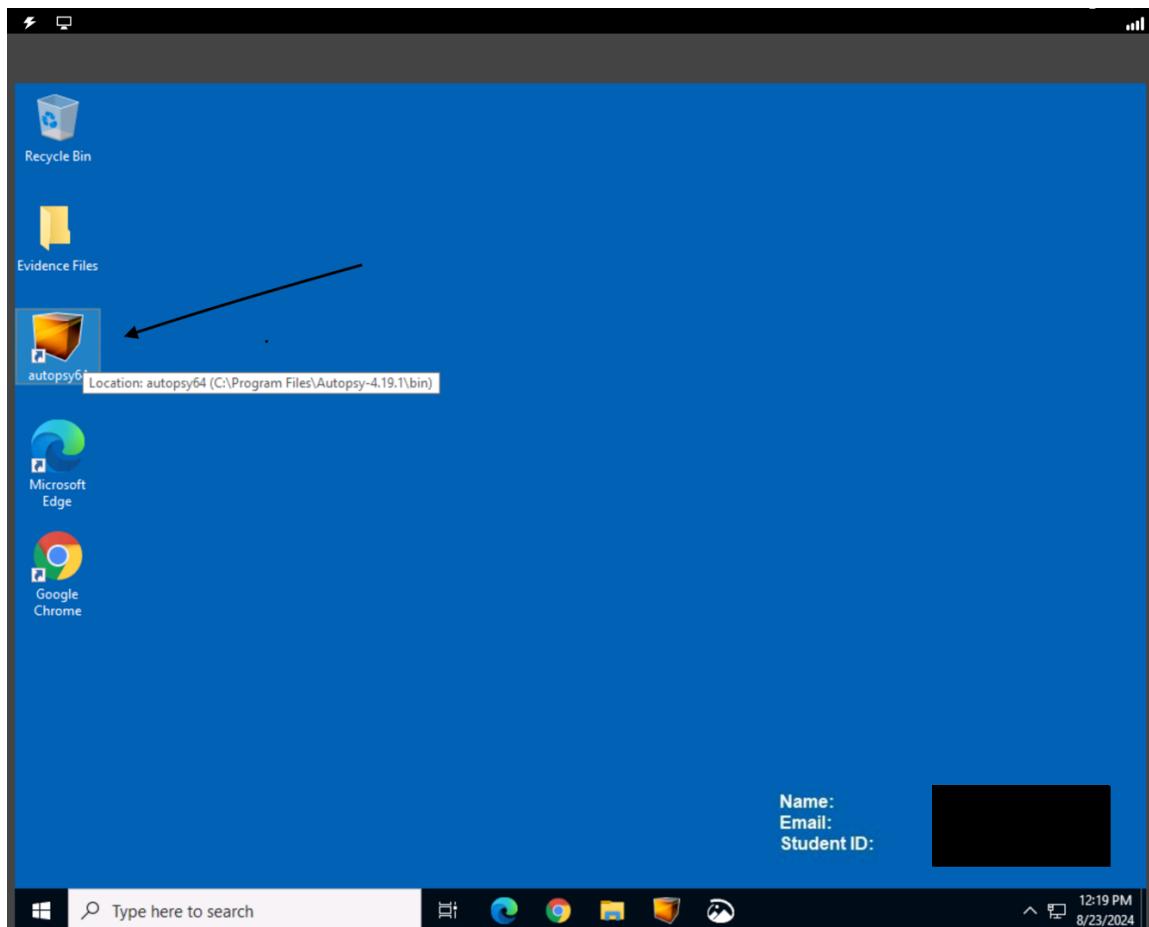


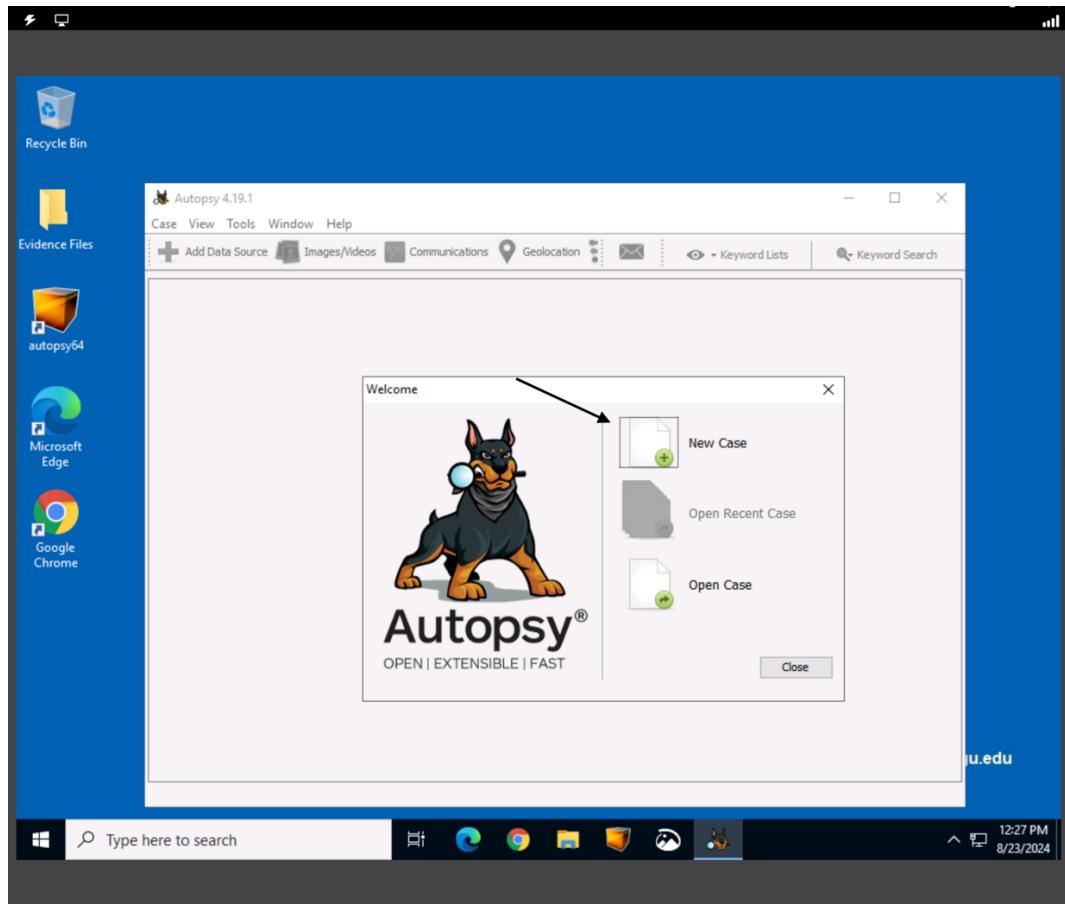
A. Write a report for the team of investigators by doing the following:

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

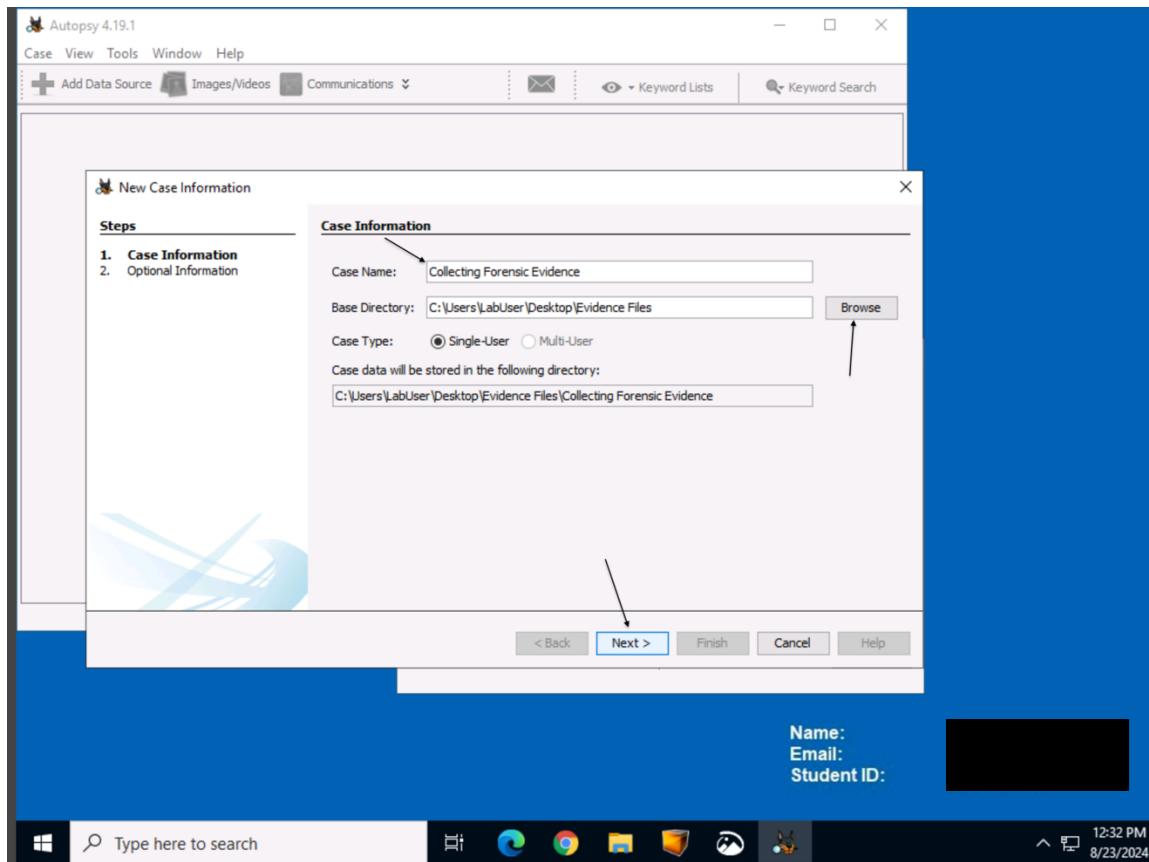


Step 2: Select new case file in Autopsy

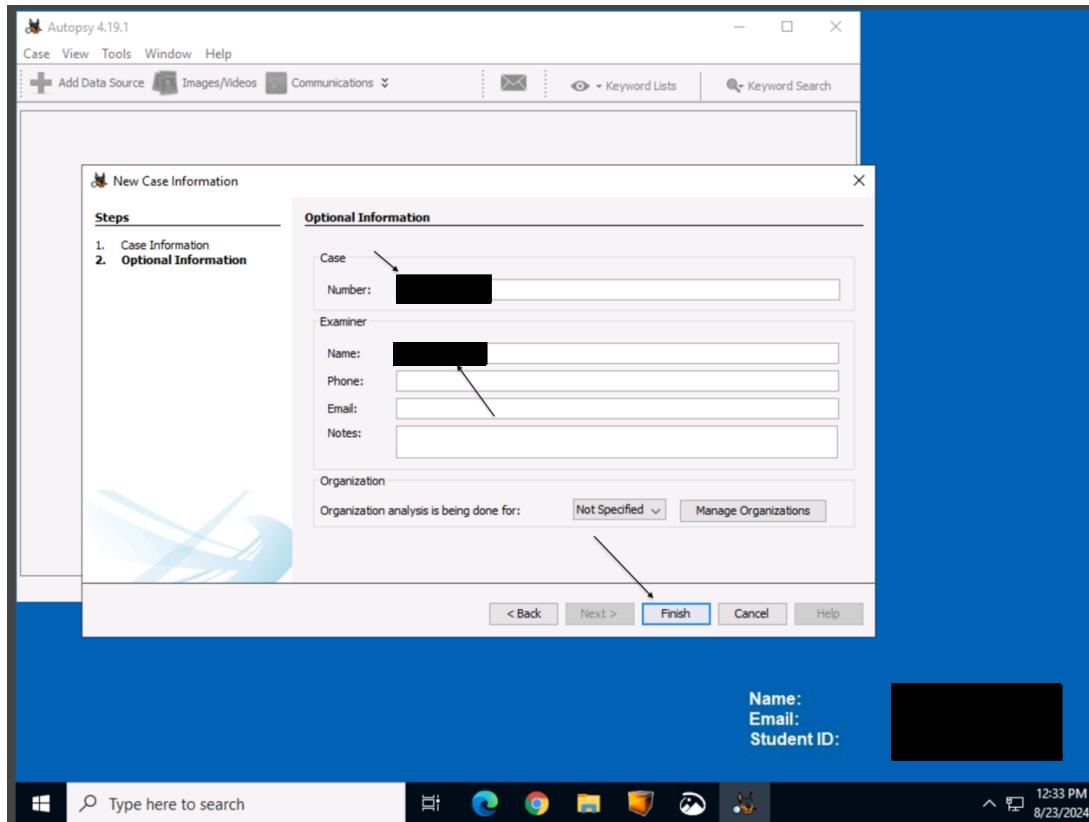


Step 3: The new case wizard dialog box opens.

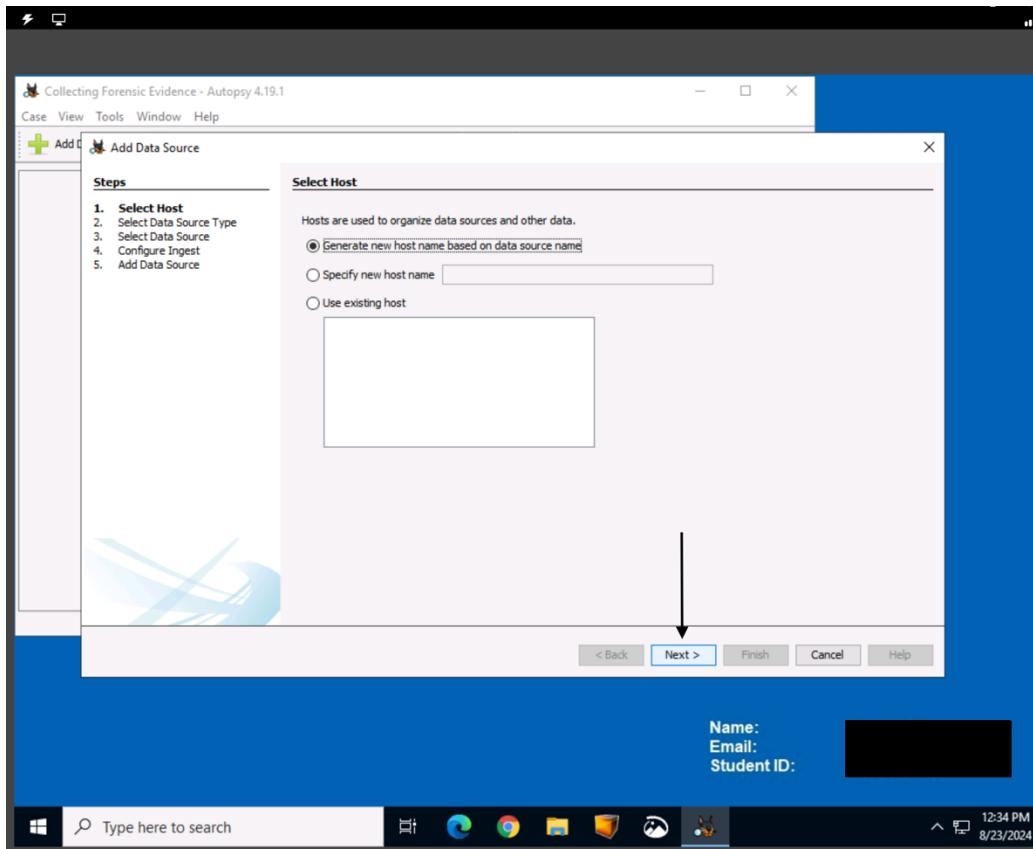
Enter the **Case Name** (Collecting Forensic Evidence) and enter a **Base Directory** using the browse button: **C:\Users\LabUser\Desktop\Evidence Files**. Then click on **Next**



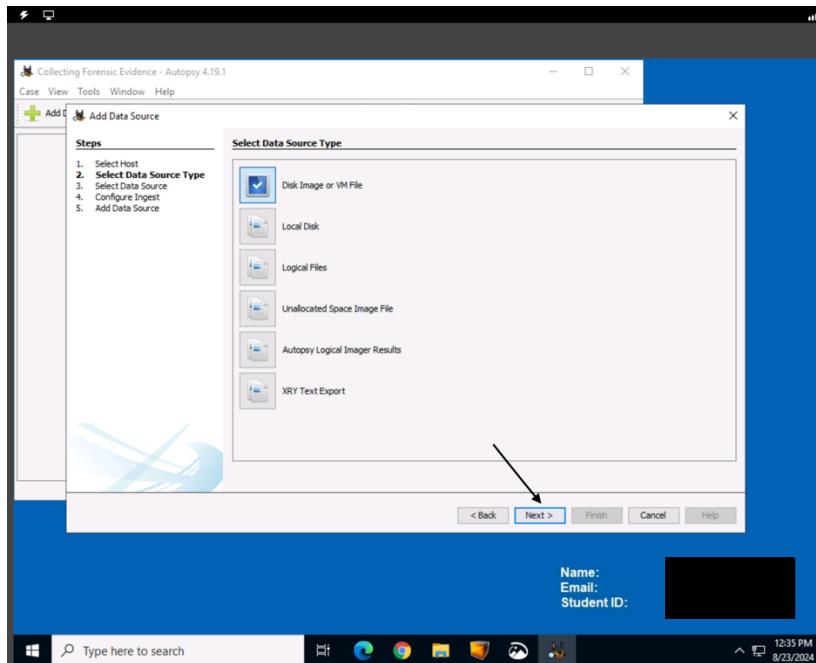
Step 4: Add Case Number = your Student ID and Add Name = your Student ID, then click on Finish



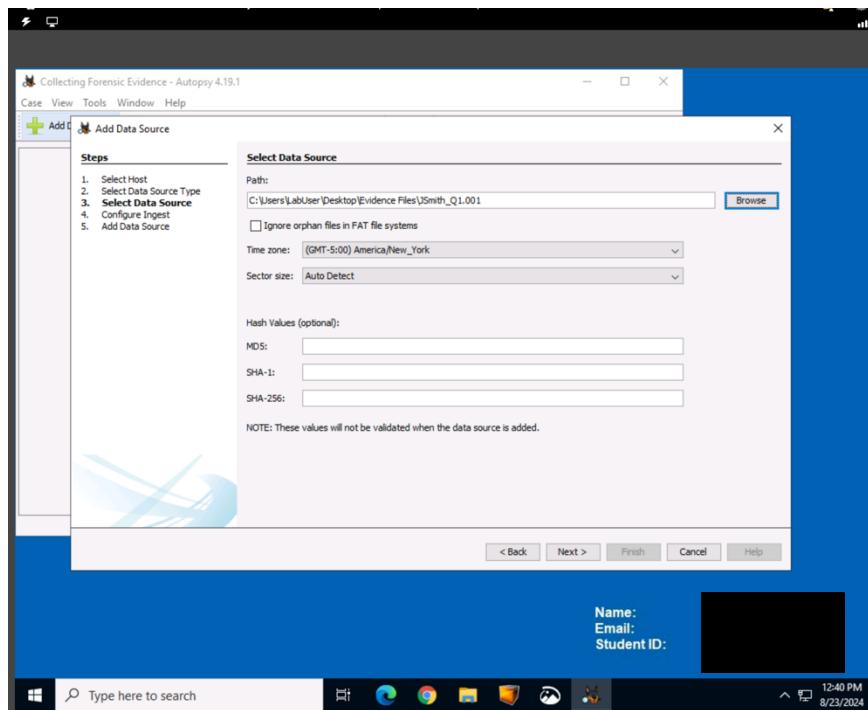
Step 5: Select Host, accept the default settings and click **Next**



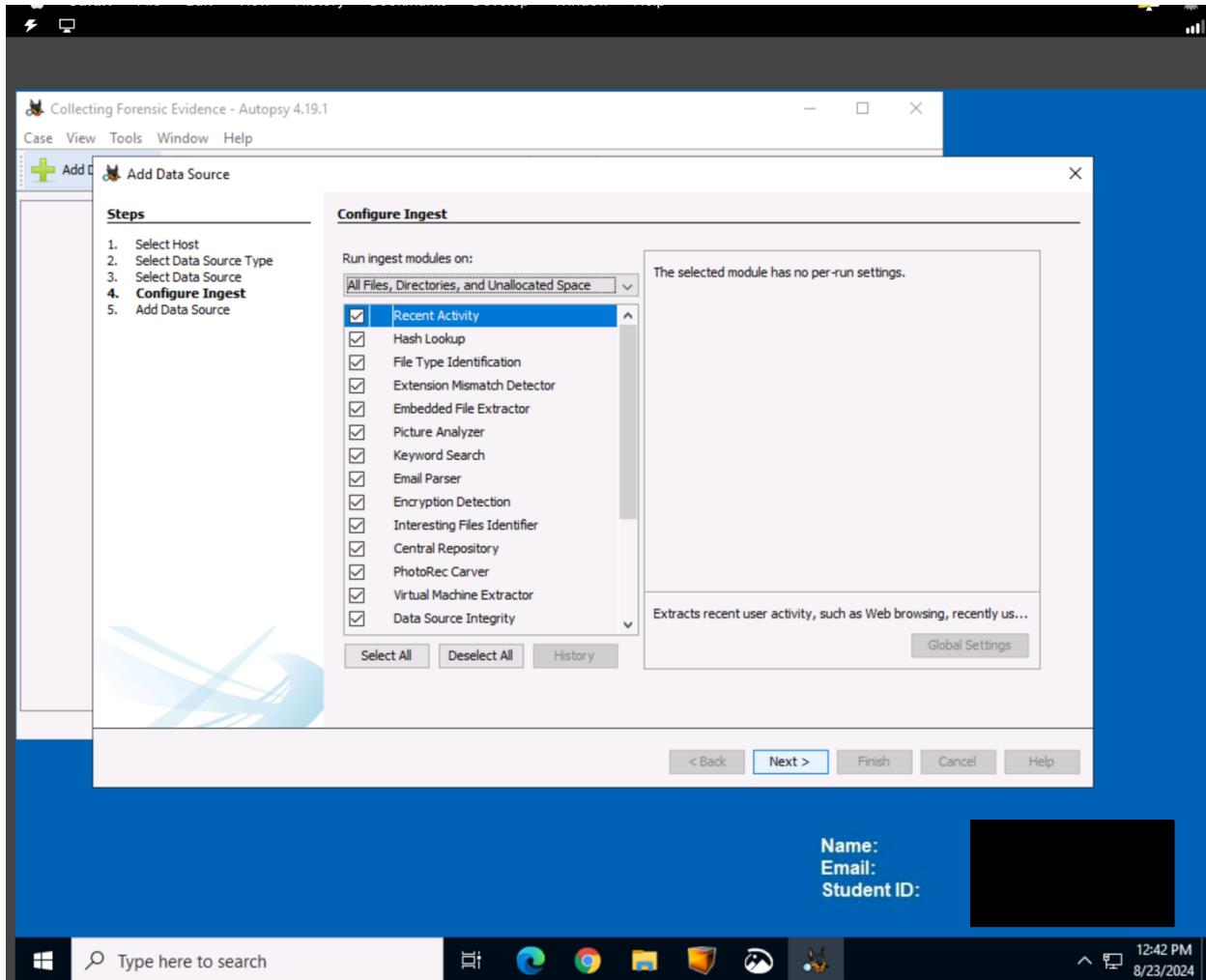
Step 6: Select the data source type, Disk Image or VM file and click Next



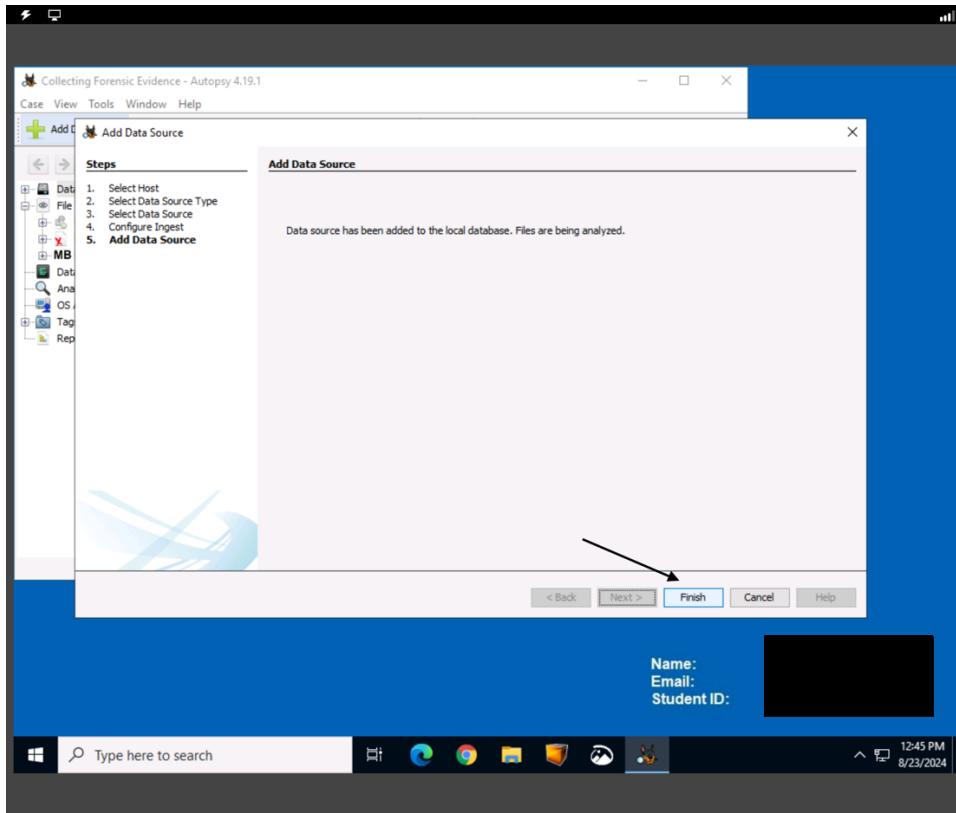
Step 7: Select Data Source path, browse to: C:\Users\LabUser\Desktop\Evidence Files\JSmith_Q1.001 and Select Data Source accept defaults, Next



Step 8: Configure Ingest, accept defaults, Next

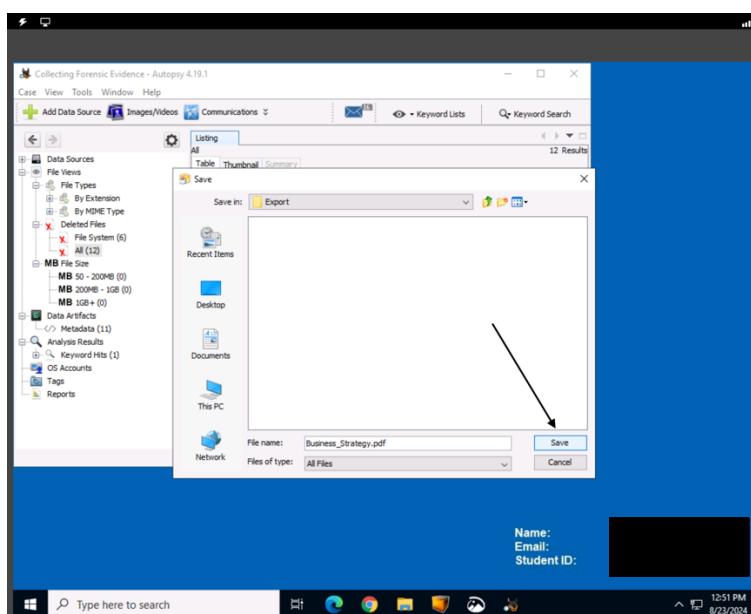
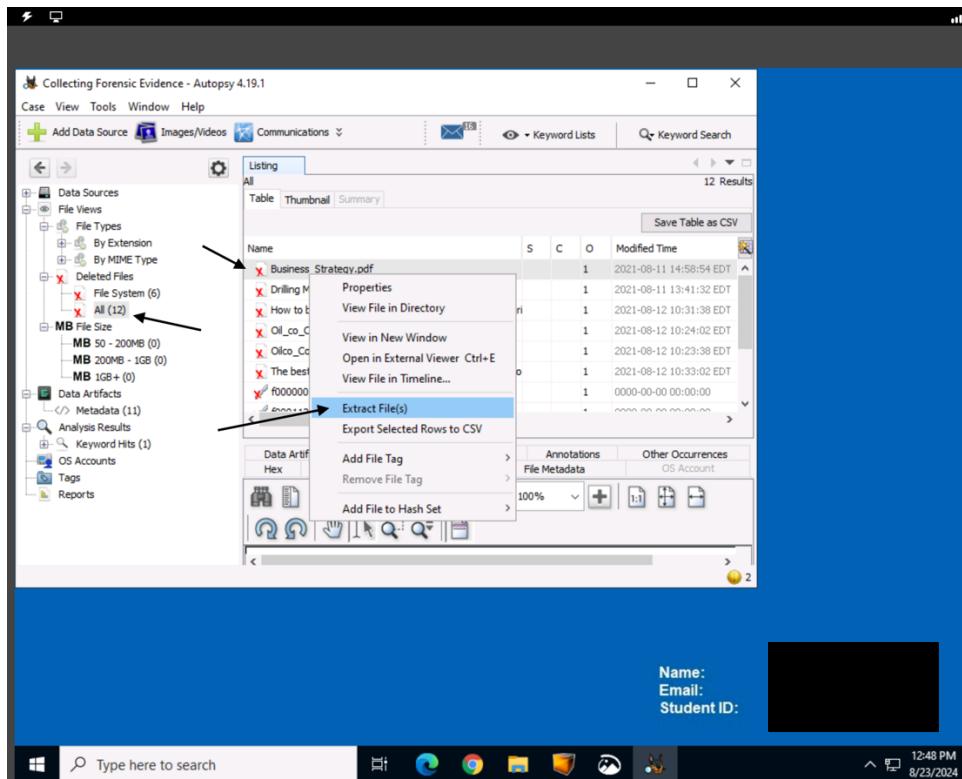


Step 9: Add Data Source, when you see the message “Data source has been added to the local database. Files are being analyzed”, click on **Finish**

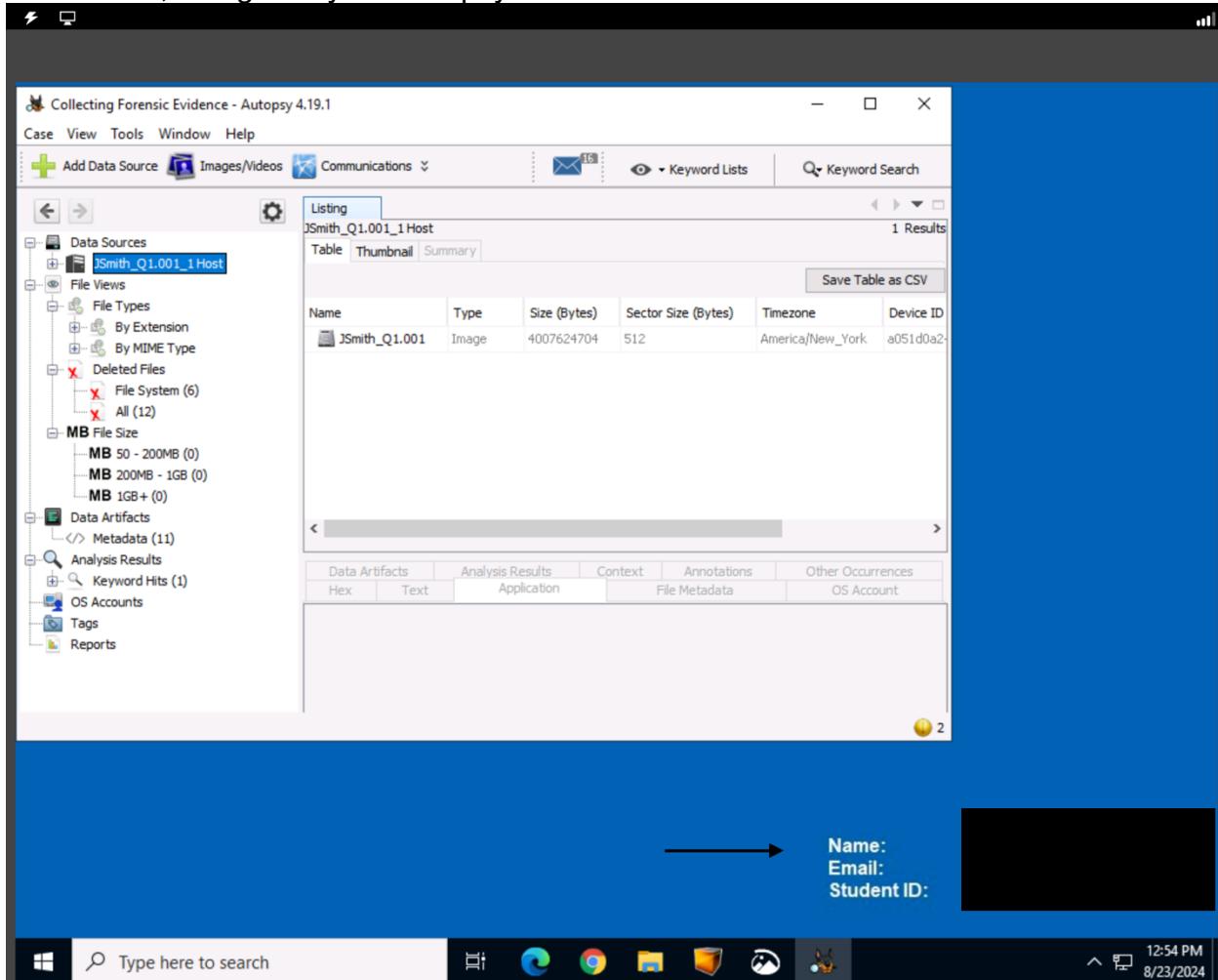


A2. Describe all steps taken in Autopsy to identify potential evidence including data files, deleted data files, directories, or drive partitions. Provide screenshots of these steps.

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.

The screenshot shows the Autopsy 4.19.1 interface. The left sidebar shows a tree view of data sources, file types, and file sizes. The main pane displays a table of deleted files with columns for Name, S, C, O, and Modified Time. One file, 'f0002784.inn', is selected. Below the table, there are tabs for Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The Data Artifacts tab is active, showing a preview of the selected file which appears to be a complex diagram or image of an industrial machine, possibly a pump or compressor. At the bottom right, there is a form for entering student information: Name, Email, and Student ID, with a placeholder 'Name:' and a redacted area for 'Email:' and 'Student ID:'.

Name	S	C	O	Modified Time
How to buy and pay with bitcoin anonymously & Compari	1			2021-08-12 10:31:38 EDT
Oil_co_Conf.jpg	1			2021-08-12 10:24:02 EDT
Oilco_Conf2.jpg	1			2021-08-12 10:23:38 EDT
The best way to hide something, is in plain sight. Crypto	1			2021-08-12 10:33:02 EDT
f0000000_business_Strategy.pdf	1			0000-00-00 00:00:00
f0001128_Drilling_Methodology.pdf	1			0000-00-00 00:00:00
f0002256.pdf	1			0000-00-00 00:00:00
f0002784.inn	1			0000-00-00 00:00:00
f0002256.pdf	1			0000-00-00 00:00:00
f0002808.jpg	1			0000-00-00 00:00:00
f0002824.pdf	1			0000-00-00 00:00:00

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

The screenshot shows the Autopsy 4.19.1 interface. The left sidebar displays a tree view of the data source structure, including Data Sources (JSmith_Q1.001_1 Host), File Views (File Types, Deleted Files, MB File Size), Data Artifacts (Metadata, Analysis Results, Keyword Hits), OS Accounts, Tags, and Reports. The main pane shows a table of deleted files with the following data:

Name	S	C	O	Modified Time
Business_Strategy.pdf	1			2021-08-11 14:58:54 EDT
Drilling Methodology.pdf	1			2021-08-11 13:41:32 EDT
How to buy and pay with bitcoin anonymously * Compari	1			2021-08-12 10:31:38 EDT
Oil_co_Conf.jpg	1			2021-08-12 10:24:02 EDT
Oilco_Conf2.jpg	1			2021-08-12 10:23:38 EDT
The best way to hide something, is in plain sight. Crypto	1			2021-08-12 10:33:02 EDT
f0000000_business_Strategy.pdf	1			0000-00-00 00:00:00
f0001128_Drilling_Methodology.pdf	1			0000-00-00 00:00:00
f0002256.pdf	1			0000-00-00 00:00:00
f00022784.jpg	1			0000-00-00 00:00:00
f0002808.jpg	1			0000-00-00 00:00:00
f0002824.pdf	1			0000-00-00 00:00:00

Annotations: The table has two annotations. One arrow points to the 'Name' column header, and another points to the first row of the table.

Bottom status bar: Email: [REDACTED] Student ID: [REDACTED]

Analysis 2:

Screen shot 2

