VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of the UGC Act, 1956)

WINTER SEMESTER 2019-20
DIGITAL FORENSICS (CSE4004)
LAB ASSIGNMENT - 6

Dishi Jain
17BCB0055

Autopsy - Digital Forensics Tool

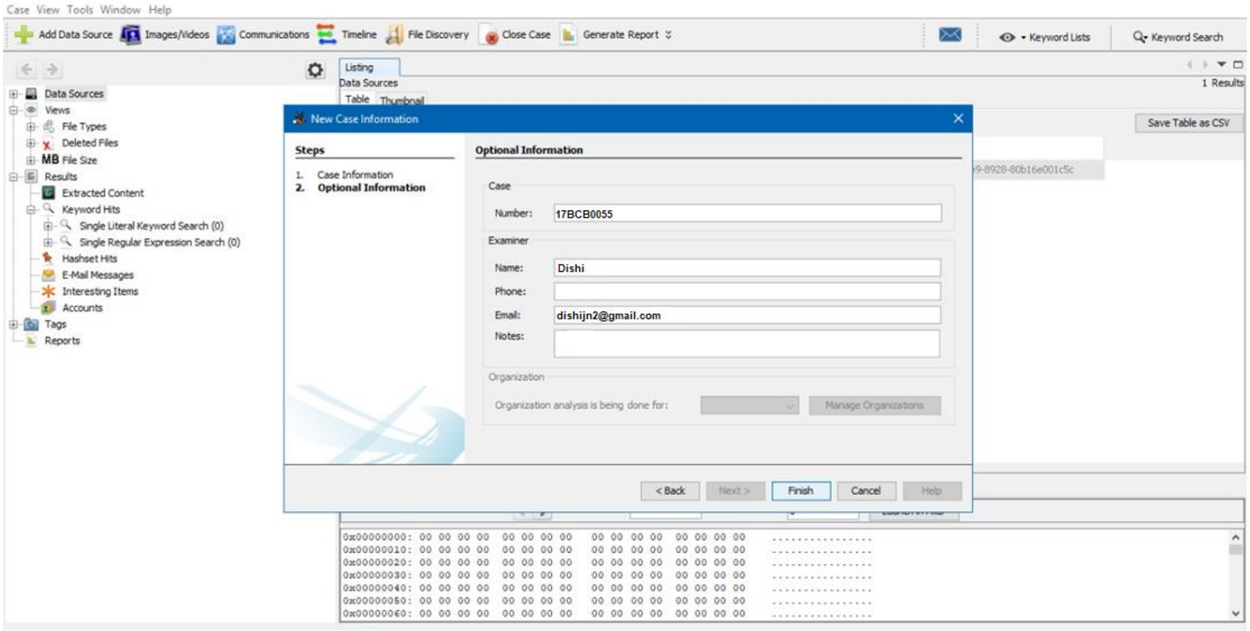
Autopsy is computer software that makes it simpler to deploy many of the open source programs and plugins used in the Sleuth kit. The graphical user interface displays the results from the forensic search of the underlying volume making it easier for investigators to flag pertinent sections of data.

Process:

Autopsy analyzes major file systems (NTFS, FAT, ExFAT, HFS+, Ext2/Ext3/Ext4, YAFFS2) by hashing all files, unpacking standard archives (ZIP, JAR etc.), extracting any EXIF values and putting keywords in an index. Some file types like standard email formats or contact files are also parsed and cataloged.Users can search these indexed files for recent activity or create a report in HTML or PDF summarizing important recent activity. If time is short, users may activate triage features that use rules to analyze the most important files first. Autopsy can save a partial image of these files in the VHD format.

Correlation:

Investigators working with multiple machines or file systems can build a central repository of data allowing them to flag phone numbers, email addresses, file or other pertinent data that might be found in multiple places. The SQL Lite or PostgreSQL data base stores the information so investigators can find all occurrences of names, domains, phone numbers or USB registry entries.



New Case Information

Steps

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

Optional Information

Case

Number: 17BCB0055

Examiner

Name: Dishi

Phone:

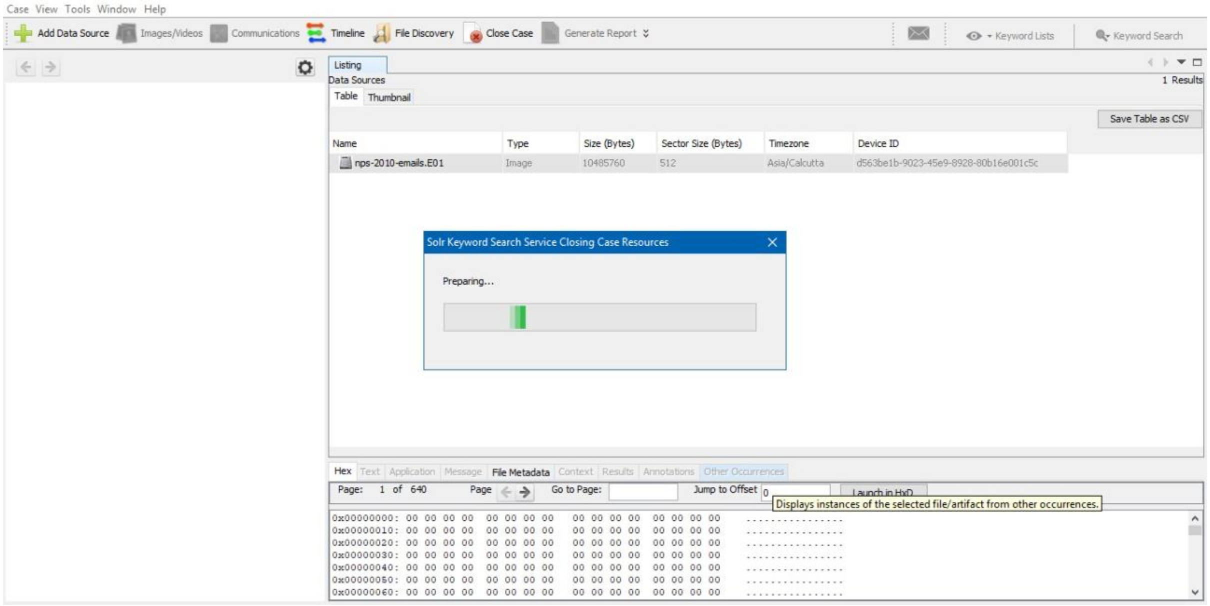
Email: dishijn2@gmail.com

Notes:

Organization

Organization analysis is being done for:

```
0x00000000: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000010: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000020: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000030: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000040: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000050: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000060: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
```



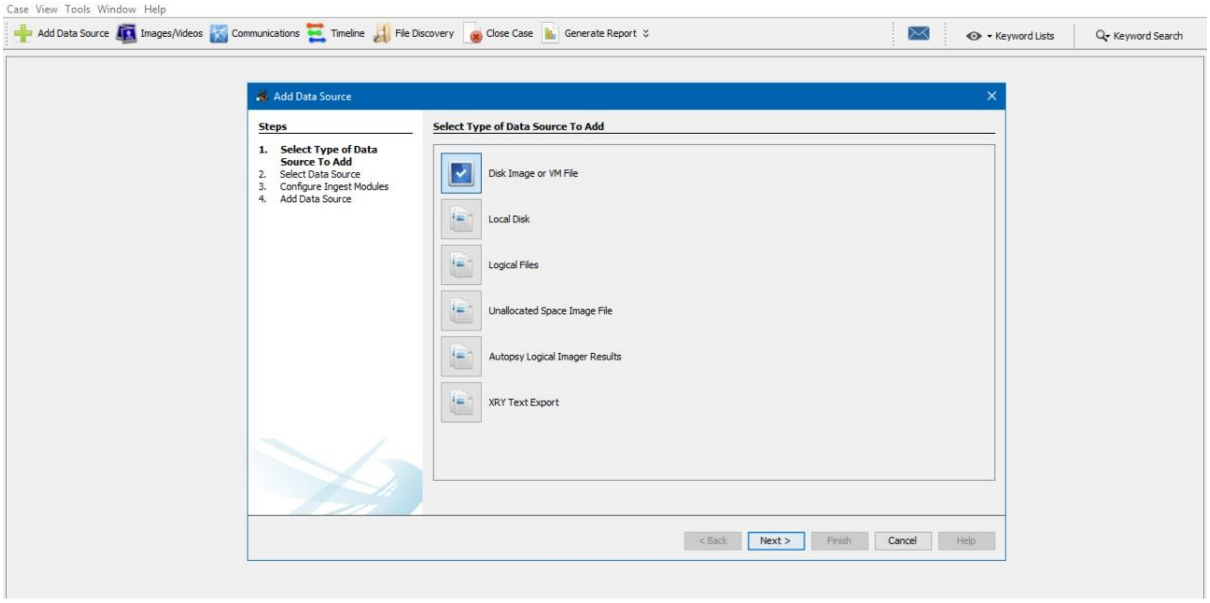
Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
nps-2010-emails.E01	Image	10485760	512	Asia/Calcutta	d563be1b-9023-45e9-8928-80b16e001c5c

Solr Keyword Search Service Closing Case Resources

Preparing...

Displays instances of the selected file/artifact from other occurrences.

```
0x00000000: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000010: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000020: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000030: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000040: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000050: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x00000060: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
```



Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source

Select Type of Data Source To Add

☑ Disk Image or VM File

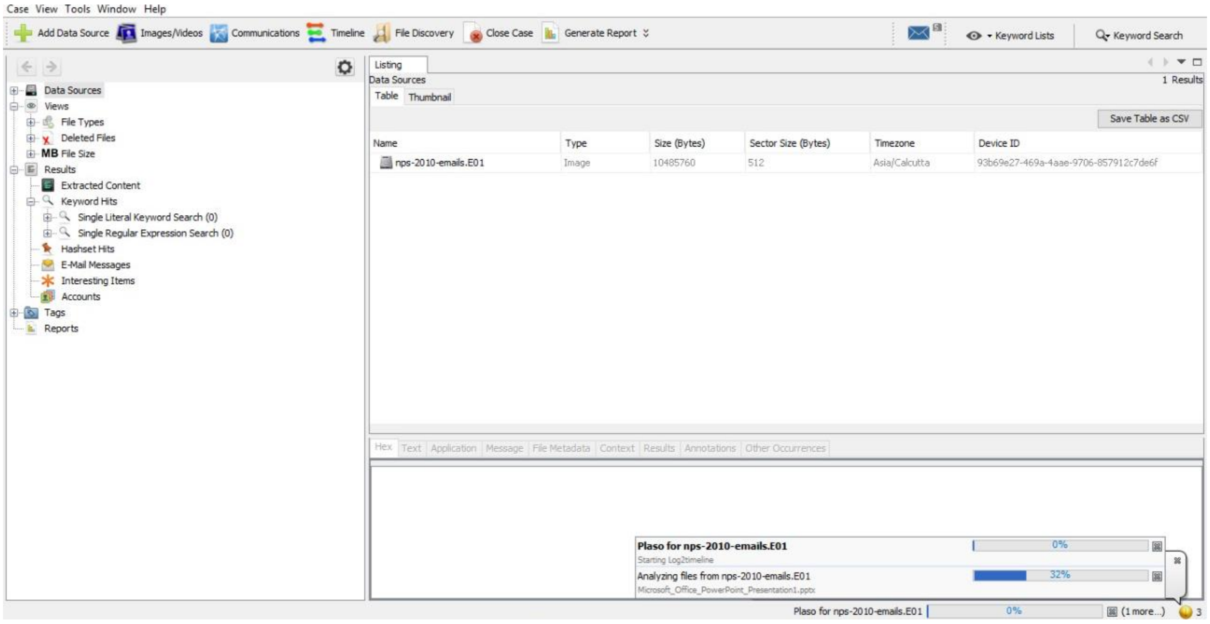
Local Disk

Logical Files

Unallocated Space Image File

Autopsy Logical Imager Results

XRY Text Export



Data Sources

1 Results

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
nps-2010-emails.E01	Image	10485760	512	Asia/Calcutta	93b69e27-469a-4aae-9706-857912c7de6f

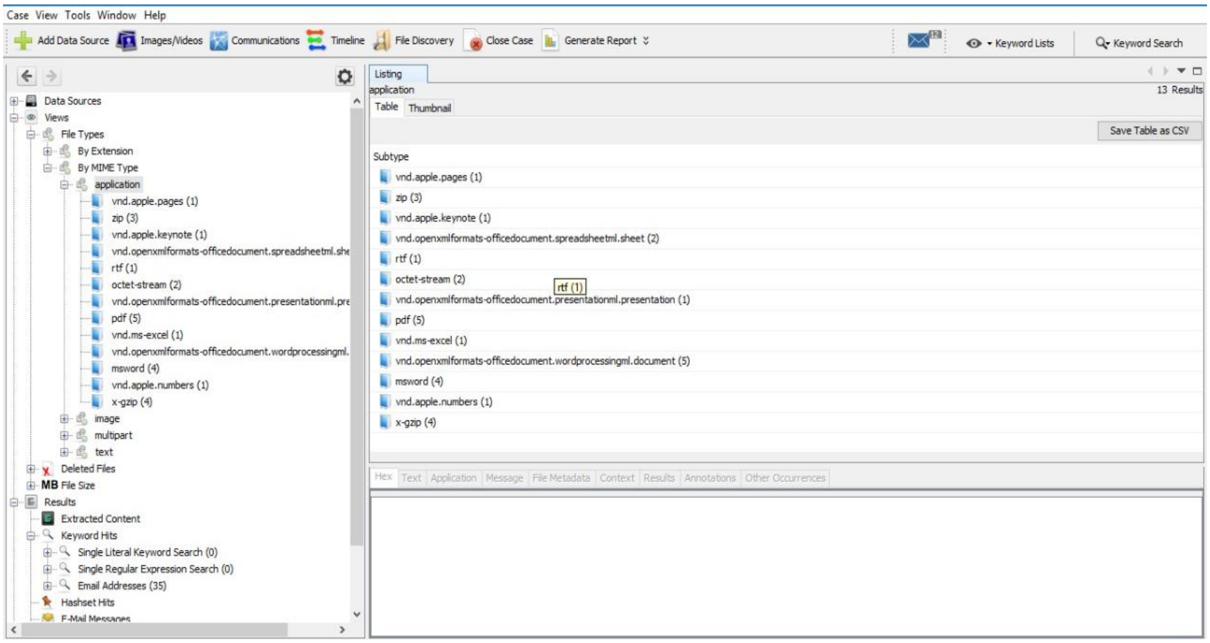
Plaso for nps-2010-emails.E01 0%

Starting Log2timeline

Analyzing files from nps-2010-emails.E01 32%

Microsoft_Office_PowerPoint_Presentation1.pptx

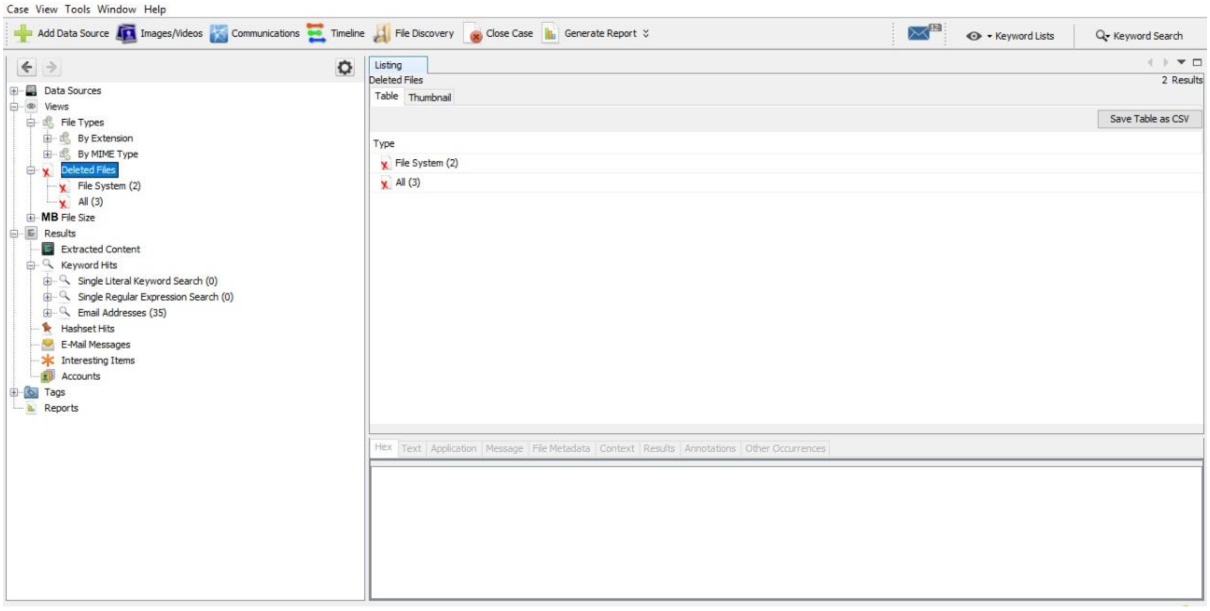
Plaso for nps-2010-emails.E01 0% (1 more...) 3



- Data Sources
- Views
  - File Types
    - By Extension
    - By MIME Type
      - application
        - vnd.apple.pages (1)
        - zip (3)
        - vnd.apple.keynote (1)
        - vnd.openxmlformats-officedocument.spreadsheetml.she
        - rtf (1)
        - octet-stream (2)
        - vnd.openxmlformats-officedocument.presentationml.pre
        - pdf (5)
        - vnd.ms-excel (1)
        - vnd.openxmlformats-officedocument.wordprocessingml.
        - msword (4)
        - vnd.apple.numbers (1)
        - x-gzip (4)
      - image
      - multipart
      - text
  - Deleted Files
  - MB File Size
- Results
  - Extracted Content
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
    - Email Addresses (35)
  - Hashset Hits
  - E-Mail Messages

application
13 Results

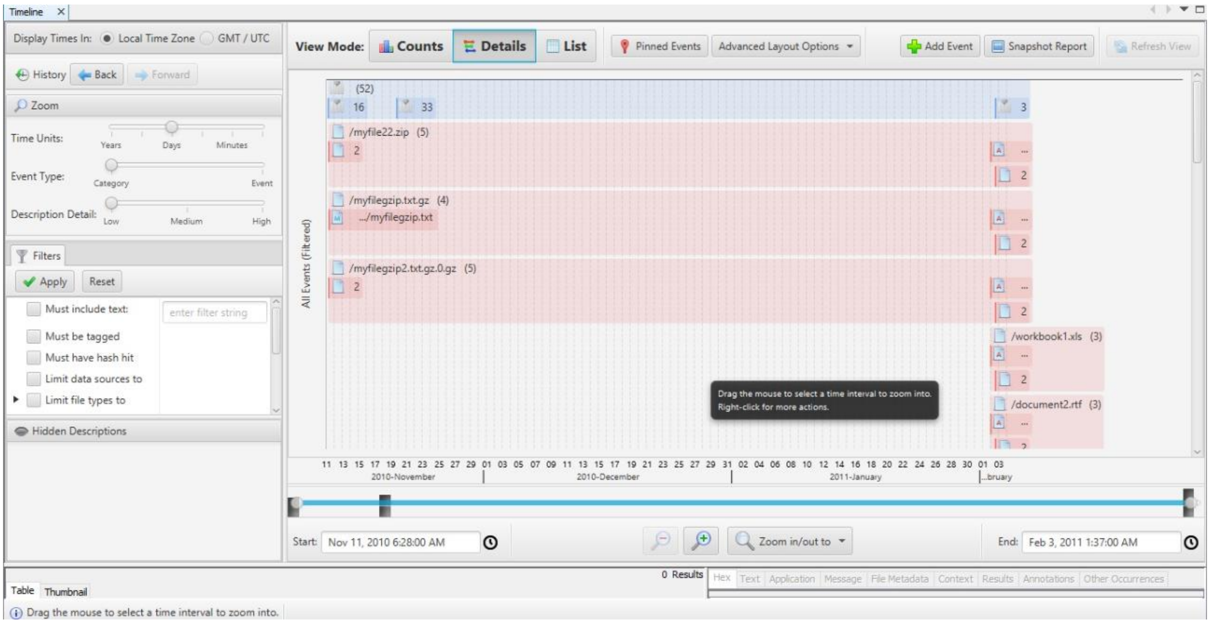
Subtype
vnd.apple.pages (1)
zip (3)
vnd.apple.keynote (1)
vnd.openxmlformats-officedocument.spreadsheetml.sheet (2)
rtf (1)
octet-stream (2)
vnd.openxmlformats-officedocument.presentationml.presentation (1)
pdf (5)
vnd.ms-excel (1)
vnd.openxmlformats-officedocument.wordprocessingml.document (5)
msword (4)
vnd.apple.numbers (1)
x-gzip (4)



- Data Sources
- Views
  - File Types
    - By Extension
    - By MIME Type
  - Deleted Files
    - File System (2)
    - All (3)
  - MB File Size
- Results
  - Extracted Content
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
    - Email Addresses (35)
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
  - Accounts
- Tags
- Reports

Deleted Files
2 Results

Type
File System (2)
All (3)



Display Times In: ● Local Time Zone ○ GMT / UTC

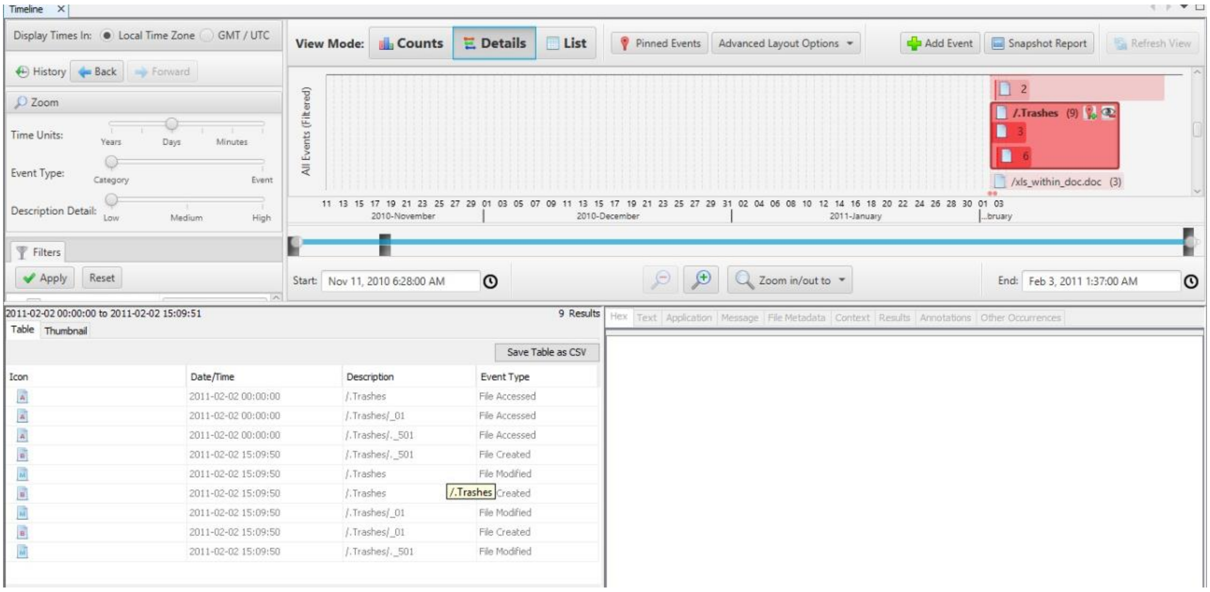
Drag the mouse to select a time interval to zoom into.
Right-click for more actions.

Start: Nov 11, 2010 6:28:00 AM

End: Feb 3, 2011 1:37:00 AM

0 Results

Drag the mouse to select a time interval to zoom into.



Display Times In: ● Local Time Zone ○ GMT / UTC

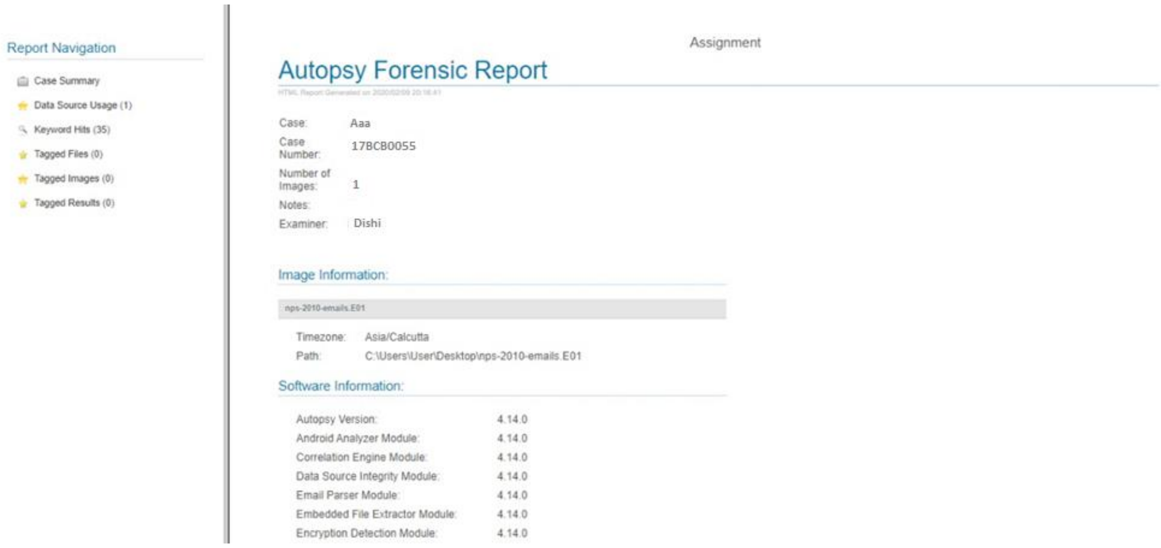
Start: Nov 11, 2010 6:28:00 AM

End: Feb 3, 2011 1:37:00 AM

2011-02-02 00:00:00 to 2011-02-02 15:09:51

9 Results

Icon	Date/Time	Description	Event Type
A	2011-02-02 00:00:00	/.Trashes	File Accessed
A	2011-02-02 00:00:00	/.Trashes/_01	File Accessed
A	2011-02-02 00:00:00	/.Trashes/._501	File Accessed
B	2011-02-02 15:09:50	/.Trashes/._501	File Created
M	2011-02-02 15:09:50	/.Trashes	File Modified
B	2011-02-02 15:09:50	/.Trashes	Created
M	2011-02-02 15:09:50	/.Trashes/_01	File Modified
B	2011-02-02 15:09:50	/.Trashes/_01	File Created
M	2011-02-02 15:09:50	/.Trashes/._501	File Modified



Assignment

Autopsy Forensic Report

HTML Report Generated on 2020/02/09 20:16:41

Case:	Aaa
Case Number:	17BCB0055
Number of Images:	1
Notes:	
Examiner:	Dishi

Image Information:

nps-2010-emails.E01

Timezone:	Asia/Calcutta
Path:	C:\Users\User\Desktop\nps-2010-emails.E01

Software Information:

Autopsy Version:	4.14.0
Android Analyzer Module:	4.14.0
Correlation Engine Module:	4.14.0
Data Source Integrity Module:	4.14.0
Email Parser Module:	4.14.0
Embedded File Extractor Module:	4.14.0
Encryption Detection Module:	4.14.0