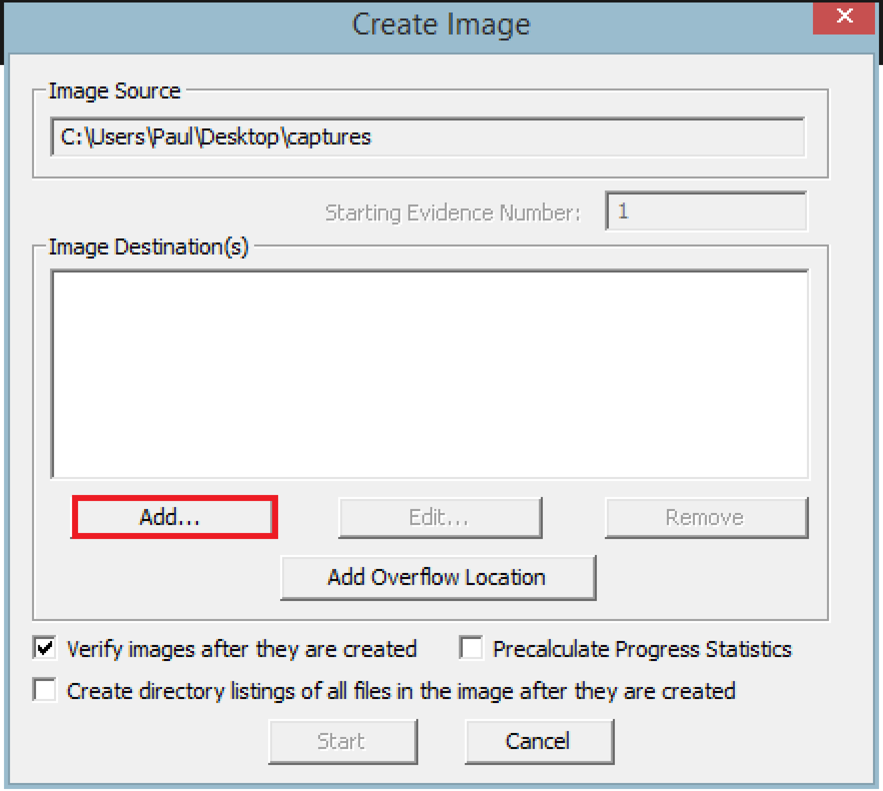
Do you want to continue?



Select File

Evidence Source Selection

Please enter the source path:



Create Image

Image Source

C:\Users\Paul\Desktop\captures

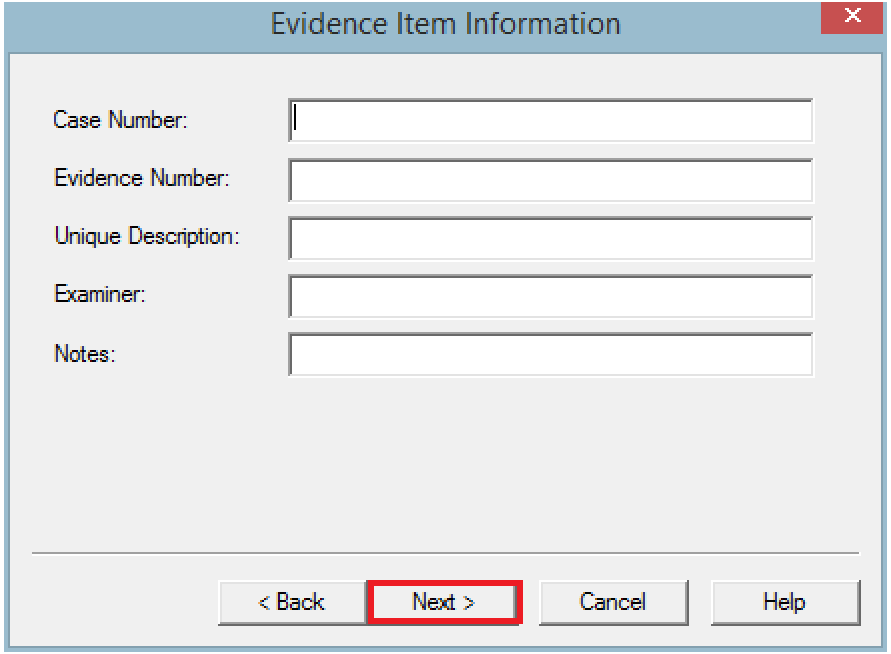
Starting Evidence Number: 1

Image Destination(s)

☑ Verify images after they are created

□ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created



Evidence Item Information

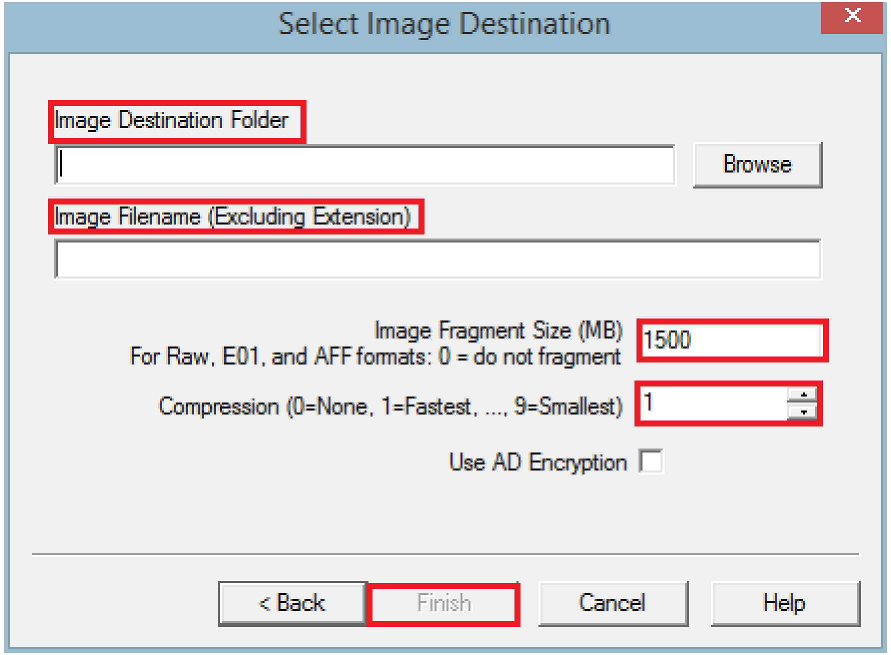
Case Number:

Evidence Number:

Unique Description:

Examiner:

Notes:



Select Image Destination

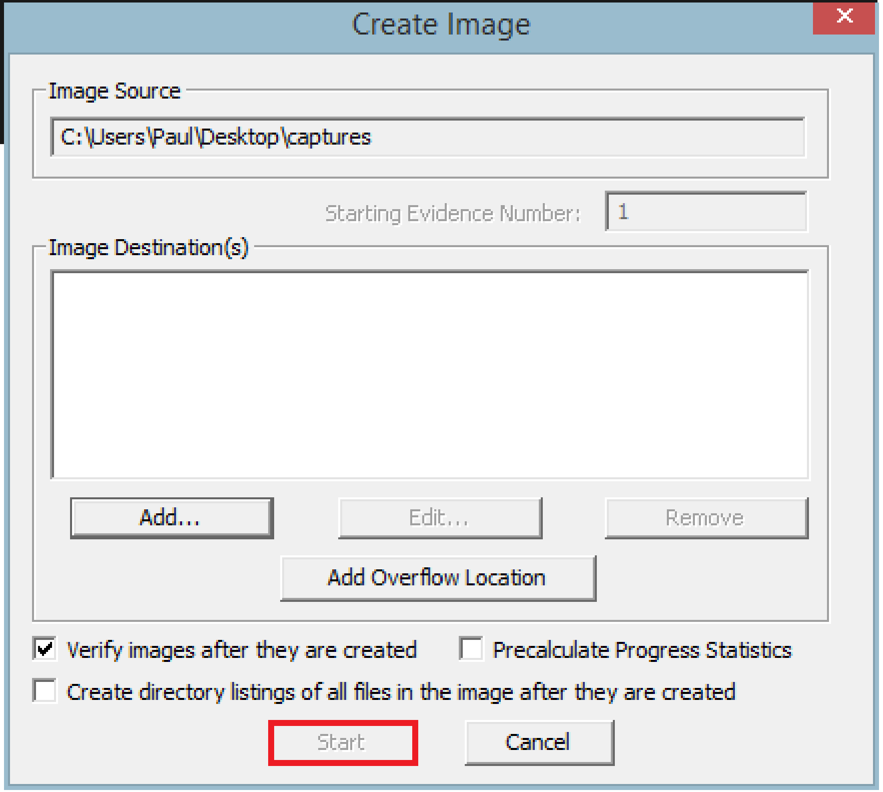
Image Destination Folder

Image Filename (Excluding Extension)

Image Fragment Size (MB) 1500
For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest) 1

Use AD Encryption □



Create Image

Image Source

C:\Users\Paul\Desktop\captures

Starting Evidence Number: 1

Image Destination(s)

☑ Verify images after they are created

□ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created

Conclusion

- Now you can correctly conduct forensic acquisitions of your own
- For more information on AccessData and FTK Imager click the link here