Ex No-5: Use Autopsy to create a case and import evidence

AIM:

To analyze a forensic disk image using Autopsy and extract digital evidence.

Description:

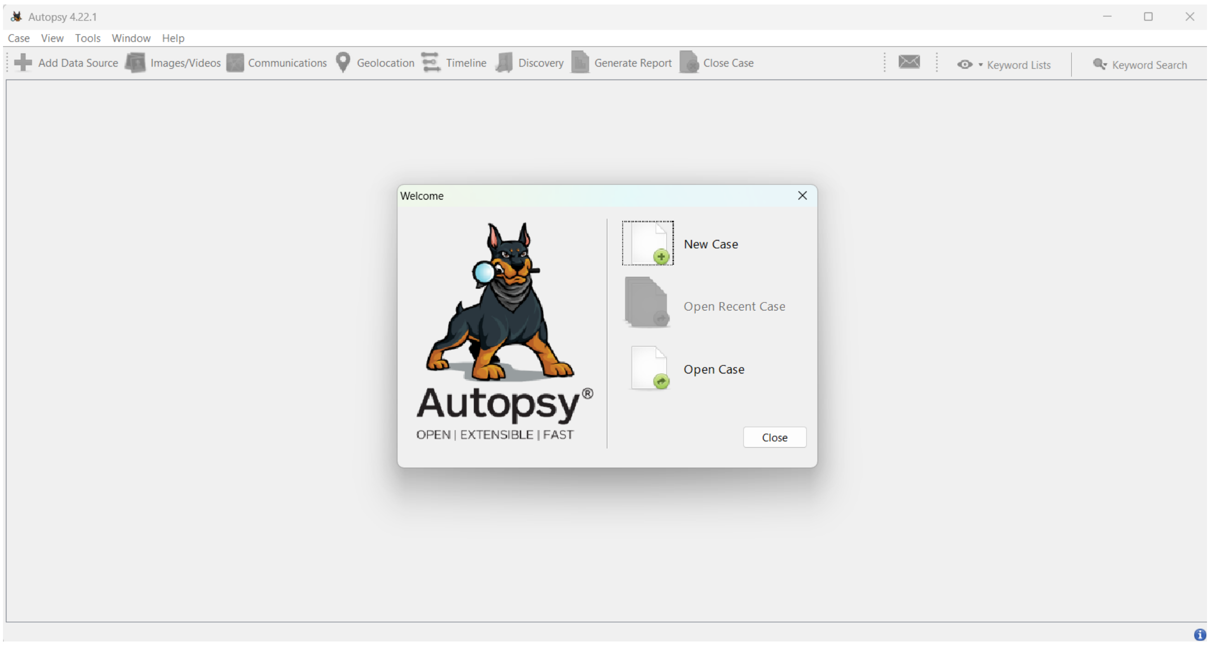
Autopsy is an open-source digital forensics platform used for analyzing and extracting data from digital devices. Here's a step-by-step process on how to use Autopsy for a basic forensic investigation.

1. Installation

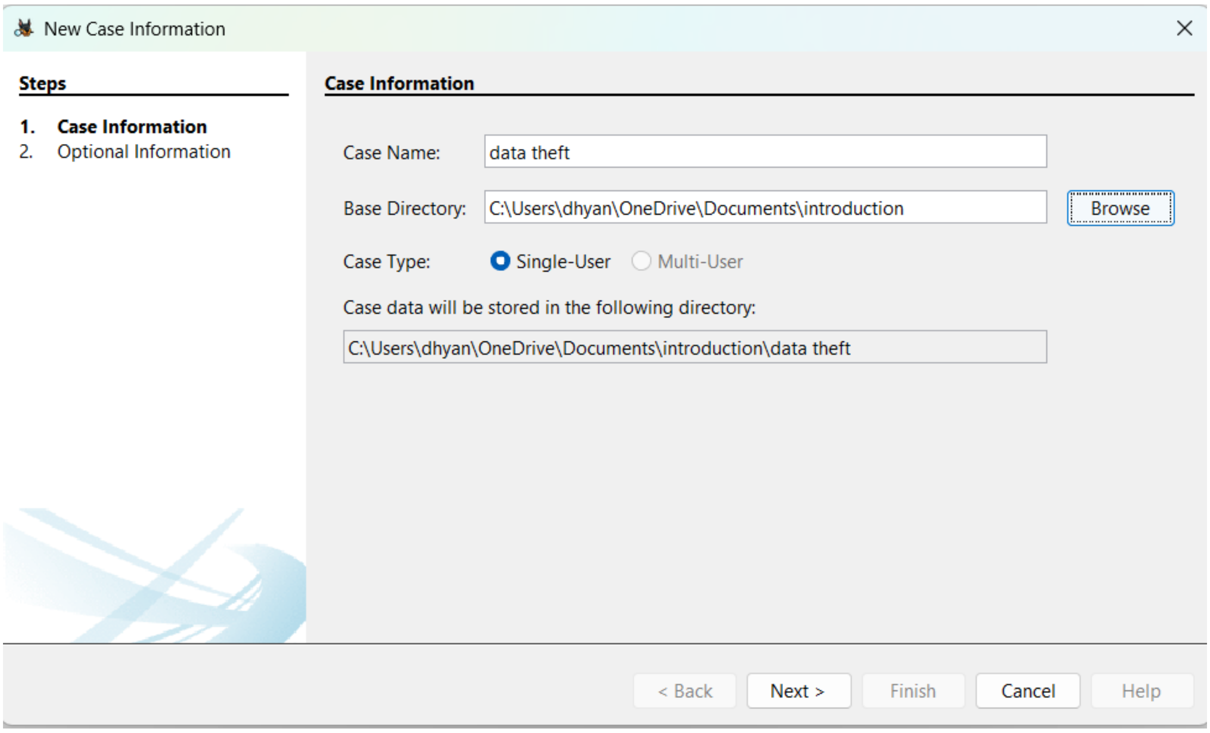
- Download and Install: Autopsy can be downloaded from the official website. Follow the installation instructions based on your operating system (Windows, Linux, or macOS).

2. Starting a New Case

- Create a new case by clicking on New Case



Step-2: Enter the case name and location where the case data will be stored. Fill in the details like the case number, examiner's name, etc., and click Next.



1. **Case Information**
2. Optional Information

Case Name: data theft

Base Directory: C:\Users\dhyan\OneDrive\Documents\introduction

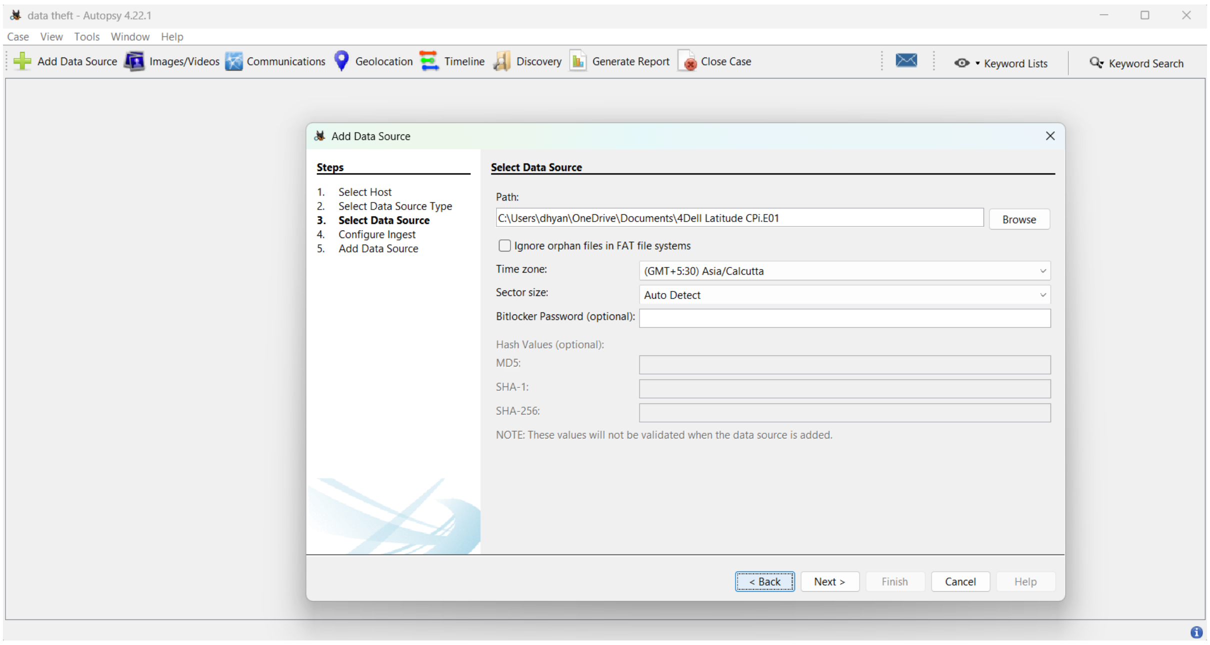
Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

C:\Users\dhyan\OneDrive\Documents\introduction\data theft

Step-3: Adding a Data Soucre

- Choose the Type of Data Source
- Select the Data Source
- Configure Ingest Modules
- Start Analysis



1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Path:

C:\Users\dhyan\OneDrive\Documents\4Dell Latitude CPi.E01

☐ Ignore orphan files in FAT file systems

Time zone: (GMT+5:30) Asia/Calcutta

Sector size: Auto Detect

Bitlocker Password (optional):

Hash Values (optional):

MD5:

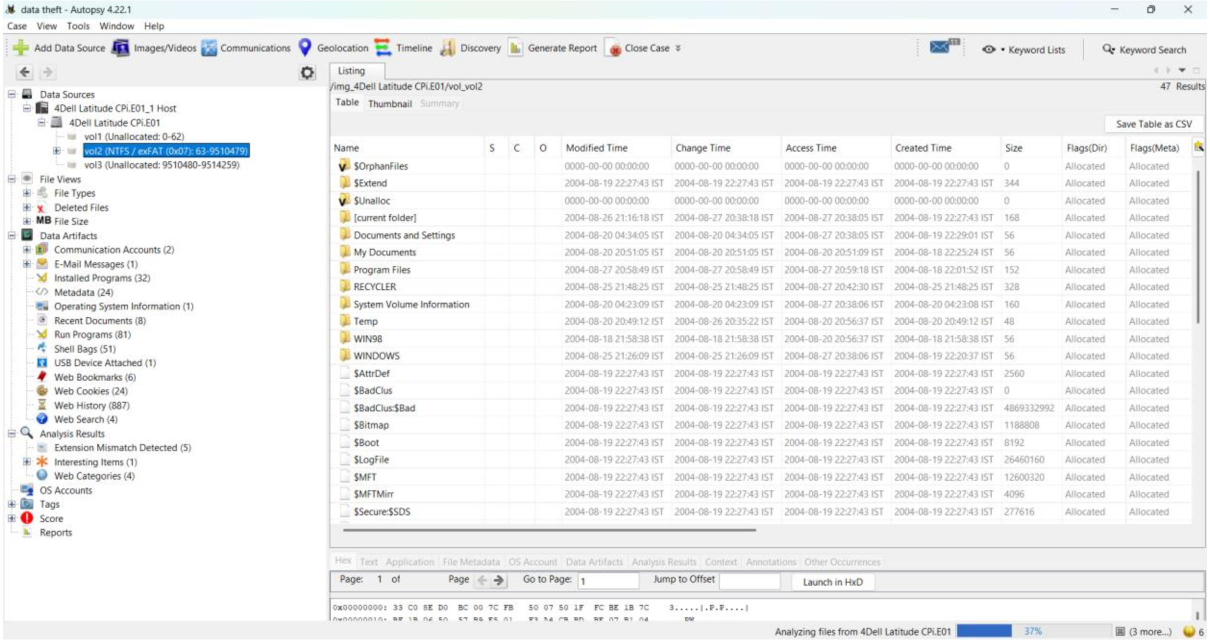
SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

Step-4: Initial Analysis and Overview

- Ingest Progress
- Explore the Resulting Artifacts
- Use the Tree Viewer



/img_4Dell Latitude CPi.E01/vol_vol2

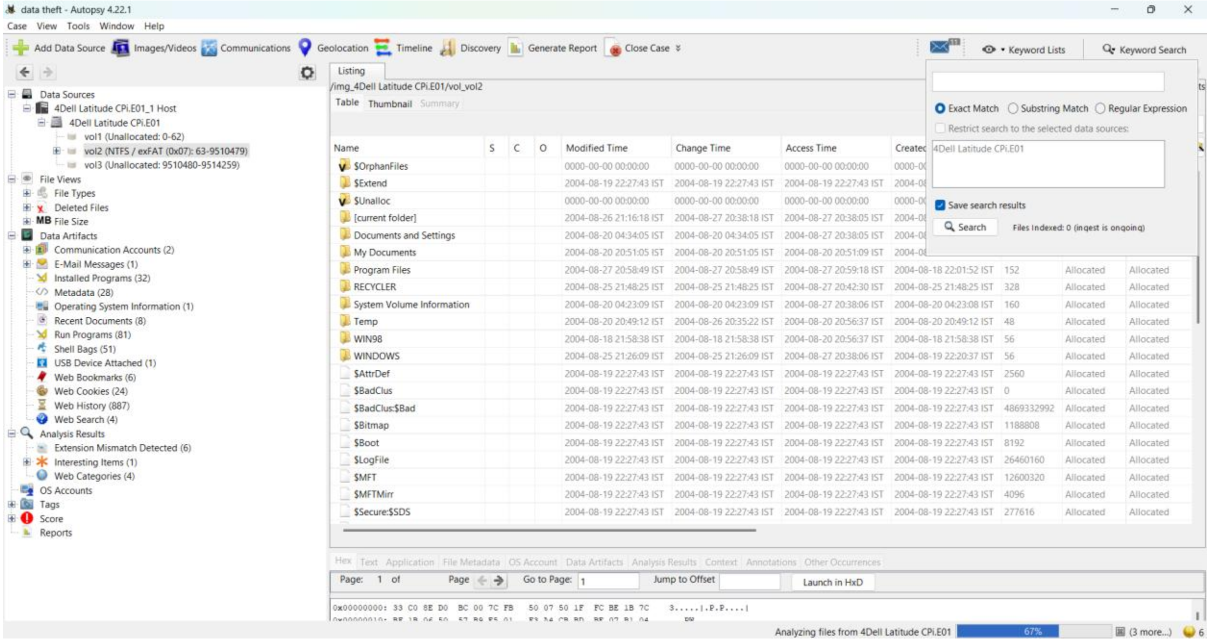
47 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
$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	Allocated	Allocated
$Extend				2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	344	Allocated	Allocated
$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	Allocated	Allocated
[current folder]				2004-08-26 21:16:18 IST	2004-08-27 20:38:18 IST	2004-08-27 20:38:05 IST	2004-08-19 22:27:43 IST	168	Allocated	Allocated
Documents and Settings				2004-08-20 04:34:05 IST	2004-08-20 04:34:05 IST	2004-08-27 20:38:05 IST	2004-08-19 22:29:01 IST	56	Allocated	Allocated
My Documents				2004-08-20 20:51:05 IST	2004-08-20 20:51:05 IST	2004-08-20 20:51:09 IST	2004-08-18 22:25:24 IST	56	Allocated	Allocated
Program Files				2004-08-27 20:58:49 IST	2004-08-27 20:58:49 IST	2004-08-27 20:59:18 IST	2004-08-18 22:01:52 IST	152	Allocated	Allocated
RECYCLER				2004-08-25 21:48:25 IST	2004-08-25 21:48:25 IST	2004-08-27 20:42:30 IST	2004-08-25 21:48:25 IST	328	Allocated	Allocated
System Volume Information				2004-08-20 04:23:09 IST	2004-08-20 04:23:09 IST	2004-08-27 20:38:06 IST	2004-08-20 04:23:08 IST	160	Allocated	Allocated
Temp				2004-08-20 20:49:12 IST	2004-08-26 20:35:22 IST	2004-08-20 20:56:37 IST	2004-08-20 20:49:12 IST	48	Allocated	Allocated
WIN98				2004-08-18 21:58:38 IST	2004-08-18 21:58:38 IST	2004-08-20 20:56:37 IST	2004-08-18 21:58:38 IST	56	Allocated	Allocated
WINDOWS				2004-08-25 21:26:09 IST	2004-08-25 21:26:09 IST	2004-08-27 20:38:06 IST	2004-08-19 22:20:37 IST	56	Allocated	Allocated
$AttrDef				2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2560	Allocated	Allocated
$BadClus				2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	0	Allocated	Allocated
$BadClus:$Bad				2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	4869332992	Allocated	Allocated
$Bitmap				2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	1188808	Allocated	Allocated
$Boot				2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	8192	Allocated	Allocated
$LogFile				2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	26460160	Allocated	Allocated
$MFT				2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	12600320	Allocated	Allocated
$MFTMirr				2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	4096	Allocated	Allocated
$Secure:$SDS				2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	277616	Allocated	Allocated

```
0x00000000: 33 C0 8E D0  BC 00 7C FB   50 07 50 1F  FC BE 1B 7C    3.....|.P.P....|
```

Step-5: Detailed Analysis

- Keyword Search:
    - You can perform specific keyword searches using the Keyword Search module.
    - Use pre-configured lists or enter custom keywords.
- File Analysis:
    - Navigate through files and folders under the File Types or File System section.
    - Open, view, or export files for further examination.
- Timeline Analysis:
    - Use the Timeline module to visualize events based on timestamps.
    - This can help track user activity over time.
- Hash Analysis:
    - Compare file hashes with known databases to identify known good or bad files.



- Data Sources
  - 4Dell Latitude CPi.E01_1 Host
    - 4Dell Latitude CPi.E01
      - vol1 (Unallocated: 0-62)
      - vol2 (NTFS / exFAT (0x07): 63-9510479)
      - vol3 (Unallocated: 9510480-9514259)
- File Views
  - File Types
  - Deleted Files
  - MB File Size
- Data Artifacts
  - Communication Accounts (2)
  - E-Mail Messages (1)
  - Installed Programs (32)
  - Metadata (28)
  - Operating System Information (1)
  - Recent Documents (8)
  - Run Programs (81)
  - Shell Bags (51)
  - USB Device Attached (1)
  - Web Bookmarks (6)
  - Web Cookies (24)
  - Web History (887)
  - Web Search (4)
- Analysis Results
  - Extension Mismatch Detected (6)
  - Interesting Items (1)
  - Web Categories (4)
- OS Accounts
- Tags
- Score
- Reports

/img_4Dell Latitude CPi.E01/vol_vol2

Name	S	C	O	Modified Time	Change Time	Access Time	Createc			
$OrphanFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-0			
$Extend				2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-0			
$Unalloc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-0			
[current folder]				2004-08-26 21:16:18 IST	2004-08-27 20:38:18 IST	2004-08-27 20:38:05 IST	2004-0			
Documents and Settings				2004-08-20 04:34:05 IST	2004-08-20 04:34:05 IST	2004-08-27 20:38:05 IST	2004-0			
My Documents				2004-08-20 20:51:05 IST	2004-08-20 20:51:05 IST	2004-08-20 20:51:09 IST	2004-0			
Program Files				2004-08-27 20:58:49 IST	2004-08-27 20:58:49 IST	2004-08-27 20:59:18 IST	2004-08-18 22:01:52 IST	152	Allocated	Allocated
RECYCLER				2004-08-25 21:48:25 IST	2004-08-25 21:48:25 IST	2004-08-27 20:42:30 IST	2004-08-25 21:48:25 IST	328	Allocated	Allocated
System Volume Information				2004-08-20 04:23:09 IST	2004-08-20 04:23:09 IST	2004-08-27 20:38:06 IST	2004-08-20 04:23:08 IST	160	Allocated	Allocated
Temp				2004-08-20 20:49:12 IST	2004-08-26 20:35:22 IST	2004-08-20 20:56:37 IST	2004-08-20 20:49:12 IST	48	Allocated	Allocated
WIN98				2004-08-18 21:58:38 IST	2004-08-18 21:58:38 IST	2004-08-20 20:56:37 IST	2004-08-18 21:58:38 IST	56	Allocated	Allocated
WINDOWS				2004-08-25 21:26:09 IST	2004-08-25 21:26:09 IST	2004-08-27 20:38:06 IST	2004-08-19 22:20:37 IST	56	Allocated	Allocated
$AttrDef				2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2560	Allocated	Allocated
$BadClus				2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	0	Allocated	Allocated
$BadClus:$Bad				2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	4869332992	Allocated	Allocated
$Bitmap				2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	1188808	Allocated	Allocated
$Boot				2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	8192	Allocated	Allocated
$LogFile				2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	26460160	Allocated	Allocated
$MFT				2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	12600320	Allocated	Allocated
$MFTMirr				2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	4096	Allocated	Allocated
$Secure:$SDS				2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	277616	Allocated	Allocated

● Exact Match ○ Substring Match ○ Regular Expression

□ Restrict search to the selected data sources:

4Dell Latitude CPi.E01

☑ Save search results

Search Files Indexed: 0 (ingest is ongoing)

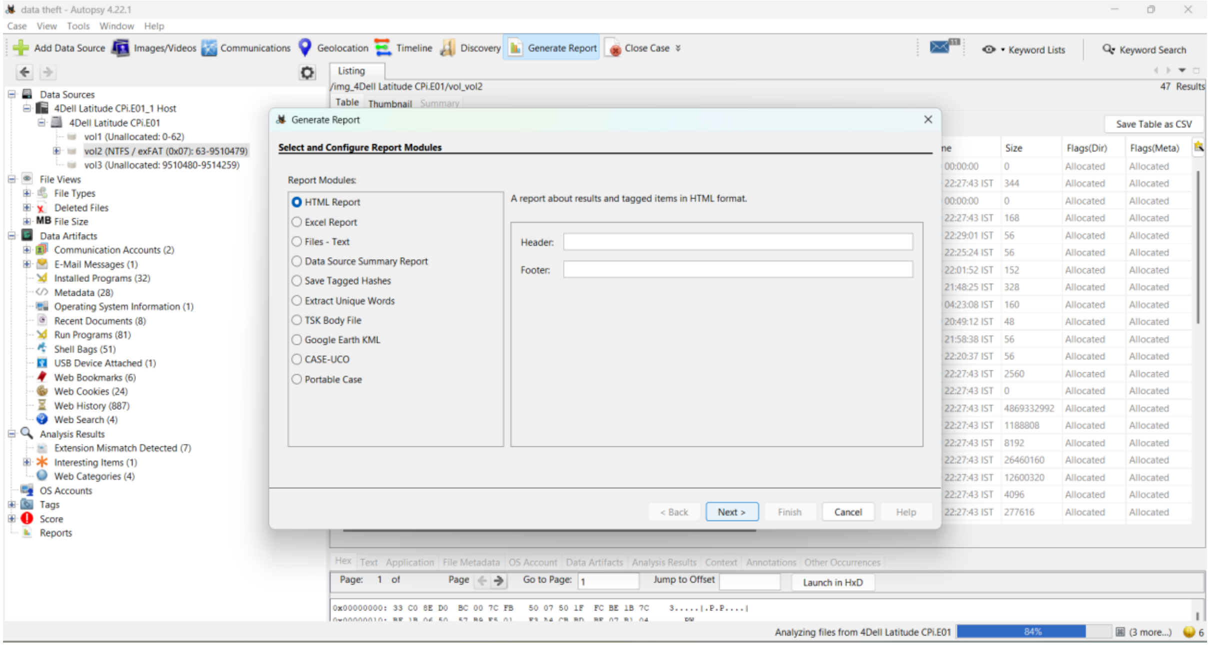
Page: 1 of Page Go to Page: 1 Jump to Offset Launch in HxD

```
0x00000000: 33 C0 8E D0  BC 00 7C FB   50 07 50 1F  FC BE 1B 7C    3.....|.P.P....|
```

Analyzing files from 4Dell Latitude CPi.E01 67% (3 more...) 6

Step-6: Reporting

- Generate a Report:
  - After analyzing the data, click on Generate Report from the toolbar.
  - Choose the type of report (HTML, CSV, Excel, etc.).
  - Select which parts of the analysis you want to include in the report.
- Export Findings:
  - Export individual files or artifacts that you need for your report or further analysis.
- Final Review:
  - Review the report to ensure it includes all relevant information.
  - Save or print the report for use in your case.



Select and Configure Report Modules

Report Modules:

- ● HTML Report
- ○ Excel Report
- ○ Files - Text
- ○ Data Source Summary Report
- ○ Save Tagged Hashes
- ○ Extract Unique Words
- ○ TSK Body File
- ○ Google Earth KML
- ○ CASE-UCO
- ○ Portable Case

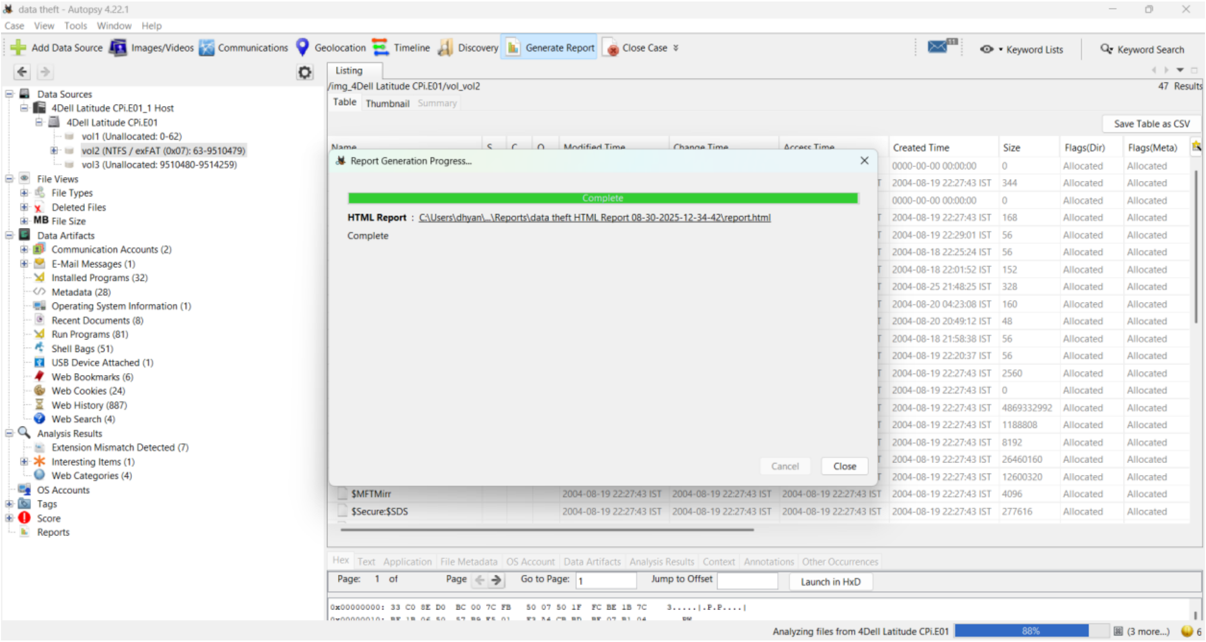
A report about results and tagged items in HTML format.

Header:

Footer:

```
0x00000000: 33 C0 8E D0  BC 00 7C FB  50 07 50 1F  FC BE 1B 7C    3.....|.P.P....|
```

Report Generation Progress

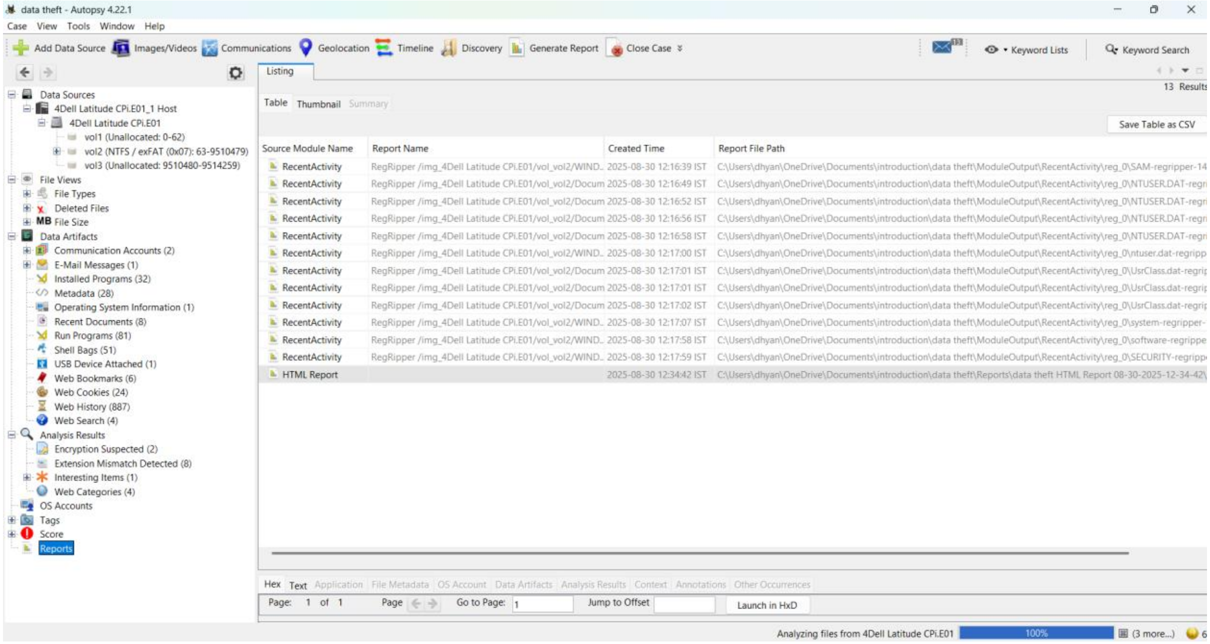


Complete

HTML Report : C:\Users\dhyan\...\Reports\data theft HTML Report 08-30-2025-12-34-42\report.html

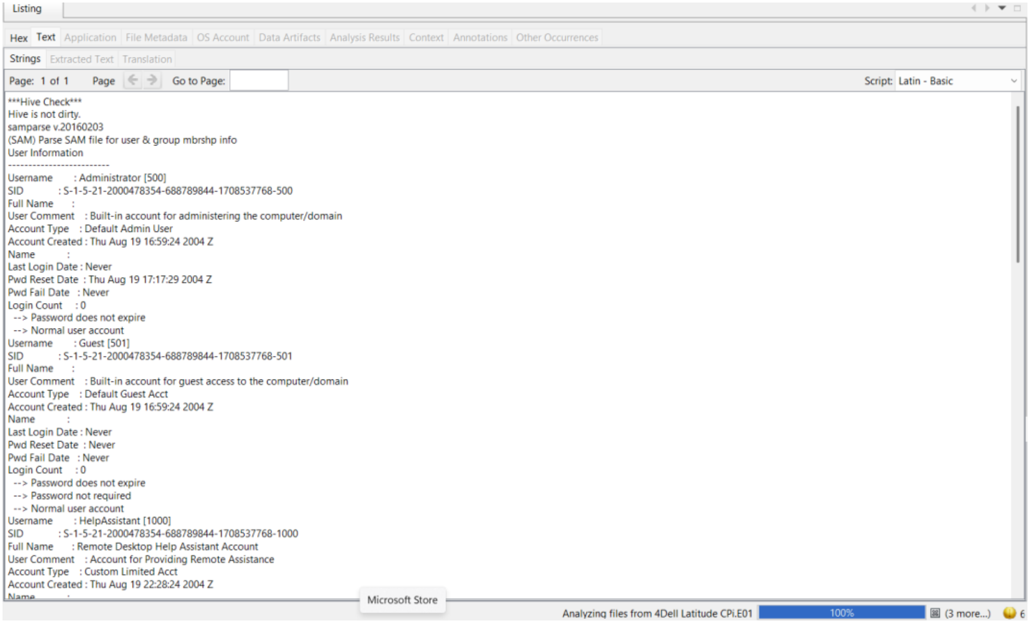
Complete

Reports



Source Module Name	Report Name	Created Time	Report File Path
RecentActivity	RegRipper /img_4Dell Latitude CPi.E01/vol_vol2/WIND...	2025-08-30 12:16:39 IST	C:\Users\dhyan\OneDrive\Documents\introduction\data theft\ModuleOutput\RecentActivity\reg_0\SAM-regripper-14
RecentActivity	RegRipper /img_4Dell Latitude CPi.E01/vol_vol2/Docum	2025-08-30 12:16:49 IST	C:\Users\dhyan\OneDrive\Documents\introduction\data theft\ModuleOutput\RecentActivity\reg_0\NTUSER.DAT-regri
RecentActivity	RegRipper /img_4Dell Latitude CPi.E01/vol_vol2/Docum	2025-08-30 12:16:52 IST	C:\Users\dhyan\OneDrive\Documents\introduction\data theft\ModuleOutput\RecentActivity\reg_0\NTUSER.DAT-regri
RecentActivity	RegRipper /img_4Dell Latitude CPi.E01/vol_vol2/Docum	2025-08-30 12:16:56 IST	C:\Users\dhyan\OneDrive\Documents\introduction\data theft\ModuleOutput\RecentActivity\reg_0\NTUSER.DAT-regri
RecentActivity	RegRipper /img_4Dell Latitude CPi.E01/vol_vol2/Docum	2025-08-30 12:16:58 IST	C:\Users\dhyan\OneDrive\Documents\introduction\data theft\ModuleOutput\RecentActivity\reg_0\NTUSER.DAT-regri
RecentActivity	RegRipper /img_4Dell Latitude CPi.E01/vol_vol2/WIND...	2025-08-30 12:17:00 IST	C:\Users\dhyan\OneDrive\Documents\introduction\data theft\ModuleOutput\RecentActivity\reg_0\ntuser.dat-regripp
RecentActivity	RegRipper /img_4Dell Latitude CPi.E01/vol_vol2/Docum	2025-08-30 12:17:01 IST	C:\Users\dhyan\OneDrive\Documents\introduction\data theft\ModuleOutput\RecentActivity\reg_0\UsrClass.dat-regrip
RecentActivity	RegRipper /img_4Dell Latitude CPi.E01/vol_vol2/Docum	2025-08-30 12:17:01 IST	C:\Users\dhyan\OneDrive\Documents\introduction\data theft\ModuleOutput\RecentActivity\reg_0\UsrClass.dat-regrip
RecentActivity	RegRipper /img_4Dell Latitude CPi.E01/vol_vol2/Docum	2025-08-30 12:17:02 IST	C:\Users\dhyan\OneDrive\Documents\introduction\data theft\ModuleOutput\RecentActivity\reg_0\UsrClass.dat-regrip
RecentActivity	RegRipper /img_4Dell Latitude CPi.E01/vol_vol2/WIND...	2025-08-30 12:17:07 IST	C:\Users\dhyan\OneDrive\Documents\introduction\data theft\ModuleOutput\RecentActivity\reg_0\system-regripper-
RecentActivity	RegRipper /img_4Dell Latitude CPi.E01/vol_vol2/WIND...	2025-08-30 12:17:58 IST	C:\Users\dhyan\OneDrive\Documents\introduction\data theft\ModuleOutput\RecentActivity\reg_0\software-regrippe
RecentActivity	RegRipper /img_4Dell Latitude CPi.E01/vol_vol2/WIND...	2025-08-30 12:17:59 IST	C:\Users\dhyan\OneDrive\Documents\introduction\data theft\ModuleOutput\RecentActivity\reg_0\SECURITY-regripp
HTML Report		2025-08-30 12:34:42 IST	C:\Users\dhyan\OneDrive\Documents\introduction\data theft\Reports\data theft HTML Report 08-30-2025-12-34-42\

Text in the report


Listing
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Strings Extracted Text Translation
Page: 1 of 1 Page Go to Page:
Script: Latin - Basic
Microsoft Store
Analyzing files from 4Dell Latitude CPi.E01 100% (3 more...) 6

```
***Hive Check***
Hive is not dirty.
samparse v.20160203
(SAM) Parse SAM file for user & group mbrshp info
User Information
-------------------------
Username        : Administrator [500]
SID             : S-1-5-21-2000478354-688789844-1708537768-500
Full Name       :
User Comment    : Built-in account for administering the computer/domain
Account Type    : Default Admin User
Account Created : Thu Aug 19 16:59:24 2004 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Thu Aug 19 17:17:29 2004 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Normal user account
Username        : Guest [501]
SID             : S-1-5-21-2000478354-688789844-1708537768-501
Full Name       :
User Comment    : Built-in account for guest access to the computer/domain
Account Type    : Default Guest Acct
Account Created : Thu Aug 19 16:59:24 2004 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Password not required
  --> Normal user account
Username        : HelpAssistant [1000]
SID             : S-1-5-21-2000478354-688789844-1708537768-1000
Full Name       : Remote Desktop Help Assistant Account
User Comment    : Account for Providing Remote Assistance
Account Type    : Custom Limited Acct
Account Created : Thu Aug 19 22:28:24 2004 Z
Name            :
```

Step-7: Case Closure

- Close the Case:
  - Once you have completed your investigation, close the case within Autopsy.
- Archiving:
  - Ensure all data and reports are properly archived according to your organization's policies.