

## Digital Forensics Lab Report: 10

Date: 19-10-2022

<b>Name:</b>	<b>Parth Patel</b>
<b>Roll No:</b>	<b>19BCP091</b>
<b>Subject Code:</b>	<b>20CP411P</b>
<b>Subject Name:</b>	<b>Digital Forensics Lab</b>

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

### Tool Names:

#### 1. FTK Manager

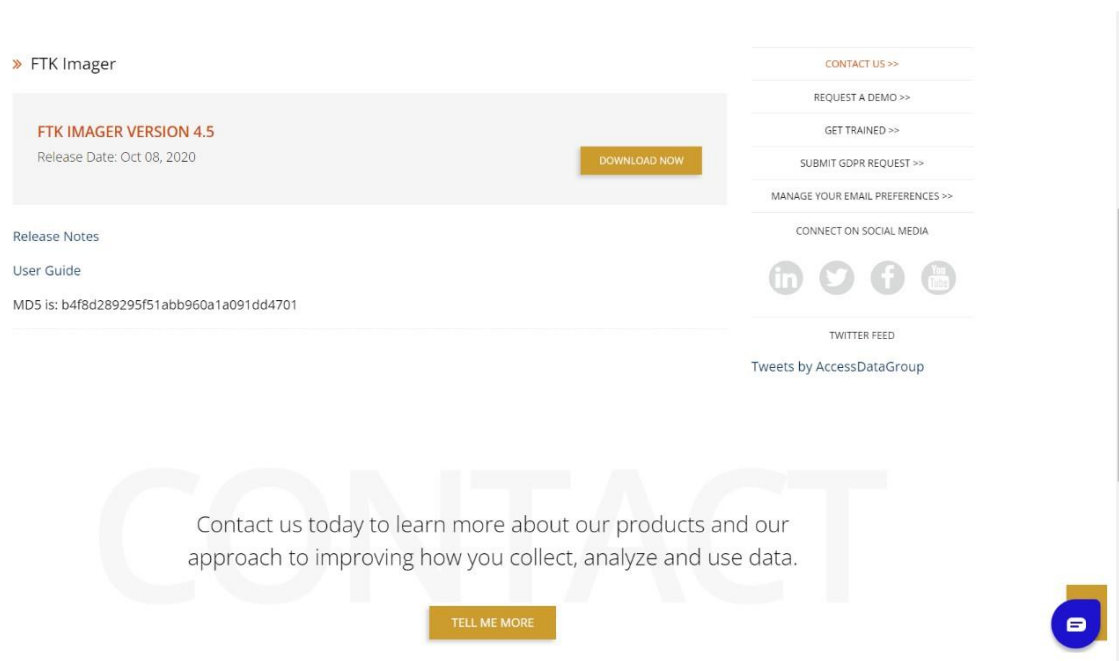
FTK Manager is a powerful tool that can be used to manage forensics investigations. It provides a user-friendly interface that makes it easy to search and analyze forensic data. FTK Manager can be used to investigate a wide range of crimes, including child pornography, terrorism, and espionage.

#### 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.

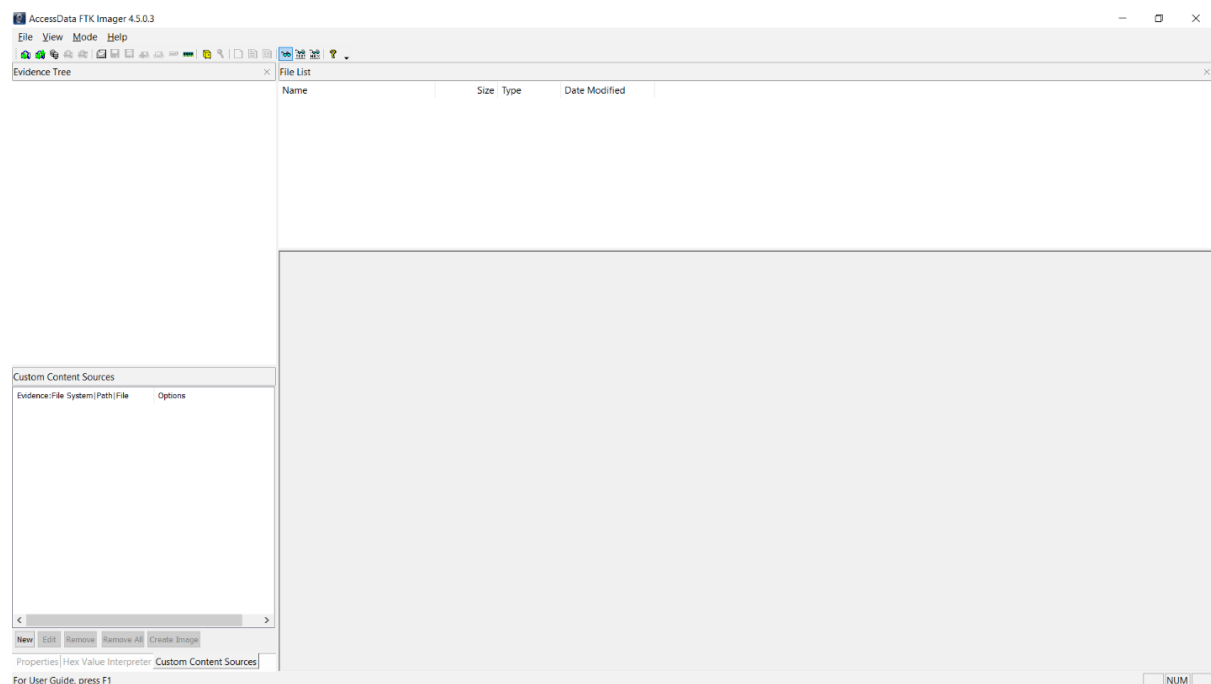
### Step 1: Download and Install FTK Imager

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

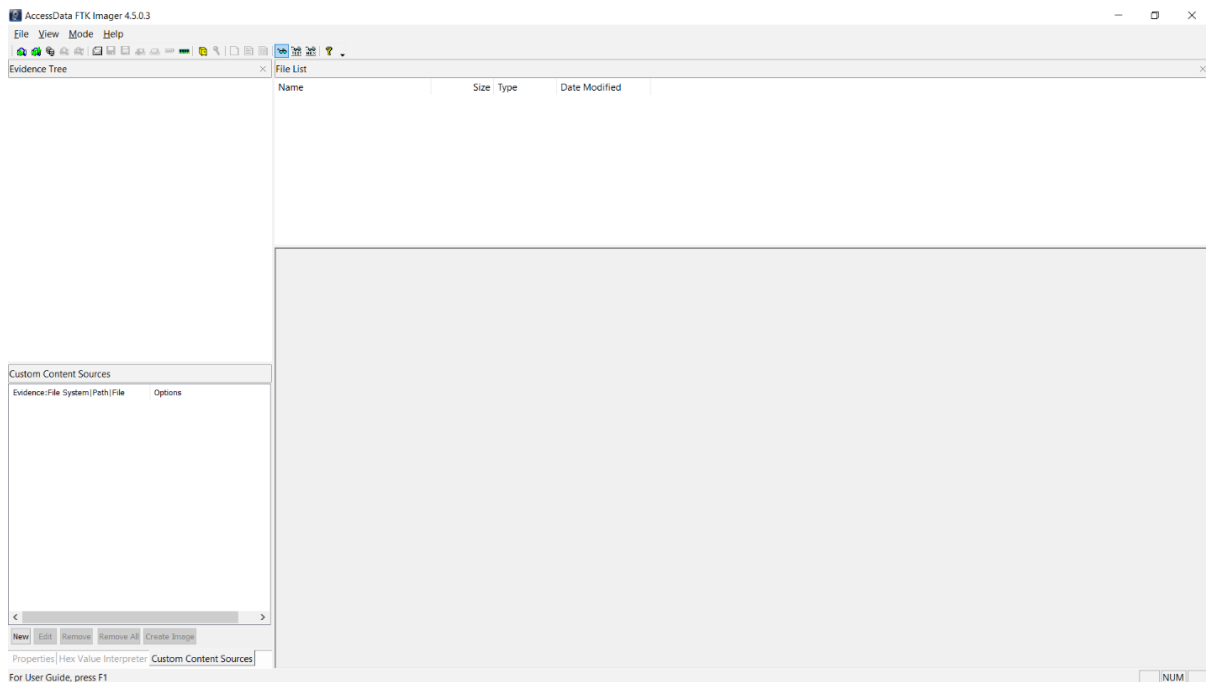


*Figure 1 FTK imager*

## 2. Install FTK Imager on your system.



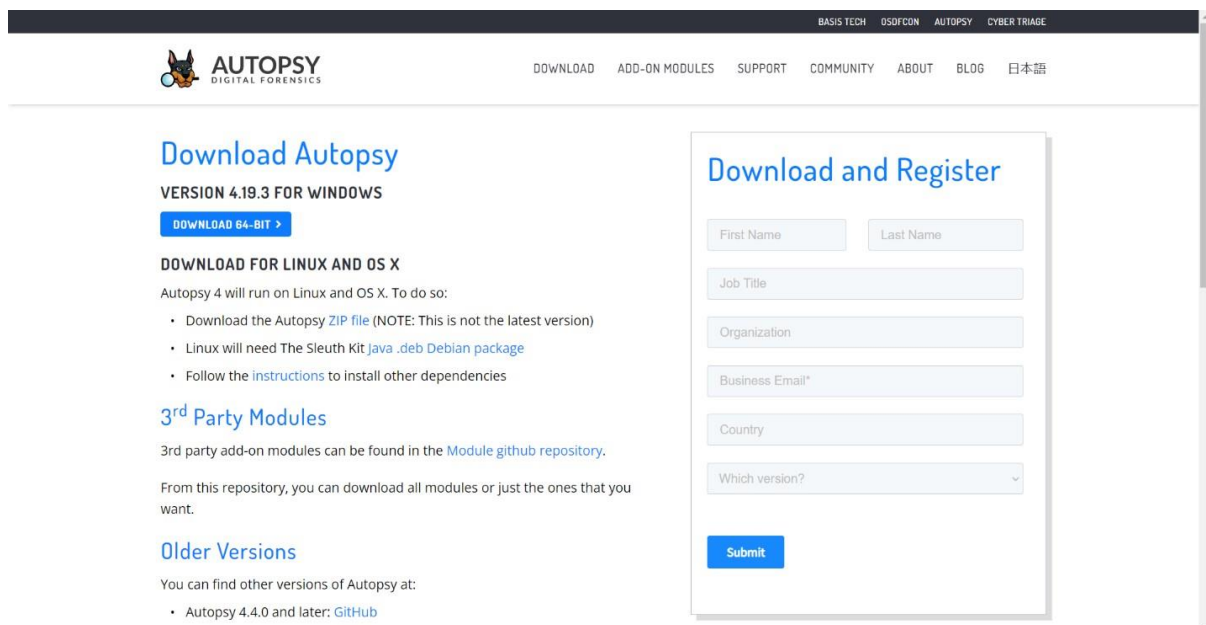
*Figure 2 FTK Imager*



*Figure 3 FTK imager*

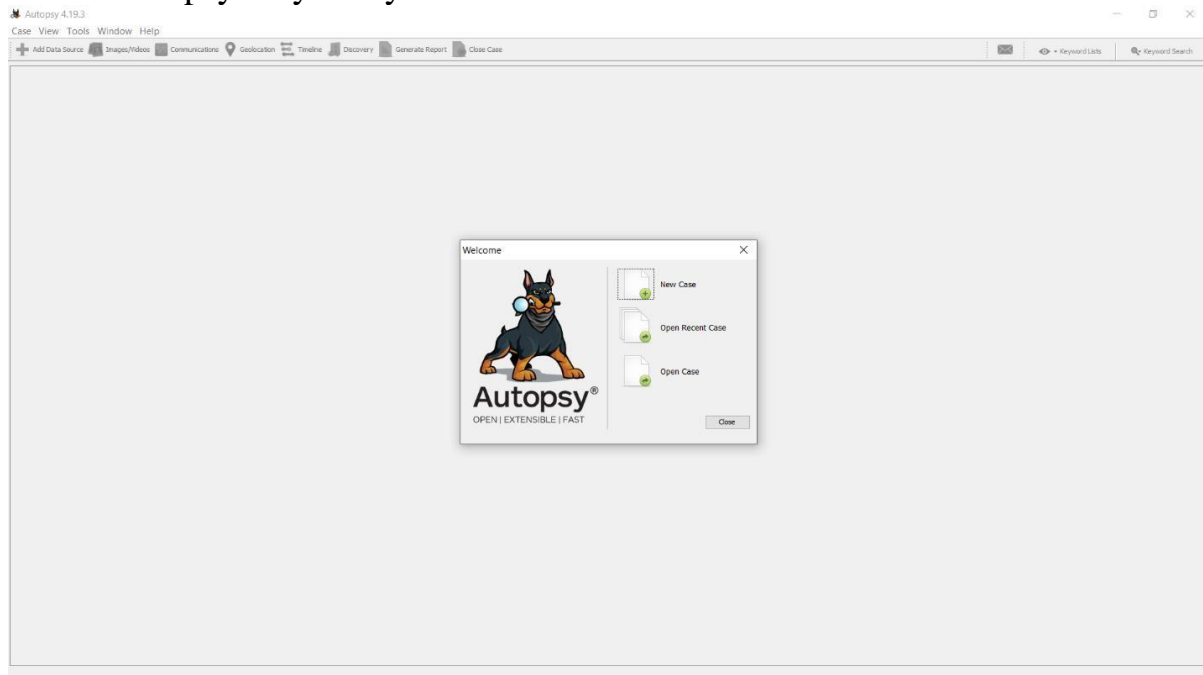
## Step 2: Download and Install Autopsy

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



*Figure 4 Autopsy*

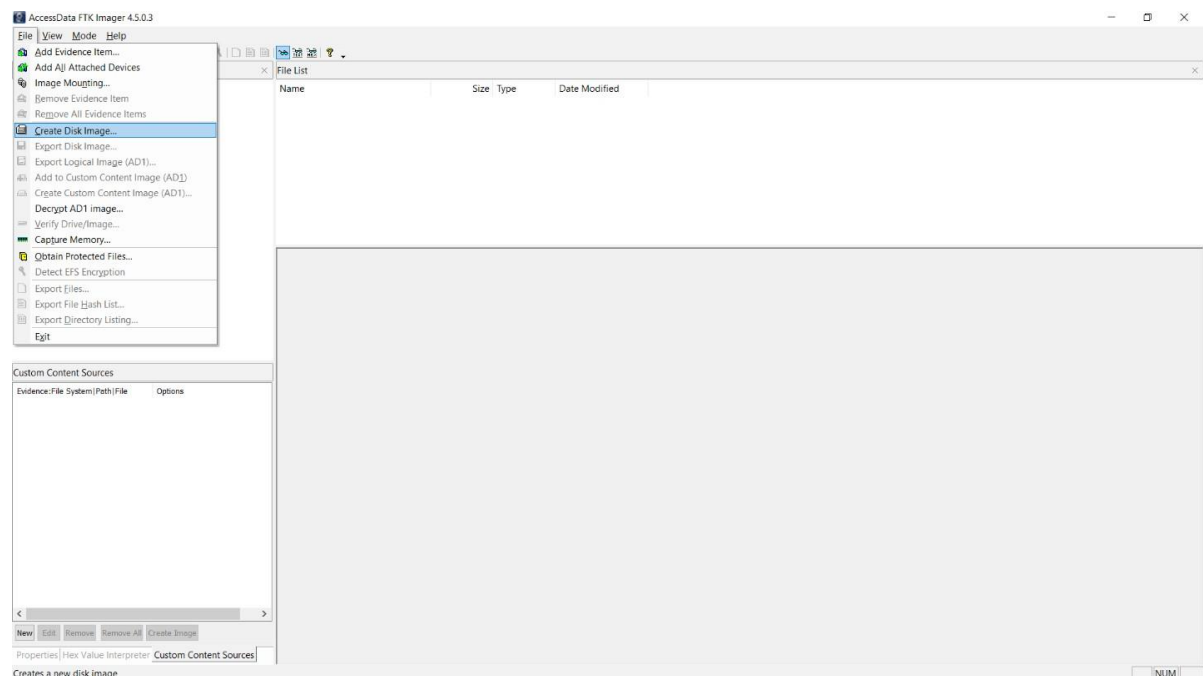
## 2. Install Autopsy on your system.



*Figure 5 Autopsy*

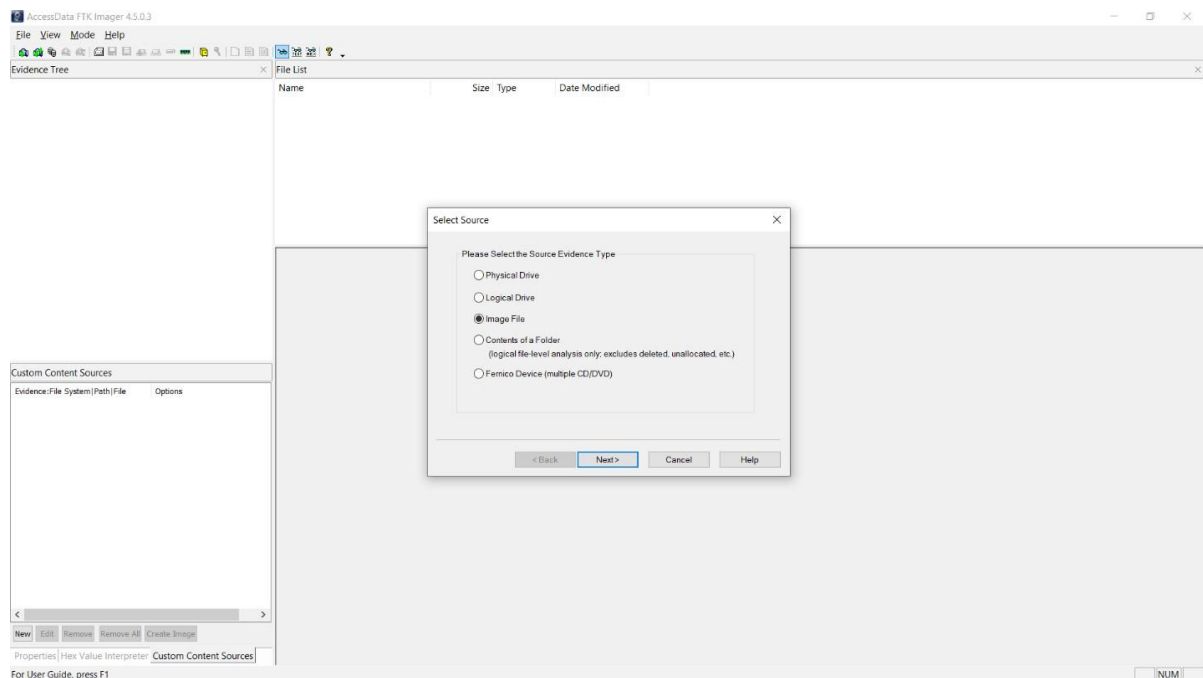
## Step 3: Create Image of a Drive

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



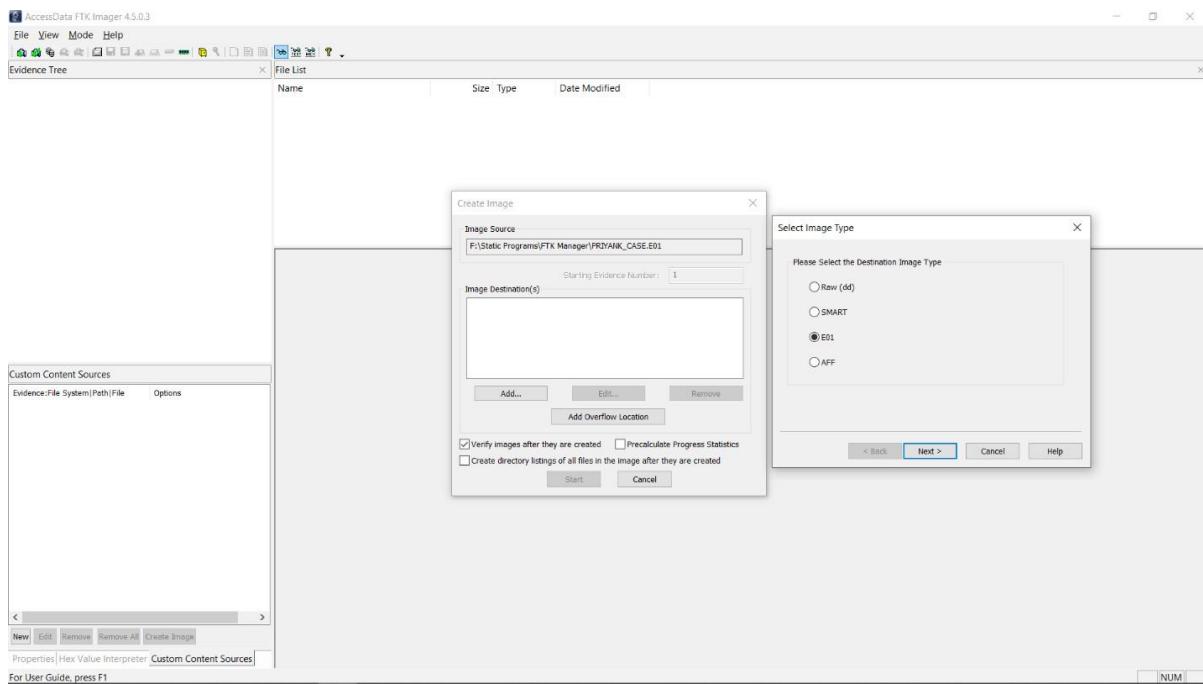
*Figure 6 FTK imager*

## 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

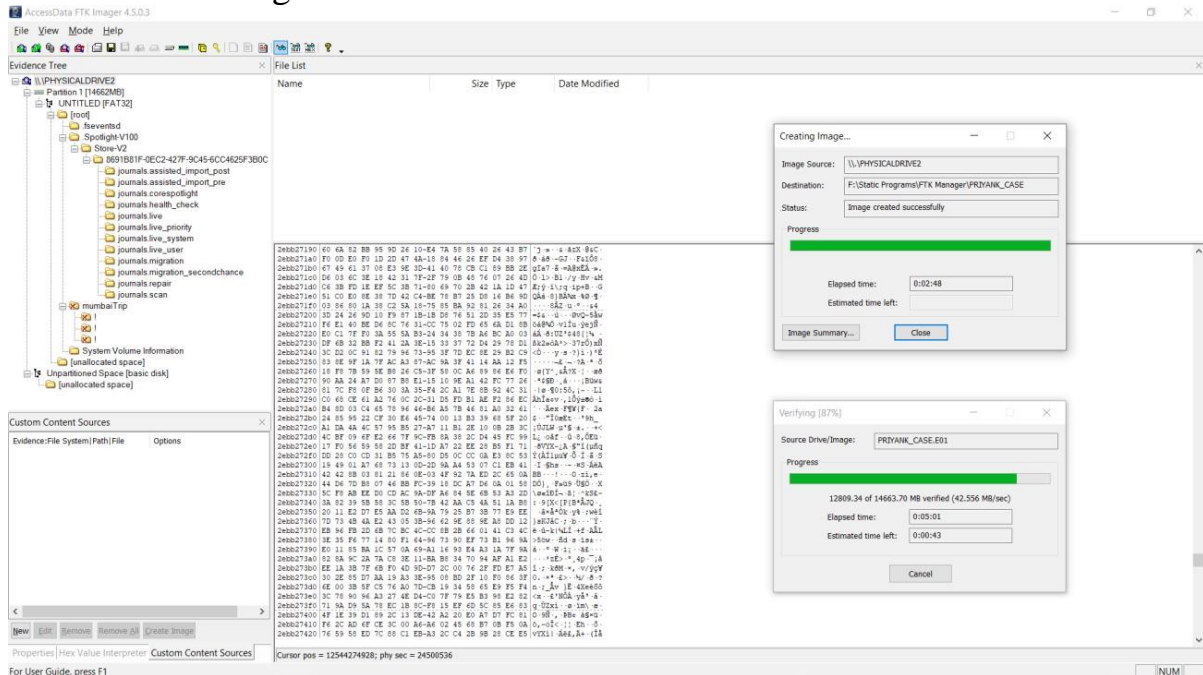


Figure 9 FTK imager

#### 5. Once the Image is created, open Autopsy

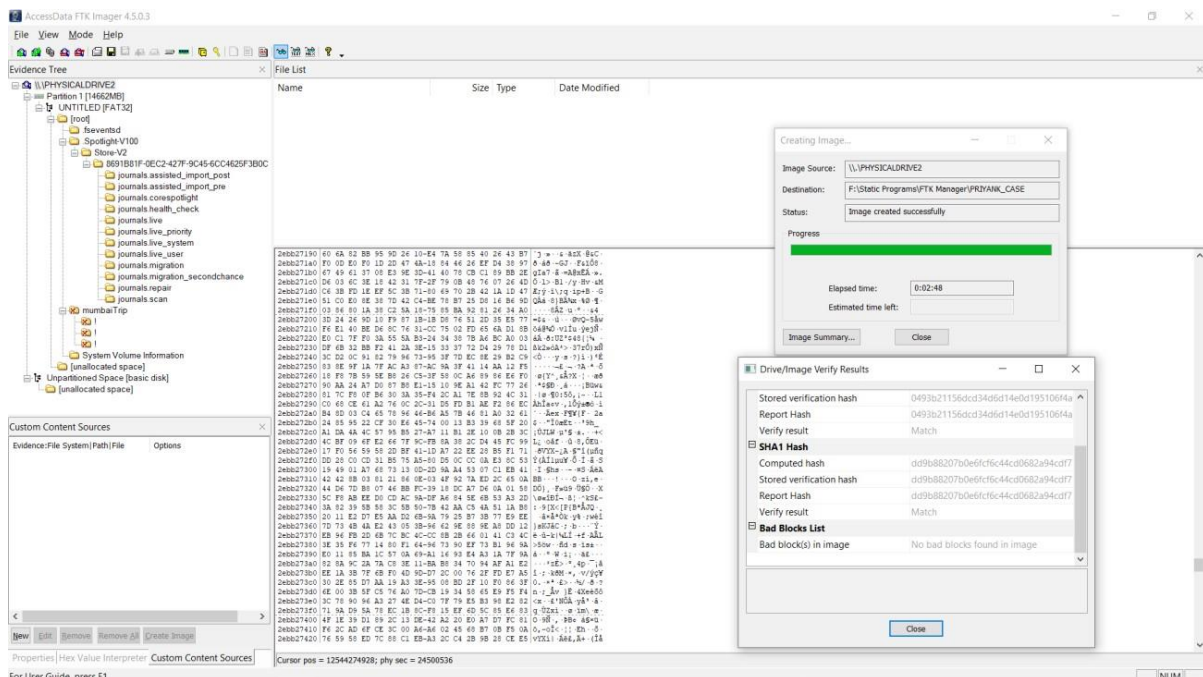
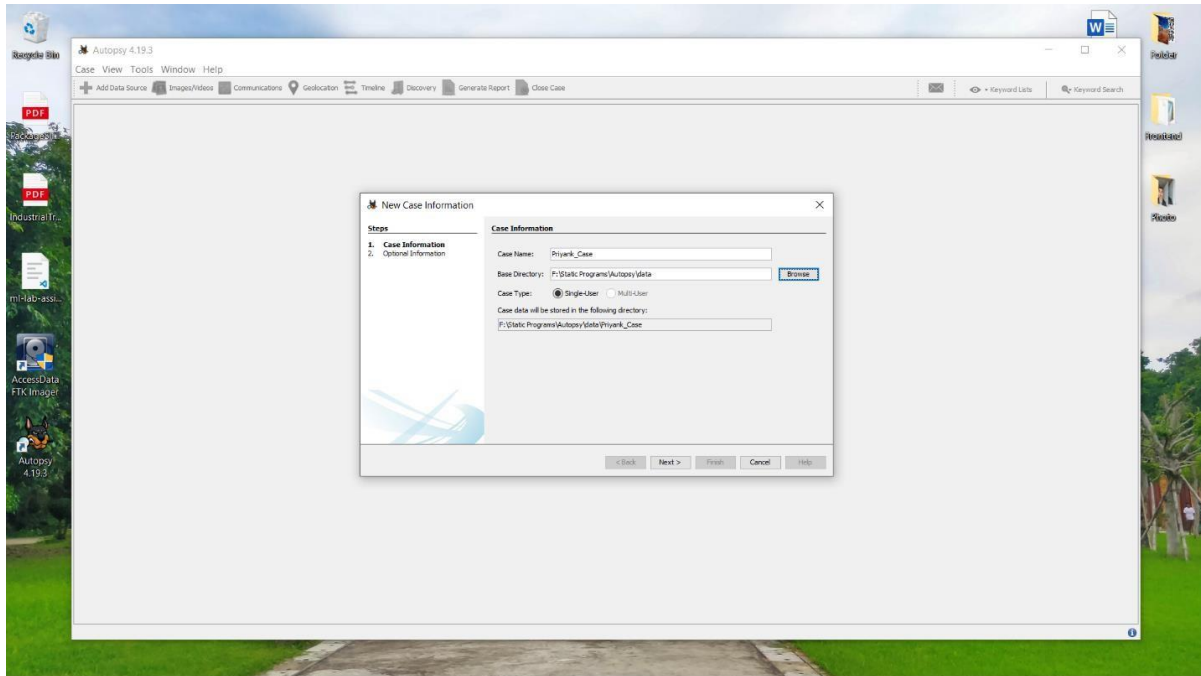


Figure 10 FTK imager

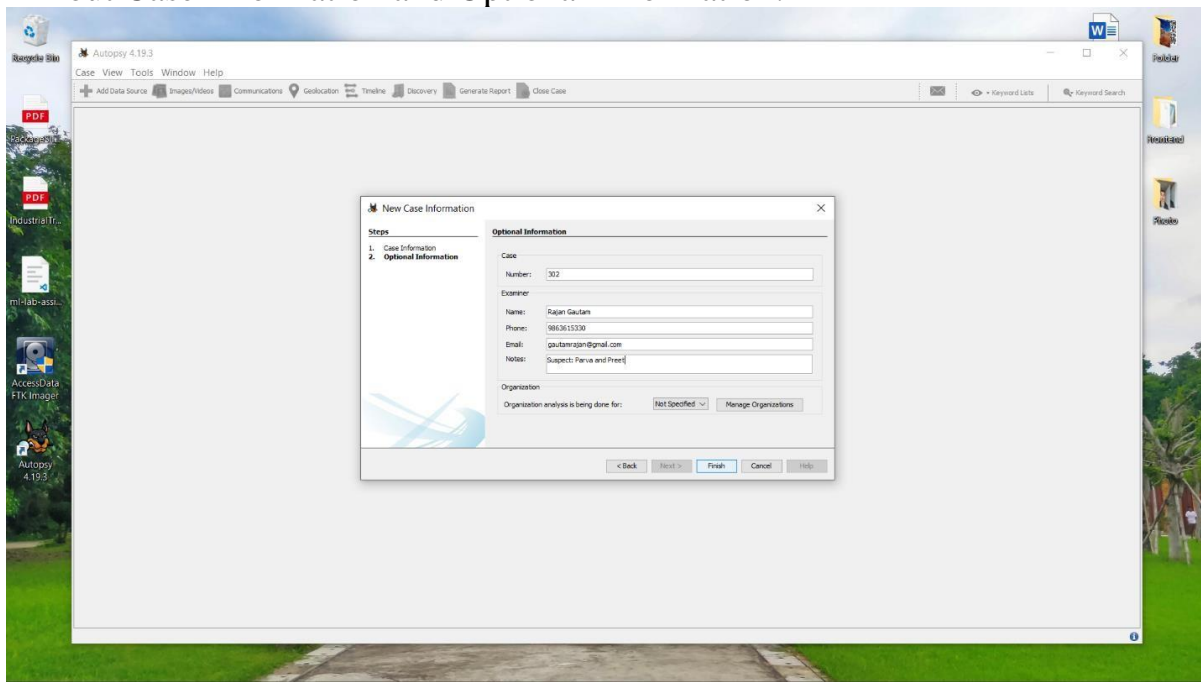
**Step 4: Open Autopsy and start working on it.**

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.

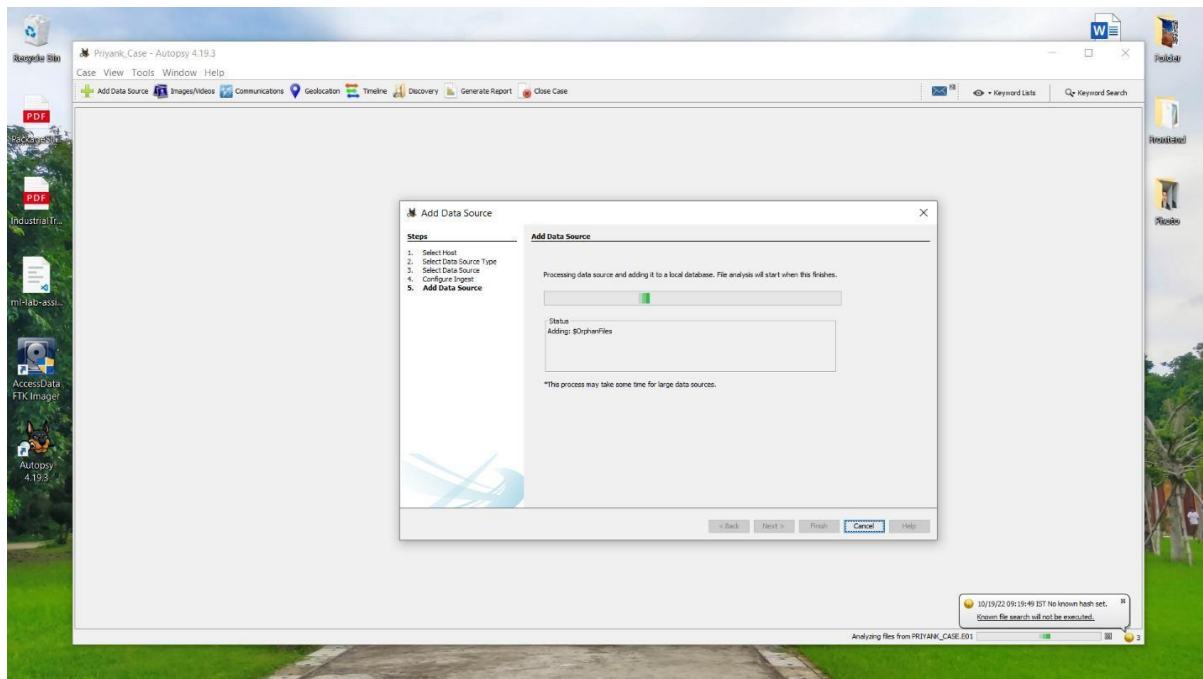


Figure 13 Autopsy

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

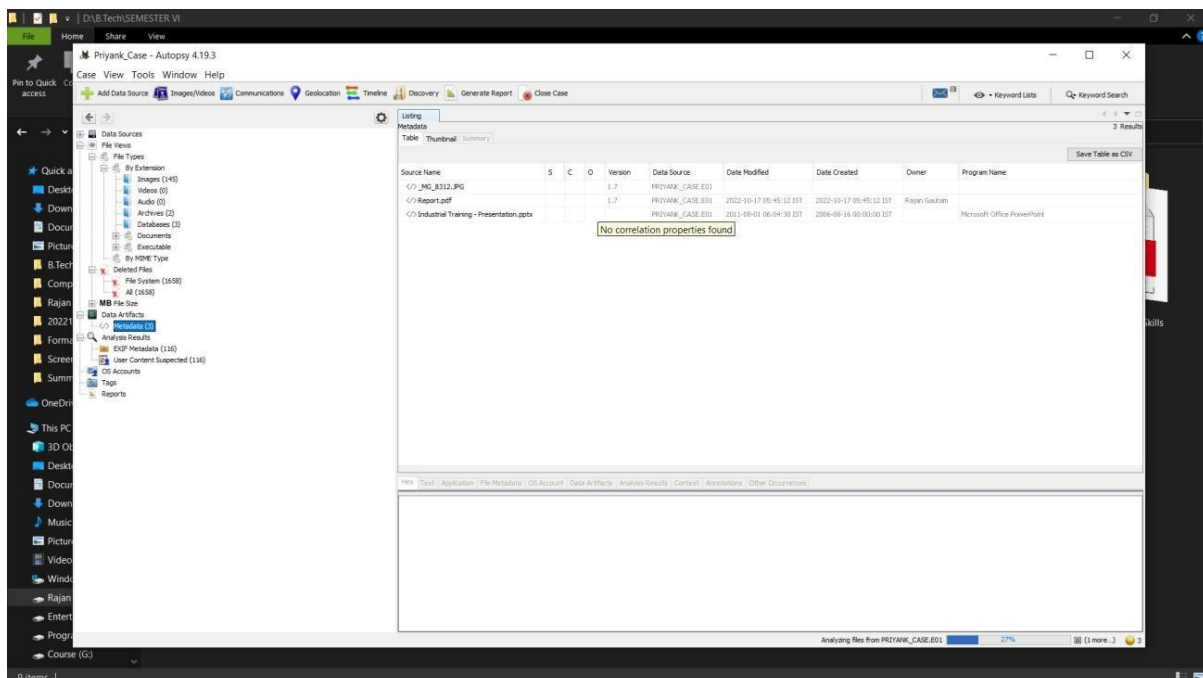


Figure 14 Autopsy



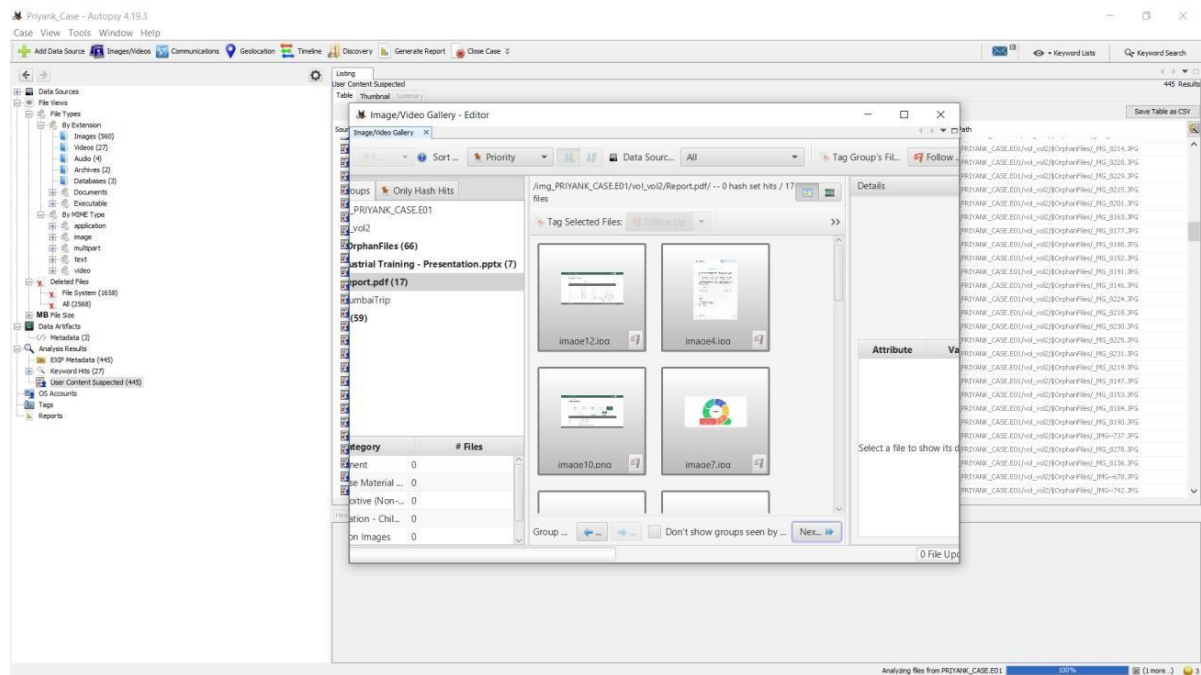


Figure 15 Autopsy

## 5. Click on Generate Report to generate Analysis Report.

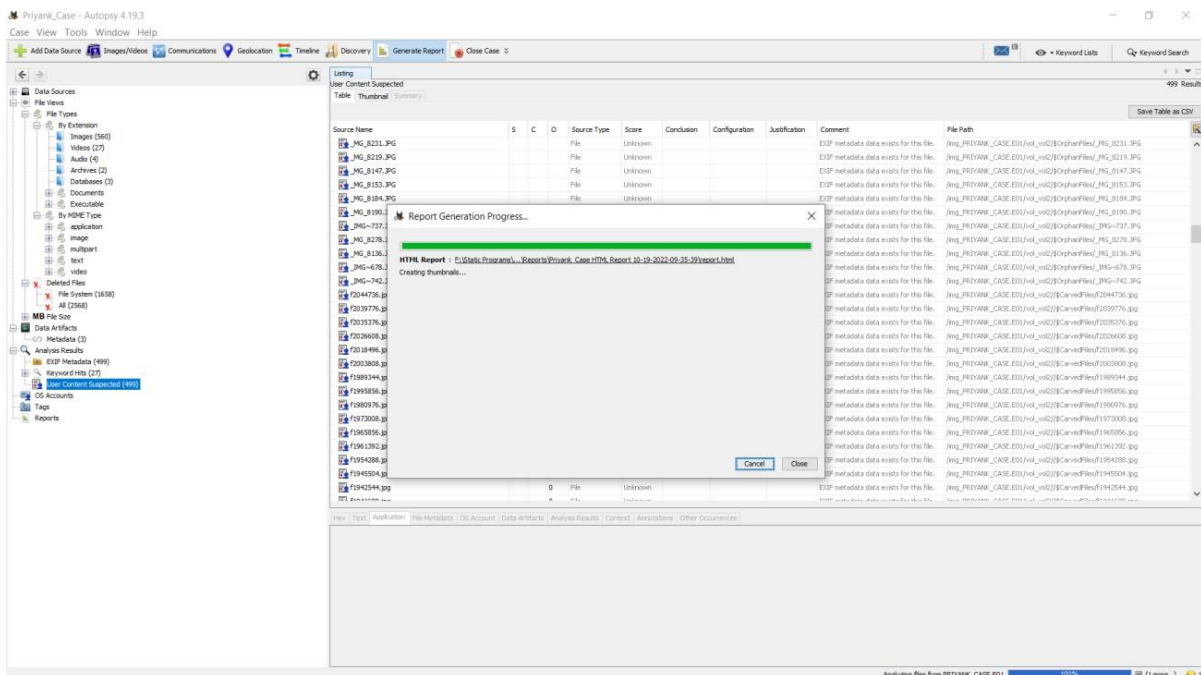


Figure 16 Autopsy

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

### Report Navigation

- Case Summary
- Data Source Usage (1)
- EXIF Metadata (499)
- Keyword Hits (27)
- Metadata (3)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- User Content Suspected (499)

### Priyank's Case

## Autopsy Forensic Report

**Warning, this report was run before ingest services completed!**

HTML Report Generated on 2022/10/19 09:35:40

Case: Priyank\_Case  
Case Number: 302  
Number of data sources in case: 1  
Notes: Suspect: Parva and Preet  
Examiner:

### Image Information:

PRIYANK\_CASE.E01

Timezone: Asia/Calcutta  
Path: F:\Static Programs\FTK Manager\PRIYANK\_CASE.E01

### Software Information:

Autopsy Version: 4.19.3  
Android Analyzer Module: 4.19.3  
Android Analyzer (aLEAPP) Module: 4.19.3

Figure 17 Autopsy

### Report Navigation

- Case Summary
- Data Source Usage (1)
- EXIF Metadata (499)
- Keyword Hits (27)
- Metadata (3)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- User Content Suspected (499)

### Priyank's Case

## EXIF Metadata

Date Taken	Device Manufacturer	Device Model	Latitude	Longitude	Altitude	Source
2022-08-12 00:12:20 IST	Apple	iPhone XS Max	23.024483333333333	72.60099722222222	42.98593902269247	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 00:12:22 IST	Apple	iPhone XS Max	23.024483333333333	72.60099722222222	42.98593902269247	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f2
2022-08-12 03:47:53 IST	Apple	iPhone XS Max	23.024666666666665	72.60130277777778	53.747280074603665	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 12:02:48 IST	Apple	iPhone XS Max	19.060630555555555	72.84130277777778	31.400608519269777	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 12:02:48 IST	Apple	iPhone XS Max	19.060630555555555	72.84130277777778	31.400608519269777	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 12:02:49 IST	Apple	iPhone XS Max	19.060605555555558	72.84129444444444	35.344792973651195	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 12:02:49 IST	Apple	iPhone XS Max	19.060605555555558	72.84129444444444	35.344792973651195	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 12:02:53 IST	Apple	iPhone XS Max	19.060580555555557	72.84130277777778	35.324713344718226	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 12:02:53 IST	Apple	iPhone XS Max	19.060580555555557	72.84130277777778	35.324713344718226	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 12:02:53 IST	Apple	iPhone XS Max	19.060580555555557	72.84130277777778	35.324713344718226	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 12:02:53 IST	Apple	iPhone XS Max	19.060580555555557	72.84130277777778	35.324713344718226	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 12:02:53 IST	Apple	iPhone XS Max	19.060580555555557	72.84130277777778	35.324713344718226	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 12:58:21 IST	Apple	iPhone XS Max	19.080663888888889	72.84566388888888	14.535368764920216	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 12:58:21 IST	Apple	iPhone XS Max	19.080663888888889	72.84566388888888	14.535368764920216	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 12:58:24 IST	Apple	iPhone XS Max	19.080636111111111	72.84566388888888	15.932068183726594	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 12:58:25 IST	Apple	iPhone XS Max	19.080636111111111	72.84566388888888	15.932068183726594	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 13:00:38 IST	Apple	iPhone XS Max	19.080680555555556	72.84511388888889	10.015454529006046	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 13:00:38 IST	Apple	iPhone XS Max	19.080680555555556	72.84511388888889	10.015454529006046	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 13:00:39 IST	Apple	iPhone XS Max	19.080697222222224	72.84512222222222	12.887371357122246	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 13:00:39 IST	Apple	iPhone XS Max	19.080697222222224	72.84512222222222	12.887371357122246	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 13:38:40 IST	Apple	iPhone XS Max	19.075305555555556	72.840775	13.506169062914244	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 13:38:40 IST	Apple	iPhone XS Max	19.075305555555556	72.840775	13.506169062914244	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 13:38:40 IST	Apple	iPhone XS Max	19.075305555555556	72.840775	13.506169062914244	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 13:38:41 IST	Apple	iPhone XS Max	19.075127777777778	72.84075277777778	13.110488727069038	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 13:38:41 IST	Apple	iPhone XS Max	19.075127777777778	72.84075277777778	13.110488727069038	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 13:38:41 IST	Apple	iPhone XS Max	19.075127777777778	72.84075277777778	13.110488727069038	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 13:38:41 IST	Apple	iPhone XS Max	19.075127777777778	72.84075277777778	13.110488727069038	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1
2022-08-12 13:38:41 IST	Apple	iPhone XS Max	19.075127777777778	72.84075277777778	13.110488727069038	/img_PRIYANK_CASE E01/vol_02/\$CarvedFiles/f1

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.