VISHVESHWARAIAH TECHNOLOGICAL UNIVERSITY

"Jnana Sangama", Belagavi-590 018, Karnataka

BANGALORE INSTITUTE OF TECHNOLOGY

K.R. Road, V.V. Puram, Bengaluru-560 00

Department of Computer Science & Engineering

EBTS WORKSHOP

CYBER SECURITY INTERNSHIP

PROJECT

Topic: File Backup with FTK Imager

Team name: **SHADOW**

Name: ATHISH RAJ MOHAN

USN: 1BI20CS037

Semester: 5

Phone number: 9916115225

Email ID:athishrajmohan21@gmail.com

Project Domain	Period Covered	Completion Date
FTK Imager	11th to 14th January, 2023	14th January, 2023

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompanies the successful completion of any task would be incomplete without complementing those who made it possible and whose guidance and encouragement made my efforts successful. So, my sincere thanks to all those who have supported me in completing this Internship successfully.

My sincere thanks to Dr. M. U. Aswath, Principal, BIT and Dr. Girija. J, HOD, Department of CS&E, BIT for their encouragement, support and guidance to the student community in all fields of education.

I would like to extend my heartfelt gratitude to Mr. Kalmesh Joshi, Mr. Vaishnavu C V and his team for carrying out this workshop and enriching our knowledge in the field of Cyber security.

CONTENTS

1. INTRODUCTION

1.1 What is FTK Imager?

FTK Imager in full stands for Forensic Toolkit Imager. This is a windows commercial forensic imaging software used by law enforcement around the world. We will just be extracting volatile memory from the PC so no need to worry about getting a license first. We will be running FTK Imager from an external drive as it is recommended to avoid interfering with the evidence.

FTK Imager is a tool for creating disk images and is absolutely free to use. It was developed by The Access Data Group. It is a tool that helps to preview data and for imaging.

With FTK Imager, you can:

- Create forensic images or perfect copies of local hard drives, floppy and Zip disks, DVDs, folders, individual files, etc. without making changes to the original evidence.
- Preview files and folders on local hard drives, network drives, floppy diskettes, Zip disks, CDs, and DVDs.
- You can also preview the contents of the forensic images that might be stored on a local machine or drive.
- You can also mount an image for a read-only view that will also allow you to view the contents of the forensic image exactly as the user saw it on the original drive.
- Export files and folders from forensic images.
- View and recover files that have been deleted from the Recycle Bin, but have not yet been overwritten on the drive.

1.2 Approach:-

To create a forensic image with FTK imager, we will need the following:

1. FTK Imager from Access Data, which can be downloaded using the following link: FTK Imager from Access Data
2. A Hard Drive that you would like to create an image of.

1.3 Overview:-

A Forensic Image is most often needed to verify the integrity of the image after an acquisition of a Hard Drive has occurred. This is usually performed by law enforcement for court because, after a forensic image has been created, its integrity can be checked to verify that it has not been tampered with. Forensic Imaging is defined as the processes and tools used in copying an electronic media such as a hard-disk drive for conducting investigations and gathering evidence that will be presentable in the law of court. This copy not only includes files that are visible to the operating system but every bit of data, every sector, partition, files, folders, master boot records, deleted files, and unallocated spaces. The image is an identical copy of all the drive structures and contents.

Further, a forensic image can be backed up and/or tested on without damaging the original copy or evidence.

Also, you can create a forensic image from a running or dead machine. It is a literal snapshot in time that has integrity checking.

2. **Theory and Methodology:-**

2.1 Need for a Forensic Image:-

1. In today's world of crime, many cases have been solved by using this technique, as evidence apart from what is available through an operating system, has been found using this technique, as incriminating data might have deleted to prevent discovery during the investigation. Unless that data is overwritten and deleted securely, it can be recovered.
2. One of the advantages includes the prevention of the loss of critical files.
3. When you suspect a custodian of deleting or altering files. A complete forensic image will, to a certain extent, allow you to recover deleted files. It can also potentially be used to identify files that have been renamed or hidden.
4. When you expect that the scope of your investigation could increase at a later date. If you aren't sure about the scope of your project, always over collect. It's better to have too much data than not enough, and you can't get much more data than a forensic image.
5. When you expect that you or someone in your organization may need to certify or testify to the forensic soundness of the collection. In most cases, this need will never arise, but will almost certainly come into play in any criminal or potential criminal proceedings.
6. The Imaging of random access memory (RAM) can be enabled by using live imaging. Live imaging can bypass most encryption.

2.2 Pros and Cons:-

Pros of FTK Imager:-

1. It has a simple user interface and advanced searching capabilities.
2. FTK supports EFS decryption.
3. It produces a case log file.
4. It has significant bookmarking and salient reporting features.
5. FTK Imager is free.

Cons of FTK Imager:-

1. FTK does not support scripting features.
2. It does not have multitasking capabilities.
3. There is no progress bar to estimate the time remaining.

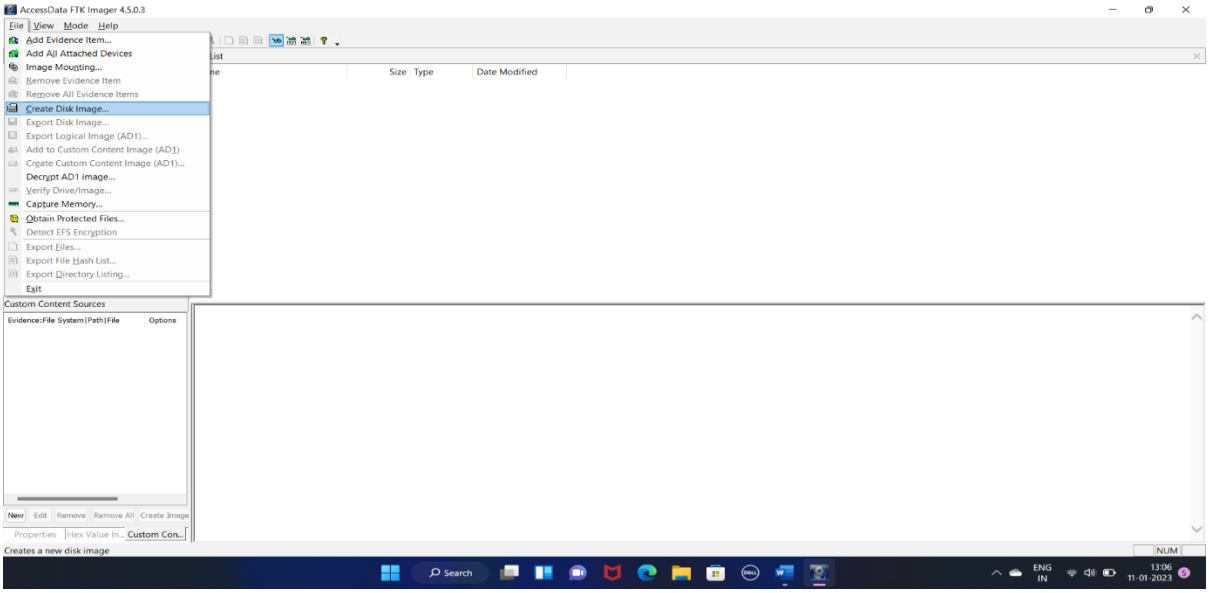
3. **Procedure:-**

Assuming that file **“Regulations relating to Import and Export from India”** is deleted from the **“SanDisk Cruzer Blade USB Device [15 GB USB]’’** we shall try to retrieve the file using FTK Imager.

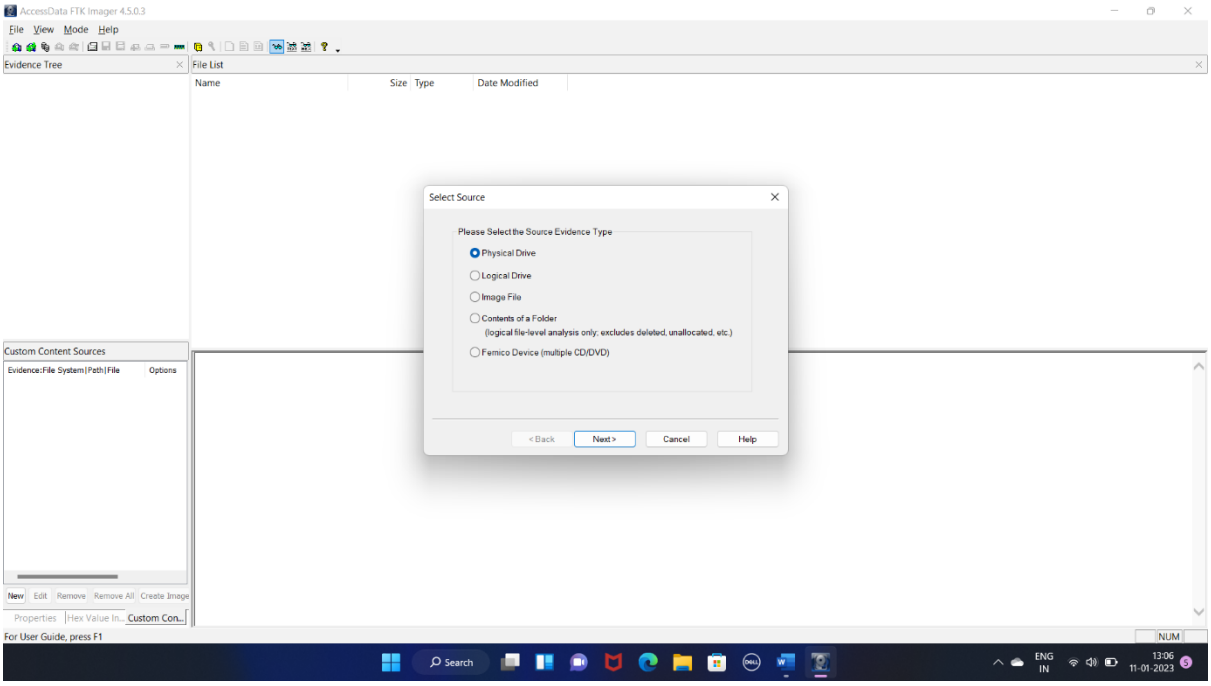
Step-1:- Download and install the FTK imager on your machine.

Step-2:- Click and open the FTK Imager, once it is installed. You should be greeted with the FTK Imager dashboard.

Step-3:- In the menu navigation bar, you need to click on the File tab which will give you a drop-down, like given in the image below, just click on the create disk image.

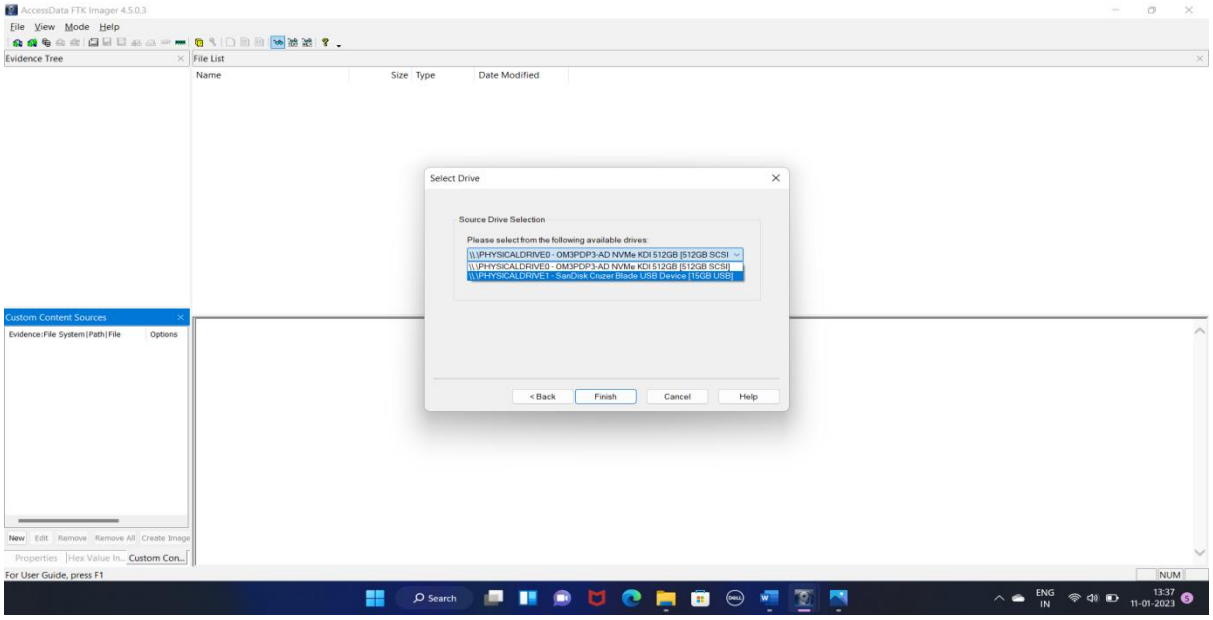


Step-4:- After that, there will be a pop-up window that will ask you to ‘Select Source’ of the Evidence.



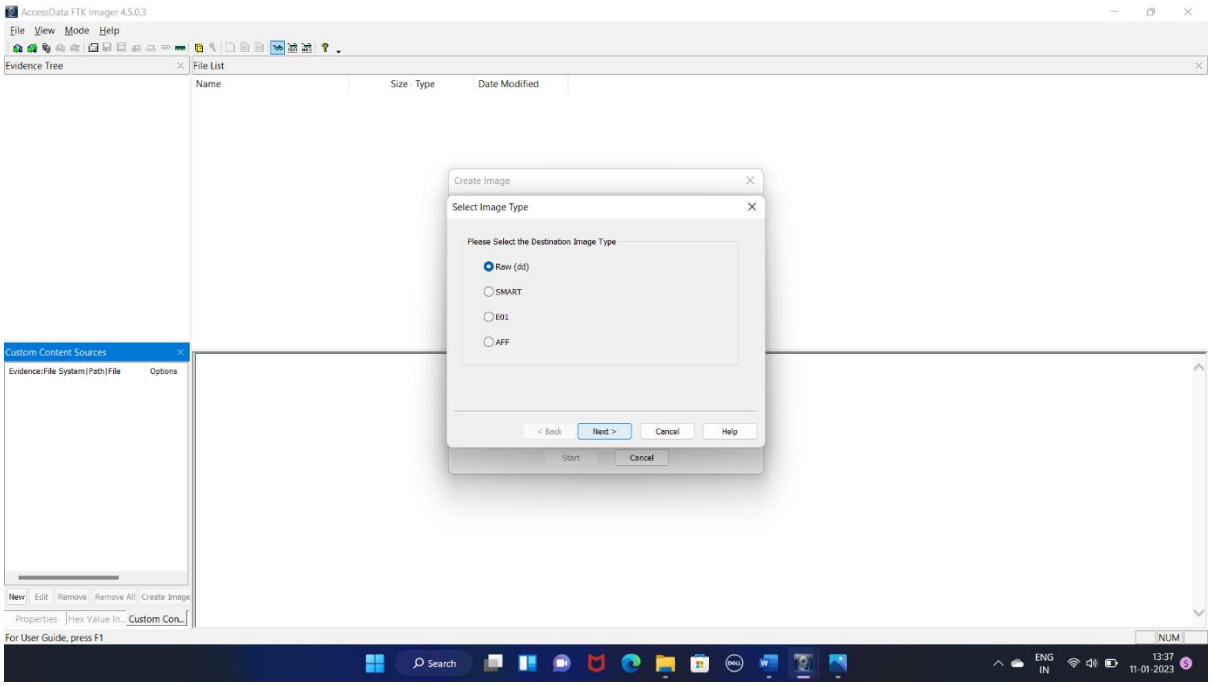
Step-5:- If you have connected a physical hard drive to the laptop/computer you are using to make the forensic image, then you will select the Physical Drive here. Click on Next.

Step-6:- Now, Select the Physical Drive that you would like to use. Please make sure that you are selecting the right drive, or you will waste your time exporting a forensic image of your own OS drive.

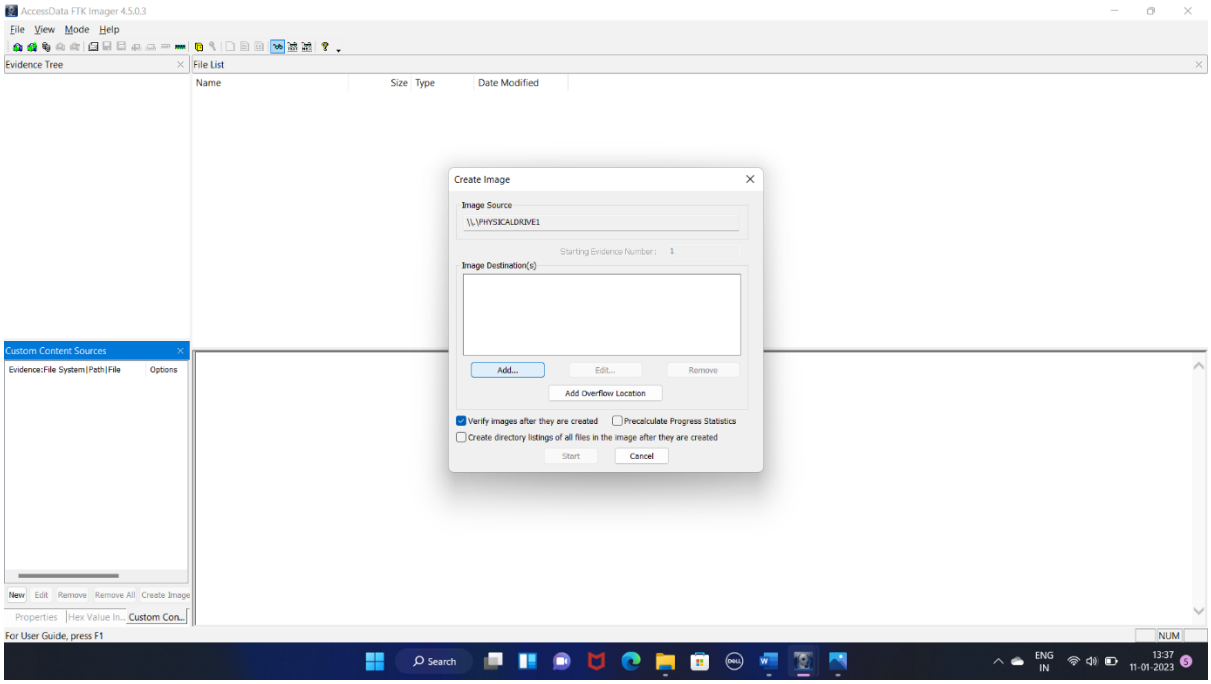


Step-7:- Now, we will export the forensic images.

- Right-click on the Physical Drive that you would like to export in the FTK Imager window. Select Export Disk Image here.

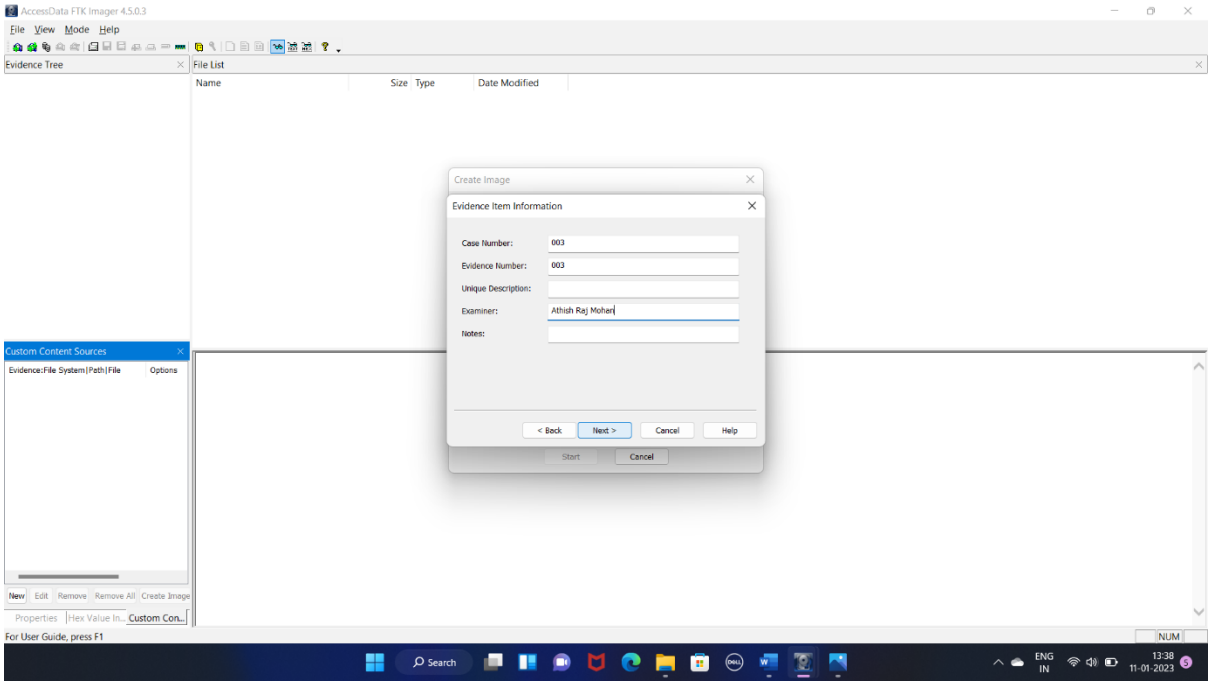


- Click the Add button for the Image Destination.



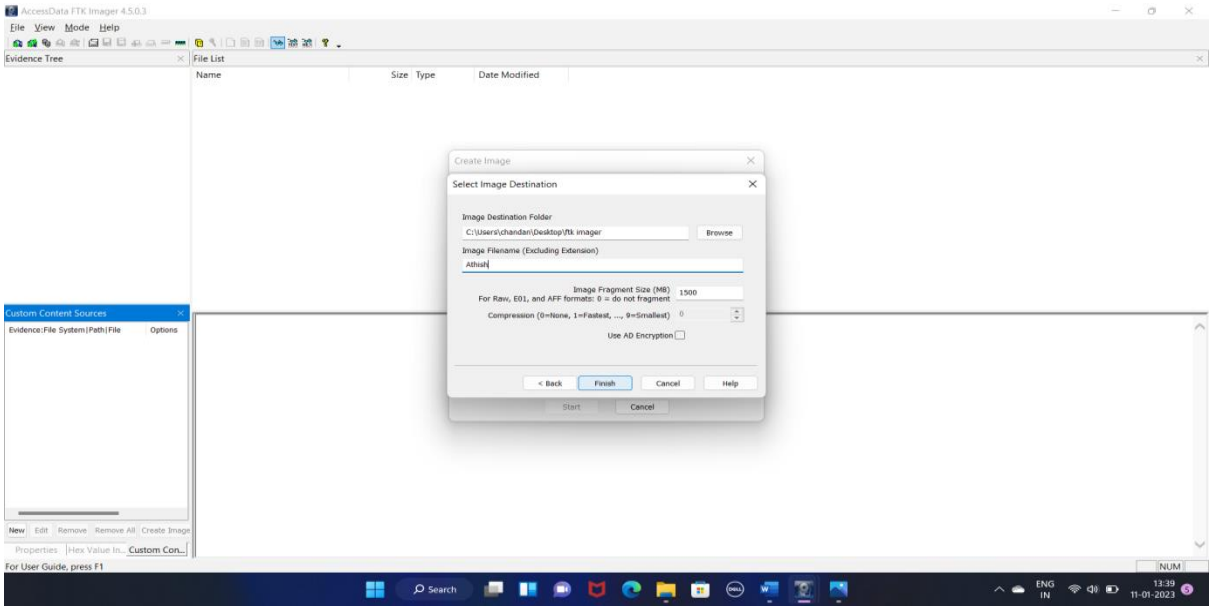
Step-8:- Select the Type of Forensic Image you would like to export. Select E01 and Click Next.

- After that, you will have to enter information regarding the case now. You can either leave them blank or keep it general, this part is totally upon you.

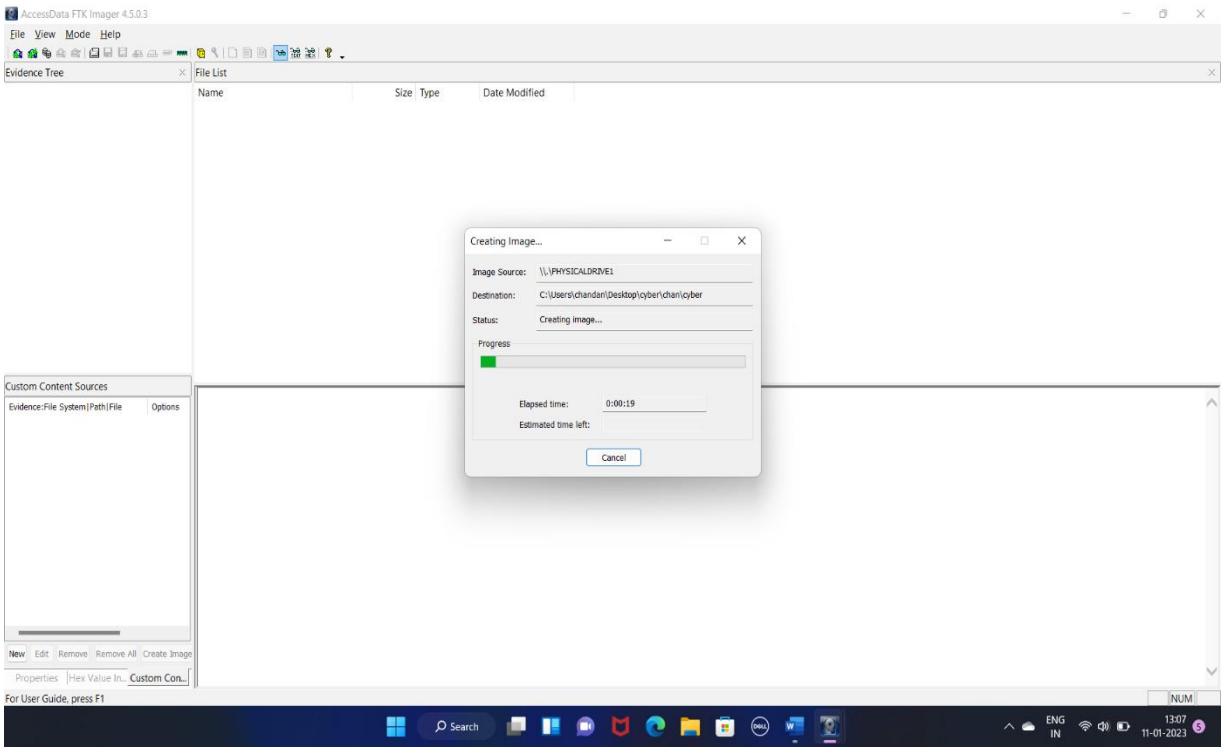


- Next, you will need to choose the Destination that you would like to export the forensic image and name the Image.

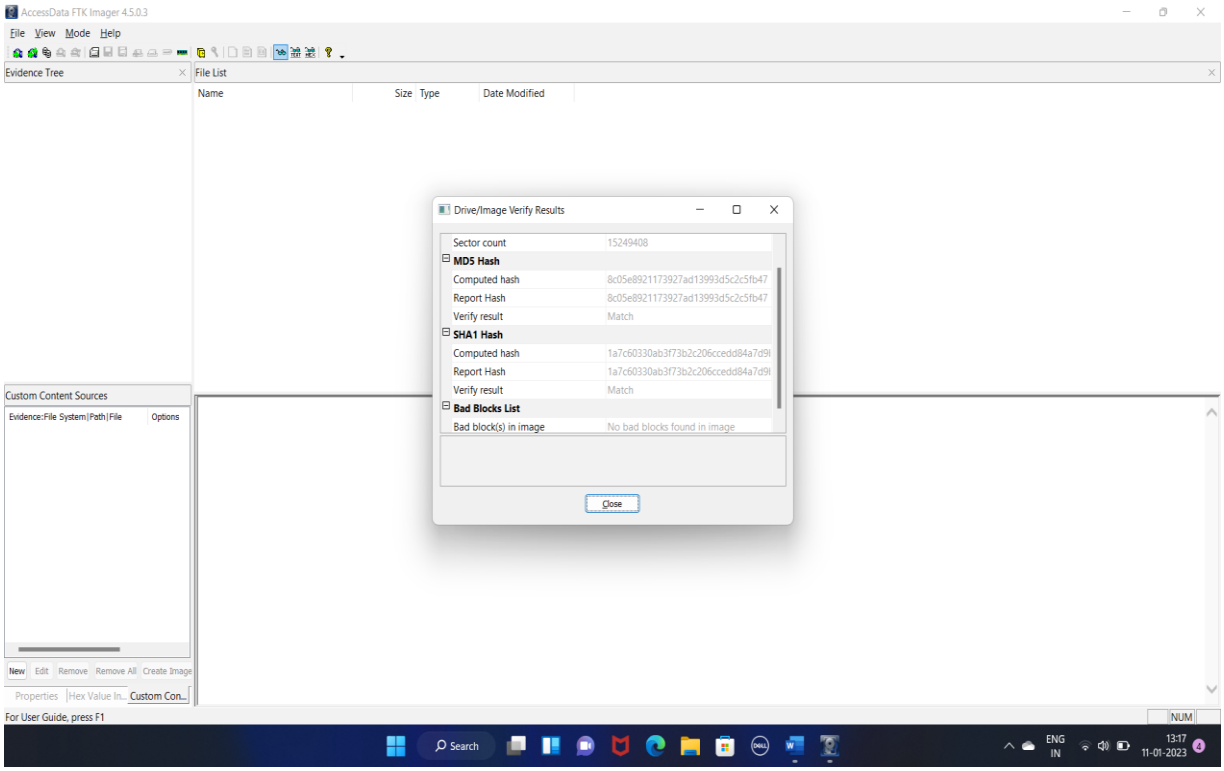
Step-9:- After naming the image click on finish.



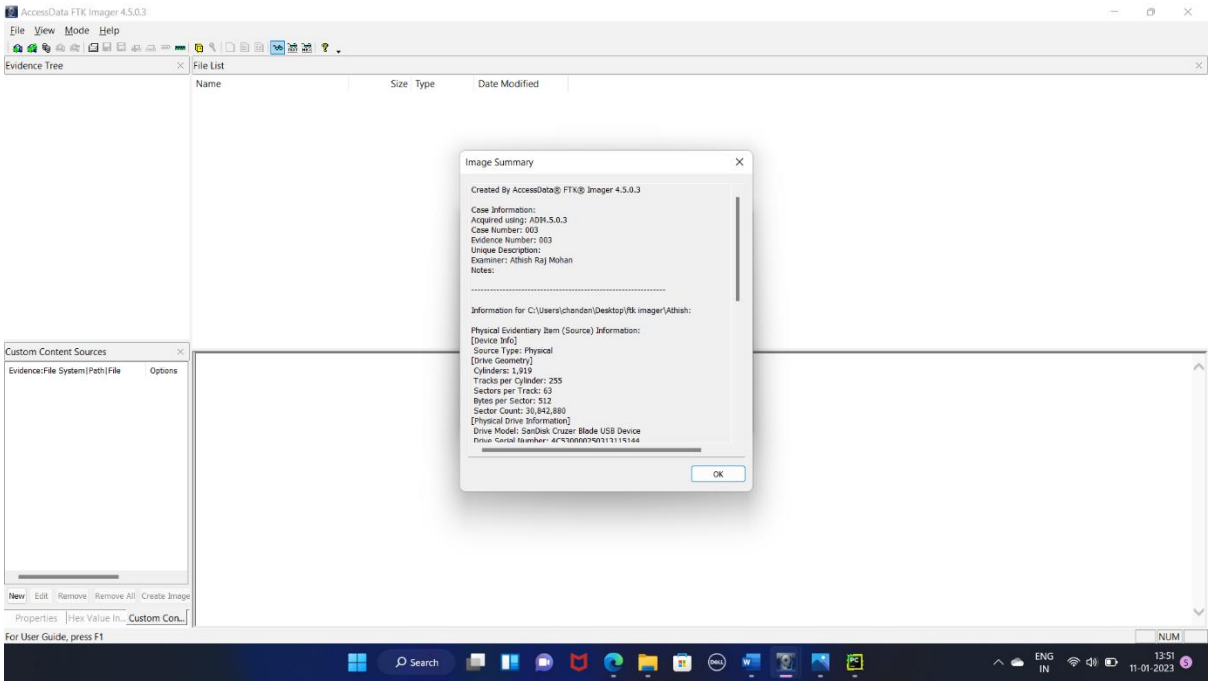
Step-10:- Now image starts creating.



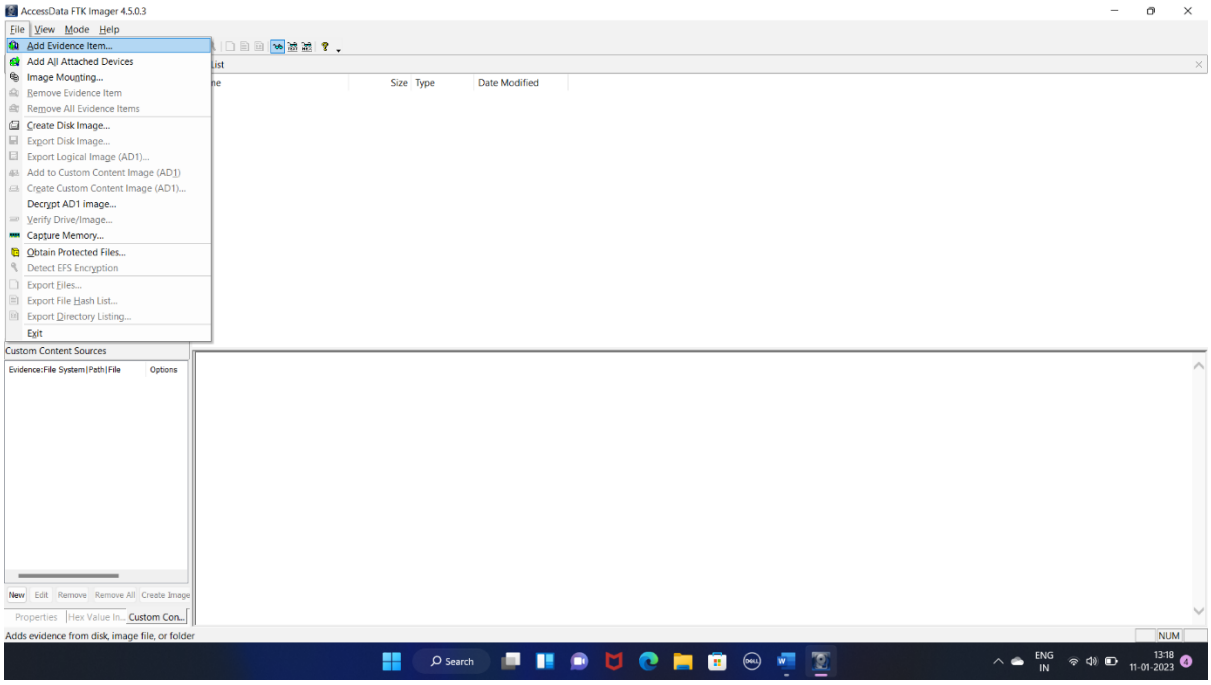
Step-11:- Now after image has been verified it shows the results.



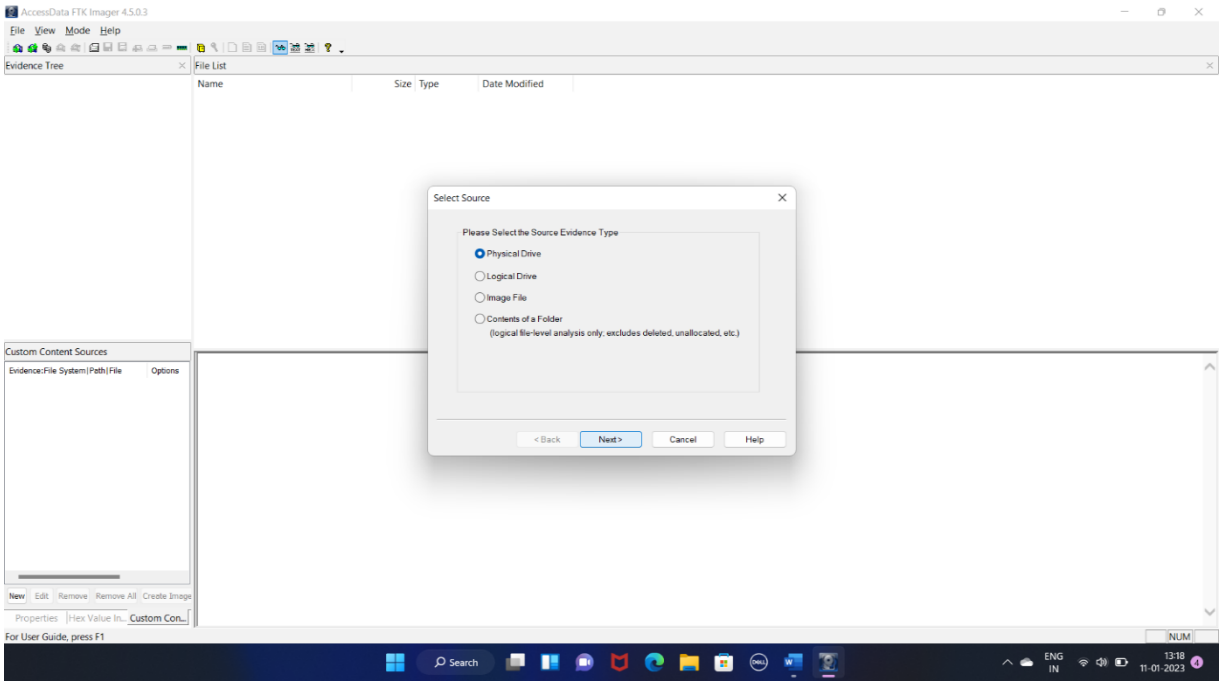
Step-12:- Now we can view the summary by clicking on image summary.



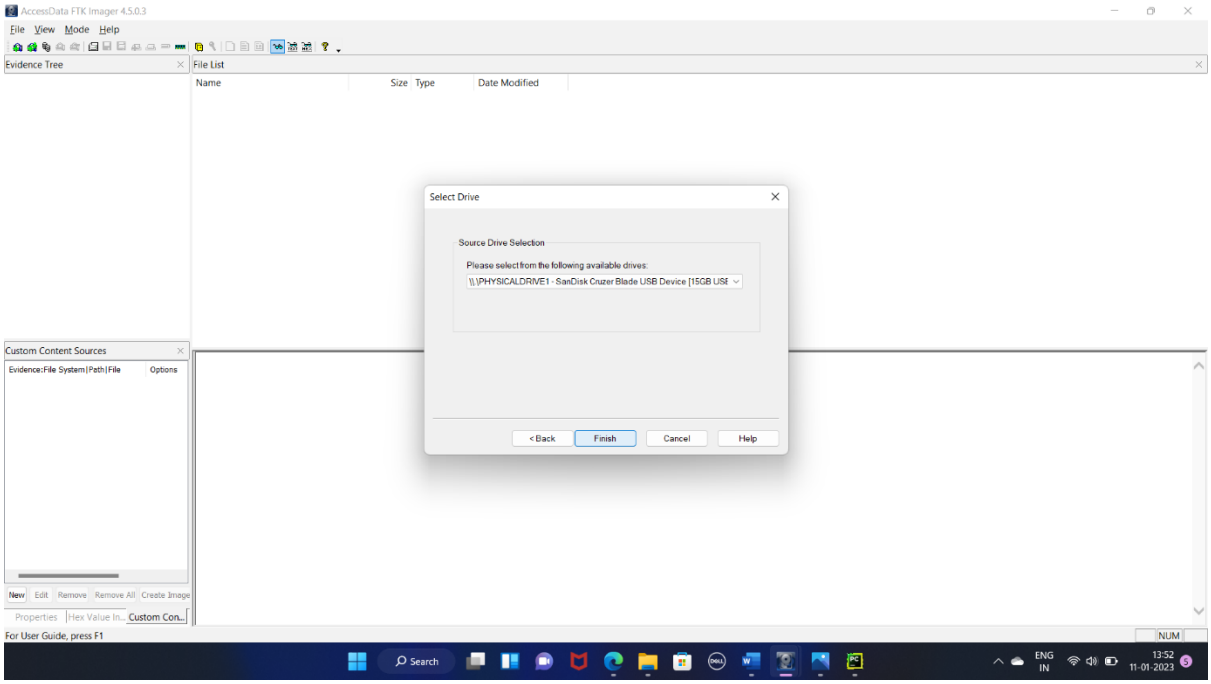
Step -13:- In the menu navigation bar, you need to click on the *File* tab which will give you a drop-down, like given in the image below, just click on the Add evidence item.



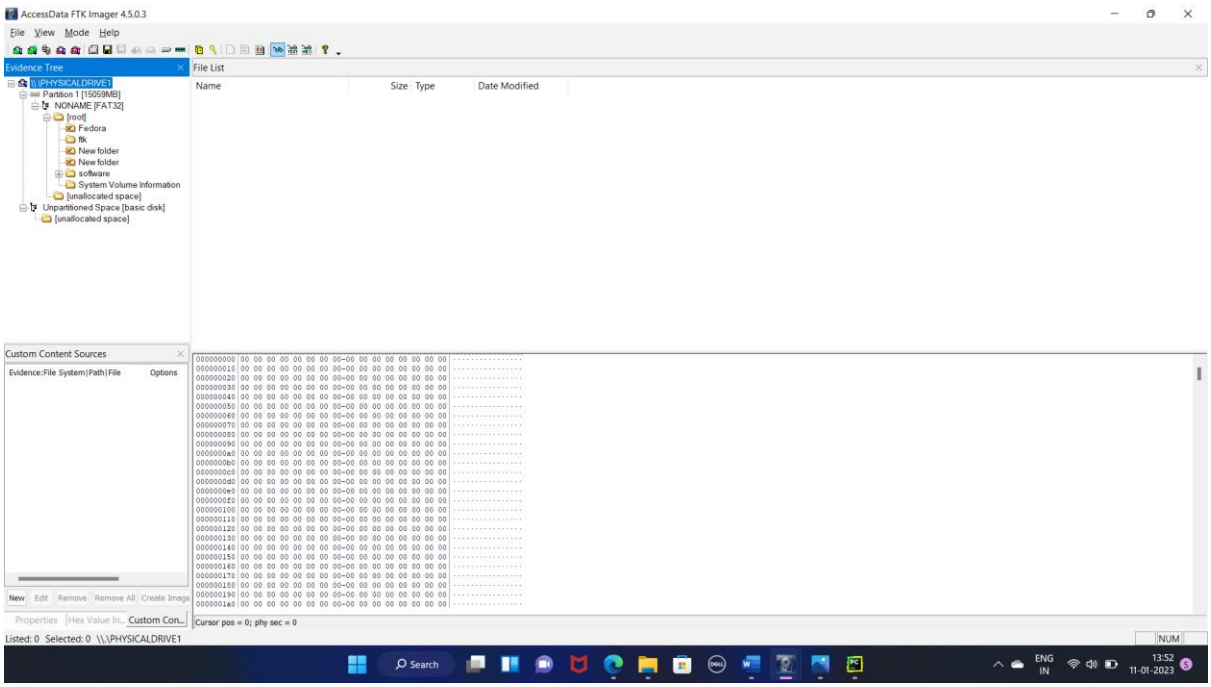
Step-14:- Now select the source evidence type either physical drive, logical drive , image file.



Step-15:- Now once again select the source drive ,and click finish.

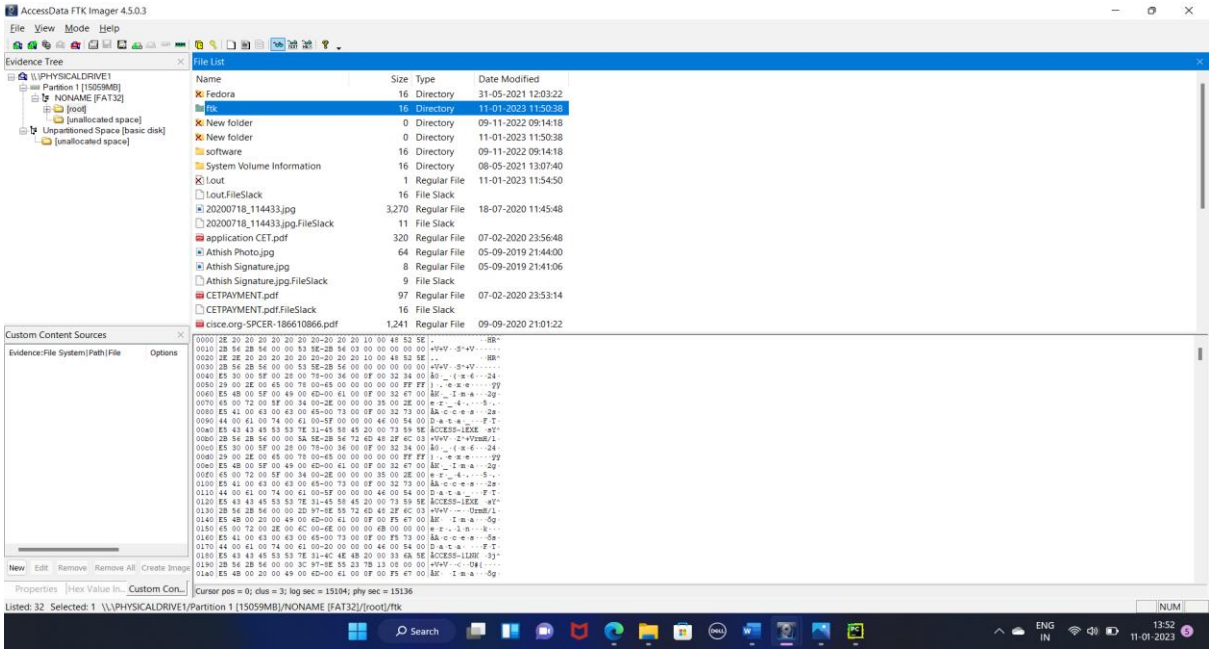


Step-16:- Now its shows the Evidence tree of physical drive.

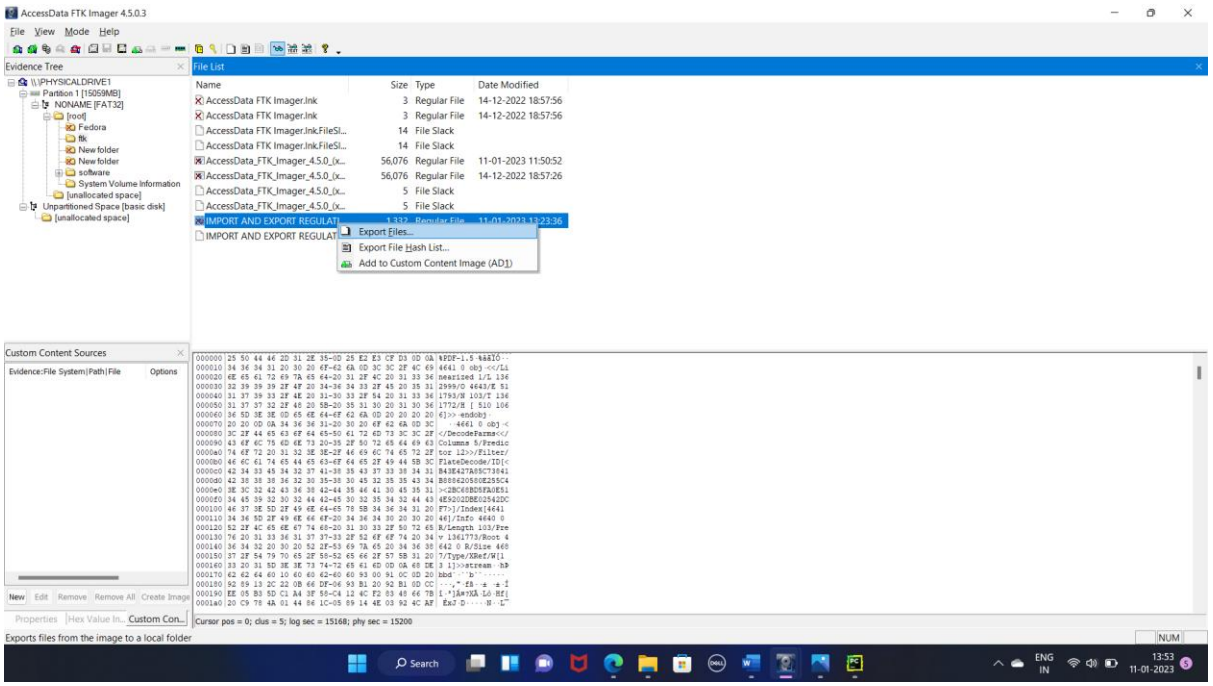


Step-17:- Now the files which have been deleted will be in red ‘X’ mark.

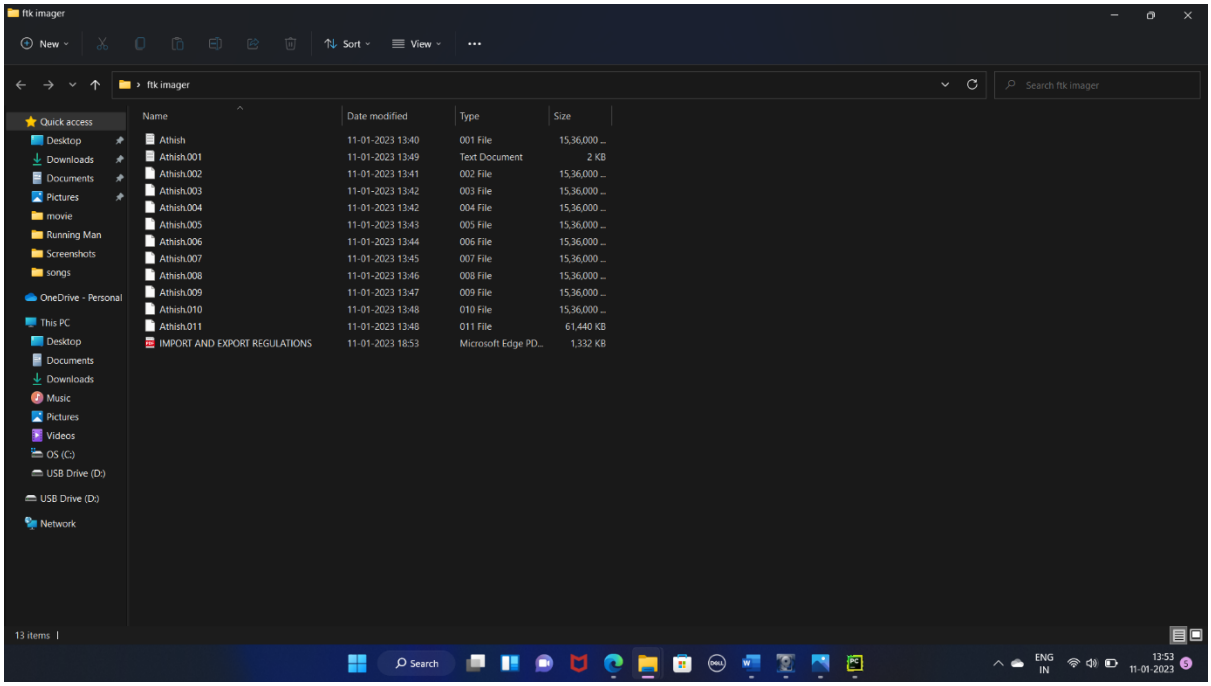
Now by right clicking on that we can export file to our destination.



Step-18:- Now by right clicking the file which we want to export, we can select the destination folder and export the file.

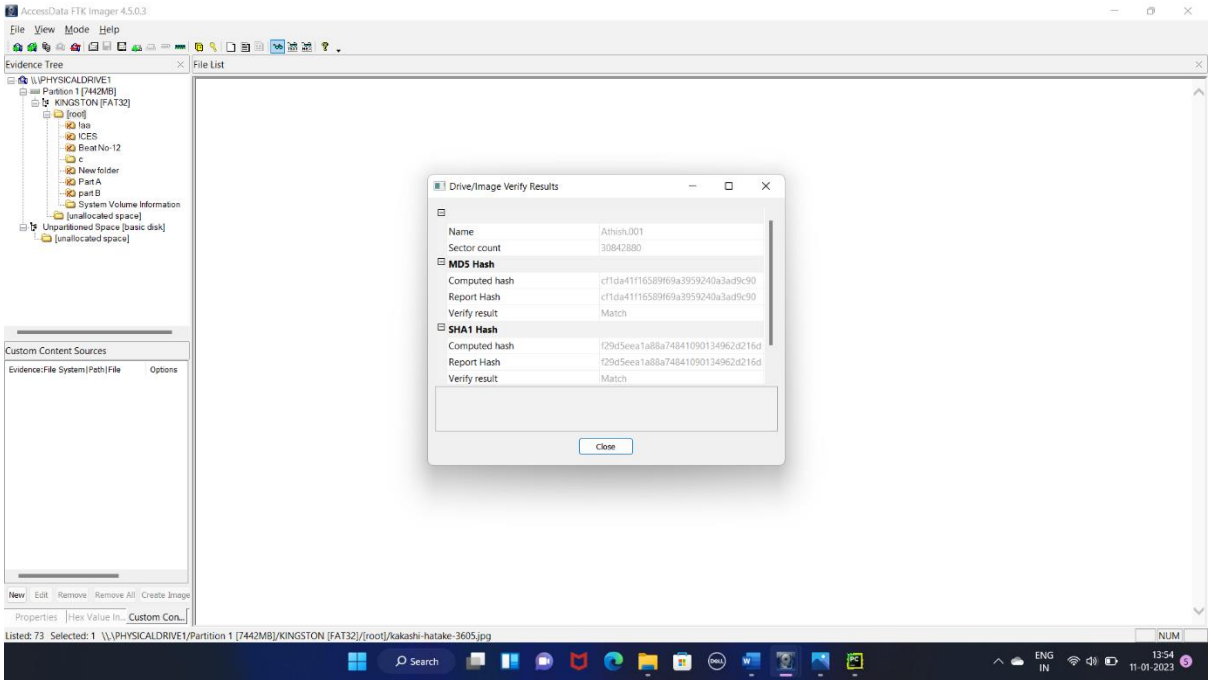


Step-19:- Now the file will be present in the destination folder ‘ftk Imager’.



Step-20:- Therefore the file can be read again.

Step-21:-Finally press close button to close the ftk imager.



Result:-

Lastly, you will need to wait for the Forensic Image to be created and then verified. The speed of creating the forensic image will vary based on your hardware. Once both have occurred, you have your forensic images ready.

So this is how a forensic report of volatile memory looks in a report, and how to extract data from volatile memory using FTK Imager.

Conclusion:-

In the above guide we were able to obtain forensic image and volatile memory image from PC using FTK Imager. Forensic images are vital sources of concrete evidence in cyber-crime cases. Steps explained above are also used by raw enforcement agencies while enforcing cyber laws. After learning and understanding this guide you can and will be able to extract and store digital forensic evidence in a professional way.