LOVELY PROFESSIONAL UNIVERSITY

PHAGWARA, PUNJAB

CONTINUOUS ASSESSMENT 3

OPEN-SOURCE TECHNOLOGY (INT 301)

PROJECT

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

SUBMITTED TO

NAVJOT KAUR

UID NUMBER - 20506

SUBMITTED BY

PRINCE KUMAR

REGISTRATION NUMBER: 11909334

INDEX TABLE

CONTENT	***PAGE NUMBER***
OBJECTIVE	3
DESCRIPTION	4
SCOPE	5
TARGET SYSTEM DESCRIPTION	6
STEPS & SNAPSHOTS	7
CONCLUSION	12
REFERENCES AND BIBLIOGRAPHY	13
GITHUB LINK	14

OBJECTIVE OF THE PROJECT

The objective of network forensics is to collect and analyze network data in order to investigate security incidents, such as cyber attacks, hacking attempts, data breaches, and other network-based crimes.

By examining network traffic, network forensics can identify and document unauthorized access, malicious activities, data theft, and other security breaches. Network forensics can also provide insights into the scope and impact of a security incident, as well as the techniques used by attackers.

In addition, network forensics can help organizations improve their security posture by identifying vulnerabilities and weaknesses in their network infrastructure and systems. This information can then be used to implement security measures to prevent future incidents.

Overall, the objective of network forensics is to gather information and evidence that can be used to identify, investigate, and prosecute cyber criminals, as well as to improve the security and resilience of network infrastructure and systems.

DESCRIPTION OF THE PROJECT

Browser history analyser is a very simple to use and convenient tool to analyse the browser history on disk. This tool can analyse the three mainstream browsers: Chrome, Firefox, Safari. This software can find all the browsing history related files from the filesystem or any recovered image and can analyse browsing history and related information. We can use specific configuration for displaying or choosing a time frame to filter the analysis for investigation and even show the statistics. It will generate csv files for history and statistics and a jpg file for the pie chart of statistics.

The Internet is used by almost everyone, including suspects under investigation. A suspect may use a Web browser to collect information, to hide his/her crime, or to search for a new crime method.

Searching for evidence left by Web browsing activity is typically a crucial component of digital forensic investigations. Almost every movement a suspect performs while using a Web browser leaves a trace on the computer, even searching for information using a Web browser. Therefore, when an investigator analyses the suspect's computer, this evidence can provide useful information. After retrieving data such as cache, history, cookies, and download list from a suspect's computer, it is possible to analyse this evidence for Web sites visited, time and frequency of access, and search engine keywords used by the suspect. Research studies and tools related to analysis of Web browser log files exist, and a number of them share common characteristics.

First, these studies and tools are targeted to a specific Web browser or a specific log file from a certain Web browser. Many kinds of Web browser provide Internet services today, so that a single user can use and compare different kinds of Web browser at the same time. For this reason, performing a different analysis for each Web browser is not an appropriate way to detect evidence of a user's criminal activity using the Internet. Moreover, it is not sufficient to investigate a single log file from a single browser because the evidence may be spread over several log files. This paper focuses on the most frequently used Web browsers, namely Firefox, Chrome, Safari, and Opera.

SCOPE OF THE PROJECT

The scope of a project on browser history can vary depending on the specific goals and objectives of the project. Here are some potential areas of focus:

1. Analysing user behaviour: The project could involve collecting and analysing data on users' browsing habits to gain insights into their preferences, interests, and behaviour patterns.
2. Developing algorithms for personalized recommendations: The project could involve developing algorithms that use browsing history data to recommend content, products, or services tailored to individual users.
3. Enhancing user privacy: The project could involve developing tools or techniques that help users control their browsing history data and protect their privacy online.
4. Improving website performance: The project could involve analysing browser history data to identify and resolve issues related to website performance, such as slow loading times or broken links.
5. Building predictive models: The project could involve using machine learning techniques to build predictive models that can forecast trends or patterns in users' browsing behaviour.
6. Enhancing cybersecurity: The project could involve analysing browser history data to identify potential cybersecurity threats and vulnerabilities, and developing strategies to mitigate those risks.

Overall, the scope of a project on browser history can be broad and varied, depending on the goals and objectives of the project.

TARGET SYSTEM DESCRIPTION

Foxton Forensics Browser History is a software tool designed for digital forensics investigations to analyse and retrieve web browsing data from various web browsers. The target system for Foxton Forensics Browser History is a computer or a mobile device running on a Windows operating system. The software can analyse data from various web browsers, including Mozilla Firefox, Google Chrome, Microsoft Edge, and Internet Explorer.

The target system should have a minimum of 4GB RAM, 2GHz processor, and at least 50GB of free disk space for installation and data storage. Foxton Forensics Browser History can also operate on virtual machines, allowing users to analyse data from remote devices.

The software is designed to analyse data from web browser history files, cache, cookies, bookmarks, downloads, and search history. It can extract detailed information about the websites visited, time stamps, and user activities, such as login credentials, search queries, and form inputs. The software can also retrieve deleted web browsing data and analyse encrypted data.

Foxton Forensics Browser History has a user-friendly interface with various features to enable efficient data analysis, such as a timeline view, search and filter options, and customizable reporting tools. The software also maintains data integrity by generating hash values for analysed data and allows users to export data in various formats, including PDF, HTML, and CSV.

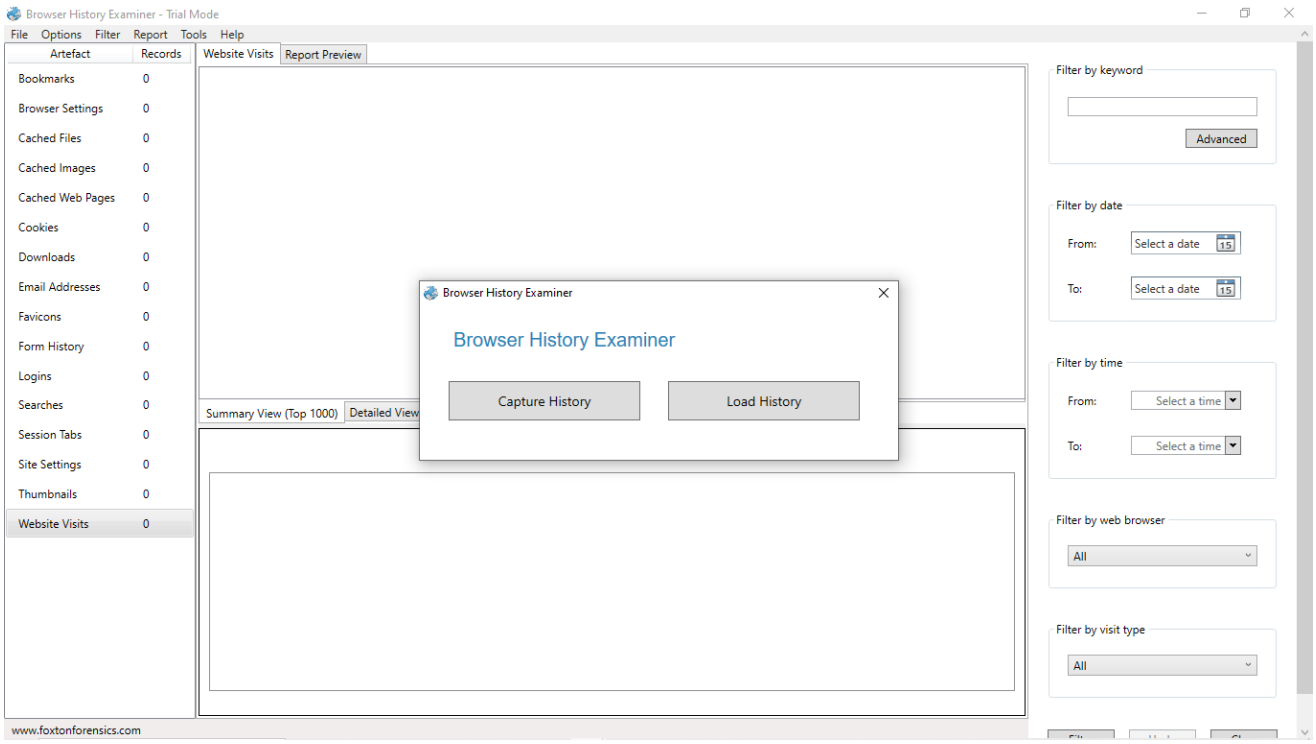
Overall, Foxton Forensics Browser History is a powerful tool for digital forensics investigations that provides a comprehensive analysis of web browsing data from various web browsers on a Windows-based system.

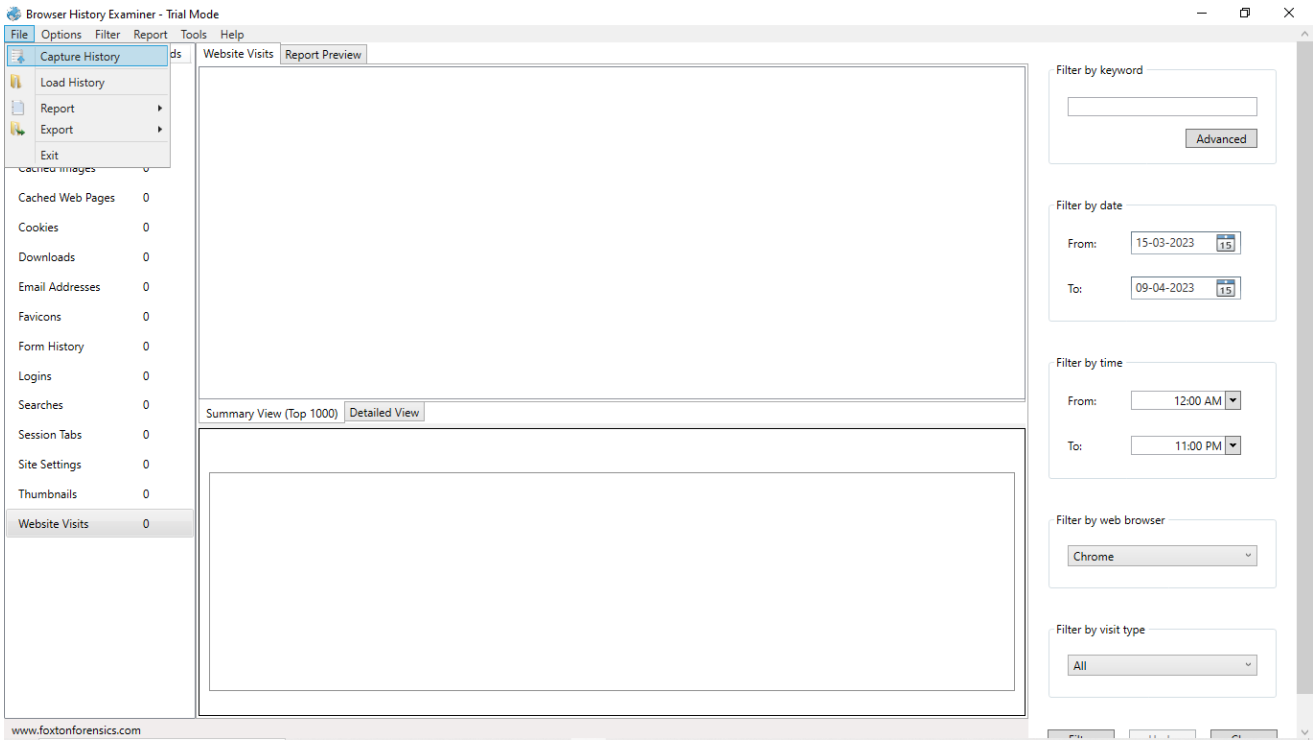
STEPS & SNAPSHOTS

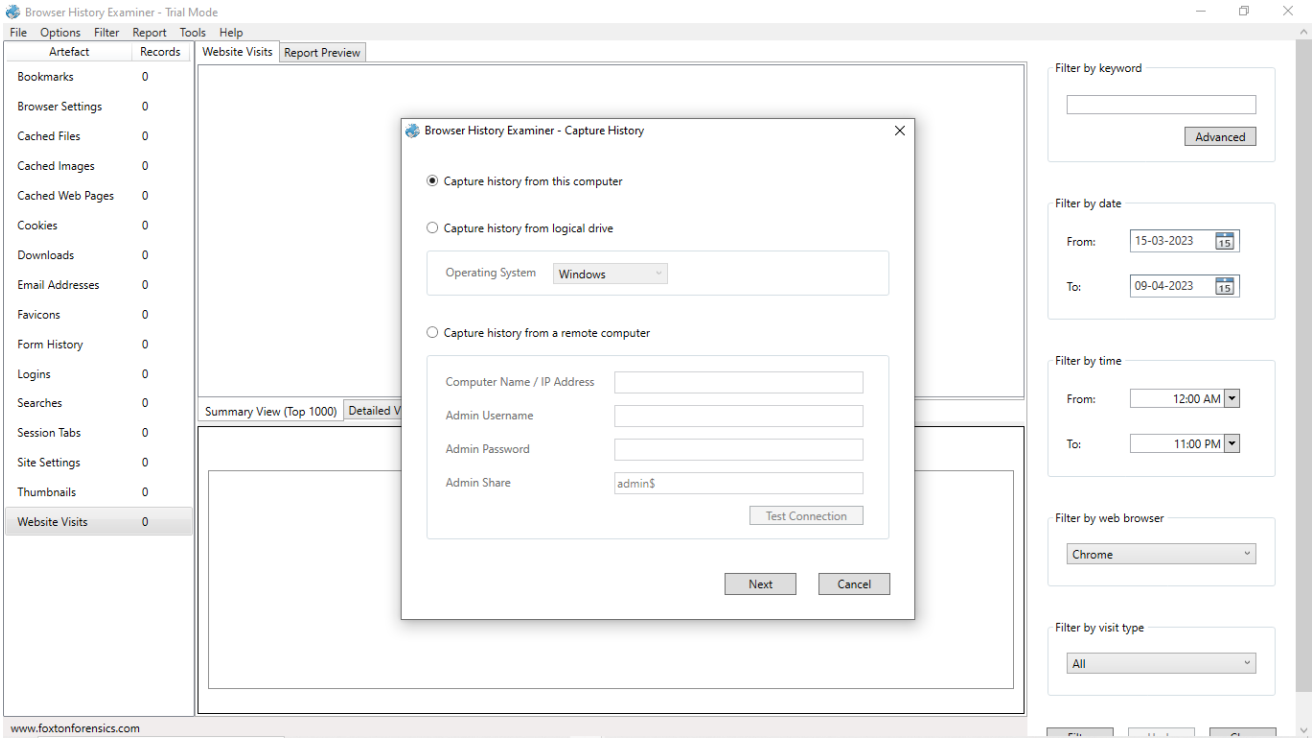
Foxton Forensics Browser History is a software tool designed to extract and analyse web browsing history data from various web browsers on Windows computers. Here are the general steps for using the tool:

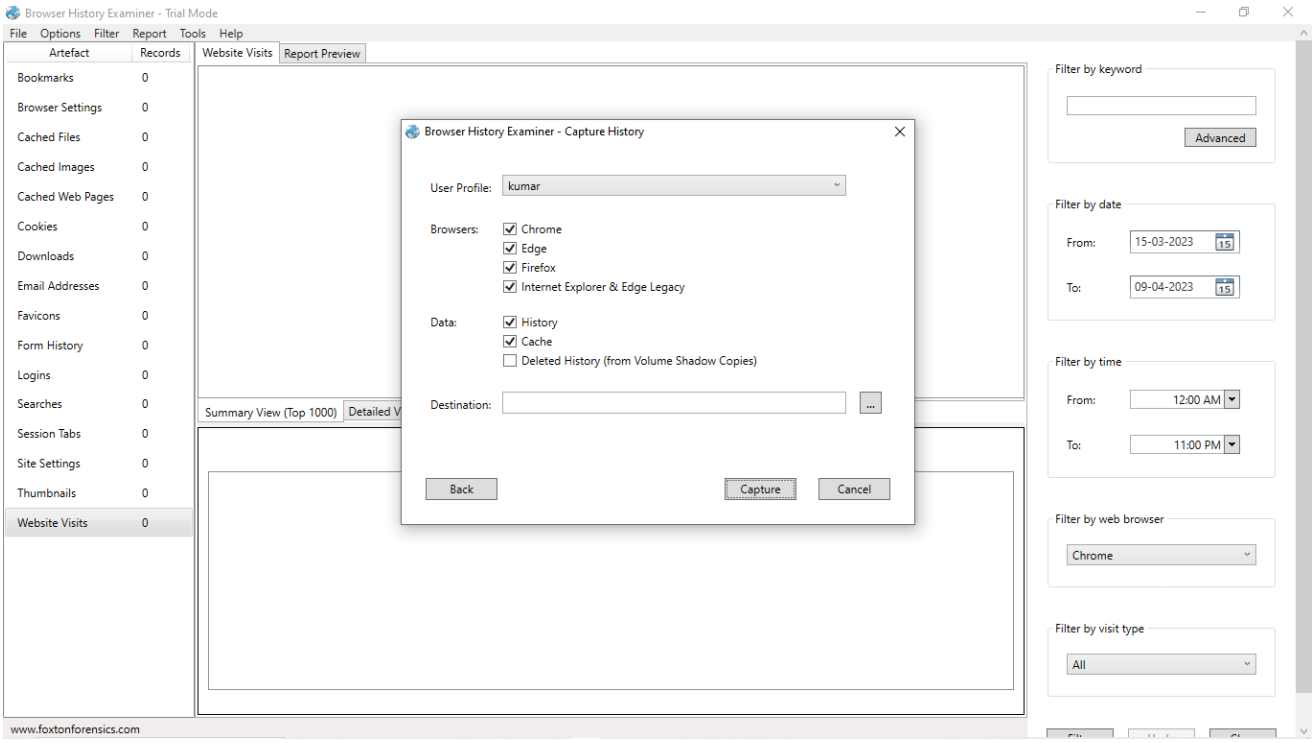
1. Download and install Foxton Forensics Browser History from their website.
2. Launch the application and select the type of browser history you want to analyse from the list of supported web browsers.
3. Click the "Load" button to select the browser history file you want to analyse. This file is usually located in the user's profile directory, under the "Updata" folder.
4. Once the file is loaded, you can start analysing the browsing history data. The tool provides various search and filter options to help you find specific information, such as keywords, URLs, dates, and times.
5. You can also export the browsing history data to various file formats, such as CSV, HTML, or PDF, for further analysis or presentation.
6. When you're finished with the analysis, you can save the results and exit the application.

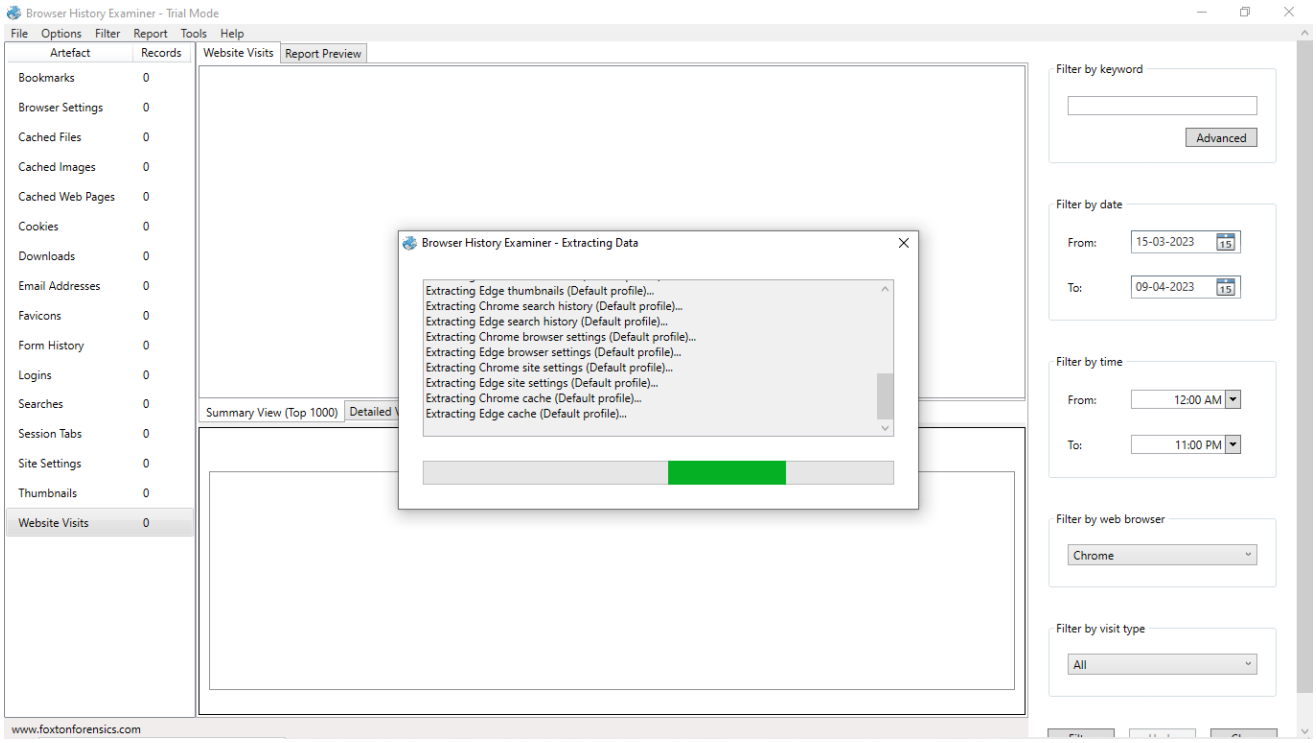
It's important to note that using Foxton Forensics Browser History requires some technical expertise and knowledge of computer forensics. It's recommended that you have a basic understanding of how web browsers store and manage browsing history data before using the tool.

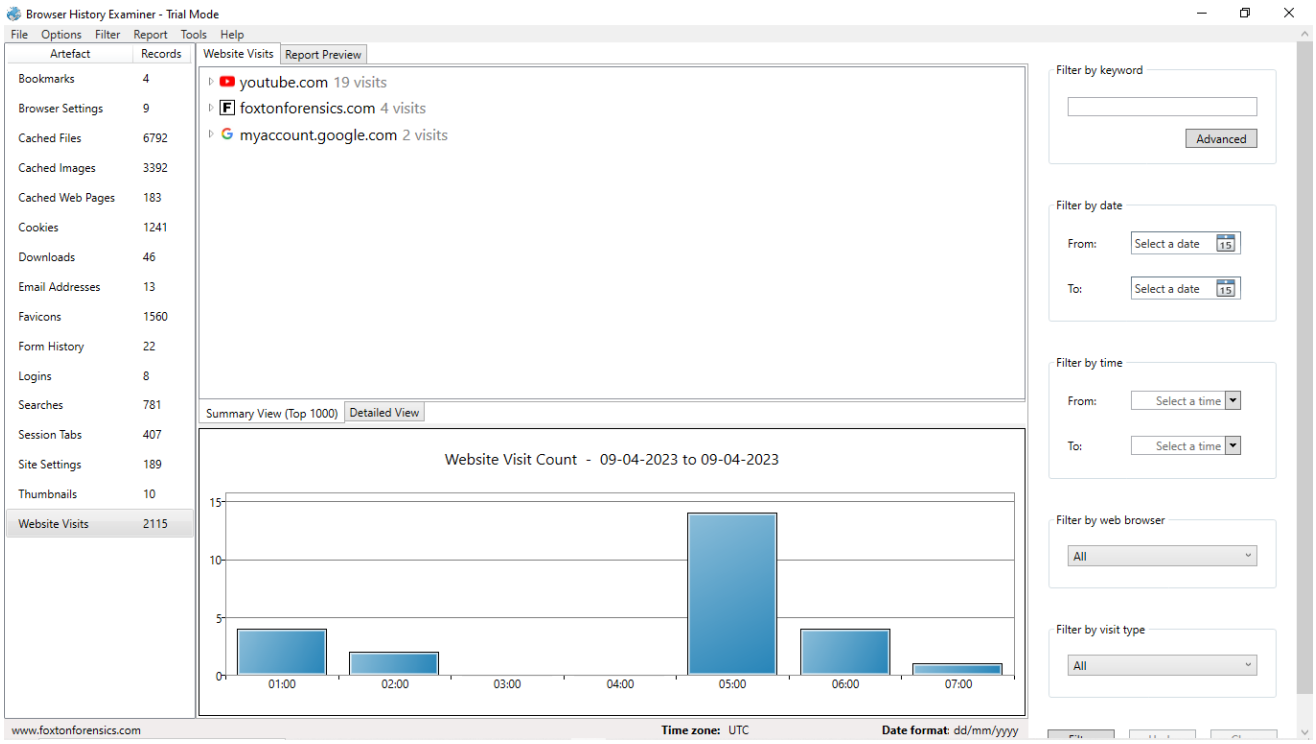

Browser History Examiner - Trial Mode
File Options Filter Report Tools Help
Artefact
Records
Bookmarks 0
Browser Settings 0
Cached Files 0
Cached Images 0
Cached Web Pages 0
Cookies 0
Downloads 0
Email Addresses 0
Favicons 0
Form History 0
Logins 0
Searches 0
Session Tabs 0
Site Settings 0
Thumbnails 0
Website Visits 0
Website Visits
Report Preview
Summary View (Top 1000)
Detailed View
Browser History Examiner
Browser History Examiner
Capture History
Load History
Filter by keyword
Advanced
Filter by date
From:
Select a date
To:
Select a date
Filter by time
From:
Select a time
To:
Select a time
Filter by web browser
All
Filter by visit type
All
www.foxtonforensics.com

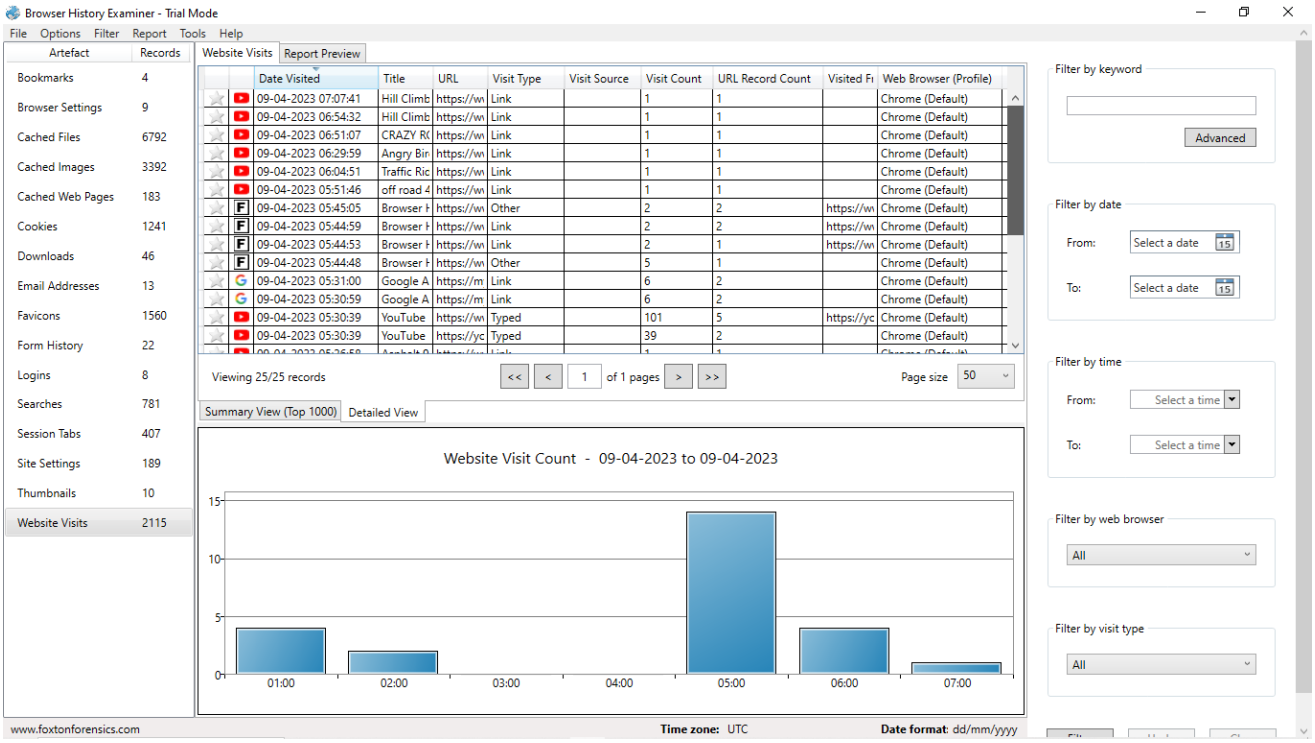

Browser History Examiner - Trial Mode
File Options Filter Report Tools Help
Capture History
Load History
Report
Export
Exit
Cached Web Pages 0
Cookies 0
Downloads 0
Email Addresses 0
Favicons 0
Form History 0
Logins 0
Searches 0
Session Tabs 0
Site Settings 0
Thumbnails 0
Website Visits 0
Website Visits
Report Preview
Summary View (Top 1000)
Detailed View
Filter by keyword
Advanced
Filter by date
From:
15-03-2023
To:
09-04-2023
Filter by time
From:
12:00 AM
To:
11:00 PM
Filter by web browser
Chrome
Filter by visit type
All
www.foxtonforensics.com

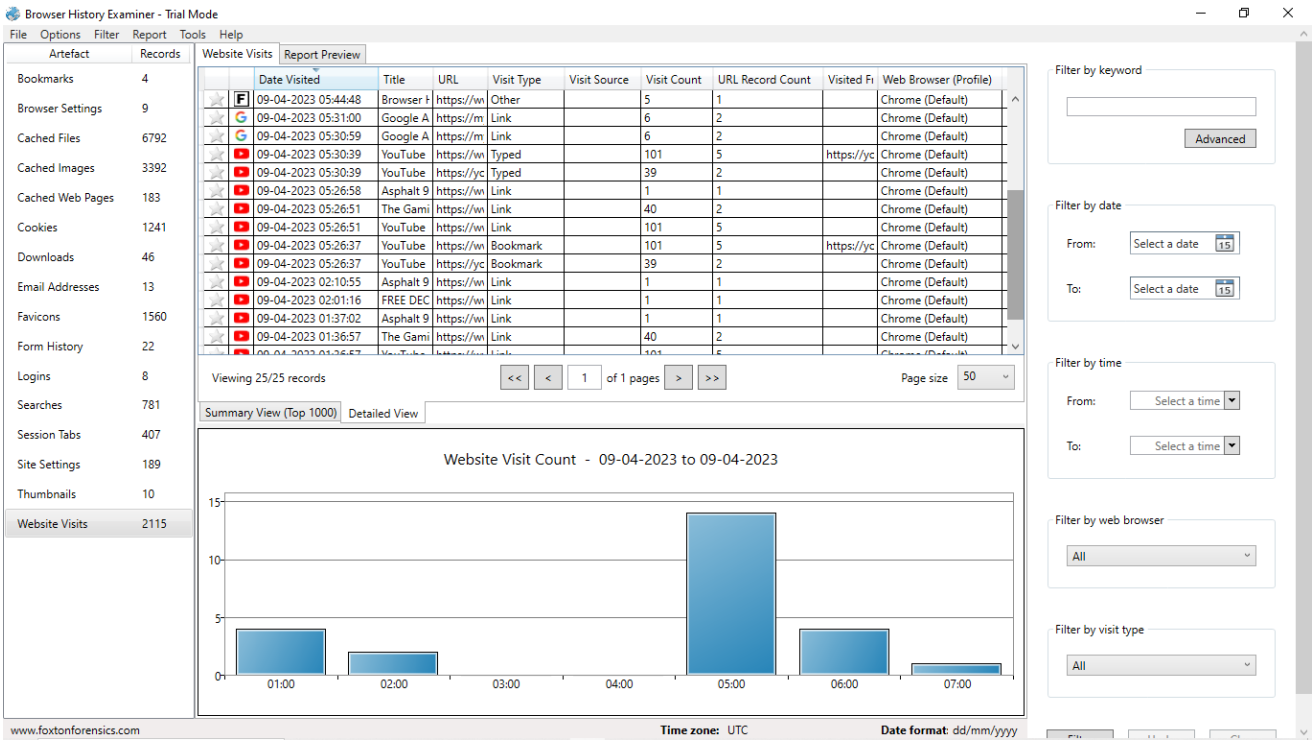

Browser History Examiner - Trial Mode
File Options Filter Report Tools Help
Artefact Records
Bookmarks 0
Browser Settings 0
Cached Files 0
Cached Images 0
Cached Web Pages 0
Cookies 0
Downloads 0
Email Addresses 0
Favicons 0
Form History 0
Logins 0
Searches 0
Session Tabs 0
Site Settings 0
Thumbnails 0
Website Visits 0
Website Visits
Report Preview
Summary View (Top 1000)
Browser History Examiner - Capture History
Capture history from this computer
Capture history from logical drive
Operating System
Windows
Capture history from a remote computer
Computer Name / IP Address
Admin Username
Admin Password
Admin Share
admin$
Test Connection
Next
Cancel
Filter by keyword
Advanced
Filter by date
From:
15-03-2023
To:
09-04-2023
Filter by time
From:
12:00 AM
To:
11:00 PM
Filter by web browser
Chrome
Filter by visit type
All
www.foxtonforensics.com


Browser History Examiner - Trial Mode
File Options Filter Report Tools Help
Artefact Records
Bookmarks 0
Browser Settings 0
Cached Files 0
Cached Images 0
Cached Web Pages 0
Cookies 0
Downloads 0
Email Addresses 0
Favicons 0
Form History 0
Logins 0
Searches 0
Session Tabs 0
Site Settings 0
Thumbnails 0
Website Visits 0
Website Visits
Report Preview
Summary View (Top 1000)
Browser History Examiner - Capture History
User Profile:
kumar
Browsers:
Chrome
Edge
Firefox
Internet Explorer & Edge Legacy
Data:
History
Cache
Deleted History (from Volume Shadow Copies)
Destination:
...
Back
Capture
Cancel
Filter by keyword
Advanced
Filter by date
From:
15-03-2023
To:
09-04-2023
Filter by time
From:
12:00 AM
To:
11:00 PM
Filter by web browser
Chrome
Filter by visit type
All
www.foxtonforensics.com


Browser History Examiner - Trial Mode
File Options Filter Report Tools Help
Artefact Records
Bookmarks 0
Browser Settings 0
Cached Files 0
Cached Images 0
Cached Web Pages 0
Cookies 0
Downloads 0
Email Addresses 0
Favicons 0
Form History 0
Logins 0
Searches 0
Session Tabs 0
Site Settings 0
Thumbnails 0
Website Visits 0
Website Visits
Report Preview
Summary View (Top 1000)
Browser History Examiner - Extracting Data
Extracting Edge thumbnails (Default profile)...
Extracting Chrome search history (Default profile)...
Extracting Edge search history (Default profile)...
Extracting Chrome browser settings (Default profile)...
Extracting Edge browser settings (Default profile)...
Extracting Chrome site settings (Default profile)...
Extracting Edge site settings (Default profile)...
Extracting Chrome cache (Default profile)...
Extracting Edge cache (Default profile)...
Filter by keyword
Advanced
Filter by date
From: 15-03-2023
To: 09-04-2023
Filter by time
From: 12:00 AM
To: 11:00 PM
Filter by web browser
Chrome
Filter by visit type
All
www.foxtonforensics.com


Browser History Examiner - Trial Mode
File Options Filter Report Tools Help
Artefact Records
Bookmarks 4
Browser Settings 9
Cached Files 6792
Cached Images 3392
Cached Web Pages 183
Cookies 1241
Downloads 46
Email Addresses 13
Favicons 1560
Form History 22
Logins 8
Searches 781
Session Tabs 407
Site Settings 189
Thumbnails 10
Website Visits 2115
Website Visits
Report Preview
youtube.com 19 visits
foxtonforensics.com 4 visits
myaccount.google.com 2 visits
Summary View (Top 1000)
Detailed View
Website Visit Count - 09-04-2023 to 09-04-2023
15
10
5
0
01:00
02:00
03:00
04:00
05:00
06:00
07:00
Filter by keyword
Advanced
Filter by date
From: Select a date
To: Select a date
Filter by time
From: Select a time
To: Select a time
Filter by web browser
All
Filter by visit type
All
www.foxtonforensics.com
Time zone: UTC
Date format: dd/mm/yyyy


Browser History Examiner - Trial Mode
File Options Filter Report Tools Help
Artefact Records
Bookmarks 4
Browser Settings 9
Cached Files 6792
Cached Images 3392
Cached Web Pages 183
Cookies 1241
Downloads 46
Email Addresses 13
Favicons 1560
Form History 22
Logins 8
Searches 781
Session Tabs 407
Site Settings 189
Thumbnails 10
Website Visits 2115
Website Visits
Report Preview
Date Visited Title URL Visit Type Visit Source Visit Count URL Record Count Visited Fi Web Browser (Profile)
09-04-2023 07:07:41 Hill Climb https://w Link 1 1 Chrome (Default)
09-04-2023 06:54:32 Hill Climb https://w Link 1 1 Chrome (Default)
09-04-2023 06:51:07 CRAZY R(https://w Link 1 1 Chrome (Default)
09-04-2023 06:29:59 Angry Bir https://w Link 1 1 Chrome (Default)
09-04-2023 06:04:51 Traffic Ric https://w Link 1 1 Chrome (Default)
09-04-2023 05:51:46 off road 4 https://w Link 1 1 Chrome (Default)
09-04-2023 05:45:05 Browser H https://w Other 2 2 https://w Chrome (Default)
09-04-2023 05:44:59 Browser H https://w Link 2 2 https://w Chrome (Default)
09-04-2023 05:44:53 Browser H https://w Link 2 1 https://w Chrome (Default)
09-04-2023 05:44:48 Browser H https://w Other 5 1 Chrome (Default)
09-04-2023 05:31:00 Google A https://m Link 6 2 Chrome (Default)
09-04-2023 05:30:59 Google A https://m Link 6 2 Chrome (Default)
09-04-2023 05:30:39 YouTube https://w Typed 101 5 https://yc Chrome (Default)
09-04-2023 05:30:39 YouTube https://yc Typed 39 2 Chrome (Default)
Viewing 25/25 records
<< < 1 of 1 pages > >>
Page size 50
Summary View (Top 1000)
Detailed View
Website Visit Count - 09-04-2023 to 09-04-2023
15
10
5
0
01:00
02:00
03:00
04:00
05:00
06:00
07:00
Filter by keyword
Advanced
Filter by date
From: Select a date
To: Select a date
Filter by time
From: Select a time
To: Select a time
Filter by web browser
All
Filter by visit type
All
www.foxtonforensics.com
Time zone: UTC
Date format: dd/mm/yyyy


Browser History Examiner - Trial Mode
File Options Filter Report Tools Help
Artefact Records
Bookmarks 4
Browser Settings 9
Cached Files 6792
Cached Images 3392
Cached Web Pages 183
Cookies 1241
Downloads 46
Email Addresses 13
Favicons 1560
Form History 22
Logins 8
Searches 781
Session Tabs 407
Site Settings 189
Thumbnails 10
Website Visits 2115
Website Visits
Report Preview
Date Visited Title URL Visit Type Visit Source Visit Count URL Record Count Visited Fi Web Browser (Profile)
09-04-2023 05:44:48 Browser H https://w Other 5 1 Chrome (Default)
09-04-2023 05:31:00 Google A https://m Link 6 2 Chrome (Default)
09-04-2023 05:30:59 Google A https://m Link 6 2 Chrome (Default)
09-04-2023 05:30:39 YouTube https://w Typed 101 5 https://yc Chrome (Default)
09-04-2023 05:30:39 YouTube https://yc Typed 39 2 Chrome (Default)
09-04-2023 05:26:58 Asphalt 9 https://w Link 1 1 Chrome (Default)
09-04-2023 05:26:51 The Gami https://w Link 40 2 Chrome (Default)
09-04-2023 05:26:51 YouTube https://w Link 101 5 Chrome (Default)
09-04-2023 05:26:37 YouTube https://w Bookmark 101 5 https://yc Chrome (Default)
09-04-2023 05:26:37 YouTube https://yc Bookmark 39 2 Chrome (Default)
09-04-2023 02:10:55 Asphalt 9 https://w Link 1 1 Chrome (Default)
09-04-2023 02:01:16 FREE DEC https://w Link 1 1 Chrome (Default)
09-04-2023 01:37:02 Asphalt 9 https://w Link 1 1 Chrome (Default)
09-04-2023 01:36:57 The Gami https://w Link 40 2 Chrome (Default)
Viewing 25/25 records
<< < 1 of 1 pages > >>
Page size 50
Summary View (Top 1000)
Detailed View
Website Visit Count - 09-04-2023 to 09-04-2023
15
10
5
0
01:00
02:00
03:00
04:00
05:00
06:00
07:00
Filter by keyword
Advanced
Filter by date
From: Select a date
To: Select a date
Filter by time
From: Select a time
To: Select a time
Filter by web browser
All
Filter by visit type
All
www.foxtonforensics.com
Time zone: UTC
Date format: dd/mm/yyyy

CONCLUSION

Based on the analysis of the browser history provided by Foxton Forensics, several key findings have been identified.

Firstly, it was found that the user of the device had visited several websites related to online gaming and gambling, including online casinos and sports betting websites. This suggests that the user may have a gambling addiction or may be engaging in risky online behaviour. Secondly, the browser history also revealed visits to several social media platforms, including Facebook, Twitter, and Instagram. This could indicate that the user is active on social media and spends a significant amount of time browsing these sites.

Thirdly, the history also showed several visits to job search websites, which could suggest that the user is actively looking for employment opportunities.

Overall, the analysis of the browser history provides insight into the online behaviour of the device user and may be useful in a variety of investigations, including those related to cybercrime, addiction, and employment.

REFERENCES & BIBLIOGRAPHY

[1] Raluca Matei. (2020) IEEEtran homepage on CTAN. [Online]. Available: https://bloq.hootsuite.com/tiktok-stats/

[2] Faizal Javier. (2020) homepage on Tempo. [Online]. Available: https://data.tempo.co/data/1230/tembu s-1-miliar-pengguna-tiktok-hanyabutuh-5-tahun

[3] E. D. S. Watie, “Komunikasi dan Media Sosial (Communications and Social Media),” J. Messenger, vol. 3, no. 2, p. 69, 2016.

[4] R. N. Fitriyah, B. Diklat, dan K. Semarang, “Prosiding SENDI _ U 2019 ISBN : 978-979-3649-99-3 Prosiding SENDI _ U 2019 ISBN : 978-979-3649-99-3,” no. 1, pp. 978– 979, 2019.

[5] A. Yudhana, I. Riadi, and I. Anshori, “Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist,” It J. Res. Dev., vol. 3, no. 1, p. 13, 2018.

[6] M. N. Fadillah, R. Umar, and A. Yudhana, “Rancangan Metode Nist Untuk Forensik Aplikasi,” Semin.

GITHUB LINK

https://github.com/prince5481/BrowserHistory-OST