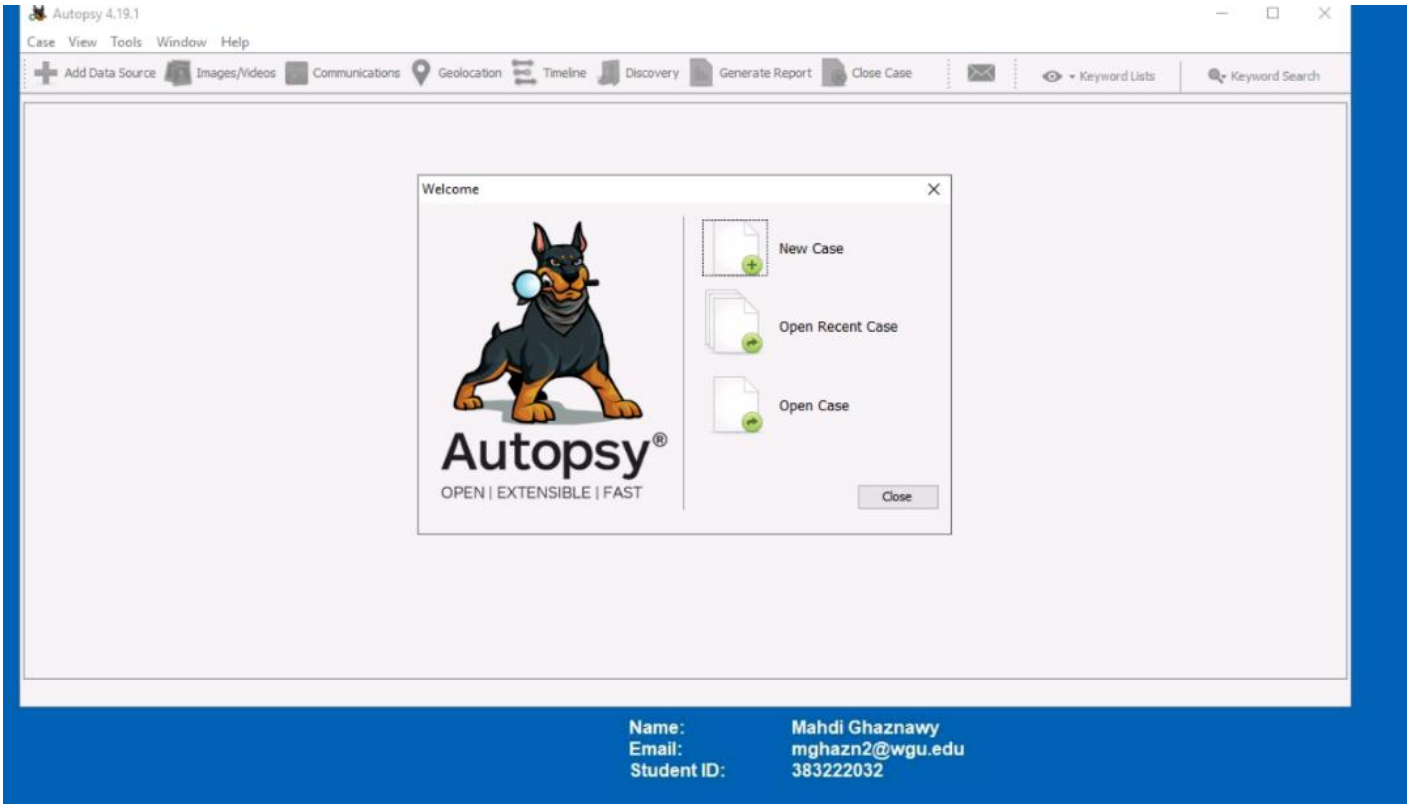
Mahdi Ghaznawy

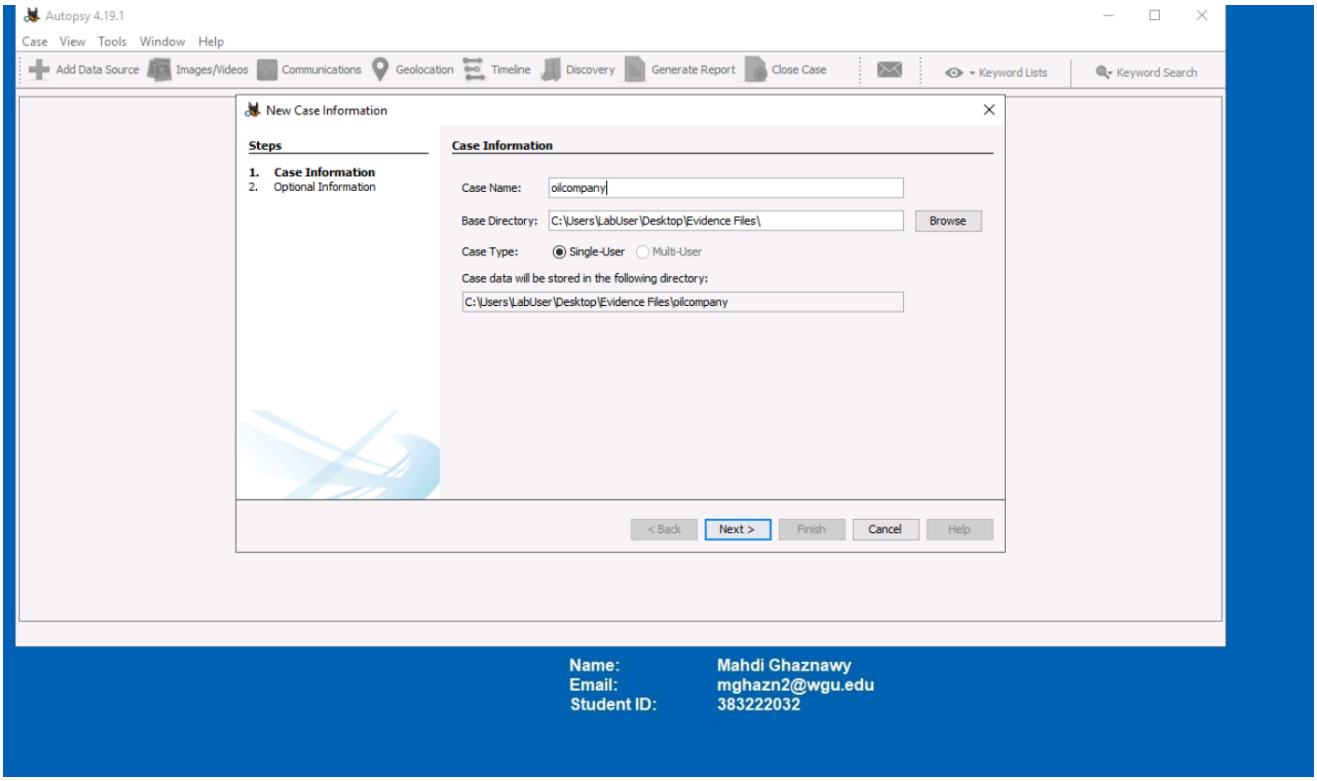
D431 – Task 2

Case File Creation and screenshots of these steps:

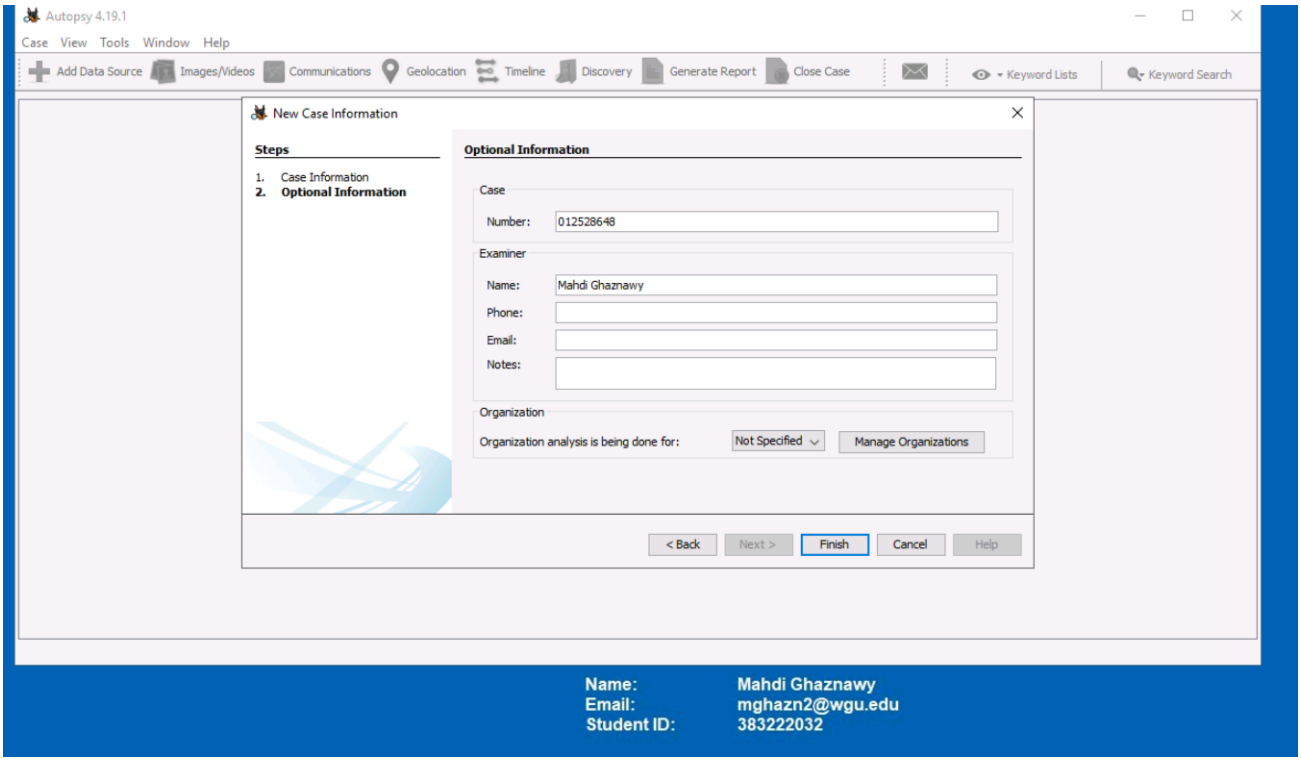
The first step was to launch the Autopsy application and create a new case. I selected "New Case" to create a forensic workspace where all investigative data and findings would be recorded and analyzed.



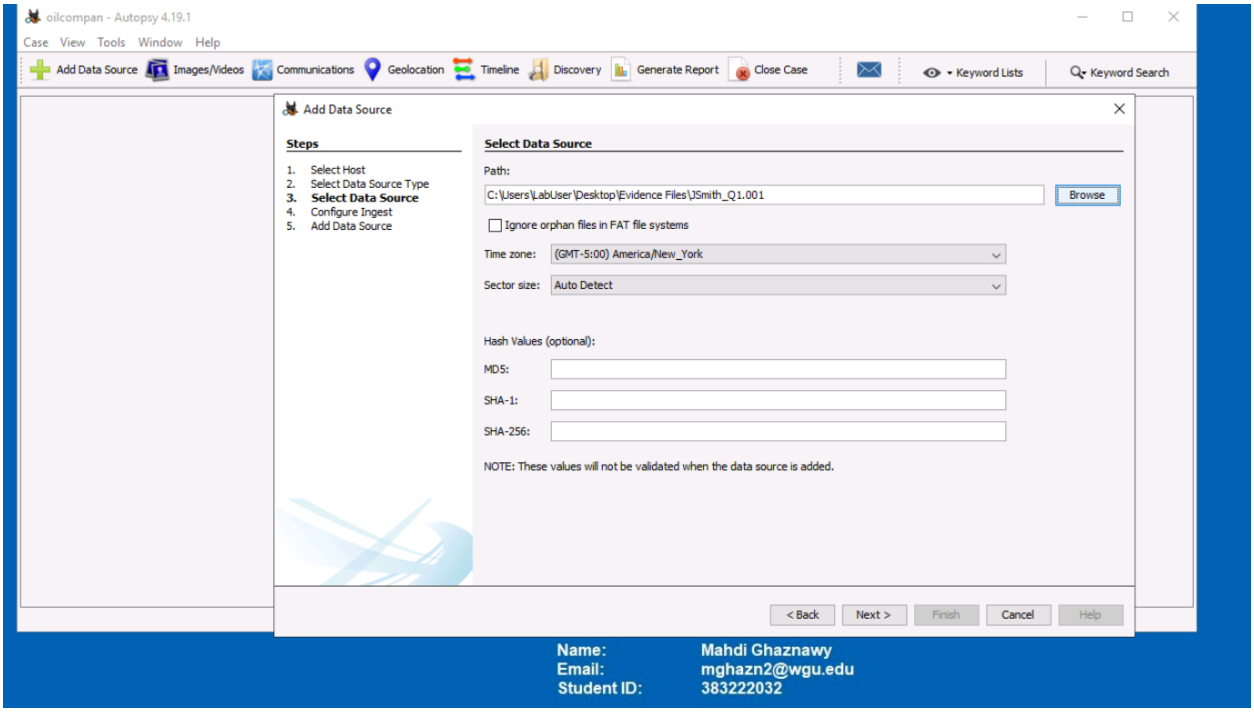
Next, I entered the necessary case details, including the case name. I also selected a base directory to store all associated files, reports, and recovered data, organizing the case for efficient analysis and future reference.



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

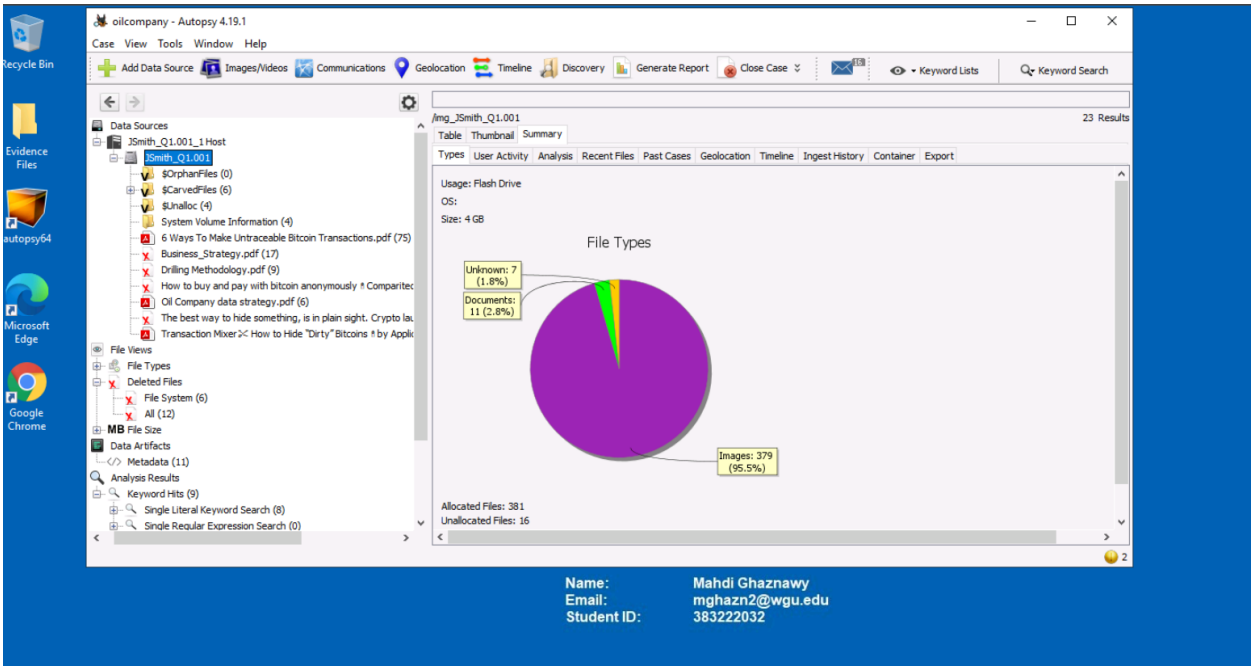


After setting up the case details, I added the data source from the disk image provided. This ensured that all relevant digital artifacts from the suspect's machine were included for analysis. After the evidence was loaded, the case was set up for a forensic investigation.

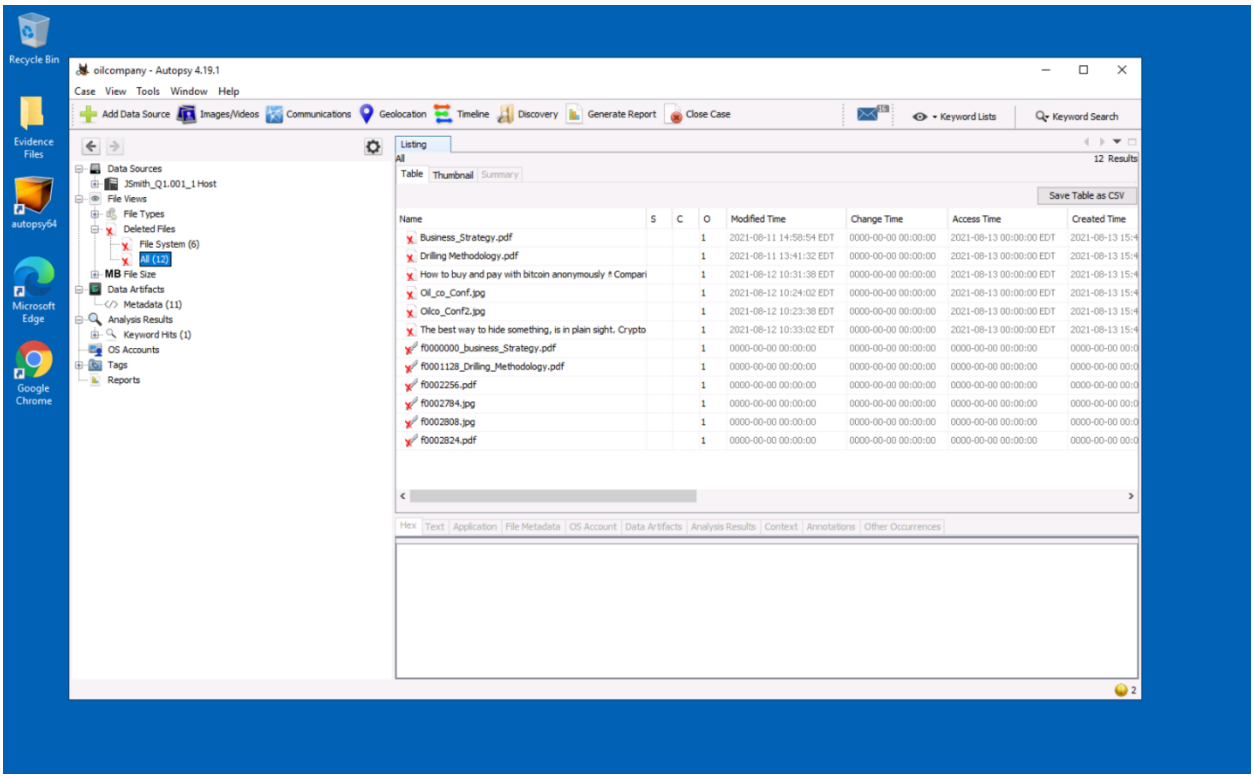


Autopsy and screenshots of these autopsy steps that support my findings and conclusions.

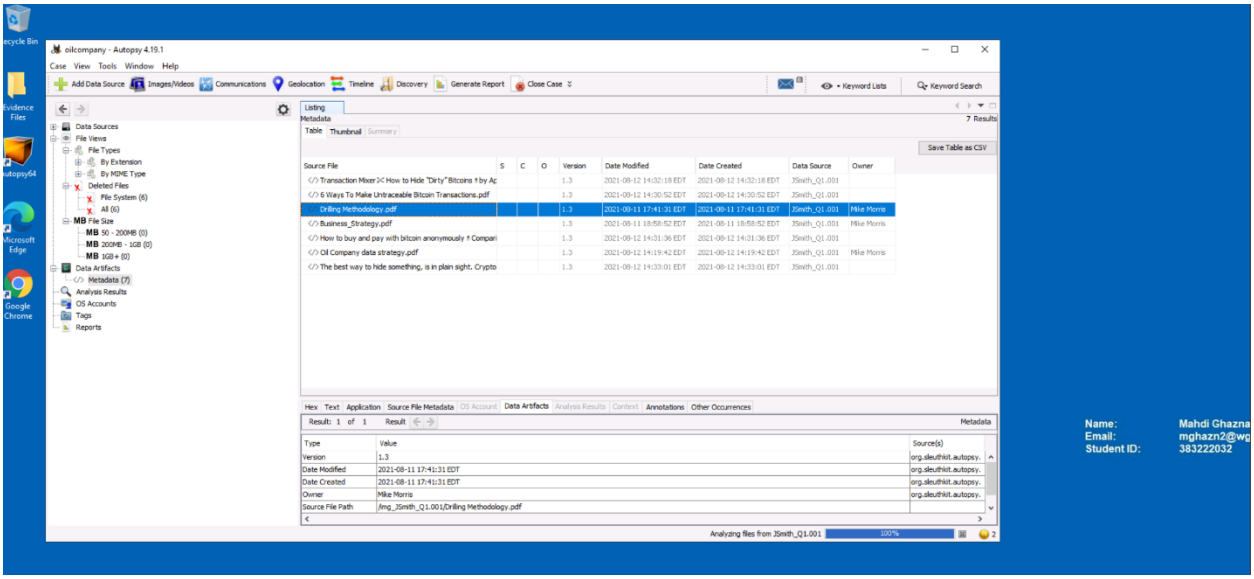
After loading the forensic image, I expanded the menus under the host JSmith_Q1.001 to get an overview of the discovered files: 379 images and 11 documents.



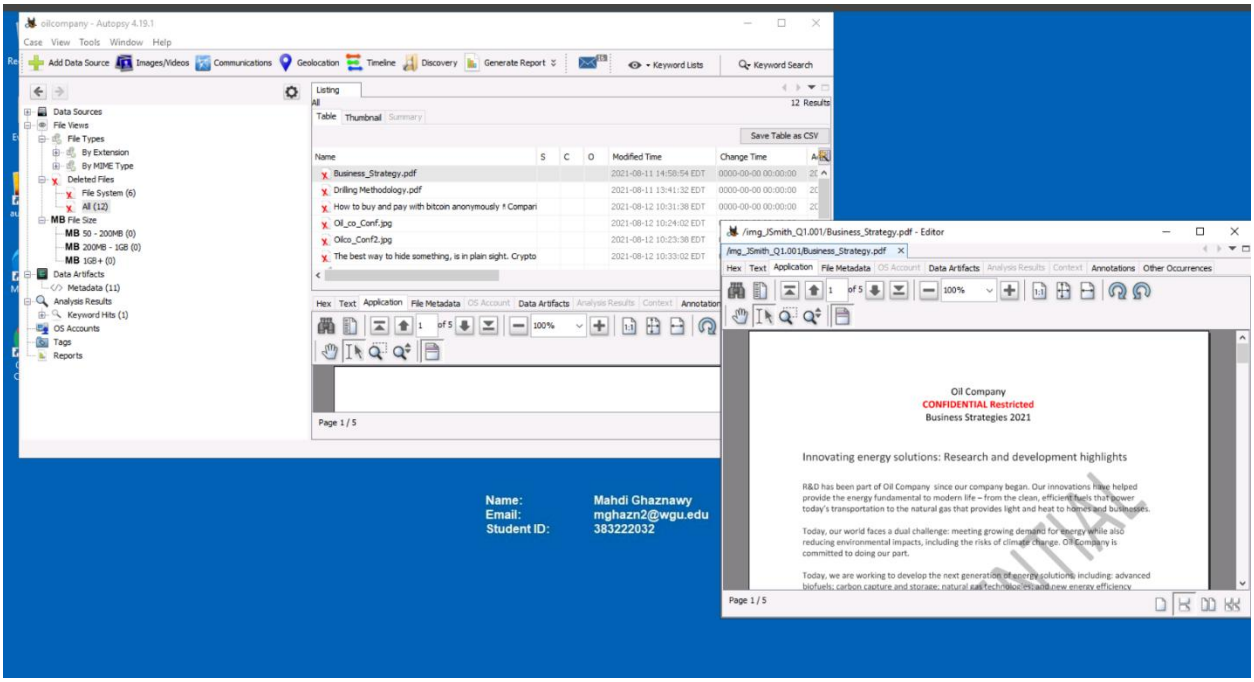
Next, I navigated to the deleted files sections within Autopsy and discovered a total of twelve deleted files.



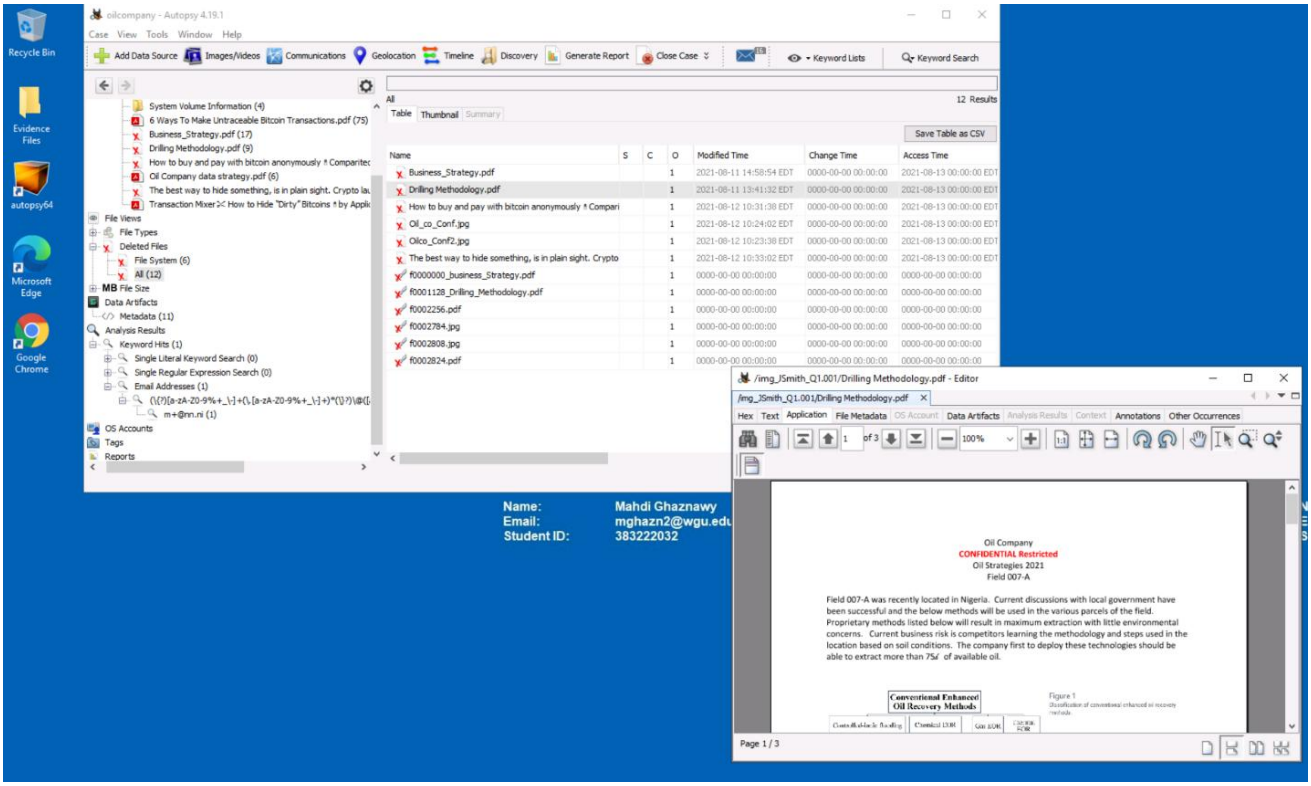
I found that Mr. Smith accessed several unauthorized image files containing confidential and proprietary information on the oil company's operations, configurations, and business strategies. Metadata confirms that these files belong to Mike Morris, not Mr. Smith.



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.

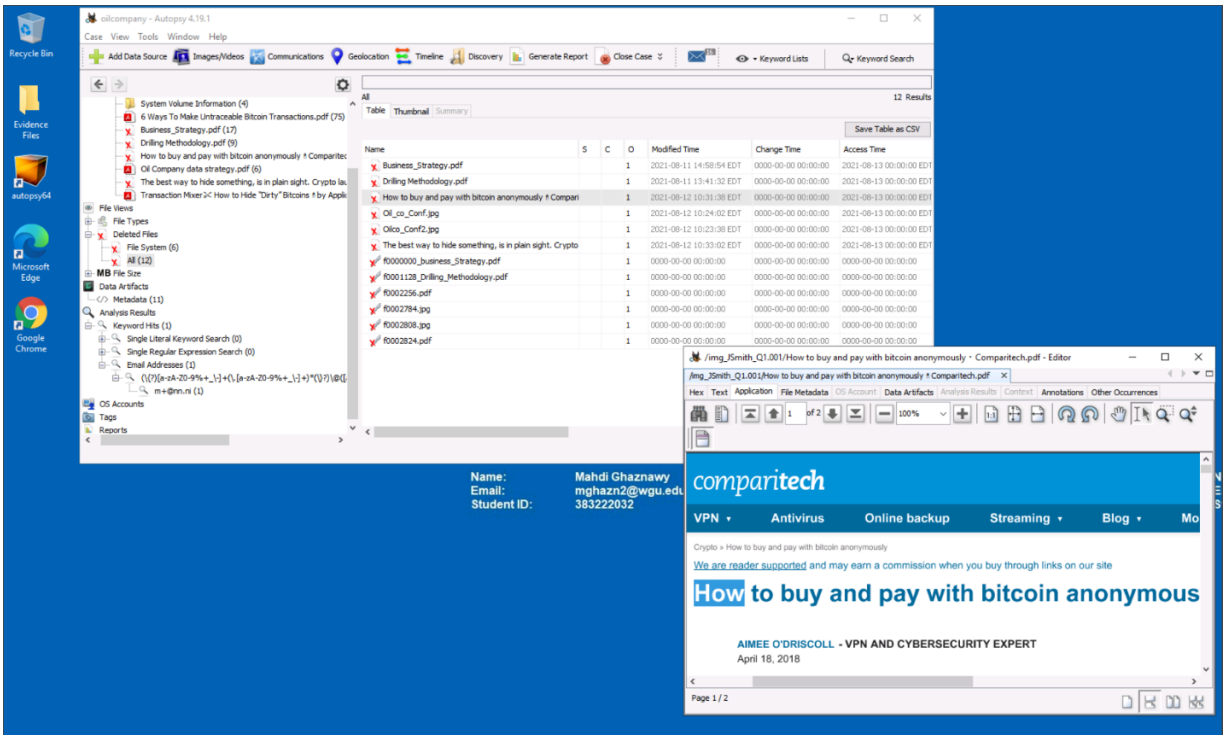


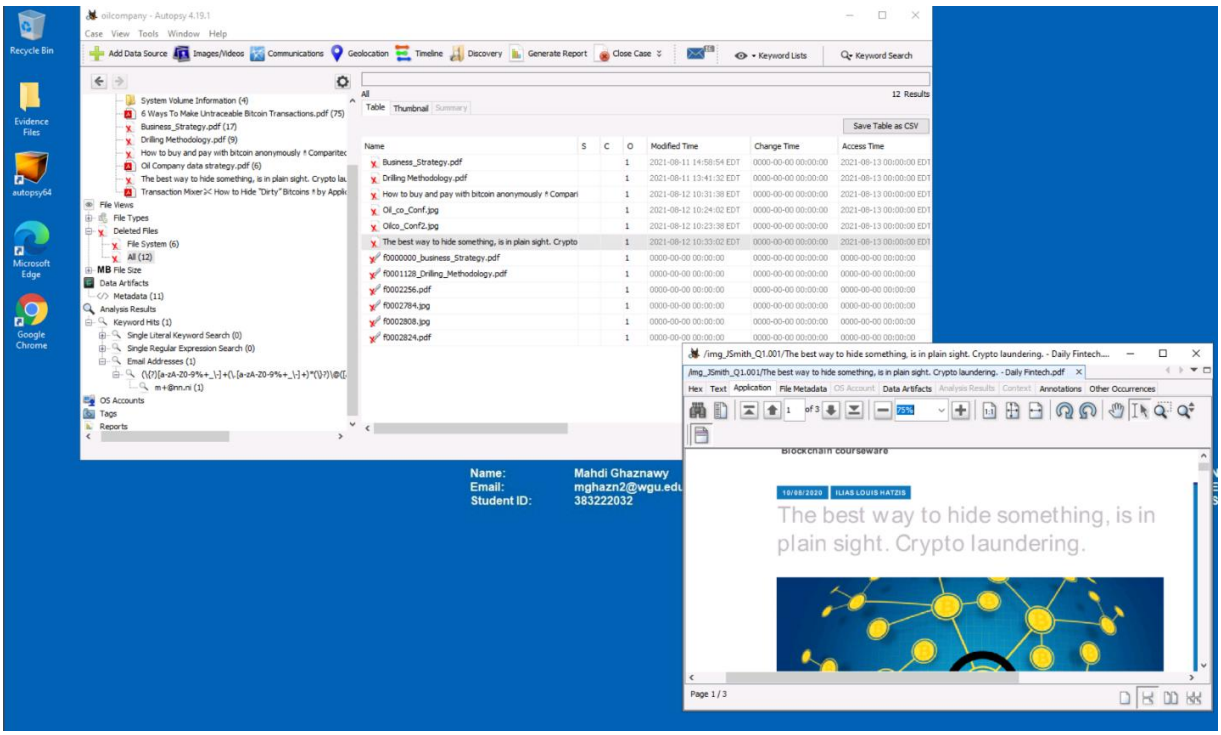
This screenshot shows another confidential file, Drilling Methodology.pdf, which was discovered to have been deleted from Mr. Smith's workstation.



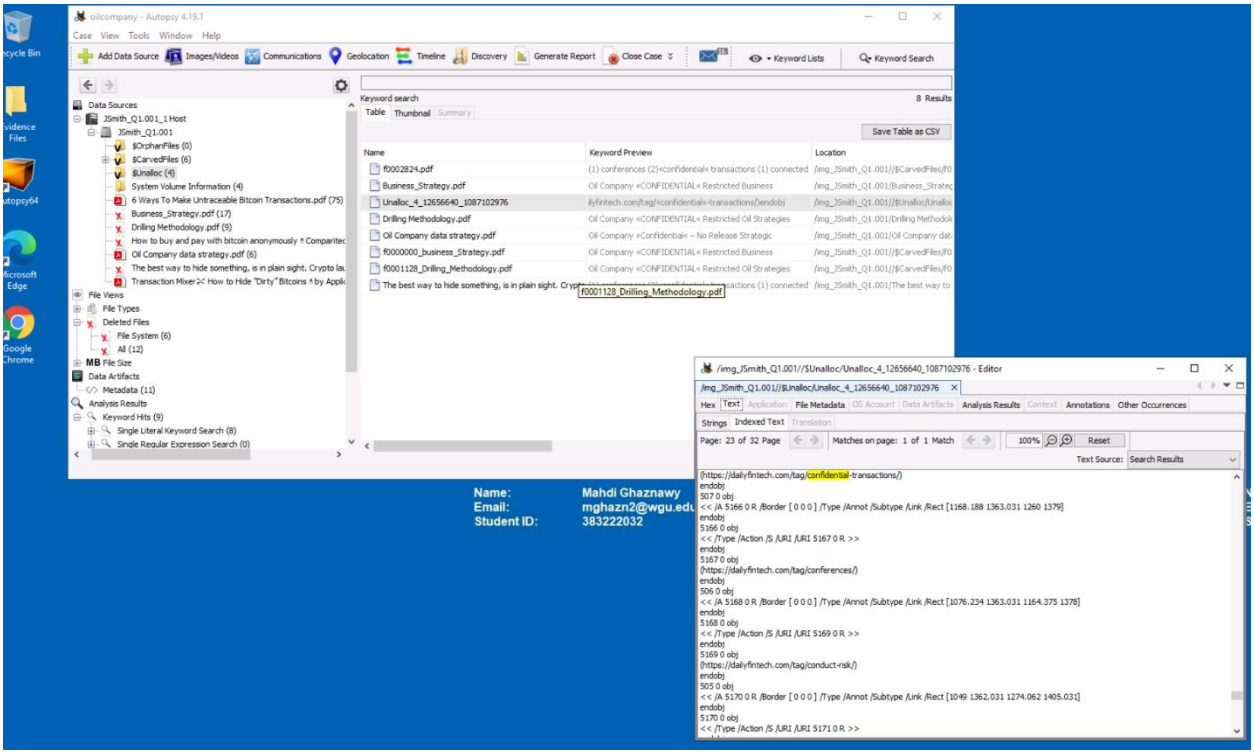
Looking more into the Files folder, it looks like John Smith was doing some extensive research on Crypto laundering and Bitcoin Transactions. This supports the claims that he

was looking to sell the proprietary information illegally.

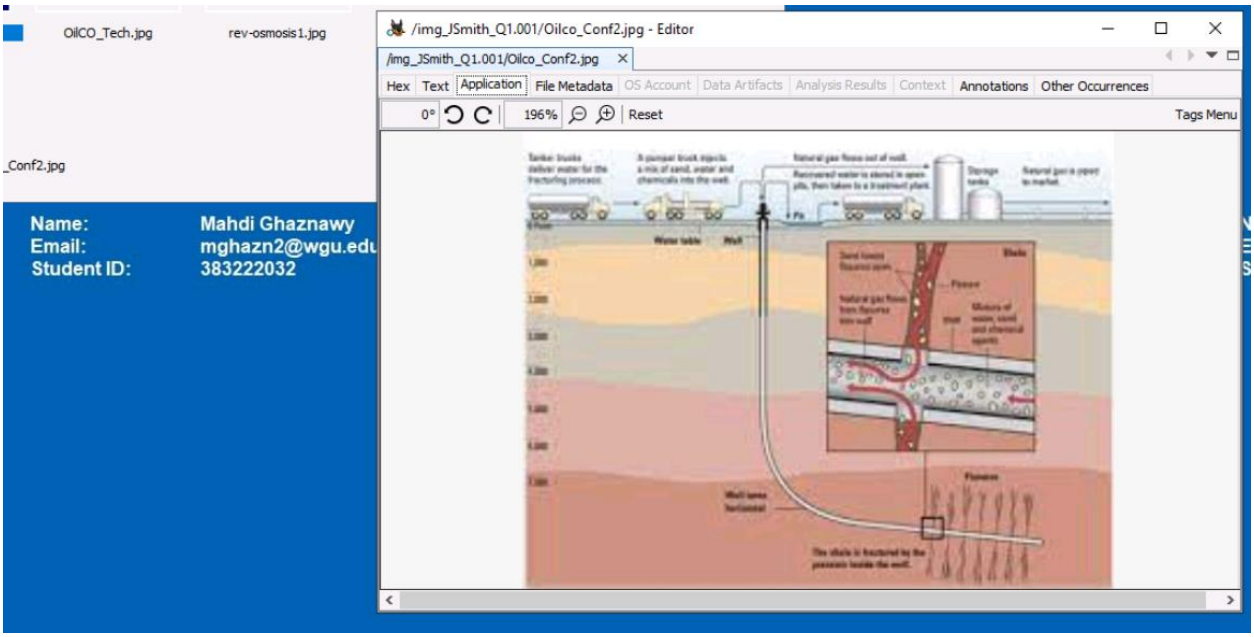


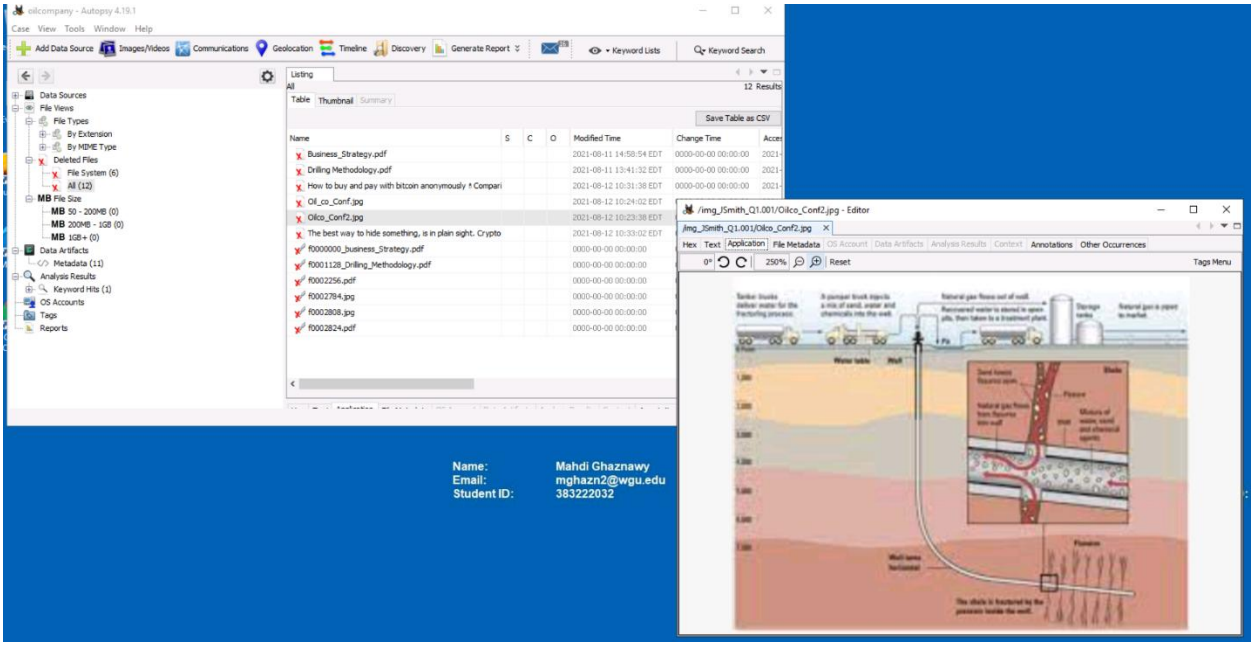


Evidence of John Smith looking at the confidential transactions. More evidence suggests that he was looking to sell the information obtained.

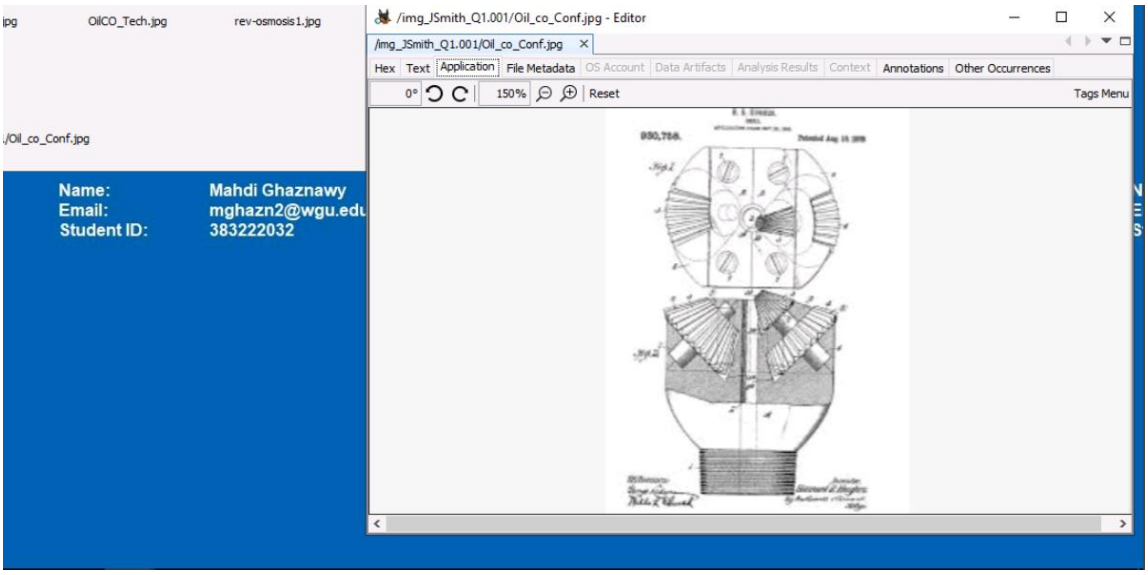


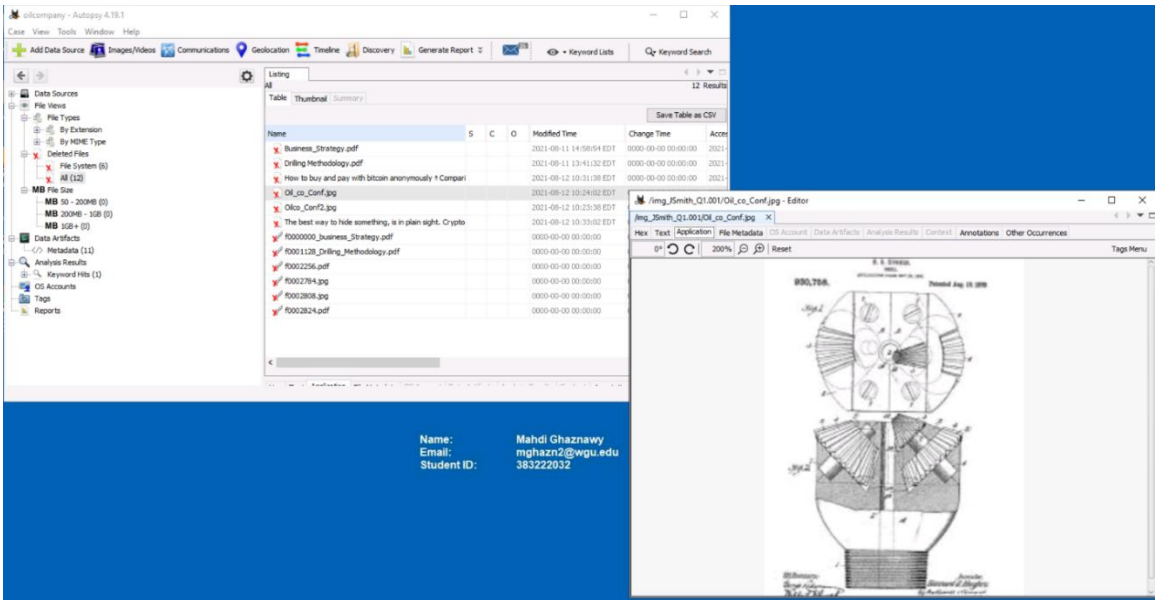
This is a screen capture of Oil_co_Conf.jpg, a proprietary schematic that was discovered in the deleted files on Mr. Smith's machine. The image contains confidential company information.





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.