PES UNIVERSITY

UE19CS336
Digital Forensics

Name : Suhan B Revankar
SRN : PES2UG19CS412
Section : G Section

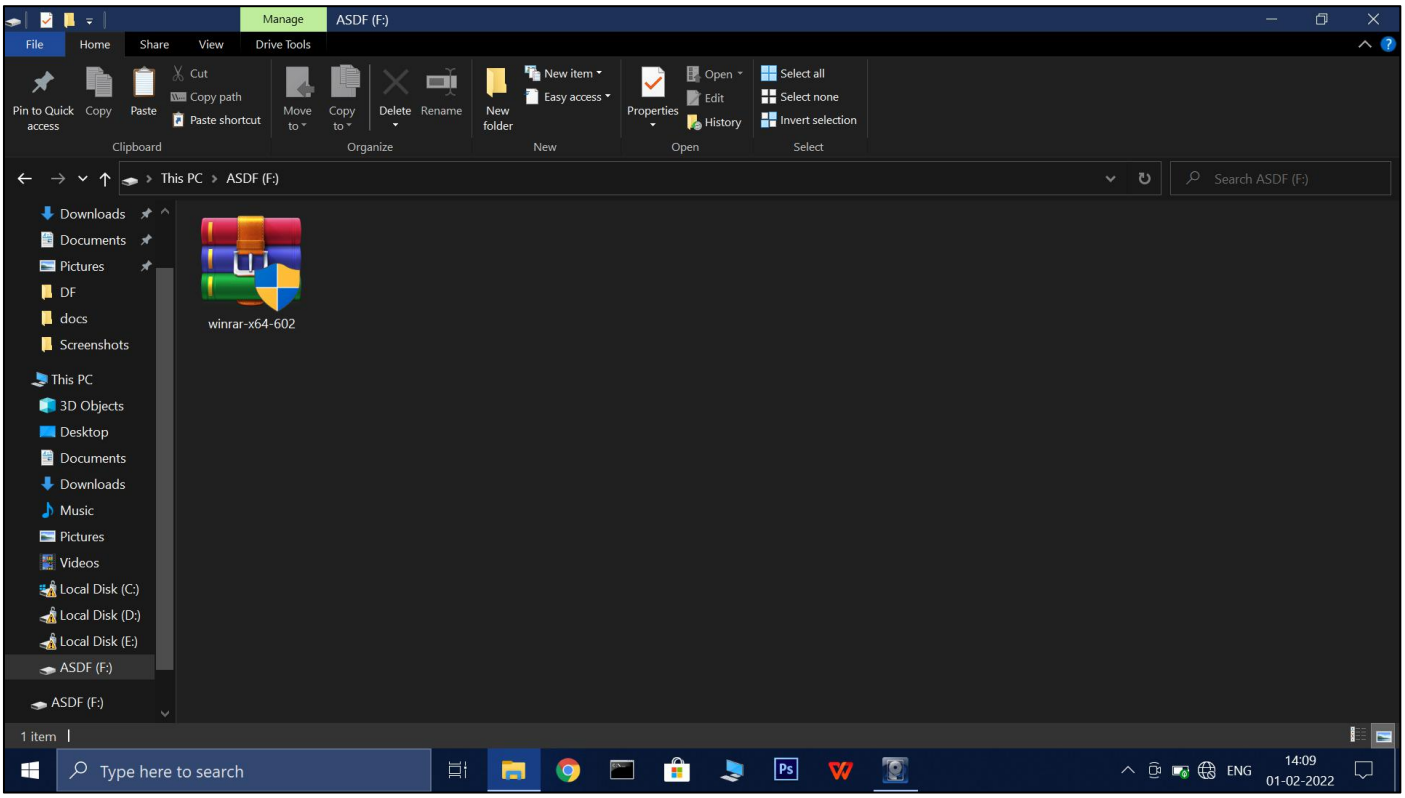
Table of Contents :

Activity 1

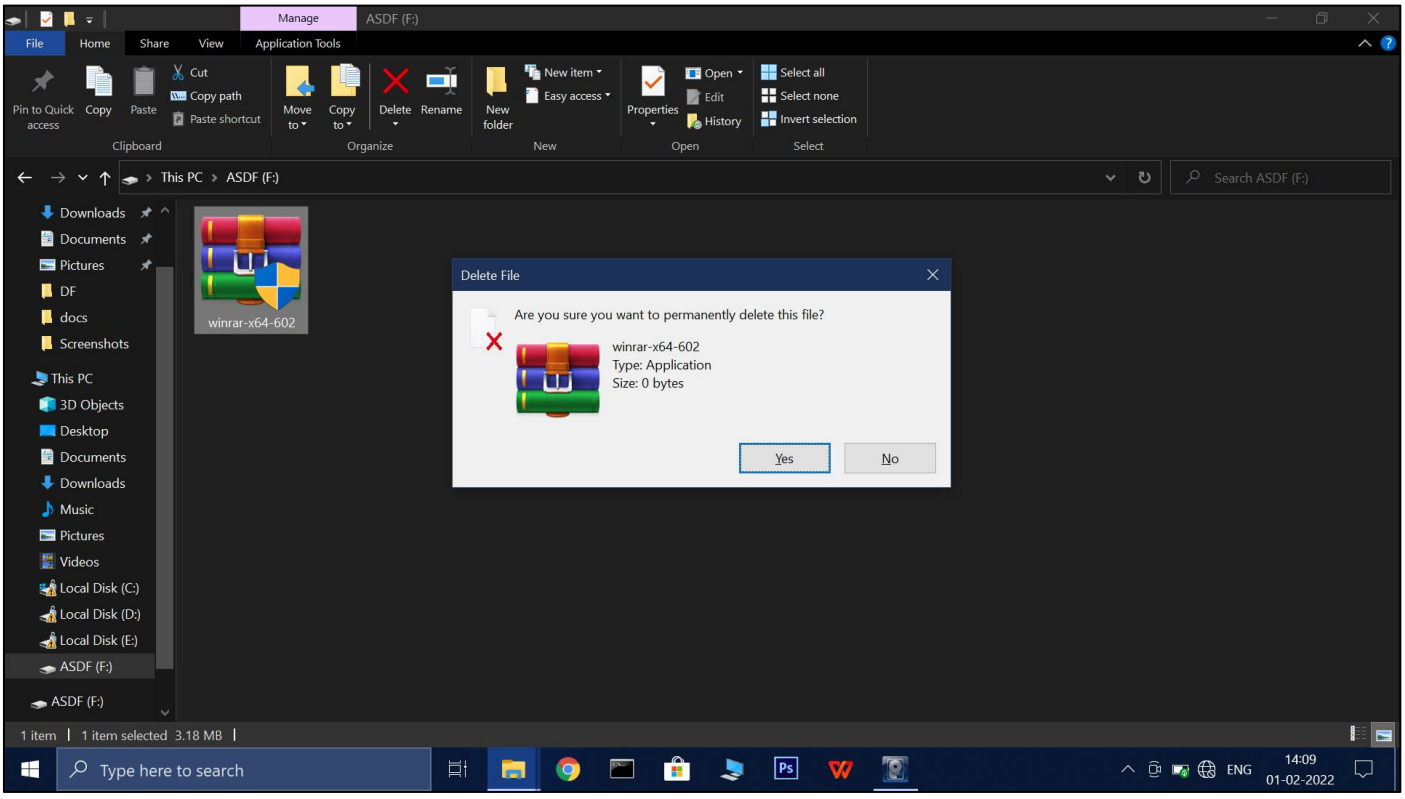
Using FTK Imager , to create a raw (.dd) or Encase (E01) image of the disk .

Part 1: Creating & Deleting of files

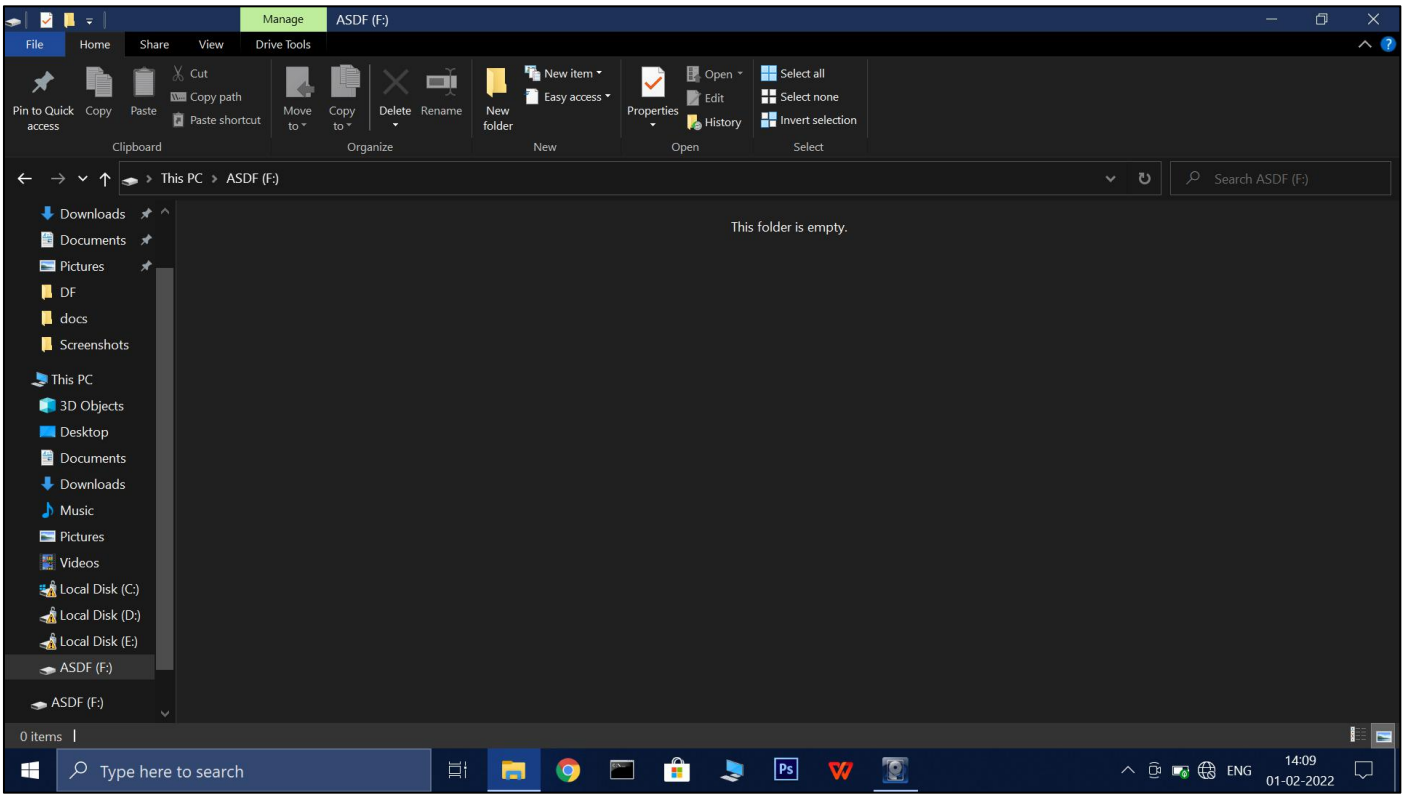
1. Ensure a file is placed in it .



2. Delete the file



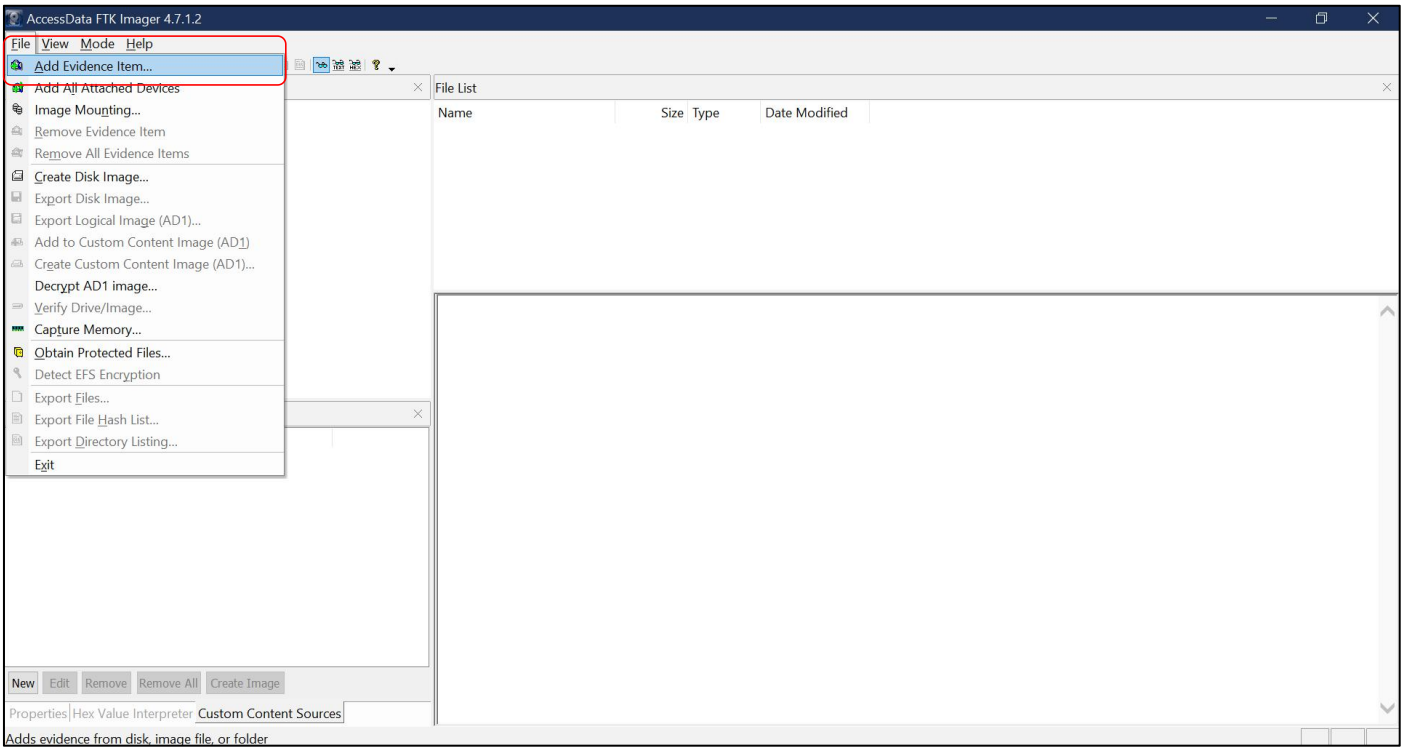
3. Ensure its deleted



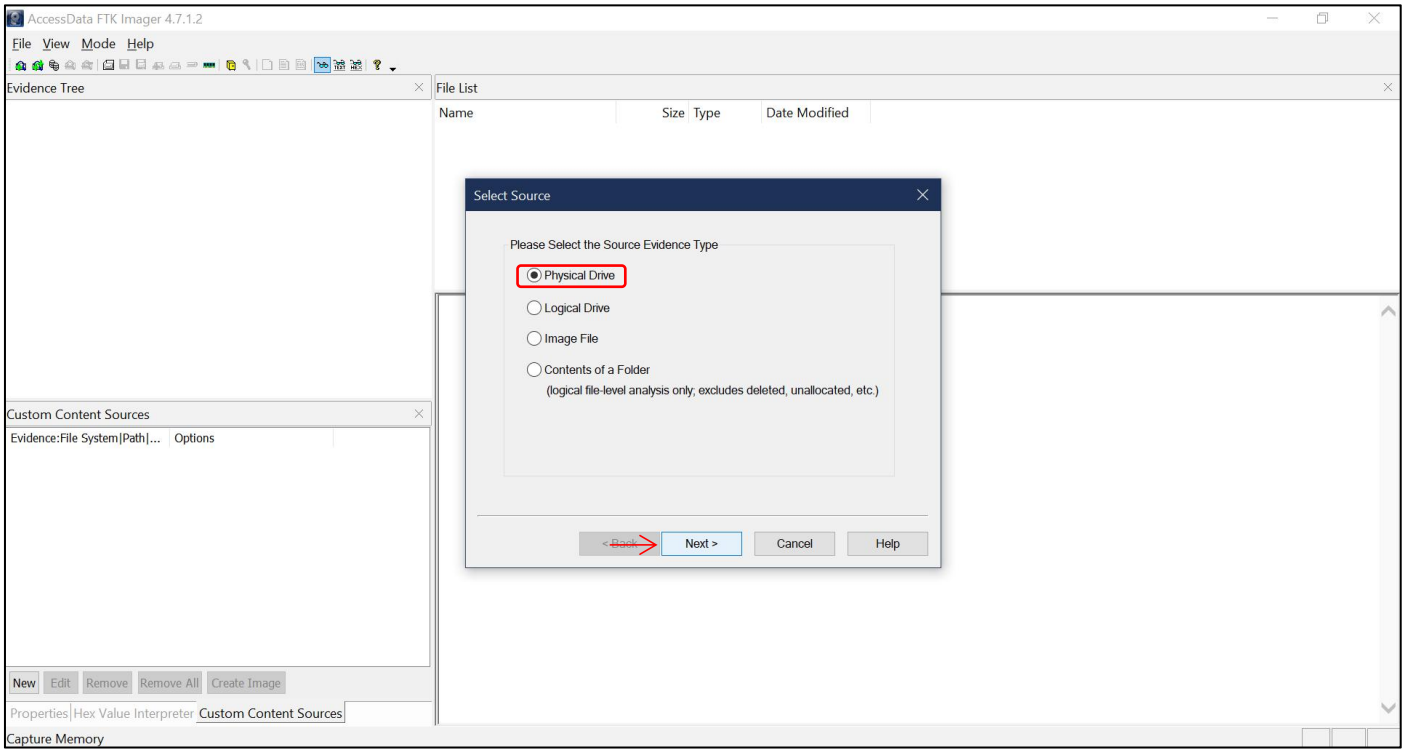
As we can see above that the file is deleted , now we are ready to proceed to next step .

Part 2: Acquiring the Forensic image of the disk

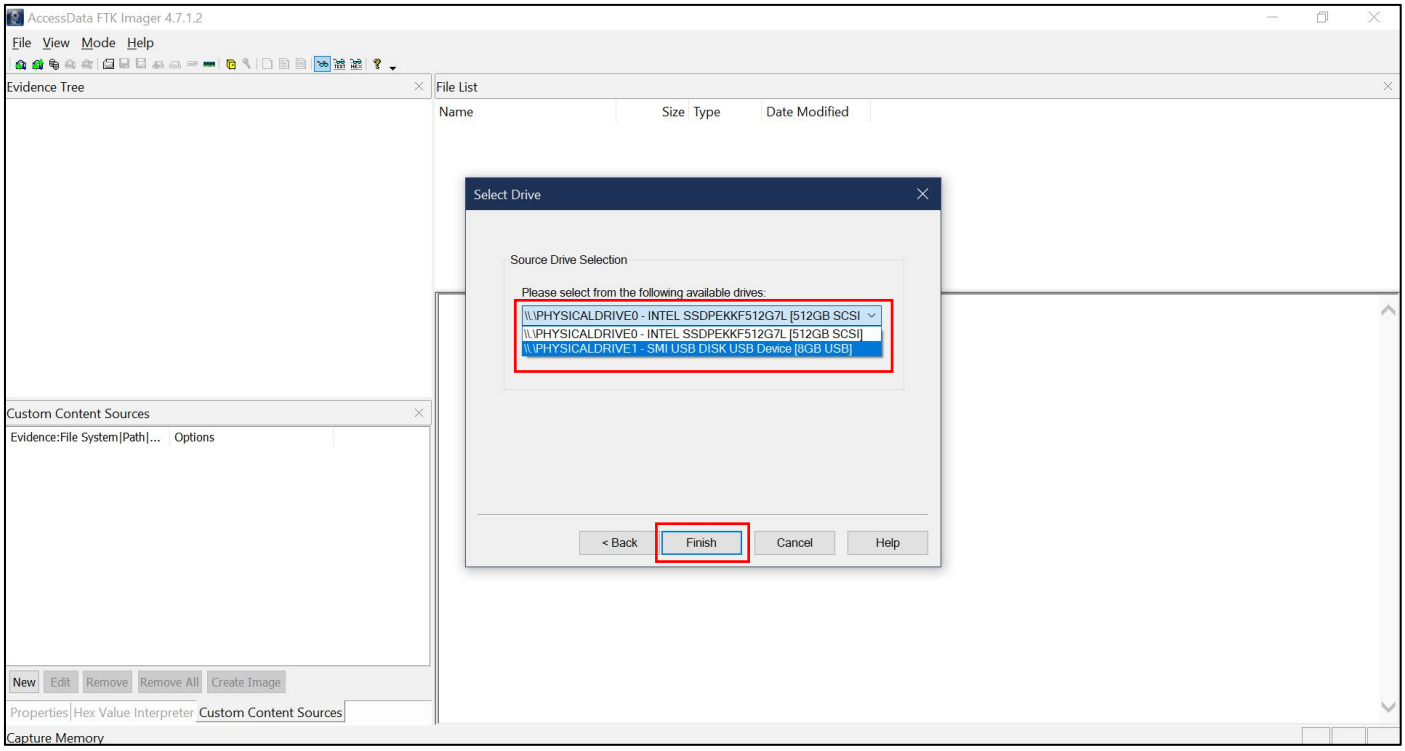
1. Open FTK Imager , then File -> Add Evidence Item



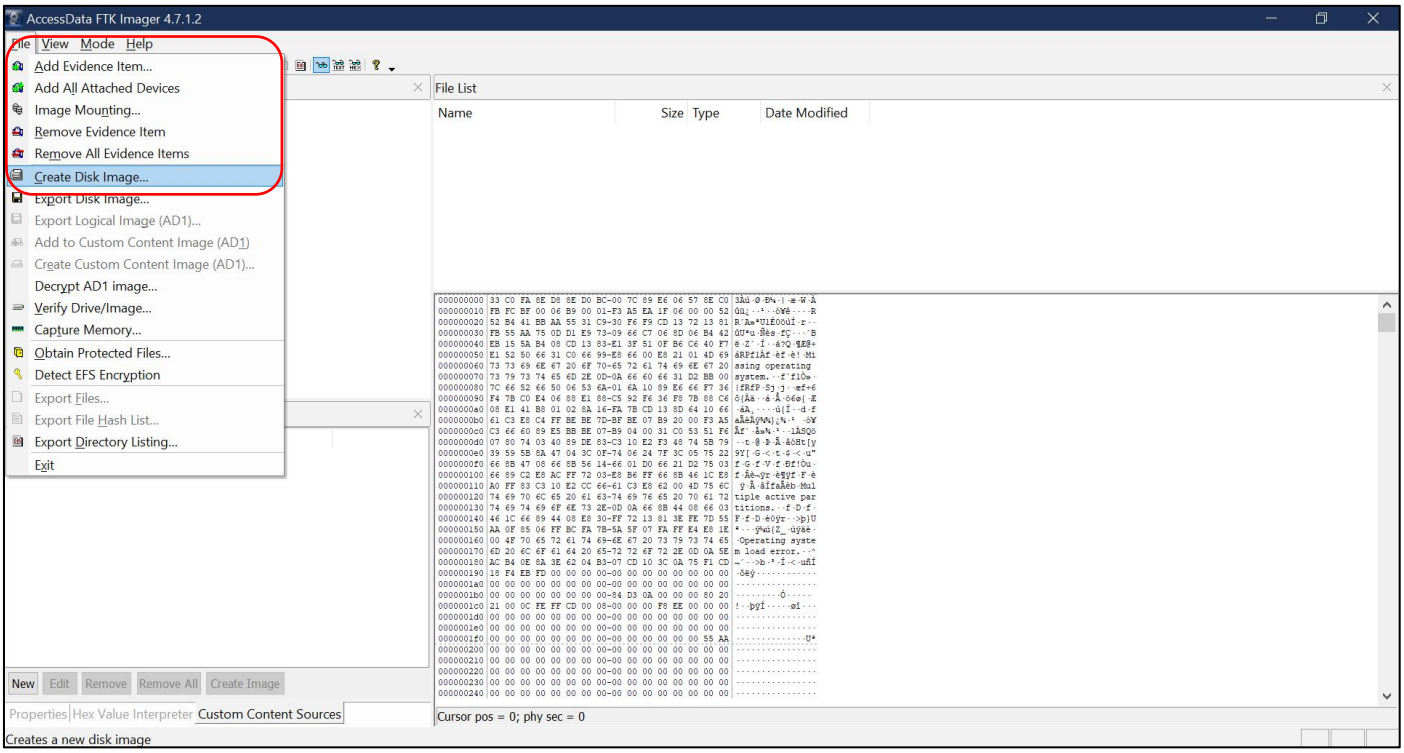
2. Select the type of drive (here its Physical Drive).



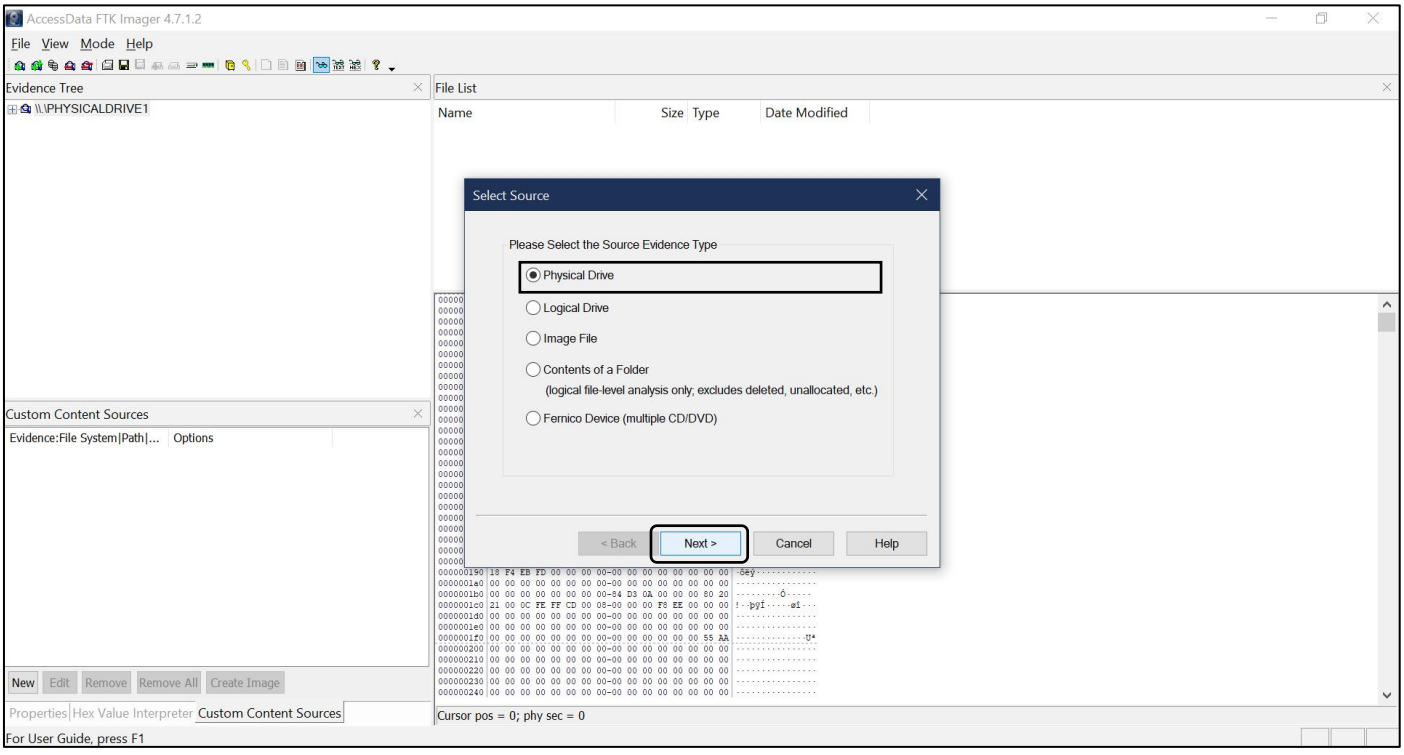
3. Select the drive from te drop down list



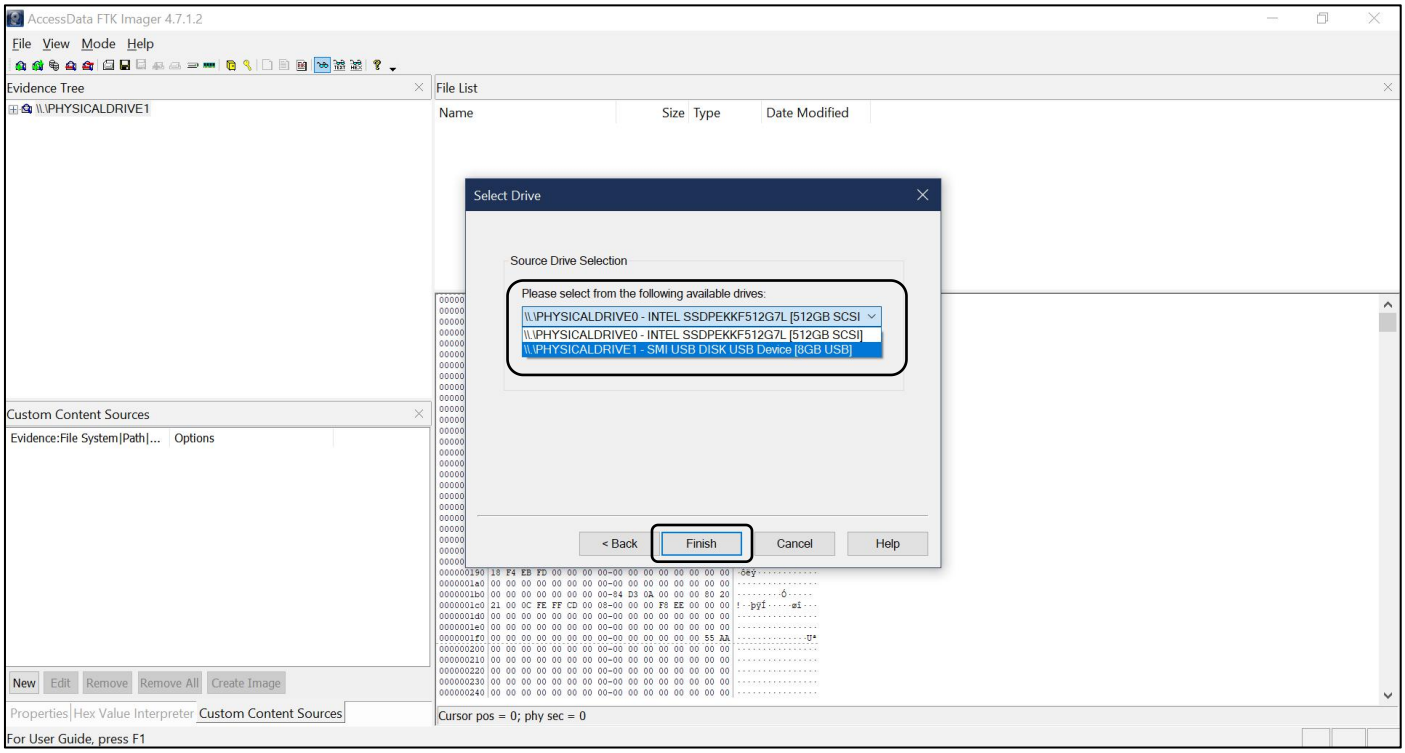
4. To create a disk Image Follow , File -> Disk Image .



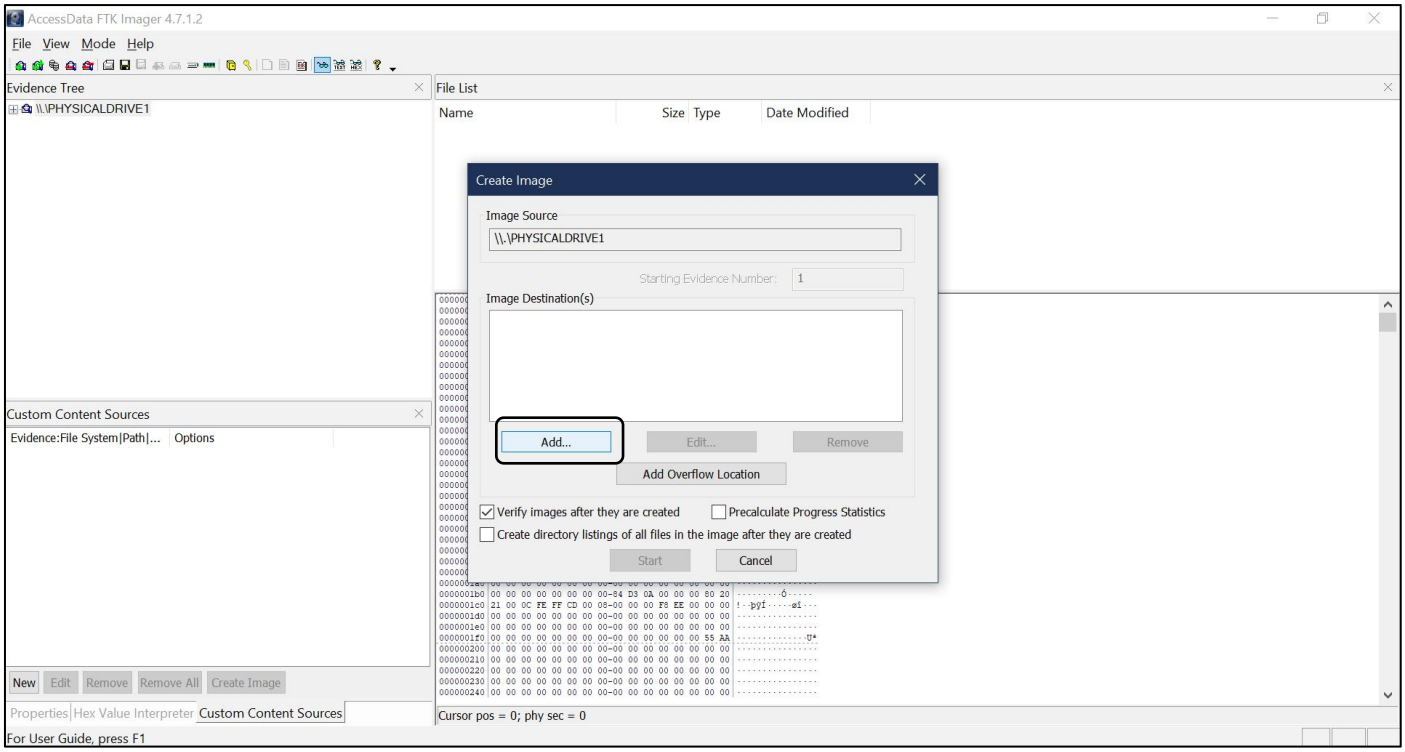
5 . Specify the disk type. (here Physical Drive)

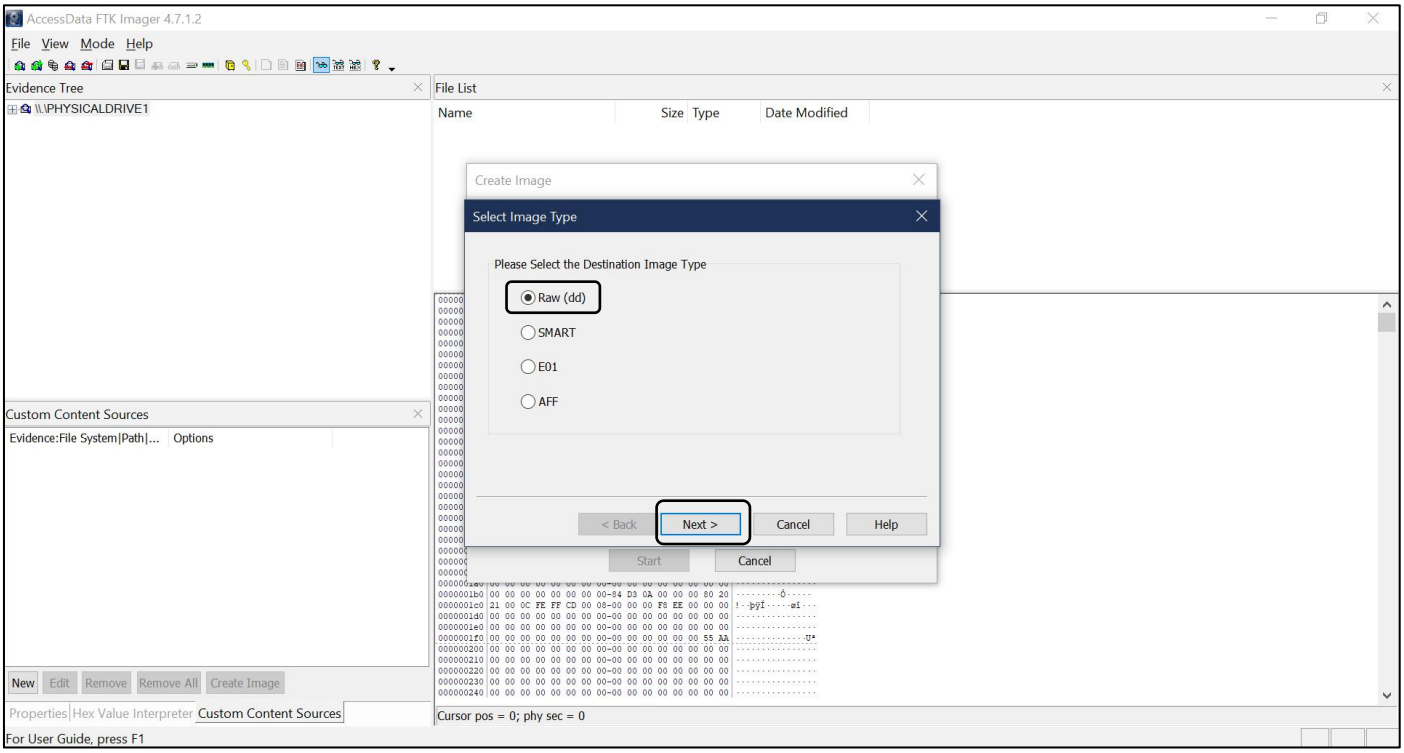


6 . Select the disk to be examined .

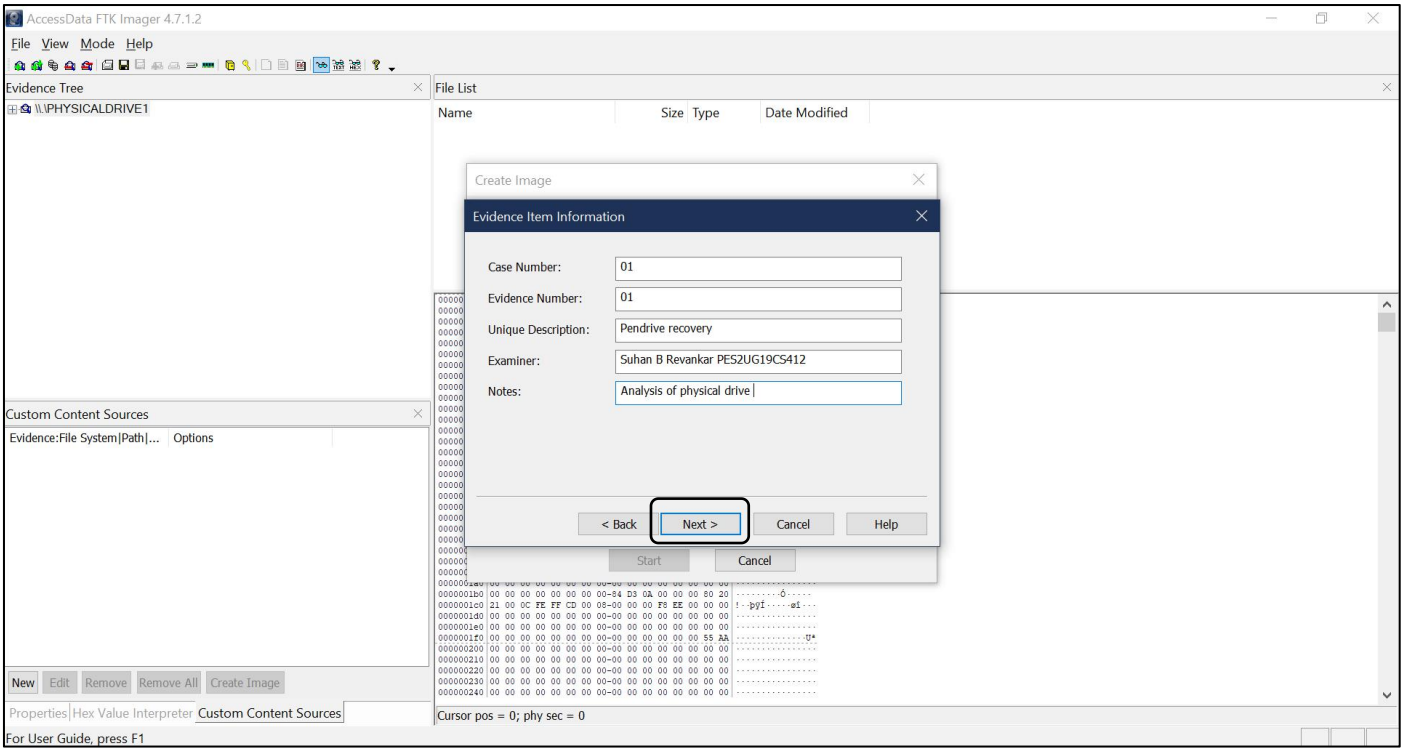


7. Select the target image type (Here Raw)

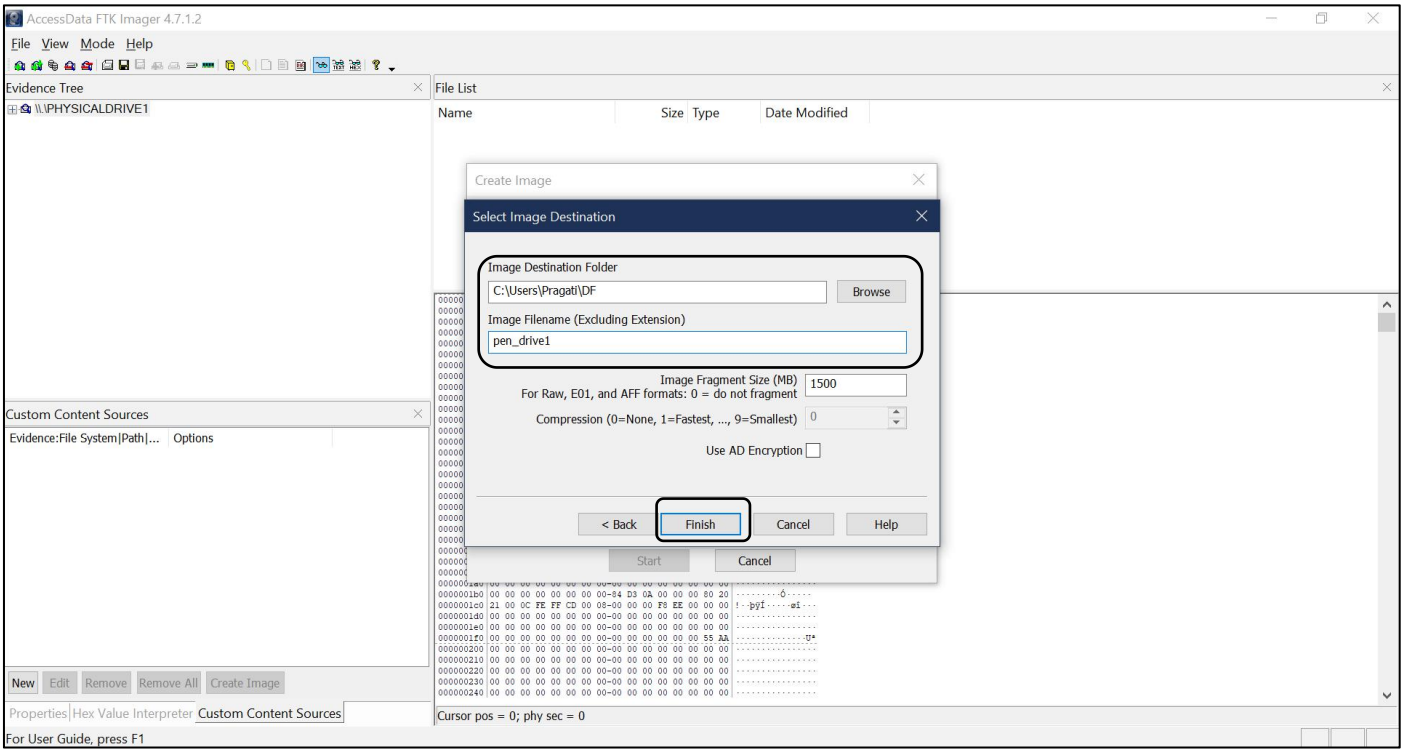




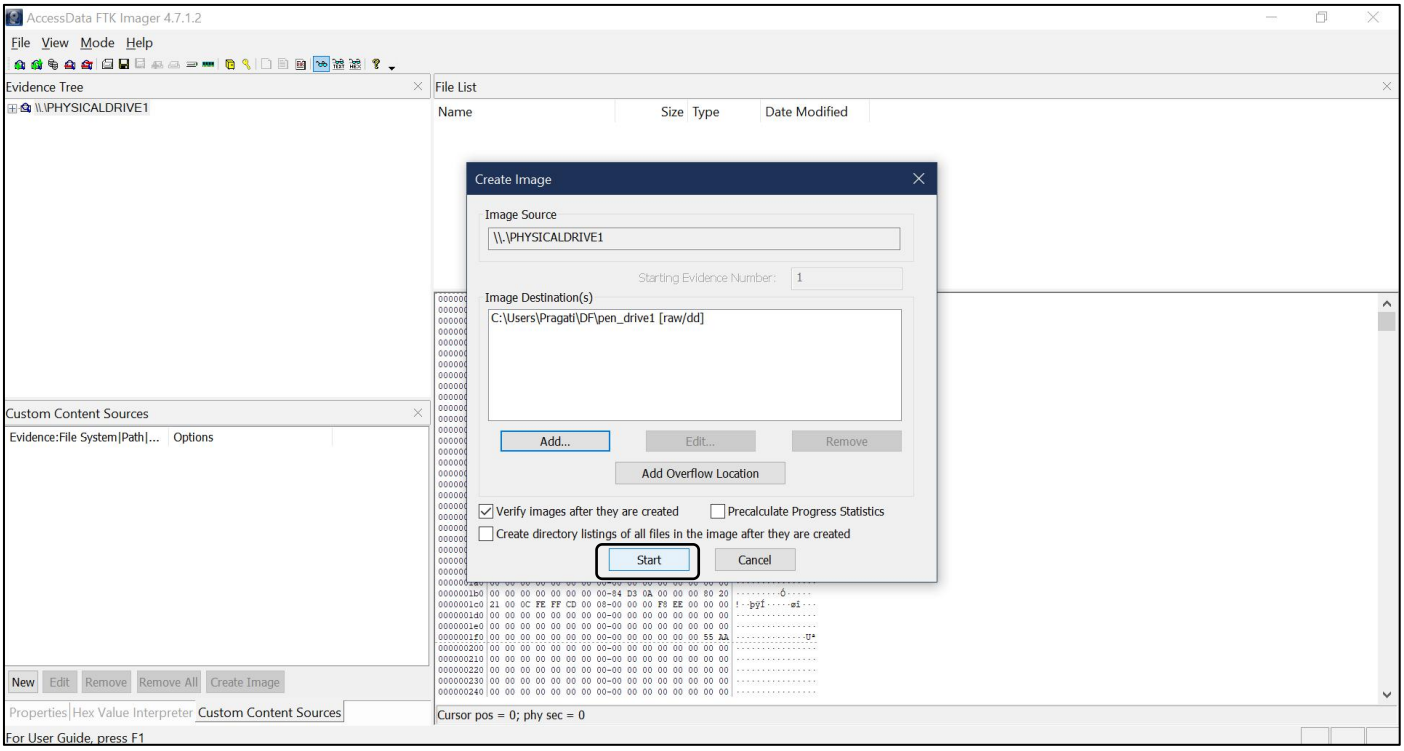
8 . Specify the details as per needs .



9 . Selecting the destination folder

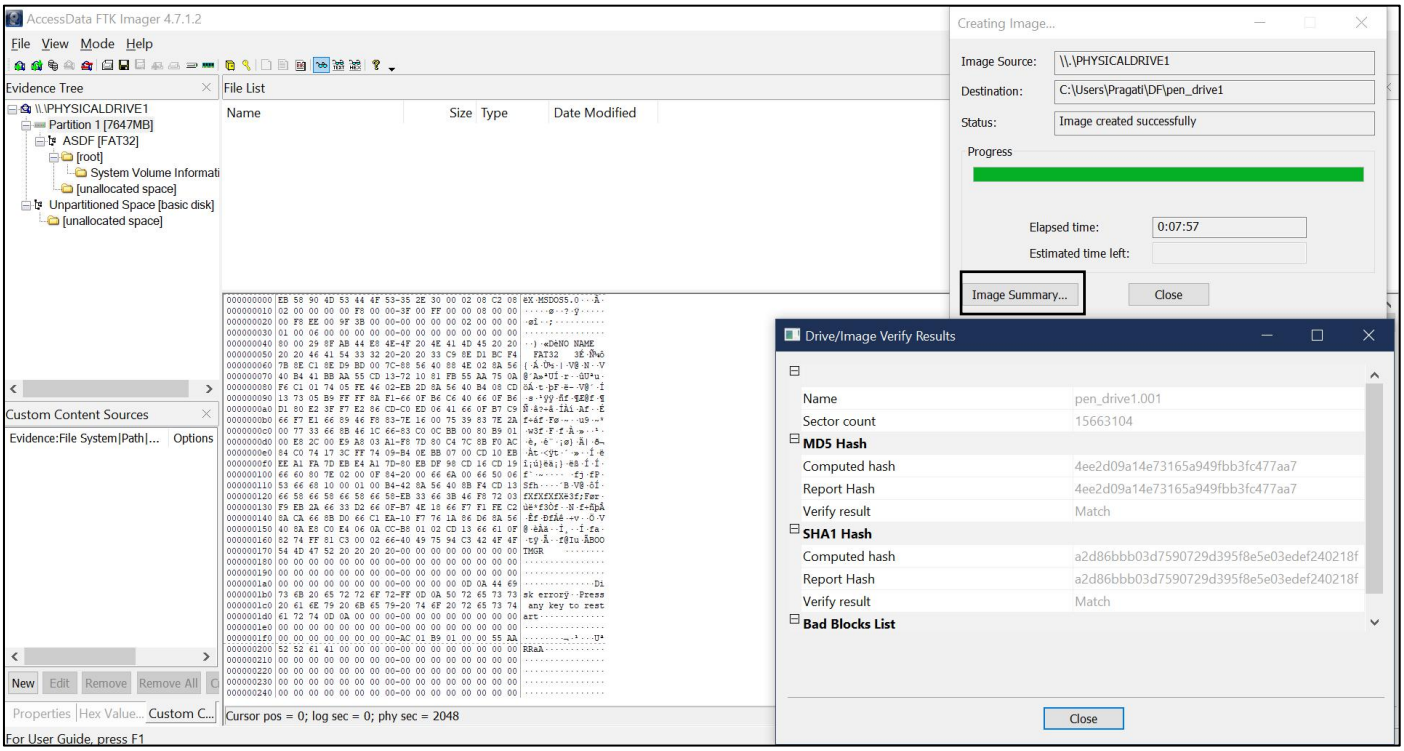


10. The target can be seen in the window click on “Start”

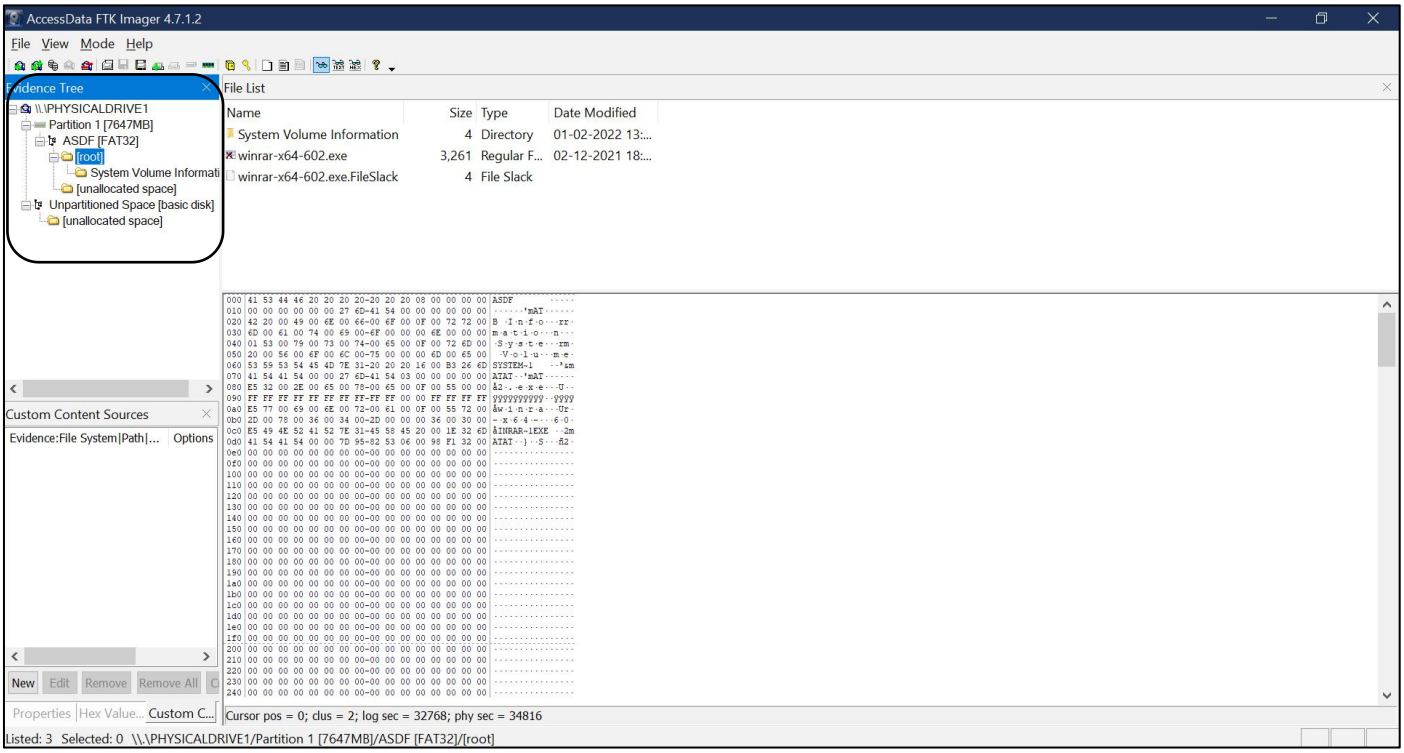


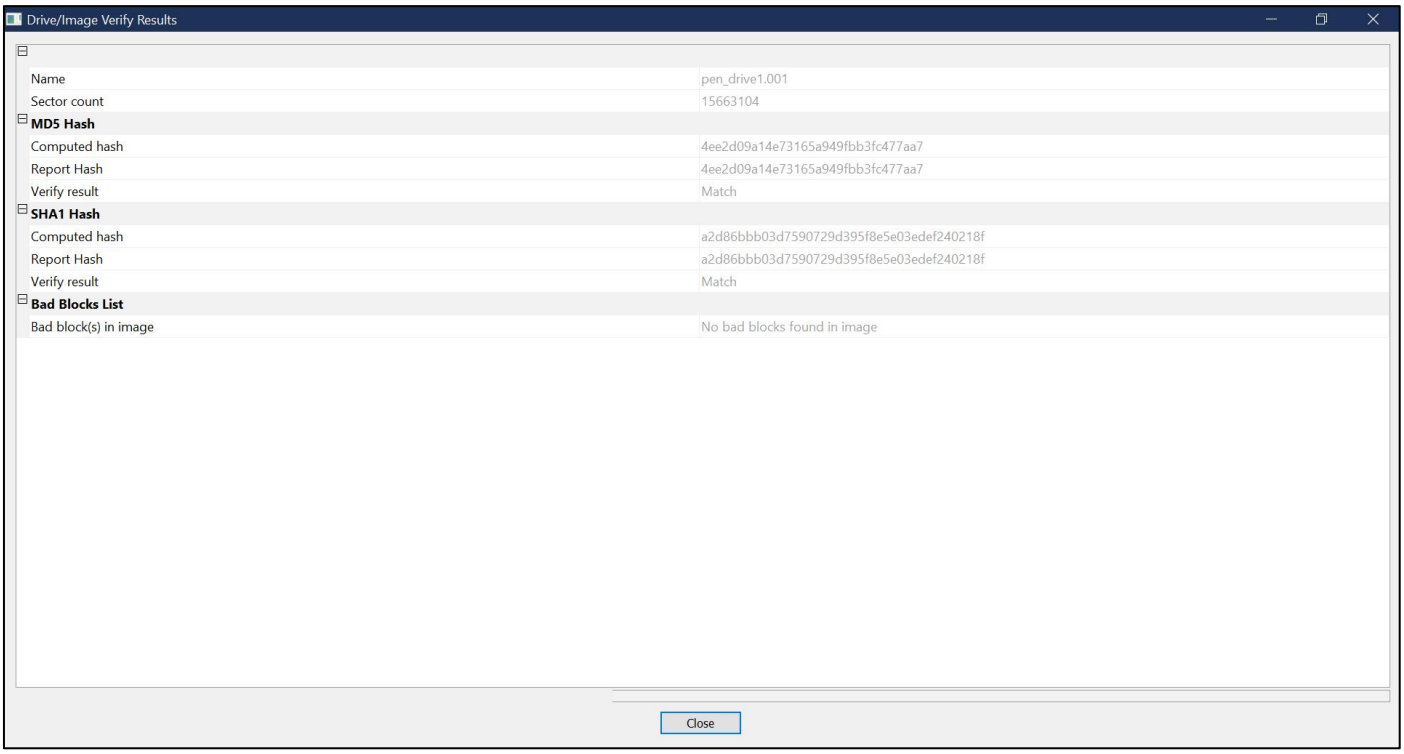
Part 3: Examining the details

1. Following are the results obtained

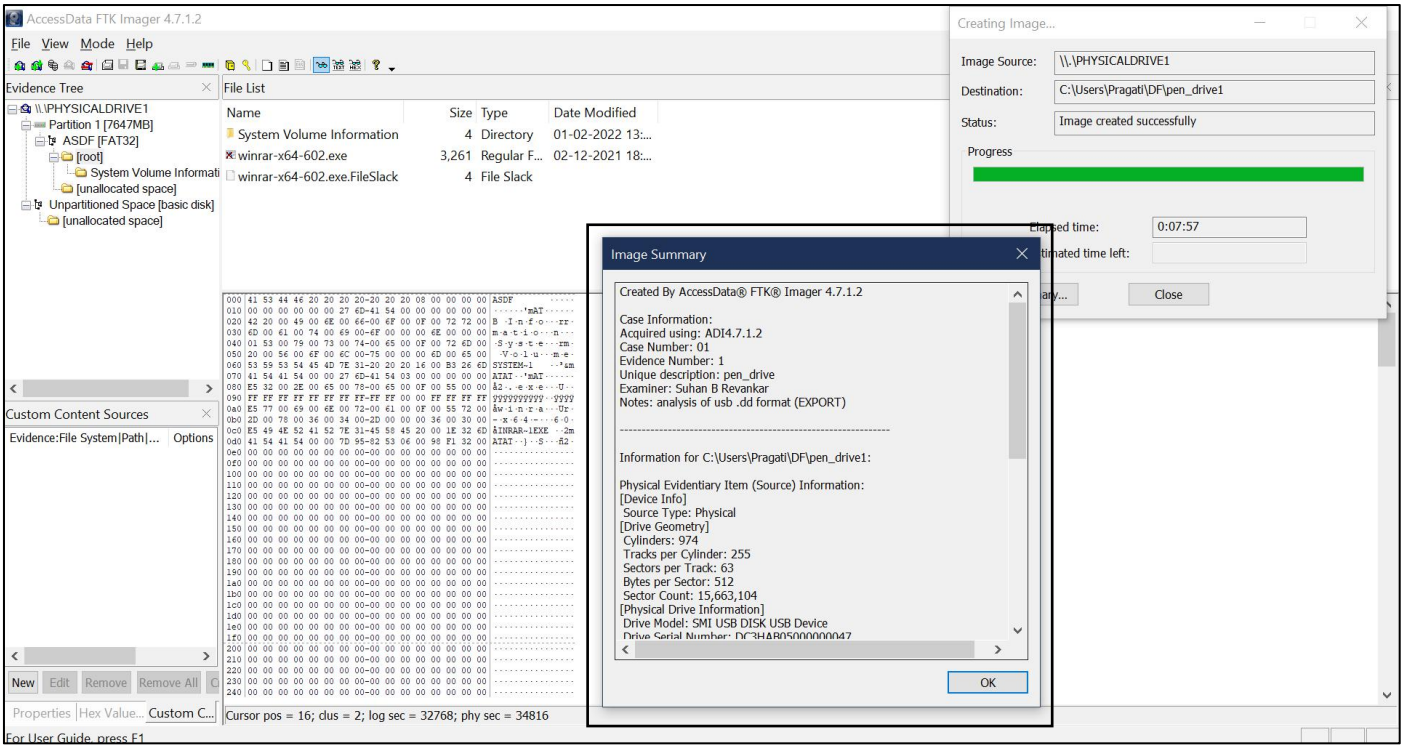


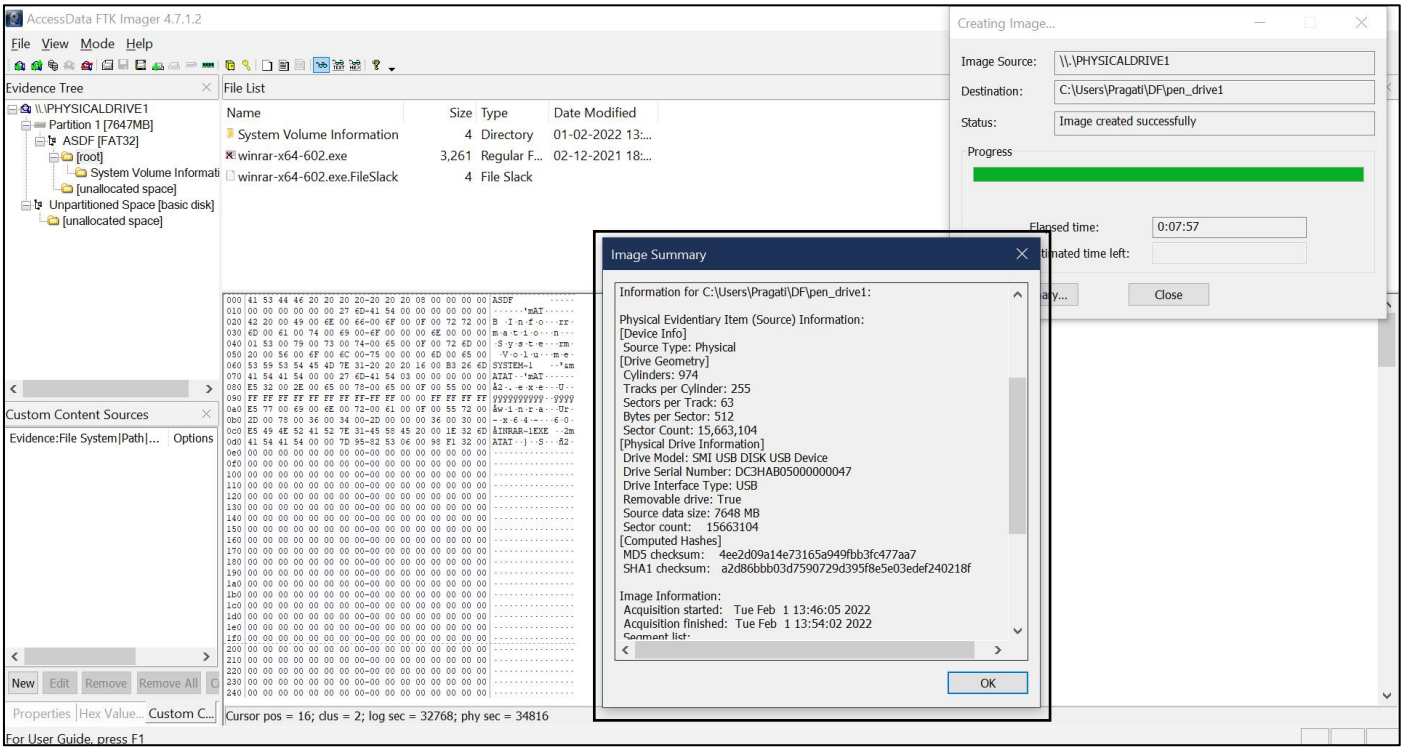
2. Evidence Tree : showing the directories , files , folders present before deletion .

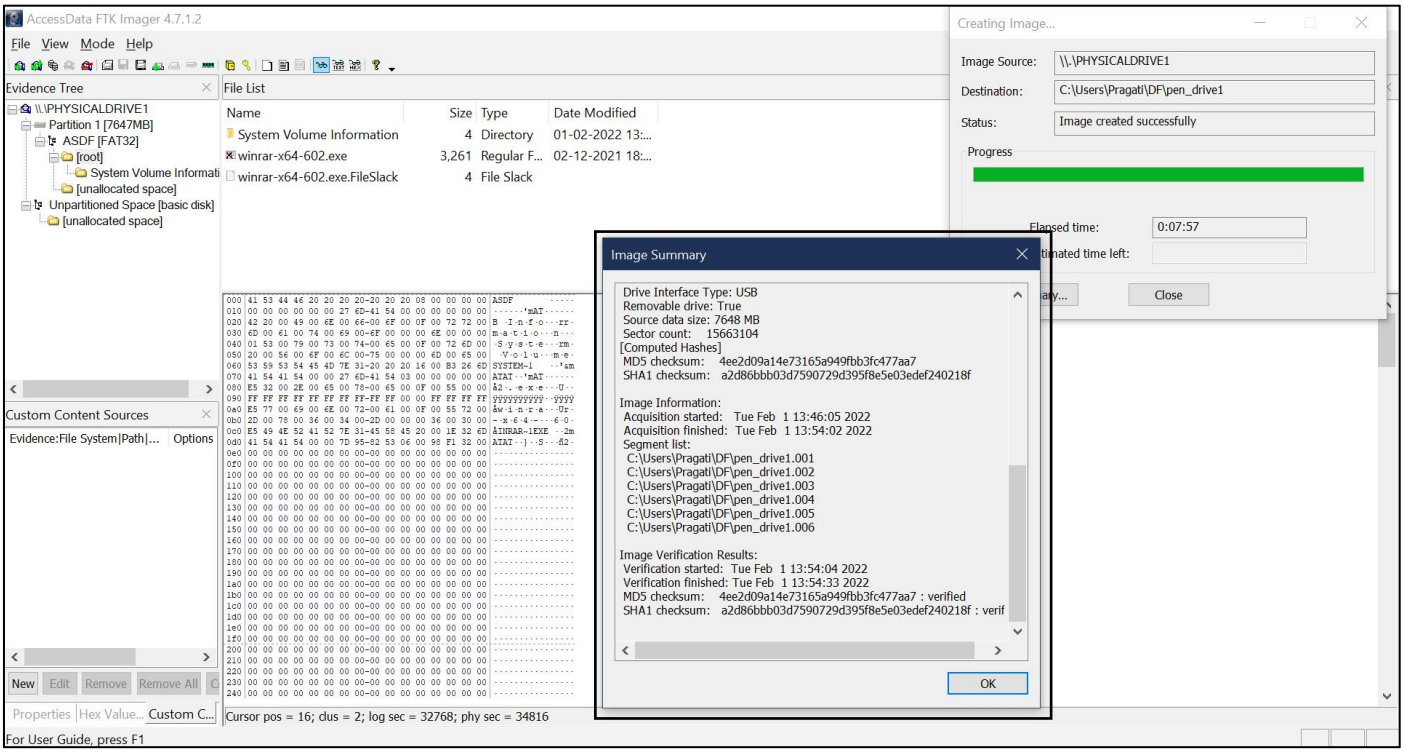




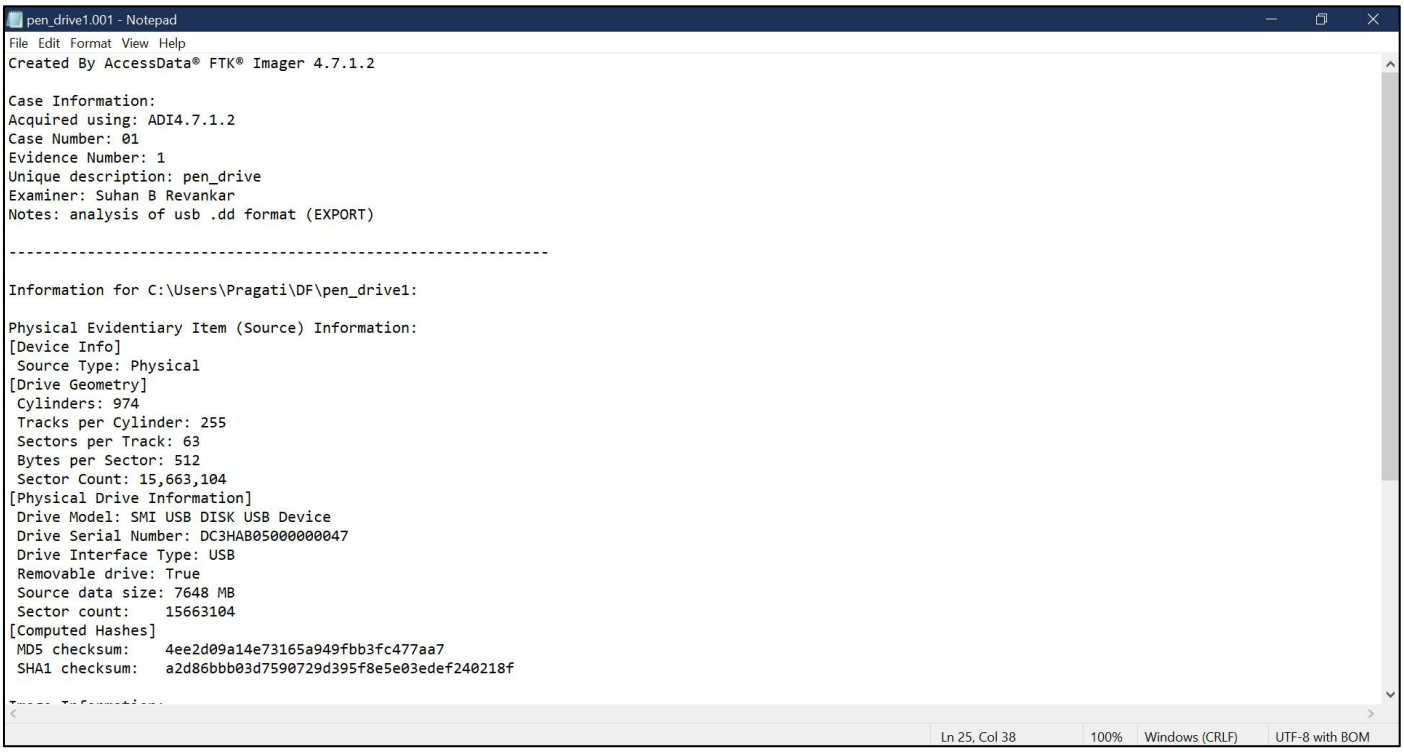
3. Image summary (also can be found in text format in the destination folder specified)

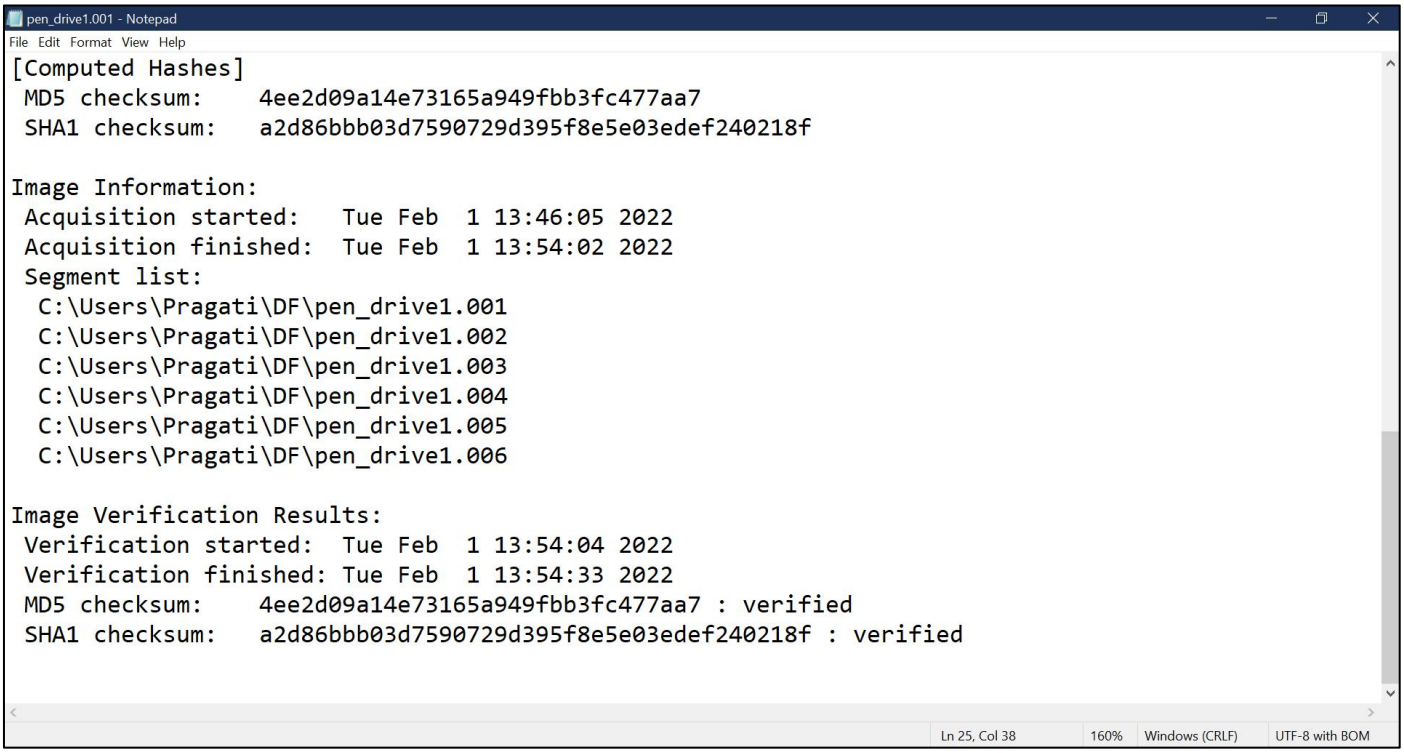




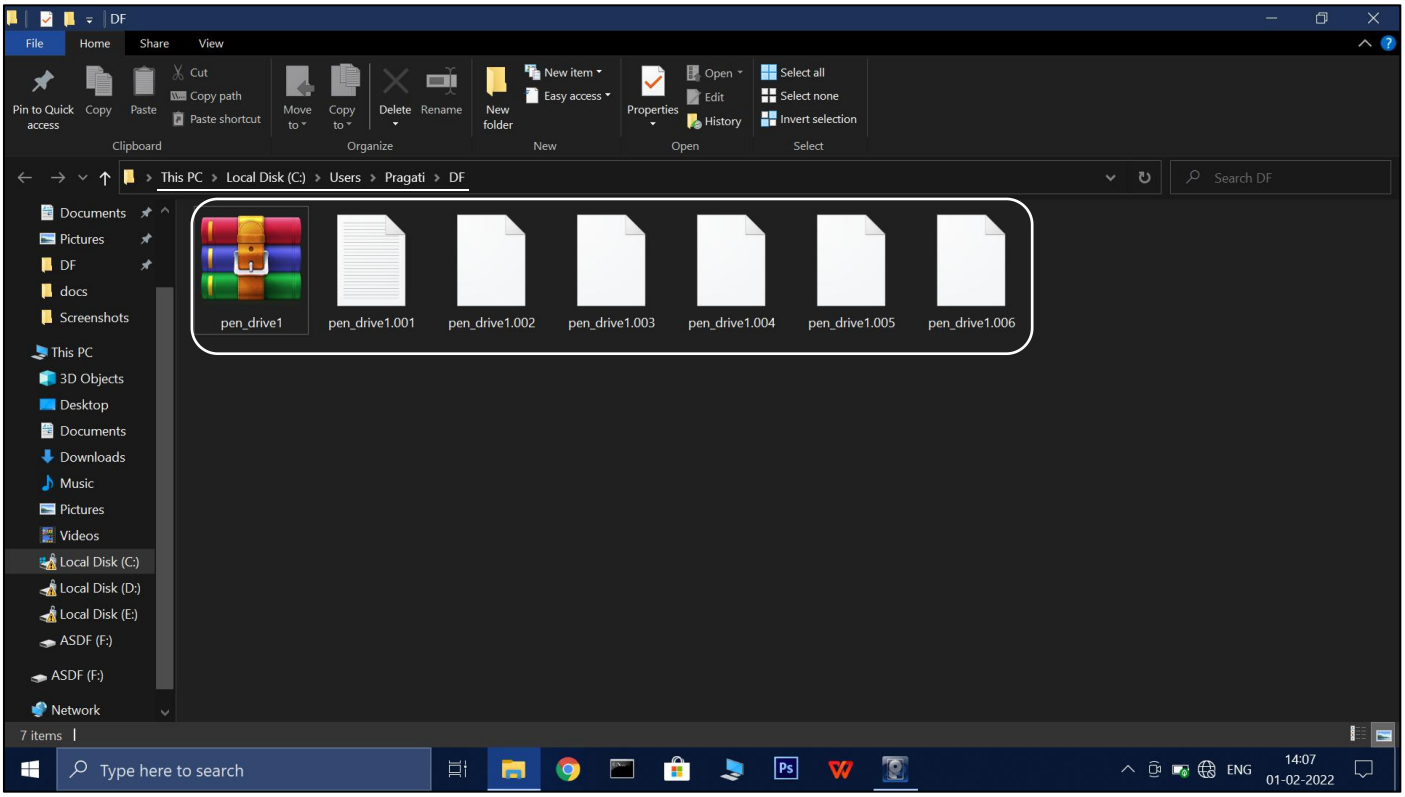


4. Image summary in .txt format

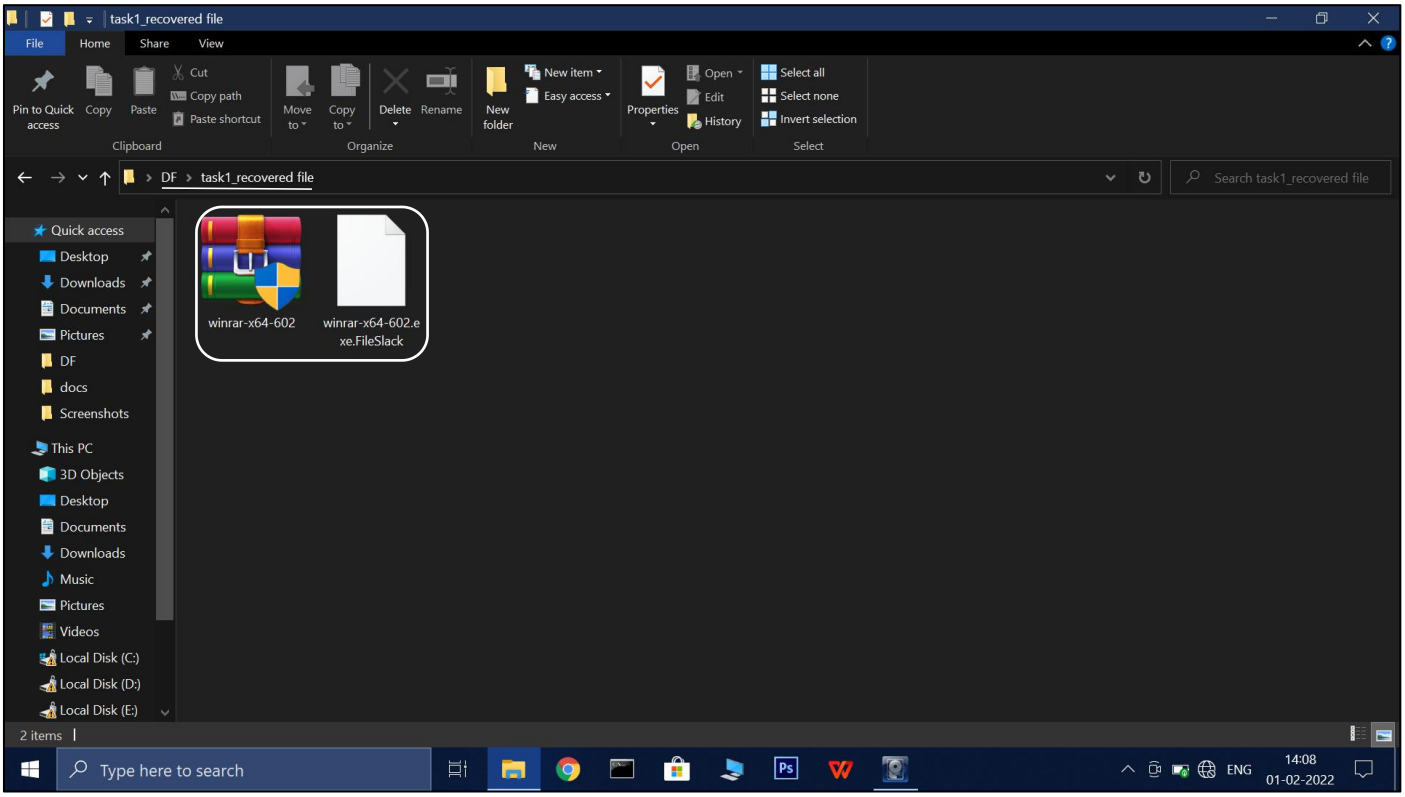




5. The analyze images can be exported for further analysis in different tools .
(can be found in the target folder)



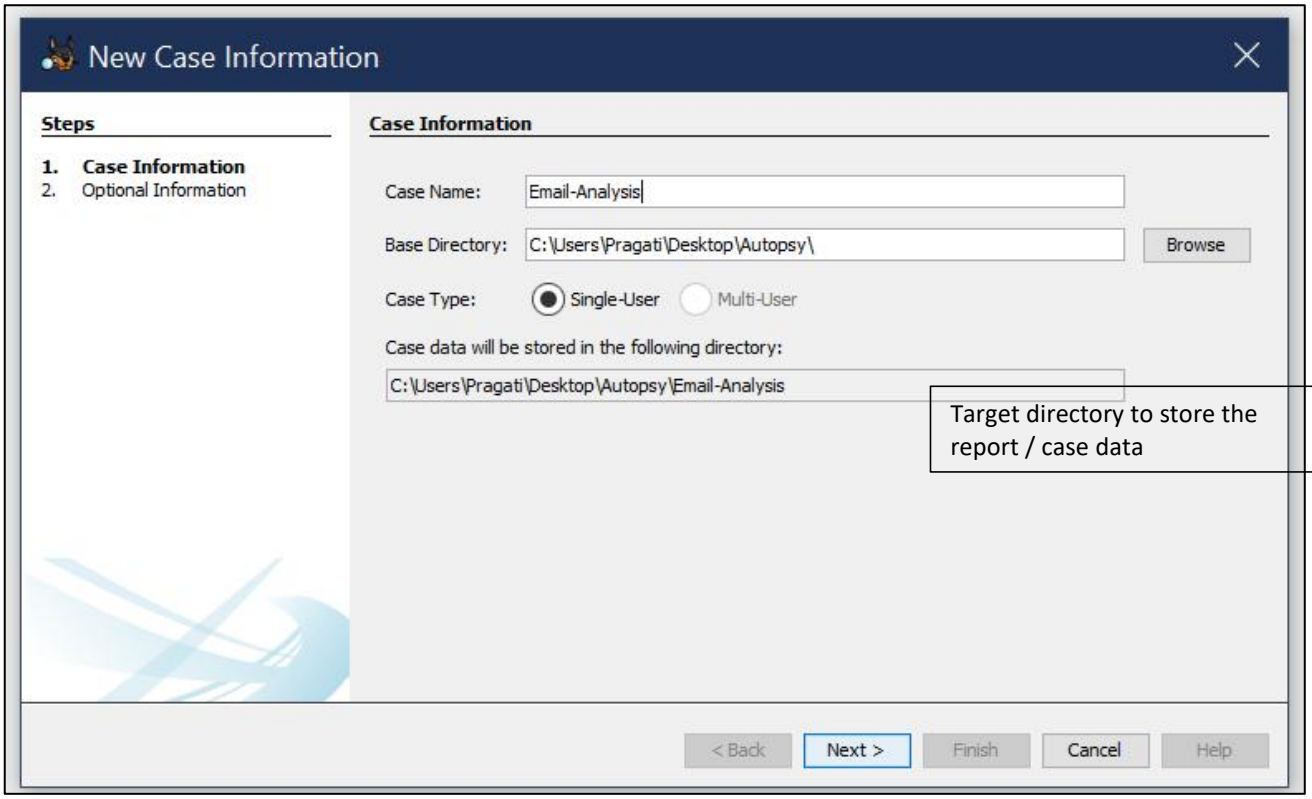
6 . At times if possible the deleted files and folders can be recovered .

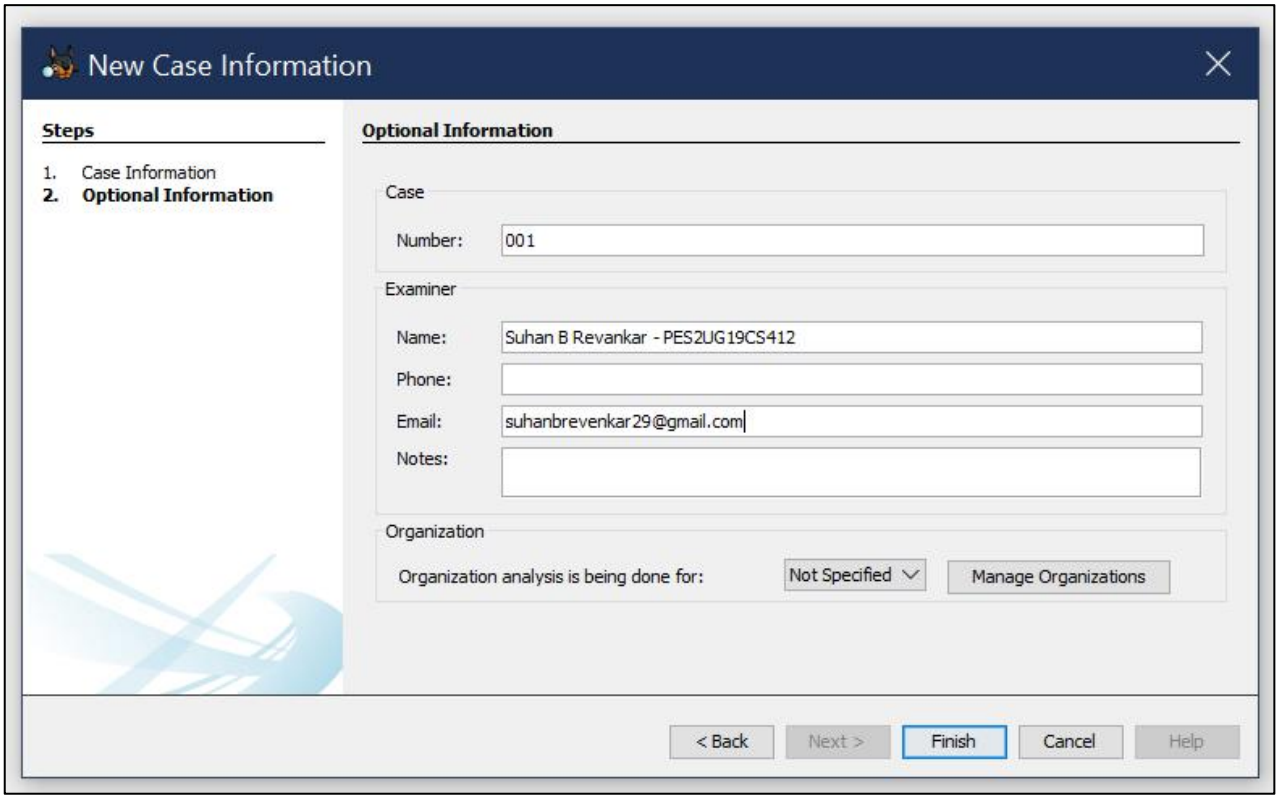


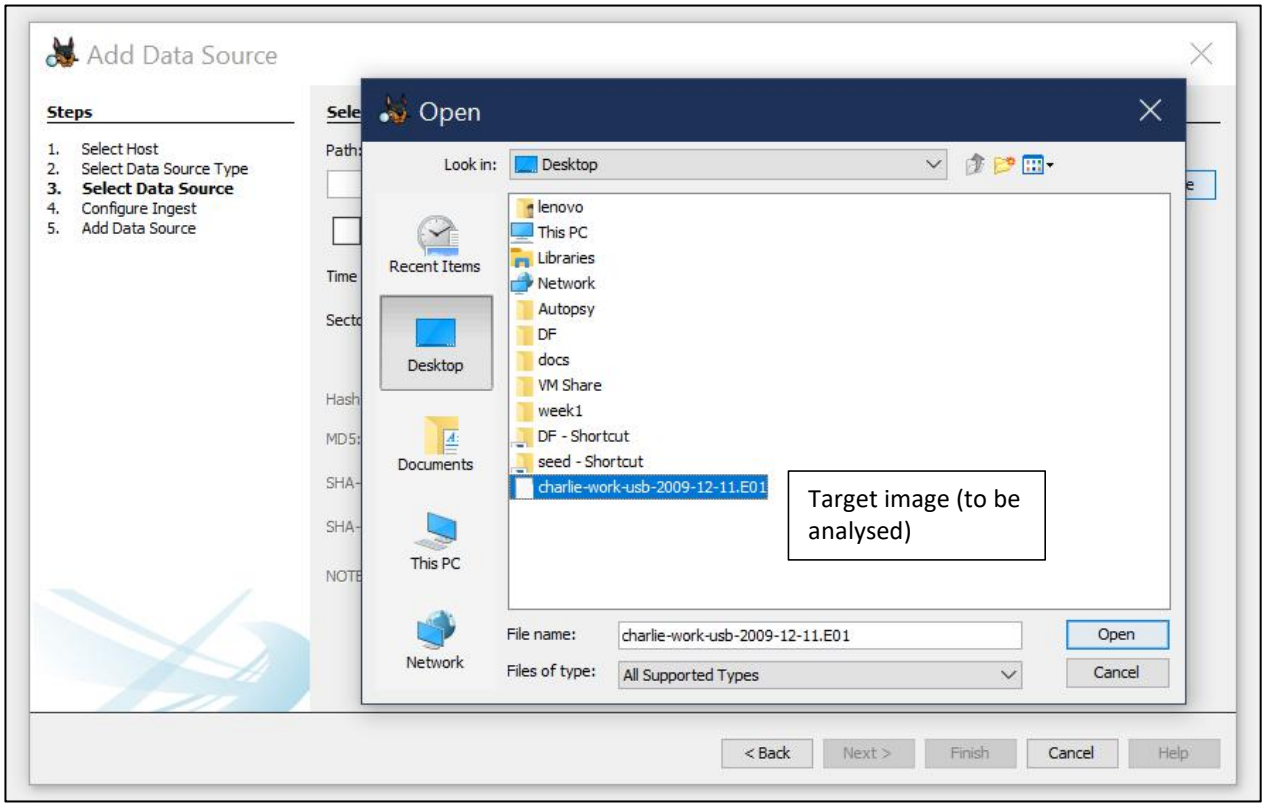
Activity 2

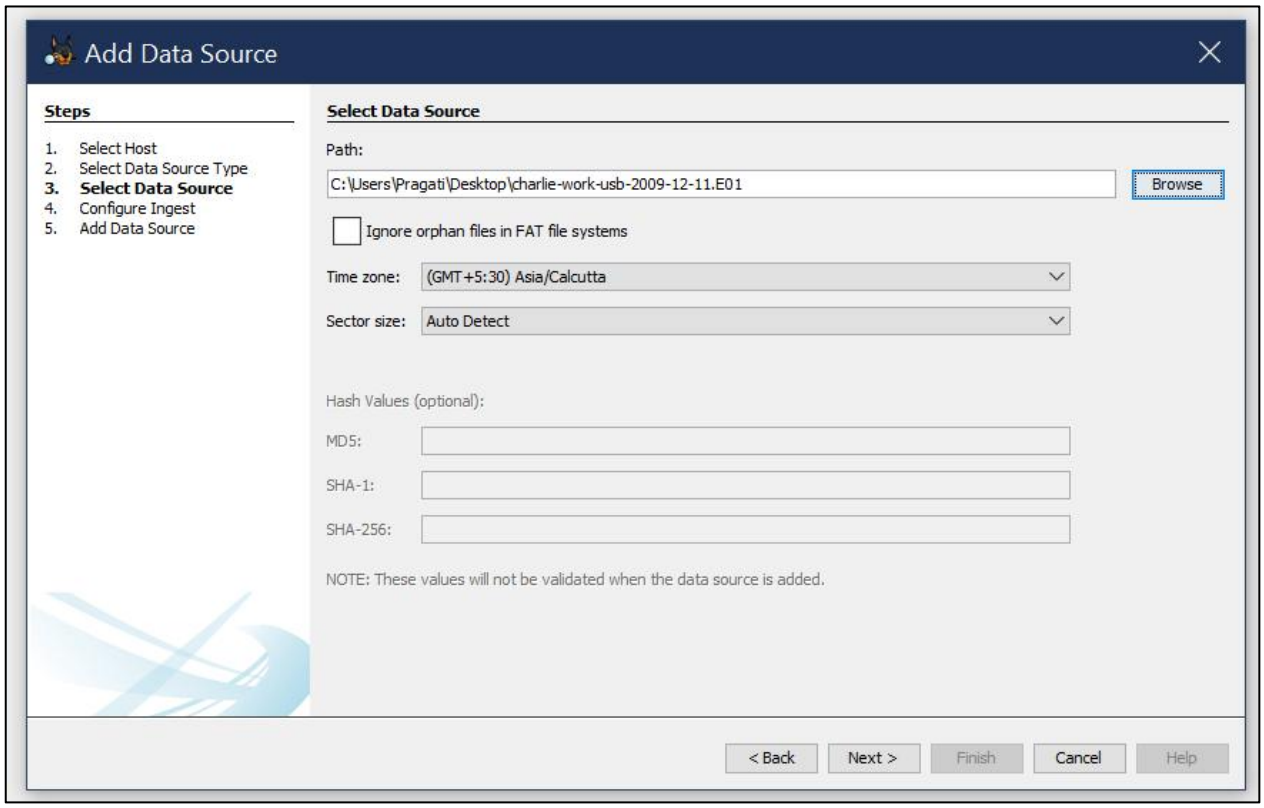
Using Autopsy tool , to analyse the Forensic images that were generated . To form a well detailed report .

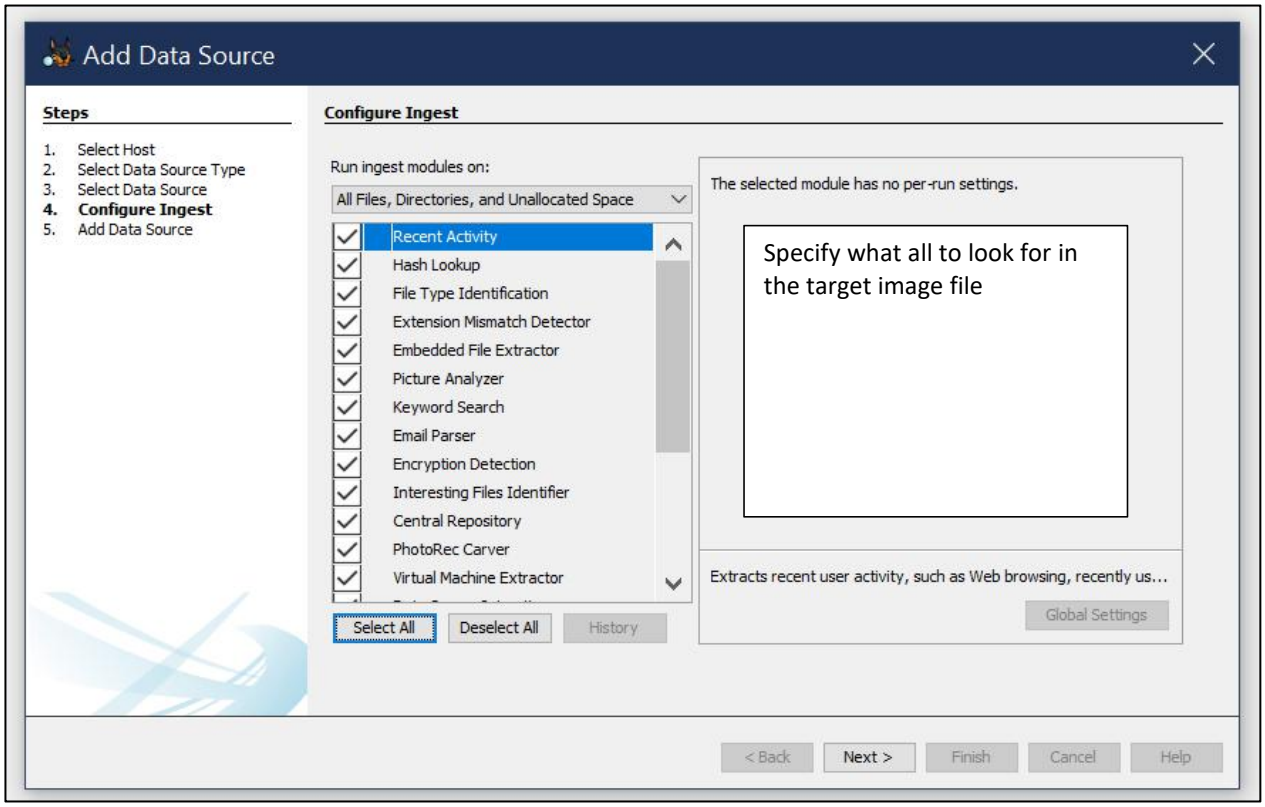
Part 1: Loading of Images

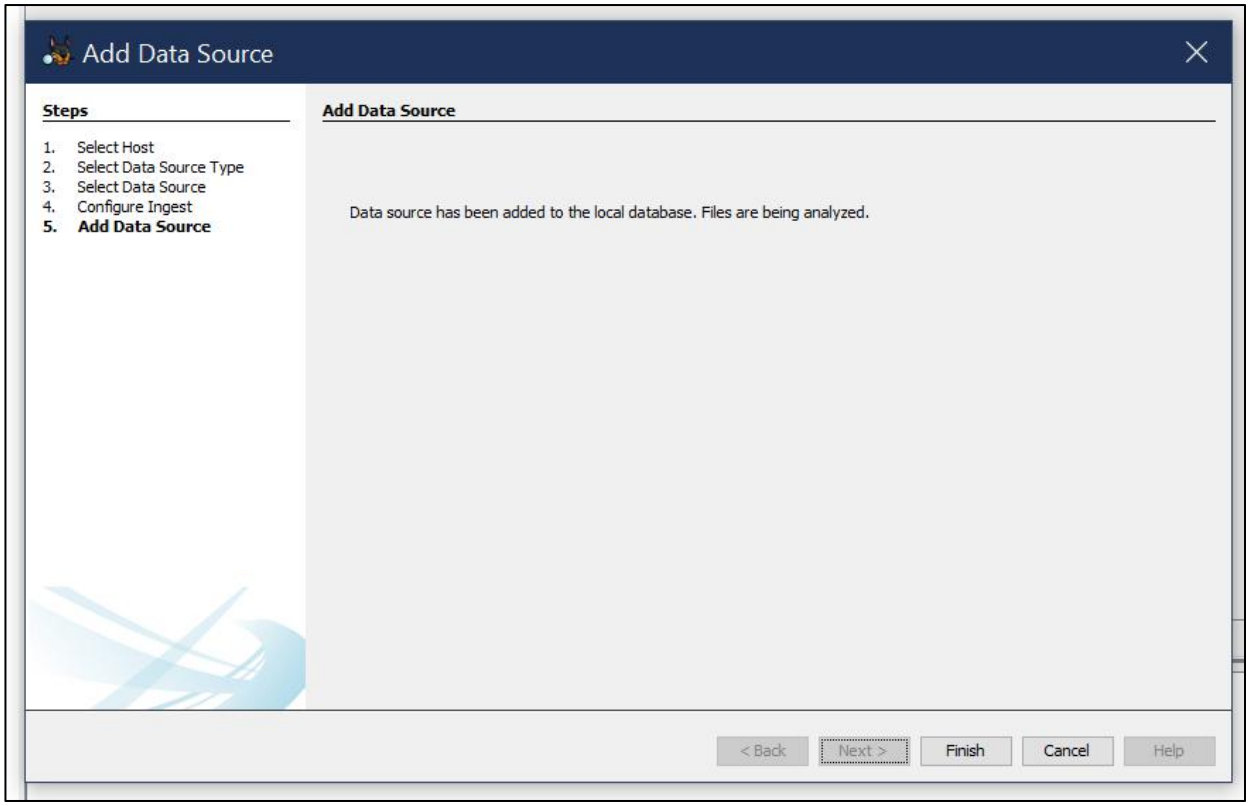




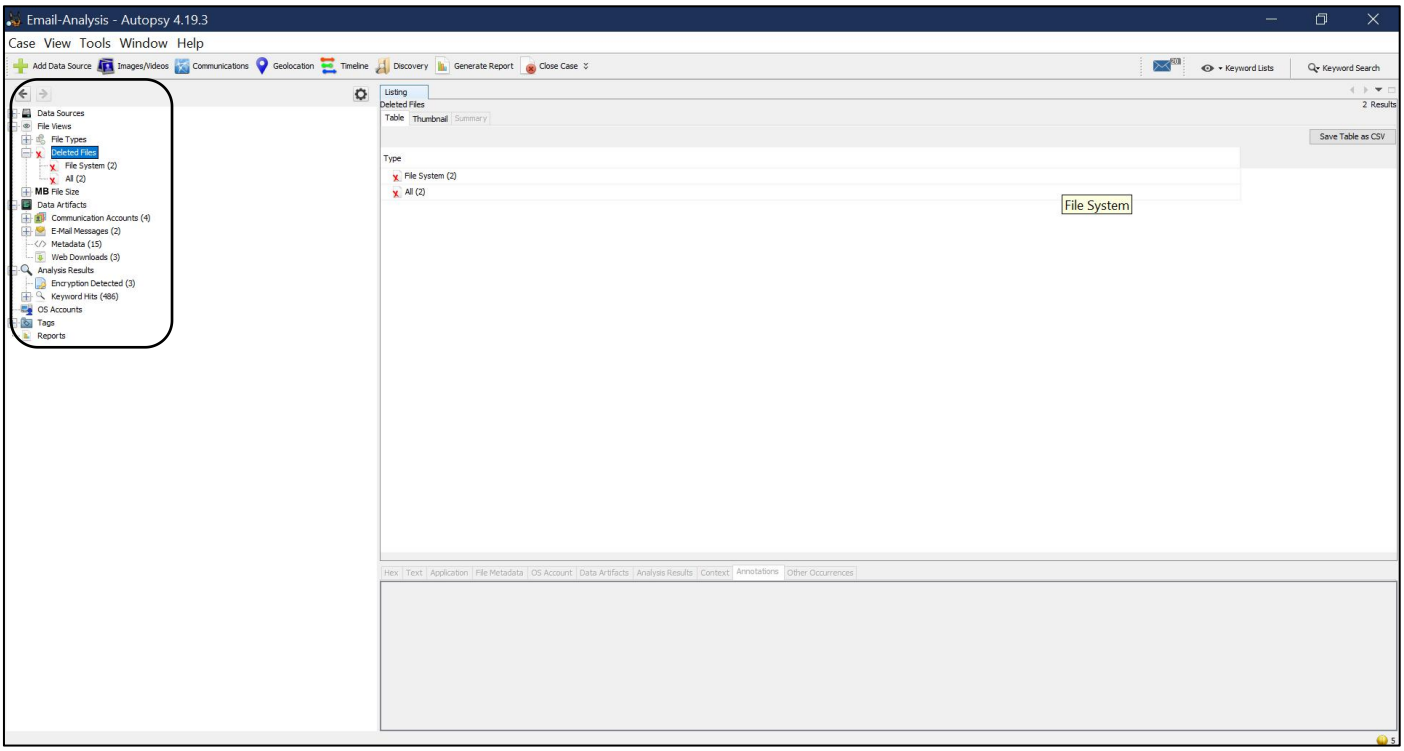

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Open
Look in: Desktop
Recent Items
Desktop
Documents
This PC
Network
lenovo
This PC
Libraries
Network
Autopsy
DF
docs
VM Share
week1
DF - Shortcut
seed - Shortcut
charlie-work-usb-2009-12-11.E01
Target image (to be analysed)
File name: charlie-work-usb-2009-12-11.E01
Files of type: All Supported Types
Open
Cancel
< Back
Next >
Finish
Cancel
Help


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source
Path:
C:\Users\Pragati\Desktop\charlie-work-usb-2009-12-11.E01
Browse
Ignore orphan files in FAT file systems
Time zone: (GMT+5:30) Asia/Calcutta
Sector size: Auto Detect
Hash Values (optional):
MD5:
SHA-1:
SHA-256:
NOTE: These values will not be validated when the data source is added.
< Back
Next >
Finish
Cancel
Help

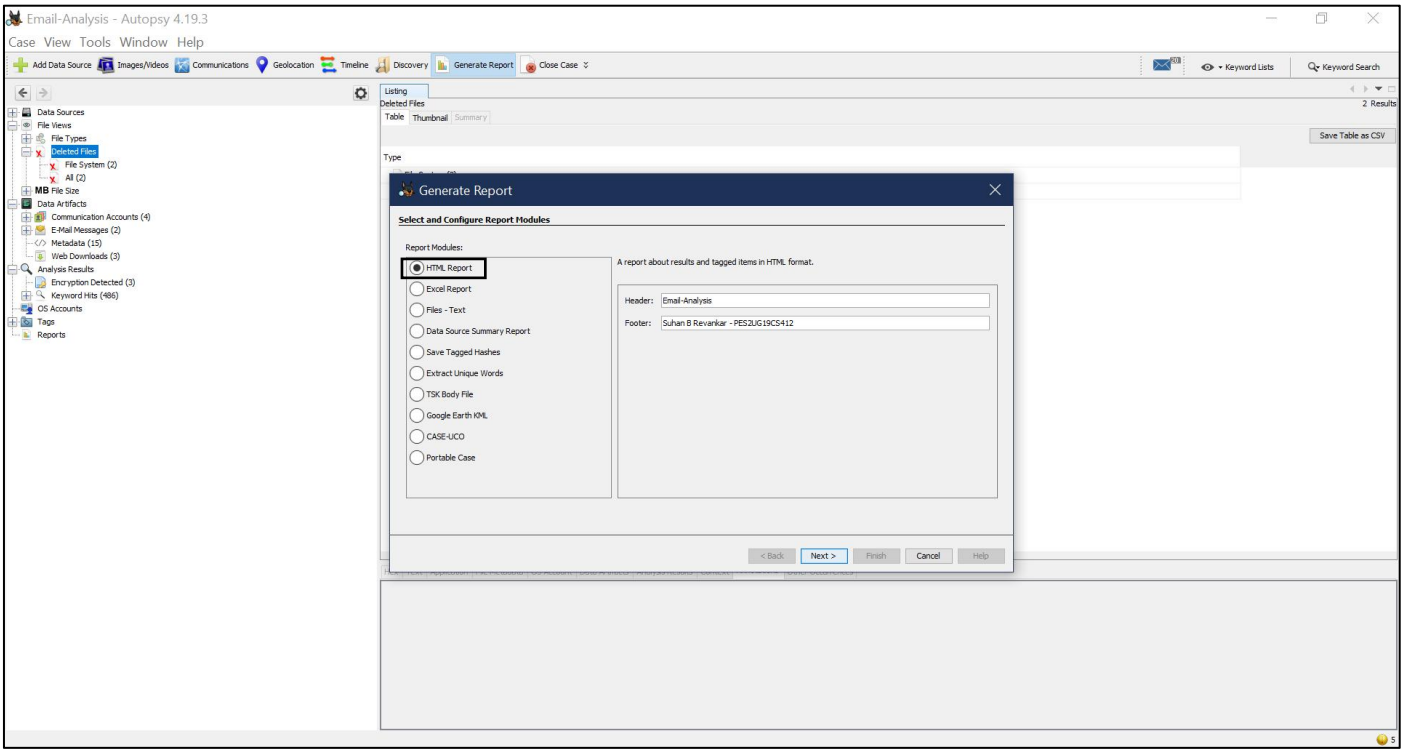

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Configure Ingest
Run ingest modules on:
All Files, Directories, and Unallocated Space
Recent Activity
Hash Lookup
File Type Identification
Extension Mismatch Detector
Embedded File Extractor
Picture Analyzer
Keyword Search
Email Parser
Encryption Detection
Interesting Files Identifier
Central Repository
PhotoRec Carver
Virtual Machine Extractor
Select All
Deselect All
History
The selected module has no per-run settings.
Specify what all to look for in the target image file
Extracts recent user activity, such as Web browsing, recently us...
Global Settings
< Back
Next >
Finish
Cancel
Help

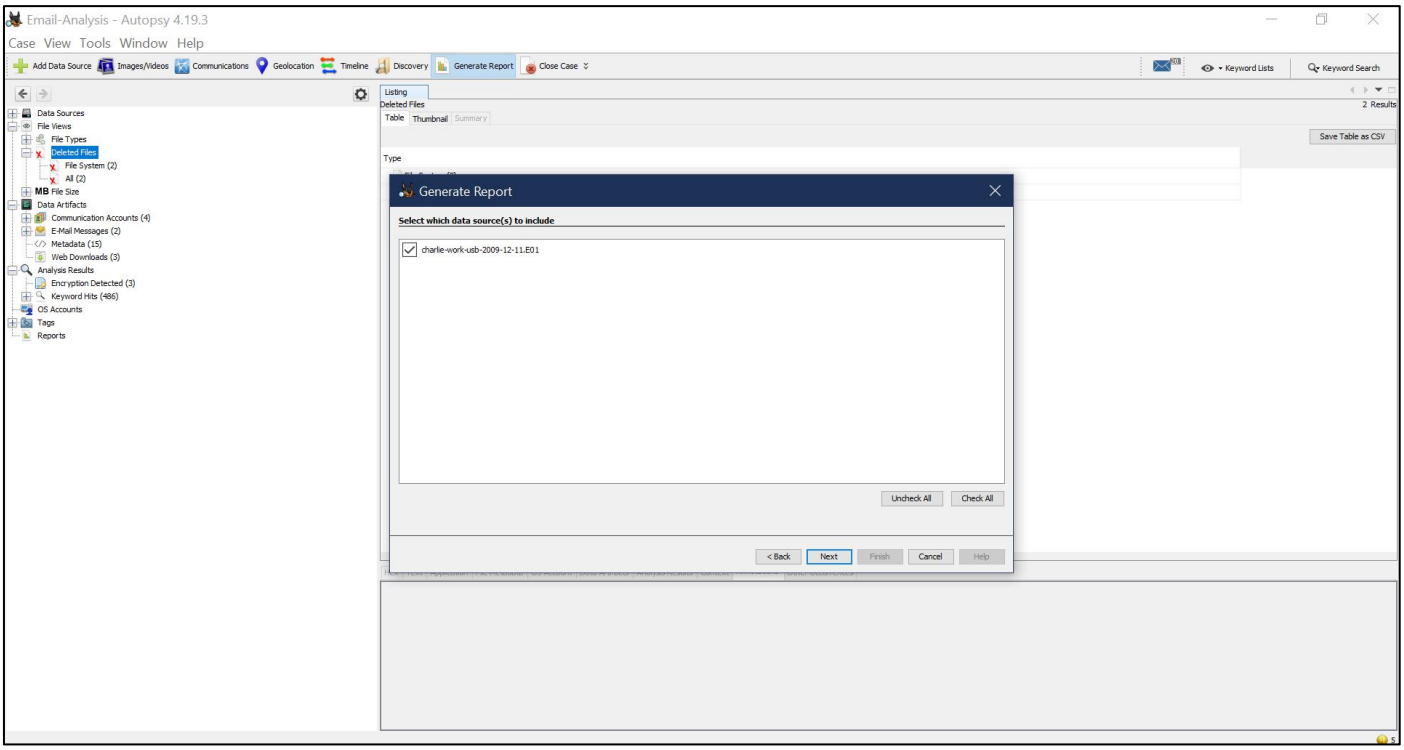

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Add Data Source
Data source has been added to the local database. Files are being analyzed.
< Back
Next >
Finish
Cancel
Help

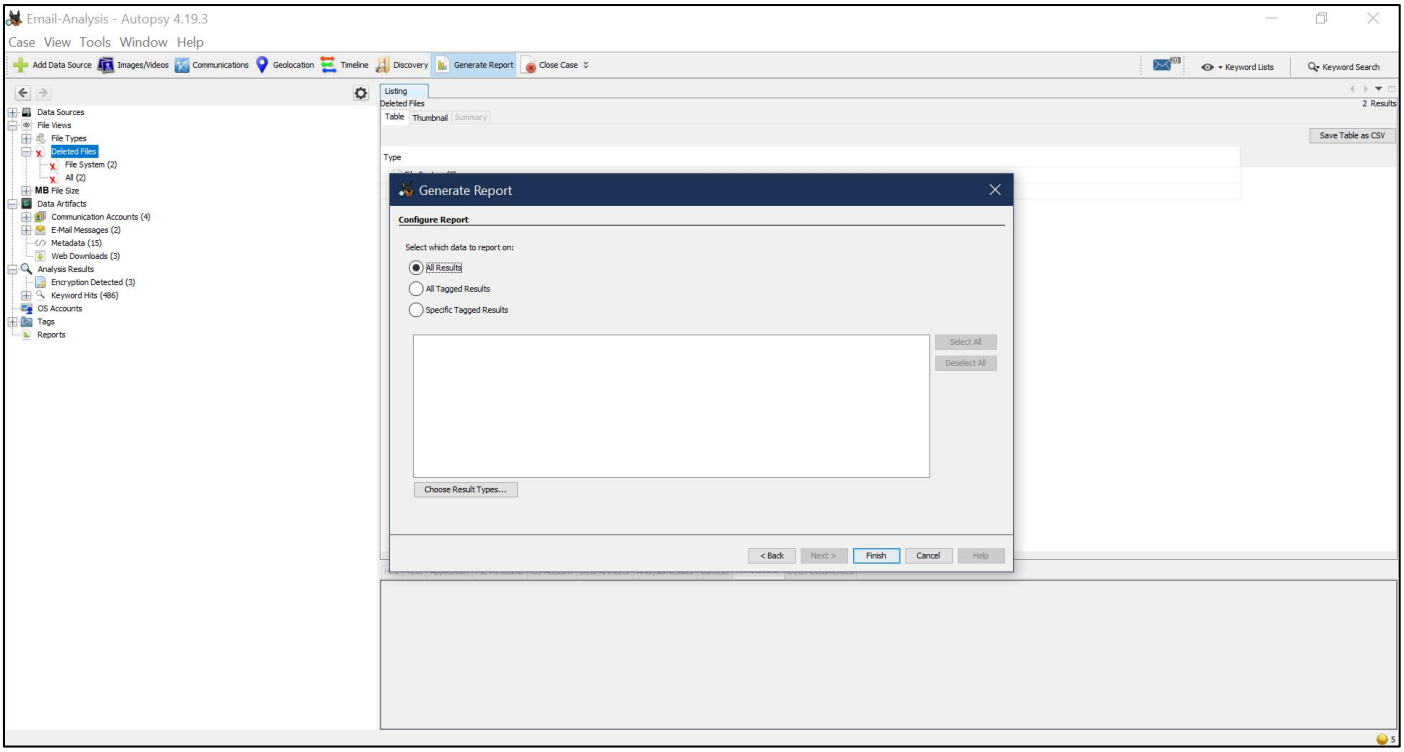
“Deleted files” specify the files , structure of directories etc . that were recovered from the target image .



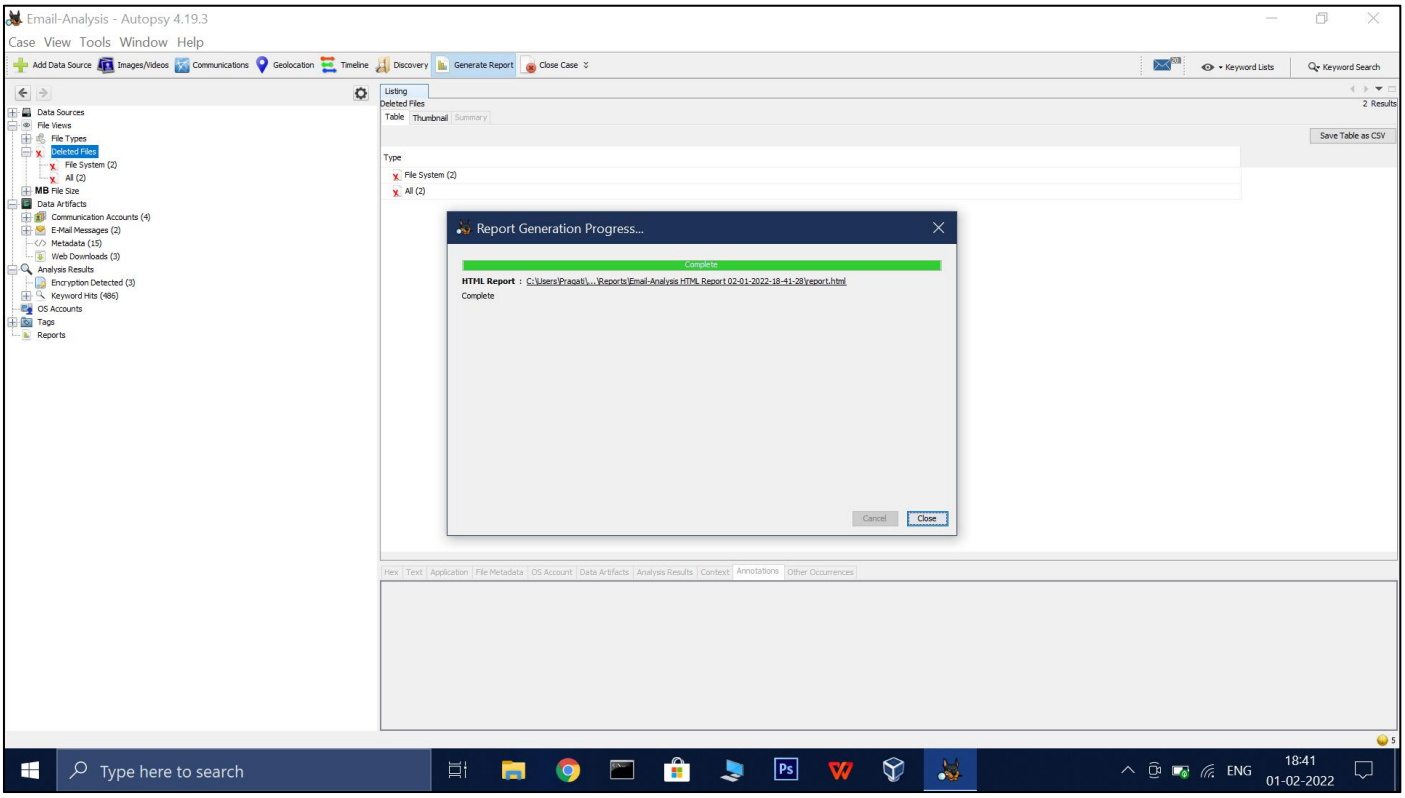
Click on “generate report” to get the detailed analysis report and select the file format of report needed .



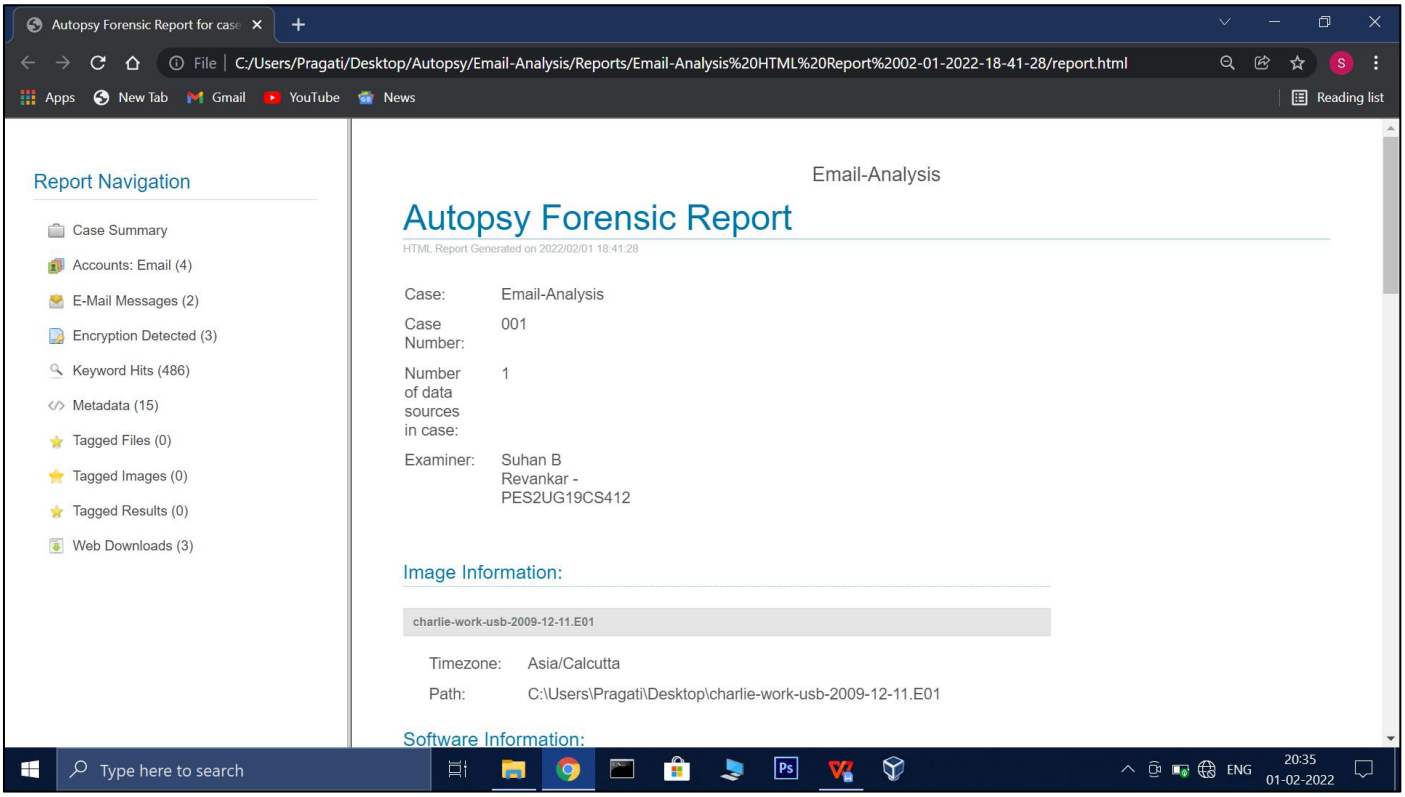

Email-Analysis - Autopsy 4.19.3
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
File Views
File Types
Deleted Files
File System (2)
All (2)
File Size
Data Artifacts
Communication Accounts (4)
E-Mail Messages (2)
Metadata (15)
Web Downloads (3)
Analysis Results
Encryption Detected (3)
Keyword Hits (486)
OS Accounts
Tags
Reports
Listing
Deleted Files
2 Results
Table
Thumbnail
Summary
Save Table as CSV
Type
Generate Report
Select which data source(s) to include
charlie-work-usb-2009-12-11.E01
Uncheck All
Check All
< Back
Next
Finish
Cancel
Help


Email-Analysis - Autopsy 4.19.3
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
File Views
File Types
Deleted Files
File System (2)
All (2)
File Size
Data Artifacts
Communication Accounts (4)
E-Mail Messages (2)
Metadata (15)
Web Downloads (3)
Analysis Results
Encryption Detected (3)
Keyword Hits (486)
OS Accounts
Tags
Reports
Listing
Deleted Files
2 Results
Table
Thumbnail
Summary
Save Table as CSV
Type
Generate Report
Configure Report
Select which data to report on:
All Results
All Tagged Results
Specific Tagged Results
Select All
Deselect All
Choose Result Types...
< Back
Next >
Finish
Cancel
Help

Report generated Successfully



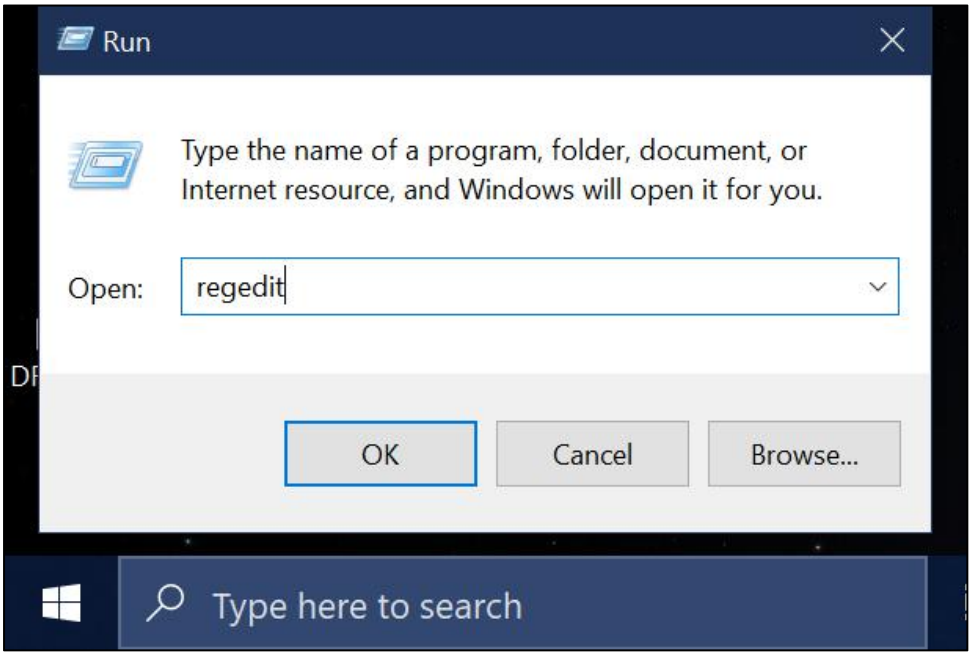
Forensic Report



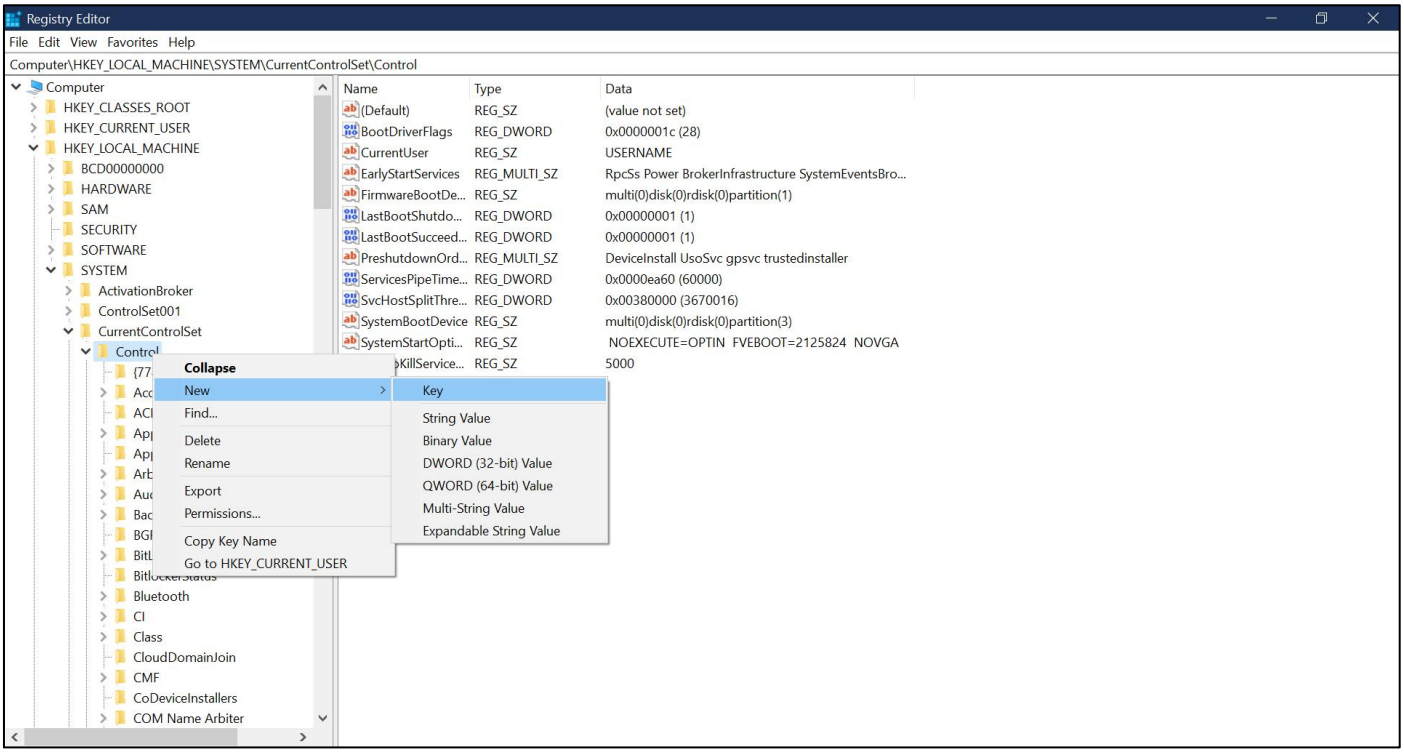
Activity 3

Write Block on USB Device

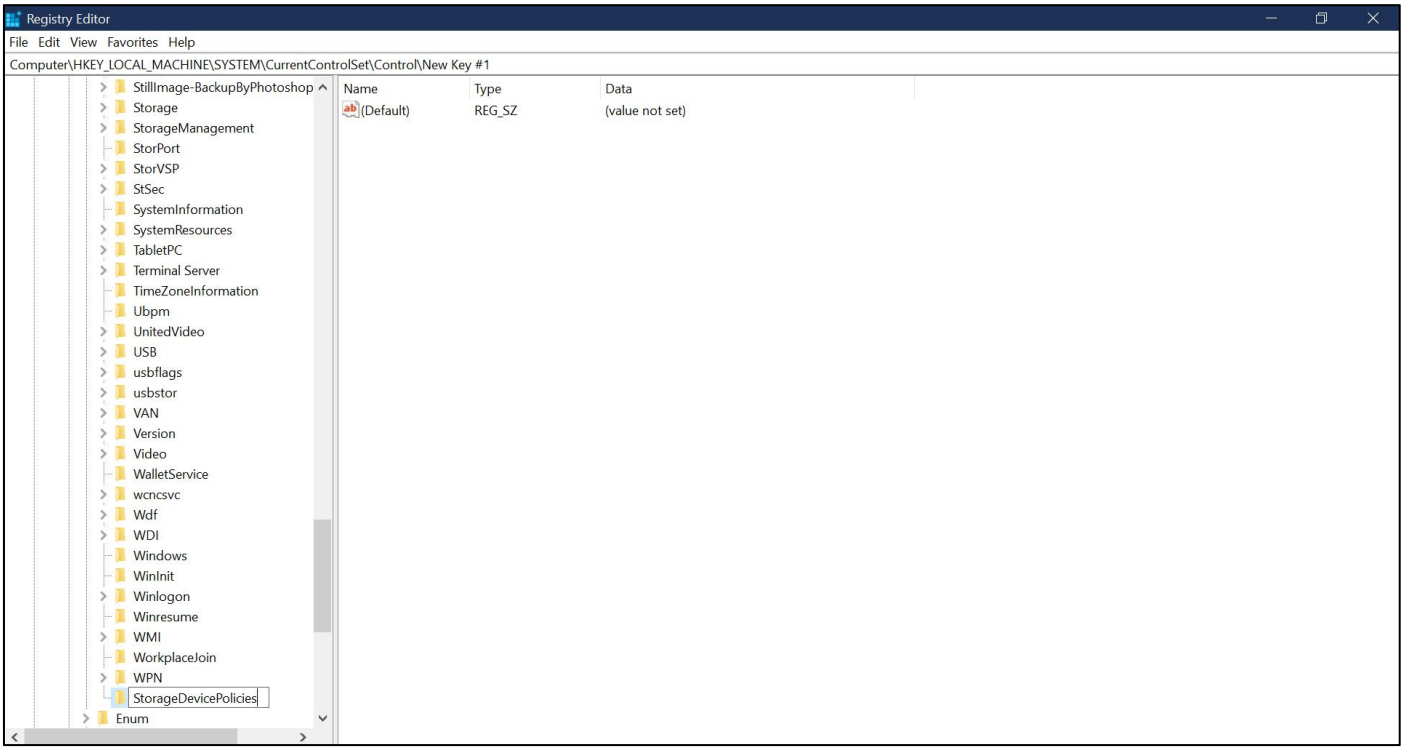
1. Open registry editor (click on run program & type ***regedit*** and click on run)



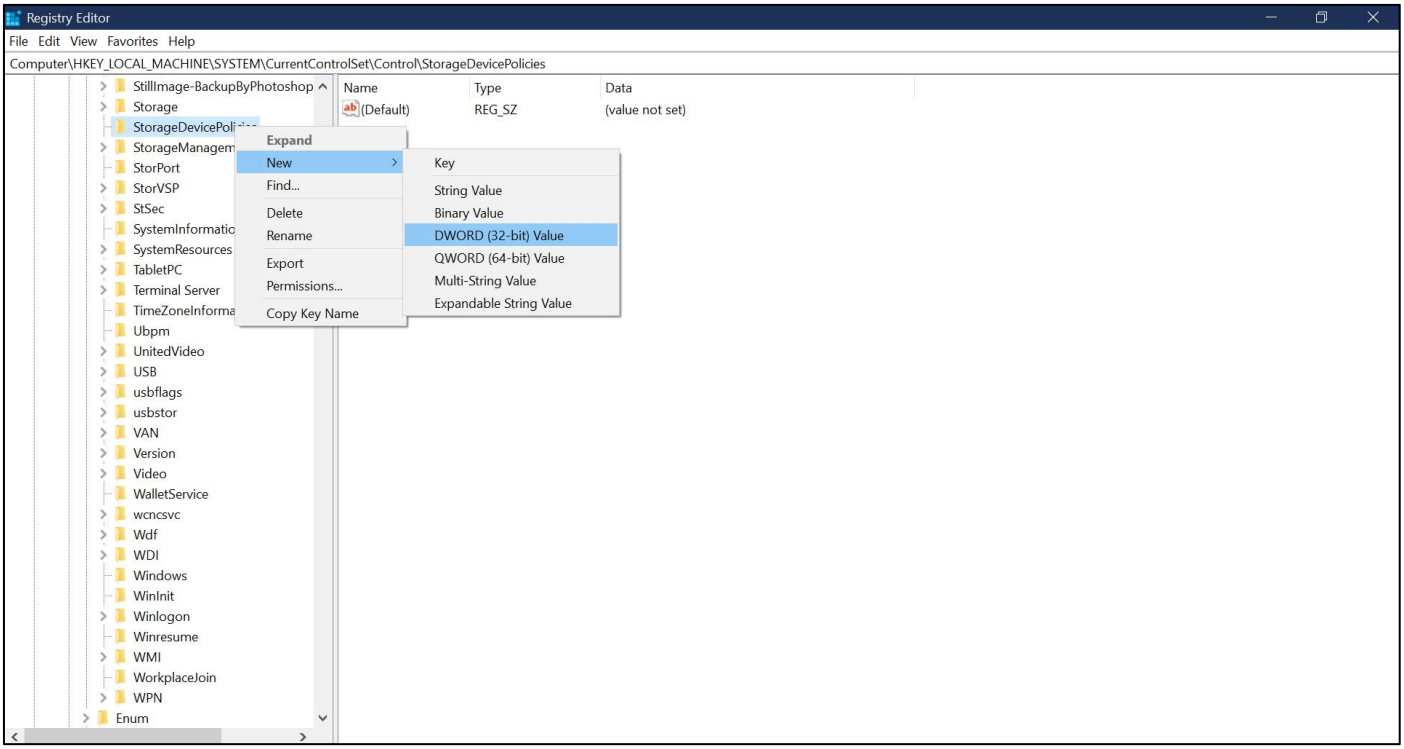
2. Navigate to HKEY_LOCAL_MACHINE -> SYSTEM -> CurrentControlSet -> Control
   Right click then *select* new -> Key



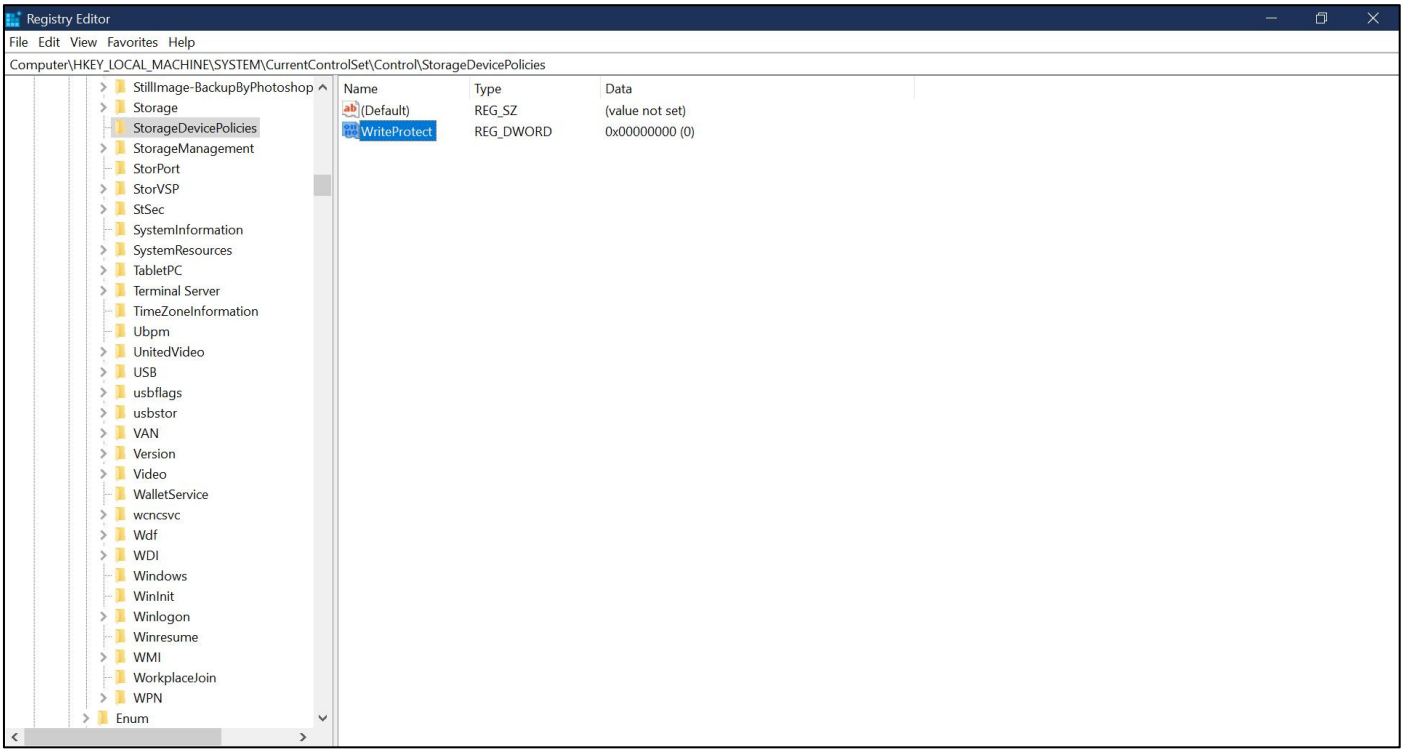
3. Name the key as StorageDevicePolicies



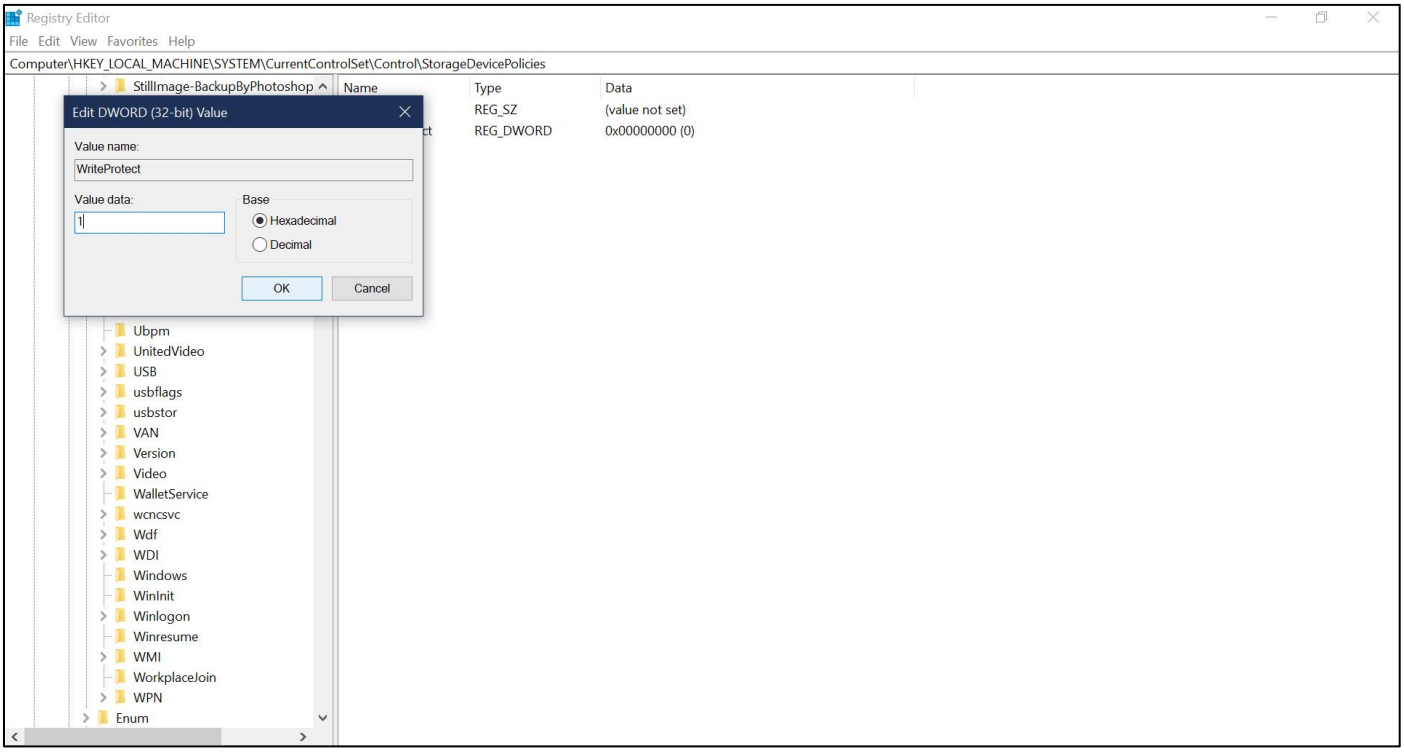
4. Right click select new -> DWORD (32-bit) Value



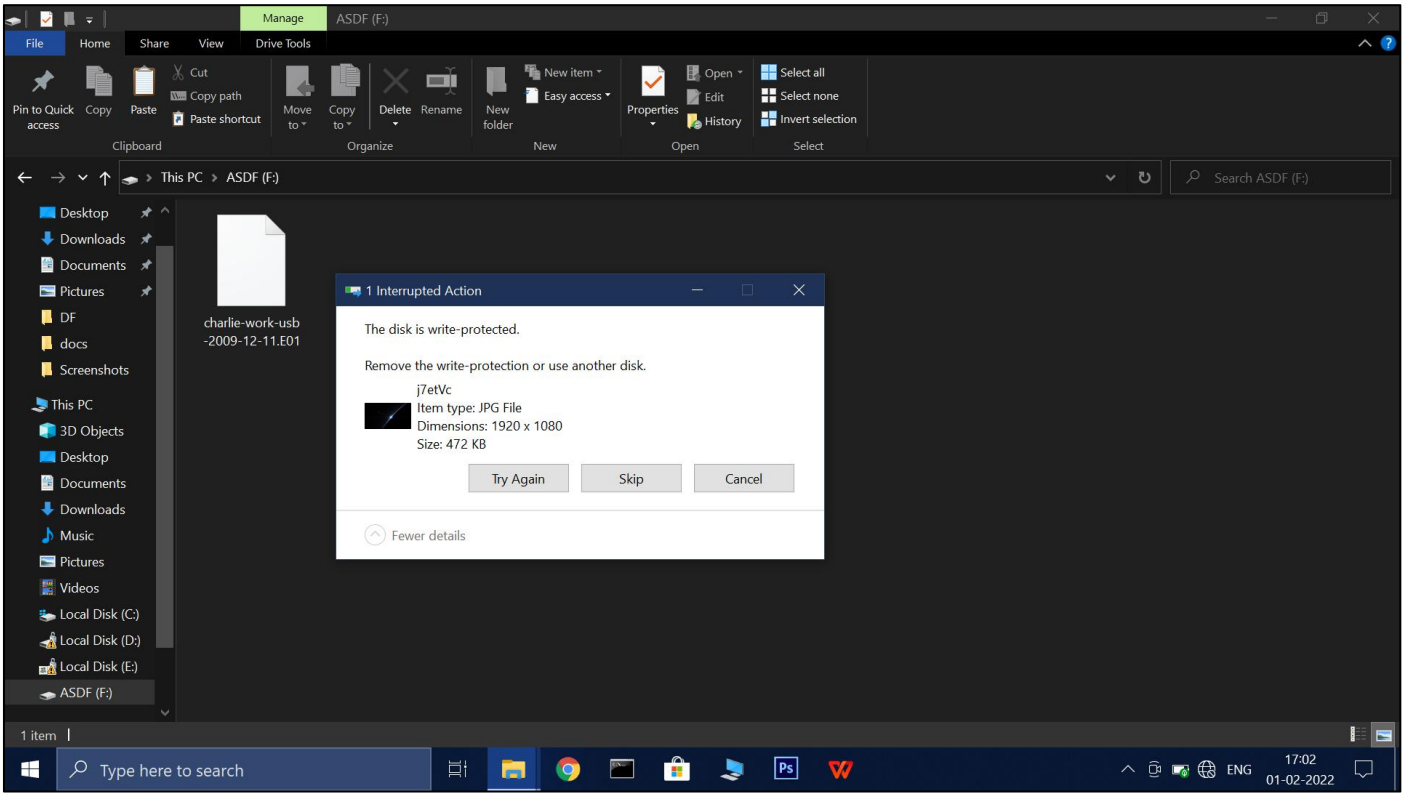
5 . Name the file as WriteProtect



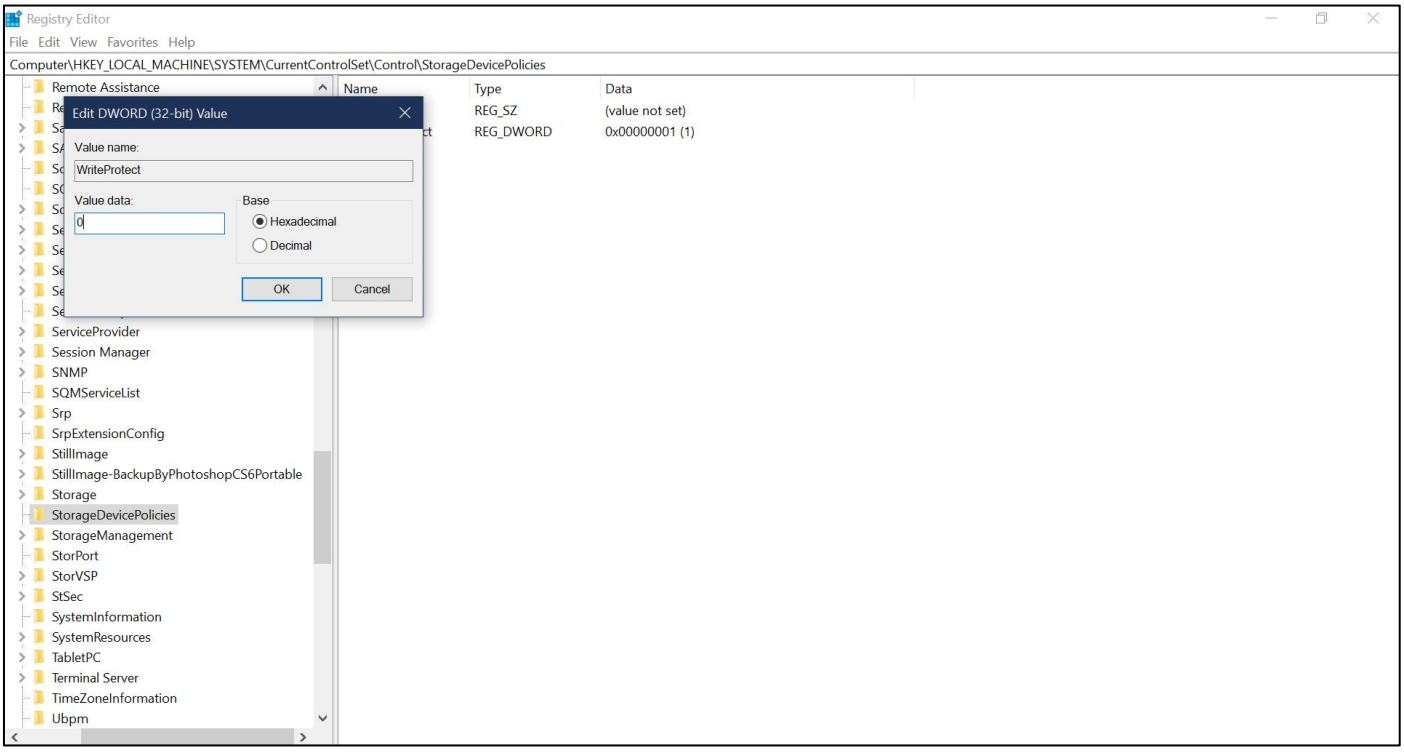
6 . Change the value from 0 to 1 [To enable write protect to or from the usb]



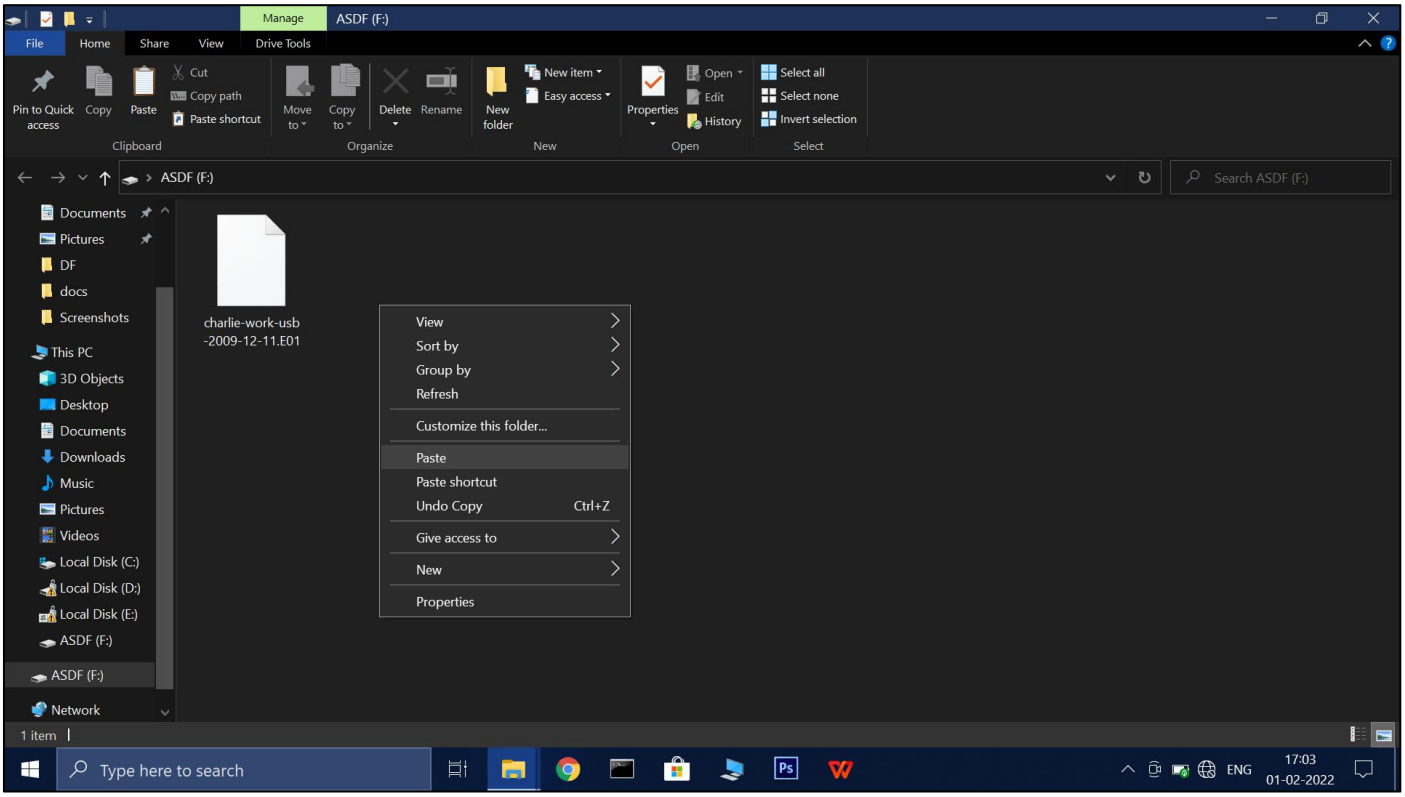
Result snapshot after enabling write Protect

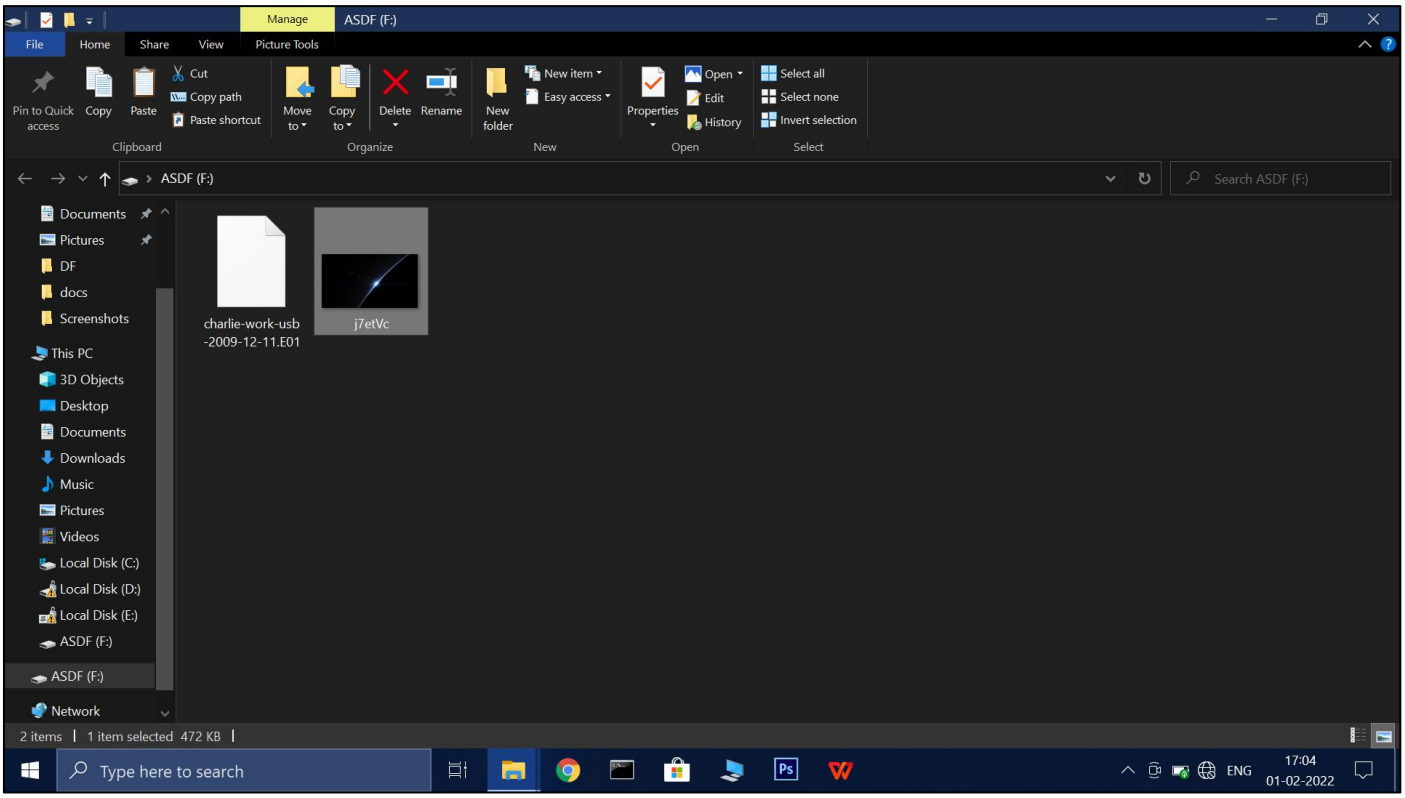


To disable the write protect to or from the usb device
Navigate to same path as previous , change the value from 1 to 0 [disabling write protect]



Result after disabling write protect





******