

EXPERIMENT NO: 03 (ii)

File Recovery using open-source tool - Autopsy

Aim: To perform File Recovery using open-source tool - Autopsy

Theory:

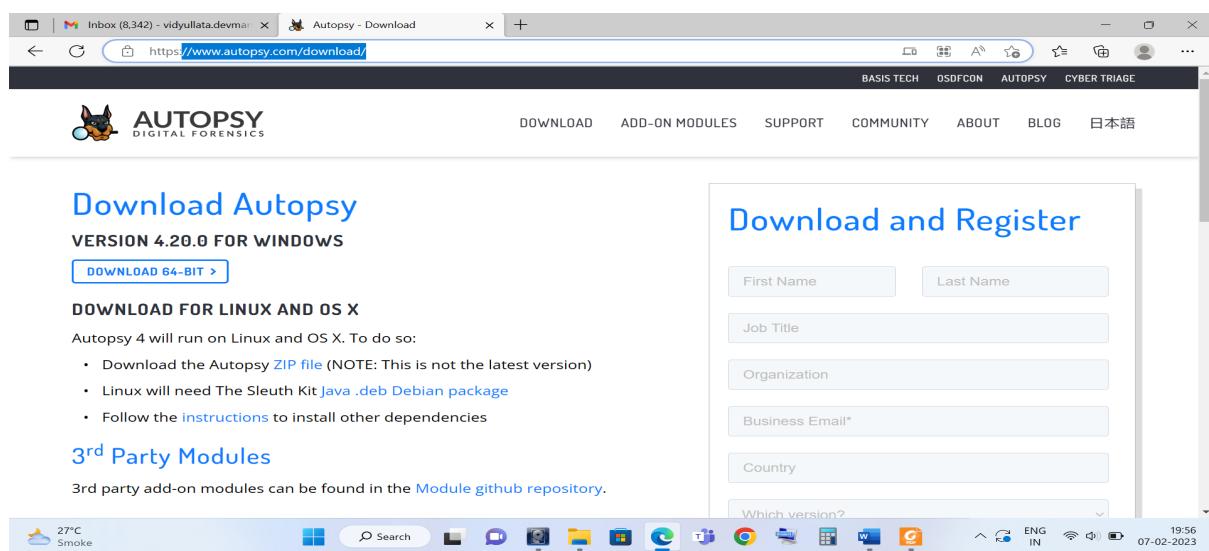
Files that are "deleted" remain on the storage medium until overwritten. This means that if the suspect deleted evidence files, until they are overwritten by the file system, they remain available to us to recover.

In this lab, we will be using the open-source The Sleuth Kit (TSK) for identifying and recovering deleted files. The Sleuth Kit was first developed for Linux, but has now been ported for Windows, so we will be using it with our Windows examination system. A GUI interface was developed for TSK named Autopsy that we will be using in this tutorial.

AUTOPSY Installation:

<http://www.autopsy.com/download/>

1. Select download for Windows

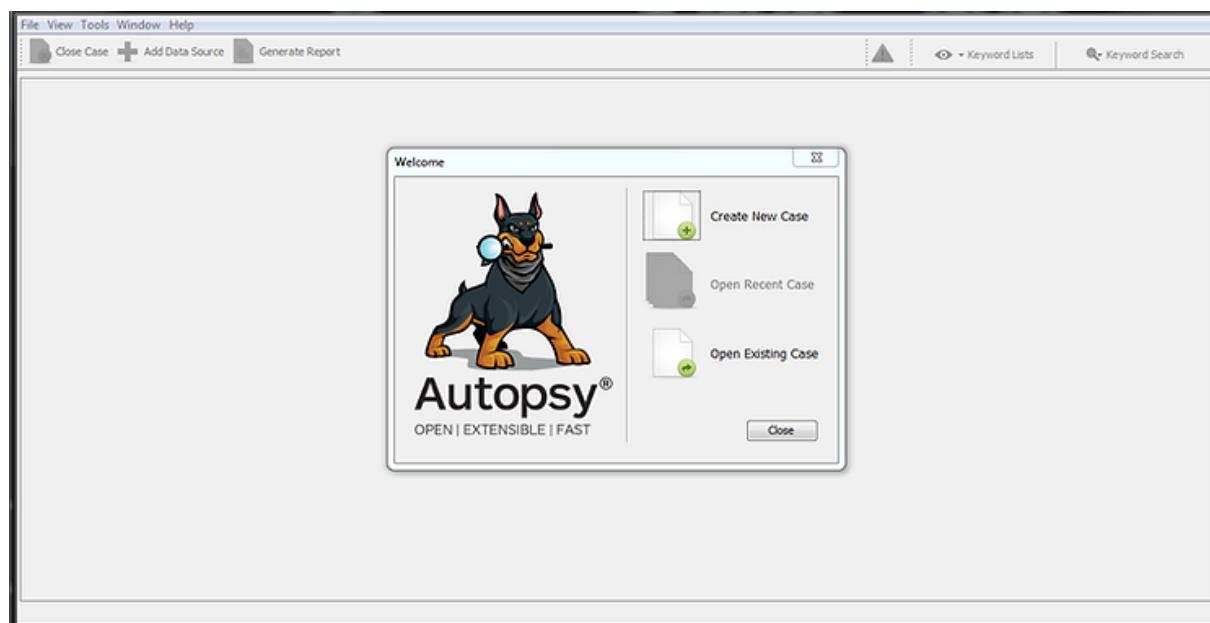


2. Fill the form & submit
3. Download 64 bit & install

The screenshot shows a web browser window with the URL <https://www.autopsy.com/download/>. The page has a header with the Autopsy logo and navigation links. Below the header, there's a section for 'Download Autopsy VERSION 4.20.0 FOR WINDOWS' with a 'DOWNLOAD 64-BIT >' button. Another section for 'DOWNLOAD FOR LINUX AND OS X' provides instructions for running Autopsy on those platforms. To the right, there's a box for 'Download and Register' with a link to 'Download Version 4.20.0 for Windows'. The browser's address bar shows 'Inbox (8,342) - vidyullata.devmar...' and the status bar shows system information like '27°C Smoke' and the date '07-02-2023'.

File Recovery Steps:

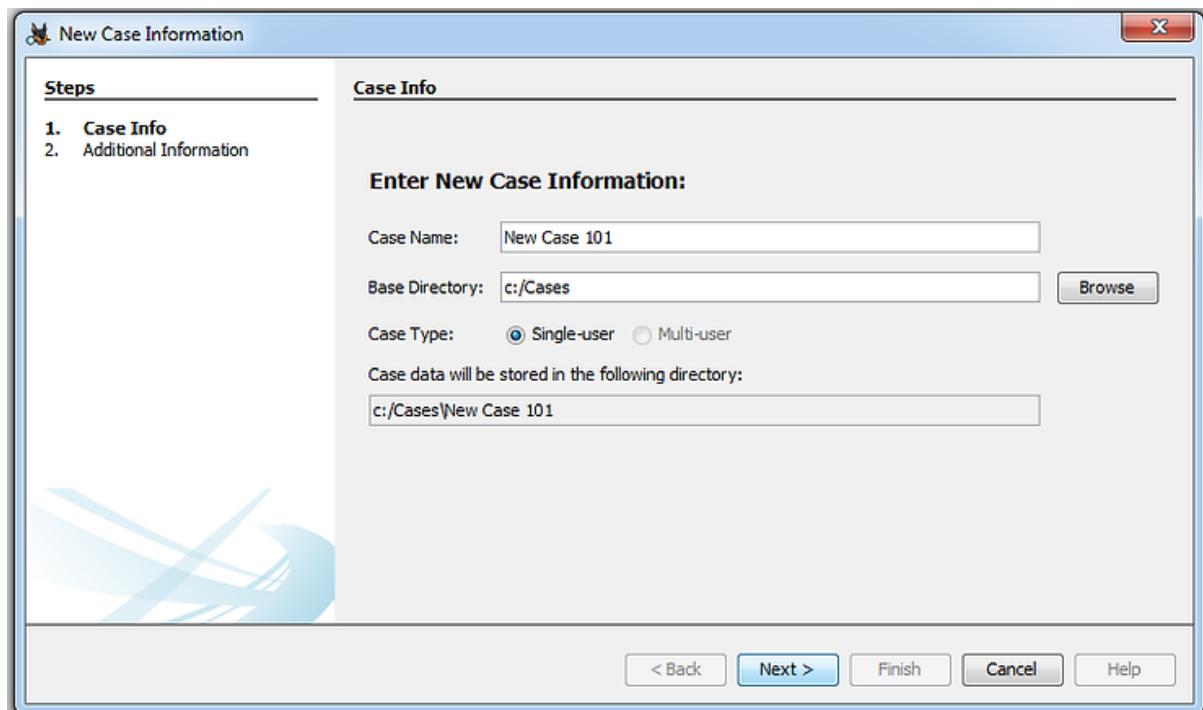
1. Install Autopsy on your system.



After installing Autopsy then starting it, you will be greeted with a screen similar to the above.

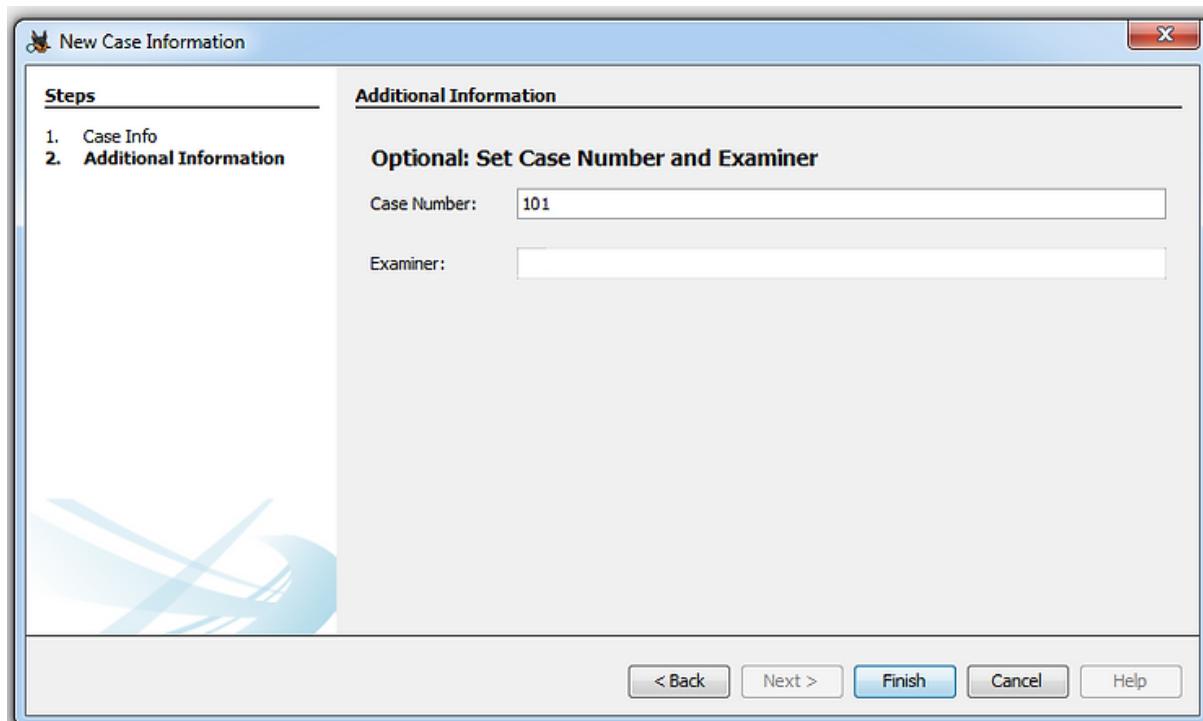
2. Click "Create New Case".

When you do, you will be greeted by a new window asking you to name your new case and what directory you want to place your cases. Enter "New Case 101" and put it in the base directory of C:\Cases.



3. Now, hit **Next**.

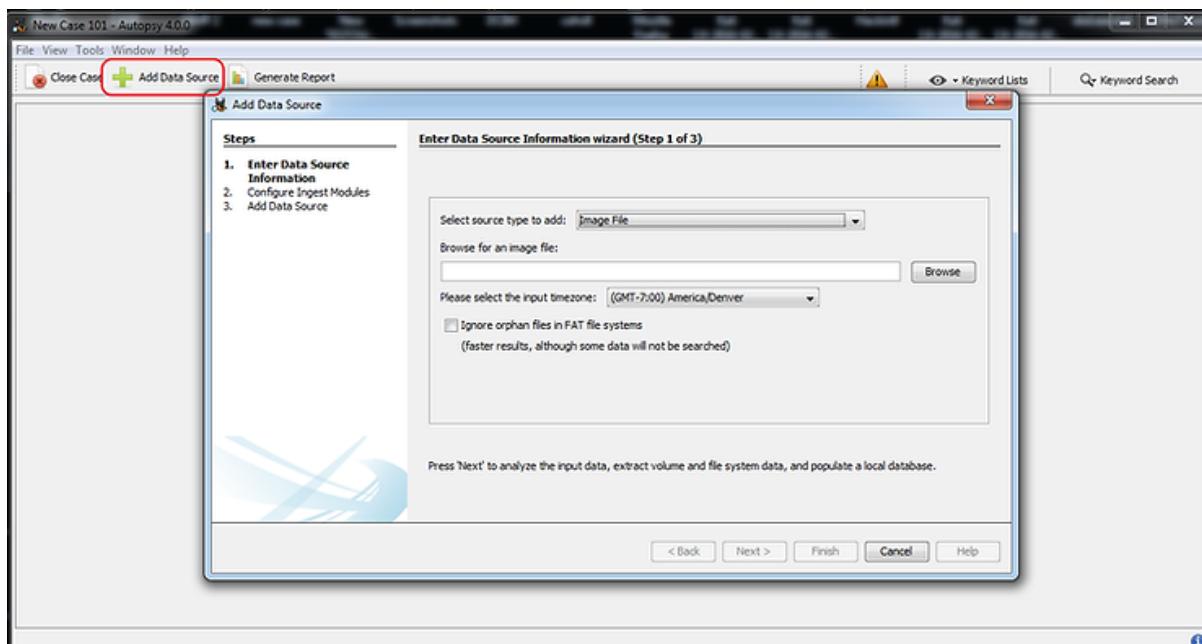
This will open another window asking you for a case number and the examiner name. Give it a case number of 101 and your name or initials for the examiner.



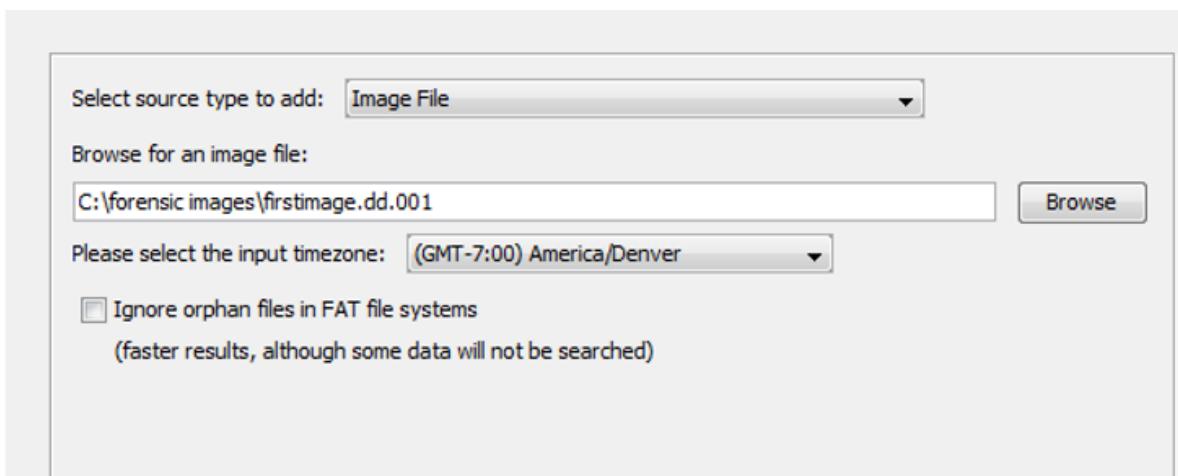
4. Click "**Finish**".

Next, click on "Add New Data" in the upper left corner. When you do, a "Add Data Source" window will open. Since we will be using the image file created in the previous module, select "Image File" and then Browse for

the image file you created in Module 1. I saved mine in a directory c:\forensic images. Yours may be different.

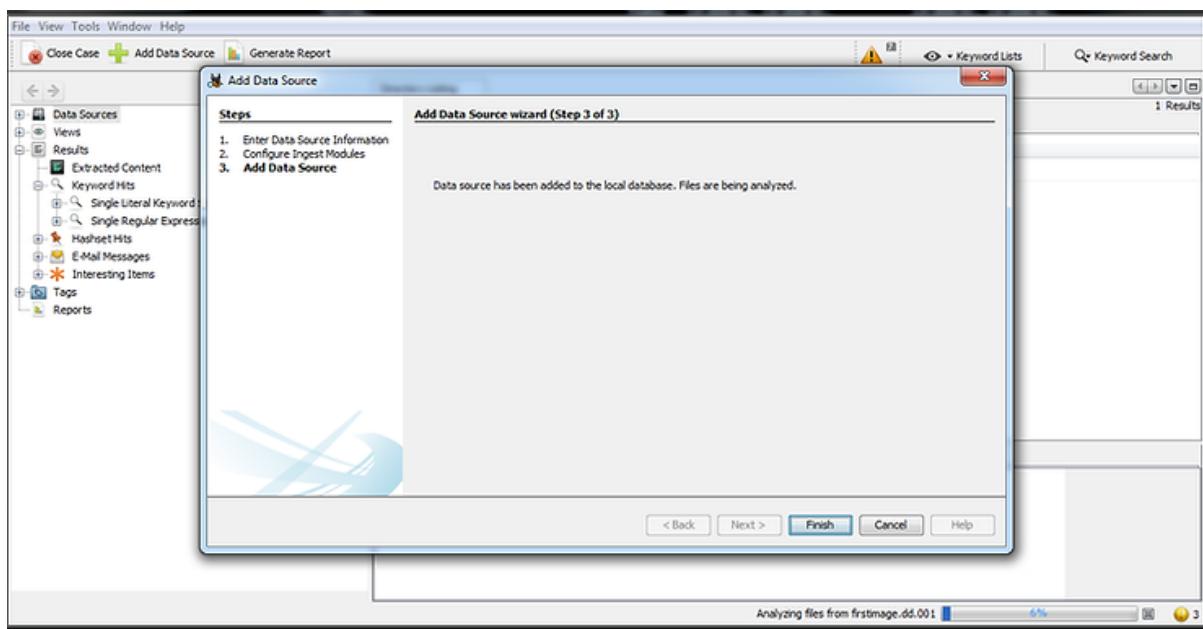


5. Now, add our first.image.dd.001 image from the first tutorial in this series.

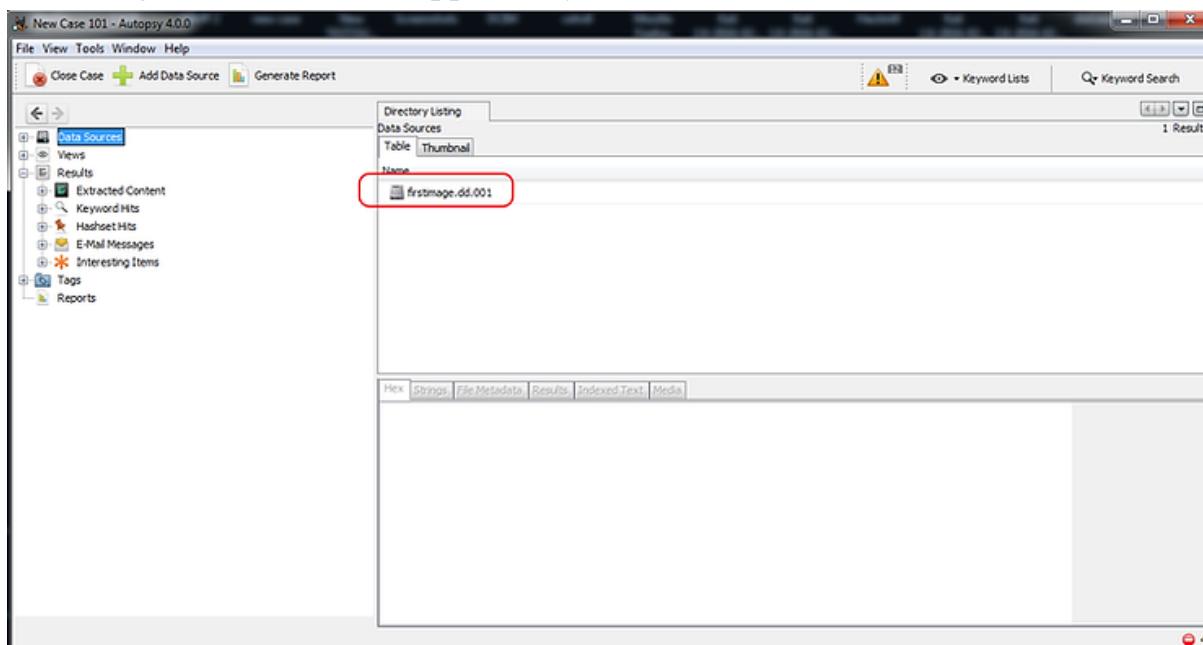


After adding the image click next and Autopsy will begin to do its analysis of the image. Eventually, you will be greeted by a screen like that below.

6. Click "Finish".



Now, you should see an interface like that below. Note that your "firstimage.dd.001" should appear as your data source.



If we expand the "File Types" in the object explorer, Autopsy will display all the file types and the number of files in each category. Below you can see I clicked on the "Images" file type and Autopsy will display all the Image files.

New Case 101 - Autopsy 4.0.0

File View Tools Window Help

Close Case Add Data Source Generate Report

Directory Listing

Images

Table Thumbnail

Name Location Modified Time Change Time

Screenshot-1.png /img/_firstimage.dd.001/vol_vo2/Screenshot-1.png 2013-02-06 16:08:14 MST 0000-00-00 00:00
Screenshot-2.png /img/_firstimage.dd.001/vol_vo2/Screenshot-2.png 2013-02-06 16:24:56 MST 0000-00-00 00:00
Screenshot-3.png /img/_firstimage.dd.001/vol_vo2/Screenshot-3.png 2013-02-07 10:14:00 MST 0000-00-00 00:00
Screenshot-4.png /img/_firstimage.dd.001/vol_vo2/Screenshot-4.png 2013-02-07 10:14:30 MST 0000-00-00 00:00
Screenshot-5.png /img/_firstimage.dd.001/vol_vo2/Screenshot-5.png 2013-02-07 10:14:54 MST 0000-00-00 00:00
Screenshot-6.png /img/_firstimage.dd.001/vol_vo2/Screenshot-6.png 2013-02-07 10:15:46 MST 0000-00-00 00:00
snapshot1.png /img/_firstimage.dd.001/vol_vo2/snapshot1.png 2013-04-05 12:35:44 MDT 0000-00-00 00:00
Screenshot-9.png /img/_firstimage.dd.001/vol_vo2/Screenshot-9.png 2013-02-08 15:23:26 MST 0000-00-00 00:00

Analyzing files from firstimage.dd.001 100% 4

A little further below in the object explorer, we can see a File Type named "Deleted Files". When we click on it will display all the deleted files.

New Case 101 - Autopsy 4.0.0

File View Tools Window Help

Close Case Add Data Source Generate Report

Directory Listing

Data Sources

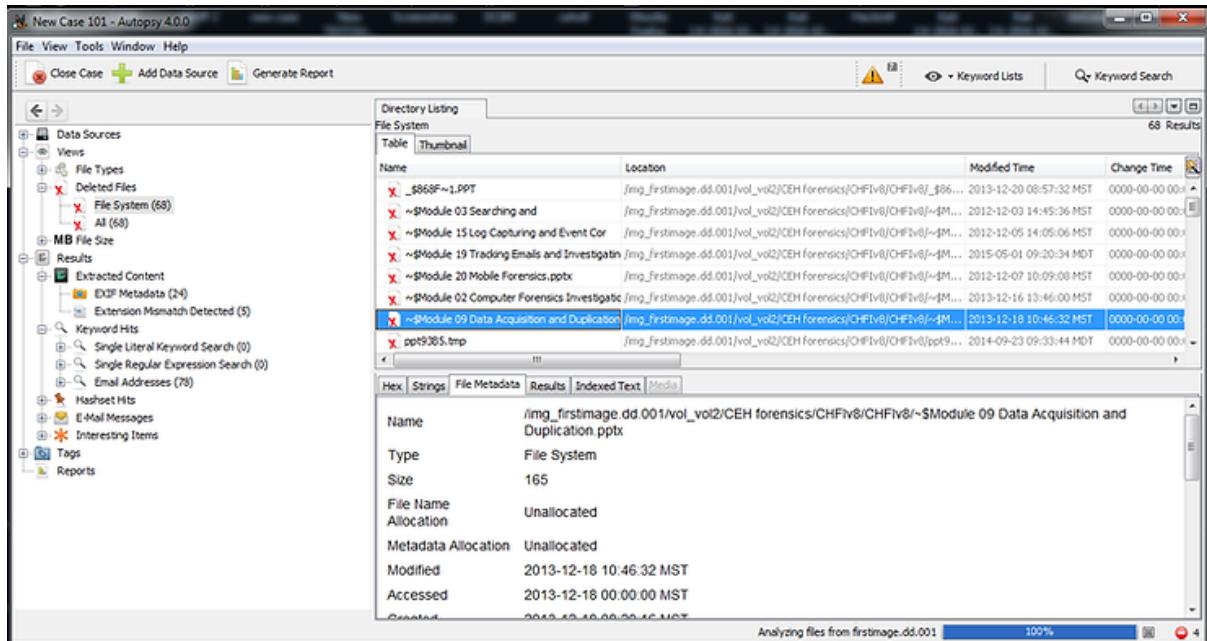
Table Thumbnail

Name

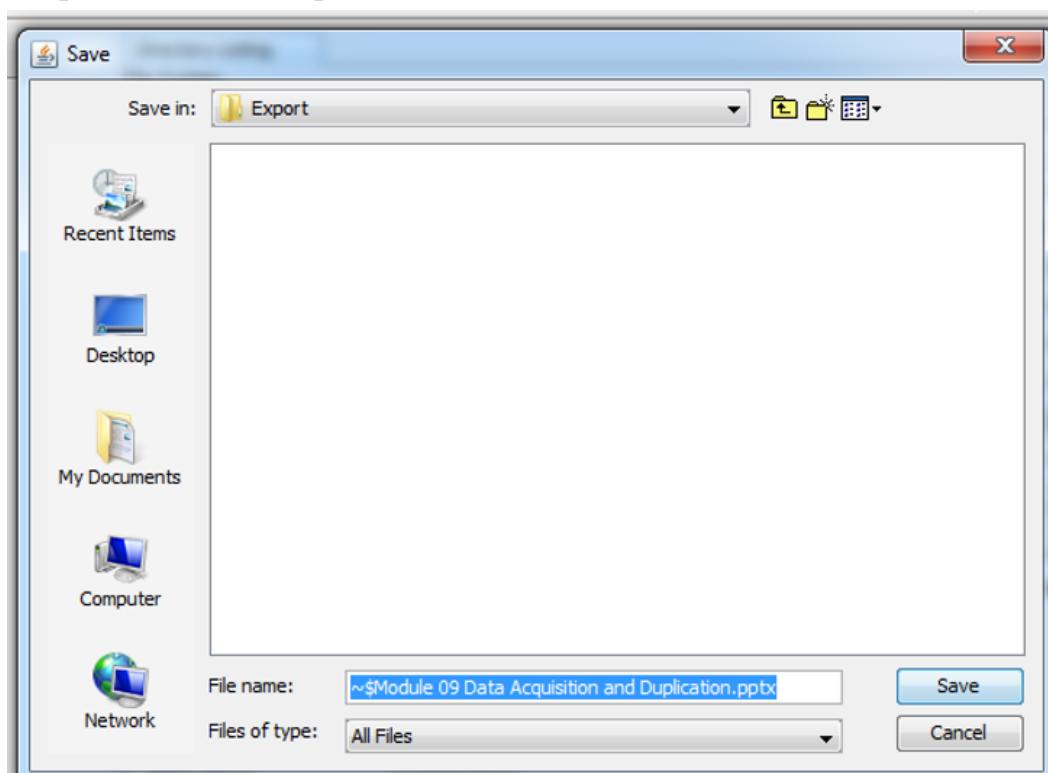
firstimage.dd.001

Hex Strings File Metadata Results Indexed Text

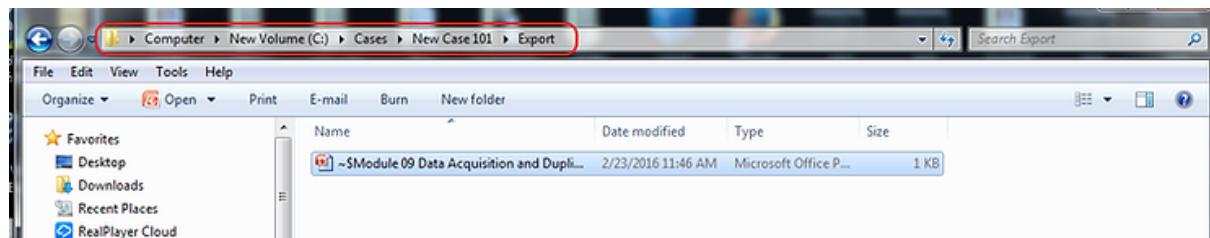
When we click on a deleted file, we can do some analysis in the lower right window. There you will see tabs labeled, Hex, Strings, File Metadata, Results and Indexed Text. In this case, click on the "File Metadata " tab and it will display the file's metadata including the name, type, size, modified, accessed and created (MAC).



Now, to recover the deleted file,right click on the deleted file and select "Export". This will open a window like that below.



Go ahead and save the deleted file into the **Export** sub-directory.
To find the exported/deleted file, navigate to;
C:\Cases\New Case 101\Export



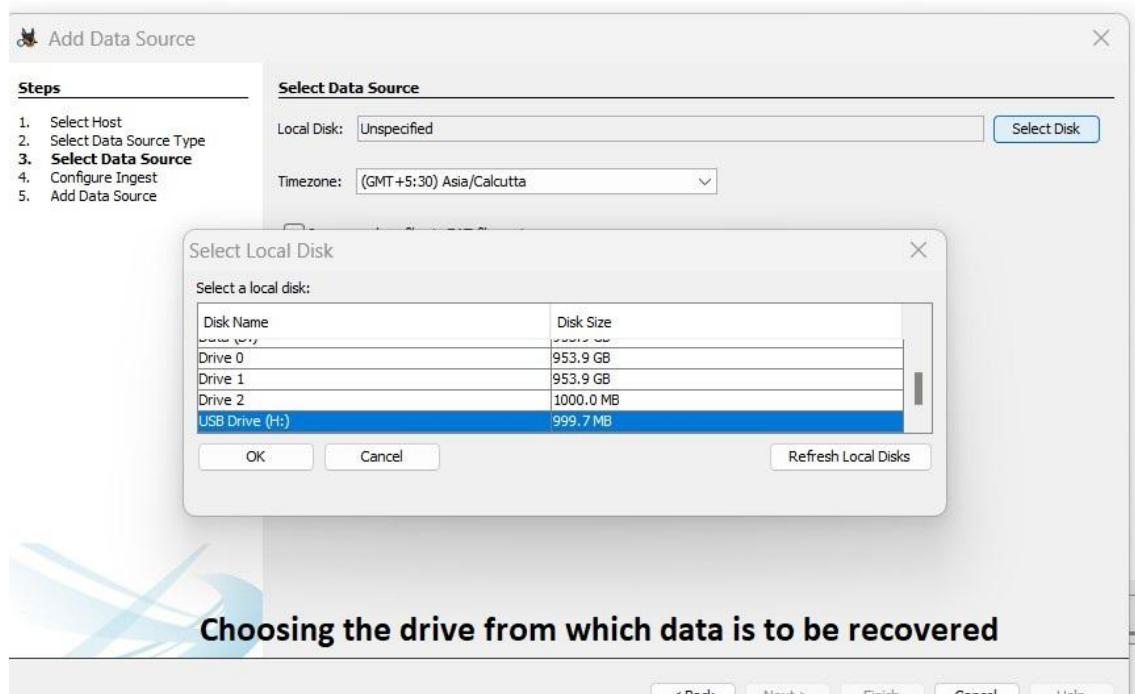
You can now double click on that file to open it in the appropriate application.

Output:

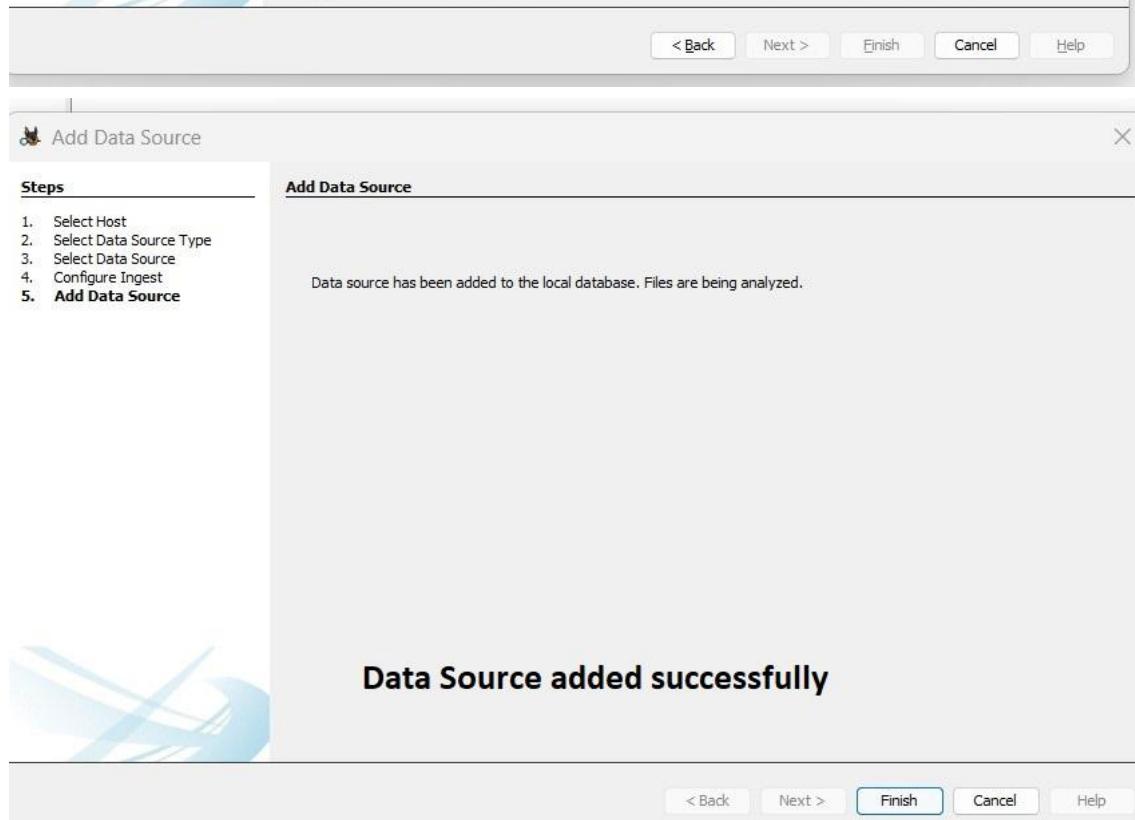
A screenshot of a Windows operating system's File Explorer window. The title bar shows the path: This PC > USB Drive (H:) > Car images >. The left sidebar shows a navigation tree with OneDrive - Personal and various local drives and folders like Desktop, Downloads, Documents, Pictures, etc. The main pane displays a list of files and a folder: buggy.gif (GIF File, 1 KB), buggy1.jpg (JPG File, 10 KB), corvette.jpg (JPG File, 55 KB), download.jpg (JPG File, 7 KB), mercedes.jpeg (JPEG File, 248 KB), Lamborghini_files (File folder), and Lamborghini.html (Opera Web Docu..., 1,378 KB).

Name	Date modified	Type	Size
buggy.gif	02-03-2023 19:41	GIF File	1 KB
buggy1.jpg	02-03-2023 19:42	JPG File	10 KB
corvette.jpg	02-03-2023 19:41	JPG File	55 KB
download.jpg	02-03-2023 19:40	JPG File	7 KB
mercedes.jpeg	02-03-2023 19:41	JPEG File	248 KB
Lamborghini_files	02-03-2023 19:42	File folder	
Lamborghini.html	02-03-2023 19:42	Opera Web Docu...	1,378 KB

Original Data (Before Formatting)



Choosing the drive from which data is to be recovered



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
X download.jpg				2023-03-02 19:40:36 IST	00:00-00 00:00:00	2023-03-02 00:00:00 IST	2023-03-02 19:40:34 IST
X _orvette.jpg				2023-03-02 19:41:24 IST	00:00-00 00:00:00	2023-03-02 00:00:00 IST	2023-03-02 19:41:22 IST
X _ORVET~1.CRD				2023-03-02 19:41:16 IST	00:00-00 00:00:00	2023-03-02 00:00:00 IST	2023-03-02 19:41:14 IST
X corvette.jpg				2023-03-02 19:41:16 IST	00:00-00 00:00:00	2023-03-02 00:00:00 IST	2023-03-02 19:41:22 IST
X _ERCED~1.JPE				2023-03-02 19:41:32 IST	0000-00-00 00:00:00	2023-03-02 00:00:00 IST	2023-03-02 19:41:30 IST
X _ERCED~1.CRD				2023-03-02 19:41:28 IST	0000-00-00 00:00:00	2023-03-02 00:00:00 IST	2023-03-02 19:41:26 IST
X MERCED~1.JPE				2023-03-02 19:41:28 IST	0000-00-00 00:00:00	2023-03-02 00:00:00 IST	2023-03-02 19:41:30 IST
X _AMBOR~1.HTM				2023-03-02 19:41:42 IST	0000-00-00 00:00:00	2023-03-02 00:00:00 IST	2023-03-02 19:41:41 IST
X _uggati.gif				2023-03-02 19:41:58 IST	0000-00-00 00:00:00	2023-03-02 00:00:00 IST	2023-03-02 19:41:56 IST
X _UGGAT~1.CRD				2023-03-02 19:41:54 IST	0000-00-00 00:00:00	2023-03-02 00:00:00 IST	2023-03-02 19:41:52 IST
X bugatti.gif				2023-03-02 19:41:54 IST	0000-00-00 00:00:00	2023-03-02 00:00:00 IST	2023-03-02 19:41:56 IST
X uggat1.ico				2023-03-02 19:42:06 IST	0000-00-00 00:00:00	2023-03-02 00:00:00 IST	2023-03-02 19:42:05 IST

↑ > Documents > New Case Vedant Dhoke > Export



download.jpg

Recovered Data

Conclusion: In conclusion, Autopsy is a powerful digital forensics tool that can be used for file recovery. Through its analysis of digital media and identification of artifacts, Autopsy can effectively recover deleted or damaged files. Overall, Autopsy is a valuable tool for any digital forensics investigation that requires file recovery.