Kiarah Pettaway

[redacted]

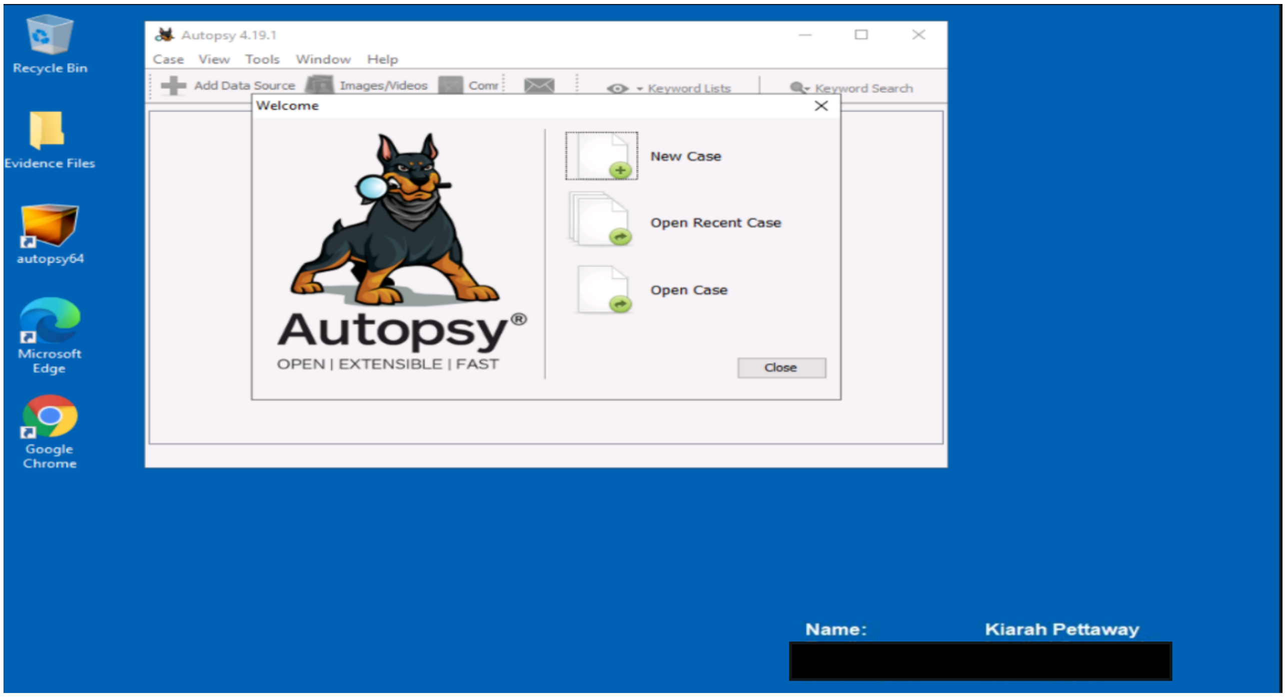
11/08/2024

D431 – Task 2

A1. Creating The Case

I began creating our case by selecting the autopsy64 application and curated a new case file by clicking “New Case”, as shown in Figure 1.

Figure 1

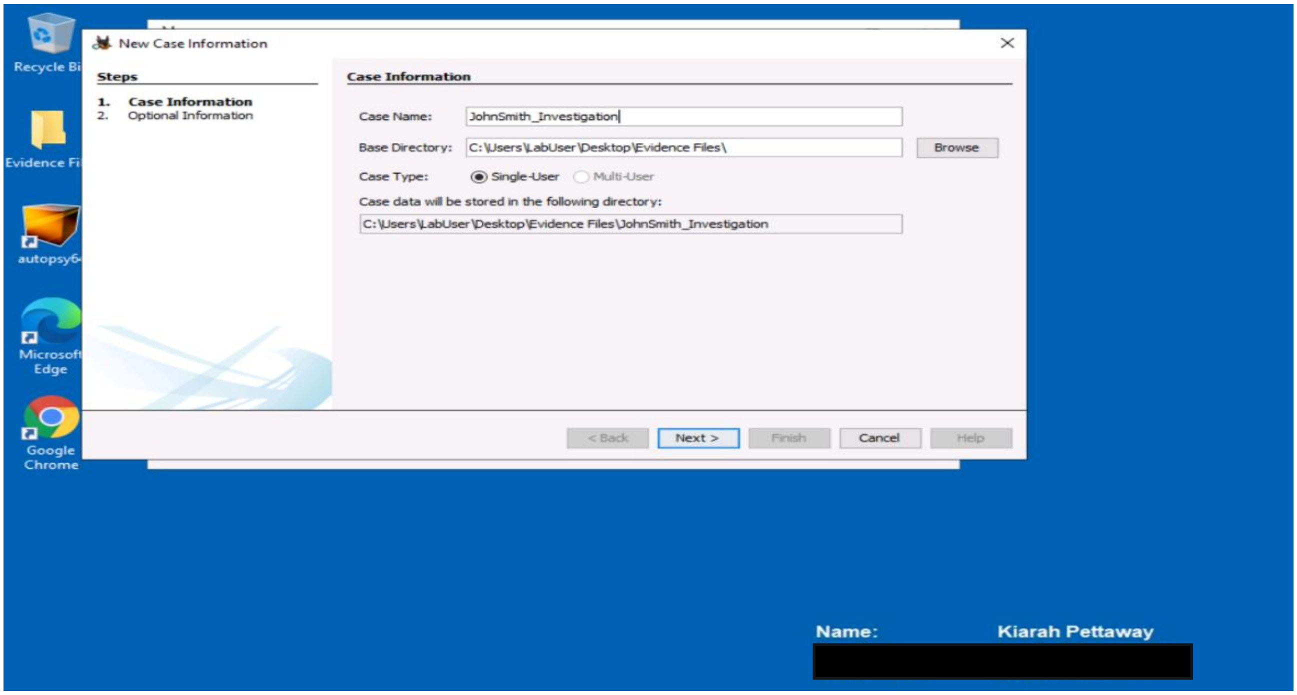


Name: Kiarah Pettaway

[redacted]

Upon the creation of the new case file, I set the directory to C:\Users\LabUser\Desktop\Evidence Files, so the data harvested from the workstation would be relatively easy to locate, as shown in Figure 2.

Figure 2



New Case Information

Steps

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

Case Information

Case Name: JohnSmith_Investigation

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

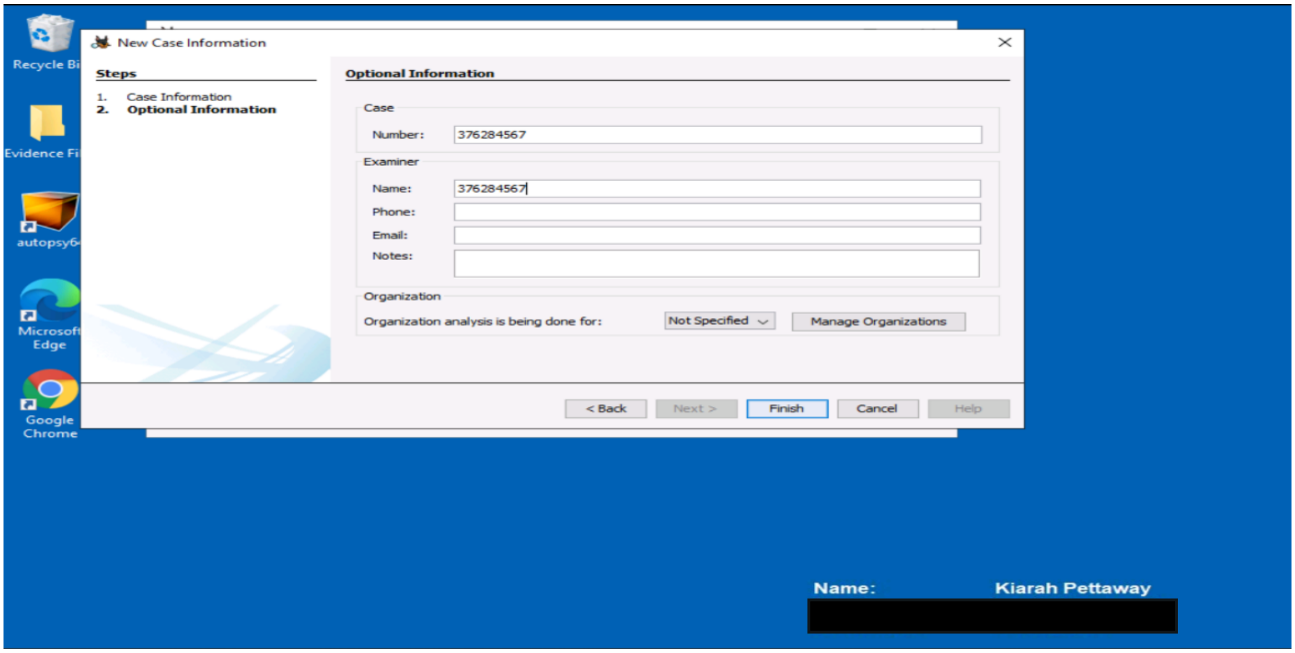
Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:
C:\Users\LabUser\Desktop\Evidence Files\JohnSmith_Investigation

Name: Kiarah Pettaway
[redacted]

In the next screen, I assigned the case number of 376284567 and proceeded to place the same number as the examiner as well, as shown in Figure 3.

Figure 3



New Case Information

Steps

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

Optional Information

Case
Number: 376284567

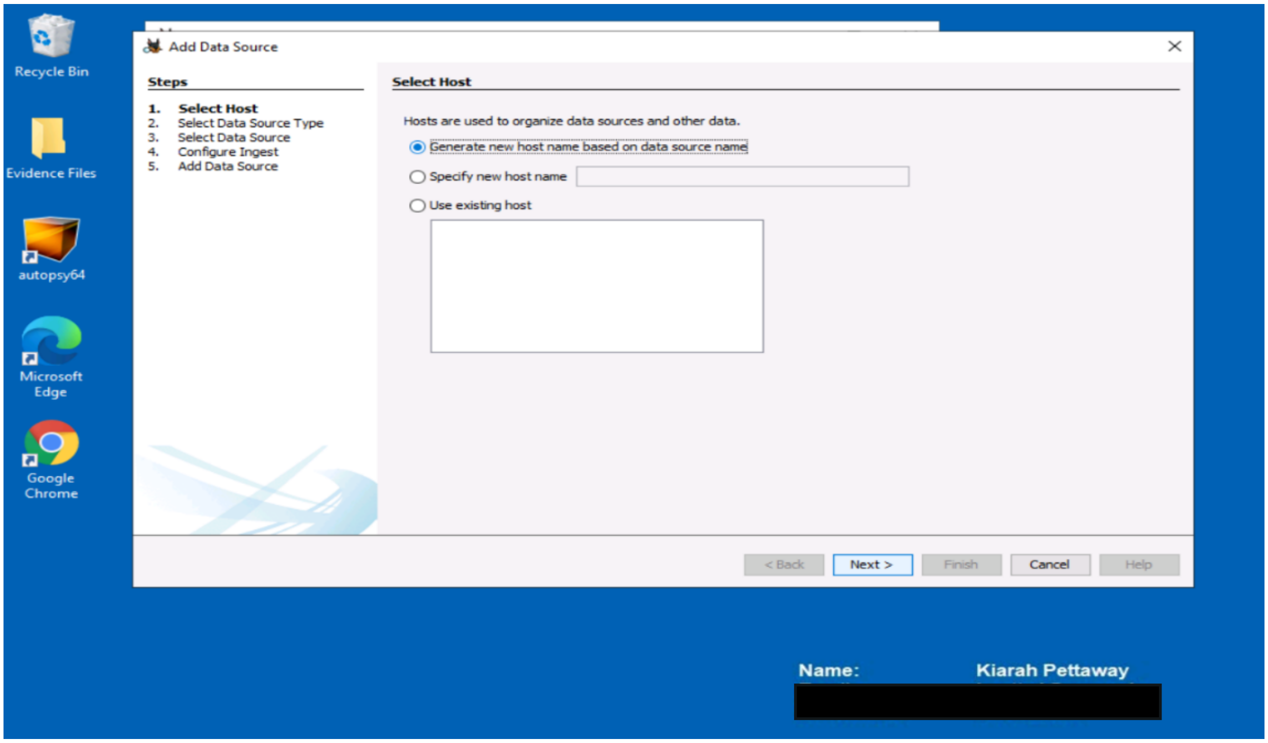
Examiner
Name: 376284567
Phone:
Email:
Notes:

Organization
Organization analysis is being done for: Not Specified

Name: Kiarah Pettaway
[redacted]

In Figure 4, I am prompted to choose a particular host, so I proceeded with the default settings.

Figure 4



Add Data Source

Steps

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

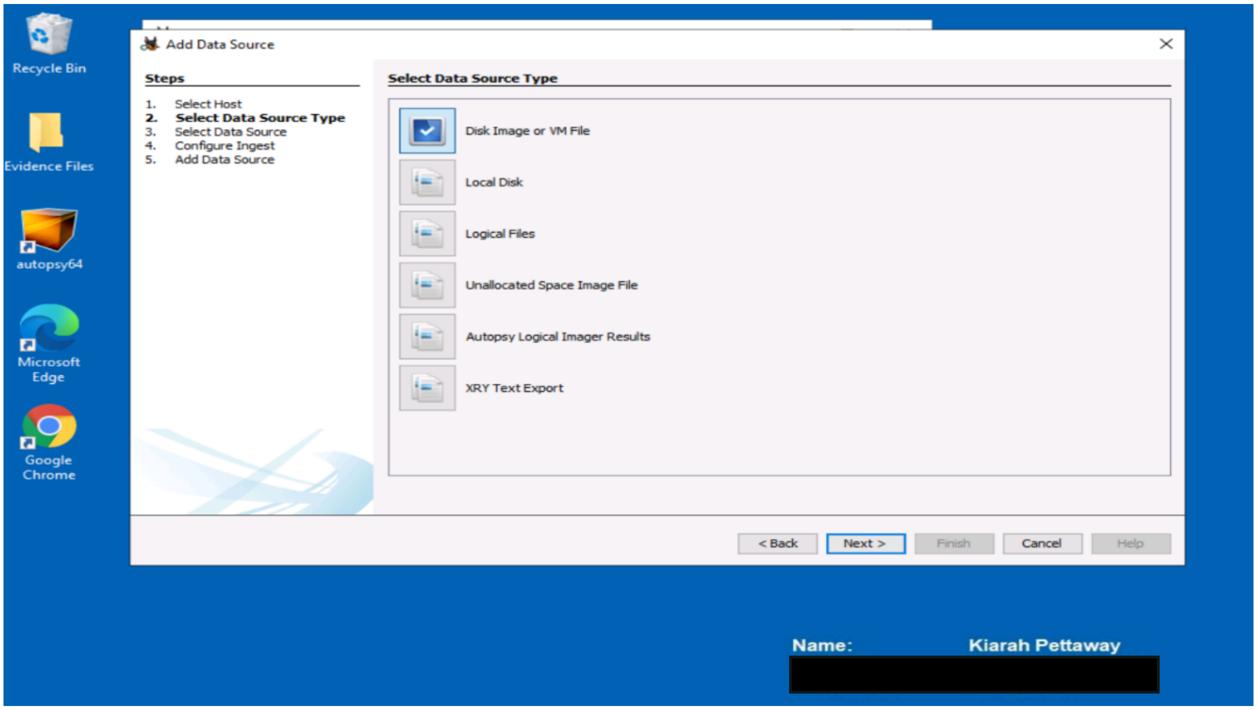
Select Host

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

Name: Kiarah Pettaway
[redacted]

The next screen prompted me with data source types to select from, and as shown in Figure 5, I proceeded to select “Disk Image/VM File.”



Steps

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

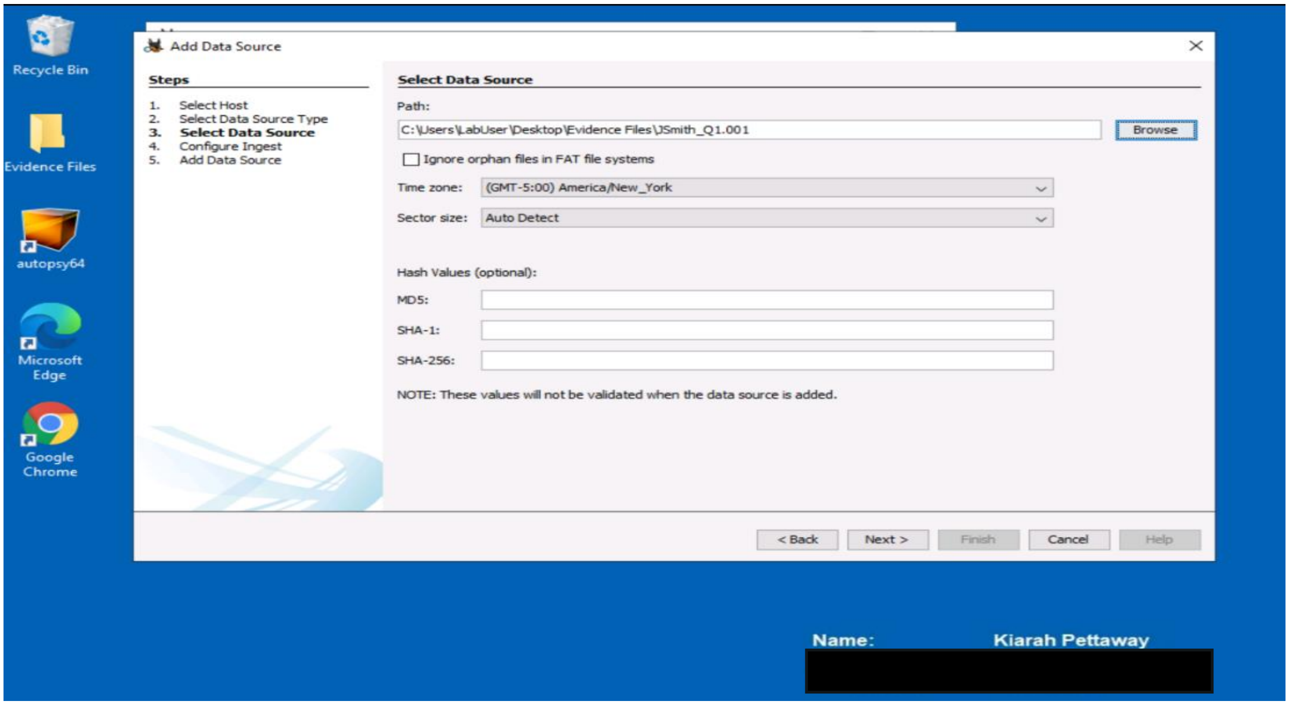
Select Data Source Type

- Disk Image or VM File
- Local Disk
- Logical Files
- Unallocated Space Image File
- Autopsy Logical Imager Results
- XRY Text Export

Name: Kiarah Pettaway
[redacted]

Figure 5

In Figure 6, I proceed with the next screen, which states to select a data source, and I navigated to the directory path then to the disk image that was curated during the forensic investigation from John Smith's company computer, which is in C:\Users\LabUser\Desktop\Evidence Files\JSmith_Q1.001 and moved forward to the next screen.



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.

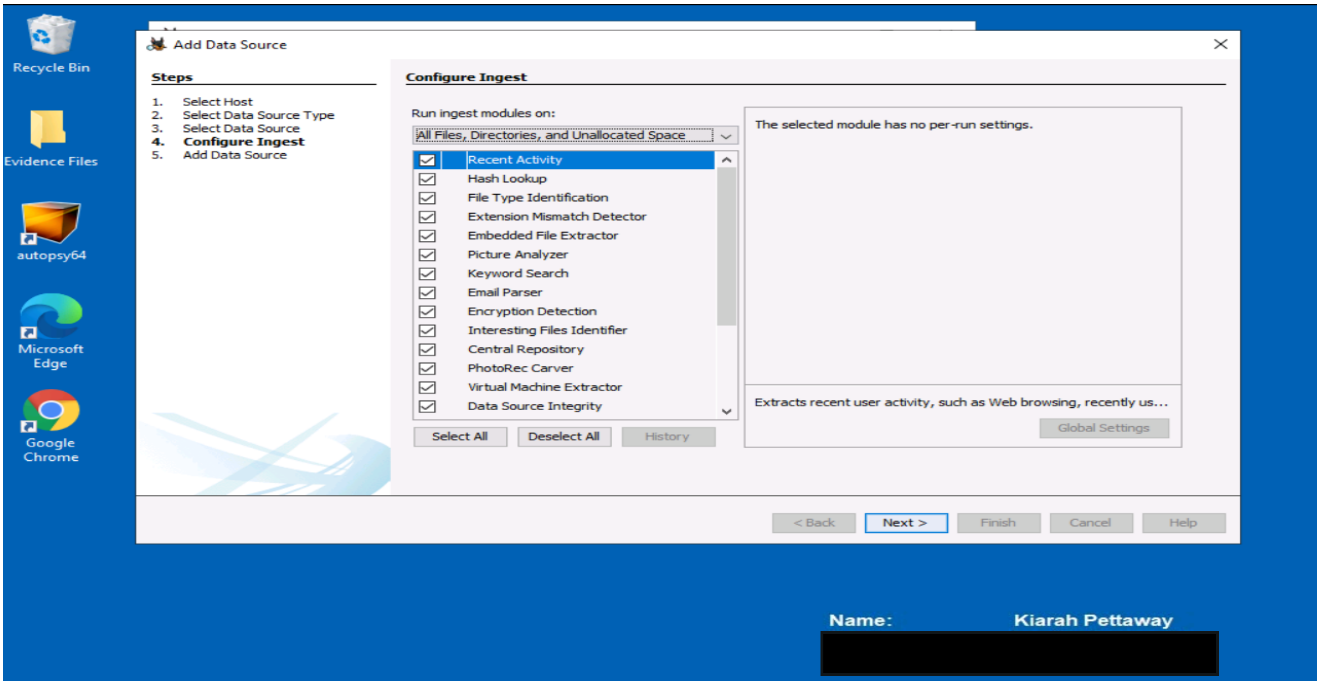
Name: Kiarah Pettaway

[redacted]

Figure 6

Proceeding, I was prompted to configure ingest modules, but kept the default configurations, as shown in Figure 7.

Figure 7



Add Data Source

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

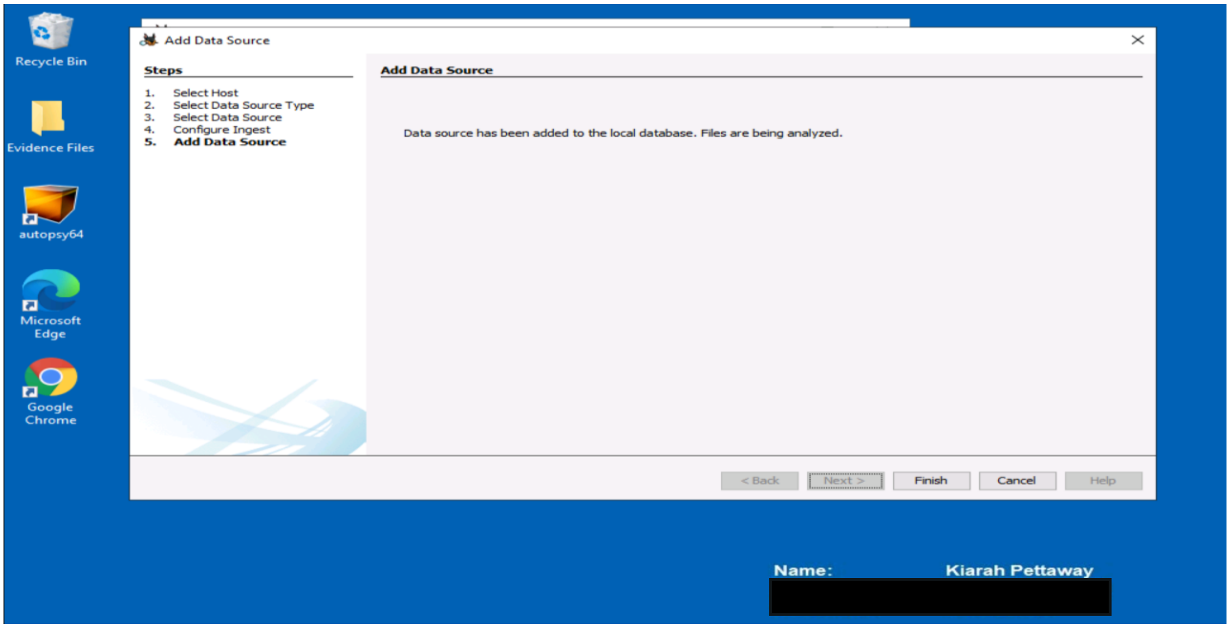
The selected module has no per-run settings.

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

Name: Kiarah Pettaway

[redacted]

In Figure 8, I proceed to click next, which Autopsy will begin loading data from “JSmith_Q1.001”, using the previous configurations from Figures 2-7, as shown in Figure 8.


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.

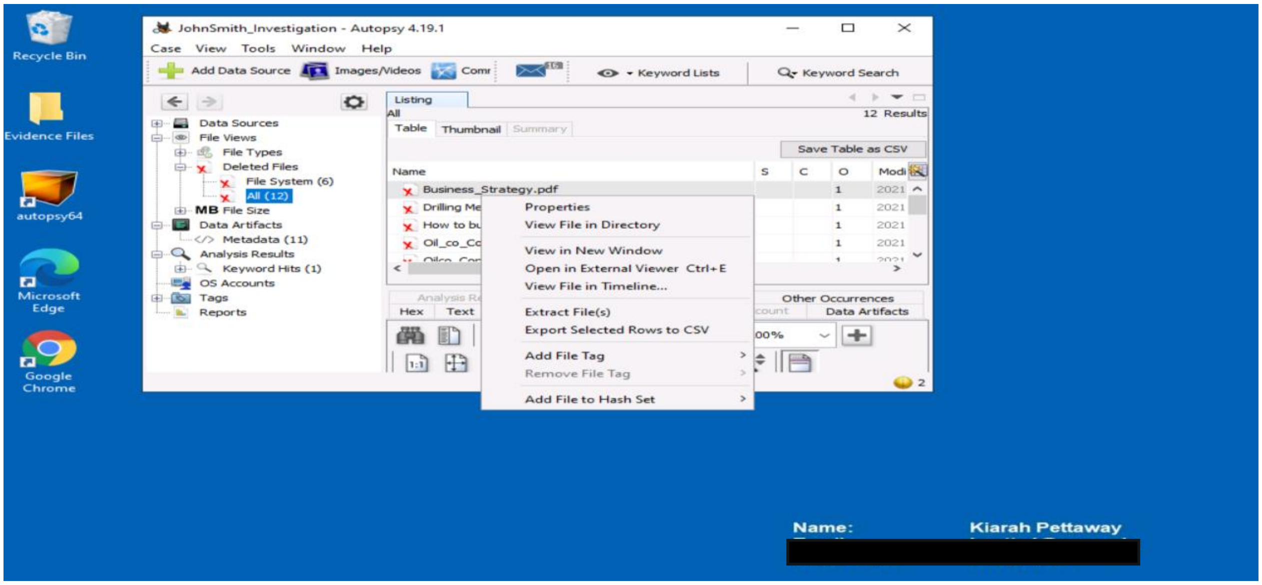
Name: Kiarah Pettaway
[redacted]

Figure 8

A2. Evidence Analysis

During our data analysis, we discovered a folder containing 12 deleted files from John Smith's workstation. These files require further examination, and to facilitate this, we will extract them to our workstation for closer inspection. The extraction location will be C:\Users\LabUser\Desktop\Evidence Files\JohnSmith_Investigation\Export, as shown in Figure 9.

Figure 9

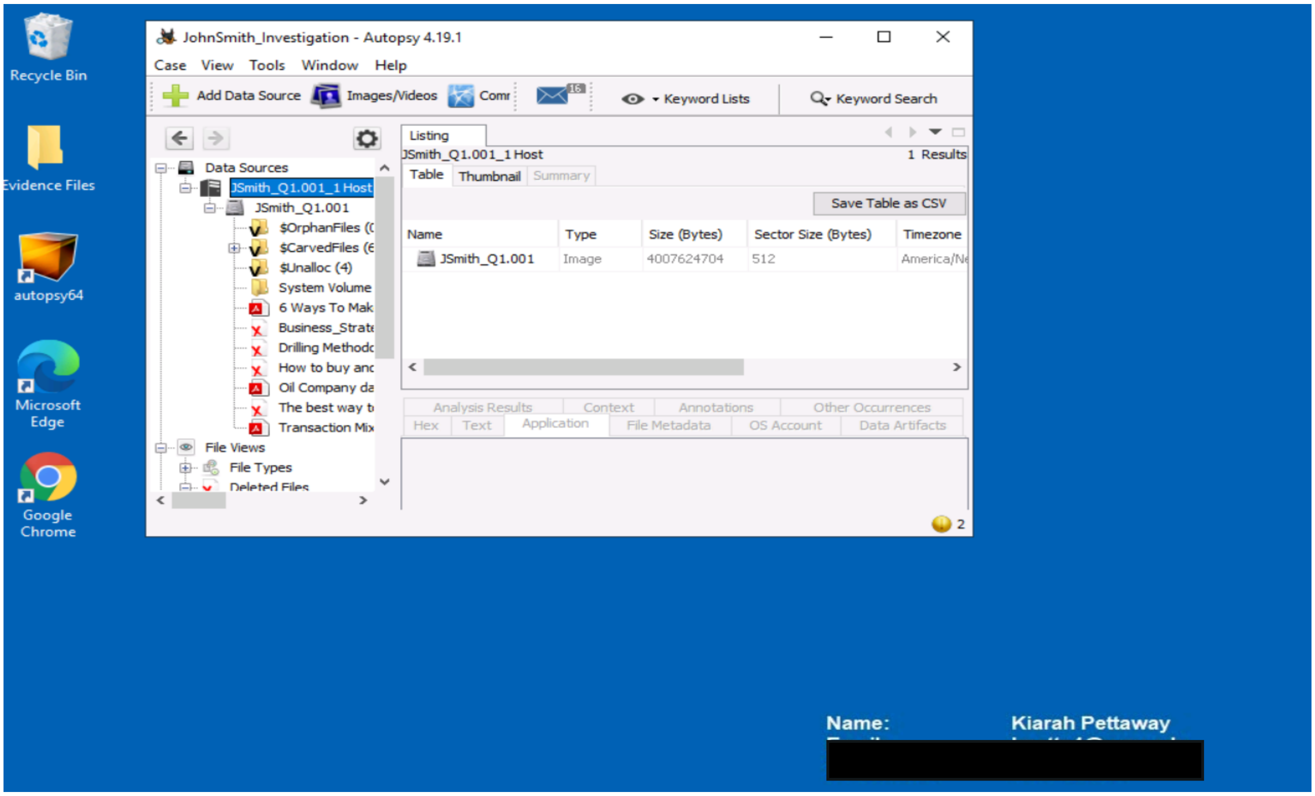


Name	S	C	O	Modi
Business_Strategy.pdf			1	2021
Drilling Me			1	2021
How to bu			1	2021
Oil_co_Co			1	2021

Name: Kiarah Pettaway
[redacted]

Once the deleted files are exported, we can access "JSmith_Q1.001 Host" followed by expanding "JSmith_Q1.001," allowing us to examine John’s files, as shown in Figures 10-11.

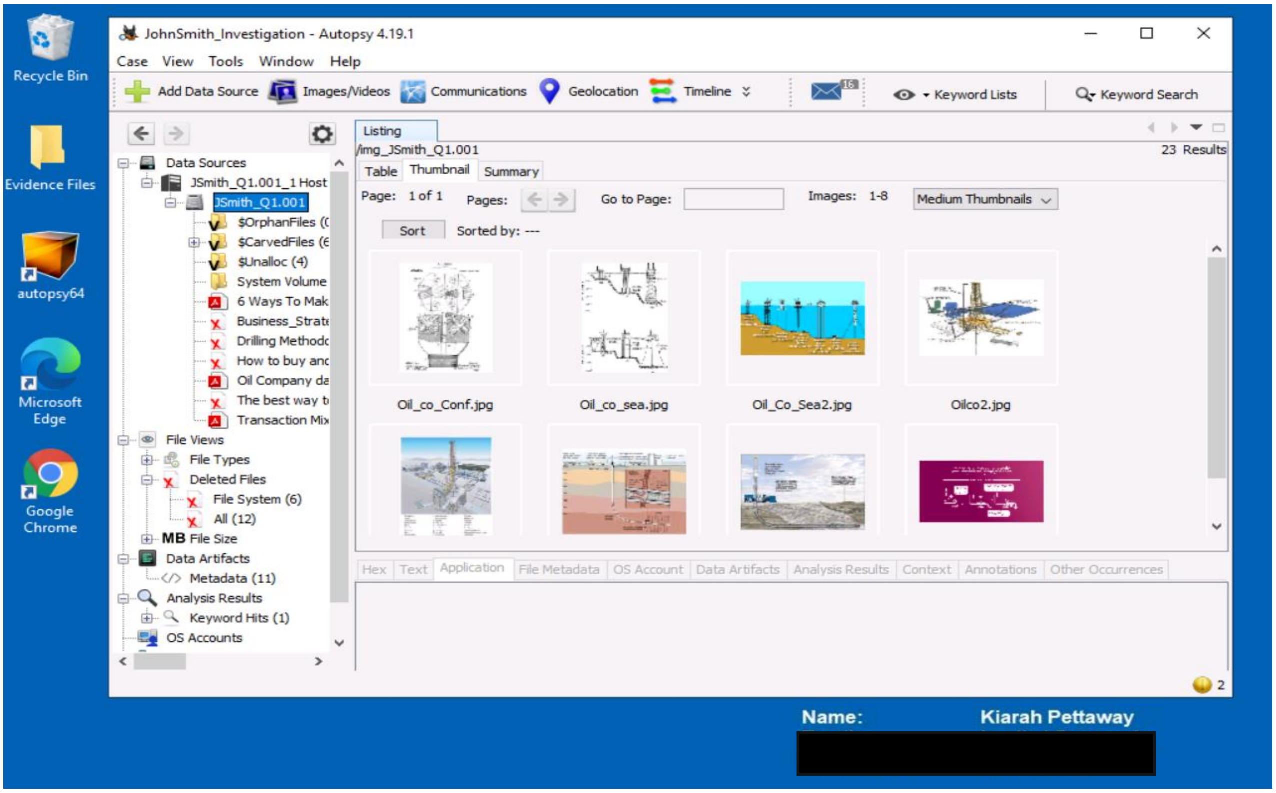
Figure 10



Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone
JSmith_Q1.001	Image	4007624704	512	America/N

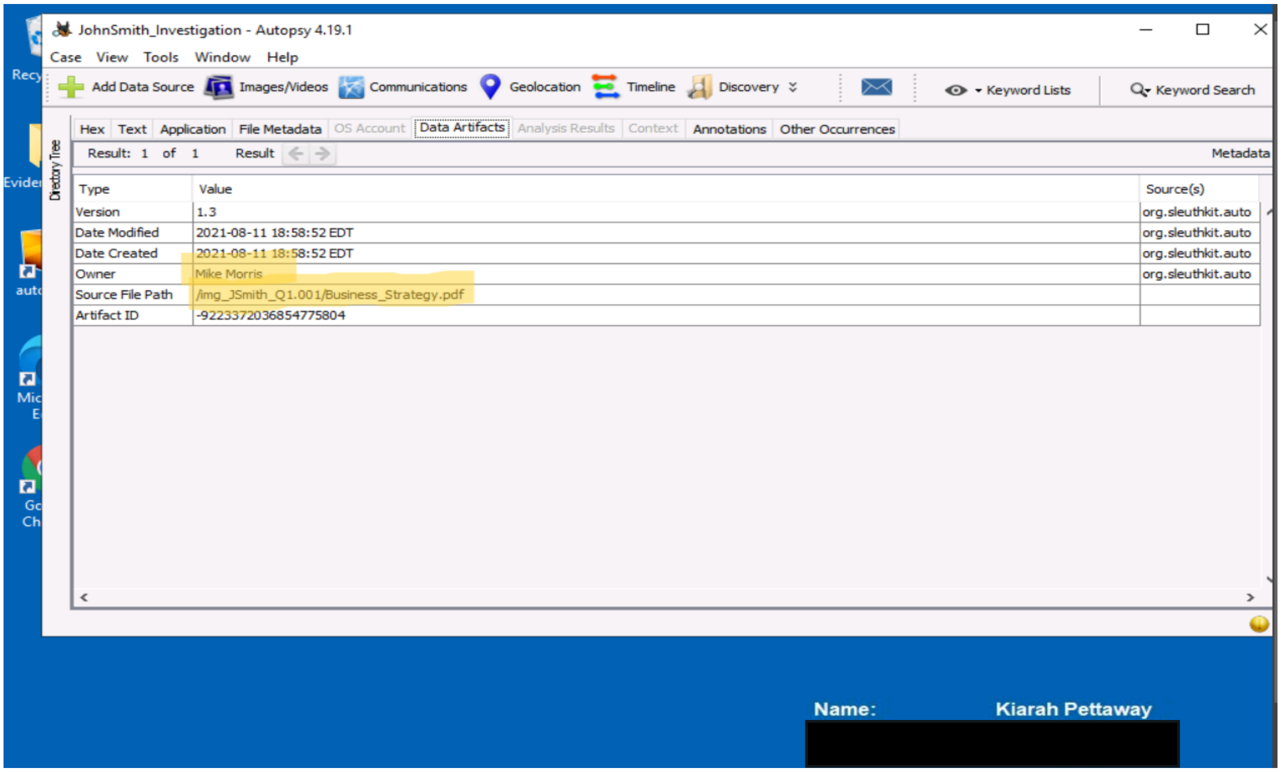
Name: Kiarah Pettaway
[redacted]

Figure 11



Name: Kiarah Pettaway
[redacted]

In Figure 12, we see the center of the application, in the Data Artifacts tab, in a file called “Business Strategy”, which is a PDF file. It shows the proprietary information attributed to "Mike Morris," who may be the owner of these files.



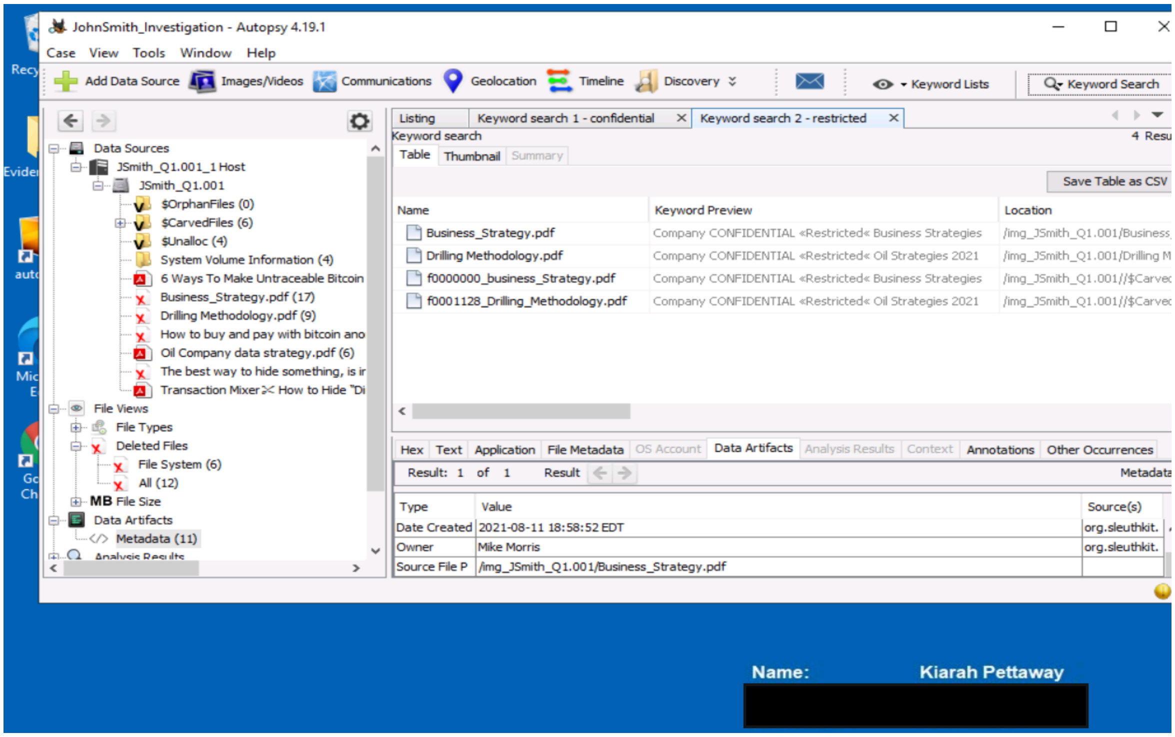
Type	Value	Source(s)
Version	1.3	org.sleuthkit.auto
Date Modified	2021-08-11 18:58:52 EDT	org.sleuthkit.auto
Date Created	2021-08-11 18:58:52 EDT	org.sleuthkit.auto
Owner	Mike Morris	org.sleuthkit.auto
Source File Path	/img_JSmith_Q1.001/Business_Strategy.pdf	
Artifact ID	-9223372036854775804	

Name: Kiarah Pettaway
[redacted]

Figure 12

Autopsy possesses a keyword search feature, which we utilized to find files with specific words such as “Proprietary”, “Confidential”, “Restricted”, and “Classified”, as shown in Figures 13-16.

Figure 13

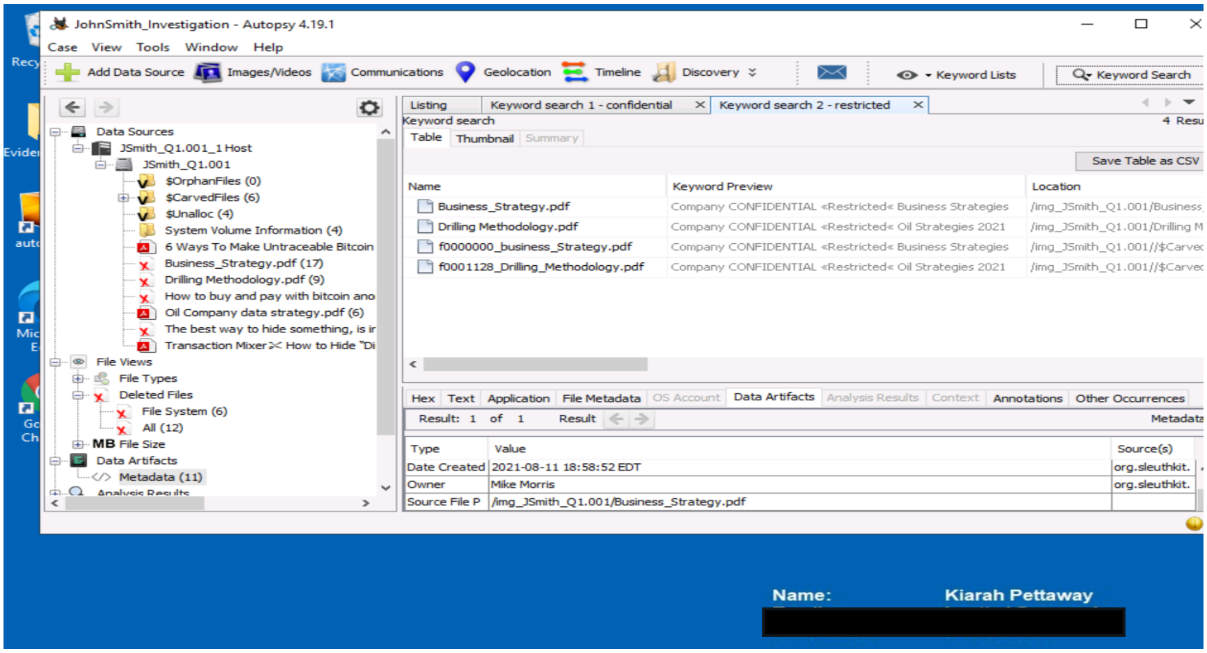

JohnSmith_Investigation - Autopsy 4.19.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Keyword Lists Keyword Search
Data Sources
JSmith_Q1.001_1 Host
JSmith_Q1.001
$OrphanFiles (0)
$CarvedFiles (6)
$Unalloc (4)
System Volume Information (4)
6 Ways To Make Untraceable Bitcoin
Business_Strategy.pdf (17)
Drilling Methodology.pdf (9)
How to buy and pay with bitcoin ano
Oil Company data strategy.pdf (6)
The best way to hide something, is ir
Transaction Mixer ✂ How to Hide "Di
File Views
File Types
Deleted Files
File System (6)
All (12)
MB File Size
Data Artifacts
Metadata (11)
Analysis Results
Listing Keyword search 1 - confidential Keyword search 2 - restricted
Keyword search
4 Resu
Table Thumbnail Summary
Save Table as CSV
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 1 of 1 Result
Metadata

Name	Keyword Preview	Location
Business_Strategy.pdf	Company CONFIDENTIAL «Restricted« Business Strategies	/img_JSmith_Q1.001/Business
Drilling Methodology.pdf	Company CONFIDENTIAL «Restricted« Oil Strategies 2021	/img_JSmith_Q1.001/Drilling M
f0000000_business_Strategy.pdf	Company CONFIDENTIAL «Restricted« Business Strategies	/img_JSmith_Q1.001//$Carvec
f0001128_Drilling_Methodology.pdf	Company CONFIDENTIAL «Restricted« Oil Strategies 2021	/img_JSmith_Q1.001//$Carvec

Type	Value	Source(s)
Date Created	2021-08-11 18:58:52 EDT	org.sleuthkit.
Owner	Mike Morris	org.sleuthkit.
Source File P	/img_JSmith_Q1.001/Business_Strategy.pdf	

Name: Kiarah Pettaway
[redacted]

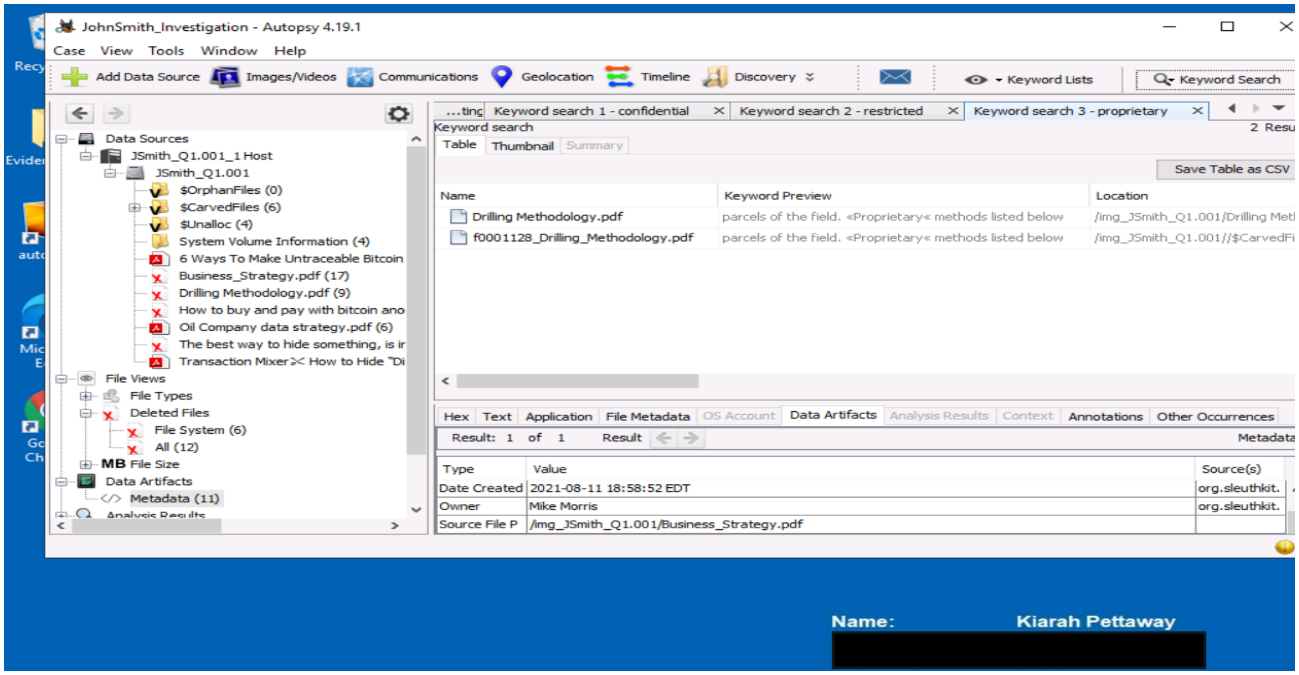
Figure 14


Name	Keyword Preview	Location
Business_Strategy.pdf	Company CONFIDENTIAL «Restricted« Business Strategies	/img_JSmith_Q1.001/Business
Drilling Methodology.pdf	Company CONFIDENTIAL «Restricted« Oil Strategies 2021	/img_JSmith_Q1.001/Drilling M
f0000000_business_Strategy.pdf	Company CONFIDENTIAL «Restricted« Business Strategies	/img_JSmith_Q1.001//$Carvec
f0001128_Drilling_Methodology.pdf	Company CONFIDENTIAL «Restricted« Oil Strategies 2021	/img_JSmith_Q1.001//$Carvec

Type	Value	Source(s)
Date Created	2021-08-11 18:58:52 EDT	org.sleuthkit.
Owner	Mike Morris	org.sleuthkit.
Source File P	/img_JSmith_Q1.001/Business_Strategy.pdf	

Name: Kiarah Pettaway
[redacted]

Figure 15



JohnSmith_Investigation - Autopsy 4.19.1

Case View Tools Window Help

Add Data Source | Images/Videos | Communications | Geolocation | Timeline | Discovery | Keyword Lists | Keyword Search

- Data Sources
  - JSmith_Q1.001_1 Host
    - JSmith_Q1.001
      - $OrphanFiles (0)
      - $CarvedFiles (6)
      - $Unalloc (4)
      - System Volume Information (4)
      - 6 Ways To Make Untraceable Bitcoin
      - Business_Strategy.pdf (17)
      - Drilling Methodology.pdf (9)
      - How to buy and pay with bitcoin ano
      - Oil Company data strategy.pdf (6)
      - The best way to hide something, is ir
      - Transaction Mixer ✂ How to Hide "Di
- File Views
  - File Types
  - Deleted Files
    - File System (6)
    - All (12)
  - MB File Size
- Data Artifacts
  - Metadata (11)
- Analysis Results

…ting | Keyword search 1 - confidential | Keyword search 2 - restricted | Keyword search 3 - proprietary

Keyword search — 2 Resu

Table | Thumbnail | Summary — Save Table as CSV

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

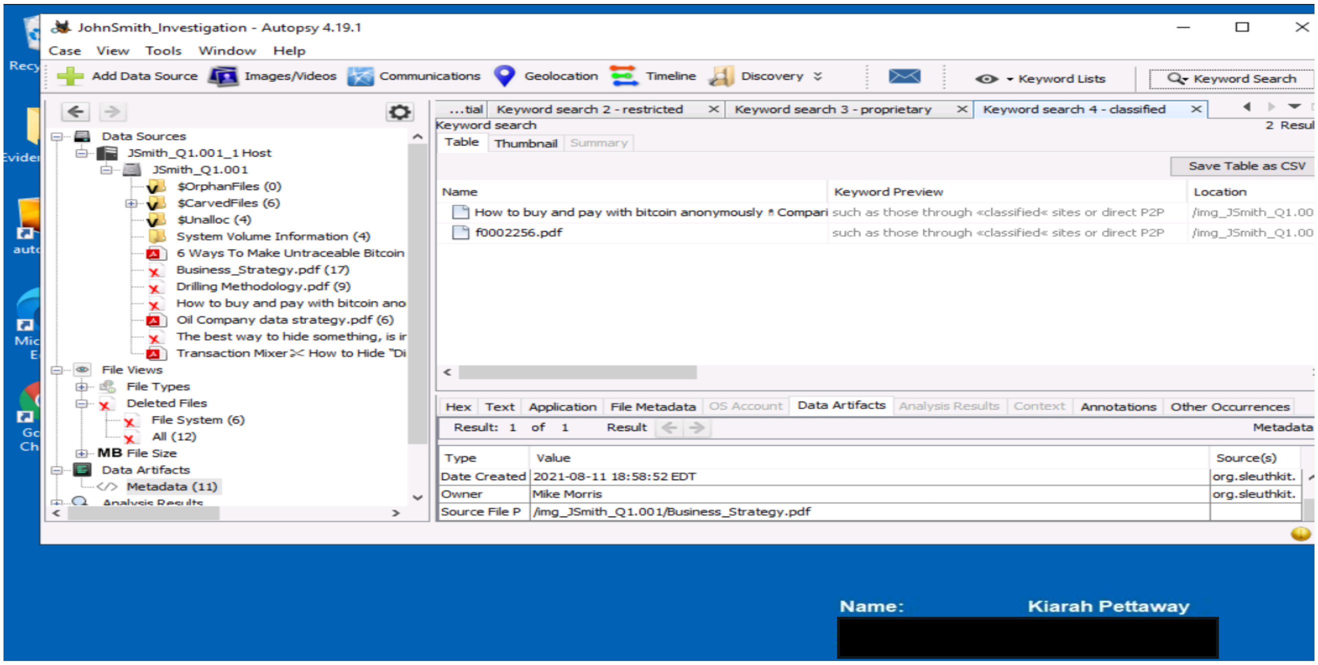
Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 1 of 1 Result — Metadata

Type	Value	Source(s)
Date Created	2021-08-11 18:58:52 EDT	org.sleuthkit.
Owner	Mike Morris	org.sleuthkit.
Source File P	/img_JSmith_Q1.001/Business_Strategy.pdf	

Name: Kiarah Pettaway
[redacted]

Figure 16



JohnSmith_Investigation - Autopsy 4.19.1

Case View Tools Window Help

Add Data Source | Images/Videos | Communications | Geolocation | Timeline | Discovery | Keyword Lists | Keyword Search

- Data Sources
  - JSmith_Q1.001_1 Host
    - JSmith_Q1.001
      - $OrphanFiles (0)
      - $CarvedFiles (6)
      - $Unalloc (4)
      - System Volume Information (4)
      - 6 Ways To Make Untraceable Bitcoin
      - Business_Strategy.pdf (17)
      - Drilling Methodology.pdf (9)
      - How to buy and pay with bitcoin ano
      - Oil Company data strategy.pdf (6)
      - The best way to hide something, is ir
      - Transaction Mixer ✂ How to Hide "Di
- File Views
  - File Types
  - Deleted Files
    - File System (6)
    - All (12)
  - MB File Size
- Data Artifacts
  - Metadata (11)
- Analysis Results

…tial | Keyword search 2 - restricted | Keyword search 3 - proprietary | Keyword search 4 - classified

Keyword search — 2 Resul

Table | Thumbnail | Summary — Save Table as CSV

Name	Keyword Preview	Location
How to buy and pay with bitcoin anonymously ⚠ Compari	such as those through «classified« sites or direct P2P	/img_JSmith_Q1.00
f0002256.pdf	such as those through «classified« sites or direct P2P	/img_JSmith_Q1.00

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

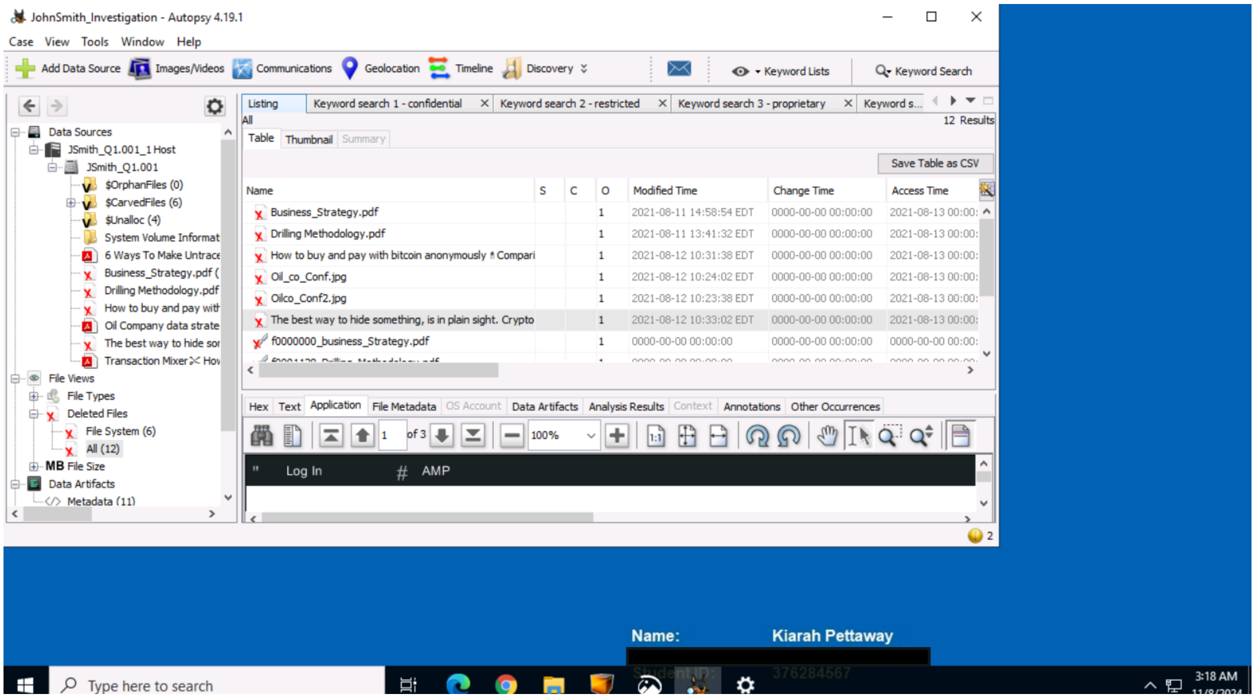
Result: 1 of 1 Result — Metadata

Type	Value	Source(s)
Date Created	2021-08-11 18:58:52 EDT	org.sleuthkit.
Owner	Mike Morris	org.sleuthkit.
Source File P	/img_JSmith_Q1.001/Business_Strategy.pdf	

Name: Kiarah Pettaway
[redacted]

Upon deeper inspection, we find several suspicious files in John Smith's possession, which are critical to the oil company's infrastructure, such as "Drilling Methodology", "Business Strategies", etc. which can be helpful for its competitors, also known as potential trade secrets, as shown in Figures 17-20.

Figure 17



All

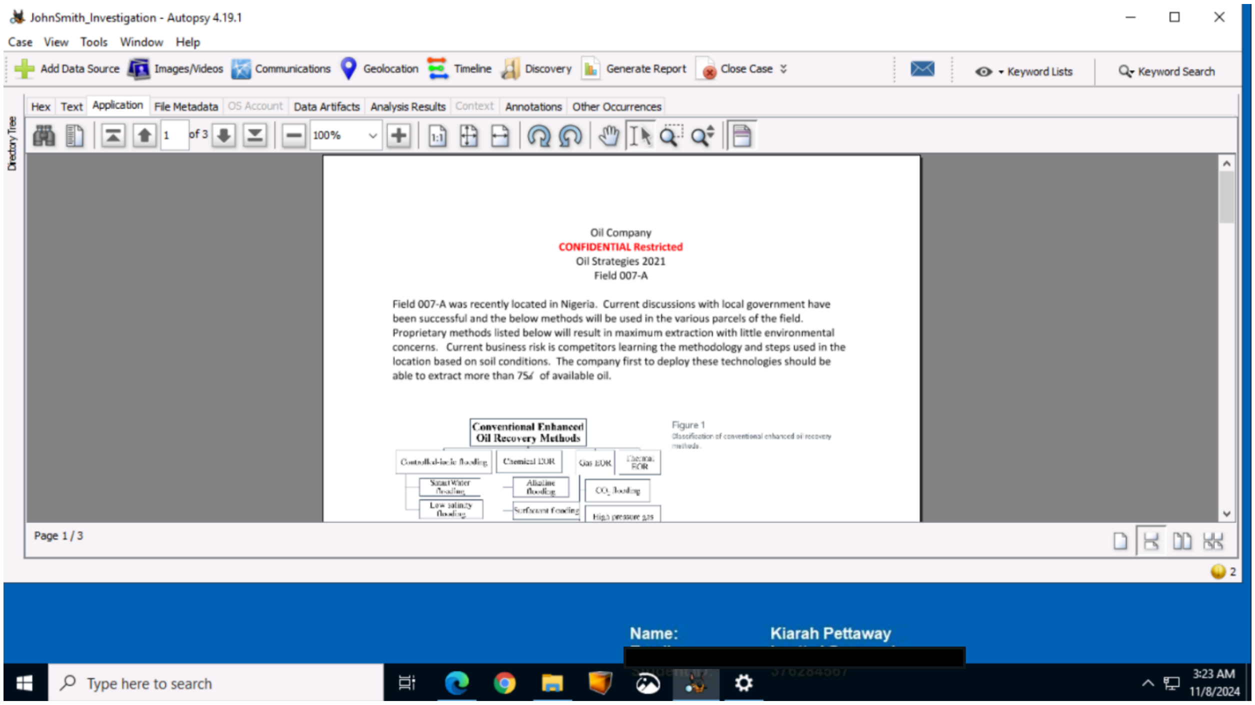
12 Results

Name	S	C	O	Modified Time	Change Time	Access Time
Business_Strategy.pdf			1	2021-08-11 14:58:54 EDT	0000-00-00 00:00:00	2021-08-13 00:00:
Drilling Methodology.pdf			1	2021-08-11 13:41:32 EDT	0000-00-00 00:00:00	2021-08-13 00:00:
How to buy and pay with bitcoin anonymously ⁸ Compari			1	2021-08-12 10:31:38 EDT	0000-00-00 00:00:00	2021-08-13 00:00:
Oil_co_Conf.jpg			1	2021-08-12 10:24:02 EDT	0000-00-00 00:00:00	2021-08-13 00:00:
Oilco_Conf2.jpg			1	2021-08-12 10:23:38 EDT	0000-00-00 00:00:00	2021-08-13 00:00:
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	2021-08-13 00:00:
f0000000_business_Strategy.pdf			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:

Name: Kiarah Pettaway

[redacted]

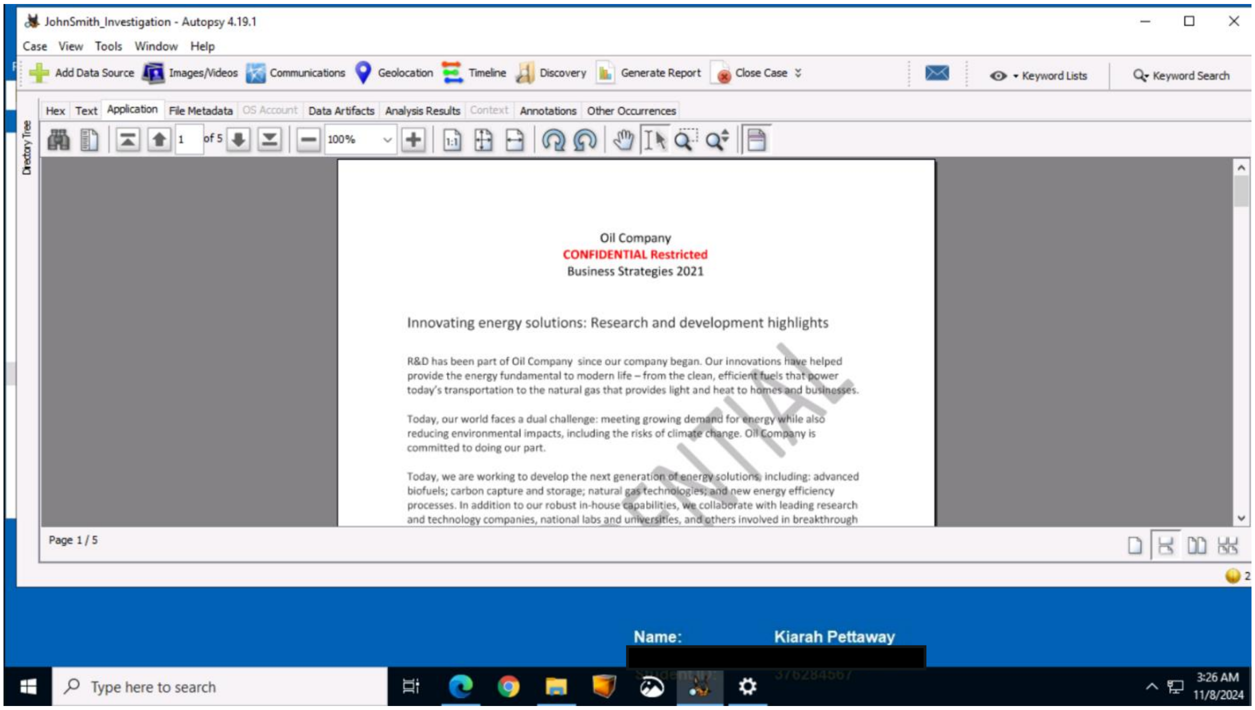
Figure 18


JohnSmith_Investigation - Autopsy 4.19.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
1 of 3 100%
Directory Tree
Conventional Enhanced Oil Recovery Methods
Controlled-ionic flooding
Chemical EOR
Gas EOR
Thermal EOR
Smart Water flooding
Low salinity flooding
Alkaline flooding
Surfactant flooding
CO2 flooding
High pressure gas
Figure 1
Classification of conventional enhanced oil recovery methods.
Page 1 / 3
Type here to search
3:23 AM
11/8/2024

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 75⁄ of available oil.

Name: Kiarah Pettaway
[redacted]


JohnSmith_Investigation - Autopsy 4.19.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
1 of 5 100%
Directory Tree
Page 1 / 5
Type here to search
3:26 AM
11/8/2024

Oil Company
CONFIDENTIAL Restricted
Business Strategies 2021

Innovating energy solutions: Research and development highlights

R&D has been part of Oil Company since our company began. Our innovations have helped provide the energy fundamental to modern life – from the clean, efficient fuels that power today's transportation to the natural gas that provides light and heat to homes and businesses.

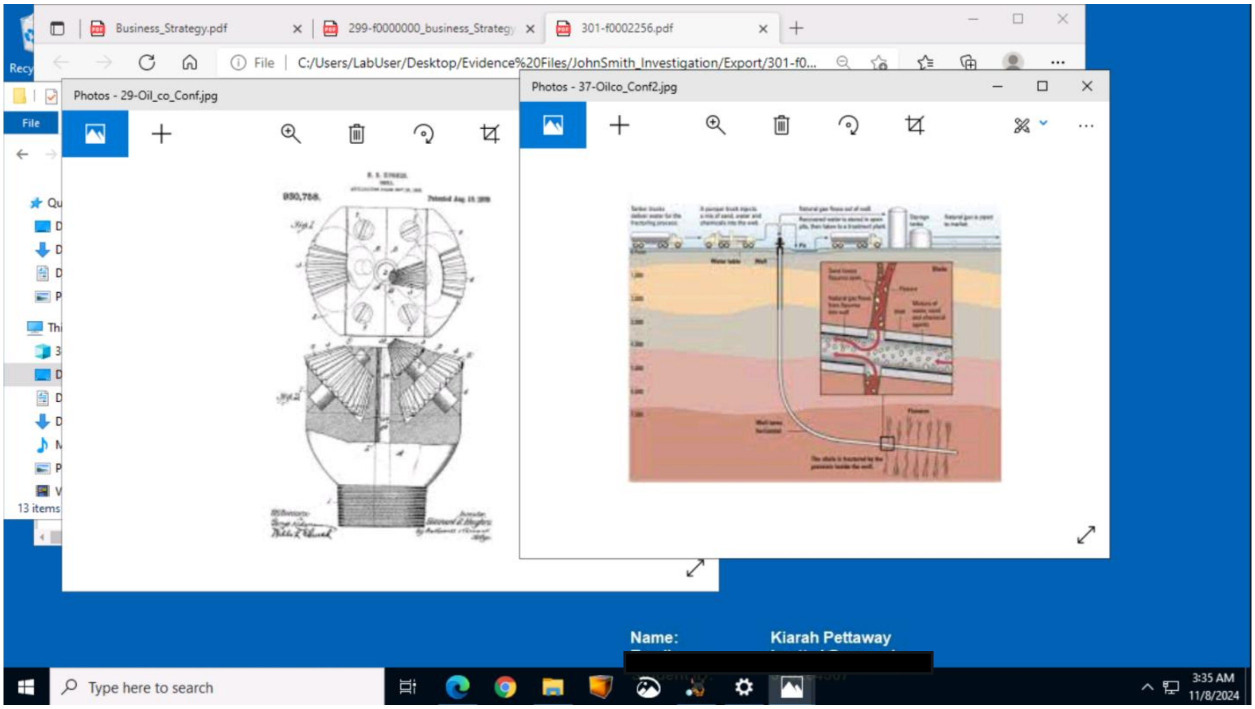
Today, our world faces a dual challenge: meeting growing demand for energy while also reducing environmental impacts, including the risks of climate change. Oil Company is committed to doing our part.

Today, we are working to develop the next generation of energy solutions, including: advanced biofuels; carbon capture and storage; natural gas technologies; and new energy efficiency processes. In addition to our robust in-house capabilities, we collaborate with leading research and technology companies, national labs and universities, and others involved in breakthrough

Name: Kiarah Pettaway
[redacted]

Figure 19

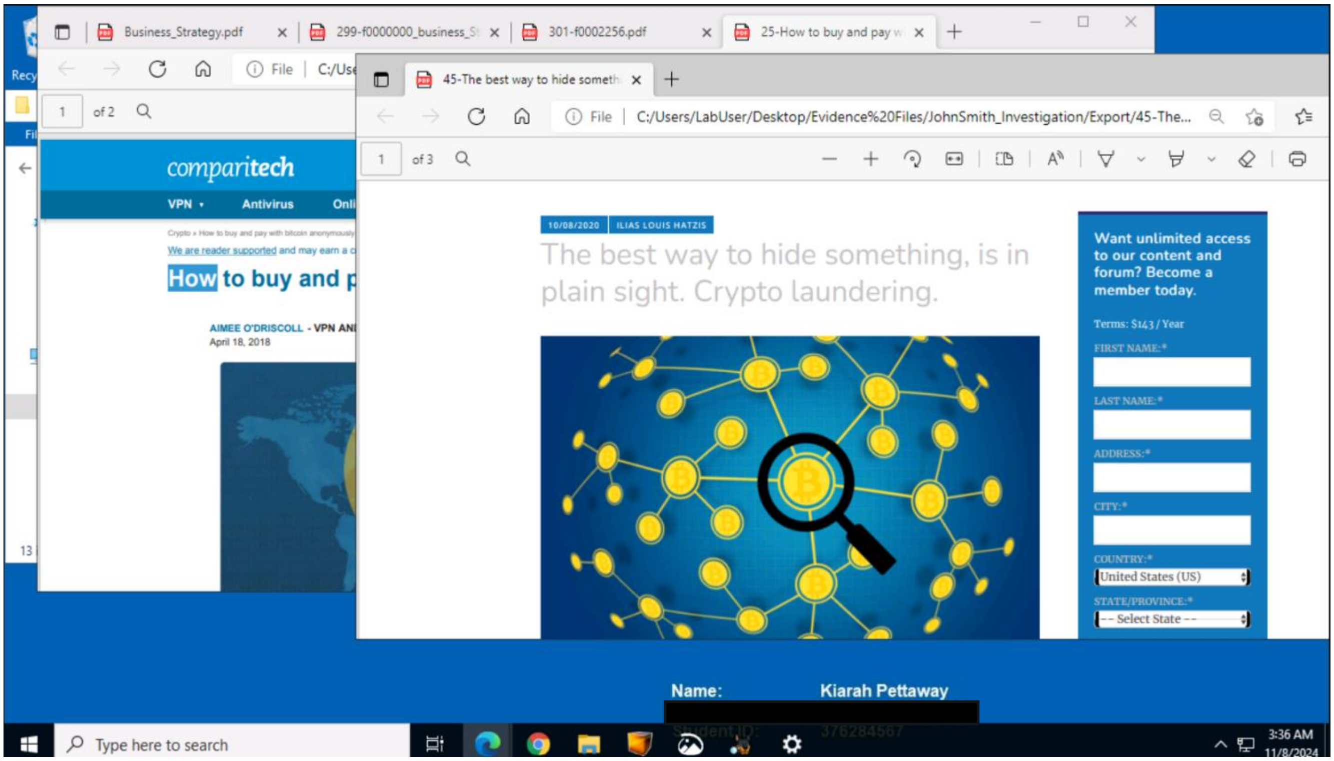
Figure 20


Business_Strategy.pdf
299-f0000000_business_Strategy
301-f0002256.pdf
File | C:/Users/LabUser/Desktop/Evidence%20Files/JohnSmith_Investigation/Export/301-f0...
Photos - 29-Oil_co_Conf.jpg
Photos - 37-Oilco_Conf2.jpg
File
13 items
Type here to search
3:35 AM
11/8/2024

Name: Kiarah Pettaway
[redacted]

In our final findings, with John already in possession of proprietary, confidential, restricted, and classified information; we also find files pertaining to anonymity by utilizing cryptocurrency and general mitigation techniques, such as “The Best Way to Hide Something in Plain Sight”, as shown in Figure 21.

Figure 21



How to buy and p

AIMEE O'DRISCOLL - VPN ANI
April 18, 2018

10/08/2020 | ILIAS LOUIS HATZIS

The best way to hide something, is in plain sight. Crypto laundering.

Want unlimited access to our content and forum? Become a member today.

Terms: $143 / Year

FIRST NAME:*

LAST NAME:*

ADDRESS:*

CITY:*

COUNTRY:* United States (US)

STATE/PROVINCE:* -- Select State --

Name: Kiarah Pettaway

[redacted]

A3. Conclusion

Following a comprehensive review of John Smith's workstation, we identified several instances that suggest a breach of company policies regarding access to proprietary, confidential, restricted, and classified information. Specifically, documents such as "Drilling Methodology.pdf," confidential diagrams, and "Business Strategy.pdf" raise concerns in relation to the Non-Disclosure Agreement. Furthermore, his involvement in financial transactions through anonymous cryptocurrency channels does not align with the Acceptable Use Policy.