INT 301: Open-Source Technologies

Project Report

(Project Semester January- May 2023)

Capture and analyse the browser history using any open-source tool. Perform a scan of bookmarks, cache data, visited websites, and cookies.

Submitted by: Anjali Nain

Submitted to: Dr.Manjot Kaur

Registration No: 11910046

Section: KE015

Course code: INT301

CHAPTER-01

Introduction

Email forensic tools are specialized software programs used by investigators to analyse and examine electronic mail messages for evidence in legal or investigative cases. These tools are designed to provide a detailed insight into the content, headers, attachments, and metadata of emails, as well as the source and recipient information. Some of the common features of email forensic tools include email recovery, email parsing, email search and analysis, email tracking, and email filtering. These tools use various techniques such as data carving, file carving, and network traffic analysis to recover deleted, corrupted, or hidden email messages. Email forensic tools are widely used in legal proceedings to investigate cybercrime, identify sources of email threats, and provide evidence in court. They are also used by corporate organizations to monitor employee communication, prevent data breaches, and ensure compliance with regulations. Some popular email forensic tools include EnCase, FTK Imager, Oxygen Forensic Suite, and Mail Xaminer. These tools are designed to provide comprehensive email analysis and reporting capabilities, making them essential tools for digital forensic investigators and law enforcement agencies.

1.1) Objective:

The objective of capturing and analyzing browser history using browser history tools is to gain insights into a user's online activity. This can be useful for various purposes, such as:

Monitoring employee internet usage: Companies can use browser history tools to monitor their employees' internet usage to ensure they are not visiting unauthorized or inappropriate websites during work hours.

a) Investigating cybercrimes: Law enforcement agencies can use browser history tools to investigate cybercrimes such as online fraud, identity theft, and cyberstalking.

b) Enhancing cybersecurity: IT professionals can use browser history tools to detect and prevent malware attacks by analysing browsing patterns and detecting any suspicious activity.

To perform a scan of bookmarks, cache data, visited websites, and cookies, a browser history tool can be used. These tools can capture and analyse the user's browsing history and provide a detailed report of the user's online activity. The scan can be used to identify any suspicious

activity, unauthorized access to websites, or malicious software that may have been installed on the system. This information can then be used to take necessary actions such as blocking certain websites, removing malware or viruses, and strengthening cybersecurity measures.

1.2) Scope of the project:

The scope of capturing and analysing browser history using a browser history tool that can scan bookmarks, cache data, visited websites, and cookies can vary depending on the purpose and context of the analysis. Here are some potential scopes:

a) Security and Forensics: In the context of security and forensics, analysing browser history can help identify potential security breaches, malware infections, and unauthorized access to sensitive information. The scope of analysis can include identifying suspicious or malicious websites, tracking user behaviour and activity, and detecting attempts to cover tracks or erase browsing history.

b) Marketing and Advertising: In the context of marketing and advertising, analysing browser history can help identify user preferences, interests, and behaviour patterns. The scope of analysis can include tracking user visits to specific websites, analysing the content and topics of visited pages, and profiling user demographics and interests based on browsing behaviour.

c)User Experience and Design: In the context of user experience and design, analysing browser history can help improve website usability, navigation, and content. The scope of analysis can include identifying user needs and goals, evaluating user satisfaction and engagement, and testing website performance and accessibility.

d)Research and Analysis: In the context of research and analysis, analysing browser history can help gather data and insights on user behaviour, trends, and preferences. The scope of analysis can include collecting data on website traffic, analysing user demographics and behaviour patterns, and identifying correlations and insights based on browsing history.

It is important to note that capturing and analysing browser history raises important ethical and privacy concerns and must be done by legal and ethical guidelines. Additionally, users must be informed and give consent before their browsing history is captured and analysed.

CHAPTER-02

System Description

Browser history tools are software features that allow users to track and view the websites and pages they have visited using their web browser. These tools are integrated into most modern web browsers and can be accessed through the browser's settings or menu options.

The primary purpose of browser history tools is to provide users with a record of their online activity, allowing them to quickly revisit previously accessed sites or pages. History tools typically display a chronological list of URLs visited, including the date and time of each visit. Some history tools offer additional features such as search functionality, the ability to delete specific items or clear the entire history, and the option to exclude certain websites or pages from being recorded. History tools may also include privacy settings that allow users to control what information is recorded and how it is used. For example, users may choose to enable private browsing modes that prevent the browser from recording any history or tracking data during a browsing session. Overall, browser history tools are a valuable feature that can help users manage their browsing habits and streamline their online experiences.

2.1) Functional/Non-Functional Dependencies:

Yes, functional and non-functional dependencies are used in open-source tools that manage browser history.

Functional dependencies refer to the relationships between different features and functionalities of the tool. For example, a browser history tool may have a functional dependency between the "search" feature and the "filter" feature, where the filter feature depends on the search feature to work properly.

Non-functional dependencies, on the other hand, refer to the relationships between the tool's features and the underlying infrastructure or technology that it relies on. For example, a browser history tool may have a non-functional dependency on the browser's cache, where the tool relies on the cache to retrieve and store browsing data efficiently.

These dependencies are important to consider when developing and testing open-source tools for managing browser history, as they can impact the tool's functionality, performance, and

overall user experience. By identifying and managing these dependencies, developers can ensure that their tools work reliably and efficiently for users.

CHAPTER-03

Analysis Report

3.1) System Snapshots and Full Analysis Report

Step1: Installation of Brower History Tool to capture the data from Browser.

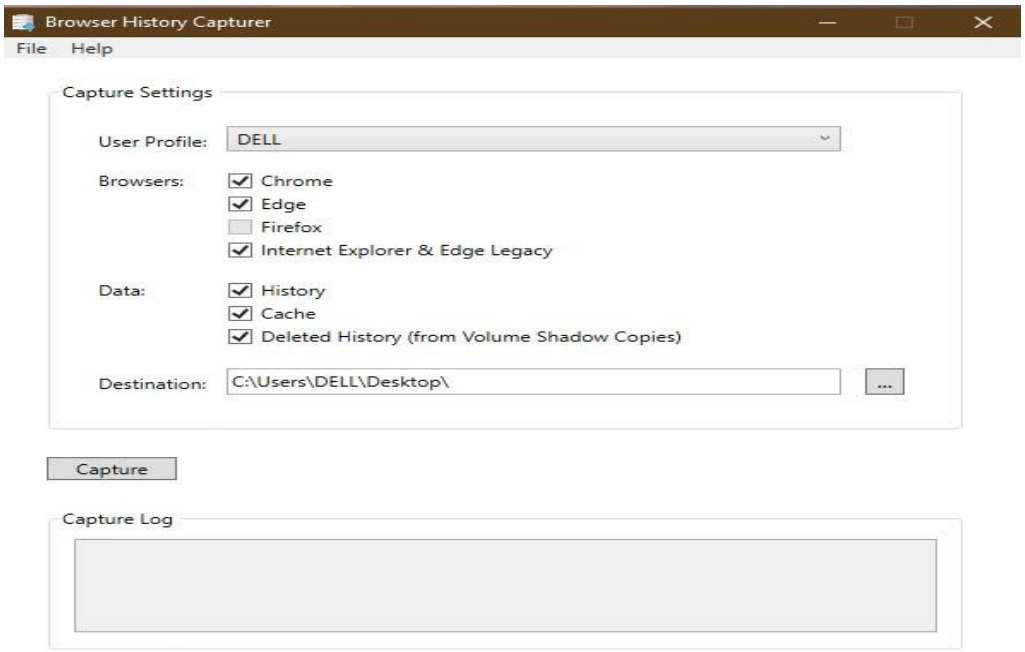

Figure 1. Installation of Browser history tools

Step 2: Click on capture then the system creates a folder (Capture).

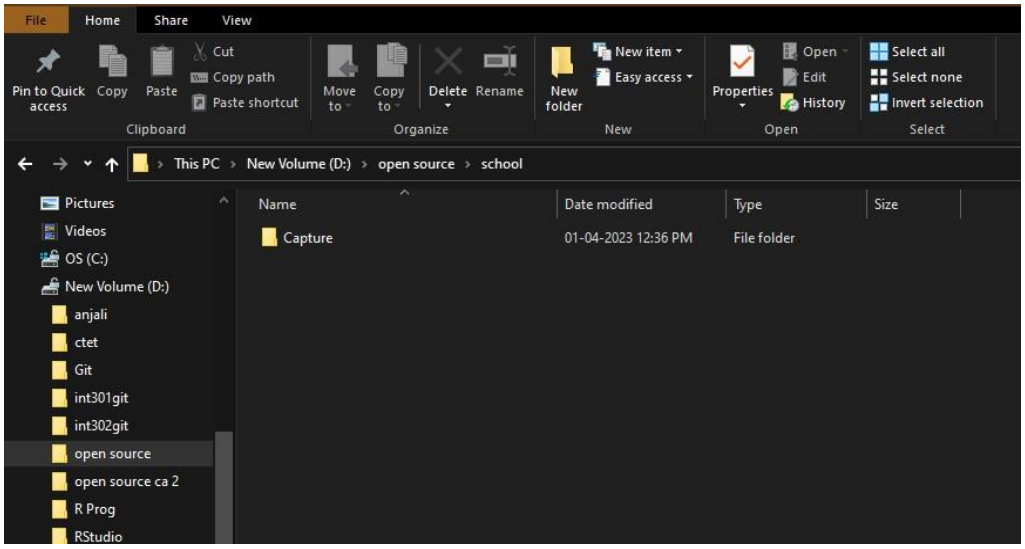

Figure 2. Folder of capture data

Step 3: In capture folders 3 folders are created, are Chrome, Edge, and Internet Explores.

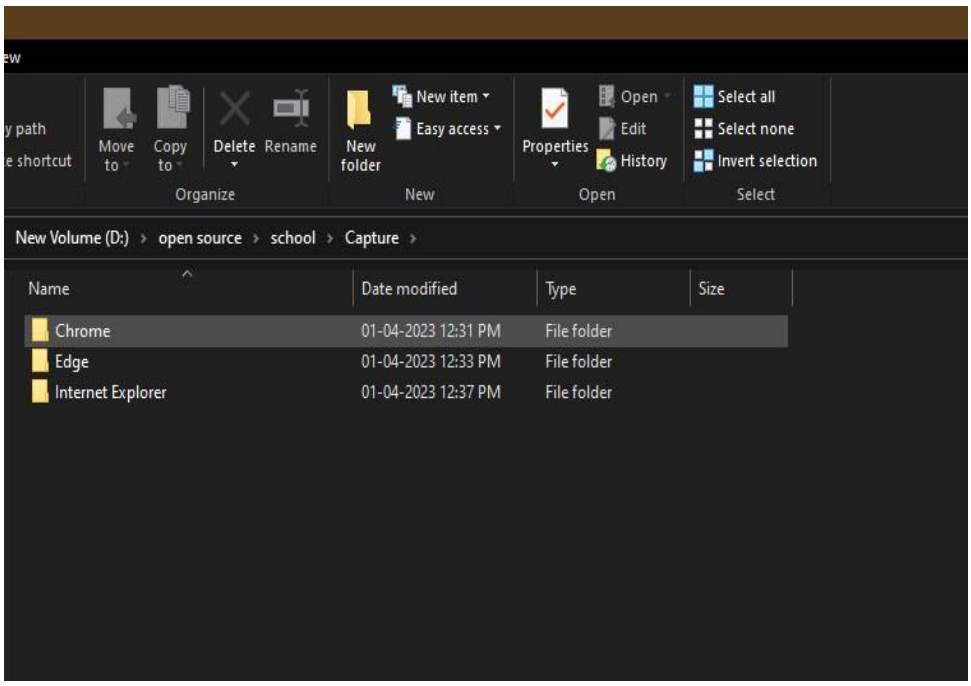

Figure 3. Folder of Chrome, Edges, and Internet Explorer

Step 4: Click on Chrome then profiles folder is there.

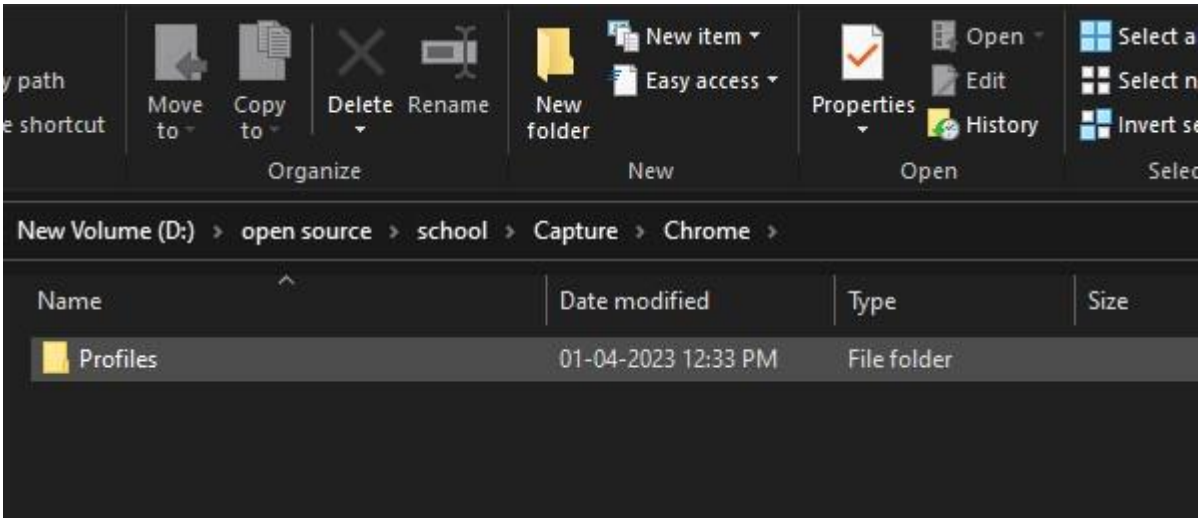

Figure 4. Profiles folder

Step 5:click on the Profile folder there are 2 folders, one is default, and other on is Profile 2.

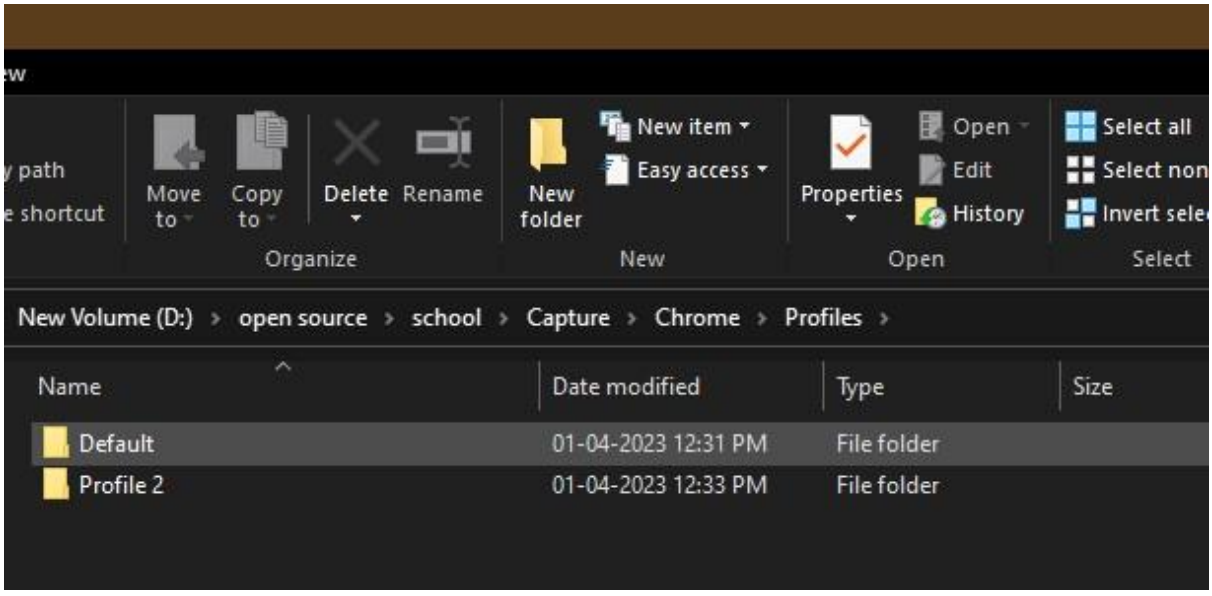

Figure 5. Default and profile 2 folders

Step 6: Click on the default folder there is two folders, one is Cache and other one is History.

Then click on the Cache folder.

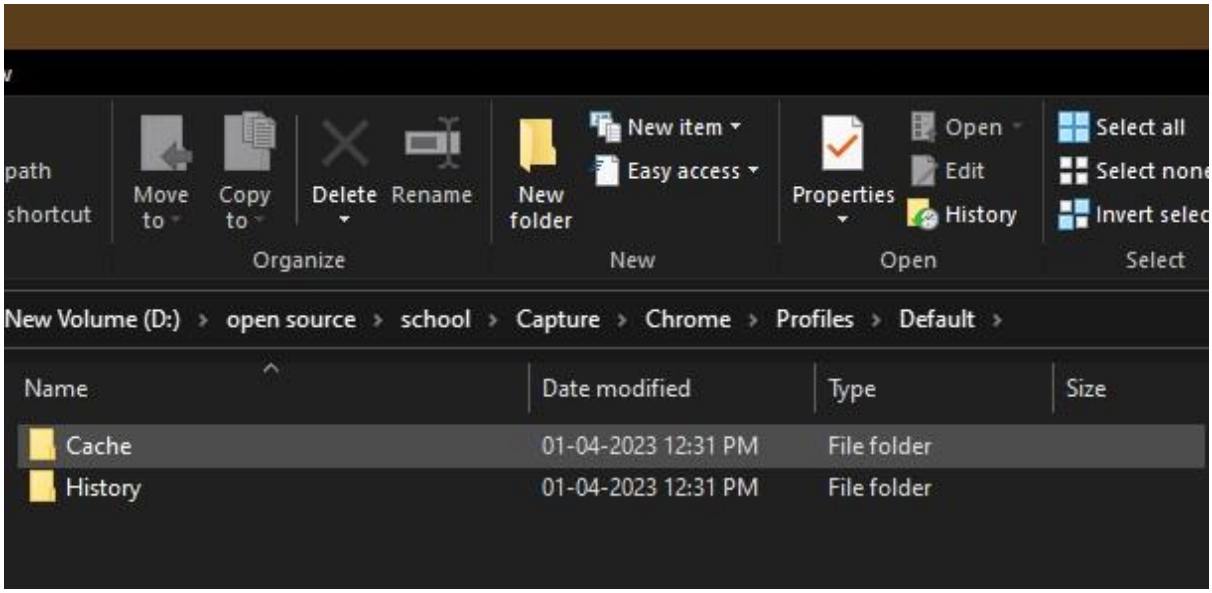

Figure 6. Cache and History folder

Step 7: After clicking on cache folder, a cache data folder is there, we all cache data is stored.

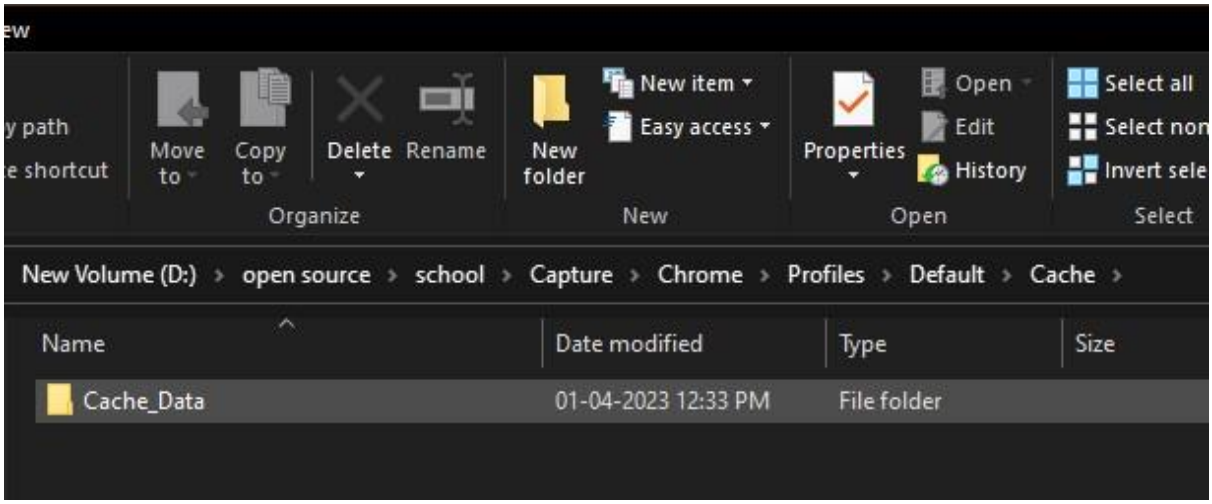

Figure 7. Cache data folders

Step 8: After click on Cache data, all files open of Cache data.

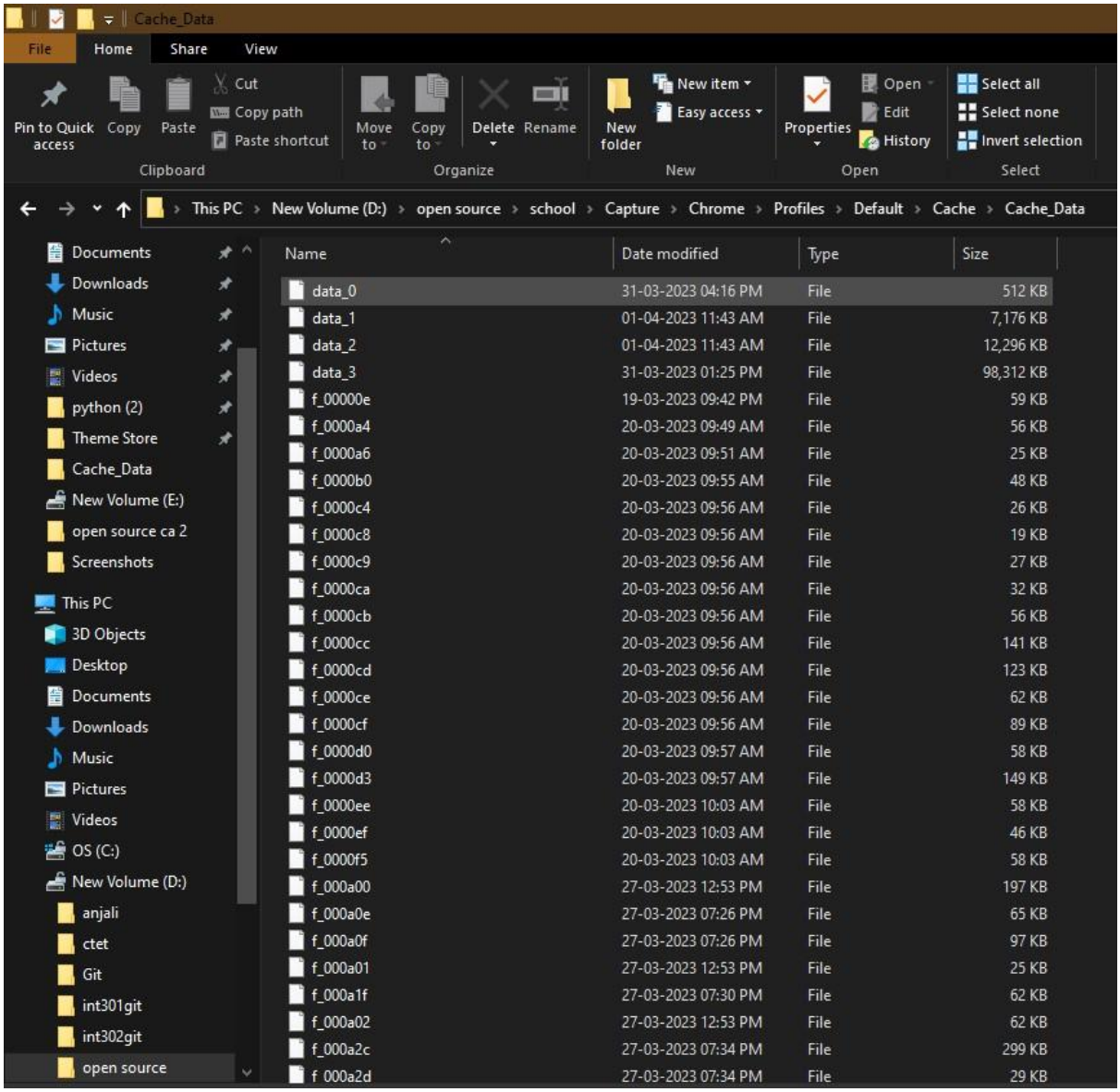

Figure 8. Cache data file.

Step 9: Click on the edge folder there are the file of Sessions, bookmarks, favicons, and History, etc.

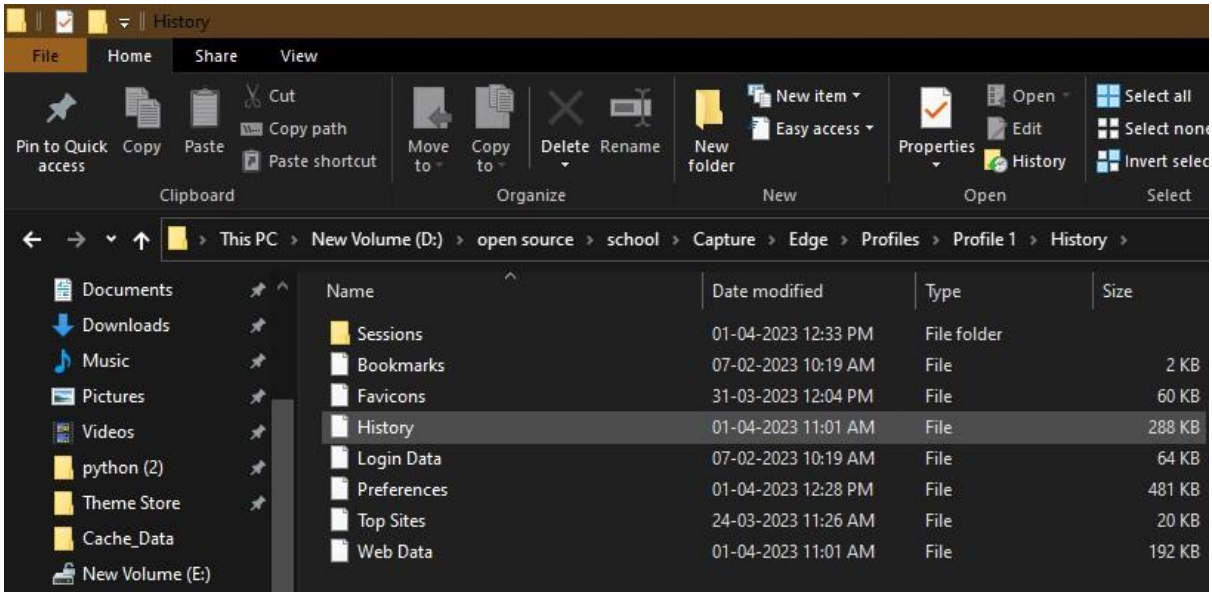

Figure 9. Edge History Folders.

Step 10: In Internet Explorer, there are 4 folders where our data is stored.

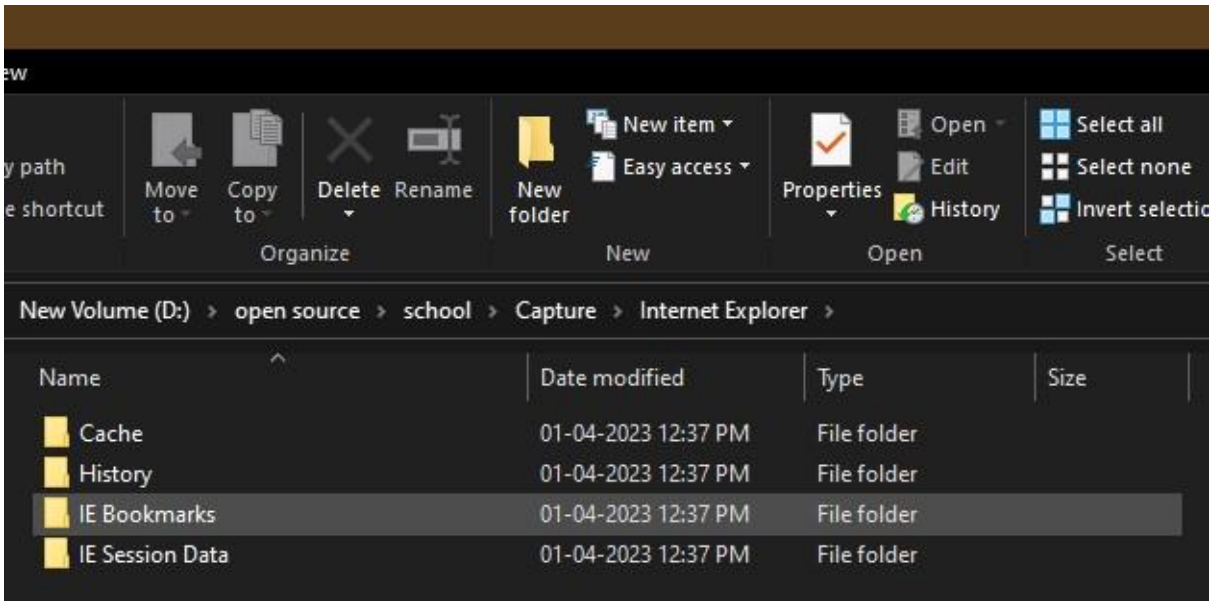

Figure 10. Folders Internet Explorer

Reference:

[1] https://ieeexplore.ieee.org/document/6524415?fbclid=IwAR2G2rRL_55D1D9N47deGryz6AJIxmFQ7eC1HCIvei_-VgJi2DMSjHMzau8 [Accessed:02/14/2019]

[2] https://pdfs.semanticscholar.org/8625/a3b17d199e5cabbb796bad0df56a7979c77c.pdf [Accessed:02/14/2019]

[3] https://ieeexplore.ieee.org/document/8228692 [Accessed:02/14/2019]

[4] https://www.virustotal.com/ [Accessed:02/14/2019]

[5] https://cuckoosandbox.org/ [Accessed:02/14/2019]

[6] https://www.systoolsgroup.com/email-forensics.html . [Accessed:02/14/2019]

[7] https://www.foxtonforensics.com/browser-history-capturer/download