Ex.No 5: Use Autopsy to Create a Case and Import Evidence

Description

Autopsy is an open-source digital forensics platform used for analyzing and extracting data from digital devices. Below is a step-by-step guide to perform a basic forensic investigation using Autopsy.

---

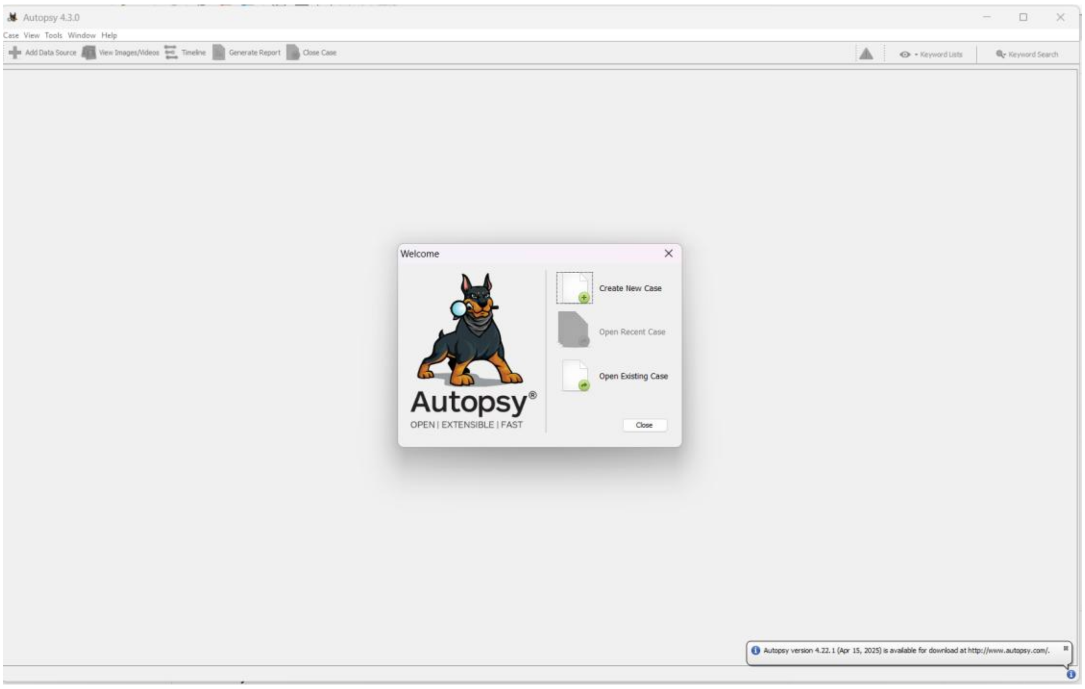
1. Installation

- Download Autopsy from the official website.
- Install it following the instructions for your operating system (Windows, Linux, or macOS).

---

2. Starting a New Case

- Launch the Autopsy application.
- Click on **New Case**.
- Enter the case name and choose a storage location for the case data.
- Fill in details such as the case number, examiner's name, and other metadata.
- Click **Next** to proceed.

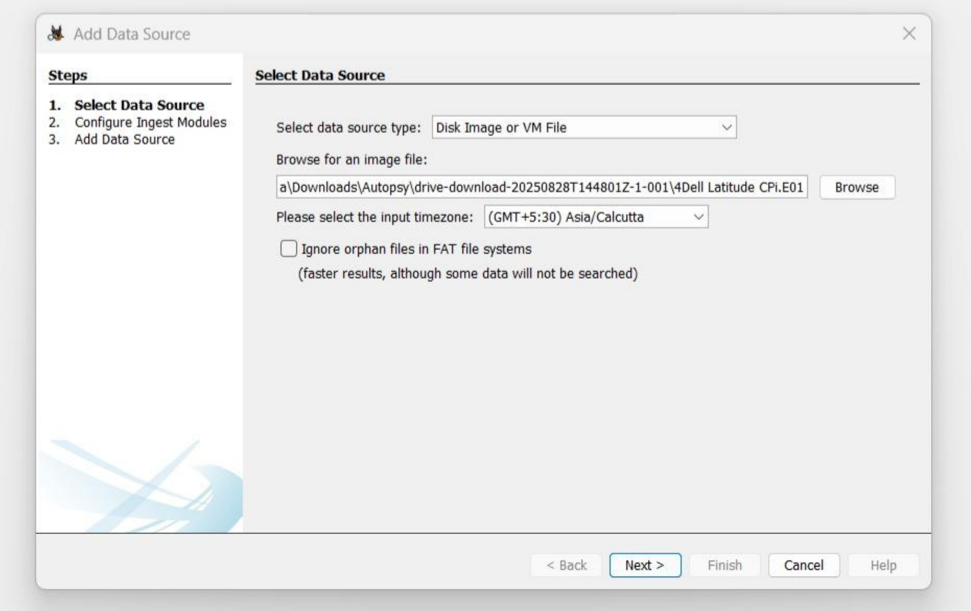


Autopsy version 4.22.1 (Apr 15, 2025) is available for download at http://www.autopsy.com/.

---

3. Adding a Data Source

- Select the type of data source (disk image, local disk, logical files, etc.).
- Browse and select the evidence file or drive.
- Configure ingest modules (such as file type identification, hash lookup, keyword search).
- Start the analysis.



Select Data Source

Select data source type: Disk Image or VM File

Browse for an image file: a\Downloads\Autopsy\drive-download-20250828T144801Z-1-001\4Dell Latitude CPi.E01

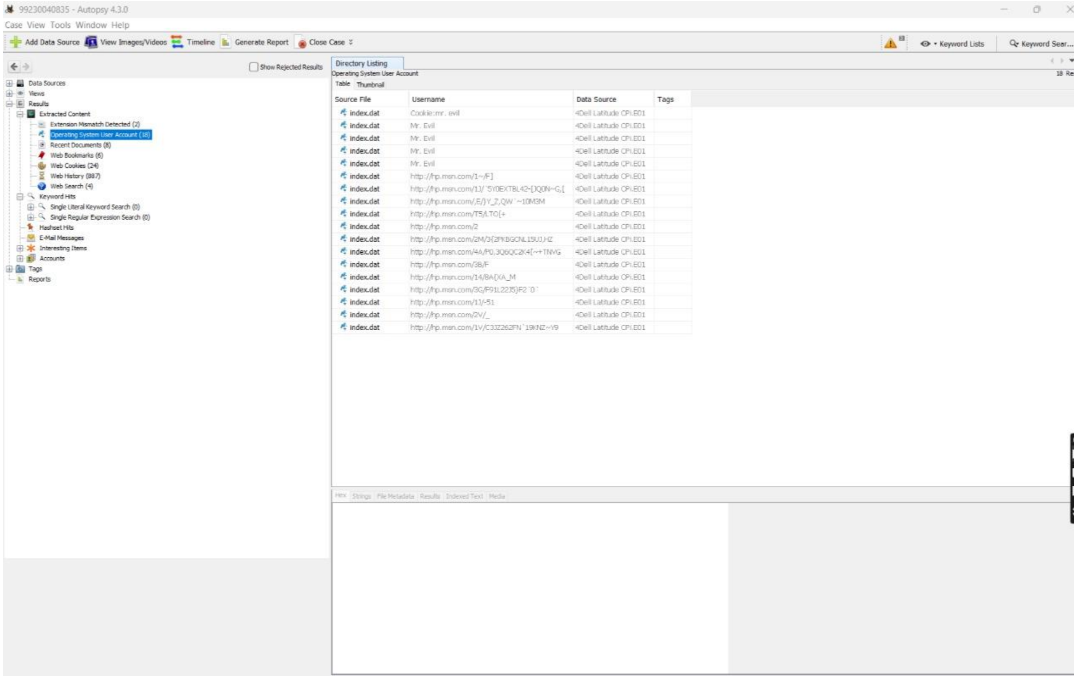
Please select the input timezone: (GMT+5:30) Asia/Calcutta

☐ Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)

---

4. Initial Analysis and Overview

- Monitor the ingest progress displayed at the bottom of the screen.
- Explore the artifacts generated by Autopsy (web history, recent documents, deleted files, etc.).
- Use the tree viewer to navigate different categories of evidence.



Operating System User Account

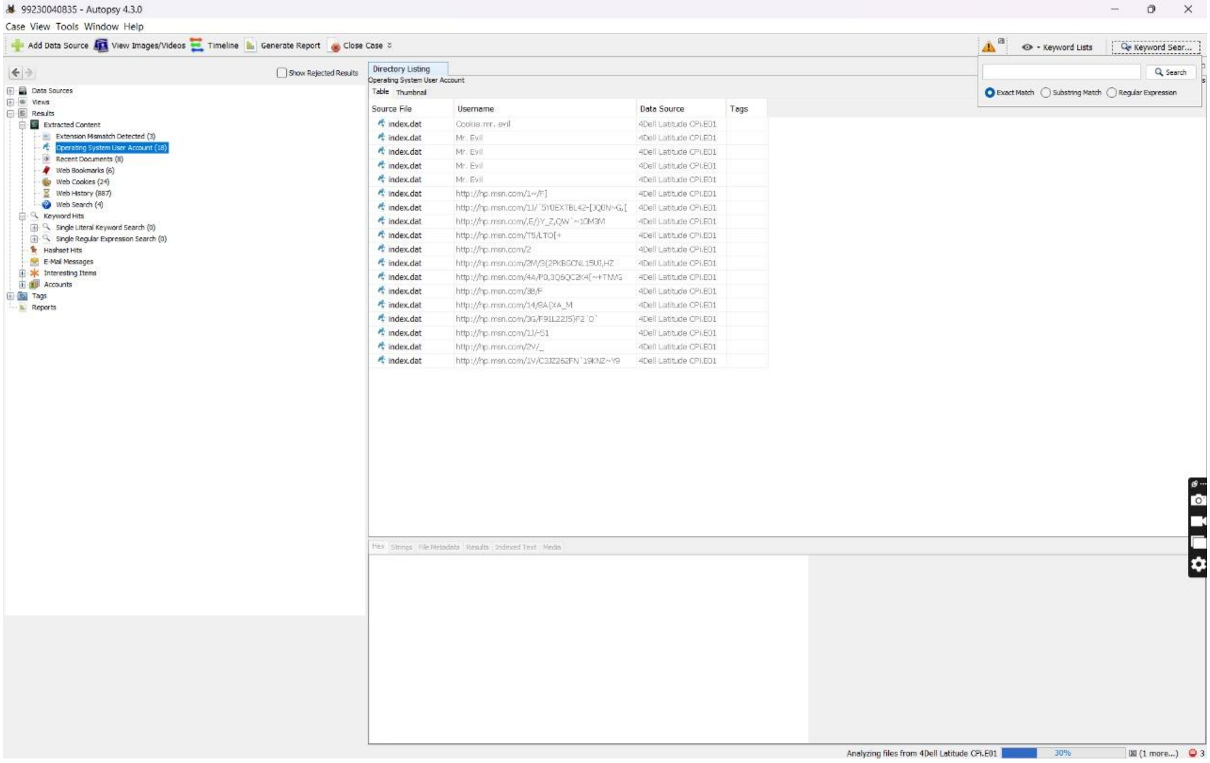
Source File	Username	Data Source	Tags
index.dat	Cookie:mr. evil	4Dell Latitude CPi.E01	
index.dat	Mr. Evil	4Dell Latitude CPi.E01	
index.dat	Mr. Evil	4Dell Latitude CPi.E01	
index.dat	Mr. Evil	4Dell Latitude CPi.E01	
index.dat	Mr. Evil	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/1~/F]	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/1J/`5Y0EXTBL42-[JQ0N~G,[	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/,E/}Y_Z,QW`~10M3M	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/T5/LTO[+	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/2	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/2M/3{2PKBGCNL15UJ,HZ	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/4A/P0,3Q6QC2K4[~+TNVG	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/38/F	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/14/8A{XA_M	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/3G/F91L22J5}F2`0`	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/1J/-51	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/2V/_	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/1V/C3JZ262FN`19KNZ~Y9	4Dell Latitude CPi.E01	

---

5. Detailed Analysis

- **Keyword Search**: Run searches with custom or pre-configured keywords.
- **File Analysis**: Browse files under File Types or File System, and export files if needed.
- **Timeline Analysis**: Visualize system events and user activities using timestamps.

- **Hash Analysis**: Compare file hashes against known databases to detect suspicious or trusted files.



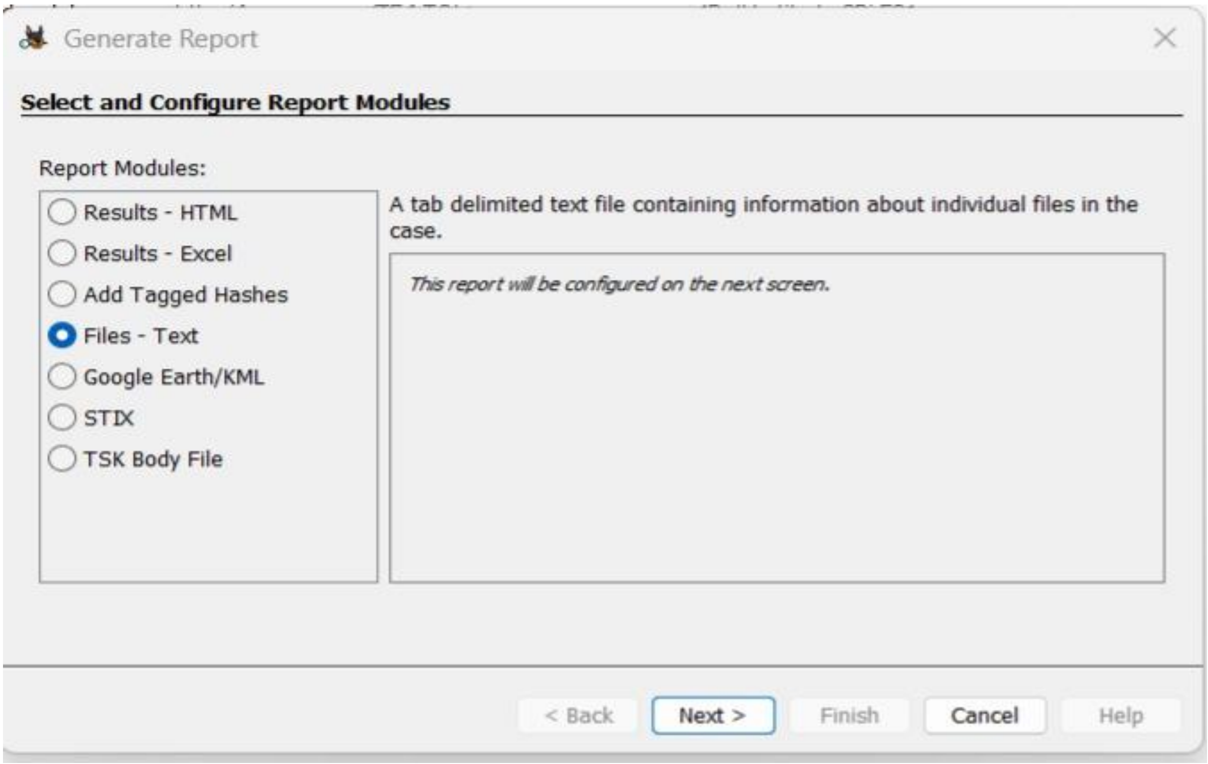
Source File	Username	Data Source	Tags
index.dat	Cookie:mr. evil	4Dell Latitude CPi.E01	
index.dat	Mr. Evil	4Dell Latitude CPi.E01	
index.dat	Mr. Evil	4Dell Latitude CPi.E01	
index.dat	Mr. Evil	4Dell Latitude CPi.E01	
index.dat	Mr. Evil	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/1~/F]	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/1J/`5Y0EXTBL42-[JQ0N~G,[	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/,E/}Y_Z,QW`~10M3M	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/T5/LTO[+	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/2	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/2M/3{2PKBGCNL15UJ,HZ	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/4A/P0,3Q6QC2K4[~+TNVG	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/38/F	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/14/8A{XA_M	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/3G/F91L22J5)F2`0`	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/1J/-51	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/2V/_	4Dell Latitude CPi.E01	
index.dat	http://hp.msn.com/1V/C3JZ262FN`19KNZ~Y9	4Dell Latitude CPi.E01	

Analyzing files from 4Dell Latitude CPi.E01 30% (1 more...) 3

---

6. Reporting

- After completing the analysis, generate a report from the toolbar.
- Reports can be exported in multiple formats (HTML, Excel, PDF, etc.).


Generate Report

Select and Configure Report Modules

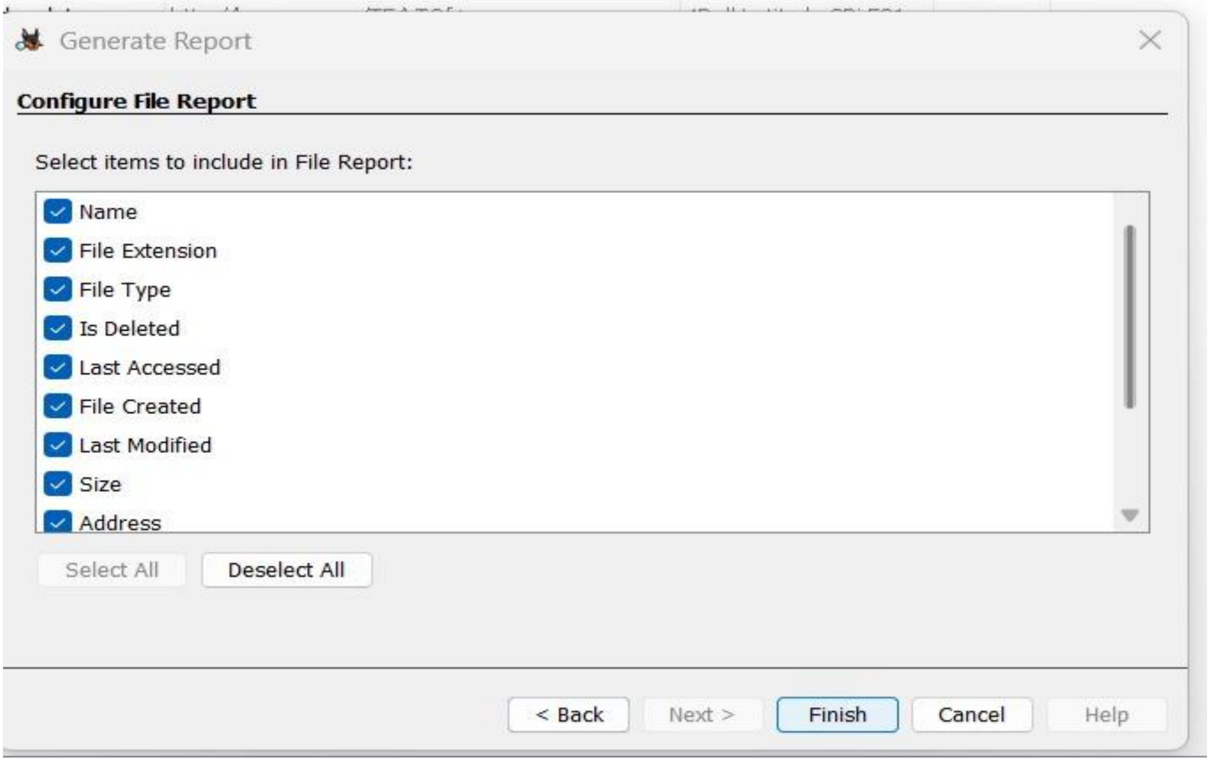
Report Modules:

○ Results - HTML
○ Results - Excel
○ Add Tagged Hashes
● Files - Text
○ Google Earth/KML
○ STIX
○ TSK Body File

A tab delimited text file containing information about individual files in the case.

This report will be configured on the next screen.

- The report will include details of findings, keyword matches, file artifacts, and timelines.



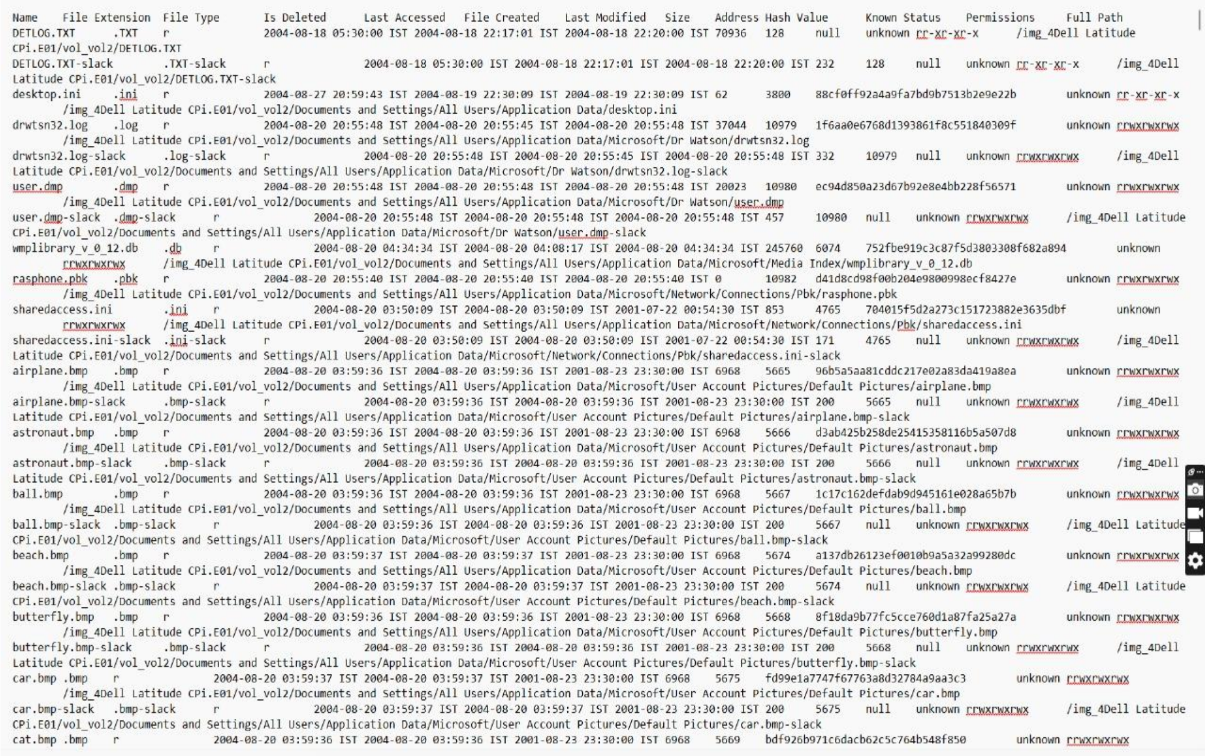
Generate Report

Configure File Report

Select items to include in File Report:

☑ Name
☑ File Extension
☑ File Type
☑ Is Deleted
☑ Last Accessed
☑ File Created
☑ Last Modified
☑ Size
☑ Address

Report



```
Name    File Extension  File Type       Is Deleted      Last Accessed   File Created    Last Modified   Size    Address Hash Value      Known Status    Permissions     Full Path
DETLOG.TXT      .TXT    r               2004-08-18 05:30:00 IST 2004-08-18 22:17:01 IST 2004-08-18 22:20:00 IST 70936   128     null    unknown rr-xr-xr-x      /img_4Dell Latitude
CPi.E01/vol_vol2/DETLOG.TXT
DETLOG.TXT-slack        .TXT-slack      r               2004-08-18 05:30:00 IST 2004-08-18 22:17:01 IST 2004-08-18 22:20:00 IST 232     128     null    unknown rr-xr-xr-x      /img_4Dell
Latitude CPi.E01/vol_vol2/DETLOG.TXT-slack
desktop.ini     .ini    r               2004-08-27 20:59:43 IST 2004-08-19 22:30:09 IST 2004-08-19 22:30:09 IST 62      3800    88cf0ff92a4a9fa7bd9b7513b2e9e22b        unknown rr-xr-xr-x
        /img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/desktop.ini
drwtsn32.log    .log    r               2004-08-20 20:55:48 IST 2004-08-20 20:55:45 IST 2004-08-20 20:55:48 IST 37044   10979   1f6aa0e6768d1393861f8c551840309f        unknown rrwxrwxrwx
        /img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/Microsoft/Dr Watson/drwtsn32.log
drwtsn32.log-slack      .log-slack      r               2004-08-20 20:55:48 IST 2004-08-20 20:55:45 IST 2004-08-20 20:55:48 IST 332     10979   null    unknown rrwxrwxrwx      /img_4Dell
Latitude CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/Microsoft/Dr Watson/drwtsn32.log-slack
user.dmp        .dmp    r               2004-08-20 20:55:48 IST 2004-08-20 20:55:48 IST 2004-08-20 20:55:48 IST 20023   10980   ec94d850a23d67b92e8e4bb228f56571        unknown rrwxrwxrwx
        /img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/Microsoft/Dr Watson/user.dmp
user.dmp-slack  .dmp-slack      r               2004-08-20 20:55:48 IST 2004-08-20 20:55:48 IST 2004-08-20 20:55:48 IST 457     10980   null    unknown rrwxrwxrwx      /img_4Dell Latitude
CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/Microsoft/Dr Watson/user.dmp-slack
wmplibrary_v_0_12.db    .db     r               2004-08-20 04:34:34 IST 2004-08-20 04:08:17 IST 2004-08-20 04:34:34 IST 245760  6074    752fbe919c3c87f5d3803308f682a894        unknown
        rrwxrwxrwx      /img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/Microsoft/Media Index/wmplibrary_v_0_12.db
rasphone.pbk    .pbk    r               2004-08-20 20:55:40 IST 2004-08-20 20:55:40 IST 2004-08-20 20:55:40 IST 0       10982   d41d8cd98f00b204e9800998ecf8427e        unknown rrwxrwxrwx
        /img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/Microsoft/Network/Connections/Pbk/rasphone.pbk
sharedaccess.ini        .ini    r               2004-08-20 03:50:09 IST 2004-08-20 03:50:09 IST 2001-07-22 00:54:30 IST 853     4765    704015f5d2a273c151723882e3635dbf        unknown
        rrwxrwxrwx      /img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/Microsoft/Network/Connections/Pbk/sharedaccess.ini
sharedaccess.ini-slack  .ini-slack      r               2004-08-20 03:50:09 IST 2004-08-20 03:50:09 IST 2001-07-22 00:54:30 IST 171     4765    null    unknown rrwxrwxrwx      /img_4Dell
Latitude CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/Microsoft/Network/Connections/Pbk/sharedaccess.ini-slack
airplane.bmp    .bmp    r               2004-08-20 03:59:36 IST 2004-08-20 03:59:36 IST 2001-08-23 23:30:00 IST 6968    5665    96b5a5aa81cddc217e02a83da419a8ea        unknown rrwxrwxrwx
        /img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/airplane.bmp
airplane.bmp-slack      .bmp-slack      r               2004-08-20 03:59:36 IST 2004-08-20 03:59:36 IST 2001-08-23 23:30:00 IST 200     5665    null    unknown rrwxrwxrwx      /img_4Dell
Latitude CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/airplane.bmp-slack
astronaut.bmp   .bmp    r               2004-08-20 03:59:36 IST 2004-08-20 03:59:36 IST 2001-08-23 23:30:00 IST 6968    5666    d3ab425b258de25415358116b5a507d8        unknown rrwxrwxrwx
        /img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/astronaut.bmp
astronaut.bmp-slack     .bmp-slack      r               2004-08-20 03:59:36 IST 2004-08-20 03:59:36 IST 2001-08-23 23:30:00 IST 200     5666    null    unknown rrwxrwxrwx      /img_4Dell
Latitude CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/astronaut.bmp-slack
ball.bmp        .bmp    r               2004-08-20 03:59:36 IST 2004-08-20 03:59:36 IST 2001-08-23 23:30:00 IST 6968    5667    1c17c162defdab9d945161e028a65b7b        unknown rrwxrwxrwx
        /img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/ball.bmp
ball.bmp-slack  .bmp-slack      r               2004-08-20 03:59:36 IST 2004-08-20 03:59:36 IST 2001-08-23 23:30:00 IST 200     5667    null    unknown rrwxrwxrwx      /img_4Dell Latitude
CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/ball.bmp-slack
beach.bmp       .bmp    r               2004-08-20 03:59:37 IST 2004-08-20 03:59:37 IST 2001-08-23 23:30:00 IST 6968    5674    a137db26123ef0010b9a5a32a99280dc        unknown rrwxrwxrwx
        /img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/beach.bmp
beach.bmp-slack .bmp-slack      r               2004-08-20 03:59:37 IST 2004-08-20 03:59:37 IST 2001-08-23 23:30:00 IST 200     5674    null    unknown rrwxrwxrwx      /img_4Dell Latitude
CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/beach.bmp-slack
butterfly.bmp   .bmp    r               2004-08-20 03:59:36 IST 2004-08-20 03:59:36 IST 2001-08-23 23:30:00 IST 6968    5668    8f18da9b77fc5cce760d1a87fa25a27a        unknown rrwxrwxrwx
        /img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/butterfly.bmp
butterfly.bmp-slack     .bmp-slack      r               2004-08-20 03:59:36 IST 2004-08-20 03:59:36 IST 2001-08-23 23:30:00 IST 200     5668    null    unknown rrwxrwxrwx      /img_4Dell
Latitude CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/butterfly.bmp-slack
car.bmp .bmp    r               2004-08-20 03:59:37 IST 2004-08-20 03:59:37 IST 2001-08-23 23:30:00 IST 6968    5675    fd99e1a7747f67763a8d32784a9aa3c3        unknown rrwxrwxrwx
        /img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/car.bmp
car.bmp-slack   .bmp-slack      r               2004-08-20 03:59:37 IST 2004-08-20 03:59:37 IST 2001-08-23 23:30:00 IST 200     5675    null    unknown rrwxrwxrwx      /img_4Dell Latitude
CPi.E01/vol_vol2/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/car.bmp-slack
cat.bmp .bmp    r               2004-08-20 03:59:36 IST 2004-08-20 03:59:36 IST 2001-08-23 23:30:00 IST 6968    5669    bdf926b971c6dacb62c5c764b548f850        unknown rrwxrwxrwx
```

7. Case Closure

- Close the case once the investigation is finished.
- Archive all data and reports securely, following your organization’s policies.