# FTK Imager Walkthrough

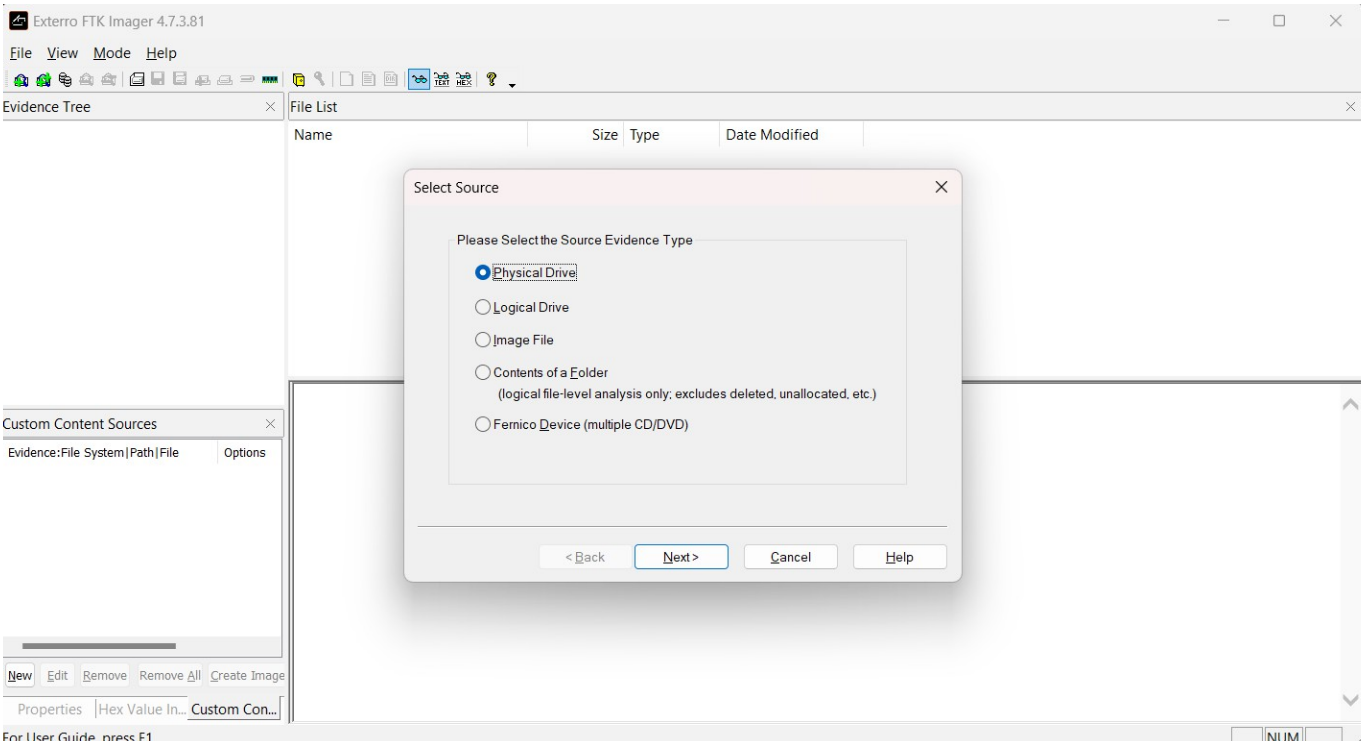
## Introduction to FTK Imager

FTK Imager is a GUI based tool that is used to make forensic images of Flash Drives, Disks, Partitions and Volatile Memory. You can preview the contents of the forensic images stored on the local machine or on the network drive. It can also mount an image and leverage the power of Windows File Explorer to see the content on the original drive as is.

## Installing FTK Imager

FTK Imager is downloaded from the website FTK Imager. Just go to the website and click on the Download button. This will take you to another website to fill in data. You don't have to give your real information. Use 33mail or 10minutemail to create a dummy account. It does not ask for verification. Once you launch the downloaded application, it will install FTK Imager into the path that you choose. Follow the steps displayed by the wizard and you will have FTK setup.

## Making a Forensic Image



Select Source

Please Select the Source Evidence Type

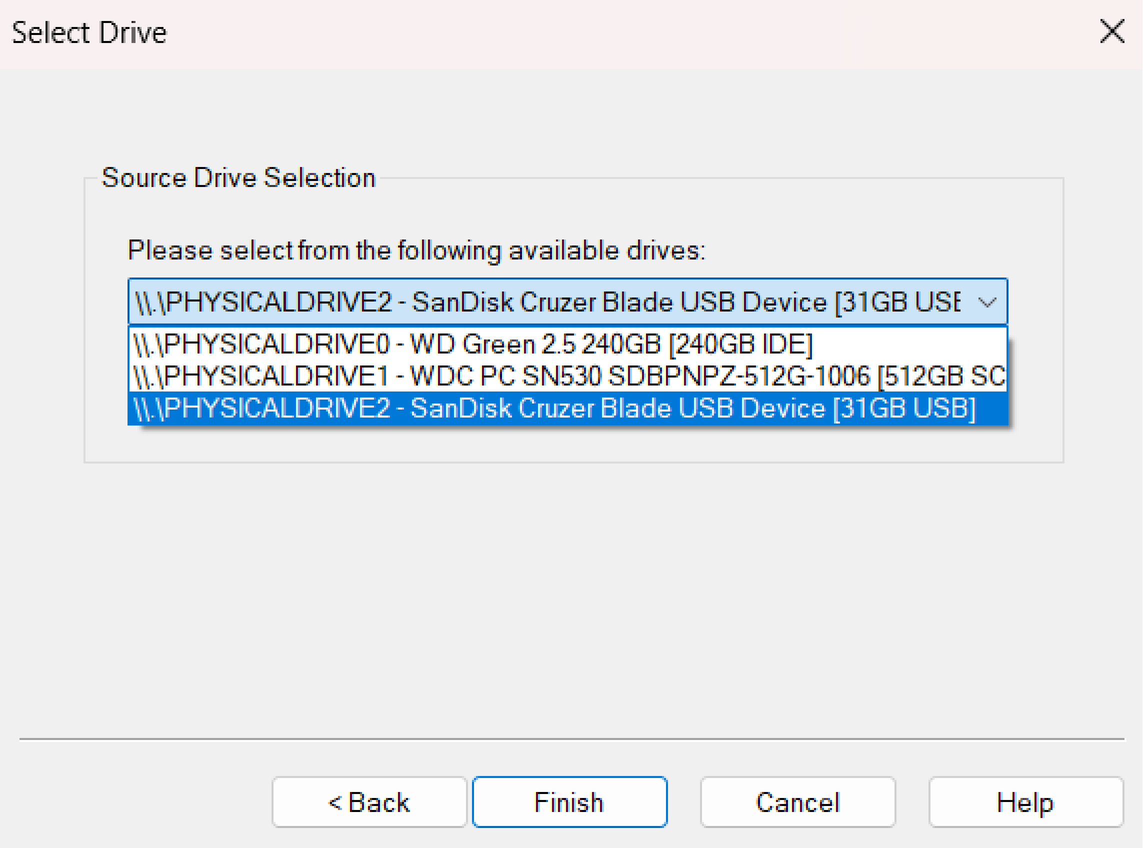
● Physical Drive
○ Logical Drive
○ Image File
○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
○ Femico Device (multiple CD/DVD)

< Back | Next > | Cancel | Help

With FTK Imager's "User Friendly" UI, you can easily make images of Physical Drives and Logical Drives. The difference between the two is quite simple. Physical Drive is the complete Physical Disk. It is the equivalent of `/dev/nvme0n1` on Linux, while a Logical Drive is the partition we created like `C:` or `D:`

## Physical Drive

Let's now connect a Flash Drive to the computer and make a Forensic Image of that USB



Select Drive

Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE2 - SanDisk Cruzer Blade USB Device [31GB USE

\\.\PHYSICALDRIVE0 - WD Green 2.5 240GB [240GB IDE]
\\.\PHYSICALDRIVE1 - WDC PC SN530 SDBPNPZ-512G-1006 [512GB SC
\\.\PHYSICALDRIVE2 - SanDisk Cruzer Blade USB Device [31GB USB]

We see a list of Physical devices here and we choose the one that we want to make an image of. In this case SanDisk Cruzer Blade is the Flash Drive that we want to make an image of.
Select it, and then click on `Finish`

This will lead us to another set of questions asking which format we want to use, where we want to save it, if we want to Verify after Imaging etc. Answer all these questions as per your need, and then clic `Start`

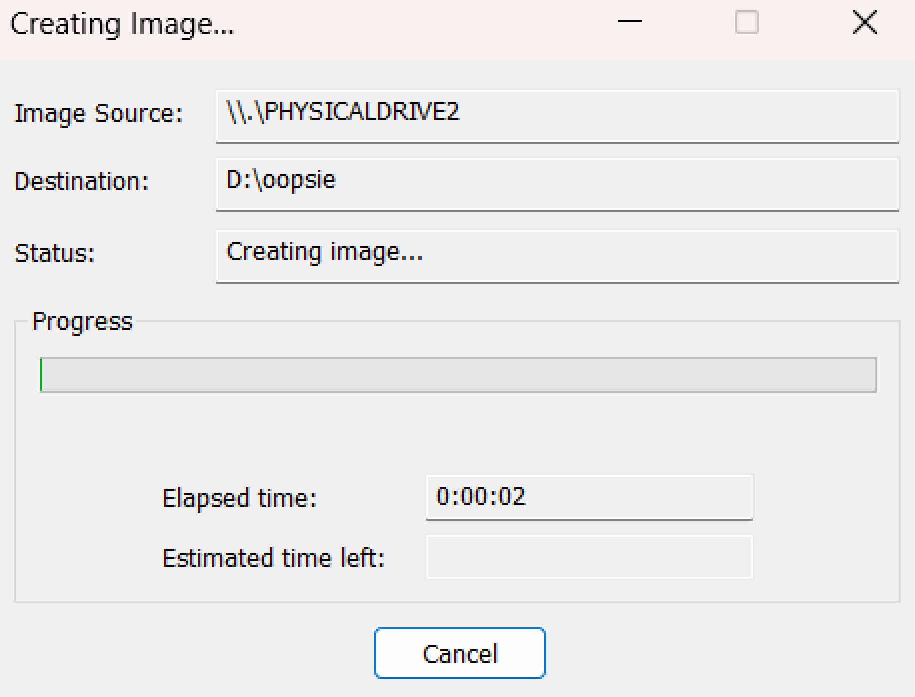

Creating Image...

Image Source: \\.\PHYSICALDRIVE2

Destination: D:\oopsie

Status: Creating image...

Elapsed time: 0:00:02

Estimated time left:

This is how it should be creating the Forensic Image. Once it is done, it will be stored in the folder of your choice

Once this is done, FTK Imager will display the results of the verification of the forensic image and compare them with the original. The `Verify Result` will be labeled as `Match` if the two images have the same Hash Values

In the same directory as the forensic images, there will be a text file which contains the details about the forensic image. It contains information about the media, file hashes and details that you entered while creating the image.

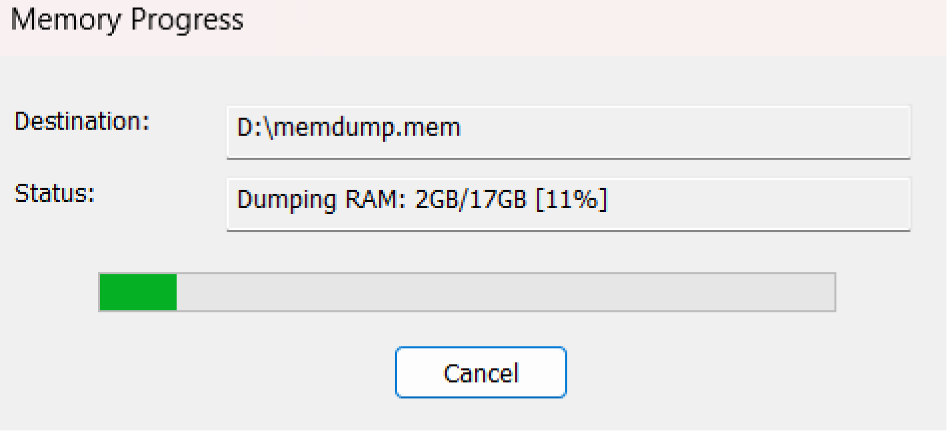
Congratulations! You made a forensic image of a physical drive.

## Logical Drive

To create a forensic image of a logical partition, you can go through the same process, but instead of choosing Physical Drive, you choose Logical Drive. No screenshots for this, because it's the exact same procedure as above, but instead of choosing Physical Drive, you choose Logical Drive. Everything else remains the same

## Memory

One thing that FTK Imager can do, but `dd` and `Guymager` can't do is create Memory Dumps. FTK Imager allows you to create Memory Dumps by clicking on the `Capture Memory` button. This starts making a memory dump at the destination file that you chose



Memory Progress

Destination: D:\memdump.mem

Status: Dumping RAM: 2GB/17GB [11%]

The reason why we want to capture the RAM is because a huge amount of information can be stored in the RAM without us noticing. Some information that can be stored in RAM includes:

- Temporary Data
- Encryption Keys
- Encrypted Data
- Deleted Data Fragments

## Disadvantages

- It's a Windows-Only Software, which is kinda sad cause Linux is the chosen OS for making these kinds of Investigative Environments
- Slow Performance with large datasets. When a physical drive that is very large is to be imaged, it will take a long time as it cannot optimized for handling high-volume data