

How-To Guide

Image a Hard Disk Using FTK Imager



Document Version 1.0
June 24, 2011
Michael G. Spohn
mspohn@malware-hunters.net

Introduction

This document is a member of the 'How-To' series of guides provided to interested parties by malware-hunters.net. In this guide, we walk you through the steps to image a hard disk using Access Data's free FTK Imager tool.

In our forensic work, we are often asked how non-incident responders (e.g. IT folks) should obtain forensic images of hard drives. This is a common requirement when doing malware containment or when you need to obtain a disk image from a computer in an off-shore or other remote location.

It *must* be noted here – the *proper* way to acquire a forensic image of a hard drive is to use the proper hardware and software. This includes write-blockers, and forensic acquisition software that has proven reliable by the courts. Plus the only way to get a *true* image of a hard drive is to do a dead-disk acquisition.

Now that the 'proper-way' lecture is over, let's explore a reliable acquisition method that you can use to image a hard disk or disk volume.

Requirements

You will need two things to acquire a hard disk image:

- Access Data's FTK Imager.
This venerable tool is used by every forensic analyst I have ever met. It is a truly remarkable and versatile piece of software. There are two versions. The standard version comes with an installer package and requires installation on a Windows host. The second version (FTK Imager Lite) is a self-contained file set that you can run from removable media such as a CD/DVD or USB thumb drive. This is the version I will use in this 'How-To.'

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

- An external USB hard disk to hold the acquired image file(s).
Obtain a hard disk large enough to hold your acquired image. In this 'How-To' I used a 320GB external USB hard drive. They are readily available at your local computer store, are inexpensive, very compact, and reasonably rugged. I purchased the Seagate USB drive used in this guide from Wal-Mart for less than \$75. In this 'How-To' I will refer to this drive as your 'evidence' disk. I will refer to the disk you are making an image of the 'suspect' disk.

I strongly encourage you to consider encrypting your evidence disk prior to using it. I have written a detailed 'How-To' titled "*Encrypt a Hard Disk Volume Using TrueCrypt*" that explains how to do this. You can find the document at: www.malware-hunters.net/how-to.

- SysInternal's SDelete Tool

SDelete is a handy command line tool that writes zeros to all the free space on a disk volume. We will use this too to wipe the free space on the TrueCrypt volume of your evidence disk. You can find the SDelete tool here:

www.sysinternals.com/sdelete.

Preparing the Evidence Disk

In this step, we prepare your evidence disk for use. I am going to assume you have followed the steps in the “Encrypt a Hard Disk Volume Using TrueCrypt” and have an external USB hard drive with a large encrypted volume.

- Wipe the TrueCrypt encrypted hard drive volume.

Prior to using a hard drive that will contain forensic image(s), I always wipe and verify the drive has no data on it. I suggest you do the same. It is very important you understand I am talking about wiping the data residing **on** the TrueCrypt volume **not** the TrueCrypt volume itself.

This is a three-step process. First plug the USB evidence drive into a workstation or laptop. Make sure you have TrueCrypt installed on this host or place the runtime files on a USB thumb drive. Start the TrueCrypt application (Figure 1).

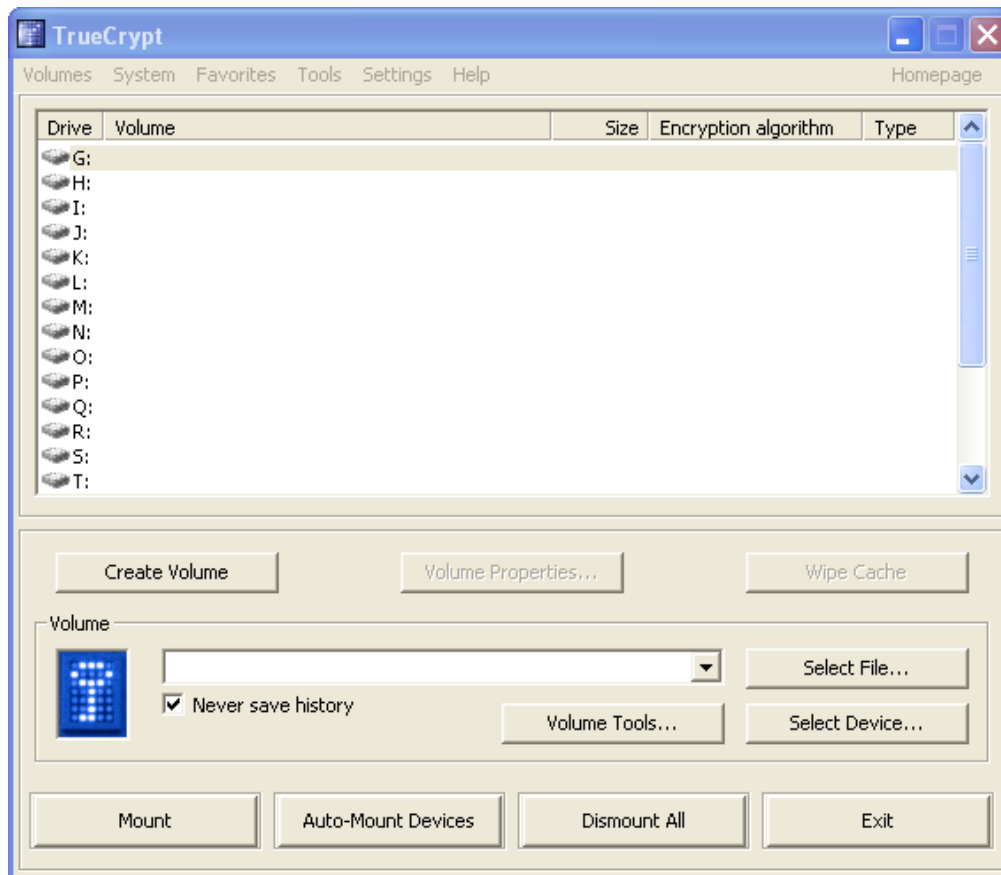


Figure 1 - TrueCrypt Application

Image a Hard Disk Using FTK Imager

Next, select the device you would like to mount by clicking on the 'Select Device...' button. From the 'Select a Partition or Device' window, select you USB drive encrypted partition and click 'OK' (Figure 2).

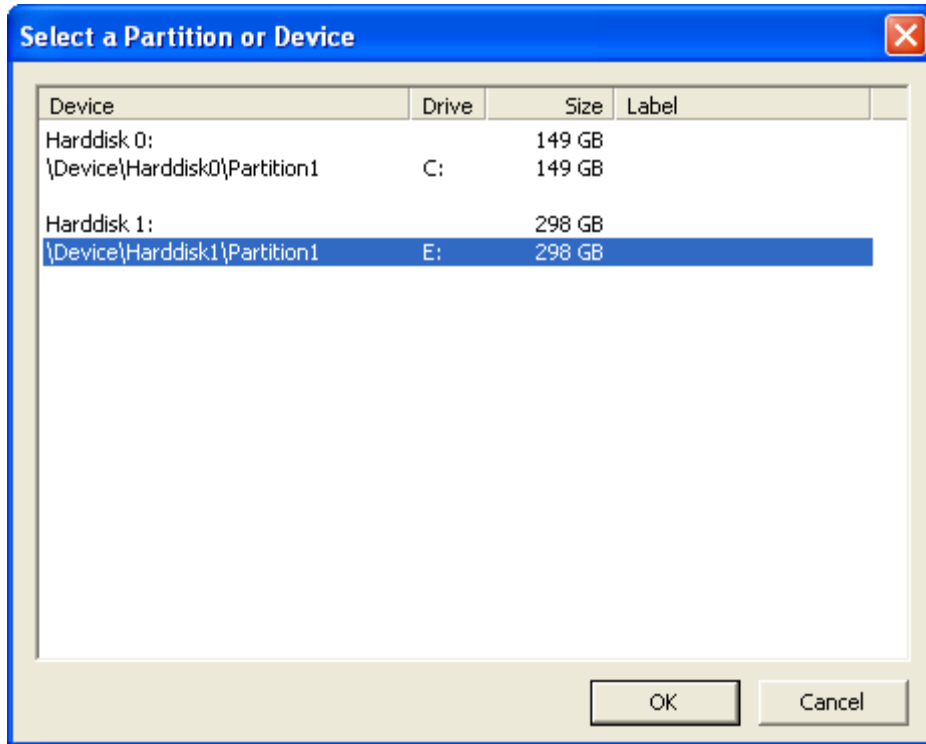


Figure 2 - Select TrueCrypt Device

Next, select a drive letter you would like to assign to the mounted TrueCrypt volume and then click 'Mount' (Figure 3).

Image a Hard Disk Using FTK Imager

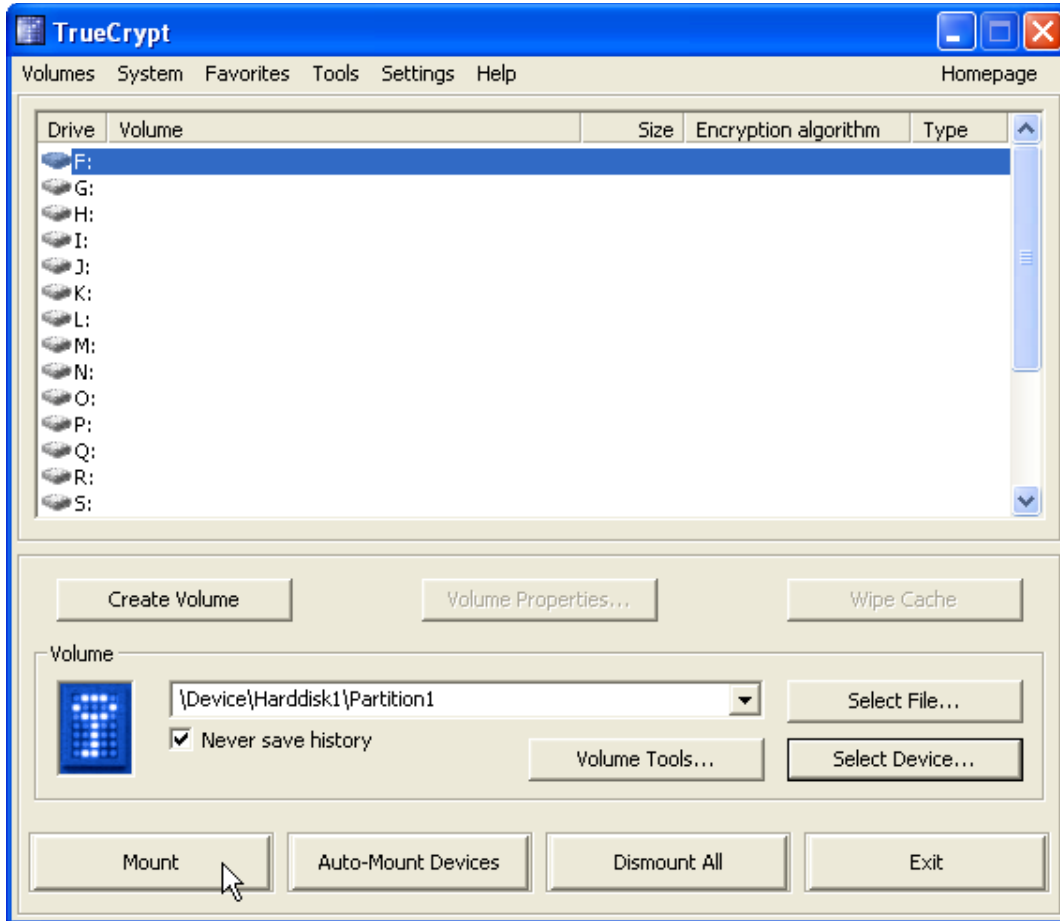


Figure 3 - TrueCrypt Mount Volume

Enter your encrypted volume password or click on 'Keyfile..' and provide the path to your keyfile (Figure 4).

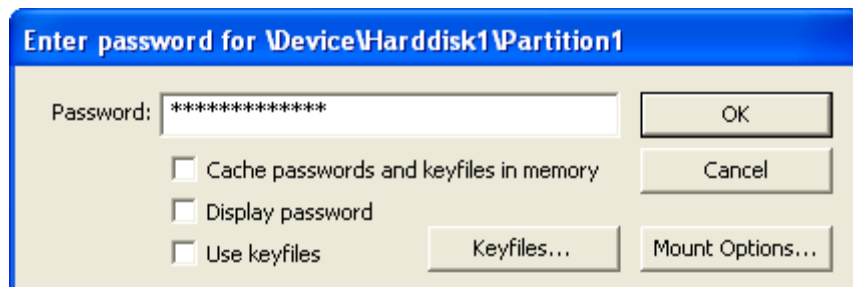


Figure 4 - TrueCrypt Password

Your encrypted volume should now be mounted and assessable. In my case, I chose drive F: (Figure 5).

Image a Hard Disk Using FTK Imager

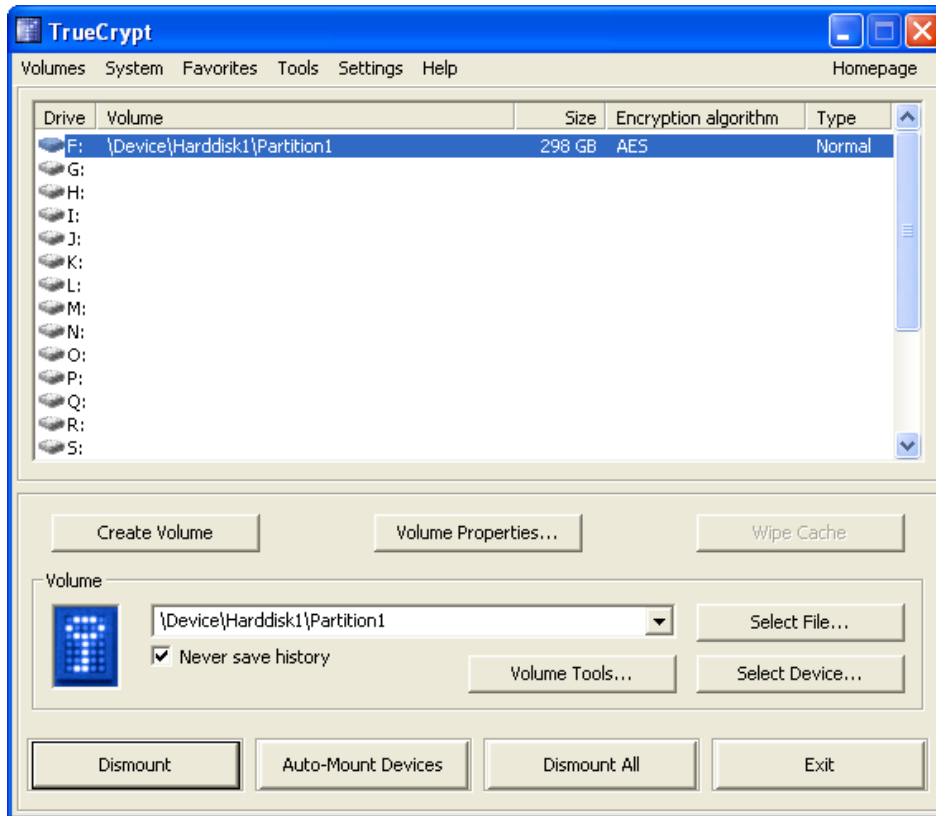


Figure 5 - Mounted TrueCrypt Volume

In my case, there are no files on my volume as shown in Figure 6.

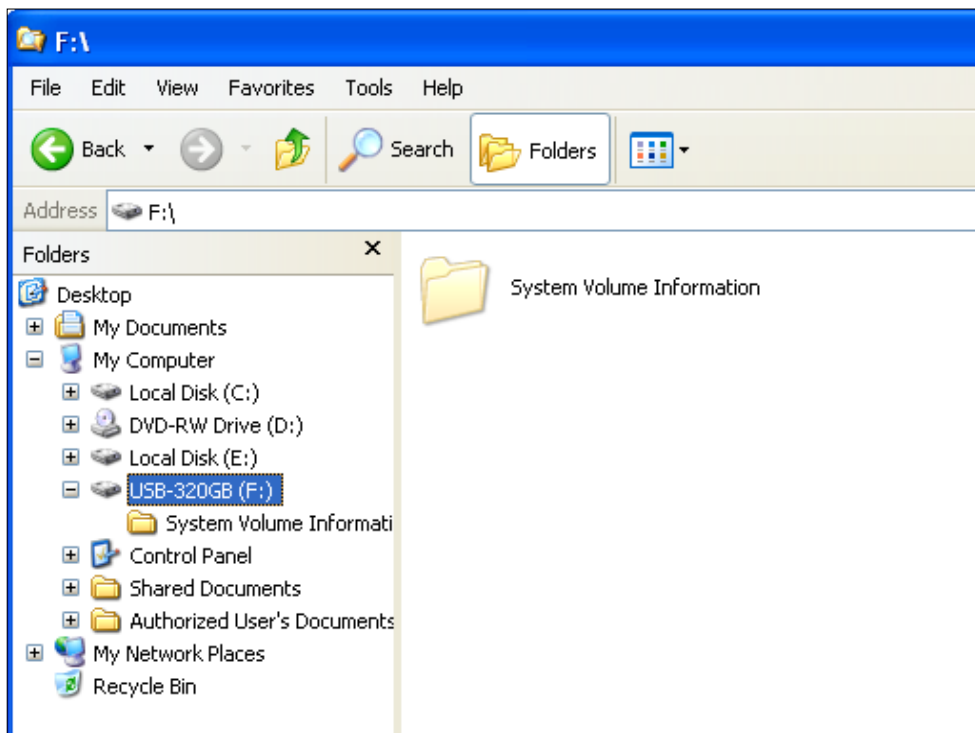


Figure 6 - Empty TrueCrypt Volume

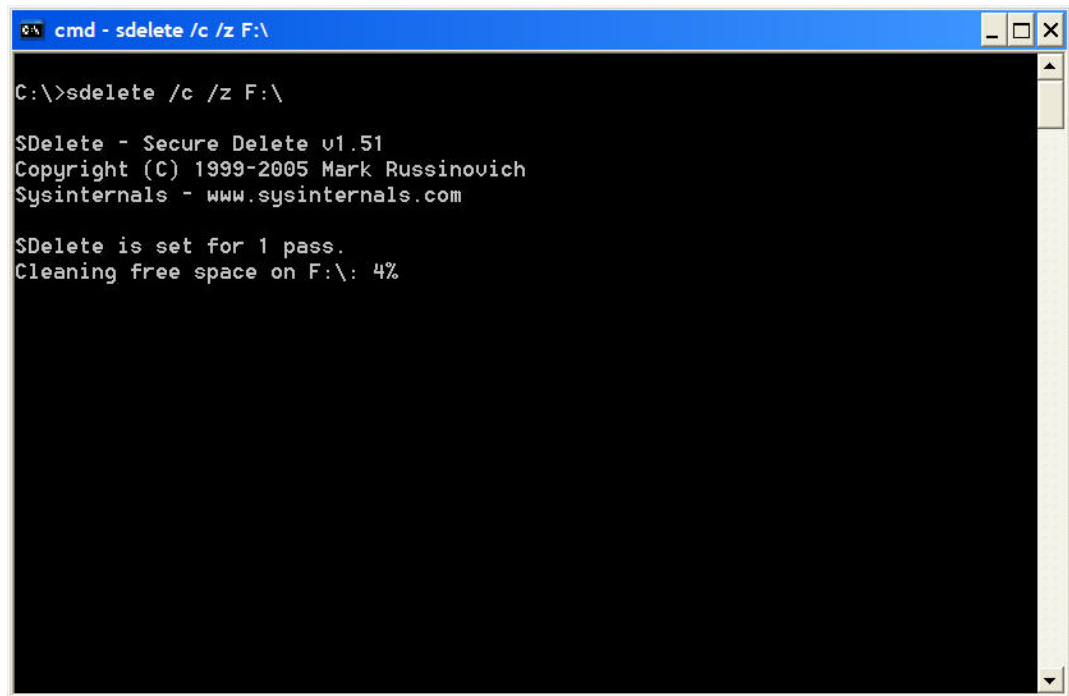
Image a Hard Disk Using FTK Imager

The final step in evidence disk preparation is to wipe the encrypted volume with SDelete. Make sure you have deleted *all* the files on the volume. Open a command window and execute SDelete using the below command:

```
SDelete /c /z F:\
```

Note: Replace the F:\ with the drive letter of your mounted encrypted volume.

SDelete will wipe all the free space on you encrypted volume as shown in Figure 7.

A screenshot of a Windows command prompt window titled "cmd - sdelete /c /z F:\". The window has a blue title bar and standard Windows window controls (minimize, maximize, close). The command prompt shows the following text:

```
C:\>sdelete /c /z F:\  
  
SDelete - Secure Delete v1.51  
Copyright (C) 1999-2005 Mark Russinovich  
Sysinternals - www.sysinternals.com  
  
SDelete is set for 1 pass.  
Cleaning free space on F:\: 4%
```

Figure 7 - SDelete in Action

Your evidence drive is now properly prepared to receive a forensic image. Dismount your TrueCrypt volume and place the disk in a secure location where you know it will not be tampered with. We always place the drives in anti-static bags and seal them with evidence tape.

Acquiring a Disk Image

In this step, we will use your prepared evidence disk to acquire an image of a live system using FTK Imager.

- Assemble the required tools.

Imaging a live system in this 'How-To' will require physical access to the system that you want to image. This means you will need to mobilize the toolset you are going to use. You will need your external USB evidence drive and a CD/DVD or USB thumb drive that has the TrueCrypt run-time files and FTK Imager Lite on it. I create two folders on my portable thumb drives: \TrueCrypt and \FTKImager and place the application files in their respective folders.

- Decide if you are going to image a physical or logical disk.

This distinction is important and depends on what your goals are. When you acquire a physical disk, you are creating an image of the entire physical hard drive from sector 0 to the last sector on the drive. Doing this means you will also acquire *all* of the logical volumes on the disk.

The advantages of acquiring a physical disk is that you capture everything including the all-important master boot record (MBR). The disadvantage to this approach is that it takes longer and requires more space on your evidence drive.

Acquiring a logical drive means you are going to image a single logical volume (e.g. C:\). The only thing you will have on your evidence drive is the data space allocated to that particular volume. This means the space starting with the volume boot record (VBR) to the last sector allocated to the volume.

Which to choose? It all depends on the investigative goal. When in doubt – always take a physical disk image. If time and space is important or you know your investigative issue is contained on a single volume, then image that logical volume.

- Mount your evidence drive on the suspect system.

Plug you USD evidence drive into the suspect host and wait until Windows Plug-N-Play does its thing. Remember, you evidence drive is encrypted so Windows will not recognize the drive as being formatted. If Windows asks you if you want to format the drive be sure to decline this offer.

Next, insert your toolkit CD/DVD or thumb drive into the suspect system. Traverse to the toolkit drive and fire up TrueCrypt. Go through the exact steps you used in the previous section to mount your encrypted volume. (Figure 8).

Image a Hard Disk Using FTK Imager

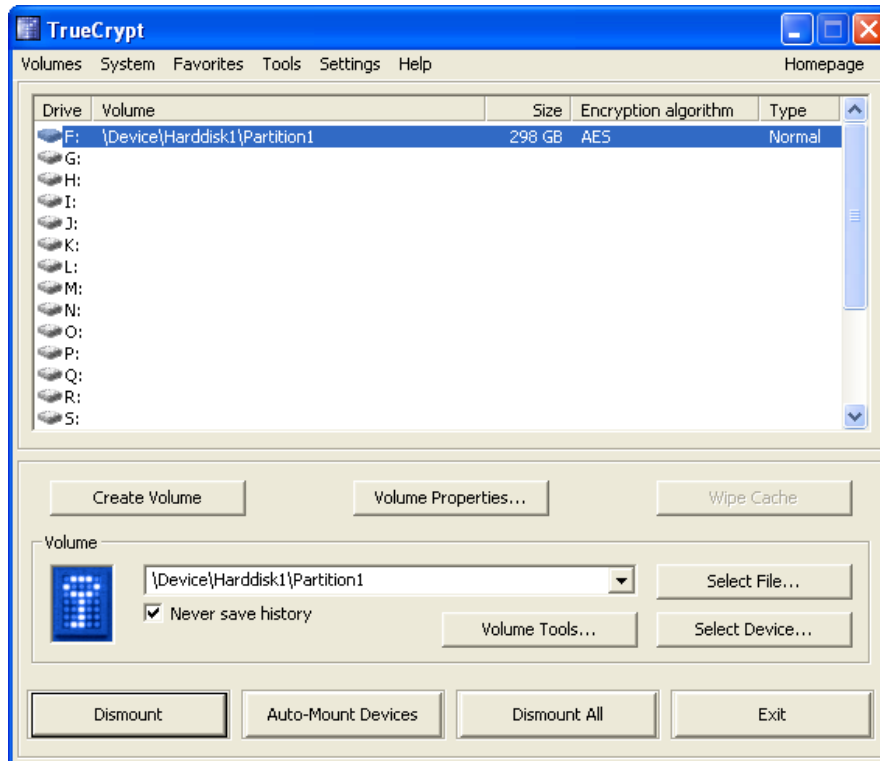


Figure 8 - Mounted TrueCrypt Volume

Traverse to you toolkit drive and start FTK Imager (Figures 9 & 10).

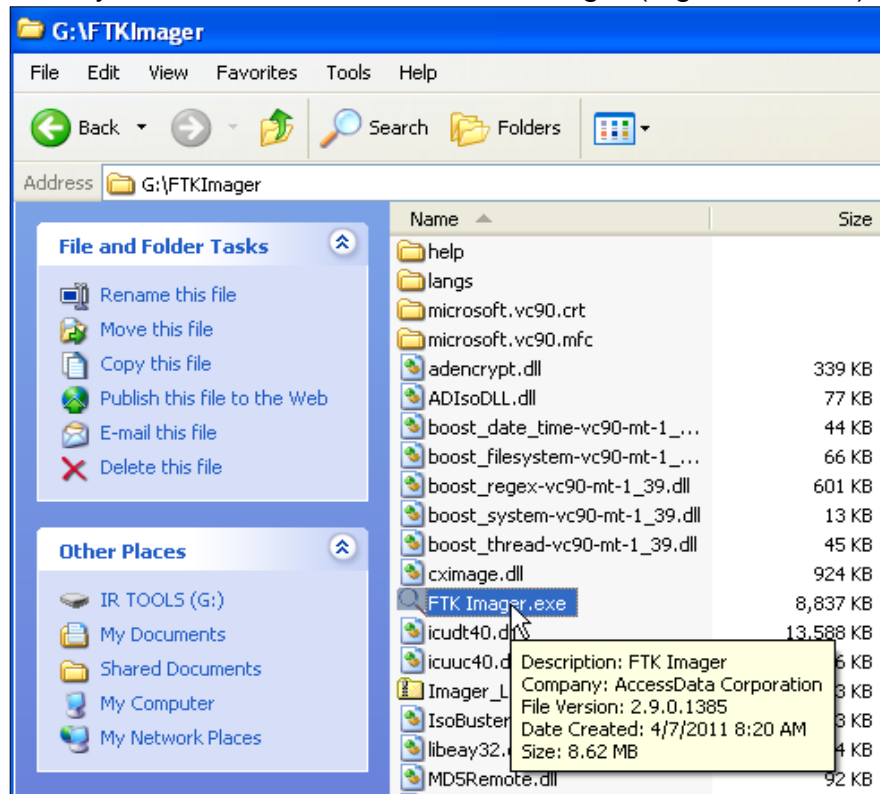


Figure 9 - FTK-Imager Startup

Image a Hard Disk Using FTK Imager

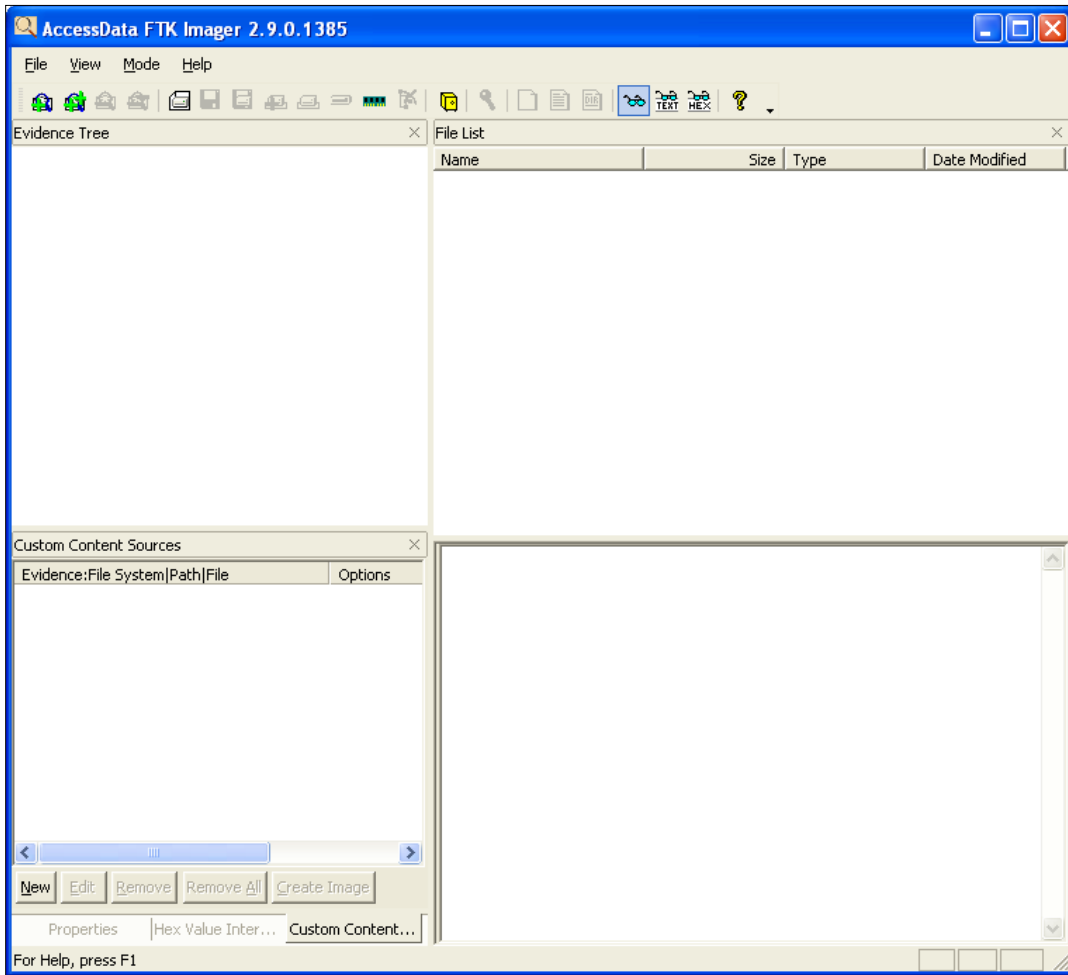


Figure 10 - FTK Imager Main Window

Click on the 'Add Evidence Item' (Figure 11).

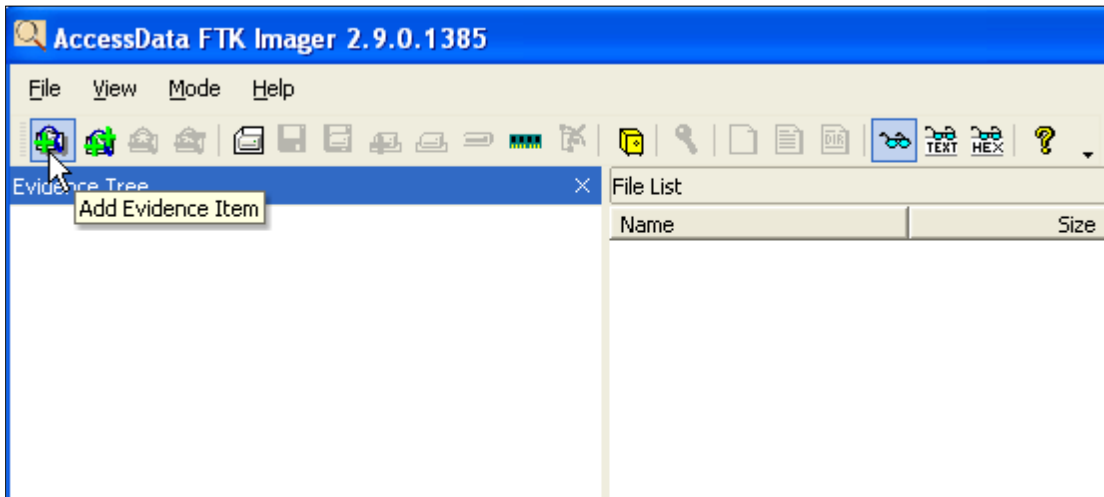


Figure 11 - FTK Imager Add Evidence

Image a Hard Disk Using FTK Imager

You now have to tell FTK Imager what you want to image (Figure 12). This is why I had you choose earlier if you wanted a physical or logical image. Note there is also a 'Image File' option. You would use this option if you want to obtain an image of a VMWare vmdk file. Yes – FTK Imager can mount and acquire a virtual machine image. How cool is that? For this example I chose 'Physical Drive.'

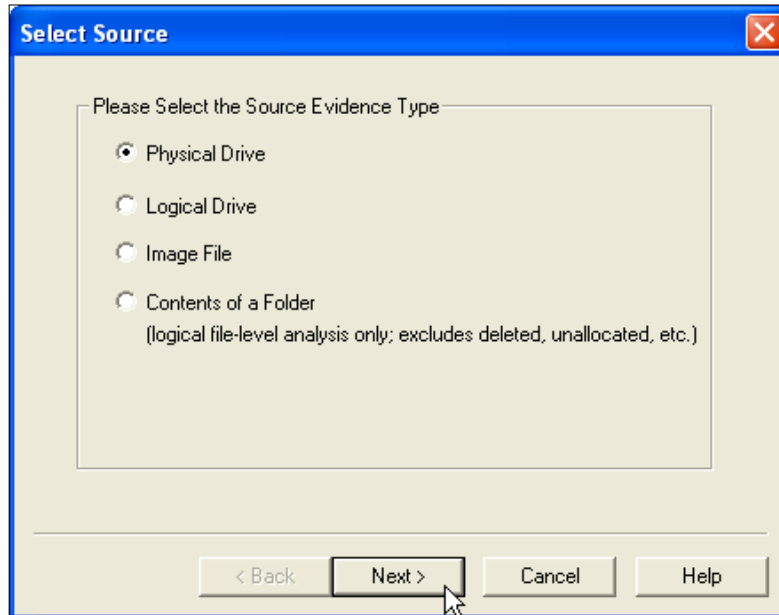


Figure 12 - FTK Imager Source Dialog

Next, from the 'Select Drive' dropdown, choose the physical drive or logical volume you want to acquire and click 'Finish' (Figure 13).

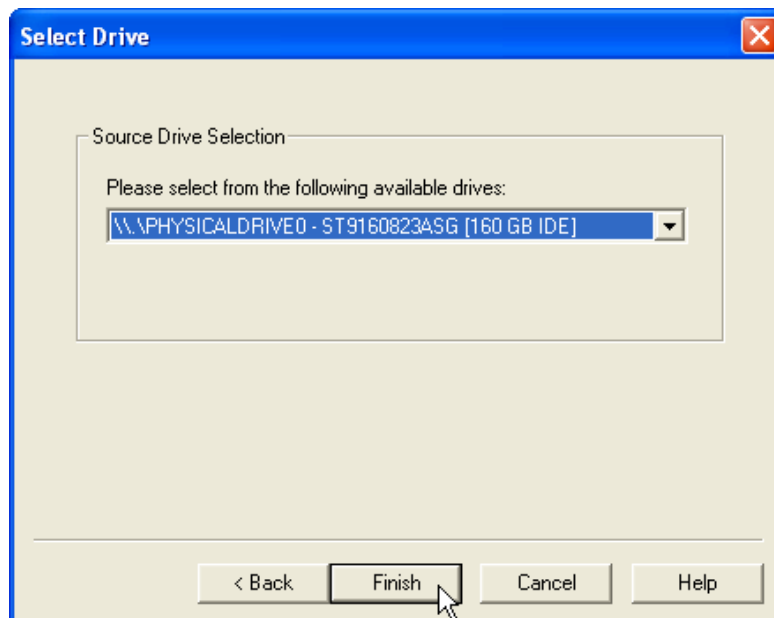


Figure 13 - FTK Imager Drive Selection

Image a Hard Disk Using FTK Imager

FTK Imager will whirl for a bit while it is mounting your suspect drive or volume. When it is mounted you will see your suspect drive in the Evidence Tree (Figure 14).

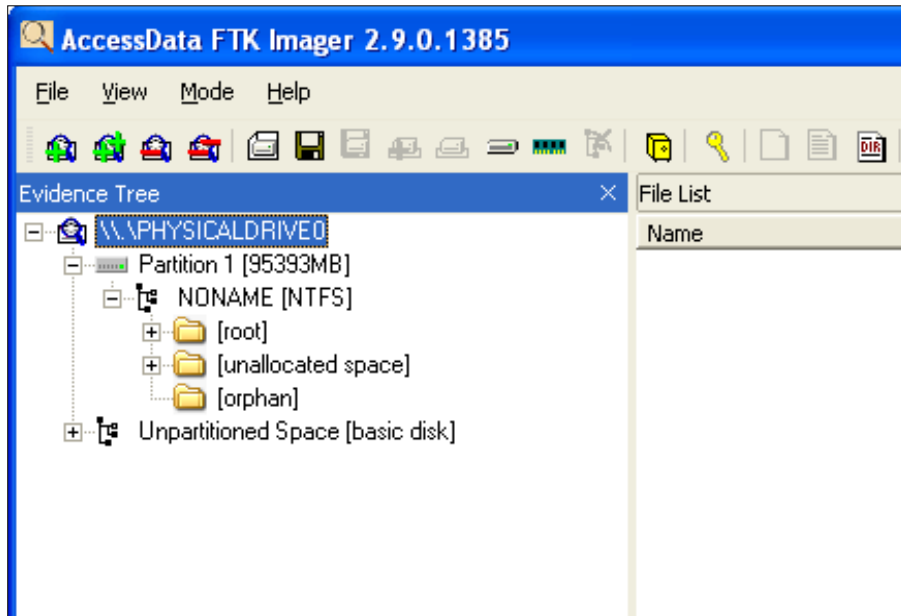


Figure 14 - FTK Imager Mounted Drive

Right click on your suspect disk or volume you want to image and select 'Export Disk Image' (Figure 15).

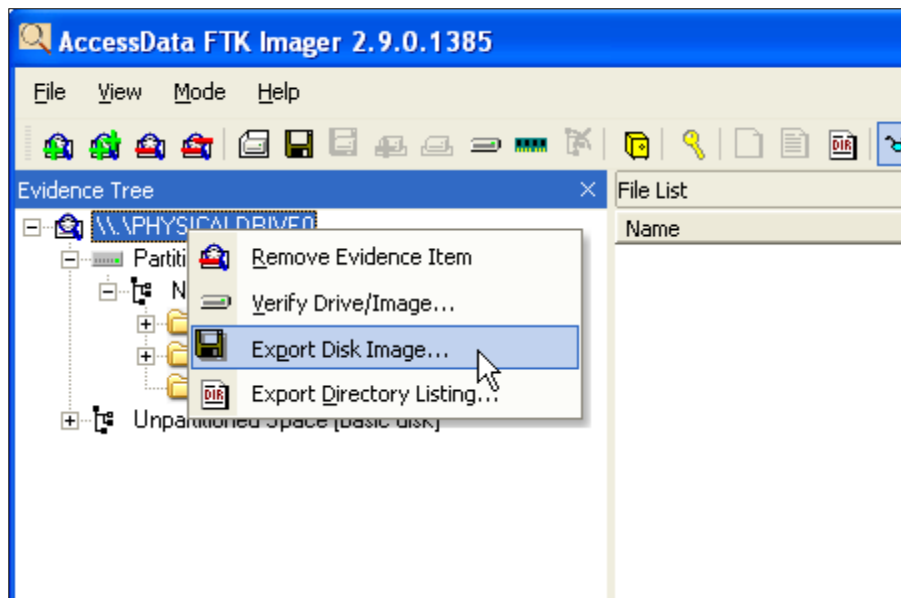


Figure 15 - FTK Imager Export Disk Image

In the next step, you must tell FTK Imager where to put the acquired disk image. Click on the 'Add' button in the 'Create Image' dialog (Figure 16).

Image a Hard Disk Using FTK Imager

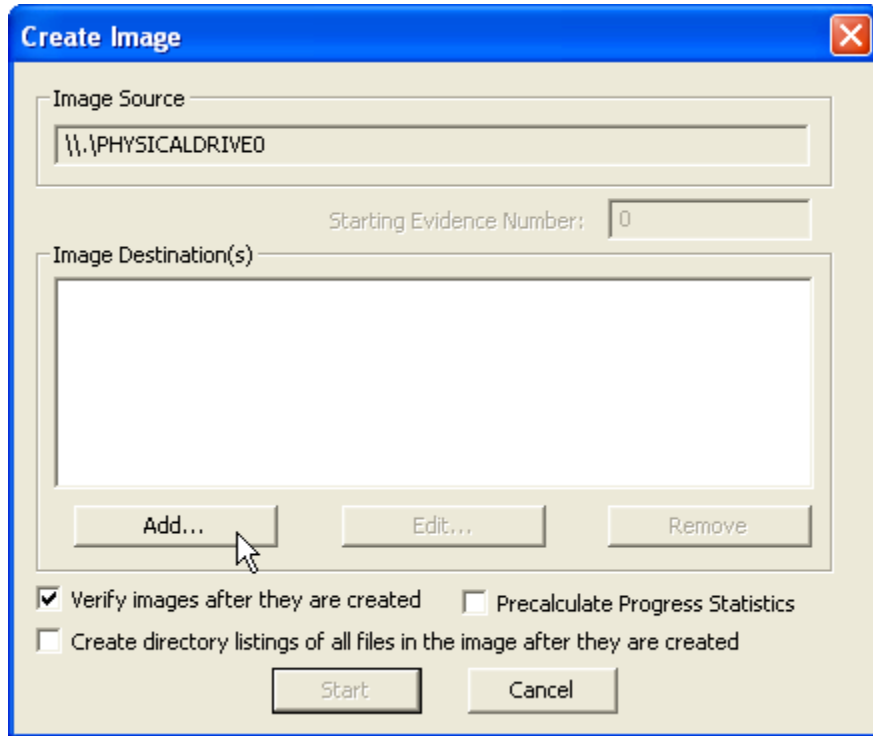


Figure 16 - FTK Imager Image Destination

Choose the image type you prefer. The most common are 'Raw (dd)' and 'E01.' The E01 format is used by the EnCase forensic tools and is recognized by most other tools. I almost always choose Raw because it is the most flexible (Figure 17).

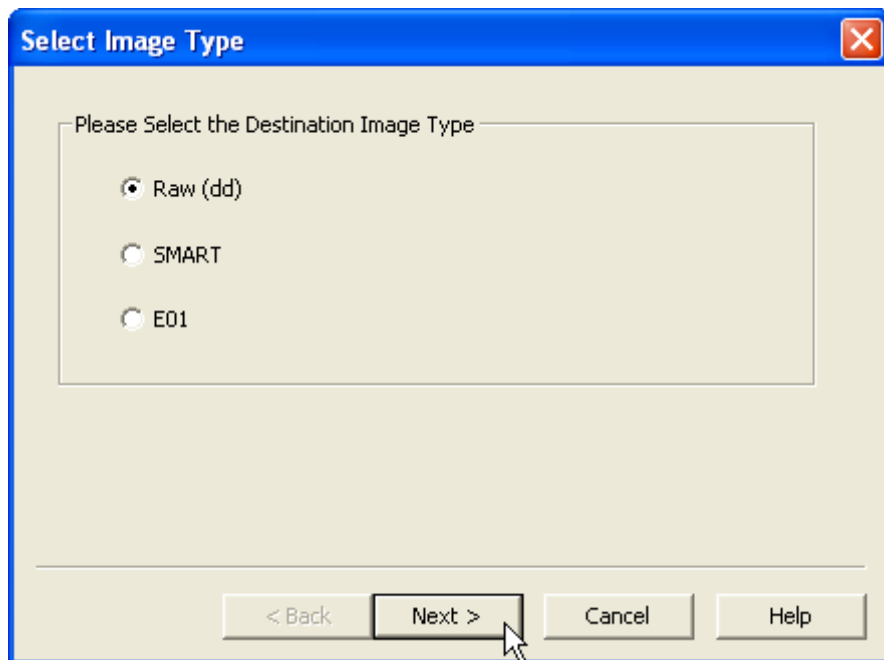


Figure 17 - FTK Imager Image Type

Image a Hard Disk Using FTK Imager

Fill out the 'Evidence Item Information' fields. I strongly encourage you to do this or you will forget why you imaged this host (Figure 18).

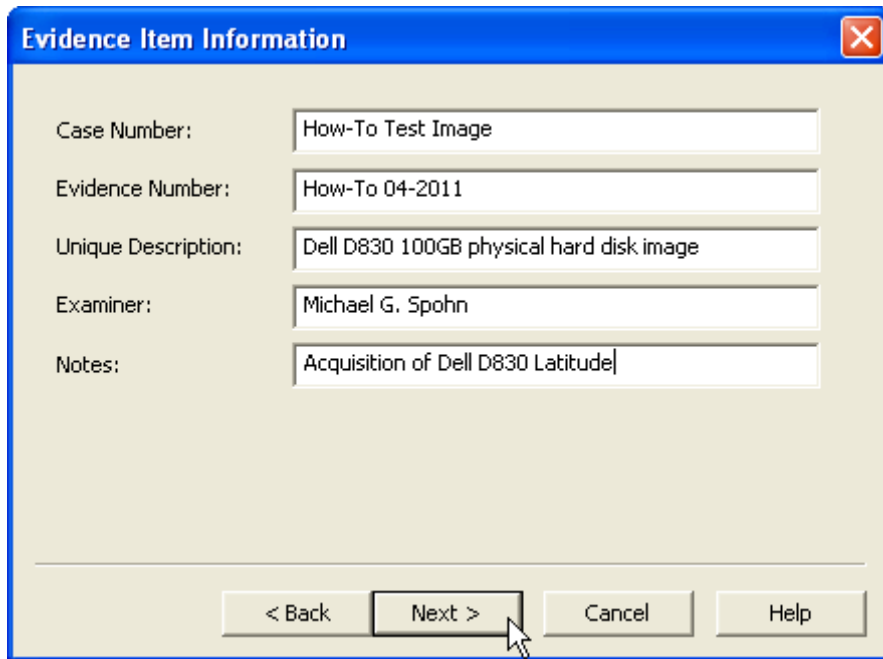


Figure 18 - FTK Imager Evidence Information

Next, you will select the destination folder where you want the evidence files placed. This will be your mounted TrueCrypt volume. Click the 'Browse' button (Figure 19).

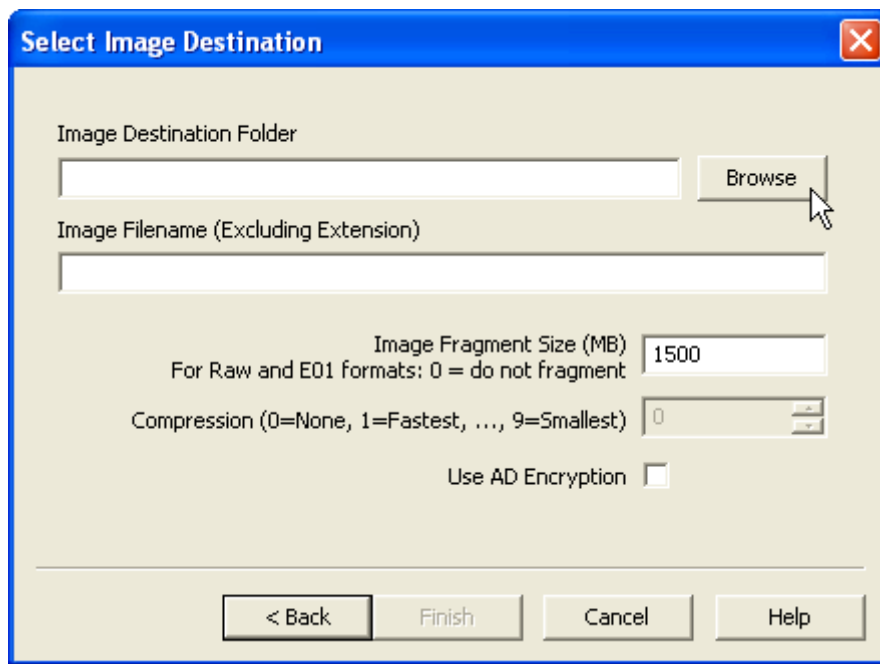


Figure 19 - FTK Imager Image Destination

Image a Hard Disk Using FTK Imager

Notice the 'Image Fragment Size (MB)' field in Figure 19. This tells FTK Imager whether you want your image file in on large file or broken up into file fragments. The default fragment size is 1500 MB (1.5 GB). This setting will divide your image into a series of sequentially numbered files all 1.5 GB in size except the last file which will be smaller. If you set this setting to 0, FTK Imager will place the image in a very large single file.

Next, select your mounted TrueCrypt volume (Figure 20).

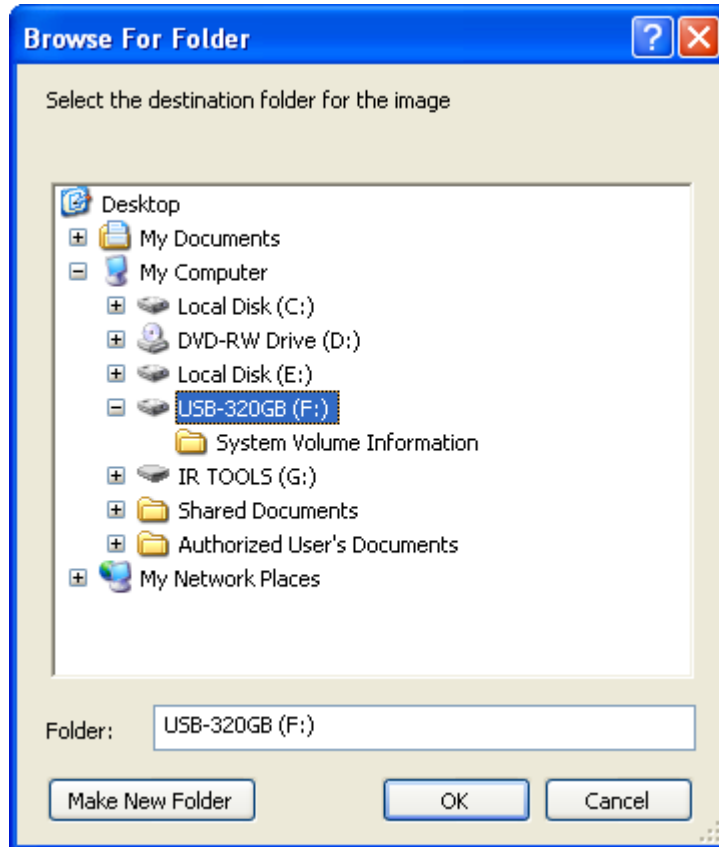


Figure 20 - Browse for Image Destination

Once you have set the destination folder, FTK Imager has all it needs to begin the acquisition of your suspect system physical disk or logical volume. Figure 21 shows the confirmation dialog.

Image a Hard Disk Using FTK Imager

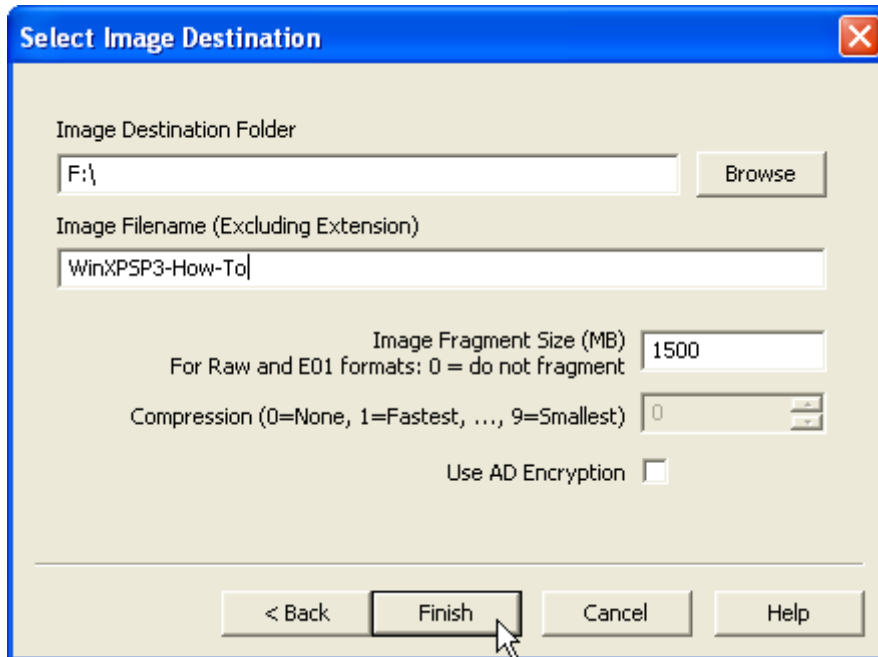


Figure 21 - FTK Imager Confirmation Dialog

Click on the Finish button and you will see a final confirmation dialog before the imaging starts (Figure 22).

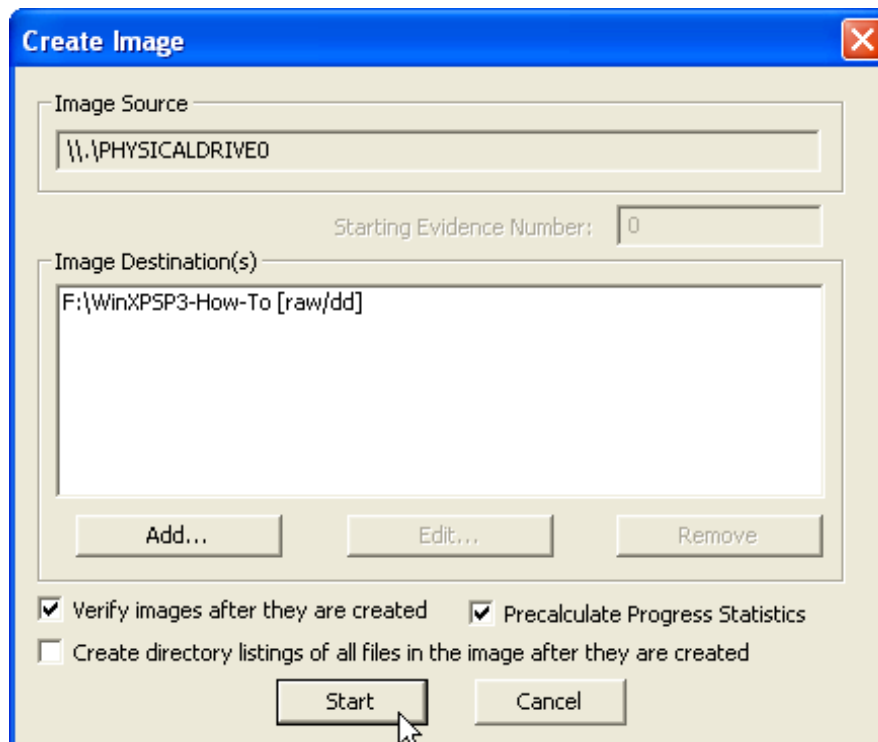


Figure 22 - FTK Imager Start Image Dialog

Image a Hard Disk Using FTK Imager

The imaging process will begin (Figure 23). Be aware the imaging of a large disk or volume can take some time, especially using an external USB evidence disk.

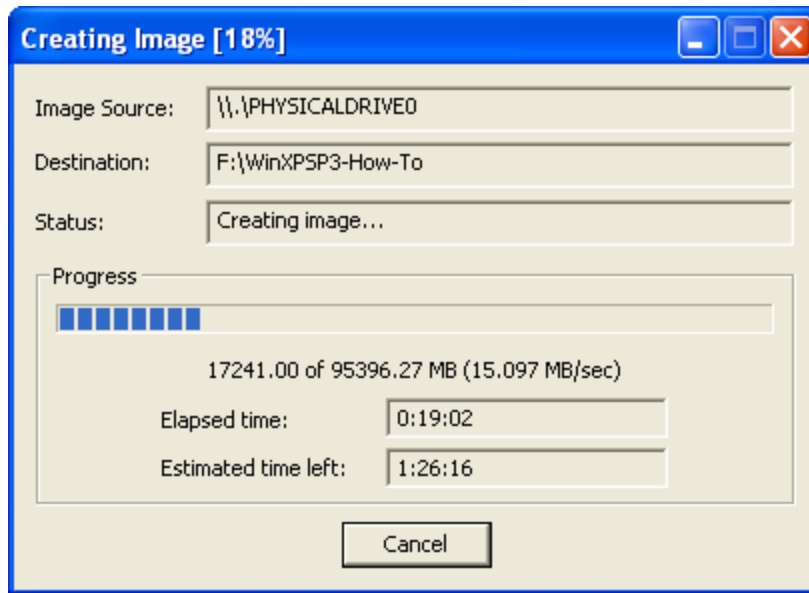


Figure 23 - FTK Imager Progress Dialog

Once the imaging process completes, FTK Imager will read through the image file and confirm the hash value is the same as the suspect drive or volume (Figure 24).

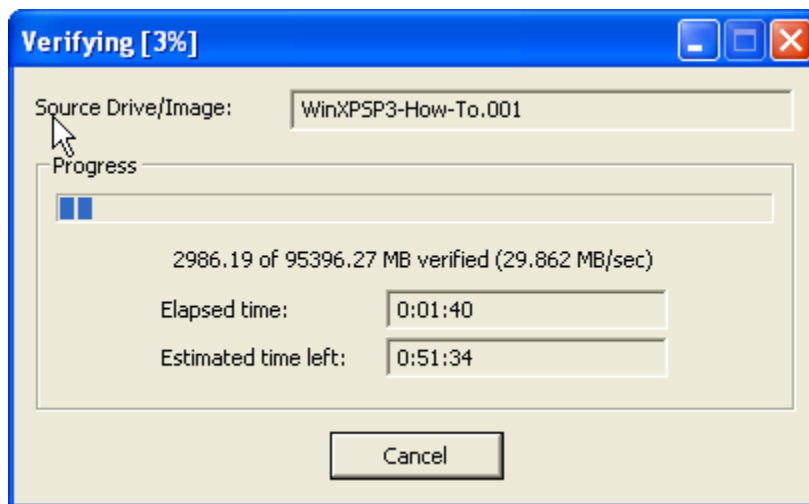


Figure 24 - FTK Imager Verification Dialog

Image a Hard Disk Using FTK Imager

Once the imaging process is complete, you are given a chance to view the image acquisition details (Figure 25).

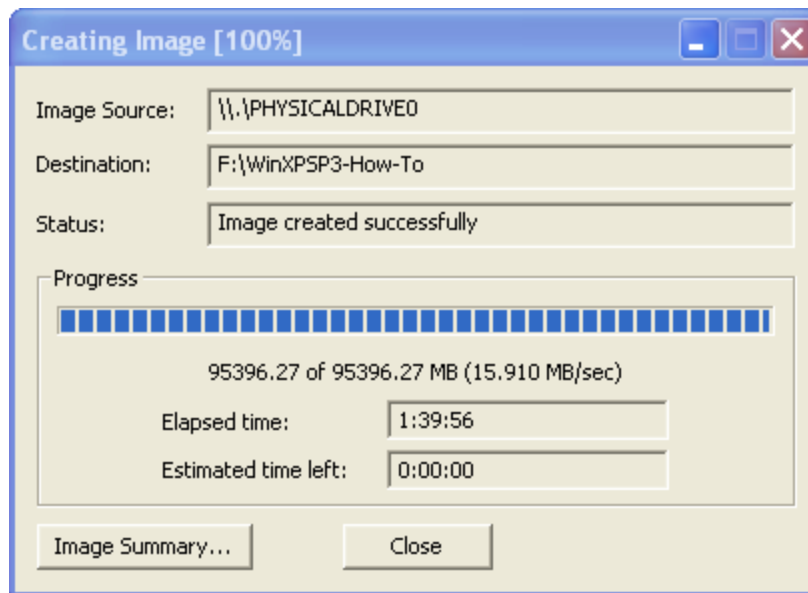


Figure 25 - FTK Imager Image Complete Dialog

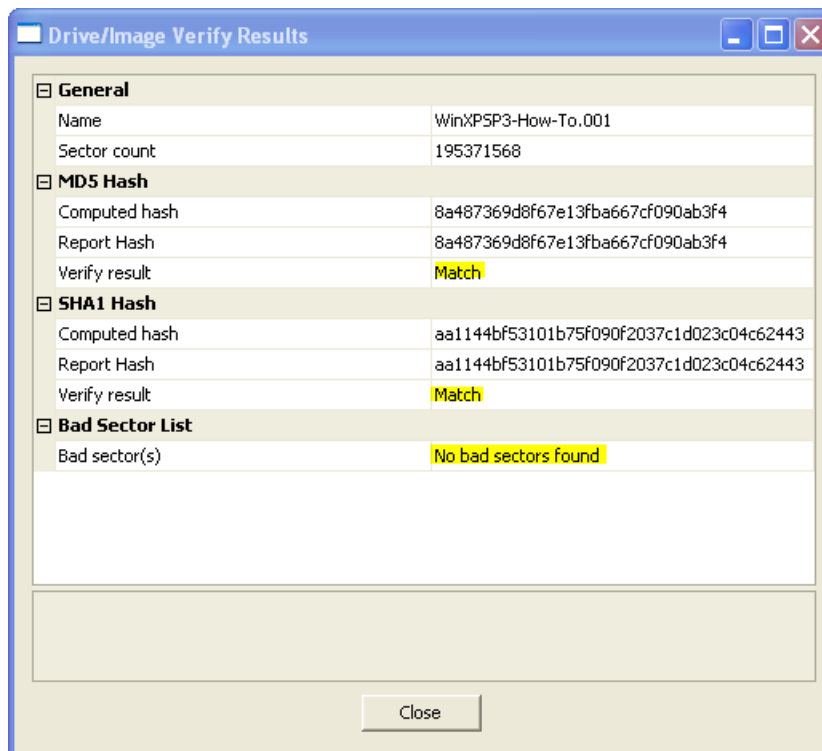


Figure 26 - FTK Imager Image Summary

Image a Hard Disk Using FTK Imager

Your evidence drive will now contain a series of files containing the suspect drive or volume image. As shown below in Figure 27, for raw images the files have a numbered suffix starting with .001.

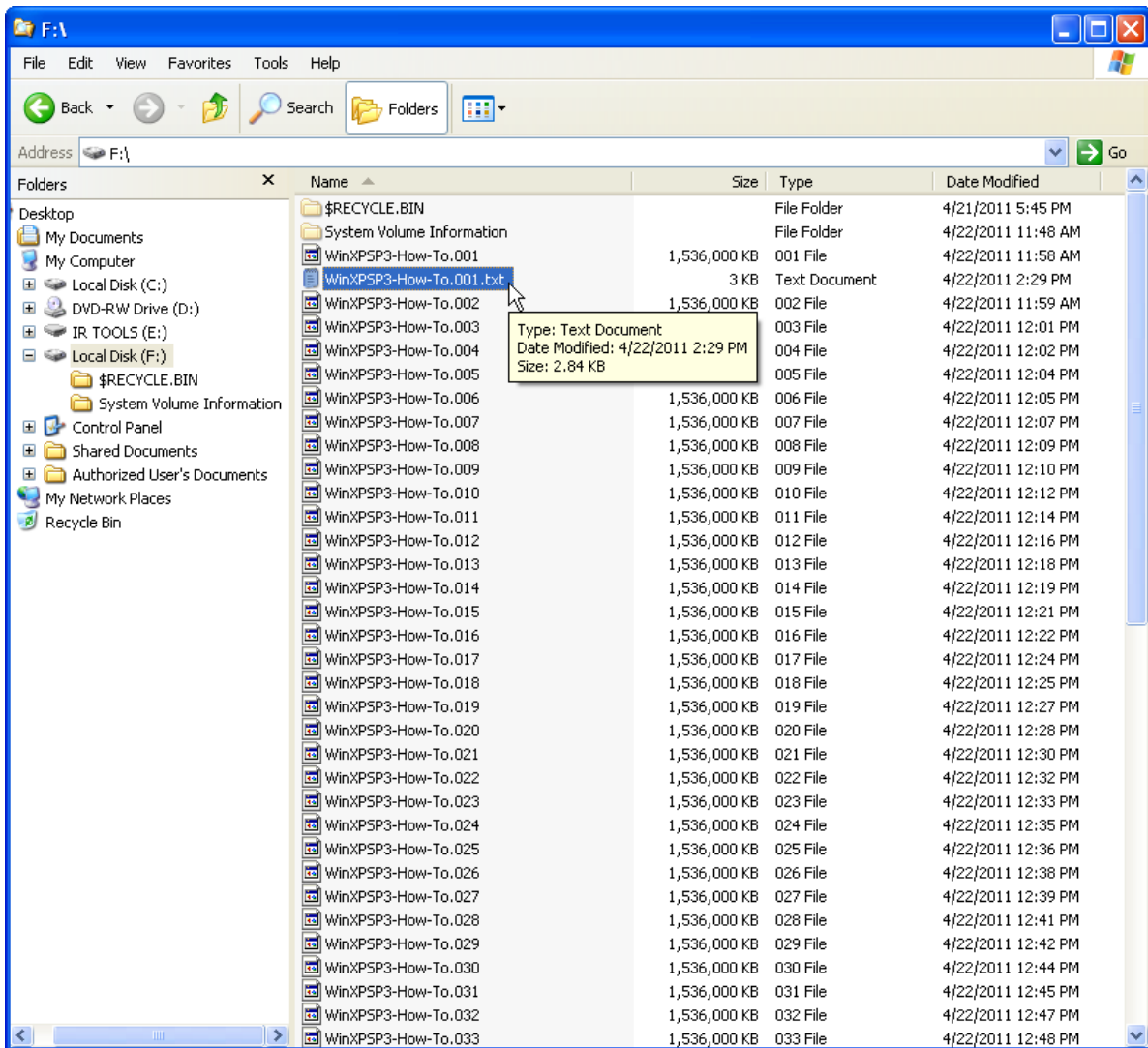
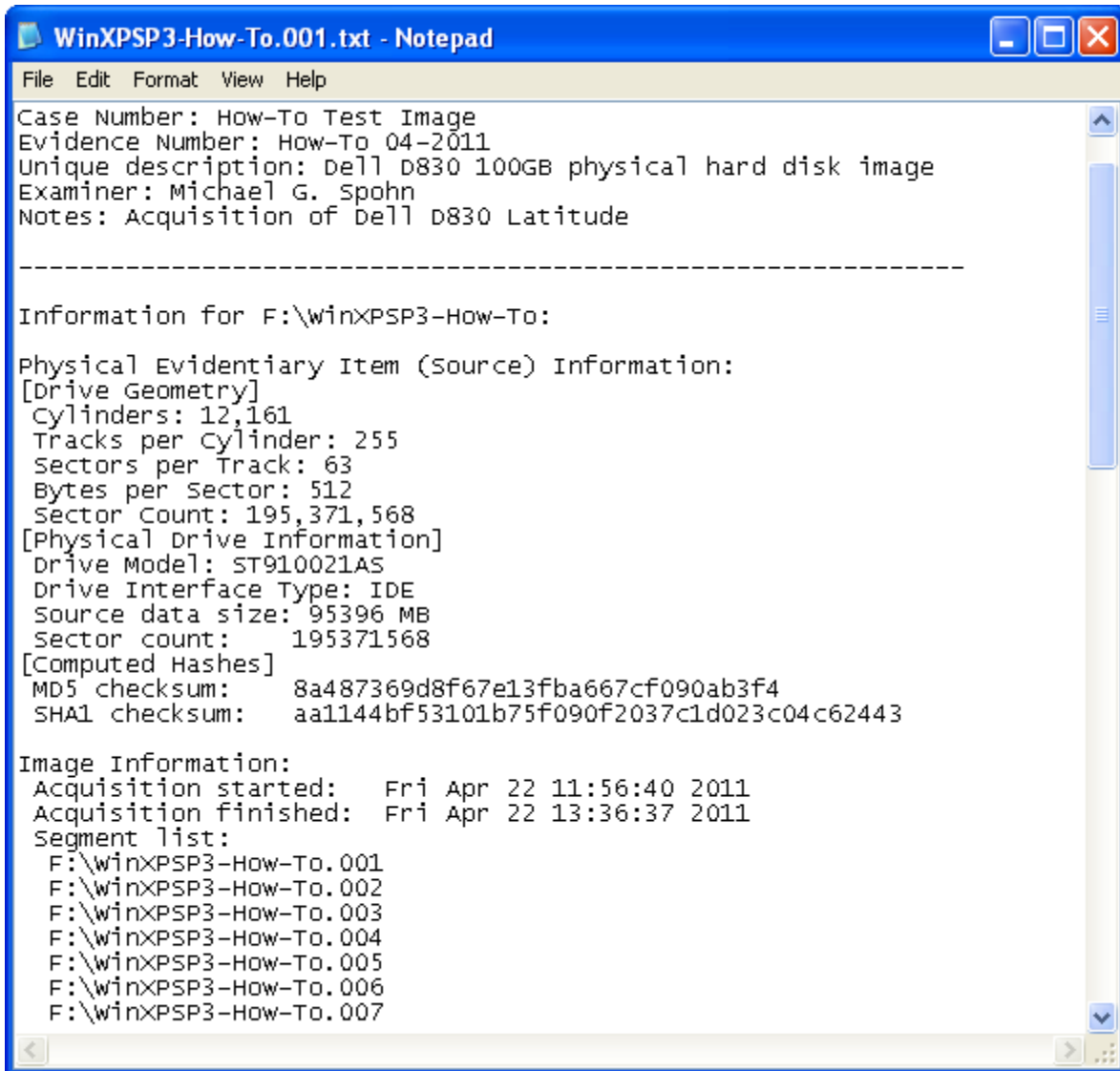


Figure 27 - Evidence Drive Image Files

FTK Imager also creates a text file that contains the details of your acquisition. In this case, the file is named *WinXPSP3-How-To.001.txt*. Figure 28 shows the level of detail this file contains.



```
WinXPSP3-How-To.001.txt - Notepad
File Edit Format View Help
Case Number: How-To Test Image
Evidence Number: How-To 04-2011
Unique description: Dell D830 100GB physical hard disk image
Examiner: Michael G. Spohn
Notes: Acquisition of Dell D830 Latitude

-----

Information for F:\winXPSP3-How-To:

Physical Evidentiary Item (source) Information:
[Drive Geometry]
Cylinders: 12,161
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 195,371,568
[Physical Drive Information]
Drive Model: ST910021AS
Drive Interface Type: IDE
Source data size: 95396 MB
Sector count: 195371568
[Computed Hashes]
MD5 checksum: 8a487369d8f67e13fba667cf090ab3f4
SHA1 checksum: aa1144bf53101b75f090f2037c1d023c04c62443

Image Information:
Acquisition started: Fri Apr 22 11:56:40 2011
Acquisition finished: Fri Apr 22 13:36:37 2011
Segment list:
F:\winXPSP3-How-To.001
F:\winXPSP3-How-To.002
F:\winXPSP3-How-To.003
F:\winXPSP3-How-To.004
F:\winXPSP3-How-To.005
F:\winXPSP3-How-To.006
F:\winXPSP3-How-To.007
```

Figure 28 - FTK Imager Acquisition Details Text File

You now have completed the acquisition of a suspect hard drive and placed the evidence files on an encrypted hard drive. All that is left to do is to dismount your encrypted evidence drive.

Open up the TrueCrypt applet, select your encrypted drive and click the 'Dismount' button as shown in Figure 29. TrueCrypt will unmount your drive. At this point you can remove the your external USB drive from the suspect computer and forward it to the person(s) responsible for the forensic examination.

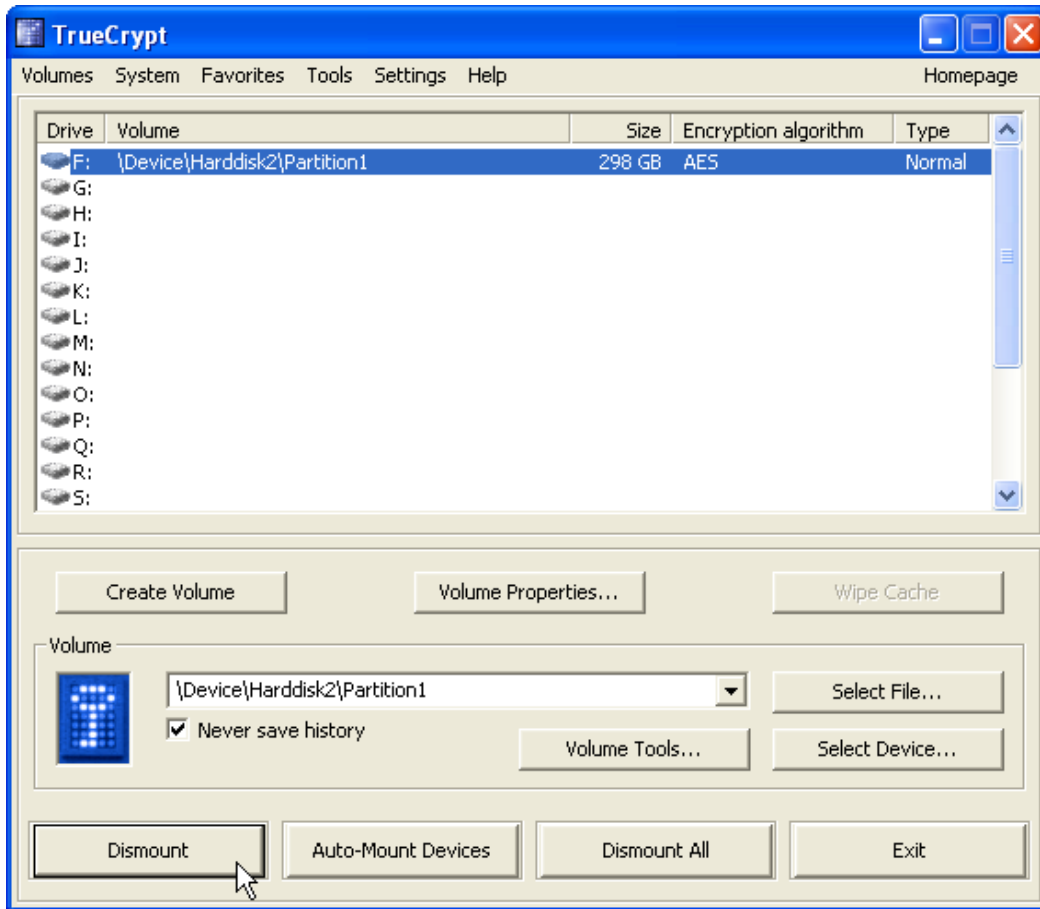


Figure 29 - TrueCrypt Volume Dismount

Summary

This 'How-To' provides a step-by-step guide to acquiring a disk image from a live computer system using FTK Imager. It is designed to assist IT and security personnel with little or no forensic experience capture a disk image of a system that need some form of forensic analysis. It is highly recommended that you always place your acquired images on an encrypted evidence disk, particularly if you have to ship the evidence drive via a common carrier such as UPS, FedEx, or the USPS.

If you have any feedback about this guide please email me (mspohn@malware-hunters.net) or visit our blog at www.malware-hunters.net.