## Aim:

To perform a live forensic case investigation on a Windows system using **Autopsy**, and to identify user activity such as recent files, browser history, downloads, and system artifacts.

## Tools Required:

- **Autopsy** (open-source digital forensic platform).
- Test system or virtual machine with sample user activity (browser usage, file operations).
- Hashing utilities (e.g., md5sum, sha256sum for evidence verification).

## Introduction:

Live Forensics refers to analyzing a system while it is still running, without shutting it down. This helps investigators collect volatile data such as running processes, open network connections, and recent activities.
Autopsy provides modules to analyze:

- File system (documents, deleted files)
- Web artifacts (cookies, history, downloads)
- Registry (user accounts, USB connections)
- Hash lookups & keyword searches

## Procedure:

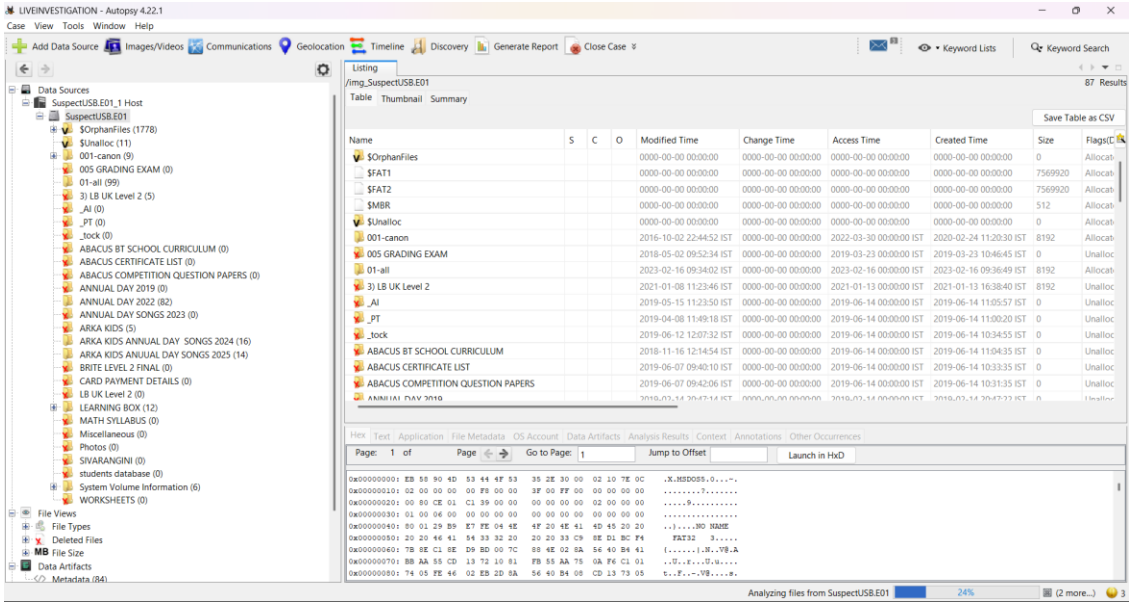
1. **Open Autopsy** from the start menu.
2. **Create a New Case**
    - Case Name: *LiveInvestigation*
    - Case Number: *002*
    - Examiner: Your Name.
    - Choose a base directory for storing case files.
3. **Add Data Source**

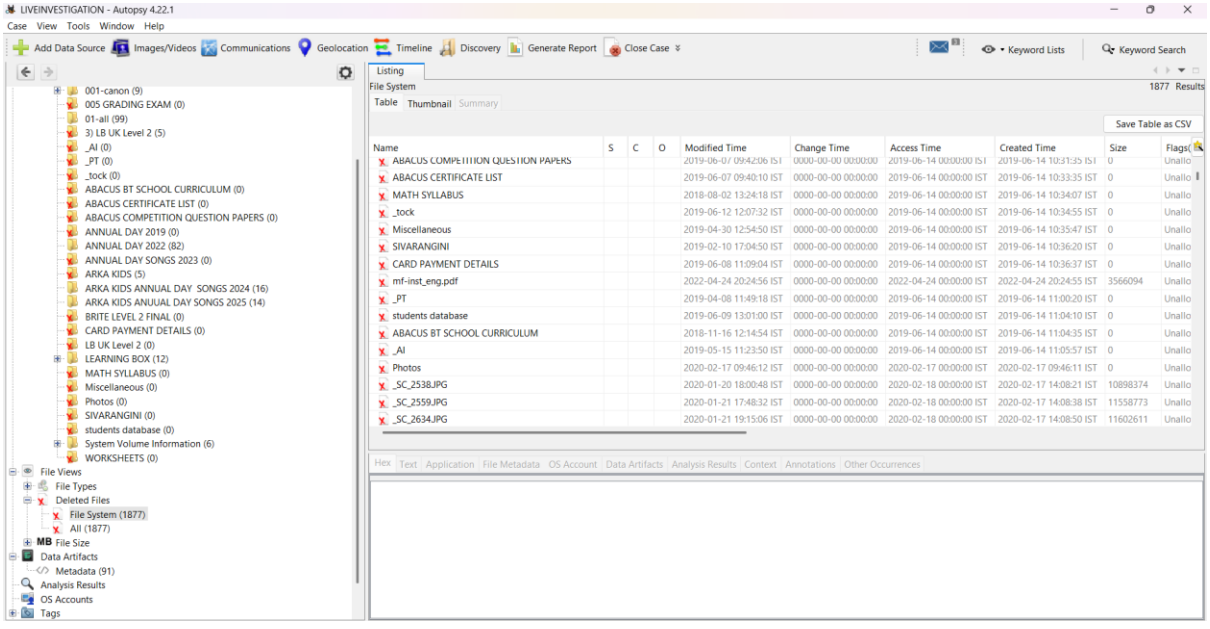
- Select **Local Disk** (for live analysis) or **Disk Image** (if working on a captured image).
- Choose the drive/partition you want to analyze.

4. **Configure Ingest Modules**
   - Enable modules such as:
     - **Hash Lookup**
     - **Keyword Search**
     - **Recent Activity**
     - **Web Artifacts**
     - **File Type Identification**
   - Click **Finish** to start analysis.
5. **Examine Results**
   - **File System Tree** → Explore directories and user documents.
   - **Views → Extracted Content** → Check emails, chat logs, browser history.
   - **Analysis Results** → Review keyword hits, hash matches, and suspicious files.
   - **Recent Activity** → Check downloads, cookies, registry, installed programs.
6. **Document Findings**
   - Note suspicious documents, deleted files, USB activity, or abnormal browsing records.
   - Save important screenshots of findings.
7. **Generate Report**
   - From the toolbar → **Case → Generate Report**.
   - Choose format (HTML, Excel, PDF).
   - Report will include summary, artifacts, and extracted evidence

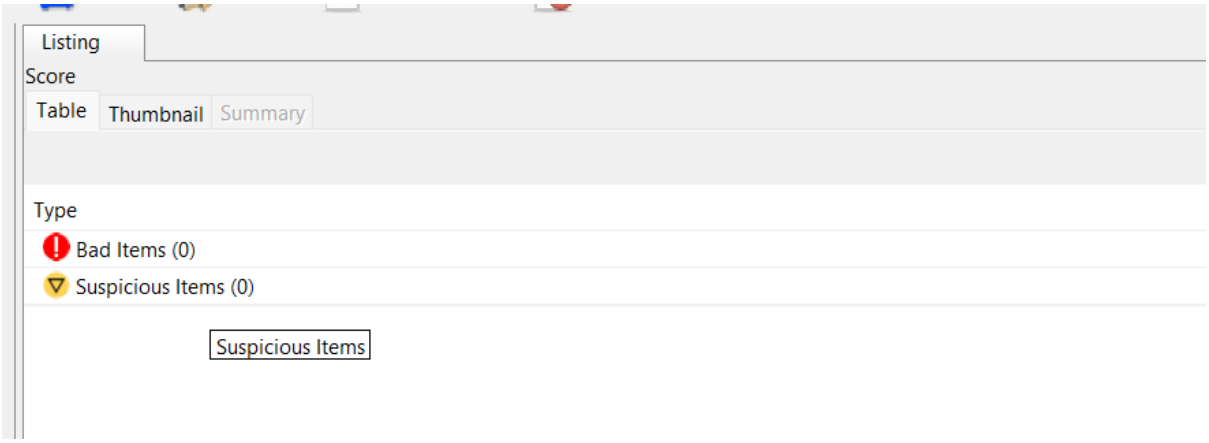
## Output:

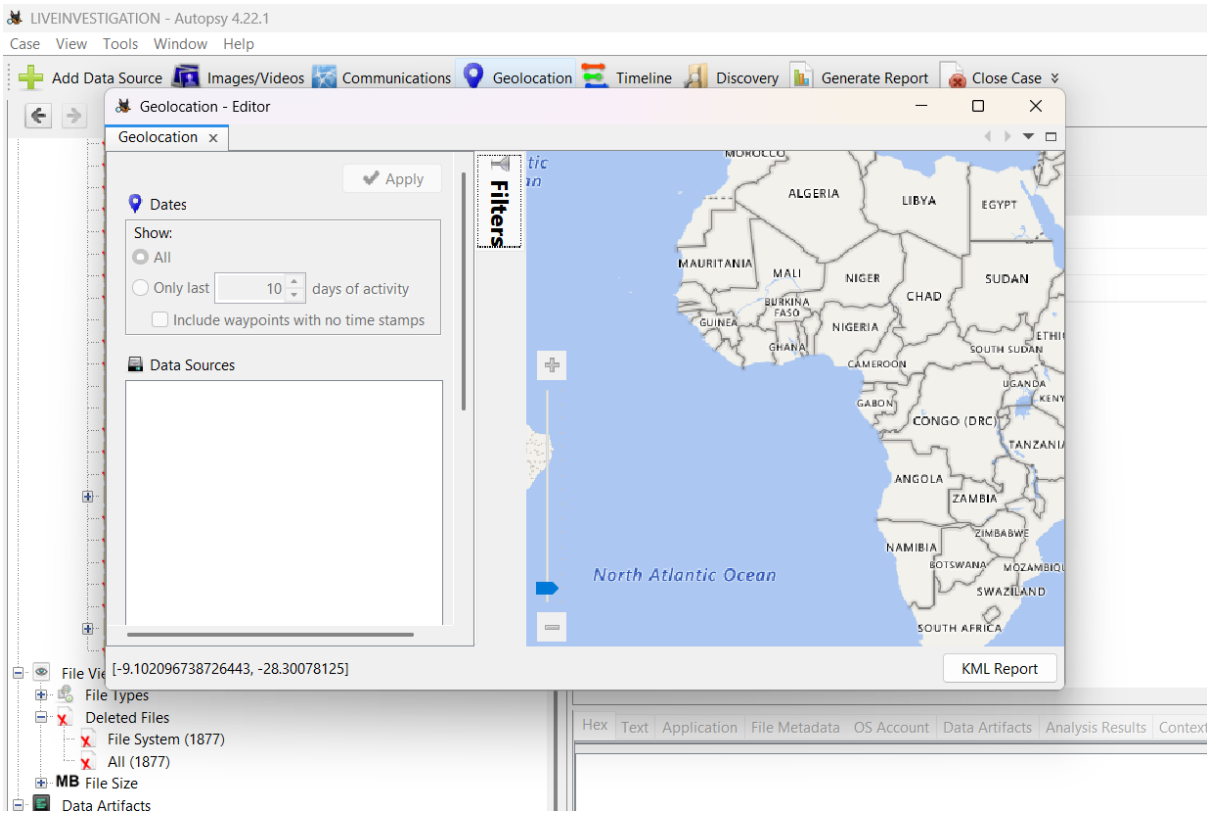
EXP NO:2 LIVE FORENSICS CASE INVESTIGATION USING AUTOPSY Madhan kumar B 231901028



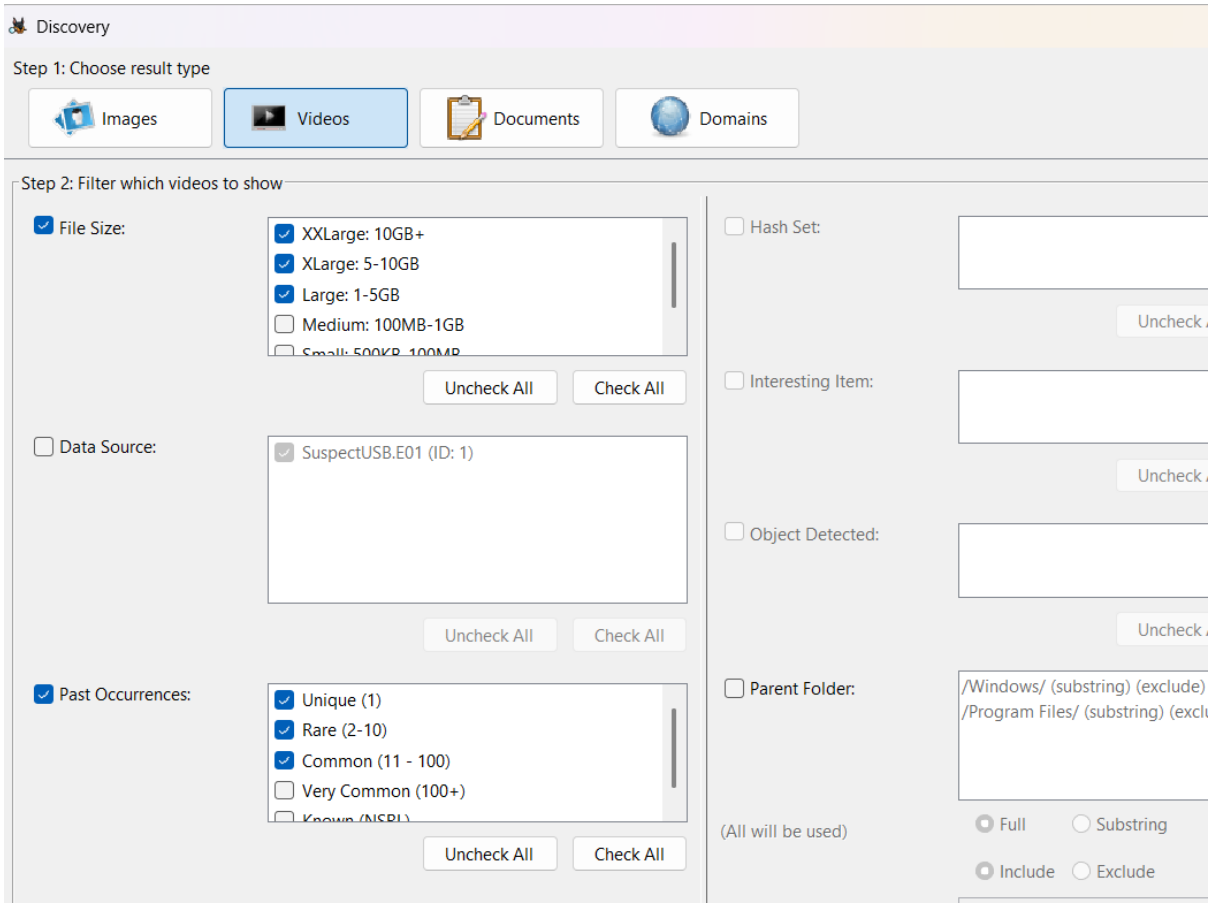



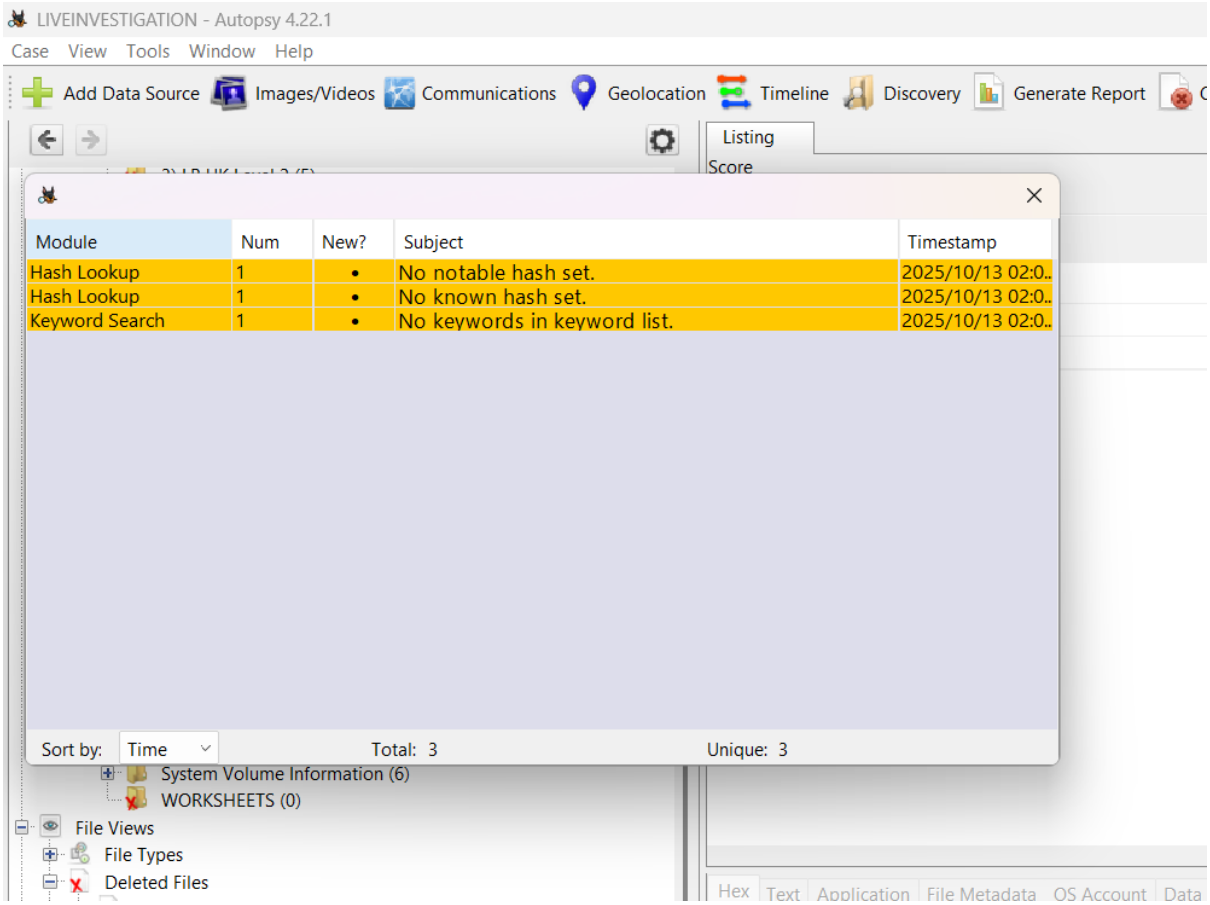
EXP NO:2 LIVE FORENSICS CASE INVESTIGATION USING AUTOPSY Madhan kumar B 231901028



EXP NO:2 LIVE FORENSICS CASE INVESTIGATION USING AUTOPSY Madhan kumar B 231901028






## Result:

Live forensic investigation was successfully performed using **Autopsy**. We analyzed the local system, identified web artifacts, deleted files, registry details, and generated a forensic case report.