Experiment 10

Aim: Generate a Timeline Report Using Autopsy

Theory:

Autopsy allows you to generate a report—in HTML, Excel, text, and other formats—that contains time information of every file in the supplied forensic image. This feature opens possibilities to use such information in other programs outside Autopsy. To generate a timeline report using Autopsy, follow these steps:

1. Go to Tools menu ➤ Generate Report. The Generate Report wizard appears; the first window allows you to select the report format. Select report format for your generated timeline in Autopsy

2. In our case, we select "Excel Report," so we can play with the data using the MS Excel spreadsheet program or any other alternative program that can read Excel files like Apache OpenOffice (www.openoffice.org). Click "Next" to continue.

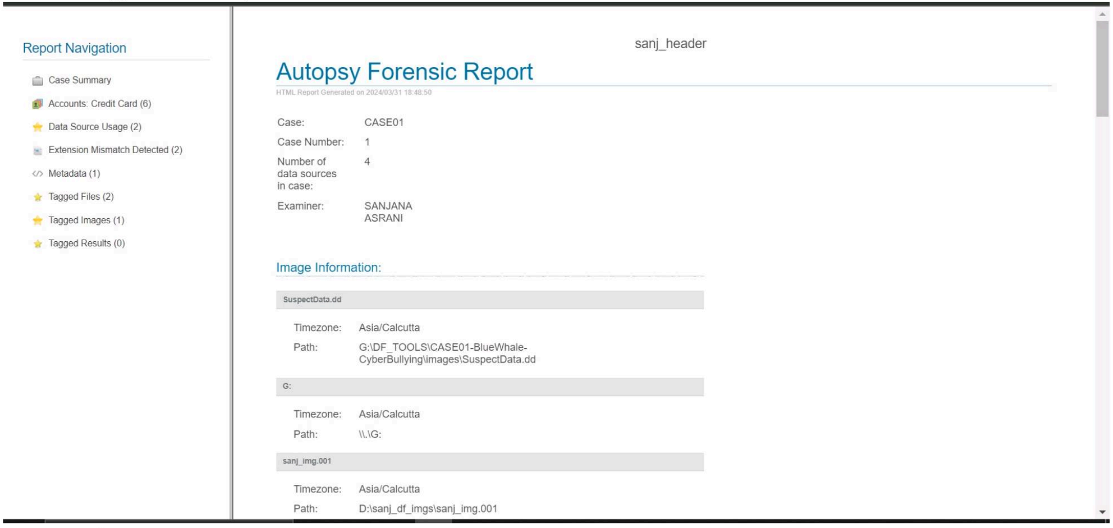
3. The next window asks you to configure the returned results. You have two options: All Results and Tagged Results. In our case, we will select all results and click "Finish"; then, Autopsy will begin the report generation process.

4. After it finishes generating the report, Autopsy will show you the link where your generated report is saved; click over this link to open the file using your default program.

5. Finally, click "Close" to close the Report Generation Progress window.

Please note that as a part of Autopsy's initial analysis, it will list the last seven days of activity—of web browsers (including web searches), installed programs, operating system, and recent changes to registry hives—of the supplied forensic image files in the Data Explorer panel under the "Extracted Content" section Remember that you need to activate the "Recent Activity" ingest module in order to retrieve this result.

Generating an html report:



sanj_header

Autopsy Forensic Report

HTML Report Generated on 2024/03/31 18:48:50

Case:	CASE01
Case Number:	1
Number of data sources in case:	4
Examiner:	SANJANA ASRANI

Image Information:

SuspectData.dd

Timezone:	Asia/Calcutta
Path:	G:\DF_TOOLS\CASE01-BlueWhale-CyberBullying\images\SuspectData.dd

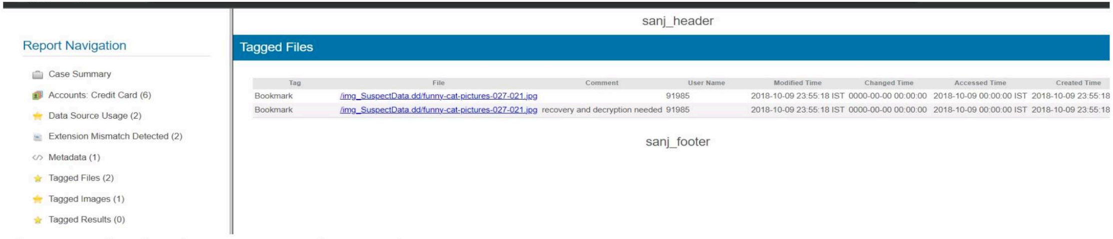
G:

Timezone:	Asia/Calcutta
Path:	\\.\G:

sanj_img.001

Timezone:	Asia/Calcutta
Path:	D:\sanj_df_imgs\sanj_img.001

Tagging files:



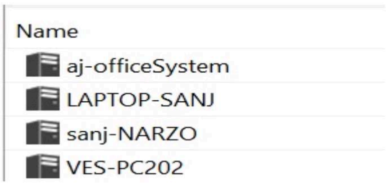
sanj_header

Tagged Files

Tag	File	Comment	User Name	Modified Time	Changed Time	Accessed Time	Created Time
Bookmark	/img_SuspectData.dd/funny-cat-pictures-027-021.jpg		91985	2018-10-09 23:55:18 IST	0000-00-00 00:00:00	2018-10-09 00:00:00 IST	2018-10-09 23:55:18
Bookmark	/img_SuspectData.dd/funny-cat-pictures-027-021.jpg	recovery and decryption needed	91985	2018-10-09 23:55:18 IST	0000-00-00 00:00:00	2018-10-09 00:00:00 IST	2018-10-09 23:55:18

sanj_footer

This case had 4 data sources from 4 hosts:



Name
aj-officeSystem
LAPTOP-SANJ
sanj-NARZO
VES-PC202

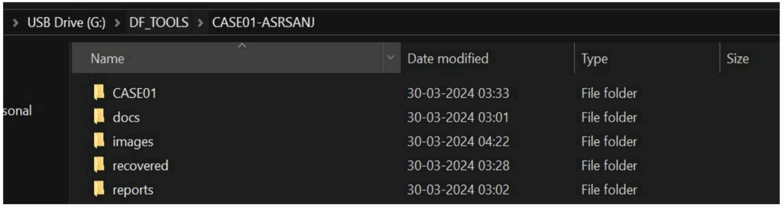
The aj-officeSystem has the .img files that were created from a drive using FTKimager

LAPTOP-SANJ has a .dd file

SANJ-NARZO has a .vmdk file

VES-PC202 has a whole drive

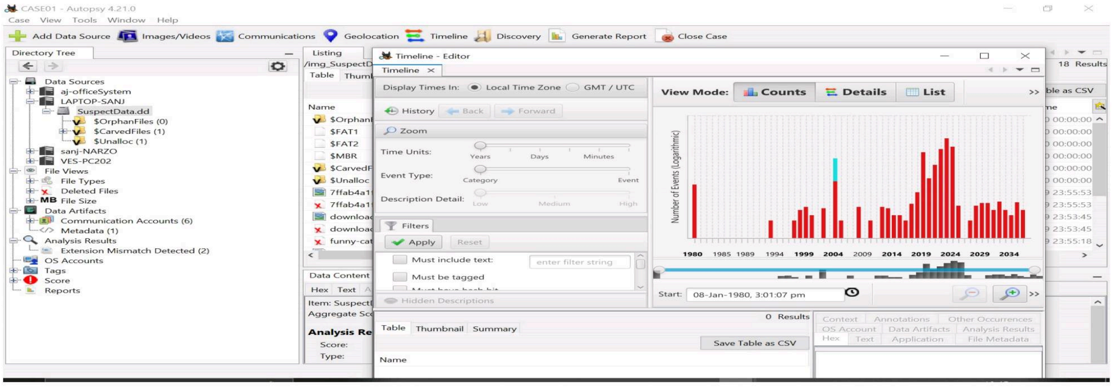
Making a folder to keep stuff sorted:



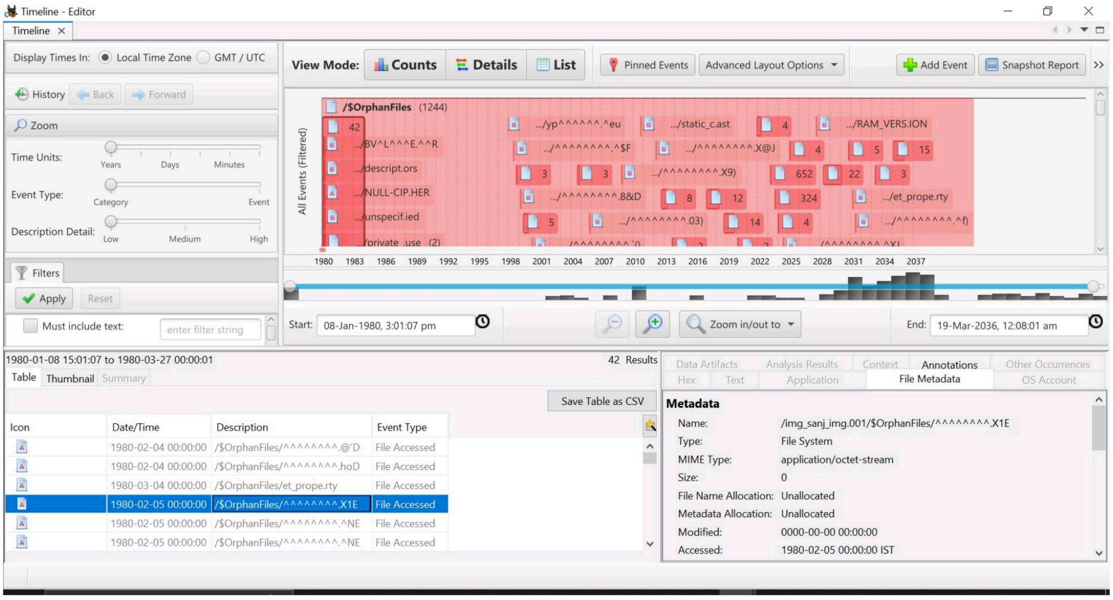
USB Drive (G:) > DF_TOOLS > CASE01-ASRSANJ

Name	Date modified	Type	Size
CASE01	30-03-2024 03:33	File folder	
docs	30-03-2024 03:01	File folder	
images	30-03-2024 04:22	File folder	
recovered	30-03-2024 03:28	File folder	
reports	30-03-2024 03:02	File folder	

Counts:



Details:



□ Must include text: enter filter string

Start: 08-Jan-1980, 3:01:07 pm

End: 19-Mar-2036, 12:08:01 am

1980-01-08 15:01:07 to 1980-03-27 00:00:01 — 42 Results

Table | Thumbnail | Summary — Save Table as CSV

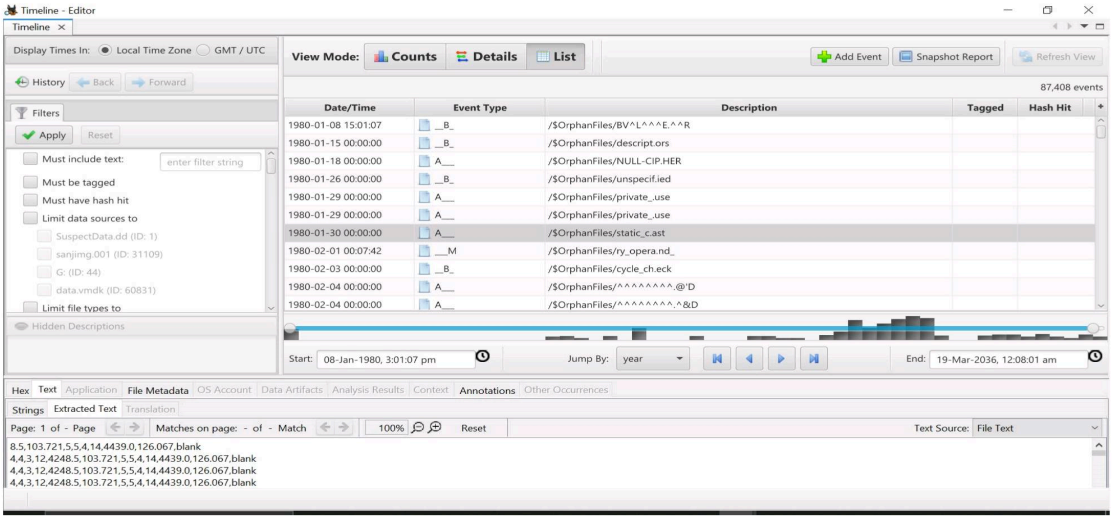
Icon	Date/Time	Description	Event Type
	1980-02-04 00:00:00	/$OrphanFiles/^^^^^^^^.@'D	File Accessed
	1980-02-04 00:00:00	/$OrphanFiles/^^^^^^^^.hoD	File Accessed
	1980-03-04 00:00:00	/$OrphanFiles/et_prope.rty	File Accessed
	1980-02-05 00:00:00	/$OrphanFiles/^^^^^^^^.X1E	File Accessed
	1980-02-05 00:00:00	/$OrphanFiles/^^^^^^^^.^NE	File Accessed
	1980-02-05 00:00:00	/$OrphanFiles/^^^^^^^^.^NE	File Accessed

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

Metadata

Name:	/img_sanj_img.001/$OrphanFiles/^^^^^^^^.X1E
Type:	File System
MIME Type:	application/octet-stream
Size:	0
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	0000-00-00 00:00:00
Accessed:	1980-02-05 00:00:00 IST

List:



□ Must include text: enter filter string
□ Must be tagged
□ Must have hash hit
□ Limit data sources to
□ SuspectData.dd (ID: 1)
□ sanjimg.001 (ID: 31109)
□ G: (ID: 44)
□ data.vmdk (ID: 60831)
□ Limit file types to

87,408 events

Date/Time	Event Type	Description	Tagged	Hash Hit
1980-01-08 15:01:07	__B_	/$OrphanFiles/BV^L^^^E.^^R		
1980-01-15 00:00:00	__B_	/$OrphanFiles/descript.ors		
1980-01-18 00:00:00	A__	/$OrphanFiles/NULL-CIP.HER		
1980-01-26 00:00:00	__B_	/$OrphanFiles/unspecif.ied		
1980-01-29 00:00:00	A__	/$OrphanFiles/private_.use		
1980-01-29 00:00:00	A__	/$OrphanFiles/private_.use		
1980-01-30 00:00:00	A__	/$OrphanFiles/static_c.ast		
1980-02-01 00:07:42	___M	/$OrphanFiles/ry_opera.nd_		
1980-02-03 00:00:00	__B_	/$OrphanFiles/cycle_ch.eck		
1980-02-04 00:00:00	A__	/$OrphanFiles/^^^^^^^^.@'D		
1980-02-04 00:00:00	A__	/$OrphanFiles/^^^^^^^^.^&D		

Start: 08-Jan-1980, 3:01:07 pm — End: 19-Mar-2036, 12:08:01 am

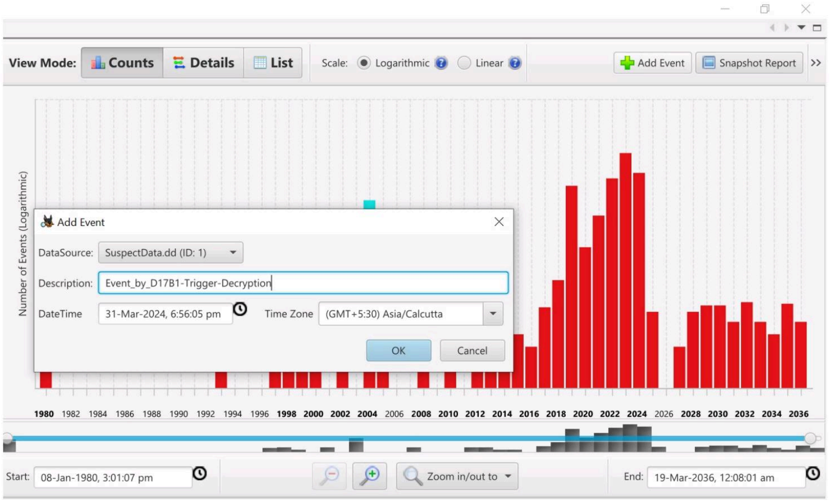
Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Strings | Extracted Text | Translation

Page: 1 of - Page — Matches on page: - of - Match — 100% — Reset — Text Source: File Text

```
8.5,103.721,5,5,4,14,4439.0,126.067,blank
4,4,3,12,4248.5,103.721,5,5,4,14,4439.0,126.067,blank
4,4,3,12,4248.5,103.721,5,5,4,14,4439.0,126.067,blank
4,4,3,12,4248.5,103.721,5,5,4,14,4439.0,126.067,blank
```

Adding a manual event:



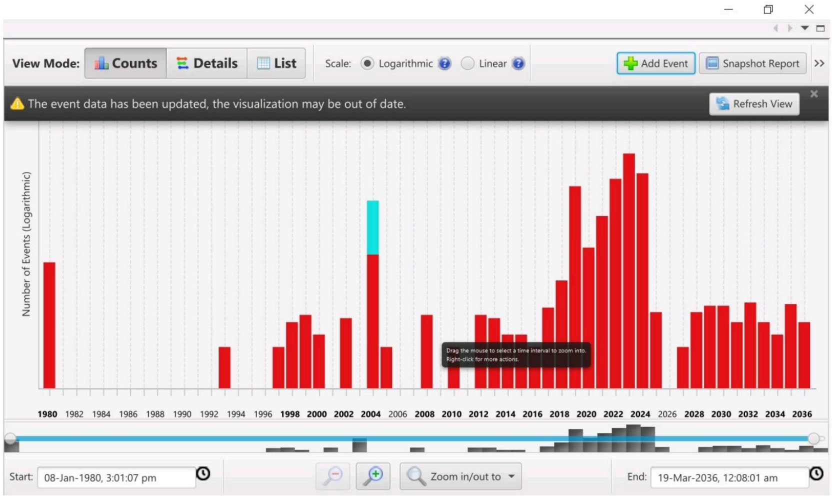
Add Event

DataSource: SuspectData.dd (ID: 1)

Description: Event_by_D17B1-Trigger-Decryption

DateTime: 31-Mar-2024, 6:56:05 pm — Time Zone: (GMT+5:30) Asia/Calcutta

Start: 08-Jan-1980, 3:01:07 pm — End: 19-Mar-2036, 12:08:01 am



View Mode: Counts | Details | List

Scale: ● Logarithmic ○ Linear

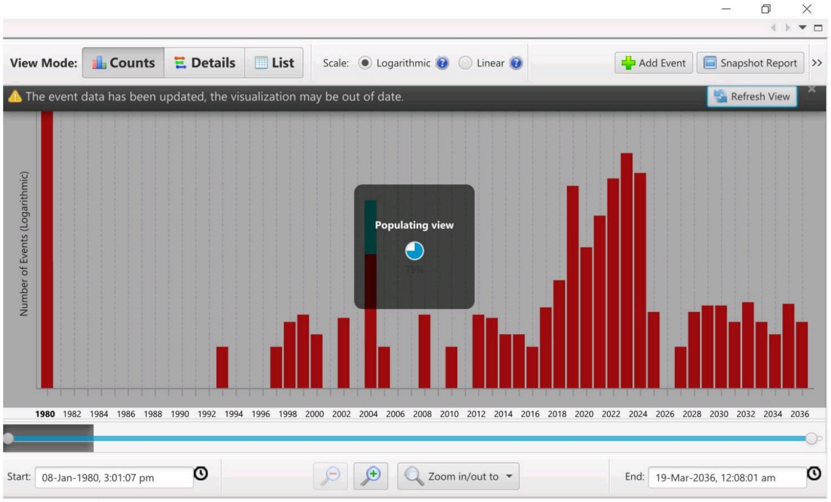
The event data has been updated, the visualization may be out of date.

Drag the mouse to select a time interval to zoom into.
Right-click for more actions.

Start: 08-Jan-1980, 3:01:07 pm

End: 19-Mar-2036, 12:08:01 am

Refresh it:



View Mode: Counts | Details | List

Scale: ● Logarithmic ○ Linear

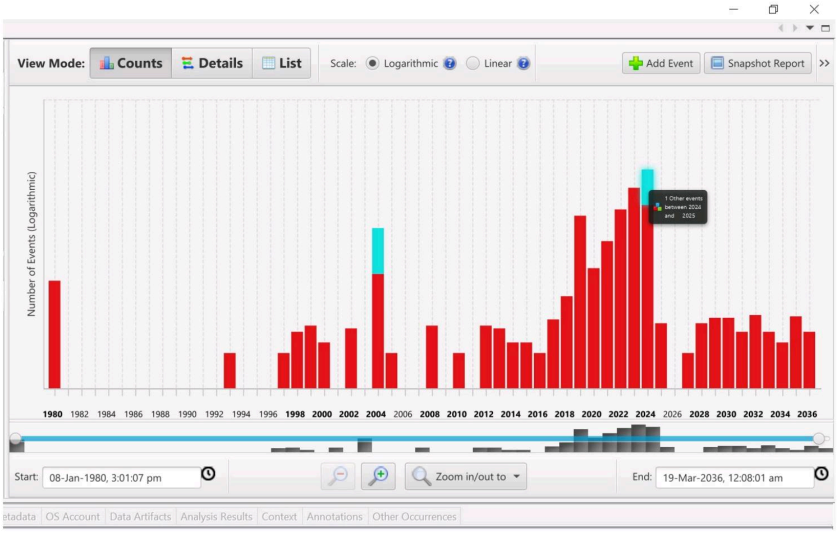
The event data has been updated, the visualization may be out of date.

Populating view

Start: 08-Jan-1980, 3:01:07 pm

End: 19-Mar-2036, 12:08:01 am

Event reflected on timeline:



View Mode: Counts | Details | List

Scale: ● Logarithmic ○ Linear

1 Other events
between 2024
and 2025

Start: 08-Jan-1980, 3:01:07 pm

End: 19-Mar-2036, 12:08:01 am