LAB REPORT

20th February 2025

Data Acquisition Practical

Name : Sarthak Das

Session : 11th February – 22nd April 2025

For the class of Computer Forensic, taught by

Drabanti Boral

Contents

1 Introduction

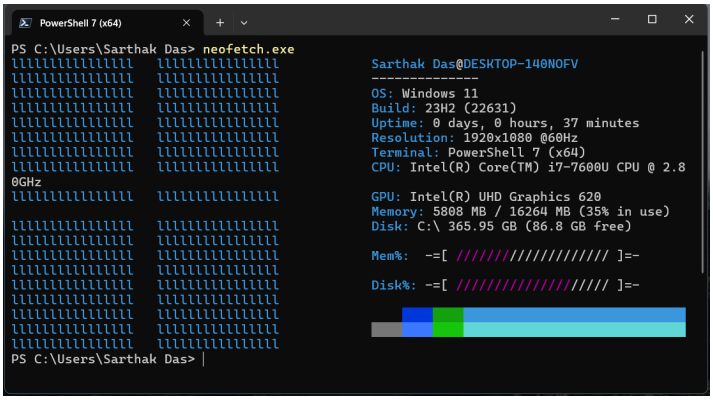
1.1 Objectives

This report is a documentation of my lab work as assigned on 18th February, 2025. The primary objectives of this lab are two-fold:

- Acquiring non-volatile data from a physical drive.
- Acquiring non-volatile data from a logical drive.

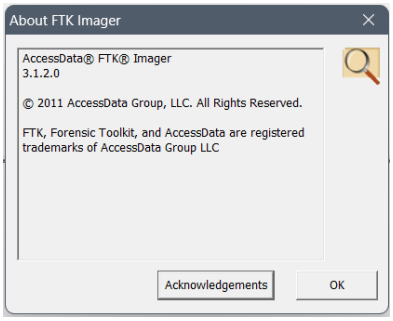
1.2 System Information

For the purposes of this lab, a Lenovo ThinkPad X270 was used, having the following system specifications: Intel Core i7-7600U CPU @ 2.80GHz with Intel UHD Graphics 620, 16GB RAM, 1TB SSD running operating system Windows 11 23H2 (Build 22631).



1.3 Software Used

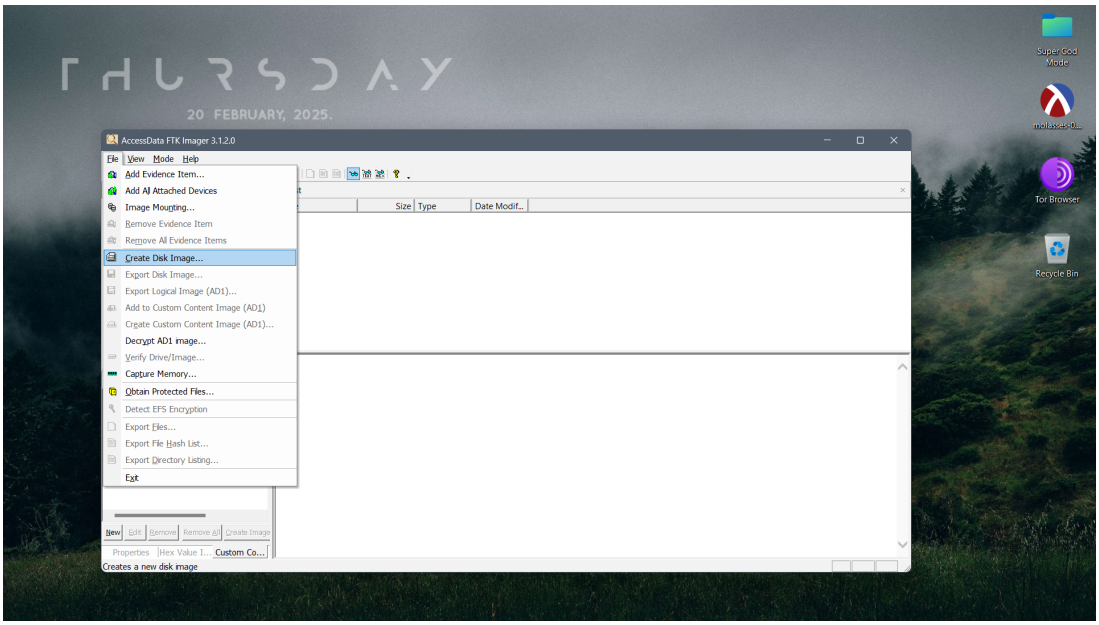
The software used for this data acquisition practical is AccessData FTK Imager version 3.1.2.0.



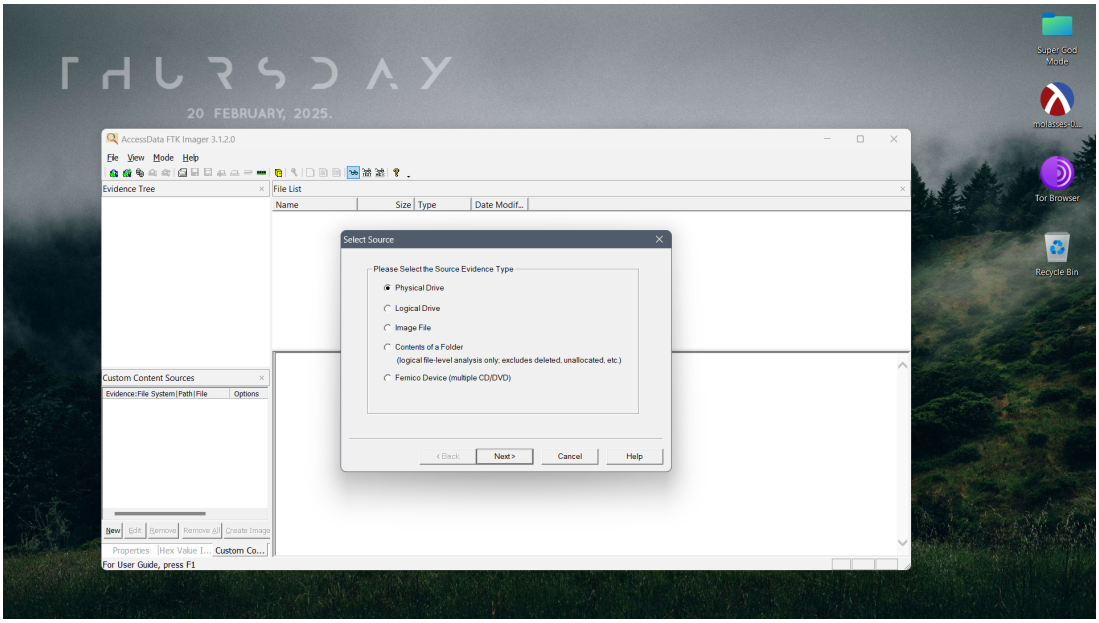
2 Objective 1: Physical Drive

2.1 Methodology

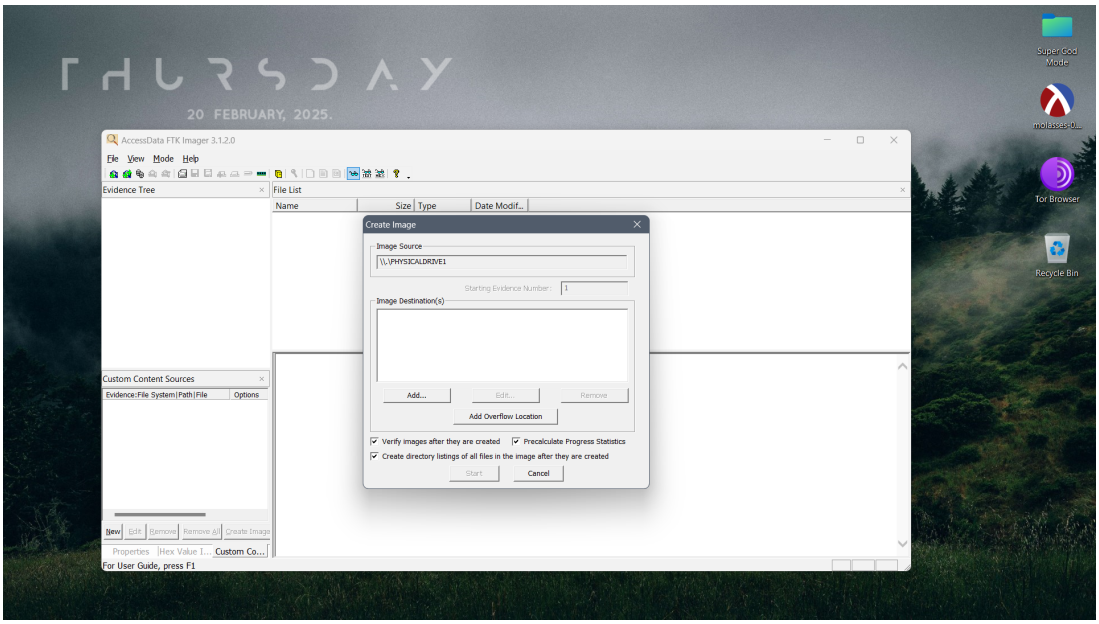
We begin by opening AccessData FTK Imager, and selecting **File** > *Create Disk Image*.



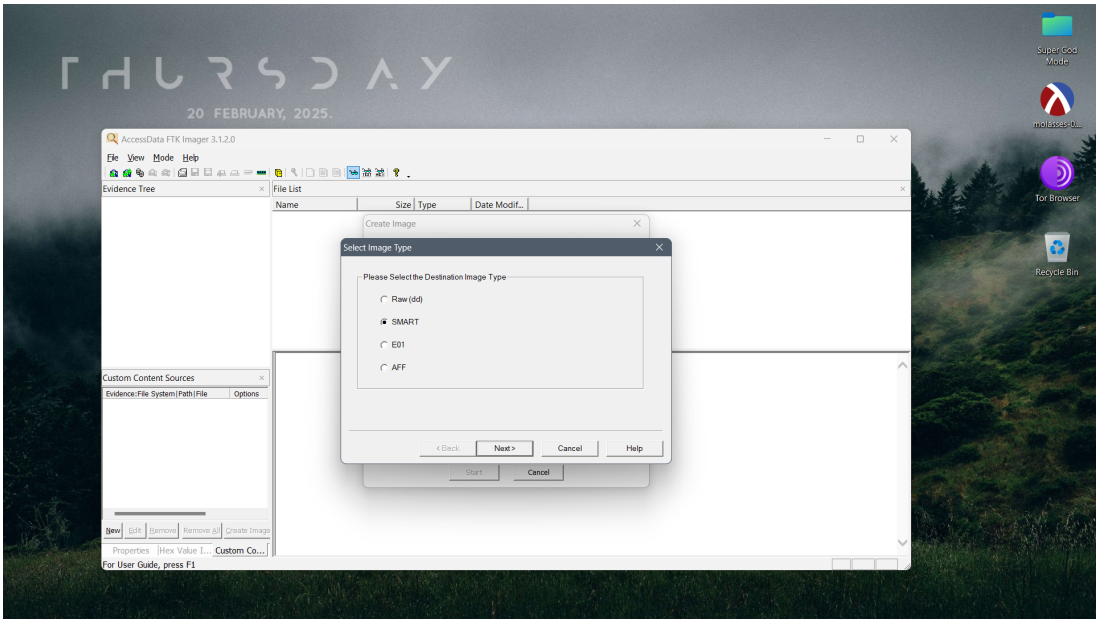
In our first objective, we will create image from a physical drive.



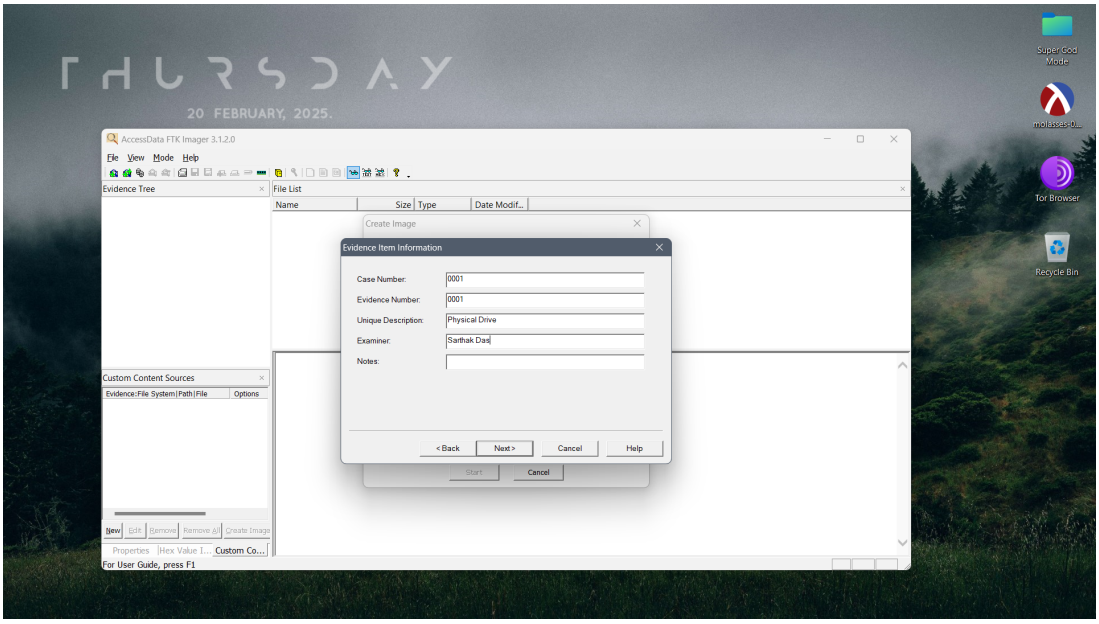
For the purposes of this lab, we have selected a 128GB SanDisk Cruzer Blade USB stick as the physical drive to image. Now, we must select a destination to save the physical drive disk image.



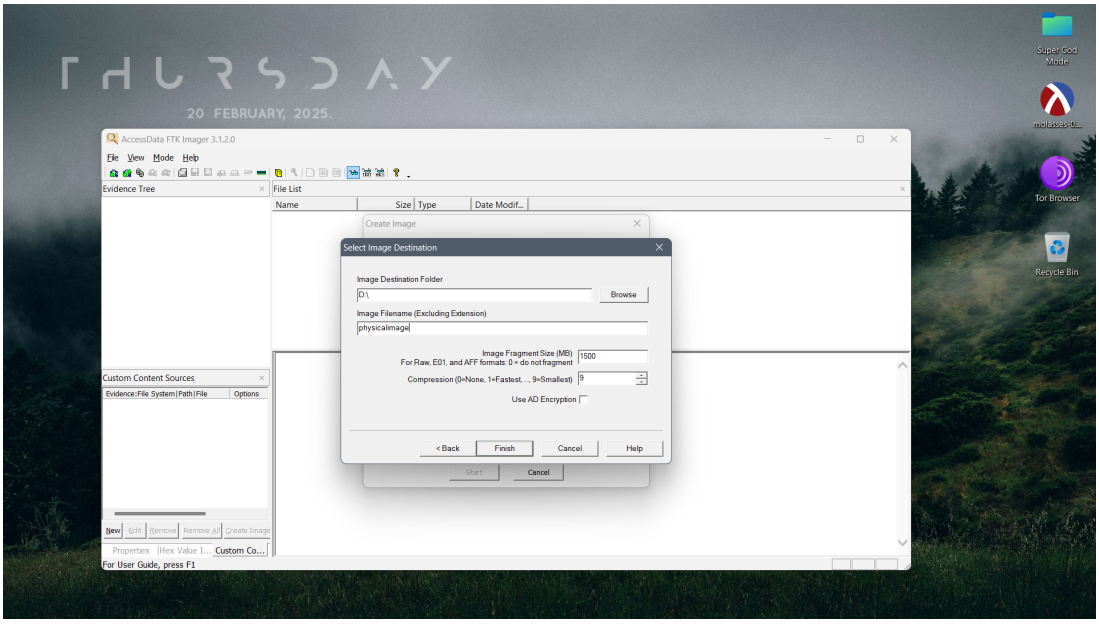
We choose the image type as *SMART*, because it enables compression, unlike *Raw (dd)*.



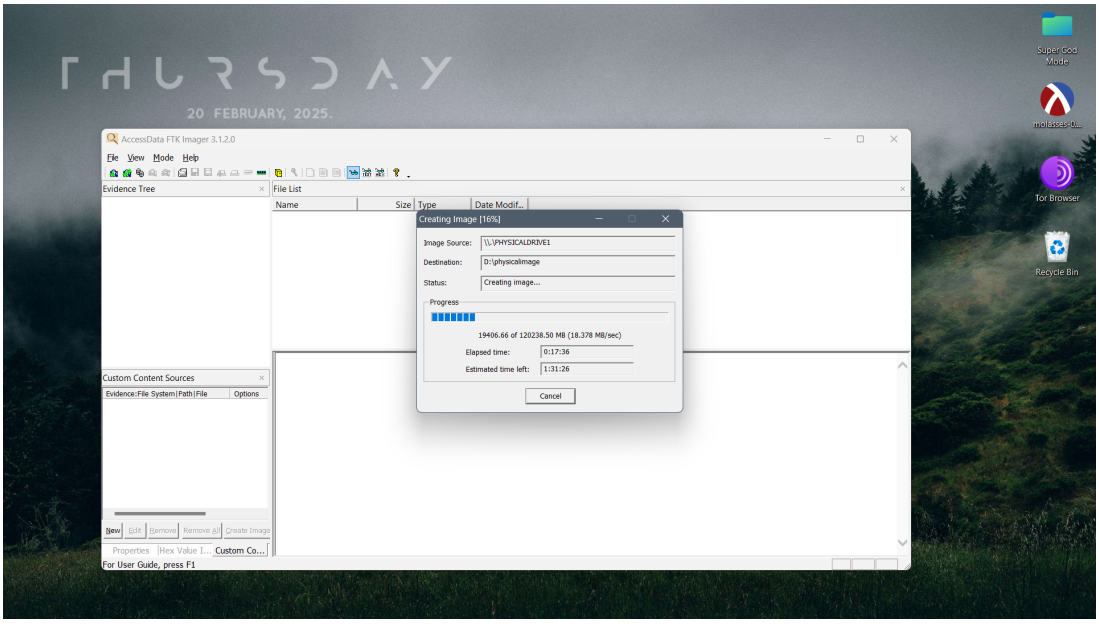
Next, we will enter the evidence item information.



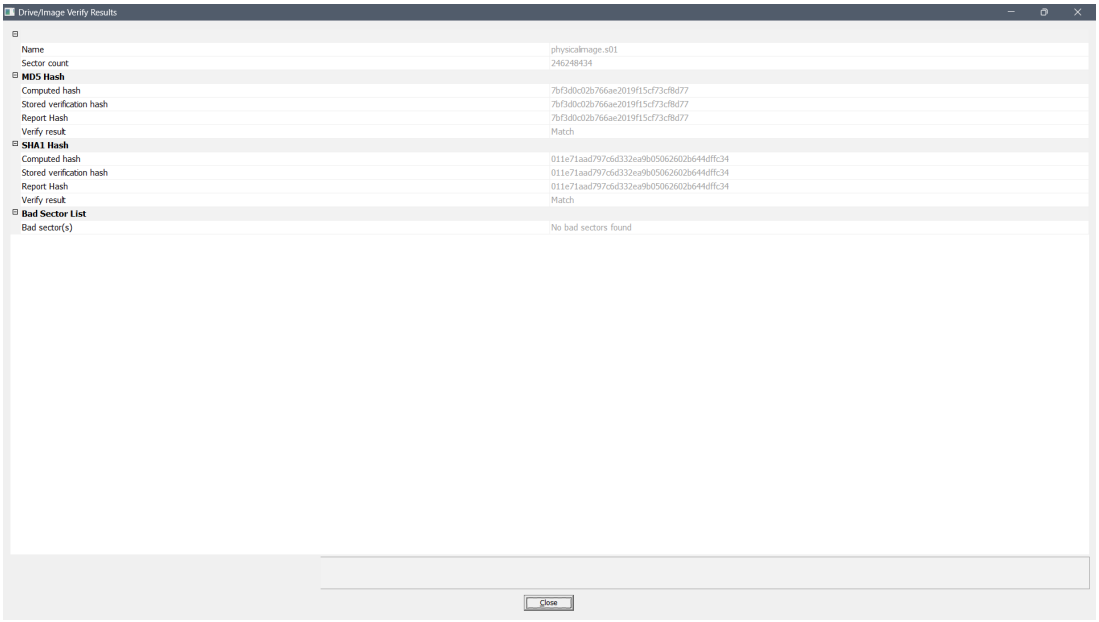
We proceed with the default value for image fragment size (1500 MB) and choose compression mode 9 with the smallest image size. We leave the *Use AD encryption* option unchecked, enter our desired image name (*physicalimage*) and click **Finish**.



The process begins upon clicking **Start**.



The process takes 2 hours, 17 minutes and 51 seconds to complete. Upon completion of the process, the directory listing is dumped into a CSV file, the image is verified and a report is generated.



2.2 Report

Report generated by AccessData FTK Imager

```
Created By AccessData® FTK® Imager 3.1.2.0

Case Information:
Acquired using: ADI3.1.2.0
Case Number: 0001
Evidence Number: 0001
Unique description: Physical Drive
Examiner: Sarthak Das
Notes:

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

Information for D:\physicalimage:

Physical Evidentiary Item Source Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 15,328
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 246,248,434
[Physical Drive Information]
 Drive Model: SanDisk Cruzer Blade USB Device
 Drive Serial Number: 03044827092321185600
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 120238 MB
 Sector count:    246248434
[Computed Hashes]
 MD5 checksum:    7bf3d0c02b766ae2019f15cf73cf8d77
 SHA1 checksum:   011e71aad797c6d332ea9b05062602b644dffc34

Image Information:
 Acquisition started:   Thu Feb 20 15:23:57 2025
 Acquisition finished:  Thu Feb 20 17:41:49 2025
 Segment list:
  D:\physicalimage.s01
  D:\physicalimage.s02
  D:\physicalimage.s03
  D:\physicalimage.s04
  D:\physicalimage.s05
  D:\physicalimage.s06
  D:\physicalimage.s07
```

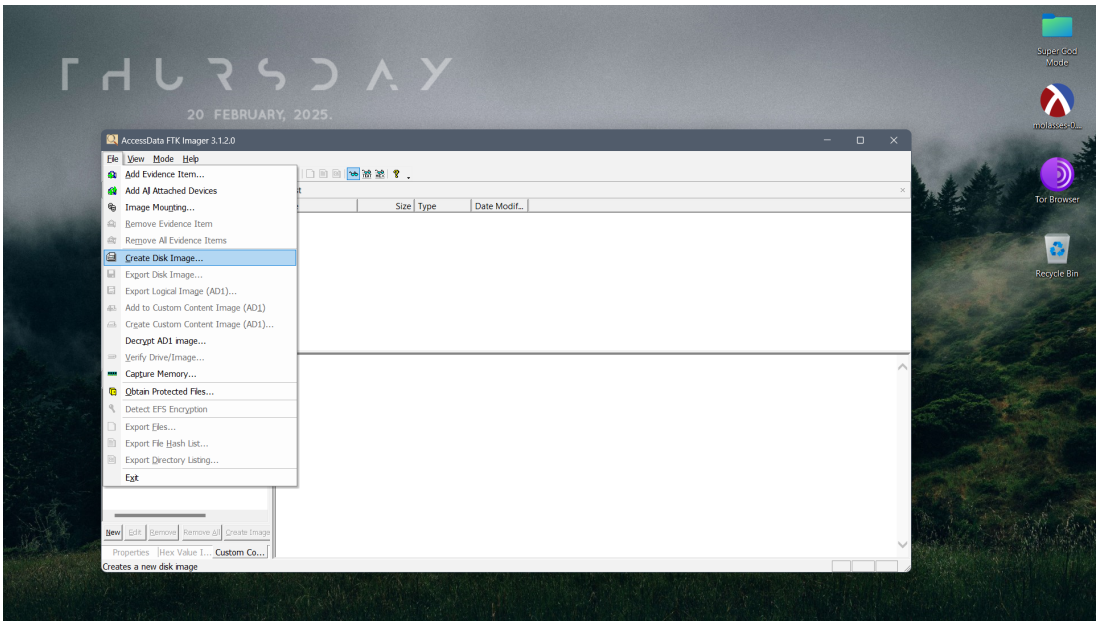
```
  D:\physicalimage.s08
  D:\physicalimage.s09
  D:\physicalimage.s10
  D:\physicalimage.s11
  D:\physicalimage.s12
  D:\physicalimage.s13
  D:\physicalimage.s14
  D:\physicalimage.s15
  D:\physicalimage.s16
  D:\physicalimage.s17
  D:\physicalimage.s18
  D:\physicalimage.s19
  D:\physicalimage.s20
  D:\physicalimage.s21
  D:\physicalimage.s22
  D:\physicalimage.s23

Image Verification Results:
 Verification started:  Thu Feb 20 17:41:49 2025
 Verification finished: Thu Feb 20 18:00:14 2025
 MD5 checksum:    7bf3d0c02b766ae2019f15cf73cf8d77 : verified
 SHA1 checksum:   011e71aad797c6d332ea9b05062602b644dffc34 : verified
```

---

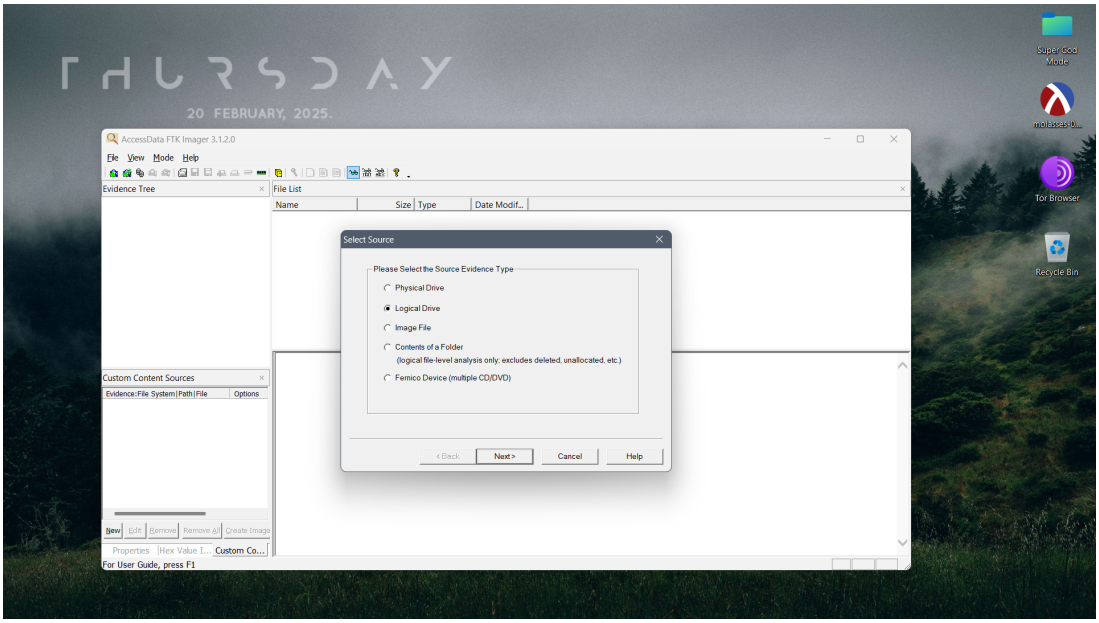
3 Objective 2: Logical Drive

3.1 Methodology

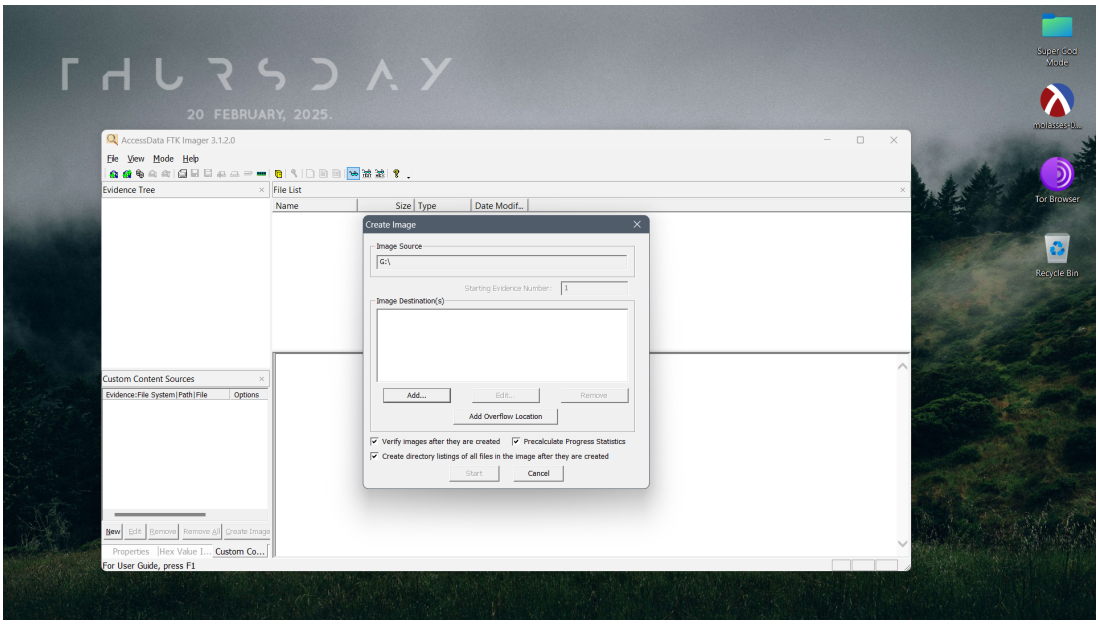
Again, we open AccessData FTK Imager and select **File** > *Create Disk Image*.



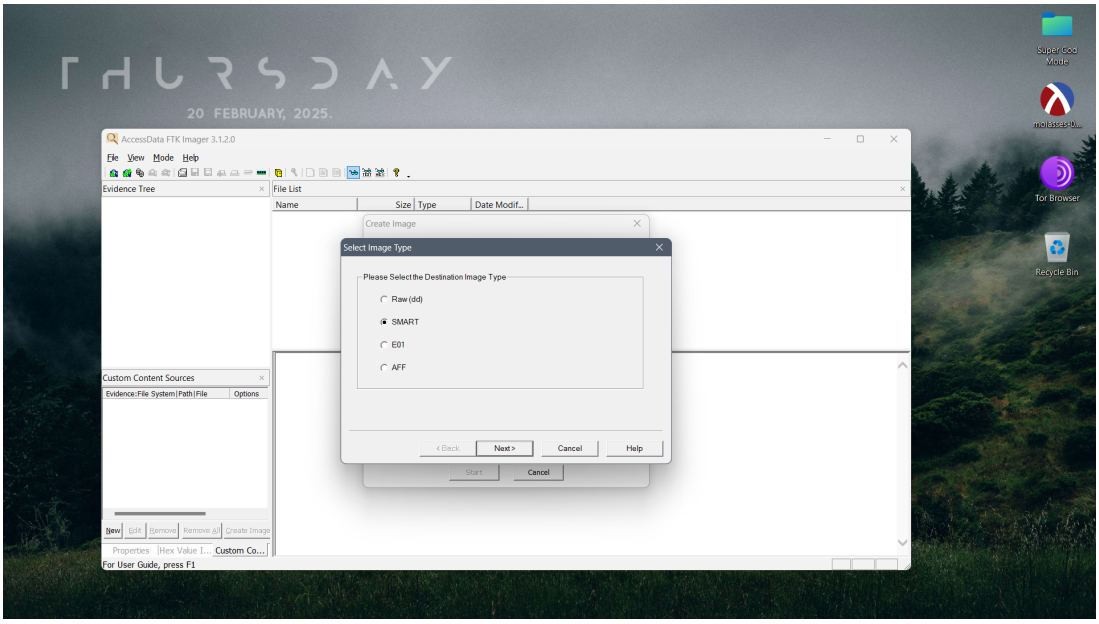
In this second objective, we will create image from a logical drive instead of a physical drive.



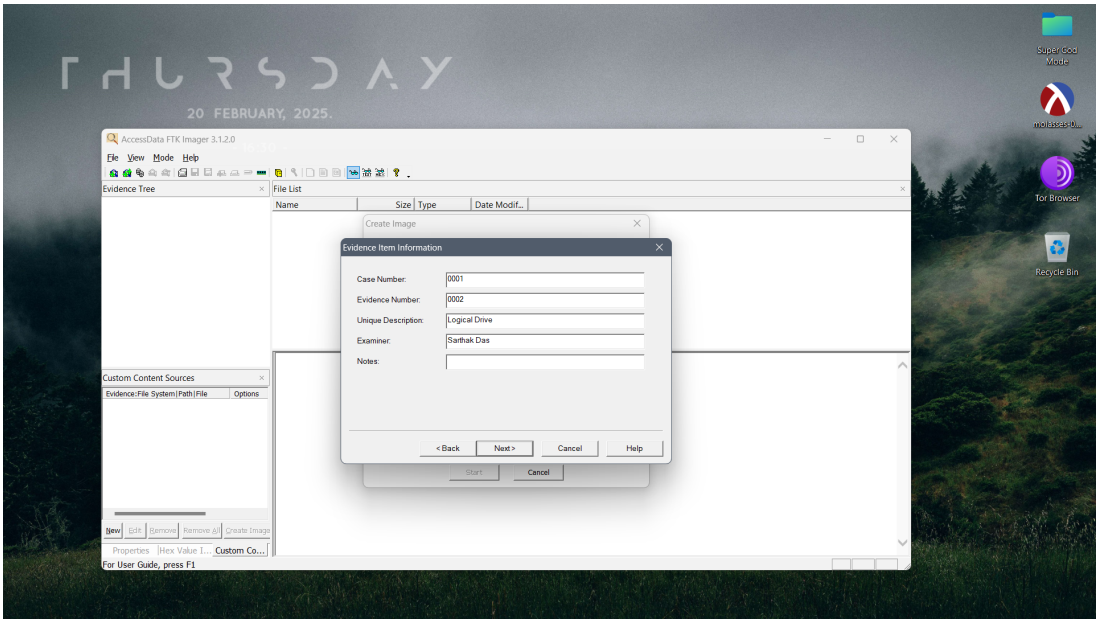
For the purposes of this lab, we have selected the first partition of our 128GB SanDisk Cruzer Blade USB stick (which has two partitions) as the logical drive to image. Now, we must select a destination to save the logical drive disk image.



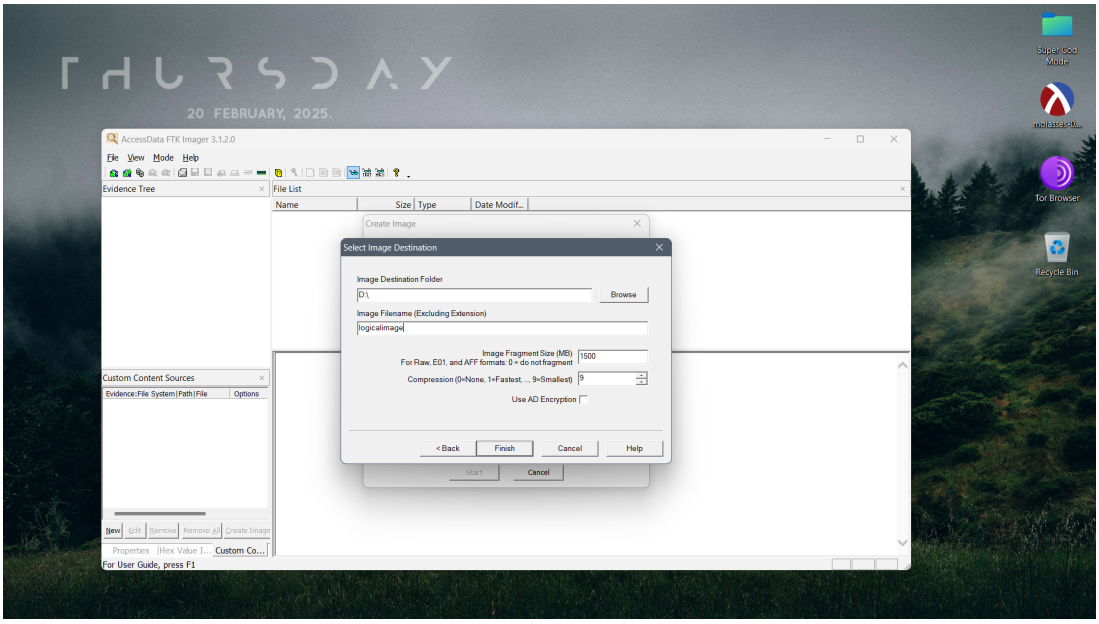
We choose the image type as *SMART*, because it enables compression, unlike *Raw (dd)*.



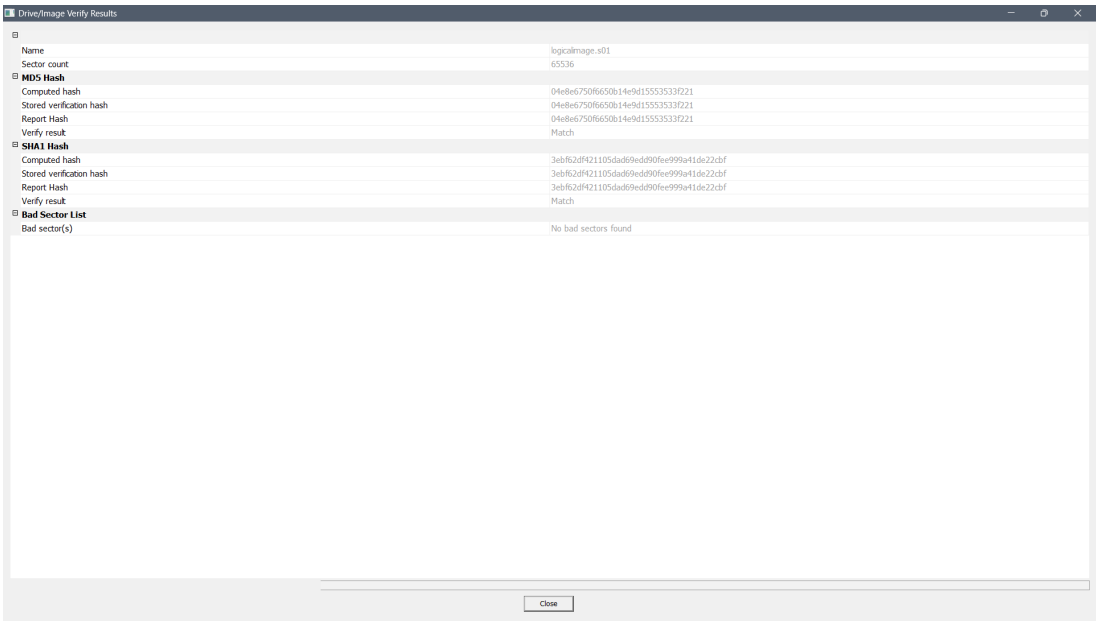
Next, we will enter the evidence item information.



We proceed with the default value for image fragment size (1500 MB) and choose compression mode 9 with the smallest image size. We leave the *Use AD encryption* option unchecked, enter our desired image name (*physicalimage*) and click **Finish**.



The process begins upon clicking **Start**, and finishes within seconds, before any screenshot can be taken. The process is fast because the logical partition in question is the EFI partition of a bootable USB drive, and is only a few megabytes in size. Upon completion of the process, the directory listing is dumped into a CSV file, the image is verified and a report is generated.



3.2 Report

Report generated by AccessData FTK Imager

```
Created By AccessData® FTK® Imager 3.1.2.0

Case Information:
Acquired using: ADI3.1.2.0
Case Number: 0001
Evidence Number: 0002
Unique description: Logical Drive
Examiner: Sarthak Das
Notes:

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

Information for D:\logicalimage:

Physical Evidentiary Item Source Information:
[Device Info]
 Source Type: Logical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 65,536
[Physical Drive Information]
 Removable drive: True
 Source data size: 32 MB
 Sector count:    65536
[Computed Hashes]
 MD5 checksum:    04e8e6750f6650b14e9d15553533f221
 SHA1 checksum:   3ebf62df421105dad69edd90fee999a41de22cbf

Image Information:
 Acquisition started:   Thu Feb 20 16:32:01 2025
 Acquisition finished:  Thu Feb 20 16:32:08 2025
 Segment list:
  D:\logicalimage.s01

Image Verification Results:
 Verification started:  Thu Feb 20 16:32:08 2025
 Verification finished: Thu Feb 20 16:32:09 2025
 MD5 checksum:    04e8e6750f6650b14e9d15553533f221 : verified
 SHA1 checksum:   3ebf62df421105dad69edd90fee999a41de22cbf : verified
```