
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

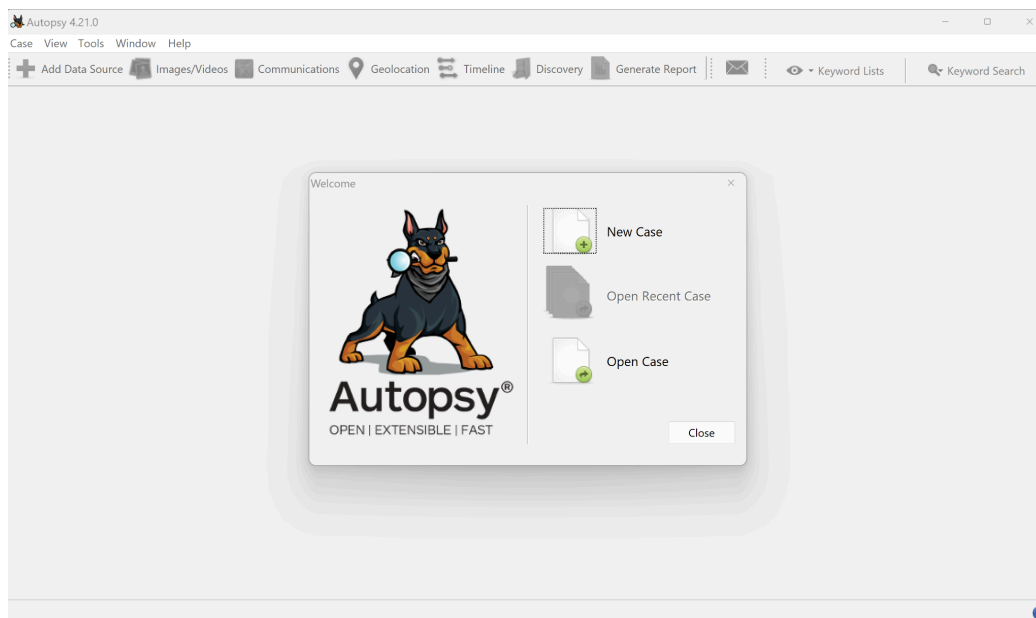
Testers installed the 64-bit version of the Autopsy software on computers running either Windows 10 or Windows 11. Three distinct data sources, representing different types of digital evidence, were arranged into separate Autopsy cases: A USB device, a 'HackingCase' case for initial review of a full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

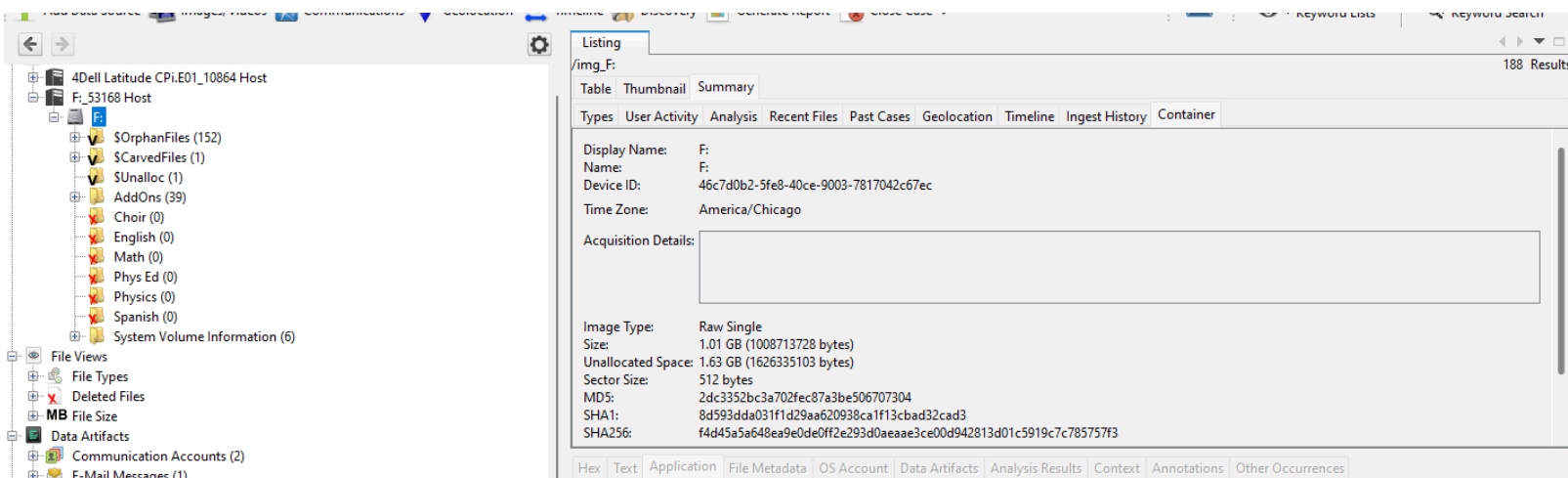
Install Autopsy



USB Examination

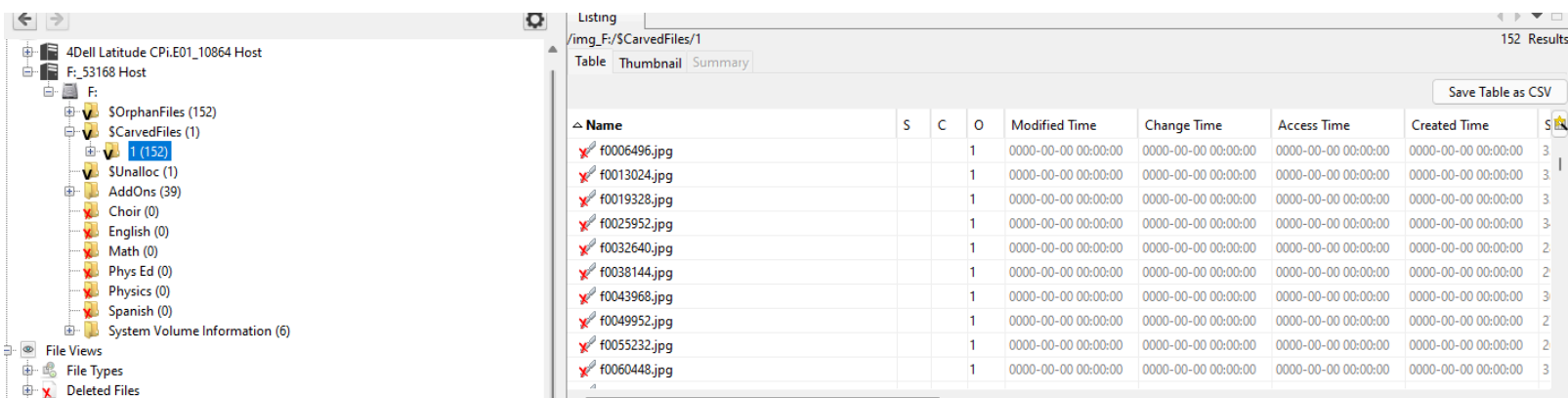
Ingest USB Disk Contents

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.

CYBR-512-HackingCase - Autopsy 4.21.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

← → ⚙

Data Sources

- 4Dell Latitude CPi.E01_1 Host
 - 4Dell Latitude CPi.E01

File Views

- File Types
- Deleted Files
- MB File Size

Data Artifacts

- Communication Accounts (2)
- E-Mail Messages (1)
- Installed Programs (32)
- Metadata (11)
- Operating System Information (1)
- Recent Documents (8)
- Run Programs (81)
- Shell Bags (51)
- USB Device Attached (1)
- Web Bookmarks (6)
- Web Cookies (24)
- Web History (887)
- Web Search (4)

Analysis Results

- Encryption Suspected (2)
- Extension Mismatch Detected (9)
- Interesting Items (1)
- Keyword Hits (11290)
- Web Categories (4)

OS Accounts

- Tags
- Score
- Reports

Listing

/img_4Dell Latitude CPi.E01

Table Thumbnail Summary

Types	User Activity	Analysis	Recent Files	Past Cases	Geolocation	Timeline	Ingest History	Container
Display Name:	4Dell Latitude CPi.E01							
Name:	4Dell Latitude CPi.E01							
Device ID:	53af6328-2d03-4c00-ae4-f0521e917a04							
Time Zone:	America/Chicago							
Acquisition Details:	System Date: Wed Sep 22 09:06:04 2004 Acquir Operating System: Windows XP Acquir 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:\Temp\4Dell Latitude CPi.E01 C:\Temp\4Dell Latitude CPi.E02							

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations C

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.

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays the 'Data Sources' tree with 'nps-2008-jean.E01' selected. The main pane shows the 'Listing' tab for '/img_nps-2008-jean.E01'. The details pane on the right provides information about the image file.

Types	User Activity	Analysis	Recent Files	Past Cases	Geolocation	Timeline	Ingest History	Container
Display Name: nps-2008-jean.E01 Name: nps-2008-jean.E01 Device ID: 083c2363-ee37-46fd-82a9-70dc588daa06 Time Zone: America/Chicago Acquisition Details: Description: Jean's hard drive from the first M57 project Evidence Number: 2008-M57-Jean Examiner Name: Donny Acquired Date: Mon Jan 31 15:38:29 2011 System Date: Mon Jan 31 15:38:29 2011 Image Type: E01 Size: 10.74 GB (10737418240 bytes) Unallocated Space: 7.49 GB (7486976734 bytes) Sector Size: 512 bytes MD5: 78a52b5bac78f4e711607707ac0e3f93 SHA1: SHA256: File Paths: C:\Temp\nps-2008-jean.E01 C:\Temp\nps-2008-jean.E02								

Review Contents of 'RECYCLER' folder

The screenshot shows the Autopsy 4.21.0 interface with the 'RECYCLER' folder selected. The left sidebar shows the 'Data Sources' tree with 'nps-2008-jean.E01' expanded to show the 'vol1 (NTFS / exFAT (0x07): 63-20948759)' volume. The main pane shows the 'Listing' tab for '/img_nps-2008-jean.E01/vol1/vol1/RECYCLER'. The details pane on the right shows the contents of the folder.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
[current 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 CDT	320	Allocated
[parent folder]				2008-07-20 14:43:28 CDT	2008-07-20 14:43:28 CDT	2008-07-20 19:44:52 CDT	2008-05-13 17:18:43 CDT	56	Allocated
S-1-5-21-484763869-796845957-839522115-1004				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 CDT	344	Allocated

The bottom pane shows the hex dump of the folder's metadata, including the file's name and other attributes.

Communications

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 CDT
[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 CDT
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 CDT
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 CDT
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 CDT

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

0°

↺

↻

55%

🗨

🔍

Reset

Tags Menu

del.icio.us / tag /

your bookmarks | your network | subscriptions | links for you | post

logged in as [slaphamspencer](#) | settings | logged | help

Popular tags on del.icio.us

This is a tag cloud - a list of tags where size reflects popularity and separates the new

.net 3d advertising ajax apple architecture art article articles aspx.net audio blog blogs book books business community computer cool css culture database design development diy download education english entertainment fashion finance firefox flash flickr food forum free freeware fun funny furniture gallery game games google graphics green gtd hardware health history home howto html humor illustration images imported inspiration interesting internet japan java javascript js jobs language library lifehacks linux list literature MAC magazine maps marketing math media microsoft mobile money movies mp3 music network news online opensource osx photo photography photos photoshop php politics portfolio productivity programming python rails reading recipes reference research resources rss ruby rubygems science search secondlife security seo shopping social software statistics tech technology tips tool tools tthread travel tutorial tutorials tv ubuntu usability video web web2.0 webdesign webdev wiki windows wordpress work writing youtube

del.icio.us | about | blog | terms of service | privacy policy | copyright policy | support

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 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.