

PES UNIVERSITY

UE19CS336  
Digital Forensics

Name : Suhan B Revankar

SRN : PES2UG19CS412

Section : G Section

## Table of Contents :

### Activity 1

1. Creating and deletion of files.....	3
2. Acquiring a Forensic copy of the disc.....	4
3. Examining the details.....	9

### Activity 2

1. Loading of the encase (E01) image.....	15
2. Locating file .....	16
3. Generating of Report.....	16

### Activity 3

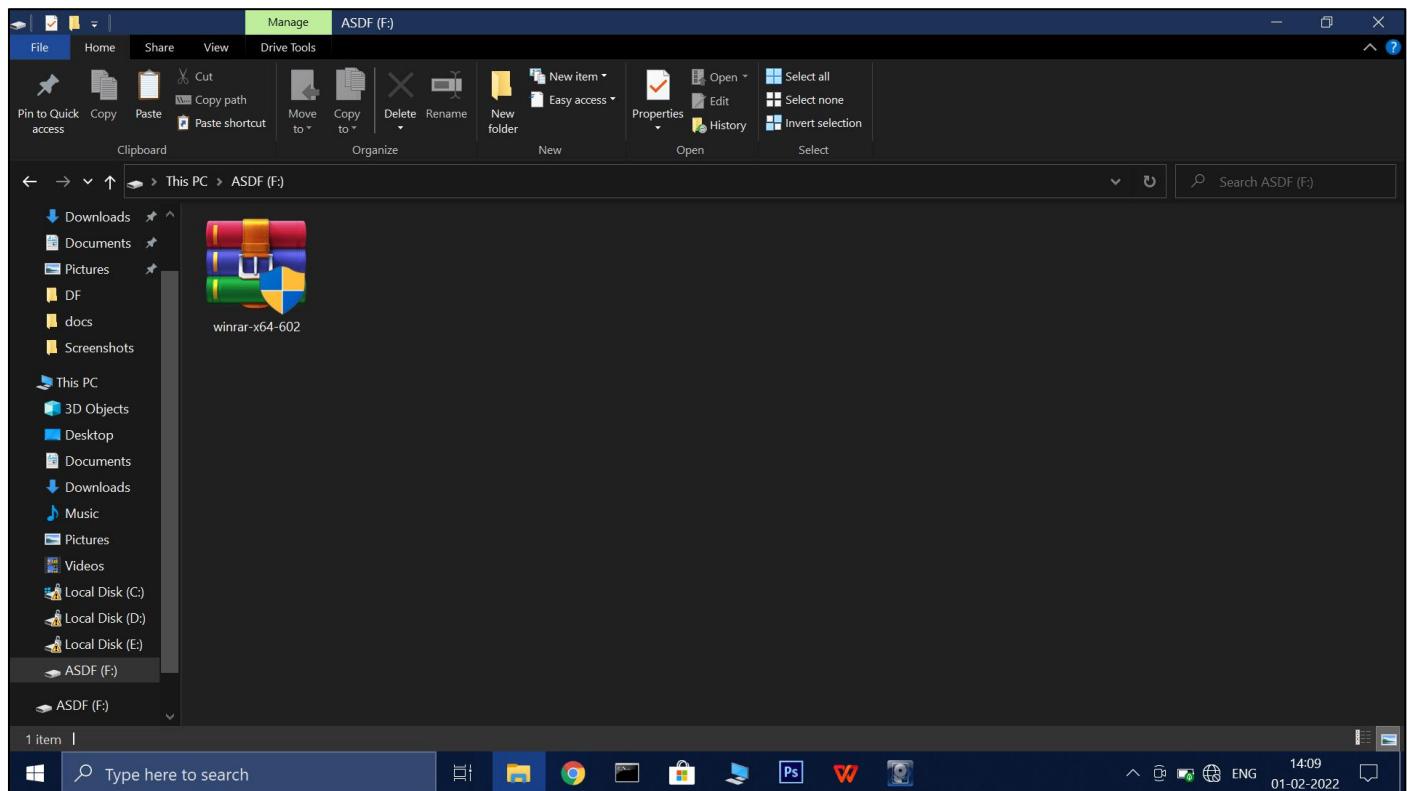
1. Regedit file.....	21
2. Modifying files .....	22
3. Enabling and disabling the writepolicy.....	25

# Activity 1

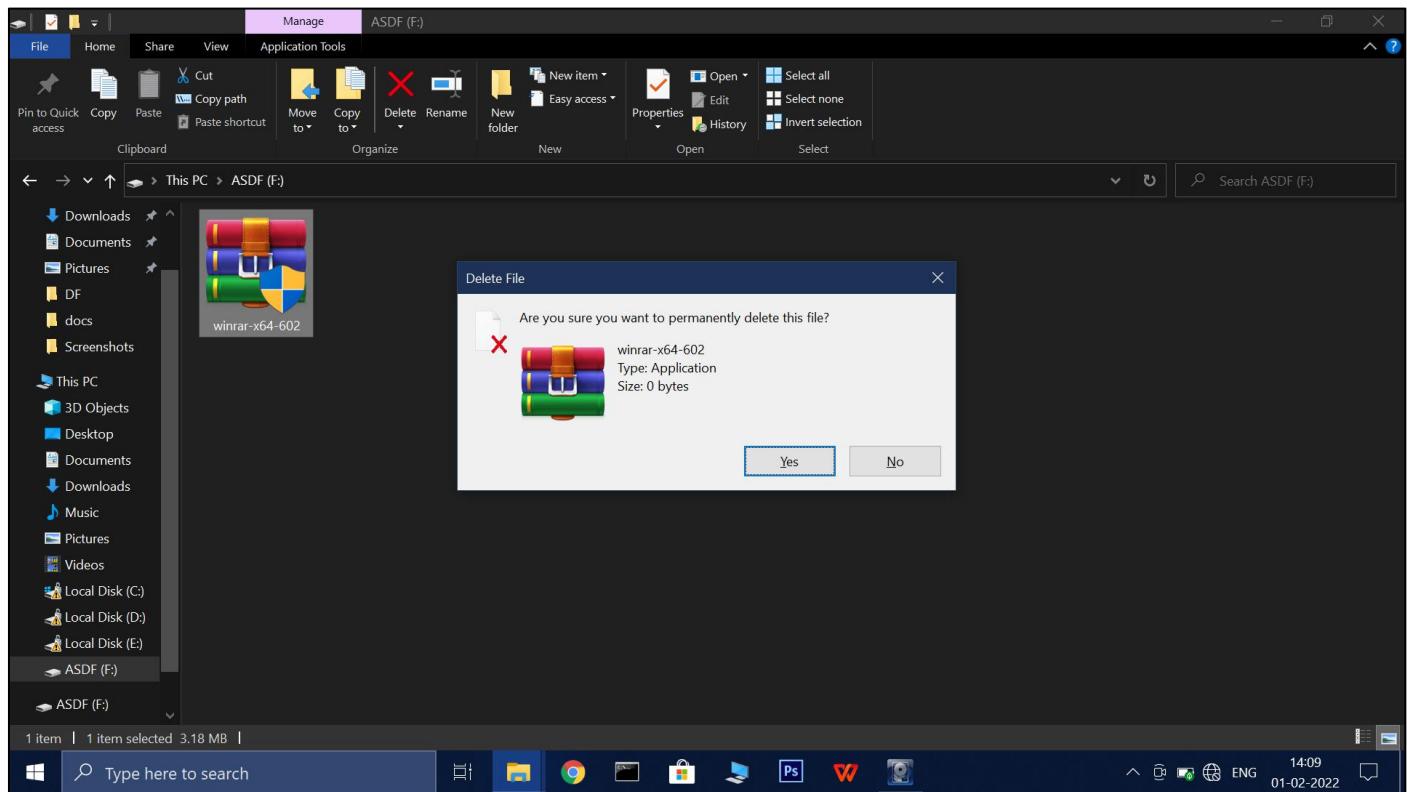
Using FTK Imager , to create a raw (.dd) or Encase (E01) image of the disk .

## Part 1: Creating & Deleting of files

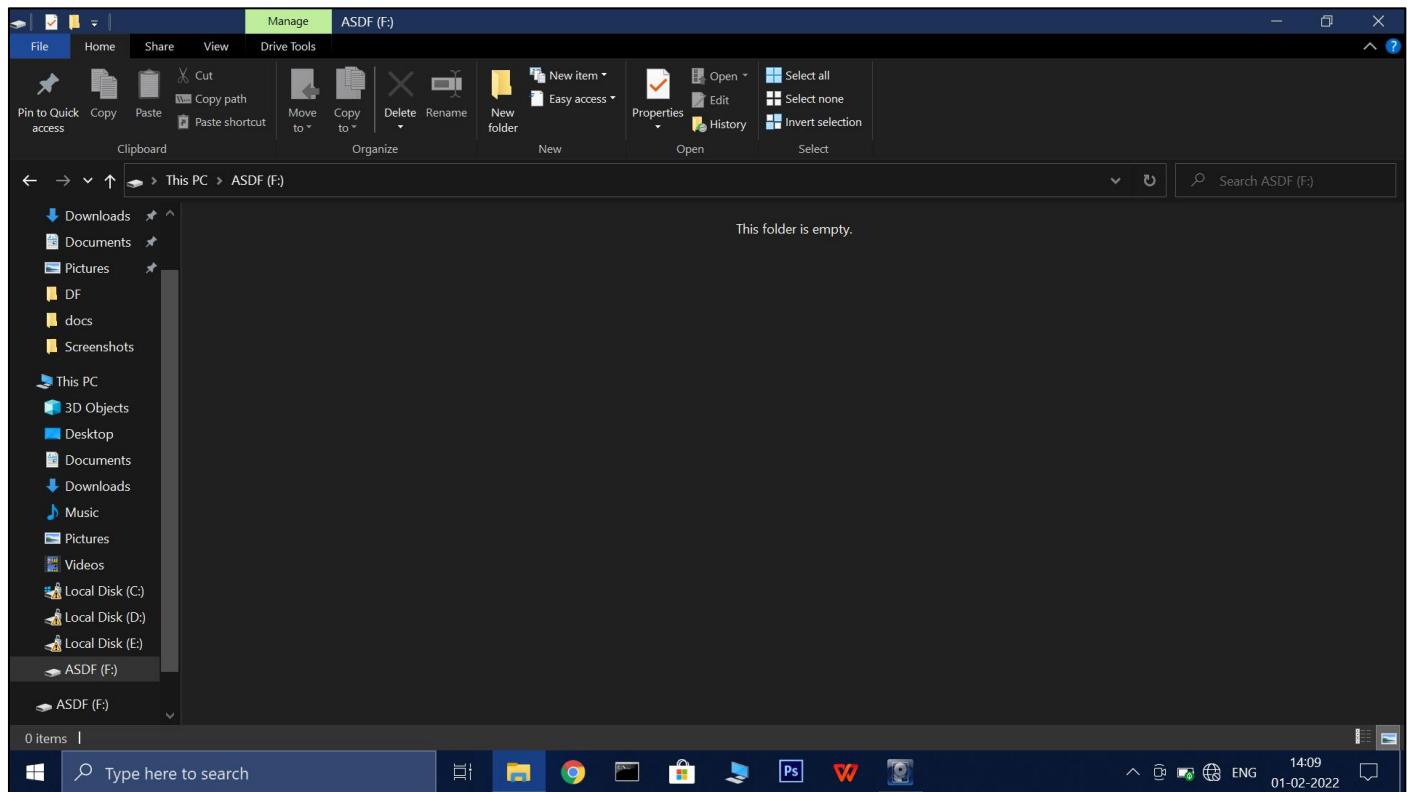
### 1. Ensure a file is placed in it .



### 2. Delete the file



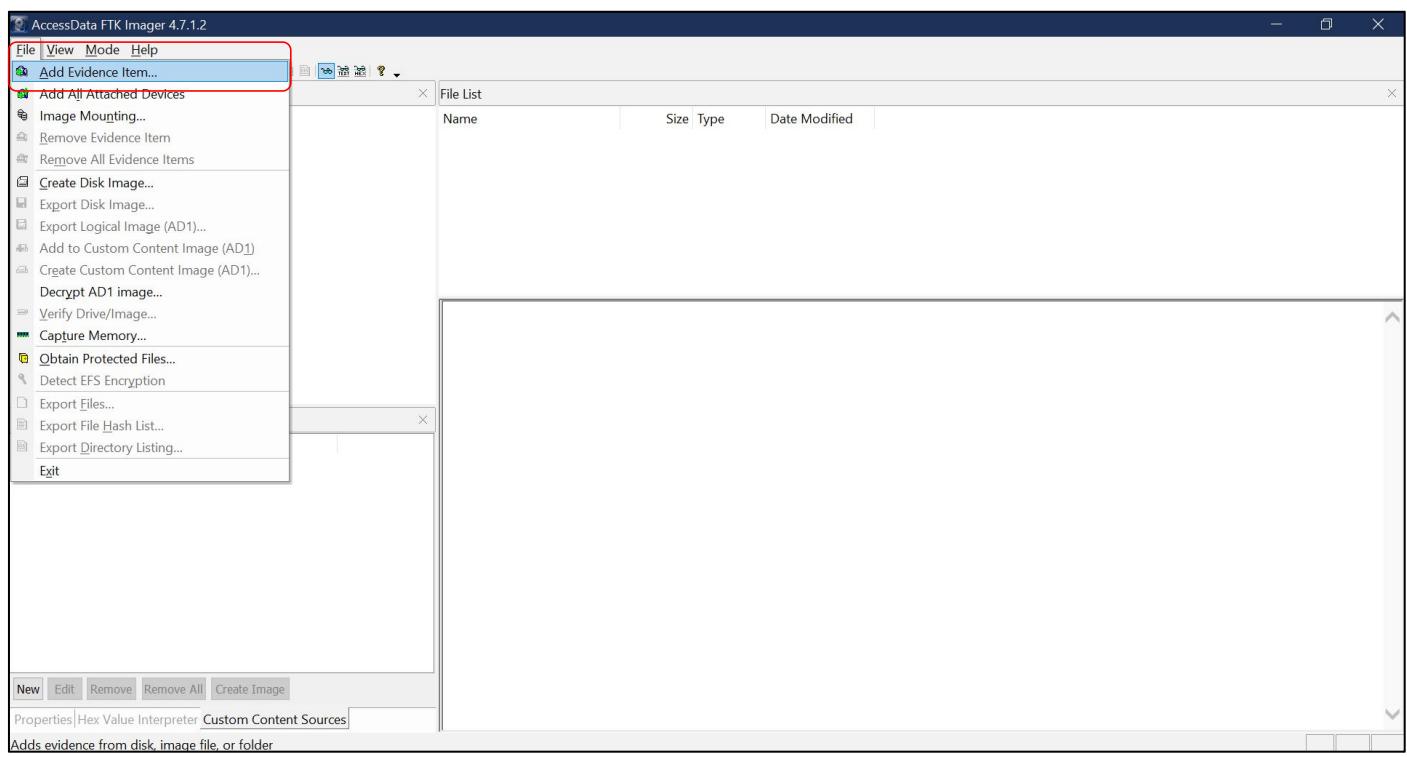
### 3. Ensure its deleted



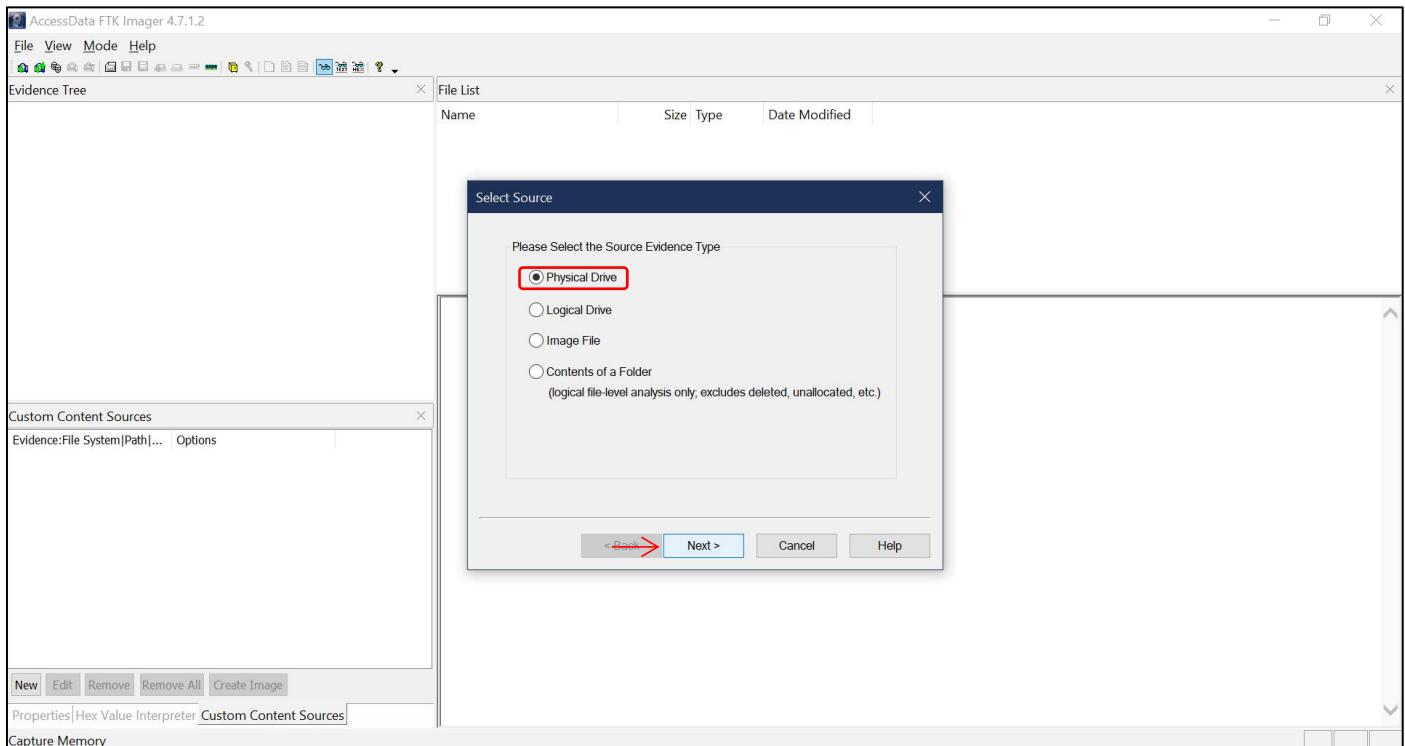
As we can see above that the file is deleted , now we are ready to proceed to next step .

## Part 2: Acquiring the Forensic image of the disk

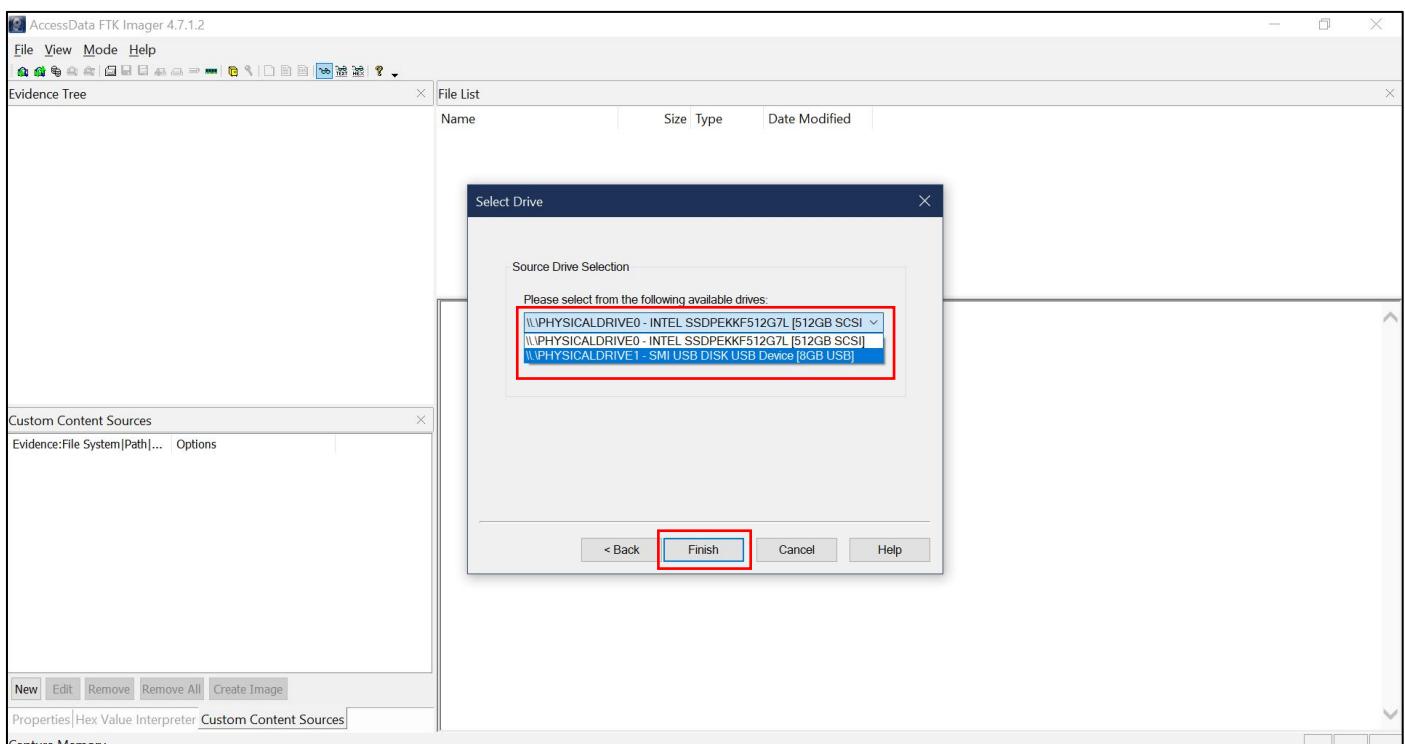
### 1. Open FTK Imager , then File -> Add Evidence Item



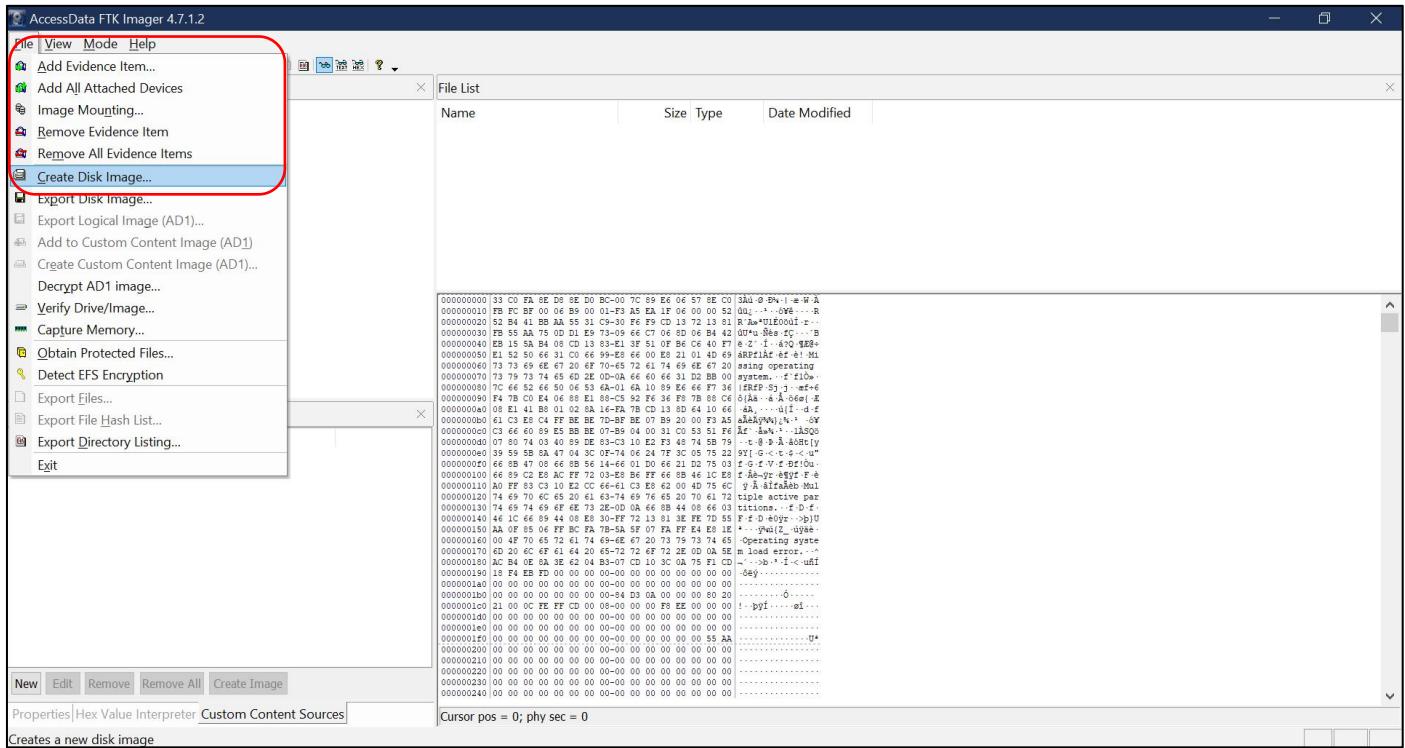
## 2. Select the type of drive (here its Physical Drive).



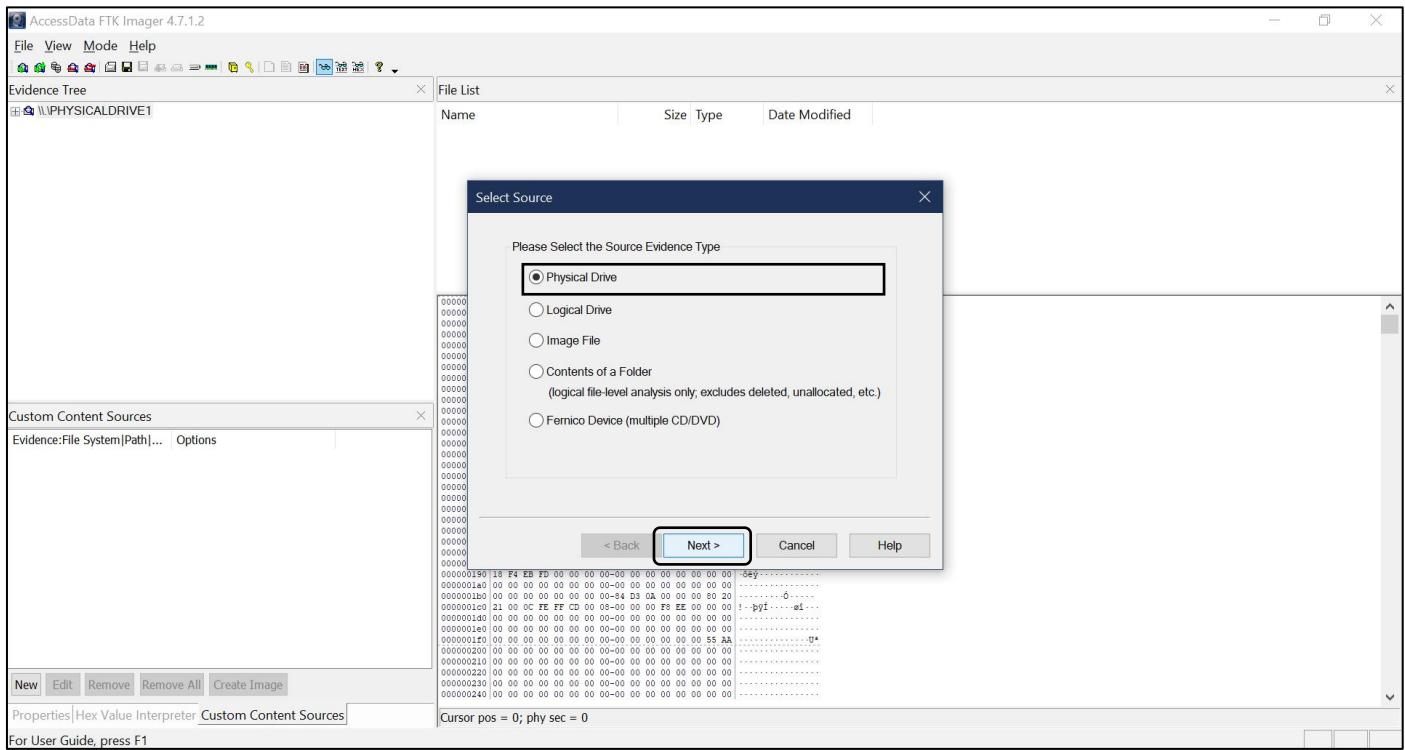
## 3. Select the drive from te drop down list



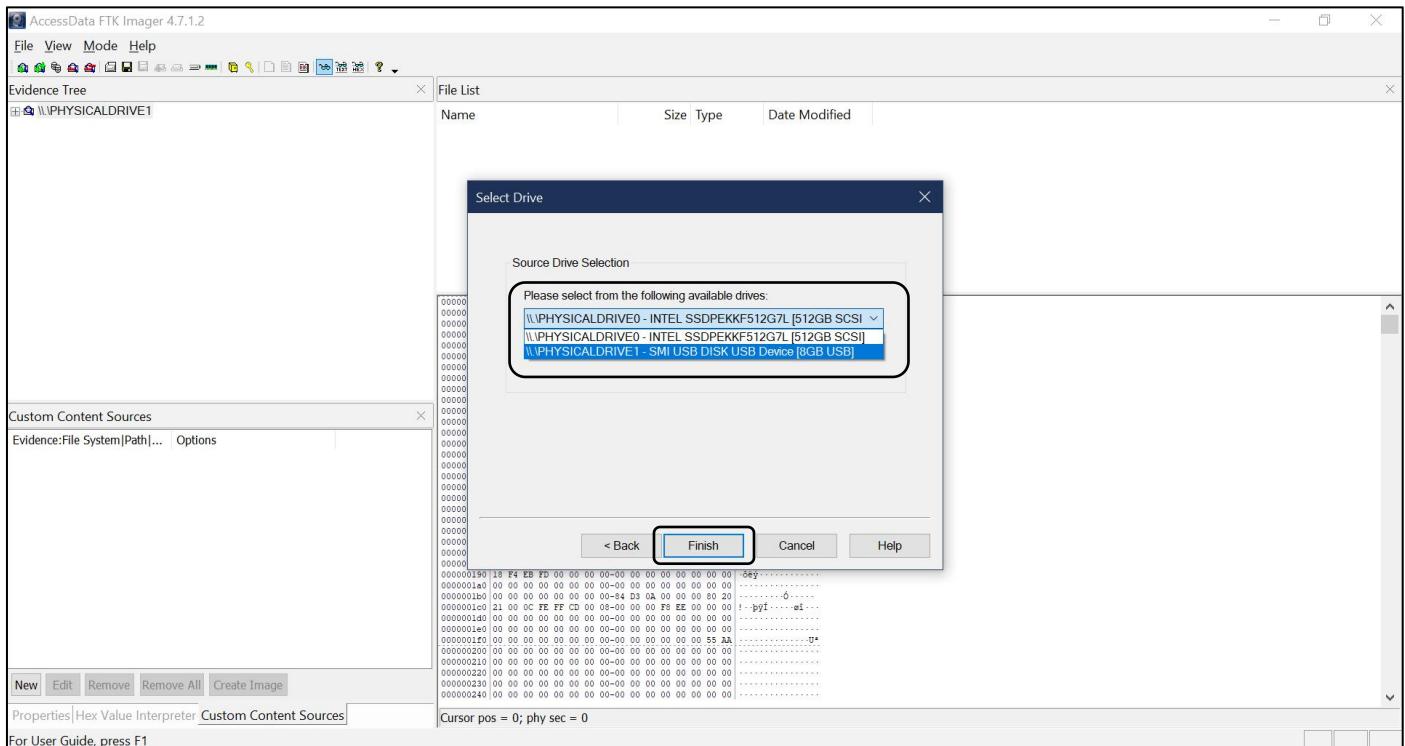
## 4. To create a disk Image Follow , File -> Disk Image .



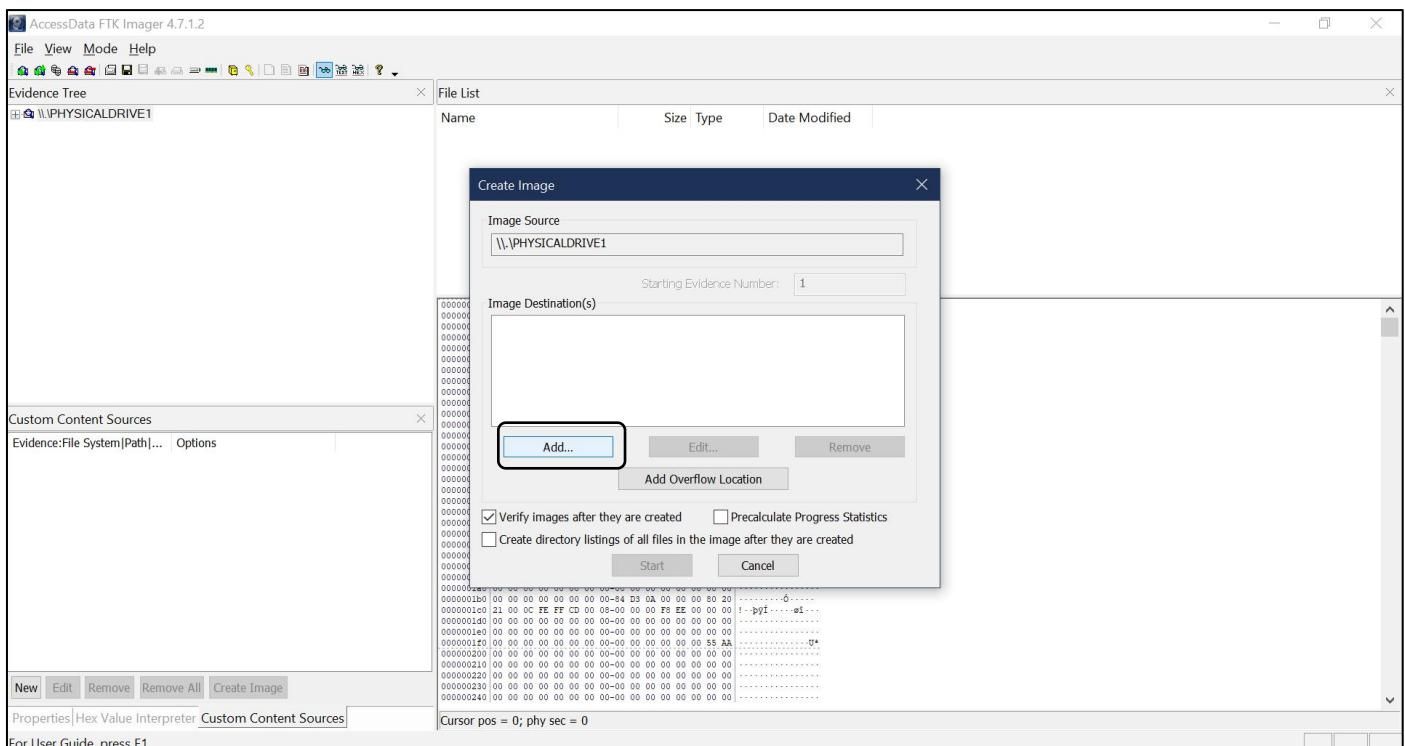
## 5 . Specify the disk type. (here Physical Drive)

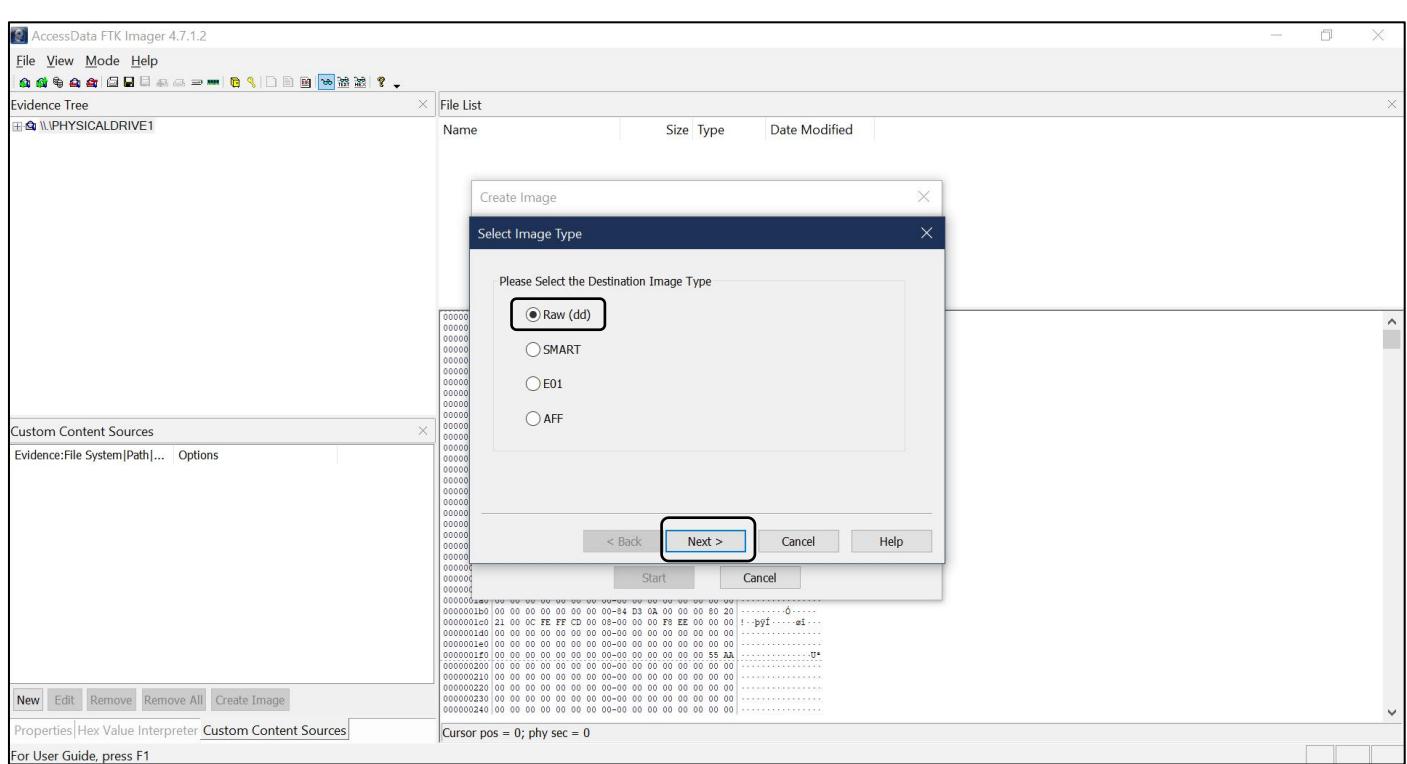


## 6 . Select the disk to be examined .

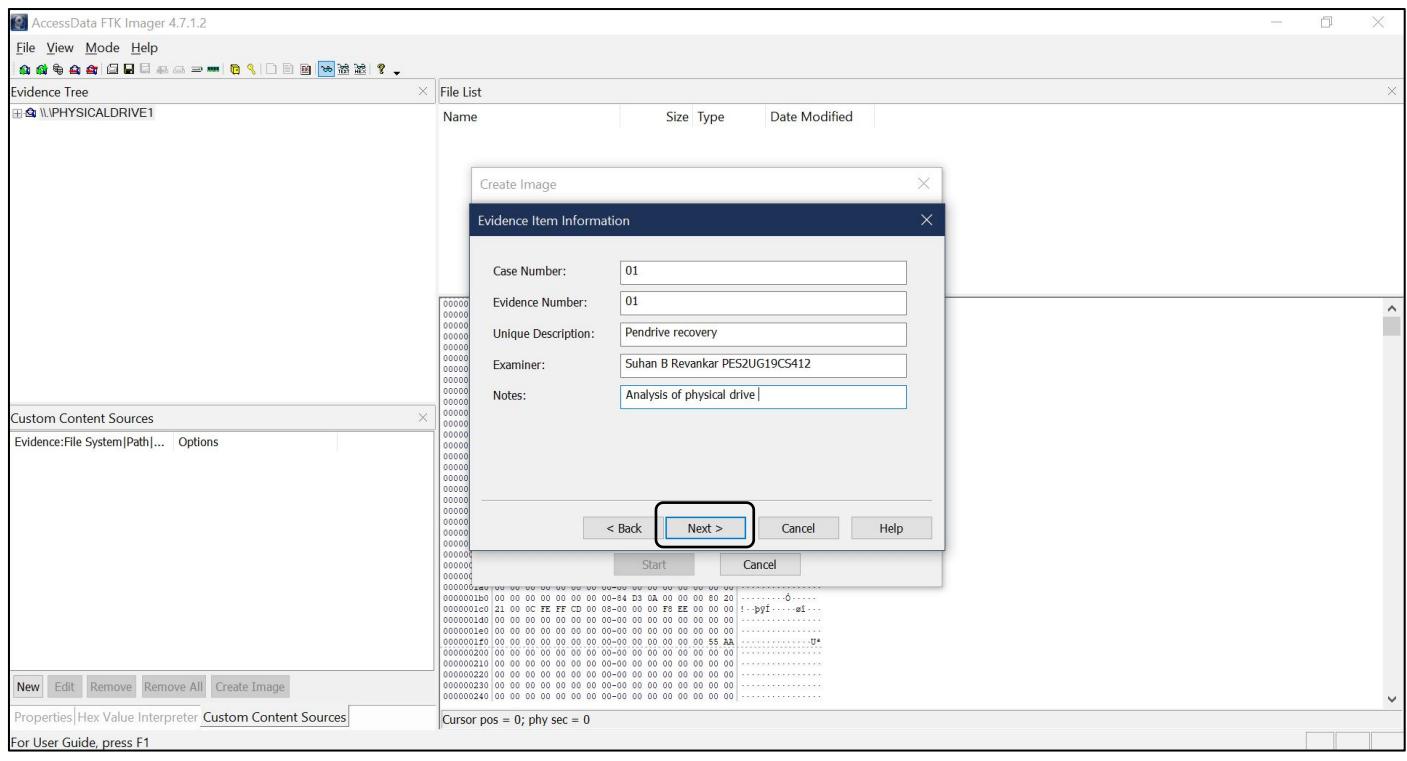


## 7. Select the target image type (Here Raw)

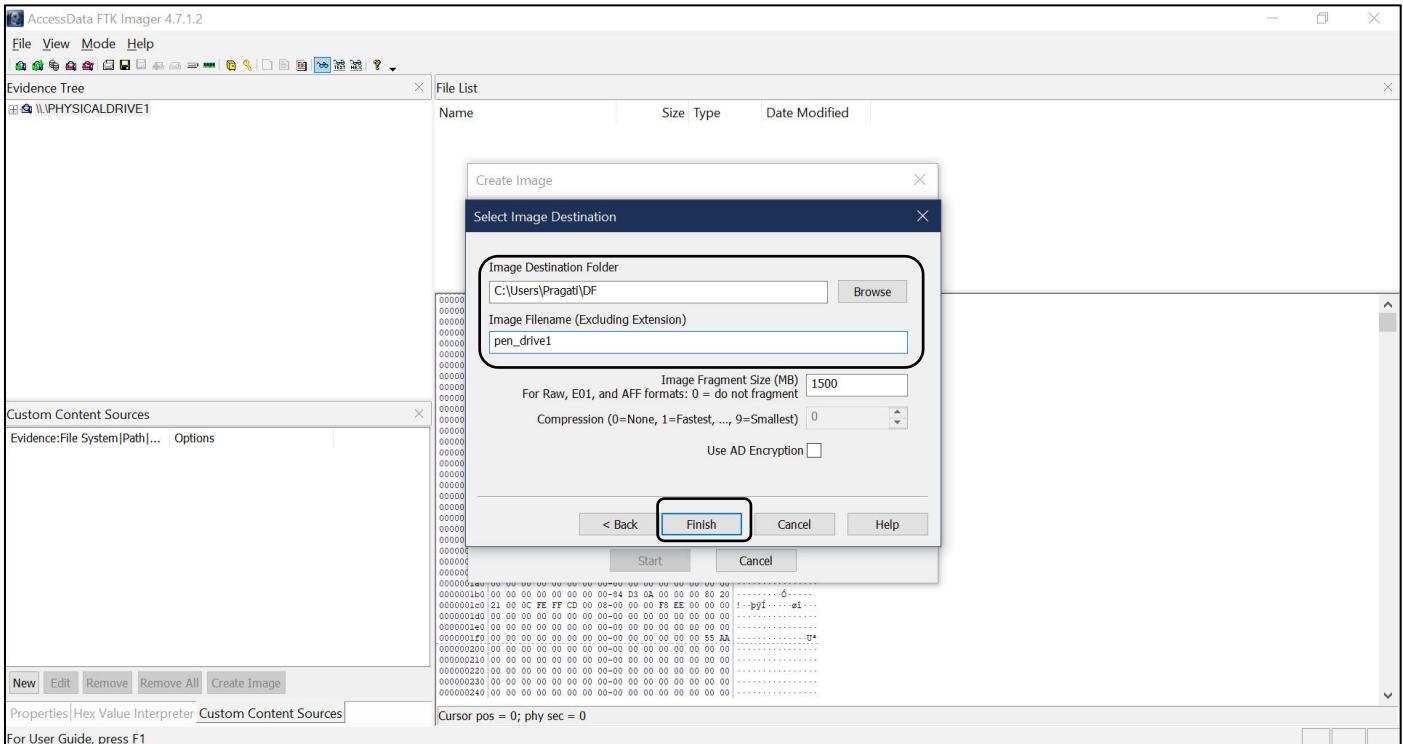




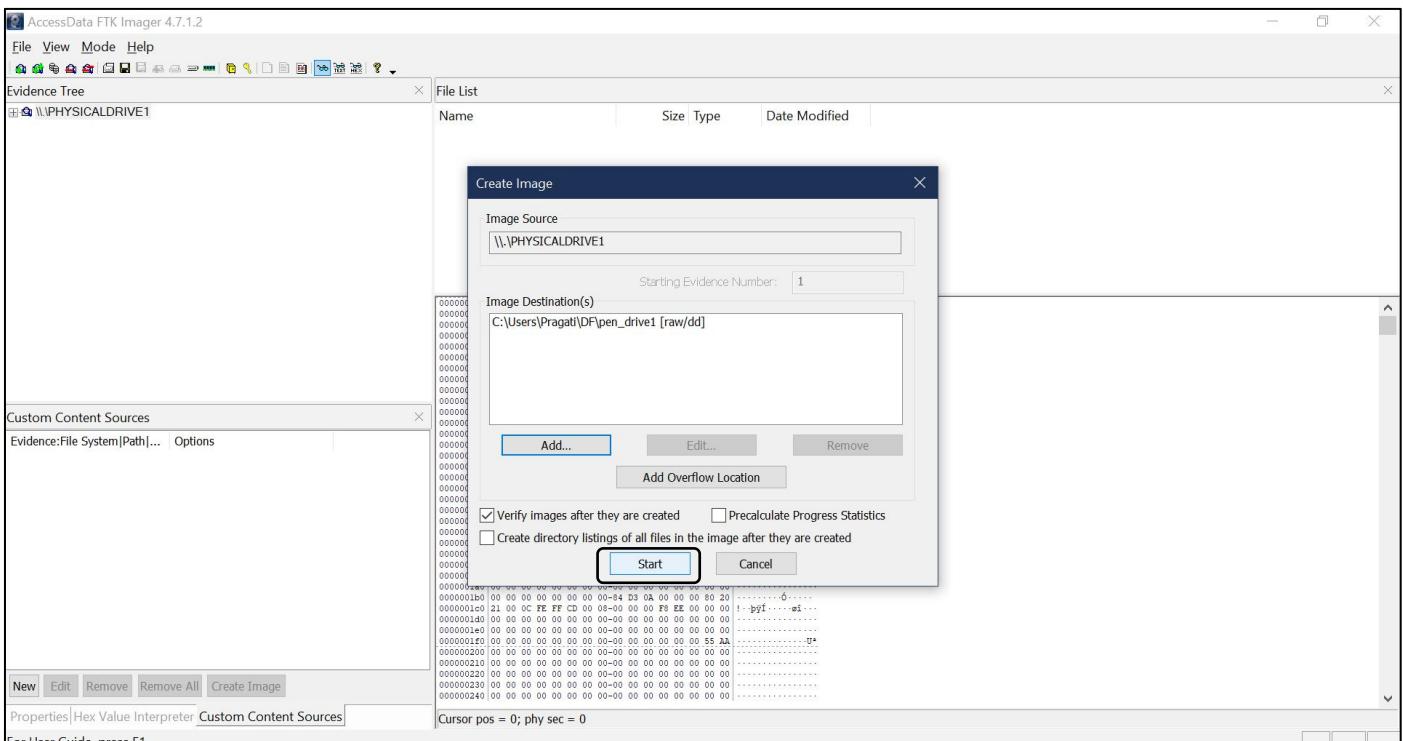
## 8 . Specify the details as per needs .



## 9 . Selecting the destination folder



## 10. The target can be seen in the window click on “Start”



## Part 3: Examining the details

### 1. Following are the results obtained

The screenshot shows the AccessData FTK Imager interface. On the left, the Evidence Tree pane displays the structure of a partition (ASDF [FAT32]) with various directories and unallocated space. The File List pane shows a detailed list of files with their names, sizes, types, and dates modified. A progress bar indicates the image creation process, which has completed successfully. The Drive/Image Verify Results pane on the right shows hash values (MD5, SHA1) for the image, comparing them with report hash values to confirm a match. The bottom status bar indicates the cursor position and log/phy seconds.

### 2. Evidence Tree : showing the directories , files , folders present before deletion .

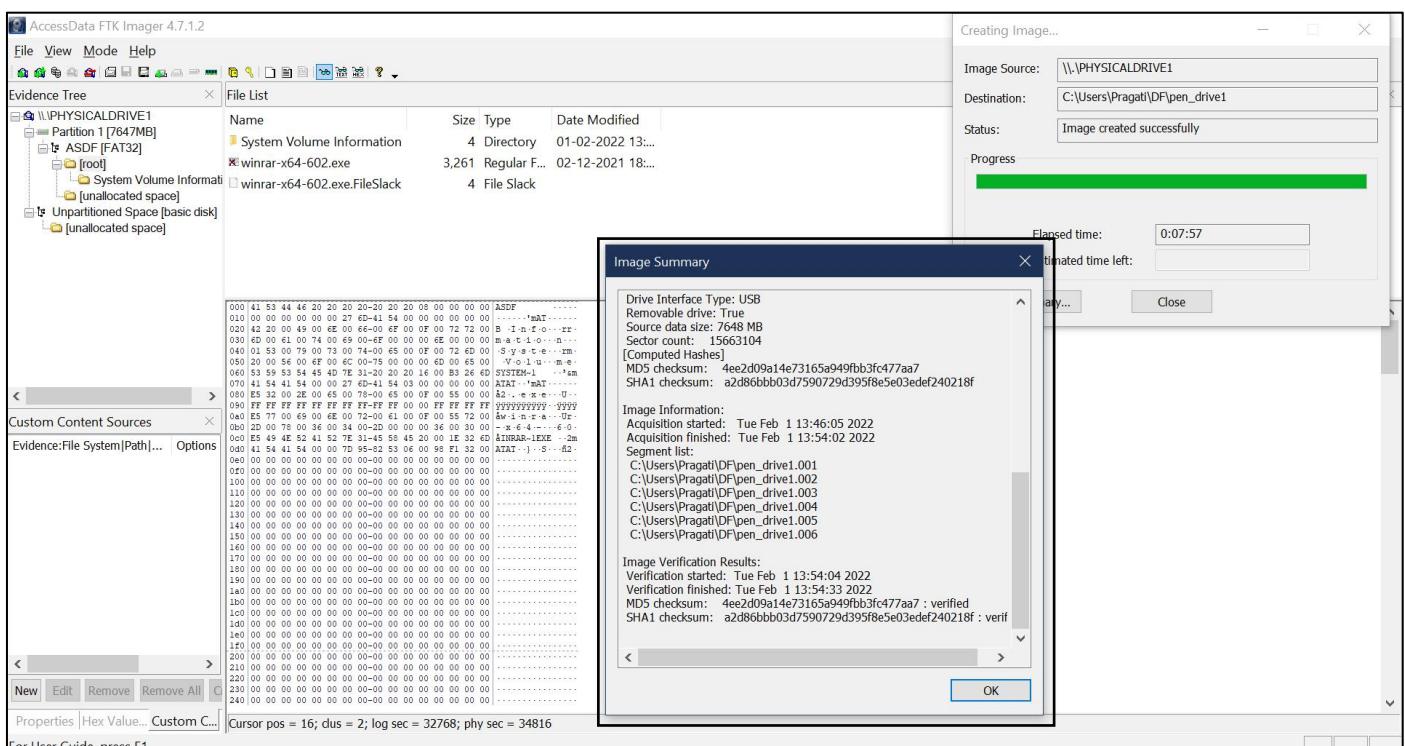
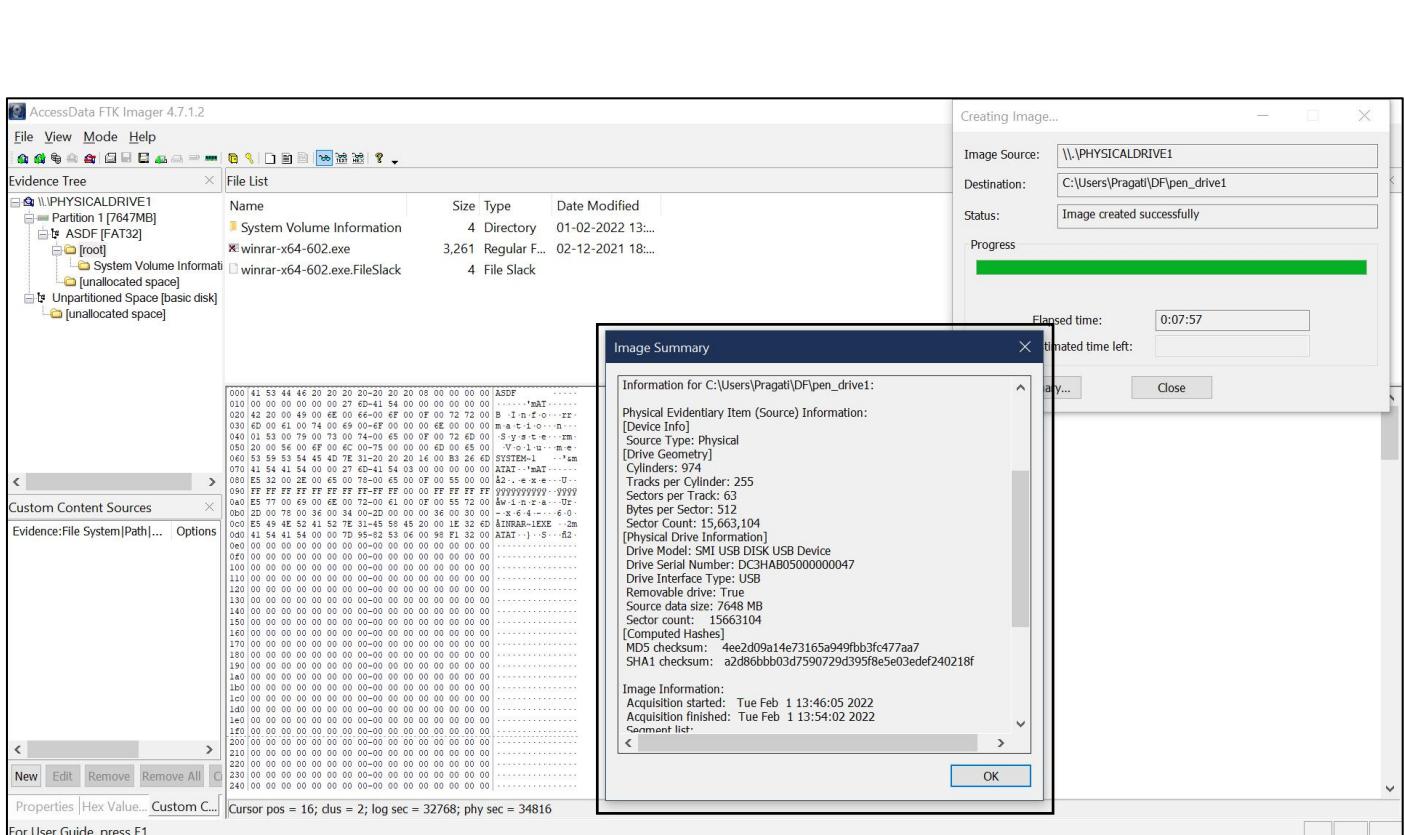
This screenshot shows the Evidence Tree pane with the same partition structure as the previous image. The File List pane below it displays a list of files, including 'winrar-x64-602.exe' and its associated slack file. The bottom status bar shows the cursor position and log/phy seconds, along with a note indicating 3 selected items.

Drive/Image Verify Results	
Name	pen_drive1.001
Sector count	15663104
MD5 Hash	
Computed hash	4ee2d09a14e73165a949fbb3fc477aa7
Report Hash	4ee2d09a14e73165a949fbb3fc477aa7
Verify result	Match
SHA1 Hash	
Computed hash	a2d86bbb03d7590729d395f8e5e03edef240218f
Report Hash	a2d86bbb03d7590729d395f8e5e03edef240218f
Verify result	Match
Bad Blocks List	No bad blocks found in image

### 3. Image summary (also can be found in text format in the destination folder specified)

The screenshot shows the AccessData FTK Imager interface. On the left, the Evidence Tree pane displays a file system structure for a partition named 'ASDF' (FAT32) on 'Partition 1 [7647MB]'. The root directory contains files like 'winrar-x64-602.exe' and 'winrar-x64-602.exe.FileSlack'. The main workspace shows a hex dump of the file 'winrar-x64-602.exe'. A modal dialog titled 'Image Summary' is open in the center, providing details about the image creation process. The summary includes:

- Created By: AccessData® FTK® Imager 4.7.1.2
- Case Information:
  - Acquired using: AD4.7.1.2
  - Case Number: 01
  - Evidence Number: 1
  - Unique description: pen\_drive
  - Examiner: Suhani B Revankar
  - Notes: analysis of usb.dd format (EXPORT)
- Information for C:\Users\Pragati\DF\pen\_drive1:
  - Physical Evidentiary Item (Source) Information:
    - [Device Info]
    - Source Type: Physical
    - [Drive Geometry]
    - Cylinders: 974
    - Tracks per Cylinder: 255
    - Sectors per Track: 63
    - Bytes per Sector: 512
    - Sector Count: 15,663,104
  - [Physical Drive Information]
    - Drive Model: SMI USB DISK USB Device
    - Drive Serial Number: DC3HARXKnnnnnnn47



## 4. Image summary in .txt format

```
pen_drive1.001 - Notepad
File Edit Format View Help
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 01
Evidence Number: 1
Unique description: pen_drive
Examiner: Suhan B Revankar
Notes: analysis of usb .dd format (EXPORT)

-----
Information for C:\Users\Pragati\DF\pen_drive1:

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 974
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 15,663,104
[Physical Drive Information]
Drive Model: SMI USB DISK USB Device
Drive Serial Number: DC3HAB05000000047
Drive Interface Type: USB
Removable drive: True
Source data size: 7648 MB
Sector count: 15663104
[Computed Hashes]
MD5 checksum: 4ee2d09a14e73165a949fbb3fc477aa7
SHA1 checksum: a2d86bbb03d7590729d395f8e5e03edef240218f

Ln 25, Col 38 | 100% | Windows (CRLF) | UTF-8 with BOM
```

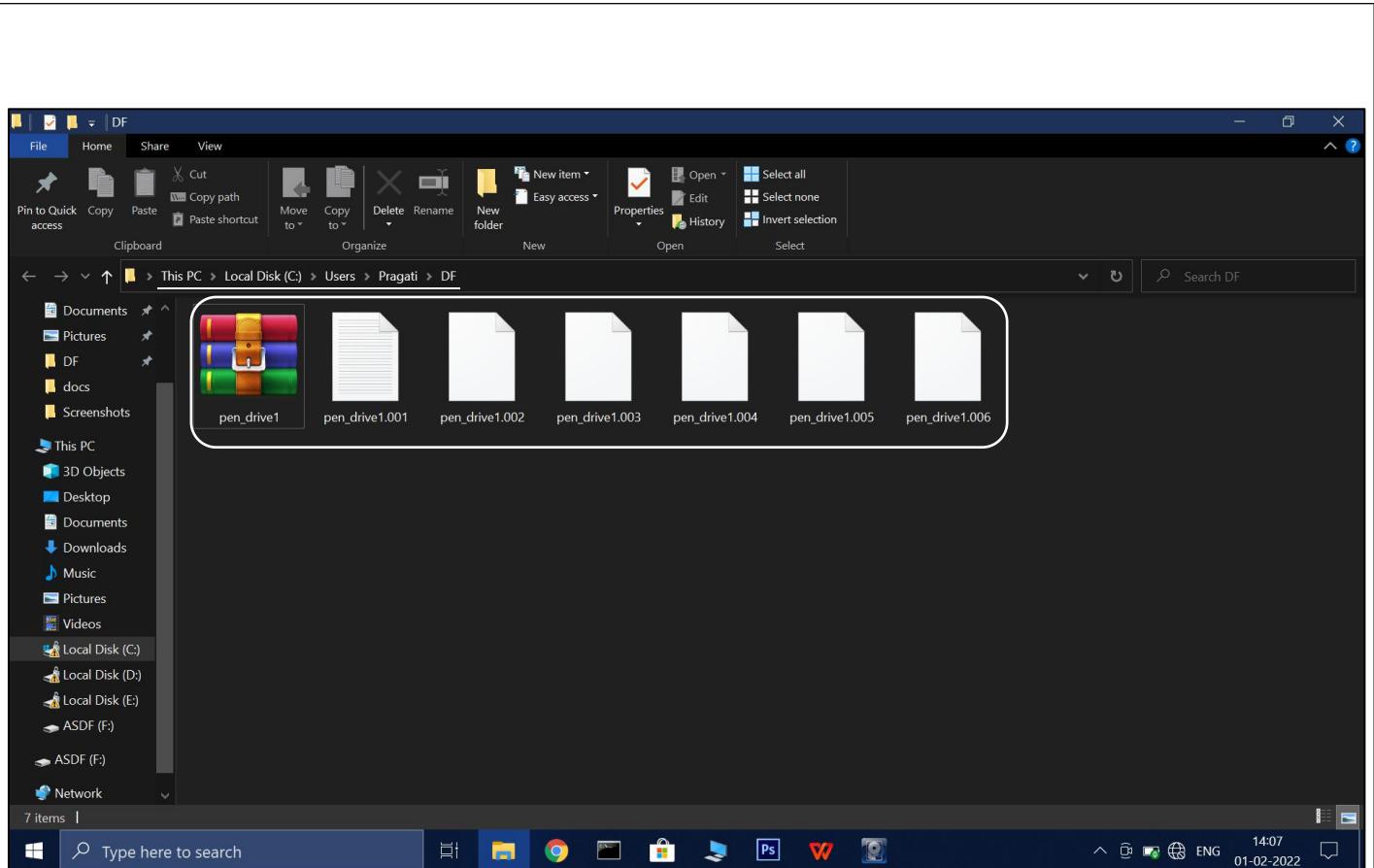
```
pen_drive1.001 - Notepad
File Edit Format View Help
[Computed Hashes]
MD5 checksum: 4ee2d09a14e73165a949fbb3fc477aa7
SHA1 checksum: a2d86bbb03d7590729d395f8e5e03edef240218f

Image Information:
Acquisition started: Tue Feb 1 13:46:05 2022
Acquisition finished: Tue Feb 1 13:54:02 2022
Segment list:
C:\Users\Pragati\DF\pen_drive1.001
C:\Users\Pragati\DF\pen_drive1.002
C:\Users\Pragati\DF\pen_drive1.003
C:\Users\Pragati\DF\pen_drive1.004
C:\Users\Pragati\DF\pen_drive1.005
C:\Users\Pragati\DF\pen_drive1.006

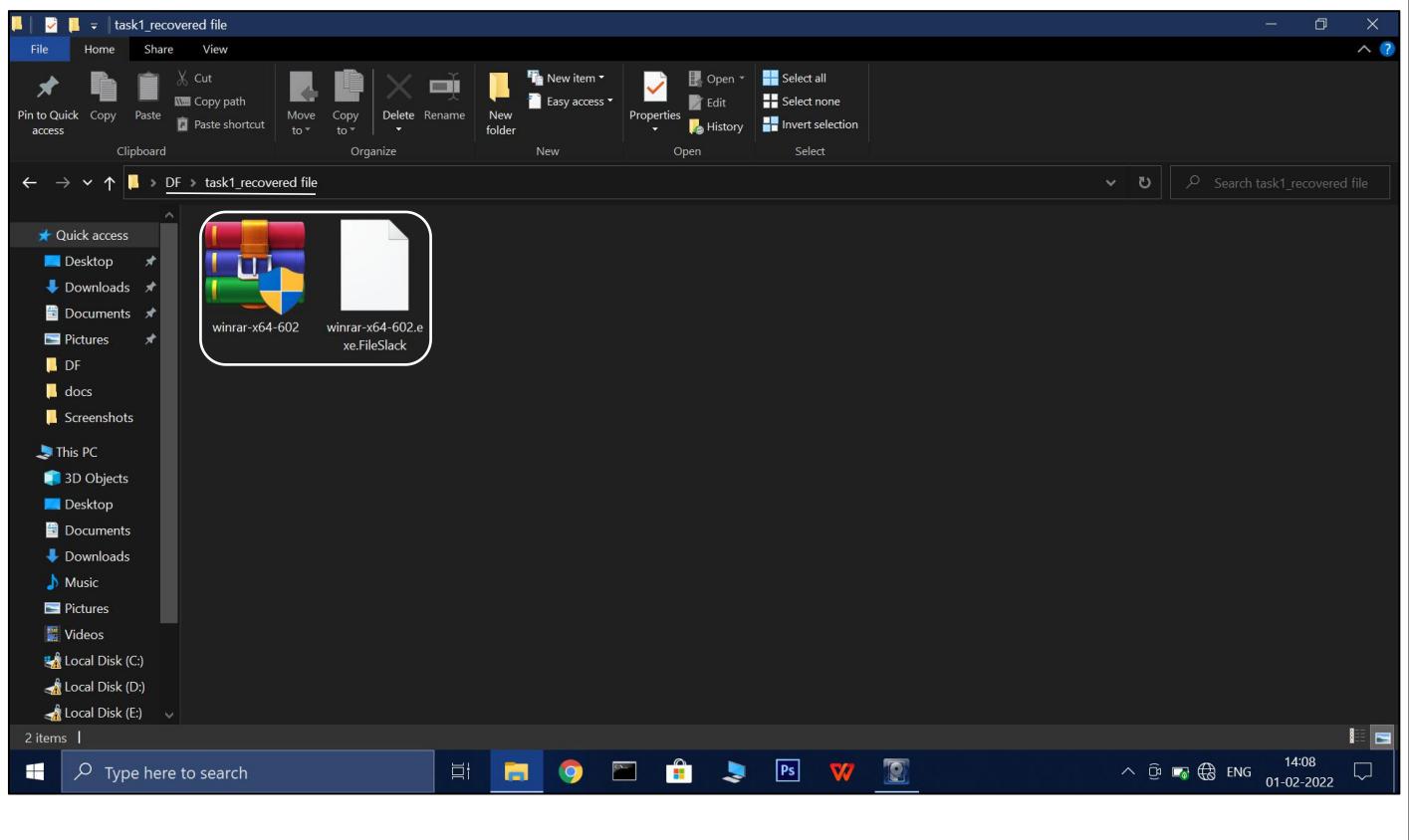
Image Verification Results:
Verification started: Tue Feb 1 13:54:04 2022
Verification finished: Tue Feb 1 13:54:33 2022
MD5 checksum: 4ee2d09a14e73165a949fbb3fc477aa7 : verified
SHA1 checksum: a2d86bbb03d7590729d395f8e5e03edef240218f

Ln 25, Col 38 | 160% | Windows (CRLF) | UTF-8 with BOM
```

5. The analyze images can be exported for further analysis in different tools .  
(can be found in the target folder)



## 6 . At times if possible the deleted files and folders can be recovered .



## Activity 2

Using Autopsy tool , to analyse the Forensic images that were generated .  
To form a well detailed report .

### Part 1: Loading of Images

**New Case Information**

**Steps**

1. Case Information  
2. Optional Information

**Case Information**

Case Name: Email-Analysis

Base Directory: C:\Users\Pragati\Desktop\Autopsy\

Case Type:  Single-User  Multi-User

Case data will be stored in the following directory:  
C:\Users\Pragati\Desktop\Autopsy\Email-Analysis

**Target directory to store the report / case data**

< Back  Finish Cancel Help

**New Case Information**

**Steps**

1. Case Information  
2. Optional Information

**Optional Information**

Case

Number: 001

Examiner

Name: Suhan B Revankar - PES2UG19CS412

Phone:

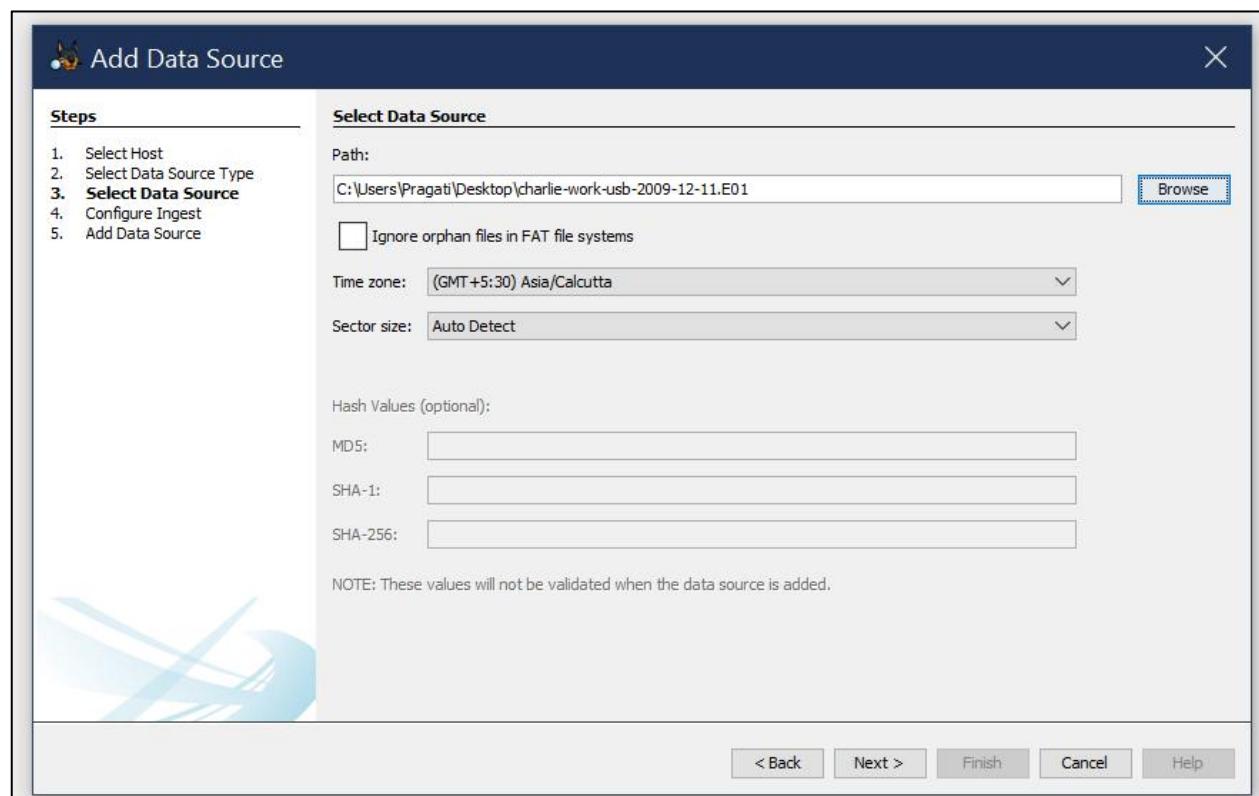
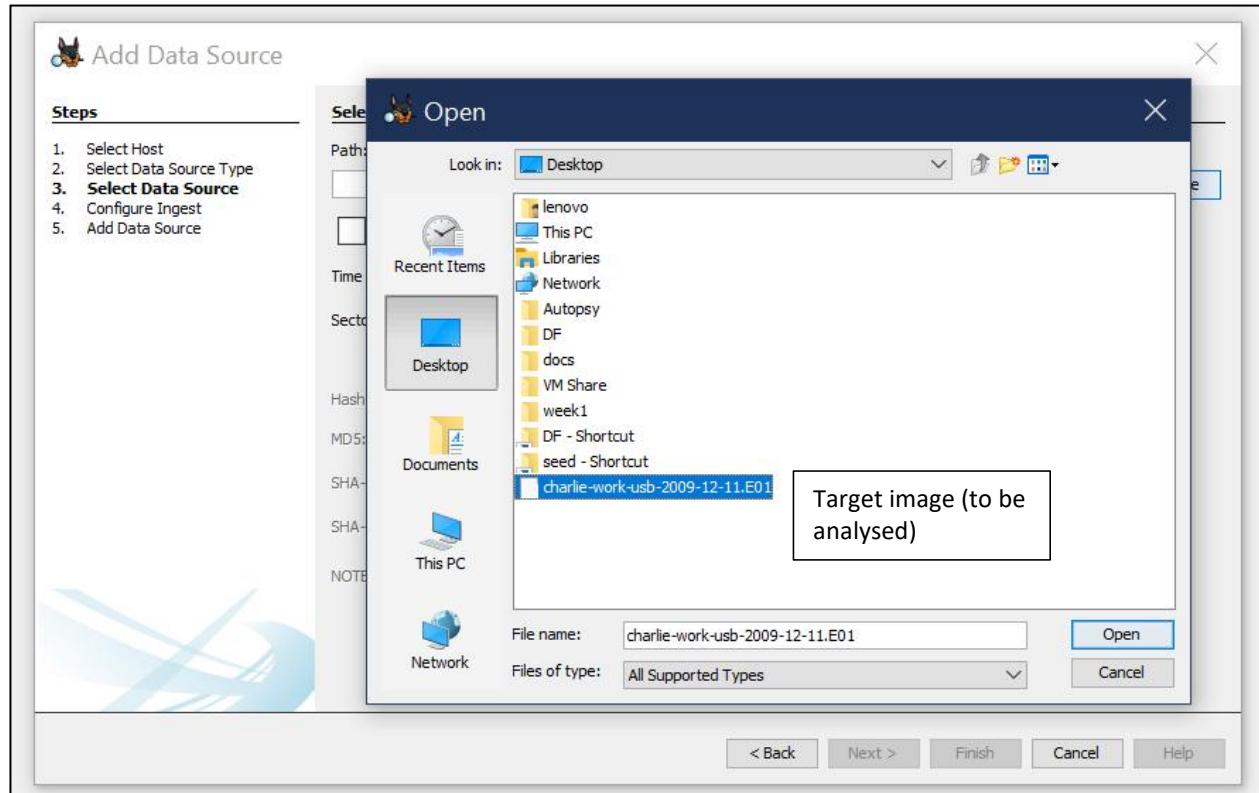
Email: suhanbrevenkar29@gmail.com

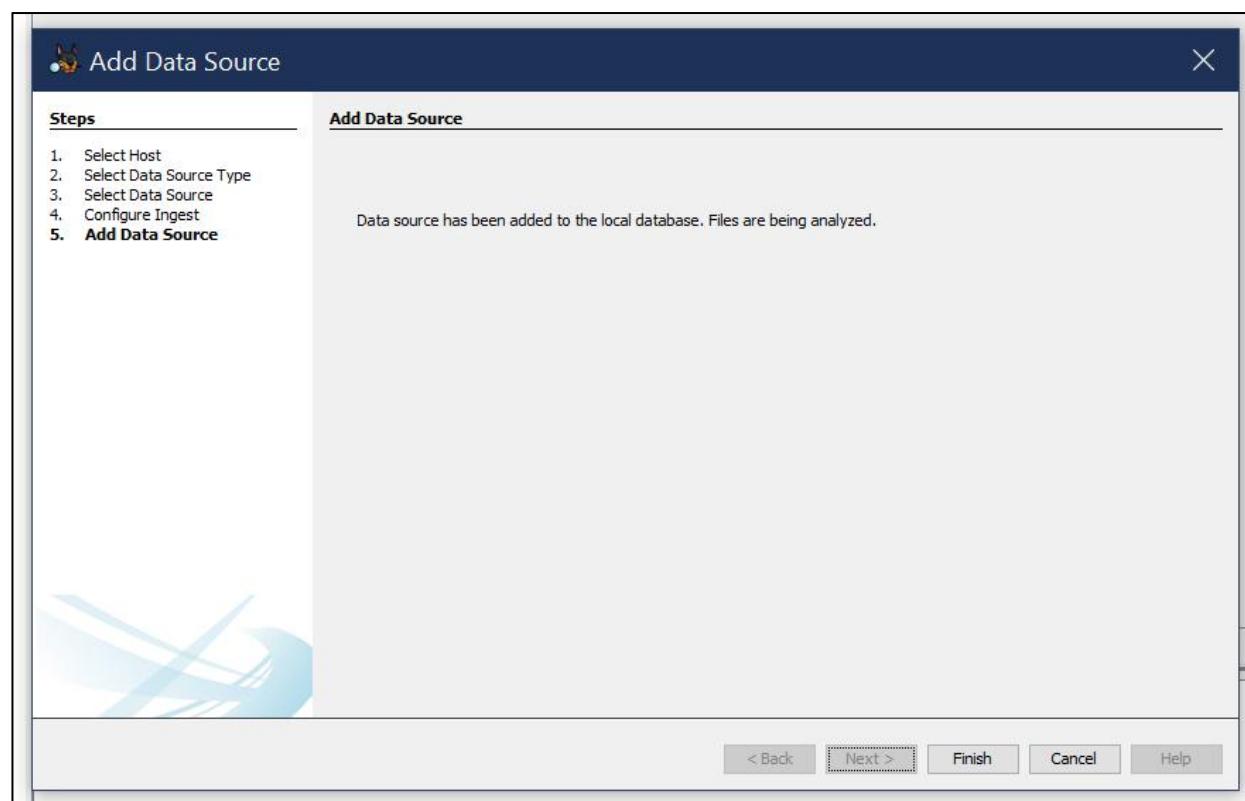
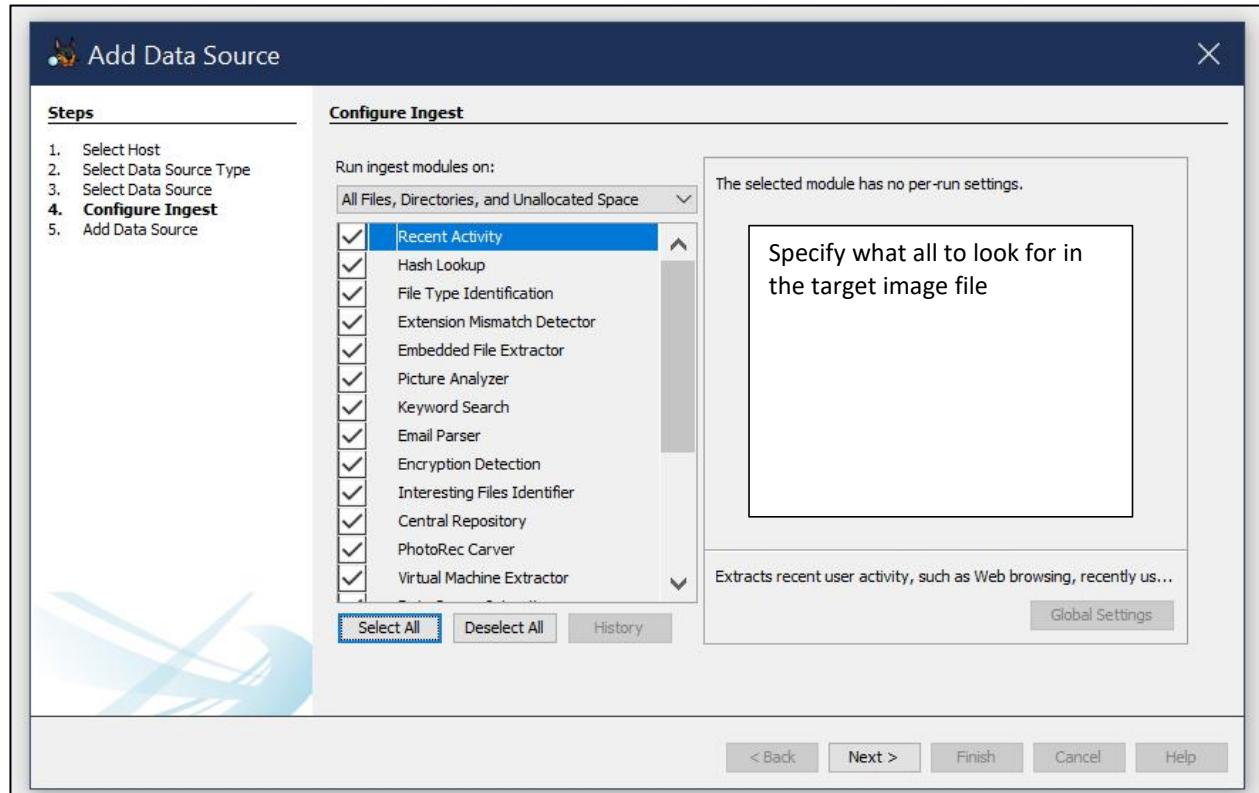
Notes:

Organization

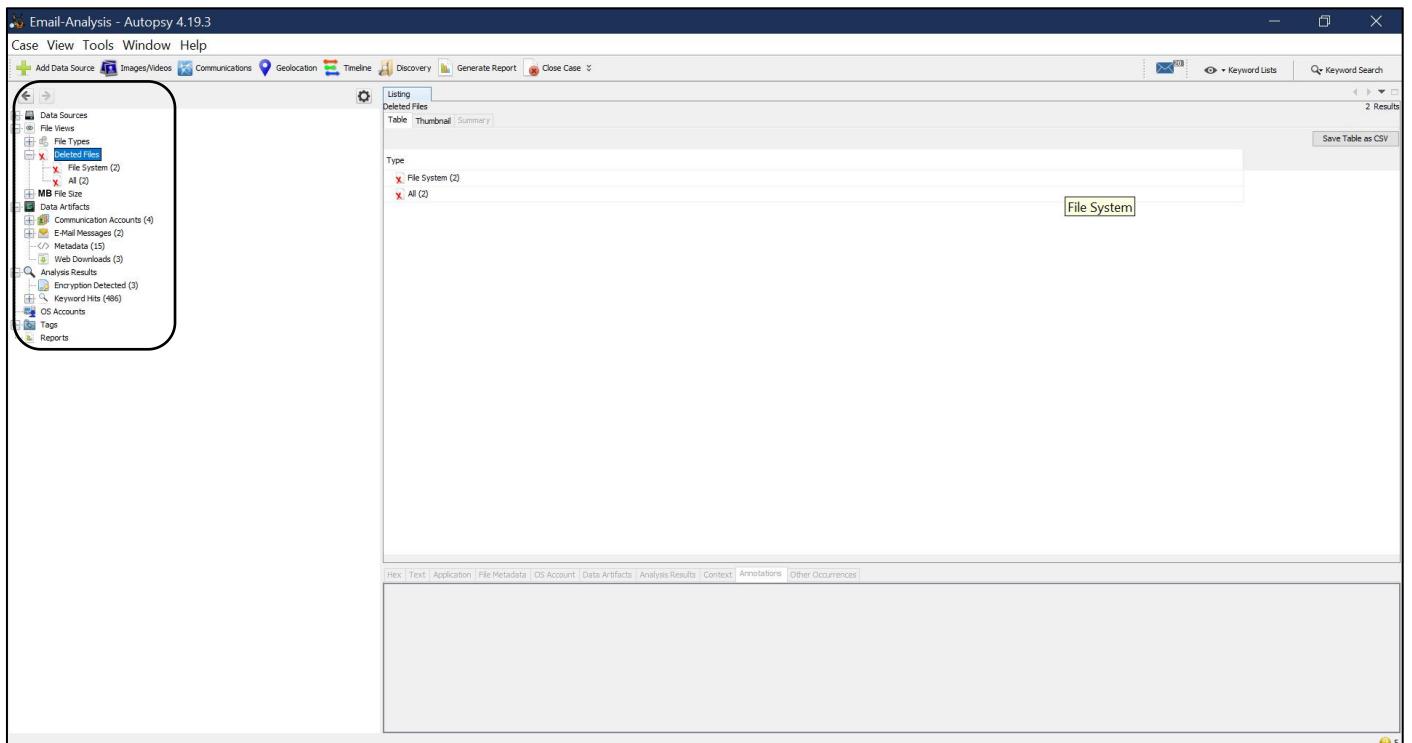
Organization analysis is being done for: Not Specified

< Back  Finish Cancel Help

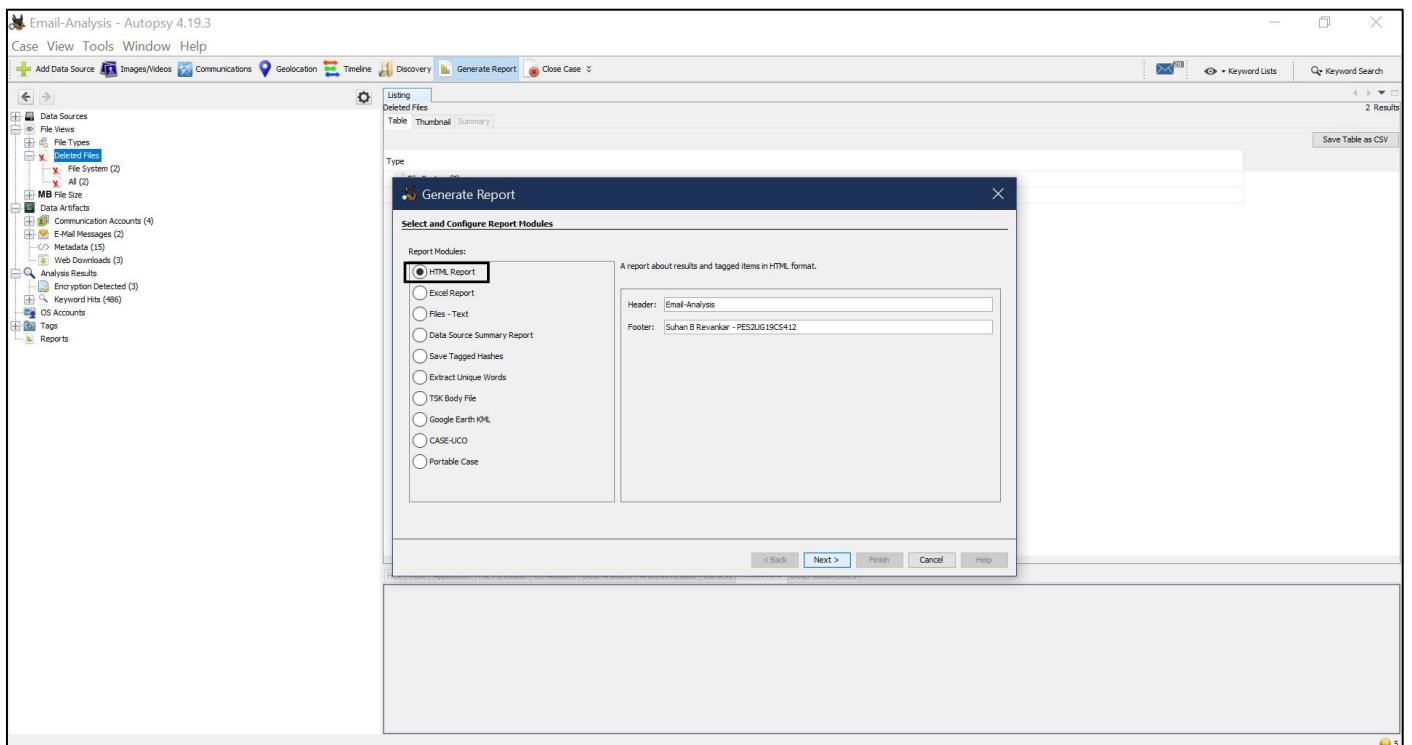


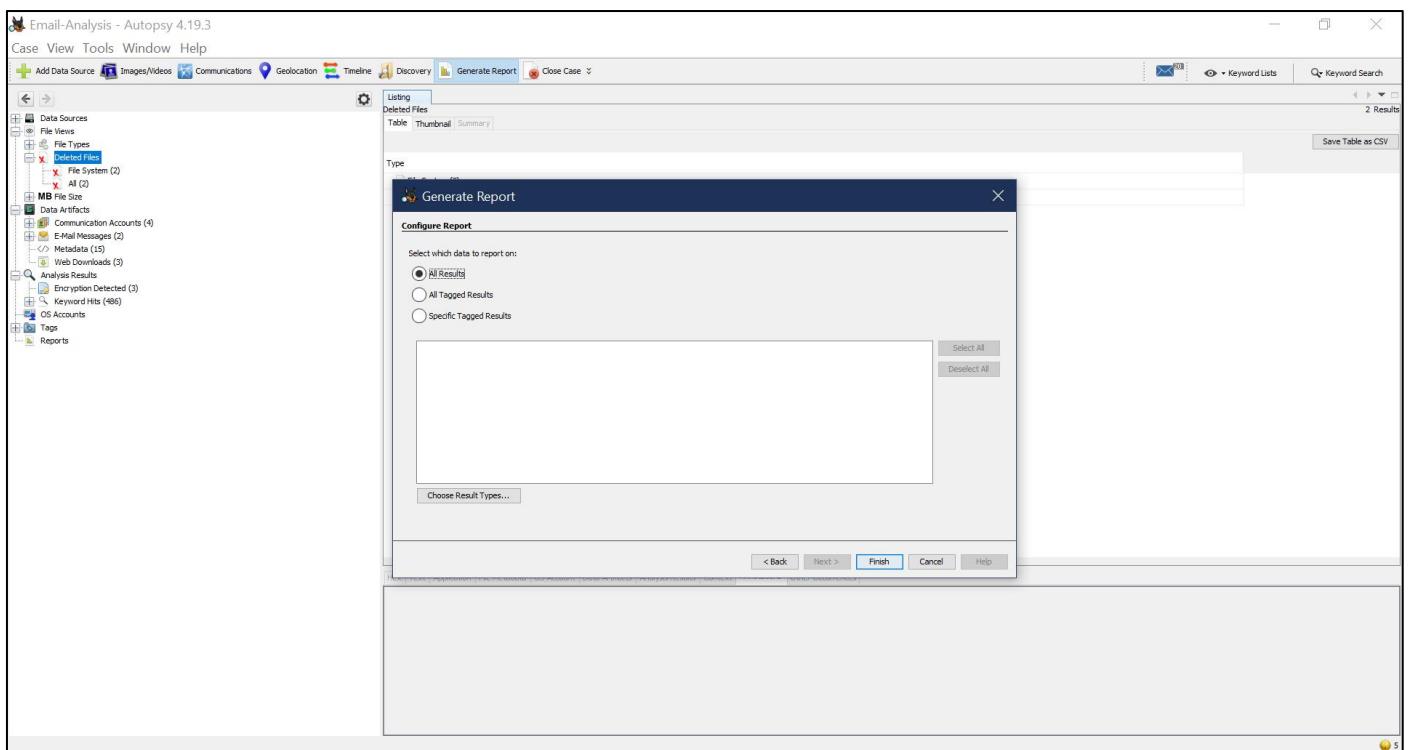
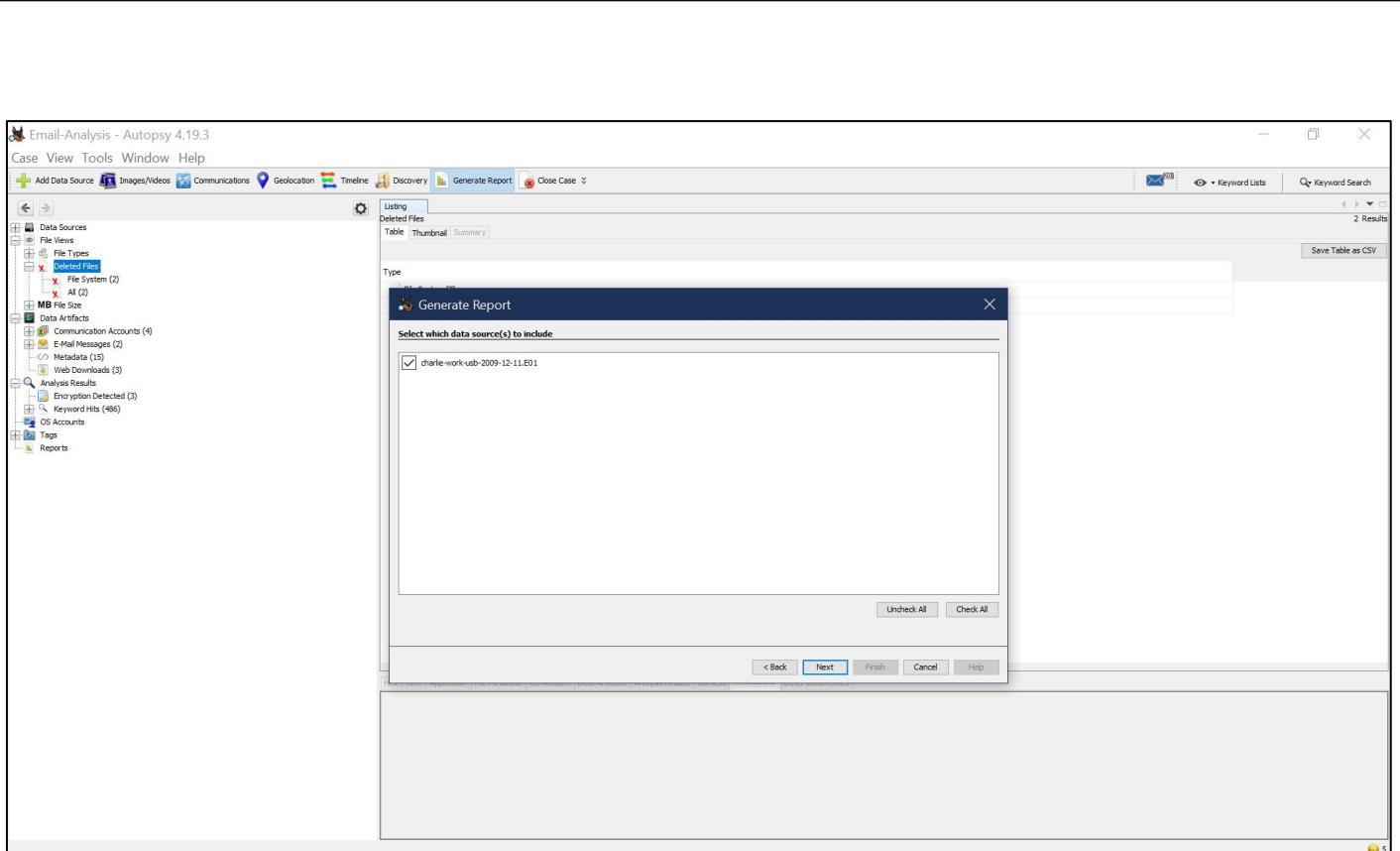


“Deleted files” specify the files , structure of directories etc . that were recovered from the target image .

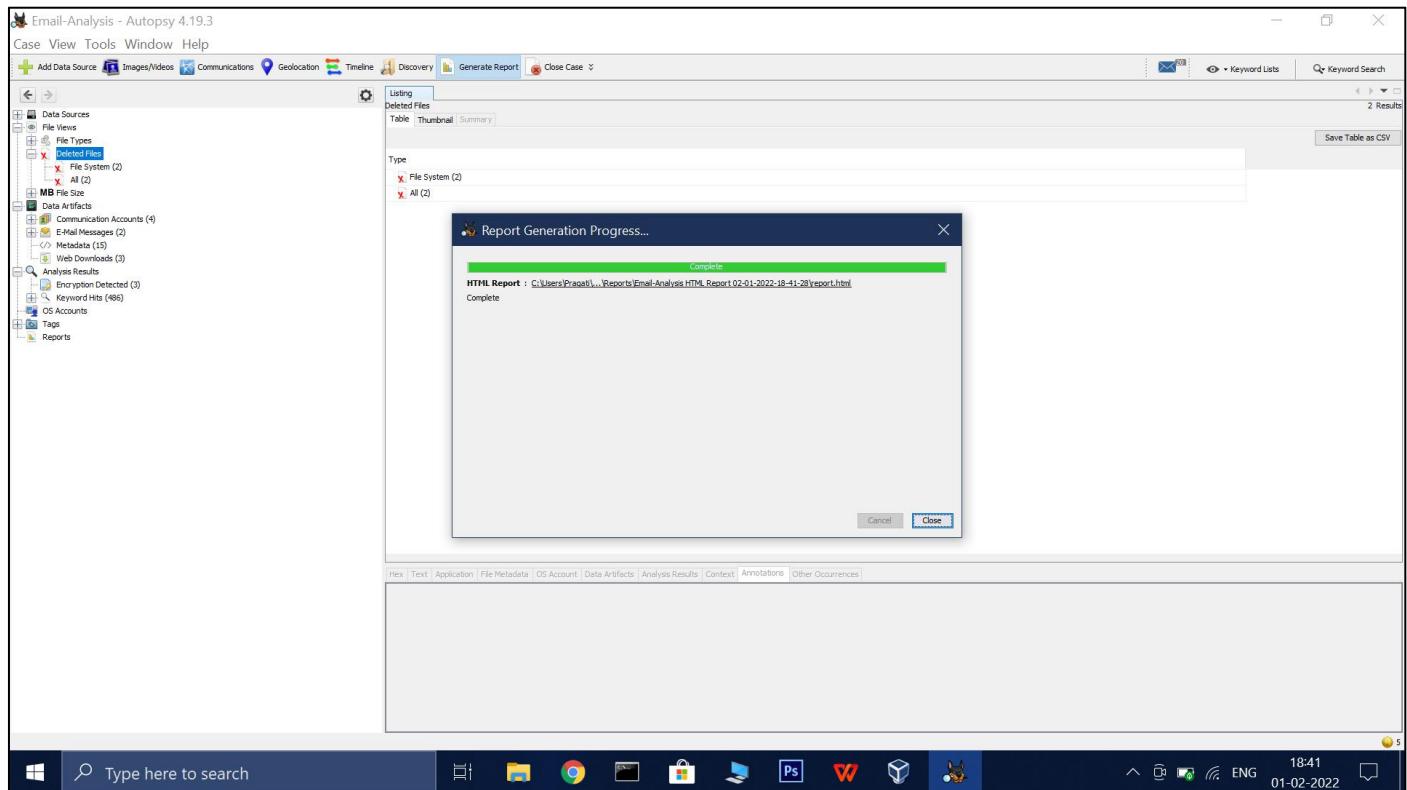


Click on “generate report” to get the detailed analysis report and select the file format of report needed .





# Report generated Successfully



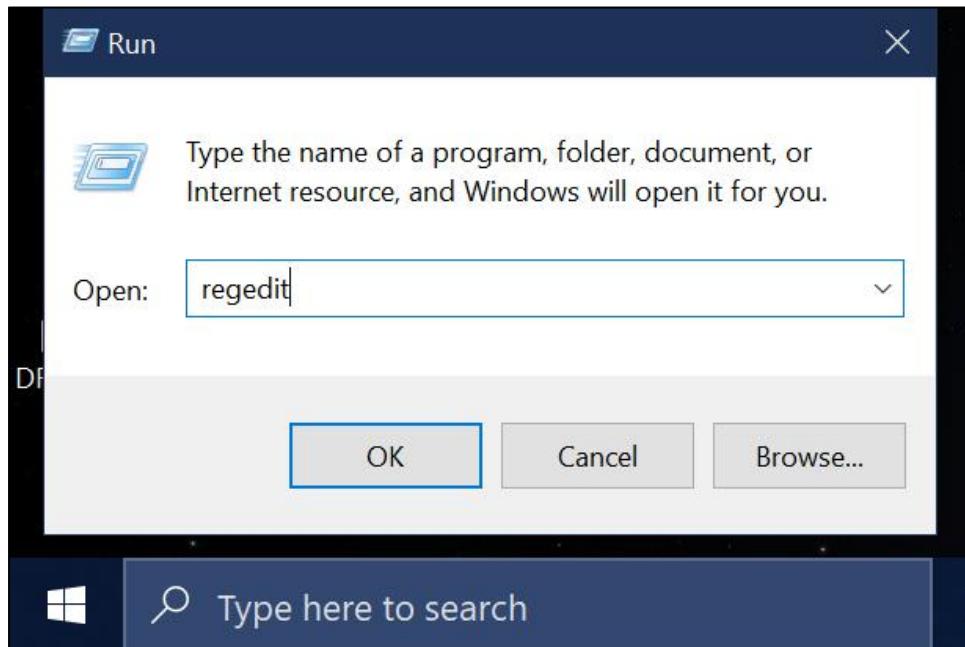
# Forensic Report

The screenshot shows the generated Autopsy Forensic Report for case 'Email-Analysis'. The title is 'Autopsy Forensic Report' and it was generated on 2022/02/01 18:41:28. The report navigation sidebar on the left includes links for Case Summary, Accounts: Email (4), E-Mail Messages (2), Encryption Detected (3), Keyword Hits (486), Metadata (15), Tagged Files (0), Tagged Images (0), Tagged Results (0), and Web Downloads (3). The main content area starts with 'Email-Analysis' and the title 'Autopsy Forensic Report'. It provides details about the case: Case: Email-Analysis, Case Number: 001, Number of data sources in case: 1, Examiner: Suhan B Revankar - PES2UG19CS412. Below this is an 'Image Information:' section showing a file named 'charlie-work-usb-2009-12-11.E01' with Timezone: Asia/Calcutta and Path: C:\Users\Pragati\Desktop\charlie-work-usb-2009-12-11.E01. The bottom status bar is identical to the one in the previous screenshot.

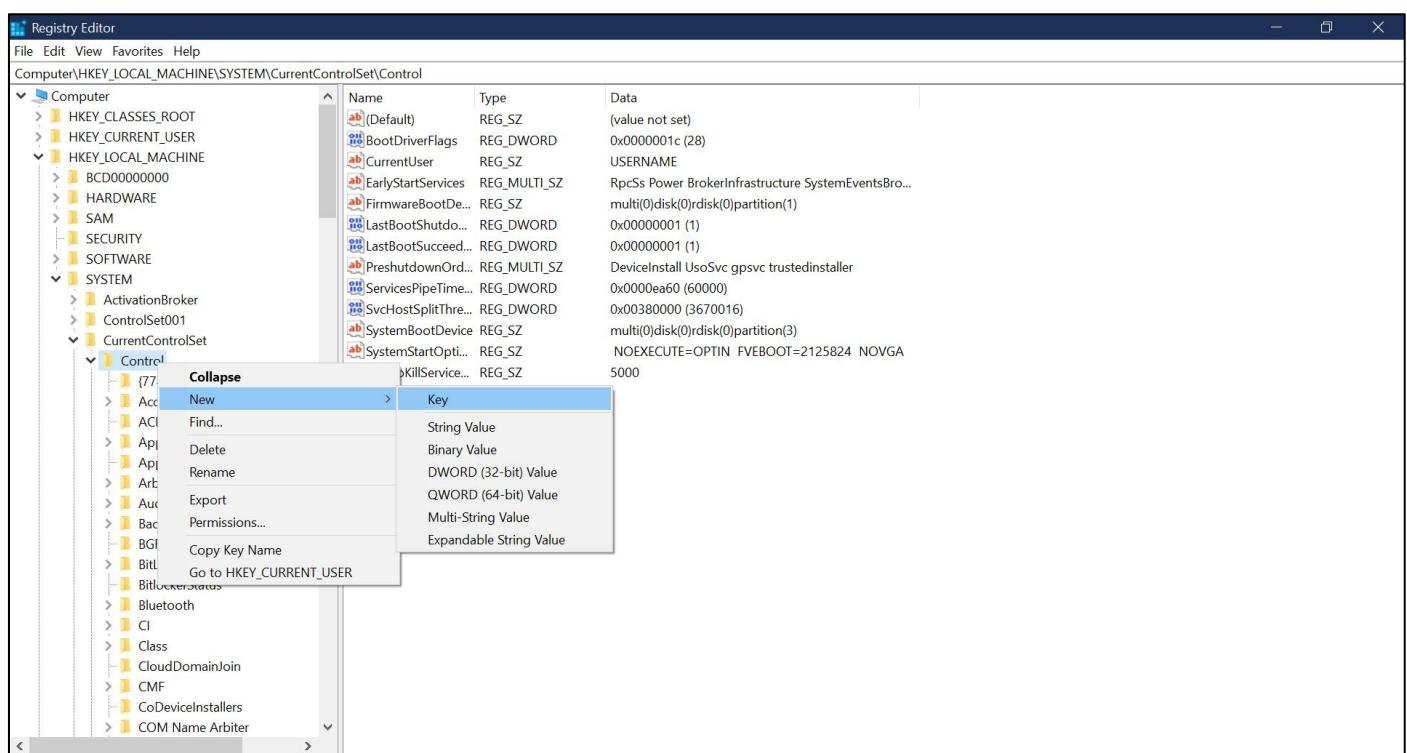
## Activity 3

### Write Block on USB Device

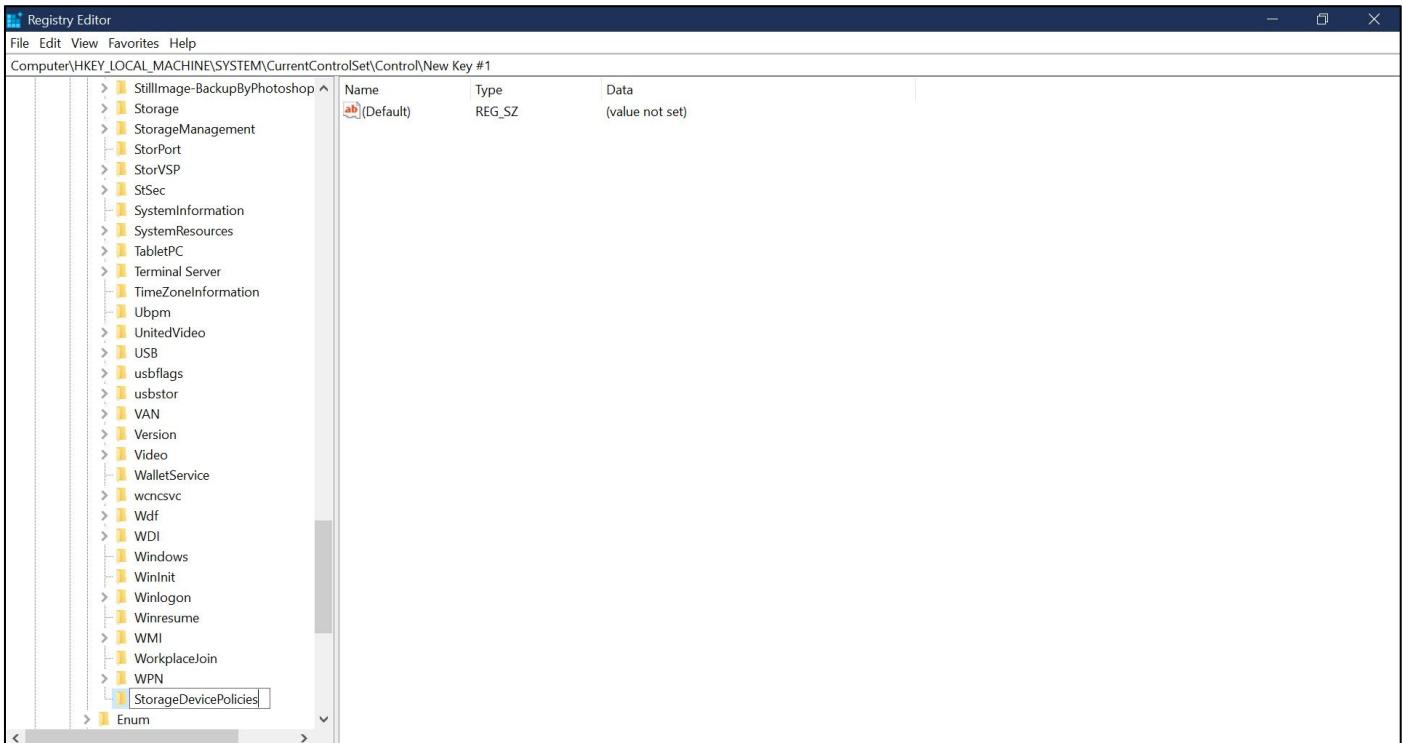
1. Open registry editor (click on run program & type **regedit** and click on run)



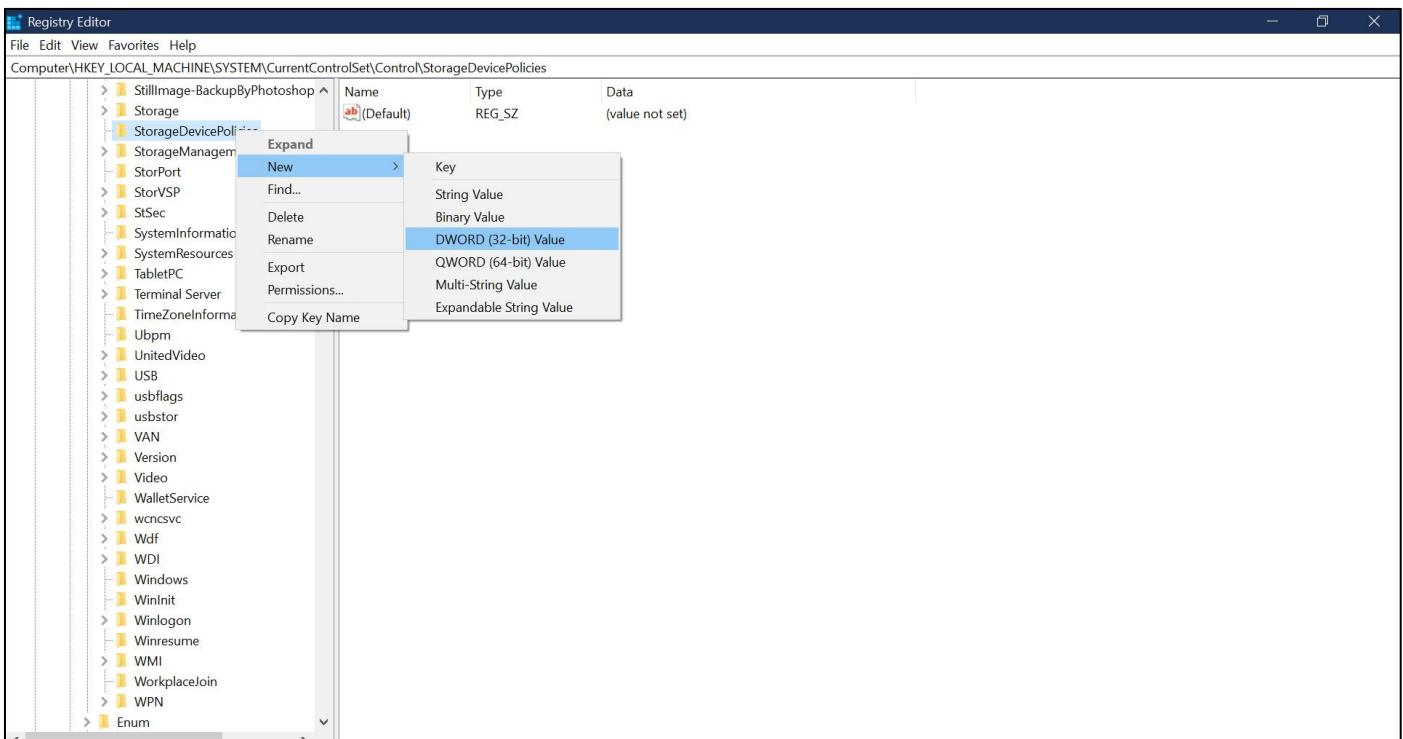
2. Navigate to HKEY\_LOCAL\_MACHINE -> SYSTEM -> CurrentControlSet -> Control  
Right click then select new -> Key



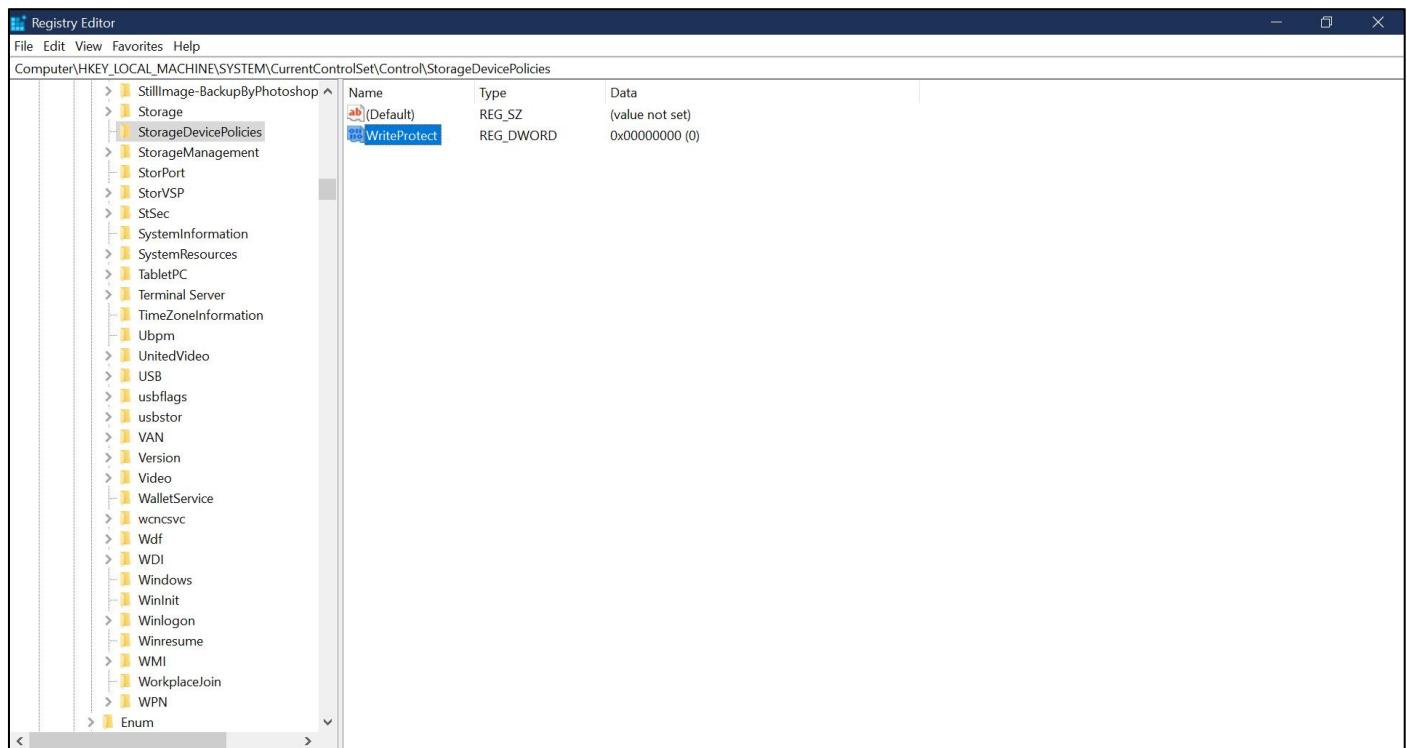
### 3. Name the key as StorageDevicePolicies



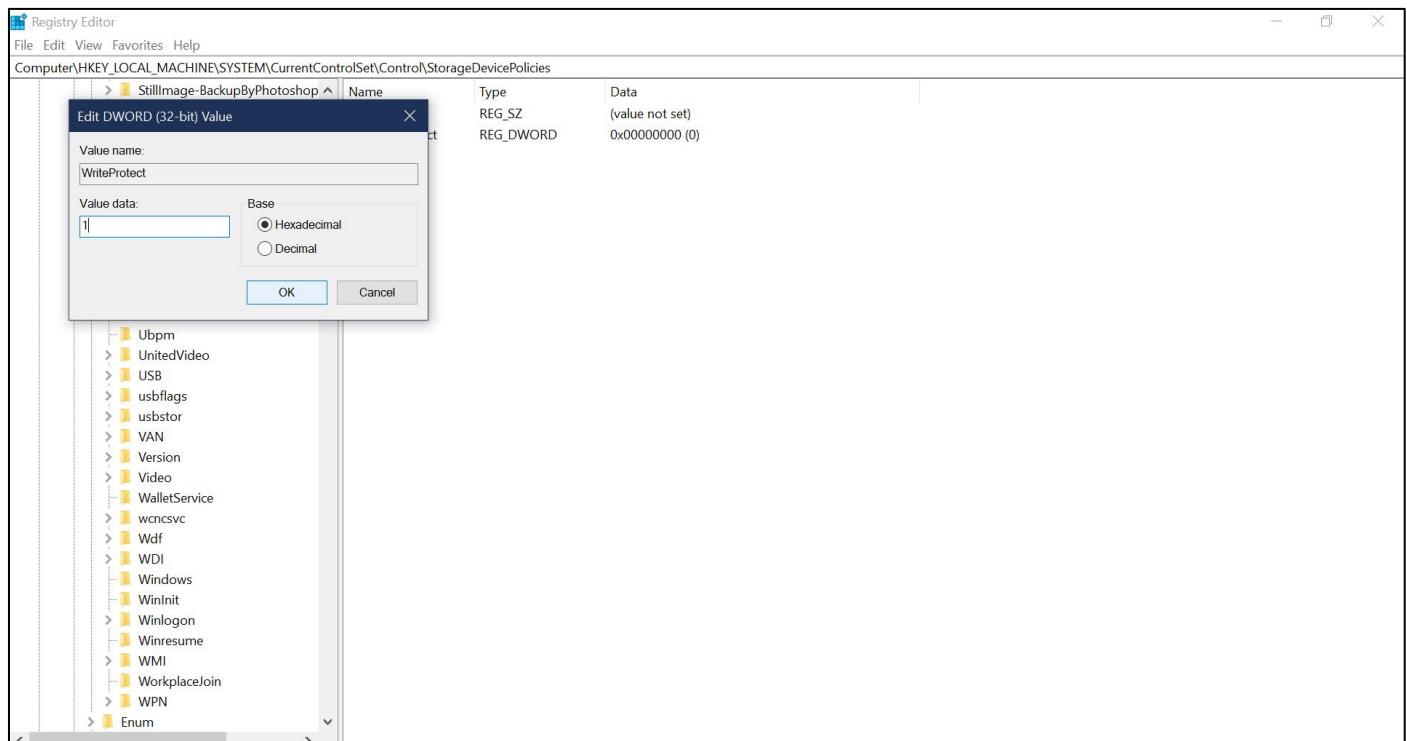
### 4. Right click select new -> DWORD (32-bit) Value



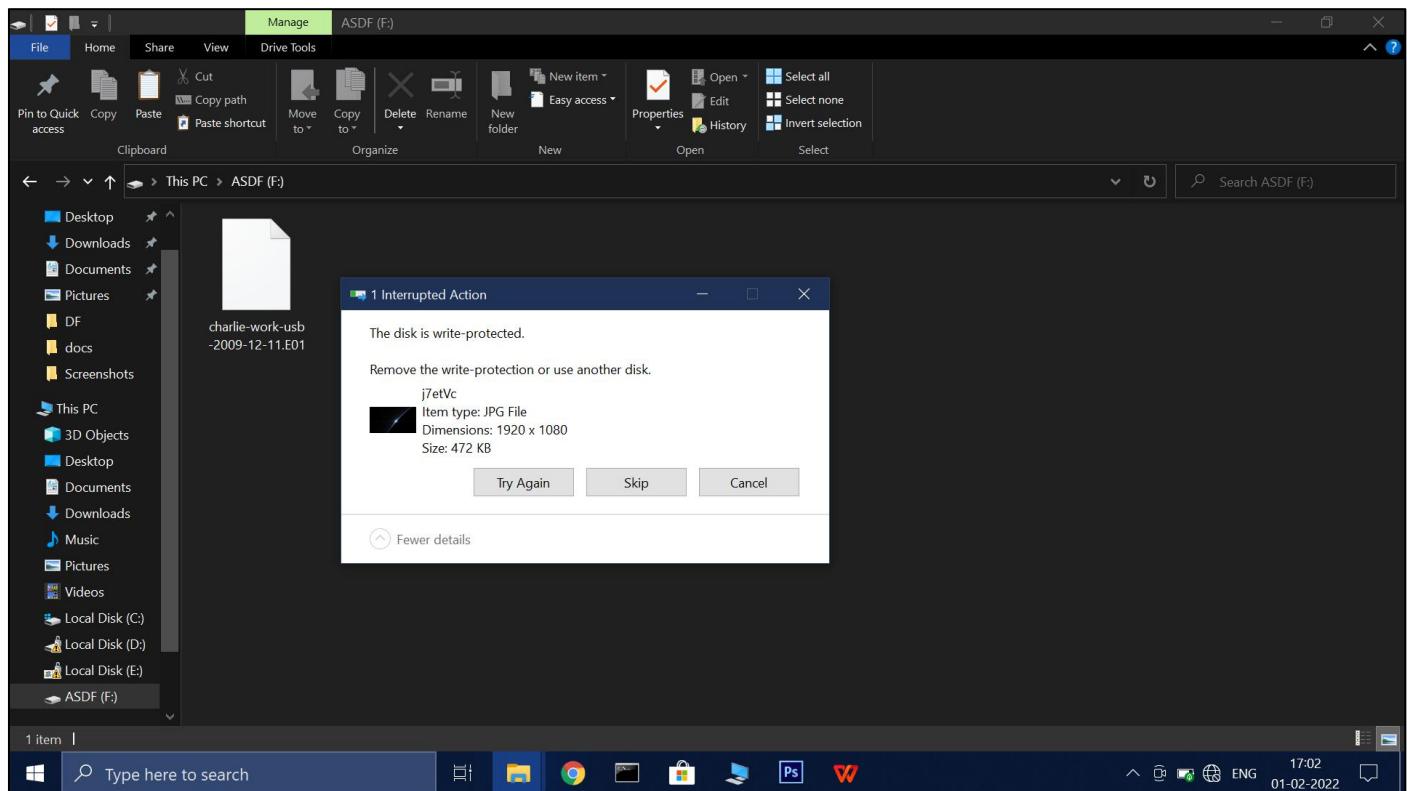
## 5 . Name the file as WriteProtect



## 6 . Change the value from 0 to 1 [To enable write protect to or from the usb]

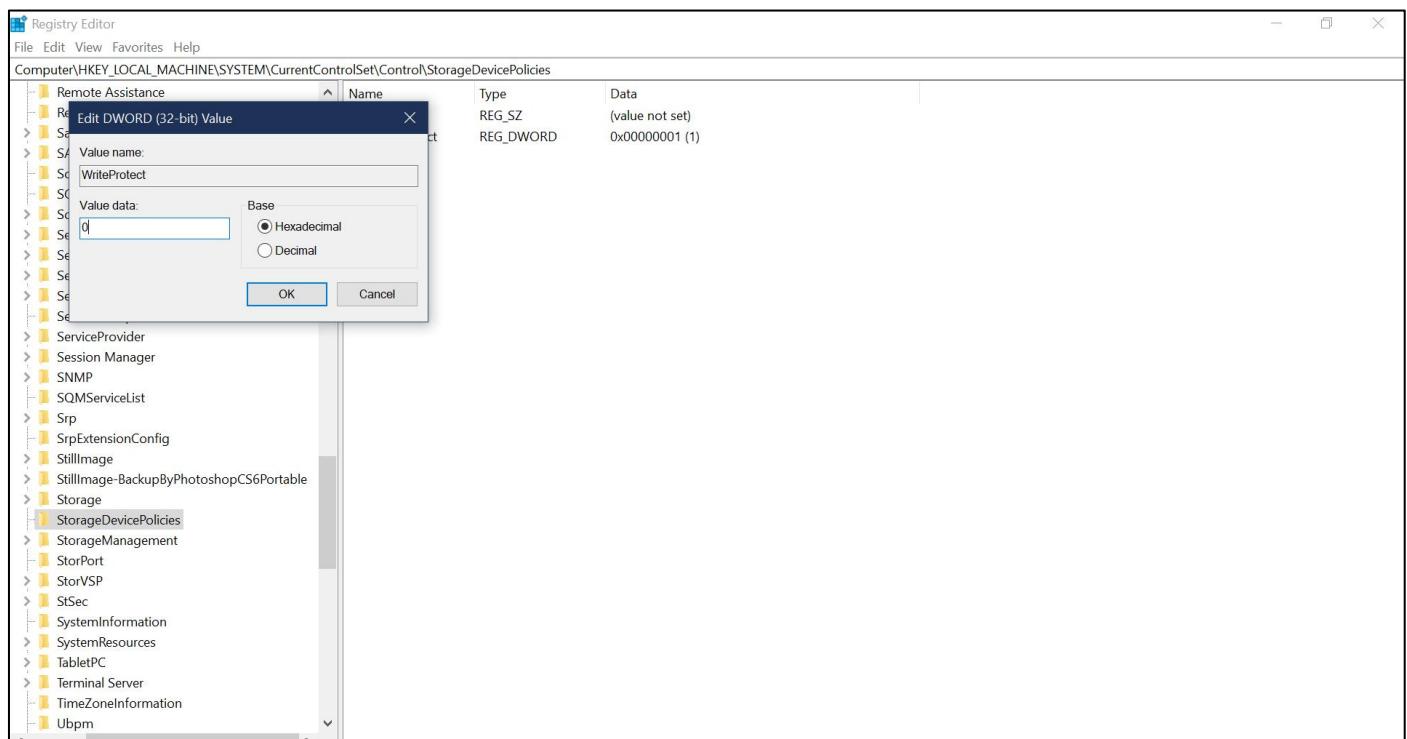


## Result snapshot after enabling write Protect

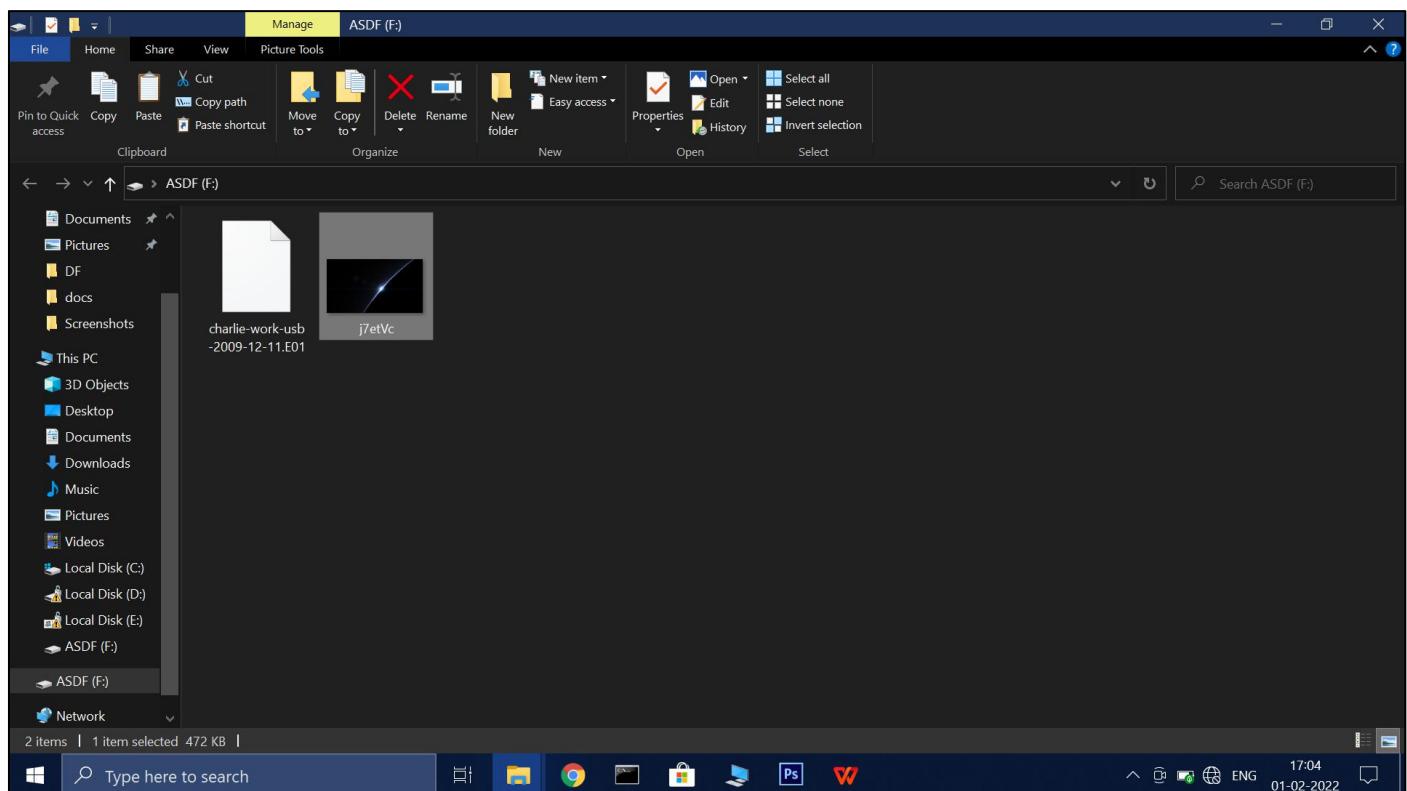
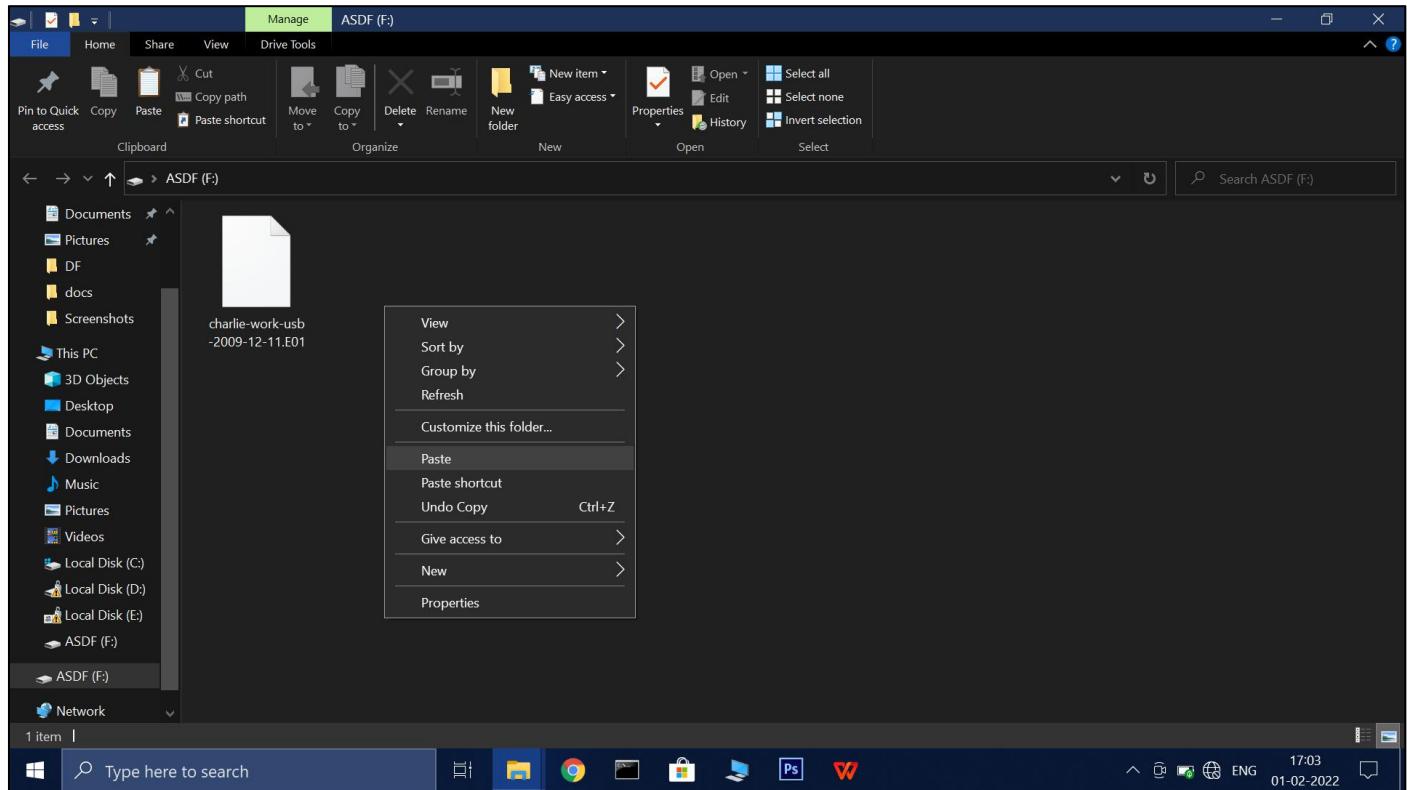


To disable the write protect to or from the usb device

Navigate to same path as previous , change the value from 1 to 0 [disabling write protect ]



## Result after disabling write protect



\*\*\*\*\*