Digital Forensic Analysis with Autopsy: Recovering and Interpreting System Artifacts

Kayvon Karimi

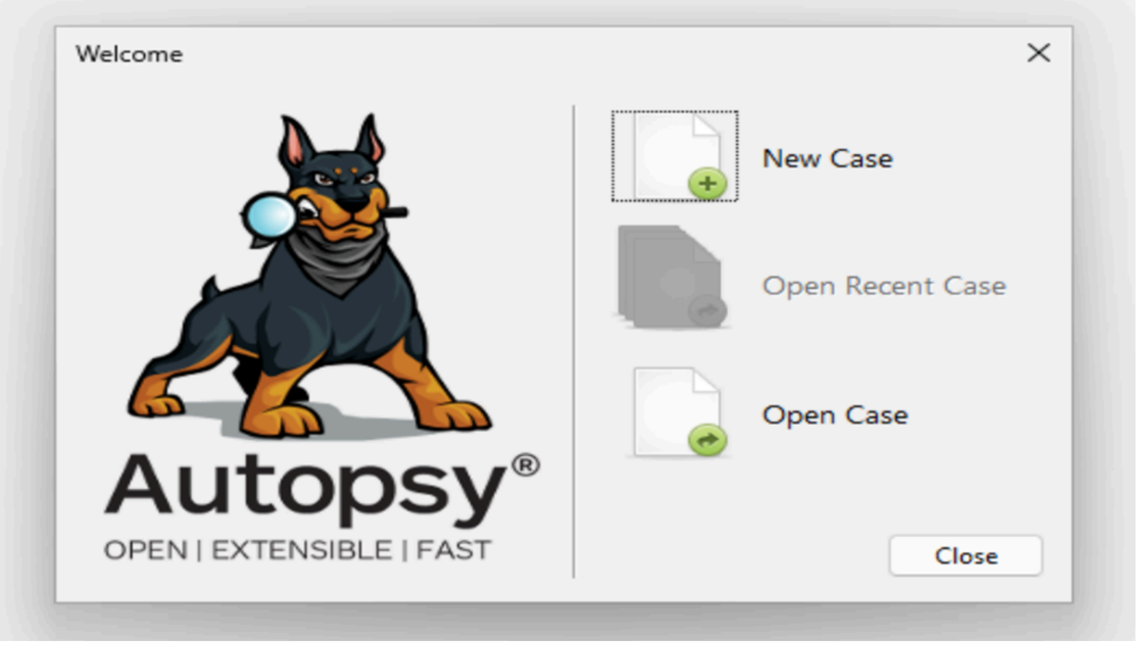
November 25, 2024

Executive Summary

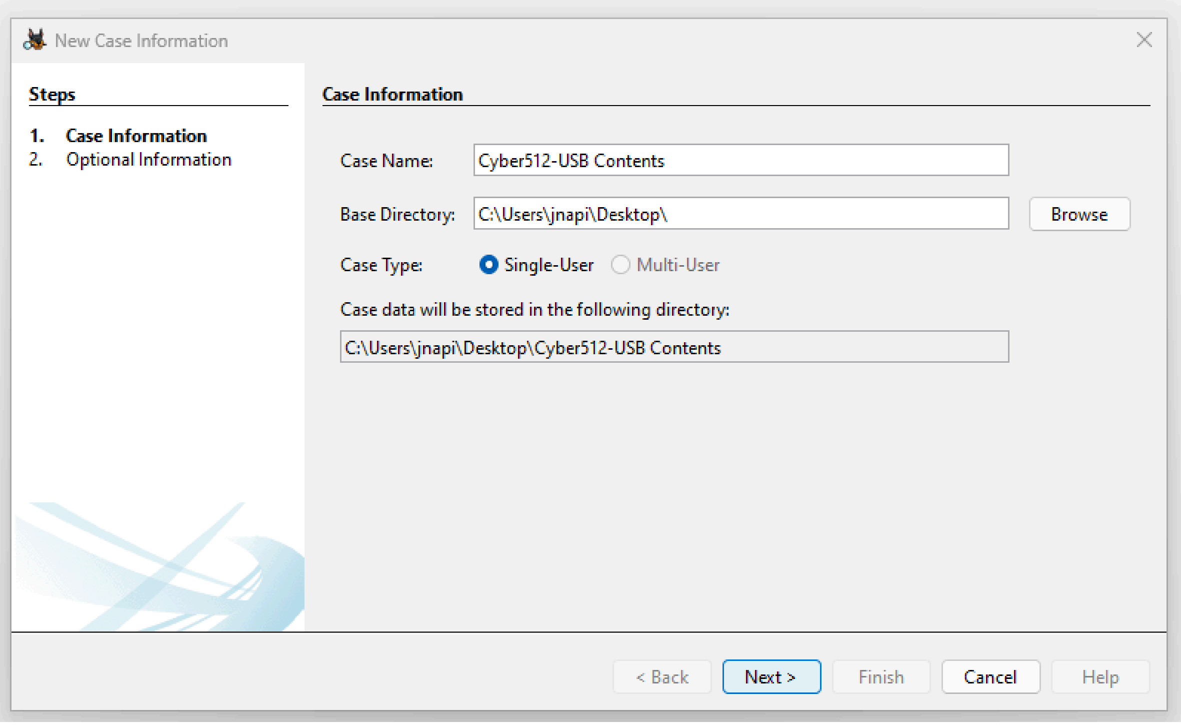
Autopsy is an open-source digital forensics platform widely used by investigators to analyze digital evidence. It provides powerful tools for examining data from devices, recovering deleted files, and identifying potential evidence in a user-friendly interface. This report outlines the use of Autopsy to perform forensic analysis on multiple data sources, including a USB drive, the HackingCase files, and the M57-Jean scenario. The purpose of this lab exercise is to practice using Autopsy for ingesting and analyzing data, identifying relevant findings, and gaining hands-on experience in digital forensics

Part 1: USB Drive Analysis using Autopsy

1. Download and install Autopsy from the official website: (https://www.autopsy.com/download)
2. Locate an old USB drive and ensure it has sufficient storage capacity (<4GB)
3. After installing Autopsy, launch the program and you will be prompted to start a new case or open an existing case.
    a. Click *New Case*.



4. Enter a Case Name and identify the directory to store case data
    a. C:\Users\jnapi\Desktop\



New Case Information

Steps

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

Case Information

Case Name: Cyber512-USB Contents

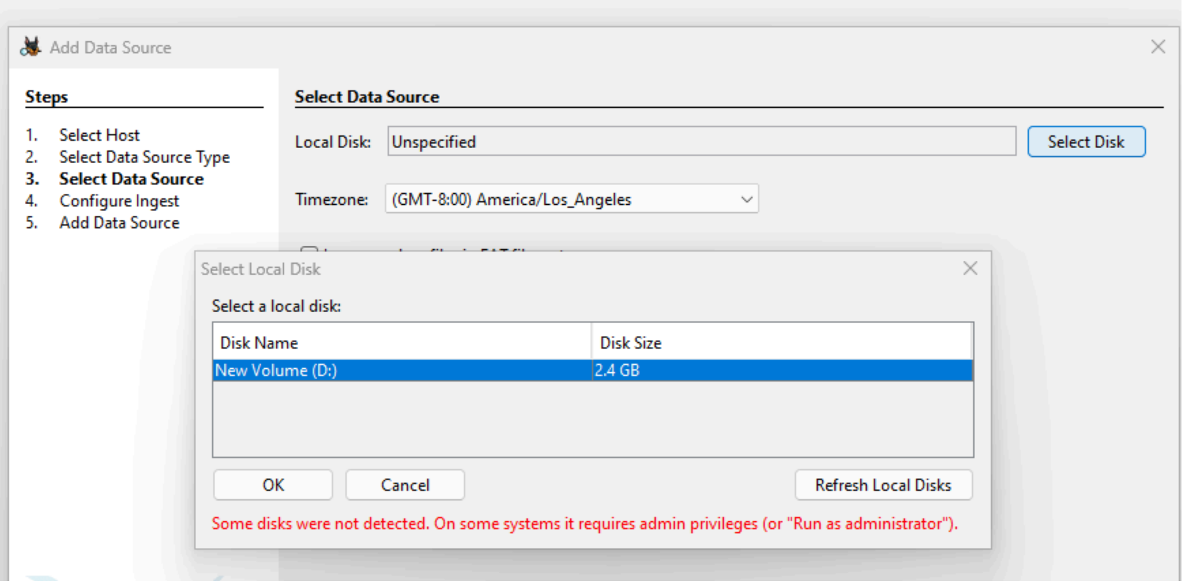
Base Directory: C:\Users\jnapi\Desktop\

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

C:\Users\jnapi\Desktop\Cyber512-USB Contents

5. Selecting Local Disk, and Volume D for the USB data source.



Add Data Source

Steps

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

Select Data Source

Local Disk: Unspecified

Timezone: (GMT-8:00) America/Los_Angeles

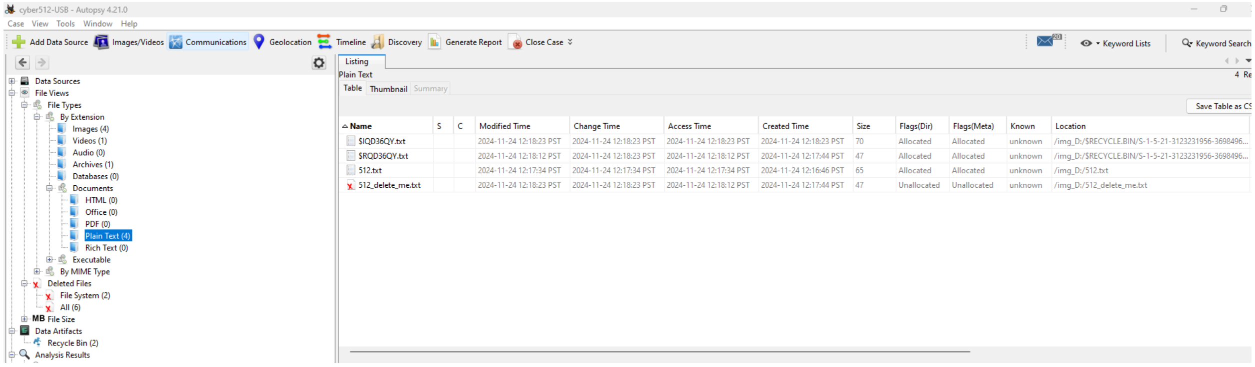
Select Local Disk

Select a local disk:

Disk Name	Disk Size
New Volume (D:)	2.4 GB

Some disks were not detected. On some systems it requires admin privileges (or "Run as administrator").

6. After initial ingestion is complete, we review the extracted files. Since this USB had been used in the past, I added 4 new files to give it additional content. Two images and two text files were added, and then one of each was deleted.

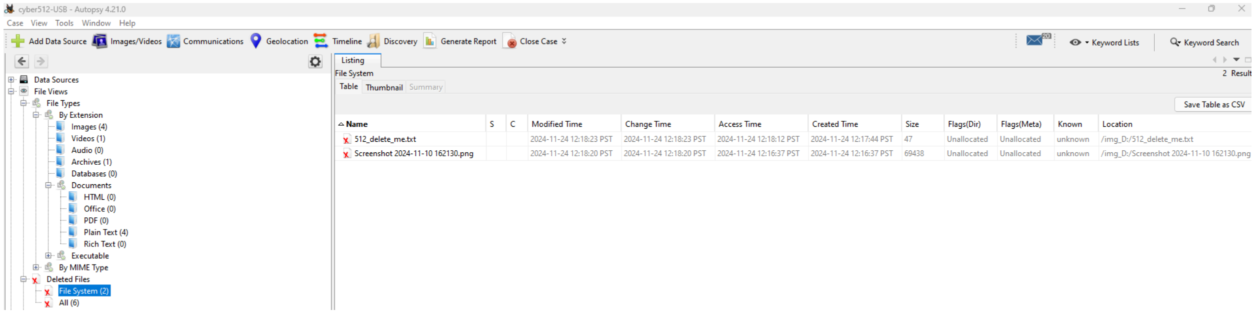


Plain Text

4 Re

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
$IQD36QY.txt			2024-11-24 12:18:23 PST	2024-11-24 12:18:23 PST	2024-11-24 12:18:23 PST	2024-11-24 12:18:23 PST	70	Allocated	Allocated	unknown	/img_D:/$RECYCLE.BIN/S-1-5-21-3123231956-3698496...
$RQD36QY.txt			2024-11-24 12:18:12 PST	2024-11-24 12:18:23 PST	2024-11-24 12:18:12 PST	2024-11-24 12:17:44 PST	47	Allocated	Allocated	unknown	/img_D:/$RECYCLE.BIN/S-1-5-21-3123231956-3698496...
512.txt			2024-11-24 12:17:34 PST	2024-11-24 12:17:34 PST	2024-11-24 12:17:34 PST	2024-11-24 12:16:46 PST	65	Allocated	Allocated	unknown	/img_D:/512.txt
512_delete_me.txt			2024-11-24 12:18:23 PST	2024-11-24 12:18:23 PST	2024-11-24 12:18:12 PST	2024-11-24 12:17:44 PST	47	Unallocated	Unallocated	unknown	/img_D:/512_delete_me.txt

7. Reviewing the deleted files within the "File System" shows the two files which were recently added and then deleted.



File System

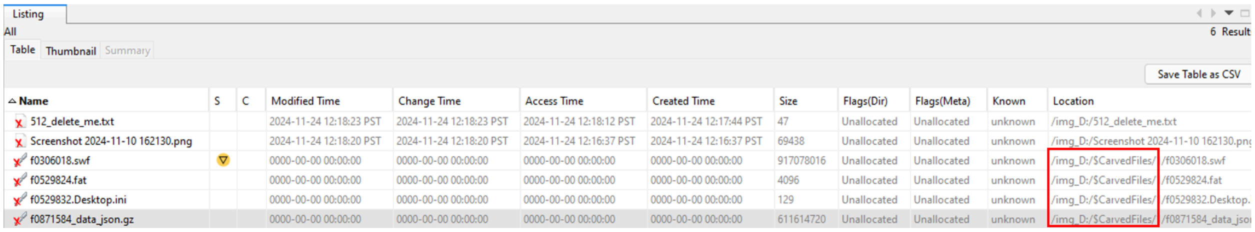
2 Result

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
512_delete_me.txt			2024-11-24 12:18:23 PST	2024-11-24 12:18:23 PST	2024-11-24 12:18:12 PST	2024-11-24 12:17:44 PST	47	Unallocated	Unallocated	unknown	/img_D:/512_delete_me.txt
Screenshot 2024-11-10 162130.png			2024-11-24 12:18:20 PST	2024-11-24 12:18:20 PST	2024-11-24 12:16:37 PST	2024-11-24 12:16:37 PST	69438	Unallocated	Unallocated	unknown	/img_D:/Screenshot 2024-11-10 162130.png

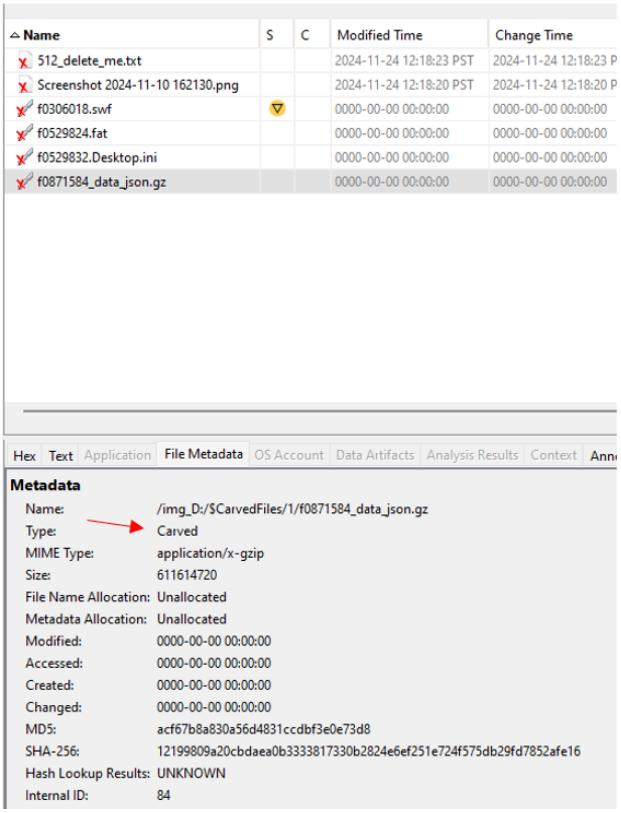
Part 1.2: What are the "CarvedFiles", if any?

- The files identified within the dataset as "Carved Files" include the following:

f0306018.swf	Small Web File, a now defunct Adobe Flash Movie file format.
f0529824.fat	"File Allocation Table" Disk Image File, or Zinf Project "FreeAmp Theme" audio file.
f0529832.Desktop.ini	Initialization text file - allows users to customize how a file system is displayed.
f0871584_data_json.gz	A compressed archive file created using the Gnu Zip utility.



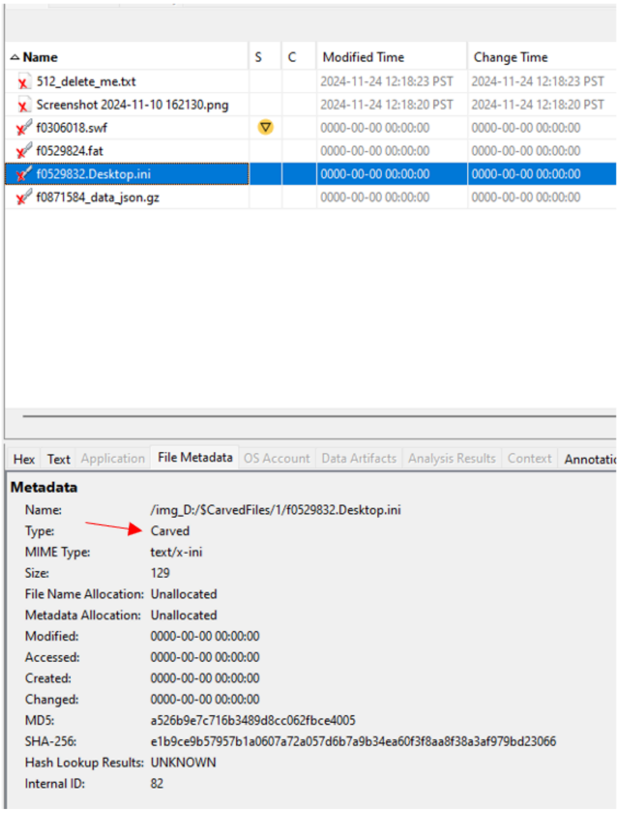
Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
512_delete_me.txt			2024-11-24 12:18:23 PST	2024-11-24 12:18:23 PST	2024-11-24 12:18:12 PST	2024-11-24 12:17:44 PST	47	Unallocated	Unallocated	unknown	/img_D:/512_delete_me.txt
Screenshot 2024-11-10 162130.png			2024-11-24 12:18:20 PST	2024-11-24 12:18:20 PST	2024-11-24 12:16:37 PST	2024-11-24 12:16:37 PST	69438	Unallocated	Unallocated	unknown	/img_D:/Screenshot 2024-11-10 162130.png
f0306018.swf	▽		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	917078016	Unallocated	Unallocated	unknown	/img_D:/$CarvedFiles/ /f0306018.swf
f0529824.fat			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Unallocated	Unallocated	unknown	/img_D:/$CarvedFiles/ /f0529824.fat
f0529832.Desktop.ini			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	129	Unallocated	Unallocated	unknown	/img_D:/$CarvedFiles/ /f0529832.Desktop.
f0871584_data_json.gz			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	611614720	Unallocated	Unallocated	unknown	/img_D:/$CarvedFiles/ /f0871584_data_jso



Name	S	C	Modified Time	Change Time
512_delete_me.txt			2024-11-24 12:18:23 PST	2024-11-24 12:18:23 P
Screenshot 2024-11-10 162130.png			2024-11-24 12:18:20 PST	2024-11-24 12:18:20 P
f0306018.swf	▽		0000-00-00 00:00:00	0000-00-00 00:00:00
f0529824.fat			0000-00-00 00:00:00	0000-00-00 00:00:00
f0529832.Desktop.ini			0000-00-00 00:00:00	0000-00-00 00:00:00
f0871584_data_json.gz			0000-00-00 00:00:00	0000-00-00 00:00:00

Metadata

Name:	/img_D:/$CarvedFiles/1/f0871584_data_json.gz
Type:	Carved
MIME Type:	application/x-gzip
Size:	611614720
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	0000-00-00 00:00:00
Accessed:	0000-00-00 00:00:00
Created:	0000-00-00 00:00:00
Changed:	0000-00-00 00:00:00
MD5:	acf67b8a830a56d4831ccdbf3e0e73d8
SHA-256:	12199809a20cbdaea0b3333817330b2824e6ef251e724f575db29fd7852afe16
Hash Lookup Results:	UNKNOWN
Internal ID:	84



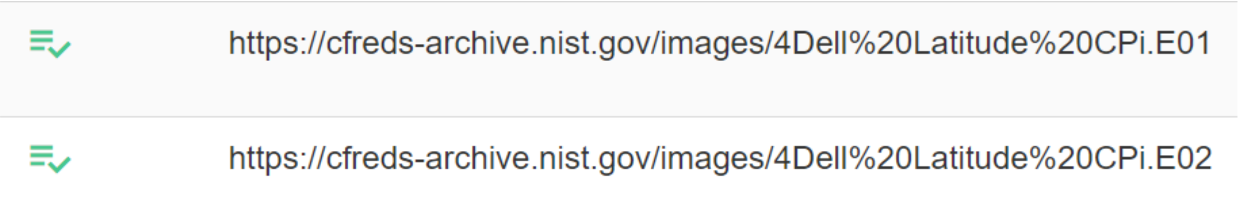
Name	S	C	Modified Time	Change Time
512_delete_me.txt			2024-11-24 12:18:23 PST	2024-11-24 12:18:23 PST
Screenshot 2024-11-10 162130.png			2024-11-24 12:18:20 PST	2024-11-24 12:18:20 PST
f0306018.swf	▽		0000-00-00 00:00:00	0000-00-00 00:00:00
f0529824.fat			0000-00-00 00:00:00	0000-00-00 00:00:00
f0529832.Desktop.ini			0000-00-00 00:00:00	0000-00-00 00:00:00
f0871584_data_json.gz			0000-00-00 00:00:00	0000-00-00 00:00:00

Metadata

Name:	/img_D:/$CarvedFiles/1/f0529832.Desktop.ini
Type:	Carved
MIME Type:	text/x-ini
Size:	129
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	0000-00-00 00:00:00
Accessed:	0000-00-00 00:00:00
Created:	0000-00-00 00:00:00
Changed:	0000-00-00 00:00:00
MD5:	a526b9e7c716b3489d8cc062fbce4005
SHA-256:	e1b9ce9b57957b1a0607a72a057d6b7a9b34ea60f3f8aa8f38a3af979bd23066
Hash Lookup Results:	UNKNOWN
Internal ID:	82

Part 2: Computer Forensics - Hacking Case using Autopsy

1. Obtain the disk image files, .E01 and .E02, for the Hacking Case from the NIST website, https://cfreds.nist.gov/all/NIST/HackingCase.
    a. Right-click the files and *Save link as…*



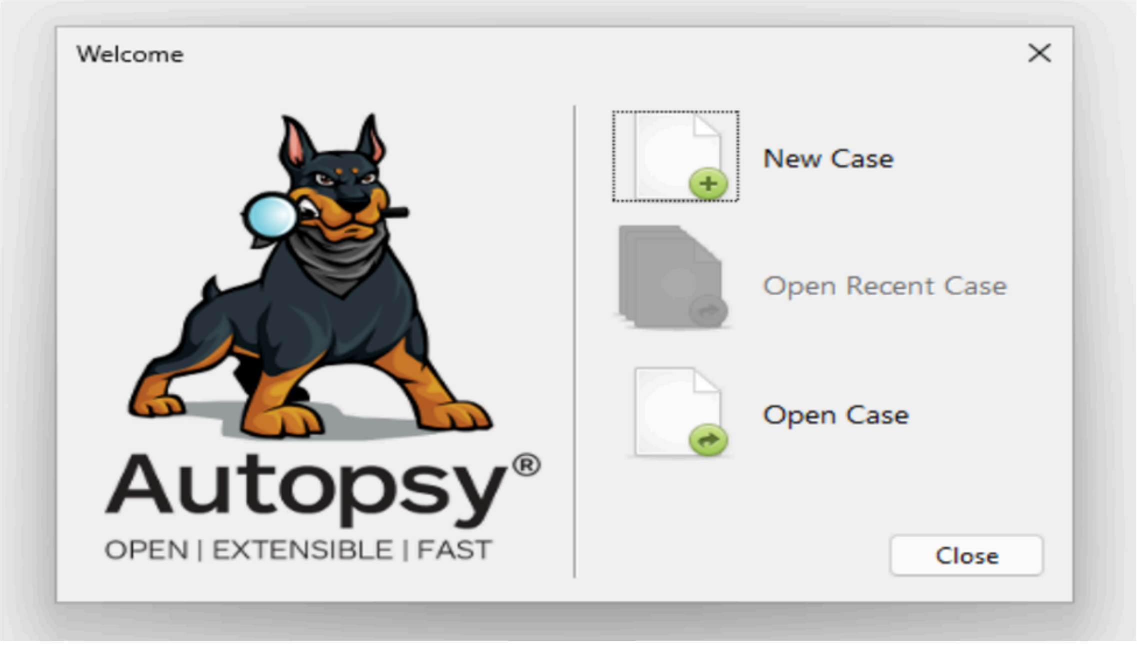
https://cfreds-archive.nist.gov/images/4Dell%20Latitude%20CPi.E01

https://cfreds-archive.nist.gov/images/4Dell%20Latitude%20CPi.E02

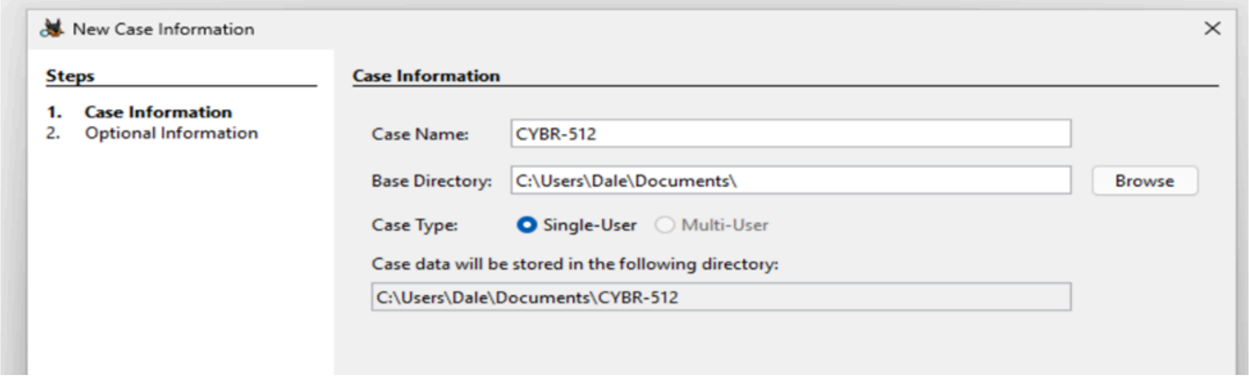
2. Both files need to be stored in the same directory with matching file names, only the extension, .E01 and .E02 being different. This will allow Autopsy to automatically detect

and ingest them both. This would work the same if there were an additional image segment titled .E03.

3. After installing Autopsy, launch the program and you will be prompted to start a new case or open an existing case.
    a. Click *New Case*.



4. Enter a Case Name and identify the directory to store case data.



Case Information

Case Name: CYBR-512

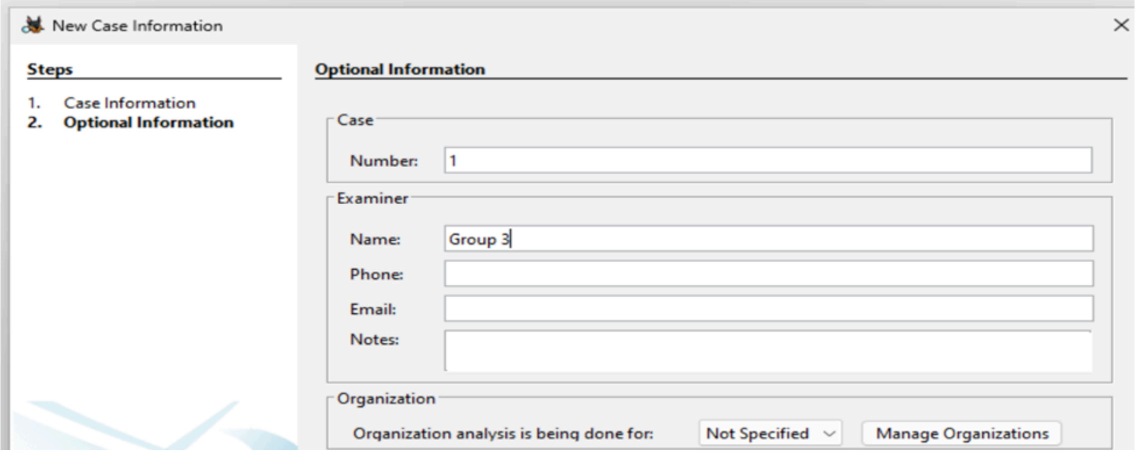
Base Directory: C:\Users\Dale\Documents\

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

C:\Users\Dale\Documents\CYBR-512

5. Click *Next* and enter any optional information that is relevant.


New Case Information

Steps

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

Optional Information

Case

Number: 1

Examiner

Name: Group 3

Phone:

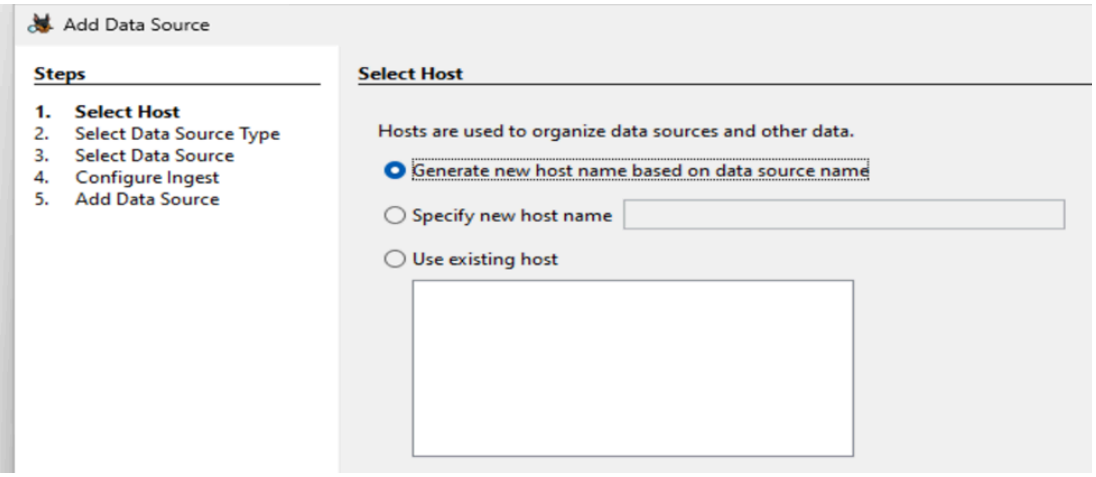
Email:

Notes:

Organization

Organization analysis is being done for: Not Specified

6. Next, you'll be prompted to add a data source, this will be the files downloaded in step 1.
    a. The data source type will be a disk image.


Add Data Source

Steps

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

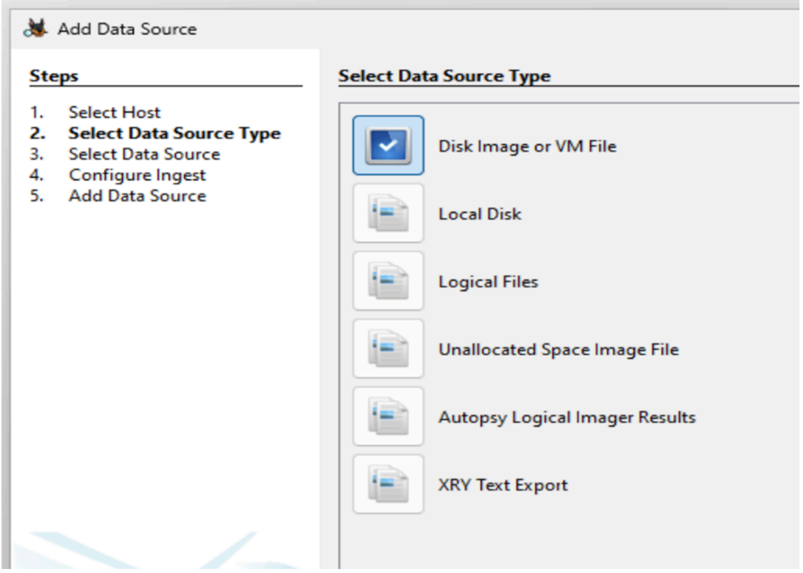
Select Host

Hosts are used to organize data sources and other data.

● Generate new host name based on data source name

○ Specify new host name

○ Use existing host


Add Data Source

Steps

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

Select Data Source Type

☑ Disk Image or VM File

Local Disk

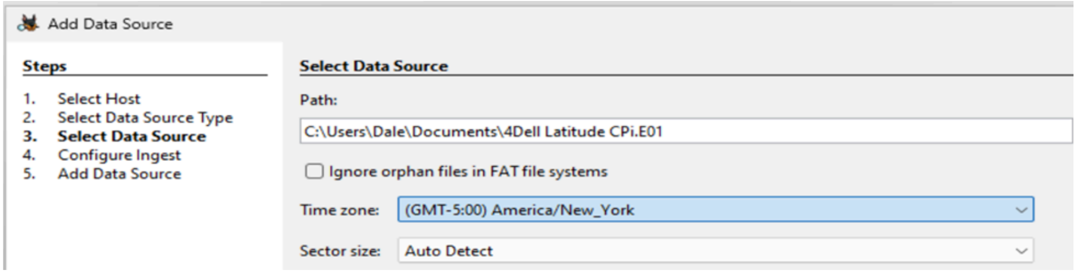
Logical Files

Unallocated Space Image File

Autopsy Logical Imager Results

XRY Text Export

7. Navigate to the directory where the disk image files are located and select the one ending in .E01. Autopsy will automatically ingest .E02.



Add Data Source

Steps

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

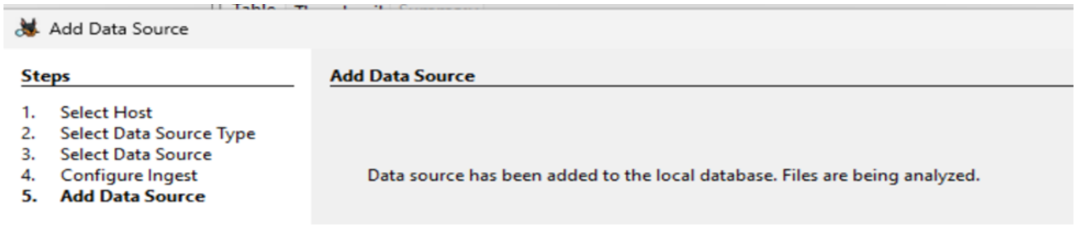
Select Data Source

Path: C:\Users\Dale\Documents\4Dell Latitude CPi.E01

☐ Ignore orphan files in FAT file systems

Time zone: (GMT-5:00) America/New_York

Sector size: Auto Detect



Add Data Source

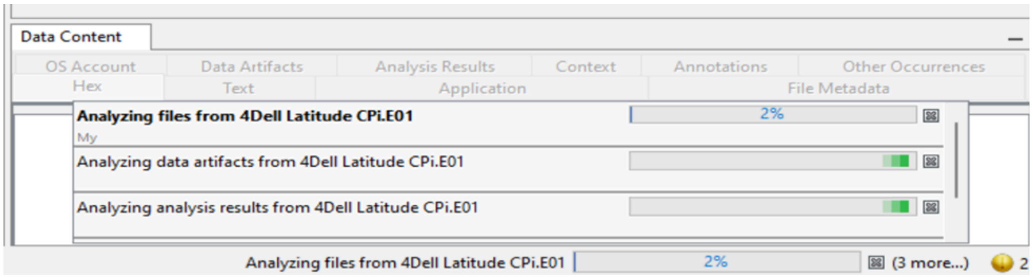
Steps

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

Add Data Source

Data source has been added to the local database. Files are being analyzed.

8. Autopsy will begin ingesting the files. Once complete, you can open the Data Sources Summary to verify the ingest was successful.

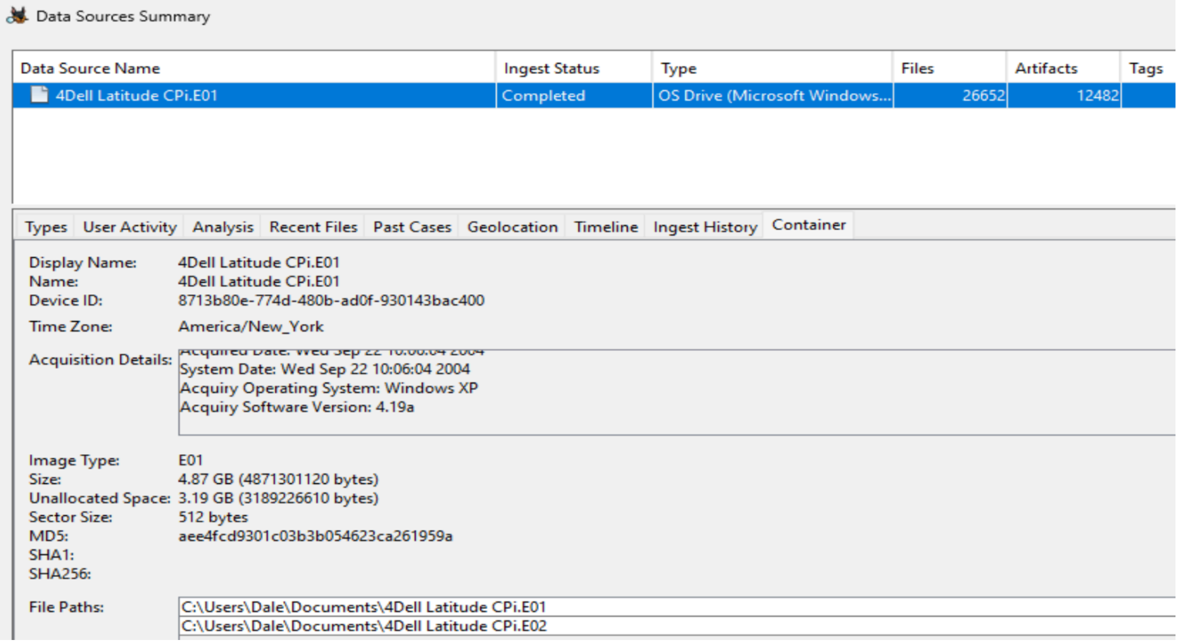


Analyzing files from 4Dell Latitude CPi.E01 2%

Analyzing data artifacts from 4Dell Latitude CPi.E01

Analyzing analysis results from 4Dell Latitude CPi.E01

Analyzing files from 4Dell Latitude CPi.E01 2% (3 more...) 2



Data Source Name	Ingest Status	Type	Files	Artifacts	Tags
4Dell Latitude CPi.E01	Completed	OS Drive (Microsoft Windows...	26652	12482	

Display Name: 4Dell Latitude CPi.E01
Name: 4Dell Latitude CPi.E01
Device ID: 8713b80e-774d-480b-ad0f-930143bac400

Time Zone: America/New_York

Acquisition Details: Acquired Date: Wed Sep 22 10:06:04 2004
System Date: Wed Sep 22 10:06:04 2004
Acquiry Operating System: Windows XP
Acquiry Software Version: 4.19a

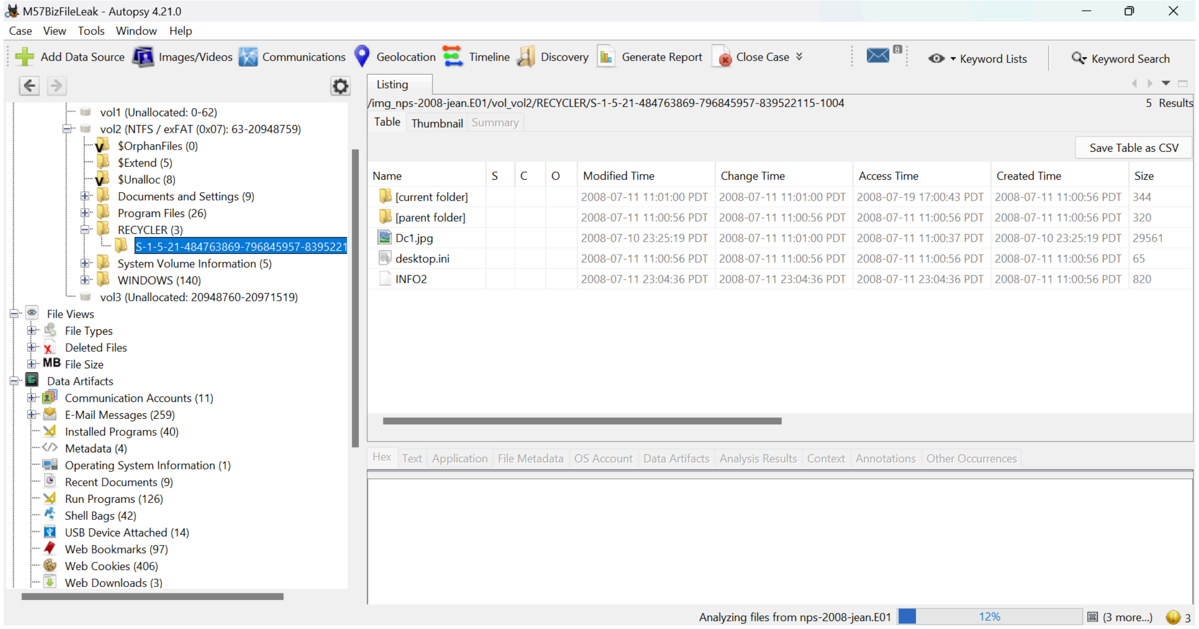
Image Type: E01
Size: 4.87 GB (4871301120 bytes)
Unallocated Space: 3.19 GB (3189226610 bytes)
Sector Size: 512 bytes
MD5: aee4fcd9301c03b3b054623ca261959a
SHA1:
SHA256:

File Paths: C:\Users\Dale\Documents\4Dell Latitude CPi.E01
C:\Users\Dale\Documents\4Dell Latitude CPi.E02

Part 3: M57-Jean Scenario Analysis using Autopsy

What are the contents of the "Recycler" in the target image?

1. The Recycler folder in the m57-jean image contains three items:



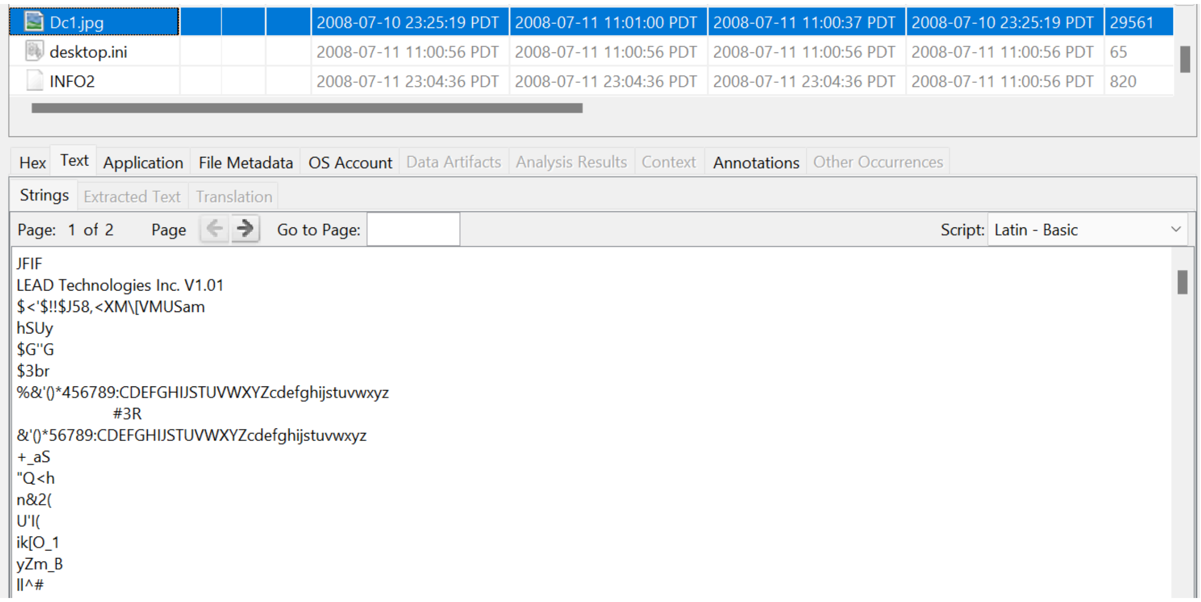
vol1 (Unallocated: 0-62)
vol2 (NTFS / exFAT (0x07): 63-20948759)
$OrphanFiles (0)
$Extend (5)
$Unalloc (8)
Documents and Settings (9)
Program Files (26)
RECYCLER (3)
S-1-5-21-484763869-796845957-8395221
System Volume Information (5)
WINDOWS (140)
vol3 (Unallocated: 20948760-20971519)
File Views
File Types
Deleted Files
MB File Size
Data Artifacts
Communication Accounts (11)
E-Mail Messages (259)
Installed Programs (40)
Metadata (4)
Operating System Information (1)
Recent Documents (9)
Run Programs (126)
Shell Bags (42)
USB Device Attached (14)
Web Bookmarks (97)
Web Cookies (406)
Web Downloads (3)

/img_nps-2008-jean.E01/vol_vol2/RECYCLER/S-1-5-21-484763869-796845957-839522115-1004 5 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2008-07-11 11:01:00 PDT	2008-07-11 11:01:00 PDT	2008-07-19 17:00:43 PDT	2008-07-11 11:00:56 PDT	344
[parent folder]				2008-07-11 11:00:56 PDT	2008-07-11 11:00:56 PDT	2008-07-11 11:00:56 PDT	2008-07-11 11:00:56 PDT	320
Dc1.jpg				2008-07-10 23:25:19 PDT	2008-07-11 11:01:00 PDT	2008-07-11 11:00:37 PDT	2008-07-10 23:25:19 PDT	29561
desktop.ini				2008-07-11 11:00:56 PDT	2008-07-11 11:00:56 PDT	2008-07-11 11:00:56 PDT	2008-07-11 11:00:56 PDT	65
INFO2				2008-07-11 23:04:36 PDT	2008-07-11 23:04:36 PDT	2008-07-11 23:04:36 PDT	2008-07-11 11:00:56 PDT	820

Analyzing files from nps-2008-jean.E01 12% (3 more...) 3

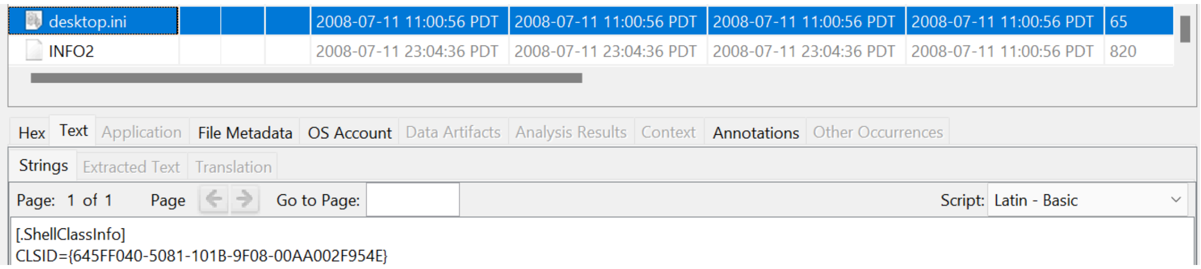
   a. **Dc1.jpg**: An image file, size 29,561 bytes, last modified on 2008-07-10.



Dc1.jpg	2008-07-10 23:25:19 PDT	2008-07-11 11:01:00 PDT	2008-07-11 11:00:37 PDT	2008-07-10 23:25:19 PDT	29561
desktop.ini	2008-07-11 11:00:56 PDT	2008-07-11 11:00:56 PDT	2008-07-11 11:00:56 PDT	2008-07-11 11:00:56 PDT	65
INFO2	2008-07-11 23:04:36 PDT	2008-07-11 23:04:36 PDT	2008-07-11 23:04:36 PDT	2008-07-11 11:00:56 PDT	820

```
JFIF
LEAD Technologies Inc. V1.01
$<'$!!$J58,<XM\[VMUSam
hSUy
$G''G
$3br
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
                #3R
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
+_aS
"Q<h
n&2(
U'I(
ik[O_1
yZm_B
||^#
```

b. **desktop.ini**: A configuration file, size 65 bytes, last modified on 2008-07-11.

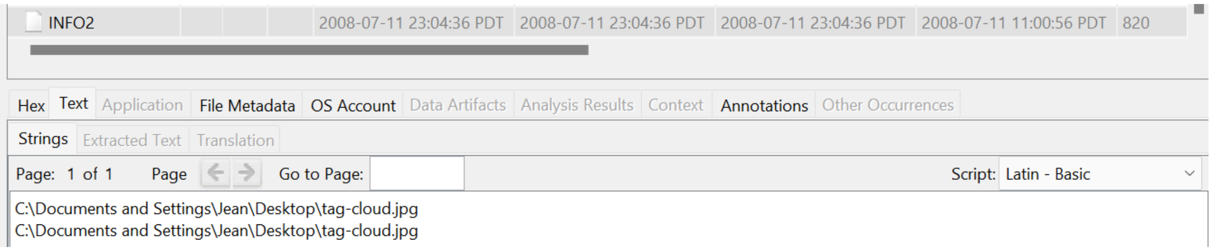


desktop.ini	2008-07-11 11:00:56 PDT	2008-07-11 11:00:56 PDT	2008-07-11 11:00:56 PDT	2008-07-11 11:00:56 PDT	65
INFO2	2008-07-11 23:04:36 PDT	2008-07-11 23:04:36 PDT	2008-07-11 23:04:36 PDT	2008-07-11 11:00:56 PDT	820

```
[.ShellClassInfo]
CLSID={645FF040-5081-101B-9F08-00AA002F954E}
```

c. **INFO2**: A metadata file, 820 bytes, last modified on 2008-07-11.

   i. This file maintains records of deleted files, including original file paths and deletion timestamps.



INFO2	2008-07-11 23:04:36 PDT	2008-07-11 23:04:36 PDT	2008-07-11 23:04:36 PDT	2008-07-11 11:00:56 PDT	820

```
C:\Documents and Settings\Jean\Desktop\tag-cloud.jpg
C:\Documents and Settings\Jean\Desktop\tag-cloud.jpg
```

Conclusion

This report demonstrates the practical application of Autopsy for digital forensic analysis, highlighting its ability to recover and examine data from diverse sources, including USB drives, disk images, and scenario-based datasets. These exercises provided valuable insights into data ingestion, artifact recovery, and evidence interpretation using a powerful forensic platform.