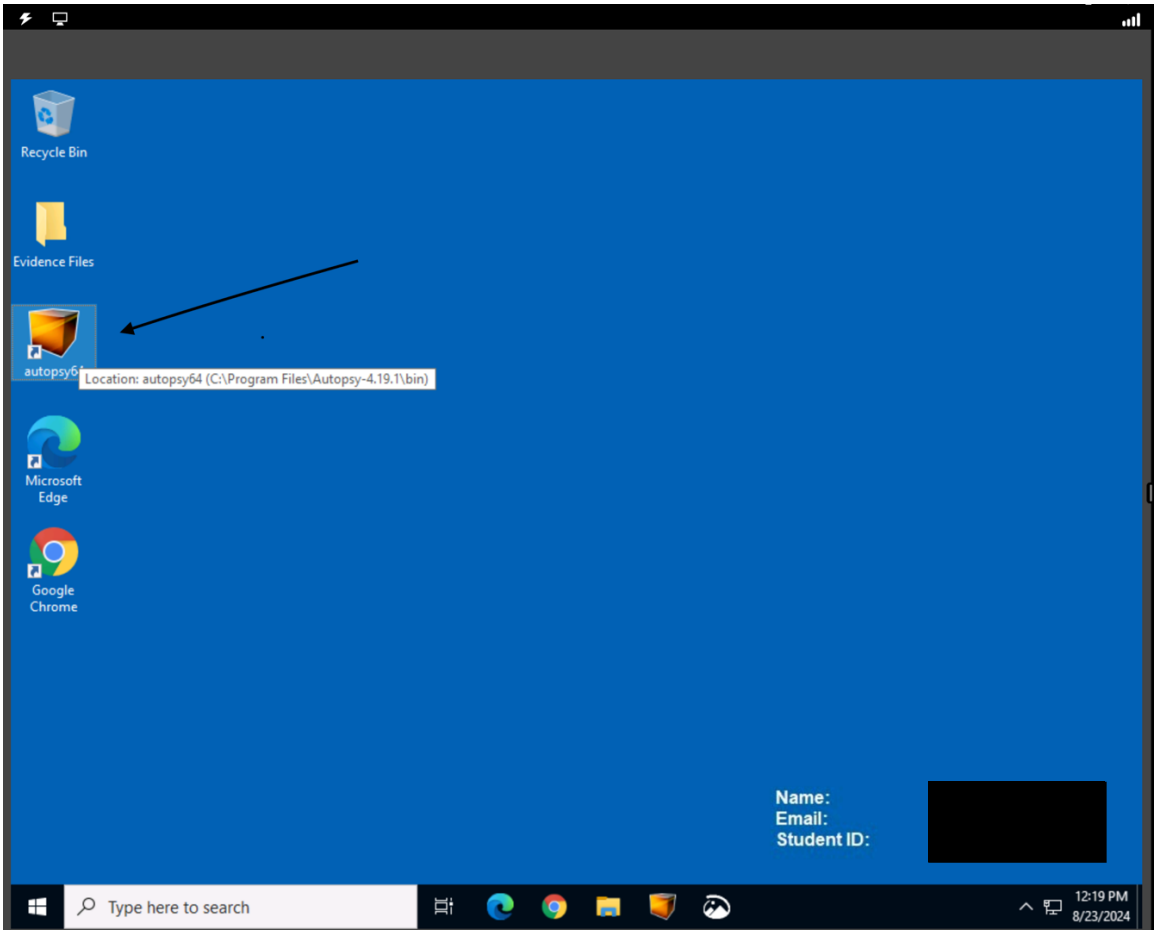
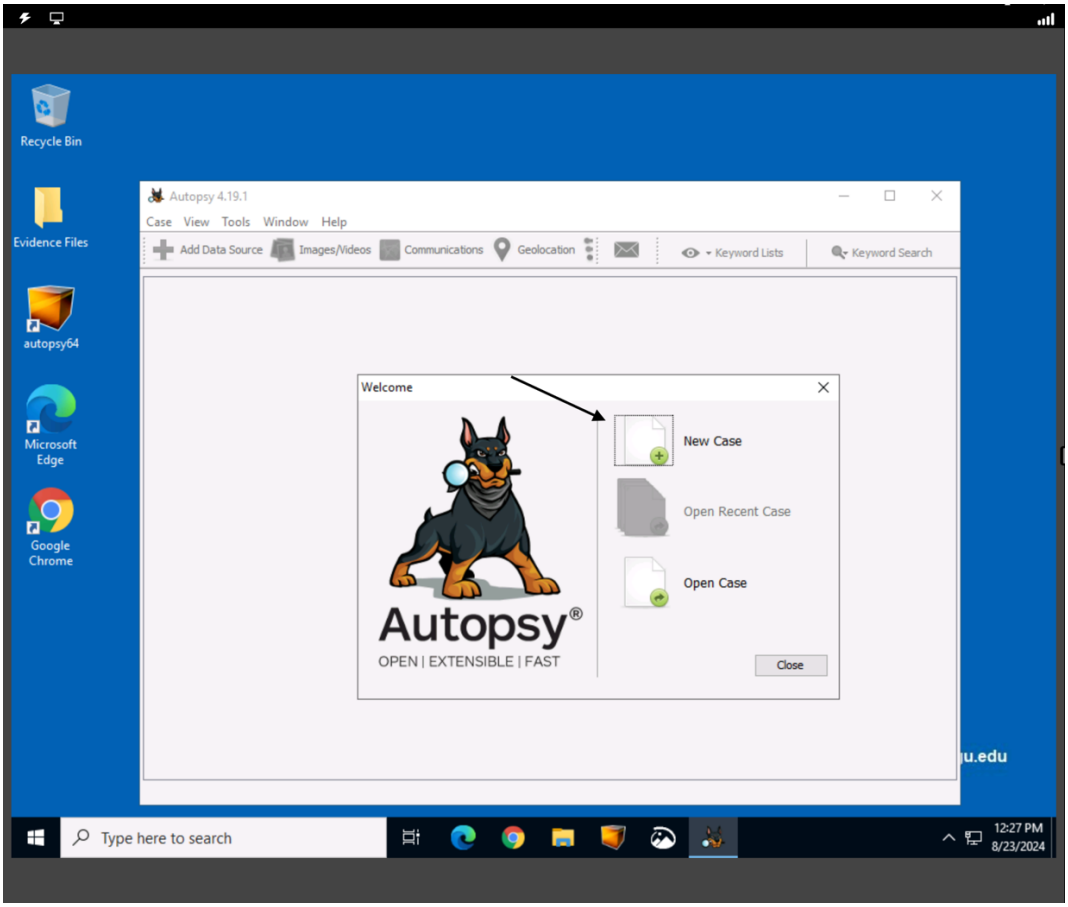
A. Write a report for the team of investigators by doing the following:

A1. Describe *all steps* taken in Autopsy to create the forensic system case file. Provide screenshots of these steps.

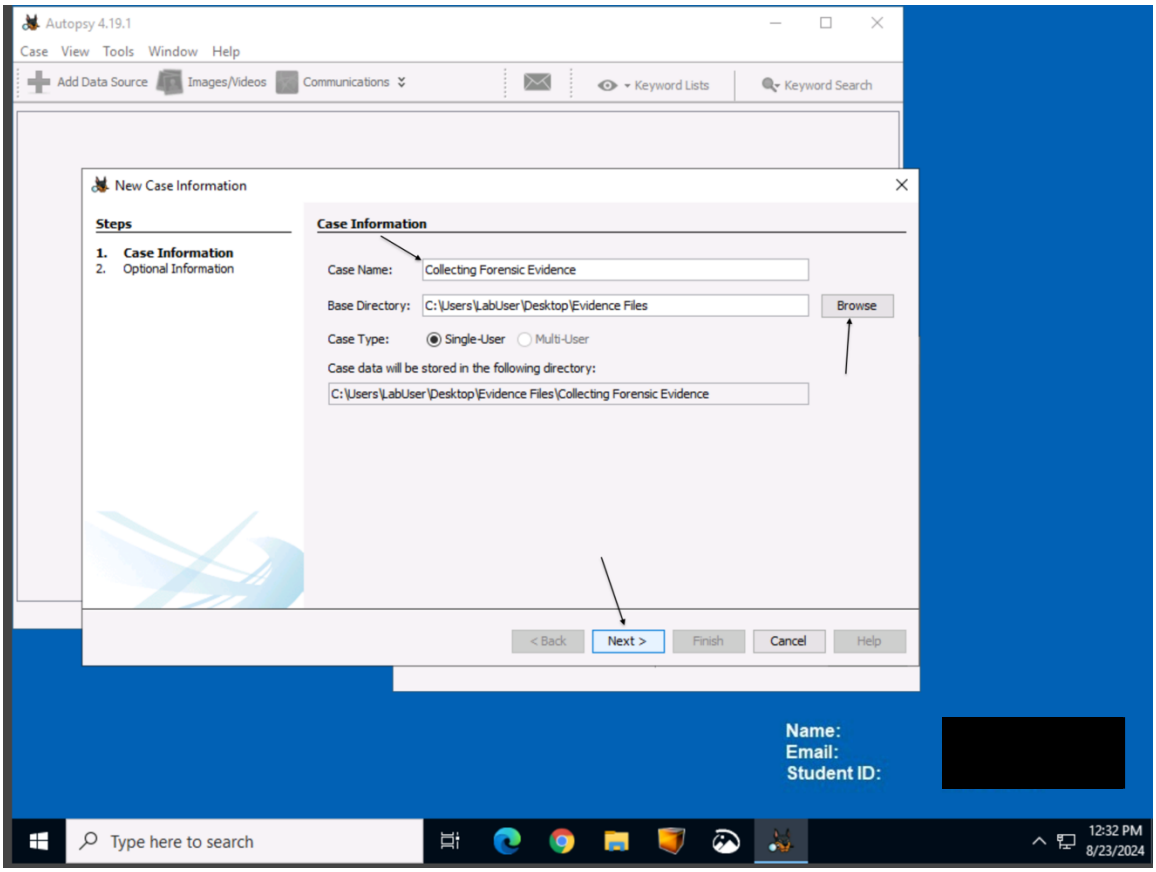
Step 1: Open and run Autopsy



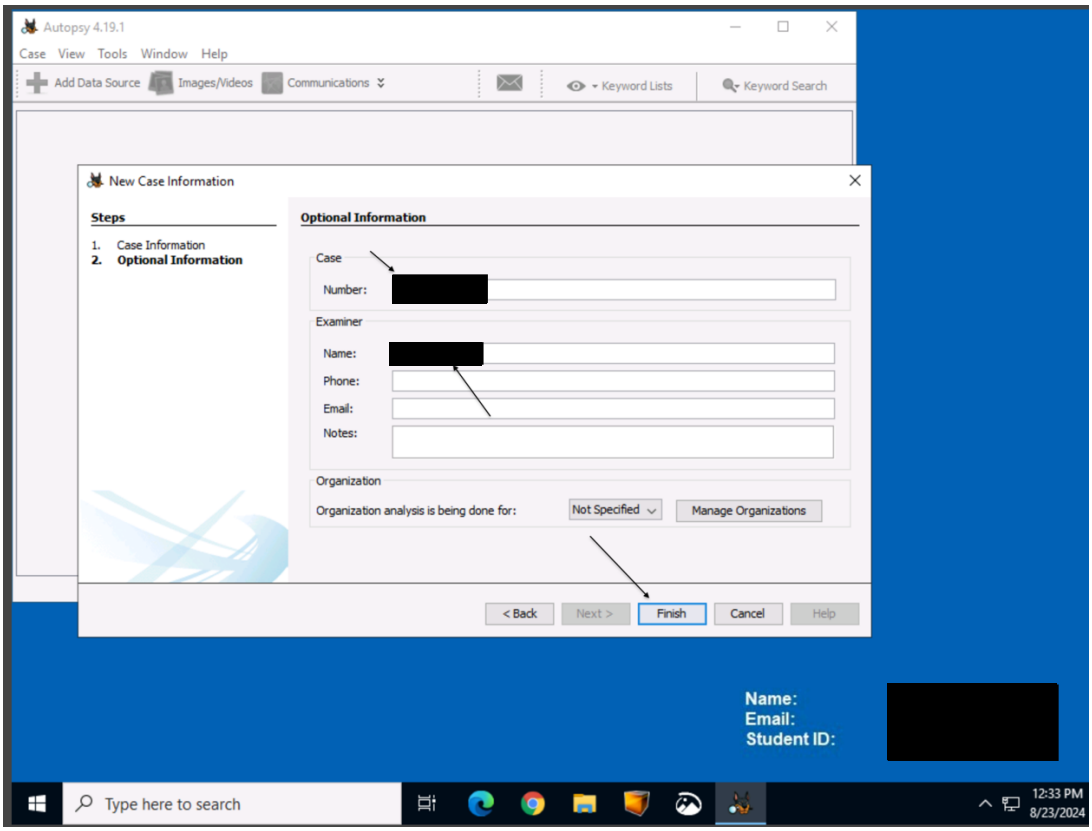
Step 2: Select new case file in Autopsy



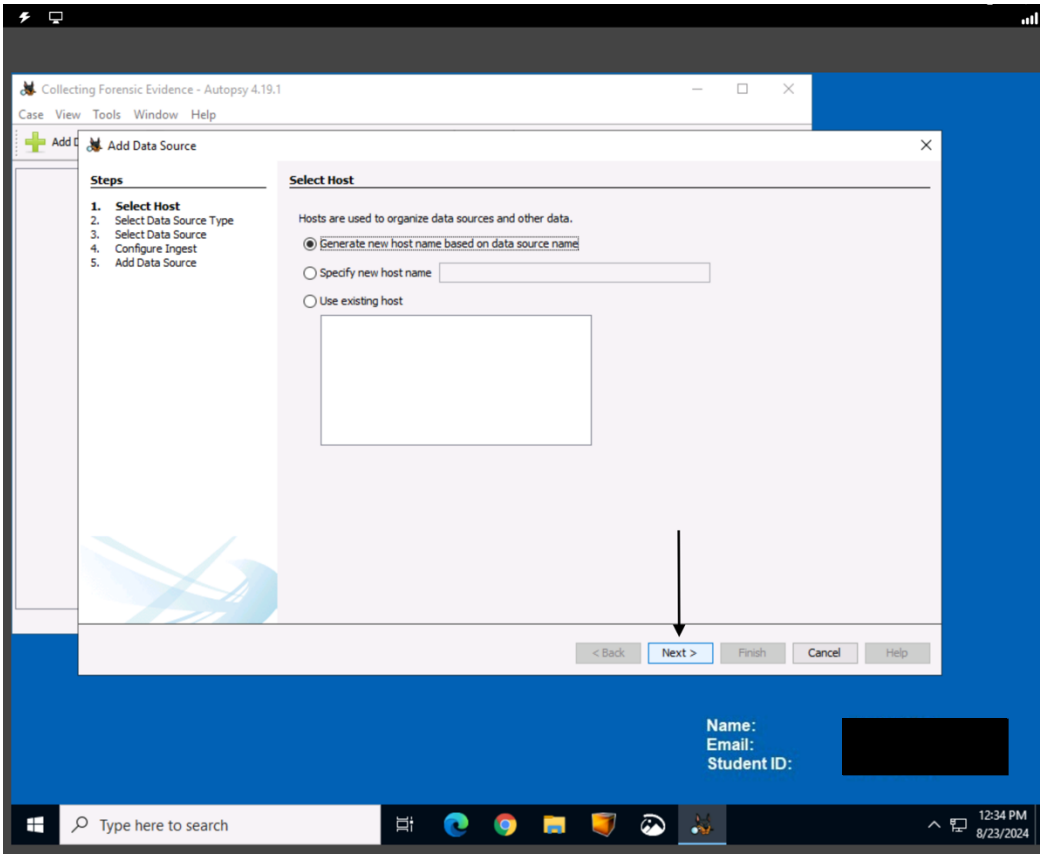
Step 3: The new case wizard dialog box opens.
Enter the **Case Name** (Collecting Forensic Evidence) and enter a **Base Directory** using the browse button: **C:\Users\LabUser\Desktop\Evidence Files.** Then click on **Next**



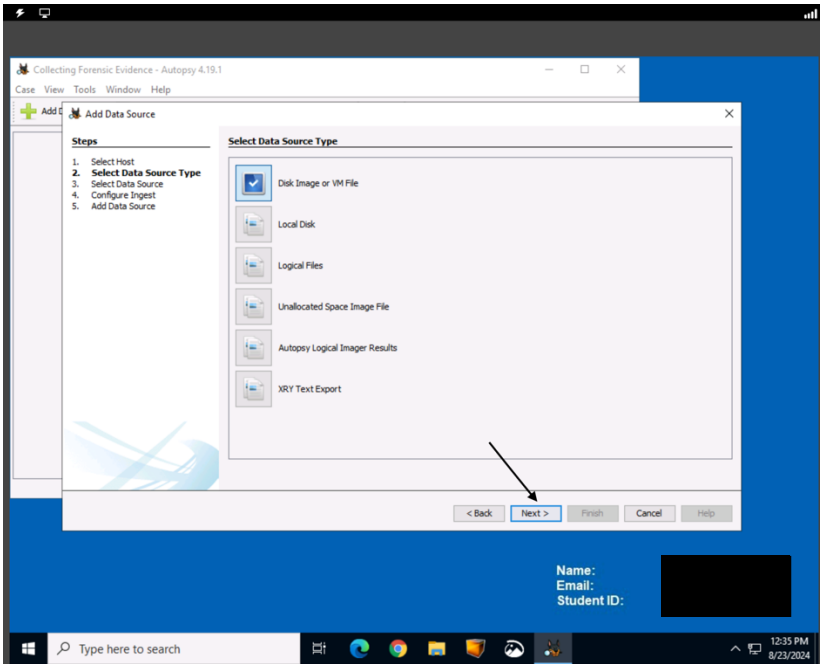
Step 4: Add **Case Number = your Student ID** and Add **Name = your Student ID**, then click on **Finish**



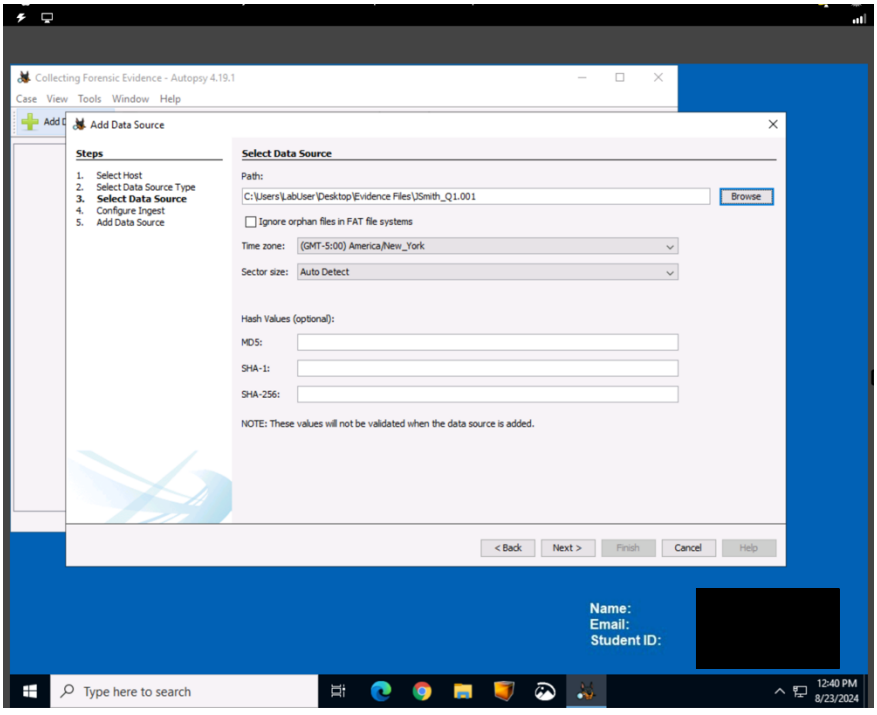
Step 5: Select Host, accept the default settings and click **Next**



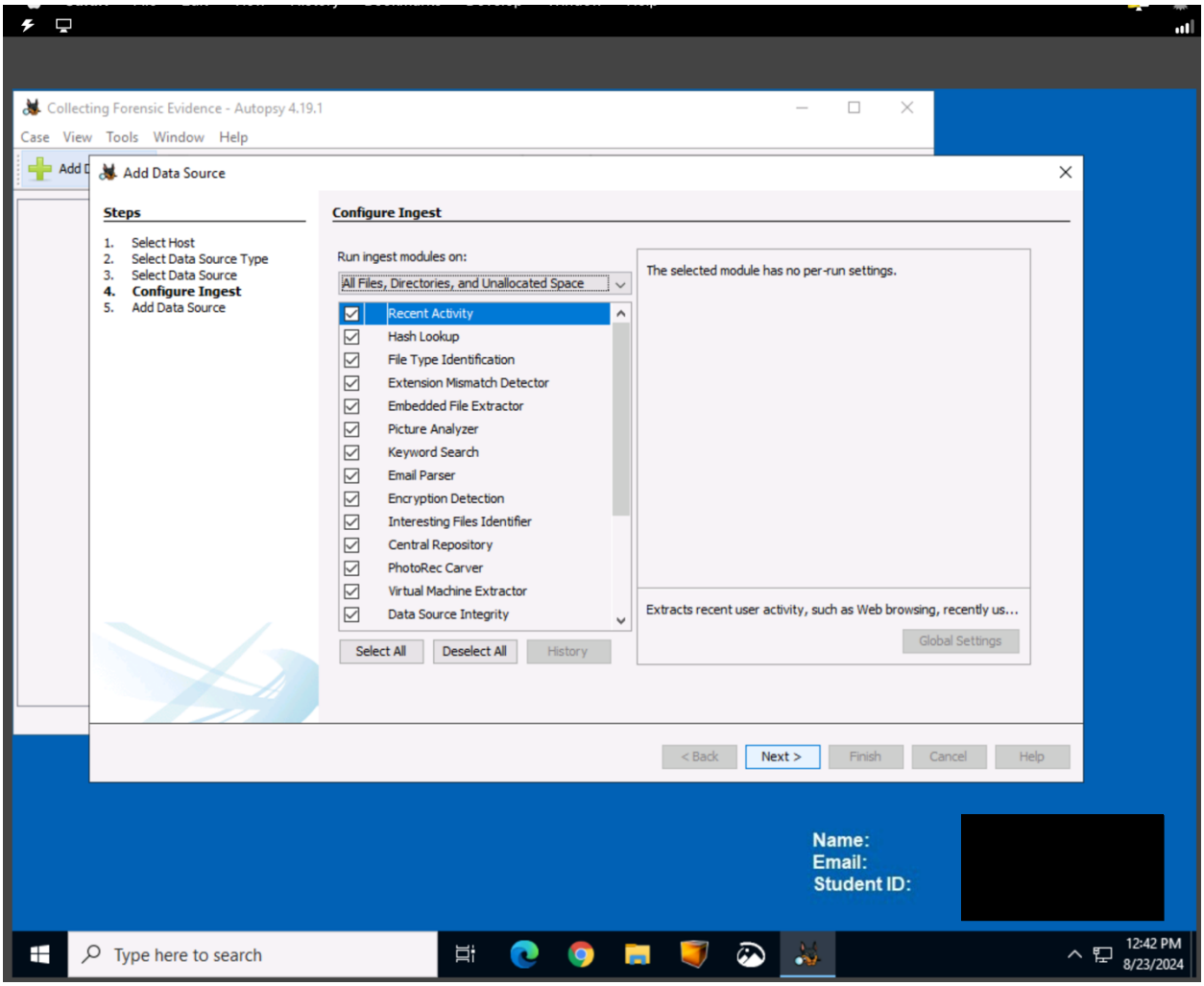
Step 6: Select the **data source type**, **Disk Image or VM file** and click **Next**



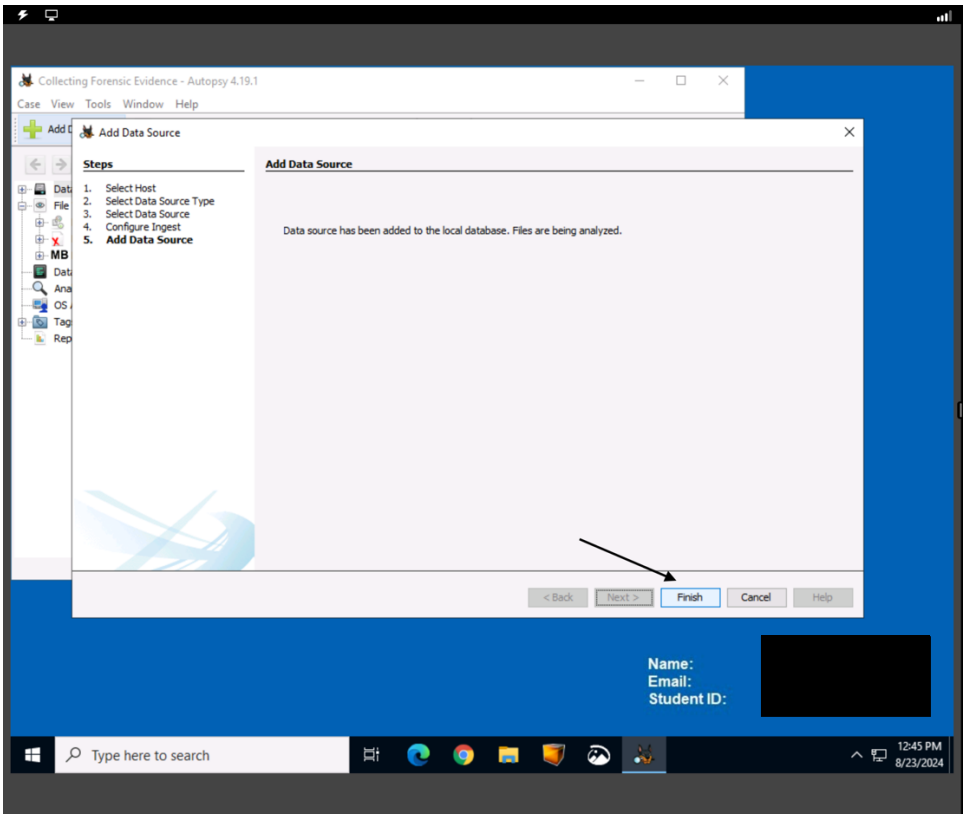
Step 7: Select **Data Source path**, browse to: **C:\Users\LabUser\Desktop\Evidence Files\JSmith_Q1.001** and **Select Data Source** accept defaults, **Next**



Step 8: Configure Ingest, accept defaults, **Next**

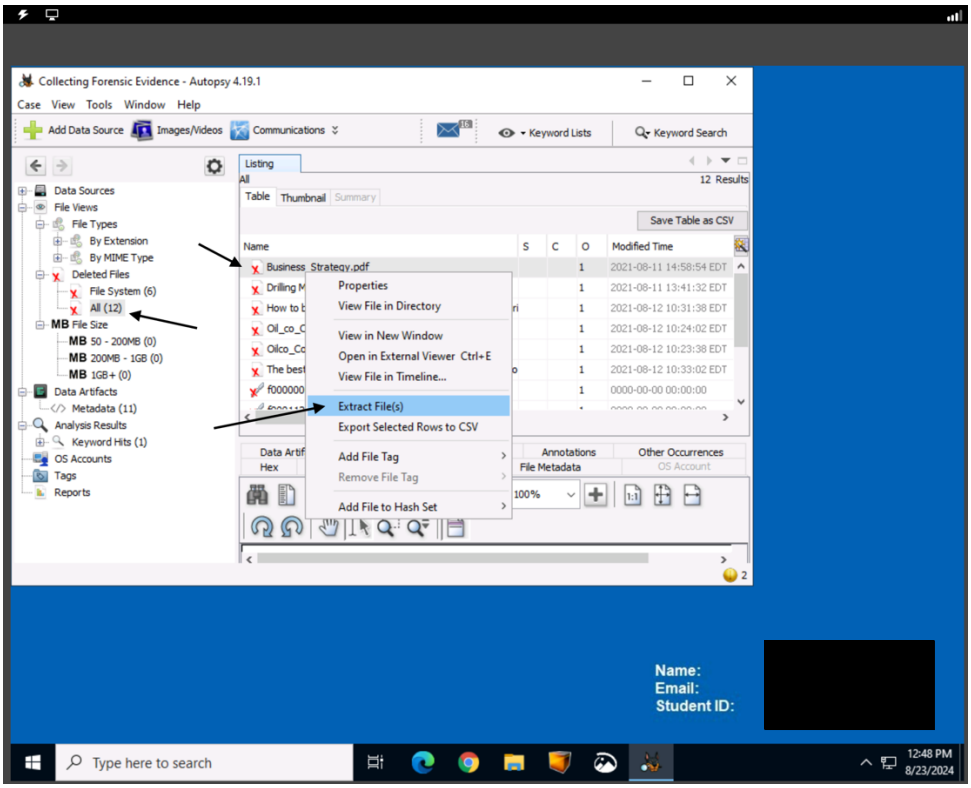


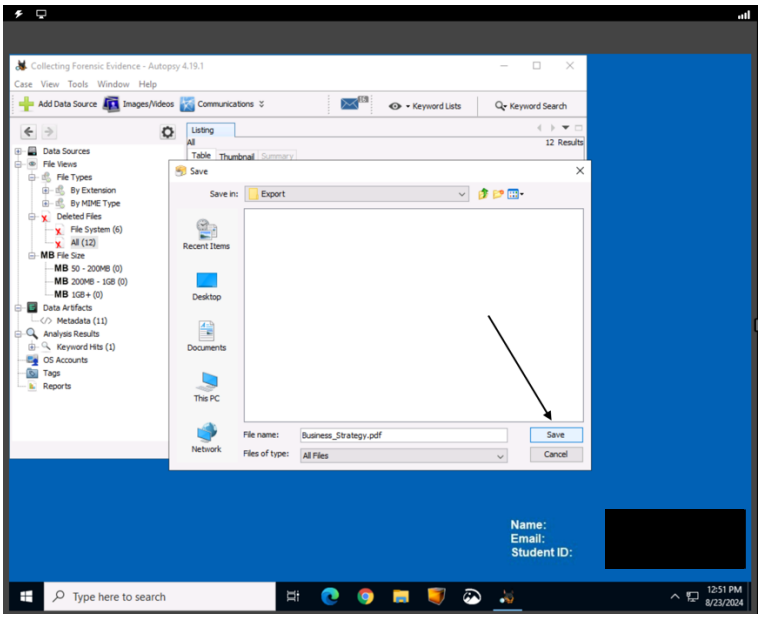
Step 9: Add Data Source, when you see the message **“Data source has been added to the local database. Files are being analyzed”**, click on **Finish**



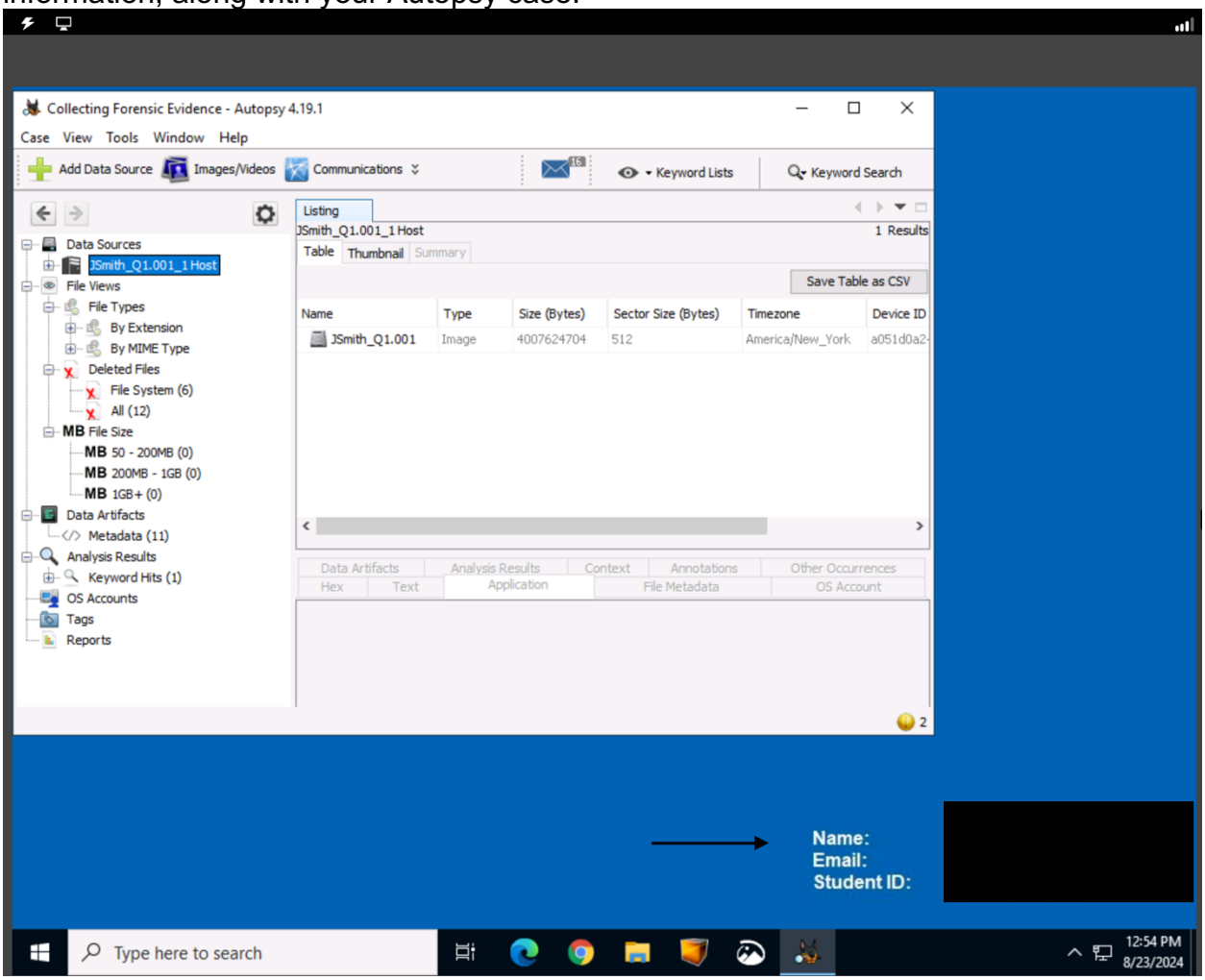
A2. Describe *all steps* taken in Autopsy to identify potential evidence including data files, deleted data files, directories, or drive partitions. Provide screenshots of these steps.

Step 1: While performing analysis. **Right click** on a file name select **Extract File(s)** and save the files to the **Export Folder**, **C:\Users\LabUser\Desktop\Evidence Files\Example\Export**



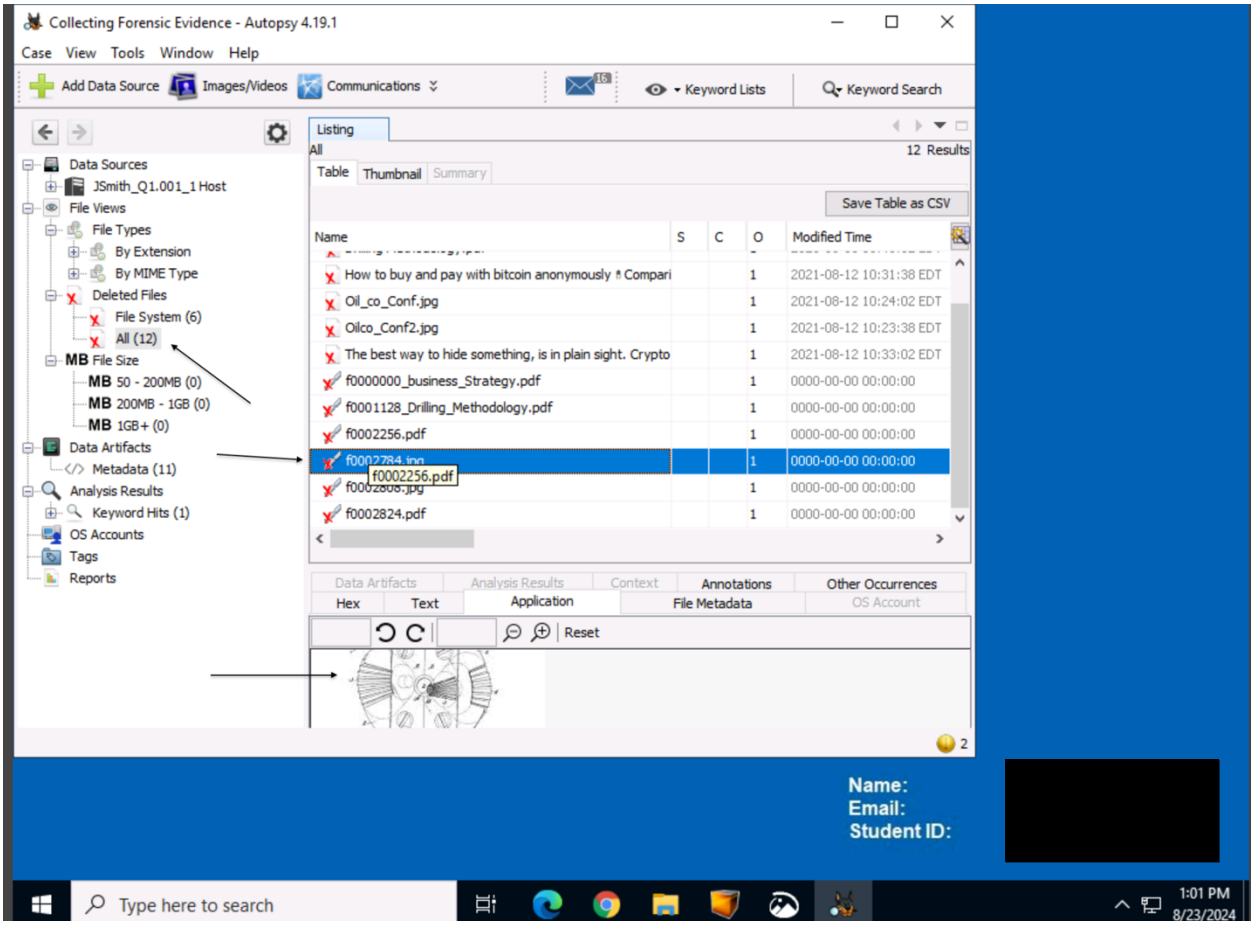


Step 2: For this task, you will need to take a screenshot that includes your student information, along with your Autopsy case.



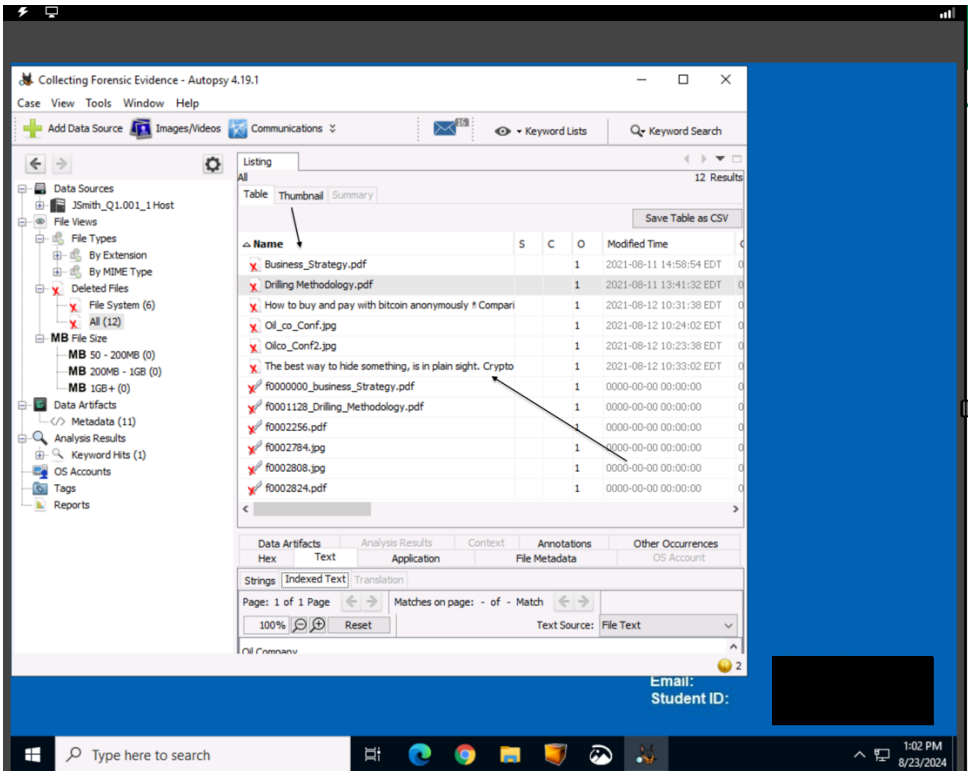
A3. Summarize the findings you identified during your investigation and the conclusions you made regarding the suspect and the collected evidence. Provide screenshots from Autopsy or reports to support your findings and conclusions.

Analysis 1: During analysis using Autopsy, this displays the deleted files in John Smith's hard drive along with the unauthorized access of proprietary images of the oil company's machinery and its functions, violating the company's AUP.



Analysis 2: During analysis using Autopsy, it was discovered John Smith's hard drive contained Deleted Files with the Company's proprietary Business_Strategy.pdf and Drilling Methodology.pdf. These files are identified as the Company's proprietary information. The analysis also revealed evidence of John Smith performing steganography. This technique is used to hide or embed messages into images, videos, or files within a file. This can be used to send the proprietary information in plain sight via email violating the Company's NDA and AUP. These implications provide evidence that John Smith had unauthorized access and attempted to conceal sensitive company information.

Screenshot 1



Analysis 2:

Screen shot 2