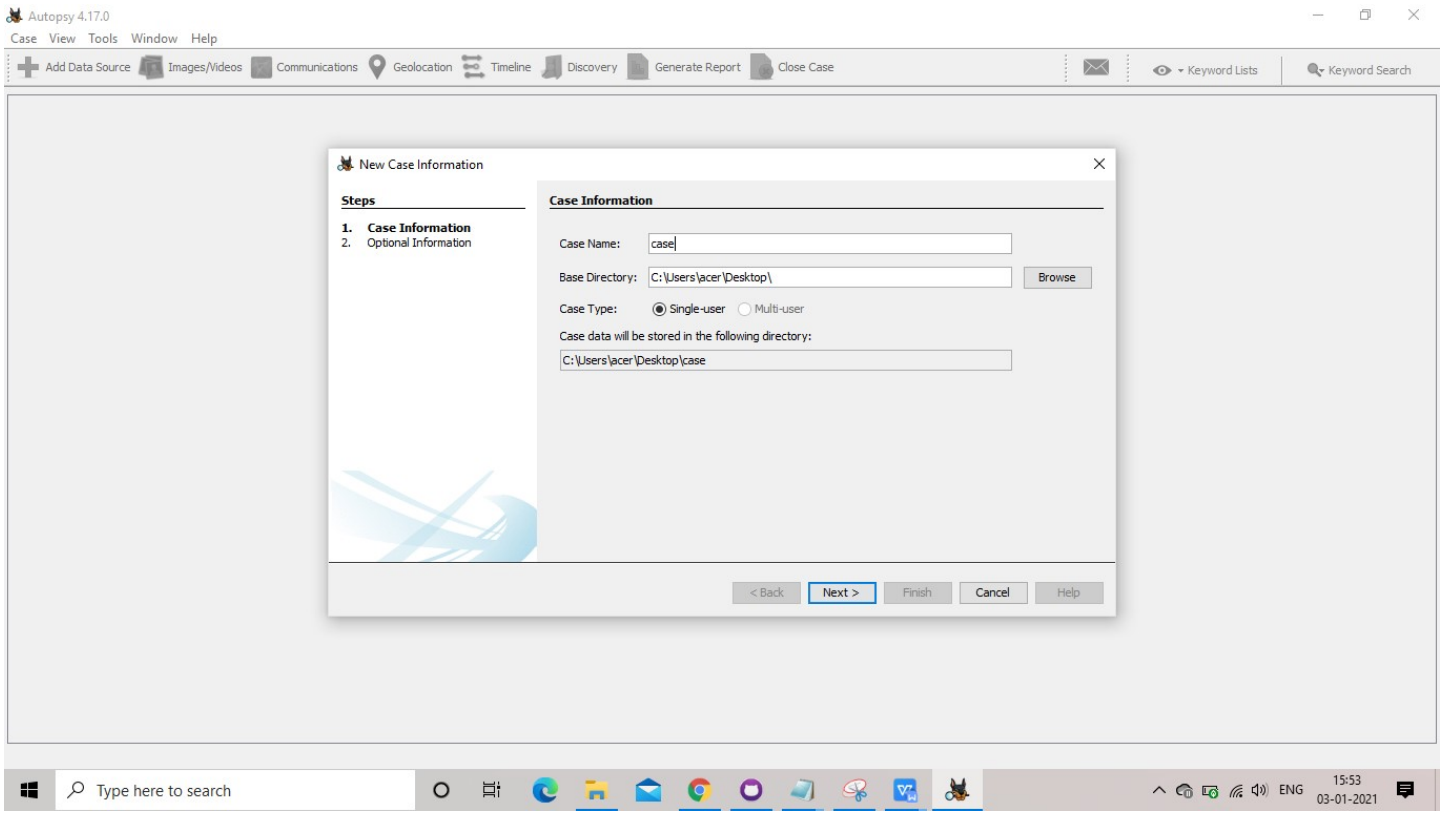
Practical No:08

Aim: Recovering and Inspecting deleted files.

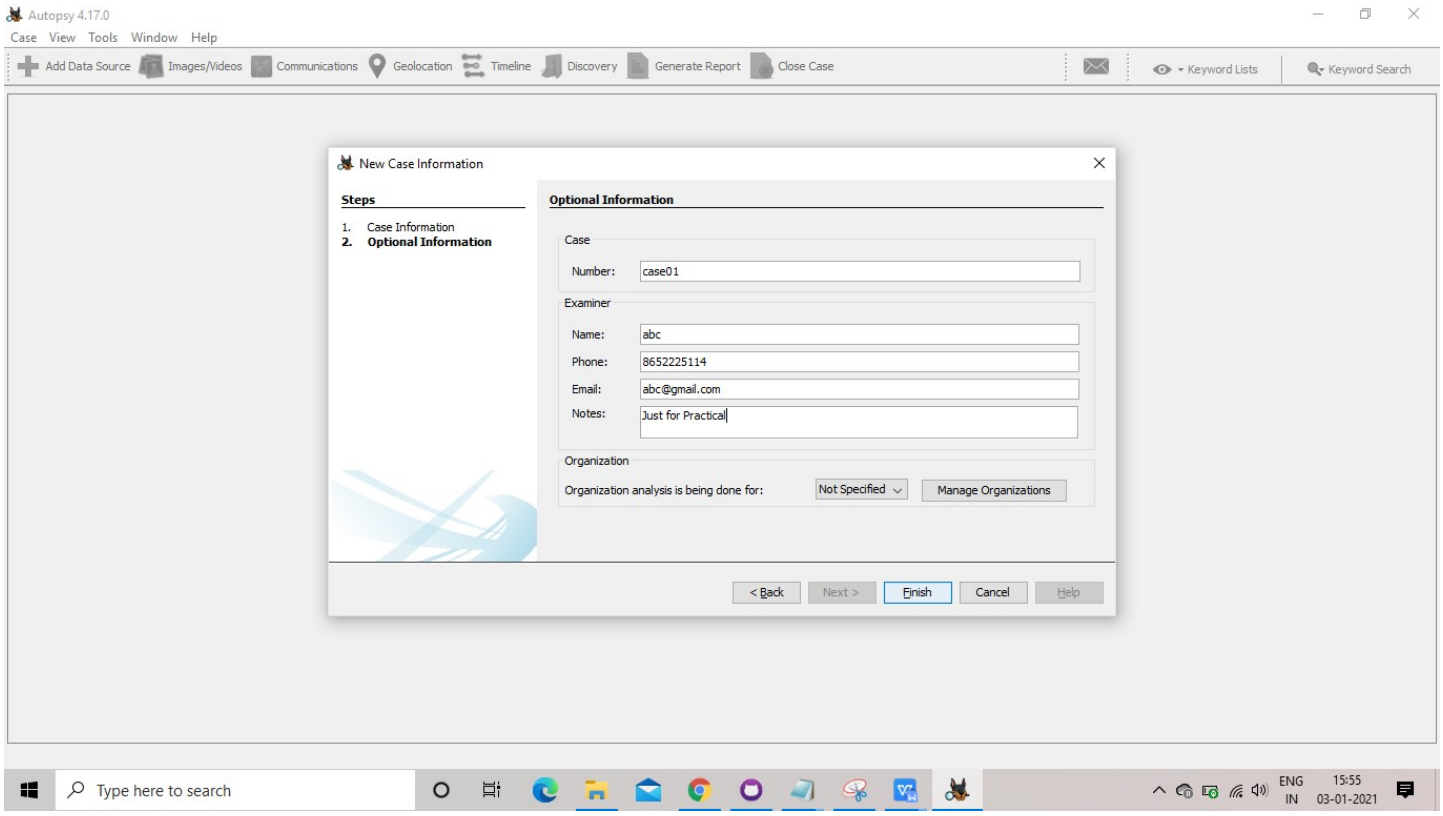
Open Autopsy

Click on new case

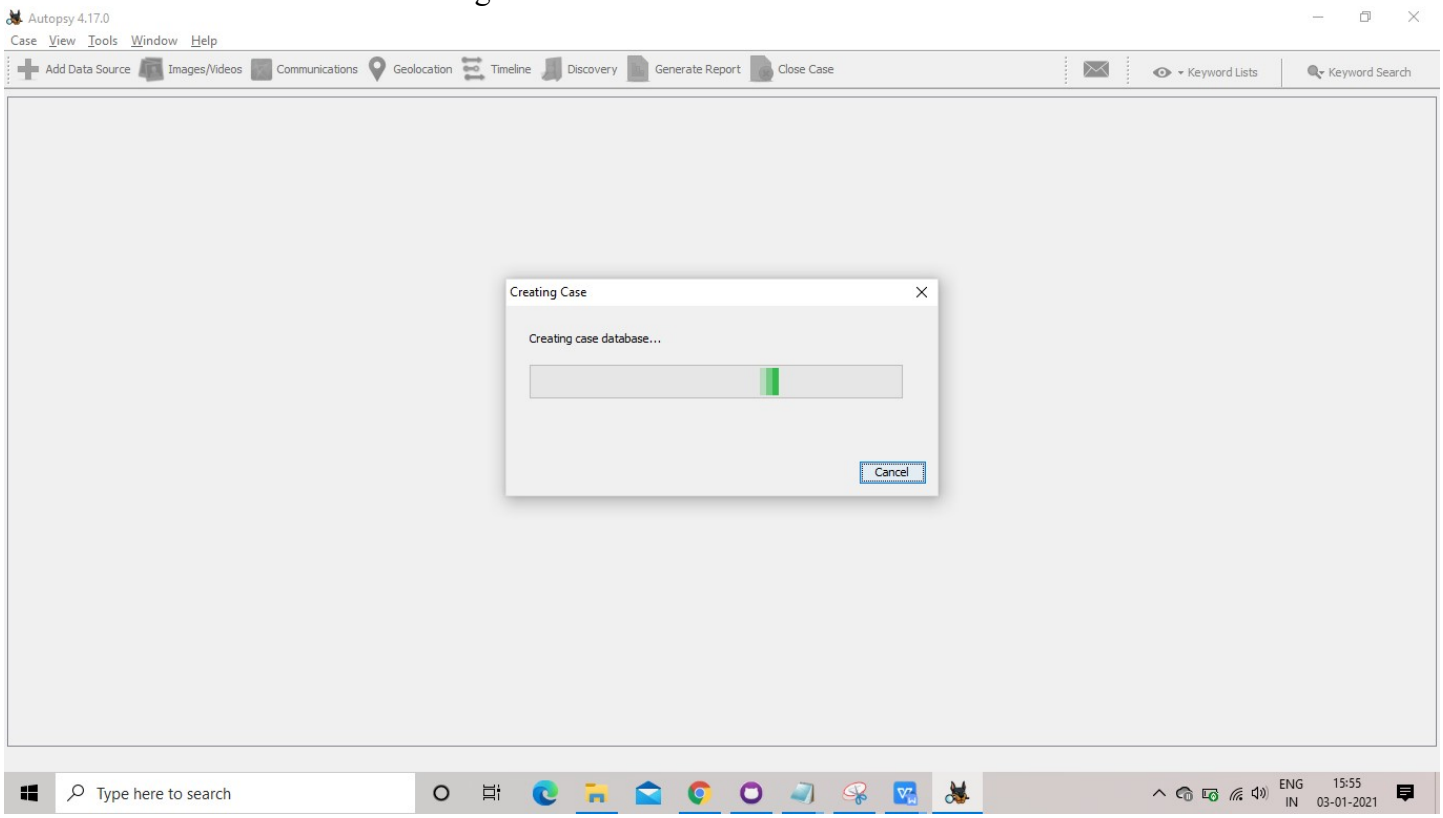
Enter the New case Information and click on Next Button.



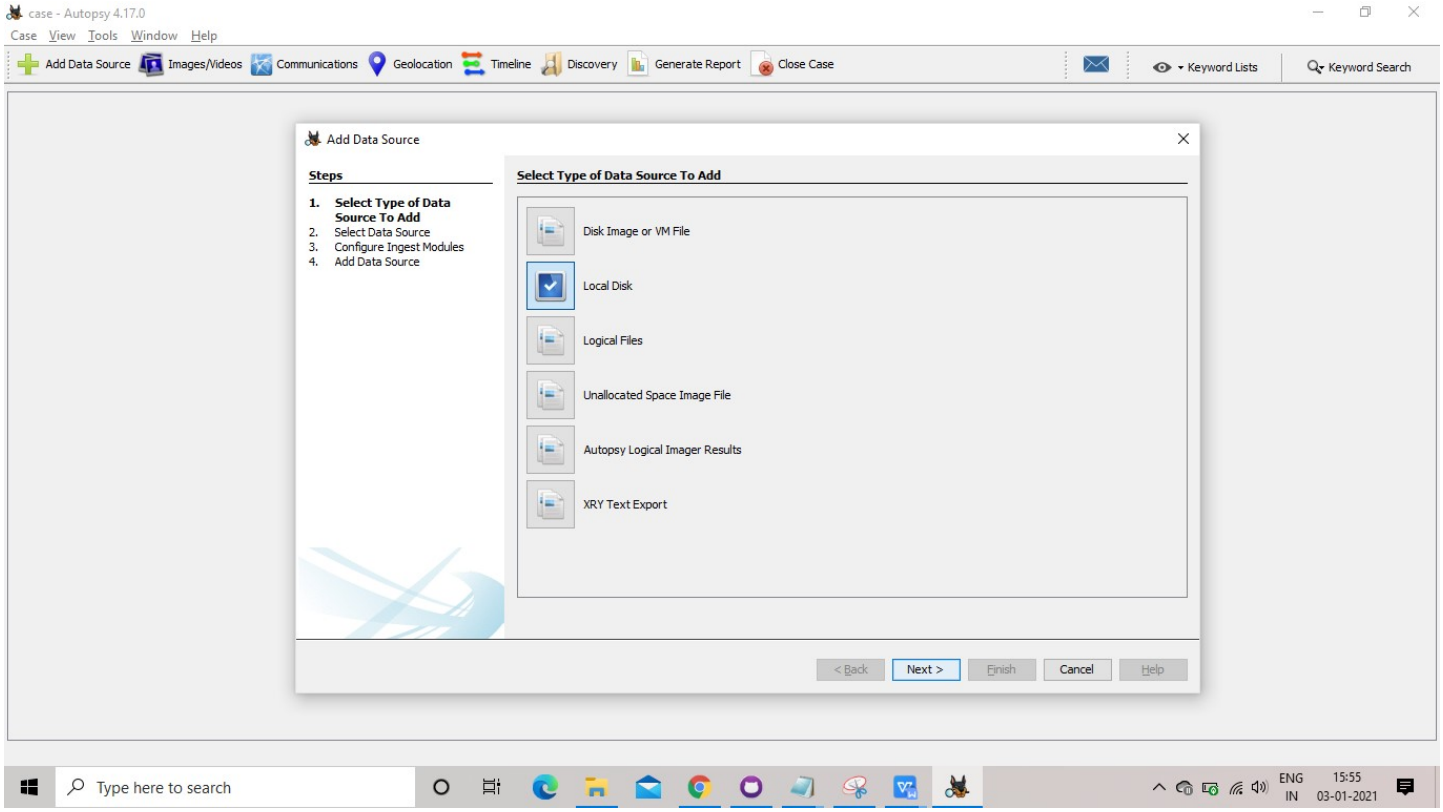
Enter the additional Information and click on Finish.

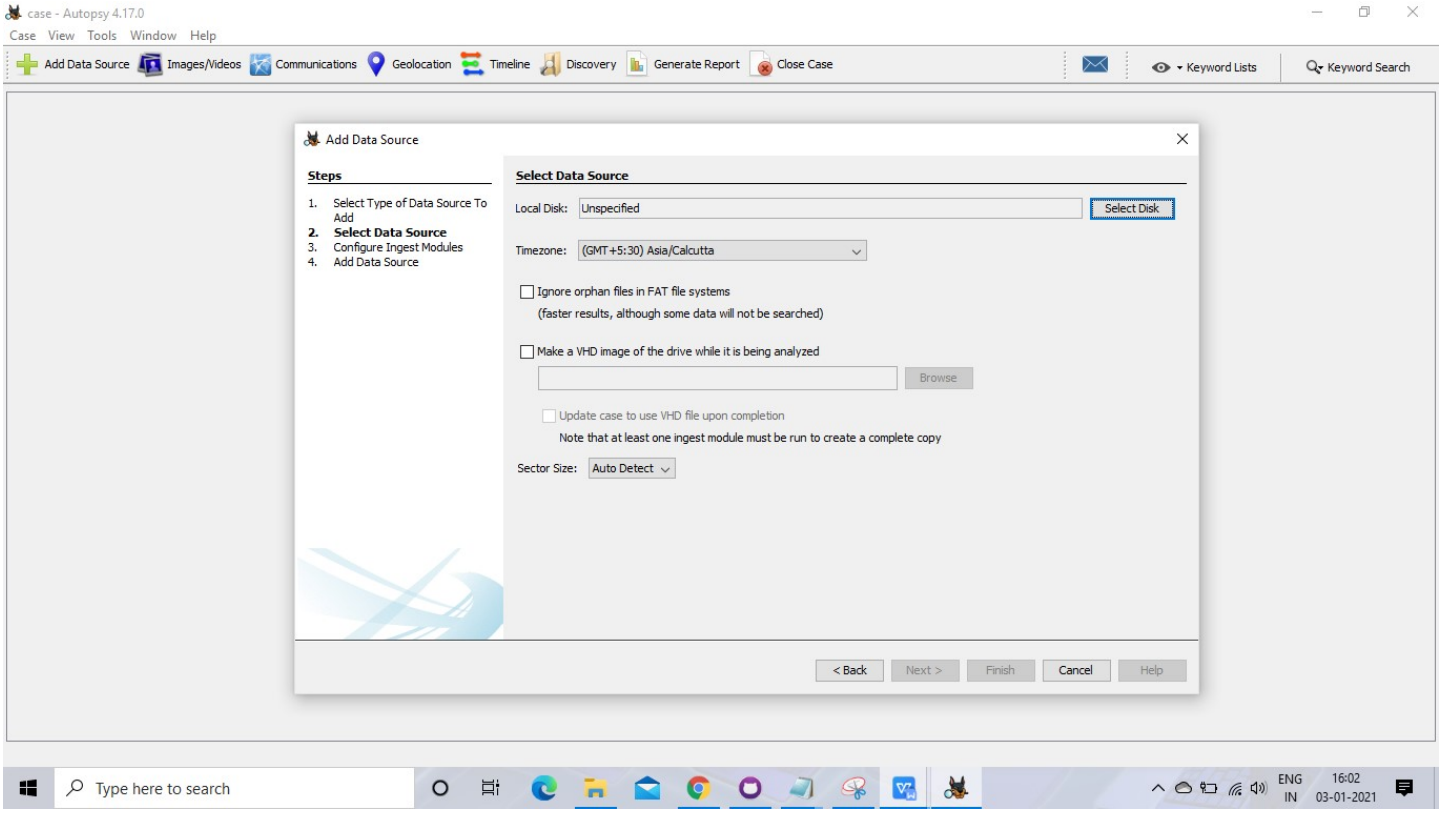


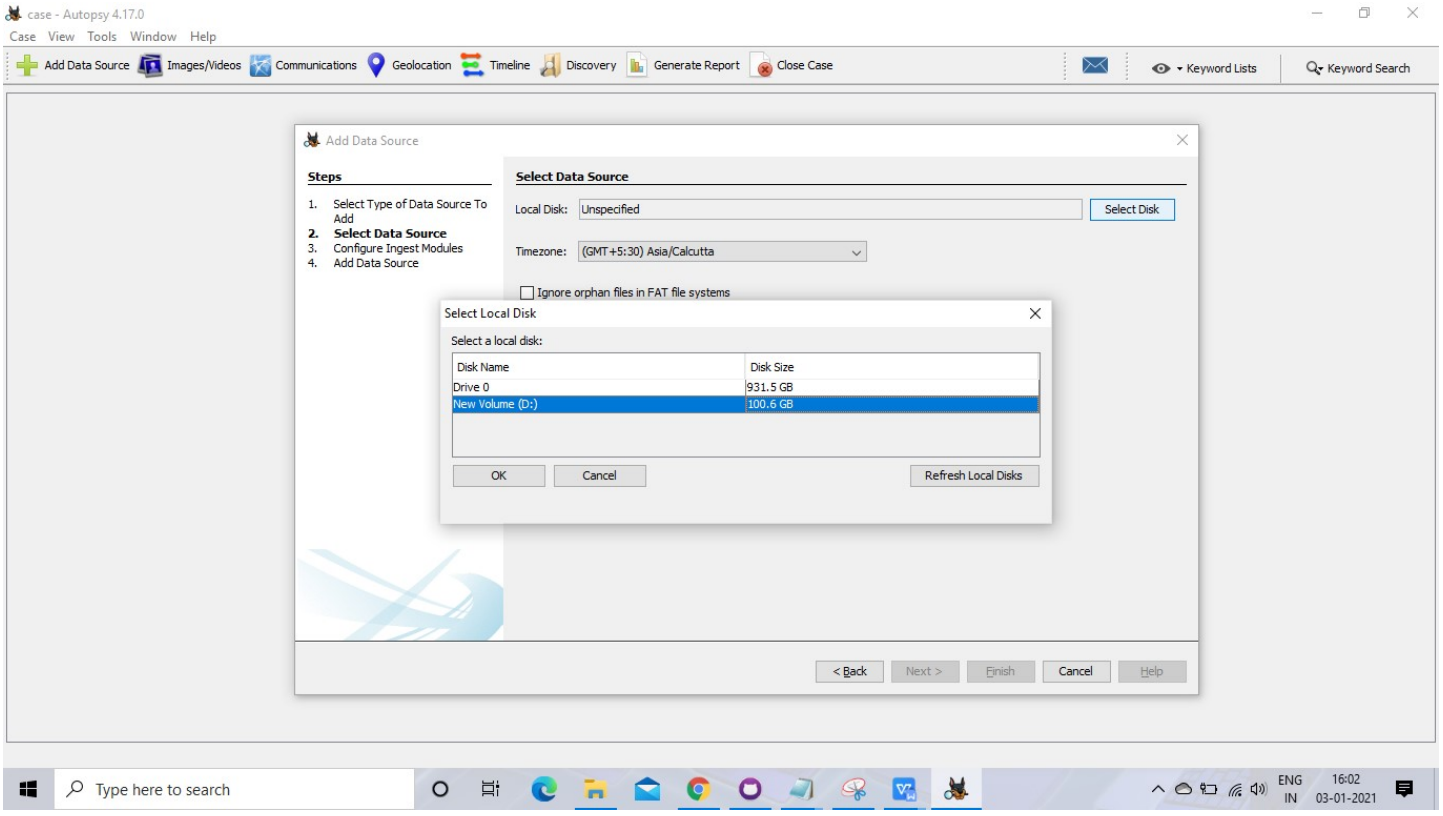
You can see that the database is being created.



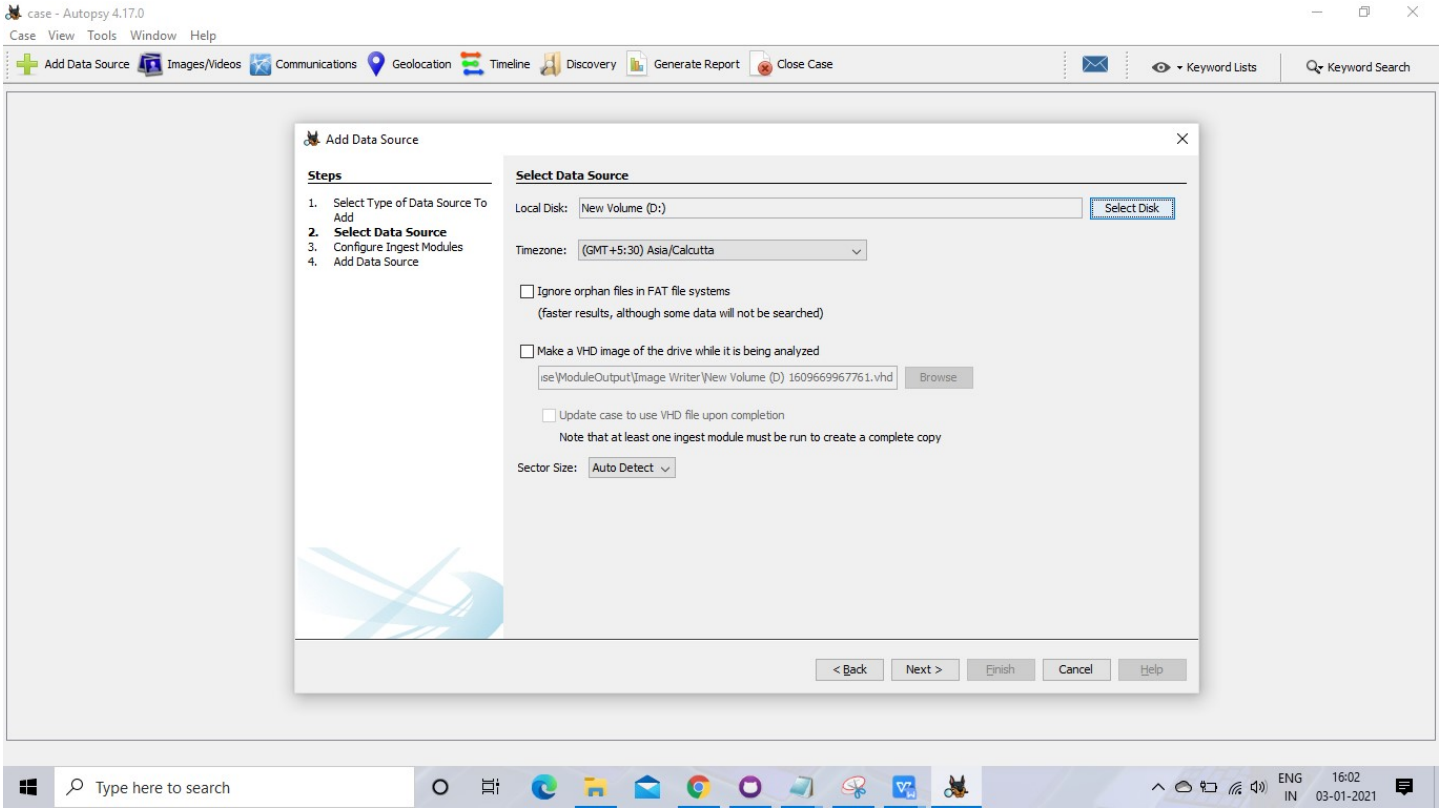
Now Select Source Type as Local disk and Select Local disk form drop down list and click on Next.

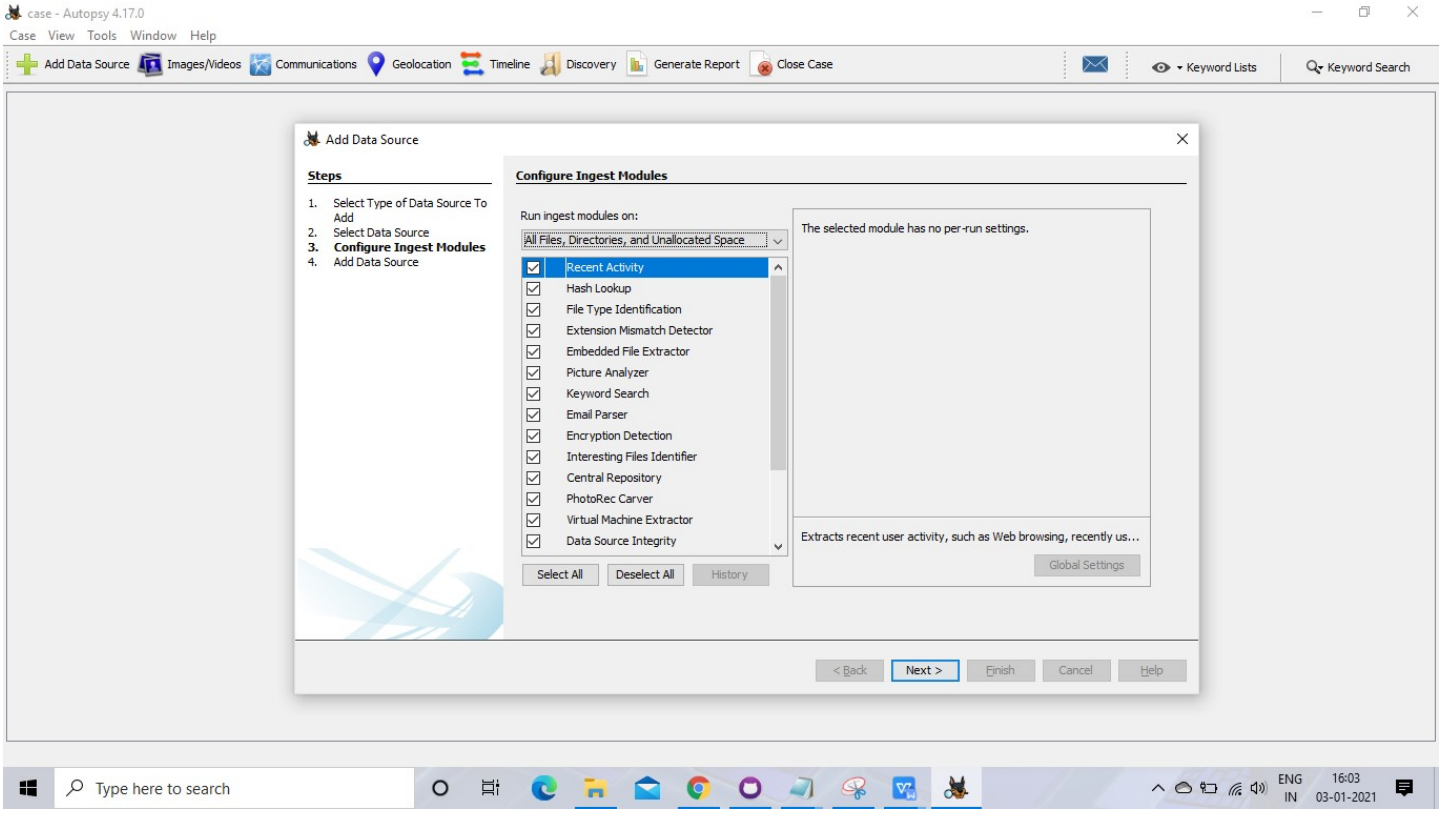



case - Autopsy 4.17.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Select Data Source
Local Disk: Unspecified
Select Disk
Timezone: (GMT+5:30) Asia/Calcutta
Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)
Make a VHD image of the drive while it is being analyzed
Browse
Update case to use VHD file upon completion
Note that at least one ingest module must be run to create a complete copy
Sector Size: Auto Detect
< Back
Next >
Finish
Cancel
Help
Type here to search
ENG
IN
16:02
03-01-2021

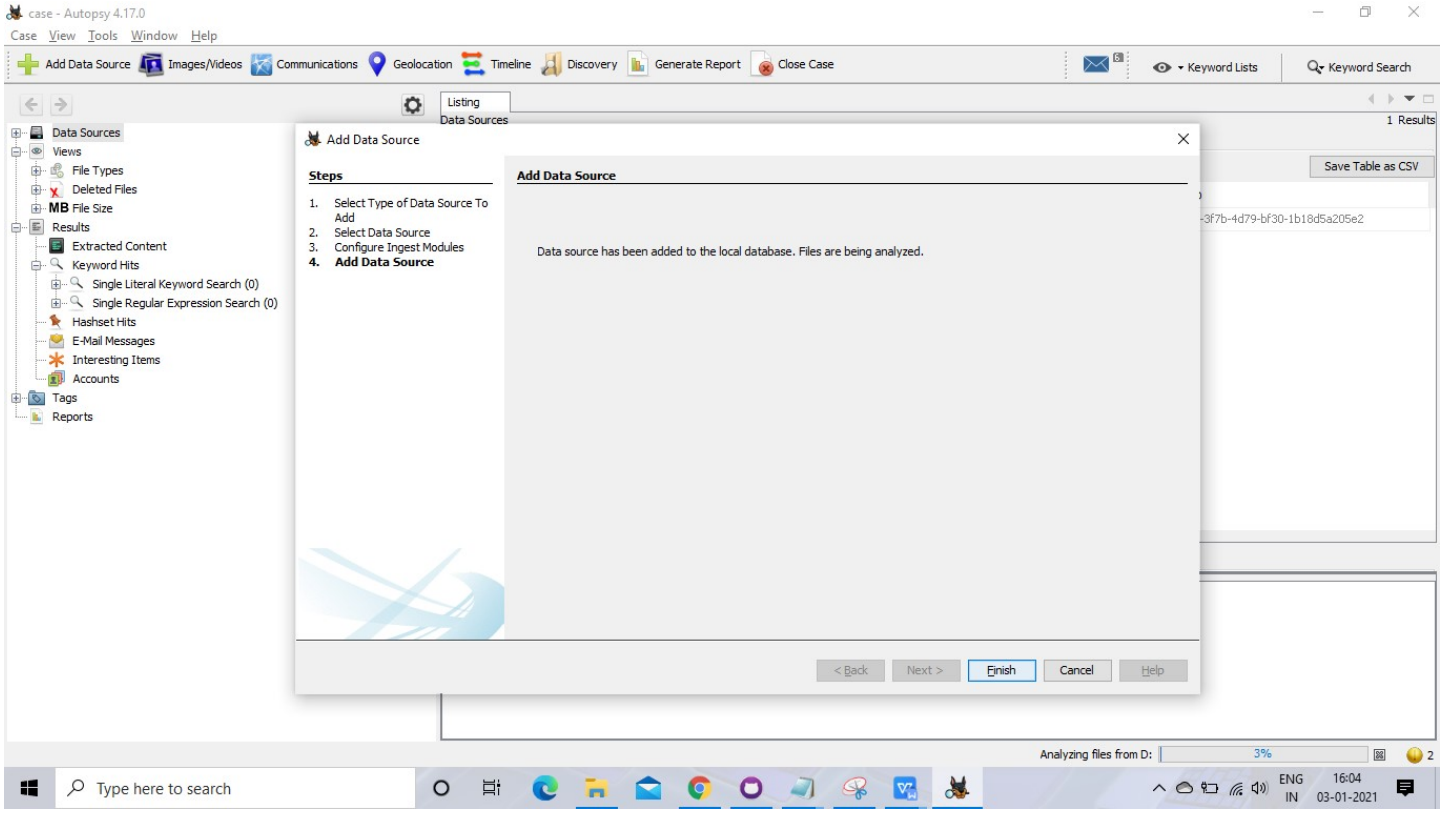

case - Autopsy 4.17.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Select Data Source
Local Disk: Unspecified
Select Disk
Timezone: (GMT+5:30) Asia/Calcutta
Ignore orphan files in FAT file systems
Select Local Disk
Select a local disk:
Disk Name
Disk Size
Drive 0
931.5 GB
New Volume (D:)
100.6 GB
OK
Cancel
Refresh Local Disks
< Back
Next >
Finish
Cancel
Help
Type here to search
ENG
IN
16:02
03-01-2021

Click on Next Button.

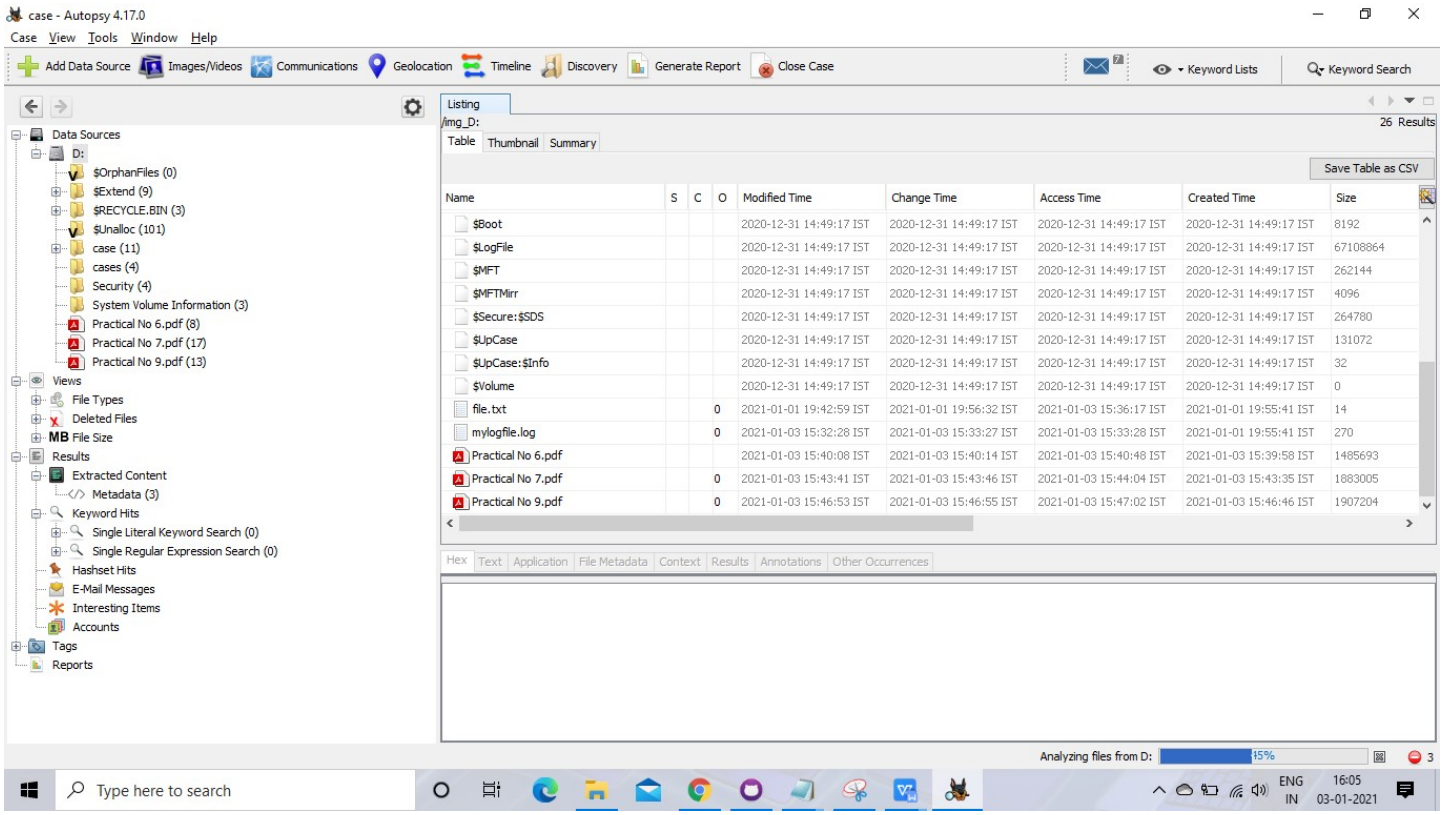




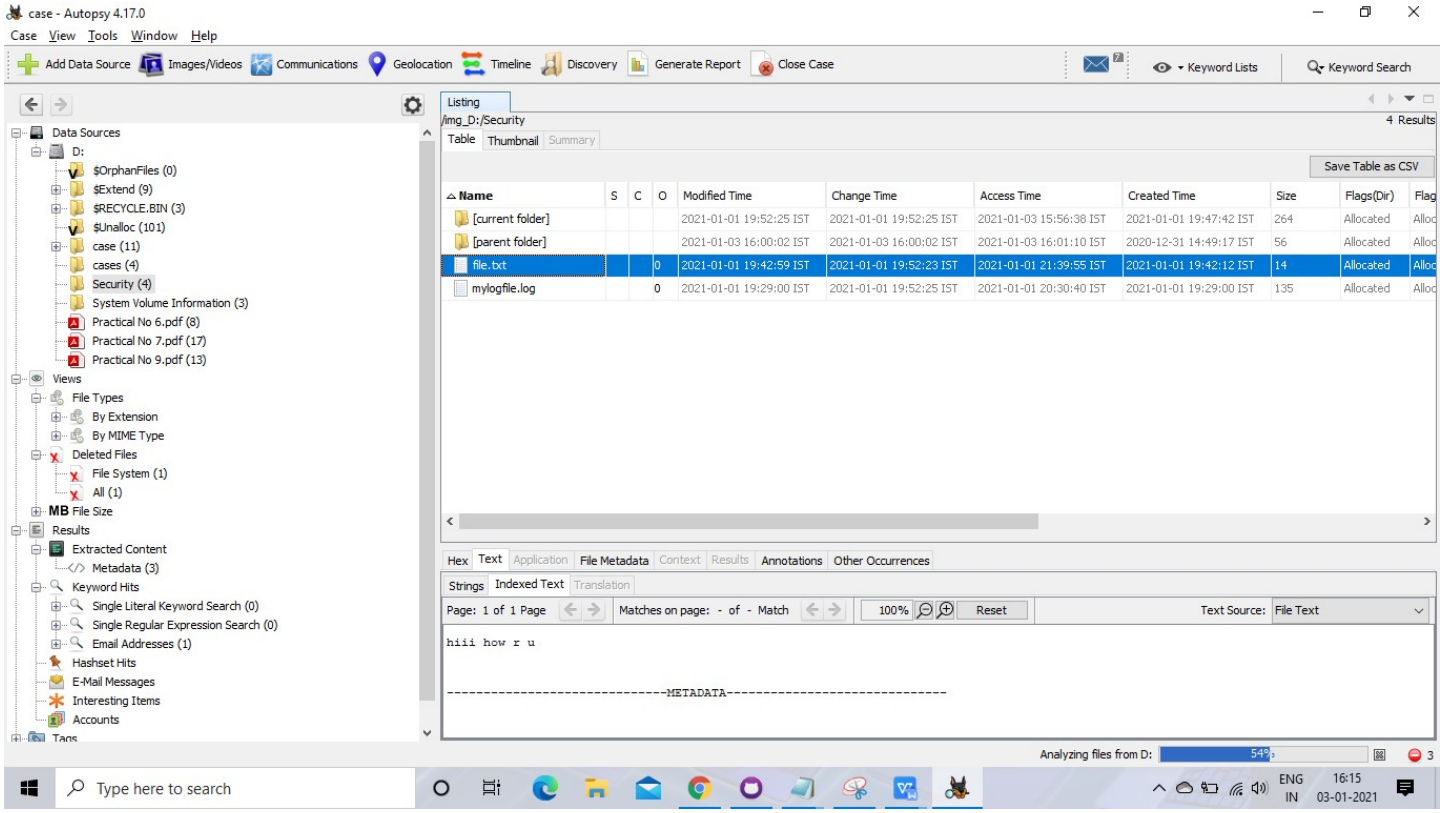
Now click On Finish.



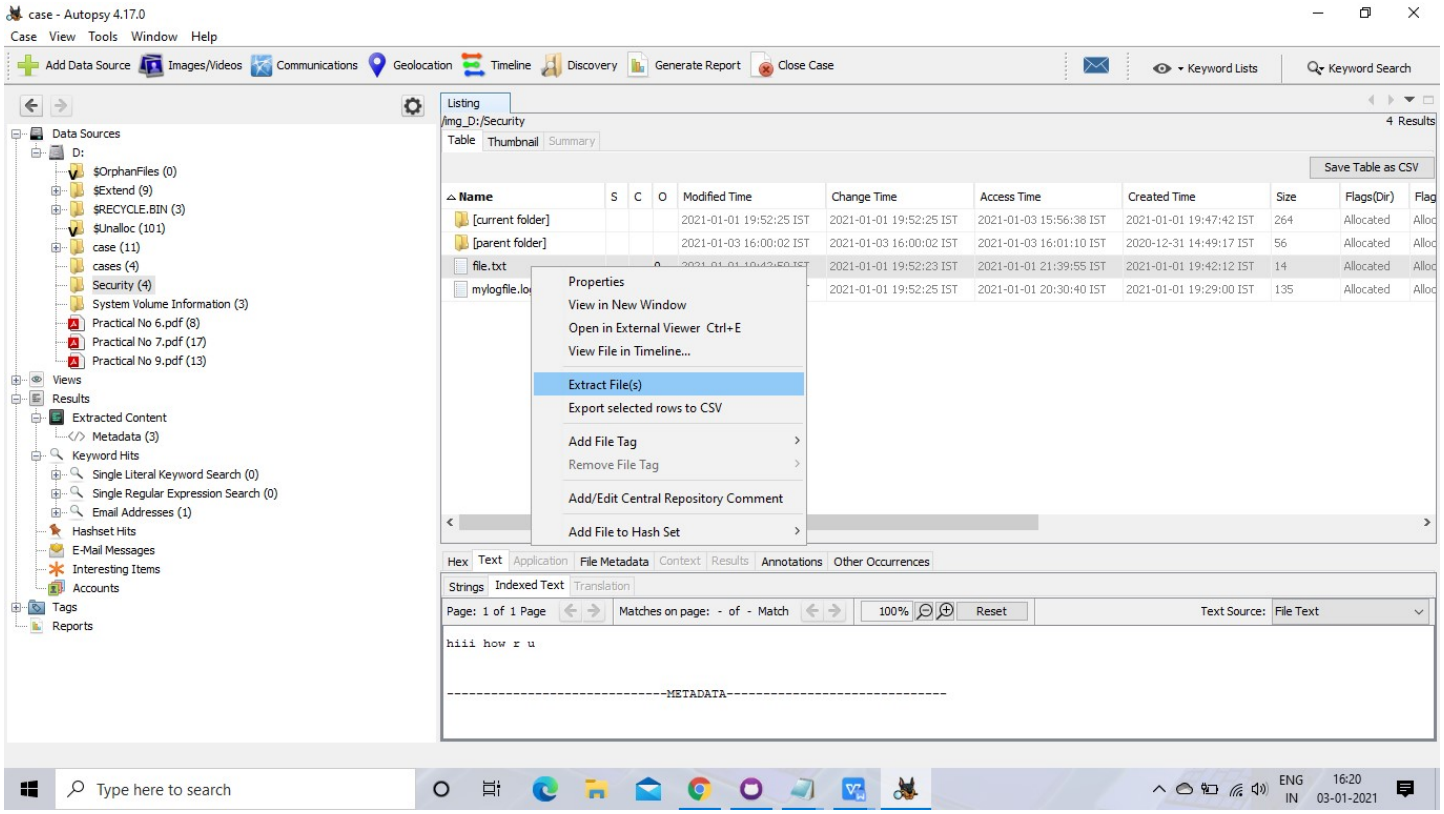
Now Autopsy window will appear and it will analyzing the disk that we have selected.



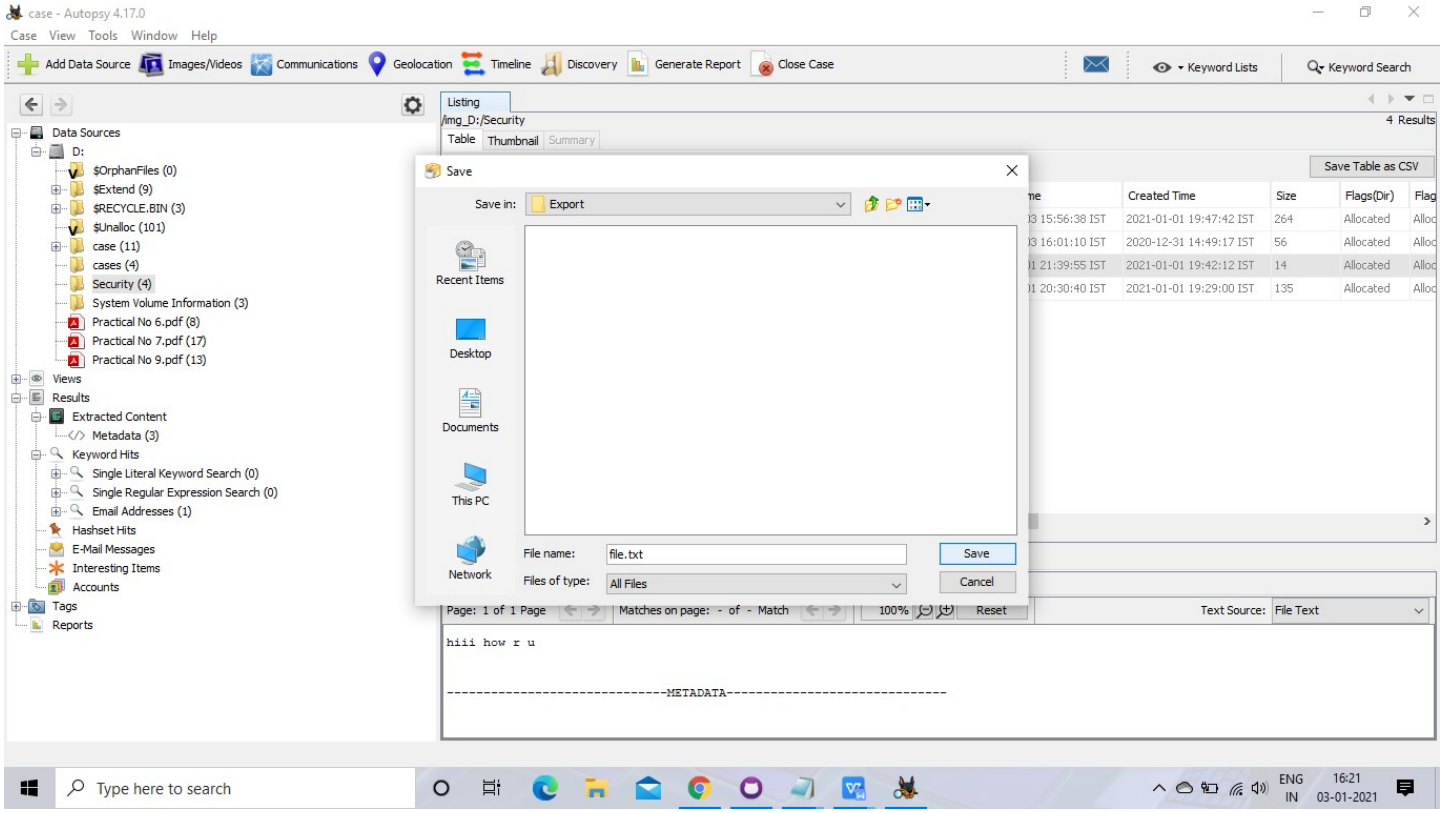
All files will appear in table tab select any file to see the data.



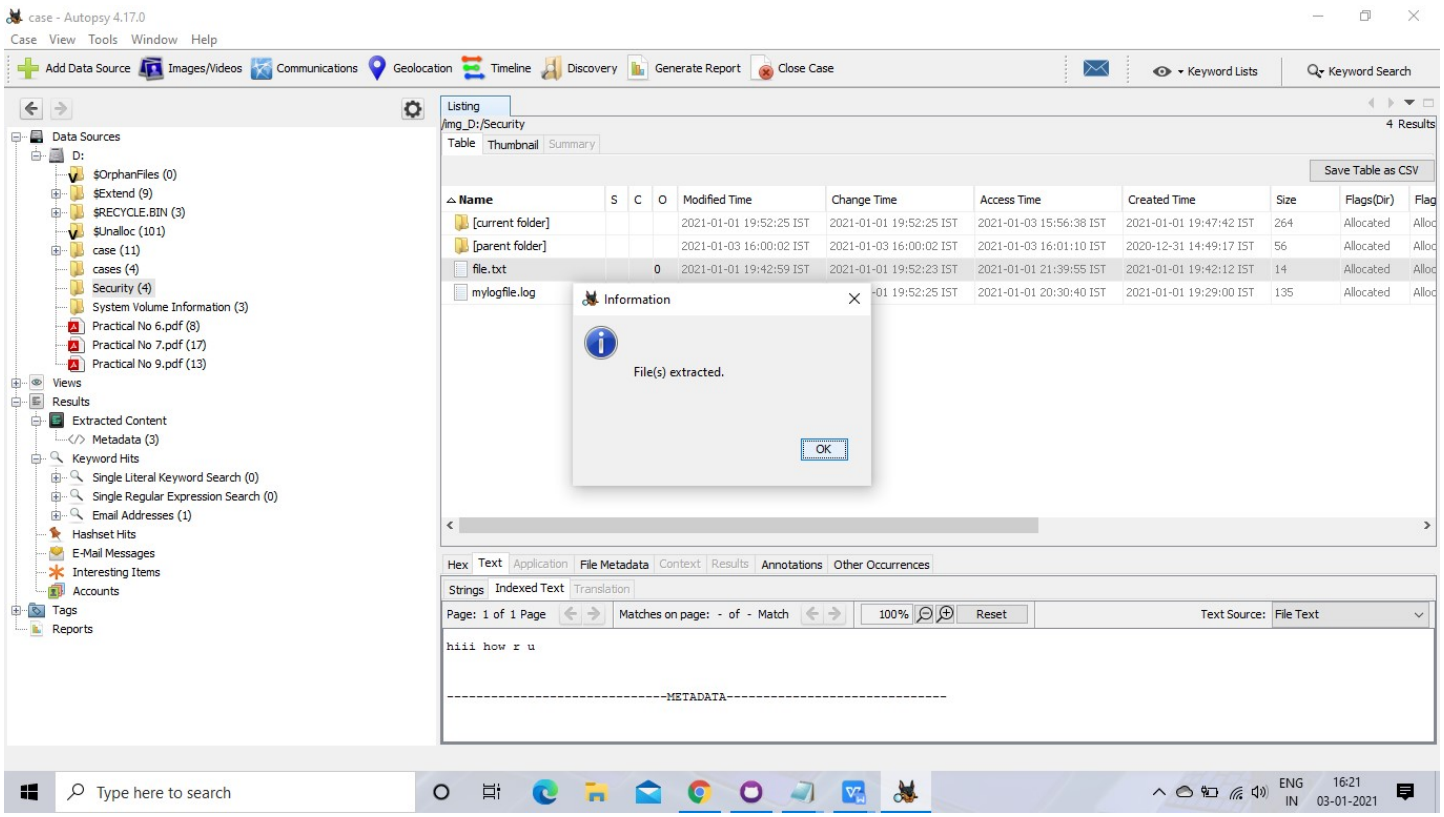
To recover the file, go to view node-> Deleted Files node , here select any file and right click on it than select Extract Files option.



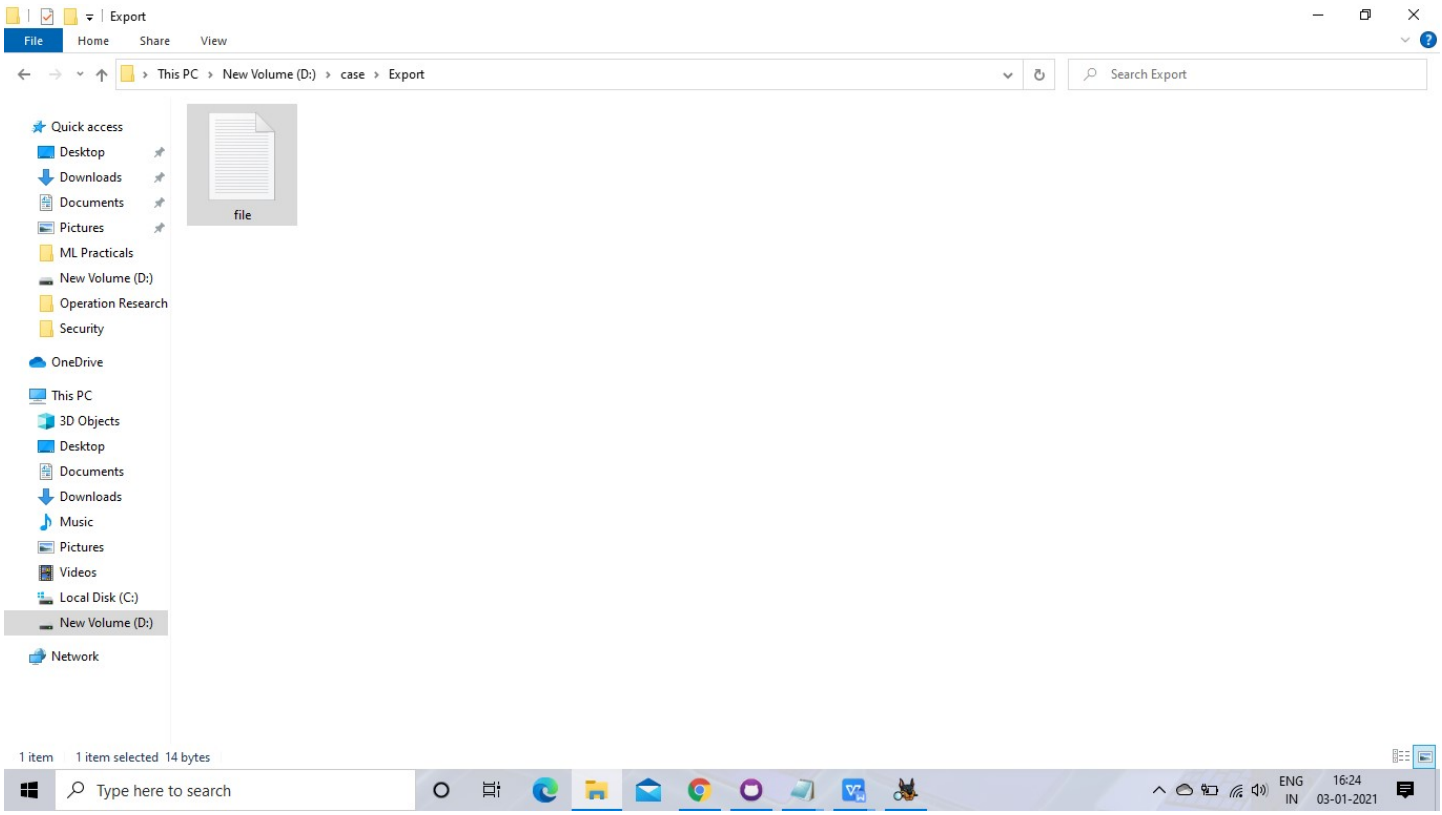
By default Export folder is choose to save the recovered file.



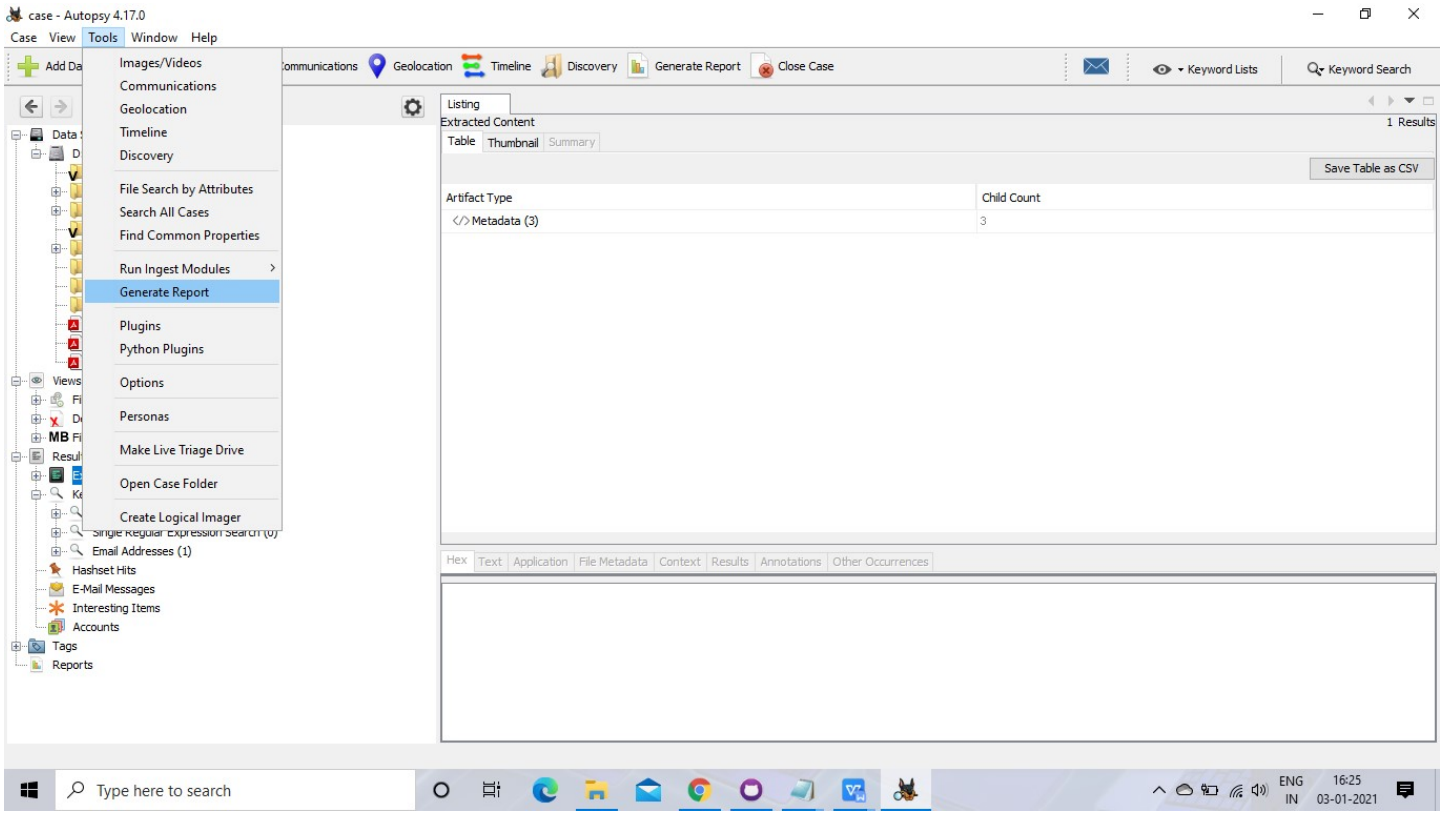
Now Click on Ok.

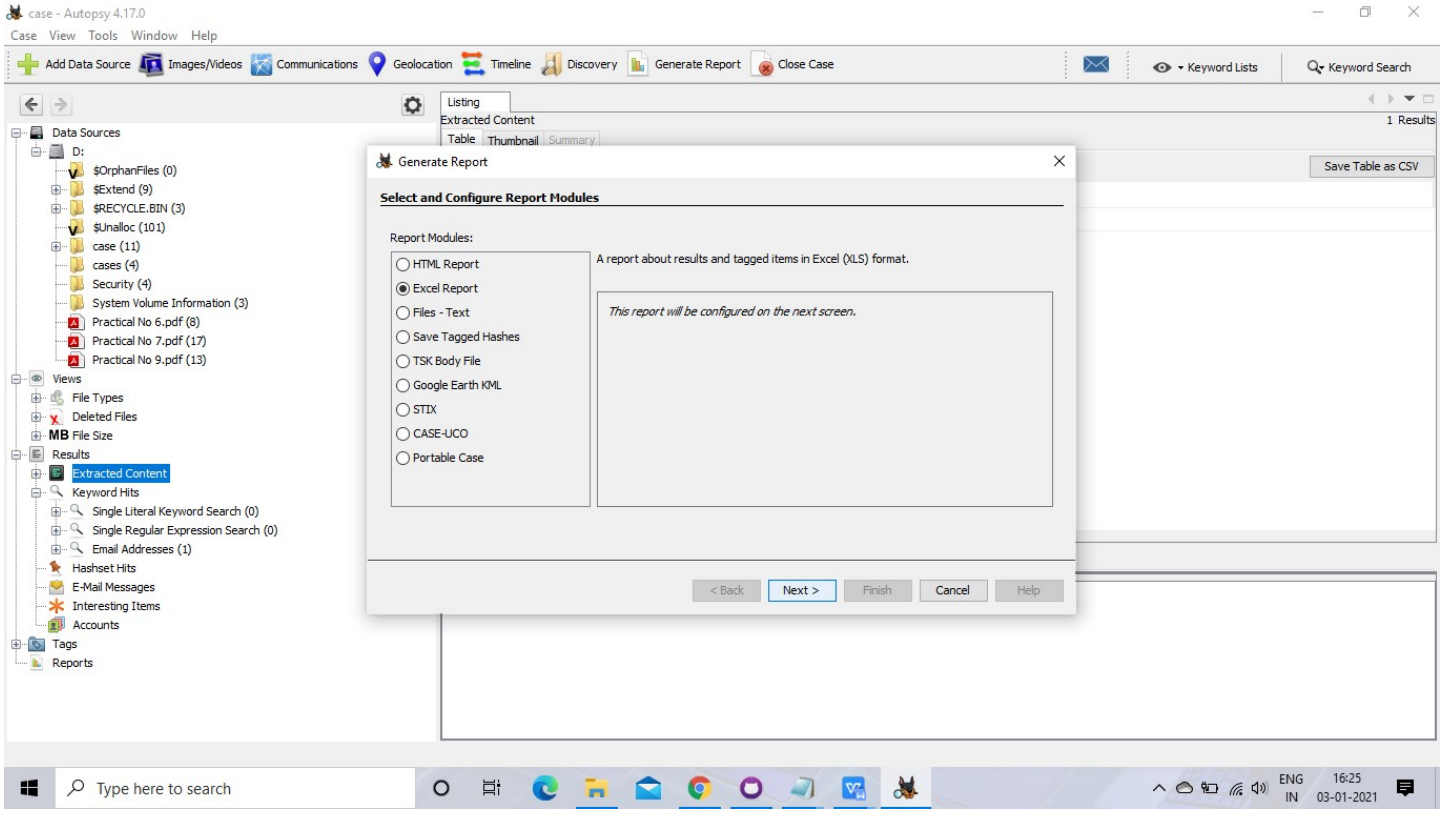


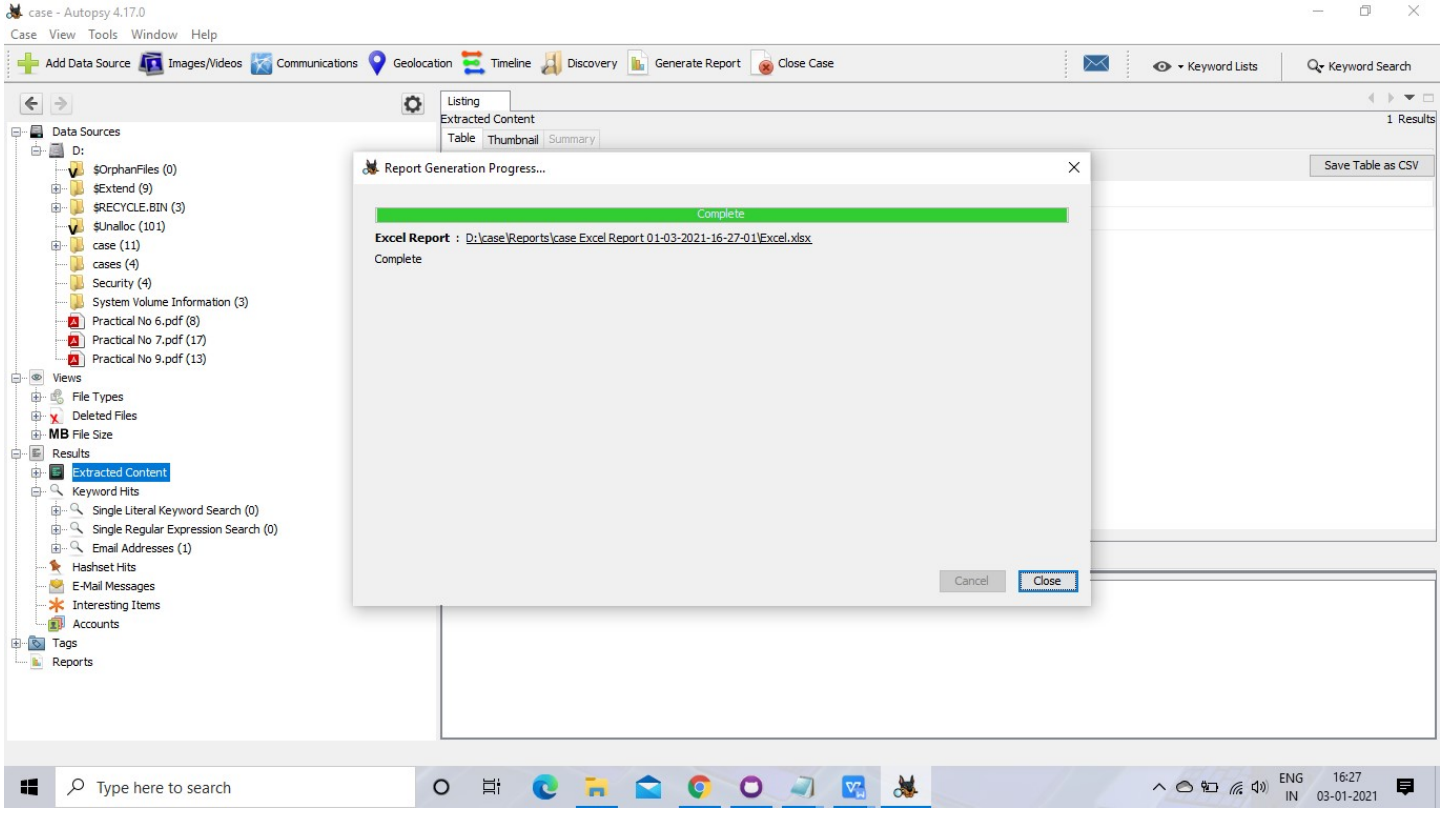
Now go to the Export Folder to view Recover file.



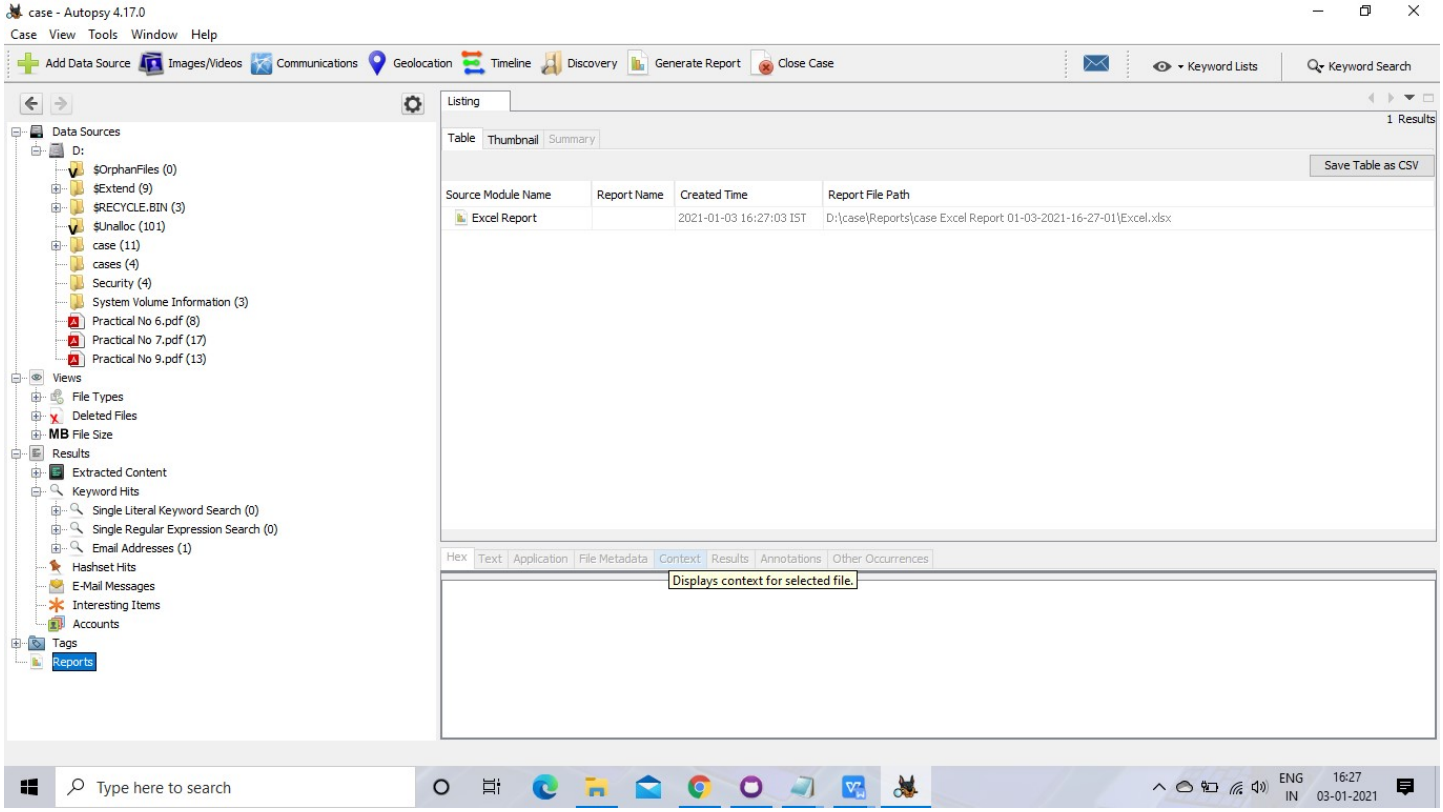
Click on Generate Report from autopsy window and Select the Excel format and click on next.




case - Autopsy 4.17.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
D:
$OrphanFiles (0)
$Extend (9)
$RECYCLE.BIN (3)
$Unalloc (101)
case (11)
cases (4)
Security (4)
System Volume Information (3)
Practical No 6.pdf (8)
Practical No 7.pdf (17)
Practical No 9.pdf (13)
Views
File Types
Deleted Files
File Size
Results
Extracted Content
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Email Addresses (1)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports
Listing
Extracted Content
1 Results
Table
Thumbnail
Summary
Save Table as CSV
Generate Report
Select and Configure Report Modules
Report Modules:
HTML Report
Excel Report
Files - Text
Save Tagged Hashes
TSK Body File
Google Earth KML
STIX
CASE-UCO
Portable Case
A report about results and tagged items in Excel (XLS) format.
This report will be configured on the next screen.
< Back
Next >
Finish
Cancel
Help
Type here to search
ENG
IN
16:25
03-01-2021


case - Autopsy 4.17.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
D:
$OrphanFiles (0)
$Extend (9)
$RECYCLE.BIN (3)
$Unalloc (101)
case (11)
cases (4)
Security (4)
System Volume Information (3)
Practical No 6.pdf (8)
Practical No 7.pdf (17)
Practical No 9.pdf (13)
Views
File Types
Deleted Files
File Size
Results
Extracted Content
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Email Addresses (1)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports
Listing
Extracted Content
1 Results
Table
Thumbnail
Summary
Save Table as CSV
Report Generation Progress...
Complete
Excel Report : D:\case\Reports\case Excel Report 01-03-2021-16-27-01\Excel.xlsx
Complete
Cancel
Close
Type here to search
ENG
IN
16:27
03-01-2021

Now Report is Generated So click on close Button .we can see the Report on Report Node.



Now open the Report folder and Open Excel File.