**Detailed Project Report**

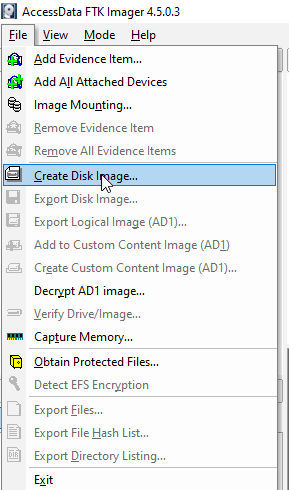
**Create image using FTK Imager**

**FTK Imager is an open-source software by AccessData that is used for creating accurate copies of the original evidence without actually making any changes to it.**

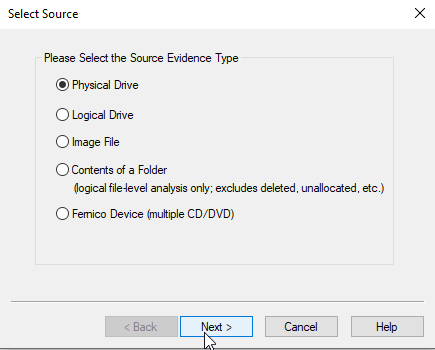
**Steps :**

**1.Open FTK Imager with admin privileges(Run as administrator)**

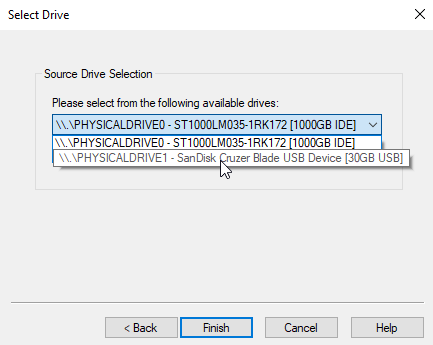
**2.Open file and select “Create disk image”**

****

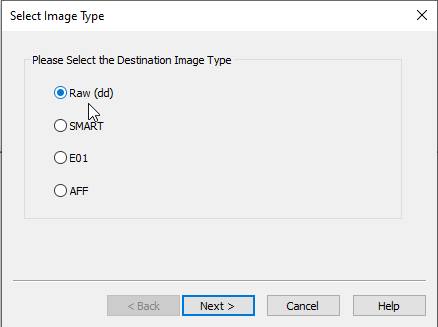
**3.Select the type of evidence . And click on next**

****

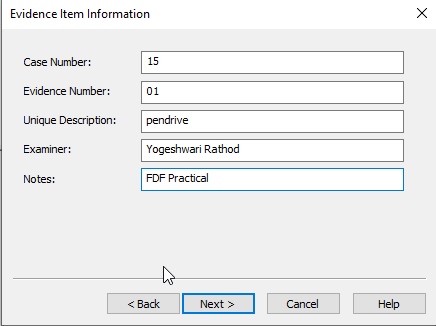
**4.Select drive. And click on Finish**

****

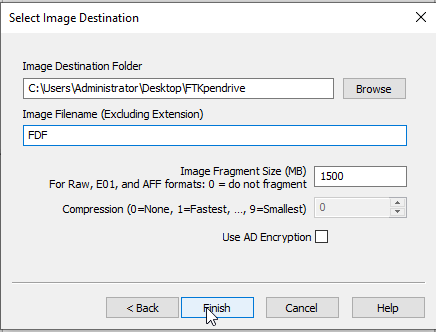
**5.Click on “Add” and select destination image type. Click on next**

****

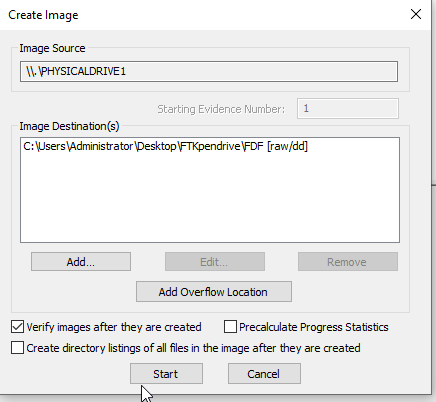
**6.Fill Evidence item Information and click on next.**

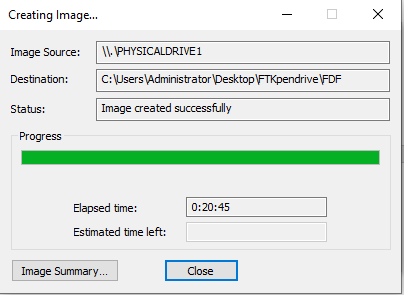
****

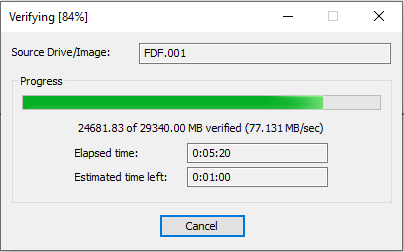
**7.Select image destination and give filename , click on finish**

****

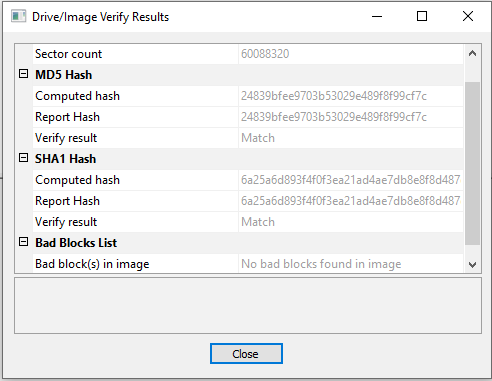
**Click on start , imaging will start and image will create or save at given destination path.**

****

****

****

**It will generate hash value which is helful to find whether the image altered or not,basically it maintains integrity.**

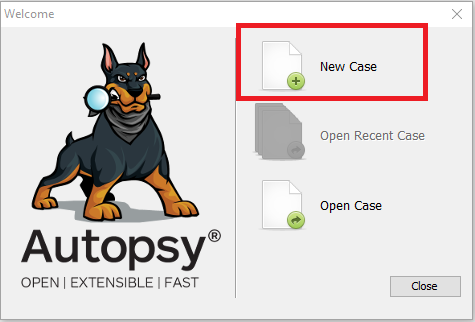
****

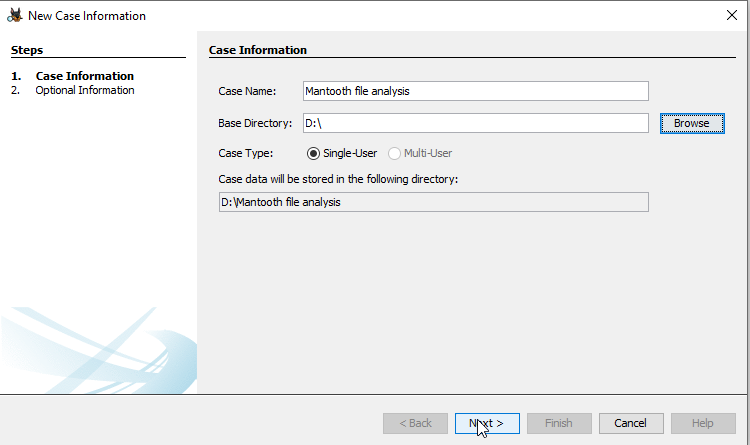
**Autopsy Tool used for recover the data.**

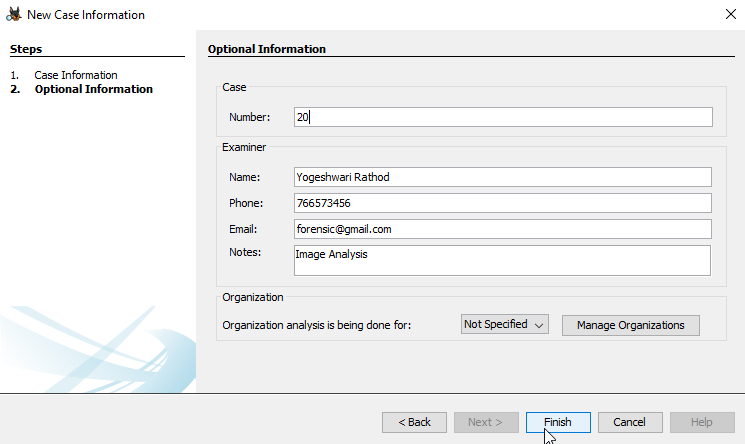
**Steps :**

Analyzing data in Autopsy uses the following workflow:

**1.Make a Case**

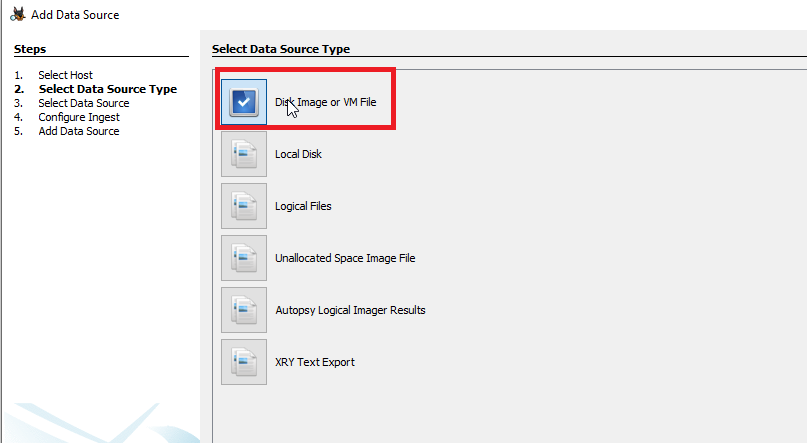
****

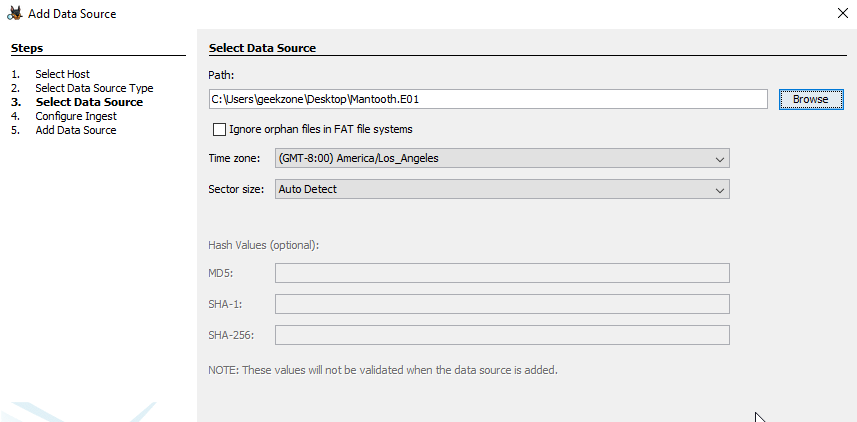
****

****

**2.Add a Data Source**

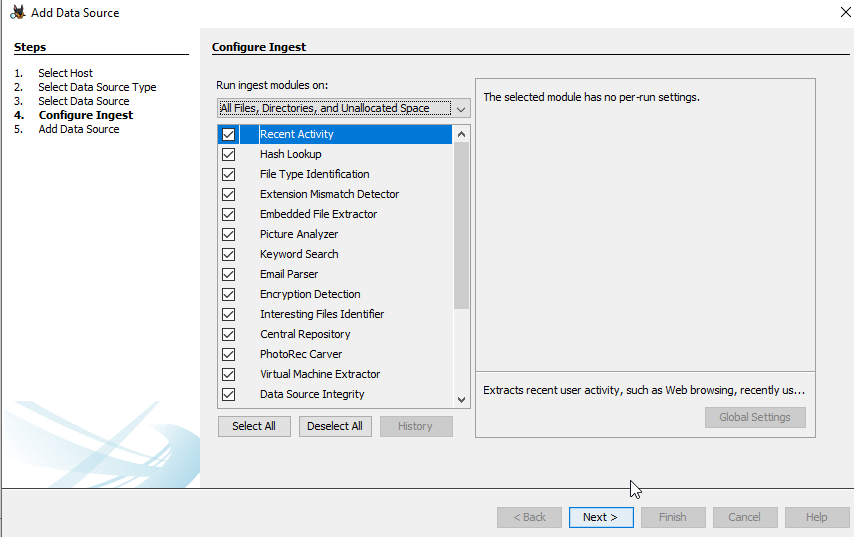
One or more data sources are added to the case. Data sources include disk images and local files.





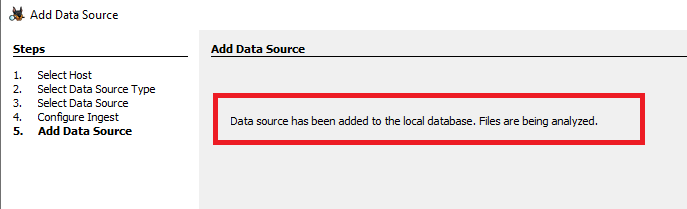
**3.Configure Ingest Modules**

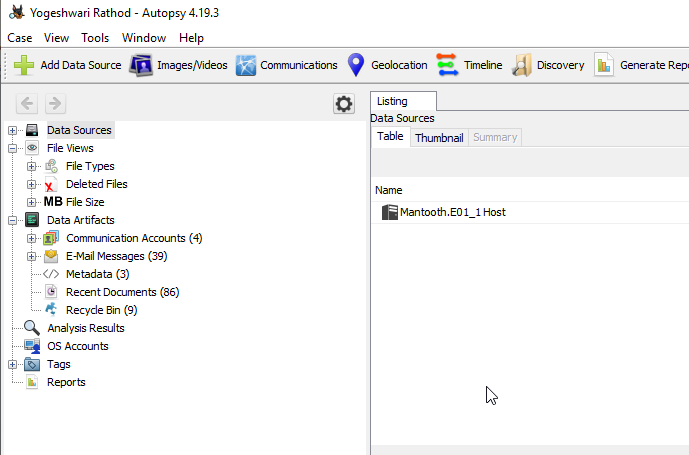
After the data source is included, ingest modules work out of sight to break down the information. Results are presented on the interface continuously and give cautions as important. Model ingests modules incorporate hash count and query, watchword looking, and web relic extraction. Third party modules can be created and added to the pipelines.

****

**4: Review of manually analyze Data**

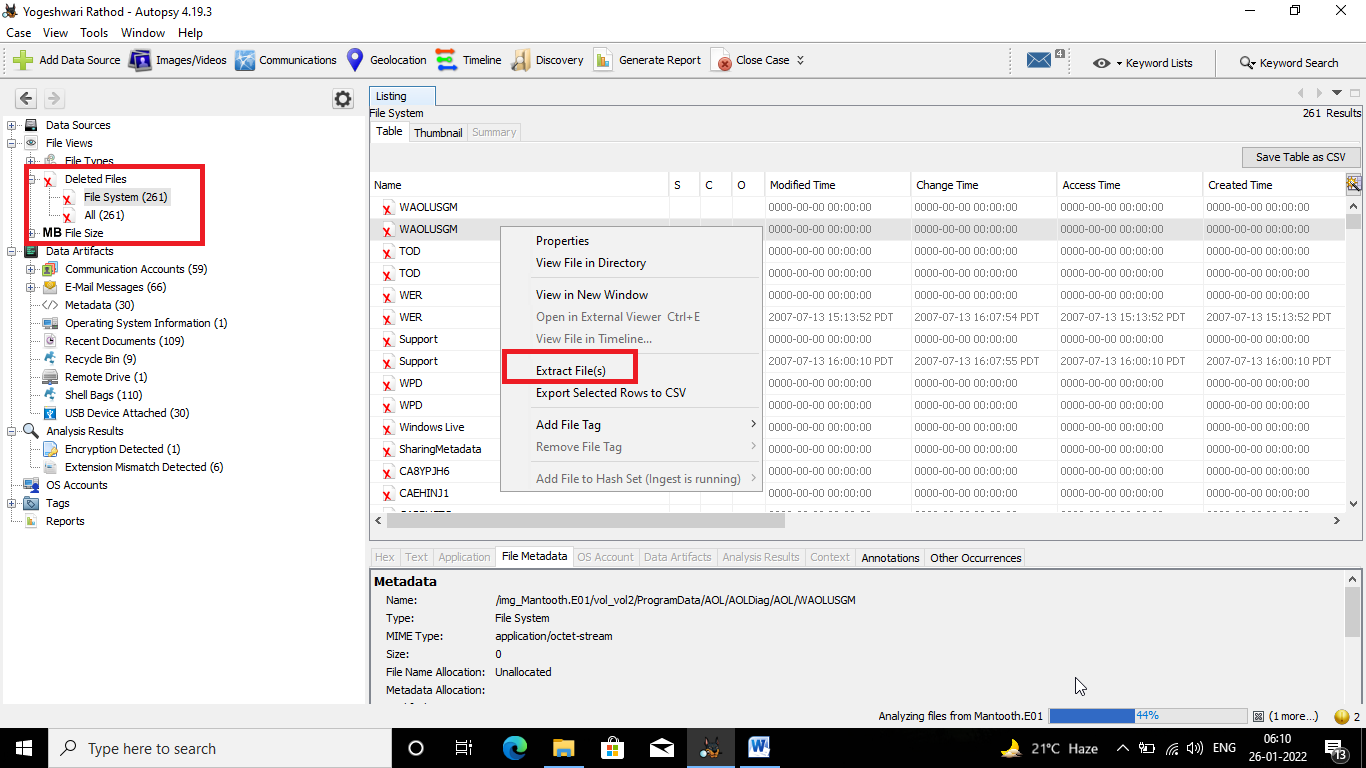
The user navigates “the interface, files contents, and ingest module results to identify the evidence”.

****

****

**Output:**

**1.Extracting Deleted Files**

****

**Conclusion**

Most of the time data analysis and recovery is performed by law enforcement agencies that are investigating cybercriminals.

However, you can still use the above steps, as well as software to recover personal or business data.