Data Acquisition 6

By the end of the practical session, the students should be able to:

- Understand FTK Imager program
- Use FTK Imager to create a disk image
- Use automated hashing tools available in FTK Imager
- Understand what the md5 and sha1 hashes represent

This lab will cover topics on understanding how to perform the data acquisition and preserving the digital evidence. By having this lab, students is able to understand the concept of digital forensics and disk imaging.

6.0 Introduction

The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations. A large part of digital forensics is working on cases to process and analyze digital evidence collected from crime scenes. The process of working on a digital forensics case include creating disk image (copies of the original suspect's drive), hashing or verifying the integrity of the disk image, write blocking the disk image (setting it to read-only to verify disk image integrity), and analyzing the drive and its contents.

Disk images are used to transfer a hard drive's contents for various reasons. A disk image can be used in several instances, including: restoration of a hard drive's contents during disaster recovery, for the transfer of contents of a hard drive from one computer to another, or to restore the contents of a hard drive after hardware upgrade or repair. Additionally, it can be used to create an exact replica of a hard drive or other device (CD, USB, etc.) for the purpose of analysis during the course of an investigation.

A disk Image is defined as a computer file that contains the contents and structure of a data storage device such as a hard drive, CD drive, phone, tablet, RAM, or USB. The disk image consists of the actual contents of the data storage device, as well as the information necessary to replicate the structure and content layout of the device. This differs from a normal backup in that the integrity of the exact storage structure remains intact, which is pivotal in maintaining the integrity of a forensic investigation. If the file structure and its contents cannot be verified as being exactly the same as the original target drive, the integrity of the evidence is in jeopardy and could be inadmissible in a court of law.

Creating a disk image file of a target is the first step of any digital forensic investigation. In any investigation, analysis is not done on the original data storage device (target), but instead on the exact copy taken.

An image may be taken locally or remotely. In the case that a disk image is taken locally, the data storage target is physically available, such as a USB key or hard drive on an acquired machine. In the case of remote acquisition, the target storage device is not present (i.e. a computer in a suspect's office at their place of work). There are various software that are specifically aimed towards one or the other.

In this particular lab, we will be making an image of a local hard drive using FTK Imager. FTK Imager is a software created by the company AccessData for the purpose of creating both local and remote images. However, the free version only allows for local imaging. This software can acquire images of locally available storage devices, such as USB, hard drives, CD drives, or even individual files.

In this tutorial, we will create an exact replica of a local drive (D:\, any applicable based on your PC setting) that will be used in the scope of a digital forensic investigation.

Lab 6.1: Imaging the Drive

6.1.1 Task

1. Launch USB Write Protect ON.
2. Launch FTK Imager by clicking on the 'AccessData FTK Imager' icon. Figure 6.1 will appear once the program has been launched.

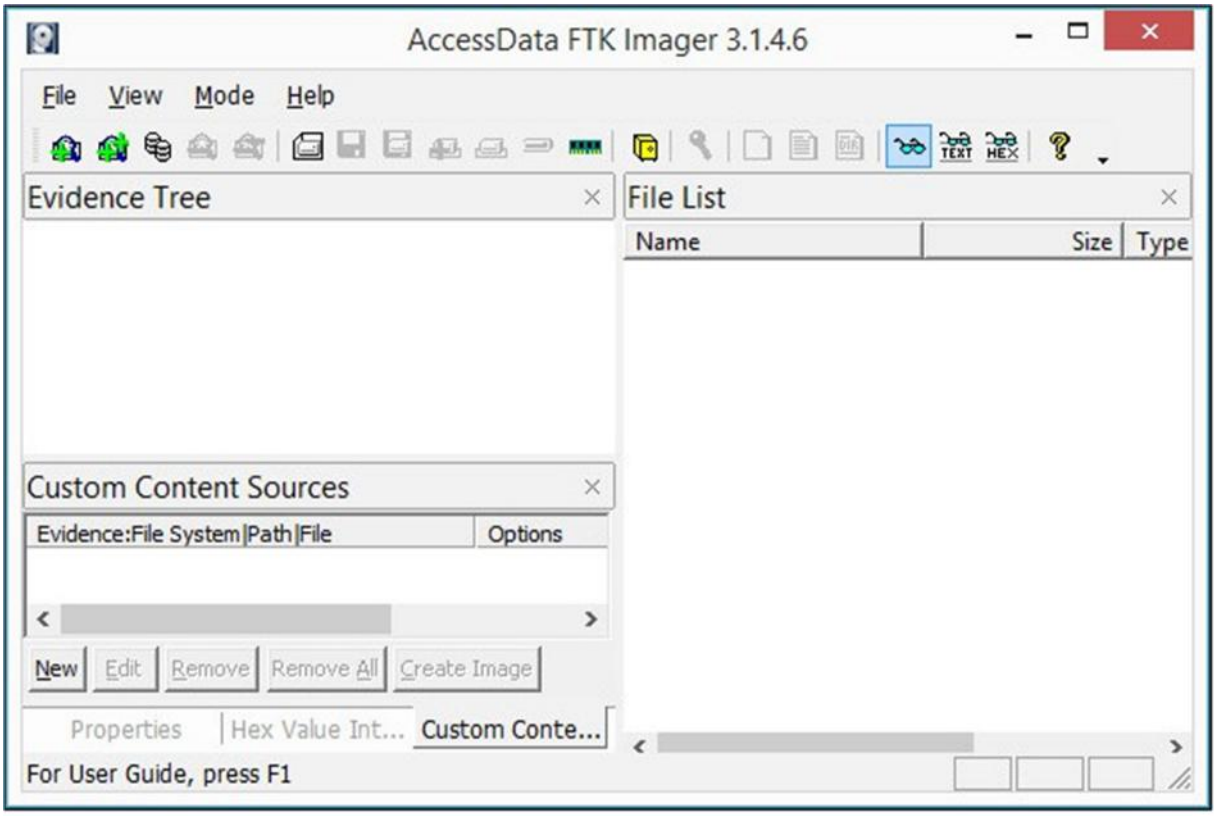


Figure 6.1 FTK Imager main screen

3. Click **File** and look over the various options for creating images. We will be using the 'Create Disk Image' option as shown in Figure 6.2. It is good to note that you can also capture from memory, and image individual items.

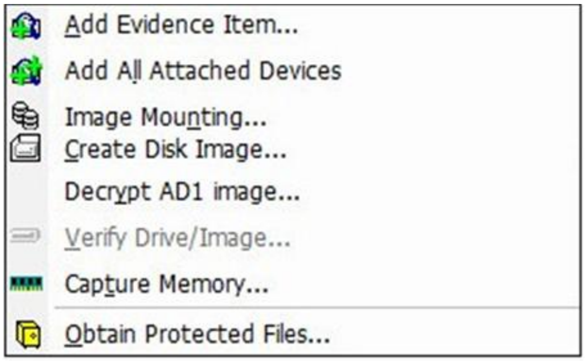
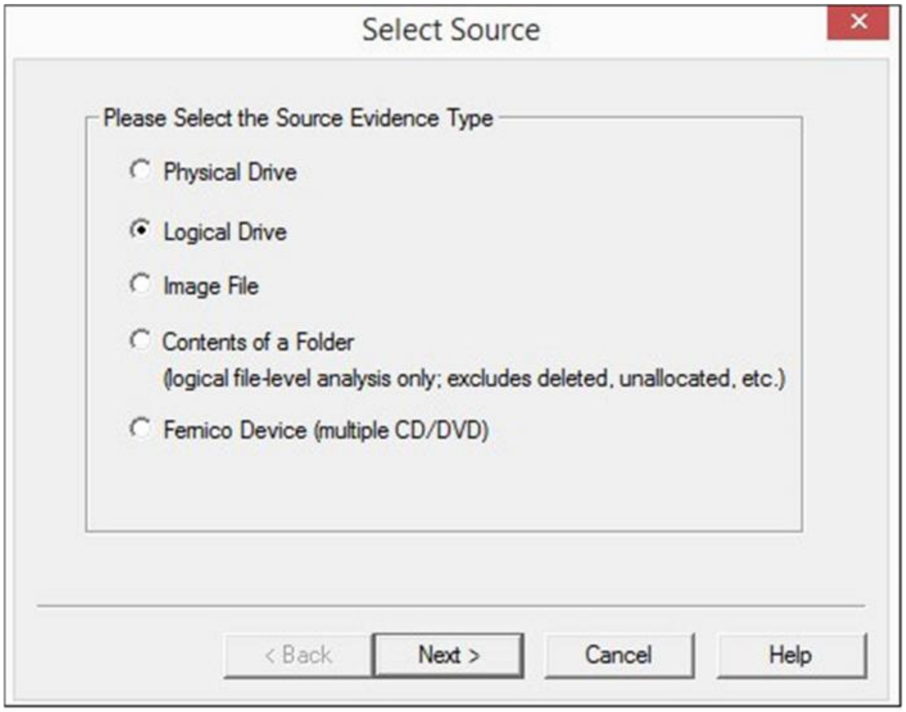


Figure 6.2 Create Disk Image

4. Click **'Create Disk Image'** and a window will appear as shown in Figure 6.3. Select the correct drive type for the situation. In this case, we are imaging a logical drive. Note that it is also possible to select individual folders and CD/DVD. Select **logical drive** and click **Next**.


Select Source

Please Select the Source Evidence Type

○ Physical Drive

● Logical Drive

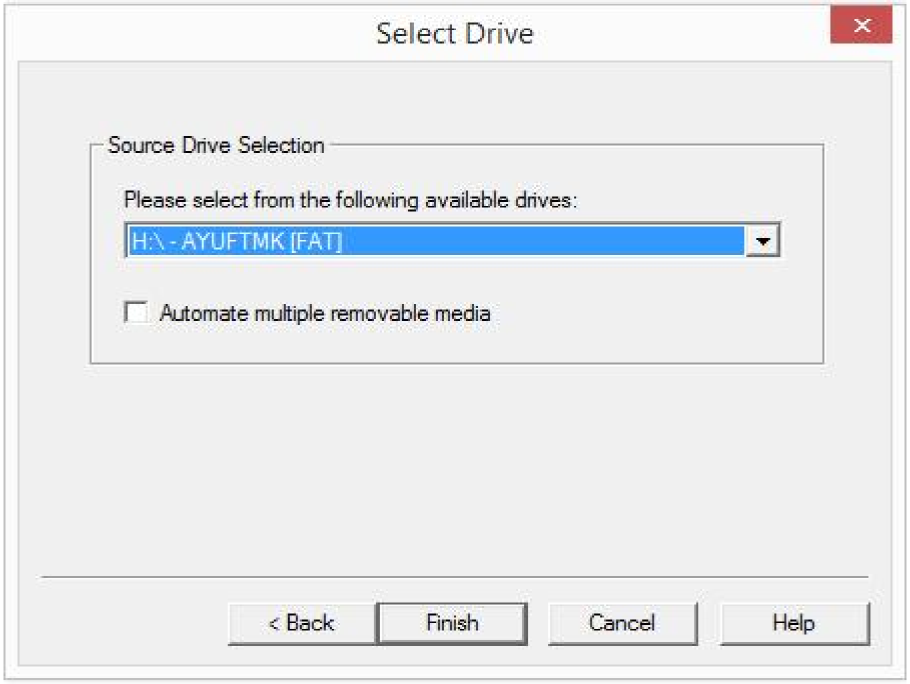
○ Image File

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

○ Femico Device (multiple CD/DVD)

Figure 6.3 Selecting source of evidence to be imaged

5. Select the desired drive in the resulting ‘Select Drive’ window as shown in Figure 6.4. In this case the drive we wish to image is your USB drive such as ‘H:\ AYUFTMK[FAT]’. Click **Finish**.


Select Drive

Source Drive Selection

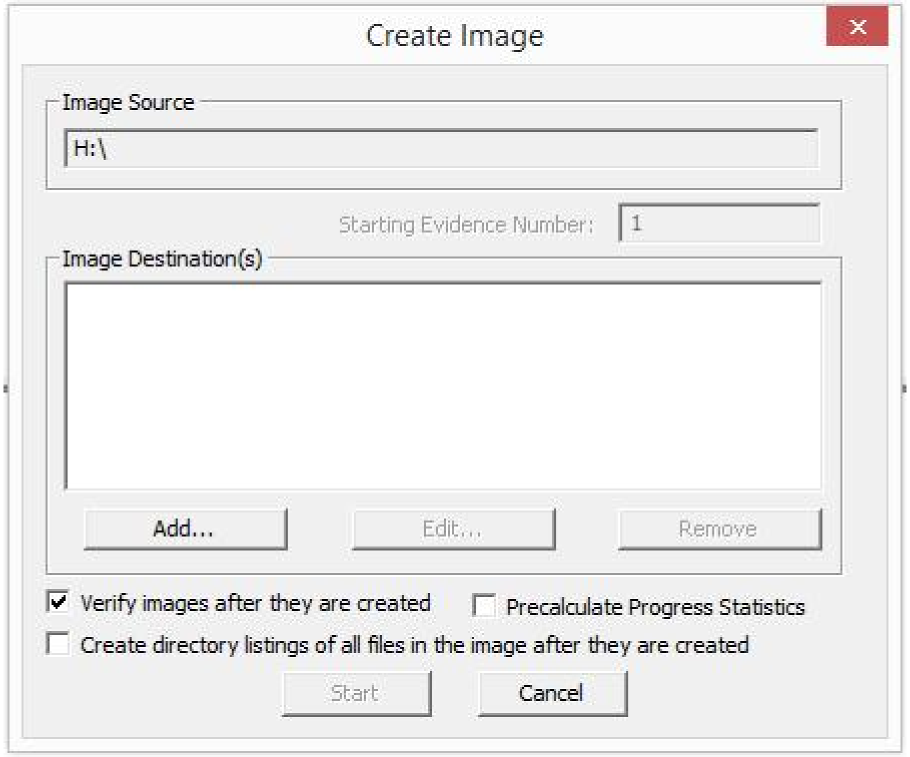
Please select from the following available drives:

H:\ - AYUFTMK [FAT]

□ Automate multiple removable media

Figure 6.4 Selecting Drive to be imaged

6. The following ‘Create Image’ window will appear as shown in Figure 6.5. Note that the appropriate Image Source has been selected. Click **Add** to select the image type and choose the Image Destination.



Create Image

Image Source: H:\

Starting Evidence Number: 1

Image Destination(s)

☑ Verify images after they are created

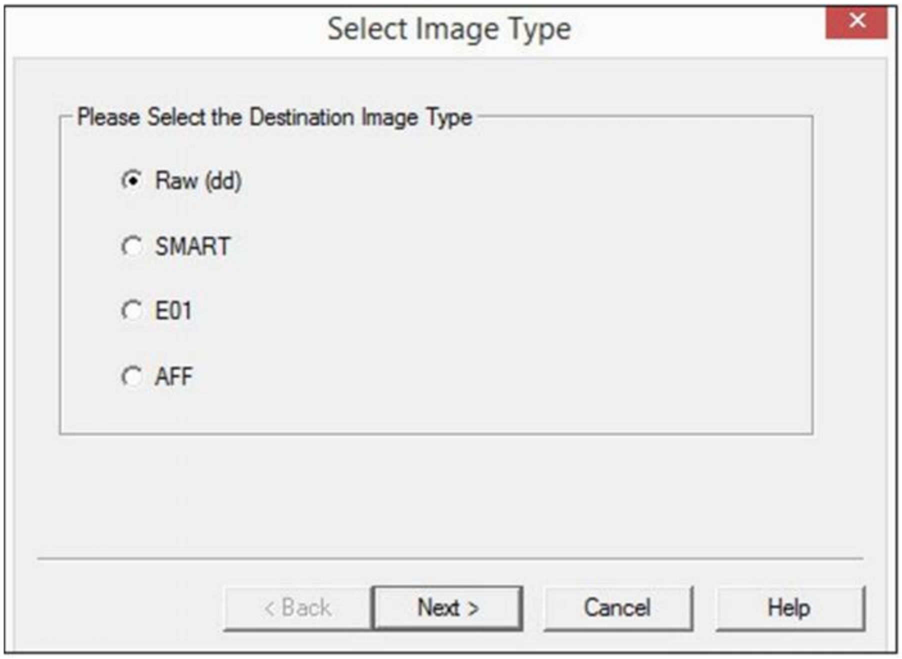
□ Precalculate Progress Statistics

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

Figure 6.5 Create image window

7. Select the desired image format. We will be using **dd**. dd (disk dump) is the raw image file format. It is used not only in Windows, but also in Linux. Select **‘Raw (dd)’** and click **Next**.

   *Note that the E01 file format is for EnCase (an enterprise digital forensics program), AFF stores all data and metadata in a single file, and SMART stores the metadata in a separate text file where the contents can be easily viewed.



Select Image Type

Please Select the Destination Image Type

● Raw (dd)

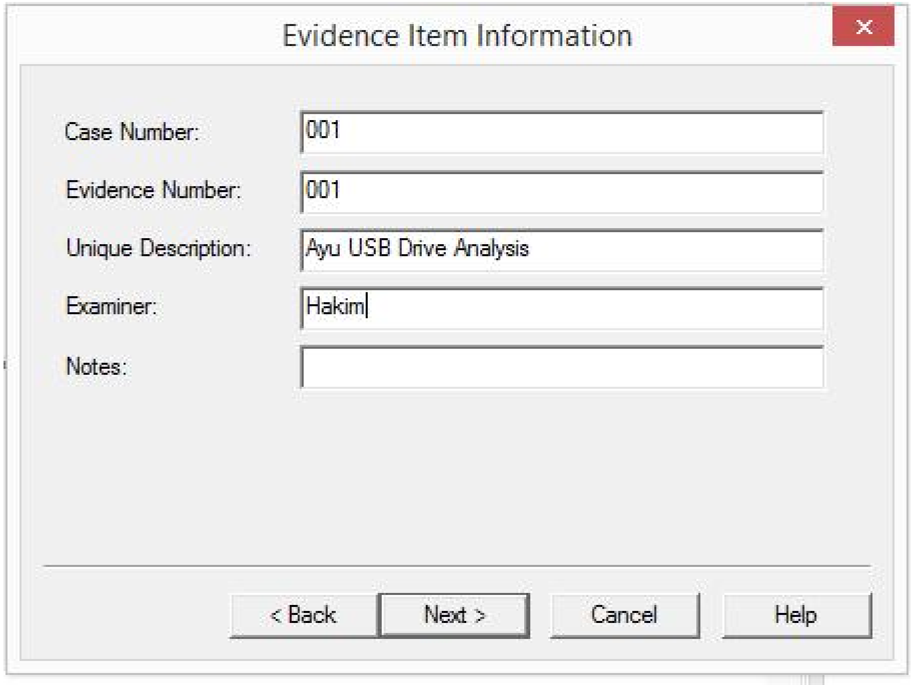
○ SMART

○ E01

○ AFF

Figure 6.6 Selecting the format type for the image

8. Windows shows in Figure 6.7 will give you the opportunity to enter information about the case for the image. This is useful for organizational purposes. Since keeping track of everything and having detailed notes is pivotal, it is helpful to enter this information. Click **Next**.

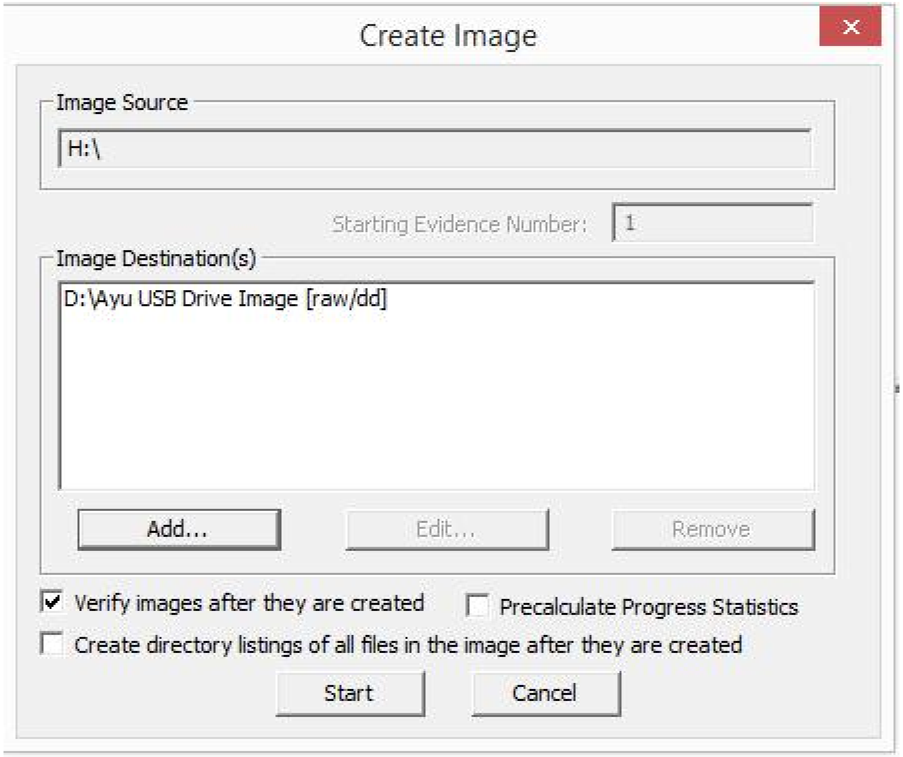


Evidence Item Information

Case Number:	001
Evidence Number:	001
Unique Description:	Ayu USB Drive Analysis
Examiner:	Hakim
Notes:	

Figure 6.7 Case Information for the image

9. Select the folder in which the image file will be placed such as (D:\ Ayu USB Drive) as shown in Figure 6.8. Also, give the image file a specific name if desired.



Create Image

Image Source: H:\

Starting Evidence Number: 1

Image Destination(s): D:\Ayu USB Drive Image [raw/dd]

☑ Verify images after they are created

□ Precalculate Progress Statistics

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

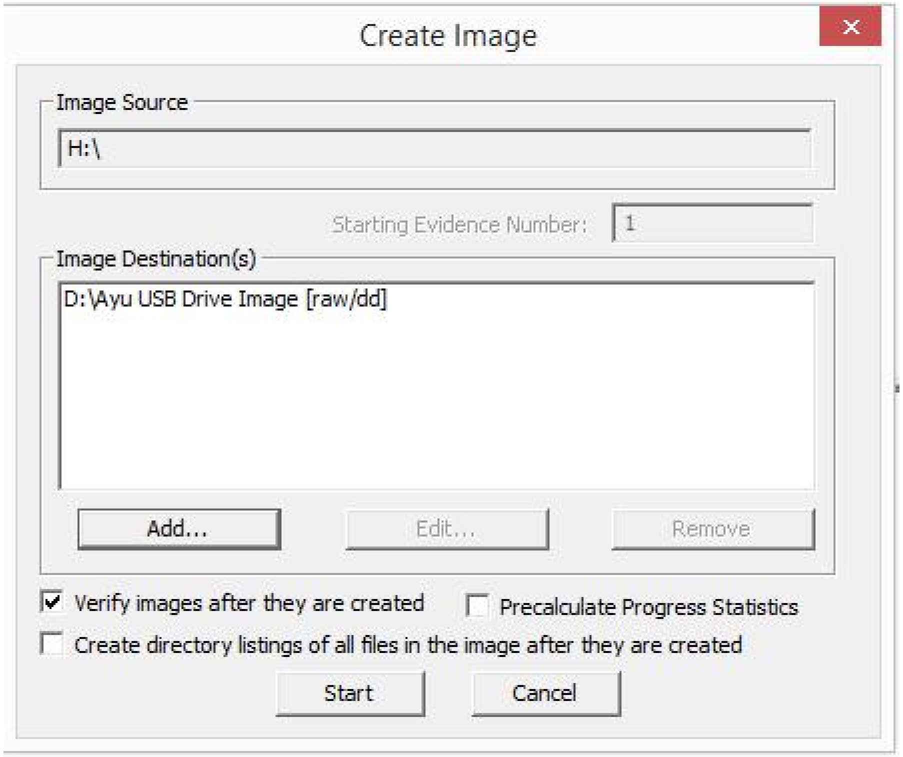
Figure 6.8 Setting destination of image

10. The 'Image Fragment Size' field specifies the number of megabytes into which FTK Imager should split each chunk of the image file; this can be helpful if the image is very large or will be transported or archived on CDs or DVDs. If a value is entered in this field larger than the size of the data to be imaged, only one file will be created and it will be the size of the data. For our tutorial, if the default value of 1500 MB is left, FTK Imager will create one 1GB file since the drive we are imaging is only 1GB.

    The second option deals with compression; dd images cannot be compressed, but some proprietary formats, like .e01, can. Click **Finish**.

11. Note that the image destination has been changed to D:\. The disk image will be saved to the Investigative Drive. Note also that the disk image will be created in raw/dd. Make sure that **'Verify images after they are created'** is checked – this will automatically create a hash for the image. The hash is used to verify that no changes have been made to the image file. More

information about hashing may be found in the hashing tutorial. Click **Start** to create the image file.



Create Image

Image Source

H:\

Starting Evidence Number: 1

Image Destination(s)

D:\Ayu USB Drive Image [raw/dd]

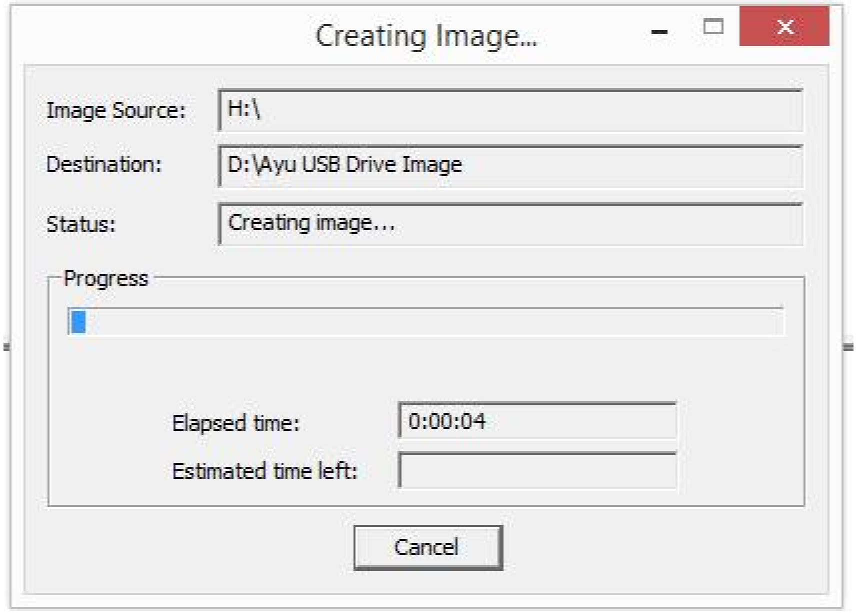
☑ Verify images after they are created

□ Precalculate Progress Statistics

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

Figure 6.9 Verify images - create a hash for an image

12. The image will be created. This may take some time depending on the file size.



Creating Image...

Image Source: H:\

Destination: D:\Ayu USB Drive Image

Status: Creating image...

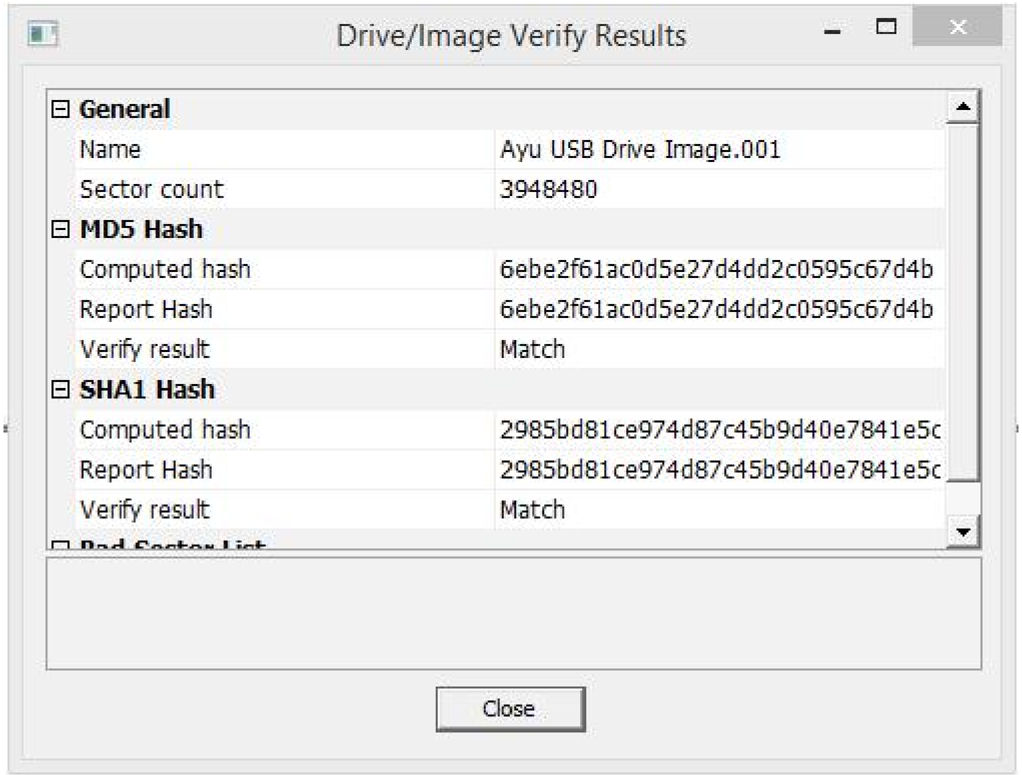
Progress

Elapsed time: 0:00:04

Estimated time left:

Figure 6.10 Process of Creating Image Status

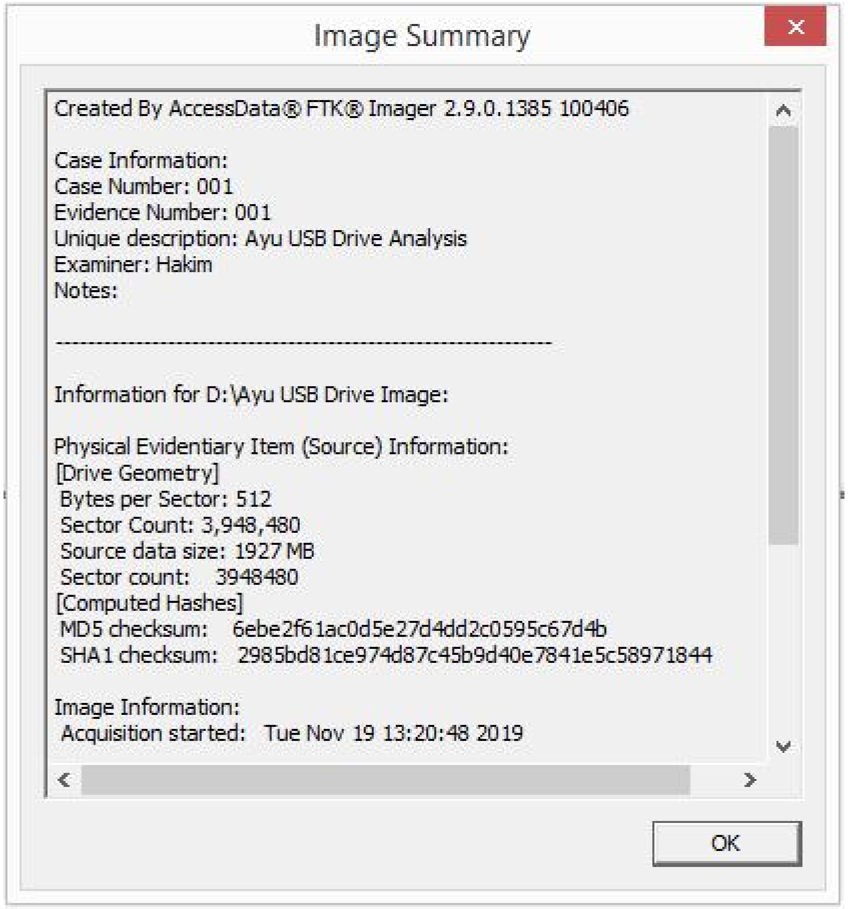
13. Once the image has been completed, Figure 6.11 will appear. Note that both an MD5 and SHA1 hash have been created and verified. The hash is the fingerprint of the disk image – if the disk image is altered, the hash values will change. Keeping track of these hashes will allow you to continually verify the hash of the image file during your investigative process. Any other investigator should be able to replicate this hash; this maintains integrity in the eyes of the court.



⊟ **General**	
Name	Ayu USB Drive Image.001
Sector count	3948480
⊟ **MD5 Hash**	
Computed hash	6ebe2f61ac0d5e27d4dd2c0595c67d4b
Report Hash	6ebe2f61ac0d5e27d4dd2c0595c67d4b
Verify result	Match
⊟ **SHA1 Hash**	
Computed hash	2985bd81ce974d87c45b9d40e7841e5c
Report Hash	2985bd81ce974d87c45b9d40e7841e5c
Verify result	Match
⊟ **Bad Sector List**	

Figure 6.11 Creating Image Completed

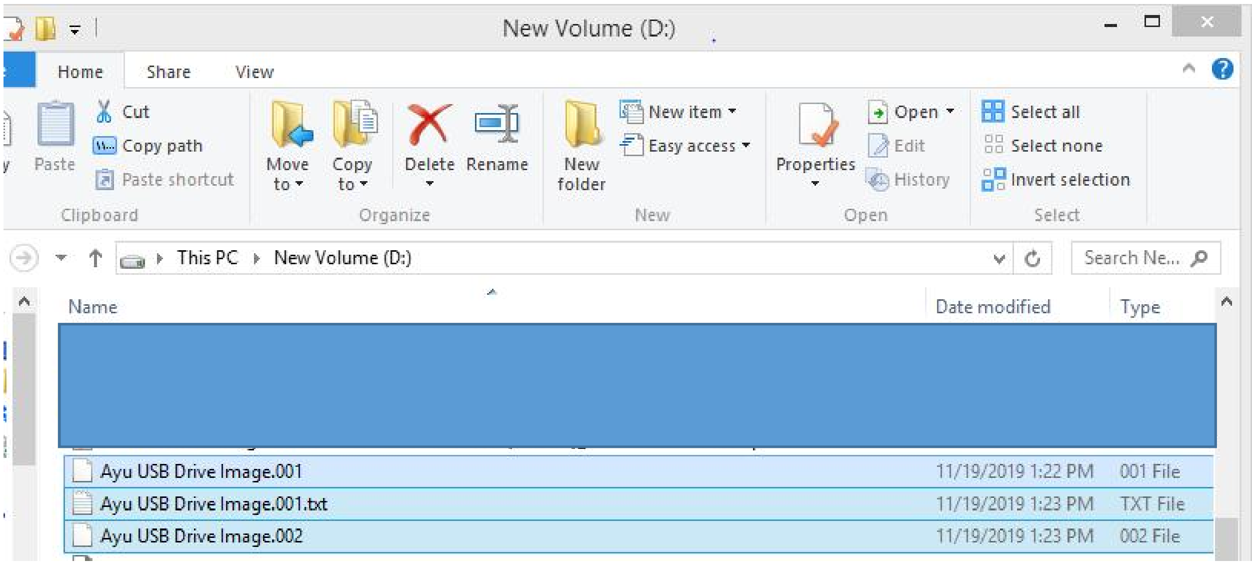
14. Click on 'Image Summary' to view the results pertaining to the image that has just been created as shown in Figure 6.12. This information should verify what was entered in the creation process. It will also verify the created hashes. Also, for your reference, this information has been printed out into a text file in the location to which the image file was saved.



```
Created By AccessData® FTK® Imager 2.9.0.1385 100406

Case Information:
Case Number: 001
Evidence Number: 001
Unique description: Ayu USB Drive Analysis
Examiner: Hakim
Notes:

--------------------------------------------------------------

Information for D:\Ayu USB Drive Image:

Physical Evidentiary Item (Source) Information:
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 3,948,480
 Source data size: 1927 MB
 Sector count:    3948480
[Computed Hashes]
 MD5 checksum:    6ebe2f61ac0d5e27d4dd2c0595c67d4b
 SHA1 checksum:   2985bd81ce974d87c45b9d40e7841e5c58971844

Image Information:
 Acquisition started:   Tue Nov 19 13:20:48 2019
```

Figure 6.12 Summary

15. Note that the image file **(Ayu USB Drive Image.001 & Ayu USB Drive Image.001)** as well as the image summary file from above **(Ayu USB Drive Image.txt)** have been saved onto the 'D: Ayu USB Drive'. The .001 extension may be left as is, or can be changed to .dd. The .001 extension is used due to the fact that many times the file to be imaged is very large and must be split into multiple chunks. In that case, you would have Ayu USB Drive Image.001, Ayu USB Drive Image.001, etc.



[redacted]

Name	Date modified	Type
Ayu USB Drive Image.001	11/19/2019 1:22 PM	001 File
Ayu USB Drive Image.001.txt	11/19/2019 1:23 PM	TXT File
Ayu USB Drive Image.002	11/19/2019 1:23 PM	002 File

Figure 6.13 Summary of Image File

At this point, the disk image has been created. This is essential for analyzing the contents without touching the original drive.