Forensics Recovery Procedures

A1. I double clicked the icon “autopsy64”.

A picture containing treemap chart

Description automatically generated

I selected the icon within Autopsy “New Case”.Graphical user interface, application, website

Description automatically generated

I began John Smith’s case by first accessing Autospy in the virtual server and naming the case “John Smith”.

Graphical user interface, text, application, email

Description automatically generated

I added my student ID for the case number and name fields and created the case. Graphical user interface

Description automatically generated

Next, I selected the host and the default settings. Graphical user interface, application

Description automatically generated

I selected the data source type as “Disk Image or VM File”. Graphical user interface, text, application

Description automatically generated

I selected the “JSmith\_Q1.001” file located in “Evidence Files” as the data source. Graphical user interface, text, application

Description automatically generated

I selected the default settings for configure ingest.Graphical user interface, text, application

Description automatically generated

Once the data source was added, I clicked the Finish button.Graphical user interface, text, application

Description automatically generated

A2. I started gathering evidence by using the keyword search tool first searching “Confidential”.Graphical user interface, text, email

Description automatically generated

I next searched for “Proprietary”.

Graphical user interface, text, application, email

Description automatically generated

The results of these searches show John Smith accessed files he does not have authorization to view.

The file “Drilling Methodology” should not be of interest to a mechanical engineer. Graphical user interface, text, application, Word

Description automatically generated

The file “The best way to hide something…” shows John Smith was researching ways to conceal information.

Graphical user interface, application

Description automatically generatedThe searches for untraceable Bitcoin transactions also shows he may have been leaking proprietary and confidential files in exchange for Bitcoin.

Graphical user interface, text, application, email

Description automatically generated

He also attempted to delete the files, presumably to try to hide that he accessed the files. This shows he knew he was doing something that was wrong and did not want it to be known.

Graphical user interface, text, application, email

Description automatically generated

A3. The evidence shows John Smith violated company polices, the NDA, and AUP polices. The documents show John Smith accessing files he did not have authorization to view along with files showing bitcoin payments and how to hide them. It is possible he was going to leak or already has leaked the documents for Bitcoin payment.