

## 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:**

LIVEINVESTIGATION - Autopsy 4.22.1

Case View Tools Window Help

Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Data Sources

SuspectUSB.E01

OrphanFiles (1778)

\$Unalloc (11)

001-canon (9)

005 GRADING EXAM (0)

01-all (99)

3) LB UK Level 2 (5)

.AI (0)

.PT (0)

.Jock (0)

ABACUS BT SCHOOL CURRICULUM (0)

ABACUS CERTIFICATE LIST (0)

ABACUS COMPETITION QUESTION PAPERS (0)

ANNUAL DAY 2019 (0)

ANNUAL DAY 2022 (82)

ANNUAL DAY SONGS 2023 (0)

ARKA KIDS (5)

ARKA KIDS ANNUAL DAY SONGS 2024 (16)

ARKA KIDS ANNUAL DAY SONGS 2025 (14)

BRITE LEVEL 2 FINAL (0)

CARD PAYMENT DETAILS (0)

LB UK Level 2 (0)

LEARNING BOX (12)

MATH SYLLABUS (0)

Miscellaneous (0)

Photos (0)

SIVARANGINI (0)

students database (0)

System Volume Information (6)

WORKSHEETS (0)

File Views

File Types

Deleted Files

MB File Size

Data Artifacts

Metadata (84)

Listing

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags
OrphanFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocat
\$FAT1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	7569920	Allocat
\$FAT2				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	7569920	Allocat
\$MBR				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	512	Allocat
\$Unalloc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocat
001-canon				2016-10-02 22:44:52 IST	0000-00-00 00:00:00	2022-03-20 00:00:00 IST	2020-02-24 11:20:30 IST	8192	Allocat
005 GRADING EXAM				2018-05-02 09:52:34 IST	0000-00-00 00:00:00	2019-03-23 00:00:00 IST	2019-03-23 10:46:45 IST	0	Unalloc
01-all				2023-02-16 09:34:02 IST	0000-00-00 00:00:00	2023-02-16 00:00:00 IST	2023-02-16 09:36:49 IST	8192	Allocat
3) LB UK Level 2				2021-01-08 11:23:46 IST	0000-00-00 00:00:00	2021-01-13 00:00:00 IST	2021-01-13 16:38:40 IST	8192	Unalloc
.AI				2019-05-15 11:23:50 IST	0000-00-00 00:00:00	2019-06-14 00:00:00 IST	2019-06-14 11:05:57 IST	0	Unalloc
.PT				2019-04-08 11:49:18 IST	0000-00-00 00:00:00	2019-06-14 00:00:00 IST	2019-06-14 11:00:20 IST	0	Unalloc
.Jock				2019-06-12 12:07:32 IST	0000-00-00 00:00:00	2019-06-14 00:00:00 IST	2019-06-14 10:34:55 IST	0	Unalloc
ABACUS BT SCHOOL CURRICULUM				2018-11-16 12:14:54 IST	0000-00-00 00:00:00	2019-06-14 00:00:00 IST	2019-06-14 11:04:35 IST	0	Unalloc
ABACUS CERTIFICATE LIST				2019-06-07 09:40:10 IST	0000-00-00 00:00:00	2019-06-14 00:00:00 IST	2019-06-14 10:33:35 IST	0	Unalloc
ABACUS COMPETITION QUESTION PAPERS				2019-06-07 09:42:06 IST	0000-00-00 00:00:00	2019-06-14 00:00:00 IST	2019-06-14 10:31:35 IST	0	Unalloc
ANNUAL DAY 2019				2019-03-14 10:47:14 IST	0000-00-00 00:00:00	2019-03-14 00:00:00 IST	2019-03-14 10:47:22 IST	0	Unalloc

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Page: 1 of 1 Page: 1 Go to Page: 1 Jump to Offset: Launch in HxD

0x00000000: E8 58 90 4D 53 44 4F 53 35 2E 30 00 02 10 7E 0C .X..ND009..0....  
0x00000010: 02 00 00 00 00 FF 00 00 00 00 00 00 00 00 00 00 .....7.....  
0x00000020: 00 80 CE 01 C1 39 00 00 00 00 00 00 02 00 00 00 .....9.....  
0x00000030: 01 00 04 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0x00000040: 80 01 29 B9 E7 FE 04 4E 4F 20 4E 41 4D 45 20 20 .....30 NAME  
0x00000050: 20 20 46 41 54 33 32 20 20 20 33 C9 EE D1 8C F4 FAT32 3.....  
0x00000060: 7B BE C1 EE D9 B0 00 7C 88 4E 02 8A 56 40 B4 41 {.....}.VB.A  
0x00000070: B8 BA 15 CD 13 12 10 81 F8 55 BA 75 0A FE C1 01 ..F.....  
0x00000080: 74 05 FE 46 02 E8 2D 8A 56 40 B4 08 CD 13 73 05 t..F...VB....

Analyzing files from SuspectUSB.E01 24% (2 more...)

LIVEINVESTIGATION - Autopsy 4.22.1

Case View Tools Window Help

Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Data Sources

SuspectUSB.E01

001-canon (9)

005 GRADING EXAM (0)

01-all (99)

3) LB UK Level 2 (5)

.AI (0)

.PT (0)

.Jock (0)

ABACUS BT SCHOOL CURRICULUM (0)

ABACUS CERTIFICATE LIST (0)

ABACUS COMPETITION QUESTION PAPERS (0)

ANNUAL DAY 2019 (0)

ANNUAL DAY 2022 (82)

ANNUAL DAY SONGS 2023 (0)

ARKA KIDS (5)

ARKA KIDS ANNUAL DAY SONGS 2024 (16)

ARKA KIDS ANNUAL DAY SONGS 2025 (14)

BRITE LEVEL 2 FINAL (0)

CARD PAYMENT DETAILS (0)

LB UK Level 2 (0)

LEARNING BOX (12)

MATH SYLLABUS (0)

Miscellaneous (0)

Photos (0)

SIVARANGINI (0)

students database (0)

System Volume Information (6)

WORKSHEETS (0)

File Views

File Types

Deleted Files

File System (1877)

MB File Size

Data Artifacts

Metadata (91)

Analysis Results

OS Accounts

Tags

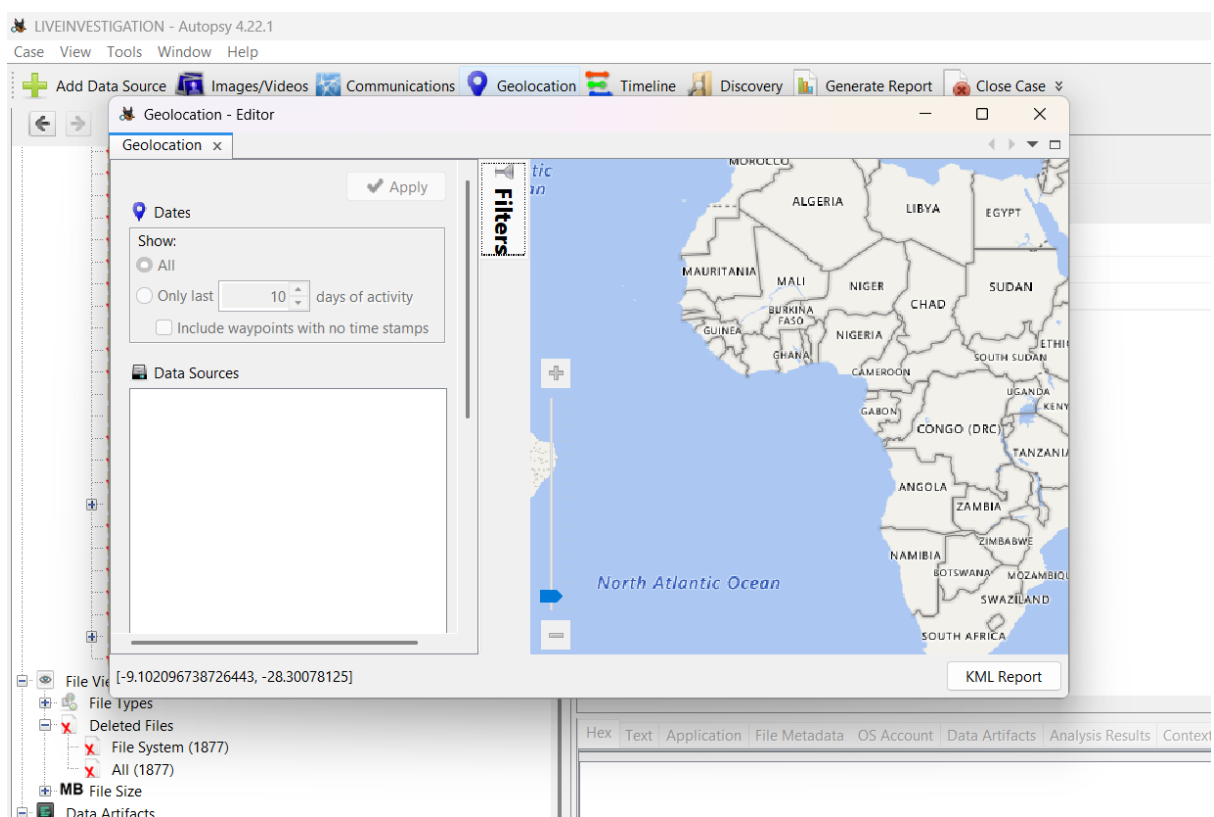
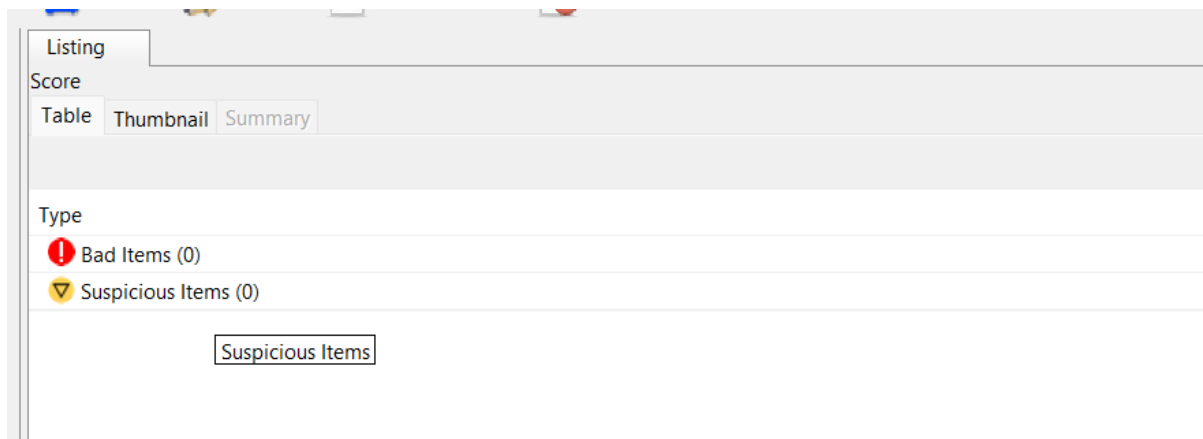
Listing

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags
ABACUS COMPETITION QUESTION PAPERS				2019-06-07 09:42:06 IST	0000-00-00 00:00:00	2019-06-14 00:00:00 IST	2019-06-14 10:31:35 IST	0	Unalloc
ABACUS CERTIFICATE LIST				2019-06-07 09:40:10 IST	0000-00-00 00:00:00	2019-06-14 00:00:00 IST	2019-06-14 10:33:35 IST	0	Unalloc
MATH SYLLABUS				2018-08-02 13:24:18 IST	0000-00-00 00:00:00	2019-06-14 00:00:00 IST	2019-06-14 10:34:07 IST	0	Unalloc
.Jock				2019-06-12 12:07:32 IST	0000-00-00 00:00:00	2019-06-14 00:00:00 IST	2019-06-14 10:34:55 IST	0	Unalloc
Miscellaneous				2019-04-30 12:54:50 IST	0000-00-00 00:00:00	2019-06-14 00:00:00 IST	2019-06-14 10:35:47 IST	0	Unalloc
SIVARANGINI				2019-02-10 17:04:50 IST	0000-00-00 00:00:00	2019-06-14 00:00:00 IST	2019-06-14 10:36:20 IST	0	Unalloc
CARD PAYMENT DETAILS				2019-06-08 11:09:04 IST	0000-00-00 00:00:00	2019-06-14 00:00:00 IST	2019-06-14 10:36:37 IST	0	Unalloc
mf-inst_eng.pdf				2022-04-24 20:24:56 IST	0000-00-00 00:00:00	2022-04-24 00:00:00 IST	2022-04-24 20:24:55 IST	3566094	Unalloc
.PT				2019-04-08 11:49:18 IST	0000-00-00 00:00:00	2019-06-14 00:00:00 IST	2019-06-14 11:00:20 IST	0	Unalloc
students database				2019-06-09 13:01:00 IST	0000-00-00 00:00:00	2019-06-14 00:00:00 IST	2019-06-14 11:04:10 IST	0	Unalloc
ABACUS BT SCHOOL CURRICULUM				2018-11-16 12:14:54 IST	0000-00-00 00:00:00	2019-06-14 00:00:00 IST	2019-06-14 11:04:35 IST	0	Unalloc
.AI				2019-05-15 11:23:50 IST	0000-00-00 00:00:00	2019-06-14 00:00:00 IST	2019-06-14 11:05:57 IST	0	Unalloc
Photos				2020-02-17 09:46:12 IST	0000-00-00 00:00:00	2020-02-17 00:00:00 IST	2020-02-17 09:46:11 IST	0	Unalloc
_SC_2538.JPG				2020-01-20 18:00:48 IST	0000-00-00 00:00:00	2020-02-18 00:00:00 IST	2020-02-17 14:08:21 IST	10898374	Unalloc
_SC_2559.JPG				2020-01-21 17:48:32 IST	0000-00-00 00:00:00	2020-02-18 00:00:00 IST	2020-02-17 14:08:38 IST	11558773	Unalloc
_SC_2634.JPG				2020-01-21 19:15:06 IST	0000-00-00 00:00:00	2020-02-18 00:00:00 IST	2020-02-17 14:08:50 IST	11602611	Unalloc

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences



Discovery

Step 1: Choose result type

Step 2: Filter which videos to show

☒ File Size:

☒ XXL Large: 10GB+  
☒ XL Large: 5-10GB  
☒ Large: 1-5GB  
☐ Medium: 100MB-1GB  
☐ Small: 500KB-100MB

☐ Data Source:

☒ SuspectUSB.E01 (ID: 1)

☒ Past Occurrences:

☒ Unique (1)  
☒ Rare (2-10)  
☒ Common (11 - 100)  
☐ Very Common (100+)  
☐ Known (NCRL)

☐ Hash Set:

☐ Interesting Item:

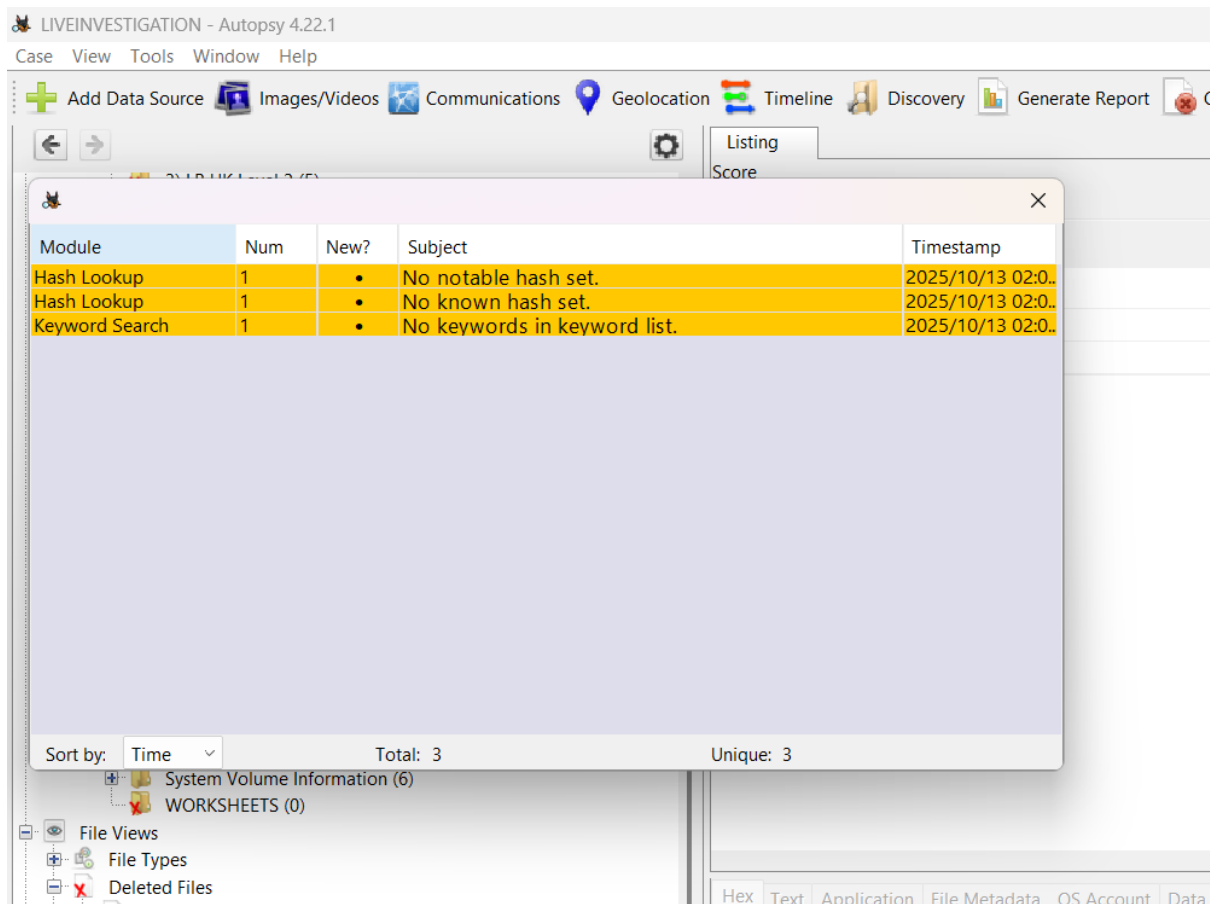
☐ Object Detected:

☐ Parent Folder:

/Windows/ (substring) (exclude)  
/Program Files/ (substring) (excl

(All will be used)

☒ Full ☐ Substring  
☒ Include ☐ Exclude



## 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.