Aim: File system Analysis using The Sleuth kit.

Step 1: Open **Autopsy 3.12** and Click on **Create New Case**

Step 2: Within **Enter New Case Information** Type Case Name **(Here it is CyberForensic)** and **Click on Browse** and Select **Base Directory** and **Click on Next**

Step 3: Within **Additional Information Set Case Number and Examiner** Here it is **Case Number 001** And **Examiner Name Rahul Kewat** and **Click on Finish**

Step 4: The next step in the investigation will be to add an image file to the case. Within **Enter Data Source Information Select source type to add: Here we select Image File** and **Click on Browse**

• After **Click on Browse** Select **evidance1.dd Click on Open**
• **Click on Next**

Step 5: In **configuration Ingest Modules Keep Default Setting** and **Click on Next**

Step 6: Click on Finish

Step 7: It Analyzing the Files From evidence 1.dd

Step 8: Expand the Data Source there is one Hard Drive under Data Source Called evidence 1.dd by selecting evidence 1.dd we can see file structure or files in main view in the main view we can see the
file name special attribute modified time change time access time.

Step 9: After the image is indexed the tree will be populated by the file system, extracted content, keyword searches, and the hash list (if any were used). the investigator should generate a report. This will allow the investigator to have an idea of what type of information is available and what to expect.
The report can be generated in three formats: Excel, XML, and HTML.

• **Click on Generate Report**
• **Select Result-HTML** and **Click on Next**
• **Select All Results** and **Click on Finish**
• Report Generation in Progress After Completion Click on Given link to view the Report
• Report Generated

Step 10: View image detail

• **Right-Click on evidence 1.dd** and **Select image Details**
• **Here we can see Image Information**