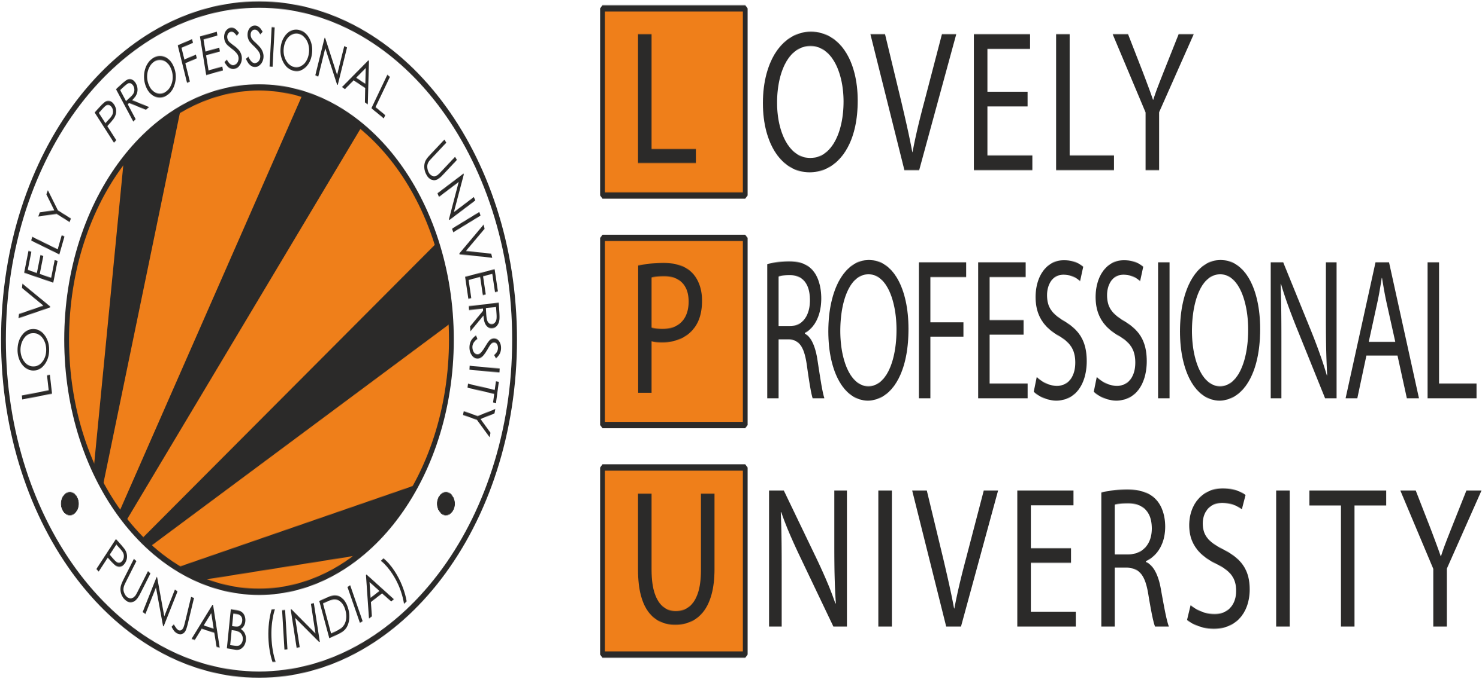
**INT301 : OPEN SOURCE TECHNOLOGIES**

****

SUBMITTED BY:

NAME : UPPU ESWAR NAGA MASTHAN

REG.NO : 11909441

ROLL.NO : 55

**INTRODUCTION**

OBJECTIVE:

Finding evidence of online activity is the main goal of removing website artefacts from different web browsers including Firefox, Edge, and Chrome. This may contain downloads, bookmarks, search history, and browsing history. By removing Through these artifacts, investigators can learn more about the user's online conduct and perhaps find proof of improper or criminal activity. The second goal is to locate specified search terms on both disc and phone using the forensic application Autopsy. An autopsy is an effective forensic method that helps detectives find and analyse digital evidence by analysing vast amounts of data. Investigators can focus their attention on important pieces of evidence that may be pertinent to their case by doing specific search phrases that will help them to focus their inquiry. This procedure might turn up significant information that could be used in legal proceedings and assist investigators in constructing a more complete picture of the user's online conduct.

DESCRIPTION :

To collect website artefacts from various web browsers like Firefox, Edge, and Chrome, various types of data stored on a computer or mobile device must be identified and removed. Downloads, cookies, cache, bookmarks, and browsing history make up this data. To access the data, either the hard disc can be imaged or a forensic image of the device can be obtained. Using a forensic programme like Autopsy, when the data has been gathered, it may be reviewed and precise search terms can be found. An autopsy, a popular open-source forensic tool, can help investigators automate the analysis of digital evidence. Additionally, it can help with categorising and identifying different types of data, including browser artefacts.

An autopsy, a popular open-source forensic tool, can help investigators automate the analysis of digital evidence. It can also help with categorising and identifying different types of data, including browser artefacts. To find specific search phrases, the investigator might use Autopsy's keyword search feature. This involves searching the retrieved artefacts for specific terms or phrases that might be relevant to the investigation. When looking for proof of drug use, the investigator may use terms like "marijuana," "cocaine," or "heroin," for example. Autopsy can also be used to find data trends, such as the frequency of specific search terms or the times and dates of online browsing activity. . By doing this, investigators might be able to identify trends in the user's behaviour and build a more complete picture of their online pursuits. Overall, retrieving website artefacts and using Autopsy to find specific search terms are essential parts of digital forensics investigations. It enables sleuths to compile priceless information and discover more about a user's online habits, which can be used to support legal proceedings or other investigations.

SCOPE OF THE OBJECT:

Extraction of website artefacts from various web browsers, such as Firefox, Edge, and Chrome, may produce significant information in digital forensic investigations. Investigators can get valuable information from browser artifacts, like browsing history, downloaded files, login information, and bookmarks, to help them pinpoint the origin, extent, and timing of a crime. The artefacts may also reveal internet behaviour like social media chats, searches, and purchases to support a claim. Using the Autopsy forensic application, investigators may extract browser artefacts from disc and phone images and assess them using a straightforward graphical user interface.

The Autopsy forensic programme has a number of modules that can be used to extract and analyse digital data. In particular, Chrome, Firefox, and Edge are only a few of the web browsers from which Autopsy's browser modules can gather website artefacts.

The tool's comprehensive data analysis allows investigators to examine specific sessions, download history, cookies, bookmarks, and other relevant data. Use the keyword search feature in Autopsy to find specific search terms on a disc or phone image. Investigators can identify and extract relevant data, such as email addresses, phone numbers, and other potential keywords, with the use of this module. In conclusion, employing Autopsy's browser and keyword search modules can help investigators analyse digital evidence and build a solid case.

**SYSTEM DESCRIPTION**

TARGET SYSTEM DESCRIPTION:

Any digital device that has the required data can be the target system for forensic software Autopsy, which can locate certain search phrases on disc and phones and extract website artefacts from different web browsers, including Firefox, Edge, and Chrome. Any digital device that stores browser data, such as a desktop computer, laptop, phone, or other mobile device, can serve as the system. The system can be utilised with any operating system, including Windows, macOS, and Linux, as long as it supports the necessary web browser. To avoid data contamination or alteration, it is essential to keep in mind that the target system shouldn't be used or modified while the data are being retrieved. A forensic image of the hard drive or phone memory of the target system is necessary for the extraction procedure.

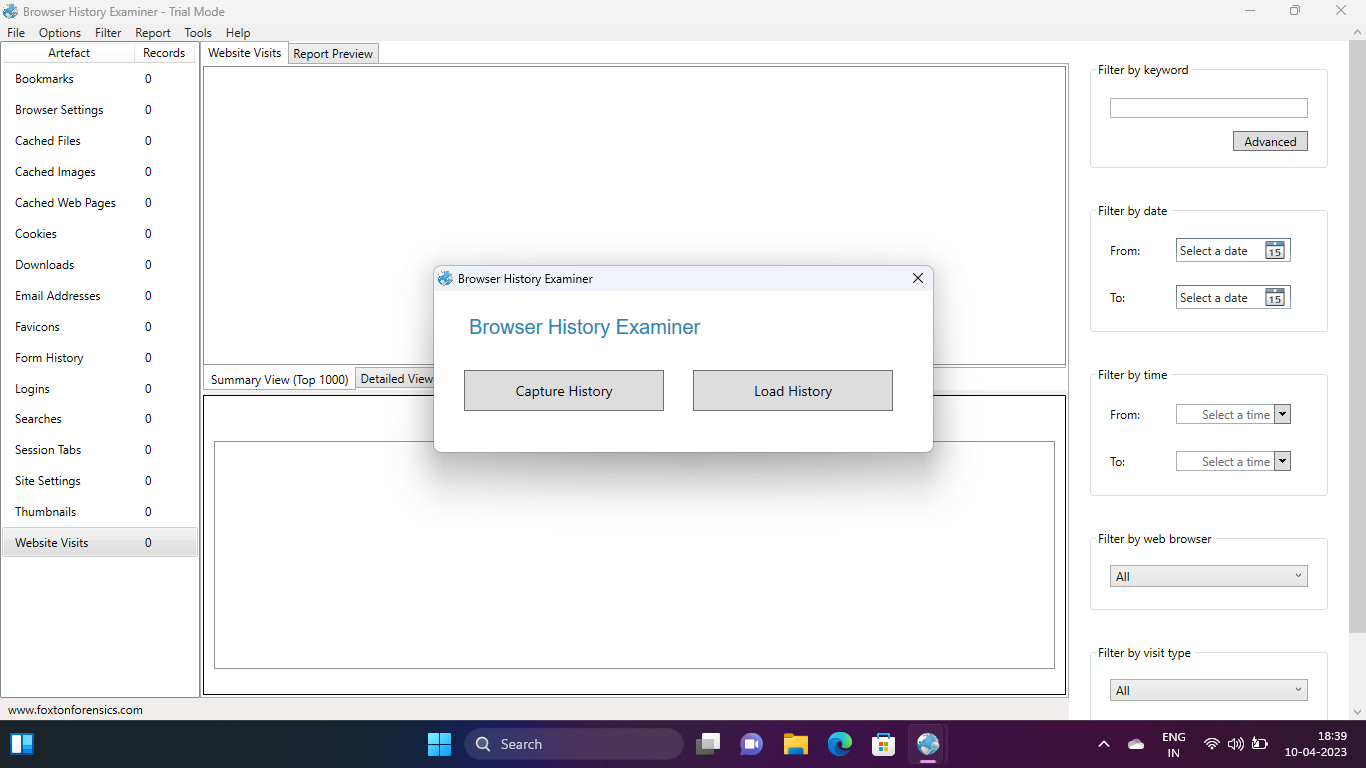
By creating a bit-by-bit copy of the original data, a forensic picture is made in order to preserve the integrity of the evidence. The image can be created using forensic imaging tools like FTK Imager, Encase, or dd. After mounting the forensic picture on a forensic workstation, it is then examined using the Autopsy forensic tool.Investigators can collect and study website artefacts and specific search keywords from a number of online browsers with the aid of the user-friendly forensic programme known as Autopsy. The Autopsy forensic programme can extract website artefacts and specific search phrases from any digital device that has relevant data, and the process requires a forensic image of the device's hard drive or phone memory.

ANALYSIS REPORT

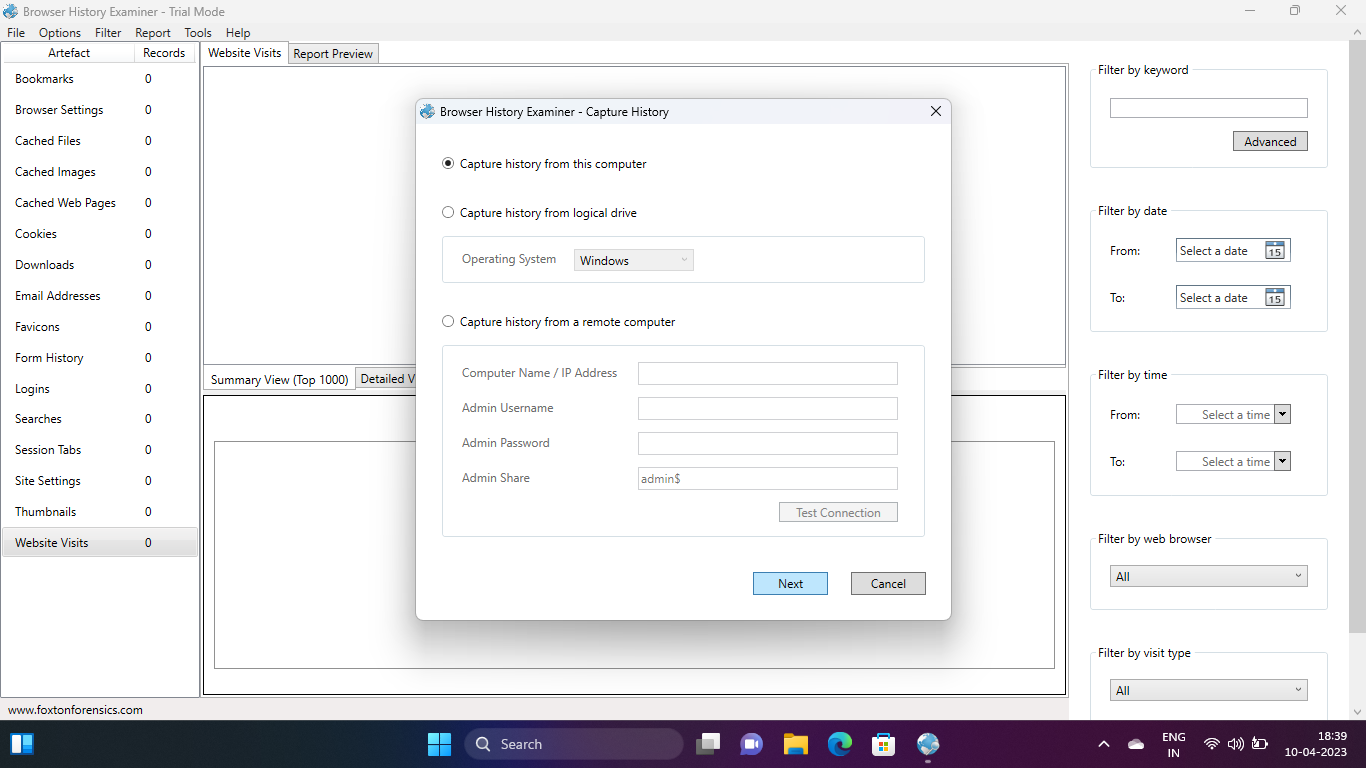
To extract website artifacts from various sources like chrome ,edge ,internet explorer use browser history examination software to easily extract the required data.

Steps to extract the artifacts:

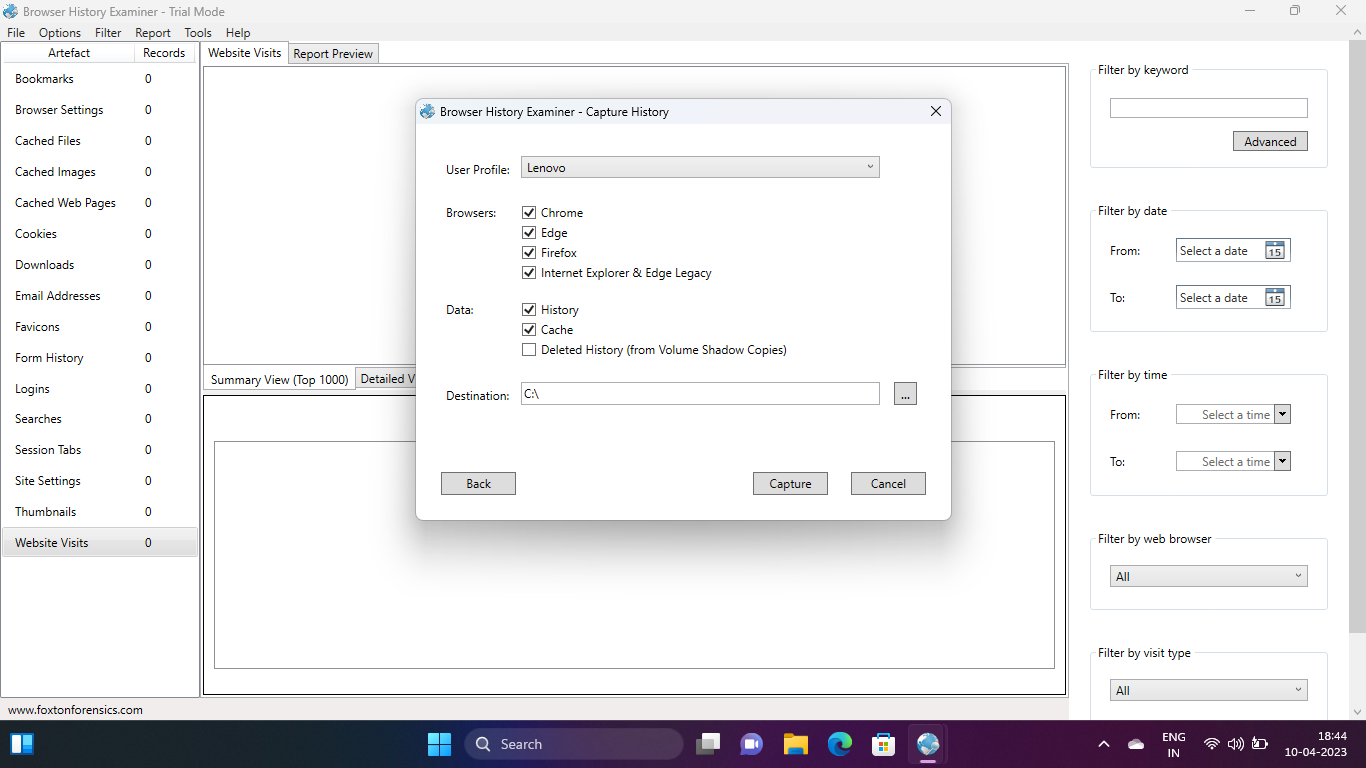
1.Install browser history examiner and select capture history:



2.Select data source :

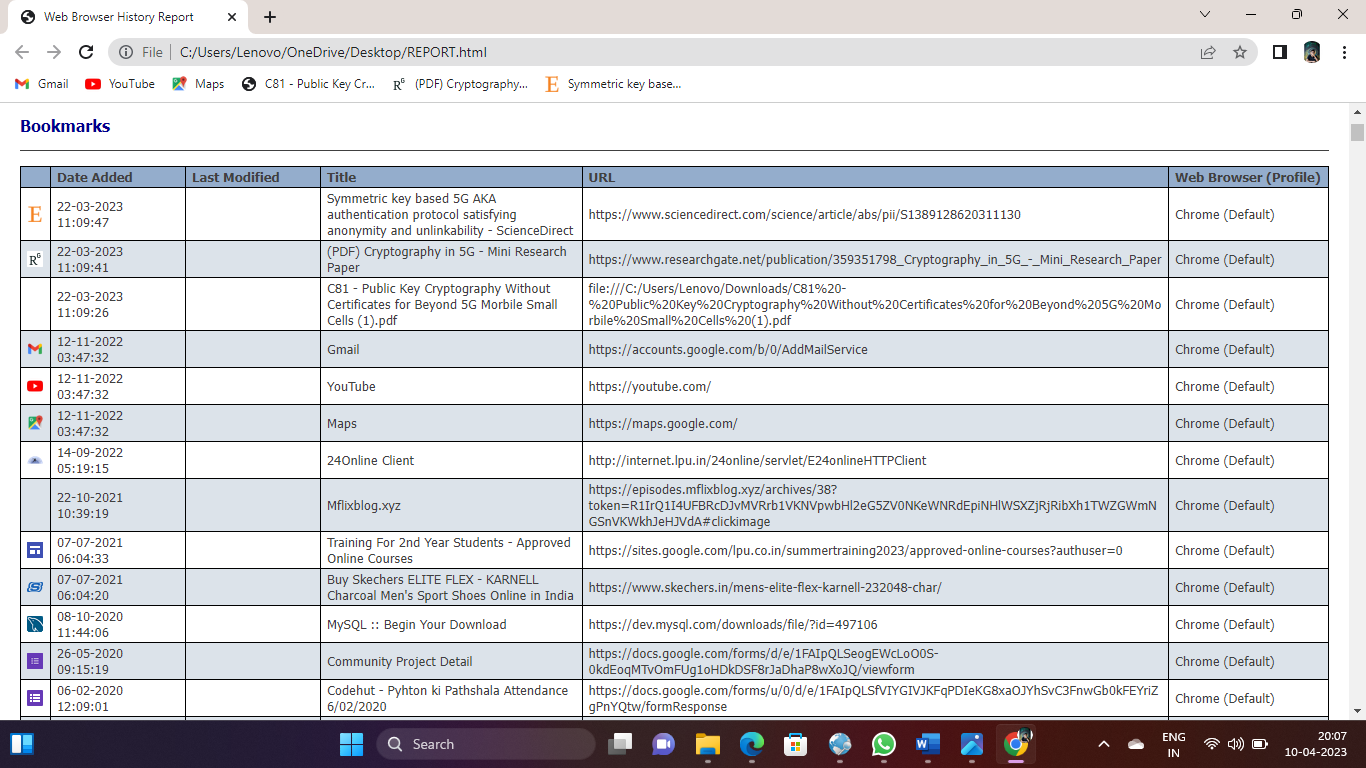


3.Tick the boxes to get the required data:



4.Export the data in a html report form as follows

Bookmarks:

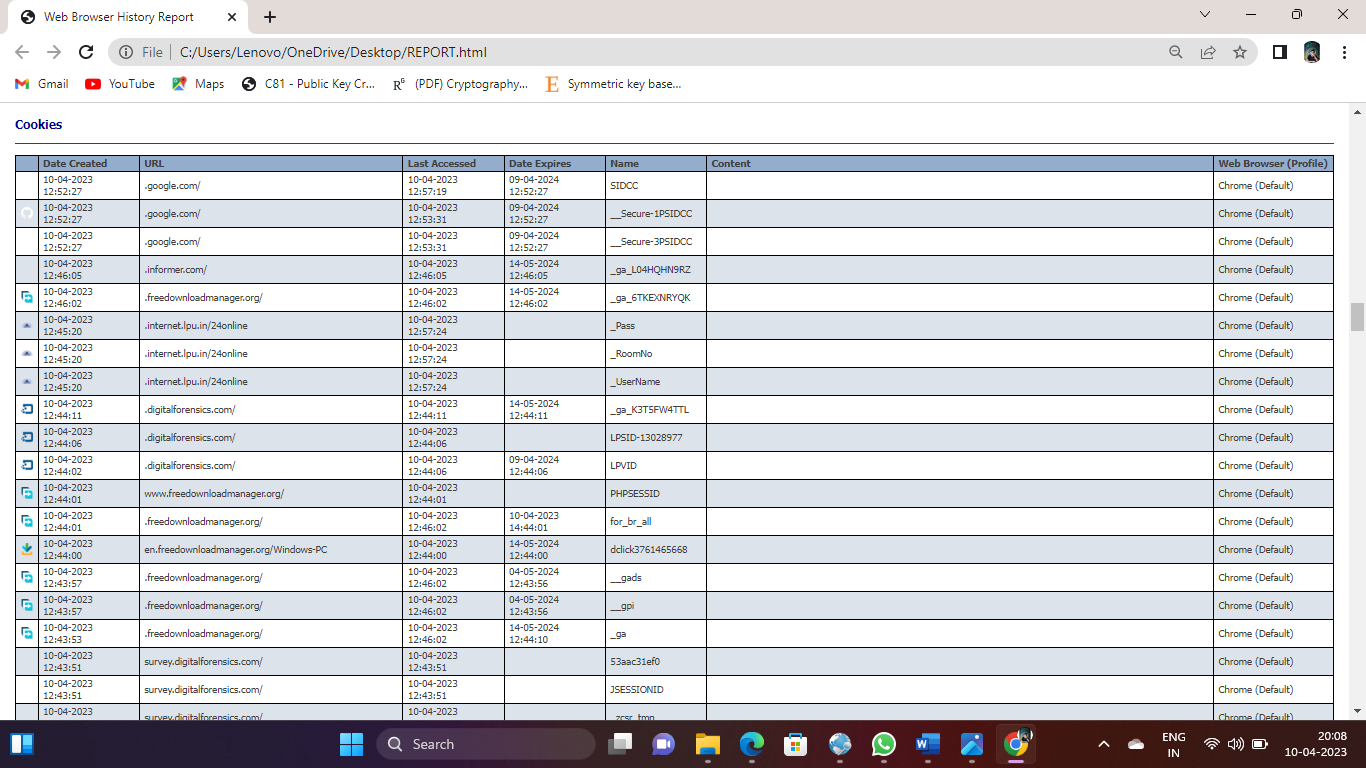


Cached files:

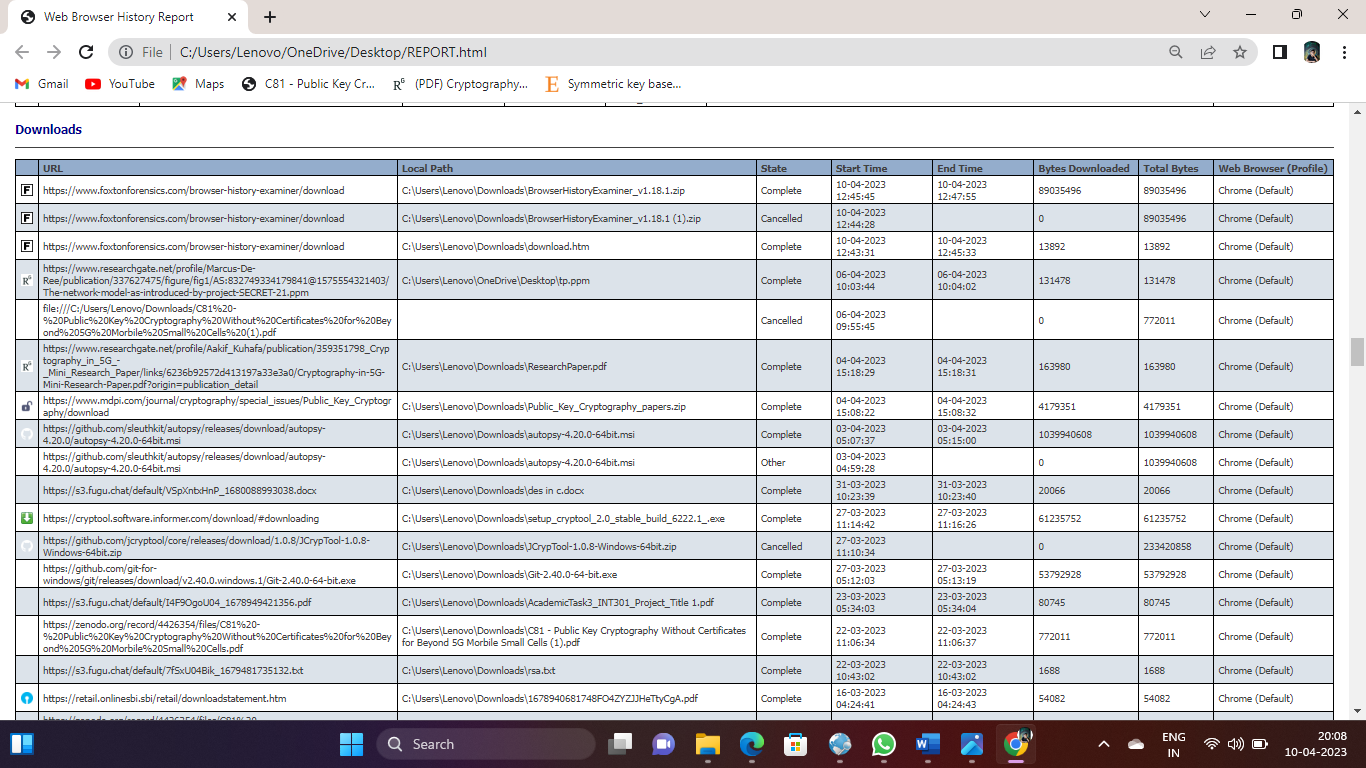
Graphical user interface, application

Description automatically generated

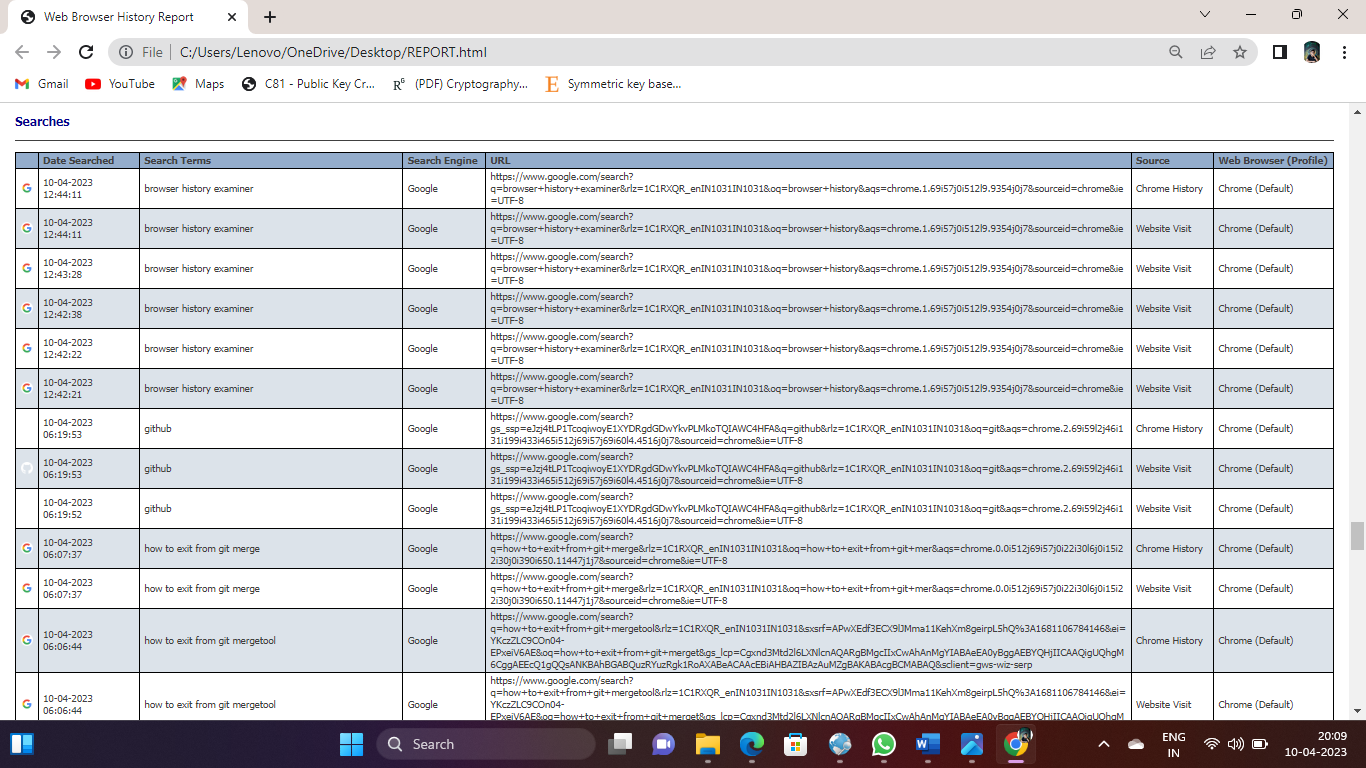
Cookies:



Downloads:



Searches:



* Now save the HTML file in a folder
* Install Autopsy forensic tool
* Load the HTML file to perform the actions

Graphical user interface, application, Word

Description automatically generated

* Use keywords search and perform to view result of the keyword

1.Autopsy

Graphical user interface, text, application, Word

Description automatically generated

2.ums

Graphical user interface, text, application

Description automatically generated

REFERENCES:

1. Autopsy User Documentation. (2021). Autopsy User Documentation. Retrieved from <https://sleuthkit.org/autopsy/docs/user-docs/>
2. Casey, E., & James, M. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. San Diego, CA: Academic Press.
3. Carrier, B. (2014). File System Forensic Analysis. Boston, MA: Addison-Wesley