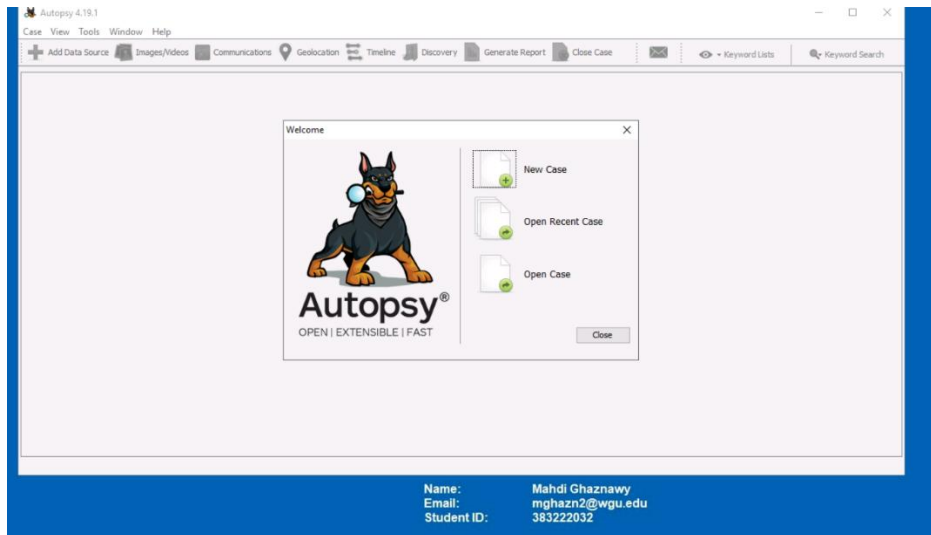


Mahdi Ghaznawy

D431 – Task 2

Case file creation screenshots of these steps.

The first step was to launch the Autopsy application and create a new case. I selected "New Case" to create a forensic workspace where all investigative data and findings would be recorded and analyzed.



Next, I entered the necessary case details, including the case name. I also selected a base directory to store all associated files, reports, and recovered data, organizing the case for

efficient analysis and future reference.

The screenshot shows the 'New Case Information' dialog box in Autopsy 4.19.1. The 'Steps' panel on the left indicates '1. Case Information' is the current step. The 'Case Information' section contains the following fields:

- Case Name:
- Base Directory:
- Case Type: ☒ Single-User ☐ Multi-User
- Case data will be stored in the following directory:

At the bottom of the dialog are buttons: < Back, Next > (highlighted), Finish, Cancel, and Help.

Name: Mahdi Ghaznawy
Email: mghazn2@wgu.edu
Student ID: 383222032

I put in my student ID number for the case number and then added my name.

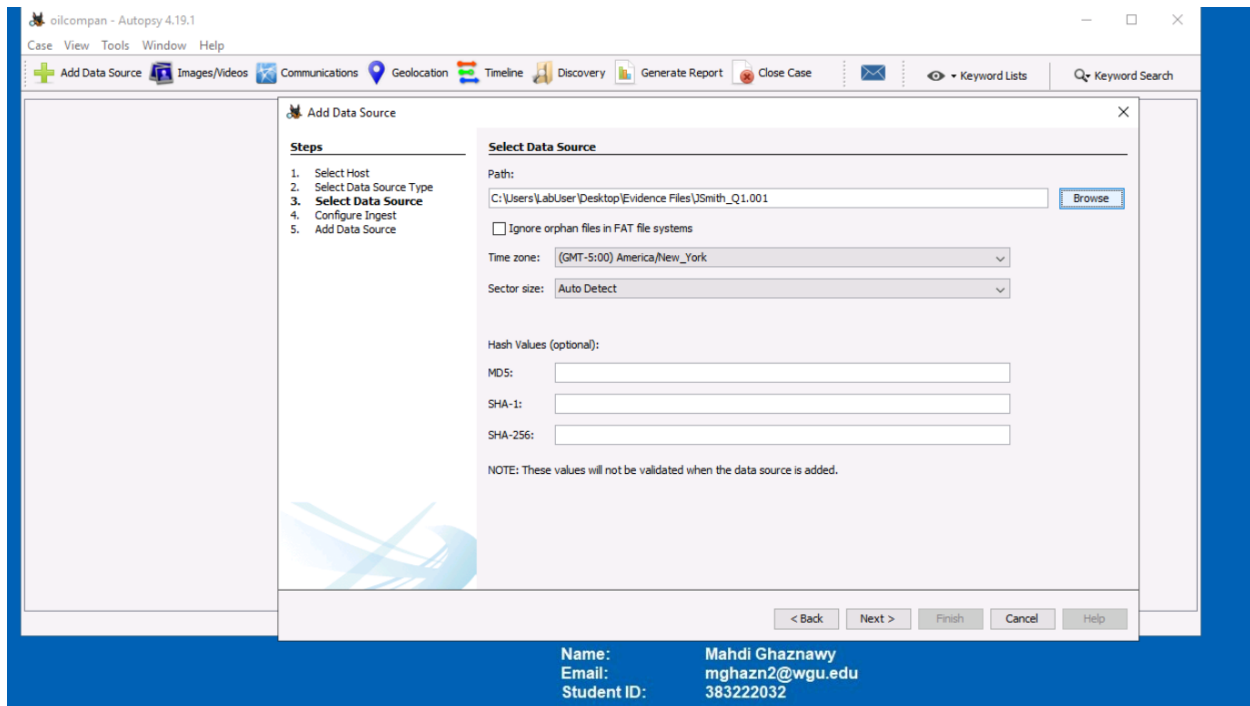
The screenshot shows the 'New Case Information' dialog box in Autopsy 4.19.1, now on 'Step 2: Optional Information'. The 'Optional Information' section contains the following fields:

- Case Number:
- Examiner:
 - Name:
 - Phone:
 - Email:
 - Notes:
- Organization:
 - Organization analysis is being done for:

At the bottom of the dialog are buttons: < Back, Next >, Finish (highlighted), Cancel, and Help.

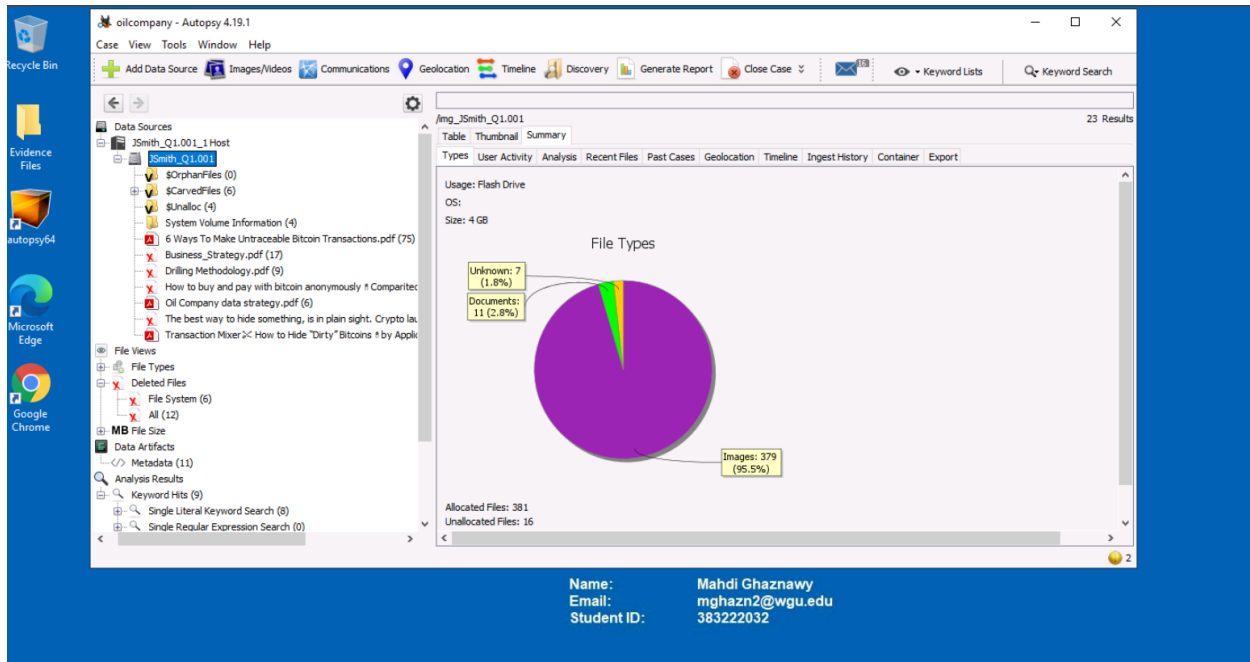
Name: Mahdi Ghaznawy
Email: mghazn2@wgu.edu
Student ID: 383222032

After setting up the case details, I added the data source from the disk image provided. This ensured that all relevant digital artifacts from the suspect's machine were included for analysis. After the evidence was loaded, the case was set up for a forensic investigation.

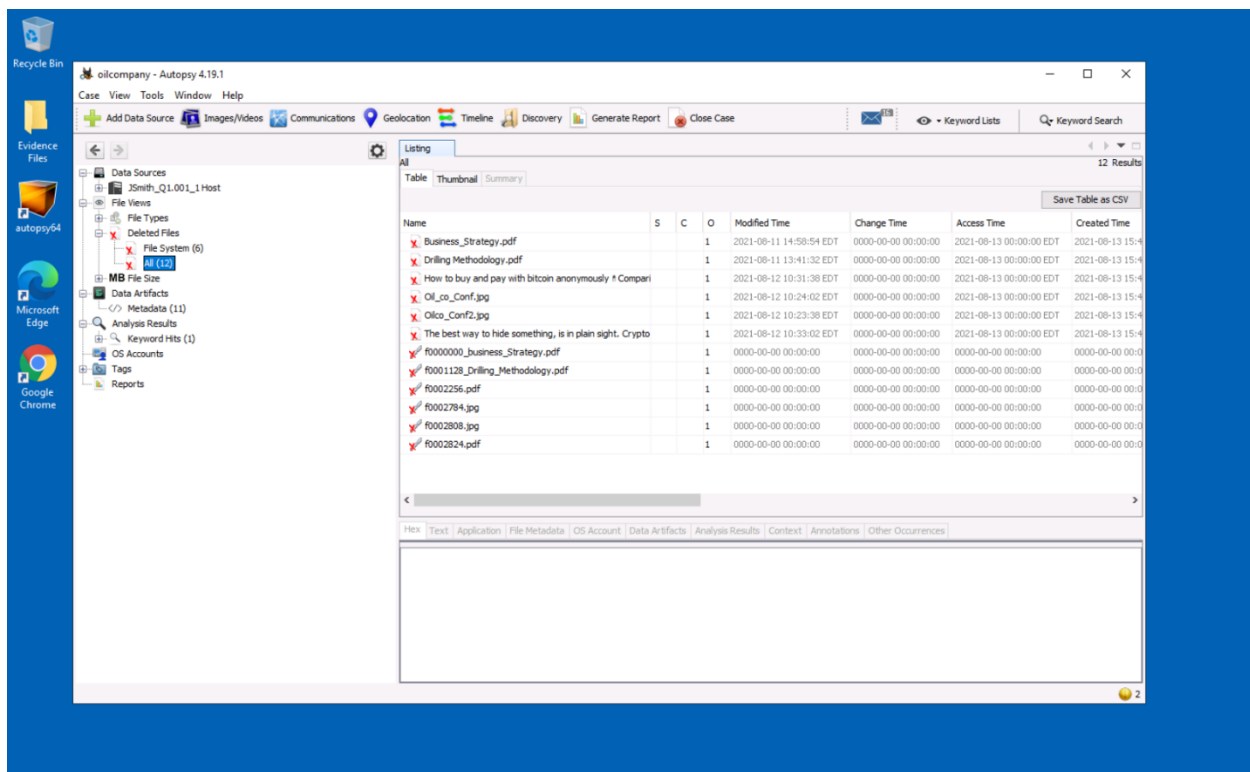


Autopsy and screenshots of these autopsy steps that support my findings and conclusions.

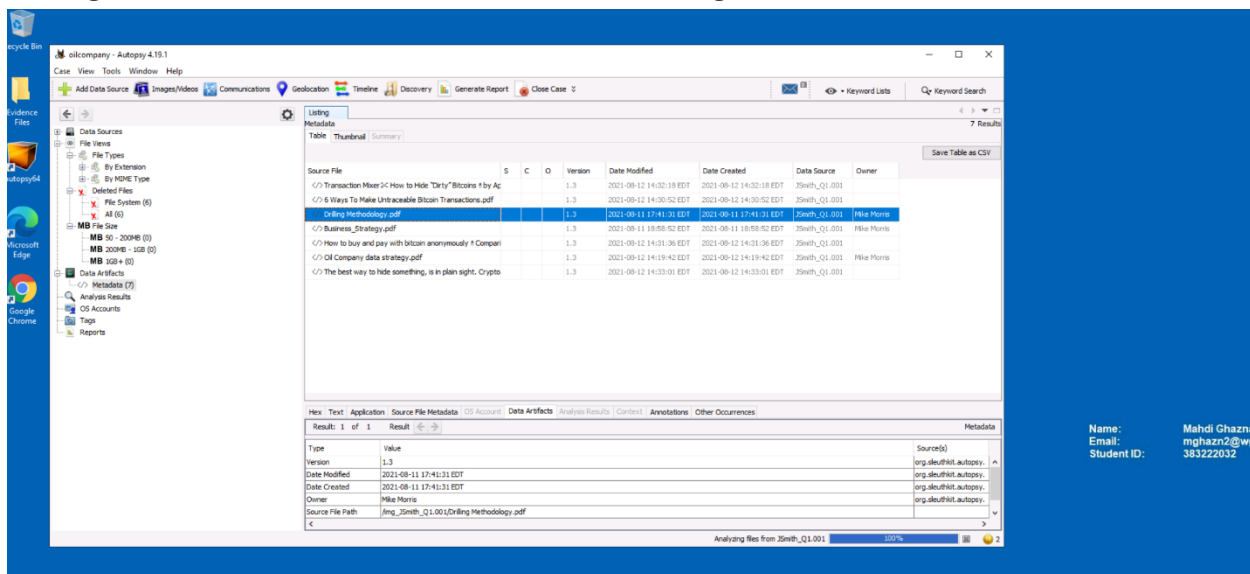
After loading the forensic image, I expanded the menus under the host JSmith_Q1.001 to get an overview of the discovered files: 379 images and 11 documents.



Next, I navigated to the deleted files section within Autopsy and discovered a total of twelve deleted files.

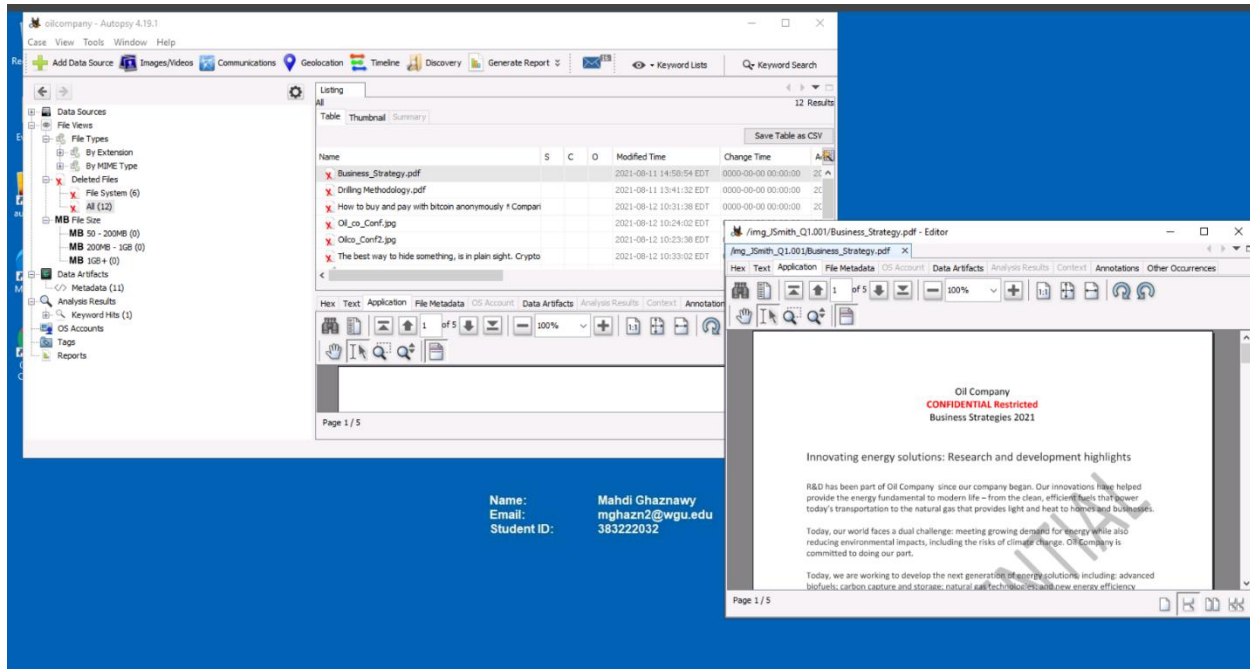


I found that Mr. Smith accessed several unauthorized image files containing confidential and proprietary information on the oil company's operations, configurations, and business strategies. Metadata confirms that these files belong to Mike Morris, not Mr. Smith.



Name: Mahdi Ghaznaw
Email: mghazn2@wgu.edu
Student ID: 383222032

This screen capture of Business_Strategy.pdf is an example of confidential data found on Mr. Smith's workstation. The file, which Mr. Smith had deleted, is one of several documents he accessed without authorization.



Name: Mahdi Ghaznaw
Email: mghazn2@wgu.edu
Student ID: 383222032

This screenshot shows another confidential file, Drilling Methodology.pdf, which was discovered to have been deleted from Mr. Smith's workstation.

The screenshot displays the Autopsy 4.19.1 interface. The left sidebar shows the file system tree with various folders like 'System Volume Information', '6 Ways To Make Untraceable Bitcoin Transactions.pdf (75)', 'Business_Strategy.pdf (17)', 'Drilling Methodology.pdf (9)', 'How to buy and pay with bitcoin anonymously * Compan...', 'Oil Company data strategy.pdf (6)', 'The best way to hide something, is in plain sight. Crypto la...', and 'Transaction Mixer 2: How to Hide "Dirty" Bitcoins * by Appli...'. The main pane shows a table of file analysis results.

Name	S	C	O	Modified Time	Change Time	Access Time
Business_Strategy.pdf	1	1	1	2021-08-11 14:58:54 EDT	0000-00-00 00:00:00	2021-08-13 00:00:00 EDT
Drilling Methodology.pdf	1	1	1	2021-08-11 13:41:32 EDT	0000-00-00 00:00:00	2021-08-13 00:00:00 EDT
How to buy and pay with bitcoin anonymously * Compan...	1	1	1	2021-08-12 10:31:38 EDT	0000-00-00 00:00:00	2021-08-13 00:00:00 EDT
Oil_co_Conf2.jpg	1	1	1	2021-08-12 10:24:02 EDT	0000-00-00 00:00:00	2021-08-13 00:00:00 EDT
Oilco_Conf2.jpg	1	1	1	2021-08-12 10:23:38 EDT	0000-00-00 00:00:00	2021-08-13 00:00:00 EDT
The best way to hide something, is in plain sight. Crypto	1	1	1	2021-08-12 10:33:02 EDT	0000-00-00 00:00:00	2021-08-13 00:00:00 EDT
F000000_Business_Strategy.pdf	1	1	1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
F0001126_Drilling_Methodology.pdf	1	1	1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
F0002256.pdf	1	1	1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
F0002784.jpg	1	1	1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
F0002808.jpg	1	1	1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
F0002824.pdf	1	1	1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

The right pane shows a preview of the file 'Drilling Methodology.pdf'. The document content includes the following text:

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.

Conventional Enhanced Oil Recovery Methods

Figure 1: Distribution of conventional enhanced oil recovery methods

Page 1 / 3

Looking more into the Files folder, it looks like John Smith was doing some extensive research on Crypto laundering and Bitcoin transactions. This supports the claims that he was looking to sell the proprietary information illegally.

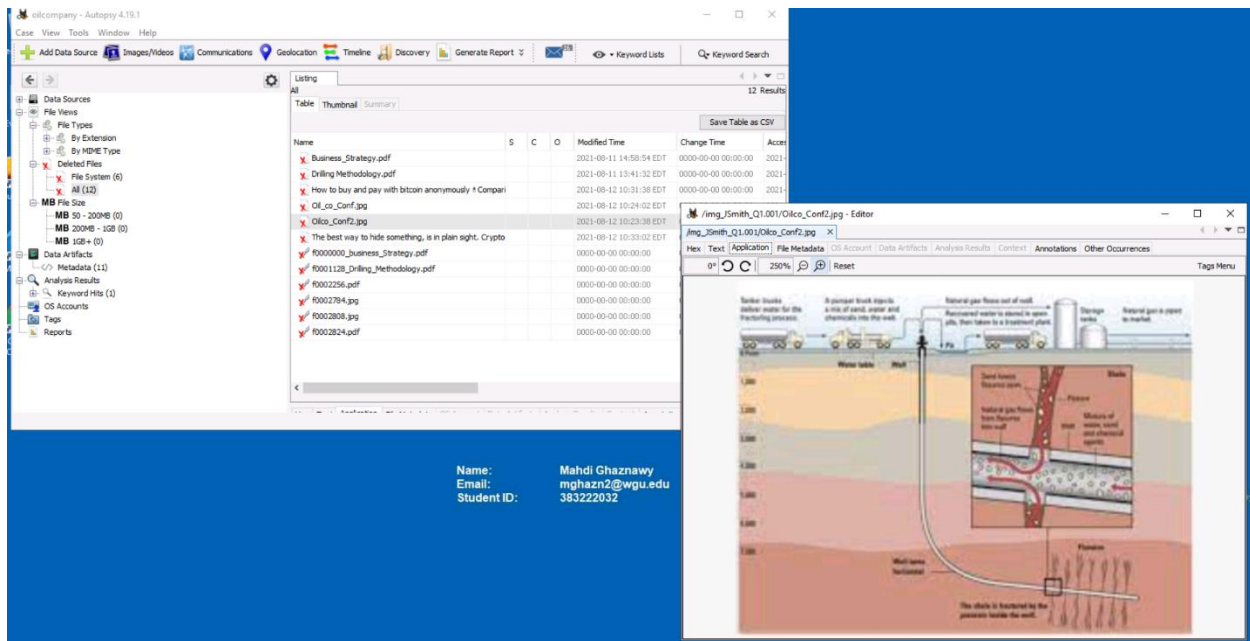
Autopsy 4.15.1 interface showing file analysis results. The table lists files such as Business_Strategy.pdf, Drilling Methodology.pdf, and various images. The browser window displays the Comparitech website, which includes a VPN service and a section titled "How to buy and pay with bitcoin anonymous".

Name: Mahdi Ghaznaw
Email: mghazn2@wgu.edu
Student ID: 383222032

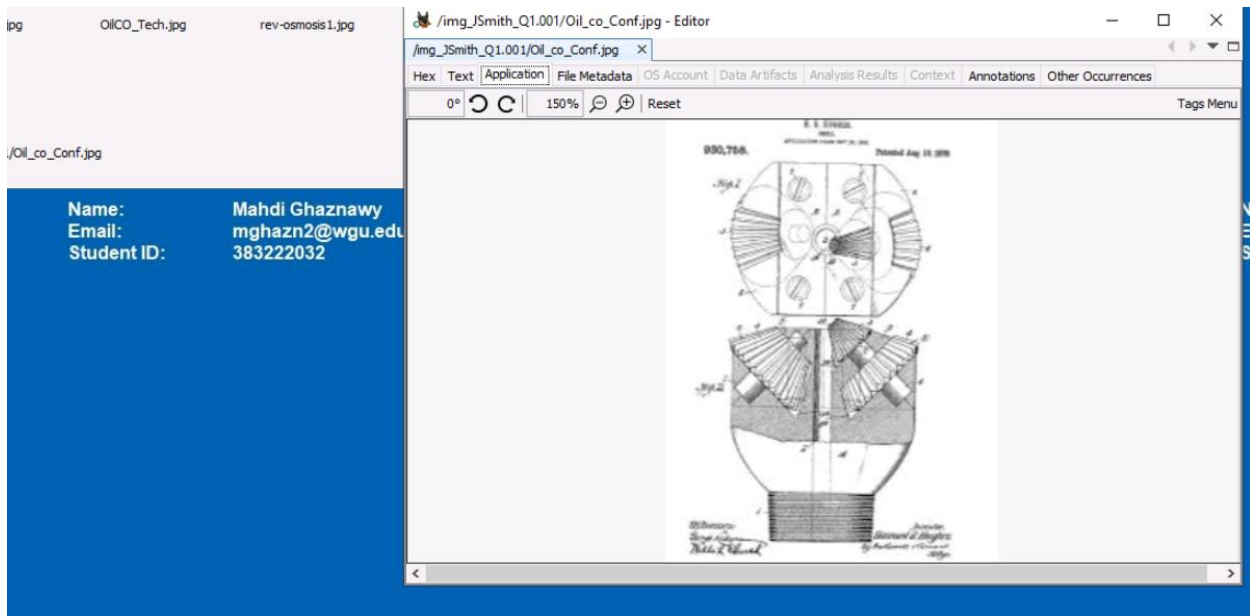
Autopsy 4.19.1 interface showing file analysis results. The table lists files such as Business_Strategy.pdf, Drilling Methodology.pdf, and various images. The browser window displays the Brockman courseware website, which includes a section titled "The best way to hide something, is in plain sight. Crypto laundering".

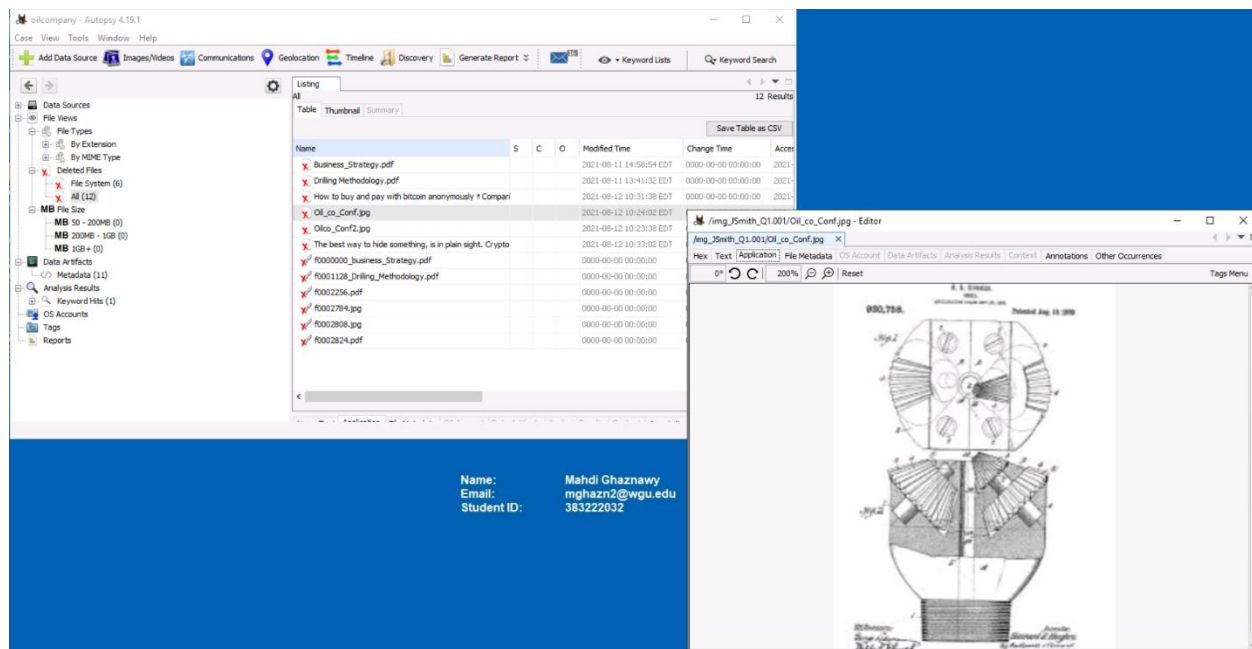
Name: Mahdi Ghaznaw
Email: mghazn2@wgu.edu
Student ID: 383222032

Evidence of John Smith looking at the confidential transactions. More evidence suggests that he was looking to sell the information obtained.



The second screen capture is Oil _ co _ Conf2.jpg, a proprietary document recovered after being deleted from Mr. Smith's machine. This file contains company information, and its deletion indicates a possible attempt to cover up unauthorized access. This file also provides evidence of policy violations related to the handling of proprietary data.





The findings and the conclusion:

The investigation unearthed substantial evidence that John Smith was engaged in the unauthorized access, distribution, and use of company secret, proprietary information. Some documents marked "Confidential" appeared on his machine and described the company's drilling methods and business plans.

Confidential documents were discovered in the forensic analysis of Smith's computer, including Business _ Strategy.pdf, Drilling _ Methodology.pdf, Oil _ co _ Conf.jpg, and Oilco _ Conf2.jpg. These files were deleted, suggesting an effort to stay away from detection.

Further investigation found that Smith searched for information concerning anonymous Bitcoin transactions, cryptocurrency laundering, and financial obfuscation. This suggests he was either searching for a buyer for the company's proprietary information or had one

already secured and was researching methods to close the deal using Bitcoin. No matter how they were conducted, these searches violated the company's Acceptable Use Policy by itself because they involved company-owned equipment used during working hours.

Along with the digital evidence, unauthorized possession of confidential documents, attempted file deletion, and research into anonymous financial transactions, John Smith obviously intended to profit from the company's trade secrets. His actions violate company policies, including sharing proprietary information with no approval. These findings suggest Smith attempted or successfully sold confidential company data for profit and deserves legal and disciplinary action.