Quinton Green

DIGITAL FORENSICS IN CYBERSECURITY — D431

TASK 2: FORENSIC INVESTIGATION

**Run Autopsy:**

A screenshot of a computer

Description automatically generated

**Create a new case:**

A screenshot of a computer

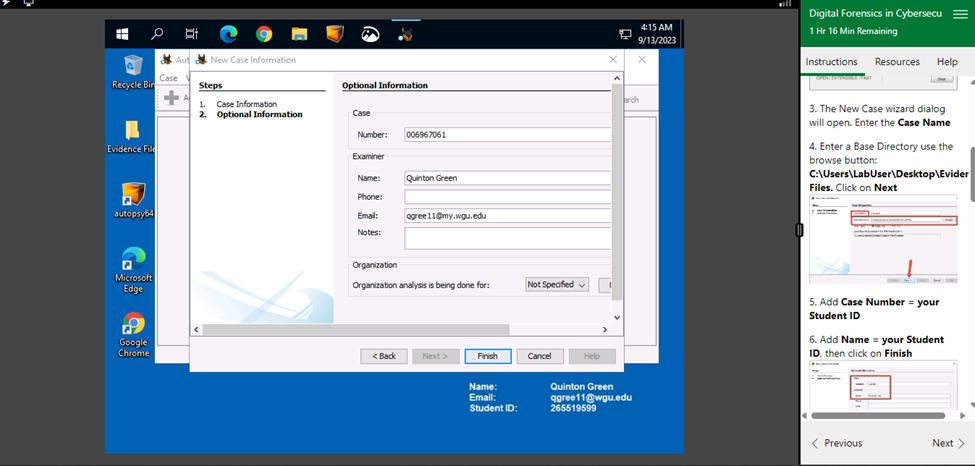
Description automatically generated

**The New Case wizard dialog will open. Enter the Case Name and Enter a Base Directory use the browse button: C:\Users\LabUser\Desktop\Evidence Files. Click on Next**

A screenshot of a computer

Description automatically generated

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

****

**Select Host**, accept the default settings and click **Next.**

A screenshot of a computer

Description automatically generated

Select the **data source type**, in this case **Disk Image or VM file** and click **Next.**

A screenshot of a computer

Description automatically generated

Select **Data Source path**, browse to: **C:\Users\LabUser\Desktop\Evidence Files\JSmith\_Q1.001 and** Select **Data Source** accept defaults, **Next.**

A screenshot of a computer

Description automatically generated

**Configure Ingest,**accept defaults, **Next.**

A screenshot of a computer

Description automatically generated

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

A computer screen shot of a computer

Description automatically generated

**Begin your analysis.**

A screenshot of a computer

Description automatically generated

While doing your 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**

**A screenshot of a computer

Description automatically generated**

**Viewing all deleted data files that were extracted.**

**A screenshot of a computer

Description automatically generated**

**View image files that were extracted:**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**View image files:**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**Viewing documents and finding 11 PDFs**

A screenshot of a computer

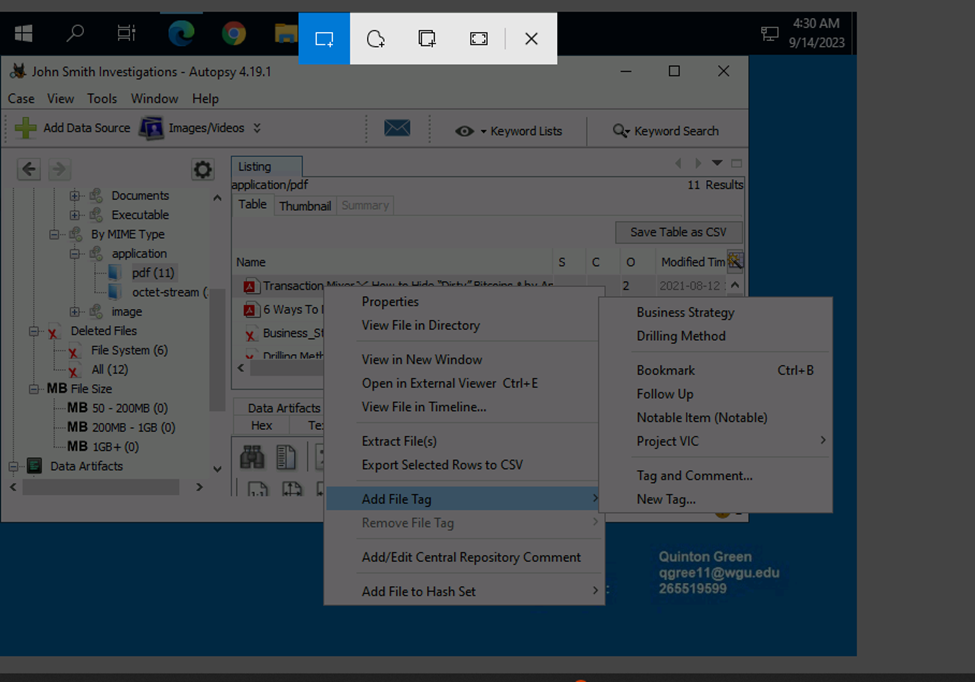
Description automatically generated

**Viewing Executable files**

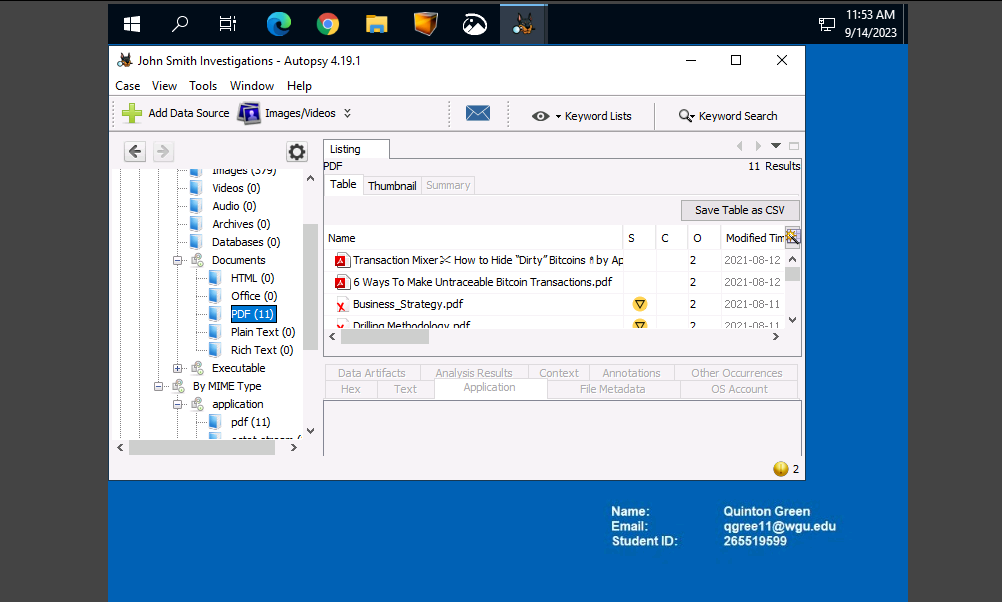
**A computer screen shot of a computer

Description automatically generated**

**Generate Report by adding tags to the files included in the report.**

****

**Viewing Tagged files**

****

**Go to Tools in the top taskbar and then to Generate Report**

**A screenshot of a computer

Description automatically generated**

**In Select and configure report Modules select: HTML Report click next  
A screenshot of a computer

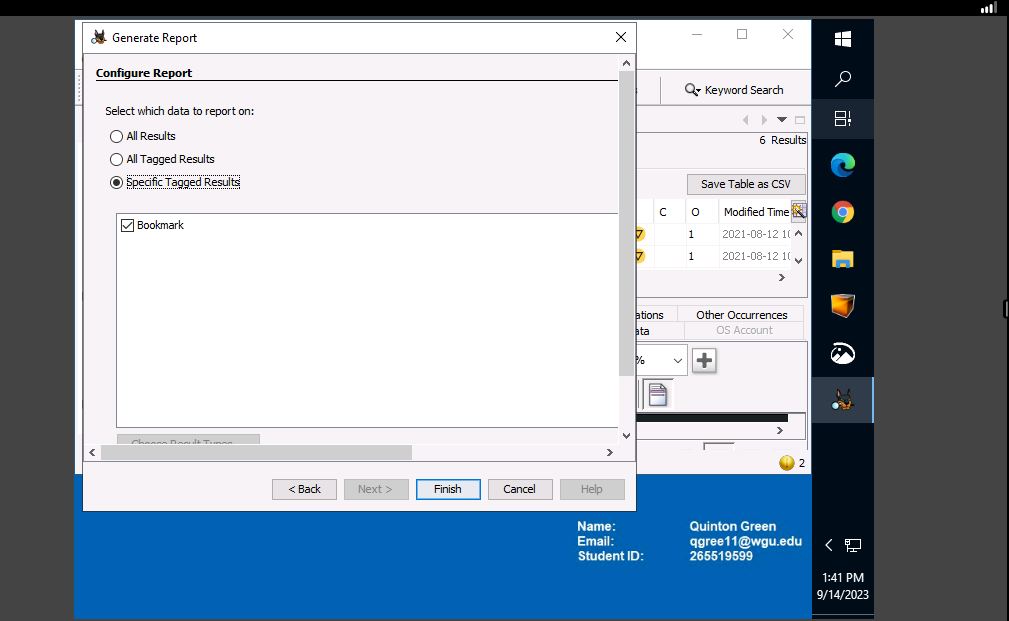
Description automatically generated**

**Select which data sources to include, File JSmith\_Q1.001 should be checked and click next.**

**A computer screen with a white screen

Description automatically generated**

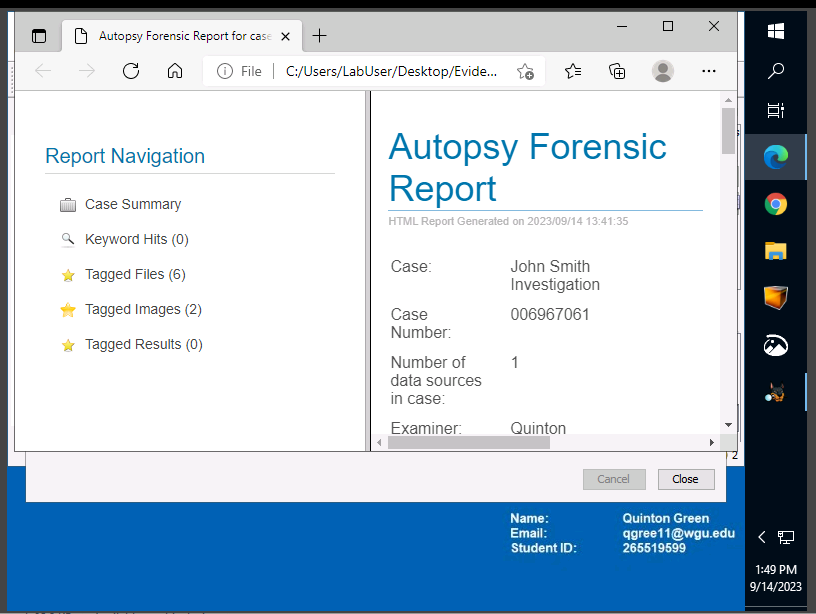
**In Configure report select Specific Tagged Results. The Bookmark option should automatically be checked. Click Finish**

****

**The report Generation progress will show Complete with an HTML link to view.**

**A screenshot of a computer

Description automatically generated**

**To View report, click the HTML Link and Autopsy Forensic Report will populate  
**

**Summary:**

**There were found 379 images files: 36 jpg and 343 png. files with blurred and distorted images. There is a possibility of the blurred /distorted images containing steganography but would need further analysis for anomalies. There were 8 files showing drilling schematics and the reverse osmosis process, 11 pdf documents consisting of the Oil Company data strategy, drilling methodology, business strategy, how to buy and pay with bitcoin anonymously, 6 ways to make bitcoin transactions untraceable, how to hide “dirty” bitcoins, the best way to hide something in plain sight: Crypto laundering. There were no files found in the directories or drive partitions, but the files found were in the deleted folder. In conclusion the alleged employee showed an interest in hiding information and partaking in the bitcoin transactions and was privy to the files stated above and deleted the information he viewed. Senior management and the legal office can view this report and its finding to determine the next steps and course of action.**