Exp:02 **Name: Hemanth kumar**

Roll no:231901010

LIVE FORENSICS CASE INVESTIGATION USING AUTOPSY

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

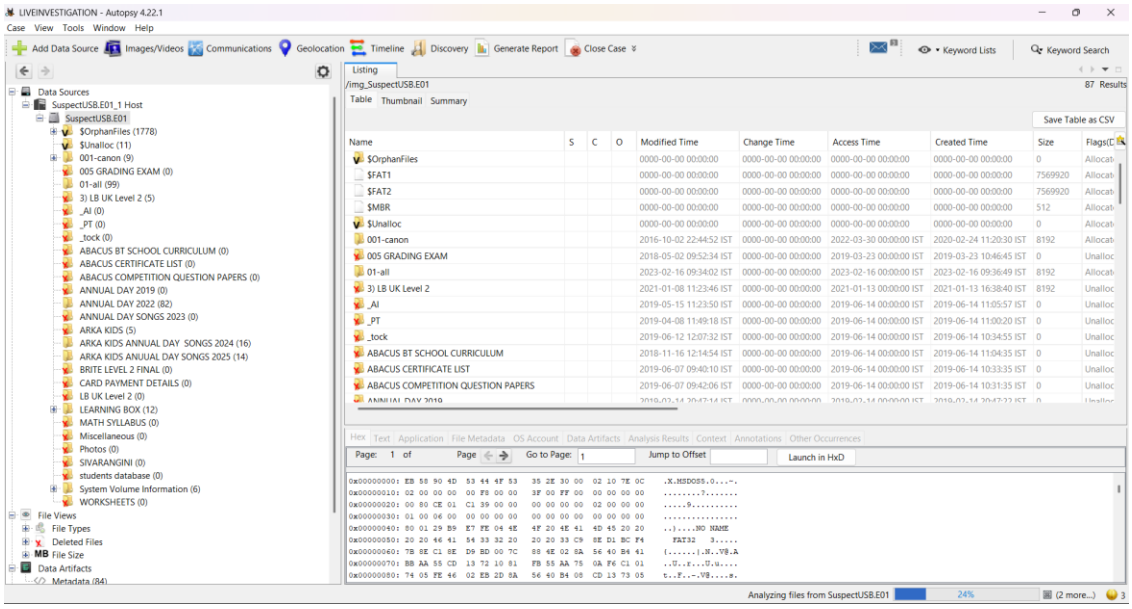
Procedure:

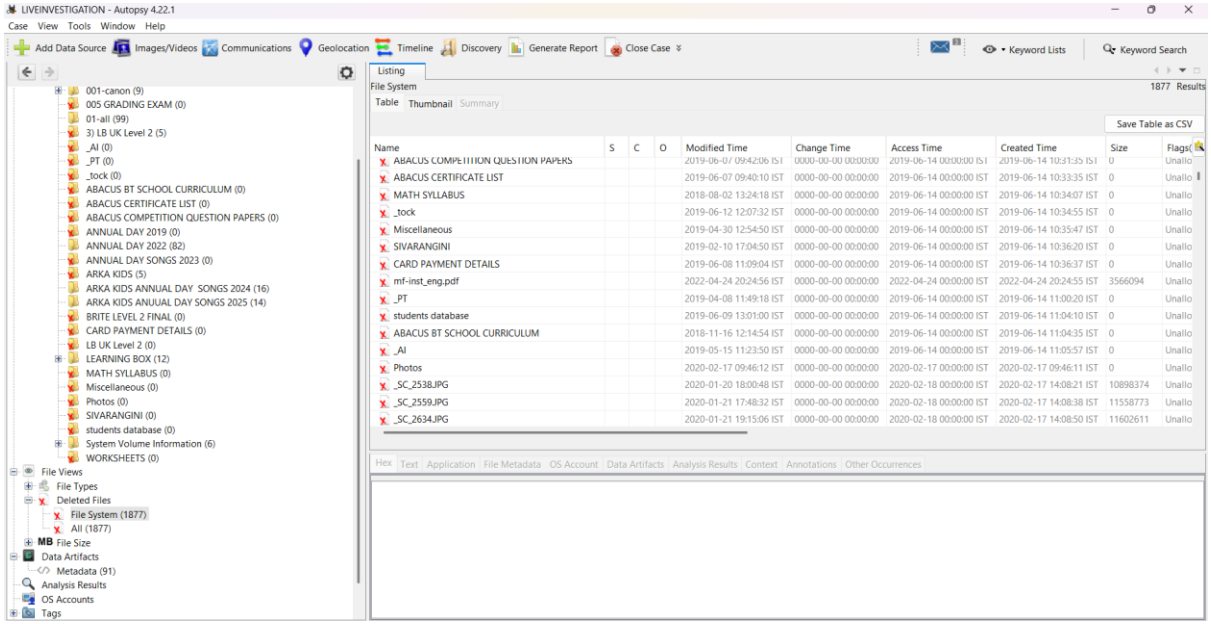
1. **Open Autopsy** from the start menu.
2. **Create a New Case**

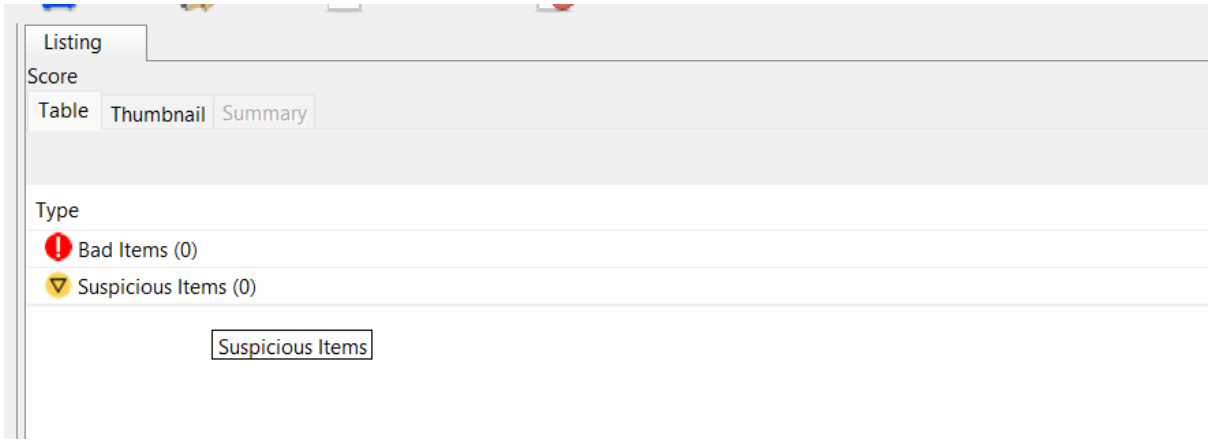
- Case Name: *LiveInvestigation*
- Case Number: *002*
- Examiner: Your Name.
- Choose a base directory for storing case files.

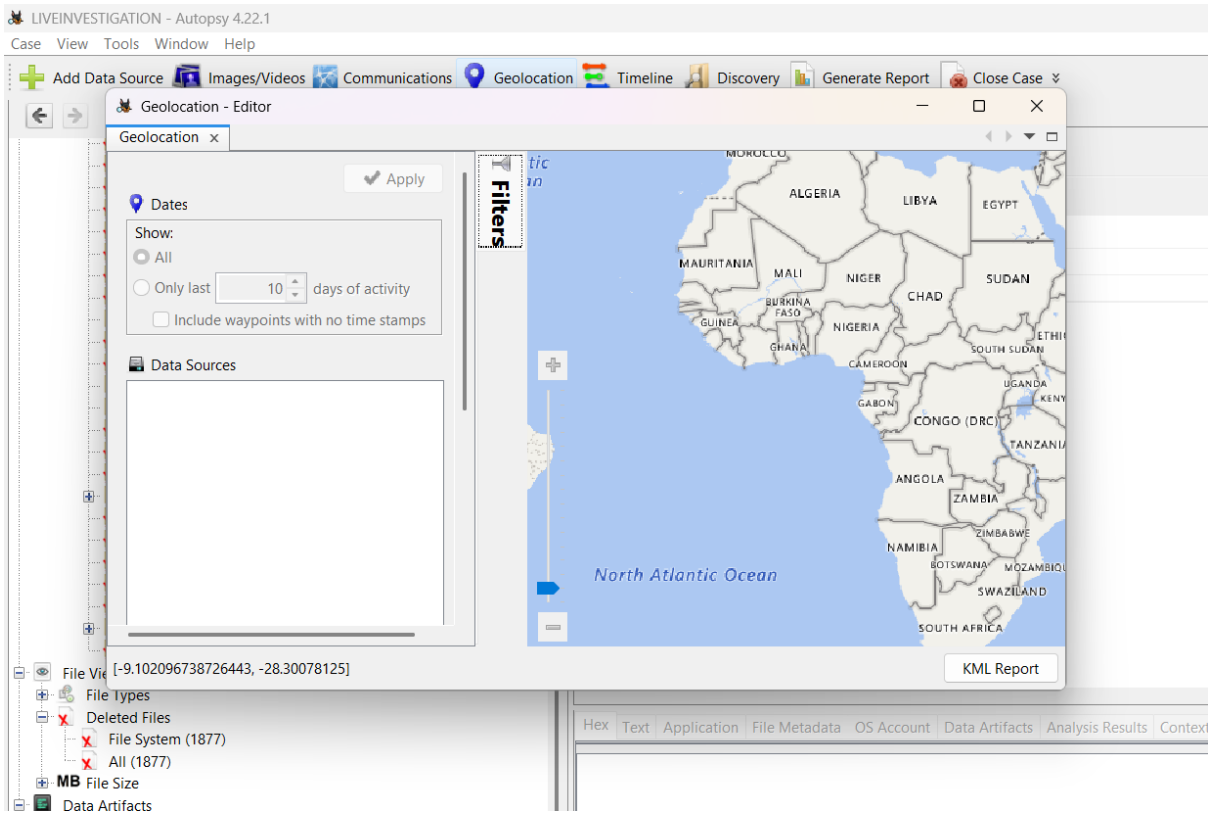
3. **Add Data Source**
   - Select **Local Disk** (for live analysis) or **Disk Image** (if working on a captured image).
   - Choose the drive/partition you want to analyze.
4. **Configure Ingest Modules**
   - Enable modules such as:
     - **Hash Lookup**
     - **Keyword Search**
     - **Recent 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

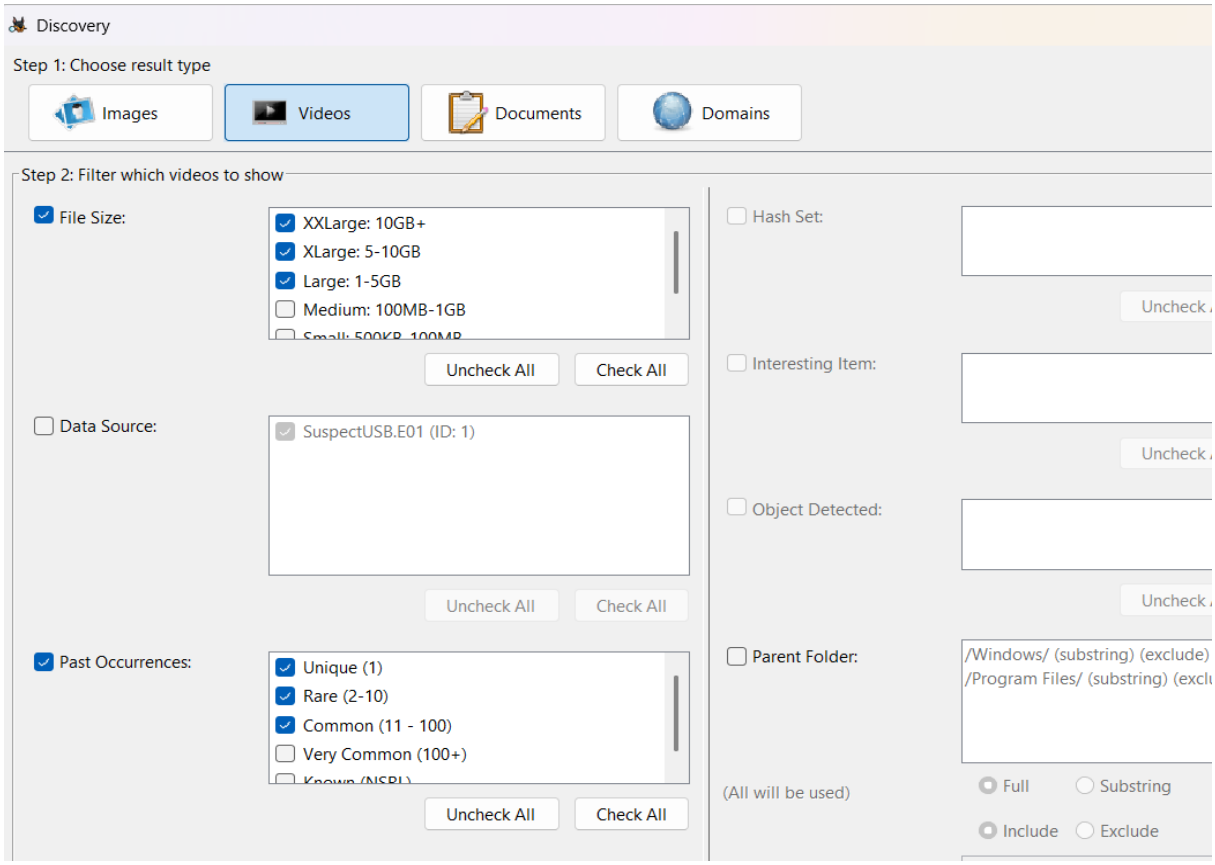
Output:

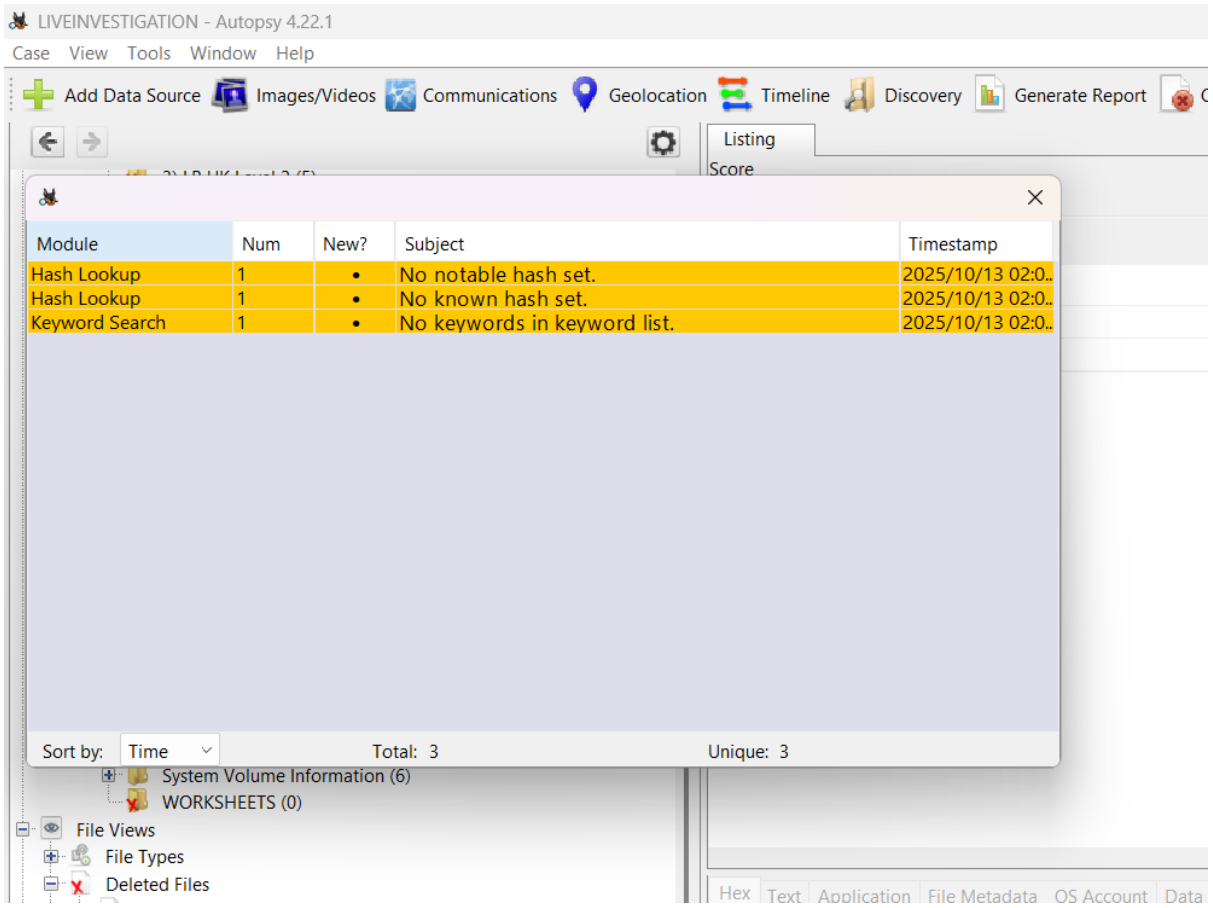

LIVEINVESTIGATION - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Data Sources
SuspectUSB.E01_1 Host
SuspectUSB.E01
$OrphanFiles (1778)
$Unalloc (11)
001-canon (9)
005 GRADING EXAM (0)
01-all (99)
3) LB UK Level 2 (5)
_AI (0)
_PT (0)
_tock (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 ANUAL 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 Size
Data Artifacts
Metadata (84)
Listing
/img_SuspectUSB.E01
87 Results
Table Thumbnail Summary
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time Size Flags(D
$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 2022-03-30 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
_tock 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
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Page: 1 of Page Go to Page: 1 Jump to Offset Launch in HxD
0x00000000: EB 58 90 4D 53 44 4F 53 35 2E 30 00 02 10 7E 0C .X.MSDOS5.0...~.
0x00000010: 02 00 00 00 00 F8 00 00 3F 00 FF 00 00 00 00 00 ....?.......
0x00000020: 00 80 CE 01 C1 39 00 00 00 00 00 00 02 00 00 00 .....9..........
0x00000030: 01 00 06 00 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 ..)....NO NAME
0x00000050: 20 20 46 41 54 33 32 20 20 20 33 C9 8E D1 BC F4 FAT32 3.....
0x00000060: 7B 8E C1 8E D9 BD 00 7C 88 4E 02 8A 56 40 B4 41 {.....|.N..V@.A
0x00000070: BB AA 55 CD 13 72 10 81 FB 55 AA 75 0A F6 C1 01 ..U..r...U.u....
0x00000080: 74 05 FE 46 02 EB 2D 8A 56 40 B4 08 CD 13 73 05 t..F..-.V@....s.
Analyzing files from SuspectUSB.E01 24% (2 more...) 3


LIVEINVESTIGATION - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
001-canon (9)
005 GRADING EXAM (0)
01-all (99)
3) LB UK Level 2 (5)
_AI (0)
_PT (0)
_tock (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 ANUAL 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)
All (1877)
File Size
Data Artifacts
Metadata (91)
Analysis Results
OS Accounts
Tags
Listing
File System
1877 Results
Table Thumbnail Summary
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time Size Flags(
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 Unallo
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 Unallo
_tock 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 Unallo
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 Unallo
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 Unallo
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 Unallo
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 Unallo
_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 Unallo
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 Unallo
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 Unallo
_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 Unallo
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 Unallo
_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 Unallo
_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 Unallo
_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 Unallo
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences


Listing
Score
Table
Thumbnail
Summary
Type
Bad Items (0)
Suspicious Items (0)
Suspicious Items


LIVEINVESTIGATION - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Geolocation - Editor
Geolocation
Apply
Dates
Show:
All
Only last 10 days of activity
Include waypoints with no time stamps
Data Sources
Filters
ALGERIA
LIBYA
EGYPT
MAURITANIA
MALI
NIGER
CHAD
SUDAN
BURKINA FASO
GUINEA
NIGERIA
GHANA
CAMEROON
SOUTH SUDAN
UGANDA
GABON
CONGO (DRC)
TANZANIA
ANGOLA
ZAMBIA
ZIMBABWE
NAMIBIA
BOTSWANA
SWAZILAND
SOUTH AFRICA
North Atlantic Ocean
[-9.102096738726443, -28.30078125]
KML Report
File Types
Deleted Files
File System (1877)
All (1877)
File Size
Data Artifacts
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results


Discovery
Step 1: Choose result type
Images
Videos
Documents
Domains
Step 2: Filter which videos to show
File Size:
XXLarge: 10GB+
XLarge: 5-10GB
Large: 1-5GB
Medium: 100MB-1GB
Uncheck All
Check All
Data Source:
SuspectUSB.E01 (ID: 1)
Uncheck All
Check All
Past Occurrences:
Unique (1)
Rare (2-10)
Common (11 - 100)
Very Common (100+)
Uncheck All
Check All
Hash Set:
Uncheck
Interesting Item:
Uncheck
Object Detected:
Uncheck
Parent Folder:
/Windows/ (substring) (exclude)
/Program Files/ (substring) (excl
(All will be used)
Full
Substring
Include
Exclude


LIVEINVESTIGATION - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Listing
Score
Module Num New? Subject Timestamp
Hash Lookup 1 • No notable hash set. 2025/10/13 02:0..
Hash Lookup 1 • No known hash set. 2025/10/13 02:0..
Keyword Search 1 • No keywords in keyword list. 2025/10/13 02:0..
Sort by: Time
Total: 3
Unique: 3
System Volume Information (6)
WORKSHEETS (0)
File Views
File Types
Deleted Files
Hex
Text
Application
File Metadata
OS Account
Data

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.