



# **Implementation of a Security Tool – AUTOPSY**

Submitted By:

**Prathmesh Batham**

16010122014

**Kaushal Bhadra**

16010122015

Guided by

**Dr Manish Potey**

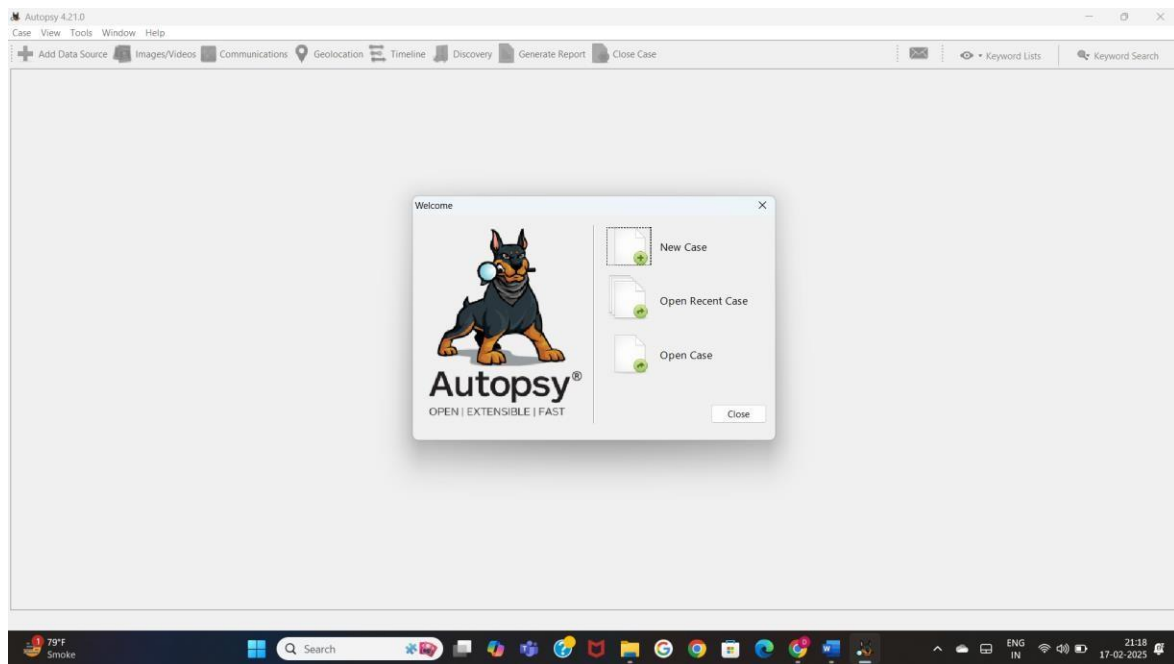
**Computer Engineering**

# INDEX

Sr.No.	Content	PageNo.
1.	Introduction	3
2.	Features/Characteristics	4
3.	Methodology	6
4.	Results	8
5.	Conclusion	16

## Introduction

Autopsy is an open-sourced digital forensic tool used by law enforcement, military, and corporate investigators to analyze digital evidence efficiently. It provides a user-friendly graphical interface for The Sleuth Kit (TSK), which is a suite of command-line forensic tools. Autopsy allows forensic analysts to recover deleted files, analyze disk images, extract metadata, and investigate cybercrimes effectively. The software is widely adopted due to its affordability, comprehensive analysis capabilities, and integration with various forensic utilities. It supports a broad range of forensic functionalities, making it suitable for cyber security investigations, cybercrime analysis, and compliance auditing. With features such as keyword searches, timeline analysis, and file recovery, Autopsy helps digital forensic investigators trace activities and detect anomalies that could indicate cyber threats or security breaches.



## **Features/Characteristics**

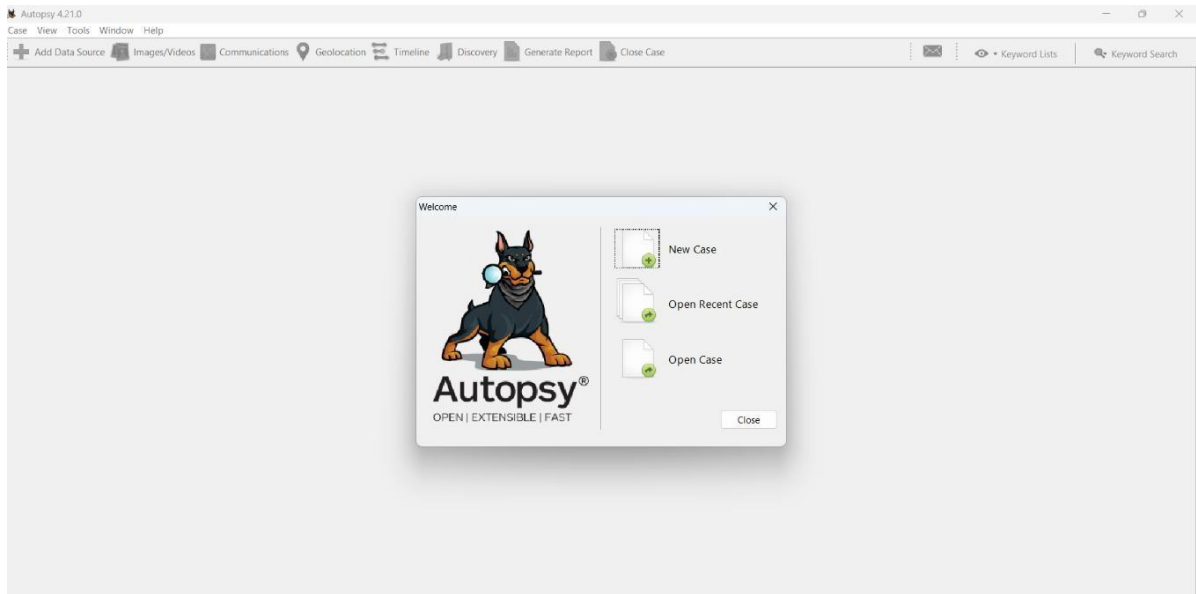
1. **Deleted Data Searching and Recovery** - Autopsy is equipped with powerful file recovery capabilities that allow forensic analysts to retrieve deleted files from NTFS, FAT, and EXT file systems. Even if files have been fragmented or partially overwritten, Autopsy can reconstruct missing data directories and retrieve usable information from allocated and unallocated disk space.
2. **Keyword Search**-The tool supports both indexed and live keyword searches, allowing investigators to find specific terms hidden within files, system logs, browser history, and unallocated space. Custom keyword lists can be used to refine searches for specific investigations, helping analysts detect suspicious activities quickly.
3. **Data Extraction** - Autopsy extracts essential information from various sources, including emails, documents, images, and browser histories. It retrieves metadata such as timestamps, author details, and GPS coordinates, helping investigators analyze user activities, file origins, and potential security incidents.
4. **Registry Analysis** - Autopsy can examine Windows registry hives, revealing unauthorized software installations, changes in system configurations, and potential malware footprints. Deleted registry keys and user activities, such as executed programs and login timestamps, can also be identified.
5. **Timeline Analysis** - The tool generates an interactive timeline of file modifications, deletions, system events, and user activities. This helps forensic investigators visualize the chronological order of events, making it easier to identify suspicious actions and reconstruct digital crime scenes.

6. **Report Generation** - Autopsy automatically generates forensic reports summarizing key findings, extracted artifacts, keyword search results, and system analysis outcomes. These reports are essential for legal proceedings, compliance audits, and cybersecurity assessments.
7. **Malware Detection** - With integration into YARA rules and VirusTotal, Autopsy scans for potential malware, detecting malicious scripts, executables, and root kits. It helps cybersecurity professionals analyze suspicious files and detect unauthorized access attempts.
8. **Hash Filtering**-Autopsy allows investigators to use hash databases, such as the National Software Reference Library (NSRL), to identify known safe or malicious files. Custom hash lists can also be used to flag suspicious data automatically.
9. **Network Traffic Analysis**- Investigators can analyze network packet captures (PCAP files) to identify unauthorized access, data breaches, or security threats. This functionality enables cybersecurity teams to detect malicious communication channels and prevent data exfiltration.
10. **Extensibility and Additional Modules** –Autopsy supports add-on modules for advanced forensic functionalities such as Android device forensics, SQLite database analysis, and encrypted file system examination. Developers can create custom plugins to extend Autopsy's capabilities further.

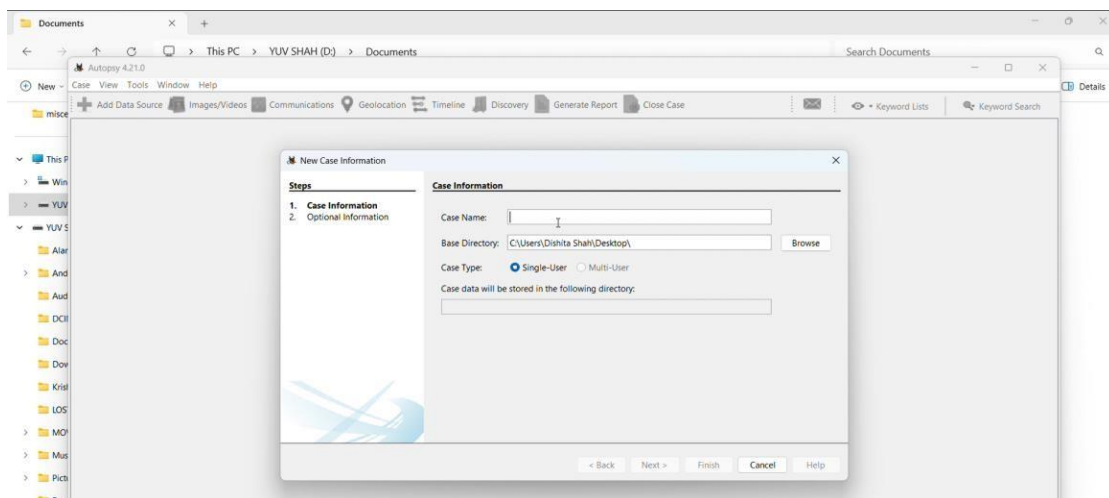
## Methodology

### 1. Case Setup

- Install Autopsy and create a new forensic case with relevant case details.



- Add a data source (disk image, local files, or a livesystem capture) for forensic analysis.



## **2. Data Processing**

- Autopsy processes the data source to extract artifacts like browser history, deleted files, and system logs.
- File system analysis is performed to identify hidden, modified, or suspicious files.

## **3. Keyword and Hash Search**

- Keyword search is conducted to find specific terms related to the investigation.
- Hash filtering is applied to identify known malicious or white listed files.

## **4. Timeline and Metadata Analysis**

- A forensic timeline is generated to trace file modifications, deletions, and system activities.
- Metadata is extracted to analyze the origins and history of digital artifacts.

## **5. Registry and Log File Examination**

- Windows registry hives and log files are analyzed to detect unauthorized changes and system events.

## **6. Reporting and Evidence Documentation**

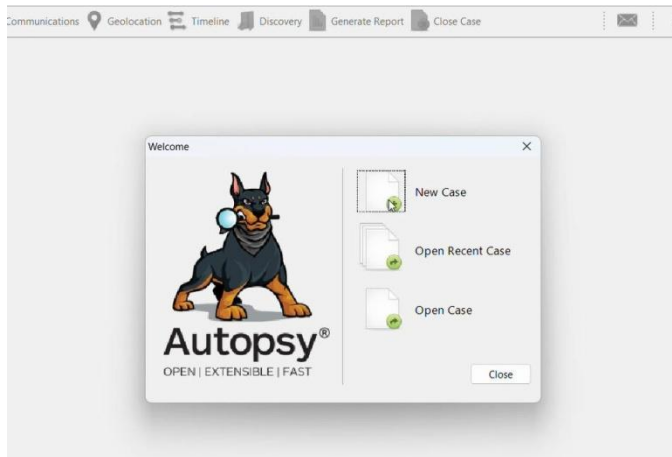
- Findings are documented in detailed forensic reports.
- Reports include case details, extracted artifacts, keyword search results, and visualized timelines.
- Exported reports can be used for legal proceedings and incident response actions.

## Results

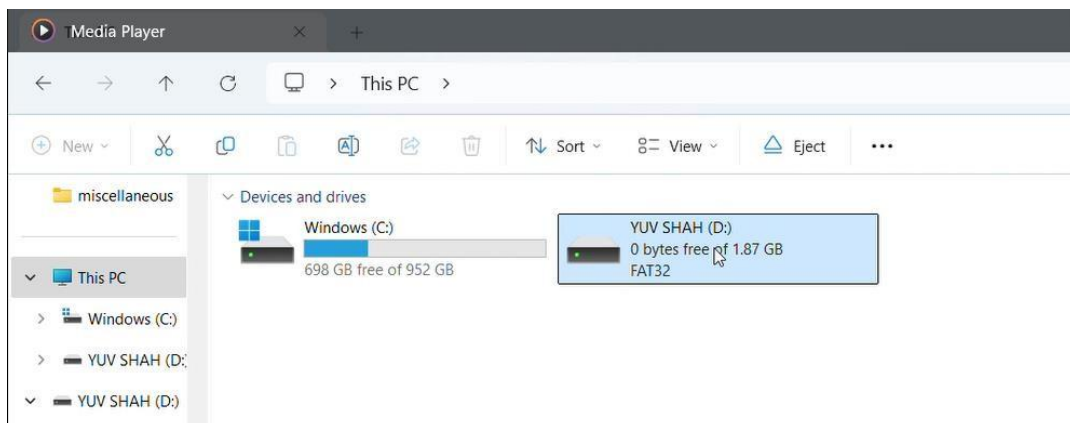
### Implementation of Autopsy for a Digital Forensic Investigation

#### Step 1: Case Creation and Data Ingestion

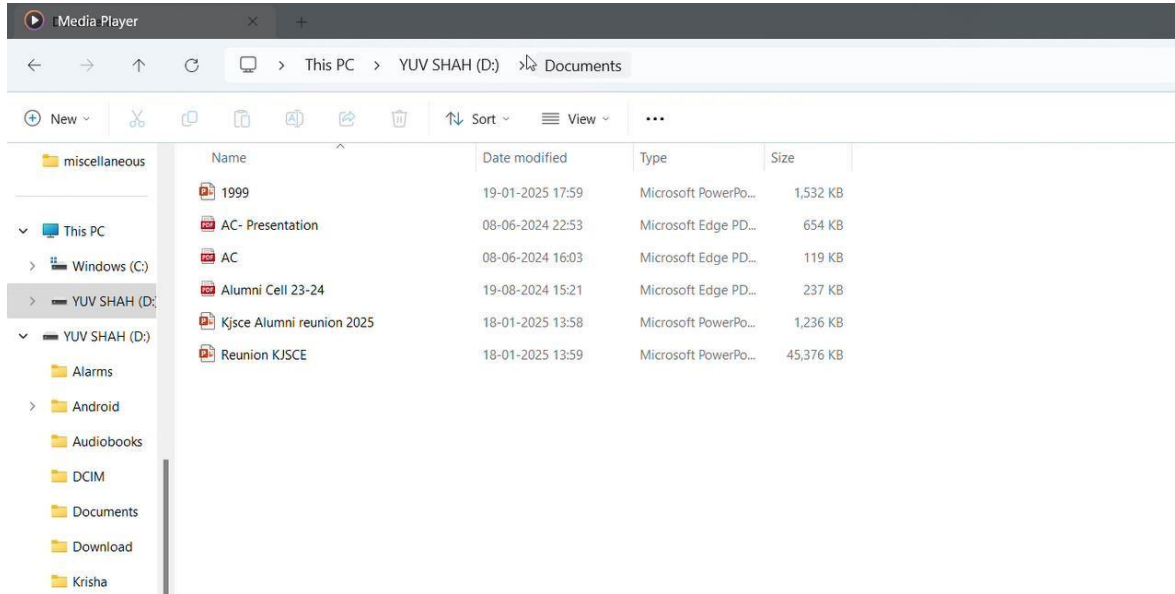
- Open Autopsy and create a new case.



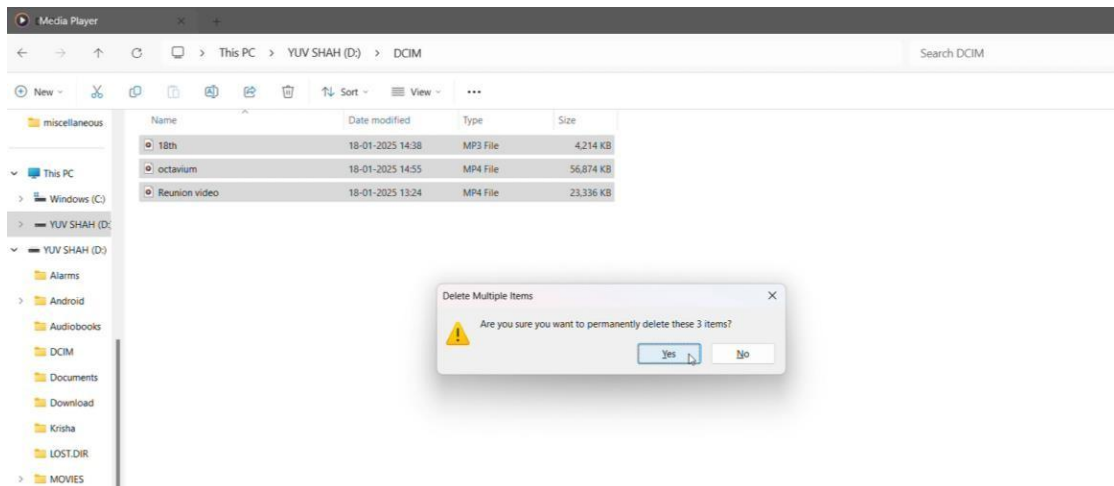
- Add a 2GB USB pendrive as the data source, which initially contained videos and documents in PDF and PPT formats.





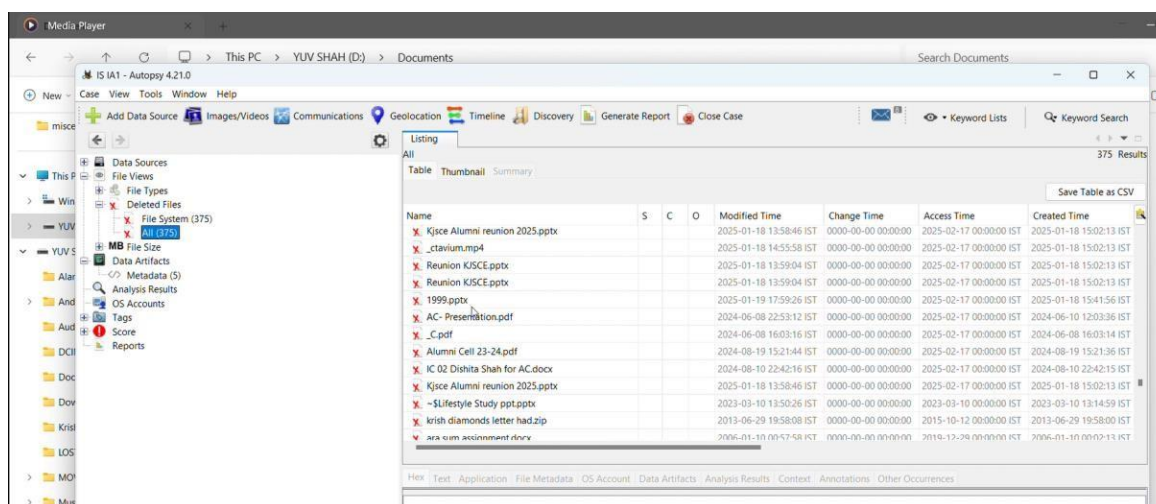
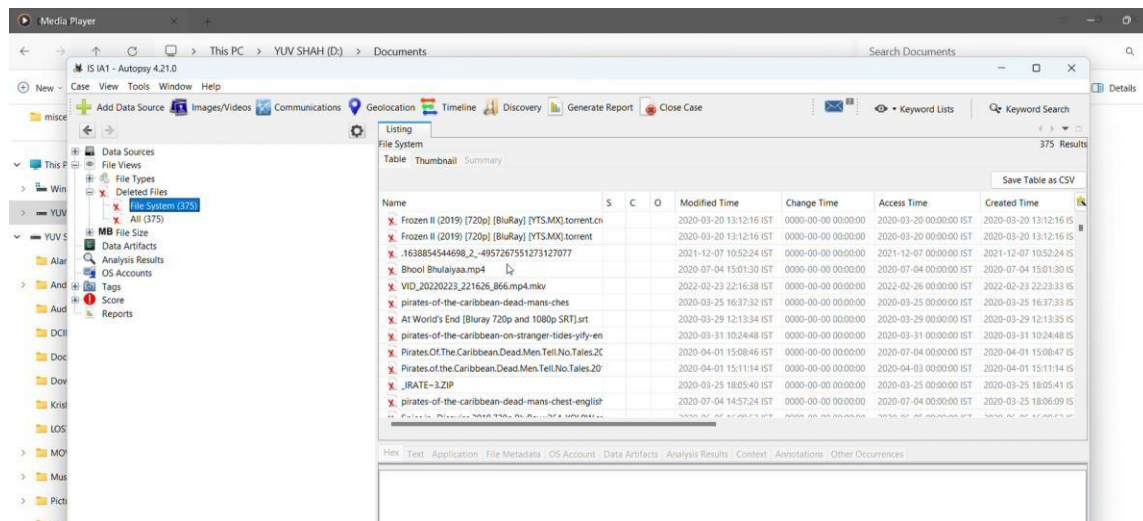


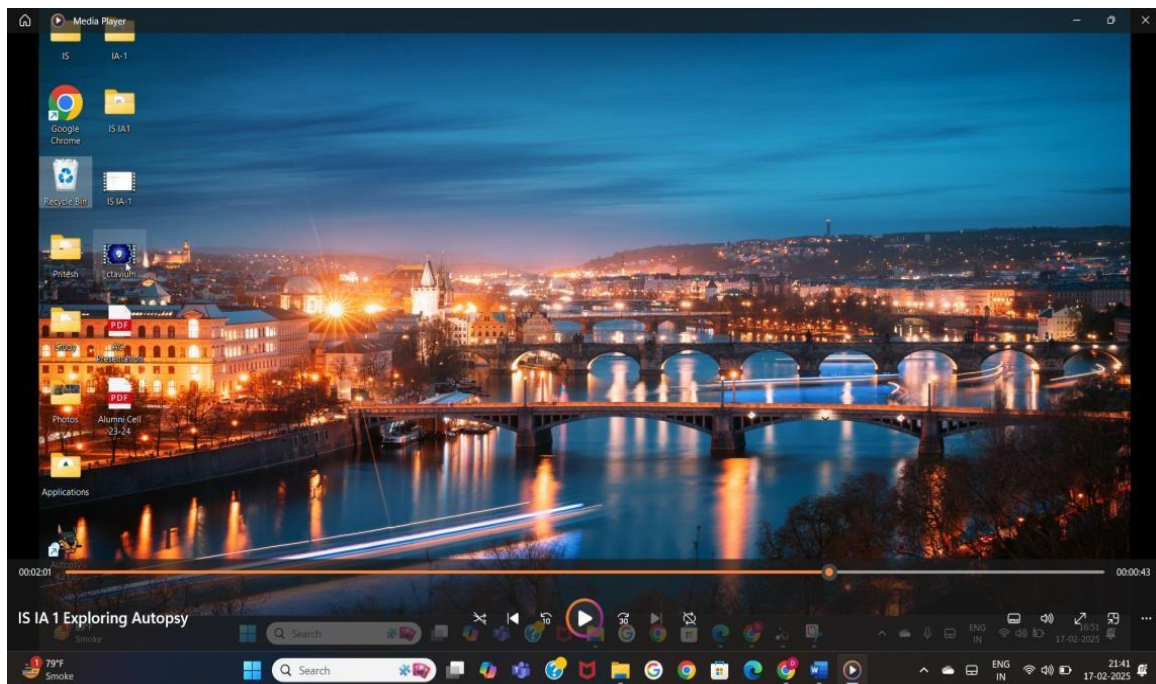
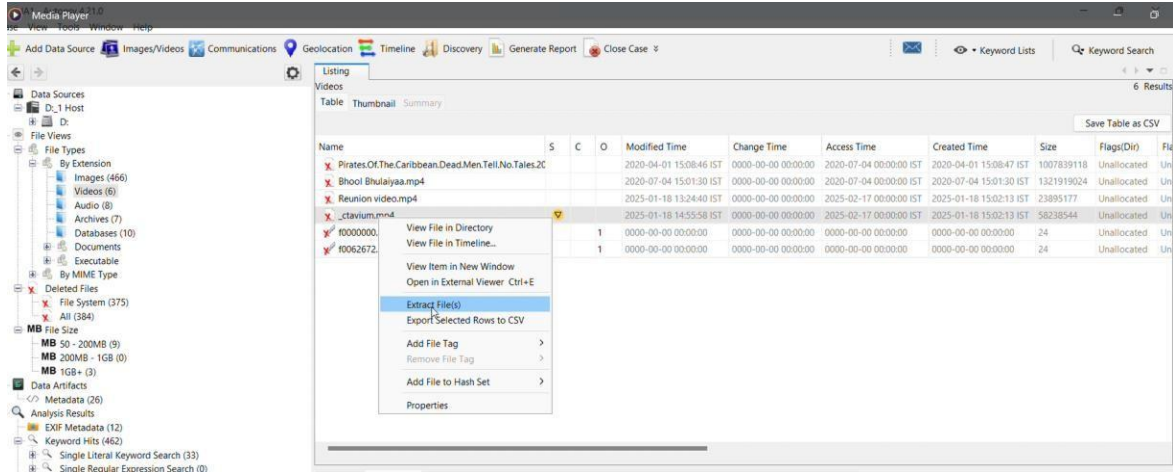
- The files on the pendrive were manually deleted before analysis to simulate a forensic investigation.



## Step2: File Recovery and Deleted Data Searching

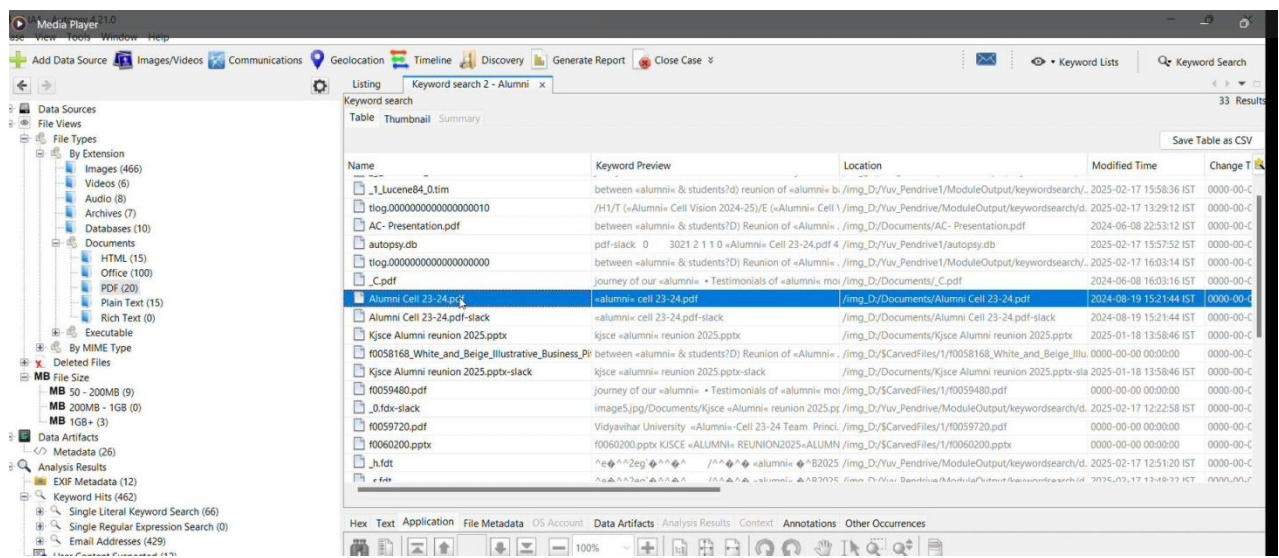
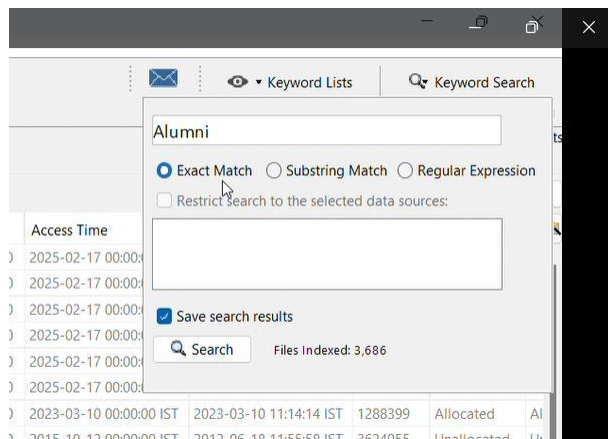
- Using Autopsy's file recovery functionality, deleted files from the USB pendrive were successfully detected.
- Even older files, deleted long before the investigation, were retrieved, showing Autopsy's ability to analyze residual data.
- The file structure was reconstructed, and the deleted PDFs, PPTs, and video files were recovered successfully.



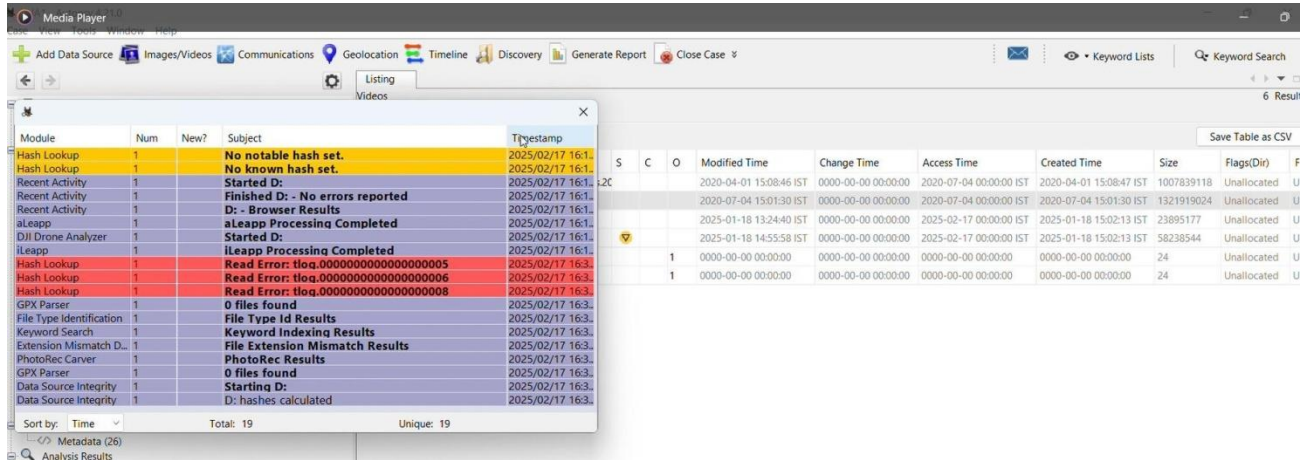


### Step3:Keyword Search and Metadata Extraction

- A keyword search was performed to locate specific filenames and content within the recovered documents.
- The keyword search successfully highlighted text within both PDFs and PPTs, demonstrating the tool's capability to analyze textual data.
- Metadata extraction was conducted on these covered files, revealing timestamps, author details, and previous modifications.



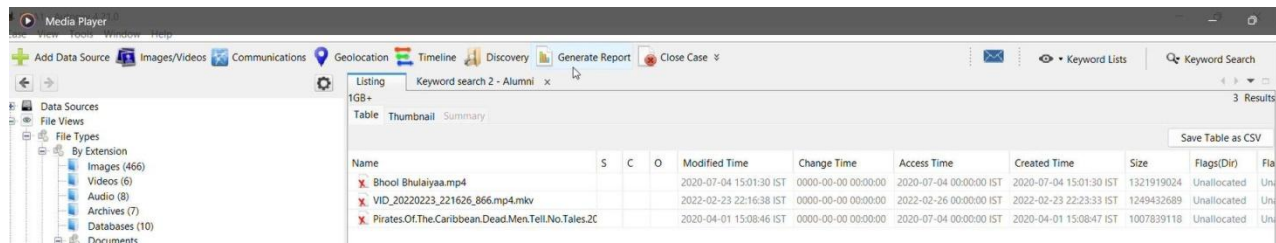




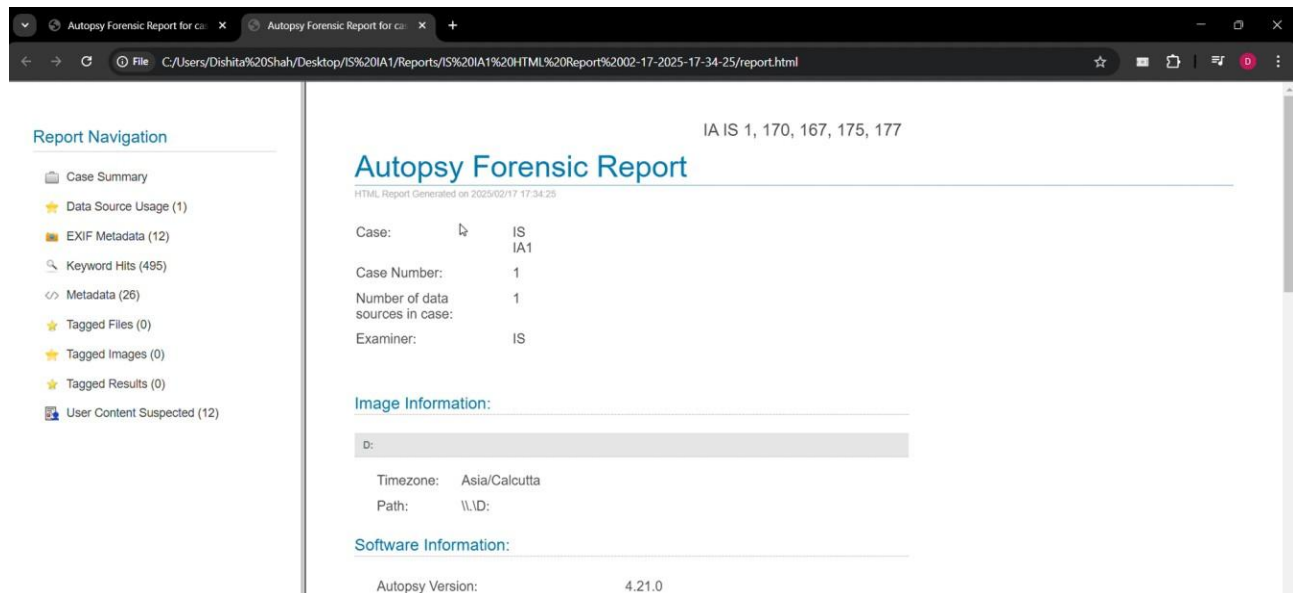
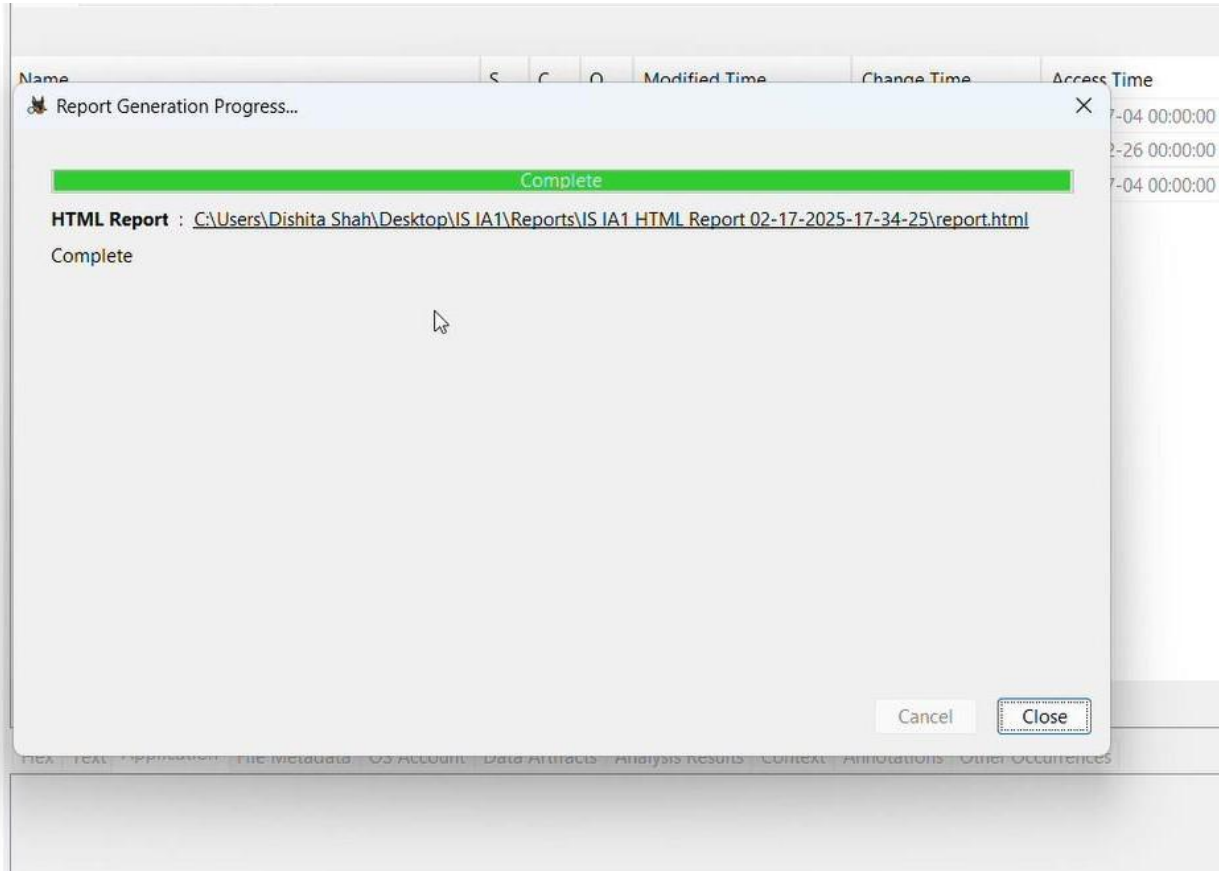
Module	Num	New?	Subject	Timestamp
Hash Lookup	1		No notable hash set.	2025/02/17 16:1
Hash Lookup	1		No known hash set.	2025/02/17 16:1
Recent Activity	1		Finished D: - No errors reported	2025/02/17 16:1
Recent Activity	1		Started D:	2025/02/17 16:1
aLeapp	1		aLeapp Processing Completed	2025/02/17 16:1
DJI Drone Analyzer	1		Started D:	2025/02/17 16:1
lLeapp	1		lLeapp Processing Completed	2025/02/17 16:1
Hash Lookup	1		Read Error: tloq.00000000000000000005	2025/02/17 16:3
Hash Lookup	1		Read Error: tloq.00000000000000000006	2025/02/17 16:3
Hash Lookup	1		Read Error: tloq.00000000000000000008	2025/02/17 16:3
GPX Parser	1		0 files found	2025/02/17 16:3
File Type Identification	1		File Type Id Results	2025/02/17 16:3
Keyword Search	1		Keyword Indexing Results	2025/02/17 16:3
Extension Mismatch D...	1		File Extension Mismatch Results	2025/02/17 16:3
PhotoRec Carver	1		PhotoRec Results	2025/02/17 16:3
GPX Parser	1		0 files found	2025/02/17 16:3
Data Source Integrity	1		Starting D:	2025/02/17 16:3
Data Source Integrity	1		D: hashes calculated	2025/02/17 16:3

## Step4: Report Generation

- A final forensic report was generated, summarizing the recovery process, keyword search results, metadata findings, and retrieved file details.
- The report provided an organized breakdown of the investigation, serving as documented forensic evidence.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Fla
X Bhool Bhulaiyaa.mp4				2020-07-04 15:01:30 IST	0000-00-00 00:00:00	2020-07-04 00:00:00 IST	2020-07-04 15:01:30 IST	1321919024	Unallocated	Un
X VID_20220223_221626_866.mp4.mkv				2022-02-23 22:16:38 IST	0000-00-00 00:00:00	2022-02-26 00:00:00 IST	2022-02-23 22:23:33 IST	1249432689	Unallocated	Un
X Pirates.Of.The.Caribbean.Death.Men.Tell.No.Tales.2C				2020-04-01 15:08:46 IST	0000-00-00 00:00:00	2020-07-04 00:00:00 IST	2020-04-01 15:08:47 IST	1007839118	Unallocated	Un





**SOMAIYA**  
VIDYAVIHAR UNIVERSITY

K J Somaiya College of Engineering

Autopsy Forensic Report for c... Autopsy Forensic Report for c...  
C:/Users/Dishita%20Shah/Desktop/IS%20IA1/Reports/IS%20IA1%20HTML%20Report%202-17-2025-17-34-25/report.html

IA IS 1, 170, 167, 175, 177

### Keyword Hits

- User Searches
- Email Addresses

### User Searches

alumni	Preview	Source File
between «alumni» & students? D) Reunion of «Alumni» batch		/img_D_/ScarvedFiles/1/f0058168_White_and_Beige_illustrative_Business_Pitch_Deck_Presentation.pdf
between «alumni» & students? D) Reunion of «Alumni» batch		/img_D_/ScarvedFiles/1/f0058168_White_and_Beige_illustrative_Business_Pitch_Deck_Presentation.pdf
journey of our «alumni» • Testimonials of «alumni» monthly		/img_D_/ScarvedFiles/1/f0059480.pdf
journey of our «alumni» • Testimonials of «alumni» monthly		/img_D_/ScarvedFiles/1/f0059480.pdf
Vidyavihar University «Alumni»-Cell 23-24 Team Principal:		/img_D_/ScarvedFiles/1/f0059720.pdf
Vidyavihar University «Alumni»-Cell 23-24 Team Principal:		/img_D_/ScarvedFiles/1/f0059720.pdf
f0060200.pptx KJSCE «ALUMNI» REUNION 2025 «ALUMNI» CELL KJSCE		/img_D_/ScarvedFiles/1/f0060200.pptx
f0060200.pptx KJSCE «ALUMNI» REUNION 2025 «ALUMNI» CELL KJSCE		/img_D_/ScarvedFiles/1/f0060200.pptx
/H1 IT («Alumni» Cell Vision 2024-25)/E («Alumni» Cell Vision		/img_D_/Unaloc/Unaloc_3511_16613376_219471872
/H1 IT («Alumni» Cell Vision 2024-25)/E («Alumni» Cell Vision		/img_D_/Unaloc/Unaloc_3511_16613376_219471872
between «alumni» & students? D) Reunion of «Alumni» batch		/img_D_/DCIM/AC- Presentation.pdf
between «alumni» & students? D) Reunion of «Alumni» batch		/img_D_/DCIM/AC- Presentation.pdf
«alumni» cell 23-24.pdf		/img_D_/DCIM/Alumni Cell 23-24.pdf
«alumni» cell 23-24.pdf		/img_D_/DCIM/Alumni Cell 23-24.pdf

Autopsy Forensic Report for c... Autopsy Forensic Report for c...  
C:/Users/Dishita%20Shah/Desktop/IS%20IA1/Reports/IS%20IA1%20HTML%20Report%202-17-2025-17-34-25/report.html

IA IS 1, 170, 167, 175, 177

### Metadata

Date Created	Date Modified	Owner	Program Name	User ID	Version
	2023-03-10 05:37:05 IST	KBS	Microsoft Office PowerPoint	Krishna Shah	
2006-08-16 00:00:00 IST	2025-01-18 08:28:45 IST		Microsoft Office PowerPoint	Dishita Shah	
2006-08-16 00:00:00 IST	2025-01-18 08:28:45 IST		Microsoft Office PowerPoint	Dishita Shah	
2006-08-16 00:00:00 IST	2025-01-18 08:28:45 IST		Microsoft Office PowerPoint	Dishita Shah	
2011-08-01 14:22:18 IST	2023-03-10 05:18:58 IST	IBM SPSS Export Facility	Microsoft Excel	KBS	
2022-06-24 08:02:49 IST	2022-07-03 10:45:03 IST	Krishna Shah	Microsoft Office PowerPoint	Krishna Shah	
2022-07-06 04:31:10 IST	2022-07-29 11:22:41 IST	Hiteshi Dhani	Microsoft Office PowerPoint	Krishna Shah	
2022-07-14 18:05:40 IST	2022-07-29 11:22:46 IST	Hiteshi Dhani	Microsoft Office PowerPoint	Krishna Shah	
2022-07-19 02:39:00 IST	2022-07-19 15:09:00 IST	Krishna Shah	Microsoft Office Word	Krishna Shah	
2022-07-29 11:22:16 IST	2023-01-21 08:48:32 IST	Krishna Shah	Microsoft Office PowerPoint	Krishna Shah	
2022-08-07 18:00:20 IST	2022-08-07 18:00:20 IST	Krishna Shah			1.7
2024-06-08 10:33:15 IST	2024-06-08 10:33:15 IST	Dishita Shah			1.7
2024-06-08 10:33:15 IST	2024-06-08 10:33:15 IST	Dishita Shah			1.7
2024-06-08 10:33:15 IST	2024-06-08 10:33:15 IST	Dishita Shah			1.7
2024-06-08 17:20:50 IST	2024-06-08 17:20:49 IST	dishitapshah			1.4
2024-06-08 17:20:50 IST	2024-06-08 17:20:49 IST	dishitapshah			1.4
2024-06-08 17:20:50 IST	2024-06-08 17:20:49 IST	dishitapshah			1.4
2024-08-19 09:51:42 IST	2024-08-19 09:51:42 IST	16010122167_FY_Shah Dishita Pritesh			1.7
2024-08-19 09:51:42 IST	2024-08-19 09:51:42 IST	16010122167_FY_Shah Dishita Pritesh			1.7
2024-08-19 09:51:42 IST	2024-08-19 09:51:42 IST	16010122167_FY_Shah Dishita Pritesh			1.7

## **Conclusion**

Autopsy proved to be a highly effective tool for digital forensic investigations, successfully recovering deleted files from the USB pendrive, identifying older lost data, and conducting an in-depth keyword search. The tool's metadata extraction capabilities provided crucial insights into the history and modifications of recovered files. By offering a structured forensic report, Autopsy enables investigators to document findings with credibility, making it an essential tool for cybercrime investigations, incident response, and compliance auditing. With its powerful search and recovery features, it continues to be a valuable resource in digital forensics.