



Vidyavardhini's College of Engineering & Technology

Department of Computer Engineering

Experiment No.1
To analyse Hard Disk images using Autopsy tool
Date of Performance:
Date of Submission:



Vidyavardhini's College of Engineering & Technology

Department of Computer Engineering

Aim: To analyse Hard Disk images using Autopsy tool

Objective: To make use of autopsy tools to extract the evidence from images of hard disk

Theory:

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. The Autopsy is

1. 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.

2. 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.

3. 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.

4. 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.

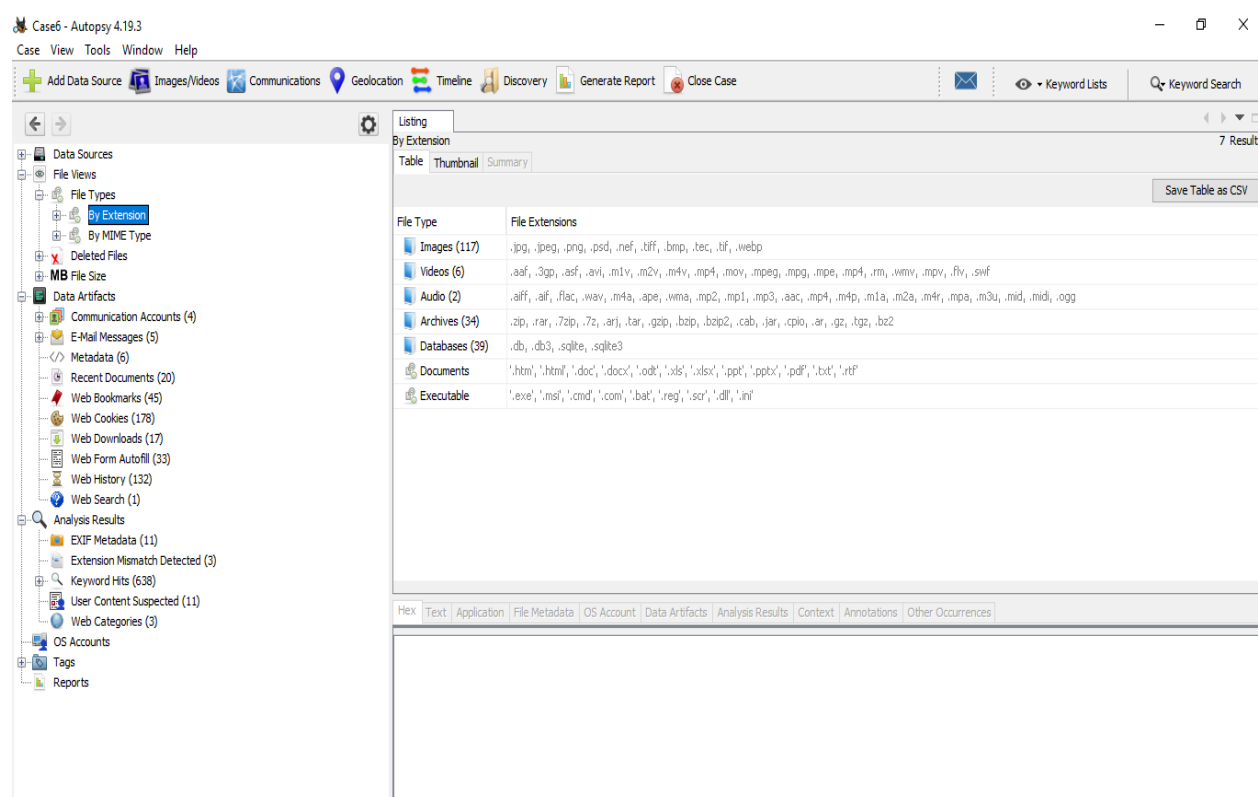


Fig.1.1 A Snapshot of Autopsy tool

KEY FEATURES

The various other important features of Autopsy are as follows

- Simple Windows installation
- Automated, intuitive workflow
- Supports hard drives and smartphones
- Extracts artifacts from web browsers



Vidyavardhini's College of Engineering & Technology

Department of Computer Engineering

- MD5 hash lookup
- Indexed keyword search
- Deleted file carving
- EXIF data extraction from JPEG images
- Timeline analysis for all events
- Standard Android database parsing
- Extension mismatch detection
- Image gallery for picture review
- Email message extraction
- Network-based collaboration

Process:

Step 1. Start the Autopsy Forensic Tool

The primary modes and functions of the Autopsy Forensic Browser are to act as a graphical front end to the Sleuth Kit and other related tools in order to provide the capabilities of analysis, search and case management in a simple but comprehensive package.

Step 2. Start a New Case

Click **New Case**. This will add a new case folder to the system and allow you to begin adding evidence. To begin, click **New Case**.

Step 3. Enter the Case Details

Begin by entering the details about the case. This will include the name of the Case itself and a description of the case.

Step 4. Add a Host to the Case

The Host name specifies the name of the computer under investigation. The user is provided with the options a. Generate new Host name based on data source name b. Specify new Host name c. Use Existing Host name.

Step 5. Select Data Source Type

This steps involves the selection of a particular type of data source Fig. 1.2 shows the various option available as a Data source type.

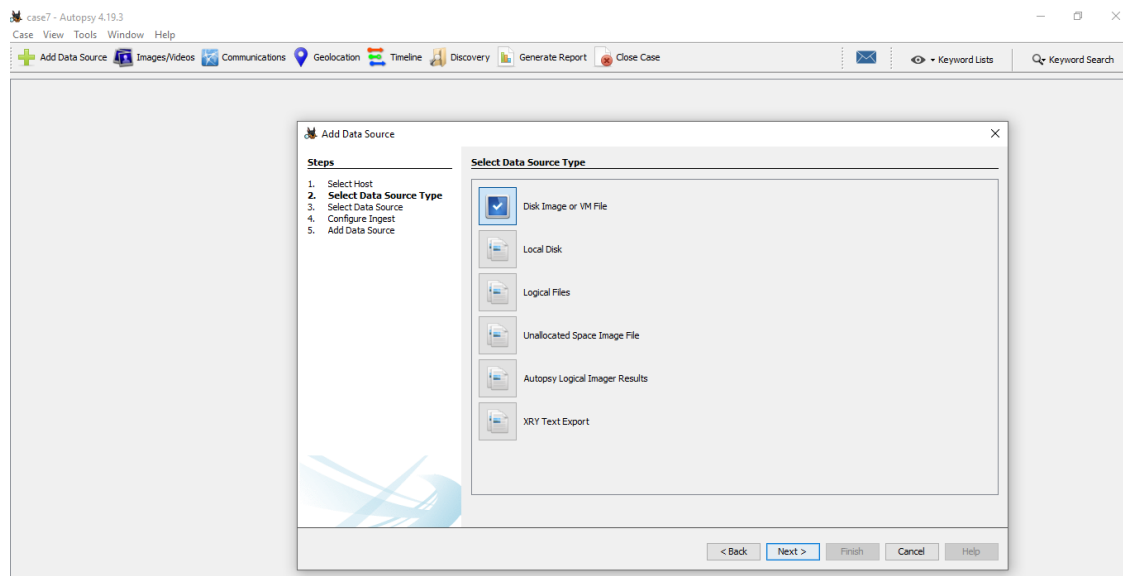


Fig.1.2 Data Source Type

Step 6. Select Data Source

In this step, the actual source of evidence is needed to be selected and a path to that source of evidence is required to be provided. The Autopsy tool then add the source of evidence to the case.

Step 7. Configure Ingest

In this step, the type of evidence needed to be extracted from the source of evidence is informed to the Autopsy tool. By ticking a particular option, the type of evidence related information will be extracted by the Autopsy tool.

Step 8. Add Data Source

In this step, the Autopsy tool finally adds the data source to the case and starts extracting the type of evidence to be searched from the source of evidence.

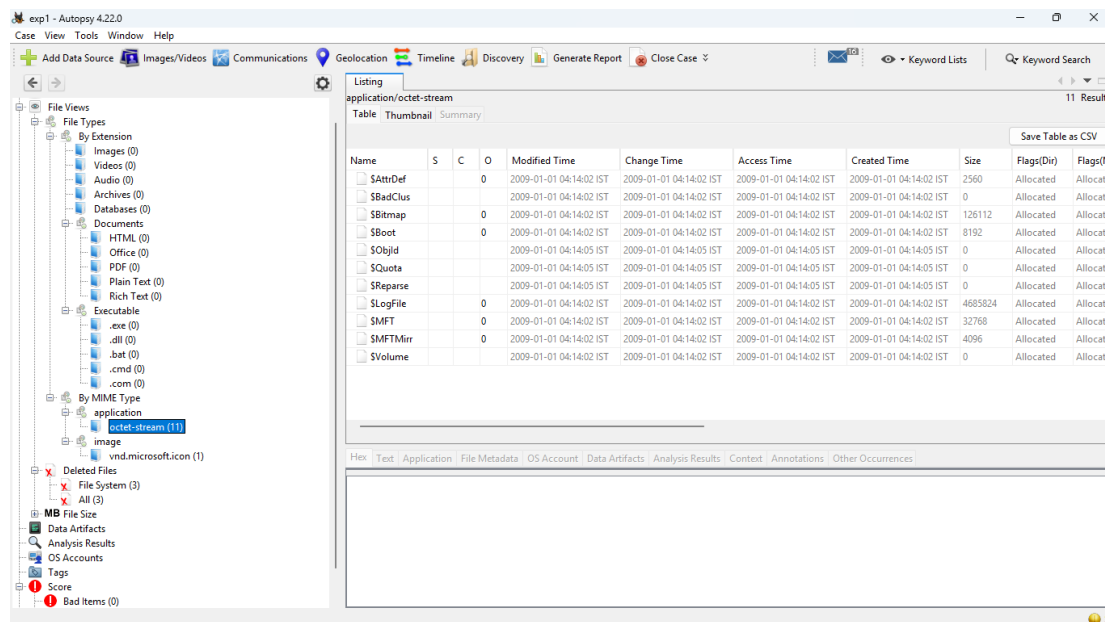
Finally the user gets the various evidence extracted by the Autopsy tool , category wise.



Vidyavardhini's College of Engineering & Technology

Department of Computer Engineering

Output:

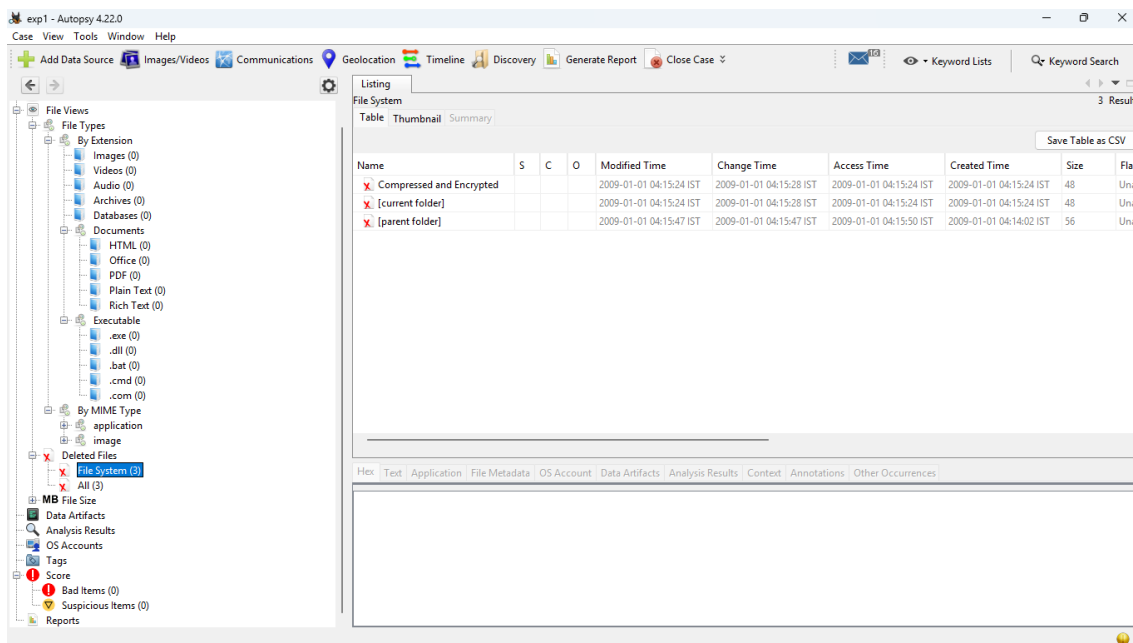


exp1 - Autopsy 4.22.0

Case View Tools Window Help

Listing application/octet-stream 11 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(M)
\$AttrDef			0	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	2560	Allocated	Allocate
\$BadClus				2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	0	Allocated	Allocate
\$Bitmap			0	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	126112	Allocated	Allocate
\$Boot				2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	8192	Allocated	Allocate
\$Solgid				2009-01-01 04:14:05 IST	2009-01-01 04:14:05 IST	2009-01-01 04:14:05 IST	2009-01-01 04:14:05 IST	0	Allocated	Allocate
\$Quota				2009-01-01 04:14:05 IST	2009-01-01 04:14:05 IST	2009-01-01 04:14:05 IST	2009-01-01 04:14:05 IST	0	Allocated	Allocate
\$Repase				2009-01-01 04:14:05 IST	2009-01-01 04:14:05 IST	2009-01-01 04:14:05 IST	2009-01-01 04:14:05 IST	0	Allocated	Allocate
\$LogFile			0	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	4685824	Allocated	Allocate
\$MFT			0	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	32768	Allocated	Allocate
\$MFTMirr			0	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	4096	Allocated	Allocate
\$Volume				2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	2009-01-01 04:14:02 IST	0	Allocated	Allocate



exp1 - Autopsy 4.22.0

Case View Tools Window Help

Listing File System 3 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flag
Compressed and Encrypted				2009-01-01 04:15:24 IST	2009-01-01 04:15:28 IST	2009-01-01 04:15:24 IST	2009-01-01 04:15:24 IST	48	Unal
[current folder]				2009-01-01 04:15:24 IST	2009-01-01 04:15:28 IST	2009-01-01 04:15:24 IST	2009-01-01 04:15:24 IST	48	Unal
[parent folder]				2009-01-01 04:15:47 IST	2009-01-01 04:15:47 IST	2009-01-01 04:15:50 IST	2009-01-01 04:14:02 IST	56	Unal

Conclusion:

In this experiment, the Autopsy tool was effectively used to perform a forensic analysis of a hard disk. By leveraging Autopsy's capabilities, we were able to identify key data, recover deleted files, and investigate file system structures in a systematic manner. The tool's user-friendly interface facilitated the extraction of valuable information, including metadata, file signatures, and the recovery of fragmented or hidden data.