Project Report

# INT301: OPEN-SOURCE TECHNOLOGY

Submitted in partial fulfilment of the requirements for the award of degree of

# Batchelor of Technology

(Computer Science and Engineering) Submitted to Prof: Dr. Manjot Kaur (28925)

LOVELY PROFESSIONAL UNIVERSITY PHAGWARA, PUNJAB



Submitted By:

Name of student: Lakshika Upadhyay

Registration Number: 11913350

Project Link:

Annexure- IX (b): Student Declaration

**To whom so It may concern**

I, **Lakshika Upadhyay,** Registration number: **11910359**, hereby declare that the work done by me on

**Capture and analyze the browser history using any opensource tool. Perform a scan of**

**bookmarks, cache data, visited websites and cookies.,** in the month of March 2023, under the supervision of Prof. Dr. Manjot Kaur (28925) School of Computer Science and Engineering at **Lovely Professional University**, Phagwara, Punjab, is a record of original work from the partial fulfilment of the requirements for the award of the degree, **Bachelor of Technology (Computer Science and Engineering).**

Name of the Student: Lakshika Registration Number: 11913350

Dated: 20 March 2023

**CHAPTER 1:**

1. INTRODUCTION

Capturing and analyzing browser history is a common task performed by digital forensics investigators, as it can provide valuable insights into a user's online activities. In this report, it is discussed how to capture and analyze browser history using an open-source tool, and perform a scan of bookmarks, cache data, visited websites, and cookies. The opensource tool used to make this project is “Browser History Examiner”. Browser History Examiner is a free and open-source tool that allows digital forensic investigators to capture and analyze browser history from various popular web browsers. BHE is designed to work on Windows operating systems and can be downloaded from the official website.

1.1 OBJECTIVE OF THE PROJECT

The objective of the project "Capture and analyze the browser history using any open-source tool" is to create a program or script that can extract information from a user's web browser, such as the websites they have visited, bookmarks, cache data, and cookies, and analyze it for different purposes. The project aims to provide a simple and efficient way to extract and save browser data for forensic analysis or personal record keeping.

* 1. DESCRIPTION OF THE PROJECT

This project involves using an open-source tool called Browser History Examiner to capture and analyze a user's browser history. This tool is designed to extract data from web browsers, including bookmarks, cache data, visited websites, and cookies, and analyze it for various purposes.

To perform the scan, the user will first need to install Browser History Examiner on their system. Once installed, the tool can be configured to capture data from various browsers, including Chrome, Firefox, Safari, and Edge. The user can select which browsers they want to scan and specify the time range for data collection.

Browser History Examiner then captures data from the selected browsers and provides a comprehensive report that includes information such as the user's browsing history, bookmarked websites, cached files, and cookies. The report can be customized to include specific data types, such as images or video files, and can also be filtered based on keywords or search terms.

The report generated by Browser History Examiner can be used for various purposes, including detecting potential security threats, identifying user behavior patterns, and analyzing web traffic. The data can be exported in various formats, such as CSV, HTML, or JSON, making it easy to import into other analysis tools.

* 1. SCOPE OF THE PROJECT

The scope of the project "Capture and analyze the browser history using any open-source tool" involves designing and implementing a program or script that can capture and analyze browser history data. The project involves the use of an open-source tool, which ensures that the project is accessible and affordable for anyone who wants to perform such an analysis.

The project's primary focus is to capture and analyze data from web browsers, including bookmarks, cache data, visited websites, and cookies. The tool can be configured to capture data from various browsers, including Chrome, Firefox, Safari, and Edge, making it flexible and adaptable to different user preferences.

The project's scope includes developing a user-friendly interface for configuring the tool's settings and generating reports based on the captured data. The reports should be customizable and provide insights into the user's browsing behavior, interests, and habits.

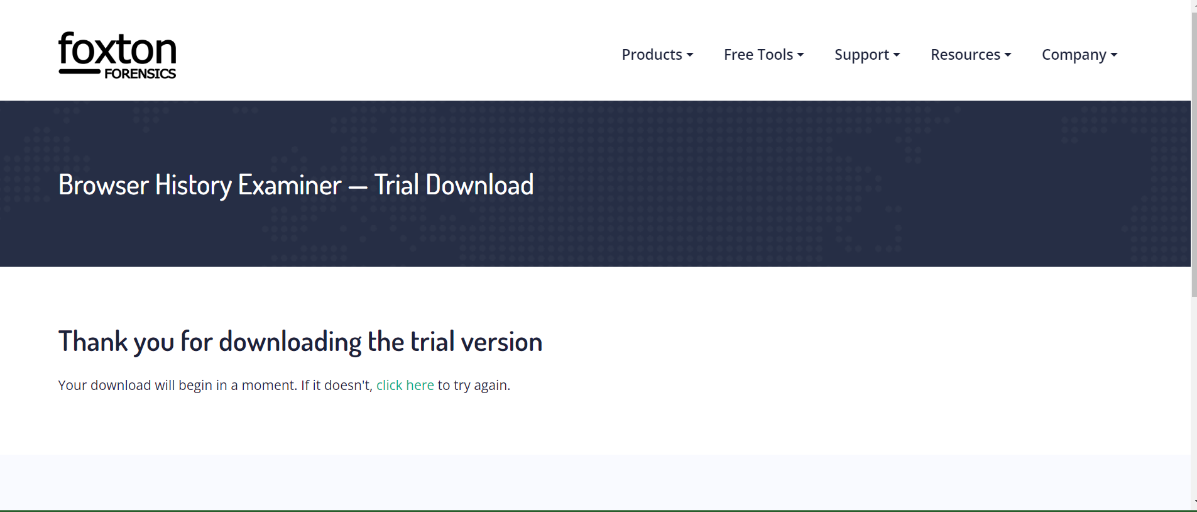
The project's scope also includes ensuring the security and privacy of the captured data. The tool should comply with data protection regulations, and users should have control over what data is captured and how it is used.

Overall, the project's scope is to provide a comprehensive and customizable solution for capturing and analyzing browser history data that can be used for various purposes, including improving user experience, identifying potential security threats, and analyzing web traffic.

* 1. FLOW CHART OF THE PROJECT

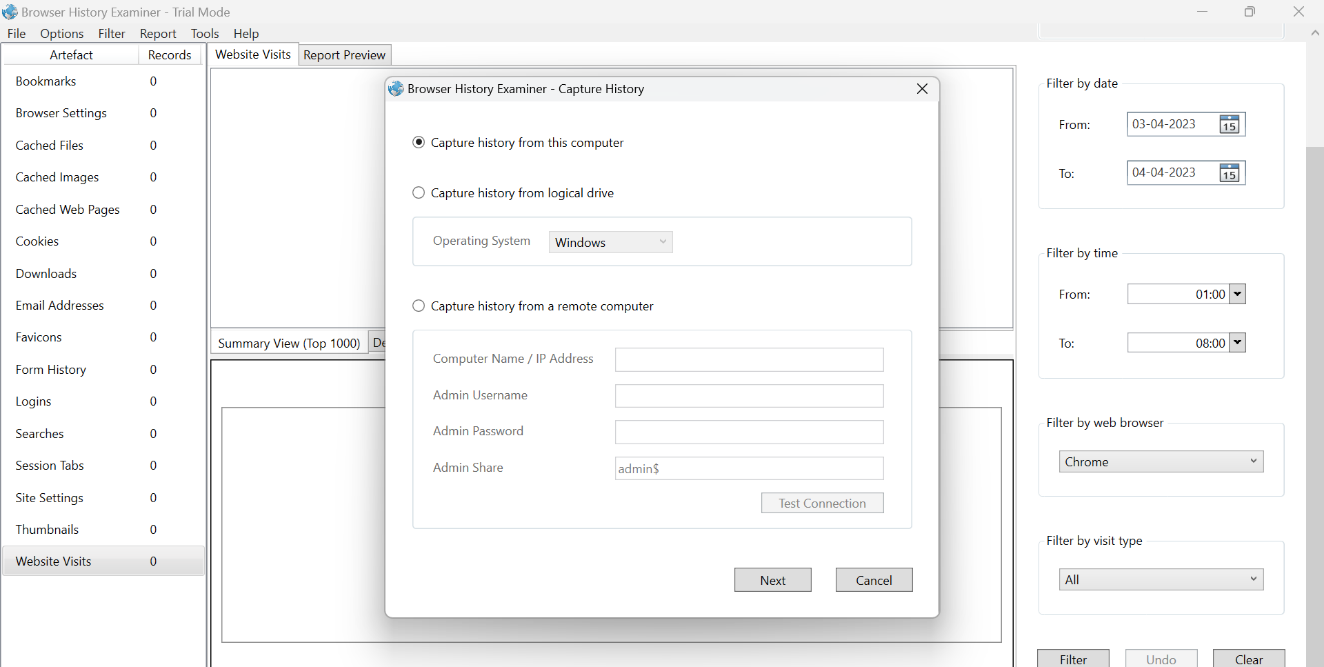
To capture browser history using BHE (Browser history examiner), follow these steps:

**Step1:** Download and install BHE Browser history examiner) on your Windows machine: as referred in fig. 1.4.1



*Fig. 1.4.1 – Installation of browser history examiner*

**Step 2:** Navigate to the "Capture history" tab and select the browser that you want to analyze.



*Fig. 1.4.2 – Capture history using BHE*

**Step3**: Select the browser of which you want to analyze history and provide destination.

Graphical user interface, application

Description automatically generated

*Fig. 1.4.3 – Selecting browser and Providing destinations.*

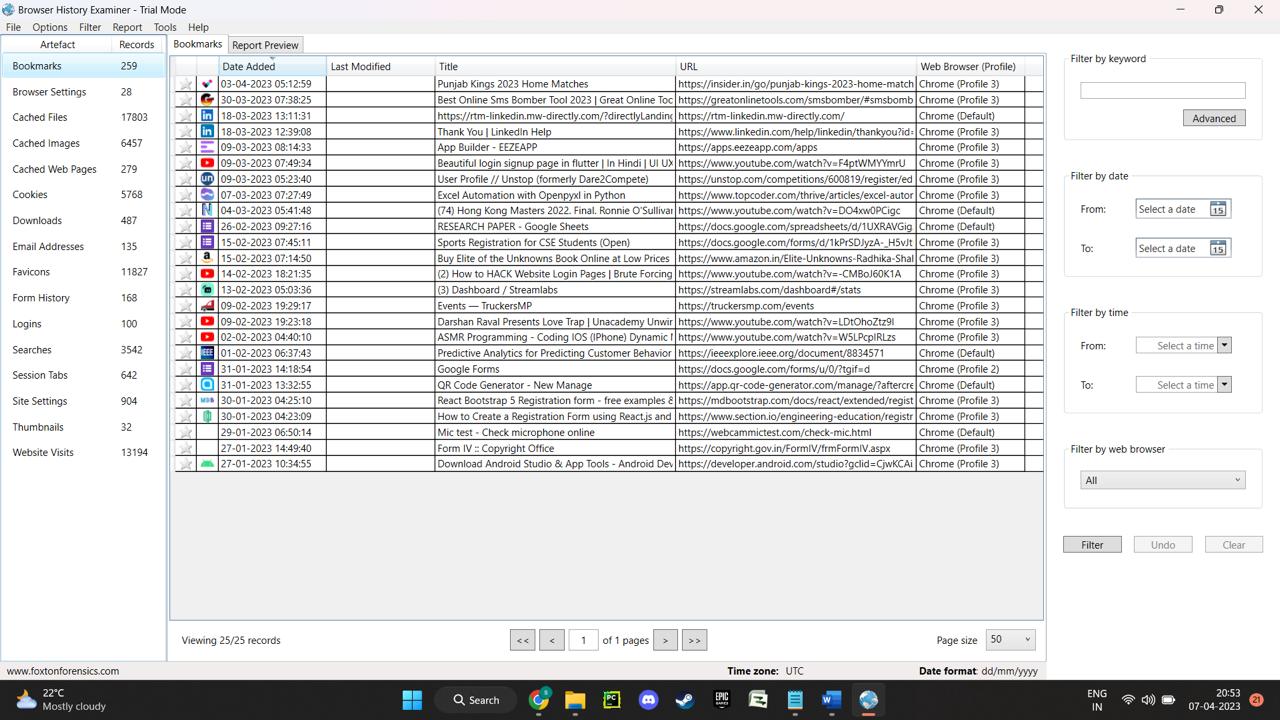
**Step 4:** Once the browser history data has been collected, the next step is to analyze it using BHE. BHE provides various built-in tools that can be used to analyze browser history data.

Graphical user interface, text

Description automatically generated

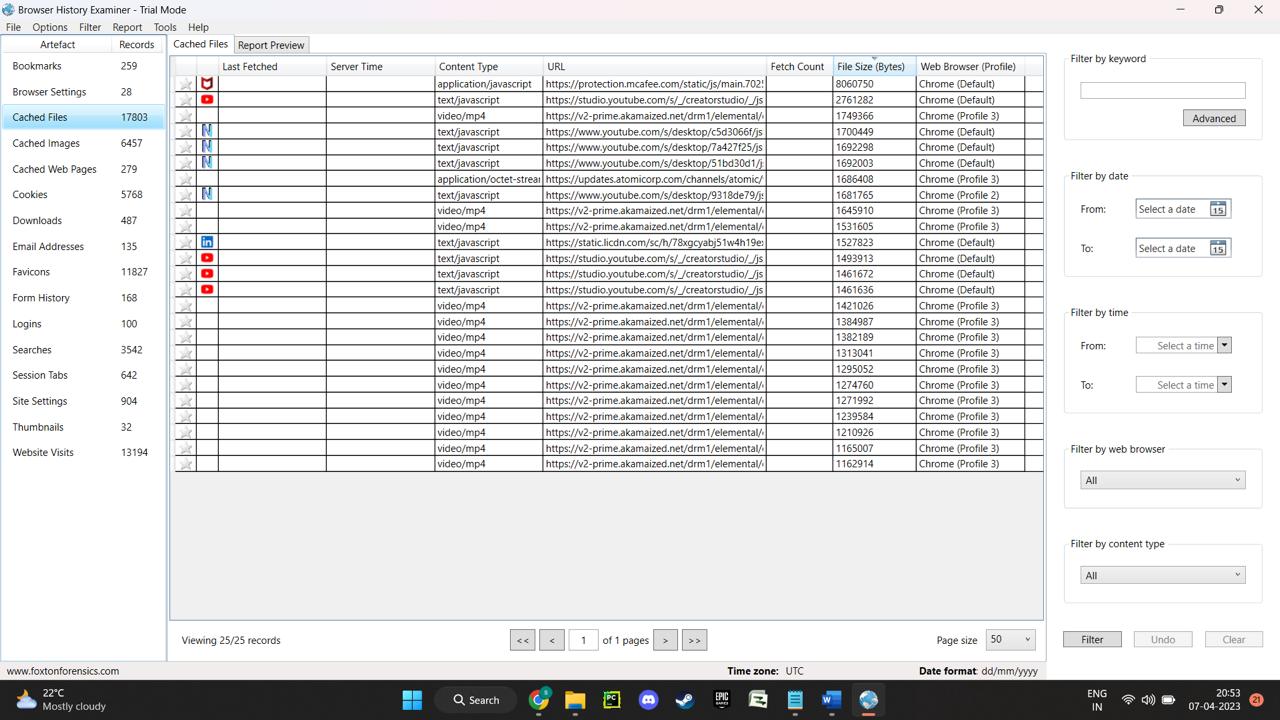
*Fig 1.4.4 – Analyzing browser data*

**Step5:** To analyze bookmarks, navigate to the "Bookmarks" tab. The bookmarks viewer displays a list of all the bookmarks saved in the browser, along with the URL, title, and date of creation.



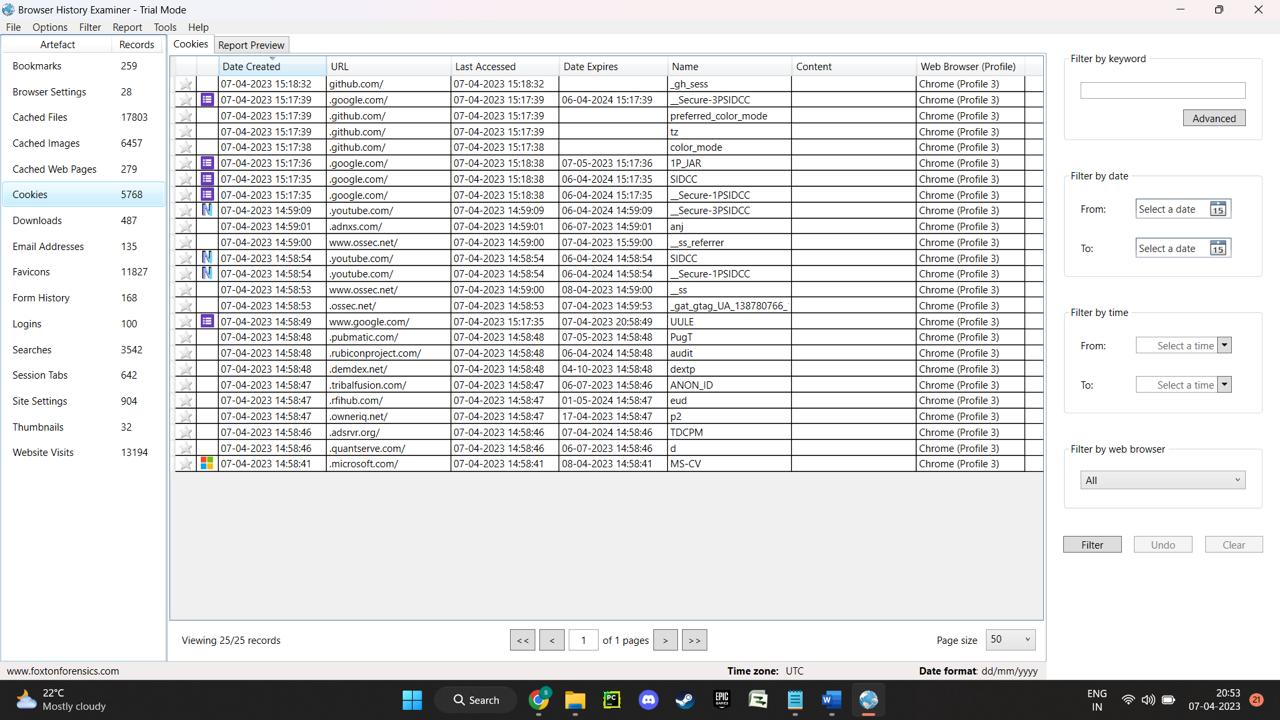
*Fig 1.4.5 – Analyzing Bookmarks*

**Step 6:** To analyze cache data, navigate to the "Cache" tab. The cache viewer displays a list of all the files that have been downloaded or cached by the browser, along with their file path and creation date.



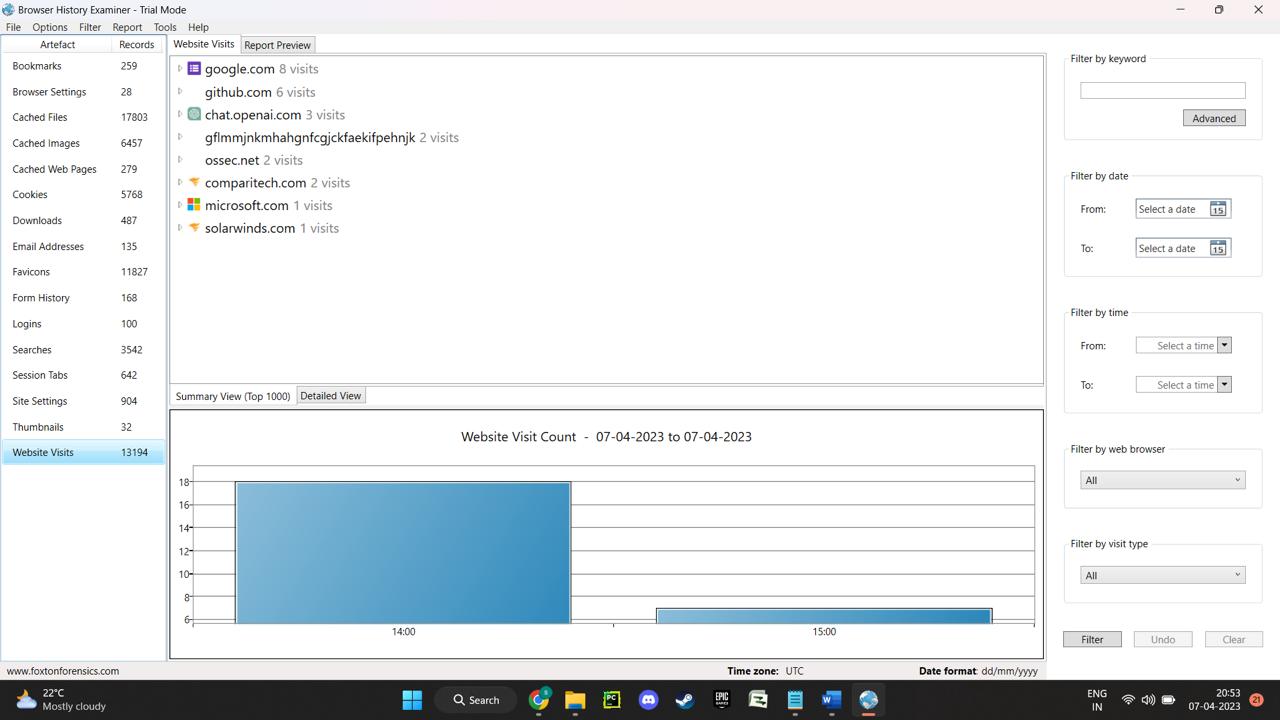
*Fig 1.4.6 – Analyzing Cache files*

**Step 7:** To analyze cookies, navigate to the "Cookies" tab. The cookie viewer displays a list of all the cookies saved by the browser, along with their name, value, domain, and expiration date.



*Fig 1.4.7 – Analyzing Cookies*

**Step 8:** To analyze visited websites, navigate to the "Website visit" tab. The history viewer displays a list of all the websites visited by the user, along with the URL, title, and date of access.



*Fig 1.4.8 – Analyzing Website visits*

**CHAPTER 2:**

2.1 SYSTEM CONFIGURATION

Operating System Used for the Project: Dell Inspiron 14 5000

Open-Source tool Used for the Project: Browser History Examiner

Browser history examiners can be used to recover deleted browsing history, analyze website visitation patterns, and identify potential security breaches. They can also help investigators to identify the type of content a user has accessed, including websites visited, search terms used, and online activity.

Browser history examiners can be used to investigate various types of crimes, such as cybercrime, fraud, identity theft, and online harassment. However, it is important to note that the use of these tools must be done within the legal boundaries and with proper authorization.

2.2 ANALYSIS REPORT

* Purpose: The purpose of the project is to extract specific types of data from a web browser and export the data in a text file format. The project can be useful for forensic analysis, data recovery, or personal record keeping.
* Scope: The scope of the project is limited to data extraction and export. The project does not cover any additional functionality beyond data extraction and export. The project can be applied to various web browsers but does not involve any modifications to the web browser or any other software used.
* Tools: The project can be implemented using various open-source software tools such as " Mozilla Firefox " or other similar software. The specific steps for extracting the data may vary depending on the software used.
* Implementation: The project can be implemented by following the specific steps for data extraction and export using the chosen opensource software tool. The implementation process should ensure that the necessary permissions and legal rights are obtained for data extraction.
* Benefits: The project provides a simple and efficient way to extract and export specific types of browser data. This can be useful for forensic investigators, individuals who want to backup or transfer their browser data, or those who want to keep personal records of their browsing history.
* Limitations: The project is limited to extracting specific types of browser data and does not cover any additional functionality. The project may also be limited by the capabilities of the open-source software tool chosen.
* Future Scope: In the future, the project could be expanded to include additional functionality such as data analysis or reporting. The project could also be expanded to cover more types of browser data, or to include additional web browsers.

2.2 REFERENCE

[2.2.1] <https://en.wikipedia.org/wiki/Web_browsing_history>

[2.2.2] <https://www.foxtonforensics.com/browser-history-examiner/download>

[2.2.3] <https://youtu.be/Aqij_uzyItY>

[2.2.4] <https://youtu.be/EaLg2evq0TI>

[2.2.5] <https://en.wikipedia.org/wiki/Web_development_tools>