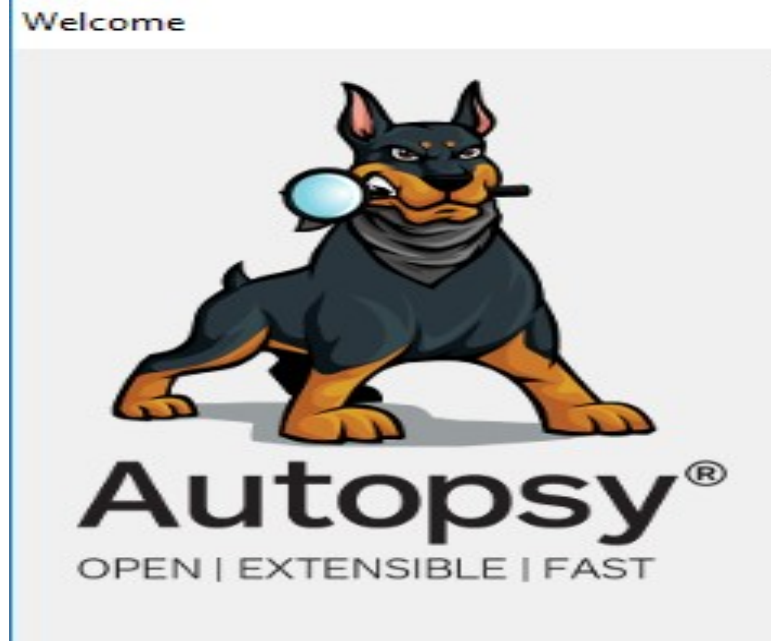
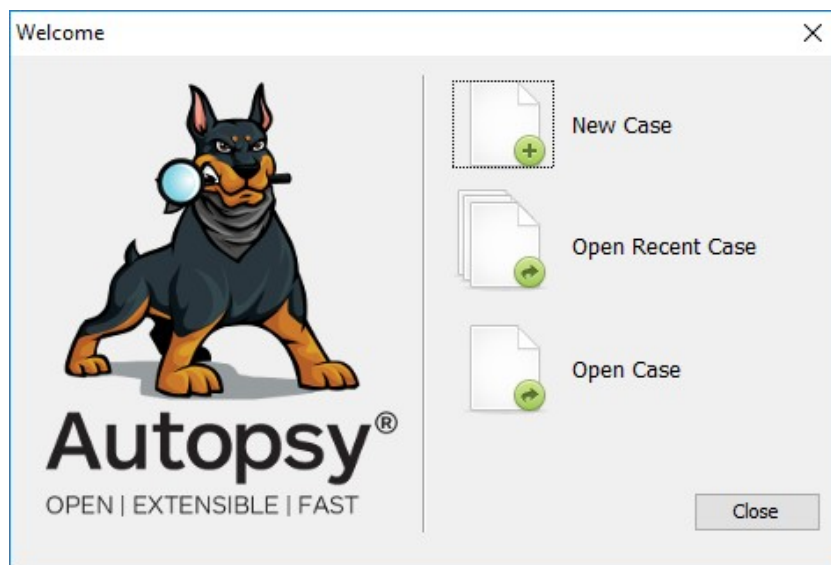


Aim: Recovering and Inspecting deleted files.

Open Autopsy



Click on new case



Enter the New case Information and click on Next Button.

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

New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name: case

Base Directory: C:\Users\acer\Desktop Browse

Case Type: ☒ Single-user ☐ Multi-user

Case data will be stored in the following directory:

C:\Users\acer\Desktop\case

< Back Next > Finish Cancel Help

Enter the additional Information and click on Finish.

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

New Case Information

Steps

1. Case Information
2. Optional Information

Optional Information

Case

Number: case01

Examiner

Name: abc

Phone: 8652225114

Email: abc@gmail.com

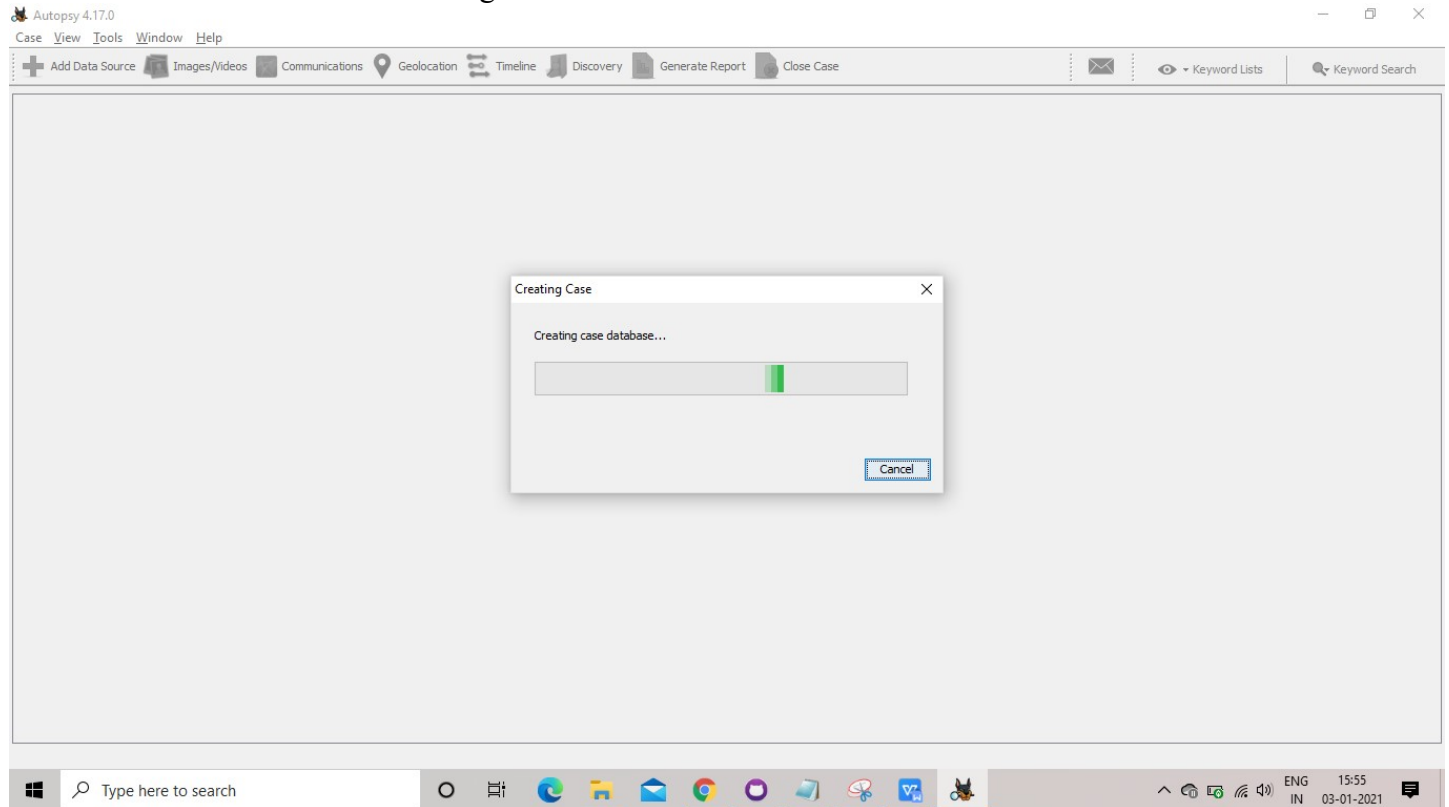
Notes: Just for Practical

Organization

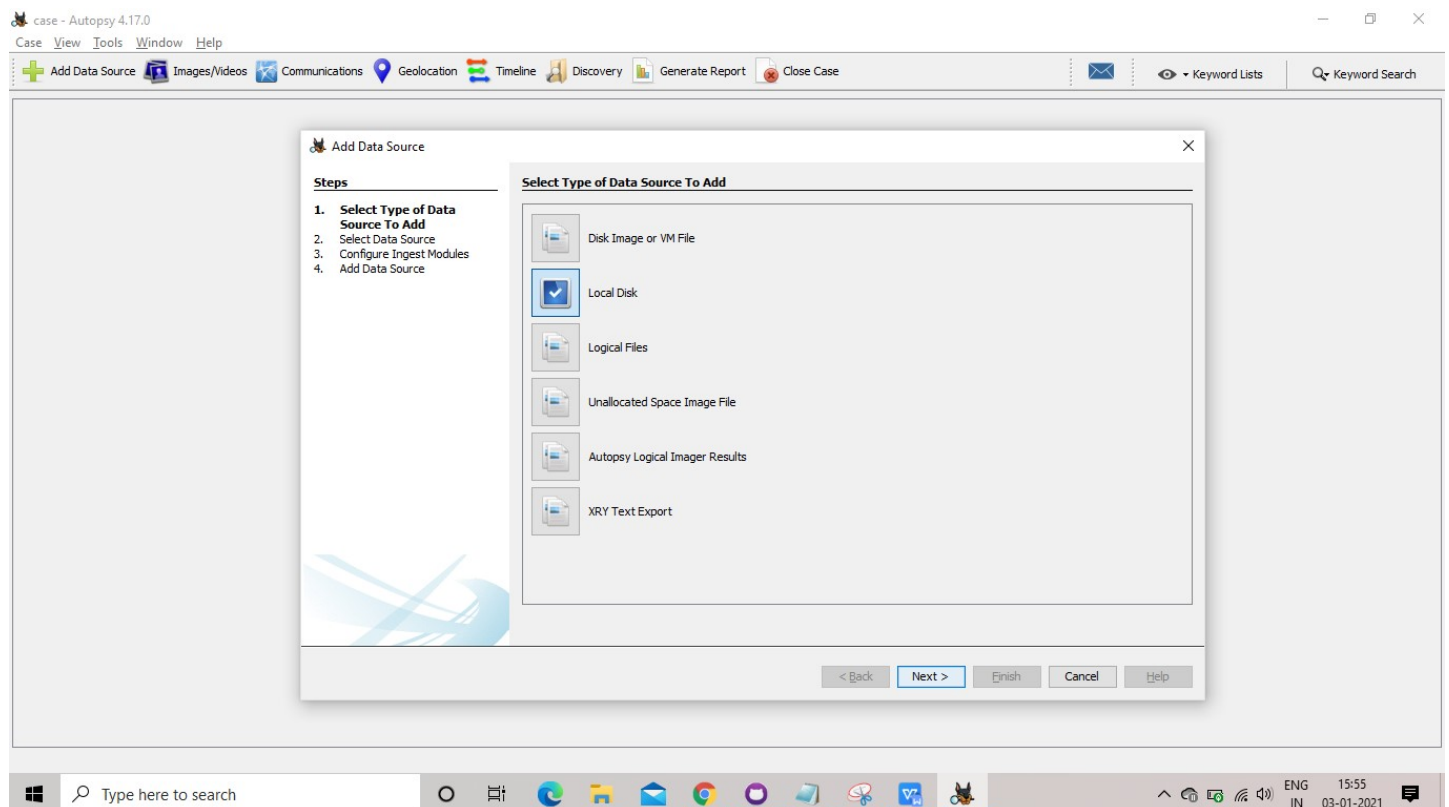
Organization analysis is being done for: Not Specified Manage Organizations

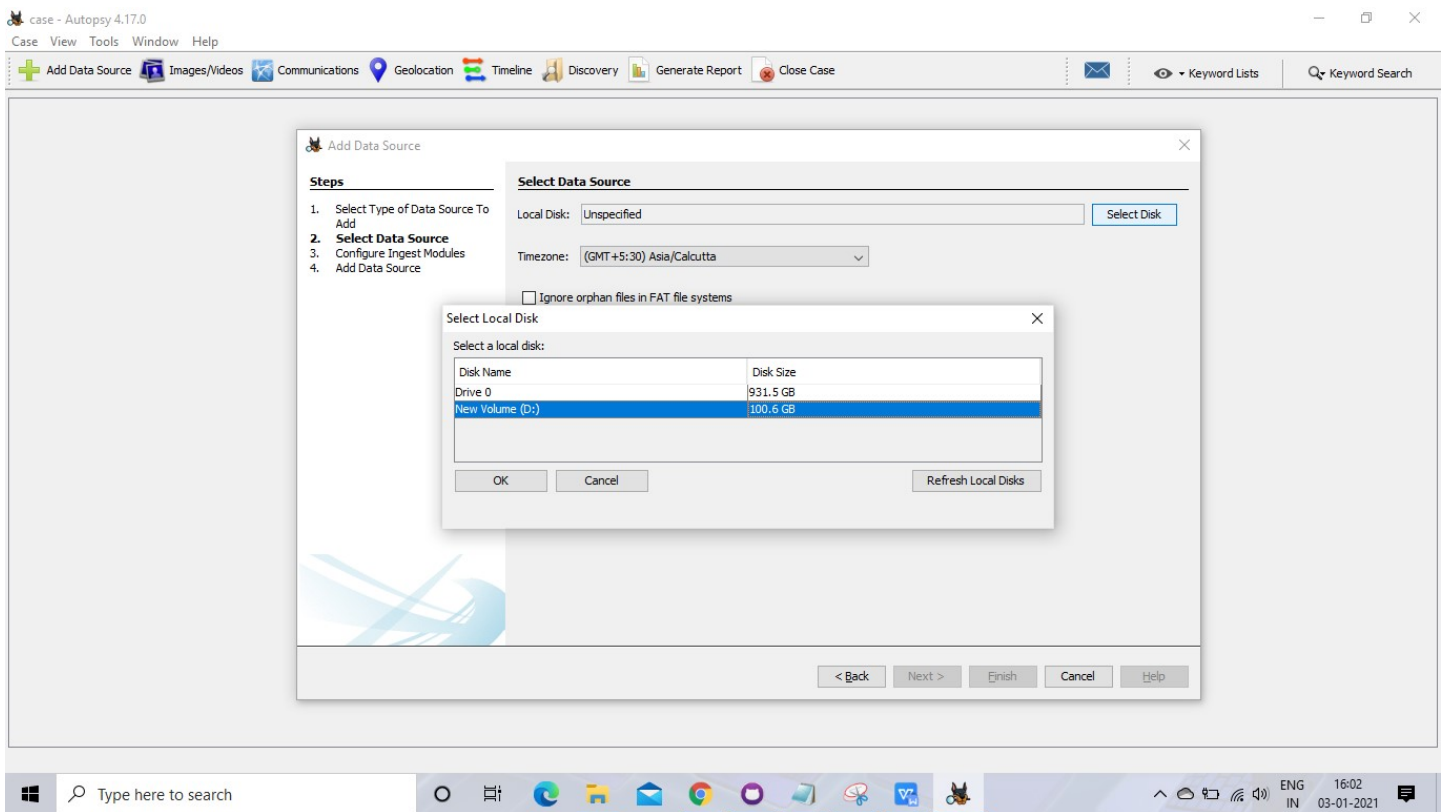
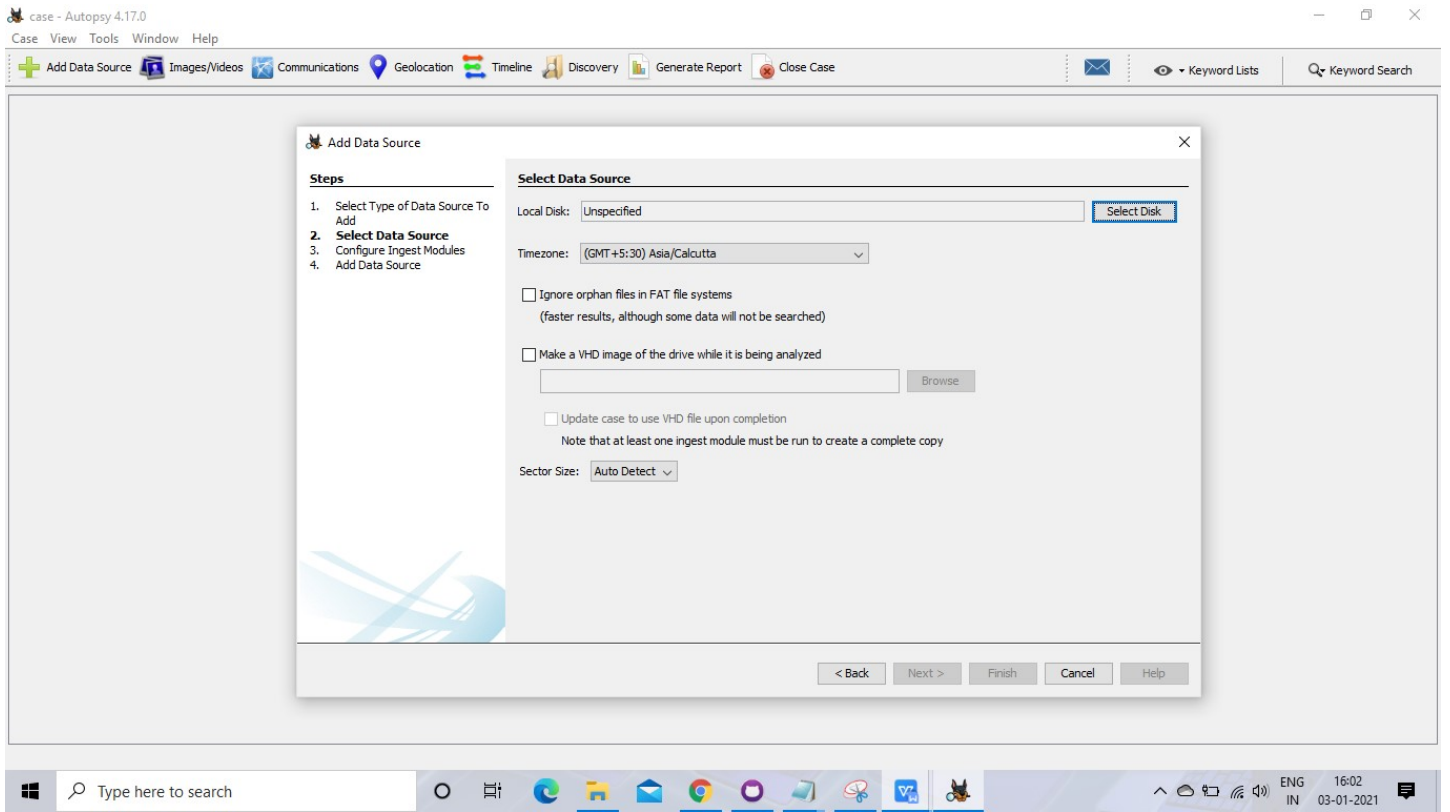
< Back Next > Finish Cancel Help

You can see that the database is being created.

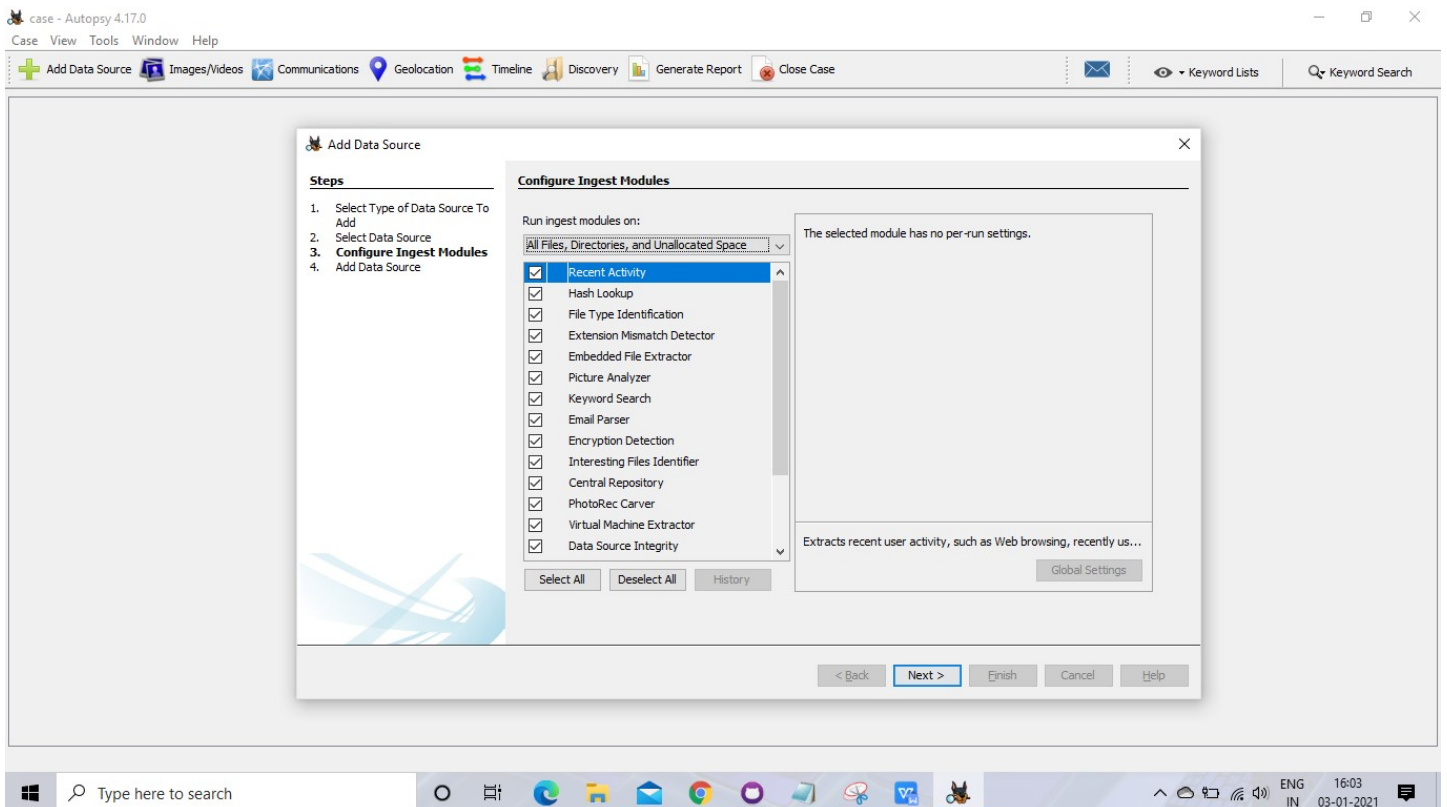
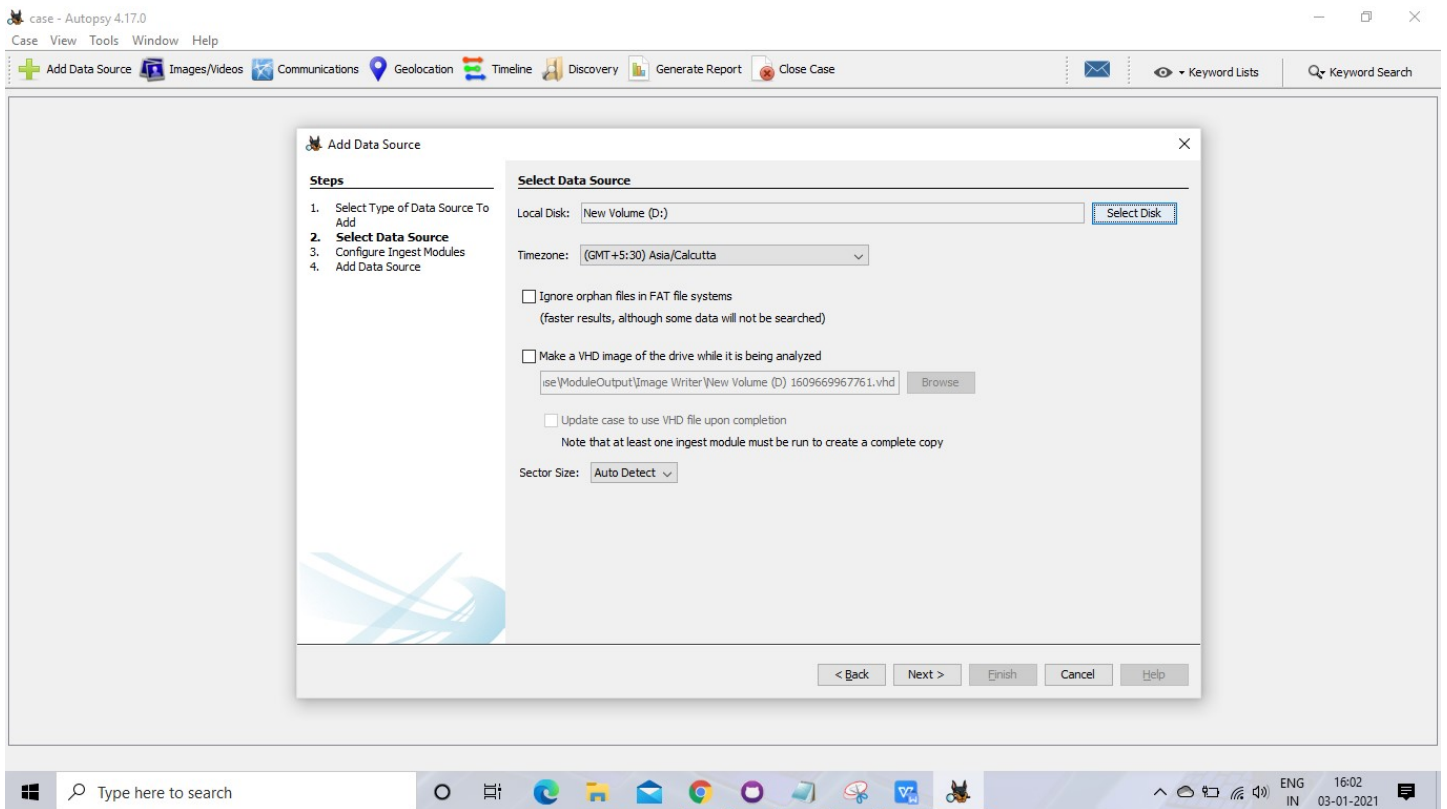


Now Select Source Type as Local disk and Select Local disk form drop down list and click on Next.

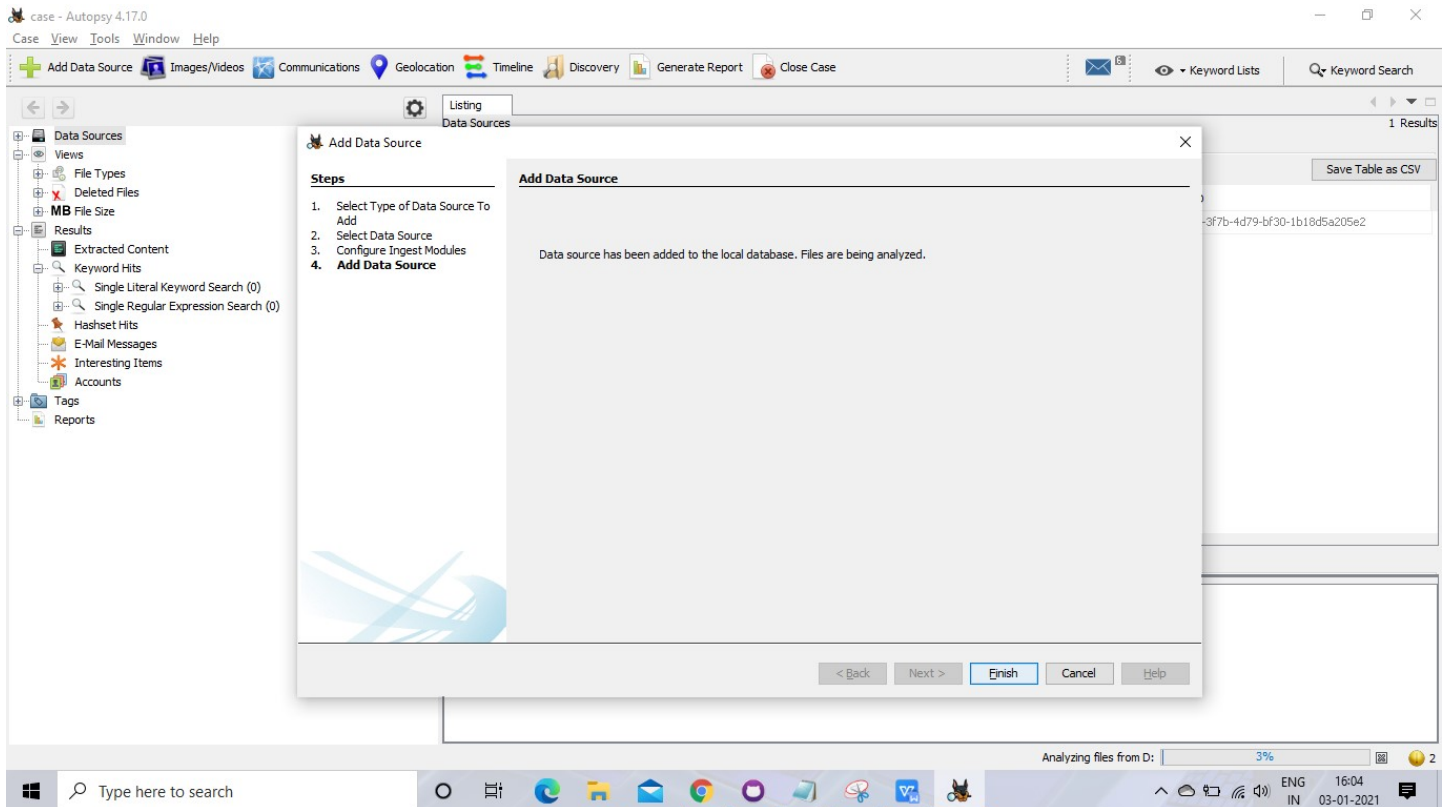




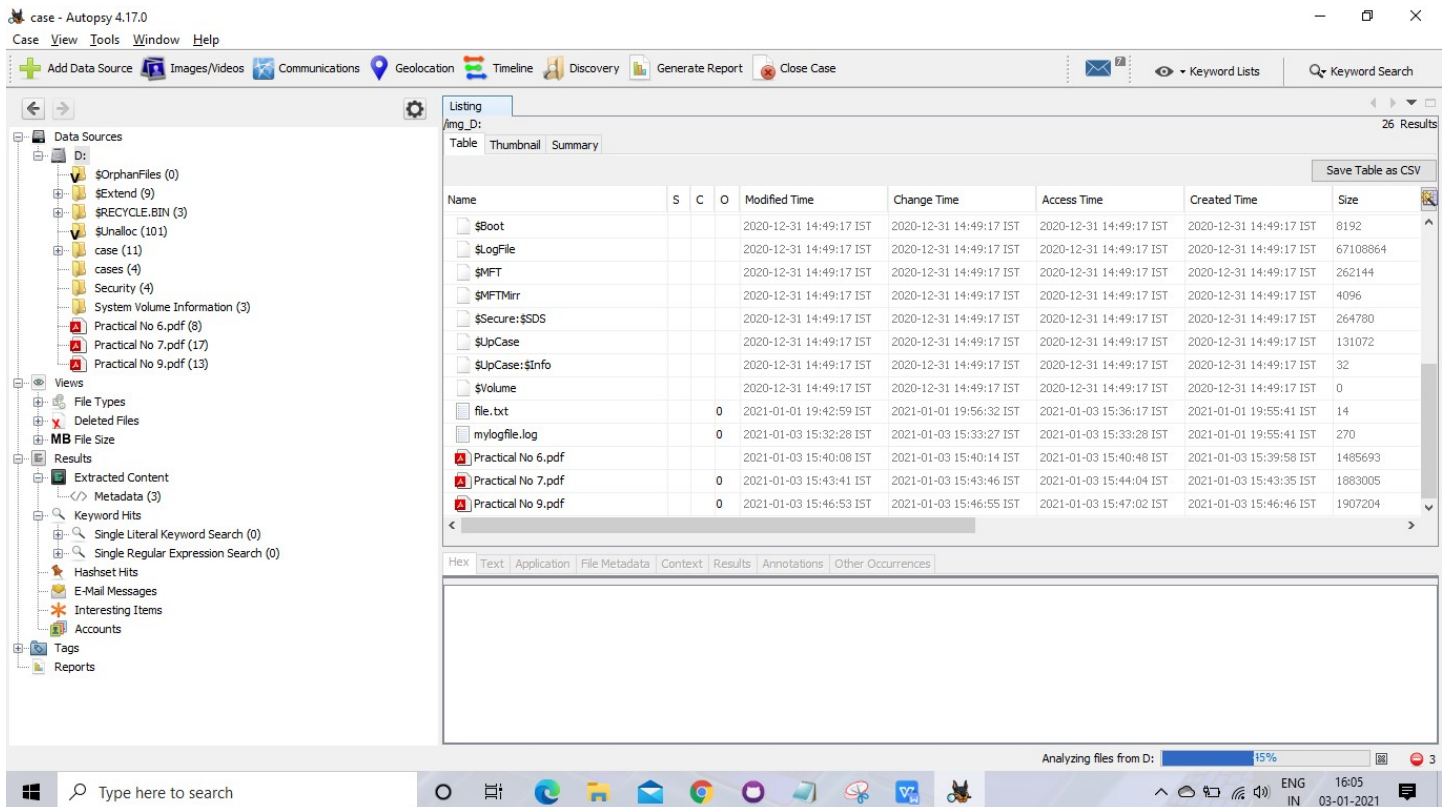
Click on Next Button.



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.

The screenshot shows the Autopsy 4.17.0 interface. The left sidebar displays the 'Data Sources' tree with 'Security (4)' selected. The main pane shows the 'Listing' view for the file 'file.txt'. The table below lists the files found in the selected directory.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flag
[current folder]				2021-01-01 19:52:25 IST	2021-01-01 19:52:25 IST	2021-01-03 15:56:38 IST	2021-01-01 19:47:42 IST	264	Allocated	Alloc
[parent folder]				2021-01-03 16:00:02 IST	2021-01-03 16:00:02 IST	2021-01-03 16:01:10 IST	2020-12-31 14:49:17 IST	56	Allocated	Alloc
file.txt			0	2021-01-01 19:42:59 IST	2021-01-01 19:52:23 IST	2021-01-01 21:39:55 IST	2021-01-01 19:42:12 IST	14	Allocated	Alloc
mylogfile.log			0	2021-01-01 19:29:00 IST	2021-01-01 19:52:25 IST	2021-01-01 20:30:40 IST	2021-01-01 19:29:00 IST	135	Allocated	Alloc

The bottom pane shows the 'Text' view of the selected file 'file.txt', displaying the content 'hihi how r u' and a section labeled '-----METADATA-----'.

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.

The screenshot shows the Autopsy 4.17.0 interface with the 'Deleted Files' view selected in the left sidebar. The main pane shows the 'Listing' view for the file 'file.txt'. A context menu is open over the file, showing the 'Extract File(s)' option.

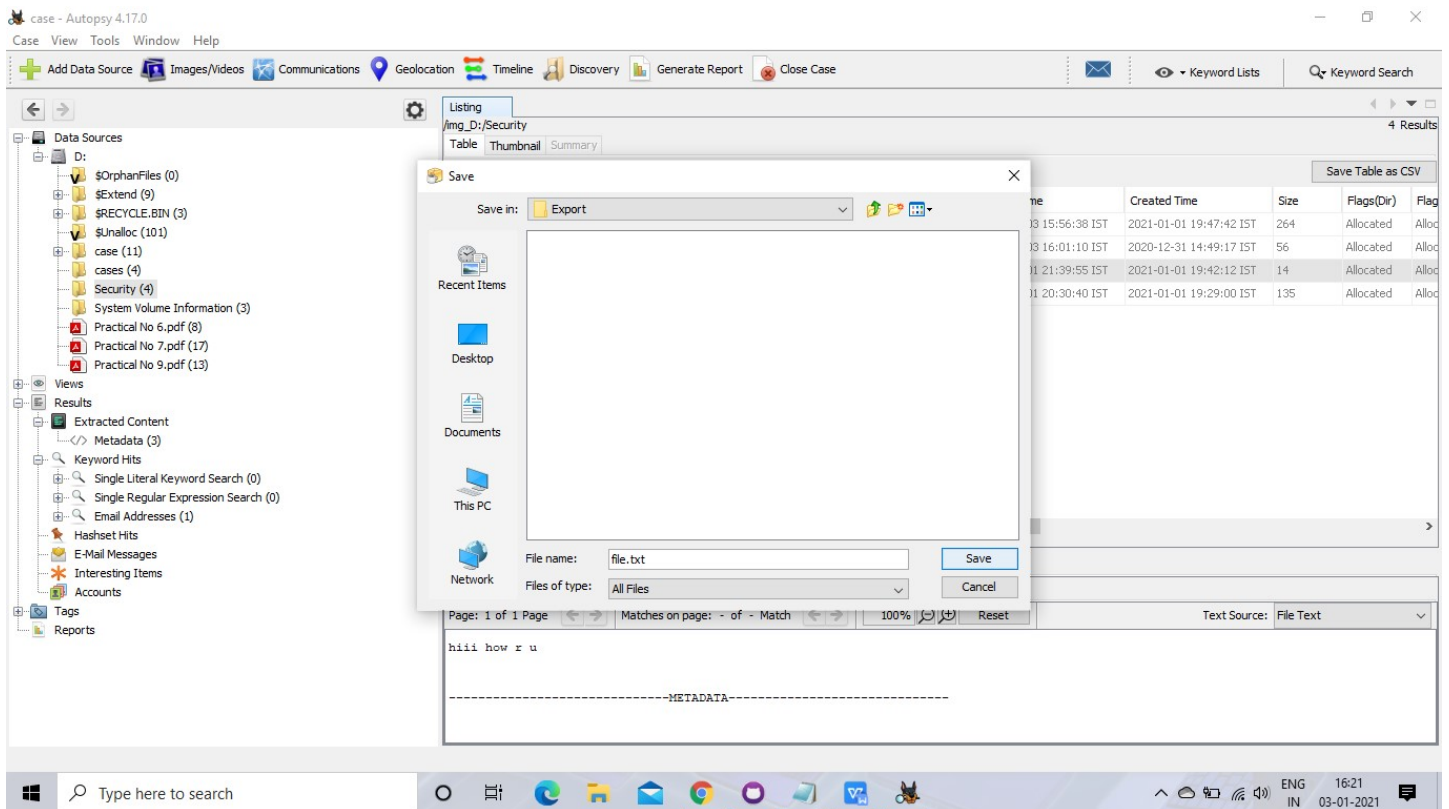
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flag
[current folder]				2021-01-01 19:52:25 IST	2021-01-01 19:52:25 IST	2021-01-03 15:56:38 IST	2021-01-01 19:47:42 IST	264	Allocated	Alloc
[parent folder]				2021-01-03 16:00:02 IST	2021-01-03 16:00:02 IST	2021-01-03 16:01:10 IST	2020-12-31 14:49:17 IST	56	Allocated	Alloc
file.txt			0	2021-01-01 19:42:59 IST	2021-01-01 19:52:23 IST	2021-01-01 21:39:55 IST	2021-01-01 19:42:12 IST	14	Allocated	Alloc
mylogfile.log			0	2021-01-01 19:29:00 IST	2021-01-01 19:52:25 IST	2021-01-01 20:30:40 IST	2021-01-01 19:29:00 IST	135	Allocated	Alloc

The context menu is open over the file 'file.txt', showing the following options:

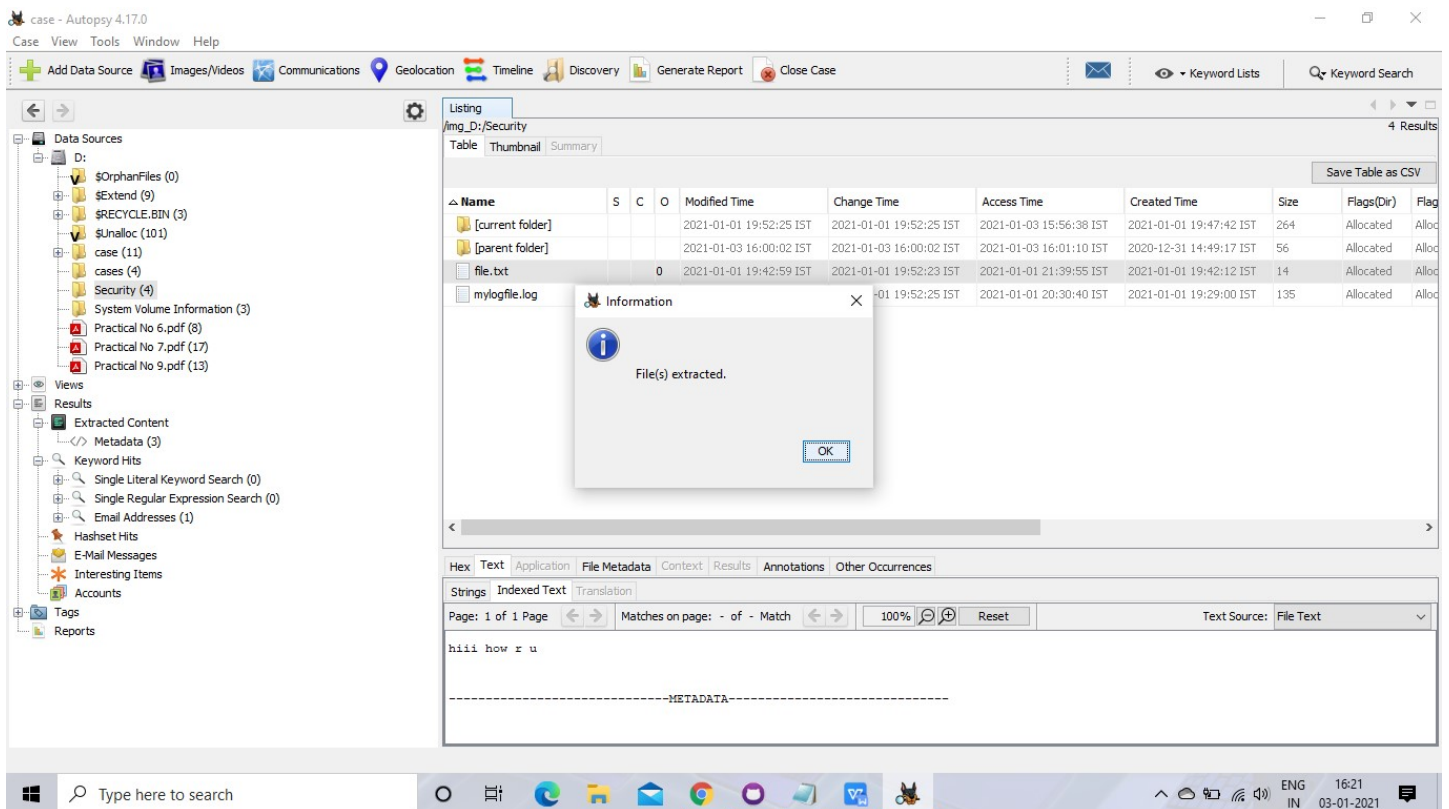
- Properties
- View in New Window
- Open in External Viewer Ctrl+E
- View File in Timeline...
- Extract File(s)**
- Export selected rows to CSV
- Add File Tag
- Remove File Tag
- Add/Edit Central Repository Comment
- Add File to Hash Set

The bottom pane shows the 'Text' view of the selected file 'file.txt', displaying the content 'hihi how r u' and a section labeled '-----METADATA-----'.

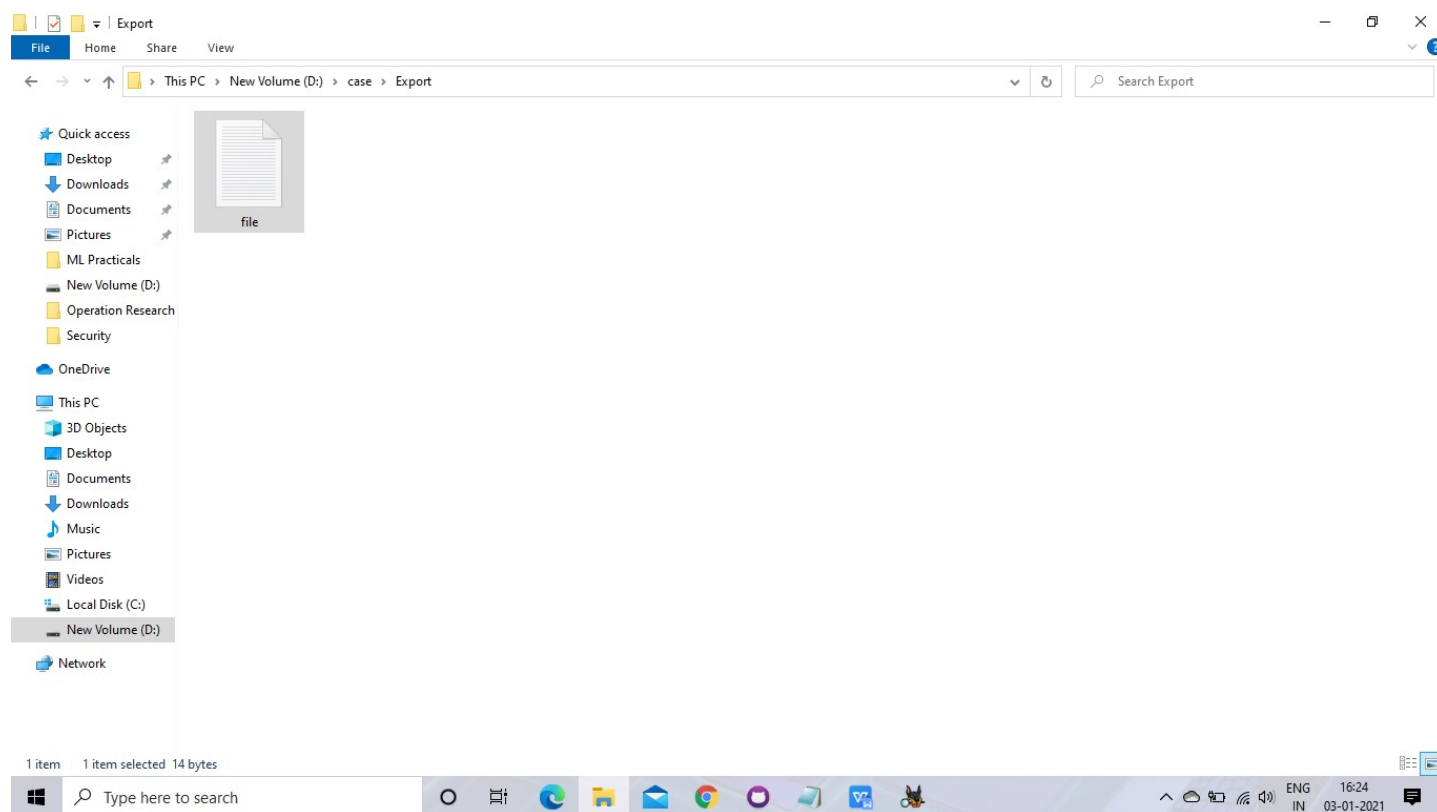
By default Export folder is choose to save the recovered file.



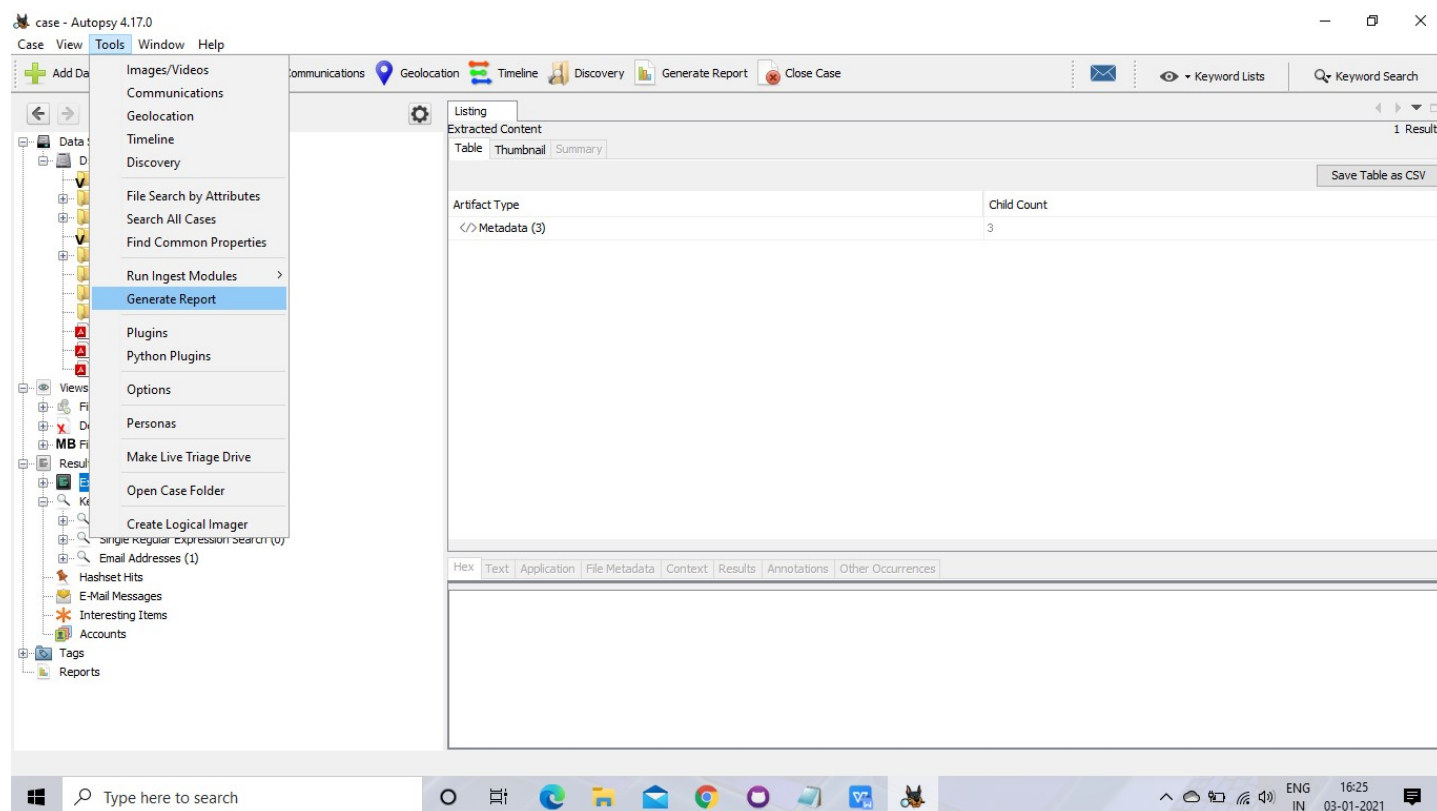
Now Click on Ok.

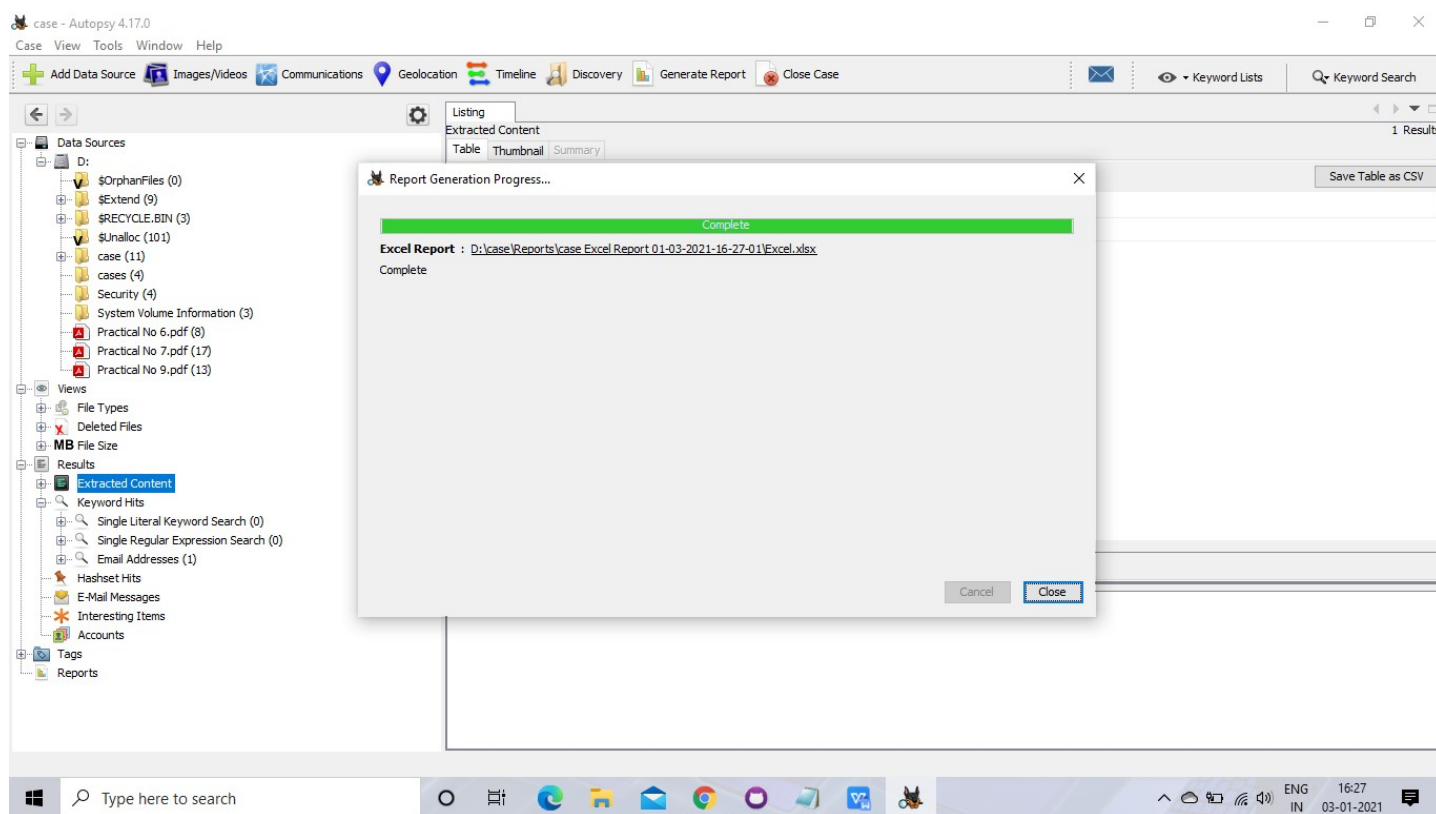
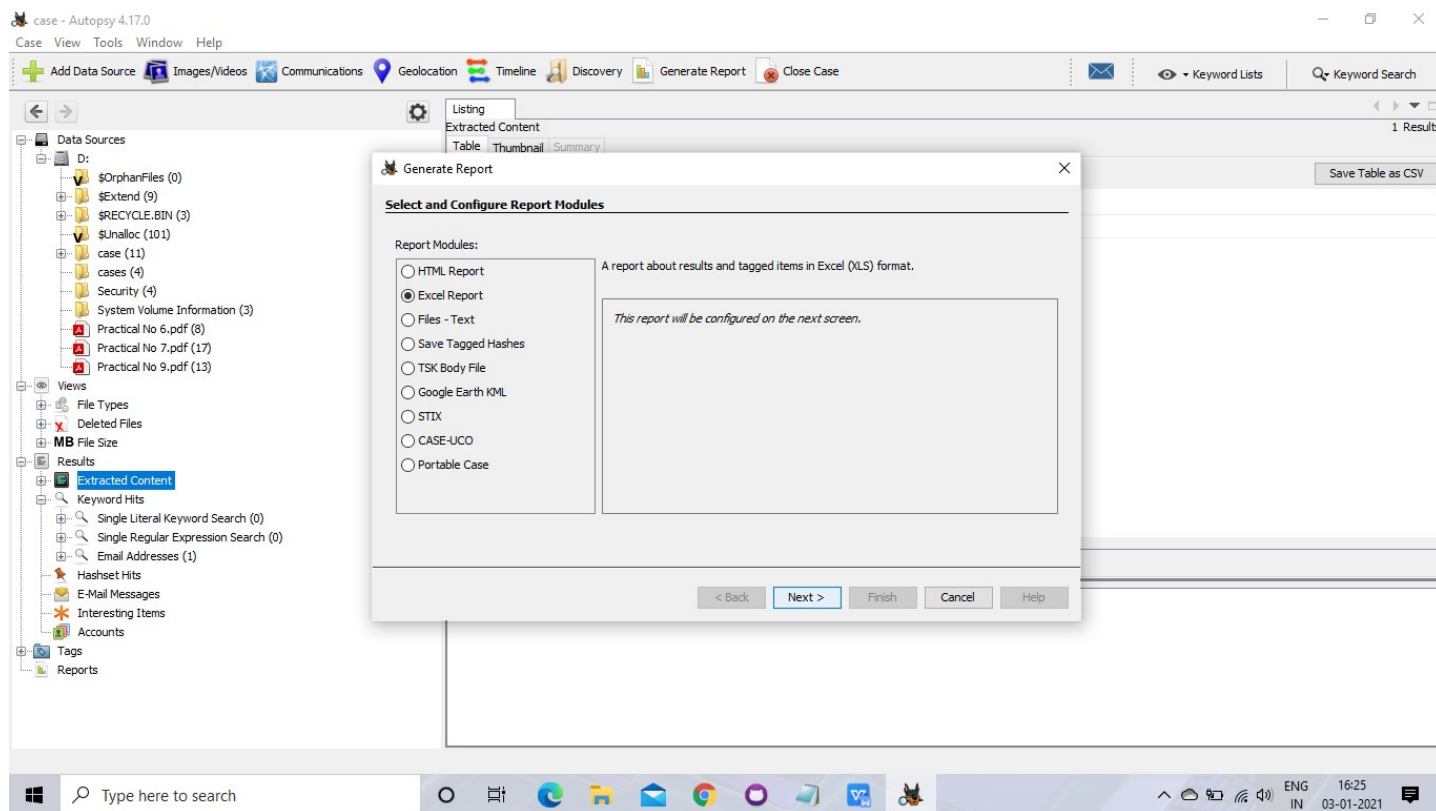


Now go to the Export Folder to view Recover file.



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





The screenshot shows the Autopsy 4.17.0 interface. On the left is a tree view of data sources and results. The main pane displays a 'Listing' table with the following data:

Source Module Name	Report Name	Created Time	Report File Path
Excel Report		2021-01-03 16:27:03 IST	D:\case\Reports\case Excel Report 01-03-2021-16-27-01\Excel.xlsx

Below the table, a tabbed interface shows 'Context' selected, displaying the text: 'Displays context for selected file.'

Excel - Excel (Unlicensed Product)

File Home Insert Page Layout Formulas Data Review View Help Tell me what you want to do

Clipboard Font Alignment Number Styles Cells Editing

NOTICE Most features are disabled because your Office product is inactive. To use for free, sign in and use the Web version. [Activate](#) [Use free at Office.com](#)

Summary

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	Summary																		
2																			
3	Case Name:	case																	
4	Case Number:	case01																	
5	Number of data sources in case:	1																	
6	Examiner:	abc																	
7																			
8																			
9																			
10																			
11																			
12																			
13																			
14																			
15																			
16																			
17																			
18																			
19																			
20																			

Summary Keyword Hits Metadata Tagged Files Tagged Results

Type here to search

ENG IN 16:28 03-01-2021