RAMNIRANJAN JHUNJHUNWALA COLLEGE
GHATKOPAR (W), MUMBAI - 400 086

DEPARTMENT OF
INFORMATION TECHNOLOGY

2021 - 2022

M.Sc. (I.T.) Part II (Sem - 3)

Subject: Computer Hacking Forensic Investigation

Name: Sneha Ramchandra Pawar.
Roll No.: 18

Hindi Vidya Prachar Samiti's

RAMNIRANJAN JHUNJHUNWALA COLLEGE

(AUTONOMOUS)

Opposite Ghatkopar Railway Station, Ghatkopar West, Mumbai-400086

CERTIFICATE

This is to certify that **Miss. Sneha Ramchandra Pawar** with Roll No. **18** has successfully completed the necessary course of experiments in the subject of **Computer Hacking Forensic Investigation** during the academic year **2021 – 2022** complying with the requirements of **RAMNIRANJAN JHUNJHUNWALA COLLEGE OF ARTS, SCIENCE AND COMMERCE**, for the course of **M.Sc. (IT) Part II Semester – III.**

_____ _____

Internal Examiner **External Examiner**

_____ _____

Head Of Department **College Seal**

INDEX

Practical No	Practical	Date

01	File System Analysis using Autopsy	26/11/2021
02	Using Windows Forensics Toolkit [AccessData FTK]	26/11/2021
03	Using Data Acquisition Tools [ProDiscover Pro]	03/12/2021
04	Creating Image Using File Recovery Tools [FTK Imager]	26/11/2021
05	File Recovery Tools [FTK Imager] using evidence	26/11/2021
06	Using Steganography Tools [S-Tools].	27/11/2021
07	Using Log and Traffic Capturing and Analysis Tools [Wireshark].	27/11/2021
08	Using Email Forensics Tools [AccessData FTK].	27/11/2021
09	Writing Reports Using FTK [AccessData FTK].	27/11/2021
10	Performing Password Cracking [Cain and Abel]	10/12/2021
11	Managing Remote Registry, Network Enumeration, Services, s. IDs [Cain and Abel]	10/12/2021
12	Investigating Website using FAW	03/11/2021
13	Using Mobile Forensics Tools [Mobiledit] .	10/11/2021
14	Forensic Investigation Using Encase	03/11/2021

Practical No. 01

Aim: File System Analysis using Autopsy.

What is Autopsy?
Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card.

Easy to Use

Autopsy was designed to be intuitive out of the box. Installation is easy and wizards guide you through every step. All results are found in a single tree. See the intuitive page for more details.

Extensible

Autopsy was designed to be an end-to-end platform with modules that come with it out of the box and others that are available from third-parties. Some of the modules provide:

- Timeline Analysis - Advanced graphical event viewing interface (video tutorial included).
- Hash Filtering - Flag known bad files and ignore known good.
- Keyword Search - Indexed keyword search to find files that mention relevant terms.
- Web Artifacts - Extract history, bookmarks, and cookies from Firefox, Chrome, and IE.
- Data Carving - Recover deleted files from unallocated space using PhotoRec
- Multimedia - Extract EXIF from pictures and watch videos.
- Indicators of Compromise - Scan a computer using STIX.

See the Features page for more details. Developers should refer to the module development page for details on building modules.

Fast

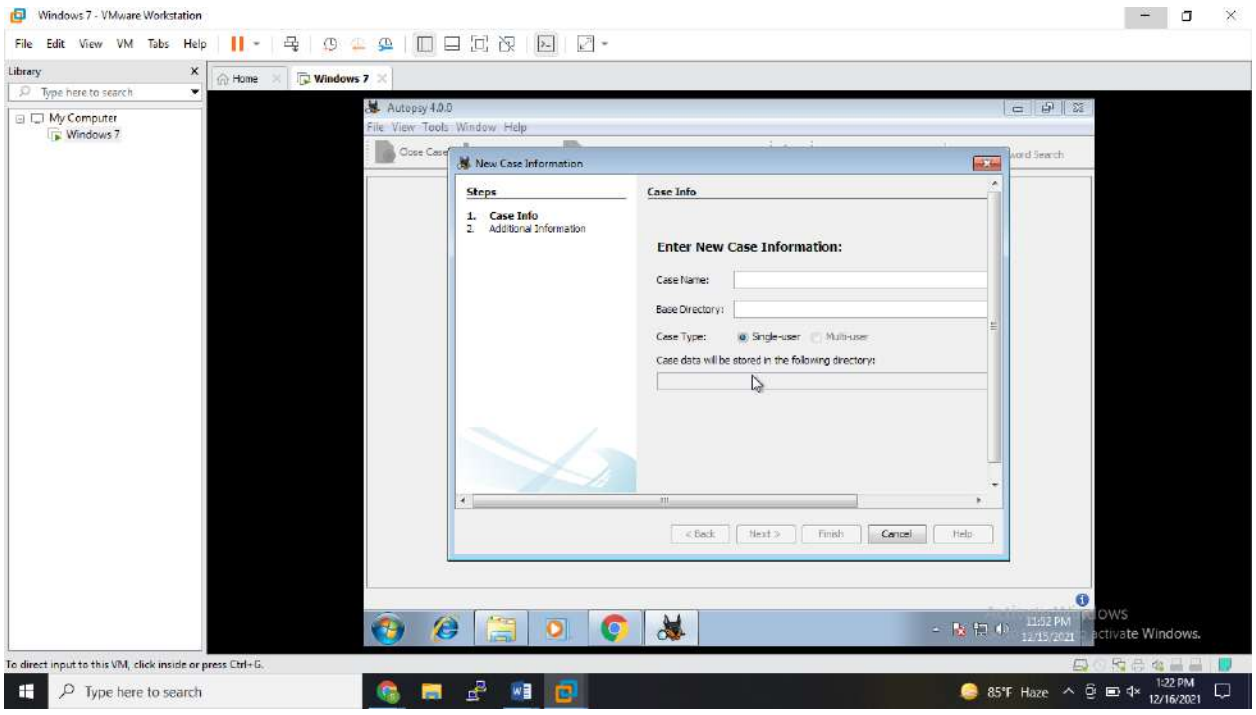
Everyone wants results yesterday. Autopsy runs background tasks in parallel using multiple cores and provides results to you as soon as they are found. It may take hours to fully search the drive, but you will know in minutes if your keywords were found in the user's home folder. See the fast results page for more details.

Cost Effective

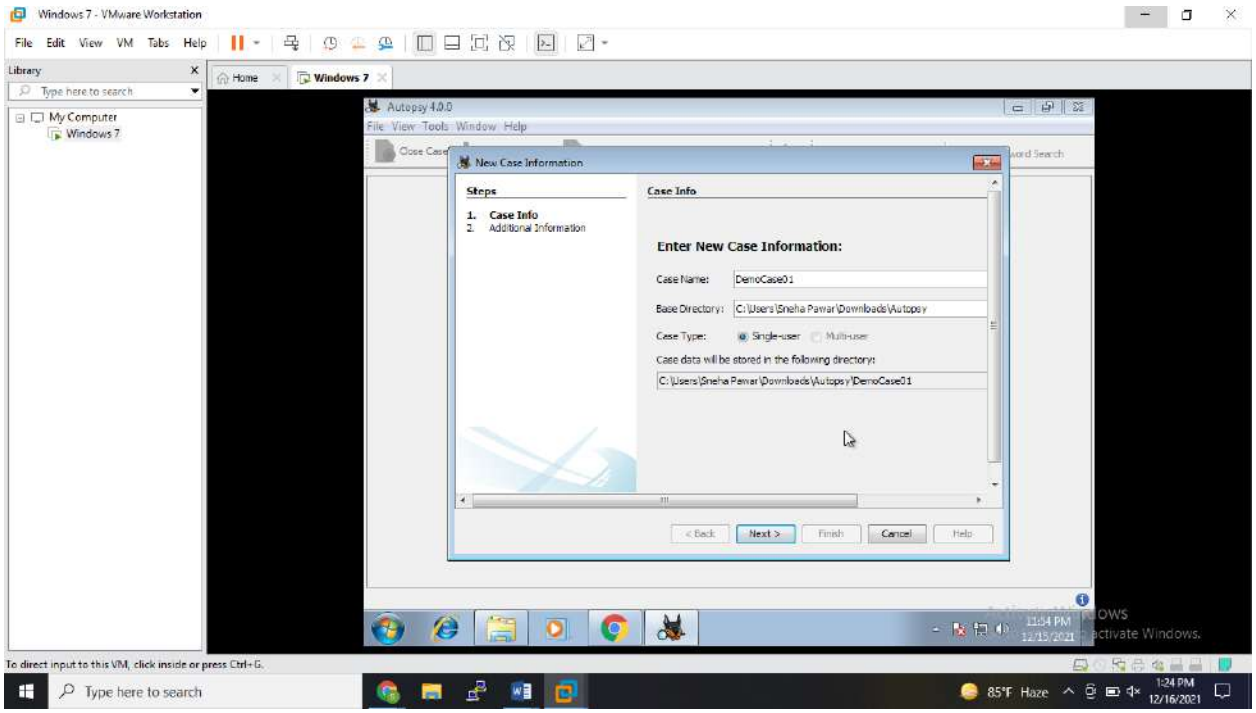
Autopsy is free. As budgets are decreasing, cost effective digital forensics solutions are essential. Autopsy offers the same core features as other digital forensics tools and offers other essential features, such as web artifact analysis and registry analysis, that other commercial tools do not provide.

Steps:

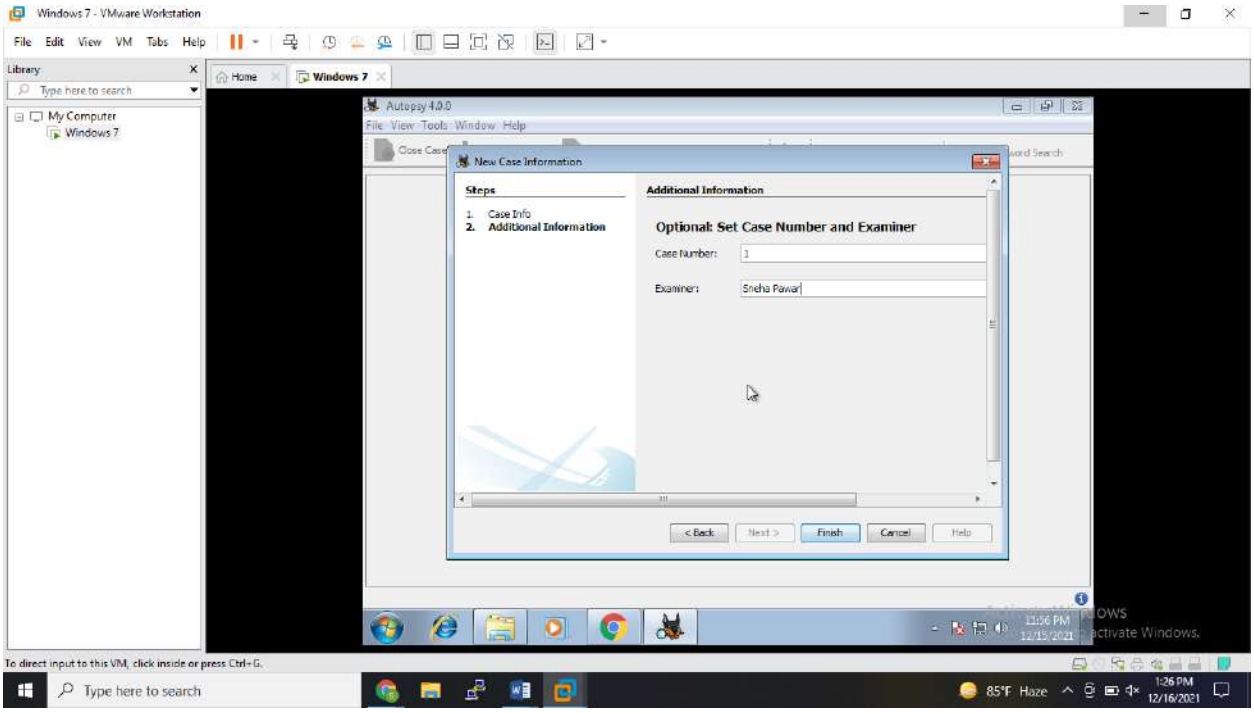
Install the Autopsy Tool. Start Autopsy Tool. Click on Create new case Or File – New Case.



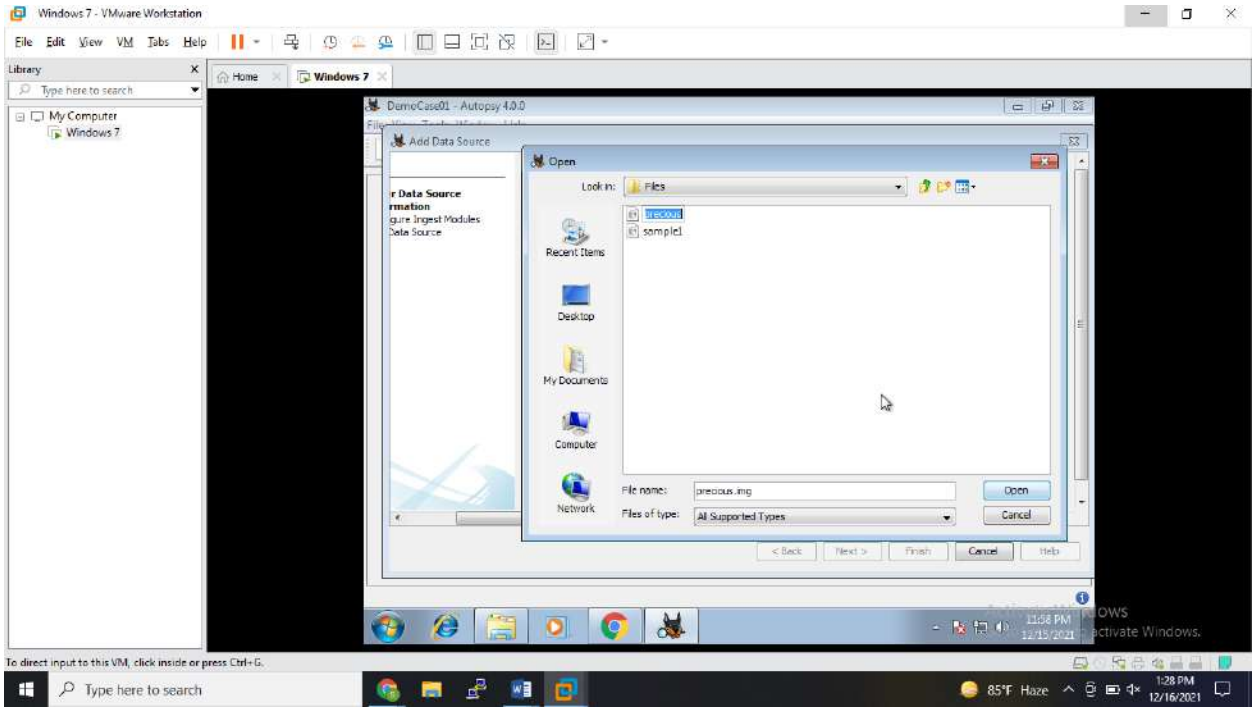
Enter case name and provide Base Directory for case. And keep rest as default and click Next.



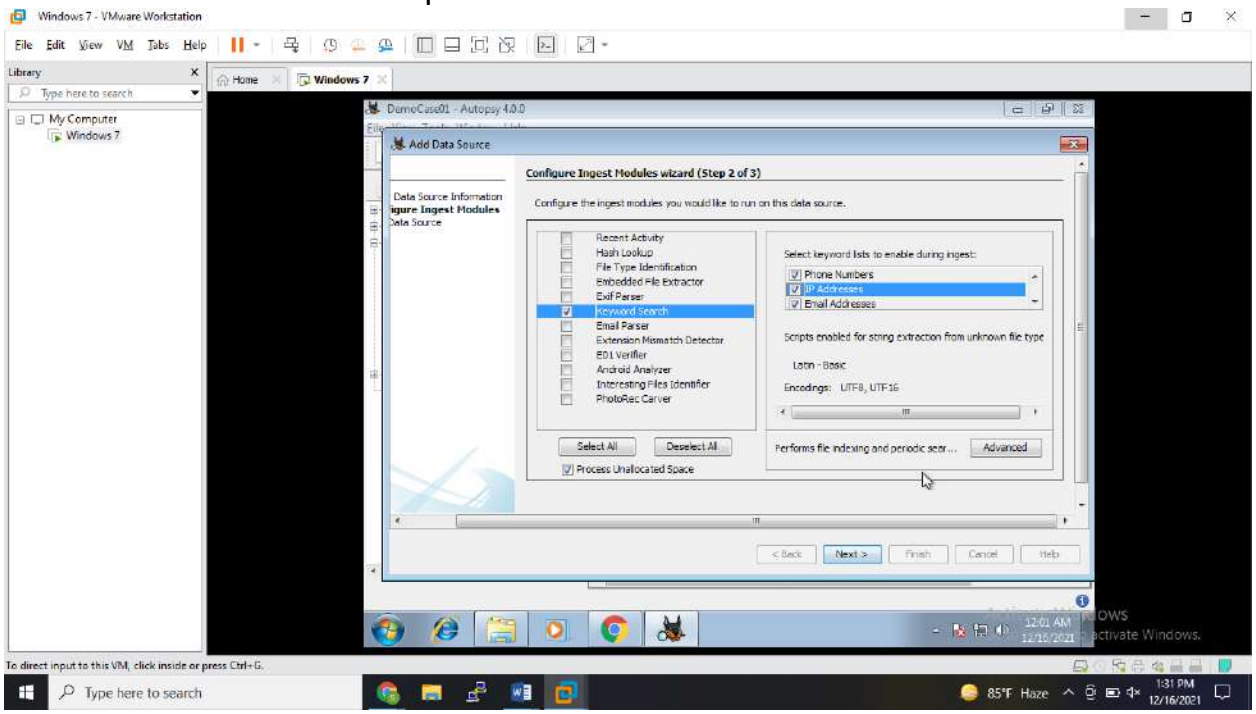
Enter case number and examiner's name. And click on Finish.



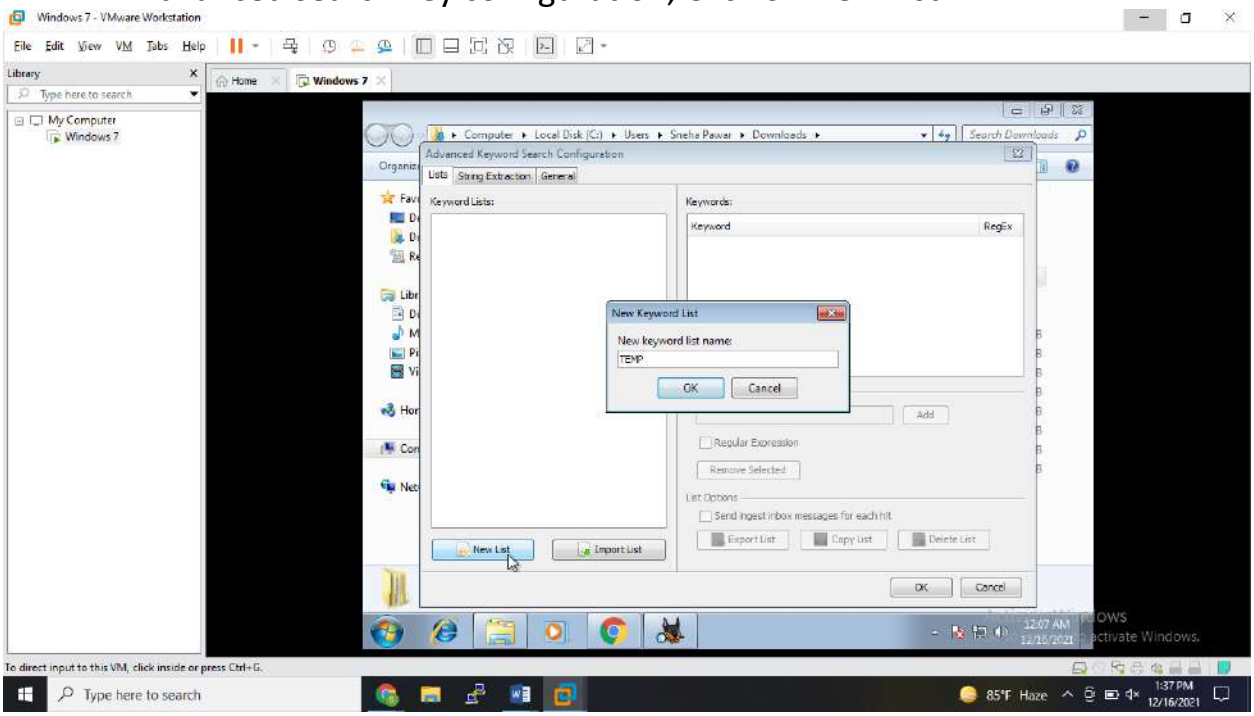
After Clicking The Finish Button In The Above Window,
A New Window Will Open For Retrieving The Datasource, Select Disk Image or VM File
Then Browse The .img File Present In The Directory Click Next.

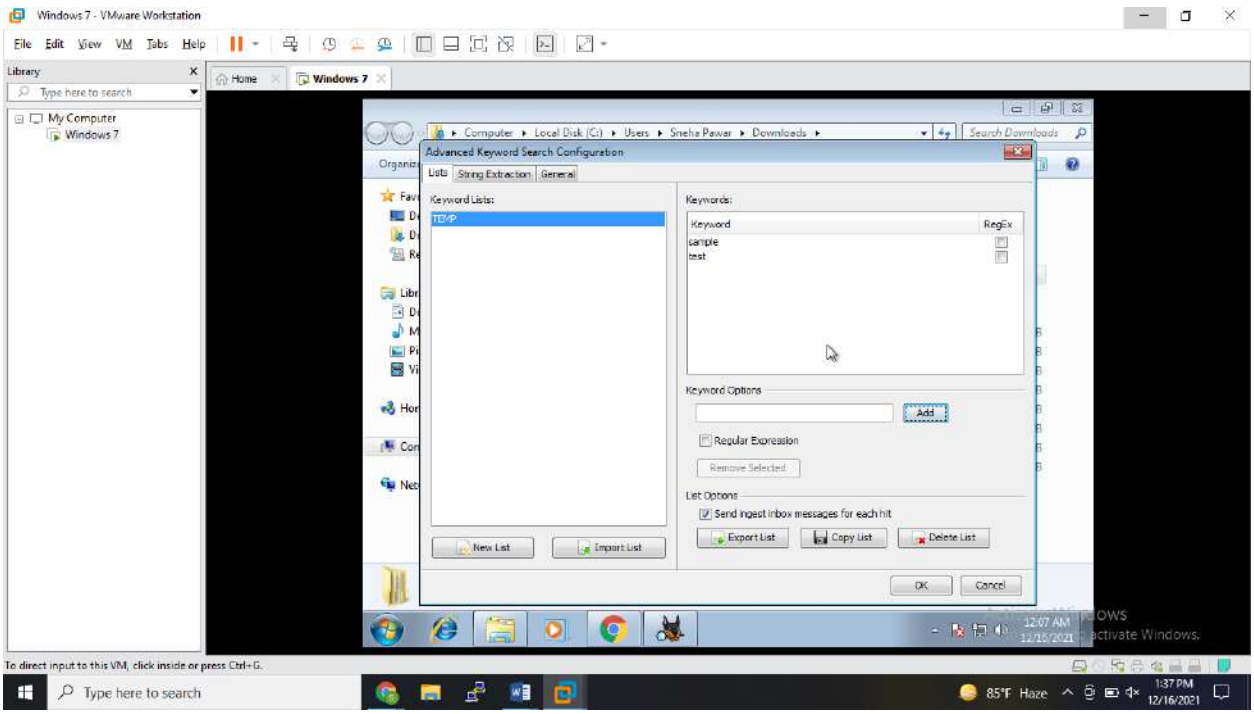


The Next Step Provides A Ingest Wizard Panel Which Aims At Increasing The Search Capability. Click Deselect all And select Keyword Search only Proceed To The Next Step.



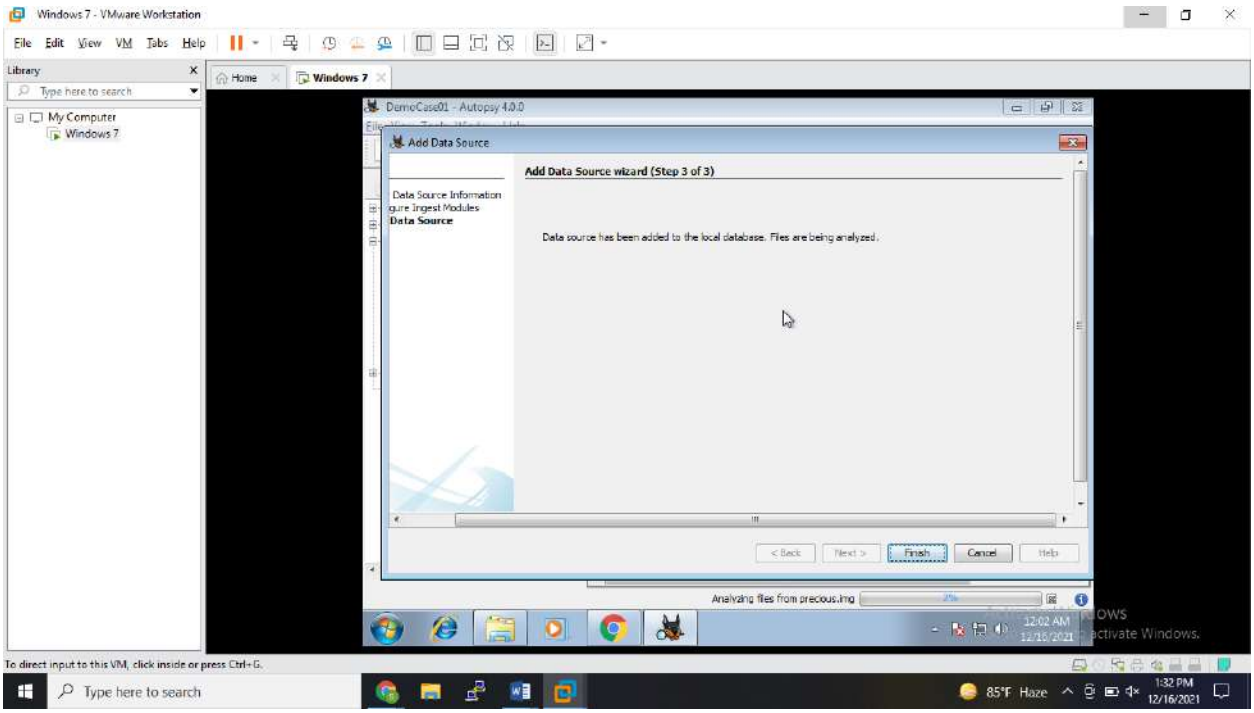
In Advanced search key configuration, Click on New List.



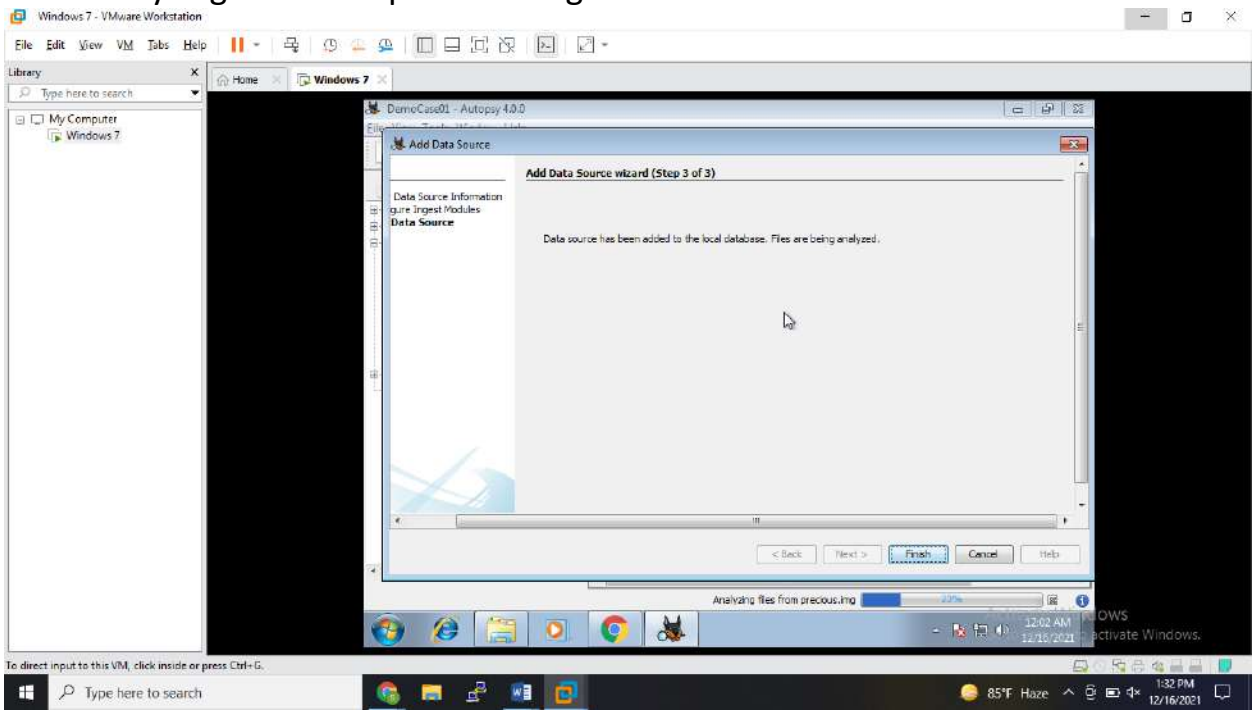


In the Resulting Window, You'll Be Notified That The Files Are Being Analysed.

Proceed to Finish.

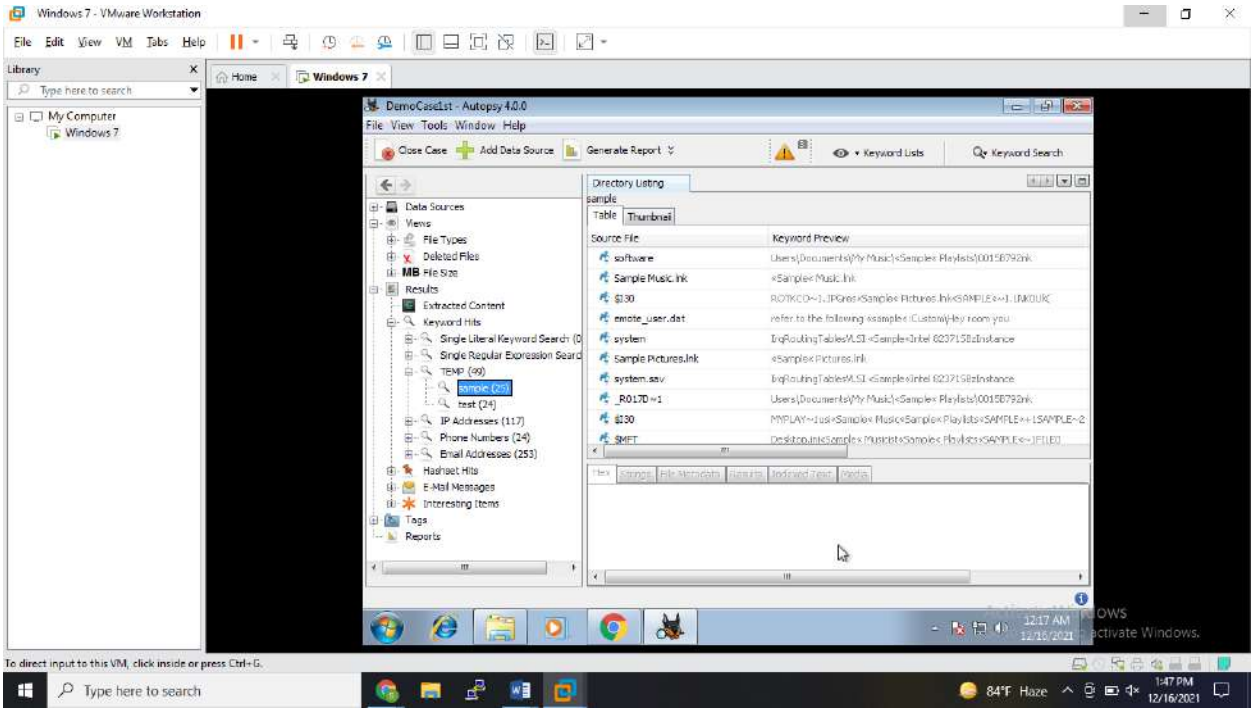


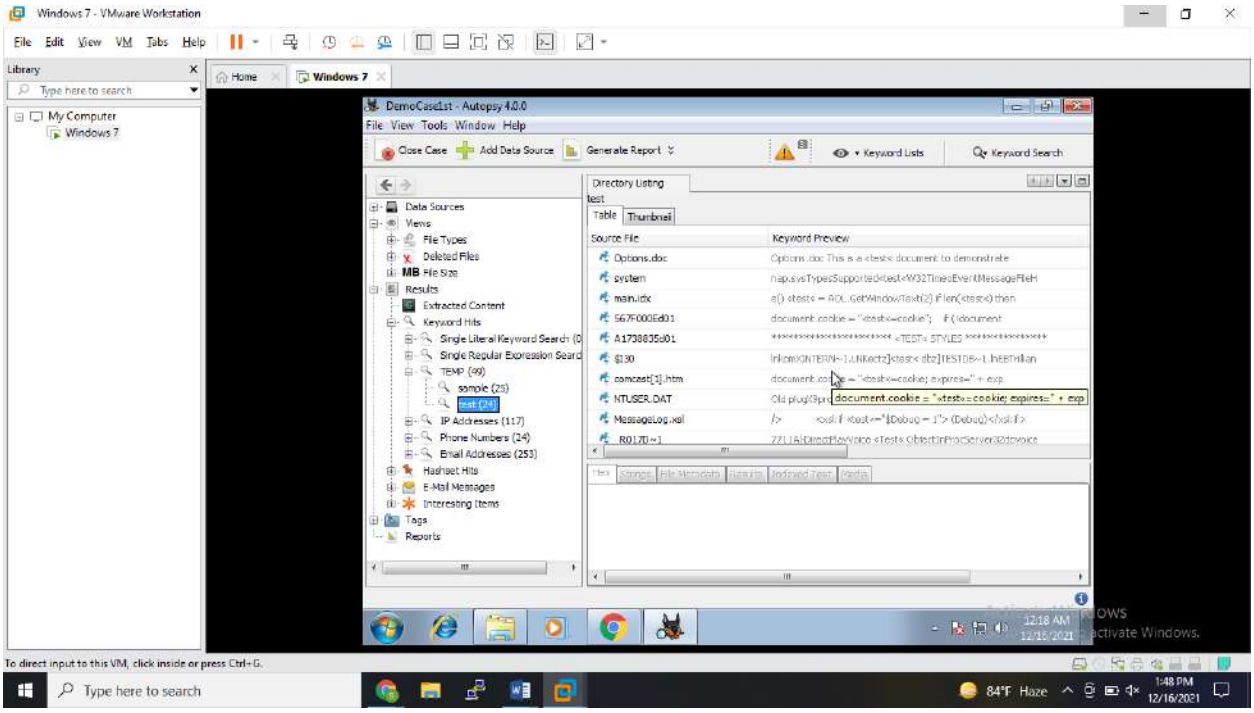
It Analyzing files from precious.img. After that Click on Finish.

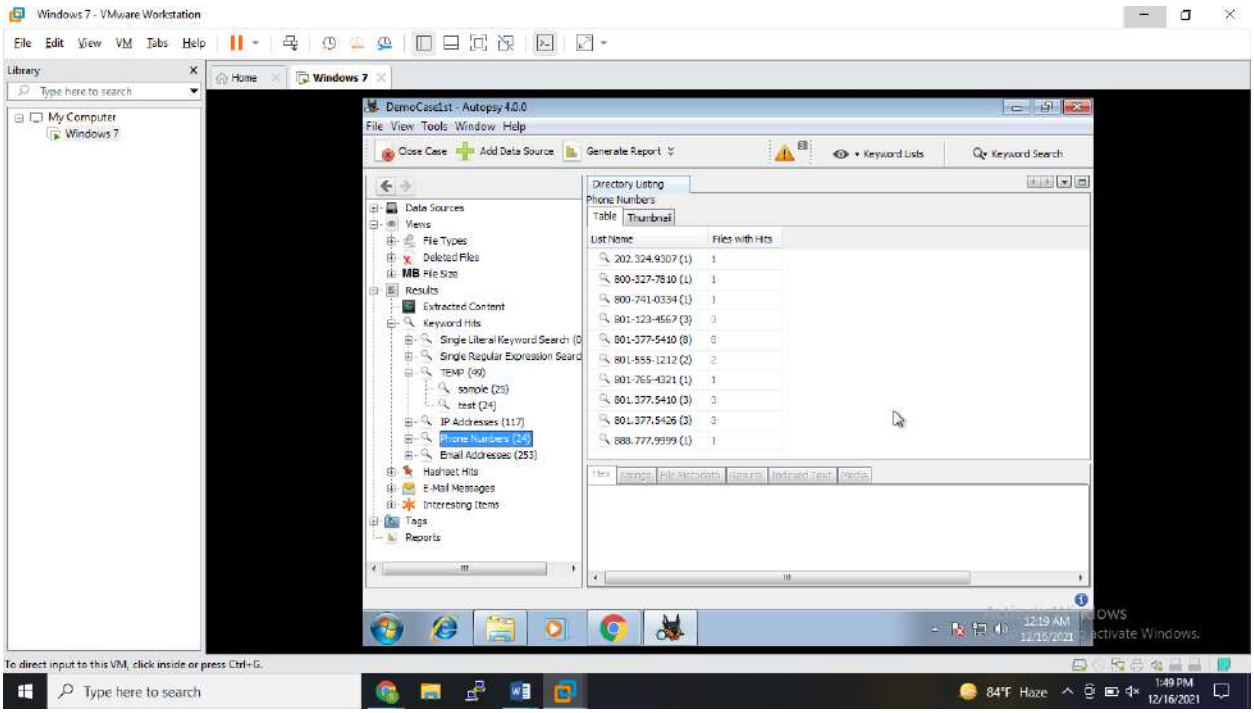


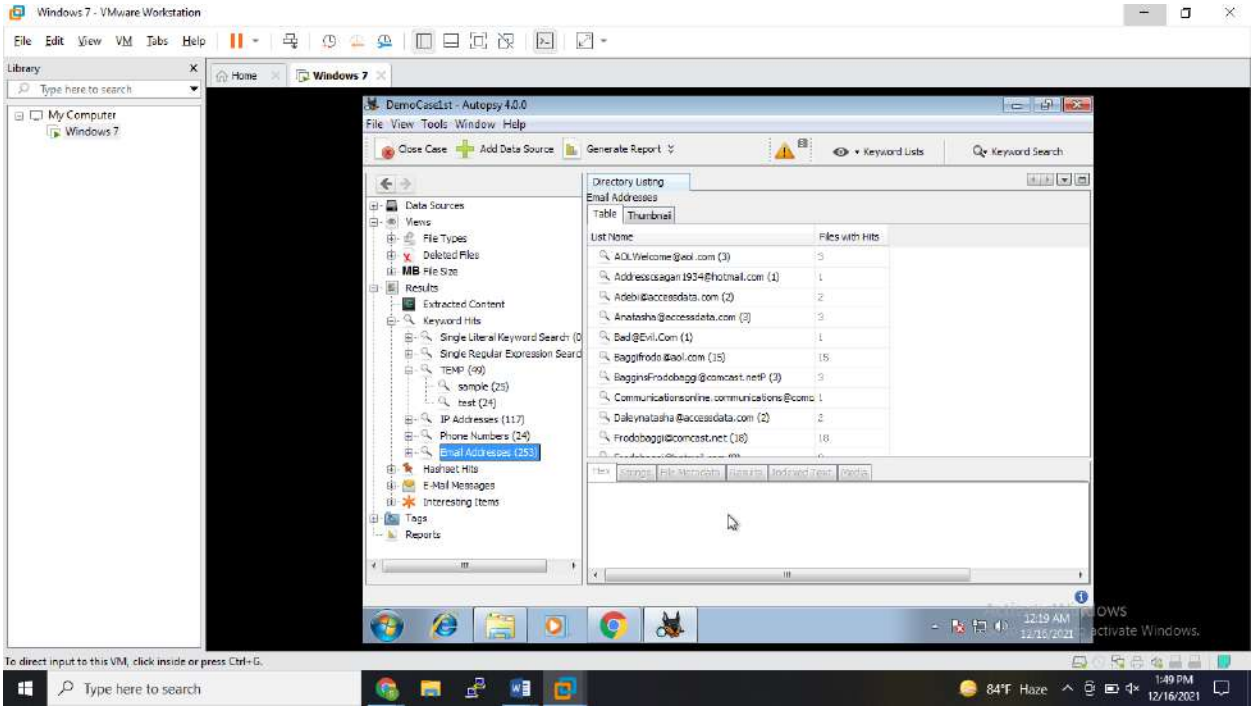
After The Image Is Indexed The Tree Will Be Populated By The File System, Extracted Content, Keyword Searches, And The Hash List (If Any Were

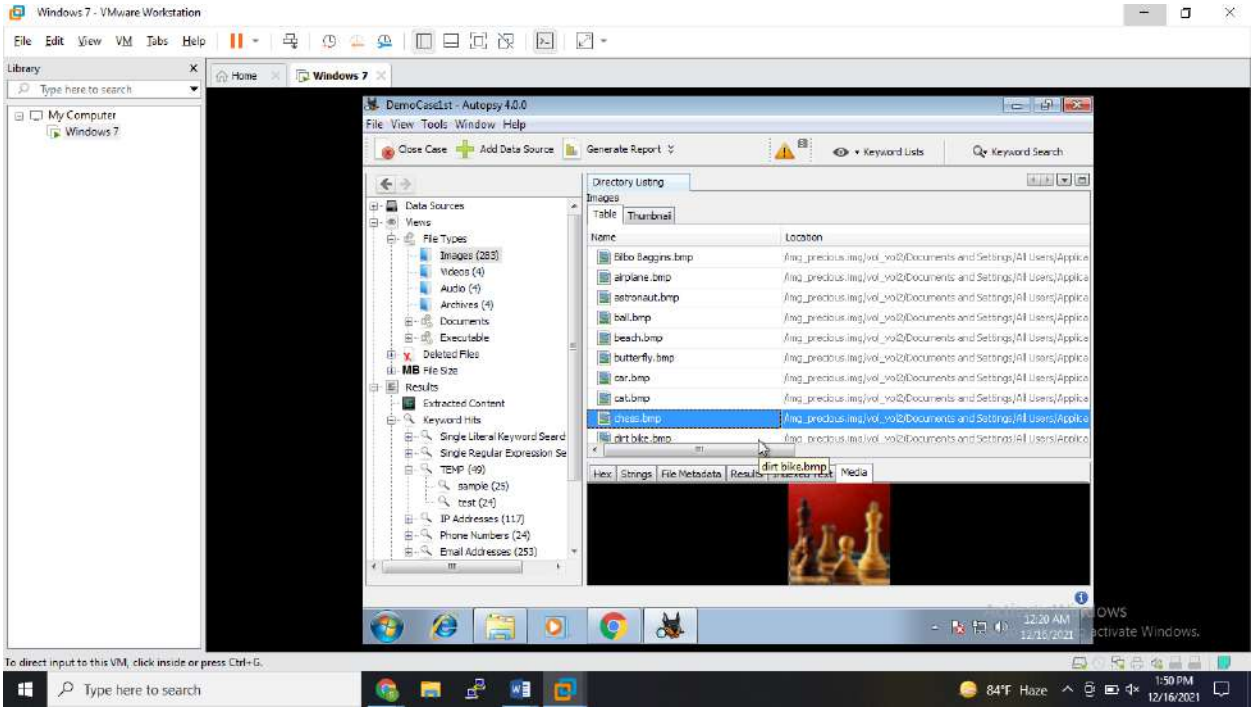
Used). This Tree Can Be To Retrieve The Information About The Image File Under Observation

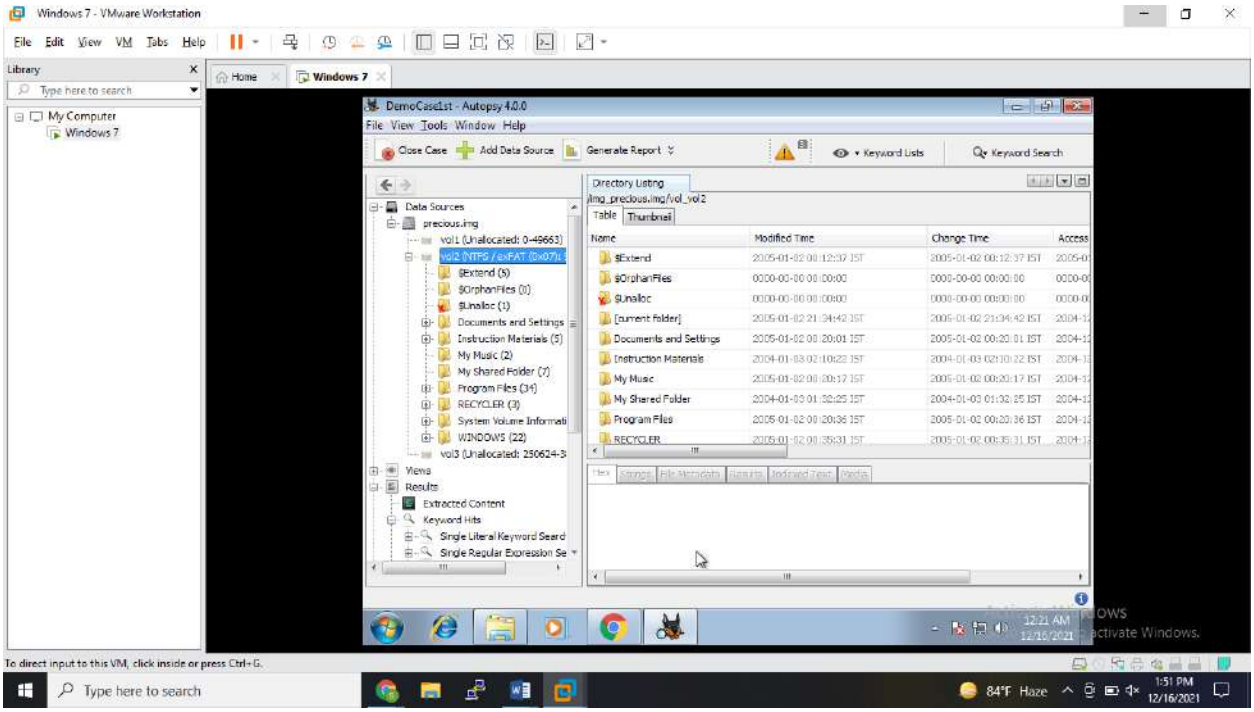


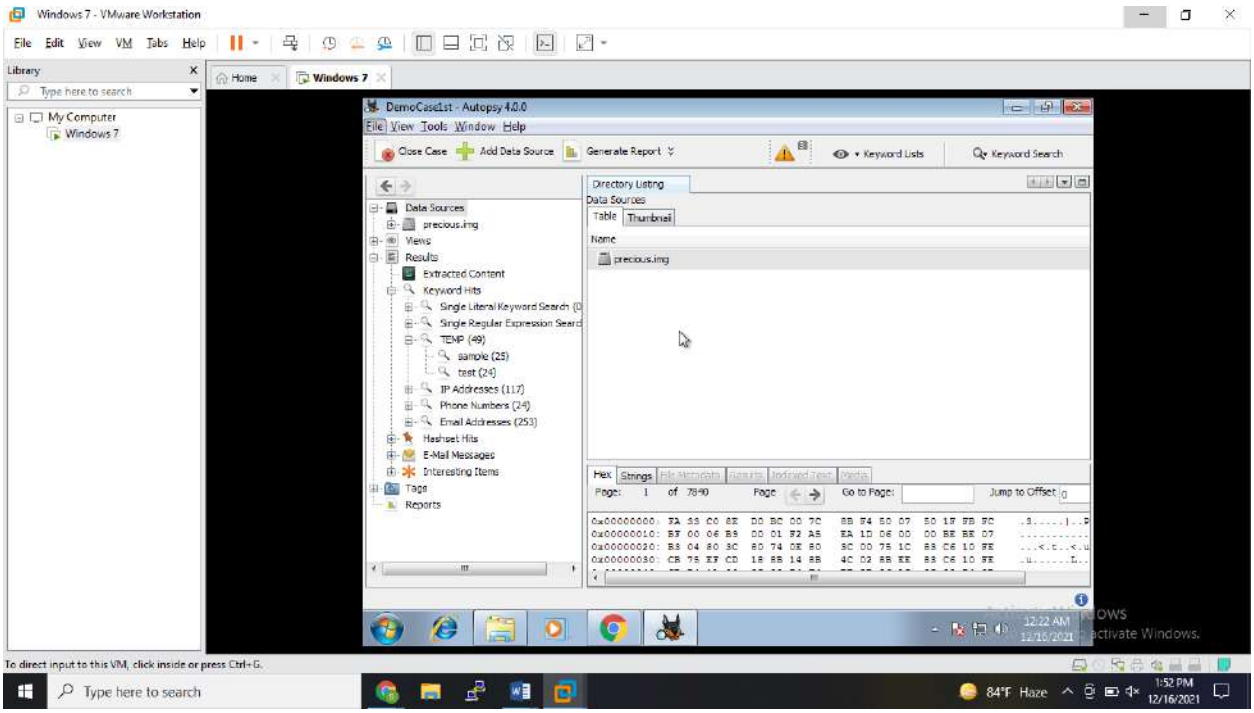



Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
DemoCase1st - Autopsy 4.0.0
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword Search
Directory Listing
Phone Numbers
Table
Thumbnail
List Name
Files with Hits
202.324.9307 (1)
800-327-7810 (1)
800-741-0334 (1)
801-123-4567 (3)
801-377-5410 (8)
801-555-1212 (2)
801-765-4321 (1)
801.377.5410 (3)
801.377.5426 (3)
888.777.9999 (1)
Data Sources
Views
File Types
Deleted Files
File Size
Results
Extracted Content
Keyword Hits
TEMP (99)
sample (25)
test (24)
IP Addresses (117)
Phone Numbers (24)
Email Addresses (253)
Hashset Hits
E-Mail Messages
Interesting Items
Tags
Reports
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
84°F Haze
1:49 PM
12/16/2021

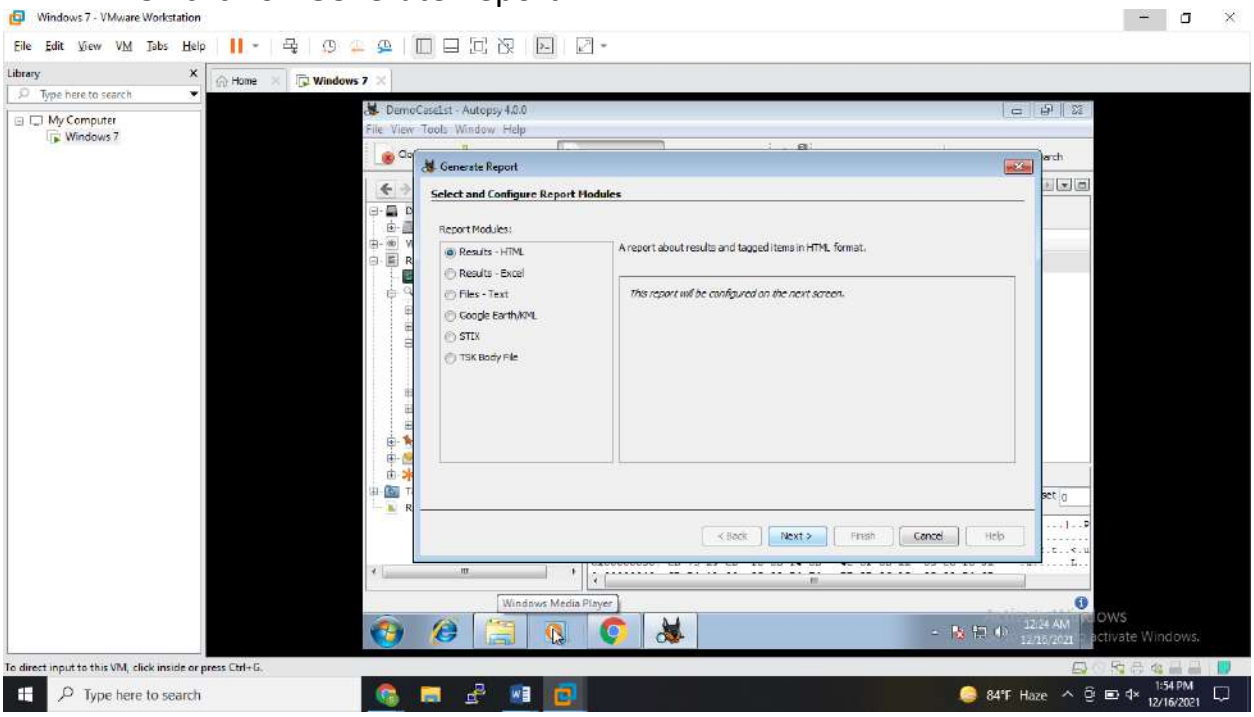

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
DemoCase1st - Autopsy 4.0.0
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword Search
Directory Listing
Email Addresses
Table
Thumbnail
List Name
Files with Hits
AOLWelcome@aol.com (3)
Addressosagan1934@hotmail.com (1)
Adebi@accessdata.com (2)
Anatasha@accessdata.com (3)
Bad@Evil.Com (1)
Baggifrodo@aol.com (15)
BagginsFrodobagg@comcast.net (3)
Communicationsonline.communications@comc
Dalevnatasha@accessdata.com (2)
Frodobaggi@comcast.net (18)
Data Sources
Views
File Types
Deleted Files
File Size
Results
Extracted Content
Keyword Hits
TEMP (99)
sample (25)
test (24)
IP Addresses (117)
Phone Numbers (24)
Email Addresses (253)
Hashset Hits
E-Mail Messages
Interesting Items
Tags
Reports
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
84°F Haze
1:49 PM
12/16/2021

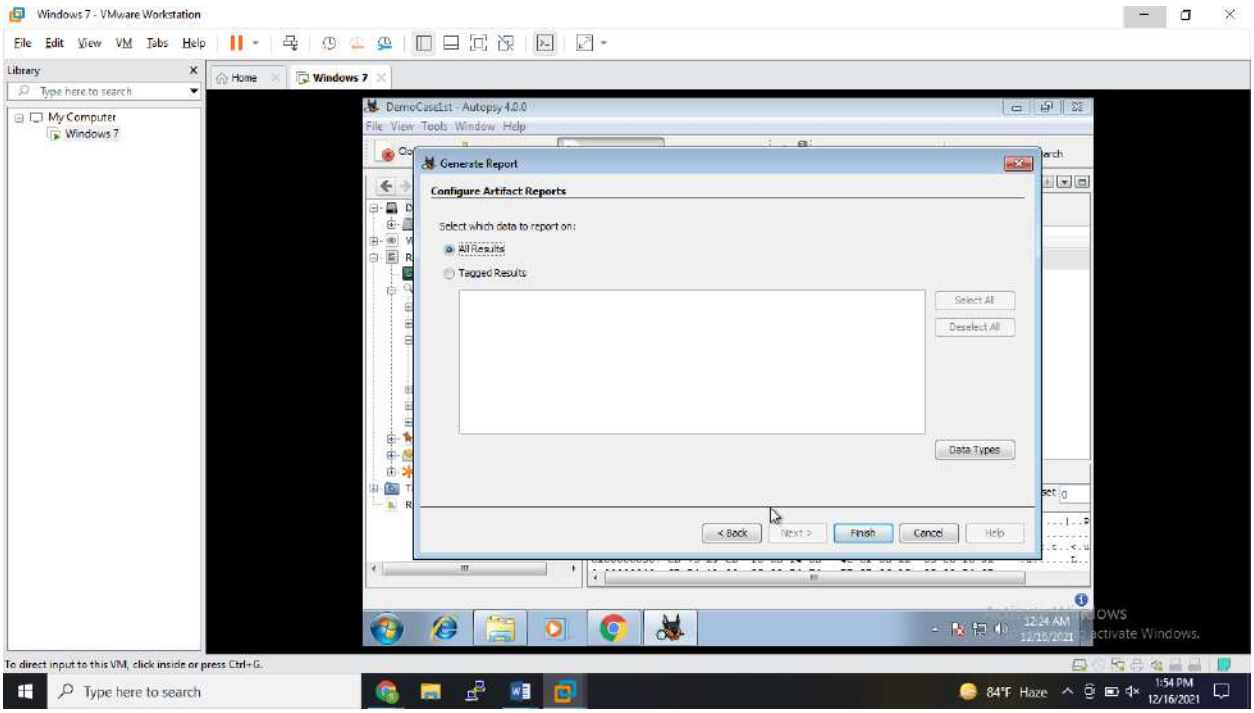

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
DemoCase1st - Autopsy 4.0.0
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword Search
Directory Listing
Images
Table
Thumbnail
Name
Location
Bibo Baggins.bmp
airplane.bmp
astronaut.bmp
ball.bmp
beach.bmp
butterfly.bmp
car.bmp
cat.bmp
chess.bmp
dirt bike.bmp
dirt bike.bmp
Hex
Strings
File Metadata
Media
Data Sources
Views
File Types
Images (283)
Videos (4)
Audio (4)
Archives (4)
Documents
Executable
Deleted Files
File Size
Results
Extracted Content
Keyword Hits
TEMP (49)
sample (25)
test (24)
IP Addresses (117)
Phone Numbers (24)
Email Addresses (253)
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
84°F Haze
1:50 PM
12/16/2021

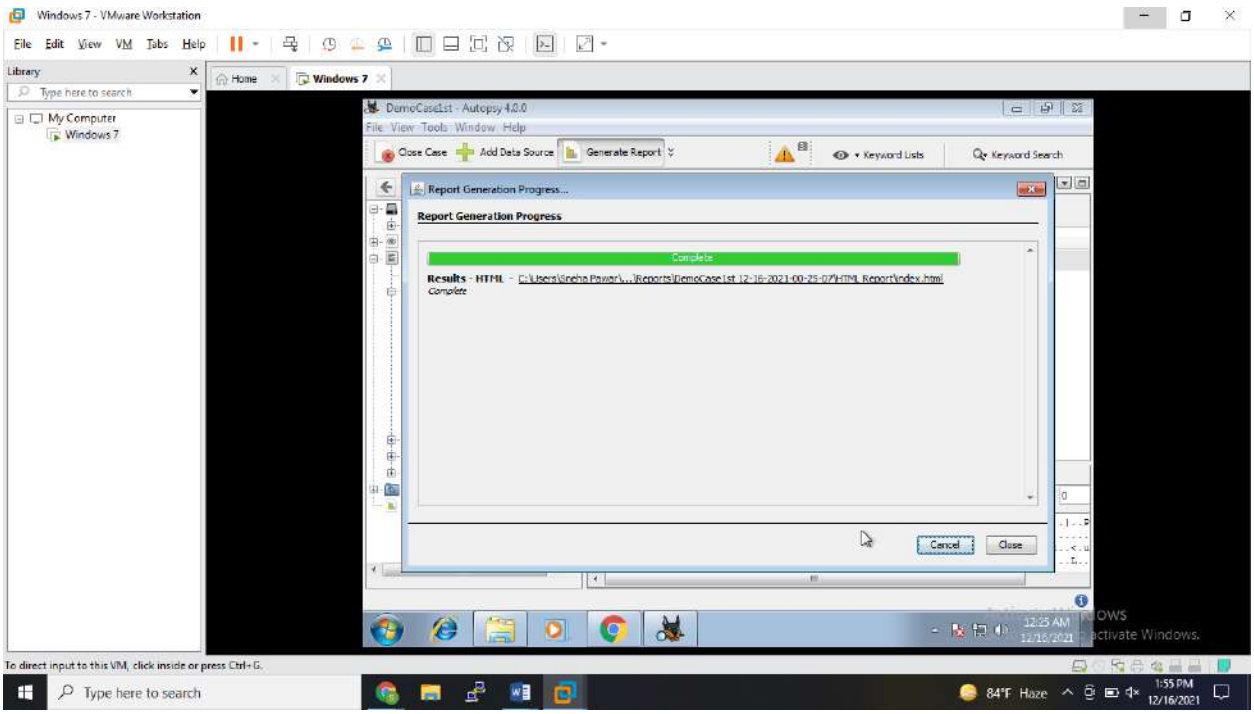

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
DemoCase1st - Autopsy 4.0.0
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword Search
Directory Listing
/img_precious.img/vol_vol2
Table
Thumbnail
Name
Modified Time
Change Time
Access
$Extend
$OrphanFiles
$Unalloc
[current folder]
Documents and Settings
Instruction Materials
My Music
My Shared Folder
Program Files
RECYCLER
Data Sources
precious.img
vol1 (Unallocated: 0-49663)
vol2 (NTFS / exFAT (0x07))
vol3 (Unallocated: 250624-3
Views
Results
Extracted Content
Keyword Hits
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
84°F Haze
1:51 PM
12/16/2021



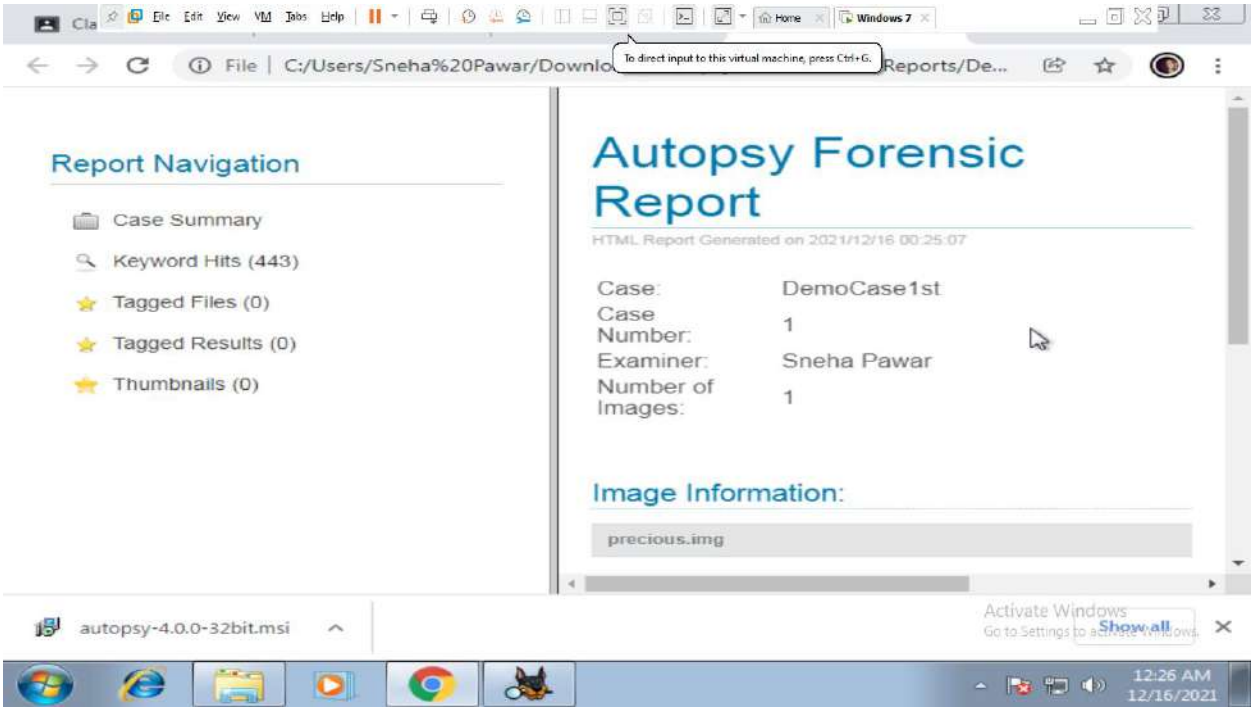
Then click on Generate Report.

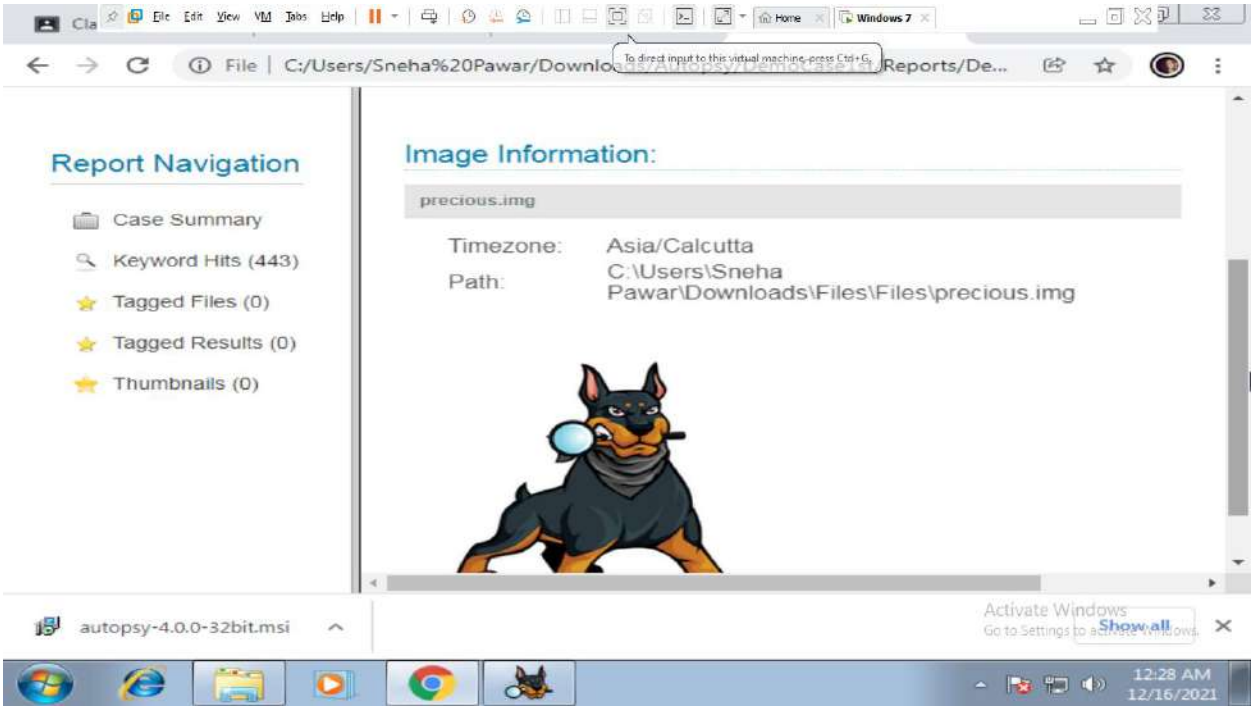


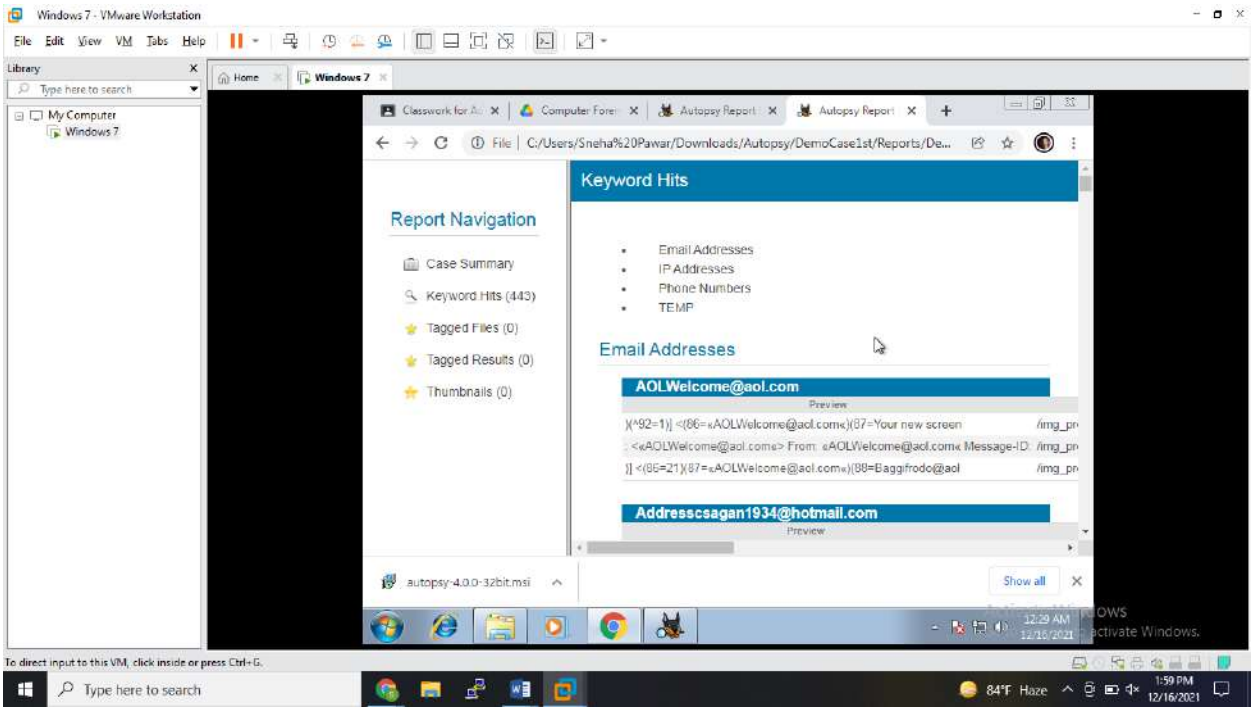




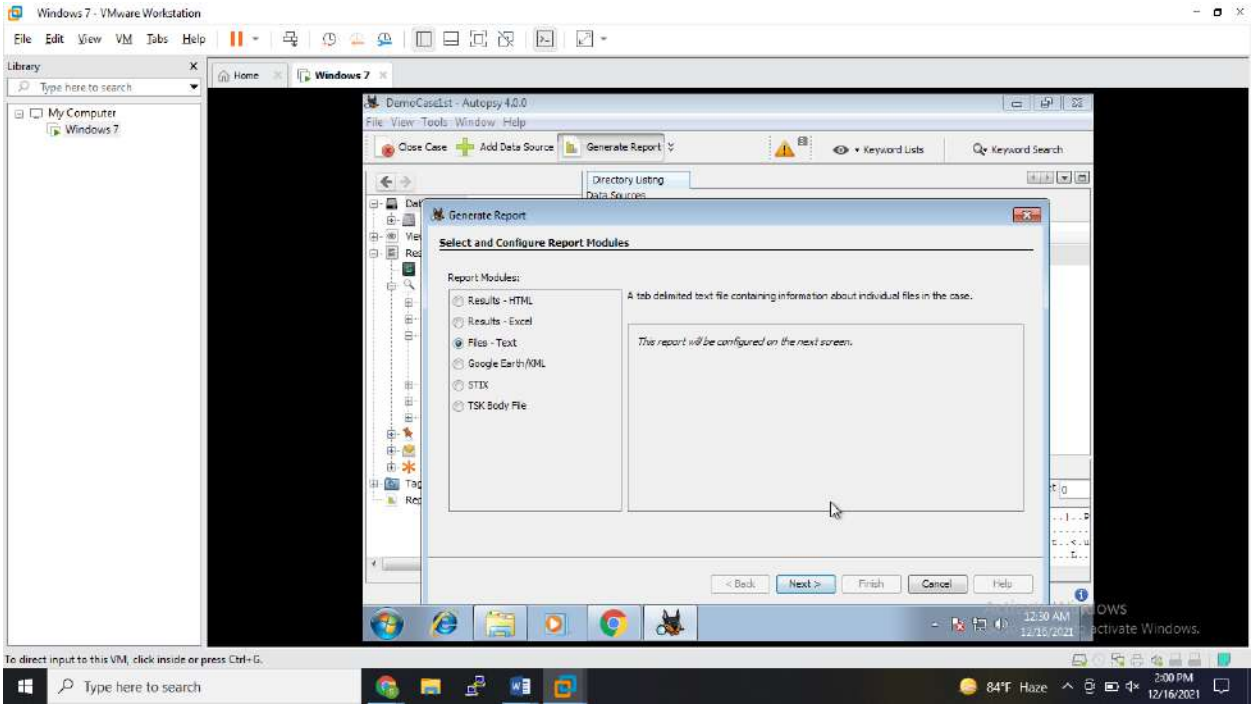
Double click on the link.

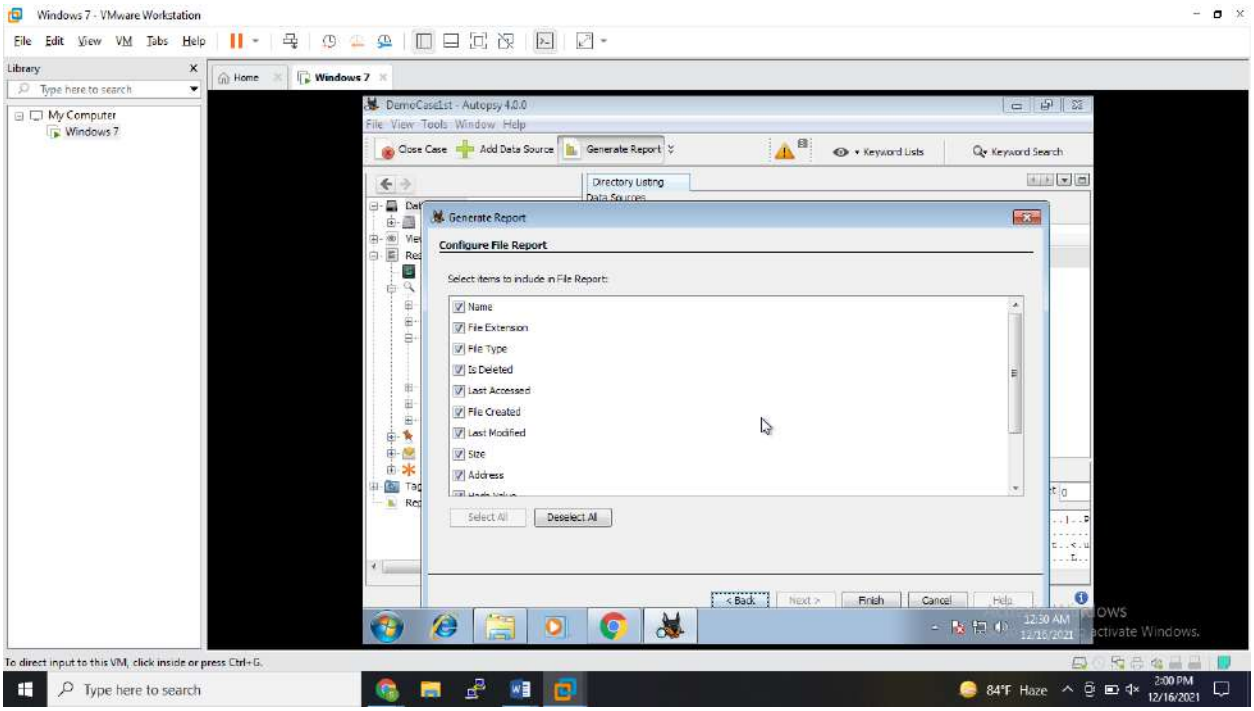

To direct input to this virtual machine, press Ctrl+G.
Report Navigation
Case Summary
Keyword Hits (443)
Tagged Files (0)
Tagged Results (0)
Thumbnails (0)
Autopsy Forensic Report
HTML Report Generated on 2021/12/16 00:25:07
Case: DemoCase1st
Case Number: 1
Examiner: Sneha Pawar
Number of Images: 1
Image Information:
precious.img
autopsy-4.0.0-32bit.msi
Activate Windows
Show all
12:26 AM
12/16/2021

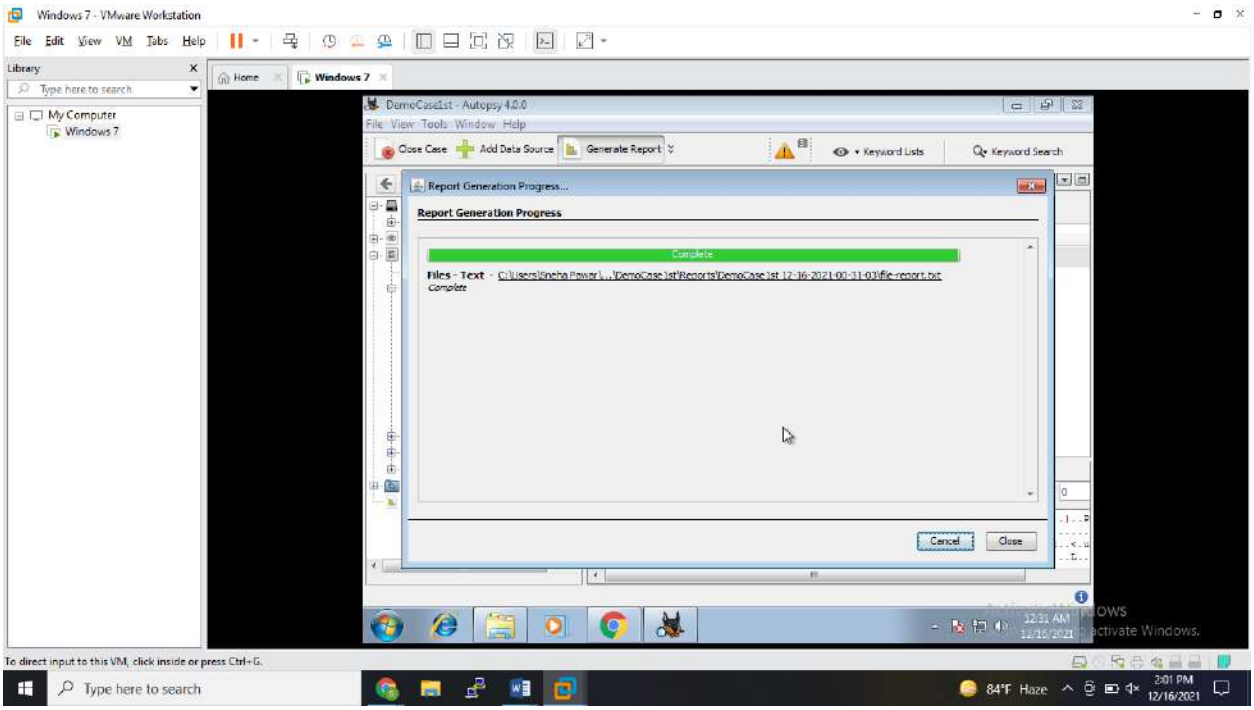

To direct input to this virtual machine, press Ctrl+G.
Report Navigation
Case Summary
Keyword Hits (443)
Tagged Files (0)
Tagged Results (0)
Thumbnails (0)
Image Information:
precious.img
Timezone: Asia/Calcutta
Path: C:\Users\Sneha Pawar\Downloads\Files\Files\precious.img
autopsy-4.0.0-32bit.msi
Activate Windows
Show all
12:28 AM
12/16/2021



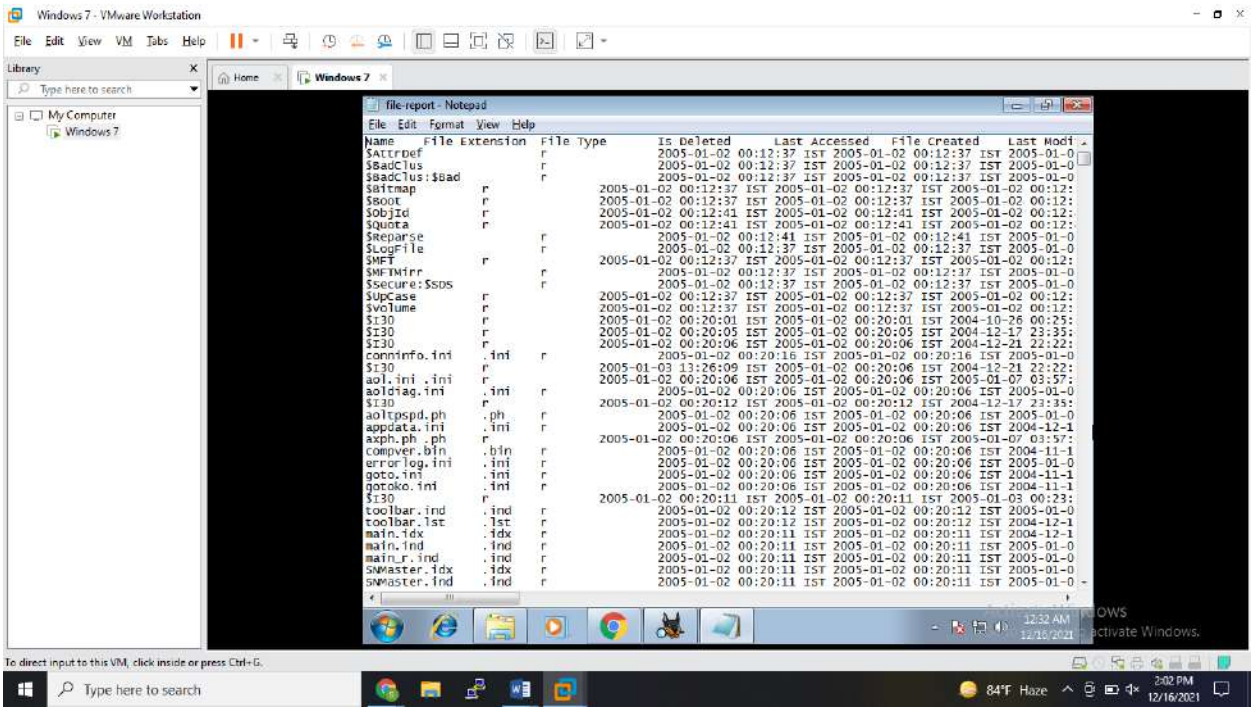
You can also generate report in text file.







Double click on link. Report in Text file will be generated.


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
file-report - Notepad
File Edit Format View Help
Name File Extension File Type Is Deleted Last Accessed File Created Last Modi
$AttrDef r 2005-01-02 00:12:37 IST 2005-01-02 00:12:37 IST 2005-01-0
$BadClus r 2005-01-02 00:12:37 IST 2005-01-02 00:12:37 IST 2005-01-0
$BadClus:$Bad r 2005-01-02 00:12:37 IST 2005-01-02 00:12:37 IST 2005-01-0
$Bitmap r 2005-01-02 00:12:37 IST 2005-01-02 00:12:37 IST 2005-01-02 00:12:
$Boot r 2005-01-02 00:12:37 IST 2005-01-02 00:12:37 IST 2005-01-02 00:12:
$ObjId r 2005-01-02 00:12:41 IST 2005-01-02 00:12:41 IST 2005-01-02 00:12:
$Quota r 2005-01-02 00:12:41 IST 2005-01-02 00:12:41 IST 2005-01-02 00:12:
$Reparse r 2005-01-02 00:12:41 IST 2005-01-02 00:12:41 IST 2005-01-0
$LogFile r 2005-01-02 00:12:37 IST 2005-01-02 00:12:37 IST 2005-01-0
$MFT r 2005-01-02 00:12:37 IST 2005-01-02 00:12:37 IST 2005-01-02 00:12:
$MFTMirr r 2005-01-02 00:12:37 IST 2005-01-02 00:12:37 IST 2005-01-0
$Secure:$SDS r 2005-01-02 00:12:37 IST 2005-01-02 00:12:37 IST 2005-01-0
$UpCase r 2005-01-02 00:12:37 IST 2005-01-02 00:12:37 IST 2005-01-02 00:12:
$Volume r 2005-01-02 00:12:37 IST 2005-01-02 00:12:37 IST 2005-01-02 00:12:
$I30 r 2005-01-02 00:20:01 IST 2005-01-02 00:20:01 IST 2004-10-26 00:25:
$I30 r 2005-01-02 00:20:05 IST 2005-01-02 00:20:05 IST 2004-12-17 23:35:
$I30 r 2005-01-02 00:20:06 IST 2005-01-02 00:20:06 IST 2004-12-21 22:22:
conninfo.ini .ini r 2005-01-02 00:20:16 IST 2005-01-02 00:20:16 IST 2005-01-0
$I30 r 2005-01-03 13:26:09 IST 2005-01-02 00:20:06 IST 2004-12-21 22:22:
aol.ini .ini r 2005-01-02 00:20:06 IST 2005-01-02 00:20:06 IST 2005-01-07 03:57:
aoldiag.ini .ini r 2005-01-02 00:20:06 IST 2005-01-02 00:20:06 IST 2005-01-0
$I30 r 2005-01-02 00:20:12 IST 2005-01-02 00:20:12 IST 2004-12-17 23:35:
aoltpspd.ph .ph r 2005-01-02 00:20:06 IST 2005-01-02 00:20:06 IST 2005-01-0
appdata.ini .ini r 2005-01-02 00:20:06 IST 2005-01-02 00:20:06 IST 2004-12-1
axph.ph .ph r 2005-01-02 00:20:06 IST 2005-01-02 00:20:06 IST 2005-01-07 03:57:
compver.bin .bin r 2005-01-02 00:20:06 IST 2005-01-02 00:20:06 IST 2004-11-1
errorlog.ini .ini r 2005-01-02 00:20:06 IST 2005-01-02 00:20:06 IST 2005-01-0
goto.ini .ini r 2005-01-02 00:20:06 IST 2005-01-02 00:20:06 IST 2004-11-1
gotoko.ini .ini r 2005-01-02 00:20:06 IST 2005-01-02 00:20:06 IST 2004-11-1
$I30 r 2005-01-02 00:20:11 IST 2005-01-02 00:20:11 IST 2005-01-03 00:23:
toolbar.ind .ind r 2005-01-02 00:20:12 IST 2005-01-02 00:20:12 IST 2005-01-0
toolbar.lst .lst r 2005-01-02 00:20:12 IST 2005-01-02 00:20:12 IST 2004-12-1
main.idx .idx r 2005-01-02 00:20:11 IST 2005-01-02 00:20:11 IST 2004-12-1
main.ind .ind r 2005-01-02 00:20:11 IST 2005-01-02 00:20:11 IST 2005-01-0
main_r.ind .ind r 2005-01-02 00:20:11 IST 2005-01-02 00:20:11 IST 2005-01-0
SNMaster.idx .idx r 2005-01-02 00:20:11 IST 2005-01-02 00:20:11 IST 2005-01-0
SNMaster.ind .ind r 2005-01-02 00:20:11 IST 2005-01-02 00:20:11 IST 2005-01-0
12:32 AM
12/16/2021
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
84°F Haze
2:02 PM
12/16/2021

Practical No. 02

Aim: Using Windows Forensics Toolkit [AccessData FTK].

What is AccessData FTK Tool?

Forensic Toolkit, or FTK, is a computer forensics software made by AccessData. It **scans a hard drive looking for various information**. It can, for example, potentially locate deleted emails and scan a disk for text strings to use them as a password dictionary to crack encryption.

FTK provides an **intuitive interface for email analysis** for forensic professionals. This includes having the ability to parse emails for certain words, header analysis for source IP address, etc. A central feature of FTK, file decryption is arguably the most common use of the software.

Steps:

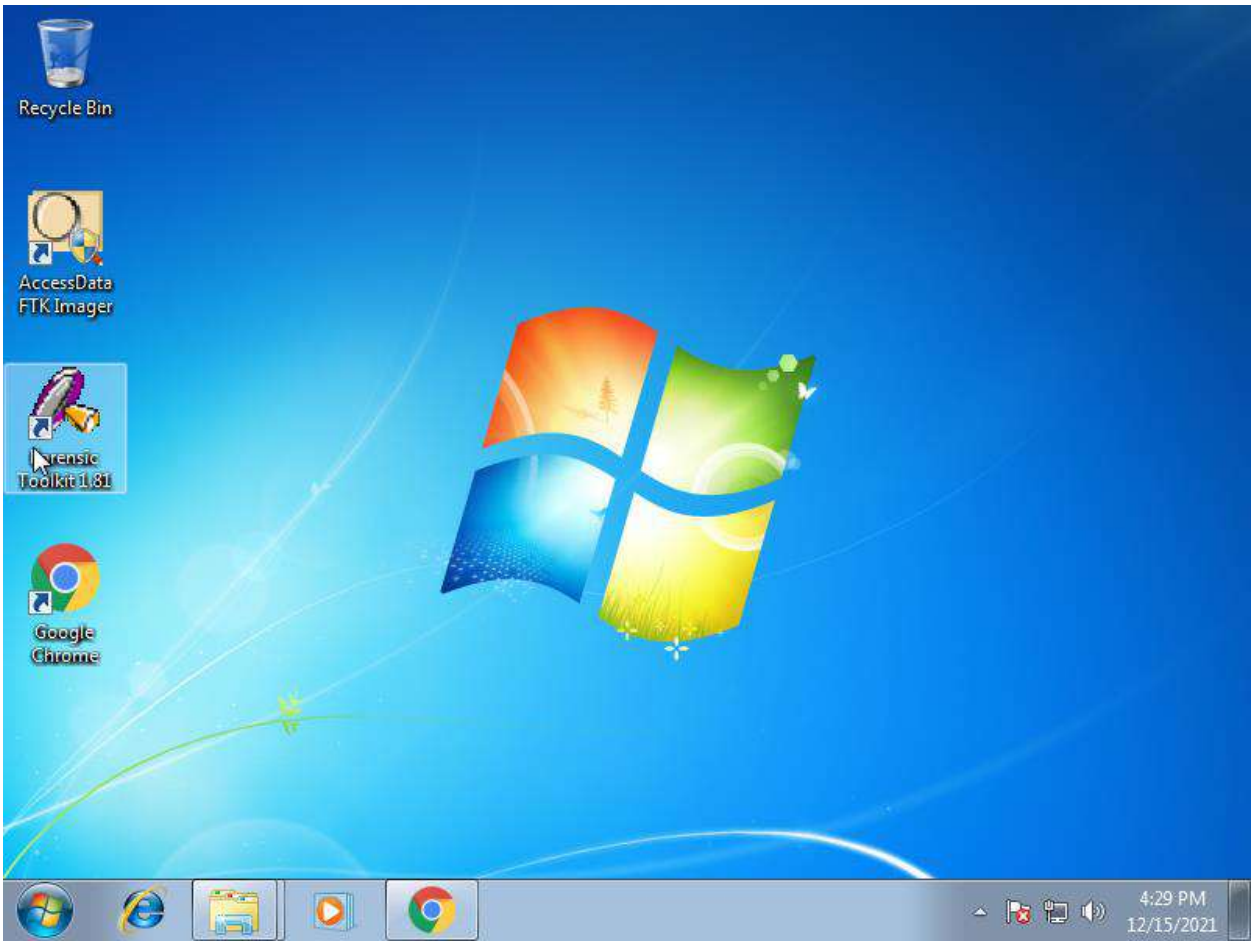
In this practical we will see how to create case, add evidence, generate reports.

After generating any case and adding evidences related to that case you can generate report by using the AccessData FTK tool.

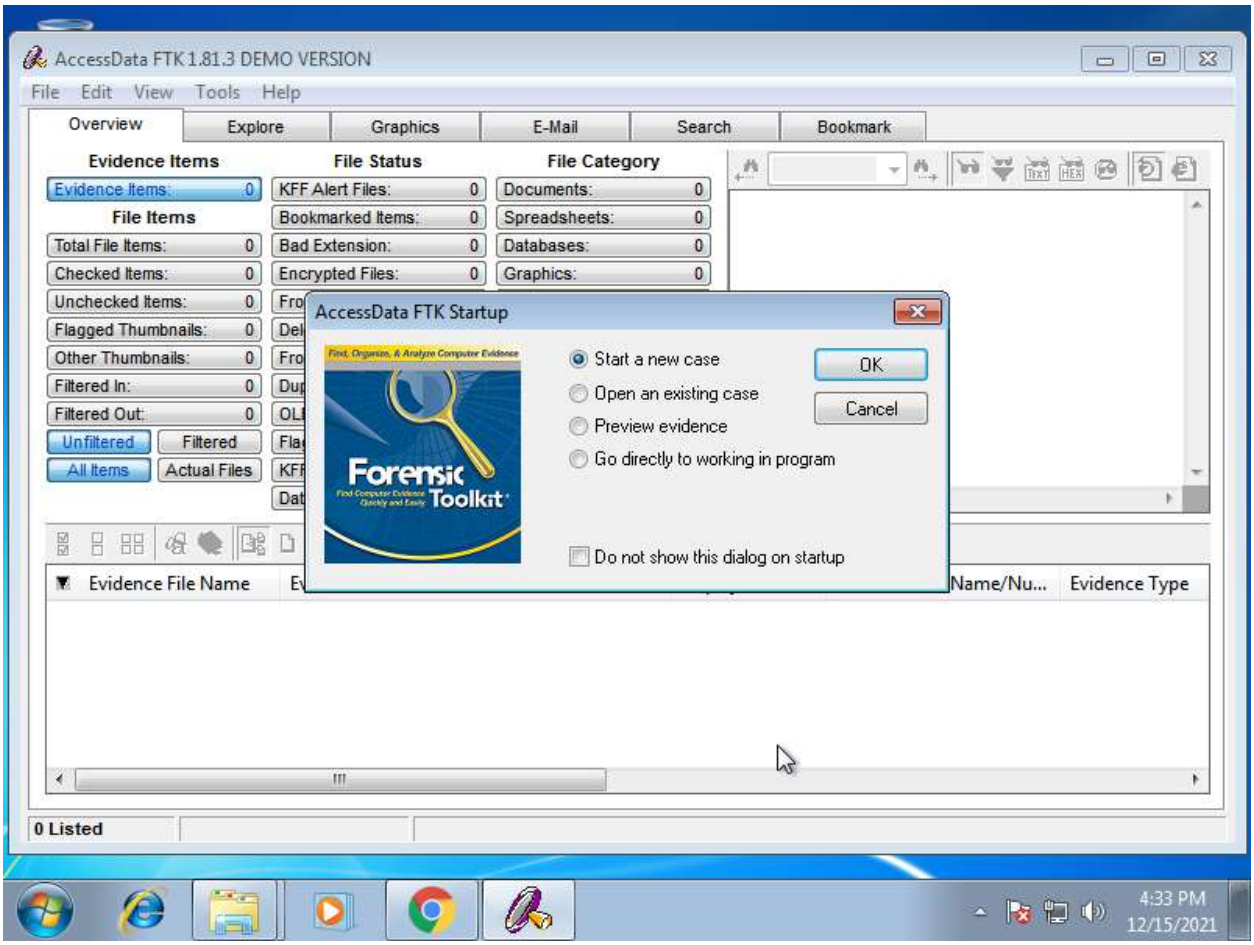
Following are the steps to create case add evidence and generate report using AccessData FTK tool.

To perform this practical you can take reference of Practical No. 08. In this I have added one case related evidences for that and generated reports for the case.

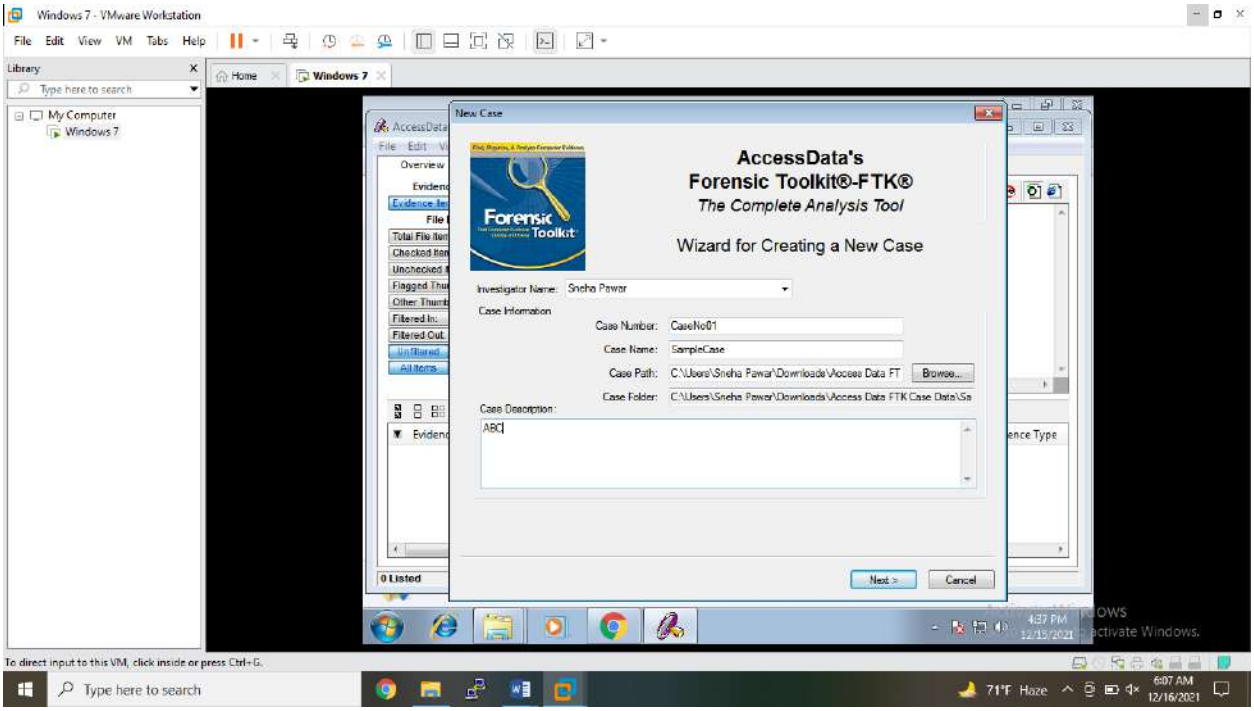
Start the forensic toolkit software.



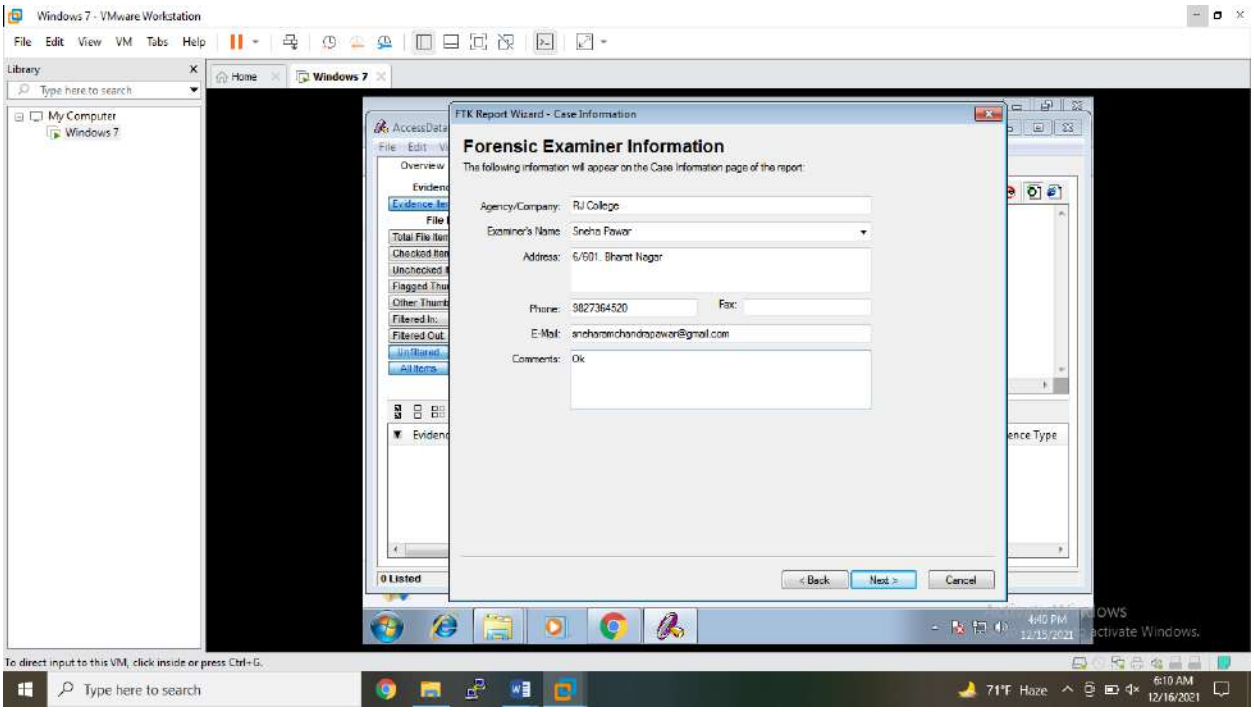
Select Start a New Case.



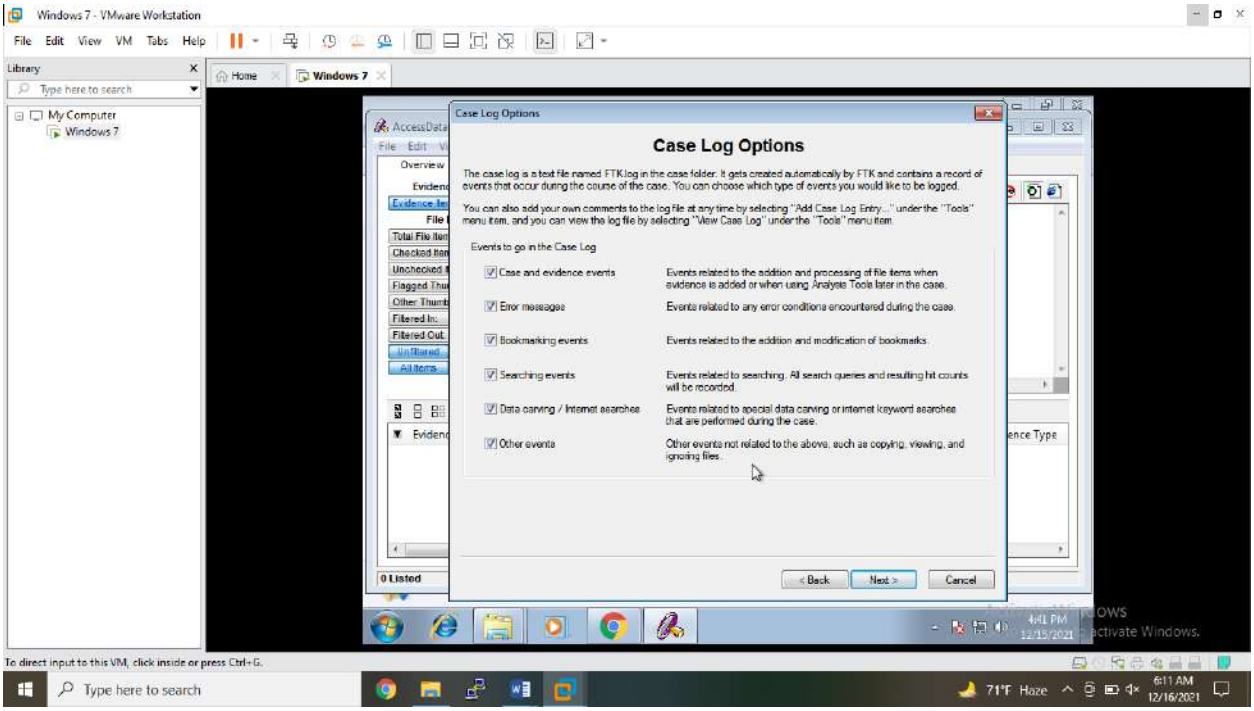
Then enter investigator's name and other details and click on Next.

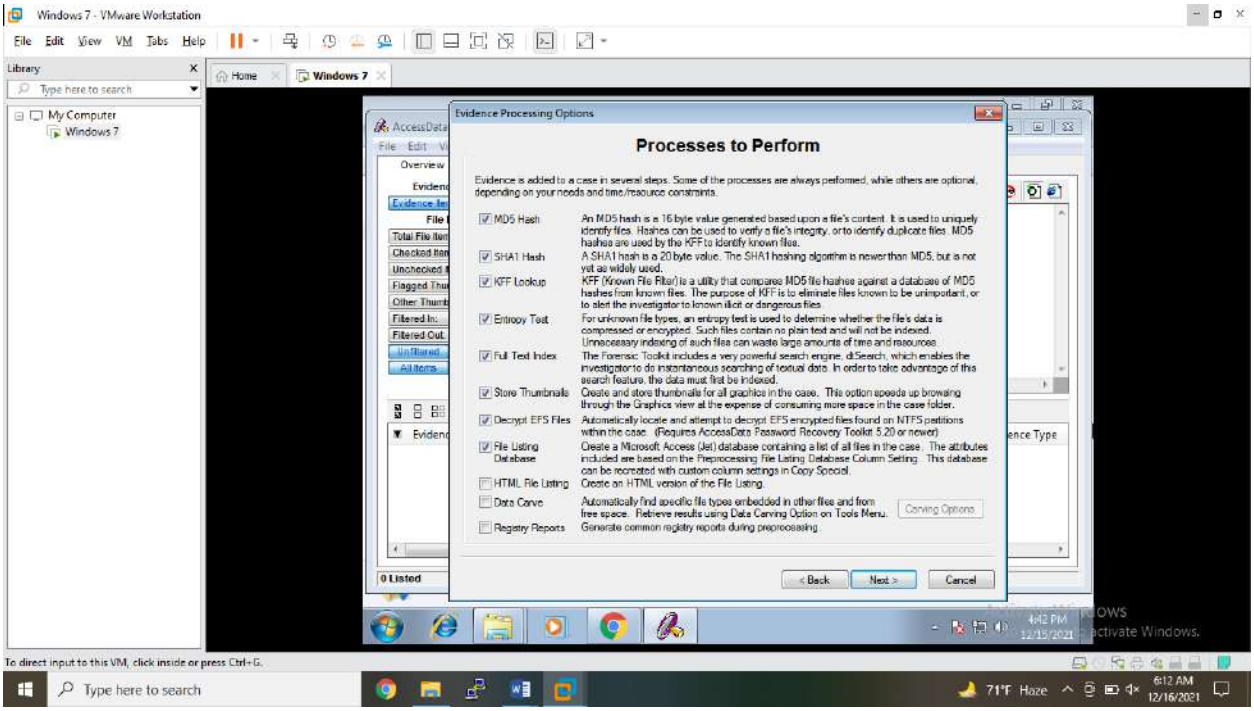


Then enter forensic examiner's details.

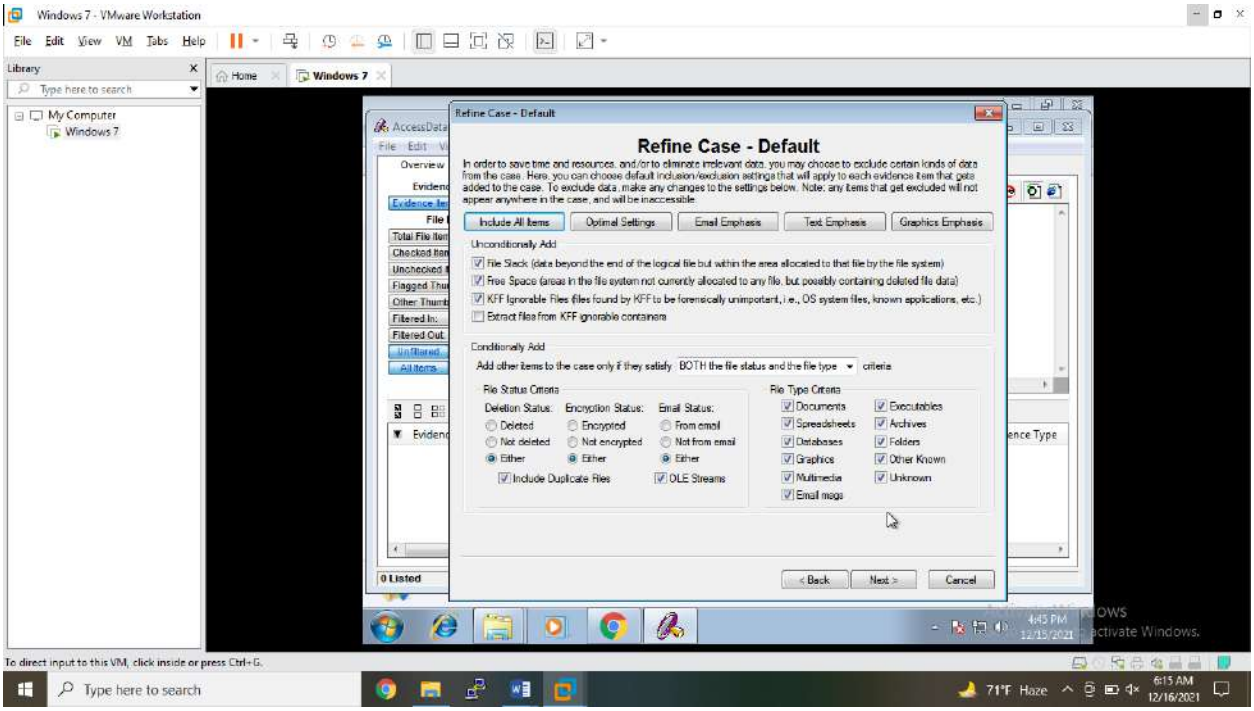


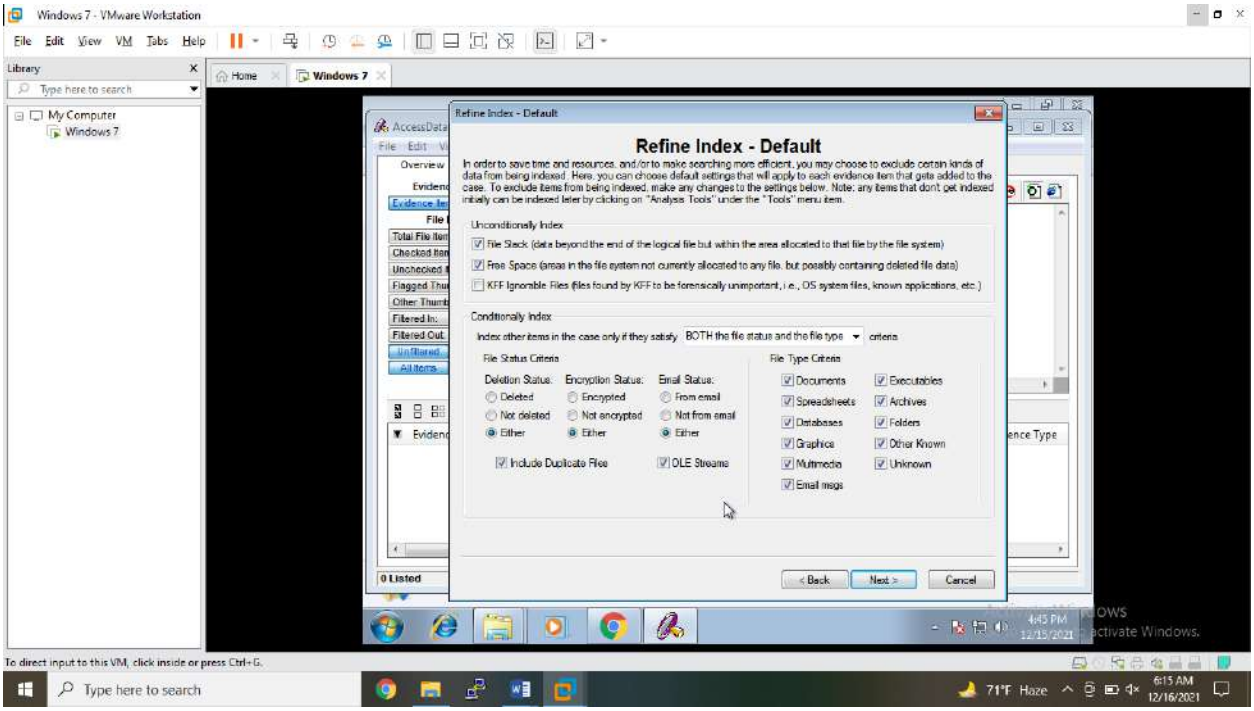
In Case Log Options & Process to perform tabs, keep everything by default.



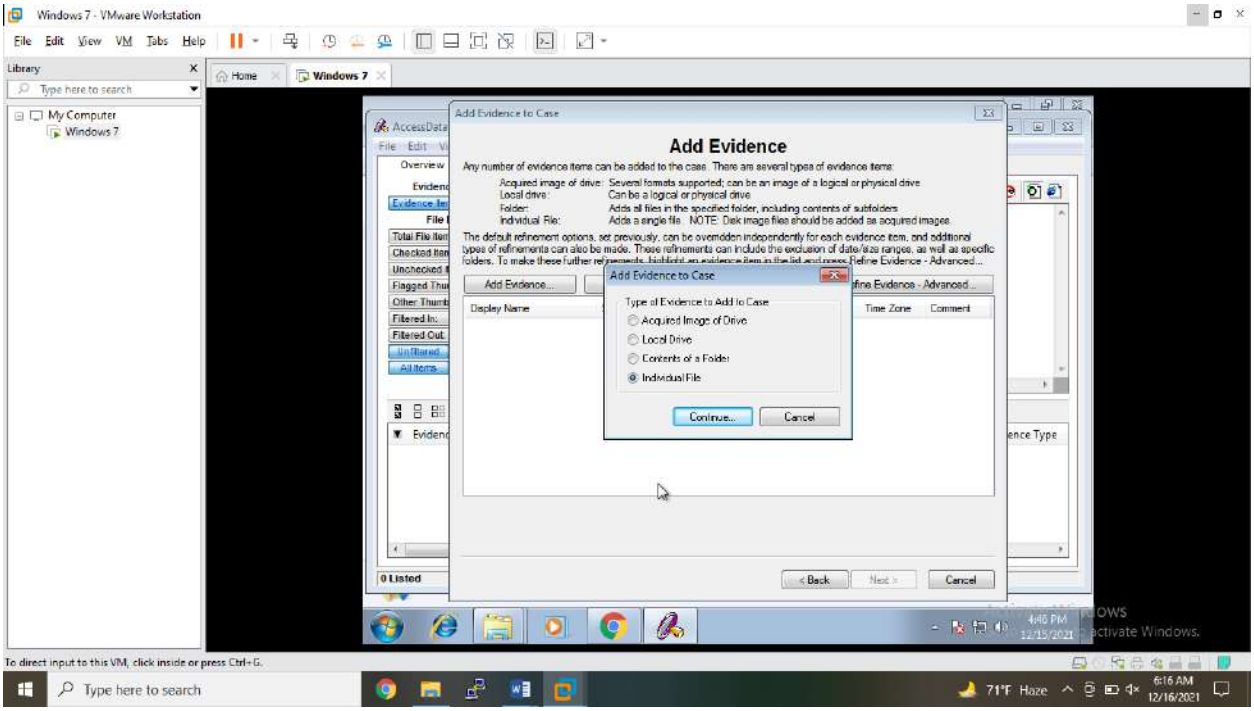


Then in Refine Case Default, Keep everything as it is, and click on Next.

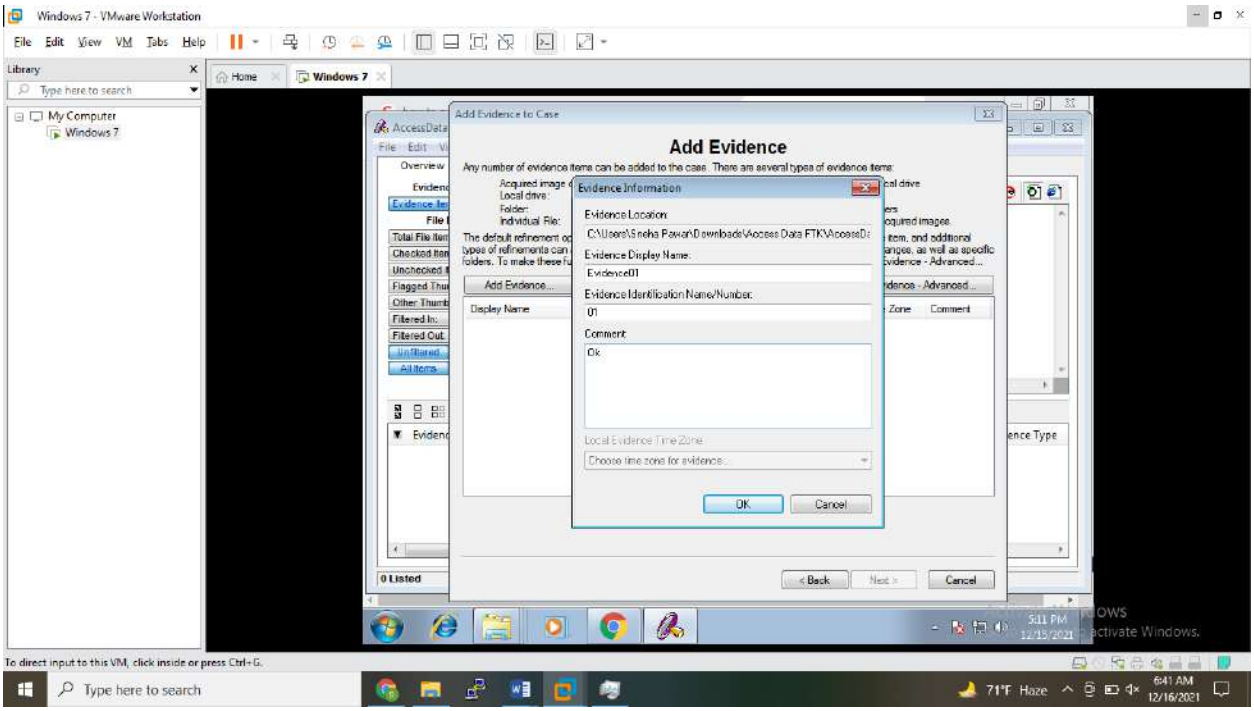


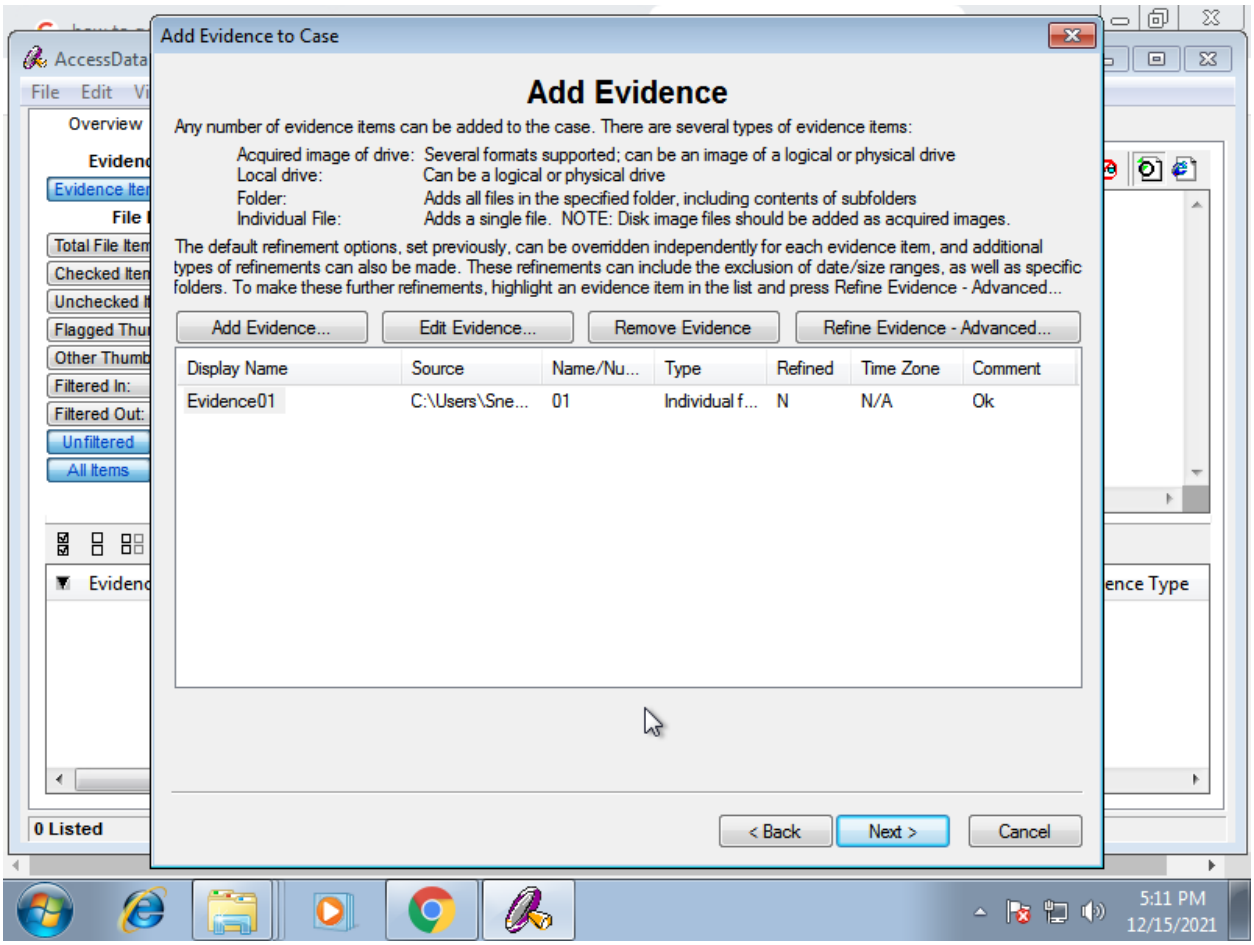


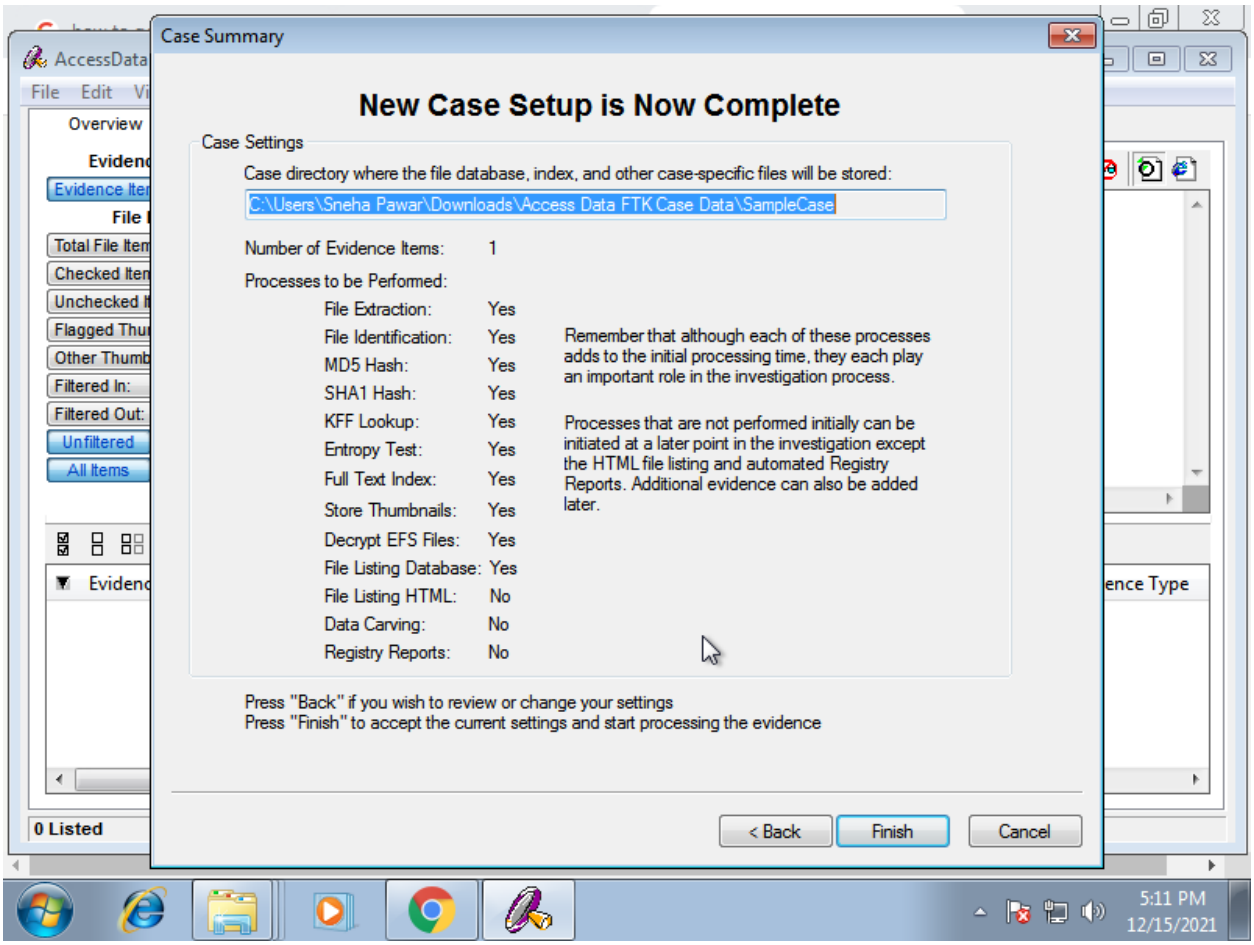
Then click on Add Evidence – Add Individual File.



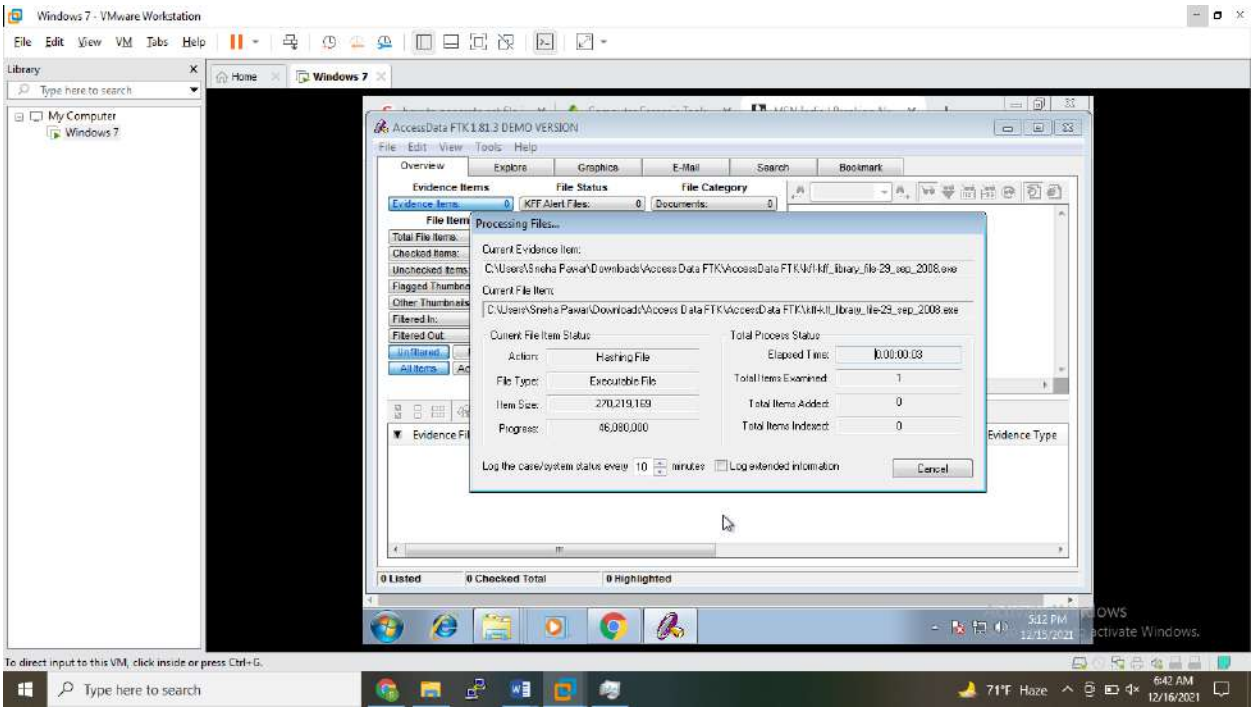
Then Browse for Evidence location, and enter other details.

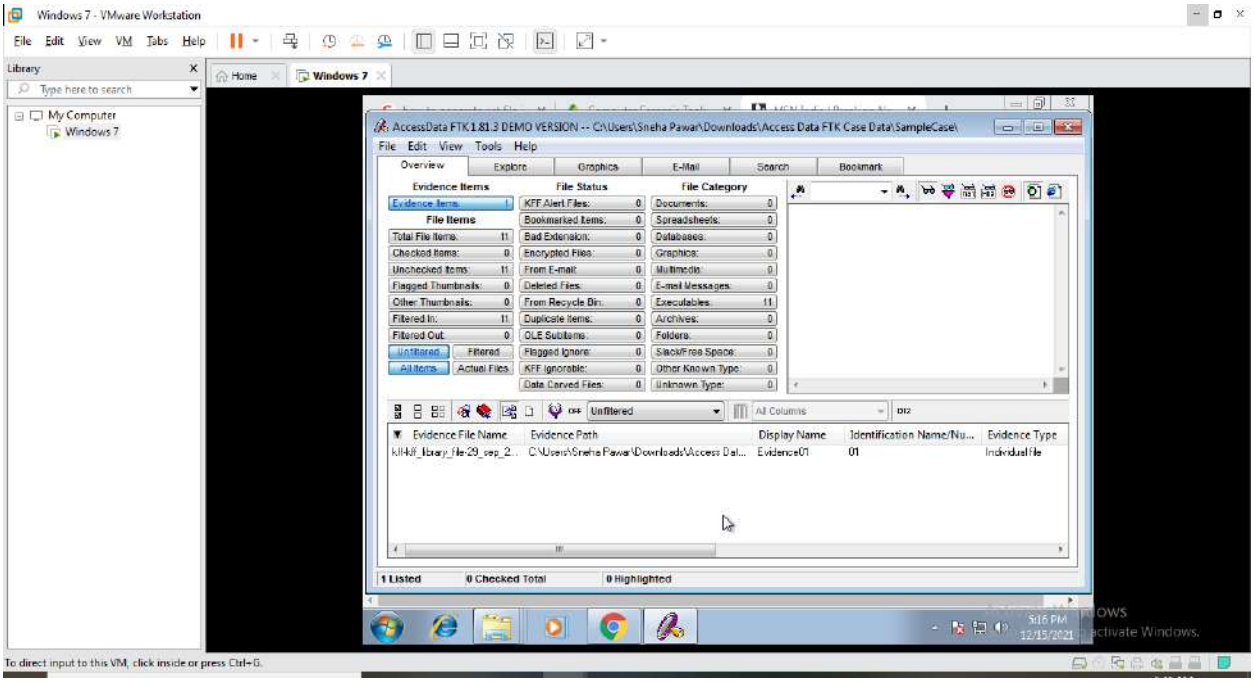


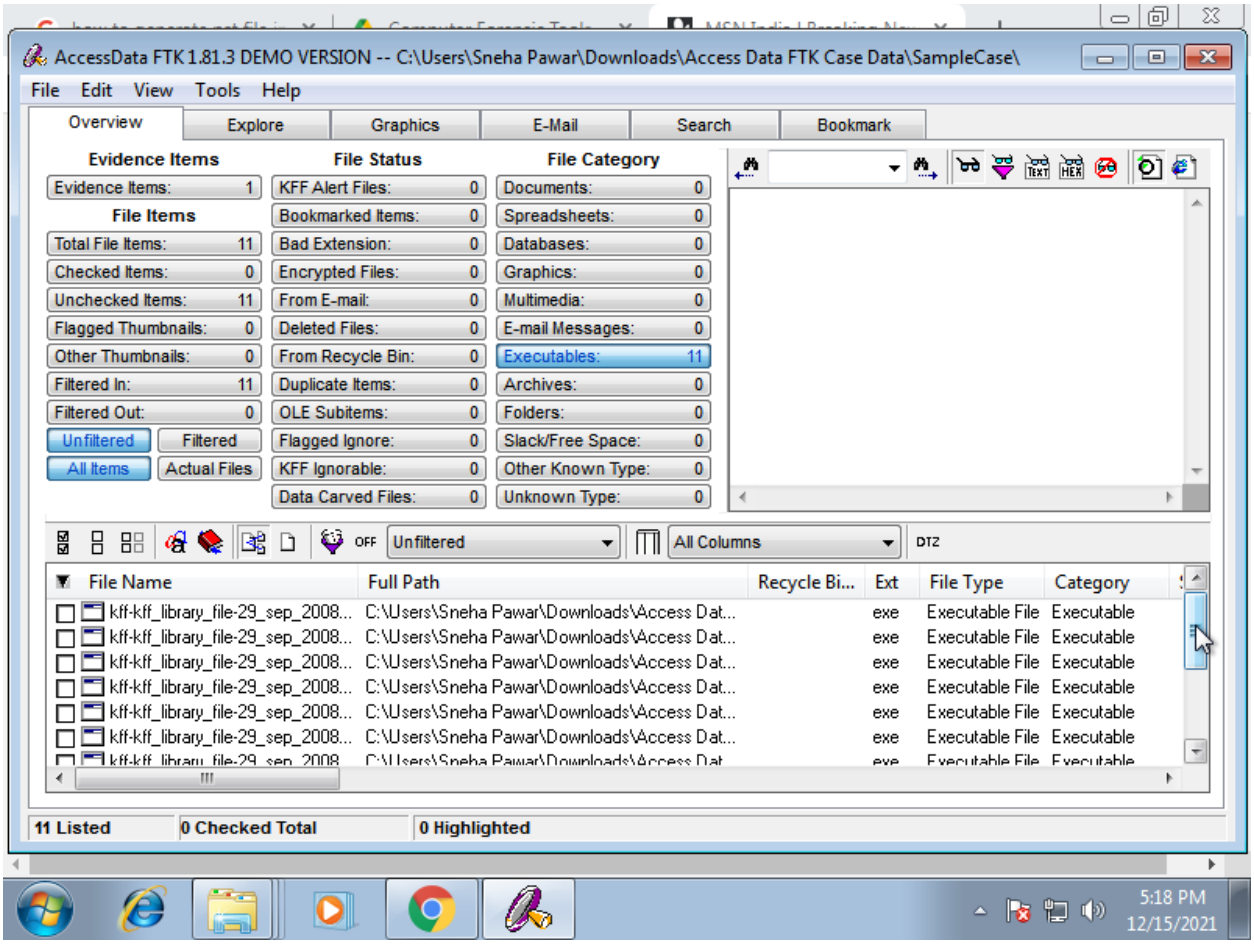

Add Evidence to Case
Add Evidence
Any number of evidence items can be added to the case. There are several types of evidence items:
Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
Local drive: Can be a logical or physical drive
Folder: Adds all files in the specified folder, including contents of subfolders
Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.
The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...
Add Evidence...
Edit Evidence...
Remove Evidence
Refine Evidence - Advanced...
Display Name
Source
Name/Nu...
Type
Refined
Time Zone
Comment
Evidence01
C:\Users\Sne...
01
Individual f...
N
N/A
Ok
< Back
Next >
Cancel
0 Listed
5:11 PM
12/15/2021



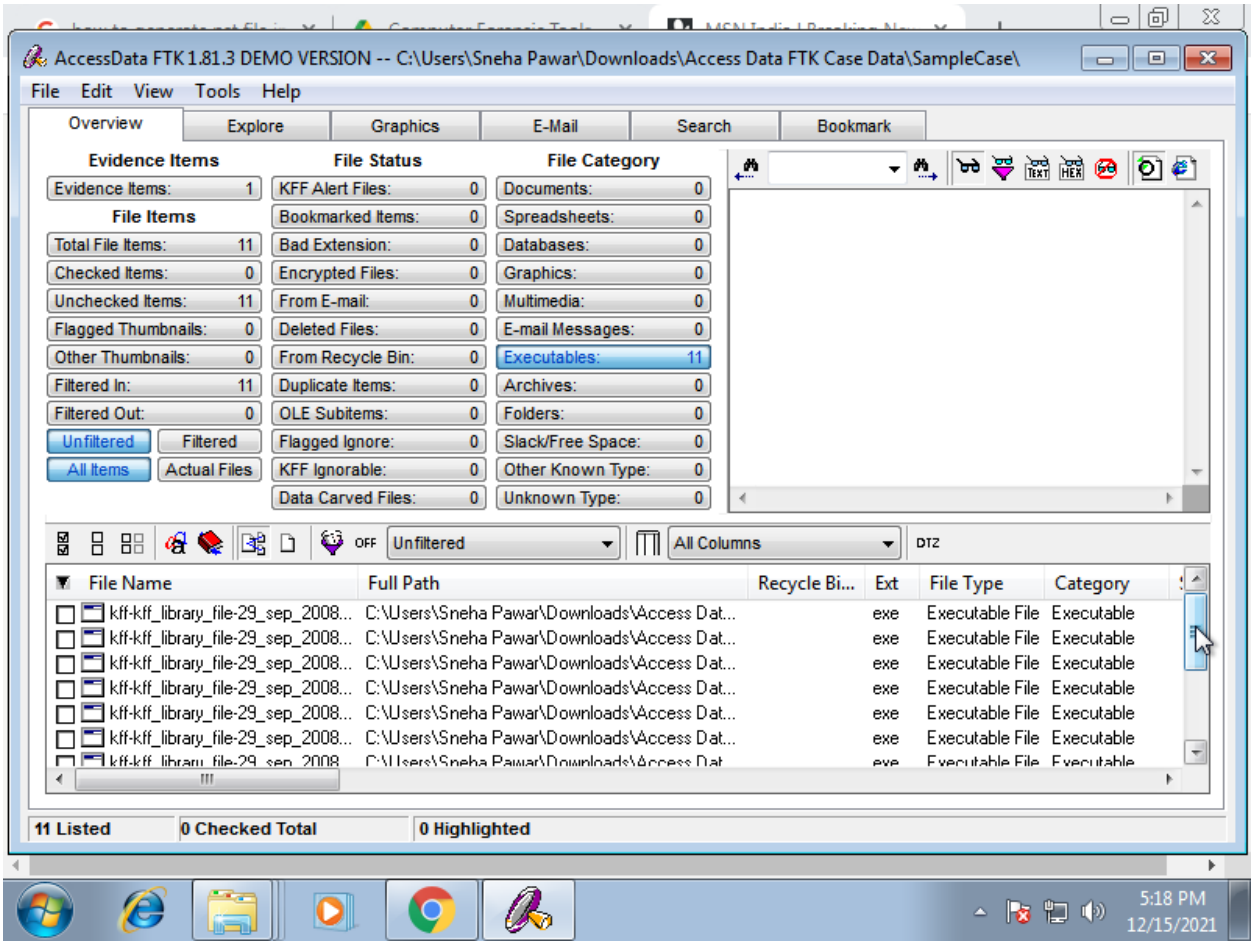
Click on Finish. It will start processing the File.

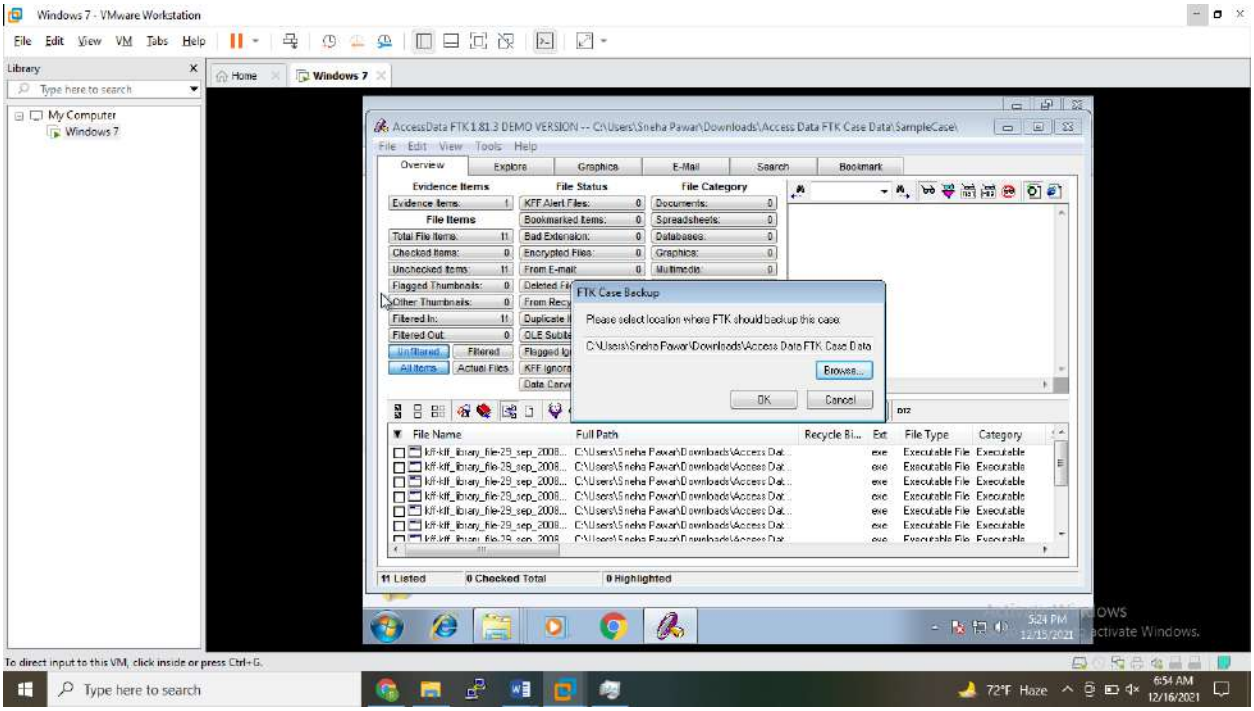


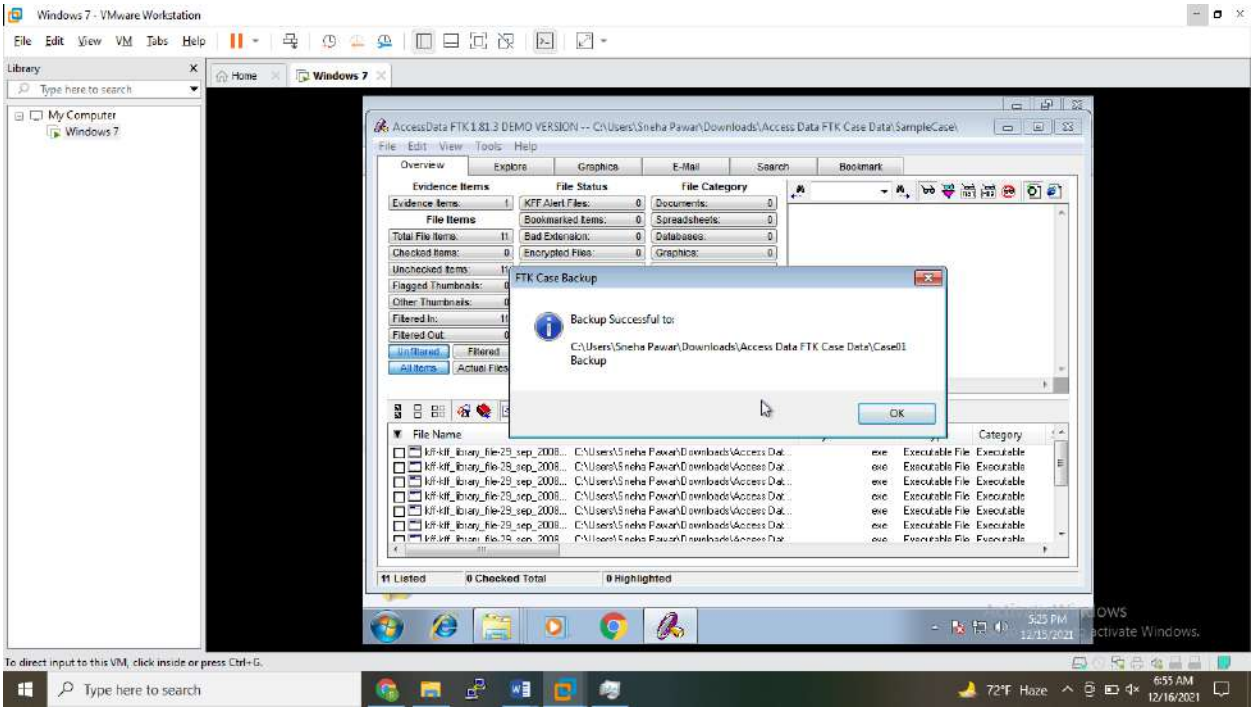

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Evidence Items
File Status
File Category
Evidence Items: 1
File Items
Total File Items: 11
Checked Items: 0
Unchecked Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 11
Filtered Out: 0
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 0
Encrypted Files: 0
From E-mail: 0
Deleted Files: 0
From Recycle Bin: 0
Duplicate Items: 0
OLE Subitems: 0
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0
Documents: 0
Spreadsheets: 0
Databases: 0
Graphics: 0
Multimedia: 0
E-mail Messages: 0
Executables: 11
Archives: 0
Folders: 0
Slack/Free Space: 0
Other Known Type: 0
Unknown Type: 0
Unfiltered
Filtered
All Items
Actual Files
Unfiltered
All Columns
DTZ
Evidence File Name
Evidence Path
Display Name
Identification Name/Nu...
Evidence Type
kff-kff_library_file-29_sep_2...
C:\Users\Sneha Pawar\Downloads\Access Dat...
Evidence01
01
Individual File
1 Listed
0 Checked Total
0 Highlighted
5:16 PM
12/15/2021
To direct input to this VM, click inside or press Ctrl+G.


AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Evidence Items
File Status
File Category
Evidence Items: 1
File Items
Total File Items: 11
Checked Items: 0
Unchecked Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 11
Filtered Out: 0
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 0
Encrypted Files: 0
From E-mail: 0
Deleted Files: 0
From Recycle Bin: 0
Duplicate Items: 0
OLE Subitems: 0
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0
Documents: 0
Spreadsheets: 0
Databases: 0
Graphics: 0
Multimedia: 0
E-mail Messages: 0
Executables: 11
Archives: 0
Folders: 0
Slack/Free Space: 0
Other Known Type: 0
Unknown Type: 0
Unfiltered
Filtered
All Items
Actual Files
OFF
Unfiltered
All Columns
DTZ
File Name
Full Path
Recycle Bi...
Ext
File Type
Category
kff-kff_library_file-29_sep_2008...
C:\Users\Sneha Pawar\Downloads\Access Dat...
exe
Executable File
Executable
11 Listed
0 Checked Total
0 Highlighted
5:18 PM
12/15/2021

To take backup of your case, Click on File – Backup Case – And browse for location where you want to take backup.

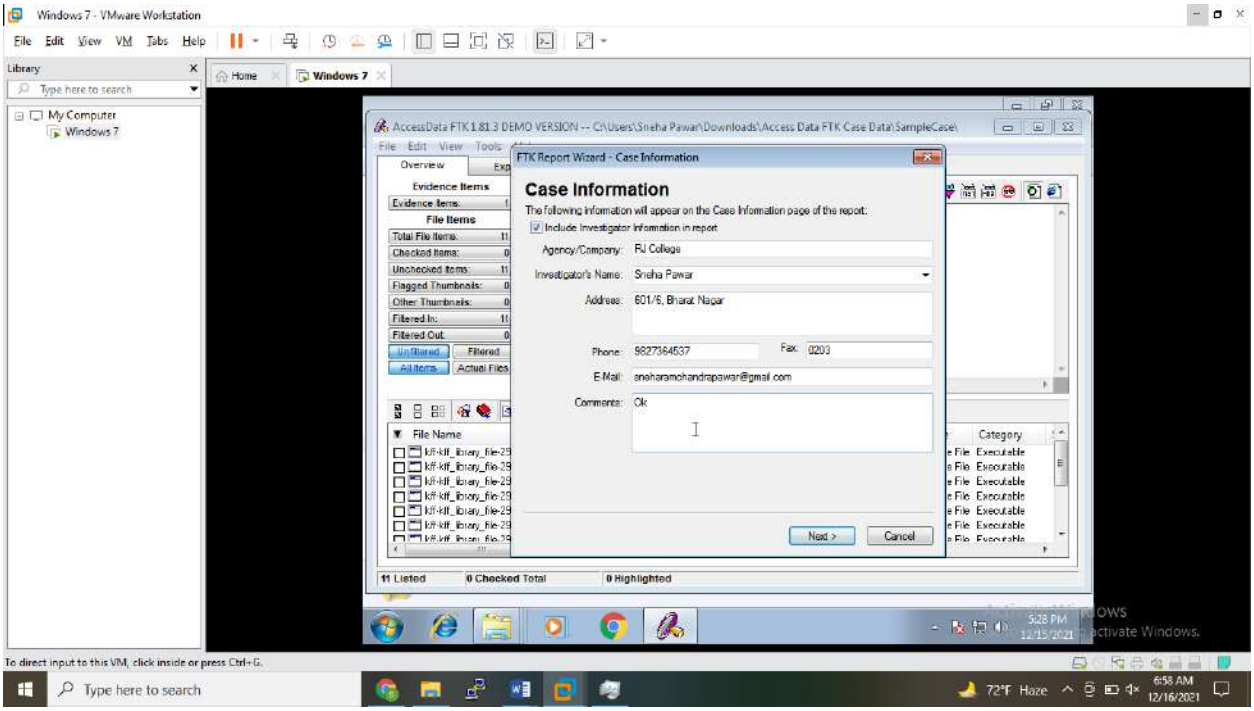


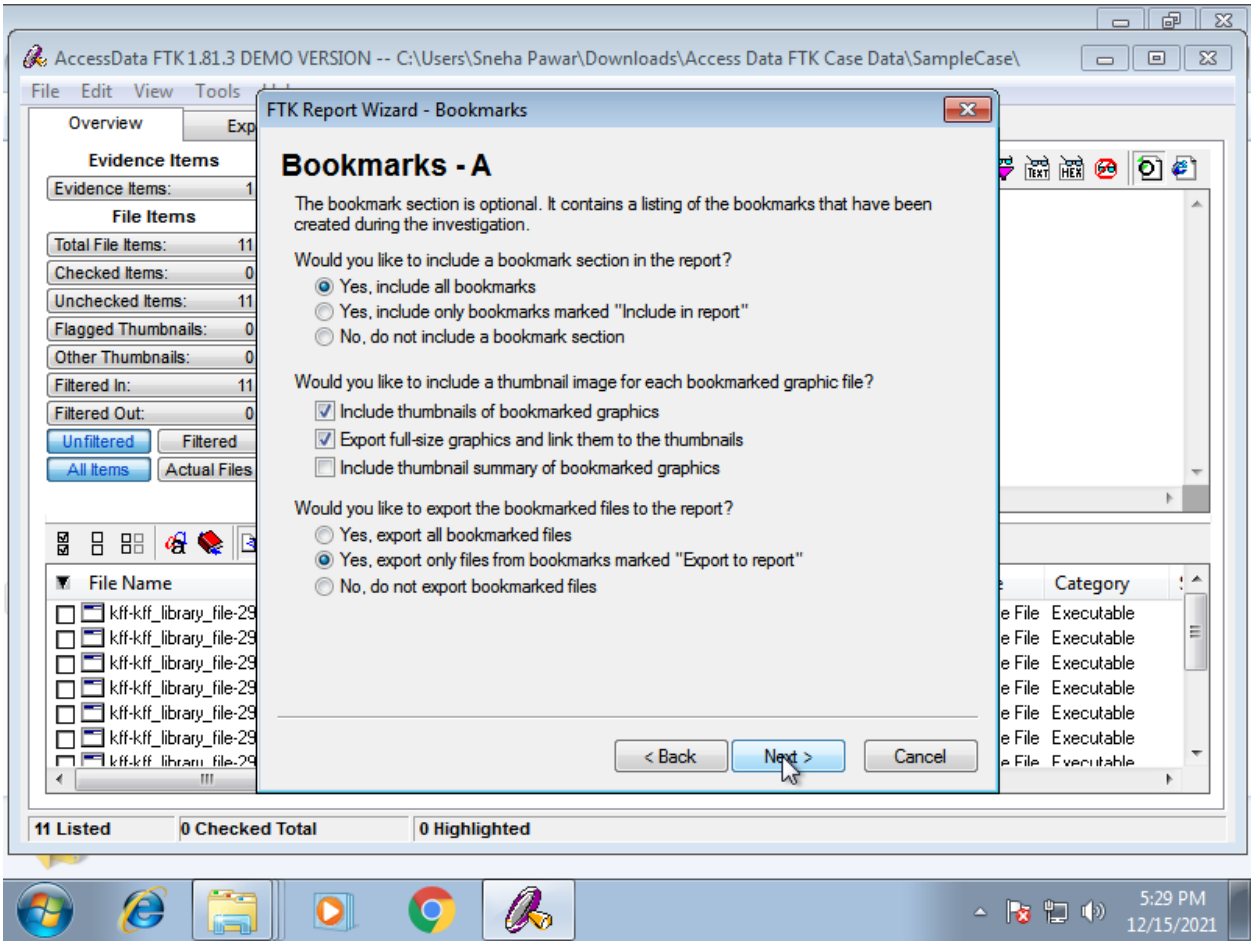


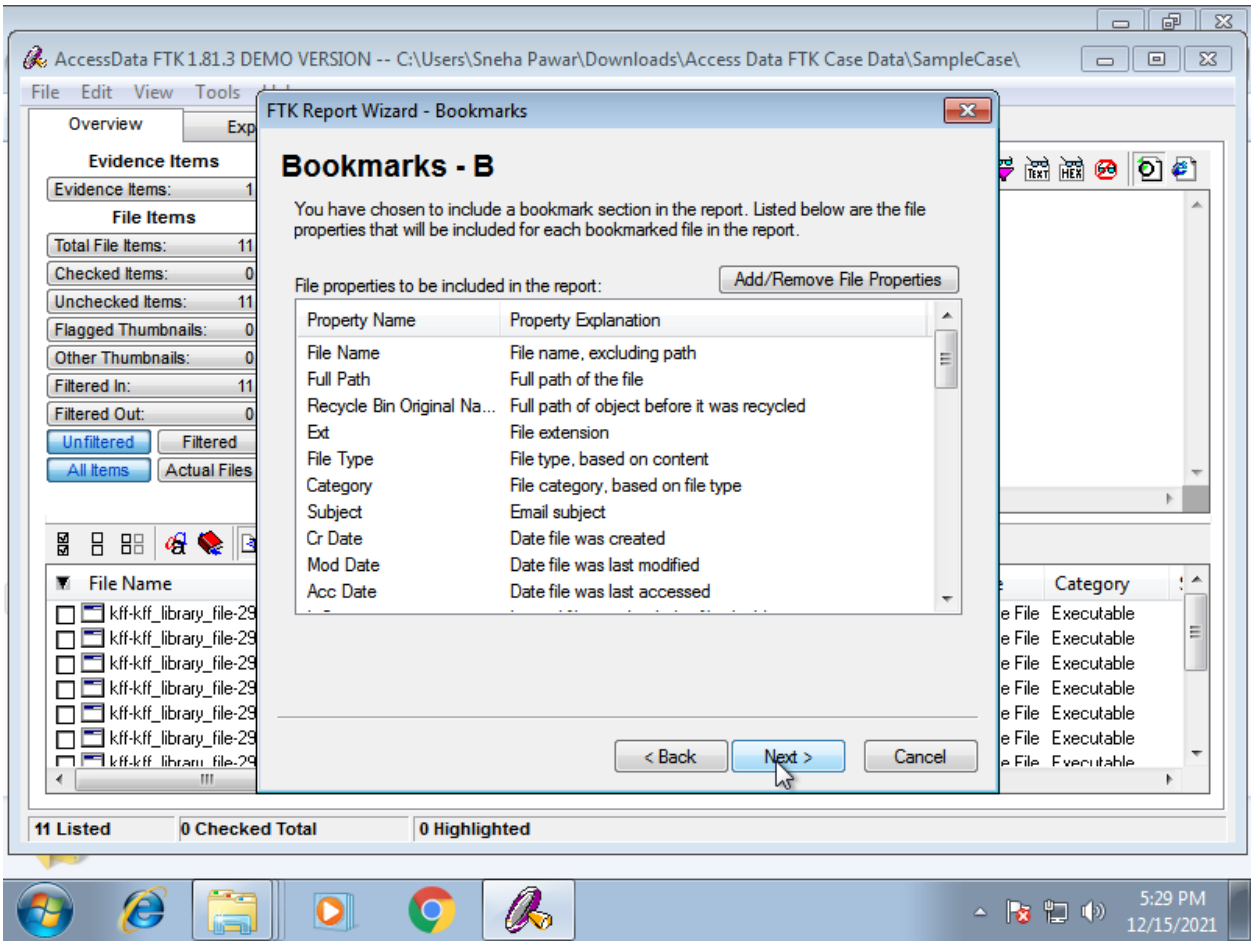


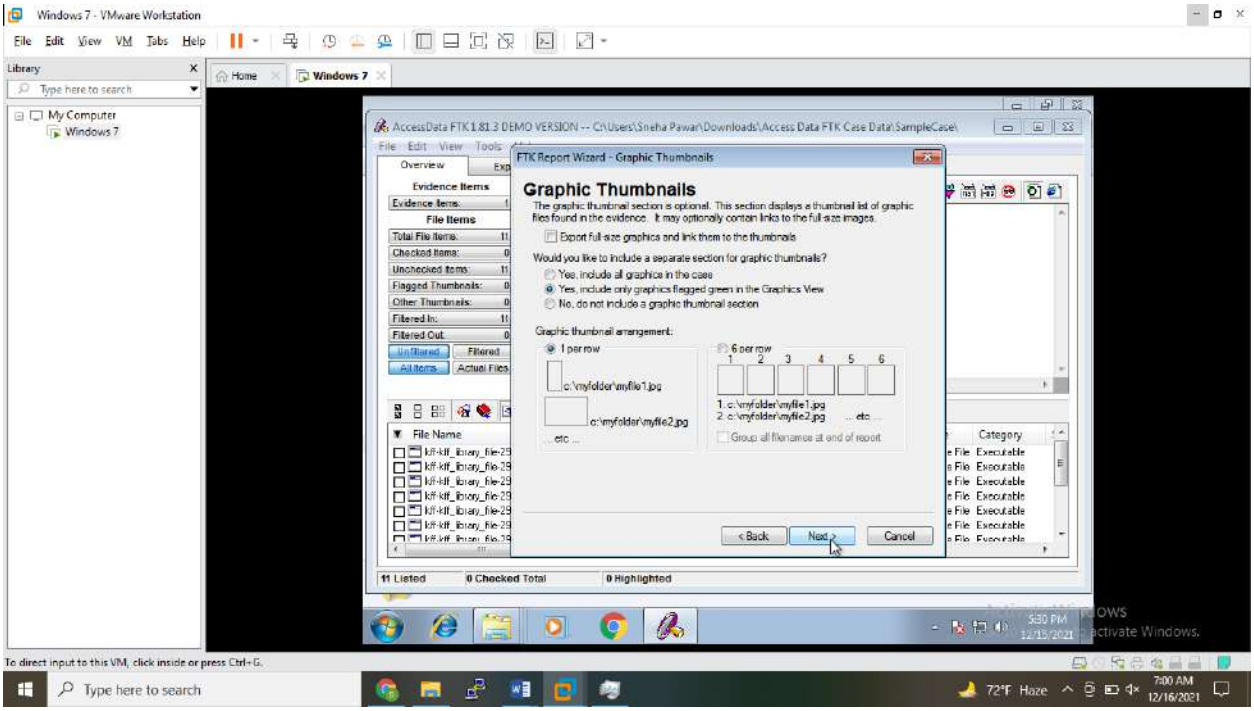
Then click on File - Report Wizard.

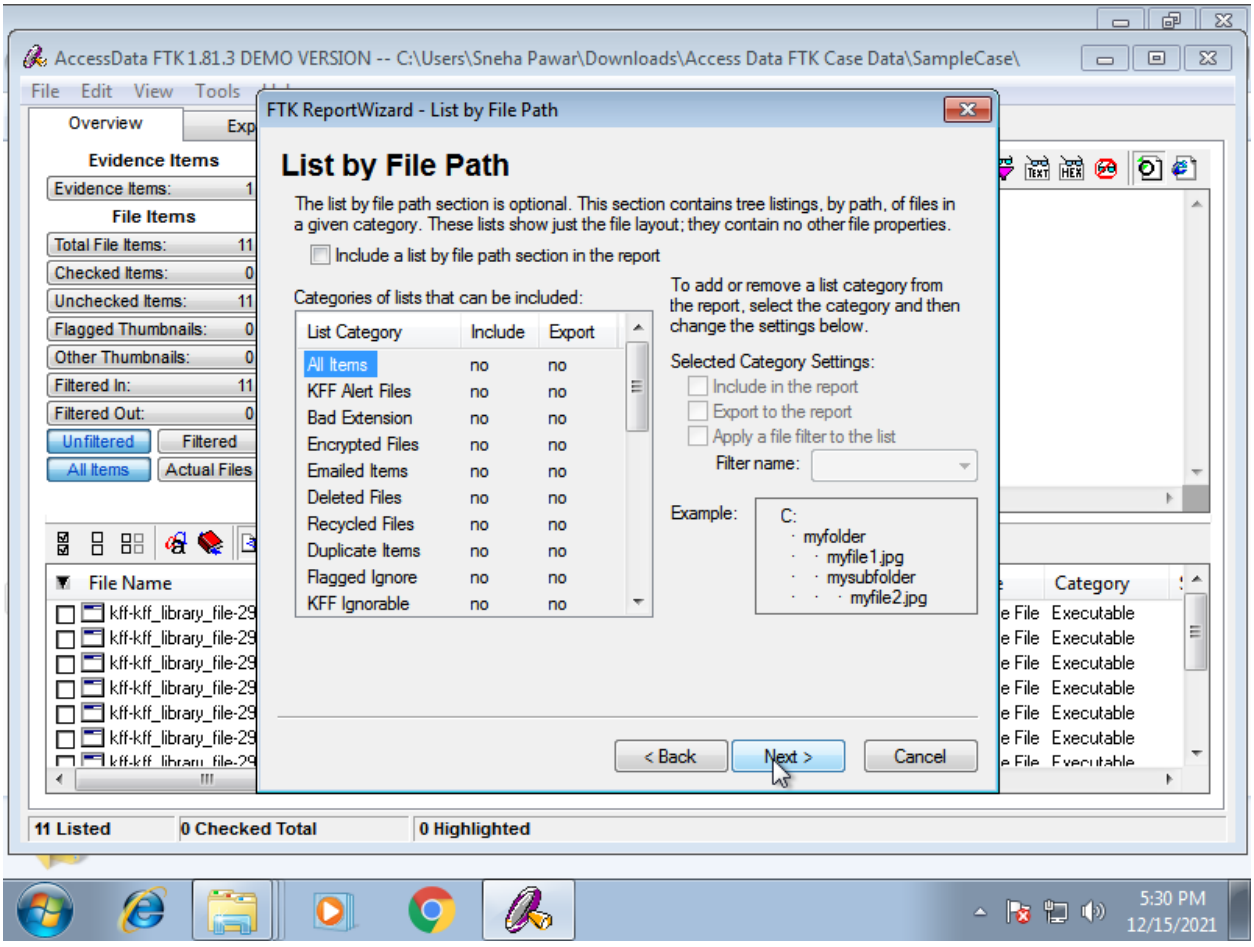
Fill the details. And click on Next.

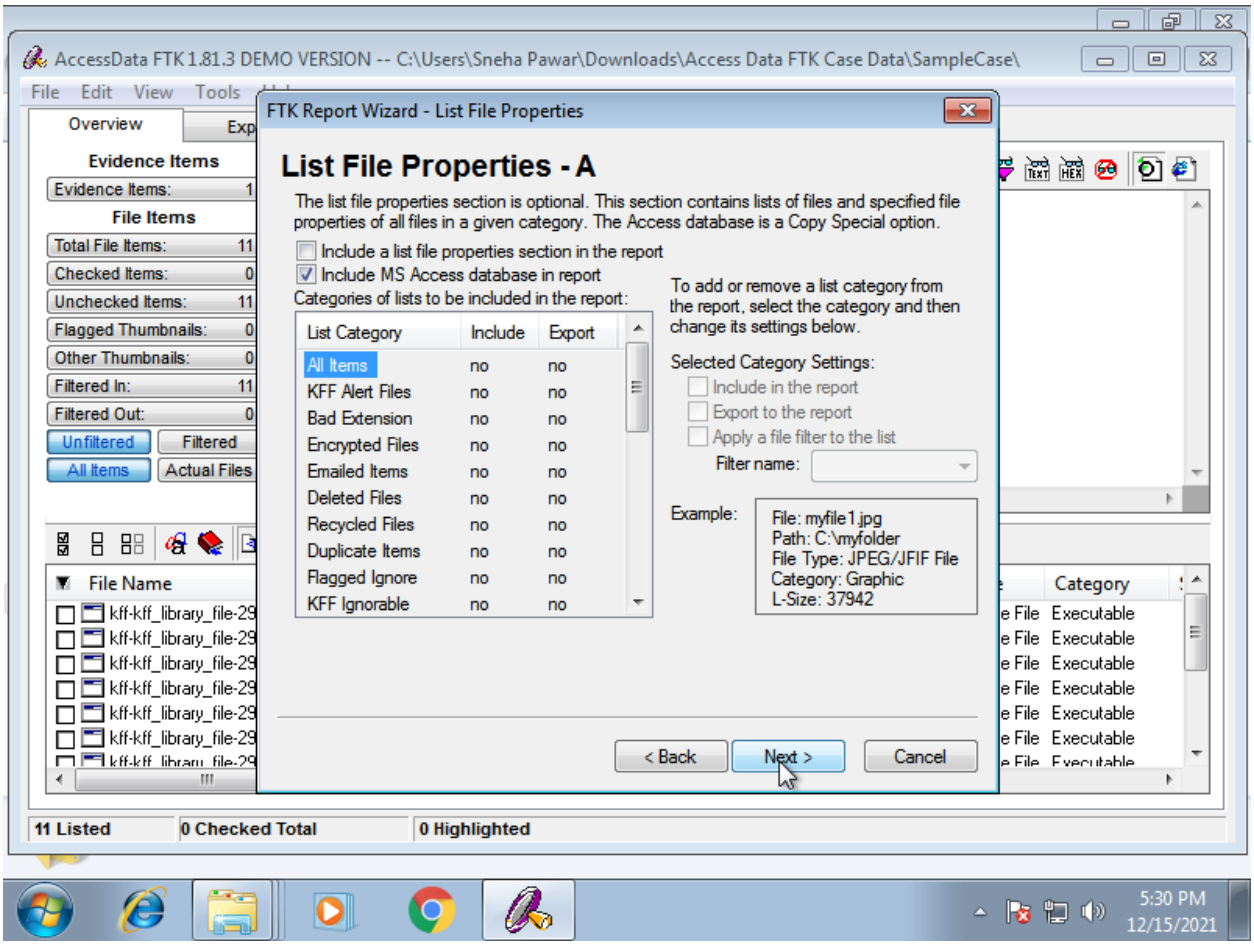

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools
Overview
Evidence Items
File Items
FTK Report Wizard - Case Information
Case Information
The following information will appear on the Case Information page of the report:
Include Investigator Information in report
Agency/Company: RJ College
Investigator's Name: Sneha Pawar
Address: 601/6, Bharat Nagar
Phone: 9827364537
Fax: 0203
E-Mail: sneharamchandrapawar@gmail.com
Comments: Ok
Next >
Cancel
11 Listed
0 Checked Total
0 Highlighted
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
72°F Haze
6:58 AM
12/16/2021

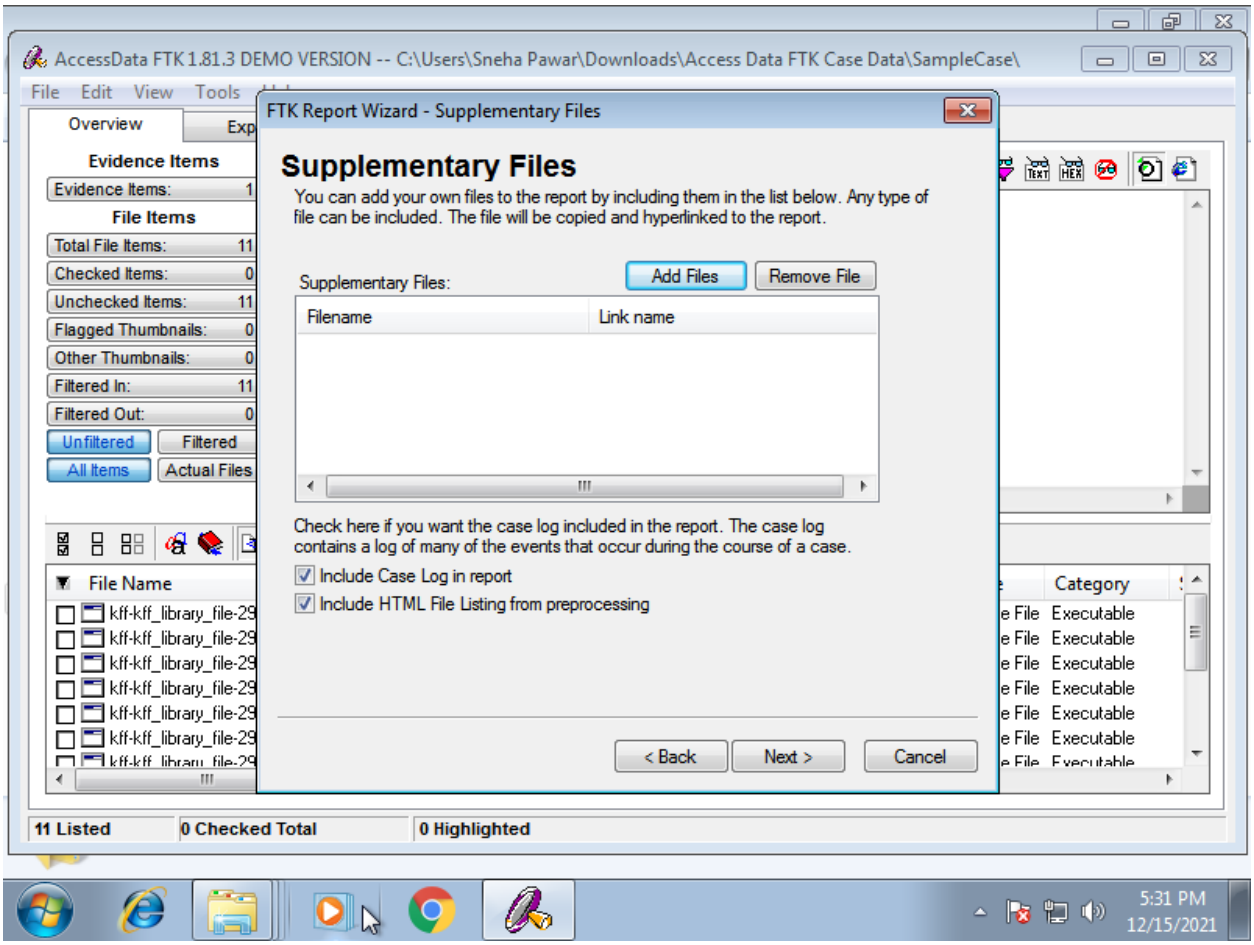

AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools
Overview
Evidence Items
Evidence Items: 1
File Items
Total File Items: 11
Checked Items: 0
Unchecked Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 11
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
File Name
kff-kff_library_file-29
Category
e File Executable
FTK Report Wizard - Bookmarks
Bookmarks - A
The bookmark section is optional. It contains a listing of the bookmarks that have been created during the investigation.
Would you like to include a bookmark section in the report?
Yes, include all bookmarks
Yes, include only bookmarks marked "Include in report"
No, do not include a bookmark section
Would you like to include a thumbnail image for each bookmarked graphic file?
Include thumbnails of bookmarked graphics
Export full-size graphics and link them to the thumbnails
Include thumbnail summary of bookmarked graphics
Would you like to export the bookmarked files to the report?
Yes, export all bookmarked files
Yes, export only files from bookmarks marked "Export to report"
No, do not export bookmarked files
< Back
Next >
Cancel
11 Listed
0 Checked Total
0 Highlighted
5:29 PM
12/15/2021


AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools
Overview
Evidence Items
Evidence Items: 1
File Items
Total File Items: 11
Checked Items: 0
Unchecked Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 11
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
File Name
kff-kff_library_file-29
Category
e File Executable
FTK Report Wizard - Bookmarks
Bookmarks - B
You have chosen to include a bookmark section in the report. Listed below are the file properties that will be included for each bookmarked file in the report.
File properties to be included in the report:
Add/Remove File Properties
Property Name
Property Explanation
File Name
File name, excluding path
Full Path
Full path of the file
Recycle Bin Original Na...
Full path of object before it was recycled
Ext
File extension
File Type
File type, based on content
Category
File category, based on file type
Subject
Email subject
Cr Date
Date file was created
Mod Date
Date file was last modified
Acc Date
Date file was last accessed
< Back
Next >
Cancel
11 Listed
0 Checked Total
0 Highlighted
5:29 PM
12/15/2021

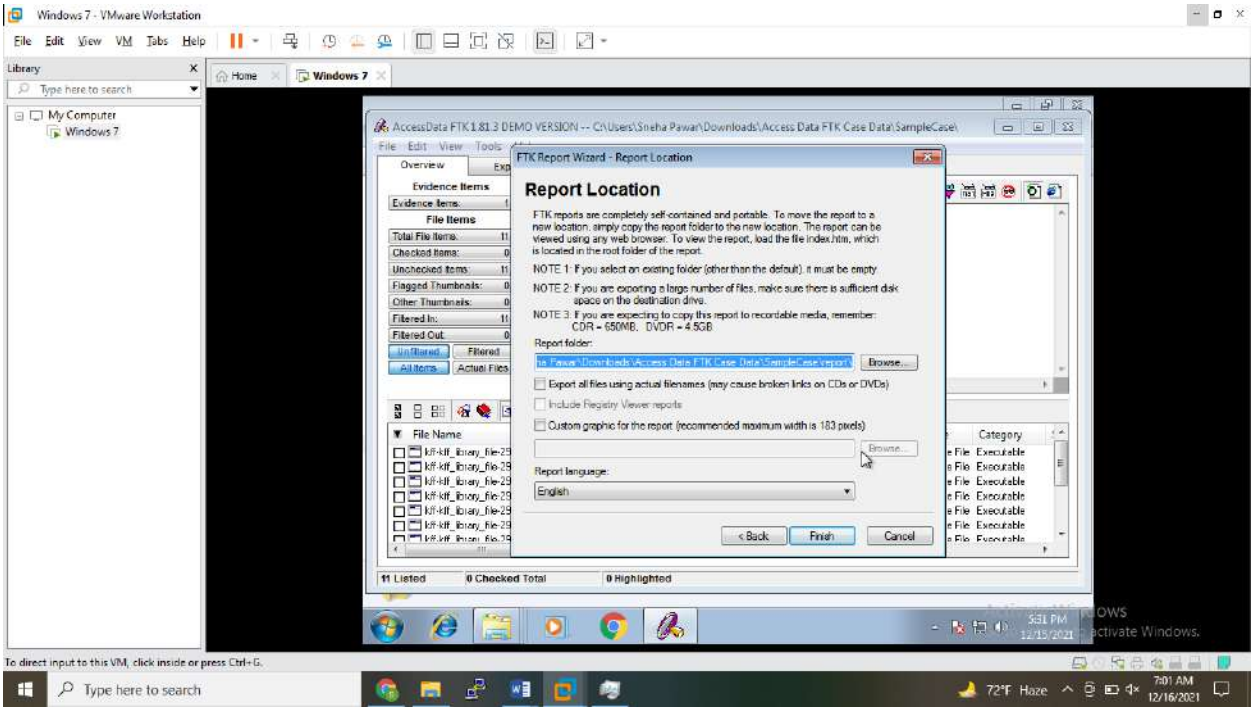

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools
Overview
Evidence Items
File Items
FTK Report Wizard - Graphic Thumbnails
Graphic Thumbnails
The graphic thumbnail section is optional. This section displays a thumbnail list of graphic files found in the evidence. It may optionally contain links to the full-size images.
Export full-size graphics and link them to the thumbnails
Would you like to include a separate section for graphic thumbnails?
Yes, include all graphics in the case
Yes, include only graphics flagged green in the Graphics View
No, do not include a graphic thumbnail section
Graphic thumbnail arrangement:
1 per row
6 per row
c:\myfolder\myfile1.jpg
c:\myfolder\myfile2.jpg
etc ...
1: c:\myfolder\myfile1.jpg
2: c:\myfolder\myfile2.jpg
Group all filenames at end of report
< Back
Next >
Cancel
File Name
Category
11 Listed
0 Checked Total
0 Highlighted
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
72°F Haze
7:00 AM
12/16/2021

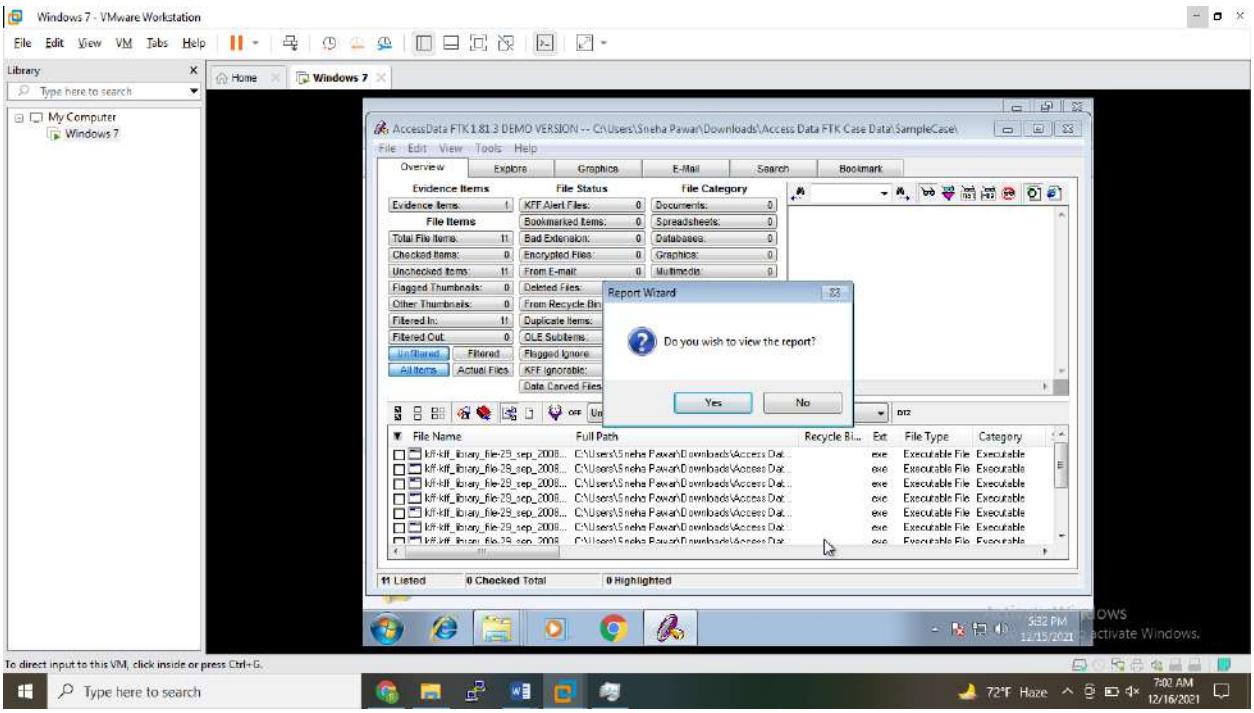

AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools
Overview
Evidence Items
Evidence Items: 1
File Items
Total File Items: 11
Checked Items: 0
Unchecked Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 11
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
File Name
kff-kff_library_file-29
FTK ReportWizard - List by File Path
List by File Path
The list by file path section is optional. This section contains tree listings, by path, of files in a given category. These lists show just the file layout; they contain no other file properties.
Include a list by file path section in the report
Categories of lists that can be included:
List Category | Include | Export
All Items | no | no
KFF Alert Files | no | no
Bad Extension | no | no
Encrypted Files | no | no
Emailed Items | no | no
Deleted Files | no | no
Recycled Files | no | no
Duplicate Items | no | no
Flagged Ignore | no | no
KFF Ignorable | no | no
To add or remove a list category from the report, select the category and then change the settings below.
Selected Category Settings:
Include in the report
Export to the report
Apply a file filter to the list
Filter name:
Example:
C:
myfolder
myfile1.jpg
mysubfolder
myfile2.jpg
< Back
Next >
Cancel
Category
e File Executable
11 Listed
0 Checked Total
0 Highlighted
5:30 PM
12/15/2021

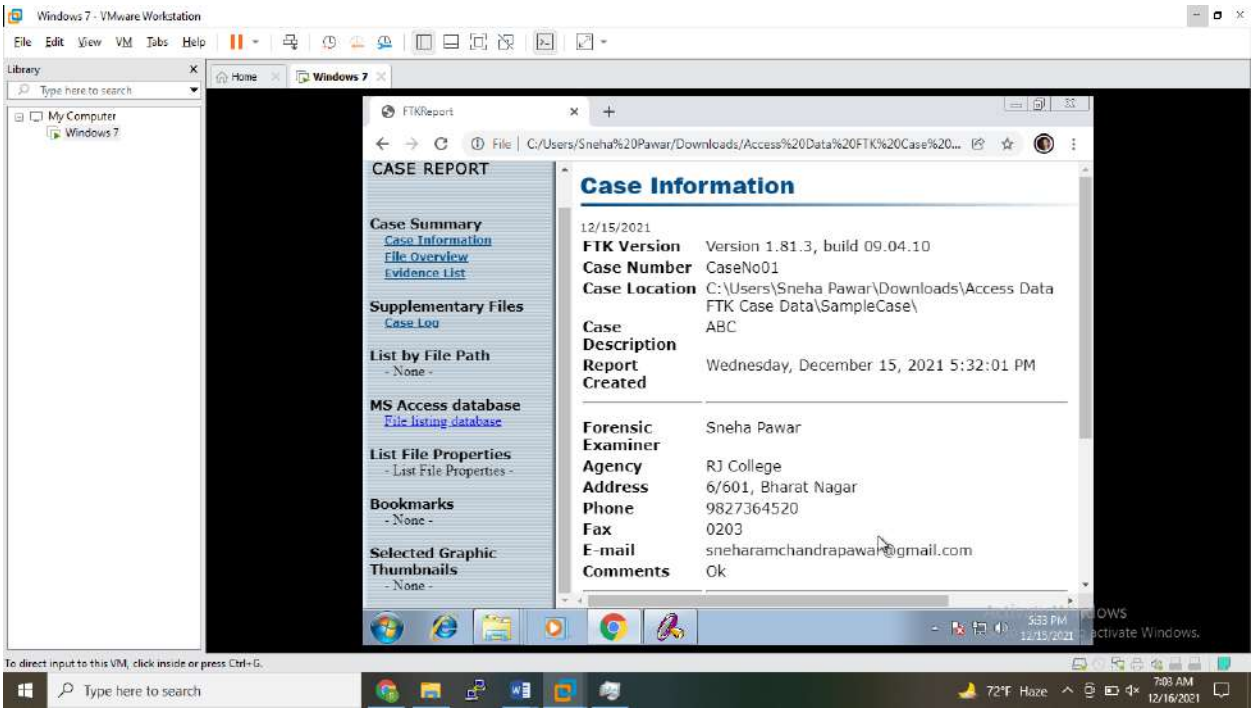

AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools
Overview
Evidence Items
Evidence Items: 1
File Items
Total File Items: 11
Checked Items: 0
Unchecked Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 11
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
File Name
Category
Executable
FTK Report Wizard - List File Properties
List File Properties - A
The list file properties section is optional. This section contains lists of files and specified file properties of all files in a given category. The Access database is a Copy Special option.
Include a list file properties section in the report
Include MS Access database in report
Categories of lists to be included in the report:
List Category
Include
Export
All Items no no
KFF Alert Files no no
Bad Extension no no
Encrypted Files no no
Emailed Items no no
Deleted Files no no
Recycled Files no no
Duplicate Items no no
Flagged Ignore no no
KFF Ignorable no no
To add or remove a list category from the report, select the category and then change its settings below.
Selected Category Settings:
Include in the report
Export to the report
Apply a file filter to the list
Filter name:
Example:
File: myfile1.jpg
Path: C:\myfolder
File Type: JPEG/JFIF File
Category: Graphic
L-Size: 37942
< Back
Next >
Cancel
11 Listed
0 Checked Total
0 Highlighted
5:30 PM
12/15/2021

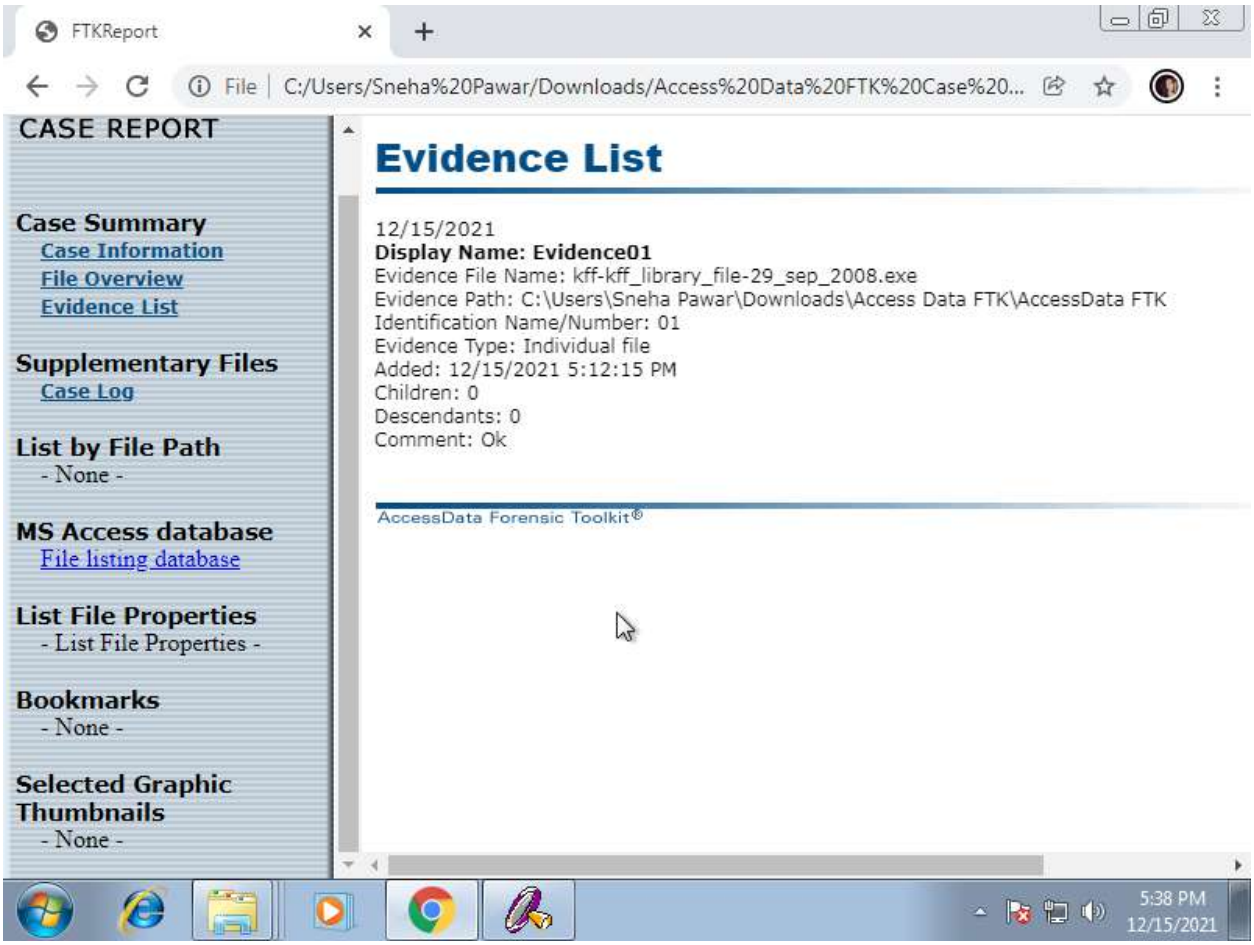


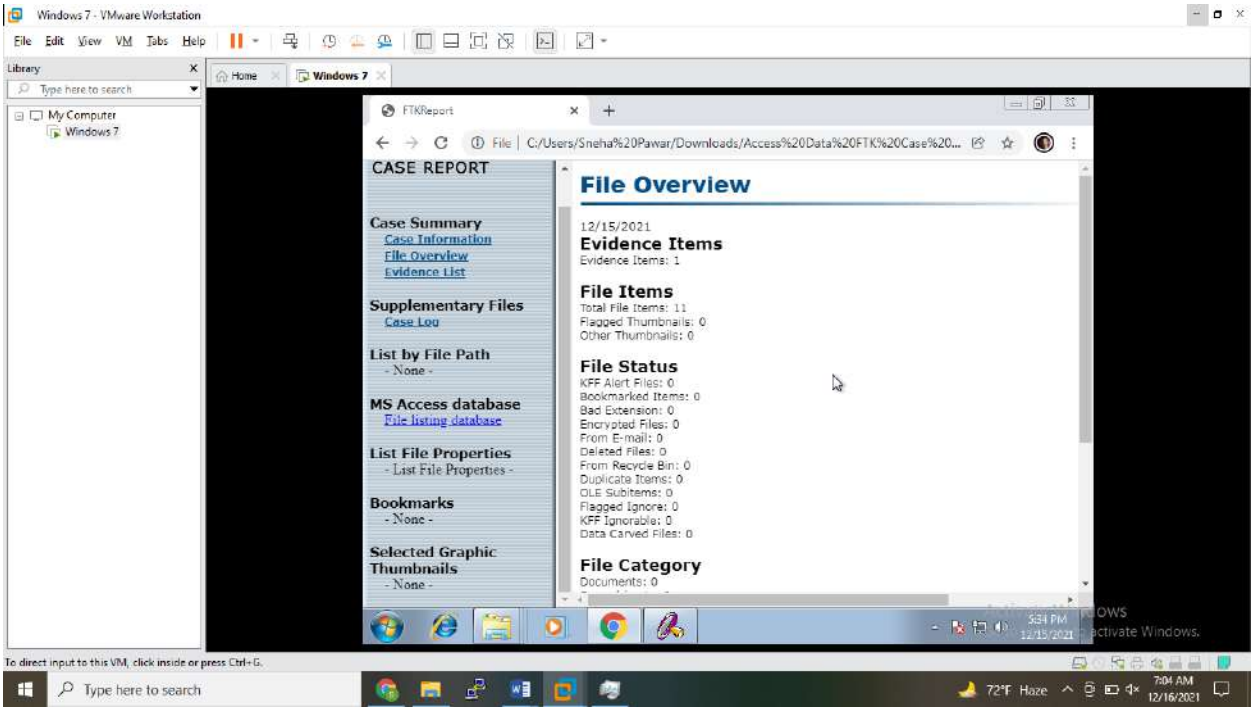
Enter report location.

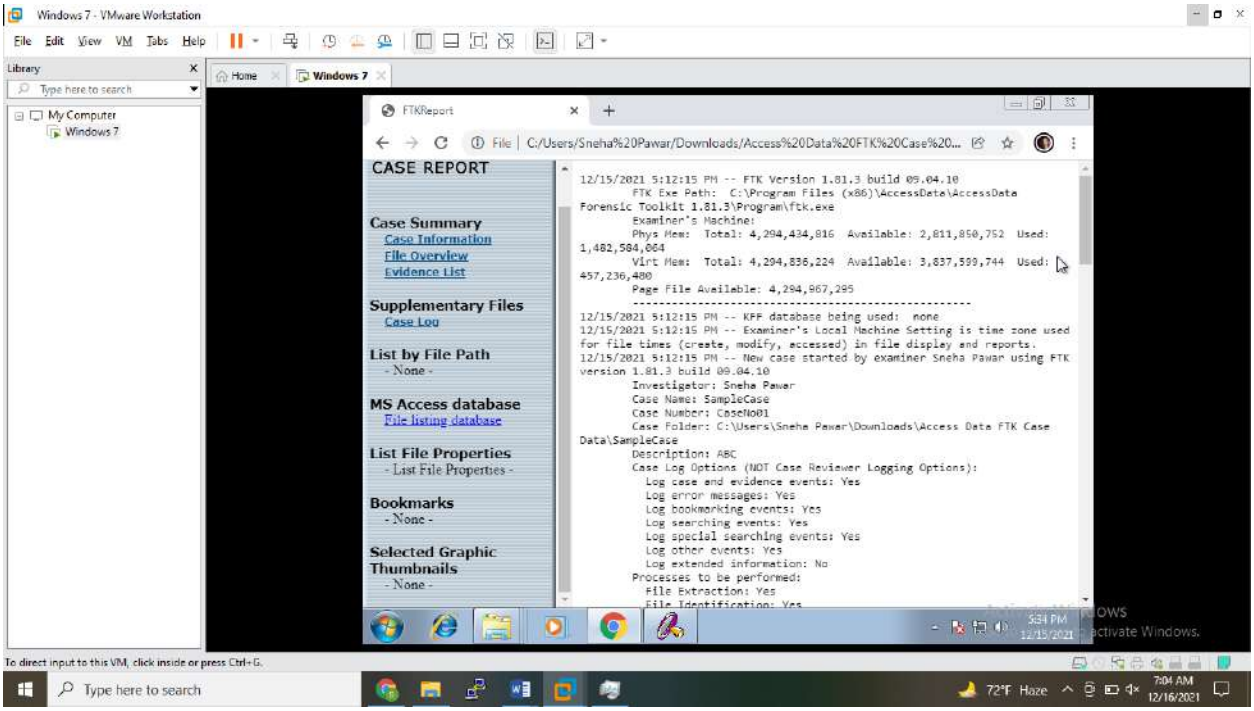

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools Help
Overview
Evidence Items
File Items
FTK Report Wizard - Report Location
Report Location
FTK reports are completely self-contained and portable. To move the report to a new location, simply copy the report folder to the new location. The report can be viewed using any web browser. To view the report, load the file index.htm, which is located in the root folder of the report.
NOTE 1: If you select an existing folder (other than the default), it must be empty.
NOTE 2: If you are exporting a large number of files, make sure there is sufficient disk space on the destination drive.
NOTE 3: If you are expecting to copy this report to recordable media, remember: CDR = 650MB; DVDR = 4.5GB
Report folder:
Browse...
Export all files using actual filenames (may cause broken links on CDs or DVDs)
Include Registry Viewer reports
Custom graphic for the report (recommended maximum width is 183 pixels)
Report language:
English
< Back
Finish
Cancel
11 Listed
0 Checked Total
0 Highlighted
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
72°F Haze
7:01 AM
12/16/2021


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Evidence Items
File Status
File Category
Report Wizard
Do you wish to view the report?
Yes
No
11 Listed
0 Checked Total
0 Highlighted
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
72°F Haze
7:02 AM
12/16/2021


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
FTKReport
File | C:/Users/Sneha%20Pawar/Downloads/Access%20Data%20FTK%20Case%20...
CASE REPORT
Case Summary
Case Information
File Overview
Evidence List
Supplementary Files
Case Log
List by File Path
- None -
MS Access database
File listing database
List File Properties
- List File Properties -
Bookmarks
- None -
Selected Graphic Thumbnails
- None -
Case Information
12/15/2021
FTK Version Version 1.81.3, build 09.04.10
Case Number CaseNo01
Case Location C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
Case Description ABC
Report Created Wednesday, December 15, 2021 5:32:01 PM
Forensic Examiner Sneha Pawar
Agency RJ College
Address 6/601, Bharat Nagar
Phone 9827364520
Fax 0203
E-mail sneharamchandrapawar@gmail.com
Comments Ok
5:33 PM
12/15/2021
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
72°F Haze
7:03 AM
12/16/2021

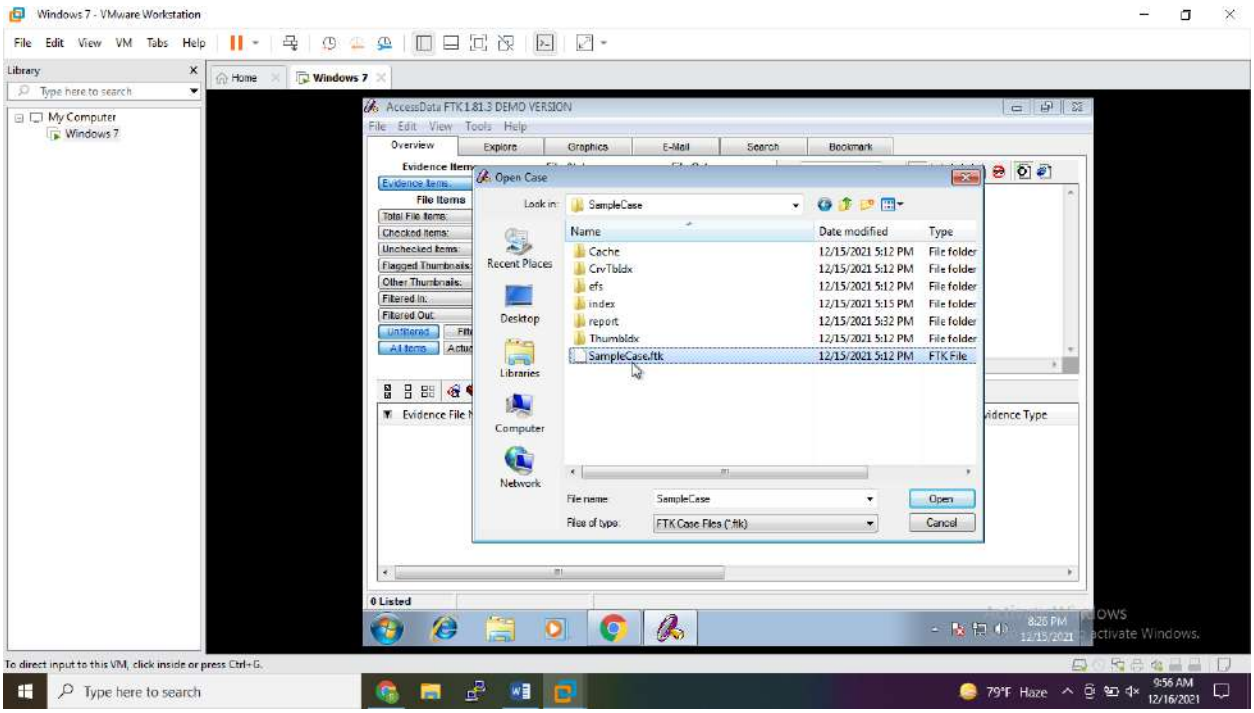

FTKReport
File | C:/Users/Sneha%20Pawar/Downloads/Access%20Data%20FTK%20Case%20...
CASE REPORT
Case Summary
Case Information
File Overview
Evidence List
Supplementary Files
Case Log
List by File Path
- None -
MS Access database
File listing database
List File Properties
- List File Properties -
Bookmarks
- None -
Selected Graphic Thumbnails
- None -
Evidence List
12/15/2021
Display Name: Evidence01
Evidence File Name: kff-kff_library_file-29_sep_2008.exe
Evidence Path: C:\Users\Sneha Pawar\Downloads\Access Data FTK\AccessData FTK
Identification Name/Number: 01
Evidence Type: Individual file
Added: 12/15/2021 5:12:15 PM
Children: 0
Descendants: 0
Comment: Ok
AccessData Forensic Toolkit®
5:38 PM
12/15/2021


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
FTKReport
File | C:/Users/Sneha%20Pawar/Downloads/Access%20Data%20FTK%20Case%20...
CASE REPORT
Case Summary
Case Information
File Overview
Evidence List
Supplementary Files
Case Log
List by File Path
- None -
MS Access database
File listing database
List File Properties
- List File Properties -
Bookmarks
- None -
Selected Graphic Thumbnails
- None -
File Overview
12/15/2021
Evidence Items
Evidence Items: 1
File Items
Total File Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
File Status
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 0
Encrypted Files: 0
From E-mail: 0
Deleted Files: 0
From Recycle Bin: 0
Duplicate Items: 0
OLE Subitems: 0
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0
File Category
Documents: 0
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
72°F Haze
7:04 AM
12/16/2021



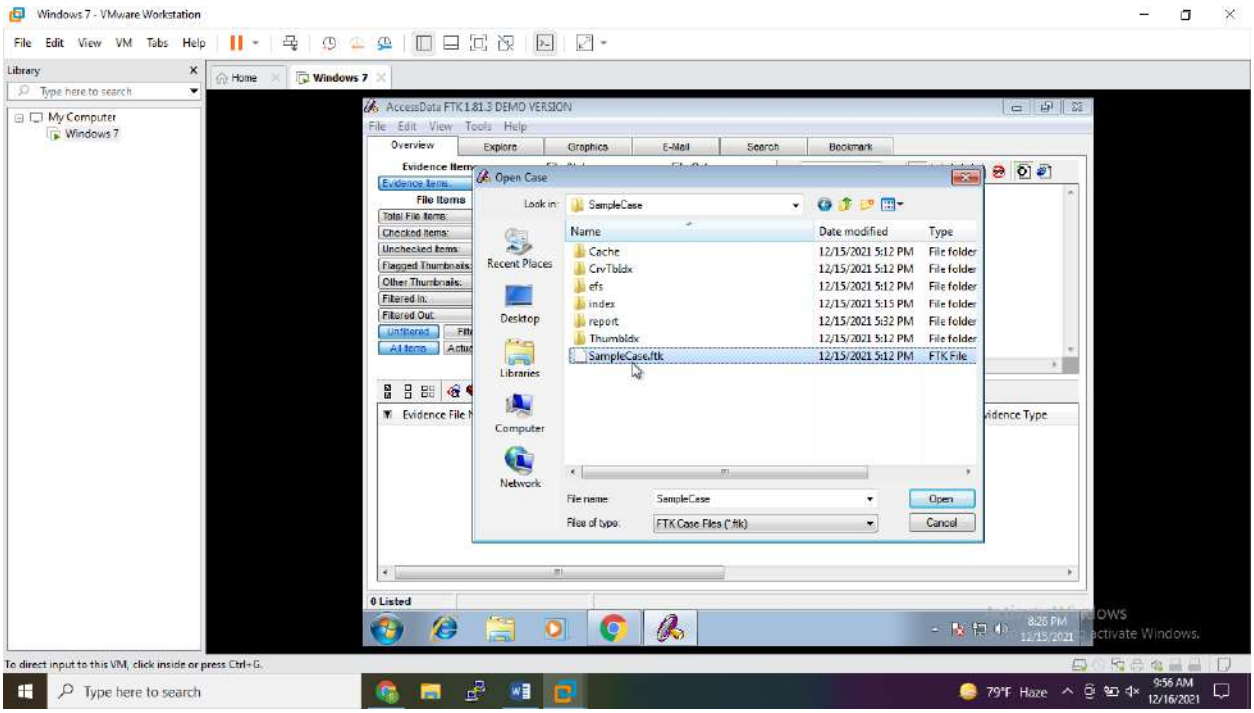
Now, let's perform Email Forensic on this. Open Existing Case that we have created.

File – Open Case

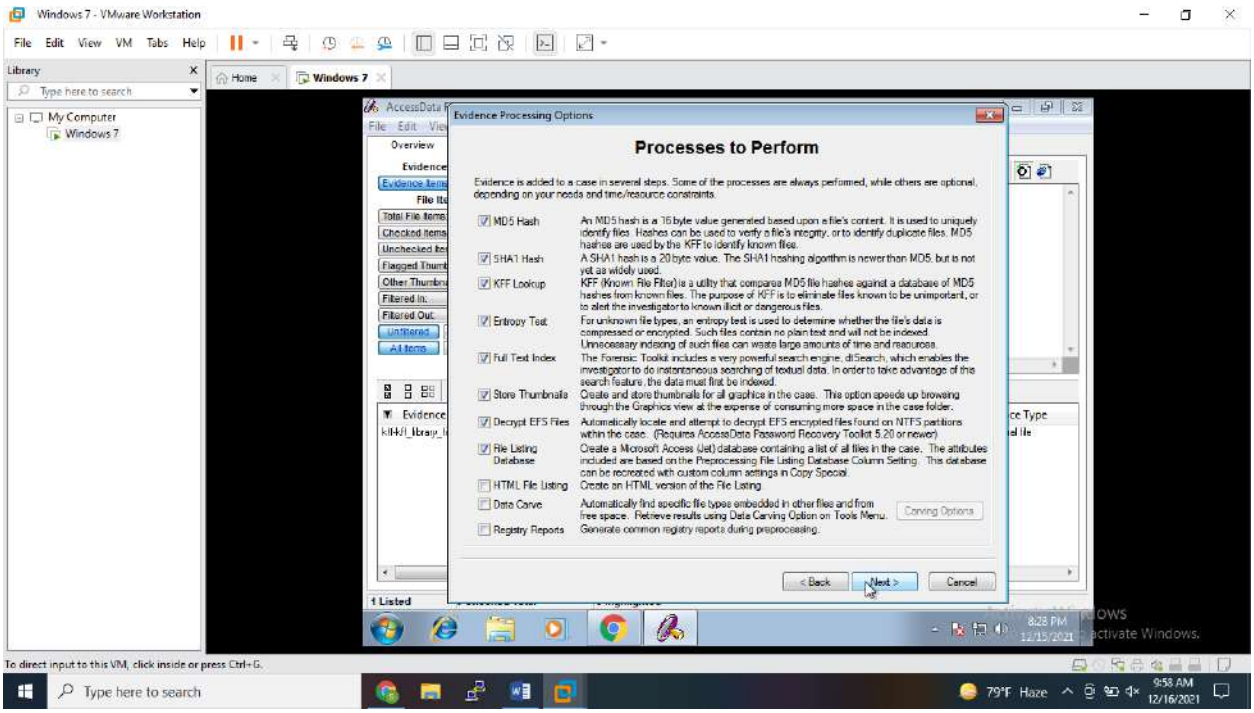


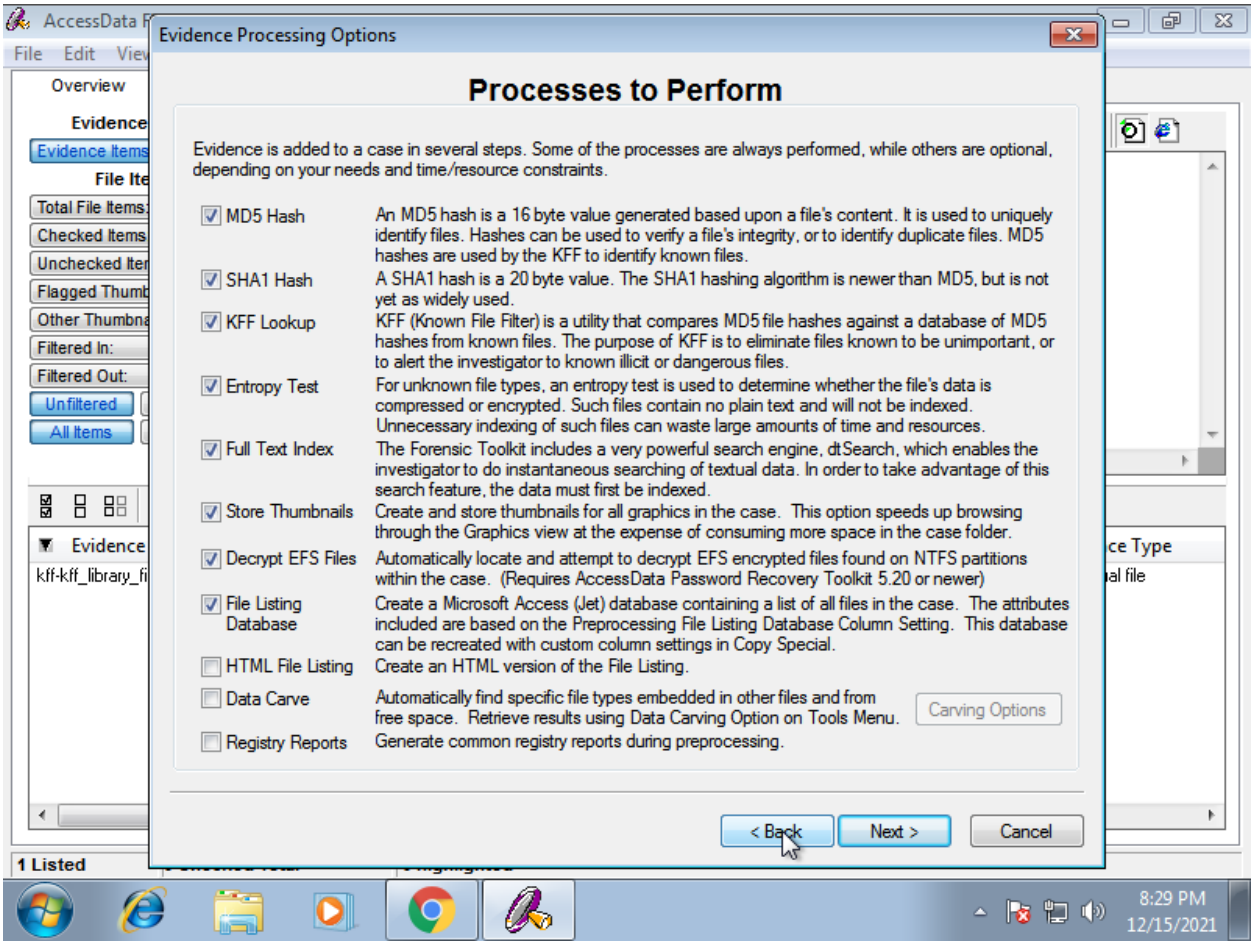
Now File – Add Evidence, and add Outlook's pst file.

Keep this by default.

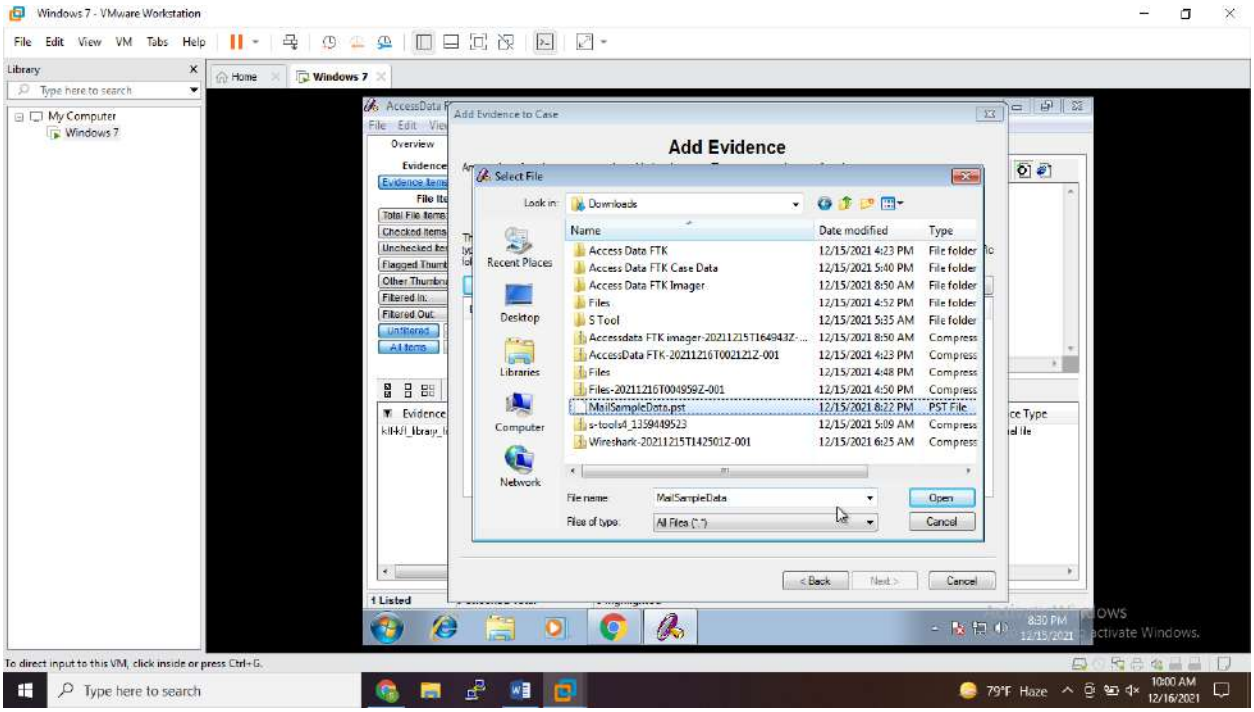


Click Next

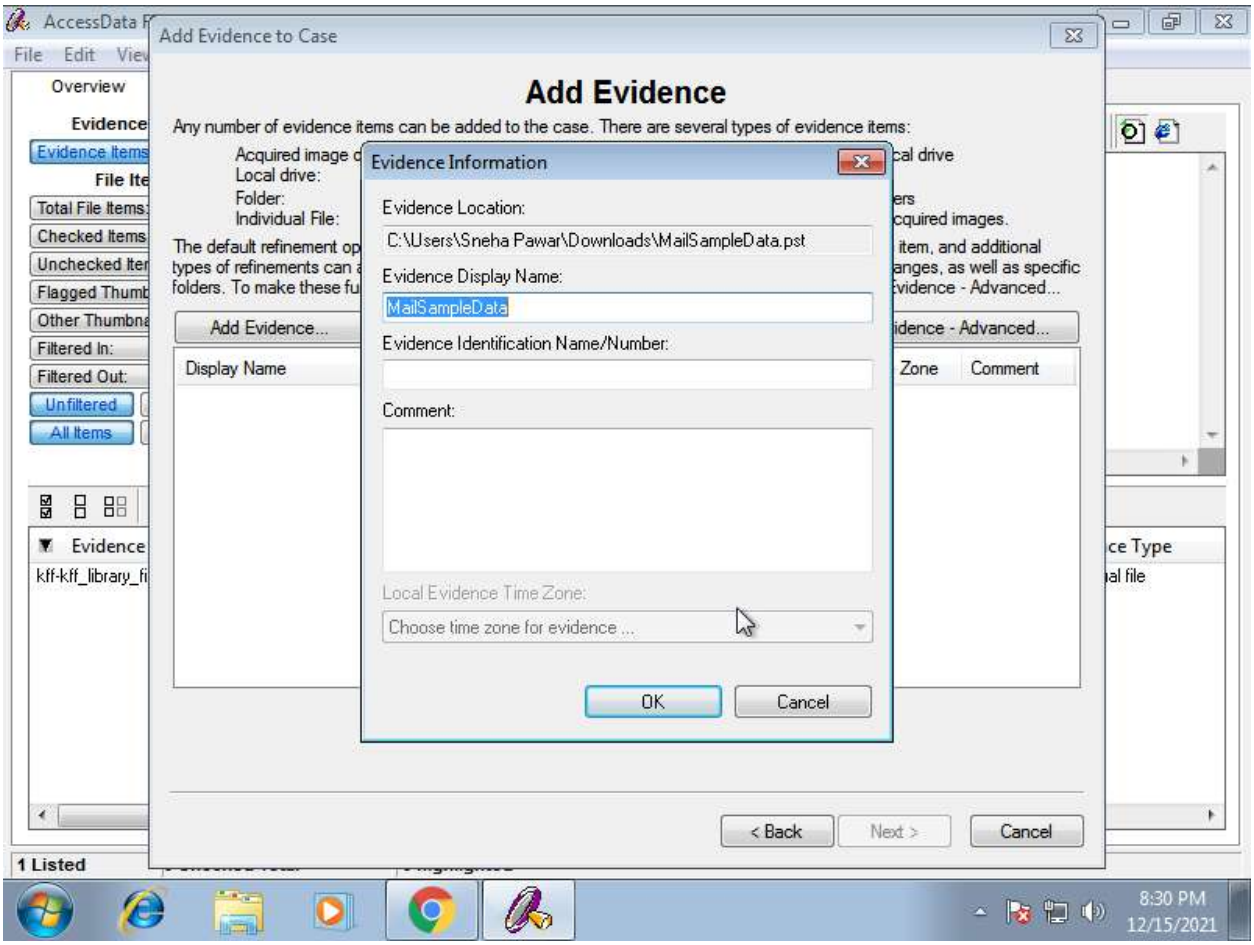

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
Evidence Processing Options
Processes to Perform
Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.
MD5 Hash
An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
SHA1 Hash
A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
KFF Lookup
KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
Entropy Test
For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.
Full Text Index
The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.
Store Thumbnails
Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.
Decrypt EFS Files
Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)
File Listing Database
Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special.
HTML File Listing
Create an HTML version of the File Listing.
Data Carve
Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.
Carving Options
Registry Reports
Generate common registry reports during preprocessing.
< Back
Next >
Cancel
1 Listed
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
9:58 AM
12/16/2021

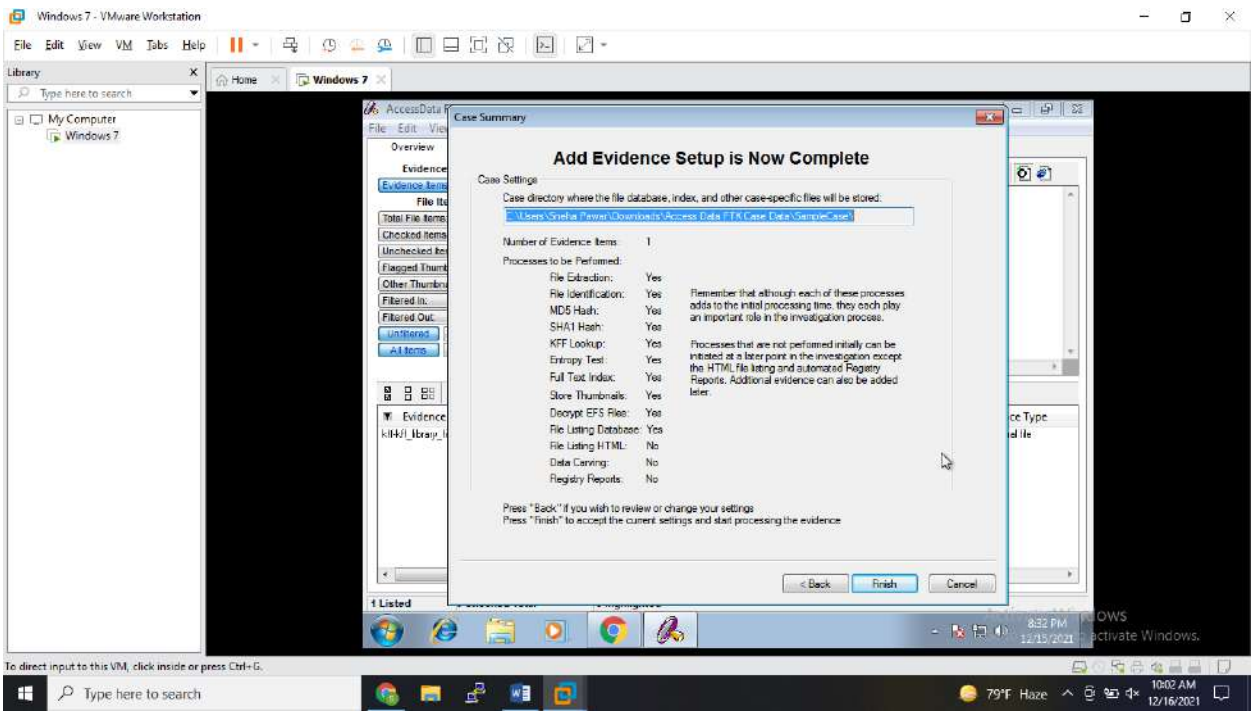

AccessData
File Edit View
Overview
Evidence
Evidence Items
File Items
Total File Items:
Checked Items
Unchecked Items
Flagged Thumbnails
Other Thumbnails
Filtered In:
Filtered Out:
Unfiltered
All Items
Evidence
kff-kff_library_files
Evidence Processing Options
Processes to Perform
Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.
MD5 Hash
An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
SHA1 Hash
A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
KFF Lookup
KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
Entropy Test
For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.
Full Text Index
The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.
Store Thumbnails
Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.
Decrypt EFS Files
Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)
File Listing Database
Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special.
HTML File Listing
Create an HTML version of the File Listing.
Data Carve
Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.
Carving Options
Registry Reports
Generate common registry reports during preprocessing.
< Back
Next >
Cancel
1 Listed
8:29 PM
12/15/2021

Then Add Evidence – Individual File – Browse location of a pst file.

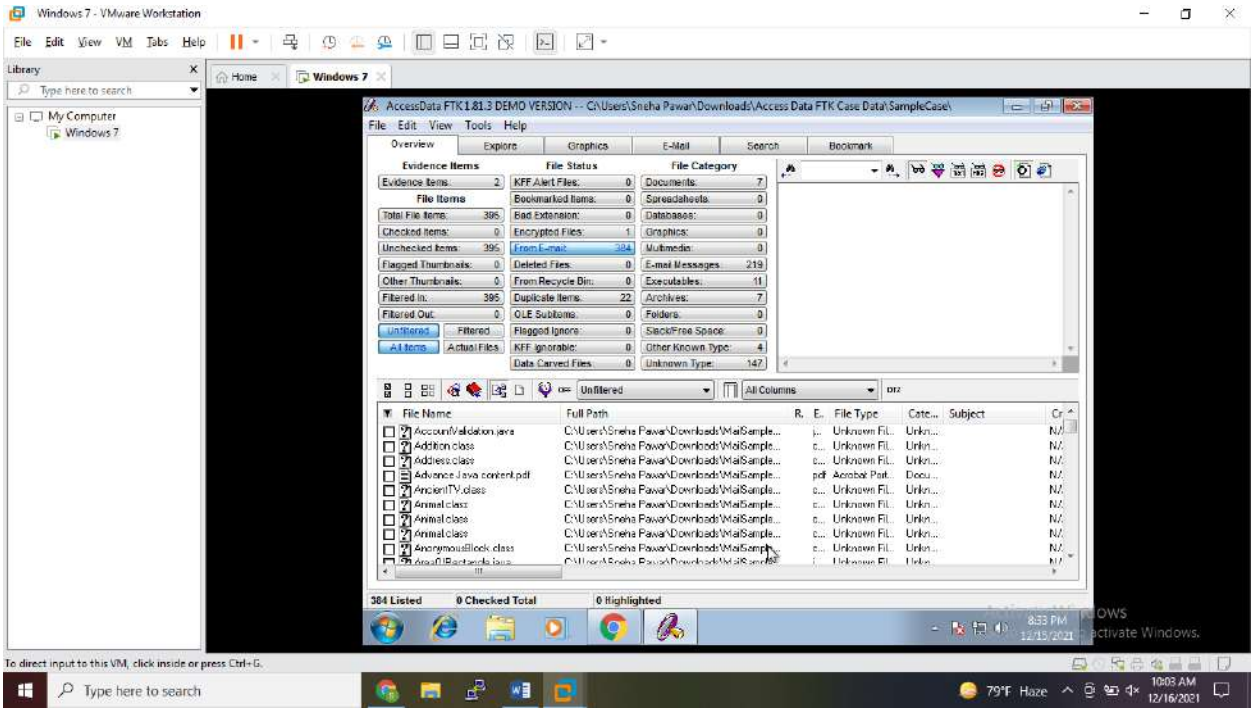


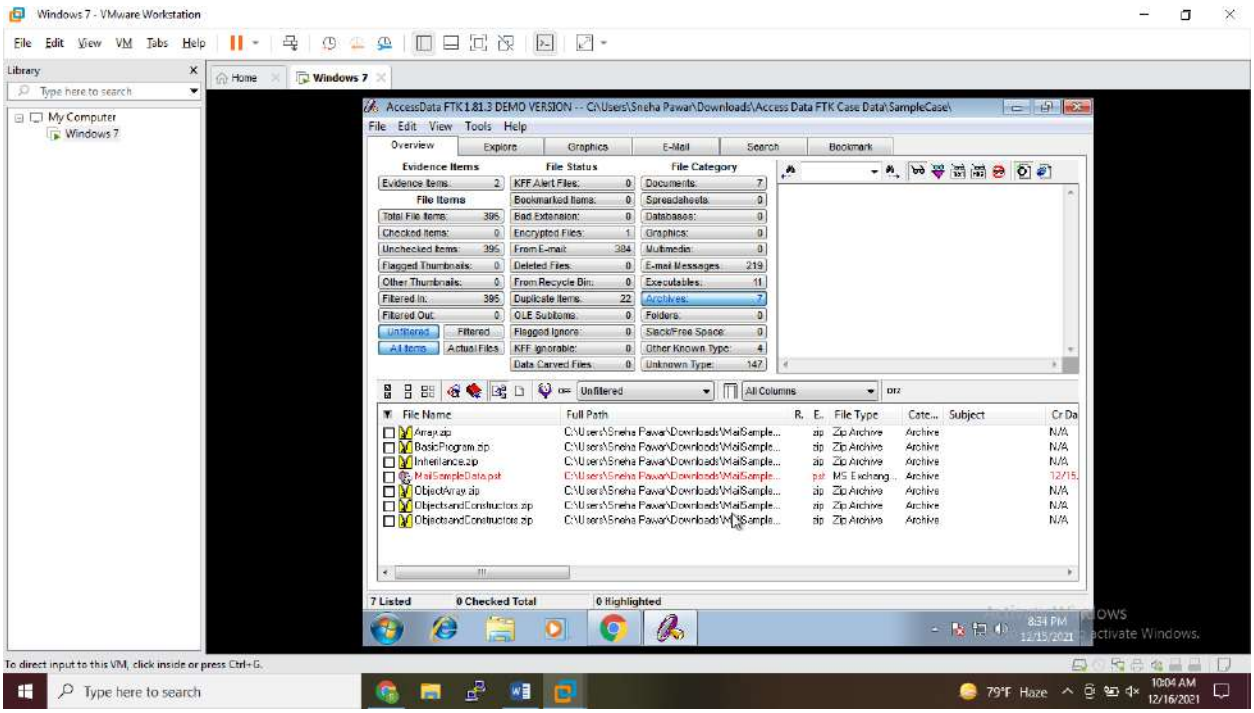
Click on Ok. And then click on Next.

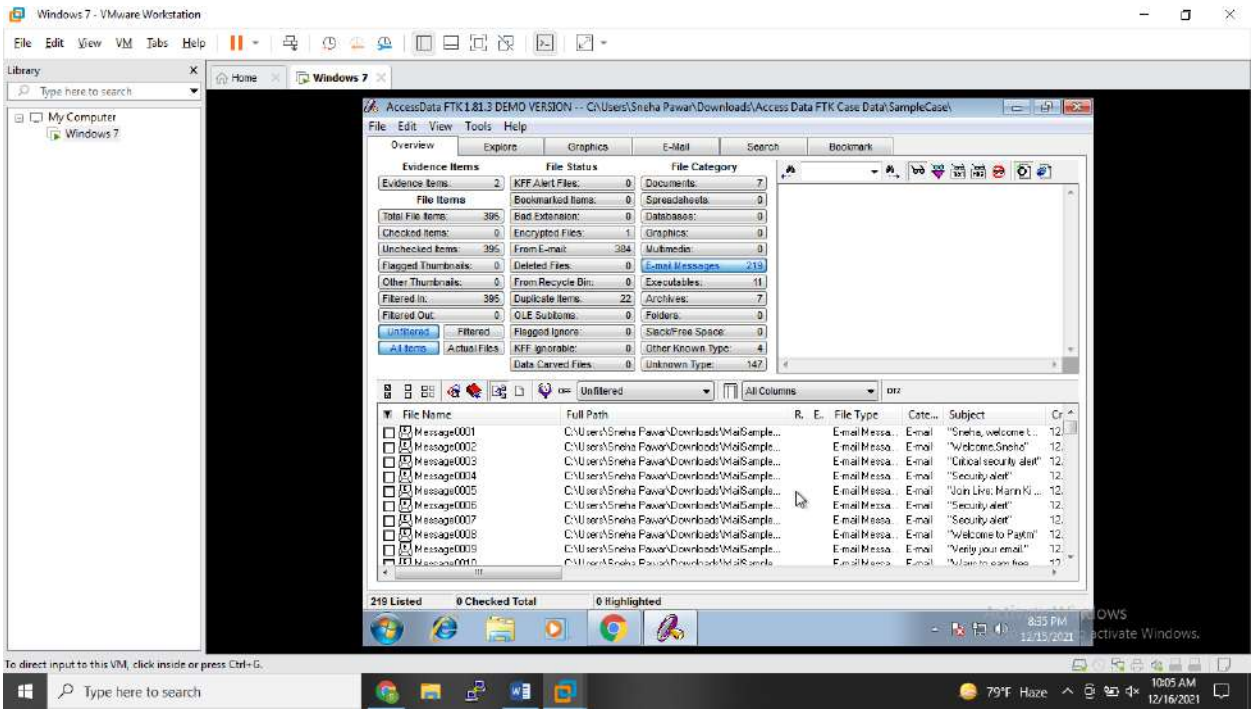

Add Evidence to Case
Add Evidence
Any number of evidence items can be added to the case. There are several types of evidence items:
Evidence Information
Evidence Location:
C:\Users\Sneha Pawar\Downloads\MailSampleData.pst
Evidence Display Name:
MailSampleData
Evidence Identification Name/Number:
Comment:
Local Evidence Time Zone:
Choose time zone for evidence ...
OK
Cancel
Add Evidence...
Display Name
Zone
Comment
< Back
Next >
Cancel
1 Listed
8:30 PM
12/15/2021


Windows 7 - VMware Workstation
Case Summary
Add Evidence Setup is Now Complete
Case Settings
Case directory where the file database, index, and other case-specific files will be stored:
Number of Evidence Items 1
Processes to be Performed:
File Extraction: Yes
File Identification: Yes
MD5 Hash: Yes
SHA1 Hash: Yes
KFF Lookup: Yes
Entropy Test: Yes
Full Text Index: Yes
Store Thumbnails: Yes
Decrypt EFS Files: Yes
File Listing Database: Yes
File Listing HTML: No
Data Carving: No
Registry Reports: No
Press "Back" if you wish to review or change your settings
Press "Finish" to accept the current settings and start processing the evidence
< Back
Finish
Cancel
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
10:02 AM
12/16/2021

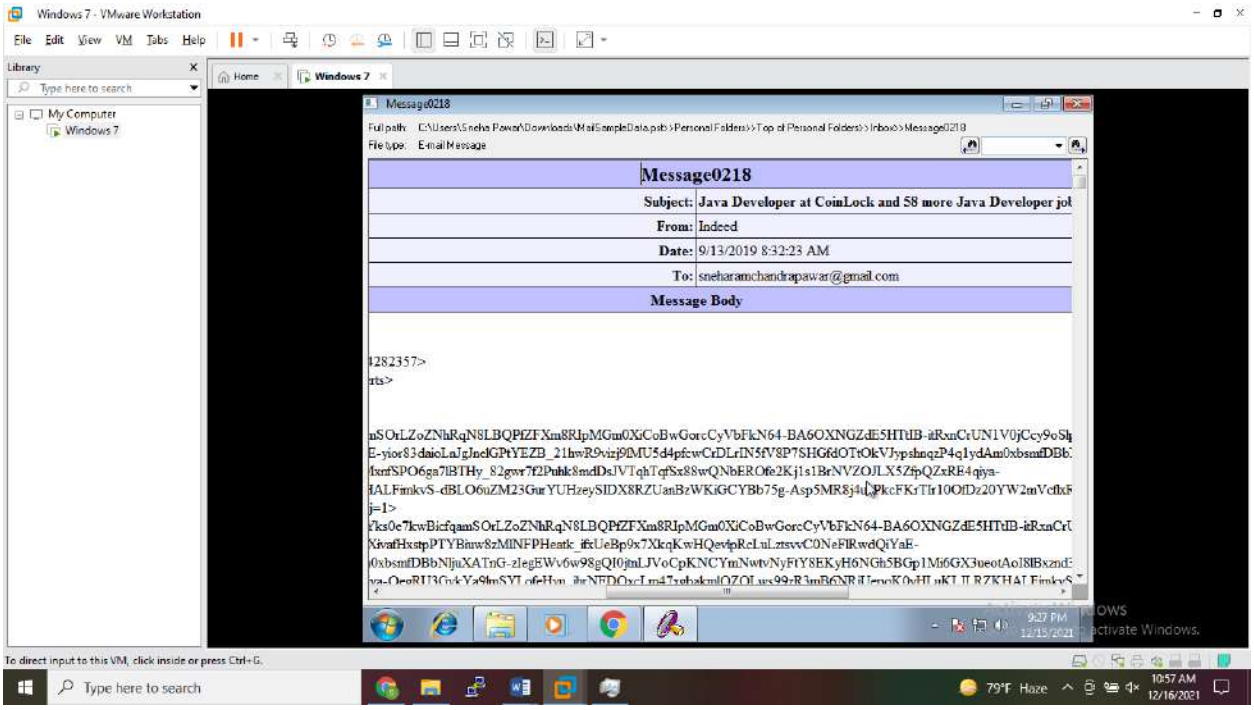
Emails will get acquired as you can see after double clicking on an evidence.





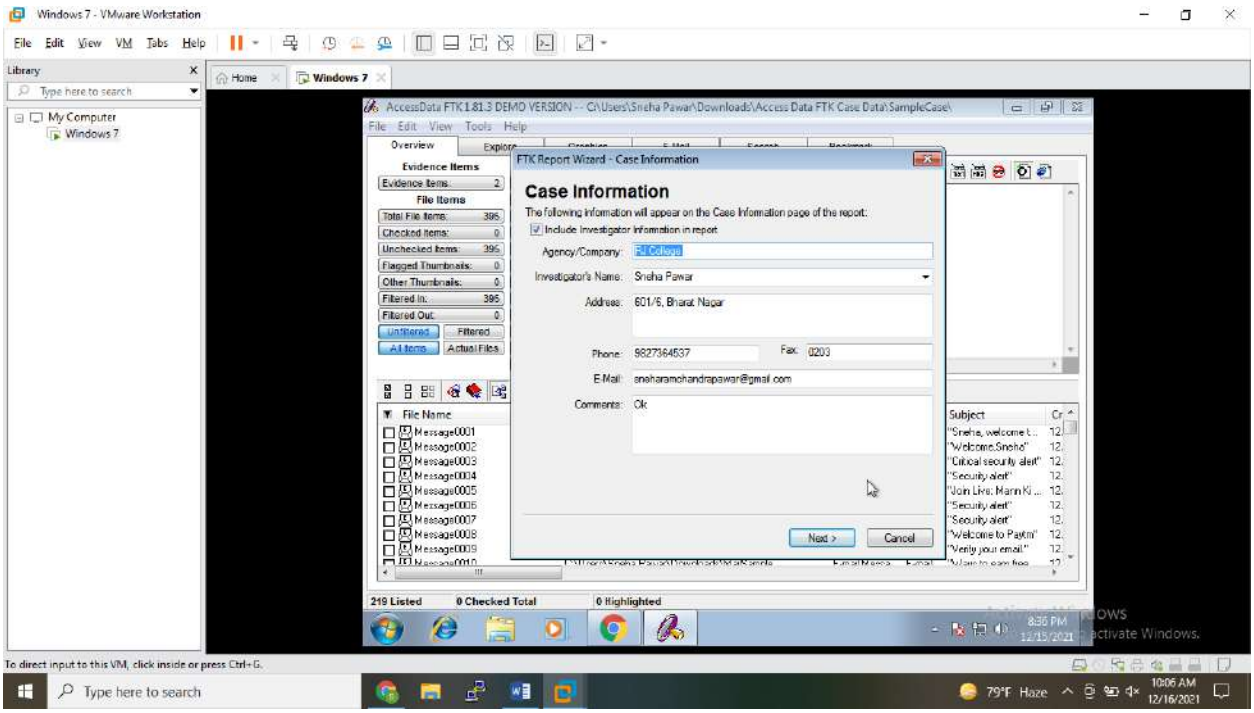


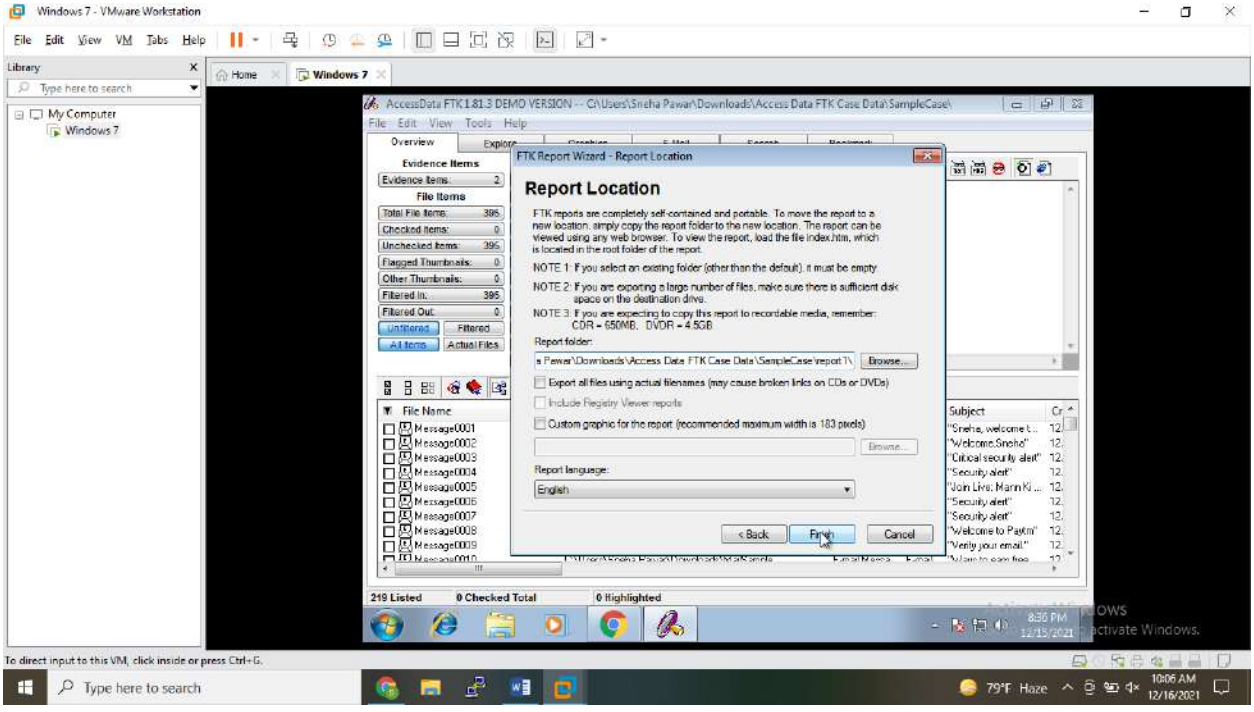
Right click on Mail to see it in Detached view.

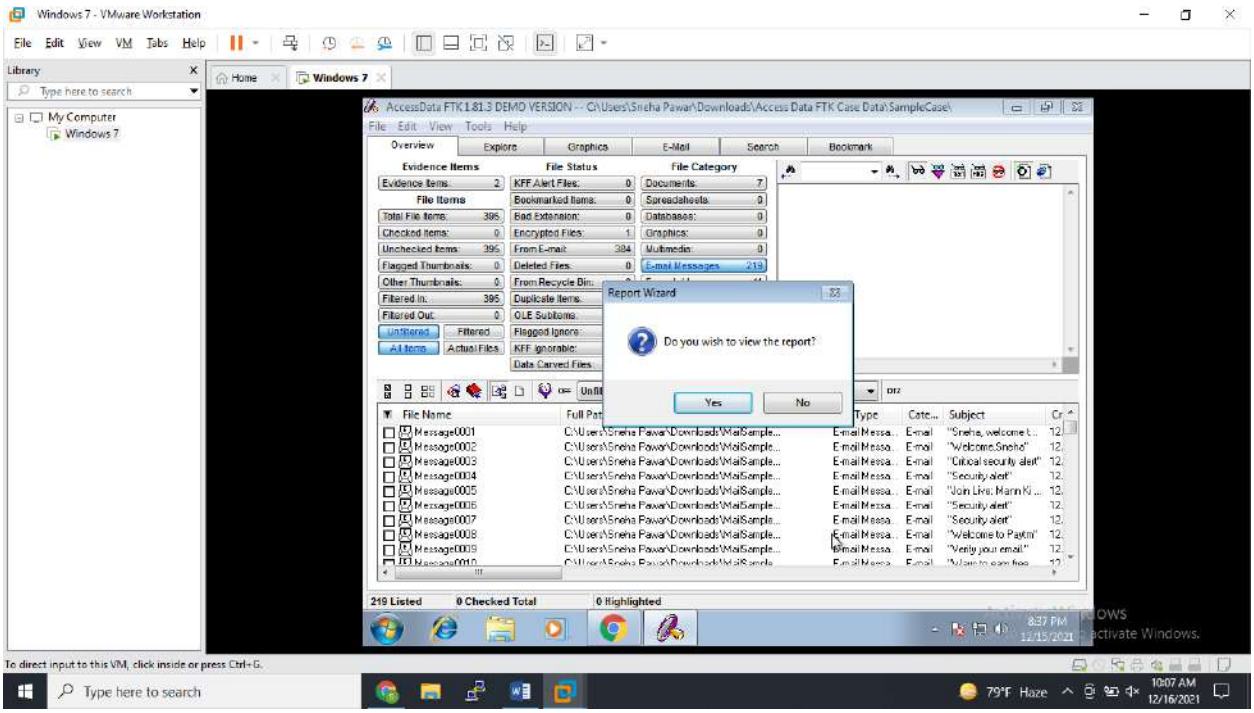


Steps:

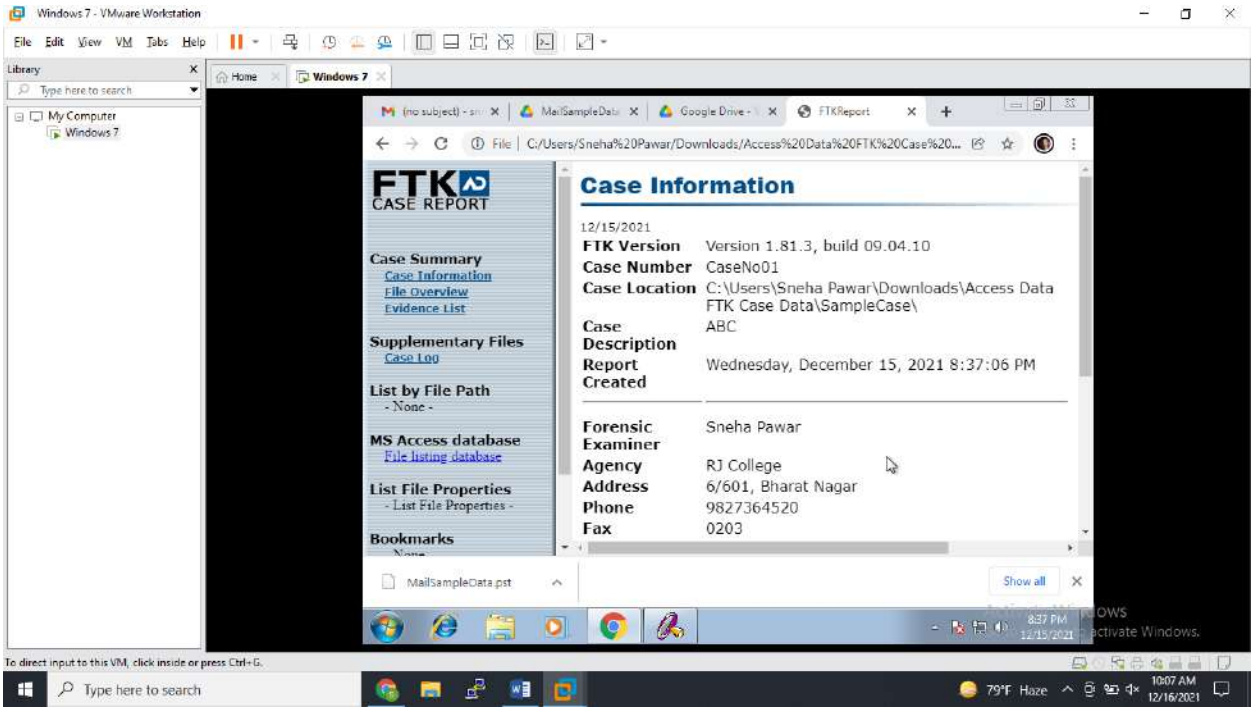
Now click on Report Wizard. And keep options by default and click on Next.

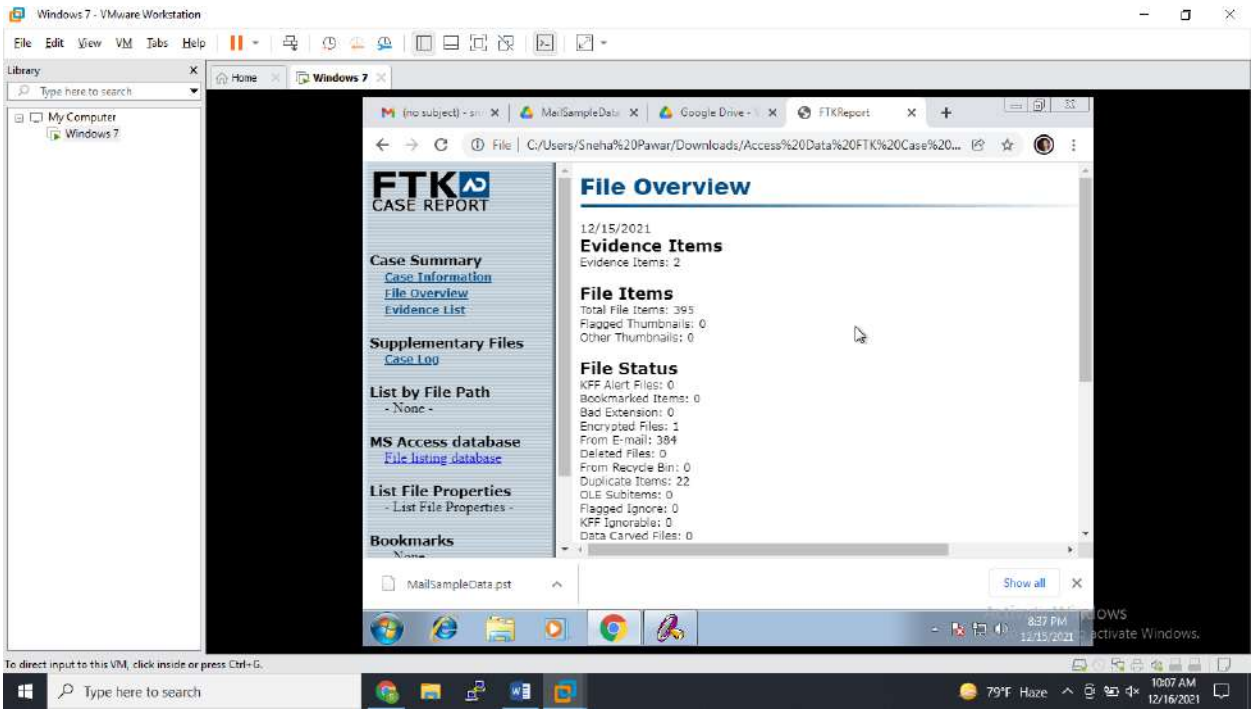

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION - C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools Help
Overview
Explore
Evidence Items
Evidence Items: 2
File Items
Total File Items: 395
Checked Items: 0
Unchecked Items: 395
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 395
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
FTK Report Wizard - Case Information
Case Information
The following information will appear on the Case Information page of the report:
Include Investigator information in report
Agency/Company: FC College
Investigator's Name: Sneha Pawar
Address: 601/6, Bharat Nagar
Phone: 9827364537
Fax: 0203
E-Mail: sneharamchandrapawar@gmail.com
Comments: Ok
Next >
Cancel
File Name
Message0001
Message0002
Message0003
Message0004
Message0005
Message0006
Message0007
Message0008
Message0009
Subject
"Sneha, welcome t...
"Welcome,Sneha"
"Critical security alert"
"Security alert"
"Join Live: Mann Ki ...
"Security alert"
"Security alert"
"Welcome to Paytm"
"Verify your email."
219 Listed
0 Checked Total
0 Highlighted
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
10:06 AM
12/16/2021

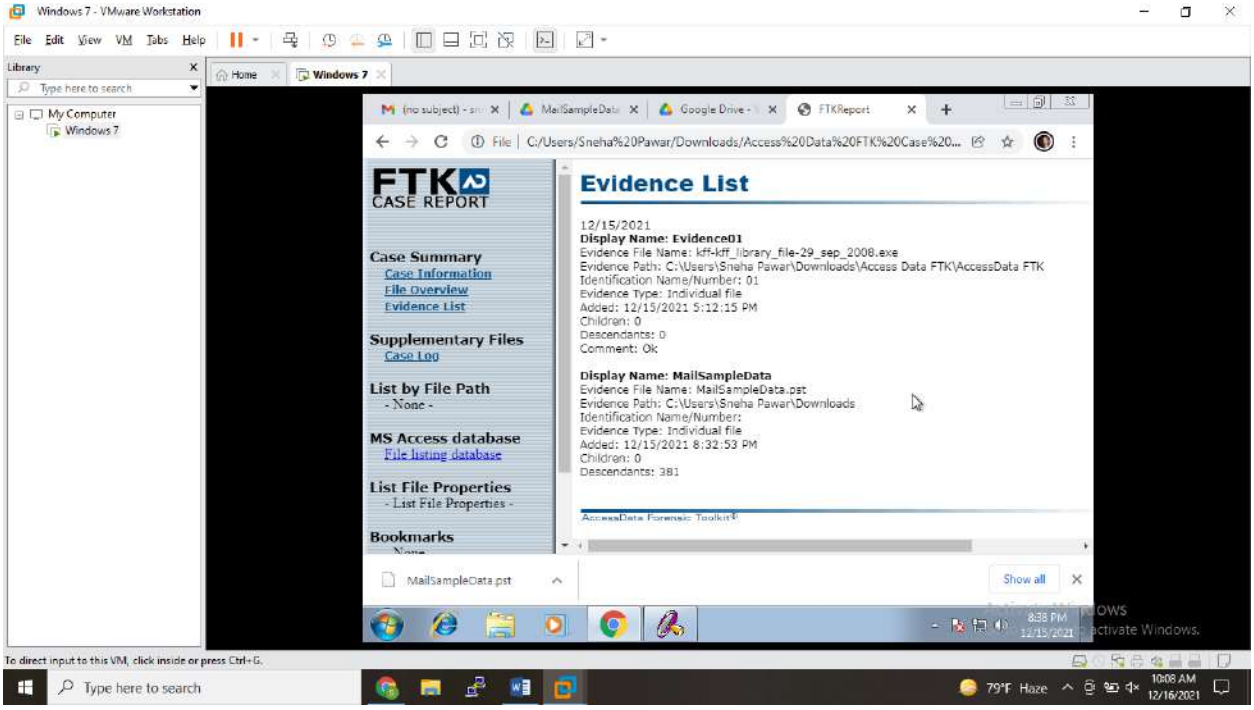

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION - C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools Help
Overview
Explore
Evidence Items
Evidence Items: 2
File Items
Total File Items: 395
Checked Items: 0
Unchecked Items: 395
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 395
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
FTK Report Wizard - Report Location
Report Location
FTK reports are completely self-contained and portable. To move the report to a new location, simply copy the report folder to the new location. The report can be viewed using any web browser. To view the report, load the file index.htm, which is located in the root folder of the report.
NOTE 1: If you select an existing folder (other than the default), it must be empty.
NOTE 2: If you are exporting a large number of files, make sure there is sufficient disk space on the destination drive.
NOTE 3: If you are expecting to copy this report to recordable media, remember:
CDR = 650MB; DVDR = 4.5GB
Report folder:
Browse...
Export all files using actual filenames (may cause broken links on CDs or DVDs)
Include Registry Viewer reports
Custom graphic for the report (recommended maximum width is 183 pixels)
Browse...
Report language:
English
< Back
Finish
Cancel
File Name
Message0001
Message0002
Message0003
Message0004
Message0005
Message0006
Message0007
Message0008
Message0009
Subject
"Sneha, welcome t...
"Welcome,Sneha"
"Critical security alert"
"Security alert"
"Join Live: Mann Ki ...
"Security alert"
"Security alert"
"Welcome to Paytm"
"Verify your email."
219 Listed
0 Checked Total
0 Highlighted
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
10:06 AM
12/16/2021


Windows 7 - VMware Workstation
Report Wizard
Do you wish to view the report?
Yes
No

Click on Yes.


Windows 7 - VMware Workstation
FTK CASE REPORT
Case Information
12/15/2021
FTK Version Version 1.81.3, build 09.04.10
Case Number CaseNo01
Case Location C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
Case Description ABC
Report Created Wednesday, December 15, 2021 8:37:06 PM
Forensic Examiner Sneha Pawar
Agency RJ College
Address 6/601, Bharat Nagar
Phone 9827364520
Fax 0203


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
FTKReport
File | C:/Users/Sneha%20Pawar/Downloads/Access%20Data%20FTK%20Case%20...
FTK CASE REPORT
Case Summary
Case Information
File Overview
Evidence List
Supplementary Files
Case Log
List by File Path
- None -
MS Access database
File listing database
List File Properties
- List File Properties -
Bookmarks
File Overview
12/15/2021
Evidence Items
Evidence Items: 2
File Items
Total File Items: 395
Flagged Thumbnails: 0
Other Thumbnails: 0
File Status
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 0
Encrypted Files: 1
From E-mail: 384
Deleted Files: 0
From Recycle Bin: 0
Duplicate Items: 22
OLE Subitems: 0
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0
MailSampleData.pst
Show all
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
10:07 AM
12/16/2021


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
FTKReport
File | C:/Users/Sneha%20Pawar/Downloads/Access%20Data%20FTK%20Case%20...
FTK CASE REPORT
Case Summary
Case Information
File Overview
Evidence List
Supplementary Files
Case Log
List by File Path
- None -
MS Access database
File listing database
List File Properties
- List File Properties -
Bookmarks
Evidence List
12/15/2021
Display Name: Evidence01
Evidence File Name: kff-kff_library_file-29_sep_2008.exe
Evidence Path: C:\Users\Sneha Pawar\Downloads\Access Data FTK\AccessData FTK
Identification Name/Number: 01
Evidence Type: Individual file
Added: 12/15/2021 5:12:15 PM
Children: 0
Descendants: 0
Comment: Ok
Display Name: MailSampleData
Evidence File Name: MailSampleData.pst
Evidence Path: C:\Users\Sneha Pawar\Downloads
Identification Name/Number:
Evidence Type: Individual file
Added: 12/15/2021 8:32:53 PM
Children: 0
Descendants: 381
AccessData Forensic Toolkit®
MailSampleData.pst
Show all
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
10:08 AM
12/16/2021

Practical No. 03

Aim: Using Data Acquisition Tools [ProDiscover Pro]

What is Data Acquisition?

Forensic Data Acquisition. Data acquisition is the **process of making a forensic image** from computer media such as a hard drive, thumb drive, CDROM, removable hard drives, thumb drives, servers and other media that stores electronic data including gaming consoles and other devices.

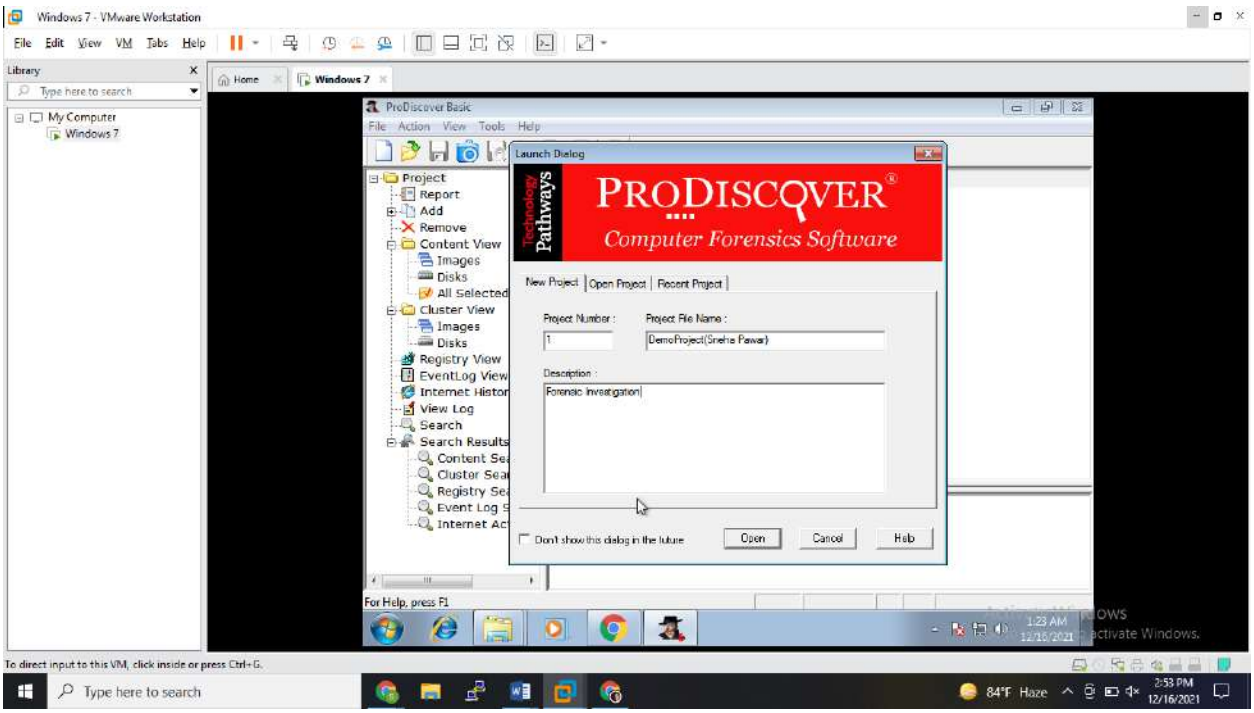
ProDiscover Tool:

ProDiscover Forensics is a comprehensive digital forensics software that empowers investigators to capture key evidence from computer systems. ProDiscover has capabilities to handle all aspects of an in-depth forensic investigation to collect, preserve, filter, and analyze evidence.

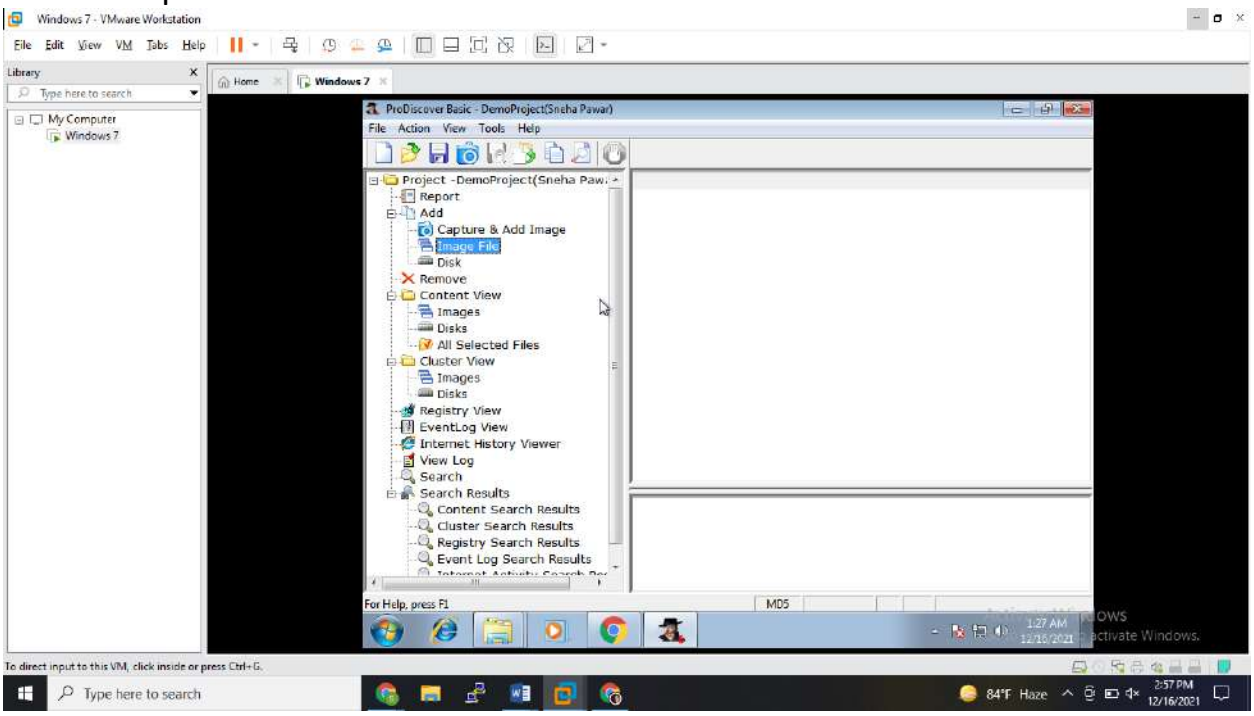
An investigator can use the tools and features of ProDiscover to identify discrete bits of evidence and connect those to form a cohesive picture. ProDiscover provides capabilities to analyze the nature and the modalities of the cybercrime. Evidentiary quality reports can be prepared and presented in the court of law.

Steps:

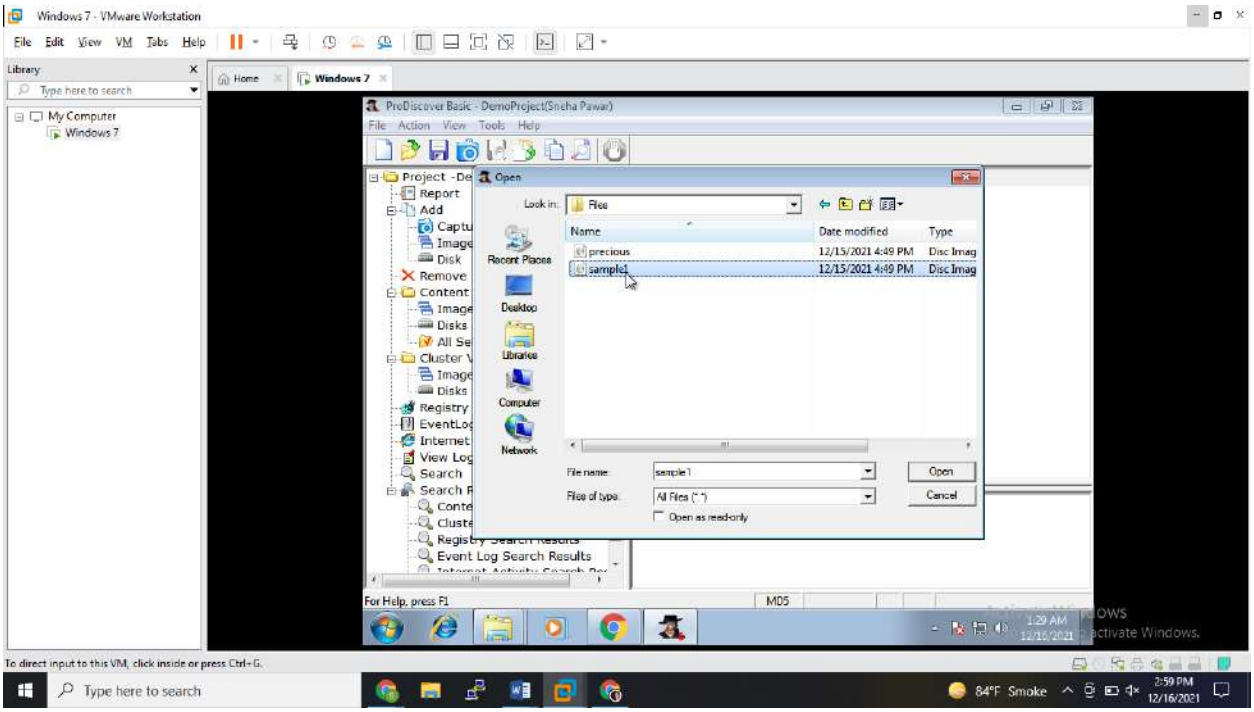
First download the ProDiscover and install it in pc and open. Enter Project Number, Project File Name, and description in ProDiscover Basic software. Click on Open.



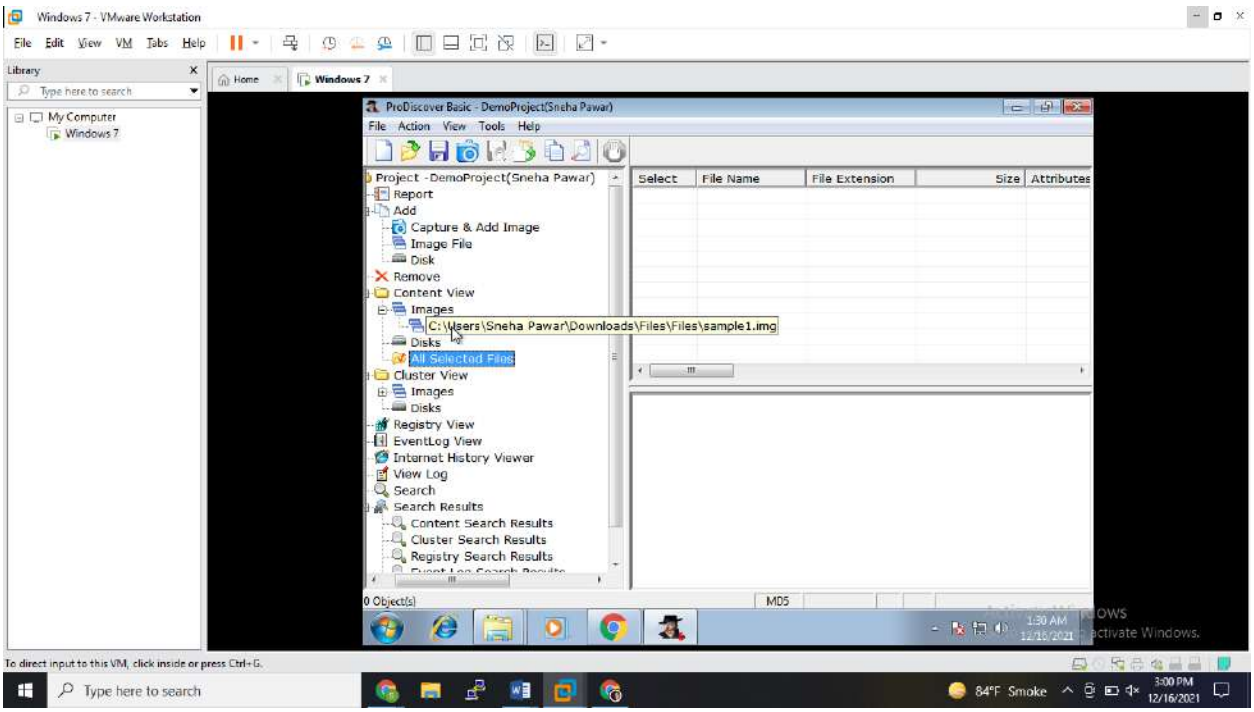
Click on Image File & browse for sample1 file. Sample1 is a sample disk file, as we are not using any USB drive or physical drive. So we will use the sample1 file.

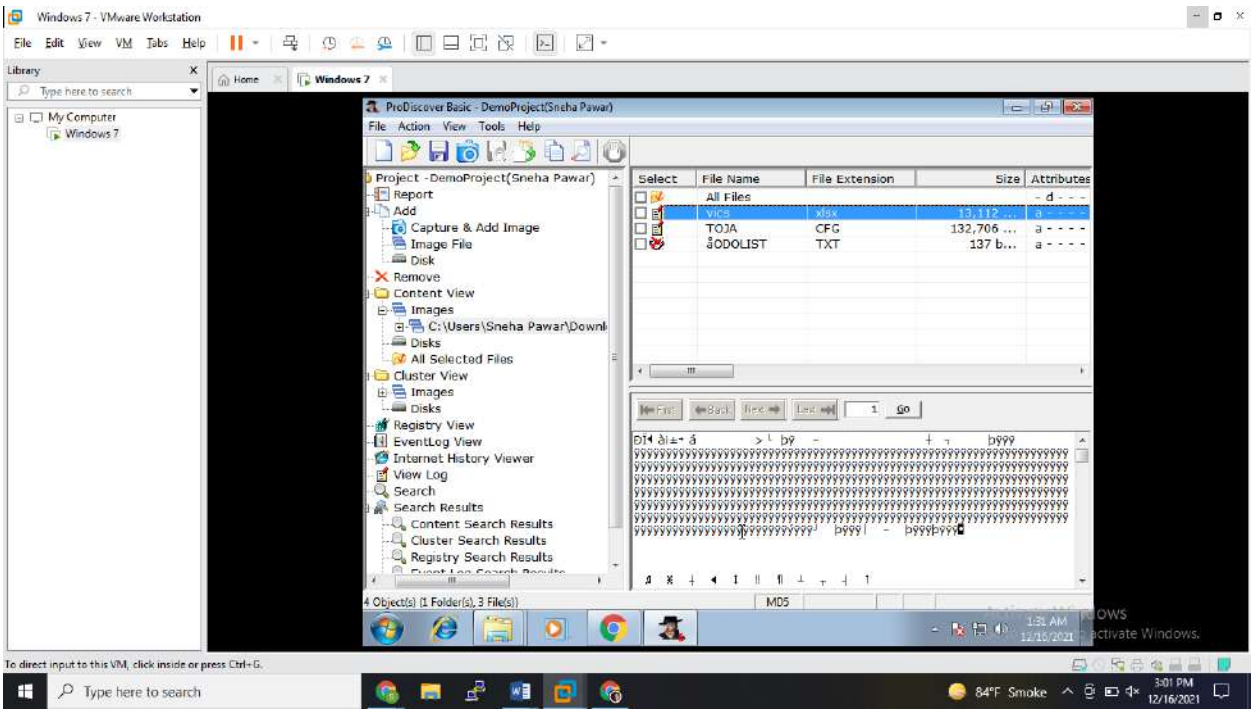


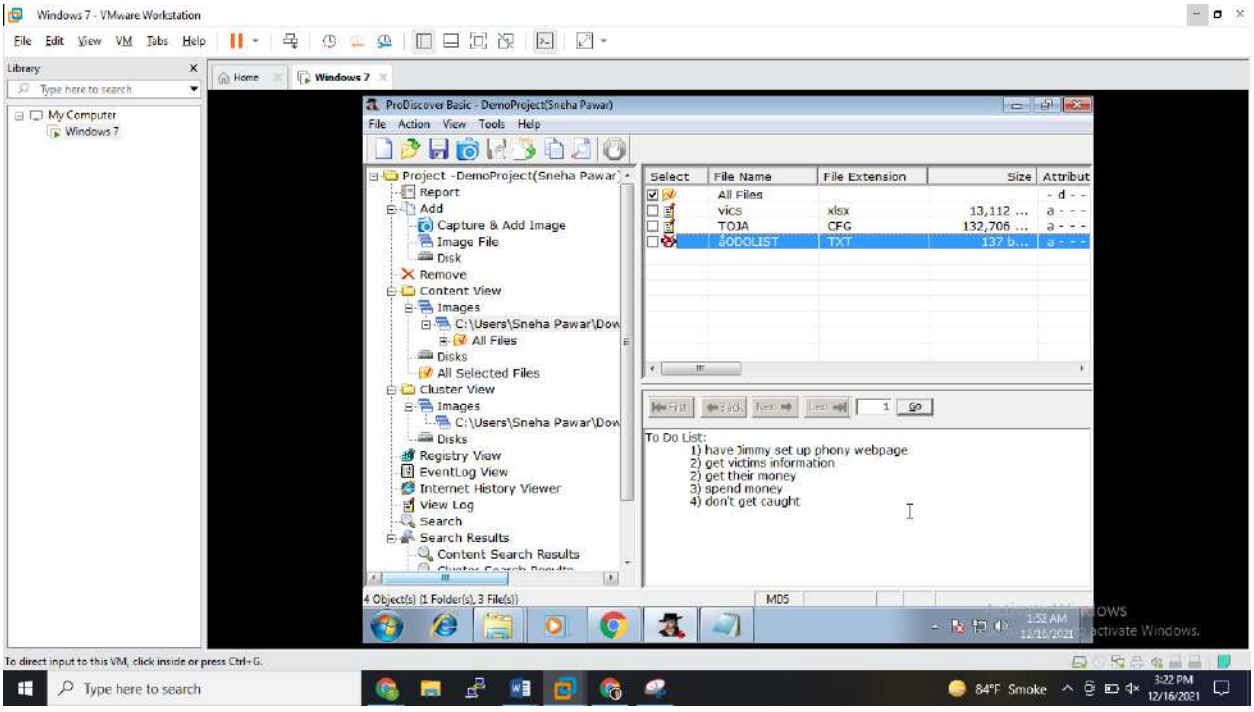
Click on Open.

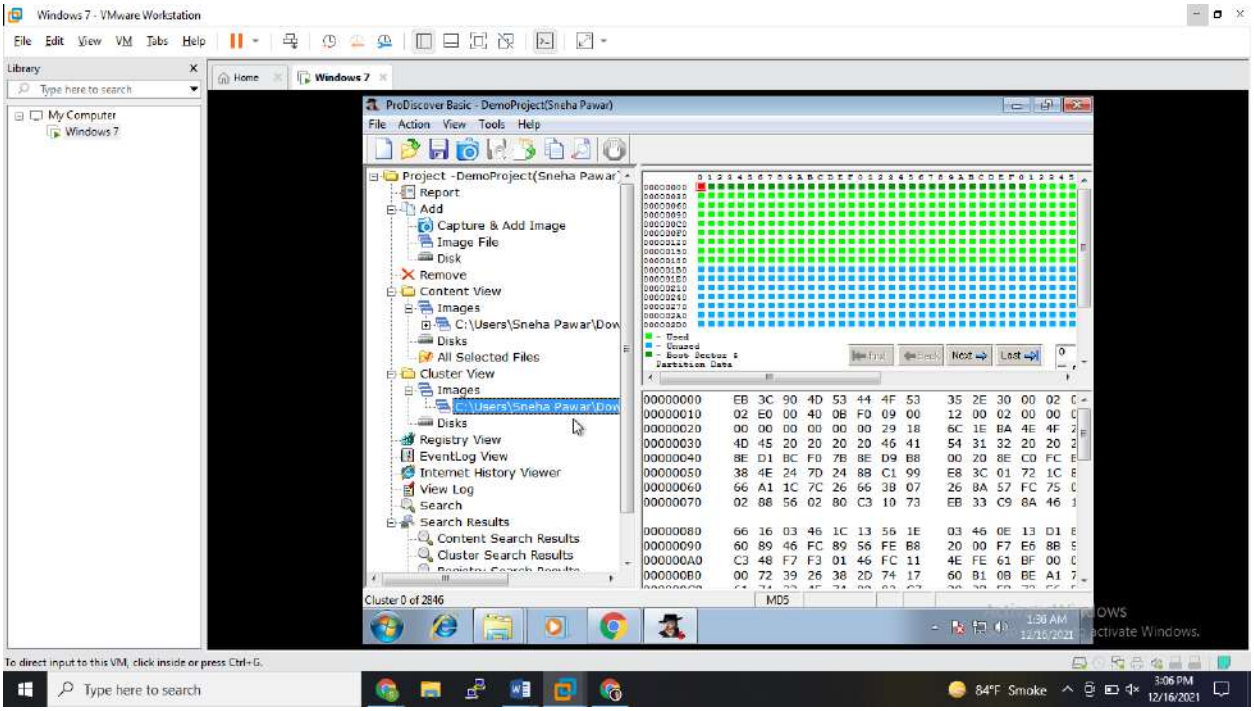


Now the project will open & go to the left menu and click on Content view. Then it will show you all the contents of evidence image file.

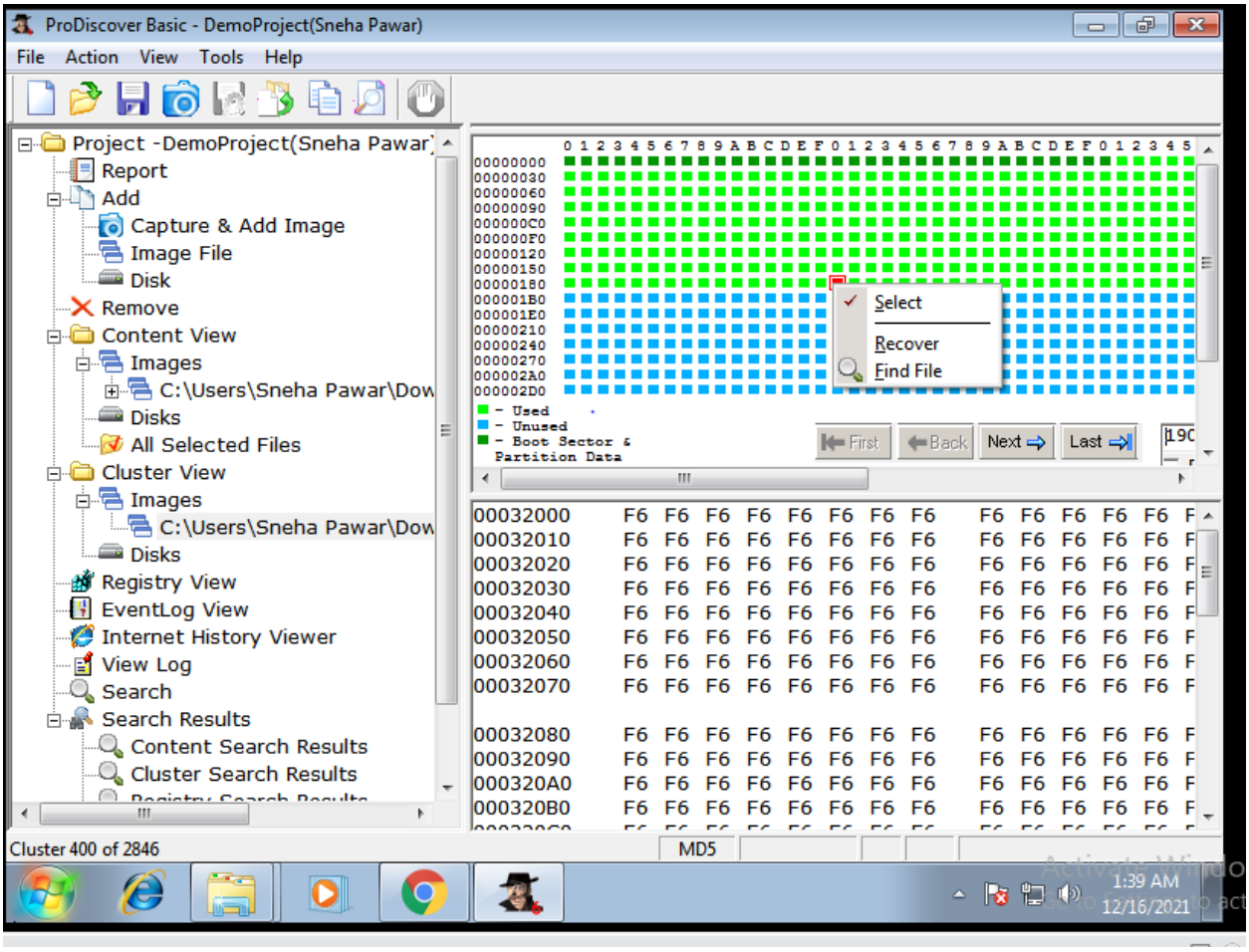



Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
ProDiscover Basic - DemoProject(Sneha Pawar)
File Action View Tools Help
Project -DemoProject(Sneha Pawar)
Report
Add
Capture & Add Image
Image File
Disk
Remove
Content View
Images
C:\Users\Sneha Pawar\Downl
Disks
All Selected Files
Cluster View
Images
Disks
Registry View
EventLog View
Internet History Viewer
View Log
Search
Search Results
Content Search Results
Cluster Search Results
Registry Search Results
Select
File Name
File Extension
Size
Attributes
All Files
vics
xlsx
13,112 ...
TOJA
CFG
132,706 ...
ŠODOLIST
TXT
137 b...
Go
4 Object(s) (1 Folder(s), 3 File(s))
MD5
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
84°F Smoke
3:01 PM
12/16/2021

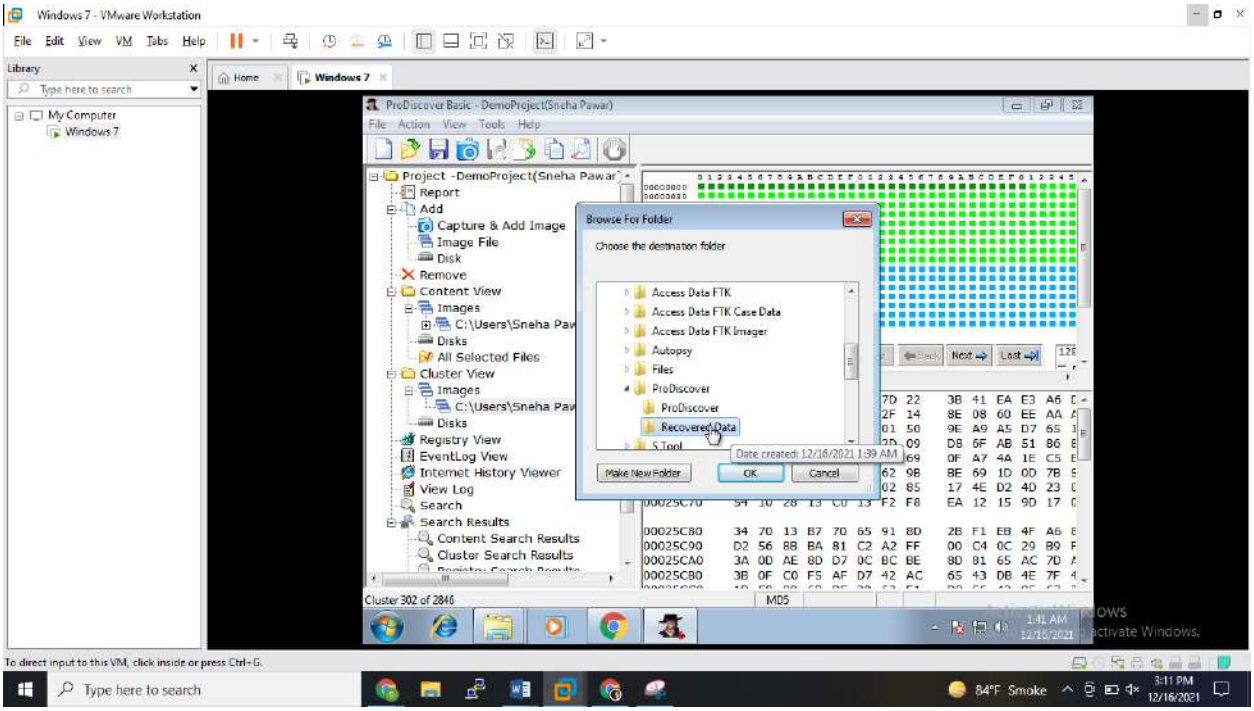

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
ProDiscover Basic - DemoProject(Sneha Pawar)
File Action View Tools Help
Project -DemoProject(Sneha Pawar)
Report
Add
Capture & Add Image
Image File
Disk
Remove
Content View
Images
C:\Users\Sneha Pawar\Dow
All Files
Disks
All Selected Files
Cluster View
Images
C:\Users\Sneha Pawar\Dow
Disks
Registry View
EventLog View
Internet History Viewer
View Log
Search
Search Results
Content Search Results
Select
File Name
File Extension
Size
Attribut
All Files
vics
xlsx
13,112 ...
TOJA
CFG
132,706 ...
ŠODOLIST
TXT
137 b...
Go
To Do List:
1) have Jimmy set up phony webpage
2) get victims information
2) get their money
3) spend money
4) don't get caught
4 Object(s) (1 Folder(s), 3 File(s))
MD5
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
84°F Smoke
3:22 PM
12/16/2021

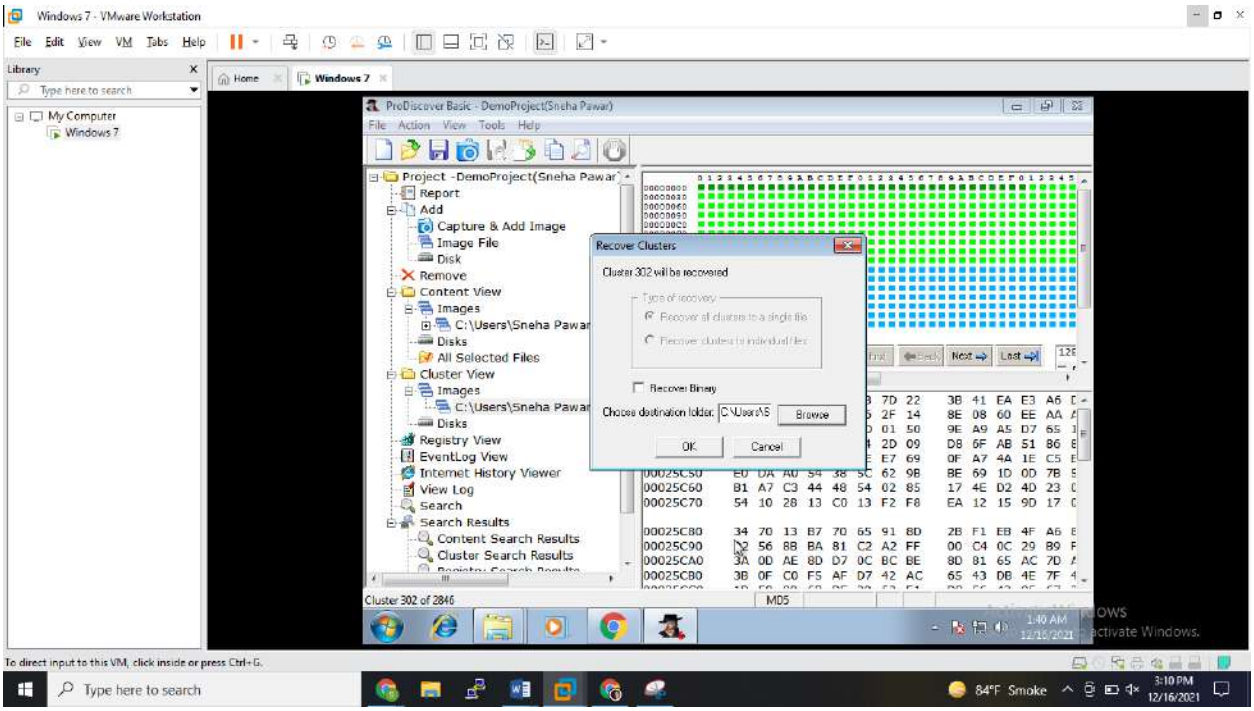


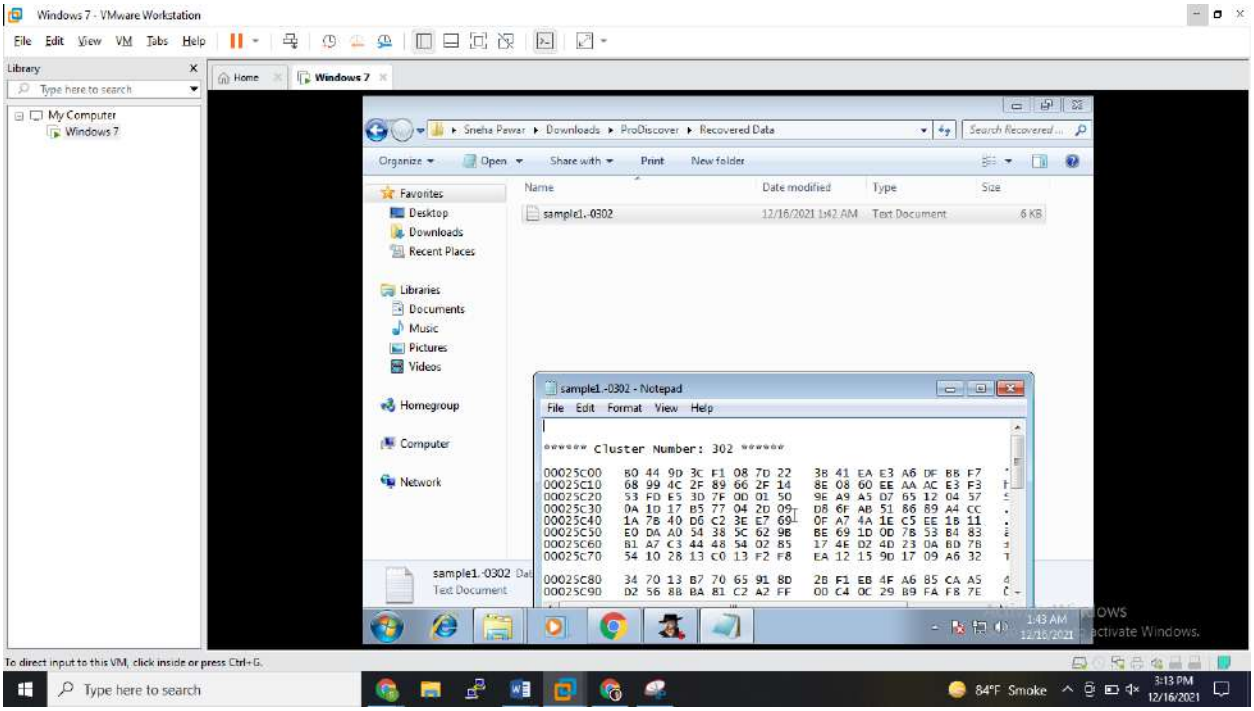
Right click on it and click on recover.



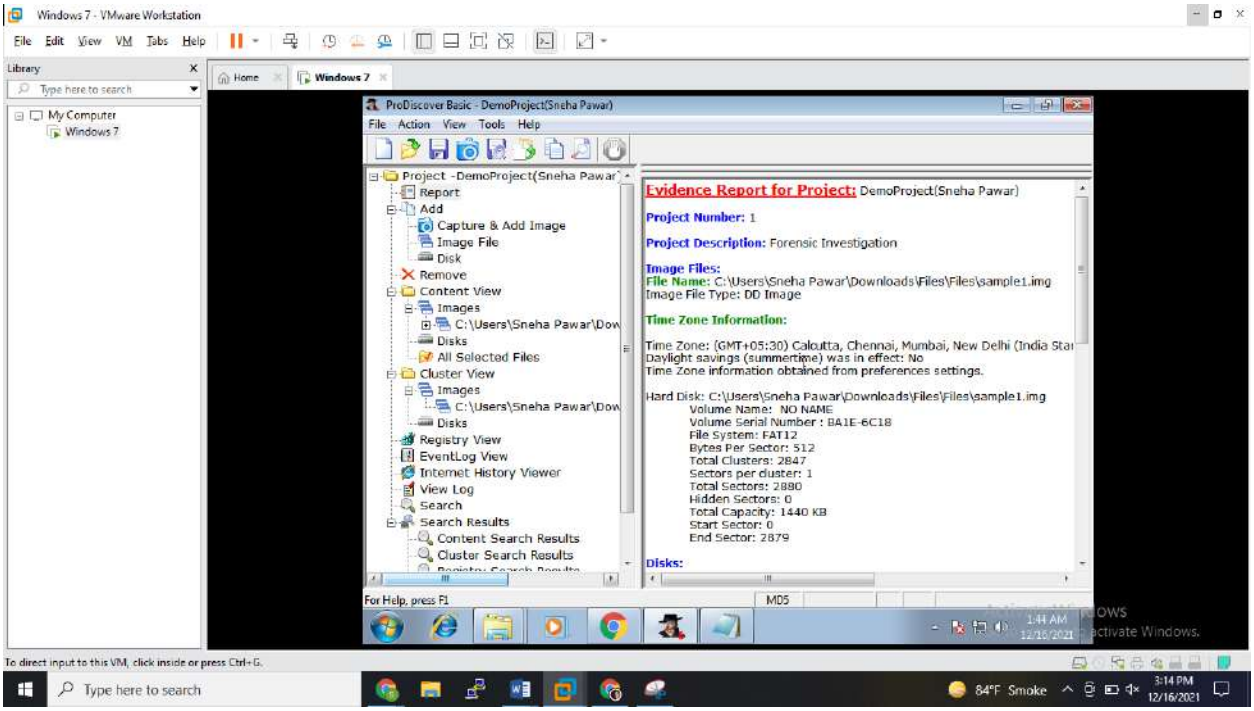
Browse for the path where you want to recover the data.


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
ProDiscover Basic - DemoProject(Sneha Pawar)
File Action View Tools Help
Project -DemoProject(Sneha Pawar)
Report
Add
Capture & Add Image
Image File
Disk
Remove
Content View
Images
C:\Users\Sneha Paw
Disks
All Selected Files
Cluster View
Images
C:\Users\Sneha Paw
Disks
Registry View
EventLog View
Internet History Viewer
View Log
Search
Search Results
Content Search Results
Cluster Search Results
Browse For Folder
Choose the destination folder
Access Data FTK
Access Data FTK Case Data
Access Data FTK Imager
Autopsy
Files
ProDiscover
ProDiscover
Recovered Data
S Tool
Date created: 12/16/2021 1:39 AM
Make New Folder
OK
Cancel
Cluster 302 of 2846
MD5
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
84°F Smoke
3:11 PM
12/16/2021


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
ProDiscover Basic - DemoProject(Sneha Pawar)
File Action View Tools Help
Project -DemoProject(Sneha Pawar)
Report
Add
Capture & Add Image
Image File
Disk
Remove
Content View
Images
C:\Users\Sneha Pawar
Disks
All Selected Files
Cluster View
Images
C:\Users\Sneha Pawar
Disks
Registry View
EventLog View
Internet History Viewer
View Log
Search
Search Results
Content Search Results
Cluster Search Results
Recover Clusters
Cluster 302 will be recovered
Type of recovery
Recover all clusters to a single file
Recover clusters to individual files
Recover Binary
Choose destination folder:
C:\Users\S
Browse
OK
Cancel
Cluster 302 of 2846
MD5
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
84°F Smoke
3:10 PM
12/16/2021



You can also see the generated report. To generate the automatic report click on report tab under the view menu. Then it will show you Evidence Report.



Practical No. 04

Aim: Creating Image using File Recovery Tools[FTK Imager].

What is File Recover?

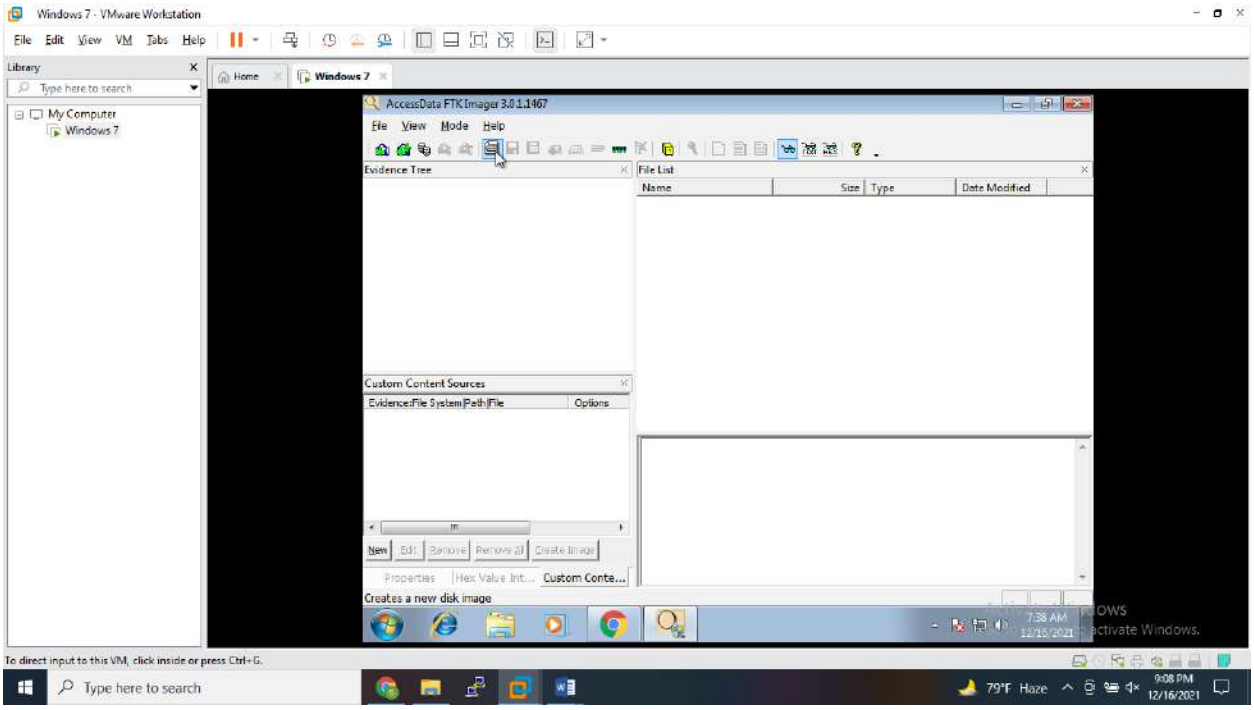
In computing, **data recovery** is a process of salvaging inaccessible, lost, corrupted, damaged or formatted data from secondary storage, removable media or files, when the data stored in them cannot be accessed in a usual way. The data is most often salvaged from storage media such as internal or external hard disk drives (HDDs), solid-state drives (SSDs), USB flash drives, magnetic tapes, CDs, DVDs, RAID subsystems, and other electronic devices. Recovery may be required due to physical damage to the storage devices or logical damage to the file system that prevents it from being mounted by the host operating system (OS).

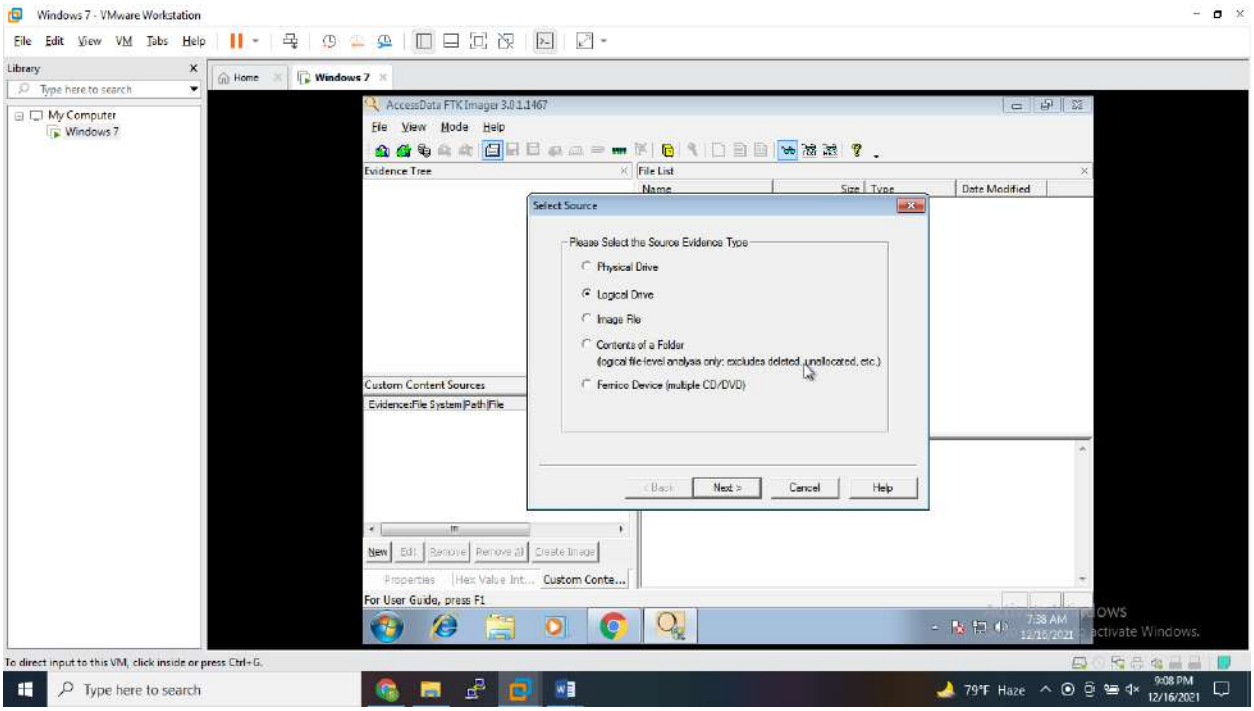
What is FTK Imager?

FTK® Imager is **a data preview and imaging tool used to acquire data (evidence) in a forensically sound manner** by creating copies of data without making changes to the original evidence. ... Export files and folders from forensic images.

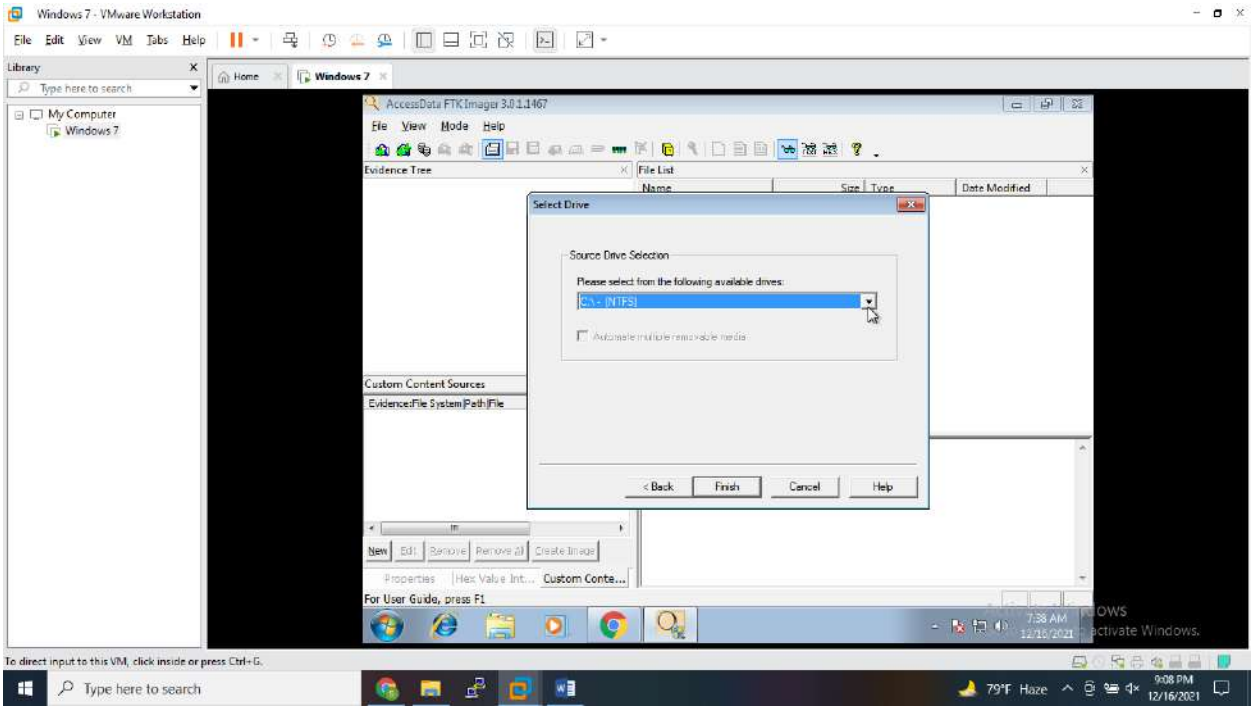
Steps:

Open Access FTK Imager. Click on create Disk image of a logical drive. Select create disk image.

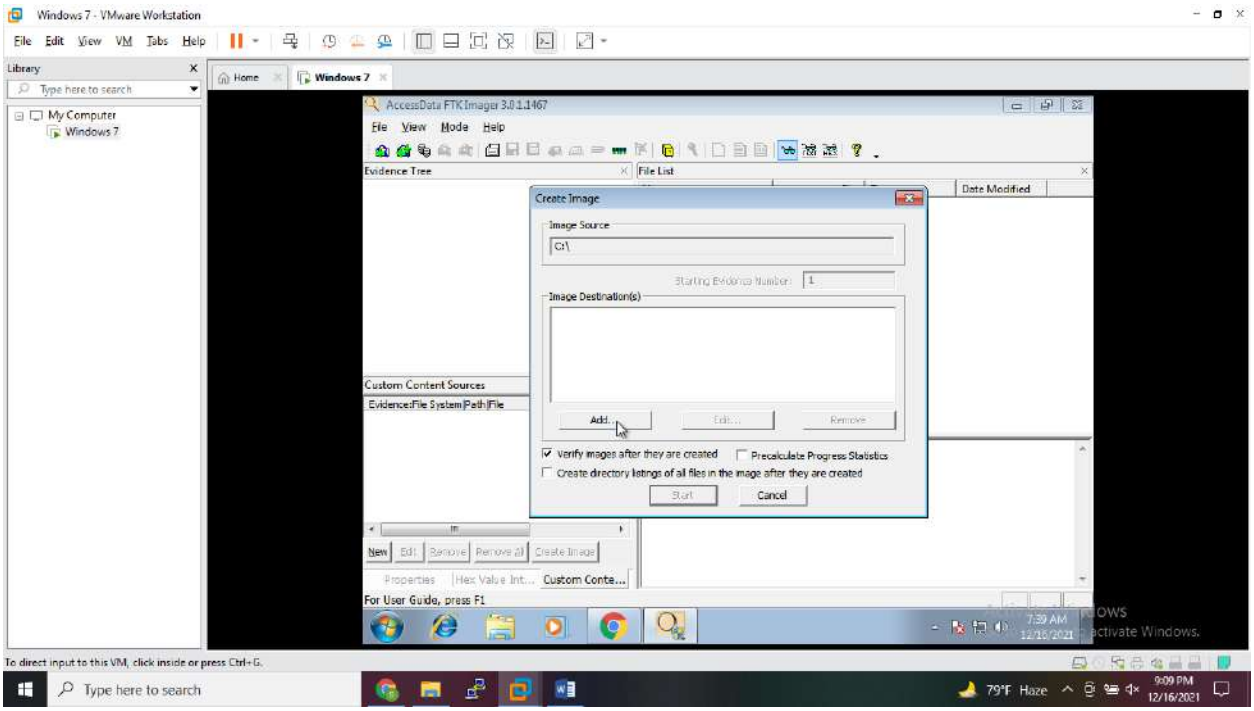




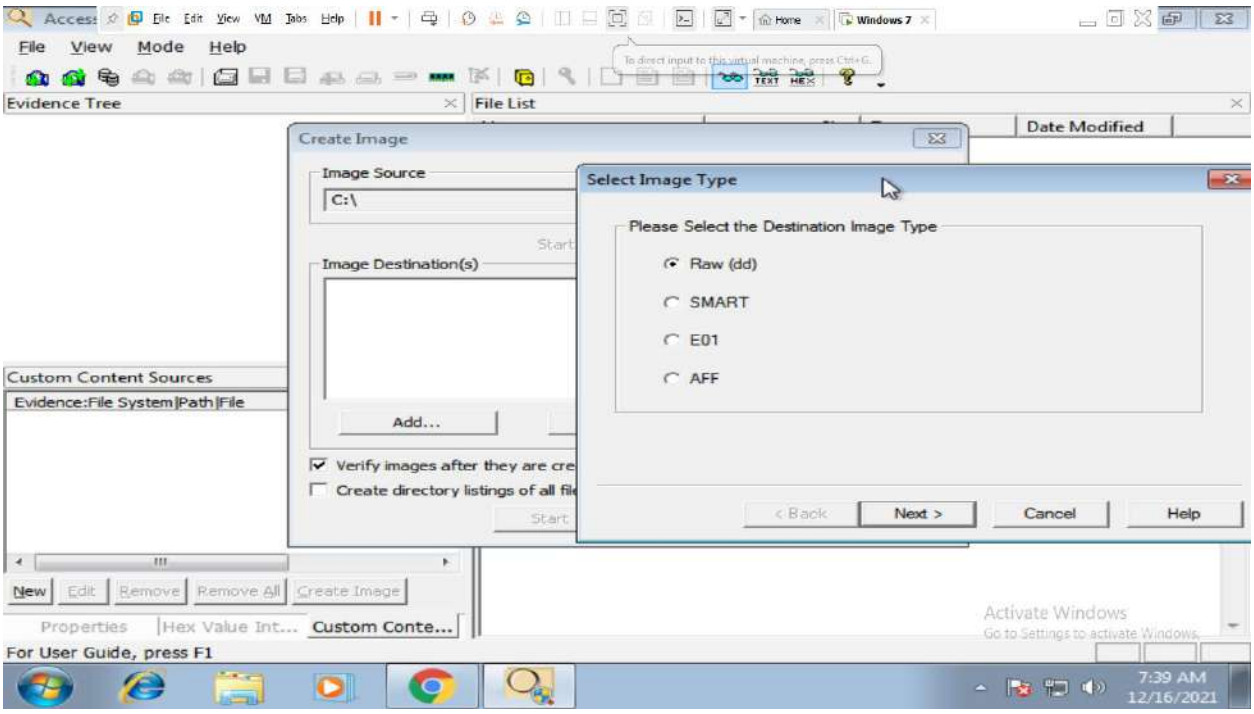
Select a Drive and click on Finish.



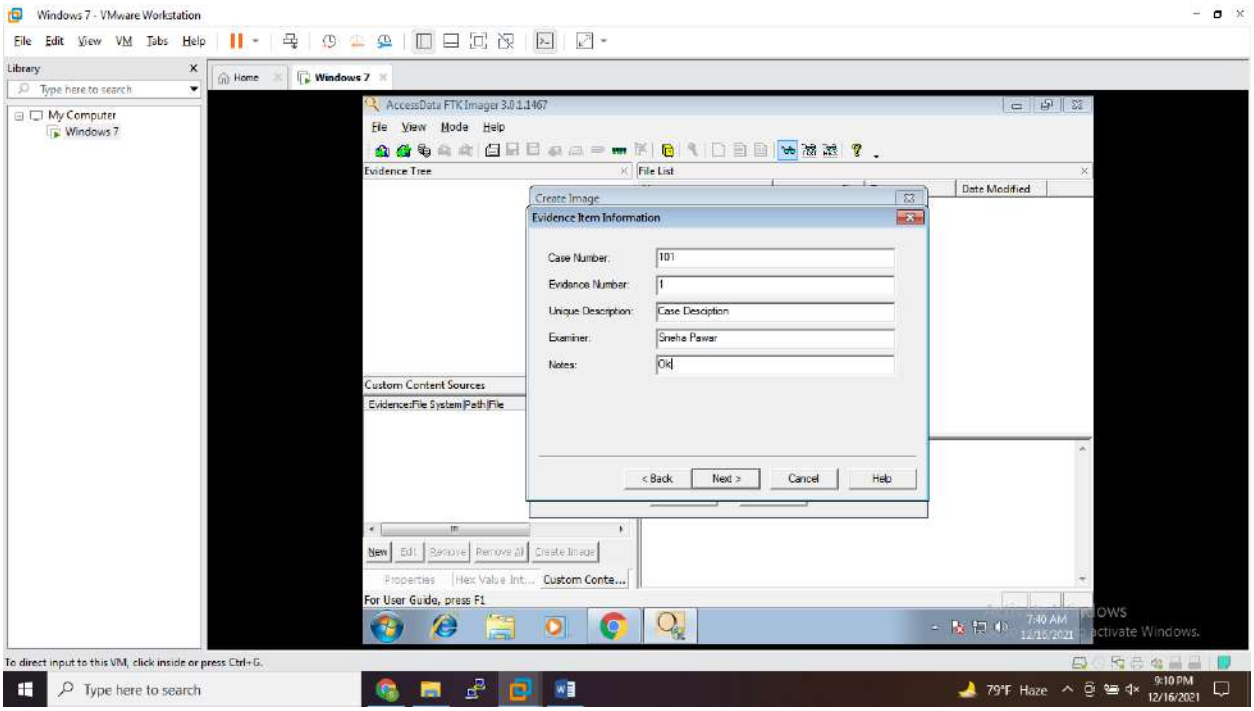
Click on ADD.



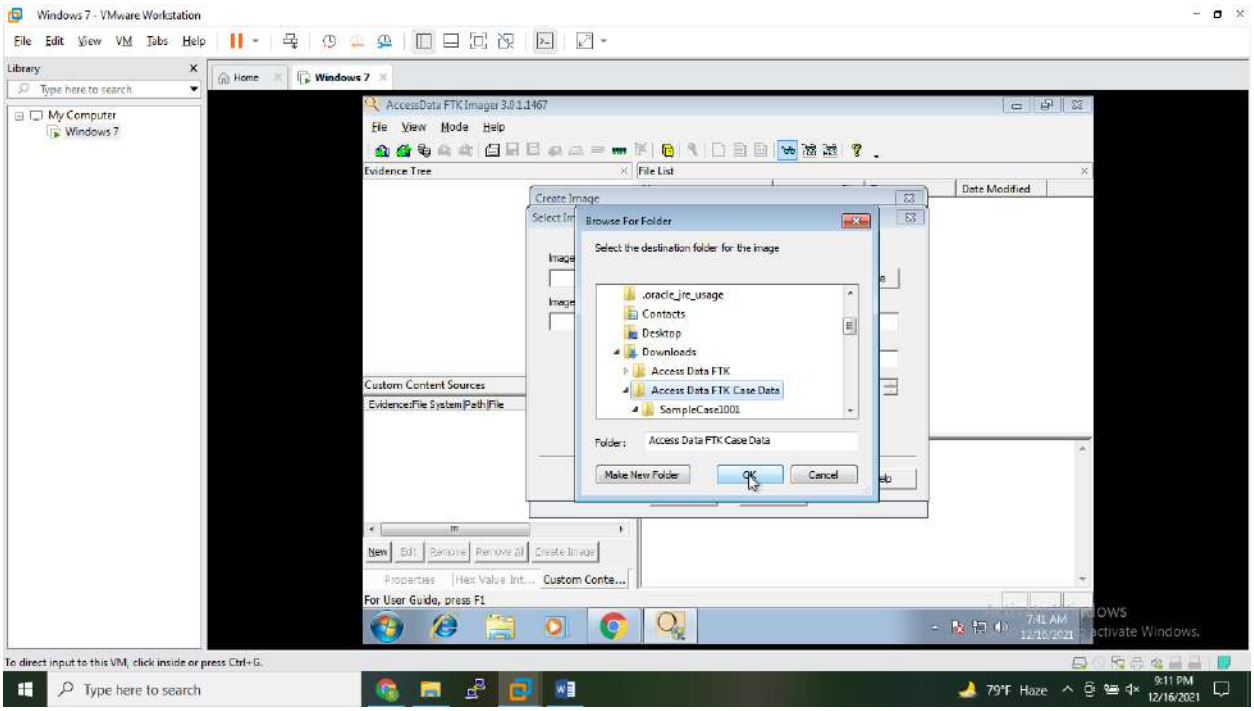
And select Image type as Raw(dd).

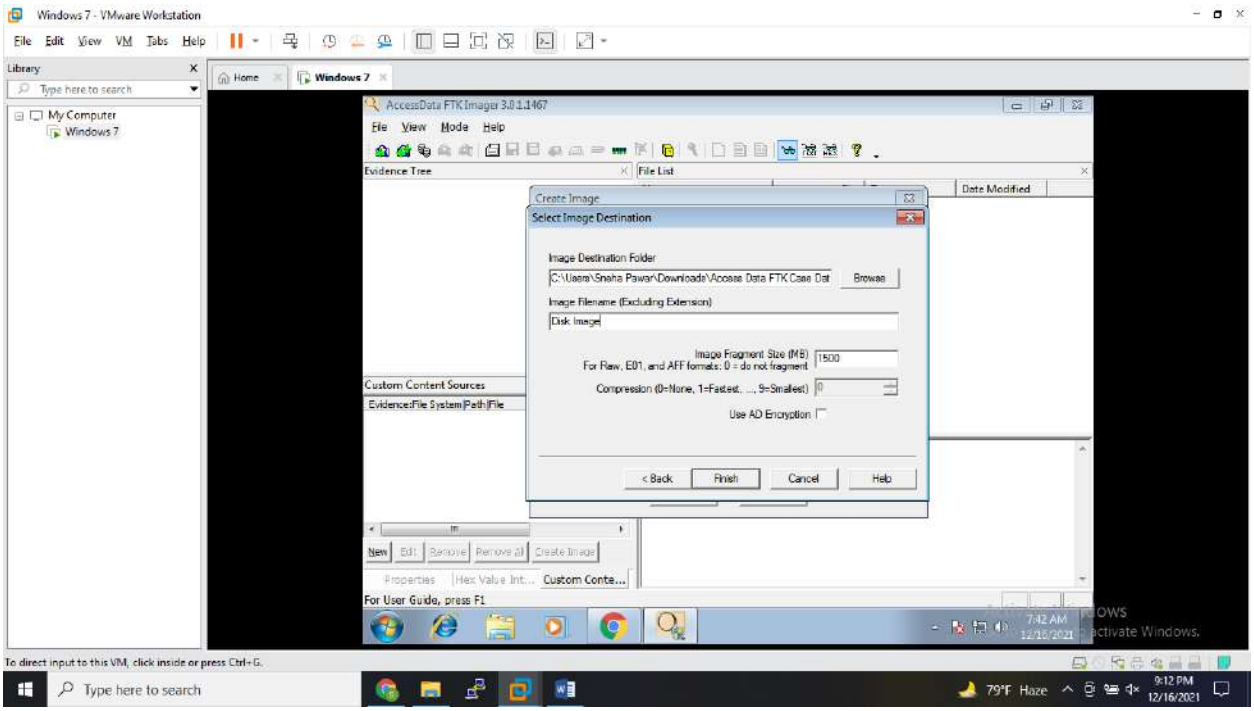


Fill the evidence item information.

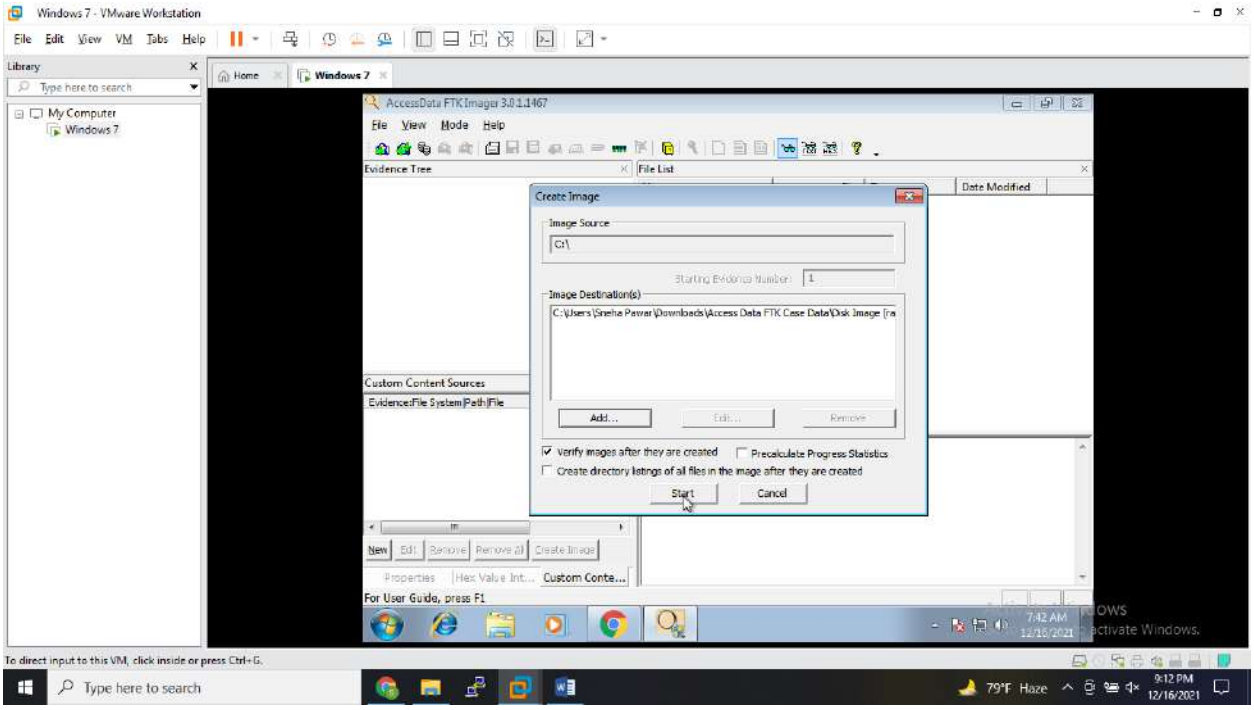


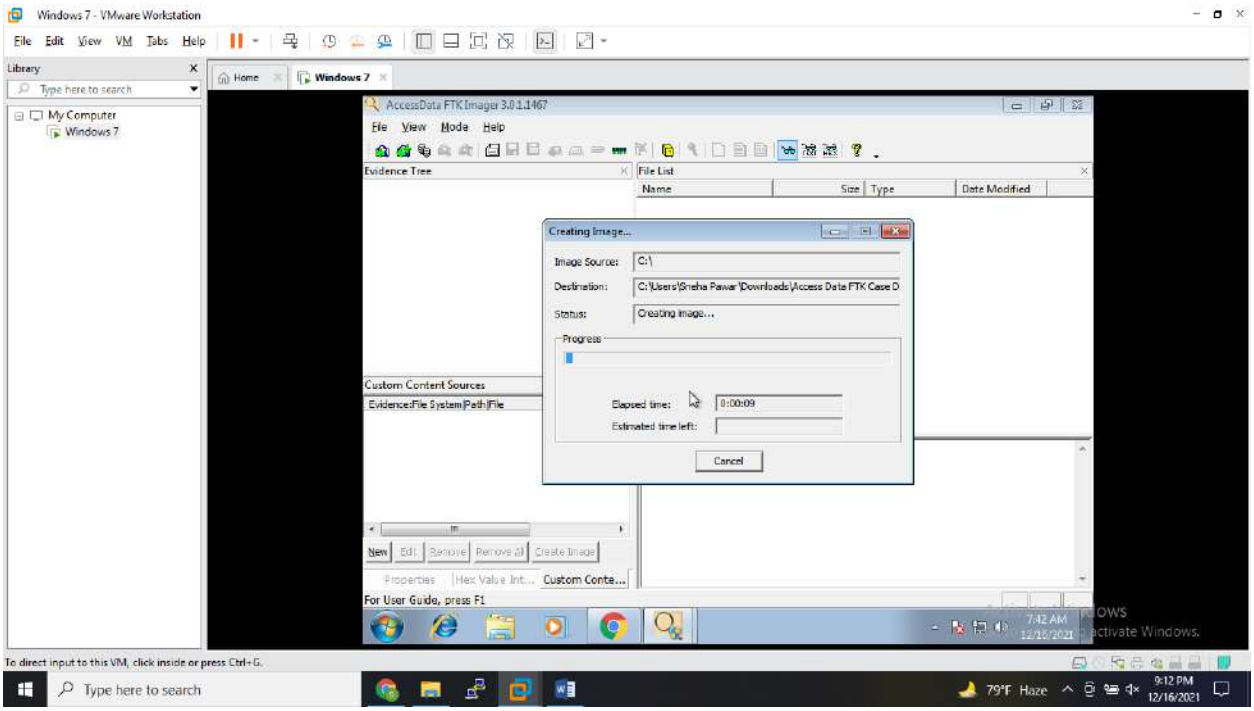
And browse for the location where you want to store the case data.



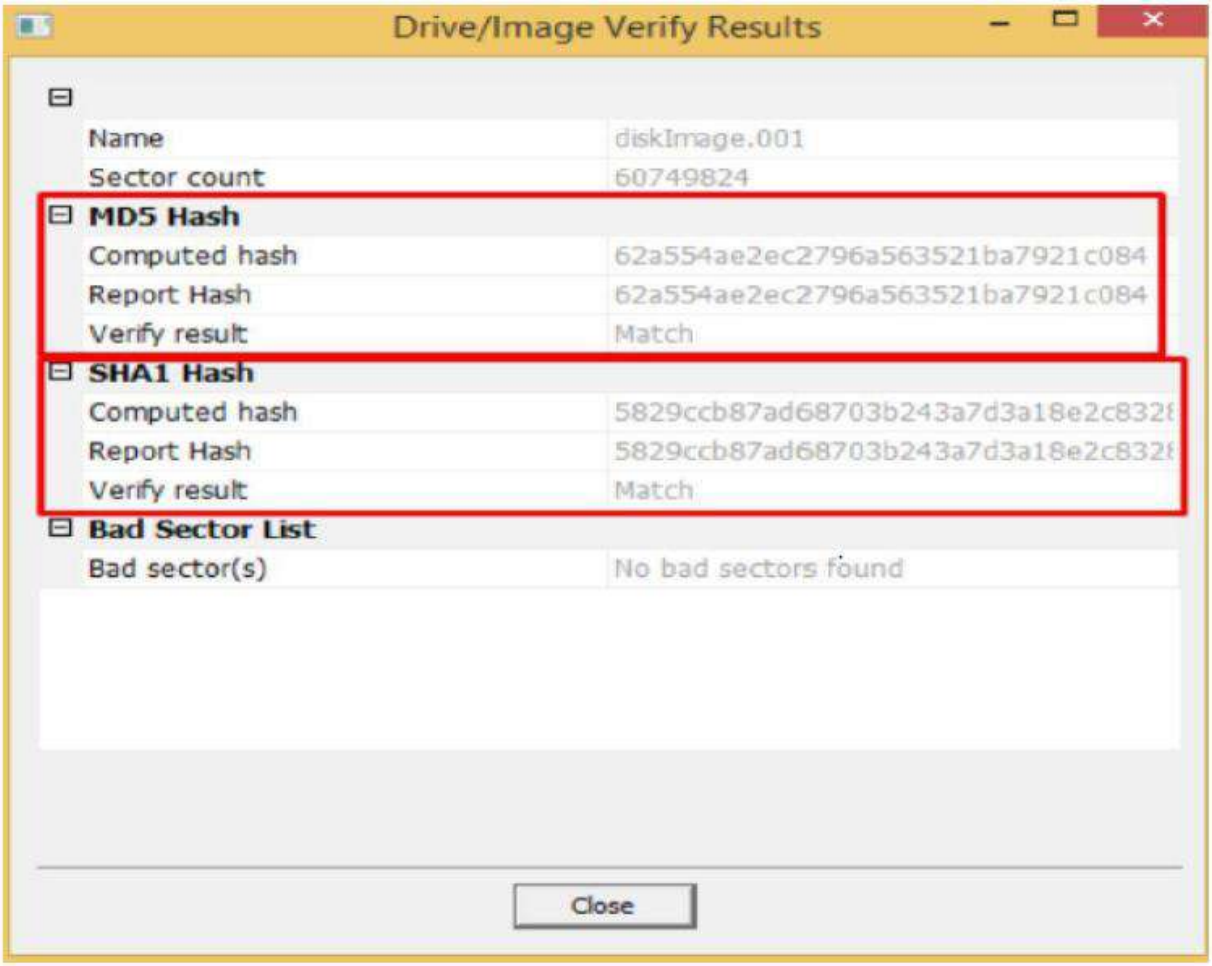


Then click on Start.





It will create the hashes of the data and verify it. After The Processing, A Dialog Box Will Show the Results.


Drive/Image Verify Results
Name
diskImage.001
Sector count
60749824
MD5 Hash
Computed hash
62a554ae2ec2796a563521ba7921c084
Report Hash
62a554ae2ec2796a563521ba7921c084
Verify result
Match
SHA1 Hash
Computed hash
5829ccb87ad68703b243a7d3a18e2c832
Report Hash
5829ccb87ad68703b243a7d3a18e2c832
Verify result
Match
Bad Sector List
Bad sector(s)
No bad sectors found
Close

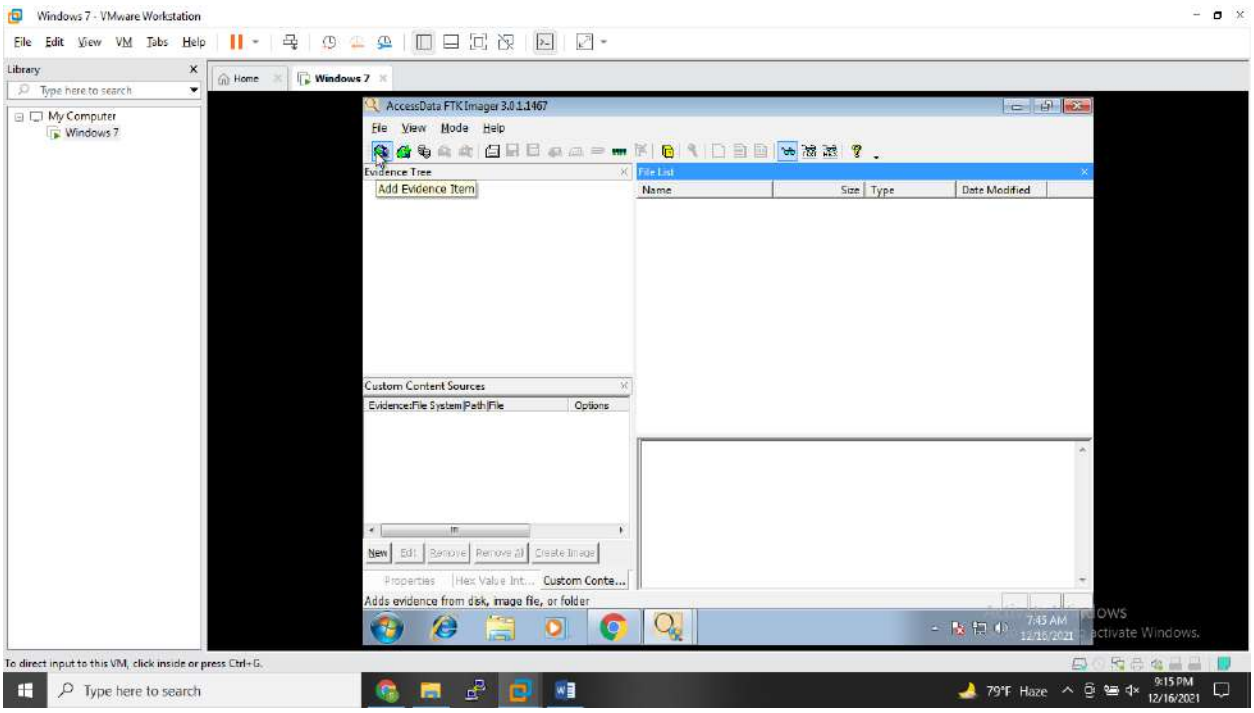
Practical No. 05

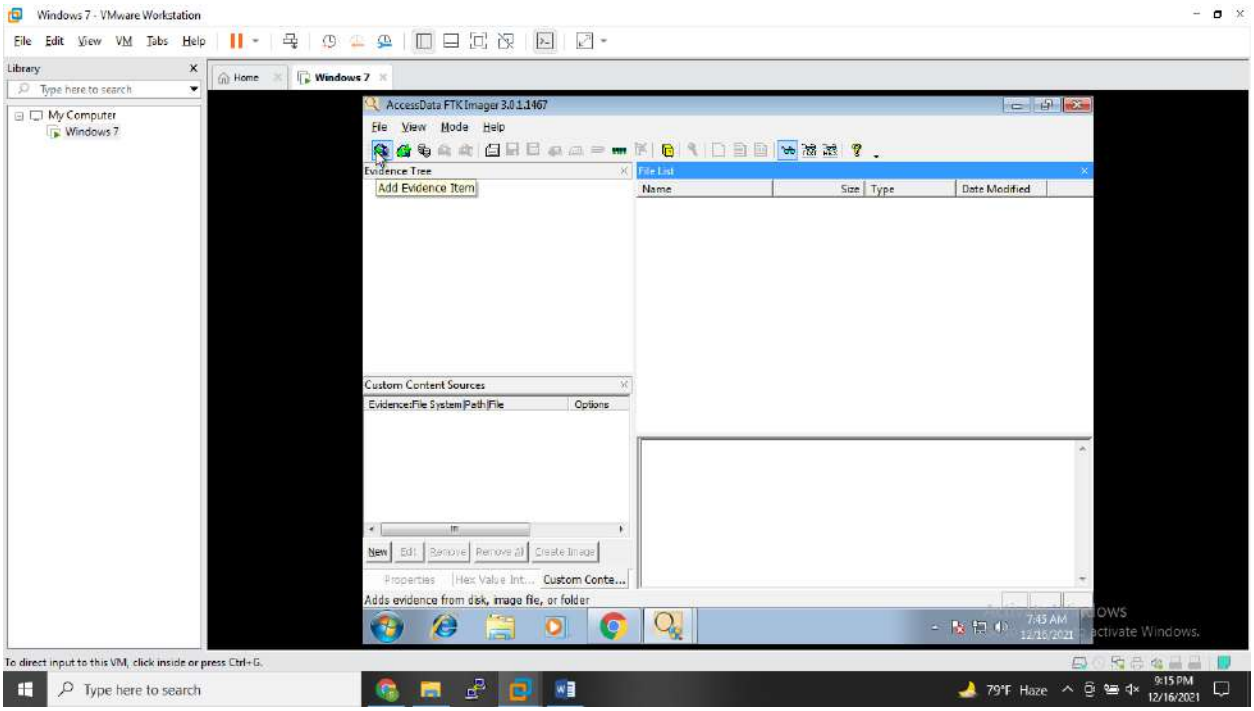
Aim: File Recovery Tools [FTK Imager] using evidence

What is FTK Imager?

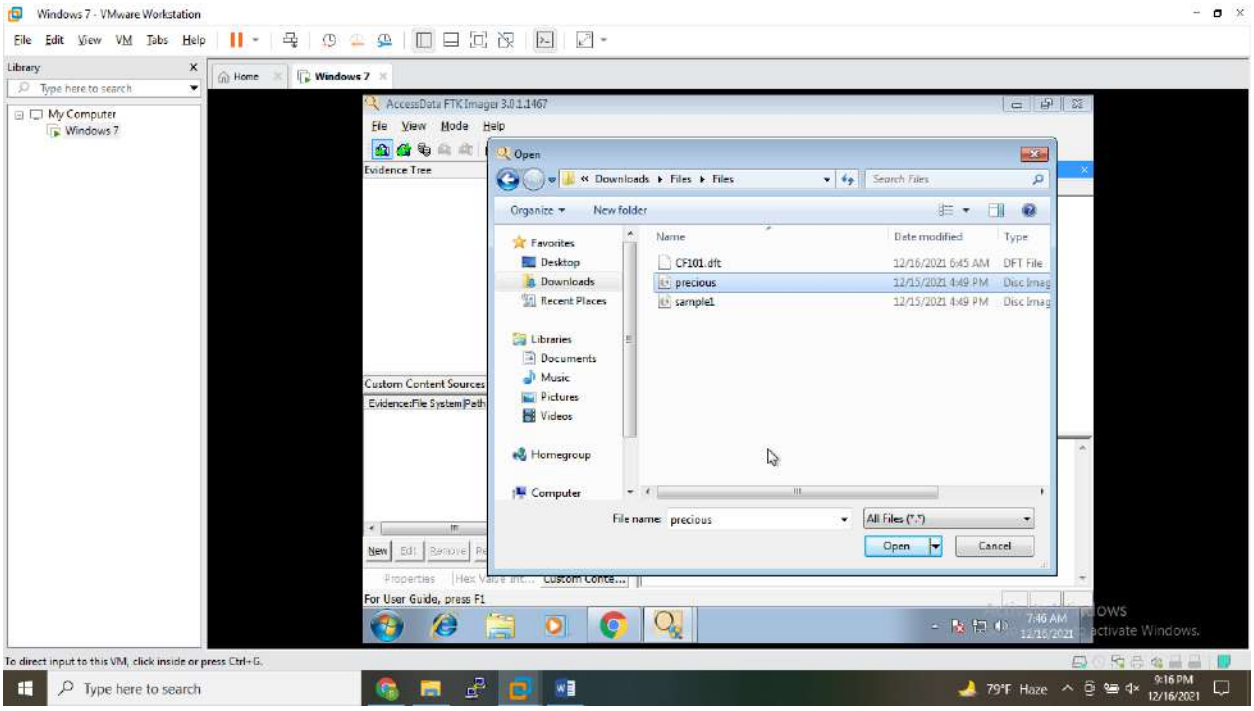
FTK® Imager is **a data preview and imaging tool used to acquire data (evidence) in a forensically sound manner** by creating copies of data without making changes to the original evidence. ... Export files and folders from forensic images.

Open Access Data FTK Imager and click on Add Evidence Item.

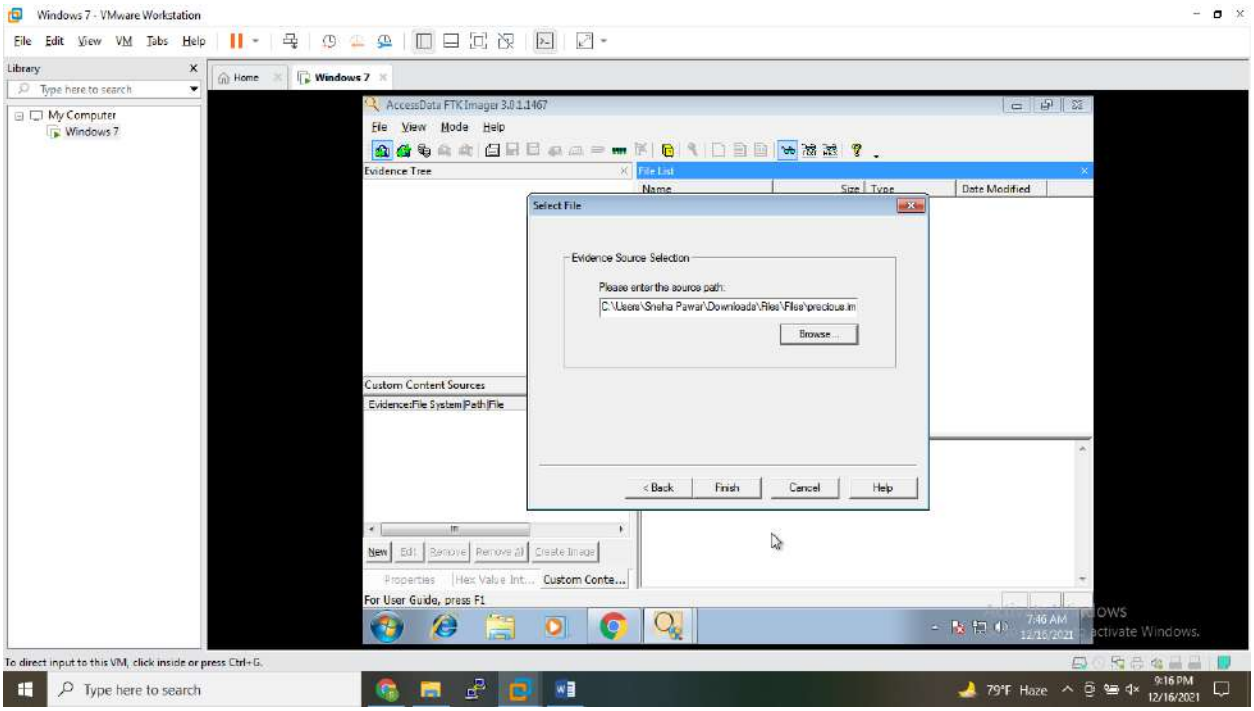




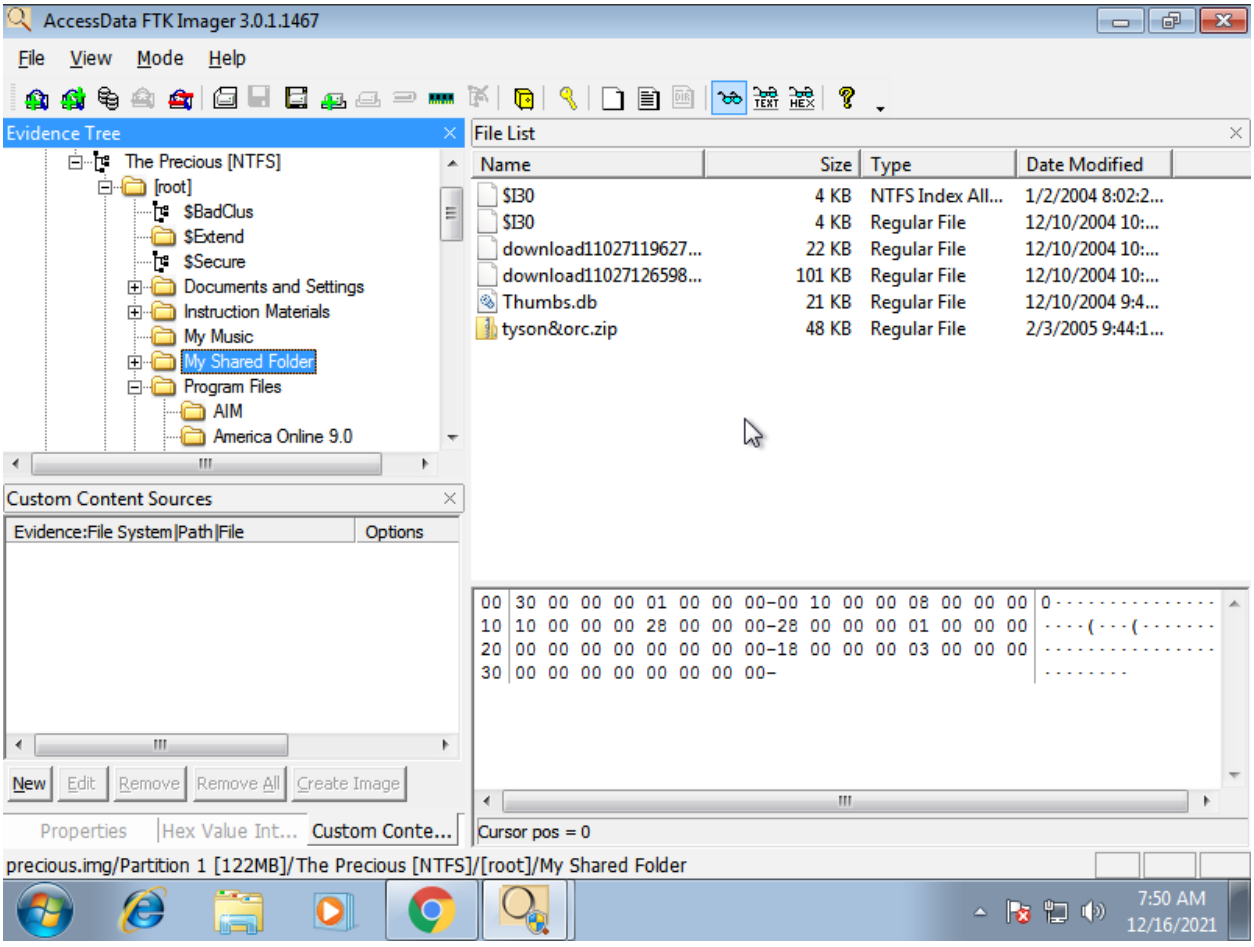
And browse for the precious.img disk image file to add as an evidence.

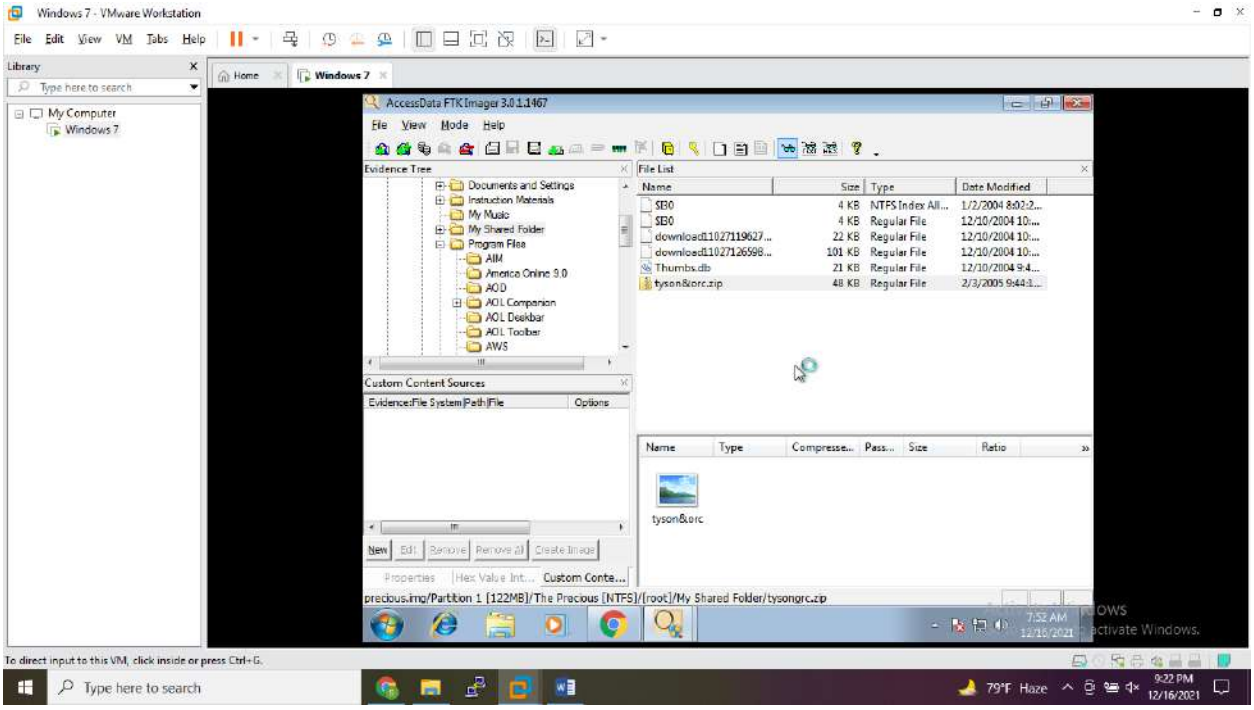


Click on Finish.



Click on My shared folder.




Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK Imager 3.0.1.1467
File View Mode Help
Evidence Tree
Documents and Settings
Instruction Materials
My Music
My Shared Folder
Program Files
AIM
America Online 3.0
AOD
AOL Companion
AOL Deskbar
AOL Toolbar
AWS
File List
Name
Size
Type
Date Modified
SE0
4 KB
NTFS Index All...
1/2/2004 8:02:2...
SE0
4 KB
Regular File
12/10/2004 10:...
download1027119627...
22 KB
Regular File
12/10/2004 10:...
download1027126598...
101 KB
Regular File
12/10/2004 10:...
Thumbs.db
21 KB
Regular File
12/10/2004 9:4...
tyson&orc.zip
48 KB
Regular File
2/3/2005 9:44:3...
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Int...
Custom Conte...
Name
Type
Compresse...
Pass...
Size
Ratio
tyson&orc
precious.img/Partition 1 [122MB]/The Precious [NTFS]/[root]/My Shared Folder/tysongrc.zip
7:52 AM
12/16/2021
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
9:22 PM
12/16/2021

Practical No. 06

Aim: Forensic Investigation Using Steganography Tools [S-Tools].

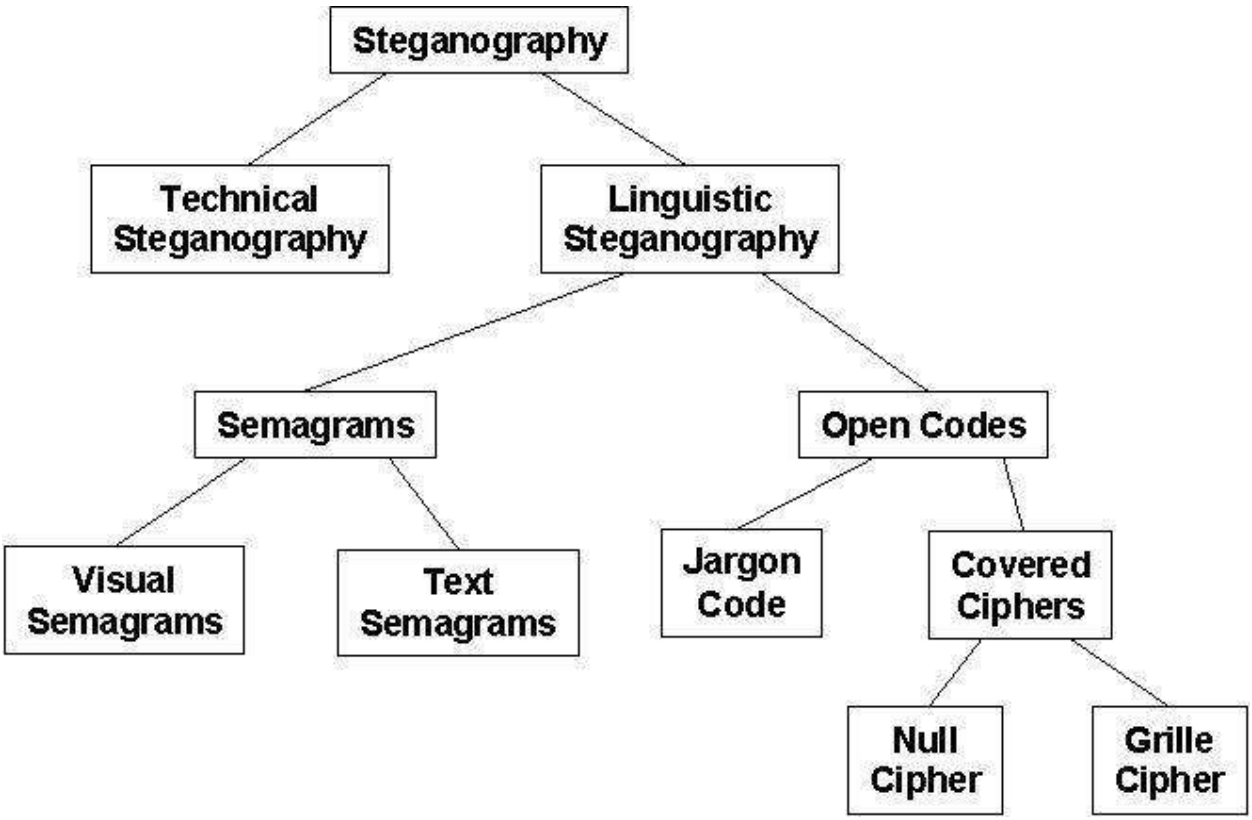
What is Steganography?

Steganography is the art of covered or hidden writing. The purpose of steganography is covert communication to hide a message from a third party. This differs from cryptography, the art of secret writing, which is intended to make a message unreadable by a third party but does not hide the existence of the secret communication. Although steganography is separate and distinct from cryptography, there are many analogies between the two, and some authors categorize steganography as a form of cryptography since hidden communication is a form of secret writing (Bauer 2002). Nevertheless, this paper will treat steganography as a separate field.

Although the term steganography was only coined at the end of the 15th century, the use of steganography dates back several millennia. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been in use for centuries-for fun by children and students and for serious espionage by spies and terrorists. Microdots and microfilm, a staple of war and spy movies, came about after the invention of photography (Arnold et al. 2003; Johnson et al. 2001; Kahn 1996; Wayner 2002).

Steganography hides the covert message but not the fact that two parties are communicating with each other. The steganography process generally involves placing a hidden message in some transport medium, called the carrier. The secret message is embedded in the carrier to form the steganography medium. The use of a steganography key may be employed for encryption of the hidden message and/or for randomization in the steganography scheme. In summary:

steganography_medium = hidden_message + carrier + steganography_key



What is S – Tool?

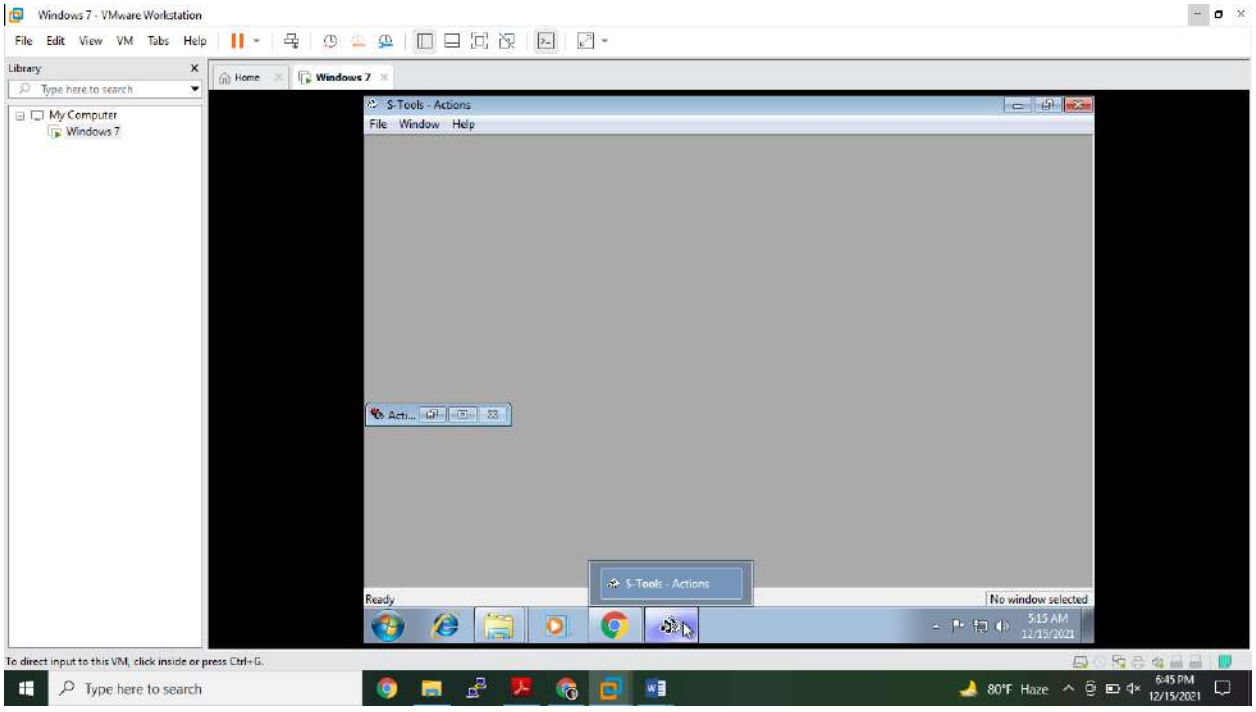
Steganography "Covered Writing"
Steganography tools provide a method that allows a user to hide a file in plain sight. For example, there are a number of stego software tools that allow the user to hide one image inside another. Some of these do it by simply appending the "hidden" file at the tail end of a JPEG file and then add a pointer to the beginning of the file. The most common way that steganography is discovered on a machine is through the detection of the steganography software on the machine. Then comes the arduous task of locating 11 of the files that may possibly contain hidden data. Other, more manual stego techniques may be as simple as hiding text behind other text. In Microsoft Word, text boxes can be placed right over the top of other text, formatted in such a way as to render the text undetectable to a casual observer. Forensic tools will allow the analyst to locate this text, but on opening the file the text won't be readily visible. Another method is to hide images behind other images using the layers feature of some photo enhancement tools, such as Photoshop.

StegAlyzerAS is a tool created by Backbone Security to detect steganography on a system. It works by both searching for known stego artifacts as well as by searching for the program files associated with over 650 steganography toolsets. Steganography hash sets are also available within the NIST database of hash sets. Hash sets are databases of MD5 hashes of known unique files associated with a particular application.

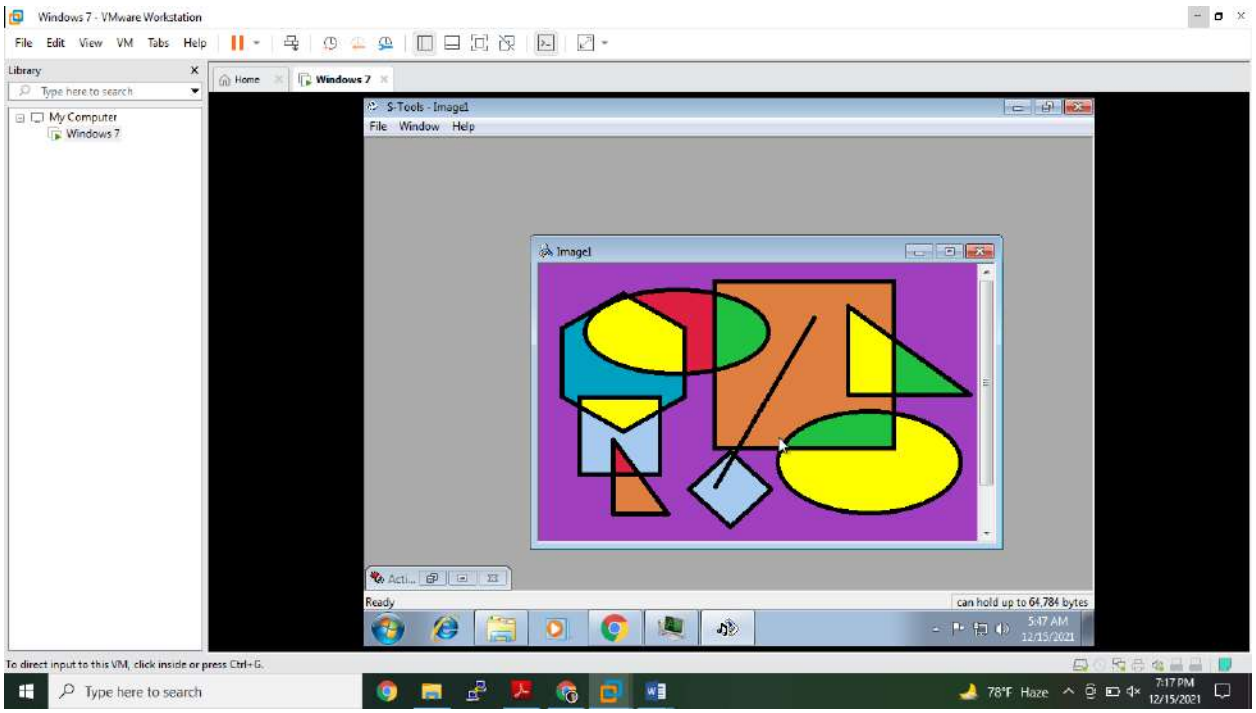
Steps:

Here we are going to hide our textual content in an image file.

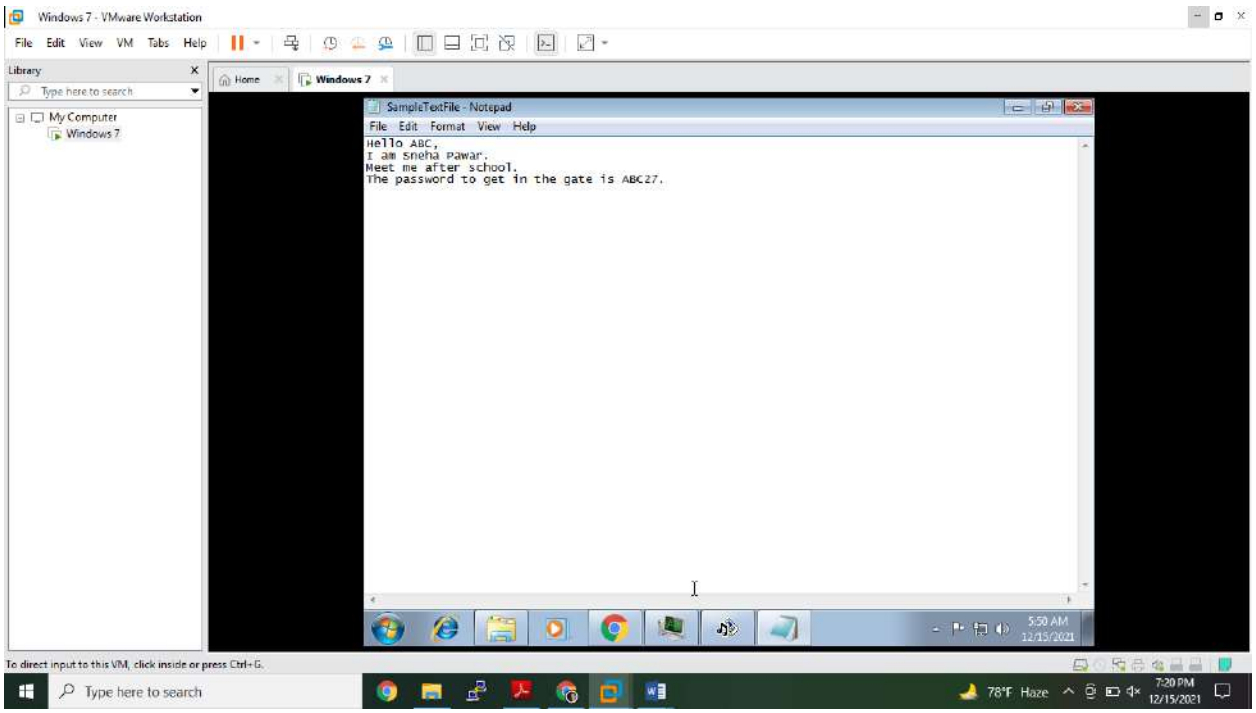
After opening S – Tool Software the interface will look like below.



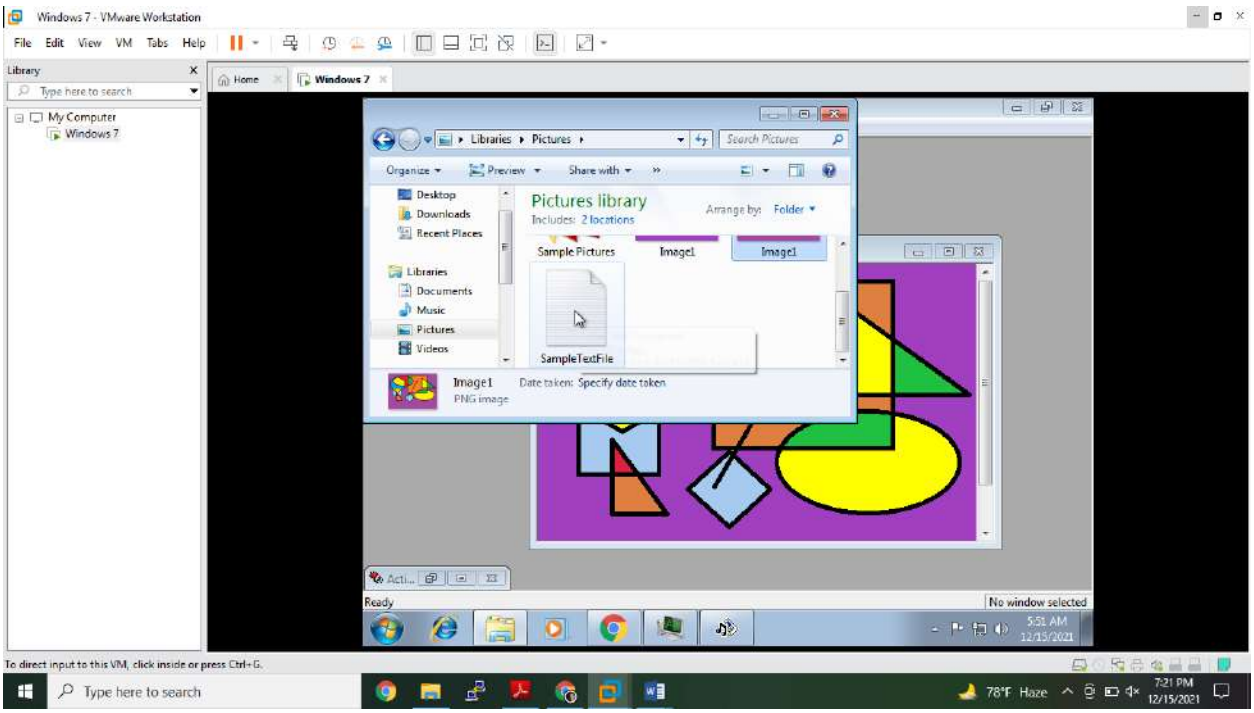
The S – Tool only supports GIF or BMP image files. So drag and drop any image on S – Tool.



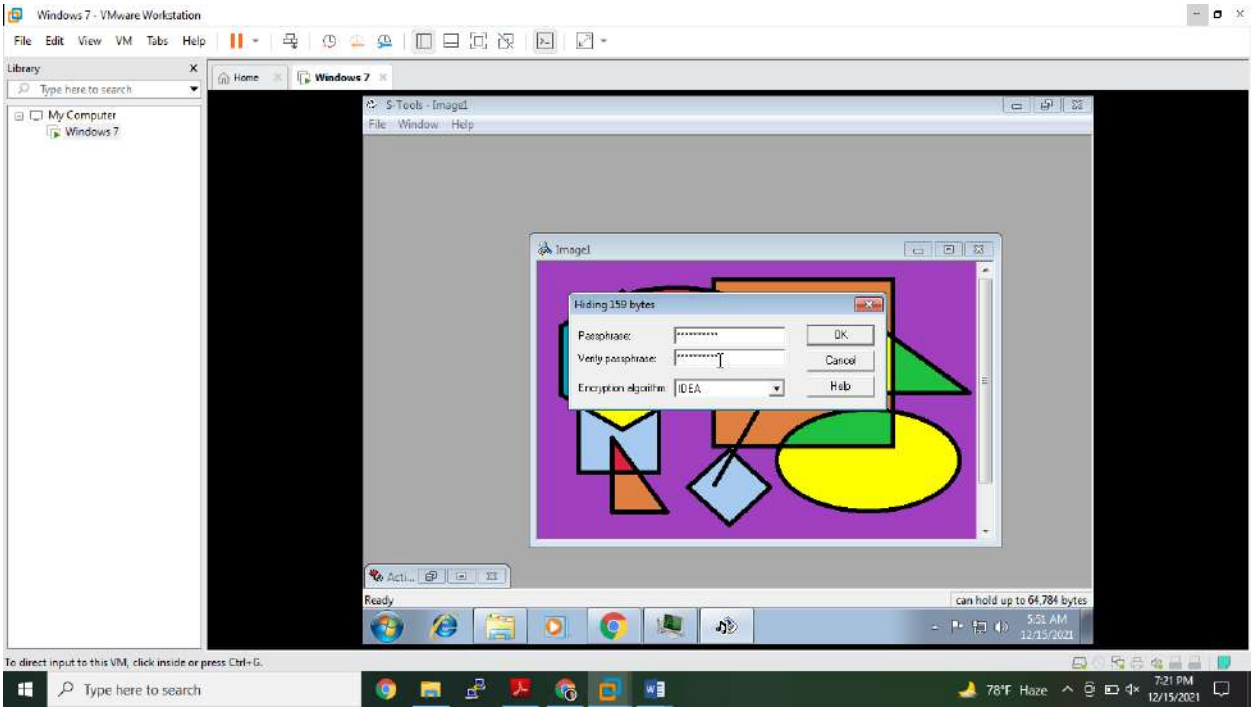
Now create one text file. Type any content that you want to in it.

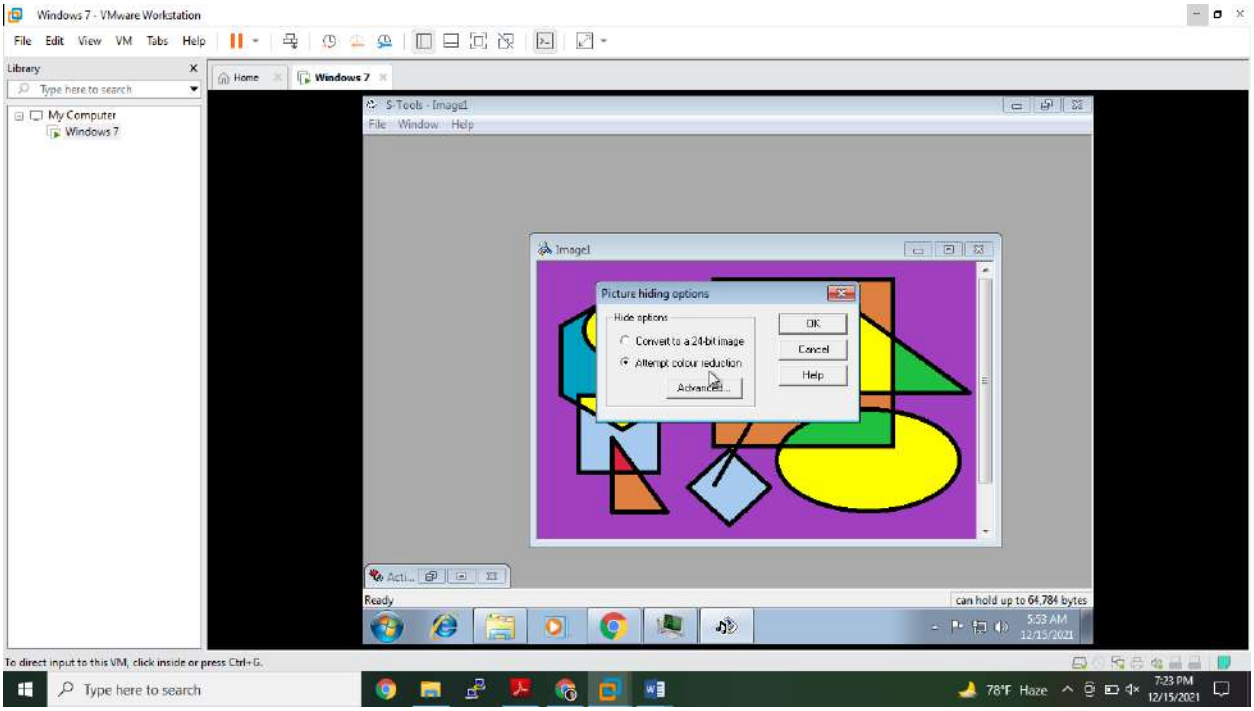


Drag and drop the text file onto the image.

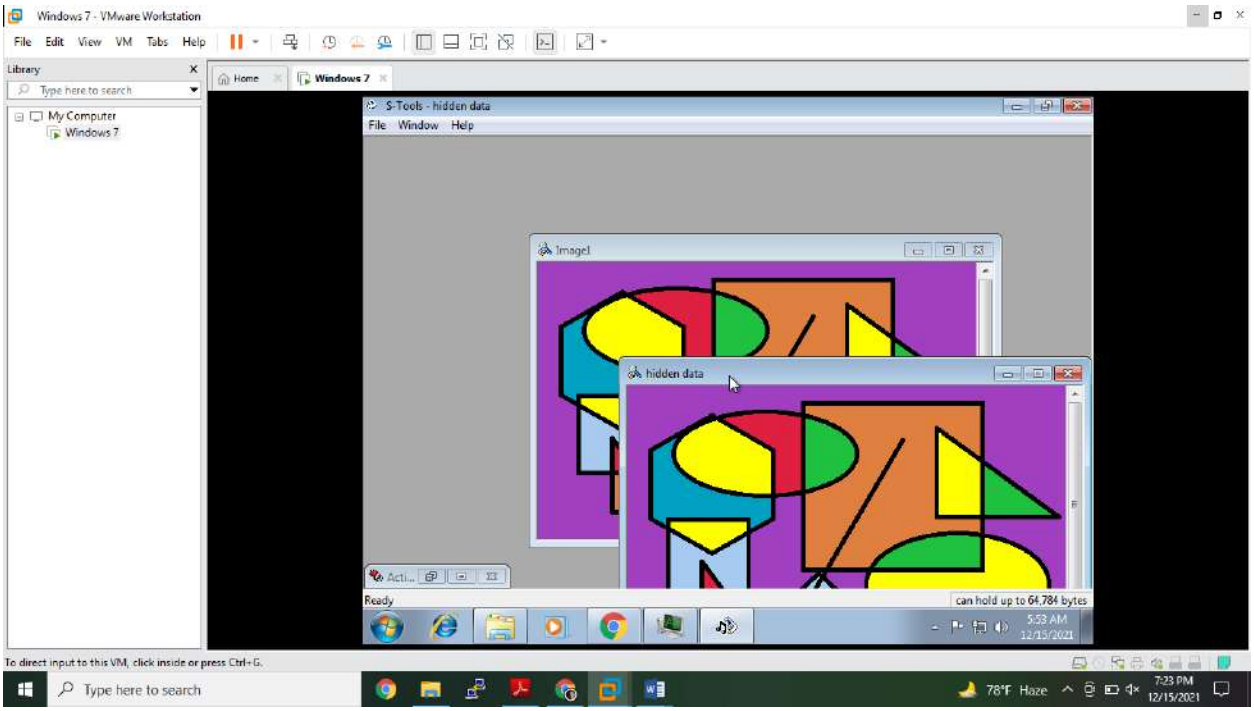


Now enter passphrase, you can type here any type of password.
I have typed here, as Sneha@12345.

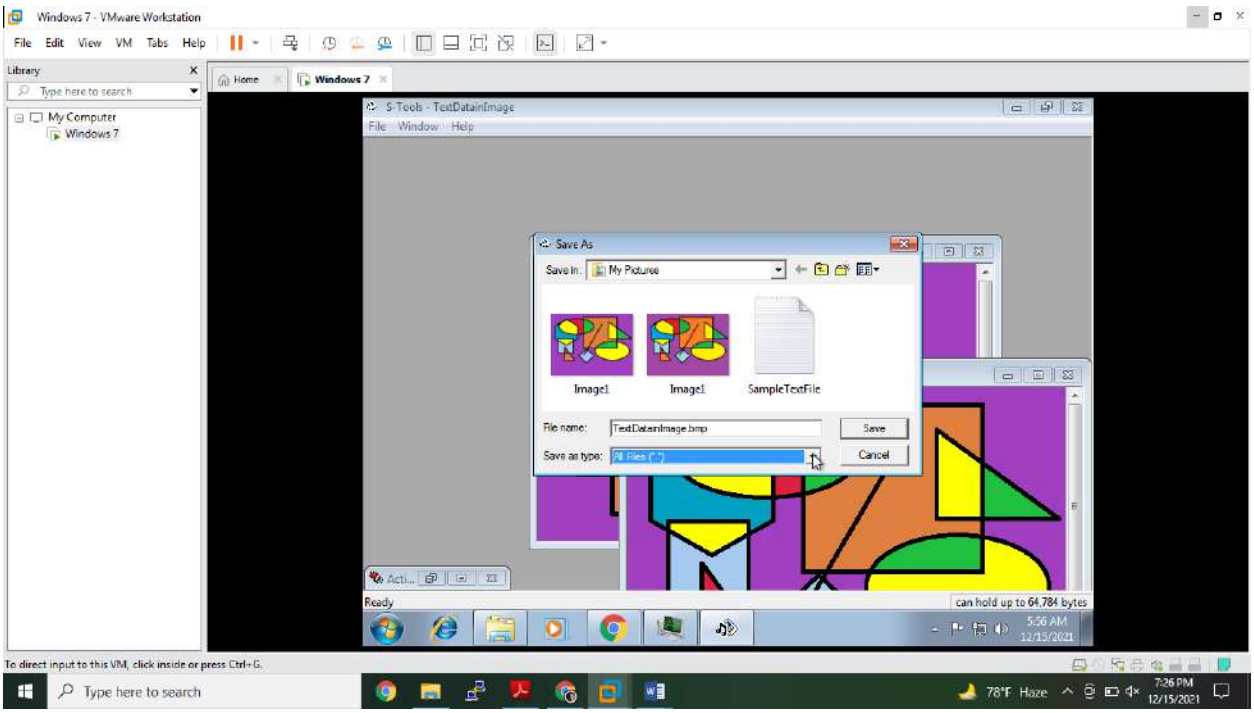




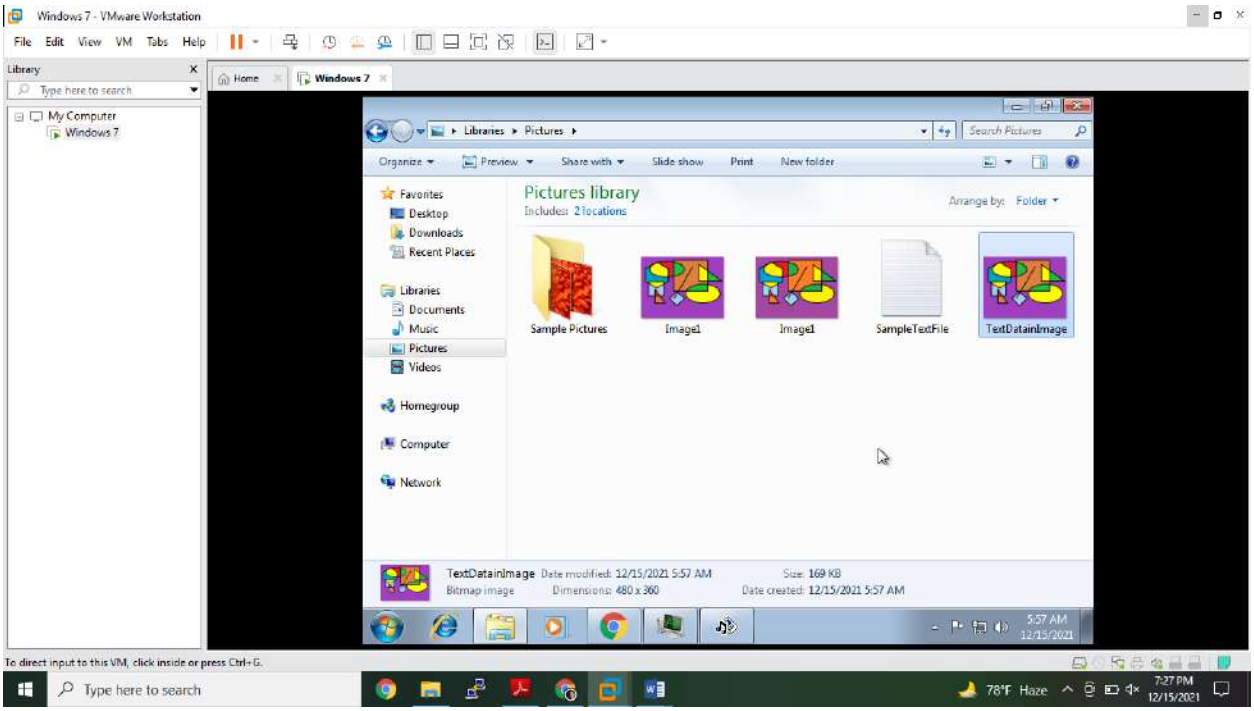
Now here is your hidden data.



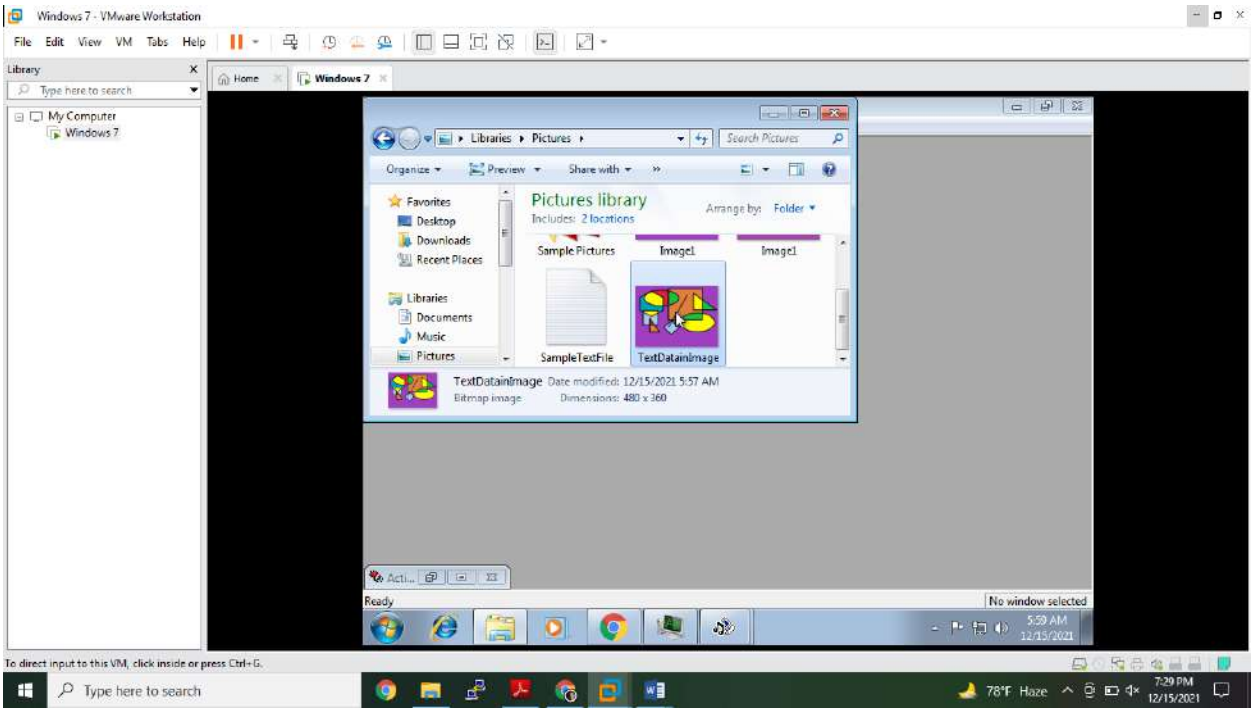
Right click on it, and save it as TextDatainImage.

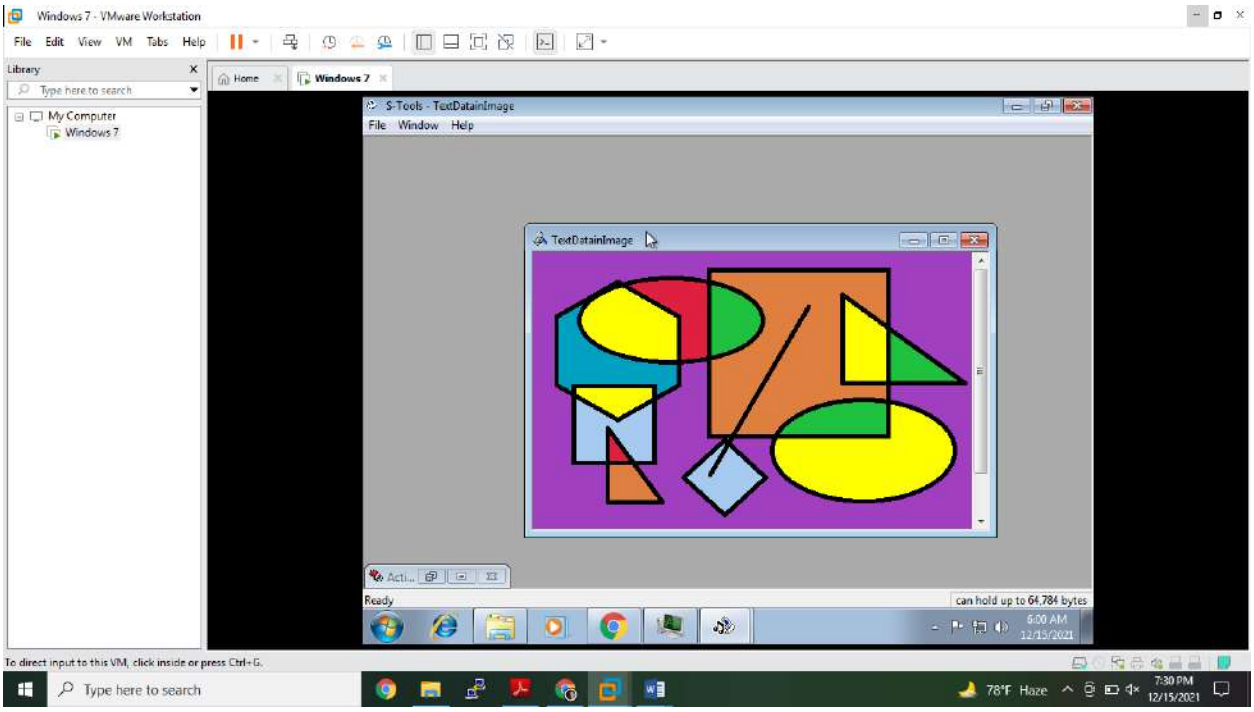


So here is your image file which has hidden text data in it.

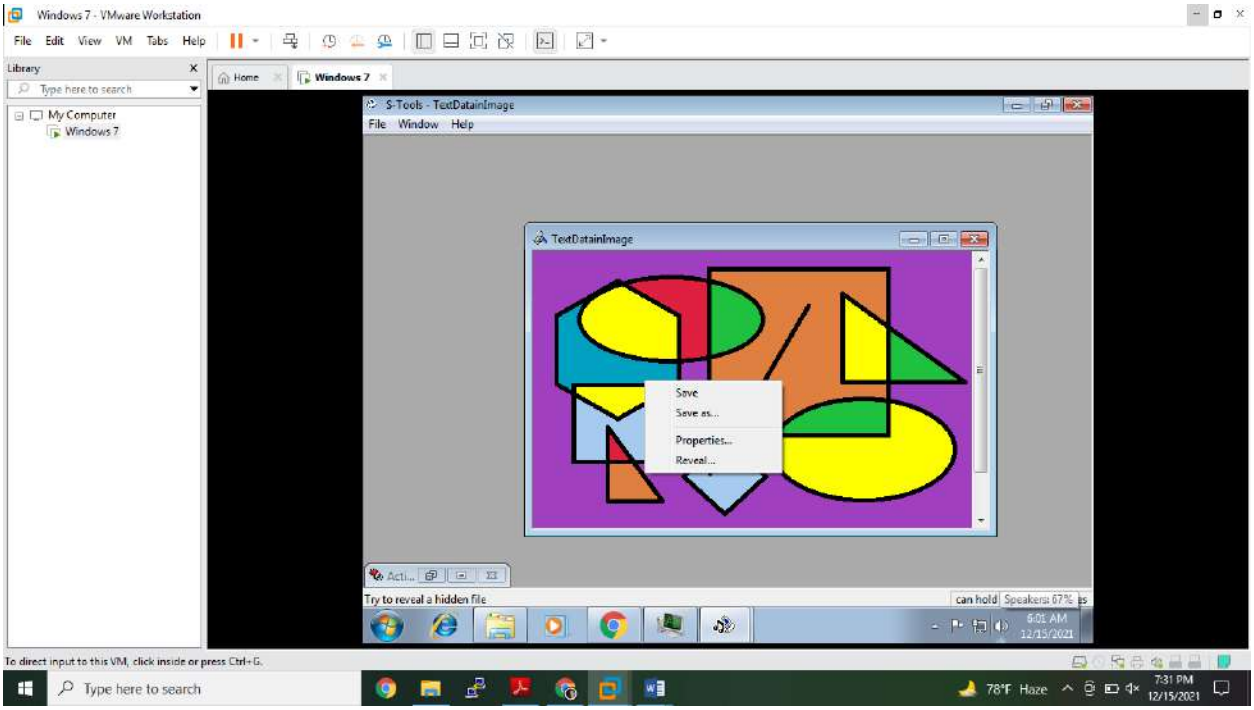


Again open the S – Tool , and drag and drop the Image file which have the text data hidden in it.

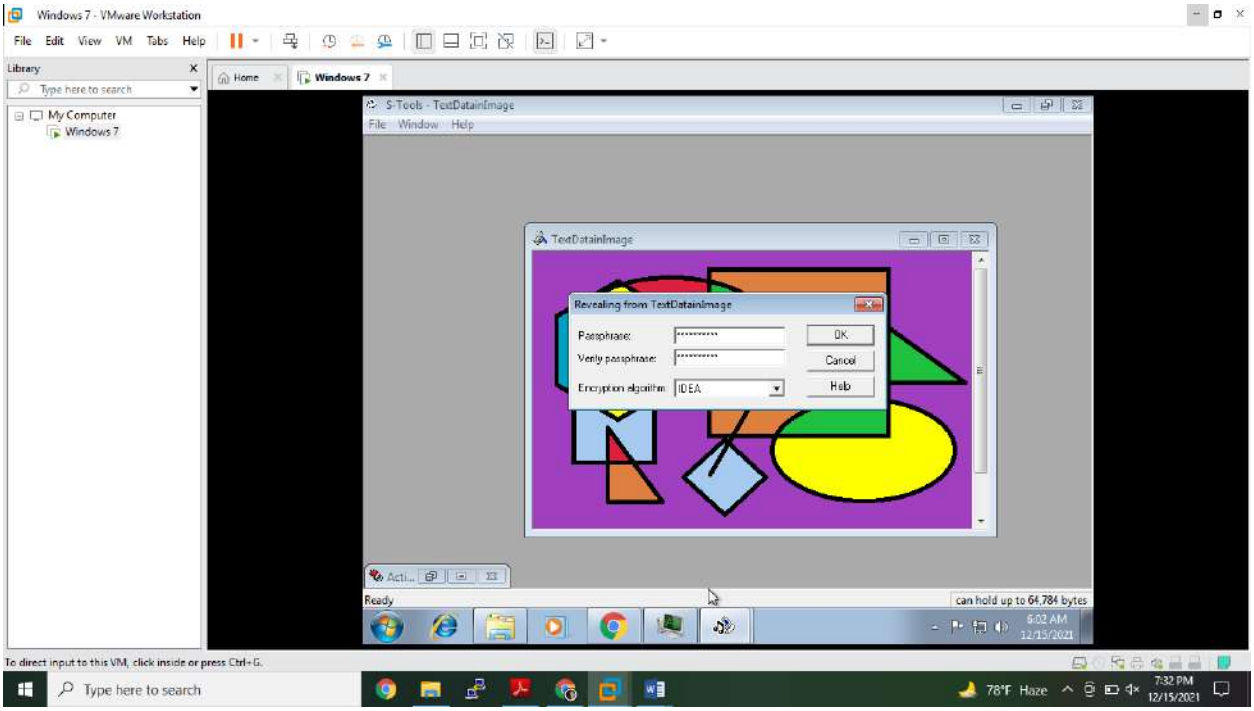


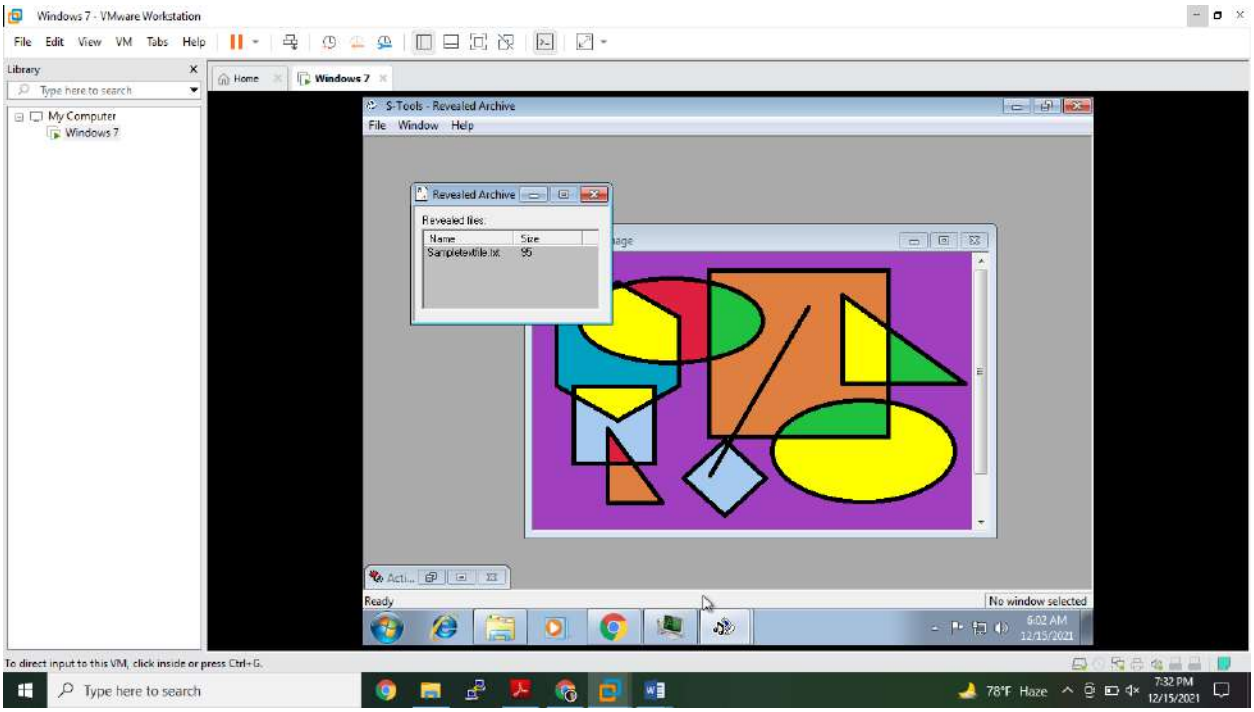


Right click on image and click on Reveal.

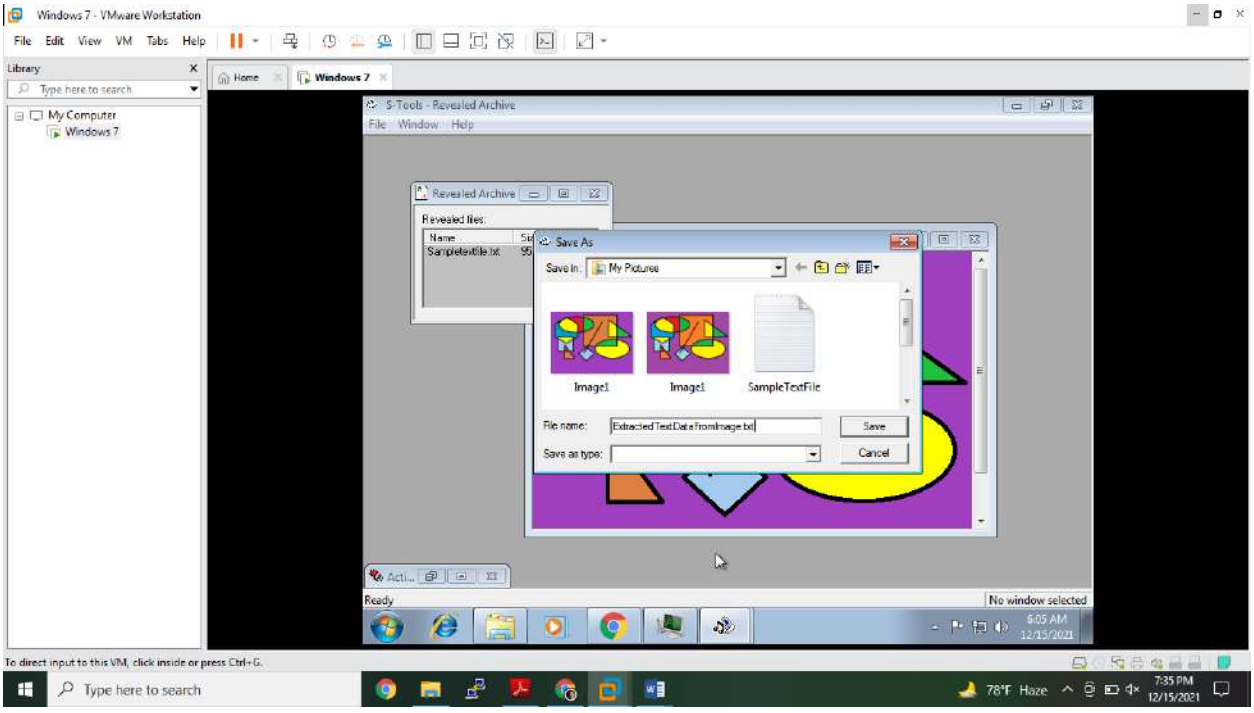


Enter the passphrase. And click on Ok

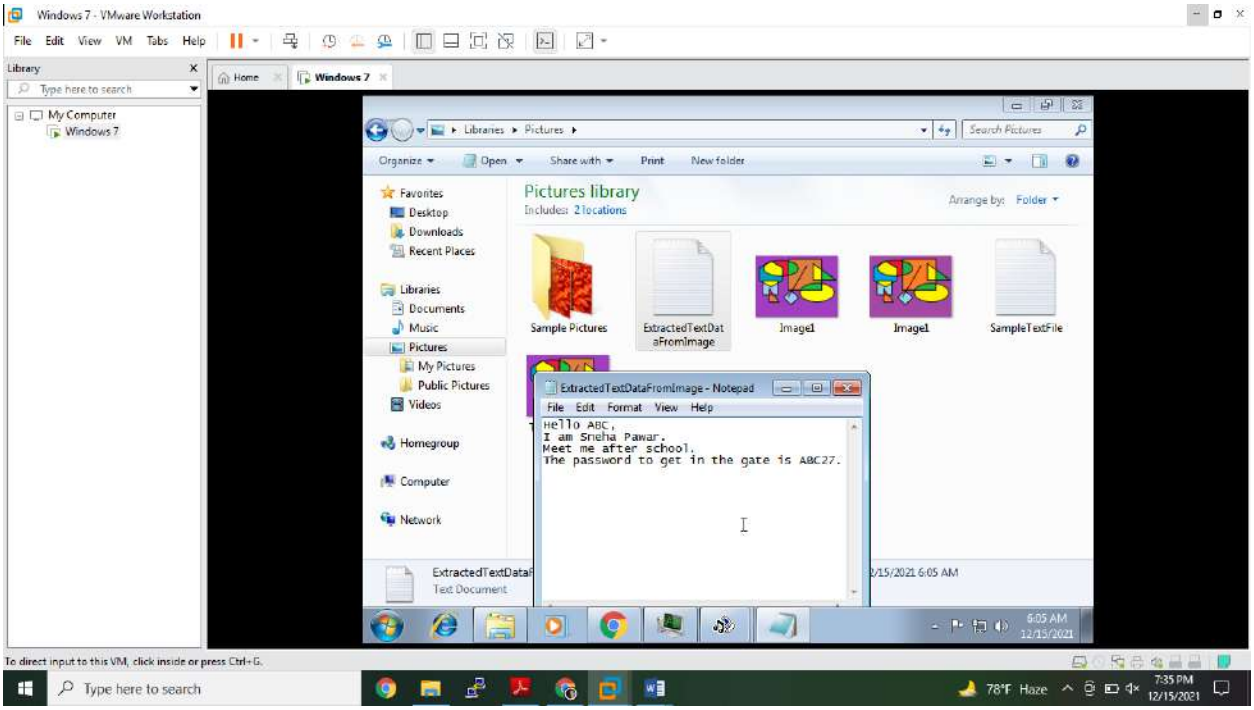




Right click on the Text file and save it as ExtractedTextDataFromImage.



Here is your extracted content from an image.



Practical No. 07

Aim: Using Log and Traffic Capturing and Analysis Tools [Wireshark].

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network.

Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

1. **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
2. **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
3. **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.
4. Packet sniffing can be compared to spelunking – going inside a cave and hiking around. Folks who use Wireshark on a network are kind of like those who use flashlights to see what cool things they can find. After all, when using Wireshark on a network connection (or a flashlight in a cave), you're effectively using a tool to hunt around tunnels and tubes to see what you can see.

   What Is Wireshark Used For?
5. Wireshark has many uses, including troubleshooting networks that have performance issues. Cybersecurity professionals often use Wireshark to trace connections, view the contents of suspect network transactions and identify bursts of network traffic. It's a major part of any IT pro's toolkit – and hopefully, the IT pro has the knowledge to use it.

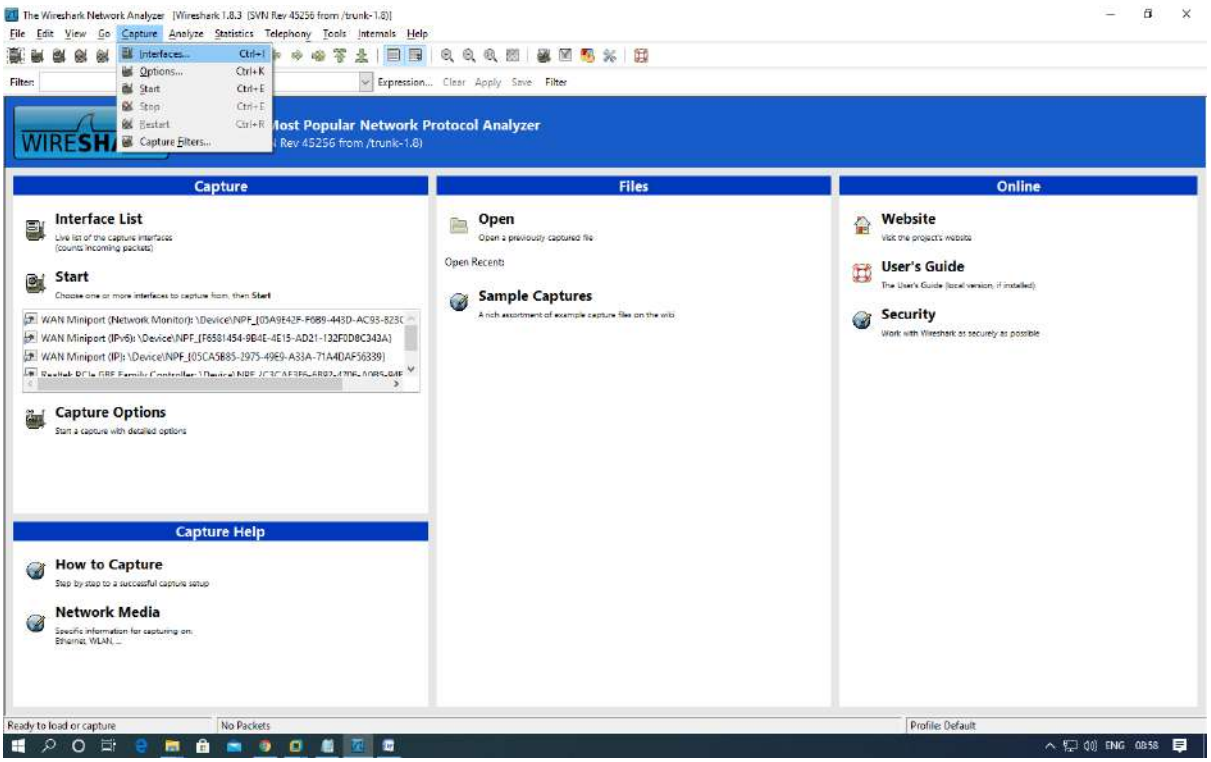
Steps:

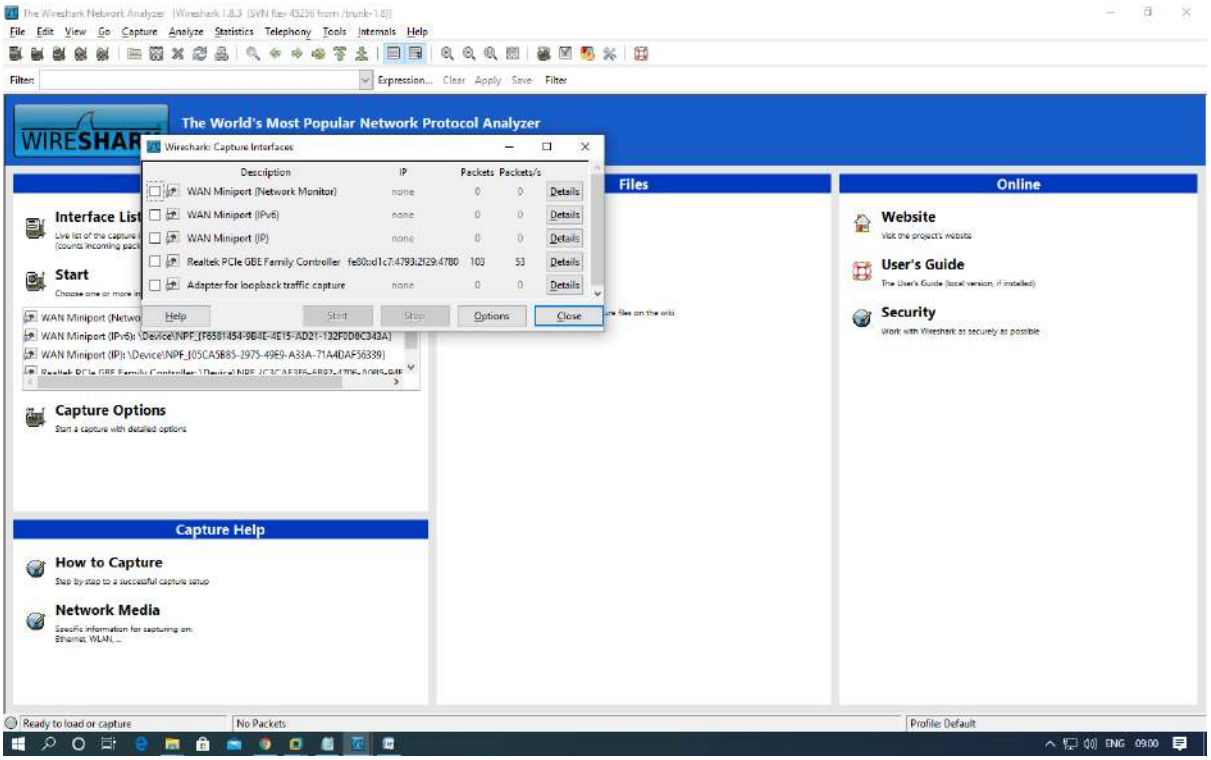
Wireshark

An open source protocol analyzer that can capture traffic in real time for

unsecured sites..

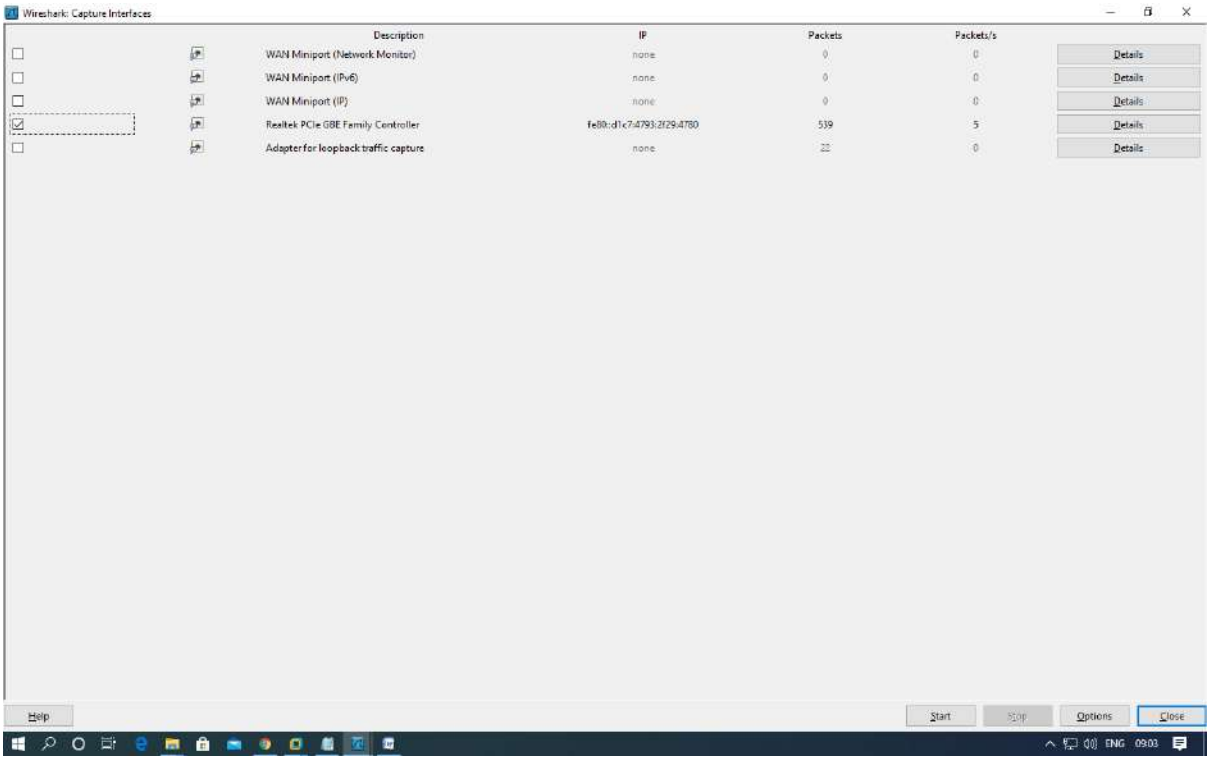
Go to Capture - Interface.



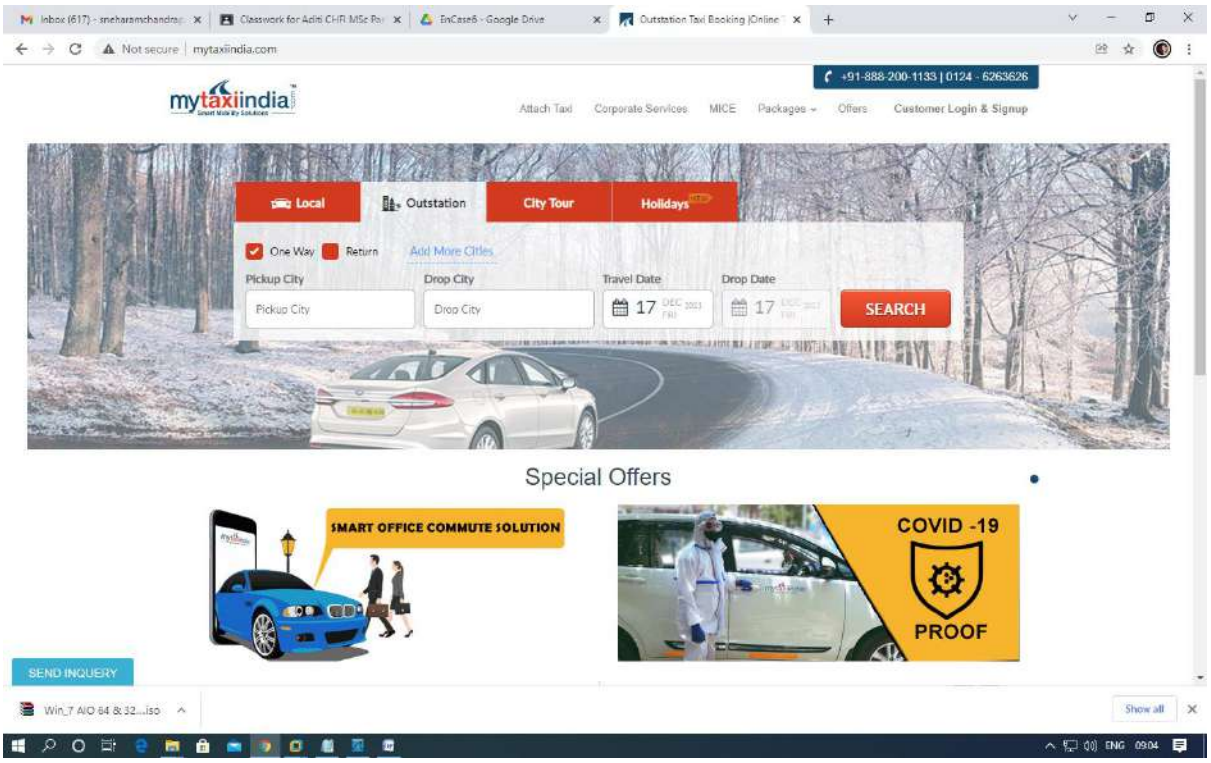


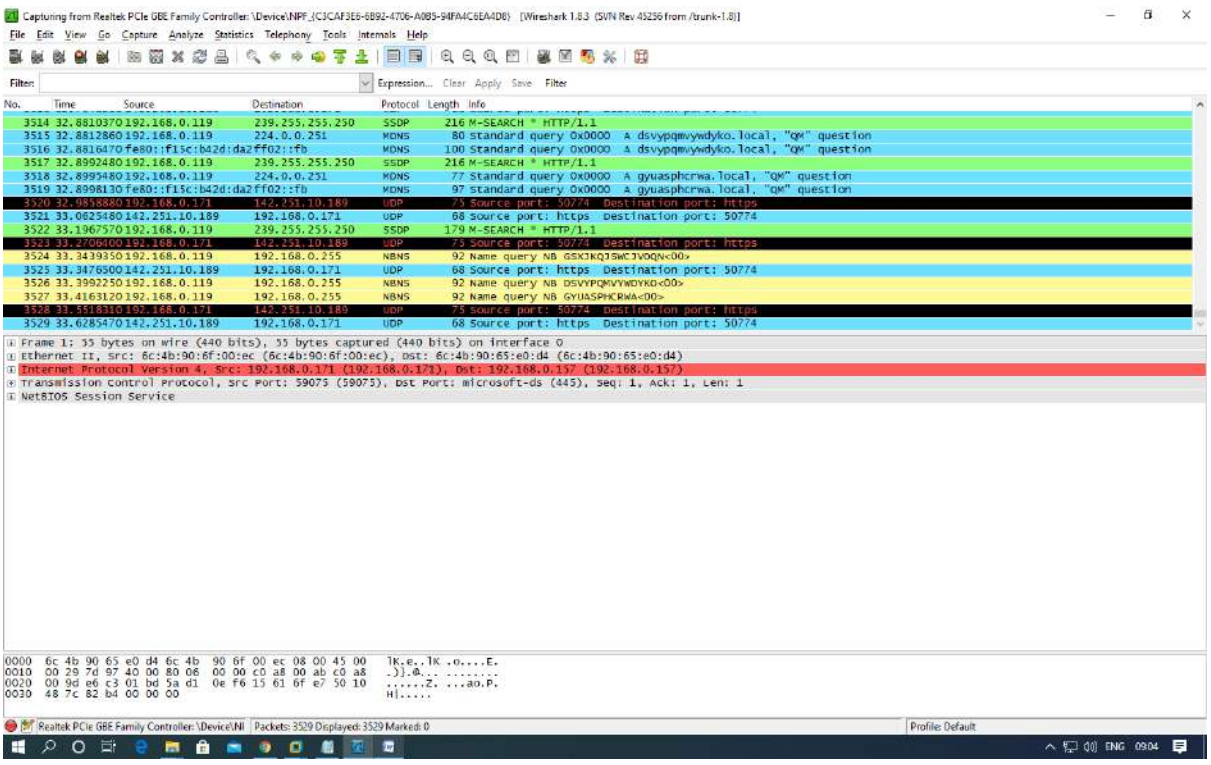
Click on Start

Select the option as shown in image and click on start

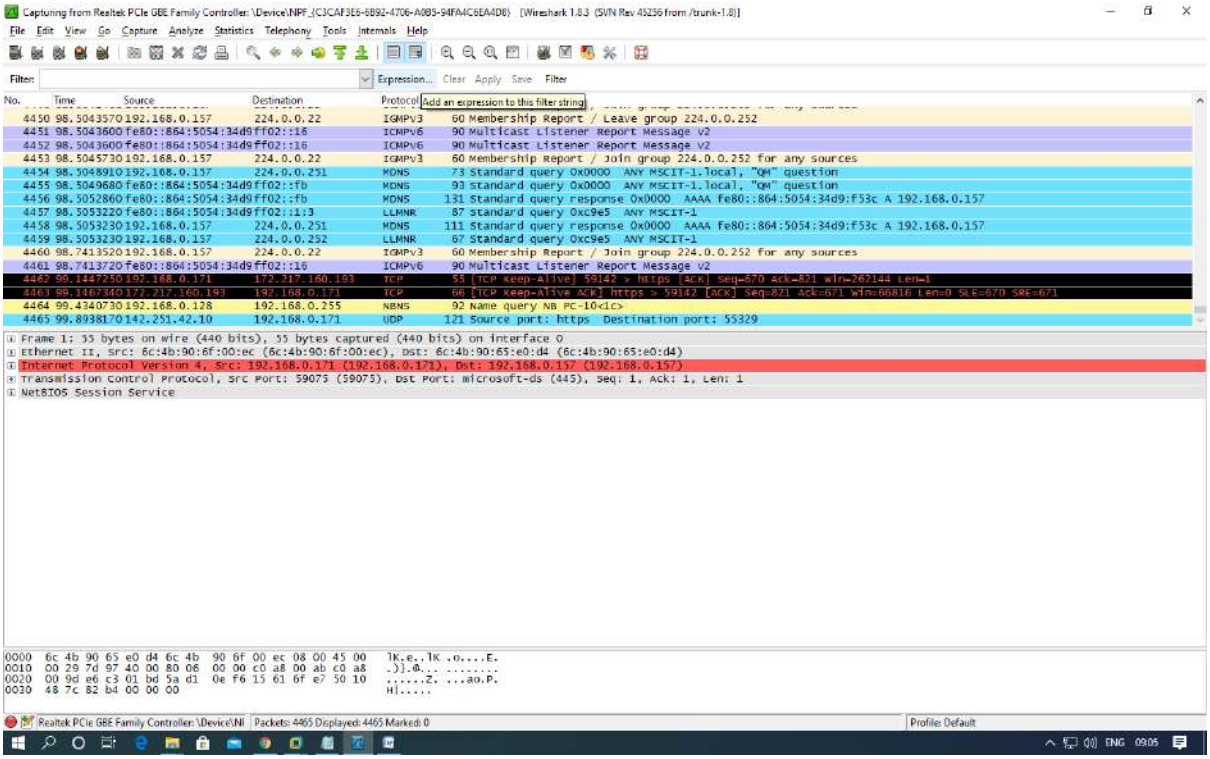


Go to unsecured site mytaxindia or some other and do some post and get operation


Not secure | mytaxiindia.com
mytaxiindia
+91-888-200-1133 | 0124 - 6263626
Attach Taxi
Corporate Services
MICE
Packages
Offers
Customer Login & Signup
Local
Outstation
City Tour
Holidays
One Way
Return
Add More Cities
Pickup City
Drop City
Travel Date
Drop Date
SEARCH
Special Offers
SMART OFFICE COMMUTE SOLUTION
COVID -19
PROOF
SEND INQUERY
Win_7 AIO 64 & 32...iso
Show all
ENG 09:04


Capturing from Realtek PCIe GBE Family Controller: \Device\NPF_{C3CAF3E6-6B92-4706-A0B5-94FA4C6EA4D8} [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save Filter
No. Time Source Destination Protocol Length Info
3514 32.8810370 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
3515 32.8812860 192.168.0.119 224.0.0.251 MDNS 80 Standard query 0x0000 A dsvypqmvywdyko.local, "QM" question
3516 32.8816470 fe80::f15c:b42d:da2 ff02::fb MDNS 100 Standard query 0x0000 A dsvypqmvywdyko.local, "QM" question
3517 32.8992480 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
3518 32.8995480 192.168.0.119 224.0.0.251 MDNS 77 Standard query 0x0000 A gyuasphcrwa.local, "QM" question
3519 32.8998130 fe80::f15c:b42d:da2 ff02::fb MDNS 97 Standard query 0x0000 A gyuasphcrwa.local, "QM" question
3520 32.9858880 192.168.0.171 142.251.10.189 UDP 75 Source port: 50774 Destination port: https
3521 33.0625480 142.251.10.189 192.168.0.171 UDP 68 Source port: https Destination port: 50774
3522 33.1967570 192.168.0.119 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
3523 33.2706400 192.168.0.171 142.251.10.189 UDP 75 Source port: 50774 Destination port: https
3524 33.3439350 192.168.0.119 192.168.0.255 NBNS 92 Name query NB GSXIKQJSWCJVOQN<00>
3525 33.3476500 142.251.10.189 192.168.0.171 UDP 68 Source port: https Destination port: 50774
3526 33.3992250 192.168.0.119 192.168.0.255 NBNS 92 Name query NB DSVYPQMVYWDYKO<00>
3527 33.4163120 192.168.0.119 192.168.0.255 NBNS 92 Name query NB GYUASPHCRWA<00>
3528 33.5518310 192.168.0.171 142.251.10.189 UDP 75 Source port: 50774 Destination port: https
3529 33.6285470 142.251.10.189 192.168.0.171 UDP 68 Source port: https Destination port: 50774
Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
Ethernet II, Src: 6c:4b:90:6f:00:ec (6c:4b:90:6f:00:ec), Dst: 6c:4b:90:65:e0:d4 (6c:4b:90:65:e0:d4)
Internet Protocol Version 4, Src: 192.168.0.171 (192.168.0.171), Dst: 192.168.0.157 (192.168.0.157)
Transmission Control Protocol, Src Port: 59075 (59075), Dst Port: microsoft-ds (445), Seq: 1, Ack: 1, Len: 1
NetBIOS Session Service
0000 6c 4b 90 65 e0 d4 6c 4b 90 6f 00 ec 08 00 45 00 lK.e..lK .o....E.
0010 00 29 7d 97 40 00 80 06 00 00 c0 a8 00 ab c0 a8 .)}.@... ....
0020 00 9d e6 c3 01 bd 5a d1 0e f6 15 61 6f e7 50 10 ......Z. ...ao.P.
0030 48 7c 82 b4 00 00 00 H|.....
Realtek PCIe GBE Family Controller: \Device\NI
Packets: 3529 Displayed: 3529 Marked: 0
Profile: Default
ENG 09:04

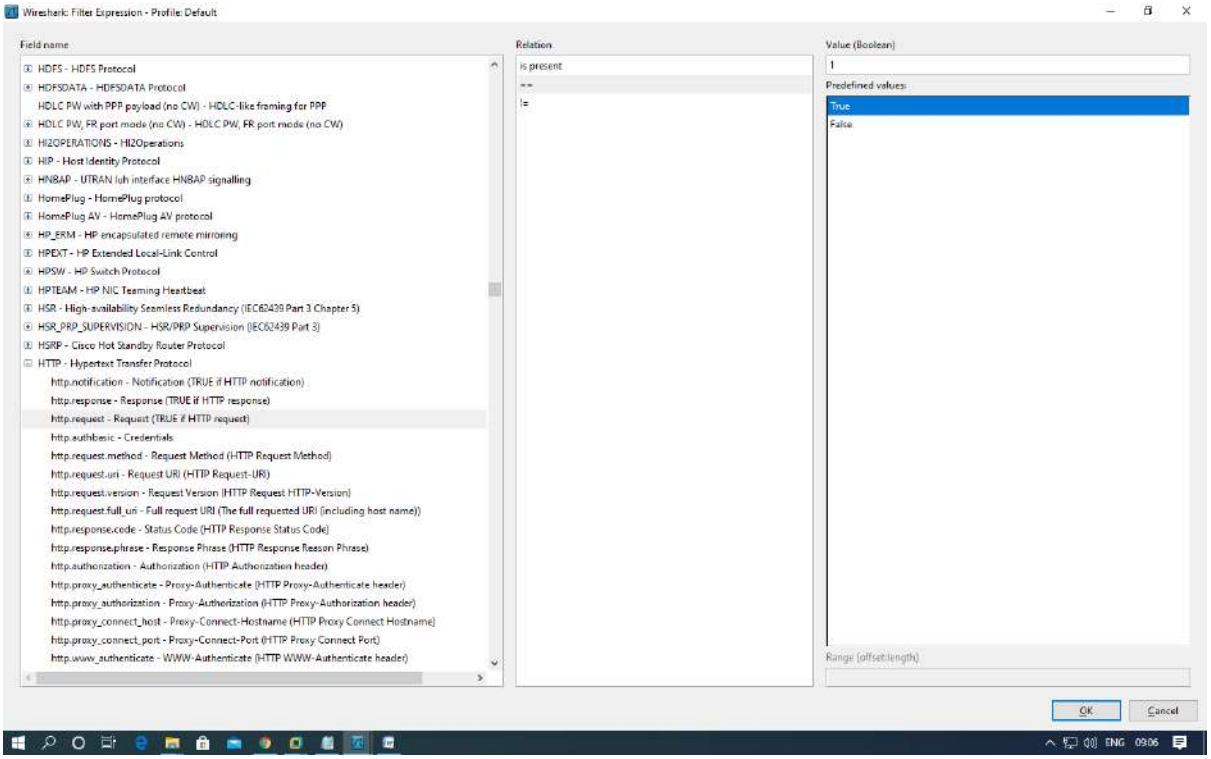
Click on Expression



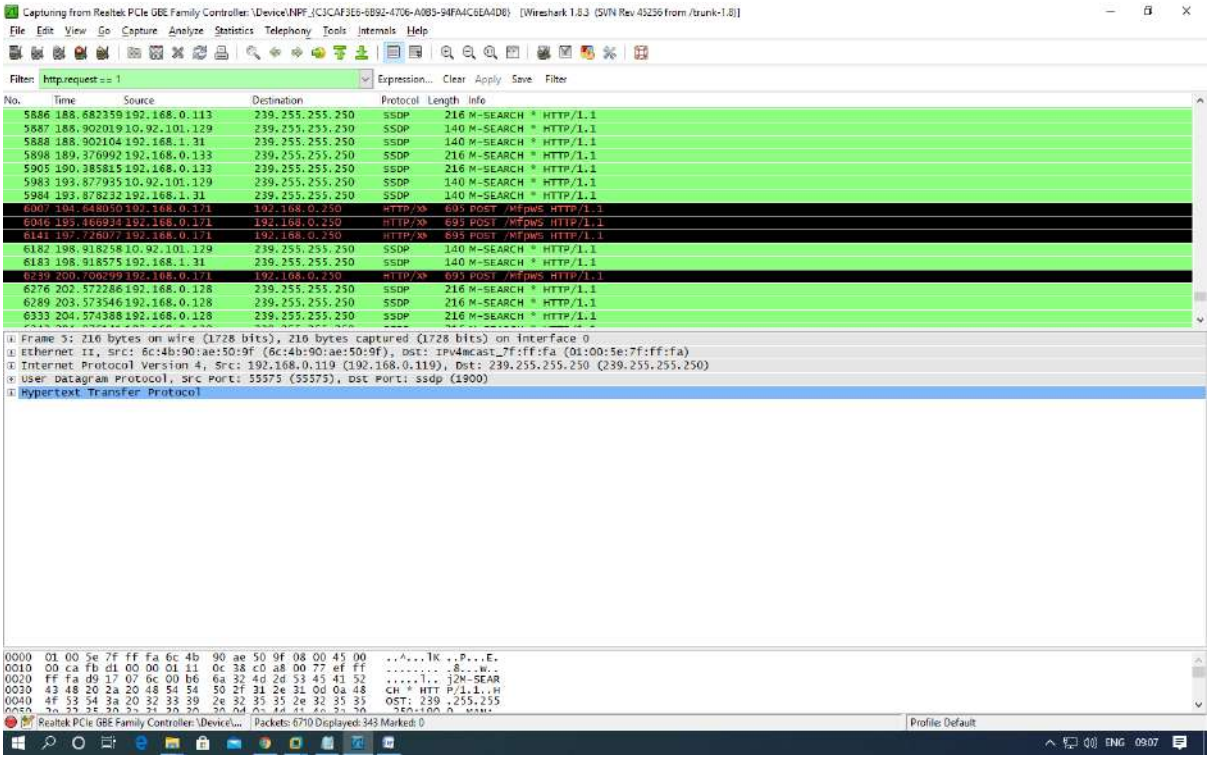
Filter Expressions Can Be Added By Clicking The Expression Button Present On The Right Side

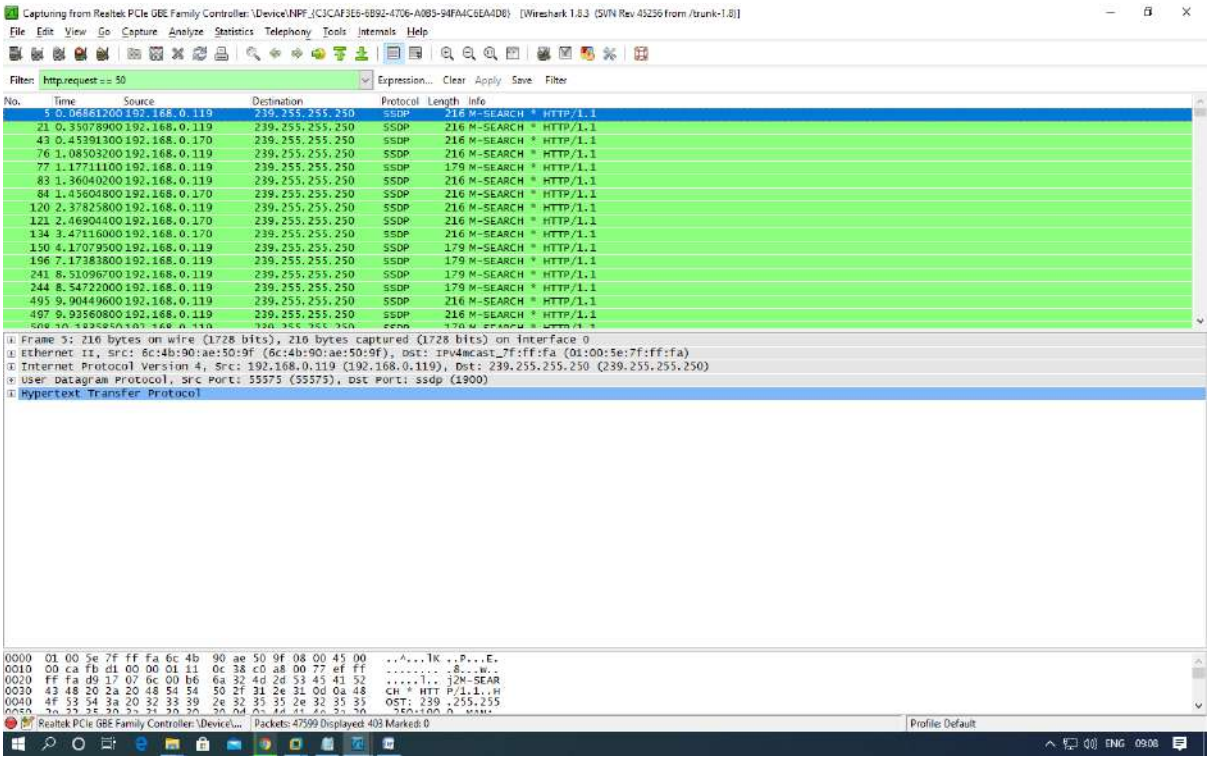
Of The Filter Bar. The Relations And The Entities Can Be Added With The Help Of The

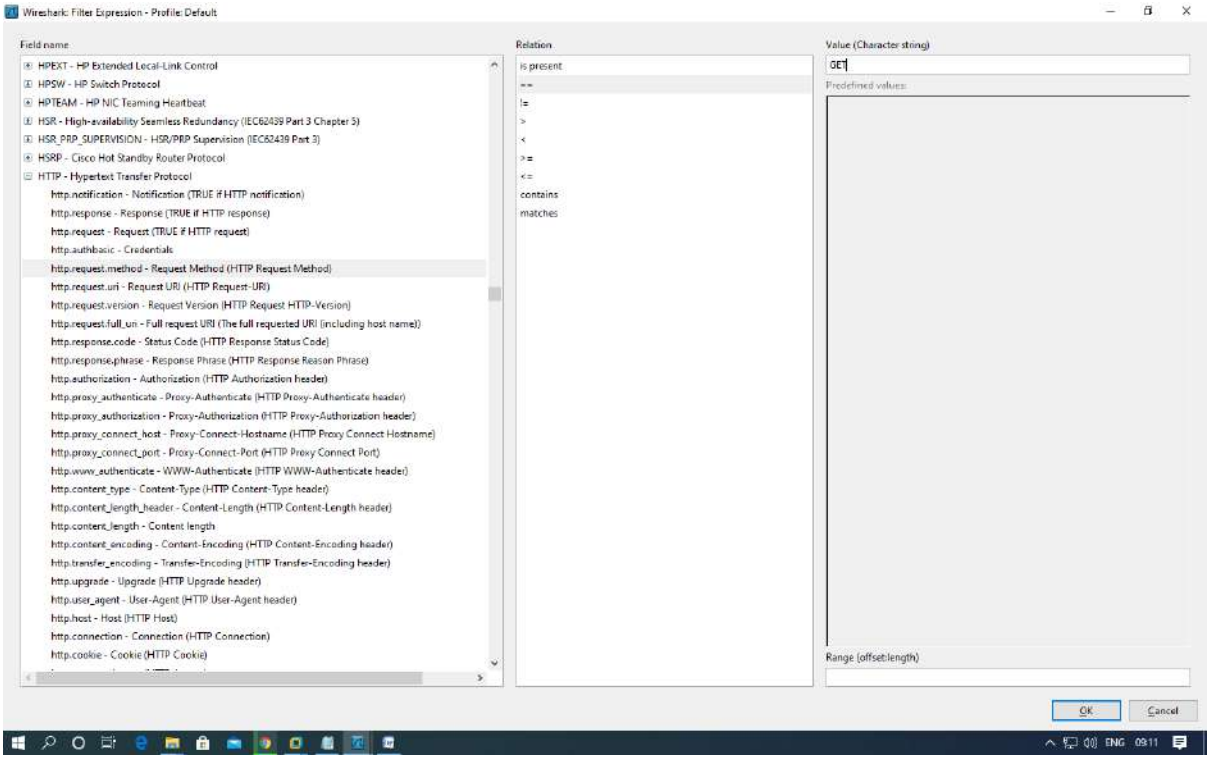
Resulting Dialog

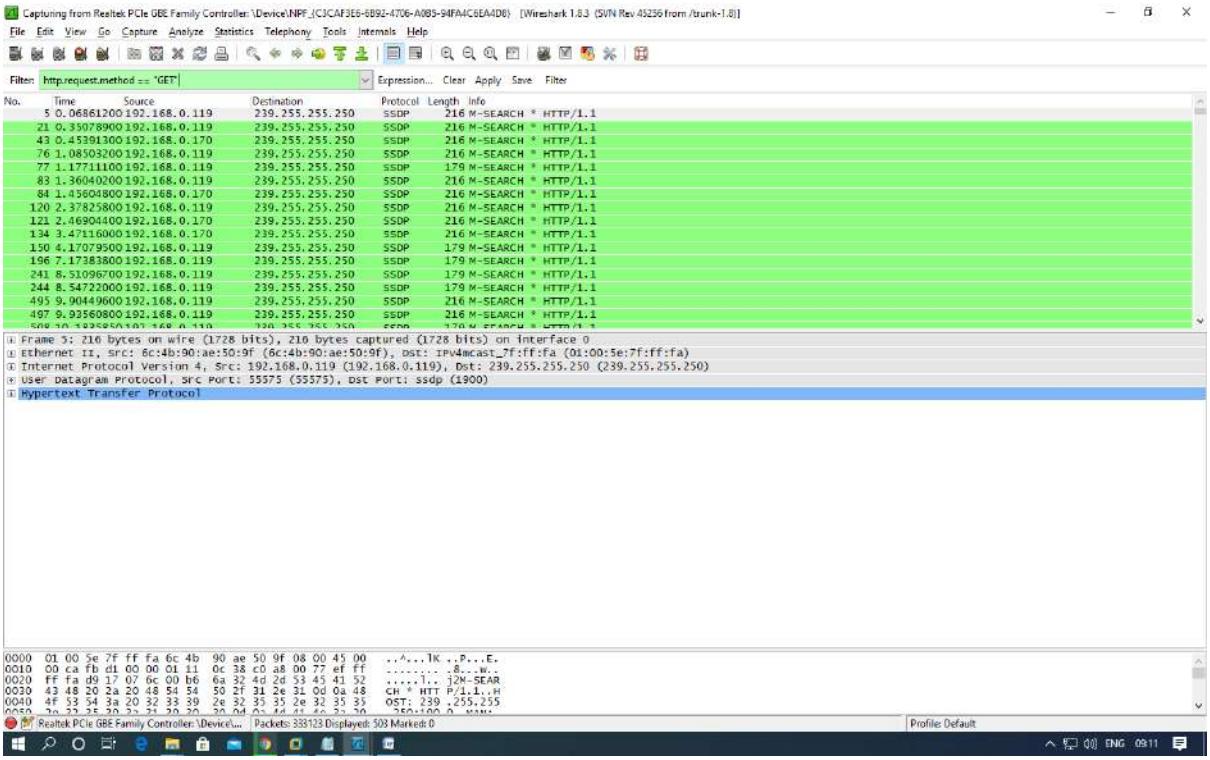


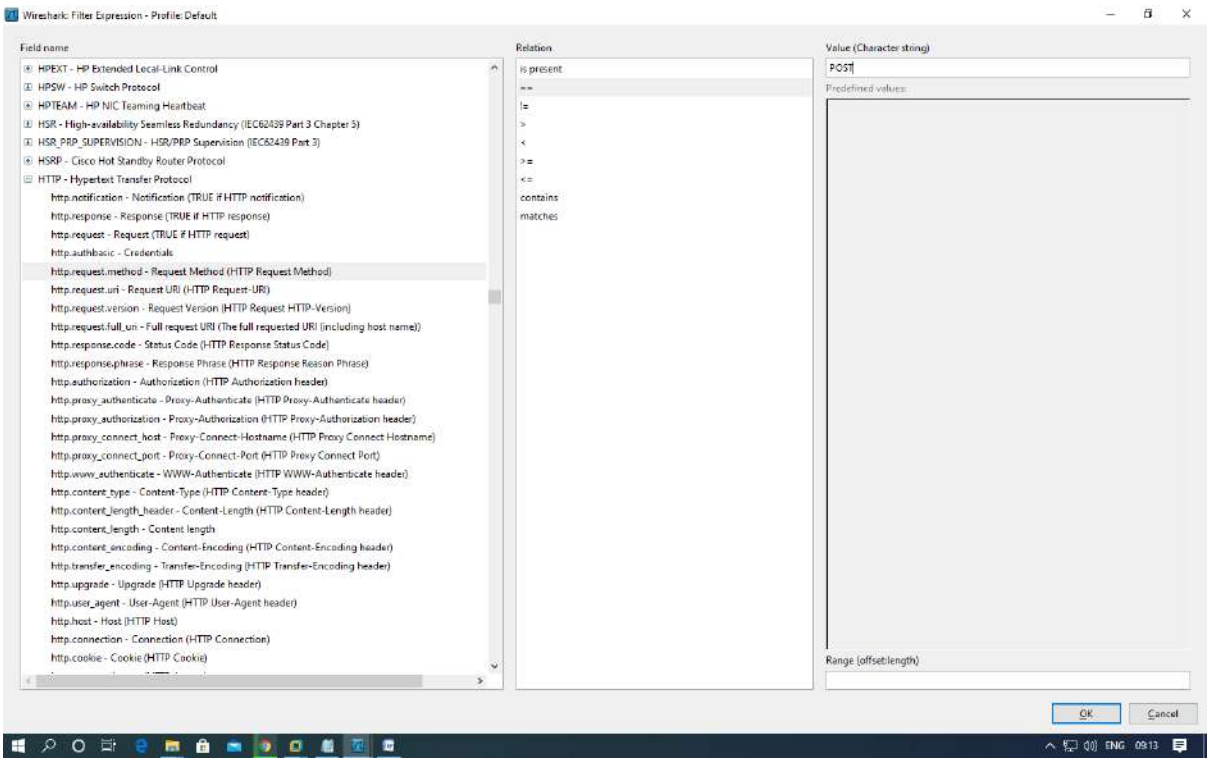
Click on Apply

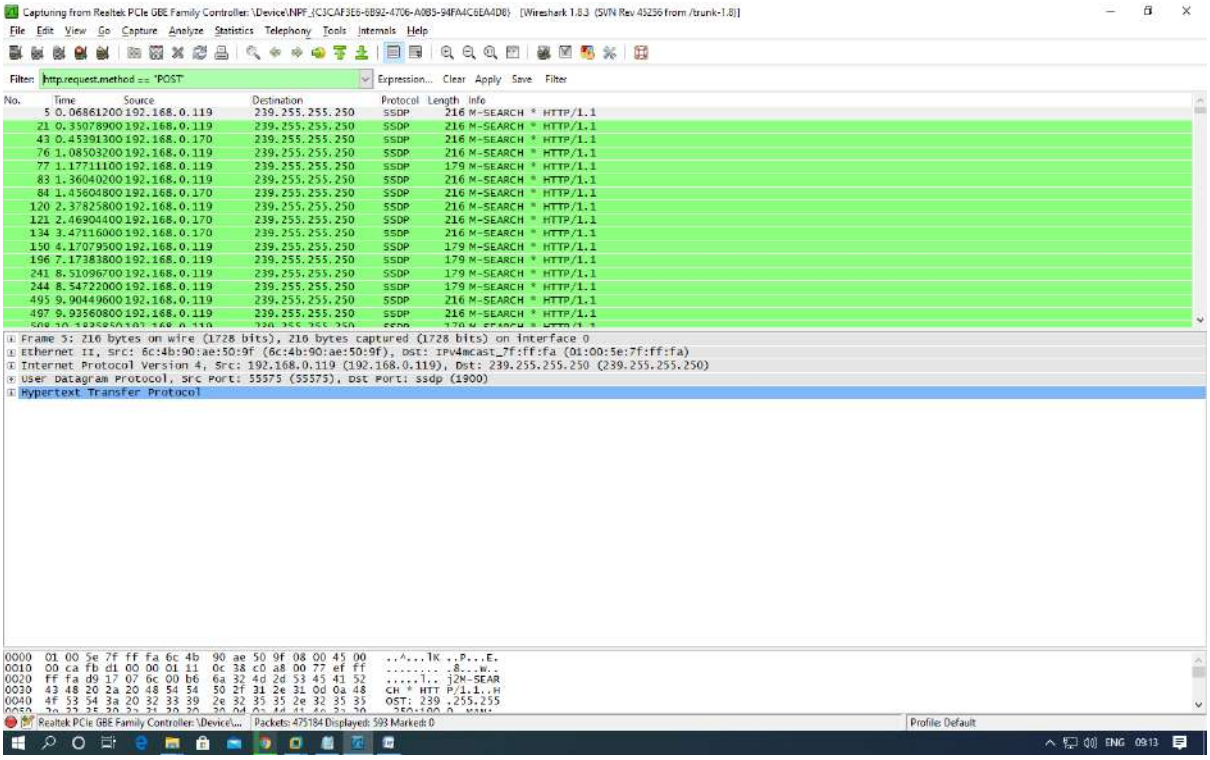


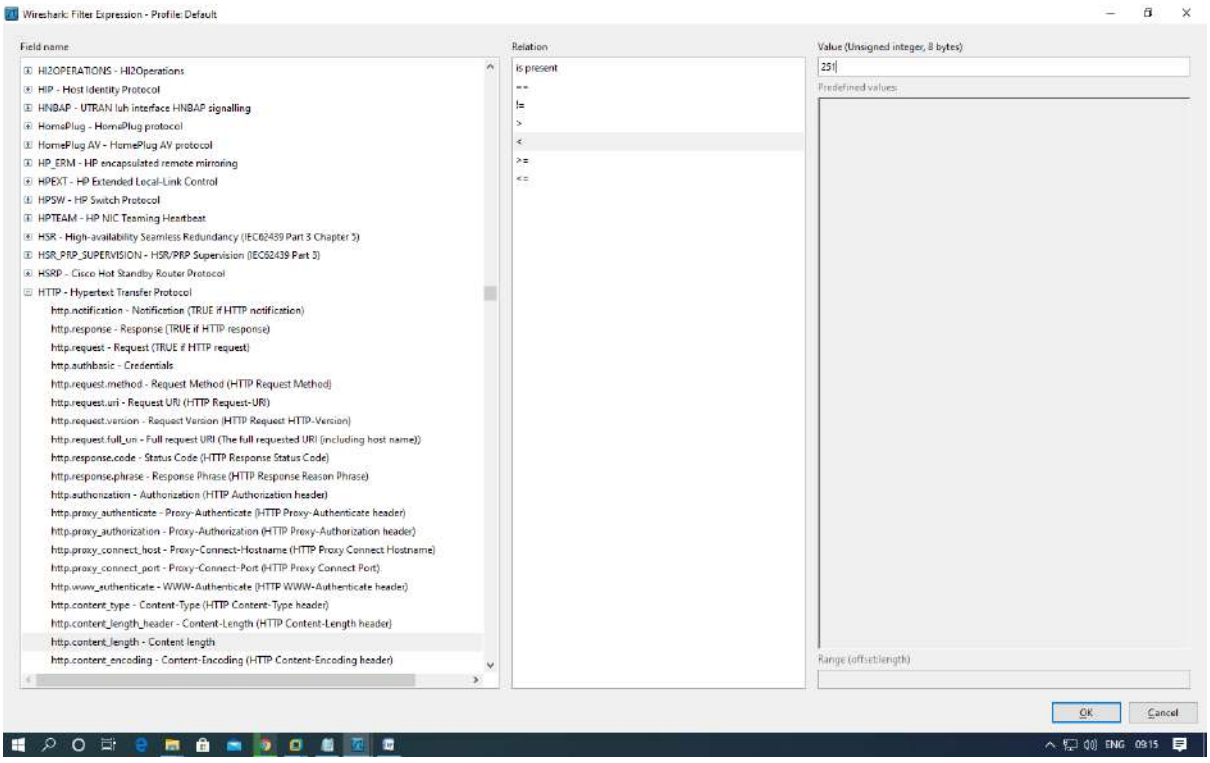

Capturing from Realtek PCIe GBE Family Controller: \Device\NPF_{C3CAF3E6-6B92-4706-A0B5-94FA4C6EA4D6} [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http.request == 50
Expression... Clear Apply Save Filter
No. Time Source Destination Protocol Length Info
5 0.06861200 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
21 0.35078900 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
43 0.45391300 192.168.0.170 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
76 1.08503200 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
77 1.17711100 192.168.0.119 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
83 1.36040200 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
84 1.45604800 192.168.0.170 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
120 2.37825800 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
121 2.46904400 192.168.0.170 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
134 3.47116000 192.168.0.170 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
150 4.17079500 192.168.0.119 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
196 7.17383800 192.168.0.119 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
241 8.51096700 192.168.0.119 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
244 8.54722000 192.168.0.119 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
495 9.90449600 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
497 9.93560800 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
Frame 5: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
Ethernet II, Src: 6c:4b:90:ae:50:9f (6c:4b:90:ae:50:9f), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.0.119 (192.168.0.119), Dst: 239.255.255.250 (239.255.255.250)
User Datagram Protocol, Src Port: 55575 (55575), Dst Port: ssdp (1900)
Hypertext Transfer Protocol
0000 01 00 5e 7f ff fa 6c 4b 90 ae 50 9f 08 00 45 00 ..^...lK ..P...E.
0010 00 ca fb d1 00 00 01 11 0c 38 c0 a8 00 77 ef ff .... .8...w..
0020 ff fa d9 17 07 6c 00 b6 6a 32 4d 2d 53 45 41 52 .....l.. j2M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1..H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239 .255.255
Realtek PCIe GBE Family Controller: \Device\... Packets: 47599 Displayed: 403 Marked: 0
Profile: Default
ENG 09:08

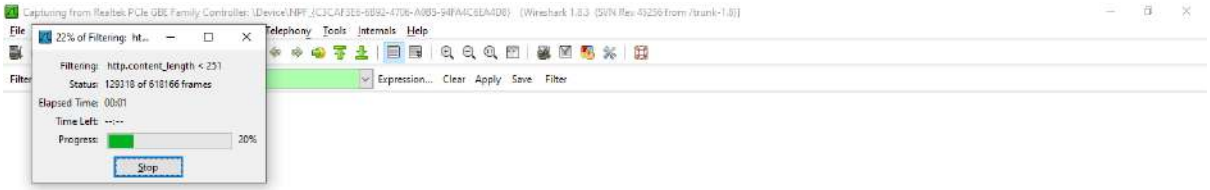

Wireshark: Filter Expression - Profile: Default
Field name
Relation
Value (Character string)
GET
Predefined values:
Range (offset:length)
OK
Cancel
HPEXT - HP Extended Local-Link Control
HPSW - HP Switch Protocol
HPTEAM - HP NIC Teaming Heartbeat
HSR - High-availability Seamless Redundancy (IEC62439 Part 3 Chapter 5)
HSR_PRP_SUPERVISION - HSR/PRP Supervision (IEC62439 Part 3)
HSRP - Cisco Hot Standby Router Protocol
HTTP - Hypertext Transfer Protocol
http.notification - Notification (TRUE if HTTP notification)
http.response - Response (TRUE if HTTP response)
http.request - Request (TRUE if HTTP request)
http.authbasic - Credentials
http.request.method - Request Method (HTTP Request Method)
http.request.uri - Request URI (HTTP Request-URI)
http.request.version - Request Version (HTTP Request HTTP-Version)
http.request.full_uri - Full request URI (The full requested URI (including host name))
http.response.code - Status Code (HTTP Response Status Code)
http.response.phrase - Response Phrase (HTTP Response Reason Phrase)
http.authorization - Authorization (HTTP Authorization header)
http.proxy_authenticate - Proxy-Authenticate (HTTP Proxy-Authenticate header)
http.proxy_authorization - Proxy-Authorization (HTTP Proxy-Authorization header)
http.proxy_connect_host - Proxy-Connect-Hostname (HTTP Proxy Connect Hostname)
http.proxy_connect_port - Proxy-Connect-Port (HTTP Proxy Connect Port)
http.www_authenticate - WWW-Authenticate (HTTP WWW-Authenticate header)
http.content_type - Content-Type (HTTP Content-Type header)
http.content_length_header - Content-Length (HTTP Content-Length header)
http.content_length - Content length
http.content_encoding - Content-Encoding (HTTP Content-Encoding header)
http.transfer_encoding - Transfer-Encoding (HTTP Transfer-Encoding header)
http.upgrade - Upgrade (HTTP Upgrade header)
http.user_agent - User-Agent (HTTP User-Agent header)
http.host - Host (HTTP Host)
http.connection - Connection (HTTP Connection)
http.cookie - Cookie (HTTP Cookie)
is present
==
!=
>
<
>=
<=
contains
matches
ENG 09:11

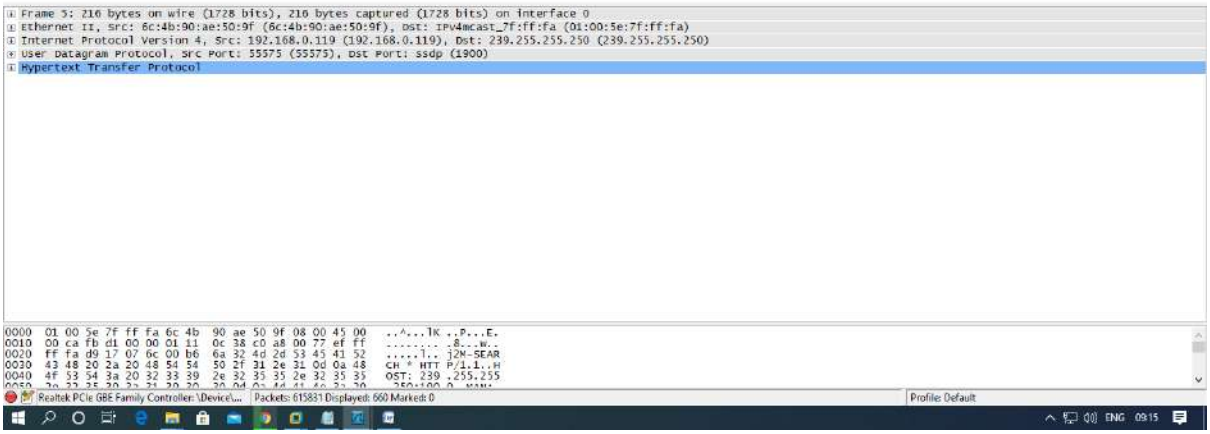

Capturing from Realtek PCIe GBE Family Controller: \Device\NPF_{C3CAF3E6-6B92-4706-A0B5-94FA4C6EA4D6} [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http.request.method == "GET"
Expression... Clear Apply Save Filter
No. Time Source Destination Protocol Length Info
5 0.06861200 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
21 0.35078900 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
43 0.45391300 192.168.0.170 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
76 1.08503200 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
77 1.17711100 192.168.0.119 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
83 1.36040200 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
84 1.45604800 192.168.0.170 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
120 2.37825800 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
121 2.46904400 192.168.0.170 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
134 3.47116000 192.168.0.170 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
150 4.17079500 192.168.0.119 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
196 7.17383800 192.168.0.119 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
241 8.51096700 192.168.0.119 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
244 8.54722000 192.168.0.119 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
495 9.90449600 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
497 9.93560800 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
Frame 5: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
Ethernet II, Src: 6c:4b:90:ae:50:9f (6c:4b:90:ae:50:9f), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.0.119 (192.168.0.119), Dst: 239.255.255.250 (239.255.255.250)
User Datagram Protocol, Src Port: 55575 (55575), Dst Port: ssdp (1900)
Hypertext Transfer Protocol
0000 01 00 5e 7f ff fa 6c 4b 90 ae 50 9f 08 00 45 00
0010 00 ca fb d1 00 00 01 11 0c 38 c0 a8 00 77 ef ff
0020 ff fa d9 17 07 6c 00 b6 6a 32 4d 2d 53 45 41 52
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35
Realtek PCIe GBE Family Controller: \Device\...
Packets: 333123 Displayed: 503 Marked: 0
Profile: Default


Wireshark: Filter Expression - Profile: Default
Field name
Relation
Value (Character string)
HPEXT - HP Extended Local-Link Control
HPSW - HP Switch Protocol
HPTEAM - HP NIC Teaming Heartbeat
HSR - High-availability Seamless Redundancy (IEC62439 Part 3 Chapter 5)
HSR_PRP_SUPERVISION - HSR/PRP Supervision (IEC62439 Part 3)
HSRP - Cisco Hot Standby Router Protocol
HTTP - Hypertext Transfer Protocol
http.notification - Notification (TRUE if HTTP notification)
http.response - Response (TRUE if HTTP response)
http.request - Request (TRUE if HTTP request)
http.authbasic - Credentials
http.request.method - Request Method (HTTP Request Method)
http.request.uri - Request URI (HTTP Request-URI)
http.request.version - Request Version (HTTP Request HTTP-Version)
http.request.full_uri - Full request URI (The full requested URI (including host name))
http.response.code - Status Code (HTTP Response Status Code)
http.response.phrase - Response Phrase (HTTP Response Reason Phrase)
http.authorization - Authorization (HTTP Authorization header)
http.proxy_authenticate - Proxy-Authenticate (HTTP Proxy-Authenticate header)
http.proxy_authorization - Proxy-Authorization (HTTP Proxy-Authorization header)
http.proxy_connect_host - Proxy-Connect-Hostname (HTTP Proxy Connect Hostname)
http.proxy_connect_port - Proxy-Connect-Port (HTTP Proxy Connect Port)
http.www_authenticate - WWW-Authenticate (HTTP WWW-Authenticate header)
http.content_type - Content-Type (HTTP Content-Type header)
http.content_length_header - Content-Length (HTTP Content-Length header)
http.content_length - Content length
http.content_encoding - Content-Encoding (HTTP Content-Encoding header)
http.transfer_encoding - Transfer-Encoding (HTTP Transfer-Encoding header)
http.upgrade - Upgrade (HTTP Upgrade header)
http.user_agent - User-Agent (HTTP User-Agent header)
http.host - Host (HTTP Host)
http.connection - Connection (HTTP Connection)
http.cookie - Cookie (HTTP Cookie)
is present
==
!=
>
<
>=
<=
contains
matches
POST
Predefined values:
Range (offset:length)
OK
Cancel

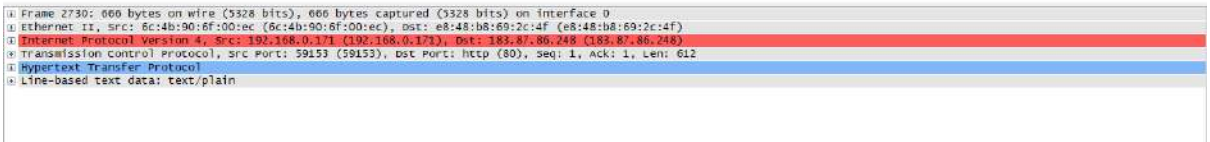

Capturing from Realtek PCIe GBE Family Controller: \Device\NPF_{C3CAF3E6-6B92-4706-A0B5-94FA4C6EA4D0} [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http.request.method == "POST"
Expression... Clear Apply Save Filter
No. Time Source Destination Protocol Length Info
5 0.06861200 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
21 0.35078900 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
43 0.45391300 192.168.0.170 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
76 1.08503200 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
77 1.17711100 192.168.0.119 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
83 1.36040200 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
84 1.45604800 192.168.0.170 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
120 2.37825800 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
121 2.46904400 192.168.0.170 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
134 3.47116000 192.168.0.170 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
150 4.17079500 192.168.0.119 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
196 7.17383800 192.168.0.119 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
241 8.51096700 192.168.0.119 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
244 8.54722000 192.168.0.119 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
495 9.90449600 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
497 9.93560800 192.168.0.119 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
Frame 5: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
Ethernet II, Src: 6c:4b:90:ae:50:9f (6c:4b:90:ae:50:9f), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.0.119 (192.168.0.119), Dst: 239.255.255.250 (239.255.255.250)
User Datagram Protocol, Src Port: 55575 (55575), Dst Port: ssdp (1900)
Hypertext Transfer Protocol
0000 01 00 5e 7f ff fa 6c 4b 90 ae 50 9f 08 00 45 00 ..^...lK ..P...E.
0010 00 ca fb d1 00 00 01 11 0c 38 c0 a8 00 77 ef ff .... .8...w..
0020 ff fa d9 17 07 6c 00 b6 6a 32 4d 2d 53 45 41 52 .....l.. j2M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1..H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239 .255.255
Realtek PCIe GBE Family Controller: \Device\... Packets: 475184 Displayed: 593 Marked: 0
Profile: Default
ENG 09:13

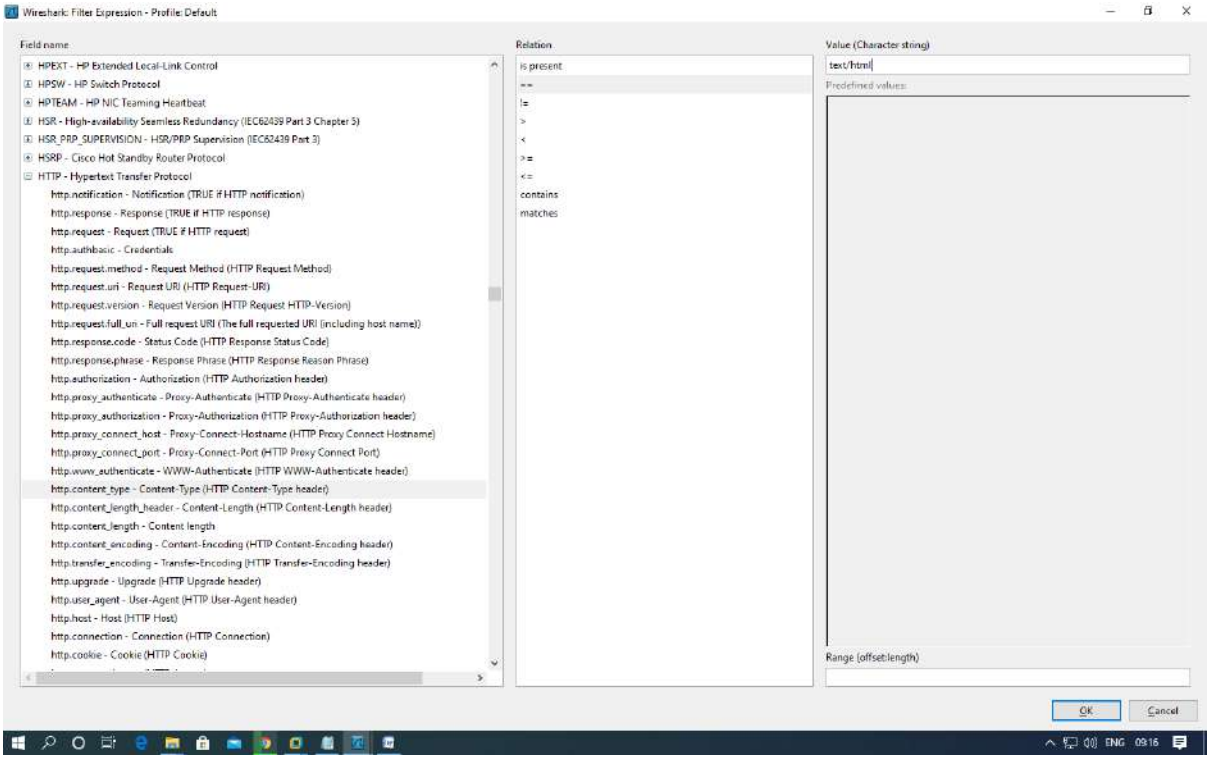

Wireshark: Filter Expression - Profile: Default
Field name
Relation
Value (Unsigned integer, 8 bytes)
is present
==
!=
>
<
>=
<=
251
Predefined values:
Range (offset:length)
HI2OPERATIONS - HI2Operations
HIP - Host Identity Protocol
HNBAP - UTRAN Iuh interface HNBAP signalling
HomePlug - HomePlug protocol
HomePlug AV - HomePlug AV protocol
HP_ERM - HP encapsulated remote mirroring
HPEXT - HP Extended Local-Link Control
HPSW - HP Switch Protocol
HPTEAM - HP NIC Teaming Heartbeat
HSR - High-availability Seamless Redundancy (IEC62439 Part 3 Chapter 5)
HSR_PRP_SUPERVISION - HSR/PRP Supervision (IEC62439 Part 3)
HSRP - Cisco Hot Standby Router Protocol
HTTP - Hypertext Transfer Protocol
http.notification - Notification (TRUE if HTTP notification)
http.response - Response (TRUE if HTTP response)
http.request - Request (TRUE if HTTP request)
http.authbasic - Credentials
http.request.method - Request Method (HTTP Request Method)
http.request.uri - Request URI (HTTP Request-URI)
http.request.version - Request Version (HTTP Request HTTP-Version)
http.request.full_uri - Full request URI (The full requested URI (including host name))
http.response.code - Status Code (HTTP Response Status Code)
http.response.phrase - Response Phrase (HTTP Response Reason Phrase)
http.authorization - Authorization (HTTP Authorization header)
http.proxy_authenticate - Proxy-Authenticate (HTTP Proxy-Authenticate header)
http.proxy_authorization - Proxy-Authorization (HTTP Proxy-Authorization header)
http.proxy_connect_host - Proxy-Connect-Hostname (HTTP Proxy Connect Hostname)
http.proxy_connect_port - Proxy-Connect-Port (HTTP Proxy Connect Port)
http.www_authenticate - WWW-Authenticate (HTTP WWW-Authenticate header)
http.content_type - Content-Type (HTTP Content-Type header)
http.content_length_header - Content-Length (HTTP Content-Length header)
http.content_length - Content length
http.content_encoding - Content-Encoding (HTTP Content-Encoding header)
OK
Cancel
ENG 09:15

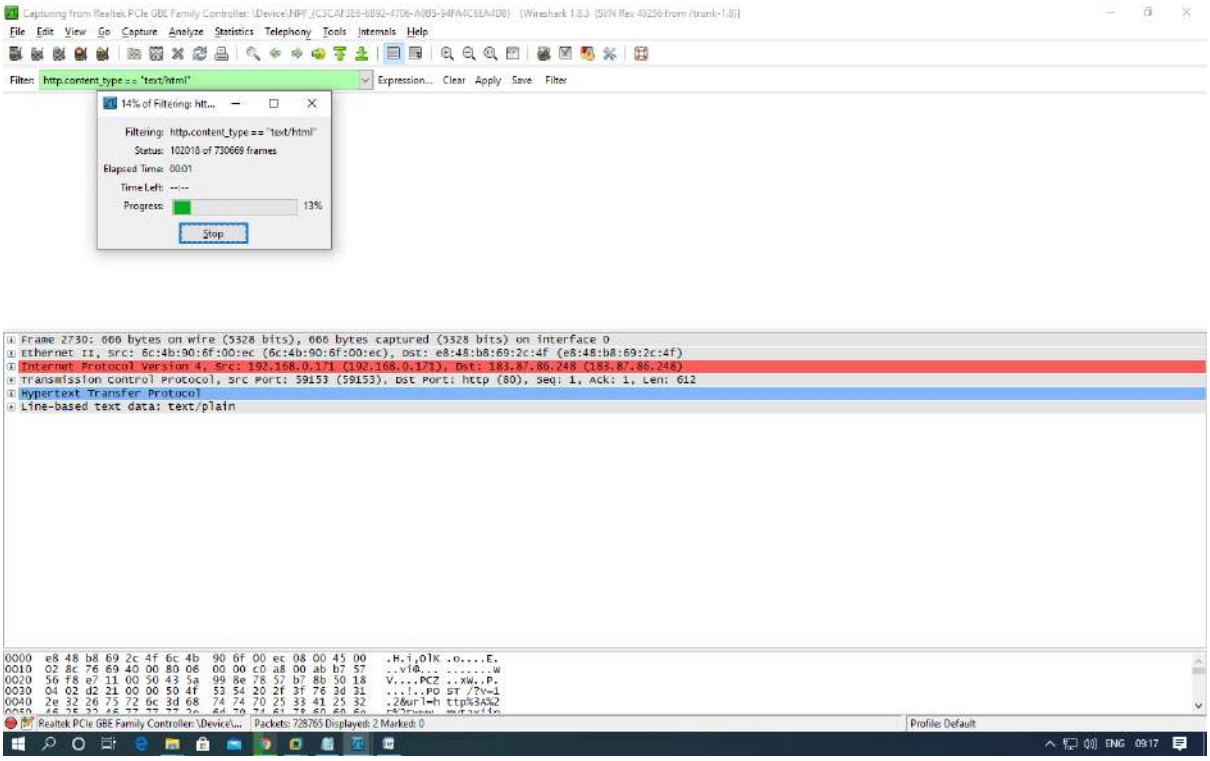

Capturing from Realtek PCIe GBE Family Controller: \Device\NPF_{C3CAF3E6-6B92-4706-A0B5-94FA4C6EA4D8} (Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8))
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
22% of Filtering: ht...
Filtering: http.content_length < 251
Status: 129318 of 618166 frames
Elapsed Time: 00:01
Time Left: --:--
Progress: 20%
Stop
Expression... Clear Apply Save Filter


Frame 3: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
Ethernet II, Src: 6c:4b:90:ae:50:9f (6c:4b:90:ae:50:9f), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.0.119 (192.168.0.119), Dst: 239.255.255.250 (239.255.255.250)
User Datagram Protocol, Src Port: 55575 (55575), Dst Port: ssdp (1900)
Hypertext Transfer Protocol
0000 01 00 5e 7f ff fa 6c 4b 90 ae 50 9f 08 00 45 00 ..^...lK ..P...E.
0010 00 ca fb d1 00 00 01 11 0c 38 c0 a8 00 77 ef ff .... .8...w..
0020 ff fa d9 17 07 6c 00 b6 6a 32 4d 2d 53 45 41 52 .....l.. j2M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1..H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239 .255.255
Realtek PCIe GBE Family Controller: \Device\... Packets: 615831 Displayed: 660 Marked: 0
Profile: Default

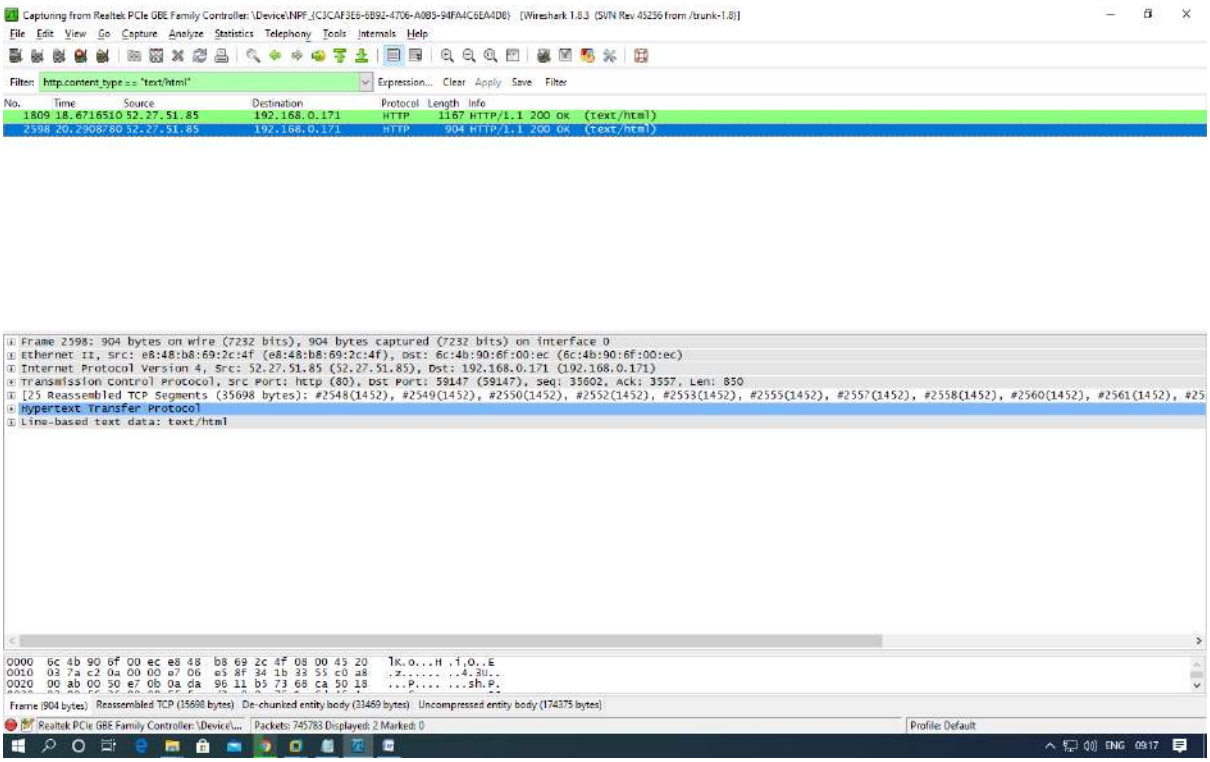

Capturing from Realtek PCIe GBE Family Controller: \Device\NPF_{C3CAF3E6-6B92-4706-A0B5-94FA4C6EA4D8} [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http.content_length < 251
Expression... Clear Apply Save Filter
No. Time Source Destination Protocol Length Info
2730 20.636073 0 192.168.0.171 183.87.86.248 HTTP 666 POST /?v=1.2&url=http%3A%2F%2Fwww.mytaxiindia.com%2F HTTP/1.1 (text/plain)
2742 20.648686 0 183.87.86.248 192.168.0.171 HTTP 893 HTTP/1.1 200 OK (application/json)


Frame 2730: 666 bytes on wire (5328 bits), 666 bytes captured (5328 bits) on interface 0
Ethernet II, Src: 6c:4b:90:6f:00:ec (6c:4b:90:6f:00:ec), Dst: e8:48:b8:69:2c:4f (e8:48:b8:69:2c:4f)
Internet Protocol Version 4, Src: 192.168.0.171 (192.168.0.171), Dst: 183.87.86.248 (183.87.86.248)
Transmission Control Protocol, Src Port: 59153 (59153), Dst Port: http (80), Seq: 1, Ack: 1, Len: 612
Hypertext Transfer Protocol
Line-based text data: text/plain
0000 e8 48 b8 69 2c 4f 6c 4b 90 6f 00 ec 08 00 45 00 .H.i,OlK .o....E.
0010 02 8c 76 69 40 00 80 06 00 00 c0 a8 00 ab b7 57 ..vi@... ....W
0020 56 f8 e7 11 00 50 43 5a 99 8e 78 57 b7 8b 50 18 V....PCZ ..xW..P.
0030 04 02 d2 21 00 00 50 4f 53 54 20 2f 3f 76 3d 31 ...!..PO ST /?v=1
0040 2e 32 26 75 72 6c 3d 68 74 74 70 25 33 41 25 32 .2&url=h ttp%3A%2
Realtek PCIe GBE Family Controller: \Device\... Packets: 634816 Displayed: 2 Marked: 0
Profile: Default


Wireshark: Filter Expression - Profile: Default
Field name
Relation
Value (Character string)
text/html
Predefined values:
Range (offset:length)
OK
Cancel


Filter: http.content_type == "text/html"
Expression... Clear Apply Save Filter
14% of Filtering: htt...
Filtering: http.content_type == "text/html"
Status: 102018 of 730669 frames
Elapsed Time: 00:01
Time Left: --:--
Progress: 13%
Stop

Frame 2730: 666 bytes on wire (5328 bits), 666 bytes captured (5328 bits) on interface 0
Ethernet II, Src: 6c:4b:90:6f:00:ec (6c:4b:90:6f:00:ec), Dst: e8:48:b8:69:2c:4f (e8:48:b8:69:2c:4f)
Internet Protocol Version 4, Src: 192.168.0.171 (192.168.0.171), Dst: 183.87.86.248 (183.87.86.248)
Transmission Control Protocol, Src Port: 59153 (59153), Dst Port: http (80), Seq: 1, Ack: 1, Len: 612
Hypertext Transfer Protocol
Line-based text data: text/plain


Capturing from Realtek PCIe GBE Family Controller: \Device\NPF_{C3CAF3E6-6B92-4706-A0B5-94FA4C6EA4D6} [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http.content_type == "text/html"
Expression... Clear Apply Save Filter
No. Time Source Destination Protocol Length Info
1809 18.6716510 52.27.51.85 192.168.0.171 HTTP 1167 HTTP/1.1 200 OK (text/html)
2598 20.2908780 52.27.51.85 192.168.0.171 HTTP 904 HTTP/1.1 200 OK (text/html)
Frame 2598: 904 bytes on wire (7232 bits), 904 bytes captured (7232 bits) on interface 0
Ethernet II, Src: e8:48:b8:69:2c:4f (e8:48:b8:69:2c:4f), Dst: 6c:4b:90:6f:00:ec (6c:4b:90:6f:00:ec)
Internet Protocol Version 4, Src: 52.27.51.85 (52.27.51.85), Dst: 192.168.0.171 (192.168.0.171)
Transmission Control Protocol, Src Port: http (80), Dst Port: 59147 (59147), Seq: 35602, Ack: 3557, Len: 850
[25 Reassembled TCP Segments (35698 bytes): #2548(1452), #2549(1452), #2550(1452), #2552(1452), #2553(1452), #2555(1452), #2557(1452), #2558(1452), #2560(1452), #2561(1452), #25
Hypertext Transfer Protocol
Line-based text data: text/html
0000 6c 4b 90 6f 00 ec e8 48 b8 69 2c 4f 08 00 45 20
0010 03 7a c2 0a 00 00 e7 06 e5 8f 34 1b 33 55 c0 a8
0020 00 ab 00 50 e7 0b 0a da 96 11 b5 73 68 ca 50 18
Frame (904 bytes) Reassembled TCP (35698 bytes) De-chunked entity body (33469 bytes) Uncompressed entity body (174375 bytes)
Realtek PCIe GBE Family Controller: \Device\... Packets: 745783 Displayed: 2 Marked: 0
Profile: Default
ENG 09:17

Practical No. 08

Aim: Using Email Forensics Tools [AccessData FTK].

What is Email Forensics?

Email forensics is **the study of source and content of email as evidence to identify the actual sender and recipient** of a message along with some other information such as date/time of transmission and intention of sender. It involves investigating metadata, port scanning as well as keyword searching.

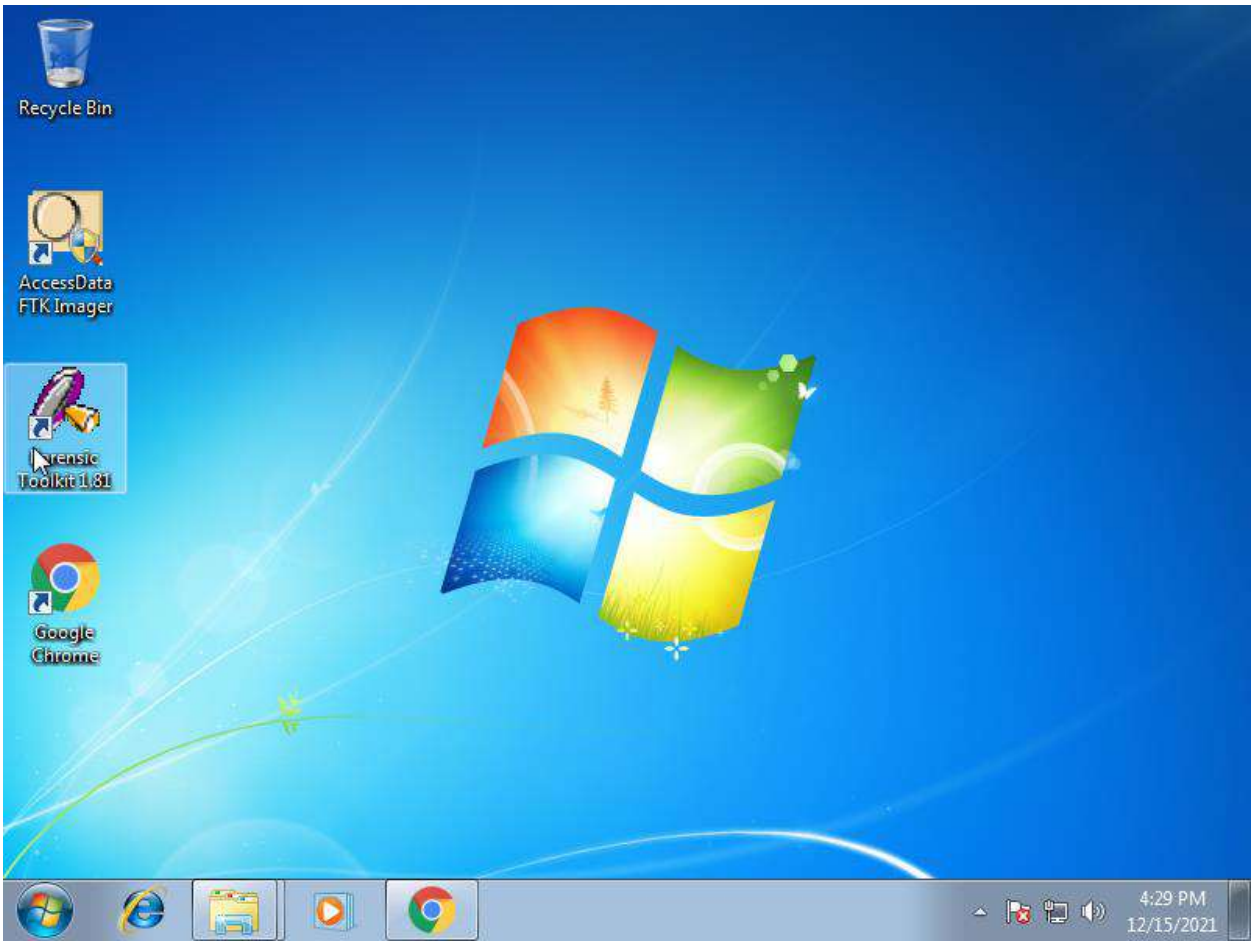
What is AccessData FTK Tool?

Forensic Toolkit, or FTK, is a computer forensics software made by AccessData. It **scans a hard drive looking for various information**. It can, for example, potentially locate deleted emails and scan a disk for text strings to use them as a password dictionary to crack encryption.

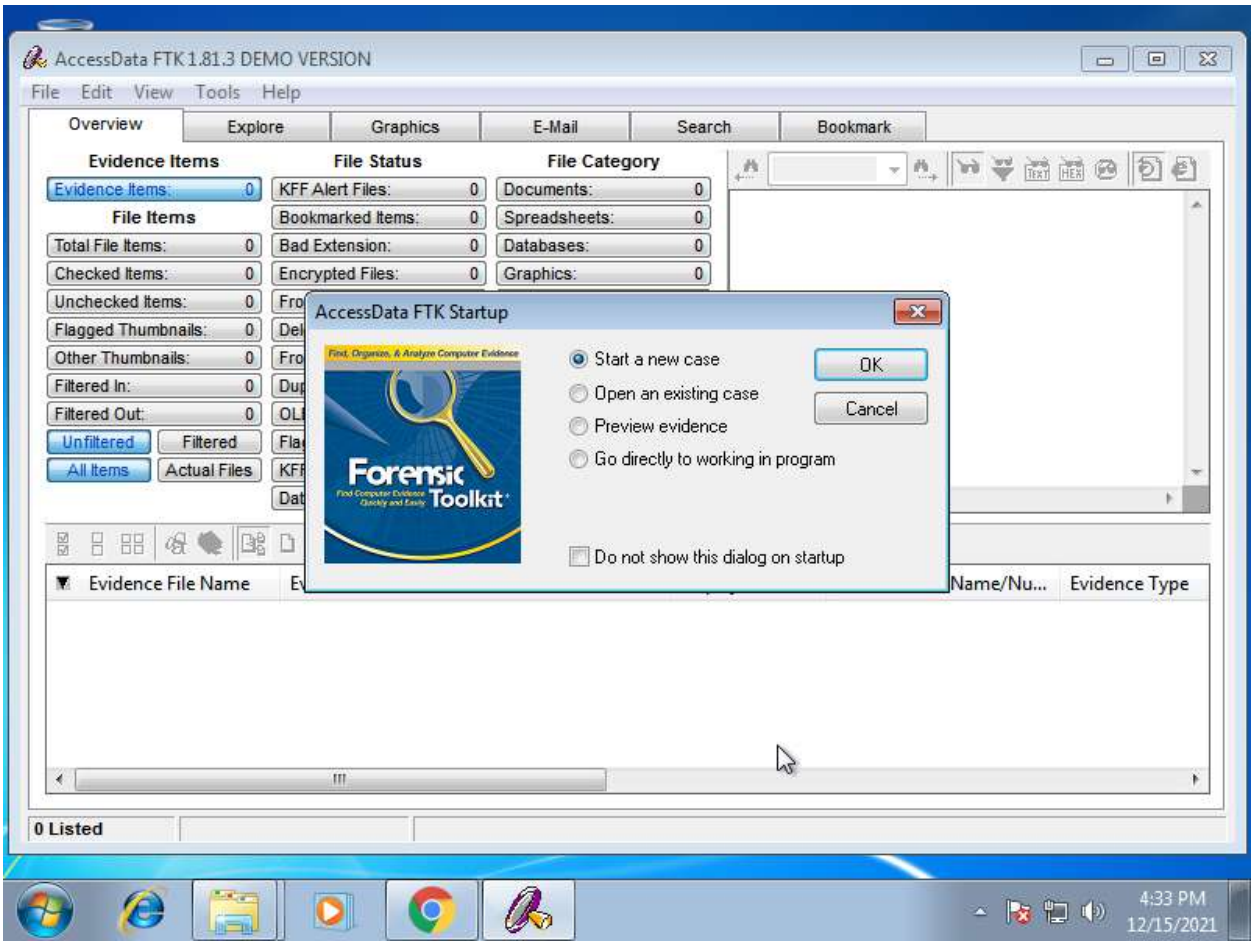
FTK provides an **intuitive interface for email analysis** for forensic professionals. This includes having the ability to parse emails for certain words, header analysis for source IP address, etc. A central feature of FTK, file decryption is arguably the most common use of the software.

Steps:

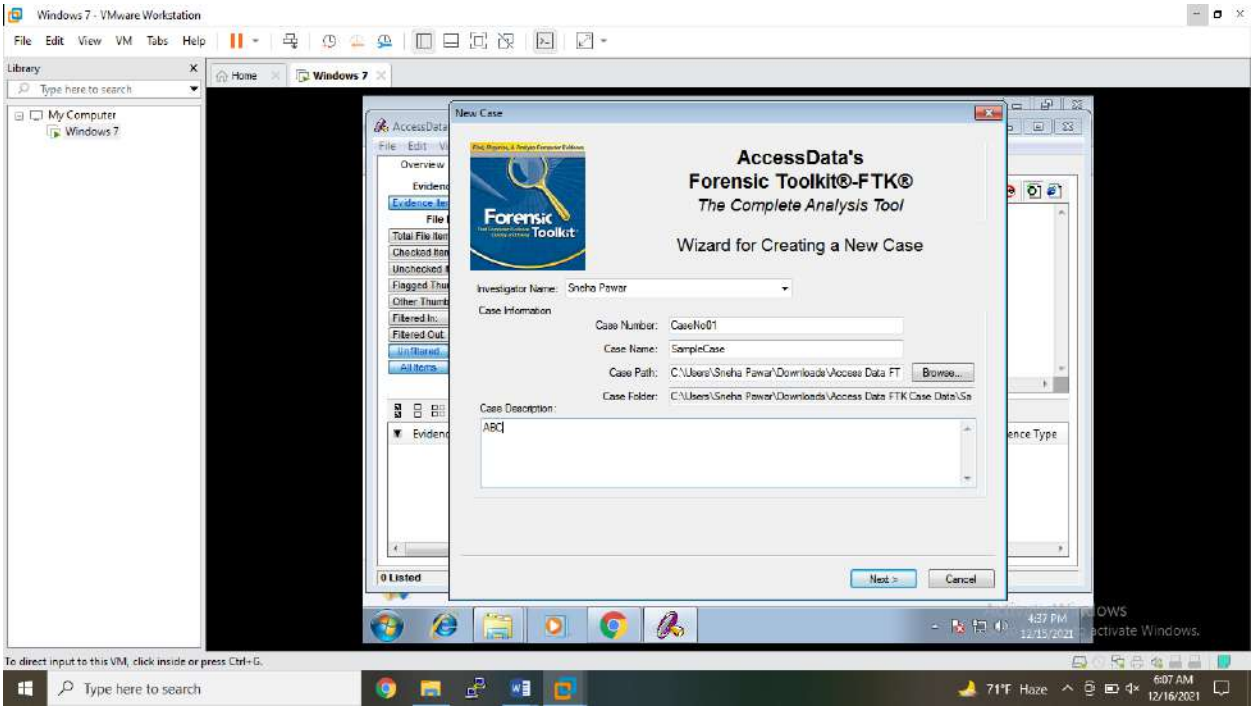
Start the forensic toolkit software.



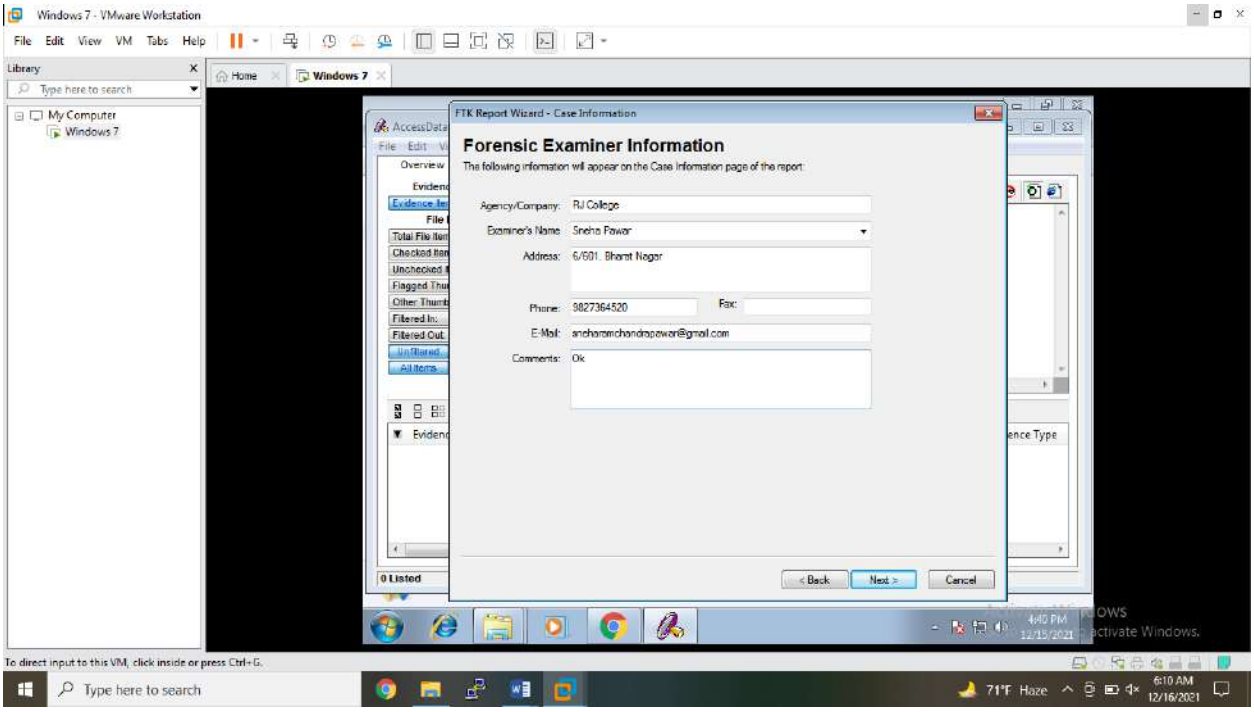
Select Start a New Case.



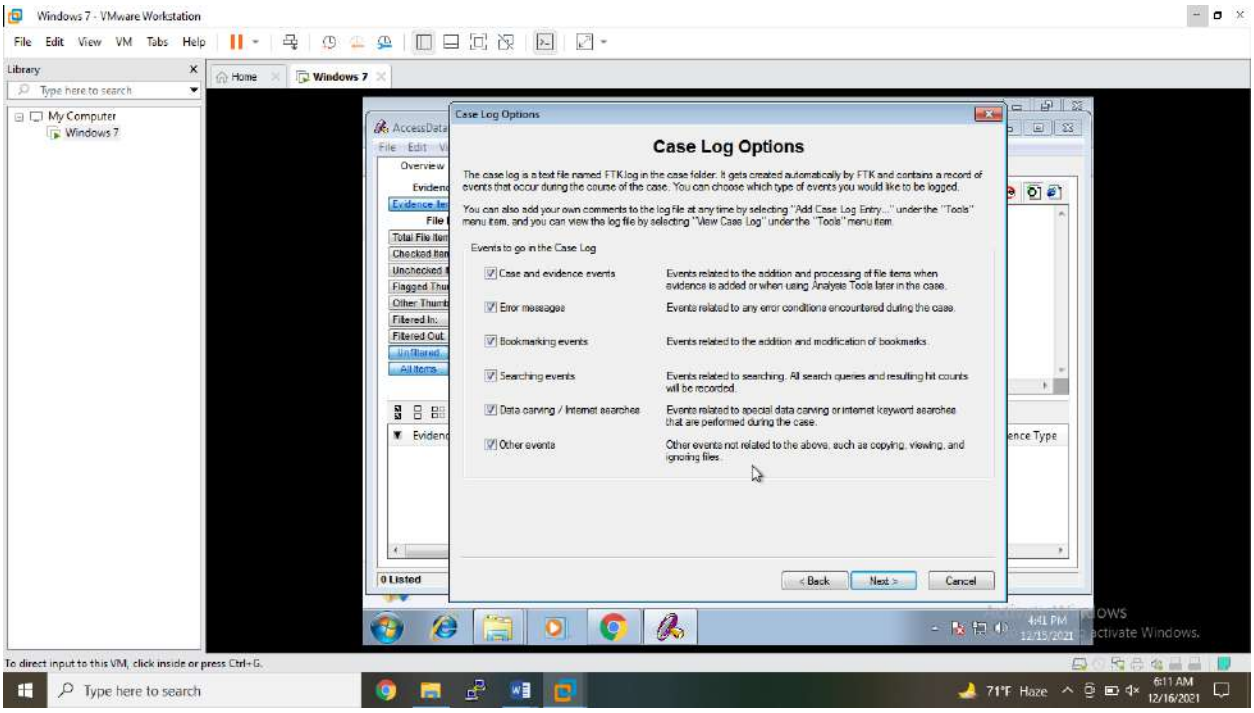
Then enter investigator's name and other details and click on Next.

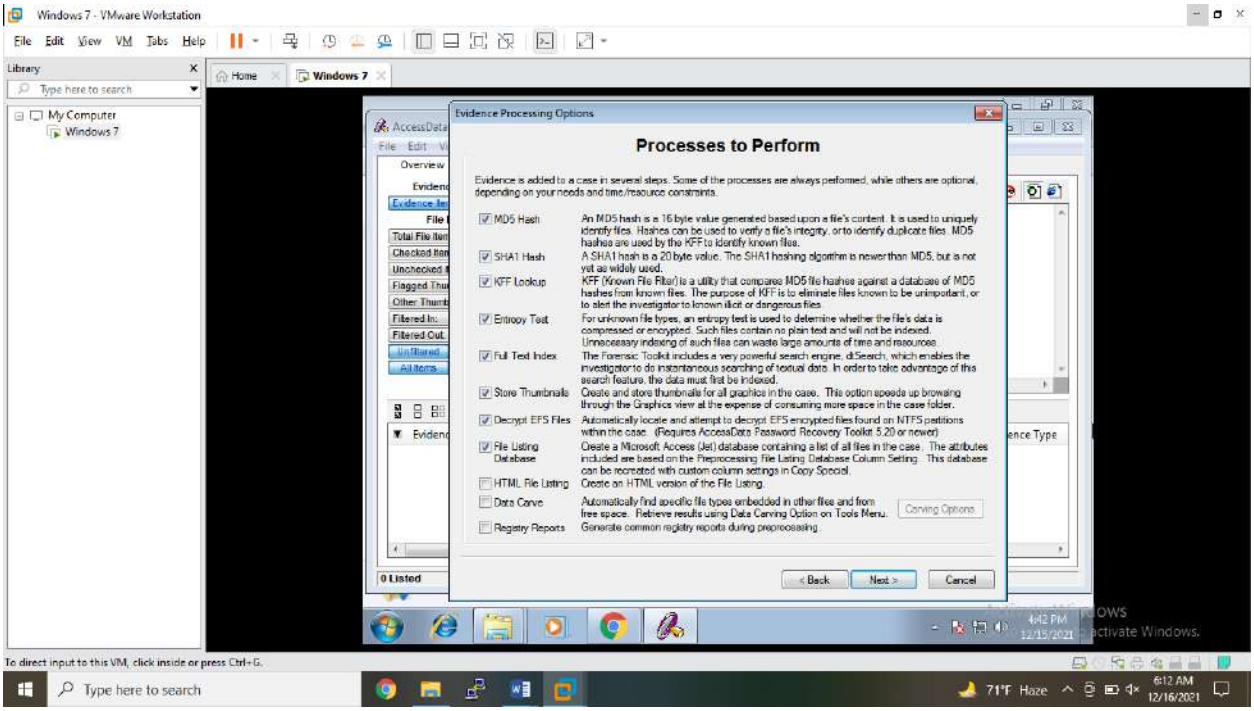


Then enter forensic examiner's details.

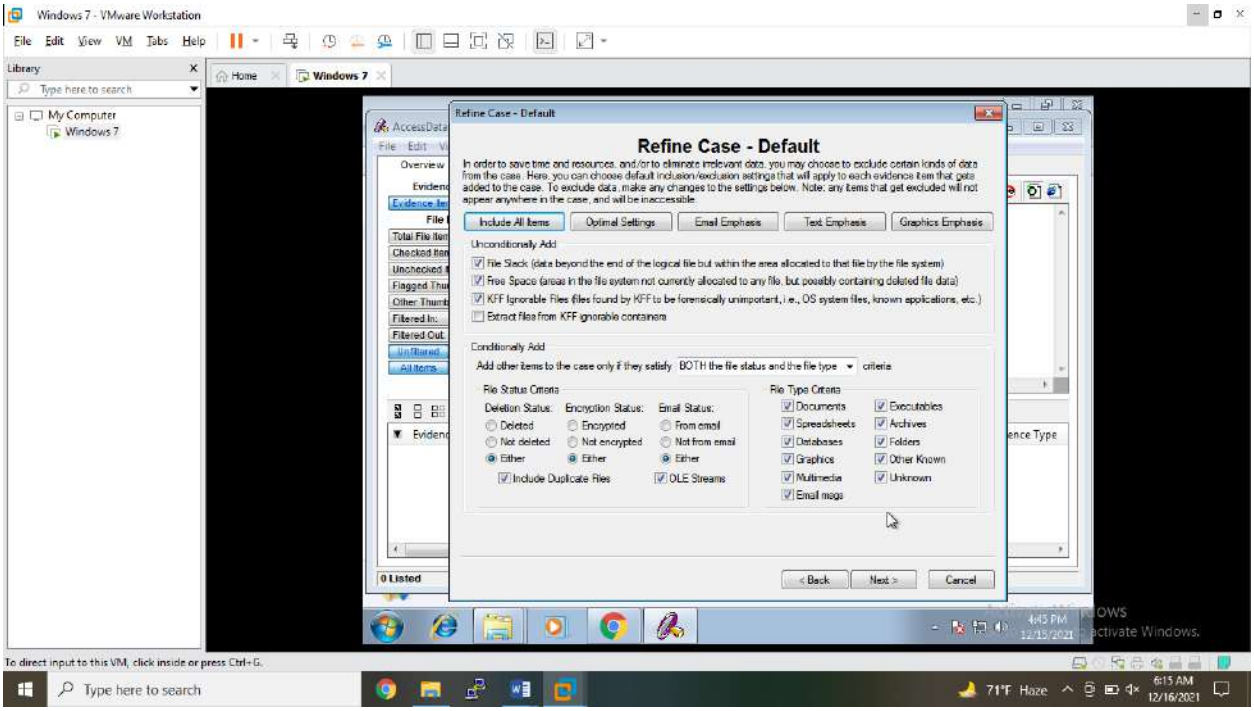


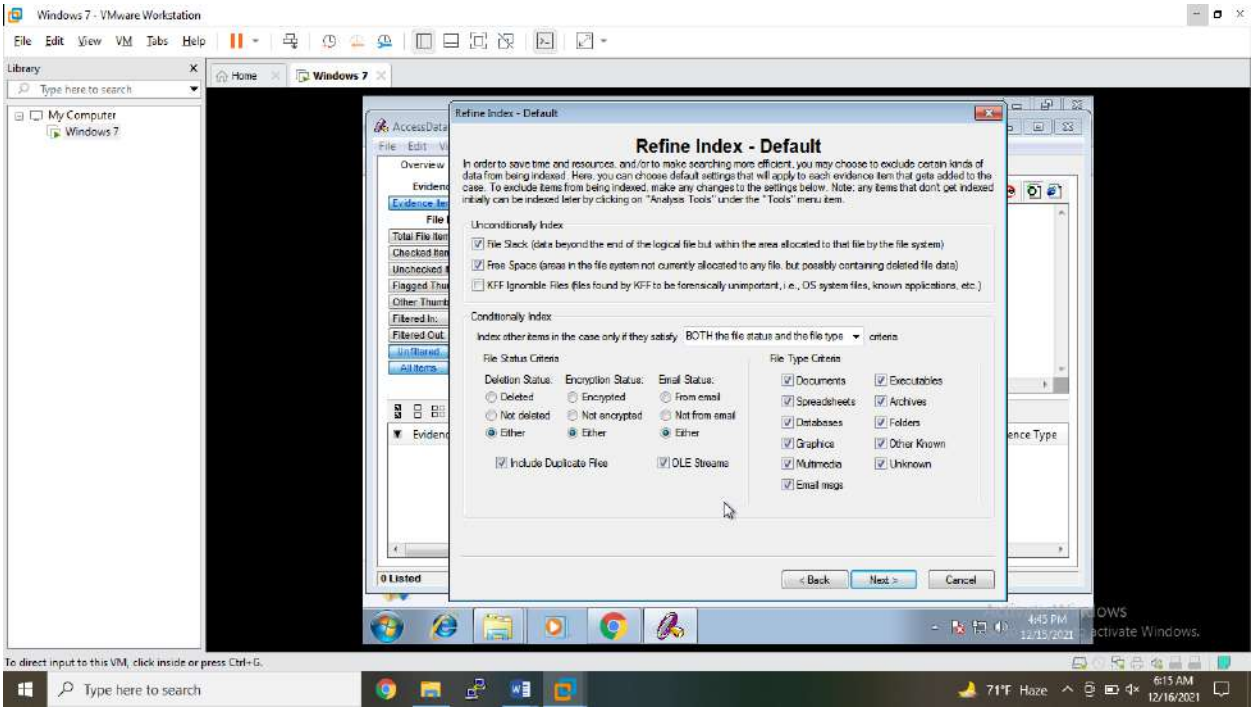
In Case Log Options & Process to perform tabs, keep everything by default.



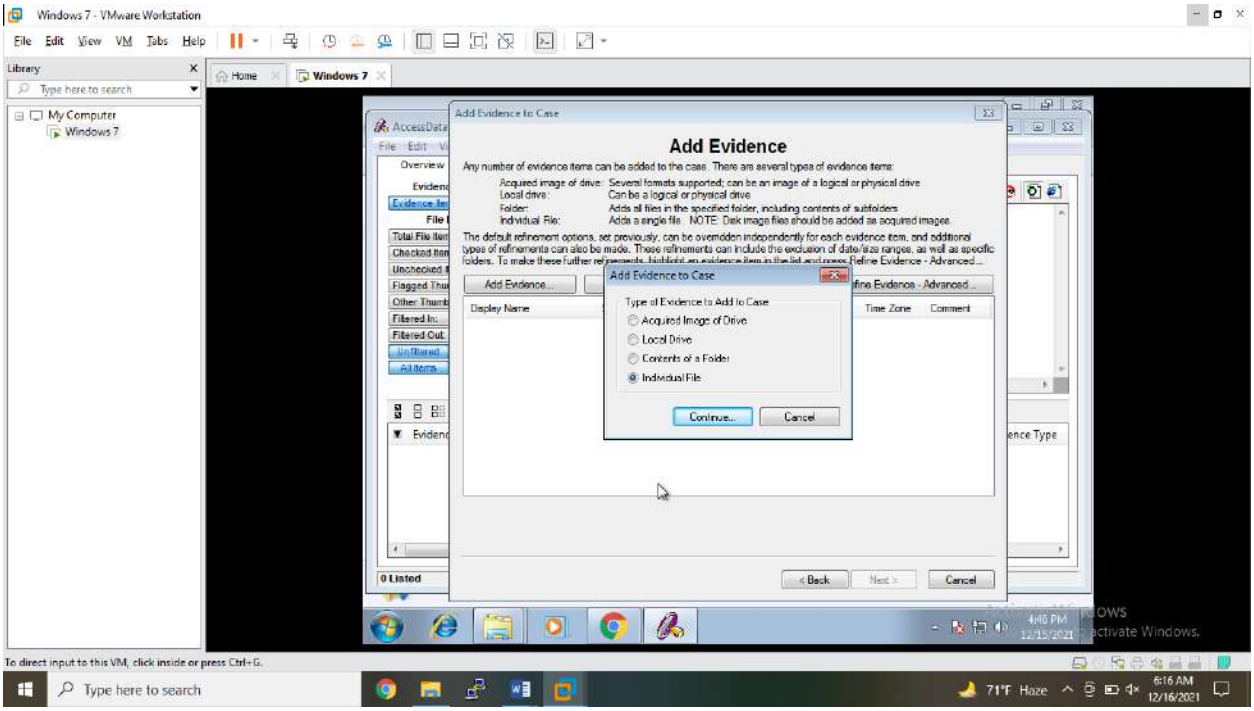


Then in Refine Case Default, Keep everything as it is, and click on Next.

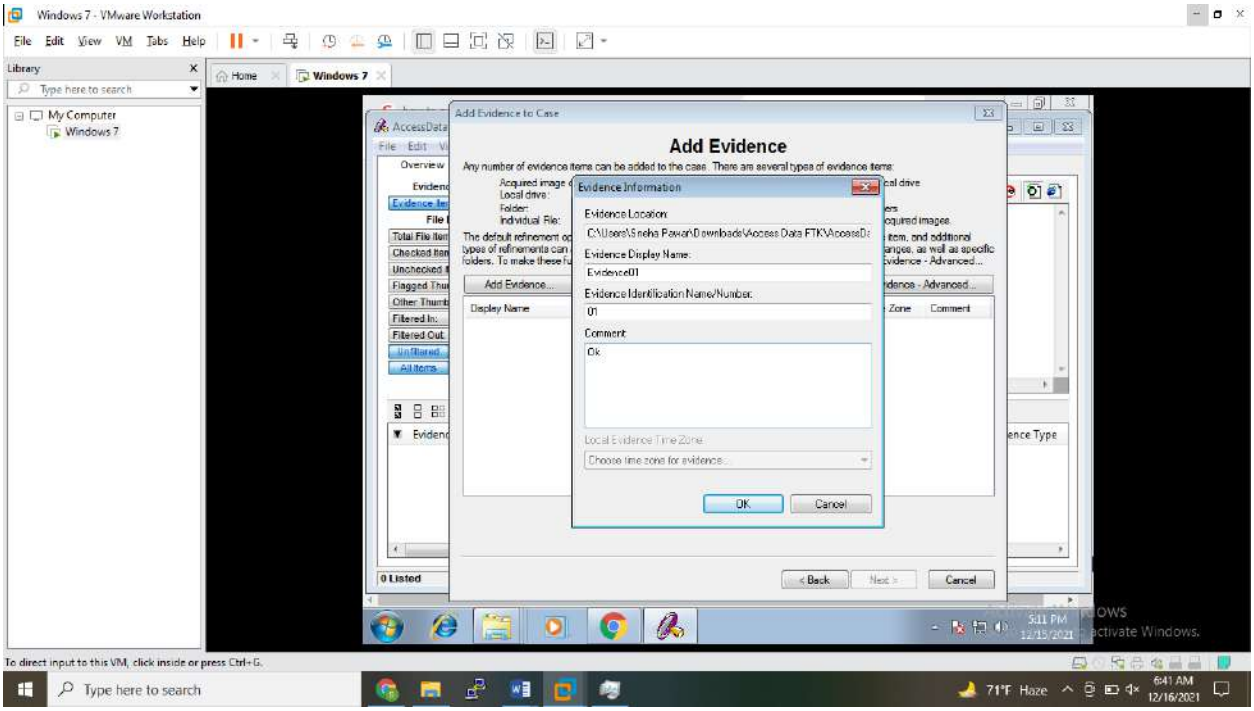


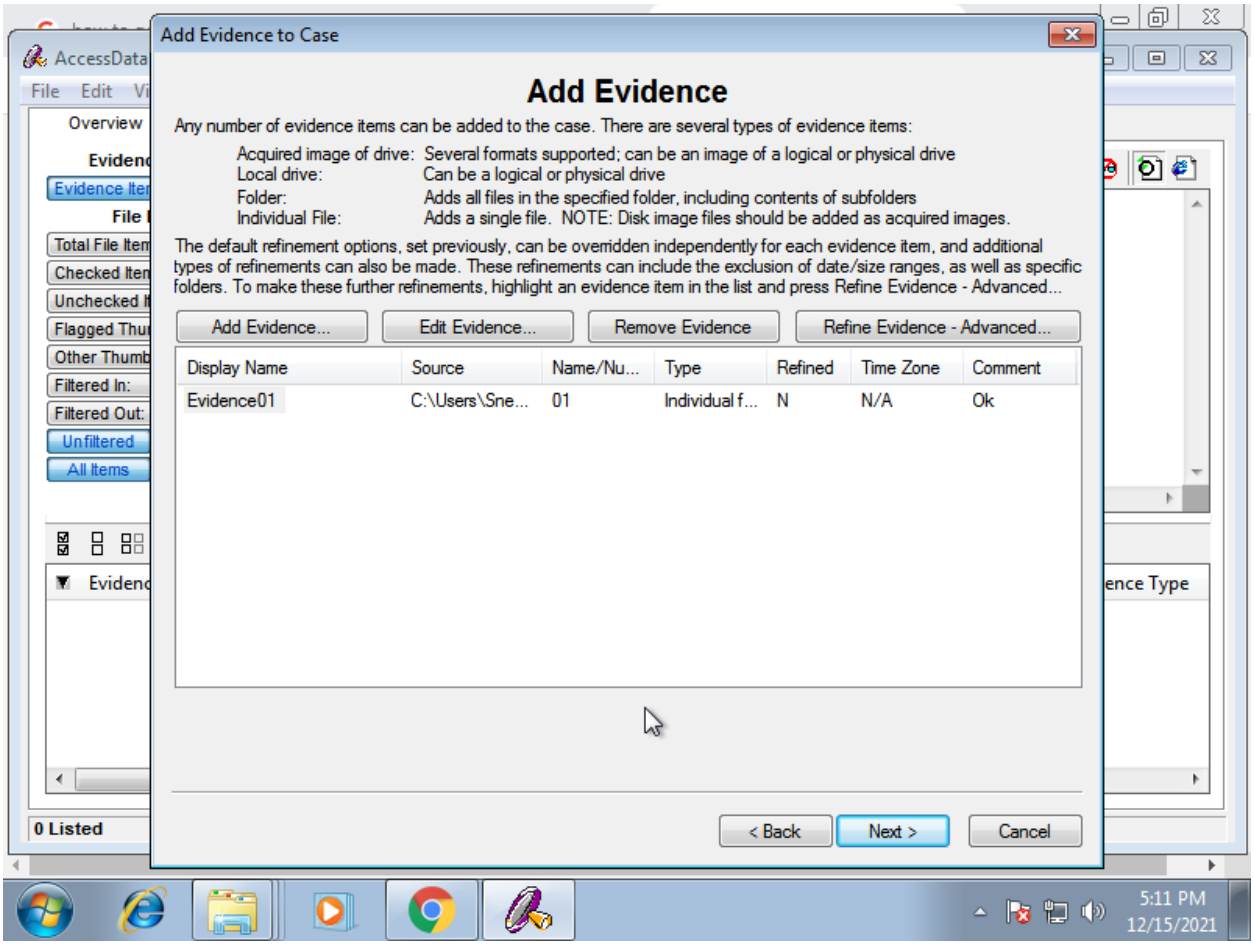


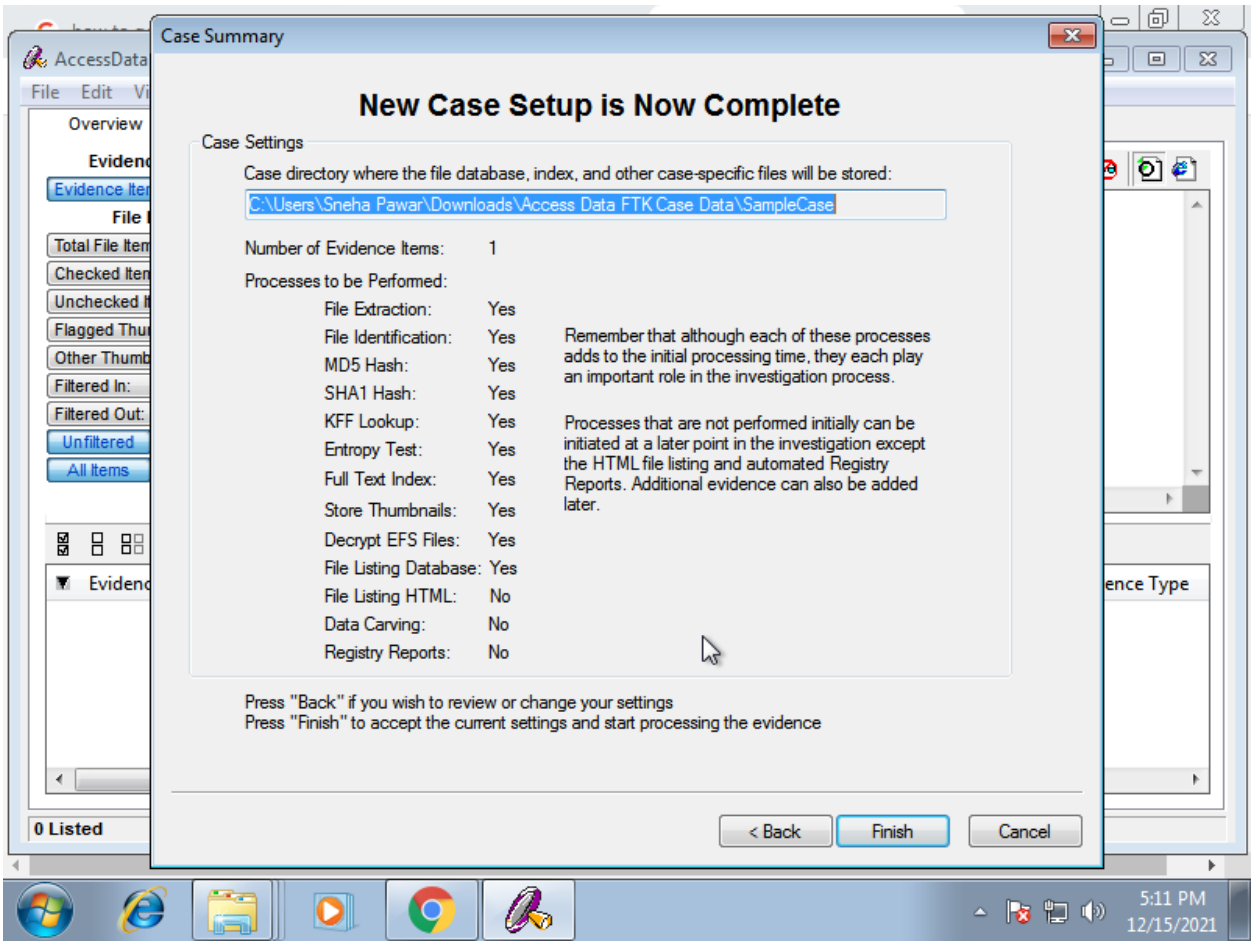
Then click on Add Evidence – Add Individual File.



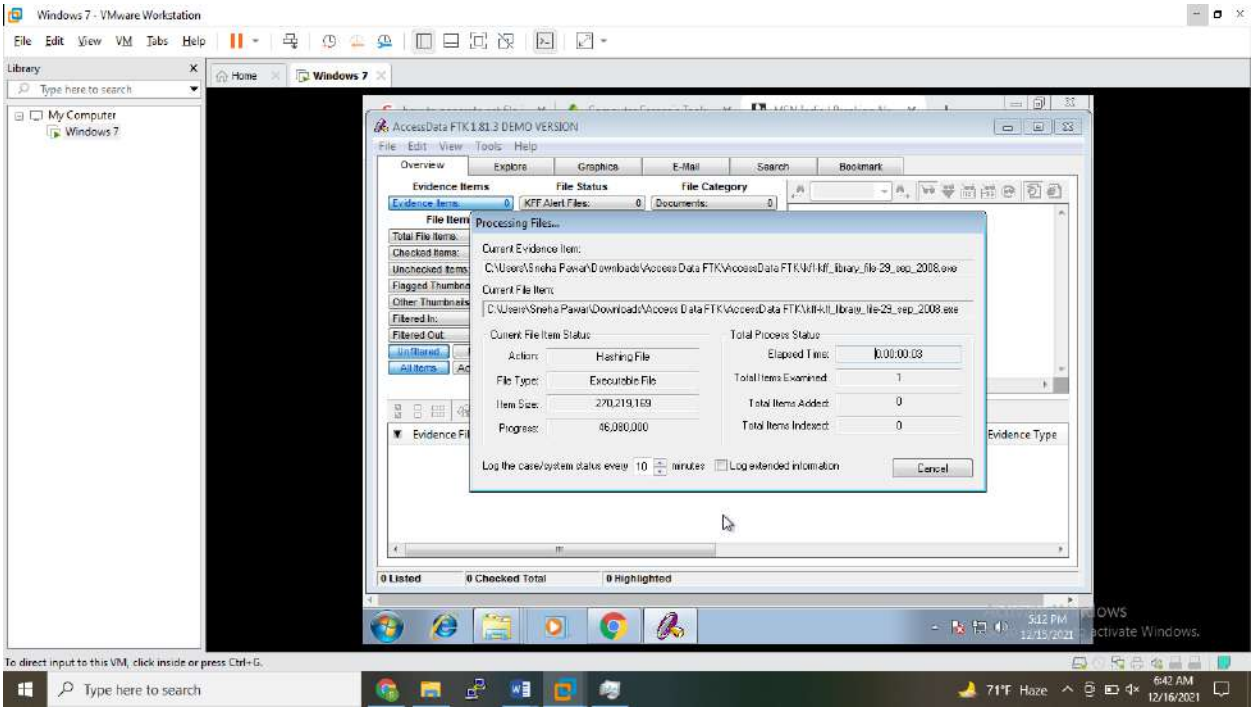
Then Browse for Evidence location, and enter other details.

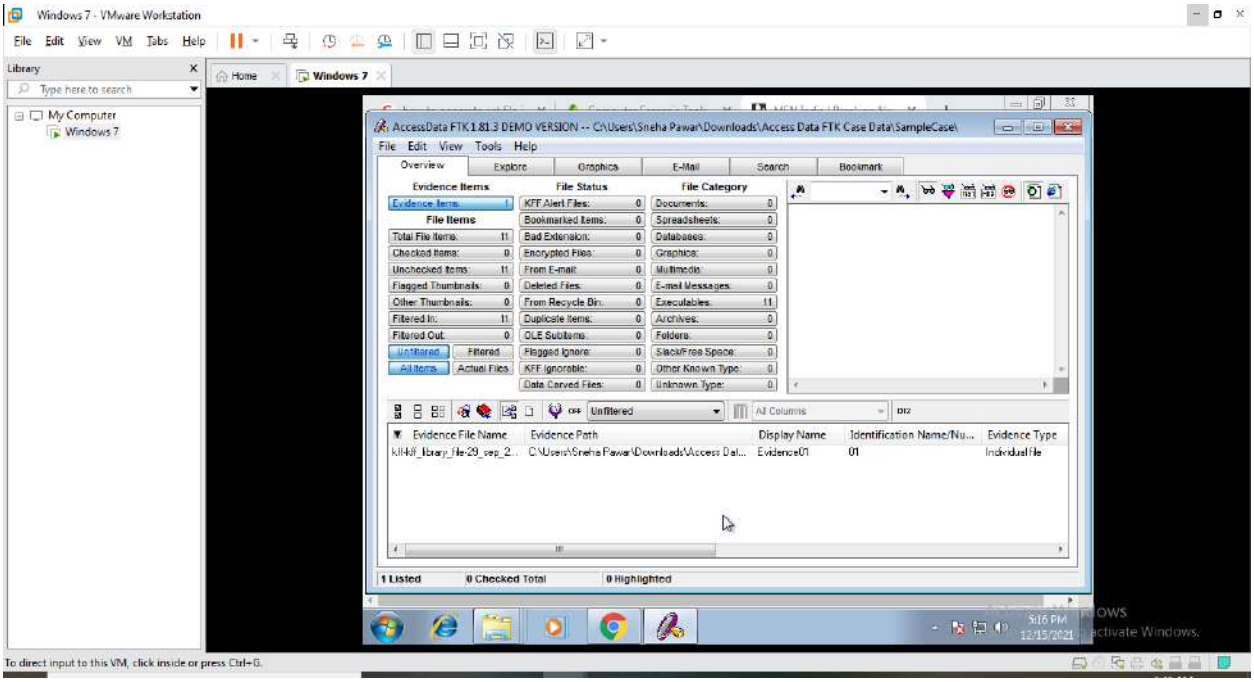

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
Add Evidence to Case
Add Evidence
Any number of evidence items can be added to the case. There are several types of evidence items:
Evidence Information
Evidence Location:
C:\Users\Sneha Pawar\Downloads\Access Data FTK\AccessDa
Evidence Display Name:
Evidence01
Evidence Identification Name/Number:
01
Comment:
Ok
Local Evidence Time Zone
Choose time zone for evidence...
OK
Cancel
Add Evidence...
Display Name
Zone
Comment
0 Listed
< Back
Next >
Cancel
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
71°F Haze
6:41 AM
12/16/2021

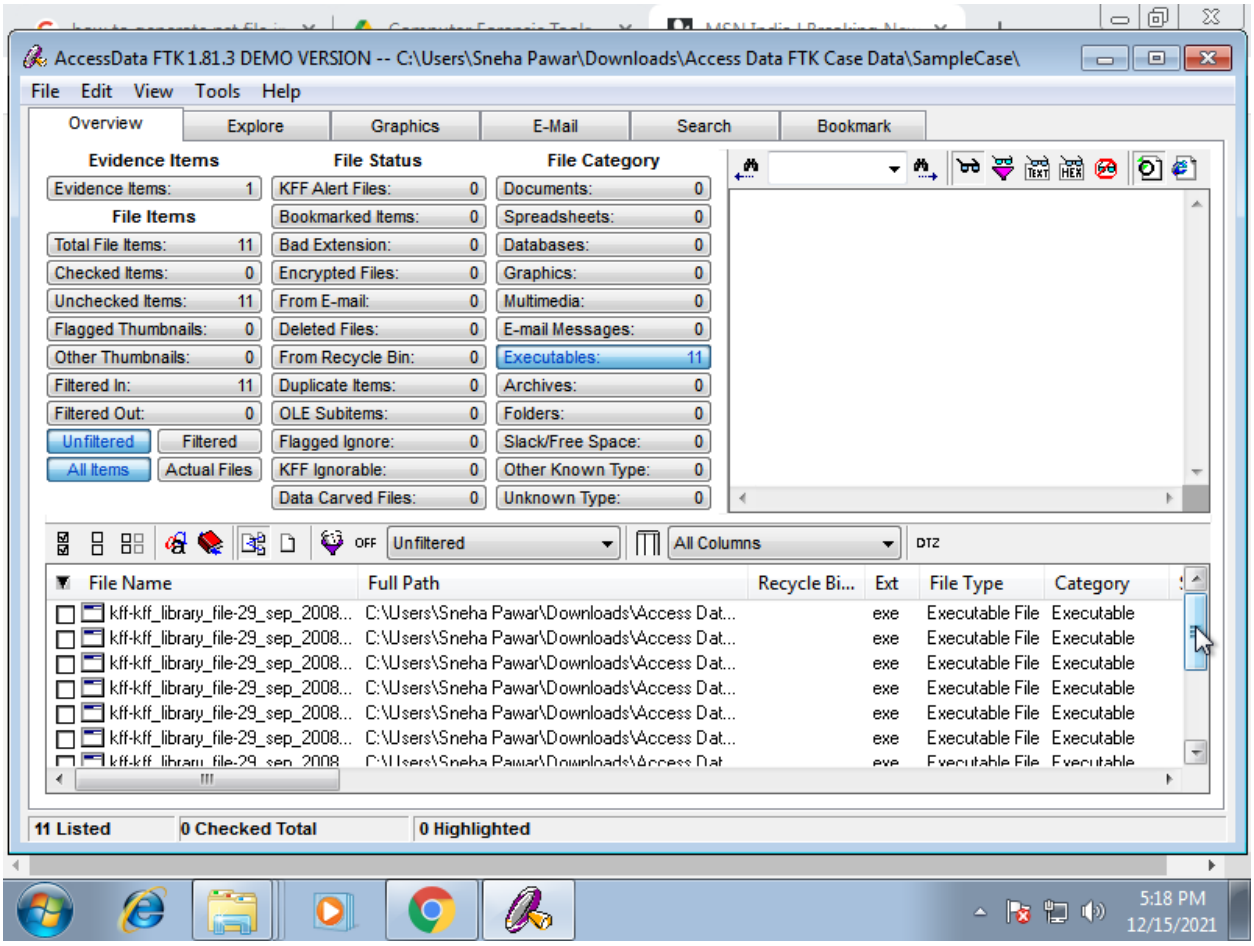

AccessData
File Edit Vi
Overview
Evidenc
Evidence Iten
File I
Total File Item
Checked Iten
Unchecked It
Flagged Thu
Other Thumb
Filtered In:
Filtered Out:
Unfiltered
All Items
Evidenc
ence Type
0 Listed
Add Evidence to Case
Add Evidence
Any number of evidence items can be added to the case. There are several types of evidence items:
Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
Local drive: Can be a logical or physical drive
Folder: Adds all files in the specified folder, including contents of subfolders
Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.
The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...
Add Evidence...
Edit Evidence...
Remove Evidence
Refine Evidence - Advanced...
Display Name
Source
Name/Nu...
Type
Refined
Time Zone
Comment
Evidence01
C:\Users\Sne...
01
Individual f...
N
N/A
Ok
< Back
Next >
Cancel
5:11 PM
12/15/2021



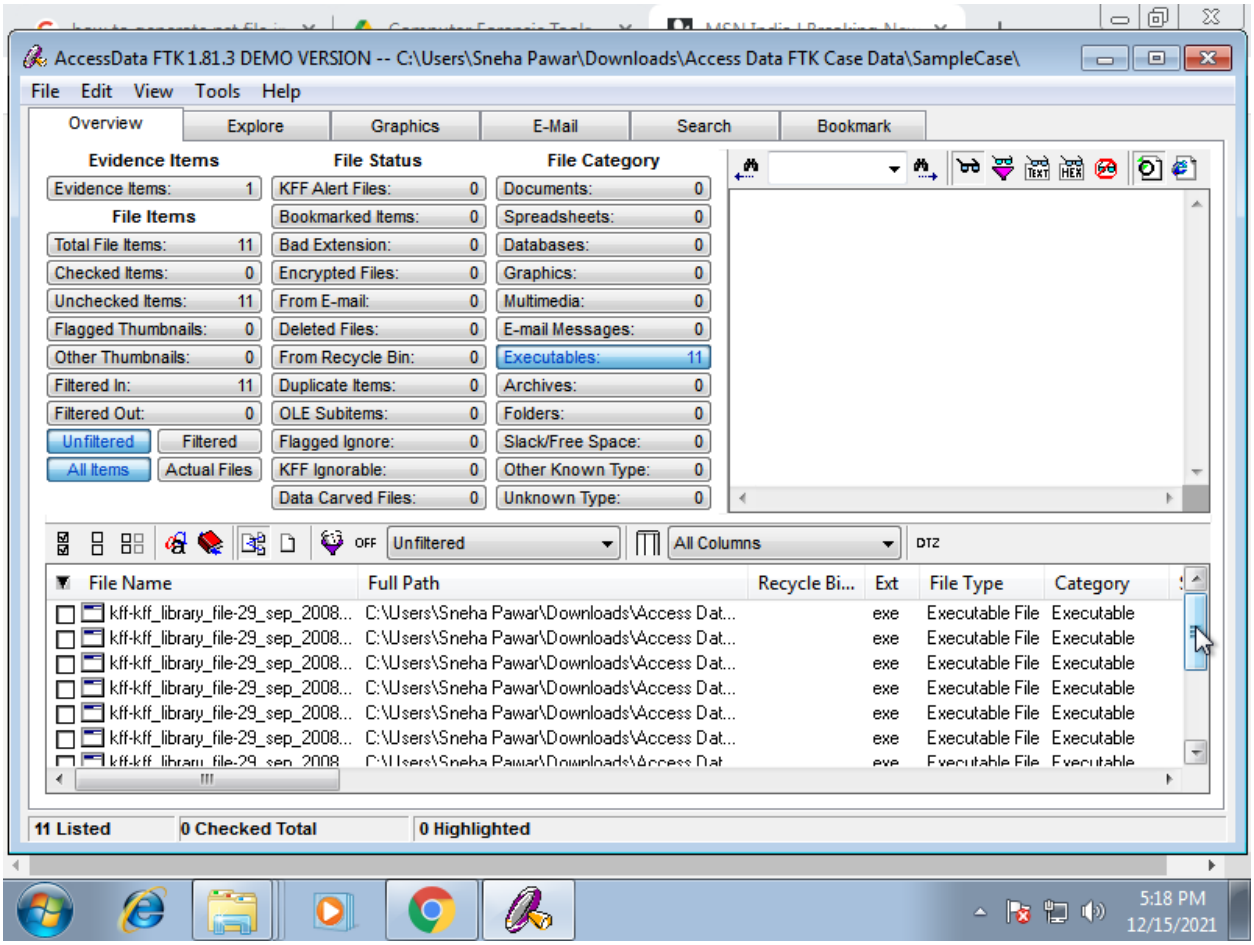
Click on Finish. It will start processing the File.

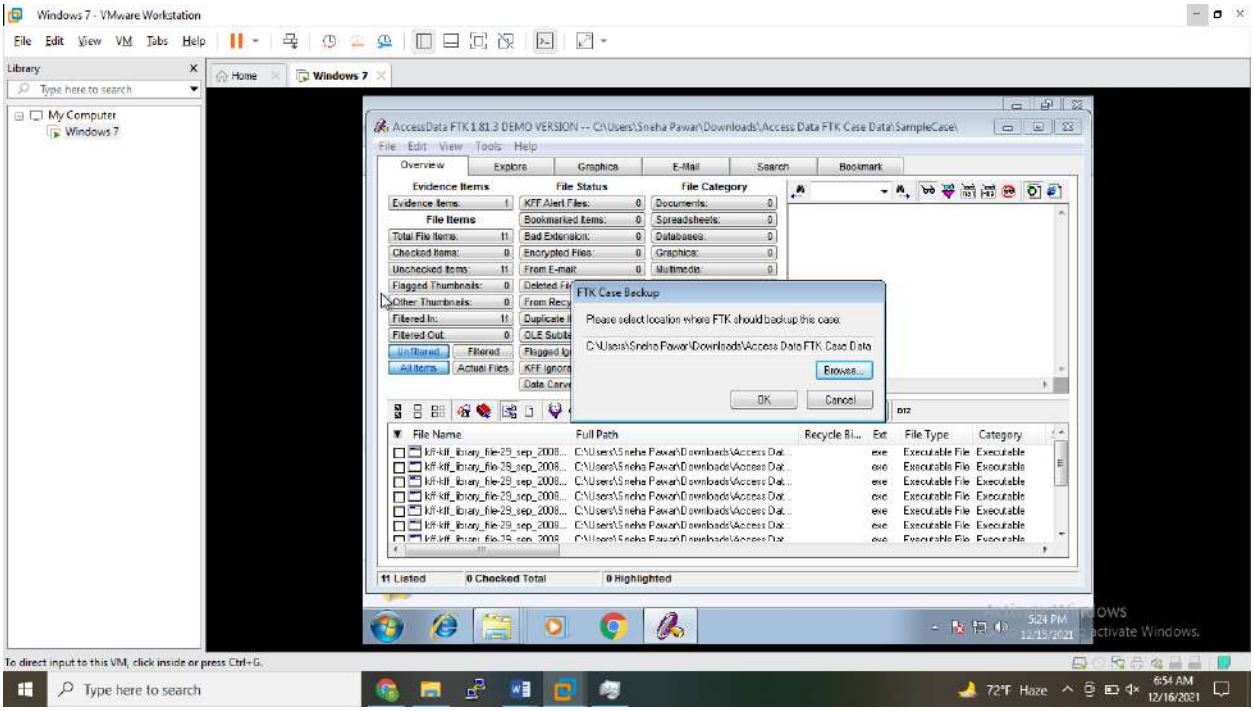


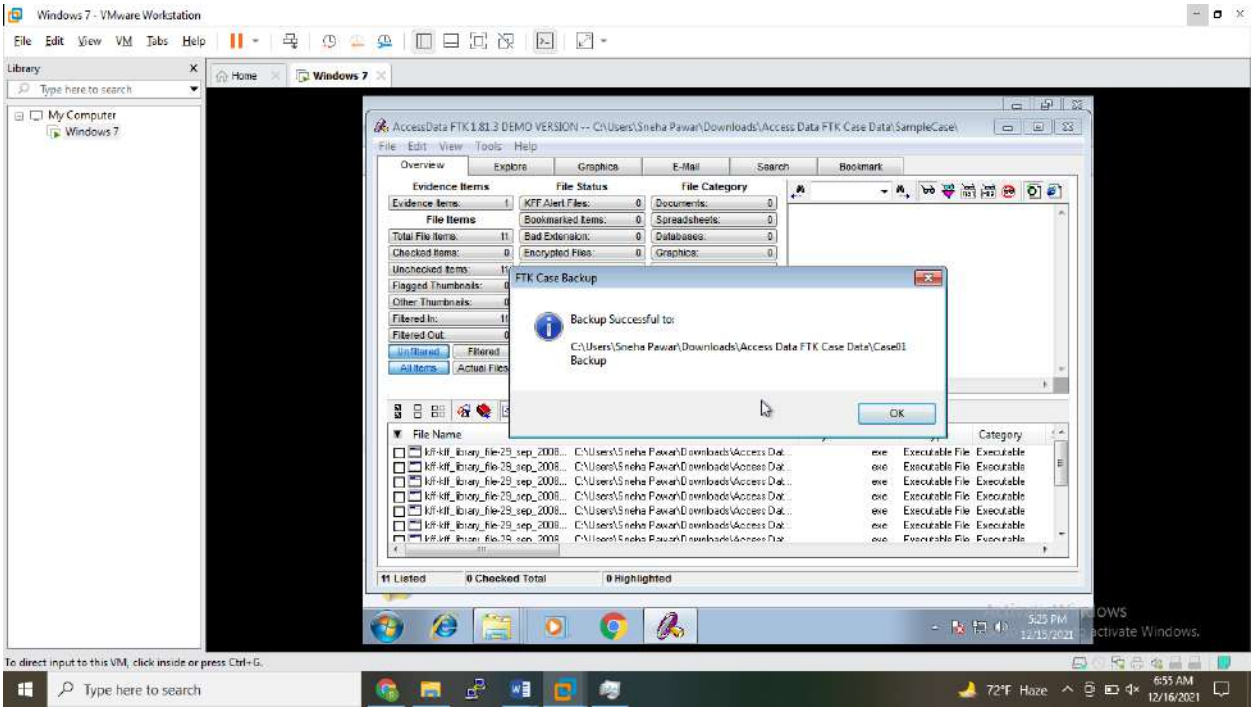

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Evidence Items
File Status
File Category
Evidence Items: 1
File Items
Total File Items: 11
Checked Items: 0
Unchecked Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 11
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 0
Encrypted Files: 0
From E-mail: 0
Deleted Files: 0
From Recycle Bin: 0
Duplicate Items: 0
OLE Subitems: 0
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0
Documents: 0
Spreadsheets: 0
Databases: 0
Graphics: 0
Multimedia: 0
E-mail Messages: 0
Executables: 11
Archives: 0
Folders: 0
Slack/Free Space: 0
Other Known Type: 0
Unknown Type: 0
Unfiltered
All Columns
DTZ
Evidence File Name
Evidence Path
Display Name
Identification Name/Nu...
Evidence Type
kff-kff_library_file-29_sep_2...
C:\Users\Sneha Pawar\Downloads\Access Dat...
Evidence01
01
Individual File
1 Listed
0 Checked Total
0 Highlighted
5:16 PM
12/15/2021
To direct input to this VM, click inside or press Ctrl+G.


AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Evidence Items
File Status
File Category
Evidence Items: 1
File Items
Total File Items: 11
Checked Items: 0
Unchecked Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 11
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 0
Encrypted Files: 0
From E-mail: 0
Deleted Files: 0
From Recycle Bin: 0
Duplicate Items: 0
OLE Subitems: 0
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0
Documents: 0
Spreadsheets: 0
Databases: 0
Graphics: 0
Multimedia: 0
E-mail Messages: 0
Executables: 11
Archives: 0
Folders: 0
Slack/Free Space: 0
Other Known Type: 0
Unknown Type: 0
OFF
Unfiltered
All Columns
DTZ
File Name
Full Path
Recycle Bi...
Ext
File Type
Category
kff-kff_library_file-29_sep_2008...
C:\Users\Sneha Pawar\Downloads\Access Dat...
exe
Executable File
Executable
11 Listed
0 Checked Total
0 Highlighted
5:18 PM
12/15/2021

To take backup of your case, Click on File – Backup Case – And browse for location where you want to take backup.

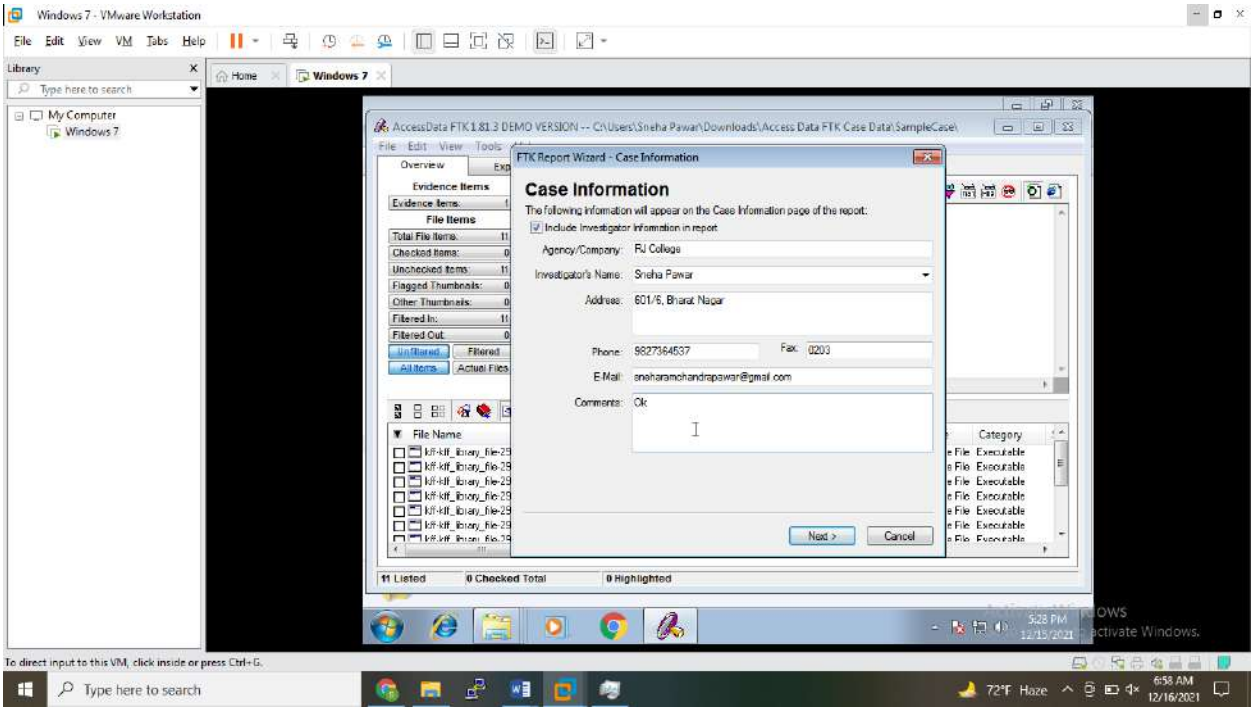


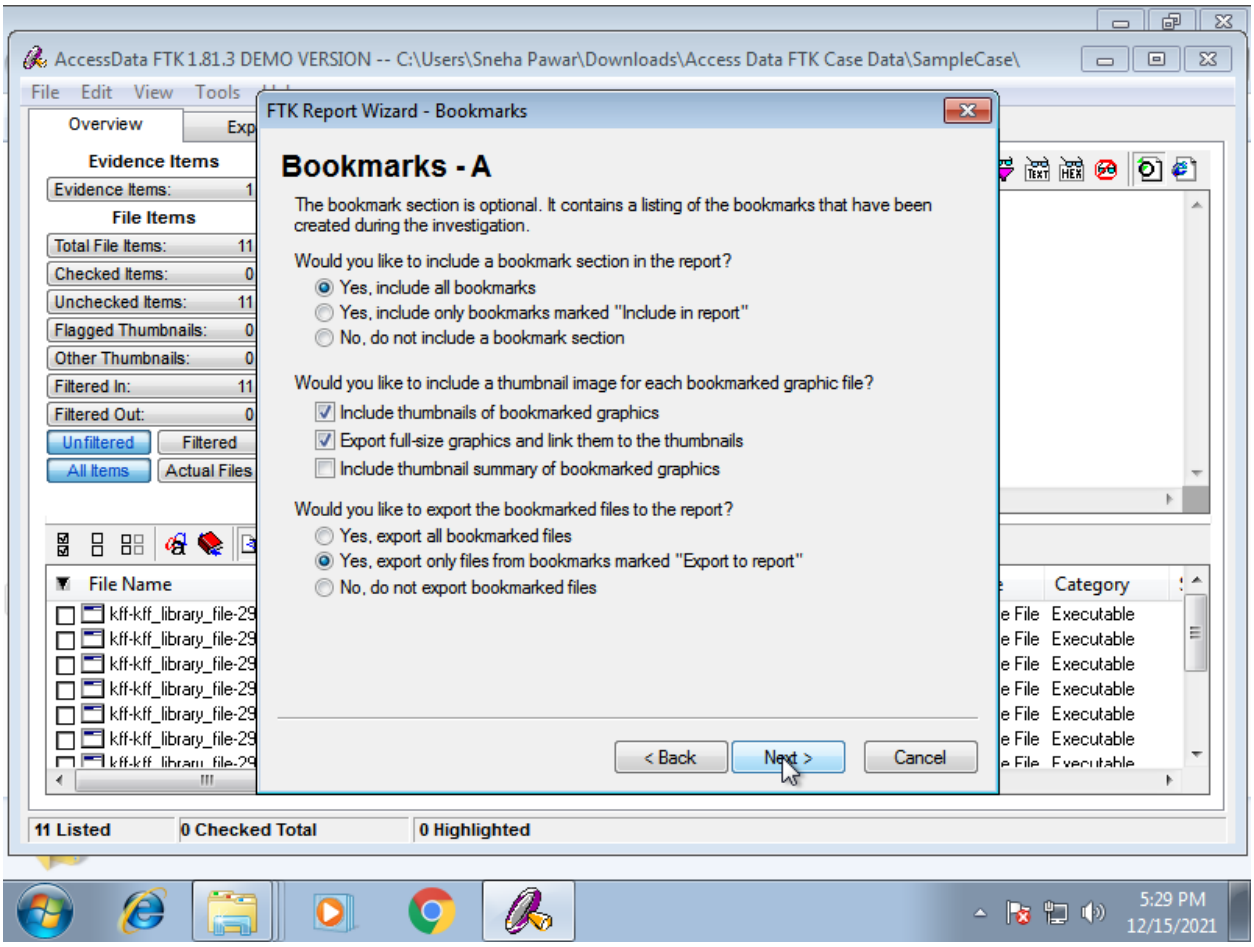


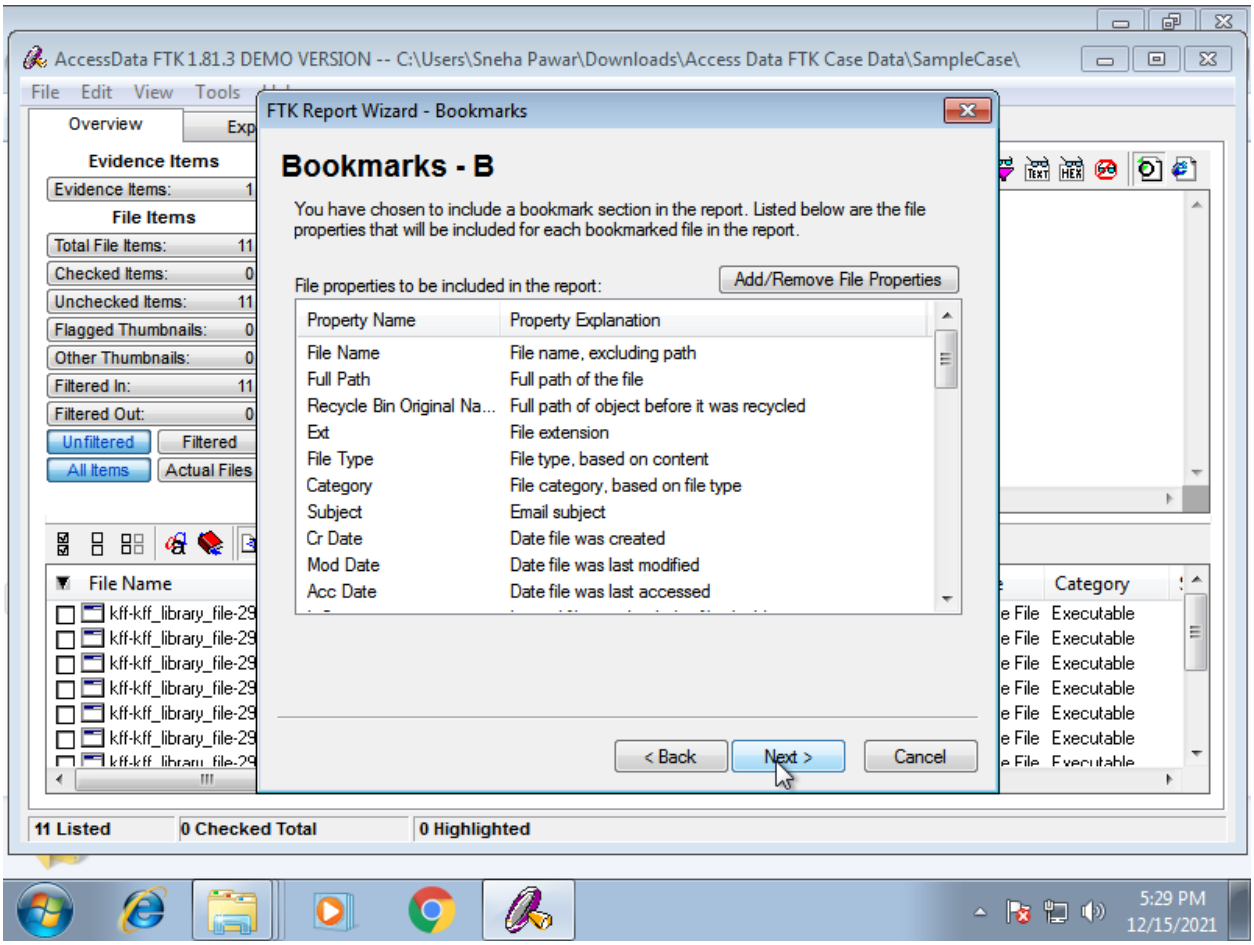


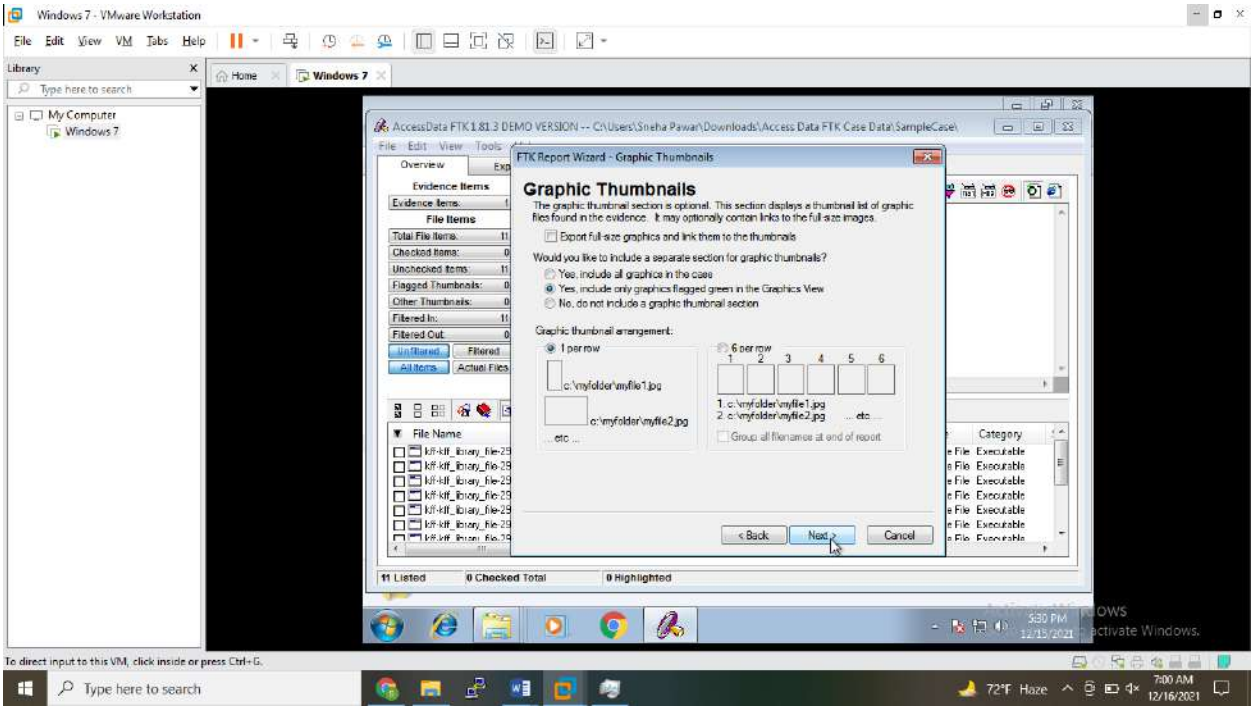
Then click on File - Report Wizard.

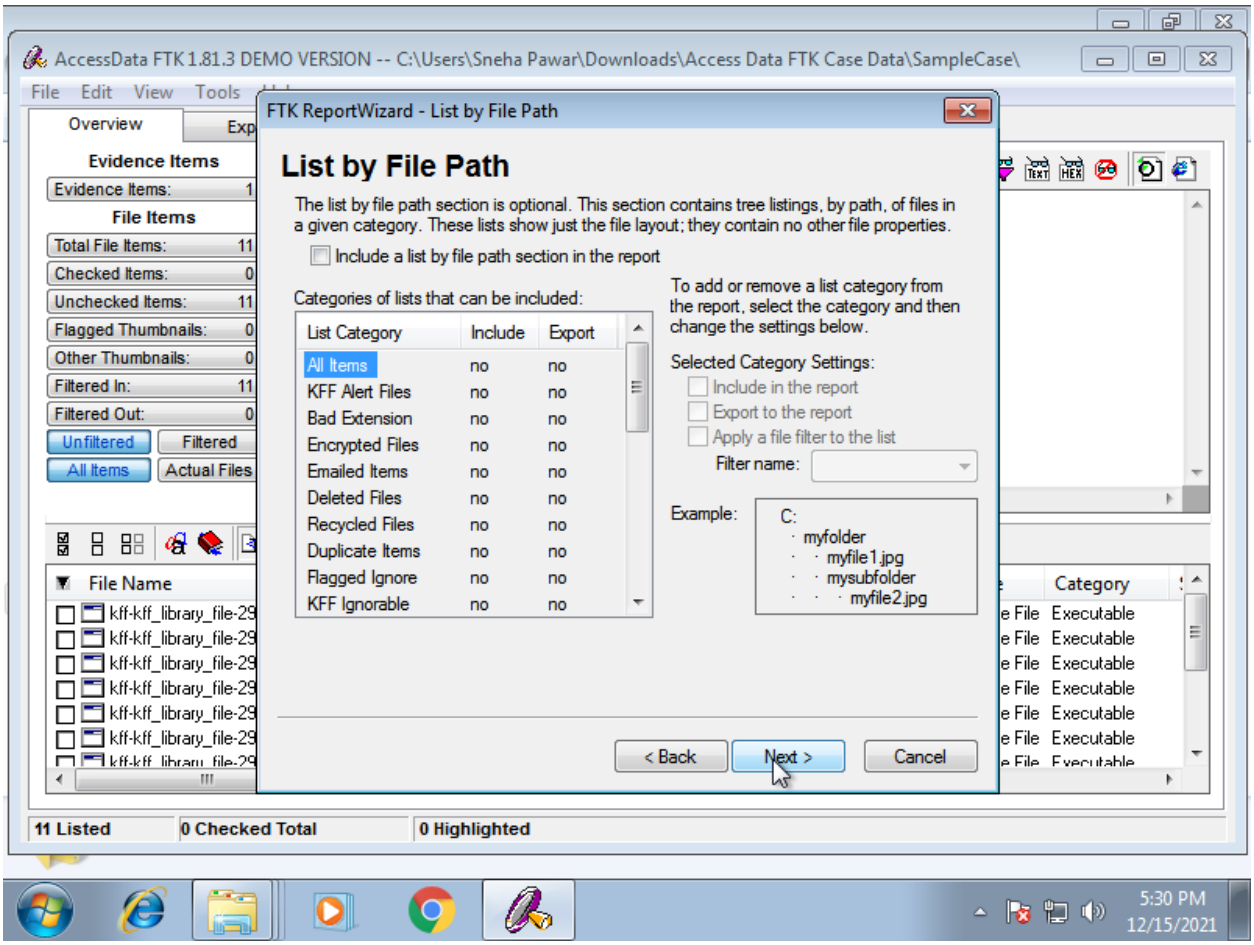
Fill the details. And click on Next.

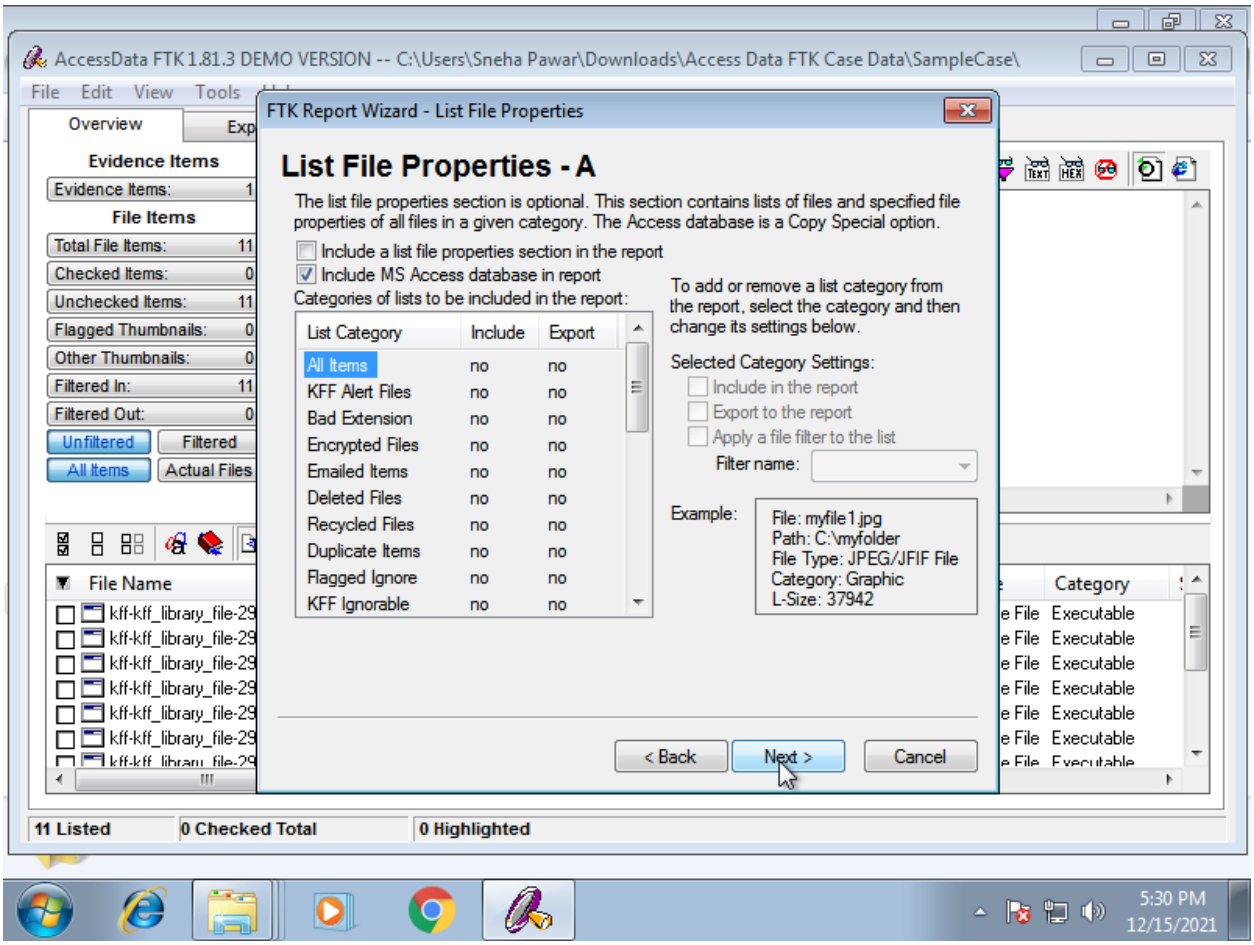

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools
Overview
Evidence Items
File Items
FTK Report Wizard - Case Information
Case Information
The following information will appear on the Case Information page of the report:
Include Investigator Information in report
Agency/Company: RJ College
Investigator's Name: Sneha Pawar
Address: 601/6, Bharat Nagar
Phone: 9827364537
Fax: 0203
E-Mail: sneharamchandrapawar@gmail.com
Comments: Ok
Next >
Cancel
11 Listed
0 Checked Total
0 Highlighted
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
72°F Haze
6:58 AM
12/16/2021

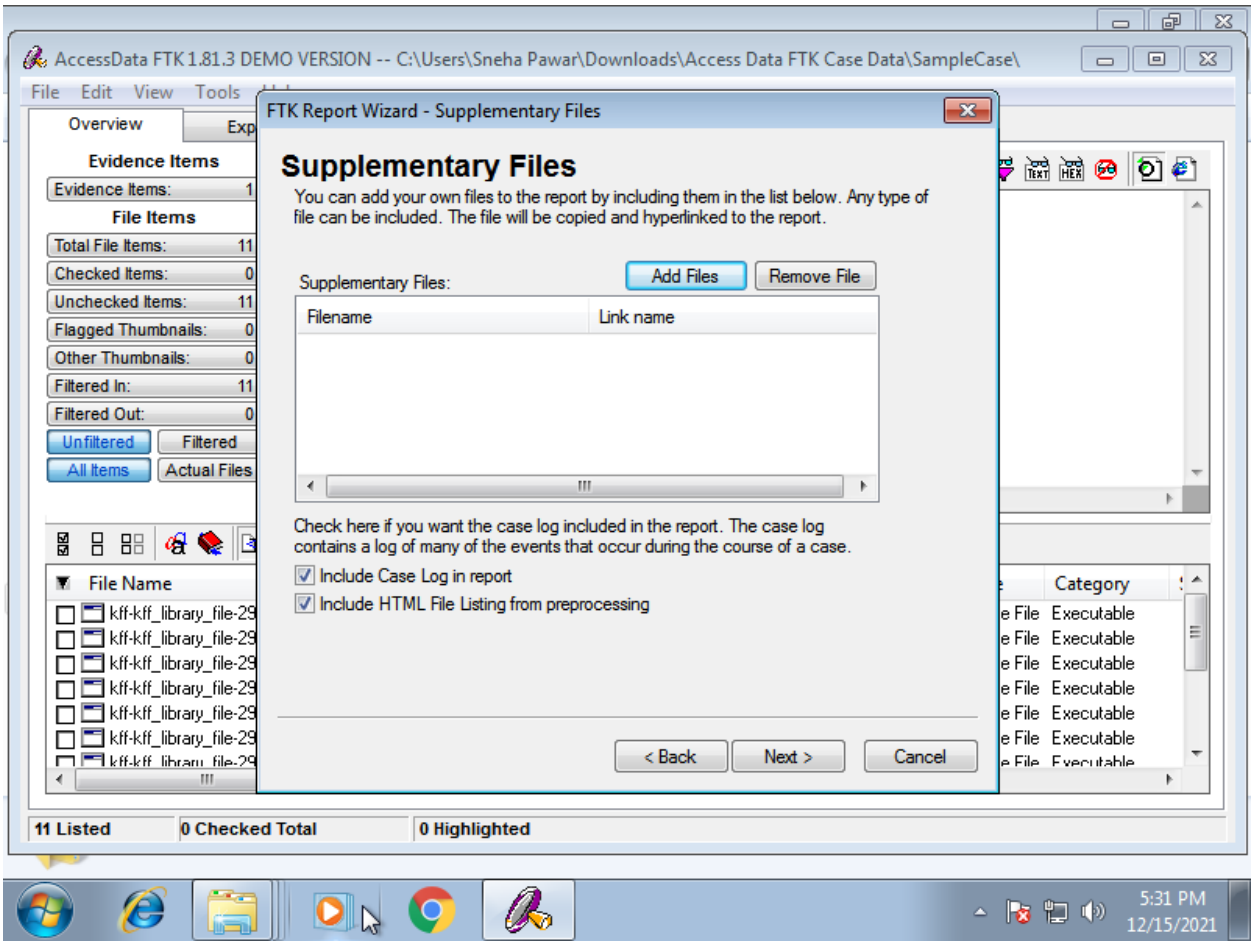

AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools
Overview
Evidence Items
Evidence Items: 1
File Items
Total File Items: 11
Checked Items: 0
Unchecked Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 11
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
File Name
Category
FTK Report Wizard - Bookmarks
Bookmarks - A
The bookmark section is optional. It contains a listing of the bookmarks that have been created during the investigation.
Would you like to include a bookmark section in the report?
Yes, include all bookmarks
Yes, include only bookmarks marked "Include in report"
No, do not include a bookmark section
Would you like to include a thumbnail image for each bookmarked graphic file?
Include thumbnails of bookmarked graphics
Export full-size graphics and link them to the thumbnails
Include thumbnail summary of bookmarked graphics
Would you like to export the bookmarked files to the report?
Yes, export all bookmarked files
Yes, export only files from bookmarks marked "Export to report"
No, do not export bookmarked files
< Back
Next >
Cancel
11 Listed
0 Checked Total
0 Highlighted
5:29 PM
12/15/2021


AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools
Overview
Evidence Items
Evidence Items: 1
File Items
Total File Items: 11
Checked Items: 0
Unchecked Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 11
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
File Name
kff-kff_library_file-29
FTK Report Wizard - Bookmarks
Bookmarks - B
You have chosen to include a bookmark section in the report. Listed below are the file properties that will be included for each bookmarked file in the report.
File properties to be included in the report:
Add/Remove File Properties
Property Name
Property Explanation
File Name
File name, excluding path
Full Path
Full path of the file
Recycle Bin Original Na...
Full path of object before it was recycled
Ext
File extension
File Type
File type, based on content
Category
File category, based on file type
Subject
Email subject
Cr Date
Date file was created
Mod Date
Date file was last modified
Acc Date
Date file was last accessed
< Back
Next >
Cancel
Category
e File Executable
11 Listed
0 Checked Total
0 Highlighted
5:29 PM
12/15/2021

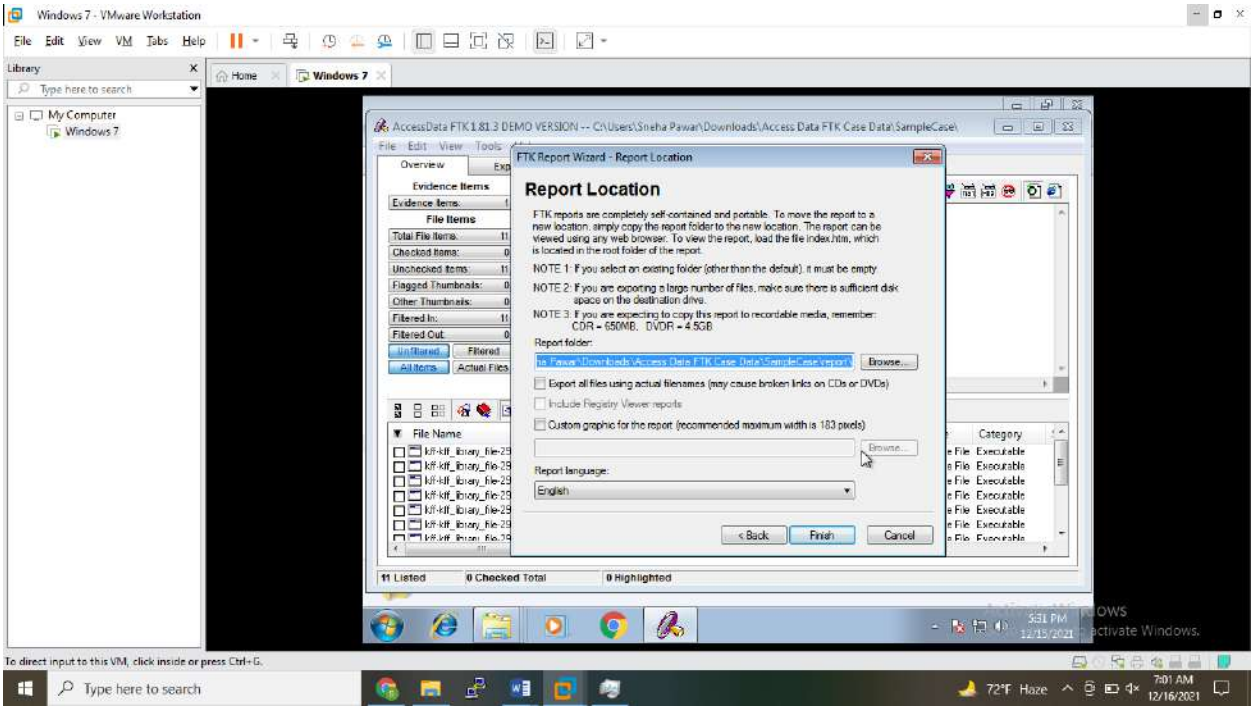

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
FTK Report Wizard - Graphic Thumbnails
Graphic Thumbnails
The graphic thumbnail section is optional. This section displays a thumbnail list of graphic files found in the evidence. It may optionally contain links to the full-size images.
Export full-size graphics and link them to the thumbnails
Would you like to include a separate section for graphic thumbnails?
Yes, include all graphics in the case
Yes, include only graphics flagged green in the Graphics View
No, do not include a graphic thumbnail section
Graphic thumbnail arrangement:
1 per row
6 per row
c:\myfolder\myfile1.jpg
c:\myfolder\myfile2.jpg
Group all filenames at end of report
< Back
Next >
Cancel
11 Listed
0 Checked Total
0 Highlighted
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
72°F Haze
7:00 AM
12/16/2021

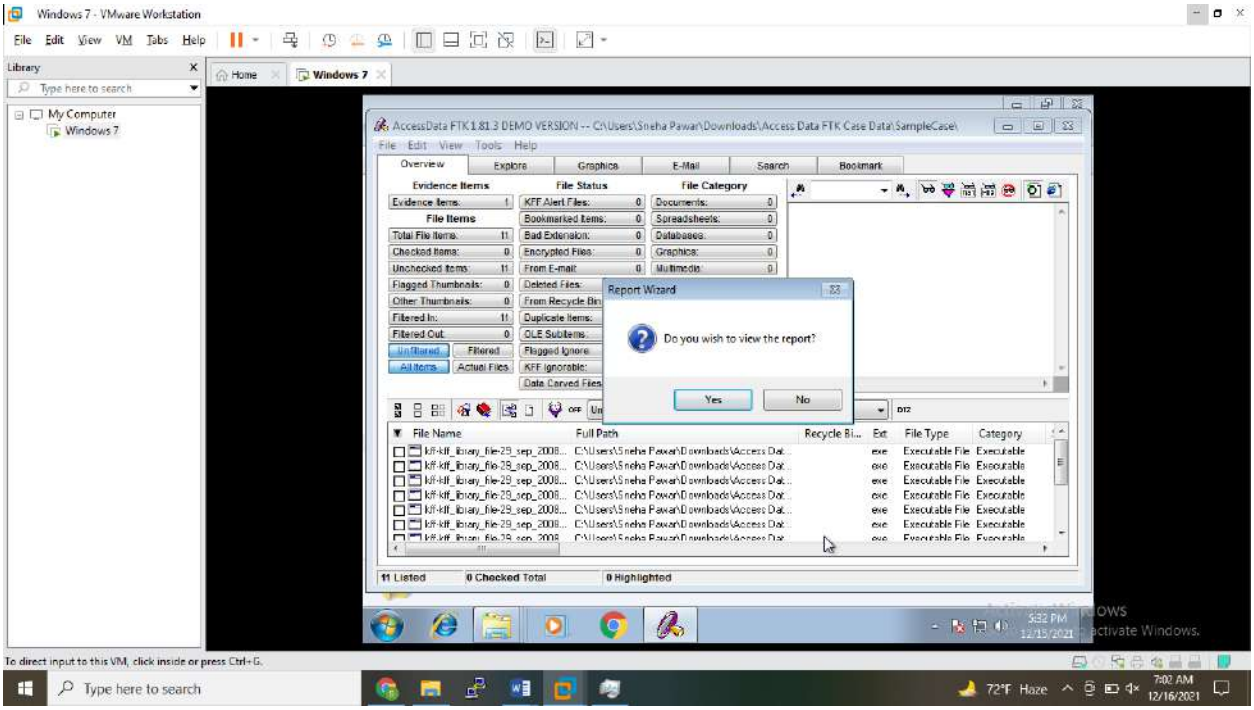

AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools
Overview
Evidence Items
Evidence Items: 1
File Items
Total File Items: 11
Checked Items: 0
Unchecked Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 11
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
File Name
FTK ReportWizard - List by File Path
List by File Path
The list by file path section is optional. This section contains tree listings, by path, of files in a given category. These lists show just the file layout; they contain no other file properties.
Include a list by file path section in the report
Categories of lists that can be included:
List Category | Include | Export
All Items no no
KFF Alert Files no no
Bad Extension no no
Encrypted Files no no
Emailed Items no no
Deleted Files no no
Recycled Files no no
Duplicate Items no no
Flagged Ignore no no
KFF Ignorable no no
To add or remove a list category from the report, select the category and then change the settings below.
Selected Category Settings:
Include in the report
Export to the report
Apply a file filter to the list
Filter name:
Example:
C:
myfolder
myfile1.jpg
mysubfolder
myfile2.jpg
< Back
Next >
Cancel
Category
e File Executable
11 Listed
0 Checked Total
0 Highlighted
5:30 PM
12/15/2021

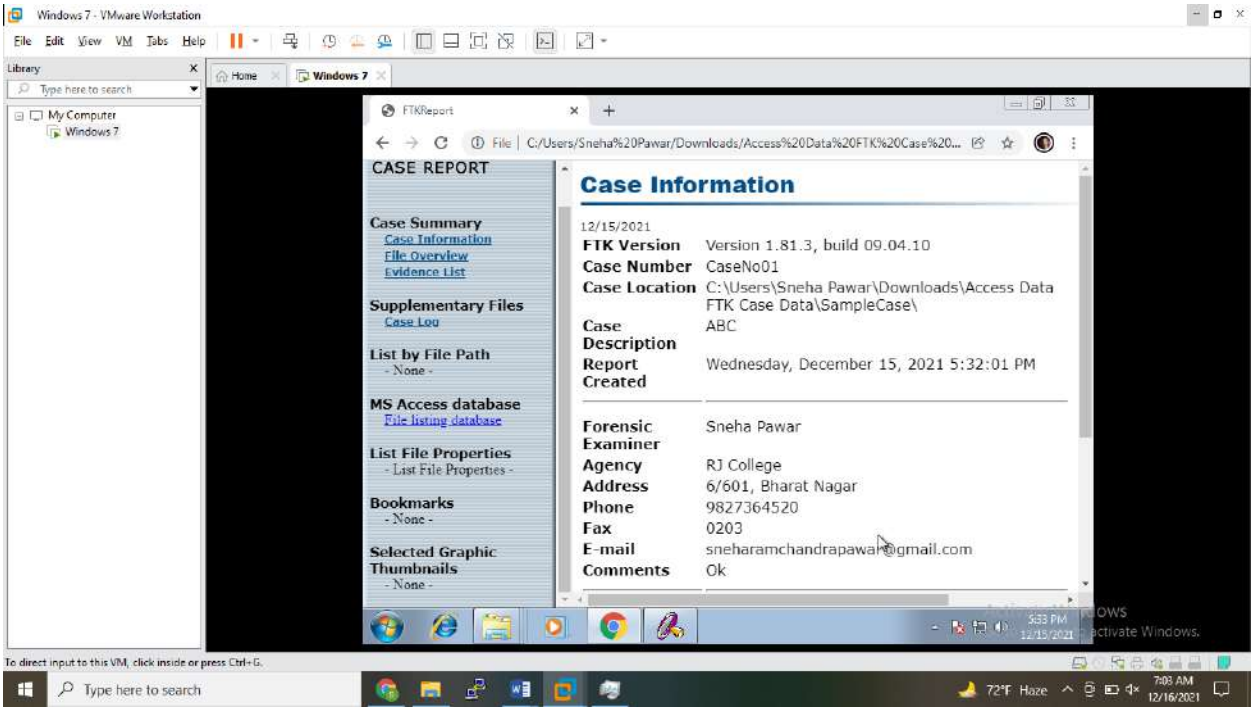

AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools
Overview
Evidence Items
Evidence Items: 1
File Items
Total File Items: 11
Checked Items: 0
Unchecked Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 11
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
File Name
Category
Executable
FTK Report Wizard - List File Properties
List File Properties - A
The list file properties section is optional. This section contains lists of files and specified file properties of all files in a given category. The Access database is a Copy Special option.
Include a list file properties section in the report
Include MS Access database in report
Categories of lists to be included in the report:
List Category
Include
Export
All Items no no
KFF Alert Files no no
Bad Extension no no
Encrypted Files no no
Emailed Items no no
Deleted Files no no
Recycled Files no no
Duplicate Items no no
Flagged Ignore no no
KFF Ignorable no no
To add or remove a list category from the report, select the category and then change its settings below.
Selected Category Settings:
Include in the report
Export to the report
Apply a file filter to the list
Filter name:
Example:
File: myfile1.jpg
Path: C:\myfolder
File Type: JPEG/JFIF File
Category: Graphic
L-Size: 37942
< Back
Next >
Cancel
11 Listed
0 Checked Total
0 Highlighted
5:30 PM
12/15/2021

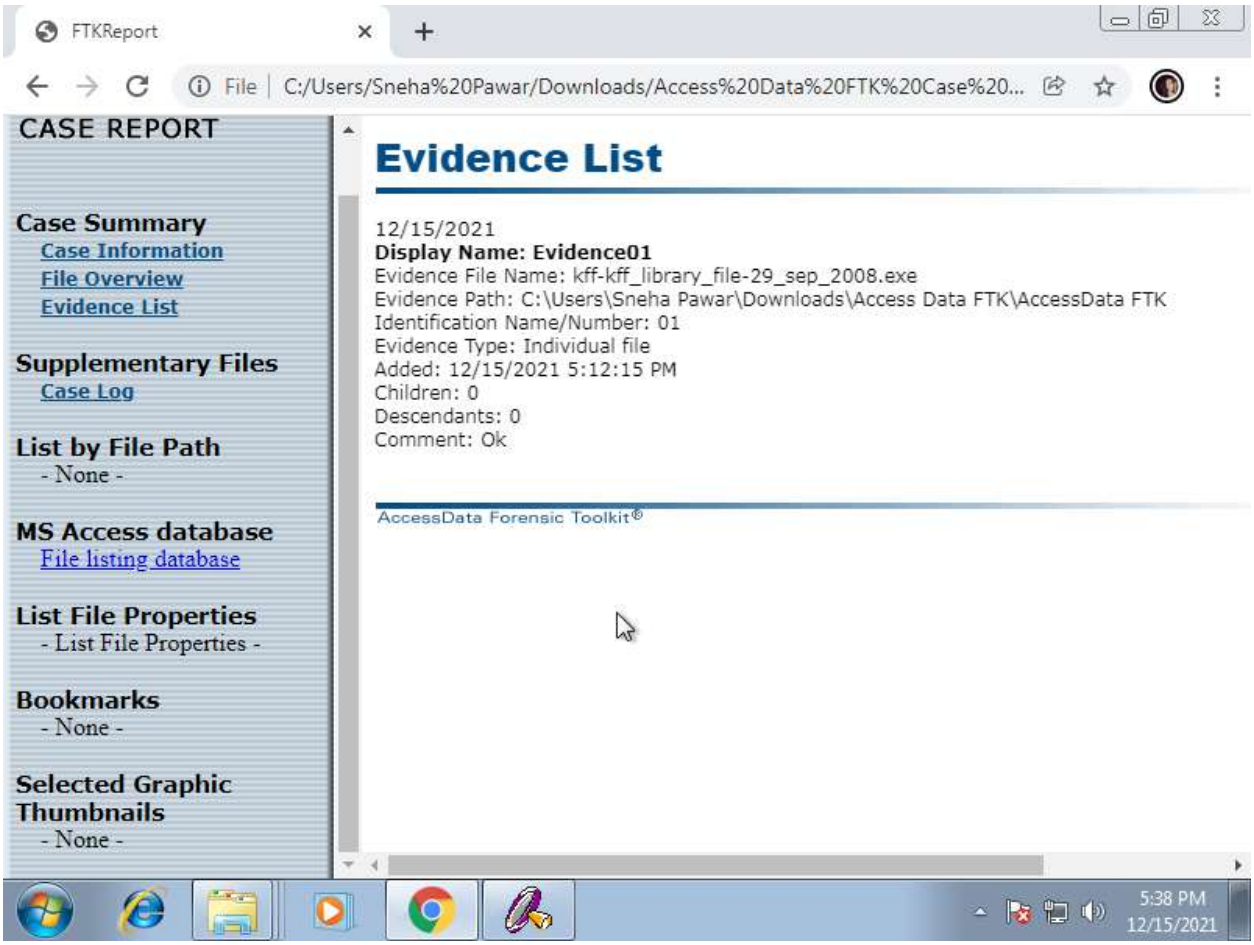


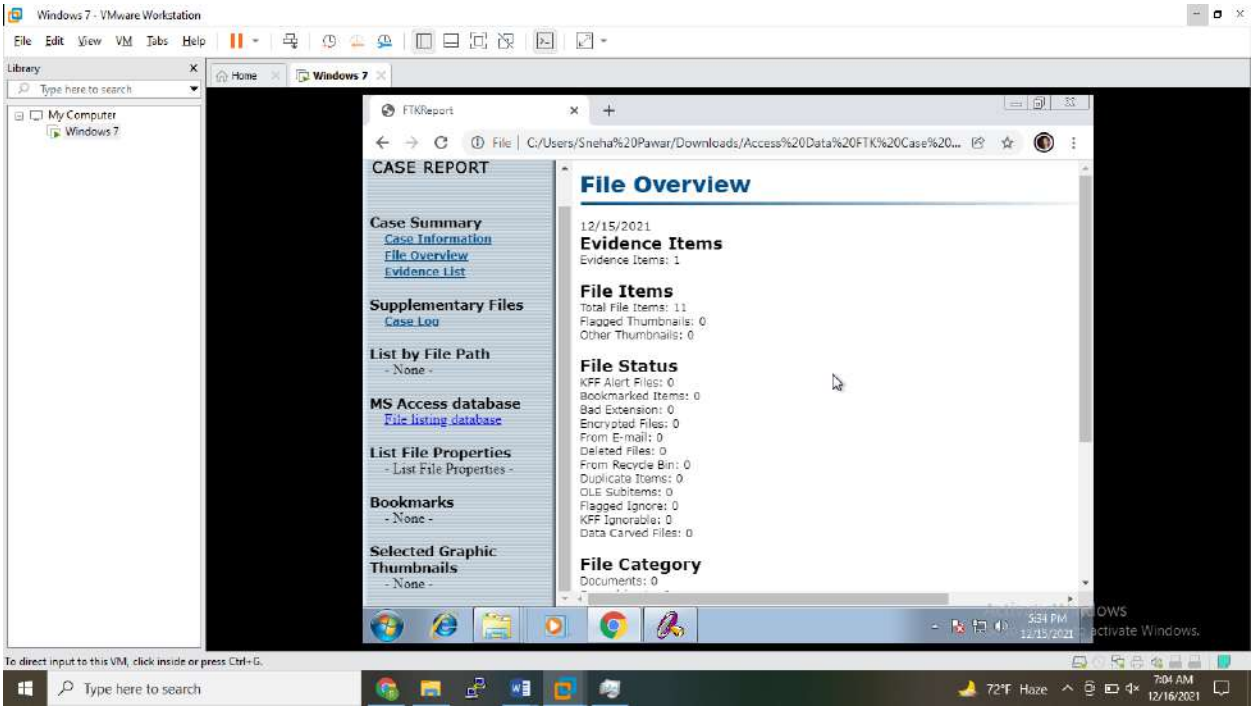
Enter report location.

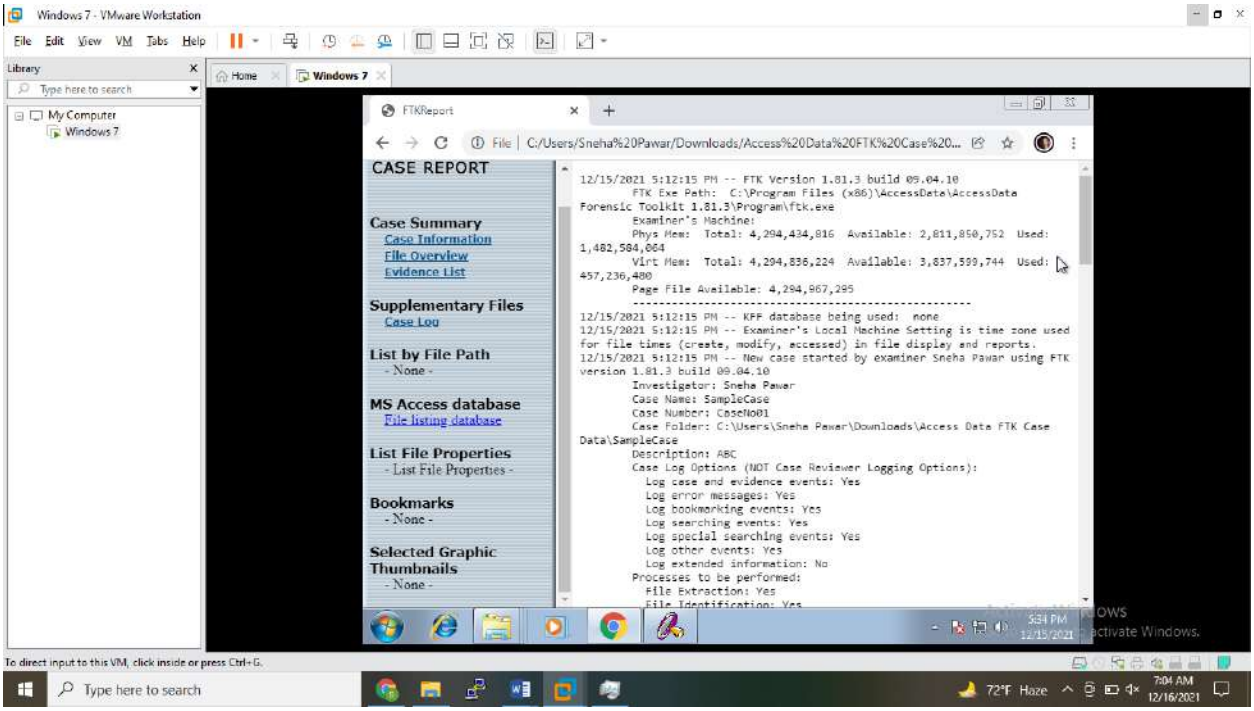



Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Evidence Items
File Status
File Category
Report Wizard
Do you wish to view the report?
Yes
No
File Name
Full Path
Recycle Bi...
Ext
File Type
Category
11 Listed
0 Checked Total
0 Highlighted
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
72°F Haze
7:02 AM
12/16/2021

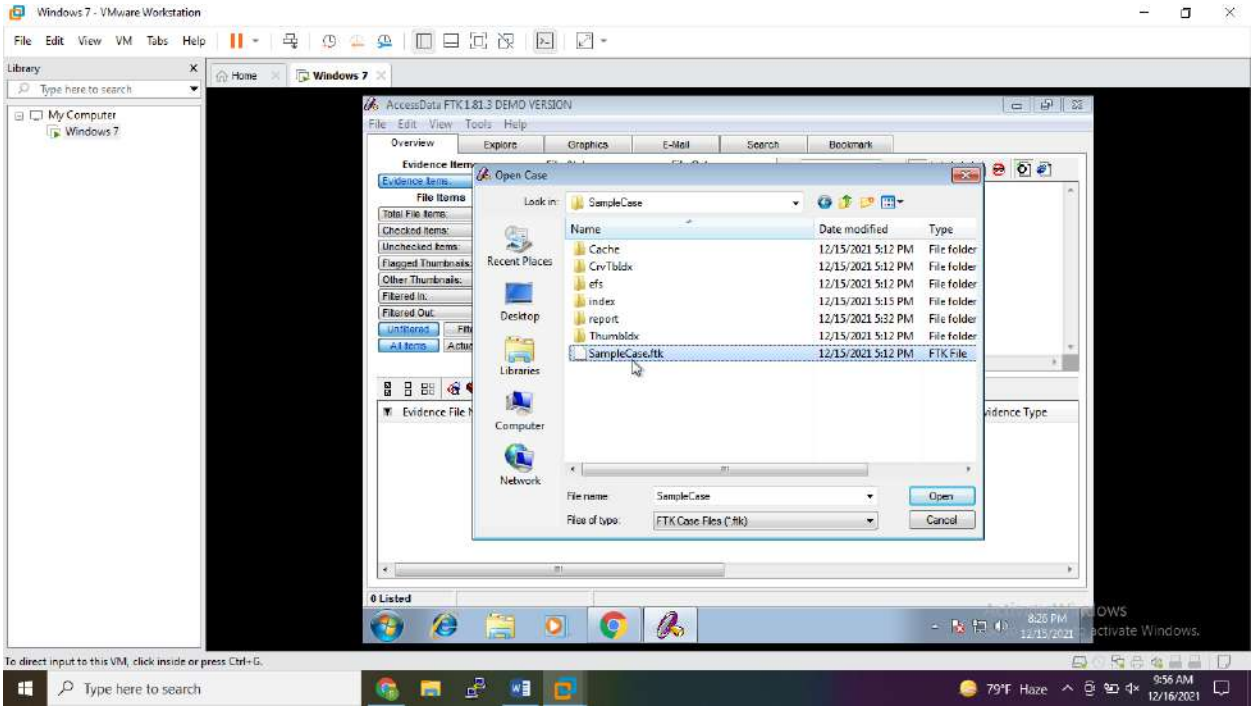

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
FTKReport
File | C:/Users/Sneha%20Pawar/Downloads/Access%20Data%20FTK%20Case%20...
CASE REPORT
Case Summary
Case Information
File Overview
Evidence List
Supplementary Files
Case Log
List by File Path
- None -
MS Access database
File listing database
List File Properties
- List File Properties -
Bookmarks
- None -
Selected Graphic Thumbnails
- None -
Case Information
12/15/2021
FTK Version Version 1.81.3, build 09.04.10
Case Number CaseNo01
Case Location C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
Case Description ABC
Report Created Wednesday, December 15, 2021 5:32:01 PM
Forensic Examiner Sneha Pawar
Agency RJ College
Address 6/601, Bharat Nagar
Phone 9827364520
Fax 0203
E-mail sneharamchandrapawar@gmail.com
Comments Ok
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
72°F Haze
7:03 AM
12/16/2021


FTKReport
File | C:/Users/Sneha%20Pawar/Downloads/Access%20Data%20FTK%20Case%20...
CASE REPORT
Case Summary
Case Information
File Overview
Evidence List
Supplementary Files
Case Log
List by File Path
- None -
MS Access database
File listing database
List File Properties
- List File Properties -
Bookmarks
- None -
Selected Graphic Thumbnails
- None -
Evidence List
12/15/2021
Display Name: Evidence01
Evidence File Name: kff-kff_library_file-29_sep_2008.exe
Evidence Path: C:\Users\Sneha Pawar\Downloads\Access Data FTK\AccessData FTK
Identification Name/Number: 01
Evidence Type: Individual file
Added: 12/15/2021 5:12:15 PM
Children: 0
Descendants: 0
Comment: Ok
AccessData Forensic Toolkit®
5:38 PM
12/15/2021


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Windows 7
Home
Windows 7
FTKReport
File | C:/Users/Sneha%20Pawar/Downloads/Access%20Data%20FTK%20Case%20...
CASE REPORT
Case Summary
Case Information
File Overview
Evidence List
Supplementary Files
Case Log
List by File Path
- None -
MS Access database
File listing database
List File Properties
- List File Properties -
Bookmarks
- None -
Selected Graphic Thumbnails
- None -
File Overview
12/15/2021
Evidence Items
Evidence Items: 1
File Items
Total File Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
File Status
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 0
Encrypted Files: 0
From E-mail: 0
Deleted Files: 0
From Recycle Bin: 0
Duplicate Items: 0
OLE Subitems: 0
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0
File Category
Documents: 0
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
72°F Haze
7:04 AM
12/16/2021

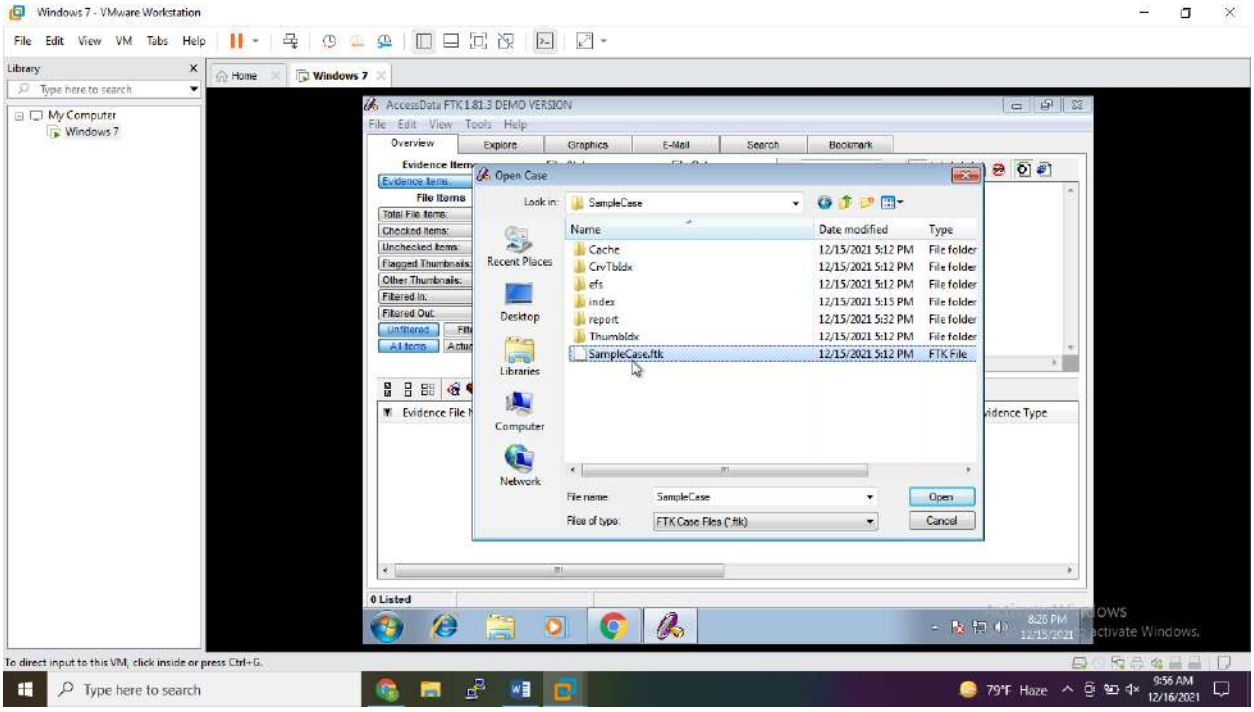


Now, let's perform Email Forensic on this. Open Existing Case that we have created.
File – Open Case

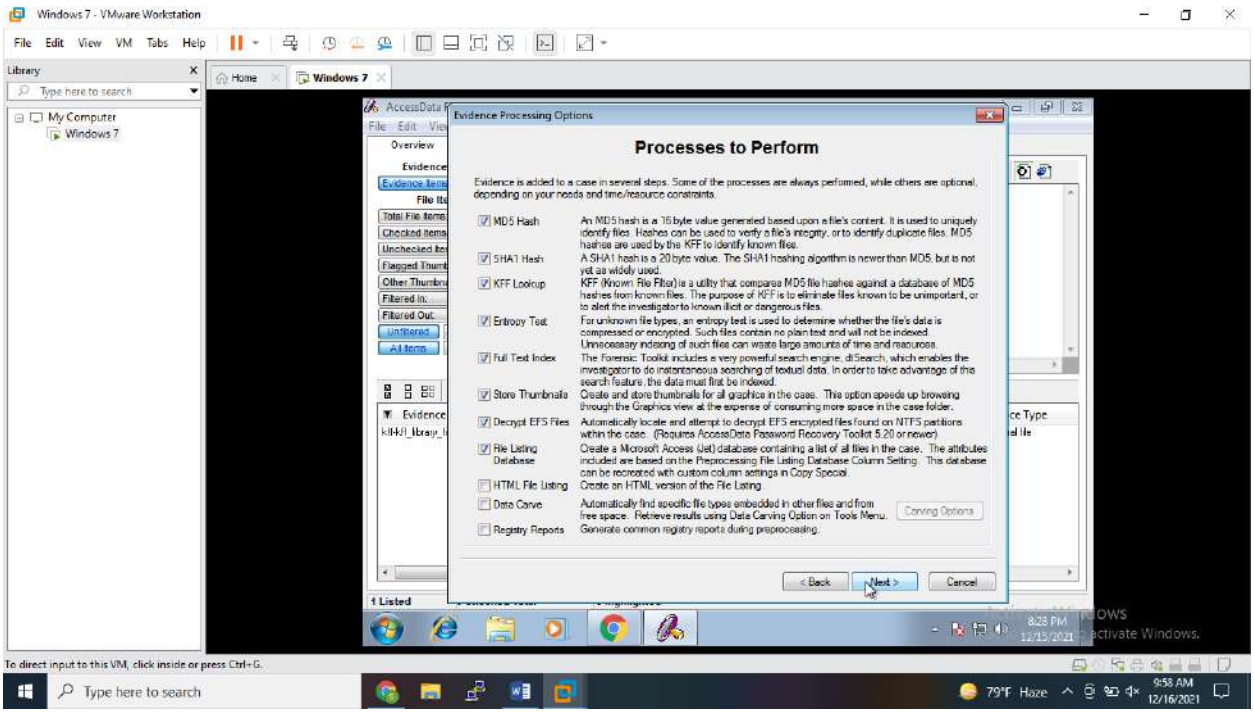


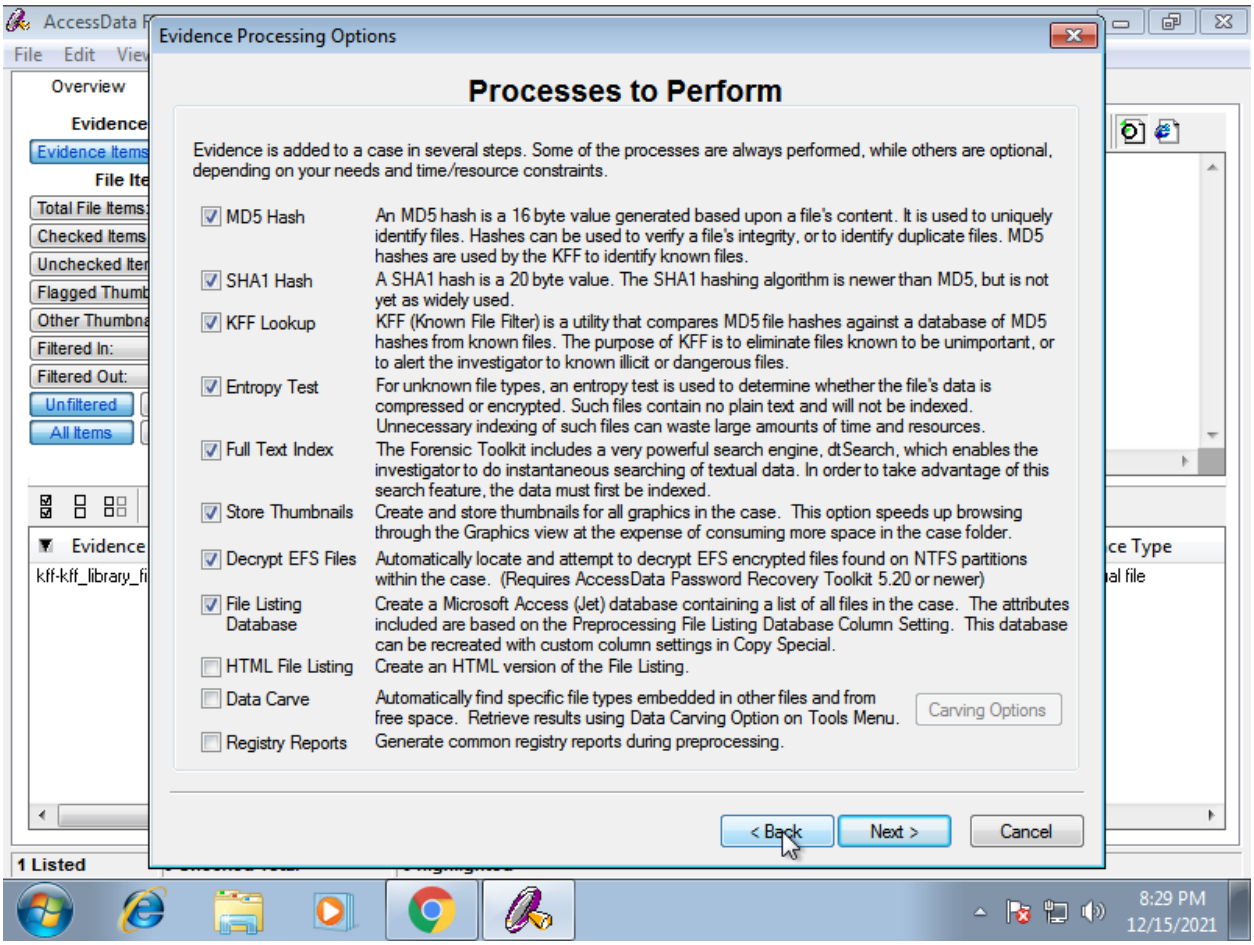
Now File – Add Evidence, and add Outlook's pst file.

Keep this by default.

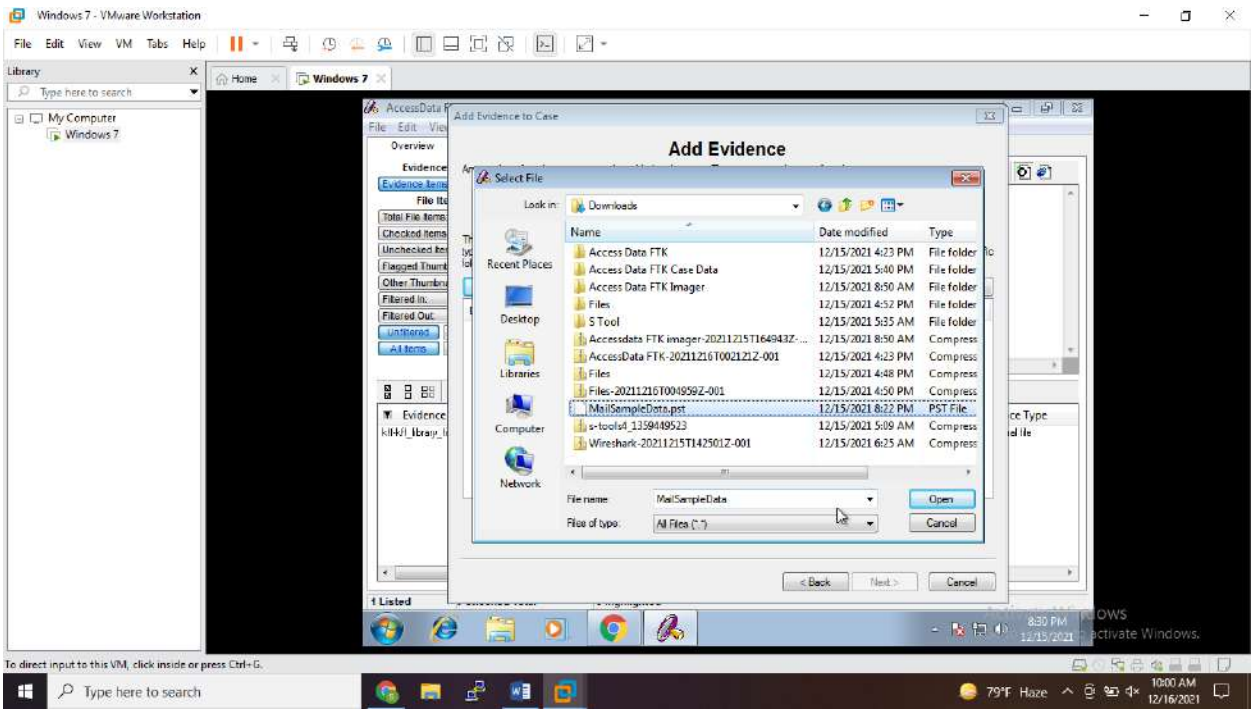


Click Next

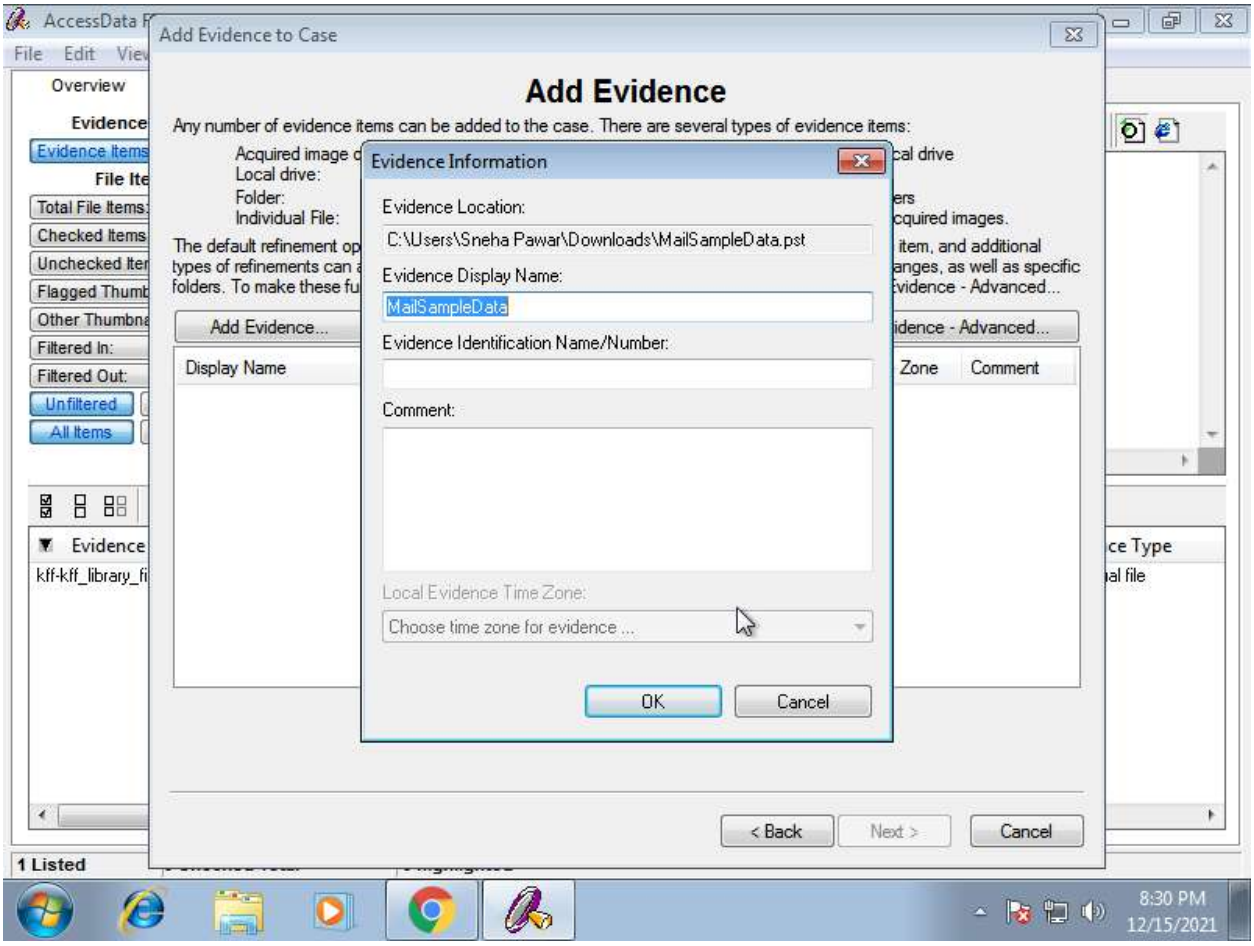


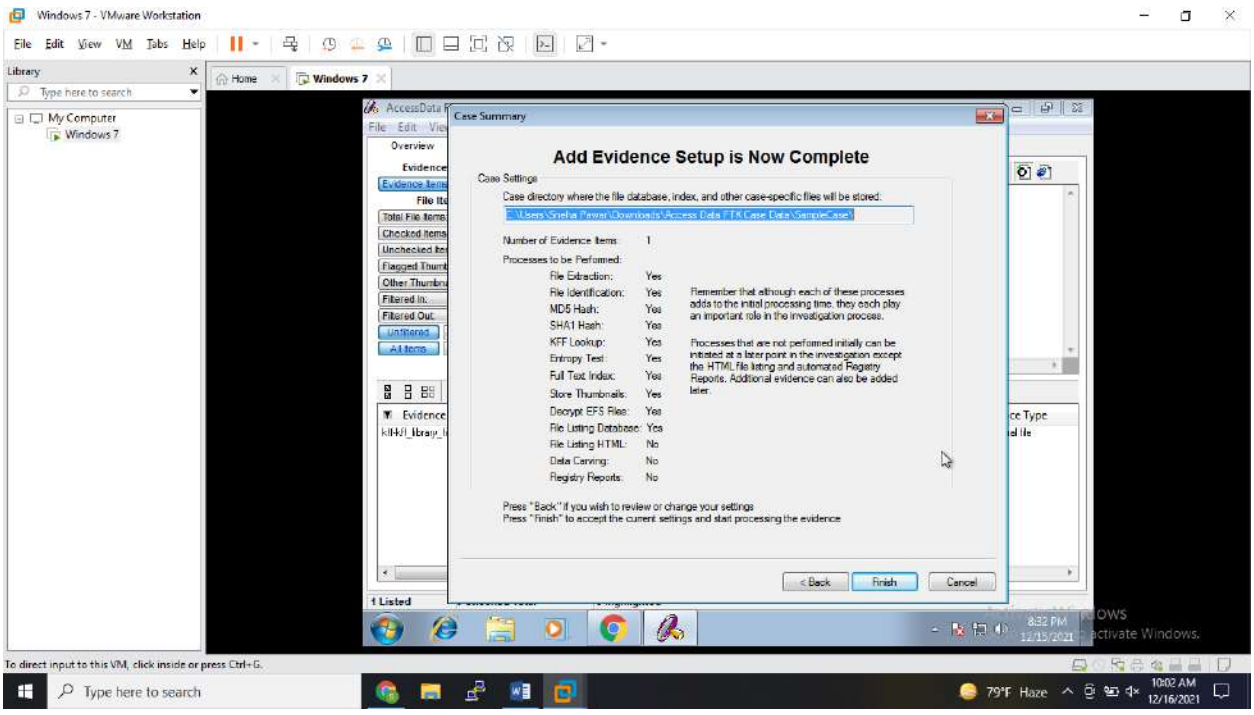


Then Add Evidence – Individual File – Browse location of a pst file.

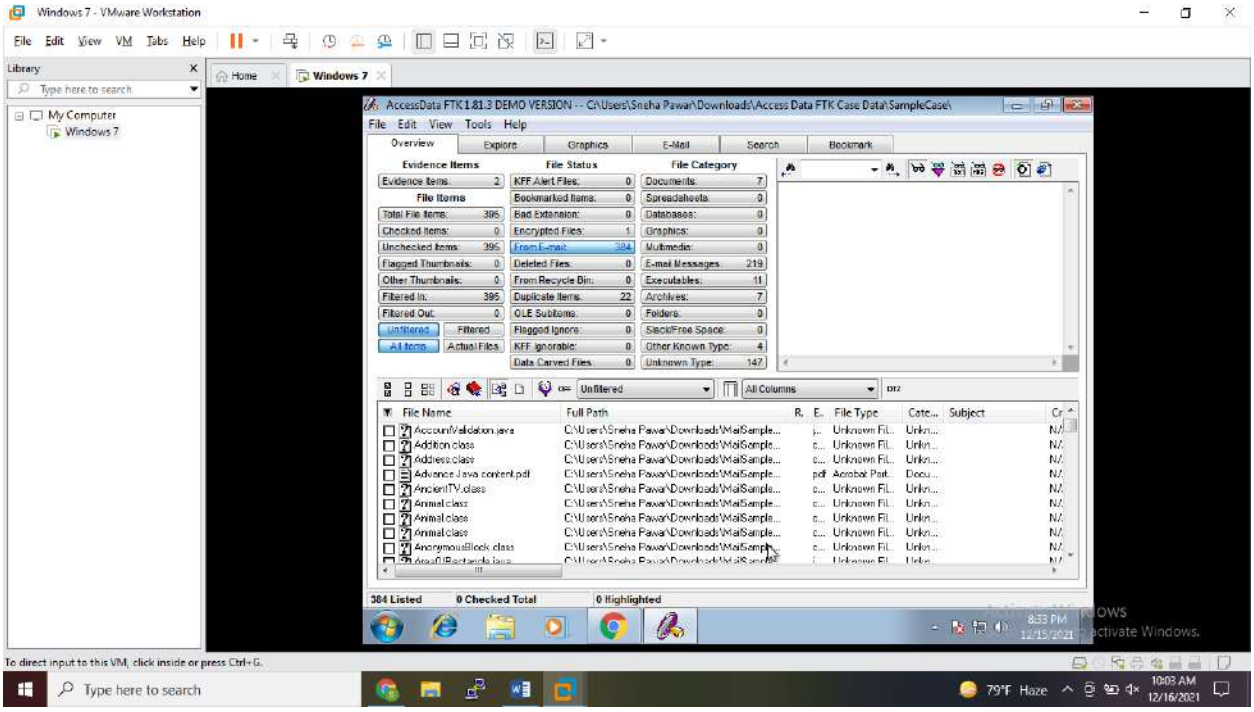


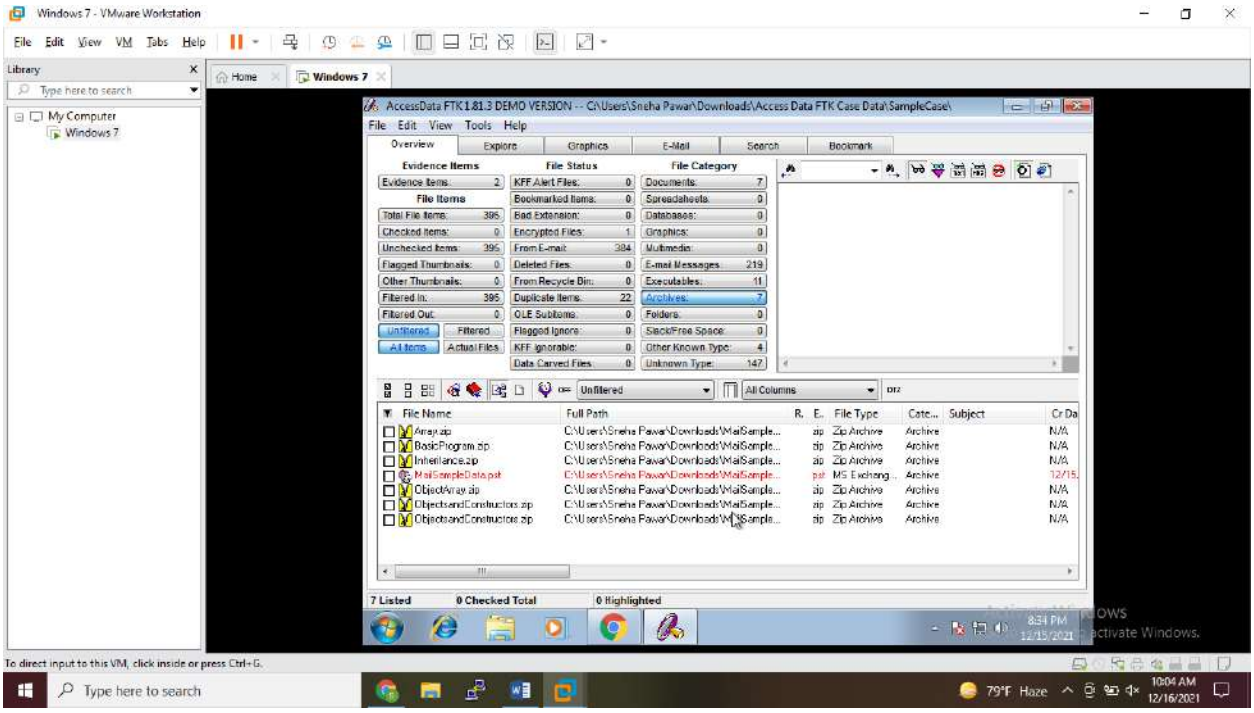
Click on Ok. And then click on Next.

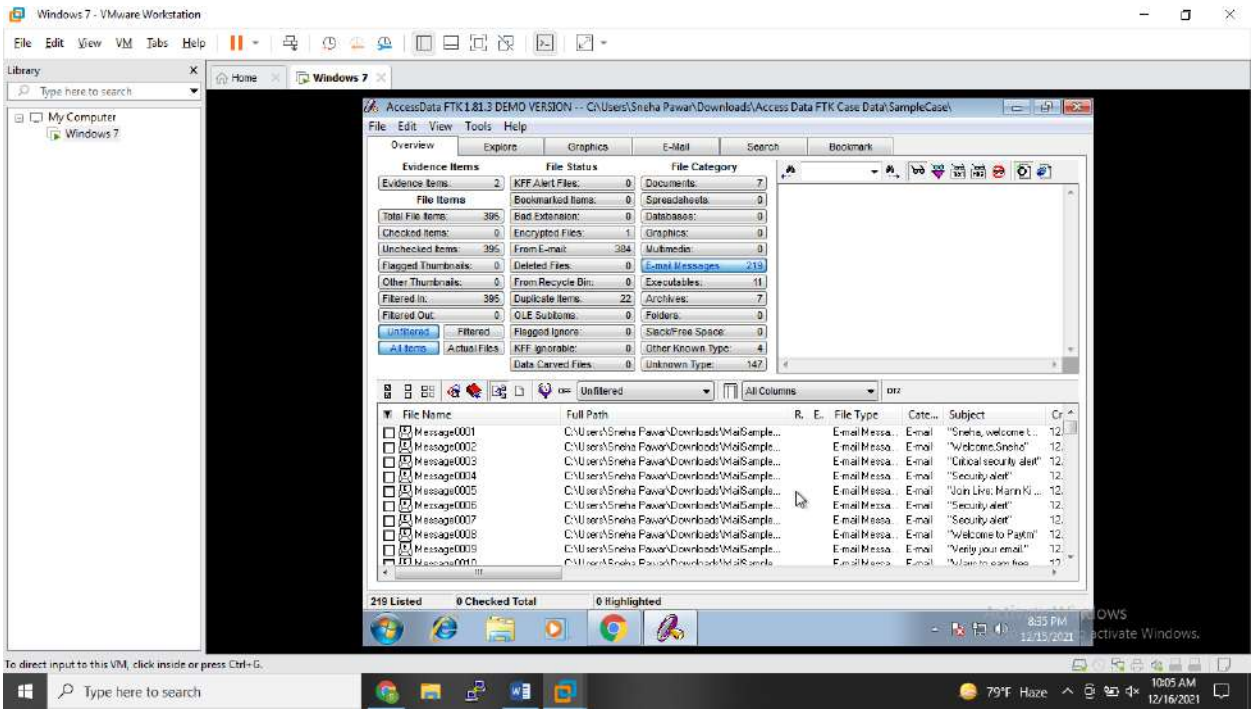




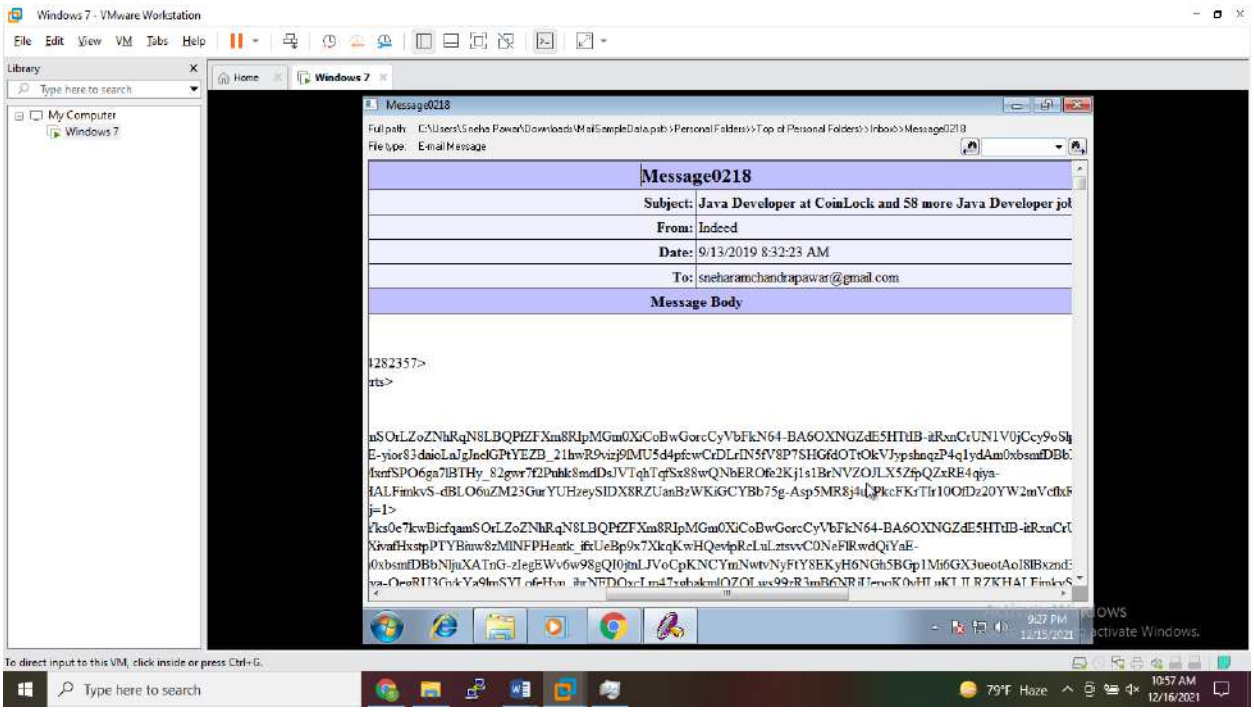
Emails will get acquired as you can see after double clicking on an evidence.





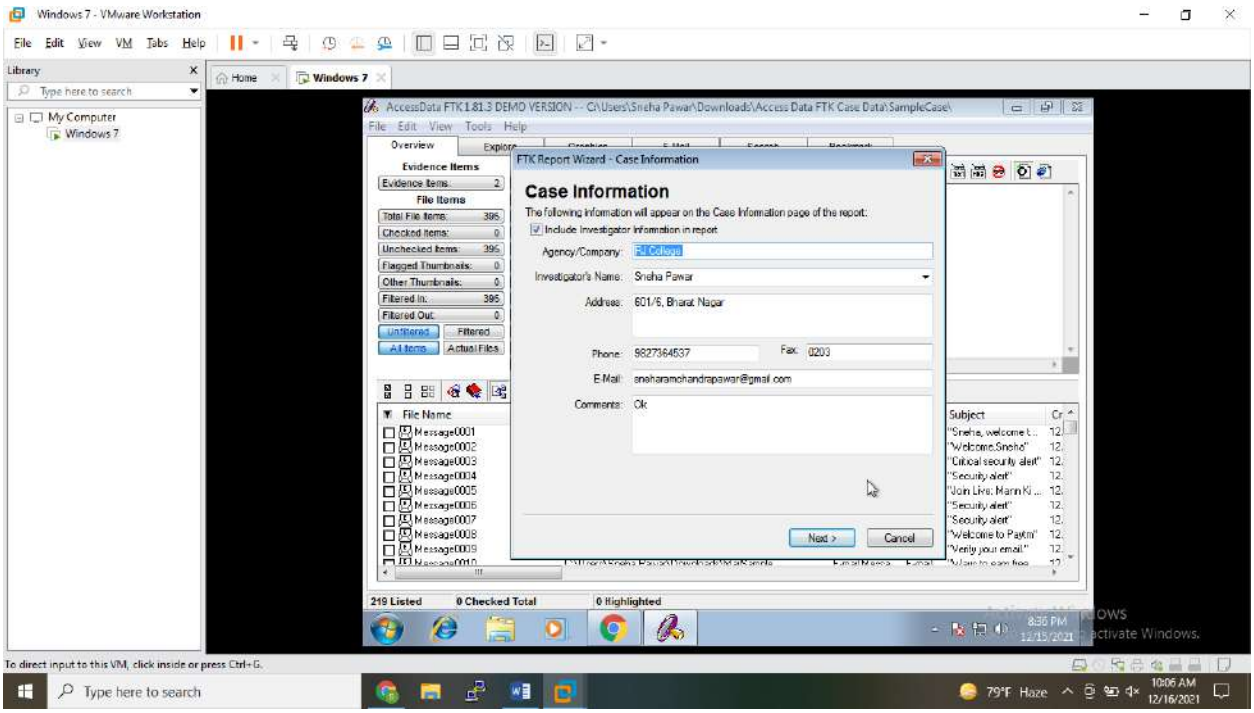


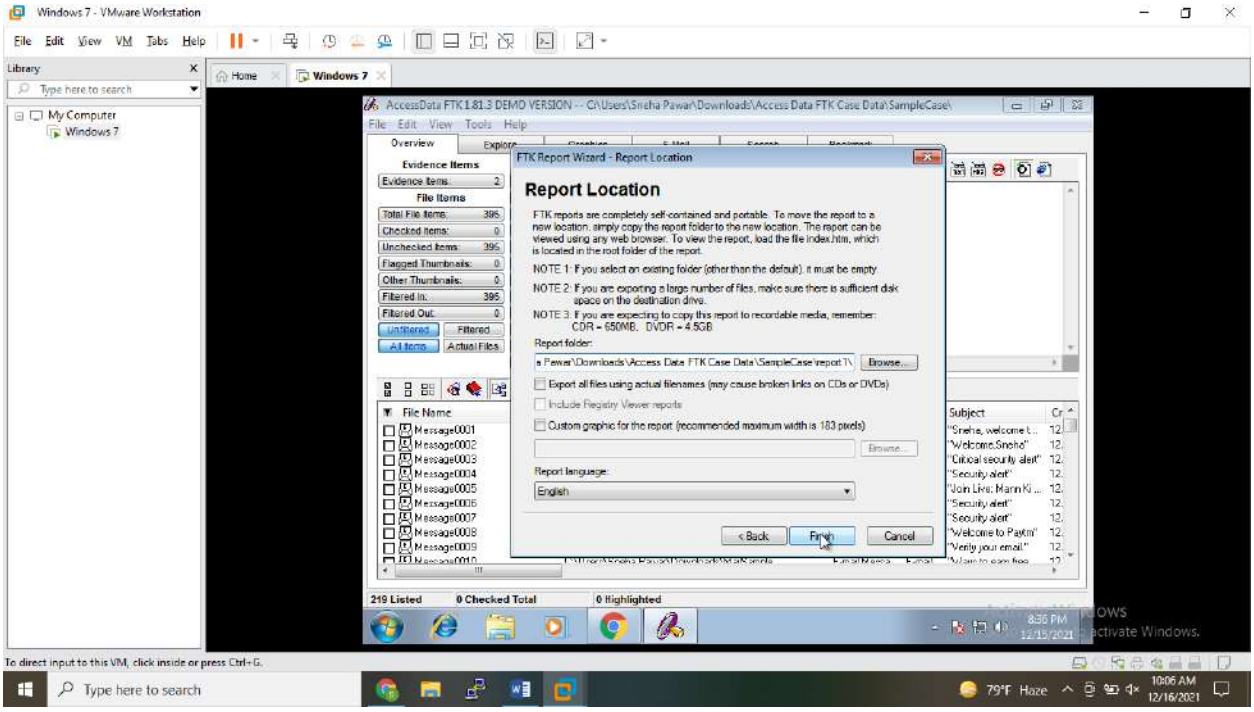
Right click on Mail to see it in Detached view.

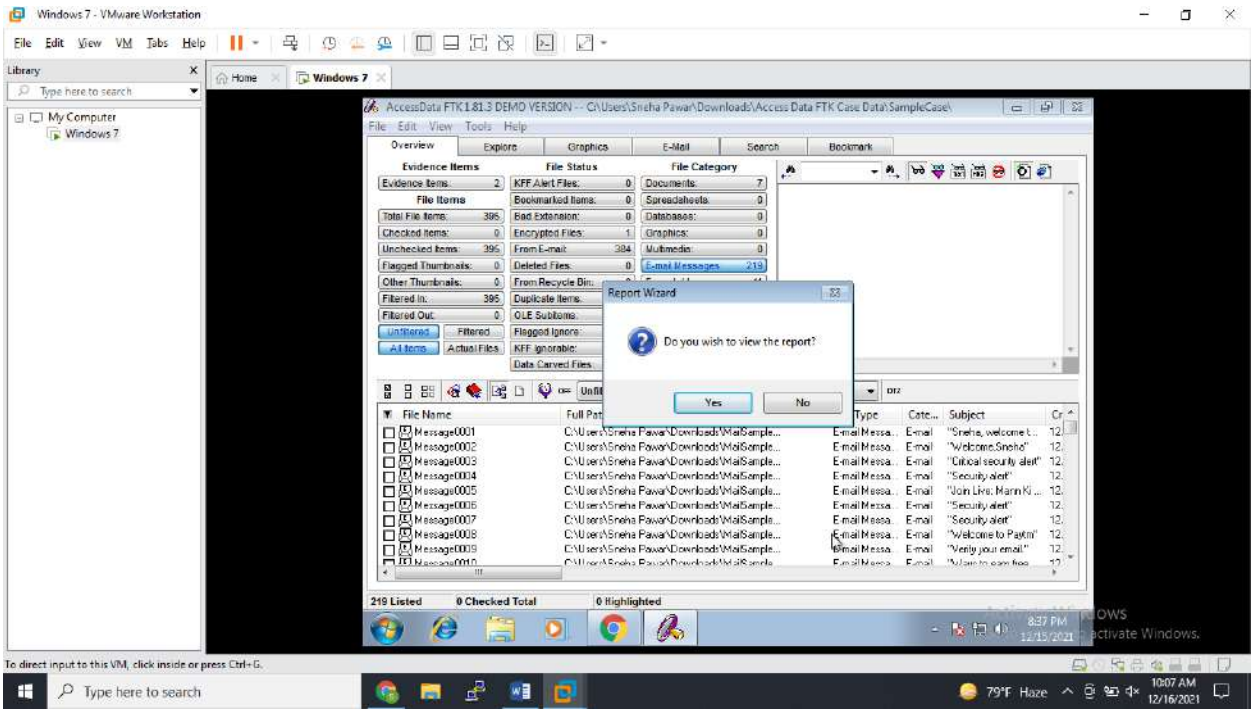


Steps:

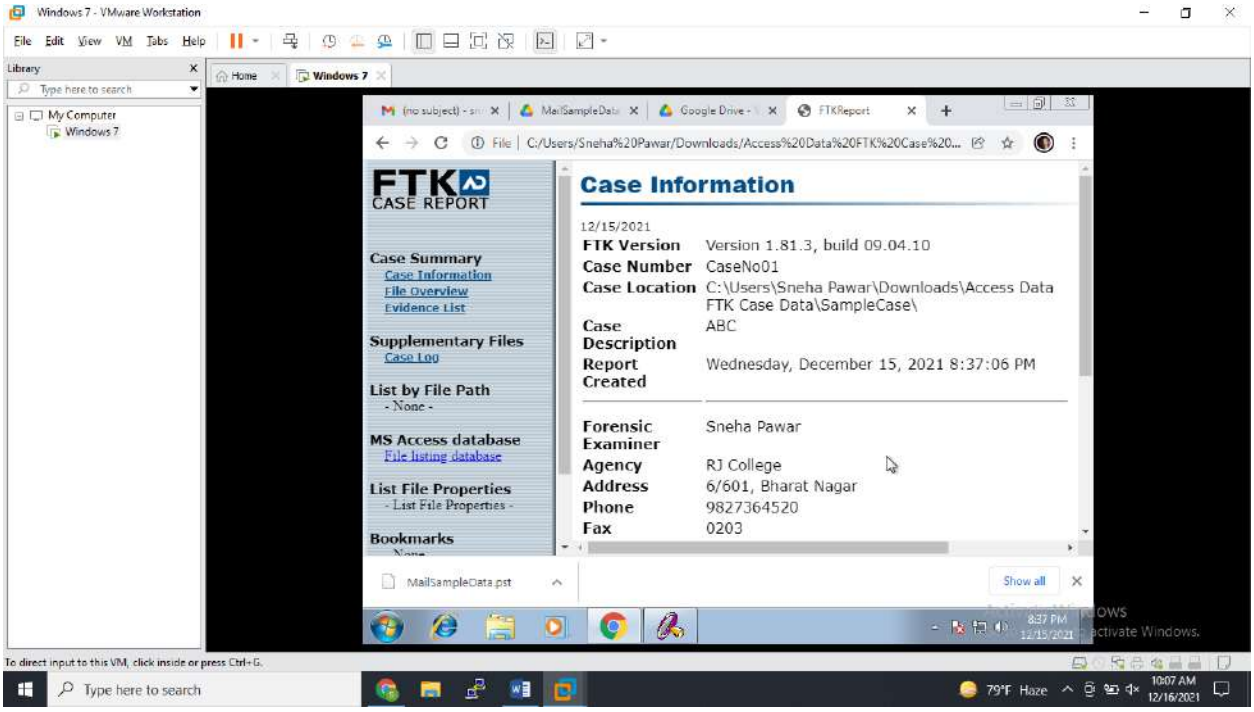
Now click on Report Wizard. And keep options by default and click on Next.

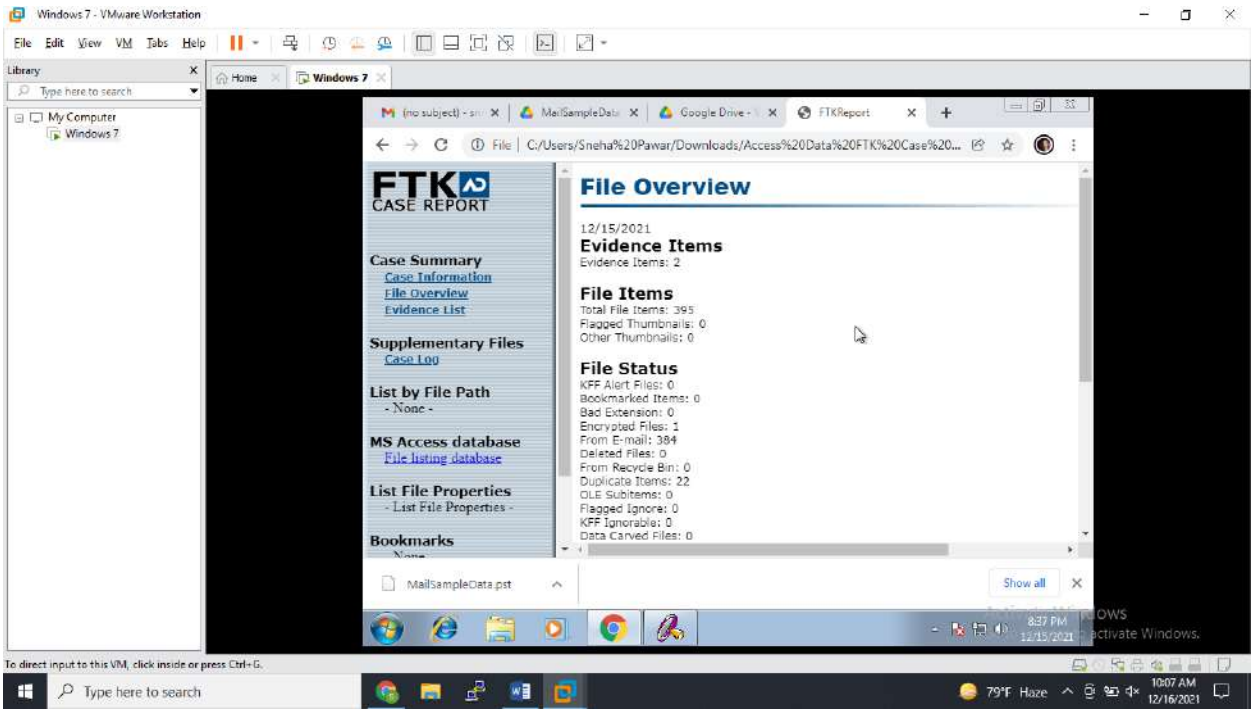

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools Help
Overview
Explore
Evidence Items
Evidence Items: 2
File Items
Total File Items: 395
Checked Items: 0
Unchecked Items: 395
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 395
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
FTK Report Wizard - Case Information
Case Information
The following information will appear on the Case Information page of the report:
Include Investigator information in report
Agency/Company: FC College
Investigator's Name: Sneha Pawar
Address: 601/6, Bharat Nagar
Phone: 9827364537
Fax: 0203
E-Mail: sneharamchandrapawar@gmail.com
Comments: Ok
Next >
Cancel
File Name
Message0001
Message0002
Message0003
Message0004
Message0005
Message0006
Message0007
Message0008
Message0009
Subject
"Sneha, welcome t...
"Welcome,Sneha"
"Critical security alert"
"Security alert"
"Join Live: Mann Ki ...
"Security alert"
"Security alert"
"Welcome to Paytm"
"Verify your email."
219 Listed
0 Checked Total
0 Highlighted
8:36 PM
12/15/2021
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
10:06 AM
12/16/2021

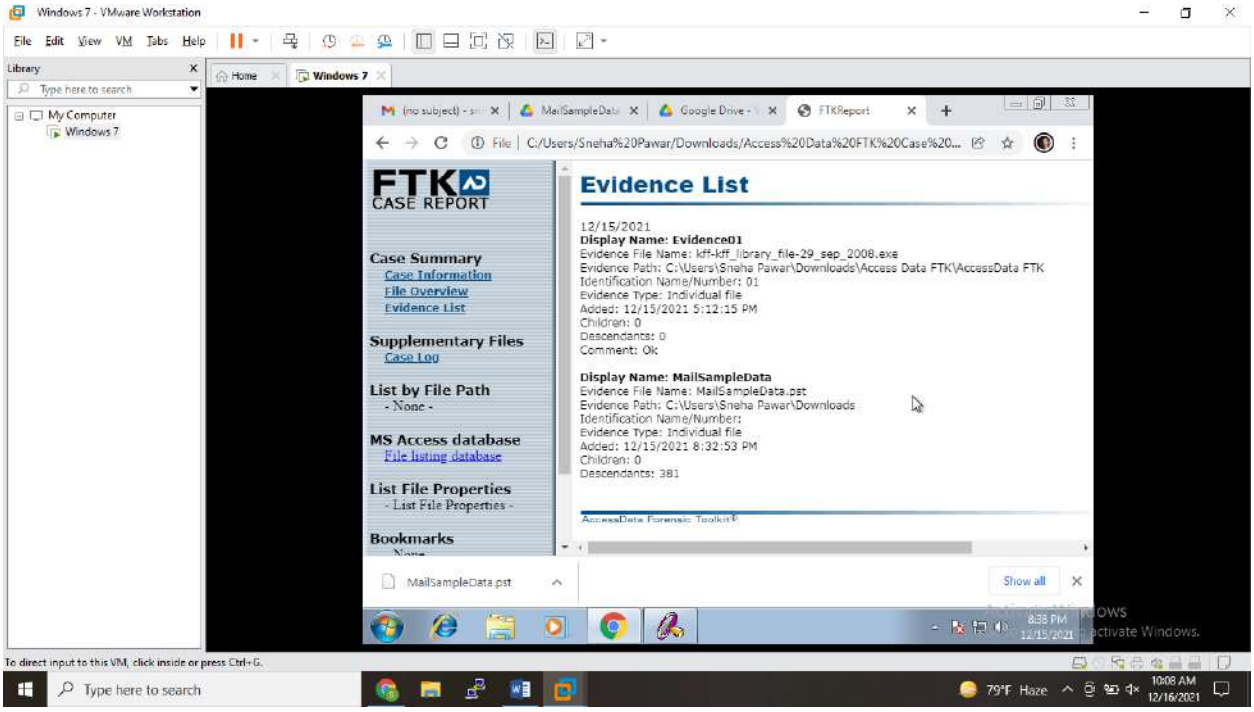

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools Help
Overview
Explore
Evidence Items
Evidence Items: 2
File Items
Total File Items: 395
Checked Items: 0
Unchecked Items: 395
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 395
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
FTK Report Wizard - Report Location
Report Location
FTK reports are completely self-contained and portable. To move the report to a new location, simply copy the report folder to the new location. The report can be viewed using any web browser. To view the report, load the file index.htm, which is located in the root folder of the report.
NOTE 1: If you select an existing folder (other than the default), it must be empty
NOTE 2: If you are exporting a large number of files, make sure there is sufficient disk space on the destination drive.
NOTE 3: If you are expecting to copy this report to recordable media, remember: CDR = 650MB, DVDR = 4.5GB
Report folder:
Pawar\Downloads\Access Data FTK Case Data\SampleCase\report T\
Browse...
Export all files using actual filenames (may cause broken links on CDs or DVDs)
Include Registry Viewer reports
Custom graphic for the report (recommended maximum width is 183 pixels)
Browse...
Report language:
English
< Back
Finish
Cancel
File Name
Message0001
Message0002
Message0003
Message0004
Message0005
Message0006
Message0007
Message0008
Message0009
Subject
"Sneha, welcome t...
"Welcome,Sneha"
"Critical security alert"
"Security alert"
"Join Live: Mann Ki ...
"Security alert"
"Security alert"
"Welcome to Paytm"
"Verify your email."
219 Listed
0 Checked Total
0 Highlighted
8:36 PM
12/15/2021
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
10:06 AM
12/16/2021

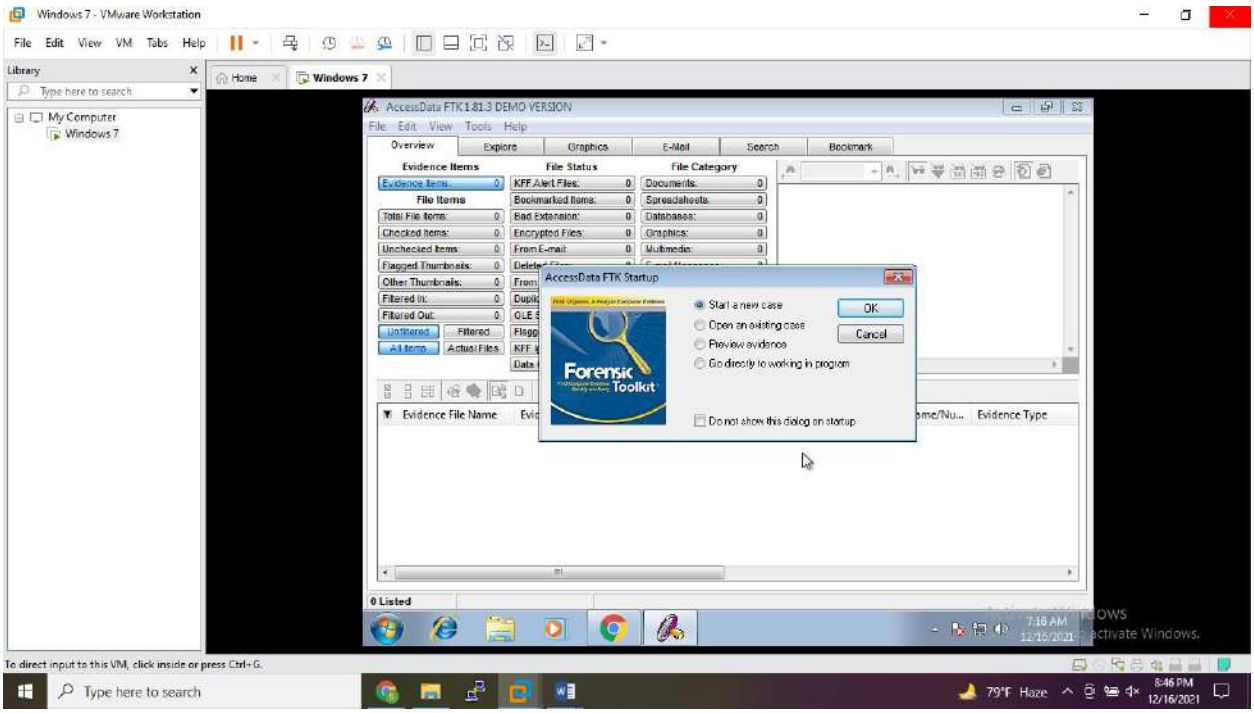

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION - C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
Report Wizard
Do you wish to view the report?
Yes
No
219 Listed
0 Checked Total
0 Highlighted
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
10:07 AM
12/16/2021

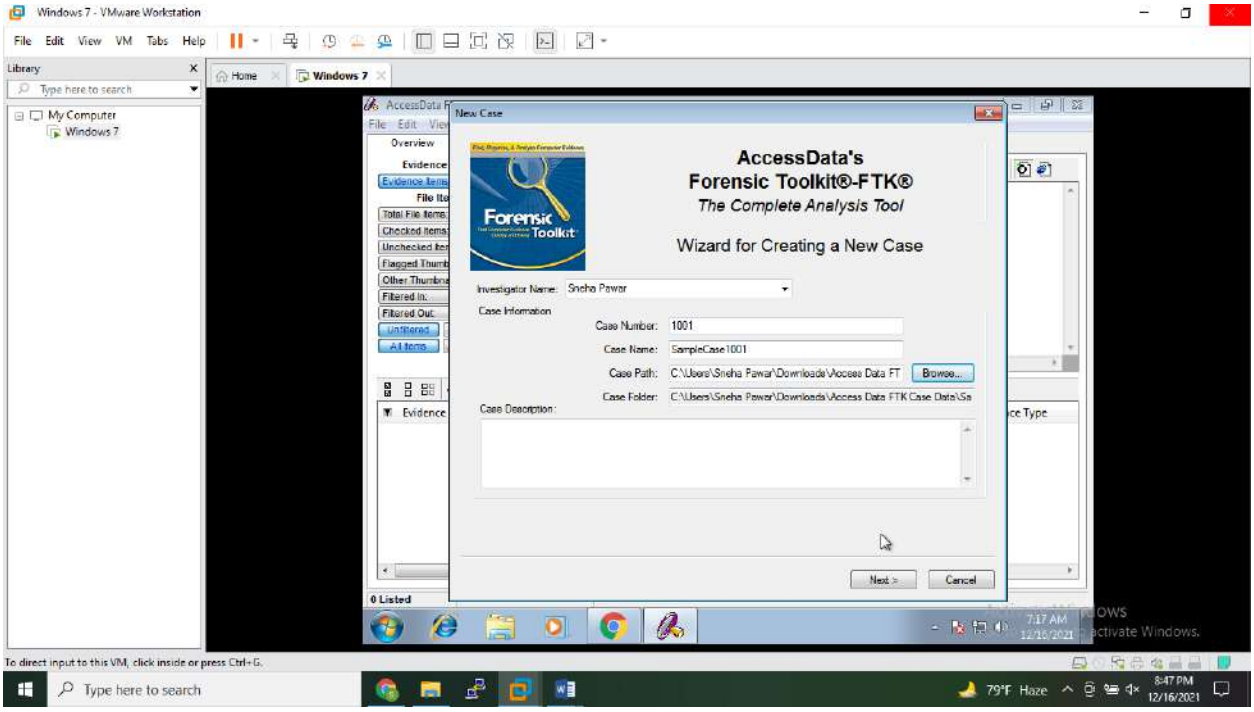
Click on Yes.

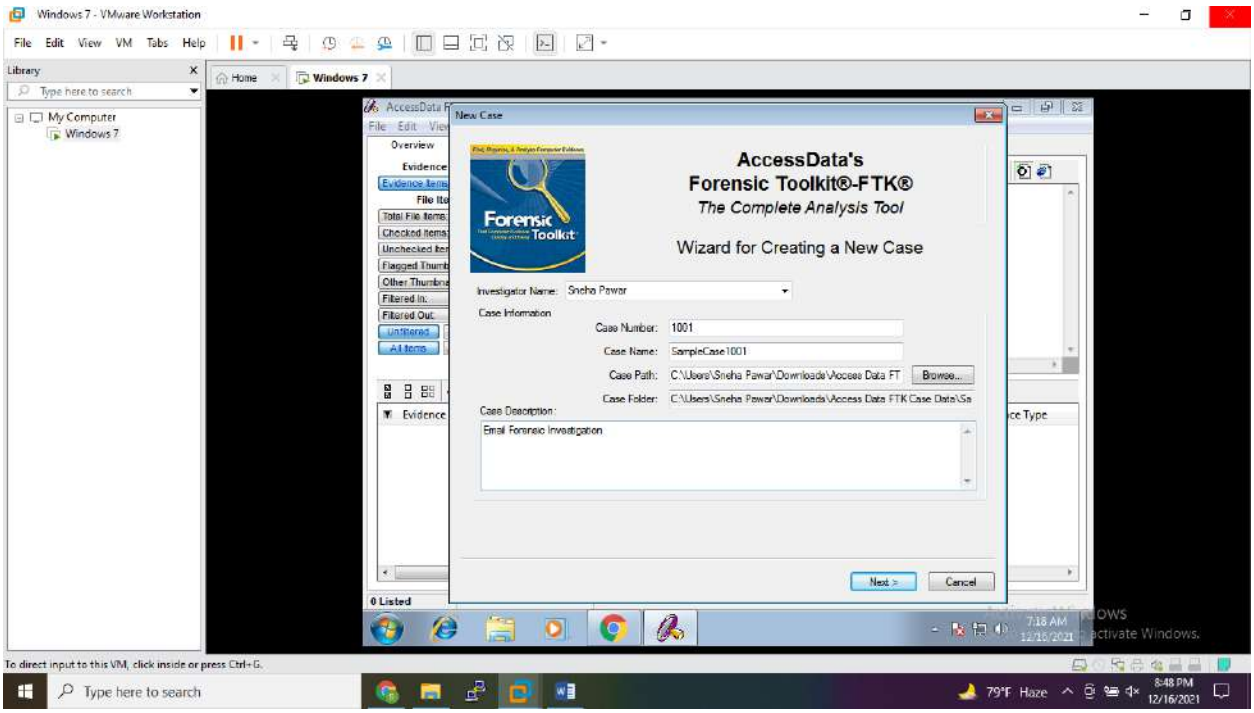

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
FTKReport
FTK CASE REPORT
Case Summary
Case Information
File Overview
Evidence List
Supplementary Files
Case Log
List by File Path
- None -
MS Access database
File listing database
List File Properties
- List File Properties -
Bookmarks
Case Information
12/15/2021
FTK Version Version 1.81.3, build 09.04.10
Case Number CaseNo01
Case Location C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
Case Description ABC
Report Created Wednesday, December 15, 2021 8:37:06 PM
Forensic Examiner Sneha Pawar
Agency RJ College
Address 6/601, Bharat Nagar
Phone 9827364520
Fax 0203
MailSampleData.pst
Show all
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
10:07 AM
12/16/2021

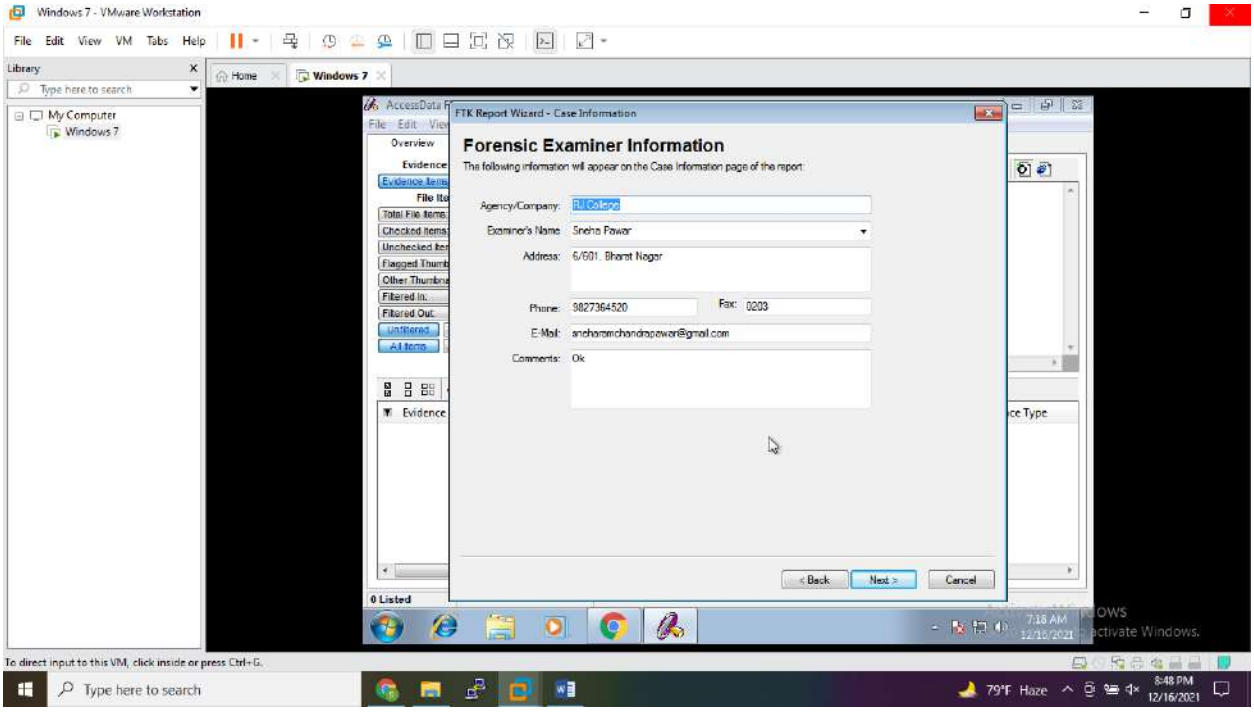

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
FTKReport
File | C:/Users/Sneha%20Pawar/Downloads/Access%20Data%20FTK%20Case%20...
FTK CASE REPORT
Case Summary
Case Information
File Overview
Evidence List
Supplementary Files
Case Log
List by File Path
- None -
MS Access database
File listing database
List File Properties
- List File Properties -
Bookmarks
File Overview
12/15/2021
Evidence Items
Evidence Items: 2
File Items
Total File Items: 395
Flagged Thumbnails: 0
Other Thumbnails: 0
File Status
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 0
Encrypted Files: 1
From E-mail: 384
Deleted Files: 0
From Recycle Bin: 0
Duplicate Items: 22
OLE Subitems: 0
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0
MailSampleData.pst
Show all
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
10:07 AM
12/16/2021

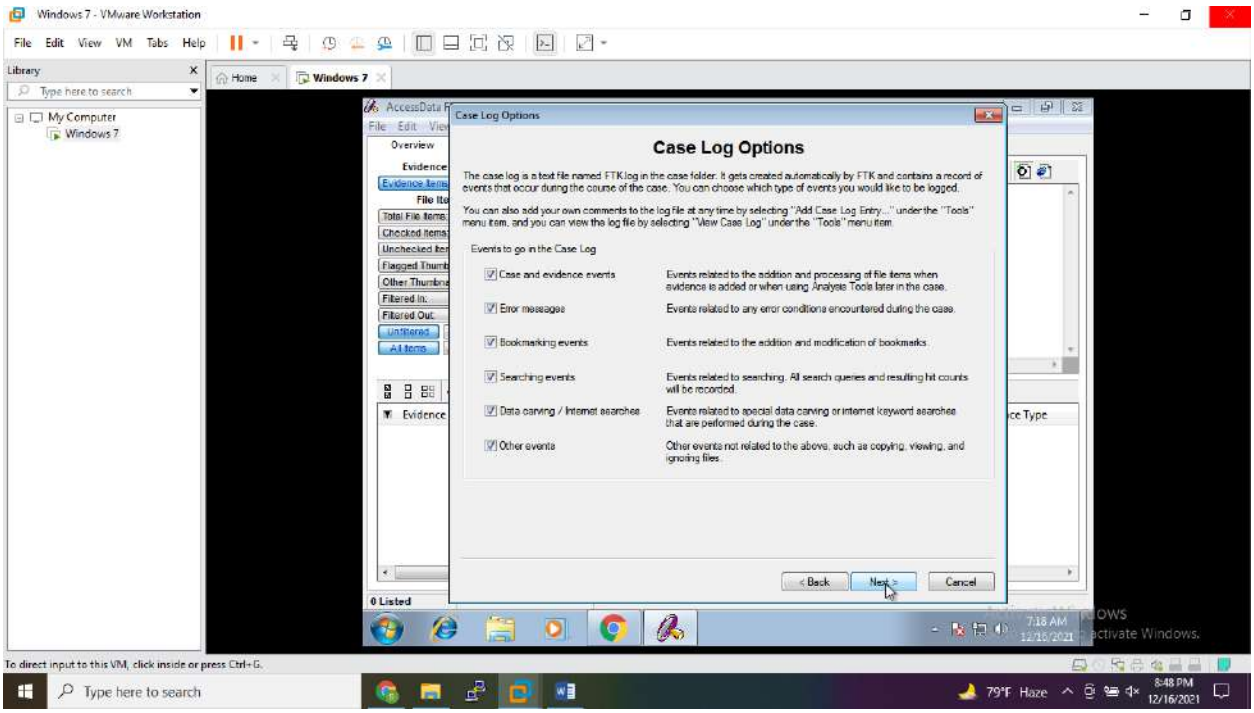

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
FTKReport
File | C:/Users/Sneha%20Pawar/Downloads/Access%20Data%20FTK%20Case%20...
FTK CASE REPORT
Case Summary
Case Information
File Overview
Evidence List
Supplementary Files
Case Log
List by File Path
- None -
MS Access database
File listing database
List File Properties
- List File Properties -
Bookmarks
Evidence List
12/15/2021
Display Name: Evidence01
Evidence File Name: kff-kff_library_file-29_sep_2008.exe
Evidence Path: C:\Users\Sneha Pawar\Downloads\Access Data FTK\AccessData FTK
Identification Name/Number: 01
Evidence Type: Individual file
Added: 12/15/2021 5:12:15 PM
Children: 0
Descendants: 0
Comment: Ok
Display Name: MailSampleData
Evidence File Name: MailSampleData.pst
Evidence Path: C:\Users\Sneha Pawar\Downloads
Identification Name/Number:
Evidence Type: Individual file
Added: 12/15/2021 8:32:53 PM
Children: 0
Descendants: 381
AccessData Forensic Toolkit®
MailSampleData.pst
Show all
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
10:08 AM
12/16/2021

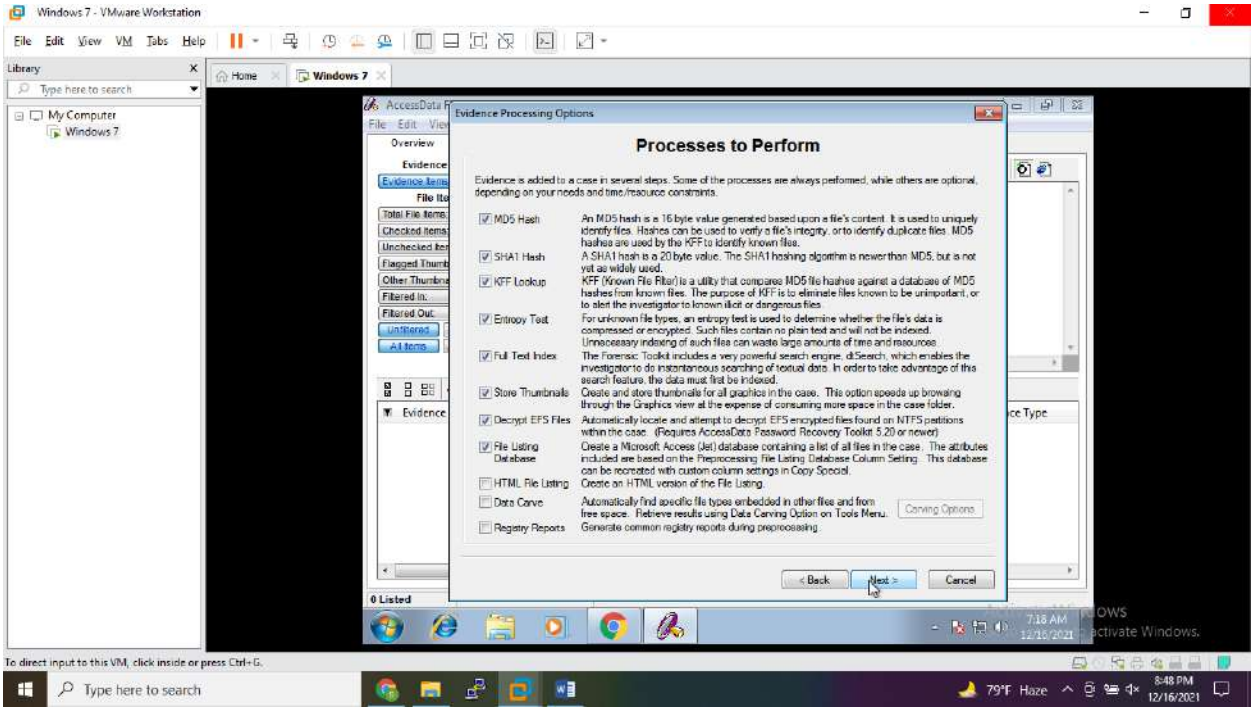

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Evidence Items
File Status
File Category
AccessData FTK Startup
Start a new case
Open an existing case
Preview evidence
Go directly to working in program
OK
Cancel
Do not show this dialog on startup
Forensic Toolkit
Evidence File Name
Evidence Type
0 Listed
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:46 PM
12/16/2021

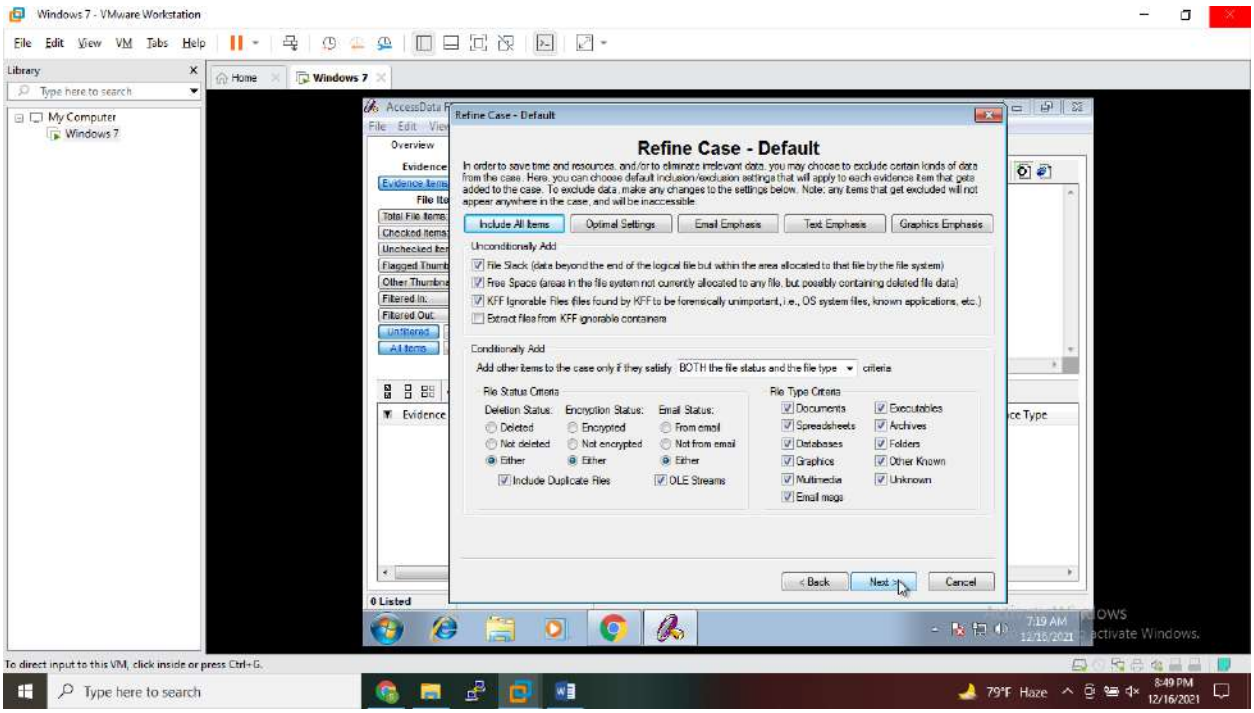

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
New Case
AccessData's
Forensic Toolkit®-FTK®
The Complete Analysis Tool
Wizard for Creating a New Case
Investigator Name:
Sneha Pawar
Case Information
Case Number:
1001
Case Name:
SampleCase1001
Case Path:
C:\Users\Sneha Pawar\Downloads\Access Data FT
Browse...
Case Folder:
C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\Sa
Case Description:
Next >
Cancel
Forensic Toolkit
0 Listed
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:47 PM
12/16/2021

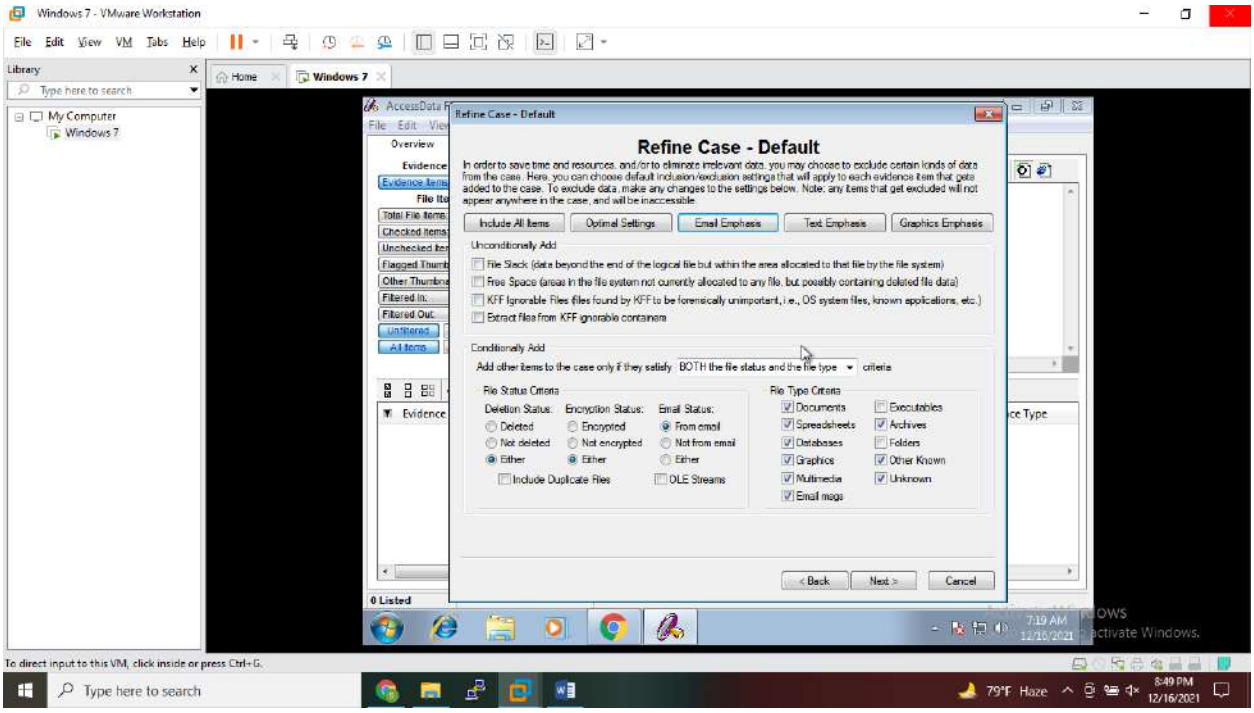

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
New Case
AccessData's
Forensic Toolkit®-FTK®
The Complete Analysis Tool
Wizard for Creating a New Case
Investigator Name: Sneha Pawar
Case Information
Case Number: 1001
Case Name: SampleCase1001
Case Path: C:\Users\Sneha Pawar\Downloads\Access Data FT
Browse...
Case Folder: C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\Sa
Case Description:
Email Forensic Investigation
Next >
Cancel
0 Listed
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:48 PM
12/16/2021

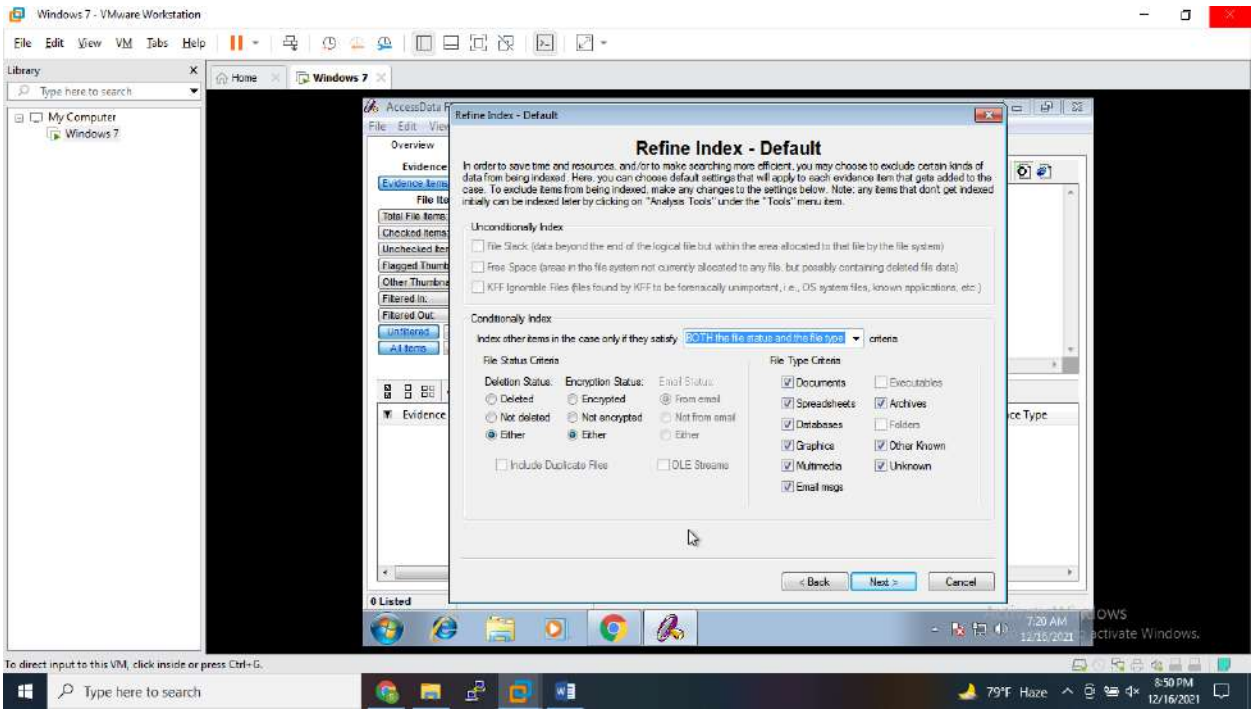

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
FTK Report Wizard - Case Information
Forensic Examiner Information
The following information will appear on the Case Information page of the report
Agency/Company: RJ College
Examiner's Name: Sneha Pawar
Address: 6/601, Bharat Nagar
Phone: 9827364520
Fax: 0203
E-Mail: archanmchandrapawar@gmail.com
Comments: Ok
< Back
Next >
Cancel
0 Listed
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:48 PM
12/16/2021

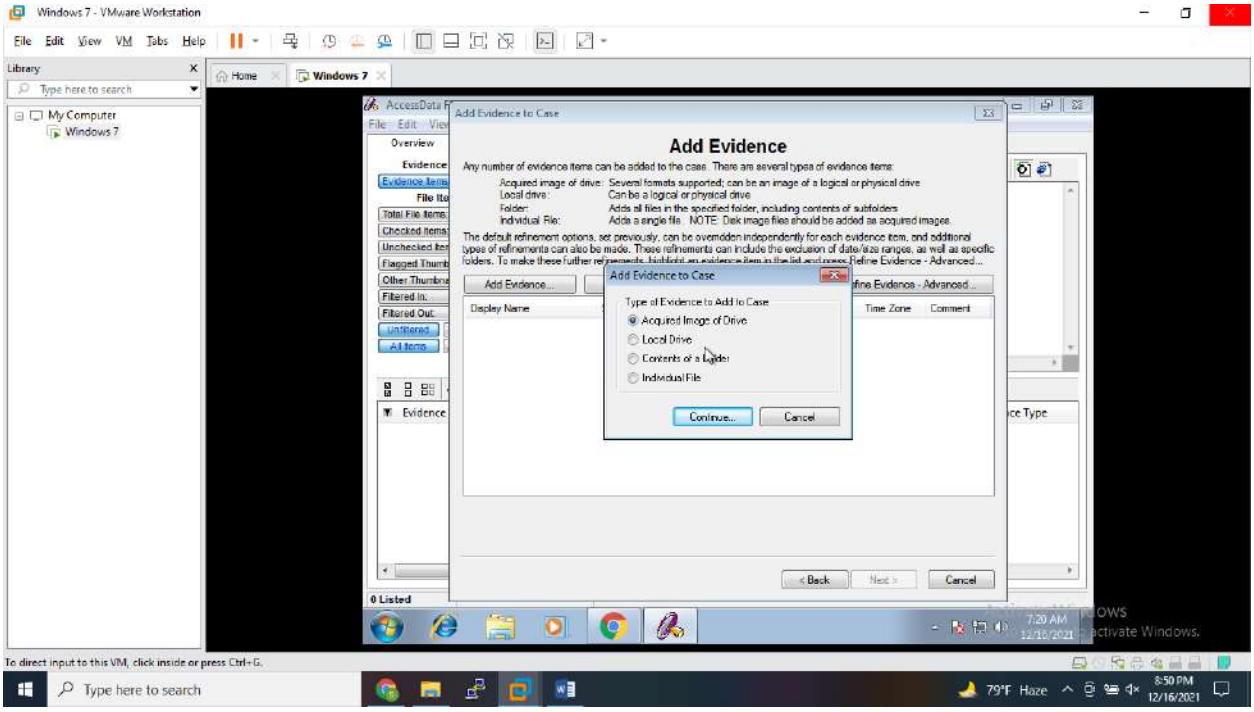

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
Case Log Options
Case Log Options
The case log is a text file named FTKLog in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged.
You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Tools" menu item, and you can view the log file by selecting "View Case Log" under the "Tools" menu item.
Events to go in the Case Log
Case and evidence events
Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.
Error messages
Events related to any error conditions encountered during the case.
Bookmarking events
Events related to the addition and modification of bookmarks.
Searching events
Events related to searching. All search queries and resulting hit counts will be recorded.
Data carving / Internet searches
Events related to special data carving or internet keyword searches that are performed during the case.
Other events
Other events not related to the above, such as copying, viewing, and ignoring files.
< Back
Next >
Cancel
0 Listed
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:48 PM
12/16/2021

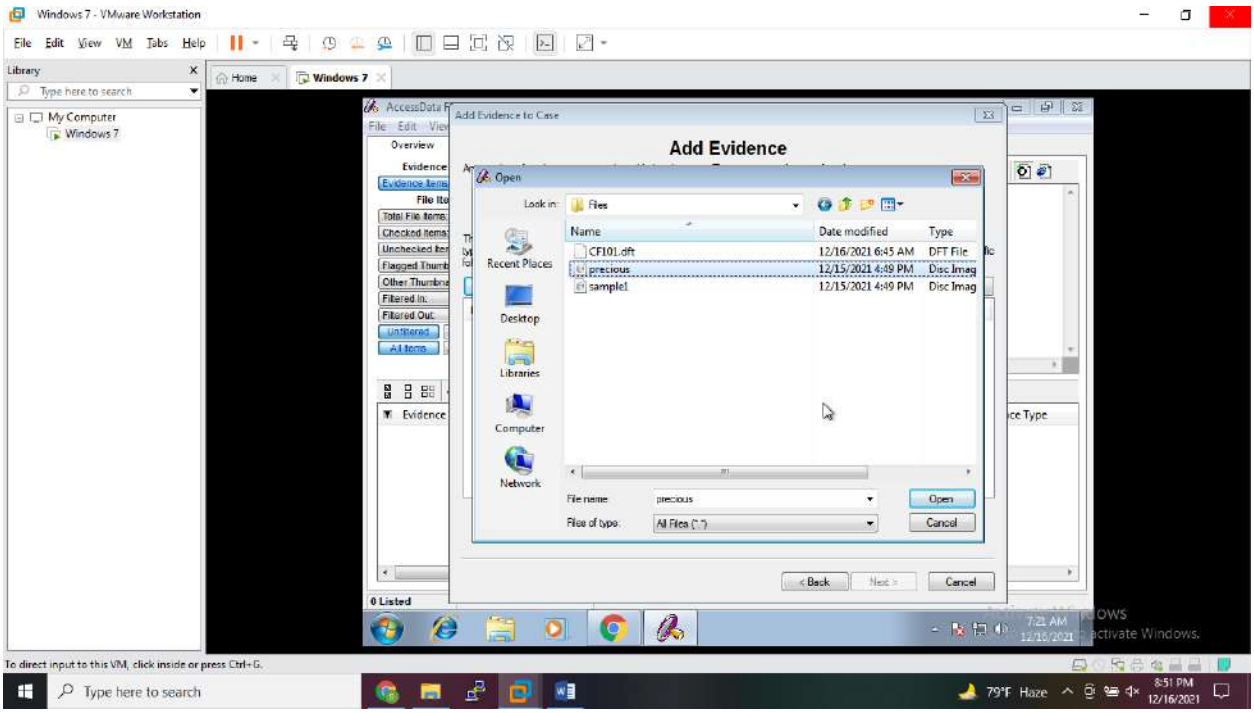

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
Evidence Processing Options
Processes to Perform
Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.
MD5 Hash
An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
SHA1 Hash
A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
KFF Lookup
KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
Entropy Test
For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.
Full Text Index
The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.
Store Thumbnails
Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.
Decrypt EFS Files
Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)
File Listing Database
Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special.
HTML File Listing
Create an HTML version of the File Listing.
Data Carve
Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.
Carving Options
Registry Reports
Generate common registry reports during preprocessing.
< Back
Next >
Cancel
0 Listed
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:48 PM
12/16/2021

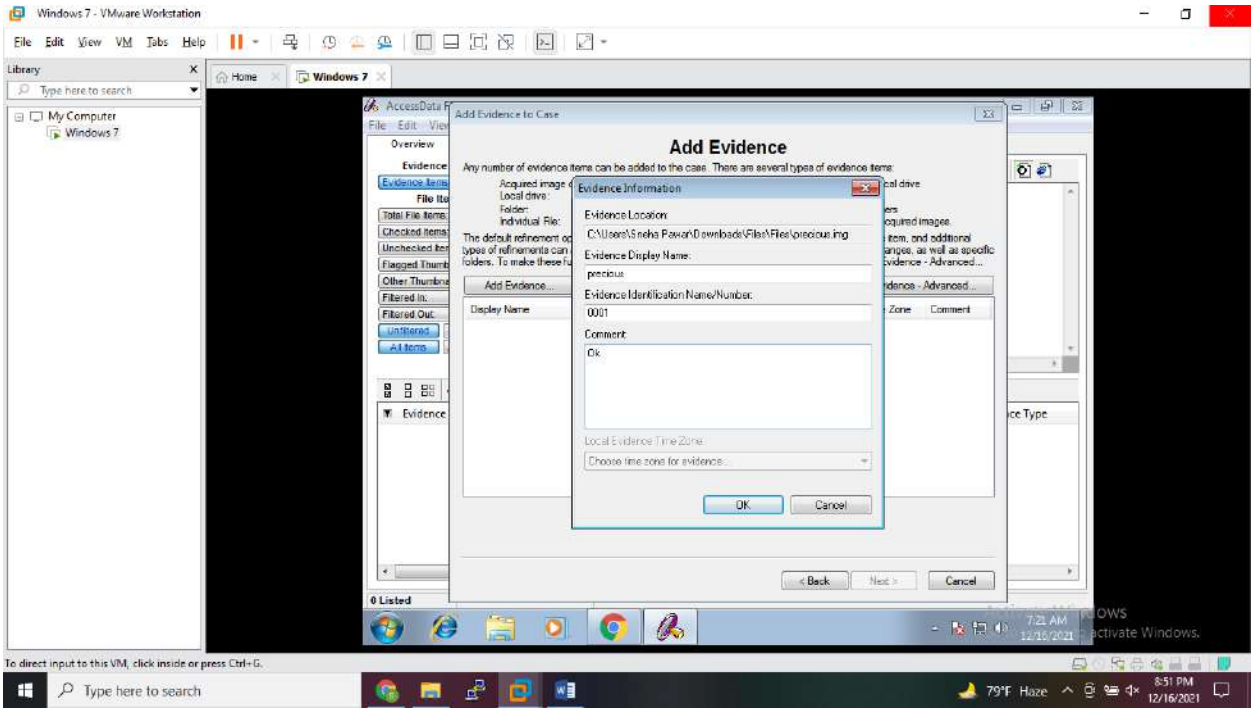

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
Refine Case - Default
Refine Case - Default
In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.
Include All Items
Optimal Settings
Email Emphasis
Text Emphasis
Graphics Emphasis
Unconditionally Add
File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)
Extract files from KFF ignorable containers
Conditionally Add
Add other items to the case only if they satisfy BOTH the file status and the file type criteria
File Status Criteria
Deletion Status:
Deleted
Not deleted
Either
Encryption Status:
Encrypted
Not encrypted
Either
Email Status:
From email
Not from email
Either
Include Duplicate Files
OLE Streams
File Type Criteria
Documents
Spreadsheets
Databases
Graphics
Multimedia
Email msgs
Executables
Archives
Folders
Other Known
Unknown
< Back
Next >
Cancel
0 Listed
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:49 PM
12/16/2021

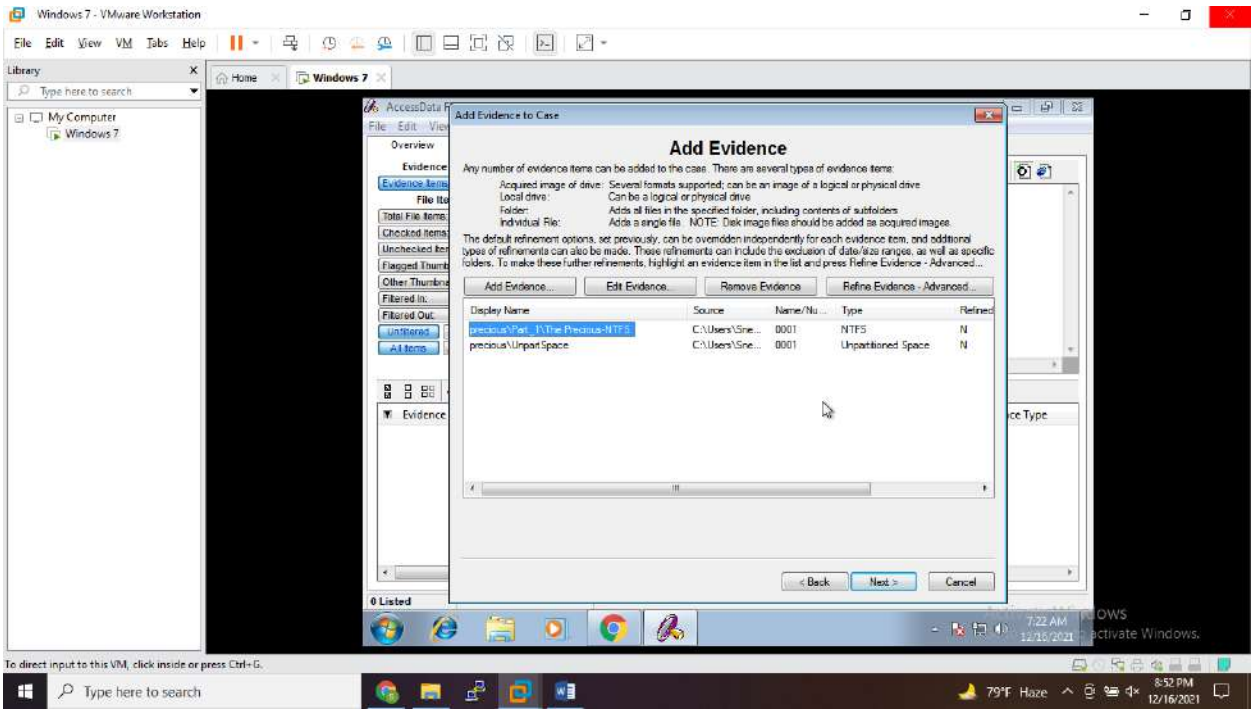

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
Refine Case - Default
Refine Case - Default
In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.
Include All Items
Optimal Settings
Email Emphasis
Text Emphasis
Graphics Emphasis
Unconditionally Add
File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)
Extract files from KFF ignorable containers
Conditionally Add
Add other items to the case only if they satisfy BOTH the file status and the file type criteria
File Status Criteria
Deletion Status:
Deleted
Not deleted
Either
Encryption Status:
Encrypted
Not encrypted
Either
Email Status:
From email
Not from email
Either
Include Duplicate Files
OLE Streams
File Type Criteria
Documents
Spreadsheets
Databases
Graphics
Multimedia
Email msgs
Executables
Archives
Folders
Other Known
Unknown
< Back
Next >
Cancel
0 Listed
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:49 PM
12/16/2021

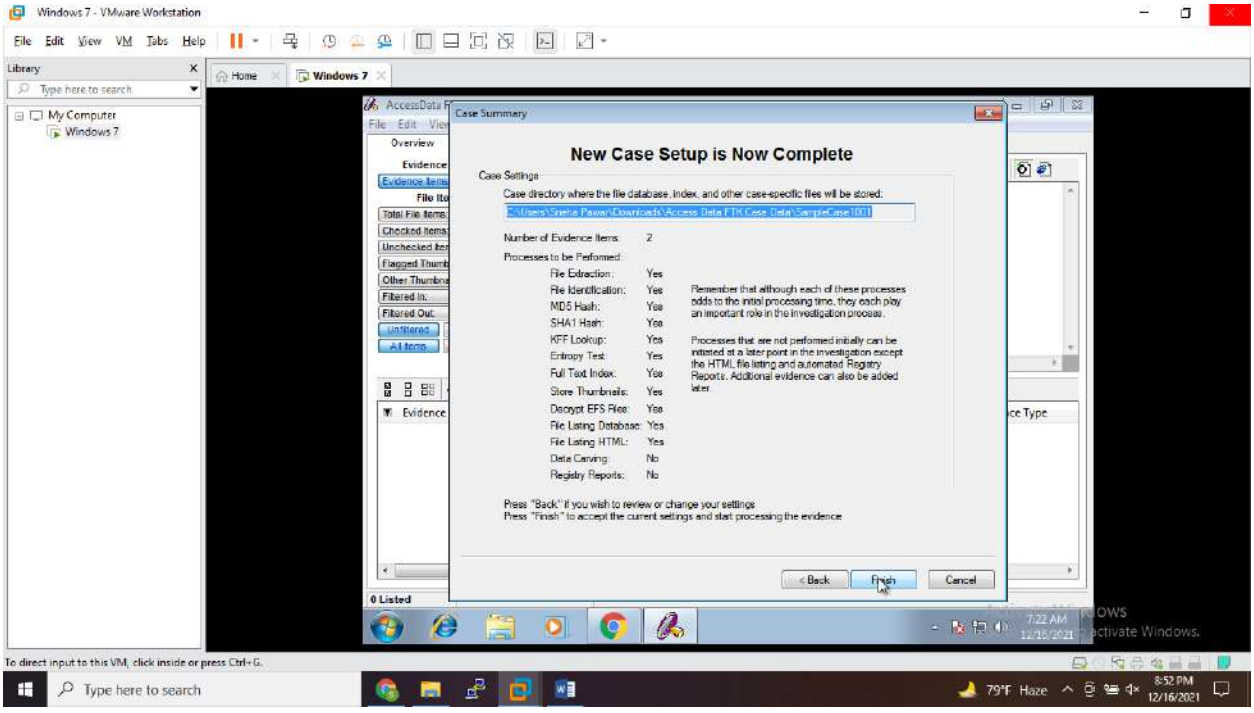

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
Refine Index - Default
Refine Index - Default
In order to save time and resources, and/or to make searching more efficient, you may choose to exclude certain kinds of data from being indexed. Here, you can choose default settings that will apply to each evidence item that gets added to the case. To exclude items from being indexed, make any changes to the settings below. Note: any items that don't get indexed initially can be indexed later by clicking on "Analysis Tools" under the "Tools" menu item.
Unconditionally Index
File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)
Conditionally Index
Index other items in the case only if they satisfy BOTH the file status and the file type criteria
File Status Criteria
Deletion Status: Deleted Not deleted Either
Encryption Status: Encrypted Not encrypted Either
Email Status: From email Not from email Either
File Type Criteria
Documents Executables
Spreadsheets Archives
Databases Folders
Graphics Other Known
Multimedia Unknown
Email msgs
Include Duplicate Files
OLE Streams
< Back
Next >
Cancel
0 Listed
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:50 PM
12/16/2021

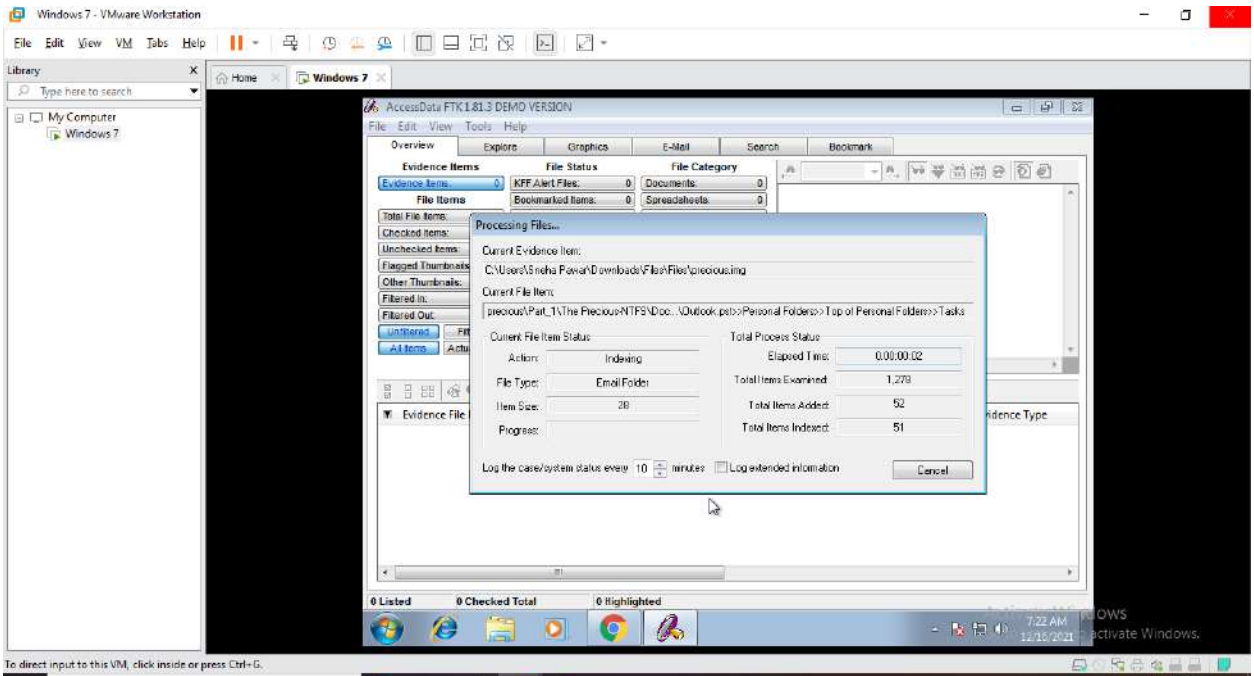

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
Add Evidence to Case
Add Evidence
Any number of evidence items can be added to the case. There are several types of evidence items:
Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
Local drive: Can be a logical or physical drive
Folder: Adds all files in the specified folder, including contents of subfolders
Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.
The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...
Add Evidence...
Refine Evidence - Advanced...
Display Name
Time Zone
Comment
Add Evidence to Case
Type of Evidence to Add to Case
Acquired Image of Drive
Local Drive
Contents of a Folder
Individual File
Continue...
Cancel
< Back
Next >
Cancel
0 Listed
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:50 PM
12/16/2021

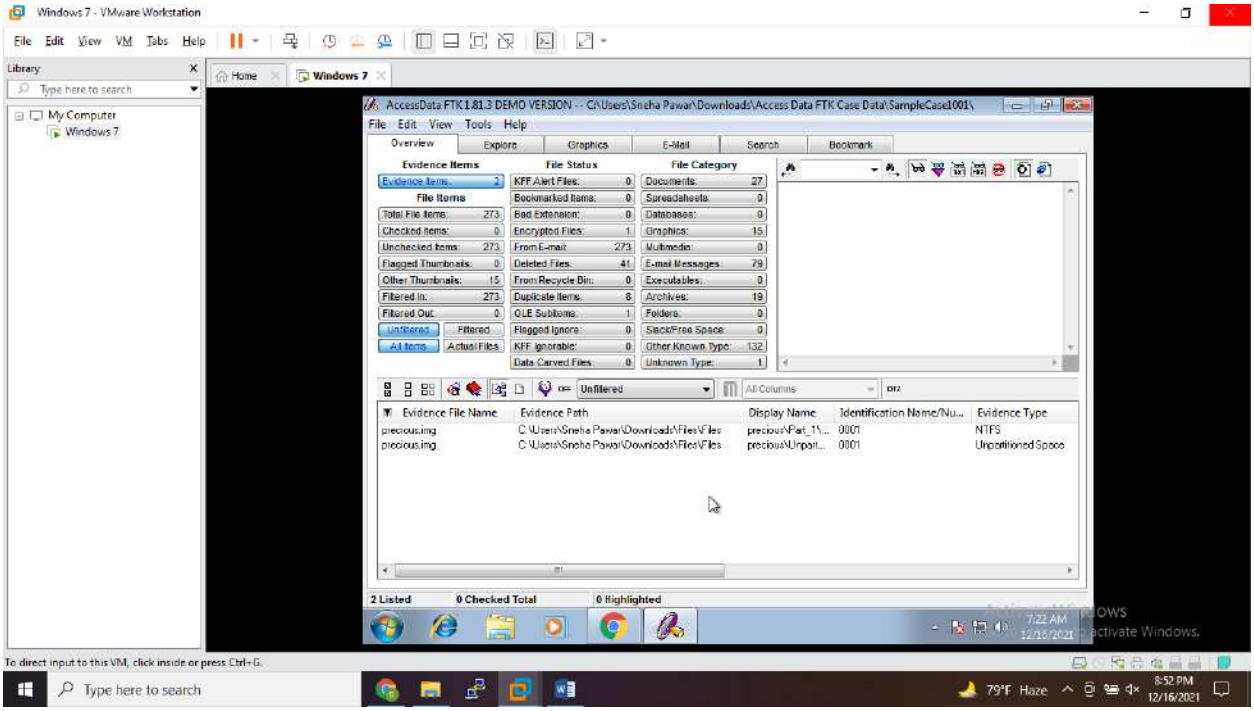

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
Add Evidence to Case
Add Evidence
Open
Look in: Files
Name
Date modified
Type
CF101.dft
12/16/2021 6:45 AM
DFT File
precious
12/15/2021 4:49 PM
Disc Imag
sample1
12/15/2021 4:49 PM
Disc Imag
Recent Places
Desktop
Libraries
Computer
Network
File name: precious
Files of type: All Files (*.*)
Open
Cancel
< Back
Next >
Cancel
0 Listed
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:51 PM
12/16/2021

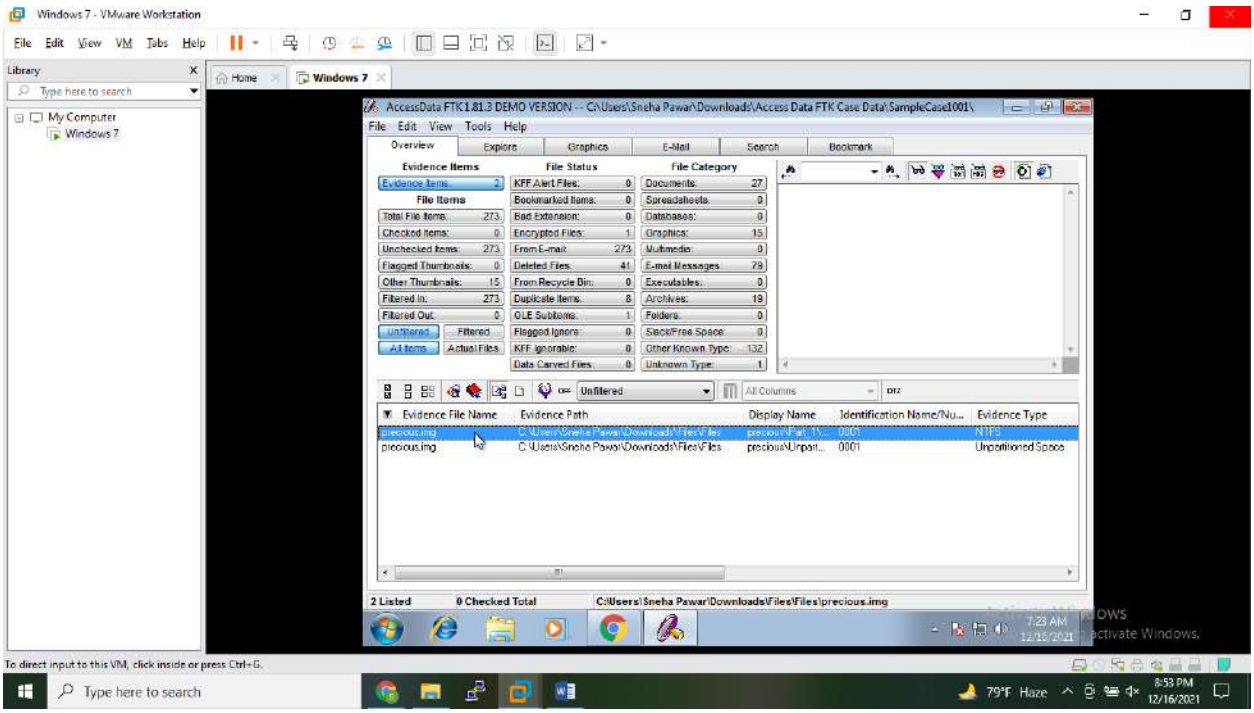

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
Add Evidence to Case
Add Evidence
Any number of evidence items can be added to the case. There are several types of evidence items:
Evidence Information
Evidence Location:
C:\Users\Sneha Pawar\Downloads\Files\Files\precious.img
Evidence Display Name:
precious
Evidence Identification Name/Number:
0001
Comment:
Ok
Local Evidence Time Zone
Choose time zone for evidence...
OK
Cancel
Add Evidence...
Display Name
< Back
Next >
Cancel
0 Listed
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:51 PM
12/16/2021

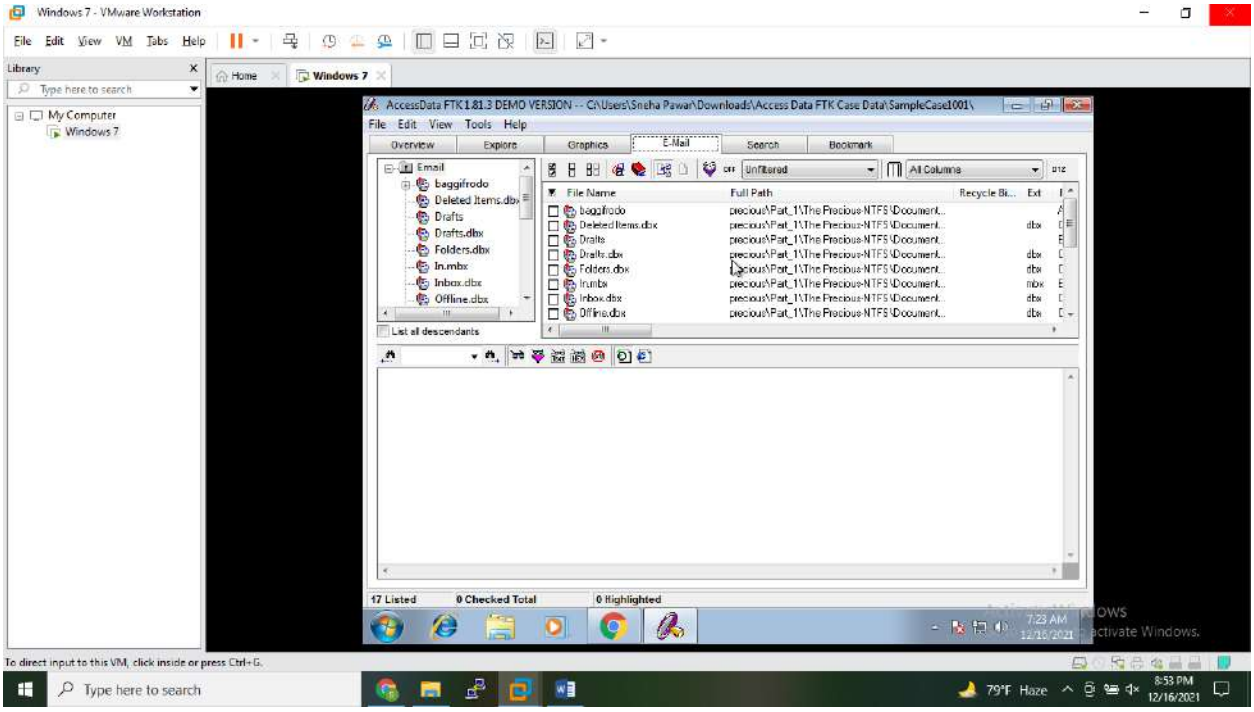

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
Add Evidence to Case
Add Evidence
Any number of evidence items can be added to the case. There are several types of evidence items:
Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
Local drive: Can be a logical or physical drive
Folder: Adds all files in the specified folder, including contents of subfolders
Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.
The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...
Add Evidence...
Edit Evidence...
Remove Evidence
Refine Evidence - Advanced...
Display Name
Source
Name/Nu...
Type
Refined
precious\Part_1\The Precious-NTFS
C:\Users\Sne...
0001
NTFS
N
precious\Unpart Space
C:\Users\Sne...
0001
Unpartitioned Space
N
< Back
Next >
Cancel
0 Listed
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:52 PM
12/16/2021


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
Case Summary
New Case Setup is Now Complete
Case Settings
Case directory where the file database, index, and other case-specific files will be stored:
C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase1001
Number of Evidence Items: 2
Processes to be Performed:
File Extraction: Yes
File Identification: Yes
MD5 Hash: Yes
SHA1 Hash: Yes
KFF Lookup: Yes
Entropy Test: Yes
Full Text Index: Yes
Store Thumbnails: Yes
Decrypt EFS Files: Yes
File Listing Database: Yes
File Listing HTML: Yes
Data Carving: No
Registry Reports: No
Remember that although each of these processes adds to the initial processing time, they each play an important role in the investigation process.
Processes that are not performed initially can be initiated at a later point in the investigation except the HTML file listing and automated Registry Reports. Additional evidence can also be added later.
Press "Back" if you wish to review or change your settings
Press "Finish" to accept the current settings and start processing the evidence
< Back
Finish
Cancel
0 Listed
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:52 PM
12/16/2021

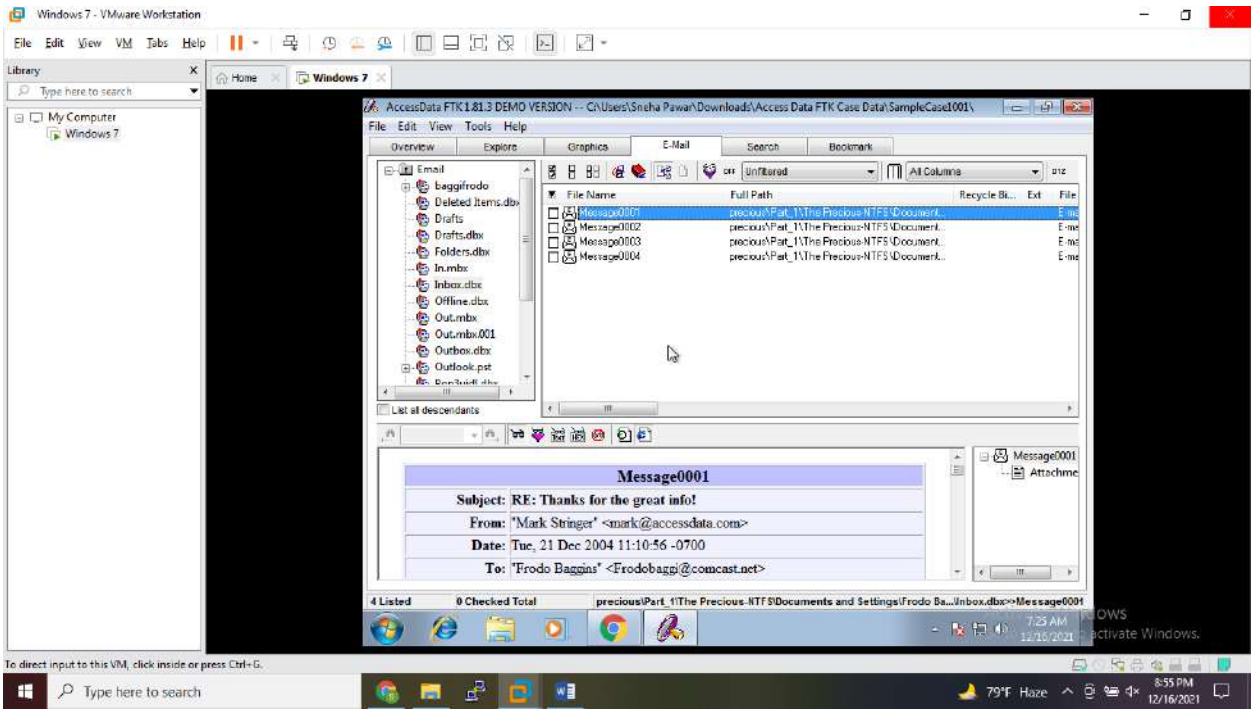

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Evidence Items
File Status
File Category
Processing Files...
Current Evidence Item:
C:\Users\Sneha Pawar\Downloads\Files\Files\precious.img
Current File Item:
precious\Part_1\The Precious-NTFS\Doc...\Outlook.pst>>Personal Folders>>Top of Personal Folder>>Tasks
Current File Item Status
Action: Indexing
File Type: Email Folder
Item Size: 28
Progress:
Total Process Status
Elapsed Time: 0:00:00:02
Total Items Examined: 1,279
Total Items Added: 52
Total Items Indexed: 51
Log the case/system status every 10 minutes
Log extended information
Cancel
0 Listed
0 Checked Total
0 Highlighted
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:52 PM
12/16/2021

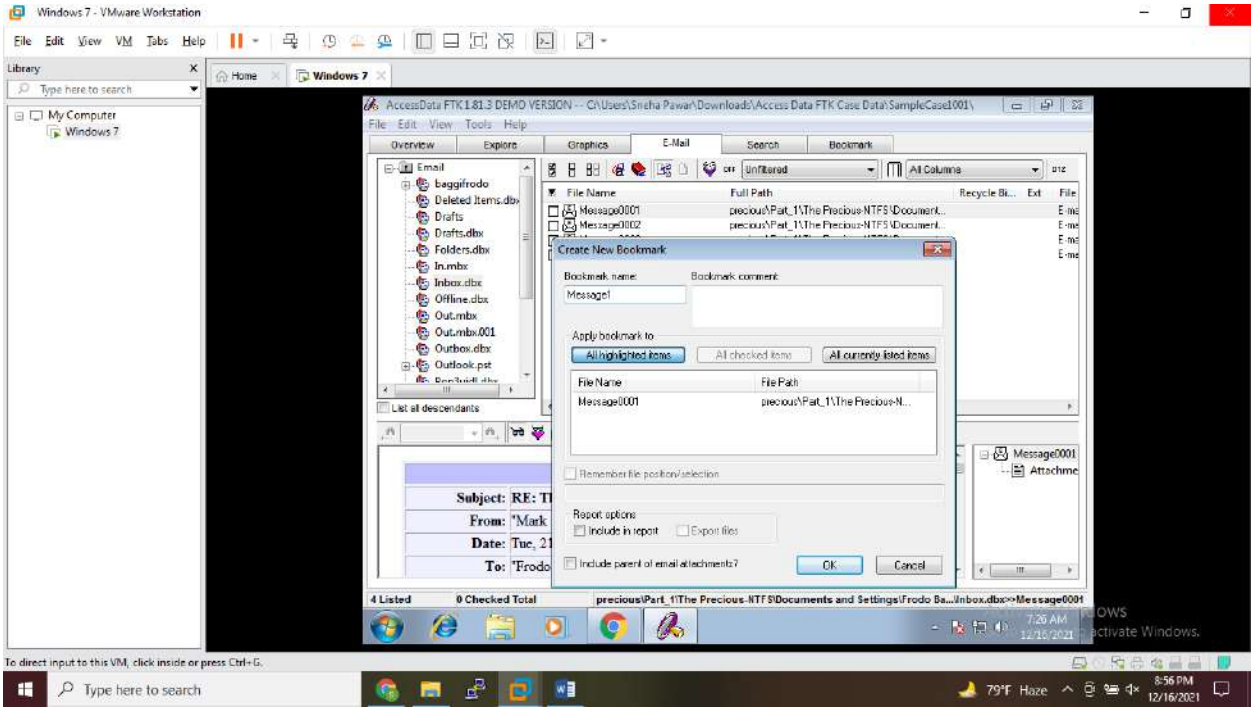

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase1001\
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Evidence Items
File Status
File Category
Evidence File Name
Evidence Path
Display Name
Identification Name/Nu...
Evidence Type
precious.img
C:\Users\Sneha Pawar\Downloads\Files\Files
precious\Part_1\...
0001
NTFS
precious.img
C:\Users\Sneha Pawar\Downloads\Files\Files
precious\Unpart...
0001
Unpartitioned Space
2 Listed
0 Checked Total
0 Highlighted
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:52 PM
12/16/2021

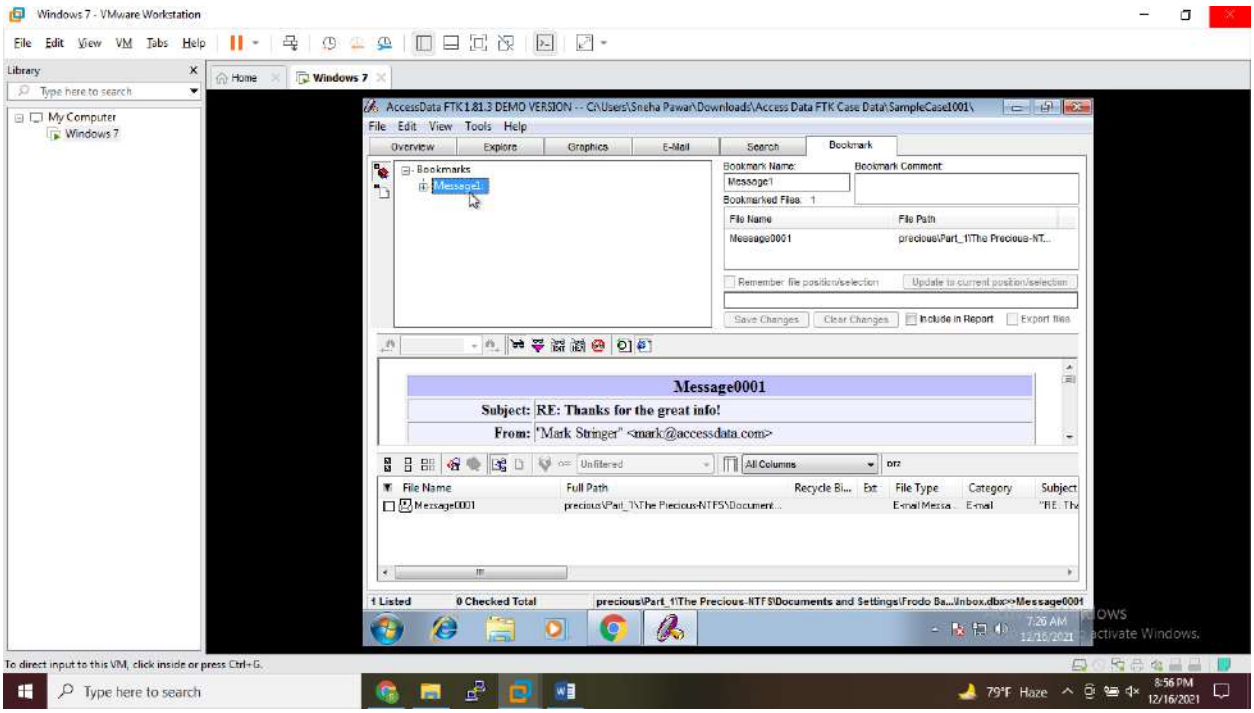

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase1001\
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Evidence Items
File Items
File Status
File Category
Evidence File Name
Evidence Path
Display Name
Identification Name/Nu...
Evidence Type
precious.img
Unpartitioned Space
2 Listed
0 Checked Total
C:\Users\Sneha Pawar\Downloads\Files\Files\precious.img
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:53 PM
12/16/2021


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase1001\
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Email
baggifrodo
Deleted Items.dbx
Drafts
Drafts.dbx
Folders.dbx
In.mbx
Inbox.dbx
Offline.dbx
File Name
Full Path
List all descendants
17 Listed
0 Checked Total
0 Highlighted
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:53 PM
12/16/2021

Inbox – Email


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase1001\
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Email
baggifrodo
Deleted Items.dbx
Drafts
Drafts.dbx
Folders.dbx
In.mbx
Inbox.dbx
Offline.dbx
Out.mbx
Out.mbx.001
Outbox.dbx
Outlook.pst
File Name
Full Path
Recycle Bi...
Ext
Message0001
Message0002
Message0003
Message0004
List all descendants
Message0001
Subject: RE: Thanks for the great info!
From: "Mark Stringer" <mark@accessdata.com>
Date: Tue, 21 Dec 2004 11:10:56 -0700
To: "Frodo Baggins" <Frodobaggi@comcast.net>
4 Listed
0 Checked Total
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:55 PM
12/16/2021


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase1001\
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Create New Bookmark
Bookmark name:
Message1
Bookmark comment:
Apply bookmark to
All highlighted items
All checked items
All currently listed items
File Name
File Path
Message0001
Remember file position/selection
Report options
Include in report
Export files
Include parent of email attachments?
OK
Cancel
4 Listed
0 Checked Total
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:56 PM
12/16/2021


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase1001\
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Bookmarks
Message1
Bookmark Name:
Message1
Bookmark Comment
Bookmarked Files: 1
File Name
File Path
Message0001
precious\Part_1\The Precious-NT...
Remember file position/selection
Update to current position/selection
Save Changes
Clear Changes
Include in Report
Export files
Message0001
Subject: RE: Thanks for the great info!
From: "Mark Stringer" <mark@accessdata.com>
Unfiltered
All Columns
File Name
Full Path
Recycle Bi...
Ext
File Type
Category
Subject
Message0001
precious\Part_1\The Precious-NTFS\Document...
E-mail Messa...
E-mail
1 Listed
0 Checked Total
precious\Part_1\The Precious-NTFS\Documents and Settings\Frodo Ba...\Inbox.dbx=>Message0001
7:26 AM
12/16/2021
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
8:56 PM
12/16/2021

Practical No. 09

Aim: Writing Reports Using FTK [AccessData FTK].

What is AccessData FTK Tool?

Forensic Toolkit, or FTK, is a computer forensics software made by AccessData. It **scans a hard drive looking for various information**. It can, for example, potentially locate deleted emails and scan a disk for text strings to use them as a password dictionary to crack encryption.

FTK provides an **intuitive interface for email analysis** for forensic professionals. This includes having the ability to parse emails for certain words, header analysis for source IP address, etc. A central feature of FTK, file decryption is arguably the most common use of the software.

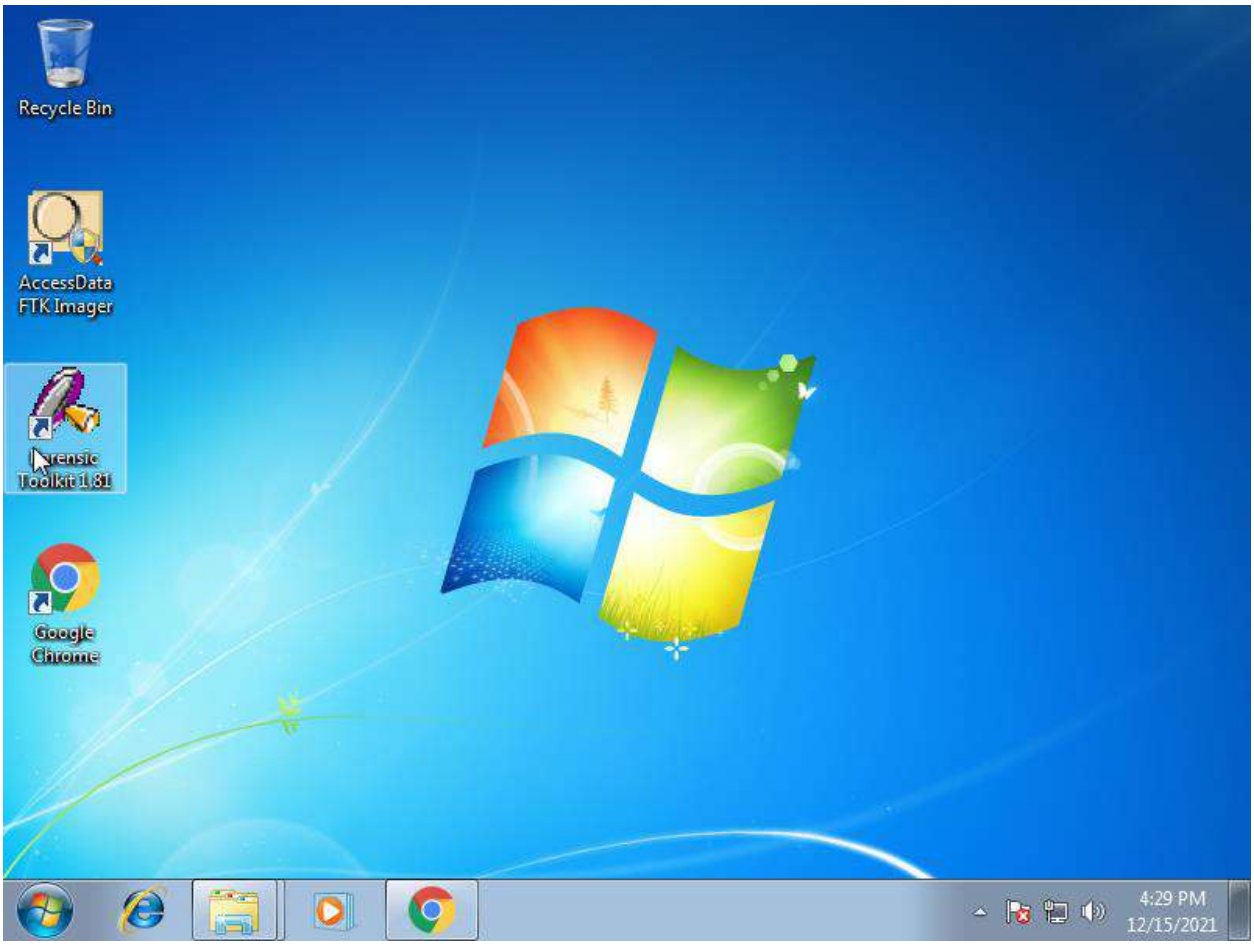
Steps:

After generating any case and adding evidences related to that case you can generate report by using the AccessData FTK tool.

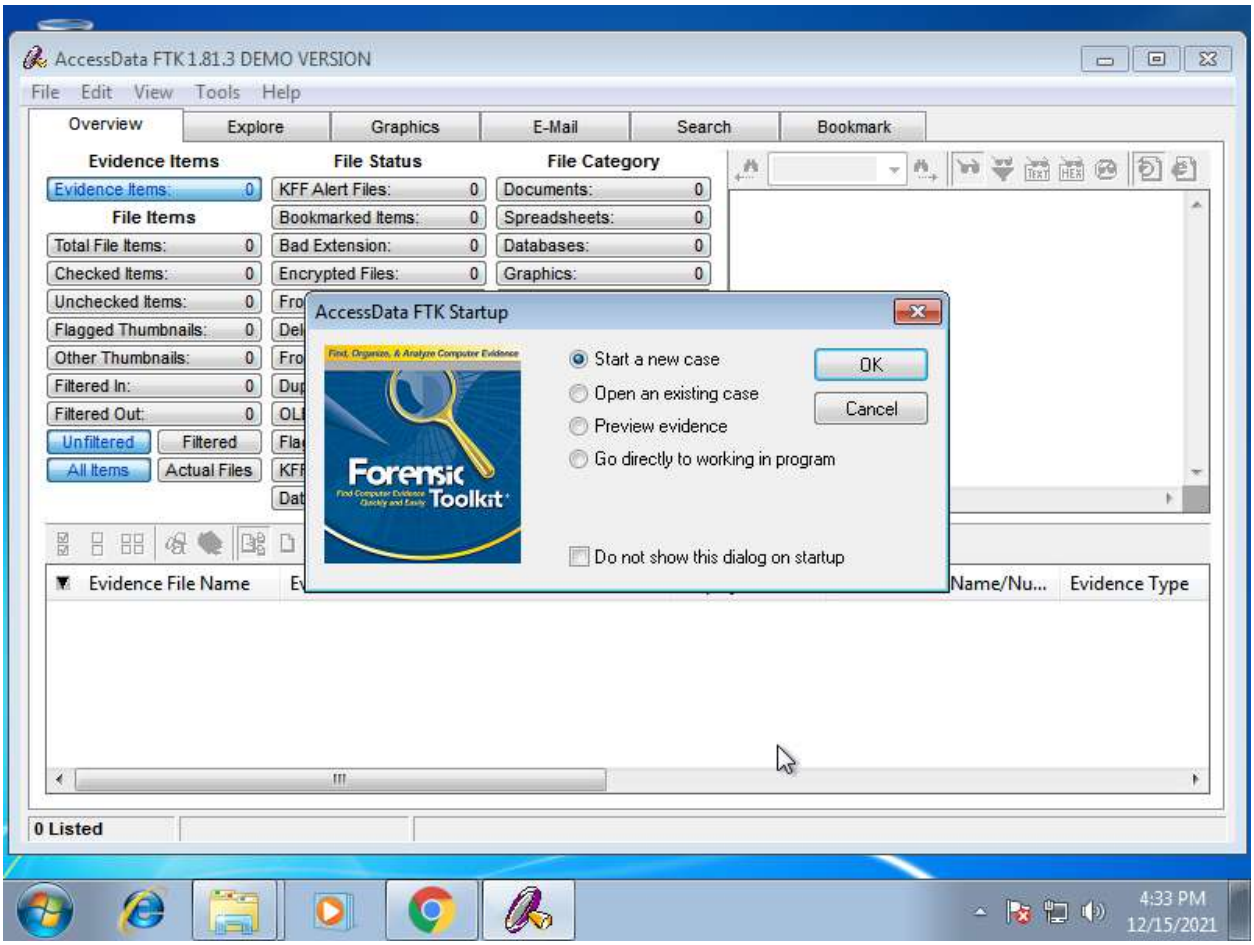
Following are the steps to create case add evidence and generate report using AccessData FTK tool.

To perform this practical you can take reference of Practical No. 08. In this I have added one case related evidences for that and generated reports for the case.

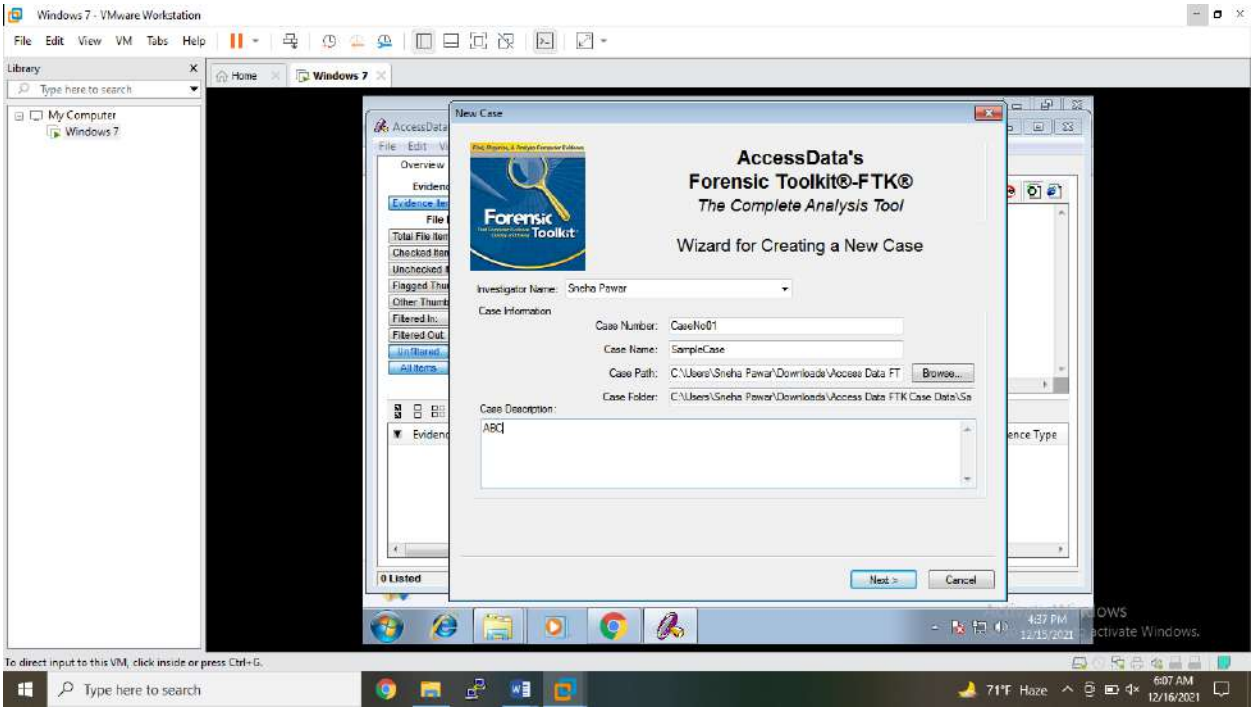
Start the forensic toolkit software.



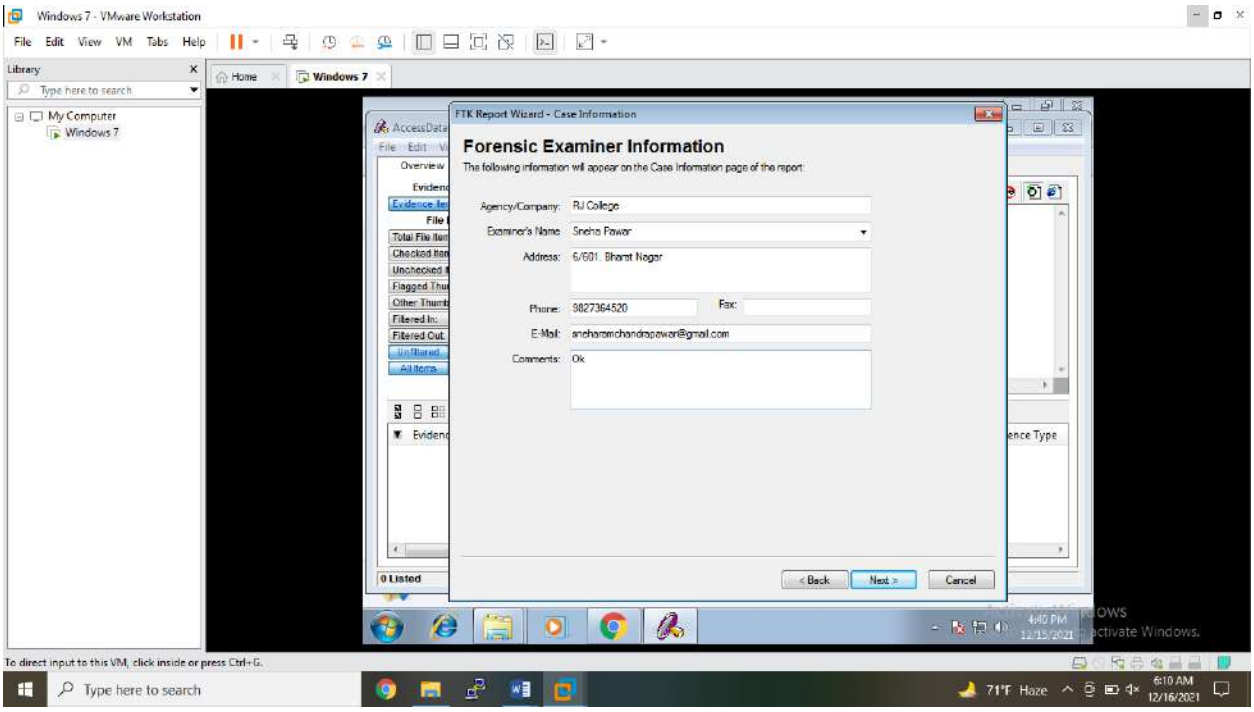
Select Start a New Case.



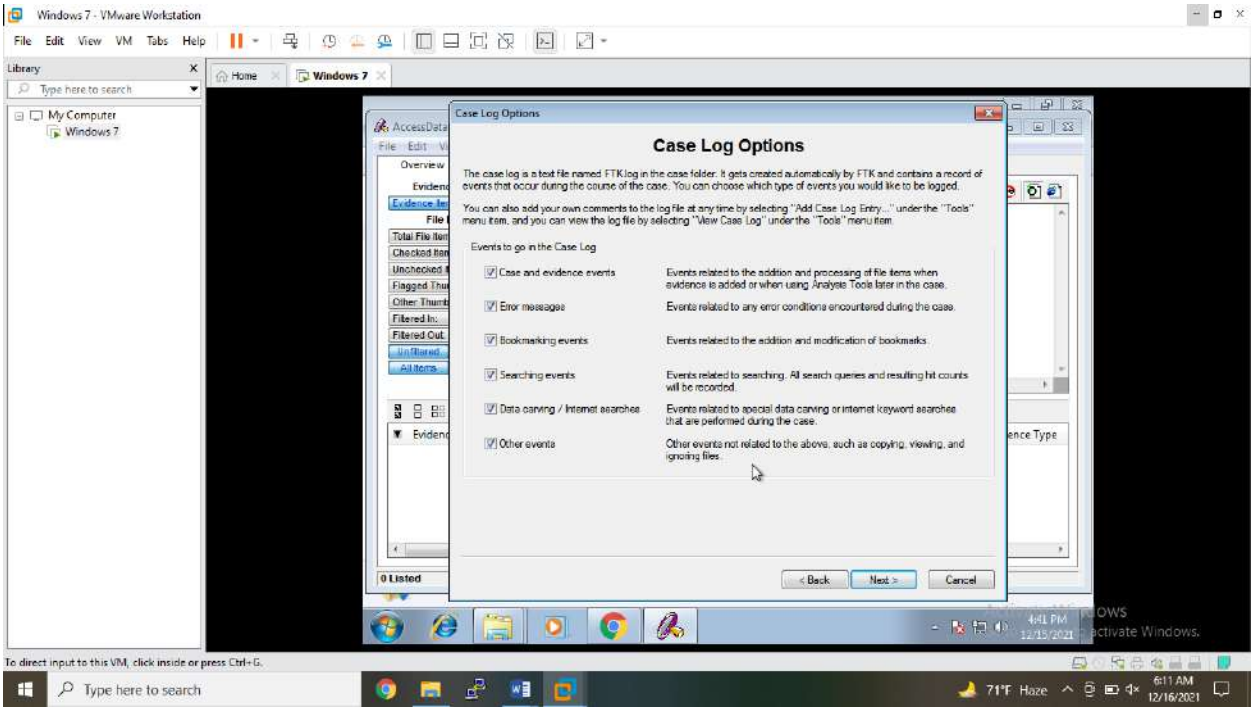
Then enter investigator's name and other details and click on Next.

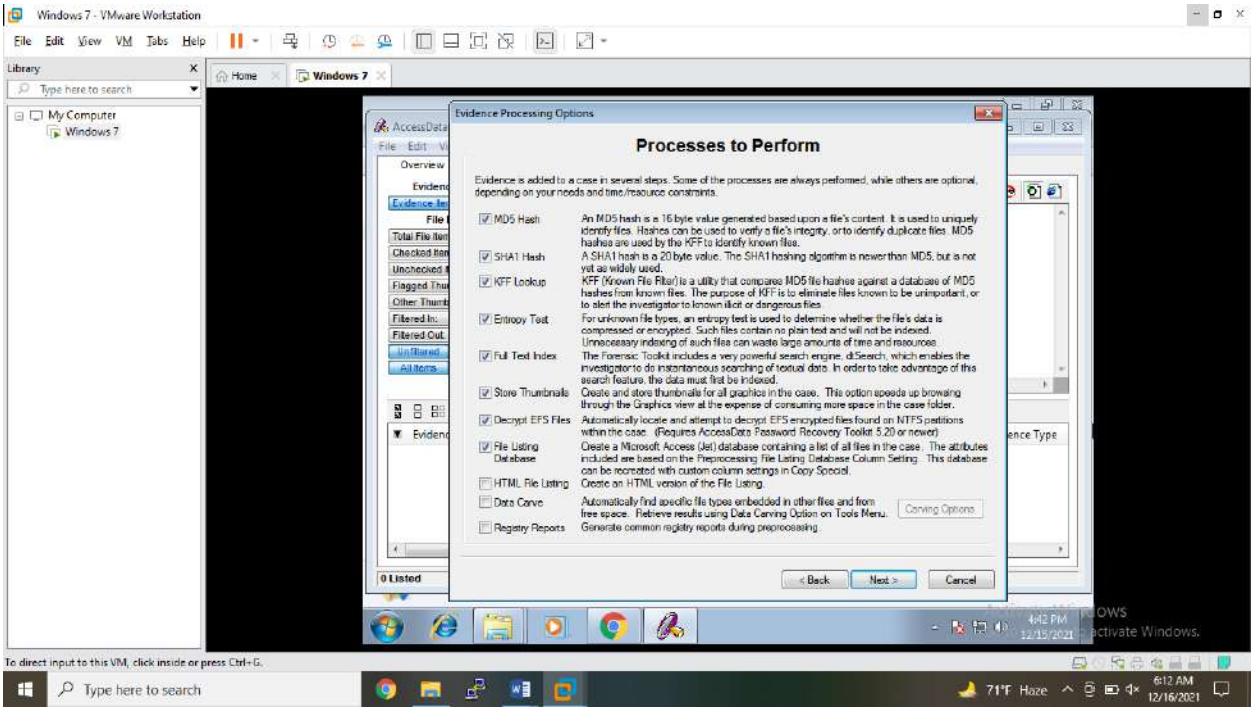


Then enter forensic examiner's details.

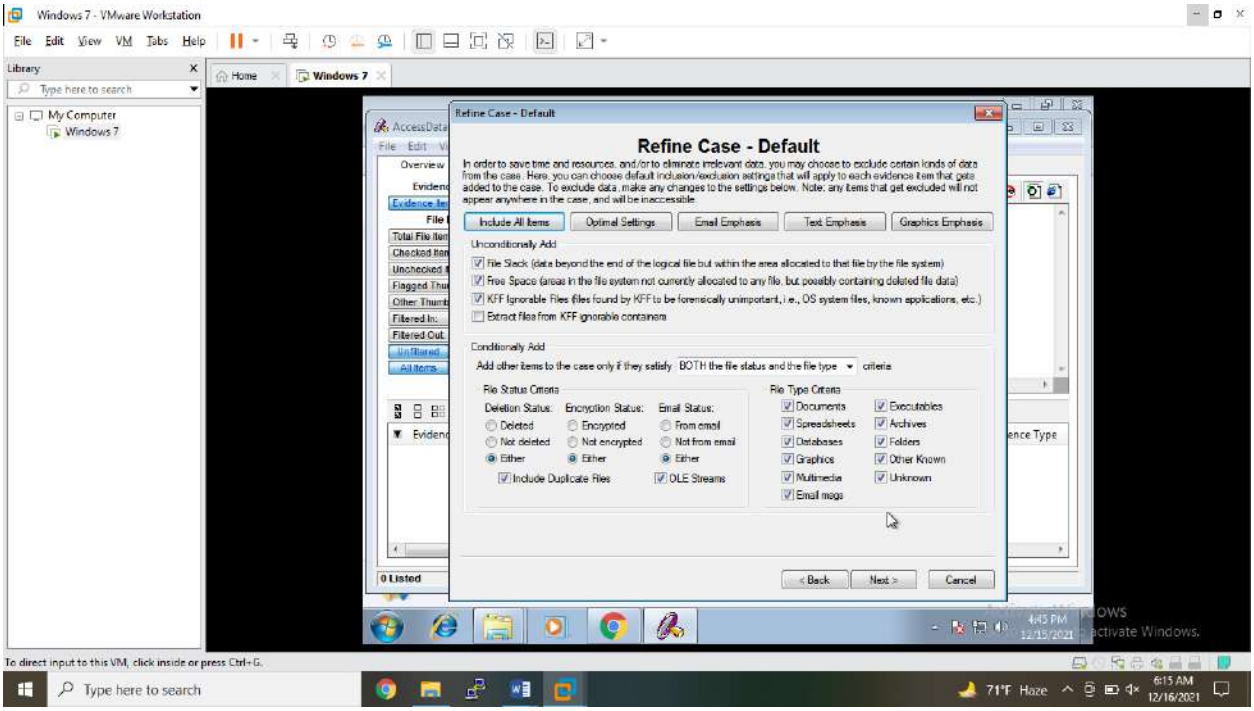


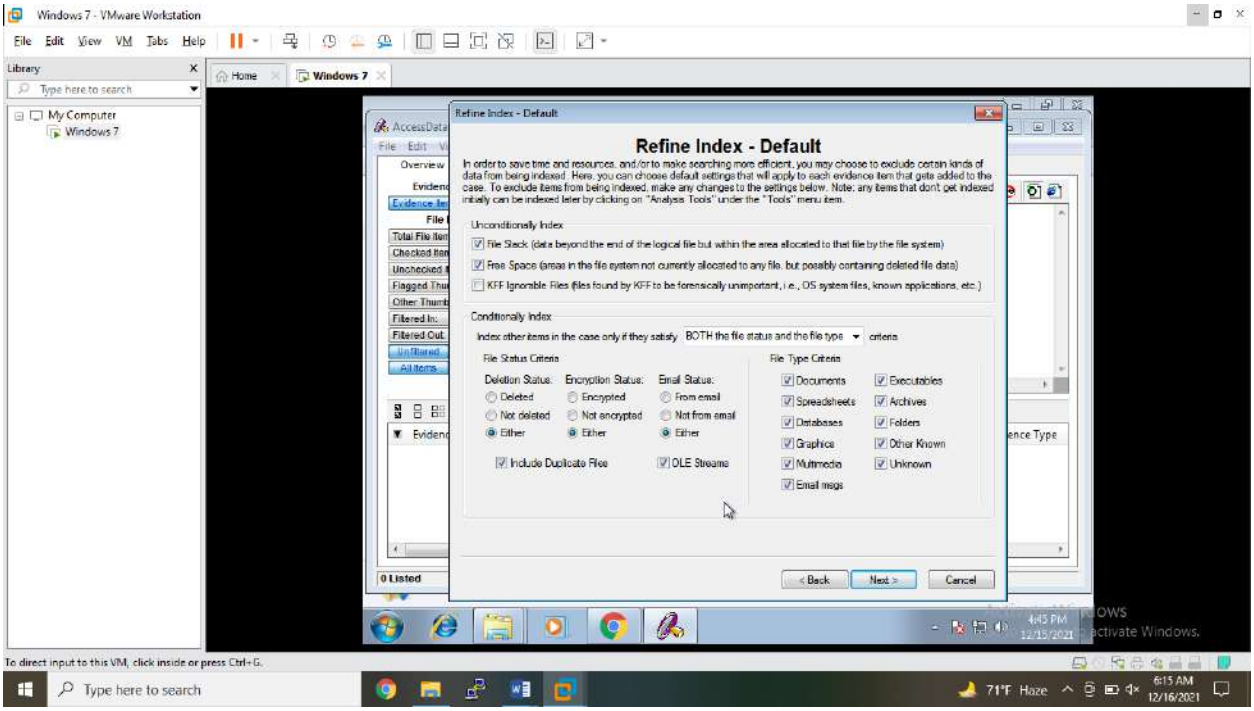
In Case Log Options & Process to perform tabs, keep everything by default.



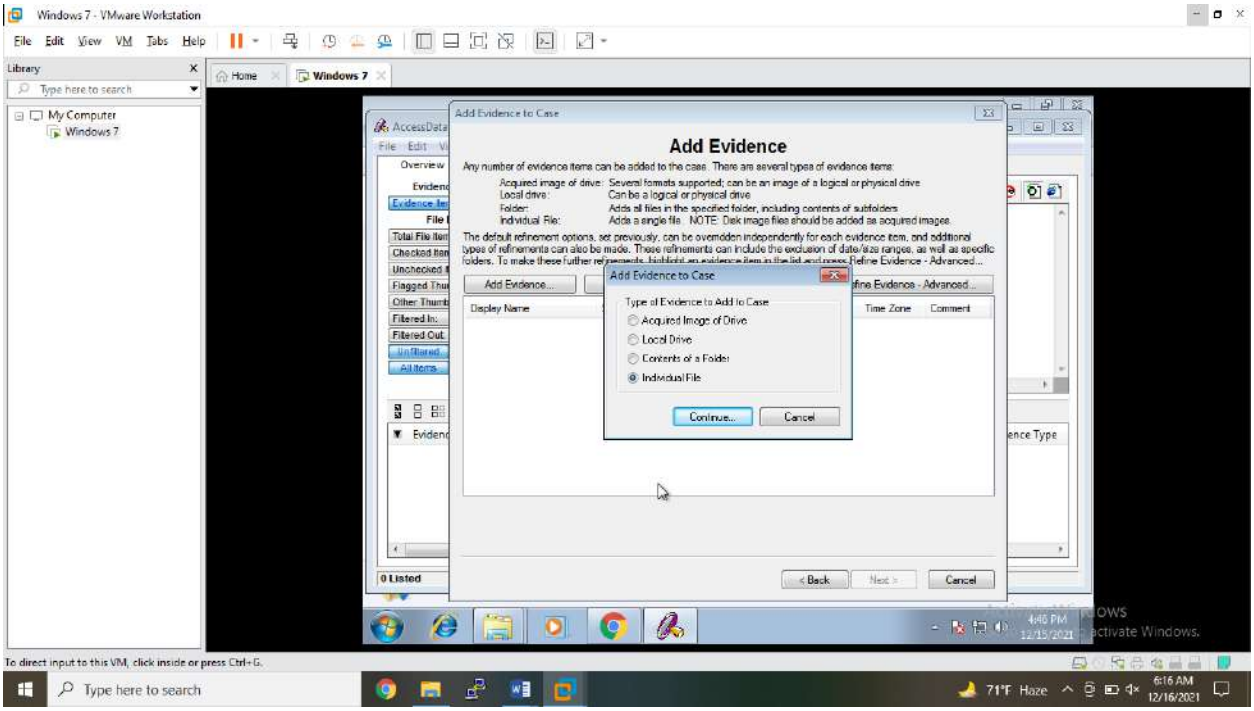


Then in Refine Case Default, Keep everything as it is, and click on Next.

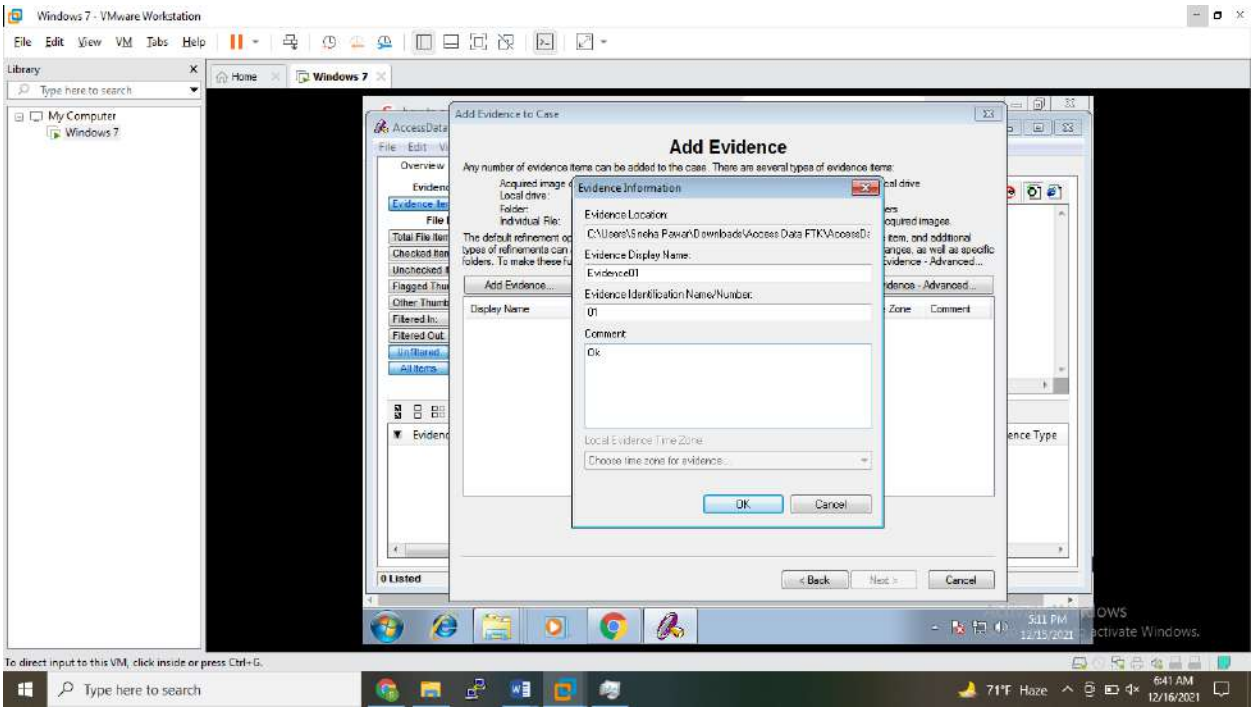


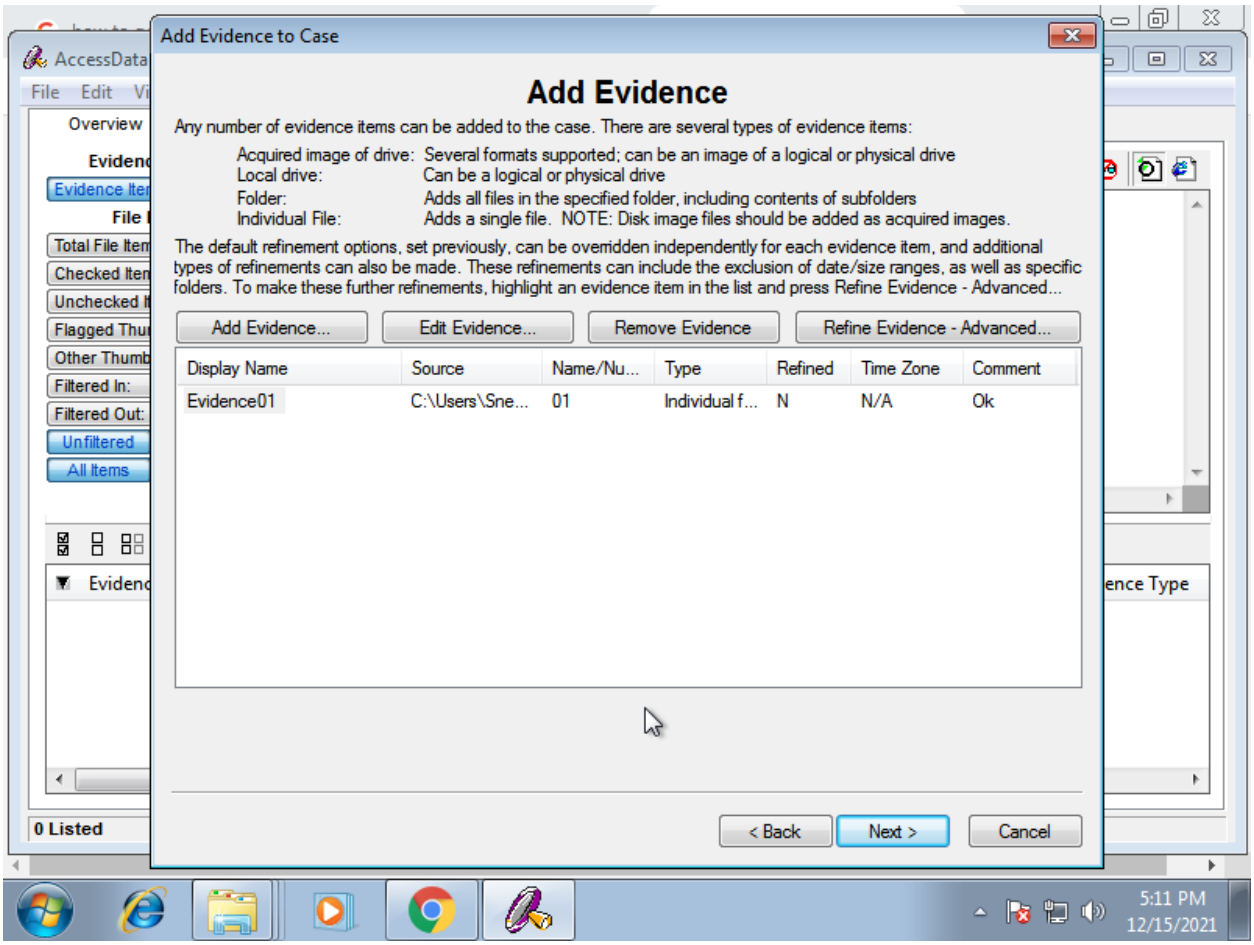


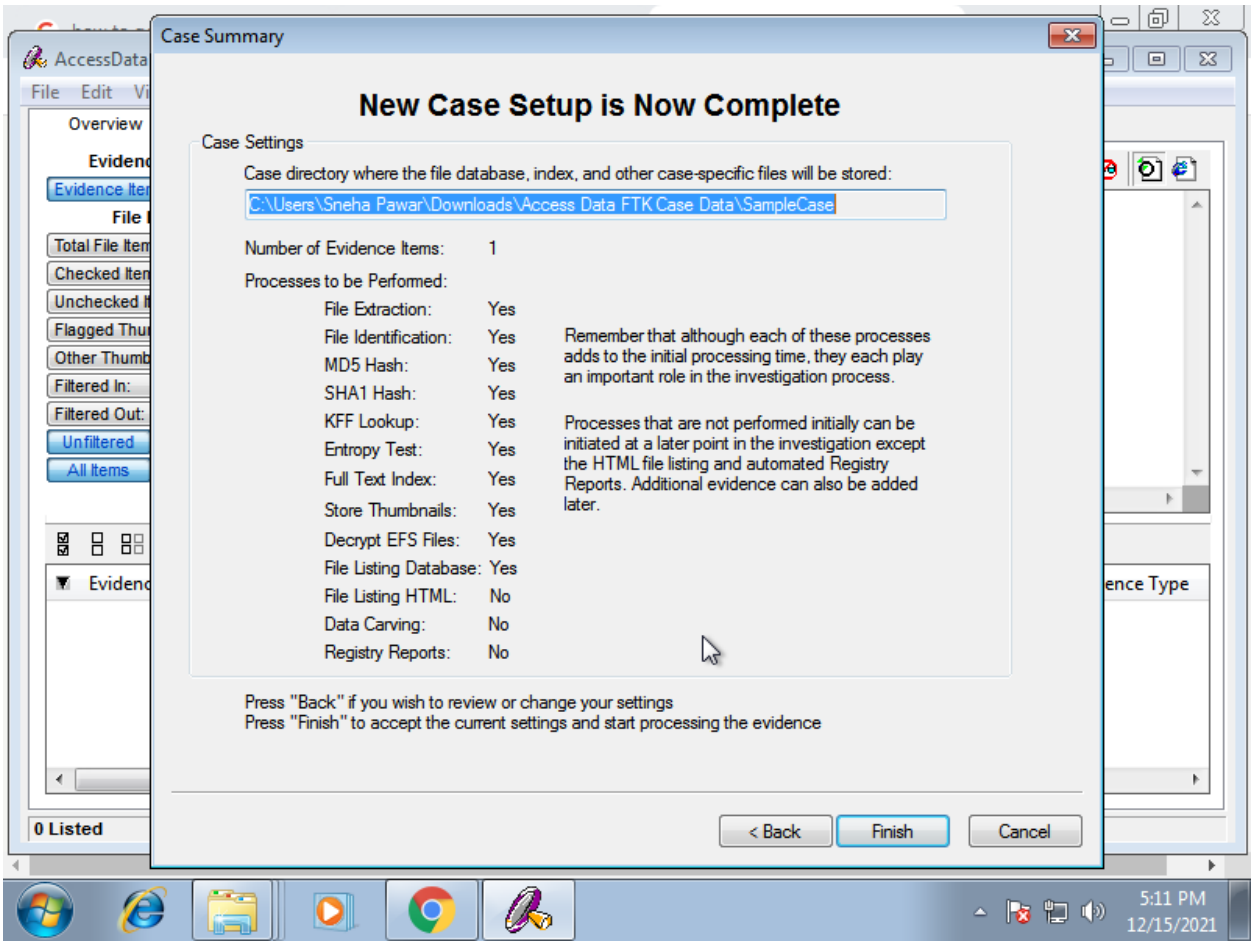
Then click on Add Evidence – Add Individual File.



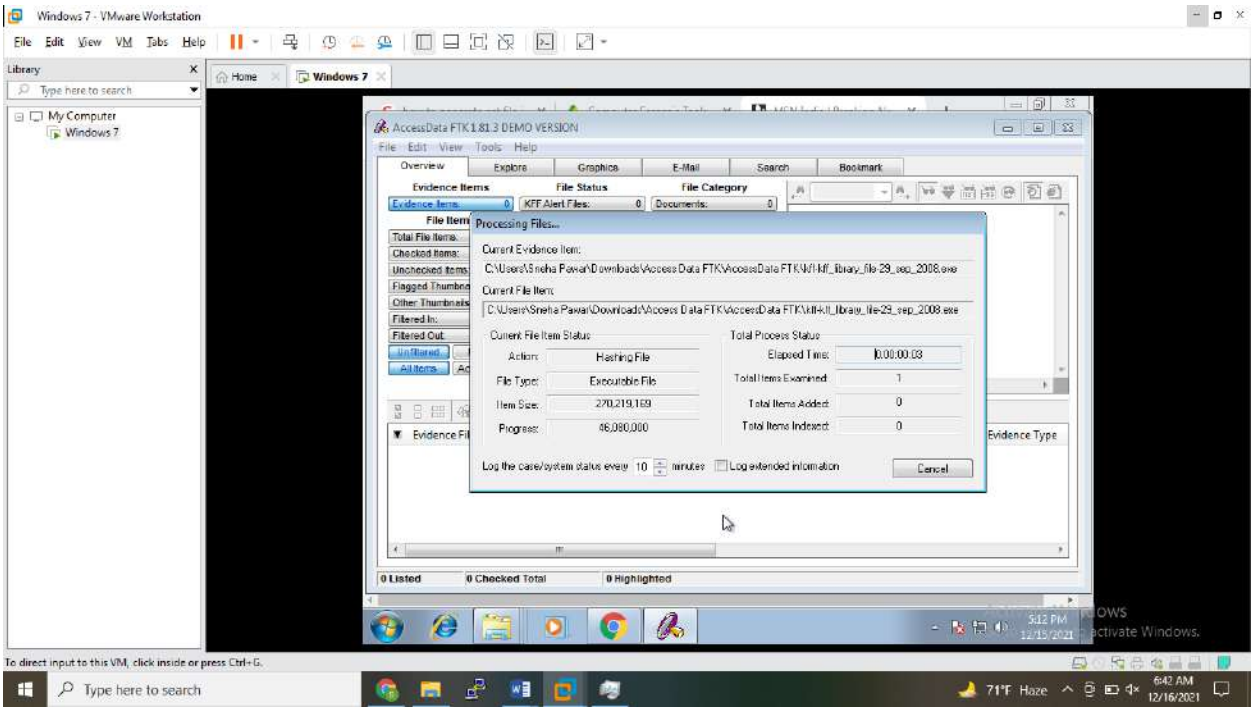
Then Browse for Evidence location, and enter other details.

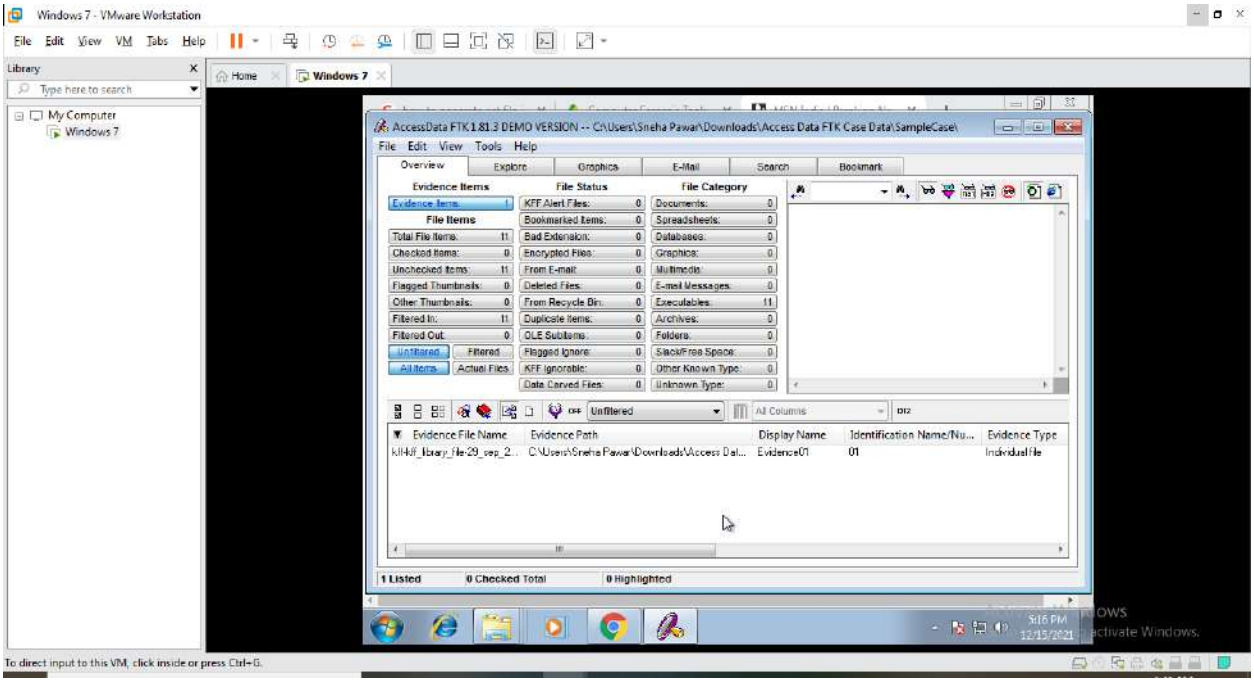


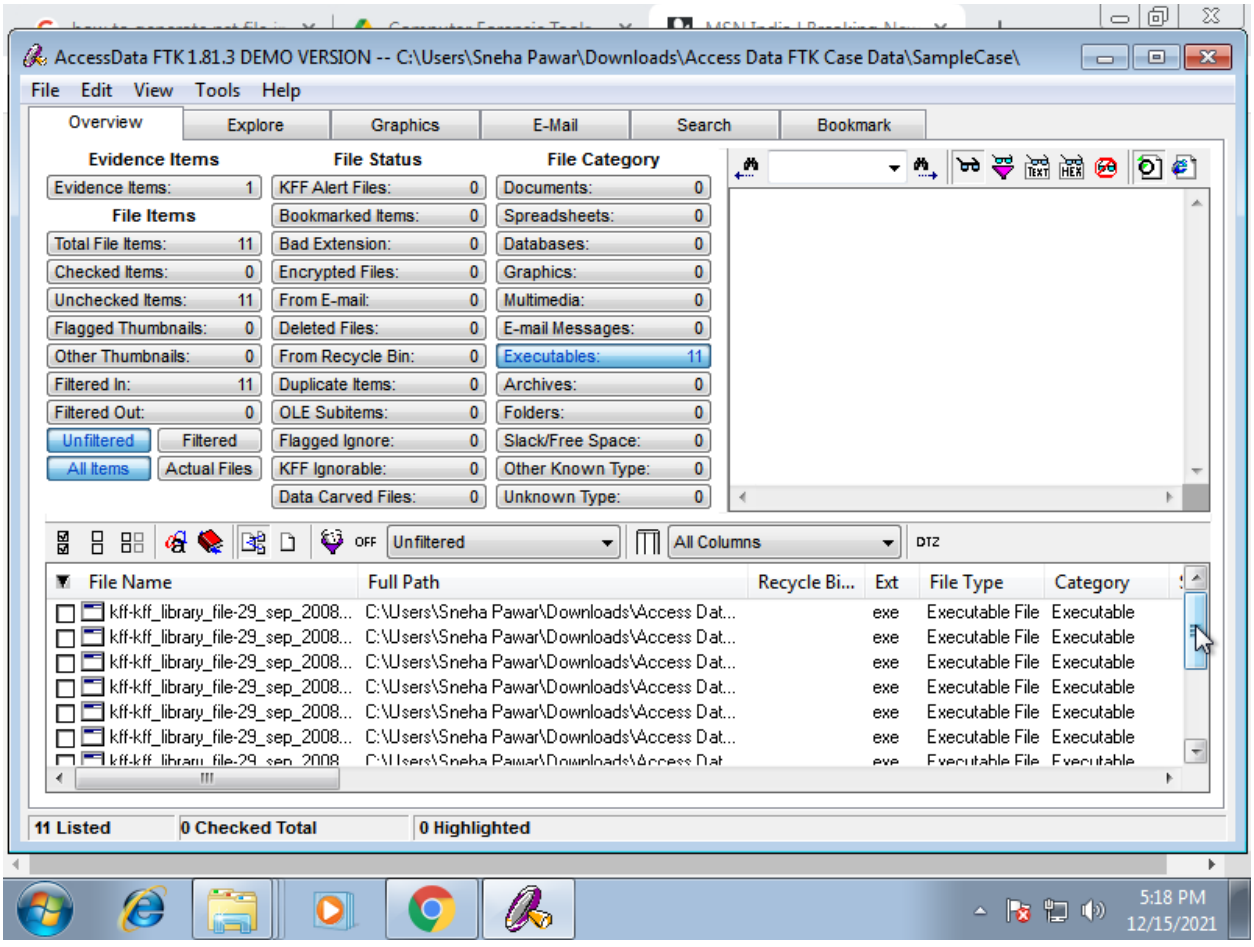

Add Evidence to Case
Add Evidence
Any number of evidence items can be added to the case. There are several types of evidence items:
Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
Local drive: Can be a logical or physical drive
Folder: Adds all files in the specified folder, including contents of subfolders
Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.
The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...
Add Evidence...
Edit Evidence...
Remove Evidence
Refine Evidence - Advanced...
Display Name
Source
Name/Nu...
Type
Refined
Time Zone
Comment
Evidence01
C:\Users\Sne...
01
Individual f...
N
N/A
Ok
< Back
Next >
Cancel
0 Listed
5:11 PM
12/15/2021



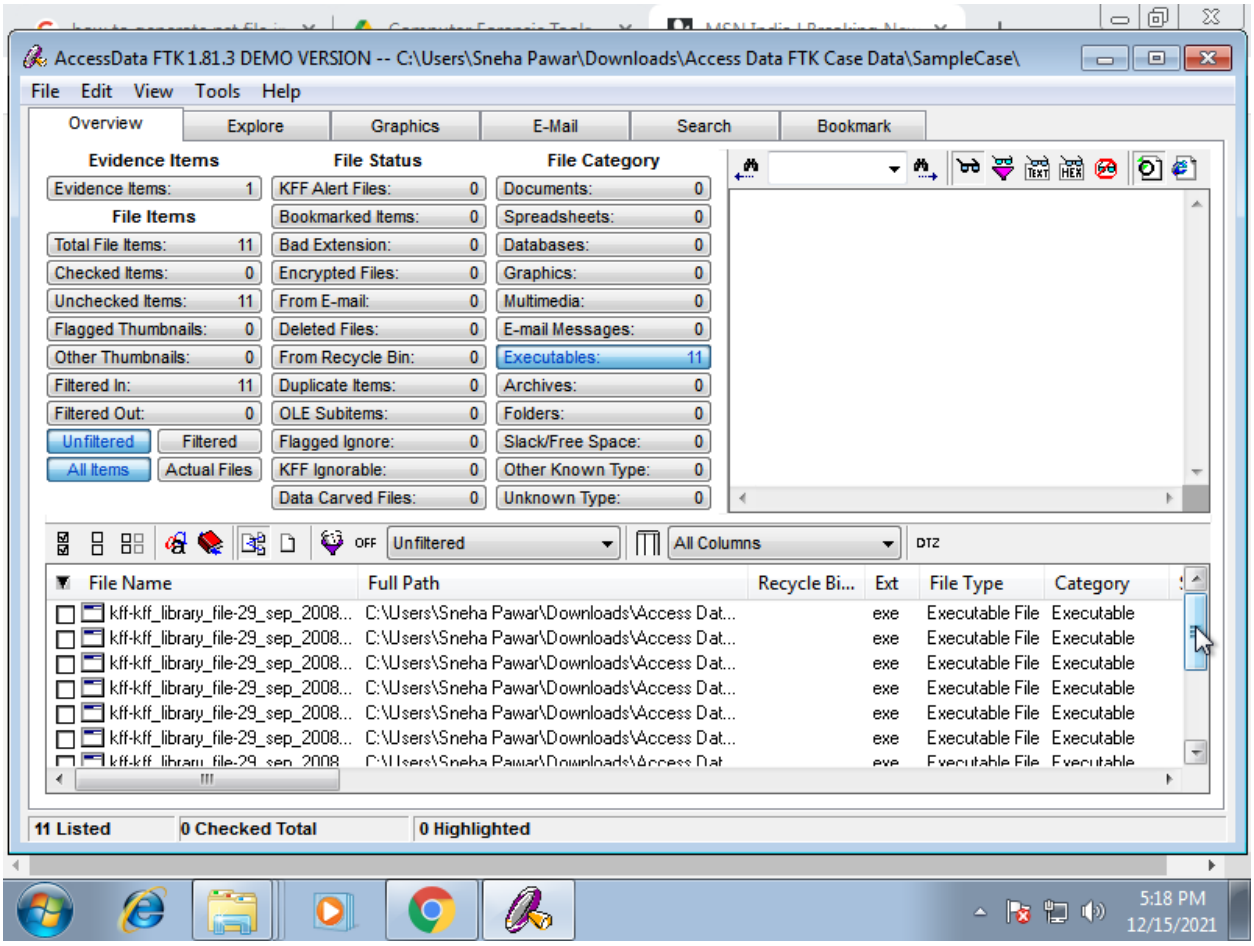
Click on Finish. It will start processing the File.

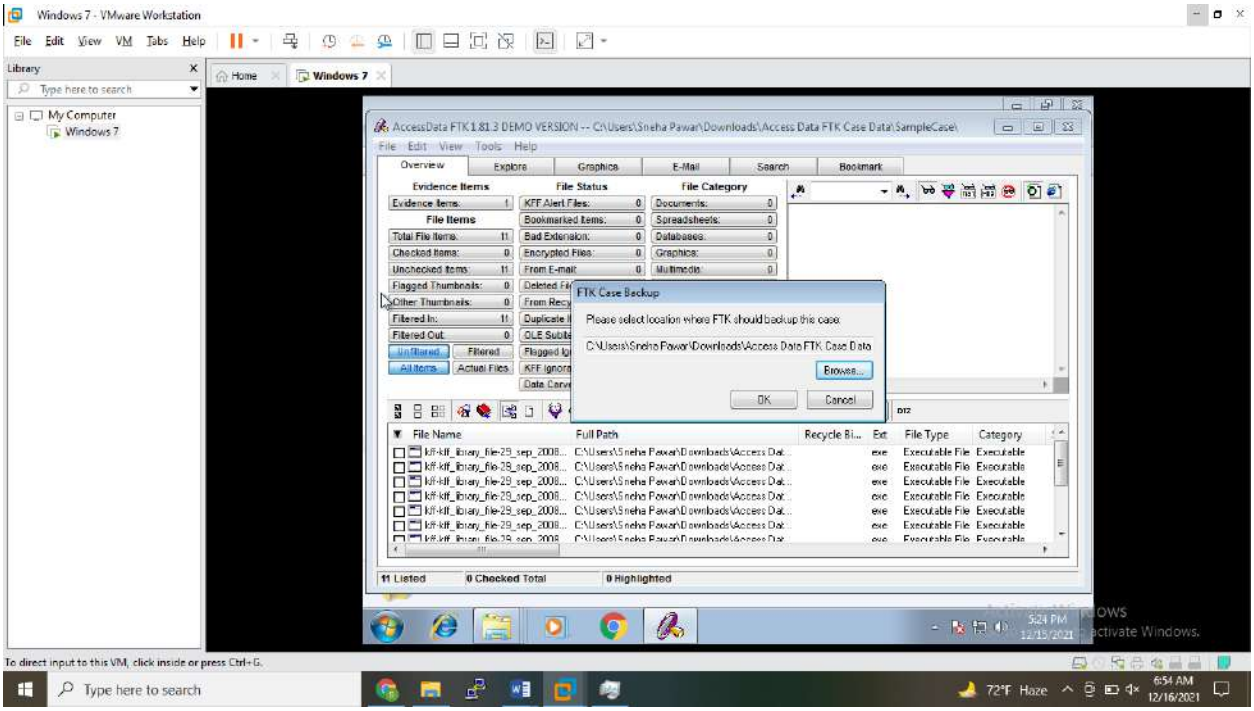


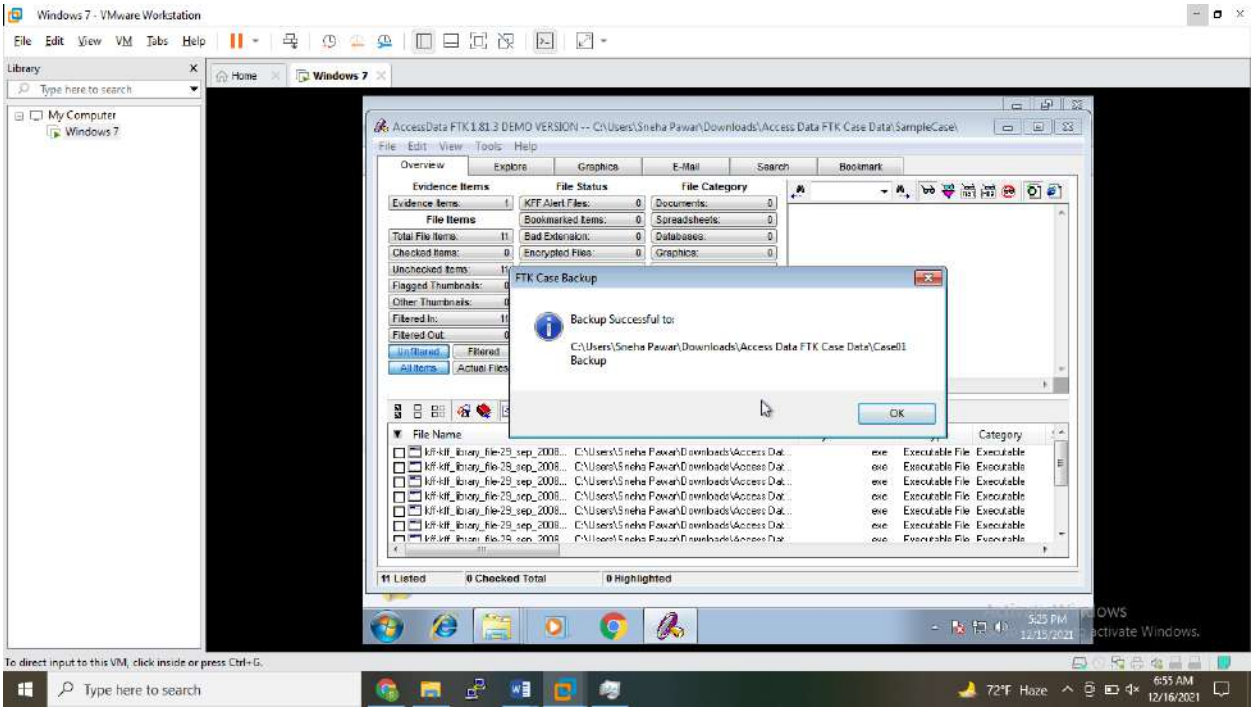

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Evidence Items
File Status
File Category
Evidence Items: 1
File Items
Total File Items: 11
Checked Items: 0
Unchecked Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 11
Filtered Out: 0
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 0
Encrypted Files: 0
From E-mail: 0
Deleted Files: 0
From Recycle Bin: 0
Duplicate Items: 0
OLE Subitems: 0
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0
Documents: 0
Spreadsheets: 0
Databases: 0
Graphics: 0
Multimedia: 0
E-mail Messages: 0
Executables: 11
Archives: 0
Folders: 0
Slack/Free Space: 0
Other Known Type: 0
Unknown Type: 0
Unfiltered
Filtered
All Items
Actual Files
Unfiltered
All Columns
DTZ
Evidence File Name
Evidence Path
Display Name
Identification Name/Nu...
Evidence Type
kff-kff_library_file-29_sep_2...
C:\Users\Sneha Pawar\Downloads\Access Dat...
Evidence01
01
Individual File
1 Listed
0 Checked Total
0 Highlighted
5:16 PM
12/15/2021
To direct input to this VM, click inside or press Ctrl+G.


AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Evidence Items
File Status
File Category
Evidence Items: 1
File Items
Total File Items: 11
Checked Items: 0
Unchecked Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 11
Filtered Out: 0
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 0
Encrypted Files: 0
From E-mail: 0
Deleted Files: 0
From Recycle Bin: 0
Duplicate Items: 0
OLE Subitems: 0
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0
Documents: 0
Spreadsheets: 0
Databases: 0
Graphics: 0
Multimedia: 0
E-mail Messages: 0
Executables: 11
Archives: 0
Folders: 0
Slack/Free Space: 0
Other Known Type: 0
Unknown Type: 0
Unfiltered
Filtered
All Items
Actual Files
OFF
Unfiltered
All Columns
DTZ
File Name
Full Path
Recycle Bi...
Ext
File Type
Category
kff-kff_library_file-29_sep_2008...
C:\Users\Sneha Pawar\Downloads\Access Dat...
exe
Executable File
Executable
11 Listed
0 Checked Total
0 Highlighted
5:18 PM
12/15/2021

To take backup of your case, Click on File – Backup Case – And browse for location where you want to take backup.

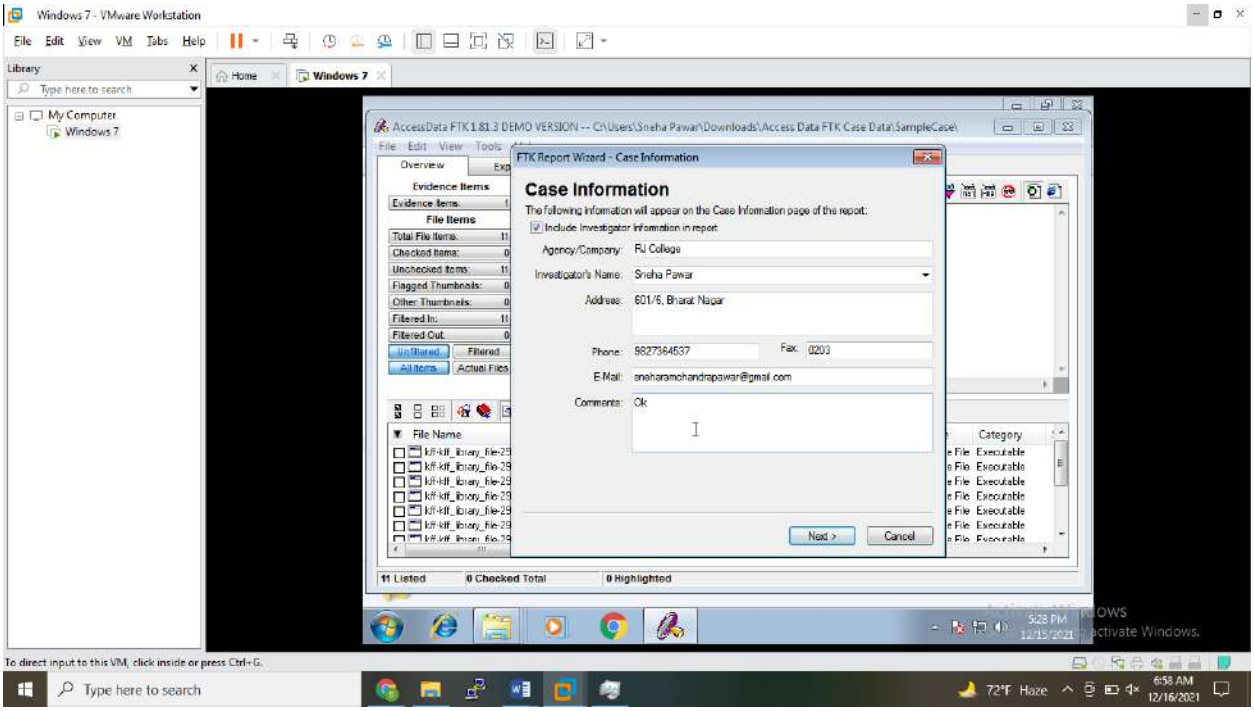


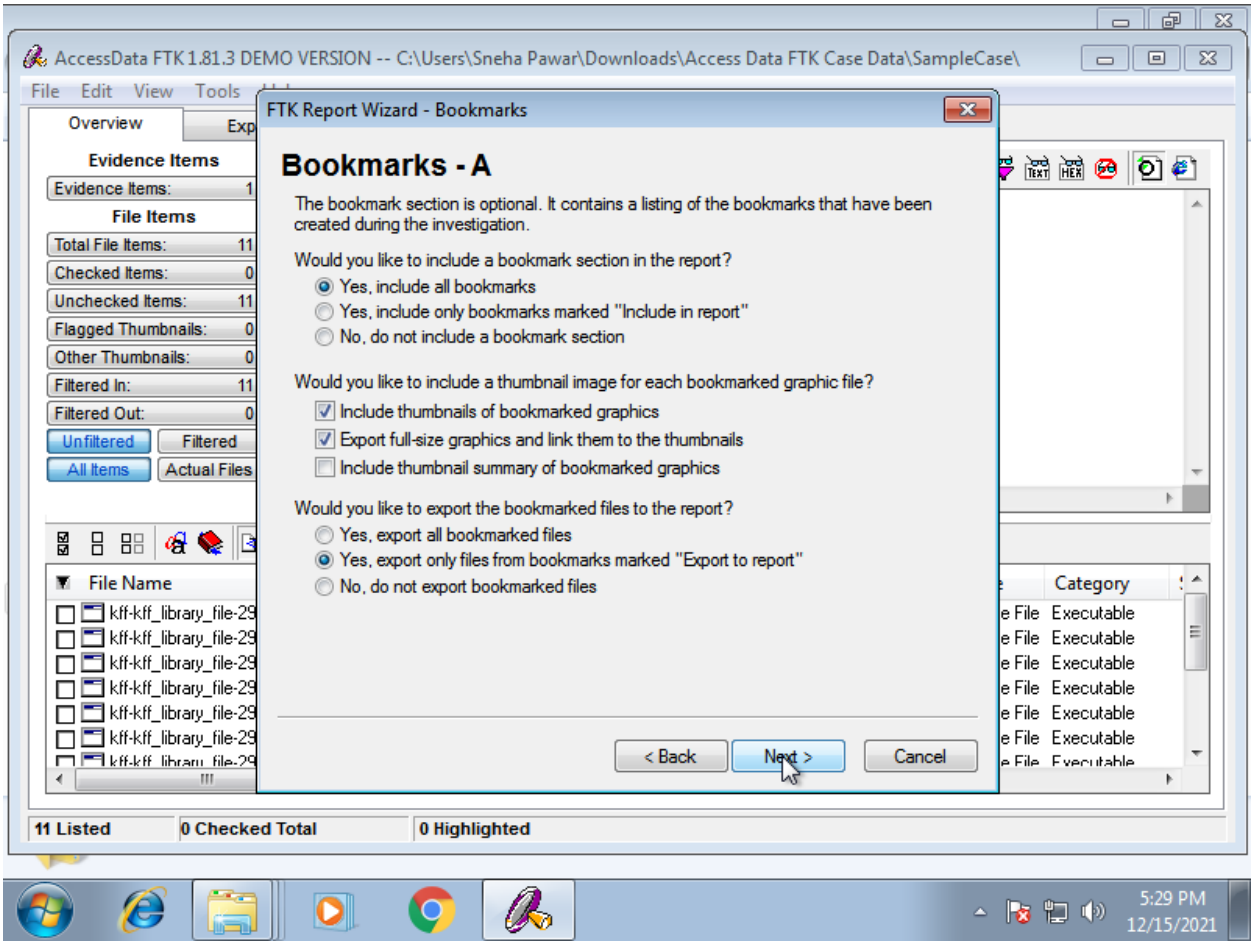


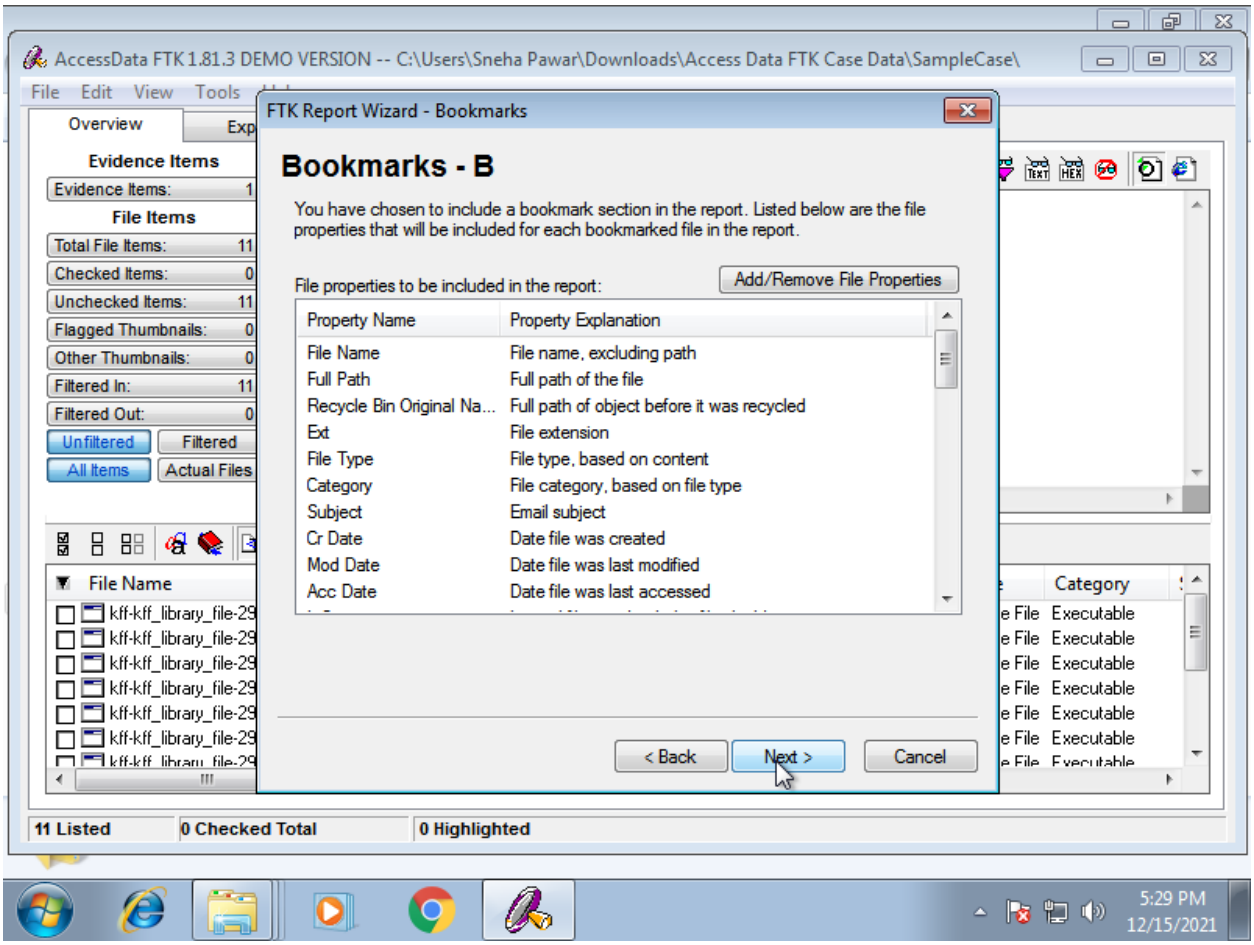


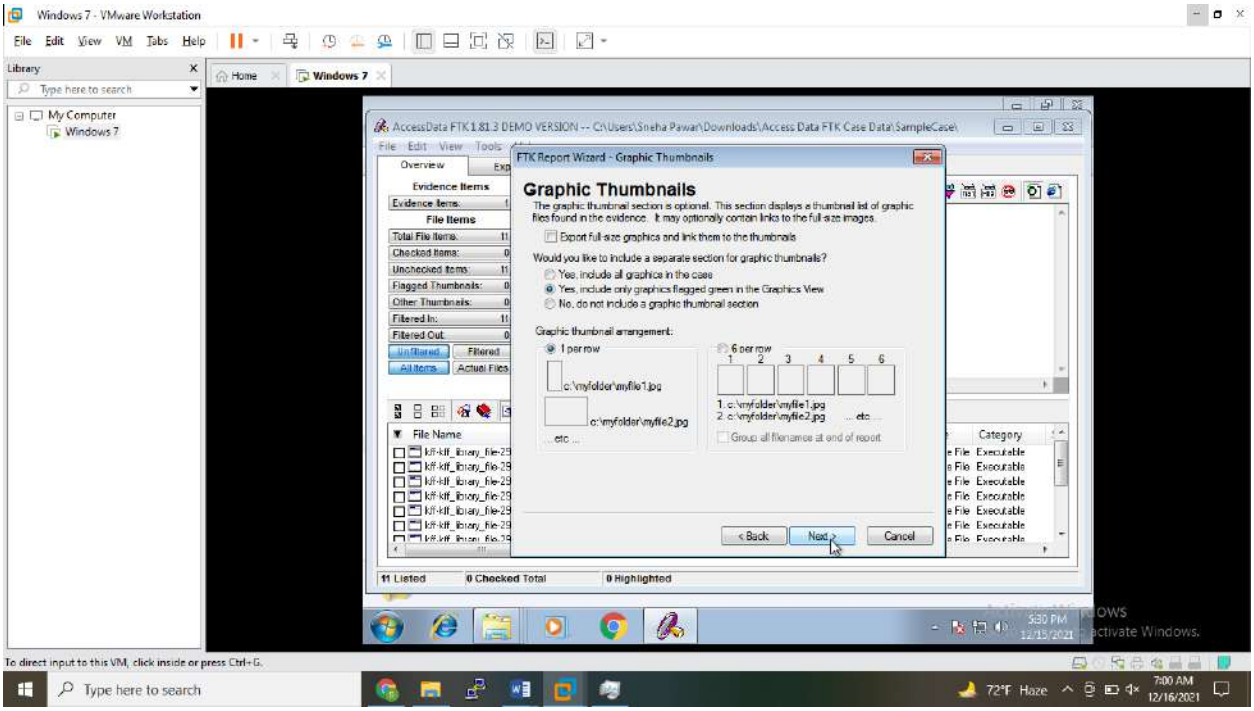
Then click on File - Report Wizard.

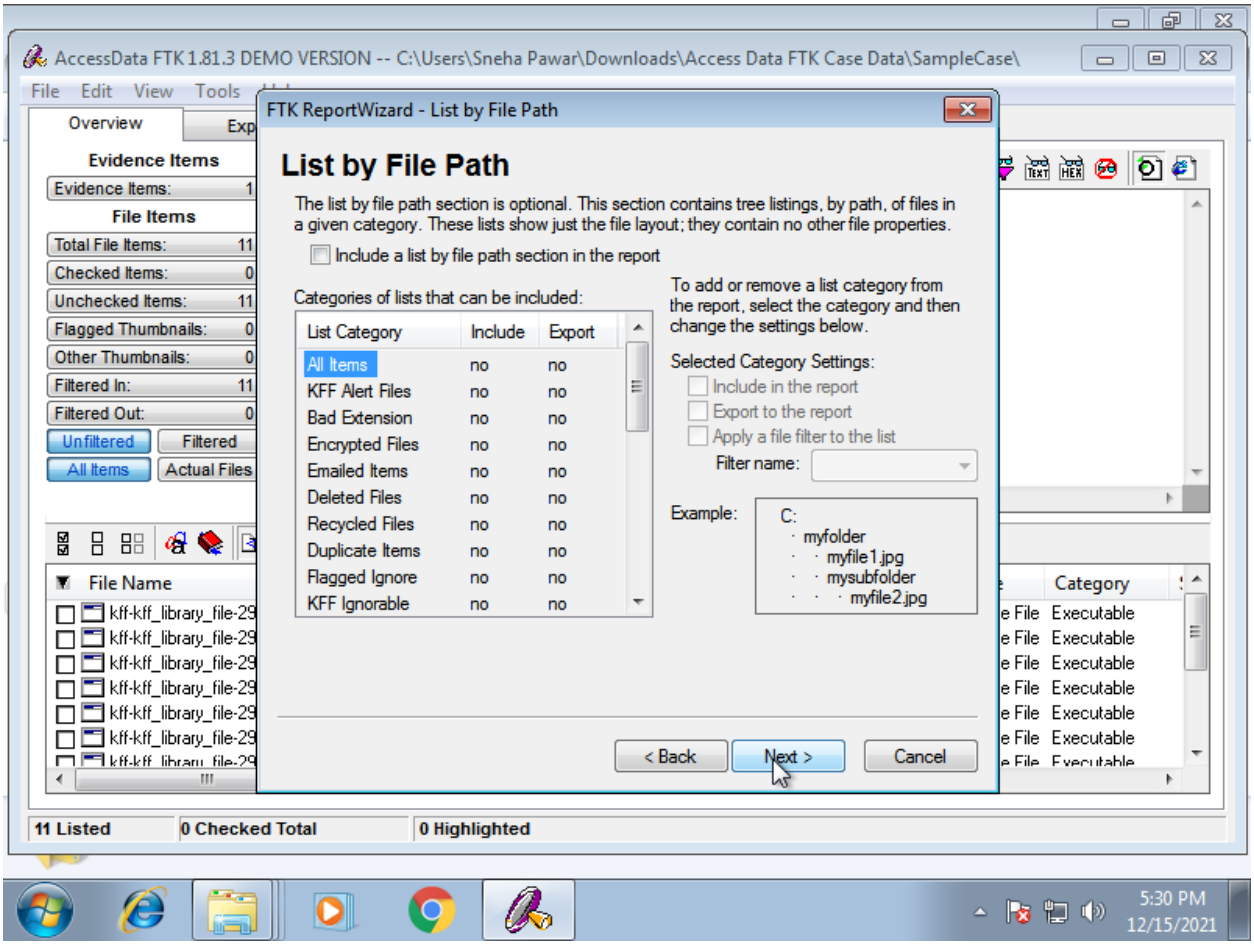
Fill the details. And click on Next.

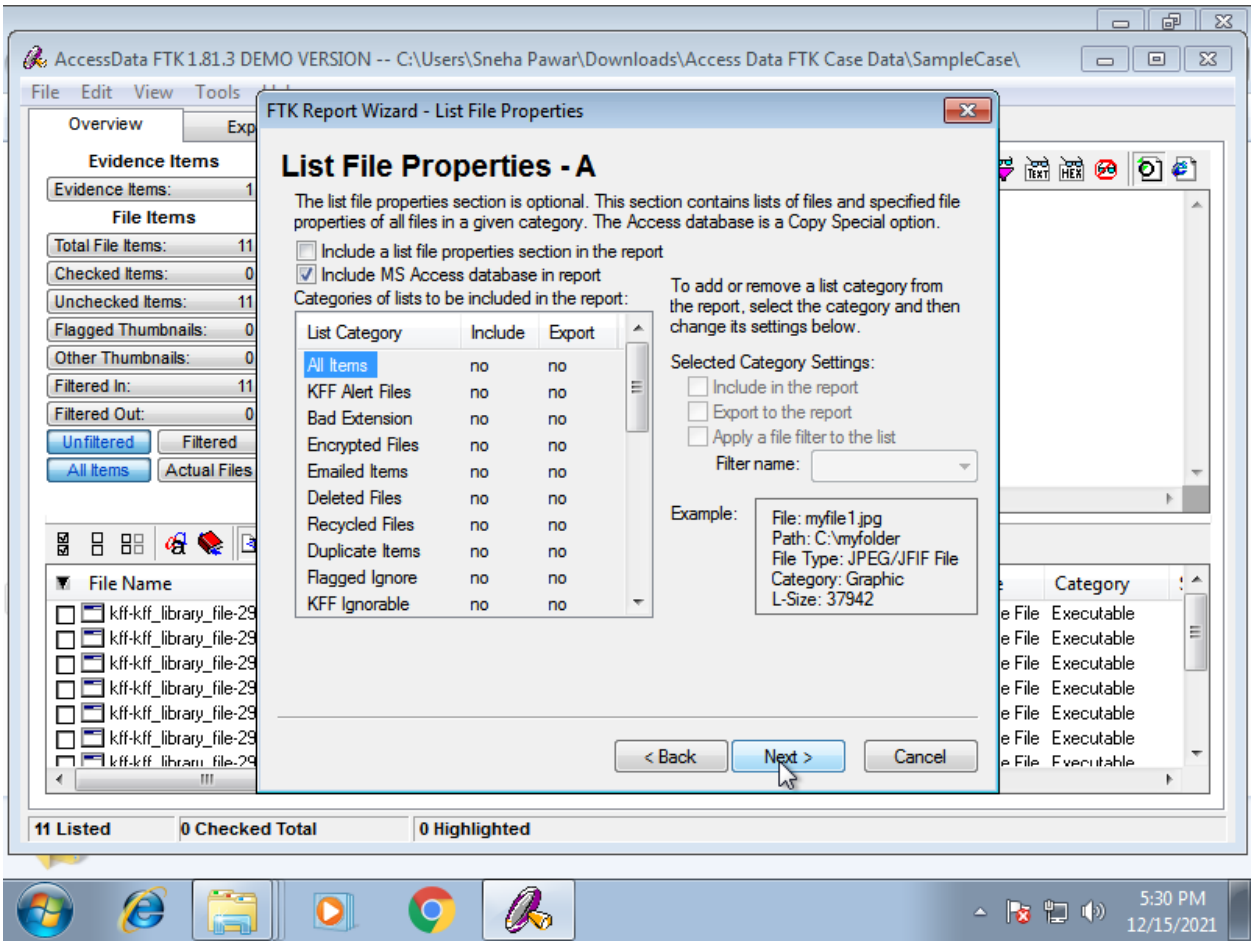

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools
Overview
Evidence Items
File Items
FTK Report Wizard - Case Information
Case Information
The following information will appear on the Case Information page of the report:
Include Investigator Information in report
Agency/Company: RJ College
Investigator's Name: Sneha Pawar
Address: 601/6, Bharat Nagar
Phone: 9827364537
Fax: 0203
E-Mail: sneharamchandrapawar@gmail.com
Comments: Ok
Next >
Cancel
11 Listed
0 Checked Total
0 Highlighted
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
72°F Haze
6:58 AM
12/16/2021

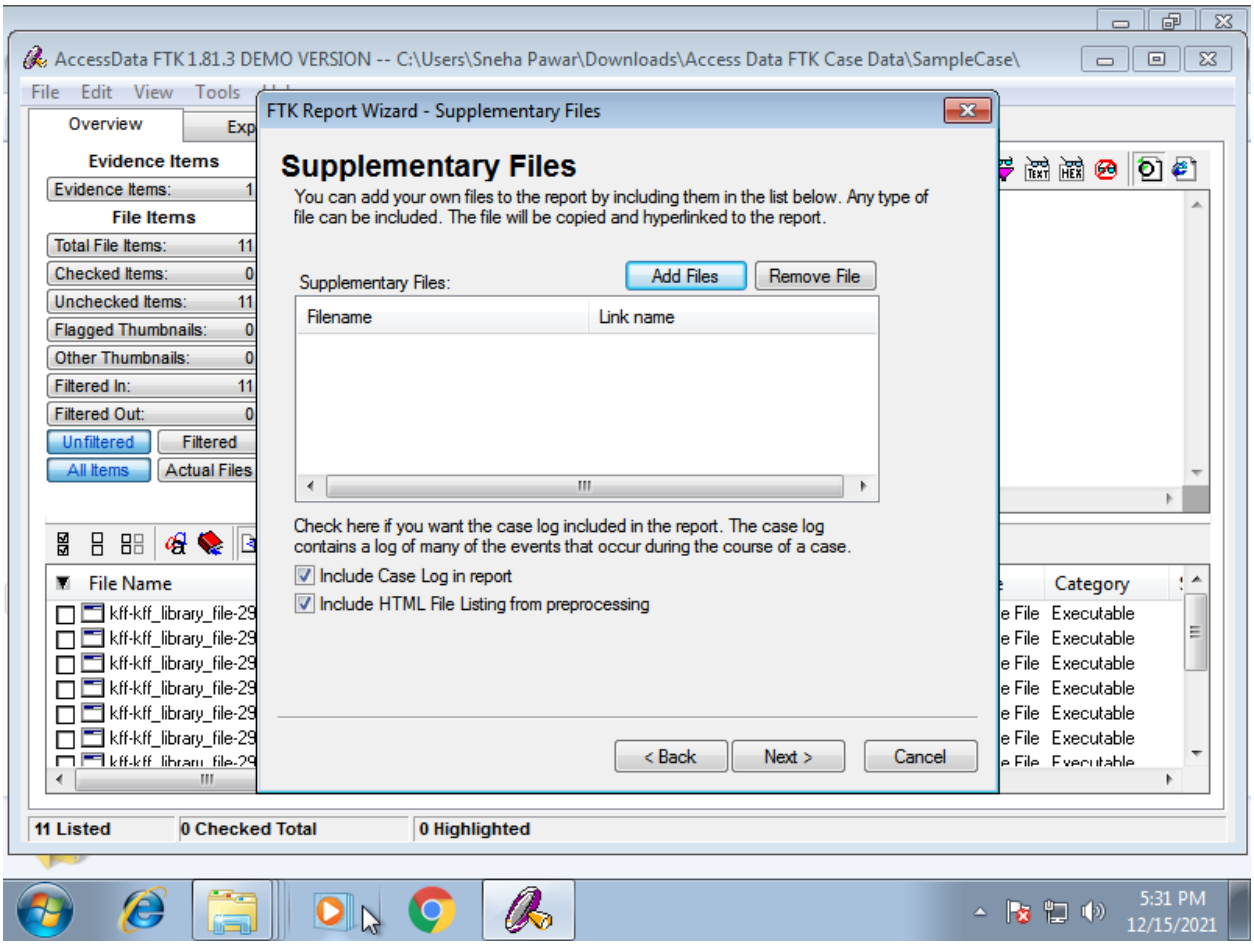

AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools
Overview
Evidence Items
Evidence Items: 1
File Items
Total File Items: 11
Checked Items: 0
Unchecked Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 11
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
File Name
kff-kff_library_file-29
Category
e File Executable
FTK Report Wizard - Bookmarks
Bookmarks - A
The bookmark section is optional. It contains a listing of the bookmarks that have been created during the investigation.
Would you like to include a bookmark section in the report?
Yes, include all bookmarks
Yes, include only bookmarks marked "Include in report"
No, do not include a bookmark section
Would you like to include a thumbnail image for each bookmarked graphic file?
Include thumbnails of bookmarked graphics
Export full-size graphics and link them to the thumbnails
Include thumbnail summary of bookmarked graphics
Would you like to export the bookmarked files to the report?
Yes, export all bookmarked files
Yes, export only files from bookmarks marked "Export to report"
No, do not export bookmarked files
< Back
Next >
Cancel
11 Listed
0 Checked Total
0 Highlighted
5:29 PM
12/15/2021


AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools
Overview
Evidence Items
Evidence Items: 1
File Items
Total File Items: 11
Checked Items: 0
Unchecked Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 11
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
File Name
kff-kff_library_file-29
Category
e File Executable
FTK Report Wizard - Bookmarks
Bookmarks - B
You have chosen to include a bookmark section in the report. Listed below are the file properties that will be included for each bookmarked file in the report.
File properties to be included in the report:
Add/Remove File Properties
Property Name
Property Explanation
File Name
File name, excluding path
Full Path
Full path of the file
Recycle Bin Original Na...
Full path of object before it was recycled
Ext
File extension
File Type
File type, based on content
Category
File category, based on file type
Subject
Email subject
Cr Date
Date file was created
Mod Date
Date file was last modified
Acc Date
Date file was last accessed
< Back
Next >
Cancel
11 Listed
0 Checked Total
0 Highlighted
5:29 PM
12/15/2021

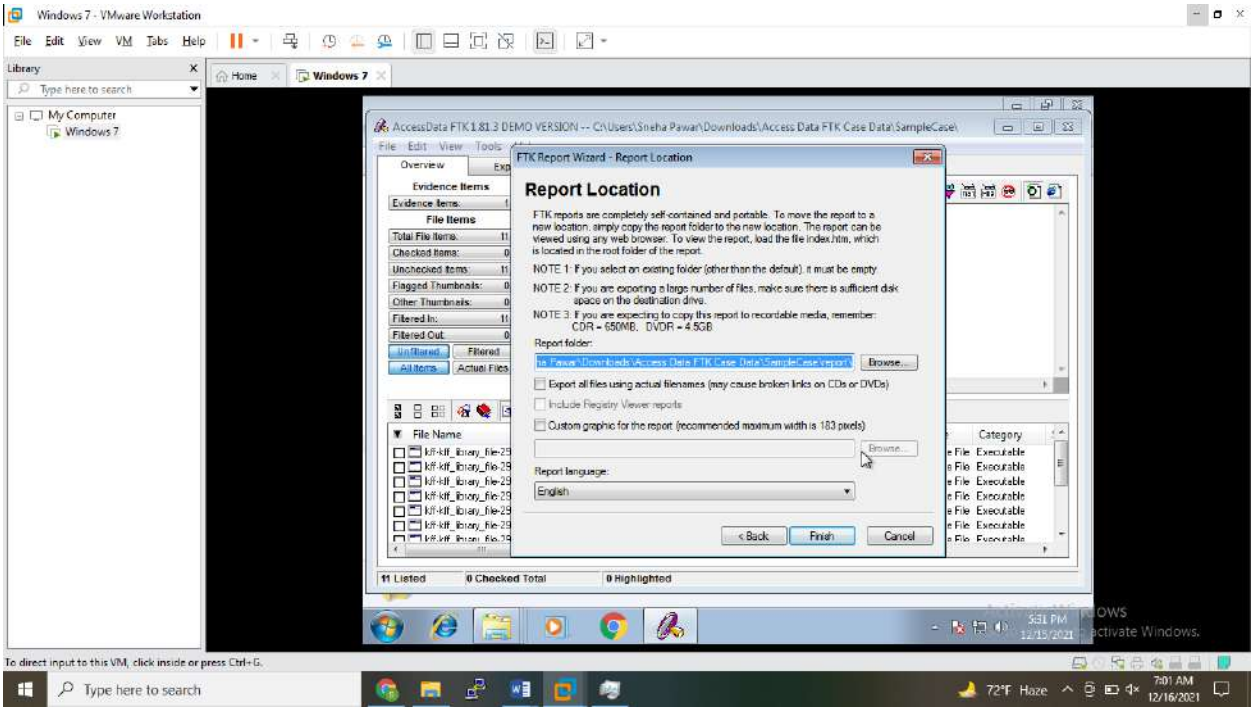

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools
Overview
Evidence Items
File Items
FTK Report Wizard - Graphic Thumbnails
Graphic Thumbnails
The graphic thumbnail section is optional. This section displays a thumbnail list of graphic files found in the evidence. It may optionally contain links to the full-size images.
Export full-size graphics and link them to the thumbnails
Would you like to include a separate section for graphic thumbnails?
Yes, include all graphics in the case
Yes, include only graphics flagged green in the Graphics View
No, do not include a graphic thumbnail section
Graphic thumbnail arrangement:
1 per row
6 per row
c:\myfolder\myfile1.jpg
c:\myfolder\myfile2.jpg
etc ...
1: c:\myfolder\myfile1.jpg
2: c:\myfolder\myfile2.jpg
Group all filenames at end of report
< Back
Next >
Cancel
File Name
Category
11 Listed
0 Checked Total
0 Highlighted
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
72°F Haze
7:00 AM
12/16/2021

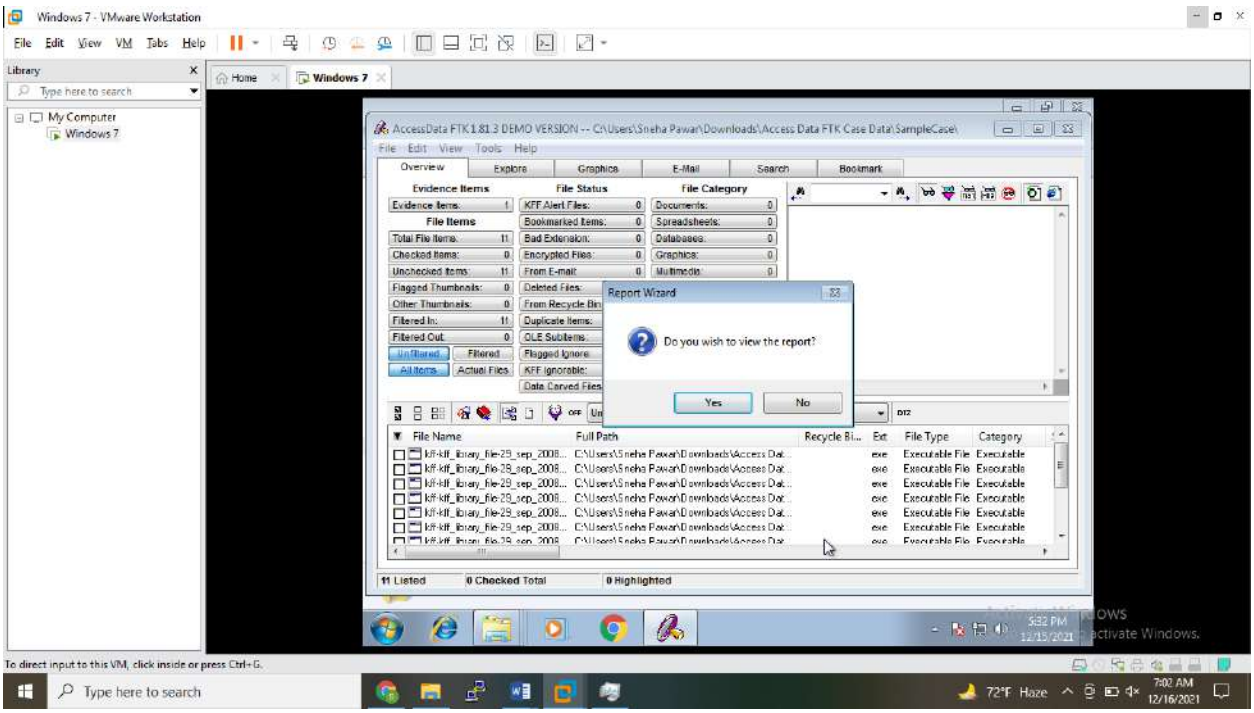

AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools
Overview
Evidence Items
Evidence Items: 1
File Items
Total File Items: 11
Checked Items: 0
Unchecked Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 11
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
File Name
kff-kff_library_file-29
FTK ReportWizard - List by File Path
List by File Path
The list by file path section is optional. This section contains tree listings, by path, of files in a given category. These lists show just the file layout; they contain no other file properties.
Include a list by file path section in the report
Categories of lists that can be included:
List Category | Include | Export
All Items | no | no
KFF Alert Files | no | no
Bad Extension | no | no
Encrypted Files | no | no
Emailed Items | no | no
Deleted Files | no | no
Recycled Files | no | no
Duplicate Items | no | no
Flagged Ignore | no | no
KFF Ignorable | no | no
To add or remove a list category from the report, select the category and then change the settings below.
Selected Category Settings:
Include in the report
Export to the report
Apply a file filter to the list
Filter name:
Example:
C:
myfolder
myfile1.jpg
mysubfolder
myfile2.jpg
< Back
Next >
Cancel
Category
e File Executable
11 Listed
0 Checked Total
0 Highlighted
5:30 PM
12/15/2021

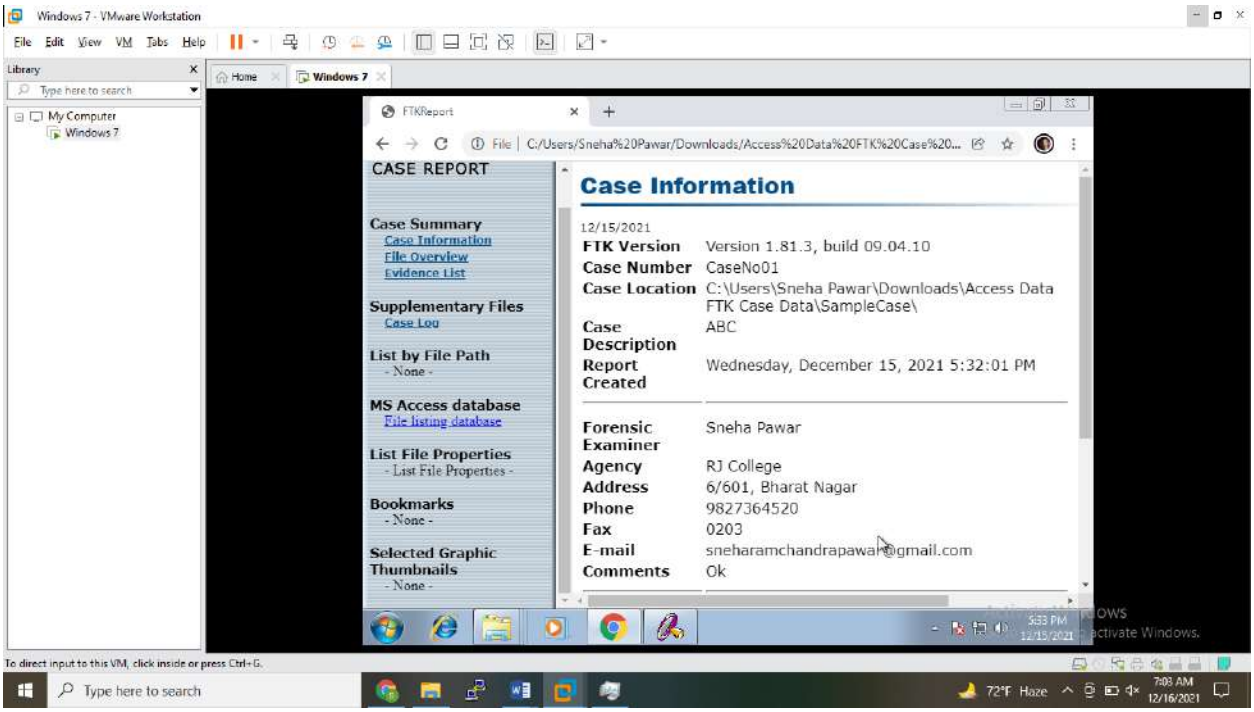

AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools
Overview
Evidence Items
Evidence Items: 1
File Items
Total File Items: 11
Checked Items: 0
Unchecked Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 11
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
File Name
Category
Executable
FTK Report Wizard - List File Properties
List File Properties - A
The list file properties section is optional. This section contains lists of files and specified file properties of all files in a given category. The Access database is a Copy Special option.
Include a list file properties section in the report
Include MS Access database in report
Categories of lists to be included in the report:
List Category
Include
Export
All Items no no
KFF Alert Files no no
Bad Extension no no
Encrypted Files no no
Emailed Items no no
Deleted Files no no
Recycled Files no no
Duplicate Items no no
Flagged Ignore no no
KFF Ignorable no no
To add or remove a list category from the report, select the category and then change its settings below.
Selected Category Settings:
Include in the report
Export to the report
Apply a file filter to the list
Filter name:
Example:
File: myfile1.jpg
Path: C:\myfolder
File Type: JPEG/JFIF File
Category: Graphic
L-Size: 37942
< Back
Next >
Cancel
11 Listed
0 Checked Total
0 Highlighted
5:30 PM
12/15/2021

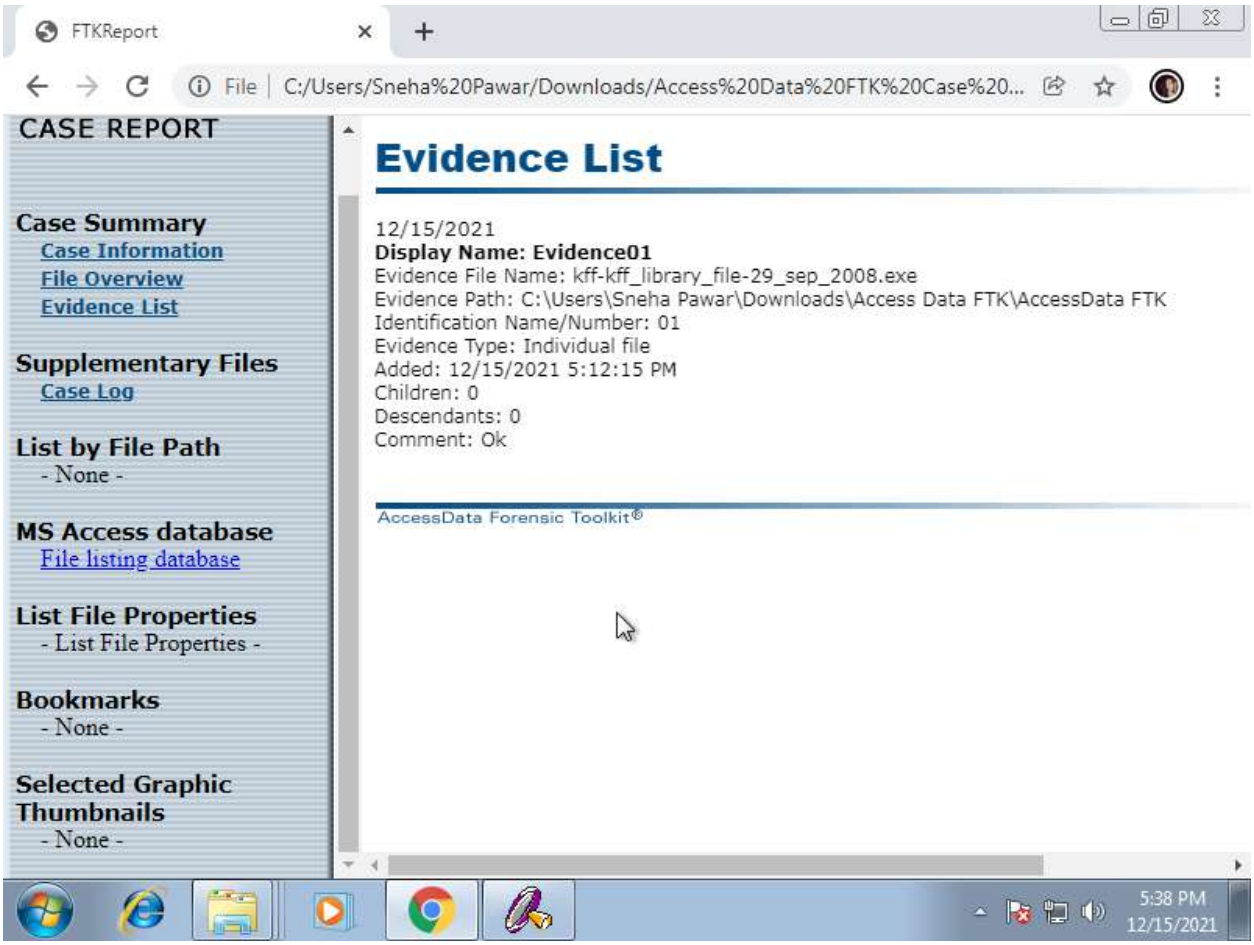


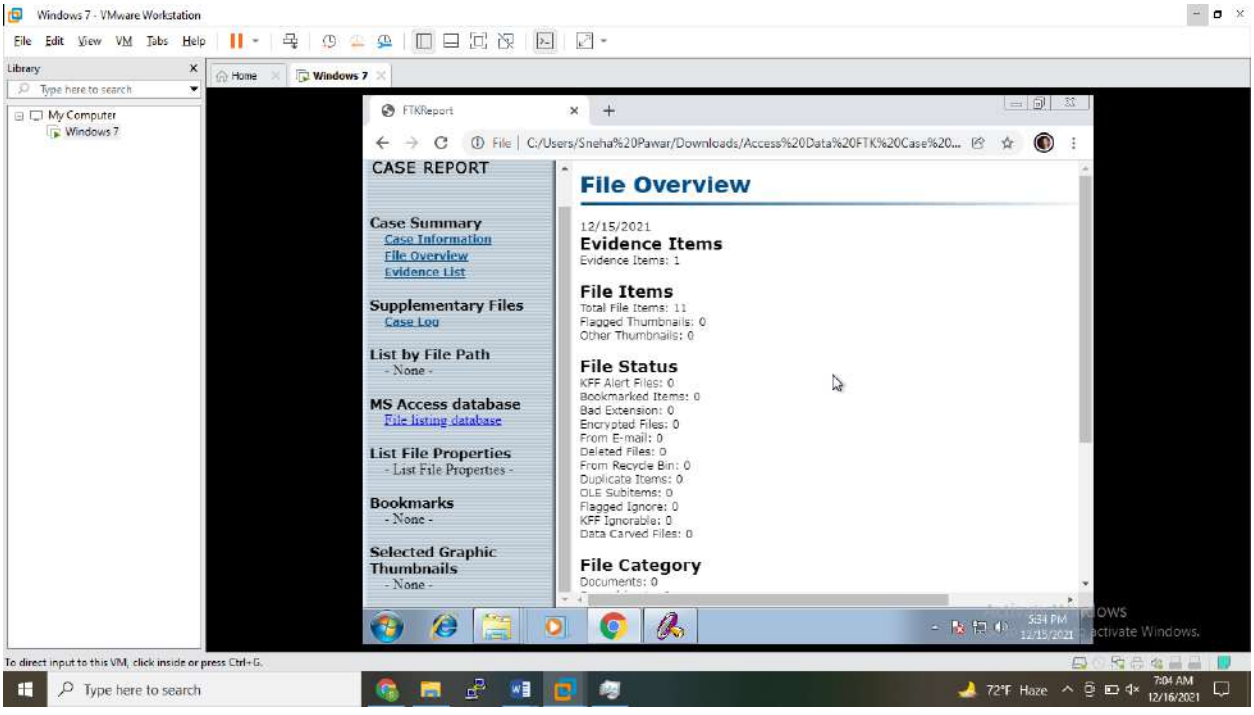
Enter report location.

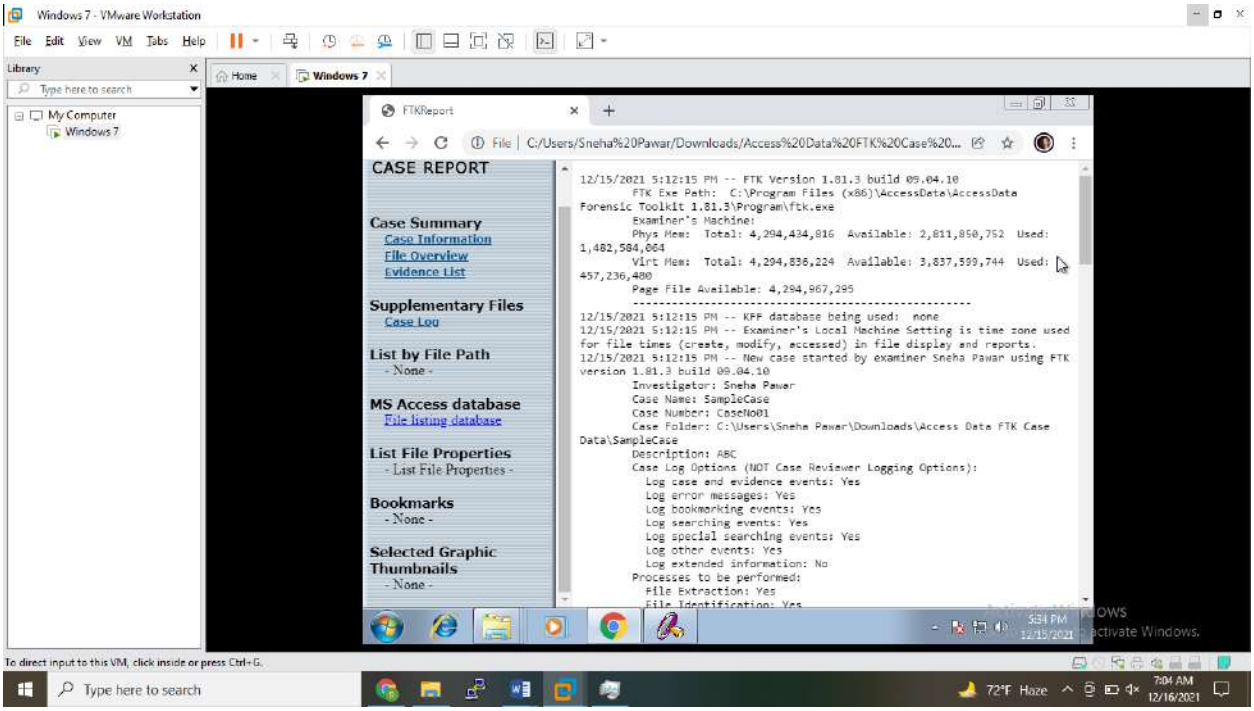

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools Help
Overview
Evidence Items
File Items
FTK Report Wizard - Report Location
Report Location
FTK reports are completely self-contained and portable. To move the report to a new location, simply copy the report folder to the new location. The report can be viewed using any web browser. To view the report, load the file index.htm, which is located in the root folder of the report.
NOTE 1: If you select an existing folder (other than the default), it must be empty.
NOTE 2: If you are exporting a large number of files, make sure there is sufficient disk space on the destination drive.
NOTE 3: If you are expecting to copy this report to recordable media, remember: CDR = 650MB; DVDR = 4.5GB
Report folder:
Browse...
Export all files using actual filenames (may cause broken links on CDs or DVDs)
Include Registry Viewer reports
Custom graphic for the report (recommended maximum width is 183 pixels)
Report language:
English
< Back
Finish
Cancel
11 Listed
0 Checked Total
0 Highlighted
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
72°F Haze
7:01 AM
12/16/2021


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Evidence Items
File Status
File Category
Report Wizard
Do you wish to view the report?
Yes
No
11 Listed
0 Checked Total
0 Highlighted
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
72°F Haze
7:02 AM
12/16/2021


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
FTKReport
File | C:/Users/Sneha%20Pawar/Downloads/Access%20Data%20FTK%20Case%20...
CASE REPORT
Case Summary
Case Information
File Overview
Evidence List
Supplementary Files
Case Log
List by File Path
- None -
MS Access database
File listing database
List File Properties
- List File Properties -
Bookmarks
- None -
Selected Graphic Thumbnails
- None -
Case Information
12/15/2021
FTK Version Version 1.81.3, build 09.04.10
Case Number CaseNo01
Case Location C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
Case Description ABC
Report Created Wednesday, December 15, 2021 5:32:01 PM
Forensic Examiner Sneha Pawar
Agency RJ College
Address 6/601, Bharat Nagar
Phone 9827364520
Fax 0203
E-mail sneharamchandrapawar@gmail.com
Comments Ok
5:33 PM
12/15/2021
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
72°F Haze
7:03 AM
12/16/2021

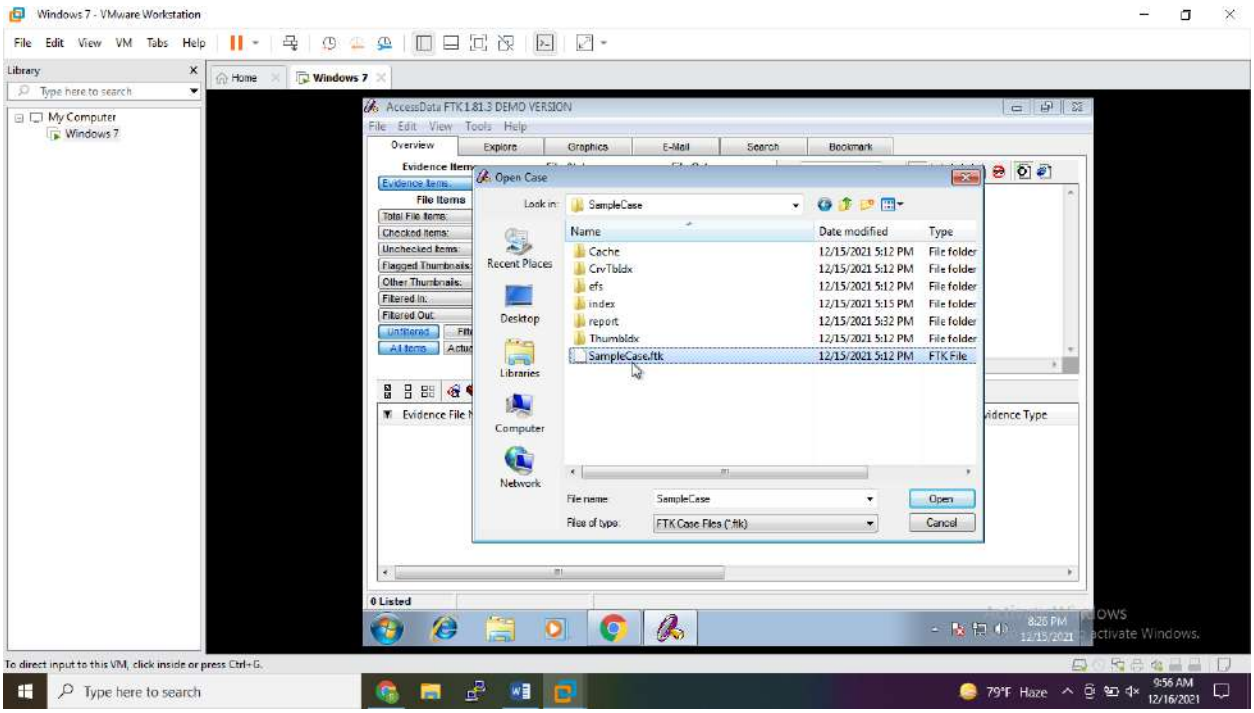

FTKReport
File | C:/Users/Sneha%20Pawar/Downloads/Access%20Data%20FTK%20Case%20...
CASE REPORT
Case Summary
Case Information
File Overview
Evidence List
Supplementary Files
Case Log
List by File Path
- None -
MS Access database
File listing database
List File Properties
- List File Properties -
Bookmarks
- None -
Selected Graphic Thumbnails
- None -
Evidence List
12/15/2021
Display Name: Evidence01
Evidence File Name: kff-kff_library_file-29_sep_2008.exe
Evidence Path: C:\Users\Sneha Pawar\Downloads\Access Data FTK\AccessData FTK
Identification Name/Number: 01
Evidence Type: Individual file
Added: 12/15/2021 5:12:15 PM
Children: 0
Descendants: 0
Comment: Ok
AccessData Forensic Toolkit®
5:38 PM
12/15/2021


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
FTKReport
File | C:/Users/Sneha%20Pawar/Downloads/Access%20Data%20FTK%20Case%20...
CASE REPORT
Case Summary
Case Information
File Overview
Evidence List
Supplementary Files
Case Log
List by File Path
- None -
MS Access database
File listing database
List File Properties
- List File Properties -
Bookmarks
- None -
Selected Graphic Thumbnails
- None -
File Overview
12/15/2021
Evidence Items
Evidence Items: 1
File Items
Total File Items: 11
Flagged Thumbnails: 0
Other Thumbnails: 0
File Status
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 0
Encrypted Files: 0
From E-mail: 0
Deleted Files: 0
From Recycle Bin: 0
Duplicate Items: 0
OLE Subitems: 0
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0
File Category
Documents: 0
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
72°F Haze
7:04 AM
12/16/2021



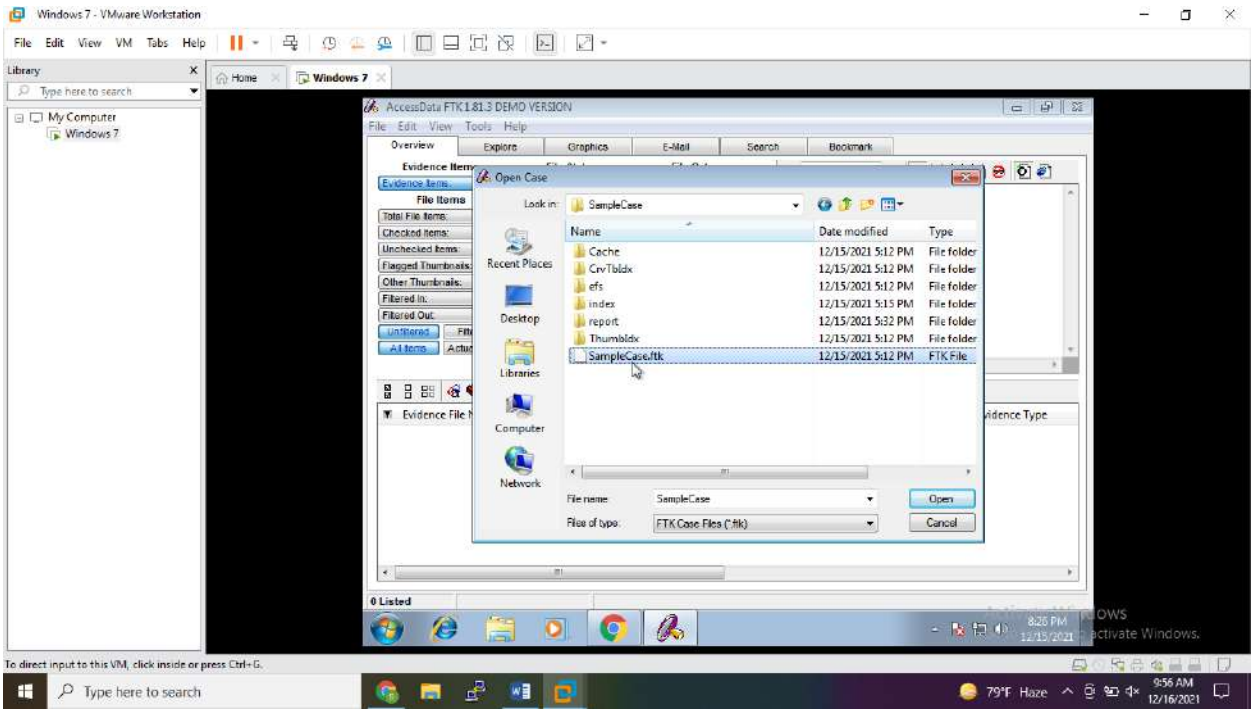
Now, let's perform Email Forensic on this. Open Existing Case that we have created.

File – Open Case

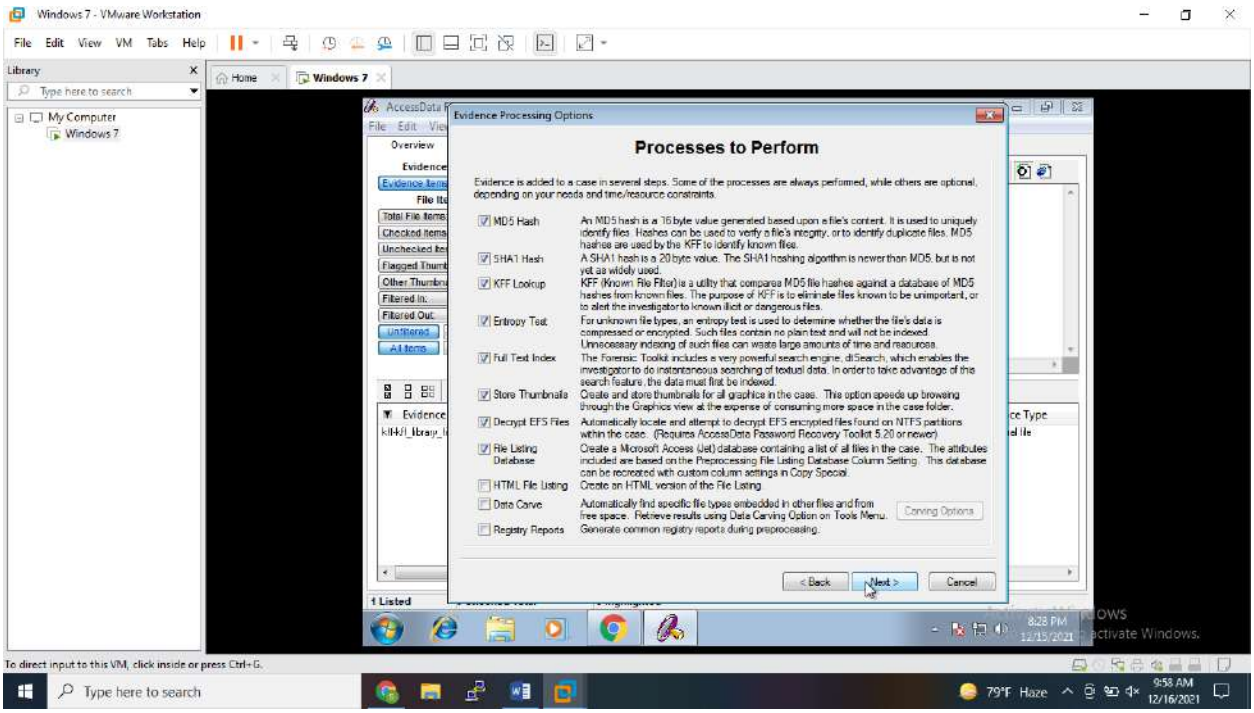


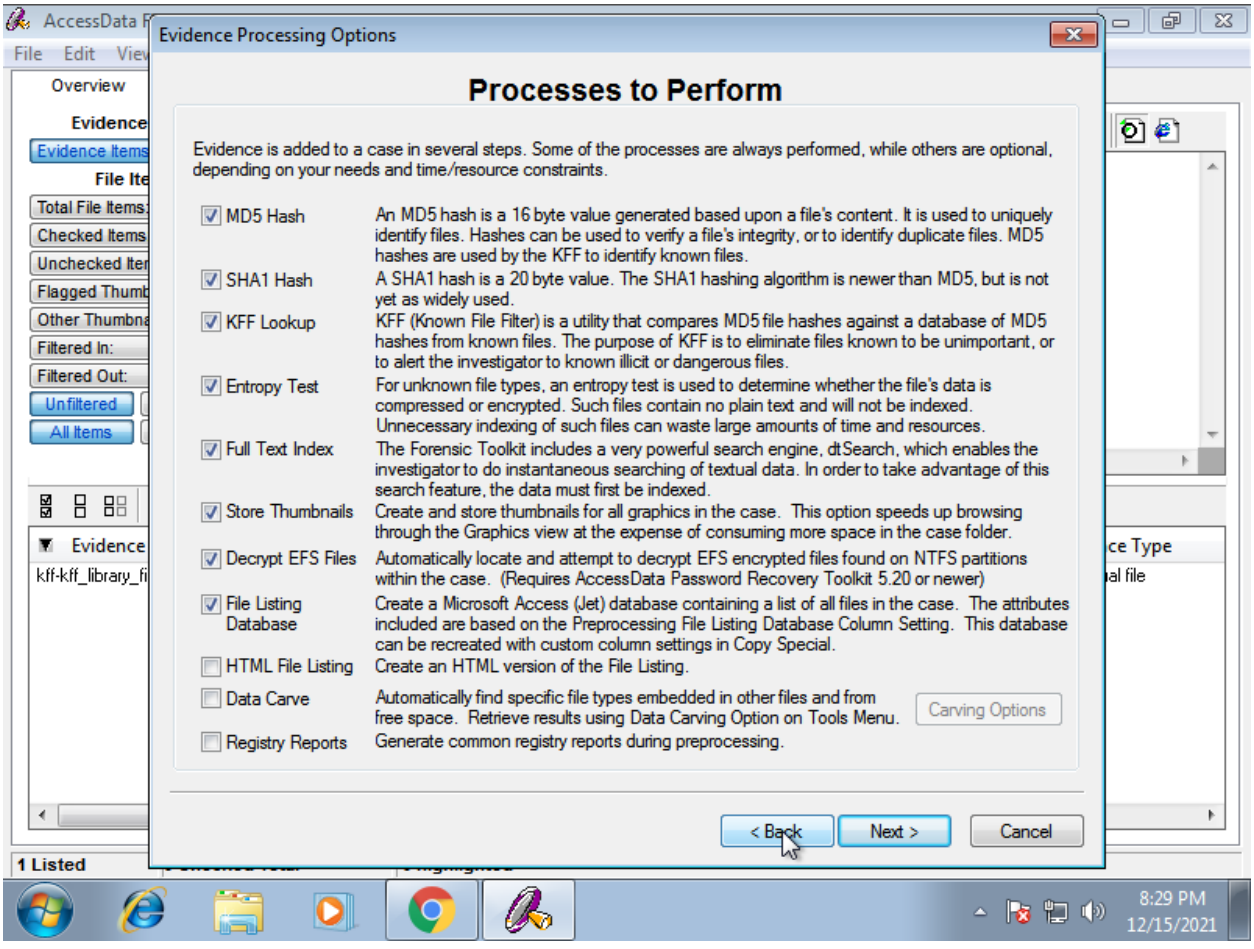
Now File – Add Evidence, and add Outlook's pst file.

Keep this by default.

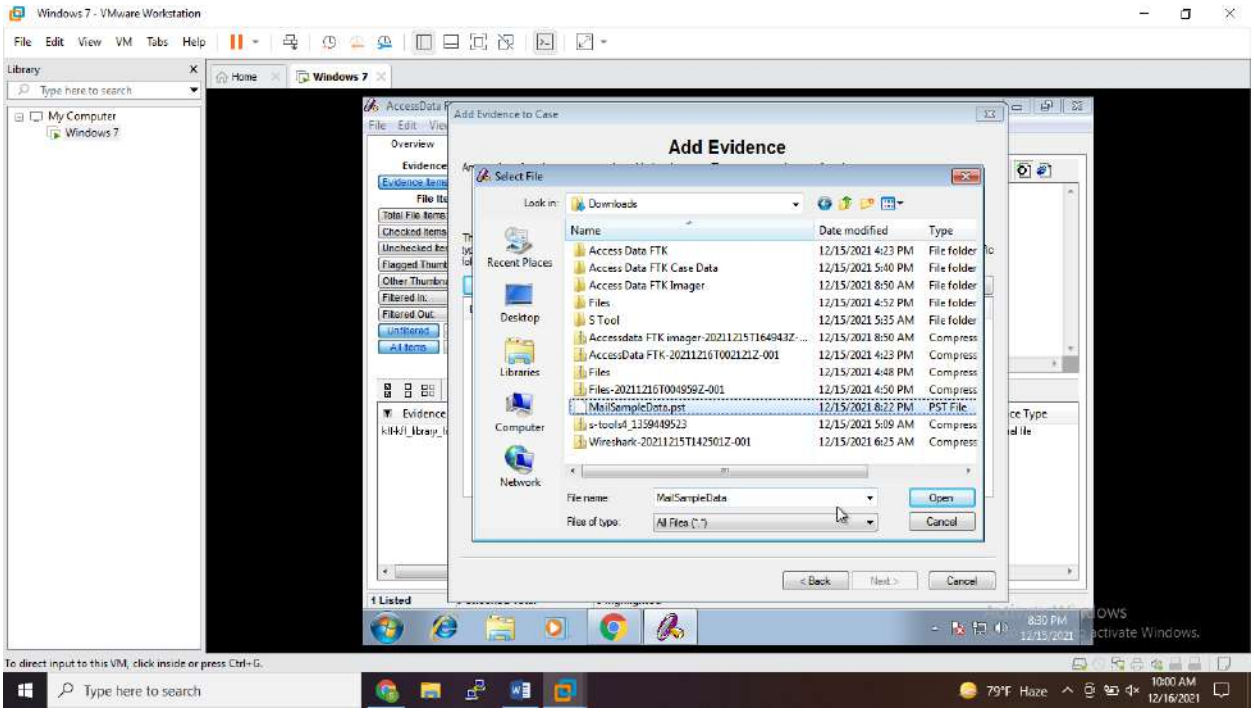


Click Next

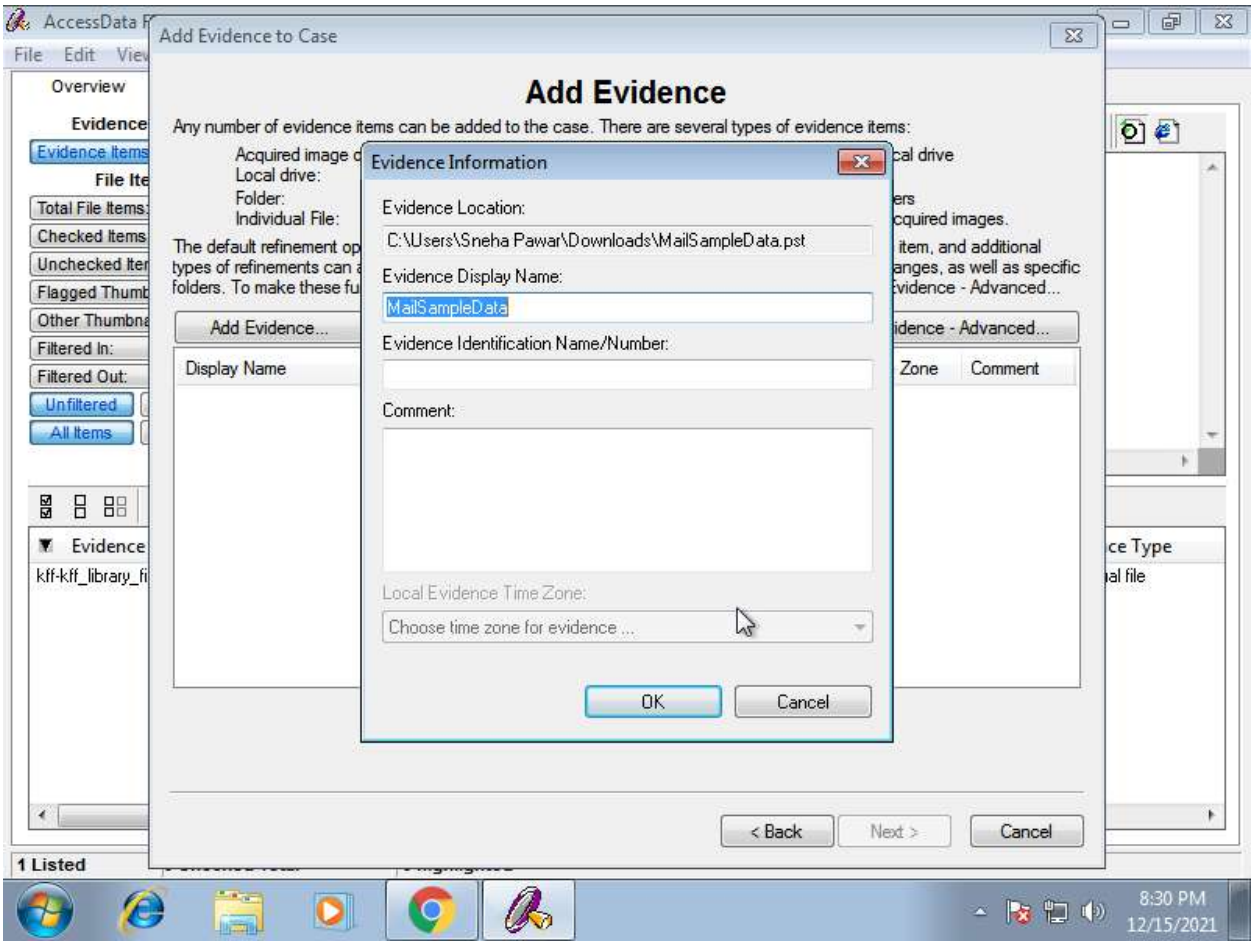

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
Evidence Processing Options
Processes to Perform
Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.
MD5 Hash
An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
SHA1 Hash
A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
KFF Lookup
KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
Entropy Test
For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.
Full Text Index
The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.
Store Thumbnails
Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.
Decrypt EFS Files
Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)
File Listing Database
Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special.
HTML File Listing
Create an HTML version of the File Listing.
Data Carve
Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.
Carving Options
Registry Reports
Generate common registry reports during preprocessing.
< Back
Next >
Cancel
1 Listed
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
9:58 AM
12/16/2021

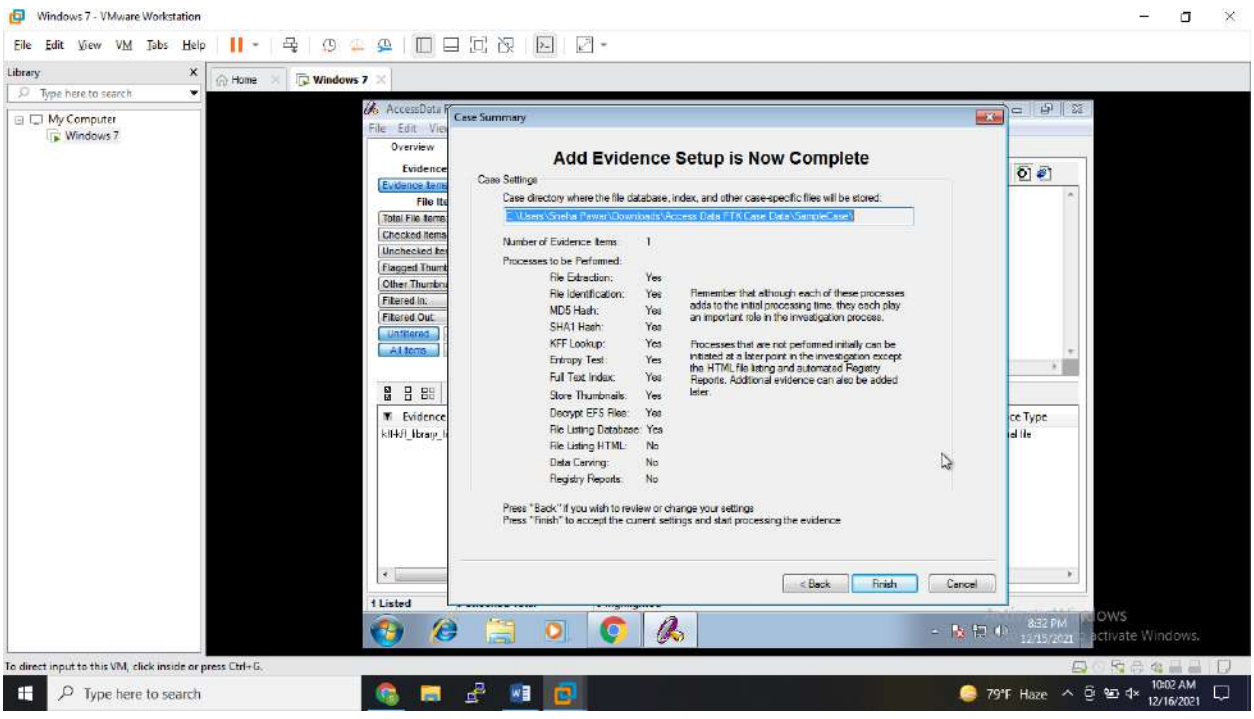

AccessData
File Edit View
Overview
Evidence
Evidence Items
File Items
Total File Items:
Checked Items
Unchecked Items
Flagged Thumbnails
Other Thumbnails
Filtered In:
Filtered Out:
Unfiltered
All Items
Evidence
kff-kff_library_files
Evidence Processing Options
Processes to Perform
Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.
MD5 Hash
An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
SHA1 Hash
A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
KFF Lookup
KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
Entropy Test
For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.
Full Text Index
The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.
Store Thumbnails
Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.
Decrypt EFS Files
Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)
File Listing Database
Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special.
HTML File Listing
Create an HTML version of the File Listing.
Data Carve
Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.
Carving Options
Registry Reports
Generate common registry reports during preprocessing.
< Back
Next >
Cancel
1 Listed
8:29 PM
12/15/2021

Then Add Evidence – Individual File – Browse location of a pst file.

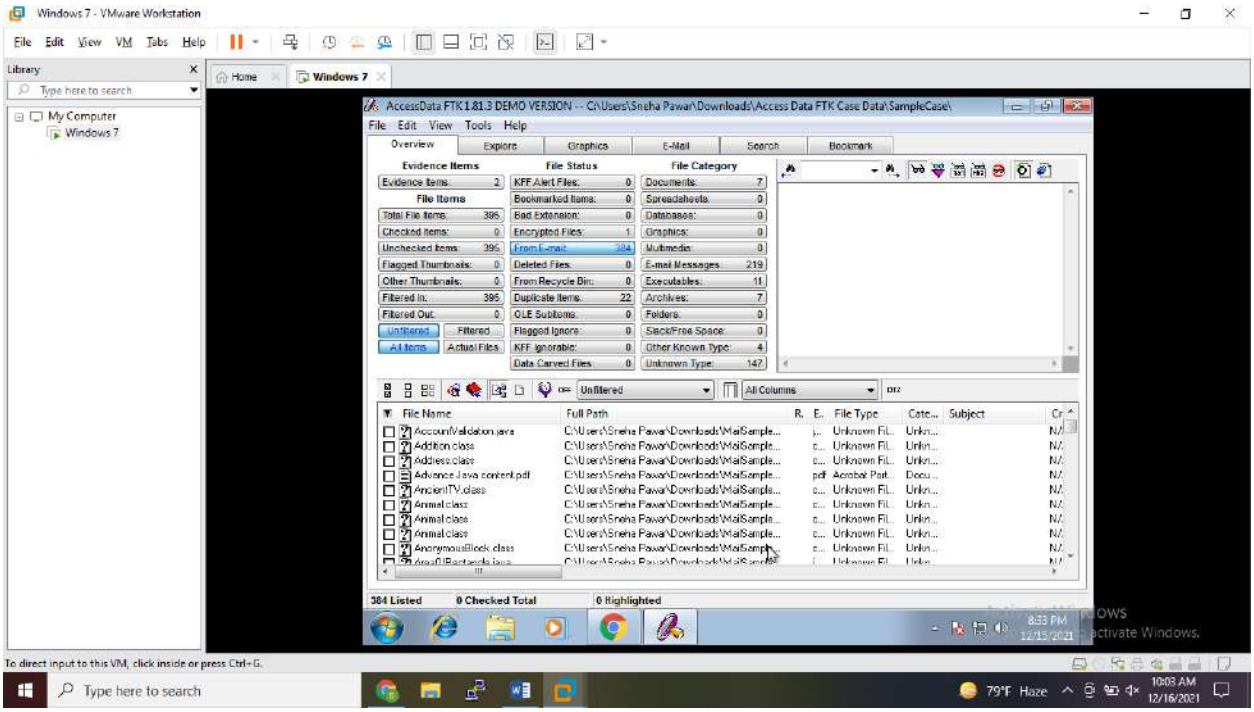


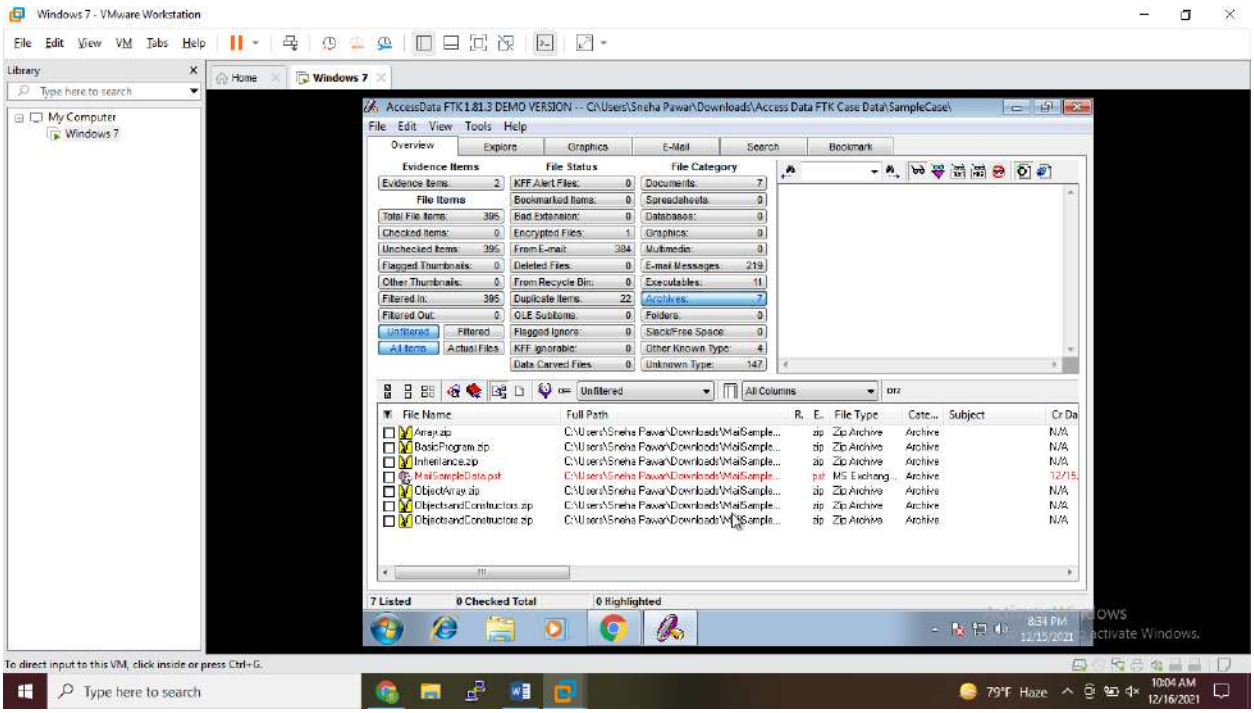
Click on Ok. And then click on Next.

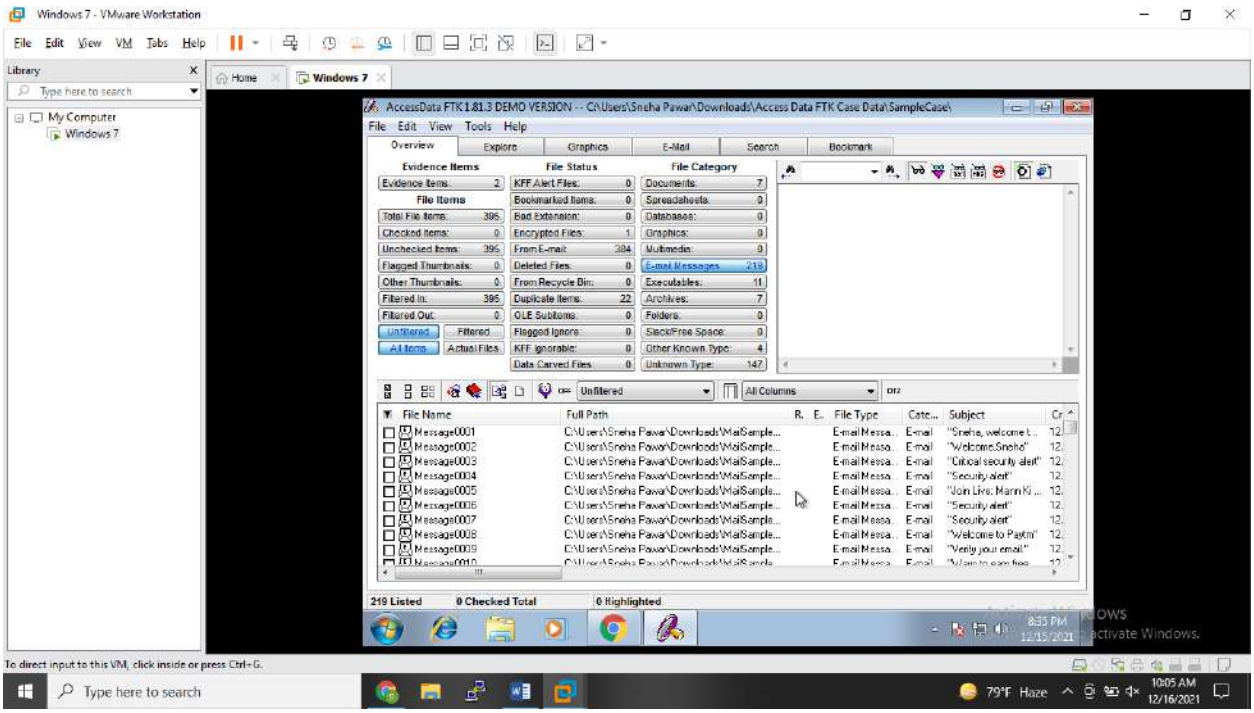

Add Evidence to Case
Add Evidence
Any number of evidence items can be added to the case. There are several types of evidence items:
Evidence Information
Evidence Location:
C:\Users\Sneha Pawar\Downloads\MailSampleData.pst
Evidence Display Name:
MailSampleData
Evidence Identification Name/Number:
Comment:
Local Evidence Time Zone:
Choose time zone for evidence ...
OK
Cancel
Add Evidence...
Display Name
Zone
Comment
< Back
Next >
Cancel
1 Listed
8:30 PM
12/15/2021


Windows 7 - VMware Workstation
Case Summary
Add Evidence Setup is Now Complete
Case Settings
Case directory where the file database, index, and other case-specific files will be stored:
Number of Evidence Items 1
Processes to be Performed:
File Extraction: Yes
File Identification: Yes
MD5 Hash: Yes
SHA1 Hash: Yes
KFF Lookup: Yes
Entropy Test: Yes
Full Text Index: Yes
Store Thumbnails: Yes
Decrypt EFS Files: Yes
File Listing Database: Yes
File Listing HTML: No
Data Carving: No
Registry Reports: No
Press "Back" if you wish to review or change your settings
Press "Finish" to accept the current settings and start processing the evidence
< Back
Finish
Cancel
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
10:02 AM
12/16/2021

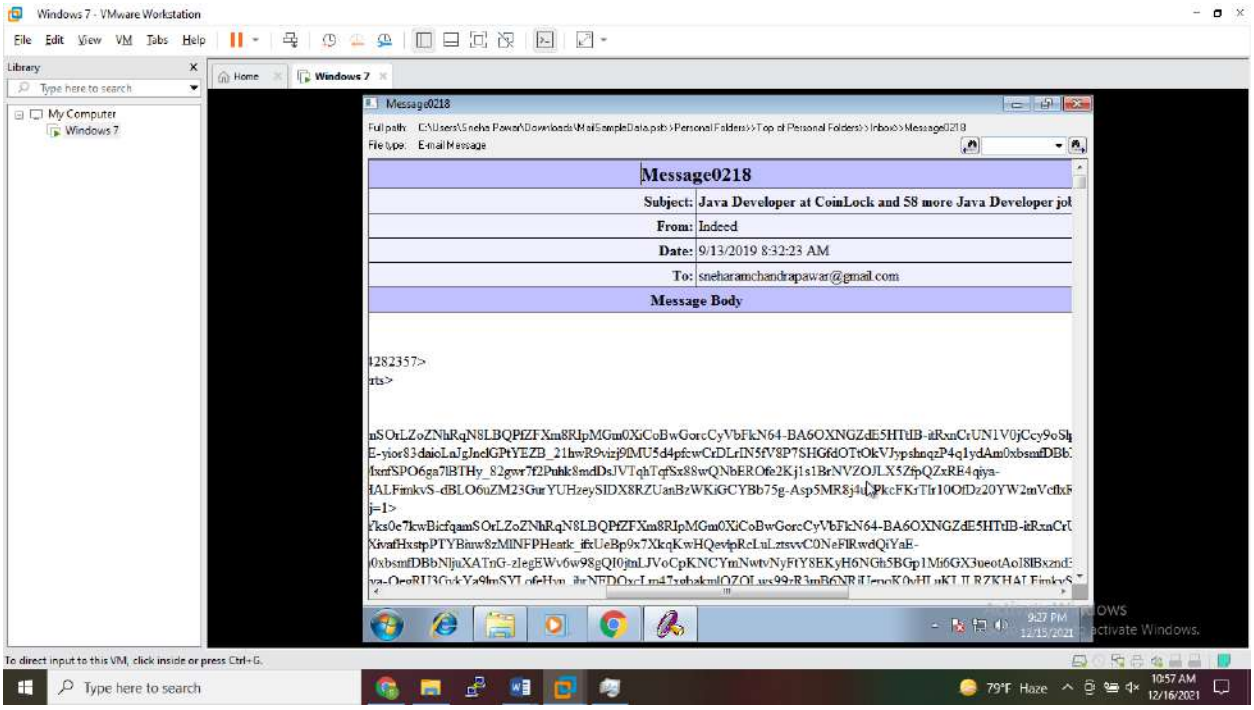
Emails will get acquired as you can see after double clicking on an evidence.





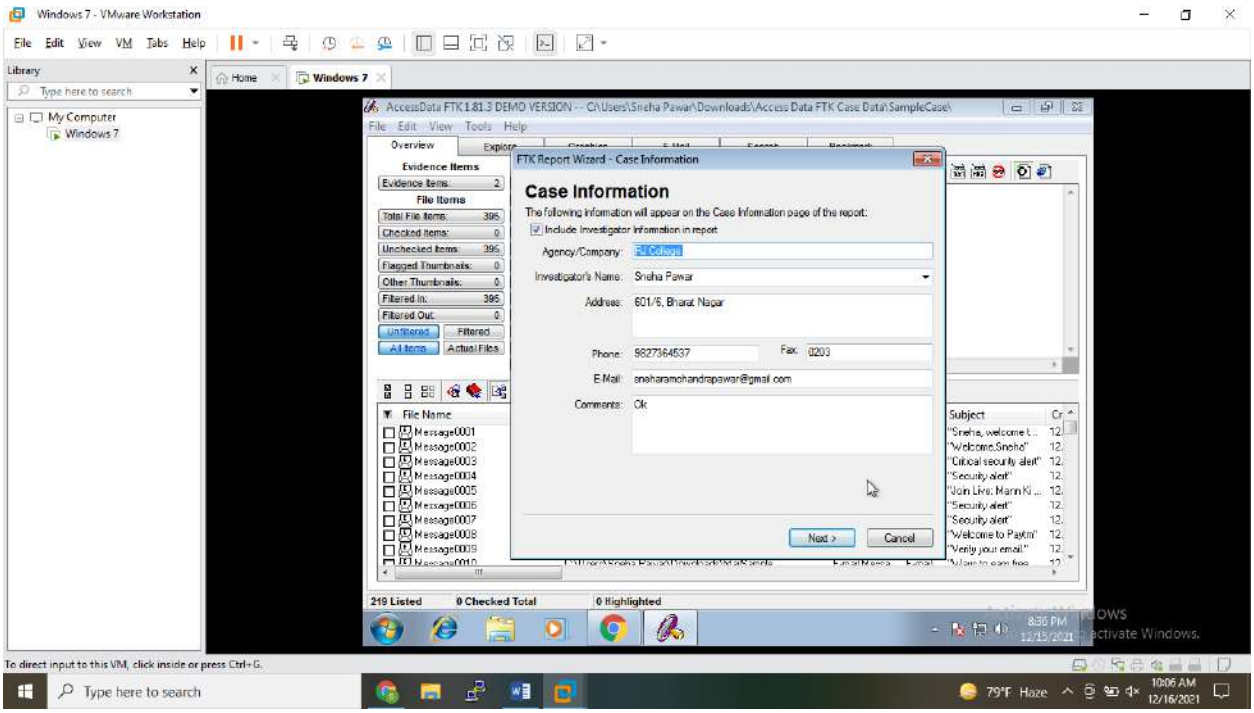


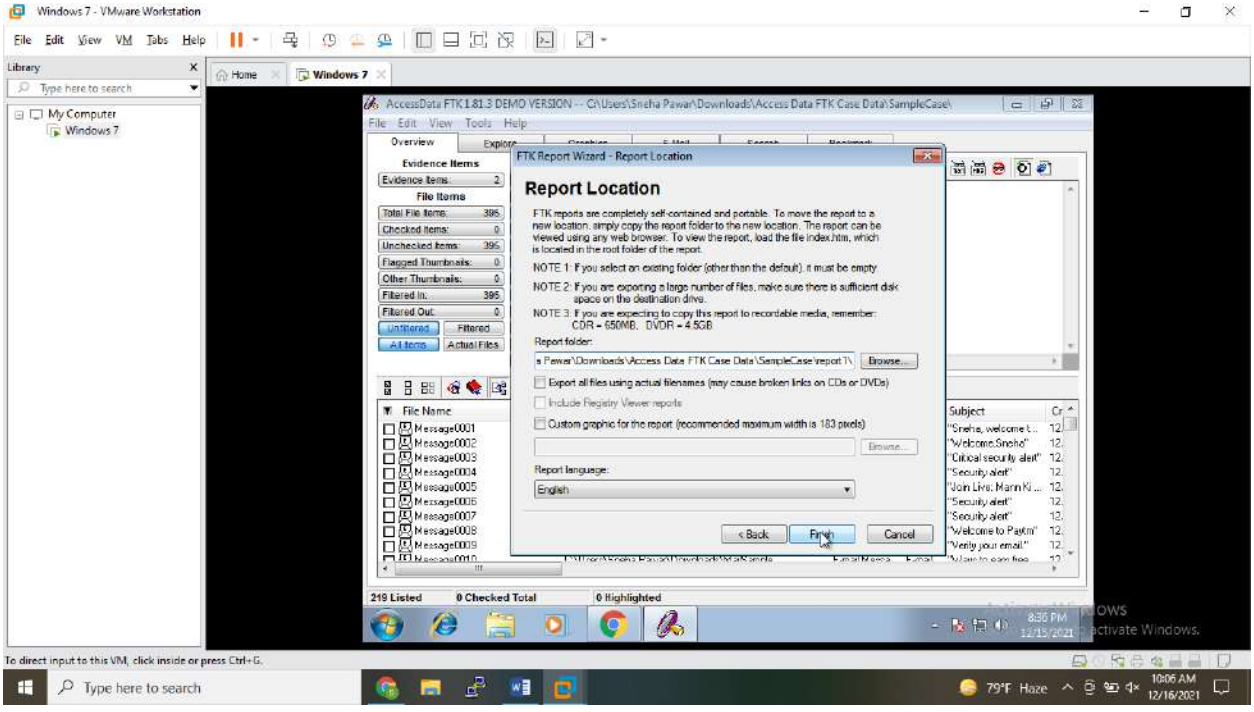
Right click on Mail to see it in Detached view.

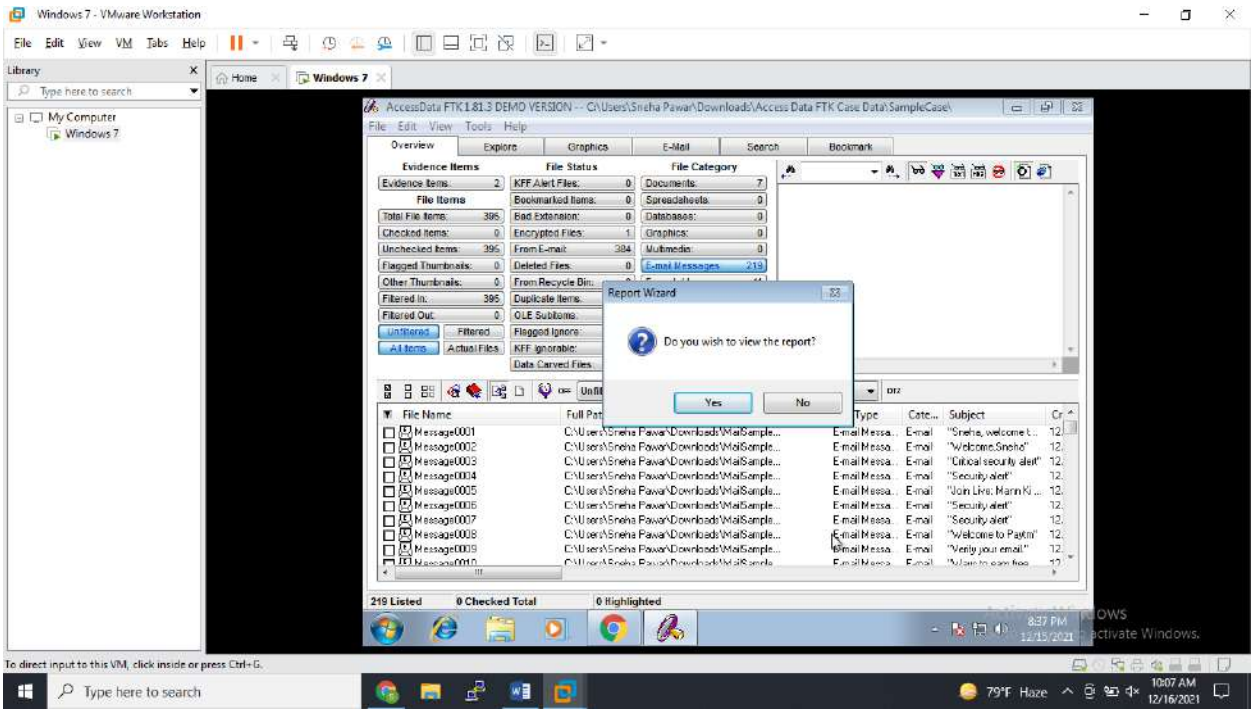


Steps:

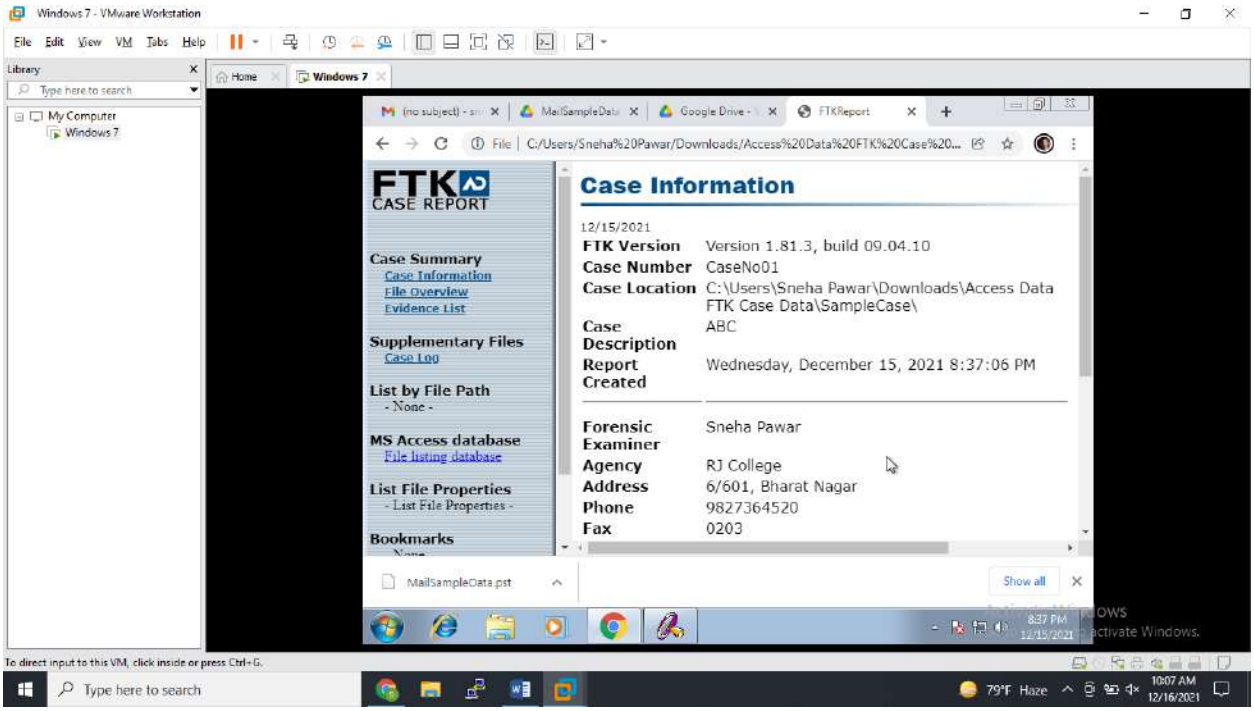
Now click on Report Wizard. And keep options by default and click on Next.

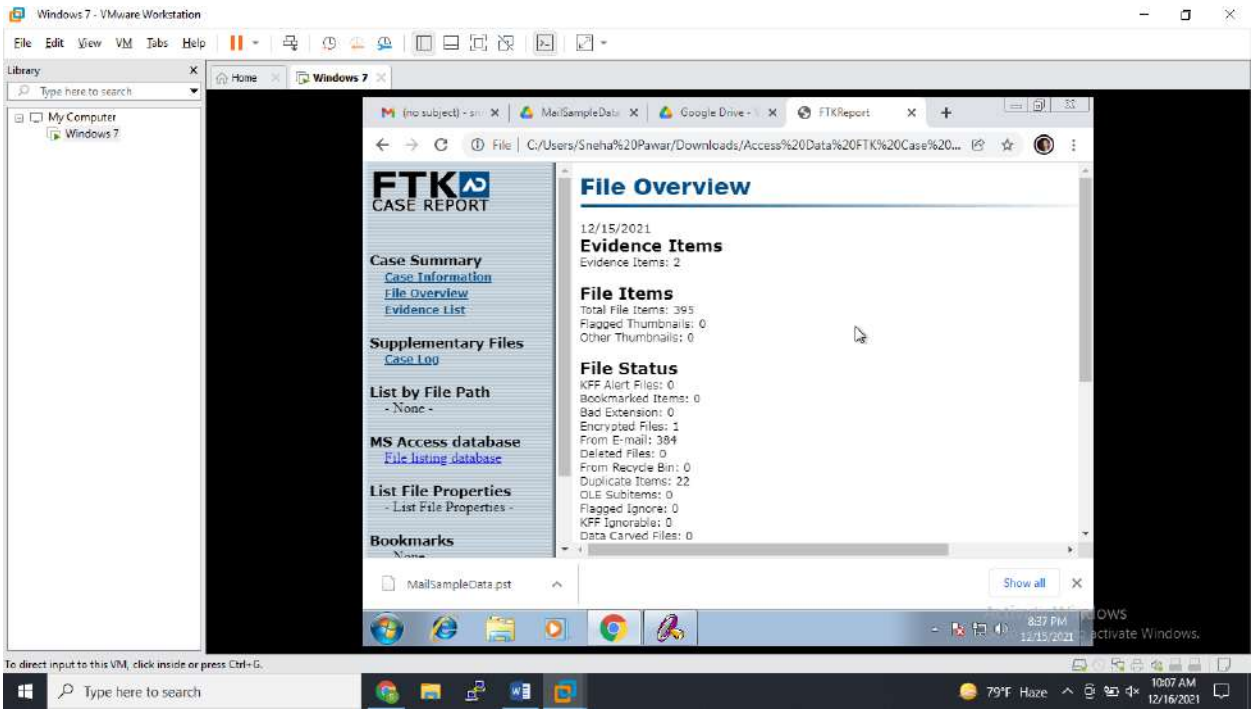

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION - C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools Help
Overview
Explore
Evidence Items
Evidence Items: 2
File Items
Total File Items: 395
Checked Items: 0
Unchecked Items: 395
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 395
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
FTK Report Wizard - Case Information
Case Information
The following information will appear on the Case Information page of the report:
Include Investigator information in report
Agency/Company: FC College
Investigator's Name: Sneha Pawar
Address: 601/6, Bharat Nagar
Phone: 9827364537
Fax: 0203
E-Mail: sneharamchandrapawar@gmail.com
Comments: Ok
Next >
Cancel
File Name
Message0001
Message0002
Message0003
Message0004
Message0005
Message0006
Message0007
Message0008
Message0009
Subject
"Sneha, welcome t...
"Welcome,Sneha"
"Critical security alert"
"Security alert"
"Join Live: Mann Ki ...
"Security alert"
"Security alert"
"Welcome to Paytm"
"Verify your email."
219 Listed
0 Checked Total
0 Highlighted
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
10:06 AM
12/16/2021

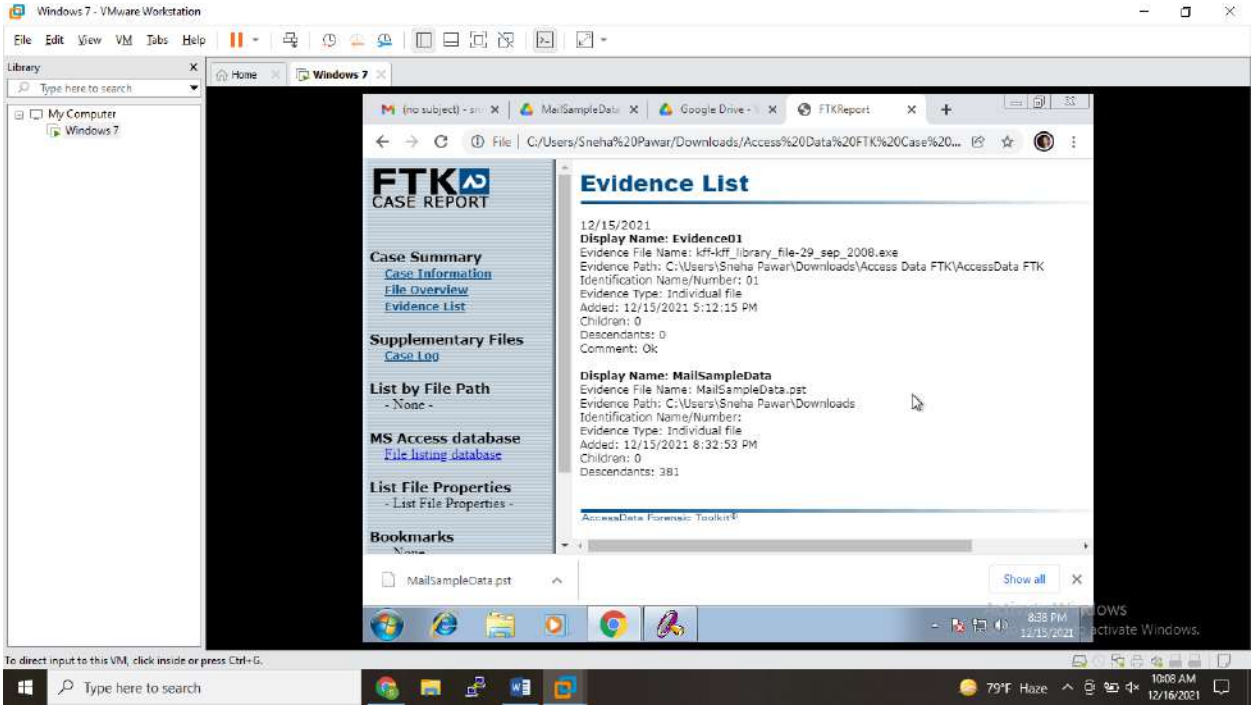

Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
AccessData FTK 1.81.3 DEMO VERSION - C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
File Edit View Tools Help
Overview
Explore
Evidence Items
Evidence Items: 2
File Items
Total File Items: 395
Checked Items: 0
Unchecked Items: 395
Flagged Thumbnails: 0
Other Thumbnails: 0
Filtered In: 395
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
FTK Report Wizard - Report Location
Report Location
FTK reports are completely self-contained and portable. To move the report to a new location, simply copy the report folder to the new location. The report can be viewed using any web browser. To view the report, load the file index.htm, which is located in the root folder of the report.
NOTE 1: If you select an existing folder (other than the default), it must be empty.
NOTE 2: If you are exporting a large number of files, make sure there is sufficient disk space on the destination drive.
NOTE 3: If you are expecting to copy this report to recordable media, remember:
CDR = 650MB; DVDR = 4.5GB
Report folder:
Browse...
Export all files using actual filenames (may cause broken links on CDs or DVDs)
Include Registry Viewer reports
Custom graphic for the report (recommended maximum width is 183 pixels)
Browse...
Report language:
English
< Back
Finish
Cancel
File Name
Message0001
Message0002
Message0003
Message0004
Message0005
Message0006
Message0007
Message0008
Message0009
Subject
"Sneha, welcome t...
"Welcome,Sneha"
"Critical security alert"
"Security alert"
"Join Live: Mann Ki ...
"Security alert"
"Security alert"
"Welcome to Paytm"
"Verify your email."
219 Listed
0 Checked Total
0 Highlighted
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
10:06 AM
12/16/2021


Windows 7 - VMware Workstation
Report Wizard
Do you wish to view the report?
Yes
No

Click on Yes.


Windows 7 - VMware Workstation
FTK CASE REPORT
Case Information
12/15/2021
FTK Version Version 1.81.3, build 09.04.10
Case Number CaseNo01
Case Location C:\Users\Sneha Pawar\Downloads\Access Data FTK Case Data\SampleCase\
Case Description ABC
Report Created Wednesday, December 15, 2021 8:37:06 PM
Forensic Examiner Sneha Pawar
Agency RJ College
Address 6/601, Bharat Nagar
Phone 9827364520
Fax 0203


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
FTKReport
File | C:/Users/Sneha%20Pawar/Downloads/Access%20Data%20FTK%20Case%20...
FTK CASE REPORT
Case Summary
Case Information
File Overview
Evidence List
Supplementary Files
Case Log
List by File Path
- None -
MS Access database
File listing database
List File Properties
- List File Properties -
Bookmarks
File Overview
12/15/2021
Evidence Items
Evidence Items: 2
File Items
Total File Items: 395
Flagged Thumbnails: 0
Other Thumbnails: 0
File Status
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 0
Encrypted Files: 1
From E-mail: 384
Deleted Files: 0
From Recycle Bin: 0
Duplicate Items: 22
OLE Subitems: 0
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0
MailSampleData.pst
Show all
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
10:07 AM
12/16/2021


Windows 7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Windows 7
Home
Windows 7
FTKReport
File | C:/Users/Sneha%20Pawar/Downloads/Access%20Data%20FTK%20Case%20...
FTK CASE REPORT
Case Summary
Case Information
File Overview
Evidence List
Supplementary Files
Case Log
List by File Path
- None -
MS Access database
File listing database
List File Properties
- List File Properties -
Bookmarks
Evidence List
12/15/2021
Display Name: Evidence01
Evidence File Name: kff-kff_library_file-29_sep_2008.exe
Evidence Path: C:\Users\Sneha Pawar\Downloads\Access Data FTK\AccessData FTK
Identification Name/Number: 01
Evidence Type: Individual file
Added: 12/15/2021 5:12:15 PM
Children: 0
Descendants: 0
Comment: Ok
Display Name: MailSampleData
Evidence File Name: MailSampleData.pst
Evidence Path: C:\Users\Sneha Pawar\Downloads
Identification Name/Number:
Evidence Type: Individual file
Added: 12/15/2021 8:32:53 PM
Children: 0
Descendants: 381
AccessData Forensic Toolkit®
MailSampleData.pst
Show all
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
79°F Haze
10:08 AM
12/16/2021

Practical No. 10

Aim: Performing Password Cracking [Cain and Abel]

What is Password Cracking?

Password cracking is the process of using an application program to identify an unknown or forgotten password to a computer or network resource. It can also be used to help a threat actor obtain unauthorized access to resources.

With the information malicious actors gain using password cracking, they can undertake a range of criminal activities. Those include stealing banking credentials or using the information for identity theft and fraud.

A password cracker recovers passwords using various techniques. The process can involve comparing a list of words to guess passwords or the use of an algorithm to repeatedly guess the password.

What does a password cracking attack look like?

The general process a password cracker follows involves these four steps:

1. Steal a password via some nefarious means. That password has likely been encrypted before being stored using a hash Hashes are mathematical functions that change arbitrary-length inputs into an encrypted fixed-length output.
2. Choose a cracking methodology, such as a brute-force or dictionary attack, and select a cracking tool.
3. Prepare the password hashes for the cracking program. This is done by providing an input to the hash function to create a hash that can be authenticated.
4. Run the cracking tool.

A password cracker may also be able to identify encrypted passwords. After retrieving the password from the computer's memory, the program may be able

to decrypt it. Or, by using the same algorithm as the system program, the password cracker creates an encrypted version of the password that matches the original.

What are password cracking techniques?

Password crackers use two primary methods to identify correct passwords: brute-force and dictionary attacks. However, there are plenty of other password cracking methods, including the following:

- **Brute force.** This attack runs through combinations of characters of a predetermined length until it finds the combination that matches the password.
- **Dictionary search.** Here, a password cracker searches each word in the dictionary for the correct password. Password dictionaries exist for a variety of topics and combinations of topics, including politics, movies and music groups.
- **Phishing.** These attacks are used to gain access to user passwords without the use of a password cracking tool. Instead, a user is fooled into clicking on an email attachment. From here, the attachment could install malware or prompt the user to use their email to sign into a false version of a website, revealing their password.
- **Malware.** Similar to phishing, using malware is another method of gaining unauthored access to passwords without the use of a password cracking tool. Malware such as keyloggers, which track keystrokes, or screen scrapers, which take screenshots, are used instead.
- **Rainbow attack.** This approach involves using different words from the original password in order to generate other possible passwords. Malicious actors can keep a list called a *rainbow table* with them. This list contains leaked and previously cracked passwords, which will make the overall password cracking method more effective.
- **Guessing.** An attacker may be able to guess a password without the use of tools. If the threat actor has enough information about the victim or the victim is using a common enough password, they may be able to come up with the correct characters.

Some password cracking programs may use hybrid attack methodologies where they search for combinations of dictionary entries and numbers or special characters. For example, a password cracker may search for ants01, ants02, ants03, etc. This can be helpful when users have been advised to include a number in their password.

What are password cracking tools?

Password crackers can be used maliciously or legitimately to recover lost passwords. Among the password cracking tools available are the following three:

1. **Cain and Abel.** This password recovery software can recover passwords for Microsoft Windows user accounts and Microsoft Access passwords. Cain and Abel uses a graphical user interface, making it more user-friendly than comparable tools. The software uses dictionary lists and brute-force attack methods.
2. **Ophcrack.** This password cracker uses rainbow tables and brute-force attacks to crack passwords. It runs on Windows, macOS and Linux.
3. **John the Ripper.** This tool uses a dictionary list approach and is available primarily for macOS and Linux systems. The program has a command prompt to crack passwords, making it more difficult to use than software like Cain and Abel.

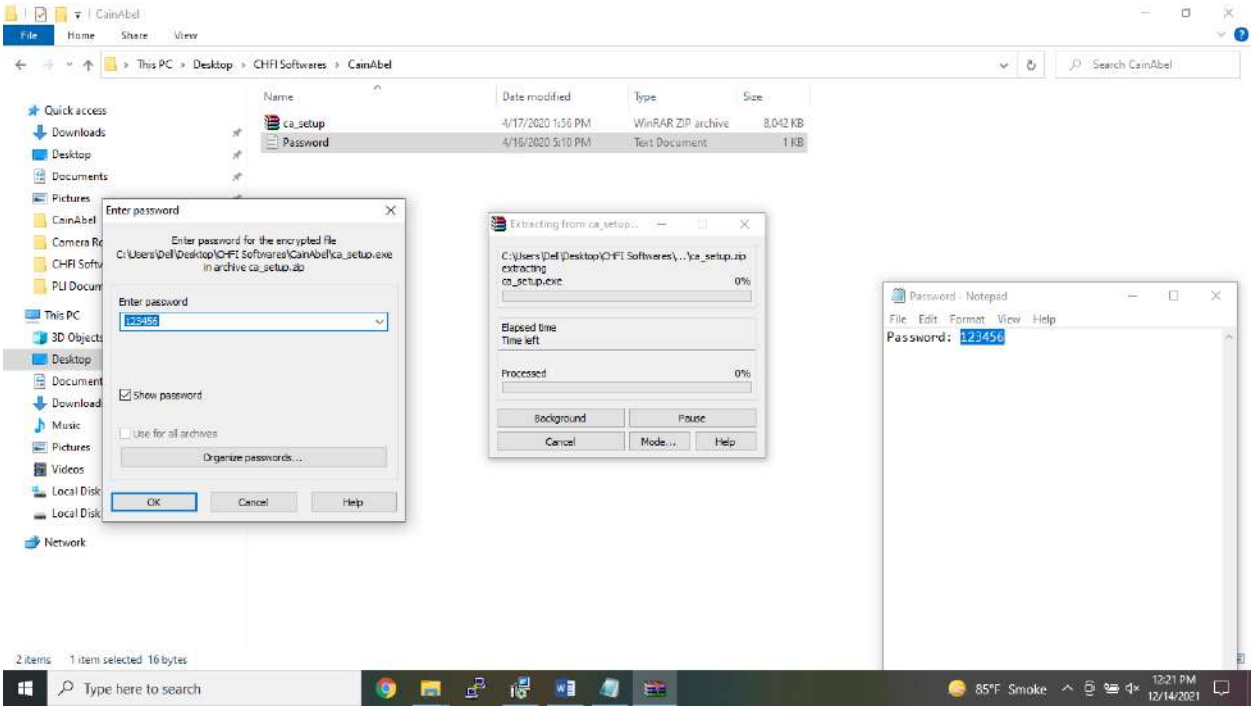
Steps:

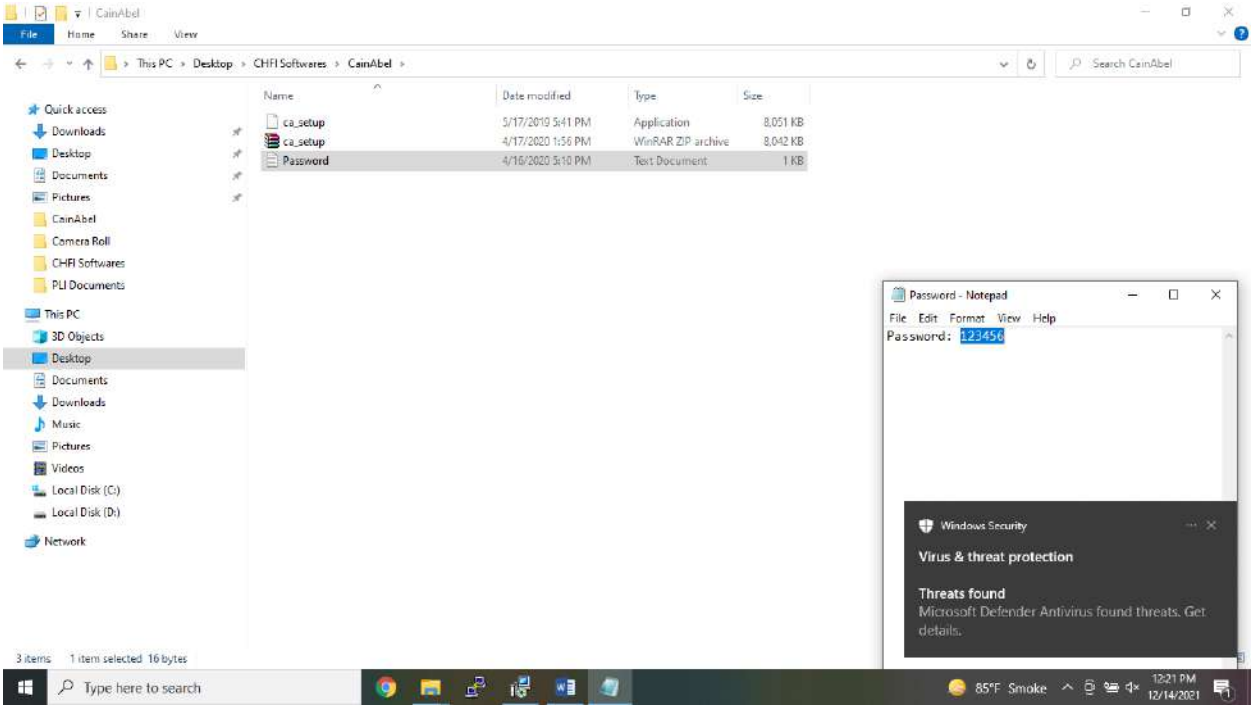
You can also download CainAbel from the link on your windows 10 Virtual Machine:

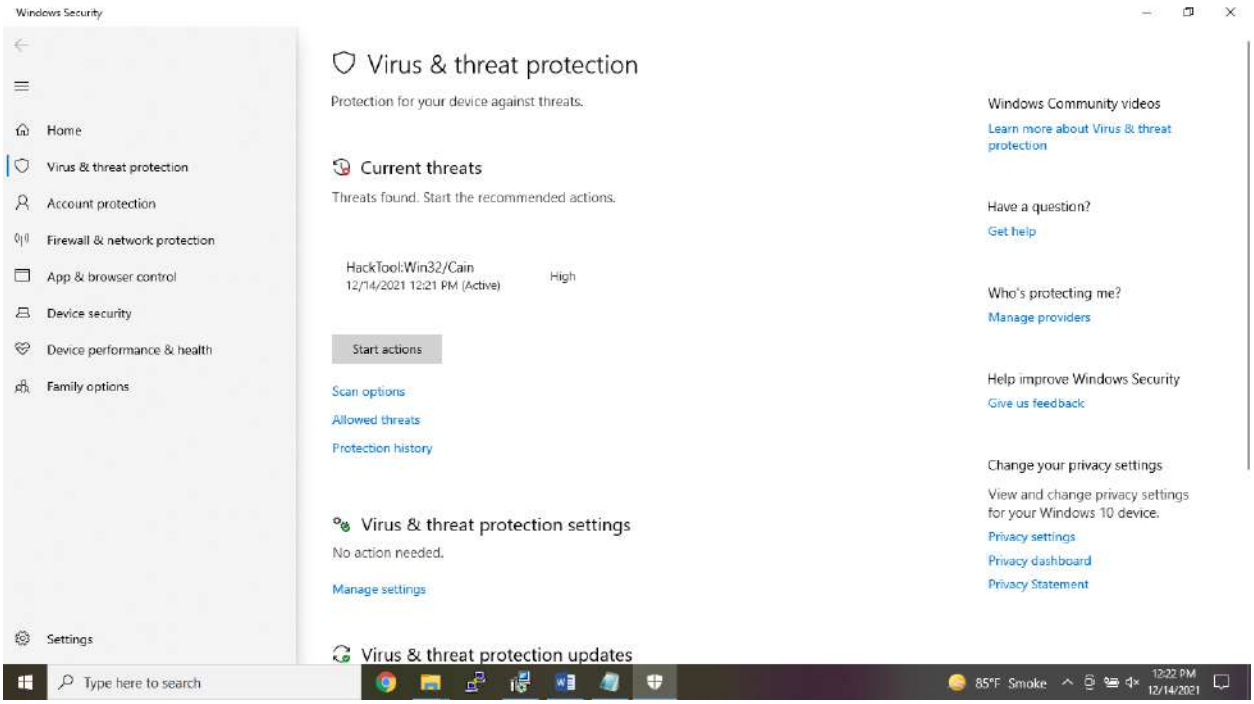
https://www.malavida.com/en/soft/cain-and-abel/download

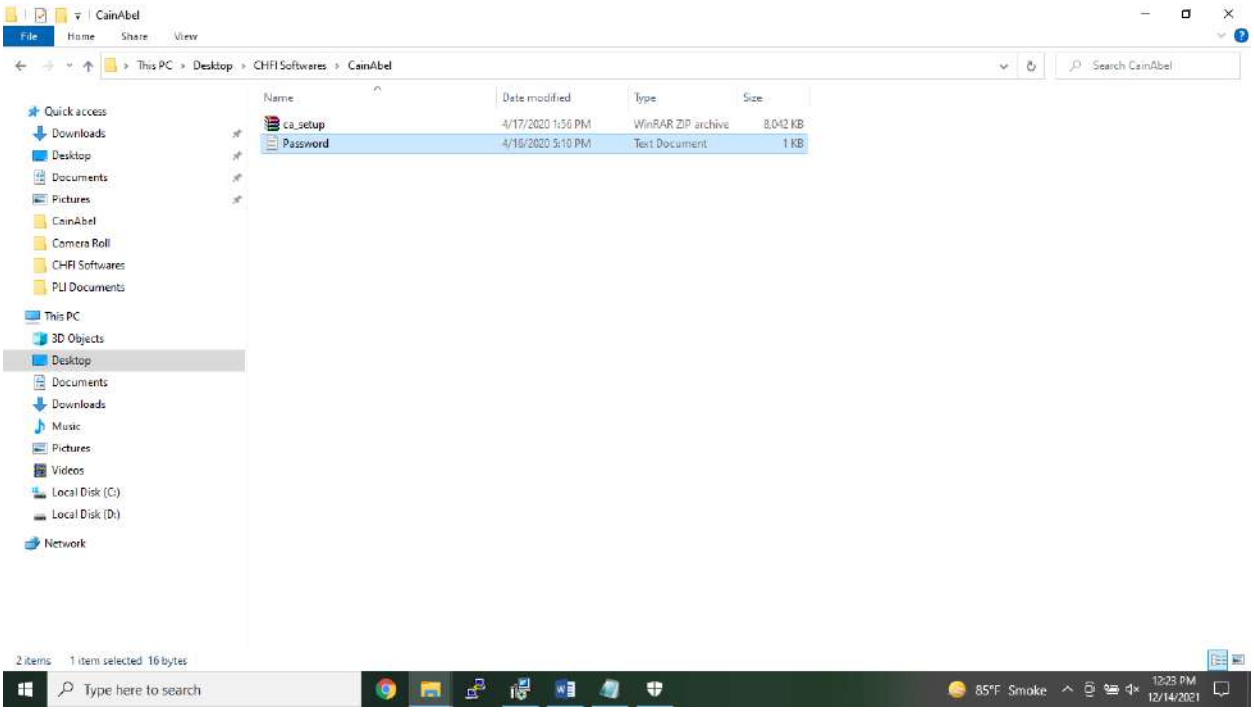
Don't install CainAbel on your primary windows computer or laptop. Install it on the Virtual machine instead. Because Windows10 will see CainAbel as a malicious software. And will give alert on system. And won't let you extract the setup on your system. It will automatically remove the setup from your machine, as shown

in below steps. If still you want to do it on your windows10 system then you need to disable the Antivirus.







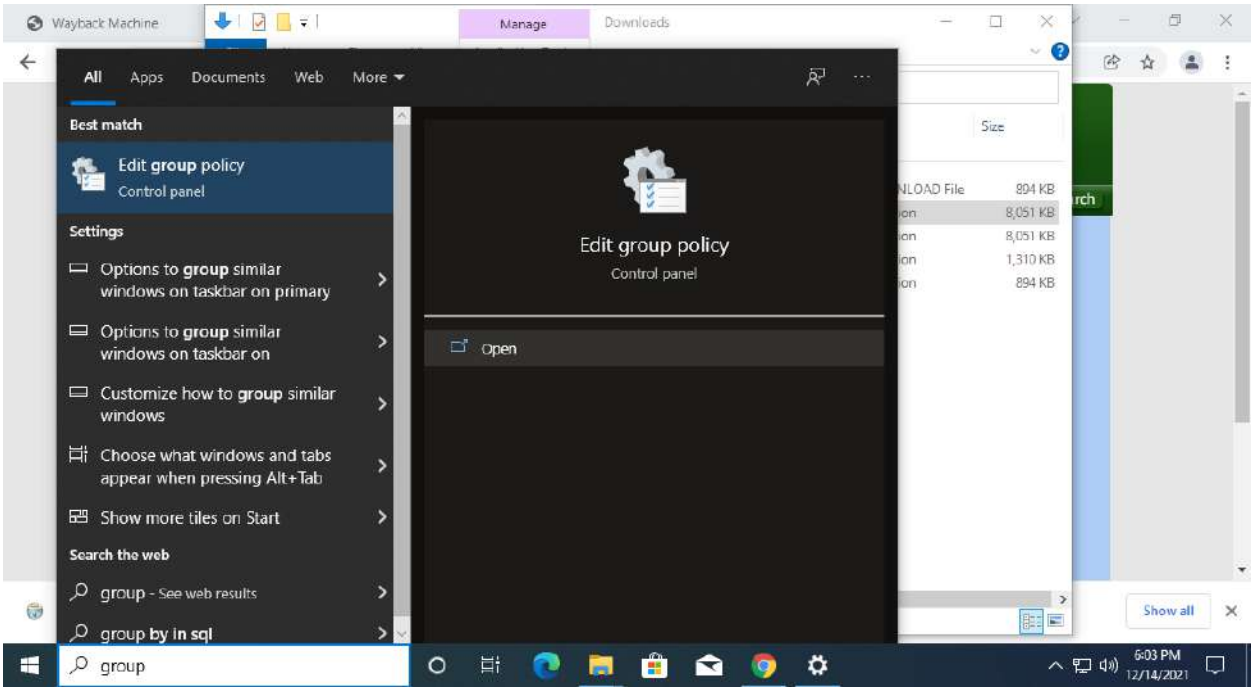


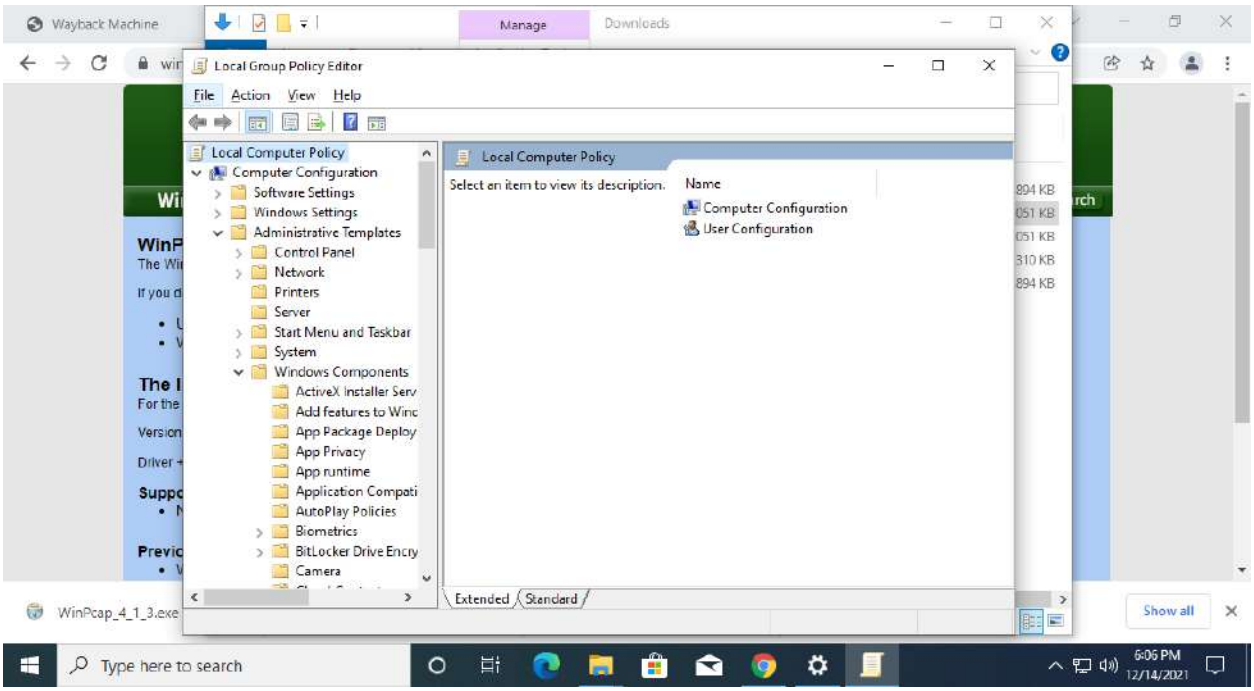
Download and install VMware workstation and create a Windows10 Virtual Machine on it.

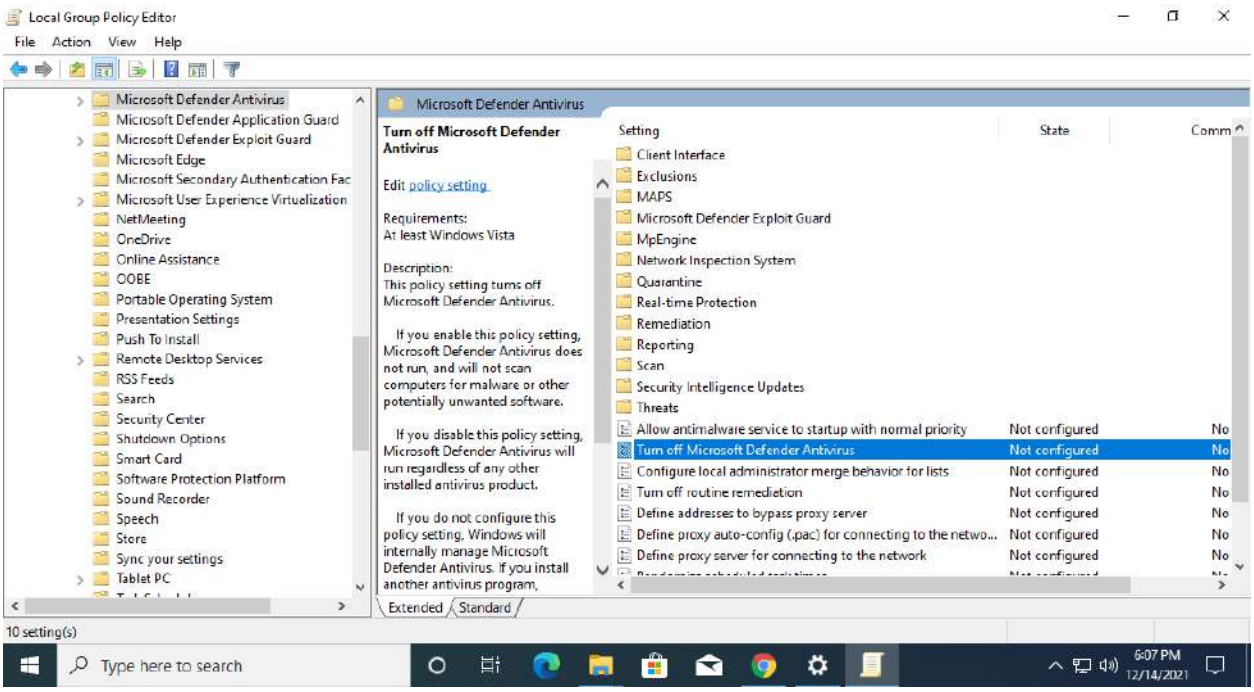
You need to disable all the options under Virus and Threat Protection settings.

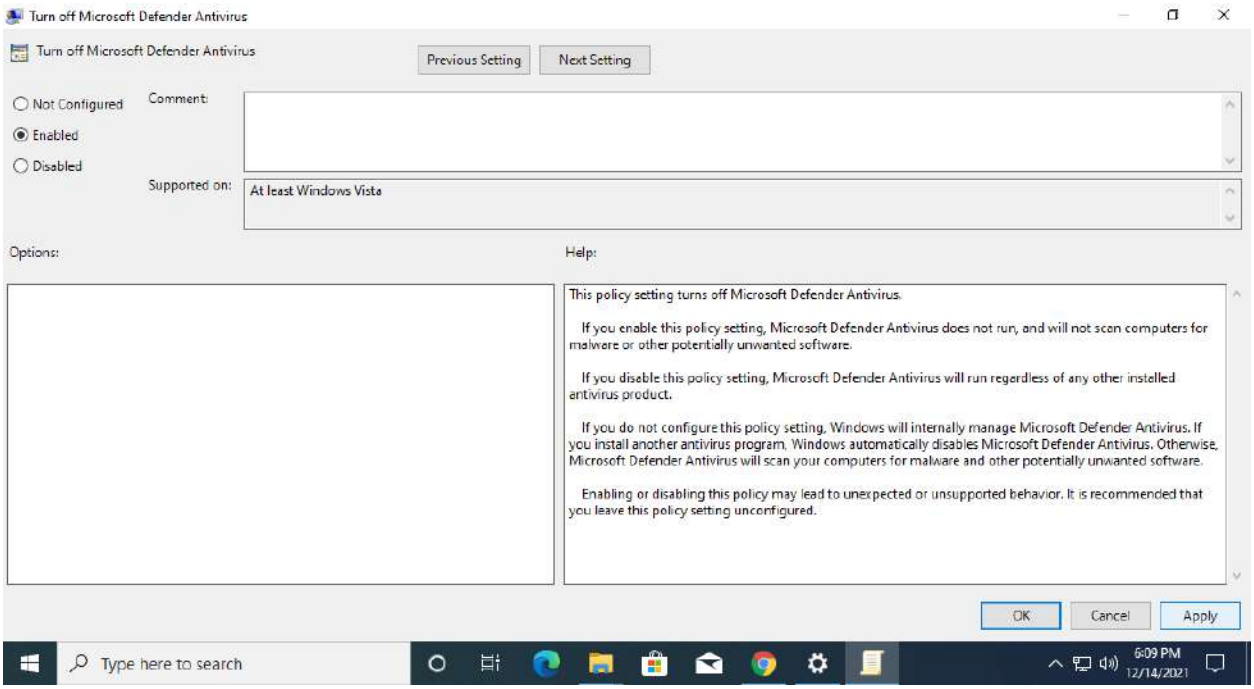
To permanently disable Microsoft Defender Antivirus. Follow the following steps:

Edit the group policy – Administrative template – Windows Component – Microsoft Defender Antivirus Double click on it – Turn off Microsoft defender Antivirus – Click on Apply.







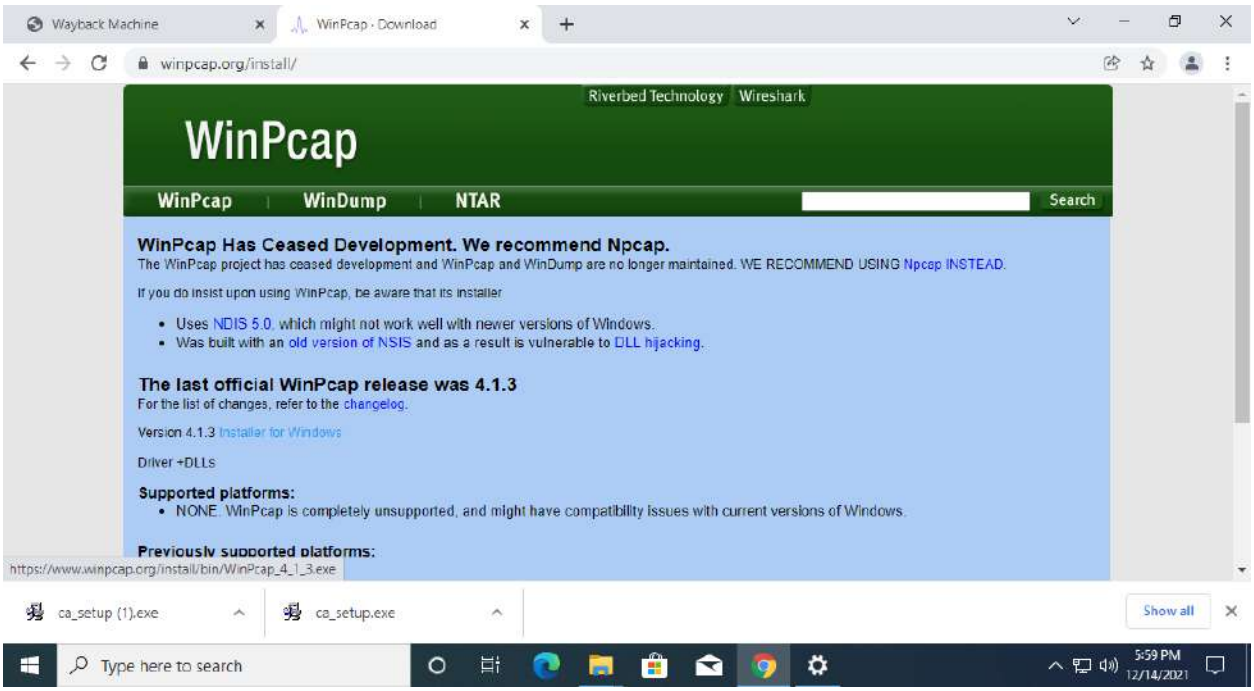


Download the Cain and abel software from the link below:-

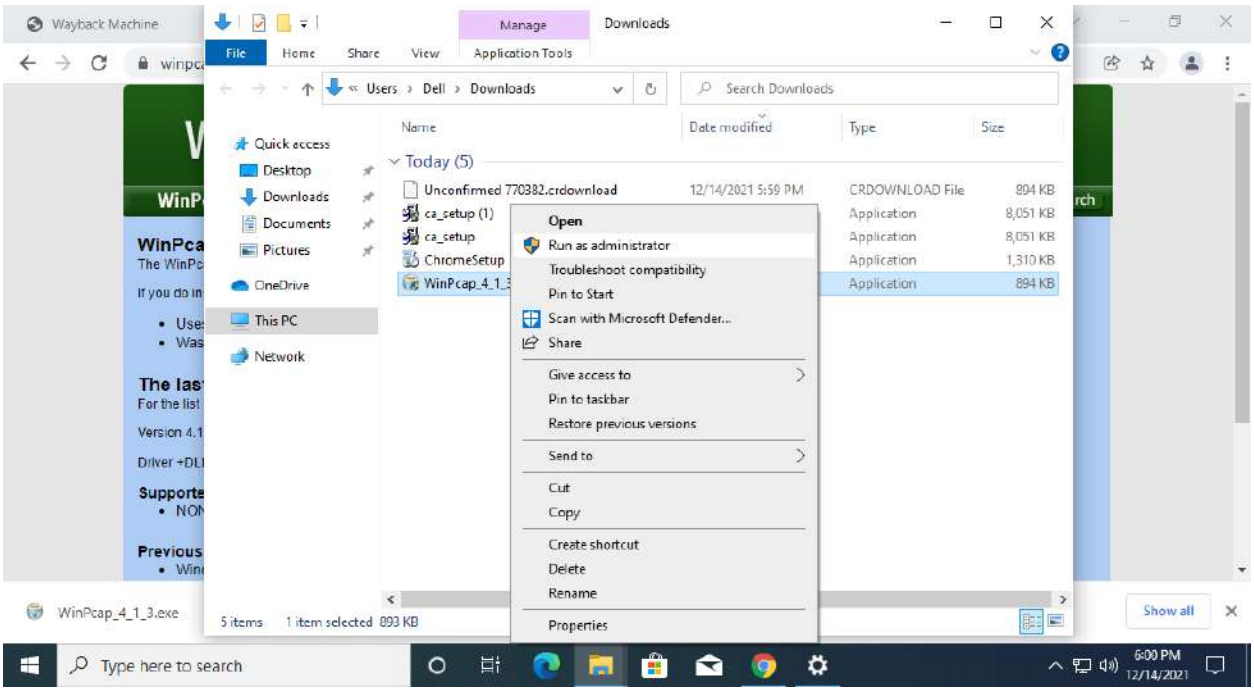
https://web.archive.org/web/20160214132154/http://www.oxid.it/cain.html

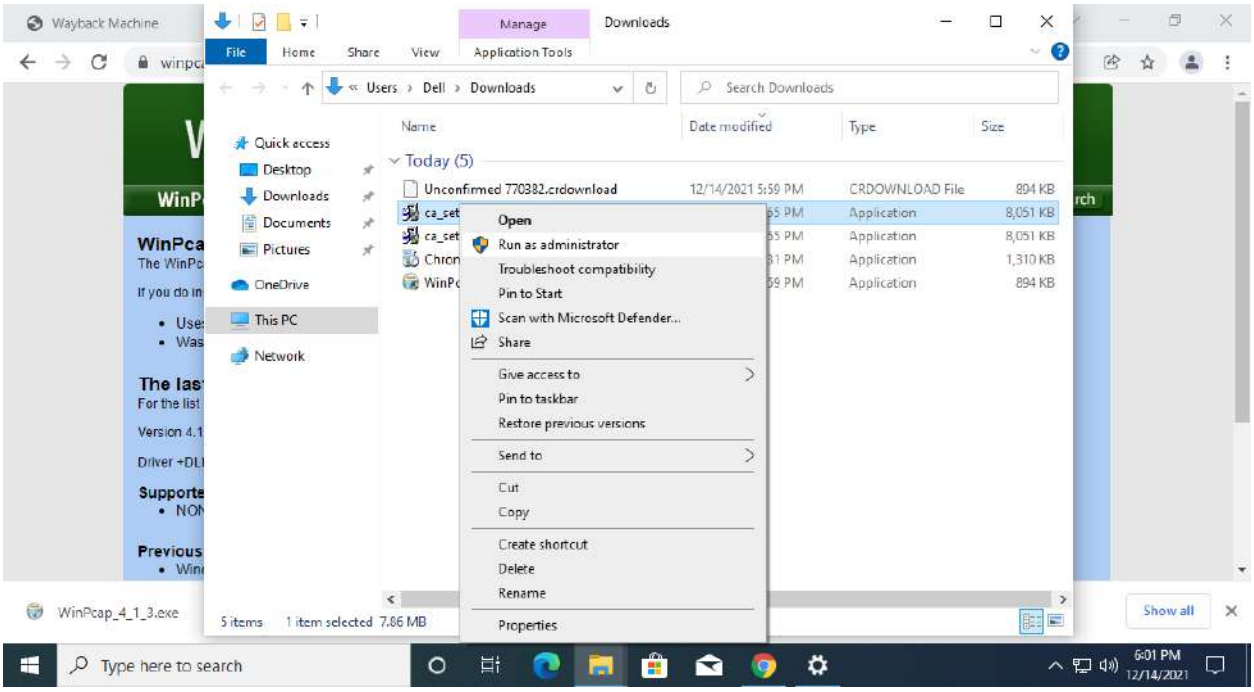
After downloading software don't run the setup quickly. Downlaod another software WinPcap.

www.winpcap.org/install

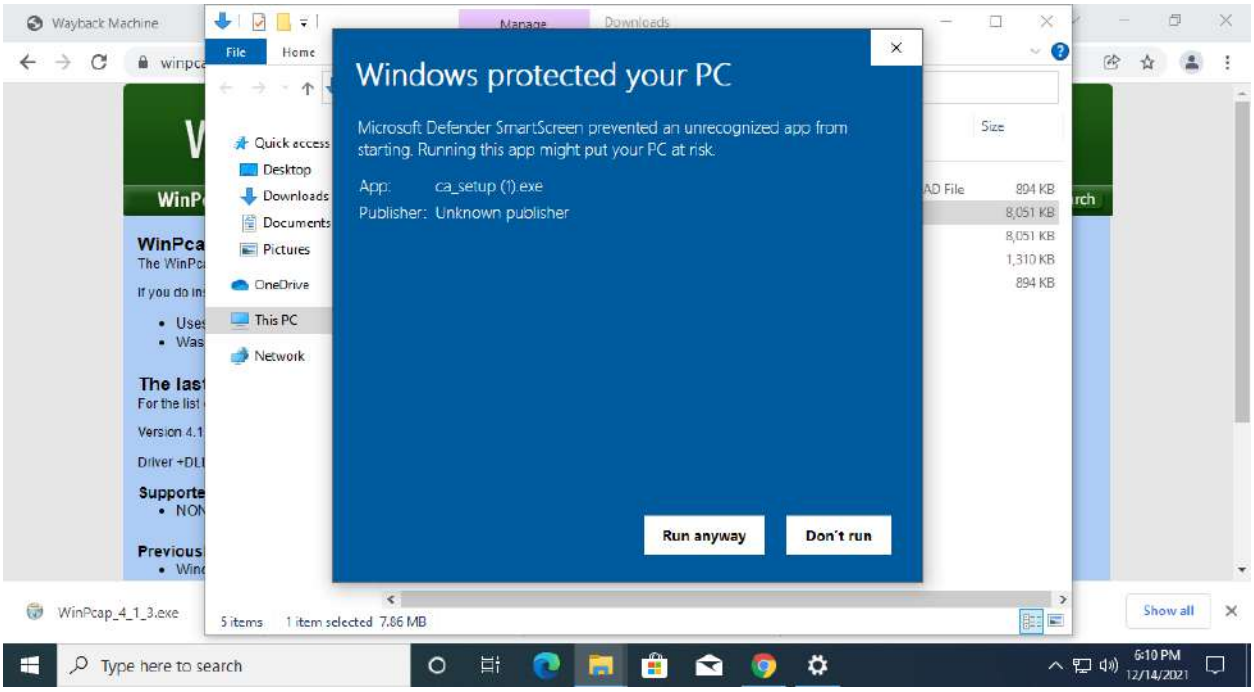


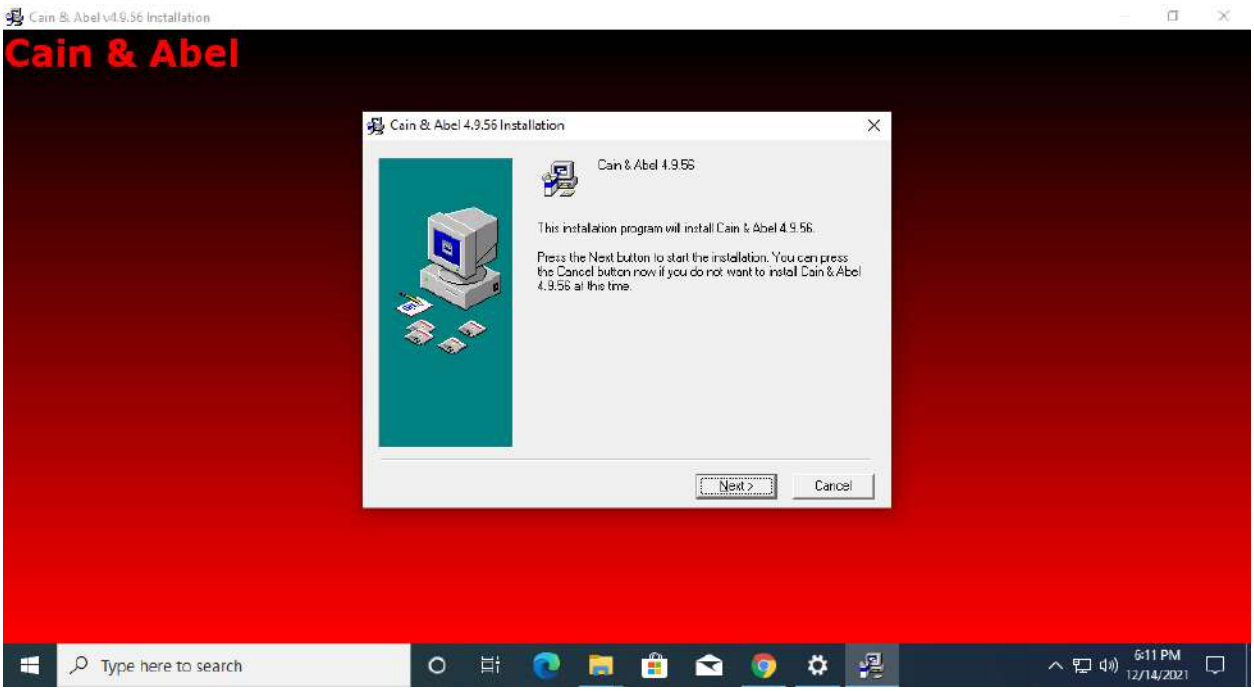
After downloading WinPcap first install it then install CainAbel.

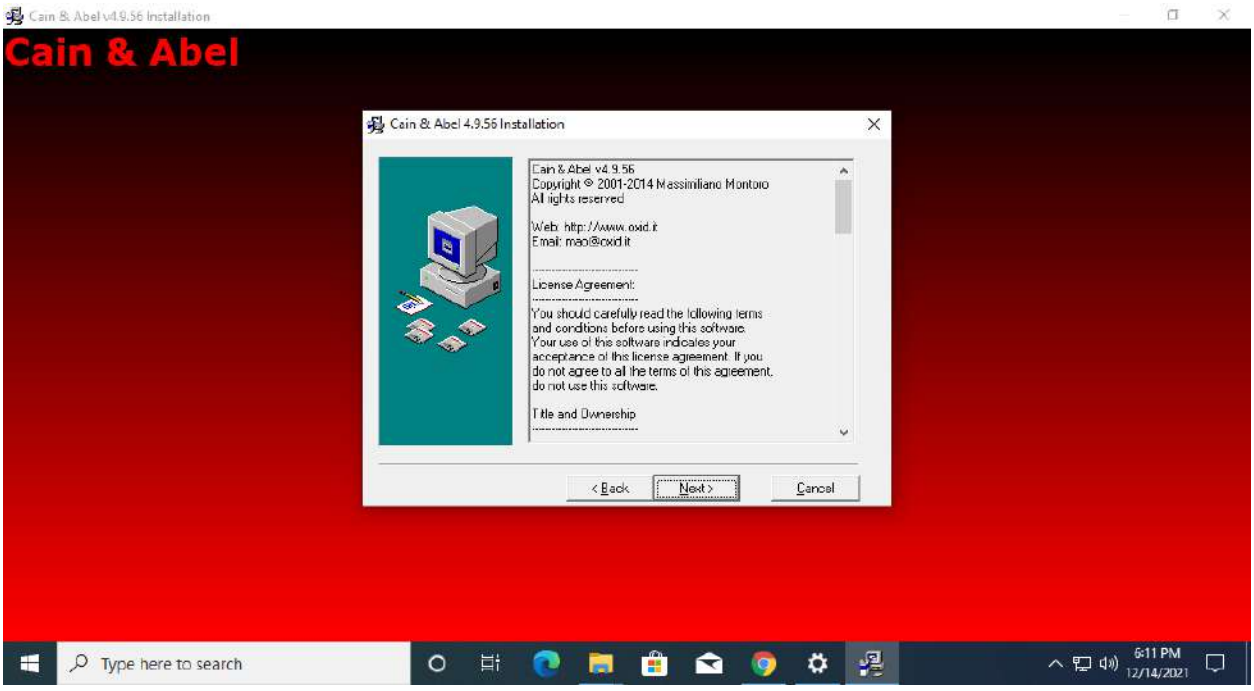




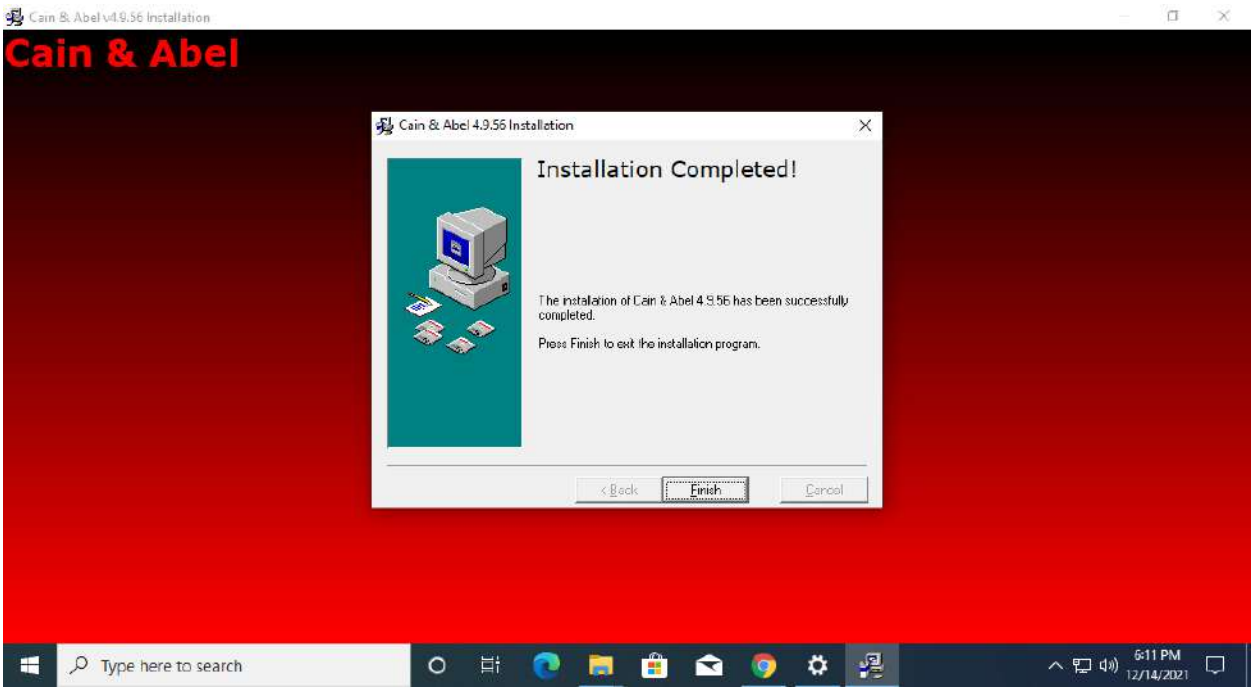
Then Click on Run Anyway.



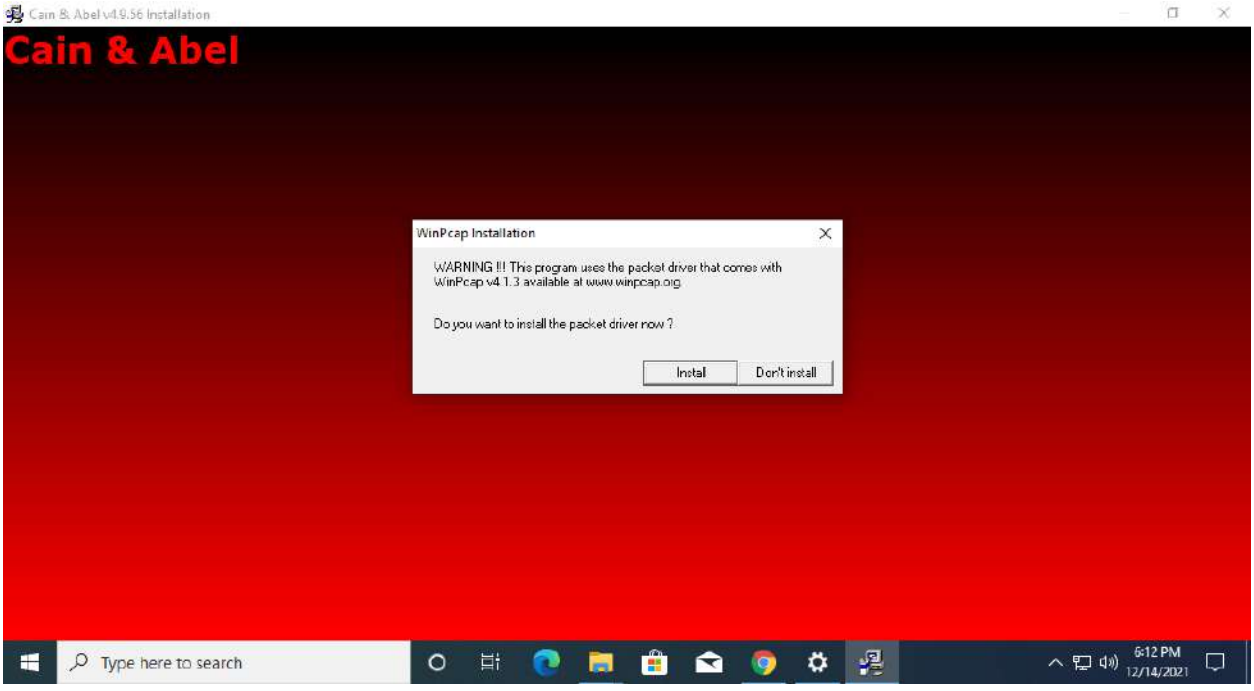




Click on Next by keeping everything default. And finish setup installation.

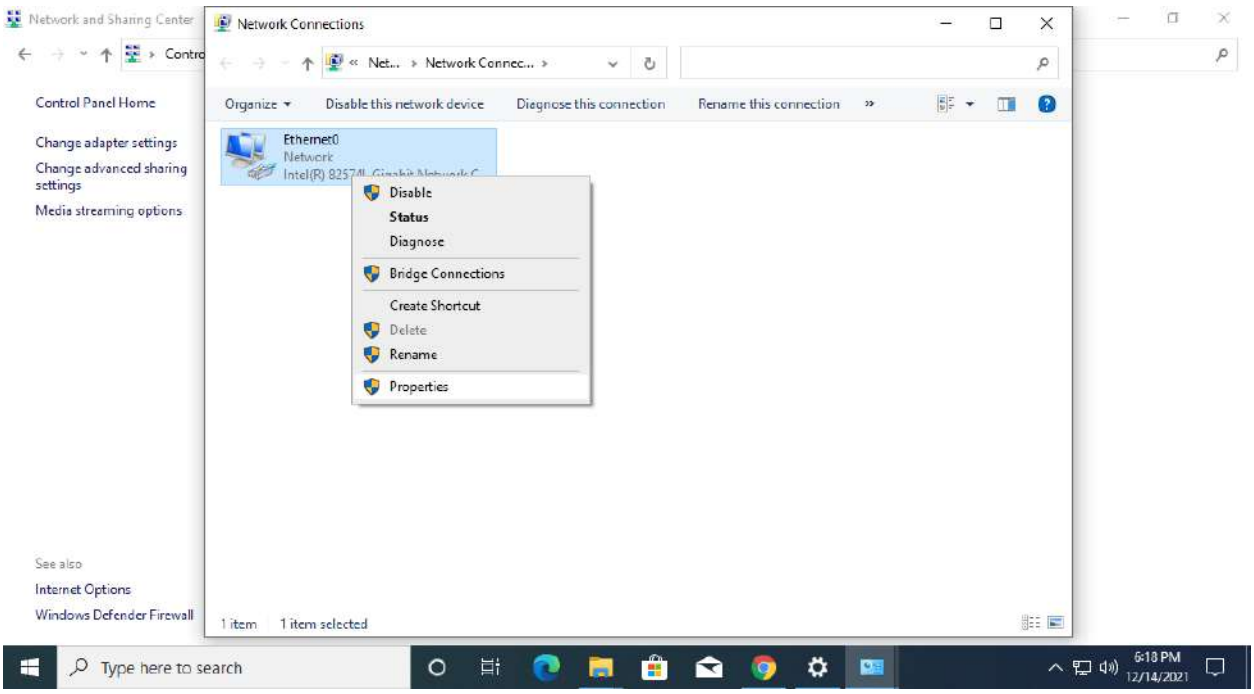


Click on Don’t install.

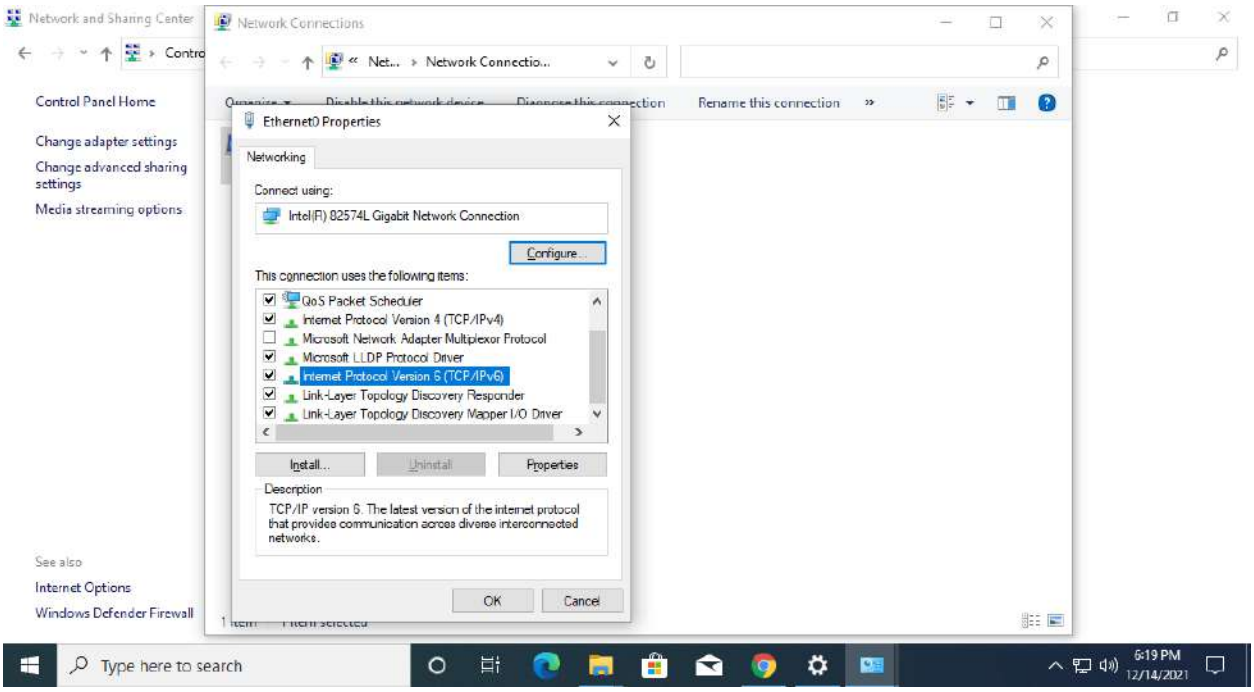


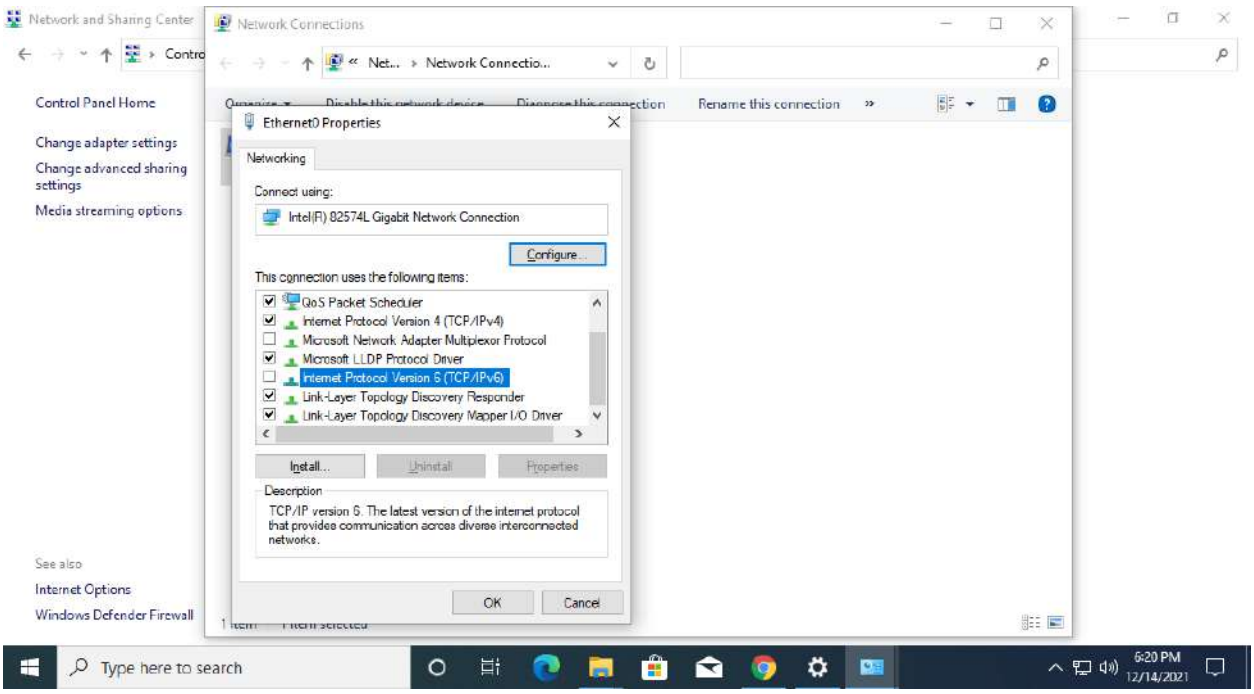
Don’t start the CainAbel yet we have to do some changes in the control panel.

Control Panel – Network & Internet – Network & Sharing Center – Change Adapter Settings – Go to Ethernet0 – Right click on it – Properties.



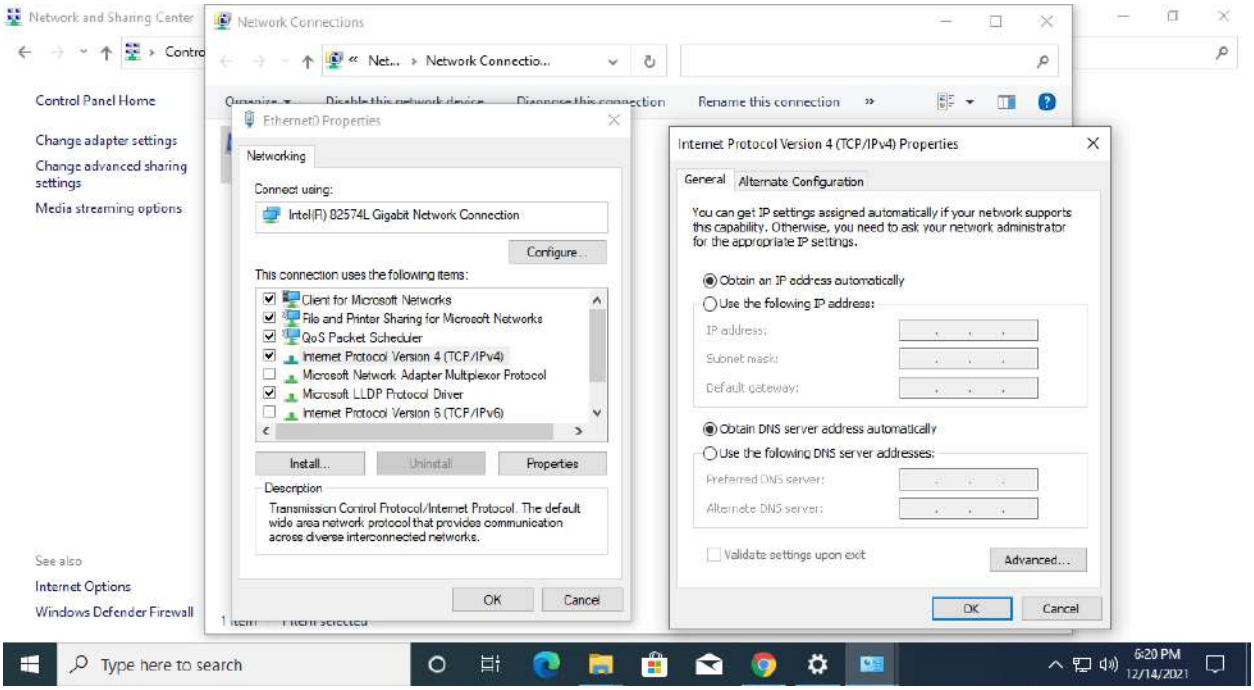
And Disable the Internet Protocol Version 6

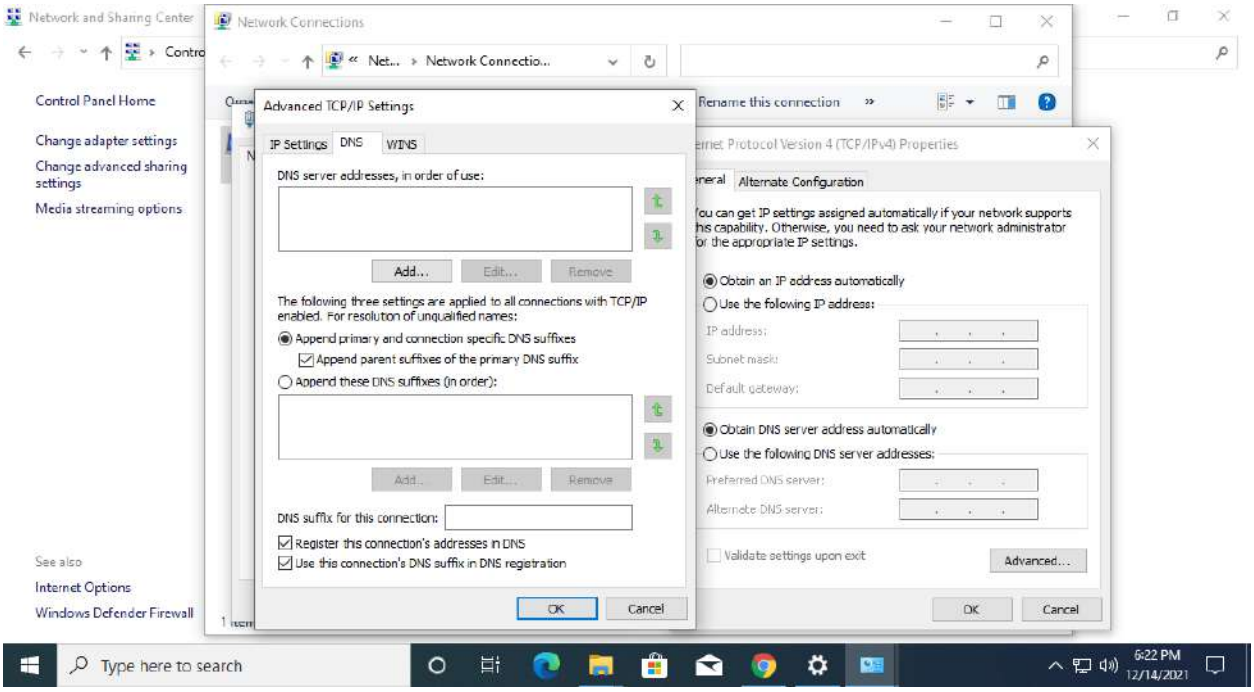




Then go to your IPV4 double click on it.

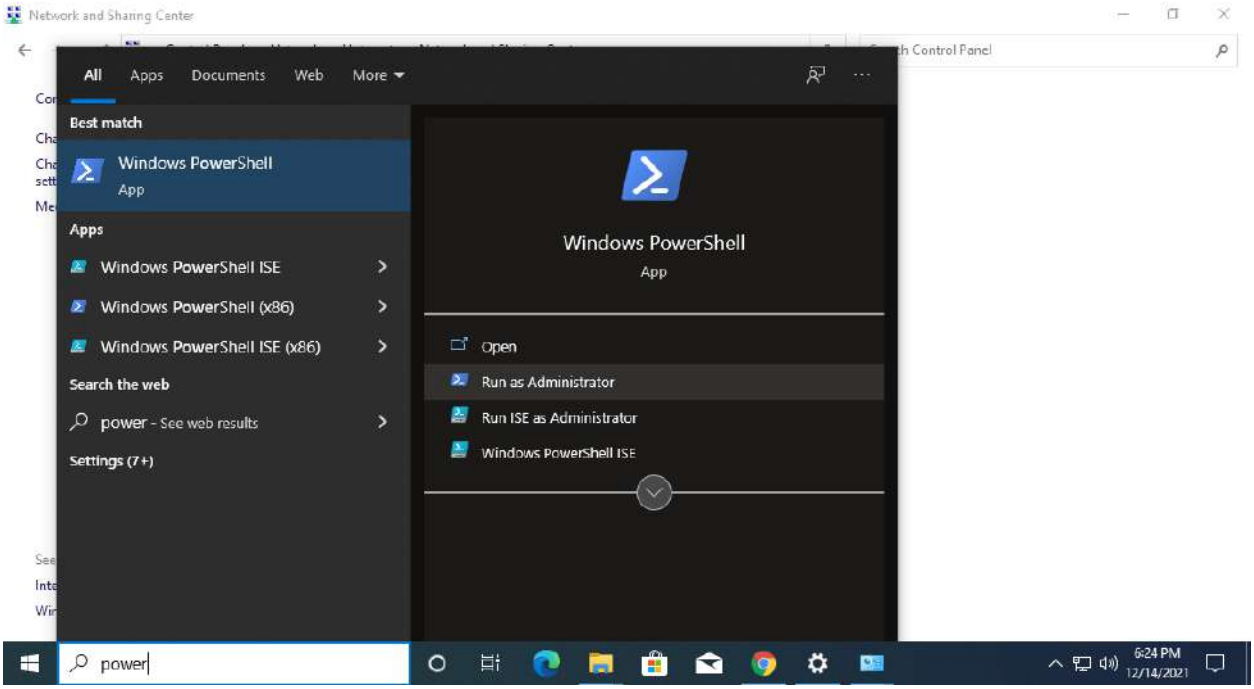
Go to Advanced – DNS – Both of the settings at the bottom of window should be checked.



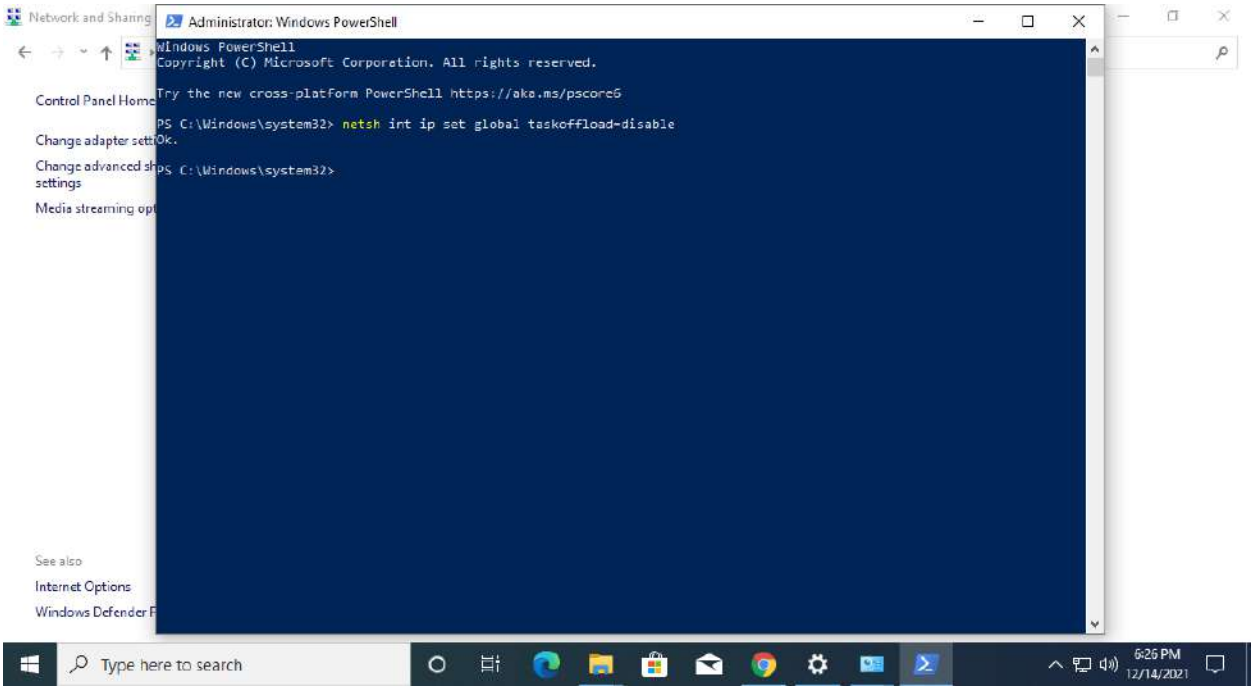


Whichever network adapter you are going to use, you need to do these settings for that network adapter.

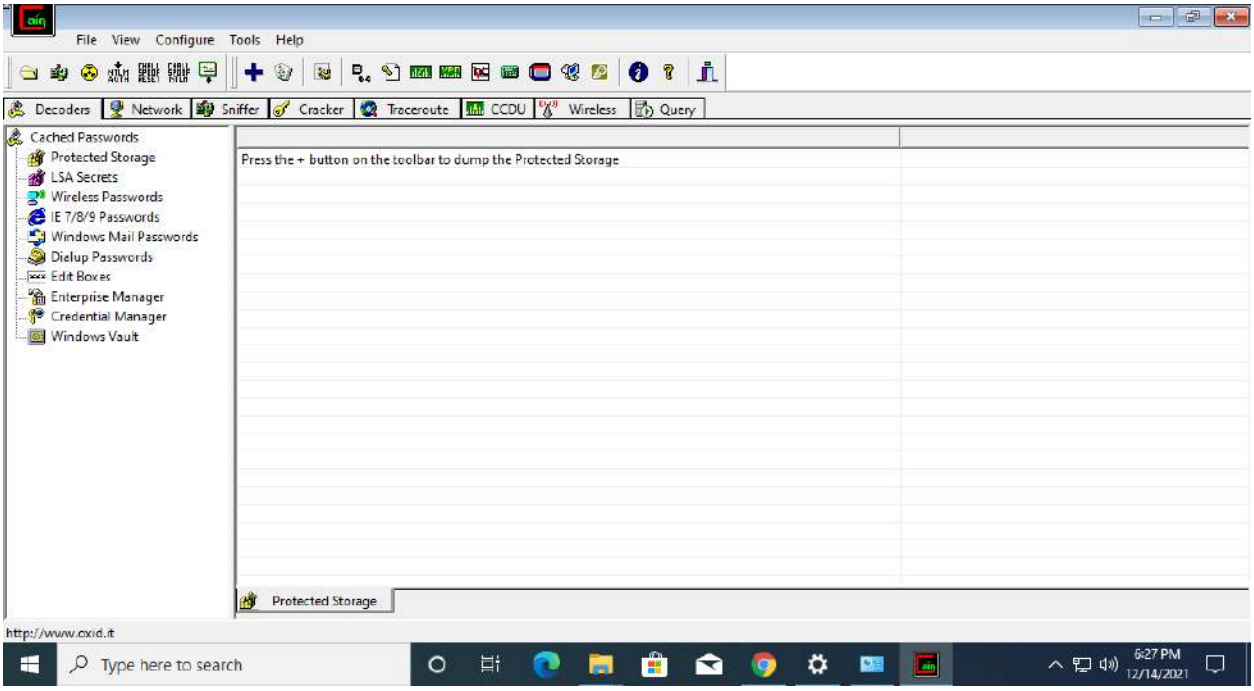
Once you done that open Powershell. Run it as an Administrator.



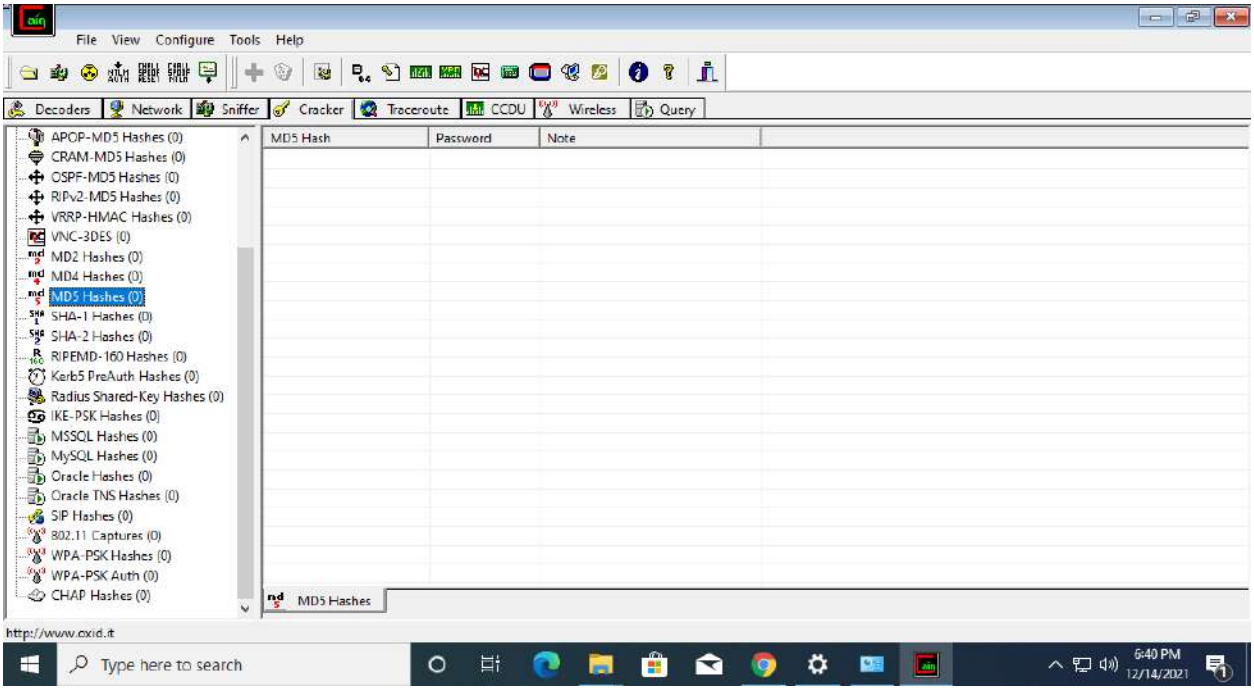
Type the command : netsh int ip set global taskoffload=disable and press enter.



Then run the CainAbel application.

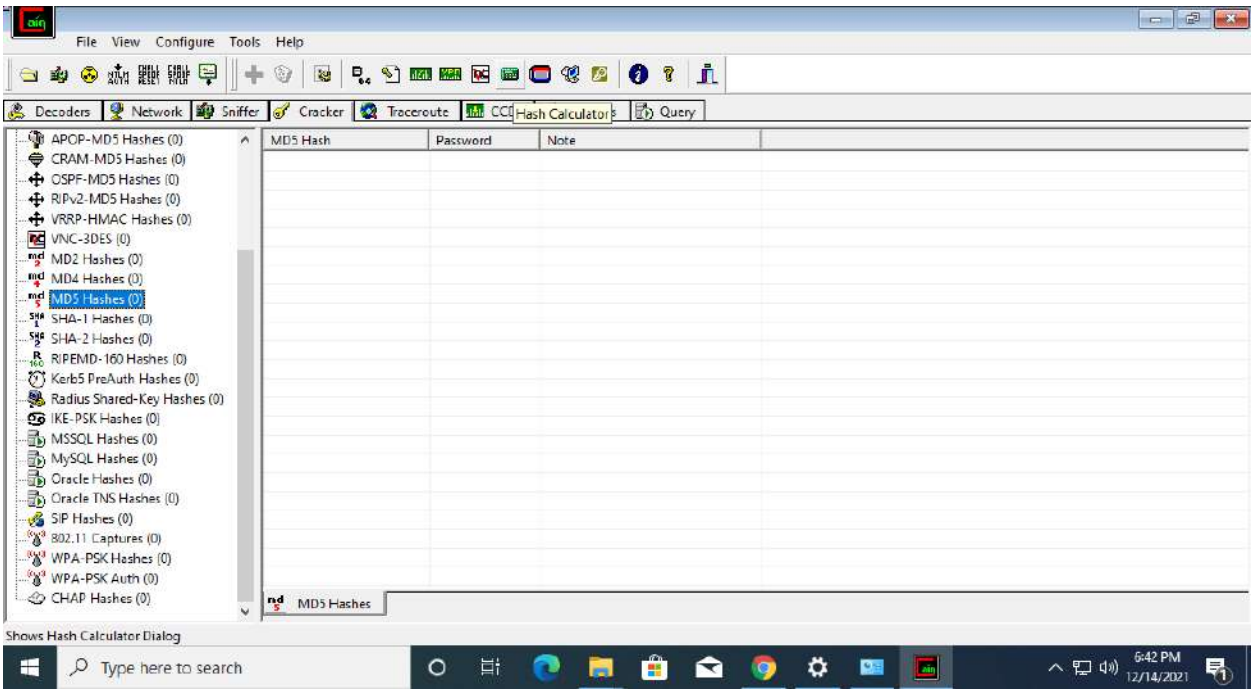


Select the “Cracker” tab with the key symbol, then click on MD5 hashes. The result should look like the image below.

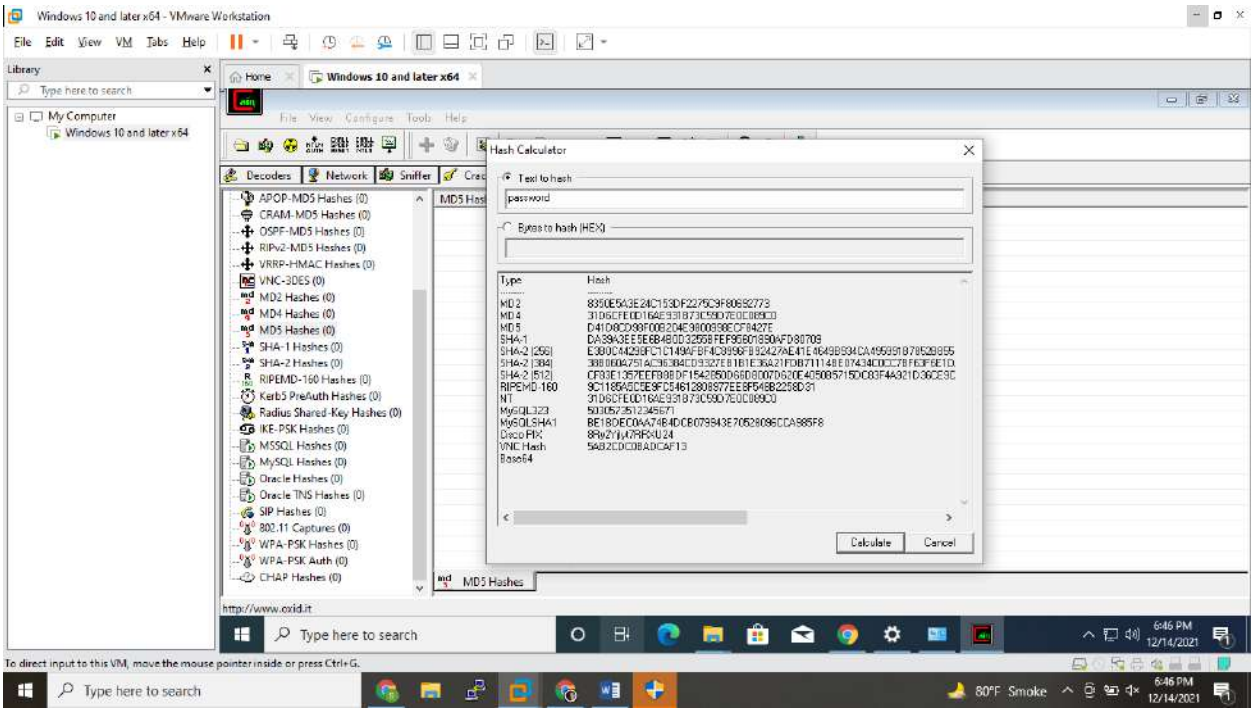


As you have might noticed we don’t have any passwords to crack. Thus for the next few steps we will create our own MD5 encrypted passwords.

First locate the hash calculator among a row of icons near the top. Open it.



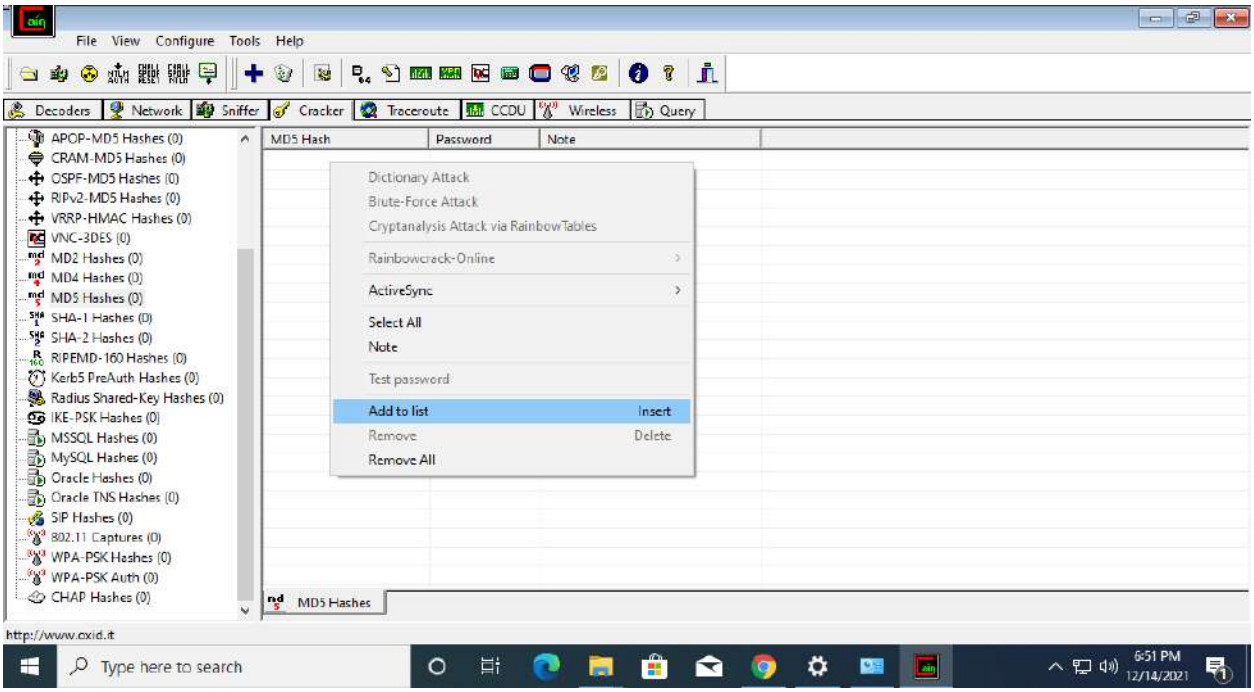
Next type password into text to hash text box. And click on calculate.



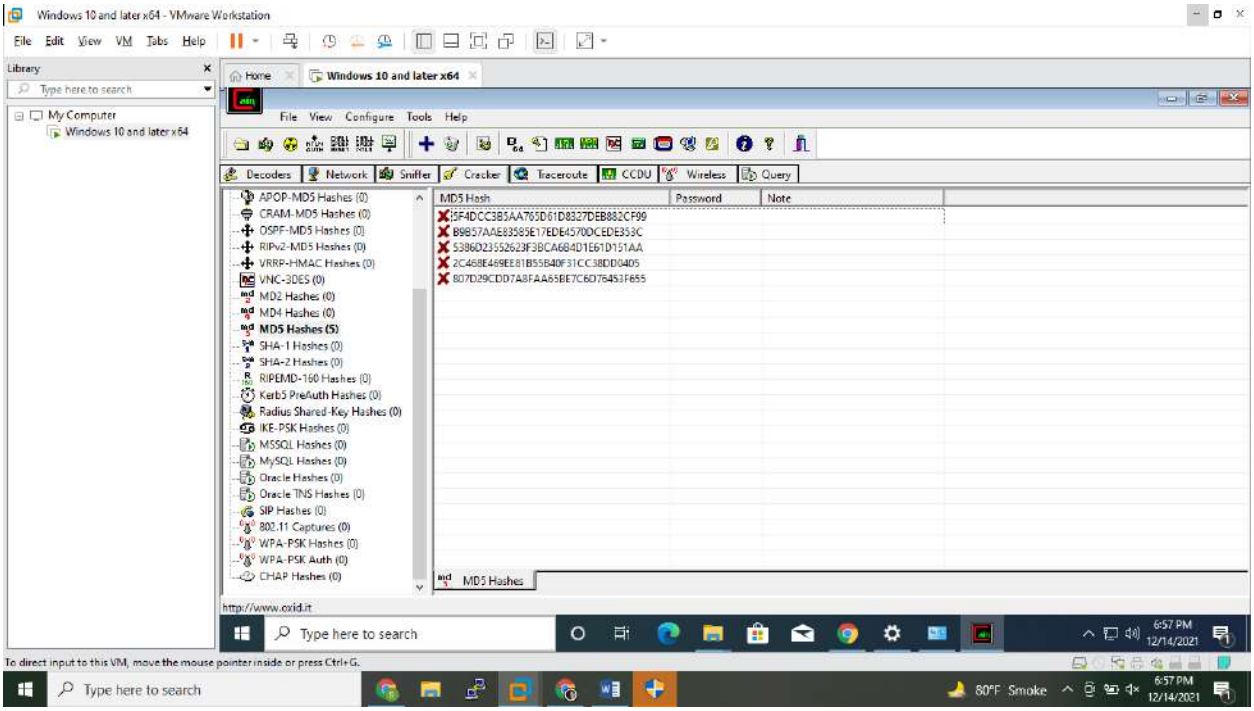
It will generate a list of hases pertaining to different type of hash algorithms. We will be focusing on MD5 hash so copy it. Then exit calculator by clicking cancel.

(Hashes are case sensitive so any slight changes to the text will change the hashes generated, try changing a letter or two and you will see. This is called avalanche effect.)

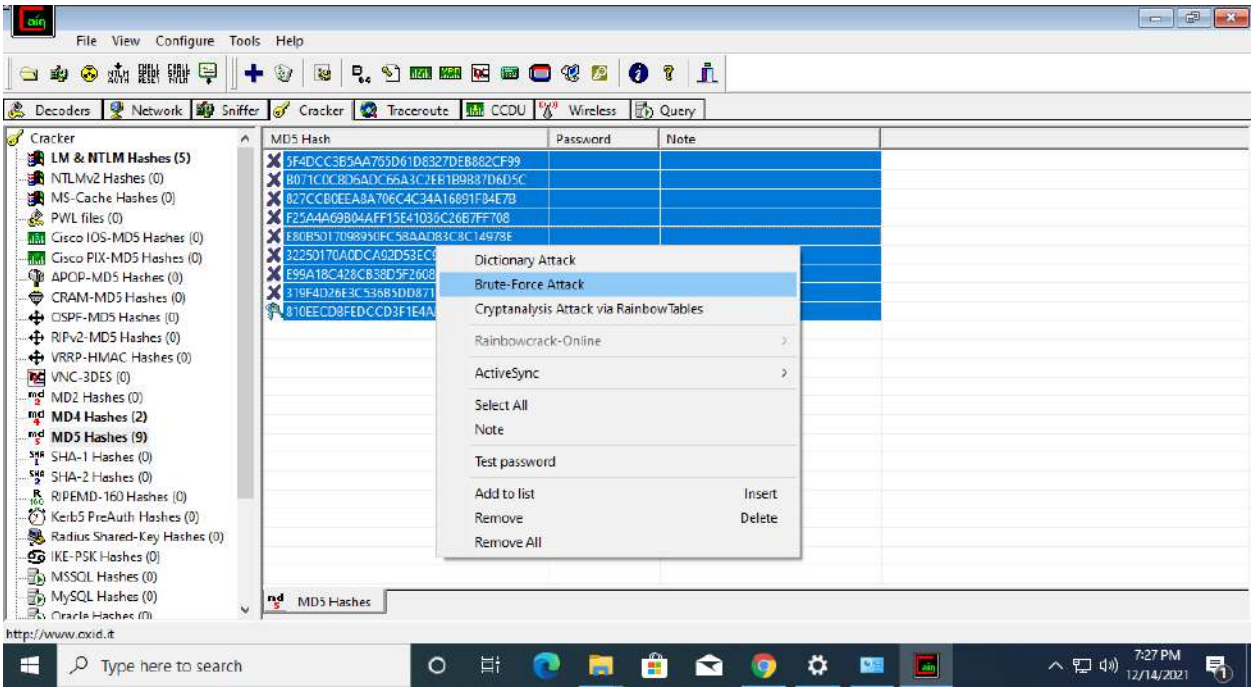
After you exit, right click and select ‘Add to list’, paste your hash then click Ok. Your first encrypted password.

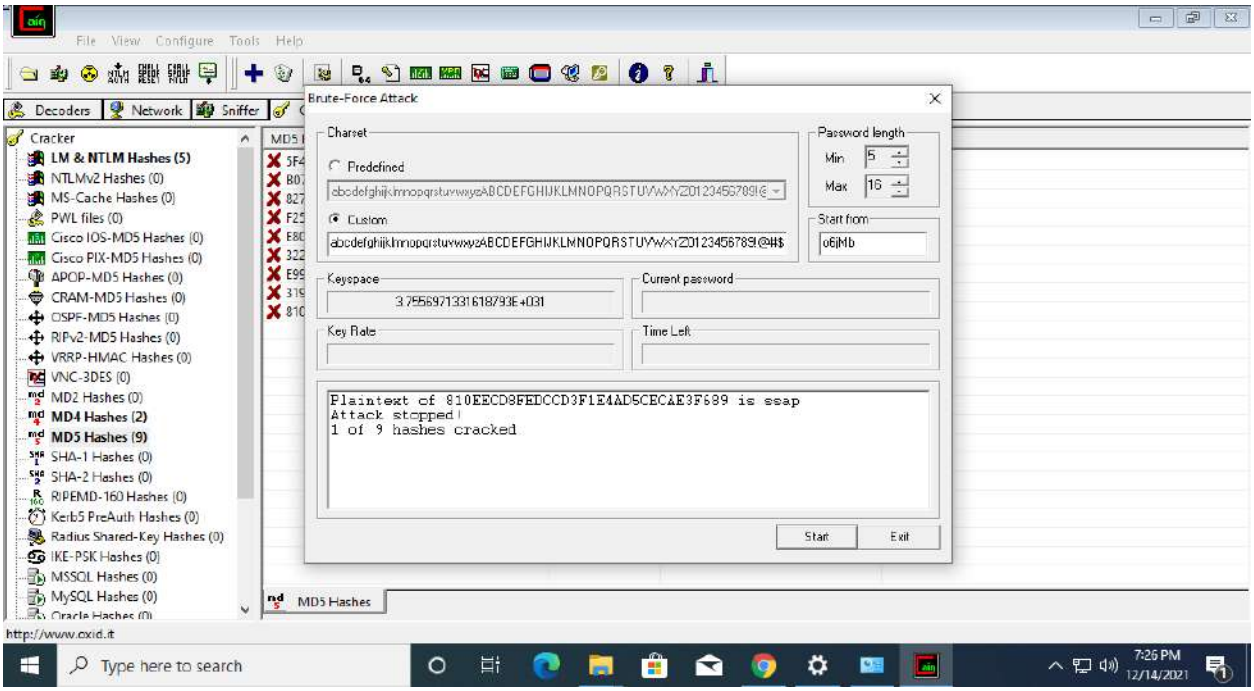


Add few more password : PaSS, ronnie, ssap, 12345, abcde.

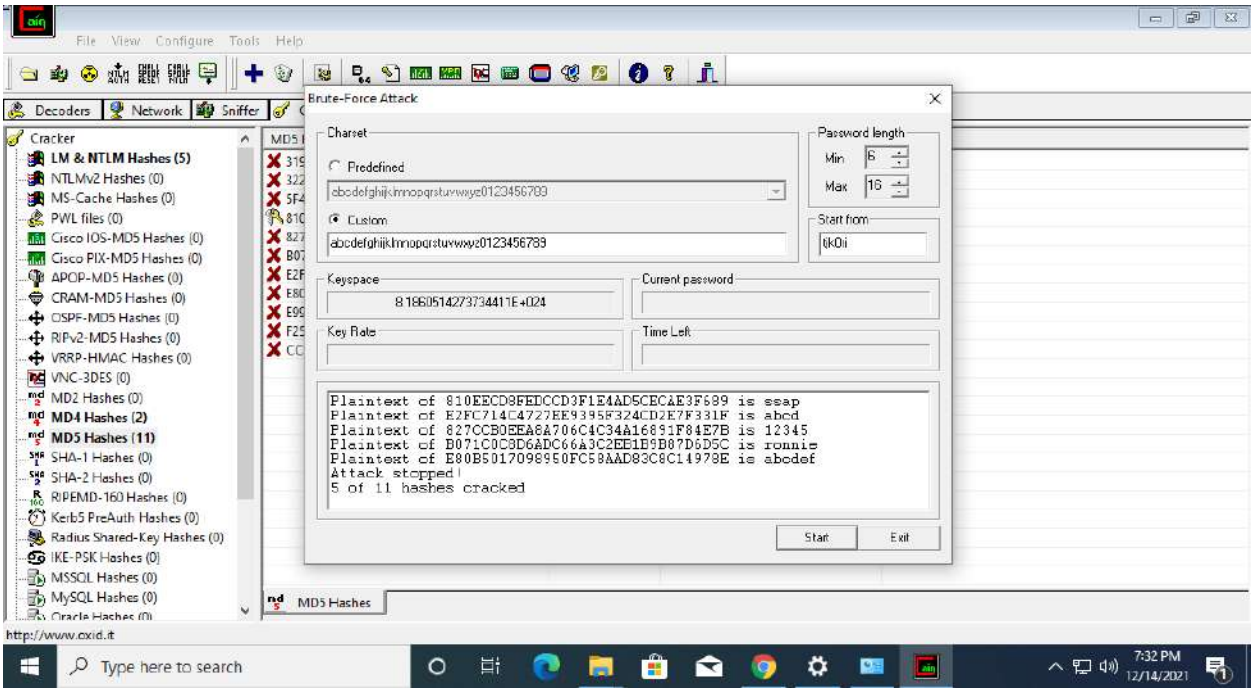


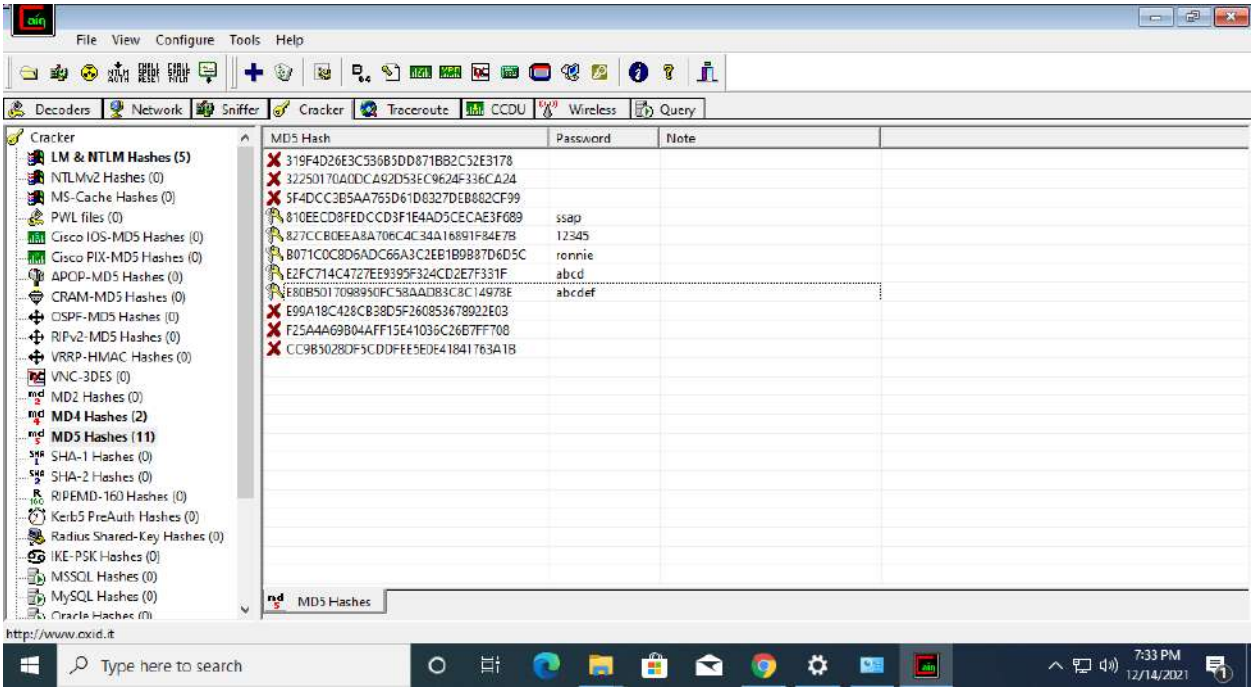
With all the encrypted MD5 password on hand, we can finally start ! Move your cursor and select all the passwords, then right click and press ‘Brute Force Attack’.





As you can see the last entered password ssap was cracked. After some time more passwords has been cracked by Brute force attack.





Softwares Drive Link :-

https://drive.google.com/drive/folders/1wLsniO3NLhkoEUo5FRLcH5BFUnfqhRwV?usp=sharing

Practical No. 11

Aim: Managing Remote Registry, Network Enumeration, Services, s. IDs [Cain and Abel]

What is Remote Registry?

The Remote Registry service enables remote users who have the appropriate permissions to modify registry settings on the domain controller. The service's default configuration allows only members of the Administrators and Backup Operators groups to access the registry remotely. This service is required for the Microsoft Baseline Security Analyzer (MBSA) tool. MBSA enables you to verify which patches are installed on each of the servers in your organization.

If the Remote Registry service stops, only the registry on the local computer can be modified. If you disable this service, any services that explicitly depend on the service cannot start, but registry operations on your local computer are not affected. However, other computers or devices cannot connect to your local computer's registry.

This service is installed by default, and its startup type is **Automatic**.

The Remote Registry service is dependent upon the following system components:

When the Remote Registry service is started in its default configuration, it logs on by using the Local Service account.

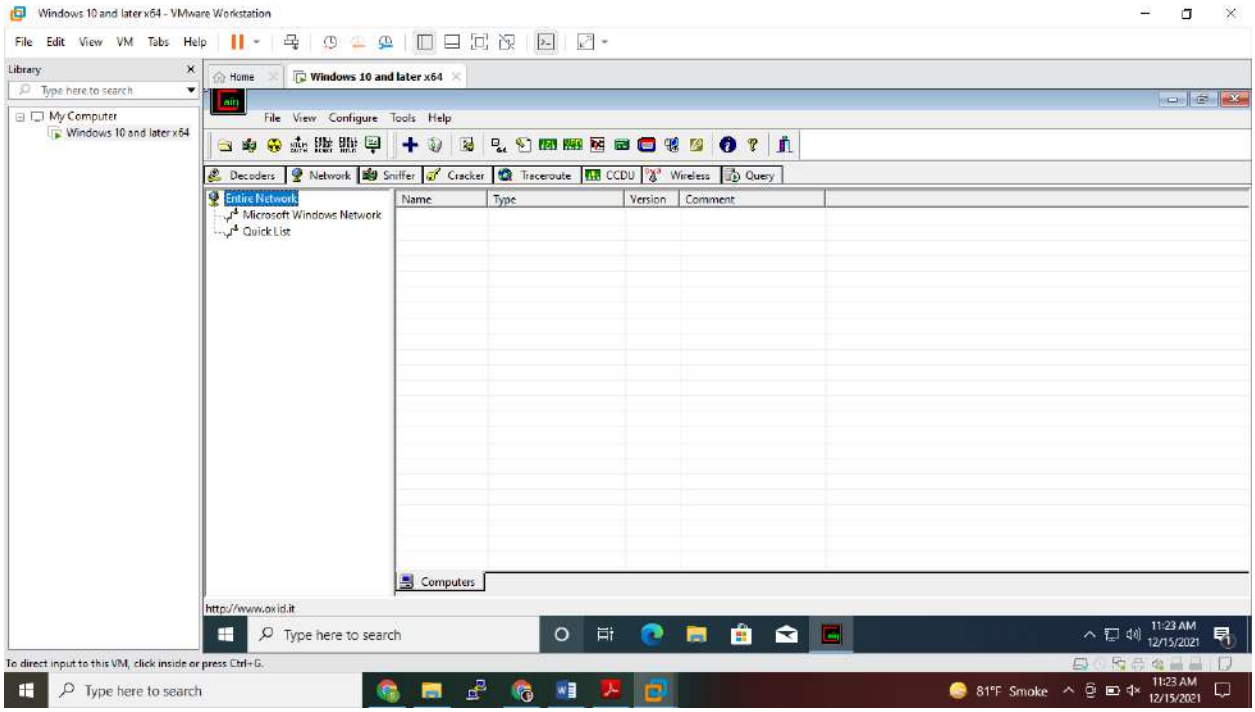
- Remote Procedure Call (RPC)
- DCOM Server Process Launcher
- RPC Endpoint Mapper

What Does Network Enumeration Mean?

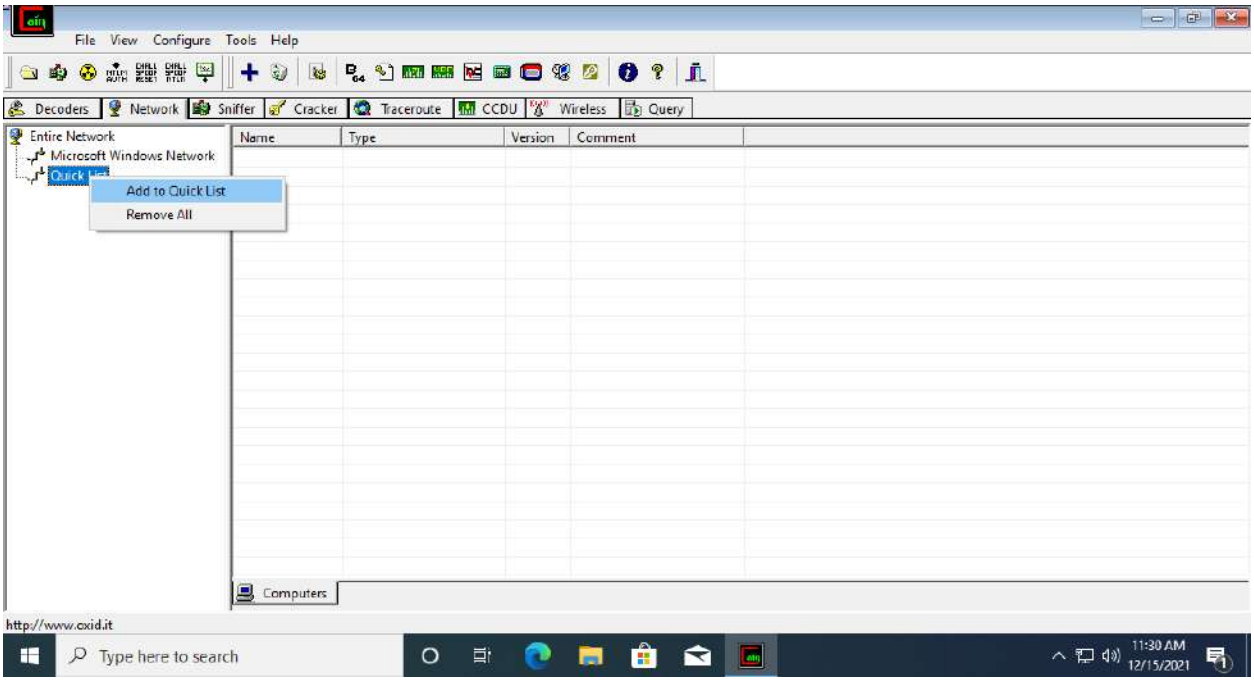
Network enumeration is a process that involves gathering information about a network such as the hosts, connected devices, along with usernames, group information and related data. Using protocols like ICMP and SNMP, network enumeration offers a better view of the network for either protection or hacking purposes.

Steps:

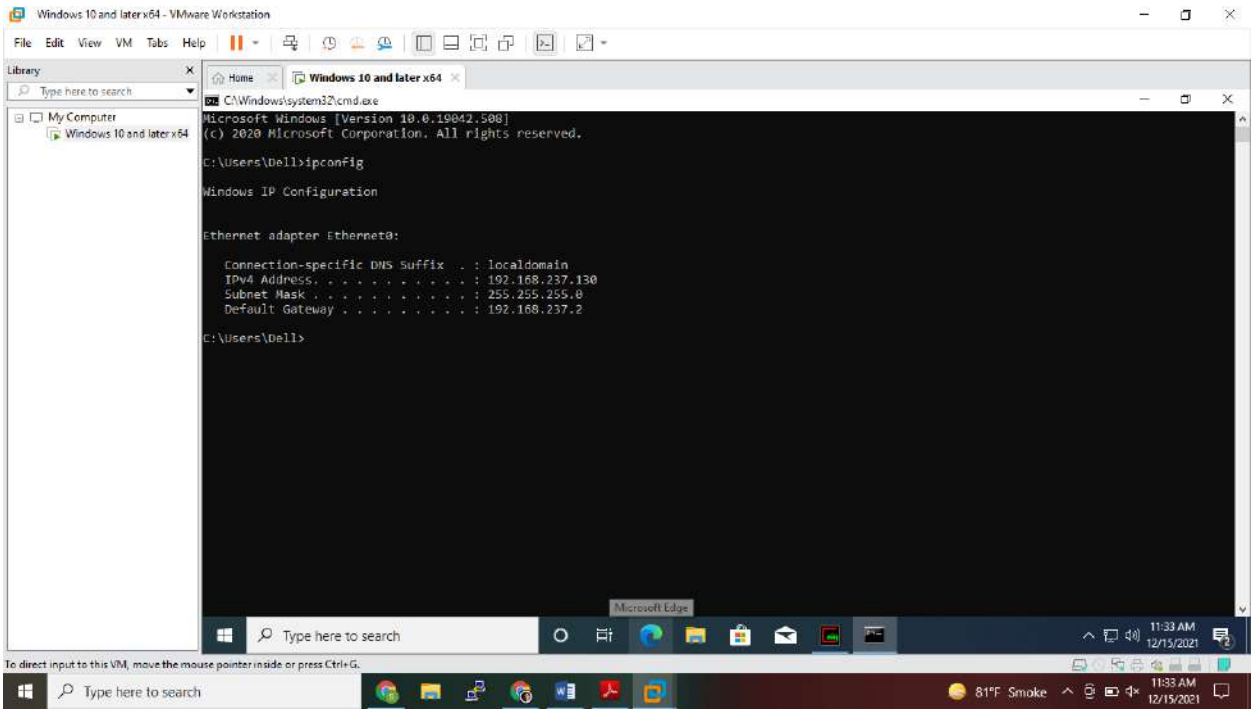
1) Start your virtual machine. Run the CainAbel as an administrator.
2) Go to Network tab.



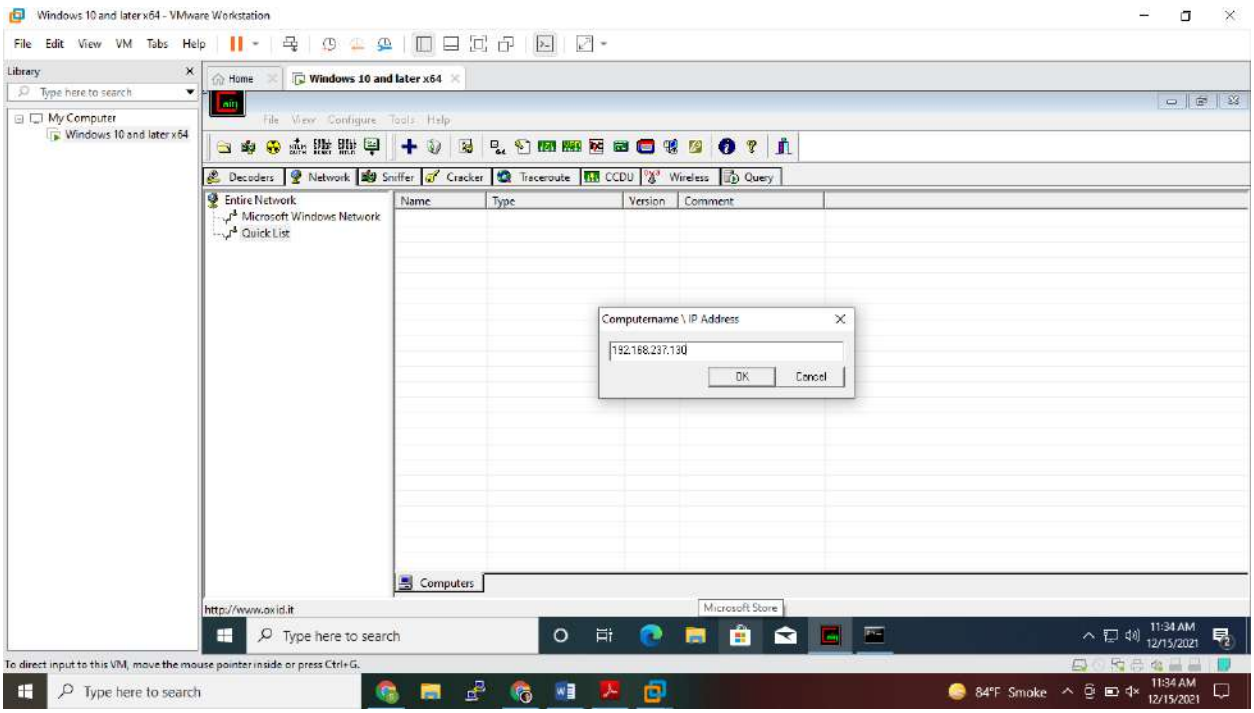
3) Expand entire network.
   Right click on Quick list & select add to quick list.



4) In the resulting popup box, enter the ip address of the system you want to study.
(You can use your ows system's IP address to examine your registry.)



Click on Ok



To Access Other System's Registry & Services, Use That System's IP Address Right Click On The Account And Enter User Credentials (Necessary Only If Using Accessing Other System)

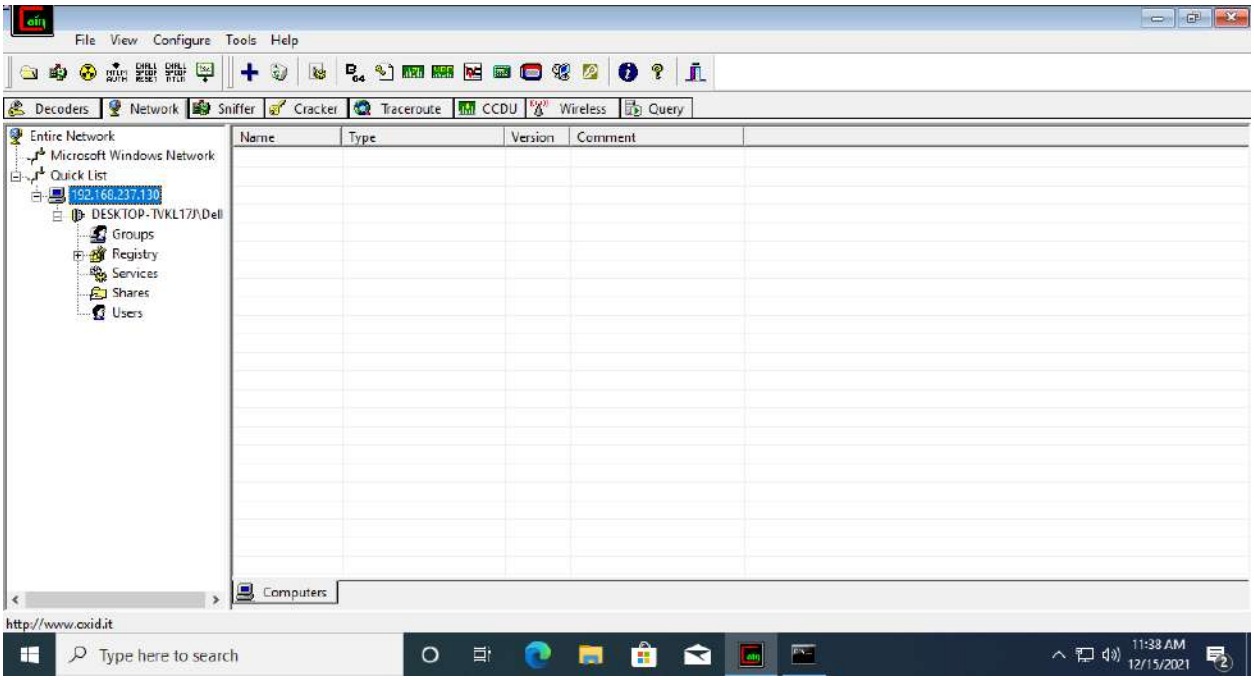
5) Double Click To Expand, This Will Provide Access To The
a. Groups

b. Registry

c. Services

d. Shares

e. Users

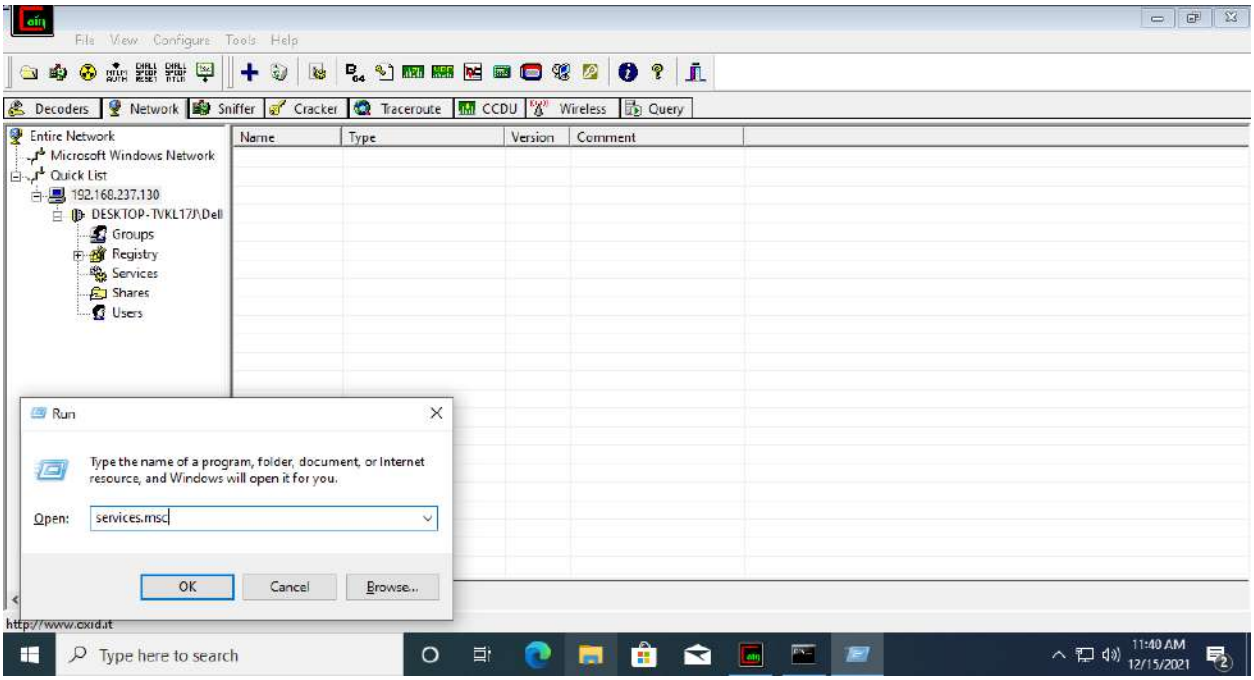


6) Make Sure To Start 'Remote Registry' Service In Both The PCs, Including Yours & The System You Are Investigating At.

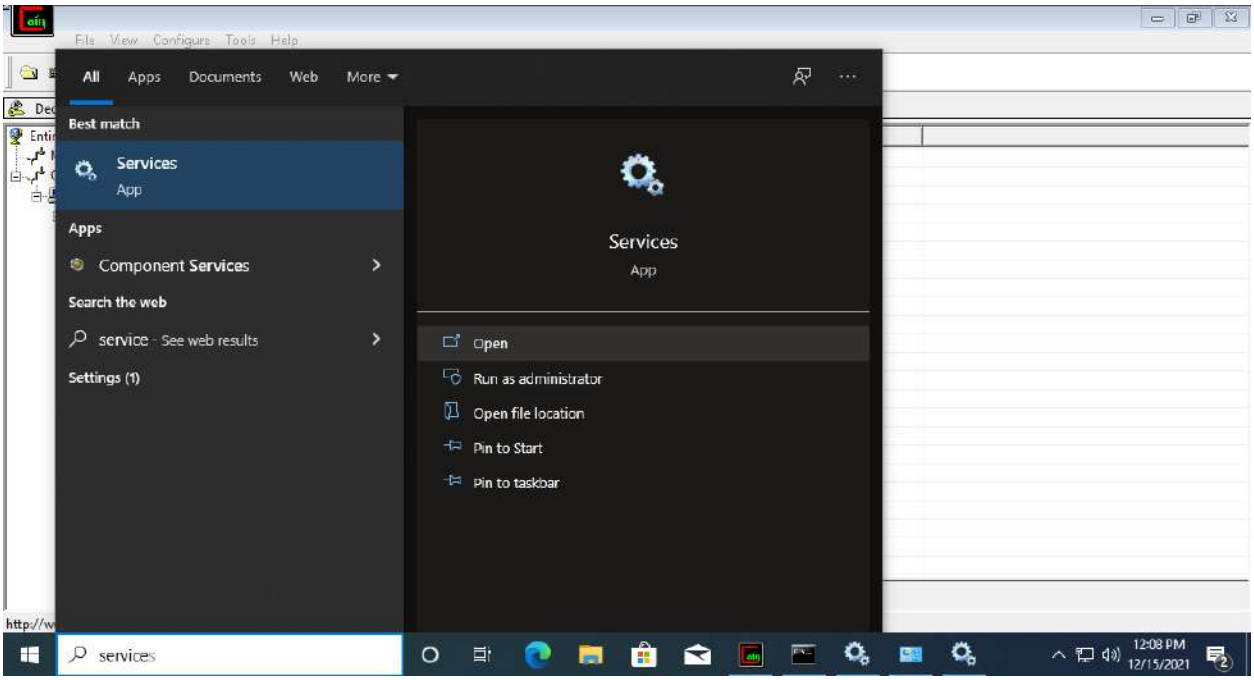
Do Windows + R & Type services.msc

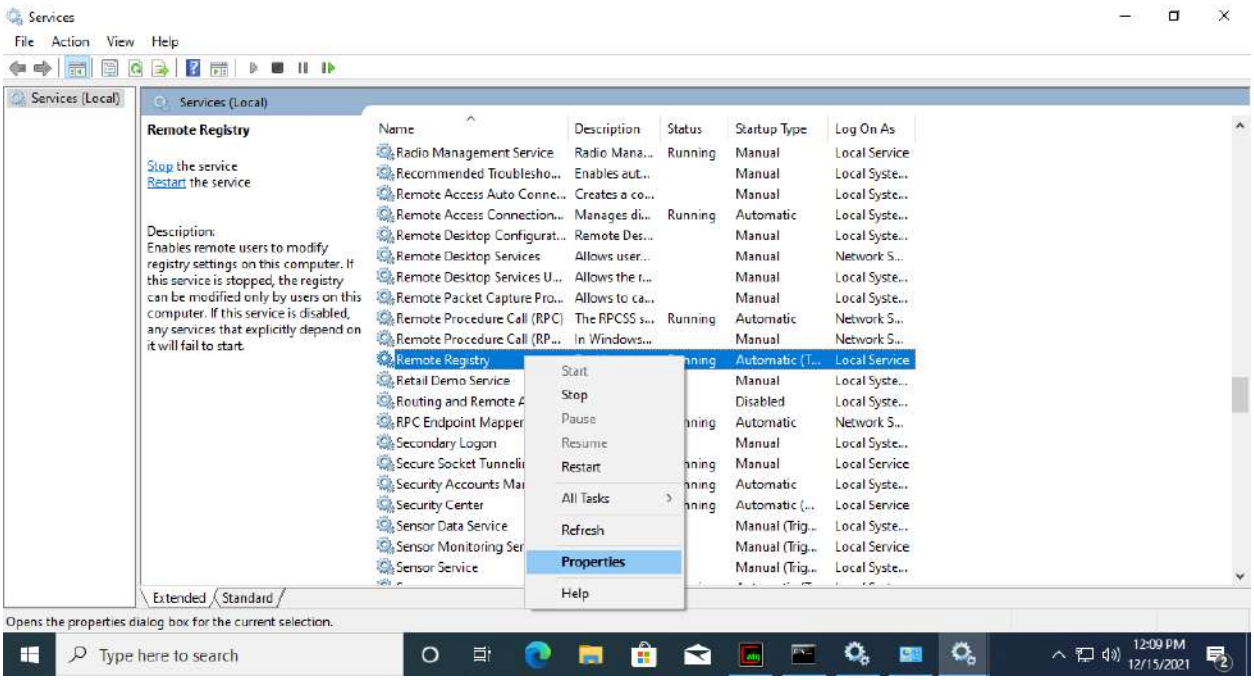
Start Remote Registry Service

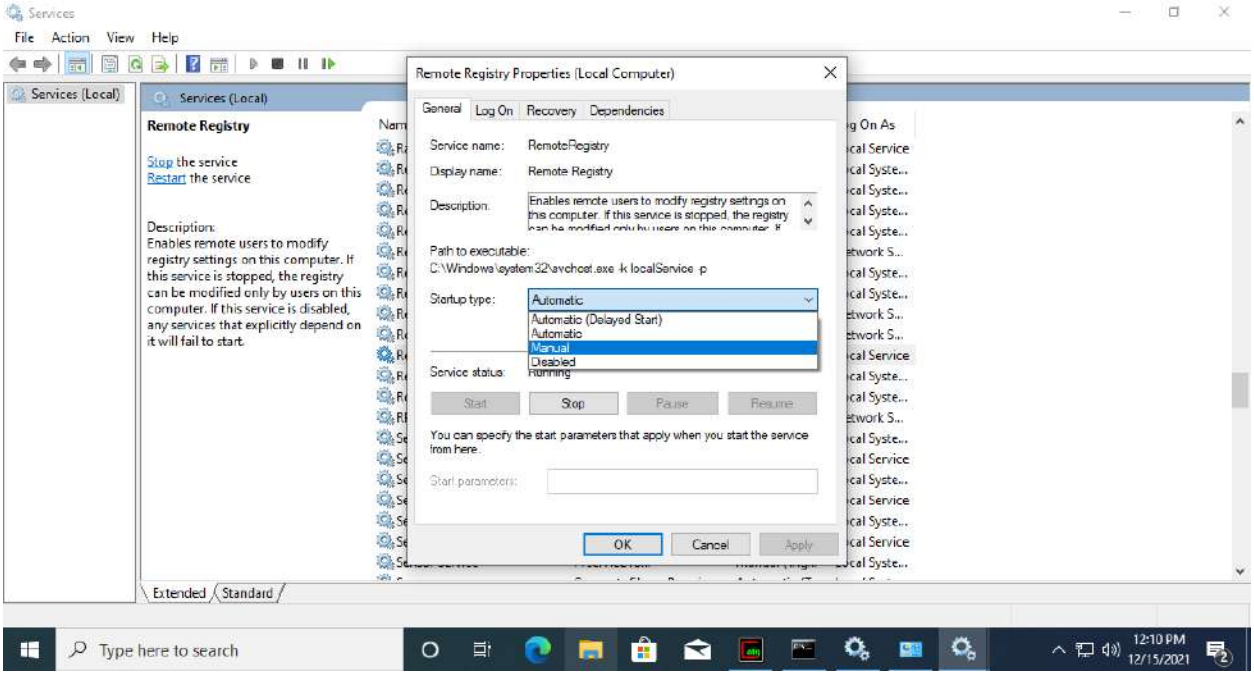
7) You Can Make Changes In The Registry By Traversing Through The Folders



Open the services App – Remote Registry – Right click on it – Properties – Startup type should be Automatic – Then Click on ok and Then on Start.

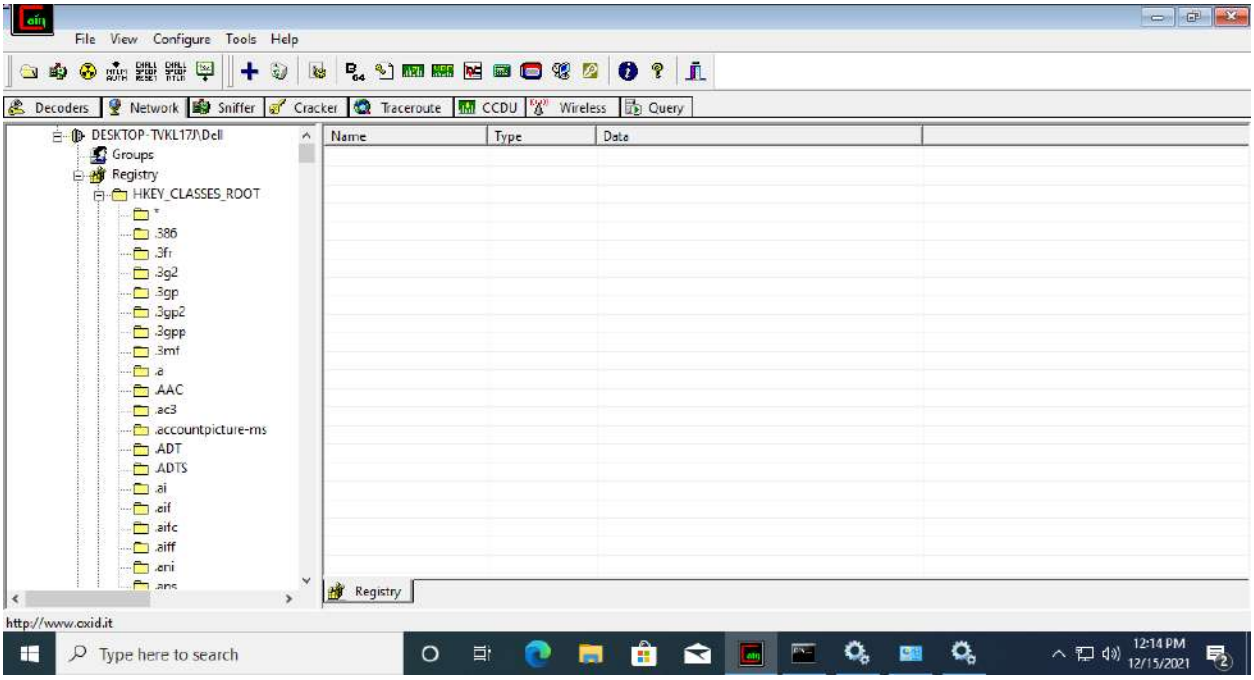


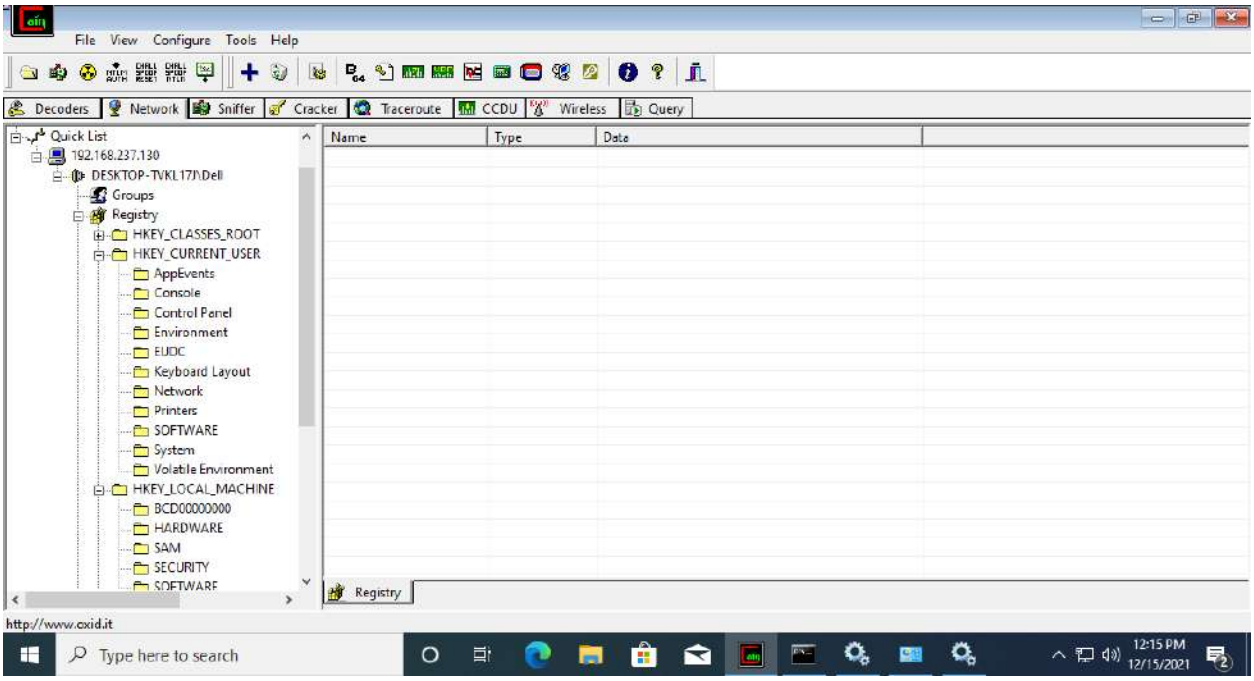


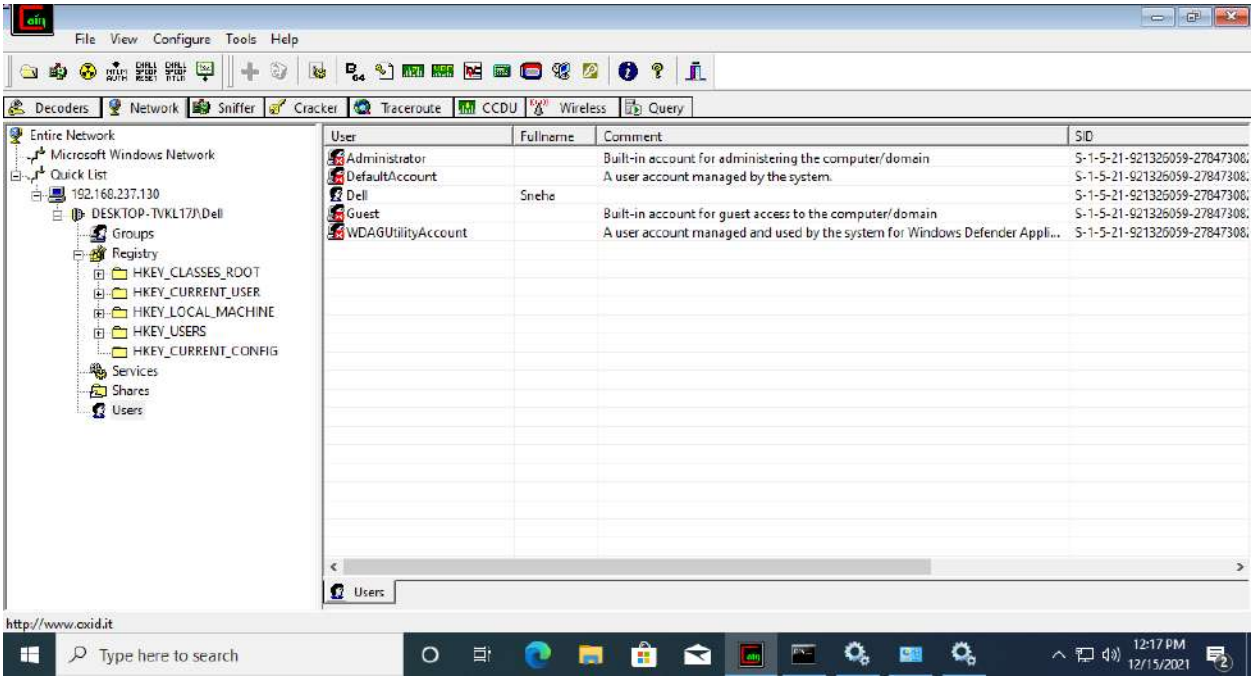


Changes Can Also Be Done In Services Section, Groups, Shares & Users (Network Enumeration) Can Be Viewed

As Well.


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
DESKTOP-TVKL17J\Dell
Groups
Registry
HKEY_CLASSES_ROOT
.386
.3fr
.3g2
.3gp
.3gp2
.3gpp
.3mf
.a
.AAC
.ac3
.accountpicture-ms
.ADT
.ADTS
.ai
.aif
.aifc
.aiff
.ani
Name
Type
Data
Registry
http://www.oxid.it
Type here to search
12:14 PM
12/15/2021


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Quick List
192.168.237.130
DESKTOP-TVKL17J\Dell
Groups
Registry
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
AppEvents
Console
Control Panel
Environment
EUDC
Keyboard Layout
Network
Printers
SOFTWARE
System
Volatile Environment
HKEY_LOCAL_MACHINE
BCD00000000
HARDWARE
SAM
SECURITY
Name
Type
Data
Registry
http://www.oxid.it
Type here to search
12:15 PM
12/15/2021



Practical No. 12

Aim: Investigating Website using FAW

What is FAW?

THE BEST PROTECTION FOR YOUR RIGHTS ON THE WEB

FAW (Forensics Acquisition of Websites) was born as a forensic browser for the acquisition of web pages with legal value.

FAW has been developed in compliance with national and international regulations, scientific papers and best practices of Digital Forensics.

IT TAKES AN ANALYTICAL AND COMPLETE PHOTOGRAPHY OF ANY CONTENT PRESENT ON THE NET

In order to obtain a valid and effective evidence in a judicial proceeding starting from web pages several acquisition technical aspect need to be considered. Indeed, it is necessary to comply with strict procedural legal rules as well as to follow best practices recognized by the forensic scientific community and experts on this field.

FAW is an innovative software simply to use. It guarantees a valid forensics acquisition method.

NEW FORM FOR THE ACQUISITION OF FACEBOOK PAGES

Expert witnesses and law enforcement agencies use FAW to extract digital evidences from the social network. It is possible to acquire complete profiles, comments, posts, photos and videos, friends, groups, likes and reactions, places, payment histories, saved collections, advertisements and information on access protection.

FORENSIC ACQUISITION OF YOUTUBE'S VIDEOS

With this module it is possible to automatically crystallize the test for legal purposes and legal value including all the texts, main video and all the multimedia elements.

CONCRETE AND UNCHANGED TESTS

FAW allows to obtain the legal proof and keep it safe with all the necessary security controls that guarantees to avoid any alteration of the data or “simply” to relies on as against third parties the authenticity of the data acquisition, thanks to the service offered by Namirial, which operates as a Certification Authority.

WHO USE FAW?

FAW is made for law enforcements, investigators, technical consultants, experts witnesses, notaries, lawyers, but also simple private individuals who ma encounter legal proofs, or important evidences, which could be easily wasted away / mutated / altered or lost, sometimes compromising the success of a “dispute”.

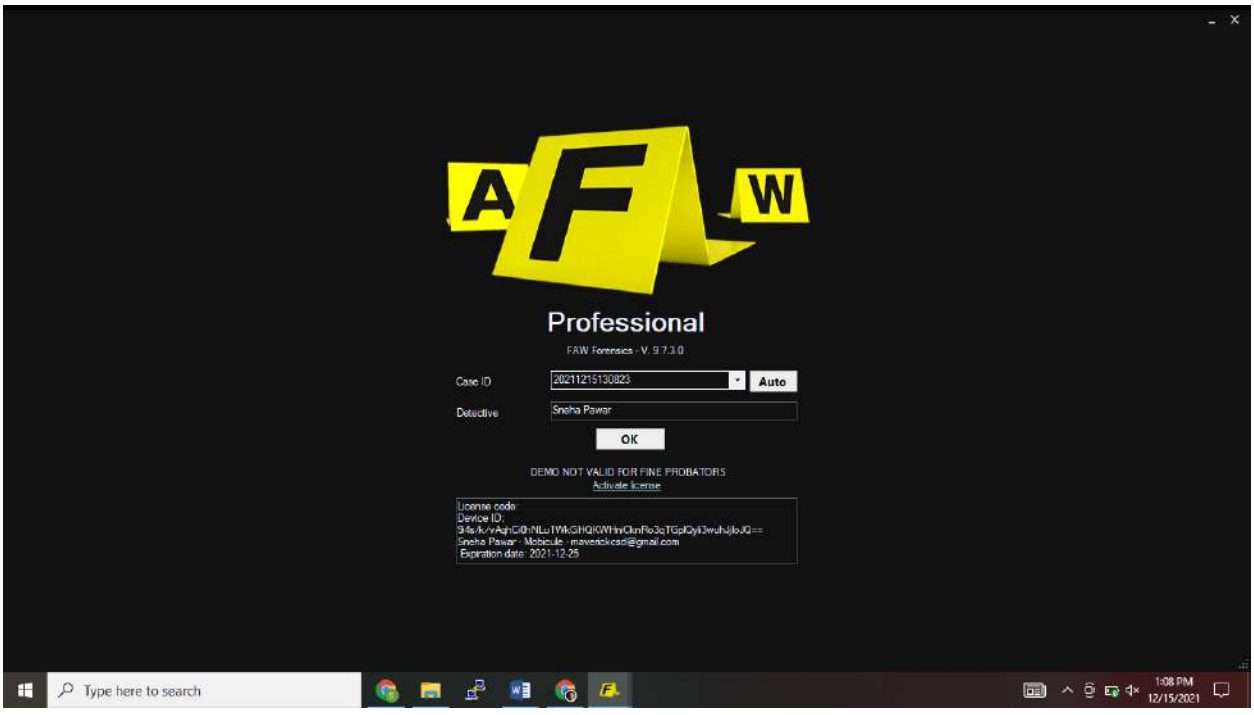
Download FAW software setup from following website and install:

While installing this software Npcap software will also get installed

https://en.fawproject.com/download/

Open FAW. Select your language, enter details, the application will start.

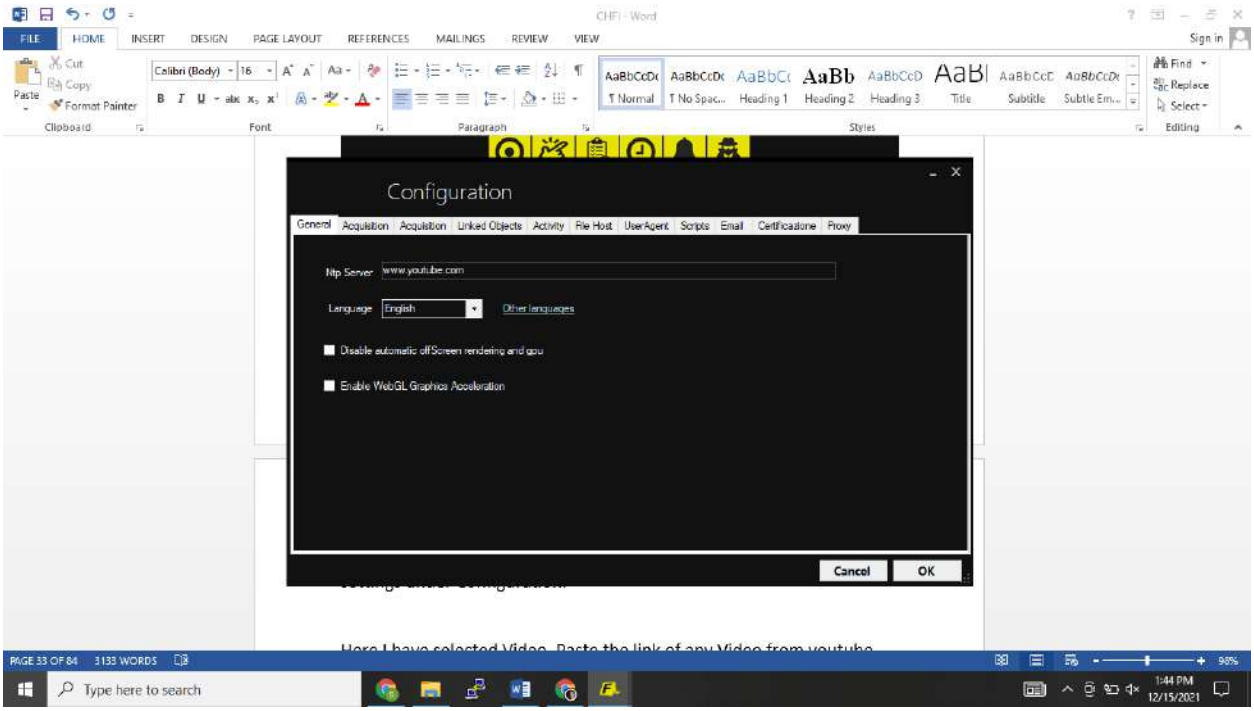
Generate Case ID Auto. Enter detector’s name.



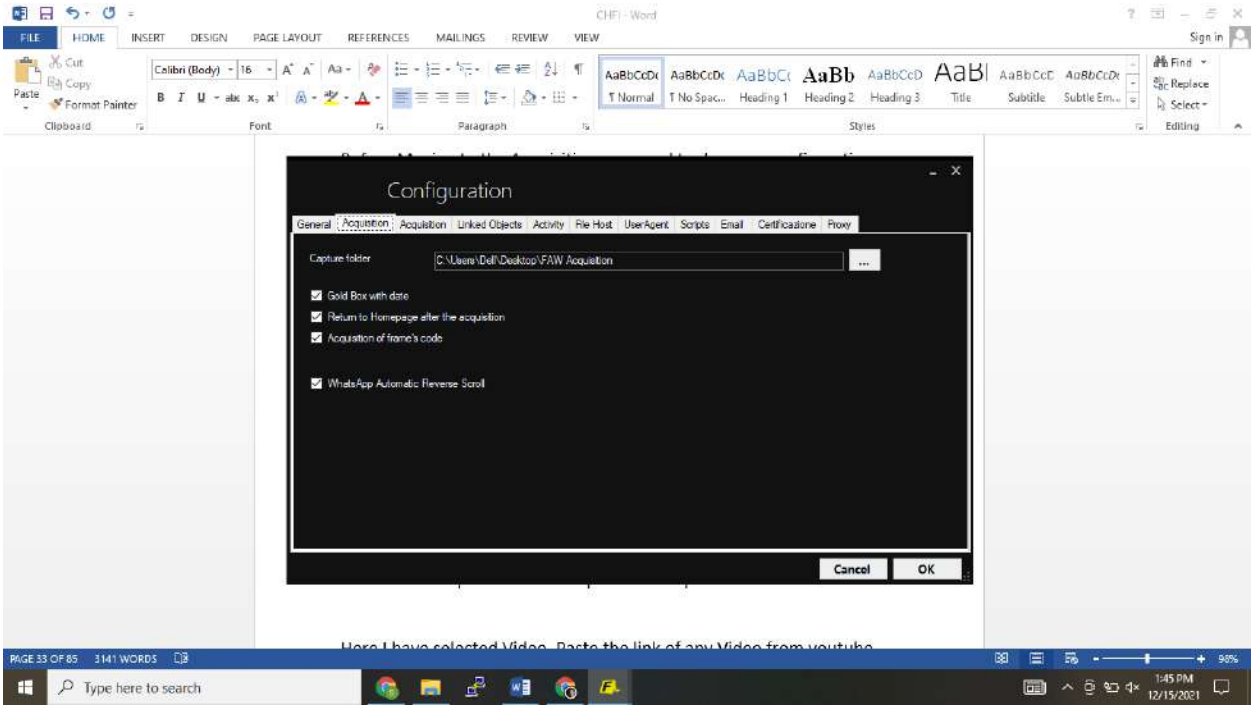
Select any social platform from below options.

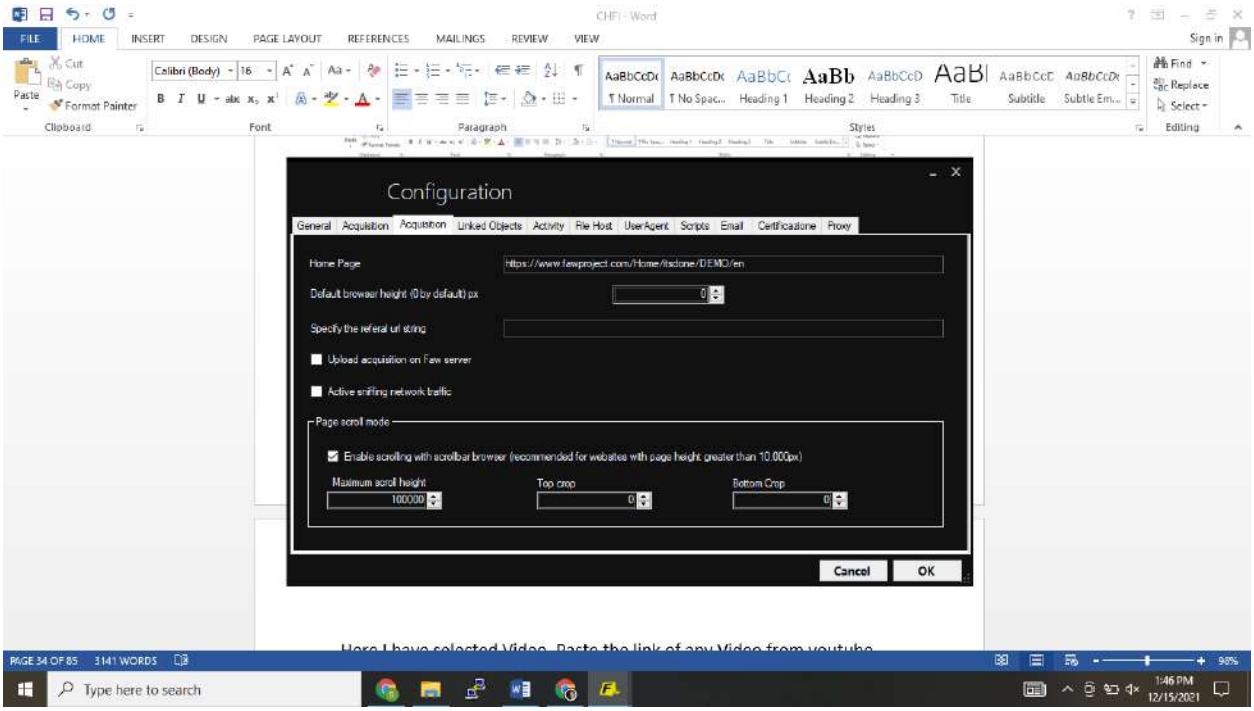
Before Moving to the Acquisition you need to do some configuration settings under Configuration.

General

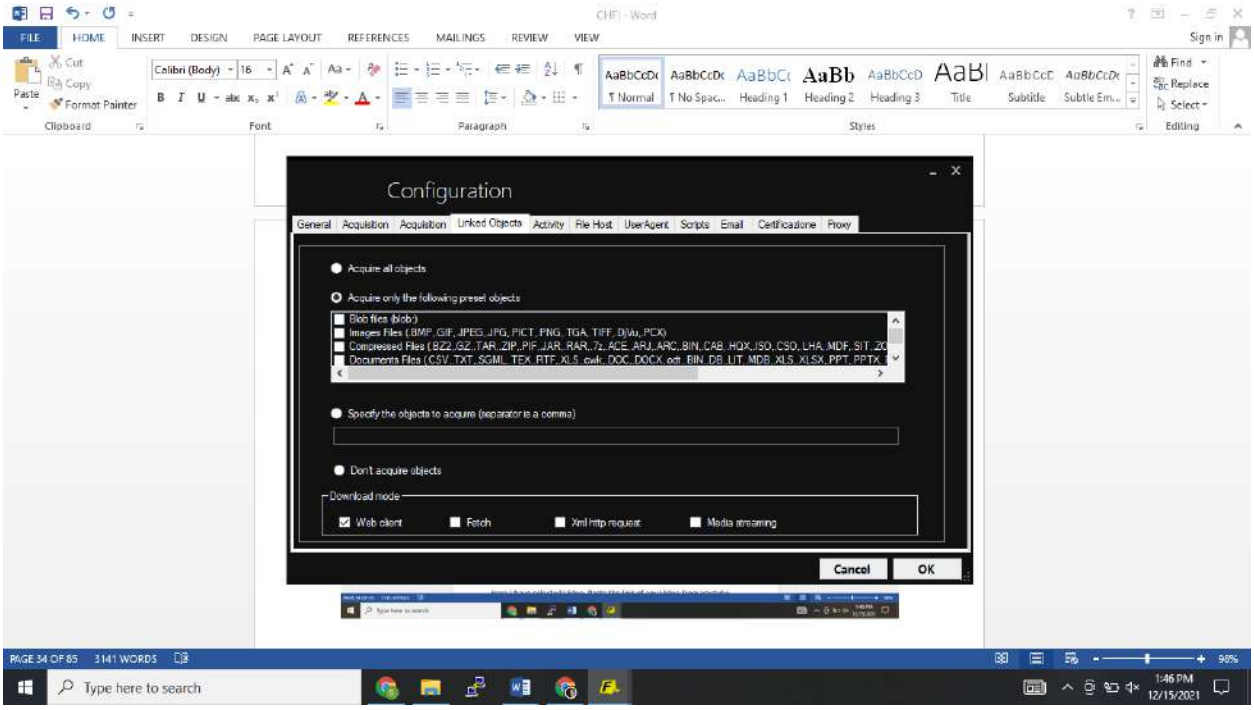


Then under acquisition enter capture folder path.

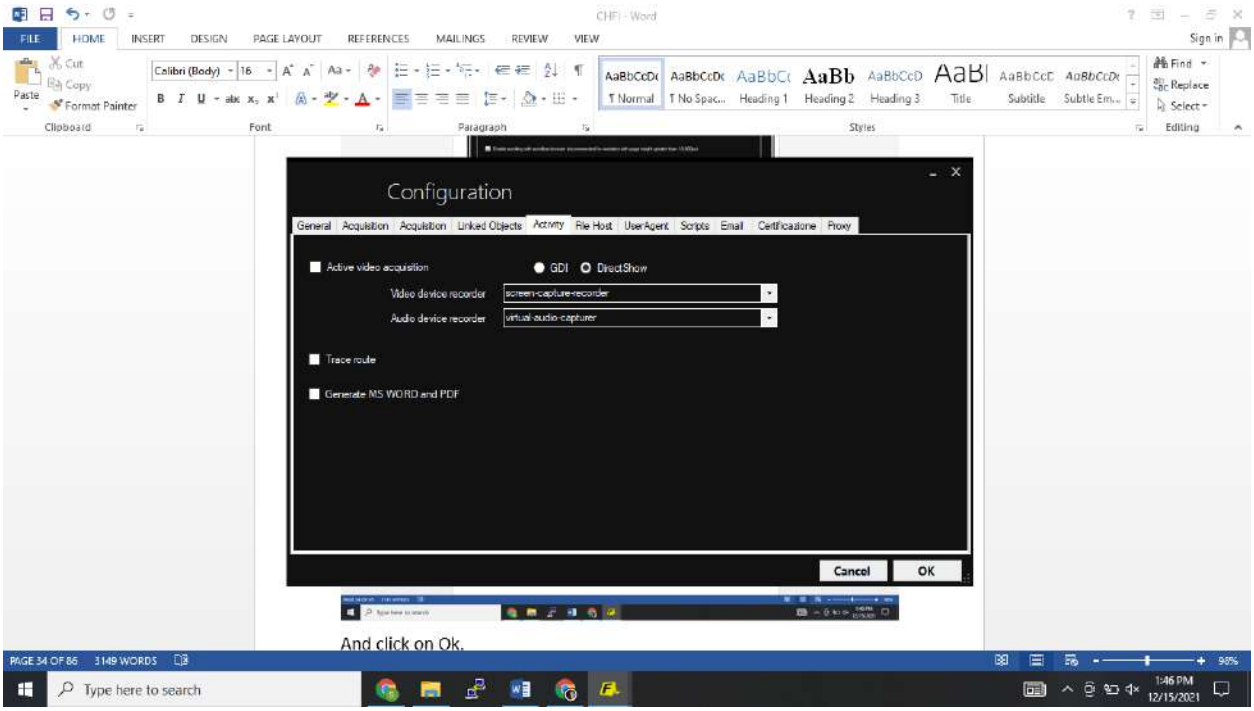




Under Linked Objects :



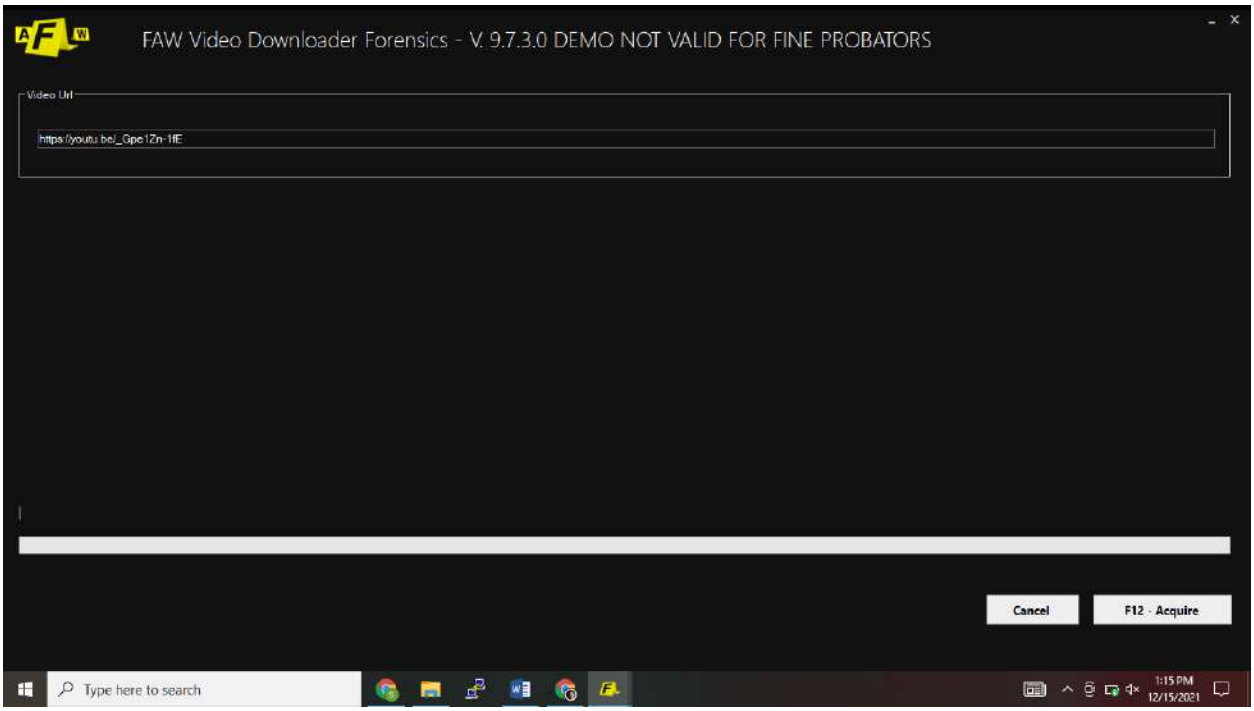
Under Activity tab



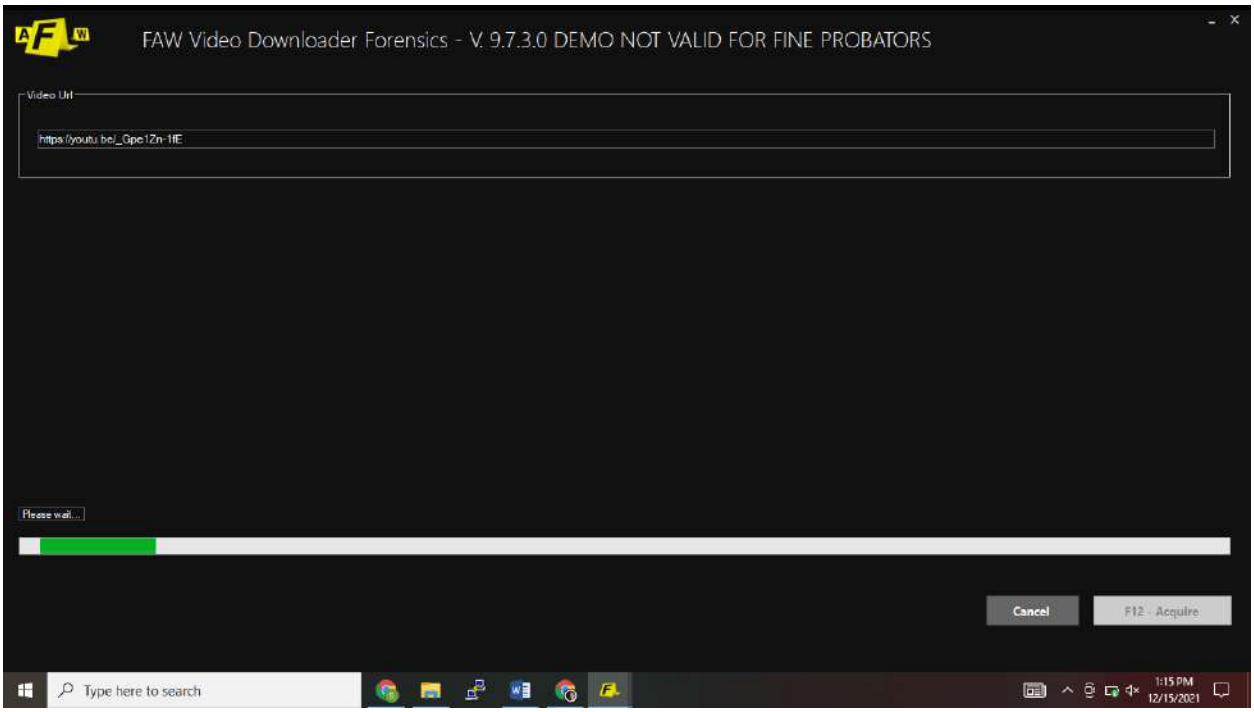
And click on Ok.

Then select option from various types. Here I have selected Video. Paste the link of any Video from youtube.

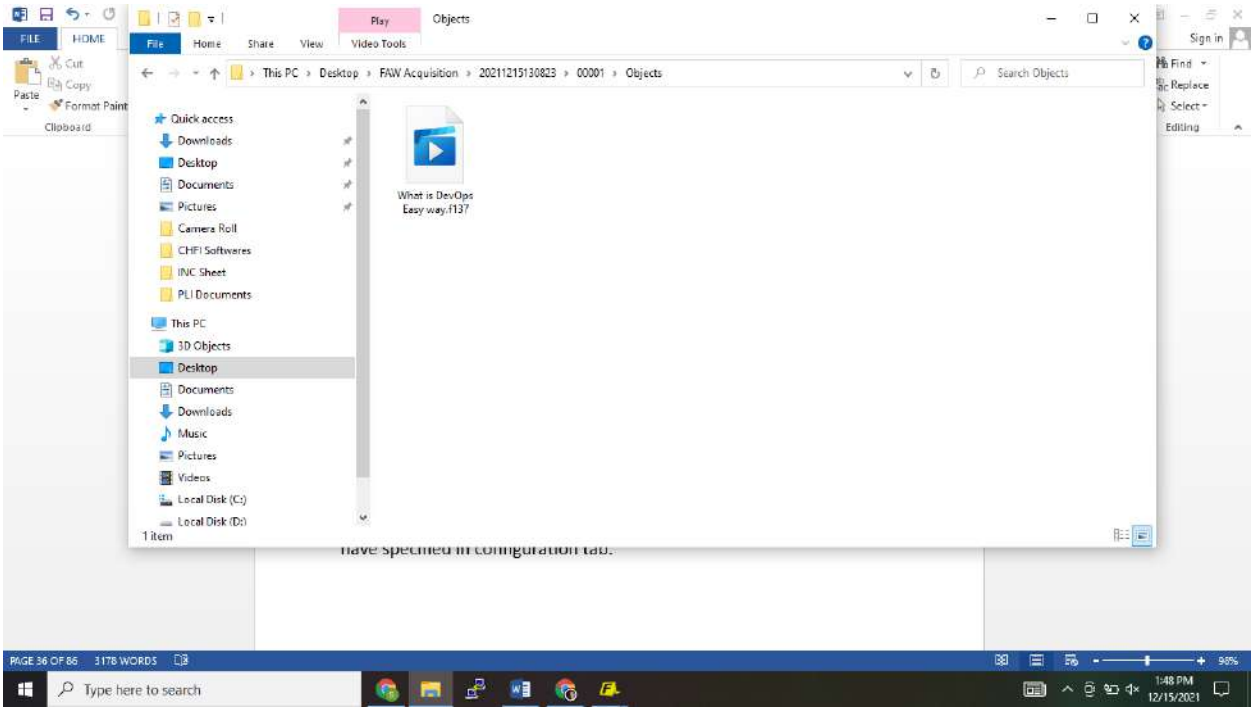
https://youtu.be/_Gpe1Zn-1fE

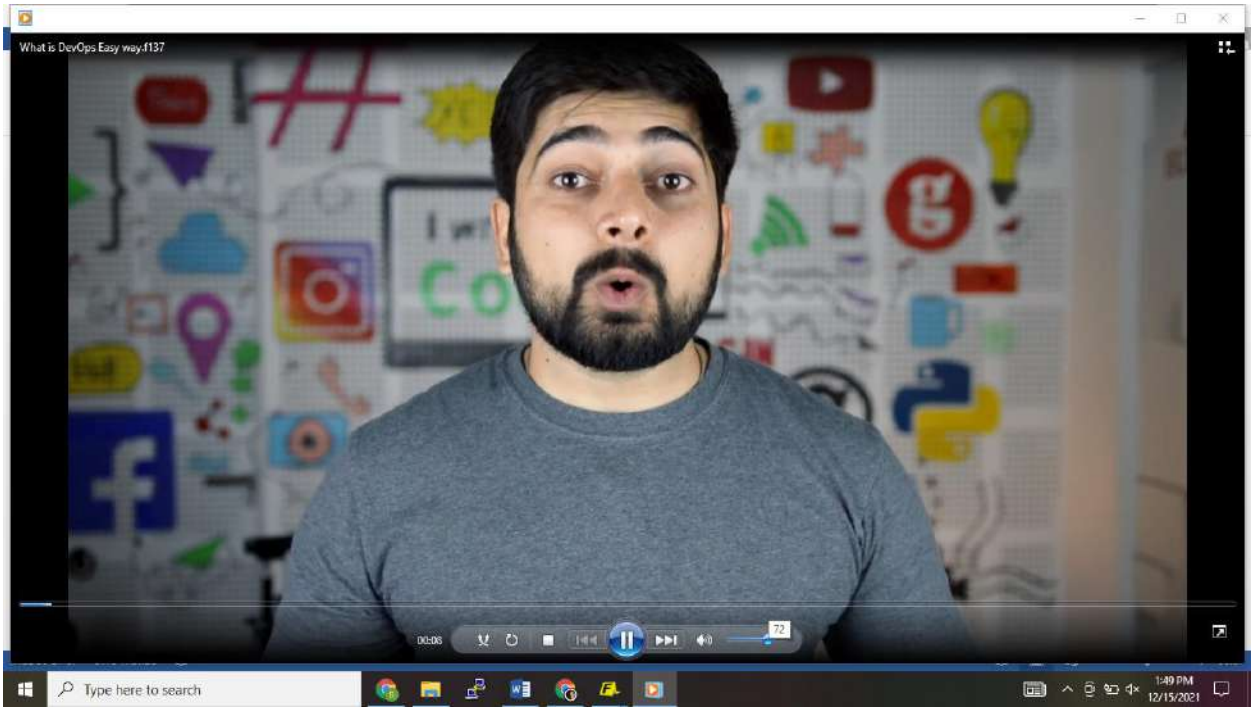


And click on F12 – Acquire.



You will get to see the entire video has got acquired in the folder you have specified in configuration tab.





Similarly you can do with other options.

Here I have acquired the content from instagram

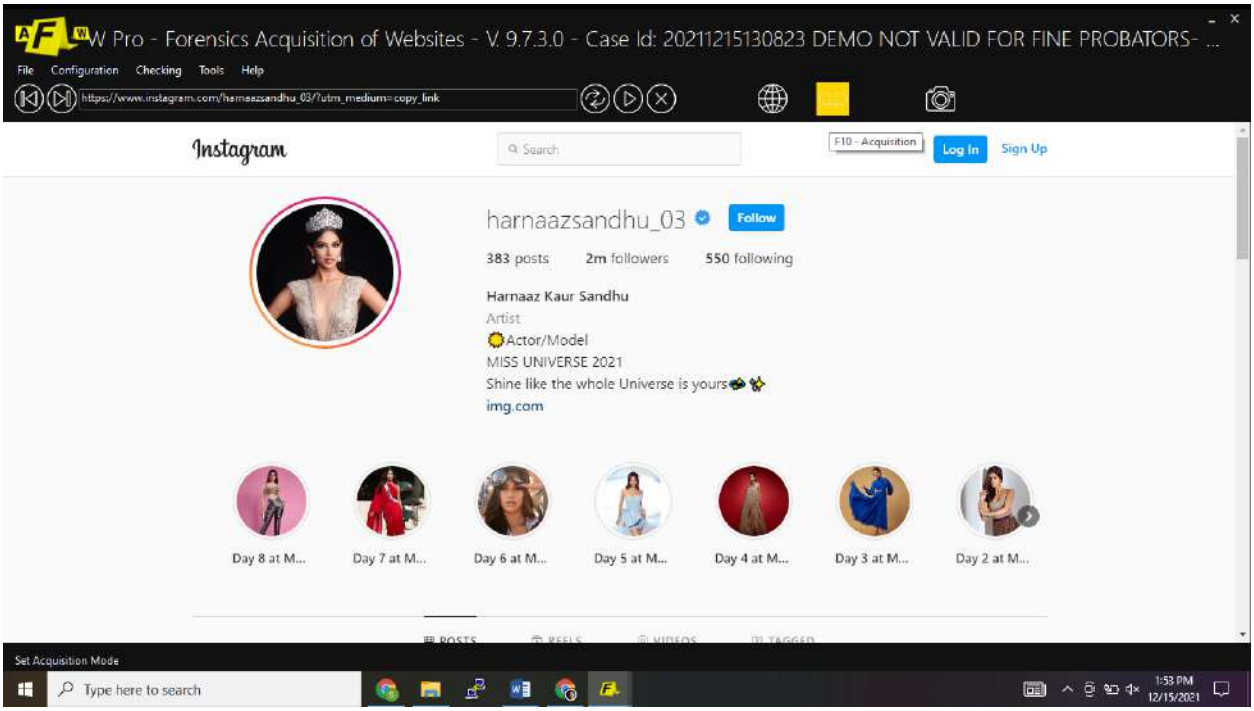
Select Instagram option and paste the link

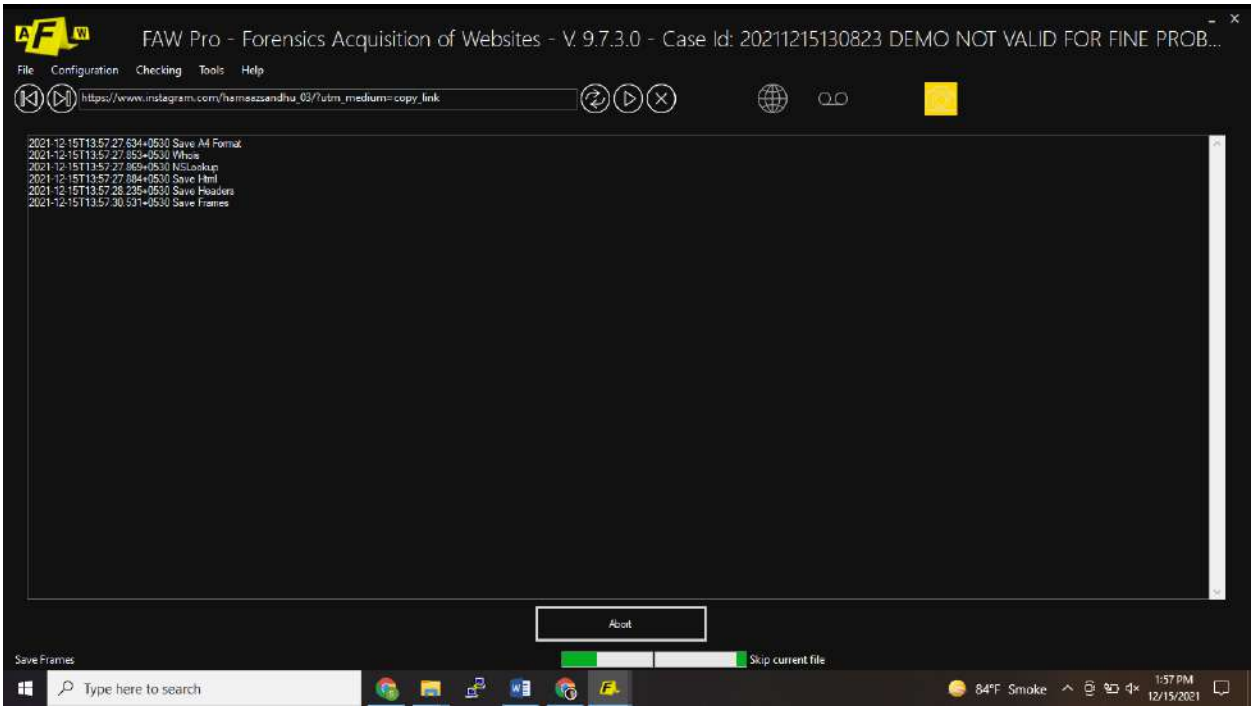
https://instagram.com/harnaazsandhu_03?utm_medium=copy_link

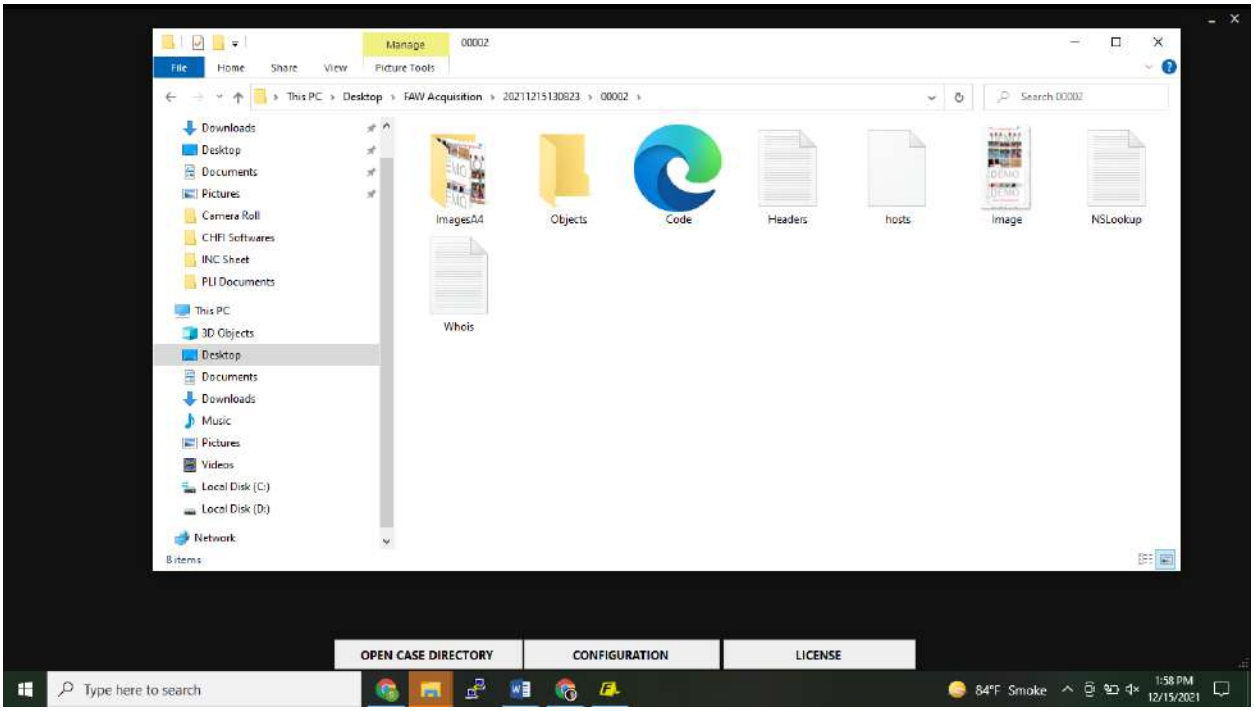
And click on F10 Acquisition.

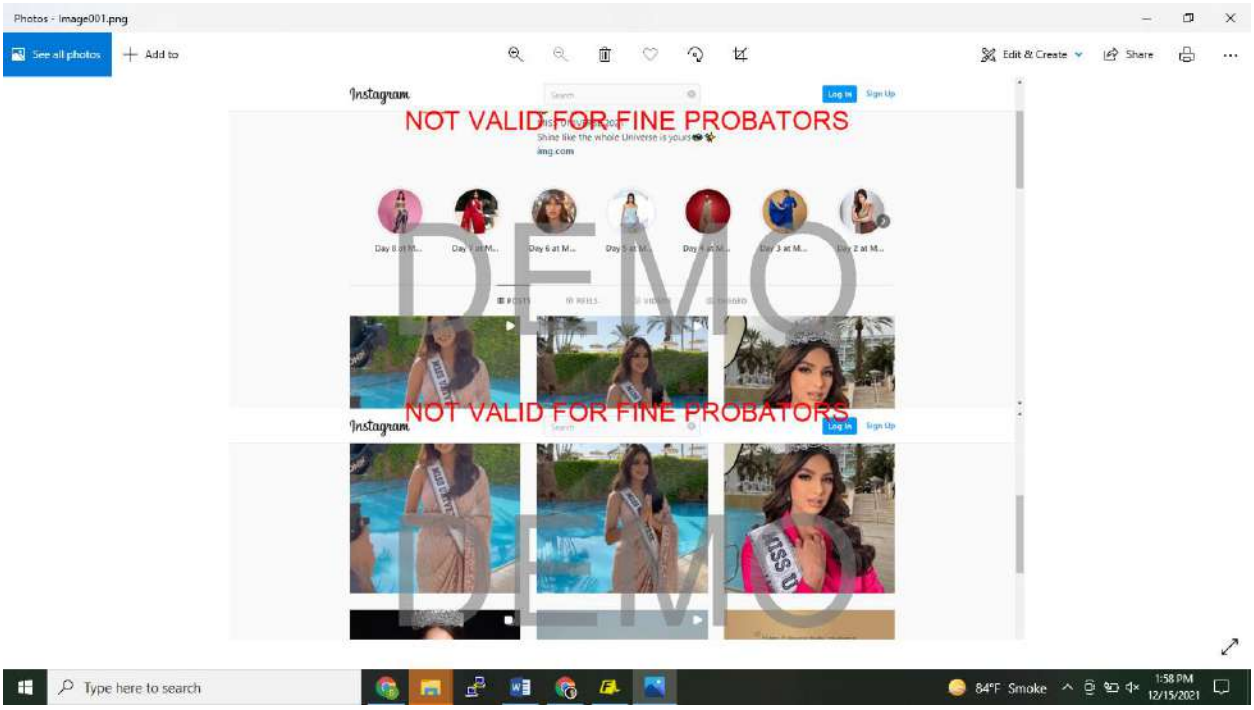
To start the acquisition you can click on Camera icon.

Acquired things you will get to see in the specified folder.


W Pro - Forensics Acquisition of Websites - V. 9.7.3.0 - Case Id: 20211215130823 DEMO NOT VALID FOR FINE PROBATORS- ...
File Configuration Checking Tools Help
https://www.instagram.com/harnaazsandhu_03/?utm_medium=copy_link
Instagram
Search
F10 - Acquisition
Log In
Sign Up
harnaazsandhu_03
Follow
383 posts
2m followers
550 following
Harnaaz Kaur Sandhu
Artist
Actor/Model
MISS UNIVERSE 2021
Shine like the whole Universe is yours
img.com
Day 8 at M...
Day 7 at M...
Day 6 at M...
Day 5 at M...
Day 4 at M...
Day 3 at M...
Day 2 at M...
Set Acquisition Mode
Type here to search
1:53 PM
12/15/2021


FAW Pro - Forensics Acquisition of Websites - V. 9.7.3.0 - Case Id: 20211215130823 DEMO NOT VALID FOR FINE PROB...
File Configuration Checking Tools Help
https://www.instagram.com/harnaazsandhu_03/?utm_medium=copy_link
2021-12-15T13:57:27.634+0530 Save A4 Format
2021-12-15T13:57:27.853+0530 Whois
2021-12-15T13:57:27.869+0530 NSLookup
2021-12-15T13:57:27.884+0530 Save Html
2021-12-15T13:57:28.235+0530 Save Headers
2021-12-15T13:57:30.531+0530 Save Frames
Abort
Save Frames
Skip current file
Type here to search
84°F Smoke
1:57 PM
12/15/2021





Practical No. 13

Aim: Forensic Investigation Using Mobile Forensics Tools [Mobiledit]

What is Forensic Investigation?

Forensics are the scientific methods used to solve a crime. Forensic investigation is the gathering and analysis of all crime-related physical evidence in order to come to a conclusion about a suspect. Investigators will look at blood, fluid, or fingerprints, residue, hard drives, computers, or other technology to establish how a crime took place. This is a general definition, though, since there are a number of different types of forensics.

What is Mobile Forensics Tools [Mobiledit]:

Complete data extraction from phones and SIM

With MOBILedit Forensic you can view, search for or retrieve all data from a phone with only a few clicks. This data includes call history, phonebook, text messages, multimedia messages, files, calendars, notes, reminders and raw application data. It will also retrieve all phone information such as IMEI, operating systems, firmware including SIM details (IMSI), ICCID and location area information. MOBILedit Forensic is also able to bypass the passcode, PIN and phone backup encryption.

Support for almost all phones

MOBILedit Forensic supports thousands of different phones including common feature phones from manufacturers like Samsung, HTC, Nokia, Sony, LG and Motorola. It also supports all smartphone operating systems including Android, iPhone, Blackberry, Symbian, Windows Mobile, Windows Phone, Bada, Meego, Chinese phones and CDMA phones.

MOBILedit used for:

1) Data Acquisition
2) Retrieval of Data
3) Recovering of Data

What is Data Acquisition?

It is a process where we acquire all the data from the cell phones which can be messages, videos, images, contacts, call logs and all other info.

MOBILedit is a tool used to acquire and recover data in mobile phones.

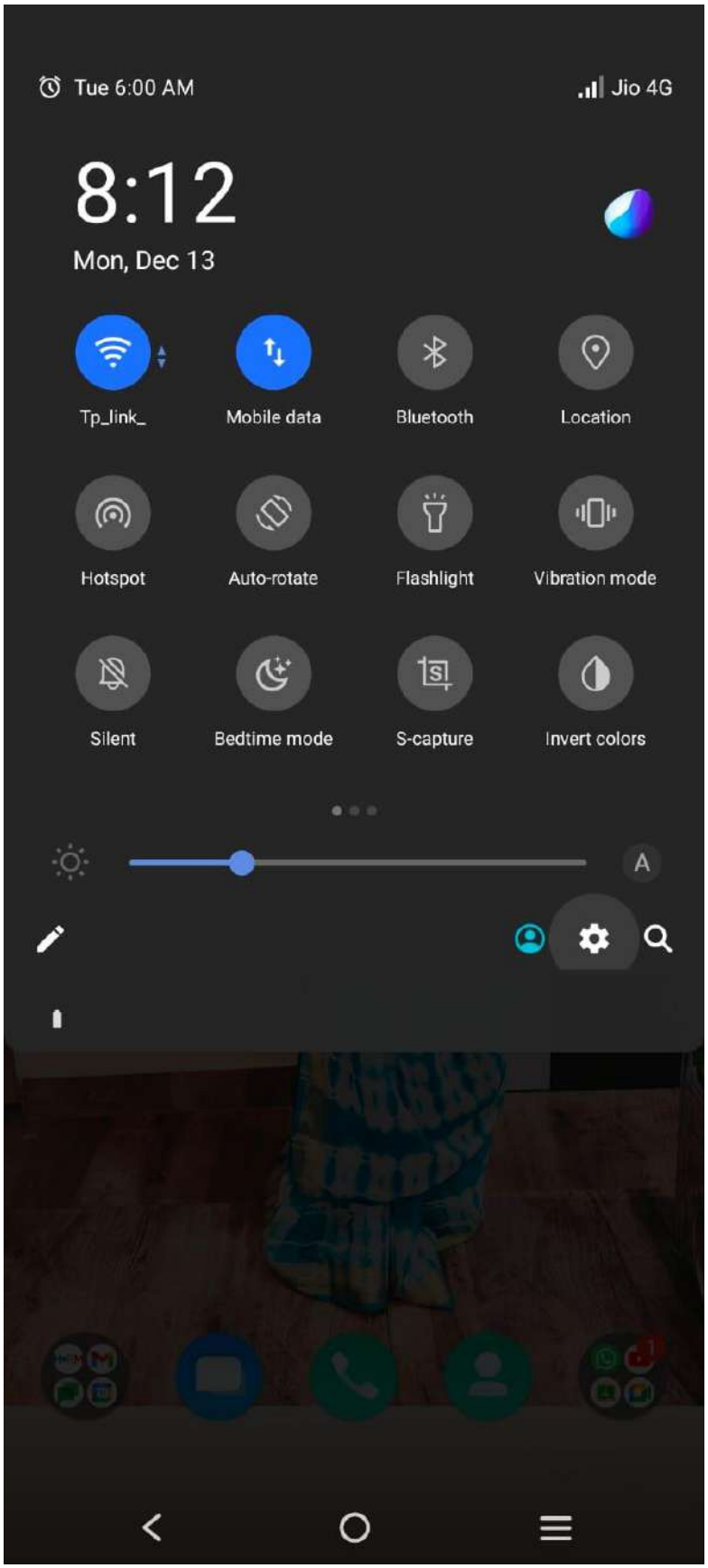
It is specially designed for mobile phone forensics.

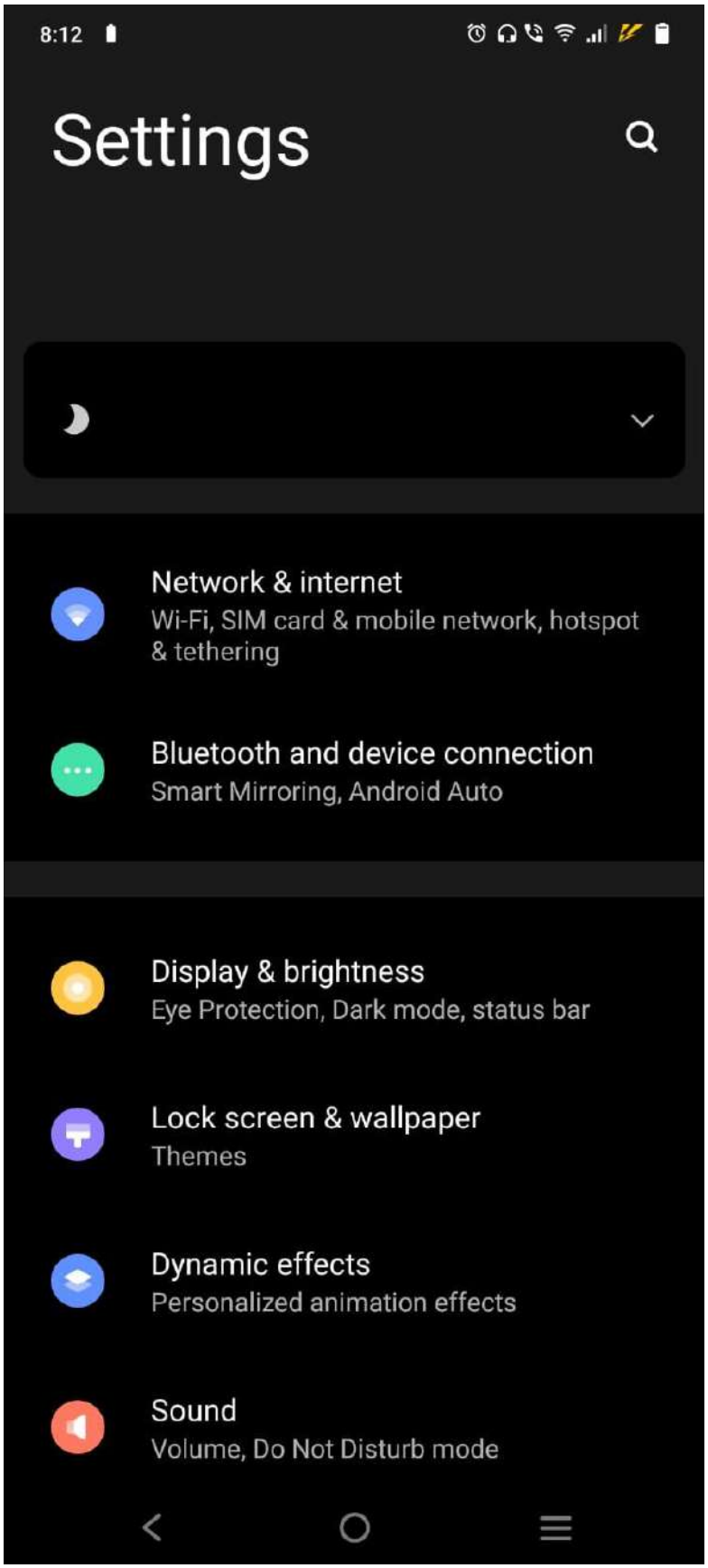
Steps:

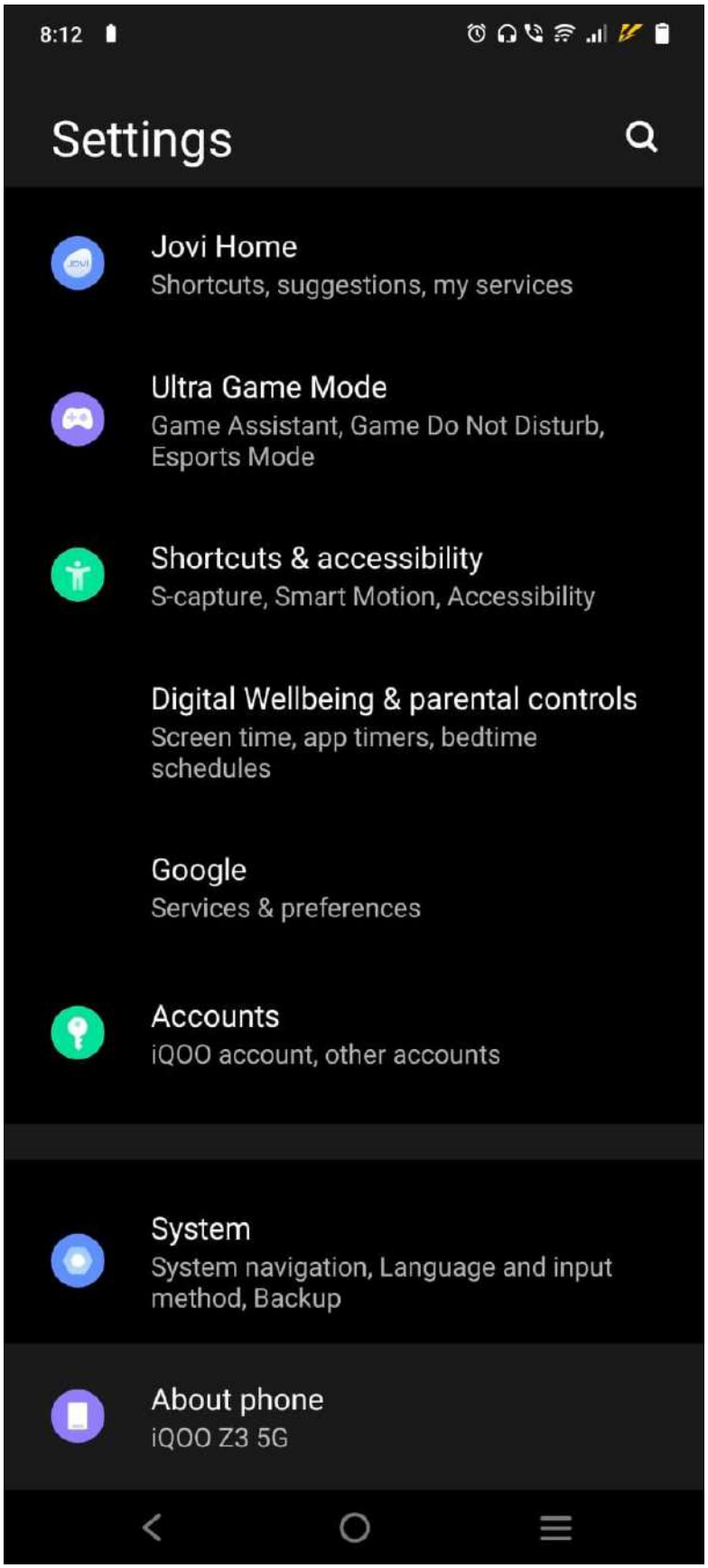
1) **How to enable developer option in any Android phone and Turn the USB debugging on.**

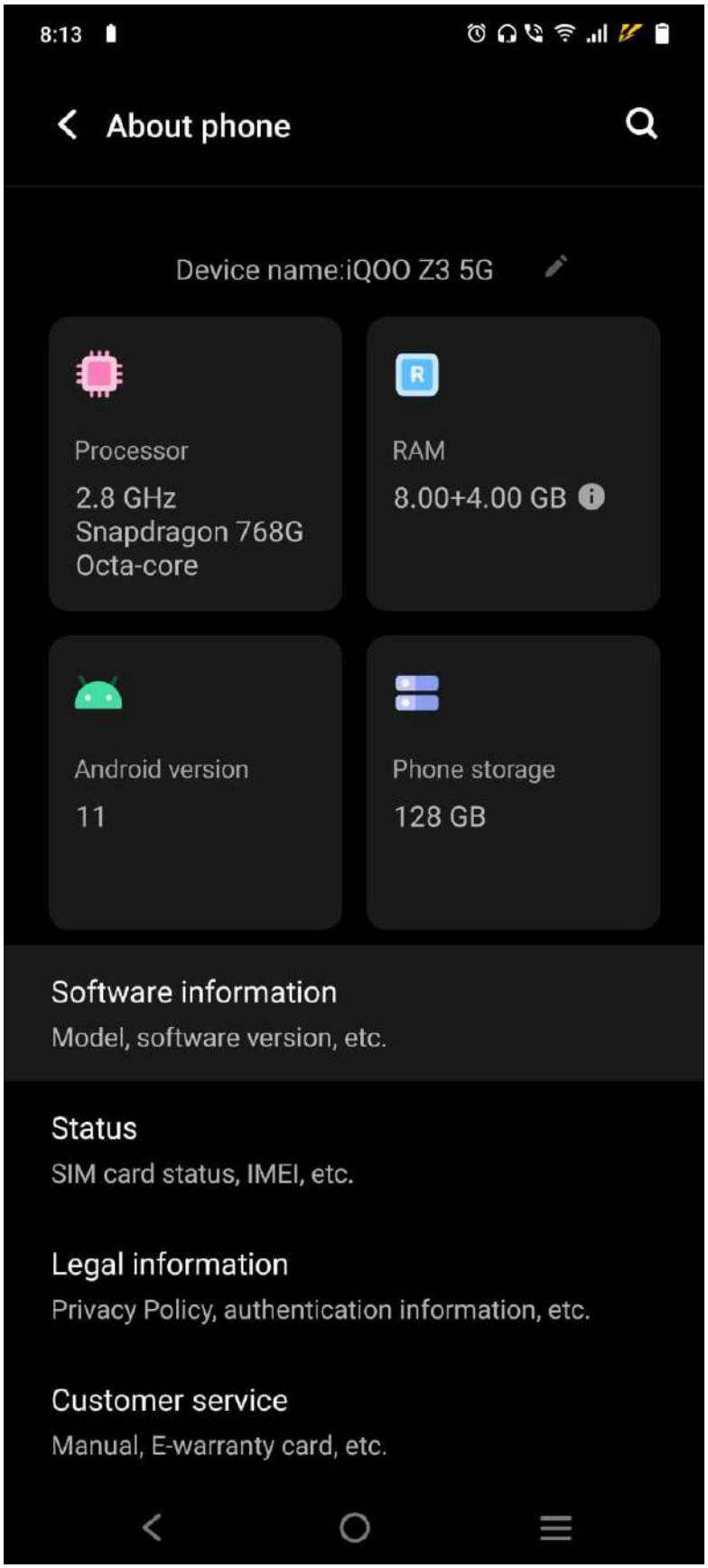
Go to Settings - About Phone – Software Information – Then tap 7 times on, Build Number.

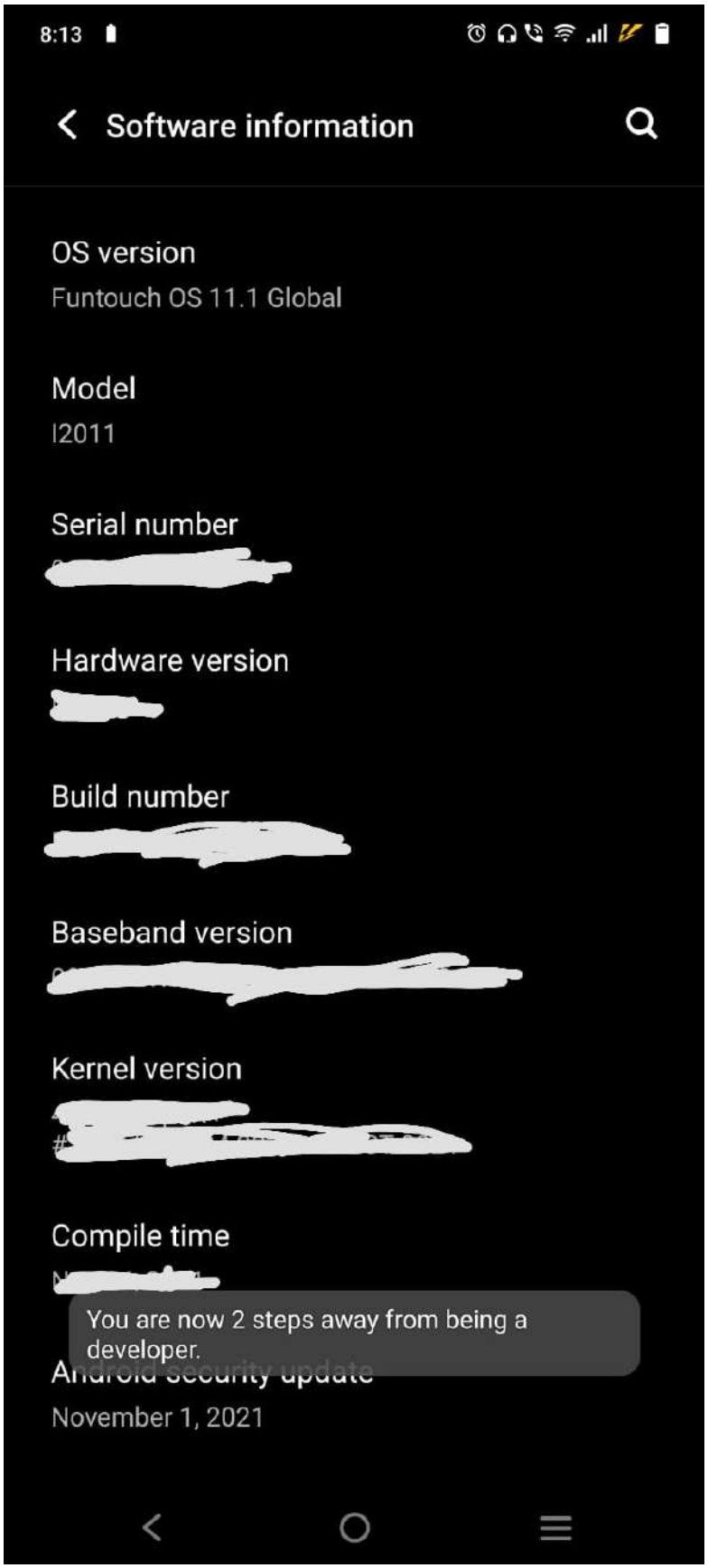
Then go to Settings – System – Developer Options – USB debugging – Turn the USB debugging on.

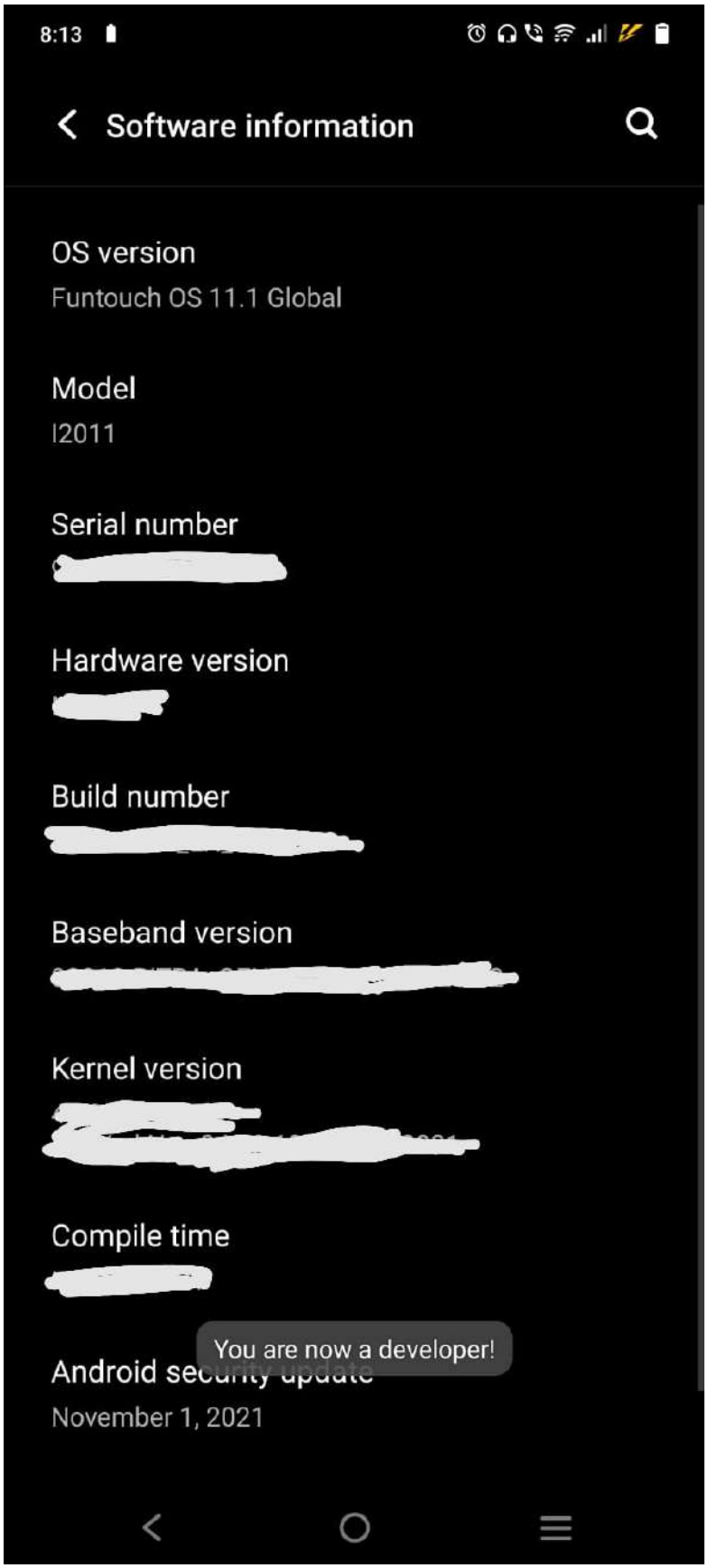

Tue 6:00 AM
Jio 4G
8:12
Mon, Dec 13
Tp_link_
Mobile data
Bluetooth
Location
Hotspot
Auto-rotate
Flashlight
Vibration mode
Silent
Bedtime mode
S-capture
Invert colors
A

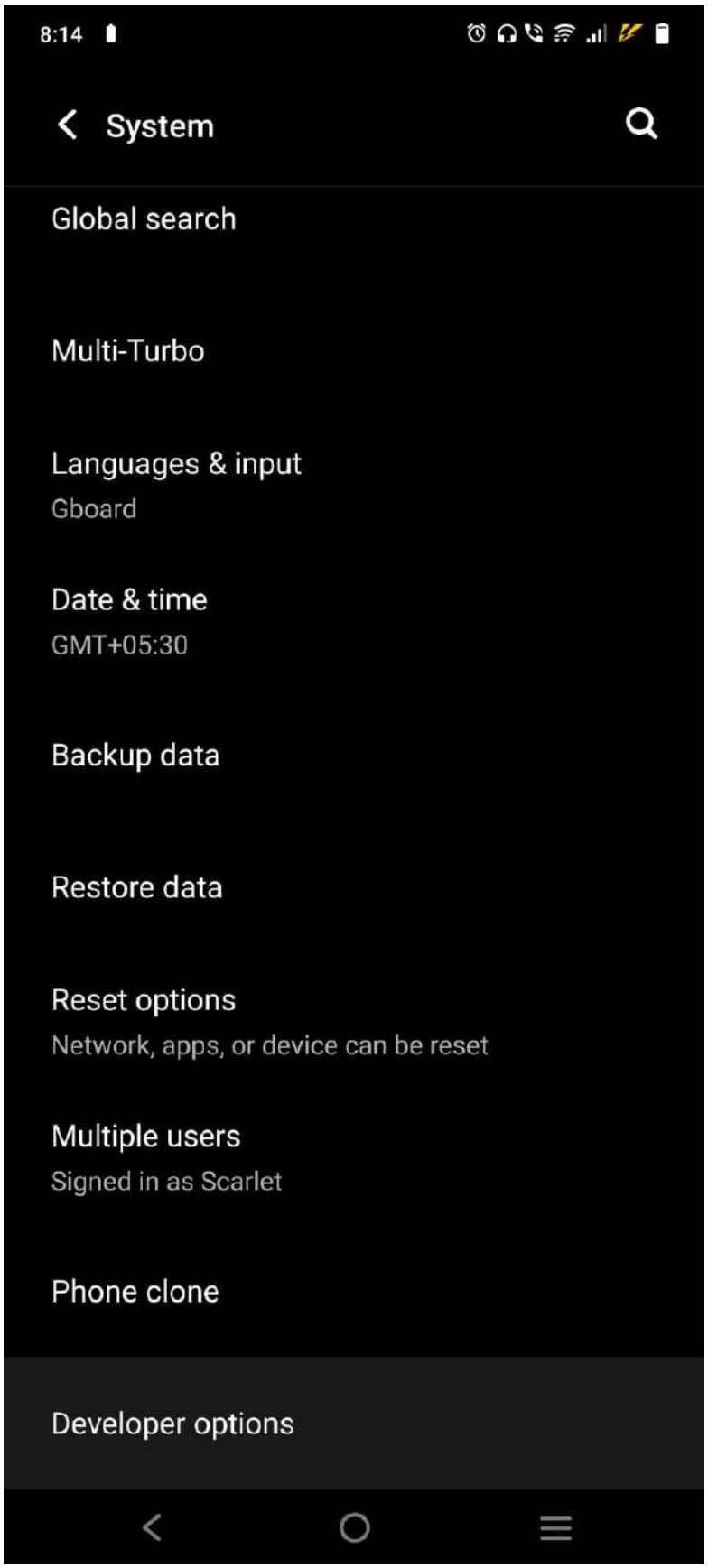

8:12
Settings
Network & internet
Wi-Fi, SIM card & mobile network, hotspot & tethering
Bluetooth and device connection
Smart Mirroring, Android Auto
Display & brightness
Eye Protection, Dark mode, status bar
Lock screen & wallpaper
Themes
Dynamic effects
Personalized animation effects
Sound
Volume, Do Not Disturb mode

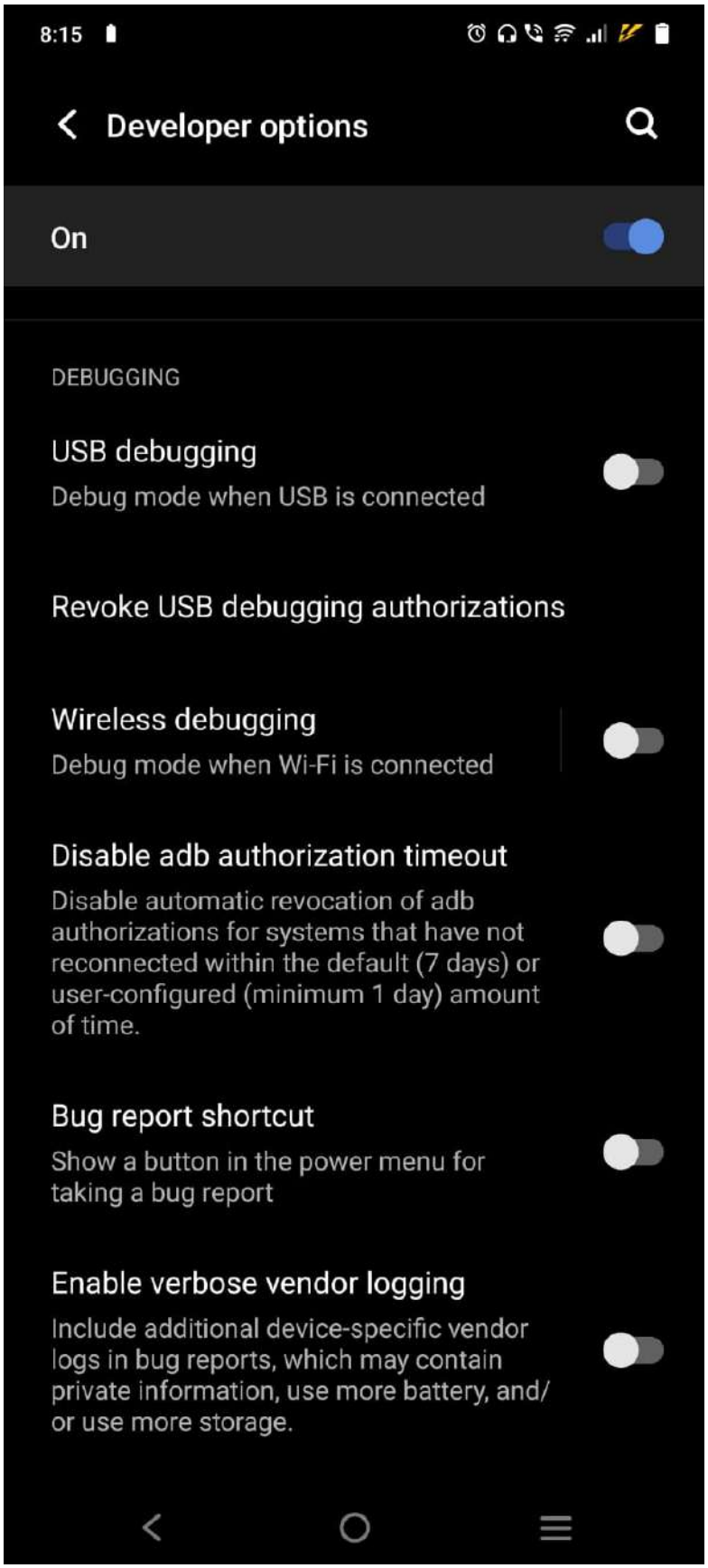

8:12
Settings
Jovi Home
Shortcuts, suggestions, my services
Ultra Game Mode
Game Assistant, Game Do Not Disturb, Esports Mode
Shortcuts & accessibility
S-capture, Smart Motion, Accessibility
Digital Wellbeing & parental controls
Screen time, app timers, bedtime schedules
Google
Services & preferences
Accounts
iQOO account, other accounts
System
System navigation, Language and input method, Backup
About phone
iQOO Z3 5G

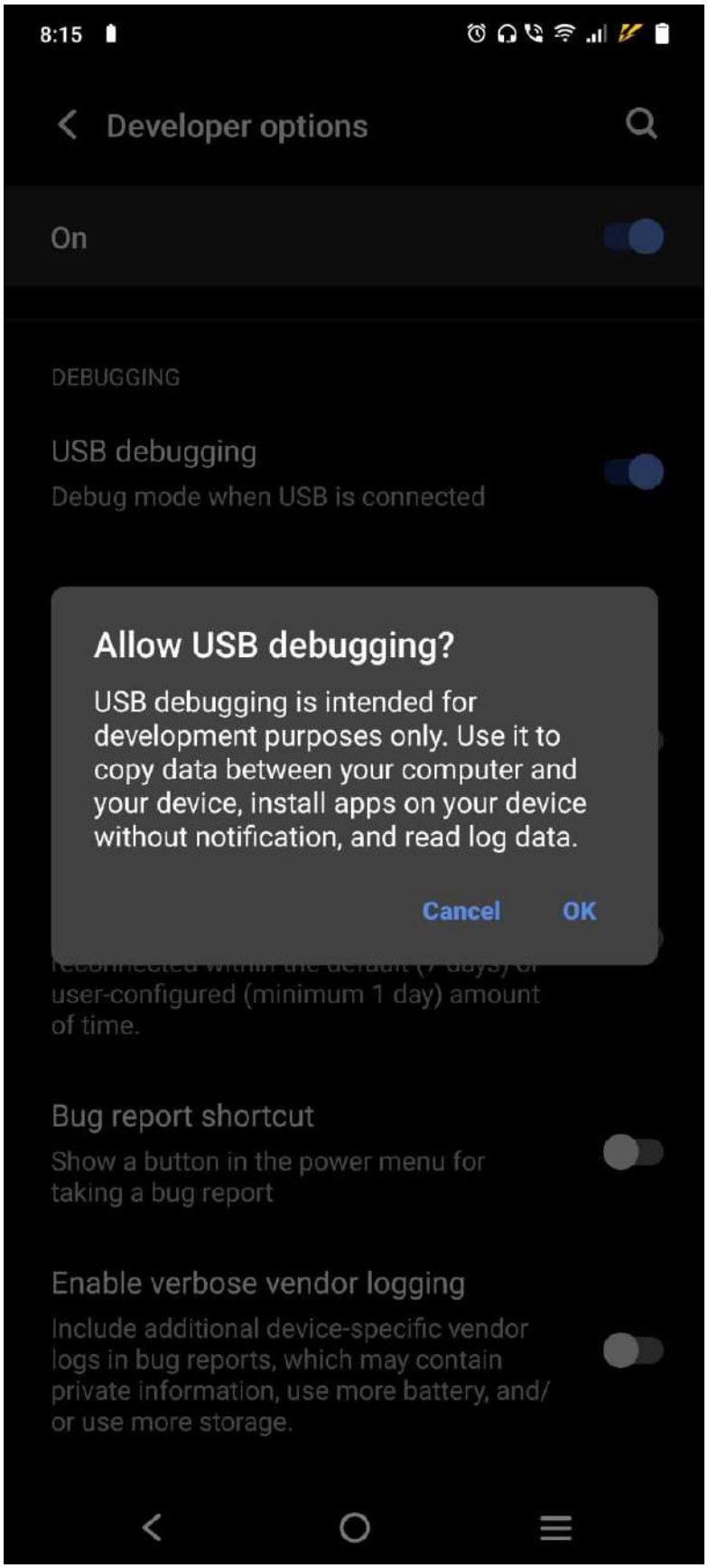

8:13
About phone
Device name:iQOO Z3 5G
Processor
2.8 GHz
Snapdragon 768G
Octa-core
RAM
8.00+4.00 GB
Android version
11
Phone storage
128 GB
Software information
Model, software version, etc.
Status
SIM card status, IMEI, etc.
Legal information
Privacy Policy, authentication information, etc.
Customer service
Manual, E-warranty card, etc.

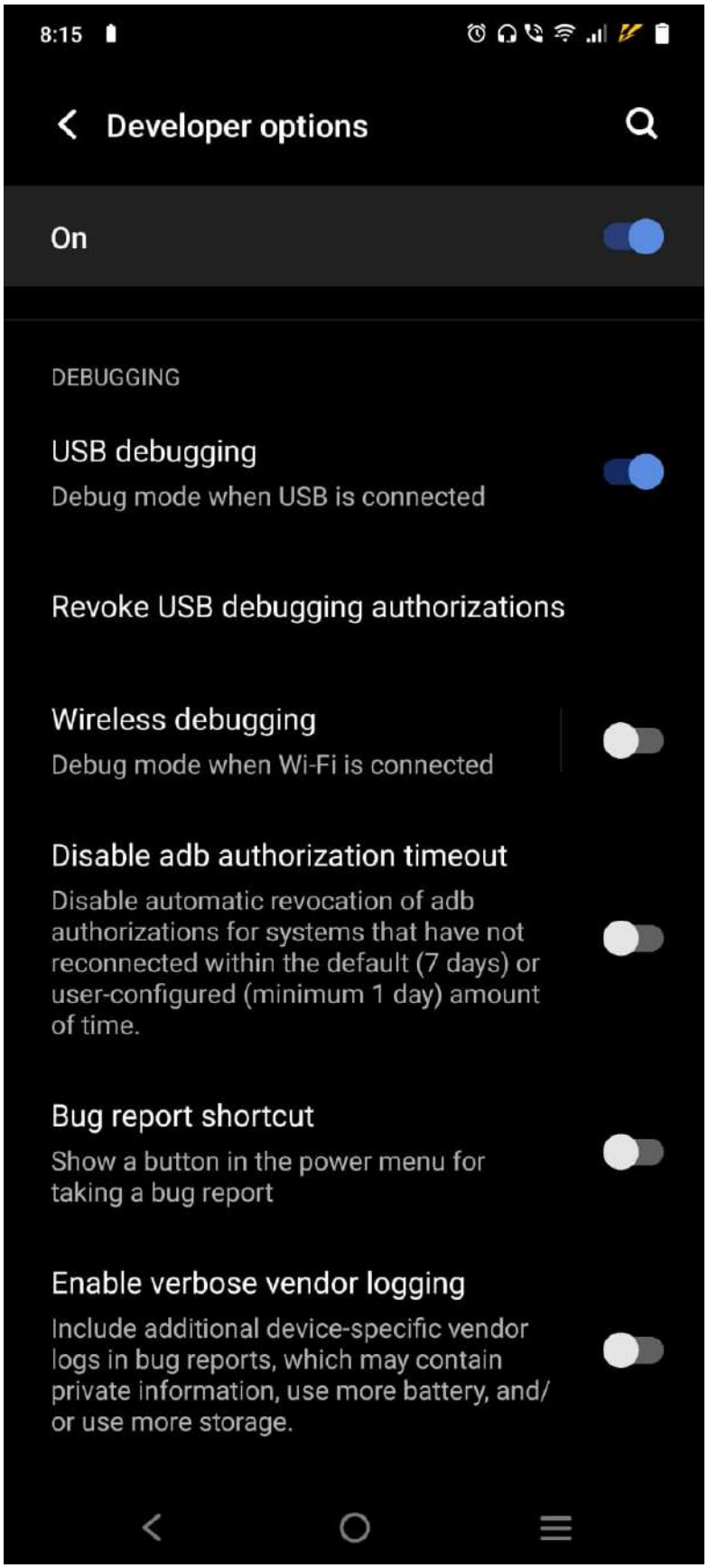

8:13
Software information
OS version
Funtouch OS 11.1 Global
Model
I2011
Serial number
Hardware version
Build number
Baseband version
Kernel version
Compile time
You are now 2 steps away from being a developer.
November 1, 2021


8:13
Software information
OS version
Funtouch OS 11.1 Global
Model
I2011
Serial number
Hardware version
Build number
Baseband version
Kernel version
Compile time
You are now a developer!
Android security update
November 1, 2021

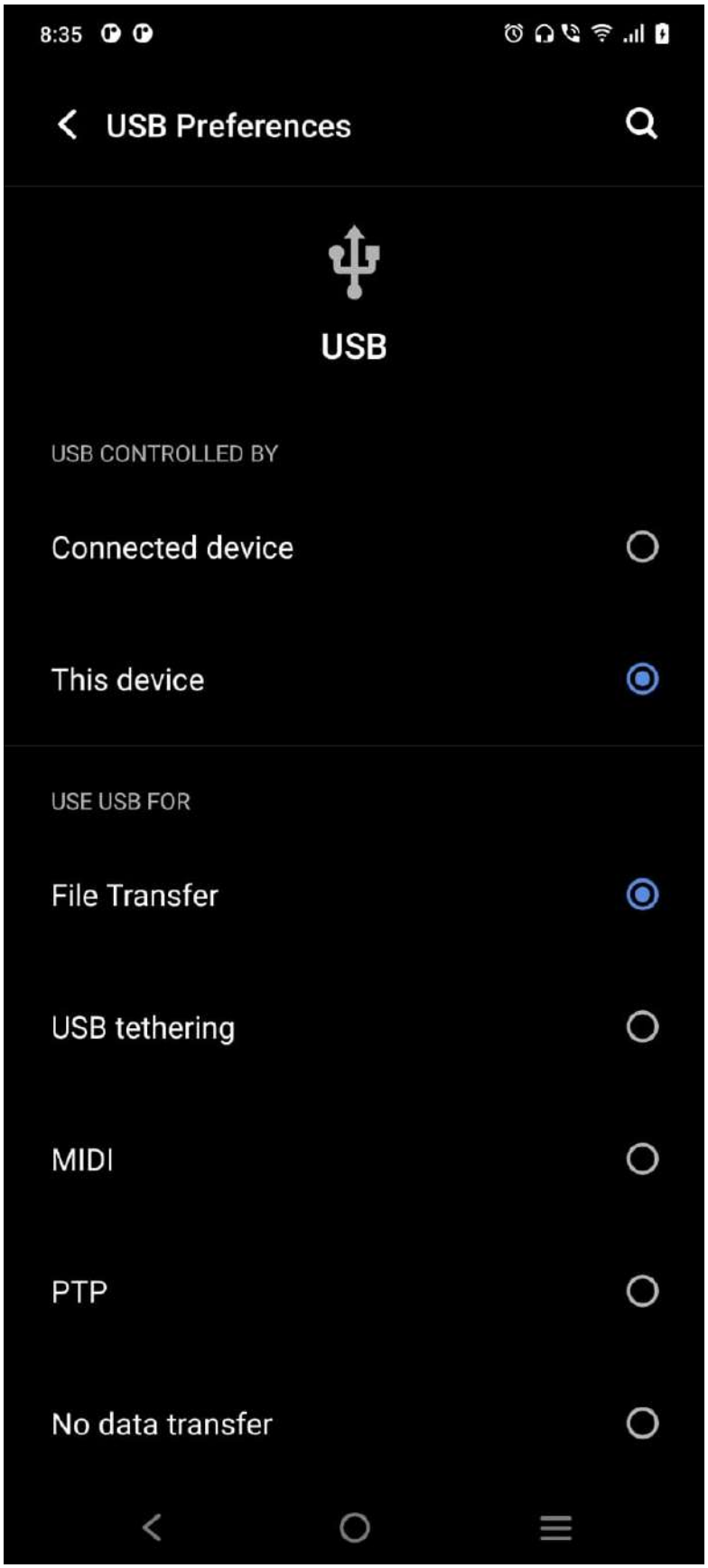

8:14
System
Global search
Multi-Turbo
Languages & input
Gboard
Date & time
GMT+05:30
Backup data
Restore data
Reset options
Network, apps, or device can be reset
Multiple users
Signed in as Scarlet
Phone clone
Developer options


8:15
Developer options
On
DEBUGGING
USB debugging
Debug mode when USB is connected
Revoke USB debugging authorizations
Wireless debugging
Debug mode when Wi-Fi is connected
Disable adb authorization timeout
Disable automatic revocation of adb authorizations for systems that have not reconnected within the default (7 days) or user-configured (minimum 1 day) amount of time.
Bug report shortcut
Show a button in the power menu for taking a bug report
Enable verbose vendor logging
Include additional device-specific vendor logs in bug reports, which may contain private information, use more battery, and/or use more storage.

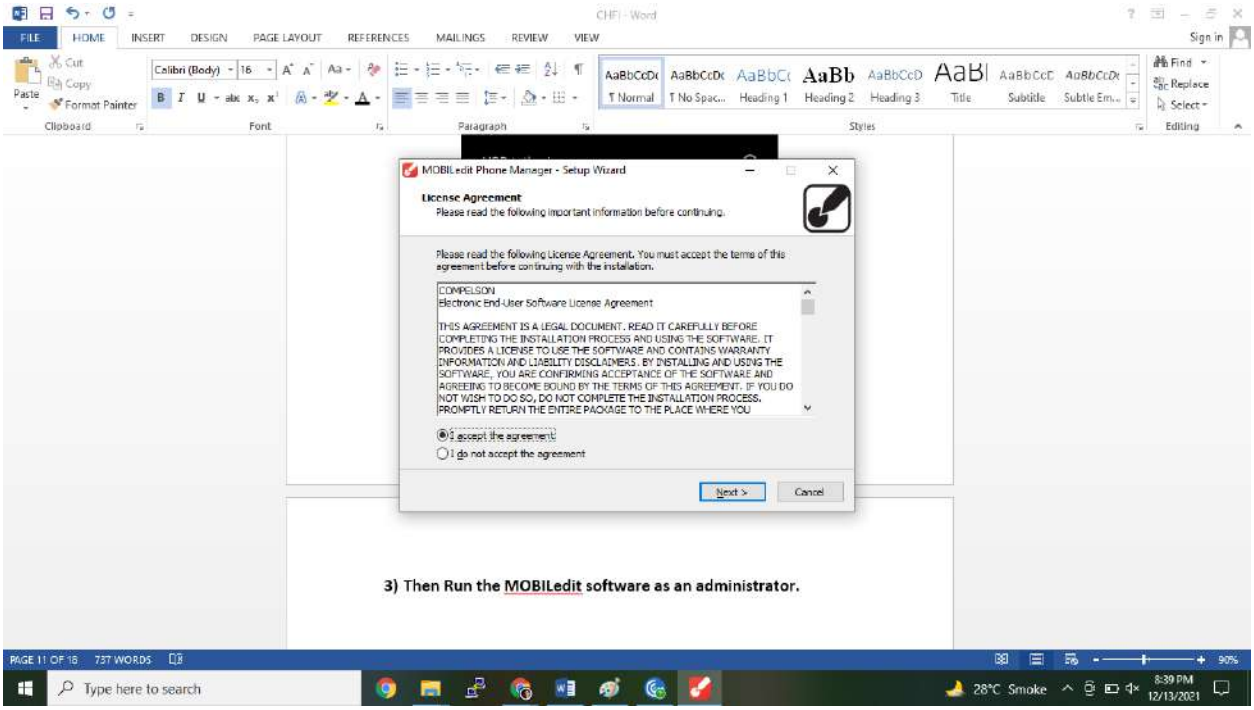

8:15
Developer options
On
DEBUGGING
USB debugging
Debug mode when USB is connected
Allow USB debugging?
USB debugging is intended for development purposes only. Use it to copy data between your computer and your device, install apps on your device without notification, and read log data.
Cancel
OK
user-configured (minimum 1 day) amount of time.
Bug report shortcut
Show a button in the power menu for taking a bug report
Enable verbose vendor logging
Include additional device-specific vendor logs in bug reports, which may contain private information, use more battery, and/or use more storage.

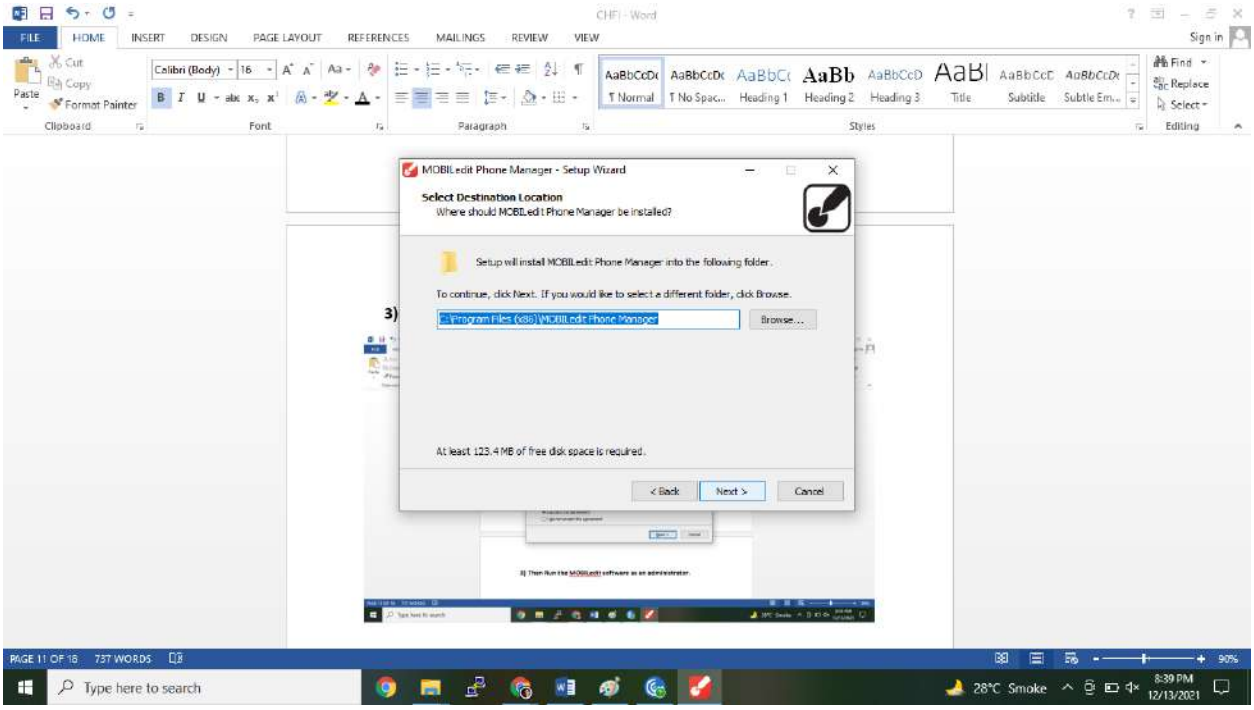

8:15
Developer options
On
DEBUGGING
USB debugging
Debug mode when USB is connected
Revoke USB debugging authorizations
Wireless debugging
Debug mode when Wi-Fi is connected
Disable adb authorization timeout
Disable automatic revocation of adb authorizations for systems that have not reconnected within the default (7 days) or user-configured (minimum 1 day) amount of time.
Bug report shortcut
Show a button in the power menu for taking a bug report
Enable verbose vendor logging
Include additional device-specific vendor logs in bug reports, which may contain private information, use more battery, and/or use more storage.

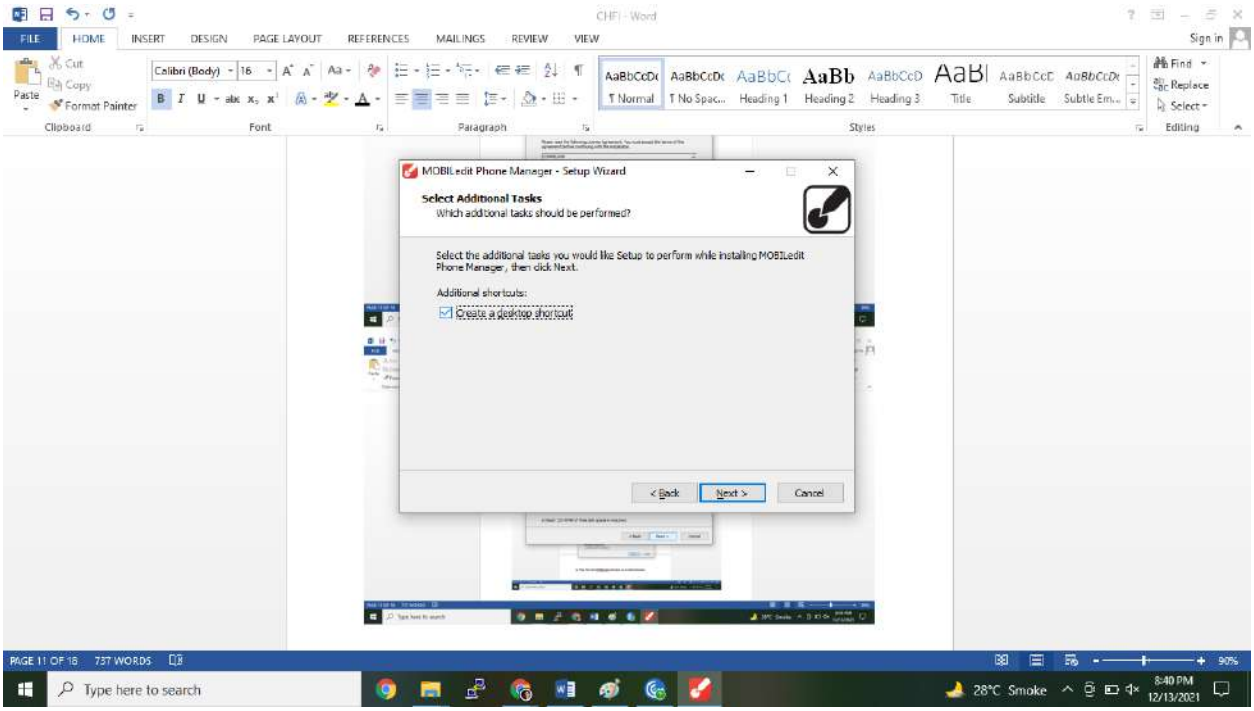
2) **Connect your phone with USB Cable with your computer or laptop. After that one popup will appear on your phone, Select File transfer from USB Preferences.**

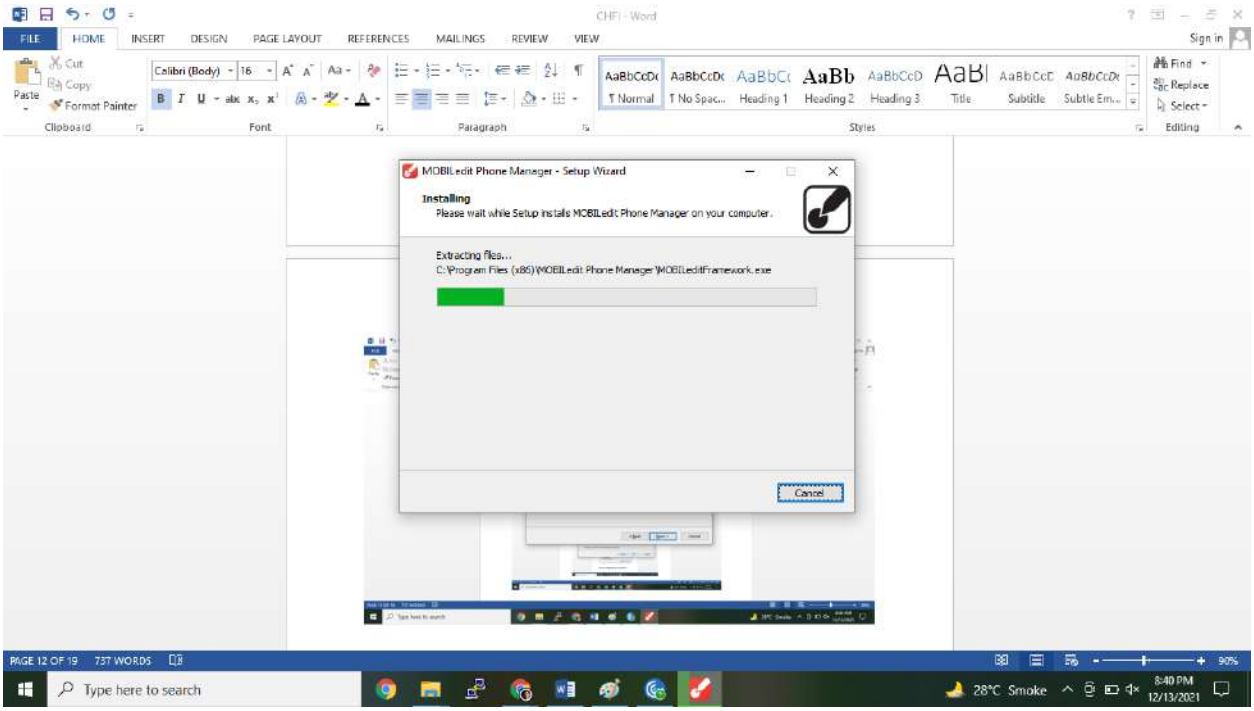

8:35
USB Preferences
USB
USB CONTROLLED BY
Connected device
This device
USE USB FOR
File Transfer
USB tethering
MIDI
PTP
No data transfer

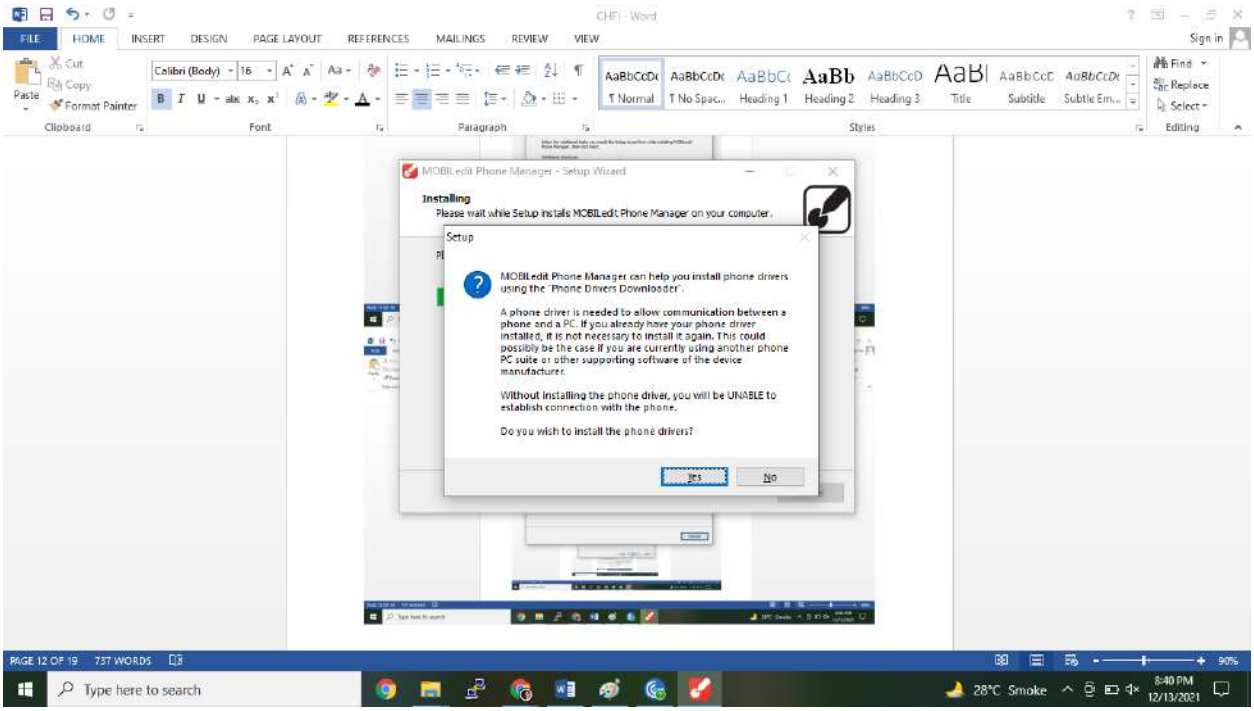
3) Then Run the MOBILedit software as an administrator.



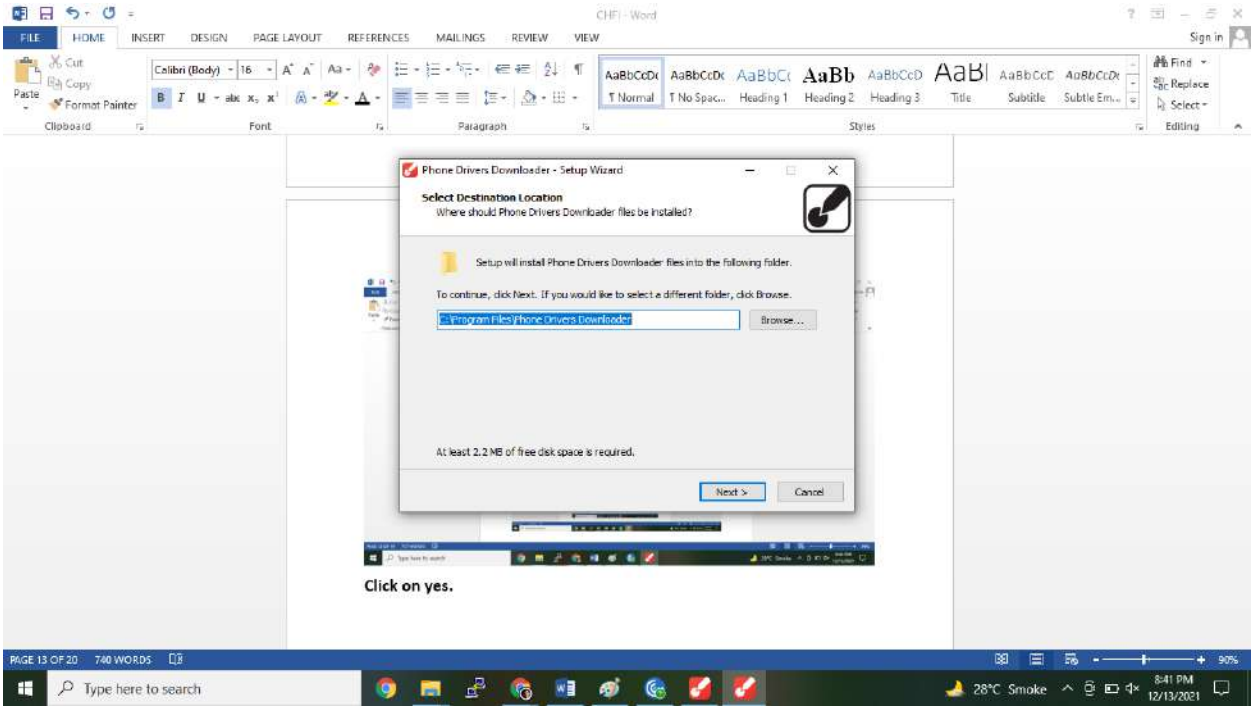



MOBILedit Phone Manager - Setup Wizard
Select Additional Tasks
Which additional tasks should be performed?
Select the additional tasks you would like Setup to perform while installing MOBILedit Phone Manager, then click Next.
Additional shortcuts:
Create a desktop shortcut
< Back
Next >
Cancel
PAGE 11 OF 18
737 WORDS
Type here to search
28°C Smoke
8:40 PM
12/13/2021

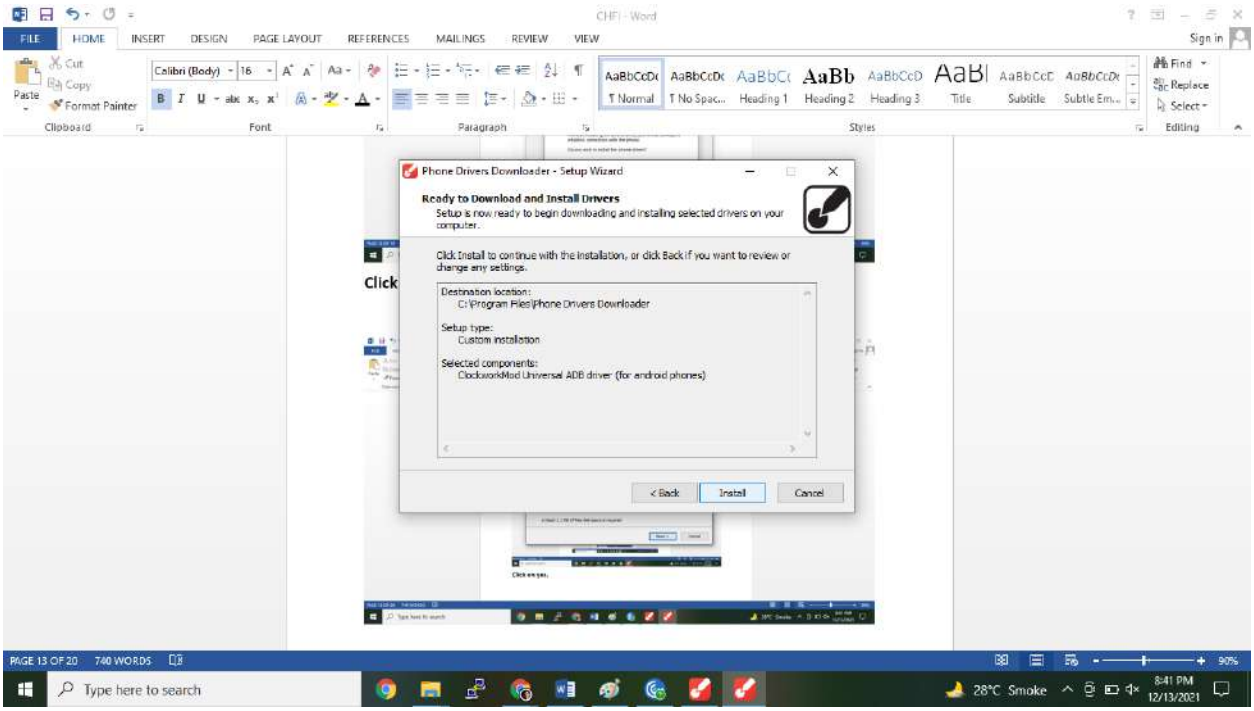

MOBILedit Phone Manager - Setup Wizard
Installing
Please wait while Setup installs MOBILedit Phone Manager on your computer.
Extracting files...
C:\Program Files (x86)\MOBILedit Phone Manager\MOBILeditFramework.exe
Cancel
PAGE 12 OF 19
737 WORDS
Type here to search
28°C Smoke
8:40 PM
12/13/2021

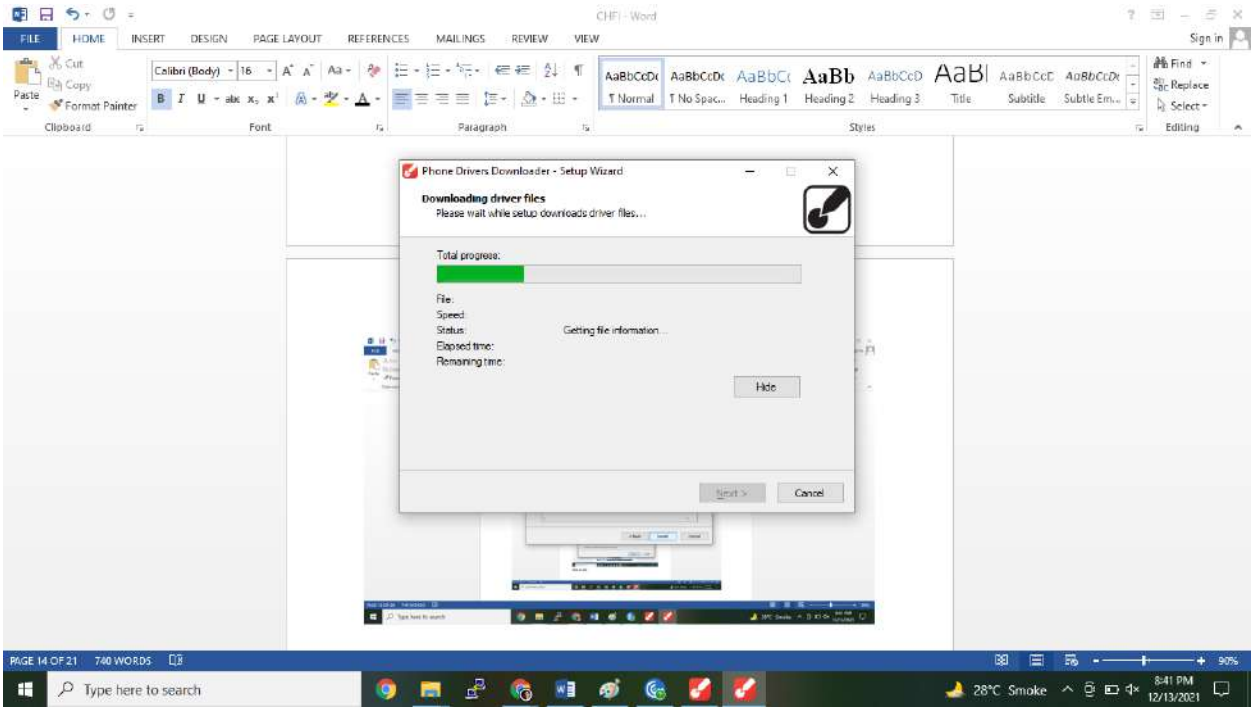


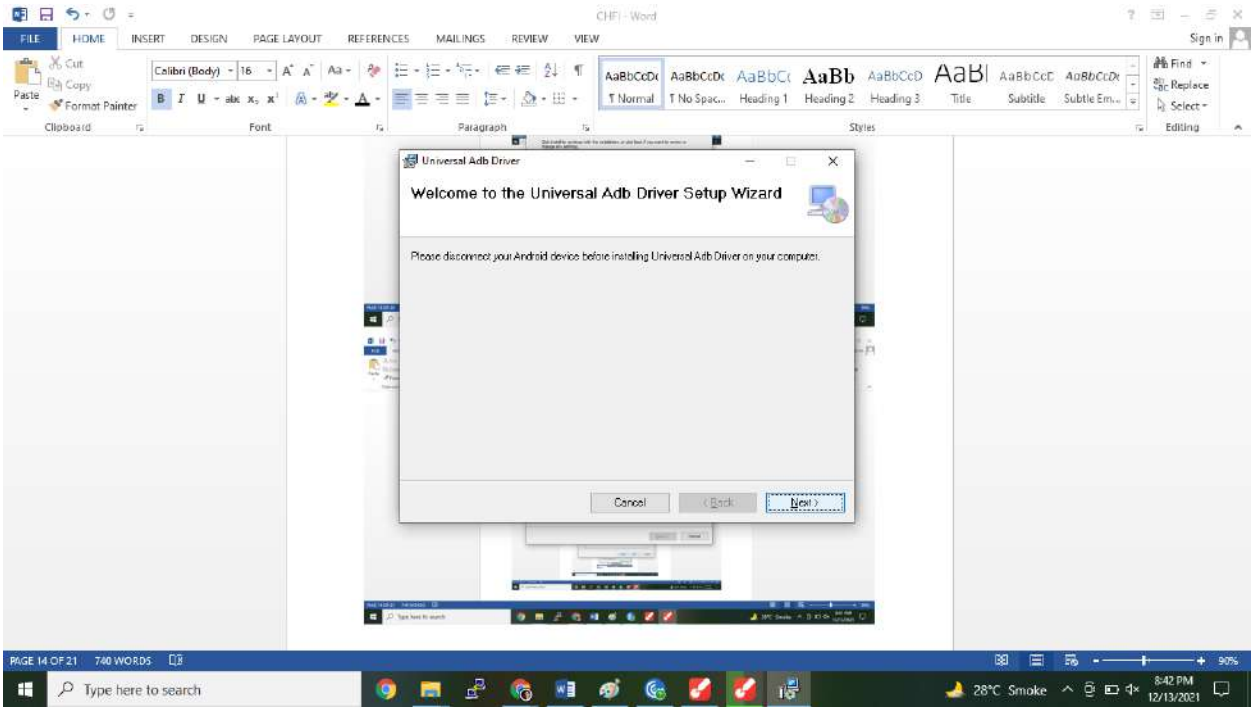
Click on yes.

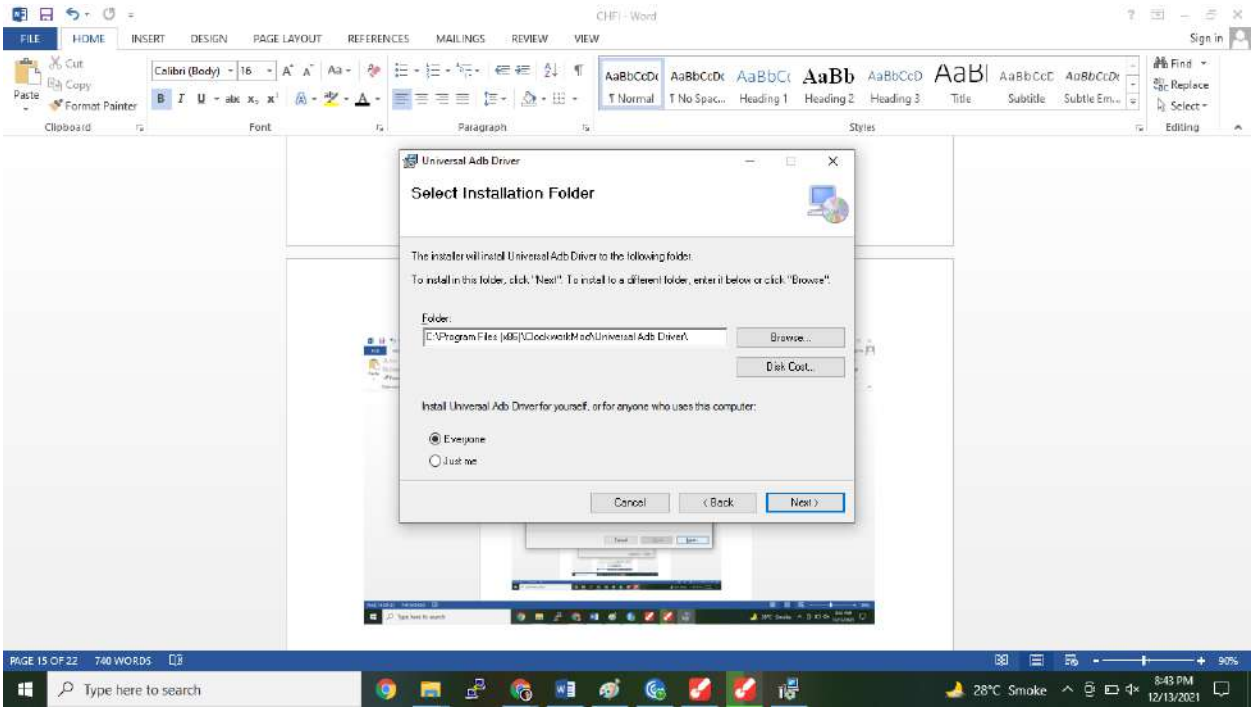


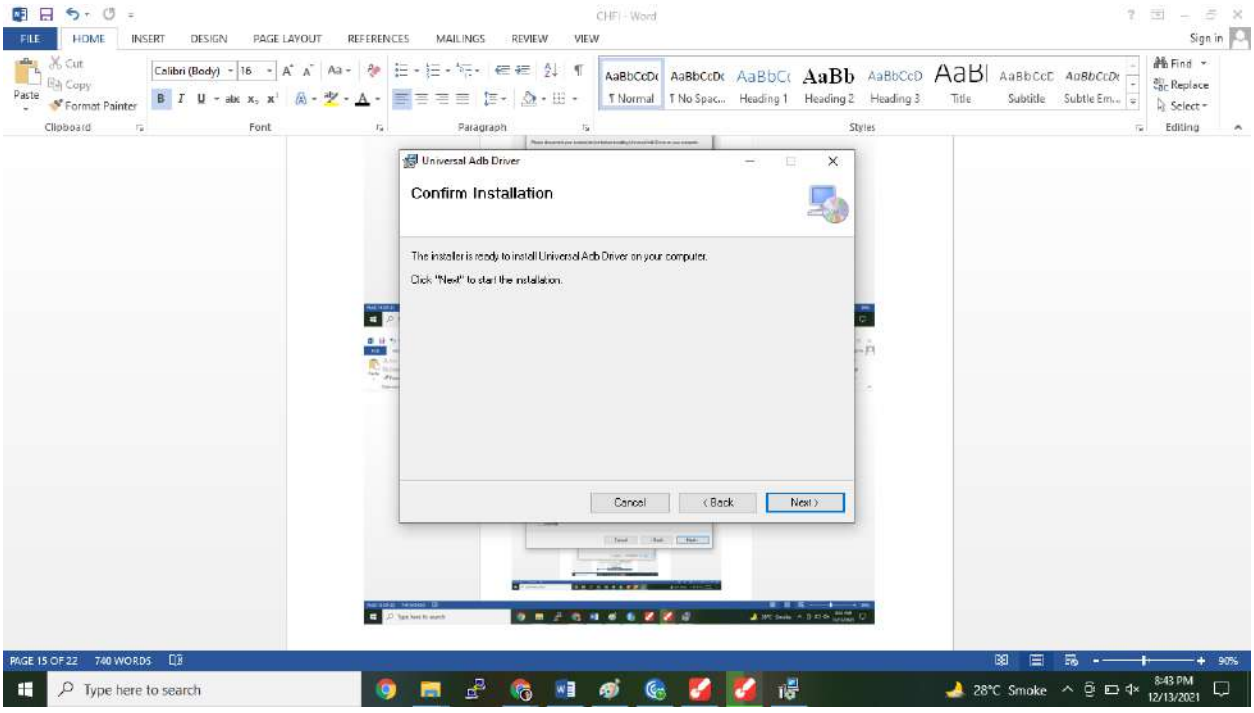
Click on yes.

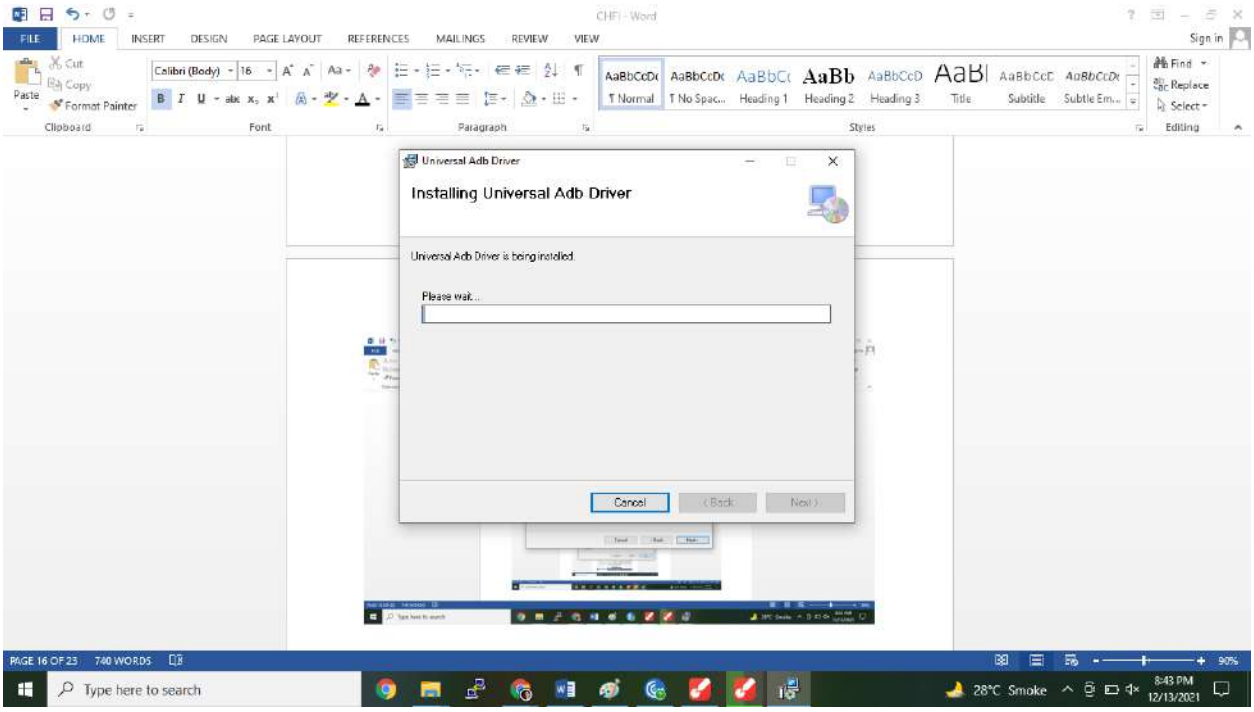

Phone Drivers Downloader - Setup Wizard
Ready to Download and Install Drivers
Setup is now ready to begin downloading and installing selected drivers on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files\Phone Drivers Downloader
Setup type:
Custom installation
Selected components:
ClockworkMod Universal ADB driver (for android phones)
< Back
Install
Cancel

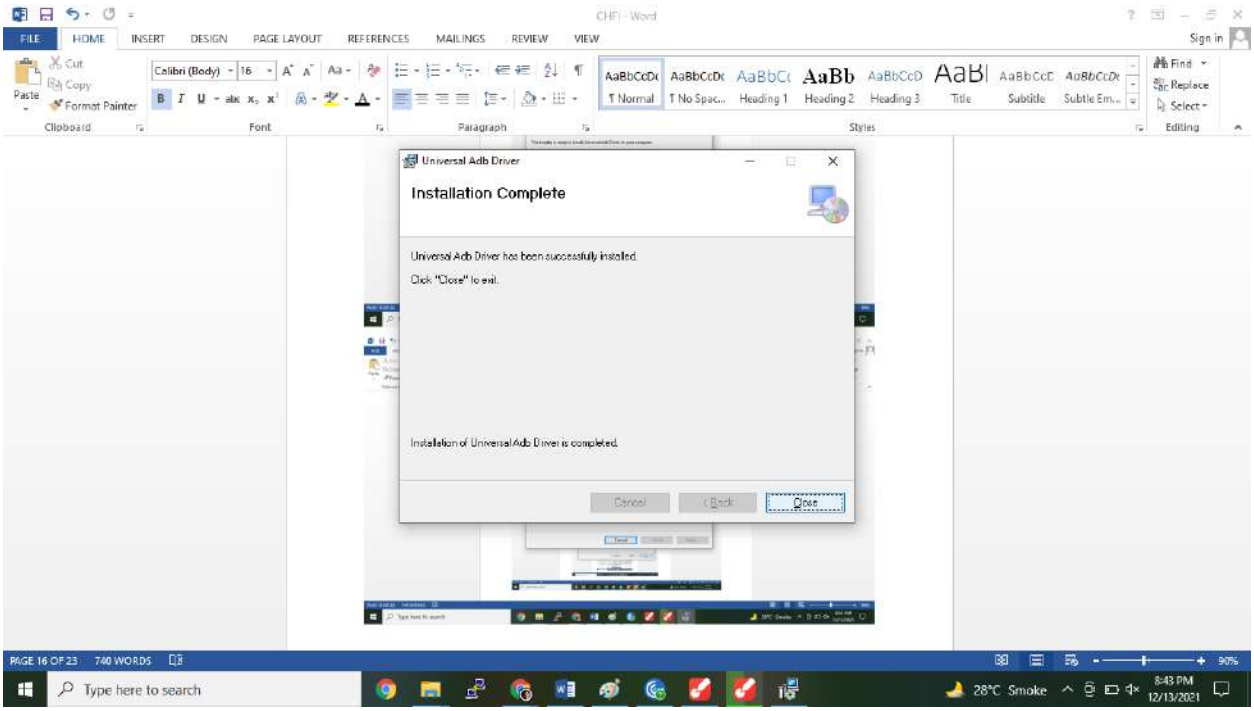

Phone Drivers Downloader - Setup Wizard
Downloading driver files
Please wait while setup downloads driver files...
Total progress:
File:
Speed:
Status:
Getting file information...
Elapsed time:
Remaining time:
Hide
Next >
Cancel

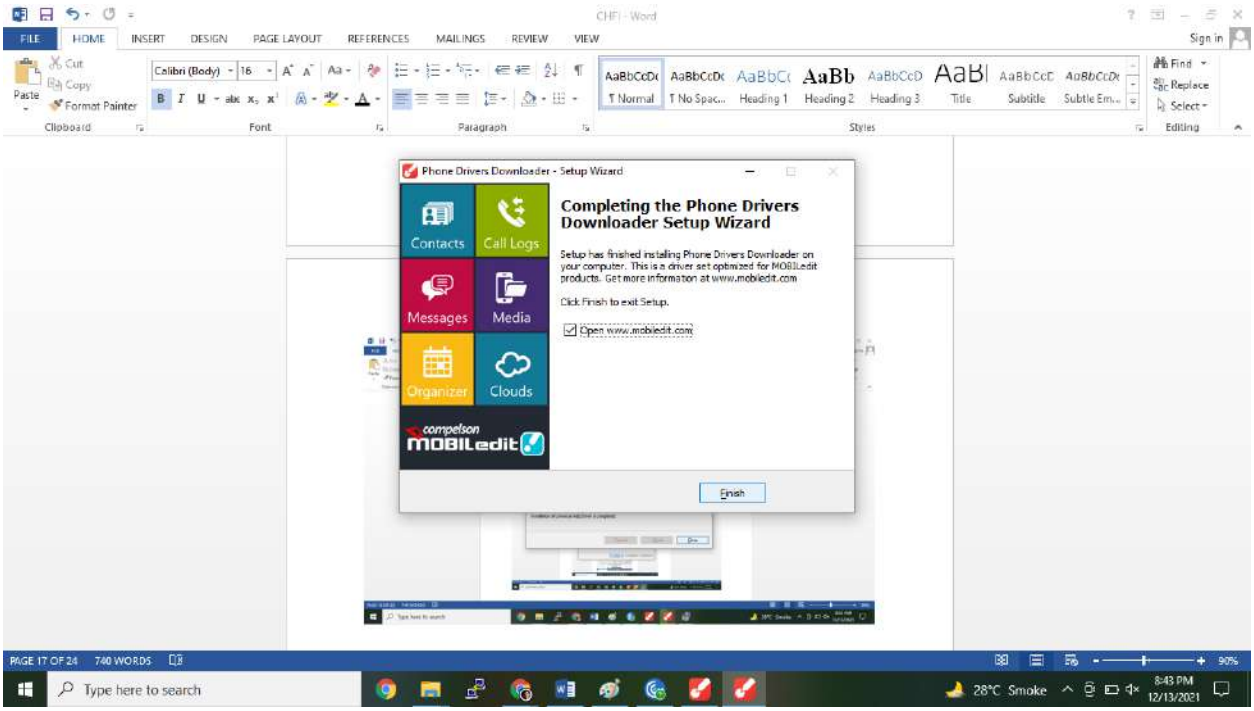

Universal Adb Driver
Welcome to the Universal Adb Driver Setup Wizard
Please disconnect your Android device before installing Universal Adb Driver on your computer.
Cancel
< Back
Next >
PAGE 14 OF 21
740 WORDS
Type here to search
28°C Smoke
8:42 PM
12/13/2021


Universal Adb Driver
Select Installation Folder
The installer will install Universal Adb Driver to the following folder.
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".
Folder:
C:\Program Files (x86)\ClockworkMod\Universal Adb Driver\
Browse...
Disk Cost...
Install Universal Adb Driver for yourself, or for anyone who uses this computer:
Everyone
Just me
Cancel
< Back
Next >
PAGE 15 OF 22
740 WORDS
Type here to search
28°C Smoke
8:43 PM
12/13/2021


Universal Adb Driver
Confirm Installation
The installer is ready to install Universal Adb Driver on your computer.
Click "Next" to start the installation.
Cancel
< Back
Next >
PAGE 15 OF 22
740 WORDS
Type here to search
28°C Smoke
8:43 PM
12/13/2021

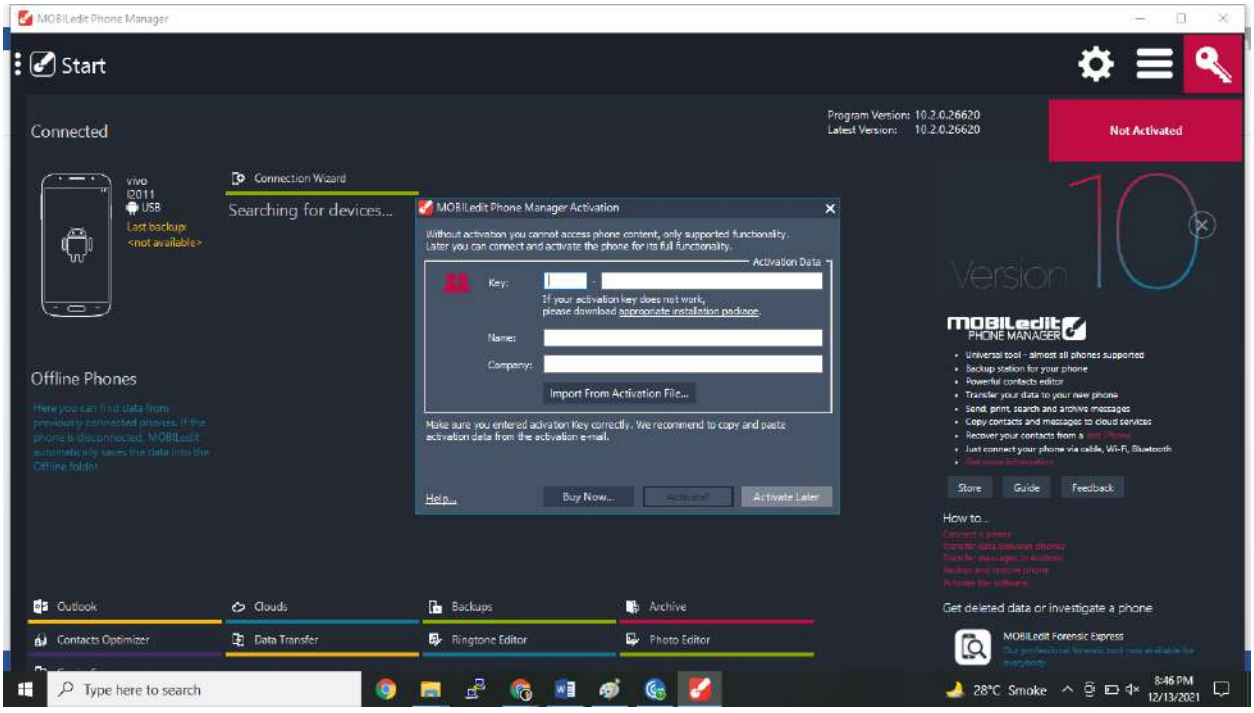

Universal Adb Driver
Installing Universal Adb Driver
Universal Adb Driver is being installed.
Please wait...
Cancel
< Back
Next >
PAGE 16 OF 23
740 WORDS
Type here to search
28°C Smoke
8:43 PM
12/13/2021

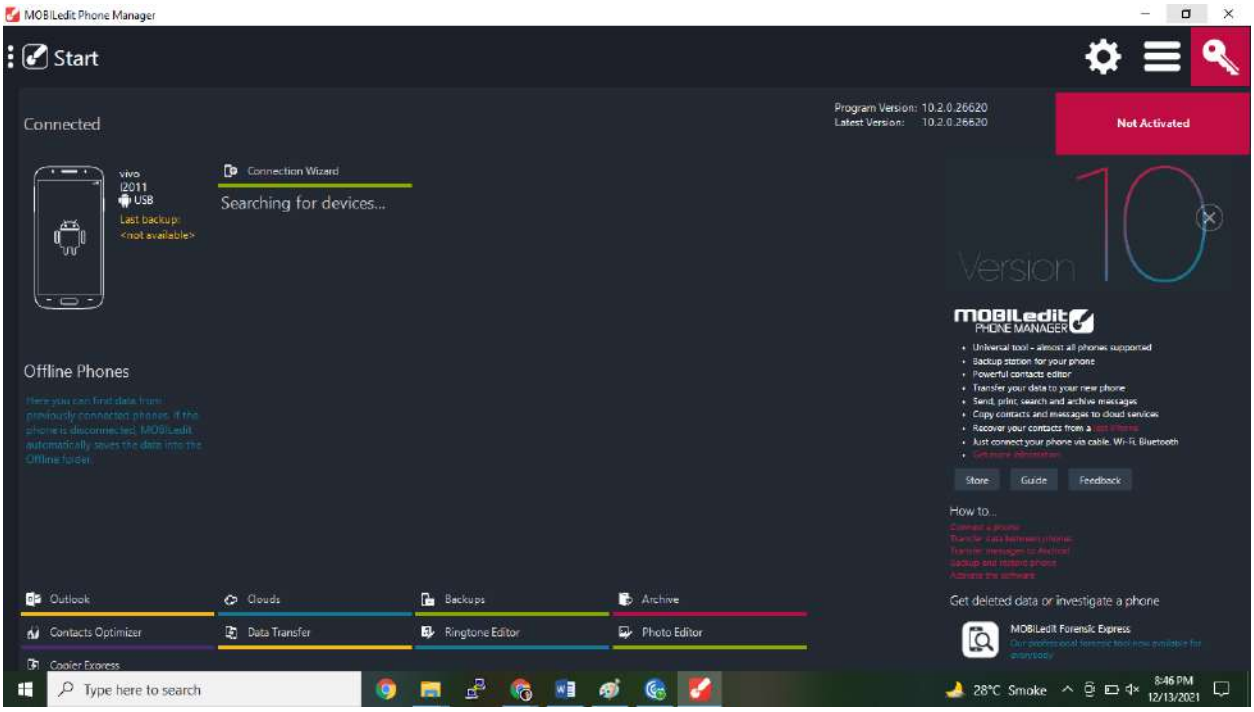




4) Allow USB debugging from this computer after connecting your mobile phone with your computer or laptop.

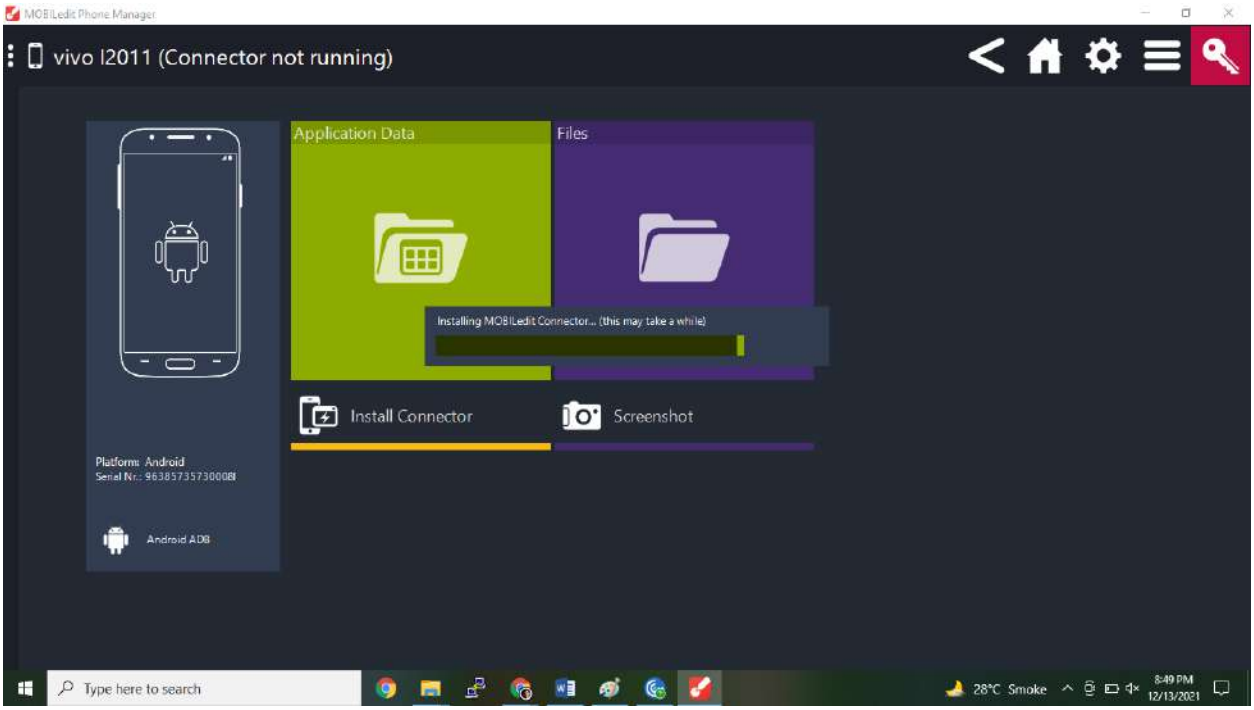
5) **Open MOBILedit Application. MOBILedit Phone Manager Activation tab will open, click on Activate Later.**



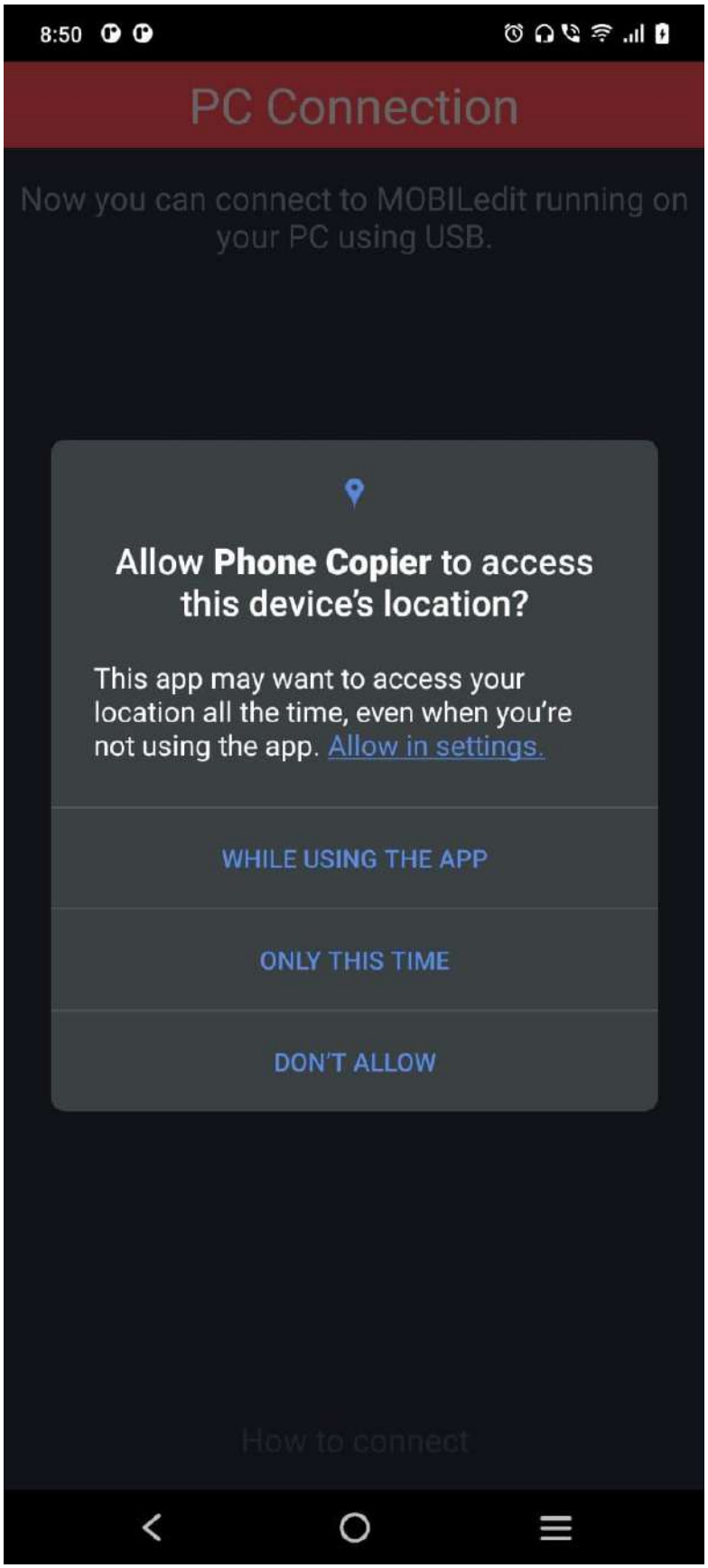


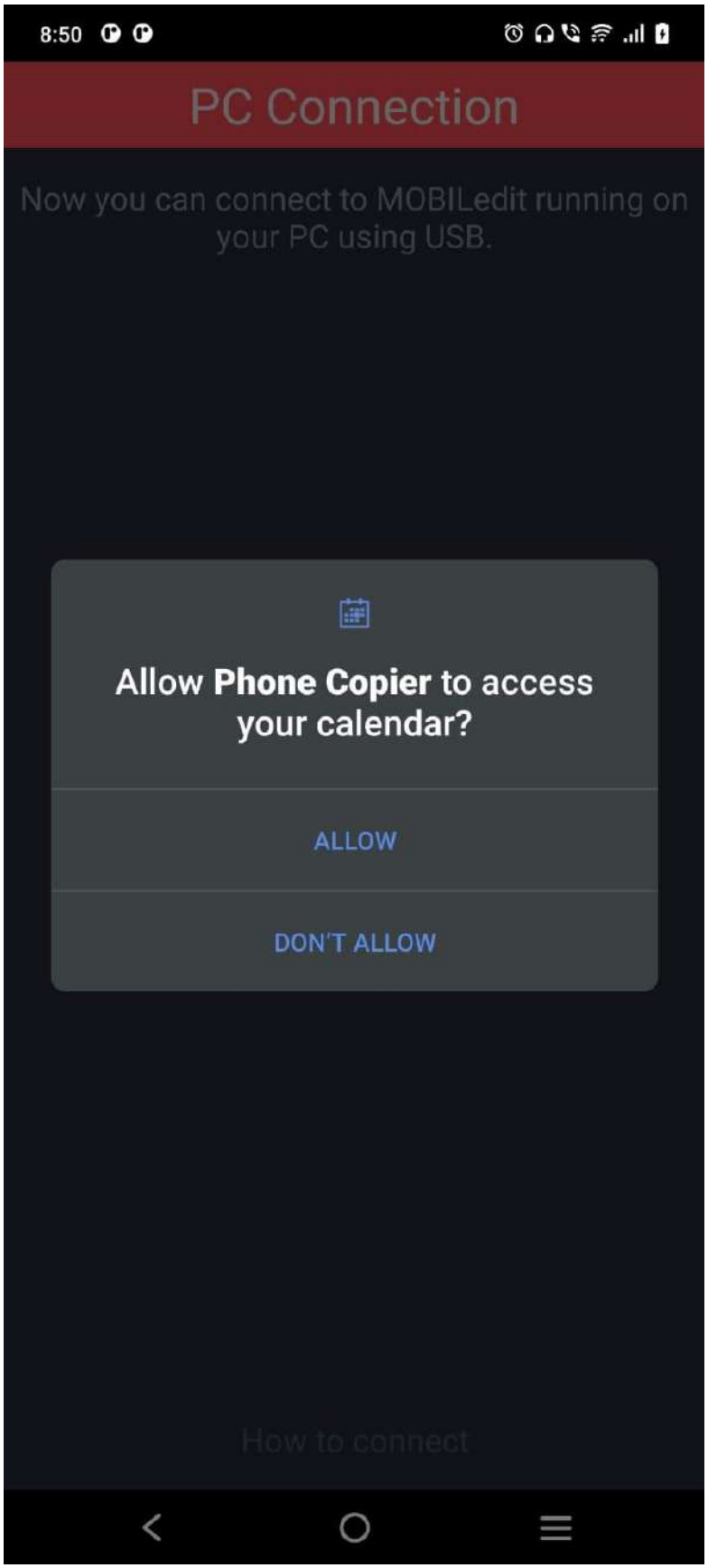
Once you click Always Allow option on your mobile phone, your phone will get connected.

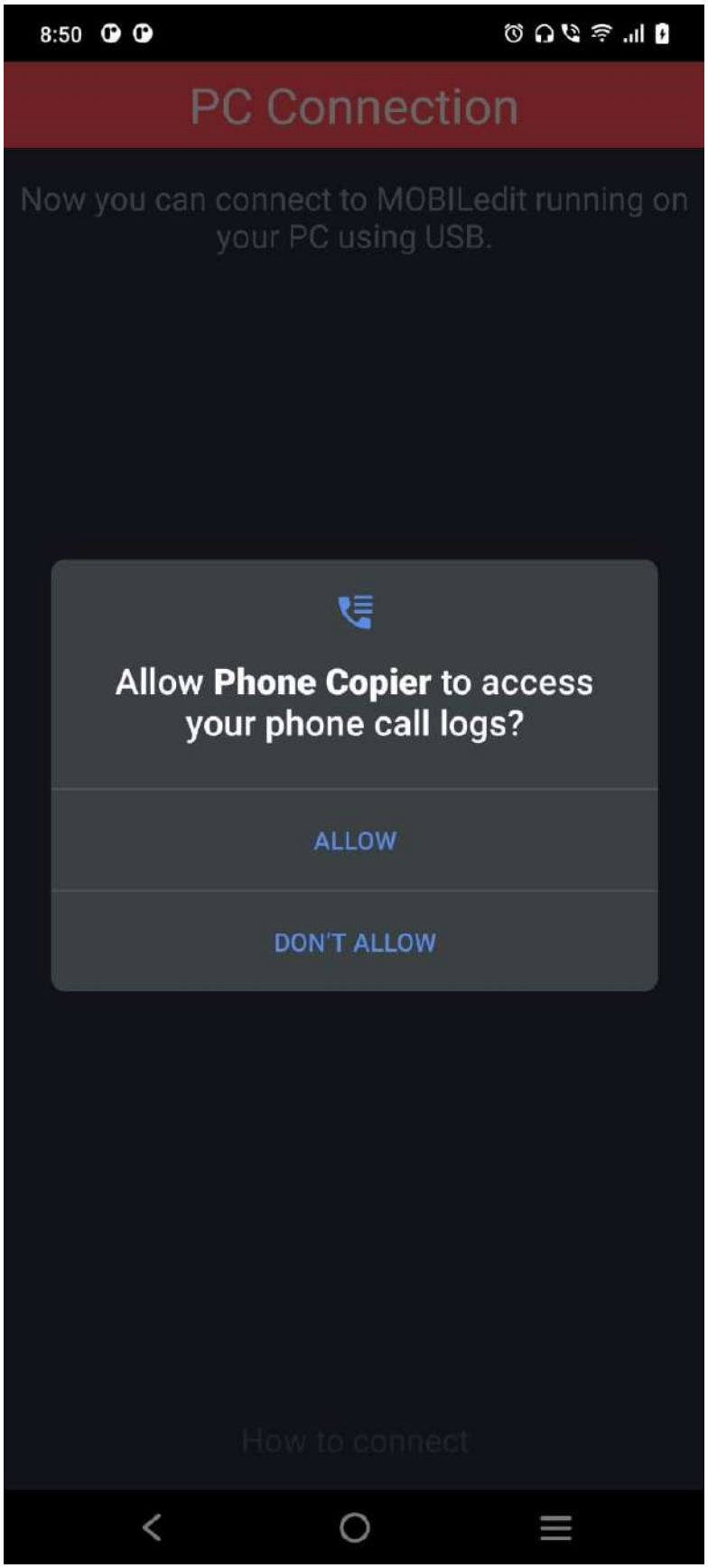
Double click on Connected phone The MOBILedit connector will start to install.

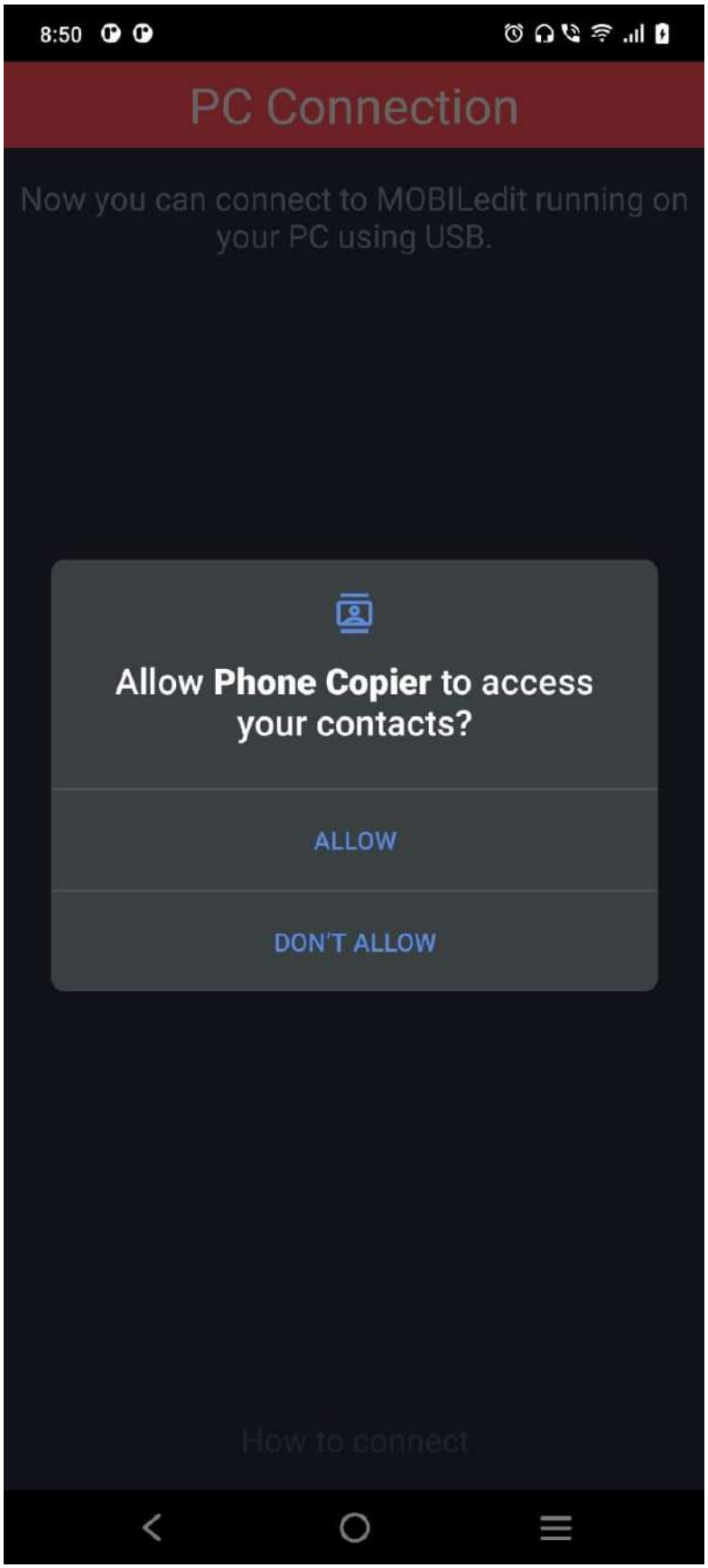


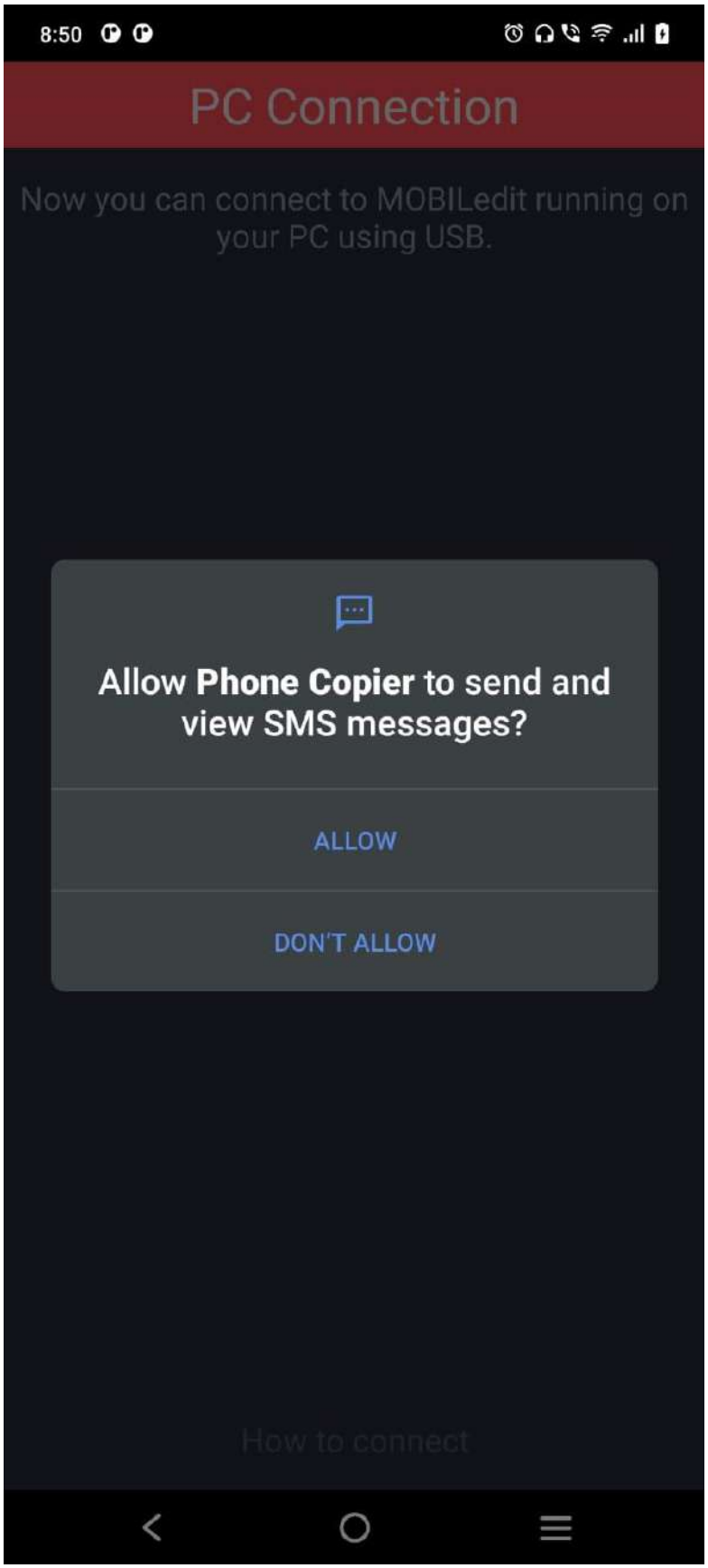
Then allow for all the popups which appear on your mobile phone.

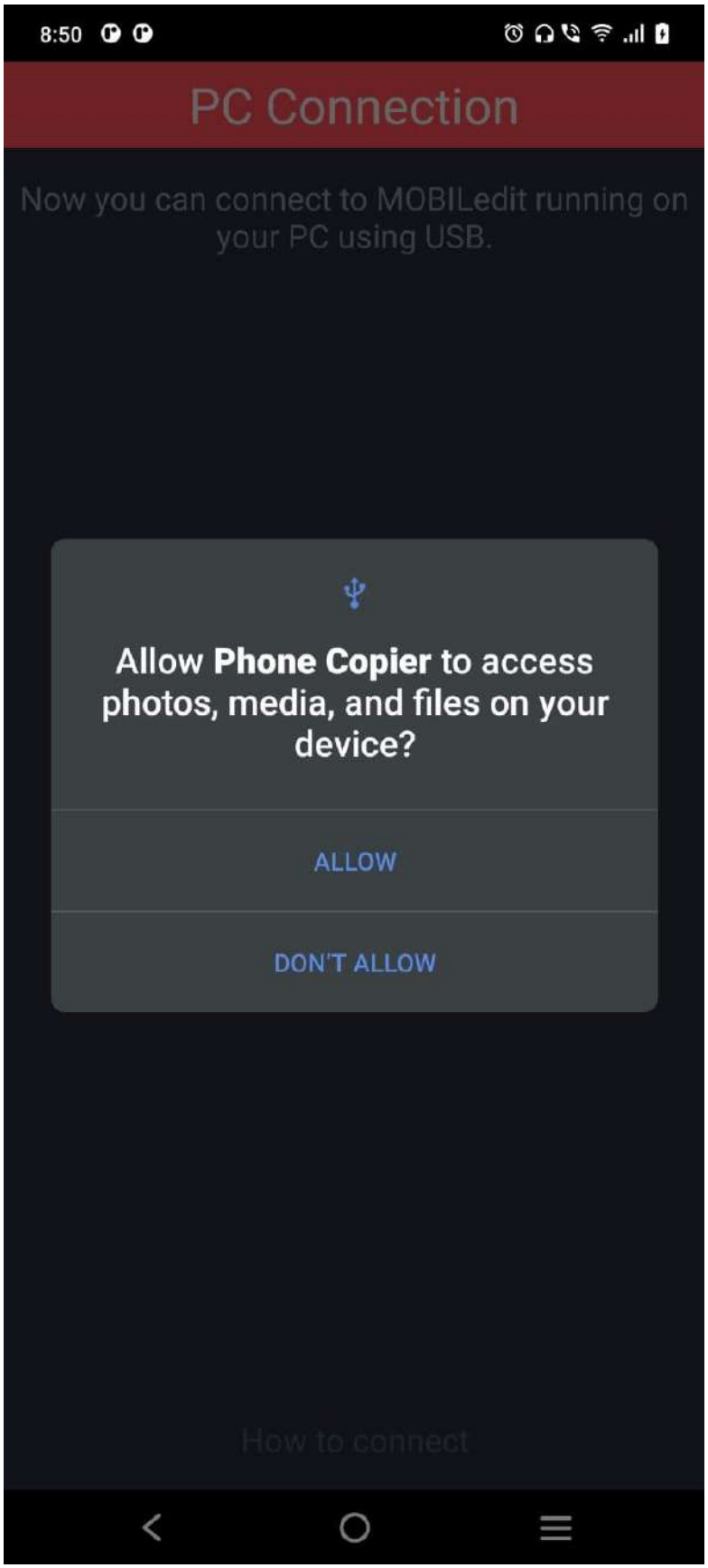

8:50
PC Connection
Now you can connect to MOBILedit running on your PC using USB.
Allow Phone Copier to access this device's location?
This app may want to access your location all the time, even when you're not using the app. Allow in settings.
WHILE USING THE APP
ONLY THIS TIME
DON'T ALLOW
How to connect

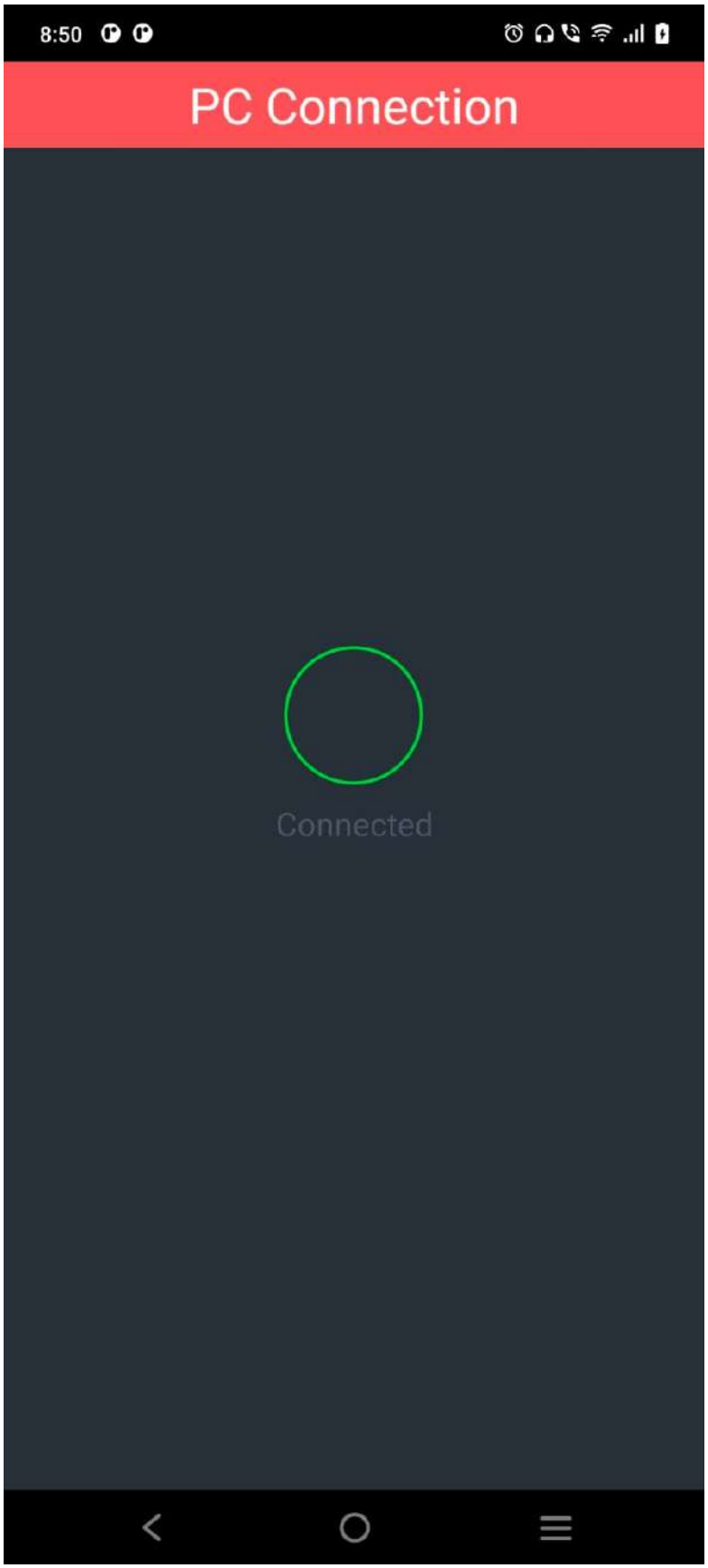

8:50
PC Connection
Now you can connect to MOBILedit running on your PC using USB.
Allow **Phone Copier** to access your calendar?
ALLOW
DON'T ALLOW
How to connect

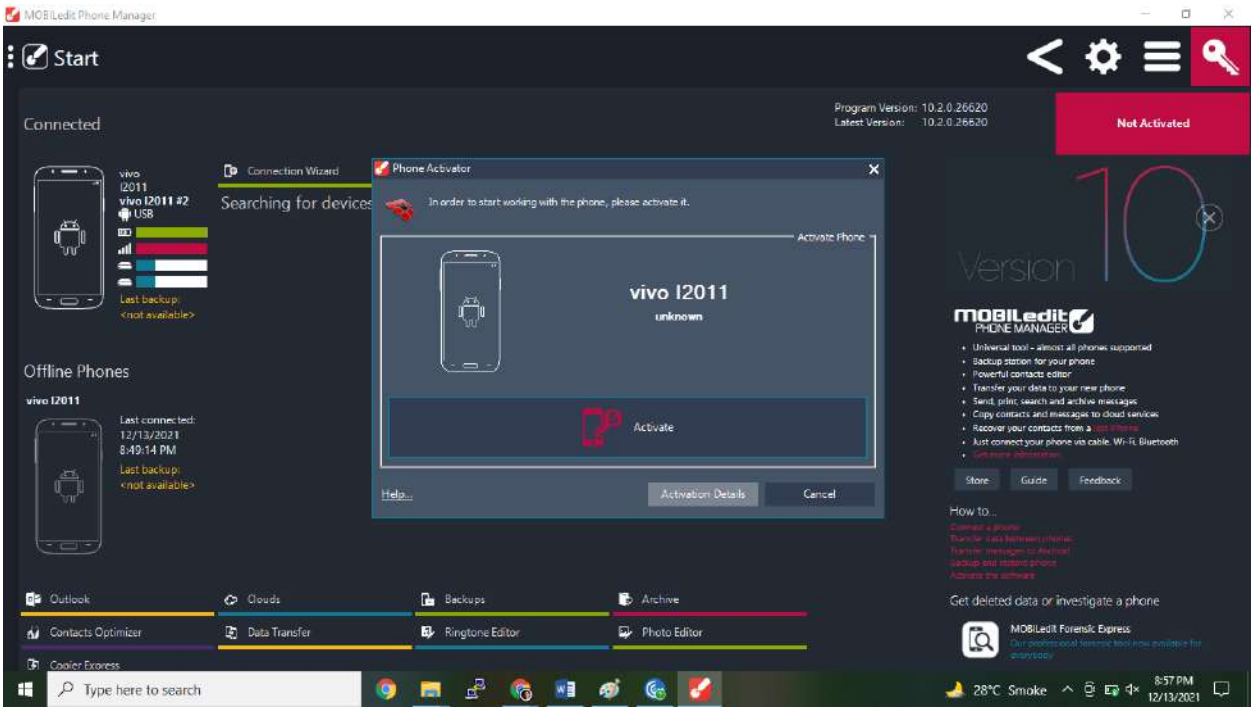

8:50
PC Connection
Now you can connect to MOBILedit running on your PC using USB.
Allow Phone Copier to access your phone call logs?
ALLOW
DON'T ALLOW
How to connect


8:50
PC Connection
Now you can connect to MOBILedit running on your PC using USB.
Allow **Phone Copier** to access your contacts?
ALLOW
DON'T ALLOW
How to connect

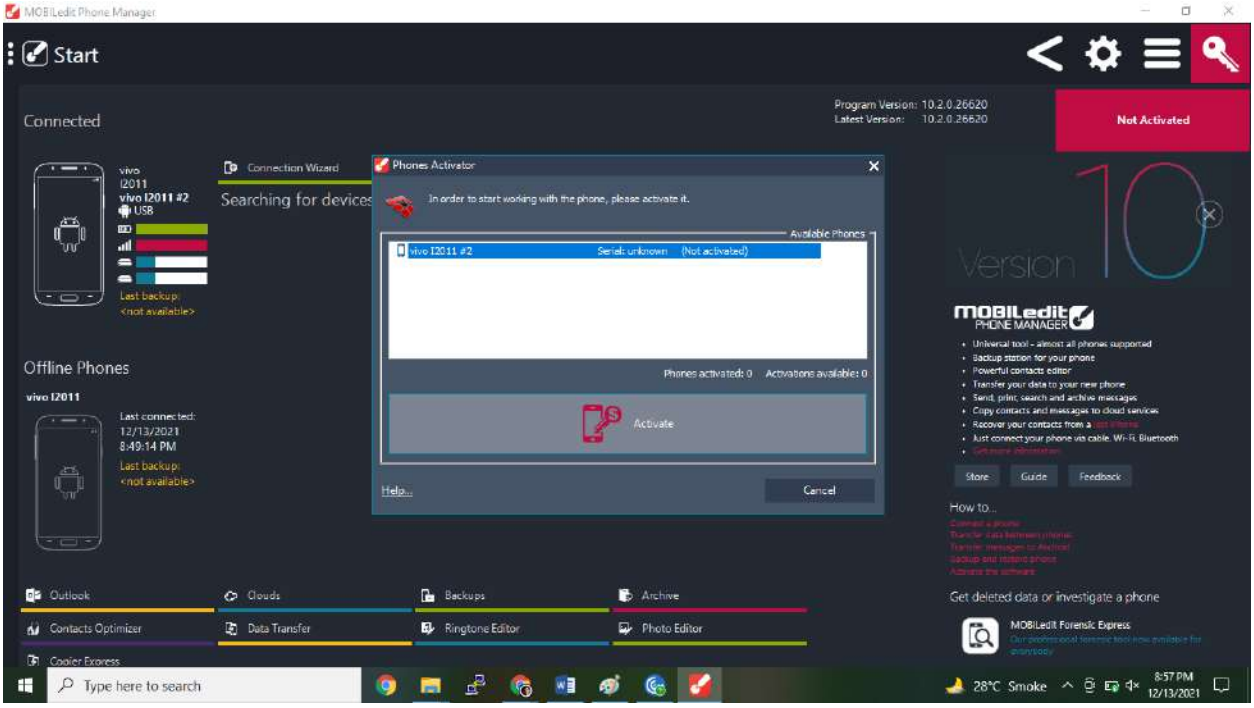

8:50
PC Connection
Now you can connect to MOBILedit running on your PC using USB.
Allow Phone Copier to send and view SMS messages?
ALLOW
DON'T ALLOW
How to connect


8:50
PC Connection
Now you can connect to MOBILedit running on your PC using USB.
Allow **Phone Copier** to access photos, media, and files on your device?
ALLOW
DON'T ALLOW
How to connect

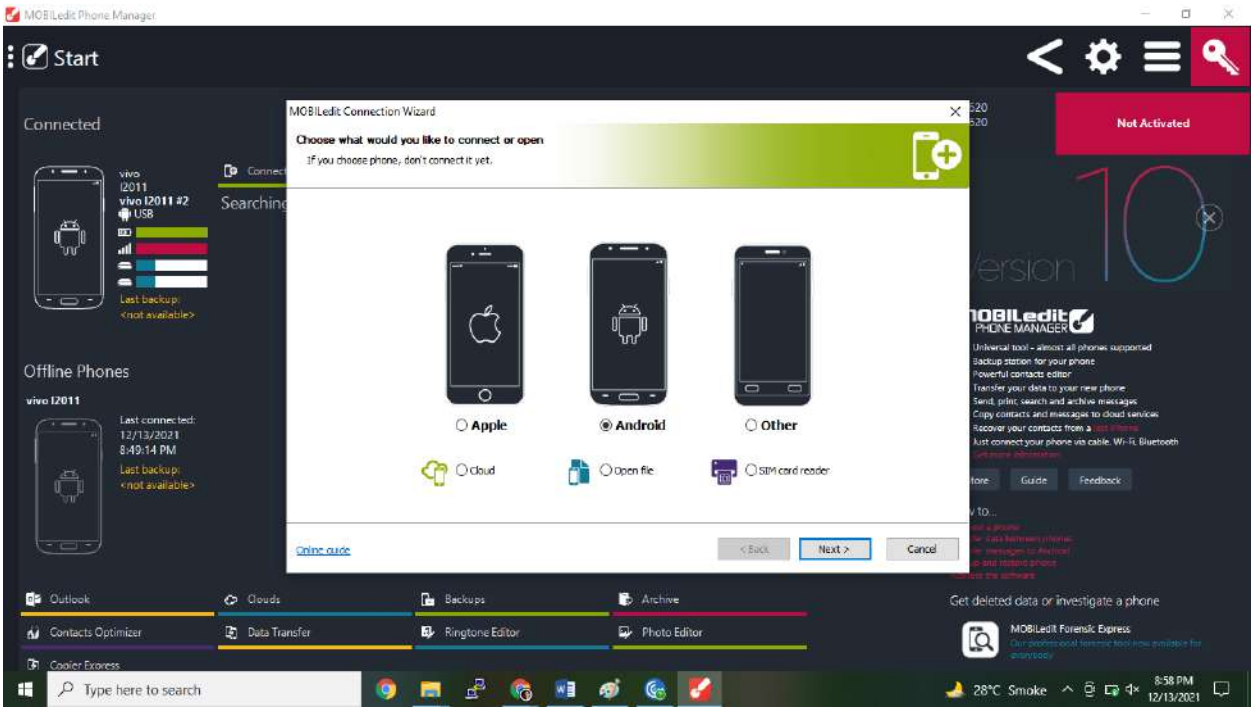

8:50
PC Connection
Connected



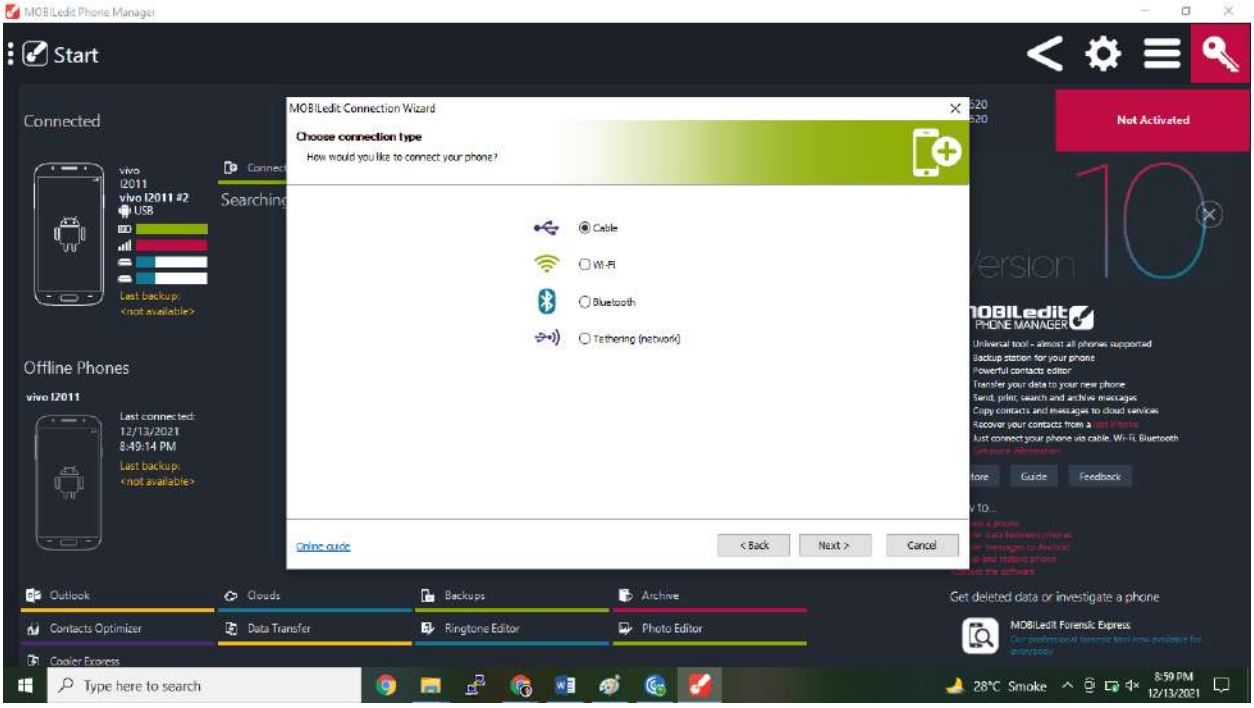
Click on Activate



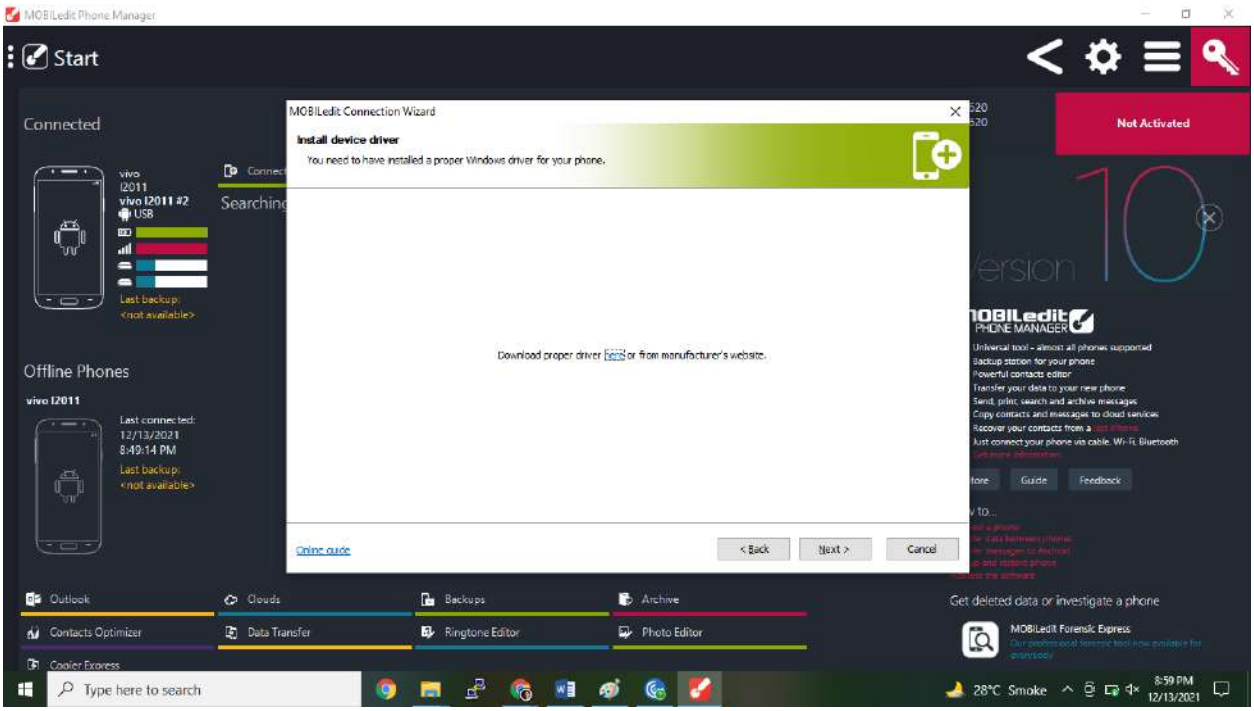
Then double click on Connection Wizard.



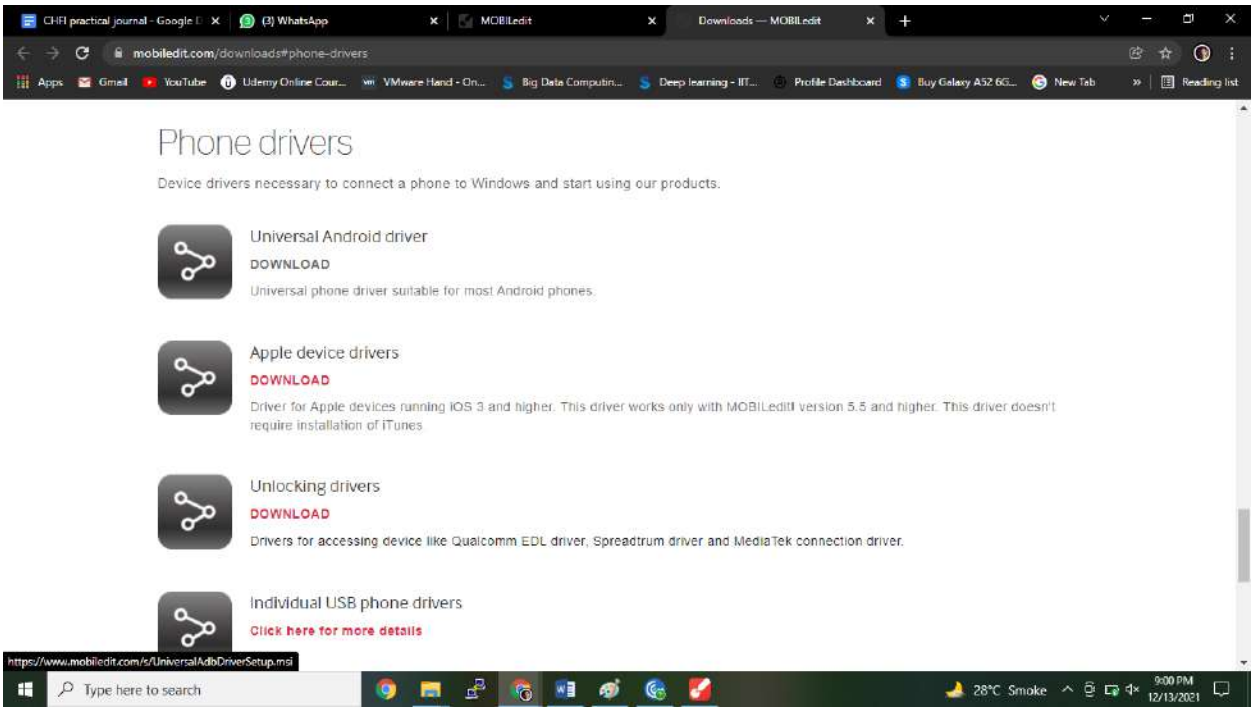
Then select and click on Next.

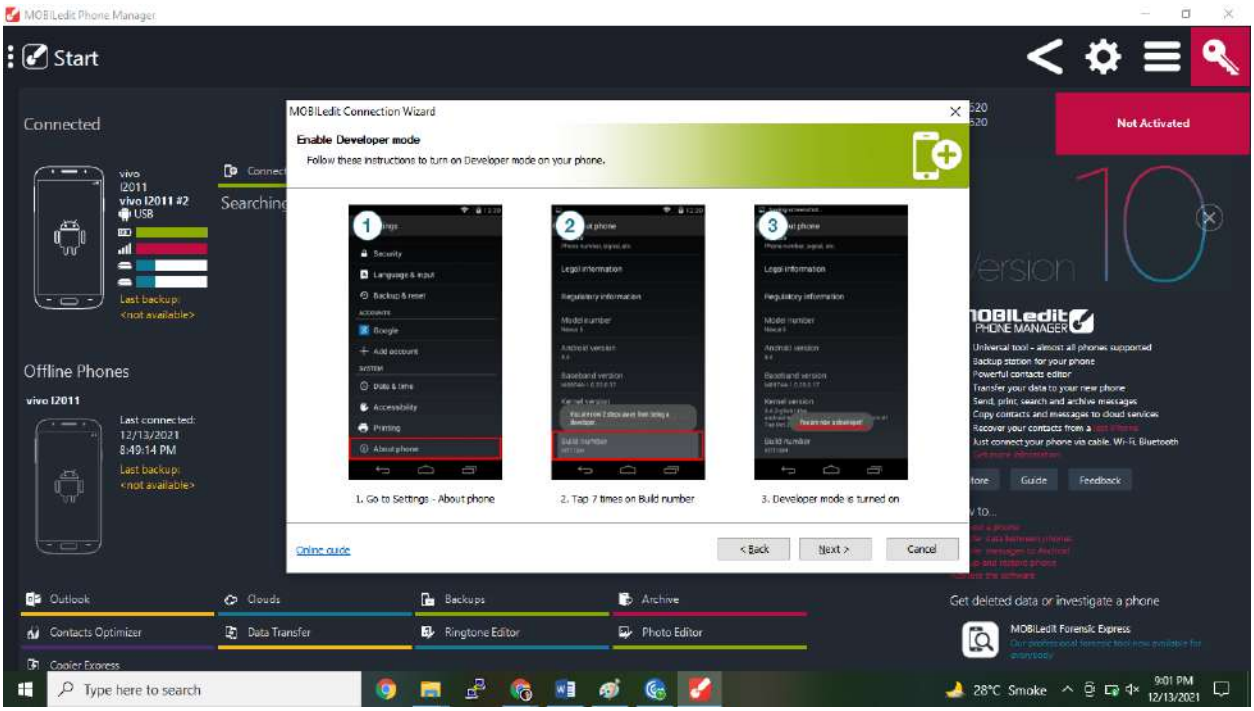


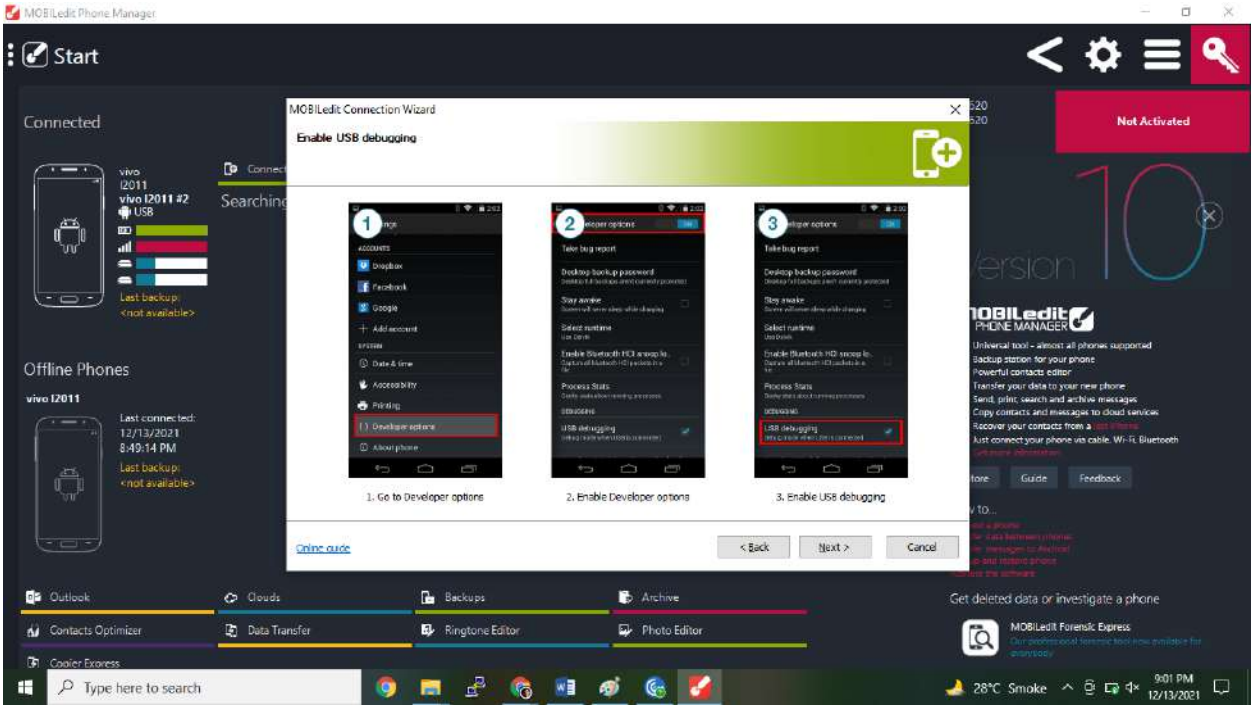
Click on here.



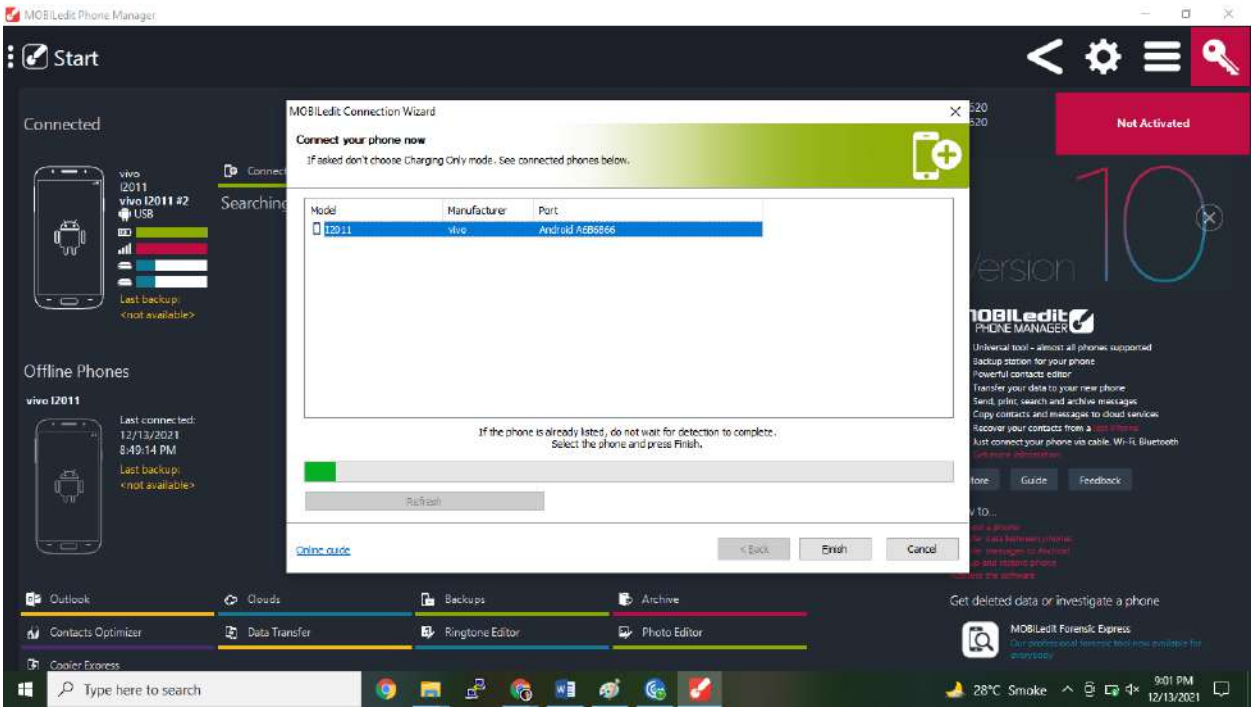
Download Universal Android Driver.



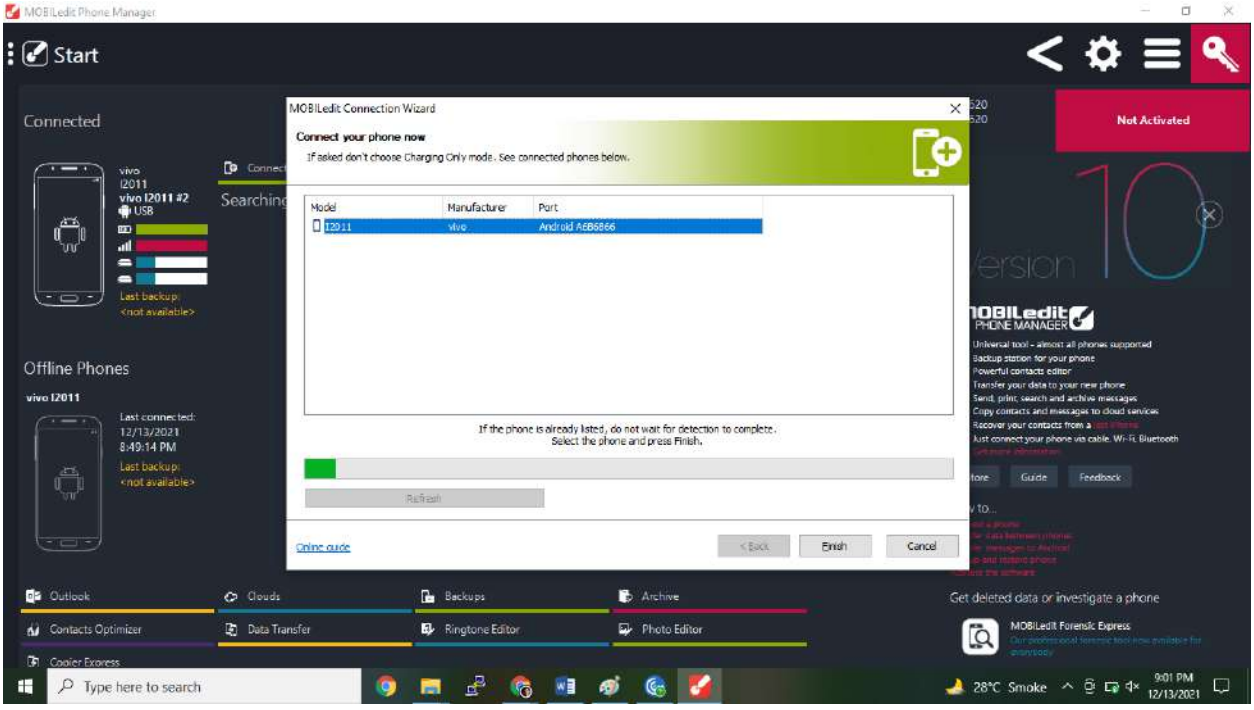




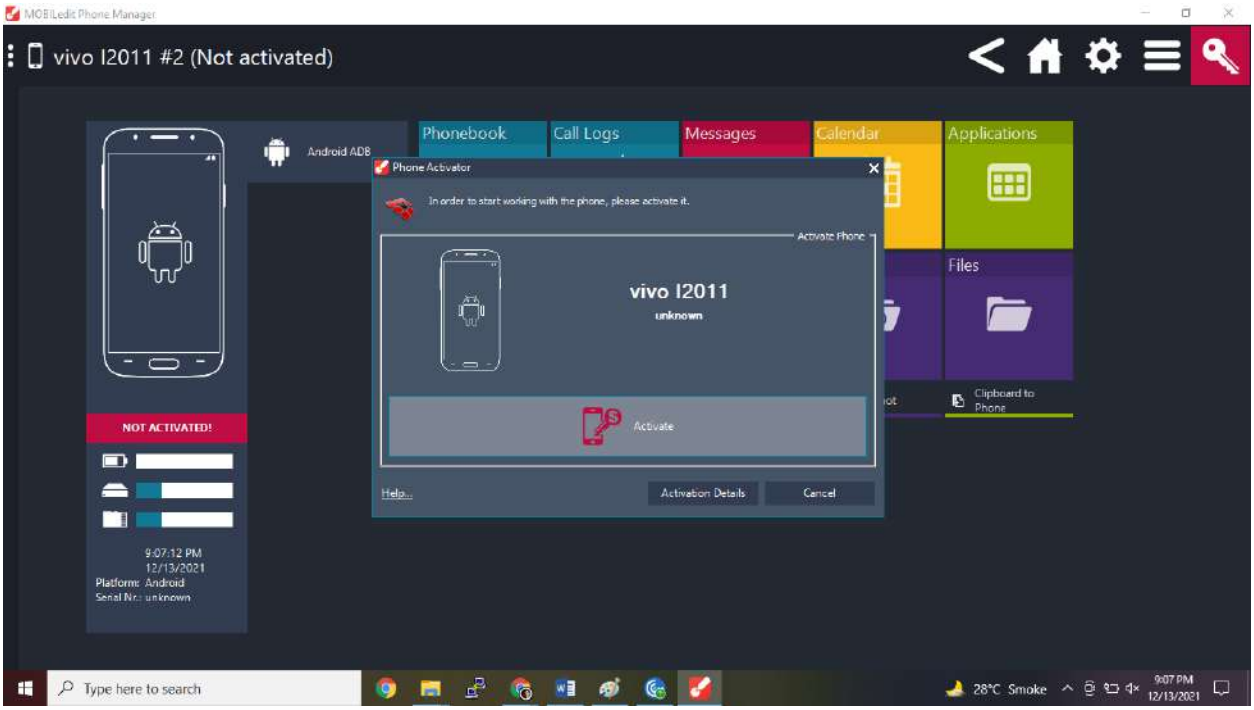
Your phone will appear here.

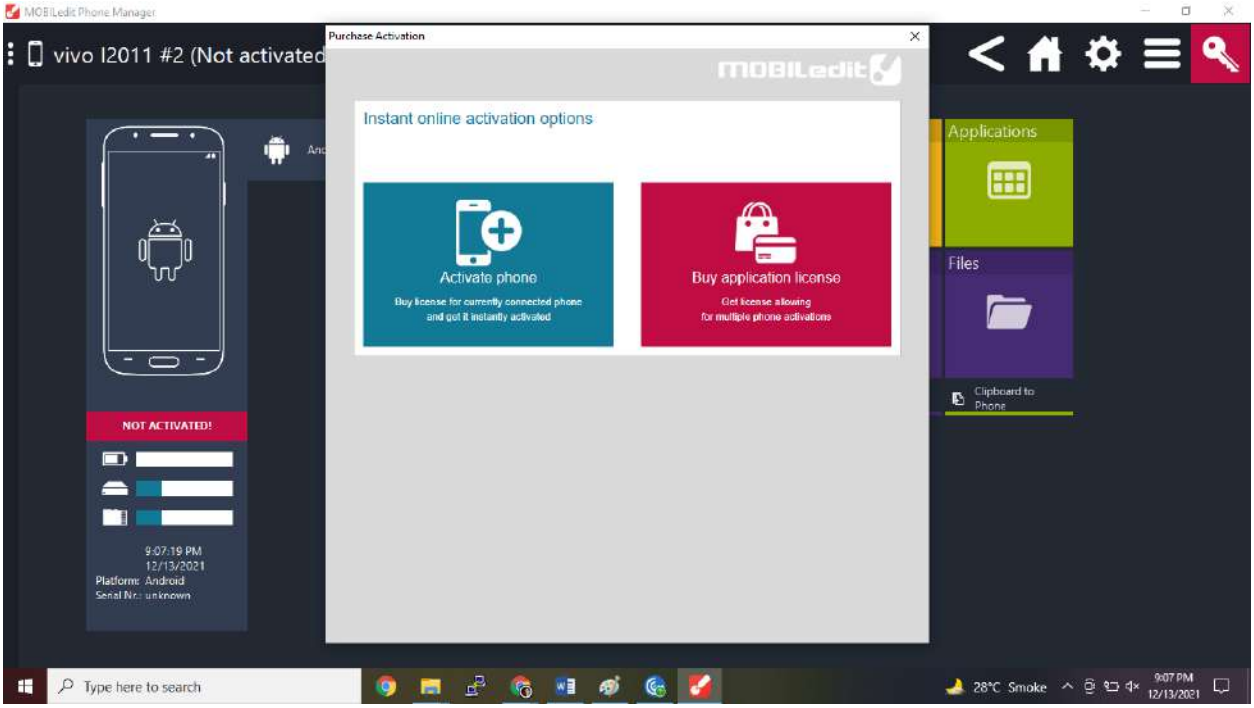


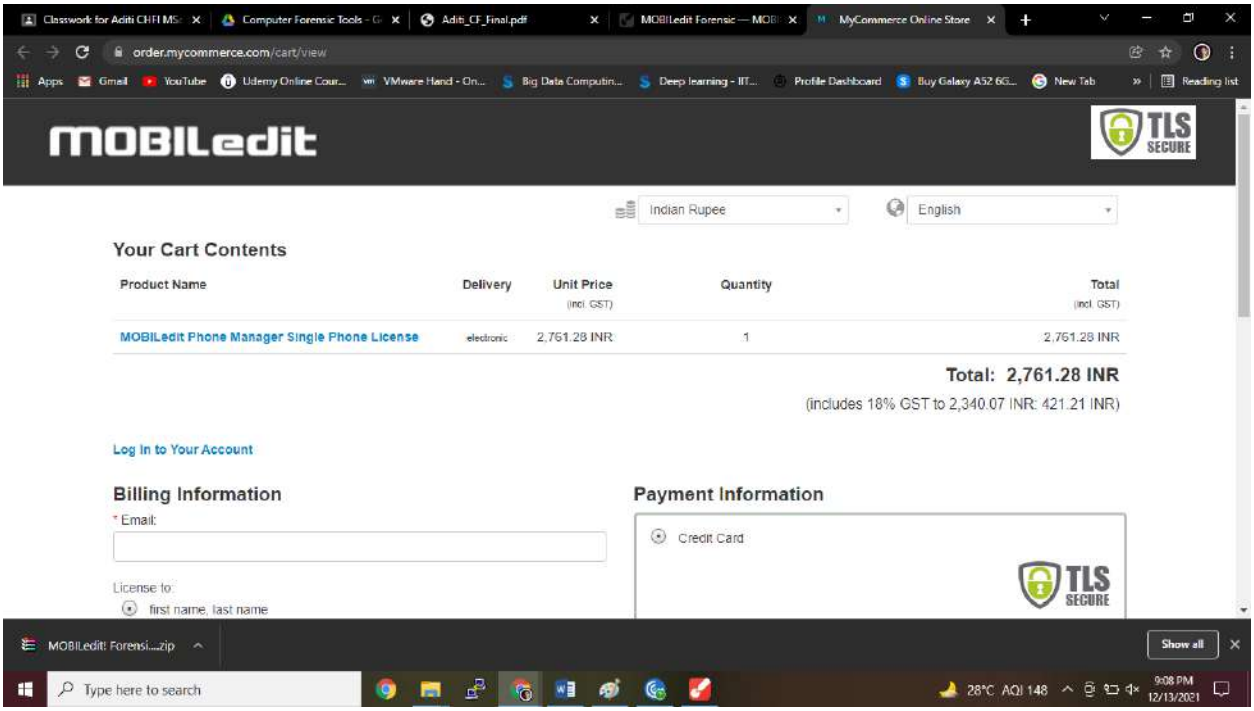
Click on Finish.



If you Activate the Phone Activator

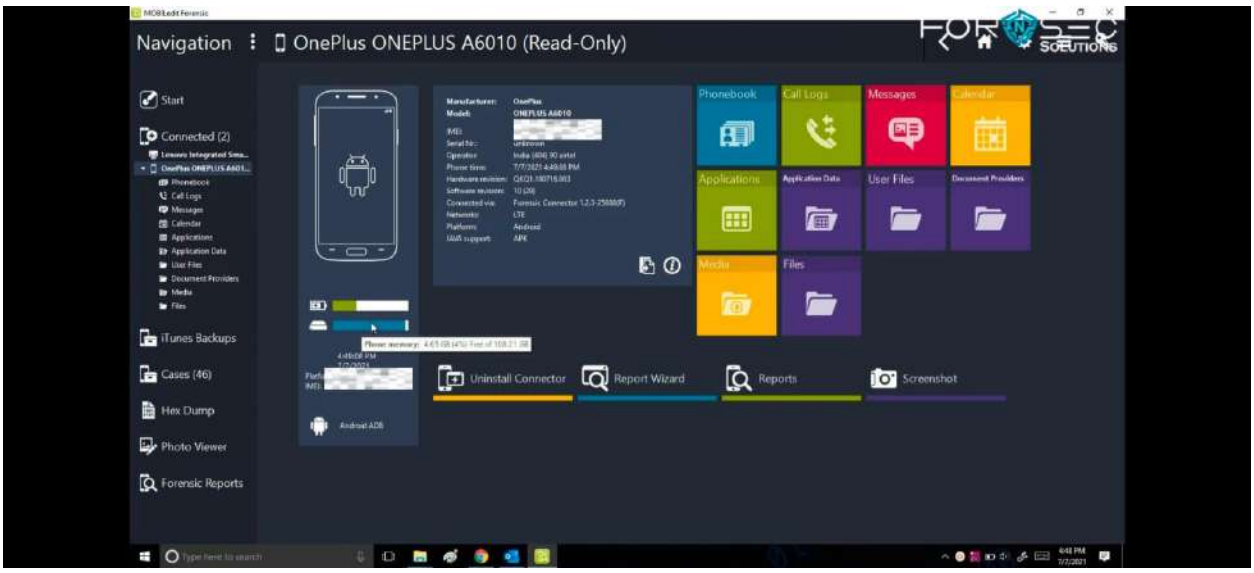

MOBILedit Phone Manager
vivo I2011 #2 (Not activated)
Phonebook
Call Logs
Messages
Calendar
Applications
Files
Android ADB
Phone Activator
In order to start working with the phone, please activate it.
Activate Phone
vivo I2011
unknown
Activate
Help...
Activation Details
Cancel
Clipboard to Phone
NOT ACTIVATED!
9:07:12 PM
12/13/2021
Platform: Android
Serial No.: unknown
Type here to search
28°C Smoke
9:07 PM
12/13/2021


MOBILedit Phone Manager
vivo I2011 #2 (Not activated)
Purchase Activation
MOBILedit
Instant online activation options
Activate phone
Buy license for currently connected phone and get it instantly activated
Buy application license
Get license allowing for multiple phone activations
Applications
Files
Clipboard to Phone
NOT ACTIVATED!
9:07:19 PM
12/13/2021
Platform: Android
Serial No.: unknown
Type here to search
28°C Smoke
9:07 PM
12/13/2021

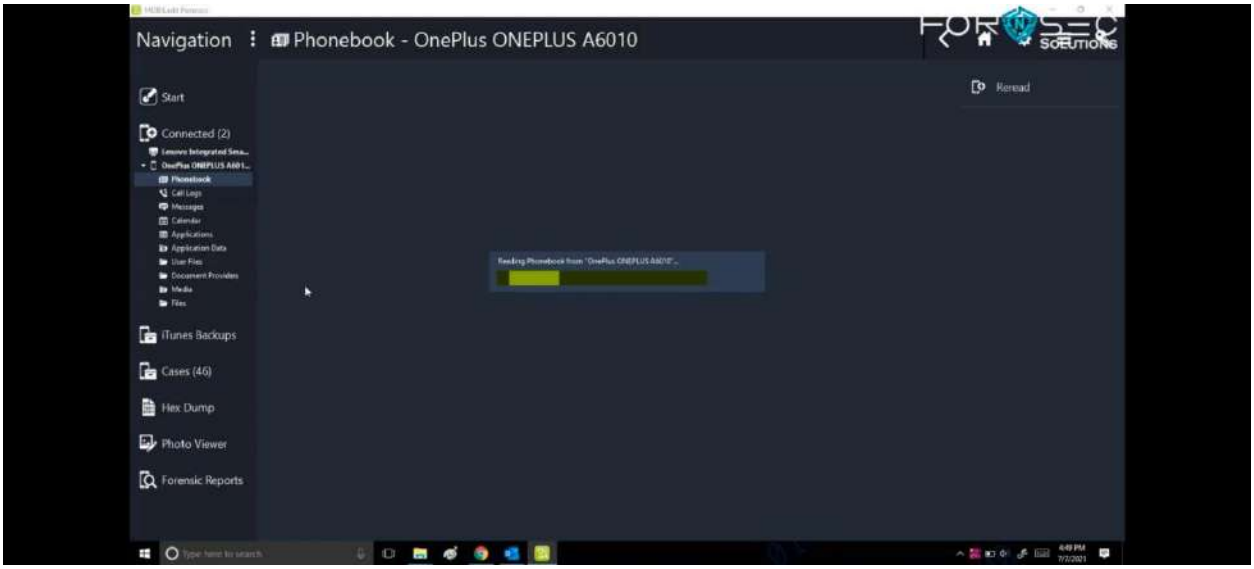


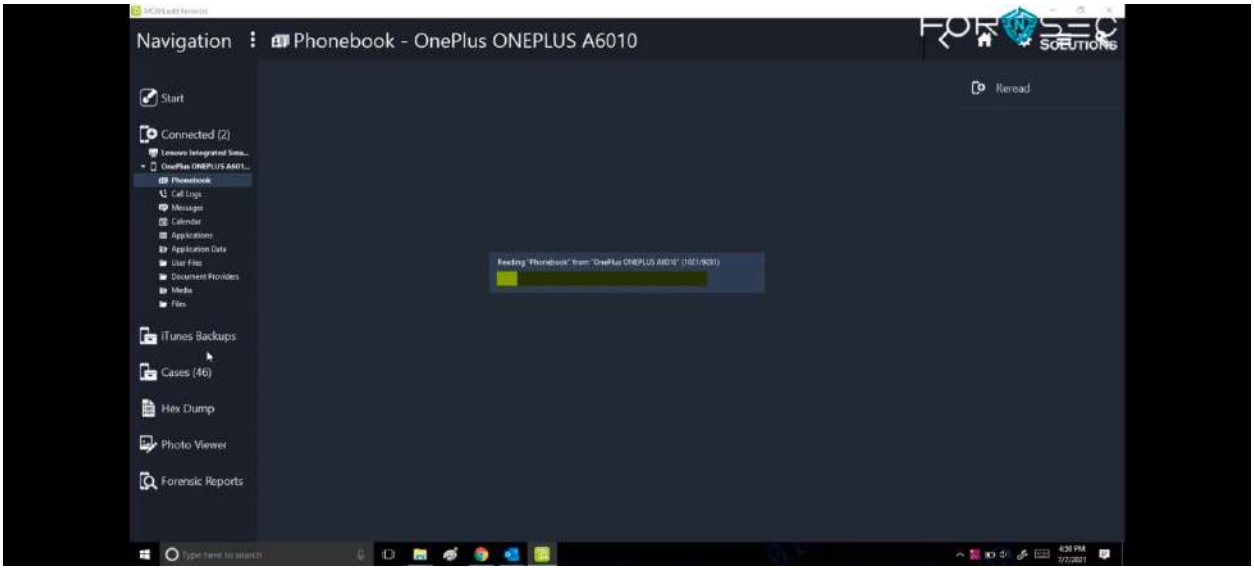
You need to purchase Activation in order to see all the details from mobile device.

After that you will get to see the details as follows. You can see all the details from mobile device, you can also make a report from it, you can export the data as well and get the report for your investigation.

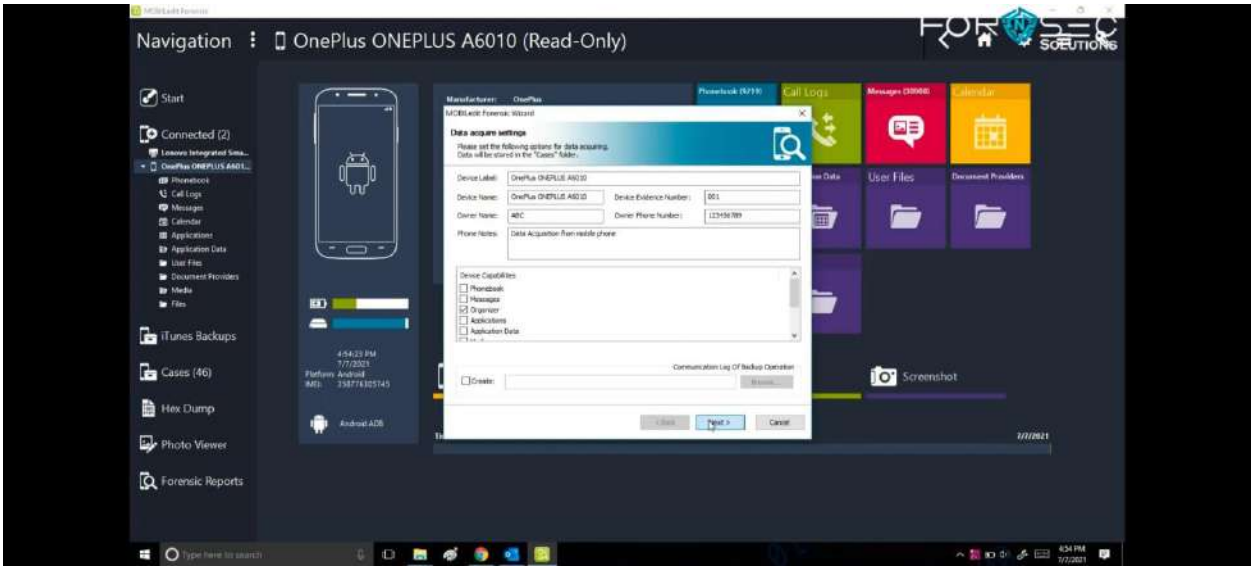


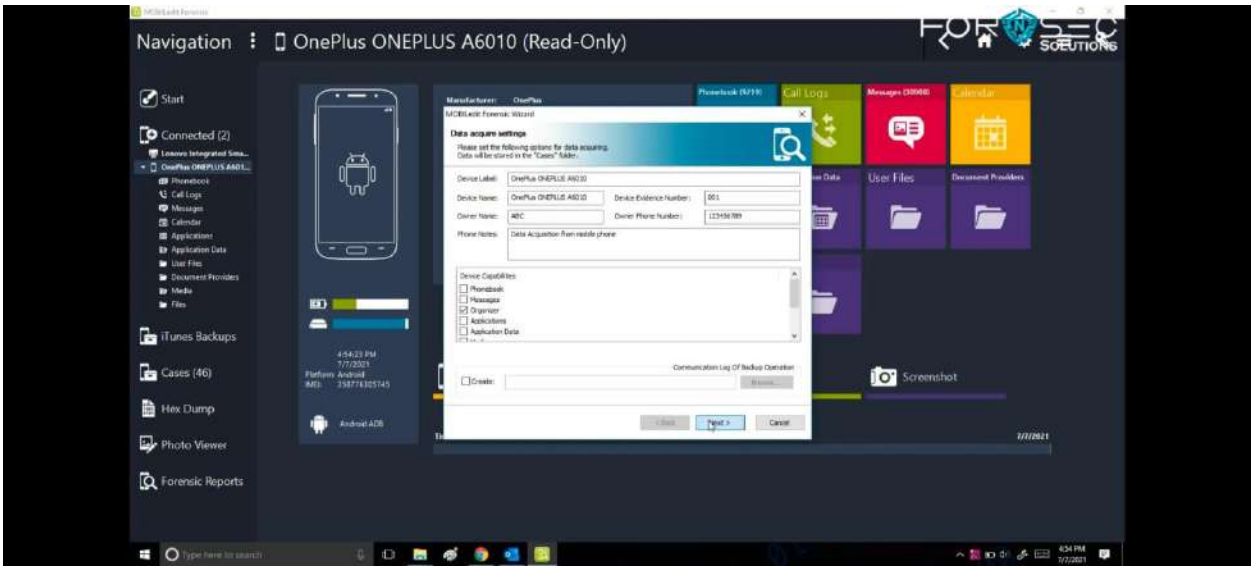

Navigation
OnePlus ONEPLUS A6010 (Read-Only)
Start
Connected (2)
iTunes Backups
Cases (46)
Hex Dump
Photo Viewer
Forensic Reports
Phonebook
Call Logs
Messages
Calendar
Applications
Application Data
User Files
Document Providers
Media
Files
Uninstall Connector
Report Wizard
Reports
Screenshot

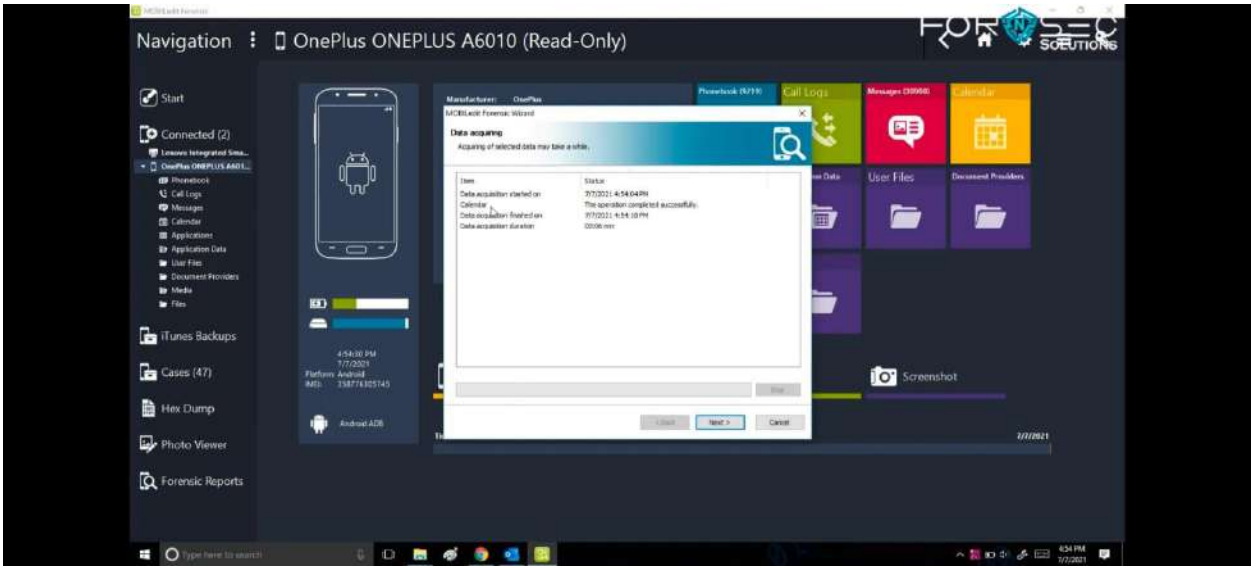

Navigation
Phonebook - OnePlus ONEPLUS A6010
Reread
Start
Connected (2)
iTunes Backups
Cases (46)
Hex Dump
Photo Viewer
Forensic Reports

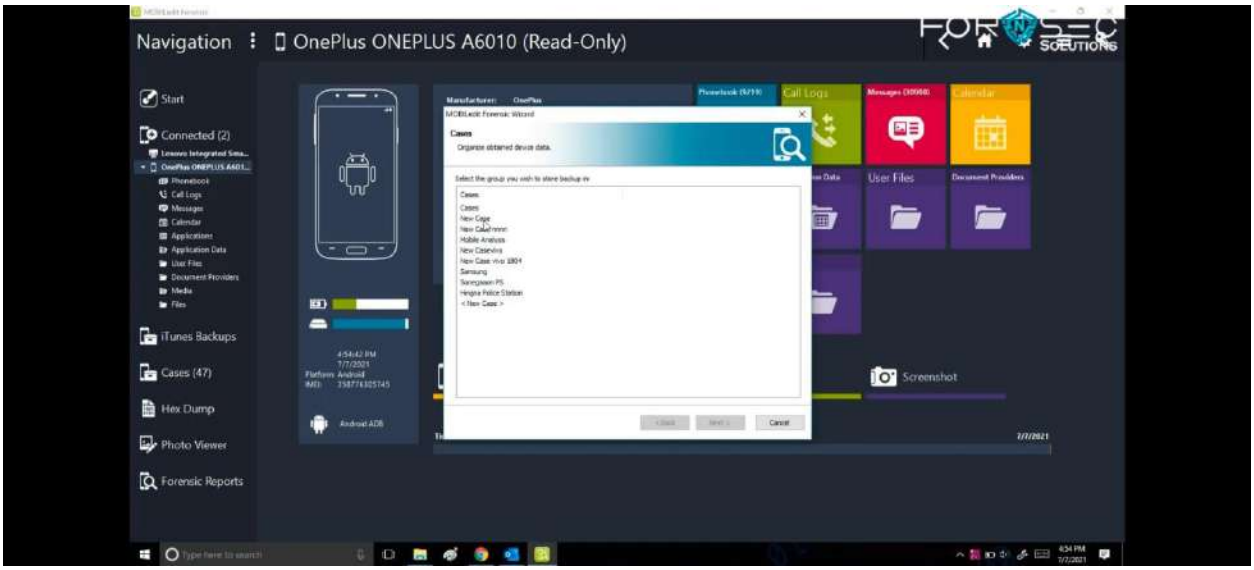

Navigation
Phonebook - OnePlus ONEPLUS A6010
Reread
Start
Connected (2)
iTunes Backups
Cases (46)
Hex Dump
Photo Viewer
Forensic Reports

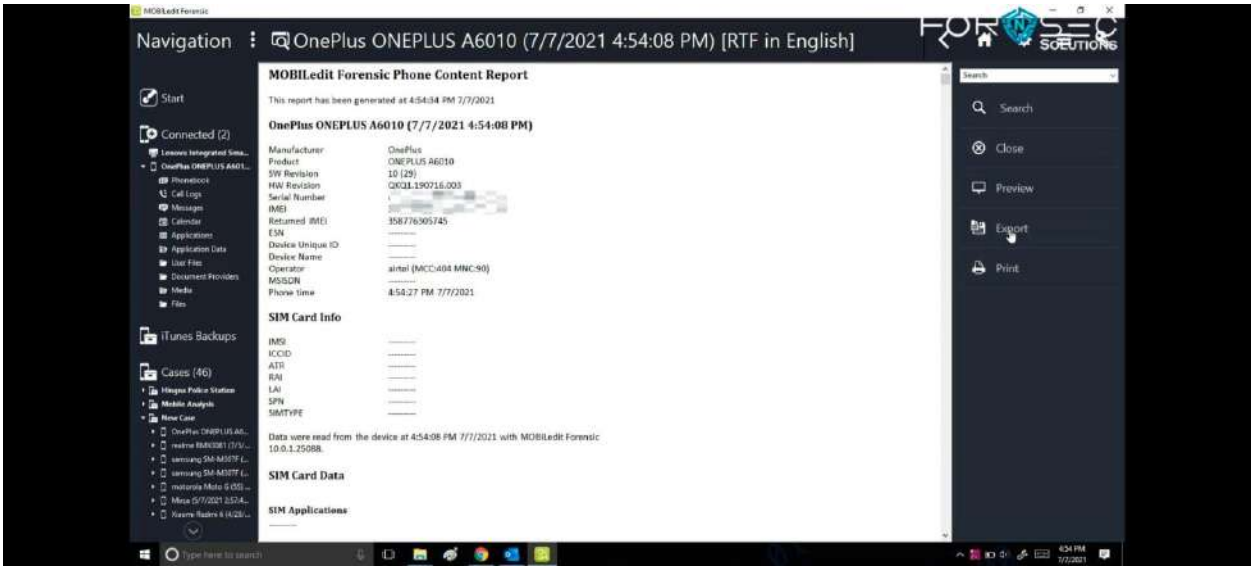

Navigation
OnePlus ONEPLUS A6010 (Read-Only)
Start
Connected (2)
iTunes Backups
Cases (46)
Hex Dump
Photo Viewer
Forensic Reports
Call Logs
Applications
User Files
Media
Files
Uninstall Connector
Report Wizard
Reports
Screenshot

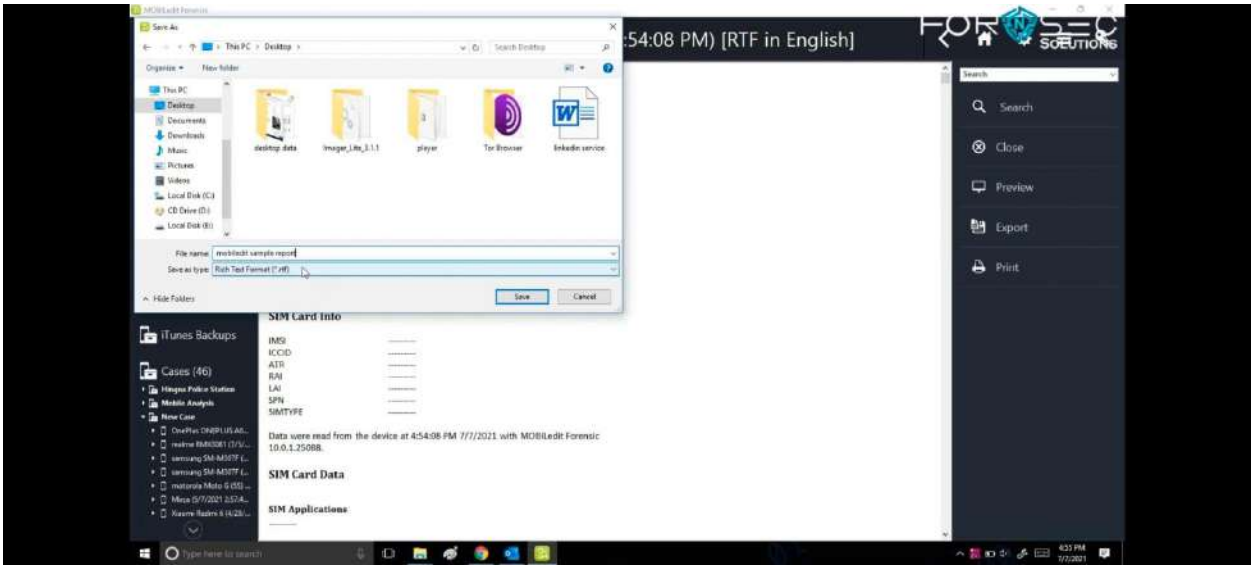

Navigation
OnePlus ONEPLUS A6010 (Read-Only)
FORENSIC SOLUTIONS
Start
Connected (2)
iTunes Backups
Cases (46)
Hex Dump
Photo Viewer
Forensic Reports
Call Logs
User Files
Screenshot
Data acquire settings
Next >
Cancel

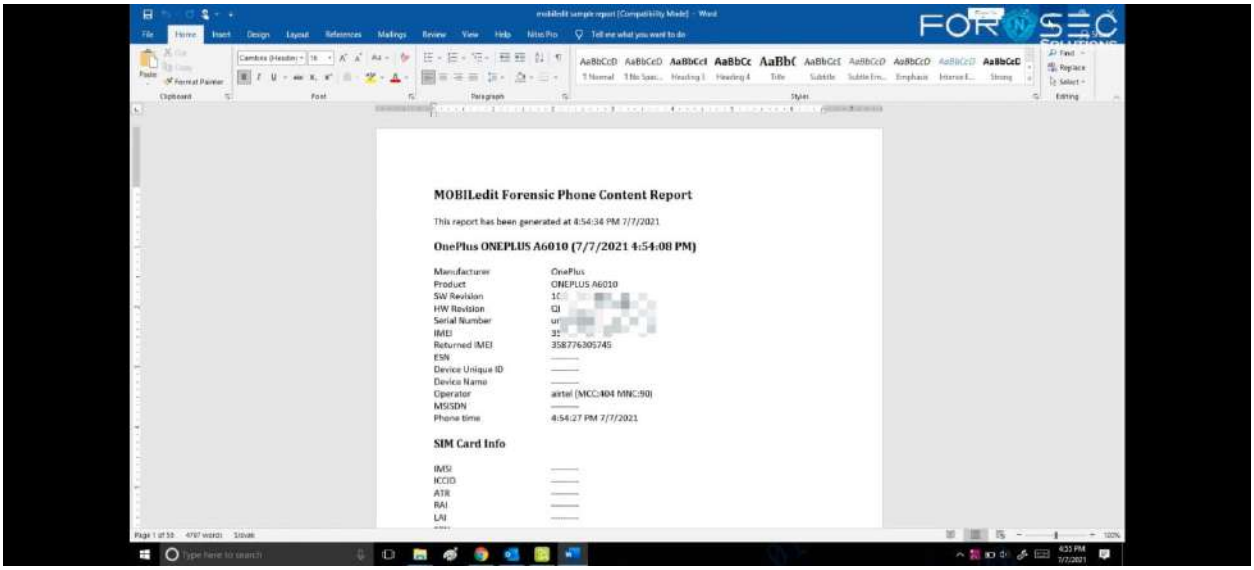

Navigation
OnePlus ONEPLUS A6010 (Read-Only)
FORENSIC SOLUTIONS
Start
Connected (2)
iTunes Backups
Cases (46)
Hex Dump
Photo Viewer
Forensic Reports
Call Logs
User Files
Screenshot
Data acquire settings
Next >
Cancel

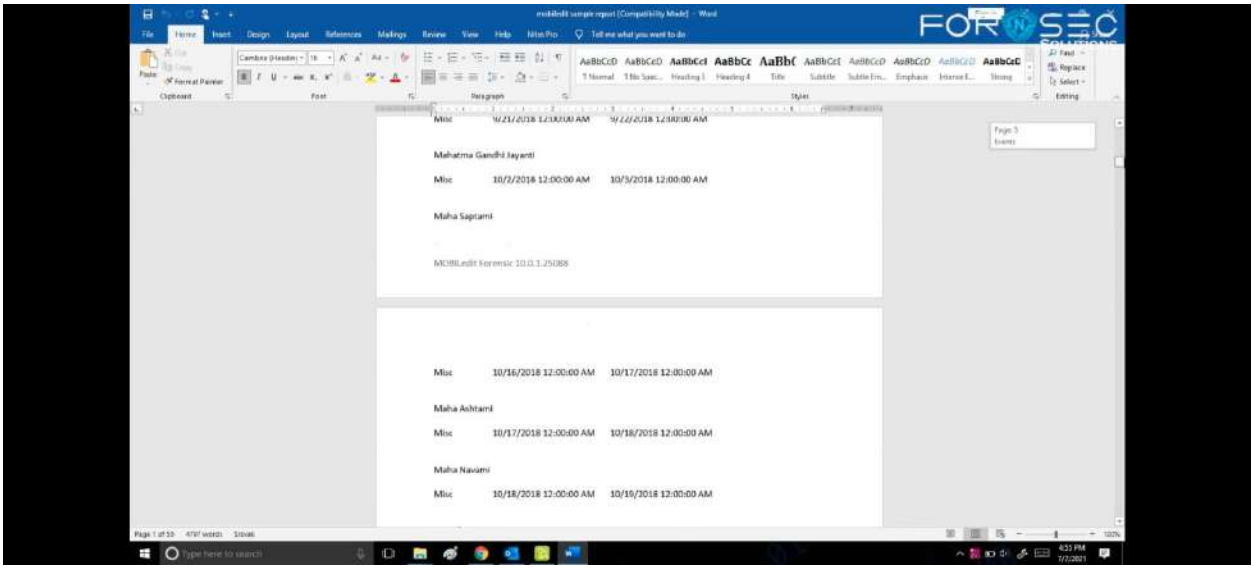

Navigation
OnePlus ONEPLUS A6010 (Read-Only)
Start
Connected (2)
iTunes Backups
Cases (47)
Hex Dump
Photo Viewer
Forensic Reports
Call Logs
User Files
Screenshot
Data acquiring
Acquiring of selected data may take a while.
Next >
Cancel


Navigation
OnePlus ONEPLUS A6010 (Read-Only)
Start
Connected (2)
iTunes Backups
Cases (47)
Hex Dump
Photo Viewer
Forensic Reports
Call Logs
User Files
Screenshot
Cases
Organize obtained device data.
Cancel


Navigation
OnePlus ONEPLUS A6010 (7/7/2021 4:54:08 PM) [RTF in English]
MOBILedit Forensic Phone Content Report
This report has been generated at 4:54:34 PM 7/7/2021
OnePlus ONEPLUS A6010 (7/7/2021 4:54:08 PM)
Manufacturer OnePlus
Product ONEPLUS A6010
SW Revision 10 (29)
HW Revision QKQ1.190716.003
Serial Number
IMEI
Returned IMEI 358776305745
ESN
Device Unique ID
Device Name
Operator airtel (MCC:404 MNC:90)
MSISDN
Phone time 4:54:27 PM 7/7/2021
SIM Card Info
IMSI
ICCID
ATR
RAI
LAI
SPN
SIMTYPE
Data were read from the device at 4:54:08 PM 7/7/2021 with MOBILedit Forensic 10.0.1.25088.
SIM Card Data
SIM Applications
Start
Connected (2)
iTunes Backups
Cases (46)
Search
Close
Preview
Export
Print


:54:08 PM) [RTF in English]
Save As
This PC > Desktop >
Search Desktop
Organize
New folder
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
CD Drive (D:)
Local Disk (E:)
desktop data
Imager_Lite_3.1.1
player
Tor Browser
linkedin service
File name: mobiledit sample report
Save as type: Rich Text Format (*.rtf)
Hide Folders
Save
Cancel
SIM Card Info
IMSI
ICCID
ATR
RAI
LAI
SPN
SIMTYPE
Data were read from the device at 4:54:08 PM 7/7/2021 with MOBILedit Forensic 10.0.1.25088.
SIM Card Data
SIM Applications
iTunes Backups
Cases (46)
Search
Close
Preview
Export
Print





Practical No. 14

Aim: Forensic Investigation Using Encase

What is Forensic Investigation?

Forensics are the scientific methods used to solve a crime. Forensic investigation is the gathering and analysis of all crime-related physical evidence in order to come to a conclusion about a suspect. Investigators will look at blood, fluid, or fingerprints, residue, hard drives, computers, or other technology to establish how a crime took place. This is a general definition, though, since there are a number of different types of forensics.

Types of Forensic Investigation:

- Forensic Accounting / Auditing
- Computer or Cyber Forensics
- Crime Scene Forensics
- Forensic Archaeology
- Forensic Dentistry
- Forensic Entomology
- Forensic Graphology
- Forensic Pathology
- Forensic Psychology
- Forensic Science
- Forensic Toxicology

EnCase Tool

EnCase is the shared technology within a suite of digital investigations products by Guidance Software (acquired by OpenText in 2017). The software comes in several products designed for forensic, cyber security, security analytics, and e-discovery use. Encase is traditionally used in forensics to recover evidence from seized hard drives. Encase allows the investigator to conduct in depth analysis of user files to collect evidence such as documents, pictures, internet history and Windows Registry information.

The company also offers EnCase training and certification.

Data recovered by EnCase has been used in various court systems, such as in the cases of the BTK Killer and the murder of Danielle van Dam. Additional EnCase forensic work was documented in other cases such as the evidence provided for the Casey Anthony, Unabomber, and Mucko (Wakefield Massacre) cases.

Features

EnCase contains tools for several areas of the digital forensic process; acquisition, analysis and reporting. The software also includes a scripting facility called EnScript with various API's for interacting with evidence.

Expert Witness File Format

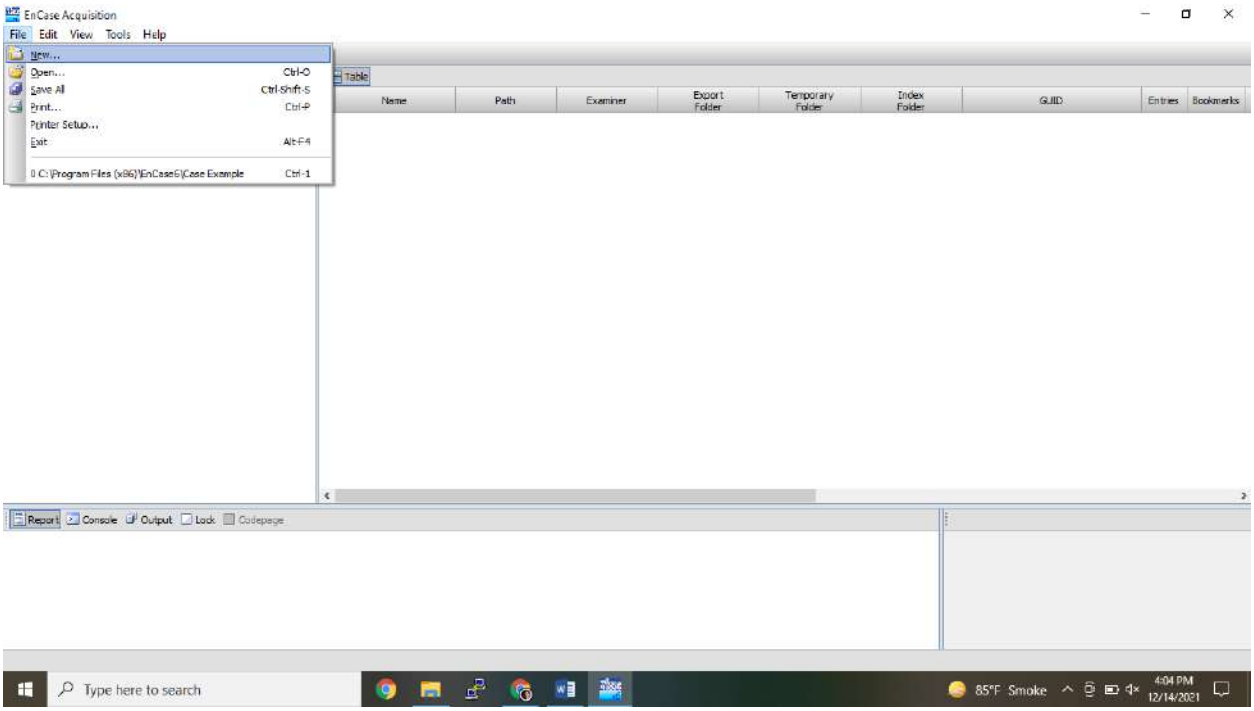
EnCase contains functionality to create forensic images of suspect media. Images are stored in proprietary Expert Witness File format; the compressible file format is prefixed with case data information and consists of a bit-by-bit (i.e. exact) copy of the media inter-spaced with CRC hashes for every 64K of data. The file format also appends an MD5 hash of the entire drive as a footer.

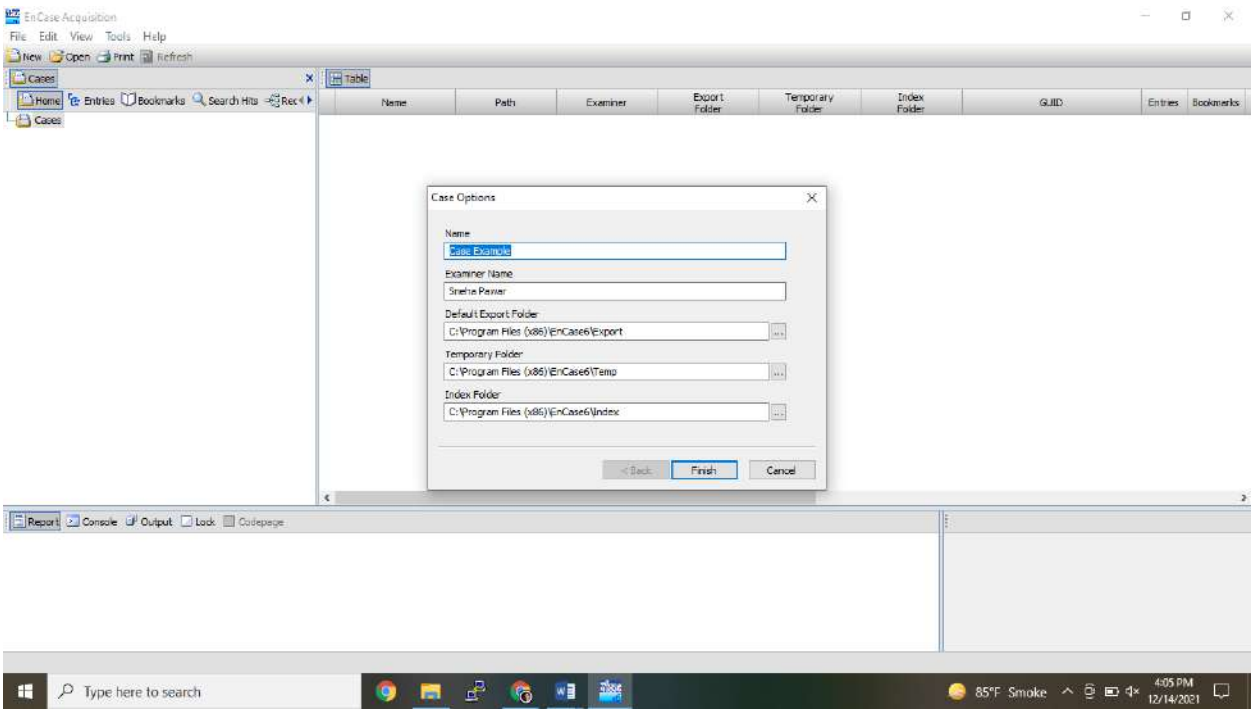
Mobile forensics

As of EnCase V7, Mobile Phone Analysis is possible with the addition some add-ons available from Guidance Software.

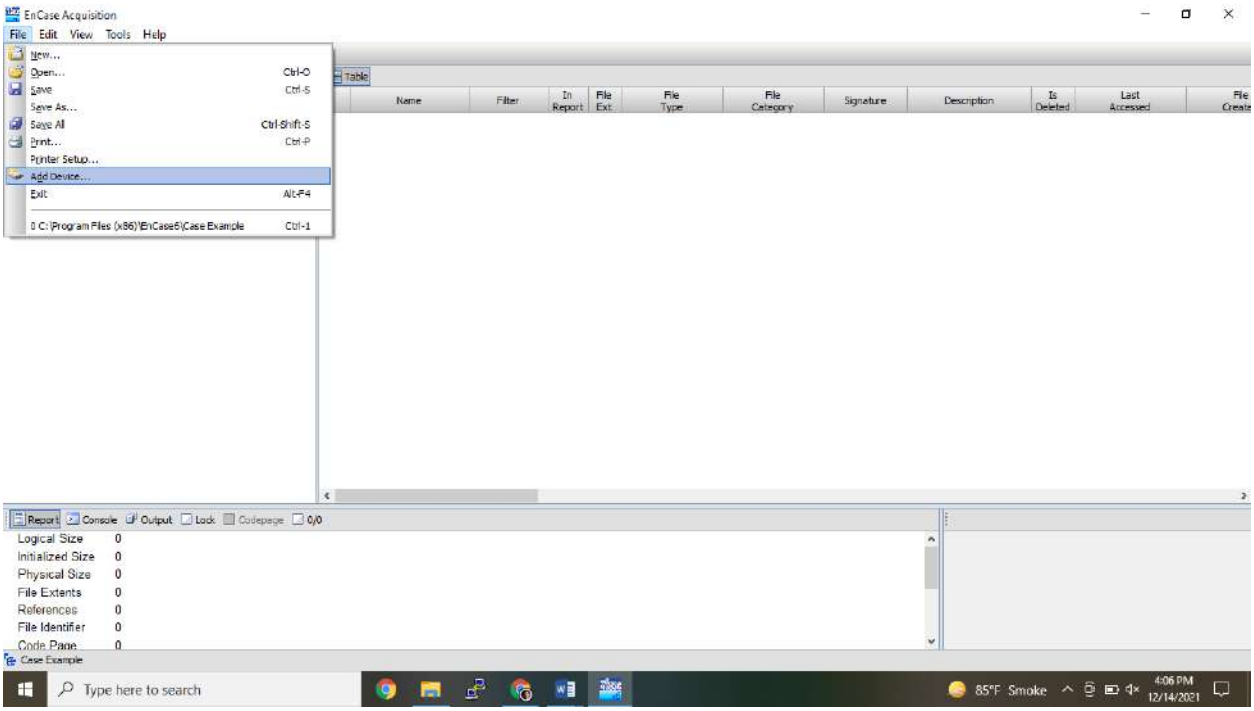
Creating a new Case and Adding Evidence in Encase

Click on New – Case – Fill details as required.





To Add Evidence – Click on File – Add device

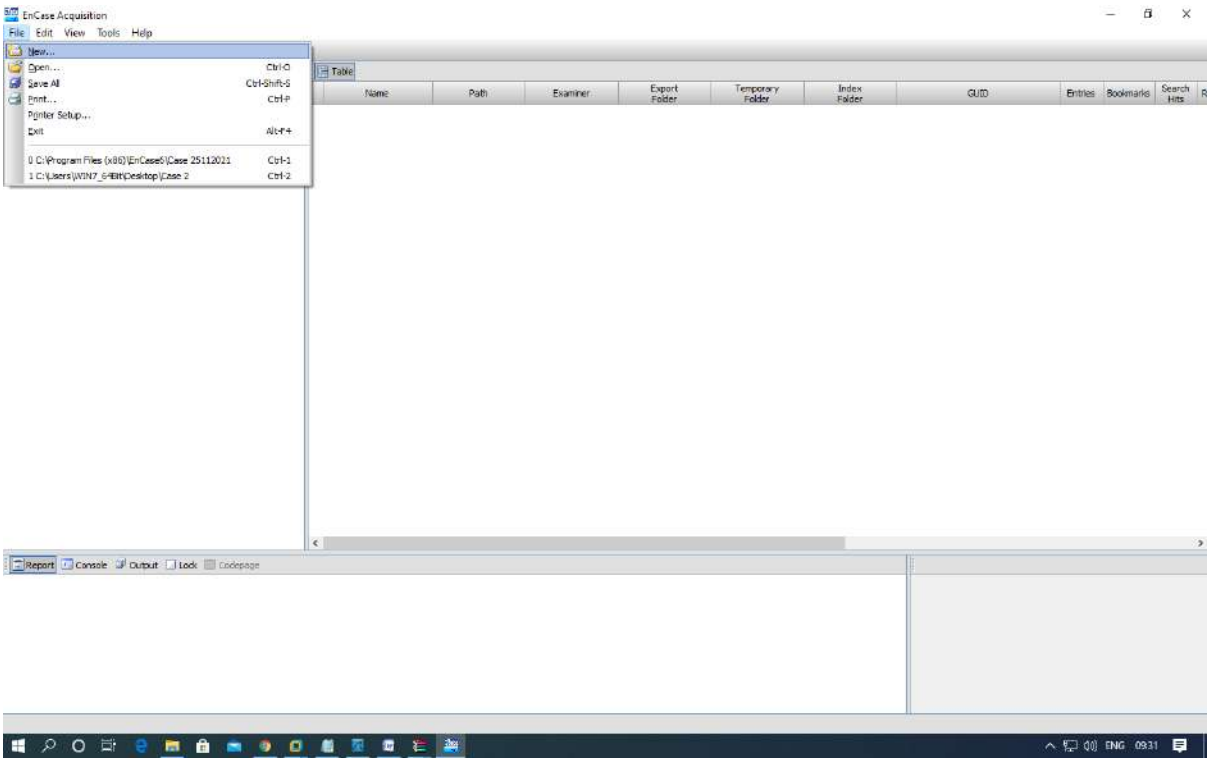


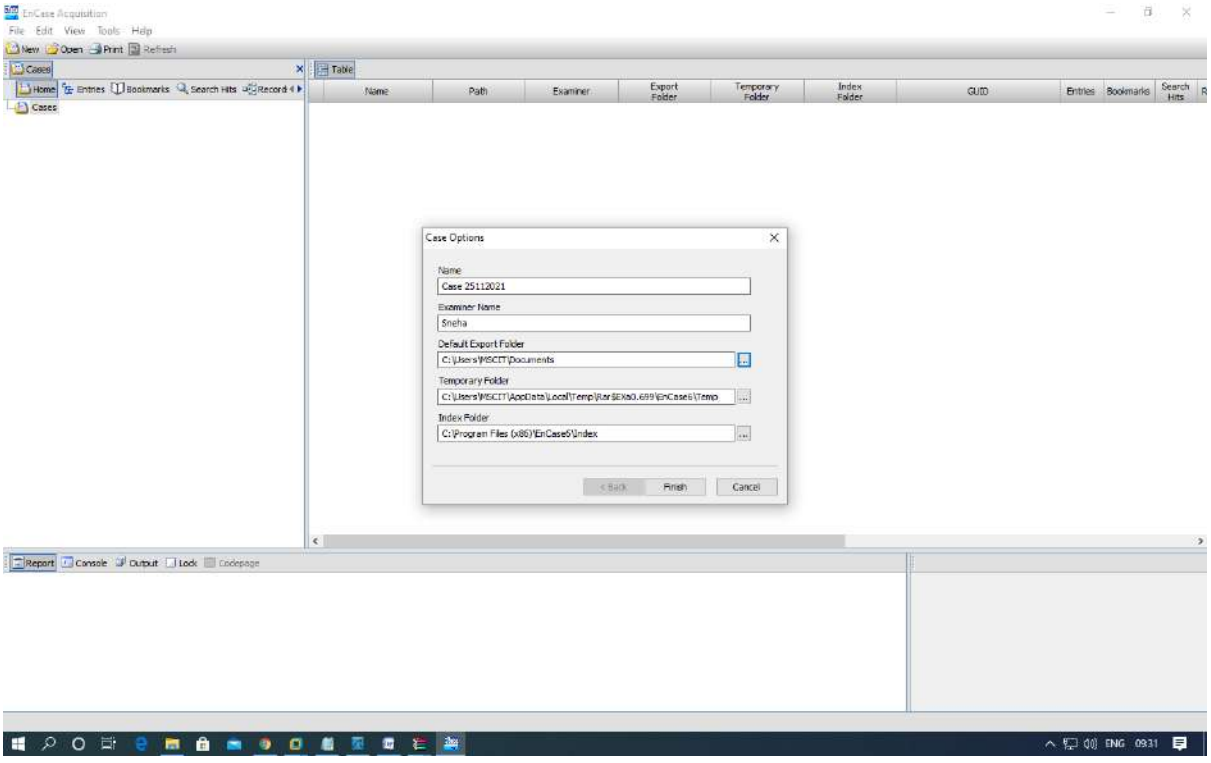
Select whichever device you want to add which contains your evidence.

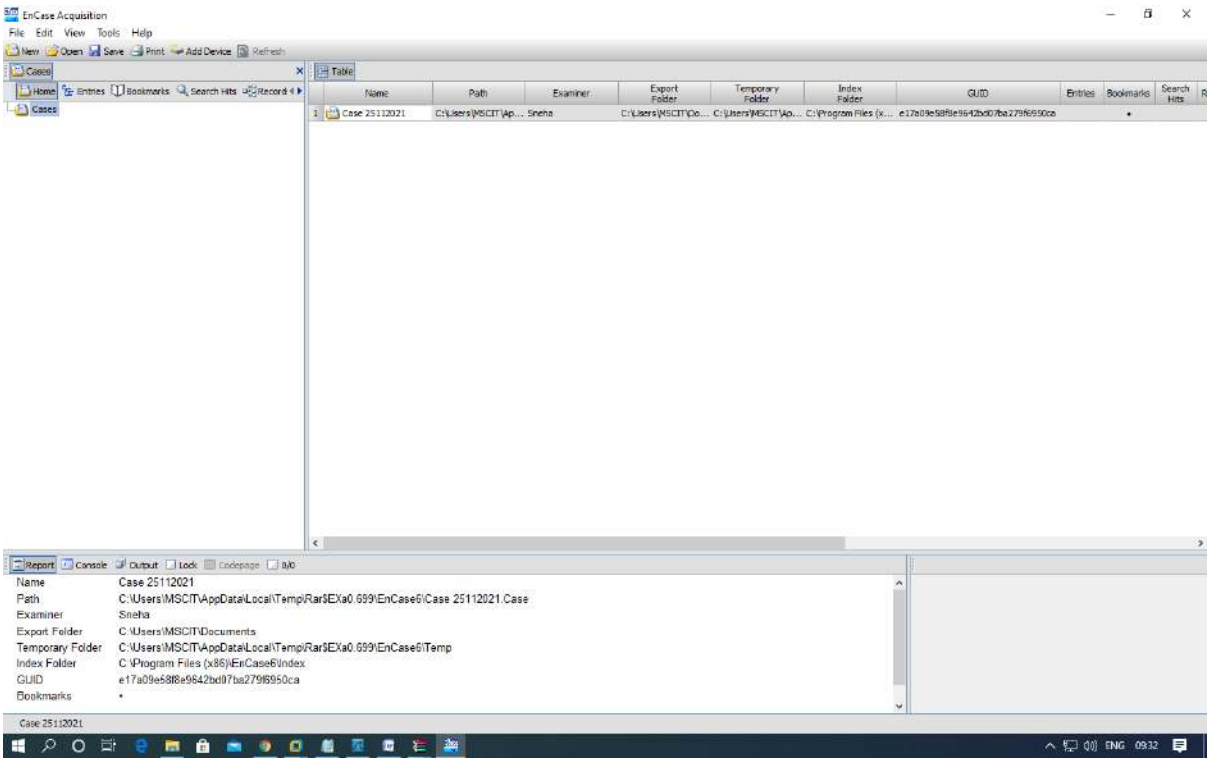
Here I have selected Hard Disk drive.

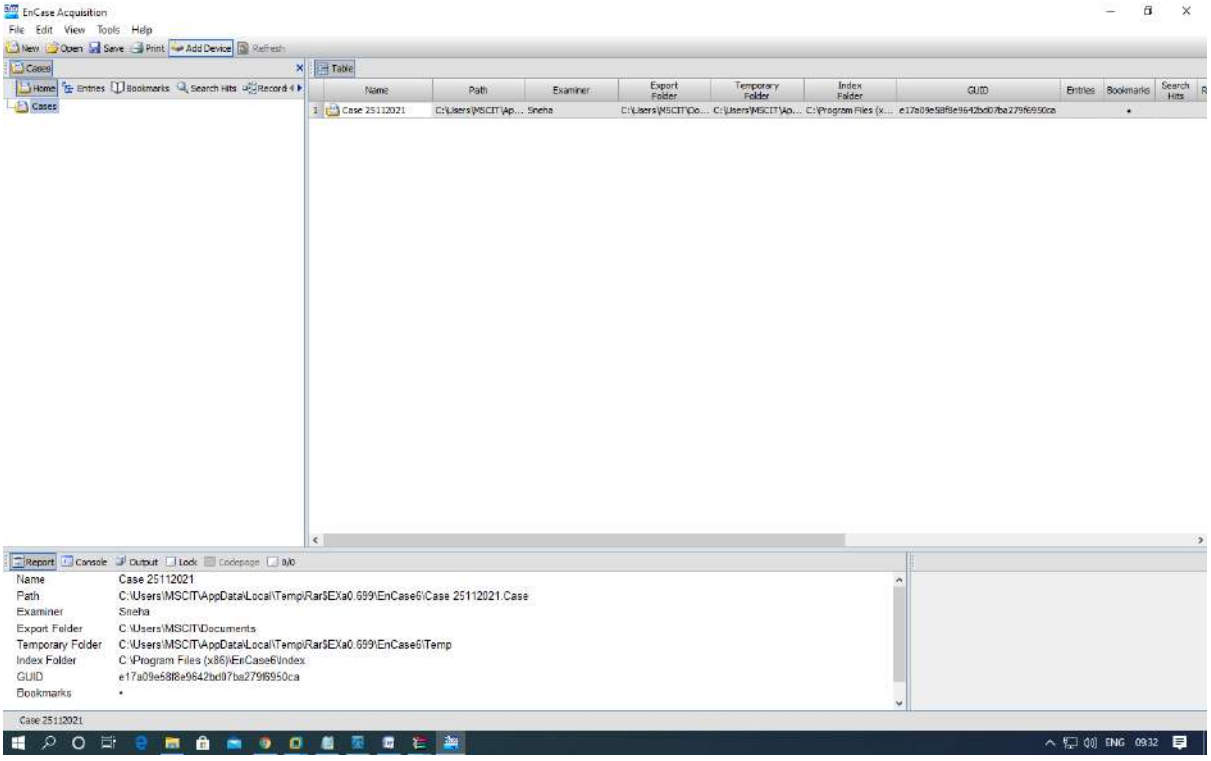
You can also select Palm Pilot and Network crossover.

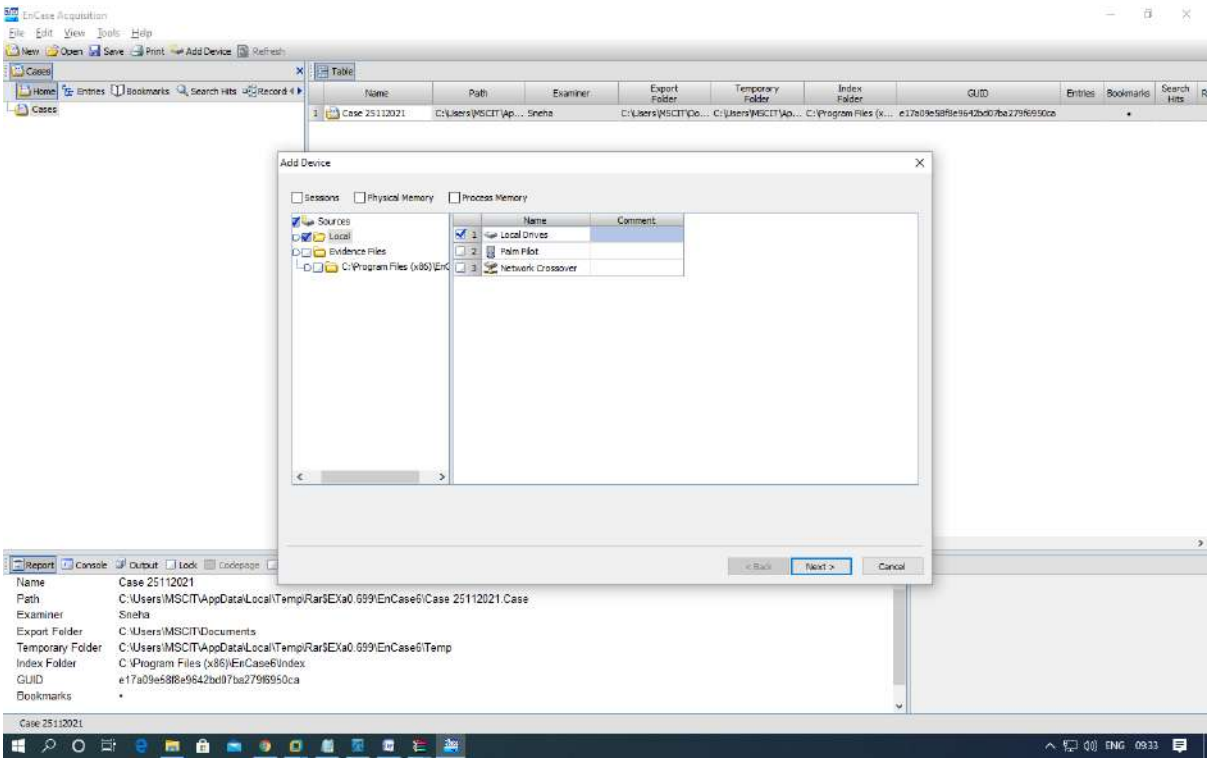
Palm Pilot: - By using the Palm Pilot the user could keep notes, manage contacts, play games, and view and manage other documents. The palm pilot receives input by means of a stylus. Users holds the stylus like a pen, tapping the screen with the tip to interact with buttons and menus.

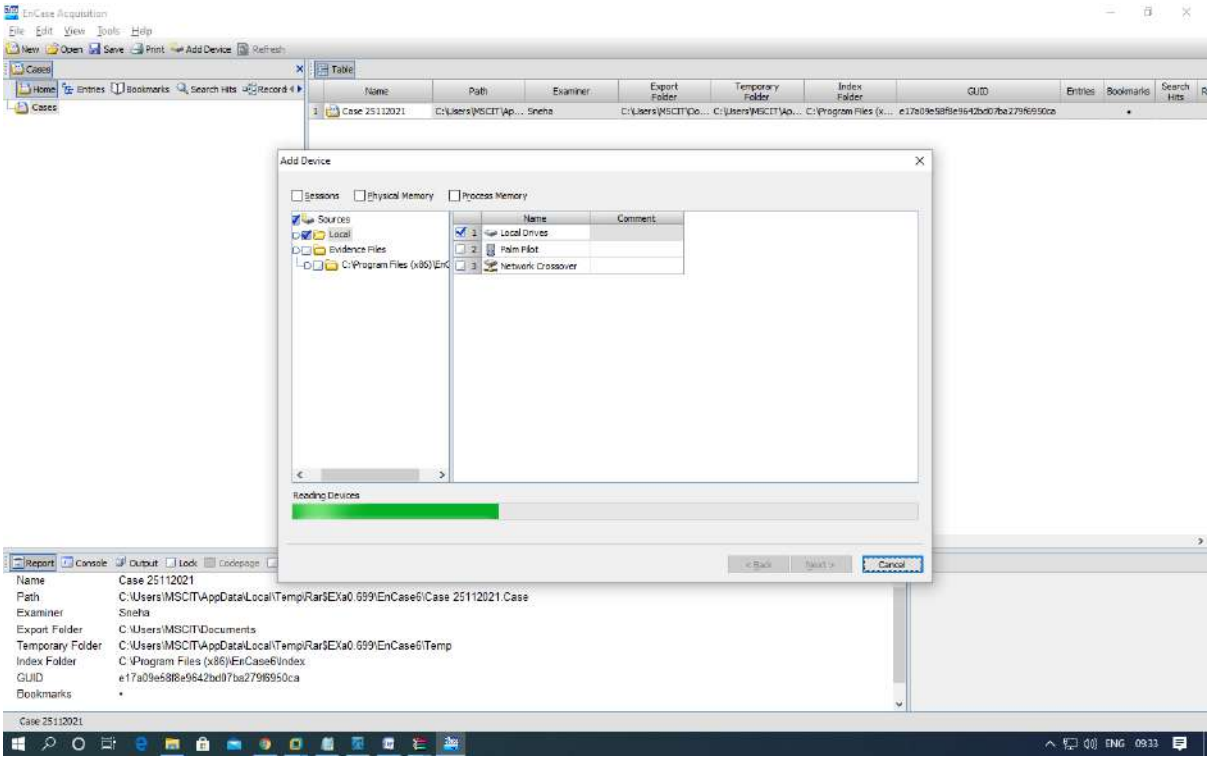

EnCase Acquisition
File Edit View Tools Help
New...
Open... Ctrl-O
Save All Ctrl-Shift-S
Print... Ctrl-P
Printer Setup...
Exit Alt-F4
0 C:\Program Files (x86)\EnCase5\Case 25112021 Ctrl-1
1 C:\Users\WIN7_64Bit\Desktop\Case 2 Ctrl-2
Table
Name
Path
Examiner
Export Folder
Temporary Folder
Index Folder
GUID
Entries
Bookmarks
Search Hits
Report
Console
Output
Lock
Codepage
ENG
09:31

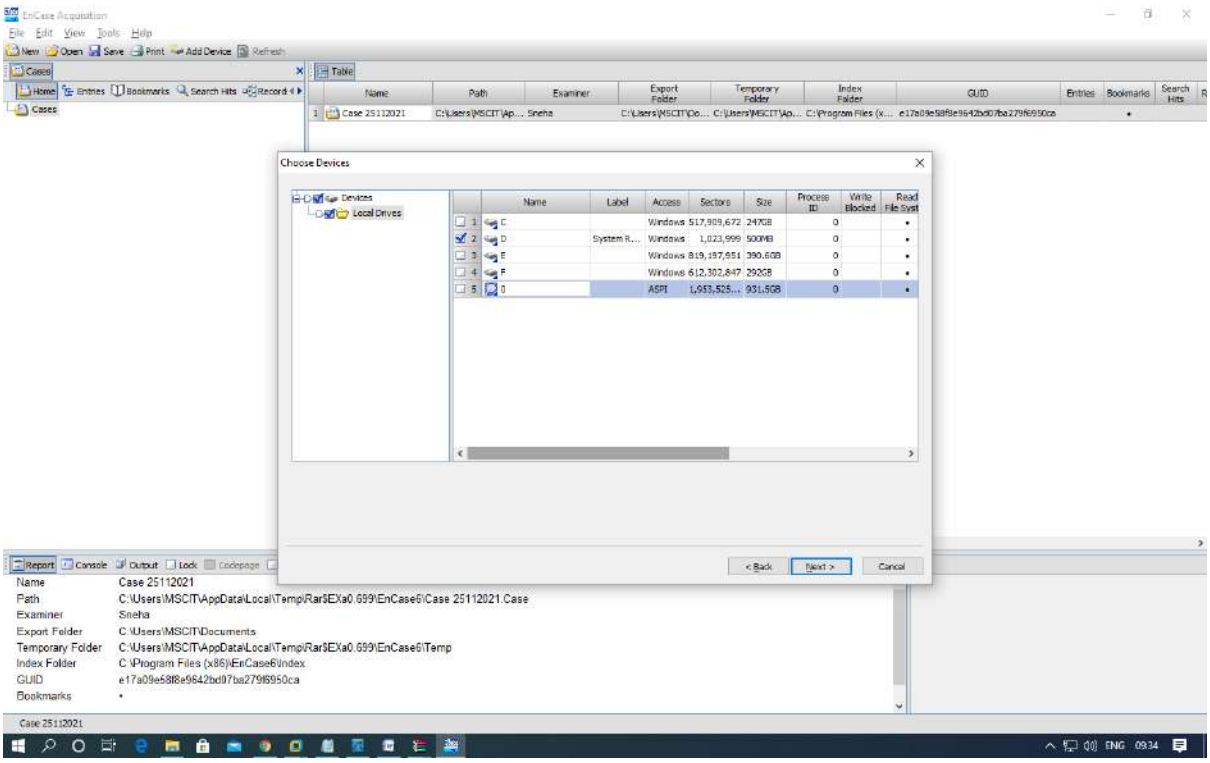

EnCase Acquisition
File Edit View Tools Help
New
Open
Print
Refresh
Cases
Home
Entries
Bookmarks
Search Hits
Record
Table
Name
Path
Examiner
Export Folder
Temporary Folder
Index Folder
GUID
Entries
Bookmarks
Search Hits
Case Options
Name
Case 25112021
Examiner Name
Sneha
Default Export Folder
C:\Users\MSCITT\Documents
Temporary Folder
C:\Users\MSCITT\AppData\Local\Temp\Rar$EXa0.699\EnCase5\Temp
Index Folder
C:\Program Files (x86)\EnCase5\Index
< Back
Finish
Cancel
Report
Console
Output
Lock
Codepage
ENG
09:31

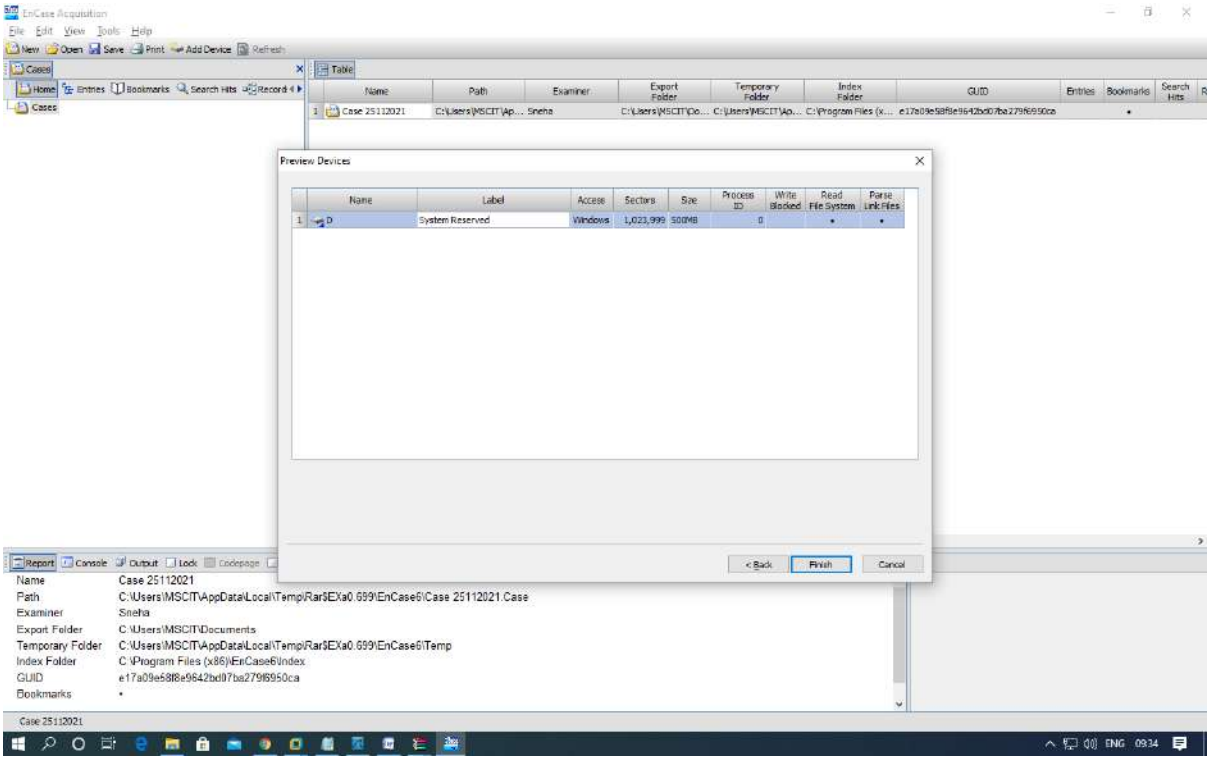

EnCase Acquisition
File Edit View Tools Help
New Open Save Print Add Device Refresh
Cases
Table
Name Path Examiner Export Folder Temporary Folder Index Folder GUID Entries Bookmarks Search Hits
1 Case 25112021 C:\Users\MSCIT\Ap... Sneha C:\Users\MSCIT\Do... C:\Users\MSCIT\Ap... C:\Program Files (x... e17a09e58f8e9642bd07ba279f6950ca
Report Console Output Lock Codepage 0/0
Name Case 25112021
Path C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.699\EnCase6\Case 25112021.Case
Examiner Sneha
Export Folder C:\Users\MSCIT\Documents
Temporary Folder C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.699\EnCase6\Temp
Index Folder C:\Program Files (x86)\EnCase6\Index
GUID e17a09e58f8e9642bd07ba279f6950ca
Bookmarks *
Case 25112021
ENG 09:32

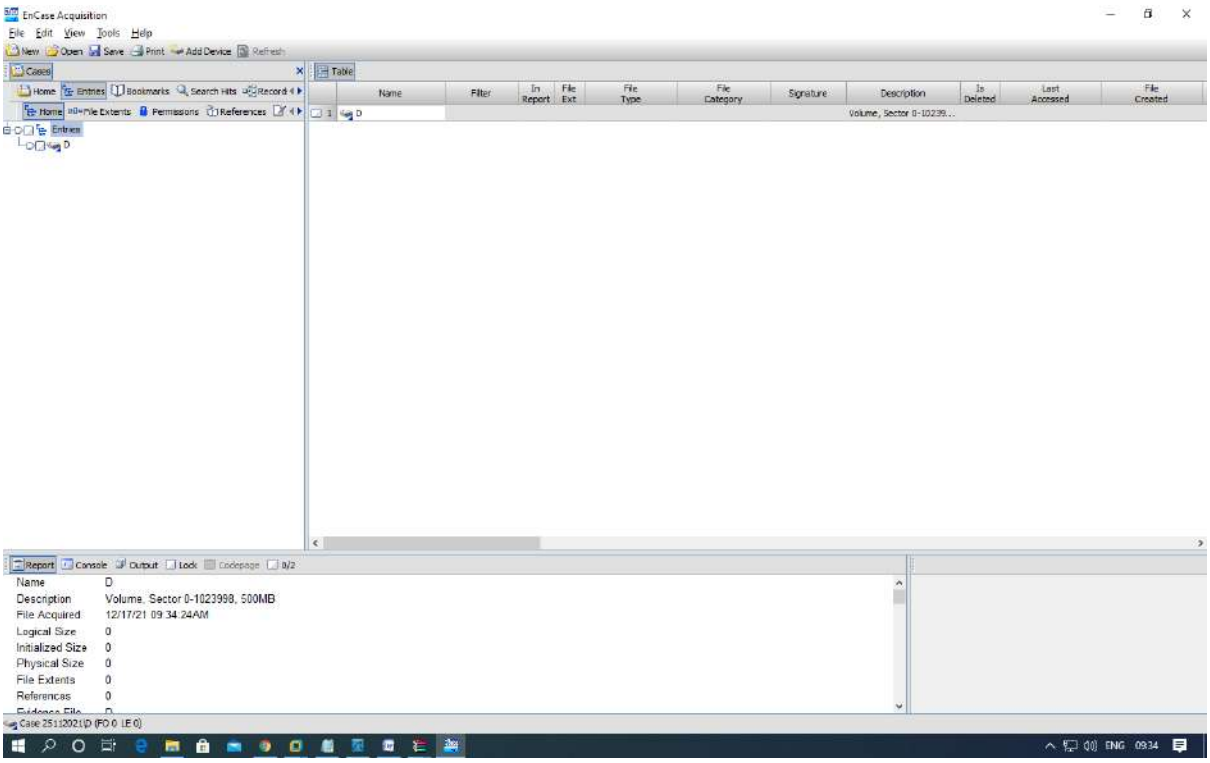

EnCase Acquisition
File Edit View Tools Help
New Open Save Print Add Device Refresh
Cases
Table
Name Path Examiner Export Folder Temporary Folder Index Folder GUID Entries Bookmarks Search Hits
1 Case 25112021 C:\Users\MSCIT\Ap... Sneha C:\Users\MSCIT\Do... C:\Users\MSCIT\Ap... C:\Program Files (x... e17a09e58f8e9642bd07ba279f6950ca
Report Console Output Lock Codepage 0/0
Name Case 25112021
Path C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.699\EnCase6\Case 25112021.Case
Examiner Sneha
Export Folder C:\Users\MSCIT\Documents
Temporary Folder C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.699\EnCase6\Temp
Index Folder C:\Program Files (x86)\EnCase6\Index
GUID e17a09e58f8e9642bd07ba279f6950ca
Bookmarks *
Case 25112021
ENG 09:32

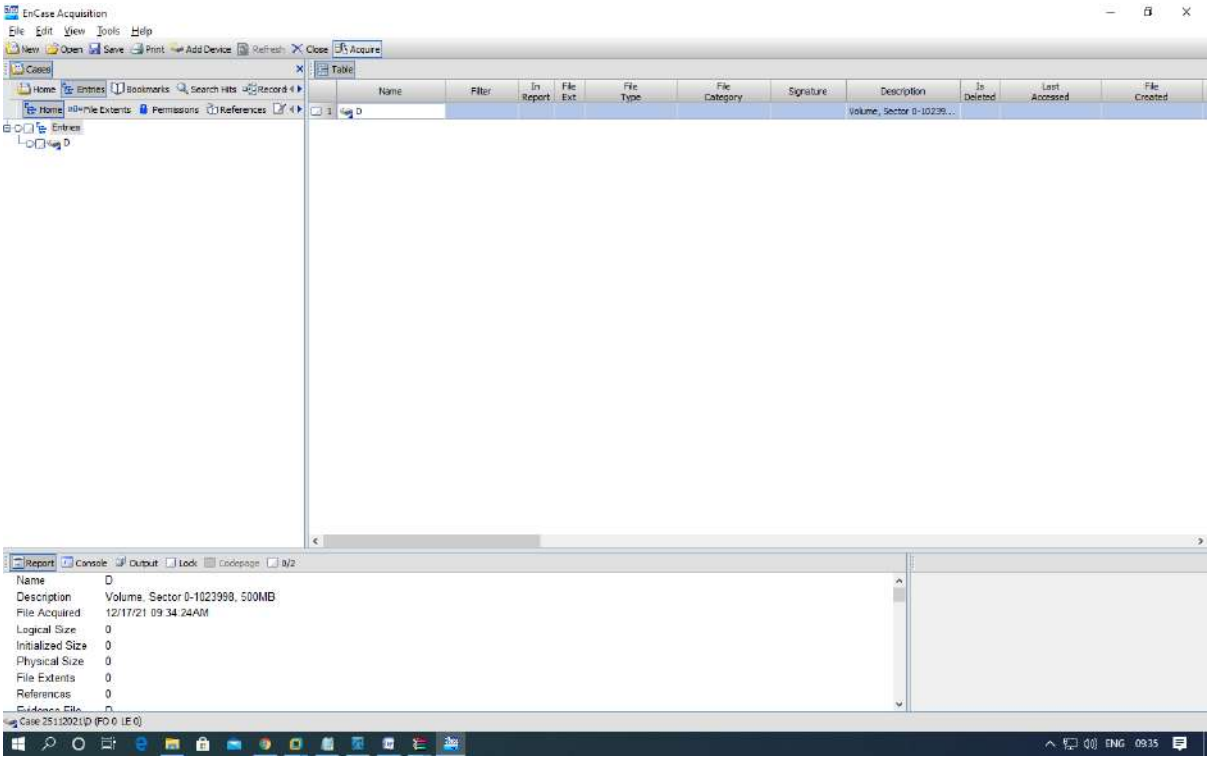

Add Device
Sessions
Physical Memory
Process Memory
Sources
Local
Evidence Files
Name
Comment
Local Drives
Palm Pilot
Network Crossover
Next >
Cancel
Name Case 25112021
Path C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.699\EnCase6\Case 25112021.Case
Examiner Sneha
Export Folder C:\Users\MSCIT\Documents
Temporary Folder C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.699\EnCase6\Temp
Index Folder C:\Program Files (x86)\EnCase6\Index
GUID e17a09e58f8e9642bd07ba279f6950ca
Bookmarks

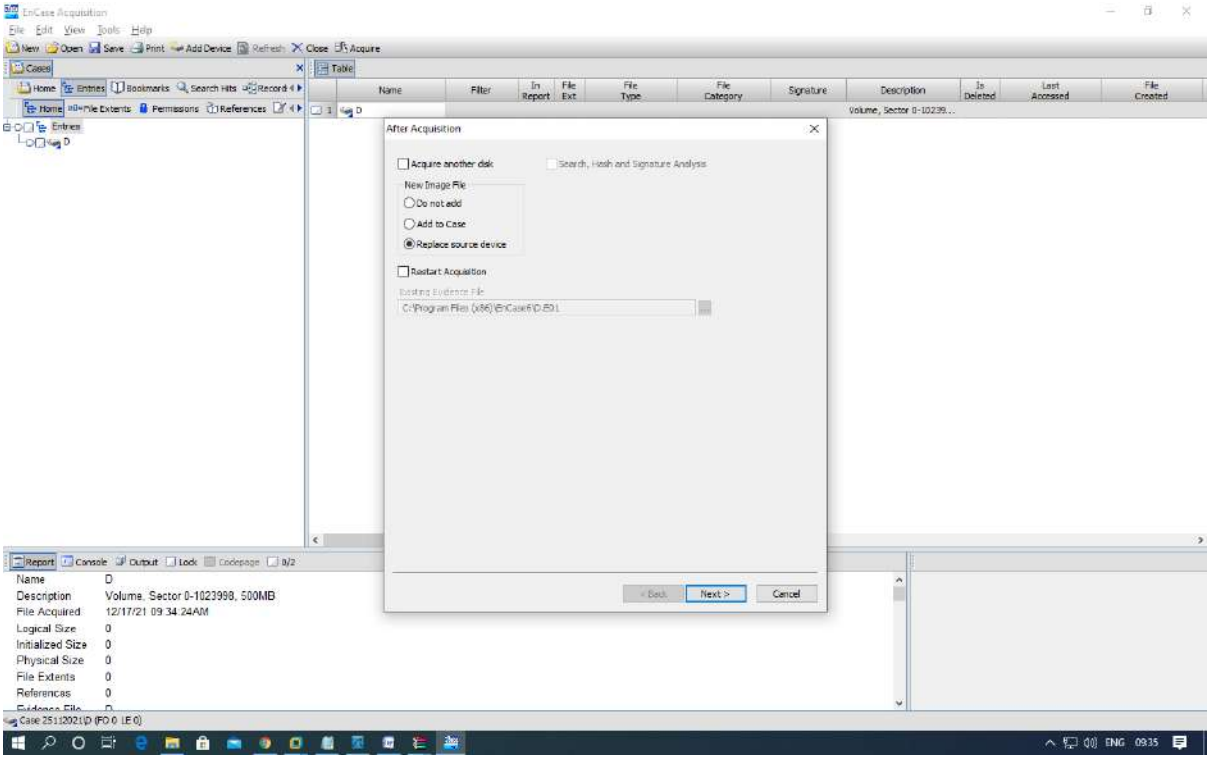

Add Device
Sessions
Physical Memory
Process Memory
Sources
Local
Evidence Files
Name
Comment
Local Drives
Palm Pilot
Network Crossover
Reading Devices
Cancel
Name Case 25112021
Path C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.699\EnCase6\Case 25112021.Case
Examiner Sneha
Export Folder C:\Users\MSCIT\Documents
Temporary Folder C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.699\EnCase6\Temp
Index Folder C:\Program Files (x86)\EnCase6\Index
GUID e17a09e58f8e9642bd07ba279f6950ca
Bookmarks

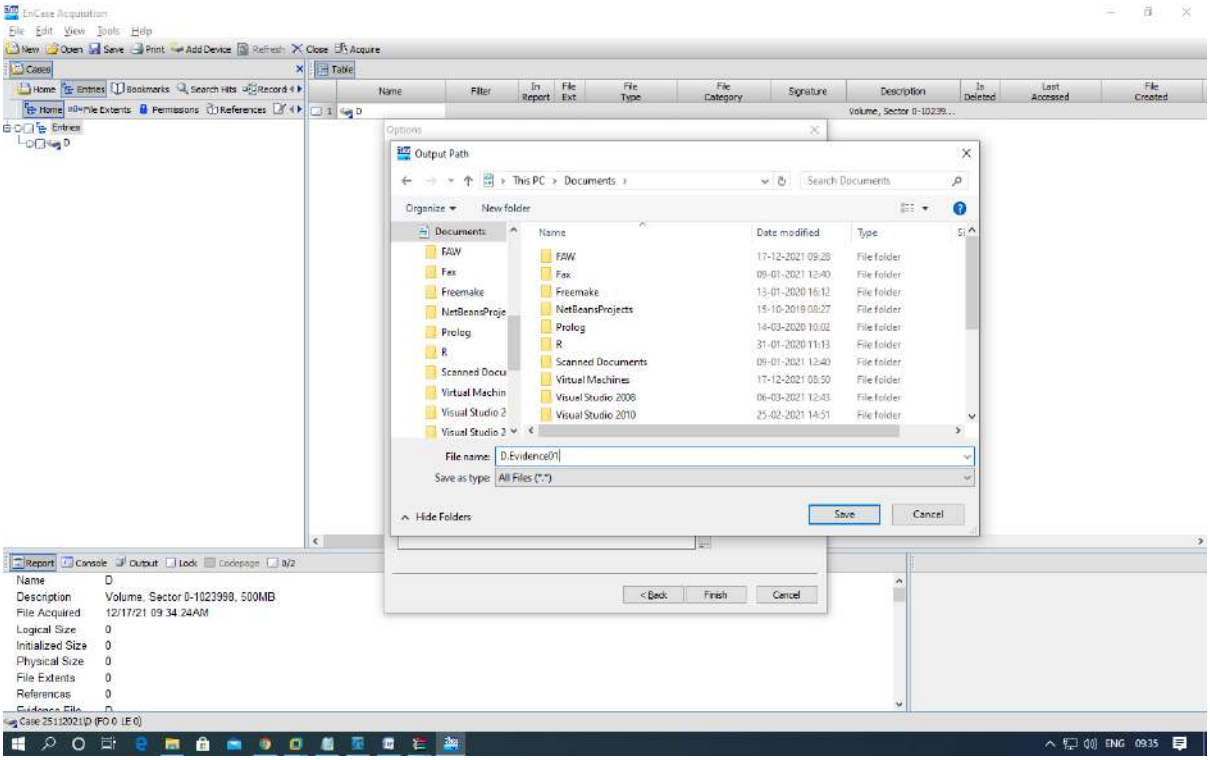

Choose Devices
Devices
Local Drives
Name
Label
Access
Sectors
Size
Process ID
Write Blocked
Read File Syst
C
Windows 517,909,672 247GB 0
D
System R...
Windows 1,023,999 500MB 0
E
Windows 819,197,951 390.6GB 0
F
Windows 612,302,847 292GB 0
0
ASPI 1,953,525... 931.5GB 0
< Back
Next >
Cancel
Name Case 25112021
Path C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.699\EnCase6\Case 25112021.Case
Examiner Sneha
Export Folder C:\Users\MSCIT\Documents
Temporary Folder C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.699\EnCase6\Temp
Index Folder C:\Program Files (x86)\EnCase6\Index
GUID e17a09e58f8e9642bd07ba279f6950ca
Bookmarks
Case 25112021

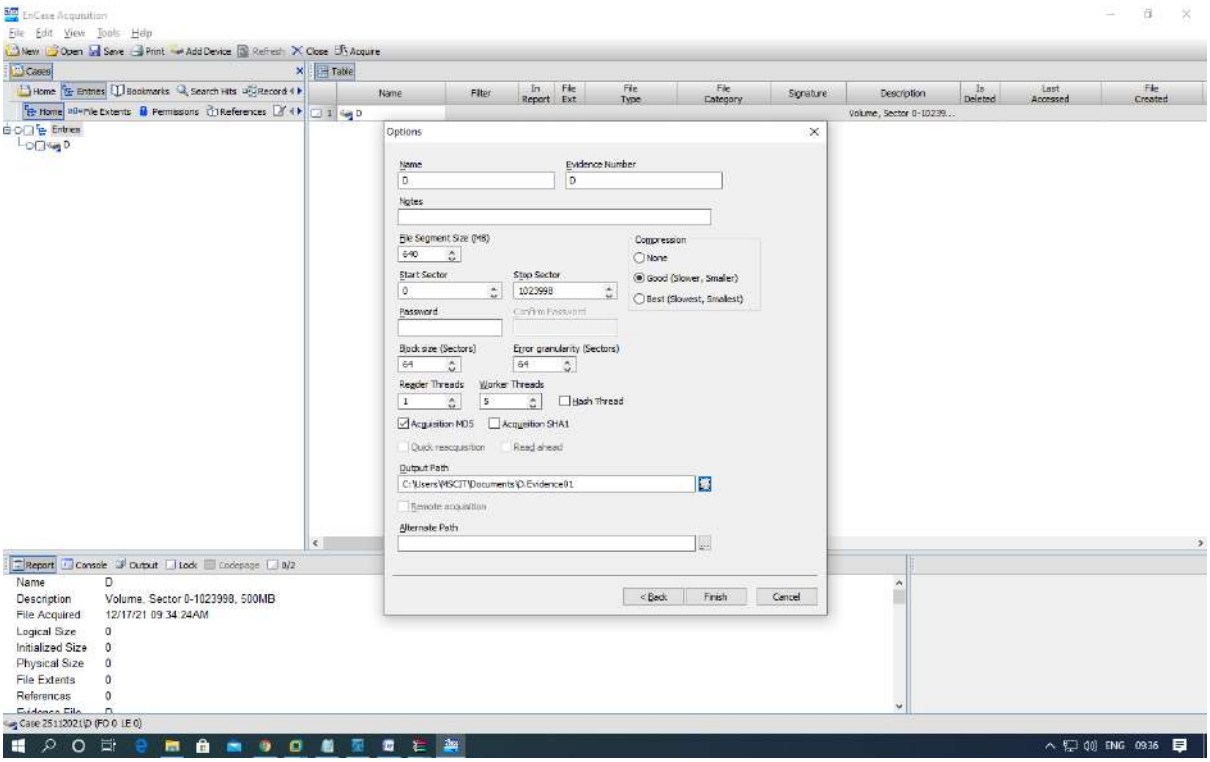

Preview Devices
Name
Label
Access
Sectors
Size
Process ID
Write Blocked
Read File System
Parse Link Files
D
System Reserved
Windows
1,023,999
500MB
0
< Back
Finish
Cancel
Name Case 25112021
Path C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.699\EnCase6\Case 25112021.Case
Examiner Sneha
Export Folder C:\Users\MSCIT\Documents
Temporary Folder C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.699\EnCase6\Temp
Index Folder C:\Program Files (x86)\EnCase6\Index
GUID e17a09e58f8e9642bd07ba279f6950ca
Bookmarks
Case 25112021

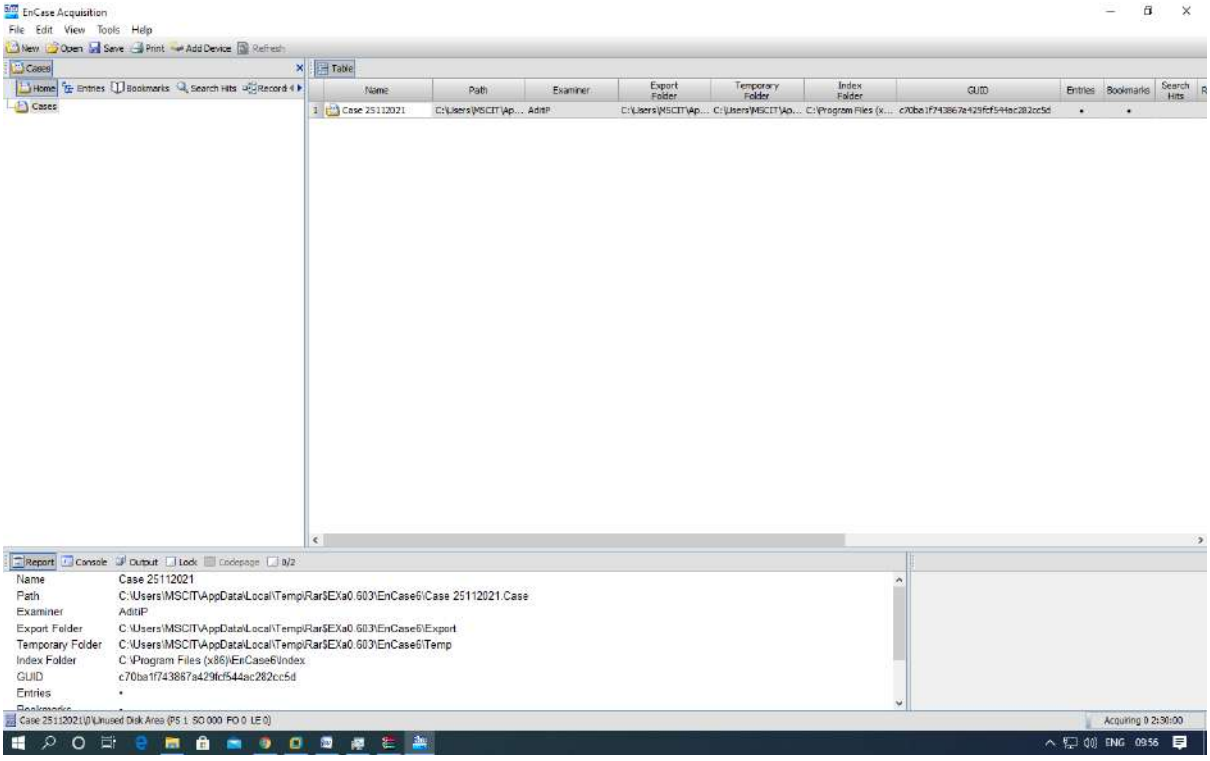

EnCase Acquisition
File Edit View Tools Help
New Open Save Print Add Device Refresh
Cases
Table
Name Filter In Report File Ext File Type File Category Signature Description Is Deleted Last Accessed File Created
Home Entries Bookmarks Search Hits Record
Home File Extents Permissions References
Entries
D
Volume, Sector 0-10239...
Report Console Output Lock Codepage 8/2
Name D
Description Volume, Sector 0-1023998, 500MB
File Acquired 12/17/21 09:34:24AM
Logical Size 0
Initialized Size 0
Physical Size 0
File Extents 0
References 0
Case 25112021(D (FO 0 LE 0)
ENG 09:34

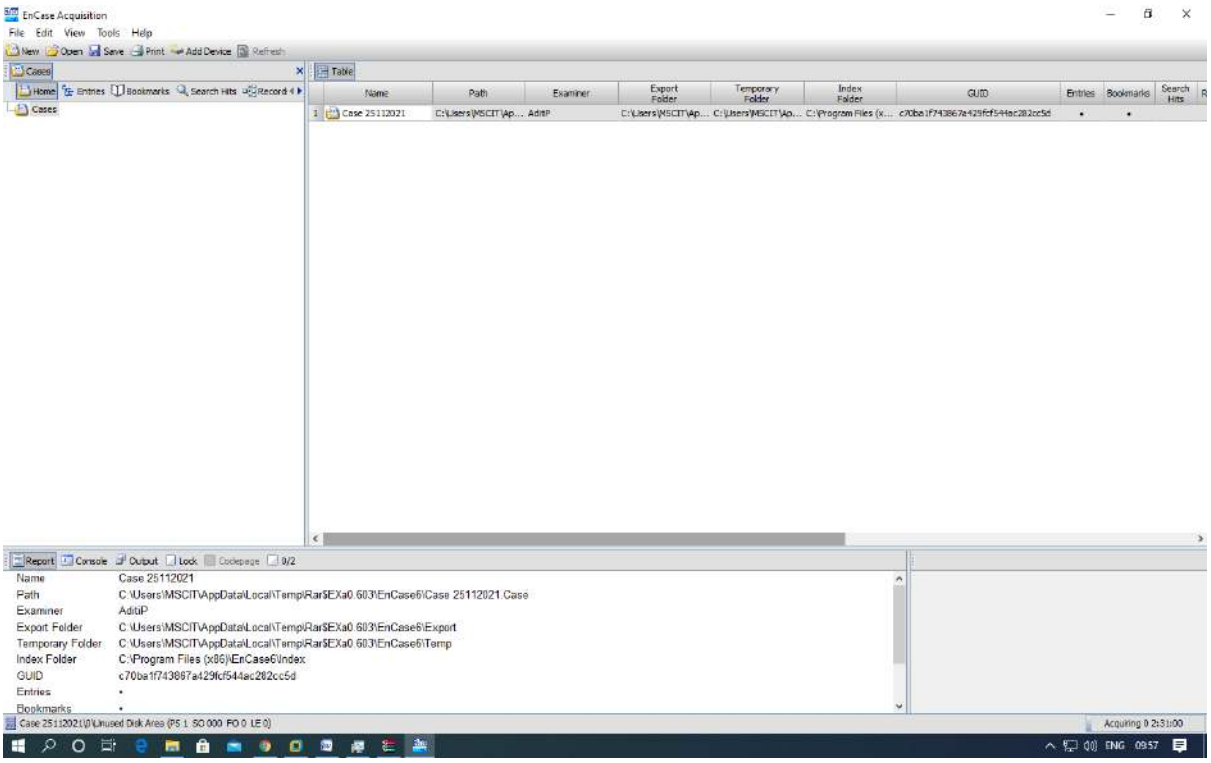

EnCase Acquisition
File Edit View Tools Help
New Open Save Print Add Device Refresh Close Acquire
Cases
Table
Name Filter In Report File Ext File Type File Category Signature Description Is Deleted Last Accessed File Created
Home Entries Bookmarks Search Hits Record
Home File Extents Permissions References
Entries
D
Volume, Sector 0-10239...
Report Console Output Lock Codepage 8/2
Name D
Description Volume, Sector 0-1023998, 500MB
File Acquired 12/17/21 09:34:24AM
Logical Size 0
Initialized Size 0
Physical Size 0
File Extents 0
References 0
Case 25112021(D (FO 0 LE 0)
ENG 09:35

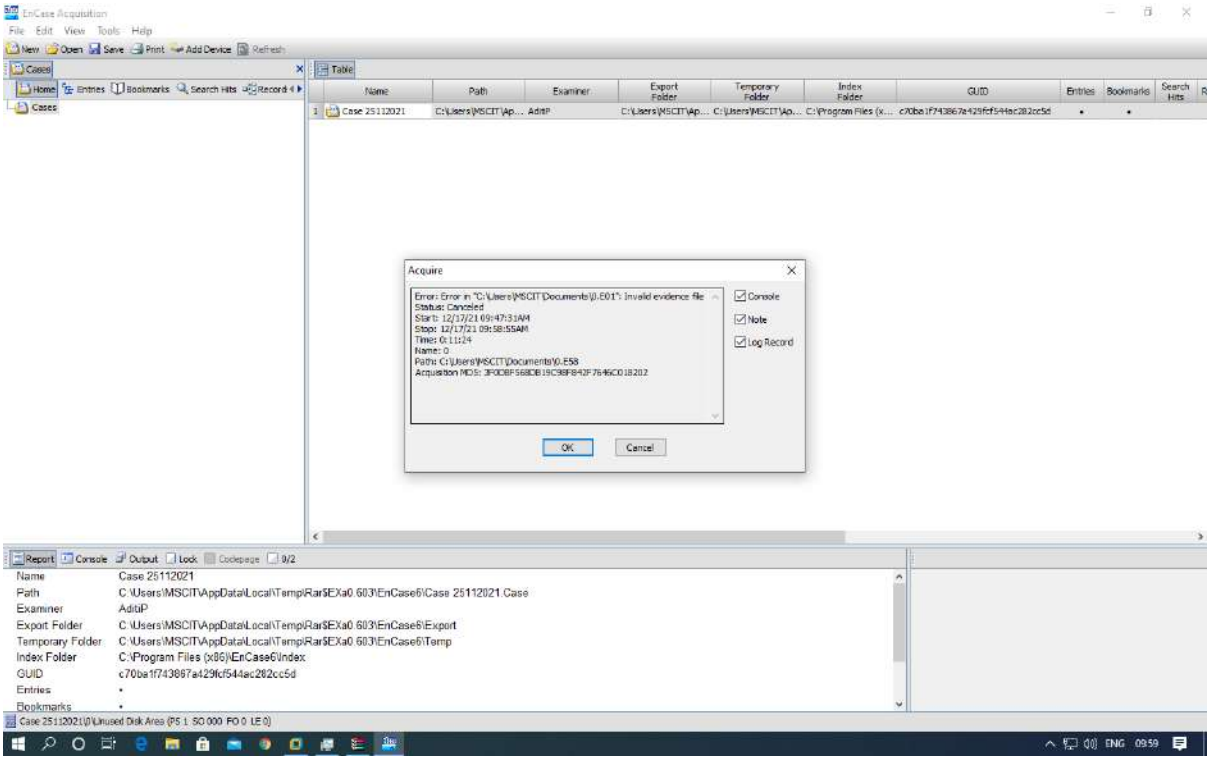

After Acquisition
Acquire another disk
Search, Hash and Signature Analysis
New Image File
Do not add
Add to Case
Replace source device
Restart Acquisition
Existing Evidence File
C:\Program Files (x86)\EnCase6\D.E01
< Back
Next >
Cancel
Name D
Description Volume, Sector 0-1023998, 500MB
File Acquired 12/17/21 09:34:24AM
Logical Size 0
Initialized Size 0
Physical Size 0
File Extents 0
References 0

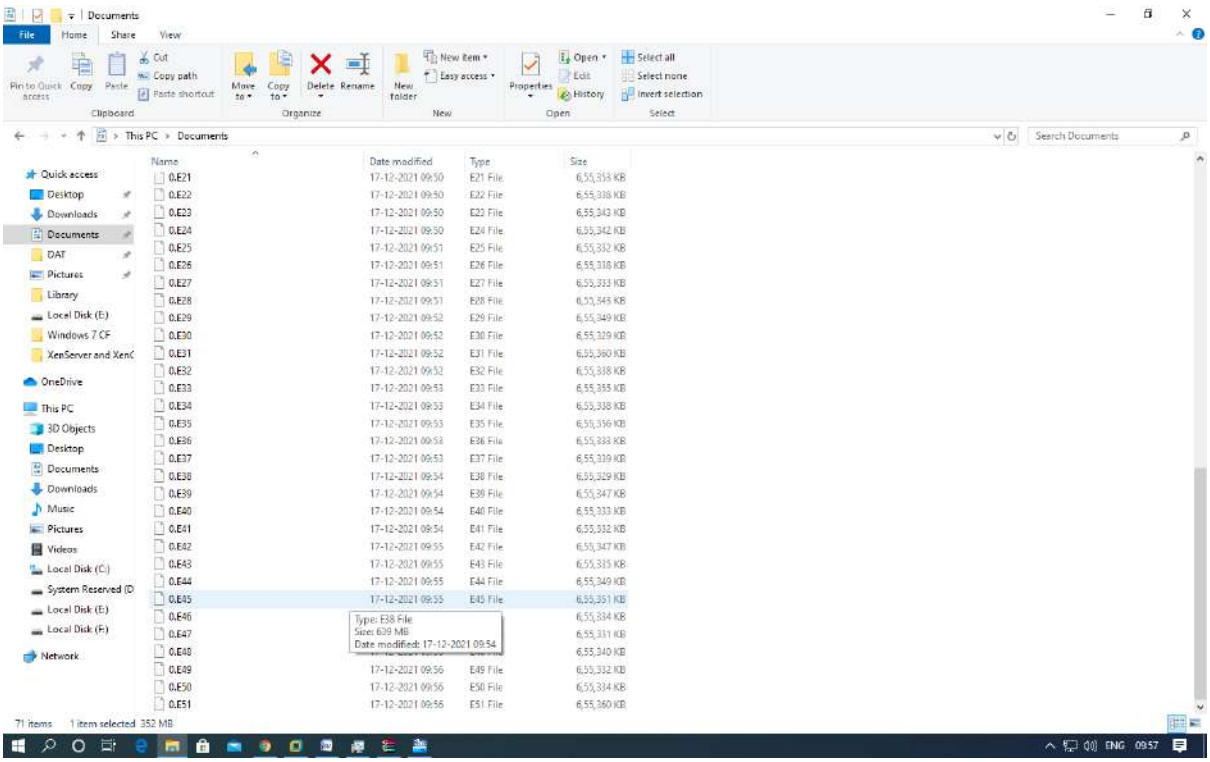

Output Path
This PC › Documents ›
Search Documents
Organize
New folder
Documents
Name
Date modified
Type
FAW
Fax
Freemake
NetBeansProjects
Prolog
R
Scanned Documents
Virtual Machines
Visual Studio 2008
Visual Studio 2010
File name: D.Evidence01
Save as type: All Files (*.*)
Hide Folders
Save
Cancel
< Back
Finish
Cancel
Name D
Description Volume, Sector 0-1023998, 500MB
File Acquired 12/17/21 09:34:24AM
Logical Size 0
Initialized Size 0
Physical Size 0
File Extents 0
References 0


EnCase Acquisition
File Edit View Tools Help
New Open Save Print Add Device Refresh Close Acquire
Cases
Home Entries Bookmarks Search Hits Record
Home File Extents Permissions References
Entries
D
Table
Name Filter In Report File Ext File Type File Category Signature Description Is Deleted Last Accessed File Created
1 D
Volume, Sector 0-10239...
Options
Name
D
Evidence Number
D
Notes
File Segment Size (MB)
640
Compression
None
Good (Slower, Smaller)
Best (Slowest, Smallest)
Start Sector
0
Stop Sector
1023998
Password
Confirm Password
Block size (Sectors)
64
Error granularity (Sectors)
64
Reader Threads
1
Worker Threads
5
Hash Thread
Acquisition MD5
Acquisition SHA1
Quick reacquisition
Read ahead
Output Path
C:\Users\MSCIT\Documents\D.Evidence01
Remote acquisition
Alternate Path
< Back
Finish
Cancel
Report Console Output Lock Codepage 0/2
Name D
Description Volume, Sector 0-1023998, 500MB
File Acquired 12/17/21 09:34:24AM
Logical Size 0
Initialized Size 0
Physical Size 0
File Extents 0
References 0
Case 25112021\D (FO 0 LE 0)
ENG 09:36


EnCase Acquisition
File Edit View Tools Help
New Open Save Print Add Device Refresh
Cases
Home Entries Bookmarks Search Hits Record
Cases
Table
Name Path Examiner Export Folder Temporary Folder Index Folder GUID Entries Bookmarks Search Hits
1 Case 25112021 C:\Users\MSCIT\Ap... AditIP C:\Users\MSCIT\Ap... C:\Users\MSCIT\Ap... C:\Program Files (x... c70ba1f743867a429fcf544ac282cc5d
Report Console Output Lock Codepage 0/2
Name Case 25112021
Path C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.603\EnCase6\Case 25112021.Case
Examiner AditIP
Export Folder C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.603\EnCase6\Export
Temporary Folder C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.603\EnCase6\Temp
Index Folder C:\Program Files (x86)\EnCase6\Index
GUID c70ba1f743867a429fcf544ac282cc5d
Entries 1
Case 25112021\0\Unused Disk Area (P5 1 SO 000 FO 0 LE 0)
Acquiring 0 2:30:00
ENG 09:56


EnCase Acquisition
File Edit View Tools Help
New Open Save Print Add Device Refresh
Cases
Home Entries Bookmarks Search Hits Record
Cases
Table
Name Path Examiner Export Folder Temporary Folder Index Folder GUID Entries Bookmarks Search Hits
1 Case 25112021 C:\Users\MSCIT\Ap... AditiP C:\Users\MSCIT\Ap... C:\Users\MSCIT\Ap... C:\Program Files (x... c70ba1f743867a429fcf544ac282cc5d
Report Console Output Lock Codepage 0/2
Name Case 25112021
Path C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.603\EnCase6\Case 25112021.Case
Examiner AditiP
Export Folder C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.603\EnCase6\Export
Temporary Folder C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.603\EnCase6\Temp
Index Folder C:\Program Files (x86)\EnCase6\Index
GUID c70ba1f743867a429fcf544ac282cc5d
Entries
Bookmarks
Case 25112021\0\Unused Disk Area (PS 1 SO 000 FO 0 LE 0)
Acquiring 0 2:31:00
ENG 09:57


EnCase Acquisition
File Edit View Tools Help
New Open Save Print Add Device Refresh
Cases
Home Entries Bookmarks Search Hits Record
Cases
Table
Name Path Examiner Export Folder Temporary Folder Index Folder GUID Entries Bookmarks Search Hits
1 Case 25112021 C:\Users\MSCIT\Ap... AditiP C:\Users\MSCIT\Ap... C:\Users\MSCIT\Ap... C:\Program Files (x... c70ba1f743867a429fcf544ac282cc5d
Acquire
Error: Error in "C:\Users\MSCIT\Documents\0.E01": Invalid evidence file
Status: Canceled
Start: 12/17/21 09:47:31AM
Stop: 12/17/21 09:58:55AM
Time: 0:11:24
Name: 0
Path: C:\Users\MSCIT\Documents\0.E58
Acquisition MD5: 3F0DBF568DB19C98F842F7646C01B202
Console
Note
Log Record
OK
Cancel
Report Console Output Lock Codepage 0/2
Name Case 25112021
Path C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.603\EnCase6\Case 25112021.Case
Examiner AditiP
Export Folder C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.603\EnCase6\Export
Temporary Folder C:\Users\MSCIT\AppData\Local\Temp\Rar$EXa0.603\EnCase6\Temp
Index Folder C:\Program Files (x86)\EnCase6\Index
GUID c70ba1f743867a429fcf544ac282cc5d
Entries
Bookmarks
Case 25112021\0\Unused Disk Area (PS 1 SO 000 FO 0 LE 0)
ENG 09:59


Documents
File
Home
Share
View
Cut
Copy path
Paste shortcut
Pin to Quick access
Copy
Paste
Move to
Copy to
Delete
Rename
New folder
New item
Easy access
Properties
Open
Edit
History
Select all
Select none
Invert selection
Clipboard
Organize
New
Open
Select
This PC > Documents
Search Documents
Quick access
Desktop
Downloads
Documents
DAT
Pictures
Library
Local Disk (E:)
Windows 7 CF
XenServer and XenC
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
System Reserved (D
Local Disk (E:)
Local Disk (F:)
Network
Name
Date modified
Type
Size
0.E21 17-12-2021 09:50 E21 File 6,55,353 KB
0.E22 17-12-2021 09:50 E22 File 6,55,338 KB
0.E23 17-12-2021 09:50 E23 File 6,55,343 KB
0.E24 17-12-2021 09:50 E24 File 6,55,342 KB
0.E25 17-12-2021 09:51 E25 File 6,55,332 KB
0.E26 17-12-2021 09:51 E26 File 6,55,316 KB
0.E27 17-12-2021 09:51 E27 File 6,55,333 KB
0.E28 17-12-2021 09:51 E28 File 6,55,345 KB
0.E29 17-12-2021 09:52 E29 File 6,55,349 KB
0.E30 17-12-2021 09:52 E30 File 6,55,329 KB
0.E31 17-12-2021 09:52 E31 File 6,55,360 KB
0.E32 17-12-2021 09:52 E32 File 6,55,338 KB
0.E33 17-12-2021 09:53 E33 File 6,55,355 KB
0.E34 17-12-2021 09:53 E34 File 6,55,338 KB
0.E35 17-12-2021 09:53 E35 File 6,55,356 KB
0.E36 17-12-2021 09:53 E36 File 6,55,333 KB
0.E37 17-12-2021 09:53 E37 File 6,55,339 KB
0.E38 17-12-2021 09:54 E38 File 6,55,329 KB
0.E39 17-12-2021 09:54 E39 File 6,55,347 KB
0.E40 17-12-2021 09:54 E40 File 6,55,333 KB
0.E41 17-12-2021 09:54 E41 File 6,55,332 KB
0.E42 17-12-2021 09:55 E42 File 6,55,347 KB
0.E43 17-12-2021 09:55 E43 File 6,55,335 KB
0.E44 17-12-2021 09:55 E44 File 6,55,349 KB
0.E45 17-12-2021 09:55 E45 File 6,55,351 KB
0.E46 6,55,334 KB
0.E47 6,55,331 KB
0.E48 6,55,340 KB
0.E49 17-12-2021 09:56 E49 File 6,55,332 KB
0.E50 17-12-2021 09:56 E50 File 6,55,314 KB
0.E51 17-12-2021 09:56 E51 File 6,55,360 KB
Type: E38 File
Size: 639 MB
Date modified: 17-12-2021 09:54
71 items
1 item selected 352 MB
ENG
09:57