

# Lab 2

## Introduction to Forensics Tools and Data Acquisition

---

**Shrutika Joshi – HA72777**

**Date – 26June23**

**Introduction** – The goal is to perform forensics investigation on two electronic devices (USB devices) using ProDiscover and FTK Imager tools and acquire image of evidence. This document outlines all steps involve during Forensic Investigation which will be helpful in maintaining records and ensuring accuracy.

**Objective** – The objective is to simulate process of acquiring evidence from two USB devices and document all steps covered during investigation. As a forensic investigator, It is suspected that two sub drives (USB devices) which search team found may contain some evidence. Also search warrant approves searching of possible crime and evidence in this found USB devices.

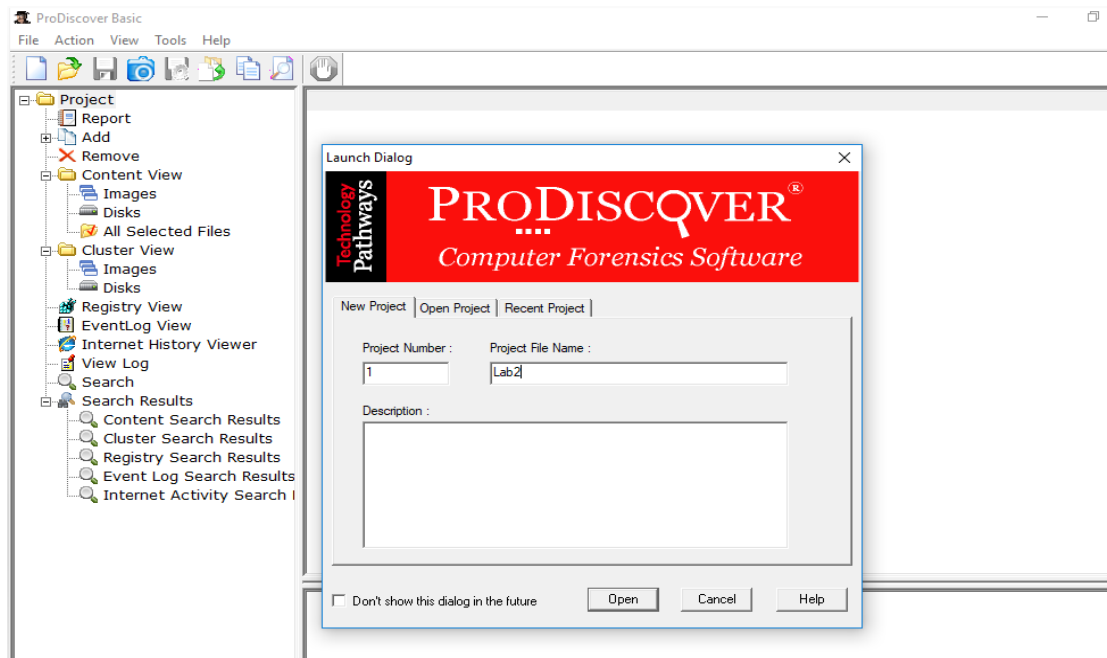
**Equipment and Tools** – During this investigation ProDiscover and FTK Imager tools are being used to capture forensic image from USB drive.

### **Acquisition Process:**

- **Identify and Label USB Devices:** The acquisition process will start with inspecting the found two USB devices and assigning unique label or identifier to each USB device to maintain accurate documents and chain of custody.
- Connect USB device to forensic workstation and ensure write-blocking device is properly attached to prevent any unintentional modification.
- Confirm whether forensic workstation is recognizing the USB device and documents USB details like model number, serial number, and manufacturer.

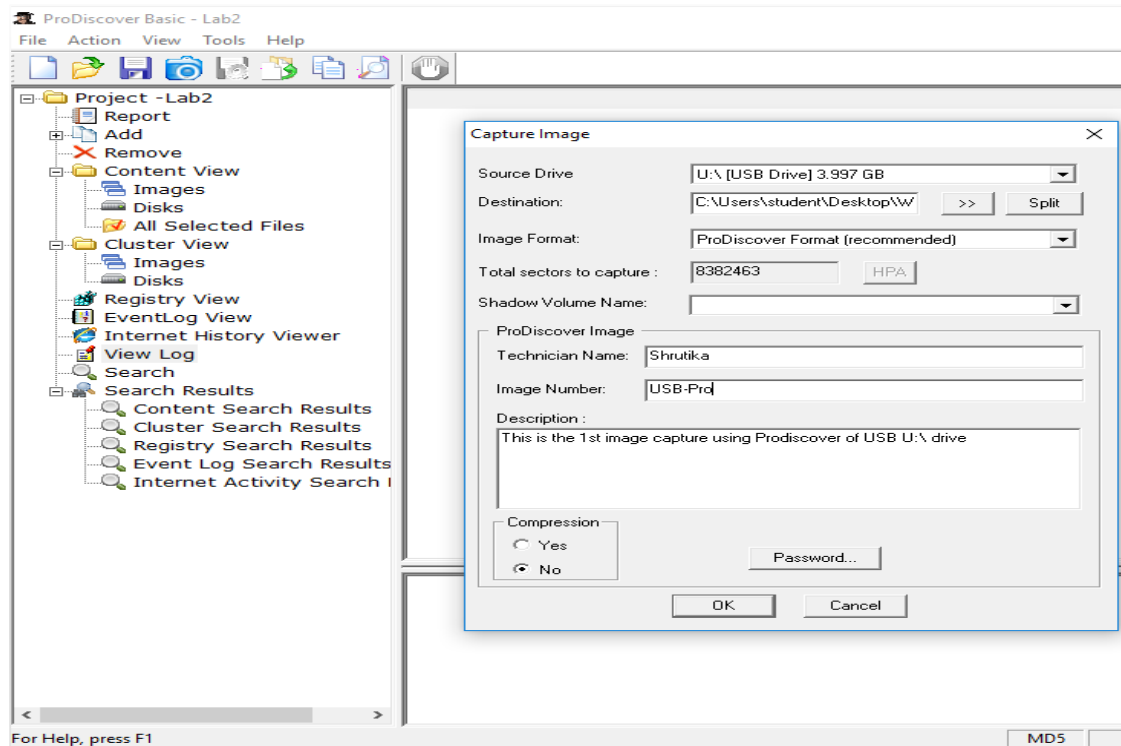
## Image Acquisition of USB Drive (U:) using ProDiscover:

- Run the Prodiscover tool as an administrator and mention the Project name and number in the text box and click 'Open'

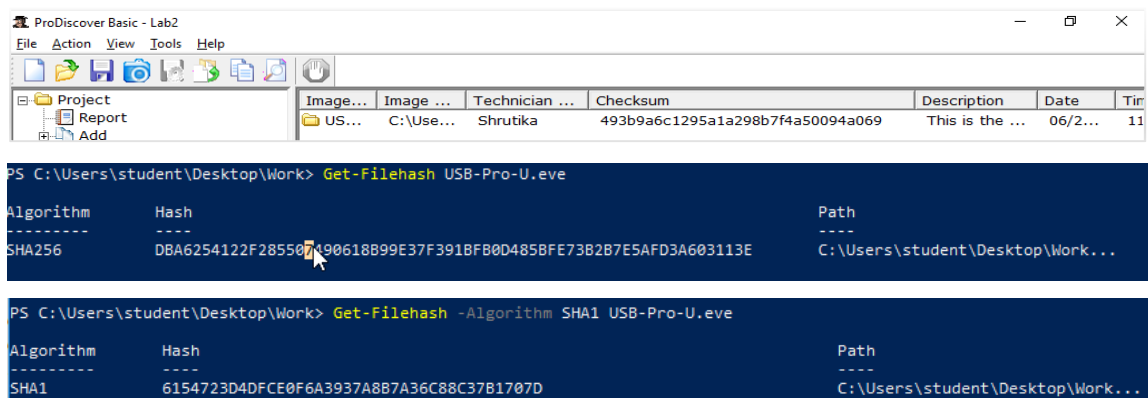


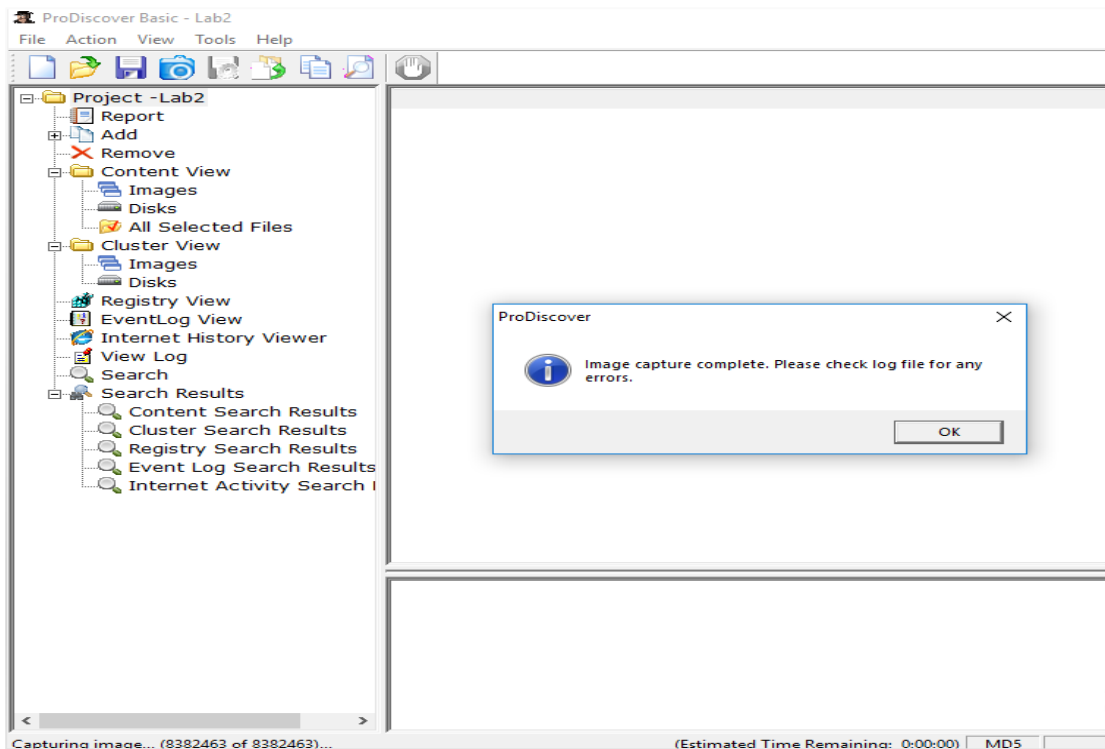
- Click on the Action → Capture Image and fill out the details in the capture image window such as
- Source drive: U:\ [USB Drive] 3.997 GB
- Select the Destination folder: C:\Users\student\Desktop\Work
- File Name: USB-Pro-U
- Image Format as: ProDiscover format
- 'Total sectors to capture' will auto populate
- Technician Name: Shrutika
- Image Name: USB-Pro
- Mention the details of project in the Description text box
- You can password protect the file as well if additional security is needed
- If you need to save space on your target drive, click the Yes option button in the Compression section.

- Click 'OK' to begin the acquisition after filling all the details in the capture image dialog box. During the process ProDiscover displays a status bar in the lower right corner to show the progress. ProDiscover creates a Image file in the selected destination folder.

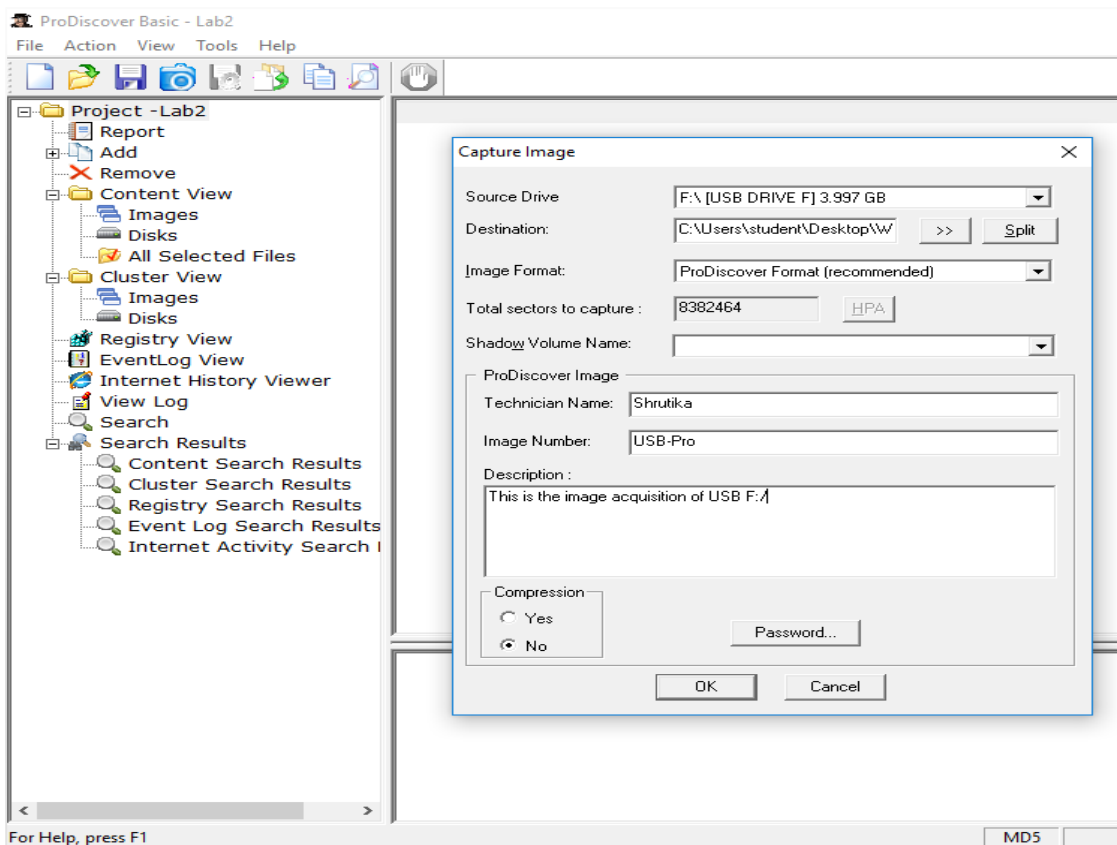


- When the acquisition is done, ProDiscover displays a message box instructing you to examine a log file for errors. Click 'OK' to complete the acquisition, and then exit ProDiscover Basic.
- ProDiscover then creates image file with '.eve extension' and log file with '.log extension' in the Work folder.
- Below are hash of file in MD5, SHA256, and SHA1 format





### Image Acquisition of USB Drive (F :) using ProDiscover:



- Below are hash of file in SHA256, SHA1 and MD5 format

```
PS C:\Users\student\Desktop\Work> Get-Filehash USB-Pro-F.eve

Algorithm      Hash
-----
SHA256         008781D3DCFE30939EB5EEA86658FD665007DFC523E457A264B2A3A6A6AD2388
Path           C:\Users\student\Desktop\Work...
```

```
PS C:\Users\student\Desktop\Work> Get-Filehash -Algorithm SHA1 USB-Pro-F.eve

Algorithm      Hash
-----
SHA1           53312501A9FEE1B32E8ADF53E65DEC1D8C8853A2
Path           C:\Users\student\Desktop\Work...
```

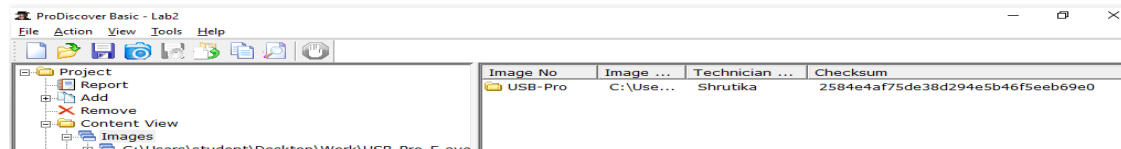
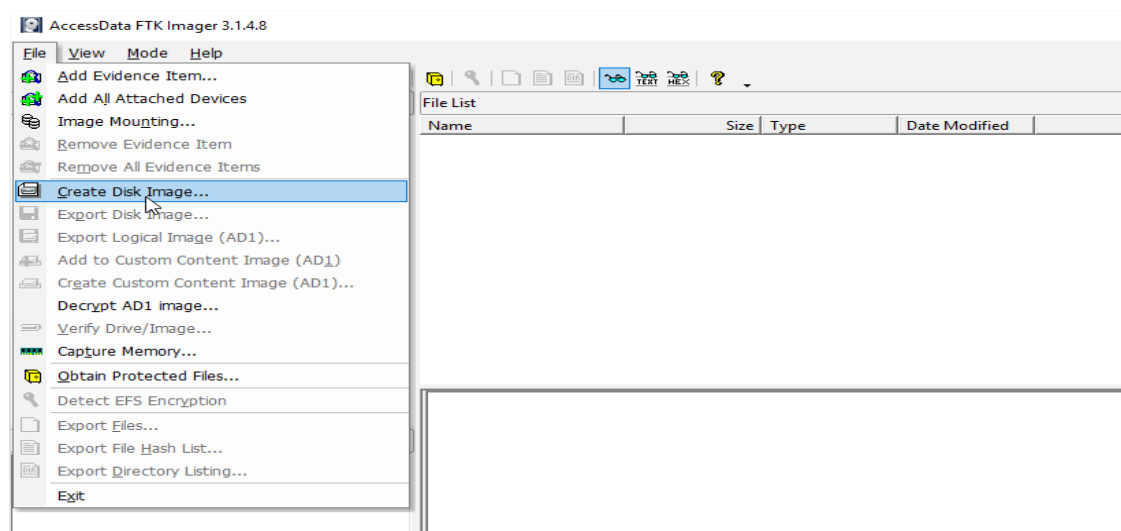


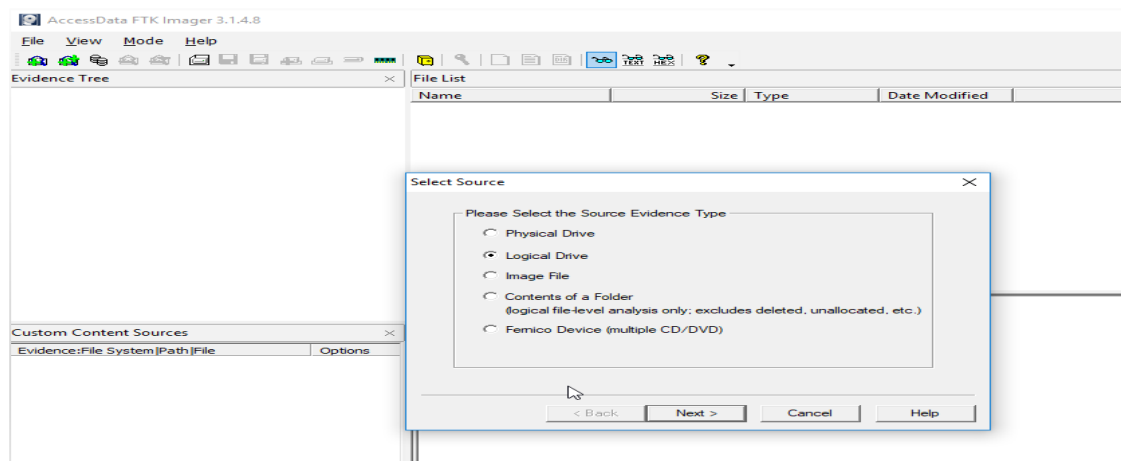
Image No	Image ...	Technician ...	Checksum
USB-Pro	C:\Use...	Shrutika	2584e4af75de38d294e5b46f5eeb69e0

## Image Acquisition of USB Drive (U :) using FTK Imager:

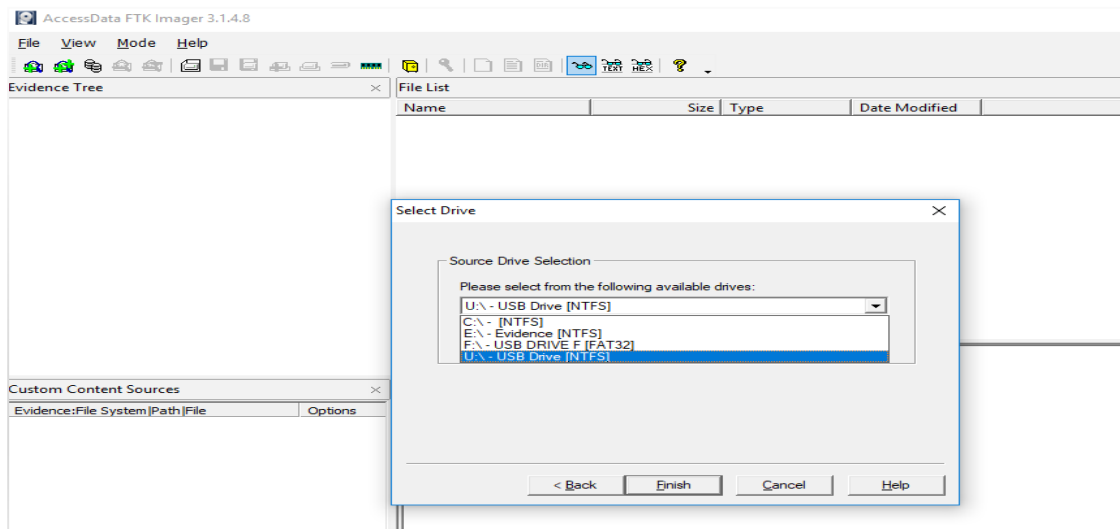
- Run the FTK Imager tool as an administrator click File → Create Disk image



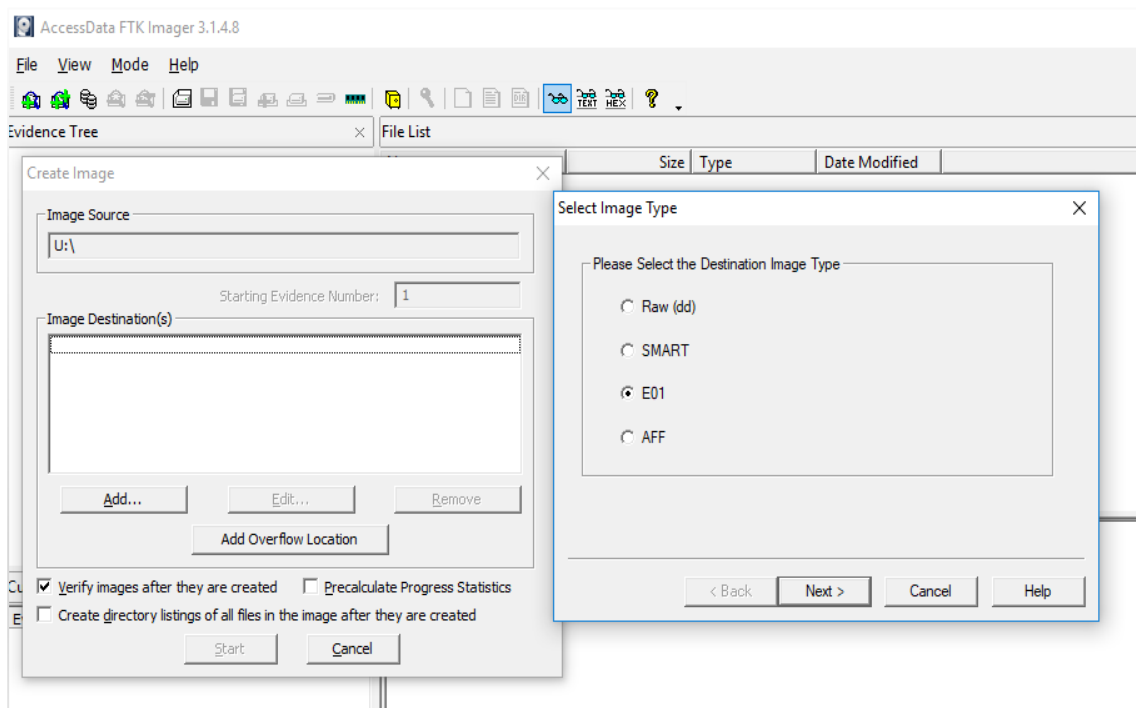
- In the Select Source dialog click 'Logical Drive' option and click Next button



- In the select Drive dialog select USB drive (U:) and click Finish

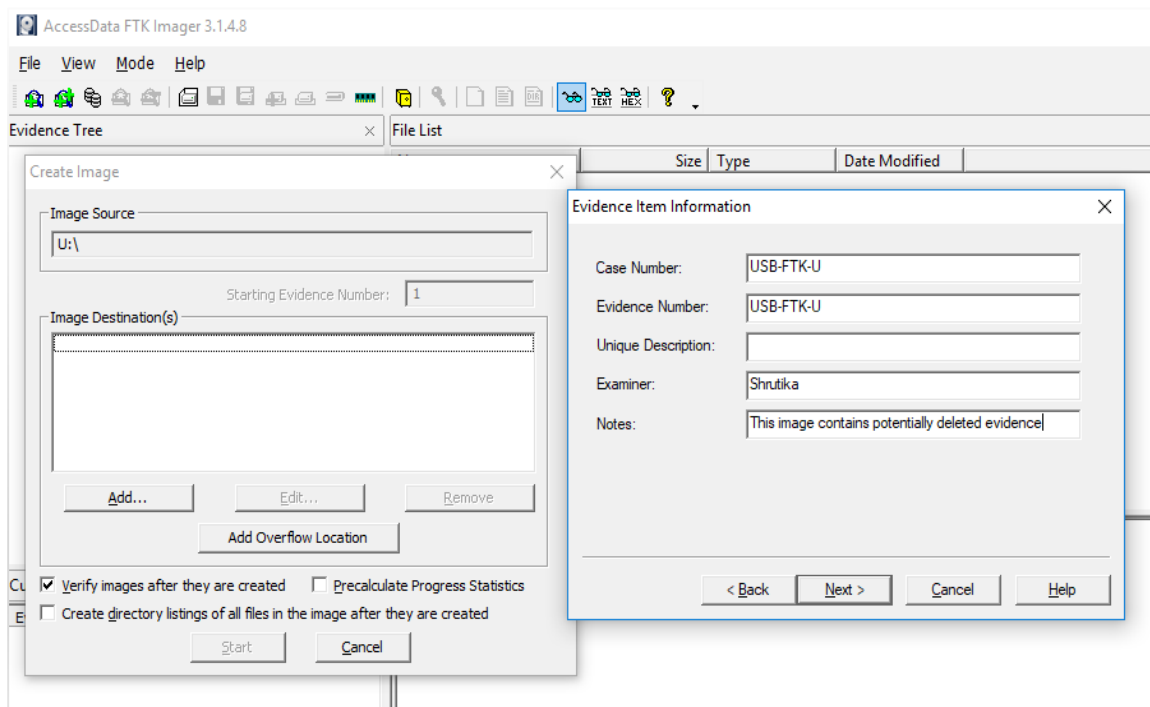


- In the create image dialog click on Add button and select E01 as a destination image type and click Next.

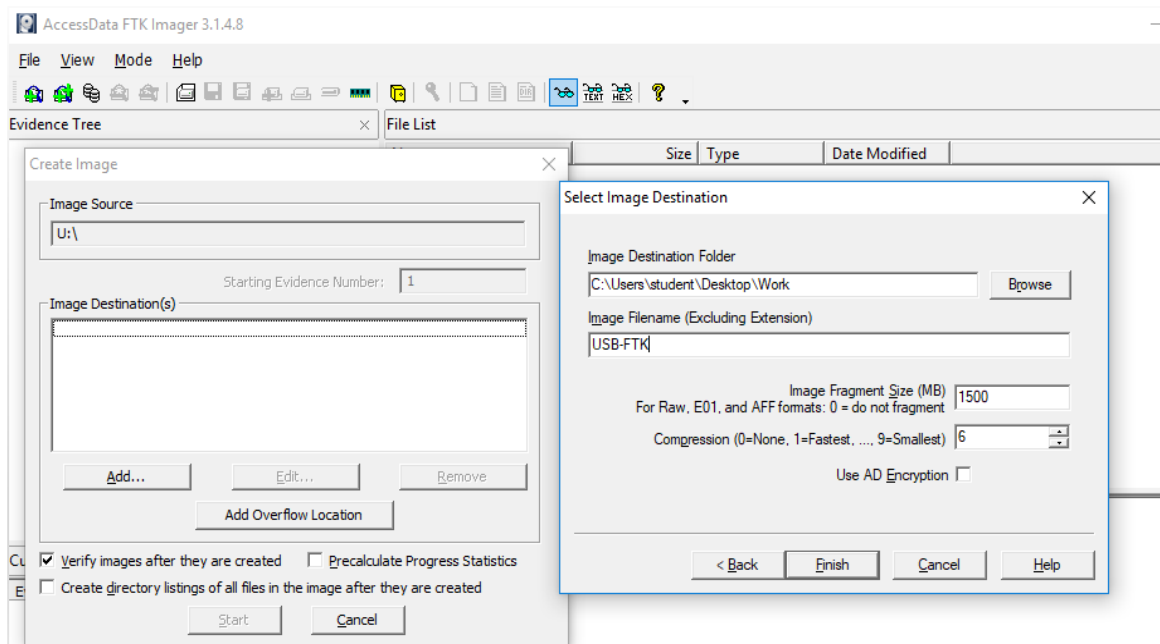


- Add the evidence item information in the dialog box as below
  - Case Number: USB-FTK-U
  - Evidence Number: UAB-FTK-U
  - Add Examiner name : Shrutika

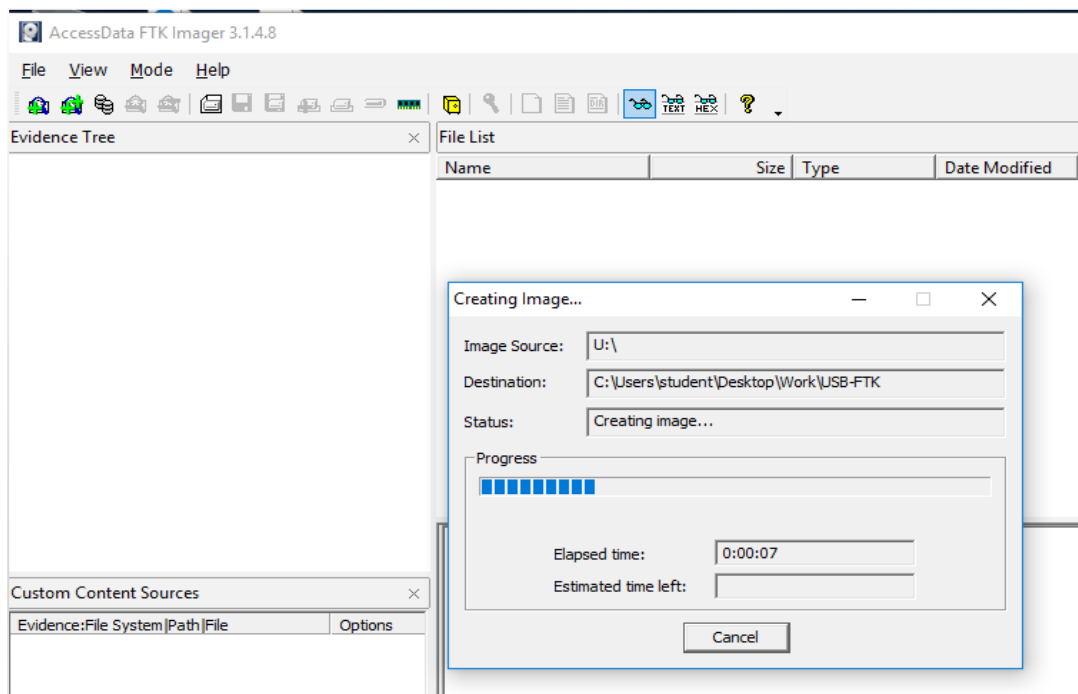
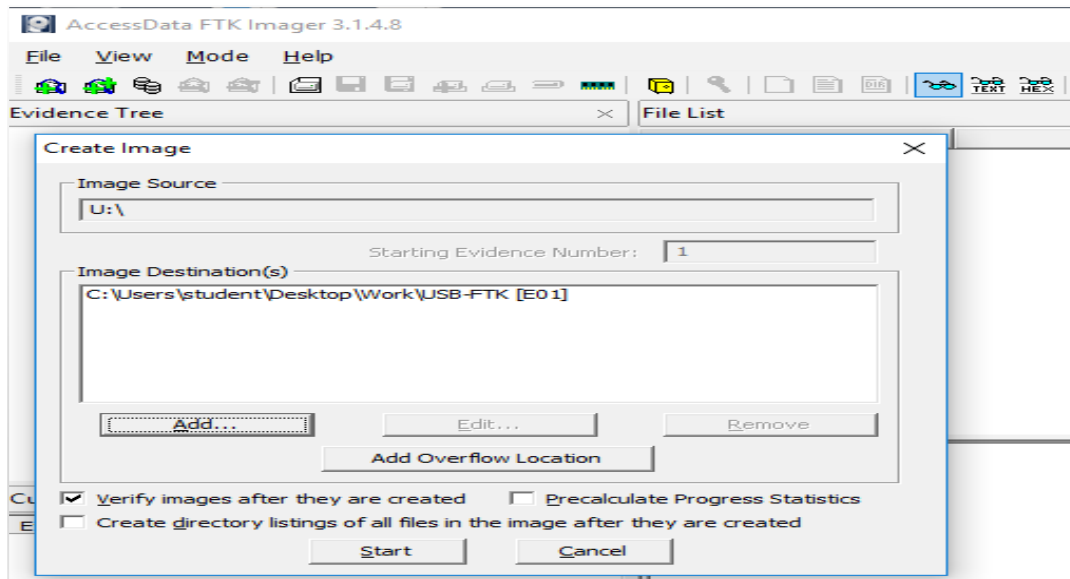
- Add the notes of case in the notes section and click Next.



- In the Image Destination folder select the working folder and add Image Name as USB-FTK and click Finish
- Use AD encryption if encryption is needed for evidence
- Image Fragment and compression details will auto populate which is as below for this evidence. Image Fragment: 1500, Compression: 06

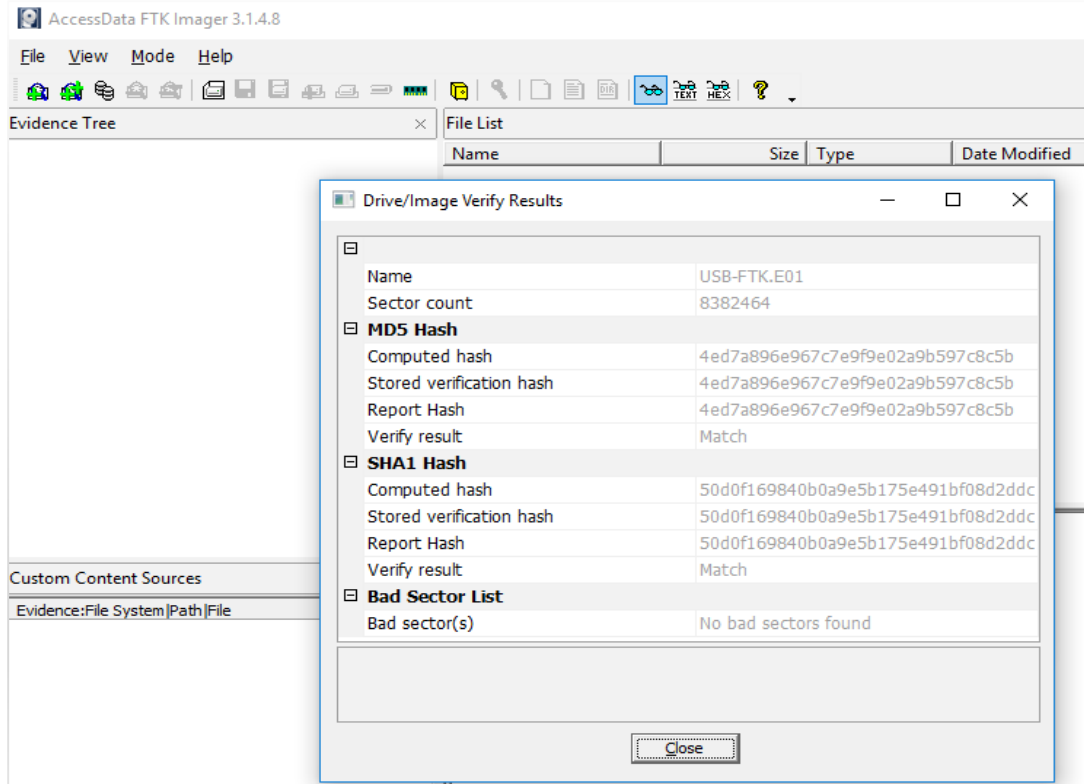


- Click on Start button and creating image dialog will populate showing the progress of image acquisition and time remaining for the process



- After completing the process hash details will generate containing hash of image in SHA1 and MD5 format and sector count is 8382464





Created By AccessData® FTK® Imager 3.1.4.8

**Case Information:**

Acquired using: ADI3.1.4.8

Case Number: USB-FTK-U

Evidence Number: USB-FTK-U

Unique description: This image contains potentially deleted evidence

Examiner: Shrutika

Notes: This image contains potentially deleted evidence

-----  
[Information for C:\Users\student\Desktop\Work\USB-FTK:

**Physical Evidentiary Item (Source) Information:**

**[Device Info]**

Source Type: Logical

**[Drive Geometry]**

Bytes per Sector: 512

Sector Count: 8,382,464

**[Physical Drive Information]**

Removable drive: False

Source data size: 4093 MB

Sector count: 8382464

**[Computed Hashes]**

MD5 checksum: 4ed7a896e967c7e9f9e02a9b597c8c5b

SHA1 checksum: 50d0f169840b0a9e5b175e491bf08d2ddc728d4c

**Image Information:**

Acquisition started: Sun Jun 25 12:51:14 2023

Acquisition finished: Sun Jun 25 12:51:45 2023

**Segment list:**

C:\Users\student\Desktop\Work\USB-FTK.E01

**Image Verification Results:**

Verification started: Sun Jun 25 12:51:45 2023

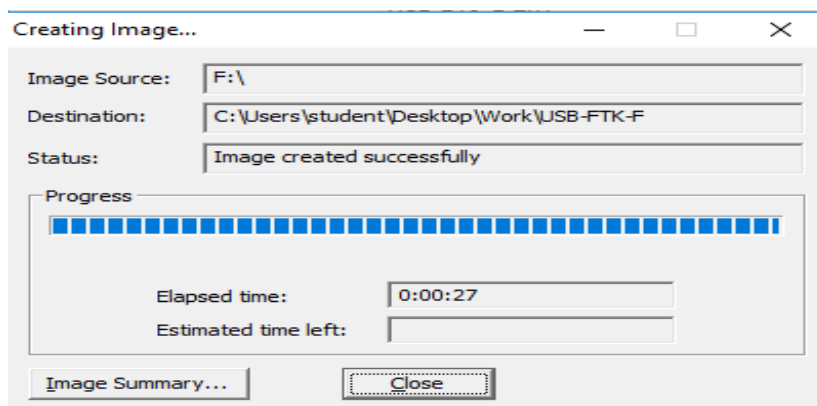
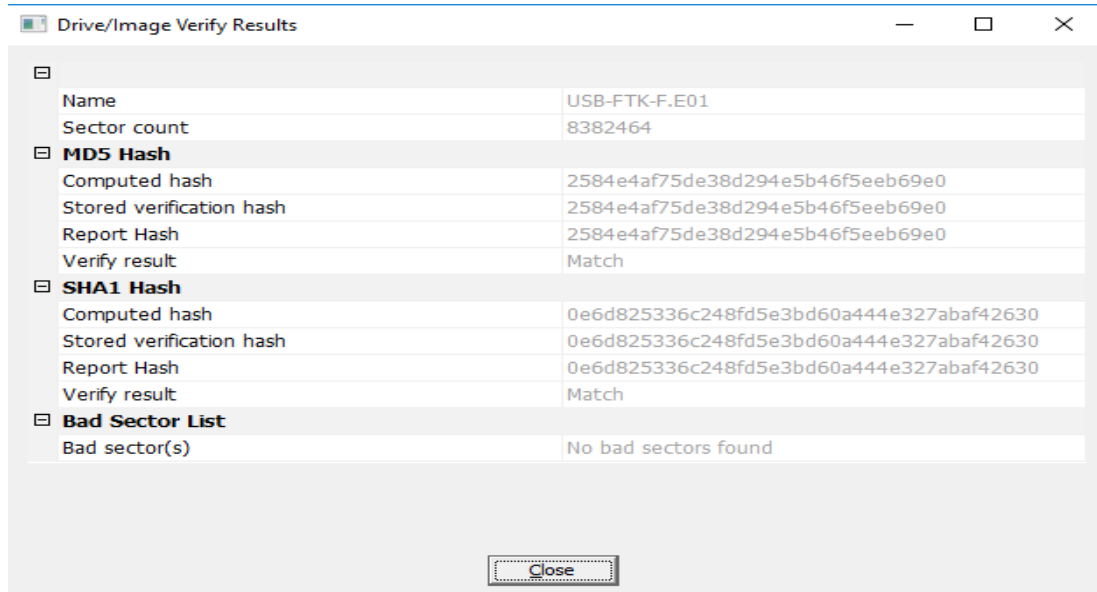
Verification finished: Sun Jun 25 12:52:03 2023

MD5 checksum: 4ed7a896e967c7e9f9e02a9b597c8c5b : verified

SHA1 checksum: 50d0f169840b0a9e5b175e491bf08d2ddc728d4c : verified

## Image Acquisition of USB Drive (F :) using FTK Imager:

- Same steps have been followed while creating image for USB drive (F:) and below are the hash details for USB drive (F:)



```
USB-FTK-F.E01.txt - Notepad
File Edit Format View Help

Case Information:
Acquired using: ADI3.1.4.8
Case Number: USB-FTK-F
Evidence Number: USB-FTK-F
Unique description: This image contains potentially deleted evidence
Examiner: Shrutika
Notes: This image contains potentially deleted evidence
-----|
Information for C:\Users\student\Desktop\Work\USB-FTK-F:

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Logical
[Drive Geometry]
Bytes per Sector: 512
Sector Count: 8,382,464
[Physical Drive Information]
Removable drive: False
Source data size: 4093 MB
Sector count: 8382464
[Computed Hashes]
MD5 checksum: 2584e4af75de38d294e5b46f5eeb69e0
SHA1 checksum: 0e6d825336c248fd5e3bd60a444e327abaf42630

Image Information:
Acquisition started: Sun Jun 25 13:06:09 2023
Acquisition finished: Sun Jun 25 13:06:36 2023
Segment list:
C:\Users\student\Desktop\Work\USB-FTK-F.E01

Image Verification Results:
Verification started: Sun Jun 25 13:06:36 2023
Verification finished: Sun Jun 25 13:06:54 2023
MD5 checksum: 2584e4af75de38d294e5b46f5eeb69e0 : verified
SHA1 checksum: 0e6d825336c248fd5e3bd60a444e327abaf42630 : verified
```

## Conclusion:

- As given above MD5 sum is generated on all of the image. The MD5 sum serves as a signature and ensure integrity of a file, any changes in contents of the image or the USB drive will cause a different MD5 sum be generated.
- After generating forensic image for both the drive (U: , F:), it is concluded that hash file both the images using different tools are defer as each forensic tool may interpret file formats differently. Also there are algorithmic differences which each forensics tool uses.
- Also metadata files are missing from the drive (F:).

## Citations:

- [1] Mahalik, Heather. "Get Started in Digital Forensics | sans Institute." *Www.sans.org*, 2023, [www.sans.org/mlp/get-started-in-digital-forensics/ppc/?utm\\_medium=CPC&utm\\_source=Google&utm\\_content=Core&utm\\_campaign=St](http://www.sans.org/mlp/get-started-in-digital-forensics/ppc/?utm_medium=CPC&utm_source=Google&utm_content=Core&utm_campaign=St)

art%20in%20DFIR&gclid=Cj0KCQjwnMWkBhDLARIsAHBOfrNCarwiBgR9suYsgEyEbMd9w1U-czwe-IH9dVejh7YSzn6v9VBikYaApPrEALw\_wcB. Accessed 26 June 2023.

- [2] Yuen, Cheuk Wai. "Global Information Assurance Certification Paper." *Giac.org*, 2023, [www.giac.org/paper/gcfa/264/analysis-seized-usb-flashdrive/108052](http://www.giac.org/paper/gcfa/264/analysis-seized-usb-flashdrive/108052) .
- [3] Smith, J. D. (2015). Forensics Analysis of USB Flash Drives in Educational Environment. *Journal of Digital Forensics, Security and Law*, 10(2), 123-137. Retrieved from ResearchGate:[https://www.researchgate.net/publication/271825884\\_Forensics\\_Analysis\\_of\\_USB\\_Flash\\_Drives\\_in\\_Educational\\_Environment](https://www.researchgate.net/publication/271825884_Forensics_Analysis_of_USB_Flash_Drives_in_Educational_Environment)
- [4] Ch, Raj, and el. "USB Forensics: Detection & Investigation." *Hacking Articles*, 9 Sept. 2020, [www.hackingarticles.in/usb-forensics-detection-investigation/](http://www.hackingarticles.in/usb-forensics-detection-investigation/).