Installing Autopsy

Mustafa Ranapurwala | Ross Barber | Carina Martinez-Lopez | Zoe Medina | Randall Seymore
27 November 2023
CYBR 512

Table of Contents

Statement of Objective **1**

Theory **1**

Description of Experimental Setup **1**

Procedure **1**

Data **2**

Install Autopsy 2

USB Examination 3

HackingCase Examination 4

M57-Jean Examination 5

Analysis of Data **7**

Discussion of Results **7**

Conclusion **7**

Statement of Objective

This report briefly details systematic analysis of digital storage media using the Autopsy forensic tool. The analysis aims to assess various digital artifacts and data structures present on disk images and computer systems. Analysts performed a comprehensive examination of the tool's functionality using constructed investigation scenarios. Insights gained will be used to prepare for future incident scenarios requiring forensic analysis.

Theory

Each of the scenarios studied for this lab should provide analysts with adequate familiarity of the Autopsy tool, enabling effective use in future assignment scenarios.

Description of Experimental Setup

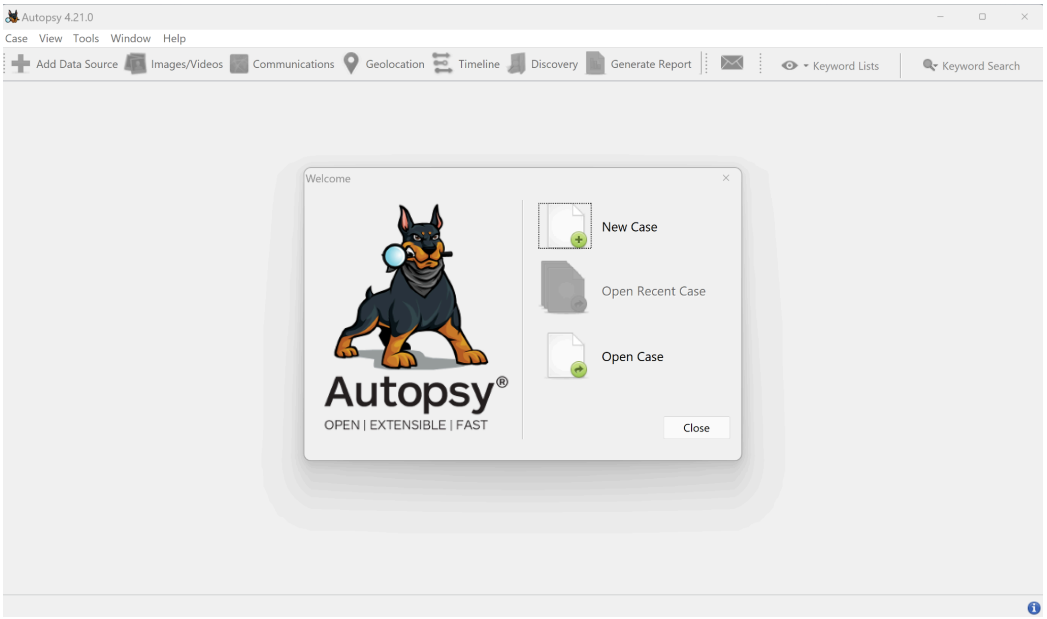
Testers installed the 64-bit version of the Autopsy software on computers running either Windows 10 or Windows 11. Three distinct data sources, representing different types of digital evidence, were arranged into separate Autopsy cases: A USB device, a 'HackingCase' case for initial review of a full computer image, and an 'M57-Jean' case to review a true incident scenario.

Procedure

Each data set was ingested into the Autopsy platform to understand tool functionality and understand ingestion behavior. Following ingestion, a brief preliminary review of each case was conducted to validate data integrity and to establish a baseline knowledge of the contents contained within.

Data

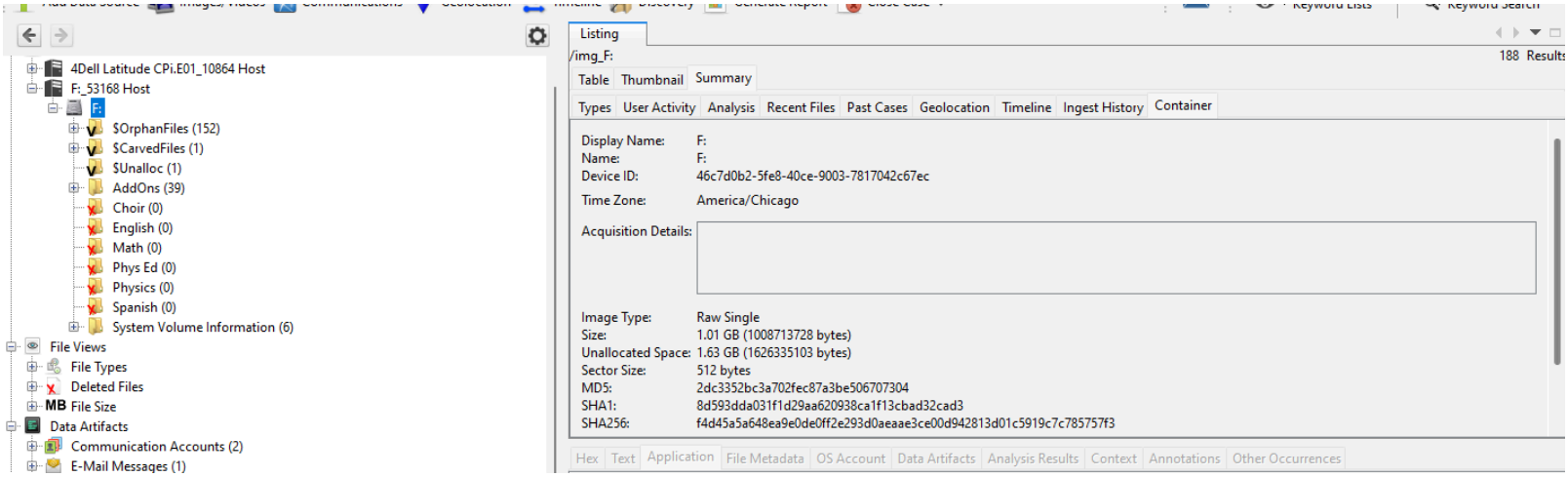
Install Autopsy



USB Examination

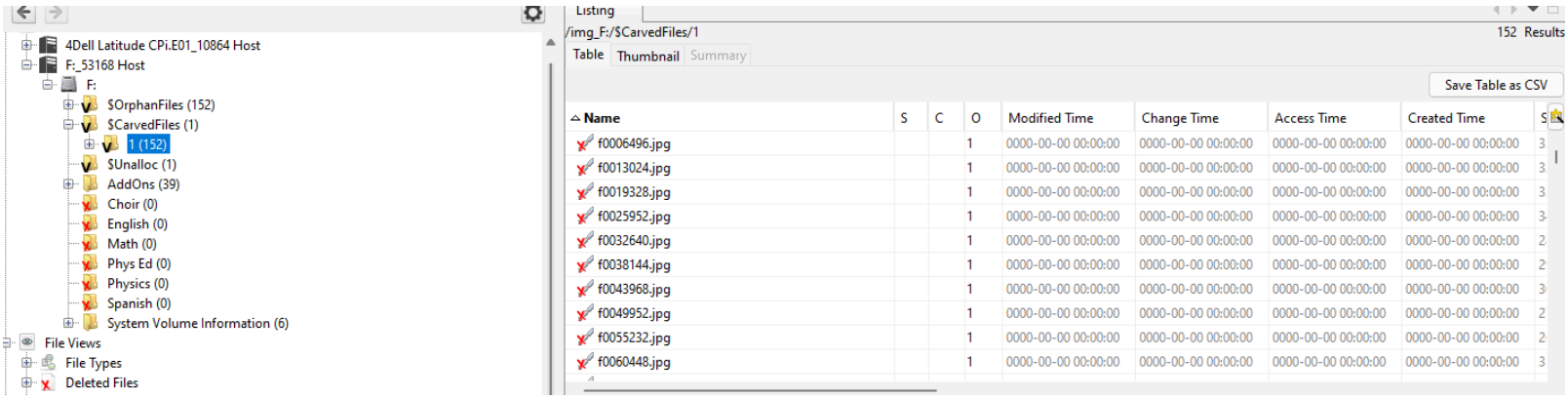
Ingest USB Disk Contents

A USB drive containing approximately 1.01 GB of data was ingested into Autopsy for analysis. Screenshot depicts contents of drive.



Review ‘CarvedFiles’

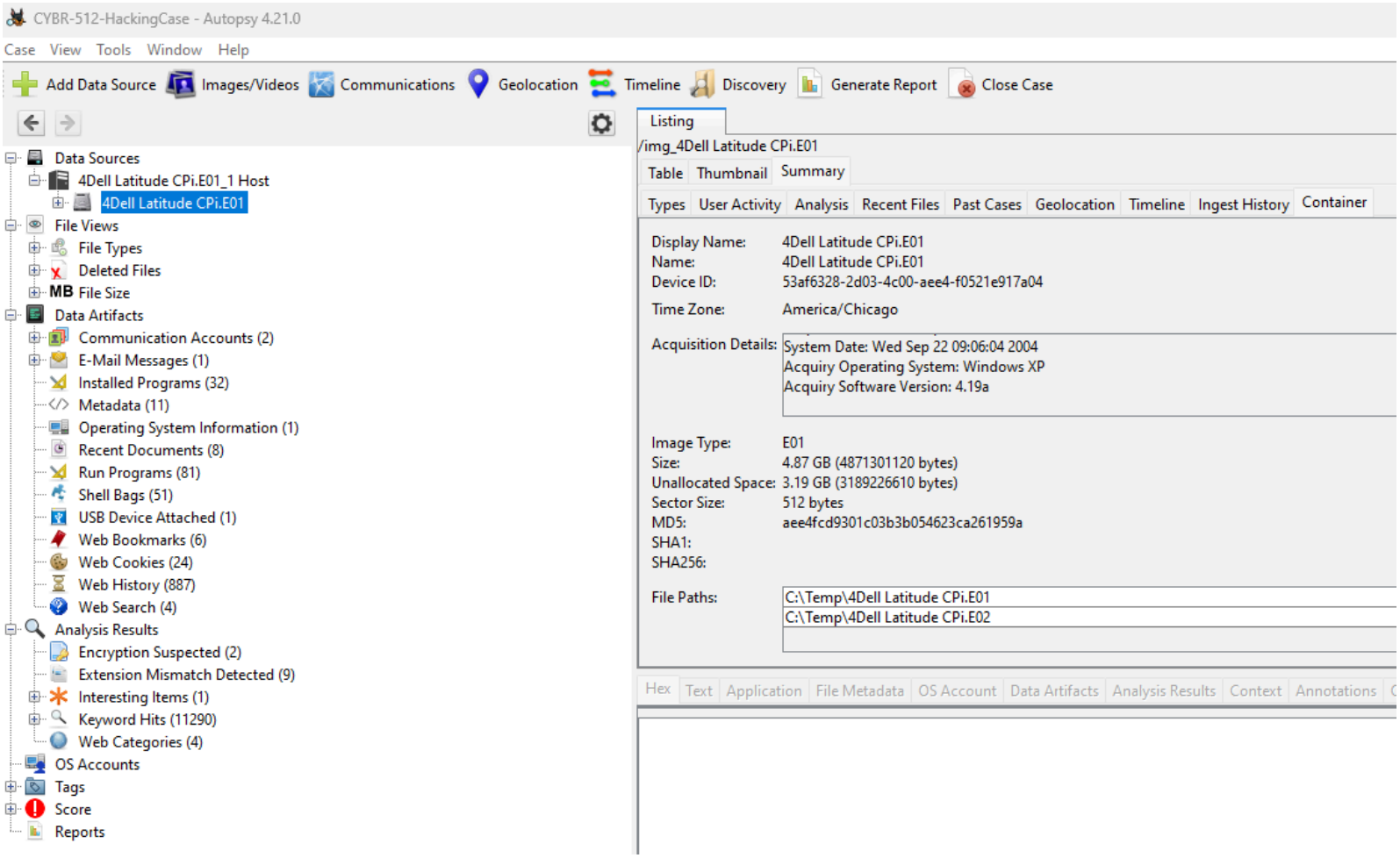
A single folder labeled ‘1’ was created by Autopsy in the CarvedFiles folder, which contained 152 files.



HackingCase Examination

Ingest HackingCase Image Files

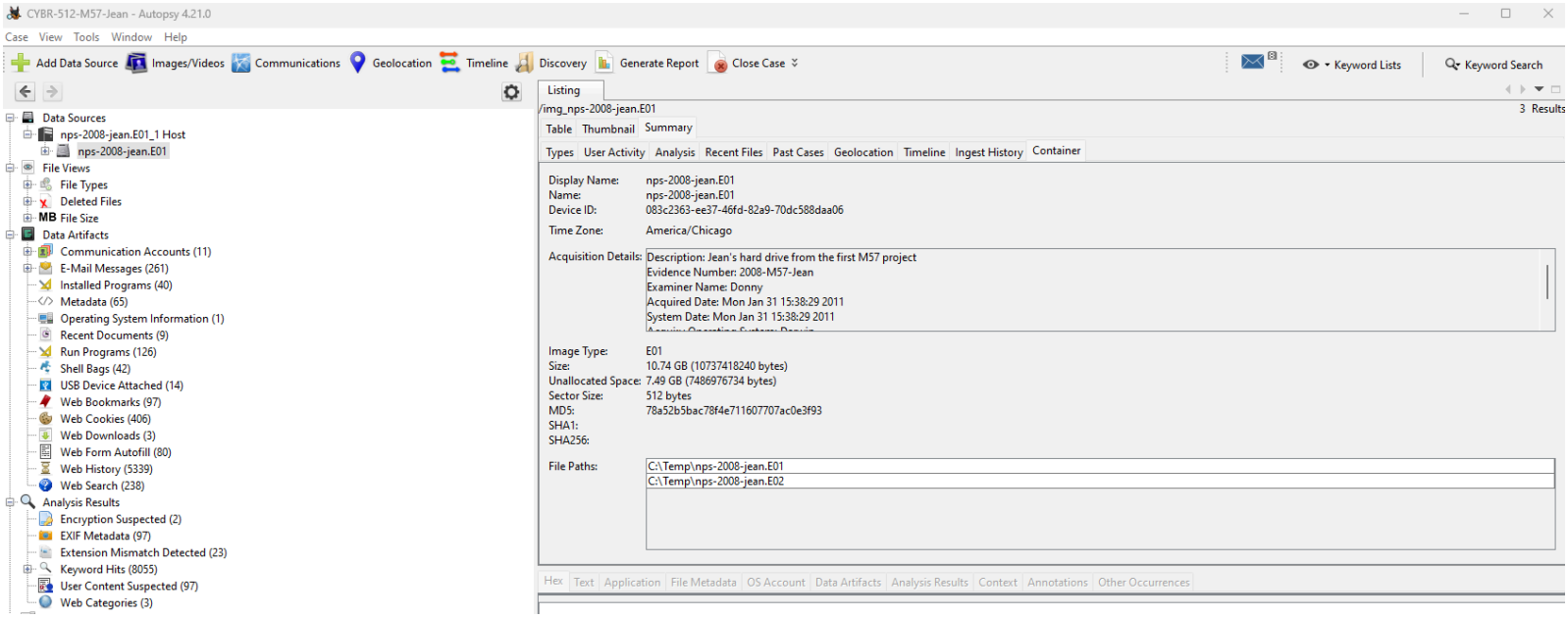
Image files ‘4Dell Latitude CPi.E01’ and ‘4Dell Latitude CPi.E02’ were ingested into Autopsy for analysis.



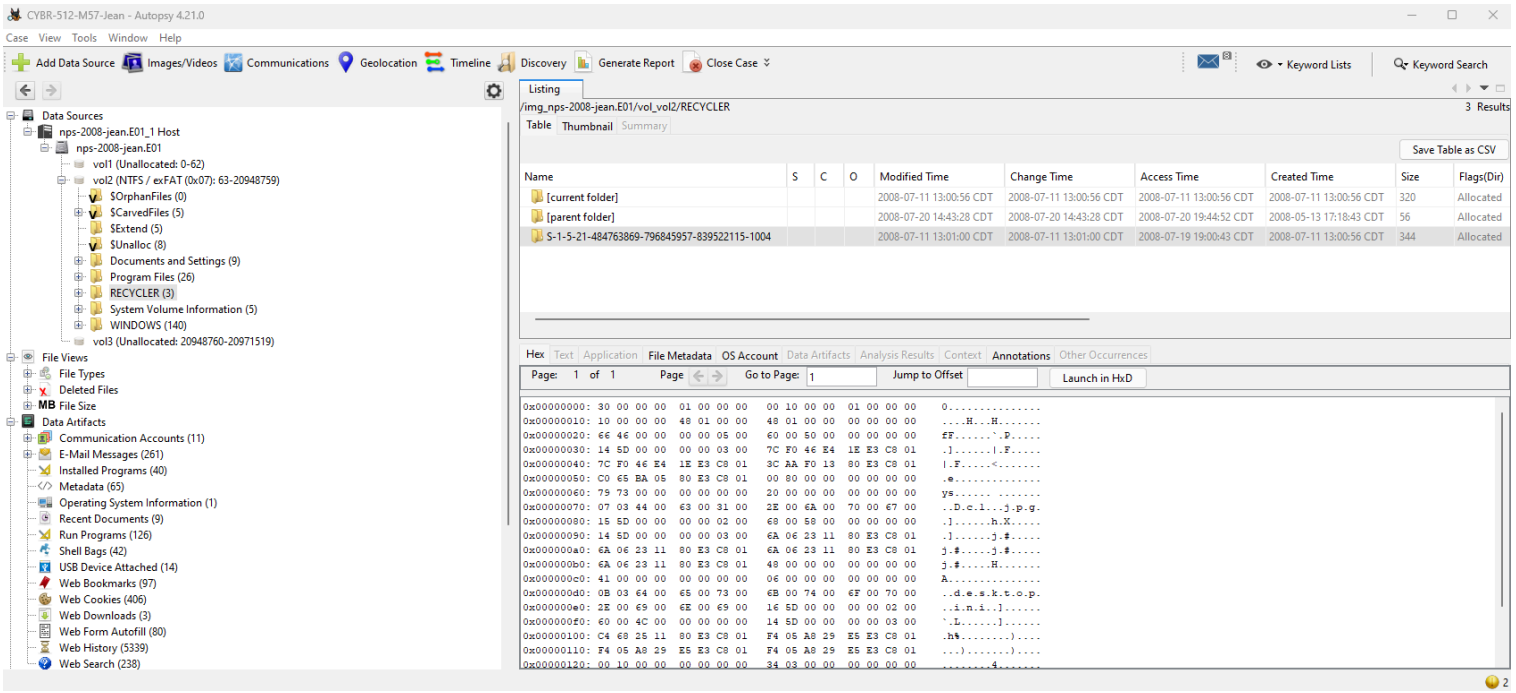
M57-Jean Examination

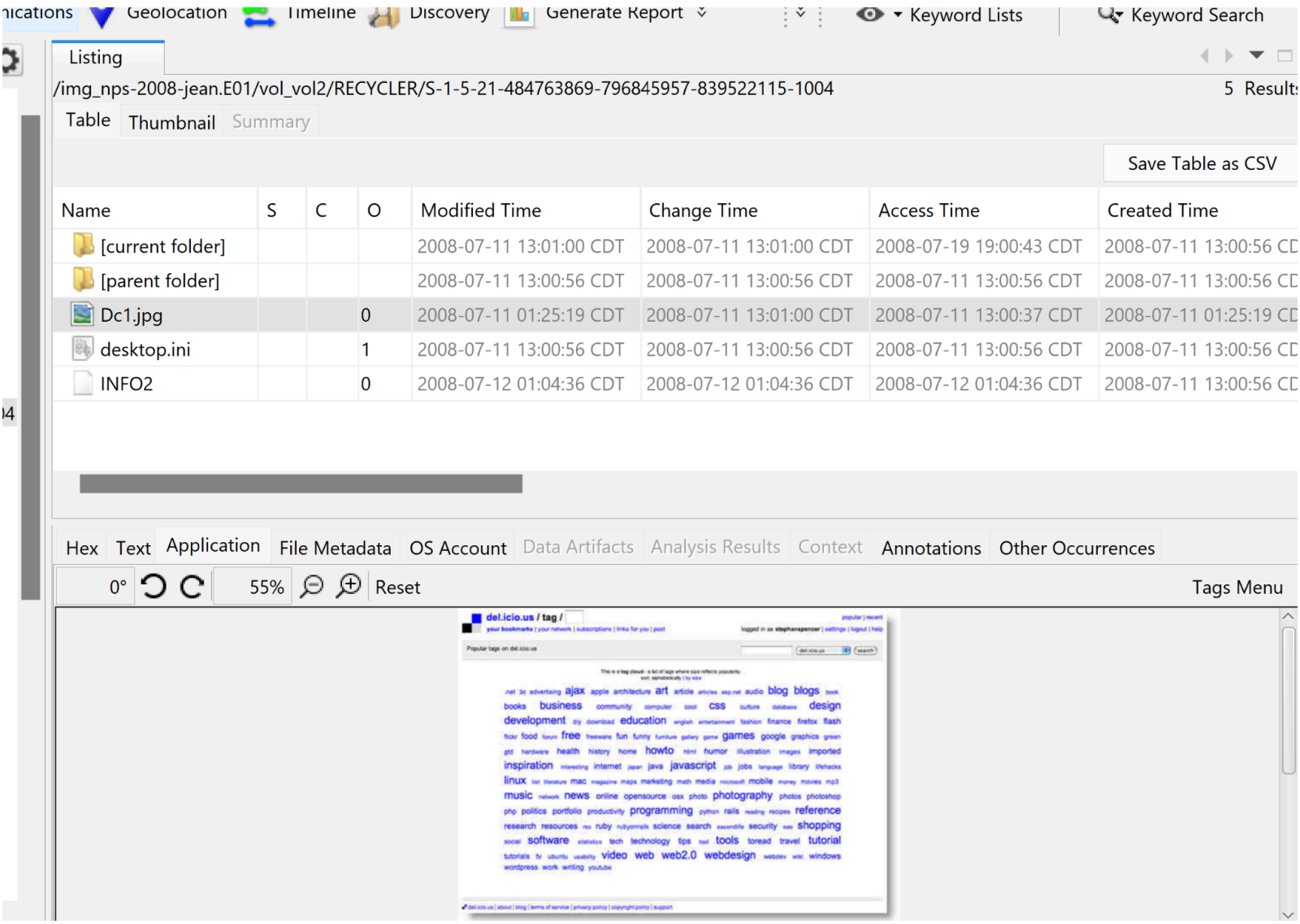
Ingest M57-Jean Image Files

Image files ‘nps-2008-jean.E01’ and ‘nps-2008-jean.E02’ were ingested into Autopsy for analysis.



Review Contents of ‘RECYCLER’ folder




Geolocation
Timeline
Discovery
Generate Report
Keyword Lists
Keyword Search
Listing
/img_nps-2008-jean.E01/vol_vol2/RECYCLER/S-1-5-21-484763869-796845957-839522115-1004
5 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
[current folder]
2008-07-11 13:01:00 CDT
2008-07-11 13:01:00 CDT
2008-07-19 19:00:43 CDT
2008-07-11 13:00:56 CD
[parent folder]
2008-07-11 13:00:56 CDT
2008-07-11 13:00:56 CDT
2008-07-11 13:00:56 CDT
2008-07-11 13:00:56 CD
Dc1.jpg
0
2008-07-11 01:25:19 CDT
2008-07-11 13:01:00 CDT
2008-07-11 13:00:37 CDT
2008-07-11 01:25:19 CD
desktop.ini
1
2008-07-11 13:00:56 CDT
2008-07-11 13:00:56 CDT
2008-07-11 13:00:56 CDT
2008-07-11 13:00:56 CD
INFO2
0
2008-07-12 01:04:36 CDT
2008-07-12 01:04:36 CDT
2008-07-12 01:04:36 CDT
2008-07-11 13:00:56 CD
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
0°
55%
Reset
Tags Menu
del.icio.us / tag /

Analysis of Data

During the USB examination of the assignment, Autopsy identified various files, including several in the ‘CarvedFiles’ folder.

During the HackingCase examination, testers reviewed image files in Autopsy to simulate an investigation of a suspicious individual. Throughout the examination, basic information such as type of operating system, timezone, and installation date were analyzed. Testers further identified the registered owner, list of account names, last known shut down, and last known user logged in. Finally, behavior of the user of the laptop was reviewed by looking at installed programs, email addresses, website visits, and deleted files.

As part of the 2009 M57-Jean scenario examination, testers primarily attempted to identify the user who created the spreadsheet and were able to confirm that the file was originally created by the ‘Alison’ user. It is currently unknown how specifically the excel document was placed on the competitors website, however initial investigation reveals Jean’s email address was used to send the excel document to Alison.

Discussion of Results

After completing investigation of the abandoned laptop, testers found a variety of hacking tools installed and a “Mr. Evil” user frequently communicating in hacker forums. Testers also identified additional noteworthy items such as a zip bomb packaged on the device, typically used to overload a system and disable it.

Conclusion

In conclusion, the team was able to successfully install the Autopsy software and begin analysis on the target subjects. The project gave us a solid foundation of understanding how to utilize Autopsy to derive information on various types of resources. The analysis of the USB drive provided us valuable insight on how to analyze various files for investigative purposes. The laptop examination allowed us to see how an analysis can be conducted to derive a multitude of useful information on such subjects. Lastly, we ran through the M57-Jean case where we were were able to determine how and who stole data from a simulated company. Overall, the assignment revealed just how useful autopsy tools can be when utilized for digital forensics.