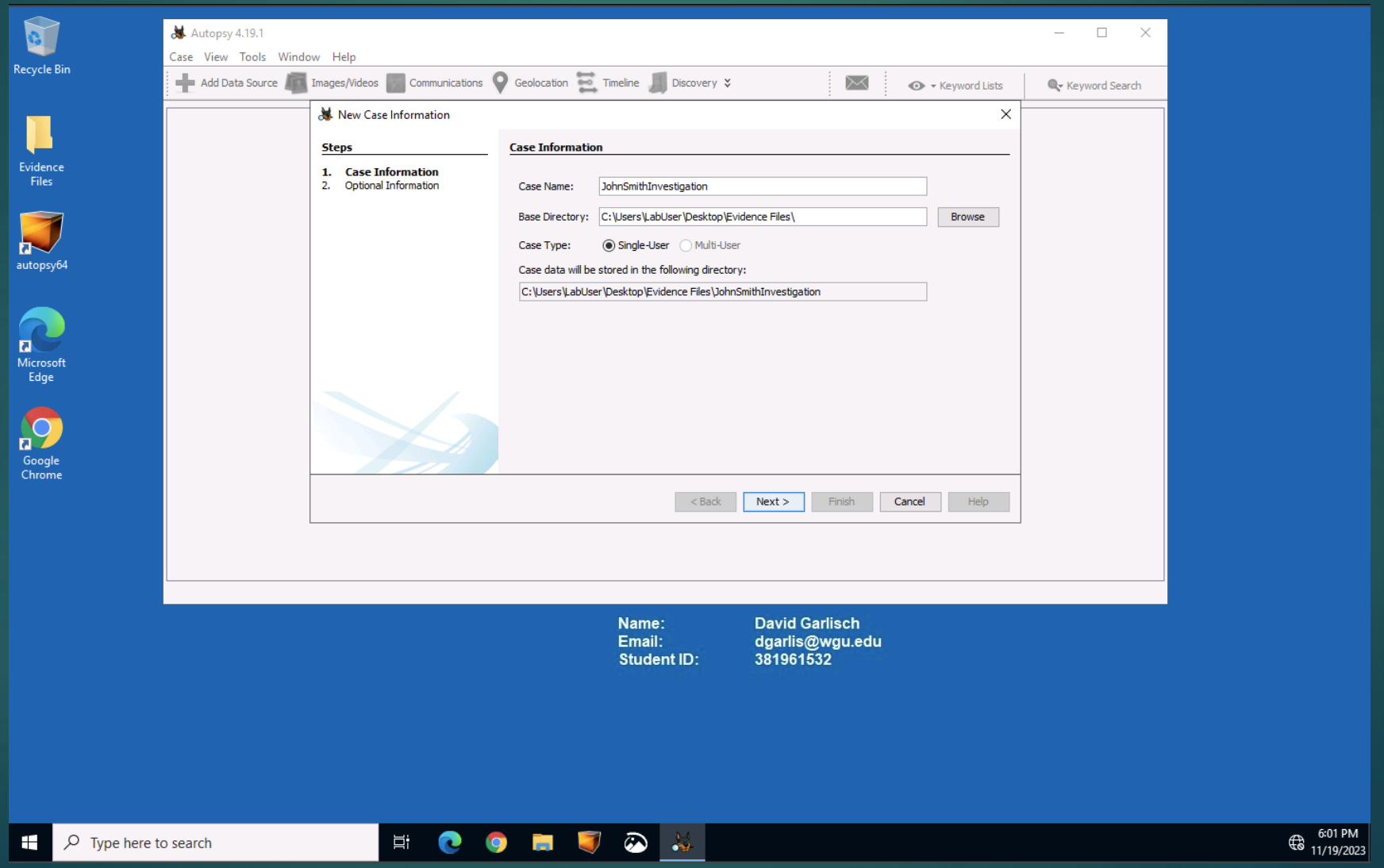
David Garlisch

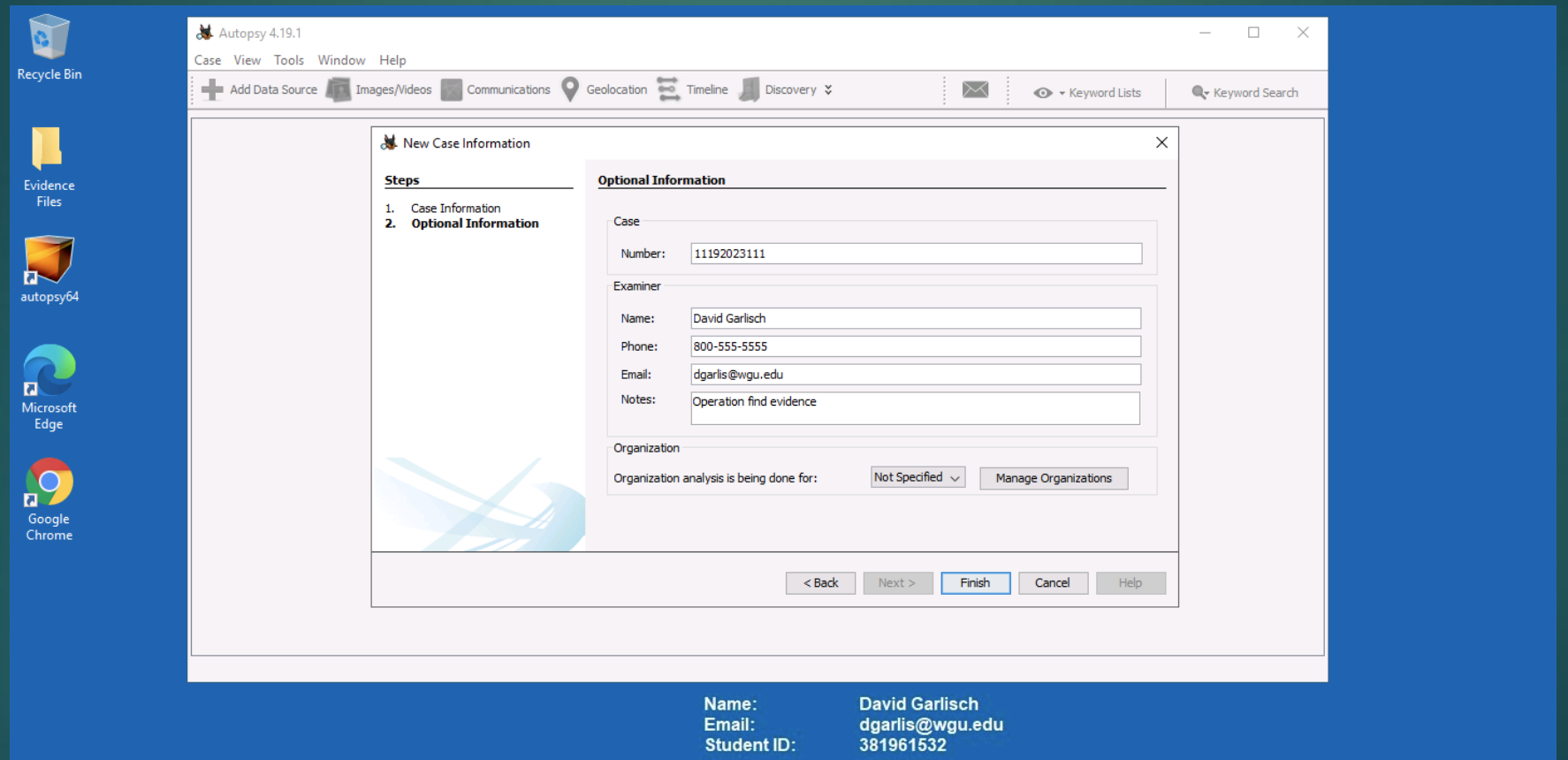
D431

TASK 2

1.) I started my investigation by loading Autopsy and entering in the Case Name and selecting the Evidence Files that was on the desktop for my Base Directory.

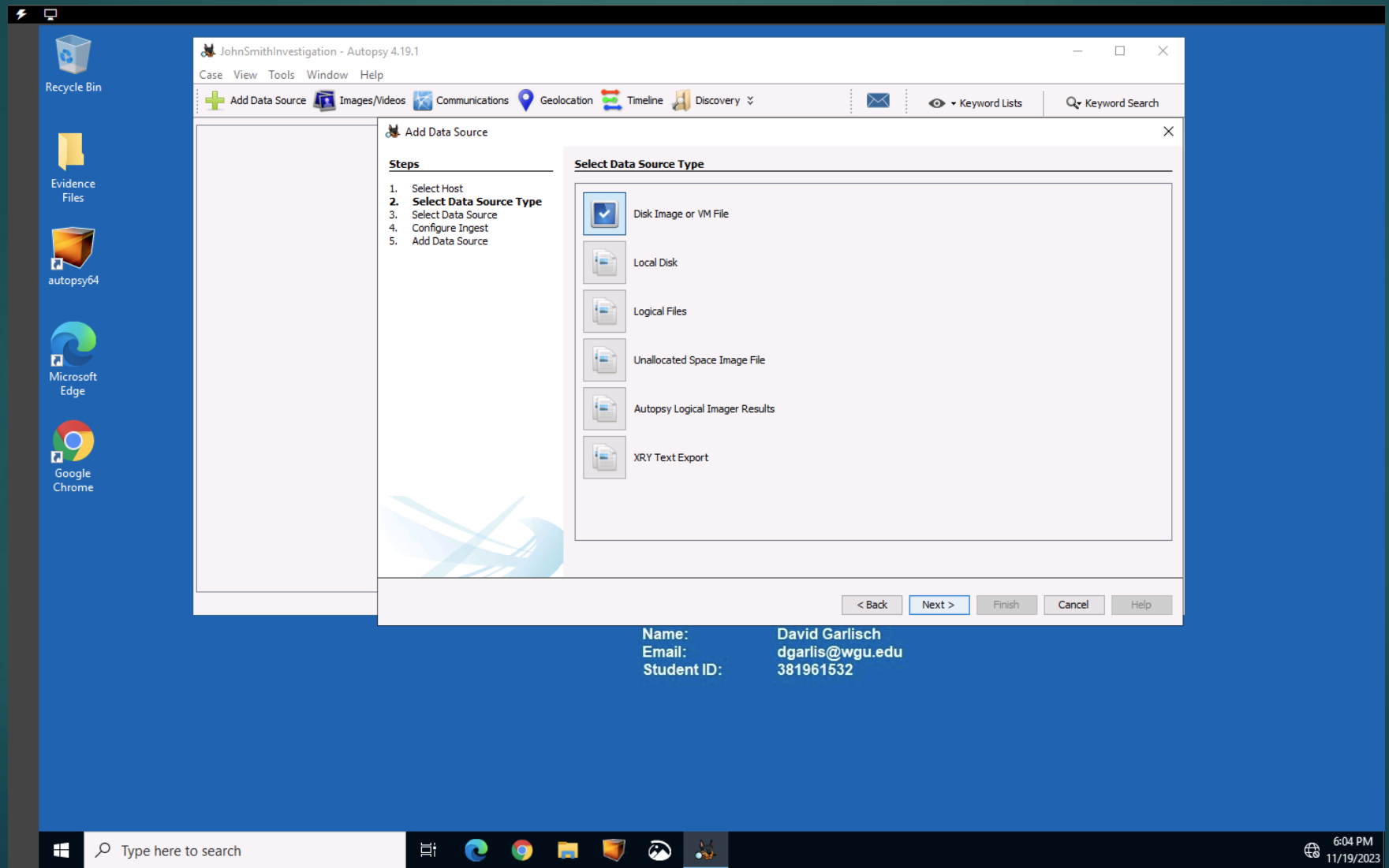


1.) I created a case number and entered in my information so it can be linked back to the one who did this investigation.

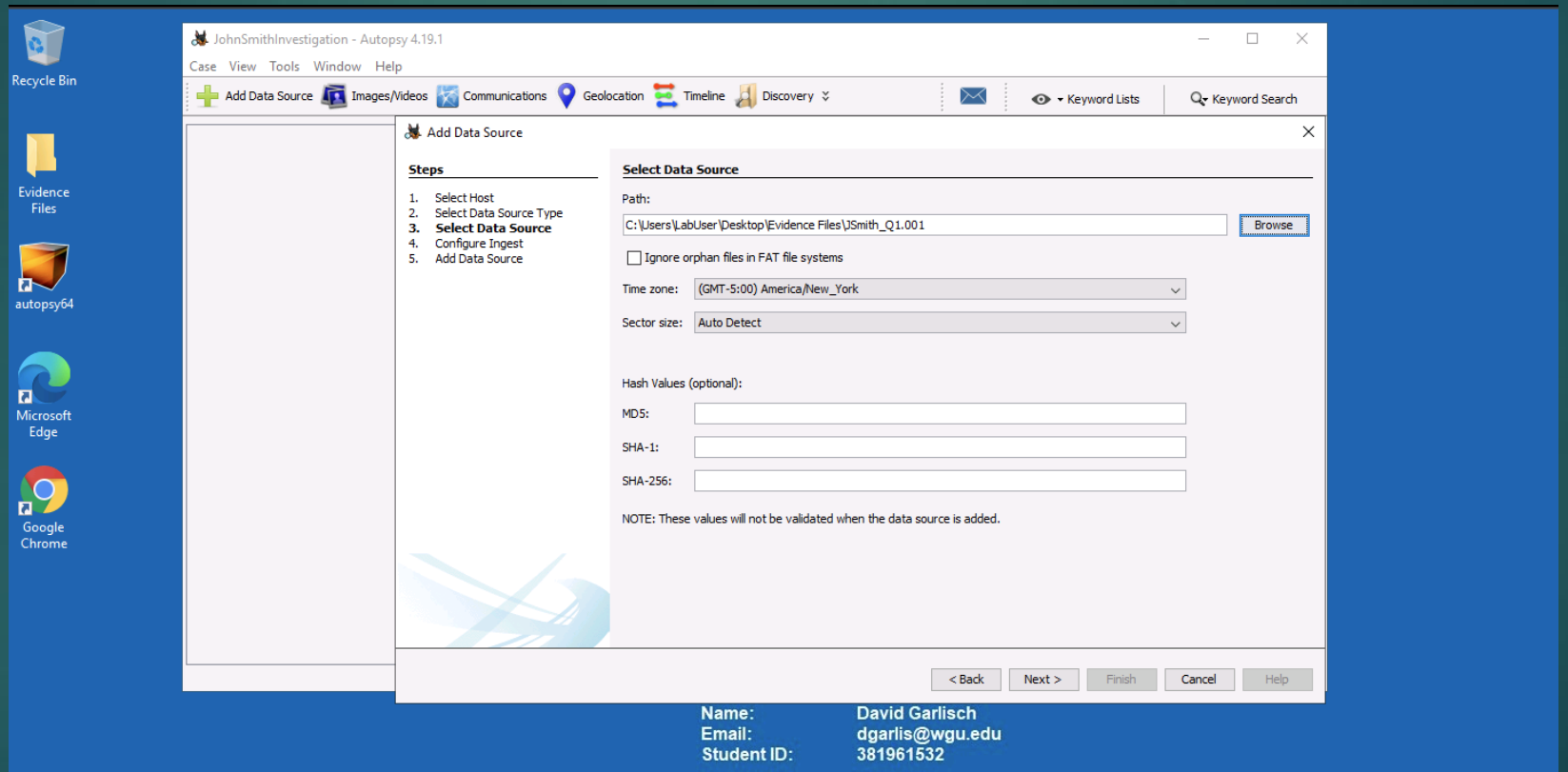


Name: David Garlisch
Email: dgarlis@wgu.edu
Student ID: 381961532

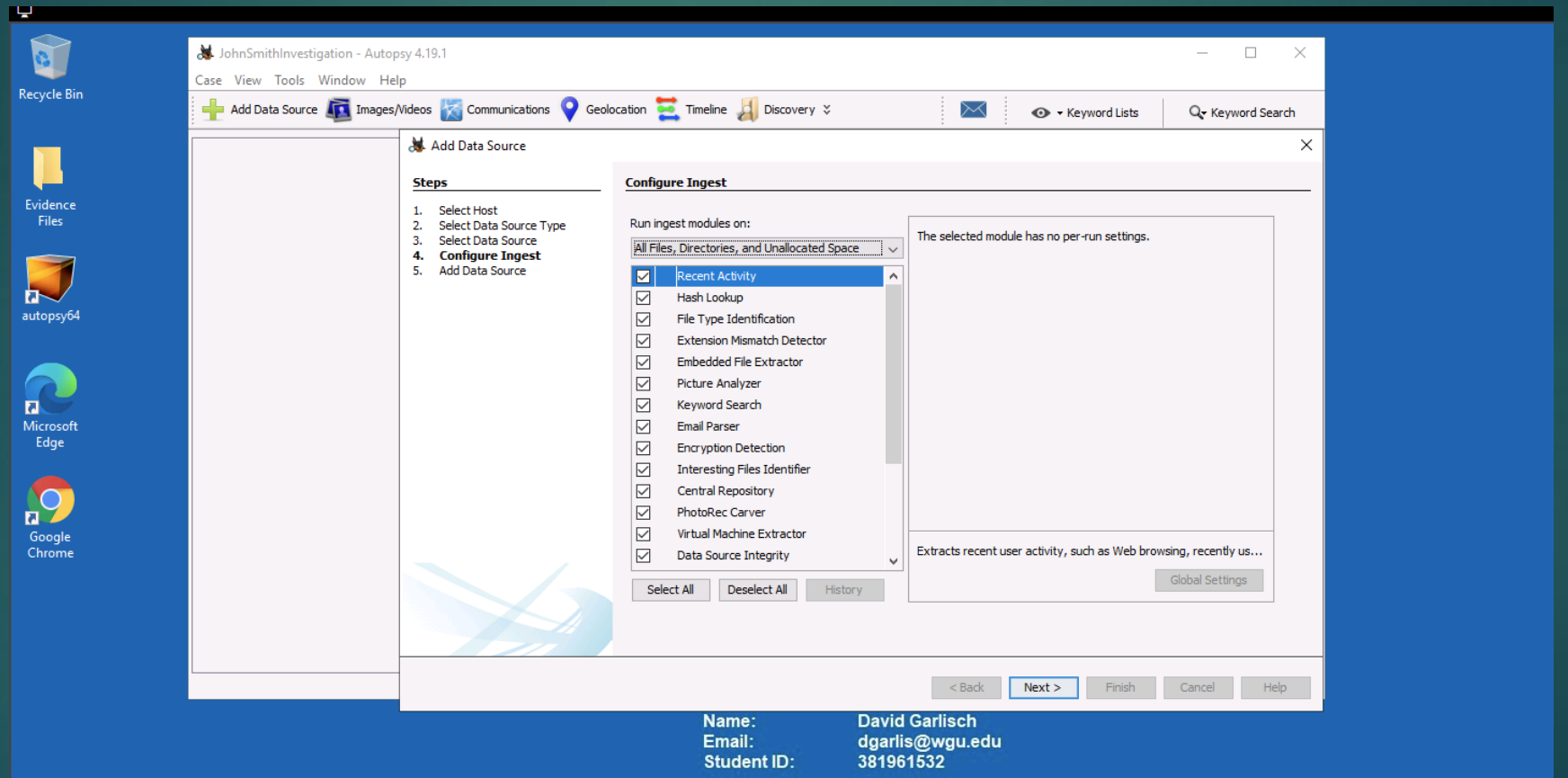
1.) I chose Disk Image or VM File as the Data Source Type



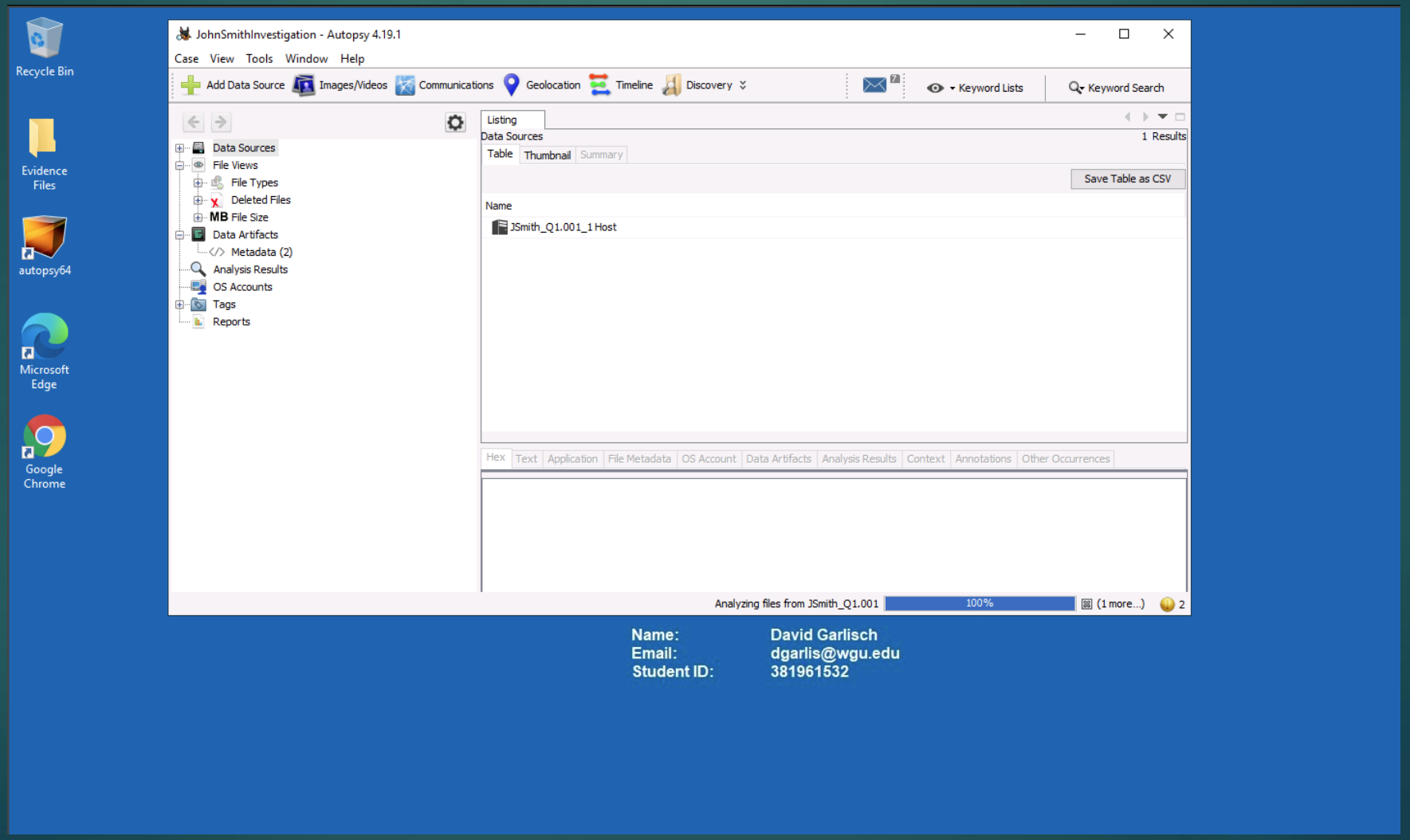
1.) I navigated to the file Jsmith_Q1.001 in Evidence Files which was on the desktop for the Path.



1.) I left these settings as default as mostly everything was checked already which concluded me creating the case.

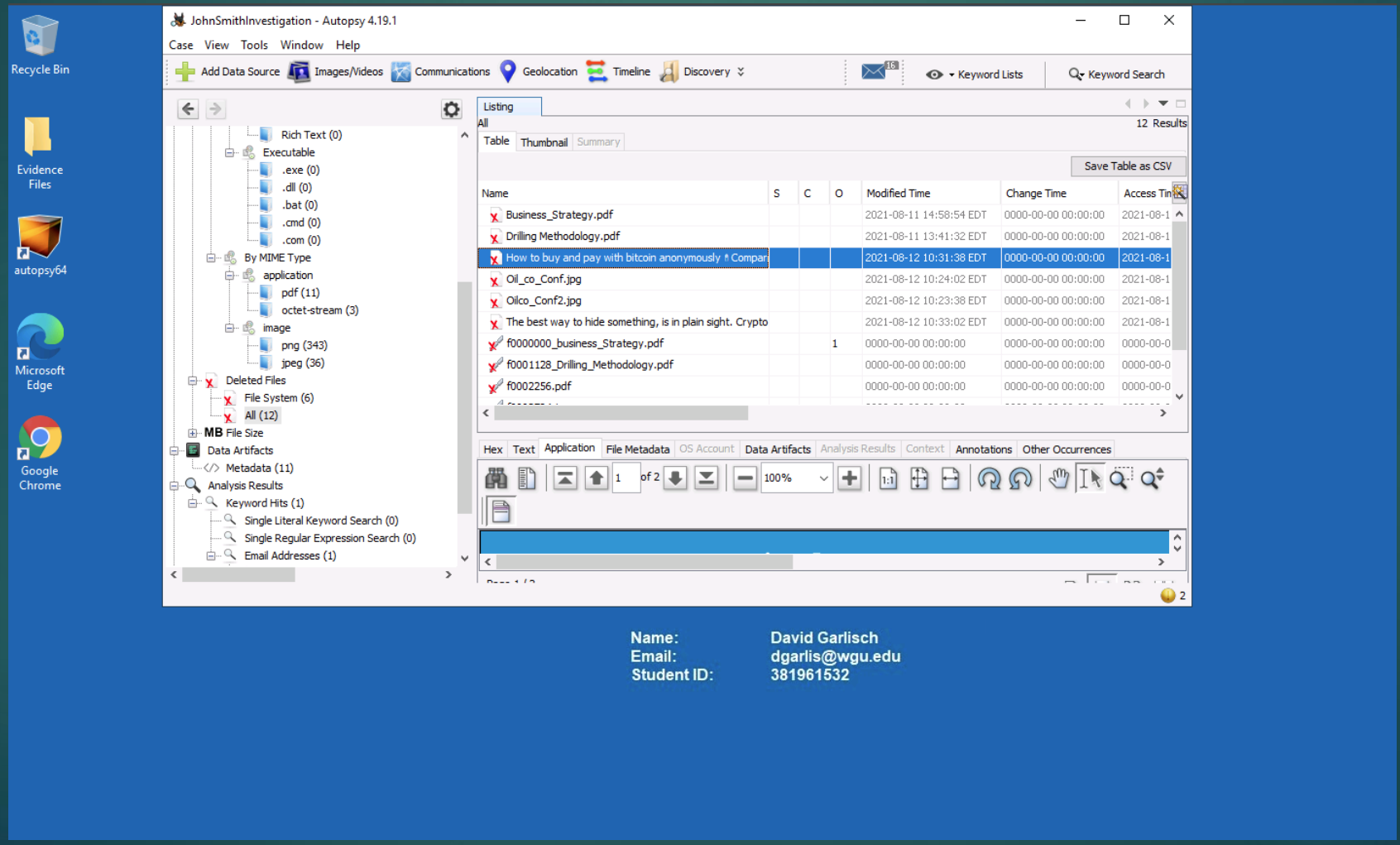


2.) I began my investigation at this point



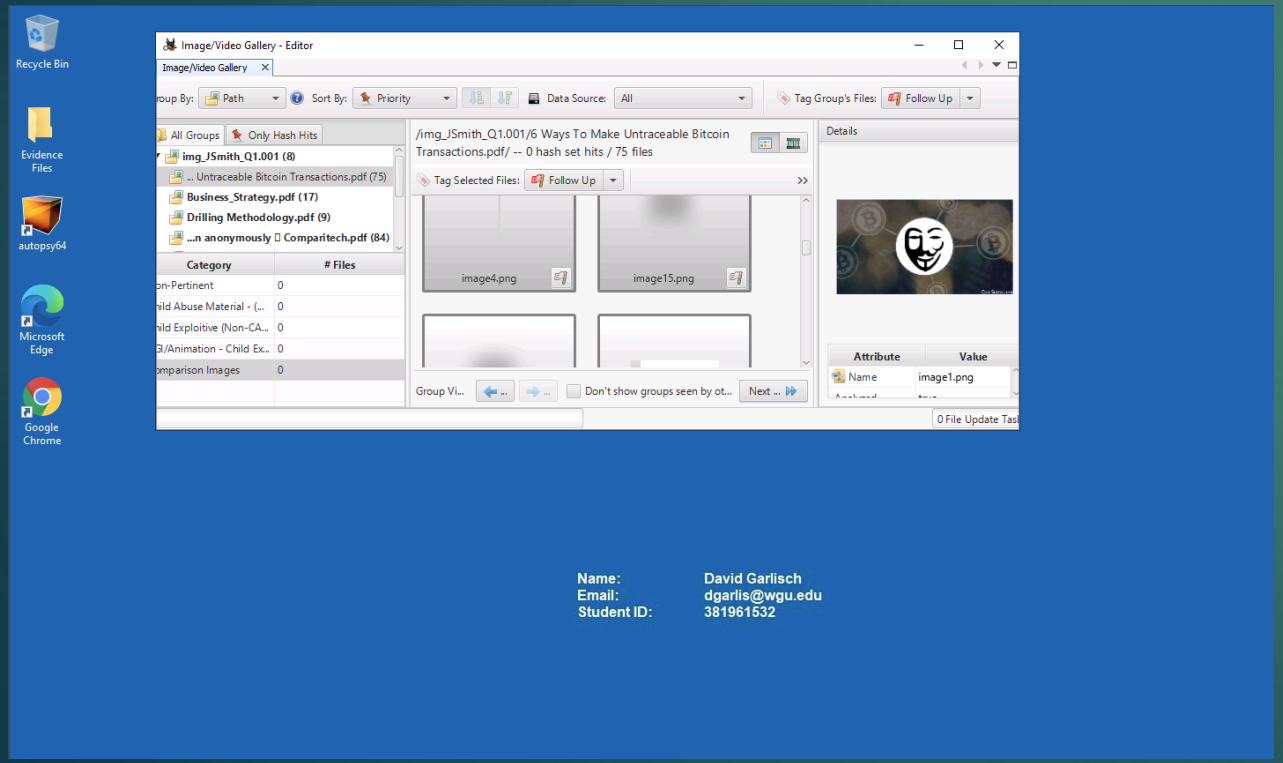
Name: David Garlisch
Email: dgarlis@wgu.edu
Student ID: 381961532

2.) I immediately was drawn to the X's saying deleted files and saw some suspicious activity there involving crypto and bitcoin. A couple files were titled as "How to buy and pay with bitcoin anonymously" and "The best way to hide something, is in plain sight". I extracted anything regarding crypto in the deleted files section.

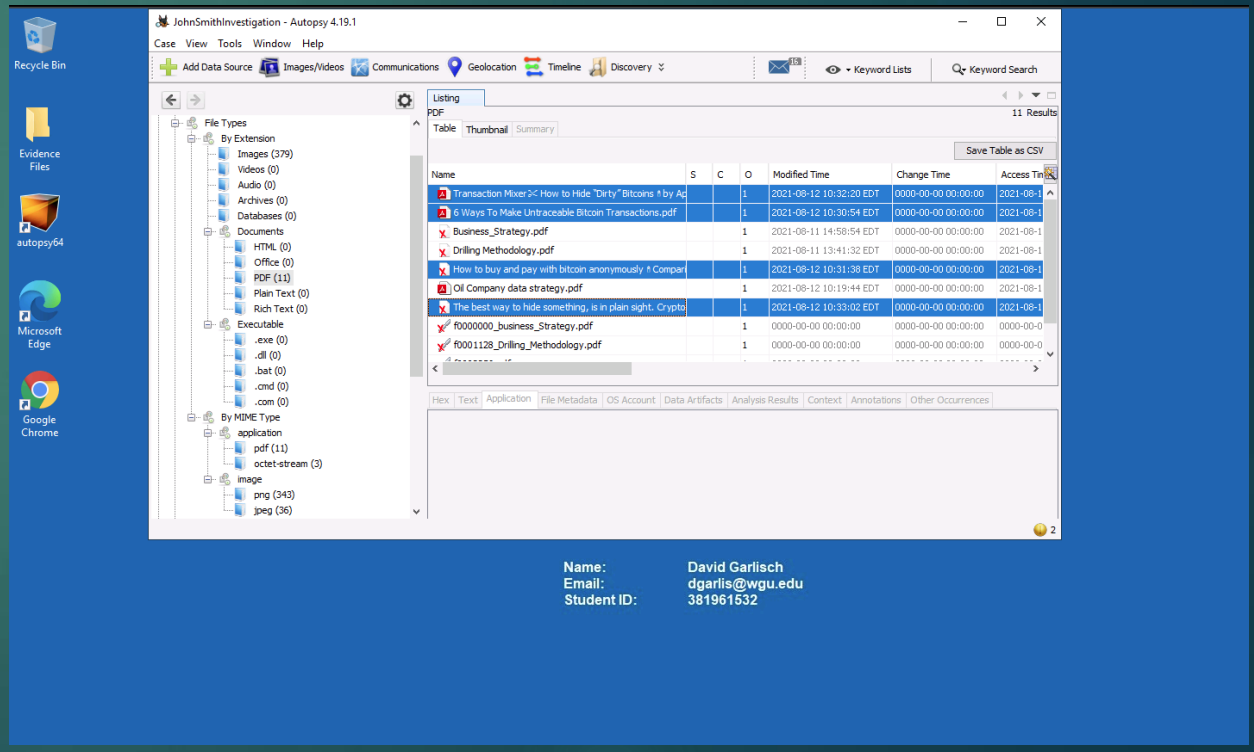


Name: David Garlisch
Email: dgarlis@wgu.edu
Student ID: 381961532

2.) I continued to see crypto references and even an anonymous picture in the pdf files. I extracted some of these files into evidence

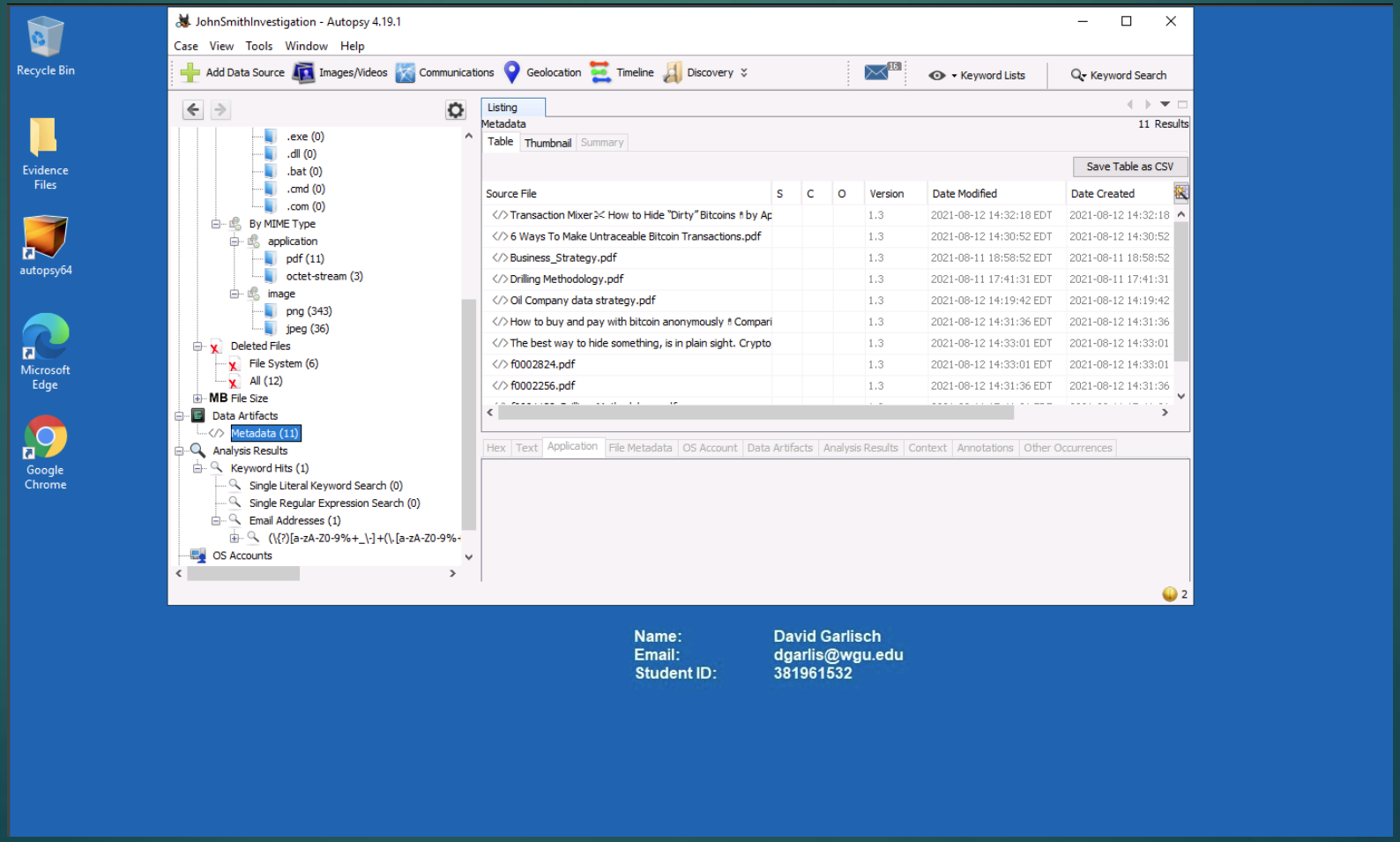


Name: David Garlisch
Email: dgarlis@wgu.edu
Student ID: 381961532

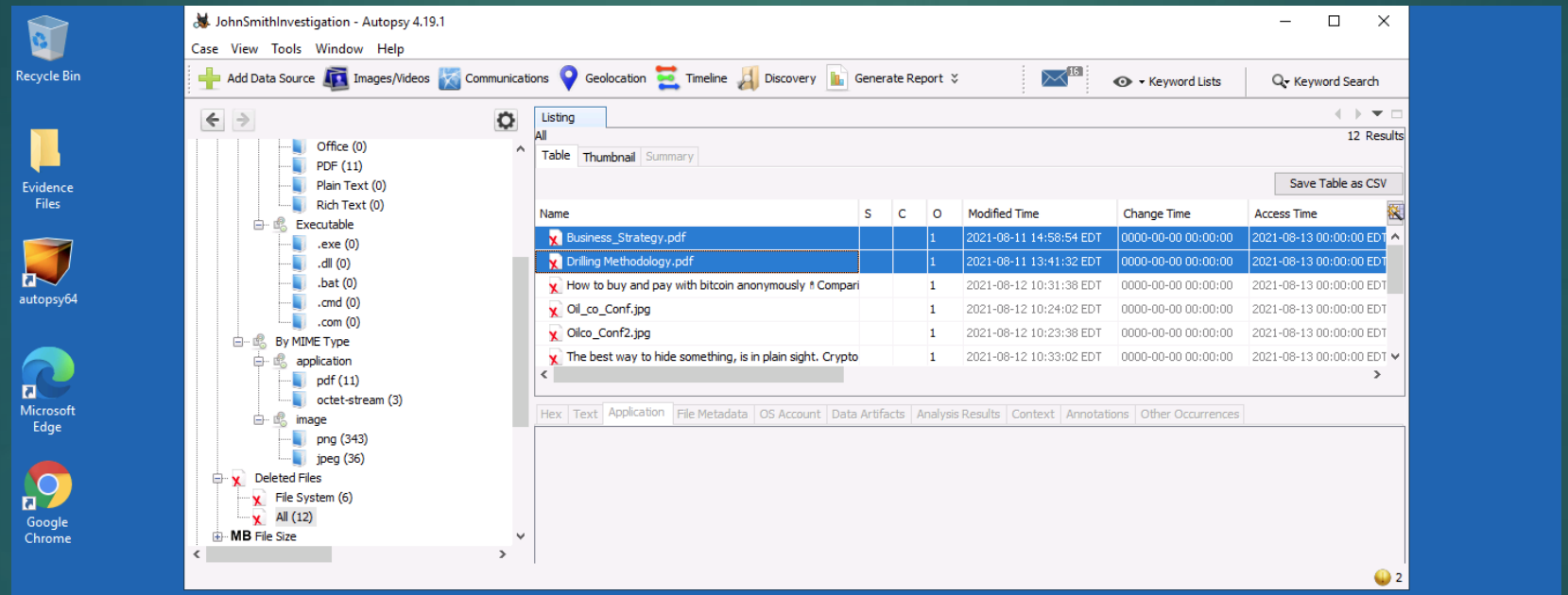


Name: David Garlisch
Email: dgarlis@wgu.edu
Student ID: 381961532

2.) I saw a folder with Metadata on some of these crypto pictures and extracted these files as well

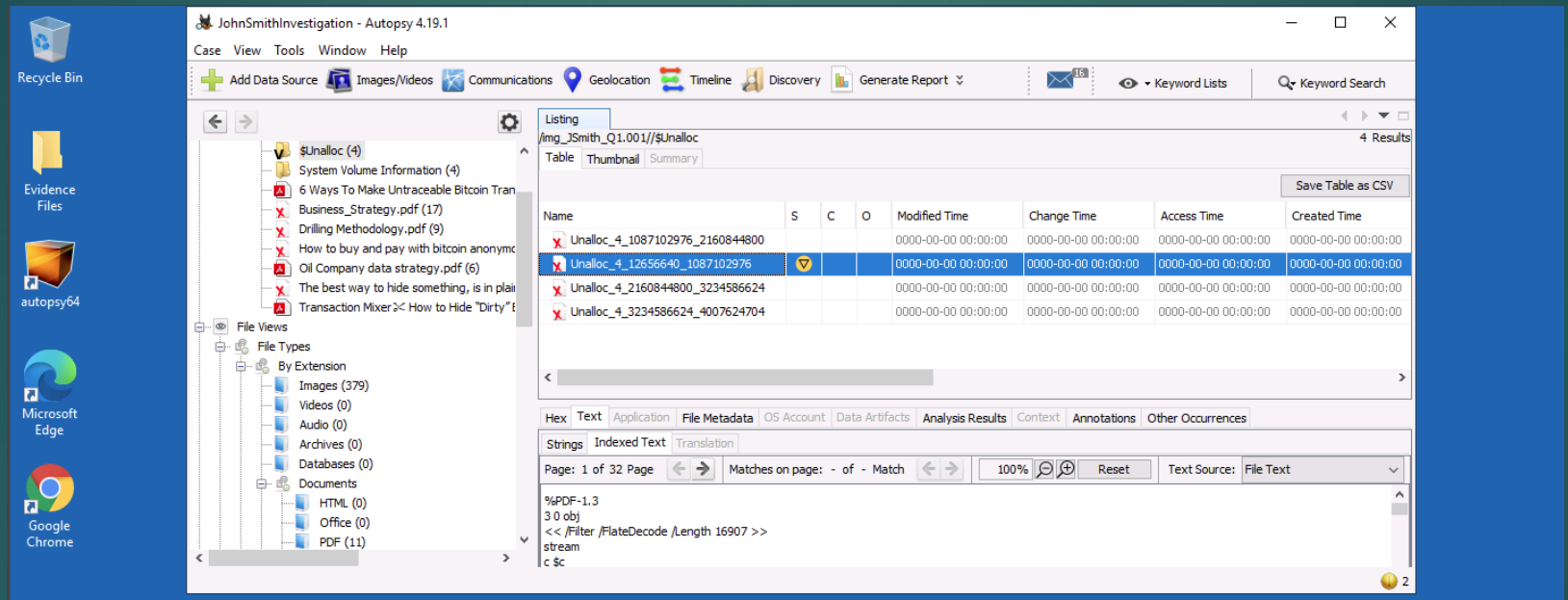


2.) As I was searching I went back to the deleted files and thought it was suspicious and odd that Business Strategy and Drilling Methodology was in the deleted files. I will treat this as if it was not on accident and extract these files as well. Deleting company information is evidence in this case. Other files here actually contained pictures that could be important to the company as well.



Name: David Garlisch
Email: dgarlis@wgu.edu
Student ID: 381961532

2.) Lastly, clicked on Keyword hits that lead to an email section. Further investigating on my part lead me to see that this email was suspicious because it looks like it contained a PDF. I extracted this for further investigation.



Name: David Garlisch
Email: dgarlis@wgu.edu
Student ID: 381961532

Summary

3.) During this investigation I would say there was suspicious activity going on by this user to warrant the investigation. The deleting of company pdfs, coupled with a suspicious email, and crypto bitcoin and anonymous images. This all suggests that John Smith is linked to having unauthorized information and violating company policies. Bitcoin being present everywhere and the suspicious email link John to possibly selling this information on the dark web.