Timothy Terrance

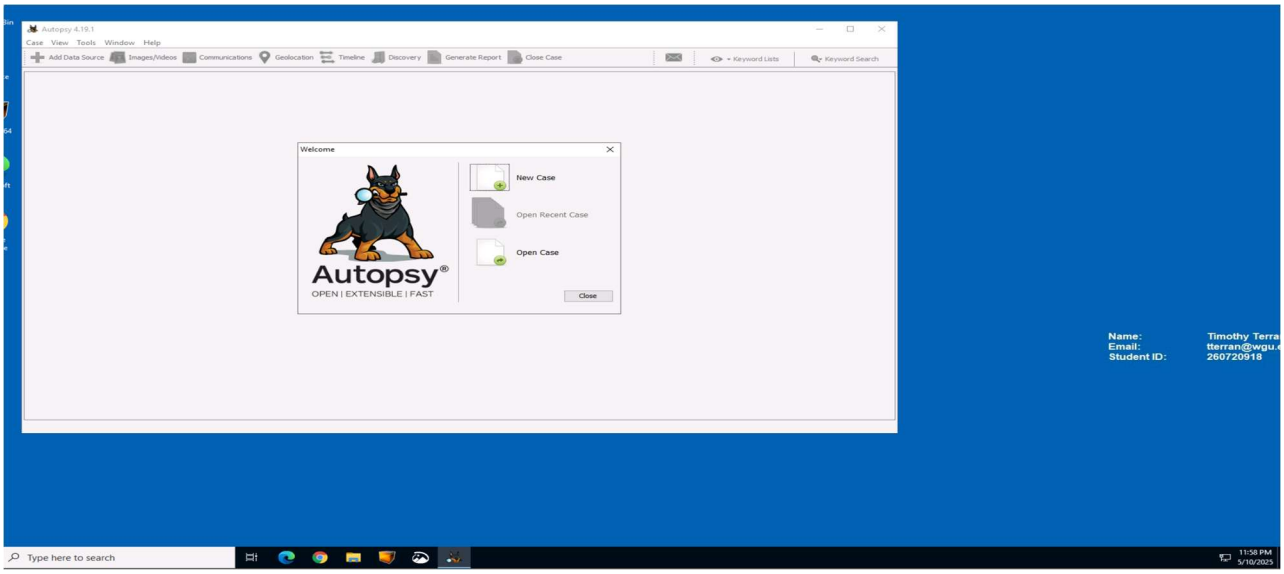
Cybersecurity and Information Assurance

Digital Forensics in Cybersecurity - D431

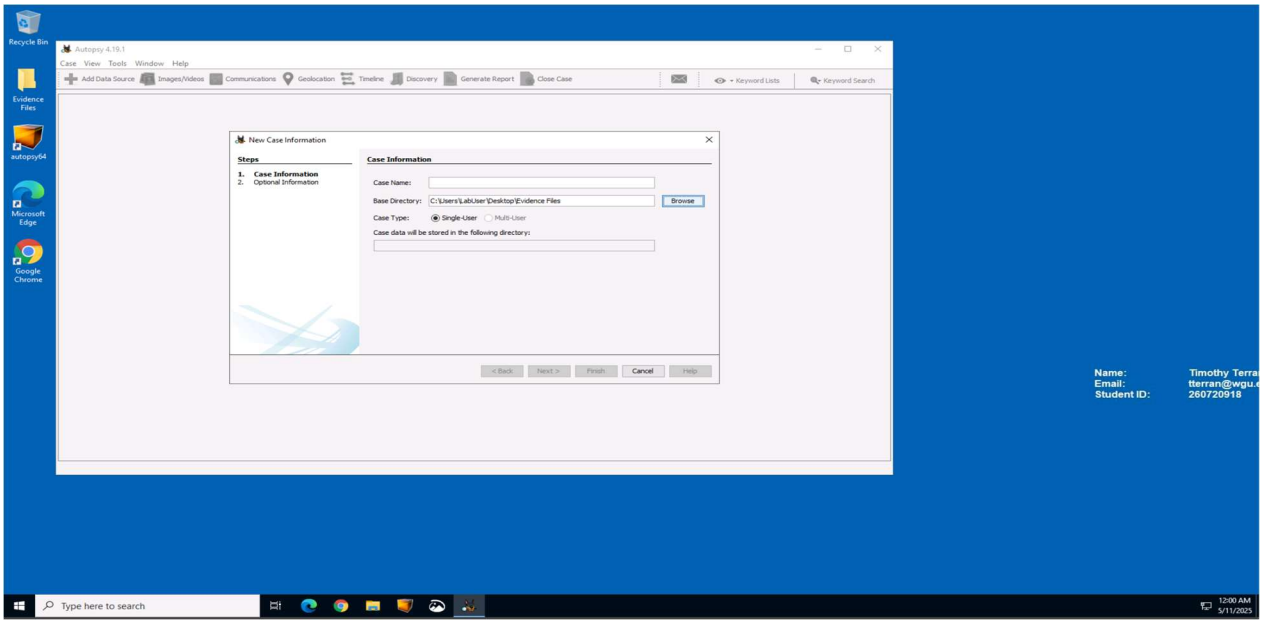
Task 2

A1 – Steps Used To Create Forensic Case File

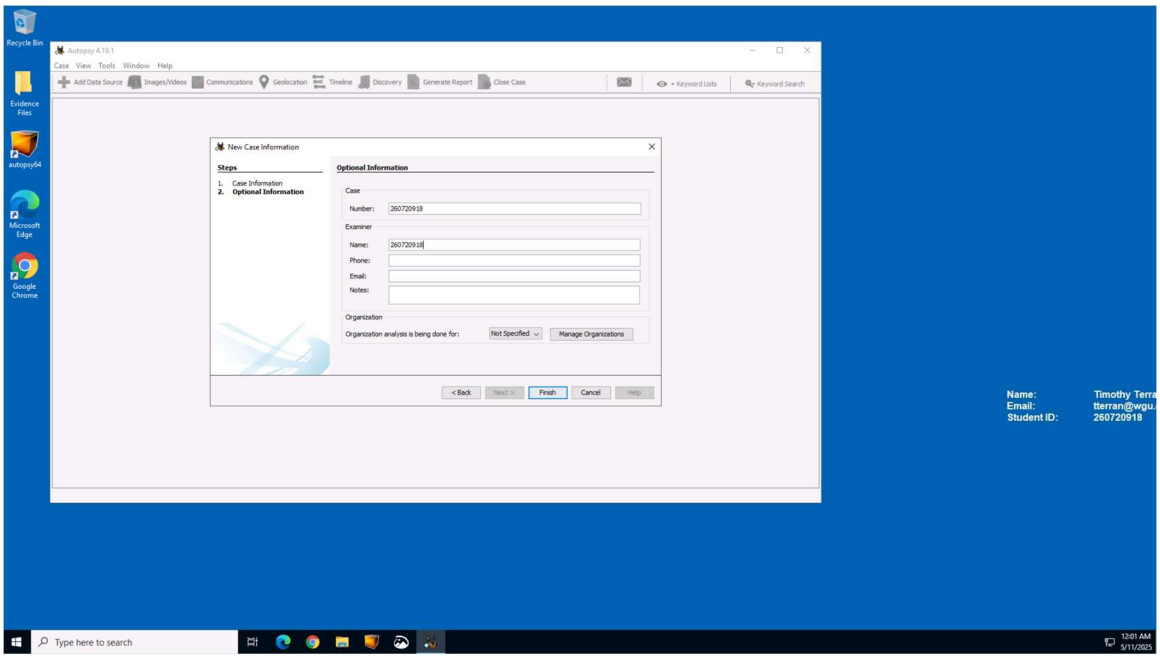
1.) First, we **open the Autopsy software** to analyze evidence.



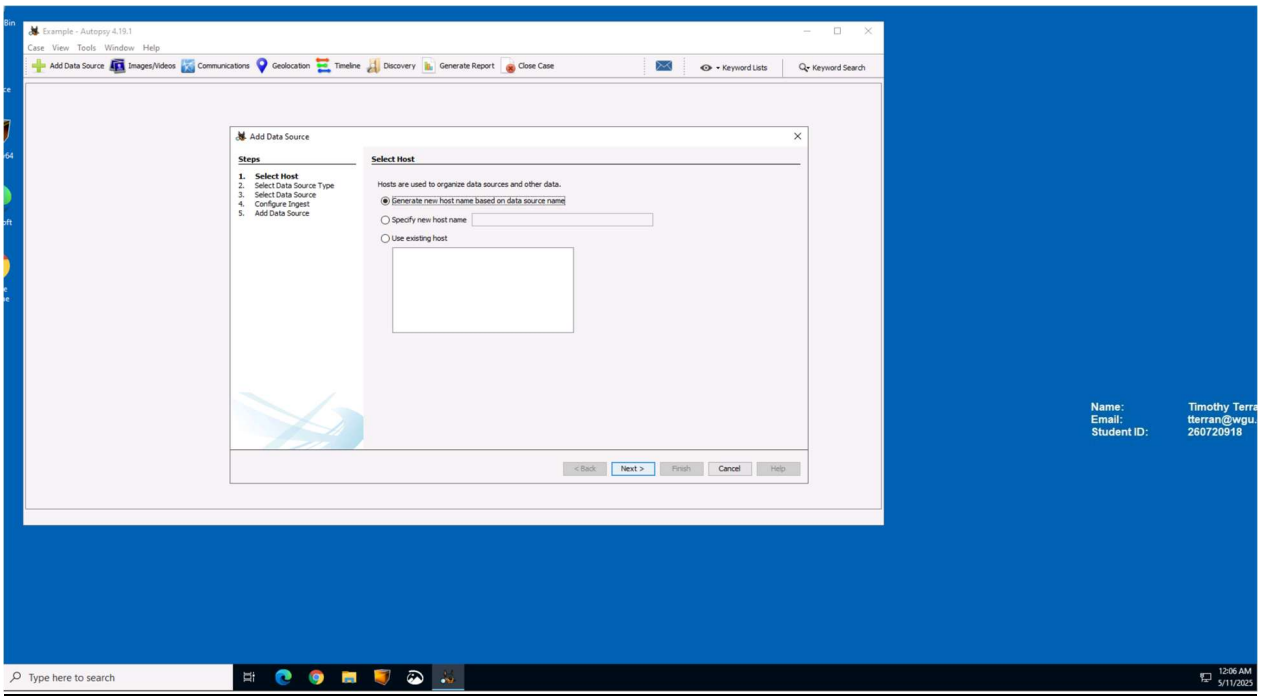
2.) In this instance we are looking to **analyze the Evidence Files folder**.



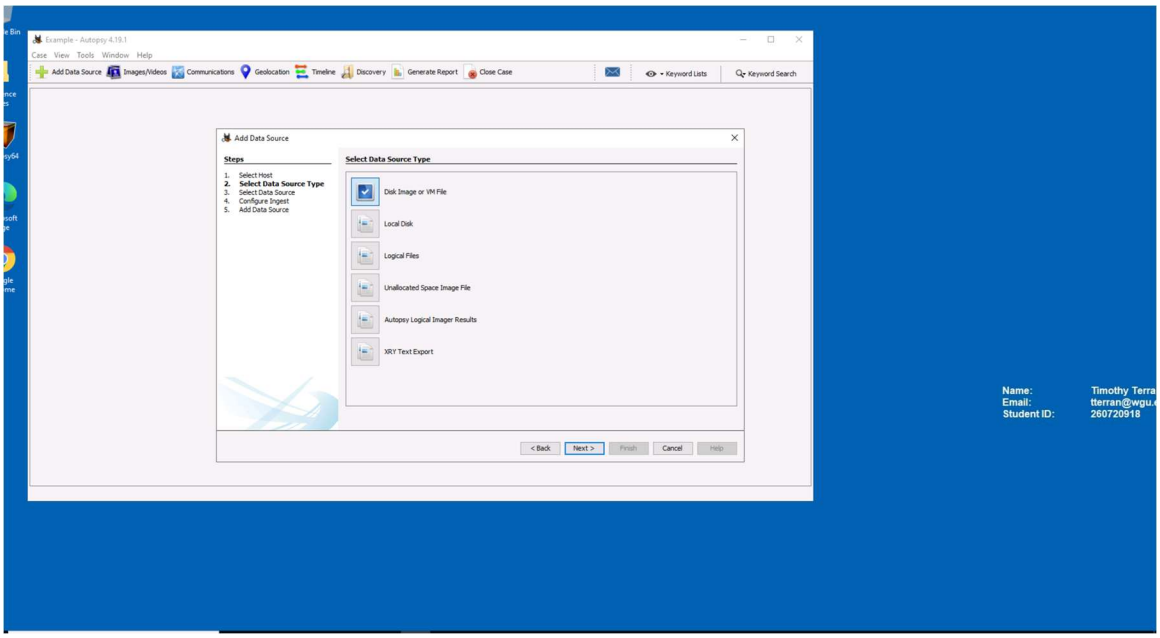
3.) I used the number **260720918 as a new case numb**er for tracking purposes.



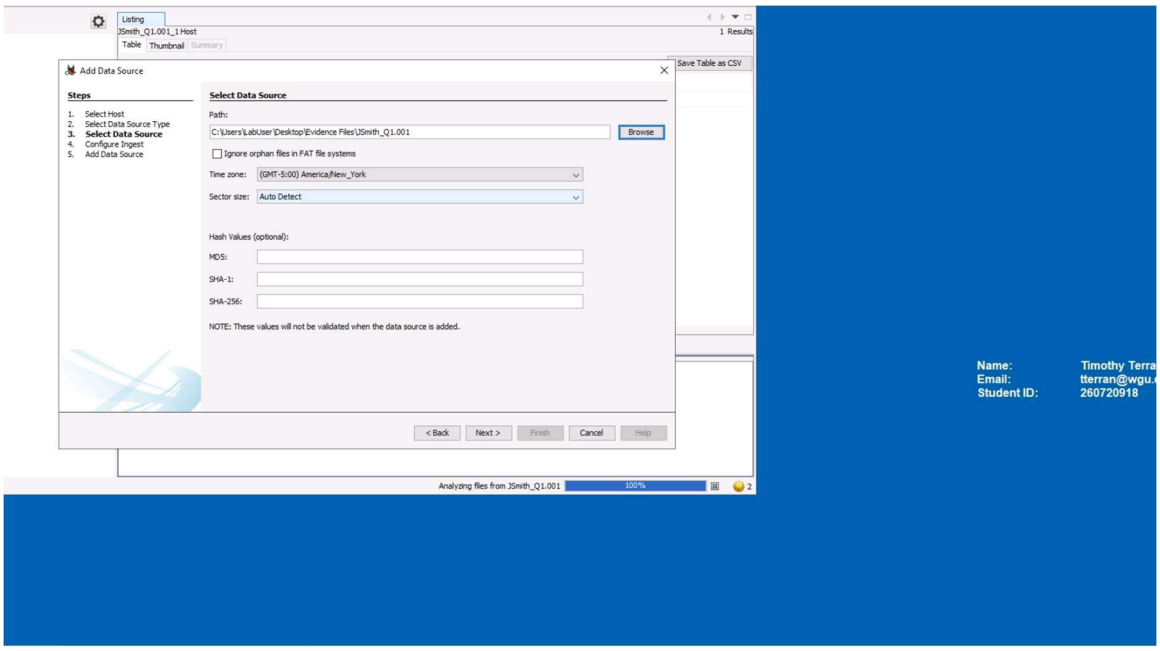
4.) Here, I chose to **Generate a new host based on data source name**.



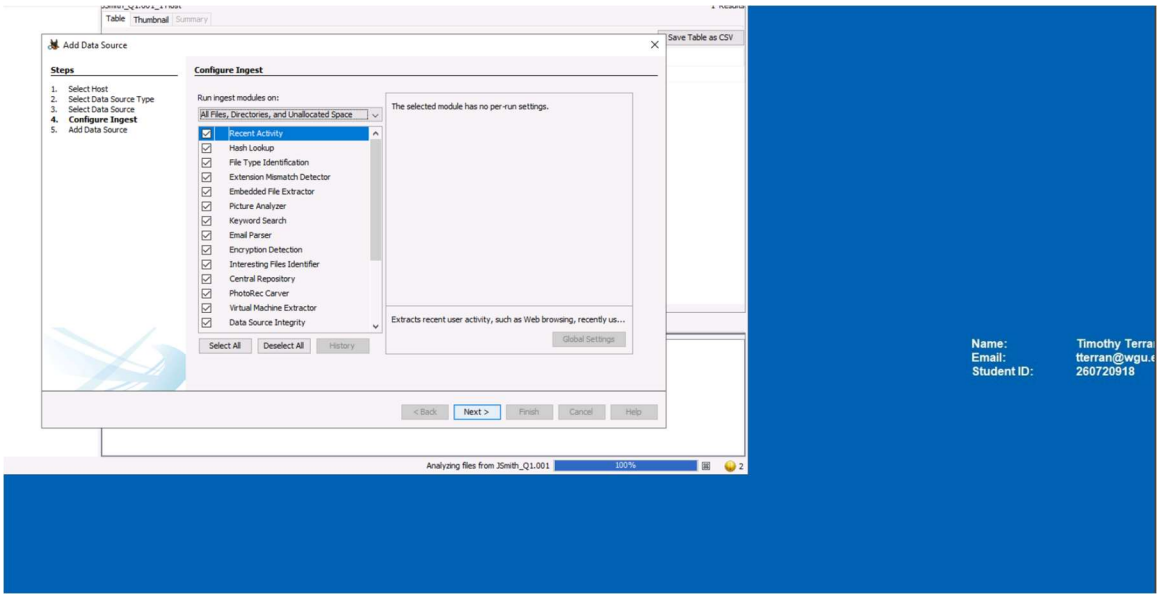
5.) Then, I selected **Disk image or VM file**.



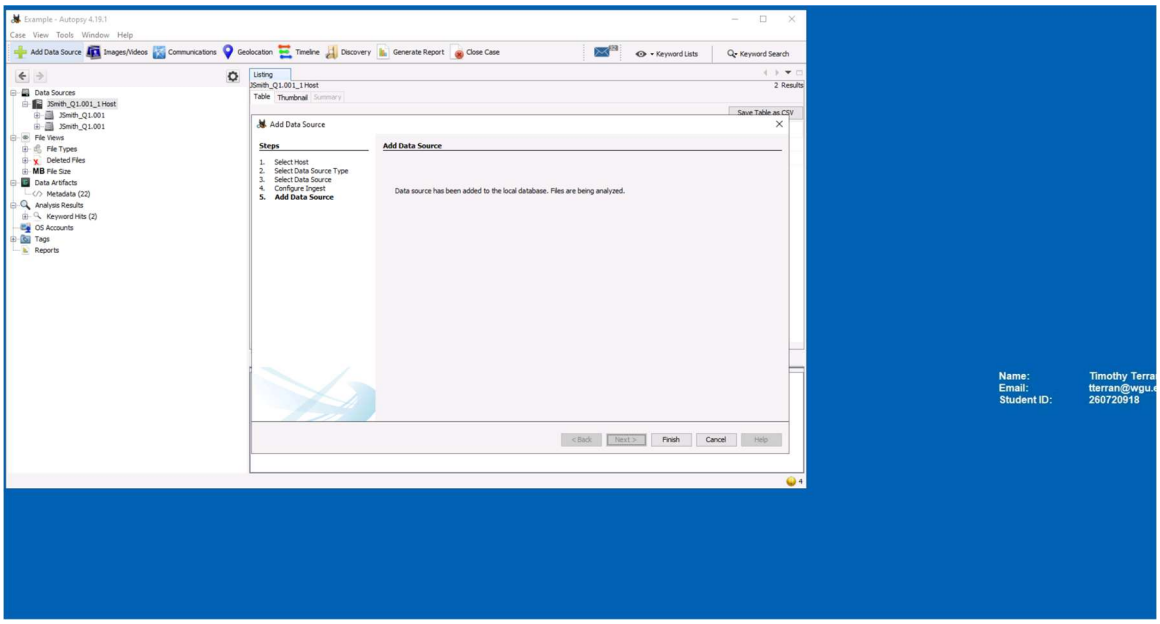
6.) I **selected JSmith_Q1.001 located in the Evidence Files** folder as the data source.



7.) Accept configure ingest defaults and click next.



8.) Once data source is added to the database, click finish.

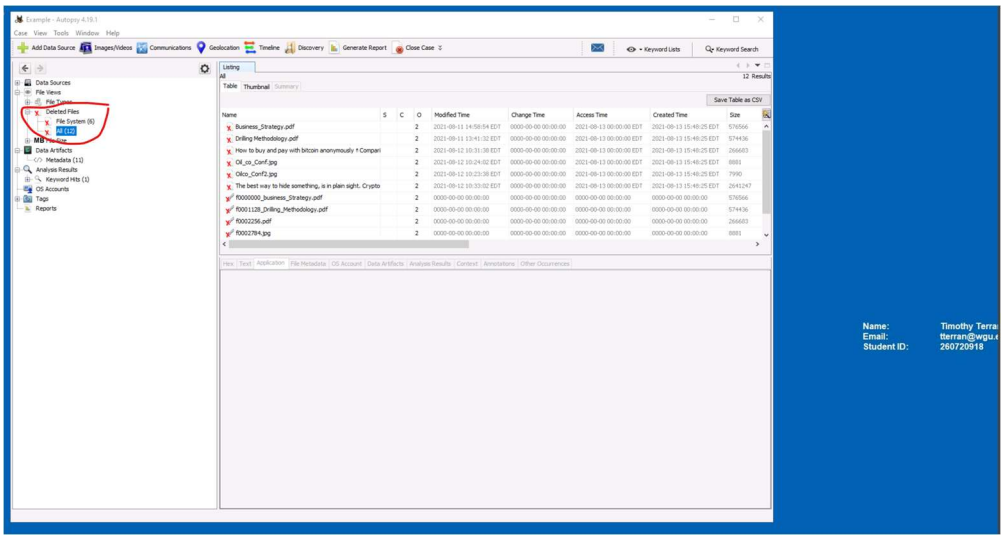


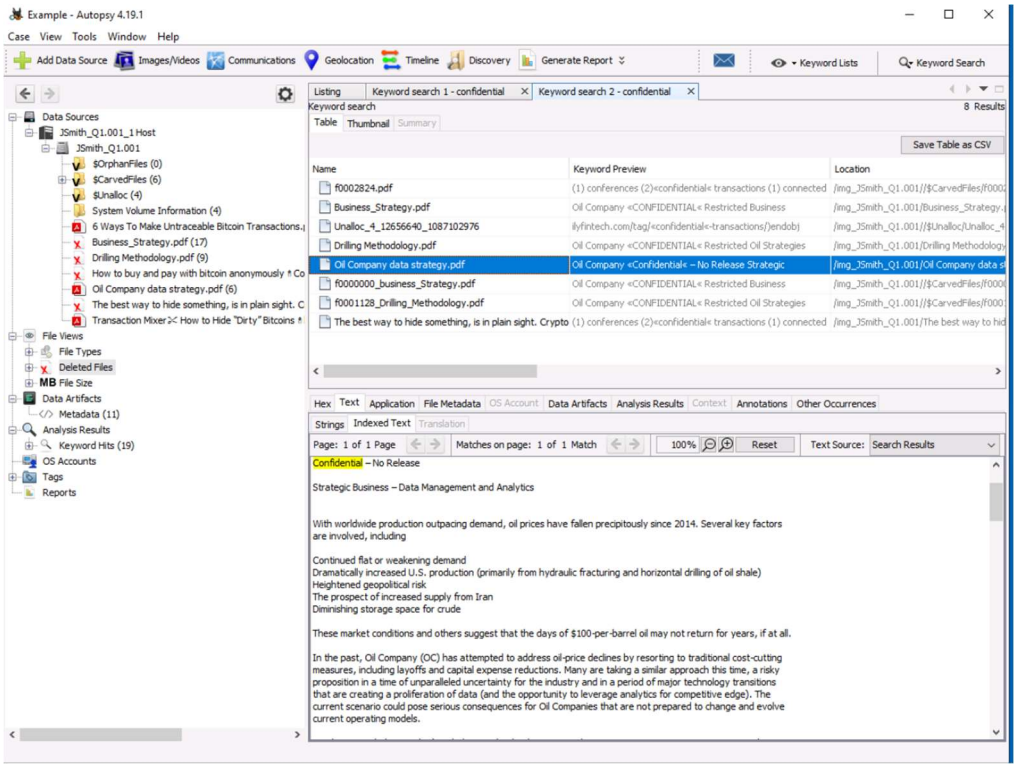
Timothy Terrance

Cybersecurity and Information Assurance

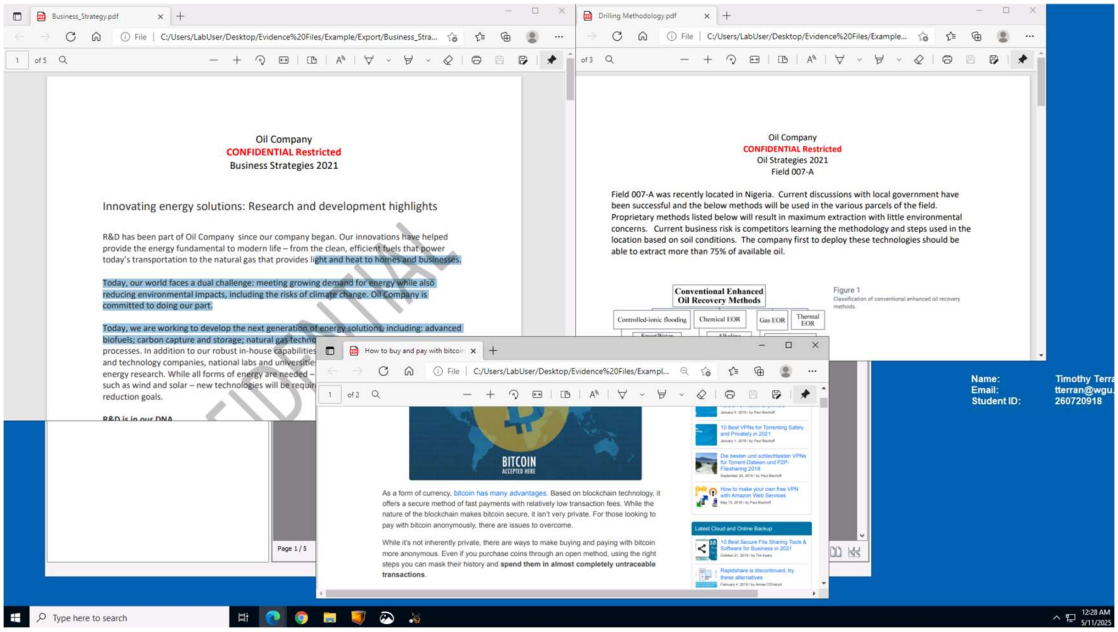
A2 – Analysis & Steps Used To Identify Potential Evidence

1.) After adding the JSmith image to the Autopsy tool, I located the deleted files collapsible tree and expanded it to reveal all files in the subdirectory below. This provided a structured breakdown of recoverable content deleted from the suspect's system. The deleted files that stood out were the ones containing keywords like "confidential," "accounts," and "strategy." These files were identified as business-relevant, possibly proprietary information, and had been recently deleted, suggesting an effort to conceal them before forensic acquisition.

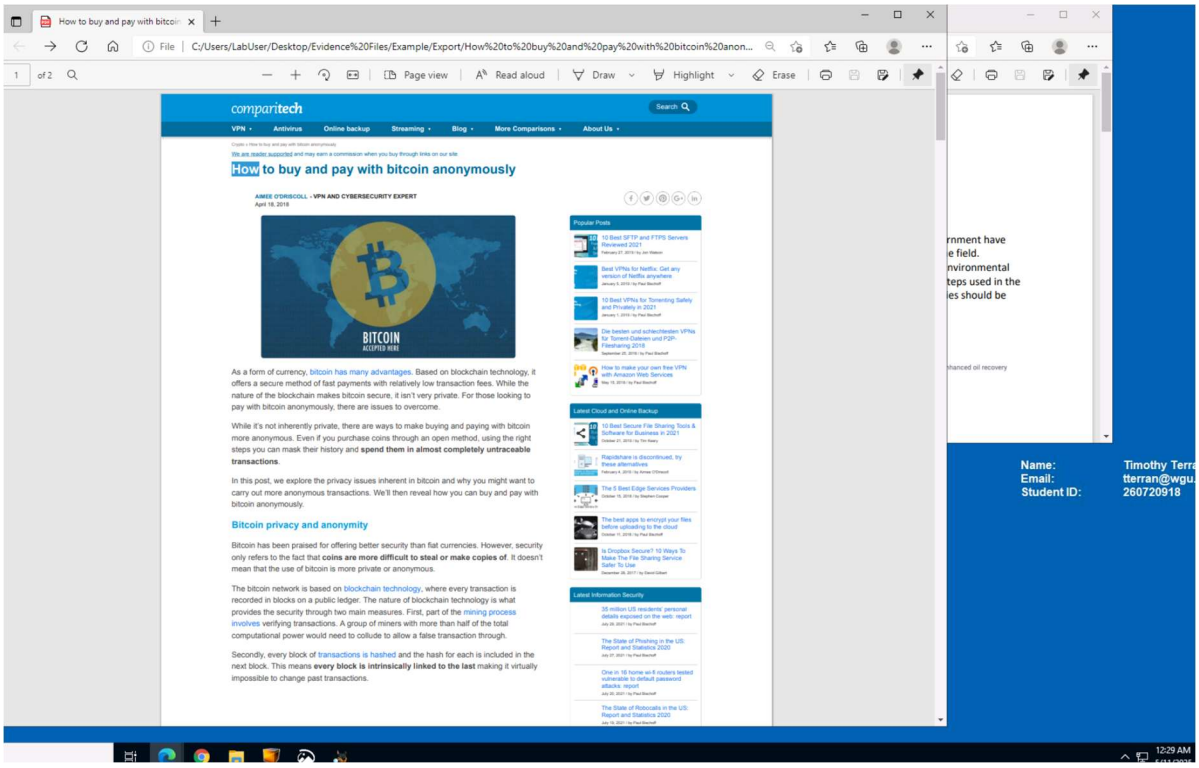




2.) Then, I opened the files in question to perform due diligence checks. This revealed several files that contained confidential, restricted business information.



3.) A document detailing ways to pay anonymously with Bitcoin to avoid having transactions traced back to the source was even found.



Timothy Terrance

Cybersecurity and Information Assurance

A3 – Summary Of Findings And Conclusions

During the analysis of the disk image JSmith_Q1.001, several key pieces of evidence were discovered using Autopsy. After loading the image and running the default ingest modules (including File Type Identification, Recent Activity, and Hash Lookup), deleted and suspicious files were identified within user-accessible directories. The evidence gathered through Autopsy strongly indicates that the user of the imaged system attempted to conceal and possibly exfiltrate sensitive company information. Deleting confidential files, paired with documentation about anonymous transactions and traces of internet research into illicit activities, supports a conclusion that the suspect violated company data policies and may have been preparing to leak proprietary information. Based on this evidence, further internal review and possibly legal action may be warranted.