May 15, 2022

AUTOPSY: DIGITAL FORENSICS

Documentation By: Giggling Fairies

Group Project Members:

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

TABLE OF CONTENTS

1.0 Purpose

2.0 Audience

3.0 Background

4.0 Installation & Opening Case

- 4.1 Creating aCase
- 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.

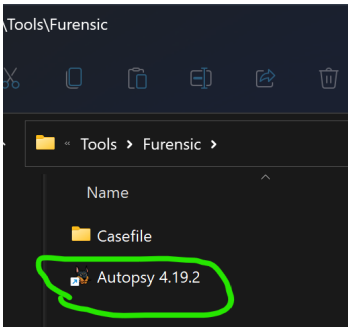
4.0 INSTALLATION & OPENING CASE

To install Autopsy, perform the following steps.

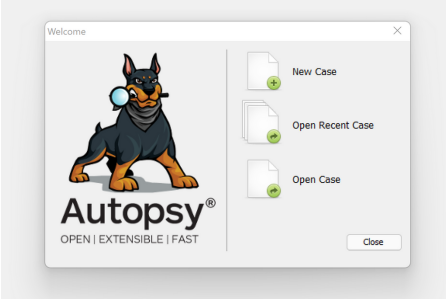
1. Download Autopsy from the website:
    a. http://sleuthkit.org/autopsy/download.php
2. Run the Autopsy msi file
3. If Windows prompts with User Account Control, click Yes
4. Click through the dialog boxes until your click a button that says Finish
5. Autopsy should now be fully installed

4.1. Creating a Case

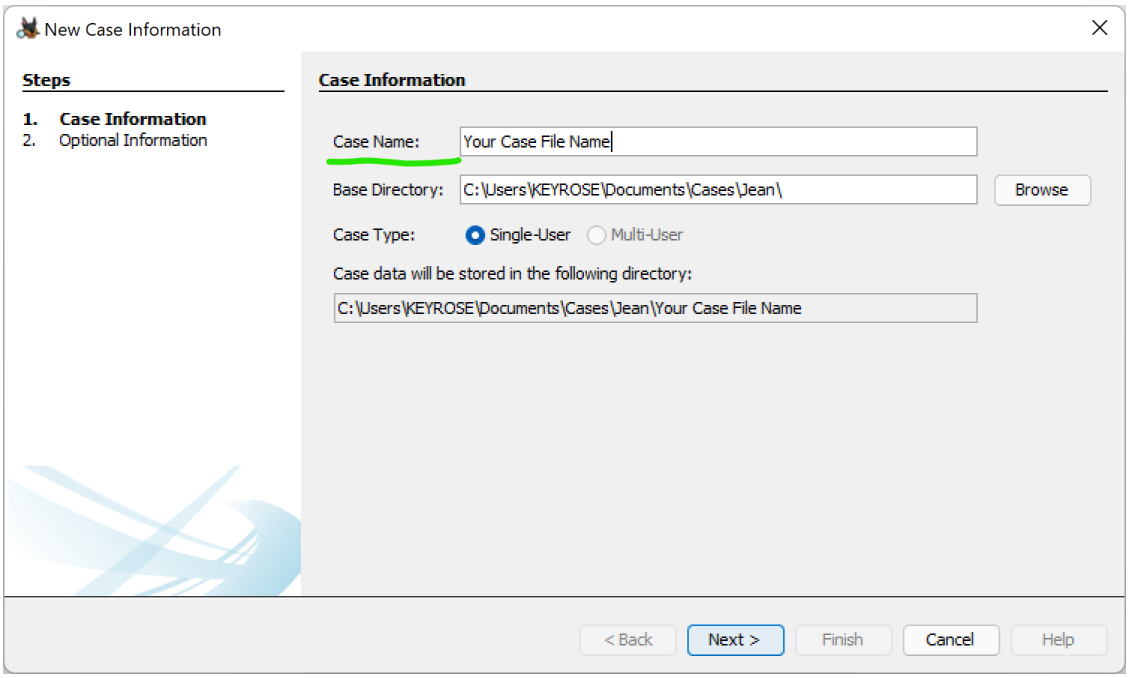
1. Open Autopsy



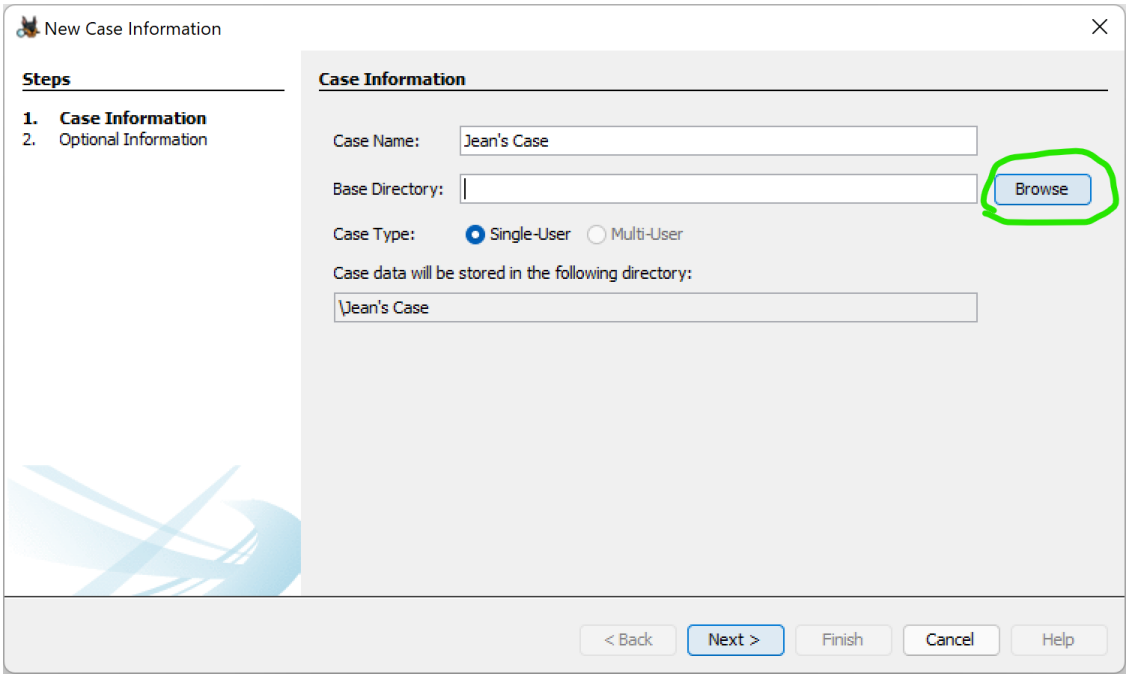
2. Select New Case

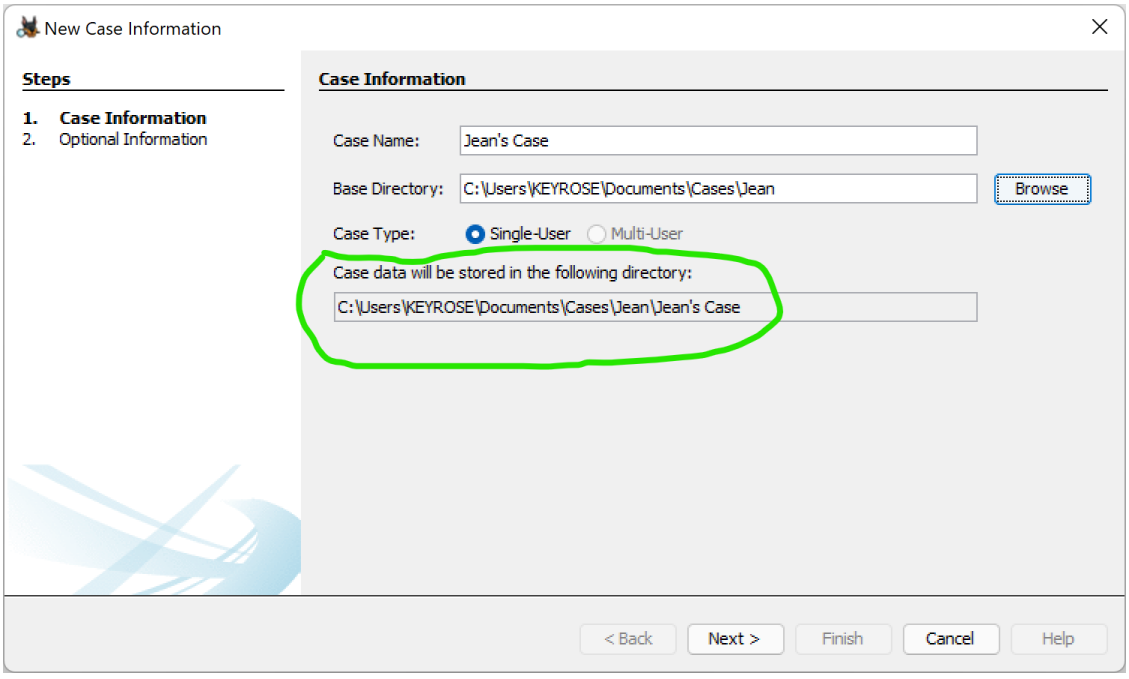


3. Name Case File in Case Name

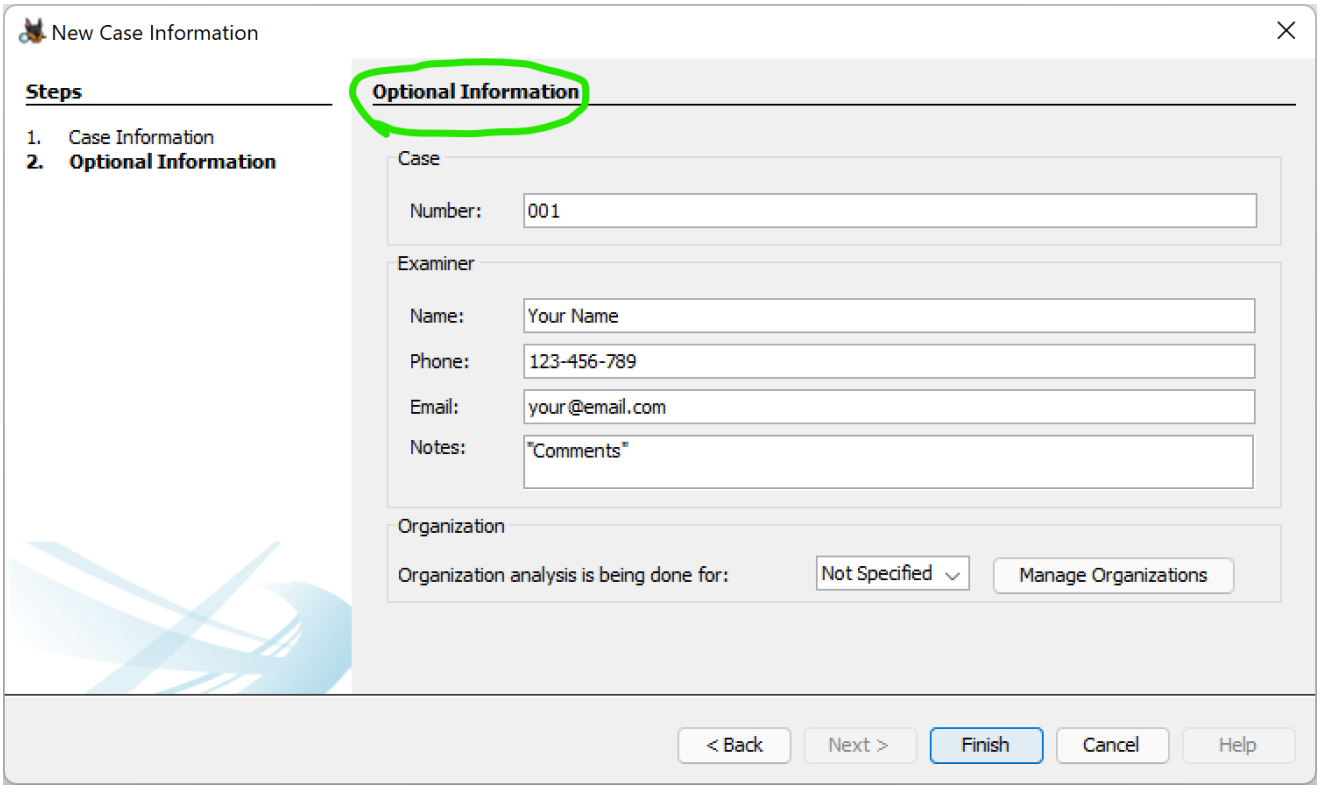


4. Select Browse to Specify a preferred directory to store Case File > Next



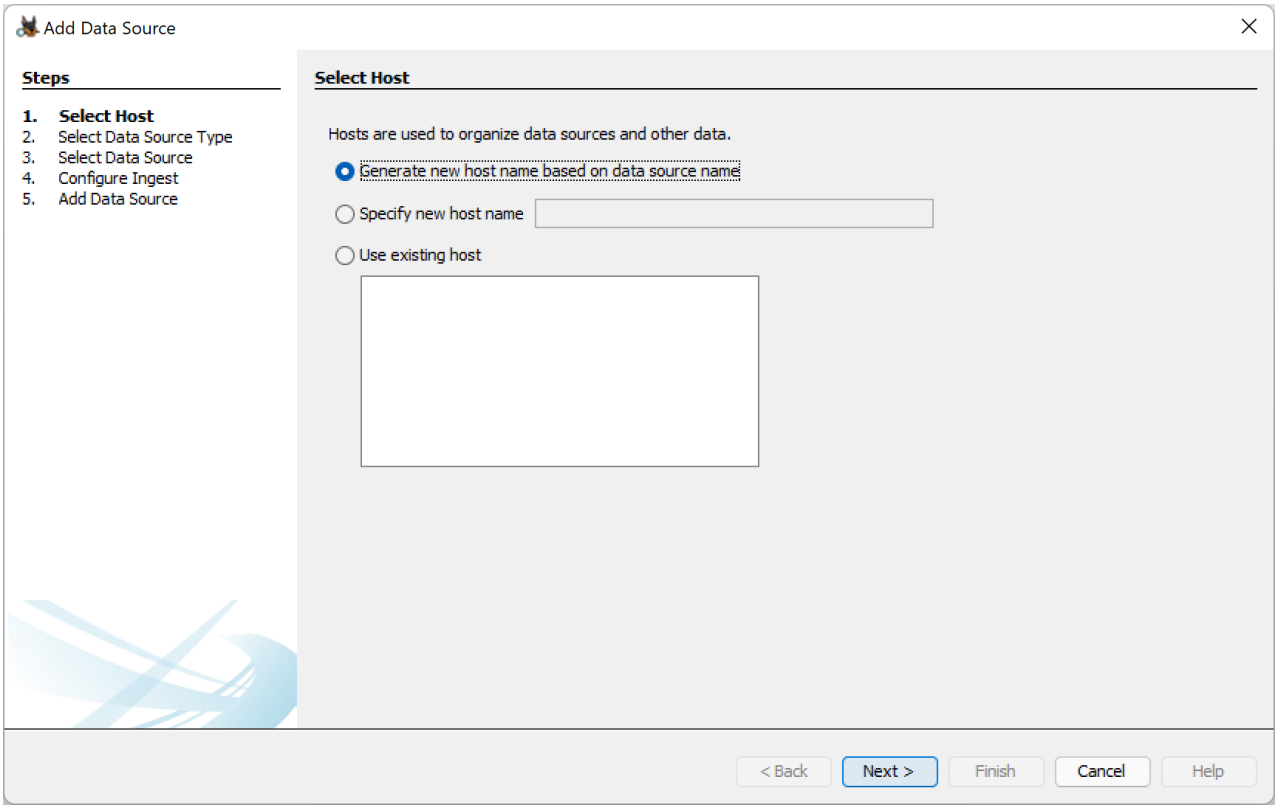


5. (Optional) Input optional information, Identify or Specify Case Number, Examiner Point of Contact > Finish

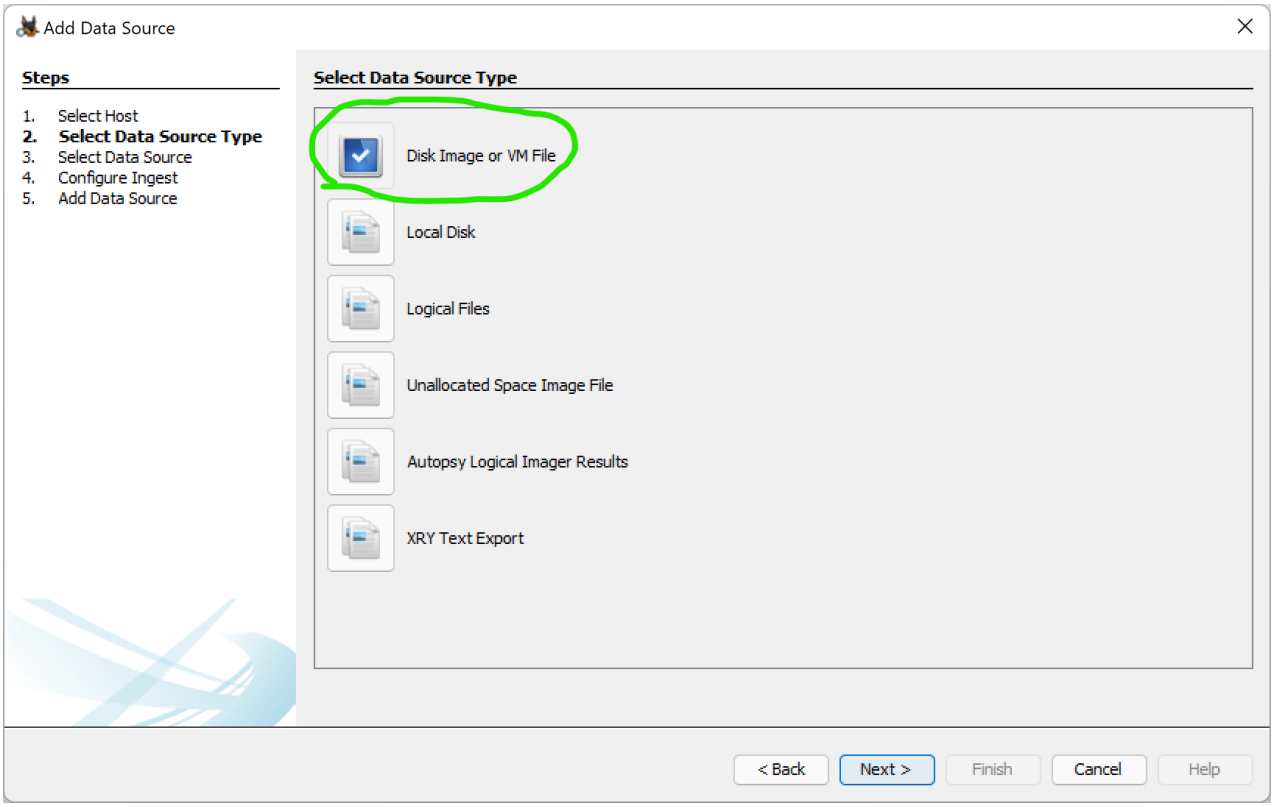


4.2 Adding a Data Source

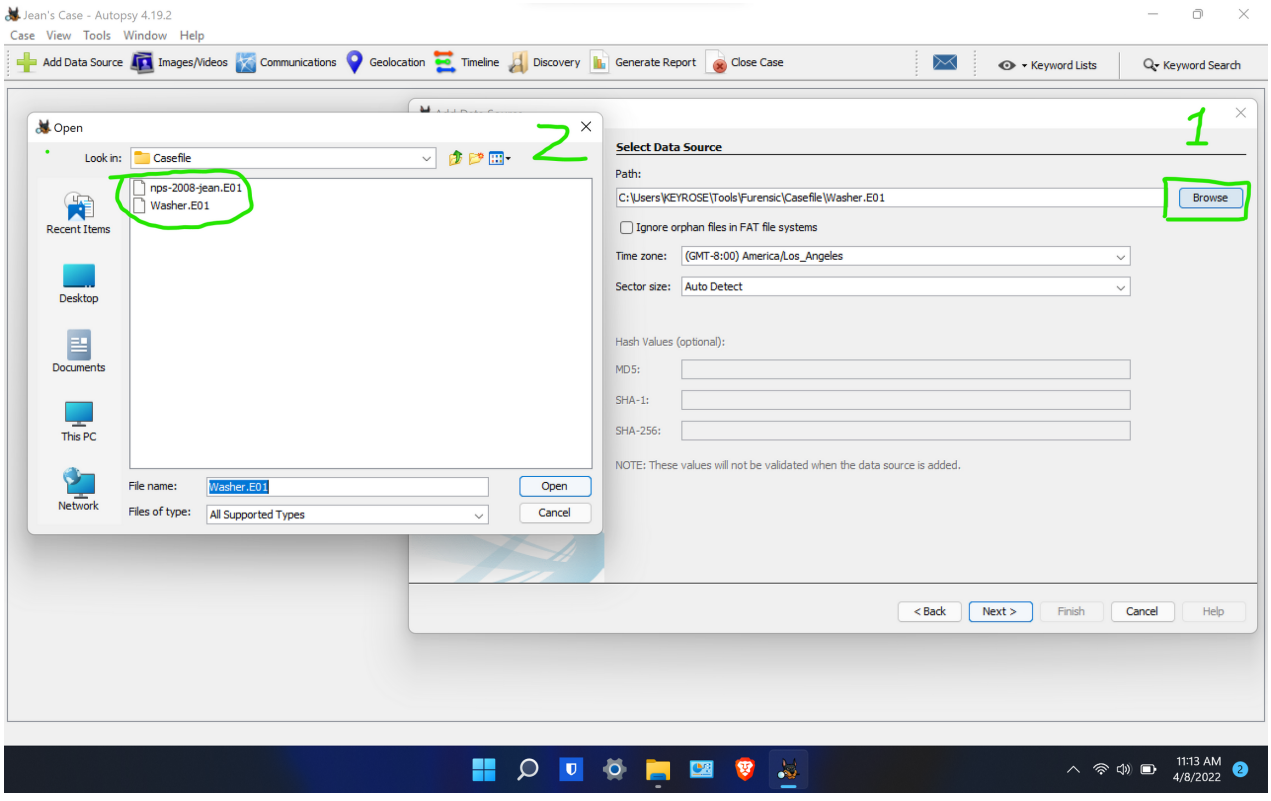
1. Select Host > Generate new host name based on data source name > Next



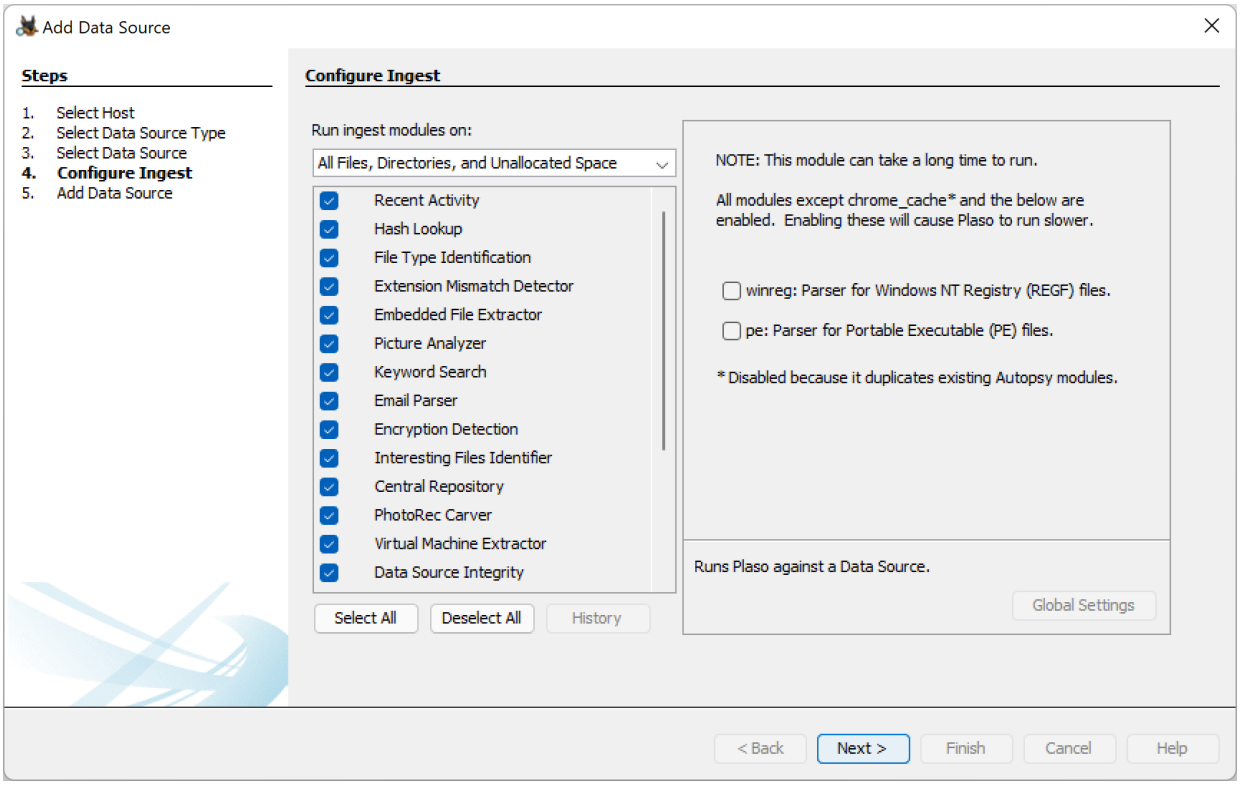
2. Select Data Source Type > Disk Image > Next



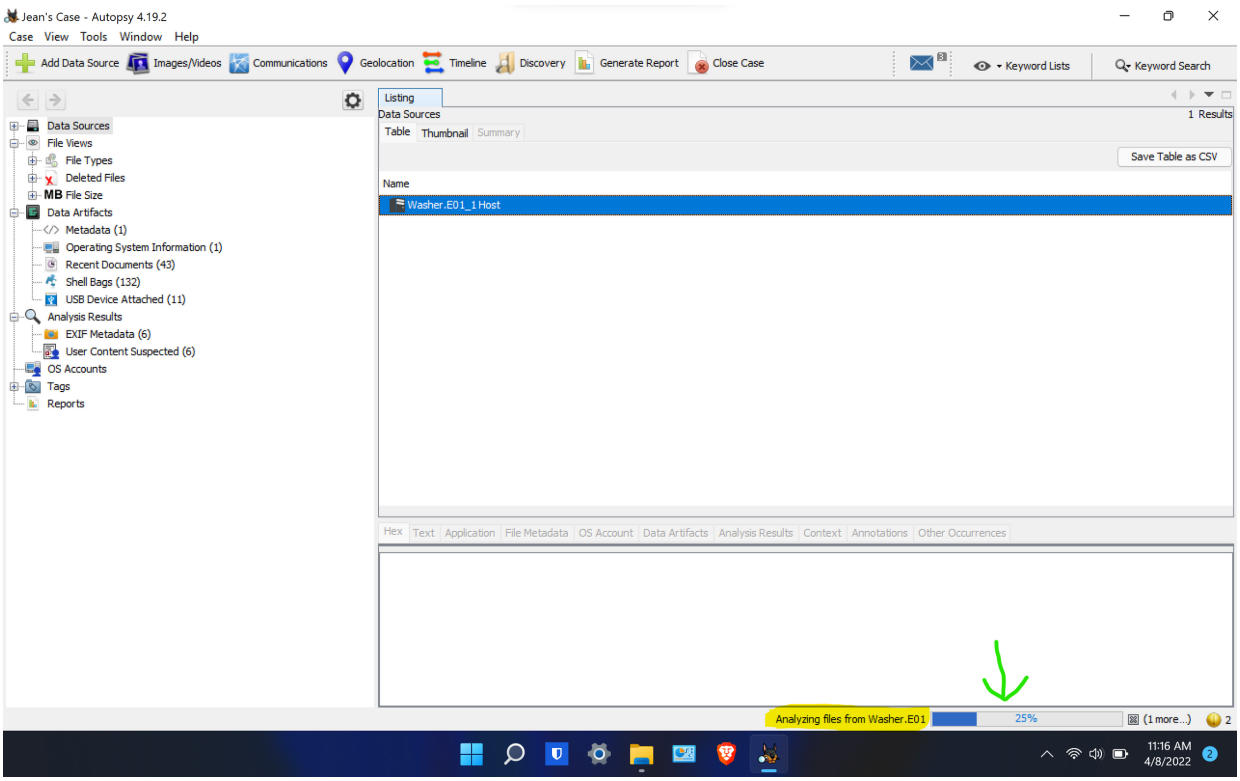
3. Select Data Source > Browse > Location of .E01 File > Next



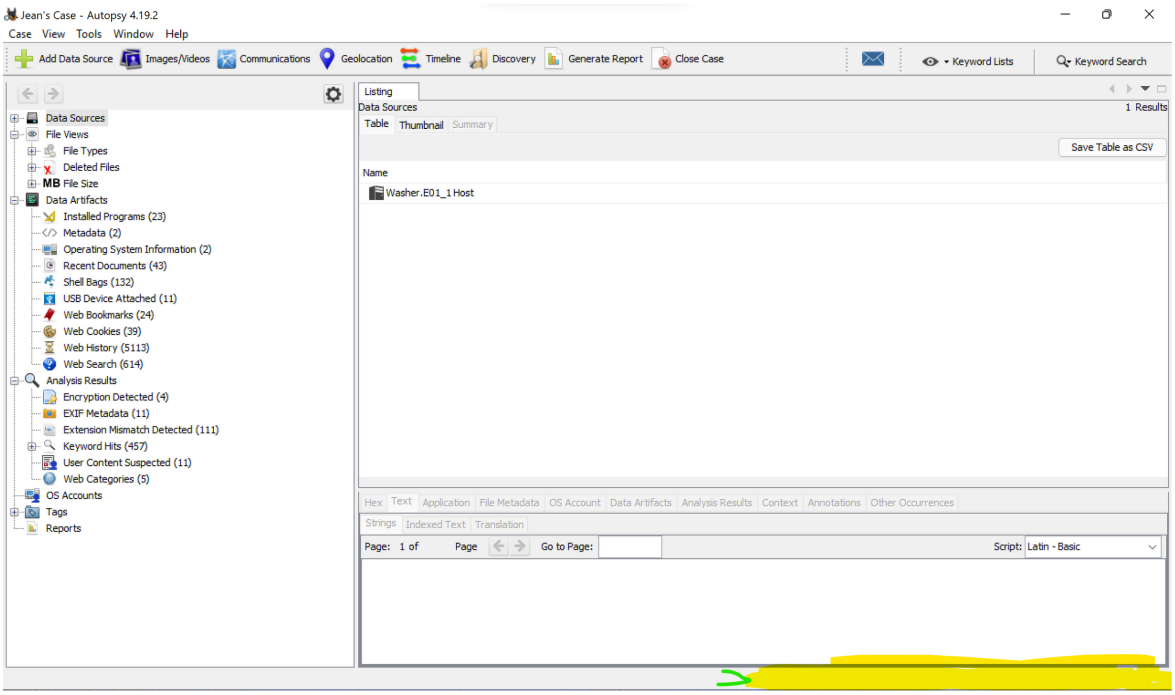
4. Configure Ingest > Next > Finish>



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

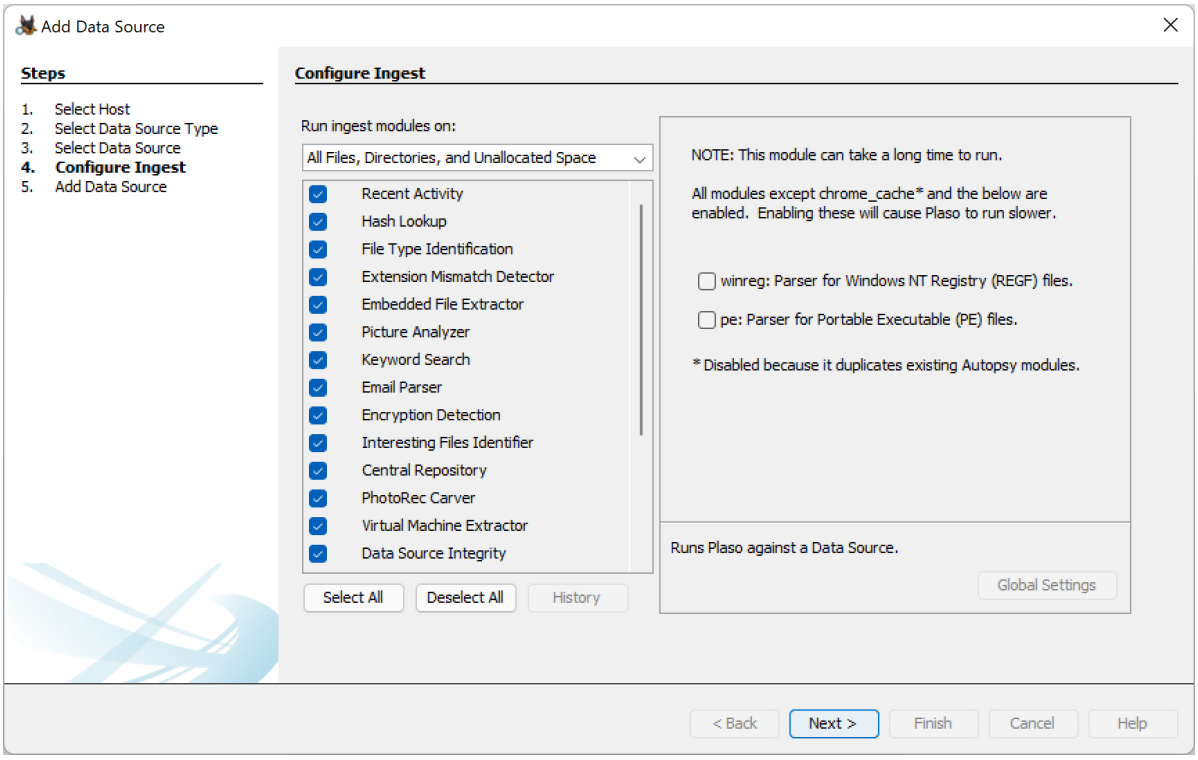


6. Completion of File analysis will remove loading bar



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.



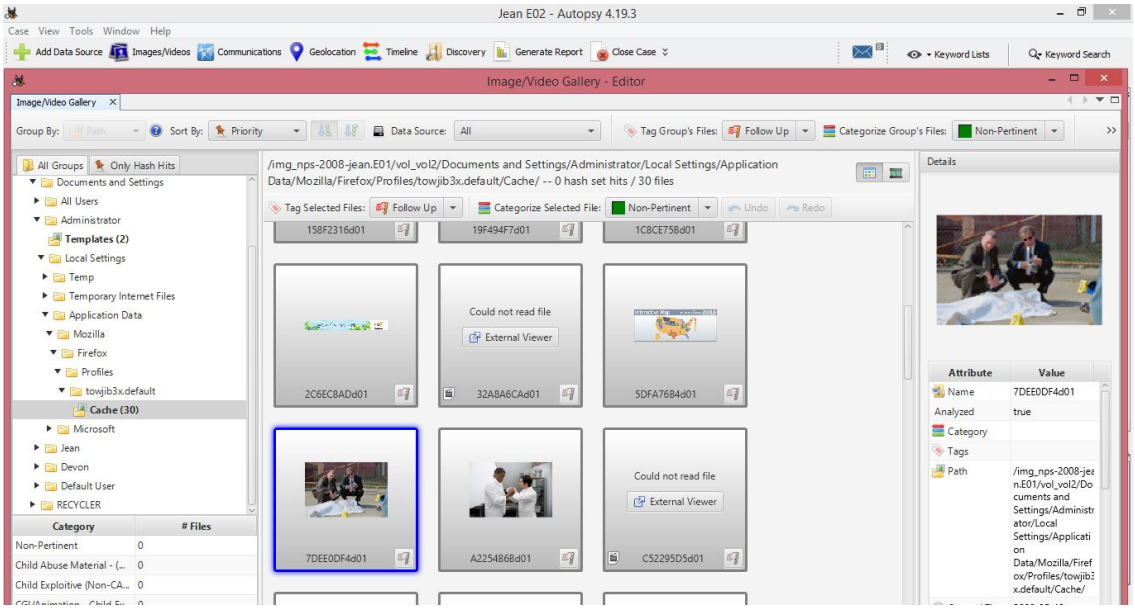
5.0 TOOLS

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.

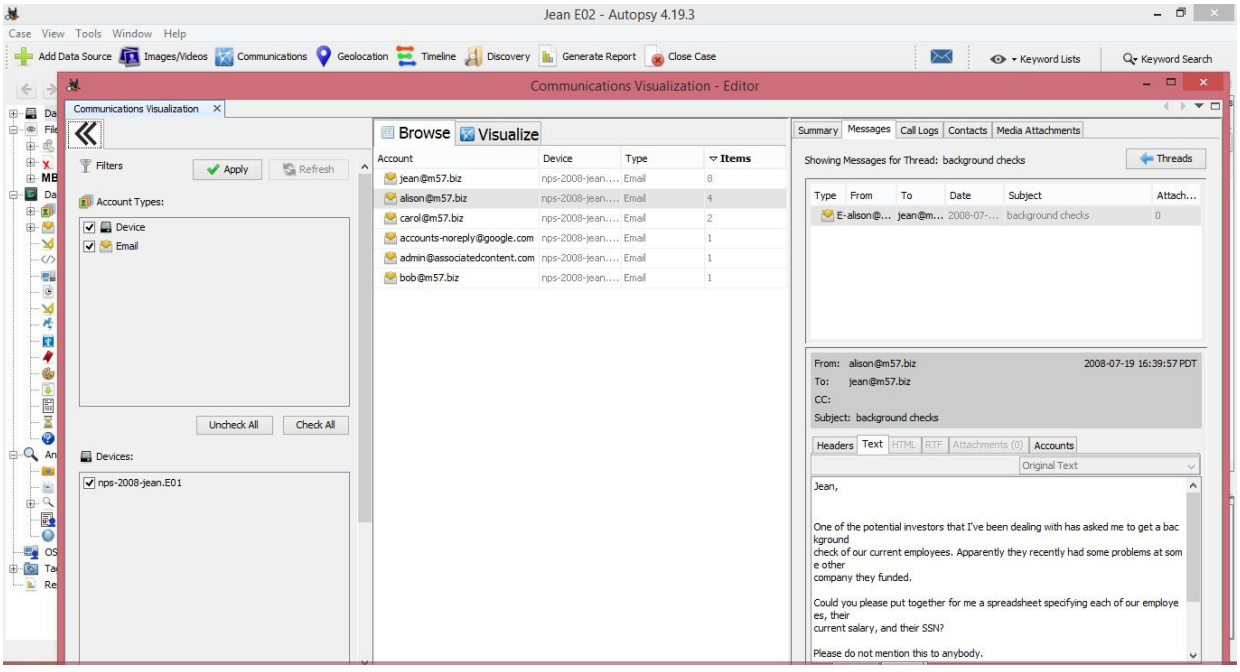
Allows the examiner to start viewing images immediately upon adding them to the case. As images are hashed, they are updated in the interface. You do not need to wait until the entire image is ingested.



5.2 Communication Visualization

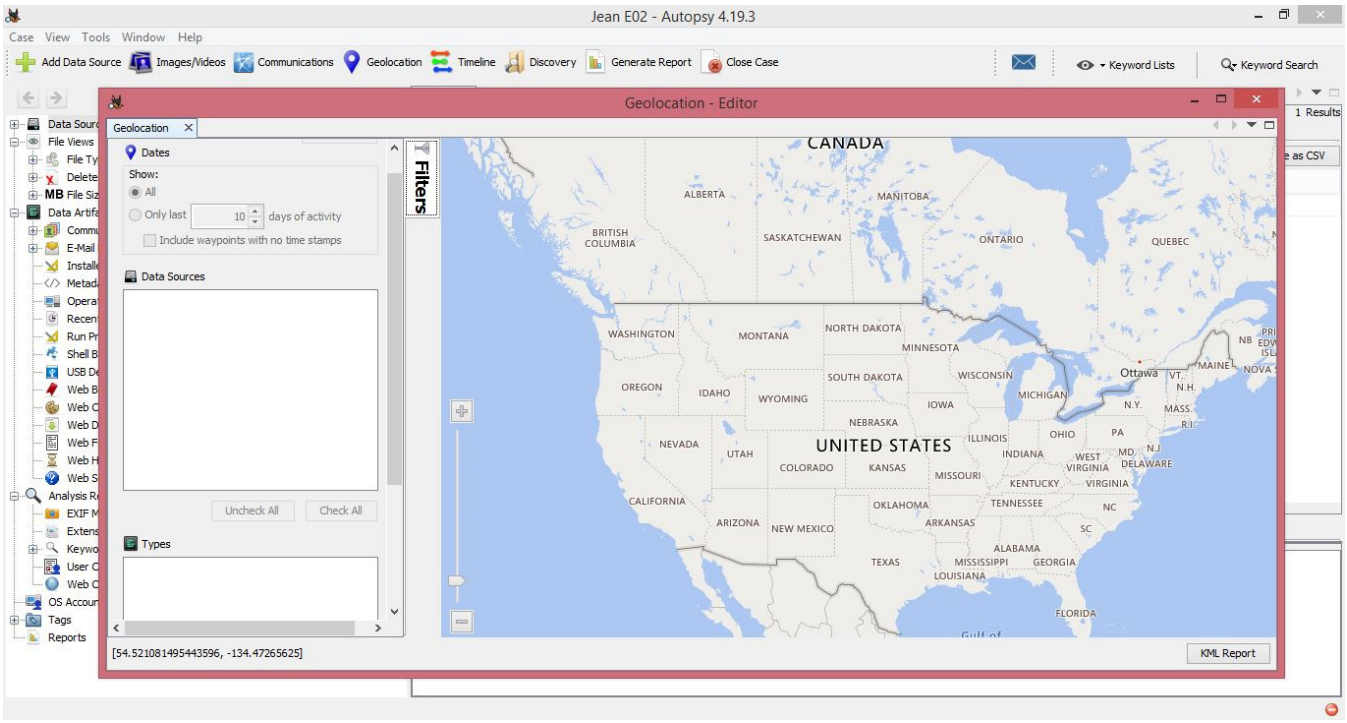
The Communications Visualization Tool gives a consolidated view of all communication events for the case. This allows an analyst to quickly view communications data such as:

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



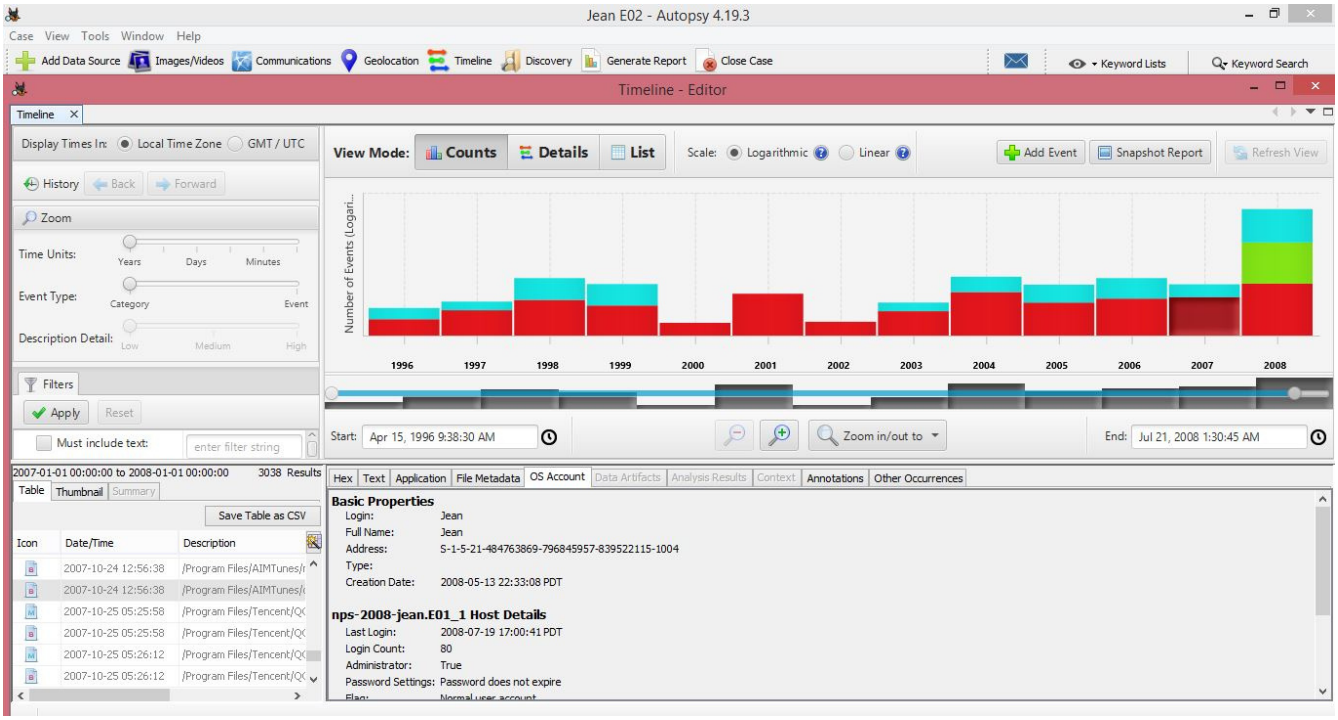
5.3 Geolocation

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.



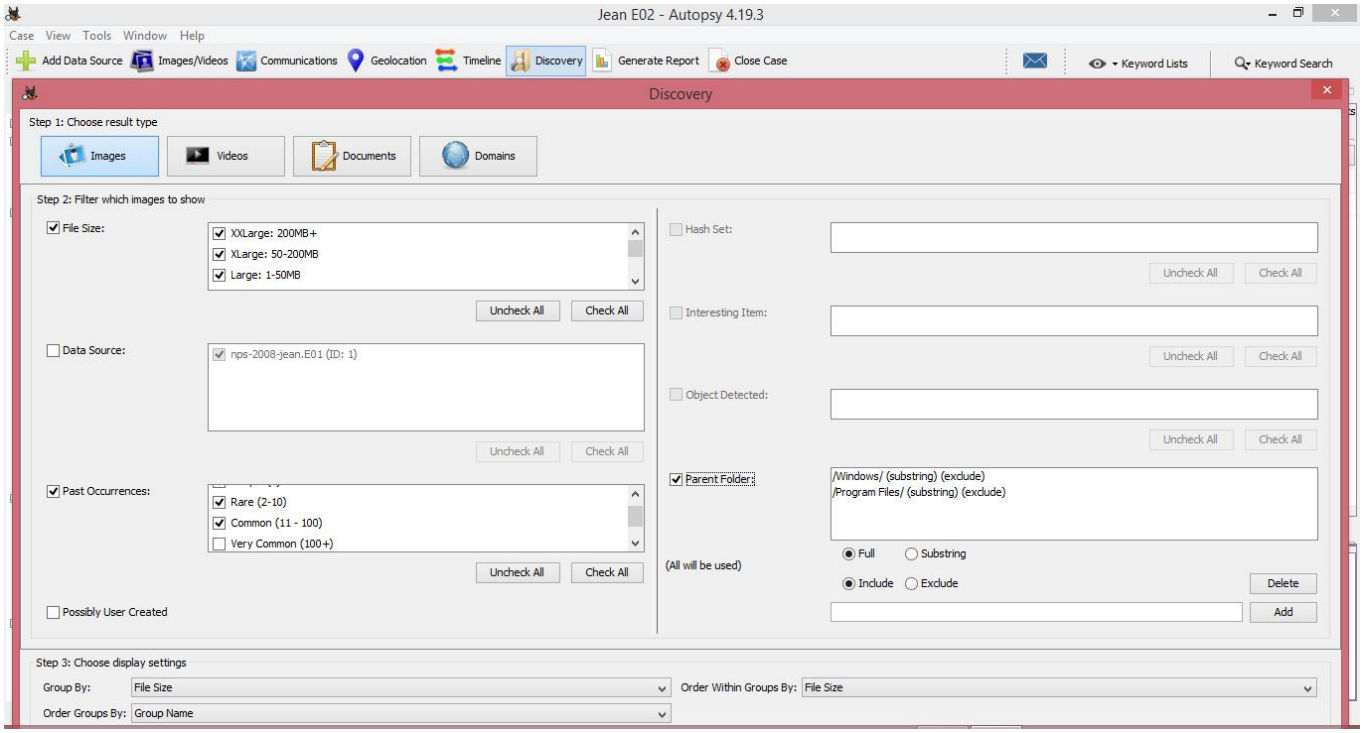
5.4 Timeline

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

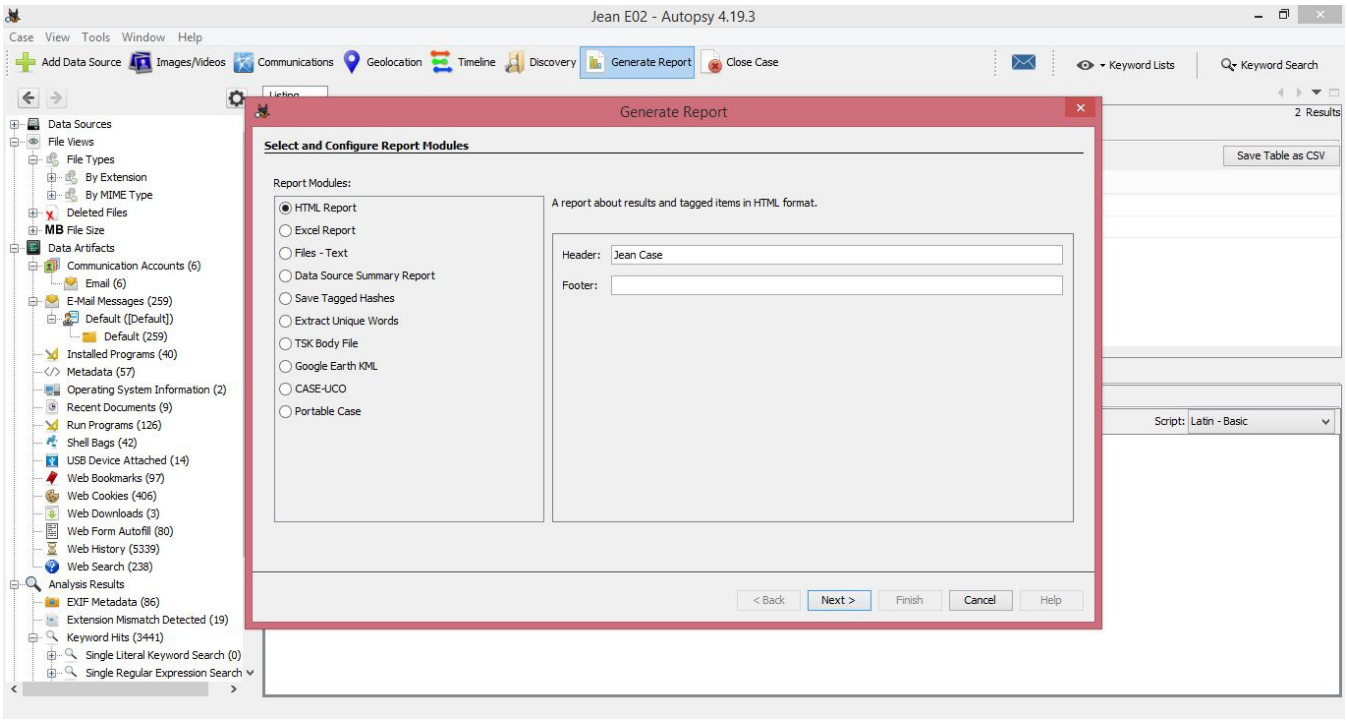
The discovery tool shows images, videos, documents, or domains that match a set of filters configured by the user. You can choose how to group and order your results in order to see the most relevant data first.

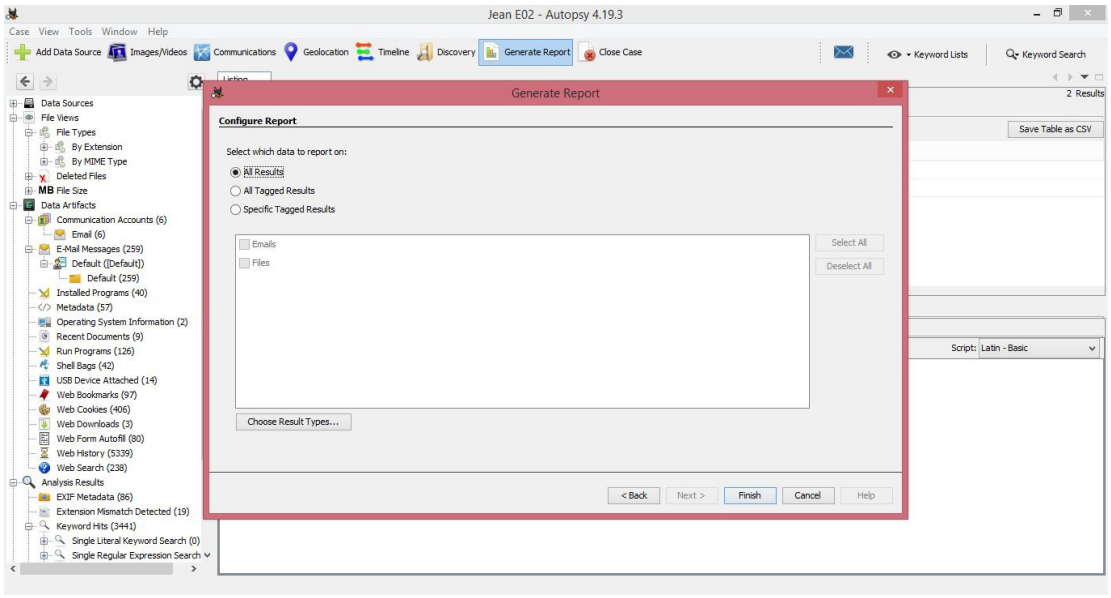


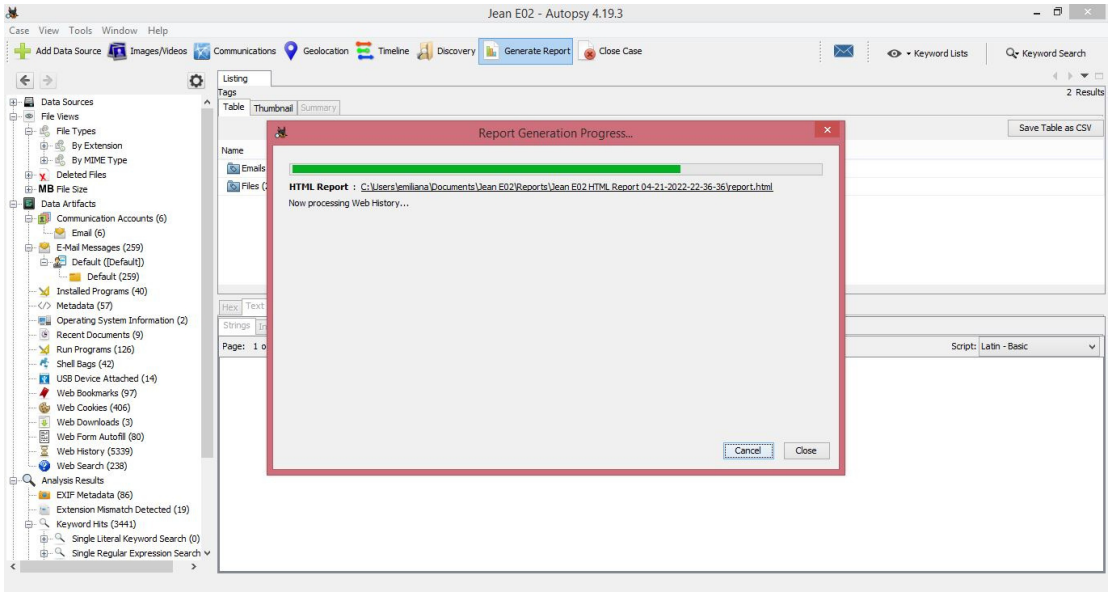
5.6 Generate Report

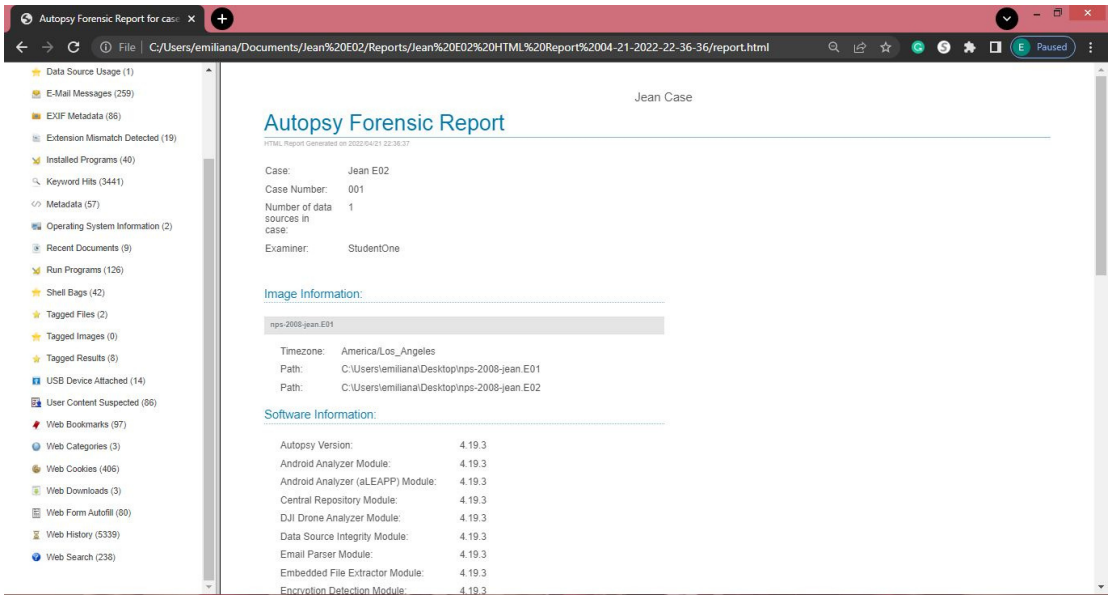
The report modules allow the user to extract key information from a case in a variety of formats. This includes making an HTML or Excel report containing all the extracted content, keyword hits, etc. from a case, or creating a KML file out of any coordinates found to load into software like Google Earth.

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



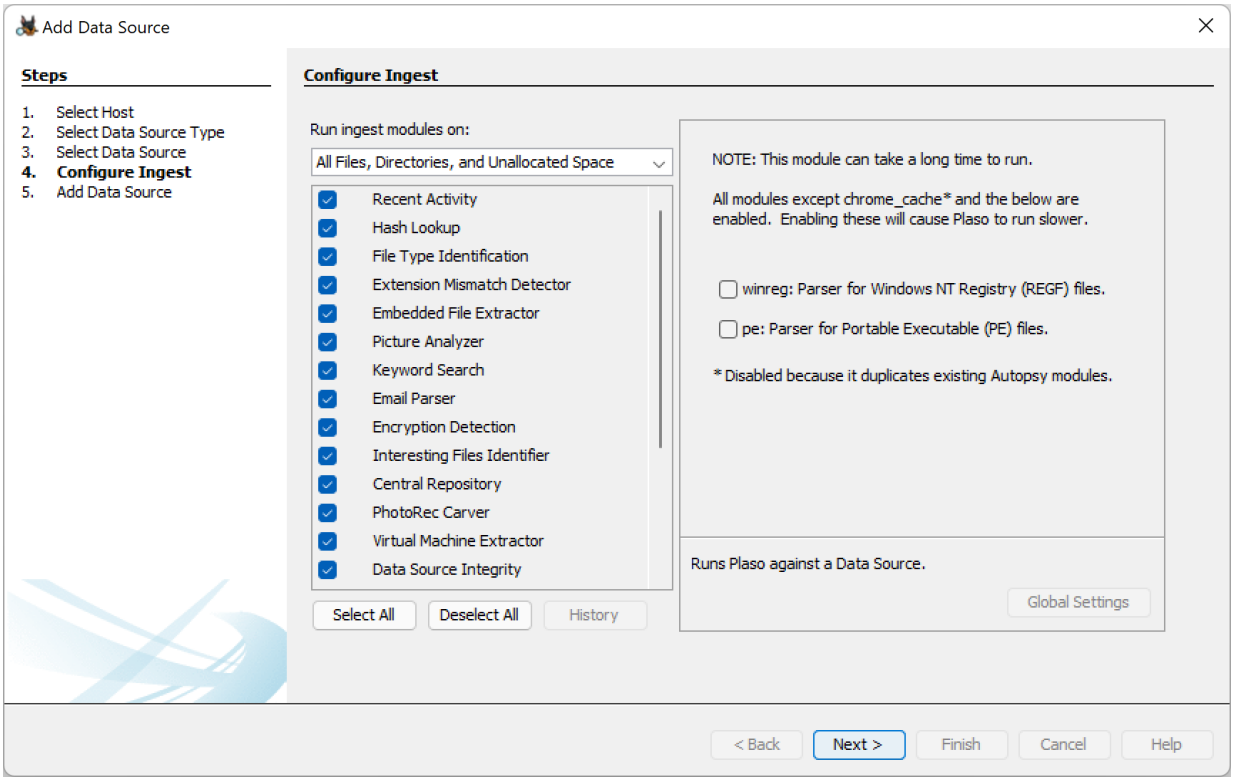

Jean E02 - Autopsy 4.19.3
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Generate Report
Configure Report
Select which data to report on:
All Results
All Tagged Results
Specific Tagged Results
Emails
Files
Select All
Deselect All
Choose Result Types...
< Back Next > Finish Cancel Help
Save Table as CSV
Script: Latin - Basic


Jean E02 - Autopsy 4.19.3
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Report Generation Progress...
HTML Report : C:\Users\emiliana\Documents\Jean E02\Reports\Jean E02 HTML Report 04-21-2022-22-36-36\report.html
Now processing Web History...
Cancel Close
Save Table as CSV
Script: Latin - Basic


Autopsy Forensic Report for case
File | C:/Users/emiliana/Documents/Jean%20E02/Reports/Jean%20E02%20HTML%20Report%2004-21-2022-22-36-36/report.html
Paused
Jean Case
Autopsy Forensic Report
Case: Jean E02
Case Number: 001
Number of data sources in case: 1
Examiner: StudentOne
Image Information:
nps-2008-jean.E01
Timezone: America/Los_Angeles
Path: C:\Users\emiliana\Desktop\nps-2008-jean.E01
Path: C:\Users\emiliana\Desktop\nps-2008-jean.E02
Software Information:
Autopsy Version: 4.19.3
Android Analyzer Module: 4.19.3
Android Analyzer (aLEAPP) Module: 4.19.3
Central Repository Module: 4.19.3
DJI Drone Analyzer Module: 4.19.3
Data Source Integrity Module: 4.19.3
Email Parser Module: 4.19.3
Embedded File Extractor Module: 4.19.3
Encryption Detection Module: 4.19.3

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.
- **Center Repository** - creates a local databse that keeps track of files and activites that youve 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:

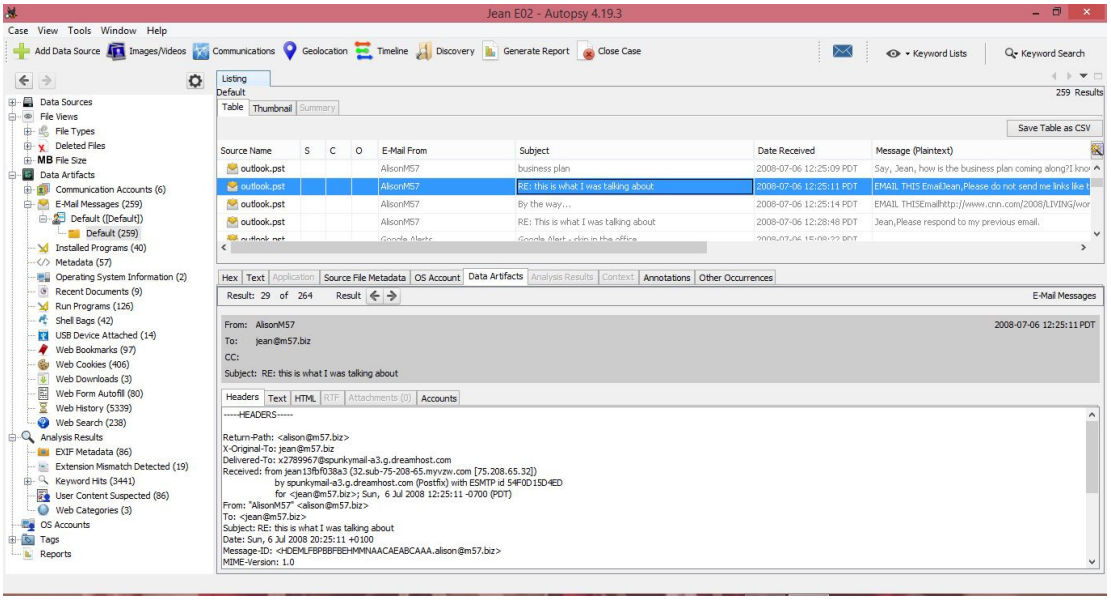
- Autopsy : https://www.autopsy.com/
- Link to Case Image: https://digitalcorpora.org/corpora/scenarios/m57-jean

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.

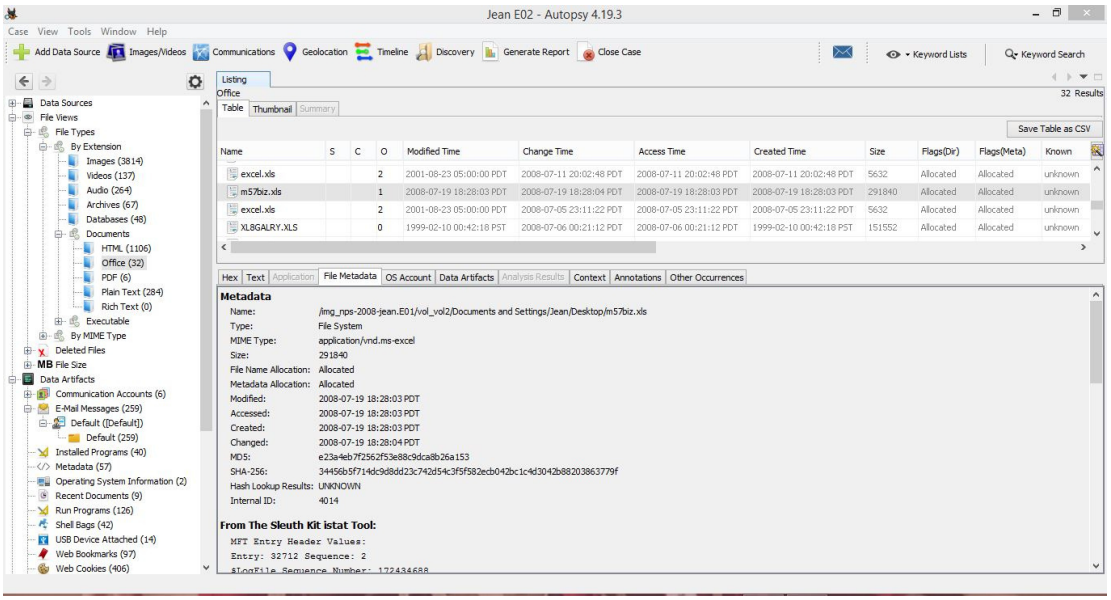


6.4 Question 2

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



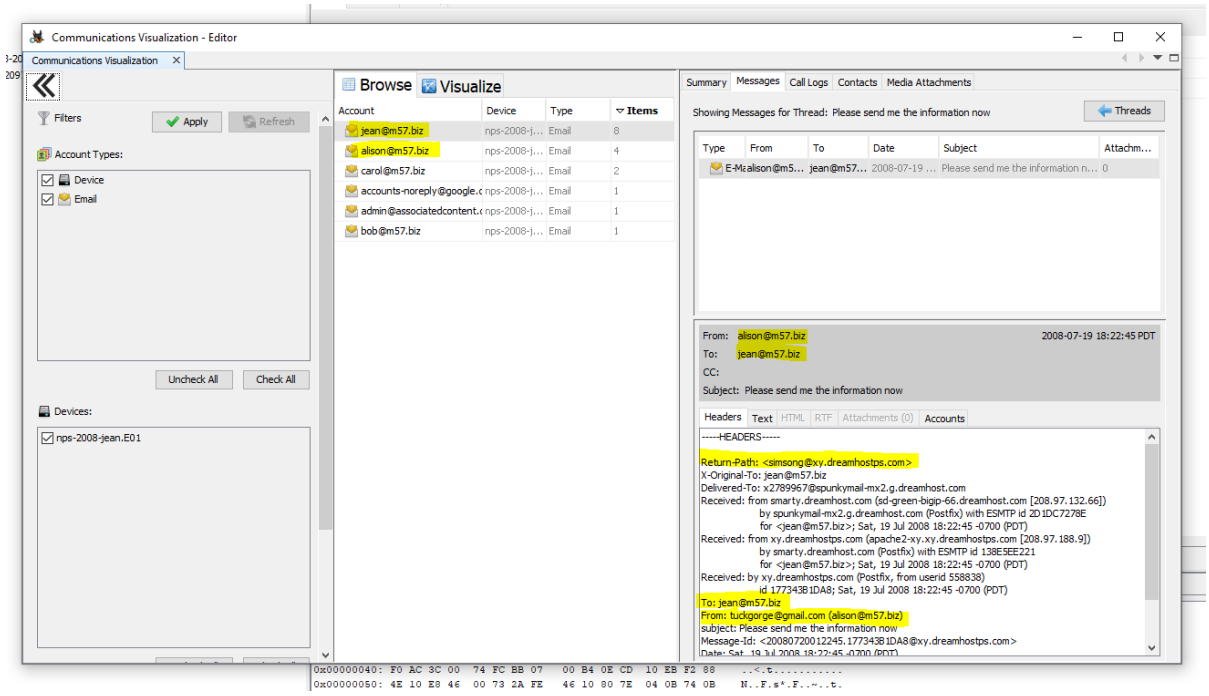
6.5 Question 3

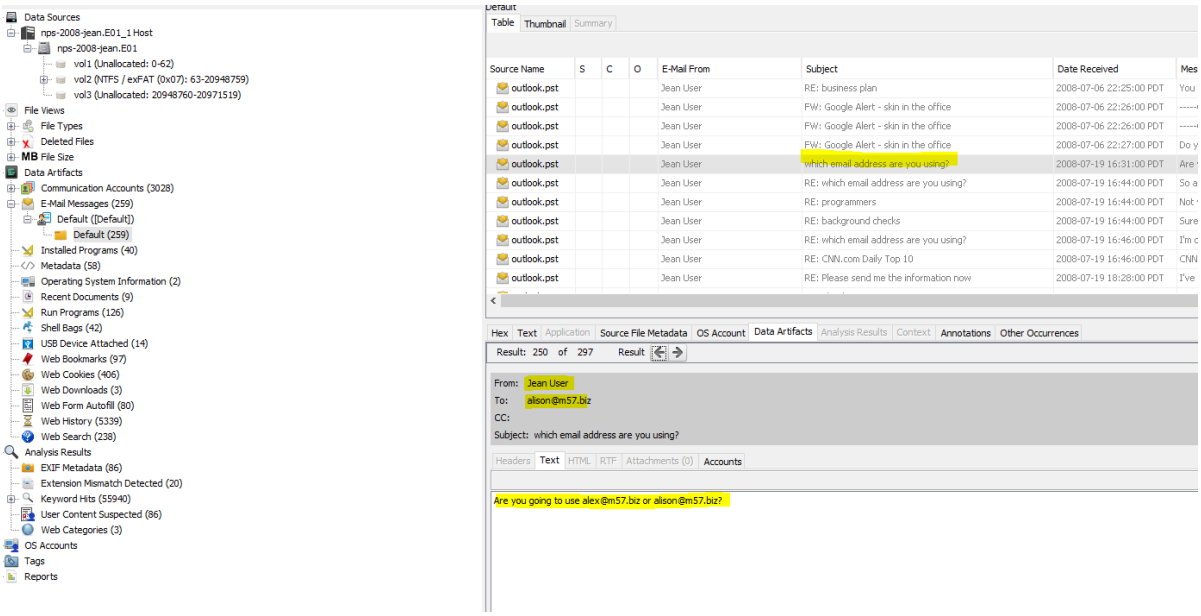
Who else from the company is involved?

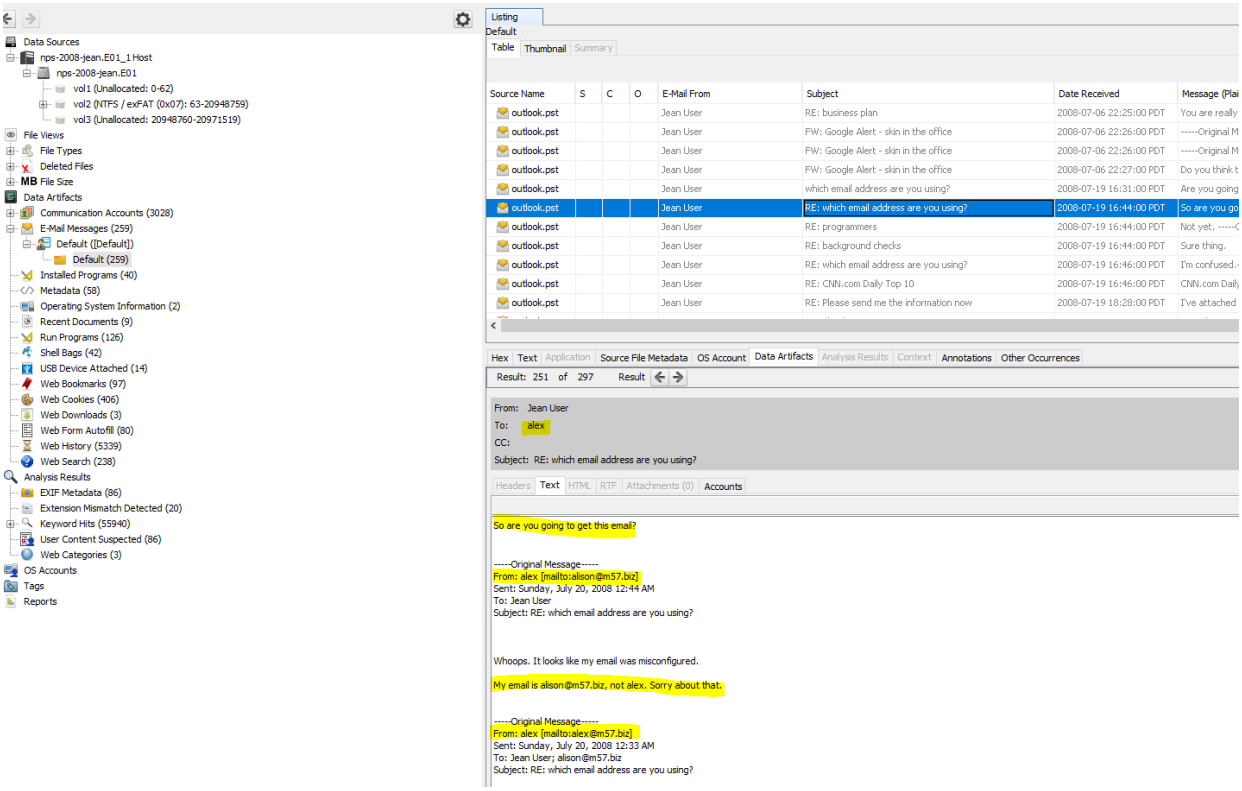
- Select “Communications Visualization” > Browse > Messages

OR

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







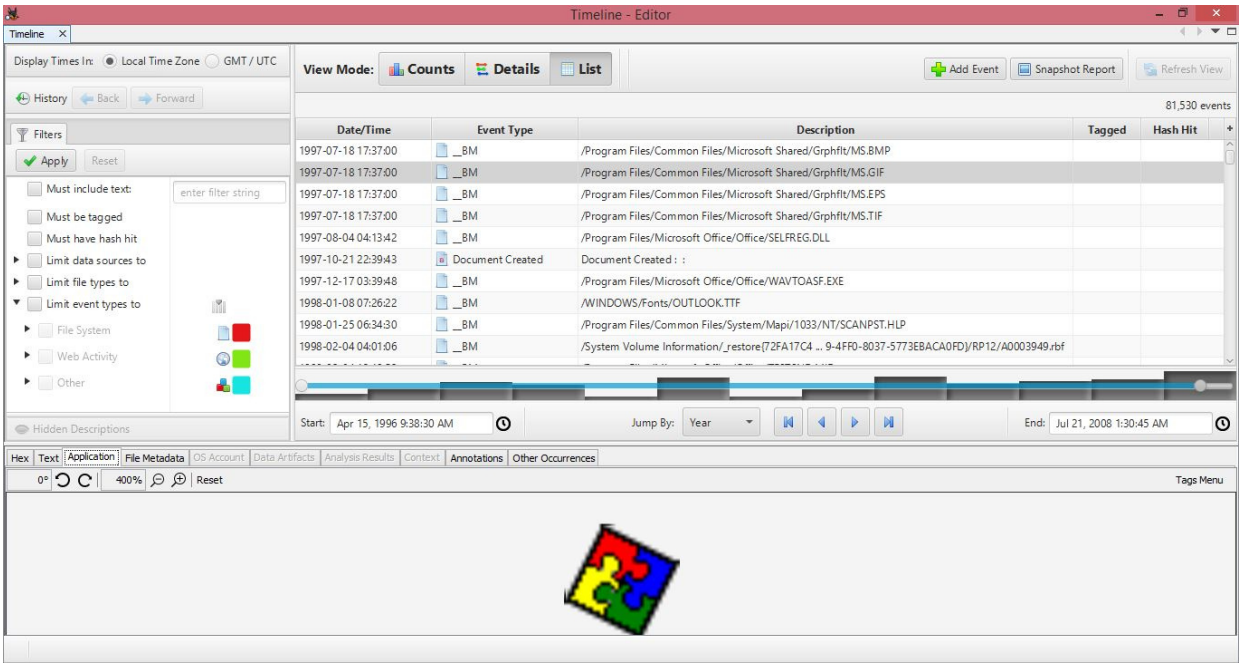
6.6 Question 4

What does the timeline look like?

- Select " Timeline" > List

Or

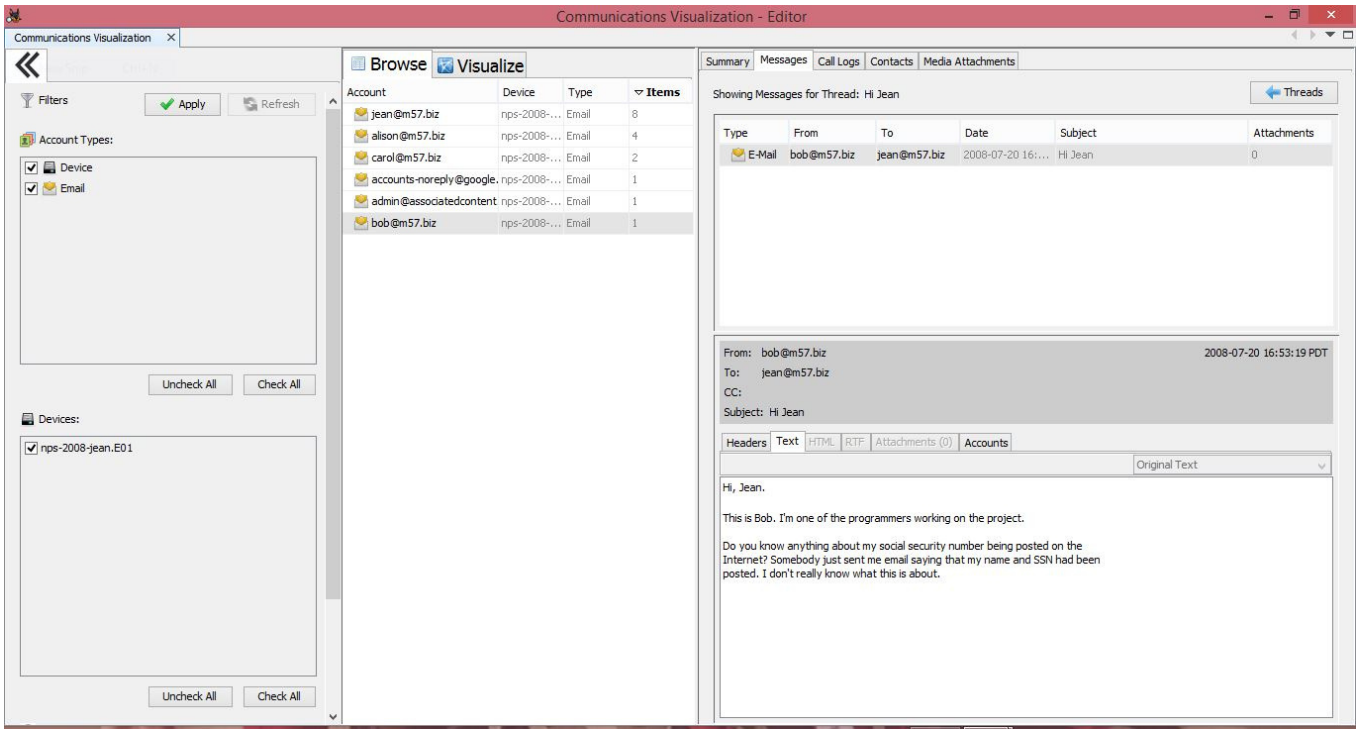
- Select "Views" > File Types > By Extension > Documents > Office (32)



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”



6.8 Question 6

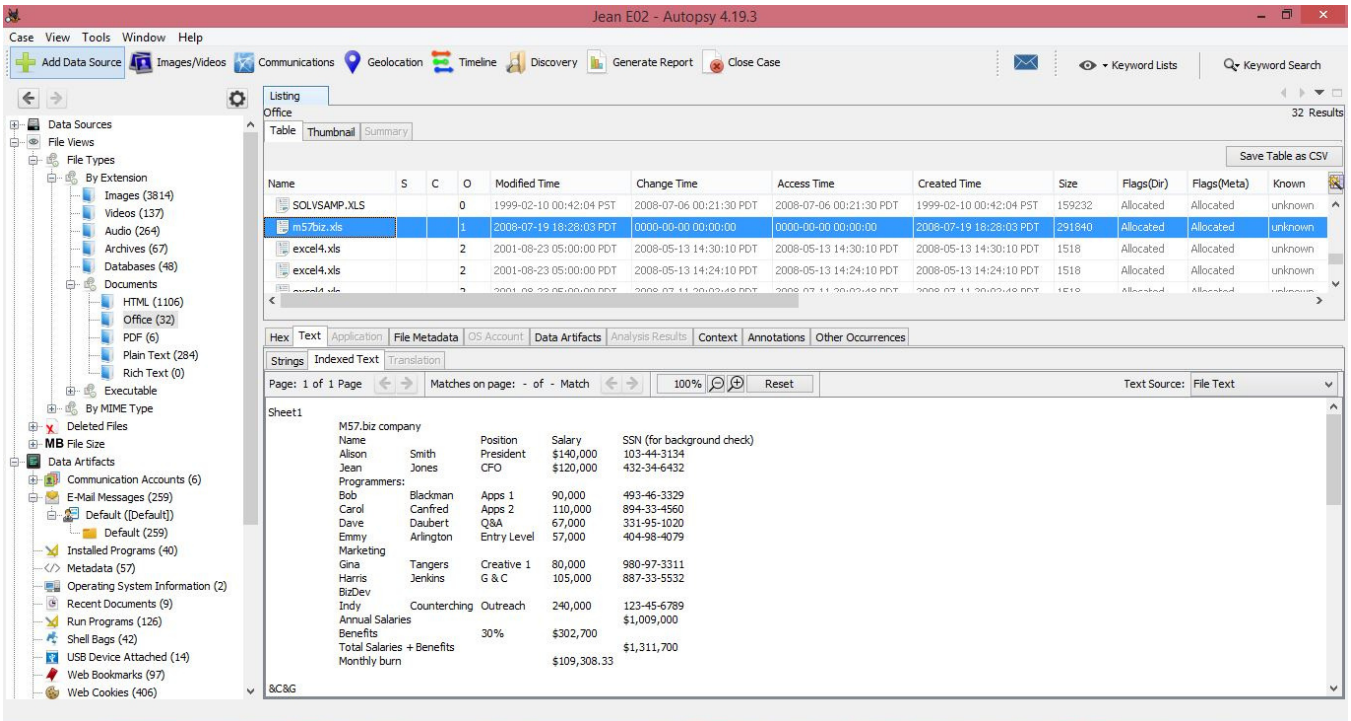
Can you list out Bob SSN, Carol salary and Indy position.

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

Bob --> 493-46-3329

Carol --> 110,000

Indy --> Outreach



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/