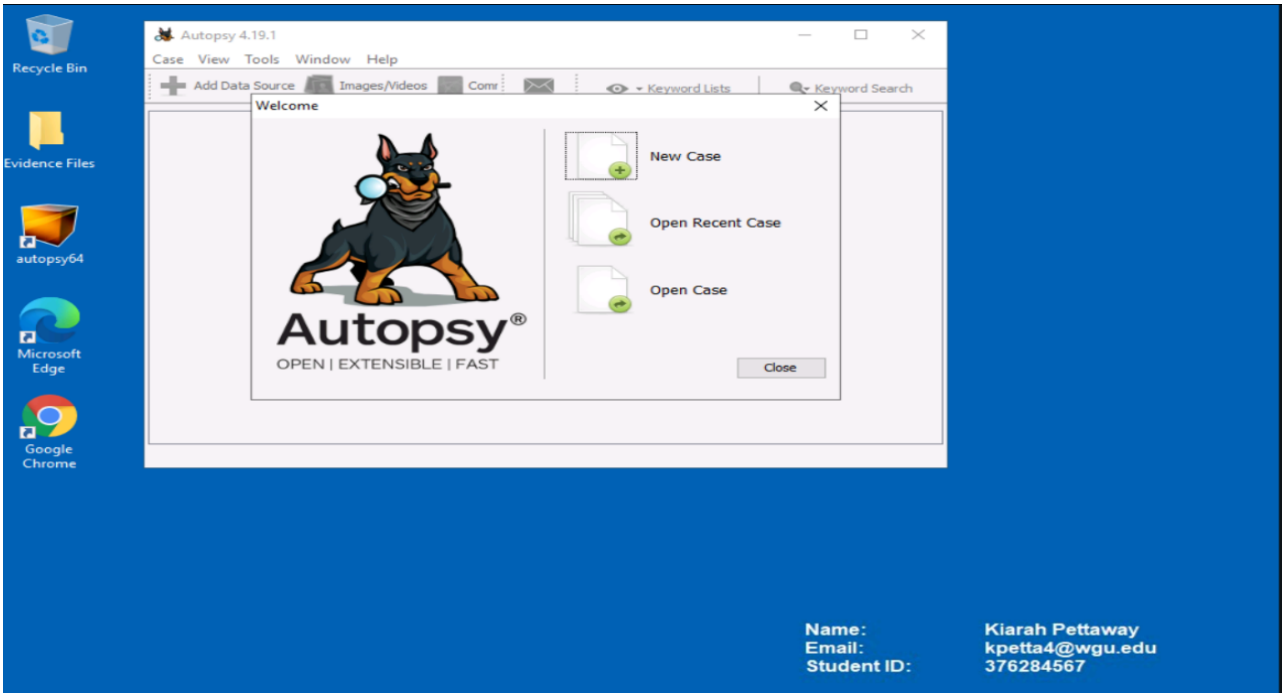
Kiarah Pettaway
ID: 011015177
11/08/2024
D431 – Task 2

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.

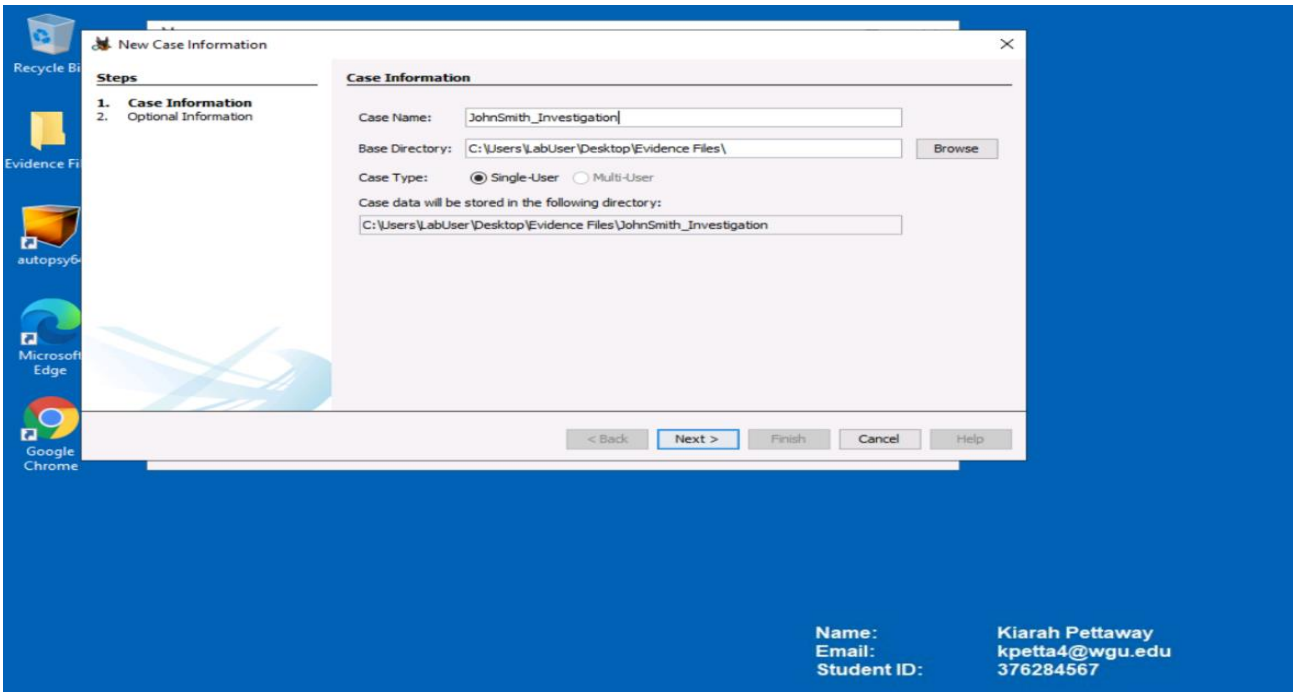
Figure 1



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.

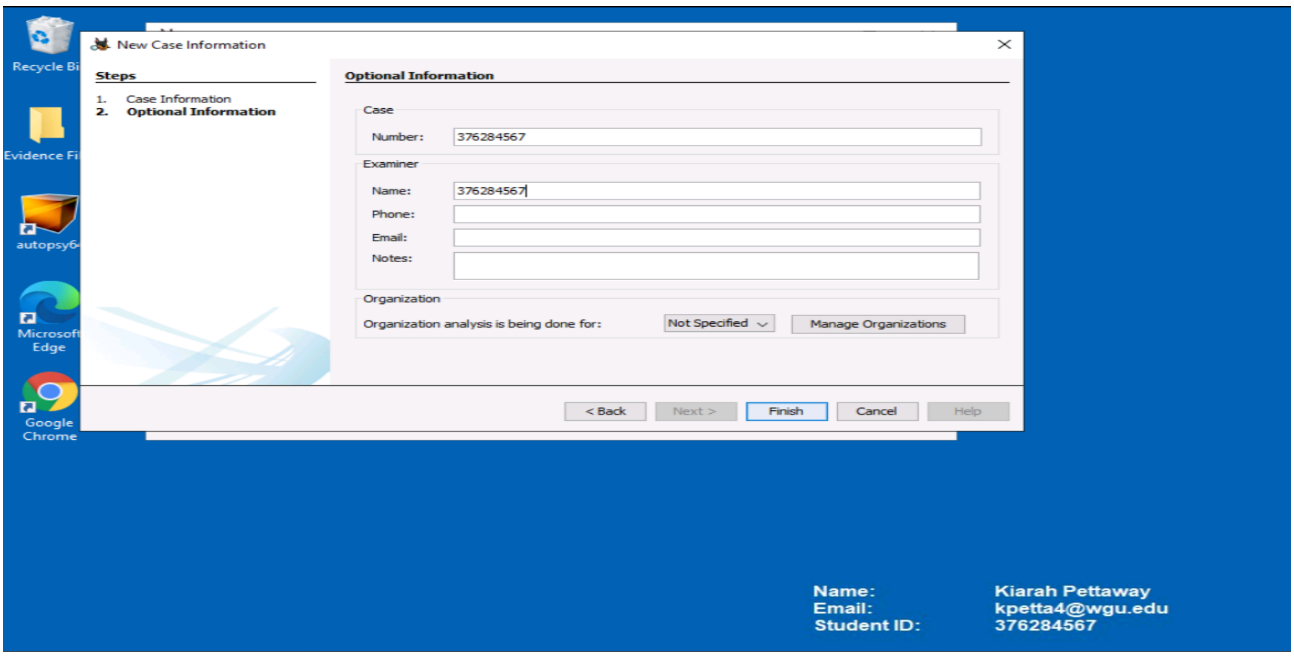
Kiarah Pettaway
ID: 011015177
11/08/2024
D431 – Task 2

Figure 2



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.

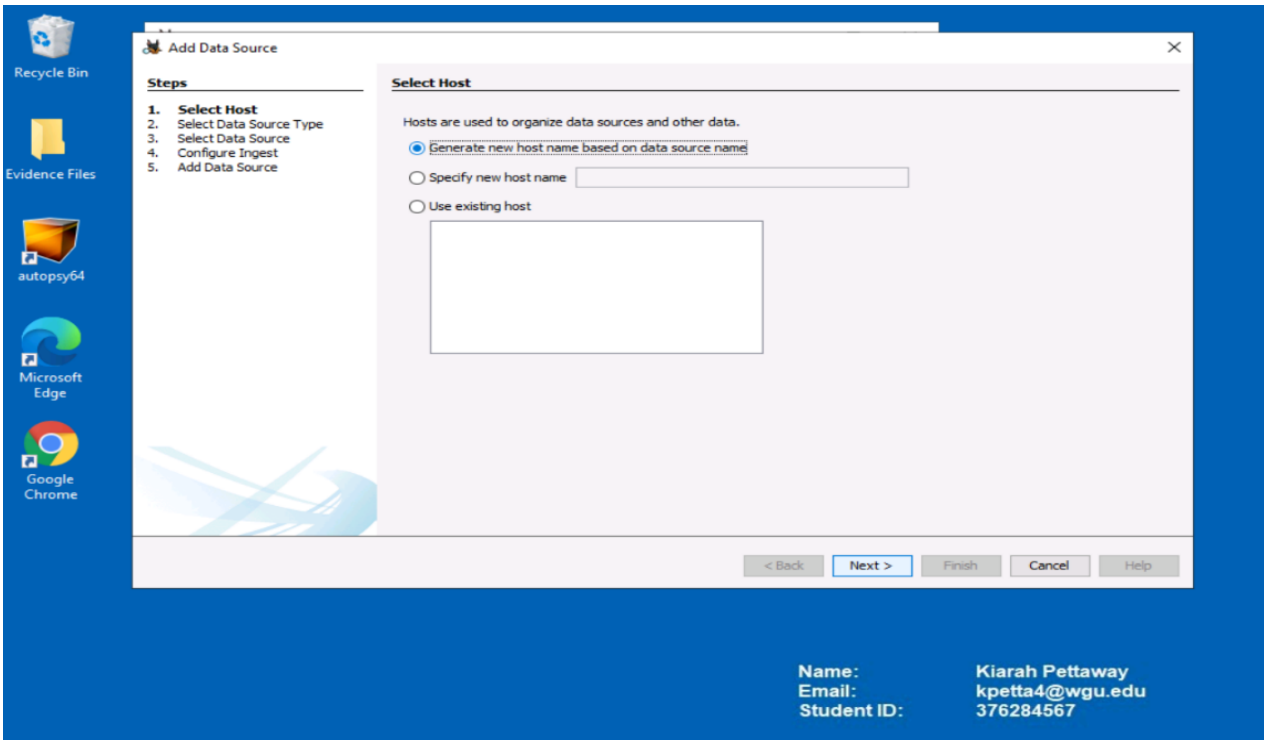
Figure 3



Kiarah Pettaway
ID: 011015177
11/08/2024
D431 – Task 2

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

Figure 4



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.”

Kiarah Pettaway
ID: 011015177
11/08/2024
D431 – Task 2

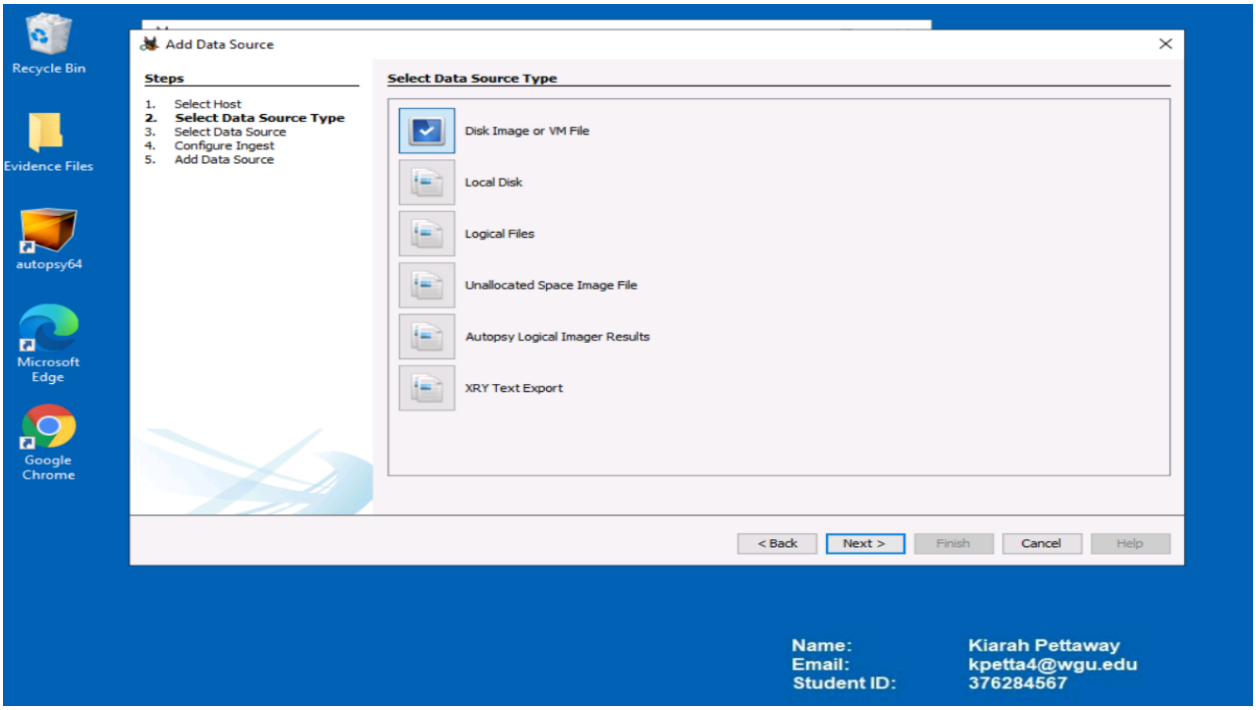


Figure 5

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.

Kiarah Pettaway
ID: 011015177
11/08/2024
D431 – Task 2

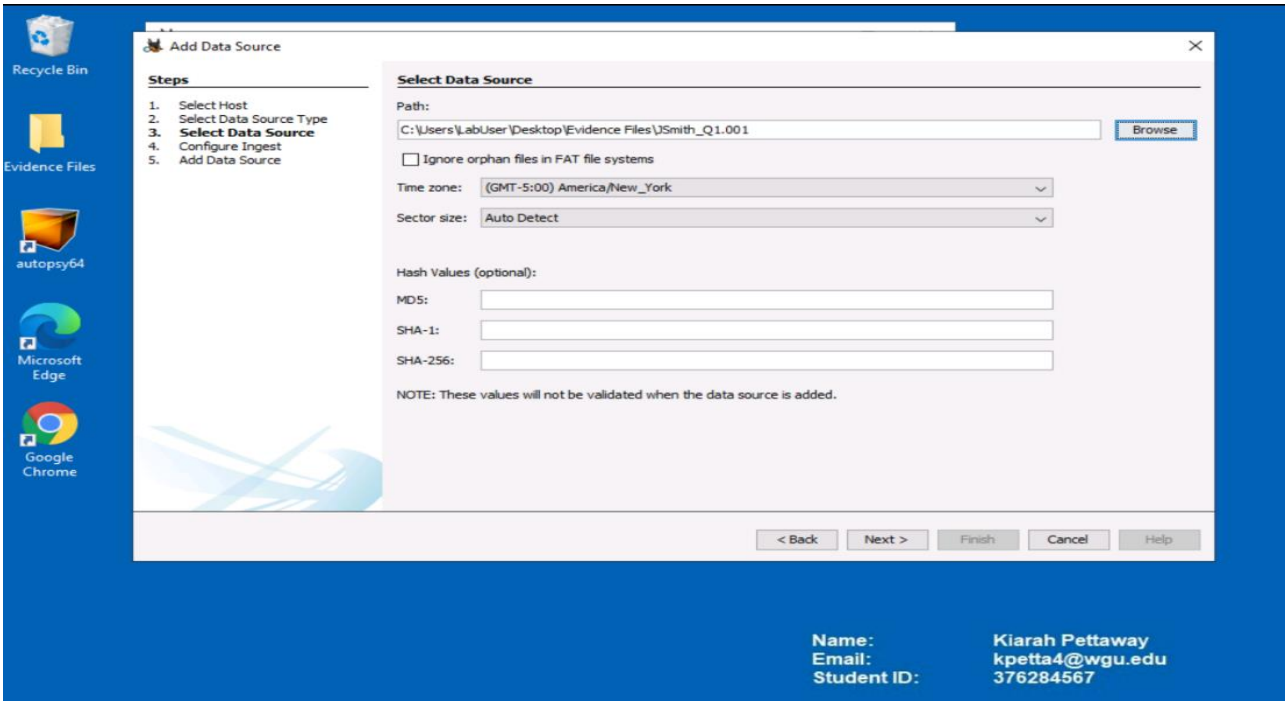
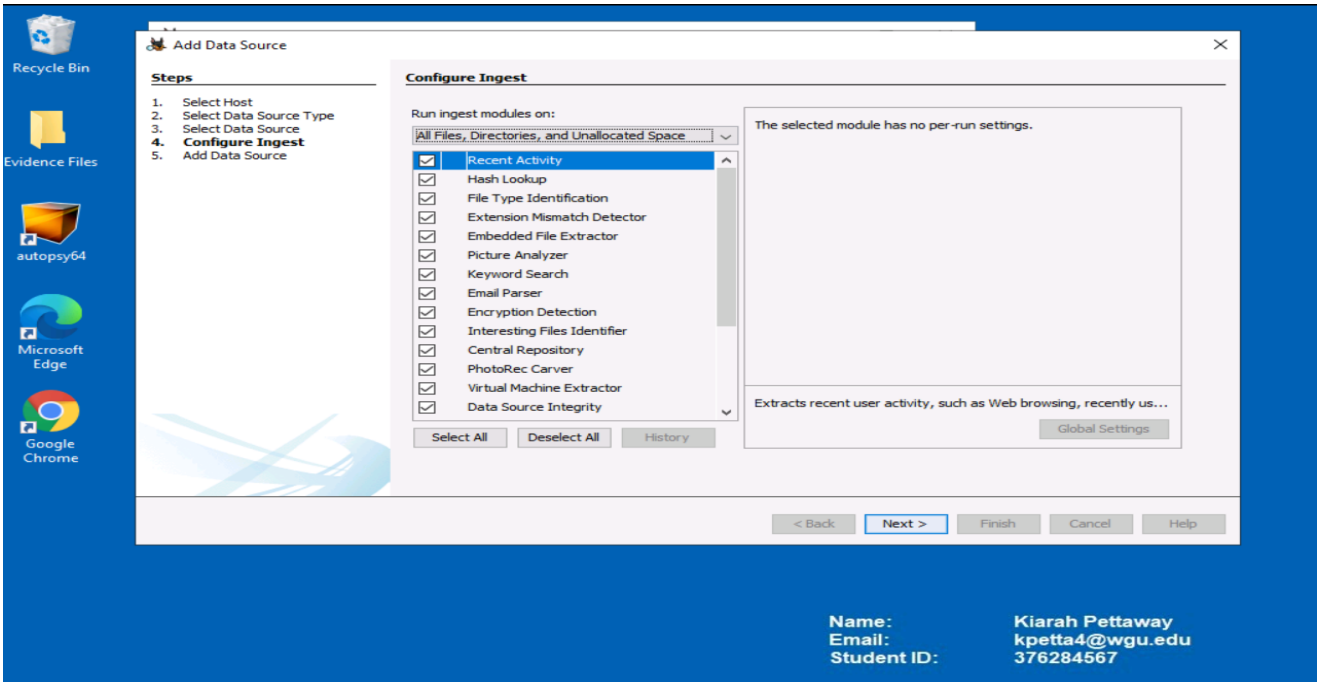


Figure 6

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

Figure 7



Kiarah Pettaway
ID: 011015177
11/08/2024
D431 – Task 2

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.

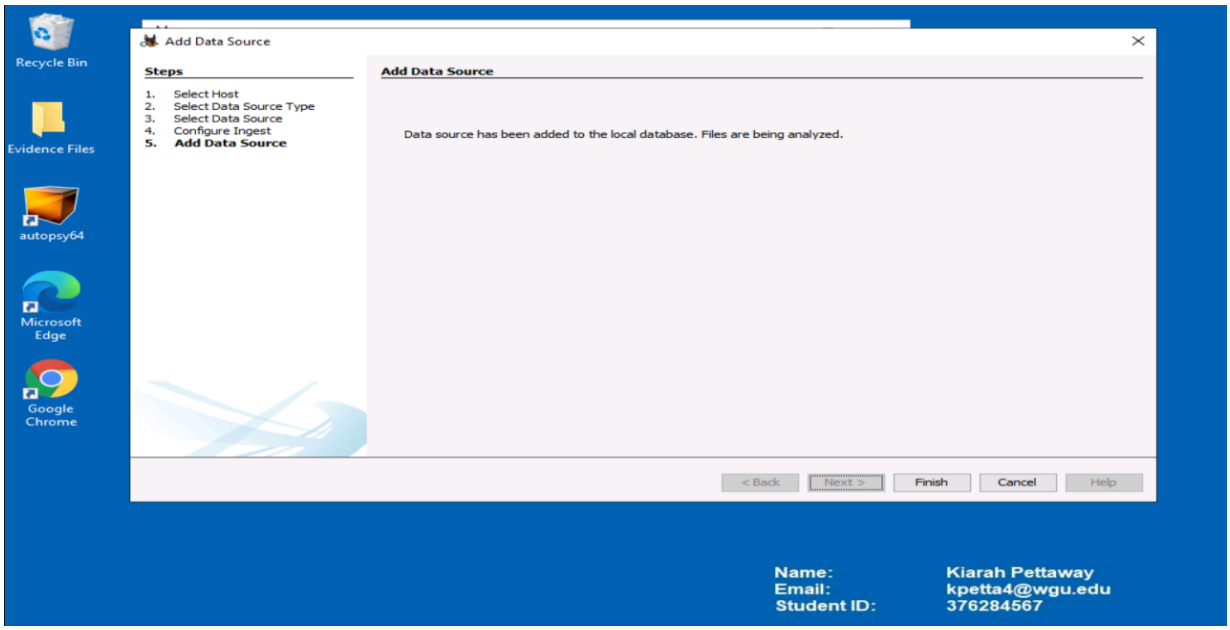
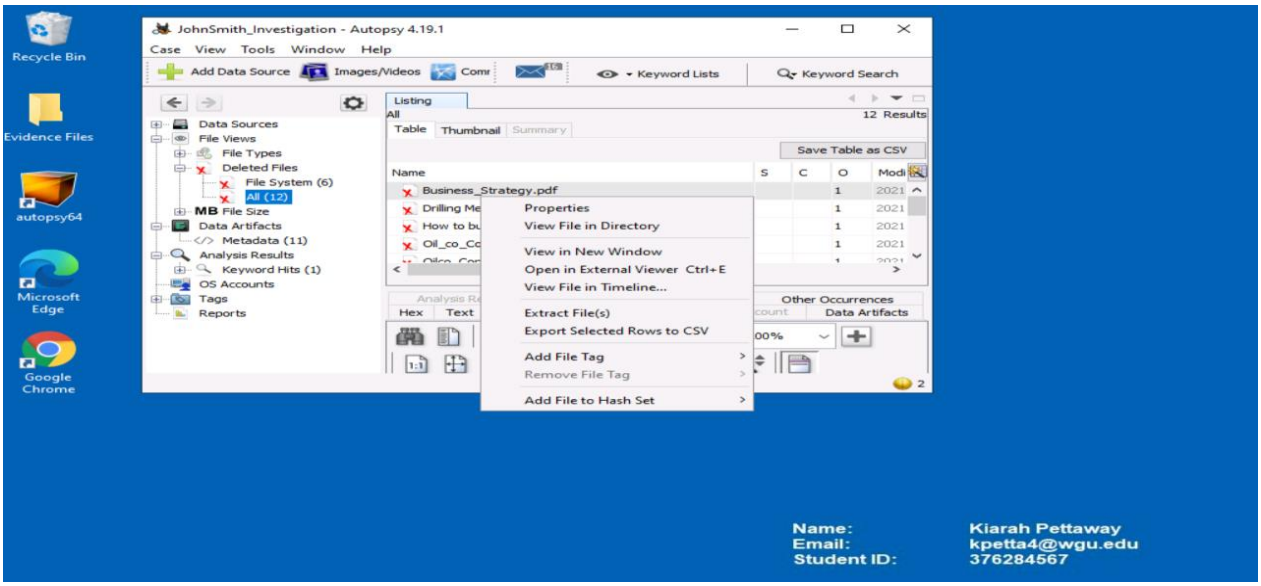


Figure 8

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



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

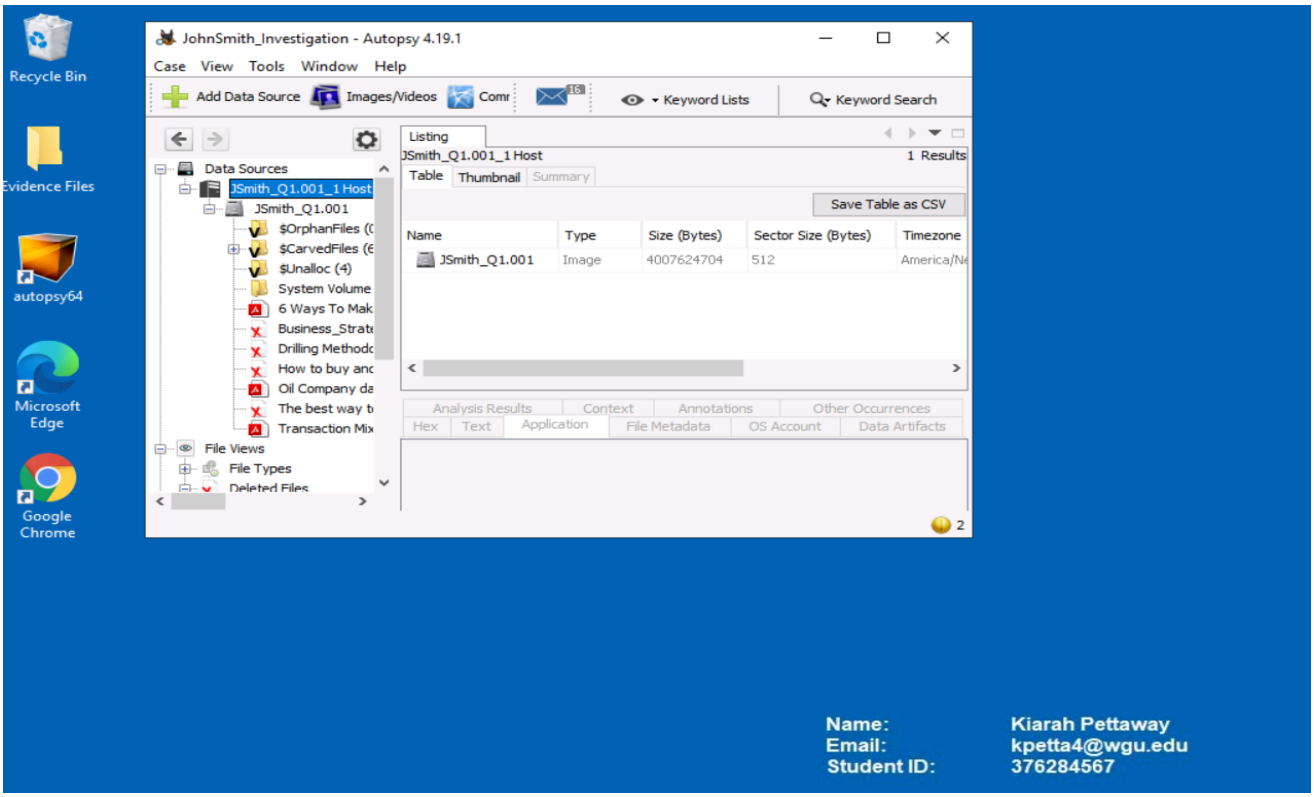
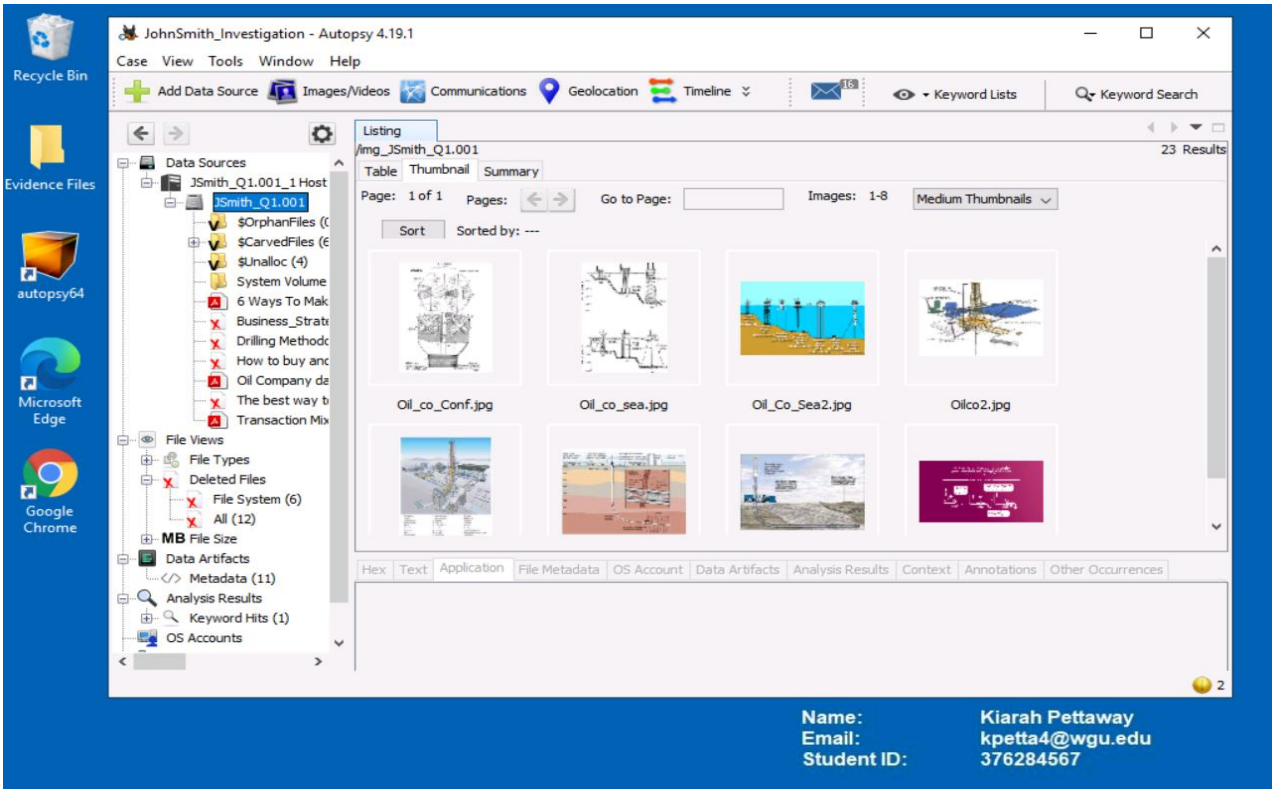


Figure 11



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.

Kiarah Pettaway
ID: 011015177
11/08/2024
D431 – Task 2

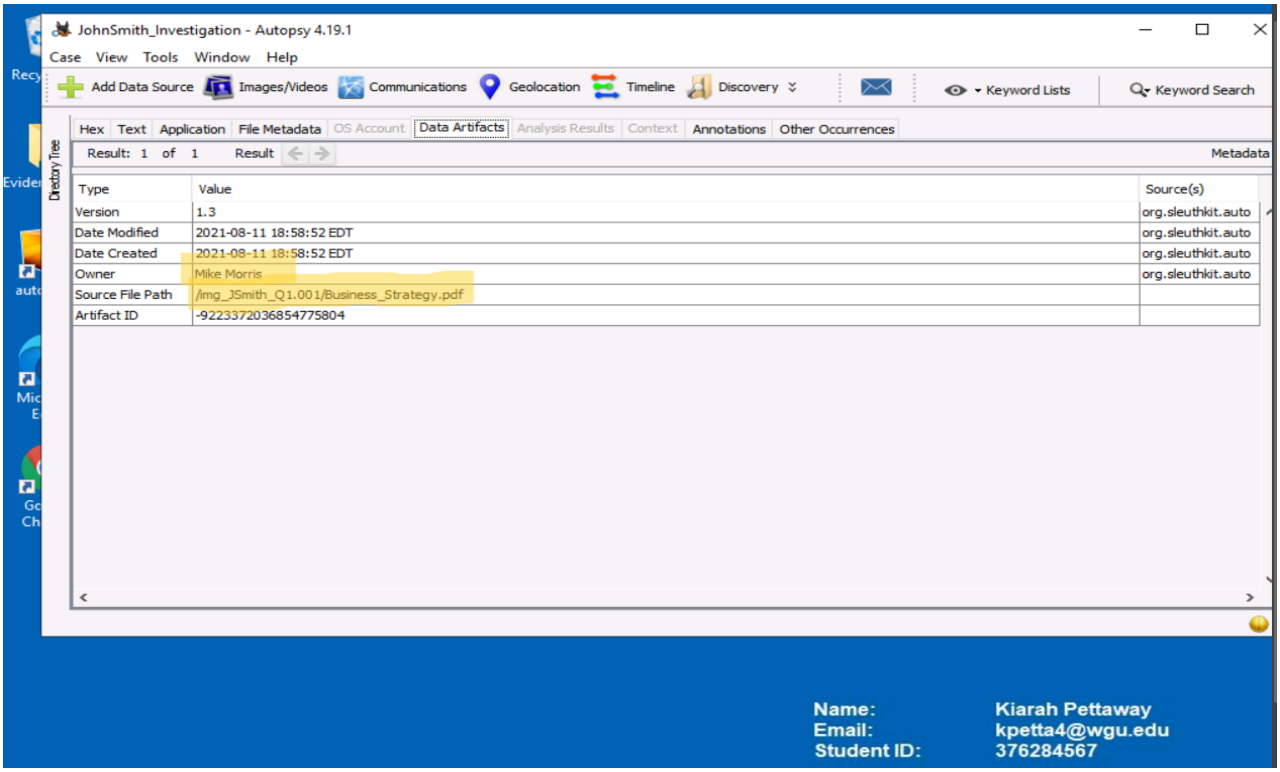


Figure 12

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.

Kiarah Pettaway
ID: 011015177
11/08/2024
D431 – Task 2

Figure 13

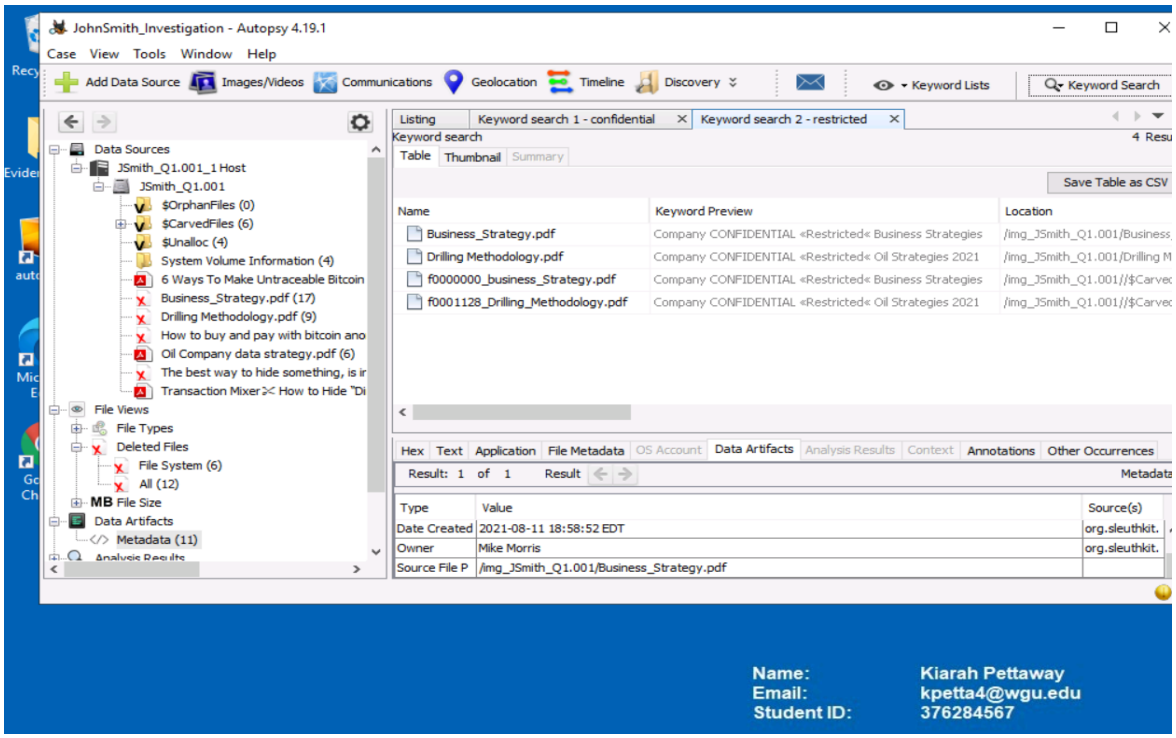
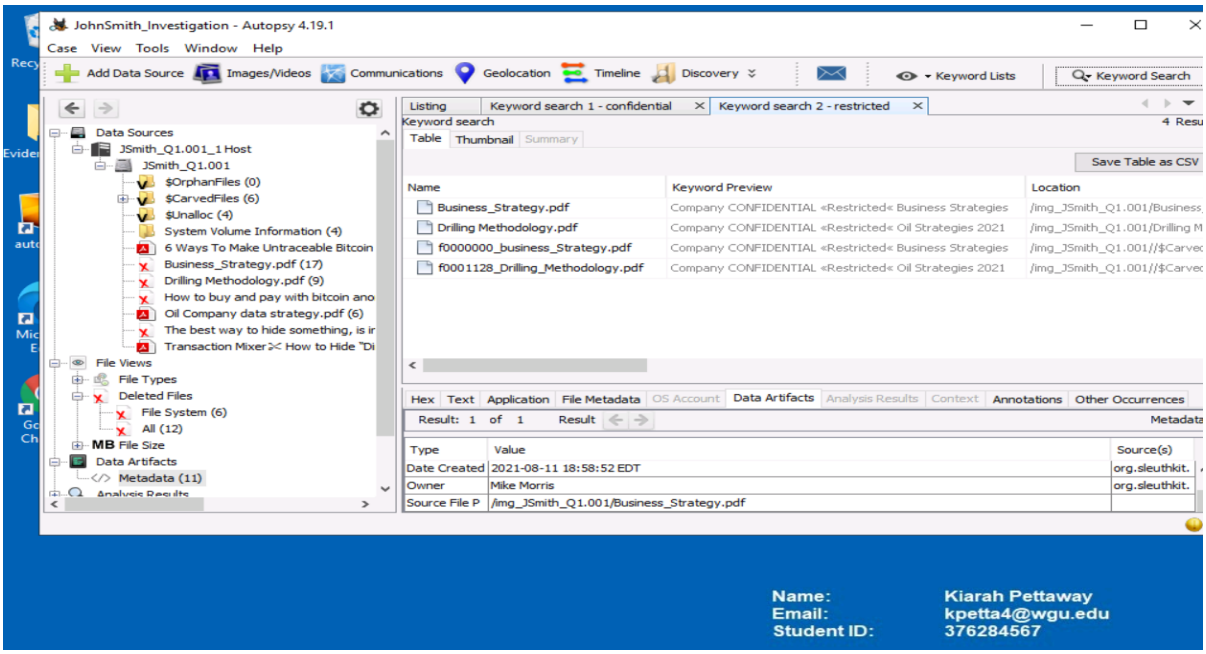


Figure 14



Kiarah Pettaway
ID: 011015177
11/08/2024
D431 – Task 2

Figure 15

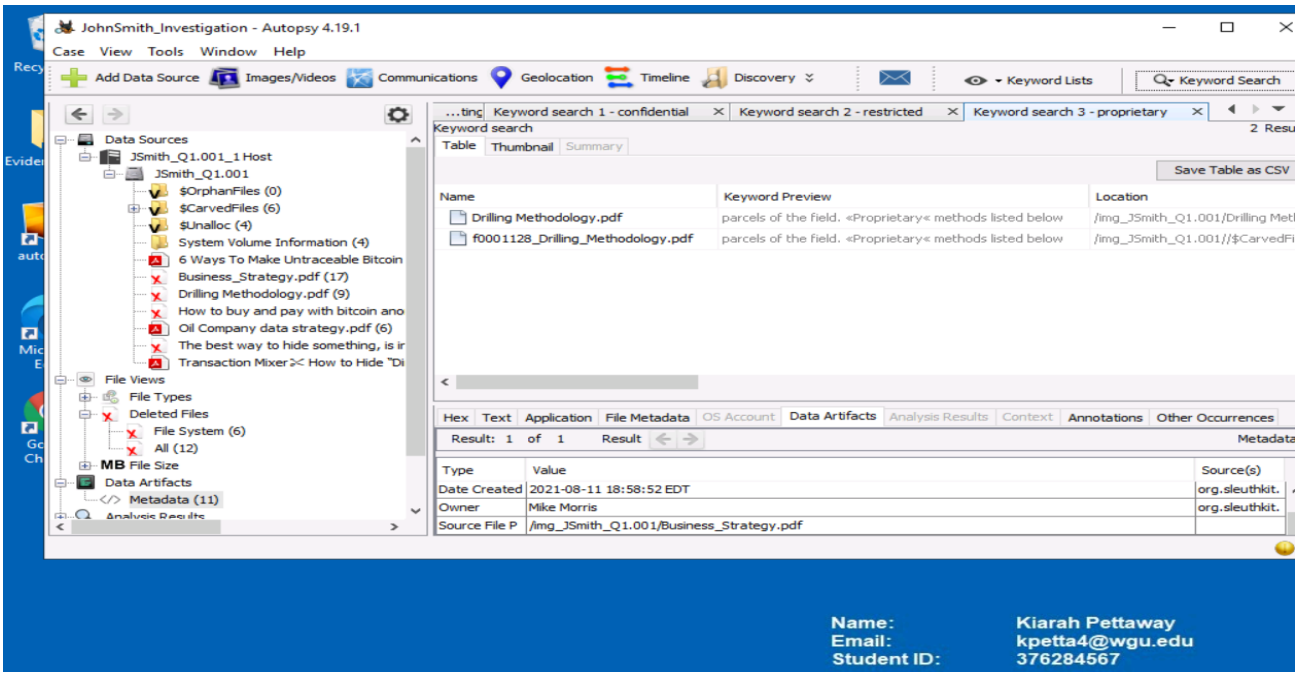
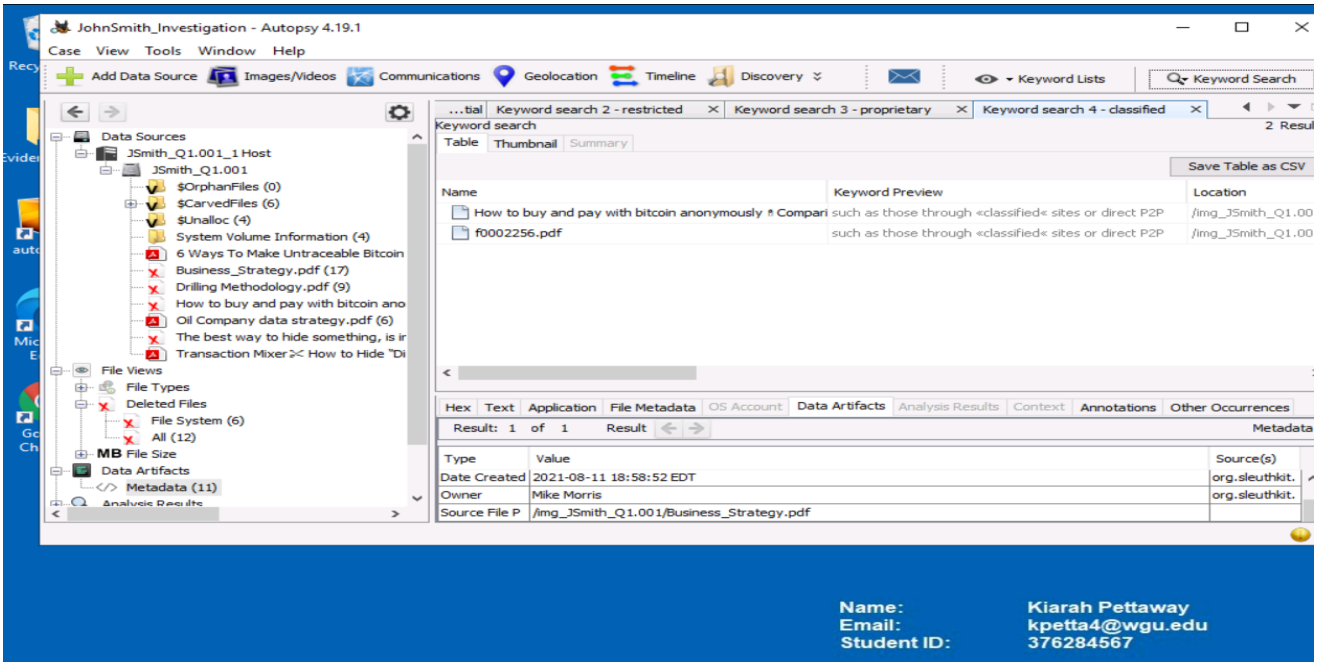


Figure 16



Kiarah Pettaway
ID: 011015177
11/08/2024
D431 – Task 2

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

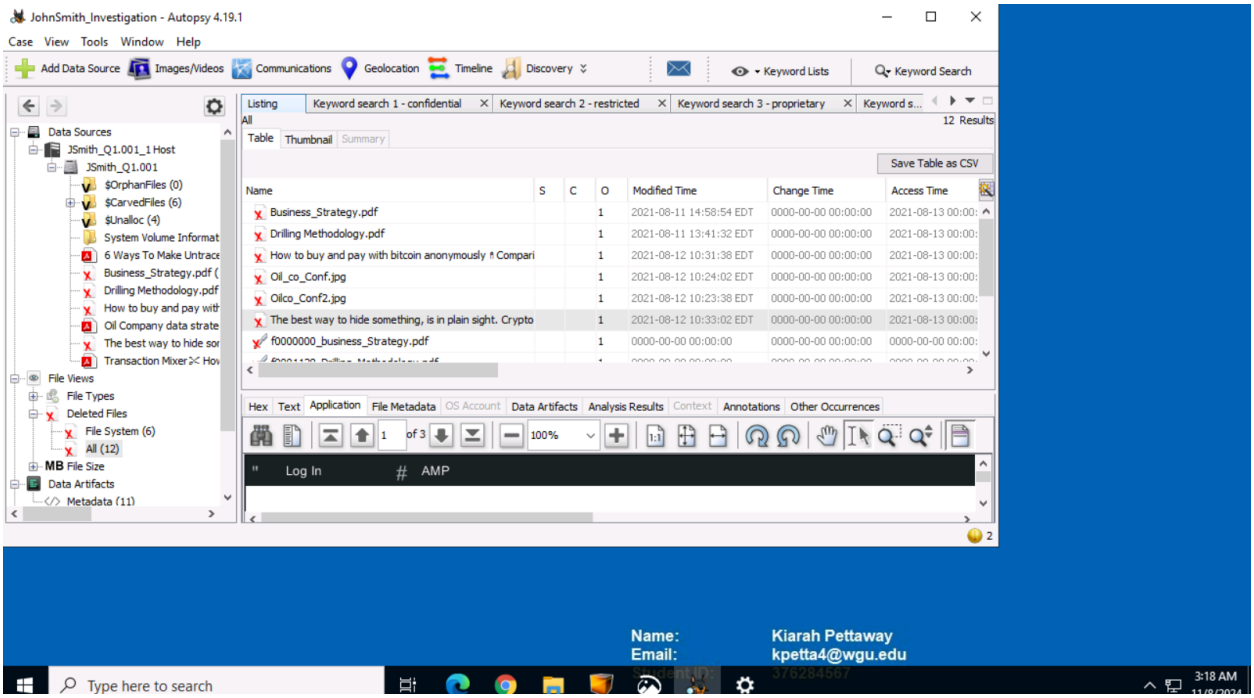
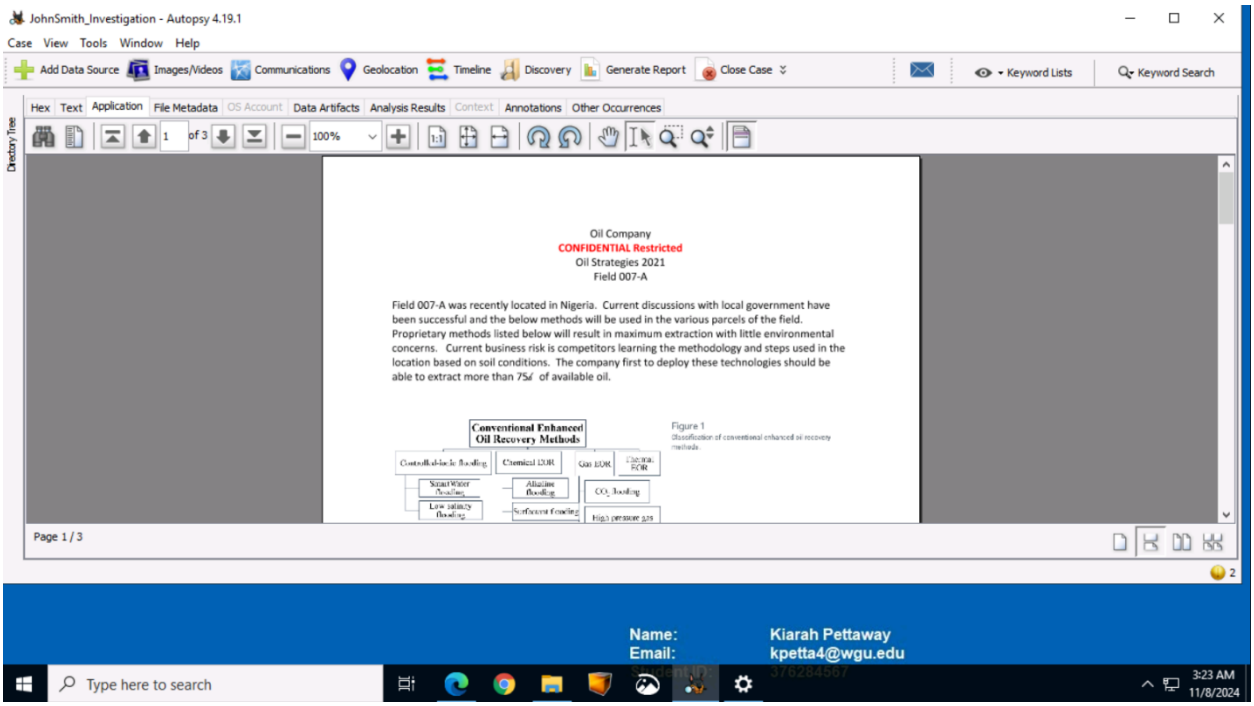


Figure 18



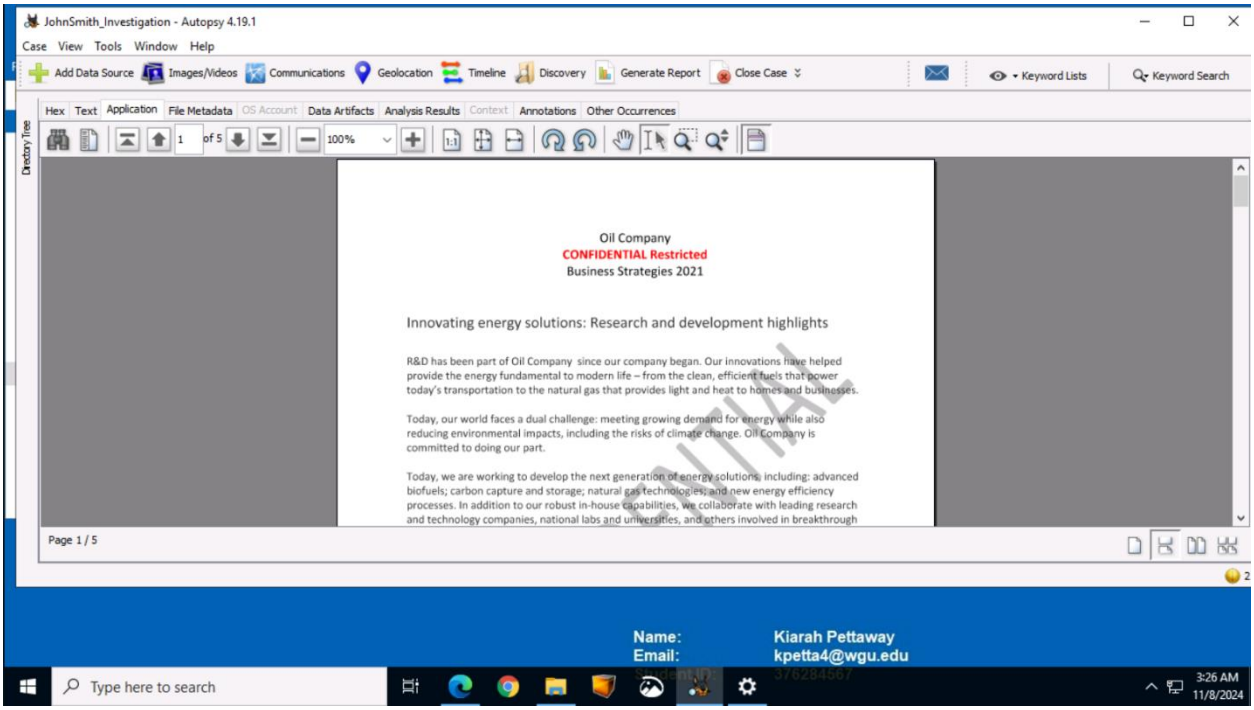
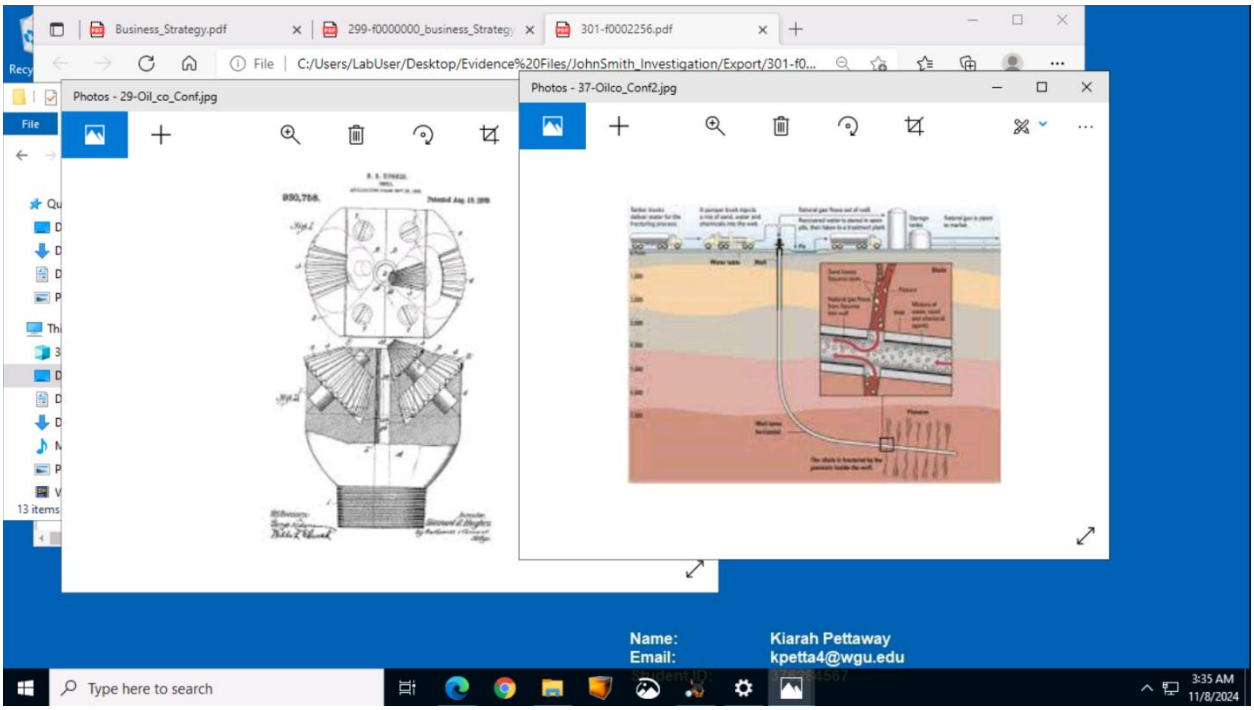


Figure 19

Kiarah Pettaway
ID: 011015177
11/08/2024
D431 – Task 2

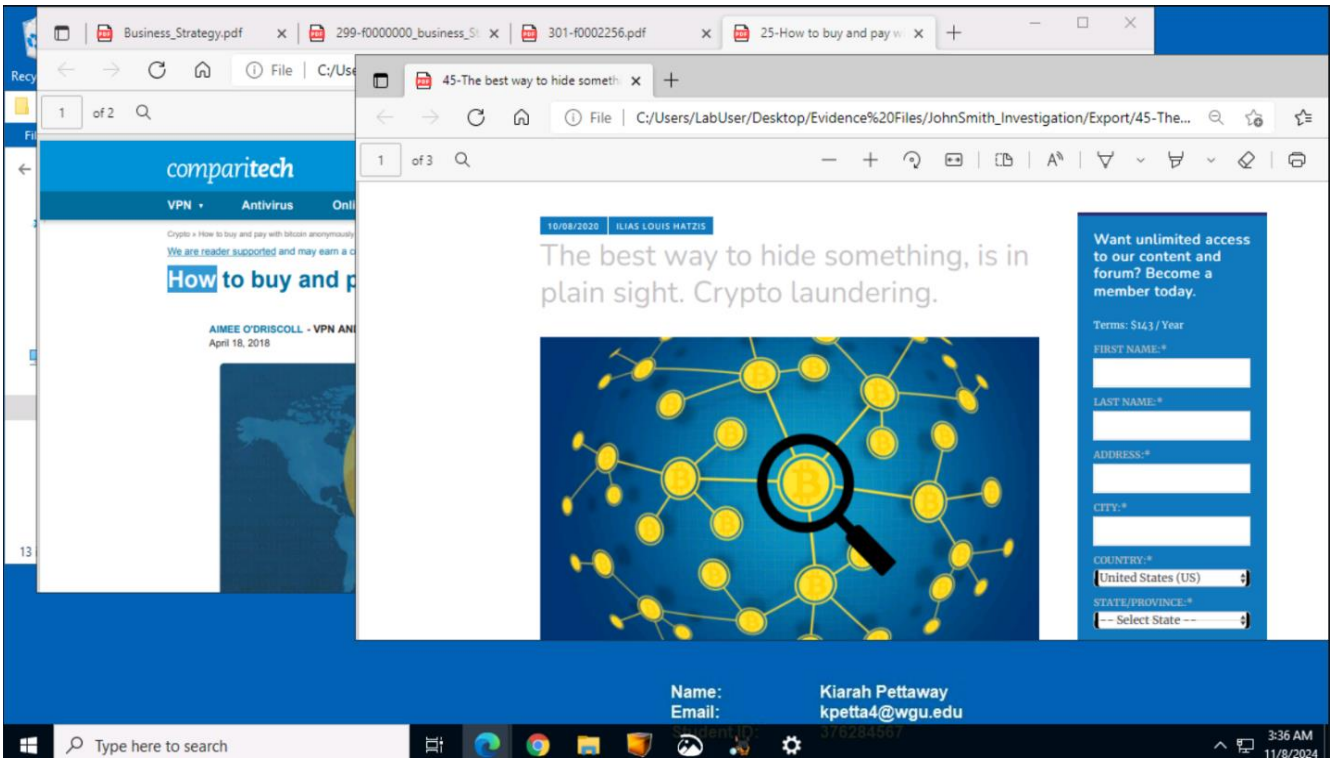
Figure 20



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.

Kiarah Pettaway
ID: 011015177
11/08/2024
D431 – Task 2

Figure 21



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.