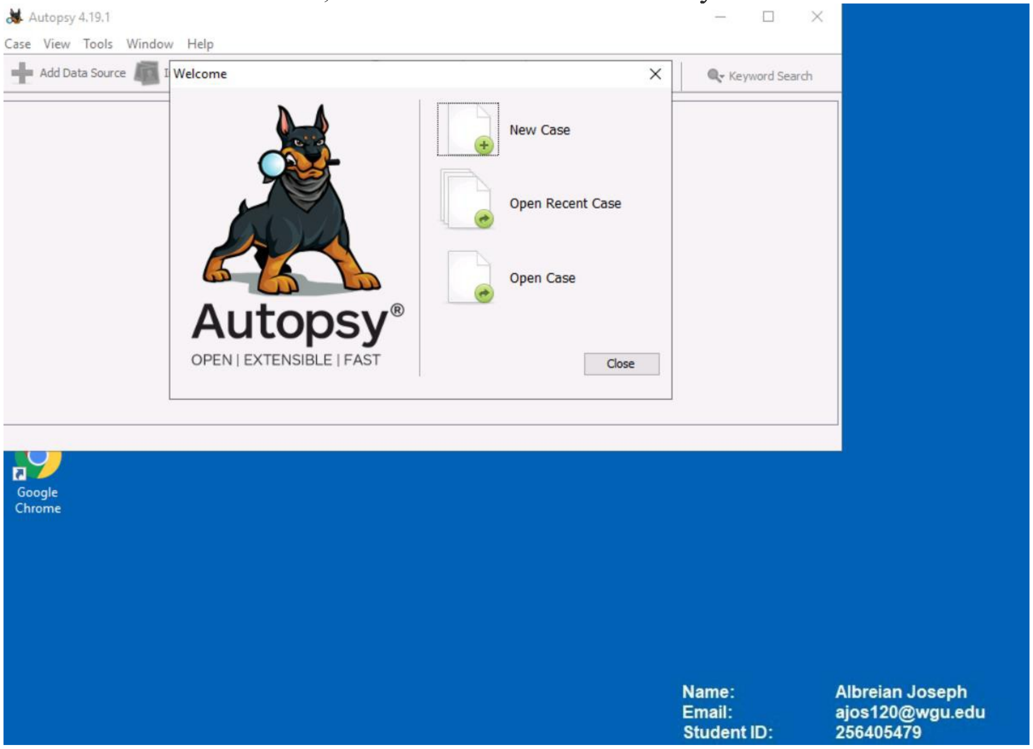
Albreian R. Joseph

Digital Forensics

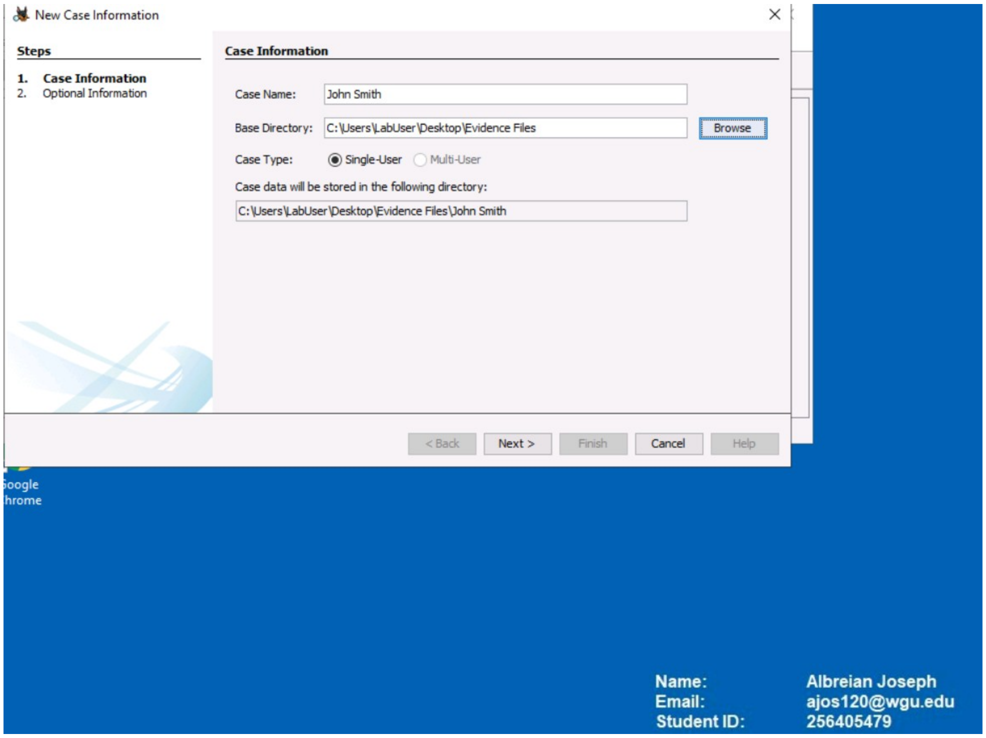
Student ID: 2589656

I. Describe *all* steps taken in Autopsy to create the forensic system case file:

- First, I will create a new case study.



- Enter a Base Directory use the browse button:



Case Name: John Smith

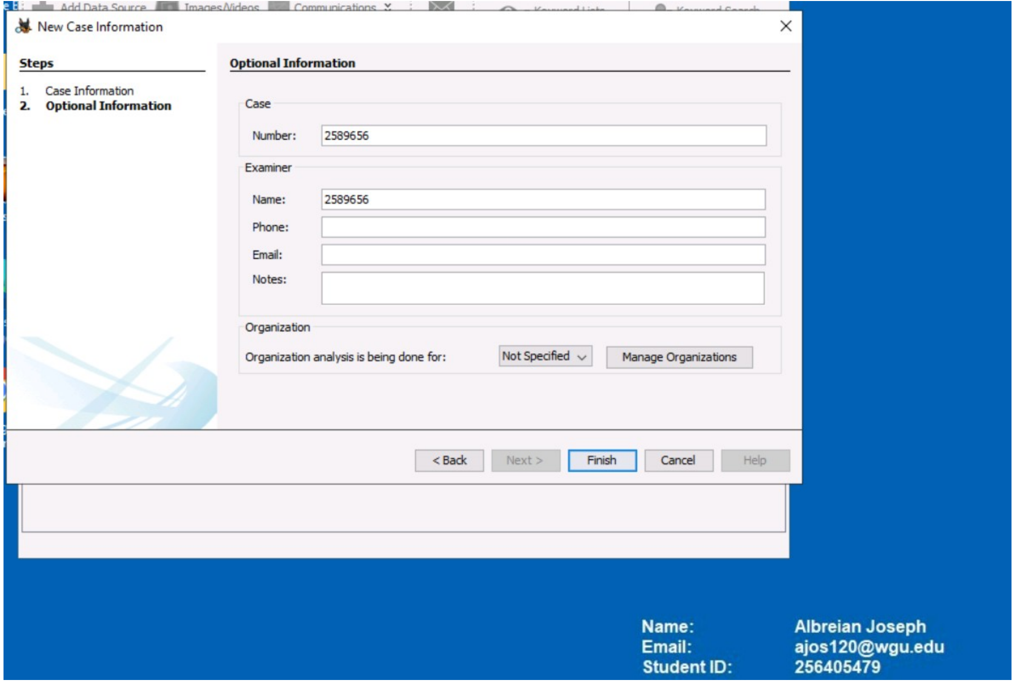
Base Directory: C:\Users\LabUser\Desktop\Evidence Files

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

C:\Users\LabUser\Desktop\Evidence Files\John Smith

- Add **Case Number,** Add **Name**



Number: 2589656

Name: 2589656

Phone:

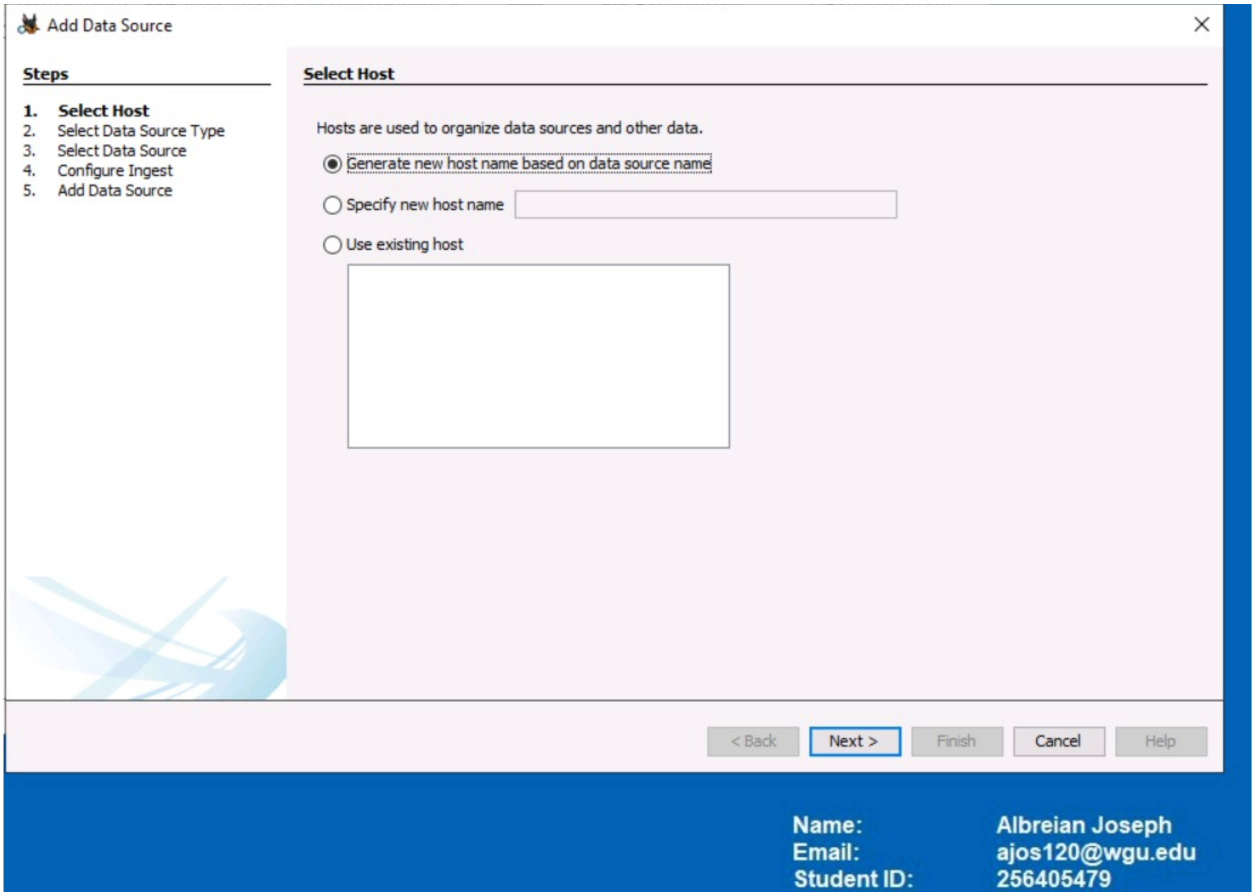
Email:

Notes:

Organization analysis is being done for: Not Specified

Name: Albreian Joseph
Email: ajos120@wgu.edu
Student ID: 256405479

- **Select Host:**



Hosts are used to organize data sources and other data.

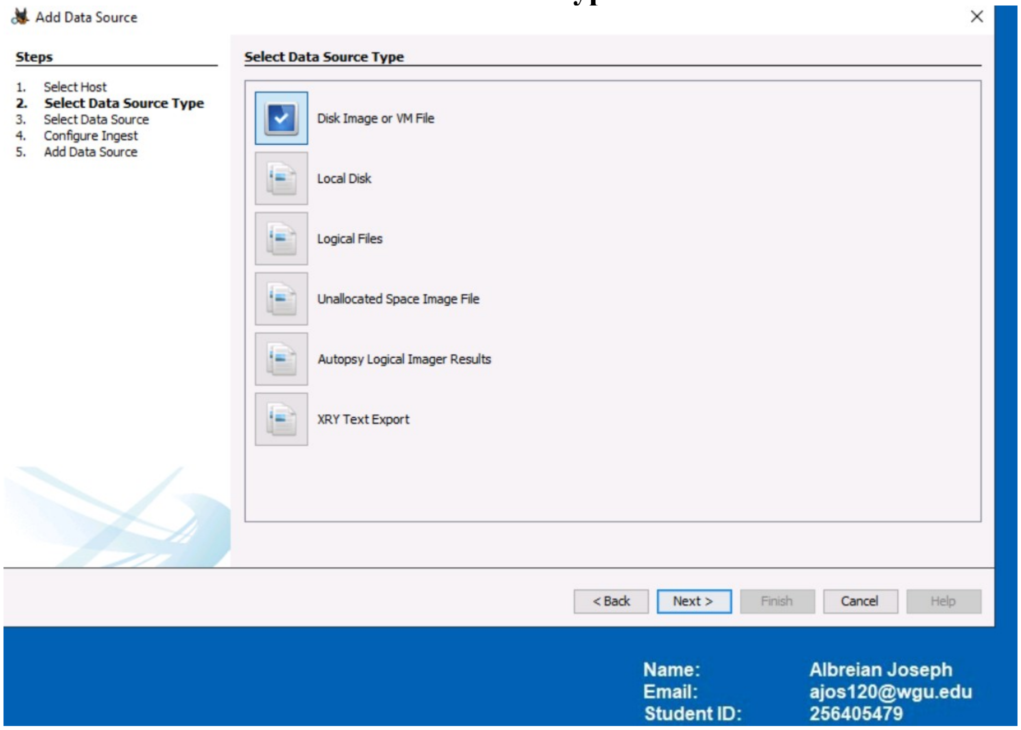
● Generate new host name based on data source name

○ Specify new host name

○ Use existing host

Name: Albreian Joseph
Email: ajos120@wgu.edu
Student ID: 256405479

- Select the **data source type:**



Add Data Source

Steps

1. Select Host
2. **Select Data Source Type**
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Data Source Type

☑ Disk Image or VM File

Local Disk

Logical Files

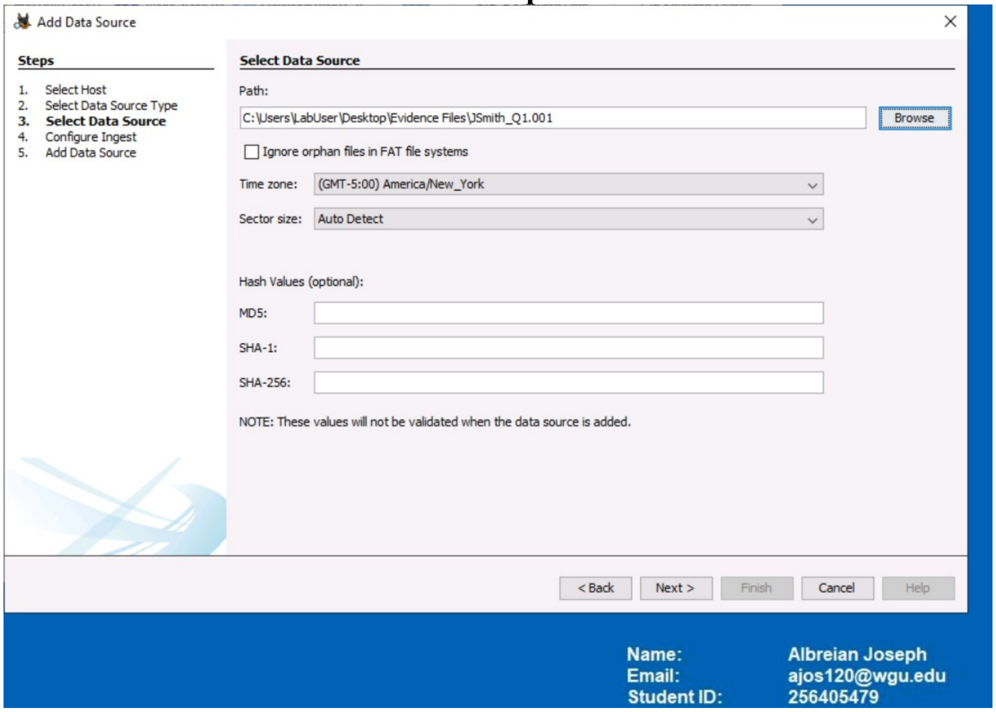
Unallocated Space Image File

Autopsy Logical Imager Results

XRY Text Export

Name: Albreian Joseph
Email: ajos120@wgu.edu
Student ID: 256405479

- Select **Data Source path**:



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path:

C:\Users\LabUser\Desktop\Evidence Files\JSmith_Q1.001

☐ Ignore orphan files in FAT file systems

Time zone: (GMT-5:00) America/New_York

Sector size: Auto Detect

Hash Values (optional):

MD5:

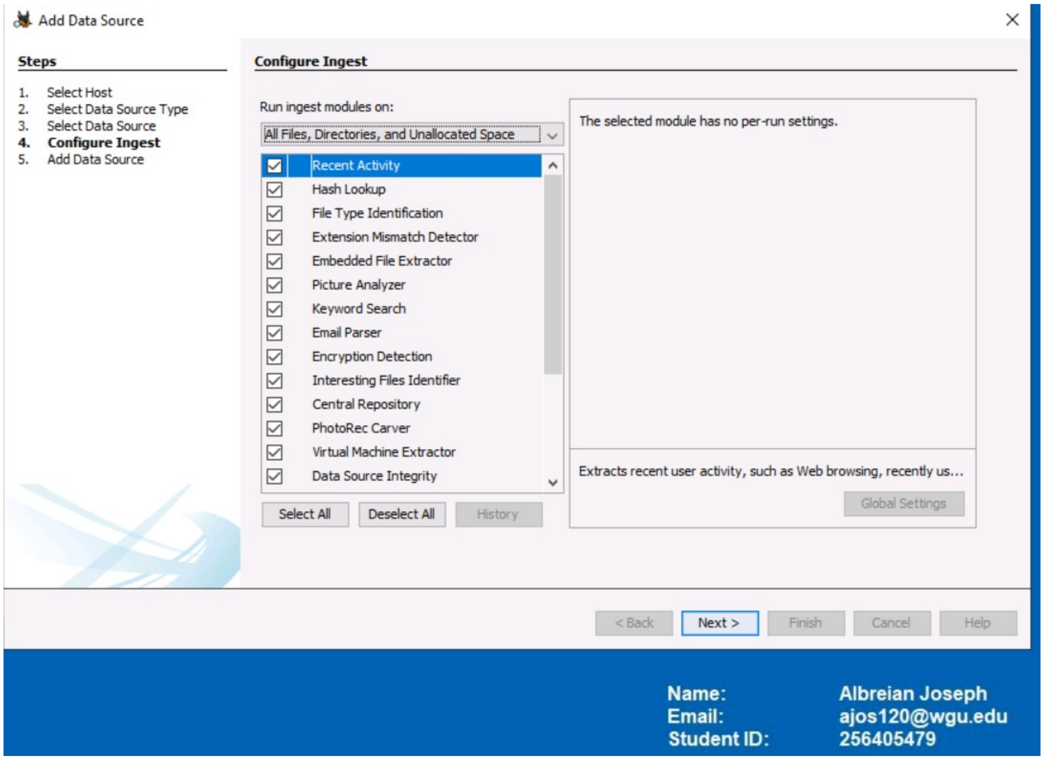
SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

Name: Albreian Joseph
Email: ajos120@wgu.edu
Student ID: 256405479

- **Configure Ingest:**



Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

Run ingest modules on:

All Files, Directories, and Unallocated Space

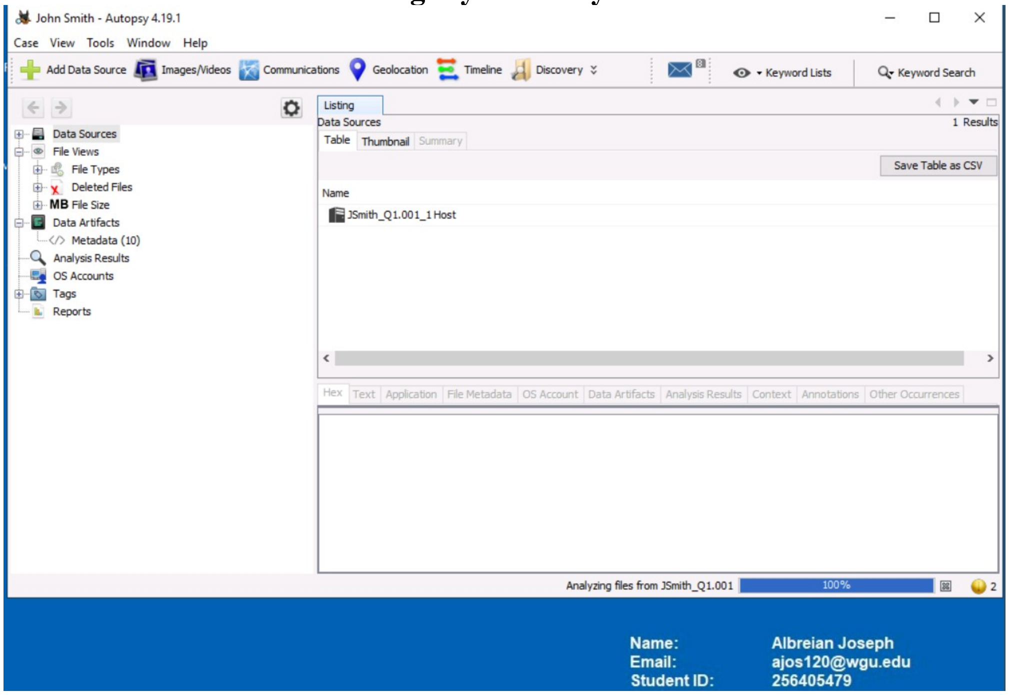
- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Extension Mismatch Detector
- ☑ Embedded File Extractor
- ☑ Picture Analyzer
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Encryption Detection
- ☑ Interesting Files Identifier
- ☑ Central Repository
- ☑ PhotoRec Carver
- ☑ Virtual Machine Extractor
- ☑ Data Source Integrity

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

Name: Albreian Joseph
Email: ajos120@wgu.edu
Student ID: 256405479

- **Time to begin your analysis:**



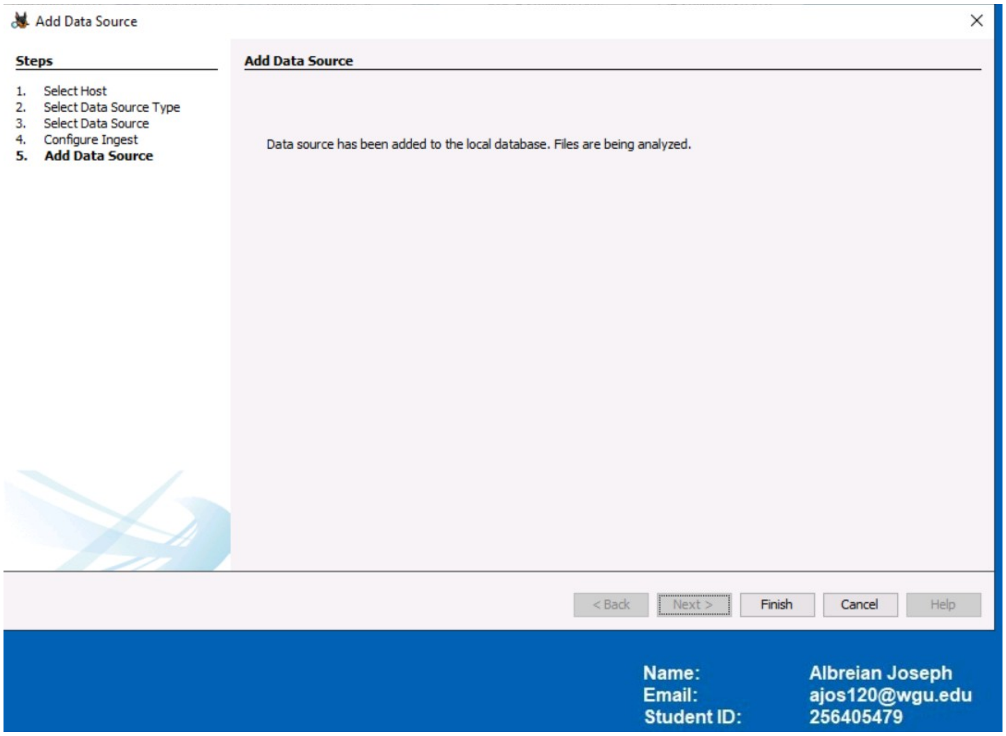
Data Sources — 1 Results

Name
JSmith_Q1.001_1 Host

Analyzing files from JSmith_Q1.001 100%

Name: Albreian Joseph
Email: ajos120@wgu.edu
Student ID: 256405479

- **Add Data Source:**



Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. **Add Data Source**

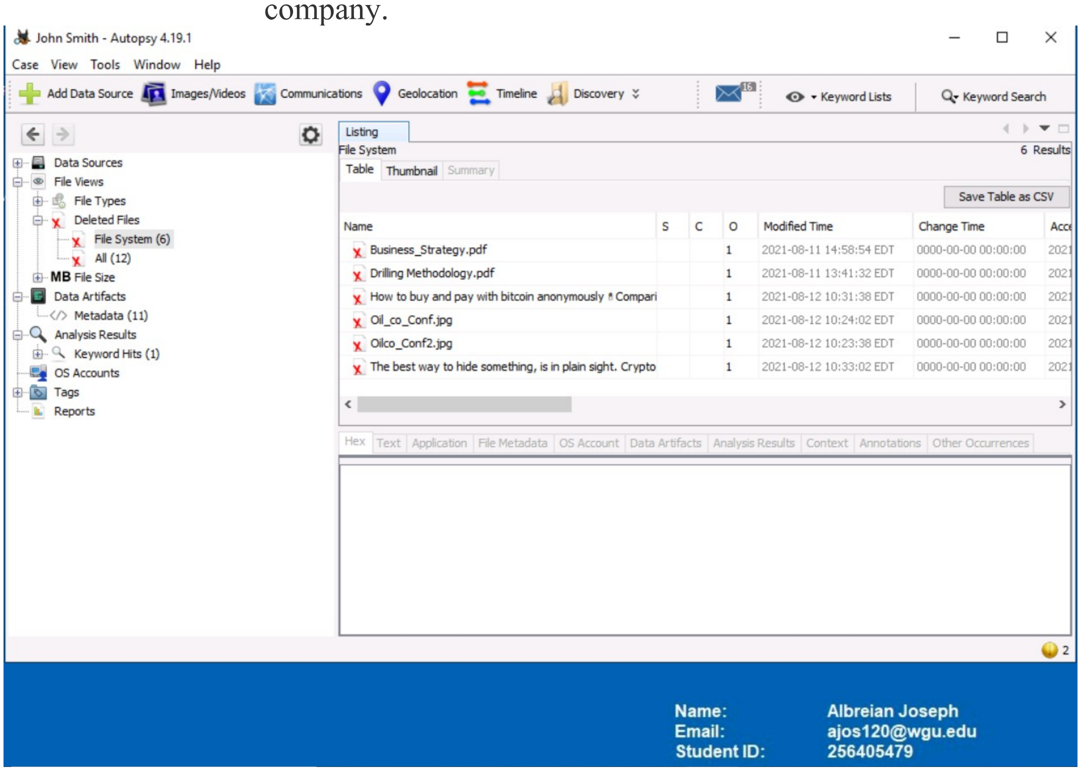
Add Data Source

Data source has been added to the local database. Files are being analyzed.

Name: Albreian Joseph
Email: ajos120@wgu.edu
Student ID: 256405479

II. Describe *all* steps taken in Autopsy to identify potential evidence:

- Looking through the deleted, unallocated files there were listings about bitcoin, hiding something in plain sight, and classified information about the company.

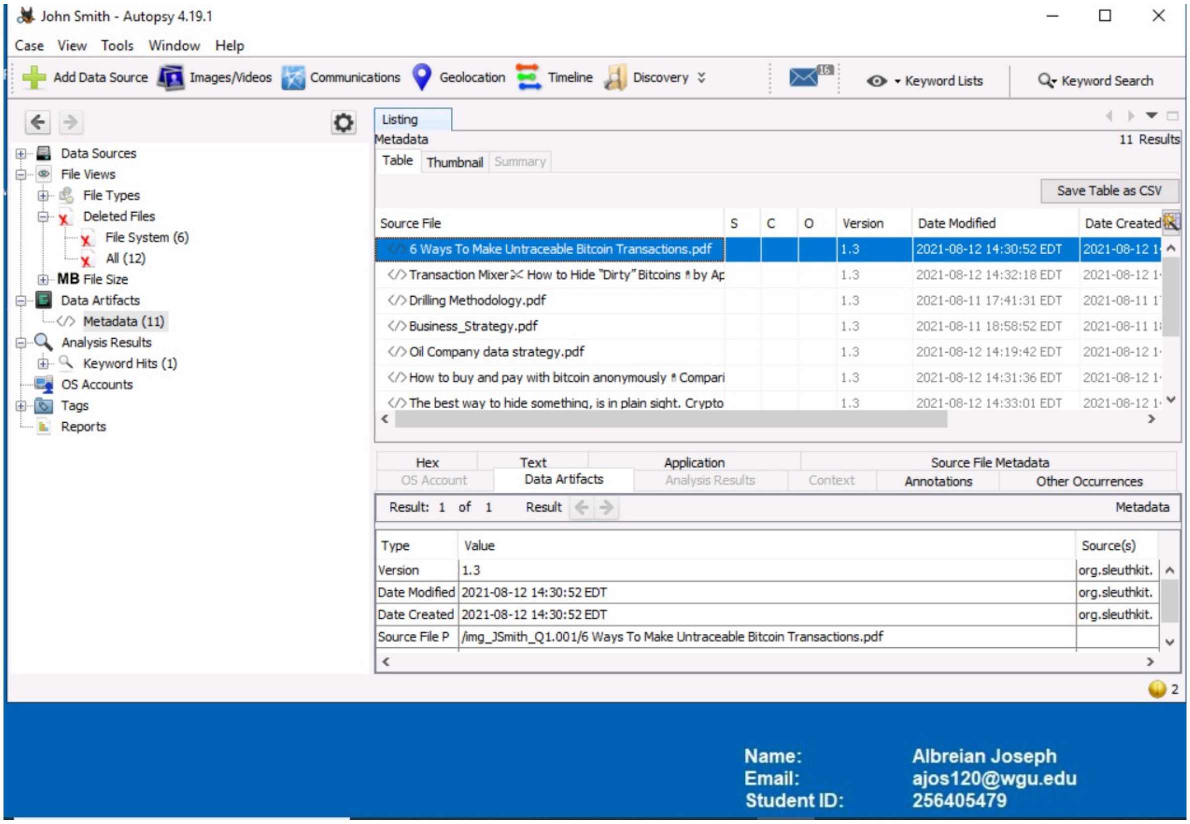


File System 6 Results

Name	S	C	O	Modified Time	Change Time	Acc
Business_Strategy.pdf			1	2021-08-11 14:58:54 EDT	0000-00-00 00:00:00	2021
Drilling Methodology.pdf			1	2021-08-11 13:41:32 EDT	0000-00-00 00:00:00	2021
How to buy and pay with bitcoin anonymously ⁝ Compari			1	2021-08-12 10:31:38 EDT	0000-00-00 00:00:00	2021
Oil_co_Conf.jpg			1	2021-08-12 10:24:02 EDT	0000-00-00 00:00:00	2021
Oilco_Conf2.jpg			1	2021-08-12 10:23:38 EDT	0000-00-00 00:00:00	2021
The best way to hide something, is in plain sight. Crypto			1	2021-08-12 10:33:02 EDT	0000-00-00 00:00:00	2021

Name: Albreian Joseph
Email: ajos120@wgu.edu
Student ID: 256405479

- In metadata a source file was found on how to hide “dirty” bitcoin and make them untraceable



Metadata

11 Results

Source File	S	C	O	Version	Date Modified	Date Created
6 Ways To Make Untraceable Bitcoin Transactions.pdf				1.3	2021-08-12 14:30:52 EDT	2021-08-12 1
Transaction Mixer ✂ How to Hide “Dirty” Bitcoins by Ap				1.3	2021-08-12 14:32:18 EDT	2021-08-12 1
Drilling Methodology.pdf				1.3	2021-08-11 17:41:31 EDT	2021-08-11 1
Business_Strategy.pdf				1.3	2021-08-11 18:58:52 EDT	2021-08-11 1
Oil Company data strategy.pdf				1.3	2021-08-12 14:19:42 EDT	2021-08-12 1
How to buy and pay with bitcoin anonymously Compari				1.3	2021-08-12 14:31:36 EDT	2021-08-12 1
The best way to hide something, is in plain sight. Crypto				1.3	2021-08-12 14:33:01 EDT	2021-08-12 1

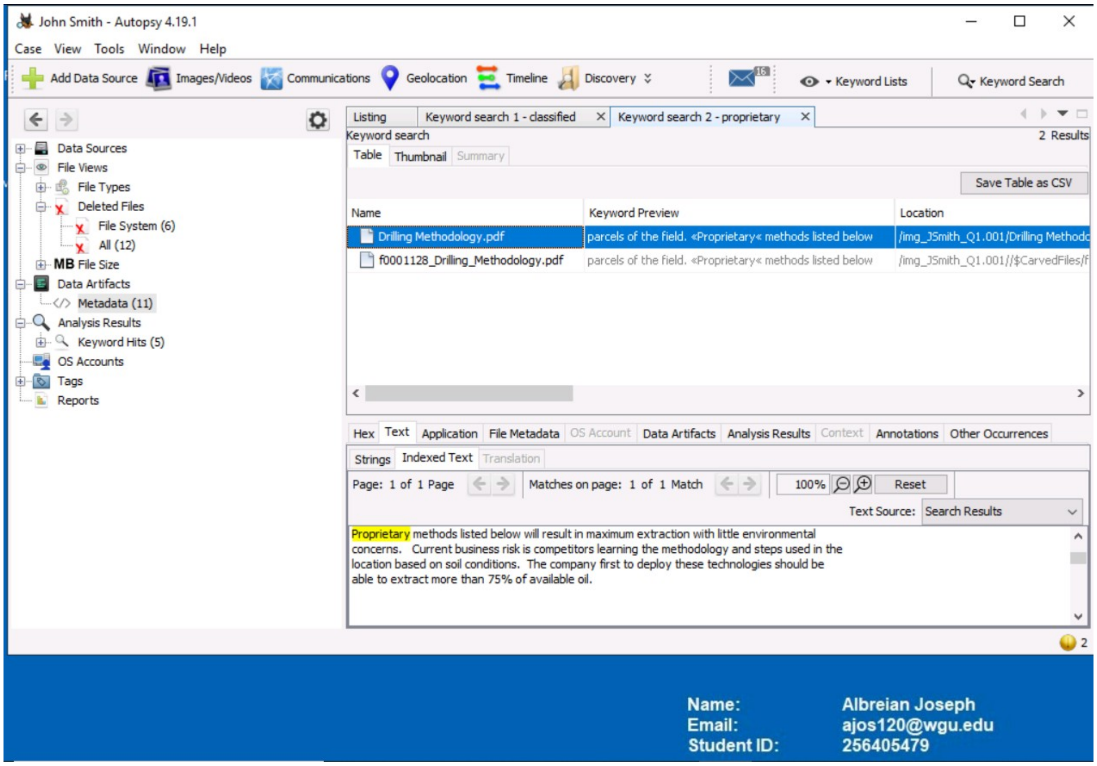
Result: 1 of 1 Result

Metadata

Type	Value	Source(s)
Version	1.3	org.sleuthkit.
Date Modified	2021-08-12 14:30:52 EDT	org.sleuthkit.
Date Created	2021-08-12 14:30:52 EDT	org.sleuthkit.
Source File P	/img_JSmith_Q1.001/6 Ways To Make Untraceable Bitcoin Transactions.pdf	

Name: Albreian Joseph
Email: ajos120@wgu.edu
Student ID: 256405479

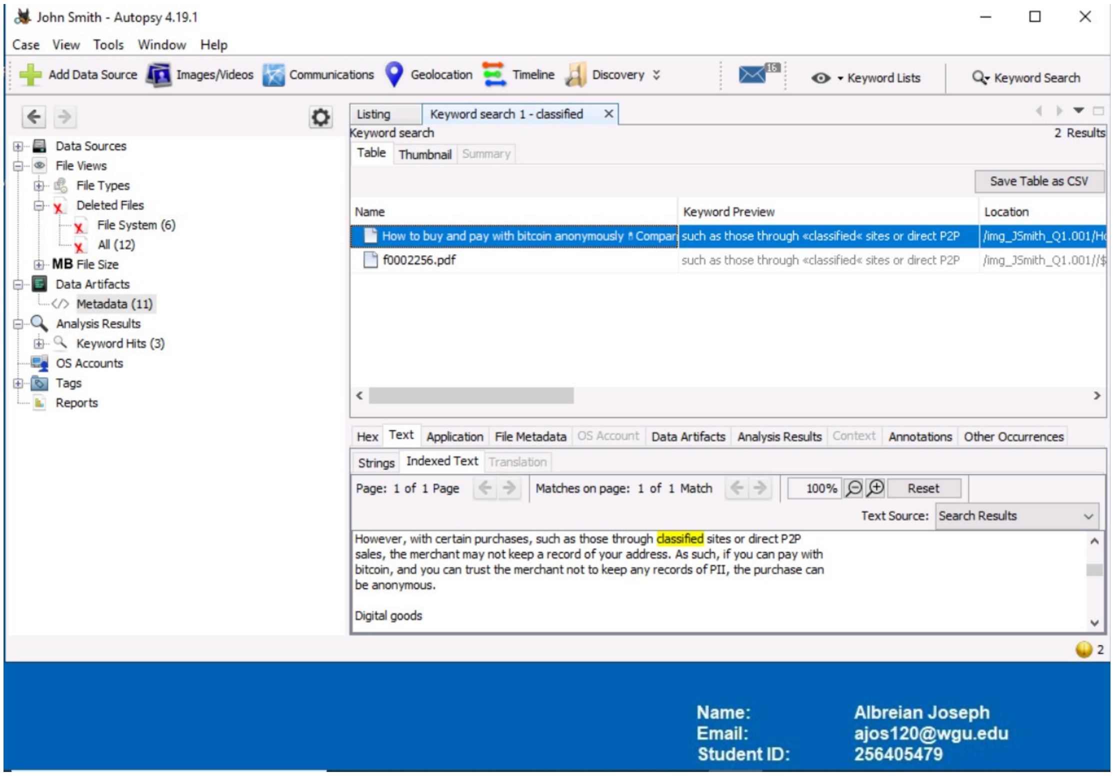
- When searching “Proprietary” and “Classified” the files below display:


John Smith - Autopsy 4.19.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery
Keyword Lists Keyword Search
Data Sources
File Views
File Types
Deleted Files
File System (6)
All (12)
MB File Size
Data Artifacts
Metadata (11)
Analysis Results
Keyword Hits (5)
OS Accounts
Tags
Reports
Listing
Keyword search 1 - classified
Keyword search 2 - proprietary
Keyword search
2 Results
Table Thumbnail Summary
Save Table as CSV
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Strings Indexed Text Translation
Page: 1 of 1 Page
Matches on page: 1 of 1 Match
100%
Reset
Text Source: Search Results

Name	Keyword Preview	Location
Drilling Methodology.pdf	parcels of the field. «Proprietary« methods listed below	/img_JSmith_Q1.001/Drilling Methodo
f0001128_Drilling_Methodology.pdf	parcels of the field. «Proprietary« methods listed below	/img_JSmith_Q1.001//$CarvedFiles/f

Proprietary methods listed below will result in maximum extraction with little environmental concerns. Current business risk is competitors learning the methodology and steps used in the location based on soil conditions. The company first to deploy these technologies should be able to extract more than 75% of available oil.

Name: Albreian Joseph
Email: ajos120@wgu.edu
Student ID: 256405479


John Smith - Autopsy 4.19.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery
Keyword Lists Keyword Search
Data Sources
File Views
File Types
Deleted Files
File System (6)
All (12)
MB File Size
Data Artifacts
Metadata (11)
Analysis Results
Keyword Hits (3)
OS Accounts
Tags
Reports
Listing
Keyword search 1 - classified
Keyword search
2 Results
Table Thumbnail Summary
Save Table as CSV
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Strings Indexed Text Translation
Page: 1 of 1 Page
Matches on page: 1 of 1 Match
100%
Reset
Text Source: Search Results

Name	Keyword Preview	Location
How to buy and pay with bitcoin anonymously • Compari	such as those through «classified« sites or direct P2P	/img_JSmith_Q1.001/H
f0002256.pdf	such as those through «classified« sites or direct P2P	/img_JSmith_Q1.001//$

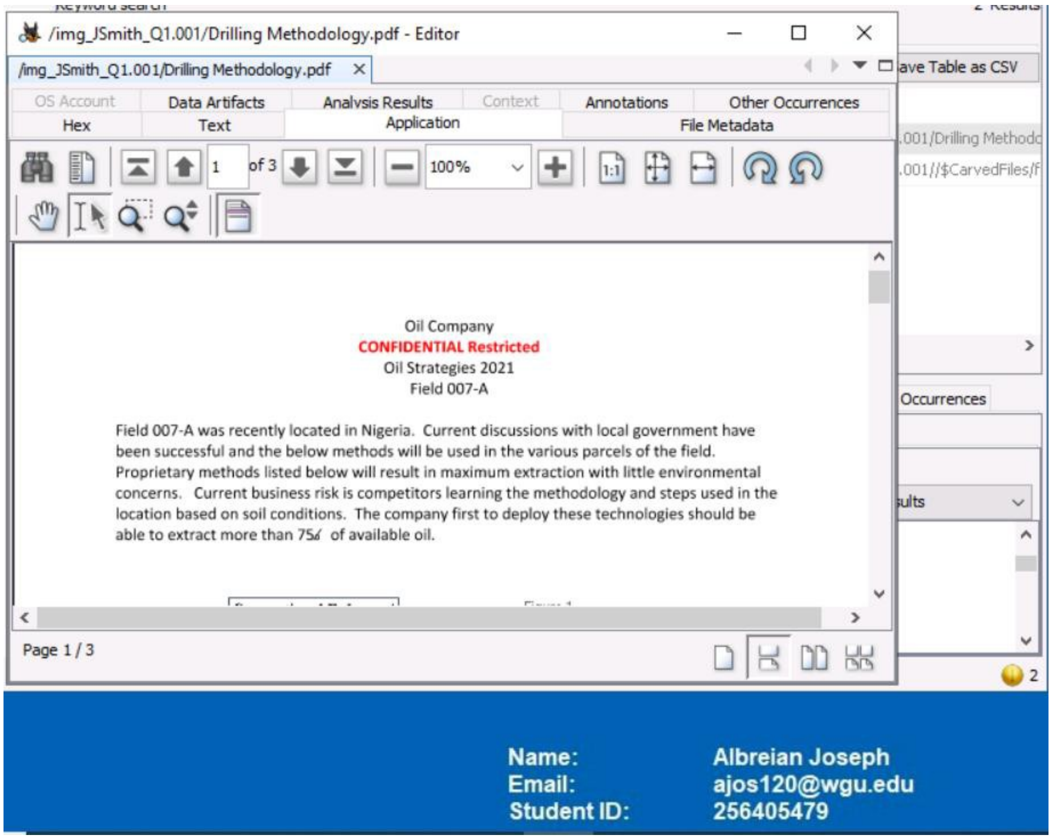
However, with certain purchases, such as those through classified sites or direct P2P sales, the merchant may not keep a record of your address. As such, if you can pay with bitcoin, and you can trust the merchant not to keep any records of PII, the purchase can be anonymous.

Digital goods

Name: Albreian Joseph
Email: ajos120@wgu.edu
Student ID: 256405479

III. Summarize the findings you identified during your investigation and the conclusions you made regarding the suspect and the collected evidence:

After conducting the investigation on the storage file Jsmith_Q1.001it is clear that John was accessing proprietary information that was not in his job description and did not have authorization to access. On his devices were sources named Business strategies, Drilling methodologies, and oil_co_config.jpg files and images. In his deleted files I discovered john attempting to figure out how to “hide something in plain sight, as well as to buy and pay with bitcoin anonymously. In his metadata file sources was an application source of how to hide “dirty” bitcoin. The imagines and evidence provided proves that John Smith was accessing source files that were not in his “need to know” status; there for John violated the companies’ policies.



Oil Company
CONFIDENTIAL Restricted
Oil Strategies 2021
Field 007-A

Field 007-A was recently located in Nigeria. Current discussions with local government have been successful and the below methods will be used in the various parcels of the field. Proprietary methods listed below will result in maximum extraction with little environmental concerns. Current business risk is competitors learning the methodology and steps used in the location based on soil conditions. The company first to deploy these technologies should be able to extract more than 75ó of available oil.

Name: Albreian Joseph
Email: ajos120@wgu.edu
Student ID: 256405479