

Lovely Professional University

INT 301: Open-Source Technologies

**A Project report on** “Extracting the website artifacts from various browsers and finding out the specific search terms on disk using Autopsy forensic tool.”

**Faculty**: Rajeshwar Sharma - 29484

**Name**: Nitin Jaiswal

**Reg No**: 11905741

**Roll No**: 55

**Section**:KE009

1. **Introduction**

In recent years, the use of digital devices has become more prevalent in our daily lives. With this increased usage, there has been a corresponding increase in cybercrime. Cybercriminals use digital devices to commit various crimes, such as identity theft, fraud, and cyberstalking, among others. Digital forensics is the process of collecting, analyzing, and preserving electronic evidence found on digital devices to investigate and solve such crimes. [1]

One of the key areas of focus in digital forensics is the extraction of website artifacts. Website artifacts are traces of digital footprints that users leave behind while browsing the internet. These artifacts can provide valuable evidence in digital forensic investigations, as they can help investigators establish a timeline of a user's internet activity and identify potential motives for cybercrime. Web browsers, such as Firefox, Edge, and Chrome, are the primary tools that users use to access the internet. These browsers store various artifacts related to web browsing activities, such as browsing history, cookies, and passwords. Extracting these artifacts from web browsers is a crucial step in digital forensic investigations, as they can provide valuable insights into a user's online behavior. [2]

Moreover, identifying specific search terms is another crucial aspect of digital forensics. Search terms are the keywords that users enter into search engines while browsing the internet. By identifying specific search terms, investigators can gain insight into the user's interests, preferences, and potential motives for cybercrime. Autopsy, a digital forensics tool, has a feature called Keyword Search, which allows investigators to search for specific search terms on a disk or phone

* 1. **Objective**

The objective of this project is to extract website artifacts from various web browsers, such as Firefox, Edge, and Chrome, and identify specific search terms using the Autopsy forensic tool. The project aims to demonstrate the process of extracting website artifacts and identifying specific search terms to gain valuable insights into a user's online behavior. The project also aims to highlight the importance of digital forensics in investigating cybercrime and providing evidence to solve such crimes. Through this project, we aim to enhance our understanding of digital forensics and its role in cybersecurity.

* 1. **Description**

The project involves extracting website artifacts from three popular web browsers, Firefox [3], Edge [4], and Chrome [5], and identifying specific search terms using the Autopsy forensic tool. The first step of the project is to collect data from the local disk that contains the web browsing history of the user.

Once the data is collected, the next step is to extract website artifacts from the web browsers. The process of extracting artifacts involves locating the files where the artifacts are stored and exporting them into a readable format. The artifacts that can be extracted from web browsers include browsing history, bookmarks, cookies, downloads, form history, and passwords.

The next step of the project is to identify specific search terms using the Autopsy forensic tool. Autopsy is an open-source digital forensic tool that enables investigators to search for specific keywords or regular expressions in a disk image. The Keyword Search feature of Autopsy allows investigators to search for specific search terms and generate a report of the search results. [6]

The project also involves analyzing the extracted artifacts and search results to gain insights into the user's online behavior. The analysis can help investigators establish a timeline of the user's internet activity and identify potential motives for cybercrime. The project aims to demonstrate the importance of digital forensics in investigating cybercrime and providing evidence to solve such crimes.

* 1. **Scope**

The project focuses on digital forensics and its role in investigating cybercrime. The project will demonstrate the importance of digital forensics in gathering electronic evidence from digital devices and analyzing that evidence to solve cybercrimes.

The project's scope also includes the use of Autopsy, an open-source digital forensic tool, to extract website artifacts and identify specific search terms. The project will demonstrate how Autopsy can be used to search for keywords or regular expressions in a disk or phone image, enabling investigators to generate a report of the search results.

The project's scope does not include the collection of data from a physical device or any illegal or unethical activity. The project only focuses on the process of extracting website artifacts and identifying specific search terms using the Autopsy forensic tool to demonstrate the importance of digital forensics in investigating cybercrime.

1. **System Description**

To perform the website artifact extraction and search term identification using Autopsy forensic tool, the following system requirements are necessary:

Hardware Requirements:

* Processor: 2 GHz or faster
* RAM: 4 GB or more
* Hard Disk Space: 500 MB or more of free space
* Internet connection (for downloading and installing software)

Software Requirements:

* Operating System: Windows 7 or later, Linux (Ubuntu, Debian, Fedora, CentOS), or macOS 10.10 or later
* Autopsy Forensic Browser: version 4.19 or later
* Mozilla Firefox: version 20 or later
* Microsoft Edge: version 80 or later
* Google Chrome: version 20 or later
* Disk or Phone Image: A disk or phone image containing the web browsing history of the user.

It is important to note that Autopsy forensic tool is a resource-intensive application, and the system requirements may vary based on the size of the digital device image being analyzed. [7] It is recommended to have a higher configuration system for analyzing larger data sets. Also, it is crucial to have sufficient storage space to store the extracted website artifacts and search results generated by the Autopsy forensic tool. [8]

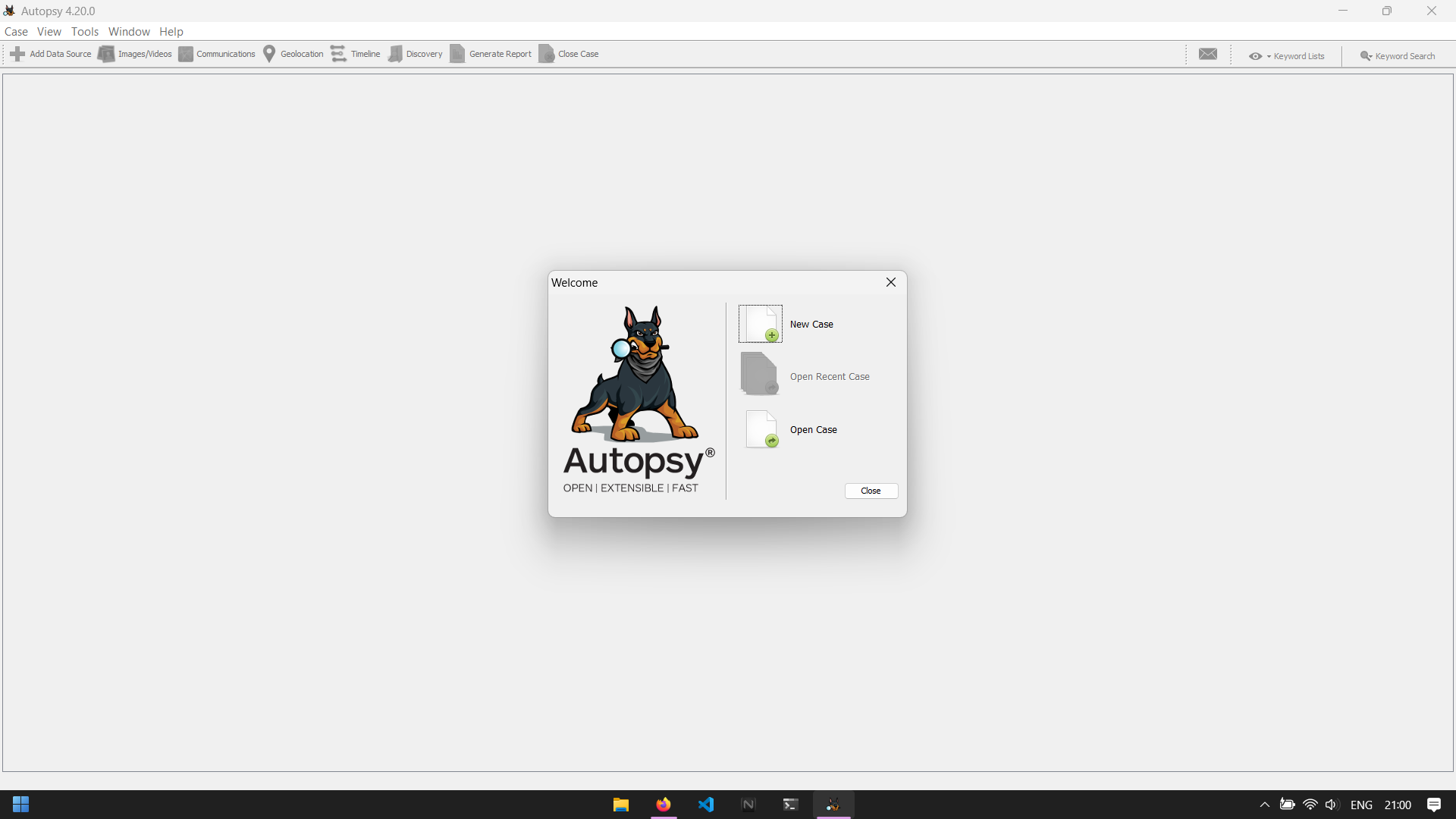
1. **Analysis Report**

**3.1 Following are the steps to extract the data using Autopsy for first-time users:**

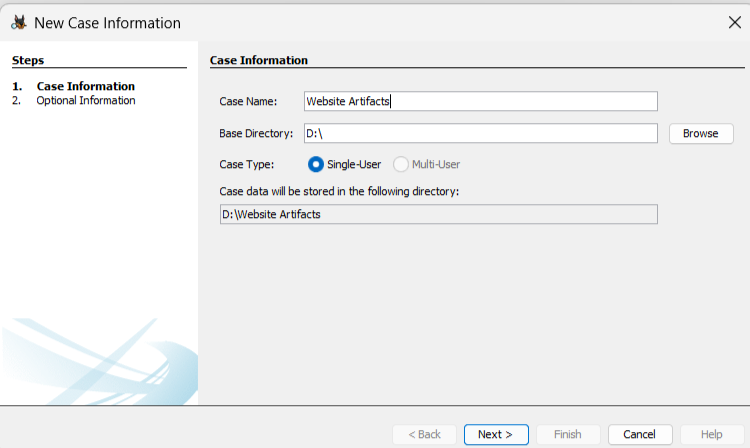
1. First, we run Autopsy as administrator since for reading the disk, admin permission is required. [9]



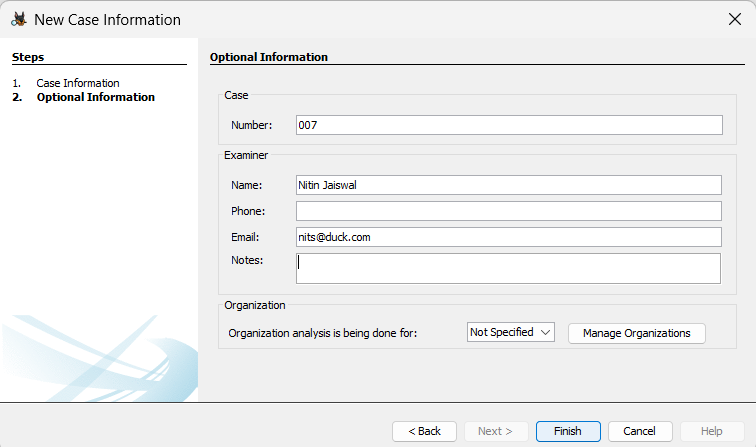
1. After running the Autopsy software with Admin privilege following dialog box will appear, we have to create a case but if you have a previous case that you have saved somewhere you can open it. Since we are working on it for the first time we'll click on **New case.**



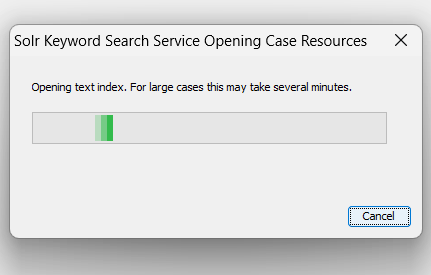
1. Now we need to name our case, here we have named it “Website Artifacts”. We must also specify the base directory where all the information will be stored. It is important to note that the base directory must be different from the disk we are about to analyze. Since we are analyzing the C disk, we’ve chosen D partition as the base. [10]



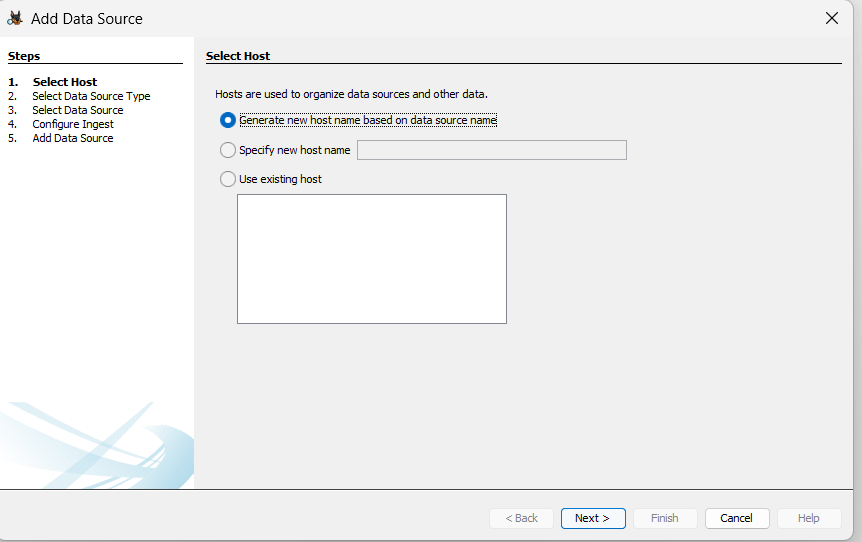
1. The case number along with other details is optional.



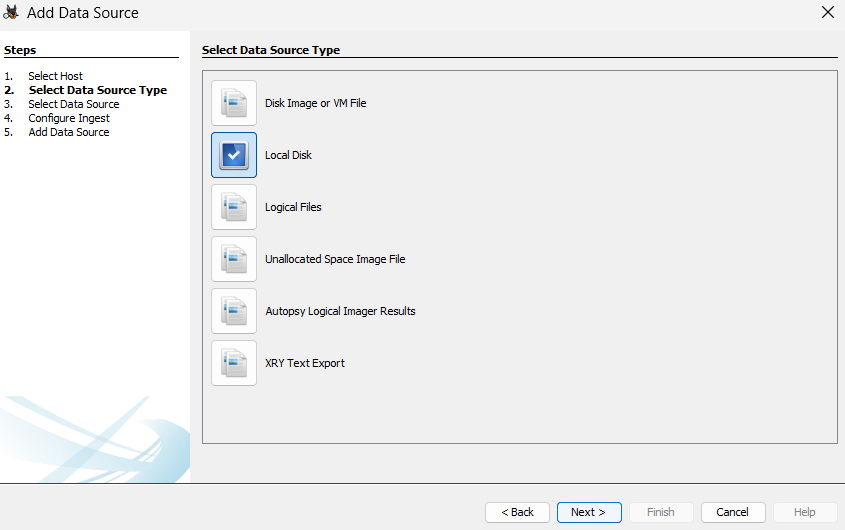
1. After clicking on Finish, it will take a moment and a new case will be created.



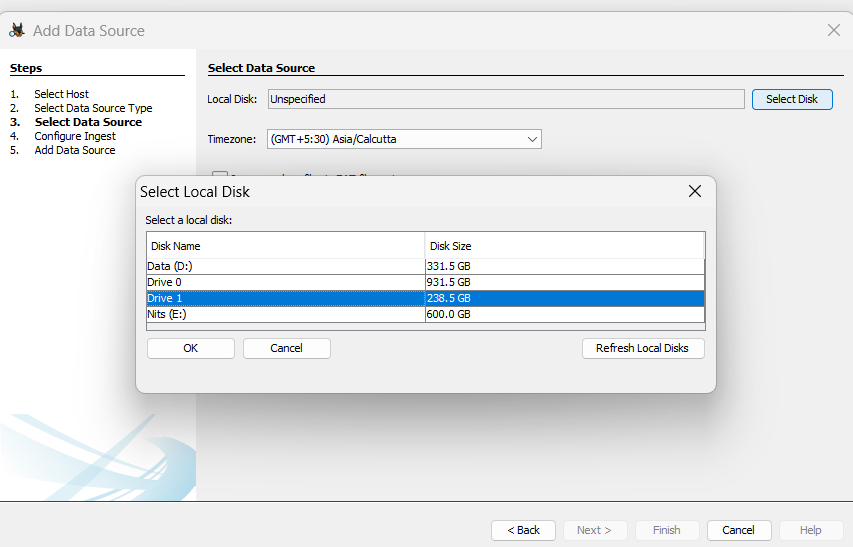
1. Now we must provide a data source for the new case created. First, we need to select a Host. You can either Generate a host name or specify it yourself. Here we have selected the former.



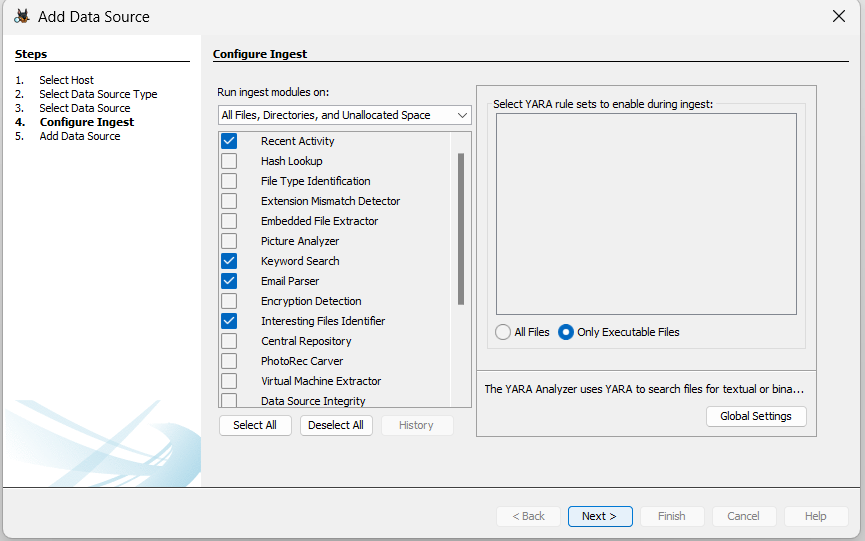
1. After selecting the option, you will see various choices for disk images. If you already have an image file on your computer, you can create a disk image using different software, such as FTK Imager. Since we are not using the existing image file, we will select a local file on the computer, such as Drive C, which is the first drive on our computer.



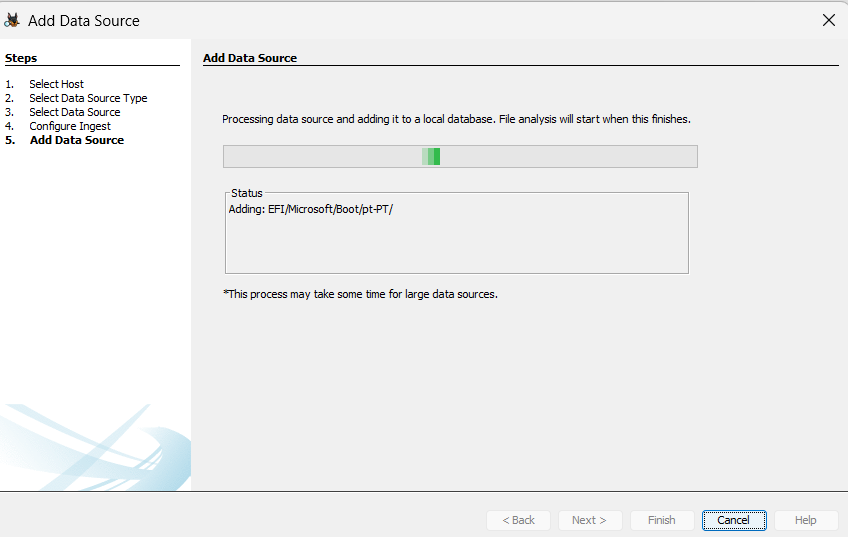
1. Afterward, we will select Drive 1 since it is the C drive of our computer. Once we have done that, we will press "OK" and then choose the time zone that matches our area. In my case, I will select the Indian time zone. Finally, we will click on "Next."



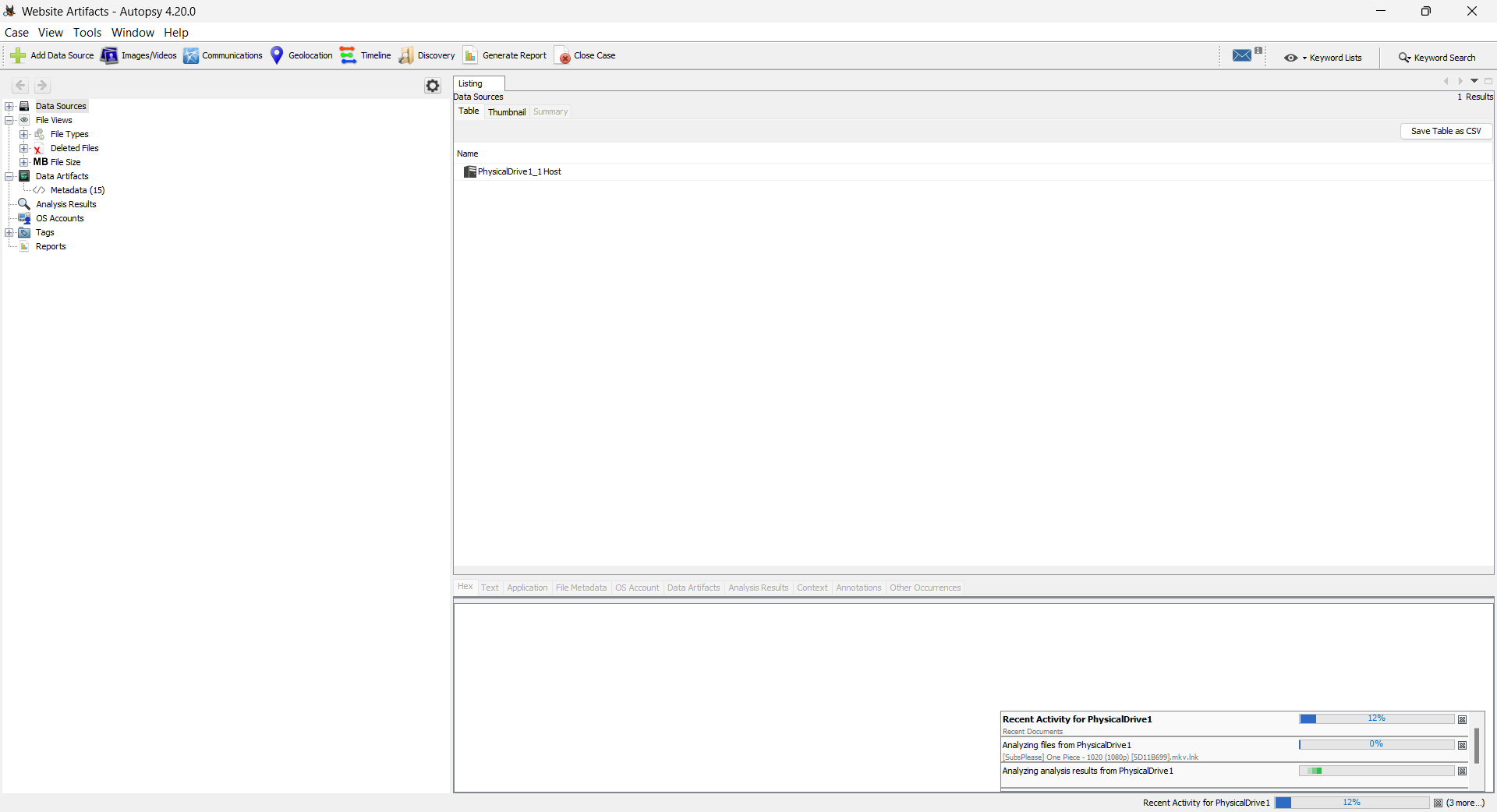
1. The options displayed on this screen include what you want to investigate on the computer, such as Recent Activity and file types, among others. The version we are using also has the capability of checking for Android and iOS analyzers, which is a valuable feature if you are investigating anything related to those platforms. As we are analysing website artifacts, we’ll select the necessary options only. After making the selection, we will click on "Next," and the tool will start processing the information. Depending on the size of the C drive, this may take some time.



1. The software is currently checking the status and creating a case to be saved in the destination, which, in this case, is the D drive

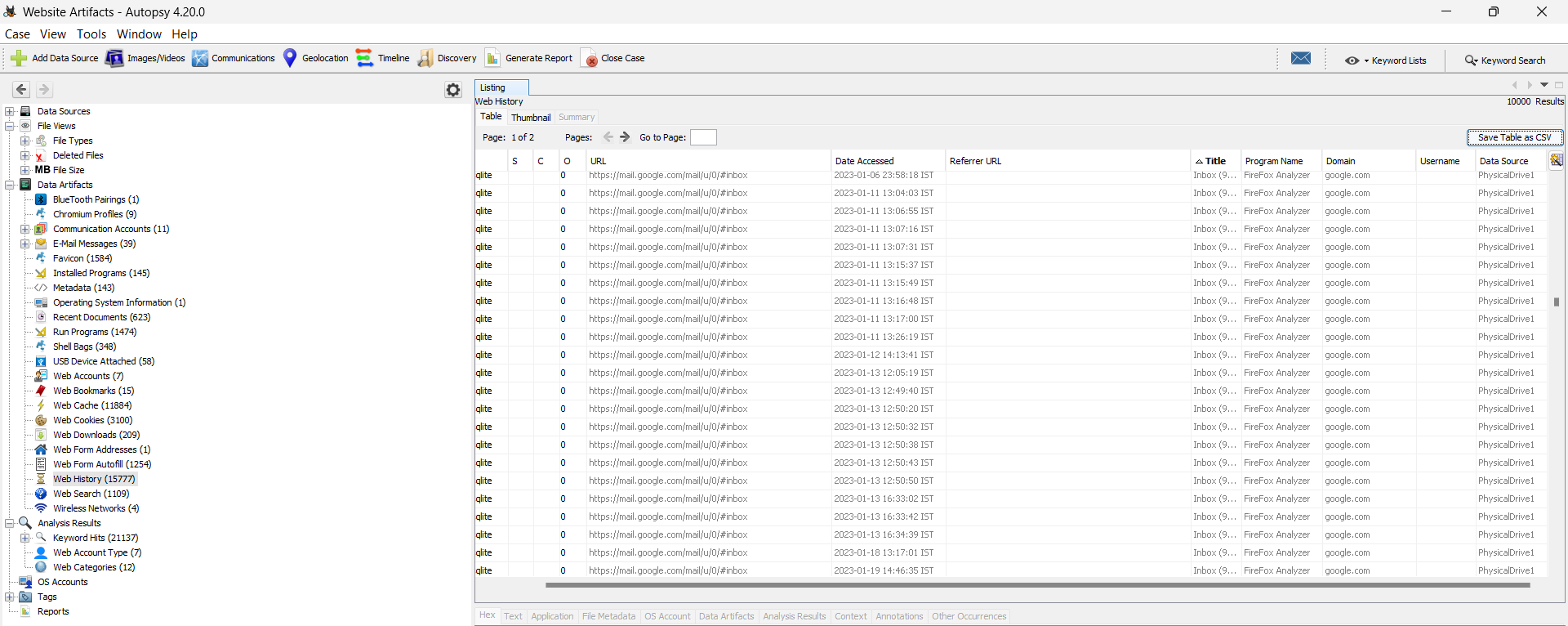


1. Currently, Autopsy is conducting the analysis of the selected disk image. The progress of the analysis is displayed in the recent activity section, which shows that only 12% of the disk has been analyzed so far. Since analyzing the hard drive can take a while, it is recommended to leave the computer as it is and let the software conduct a thorough analysis. The progress and the files being analyzed can be viewed by clicking on the progress section. We can check back later to see the final results.

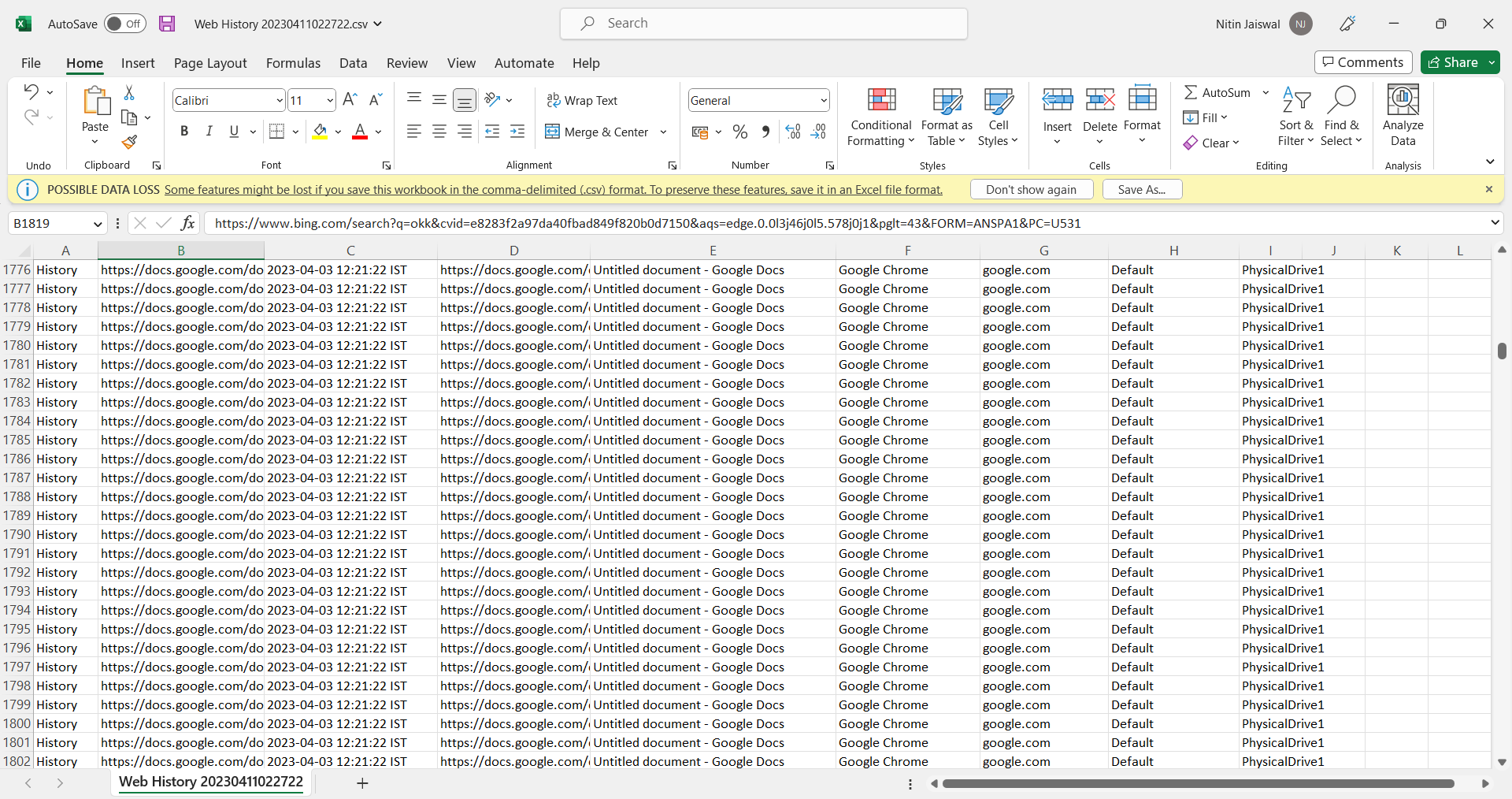


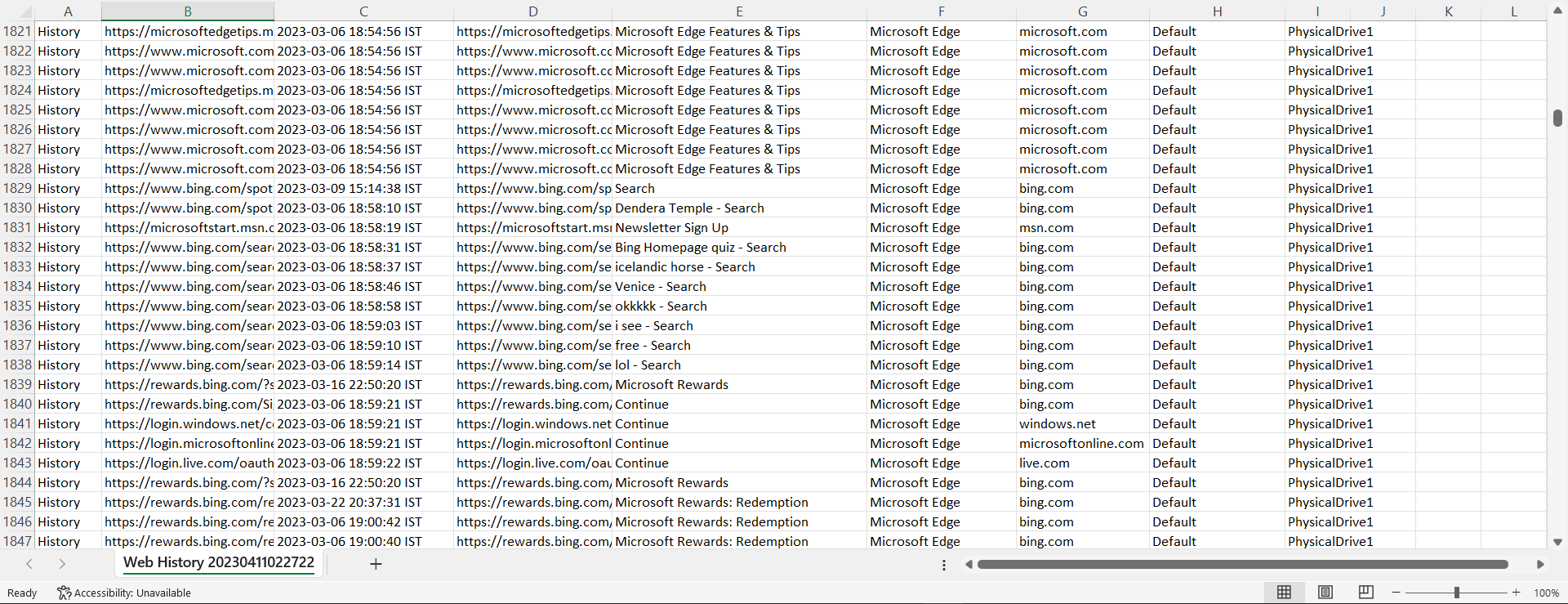
**3.2 Results**

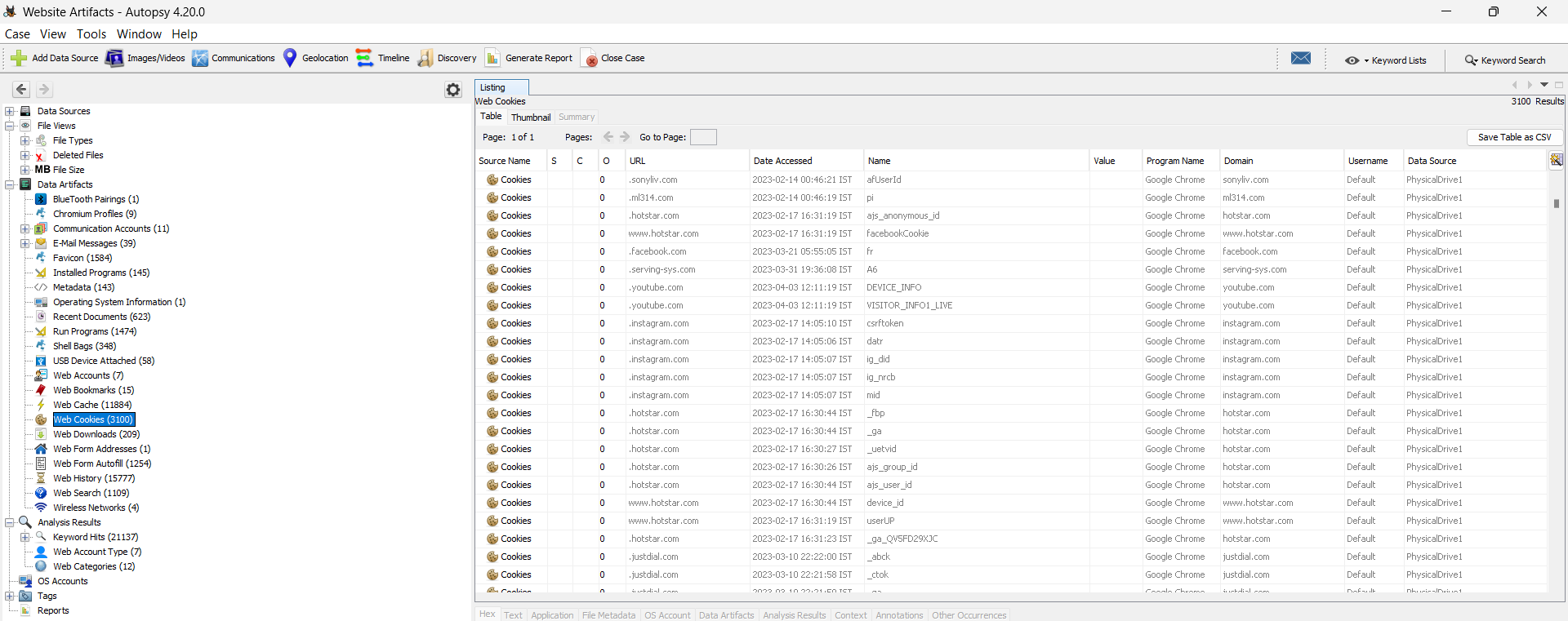
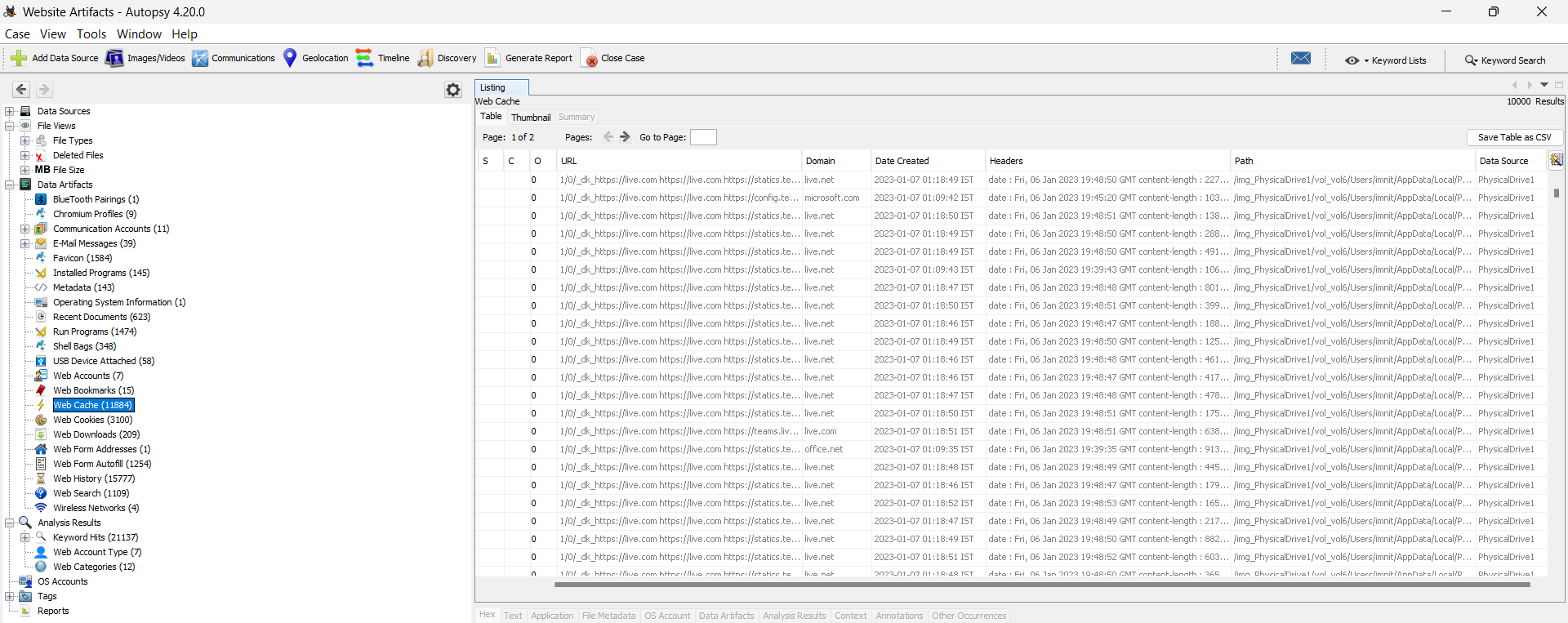
We select Web History and here we can see the history of the Firefox browser installed on our system. It shows the URL along with the date, domain, and other details. We can also export the data as “CSV” file. [11]

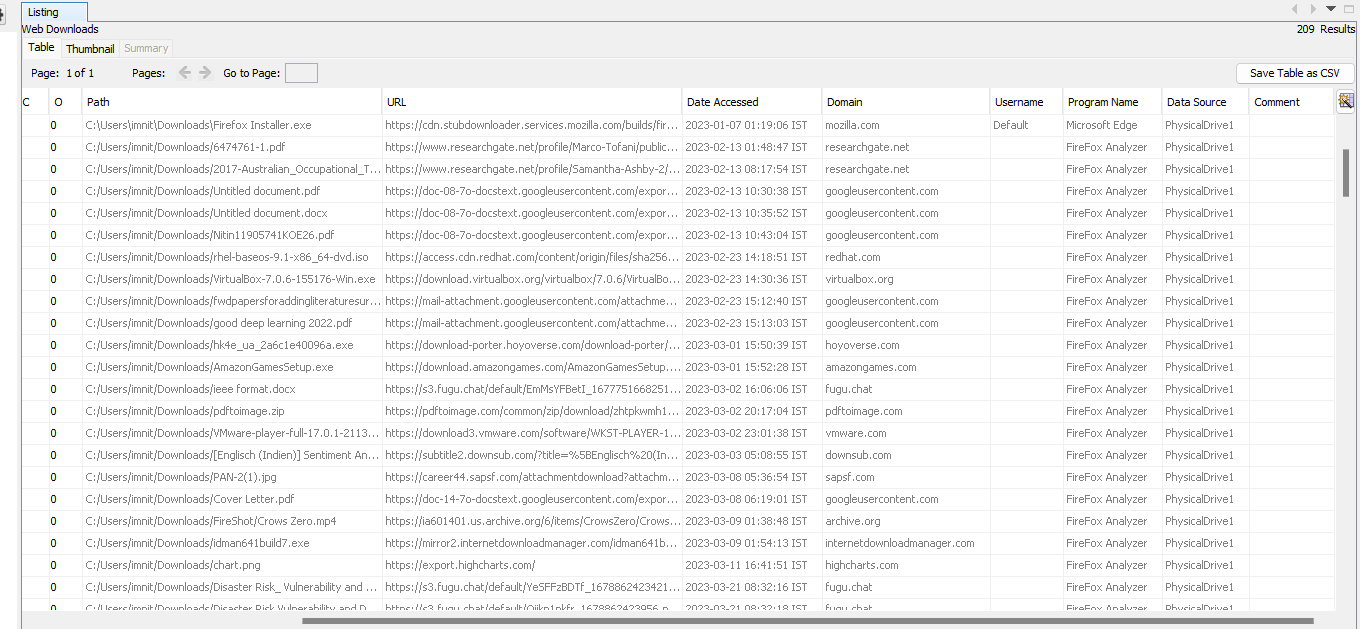
****

Here we can see the web history of other browsers such as Google Chrome and Microsoft Edge.

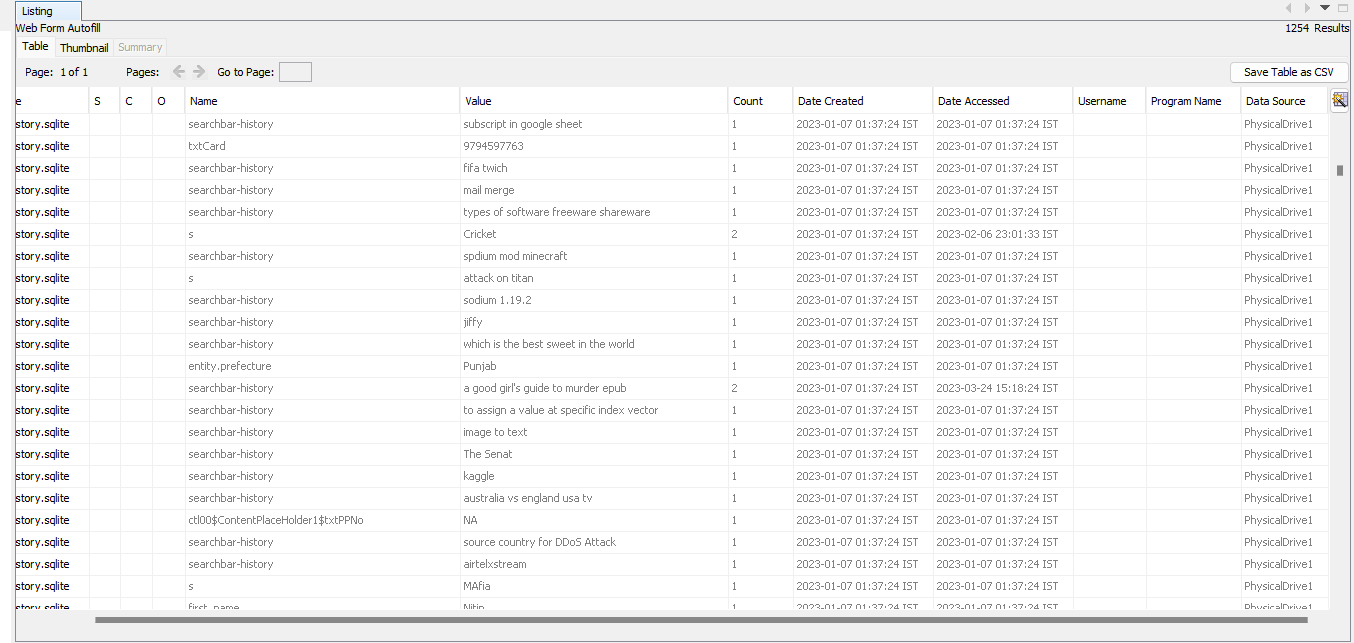
****

****

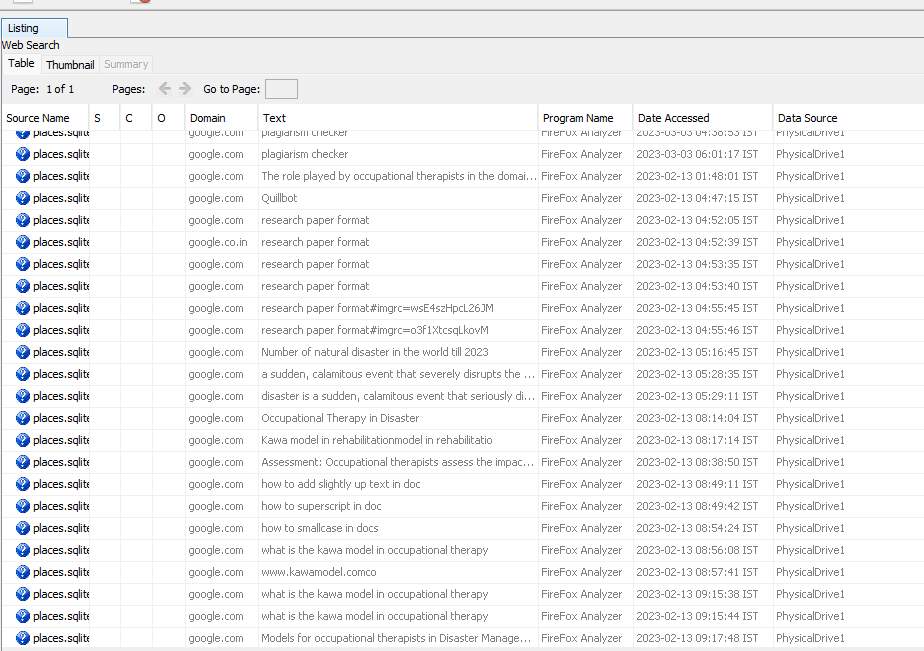
Here we can see the Cache and Cookies of the various websites browsed on the system. Cache and Cookies are essential information to know what websites user uses the most and what websites take data storage. ****

The autopsy tool can also show the files a user has downloaded on their system.****

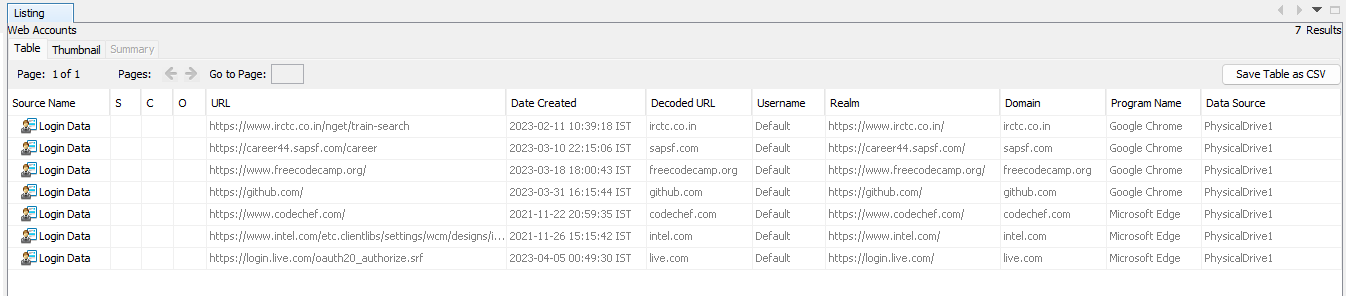
The web forms autofill can also be analysed through Autopsy.

****

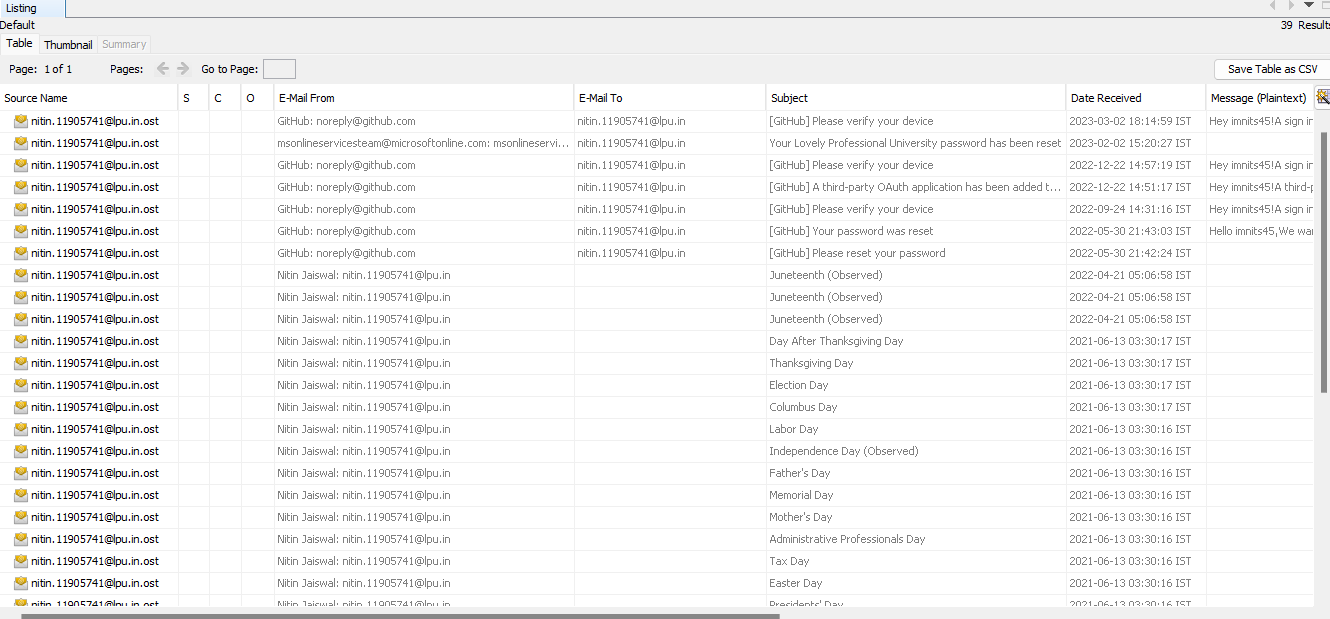
On selecting the search history, the user’s search history across the browsers will be displayed.

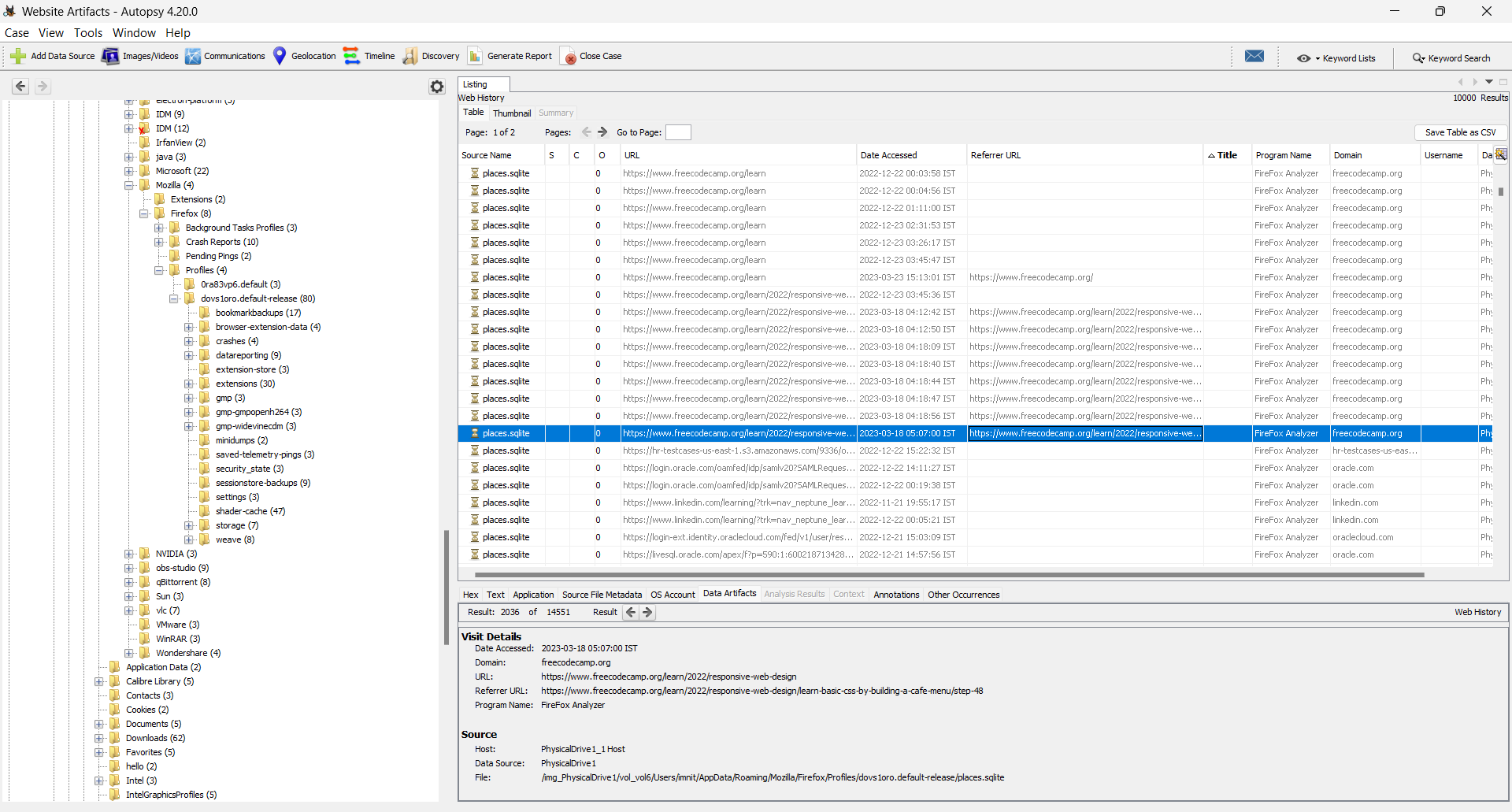
****

We can also see the login data such as usernames and passwords. For security reasons, we’ve not displayed the password.

****

If you have mailing applications such as Outlook installed on your system then the emails will also be displayed.

****

You can check the details of any component by clicking over it.****

**4. Conclusion**

In conclusion, Autopsy is a powerful forensic tool that can extract website artifacts from various providers such as Firefox, Edge, and Chrome, and help investigators find specific search terms on disks and phones. In this project, we successfully demonstrated how to use Autopsy to create a disk image, analyze it, and view the results. We also highlighted the importance of saving the image or analysis results in another partition, other than the one being analyzed.

The project's objectives were met, and the results were satisfactory. We were able to show how Autopsy can be used to investigate different types of cases. Overall, the project's scope and system requirements were well-defined, and the analysis report was thorough and detailed. Autopsy is an essential tool for digital forensic investigators and can aid in solving complex cases by providing crucial evidence. It is a versatile and user-friendly tool that can help analyze disk images quickly and efficiently

**5. References**

1. Monteith, S., Bauer, M., Alda, M., *et al.* Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Curr Psychiatry Rep* **23**, 18 (2021). <https://doi.org/10.1007/s11920-021-01228-w>
2. Graeme Horsman. Faculty of Computer Science, The David Goldman Informatics Centre, St Peter's Way, SR6 0DD, Sunderland, United Kingdom(2018)
3. Mozilla Firefox, Mozilla, 2021,<https://www.mozilla.org/en-US/firefox/>.
4. Microsoft Edge, Microsoft, 2021,<https://www.microsoft.com/en-us/edge>.
5. Google Chrome, Google, 2021,<https://www.google.com/chrome/>.
6. Autopsy. <https://www.autopsy.com>
7. https://www.cybervie.com/blog/introduction-to-autopsy-an-open-source-digital-forensics-tool/
8. <https://en.wikipedia.org/wiki/Autopsy_(software)>
9. Autopsy. The SleuthKit, <https://sleuthkit.org/autopsy/docs/user-docs/4.2/ds_page.html>
10. FreeEduHub. <https://www.youtube.com/watch?v=S6V66G2tVr8&t=454s>
11. DFIRScience <https://www.youtube.com/watch?v=fEqx0MeCCHg>

**Github Link:**

<https://github.com/imnits45/INT301CA3>