****

NAME: Sahil ashraf

REG. NUMBER: 11903730

ROLL NUMBER: 13

Submitted to: Navjot kaur

**1. Introduction**

1.1 Objective of the Project: This project aims to extract the website artifacts from various providers such as Firefox, edge and chrome using open source tool Autopsy and to find specific search terms on disk using autopsy forensic tool.

1.2 Description of the Project: Using Autopsy tool, the project extracts various web artifacts like bookmarks,history ,cache, auto fill passwords to gain insight into browsing habits and activities. In this project we have also used search option of Autopsy to find out specific search terms.

1.3 Scope of the Project: The project focuses on extracting various artifacts using Autopsy tool. It does not involve any modifications to the tool or other additional functionalities beyond the data extraction.We have also found oyt specifi search terms using the same tool.

**2. System Description**

2.1 Target System Description: The target system is a laptop running Windows 11 with Microsoft Edge as the default web browser.

2.2 Assumptions and Dependencies:

• Autopsy tool is installed and configured correctly on the target system.

• The target system is permitted to extract various artifacts, and it also has the necessary permissions.

• The target system has Microsoft Edge as the default web browser and contains relevant data in bookmarks, cache, visited websites,cookies, autofill forms etc.

2.3 Functional/Non-Functional Dependencies:

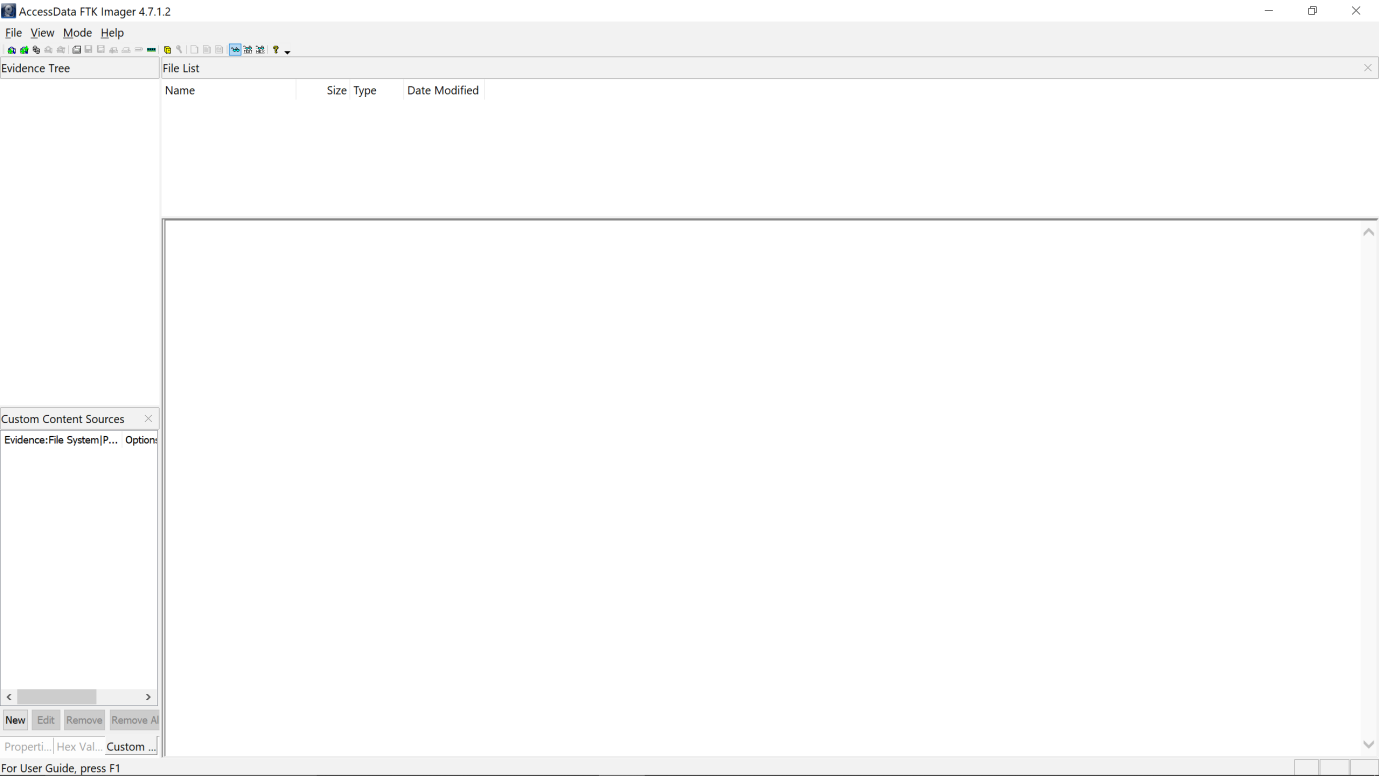
• Functional dependencies: Autopsy Tool is functional and capable of extracting artifacts from various browsers like edge, chrome , firefox.Autopsy’s search engine is also capable of finding out specific search terms so that we can check the information that we want and leave the rest.

• Non-functional dependencies: The effectiveness and accuracy of the analysis may be impacted by the calibre and completeness of the data that was gathered.

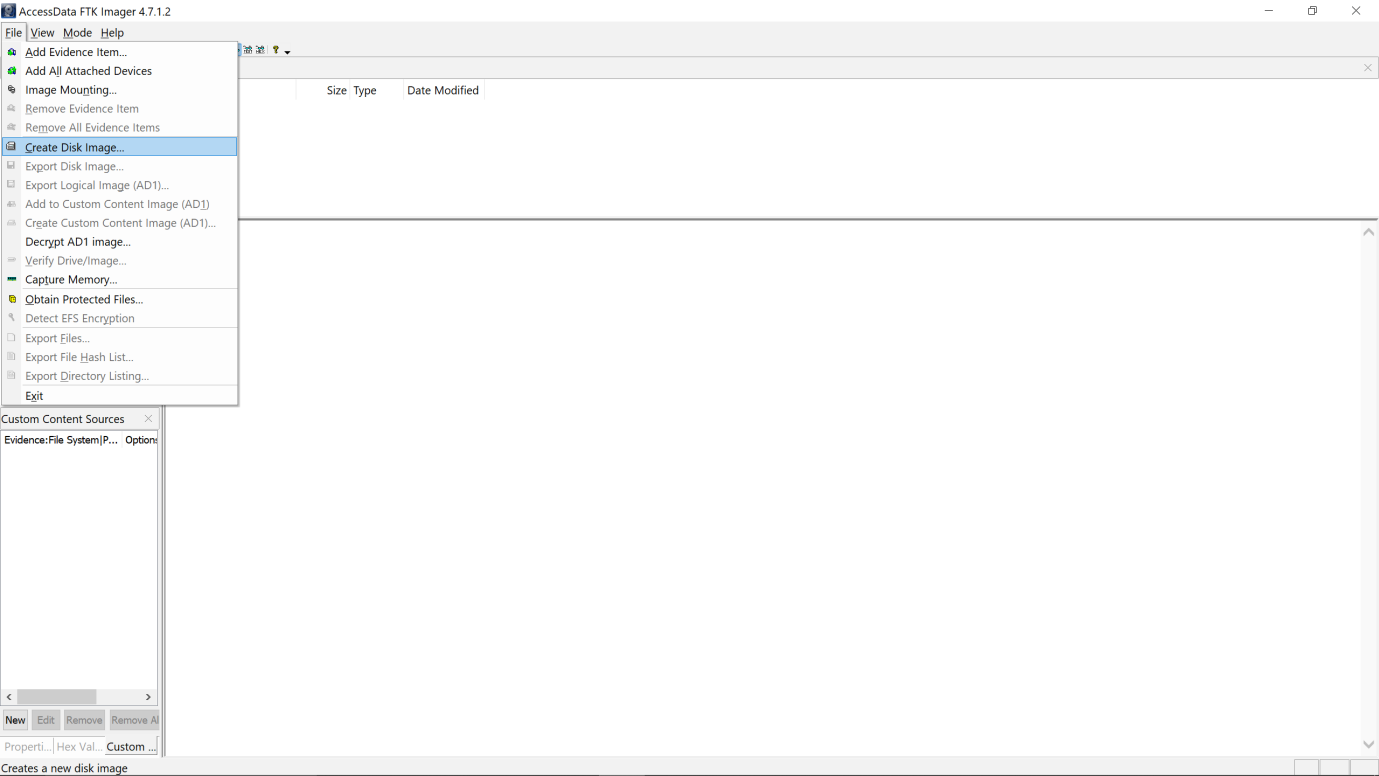
2.4 Data Set Used in Support of Your Project: The data set used in this project are various artifacts gathered using Autopsy tool.

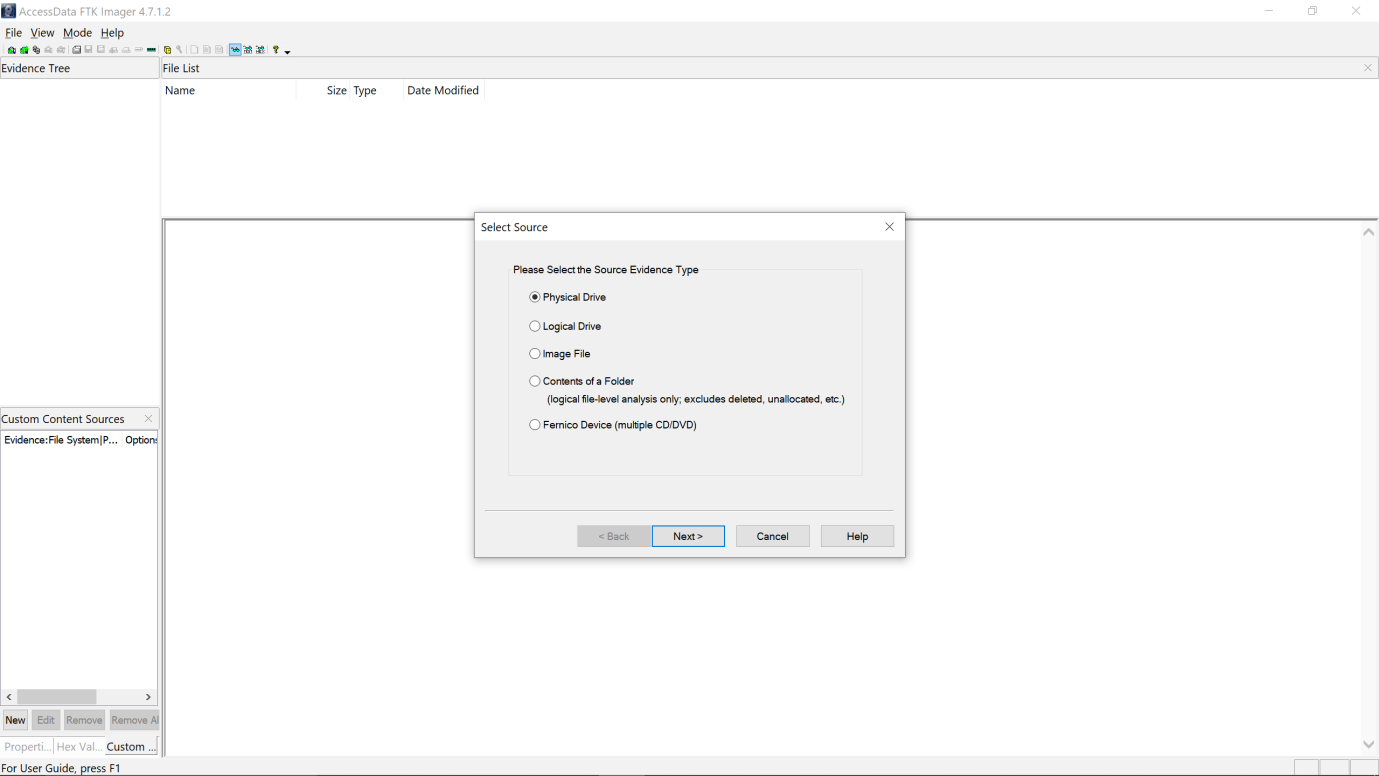
3. Analysis Report

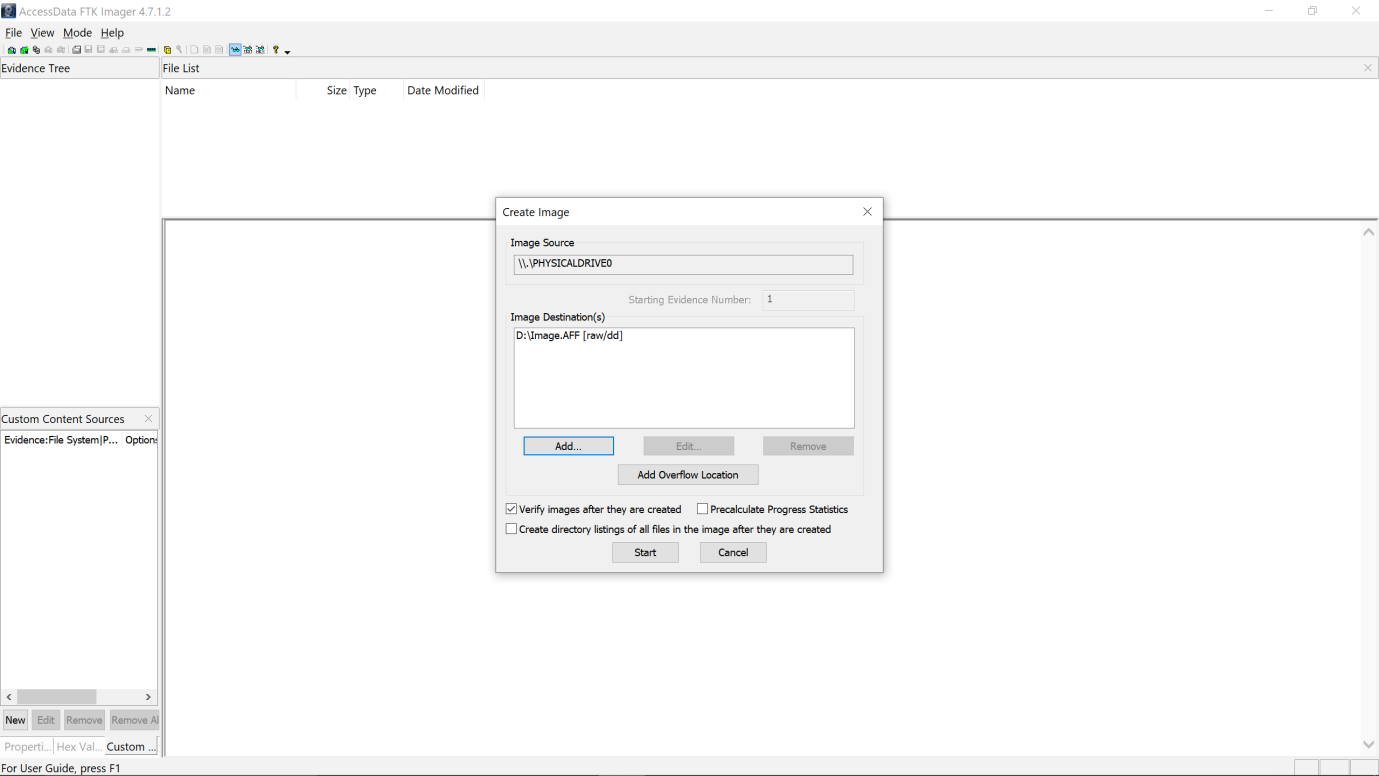
STEP 1: Open FTK Imager tool.

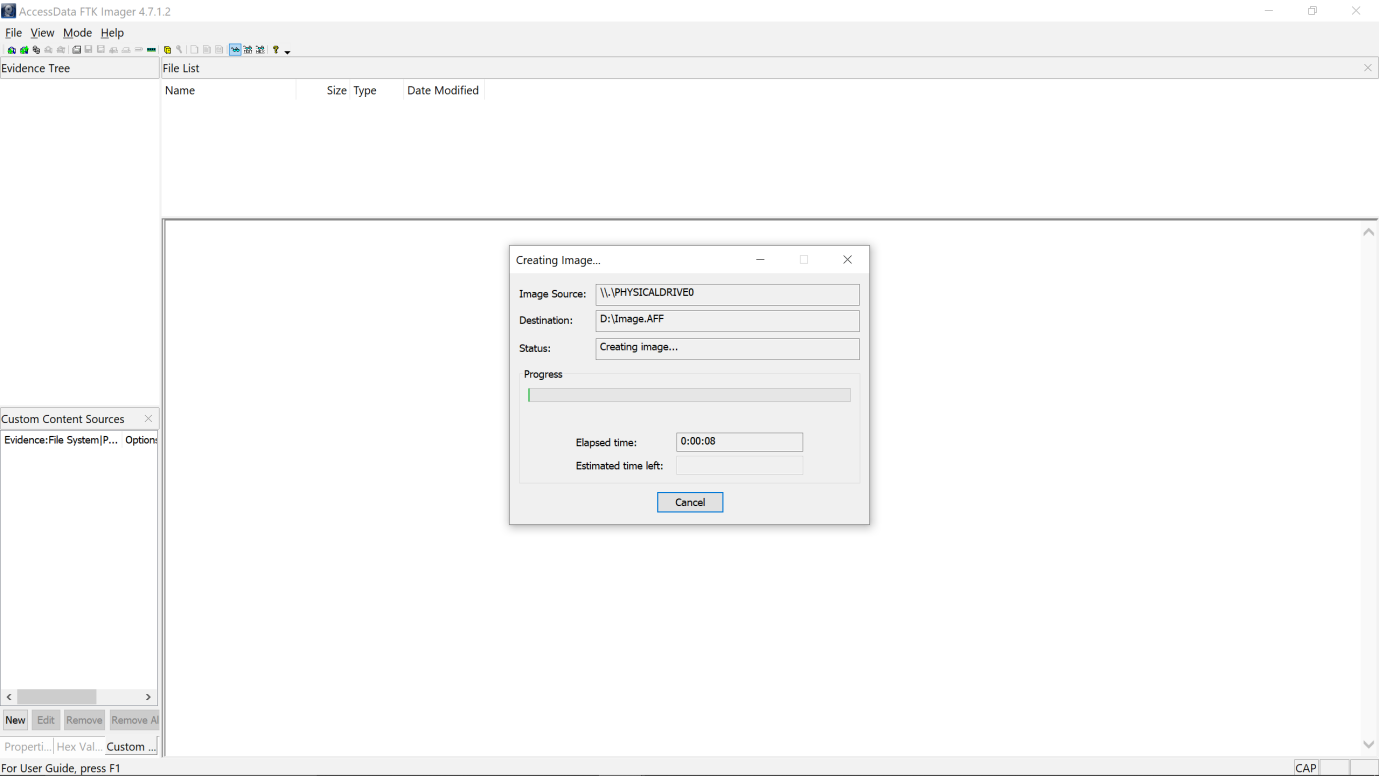


STEP 2: To create a hard disk image, select the file option and then select create disk image..

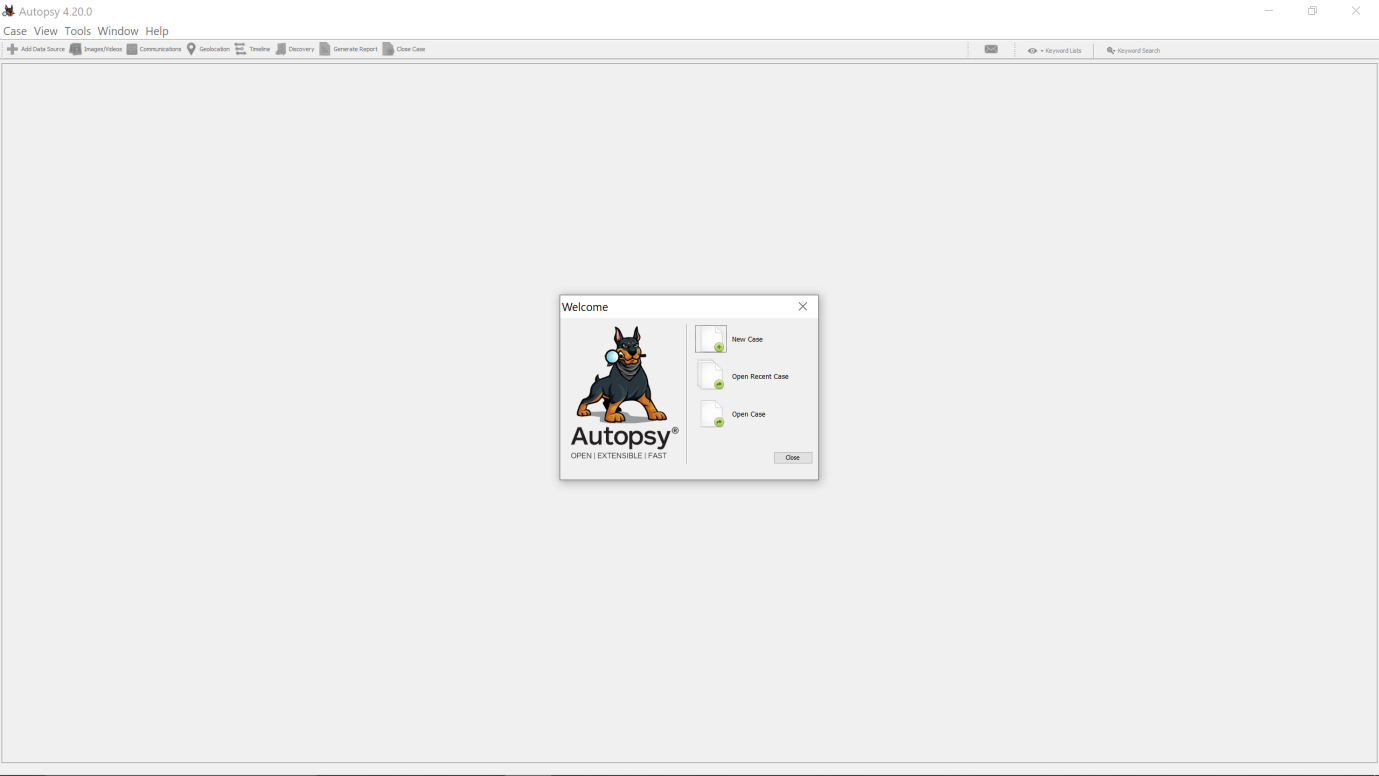


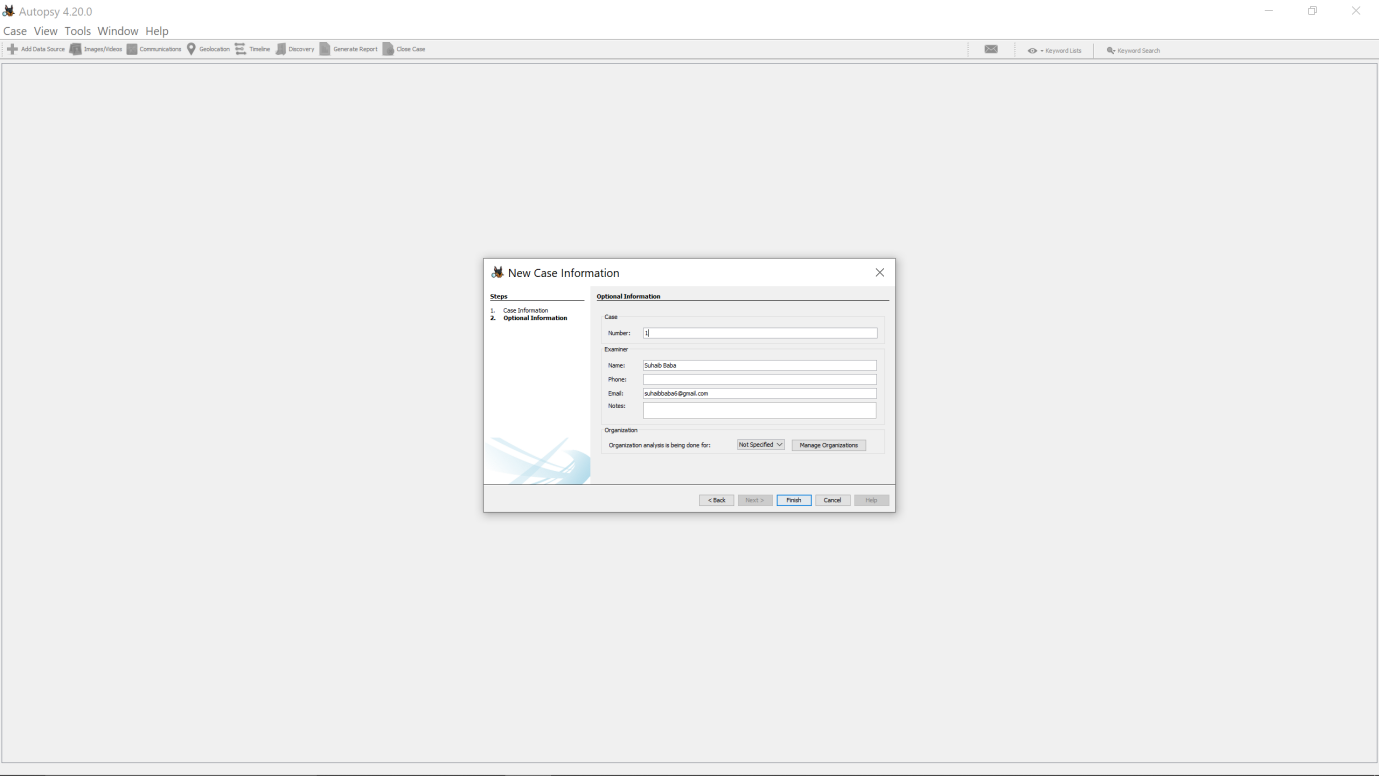
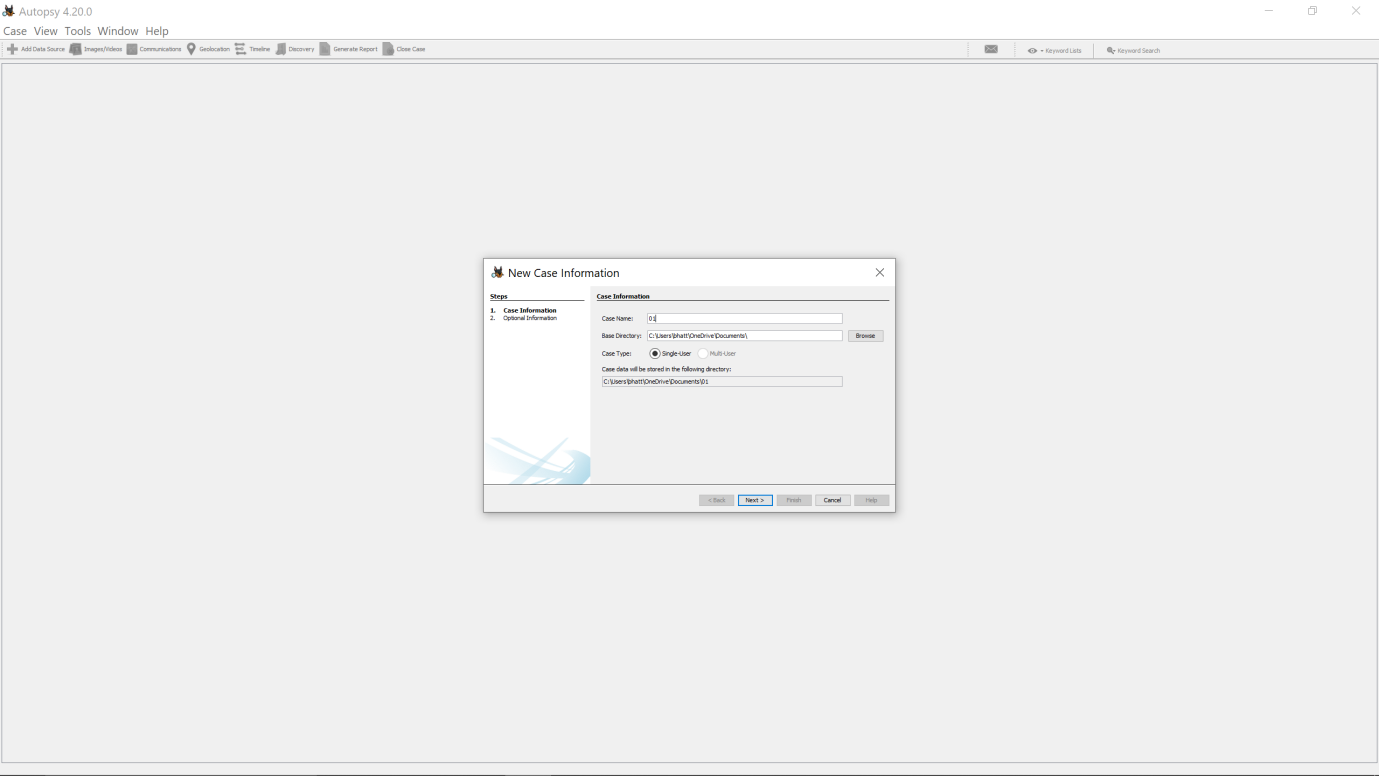
STEP 3: A new pop-up window appears, allowing you to select the source of evidence as physical drive.And then select the next option. 

STEP4: A new window appears, allowing you to select a disk to image and specify a destination location for the disk to be imaged. And then select the start option to begin the process.STEP5: Disk image creation has begun after selecting the Start option.

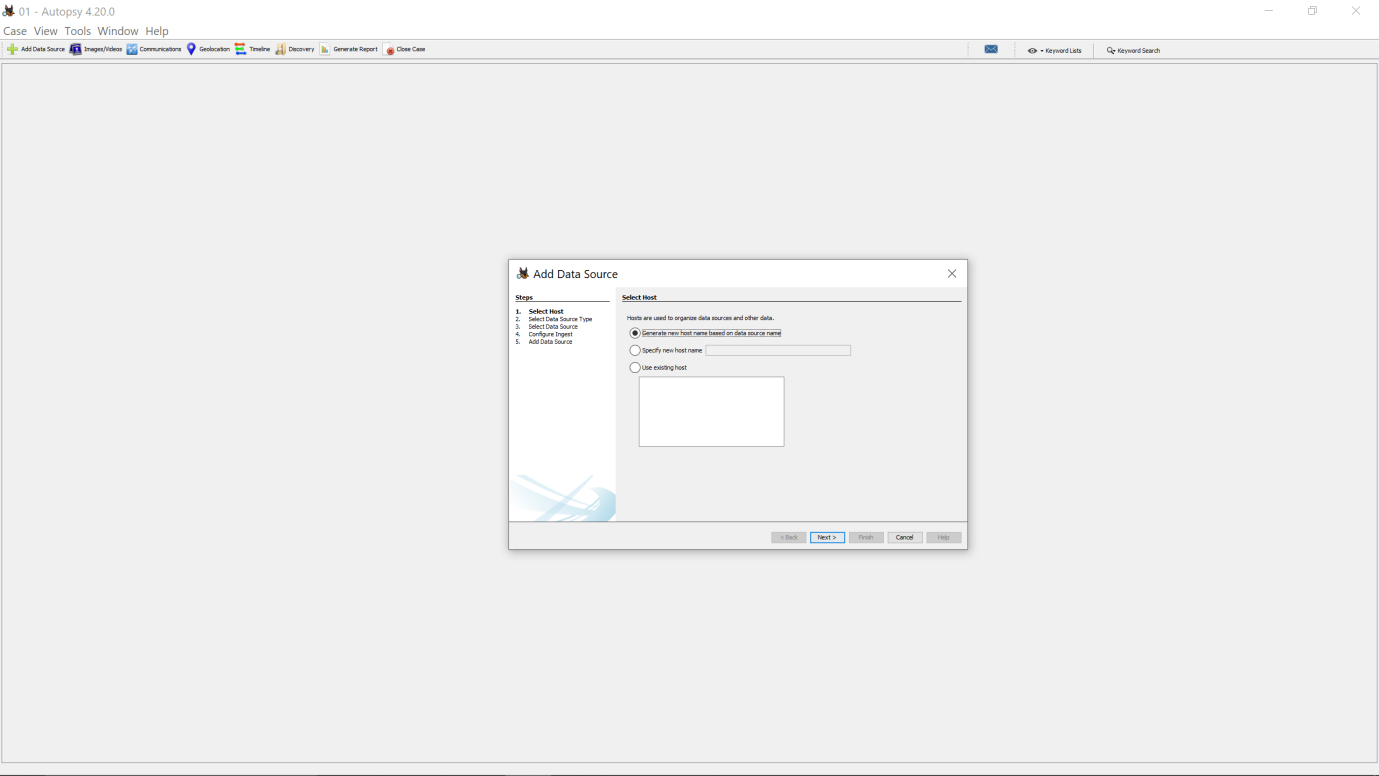
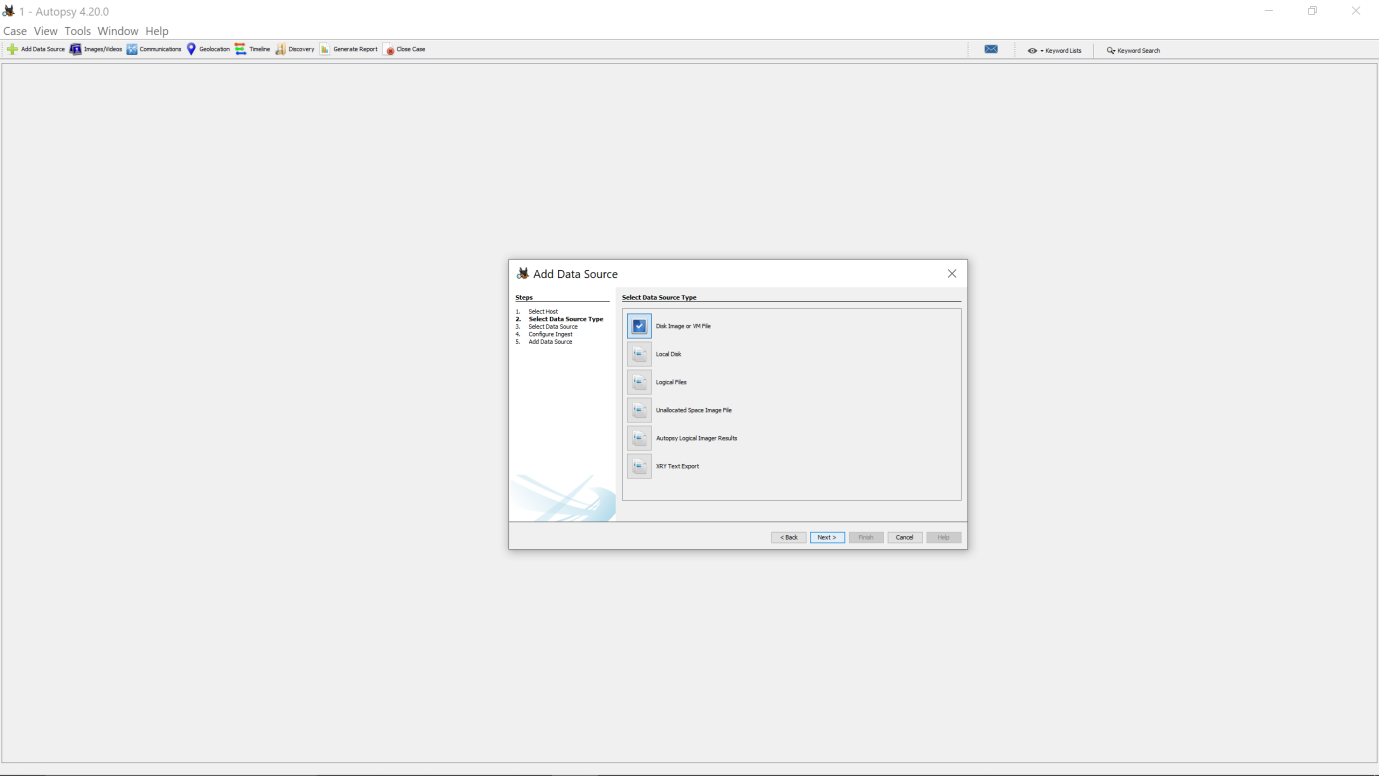


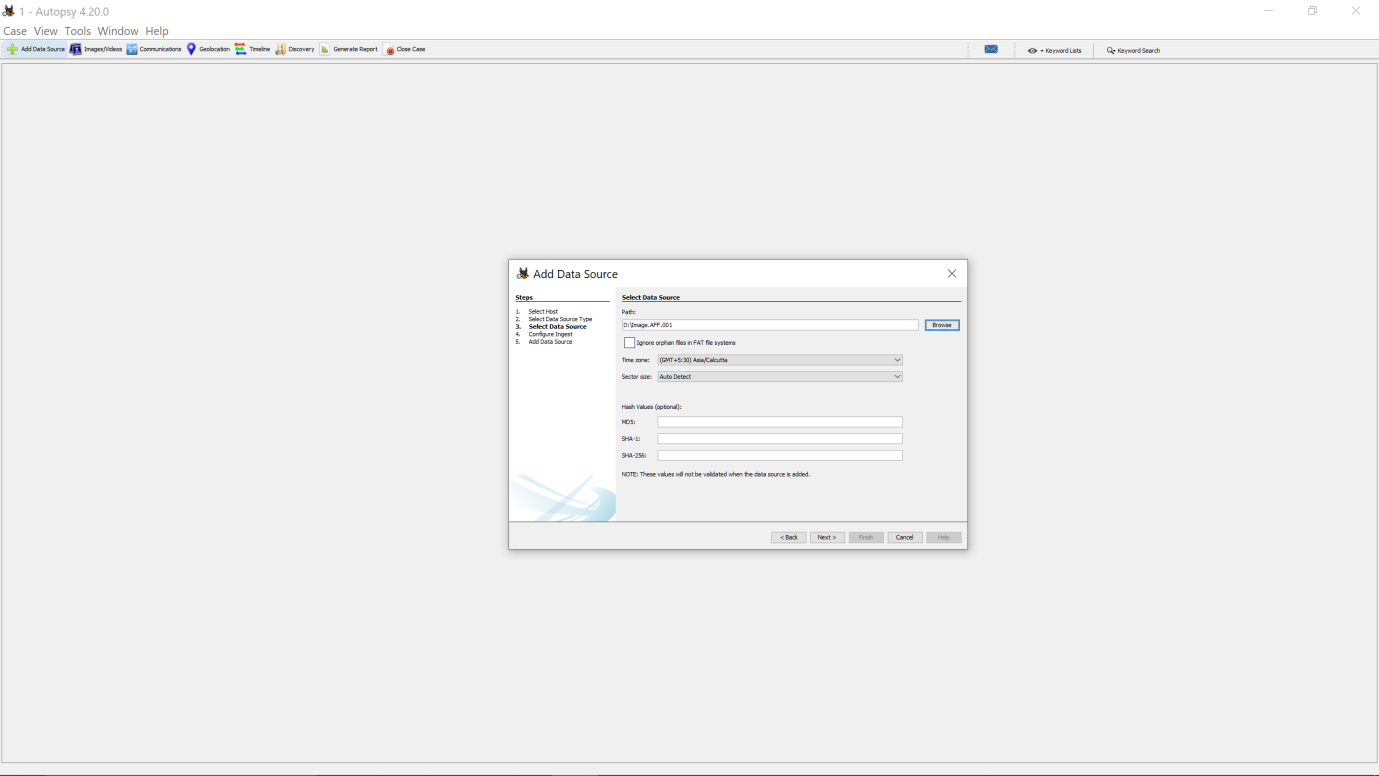
STEP 6: After creating the disk image, we must use the autopsy tool to capture and analyze the browser history, cache, bookmarks, and cookies. Now we must create a new case to collect data from an image file and add data like case name, case number, investigator name, email id, etc

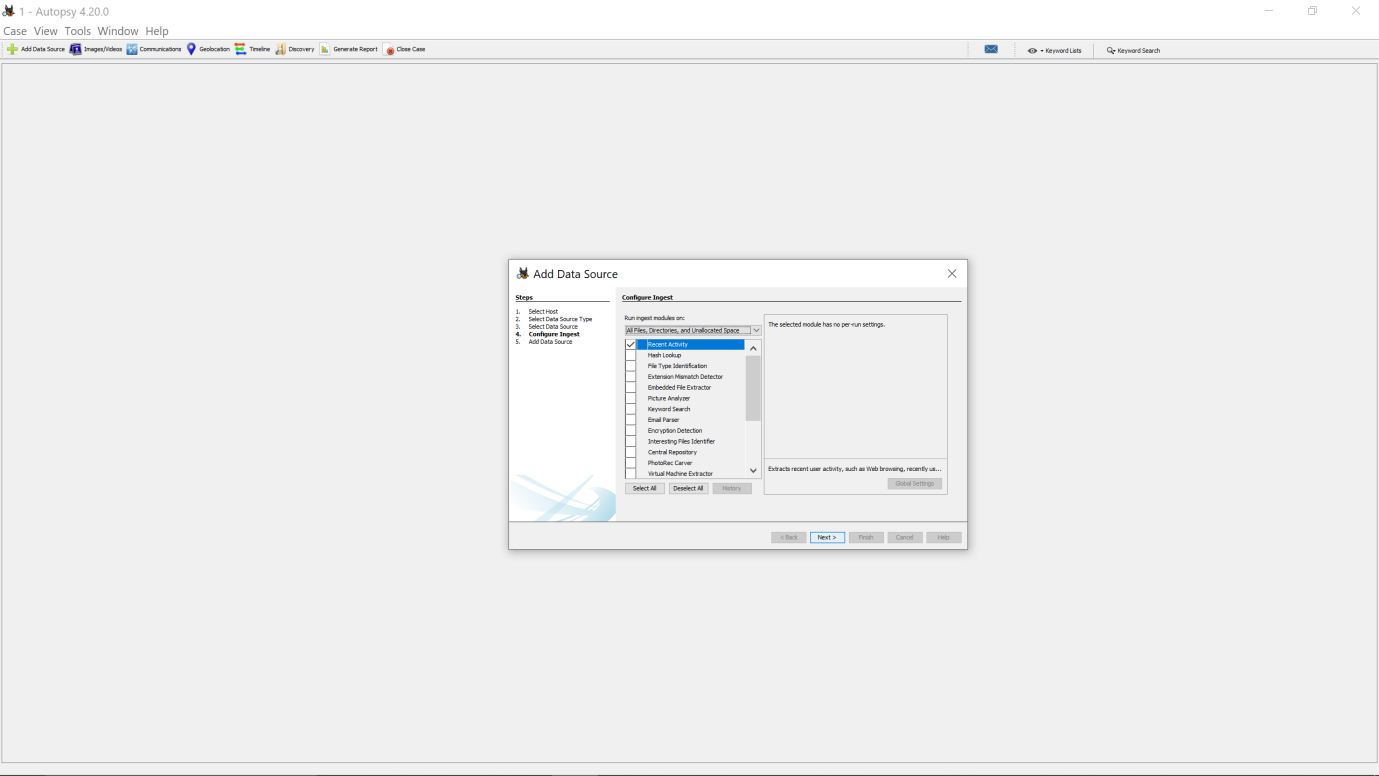


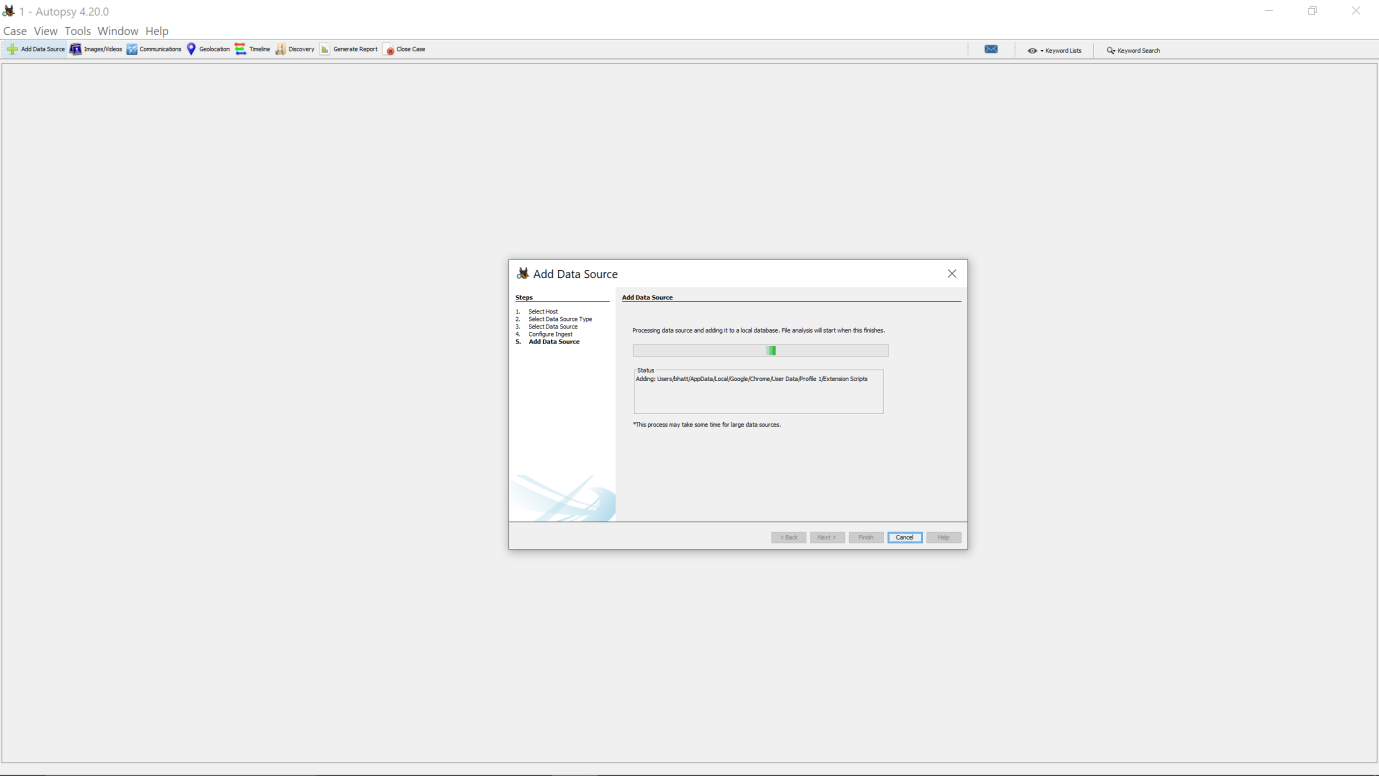


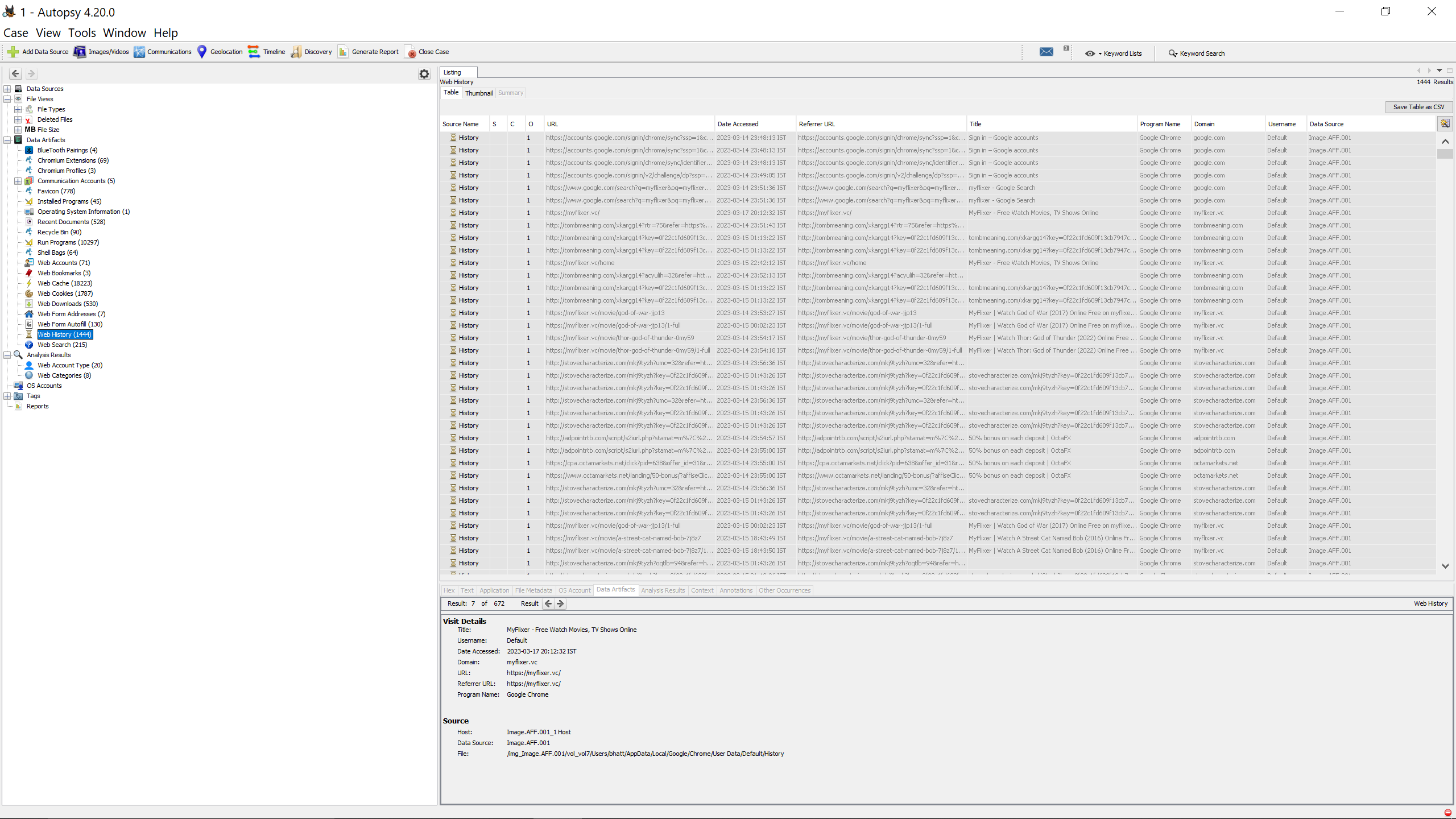
STEP7: After creating a new case, we must now add a data source.Now, click the next option to bring up a new window.

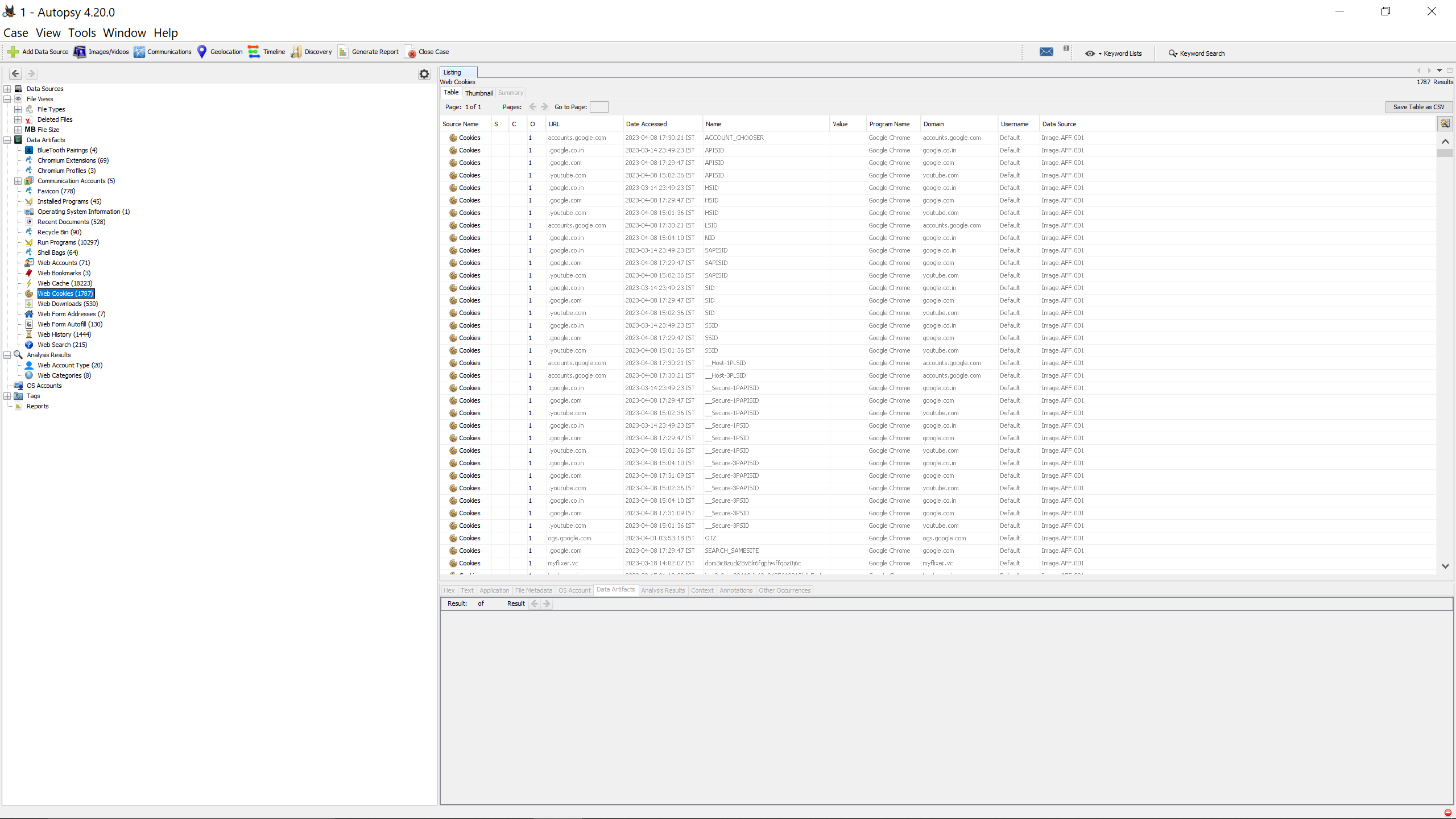
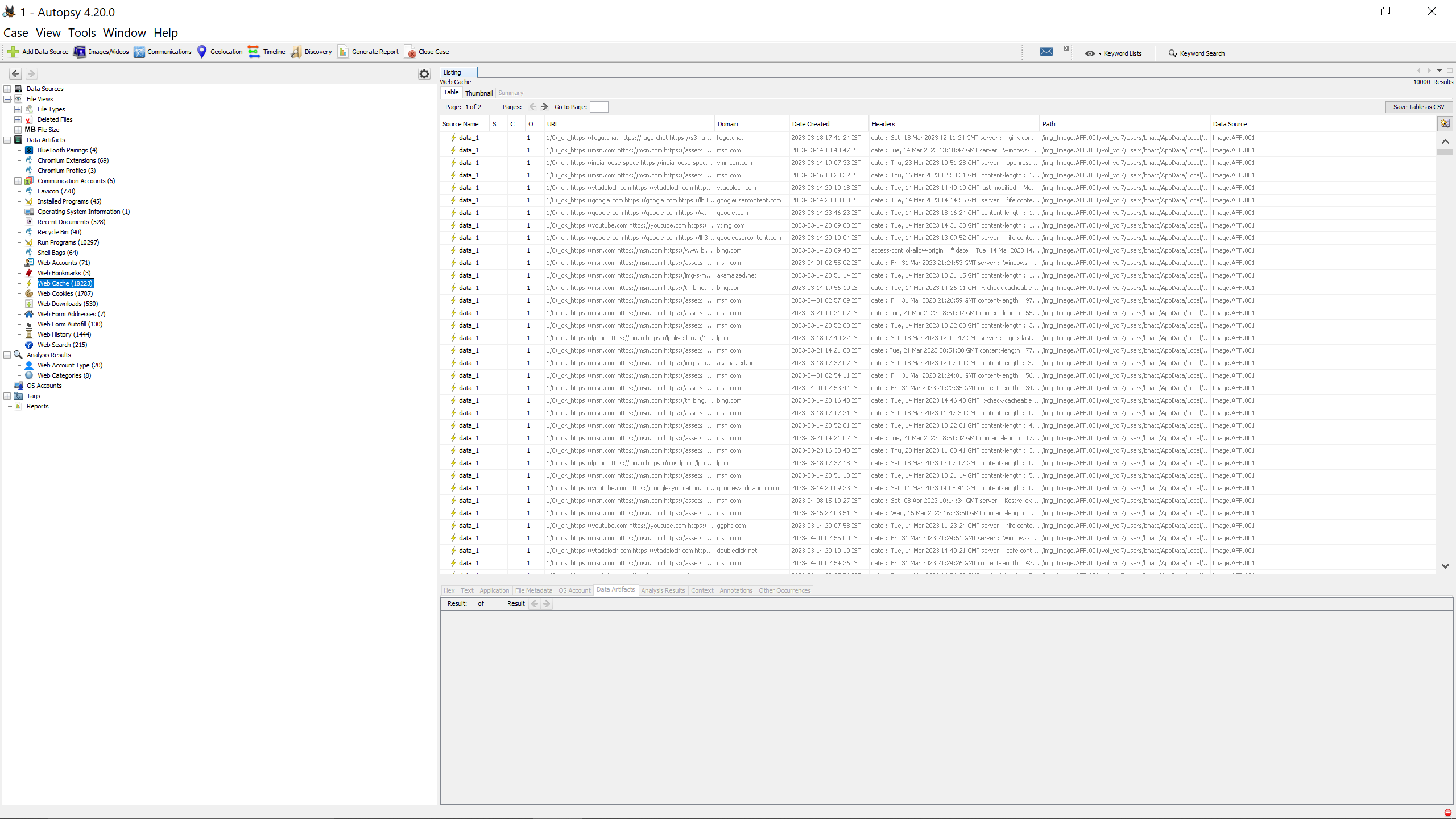
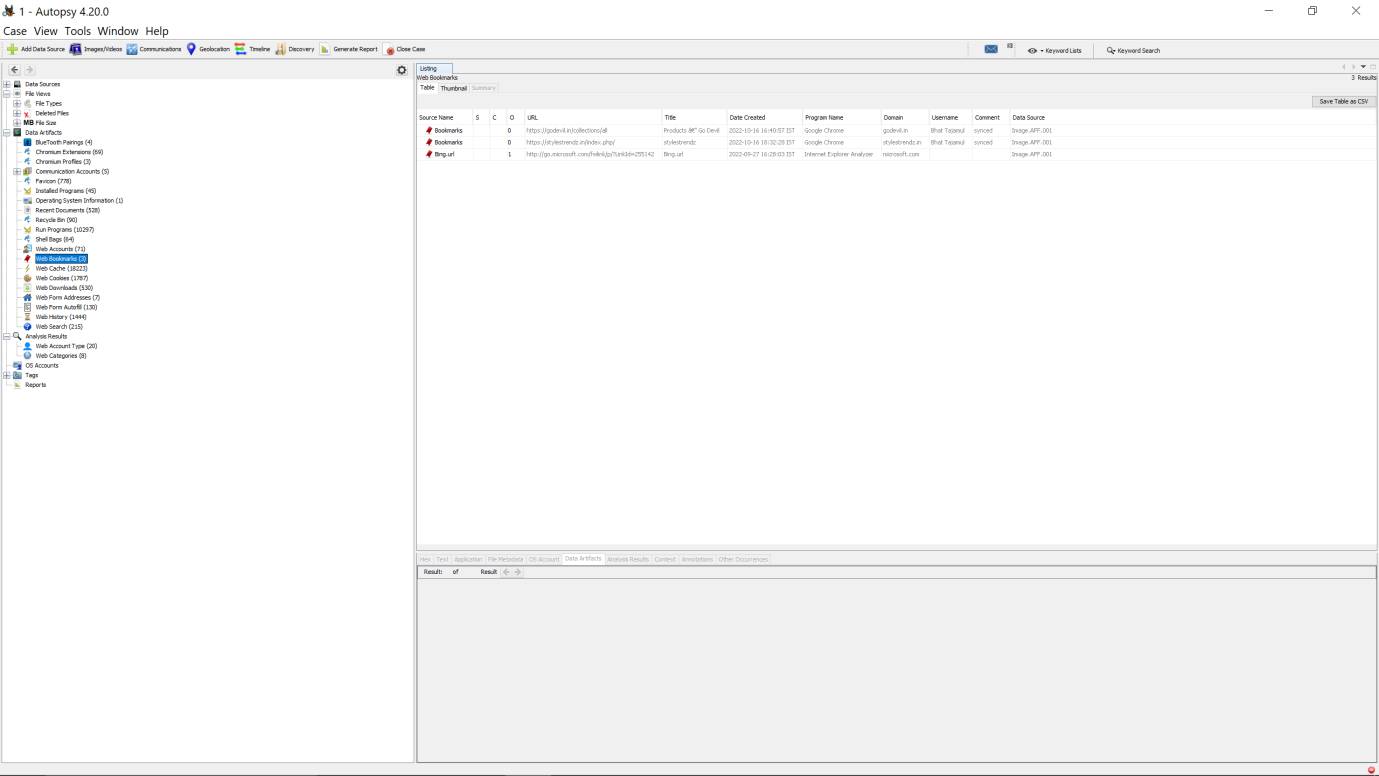
STEP8:Select the disk image option and then click next. STEP 9: Navigate to the disk image path and then click Next.

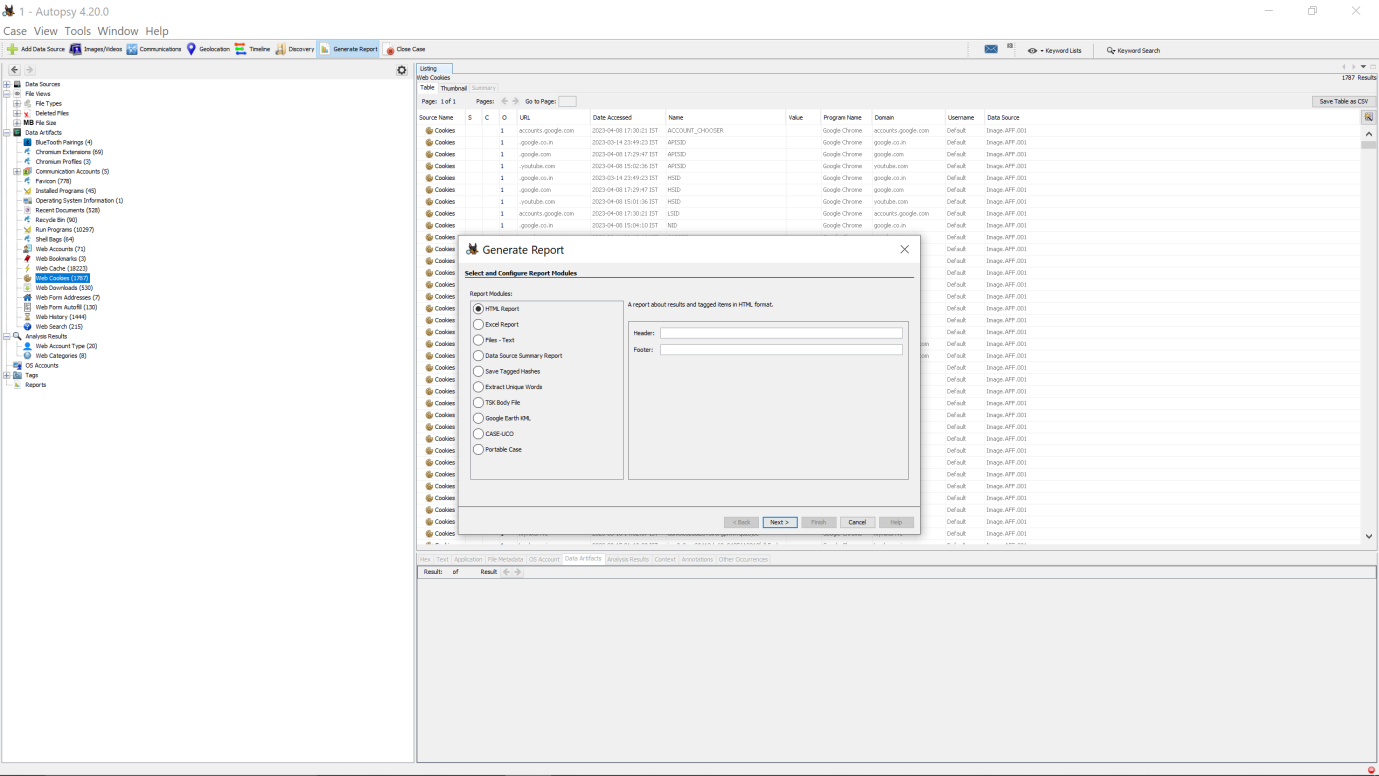
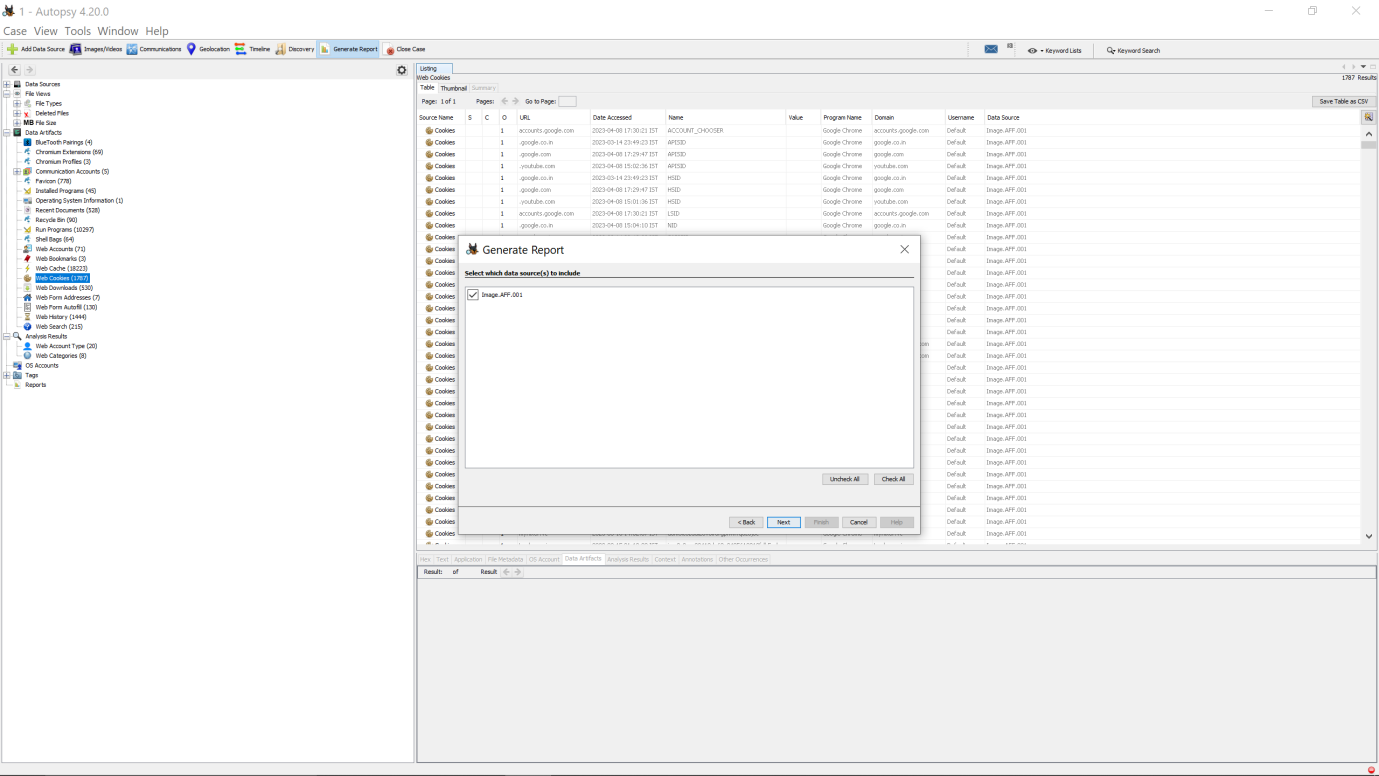
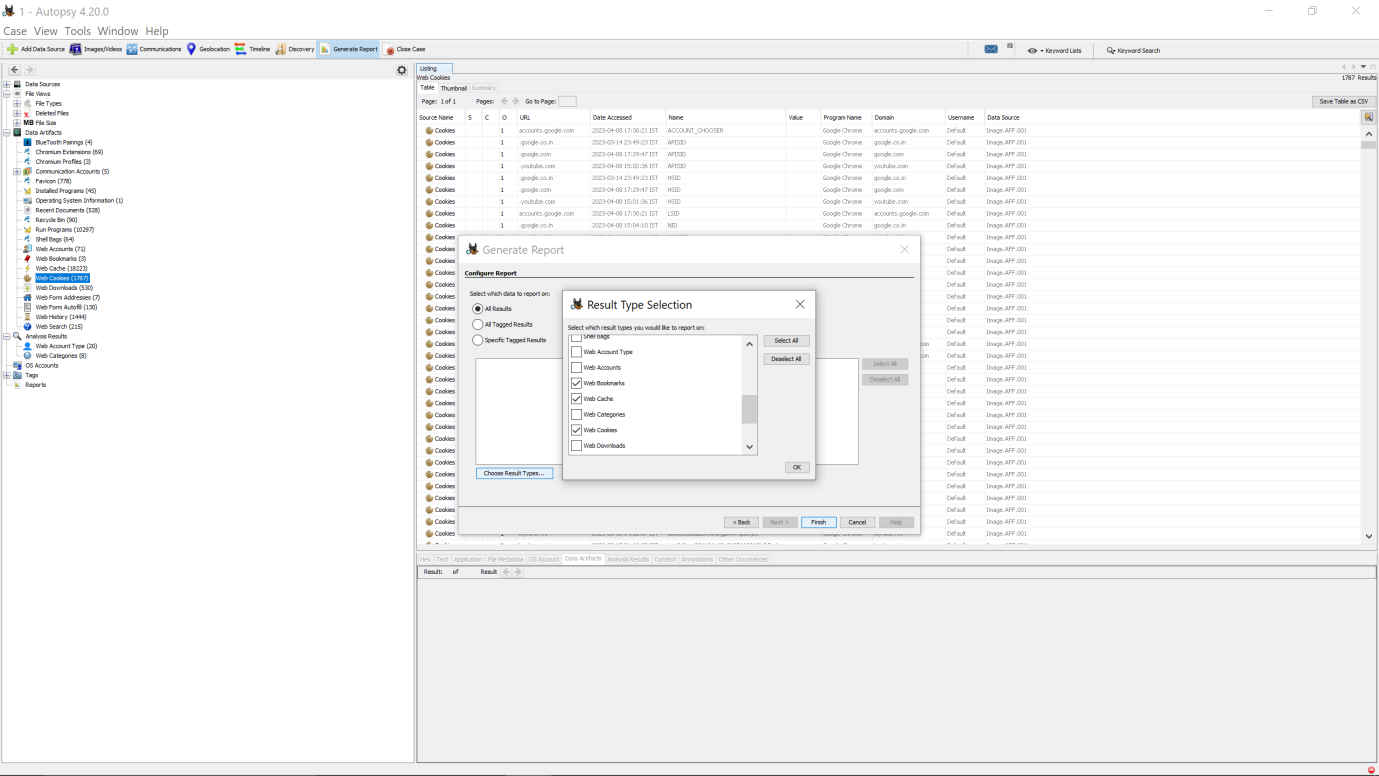
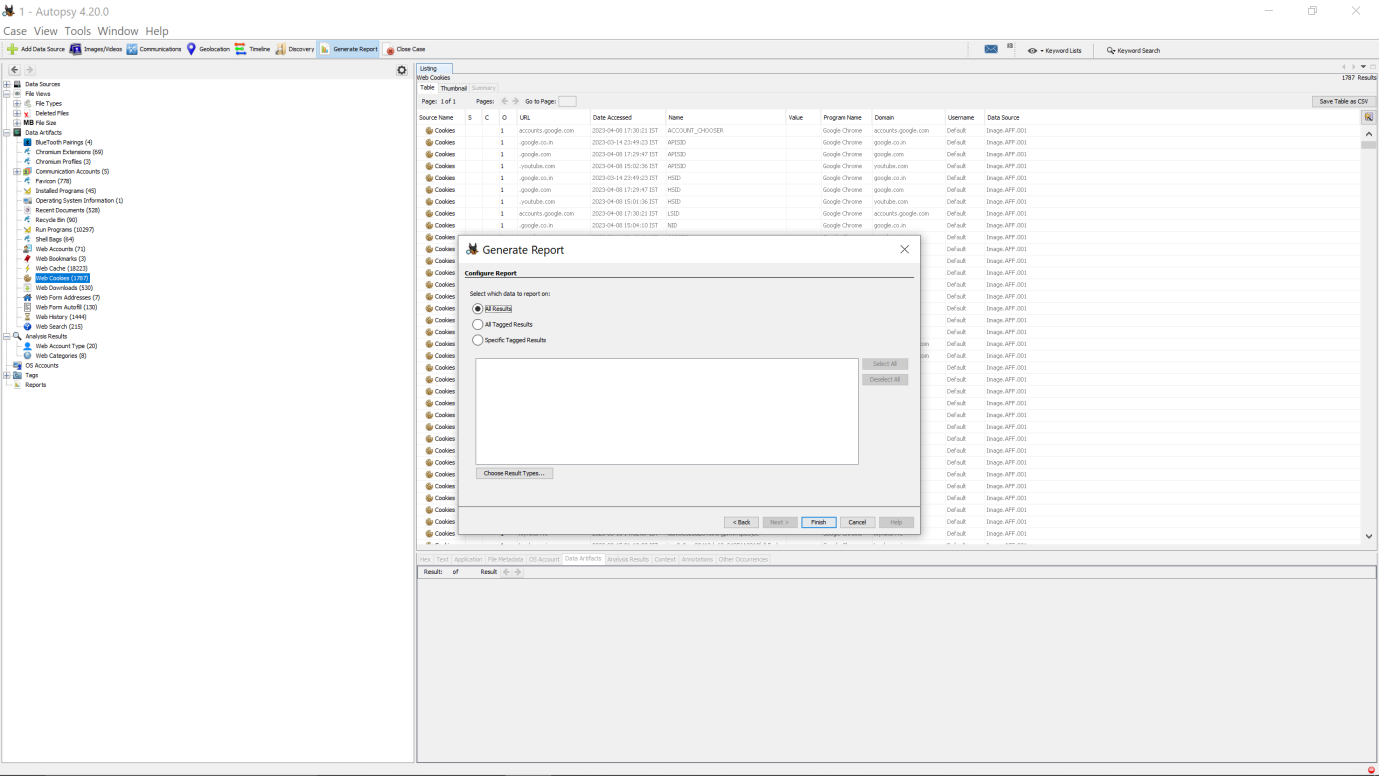
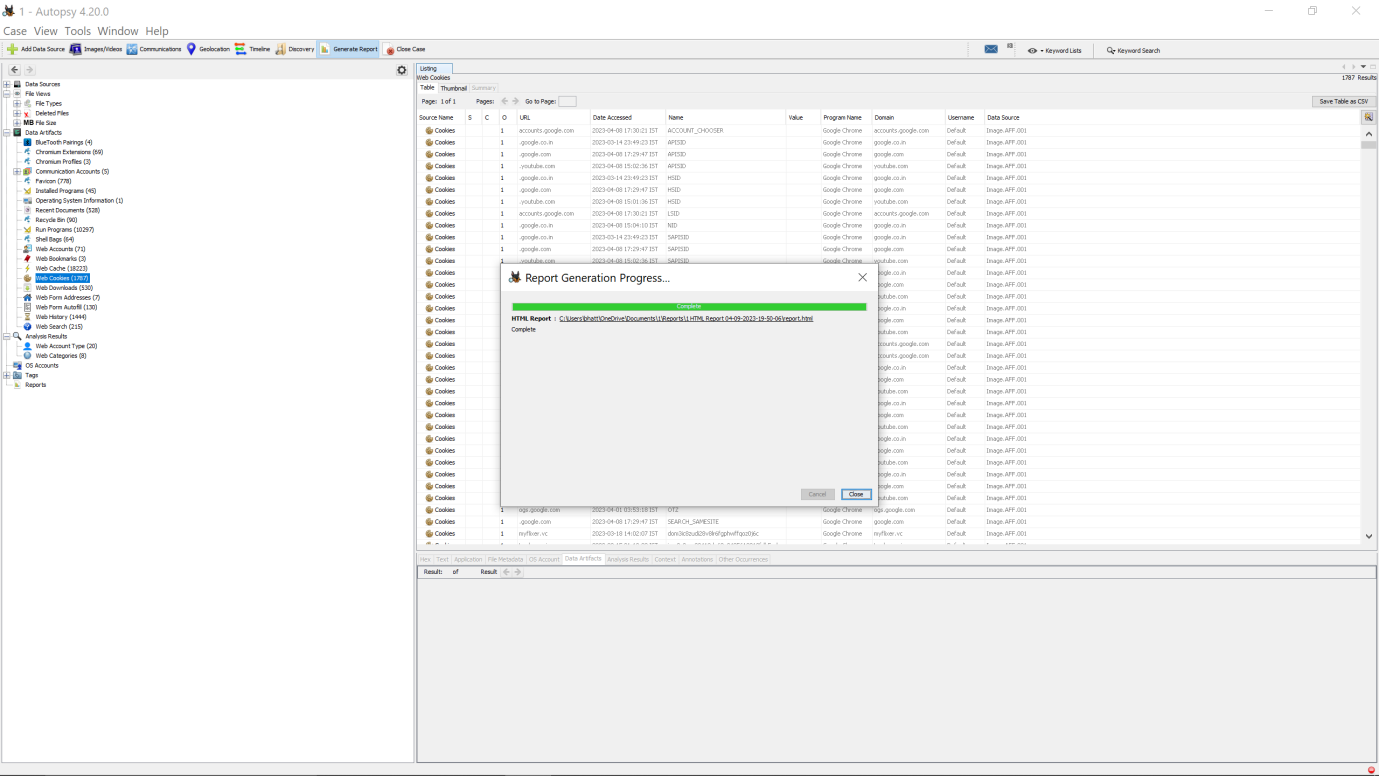
.

STEP10: Selecting the recent activity option to extract artifacts like browser history, cache, cookies, and bookmarks. And then click next. STEP 11: Now that the data source is being processed and added to the local data.  After it is completed click on the finish option

.STEP12:We can now examine all the artifacts we required.

.

STEP 12: To create the report file in the desired format, click the generate report option.Then click next option.

STEP13: Click on the image file and then click next. STEP14: Click on all result option and then click on choose result types to select which result types we want on our report. STEP15: Finally, the report has been generated. 

Now to find out the specific search terms using autopsy we will use the following steps:

Select the "Keyword Search" module from the left-hand menu.

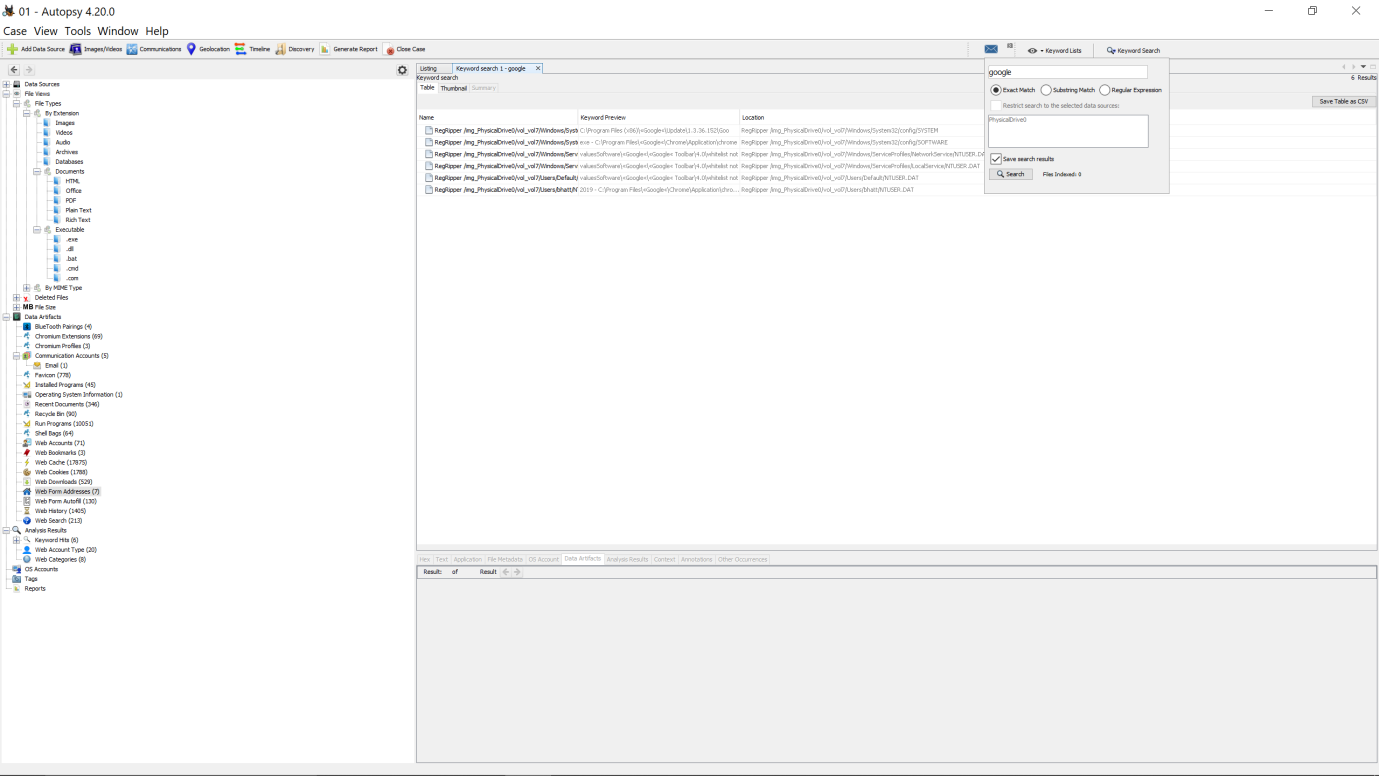
In the "Keyword List" tab, click on the "Add" button to add the specific search terms you want to search for.

You can further customize the search settings by selecting various options such as "Case Insensitive," "Whole Word," "Regex," etc.

Click on the "Start" button to initiate the search.

Autopsy will now search for the specific search terms across the disk image or mobile device and will display the search results in the "Keyword Hits" tab.

You can further analyze the search results by clicking on each hit and viewing the corresponding file or artifact in the "File Details" or "Artifact Details" tabs.



In the above picture we have searched “google” and it shows all the artifacts related to google on the screen

4. Reference/Bibliography:

• https://www.autopsy.com/

1. GitHub Link: Link to the GitHub repository containing the project files and report