Assignment no :- 4

**Aim** - Demonstrate a digital Forensic Tool Autopsy perform the forensic analysis using the Autopsy tool

**Introduction :**

****

An autopsy, also known as a post-mortem examination, is a specialized surgical procedure used to determine the cause and manner of death. The cause of death is the medical reason explaining why a patient passed. The manner of death is the circumstances surrounding the death. Connecticut recognizes the following manners of death: natural, accident, homicide, suicide, and unknown. Only deaths due to natural causes are examined at Yale New Haven Hospital. All other manners of death are referred to the Office of Chief Medical Examiner (OCME) for further investigation.

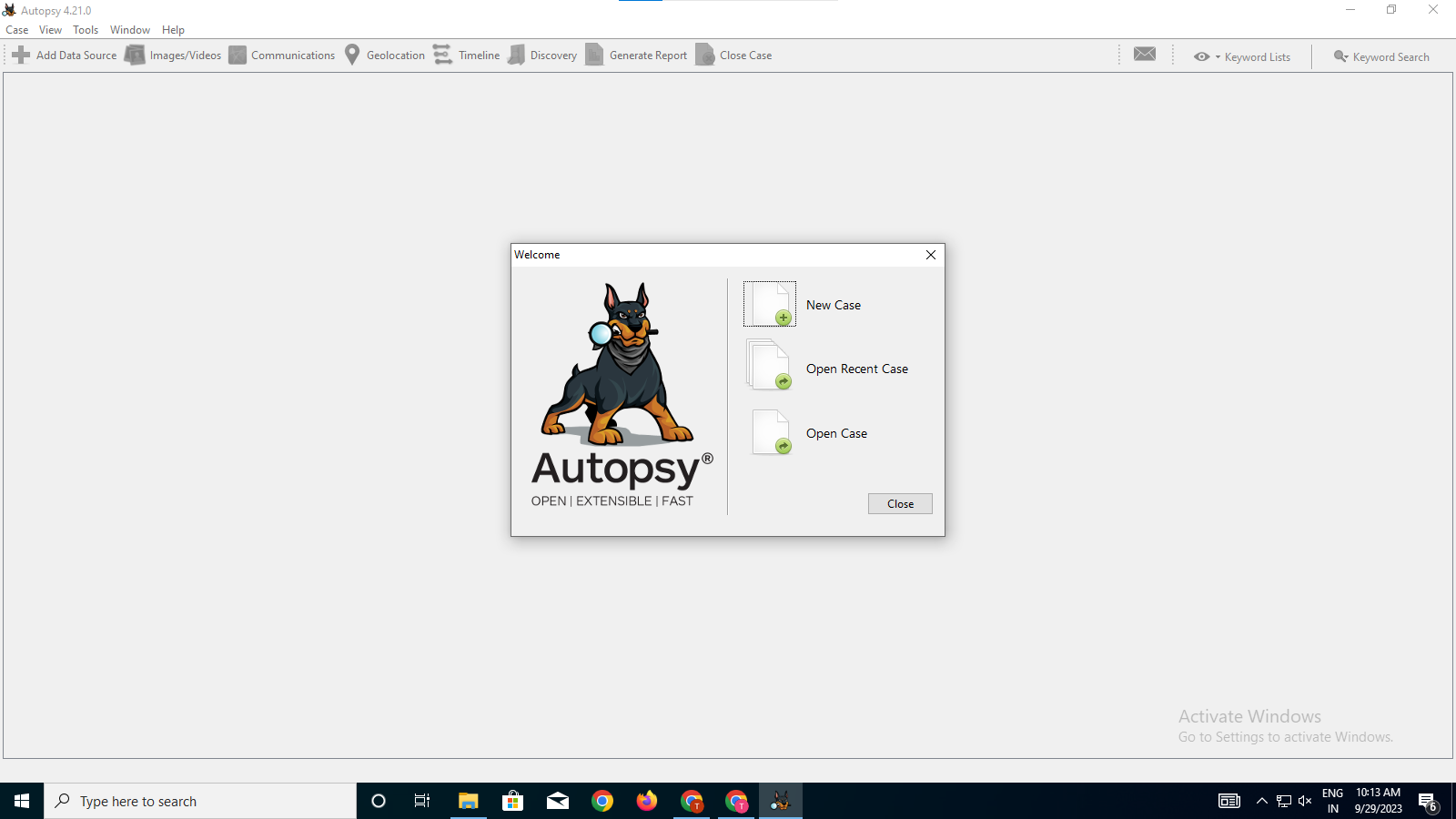
Autopsies continually advance our understanding of disease. What we learn from autopsies allows clinicians to better understand disease processes, accurately diagnose diseases, improve therapy, and potentially aid other patients who are currently suffering from a similar disease. There are many reasons why families choose to pursue having an autopsy done. Consent for an autopsy at Yale includes diagnostic, education, quality improvement, and research.

**\**

**How to run Autopsy :-**

Step 1 : -

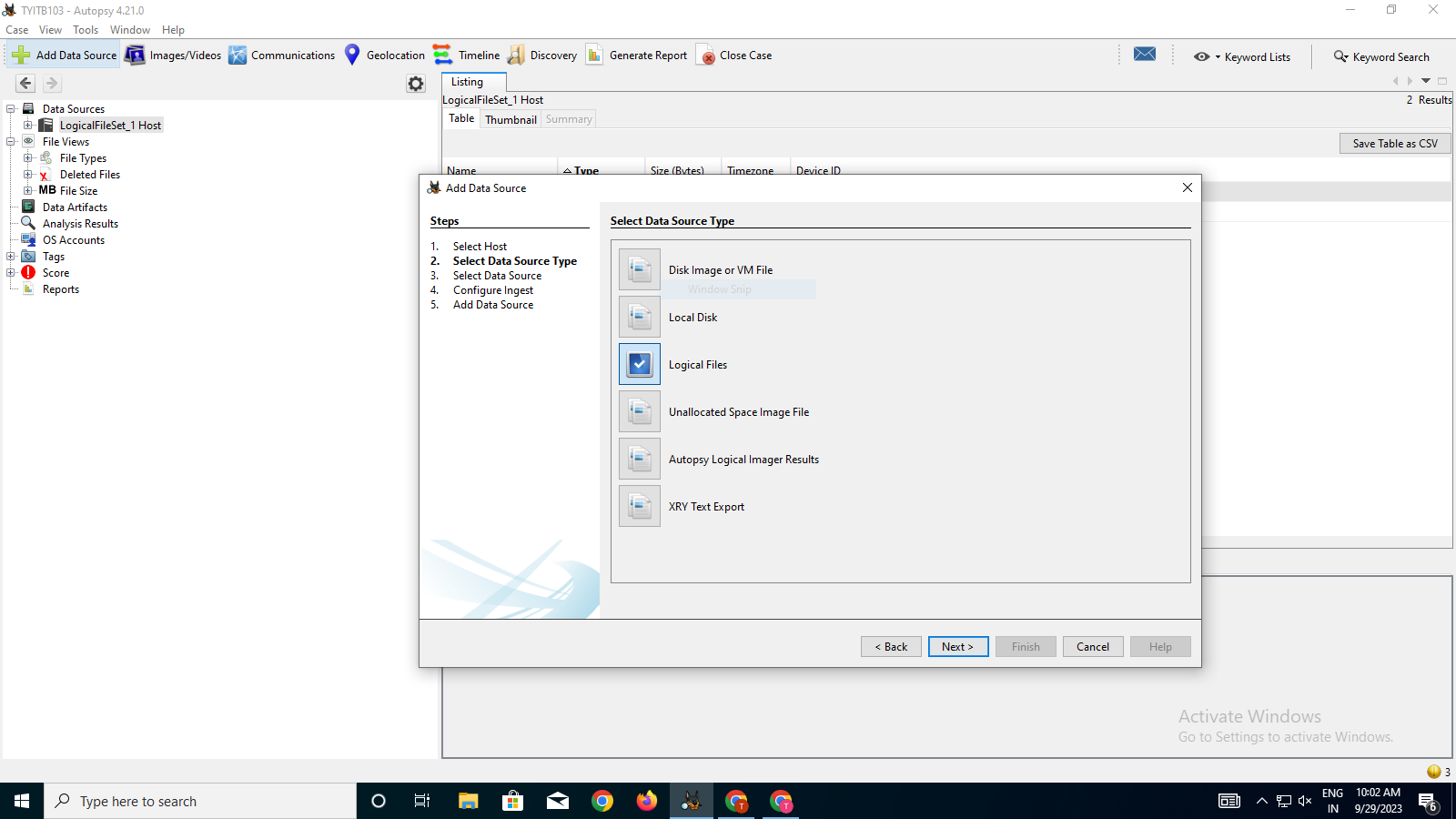
Open the Autopsy and Create the new Case



Step 2 :-

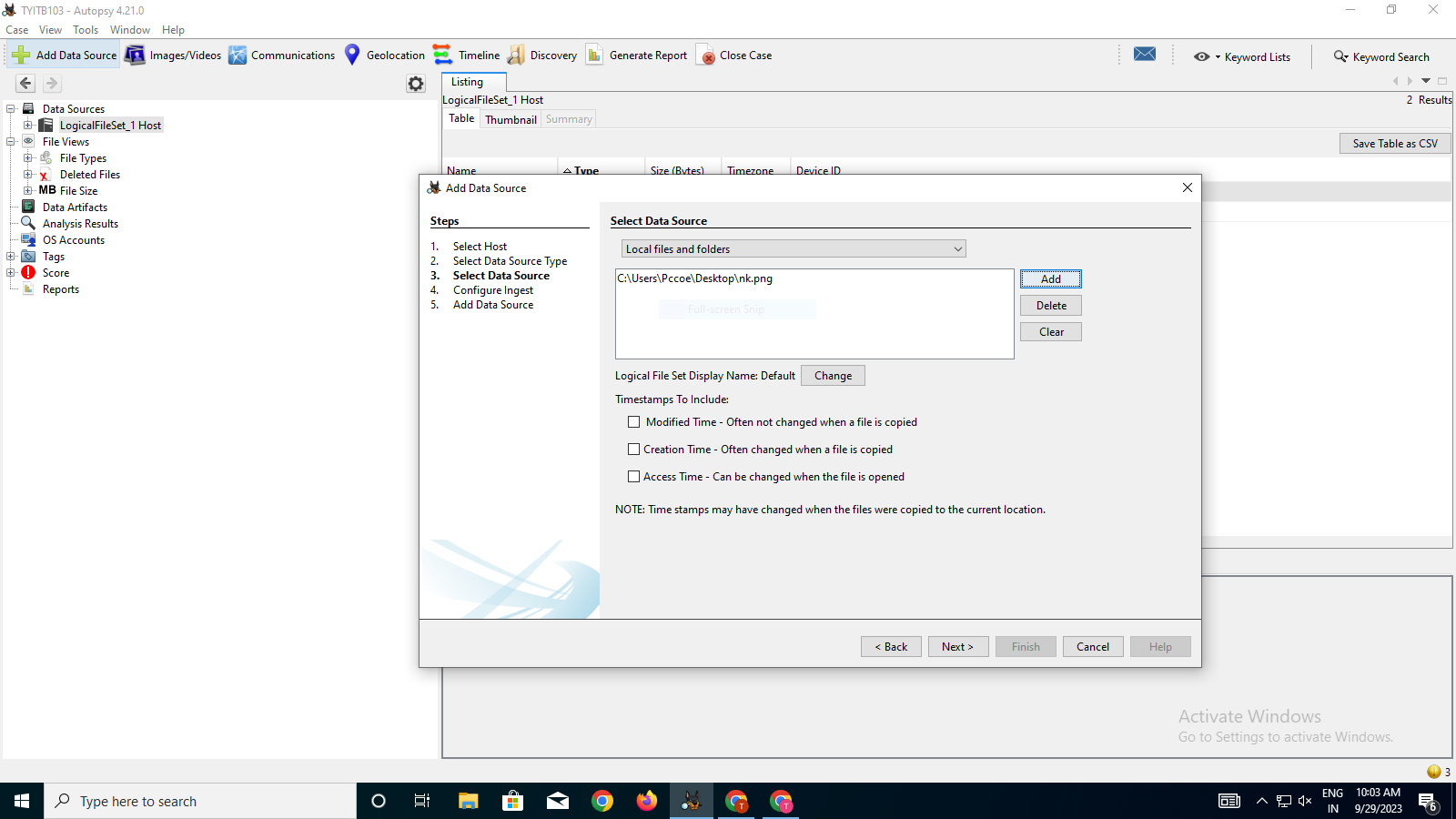
**Add a data source.**

Select the appropriate data source type.



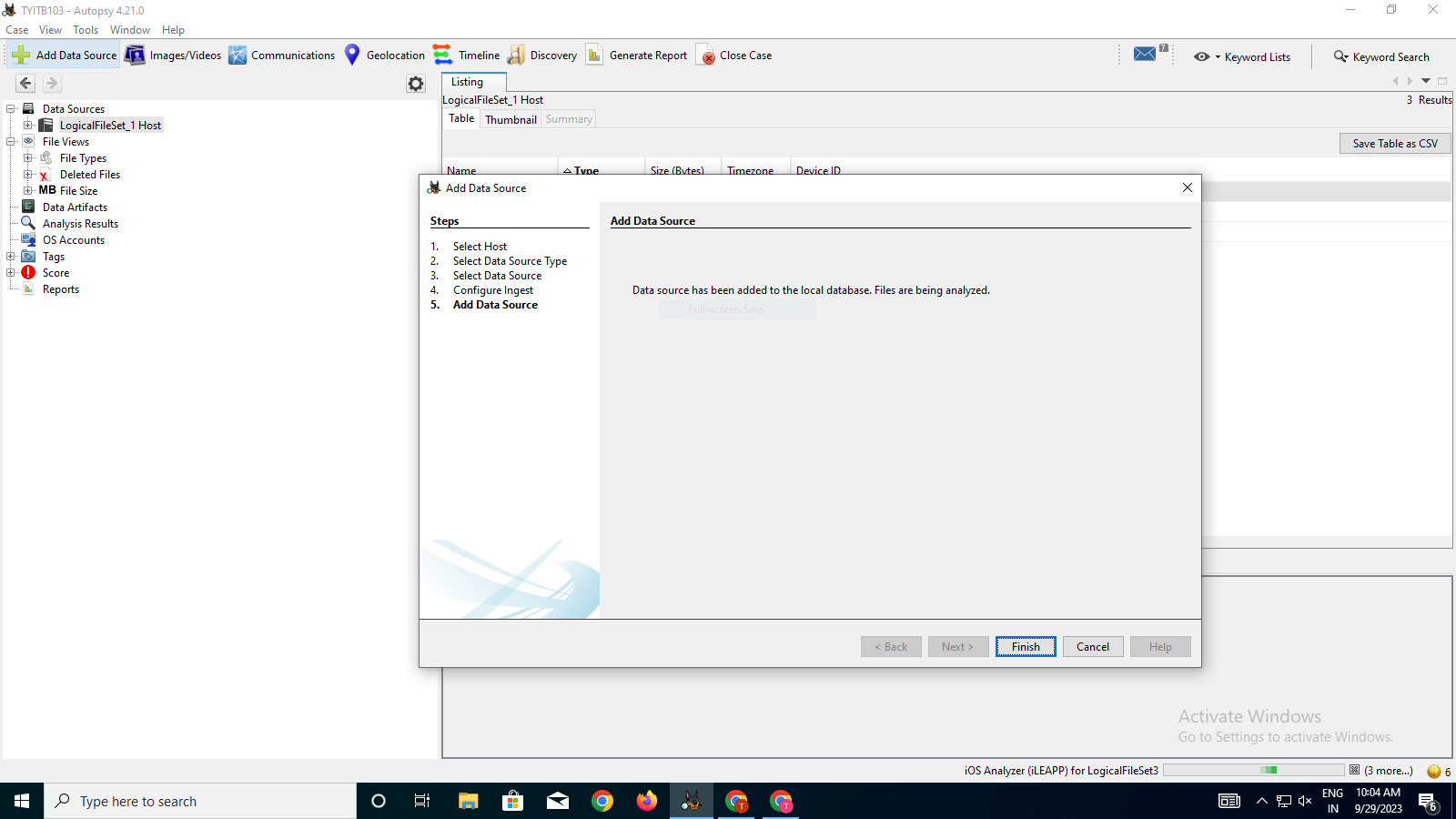
Step 3:-

Add the files which has to be monitor



Step 4:-

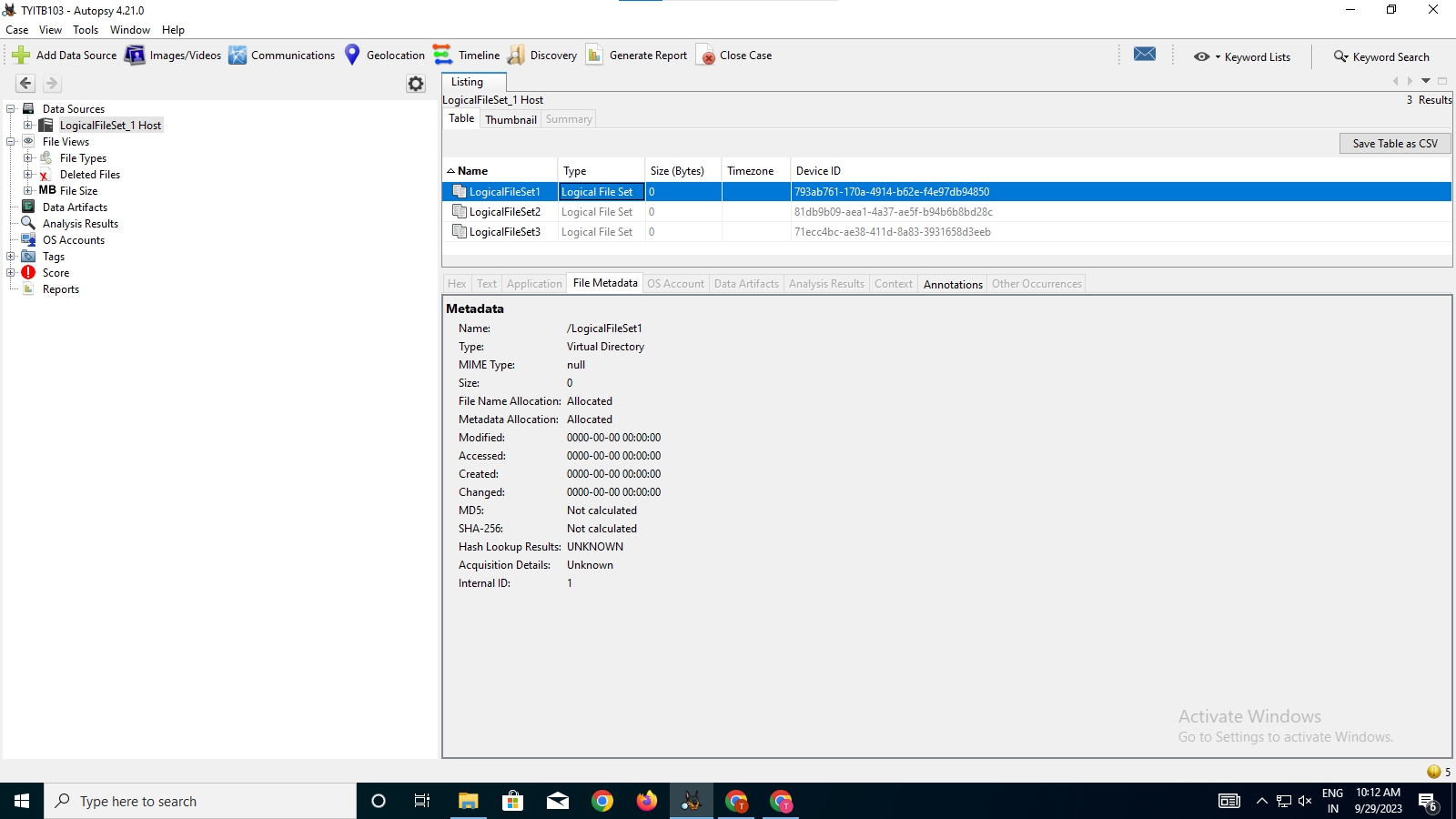
Click on **Finish**

****

**Step 5 :-**

**Generate the Reports**

Generate detailed report of your findings ,including any relevant artifacts ,extracted files, and timeline analysis



**Autopsy’s Crucial Roles :-**

Autopsy software is a digital forensics tool primarily used for analyzing digital media in investigations. It plays a crucial role in examining digital evidence to uncover information relevant to criminal or civil cases. Here are some of the key roles and functionalities of autopsy software:

**File System Analysis**: Autopsy software is designed to analyze various file systems, including NTFS, FAT, exFAT, HFS+, and more. It helps in recovering and parsing file metadata, directory structures, and file content.

**Keyword Searching:** It allows for the search of specific keywords or patterns within files. This is especially important for locating relevant information within a large volume of digital data.

**Timeline Analysis:** Autopsy creates a chronological timeline of file activity, showing when files were created, modified, accessed, or deleted. This helps investigators establish a timeline of events.

**Artifact Analysis**: Autopsy identifies and interprets various digital artifacts such as internet history, chat logs, email headers, and other forms of user-generated data.

Hashing and Integrity Checking: It calculates hash values (e.g., MD5, SHA-1, SHA-256) for files to ensure data integrity and assist in verifying file authenticity.

**Email Analysis**: Autopsy can process and analyze email data from various sources, such as email clients, webmail services, and email archives.

**Report Generation:** It allows investigators to generate detailed reports summarizing the findings, which can be used as evidence in legal proceedings.

**Integration with Other** Tools: Autopsy can often be integrated with other digital forensics tools and databases, enhancing its capabilities and allowing for a more comprehensive investigation.

**Features :-**

**Multi-User Cases**: Collaborate with fellow examiners on large cases.

**Timeline Analysis**: Displays system events in a graphical interface to help identify activity.

**Keyword Search**: Text extraction and index searched modules enable you to find files that

mention specific terms and find regular expression patterns.

**Web Artifacts:** Extracts web activity from common browsers to help identify user activity.

**LNK File Analysis:** Identifies short cuts and accessed documents]

**EXIF:** Extracts geo location and camera information from JPEG files.

**File Type Sorting:** Group files by their type to find all images or documents.

**Media Playback**: View videos and images in the application and not require an external viewer.

**Conclusion**

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.