

Practical 8

Aim: - Recovering and inspecting deleted files.

Step 1: Open Autopsy and “Run as Admin” then create a new Case

New Case Information

Steps

1. **Case Information**
2. Optional Information

Case Information

Case Name:

Base Directory:

Case Type: ☒ Single-user ☐ Multi-user

Case data will be stored in the following directory:

Step 2: Fill in the Information as show below

New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number:

Examiner

Name:

Phone:

Email:

Notes:

Organization

Organization analysis is being done for:

Step 3: Select local disk and click next

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 Type of Data Source To Add

☐ Disk Image or VM File

☒ Local Disk

☐ Logical Files

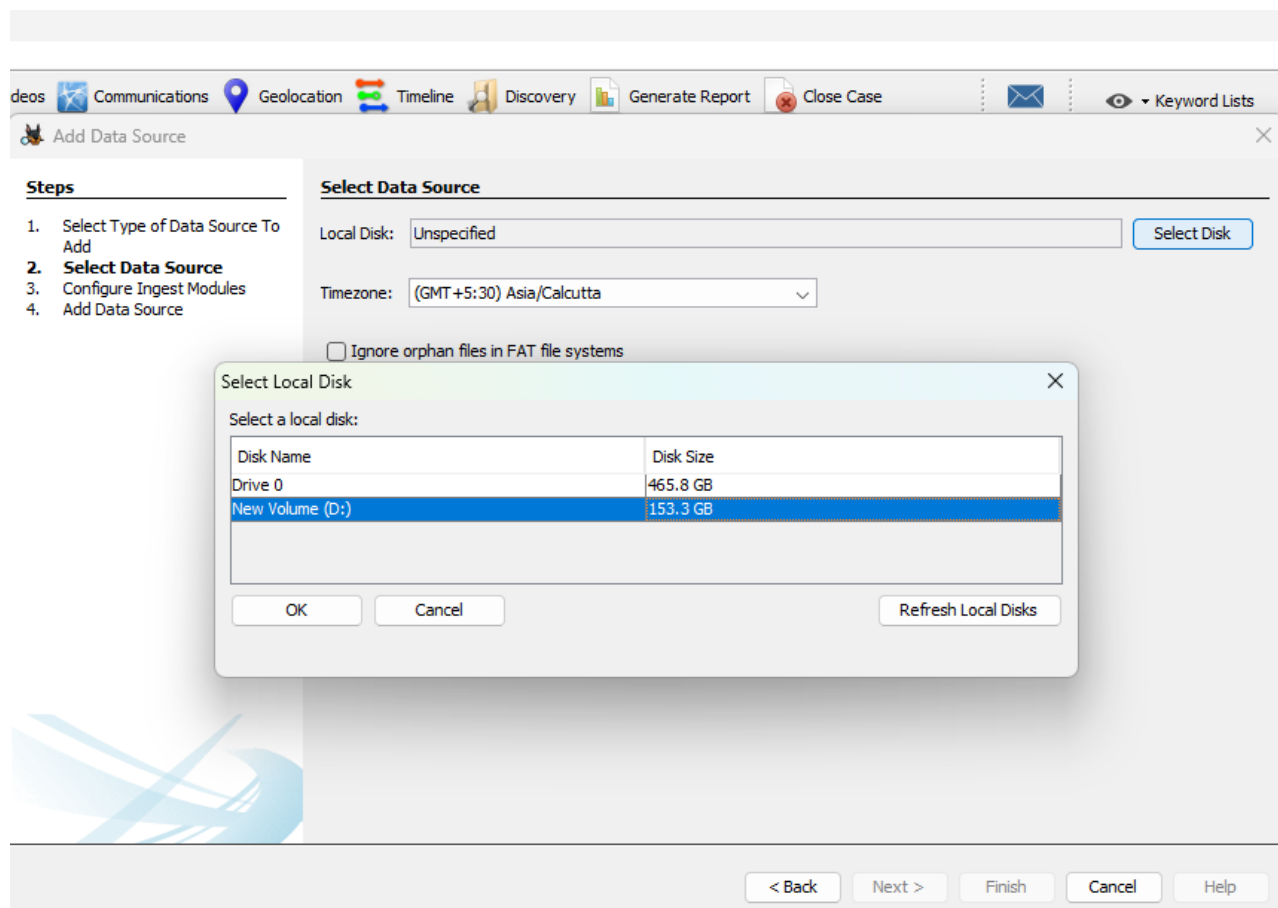
☐ Unallocated Space Image File

☐ Autopsy Logical Imager Results

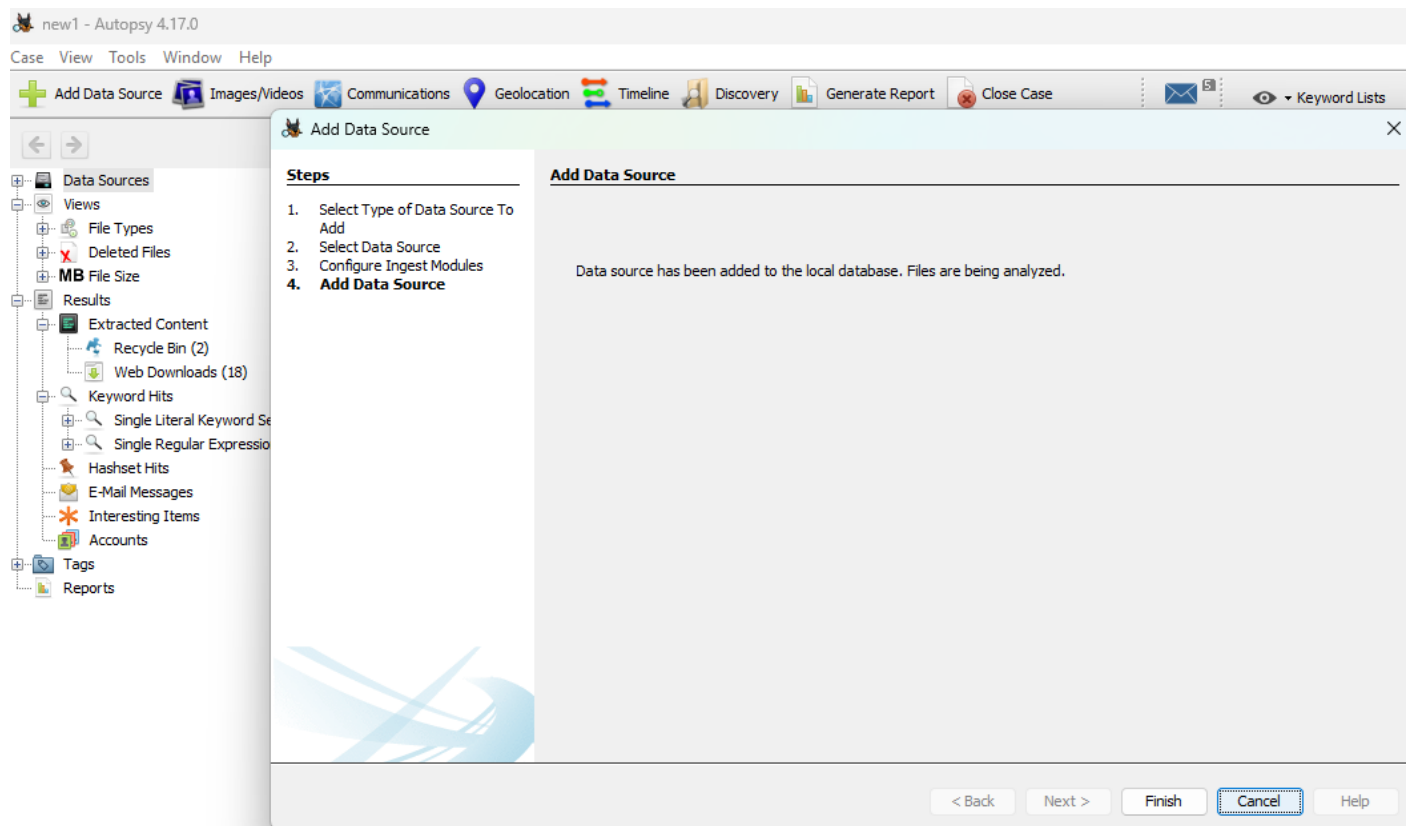
☐ XRY Text Export

< Back **Next >** Finish Cancel Help

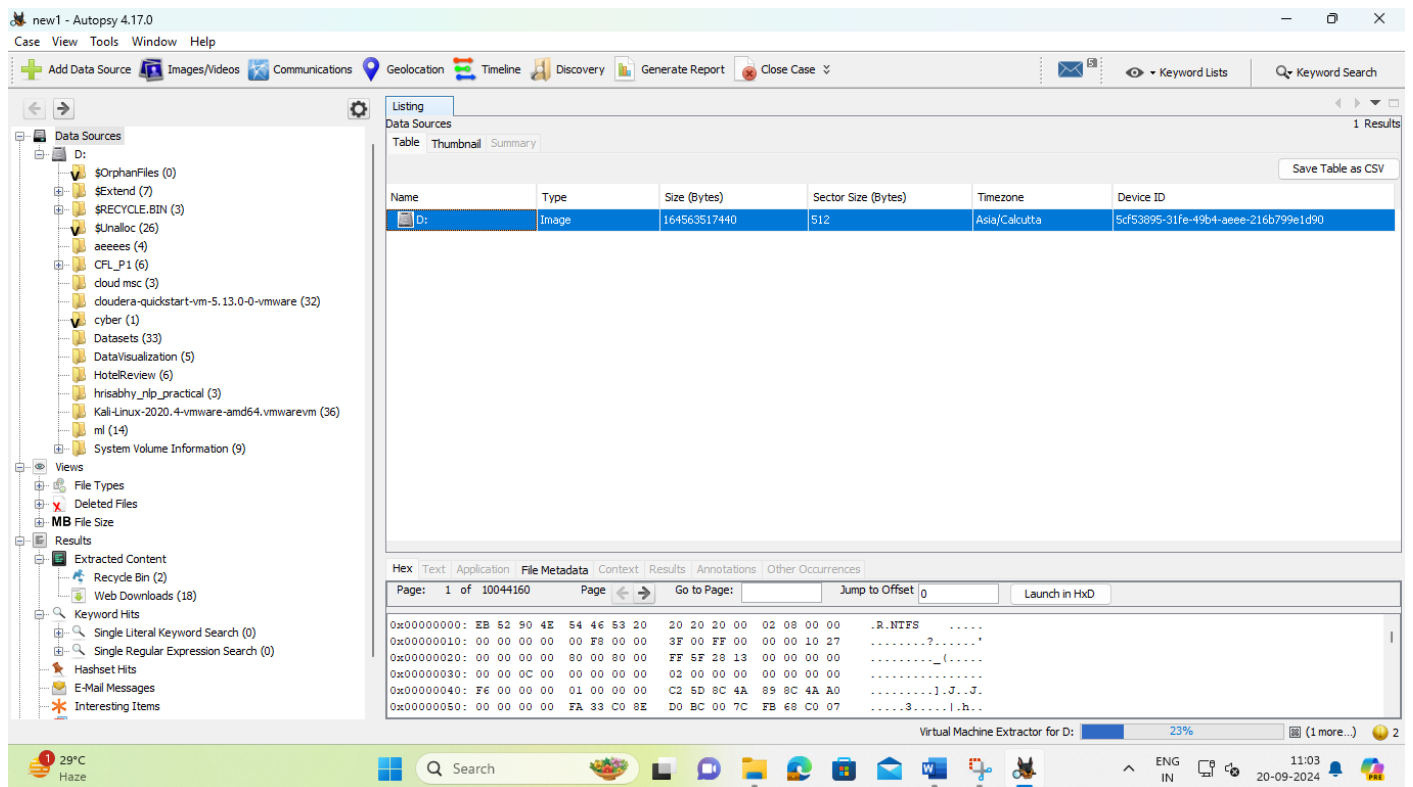
Step 4: Select Disk



Step 5: Select all checkbox's and click on next then finish



Step 6: Click on D to open the contents of the Drive

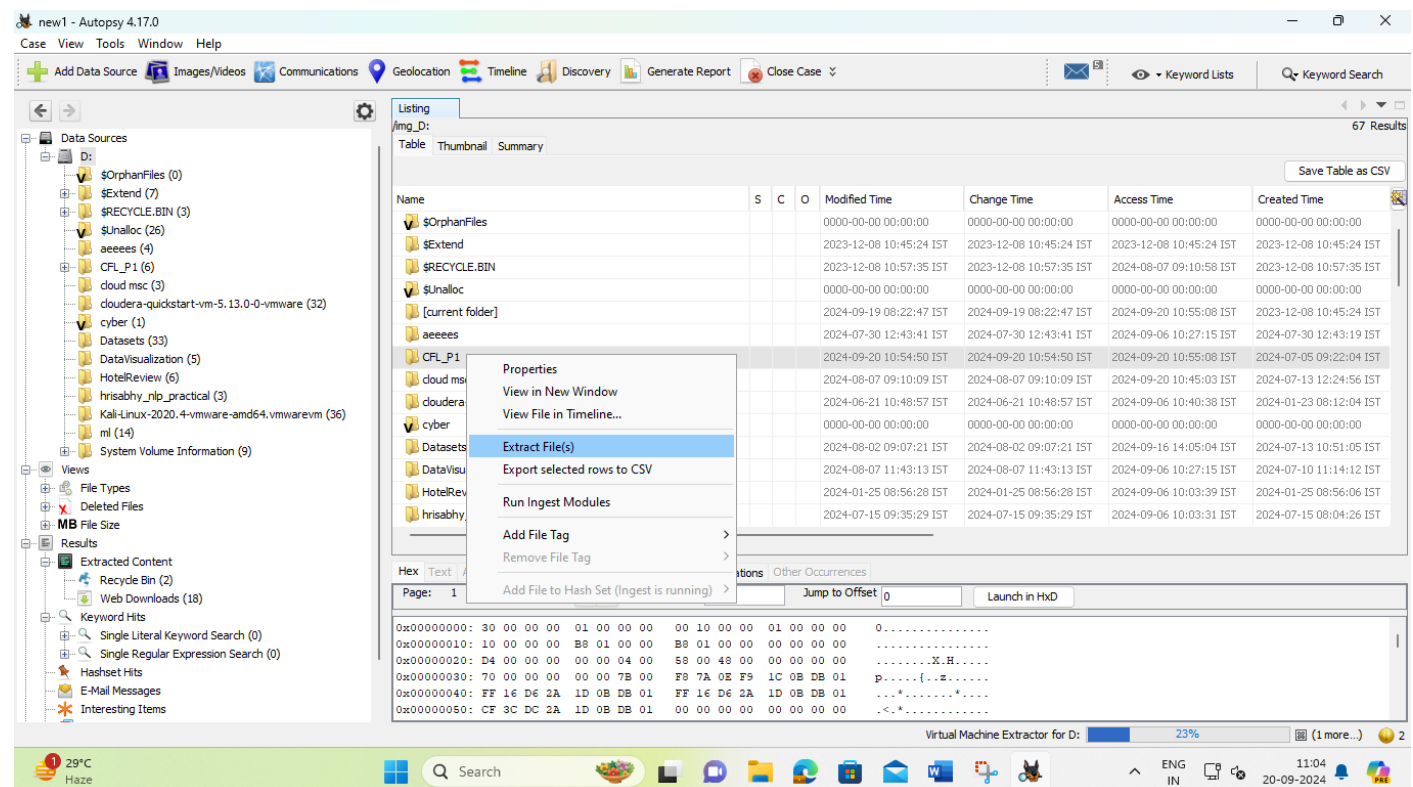


The screenshot shows the Autopsy 4.17.0 interface. On the left, the 'Data Sources' pane shows the 'D:' drive selected. The main window displays a table with 1 result for 'D:'.

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
D:	Image	164563517440	512	Asia/Calcutta	5cf53895-31fe-49b4-aeec-216b799e1d90

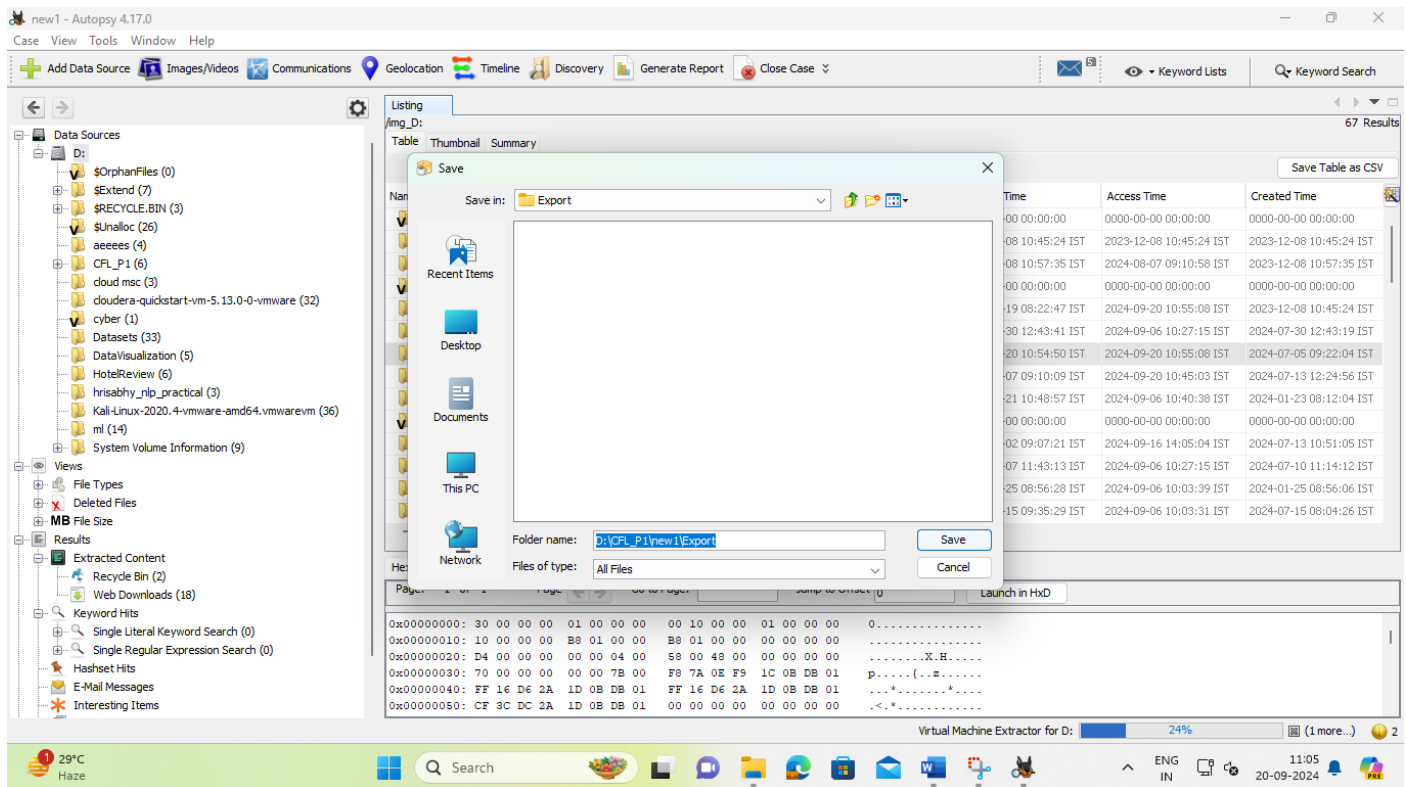
The bottom pane shows the hex view of the drive's metadata, including file names like 'R.NTFS' and '3'.

Step 7: Select any folder and right click on it and select Export files.



The screenshot shows the Autopsy 4.17.0 interface. On the left, the 'Data Sources' pane shows the 'D:' drive selected. The main window displays a table with 67 results for 'D:'. A context menu is open over the 'CFL_P1' folder, with 'Extract File(s)' selected.

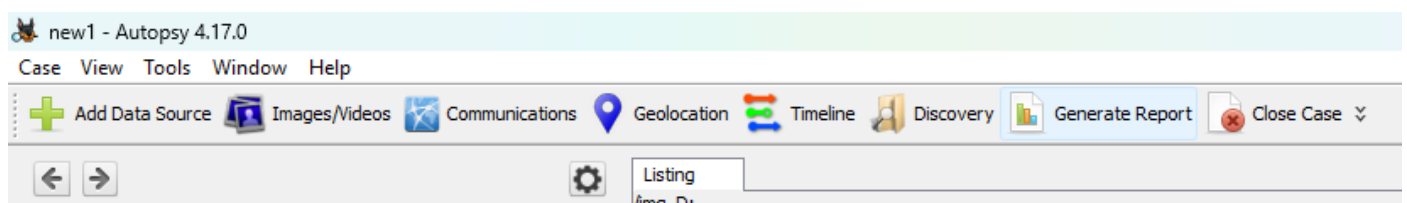
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
\$OrphanFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
\$Extend				2023-12-08 10:45:24 IST	2023-12-08 10:45:24 IST	2023-12-08 10:45:24 IST	2023-12-08 10:45:24 IST
\$RECYCLE.BIN				2023-12-08 10:57:35 IST	2023-12-08 10:57:35 IST	2024-08-07 09:10:58 IST	2023-12-08 10:57:35 IST
\$Unalloc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
[current folder]				2024-09-19 08:22:47 IST	2024-09-19 08:22:47 IST	2024-09-20 10:55:08 IST	2023-12-08 10:45:24 IST
aecees				2024-07-30 12:43:41 IST	2024-07-30 12:43:41 IST	2024-09-06 10:27:15 IST	2024-07-30 12:43:19 IST
CFL_P1				2024-09-20 10:54:50 IST	2024-09-20 10:54:50 IST	2024-09-20 10:55:08 IST	2024-07-05 09:22:04 IST
cloud msc				2024-08-07 09:10:09 IST	2024-08-07 09:10:09 IST	2024-09-20 10:45:03 IST	2024-07-13 12:24:56 IST
cloudera				2024-06-21 10:48:57 IST	2024-06-21 10:48:57 IST	2024-09-06 10:40:38 IST	2024-01-23 08:12:04 IST
cyber				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Datasets				2024-08-02 09:07:21 IST	2024-08-02 09:07:21 IST	2024-09-16 14:05:04 IST	2024-07-13 10:51:05 IST
DataVisu				2024-08-07 11:43:13 IST	2024-08-07 11:43:13 IST	2024-09-06 10:27:15 IST	2024-07-10 11:14:12 IST
HotelRev				2024-01-25 08:56:28 IST	2024-01-25 08:56:28 IST	2024-09-06 10:03:39 IST	2024-01-25 08:56:06 IST
hrisabhy				2024-07-15 09:35:29 IST	2024-07-15 09:35:29 IST	2024-09-06 10:03:31 IST	2024-07-15 08:04:26 IST



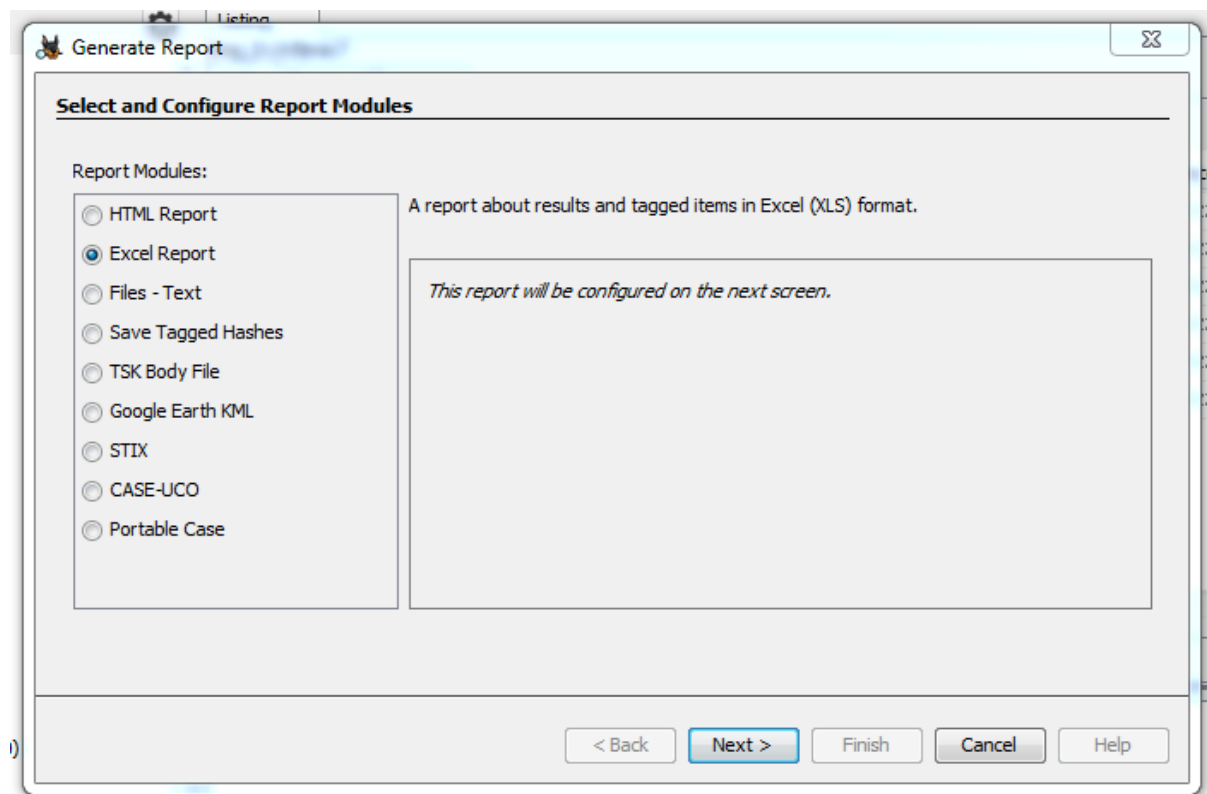
Output:

This PC > New Volume (D:) > CFL_P1 > new1 > Export > 76-CFL_P1 > new1 >				
Sort View ...				
Name	Date modified	Type	Size	
Cache	20-09-2024 11:11	File folder		
Export	20-09-2024 11:11	File folder		
Log	20-09-2024 11:11	File folder		
ModuleOutput	20-09-2024 11:11	File folder		
Reports	20-09-2024 11:11	File folder		
autopsy	20-09-2024 11:11	Data Base File	0 KB	
autopsy.db-journal	20-09-2024 11:11	DB-JOURNAL File	9 KB	
autopsy.db-journal-slack	20-09-2024 11:11	DB-JOURNAL-SLA...	3 KB	
autopsy.db-slack	20-09-2024 11:11	DB-SLACK File	0 KB	
new1.aut	20-09-2024 11:11	AUT File	1 KB	
new1.aut-slack	20-09-2024 11:11	AUT-SLACK File	4 KB	
SolrCore	20-09-2024 11:11	Properties Source ...	1 KB	

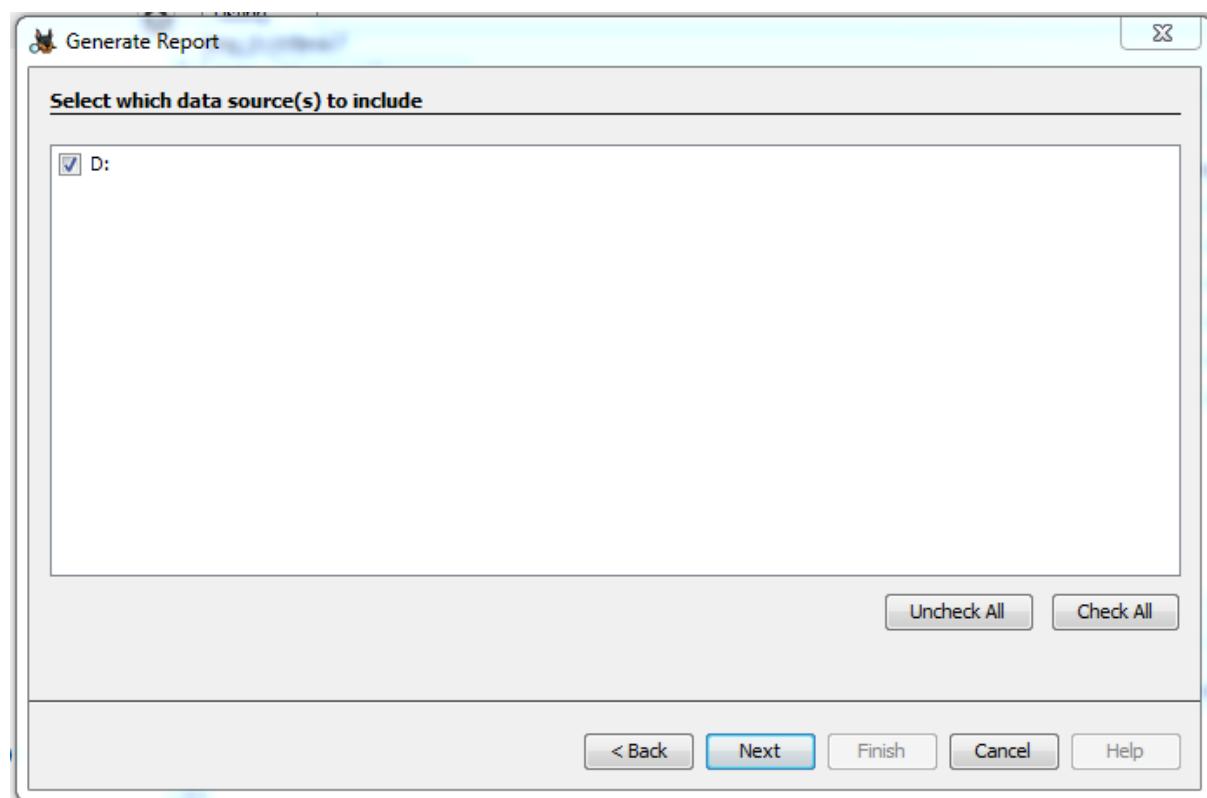
Step 8: Click on generate report



Step 9: Select Excel Report



Step 10: Select D then next and then select All results



Generate Report

Configure Report

Select which data to report on:

☒ All Results
☐ All Tagged Results
☐ Specific Tagged Results

Output:

Computer > Local Disk (D:) > cfprac8 > Recover Files > Reports > Recover Files Excel Report 07-13-2022-12-14-26

Name	Date modified	Type	Size
Excel	13-07-2022 12:14	Microsoft Office E...	7 KB

Clipboard		Font		Align
A1		Summary		
	A	B	C	
1	Summary			
2				
3	Case Name:	Recover Files		
4	Case Number:	26		
5	Number of data sources in case:		1	
6	Case Notes:	recovery of deleted data		
7	Examiner:	Michael Winston		
8				
9				
10				
11				

