



الجامعة الدولية للرباط
ⵜⴰⵎⴰⵎⴰⵔⵜ ⵜⴰⵖⵔⴰⵎⵜ | QQΘ◊E
Université Internationale de Rabat

Browser Forensic Report

Made by : Ilias Belharda

Chihab Alaoui

Mohammed Amine Stour

Supervised by: Mr Khalid Choug dali

Academic year : 2024/2025

Table de matières

Introduction	2
Objectives	2
Methodology.....	3
Results.....	6
Limitations and Precautions	12
Conclusion and Recommendations	14
Références	14

Introduction

Browsers have become an inherent part of our virtual life and we all make use of browsers for surfing the internet in some or the other way. Also, browsers can be used not only for surfing, we can make use of browsers for navigating through the file system of the OS.

You might have observed by default browsers store data like search queries, username, password, form data, emails, credit card data and other sensitive information. Also, browsers do contain downloaded media like Images, Videos, Exe's, documents etc. Bookmarks and browser history gives an idea of the user's surfing habit and interest.

You might have realised the browser stores a lot of sensitive information about the user and its surfing habit. Thus they play a very important role in forensics due to the nature and amount of data they store with them.

With the help of **Browser Forensics** and with the assistance of **forensics tools** (we used **browser history Examiner**) one can extract sensitive data and chosen keywords from most web browsers. One can retrieve deleted data and keywords, check whether history was cleared, retrieve artifacts like Cookies, Downloads data, History, Saved Password, websites visited etc. Also, Browser Forensics helps a lot to understand how an attack on a system was conducted, helping in finding the source of Malwares/Adwares/Spywares, Malicious Emails and Phishing Websites etc.



**Browser History
Examiner**
www.p30download.com

There are many web browsers available like Chrome, Firefox, Safari, IE and Opera etc. depending upon the platform being used. In this post, we will be learning about how to conduct forensics for **Google Edge** and **Mozilla Firefox**

Objectives

Judicial Forensics

The objective of investigating digital traces is to demonstrate evidence and facts related to the intrusion, bridging technical cybersecurity investigations with legal proceedings. This allows the victimized organization to compile a case and present well-founded arguments based on findings to a legal representative, such as a lawyer, legal advisor, or forensic expert. Ensuring the collected evidence is admissible and complies with legal standards is critical for initiating legal action, such as lawsuits or filing complaints.

More specifically, forensic analysis remains consistent across investigative techniques, focusing on data acquisition (e.g., disk imaging) and analysis (e.g., timeline reconstruction or pattern recognition). However, the key distinction lies in the type of information collected and how the report is tailored for clarity and legal relevance, ensuring it meets the standards required in court.

Technical Forensics

This approach enables the recovery of digital traces, such as disks, logs, or system journals, to determine the reasons behind the compromise of an organization's system or application. It often involves identifying exploited vulnerabilities (e.g., by a hacker), internal data theft, or human error. By analyzing these root causes, technical forensics bridges investigative insights with actionable security improvements.

In this context, the process is conducted privately, primarily for corrective purposes, allowing for the continuous enhancement of the organization's information system security. The findings are documented and formalized to ensure clarity and to serve as a foundation for future preventive measures and system hardening.

Objectives

1. Identify websites visited from browsing histories.
2. Analyze online behavior through the retrieved data.
3. Highlight key information such as:
 - Dates and times of access.
 - Searches performed.
 - Bookmarks or marked important items.
4. Compare the retrieved data between Firefox and Edge.



Methodology

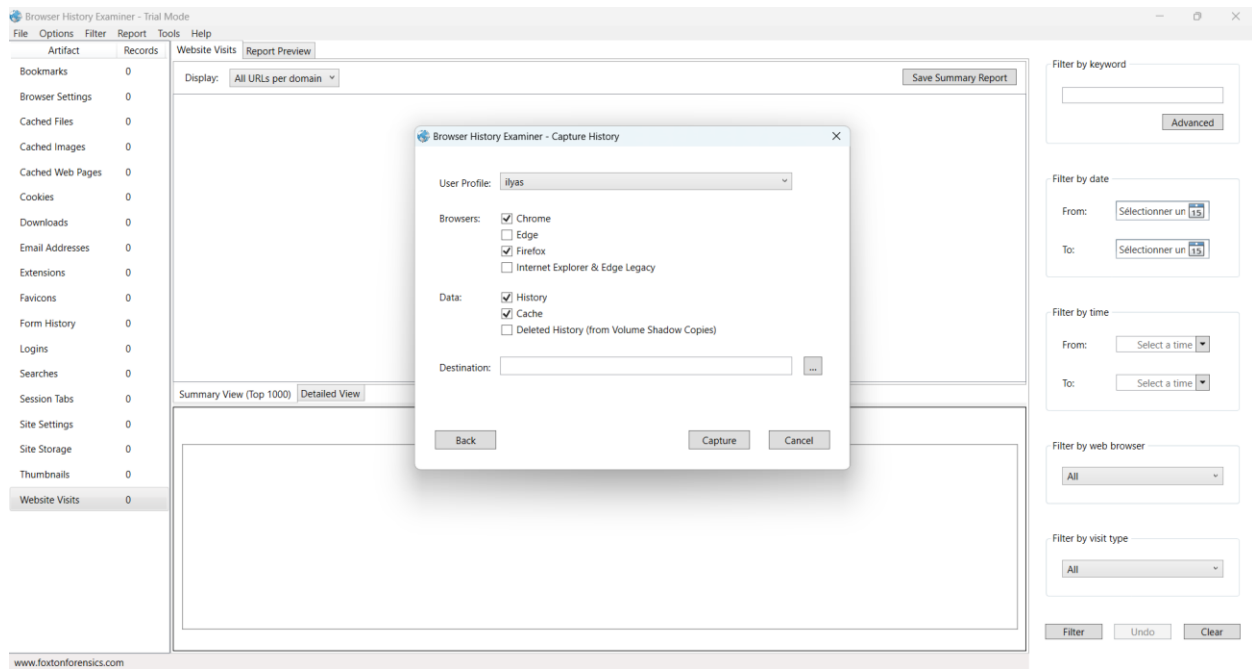
1. Tools Used

The analysis was performed using **Browser History Examiner**, a software tool specialized in extracting and analyzing browser histories. This tool can process SQLite databases used by Firefox and Edge to store their information.

2. Steps of the Process:

○ Data Extraction:

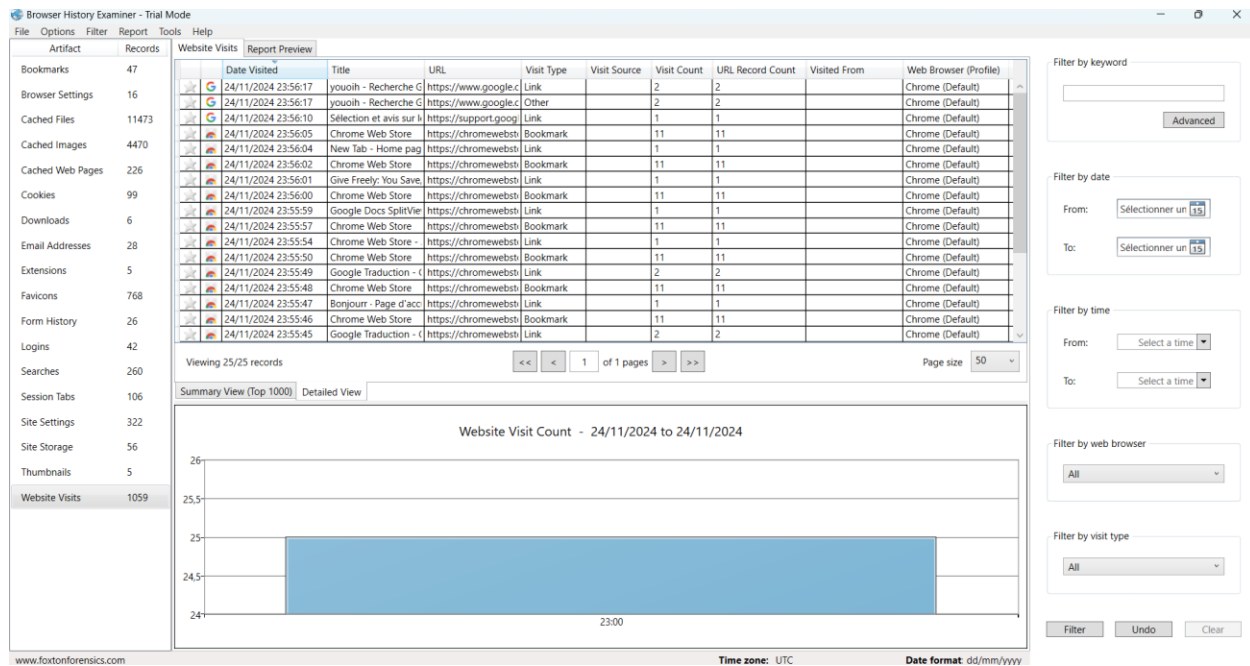
Browser history files located on the operating system were copied into a secure environment for analysis.



○ Data Analysis:

The tool extracted data into tables containing the following information:

- URLs of visited websites.
- Timestamps of visits.
- Number of visits (frequency).
- Search terms used via search engines.
- Information about open sessions.



- **Data Classification and Sorting:**

The data was organized for clearer readability and interpreted according to the defined objectives.

First we explain the **Browser History Examiner** interface:

Main Menu (Top Bar)

- **File:** Import or export data.
- **Options:** Configure general settings for the tool.
- **Filter:** Apply advanced filters to narrow down results (by keywords, dates, times).
- **Report:** Generate a detailed report of the analysis performed.
- **Tools:** Provide additional tools for browser analysis.

Left Panel (List of Artifacts)

- Displays the different categories of artifacts collected from the browser:
 - **Bookmarks:** List of saved favorites.
 - **Browser Settings:** Analyzed browser settings.
 - **Cached Files/Images/Web Pages:** Cached data, including temporarily downloaded pages, files, or images.
 - **Cookies:** Active or saved sessions from visited sites.

- **Downloads:** History of downloaded files.
- **Email Addresses:** Associated email accounts.
- **Searches:** Searches performed in the browser.
- **Logins:** Saved login credentials.

Right Panel (Filtering Area)

- Allows narrowing down the analysis by applying filters:
 - **Keyword:** Search for a specific keyword.
 - **Date:** Limit results to a specific date range.
 - **Time:** Filter by specific times.
 - **Web Browser:** Select a particular browser (in this case, Edge).

Results

1. Browsing History – Firefox

Artifact	Records	Date Added	Last Modified	Title	URL	Web Browser (Profile)
Bookmarks	4	24/11/2024 23:53:44	24/11/2024 23:53:44	Get Help	https://support.mozilla.org/products/firefox	Firefox (4b/vhy4g.defa)
Browser Settings	0	24/11/2024 23:53:44	24/11/2024 23:53:44	Customize Firefox	https://support.mozilla.org/kb/customize-firefox-cont	Firefox (4b/vhy4g.defa)
Cached Files	3	24/11/2024 23:53:44	24/11/2024 23:53:44	Get Involved	https://www.mozilla.org/contribute/	Firefox (4b/vhy4g.defa)
Cached Images	0	24/11/2024 23:53:44	24/11/2024 23:53:44	About Us	https://www.mozilla.org/about/	Firefox (4b/vhy4g.defa)

We filtered to web browser Firefox to check only its results:

- **Bookmarks :** 4
- **Cached files :** 3
- **Cached web Pages and Cookies:** 5

- **Email Addresses: 2**

There wasn't much browsing to analyse correctly firefox, so let's jump directly to Microsoft edge.

2. Browsing History – Edge

First, we filter to Edge as web browser:

- Here we can see that we have 21 Bookmarks.

Browser History Examiner - Trial Mode

File Options Filter Report Tools Help

Artifact Records

Bookmarks

Date Added	Last Modified	Title	URL	Web Browser (Profile)
13/03/2023 15:16:04		Alienware	http://www.alienwarearena.com/welcome-us	Edge (Default)
13/03/2023 15:16:04		Alienware Support	http://www.dell.com/support/home	Edge (Default)
02/06/2021 23:19:29		Cambridge LMS	https://www.cambridgeilms.org/main/p/splash	Edge (Default)
23/05/2021 11:54:31		Connexion - Instagram	https://www.instagram.com/accounts/login/?next=/d	Edge (Default)
22/04/2021 23:17:07		Téléchargement Youtube Mp4 Youtube Mp4	https://youtube-mp4.download.fr/the-online-conver	Edge (Default)
01/02/2021 19:23:17		BMW Serie 3 318d pack sport 2013 diesel 302951 occ	https://www.moteur.ma/fr/voiture/achat-voiture-occ	Edge (Default)
16/01/2021 16:01:59		Front page Cambridge LMS	https://www.cambridgeilms.org/main/p/en/frontpage	Edge (Default)
29/12/2020 20:39:09		مراجعة فيلم Me Before You (2016) مترجم اجدي بست	https://roof.egybest.cyou/movie/me-before-you-2016	Edge (Default)
29/12/2020 20:36:38		مراجعة فيلم Warrior مترجم كامل اجدي بست	https://roof.egybest.cyou/season/warrior-2019-seaso	Edge (Default)
29/12/2020 20:34:42		مراجعة فيلم Virgin River (2019) مترجم كامل اجدي بست	https://roof.egybest.cyou/series/virgin-river/?ref=tv-c	Edge (Default)
29/12/2020 20:33:27		مراجعة فيلم Cobra Kai مترجم كامل اجدي بست	https://roof.egybest.cyou/episode/cobra-kai-season-	Edge (Default)
27/12/2020 17:05:47		annonces au Maroc Avito.ma	https://www.avito.ma/	Edge (Default)
18/12/2020 20:11:38		بست مشاهدة افلام ومسلسلات مترجمة مائاً بجودة عالية	https://roof.egybest.cyou/	Edge (Default)
16/12/2020 13:26:18		(S6) ROBOT : Vers la disparition du travail humain ? - 1	https://www.youtube.com/watch?v=Ss8Z2R81mo8	Edge (Default)
16/12/2020 12:28:22		Google Traduction	https://translate.google.com/?hl=auto&tl=ar&op=tra	Edge (Default)
15/12/2020 14:37:00		Courrier - Ilias BELHARDA - Outlook	https://outlook.office365.com/mail/inbox	Edge (Default)
12/12/2020 19:38:54		Google	https://www.google.fr/	Edge (Default)
24/11/2020 23:23:20		Google	https://www.google.com/	Edge (Default)
24/11/2020 23:15:30		GSMarena.com - mobile phone reviews, news, speci	https://www.gsmarena.com/	Edge (Default)
24/11/2020 23:11:46		www.wandaloo.com	https://www.wandaloo.com/	Edge (Default)
12/11/2020 11:01:53		(Microsoft Word - Correction_TD1_R351vision_Electri	https://uiabat.sharepoint.com/teams/TDGrElectricit	Edge (Default)

Viewing 21/25 records

Page size: 50

Time zone: UTC Date format: dd/mm/yyyy

We can analyse the browser settings in this artifact, we can notice that every setting is on.

Browser Settings	14	Account Name (0)		Edge (Default)
Browser Settings	14	Account Email (0)	vy...@gmail.com	Edge (Default)
Cached Files	21	Sync Apps	Yes	Edge (Default)
Cached Images	14	Sync Autofill	Yes	Edge (Default)
Cached Web Pages	18	Sync Bookmarks	Yes	Edge (Default)
Cached Web Pages	18	Sync Extensions	Yes	Edge (Default)
Cookies	0	Sync Passwords	Yes	Edge (Default)
Downloads	6	Sync Preferences	Yes	Edge (Default)
Email Addresses	22	Sync Tabs	Yes	Edge (Default)
Extensions	3	Sync Typed URLs	Yes	Edge (Default)
Favicons	1	Profile Creation Time	16/07/2024 12:29:29	Edge (Default)
		Profile Last Engagement Time	24/11/2024 23:32:17	Edge (Default)
		Default File Save Directory	C:\Users\Ilyas\Desktop	Edge (Default)
		Last File Select Directory	C:\Users\Ilyas\Desktop\certificates	Edge (Default)

			Last Fetched	Server Time	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser (Profile)
Bookmarks	21				text/javascript	https://static.licdn.com/aero-v1/sc/h/aq5hd6kqrd	3400670		Edge (Default)
Browser Settings	14				text/javascript	https://static.licdn.com/aero-v1/sc/h/f5b36kgvtyj	3394954		Edge (Default)
Cached Files	21				text/javascript	https://static.licdn.com/aero-v1/sc/h/4uy0wnmc	3369345		Edge (Default)
					text/javascript	https://static.licdn.com/aero-v1/sc/h/6detry3gio4	3369012		Edge (Default)
Cached Images	14				text/javascript	https://static.licdn.com/aero-v1/sc/h/5yq4kxempw	2449816		Edge (Default)
					text/javascript	https://static.licdn.com/aero-v1/sc/h/4f5jcwfkwglo	2445690		Edge (Default)
Cached Web Pages	18				text/javascript	https://static.licdn.com/aero-v1/sc/h/afd10xvzkoji	2439264		Edge (Default)
					application/json	https://static.xx.fbcdn.net/btmanifest/1017430416	1824311		Edge (Default)
Cookies	0				text/javascript	https://www.youtube.com/s/desktop/e38d7834/js	1564404		Edge (Default)
Downloads	6				text/javascript	https://www.youtube.com/s/desktop/c4395877/js	1559677		Edge (Default)
					text/javascript	https://www.youtube.com/s/desktop/fd504f58/jsl	1557757		Edge (Default)
Email Addresses	22				application/octet-stream	https://referrals.brave.com/latest/BraveBrowserSe	1275176		Edge (Default)
						https://prod-streaming-video-msn-com.akamaize	1048576		Edge (Default)
Extensions	3					https://prod-streaming-video-msn-com.akamaize	1048576		Edge (Default)
Favicons	1					https://prod-streaming-video-msn-com.akamaize	1048576		Edge (Default)
Form History	24					https://prod-streaming-video-msn-com.akamaize	1048576		Edge (Default)
						https://prod-streaming-video-msn-com.akamaize	1048576		Edge (Default)
Logins	25					https://prod-streaming-video-msn-com.akamaize	1048576		Edge (Default)
						https://prod-streaming-video-msn-com.akamaize	1048028		Edge (Default)
Searches	20				text/css	https://portswigger.net/content/psforms.css	1011178		Edge (Default)
Session Tabs	0				font/ttf	https://app.jointherealworld.com/assets/sequisym	961040		Edge (Default)

	Last Fetched	Server Time	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser (Profile)
Bookmarks	21						
Browser Settings	14						
Cached Files	21						
Cached Images	14						
Cached Web Pages	18						
Cookies	0						
Downloads	6						
Email Addresses	22						
Extensions	3						
Favicons	1						
Form History	24						
Logins	25						
Searches	20						
Session Tabs	0						
Site Settings	16						
Site Storage	22						
Thumbnails	4						
Website Visits	0						

Last Fetched	Server Time	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser (Profile)
		image/png	https://www.charika.ma/ressources/openx-banner/ba	2277161	Edge (Default)	
		image/gif	https://media.licdn.com/dms/image/sync/v2/D4E10A	1878722	Edge (Default)	
		image/gif	https://ci3.googleusercontent.com/meips/ADKq_Naa'	1815145	Edge (Default)	
		image/gif	https://assets.therealworld.ag/avatars/01HGK1YC8YB:	1427757	Edge (Default)	
		image/png	https://edgestatic.azureedge.net/shared/cms/lrs1c69;	1312467	Edge (Default)	
		image/jpeg	https://www.bing.com/th?id=OBTQ.BT914ED4F173BC	1207826	Edge (Default)	
		image/png	https://edgestatic.azureedge.net/shared/cms/lrs1c69;	1160264	Edge (Default)	
		image/png	https://www.charika.ma/ressources/openx-banner/ba	1130548	Edge (Default)	
		image/jpeg	https://laving.cc/b51g8k2dgdwe0000.jpg	1044290	Edge (Default)	
		image/png	https://assets.therealworld.ag/uploads/01HPYAUBFYf	801638	Edge (Default)	
		image/png	https://files.oaiusercontent.com/file-0iw1nJRFDLfuXL	698865	Edge (Default)	
		image/jpeg	https://scontent.frbz2-1.fna.fbcdn.net/v/t39.30808-6/	682093	Edge (Default)	
		image/jpeg	https://new.honadrama.xyz/wp-content/uploads/202	675977	Edge (Default)	
		image/png	https://edgestatic.azureedge.net/shared/cms/lrs1c69;	651723	Edge (Default)	

Viewing 14/25 records << < 1 of 1 pages > >> Page size 50 ▼

Bookmarks	21									
Browser Settings	14									
Cached Files	21									
Cached Images	14									
Cached Web Pages	18									
Cookies	0									
Downloads	6									

We can also retrieve the Email addresses, the last time they have been used, where(domain) and the source:

Artifact	Records	Email Addresses	Report Preview
Bookmarks	21		
Browser Settings	14		
Cached Files	21		
Cached Images	14		
Cached Web Pages	18		
Cookies	0		
Downloads	6		
Email Addresses	22		
Extensions	3		
Favicons	1		
Form History	24		
Logins	25		
Searches	20		
Session Tabs	0		

Last Used	Email Address	Domain	Source	Web Browser (Profile)
20/11/2024 20:40:13	[REDACTED]@gmail.com	auth0.openai.com	Website Visit	Edge (Default)
11/11/2024 14:24:54	[REDACTED]@gmail.com	mail.google.com	Website Visit	Edge (Default)
11/11/2024 14:21:48	[REDACTED]@gmail.com	mail.google.com	Website Visit	Edge (Default)
11/11/2024 14:21:46	[REDACTED]@gmail.com	accounts.google.com	Website Visit	Edge (Default)
11/11/2024 14:21:05	[REDACTED]@gmail.com	accounts.google.com	Website Visit	Edge (Default)
20/10/2024 13:58:05	[REDACTED]@uir.ac.ma	tryhackme.com	Form History	Edge (Default)
18/10/2024 16:12:27	[REDACTED]@uir.ac.ma	portswigger.net	Saved Login	Edge (Default)
17/10/2024 17:04:59	[REDACTED]@gmail.com		Form History	Edge (Default)
12/10/2024 15:55:51	[REDACTED]@gmail.com	linkedin.com	Form History	Edge (Default)
21/07/2024 21:47:37	[REDACTED]@gmail.com		Form History	Edge (Default)
29/04/2024 21:46:18	[REDACTED]@gmail.com		Form History	Edge (Default)
	[REDACTED]@gmail.com	gaming.inwi.ma	Saved Login	Edge (Default)
	[REDACTED]@taalim.ma	login.microsoftonline.com	Saved Login	Edge (Default)
	[REDACTED]@gmail.com	id.cisco.com	Saved Login	Edge (Default)
	[REDACTED]@gmail.com	instagram.com	Saved Login	Edge (Default)
	[REDACTED]@uir.ac.ma	login.microsoftonline.com	Saved Login	Edge (Default)
	[REDACTED]@gmail.com	accounts.google.com	Saved Login	Edge (Default)
	[REDACTED]@gmail.com		Saved Login	Edge (Default)
	[REDACTED]@gmail.com		Saved Login	Edge (Default)
	[REDACTED]@gmail.com	app.jointherealworld.com	Saved Login	Edge (Default)
	[REDACTED]@2.0.4	unpkg.com	Cache	Edge (Default)
	[REDACTED]@1.11.14	unpkg.com	Cache	Edge (Default)

Check the extensions downloaded:

Artifact	Records	Extensions	Report Preview
Bookmarks	21		
Browser Settings	14		
Cached Files	21		
Cached Images	14		
Cached Web Pages	18		
Cookies	0		
Downloads	6		
Email Addresses	22		
Extensions	3		

Name	Description	Version	App ID	Web Browser (Profile)
Adblock Plus - free ad blocker	Remove ads on YouTube and everywhere else you bro	4.9.3	gmgoamodcdjnbaoibgkjelfplakmdhh	Edge (Default)
Edge relevant text changes	Edge relevant text changes on select websites to impr	1.2.1	jmyflgipcpeafmmgdpfkogkghcpiha	Edge (Default)
Google Docs Offline	Edit, create, and view your documents, spreadsheets, a	1.83.1	ghbmnnjooekpmoecnnlinnlidloihki	Edge (Default)

Logins shows the hostname, origin Url, username, date Created, last used, if the password has been changed and how many times were used:

Bookmarks	21								
Browser Settings	14								
Cached Files	21								
Cached Images	14								
Cached Web Pages	18								
Cookies	0								
Downloads	6								
Email Addresses	22								
Extensions	3								
Favicons	1								
Form History	24								
Logins	25								
Searches	20								
Session Tabs	0								
Site Settings	16								
Site Storage	22								

Hostname	Origin URL	Submit URL	Username	Date Created	Last Used	Password Changed	Times Used	Web Browser (Profile)
https://www.faci	https://www.faci	https://www.faci	[REDACTED]	31/07/2023 14:01:32			0	Edge (Default)
https://www.e-c	https://www.e-c	https://www.e-c	[REDACTED]	13/03/2023 15:20:31			0	Edge (Default)
https://accounts	https://accounts	https://accounts	[REDACTED]	29/04/2024 21:46:40			0	Edge (Default)
android://xUJTs	android://xUJTs		[REDACTED]	13/03/2023 15:20:31			0	Edge (Default)
https://www.faci	https://www.faci		[REDACTED]	13/03/2023 15:20:31			3	Edge (Default)
android://zQxb6	android://zQxb6		[REDACTED]	13/03/2023 15:20:31			0	Edge (Default)
https://secure.ik	https://secure.ik		[REDACTED]	13/03/2023 15:20:31			0	Edge (Default)
https://id.cisco.c	https://id.cisco.c	https://id.cisco.c	[REDACTED]	06/12/2021 08:14:22			0	Edge (Default)
https://app.join	https://app.join	https://app.join	[REDACTED]	21/07/2024 21:47:38			0	Edge (Default)
android://rIT6tH	android://rIT6tH		[REDACTED]	13/03/2023 15:20:31			0	Edge (Default)
https://signup.e	https://signup.e		[REDACTED]	13/03/2023 15:20:31			0	Edge (Default)
android://79xEc	android://79xEc		[REDACTED]	13/03/2023 15:20:31			0	Edge (Default)
android://BnX9M	android://BnX9M		[REDACTED]	13/03/2023 15:20:31			0	Edge (Default)
android://19HCl	android://19HCl		[REDACTED]	13/03/2023 15:20:31			0	Edge (Default)
https://signin.ro	https://signin.ro		[REDACTED]	13/03/2023 15:20:31			0	Edge (Default)
https://accounts	https://accounts		[REDACTED]	13/03/2023 15:20:31			0	Edge (Default)
https://signup.vi	https://signup.vi		[REDACTED]	13/03/2023 15:20:31			0	Edge (Default)
android://2Q82i	android://2Q82i		[REDACTED]	13/03/2023 15:20:31			0	Edge (Default)
android://M2_Ai	android://M2_Ai		[REDACTED]	13/03/2023 15:20:31			0	Edge (Default)
android://qbMC	android://qbMC		[REDACTED]	13/03/2023 15:20:31			0	Edge (Default)
https://tryhackr	https://tryhackr	https://tryhackr	[REDACTED]	20/10/2024 13:58:09			0	Edge (Default)
android://qbMC	android://qbMC		[REDACTED]	13/03/2023 15:20:31			0	Edge (Default)
android://qbMC	android://qbMC		[REDACTED]	13/03/2023 15:20:31			0	Edge (Default)
https://tryhackr	https://tryhackr		[REDACTED]	20/10/2024 13:57:19			0	Edge (Default)
https://accounts	https://accounts	https://accounts	[REDACTED]	17/03/2023 12:38:06			0	Edge (Default)

The history of searches:

Artifact	Records	Searches	Report Preview
Bookmarks	21		
Browser Settings	14		
Cached Files	21		
Cached Images	14		
Cached Web Pages	18		
Cookies	0		
Downloads	6		
Email Addresses	22		
Extensions	3		
Favicons	1		
Form History	24		
Logins	25		
Searches	20		

Date Searched	Search Terms	Search Engine	URL	Source	Web Browser (Profile)
24/11/2024 23:32:19	epic games	Bing	https://www.bing.com/search?q=epic+game	Edge History	Edge (Default)
24/11/2024 23:32:19	epic games	Bing	https://www.bing.com/search?q=epic+game	Website Visit	Edge (Default)
24/11/2024 23:32:18	epic games	Bing	https://www.bing.com/search?q=epic+game	Website Visit	Edge (Default)
24/11/2024 23:32:17	epic games	Bing	https://www.bing.com/search?q=epic+game	Edge History	Edge (Default)
24/11/2024 23:32:17	epic games	Bing	https://www.bing.com/search?q=epic+game	Website Visit	Edge (Default)
11/11/2024 22:09:08	gmail	Bing	https://www.bing.com/search?pglt=297&q=	Edge History	Edge (Default)
11/11/2024 15:14:56	vmworld	Bing	https://www.bing.com/search?q=vmworld&f	Website Visit	Edge (Default)
11/11/2024 15:14:56	vmworld	Bing	https://www.bing.com/search?q=vmworld&f	Edge History	Edge (Default)
11/11/2024 15:14:55	vmworld	Bing	https://www.bing.com/search?q=vmworld&f	Website Visit	Edge (Default)
11/11/2024 14:21:45	gmail	Bing	https://www.bing.com/search?q=vmworld&f	Edge History	Edge (Default)
11/11/2024 14:21:45	gmail	Bing	https://www.bing.com/search?q=vmworld&f	Website Visit	Edge (Default)
11/11/2024 14:21:44	gmail	Bing	https://www.bing.com/search?q=vmworld&f	Edge History	Edge (Default)
11/11/2024 14:21:44	gmail	Bing	https://www.bing.com/search?q=vmworld&f	Website Visit	Edge (Default)
11/11/2024 14:16:27	gmail	Bing	https://www.bing.com/search?pglt=297&q=	Edge History	Edge (Default)

Viewing 20/25 records

Page size: 50

Firefox vs Edge Comparison

- **Data Volume:** Edge contained more entries, likely due to more frequent use.
- **Types of Visited Sites:**
 - Edge showed more usage focused on leisure and personal research.
 - Firefox was more likely forgotten.

Let's now try and configure pdf and html reports:

Pdf:

First thing to do is to mark, if we think it's some important content, like this:

★	★			applicati
★	★			text/java
★	★	★	Add to report	text/java
★	★	★	Remove from report	text/java

To save as pdf, we go to file, click on reports and select "save as PDF":

File	Options	Filter	Report	Tools	Help
Capture History			Logins	Report Preview	
Load History			Hostname		
Report			Save as PDF		
Export			Save as HTML		
Exit					

Here we go, we got our Web browser history Report:

The screenshot displays a 'Web Browser History Report' with two main sections: 'Cached Images' and 'Cached Web Pages'.

Cached Images:

- URL:** https://www.infofrance.be/fr/observatoire-des-delais-de-paiement
- Content Type:** image/png
- Content Size:** 1000000
- Access Date:** 2017-01-10
- Access Time:** 10:00:00
- Access User:** infofrance

Cached Web Pages:

- URL:** https://www.infofrance.be/fr/observatoire-des-delais-de-paiement
- Content Type:** text/html
- Content Size:** 1000000
- Access Date:** 2017-01-10
- Access Time:** 10:00:00
- Access User:** infofrance

The report also includes a 'Downloads' section with a table of downloaded files and an 'Attachments' section with a table of attached files.

Html:

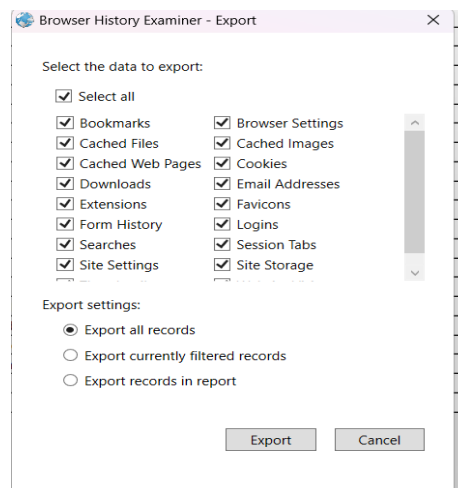
To all export all records as html, here's the method

The screenshot shows the 'File' menu of a web browser history tool. The 'Export' option is selected, and a submenu is displayed with the following options:

- Export to HTML (for printing)
- Export to HTML (for viewing)
- Export to Excel
- Export to CSV

The 'Export to HTML (for viewing)' option is highlighted.

We can select and choose the data to select, we just checked everything for a detailed report:



And here we go, we got a detailed browser history :

Last Fetched	Server Time	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser (Profile)
		text/javascript	https://www.youtube.com/desktop/8b0677e9/jsbin/desktop_polymer.vfiset/desktop_polymer	5	18751357	Firefox (48vyhy4g.default-release)
		application/octet-stream	https://edgedl.me.gvt1.com/edgedl/release2/chrome_component/acccb66wswpxzpbob4hojndwkqt_4.10.2830.0/oimompeagnajdejgnnjjobebaeigek_4.10.2830.0_win64_dldxogwi36sxwpr57ta4lg57z4.cnx3	1	14507539	Firefox (48vyhy4g.default-release)
		text/javascript	https://static.lidn.com/aero-v1/sc/h/5q5hd6kqdsbj86fe5mfvtu0		3400670	Edge (Default)
		text/javascript	https://static.lidn.com/aero-v1/sc/h/5b36kgvtvjzh0oqq4e2w7b3		3394954	Edge (Default)
		text/javascript	https://static.lidn.com/aero-v1/sc/h/4uyr0wnncwzgzaspwawe1438		3369345	Edge (Default)
		text/javascript	https://static.lidn.com/aero-v1/sc/h/6detpy3gio42zzuzhps4weuya		3369012	Edge (Default)
		text/javascript	https://static.lidn.com/aero-v1/sc/h/5yq4xempw18gq7e53029btyfm		2449816	Edge (Default)
		text/javascript	https://static.lidn.com/aero-v1/sc/h/4fjcwfkvgkx6bk0k3en4enim		2445690	Edge (Default)

Limitations and Precautions

Browser forensic analysis, while useful, has several limitations and requires careful interpretation. Below are the main challenges and considerations:

Data Context

- **Shared Devices:** If the browser is used by multiple people, the history represents mixed behaviors, making it hard to link actions to one user.
- **Account Sharing:** Shared browser accounts across devices can create overlapping or unrelated data.
- **User Intent:** It's impossible to determine the exact reason for visiting a site based on history alone.

Timestamp Accuracy

- **System Time Changes:** Incorrect system clocks or manual adjustments can affect the timestamps.
- **Time Zone Issues:** Timestamps depend on the local system time and may not reflect the user's actual location or time zone.
- **Incomplete Logs:** Some activities may not record timestamps accurately in the browser history.

Missing Data

- **Private Browsing:** Activities in incognito or private mode are not saved in the history.
- **Deleted History:** Users can manually erase browsing history, leading to missing data.
- **Third-Party Tools:** Some tools or extensions may clear or alter the history automatically.

Browser-Specific Limitations

- **Encrypted Databases:** Some browsers protect their data with encryption, requiring additional tools to decrypt it.
- **Multiple Browsers:** Users may switch between browsers, leaving only partial data in each.

Potential for Misinterpretation

- **Background Processes:** Some entries, like pop-ups or auto-refreshing pages, may not result from deliberate user actions.
- **Search Terms:** Queries may not always reflect meaningful intent and could be exploratory.

Ethical and Legal Concerns

- **User Privacy:** Analyzing browsing history without consent can violate privacy laws.
- **Data Sensitivity:** Browsing history often contains personal information, requiring secure handling to prevent misuse.
- **Legal Validity:** For use in legal cases, data must be collected and handled according to strict forensic procedures.

These limitations highlight the need for cautious interpretation and, where possible, the inclusion of complementary data sources for a complete analysis.

Conclusion and Recommendations

The use of *Browser History Examiner* enabled a detailed extraction and analysis of the browsing histories of Firefox and Chrome. These results provide a clear view of online behavior and could be used in various contexts, such as judicial investigations, security audits, or user behavior studies.

Recommendations:

- Raise awareness among users about the impact of their online activities, particularly regarding privacy.
- Use complementary solutions to retrieve data from private browsing or other browsers.
- Combine this analysis with other data sources (cookies, network logs) for a more comprehensive view.

Références

[Browser Forensics: IE 11 | Infosec](#)

[Forensic : focus sur l'analyse suite à une attaque informatique](#)