# Digital Forensics Lab Report: 10

Date: 19-10-2022

| | |
|---|---|
| **Name:** | **Parth Patel** |
| **Roll No:** | **19BCP091** |
| **Subject Code:** | **20CP411P** |
| **Subject Name:** | **Digital Forensics Lab** |

**Aim/Purpose:** Study of a Data Acquisition tools

**Tool Names:**

1. FTK Manager

   **F**TK Manager is a powerful tool that can be used to manage forensics investigations. It provides a user-friendly interface that makes it easy to search and analyze forensic data. FTK Manager can be used to investigate a wide range of crimes, including child pornography, terrorism, and espionage.

2. Autopsy

   Autopsy is a digital forensics tool used to examine data stored on a computer. It can be used to examine data stored in a variety of formats, including images, text, and email. Autopsy can be used to investigate a variety of crimes, including murder, theft, and fraud.

## Step 1: Download and Install FTK Imager

1. Visit https://accessdata.com/product-download/ftk-imagerversion-4-5 and click on Download button.

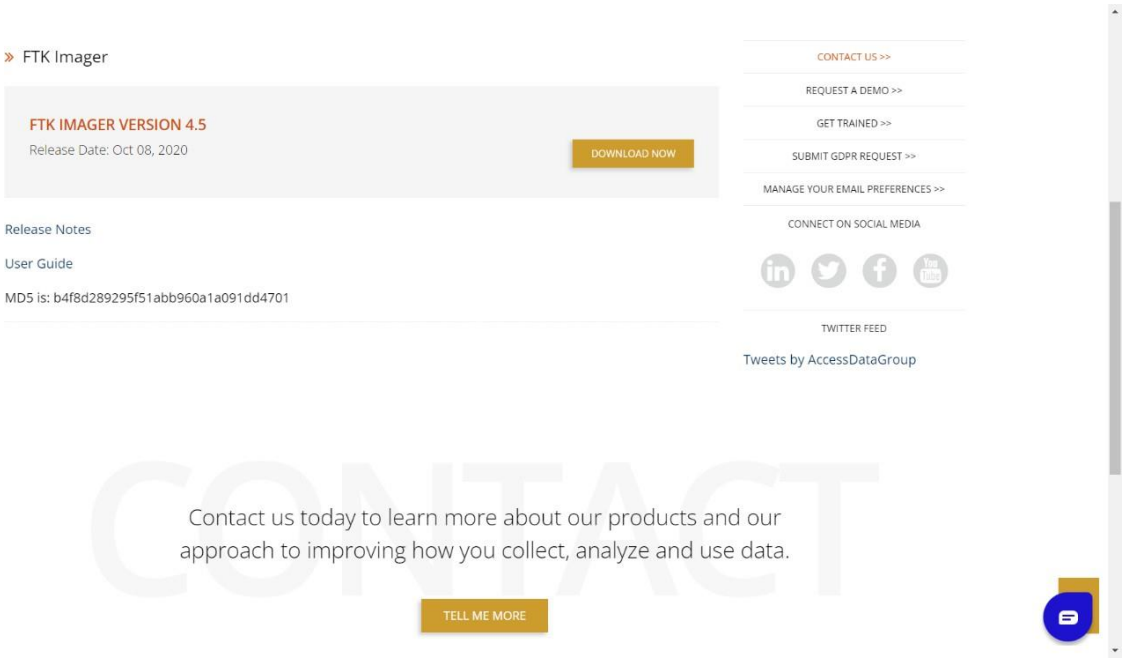


*Figure 1 FTK imager*

2. Install FTK Imager on your system.

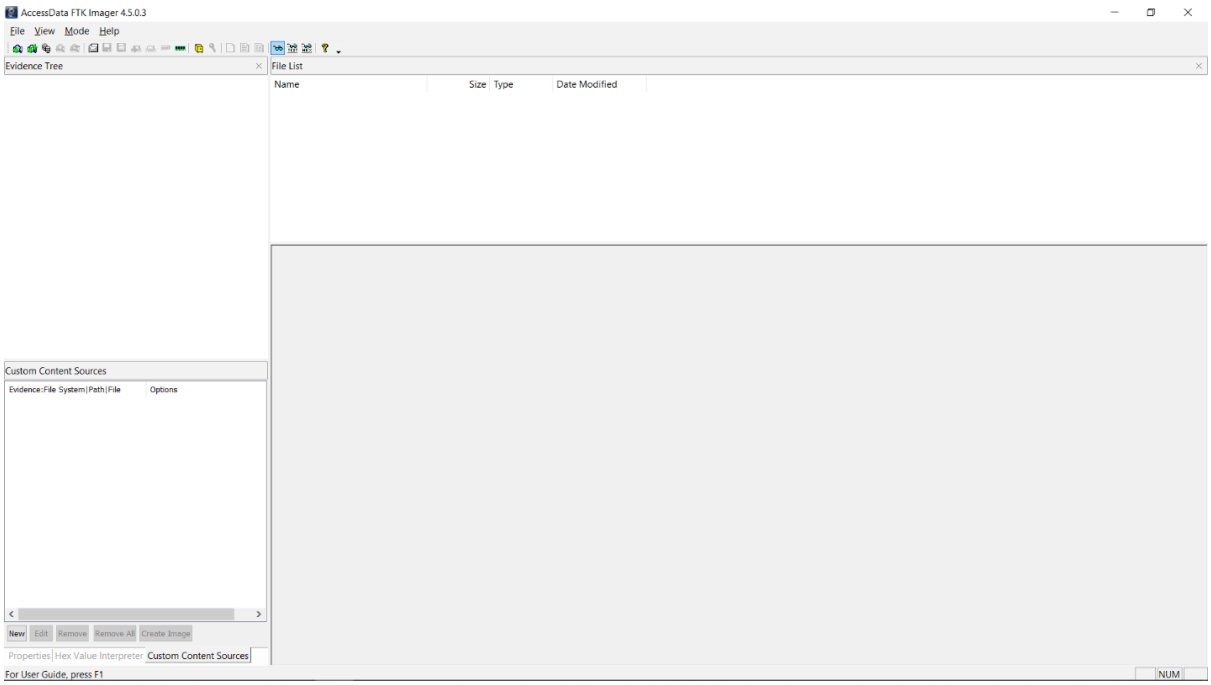


*Figure 2 FTK Imager*

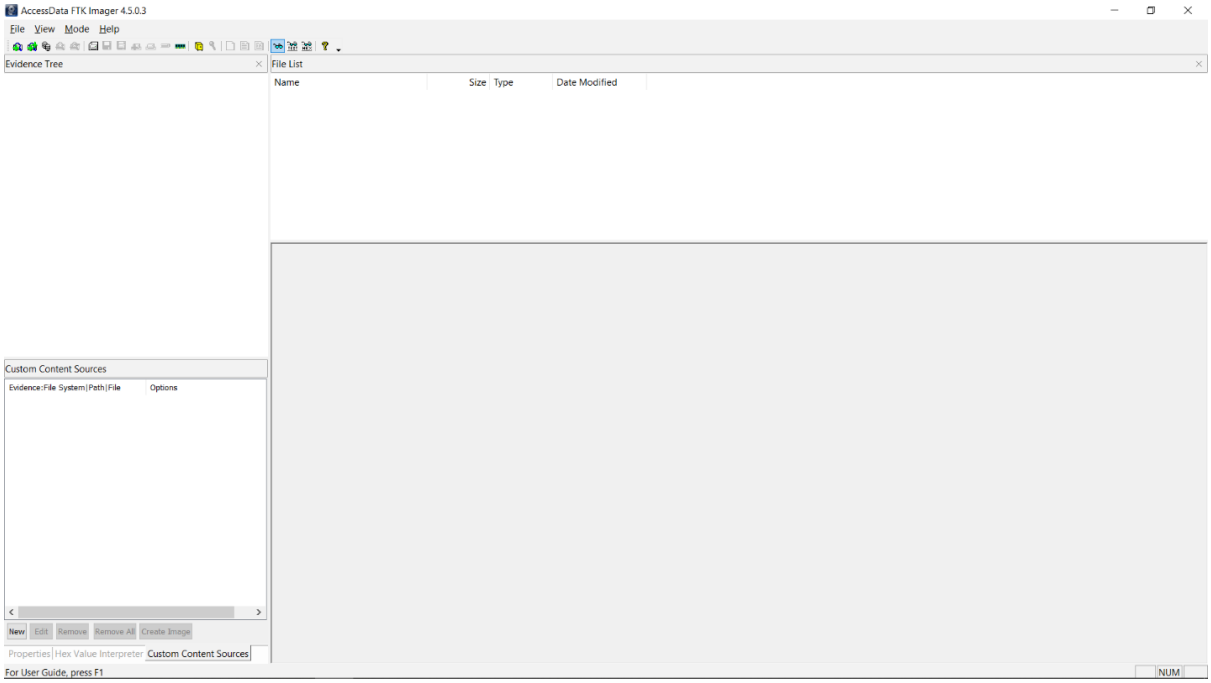


*Figure 3 FTK imager*

## Step 2: Download and Install Autopsy

1. Visit https://www.autopsy.com/download/ and click on Download 64 – Bit.

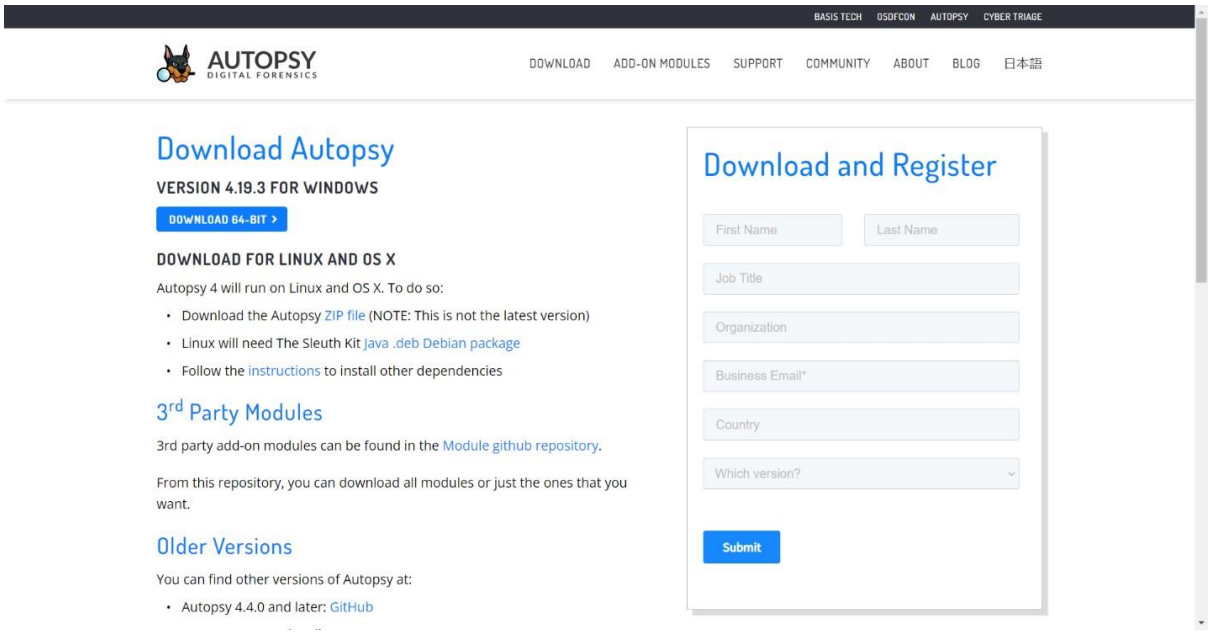


*Figure 4 Autopsy*

2. Install Autopsy on your system.

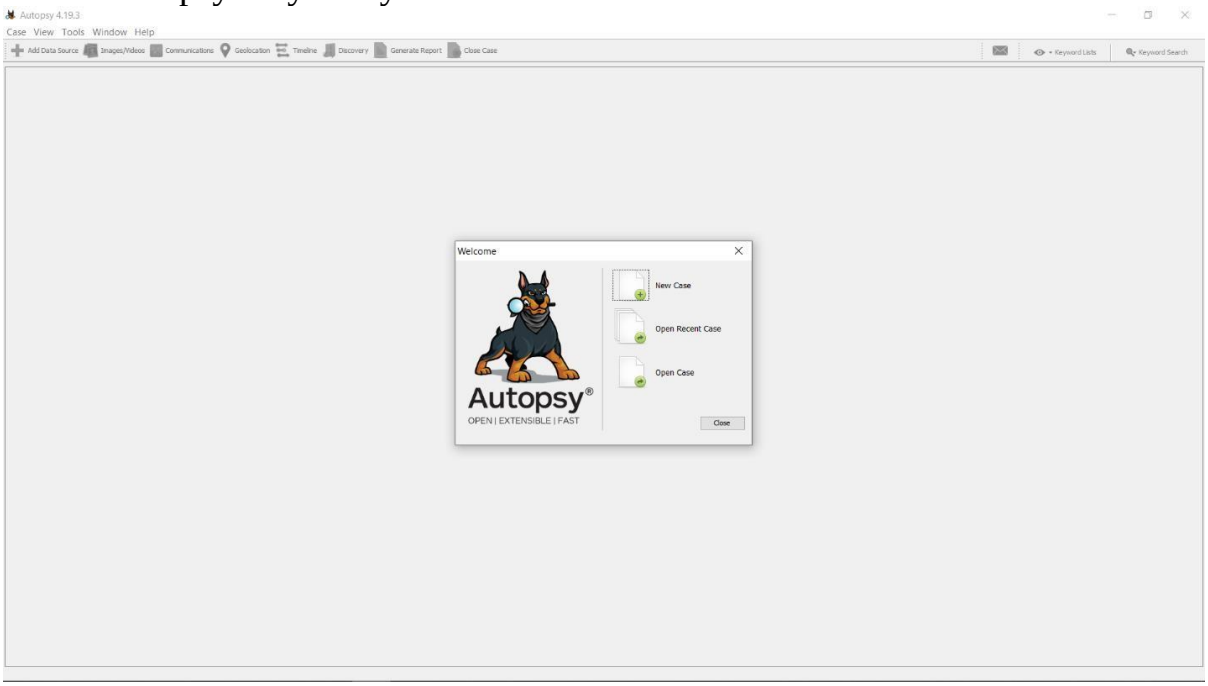


*Figure 5 Autopsy*

**Step 3: Create Image of a Drive**

1. Open FTK Imager and go to Files and Click on Create Disk Image.

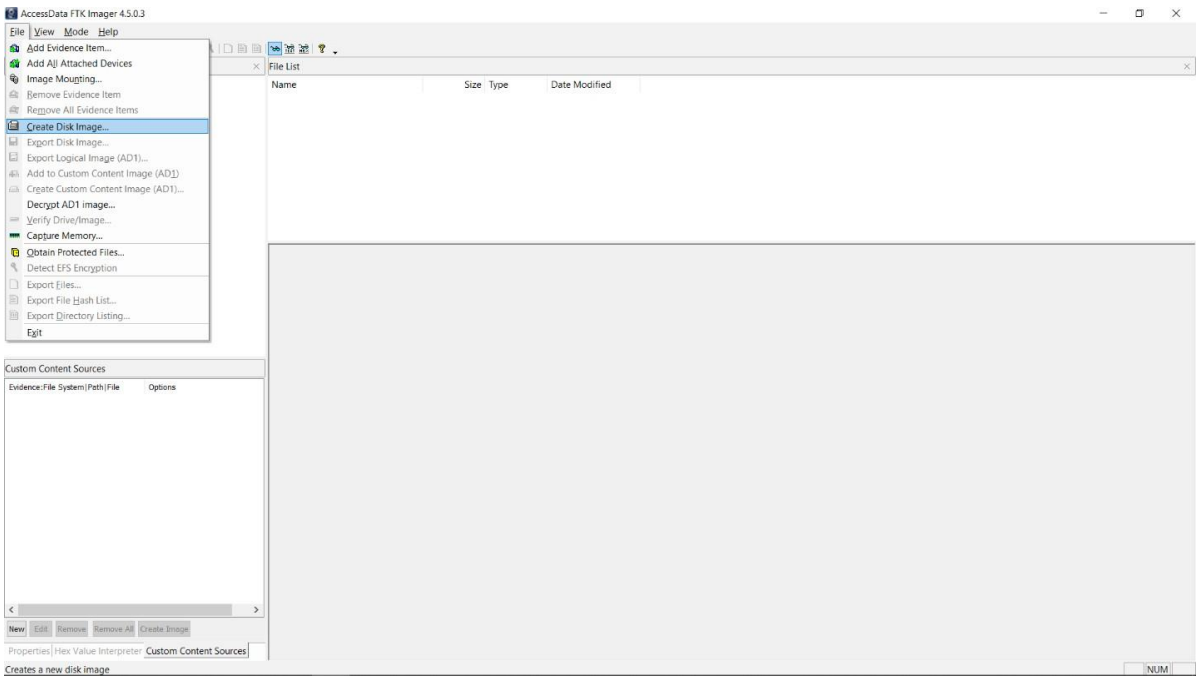


*Figure 6 FTK imager*

2. Select Image File and on the next screen, select image path and click on Finish

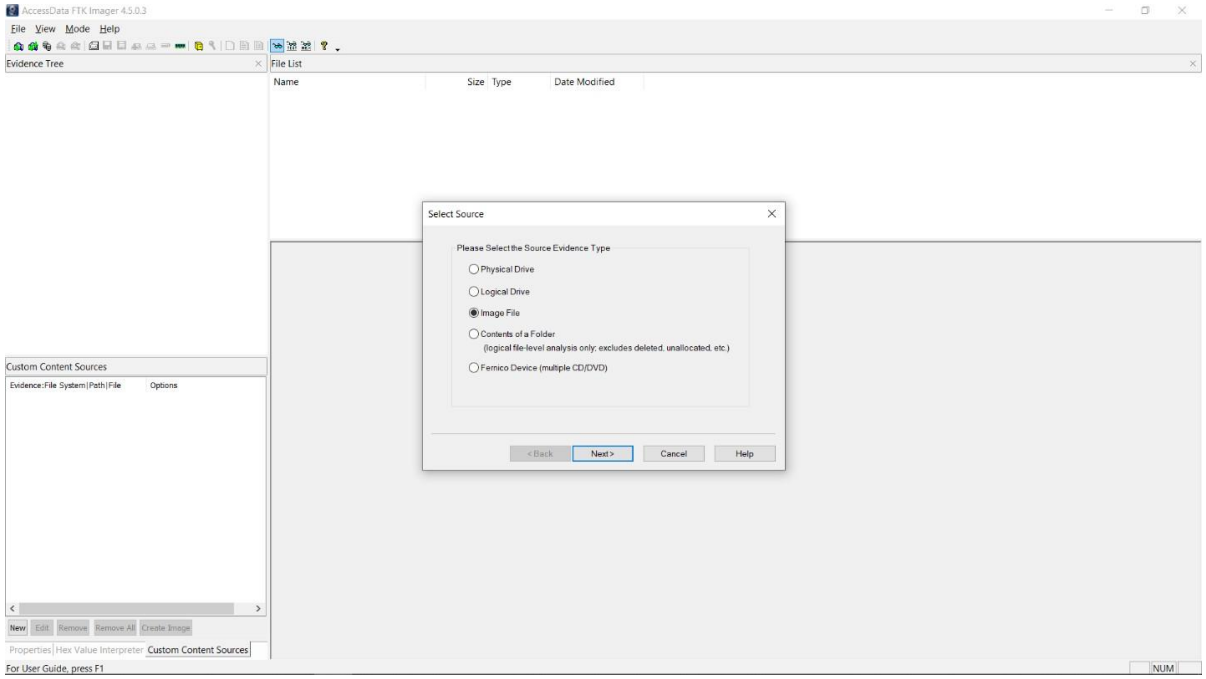


*Figure 7 FTK imager*

3. Select File Type as E01 and fill out the evidence details as asked.

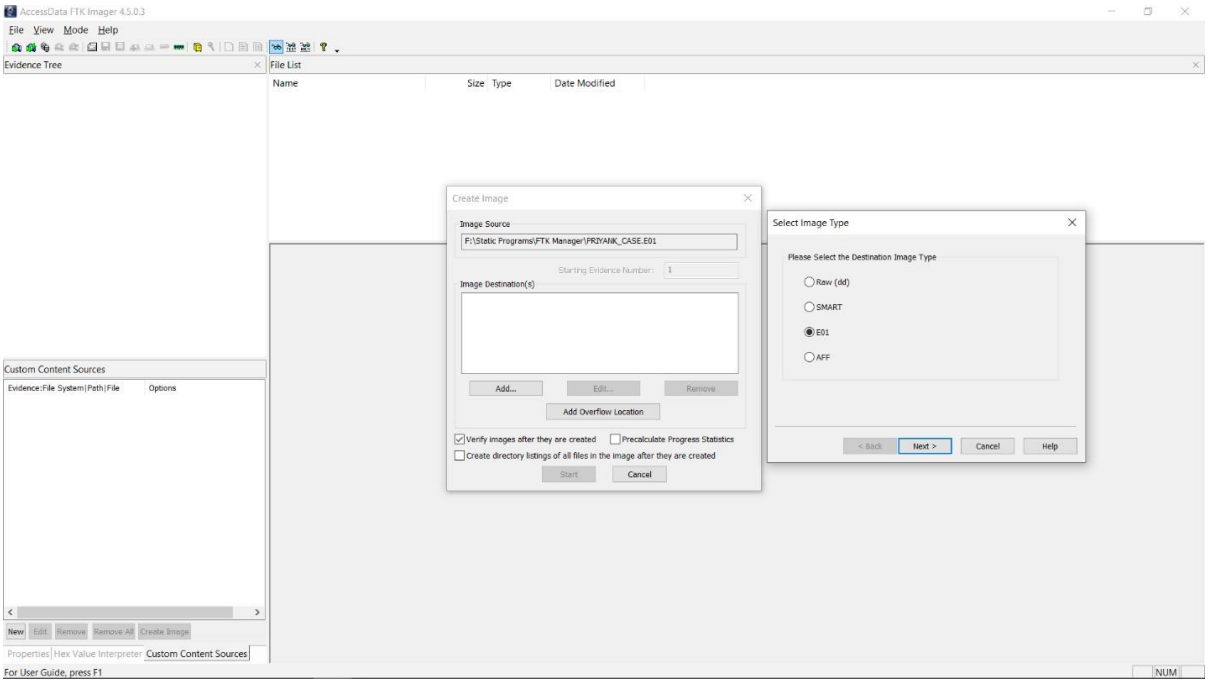


*Figure 8 FTK imager*

4. Wait until the image file is created

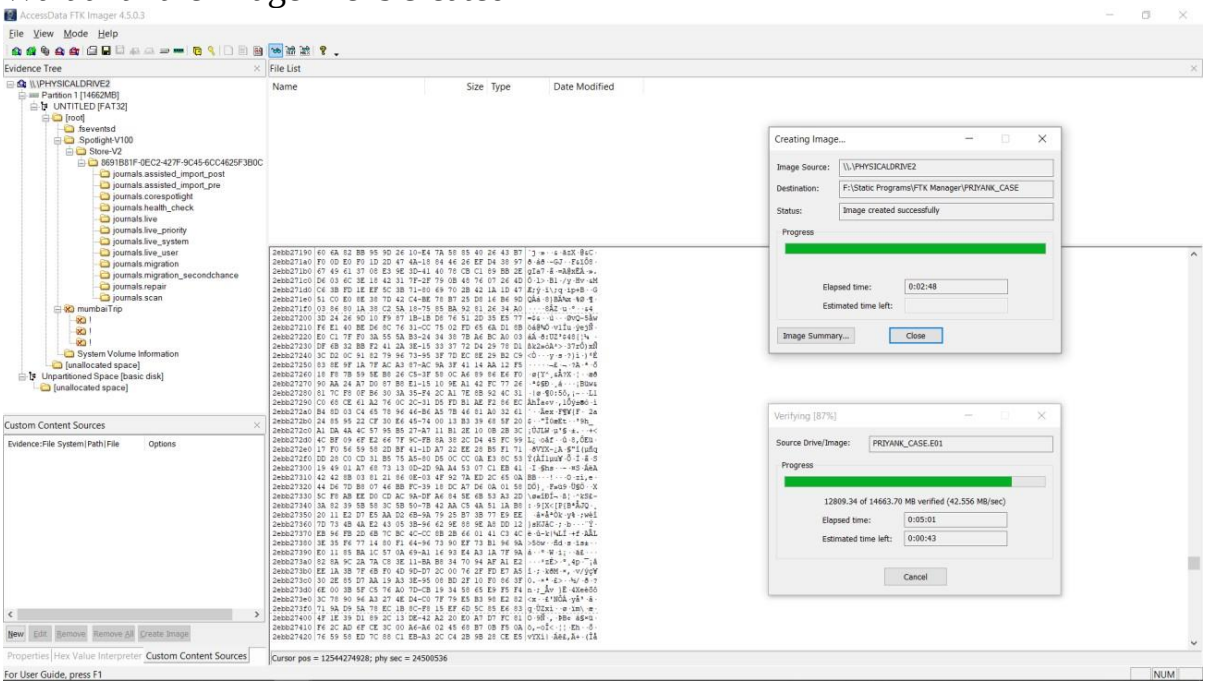


*Figure 9 FTK imager*

5. Once the Image is created, open Autopsy

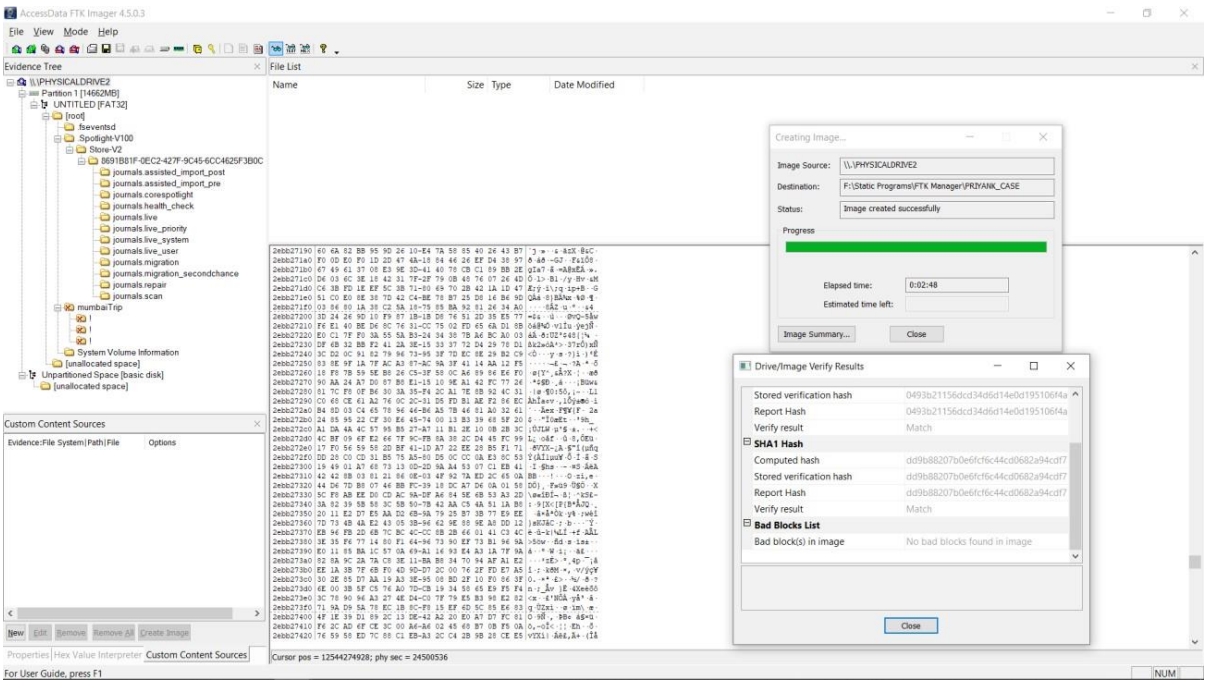


*Figure 10 FTK imager*

**Step 4: Open Autopsy and start working on it.**

1. Open Autopsy and click on New Case.

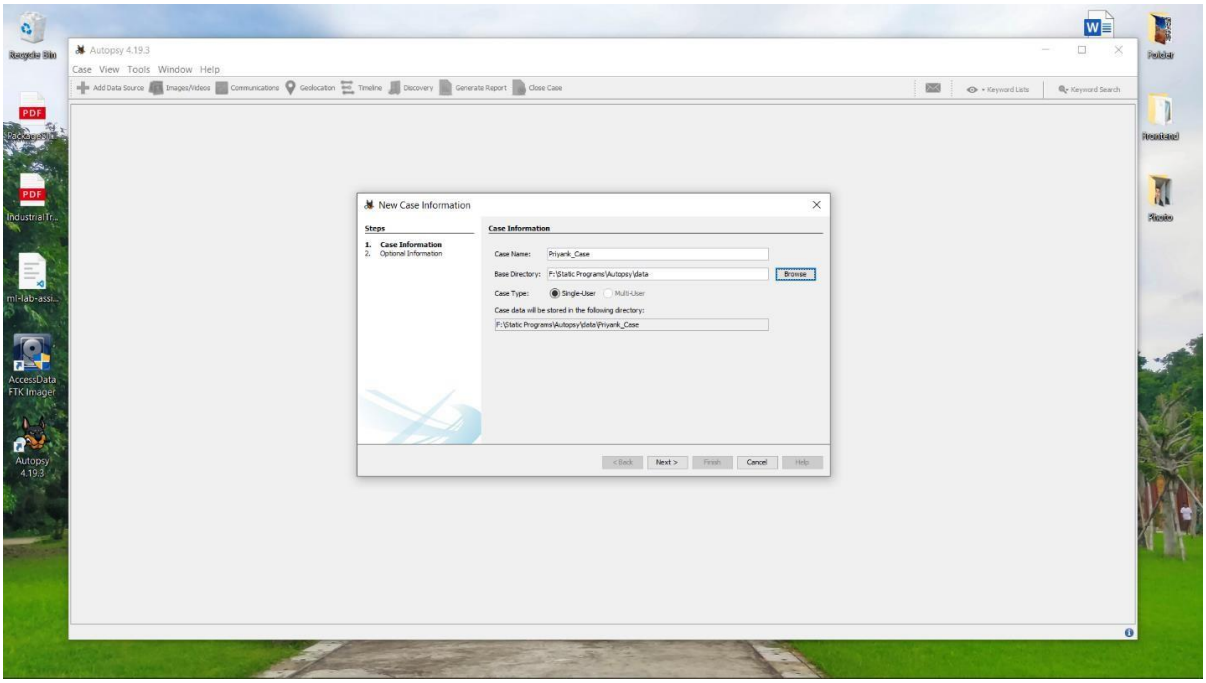


*Figure 11 Autopsy*

2. Fill out Case Information and Optional Information.

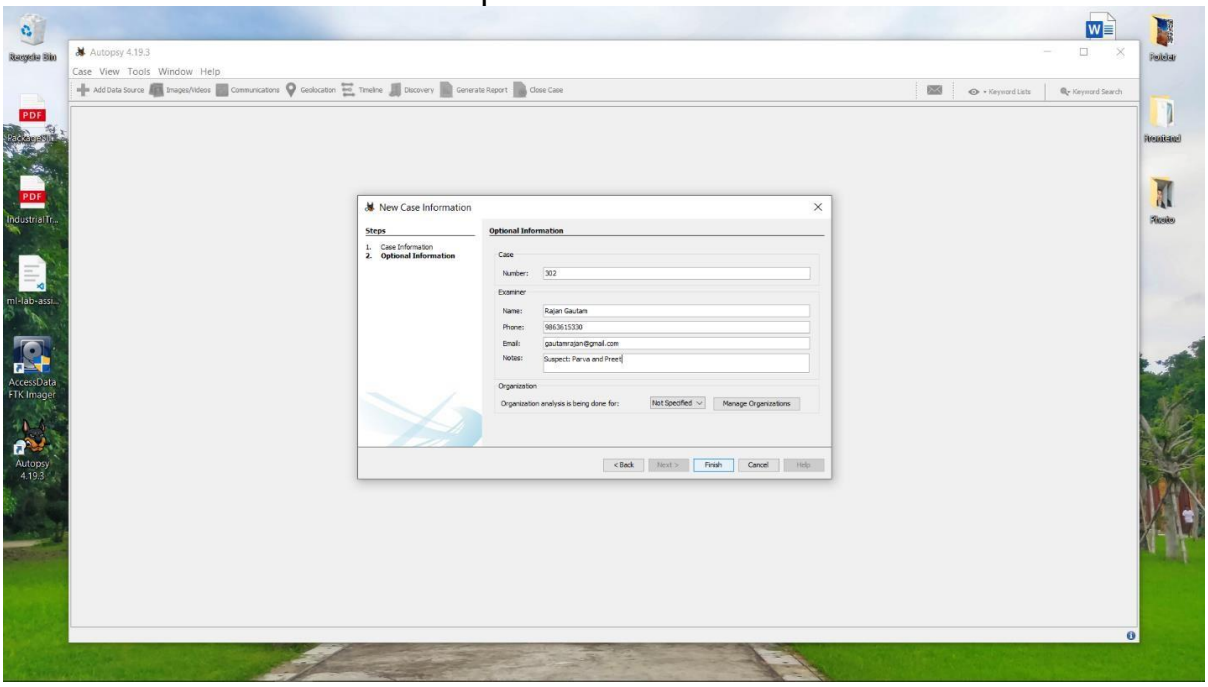


*Figure 12 Autopsy*

3. Once a case is created, add an image file for analysis.

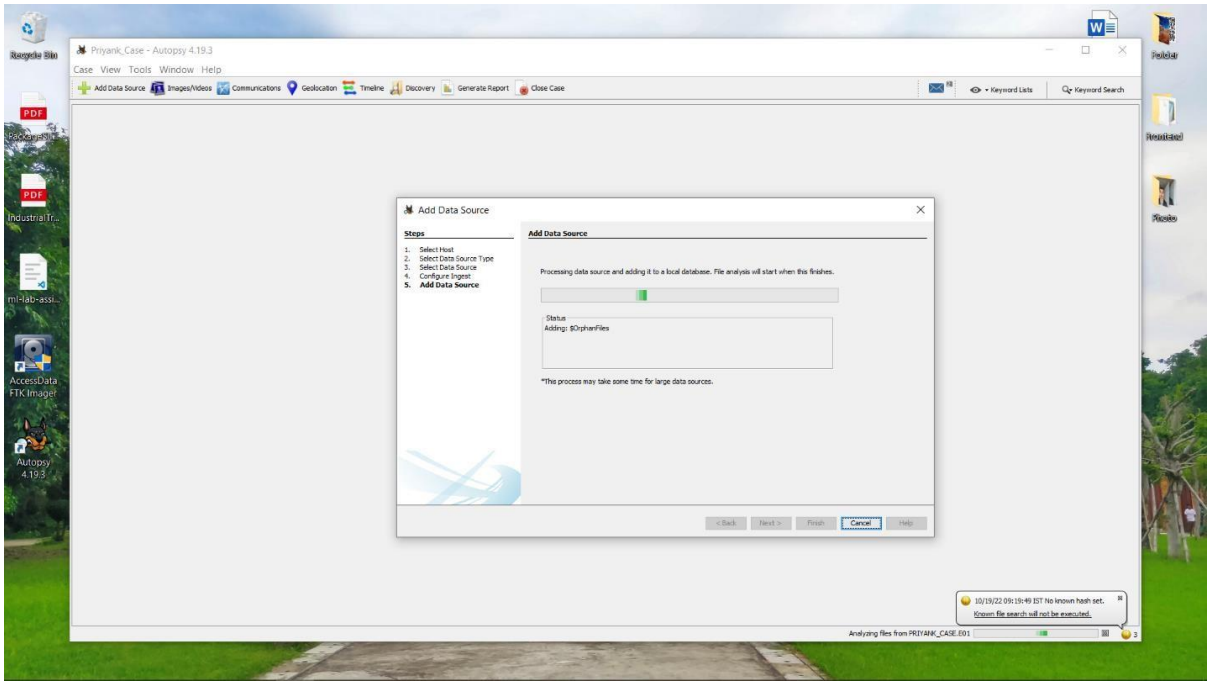


*Figure 13 Autopsy*

4. You can view the file contents on the screen.

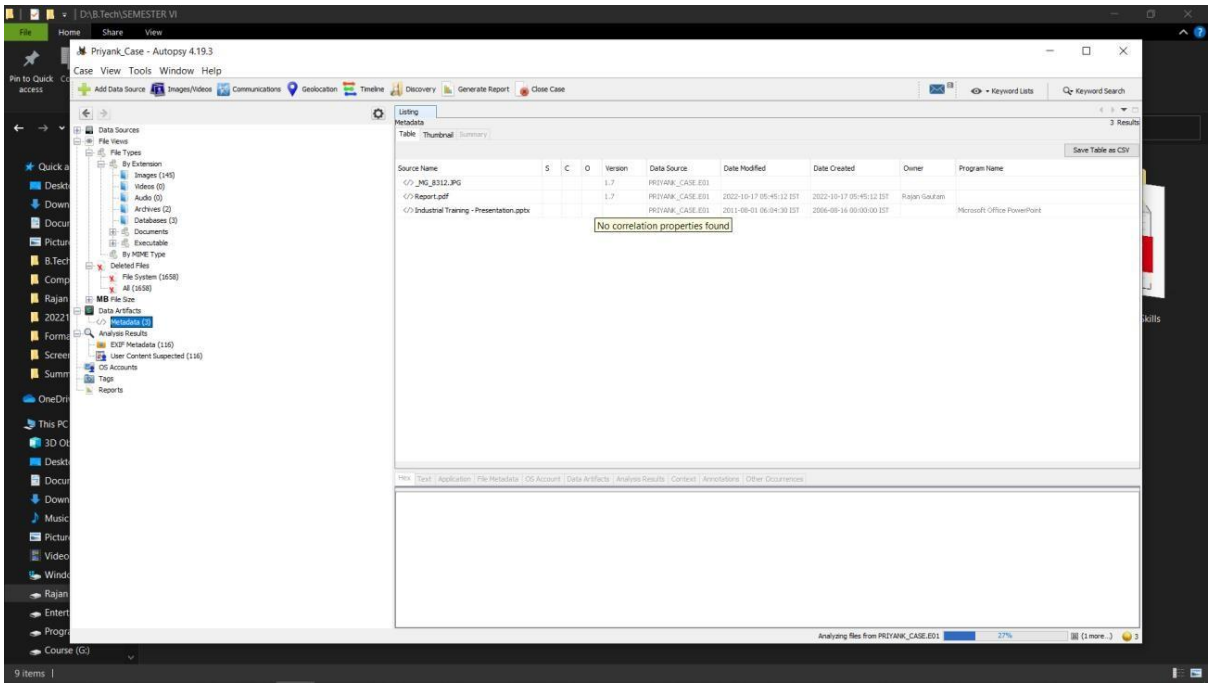


*Figure 14 Autopsy*

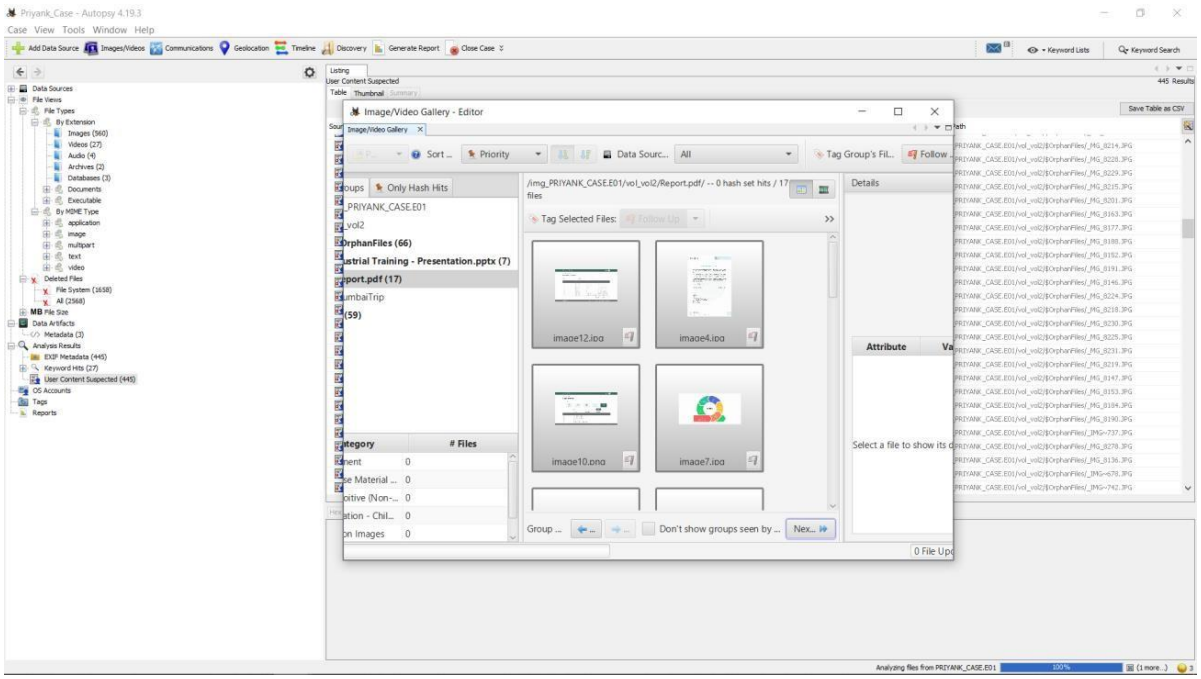


*Figure 15 Autopsy*

5. Click on Generate Report to generate Analysis Report.

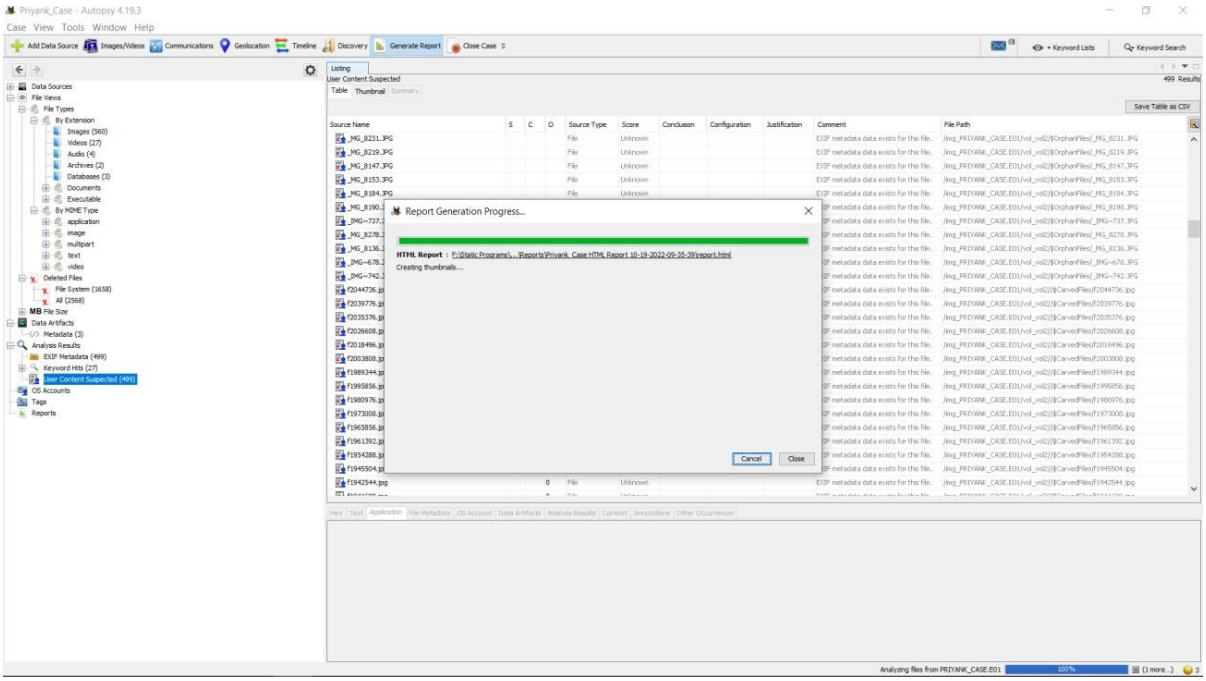


*Figure 16 Autopsy*

6. You can view the report in the web browser.

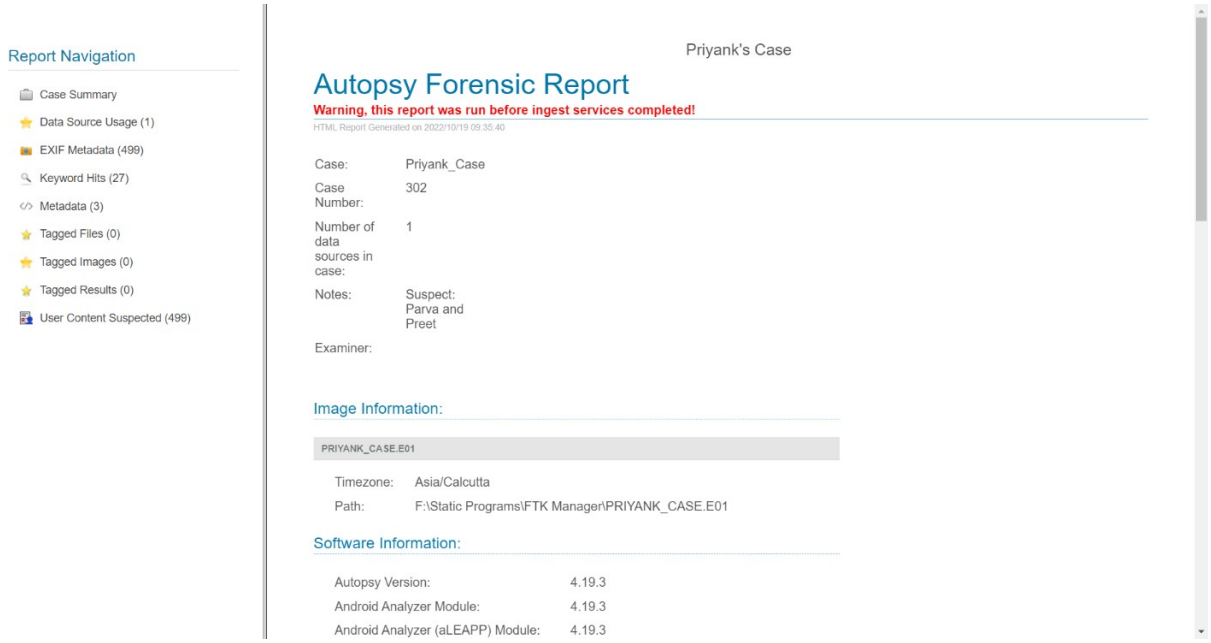


*Figure 17 Autopsy*

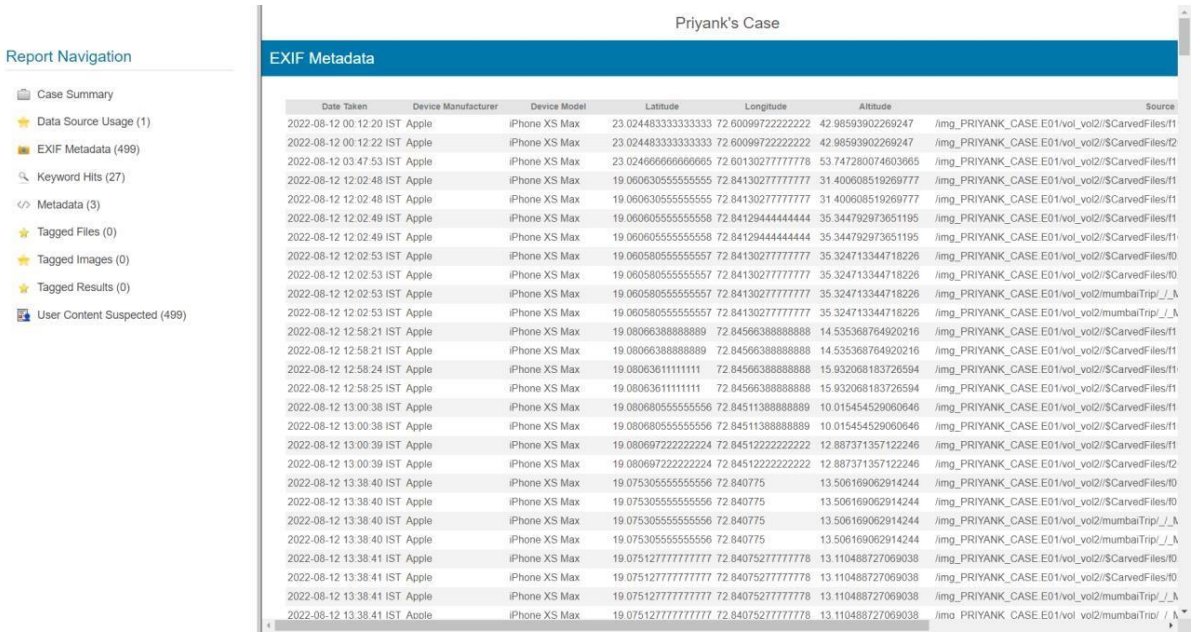


*Figure 18 Autopsy*

**Conclusion:**

1. The FTK Imager is a reliable and easy-to-use data acquisition tool that can be used to obtain forensically sound images of computers. The Autopsy tool is a powerful open-source digital forensics platform that can be used to examine the images obtained with the FTK Imager.
2. FTK Imager is a data acquisition tool that can be used to image a hard drive or other data storage device. The Imager can be used to create an image of the entire drive, or just a portion of the drive. The Imager can also be used to create an image of a specific file or folder.
3. Autopsy tool is a data analysis tool that can be used to examine the contents of a hard drive or other data storage device. Autopsy can be used to examine the contents of an entire drive, or just a portion of the drive. Autopsy can also be used to examine the contents of a specific file or folder.