Aim: Using Forensic Toolkit (FTK) &Writing report using FTK (AccessData FTK).

Step 1: Open **AccessData FTK 1.81.0 DEMO VERSION** and **Click on Start a new case** and **Click** on **OK**
Step 2: Type **Investigator Name** and **Case Number, Case Name** and **Set** the **Case Path** and **Click on Next**
Step 3: Keep Default Setting and **Click on Next**
Step 4: Keep Default Setting and **Click on Next**
Step 5: Select Data Carve and **Registry Report** and **Click on Next**
Step 6: Keep Default Setting and **Click on Next**
Step 7: Click on Add Evidence Within Type of Evidence to Add to Case Select Acquired Image of Drive and Click on Continue

- **Within Add Evidence Select evidence 1.dd and click on open**
- **Click on OK**
- **Click on Next**
- **Click on Finish**
- It Start the Processing Files

Step 8: Data Carving Files in an Existing Case

- **Select Tools,** and then **Data Carving.**
- **Select BMP Files, GIF Files,** and **PNG Files** and **Click on OK**
- It Will Start Carving BMP Files
- After Carving BMP Files It Will Start Carving GIF Files
- After Carving BMP and GIF Files and then Next It Will Start Carving PNG Files
- After Carving BMP and GIF, PNG Files and then Next It Will Start Initializing the list
- After Initializing the list Here, We Can See the **Data Carving Results**

Step 9: Modifying or Creating a Filter

- **Select View,** and then **File Filter Manager**
- Select the filter that you want to modify
- If you are modifying an existing filter, **click Save/Apply.** Or If you are creating a new filter, **click Save As,** enter the name, and **click OK.**

Step 10: Deleting a Filter

- You can delete a filter if you no longer need it. To delete a filter:
- **Select View**, and then **File Filter Manager.**
- **Click Delete**
- Deleted Files

Step 12: Searching the Registry

- **Launching Registry Viewer** as a Separate Application:
- To run Registry Viewer as a separate application, select Start, then Programs, then AccessData, and then Registry Viewer, and then Registry Viewer
- Launching Registry Viewer from FTK:

- To run Registry Viewer from FTK:
- In FTK, open an existing case by selecting File, and then Open Case.
- Or if you have chosen to always display the FTK Startup screen, select Open an Existing Case and click OK
- **Select** the case you want to open.
- **Select File,** and then **Registry Viewer** to **open Registry Viewer.**
- (Can't perform ahead of this step because Registry viewer is disabled in demo version)

Step 13: Obtaining Protected **Registry Files** Using **FTK Imager**

- To obtain the protected **registry files** using **FTK Imager:**
- **Launch FTK Imager.**
- **Click File,** and then Obtain **Protected Files**
- Select the destination folder **(Here it is 001-2024)** and **Click on OK**
- **Under System Files Options Select Password recovery and all registry files and Click on OK**
- **Scanning MFT**

Step 14: Generating a Report

- From the menu, **select Report**, and then **Generate Report** or **click the button on the toolbar**
- **Click on OK**
- Under **Case Information** Enter Following Information **and Click on Next**
- **Keep the Default Setting** and **Click on Next**
- **Keep the Default Setting** and **Click on Next**
- **Keep the Default Setting** and **Click on Next**
- **Click on Next**
- **Click on Next**
- **Click on Add Files and Select the Supplementary Files and Click on Next**
- **Click on Finish**
- **Click on OK**
- **Generated Report**
- **File Overview**
- **Evidence List**