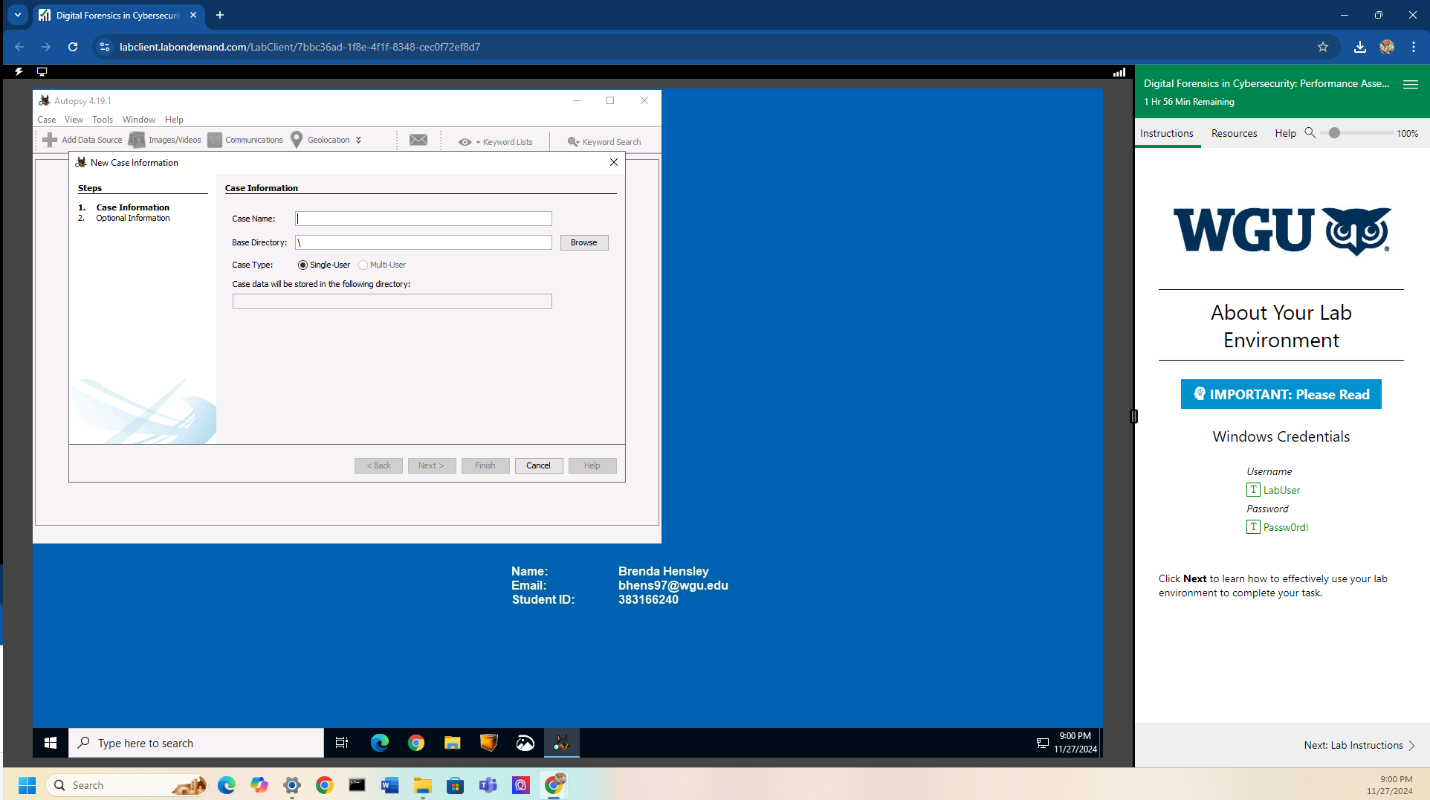
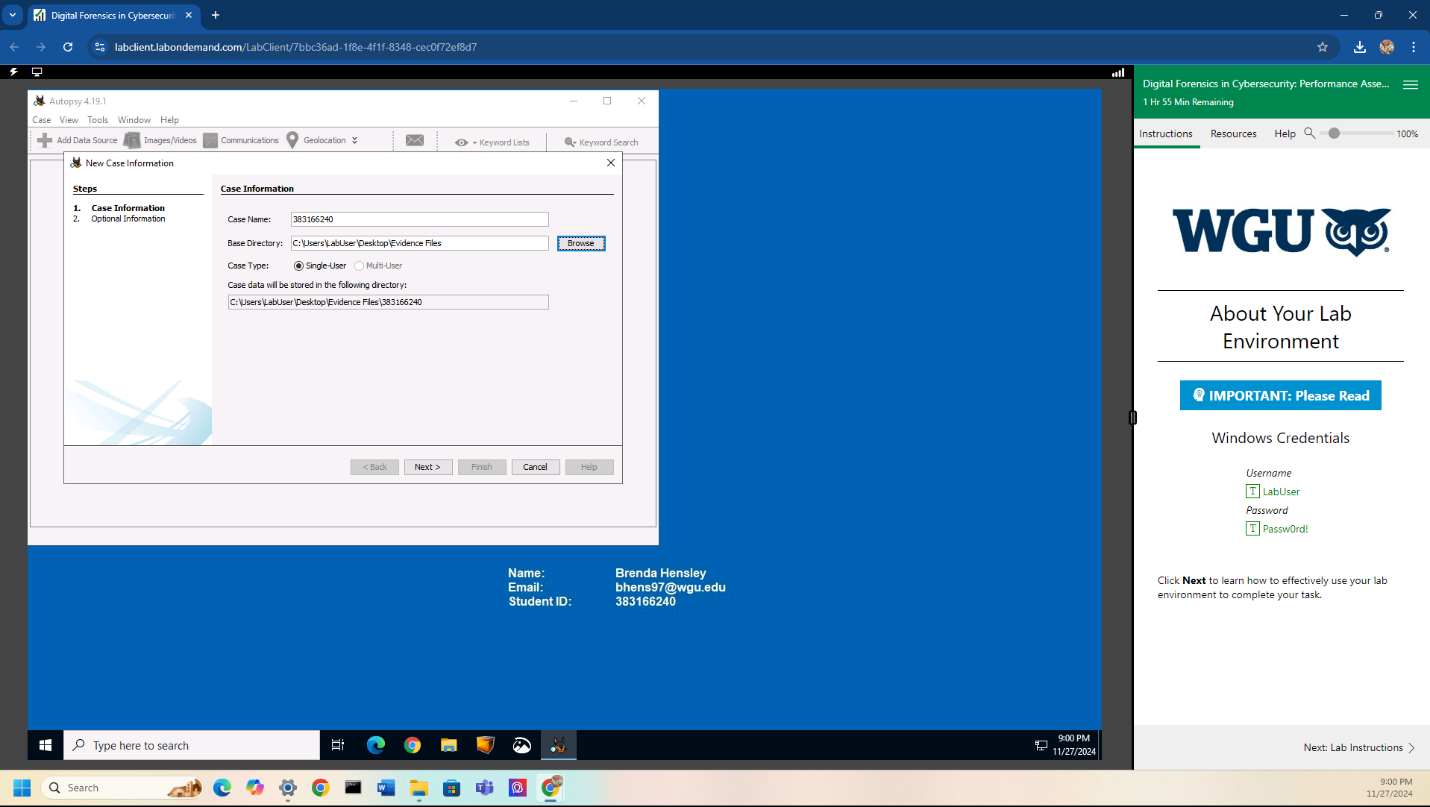
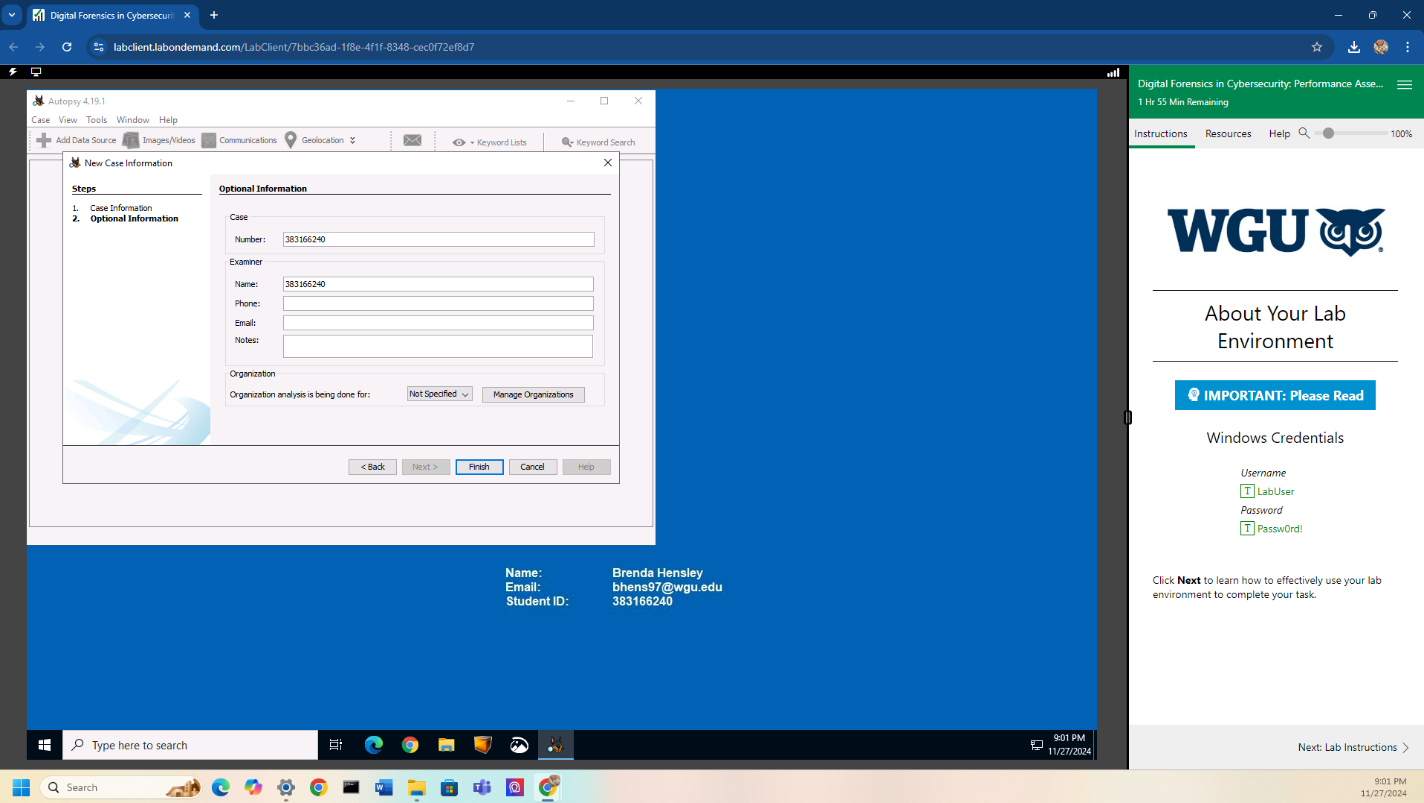
**A1**

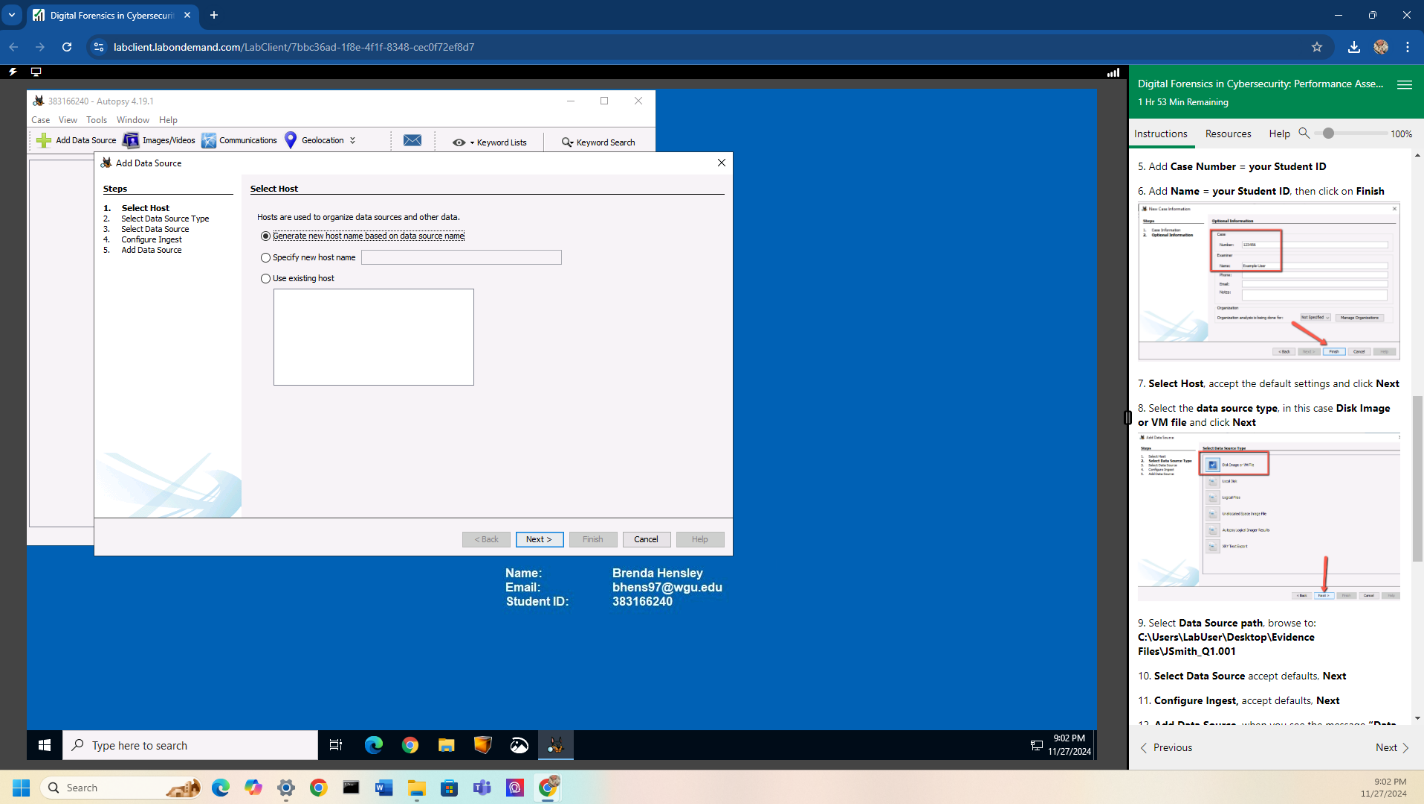
The following screenshots show the exact steps that I took while opening a new case file within the Autopsy program. I gave the case file the title of my student ID, 383166240. The case data will be saved to C:\Users\LabUser\Desktop\EvidenceFiles\383166240. I used my student ID as the case number as well as the name of the examiner and chose the option to generate a new host name based on data source names, choosing data source type as Disk Image or VM File. From there, I chose the JSmith\_Q1.001 disk file as the source and set the source path as C:\Users\LabUser\Desktop\EvidenceFiles\JSmith\_Q1.001. I accepted all defaults to configure ingest and then waited for the case to be opened. It was generated using the JSmith\_Q1.001 disk image.





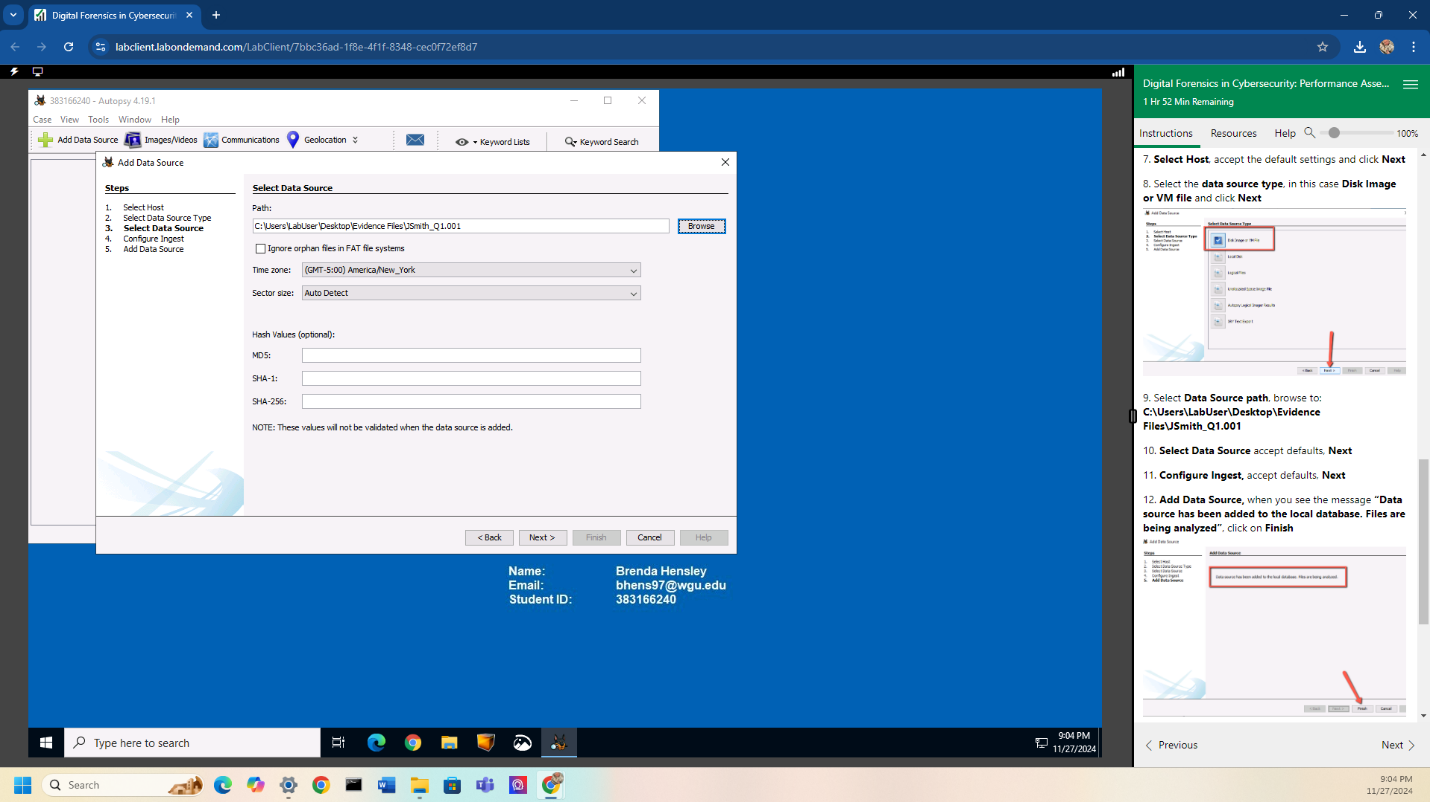


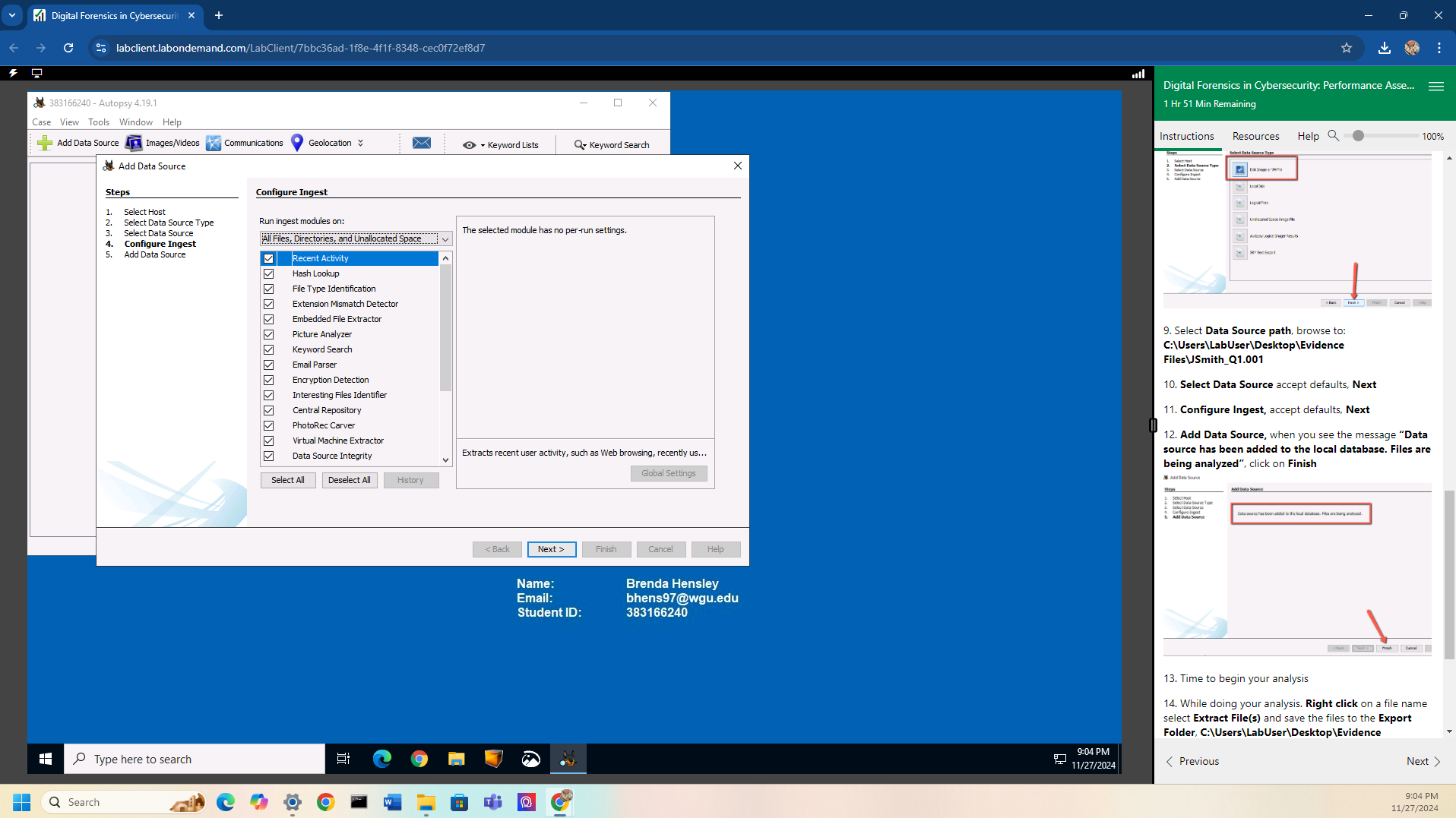
A computer screen with a blue background

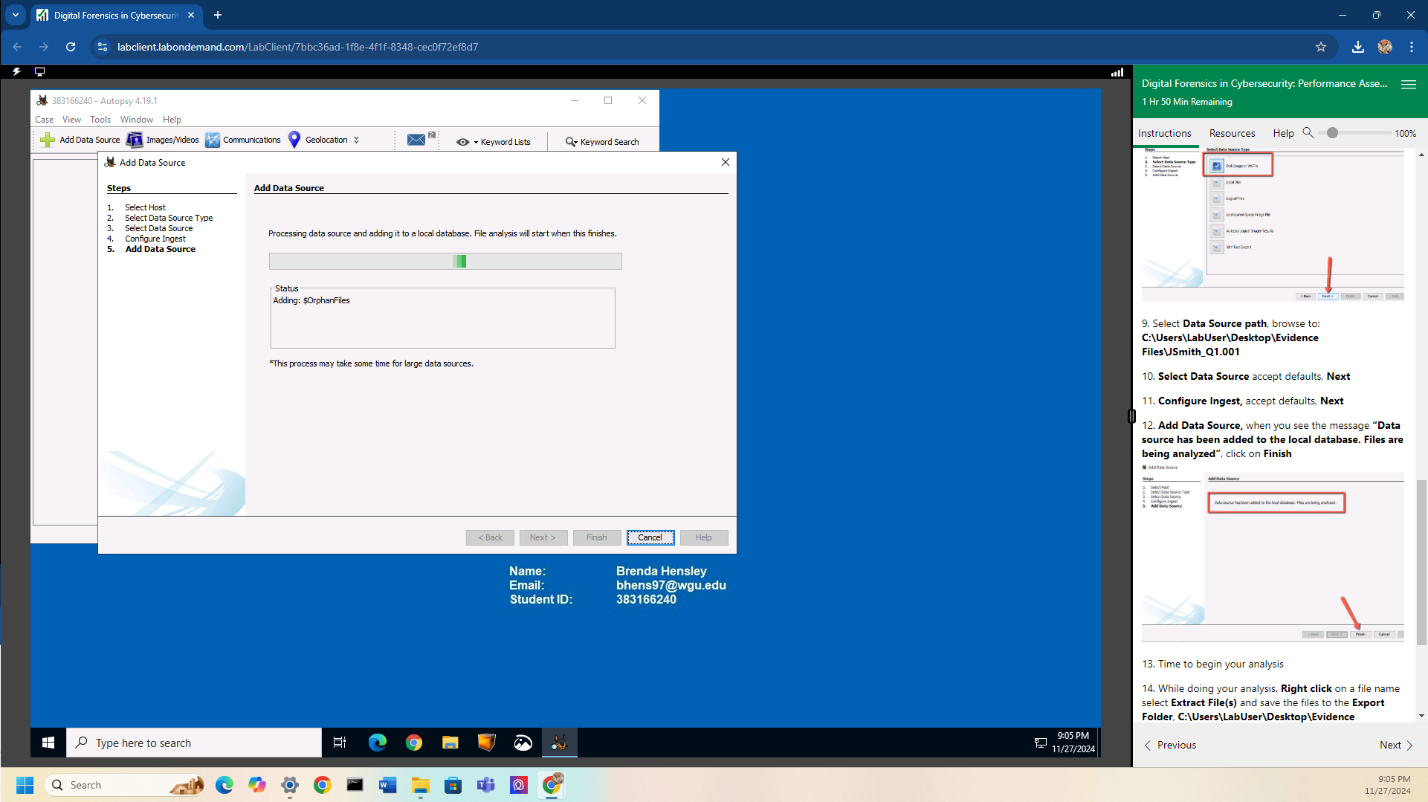
Description automatically generated

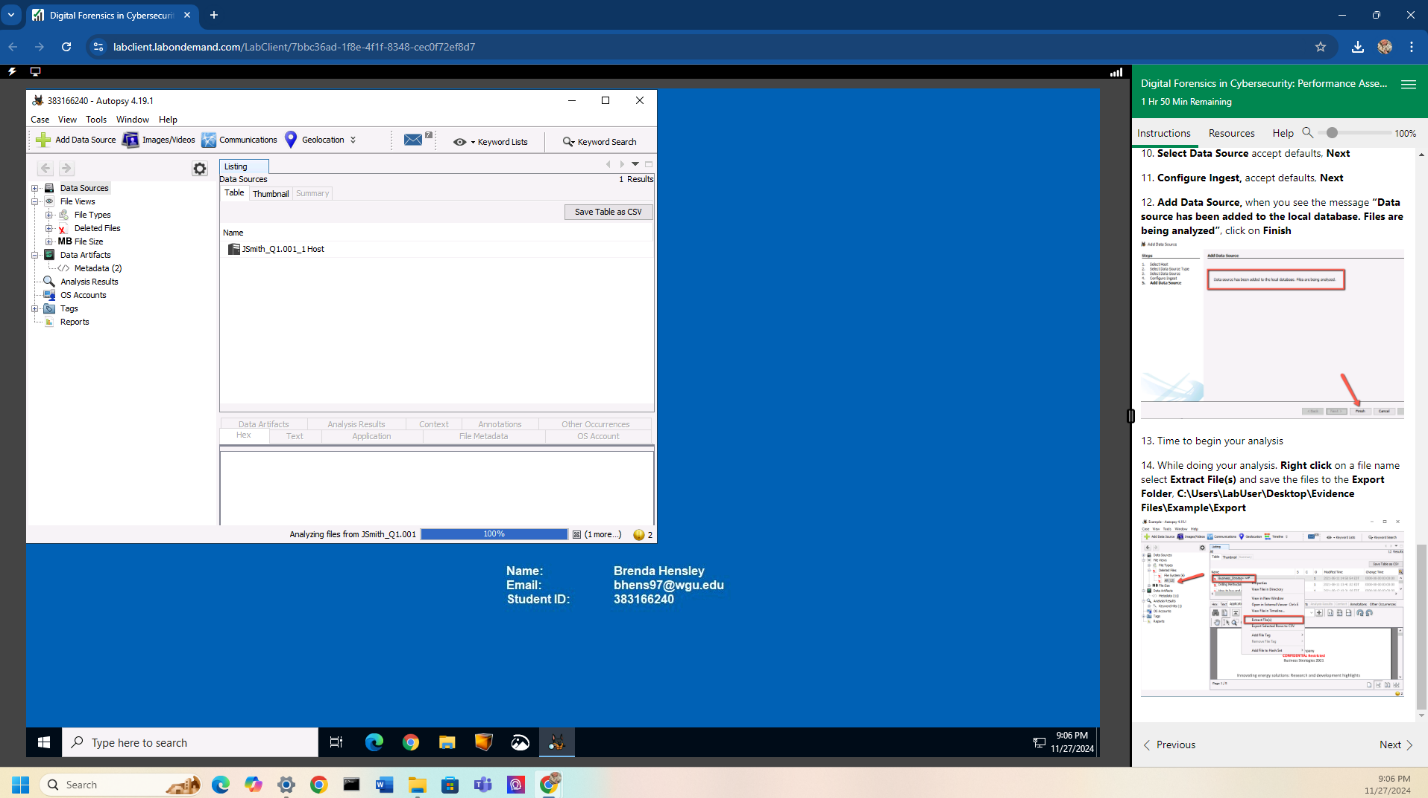
A computer screen with a blue background

Description automatically generated

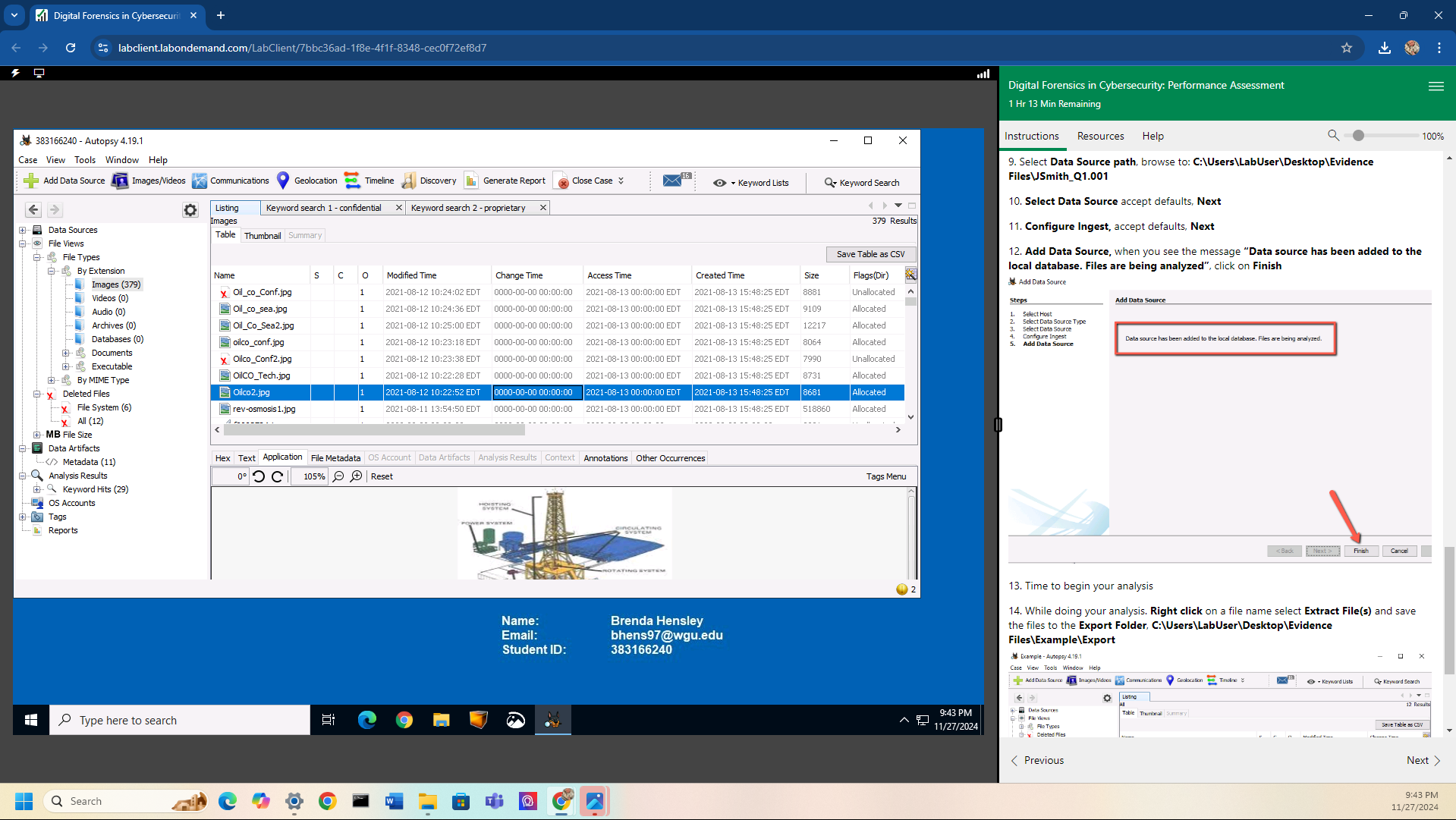
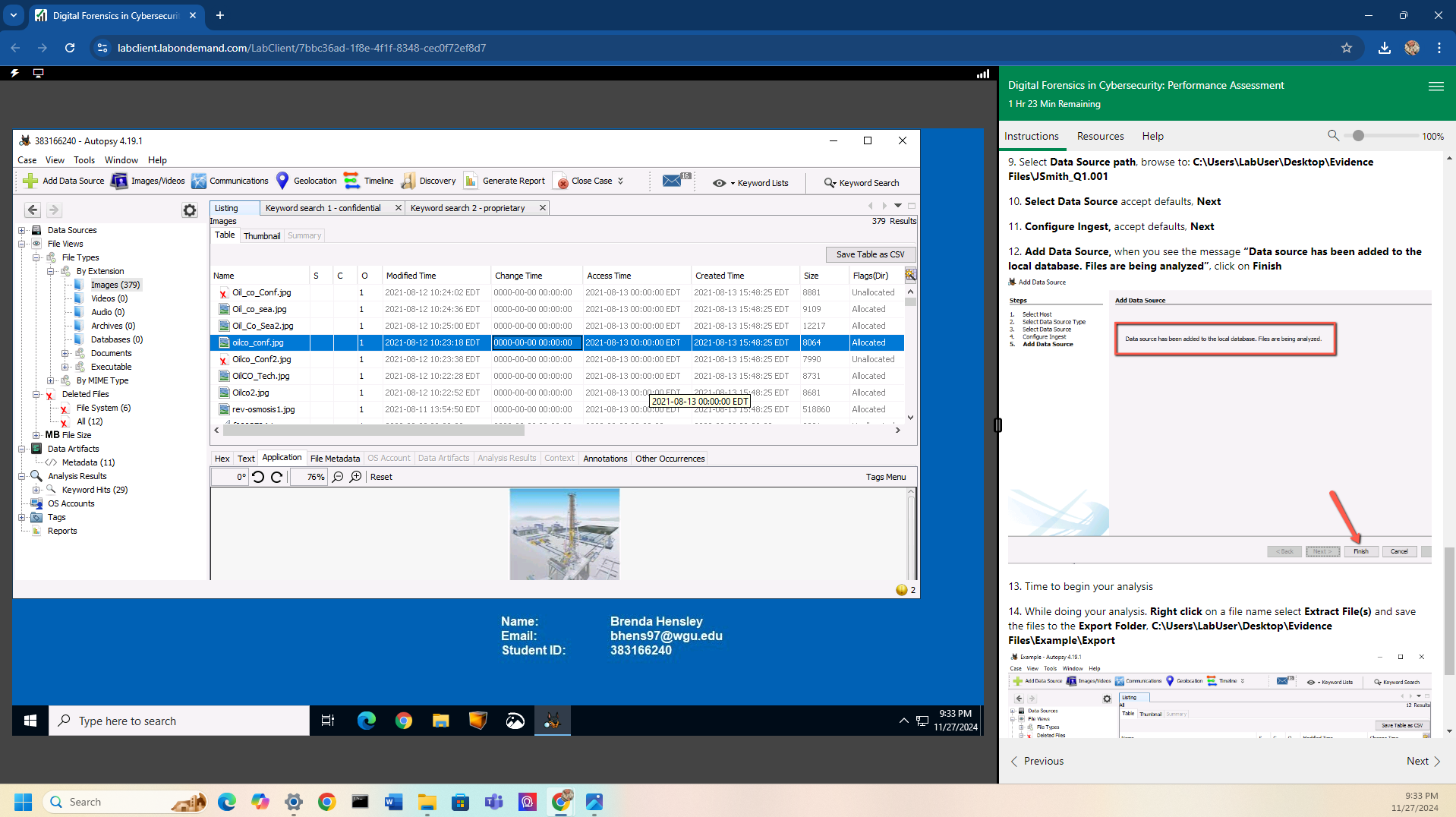
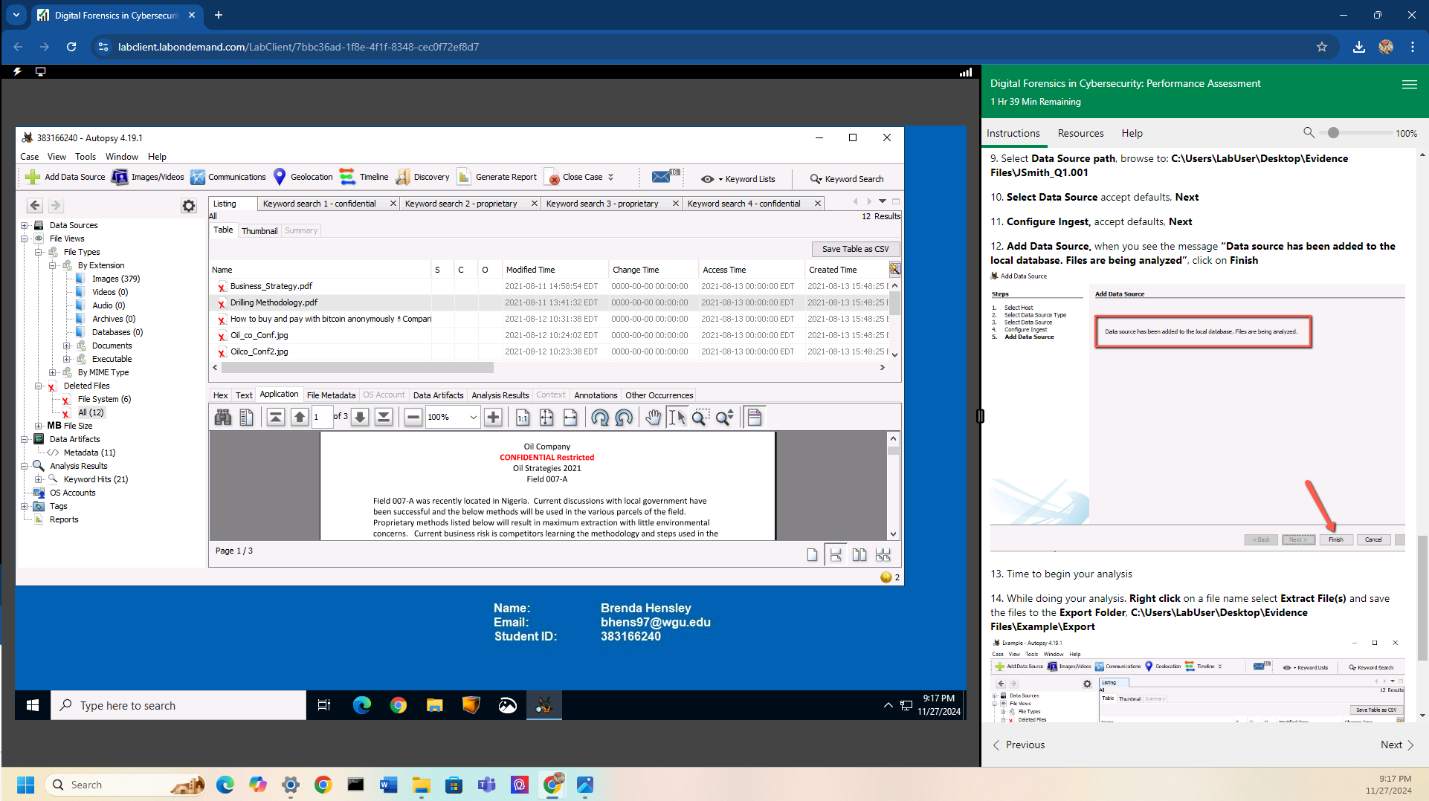
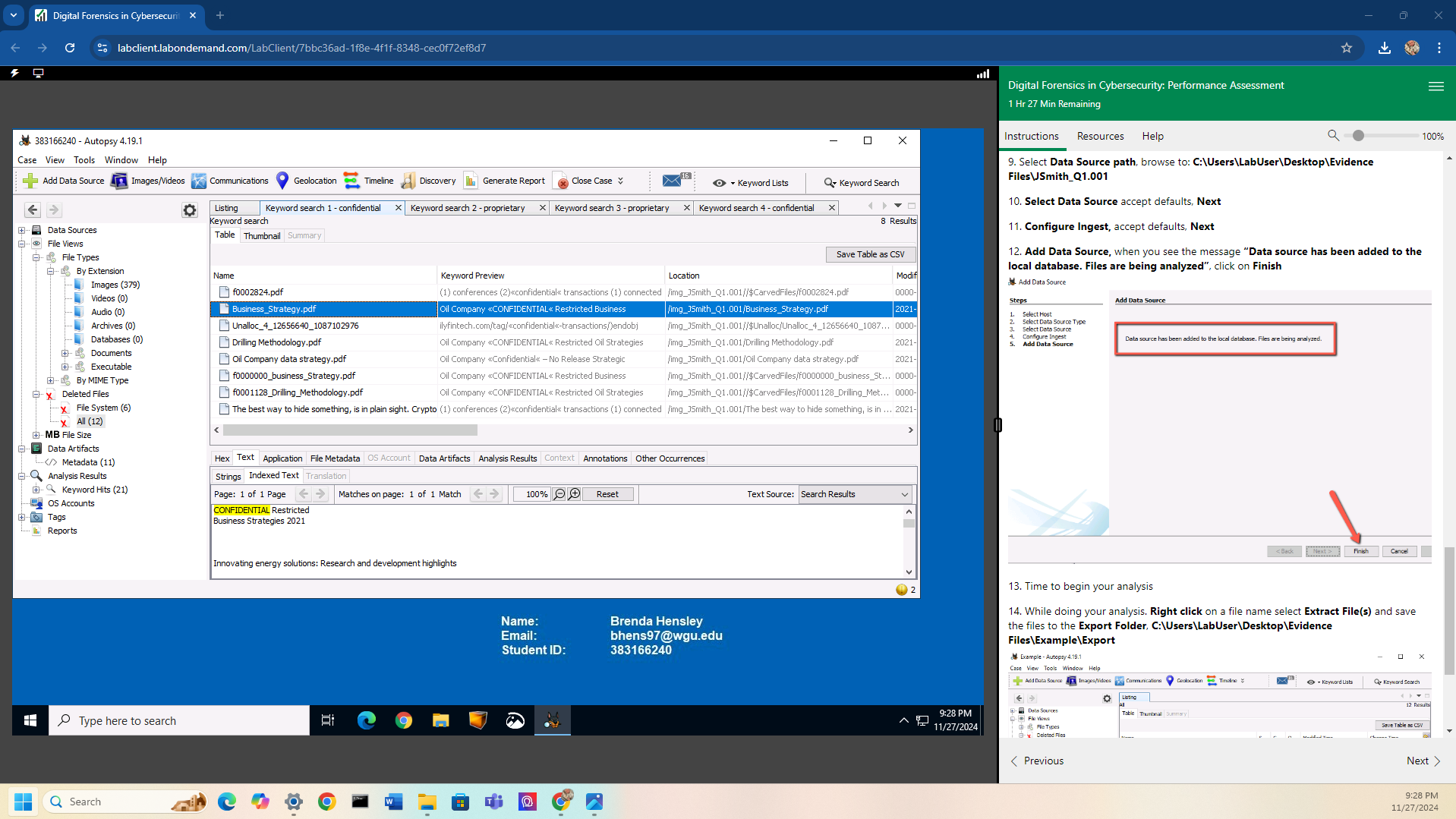
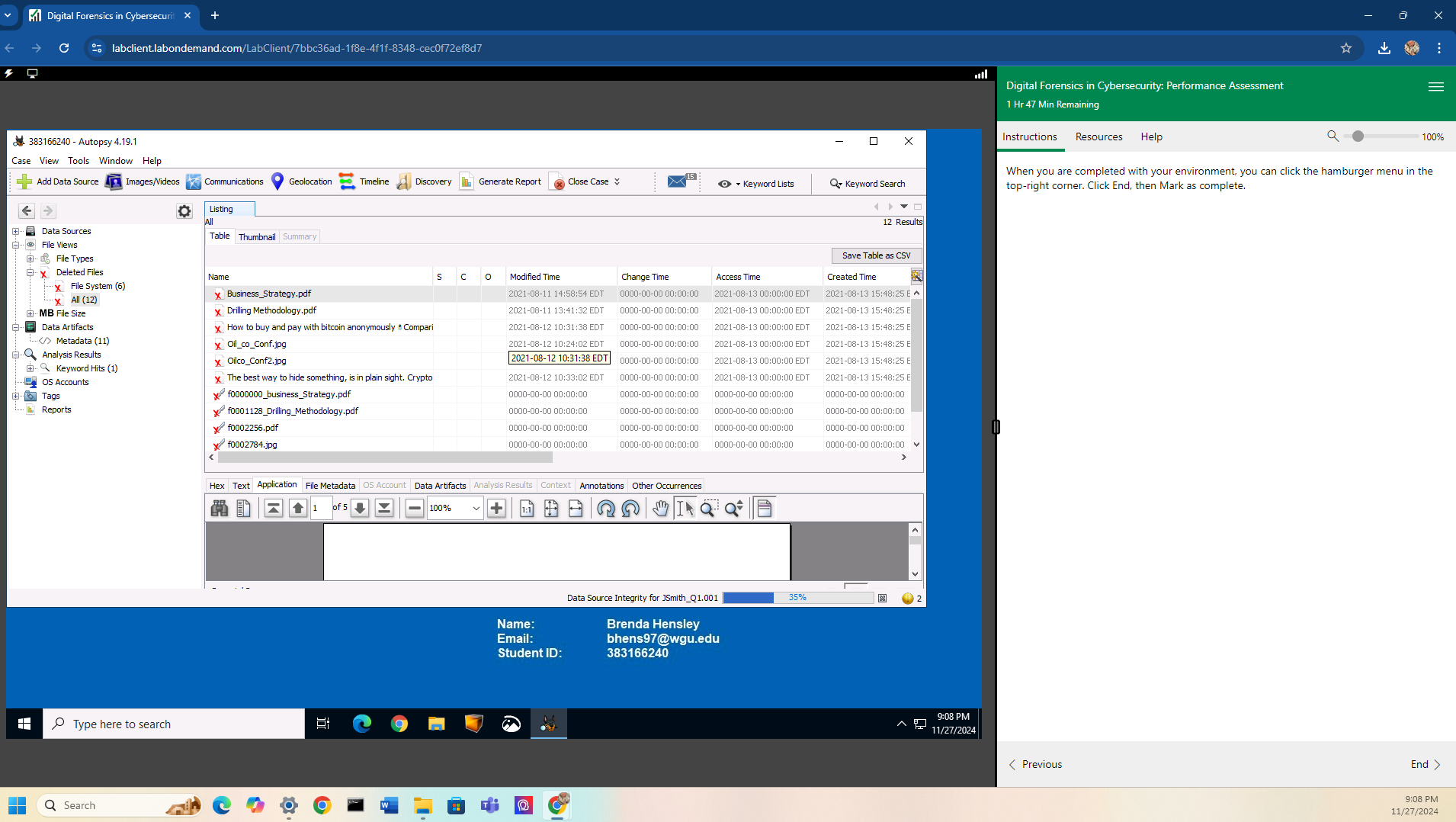
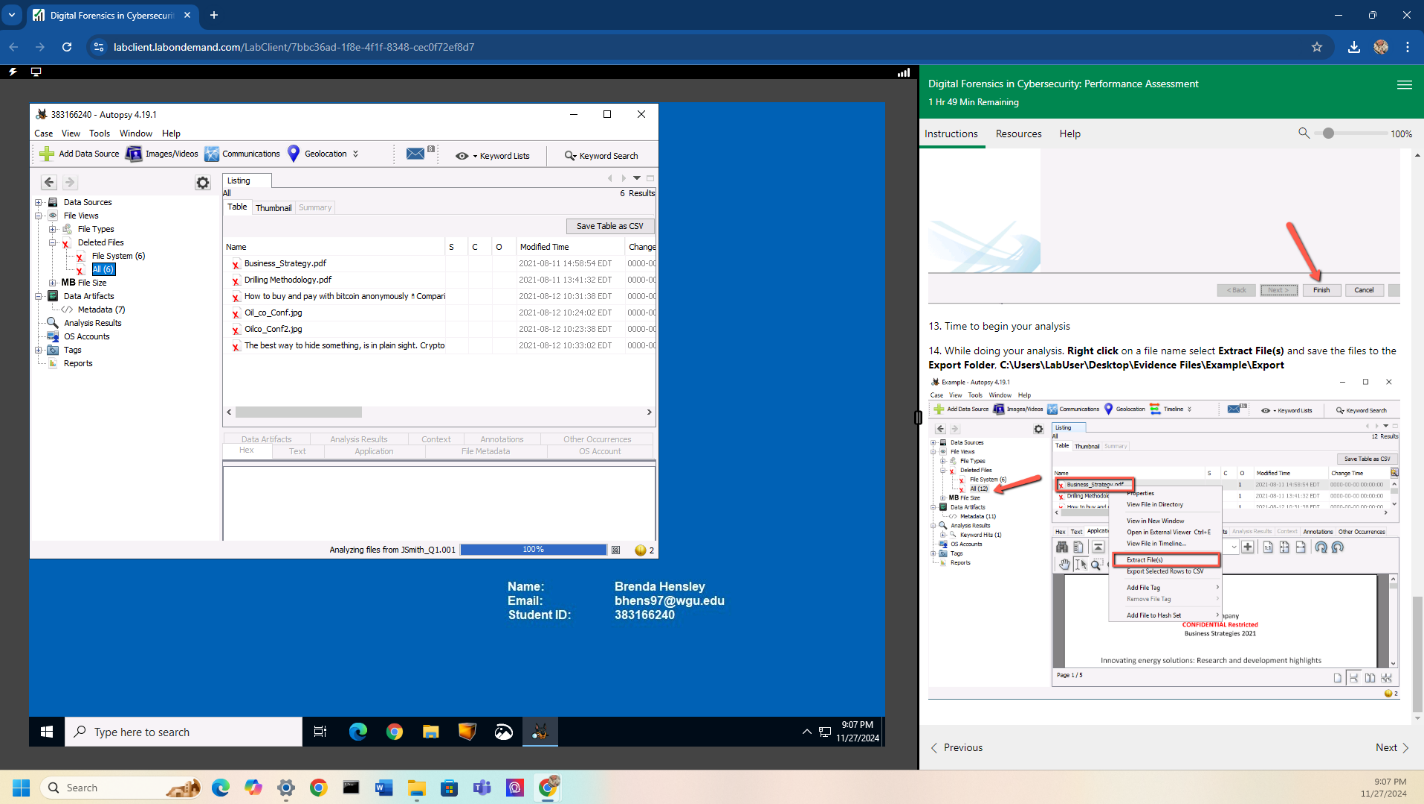


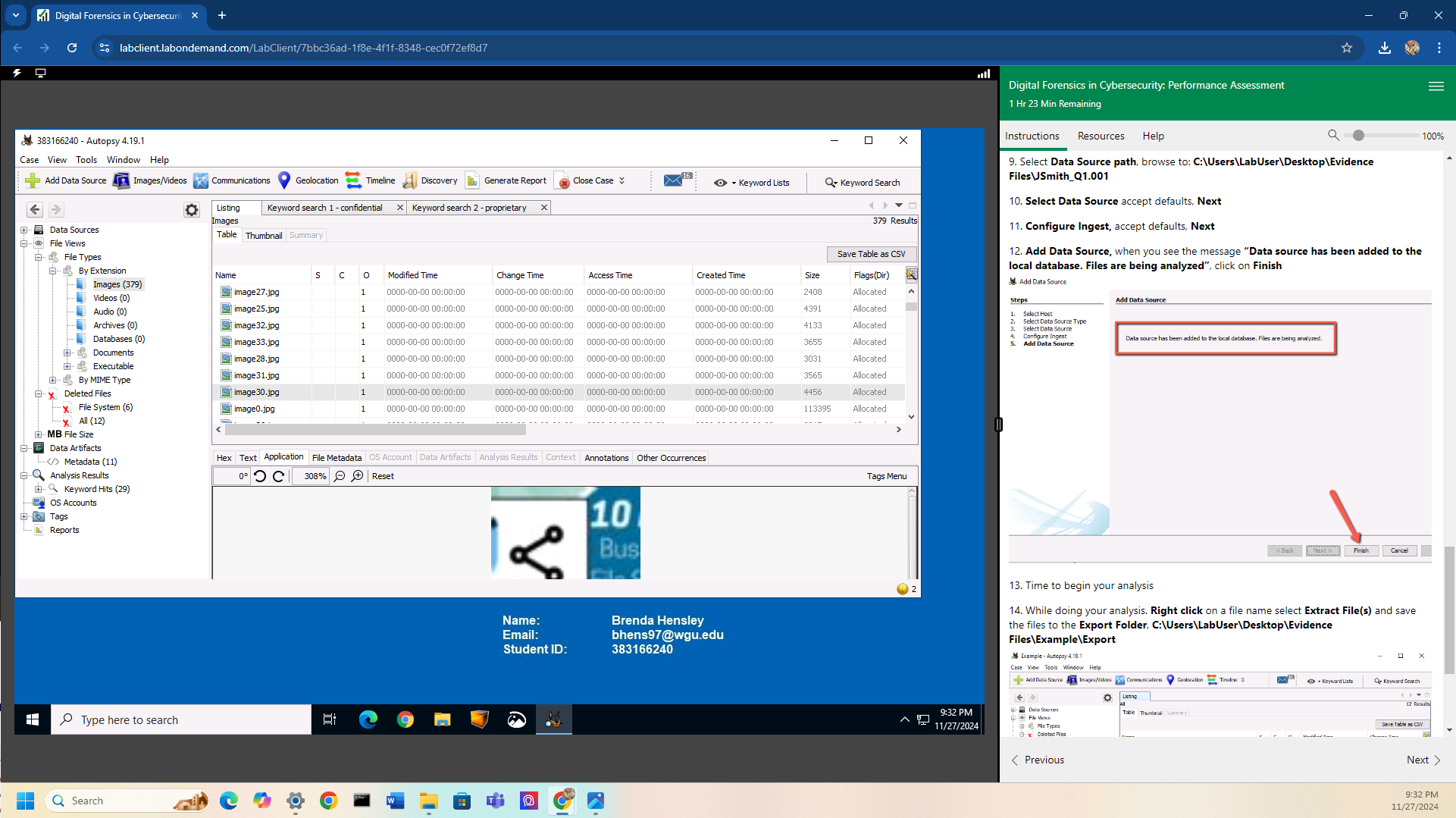


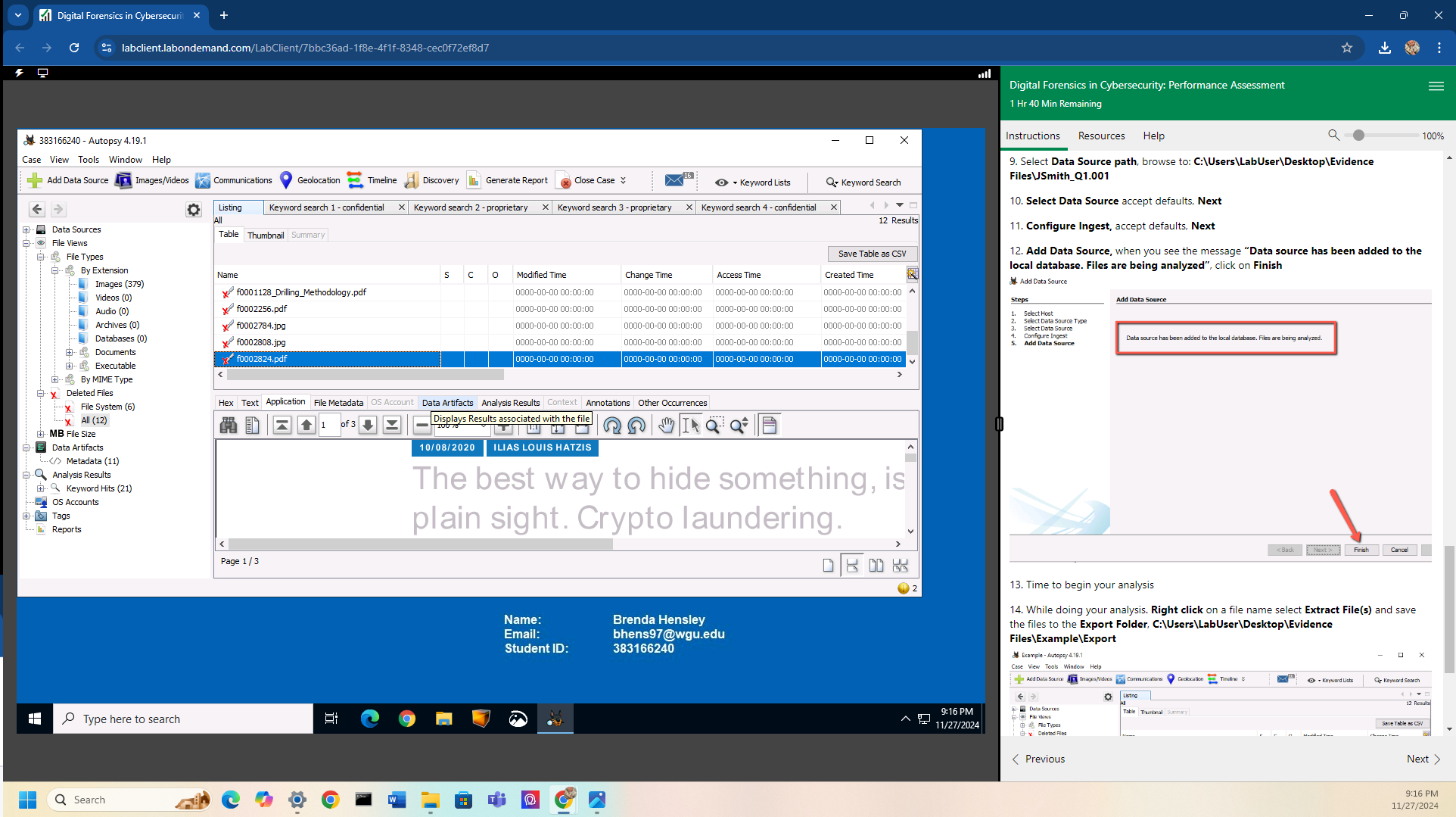




**A2**

During my initial walkthrough of the JSmith\_Q1.001 disk image, I noticed that there were quite a few photos as well as deleted files. There were 12 deleted files and 379 images. I used the keyword search to find files specifically labeled as “Confidential” or “Proprietary.” There were 8 results, including “Drilling Methodology.pdf” and “Business\_Strategy.pdf” under the “Confidential” keyword search, as well as 2 documents under the “Proprietary” keyword search, “Drilling Methodology.pdf” and “f000128\_Drilling\_Methodology.pdf.” Upon further inspection of the images, I found many photos of the oil company’s rig configurations and diagrams. There were also some blurry images that I believe could be related to steganography, which would correspond to a deleted file that seems to be a website titled “The best way to hide something, is in plain sight. Crypto laundering”.





**A3**

After investigating the JSmith\_Q1.001 disk image, it was discovered that John Smith had confidential and proprietary information that he was not authorized to access. The screenshots provided prove the allegations against John Smith are correct. Evidence points to John Smith planning to sell confidential/proprietary information anonymously using Bitcoin transactions, possibly using steganography as the vessel to release the information.