

Digital Forensics 101 : Capturing a Forensic Image

Digital forensics is one of the most important step of L3 investigations. To analyze effectively, you need to collect data carefully.

Before any forensic investigation or analysis can begin, a forensically sound image must be captured of the data storage device. These forensically sound images must be a bit-by-bit, physical copy of the device. Without such a copy, any evidence will likely be inadmissible in a court of law.

There are multiple ways to capture forensic image of a storage device. We will look a few of the most popular methods here.

1. Using Linux/UNIX dd command

The Linux dd command is built into nearly distribution of Linux. It simply copies a storage device bit-by-bit from a input or source file (if) to an output or destination file (of). We can use it here with our Kali, or for that matter any Linux distribution, to do this.

First, we need to find out how our USB flash drive is represented in the Linux operating system. We can do this by typing;

```
kali > fdisk -l
```

To then capture the flash drive entirely, we simply need to invoke the dd command followed by the input file if=/dev/sdb and then the output file. This can be anything we want to name our output file. Here I will name it usbimage.dd.

```
kali > dd if=/dev/sdb of= usbimage.dd
```

After hitting enter, the dd command will begin to copy, bit-by-bit, the data from the USB drive to the file we designated usbimage.dd. If we want to check to see whether anything is actually happening, we can open another terminal window and type ls -l.

dd represents the most basic of all image capture techniques and creates the foundation used in many other methods

2. Using dcfldd

A few years back, the Department of Defense Computer Forensics Lab (dcfl) developed of an open source version of dd specifically designed for creating forensic images. While the dd command is a generic command for copying storage devices, this command has options tailored for creating forensic images, but at its heart, it is still dd.

dcfldd has the capabilities to;

- hash the image on the fly
- a progress bar
- wiping disks
- verification that the new image is identical to the original
- simultaneous output to multiple files or disks
- logs and output can be piped to external applications

Like dd, dcfldd can ONLY produce raw images.

To create a forensically sound image of our USB flash drive, we can use `dcfldd` similarly to `dd`, but we have more options. So for instance, if we wanted to create a MD5 hash of the image (a good idea), we can type;

```
kali > dcfldd if=/dev/sdb of= usbimage2.dd hash=md5 hashlog=usbimage.log
```

When `dcfldd` has completed its imaging, it responds by telling how many blocks were written and how many blocks went in and how many blocks out.

Once the capture is complete, we can then check to see whether the images and log have been completed by typed `ls -l`.

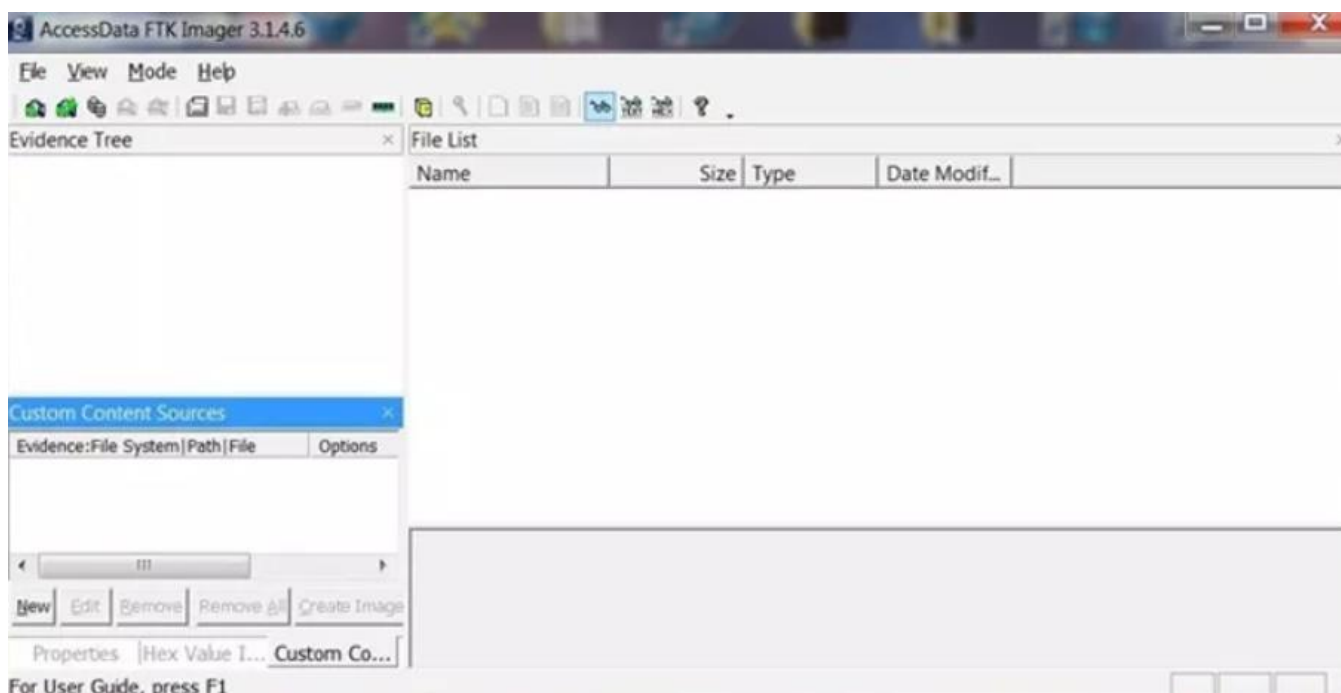
`dcfldd` is an excellent, if rudimentary, tool for creating forensically sound device images. Very few frills and no GUI, but fast and straightforward.

3. FTK Imager

The software developer, Access Data, sells a forensic suite known as the Forensic Tool Kit or FTK. As part of that suite of tools they have developed a tool known as the FTK Imager. This tool is designed specifically to create forensically sound images with a easy to use GUI. They have long provided this tool for free and as a result it has become the tool of choice in many forensic environments for creating forensically sound images.

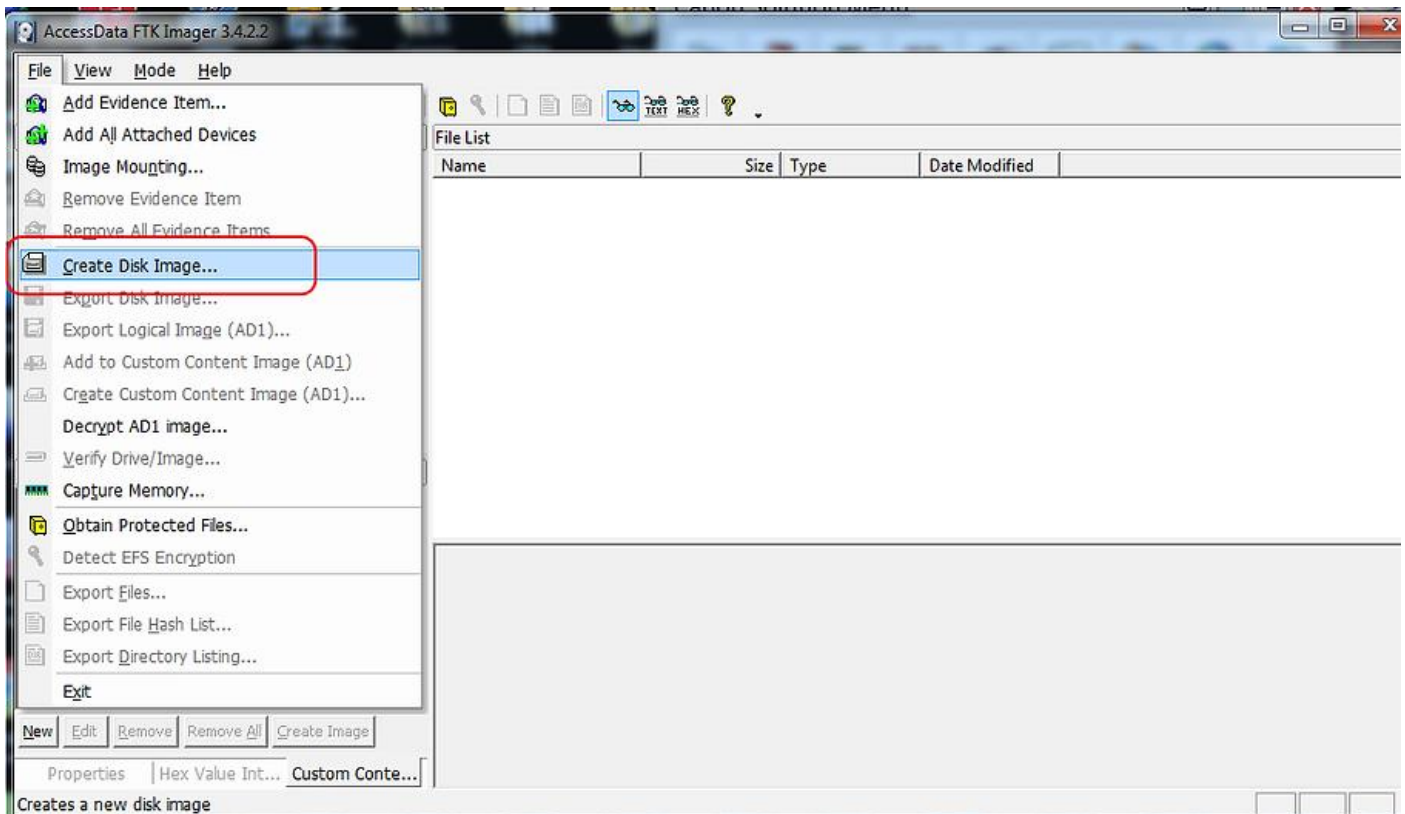
You can download the FTK Imager at www.accessdata.com/downloads.

After installing and executing FTK Imager, you will be greeted with a familiar interface like that below.



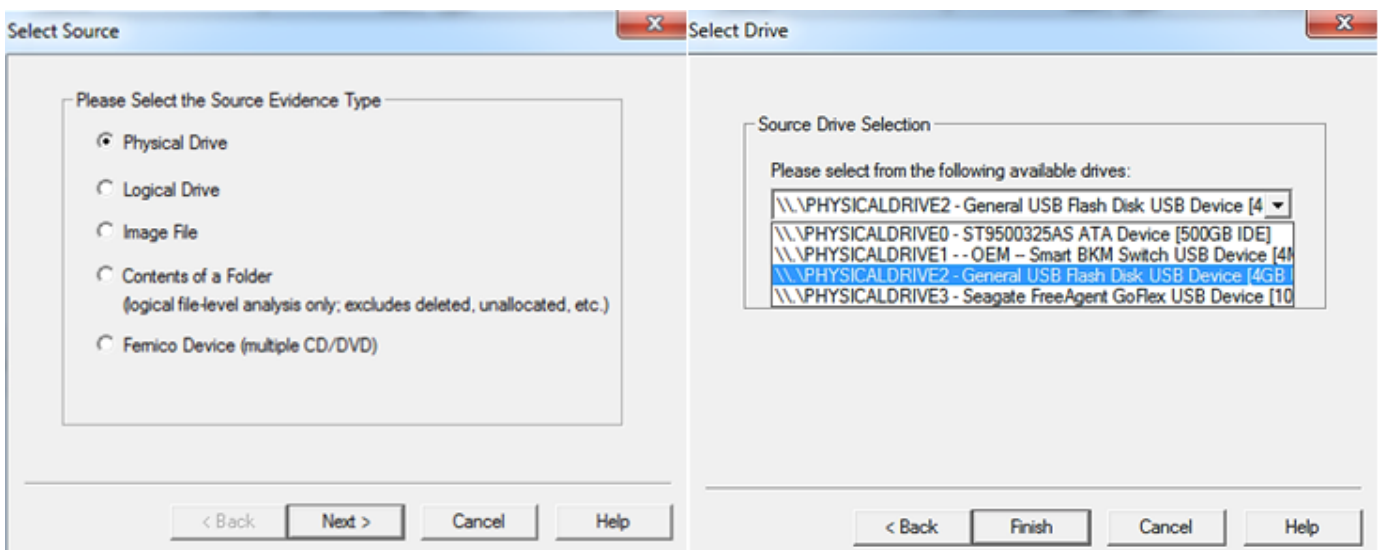
Note that like many Windows applications, it has the familiar top-line pull-down menus starting with "File".

Click on "File" and go to "Create Disk Image".



When you so, it will open a window like that below. Select "Physical Drive"

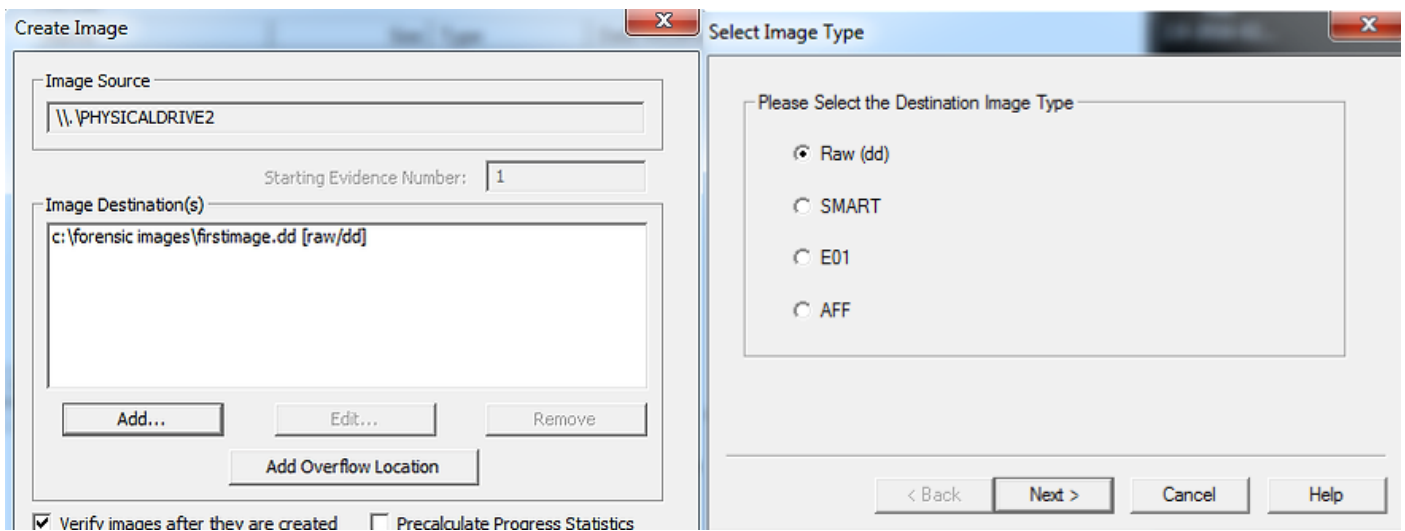
This will open another window asking you to select the source drive location. Here, I have selected "General USB Flash Disk". Yours may be slightly different.



Click "Finish" after selecting the device.

Next, you will be prompted to enter the "Image Destination". Click "Add". Note also that I have indicated in the lower left corner that I want the images verified after they are created.

You should then be prompted for the type of image you would like to create. Select a "Raw" or dd image.



After we have entered all that information about our image creation, FTK Imager will prompt us to create a case. The case creation process requires;

- a case number
- evidence number
- a unique description
- the examiners name
- notes

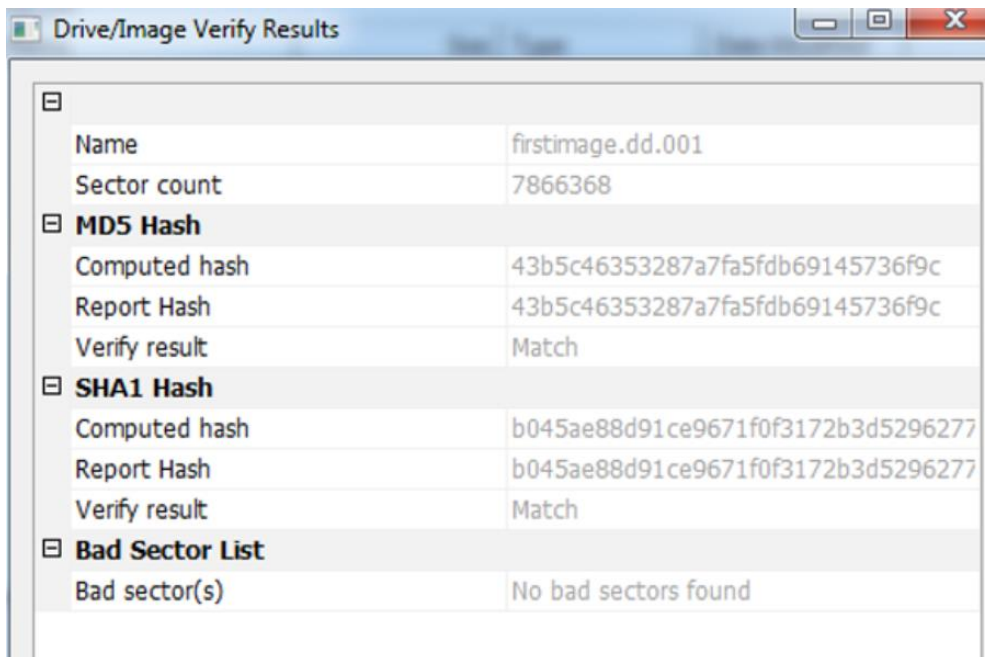
Fill in this form appropriately and hit "Next". We will next be prompted for the image destination. Here, I have created a folder specifically for forensic images named unimaginatively, c:\forensic images. I have also named the image file, "firstimage.dd".

Now, click "Finish". You will now be returned to the "Create Image" window. Click "Start".

FTK Imager will now begin the time consuming process of copying the device, bit-by-bit to the file you have designated.

When it has successfully completed, you will see it stop and in the status window you will see "Image created successfully". It will then begin to try to verify that that the newly created image is identical to the original.

Finally, when the image verification is complete, click on "Image Summary" and it will open a window of summary statistics on the image including the all important hashes like that below.



The screenshot shows a window titled "Drive/Image Verify Results". It contains a table with the following data:

[-]	
Name	firstimage.dd.001
Sector count	7866368
[-] MD5 Hash	
Computed hash	43b5c46353287a7fa5fdb69145736f9c
Report Hash	43b5c46353287a7fa5fdb69145736f9c
Verify result	Match
[-] SHA1 Hash	
Computed hash	b045ae88d91ce9671f0f3172b3d5296277
Report Hash	b045ae88d91ce9671f0f3172b3d5296277
Verify result	Match
[-] Bad Sector List	
Bad sector(s)	No bad sectors found

Success! We have created a forensically sound image of our USB device, verified that it identical to the original and generated both a MD5 hash and a SHA1 hash.

In this tutorial, we have created a forensically sound image using the three (3) most popular methods. This is usually the first step in any investigation and is critical to the overall success of the investigation. Without a good image, any further work invested in the investigation may assumed wasted.