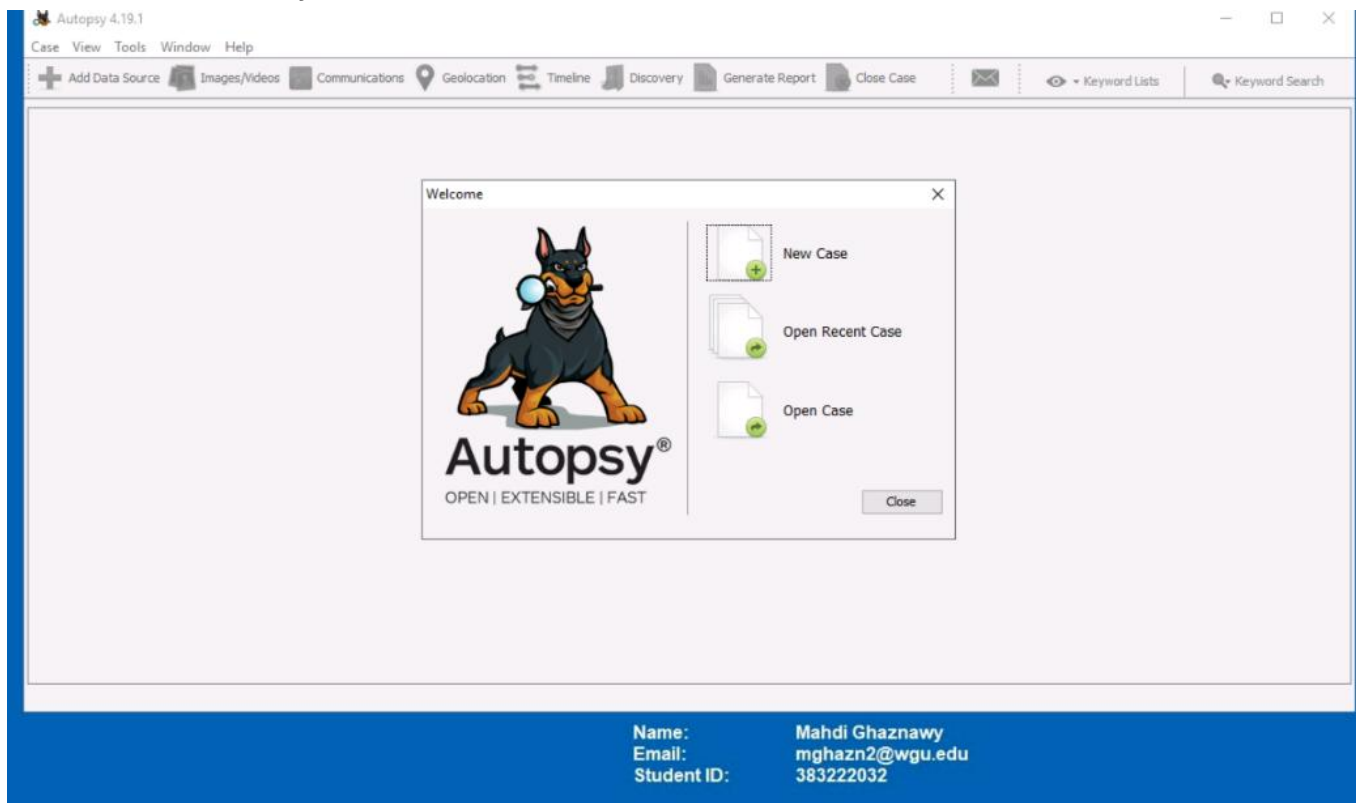


Mahdi Ghaznawy

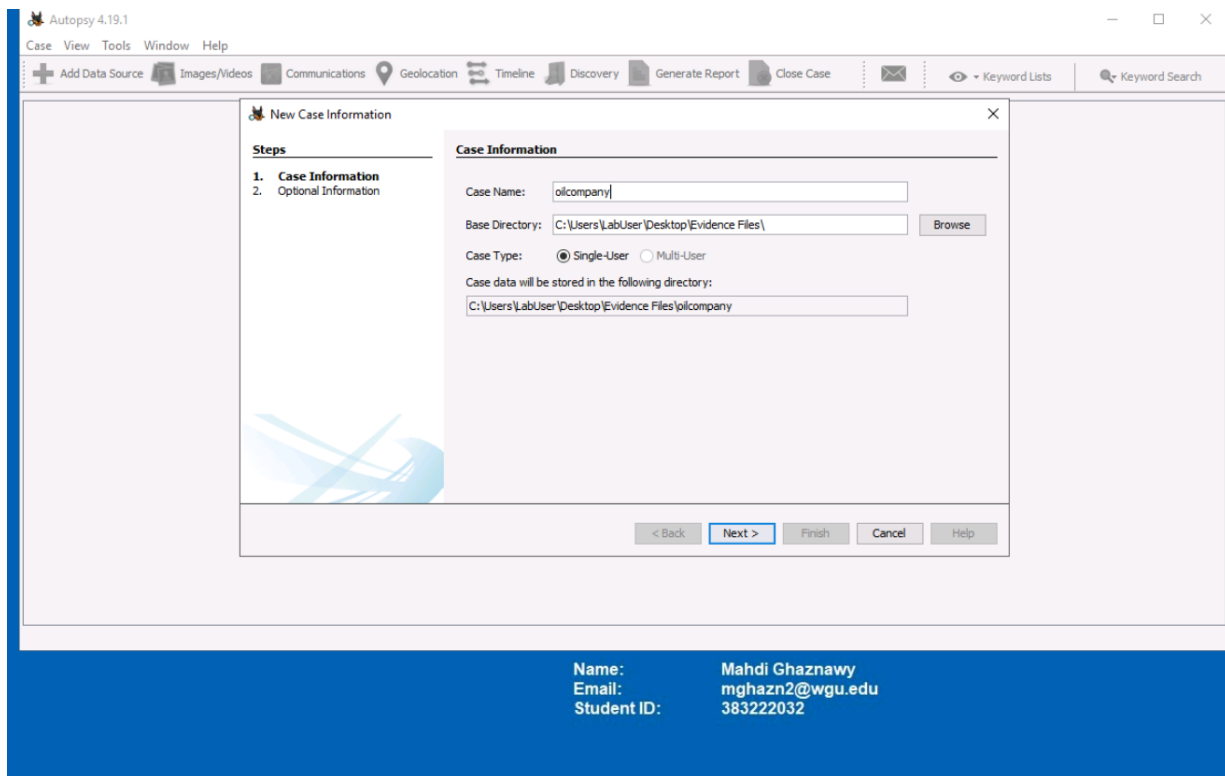
D431 – Task 2

Case File Creation and screenshots of these steps:

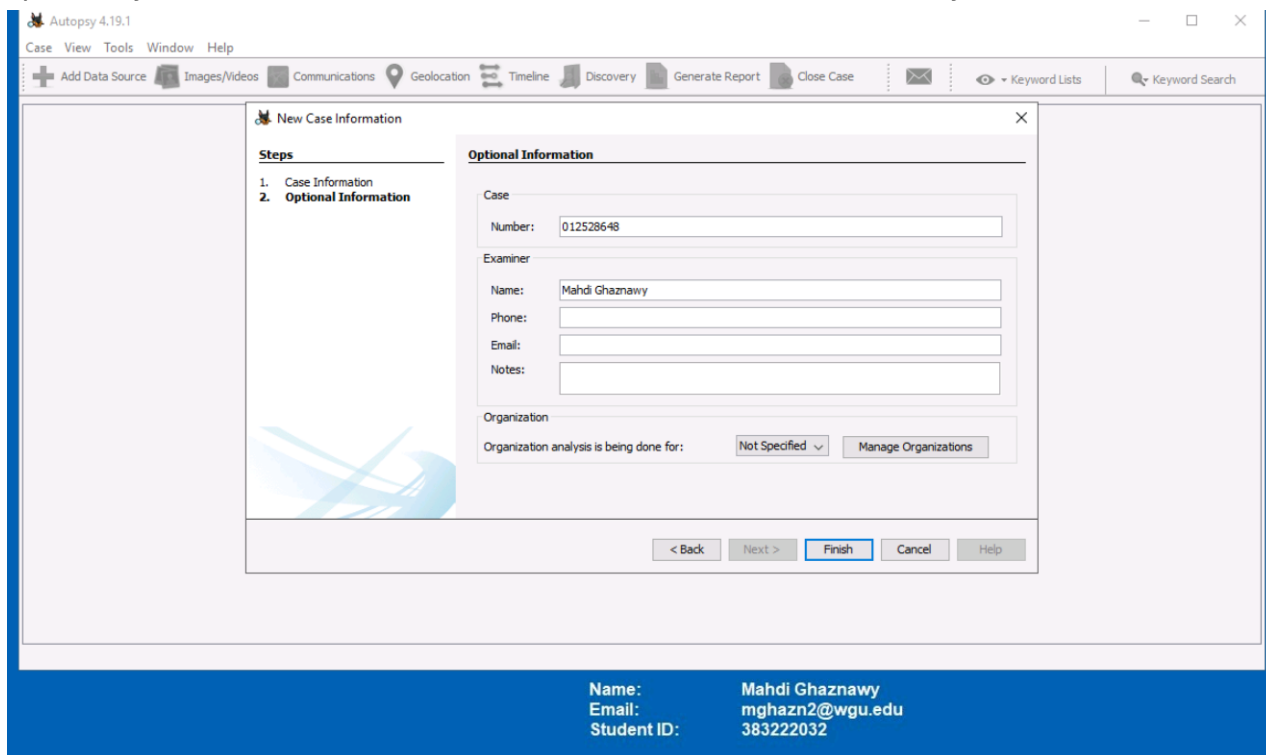
The first step was to launch the Autopsy application and create a new case. I selected “New Case” to create a forensic workspace where all investigative data and findings would be recorded and analyzed.



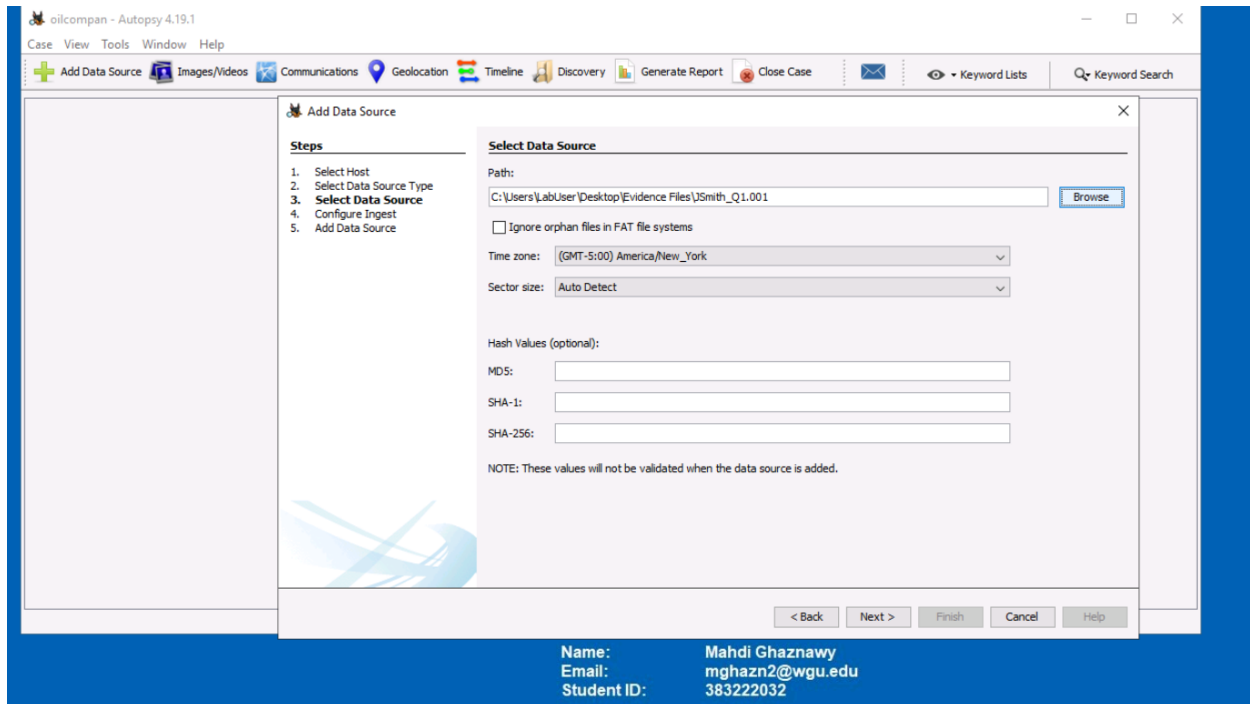
Next, I entered the necessary case details, including the case name. I also selected a base directory to store all associated files, reports, and recovered data, organizing the case for efficient analysis and future reference.



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

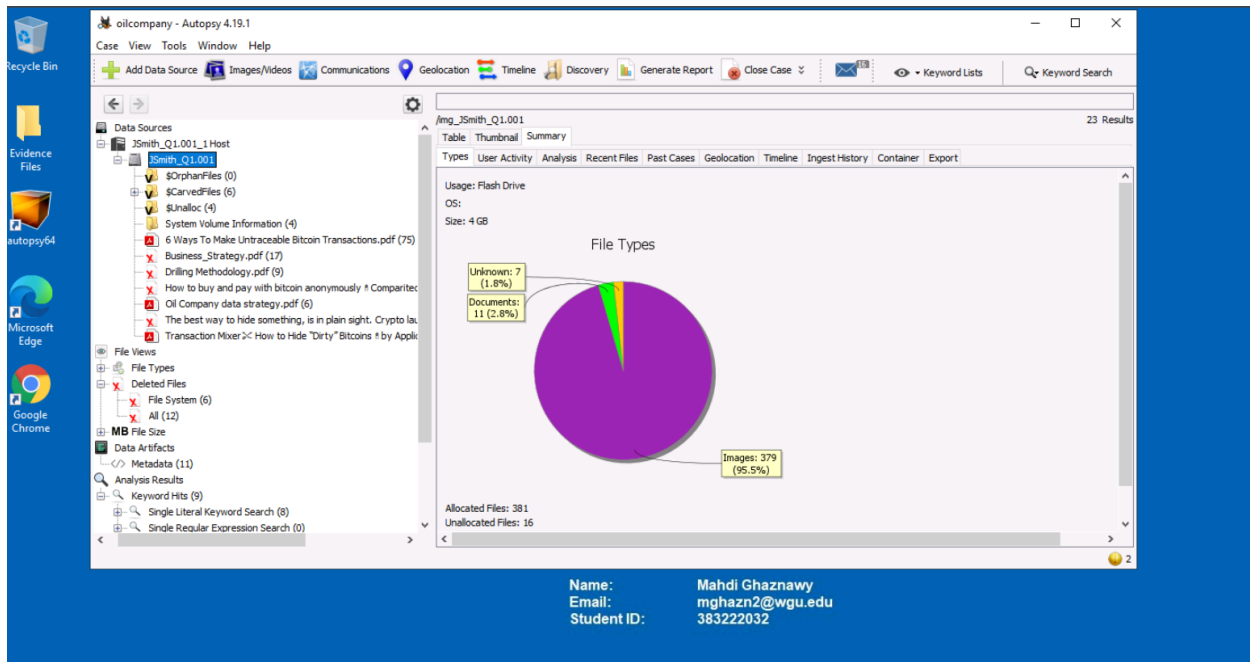


After setting up the case details, I added the data source from the disk image provided. This ensured that all relevant digital artifacts from the suspect's machine were included for analysis. After the evidence was loaded, the case was set up for a forensic investigation.



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.

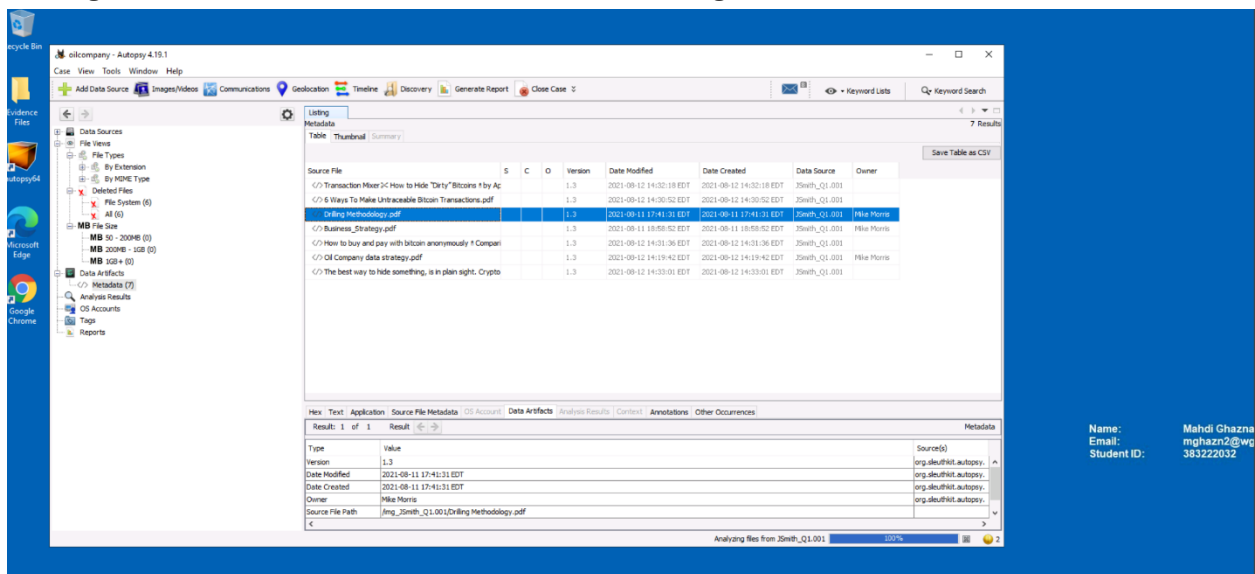


Next, I navigated to the deleted files sections within Autopsy and discovered a total of twelve deleted files.

The screenshot shows the 'Deleted Files' section in Autopsy. The left sidebar has 'Deleted Files' selected under 'File Views'. The main pane displays a table of 12 deleted files. The table has columns: Name, S, C, O, Modified Time, Change Time, Access Time, and Created Time. The files listed are:

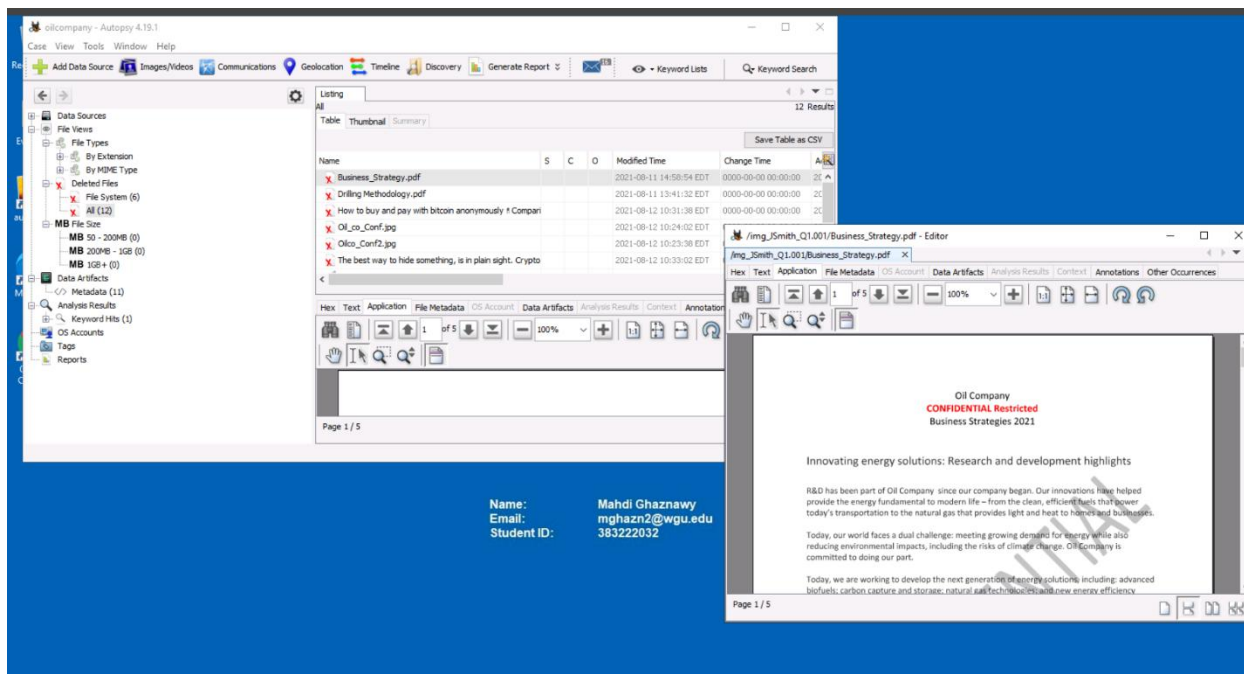
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
Business_Strategy.pdf			1	2021-08-11 14:58:54 EDT	0000-00-00 00:00:00	2021-08-13 00:00:00 EDT	2021-08-13 15:4
Drilling Methodology.pdf			1	2021-08-11 13:41:32 EDT	0000-00-00 00:00:00	2021-08-13 00:00:00 EDT	2021-08-13 15:4
How to buy and pay with bitcoin anonymously * Compari			1	2021-08-12 10:31:38 EDT	0000-00-00 00:00:00	2021-08-13 00:00:00 EDT	2021-08-13 15:4
Oil_co_Conf.jpg			1	2021-08-12 10:24:02 EDT	0000-00-00 00:00:00	2021-08-13 00:00:00 EDT	2021-08-13 15:4
Oilco_Conf2.jpg			1	2021-08-12 10:23:38 EDT	0000-00-00 00:00:00	2021-08-13 00:00:00 EDT	2021-08-13 15:4
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 00:00:00 EDT	2021-08-13 15:4
f0000000_business_Strategy.pdf			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00
f0001128_Drilling_Methodology.pdf			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00
f0002256.pdf			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00
f0002784.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00
f0002808.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00
f0002824.pdf			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00

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 'All (12)' selected. The main pane shows a table of 12 results. The table has columns: Name, S, C, O, Modified Time, Change Time, and Access Time. The results list various files, including 'Business_Strategy.pdf', 'Drilling Methodology.pdf', 'Oil Company data strategy.pdf', and 'Transaction Mixer 2C How to Hide "Dirty" Bitcoins * by Appli...'. The 'Drilling Methodology.pdf' file is highlighted. Below the table, there is a preview of the PDF document. The preview shows the title 'Oil Company CONFIDENTIAL Restricted Oil Strategies 2021 Field 007-A'. The text in the preview describes the field and the methods used for oil extraction. The preview also includes a diagram labeled 'Figure 1: Distribution of conventional enhanced recovery methods'.

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 00:00:00 EDT
Drilling Methodology.pdf	1			2021-08-11 13:41:32 EDT	0000-00-00 00:00:00	2021-08-13 00:00:00 EDT
Oil Company data strategy.pdf	1			2021-08-12 10:31:38 EDT	0000-00-00 00:00:00	2021-08-13 00:00:00 EDT
Transaction Mixer 2C How to Hide "Dirty" Bitcoins * by Appli...	1			2021-08-12 10:24:02 EDT	0000-00-00 00:00:00	2021-08-13 00:00:00 EDT
Oil_co_Conf2.jpg	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 la...	1			2021-08-12 10:33:02 EDT	0000-00-00 00:00:00	2021-08-13 00:00:00 EDT
f0000000_business_Strategy.pdf	1			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0001128_Drilling_Methodology.pdf	1			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0002256.pdf	1			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0002784.jpg	1			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0002808.jpg	1			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0002824.pdf	1			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

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 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.

The screenshot shows the Autopsy 4.19.1 interface. The left sidebar displays the file system structure, including 'System Volume Information', '6 Ways To Make Untraceable Bitcoin Transactions.pdf', 'Business_Strategy.pdf', 'Drilling Methodology.pdf', 'How to buy and pay with bitcoin anonymously + Comparitech', 'Oil Company data strategy.pdf', 'The best way to hide something, is in plain sight. Crypto la...', and 'Transaction Mixer >C How to Hide "Dirty" Bitcoins # by Appl...'. The main window shows a table of search results with columns: Name, S, C, O, Modified Time, Change Time, and Access Time. The table lists various files, including 'Business_Strategy.pdf', 'Drilling Methodology.pdf', 'Oil_Conf2.jpg', 'Oil_Conf2.jpg', 'The best way to hide something, is in plain sight. Crypto', 'f0000000_business_strategy.pdf', 'f0002256.pdf', 'f0002784.jpg', 'f0002808.jpg', and 'f0002824.pdf'. A preview window on the right shows the document 'How to buy and pay with bitcoin anonymously + Comparitech.pdf'. The document content includes the Comparitech logo, navigation links (VPN, Antivirus, Online backup, Streaming, Blog, More), and the title 'How to buy and pay with bitcoin anonymously'. The author is listed as 'AIMEE O'DRISCOLL - VPN AND CYBERSECURITY EXPERT' with the date 'April 18, 2018'.

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

The screenshot shows the Autopsy 4.19.1 interface. The left sidebar displays the file system structure, including 'System Volume Information', '6 Ways To Make Untraceable Bitcoin Transactions.pdf', 'Business_Strategy.pdf', 'Drilling Methodology.pdf', 'How to buy and pay with bitcoin anonymously + Comparitech', 'Oil Company data strategy.pdf', 'The best way to hide something, is in plain sight. Crypto la...', and 'Transaction Mixer >C How to Hide "Dirty" Bitcoins # by Appl...'. The main window shows a table of search results with columns: Name, S, C, O, Modified Time, Change Time, and Access Time. The table lists various files, including 'Business_Strategy.pdf', 'Drilling Methodology.pdf', 'Oil_Conf2.jpg', 'Oil_Conf2.jpg', 'The best way to hide something, is in plain sight. Crypto', 'f0000000_business_strategy.pdf', 'f0002256.pdf', 'f0002784.jpg', 'f0002808.jpg', and 'f0002824.pdf'. A preview window on the right shows the document 'The best way to hide something, is in plain sight. Crypto laundering - Daily Fintech...'. The document content includes the title 'The best way to hide something, is in plain sight. Crypto laundering.', the author 'ILIAS LOUIS HATZIS', the date '10/08/2020', and a graphic of a network diagram.

Name: Mahdi Ghaznawy
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.

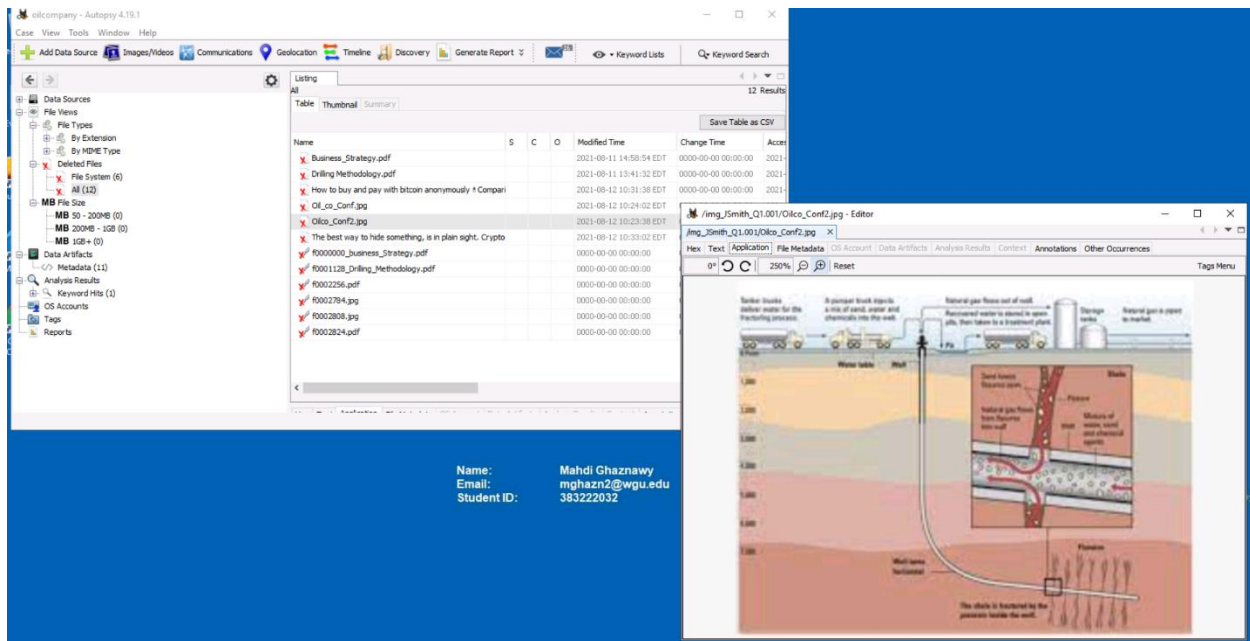
Name: Mahdi Ghaznawy
Email: mghazn2@wgu.edu
Student ID: 383222032

/img_JSmith_Q1.001/Unaloc/Unaloc_4_12656640_1087102976 - Editor
 Hex [Text] Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
 Strings Indexed Text Transaction
 Page: 23 of 32 Page Matches on page: 1 of 1 Match 100% Reset
 Text Source: Search Results
 (https://dailyfrtech.com/tag/confidential-transactions/)
 endobj
 507 0 obj
 << /JA 5168 0 R /Border [0 0 1] /Type /Annot /Subtype /Link /Rect [1168 188 1363 031 1260 1378]
 5166 0 obj
 << /Type /Action /S /URI /URI 5167 0 R >>
 endobj
 5167 0 obj
 (https://dailyfrtech.com/tag/conferences/)
 endobj
 506 0 obj
 << /JA 5168 0 R /Border [0 0 1] /Type /Annot /Subtype /Link /Rect [1076 224 1363 031 1164 375 1378]
 5168 0 obj
 << /Type /Action /S /URI /URI 5169 0 R >>
 endobj
 5169 0 obj
 (https://dailyfrtech.com/tag/conduct-risk/)
 endobj
 505 0 obj
 << /JA 5170 0 R /Border [0 0 1] /Type /Annot /Subtype /Link /Rect [1049 1362 031 1274 062 1405 031]
 5170 0 obj
 << /Type /Action /S /URI /URI 5171 0 R >>

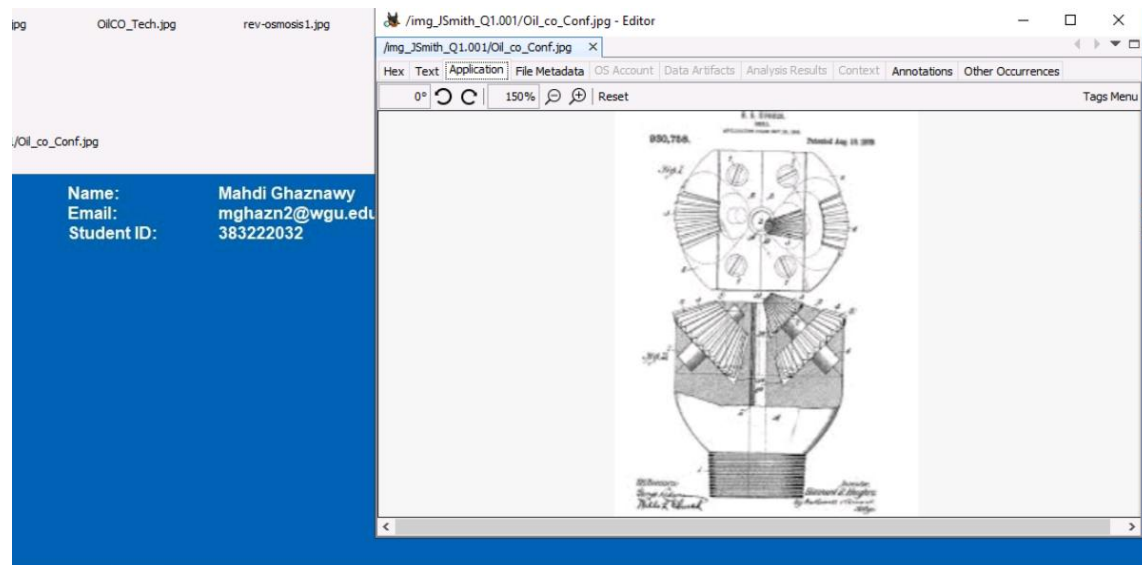
This is a screen capture of Oil_co_Conf.jpg, a proprietary schematic that was discovered in the deleted files on Mr. Smith’s machine. The image contains confidential company information.

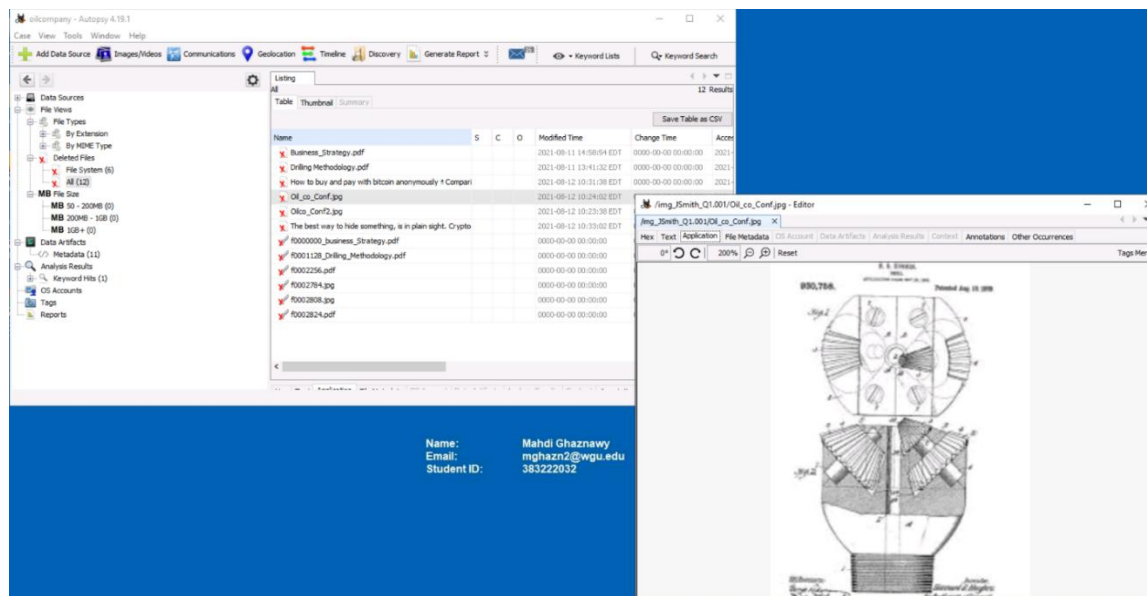
Name: Mahdi Ghaznawy
Email: mghazn2@wgu.edu
Student ID: 383222032

/img_JSmith_Q1.001/Oilco_Conf2.jpg - Editor
 Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
 0° 196% Reset
 Tags Menu



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, describing the company’s drilling methods and business plans.

The confidential documents that were discovered in the forensic analysis of Smith’s computer, including Business_Strategy.pdf, Drilling Methodology.pdf, Oil_co_Conf.jpg, and Oil_co_Conf2.jpg. These were deleted, suggesting an effort to avoid detection.

Further investigation found that Smith searched for information concerning anonymous Bitcoin transactions, cryptocurrency laundering, and financial obfuscation. This suggests that 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 activities 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.