Forensics Investigation Report

Scenario: An oil company’s senior management has reason to suspect that John Smith, one of the company’s mechanical engineers allegedly took information that was clearly identified as proprietary. The company’s legal office has requested digital evidence regarding the potential violation of company policy, which prohibits the sharing of proprietary information without prior approval. The employee was not authorized to access proprietary information. All employees sign nondisclosure agreements (NDAs) and acceptable use policies (AUPs). Senior management and the legal office have approved this request.  
  
You are a member of the investigative team that has been assigned to examine the digital evidence captured from the suspect’s office laptop computer and create an incident report.

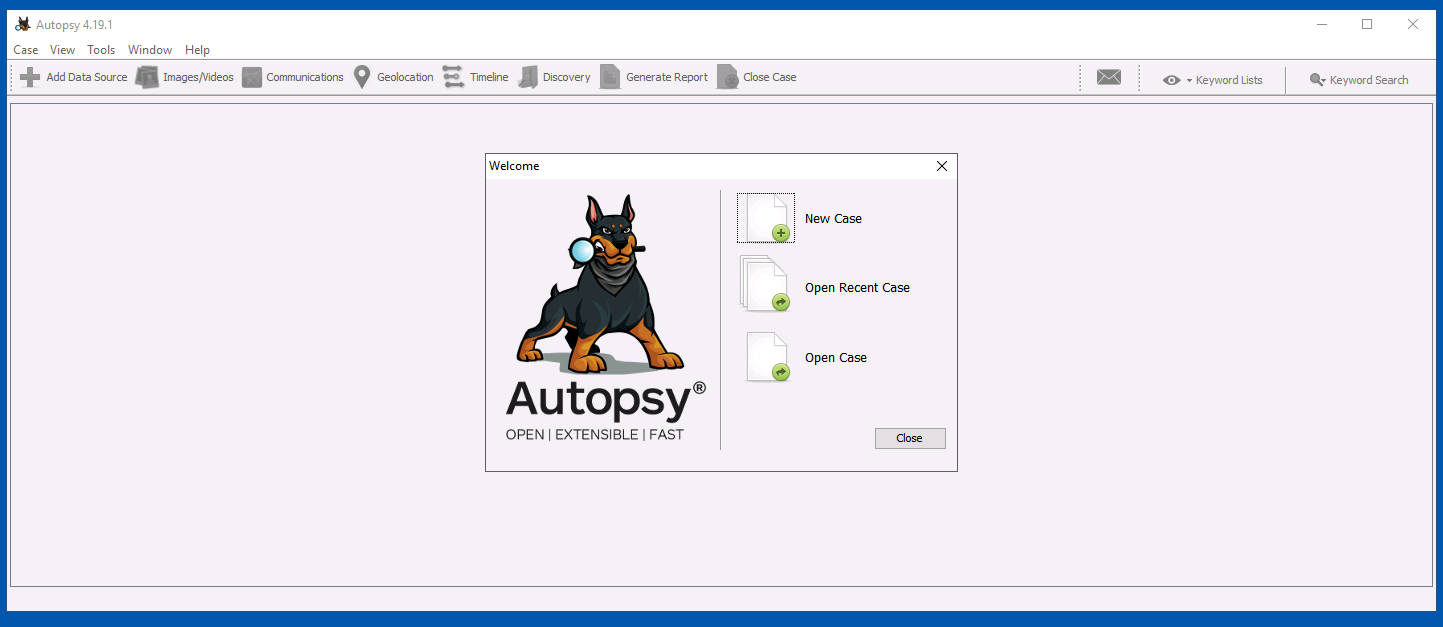
Requirements:

A.  Write a report for the team of investigators by doing the following:

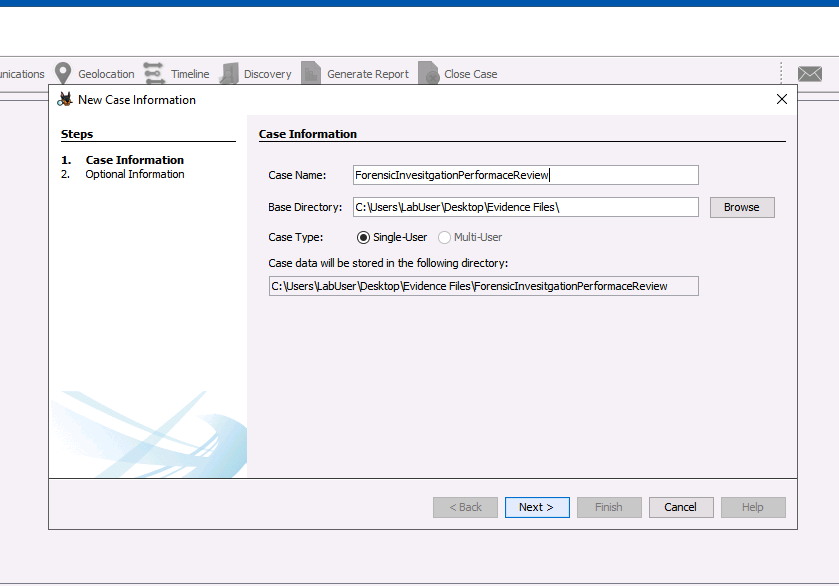
1.  Describe all steps taken in Autopsy to create the forensic system case file. Provide screenshots of these steps along with the Name, Email, and Student ID located on the desktop of the virtual environment.

* - Start Autopsy
* 

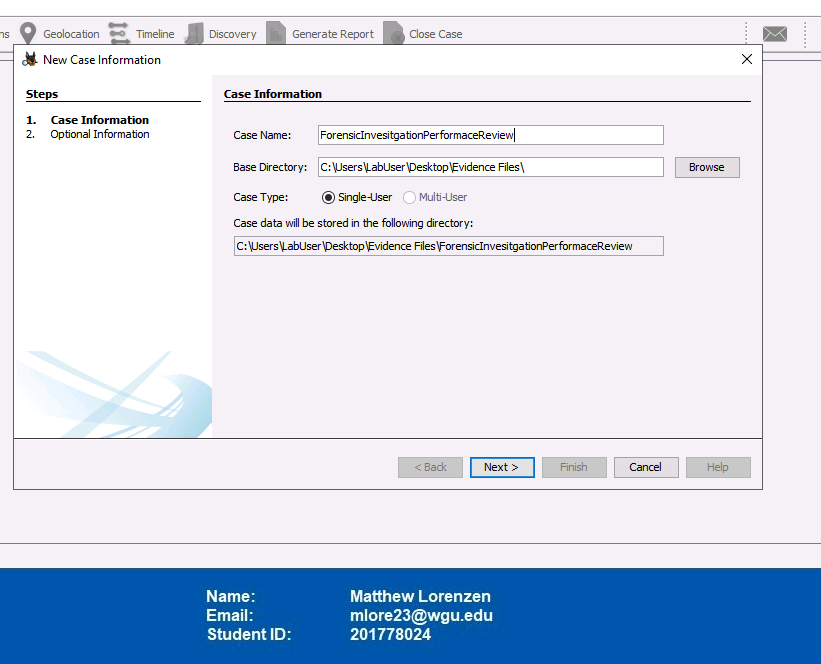
Create New Case



Name the Case



Choose directory to save case too



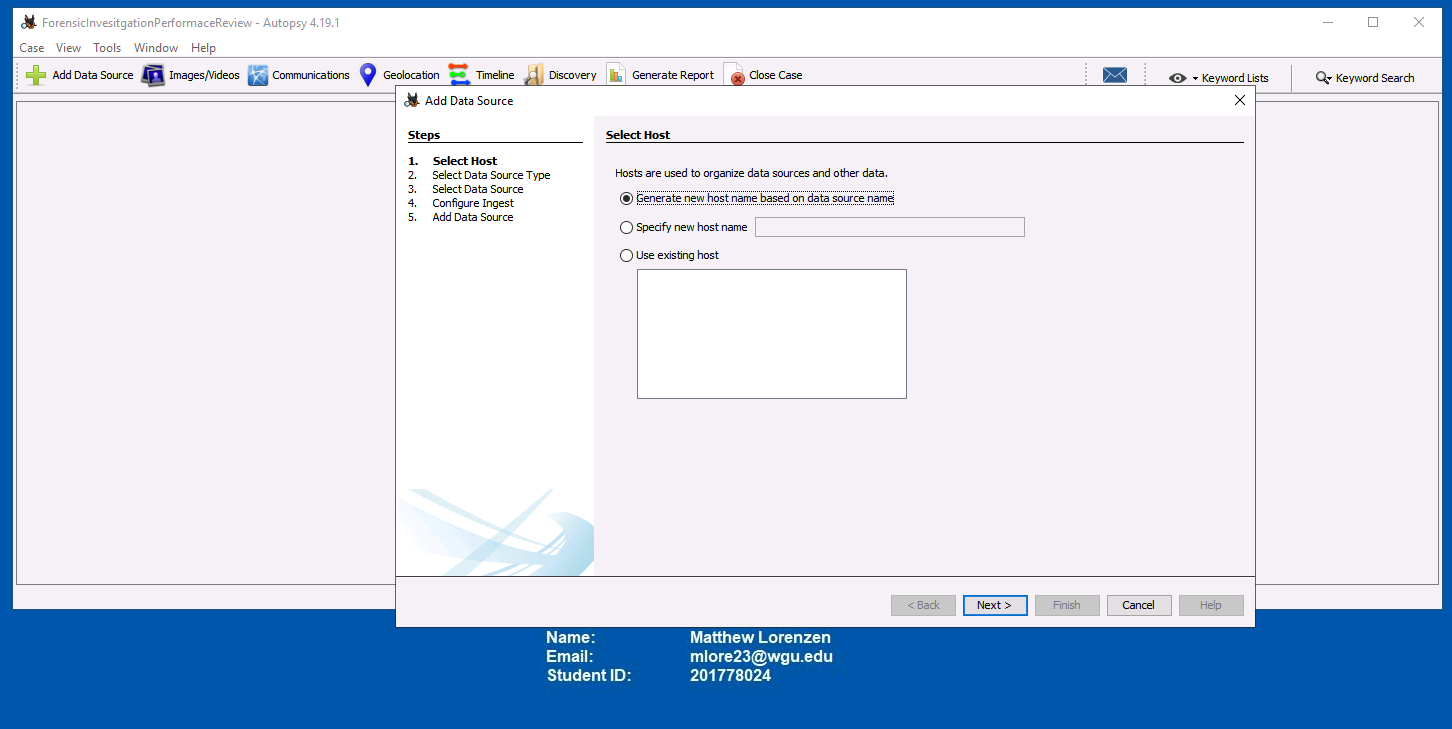
Add a case number



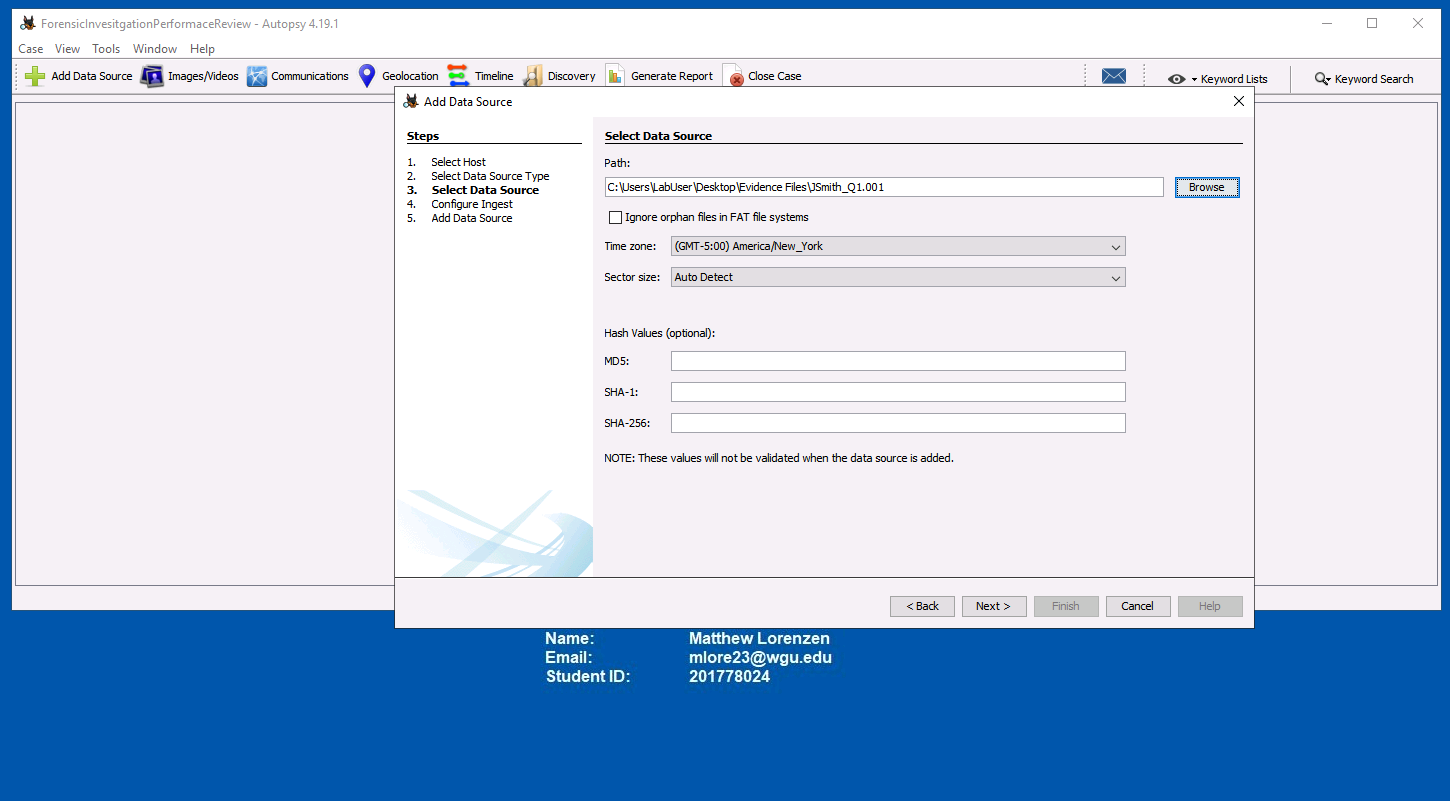
Add Investigator’s name in the Autopsy Wizard



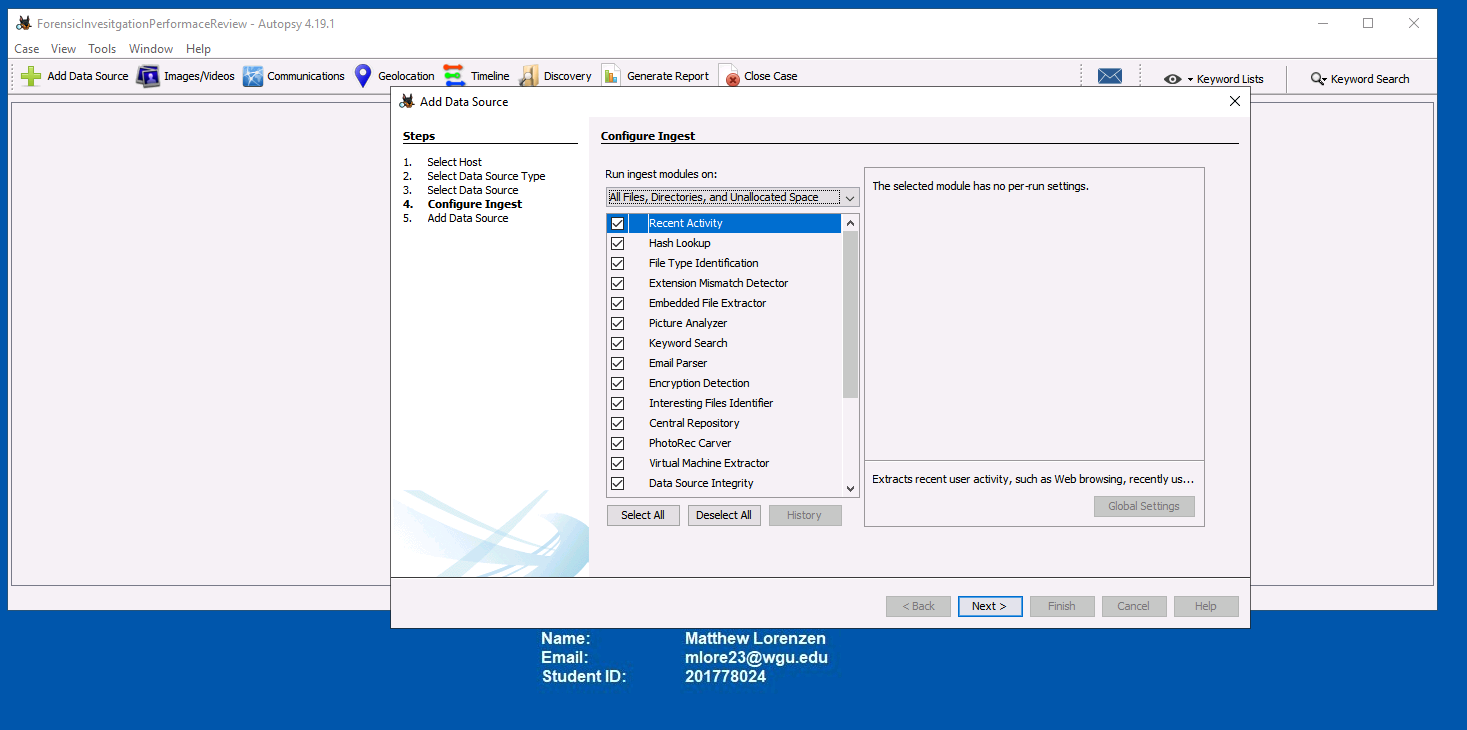
Select the host



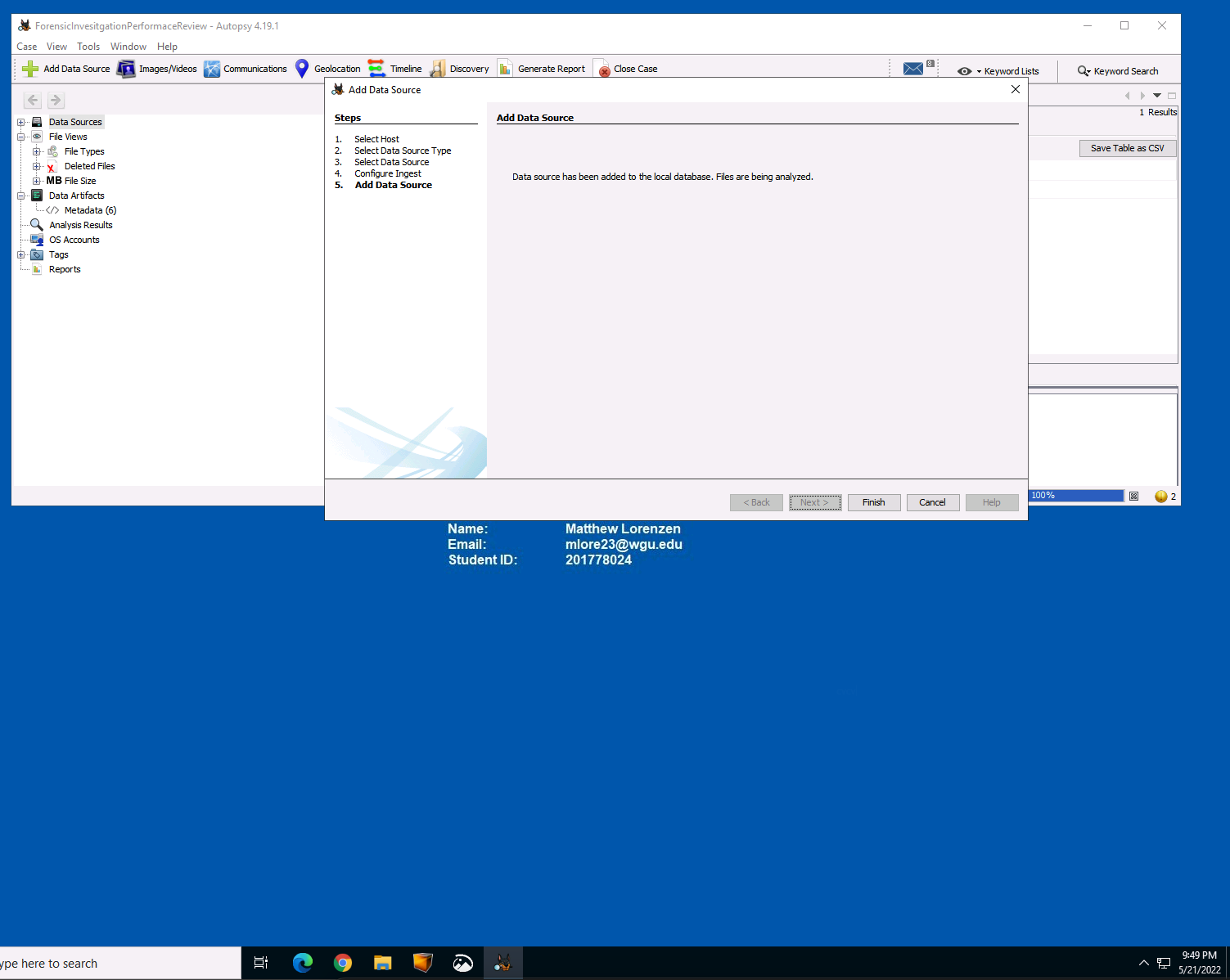
Select a data source



Configure the ingest



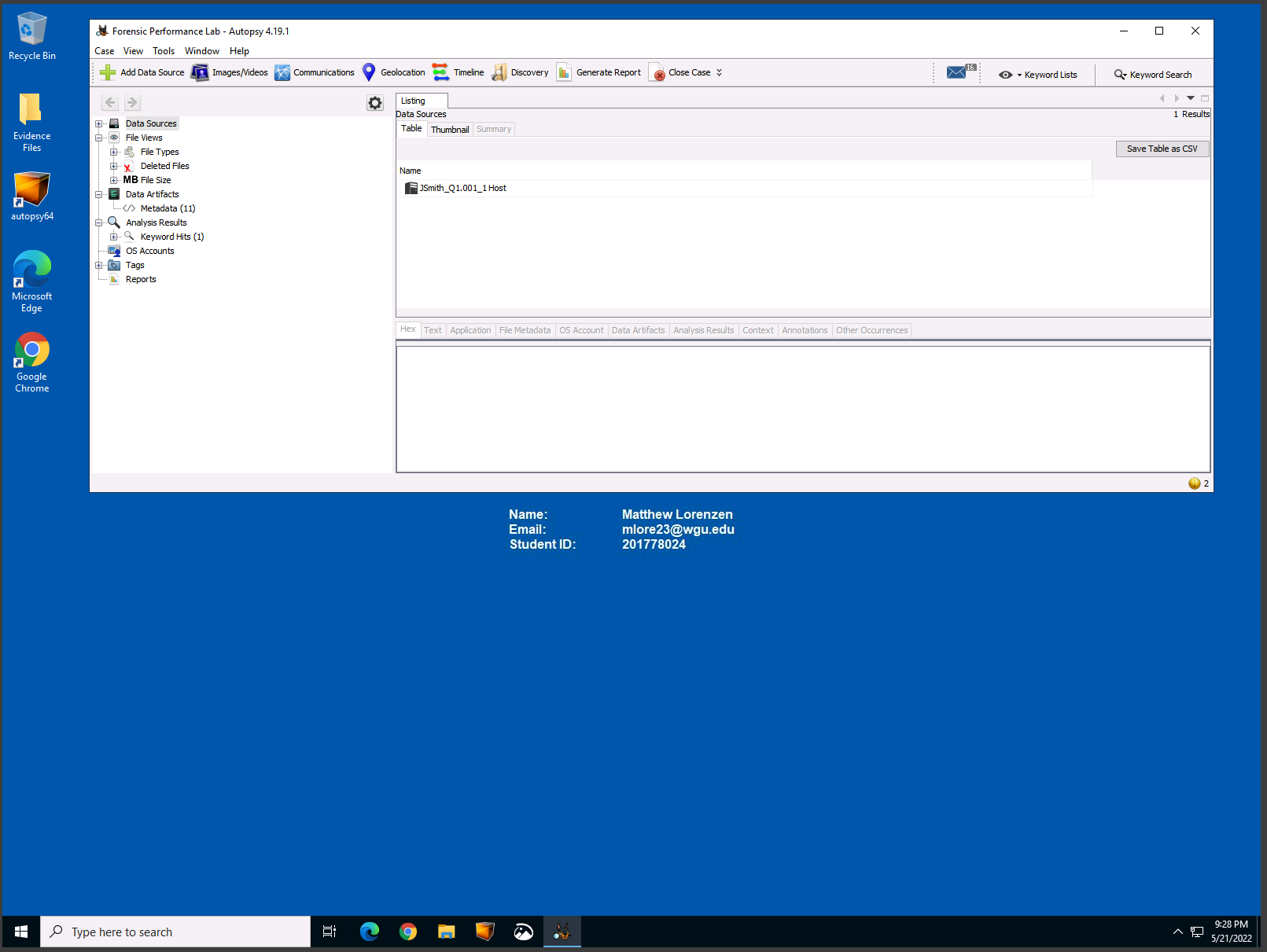
Add Data Source



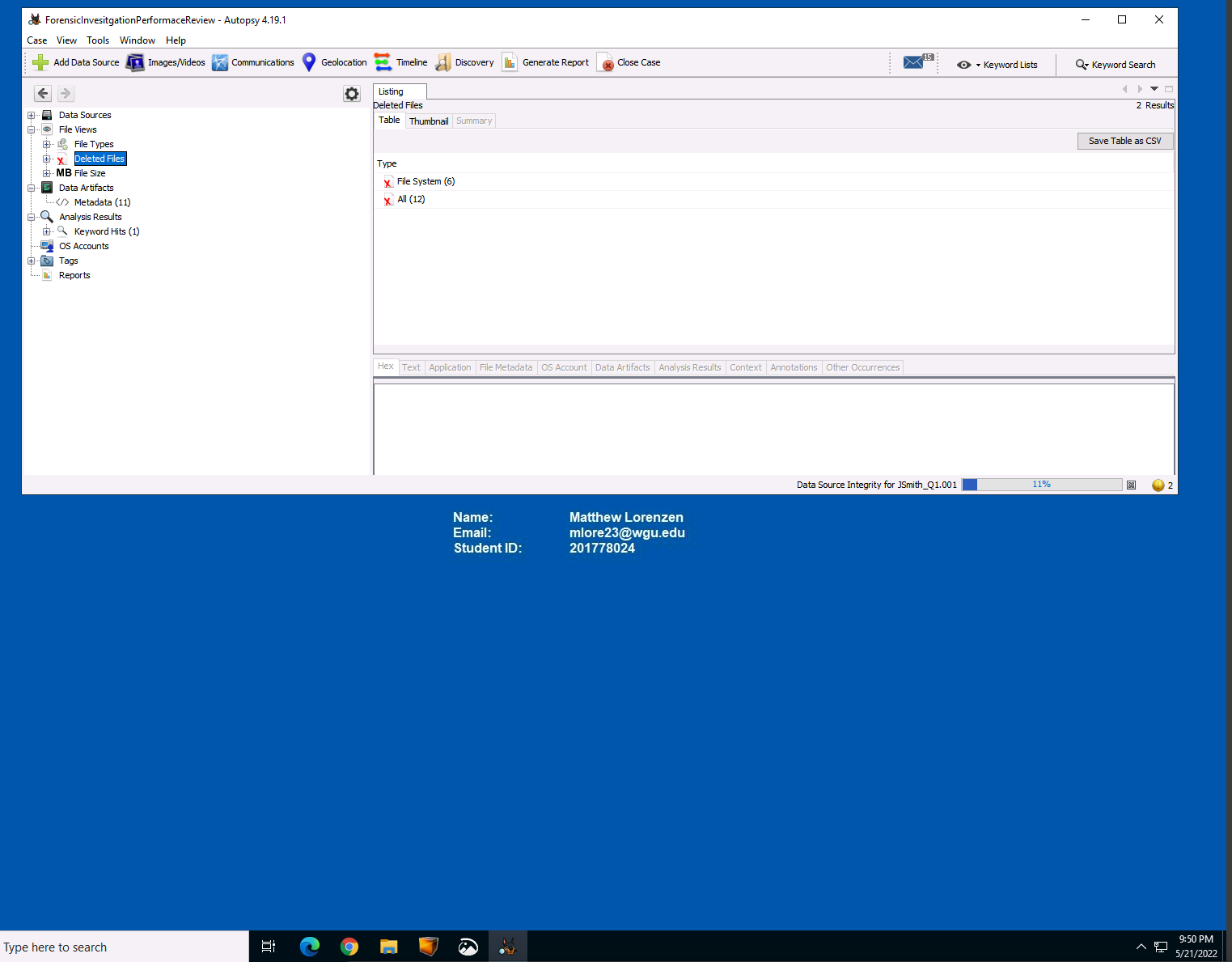
Let Autopsy run the data source

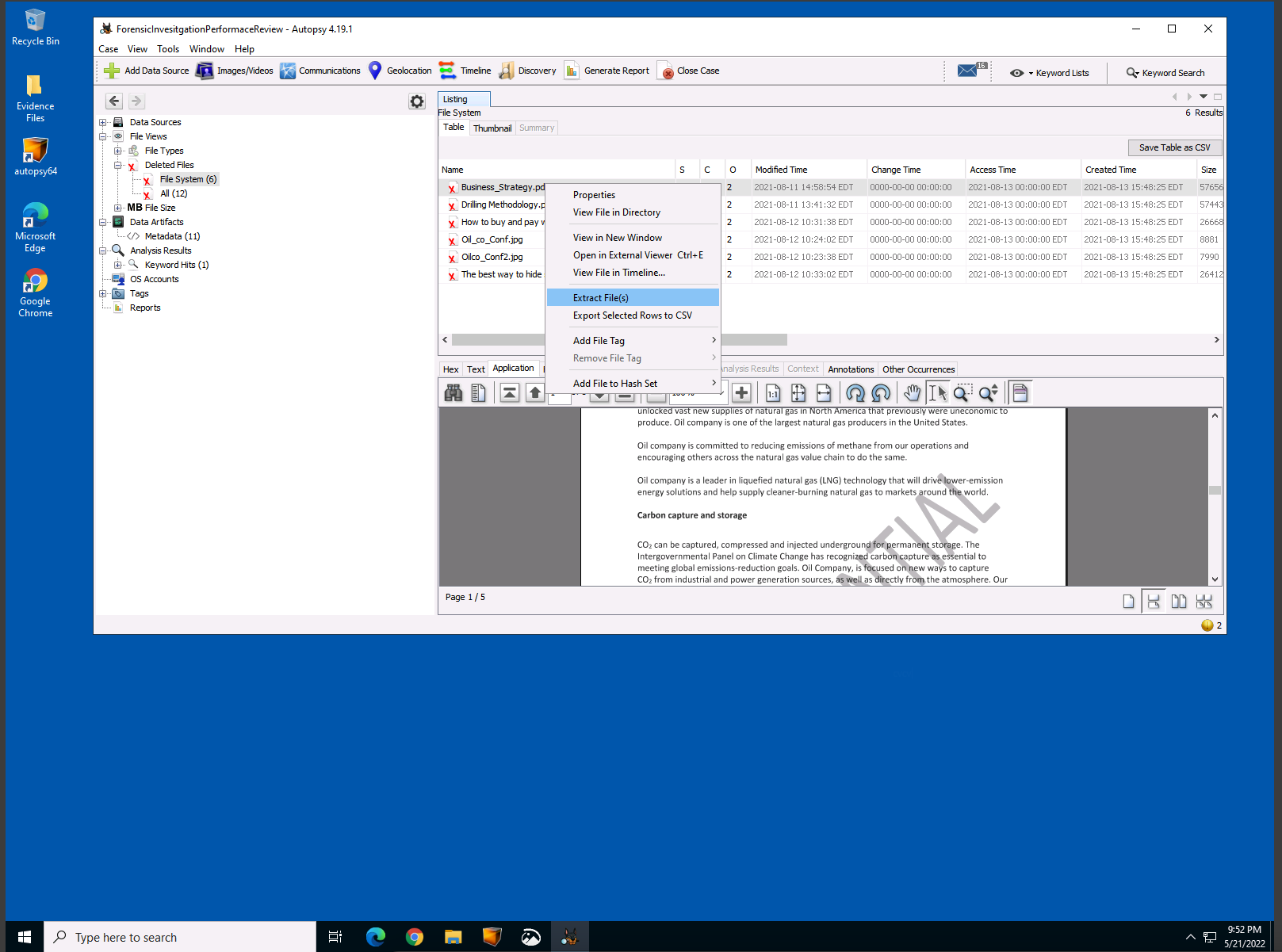
Select Finish

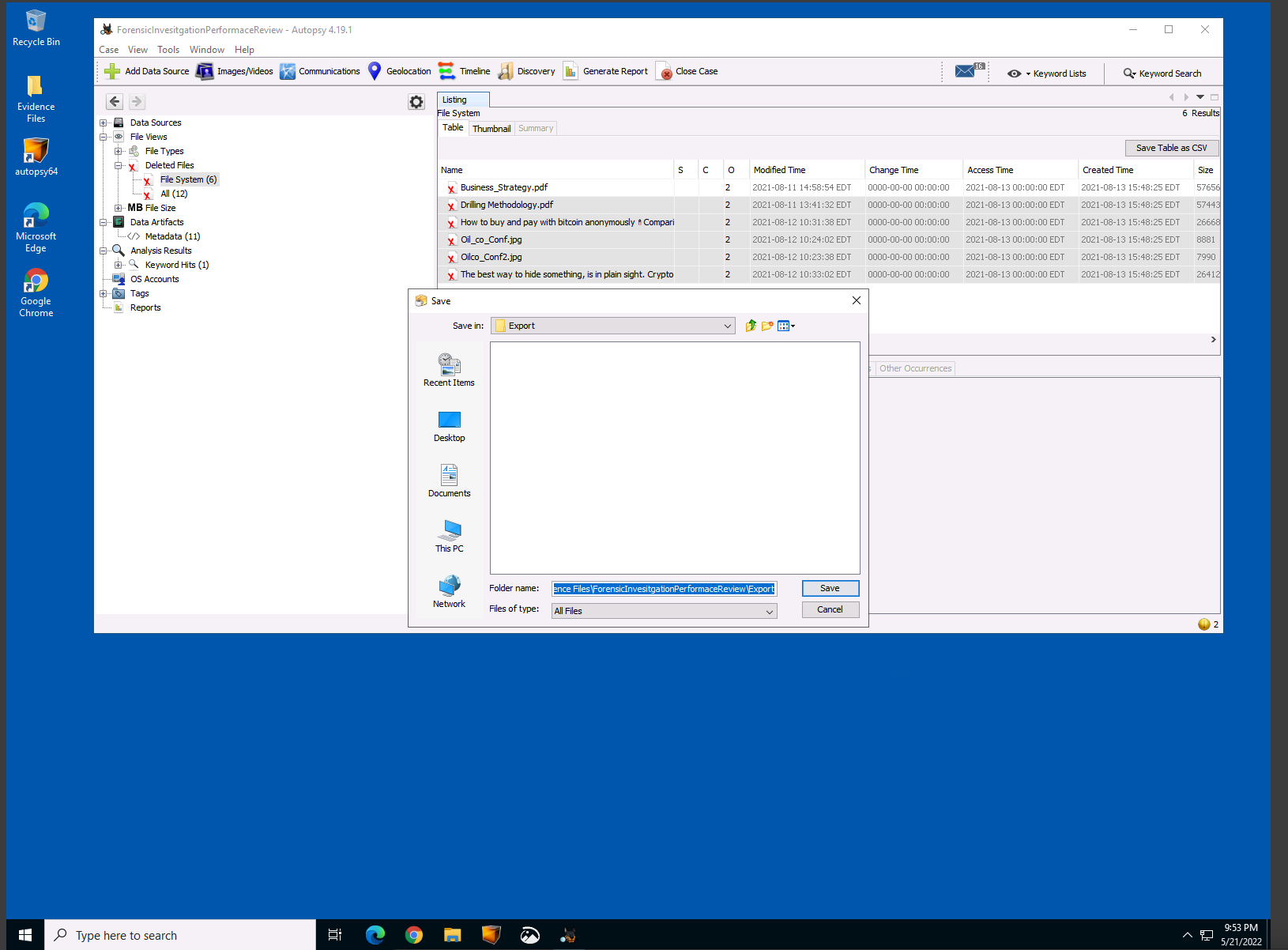
Begin analysis

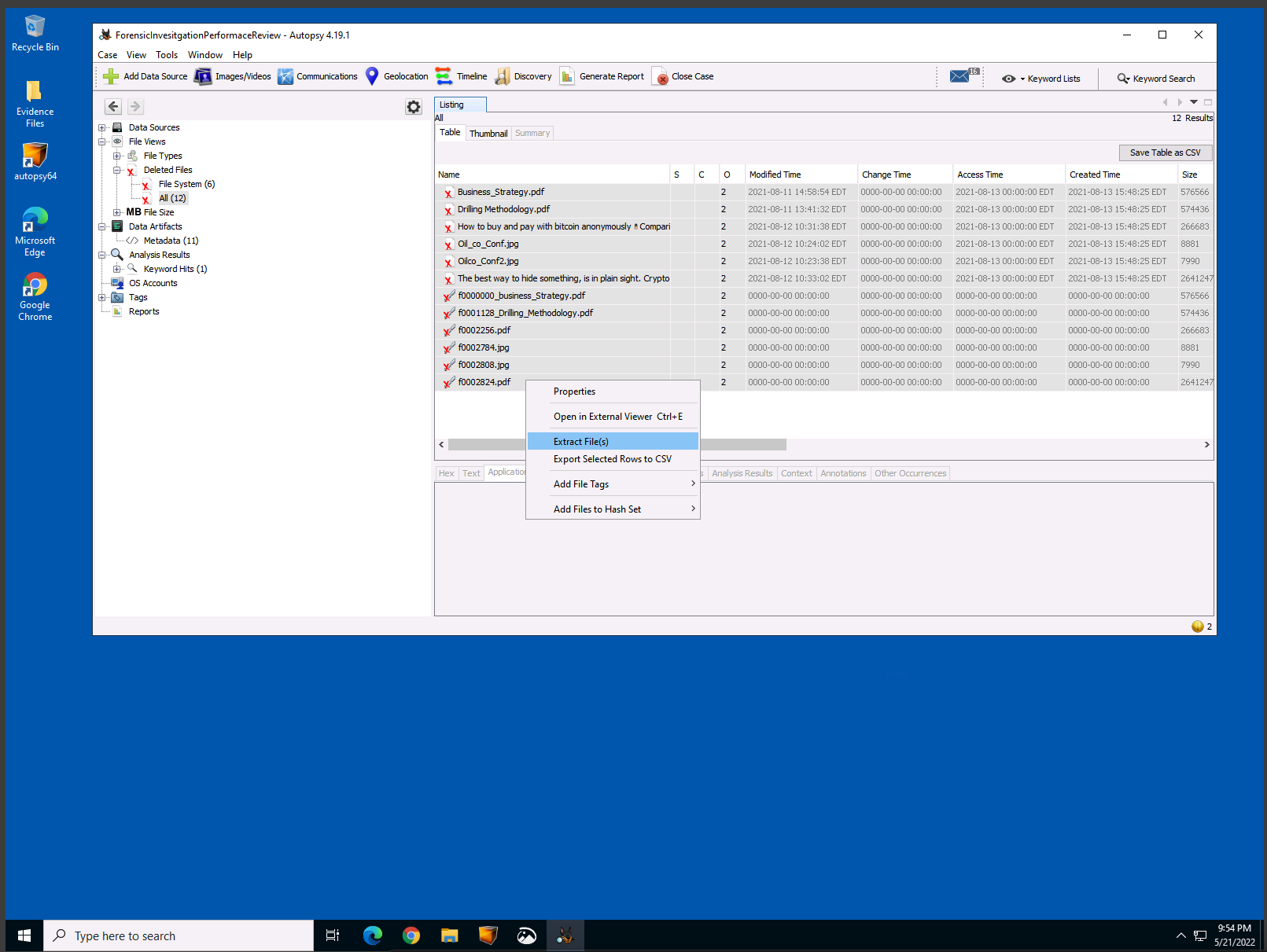


2.  Describe all steps taken in Autopsy to identify potential evidence, including data files, deleted data files, directories, or drive partitions. Provide screenshots of these steps along with the Name, Email, and Student ID located on the desktop of the virtual environment.

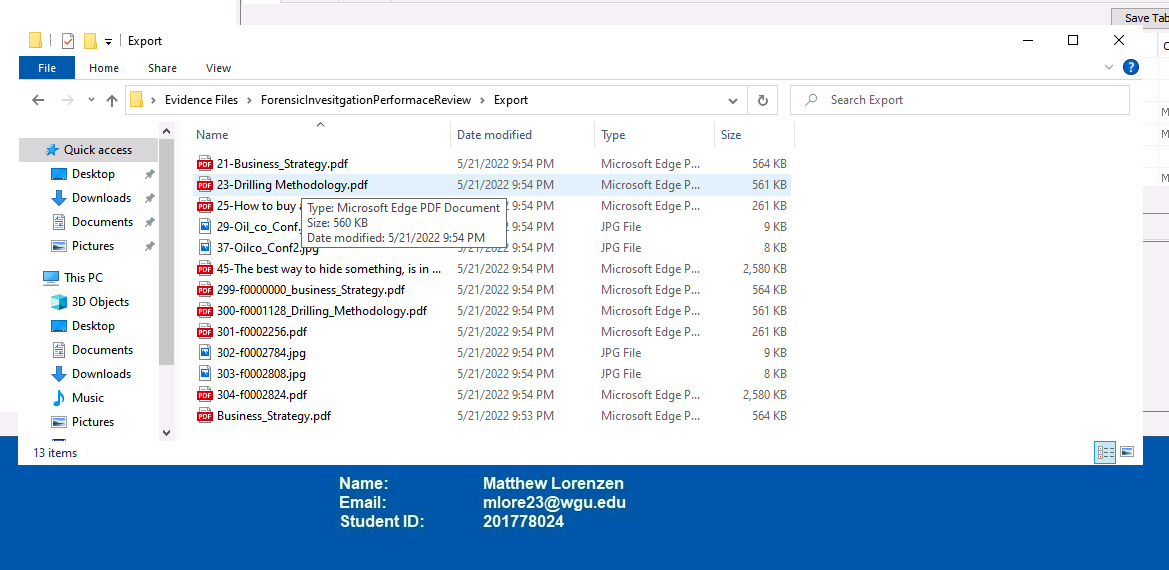
First thing we will look at is the deleted files: 

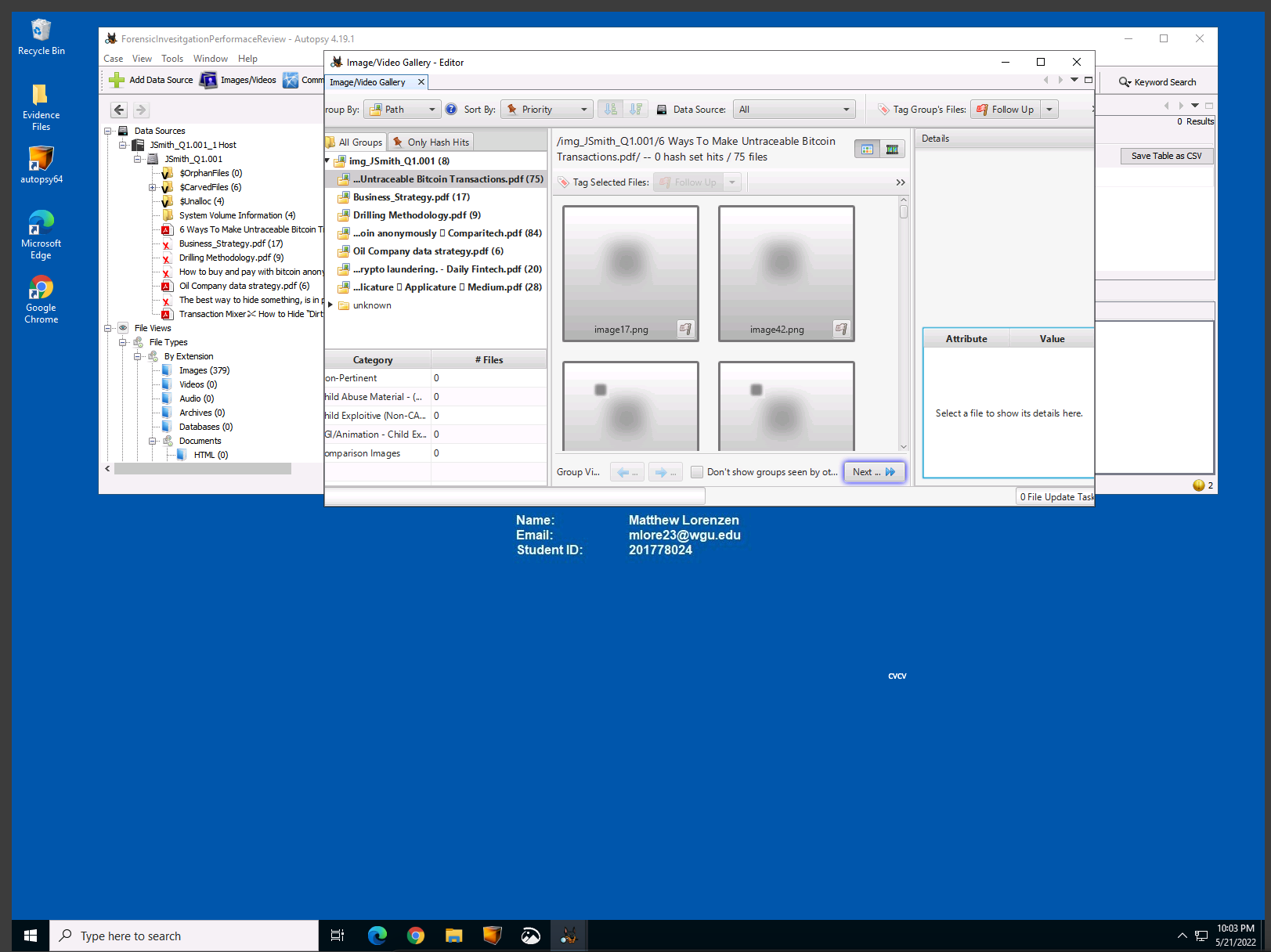
Extracting Deleted Files to Example\Export

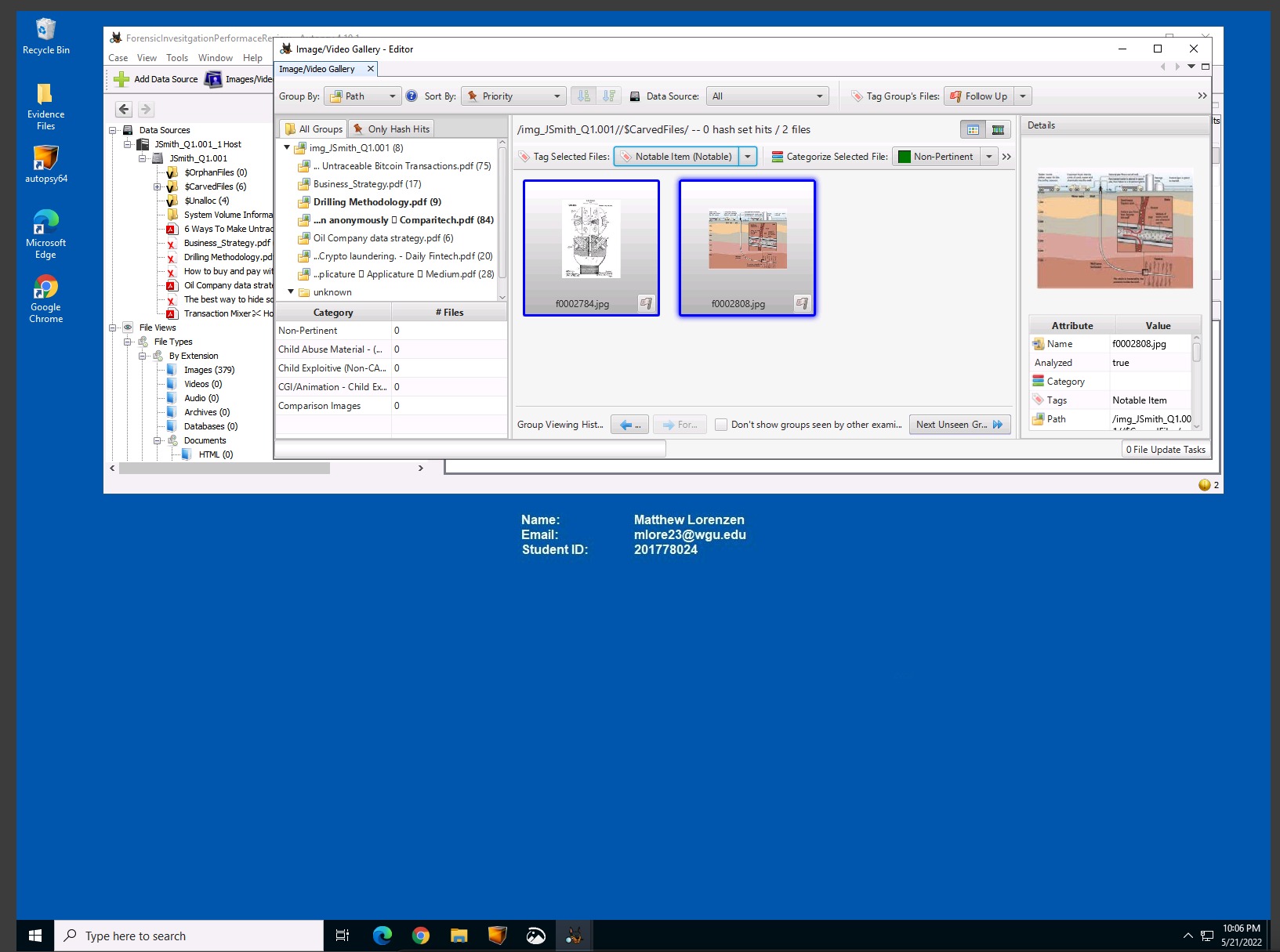
Extracting a total of 6 System files 

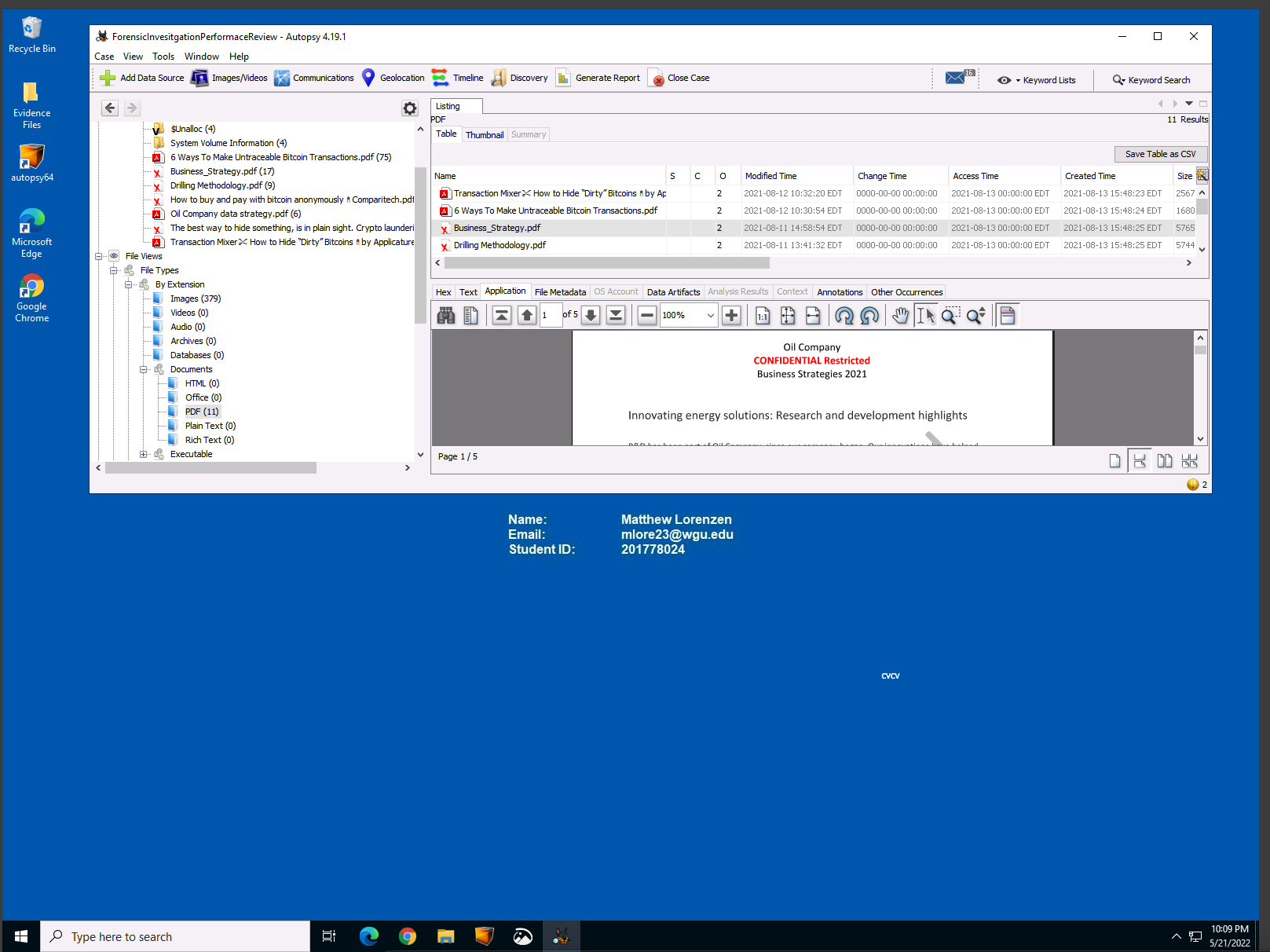
Extracting an additional 12 file of various types including pdf and jpg

Extracted files in Export

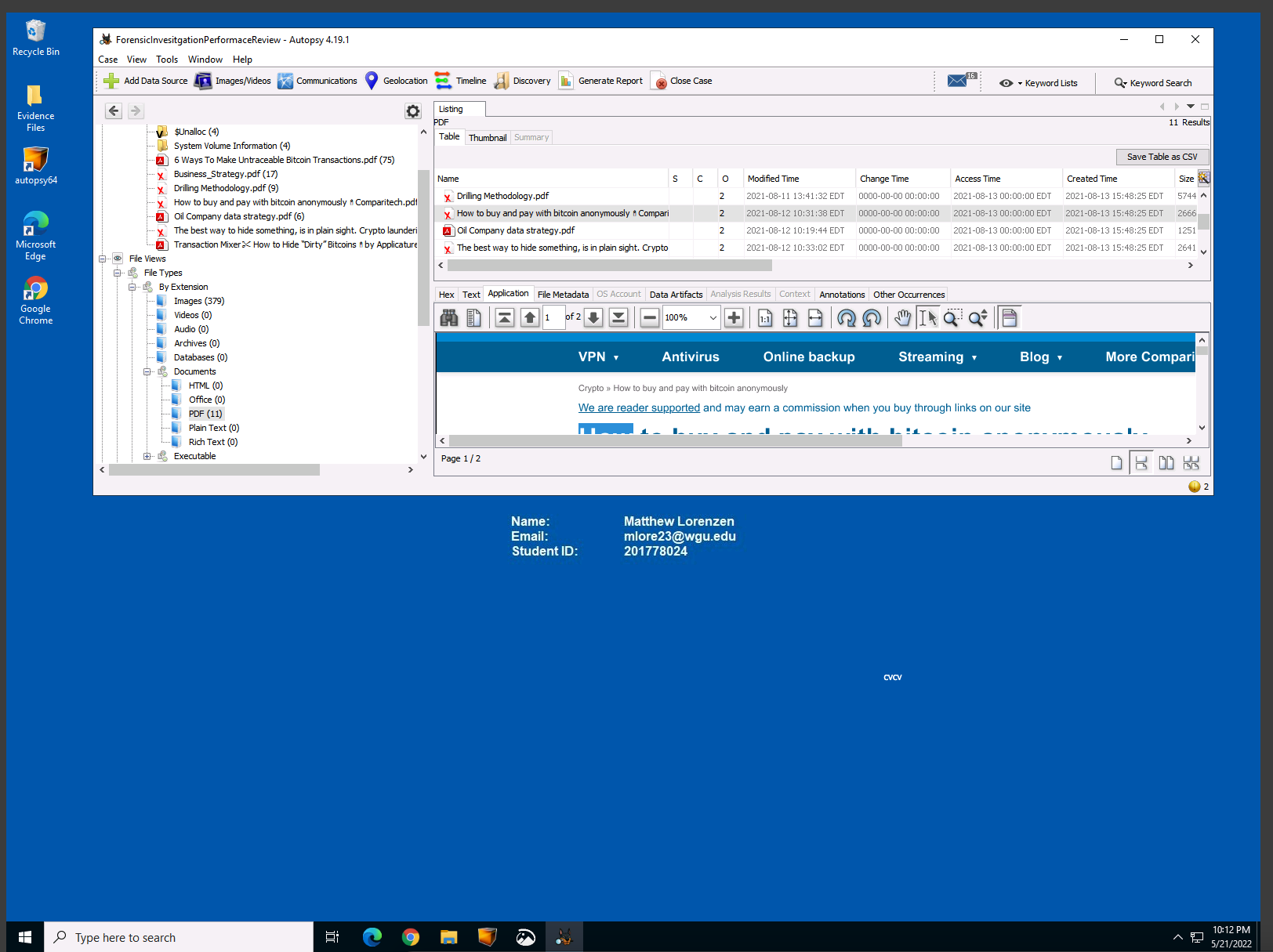


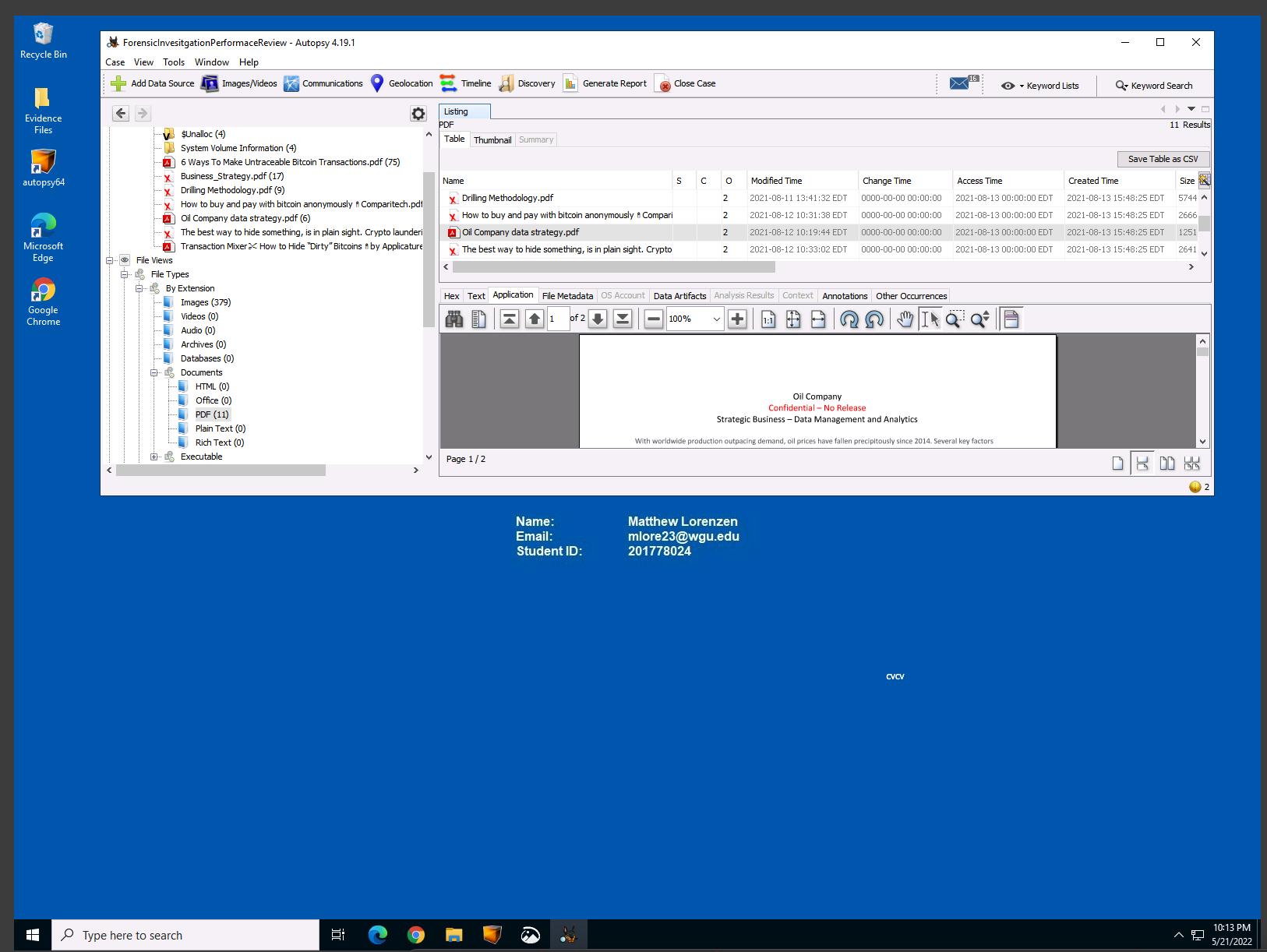
Extracting Images 

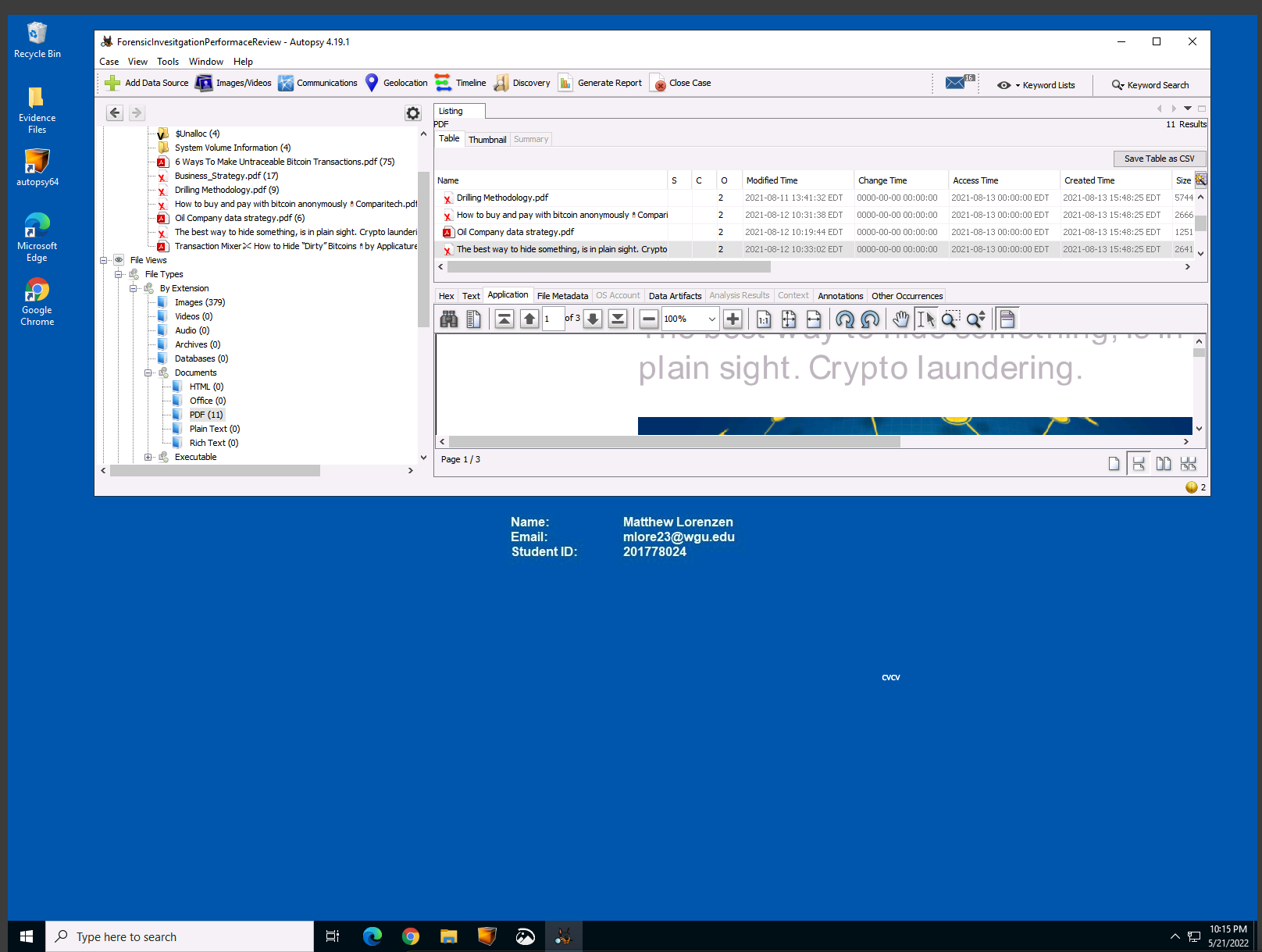
Additional Images discovered $CarvedFiles/

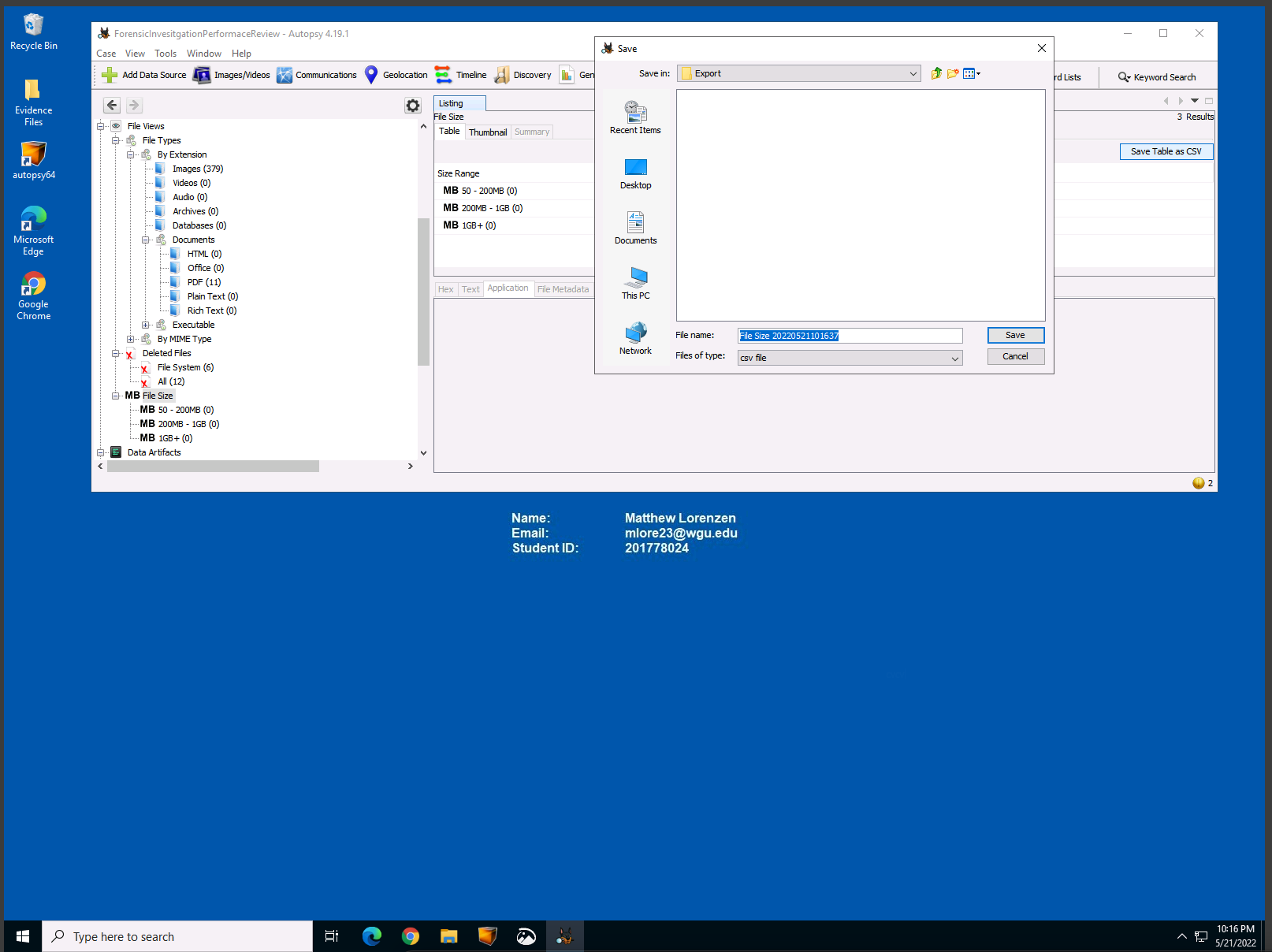
Discovery of “Confidential Restricted Documentation (Business\_Strategy.pdf)

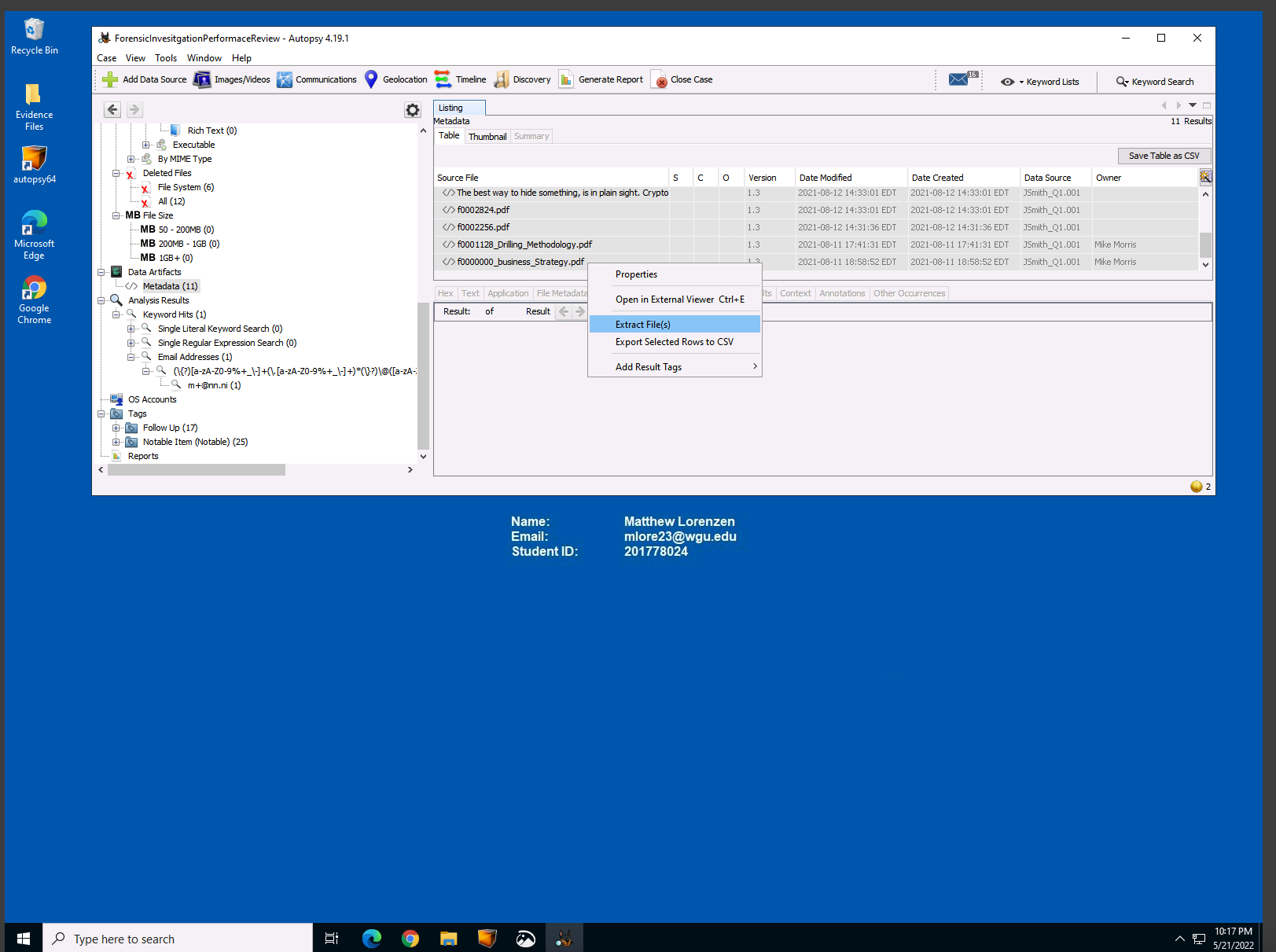
Discovery of Confidential Restricted (Drilling Methodolgy.pdf)

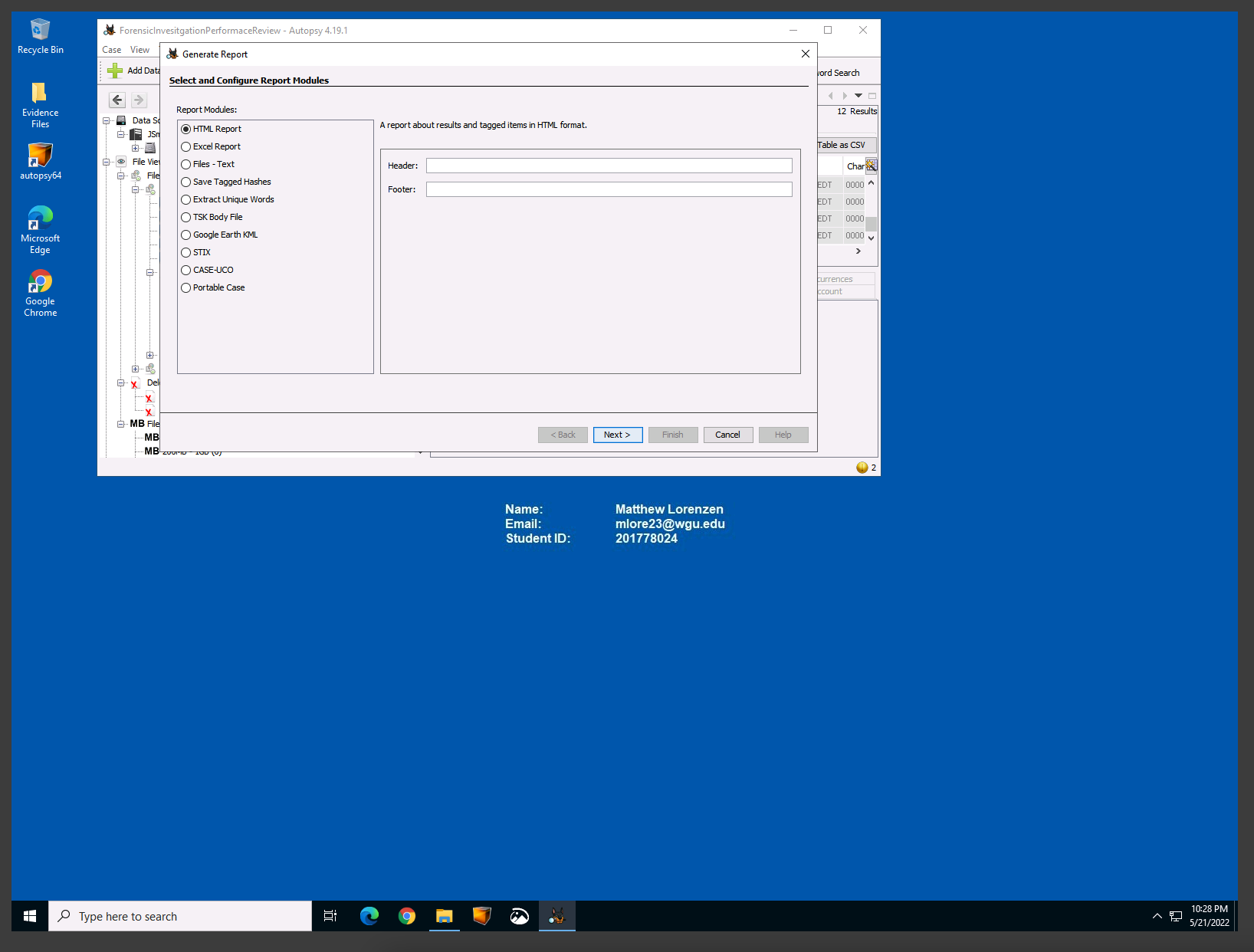
Discovery of documentation indicating John Smith has been extensively researching Cryptocurrency (How to buy and pay with bitcoin anonymously.pdf)

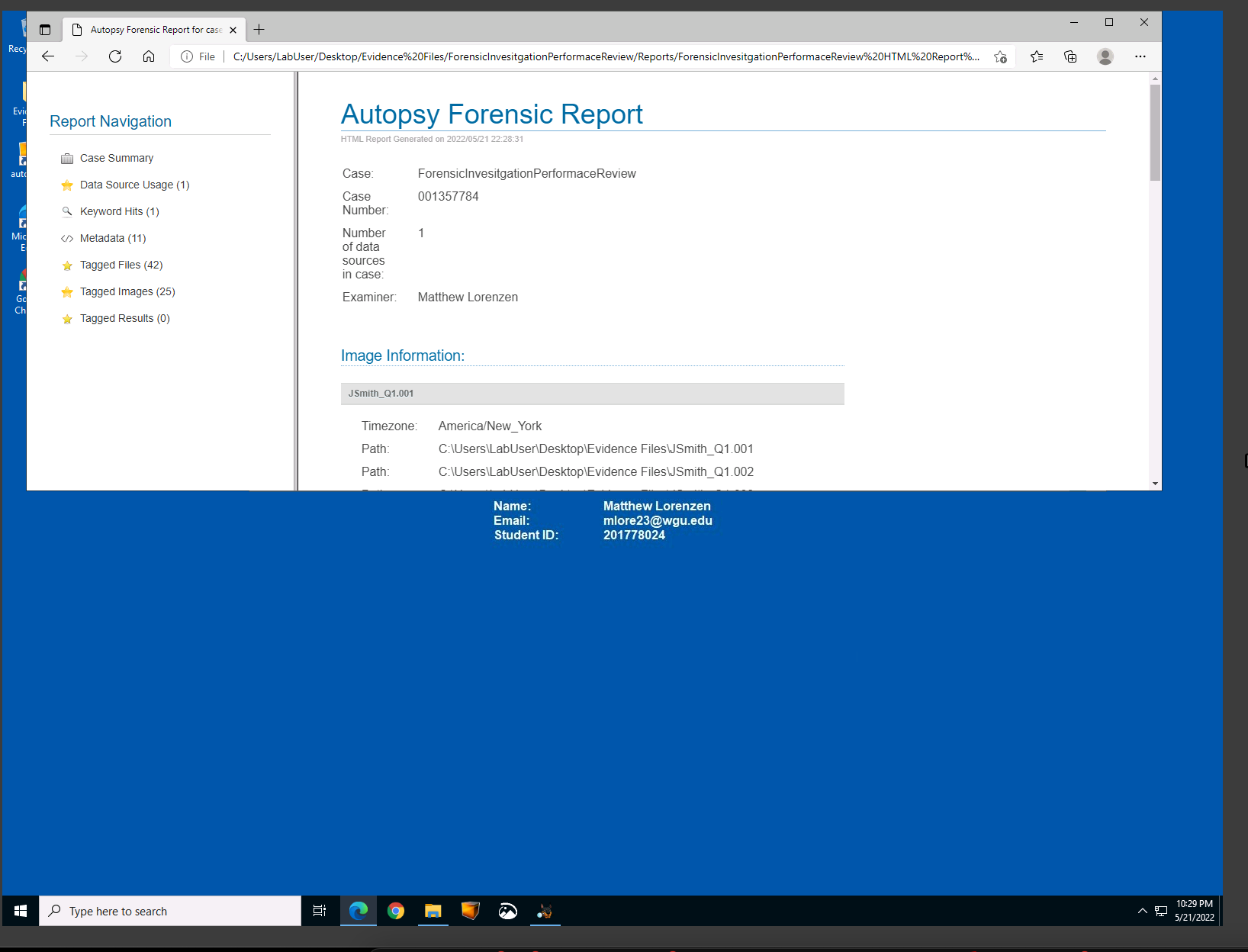
Discovery of Confidential Information (Oil Company Data Strategy.pdf)

Discovery of evidence supporting John Smith was researching Crypto Laundering (The Best way to hide something, is in plain sight. Crypto Laundering.pdf)

Screen shot of partitions

Extracting Data Artifacts (Metadata) 

Running Report

Snippit of Report  


3.  Summarize the findings you identified during your investigation and the conclusions you made regarding the suspect and the collected evidence. Provide screenshots from Autopsy or reports in support of your findings and conclusions. In each screenshot, include the Name, Email, and Student ID located on the desktop of the virtual environment.

**Summary of Evidence:**

Upon review of the forensic images discovered during the investigation there is high-probability that John Smith was involved in exfiltrating “confidential documentation” pertinent to an Oil Drilling process. This is apparent through the findings of confidential documents as seen above. These documents not only appear to have been deleted by John Smith, but supporting documentations indicate John Smith was looking to gain profit through his actions. This is supported by the evidence found indicating research being performed in Bitcoin payments and Cryptocurrency laundering.