**BFN2 TASK 2: FORENSIC INVESTIGATION**

Open and run Autopsy by clicking on the **autopsy64** icon on your desktop.

A logo of a software company

Description automatically generated

Once the Welcome menu has opened you will select **New Case**.

A screenshot of a computer

Description automatically generated

New Case Information window is open and select the Browse button next to Base Directory.

Then browse to folder **C:\Users\LabUser\Desktop\Evidence Files** and click on the **Select** button.

A screenshot of a computer

Description automatically generated

The Base Directory will have the following location: **C:\Users\LabUser\Desktop\Evidence Files**.

A screenshot of a computer

Description automatically generated

Enter student ID – XXXXXXXXX for **Case Name**, then click **Next**.

A screenshot of a computer

Description automatically generated

In the Optional Information window Enter student ID – XXXXXXXXX for **Number** under **Case**.

Include your **Name** under the Examiner option, then click on **Finish**.

A screenshot of a computer

Description automatically generated

Add Data Source window will open and for **Select Host**, accept the default settings and click **Next**.

A screenshot of a computer

Description automatically generated

For **Select Data Source Type**, select **Disk Image or VM File**, then click on **Next**.

A screenshot of a computer

Description automatically generated

Then select Browse to **Path:** **C:\Users\LabUser\Desktop\EvidenceFiles\JSmith\_Q1.001**

**Select Data Source** accept the defaults and click on **Next**.

A screenshot of a computer

Description automatically generated

**Configure Ingest** accept the defaults then click on **Next**.

A screenshot of a computer

Description automatically generated

The Add Data Source window will open with the message “Data source has been added to the local database. Files are being analyzed.” Then click on **Finish**.

A screenshot of a computer

Description automatically generated

Once that is done the following window is displayed, and we can begin the analysis.

A screenshot of a computer

Description automatically generated

When investing a file, Right-click on the file name to Extract File(s) and save the file to the Export Folder, **C:\Users\LabUser\Desktop\EvidenceFiles\Example\Export.** From this folder, we can open saved files and investigate them closely.

A screenshot of a computer

Description automatically generated

We will begin our investigation from the data and evidence collected under **Data Sources**, and we can expand all files. We can then navigate to folder **JSmith\_Q1.001\_1 Host** and expand **JSmith\_Q1.001** to list all files.

A screenshot of a computer

Description automatically generated

By selecting the Thumbnail tab, we can see .jpg files accessed by John Smith.

A screenshot of a computer

Description automatically generated

The summary tab displays more information about the file types in a pie chart.

A screenshot of a computer

Description automatically generated

We can then move to the folder **$CarvedFiles (6)** and notice a few files saved by John Smith. The first file is listed as **f0000000\_bunsiness\_Strategy.pdf** with the title Oil Company CONFIDENTIAL Restricted Business Strategies 2021 file.

A screenshot of a computer

Description automatically generated

There was also another file **f0001128\_Drilling\_Methodolgy.pdf** with the title Oil Company CONFIDENTIAL Restricted Oil Strategies 2021 Field 007-A file.

A screenshot of a computer

Description automatically generated

As we open the file **f0002256.pdf** we notice the title How to buy and pay with bitcoin anonymously.

A screenshot of a computer

Description automatically generated

The file **f0002824.pdf** has information with the title The best way to hide something, is in plain sight. Crypto laundering. To view the whole article, you can right-click on the file name and Extract File to the Evidence Folder to view the entire article.

A screenshot of a computer

Description automatically generated

We can then move to the folder **$Unalloc (4)** to investigate those findings. We noticed that the file name **Unalloc\_4\_12656640\_1087102976** has a mark on it so we right-click and open properties to investigate further.

A screenshot of a computer

Description automatically generated

On **S**, it **Has an Likely Notable analysis result score** so we will investigate further.

A screenshot of a computer

Description automatically generated

Then we move to the **Analysis Results** tab.

A screenshot of a computer

Description automatically generated

If we move down to the **File Views**, and **File Types** and expand to **Documents** and **PDF** **(11)** it will also give us more results to investigate.

A screenshot of a computer

Description automatically generated

When we can see a suspicious file name titled **6 Ways To Make Untraceable Bitcoin Transactions.pdf** (75) under the **Application** tab.

A screenshot of a computer

Description automatically generated

Then open the **File Metadata** tab and name verifies the pdf is from John Smith.

A screenshot of a computer

Description automatically generated

If we move down to Data Artifacts then Metadata (11). This will show that the owner of the files was Mike Morris.

A screenshot of a computer

Description automatically generated

We can also see in the **Data Artifacts** where the Source File Path was saved by John Smith.

A screenshot of a computer

Description automatically generated

If we select the **Timeline** and select the **Details** tab it will give us information on the system usage and the list of forms and files accessed by John Smith.

A screenshot of a computer

Description automatically generated

If we moved to the **List** tab it will also give us a list of files in Date and Time and a description of each file.

A screenshot of a computer

Description automatically generated

Lastly, we can run an Autopsy Forensic Report with the following results.

A screenshot of a computer

Description automatically generated

A screen shot 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

We can conclude that John Smith did access confidential files that were against company policy and unauthorized to proprietary information. After running our tool for the investigation, we can see that files for the plans on fuel cell technology and diagrams explain how it can work. This would bring significant profits to the oil company and beat other competitors. This is why these plans should not be shared externally and steal their ideas. Other files explain the proprietary methods of drilling and risk of competitors learning the methodology and steps used in the location based on soil conditions. This should also be kept confidential and not leaked to another competitor. John Smith has visited sites on How to buy and pay with Bitcoin anonymously which draws a red flag on his intentions. Along with other findings was a file The best way to hide something, is in plain sight Crypto laundering explaining how easy it is to do Bitcoin transactions. These files were deleted but uncovered by Autopsy and the Owner of the files was Mike Morris. The Autopsy Forensic Report gives a summary of what was accessed by John Smith and the URLs websites along with dates and times.