

May 15, 2022

AUTOPSY: DIGITAL FORENSICS



Group Project Members:

- Wesley Hancock
- Fabian Quirox
- Kailynn Coronel
- Emiliiana Merida

» Documentation By: Giggling Fairies

TABLE OF CONTENTS

1.0 Purpose

2.0 Audience

3.0 Background

4.0 Installation & Opening Case

 4.1 Creating a Case

 4.2 Adding a Data Source

 4.3 Ingest Modules

5.0 Tools

 5.1 Images/Videos

 5.2 Communication Visualization

 5.3 Geolocation

 5.4 Timeline

 5.5 Discovery

 5.6 Generate Report

 5.7 Configure Ingest

6.0 Lab

 6.1 Background on Case

 6.2 Resources Needed

 6.3 Question 1

 6.4 Question 2

 6.5 Question 3

 6.6 Question 4

 6.7 Question 5

 6.8 Question 6

7.0 Acknowledgements

1.0 PURPOSE

The reason for this documentation is to offer a guideline for users who would like to learn the background history of Autopsy and how to utilize the tool. It additionally provides a walk through that covers a hands-on lab activity.

2.0 AUDIENCE

The targeted audience for this technical report is;

- Users or customers interested in Autopsy/Forensics
- College Students
- Novice & Experts

3.0 BACKGROUND

Autopsy® is a free digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card.

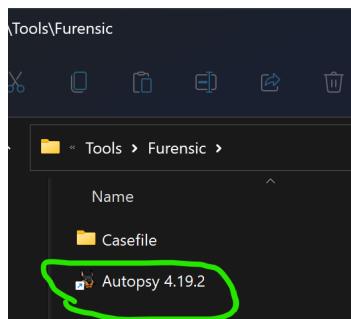
4.0 INSTALLATION & OPENING CASE

To install Autopsy, perform the following steps.

1. Download Autopsy from the website:
 - a. <http://sleuthkit.org/autopsy/download.php>
2. Run the Autopsy msi file
3. If Windows prompts with User Account Control, click Yes
4. Click through the dialog boxes until you click a button that says Finish
5. Autopsy should now be fully installed

4.1. Creating a Case

1. Open Autopsy



2. Select New Case



3. Name Case File in Case Name

New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name:

Base Directory: Browse

Case Type: Single-User Multi-User

Case data will be stored in the following directory:

< Back Next > Finish Cancel Help

4. Select Browse to Specify a preferred directory to store Case File > Next

New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name:

Base Directory: Browse

Case Type: Single-User Multi-User

Case data will be stored in the following directory:

< Back Next > Finish Cancel Help

New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name:

Base Directory: Browse

Case Type: Single-User Multi-User

Case data will be stored in the following directory:

< Back Next > Finish Cancel Help

5. (Optional) Input optional information, Identify or Specify Case Number, Examiner Point of Contact > Finish

New Case Information

Steps

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

Optional Information

Case

Number: 001

Examiner

Name: Your Name

Phone: 123-456-789

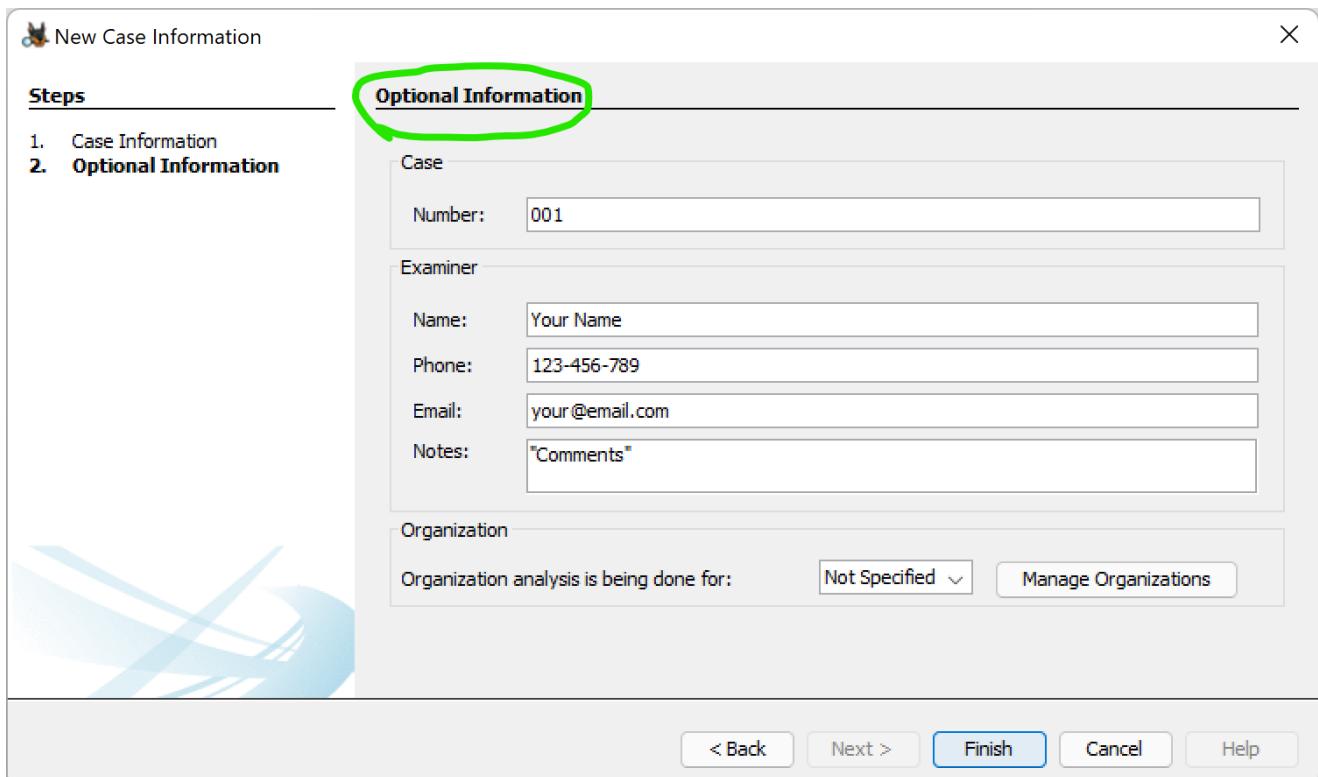
Email: your@email.com

Notes: "Comments"

Organization

Organization analysis is being done for: Not Specified Manage Organizations

< Back Next > **Finish** Cancel Help



4.2 Adding a Data Source

1. Select Host > Generate new host name based on data source name > Next

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

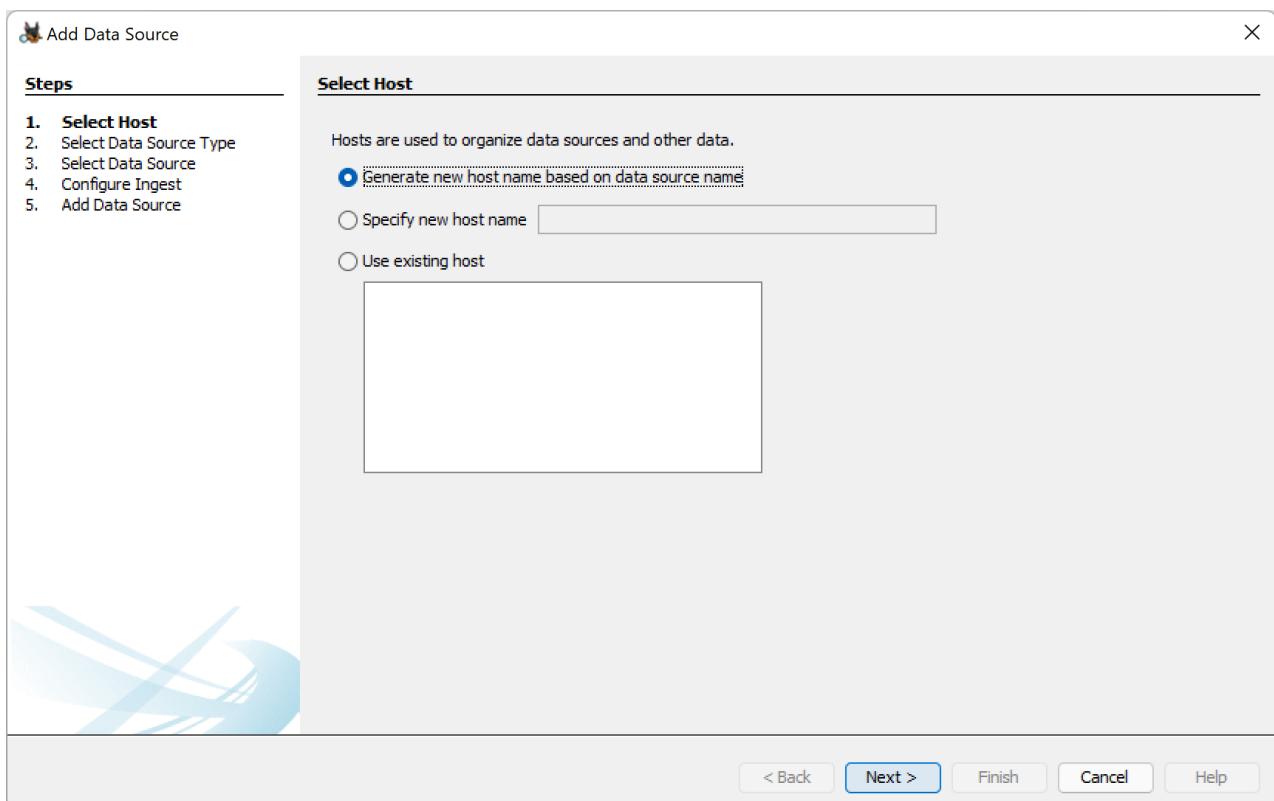
Hosts are used to organize data sources and other data.

Generate new host name based on data source name

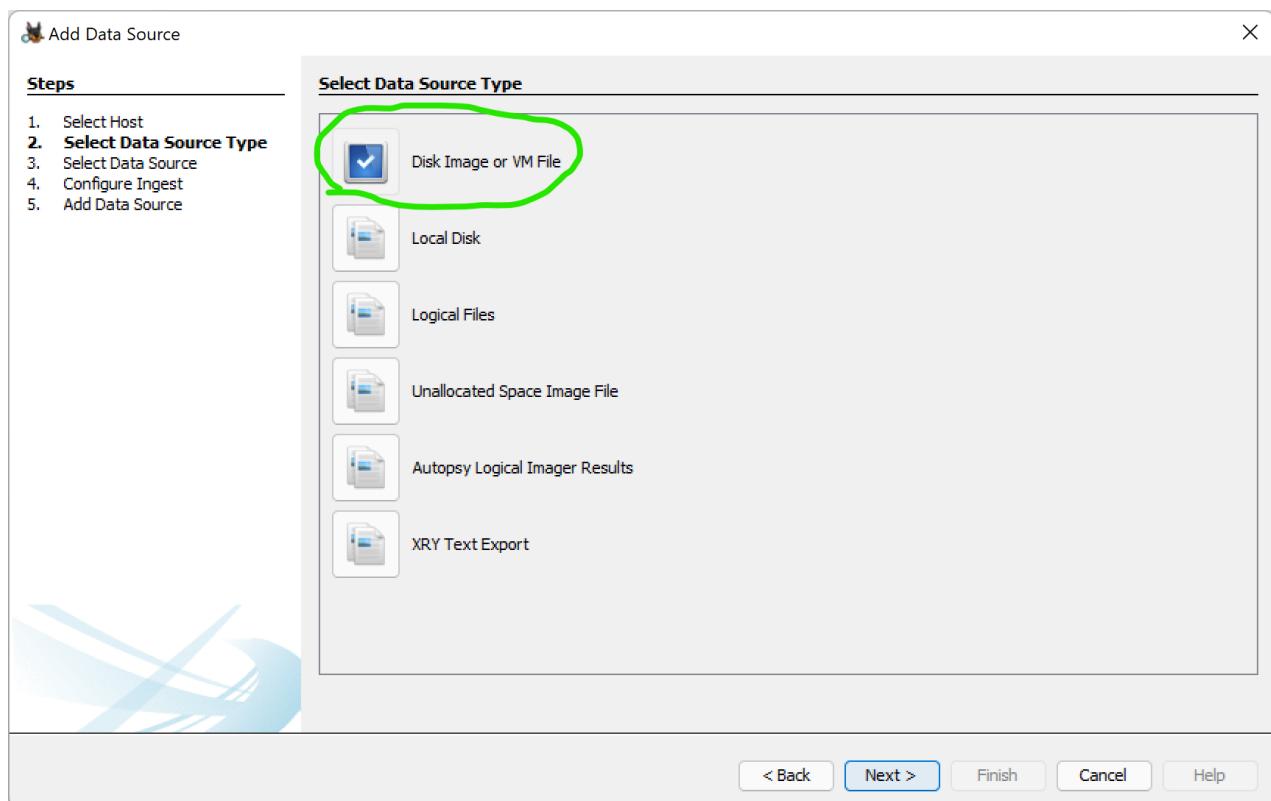
Specify new host name

Use existing host

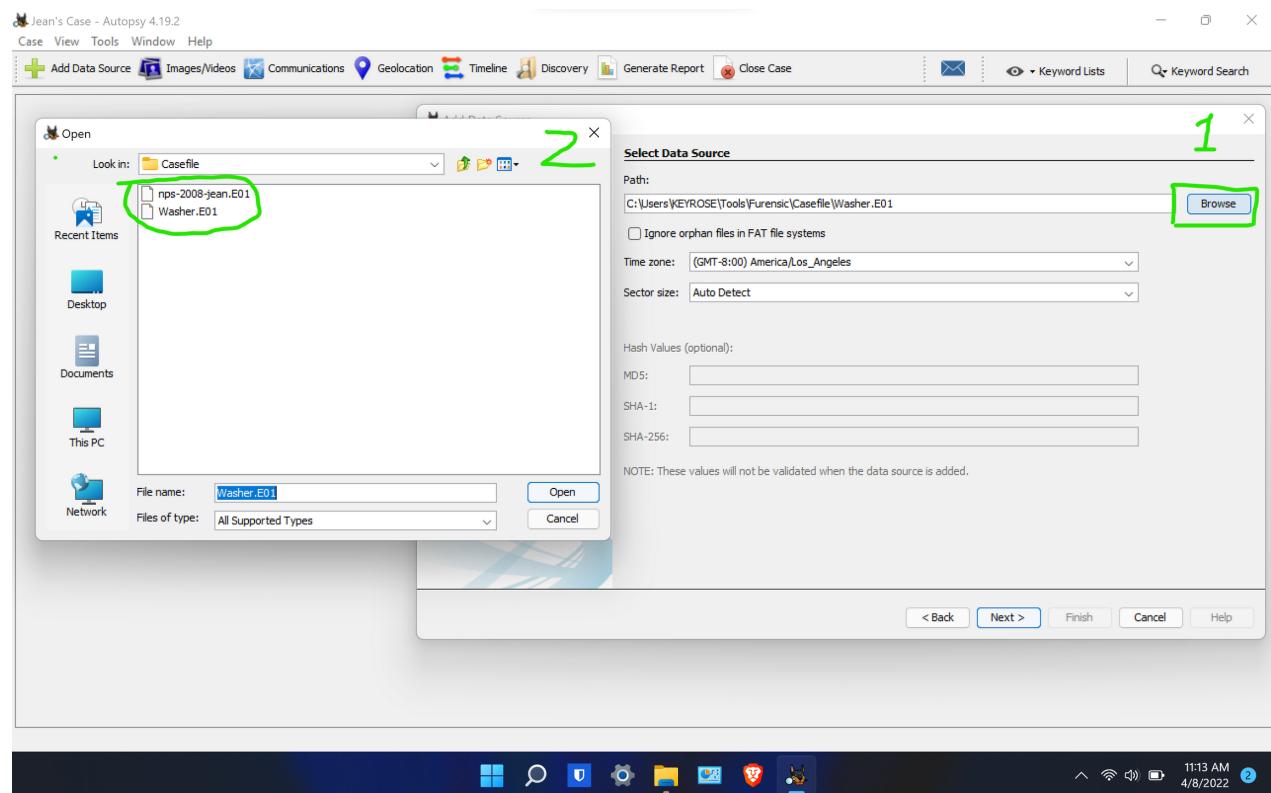
< Back Next > **Finish** Cancel Help



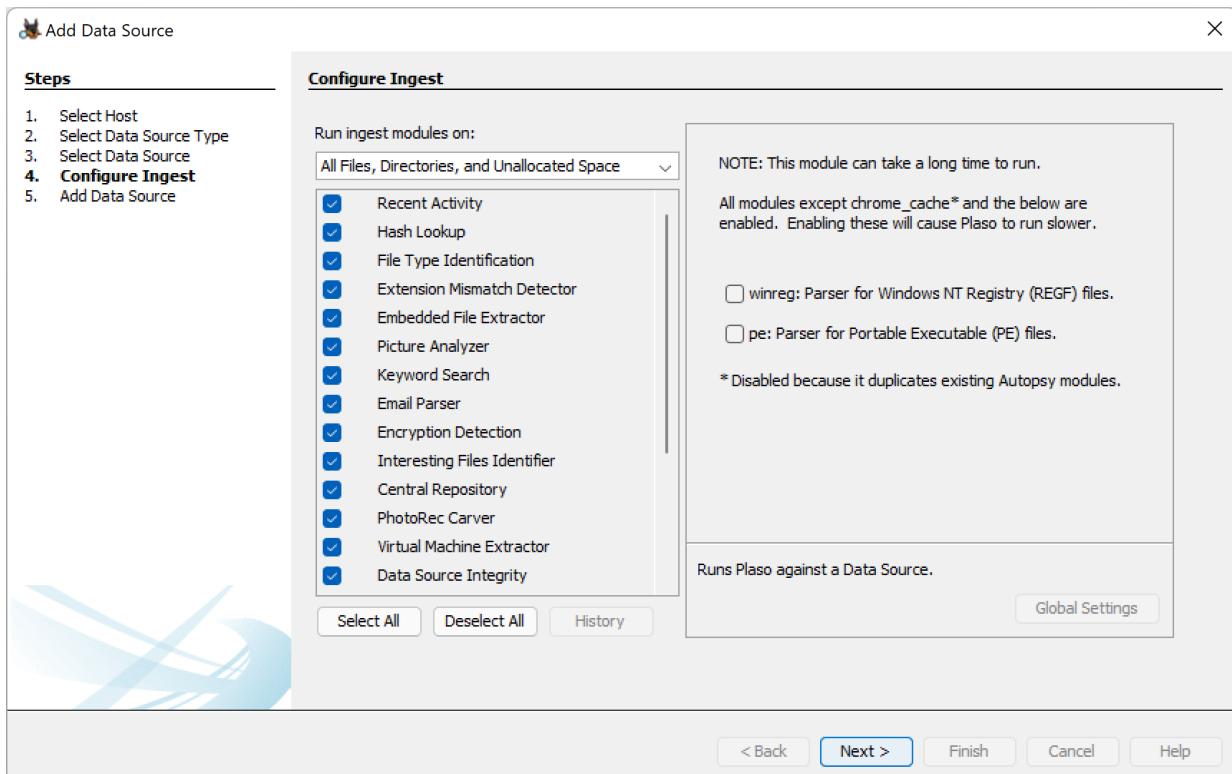
2. Select Data Source Type > Disk Image > Next



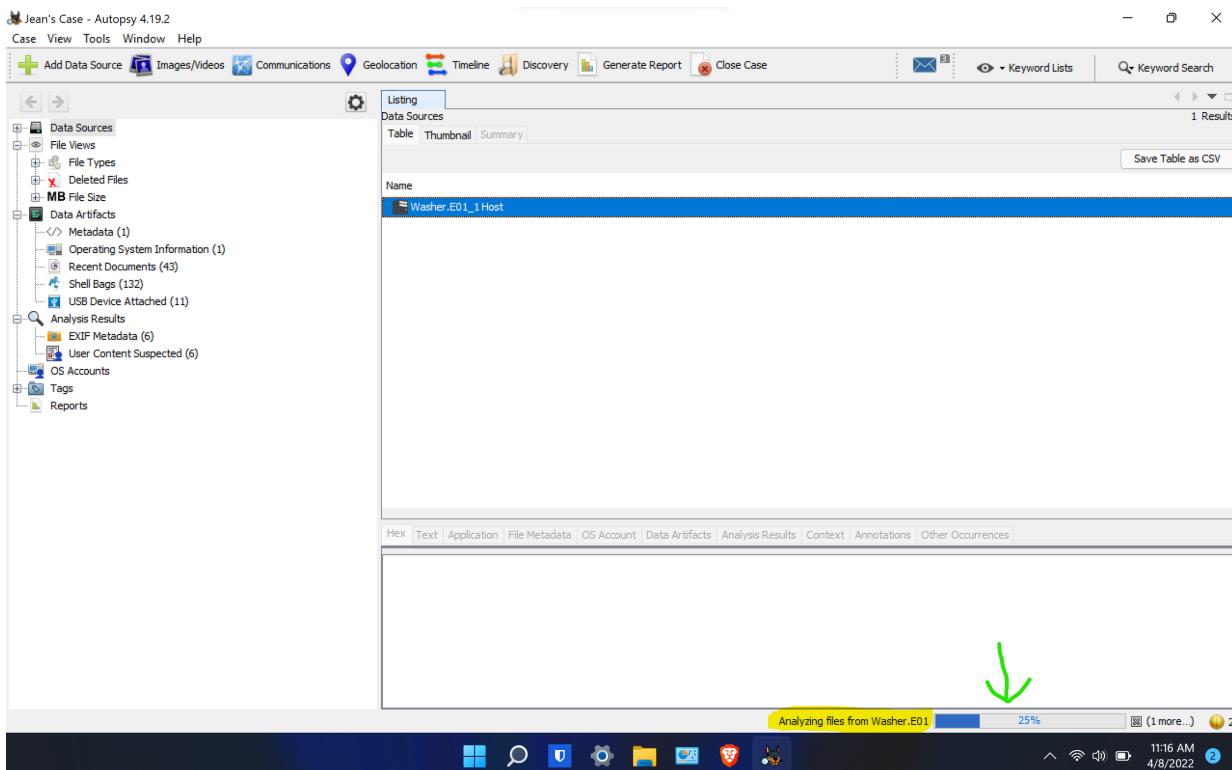
3. Select Data Source > Browse > Location of .E01 File > Next



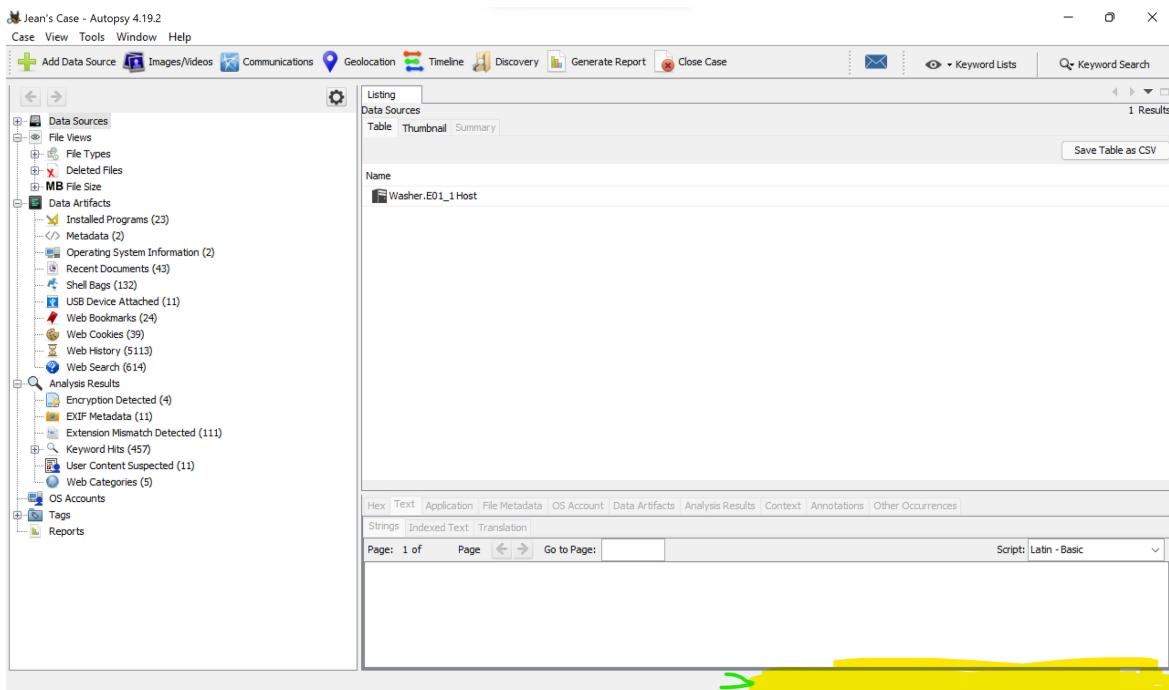
4. Configure Ingest > Next > Finish>



5. Autopsy image analysis may take some time to complete(depending on size of File)

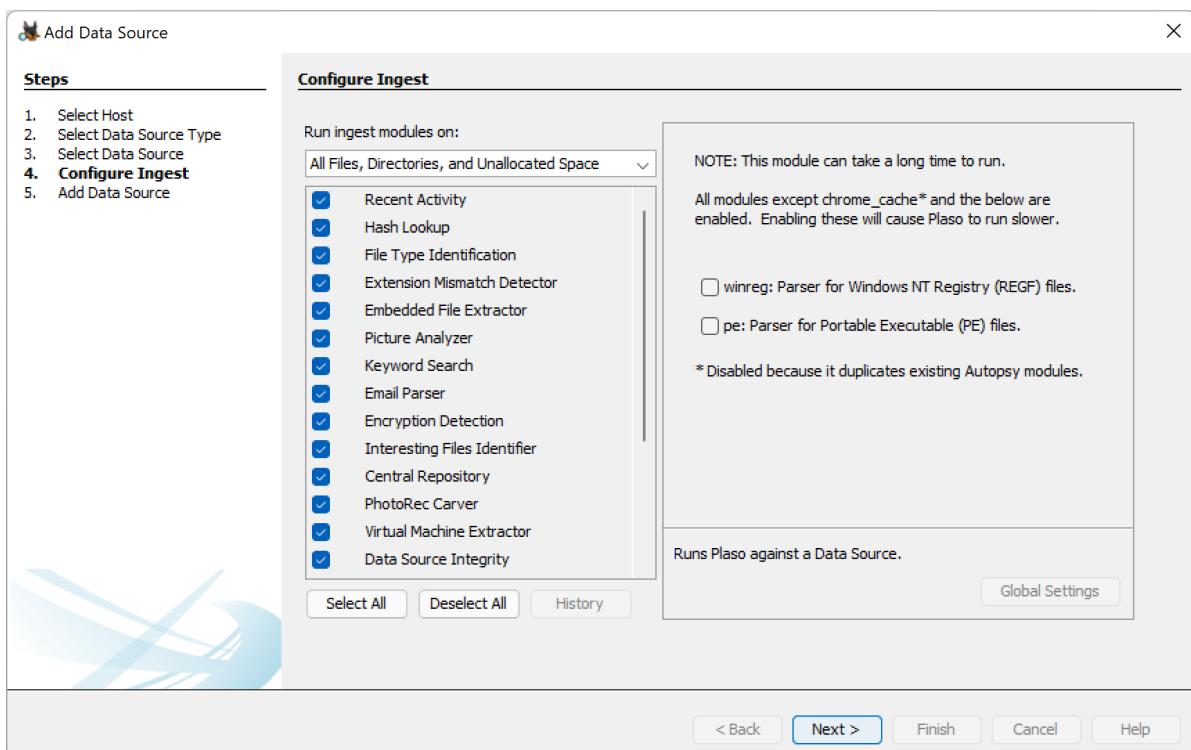


6. Completion of File analysis will remove loading bar



4.3 Ingest Modules

Here you will be presented with an interface to configure the ingest modules. From here you can choose to enable or disable each module and some modules will have further configuration settings. You may leave as default.



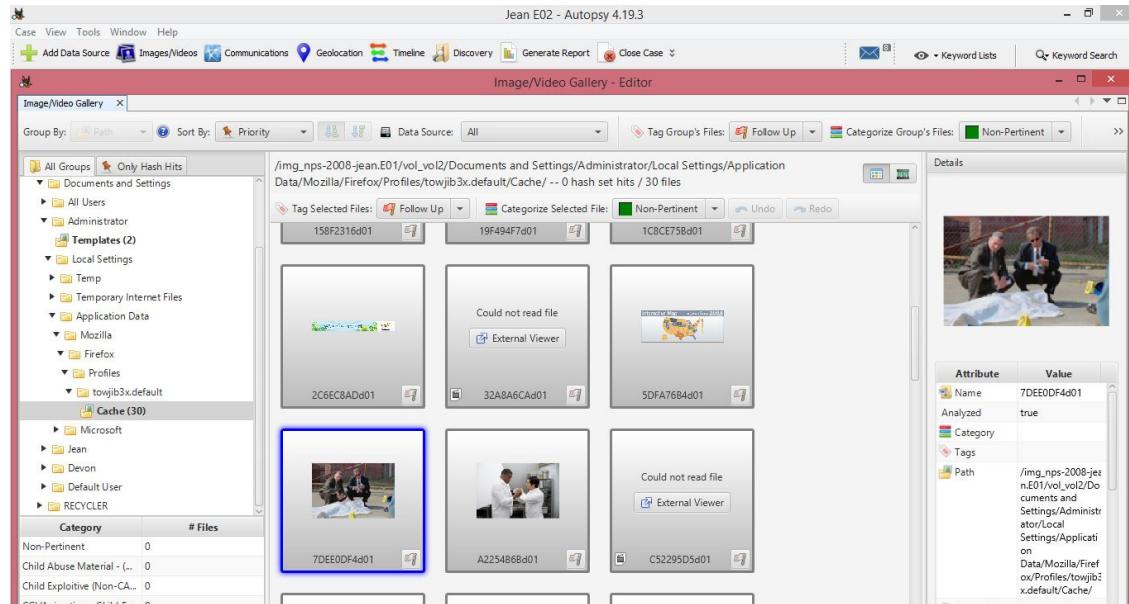
5.0 TOOLS

5.1 Images/Videos

The new image gallery feature has been designed specifically with child-exploitation cases in mind, but can be used for a variety of other investigation types that involve images and videos. It offers the following features beyond the traditional long list of thumbnails that Autopsy and other tools currently provide.

- Groups images by folder (and other attributes) to help the examiner break the large set of images into smaller groups and to help focus on areas with images of interest.

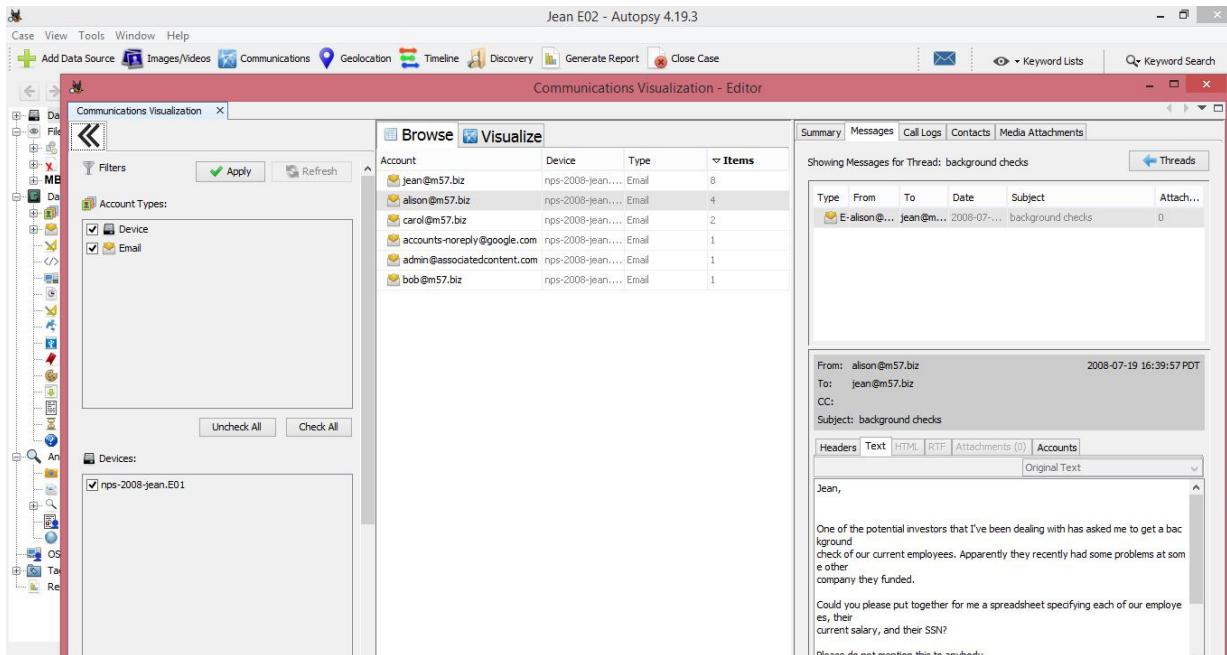
Allows the examiner to start viewing images immediately upon adding them to the case. As images are hashed, they are updated in the interface. You do not need to wait until the entire image is ingested.



5.2 Communication Visualization

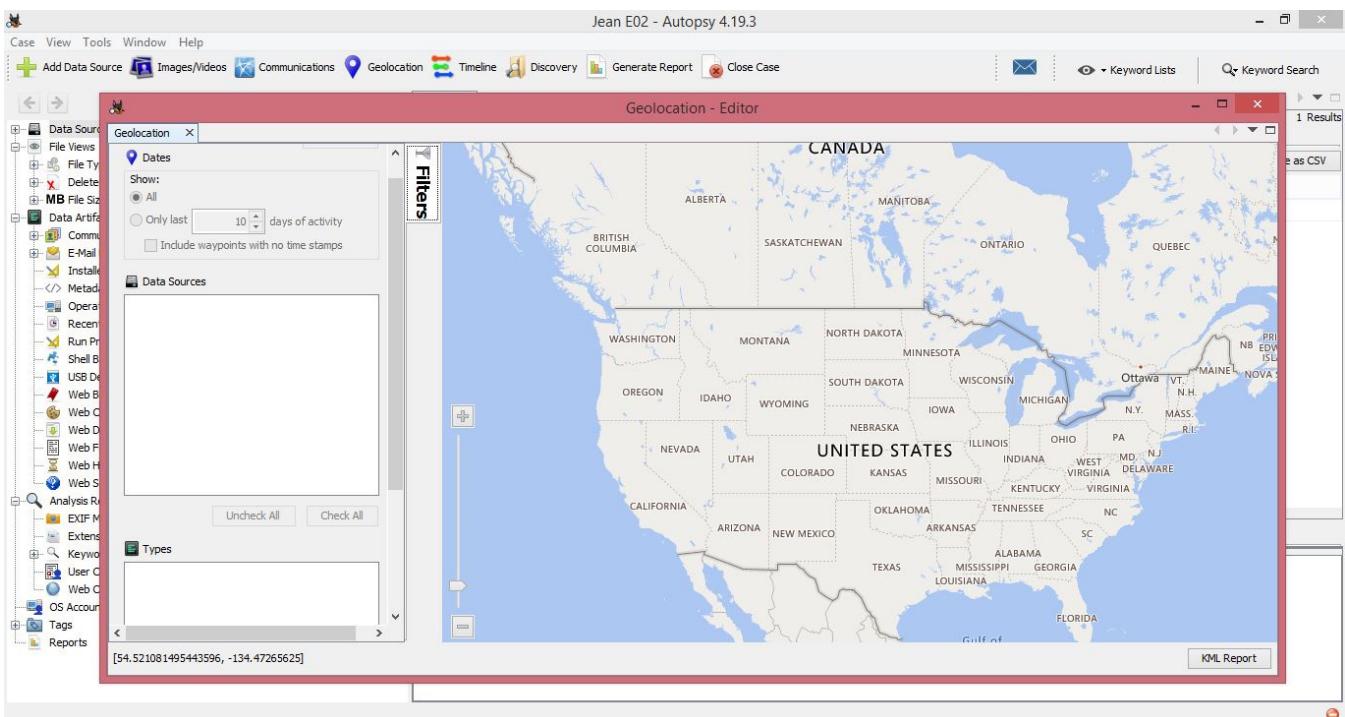
The Communications Visualization Tool gives a consolidated view of all communication events for the case. This allows an analyst to quickly view communications data such as:

- The most commonly used accounts
- Communications within a specific time frame



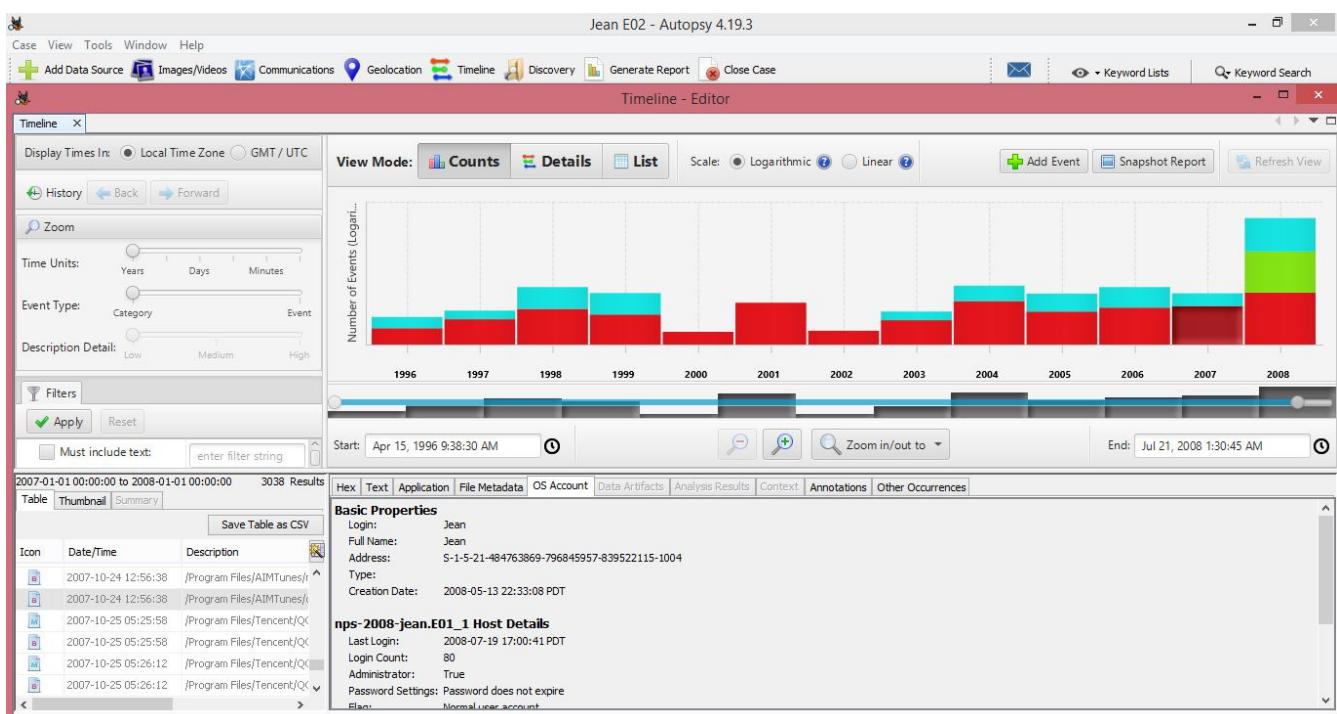
5.3 Geolocation

The Geolocation window shows artifacts that have longitude and latitude attributes as waypoints on a map. In the field, when access to online map tile servers may not be available, the Geolocation window provides support for offline map tile data sources.



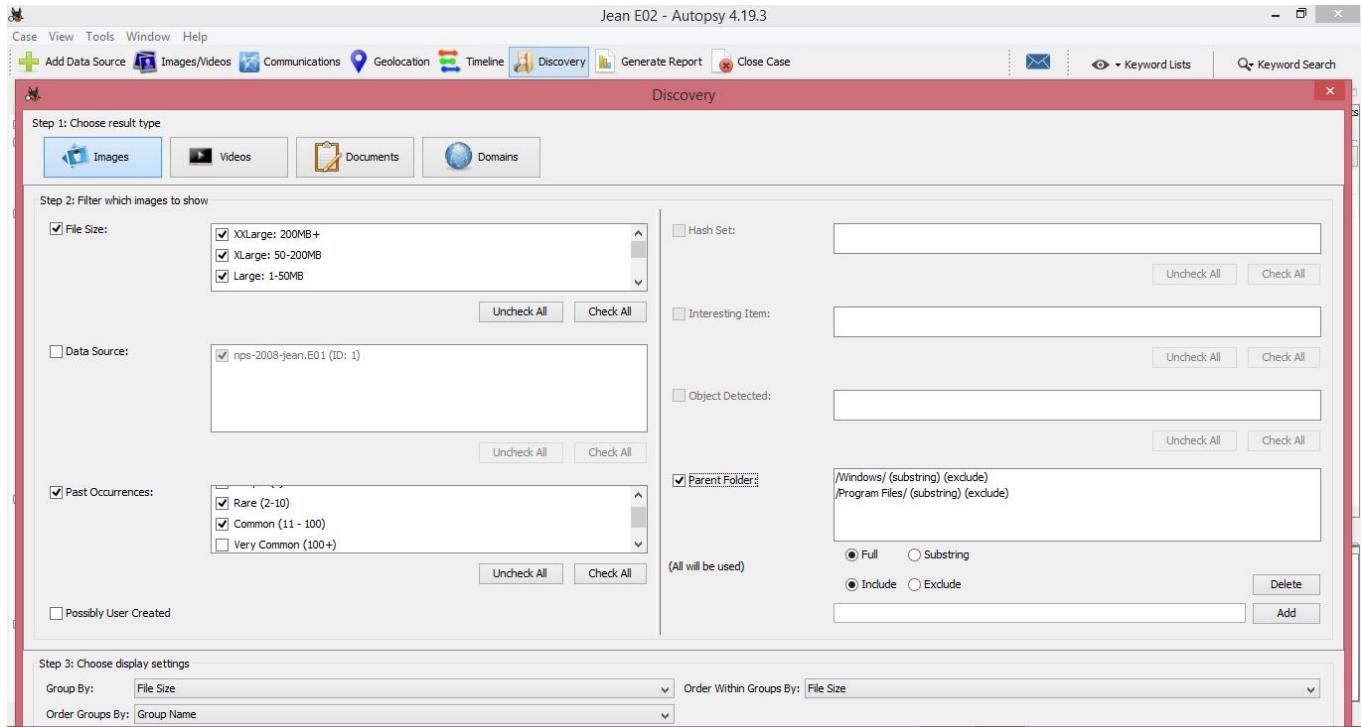
5.4 Timeline

The timeline tool is organized around events. An Event has a timestamp, a type, and a description. Note: all Events are discrete, but might be grouped together to form clusters with a duration in the Details View depending on the level of Description that is enabled in the UI.



5.5 Discovery

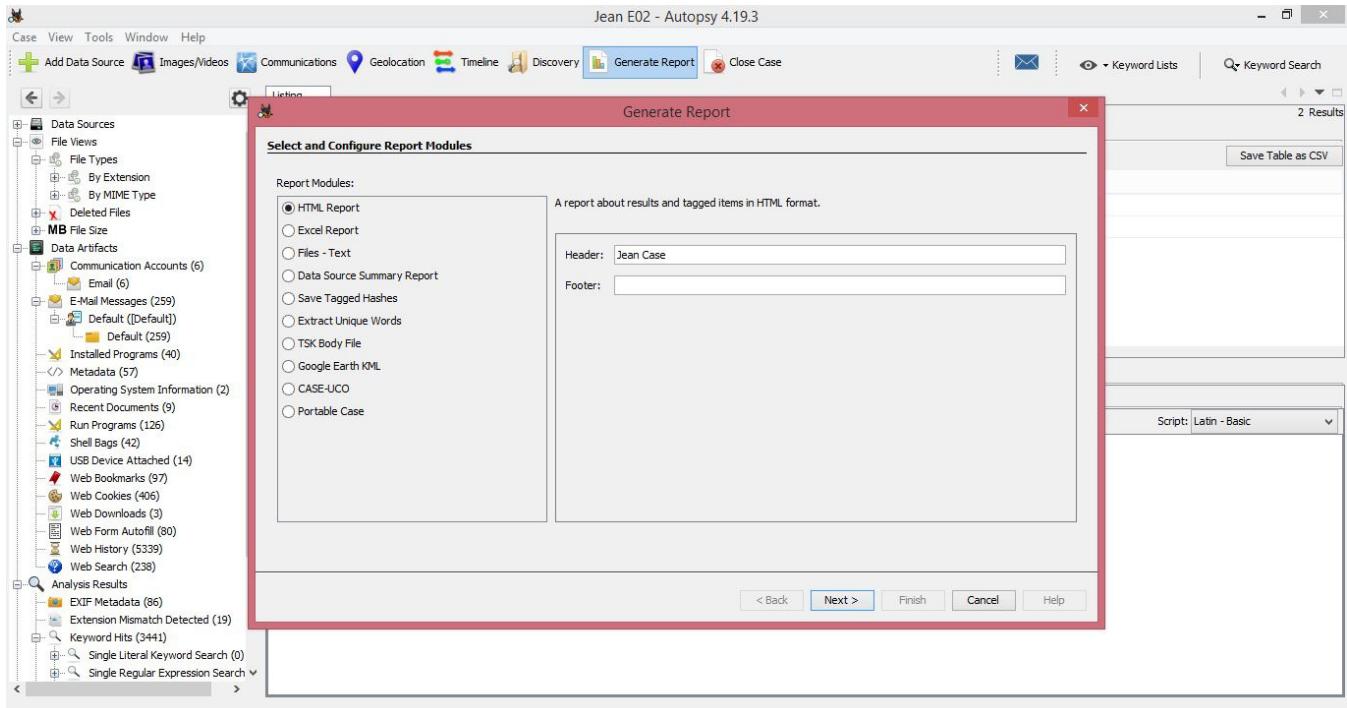
The discovery tool shows images, videos, documents, or domains that match a set of filters configured by the user. You can choose how to group and order your results in order to see the most relevant data first.

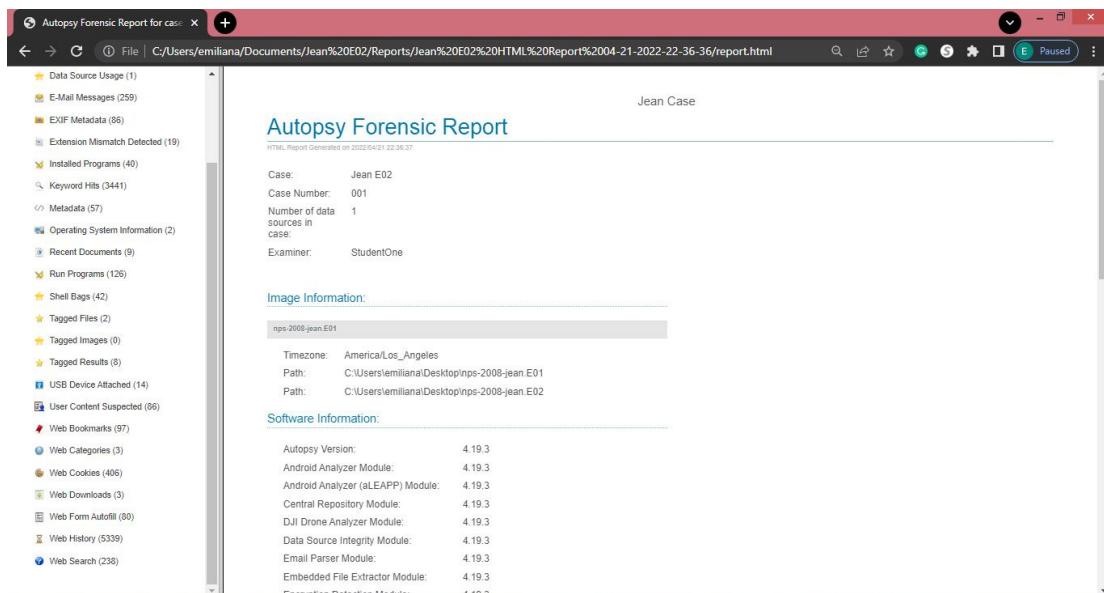
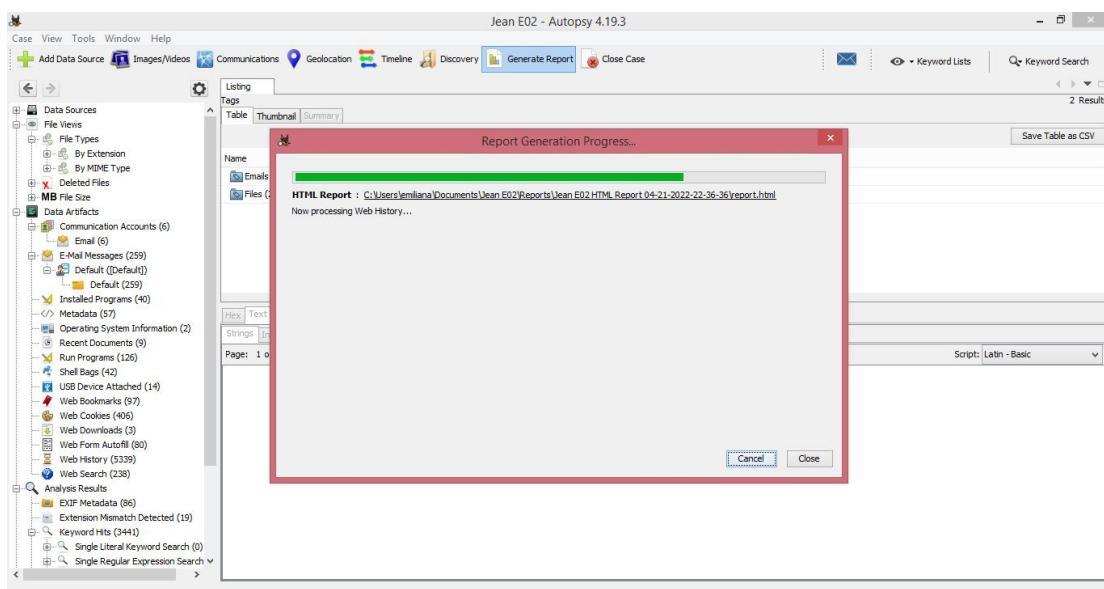
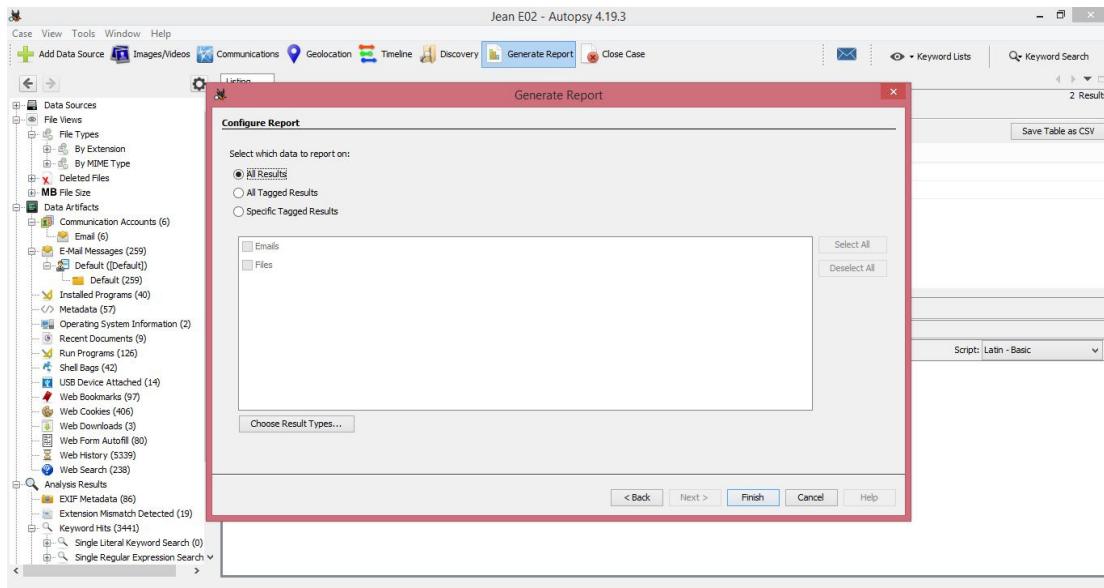


5.6 Generate Report

The report modules allow the user to extract key information from a case in a variety of formats. This includes making an HTML or Excel report containing all the extracted content, keyword hits, etc. from a case, or creating a KML file out of any coordinates found to load into software like Google Earth.

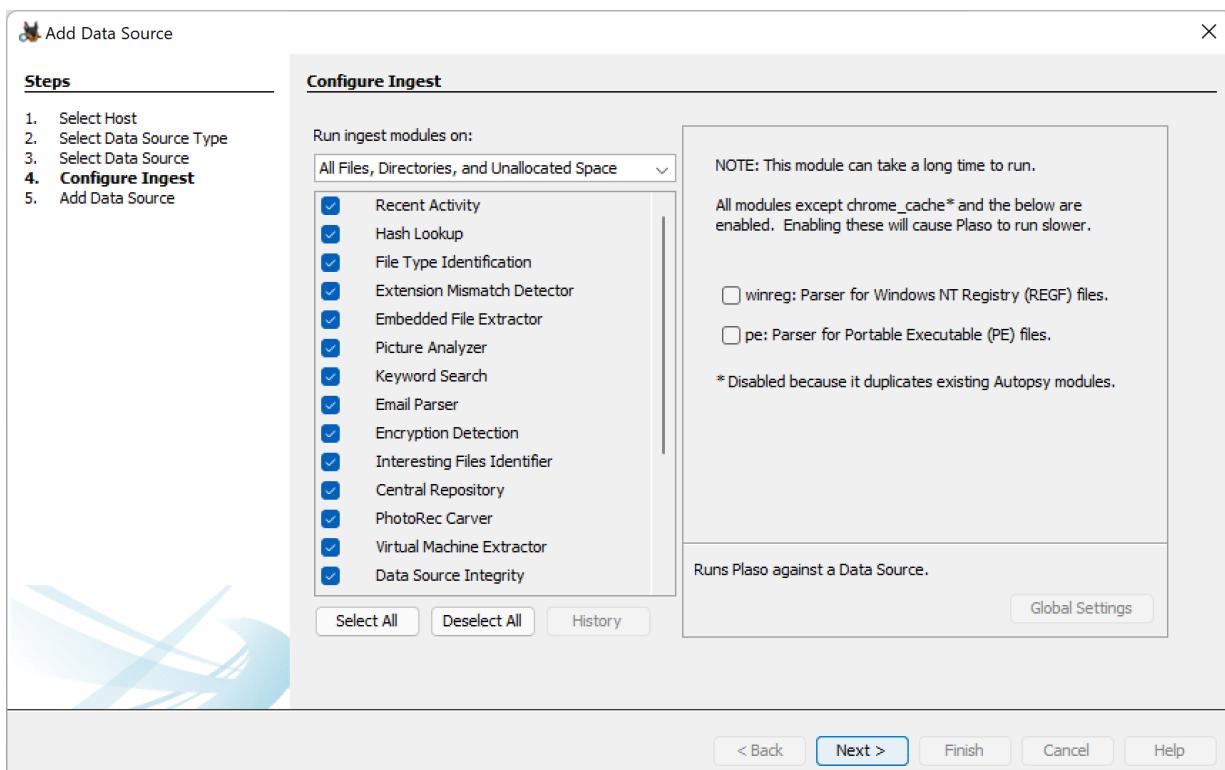
- Bookmarking your evidence you find beforehand will help you create your report.





5.7 Configure Ingest

- **Recent Activity** - looks through web browsing activity, recent documents, recently installed programs, recent activity from a system
- **Hash Lookup** - can set hash databases of known good files and known bad files
- **File Type Identification** - matches file types based on binary signatures
- **Extension Mismatch Detector** - uses the results from the File Type Identification and flags files that have an extension not traditionally associated with the file's detected type.
- **Embedded File Extractor** - It extracts embedded files such as .zip, .rar, etc. and uses the derived file for analysis. Another example could be a PNG image saved inside a doc to make it appear as a document and thus hide crucial information.
- **Picture Analyzer** - looking at images and extracting
- **Keyword Search** - Search for a particular keyword/pattern in the data source
- **Email Parser** - If the disk holds any form of email database, for example, pst/ost files of outlook then information from these files can be extracted using an email parser.
- **Encryption Detection** - Detects and identifies encrypted / password-protected files.
- **Interesting File Identifier** - Lets set custom rules regarding the filtering of data. Examiner is notified when results pertaining to these rules are found.
- **Central Repository** - creates a local database that keeps track of files and activities that you've seen in the past cases
- **PhotoRec Carver** - Recover files, photos, etc. from the unallocated space.
- **Virtual Machine Extractor** - Extract and analyze any Virtual machine found on the data source.
- **Data Source Integrity** - Calculates the hash values and stores them in the database in case they aren't already present. Otherwise, it will verify the hash values associated with the database.



6.0 LAB

6.1 Background on Case

Scenario: A document is leaked on the Internet which contains confidential information about M57's employees such as SSN, salaries and positions in the company. This sensitive Excel sheet has mysteriously appeared on a competitor's website. Jean, the CFO, is believed to be involved since she had access to this file. She claims that the president, Alison Smith, asked explicitly for this information. However, Alison denies having asked for it or having received it.

This is a corporate breach of contract, due to not maintaining data integrity and company confidentiality for its Stakeholders/Users.

Facts of the case:

- \$3M in seed funding; now closing \$10M round
- 2 founder/owners
- 10 employees hired first year

Current staff

- President: Alison Smith
- CFO: Jean
- Programmers: Bob, Carole, David, Emmy
- Marketing: Gina, Harris
- BizDev: Indy

Programmers:

- Work out of their houses
- Daily online chat session; Weekly in-person meetings office park

Marketing & BizDev:

- Work out of hotel rooms or Starbucks (mostly on the road)
 - In-person meetings once every two weeks.
 - Most documents are exchanged by email.

Summaries Of Interview

Alison (President):

- I don't know what Jean is talking about.
- I never asked Jean for the spreadsheet.
- I never received the spreadsheet by email.

Jean (CFO):

- Alison asked me to prepare the spreadsheet as part of new funding round.
- Alison asked me to send the spreadsheet to her by email.
- That's all I know.

6.2 Resources Needed

Down below is a list of resources you will need:

- Autopsy : <https://www.autopsy.com/>
- Link to Case Image: <https://digitalcorpora.org/corpora/scenarios/m57-jean>

6.3 Question 1

How did the documents get on the competitor's website?

- Select "E-Mail Messages" > Default (Default) > Default (259)
 - Select the email called "This is what I was talking about" > Headers > Delivered to
- Alison got spoofed from an email that Jean sent. It was not Alison sending the email.

Jean E02 - Autopsy 4.19.3

Case View Tools Window Help

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

Listing Default

Table Thumbnail Summary

Source Name S C O E-Mail From Subject Date Received Message (Plaintext)

outlook.pst AlisonM57 business plan 2008-07-06 12:25:09 PDT Say, Jean, how is the business plan coming along? I know...

outlook.pst AlisonM57 RE: This is what I was talking about 2008-07-06 12:25:11 PDT EMAIL THIS Email Dean, Please do not send me links like i...

outlook.pst AlisonM57 By the way... 2008-07-06 12:25:14 PDT EMAIL THIS Email http://www.cnn.com/2008/LIVING/wor...

outlook.pst AlisonM57 RE: This is what I was talking about 2008-07-06 12:28:48 PDT Jean, Please respond to my previous email.

outlook.pst Claude Mentre Claude Mentre <claudem@intra.hk> 2008-07-06 12:28:48 PDT

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

Result: 29 of 264 Result < >

E-Mail Messages

From: AlisonM57 To: Jean@m57.biz Cc: Subject: RE: this is what I was talking about

Headers Text HTML RTF Attachments (0) Accounts

-----HEADERS-----

Return-Path: <alison@m57.biz>
X-Original-To: jeann@m57.biz
Delivered-To: x2789957@spunkymail-a3.g.dreamhost.com
Received: from jeann19f038a3 (sub2-75-208-65.mywzv.com [75.208.65.32])
for alisonm57@m57.biz (Sun, 6 Jul 2008 12:25:11 -0700 (PDT))
From: <AlisonM57> <alison@m57.biz>
To: <Jean@m57.biz>
Subject: RE: this is what I was talking about
Date: Sun, 6 Jul 2008 20:25:11 +1000
Message-ID: <>IDELFBPPBFEBIMNAAEACBAAA.alison@m57.biz>
MIME-Version: 1.0

6.4 Question 2

When did Jean create this spreadsheet?

- Select "Views" > File Types > By Extension > Documents > Office (32)
- Select the excel sheet "m57biz.xls"

Date Created: 7/19/2008 6:28:03 PM

Jean E02 - Autopsy 4.19.3

Case View Tools Window Help

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

Listing Office

Table Thumbnail Summary

Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags(Meta) Known

excel.xls 2 2001-08-23 05:00:00 PDT 2008-07-11 20:02:48 PDT 2008-07-11 20:02:48 PDT 5632 Allocated Allocated unknown

m57biz.xls 1 2008-07-19 18:28:03 PDT 2008-07-19 18:28:03 PDT 2008-07-19 18:28:03 PDT 2008-07-19 18:28:03 PDT 291840 Allocated Allocated unknown

excel.xls 2 2001-08-23 05:00:00 PDT 2008-07-05 23:11:22 PDT 2008-07-05 23:11:22 PDT 5632 Allocated Allocated unknown

XL8GALRY.XLS 0 1999-02-10 00:42:18 PST 2008-07-06 00:21:12 PDT 1999-02-10 00:42:18 PST 151552 Allocated Allocated unknown

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

Metadata

Name: /img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Desktop/m57biz.xls
Type: File System
MIME Type: application/vnd.ms-excel
Size: 291840
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2008-07-19 18:28:03 PDT
Accessed: 2008-07-19 18:28:03 PDT
Created: 2008-07-19 18:28:03 PDT
Changed: 2008-07-19 18:28:04 PDT
MD5: e23a4eb7f25cf5f3e889cdca8b26a153
SHA-256: 344565f714dd8d8d23c2742d5c3f5f582ecb042bc1c4d3042b88203863779f
Hash Lookup Results: UNKNOWN
Internal ID: 4014

From The Sleuth Kit stat Tool:

MFT Entry Header Values:
Entry: 32712 Sequence: 2
Allocation Reference Number: 172434688

6.5 Question 3

Who else from the company is involved?

- Select “Communications Visualization” > Browse > Messages

OR

- Select “E-Mail Messages” > Default (Default) > Default (259)
- Alison - President
- Jean - CFO
- Alex - Fake
- Simsong - Fake
- Tuck George - Main person who spoofed

The screenshot shows the Communications Visualization - Editor application. On the left, there's a sidebar with filters, account types (Device, Email), and devices (nps-2008-jean.E01). The main area has tabs for 'Browse' and 'Visualize'. Under 'Browse', a table lists accounts: jeann@m57.biz (8 items), alison@m57.biz (4 items), carol@m57.biz (2 items), accounts-noreply@google.c (1 item), admin@associatedcontent.c (1 item), and bob@m57.biz (1 item). A specific message is selected in the list: "E-Mailson@m5... jeann@m5... 2008-07-19 ... Please send me the information now". The right panel shows the message details: From: alison@m57.biz, To: jeann@m57.biz, Subject: Please send me the information now. The message body contains a reply-to header and a message-id. The message content pane shows hex and text representations of the message.

The screenshot shows the Hex Editor interface. The left sidebar includes Data Sources (nps-2008-jean.E01_1 Host), File Views, Deleted Files, MB File Size, Data Artifacts (Communication Accounts (3028), E-Mail Messages (259), Default (Default) (259)), Installed Programs (40), Metadata (58), Operating System Information (2), Recent Documents (9), Run Programs (126), Shell Bags (42), USB Device Attached (14), Web Bookmarks (97), Web Cookies (406), Web Downloads (3), Web Form Autofill (80), Web History (5339), and Web Search (238). The right panel shows a table of messages from Jean User to various recipients. A specific message is highlighted: "outlook.pst" (Subject: which email address are you using?). Below the table is a detailed view of the message, showing the message body: "From: Jean User", "To: alison@m57.biz", "Subject: which email address are you using?", and the message content pane with headers and text.

Screenshot of a digital forensics tool interface showing a file analysis session.

Left Panel (File Explorer):

- Data Sources: nps-2008-jean.E01_1 Host
 - vol1 (Unallocated: 0-62)
 - vol2 (NTFS /extFAT (0x07): 63-20948760-20971519)
 - vol3 (Unallocated: 20948760-20971519)
- File Views
- File Types
- Deleted Files
- MB File Size
- Data Artifacts
- Communication Accounts (3028)
- E-Mail Messages (259)
 - Default [Default]
 - Default (259)
- Installed Programs (40)
- Metadata (58)
- Operating System Information (2)
- Recent Documents (9)
- Run Programs (126)
- Shell Bags (42)
- USB Device Attached (14)
- Web Bookmarks (97)
- Web Cookies (406)
- Web Downloads (3)
- Web Form Autofill (80)
- Web History (5339)
- Web Search (238)

Analysis Results

- EXIF Metadata (86)
- Extension Mismatch Detected (20)
- Keyword Hits (55940)
- User Content Suspected (86)
- Web Categories (3)

OS Accounts

Tags

Reports

6.6 Question 4

What does the timeline look like?

- Select “Timeline” > List
- Or
- Select “Views” > File Types > By Extension > Documents > Office (32)

Screenshot of a digital forensics tool interface showing a timeline analysis session.

Left Panel (Timeline Filters):

- Display Times In: Local Time Zone (selected) / GMT / UTC
- History: Back, Forward
- Filters: Must include text, Must be tagged, Must have hash hit, Limit data sources to, Limit file types to, Limit event types to (File System, Web Activity, Other), Hidden Descriptions
- Enter filter string: enter filter string

Right Panel (Timeline View):

Timeline - Editor

View Mode: Counts, Details, List (selected)

81,530 events

Date/Time	Event Type	Description	Tagged	Hash Hit
1997-07-18 17:37:00	_BM	/Program Files/Common Files/Microsoft Shared/Gpflit/MS.BMP		
1997-07-18 17:37:00	_BM	/Program Files/Common Files/Microsoft Shared/Gpflit/MS.GIF		
1997-07-18 17:37:00	_BM	/Program Files/Common Files/Microsoft Shared/Gpflit/MS.EPS		
1997-07-18 17:37:00	_BM	/Program Files/Common Files/Microsoft Shared/Gpflit/MS.TIF		
1997-08-04 04:13:42	_BM	/Program Files/Microsoft Office/SELREG.DLL		
1997-10-21 22:39:43	Document Created	Document Created : ;		
1997-12-17 03:39:48	_BM	/Program Files/Microsoft Office/Office/WAVTOASF.EXE		
1998-01-08 07:26:22	_BM	/WINDOWS/Fonts/OUTLOOK.TTF		
1998-01-25 06:34:30	_BM	/Program Files/Common Files/System/Map/1033/NT/SCANPST.HLP		
1998-02-04 04:01:06	_BM	/System Volume Information/_restore/72FA17C4 .. 9-FF0-8037-5773EBACA0FD/RP12/A0003949.rbf		

Start: Apr 15, 1996 9:38:30 AM | Jump By: Year, Month, Day, Hour, Minute | End: Jul 21, 2008 1:30:45 AM

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

0° C 400% ⌂ Reset Tags Menu



6.7 Question 5

Who reached out to Jean too ask if there social security # was posted on the internet? --> Bob

- Select “Communications Visualizations” > bob@m57.biz > “Messages”

The screenshot shows the 'Communications Visualization - Editor' window. On the left, there are filters for 'Account Types' (Device, Email) and 'Devices' (nps-2008-jean.E01). The main area displays a list of accounts with their device and type. A message thread for 'Hi Jean' is selected. The message details show it's from bob@m57.biz to jean@m57.biz on 2008-07-20 at 16:53:19 PDT. The message body contains:

From: bob@m57.biz
To: jean@m57.biz
CC:
Subject: Hi Jean
Headers | Text | HTML | RTF | Attachments (0) | Accounts
Original Text
Hi, Jean.
This is Bob. I'm one of the programmers working on the project.
Do you know anything about my social security number being posted on the Internet? Somebody just sent me email saying that my name and SSN had been posted. I don't really know what this is about.

6.8 Question 6

Can you list out Bob SSN, Carol salary and Indy position.

- Select “File Types” > “Documents” > “office ” > “m57biz.xls”

Bob --> 493-46-3329

Carol --> 110,000

Indy --> Outreach

The screenshot shows the 'Jean E02 - Autopsy 4.19.3' interface. The left sidebar shows various data sources and file views, including 'File Types' (By Extension, By MIME Type) and 'Communication Accounts'. The main pane shows a table of files with columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known. There are four files listed: SOLVSAMP.XLS, m57biz.xls, excel4.xls, and excel4.xls. The 'm57biz.xls' file is selected. Below the table, a spreadsheet view of the file contents is shown:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
SOLVSAMP.XLS	0			1999-02-10 00:42:04 PST	2008-07-06 00:21:30 PDT	2008-07-06 00:21:30 PDT	1999-02-10 00:42:04 PST	159232	Allocated	Allocated	unknown
m57biz.xls	1			2008-07-19 18:28:03 PDT	2000-00-00 00:00:00	2000-00-00 00:00:00	2008-07-19 18:28:03 PDT	291840	Allocated	Allocated	unknown
excel4.xls	2			2001-08-23 05:00:00 PDT	2008-05-13 14:30:10 PDT	2008-05-13 14:30:10 PDT	2008-05-13 14:30:10 PDT	1518	Allocated	Allocated	unknown
excel4.xls	2			2001-08-23 05:00:00 PDT	2008-05-13 14:24:10 PDT	2008-05-13 14:24:10 PDT	2008-05-13 14:24:10 PDT	1518	Allocated	Allocated	unknown
excel4.xls	2			2001-08-23 05:00:00 PDT	2008-07-11 20:00:10 PDT	2008-07-11 20:00:10 PDT	2008-07-11 20:00:10 PDT	1518	Allocated	Allocated	unknown

Below the table, the spreadsheet content is displayed:

Sheet1					
M57.biz company					
Name	Position	Salary	SSN (for background check)		
Alison Smith	President	\$140,000	103-44-3134		
Jean Jones	CFO	\$120,000	432-34-6432		
Programmers:					
Bob Blackman	Apps 1	90,000	493-46-3329		
Carol Canfield	Apps 2	110,000	894-33-4560		
Dave Daubert	Q&A	67,000	331-95-1020		
Emmy Arlington	Entry Level	57,000	404-98-4079		
Marketing					
Gina Tangers	Creative 1	80,000	980-97-3311		
Harris Jenkins	G & C	105,000	887-33-5532		
BizDev					
Indy	Counterhitting	240,000	123-45-6789		
Annual Salaries					
Benefits	30%	\$302,700	\$1,009,000		
Total Salaries + Benefits			\$1,311,700		
Monthly burn			\$109,308.33		

ACKNOWLEDGEMENTS

Group Project Members:

- Wesley Hancock
- Fabian Quirox
- Kailynn Coronel
- Emiliana Merida

References

- Sleuthkit.Org Autopsy
- Autopsy User Documentation 4.1
- Sleuthkit.org:/autopsy/docs/user-docs/3.1/image_viewer.html
- Sleuthkit.org : Autopsy User Documentation Communication Visualization Tool
- Sleuthkit.org : Autopsy User Documentation Geolocation
- Sleuthkit.org : Autopsy User Documentation Timeline
- Autopsy User Documentation: Discovery
- Autopsy User Documentation: Reporting
- InfoSec:Forensics investigation of document exfiltration involving spear phishing: The M57 Jean case
- Analysis of Data Source Using Autopsy:
<https://www.geeksforgeeks.org/analysis-of-data-source-using-autopsy/>

