



Browser Forensic Report

Made by : Ilias Belharda

Chihab Alaoui

Mohammed Amine Stour

Supervised by: Mr Khalid Chougdali

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:
 - o Dates and times of access.
 - o Searches performed.
 - o Bookmarks or marked important items.
4. Compare the retrieved data between Firefox and Edge.



Methodology

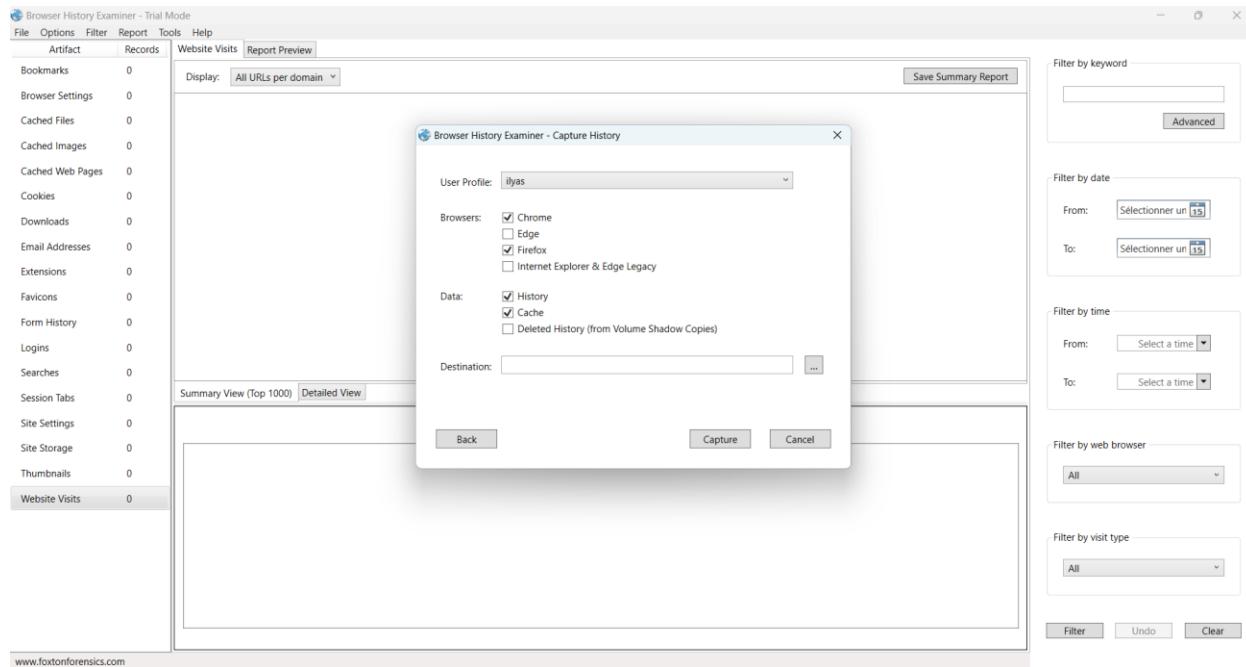
1. Tools Used

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:**

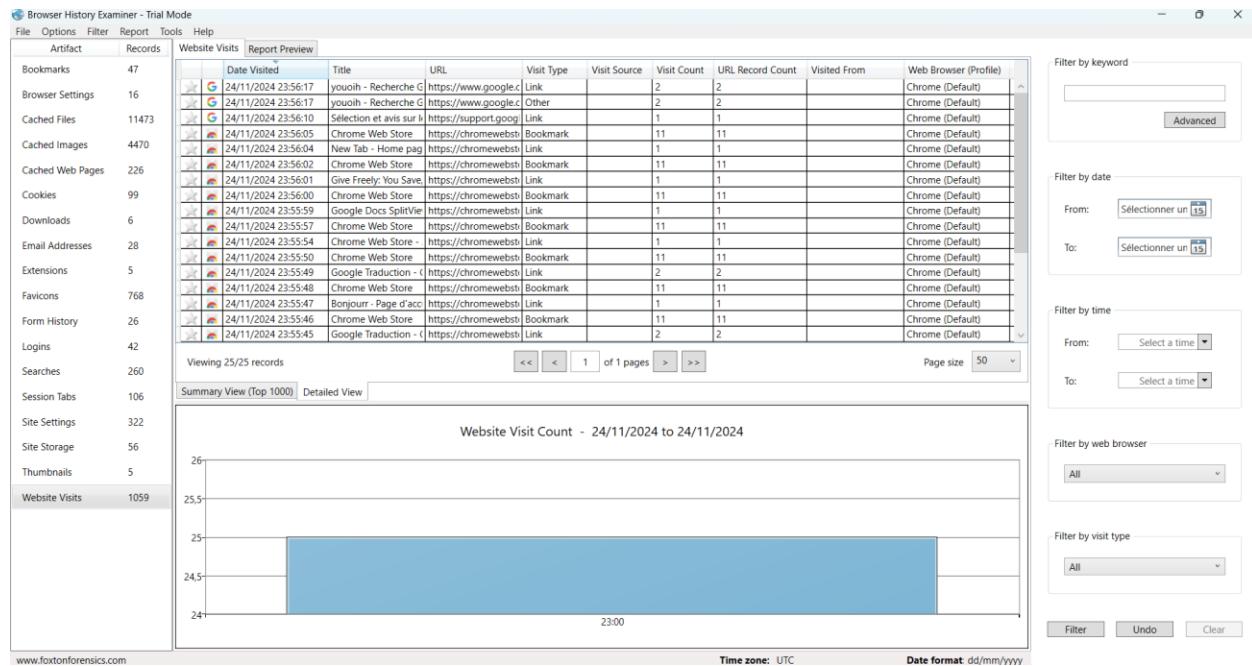
Browser history files located on the operating system were copied into a secure environment for analysis.



- **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
Bookmarks	4
Browser Settings	0
Cached Files	3
Cached Images	0
Cached Web Pages	5
Cookies	5
Downloads	0
Email Addresses	2
Extensions	0
Favicons	0
Form History	1
Logins	0
Searches	2
Session Tabs	0
Site Settings	0
Site Storage	0
Thumbnails	0
Website Visits	1

Viewing 4/25 records

Page size: 50

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

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.

Artifact	Records	Bookmarks	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		
Site Settings	16		
Site Storage	22		
Thumbnails	4		
Website Visits	0		

The screenshot shows the 'Report Preview' tab of the Browser History Examiner tool. It displays a list of 21 bookmarks. The columns include Date Added, Last Modified, Title, URL, and Web Browser (Profile). A sidebar on the right contains three filter panels: 'Filter by keyword', 'Filter by date', and 'Filter by time'. The 'Filter by keyword' panel has an empty search field and an 'Advanced' button. The 'Filter by date' panel has 'From' and 'To' fields set to 'Selectionner un'. The 'Filter by time' panel has 'From' and 'To' fields set to 'Select a time'. Below the main table, there are buttons for 'Filter', 'Undo', and 'Clear'.

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

Browser Settings	14	Account Name (0) Account Email (0)	[REDACTED]@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)
Cookies	0	Sync Extensions	Yes	Edge (Default)
Downloads	6	Sync Passwords	Yes	Edge (Default)
Email Addresses	22	Sync Preferences	Yes	Edge (Default)
Extensions	3	Sync Tabs	Yes	Edge (Default)
Favicons	1	Sync Typed URLs	Yes	Edge (Default)
		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\lyas\Desktop	Edge (Default)
		Last File Select Directory	C:\Users\lyas\Desktop\certificates	Edge (Default)

The Cached Files shows us the content type (javascript, text, css ..), the url and the File size in Bytes.

Bookmarks	21	Last Fetched	Server Time	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser (Profile)
Browser Settings	14	star	in		text/javascript	https://static.lcicdn.com/aero-v1/sc/h/aq5hd6kqrjd	3400670	Edge (Default)
Cached Files	21	star	in		text/javascript	https://static.lcicdn.com/aero-v1/sc/h/f5b36kgvtvbj	3394954	Edge (Default)
Cached Images	14	star	in		text/javascript	https://static.lcicdn.com/aero-v1/sc/h/4uy0rmcmx	3369345	Edge (Default)
Cached Web Pages	18	star	in		text/javascript	https://static.lcicdn.com/aero-v1/sc/h/6d6tpy3gjo4	3369012	Edge (Default)
Cookies	0	star	fb		text/javascript	https://static.lcicdn.com/aero-v1/sc/h/5y94xempw	2449816	Edge (Default)
Downloads	6	star	yt		text/javascript	https://static.lcicdn.com/aero-v1/sc/h/4fjswfkvgkb	2445690	Edge (Default)
Email Addresses	22	star	yt		application/json	https://static.xx.fbcdn.net/btmanifest/10174430416	2439264	Edge (Default)
Extensions	3	star			text/javascript	https://www.youtube.com/s/desktop/e38d7834/jst	1824311	Edge (Default)
Favicons	1	star			text/javascript	https://www.youtube.com/s/desktop/4395877/jst	1564404	Edge (Default)
Form History	24	star			text/javascript	https://www.youtube.com/s/desktop/fd504f58/jst	1559775	Edge (Default)
Logins	25	star			application/octet-stream	https://referrals.brave.com/latest/BraveBrowserSe	1275176	Edge (Default)
Searches	20	star	fb			https://prod-streaming-video-msn-com.akamaize	1048576	Edge (Default)
Session Tabs	0	star	fb		text/css	https://prod-streaming-video-msn-com.akamaize	1048576	Edge (Default)
						https://prod-streaming-video-msn-com.akamaize	1048576	Edge (Default)
						https://prod-streaming-video-msn-com.akamaize	1048576	Edge (Default)
						https://prod-streaming-video-msn-com.akamaize	1048576	Edge (Default)
						https://prod-streaming-video-msn-com.akamaize	1048576	Edge (Default)
						https://prod-streaming-video-msn-com.akamaize	1048576	Edge (Default)
						https://prod-streaming-video-msn-com.akamaize	1048028	Edge (Default)
						https://portswigger.net/content/pfsorms.css	1011178	Edge (Default)
						https://app.jointhereworld.com/assets/seguisym	961040	Edge (Default)

Same for Cached Images and Cached Web Pages :

Downloads shows the local paths of every download, the state if it's completed or not, the start and end time and the how much storage it took the download.

Bookmarks	21		URL	Local Path	State	Start Time	End Time	Bytes Downloaded	Total Bytes	Web Browser (Profile)
Browser Settings	14	★	blob:https://chatgpt	C:\Users\ilyas\Down	Complete	22/11/2024 15:46:19	22/11/2024 15:46:19	462316	462316	Edge (Default)
Cached Files	21	🔗	https://dl.dell.com/u	C:\Users\ilyas\Down	Complete	22/10/2024 10:39:47	22/10/2024 10:41:36	51997192	51997192	Edge (Default)
Cached Images	14	🔗	https://api30.ilovery	C:\Users\ilyas\Down	Complete	11/10/2024 12:06:31	11/10/2024 12:06:32	19203	19203	Edge (Default)
Cached Web Pages	18	🔗	https://api86.ilovery	C:\Users\ilyas\Down	Complete	04/10/2024 15:31:54	04/10/2024 15:31:55	18082	18082	Edge (Default)
Cookies	0	🔗	https://laptop-upda	C:\Users\ilyas\Down	Complete	16/07/2024 12:38:32	16/07/2024 12:38:32	1275176	1275176	Edge (Default)
Downloads	6	🔗	https://laptop-upda	C:\Users\ilyas\Down	Complete	16/07/2024 12:38:08	16/07/2024 12:38:10	1275176	1275176	Edge (Default)

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	Last Used	Email Address Domain Source Web Browser (Profile)
Browser Settings	14	20/11/2024 20:40:13	@gmail.com auth0.openai.com Website Visit Edge (Default)
Cached Files	21	11/11/2024 14:24:54	@gmail.com mail.google.com Website Visit Edge (Default)
Cached Images	14	11/11/2024 14:21:48	@gmail.com mail.google.com Website Visit Edge (Default)
Cached Web Pages	18	11/11/2024 14:21:46	@gmail.com accounts.google.com Website Visit Edge (Default)
Cookies	0	11/11/2024 14:21:05	@gmail.com accounts.google.com Website Visit Edge (Default)
Downloads	6	20/10/2024 13:58:05	@ur.ac.ma tryhackme.com Form History Edge (Default)
Email Addresses	22	18/10/2024 16:12:27	@ur.ac.ma portswigger.net Saved Login Edge (Default)
Extensions	3	17/10/2024 17:04:59	@gmail.com Form History Edge (Default)
Favicons	1	12/10/2024 15:55:51	@gmail.com Form History Edge (Default)
Form History	24	21/07/2024 21:47:37	@gmail.com Form History Edge (Default)
Logins	25	29/04/2024 21:46:18	@gmail.com Form History Edge (Default)
Searches	20		@gmail.com Saved Login Edge (Default)
Session Tabs	0		@taalim.ma login.microsoftonline.com Saved Login Edge (Default)
			@gmail.com id.cisco.com Saved Login Edge (Default)
			@gmail.com instagram.com Saved Login Edge (Default)
			@ur.ac.ma login.microsoftonline.com Saved Login Edge (Default)
			@gmail.com accounts.google.com Saved Login Edge (Default)
			@gmail.com gaming.invi.ma Saved Login Edge (Default)
			@2.0.4 unpkg.com Saved Login Edge (Default)
			1.11.14 unpkg.com Cache Edge (Default)
			1.11.14 unpkg.com Cache Edge (Default)

Check the extensions downloaded:

Artifact	Records	Extensions	Report Preview
Bookmarks	21	Name Description Version App ID Web Browser (Profile)	
Browser Settings	14	Adblock Plus - free ad blocker Remove ads on YouTube and everywhere else you bro 4.9.3 gmgoamodcdcjnbaoibgkjelfplakmdhh Edge (Default)	
Cached Files	21	Edge relevant text changes Edge relevant text changes on select websites to impr 1.2.1 jmjfgjpcpepeafmmgdpfkqkghcpjh Edge (Default)	
Cached Images	14	Google Docs Offline Edit, create, and view your documents, spreadsheets, a 1.83.1 ghmnnjoekpmoeecnlnilnnbdolhkhi Edge (Default)	
Cached Web Pages	18		
Cookies	0		
Downloads	6		
Email Addresses	22		
Extensions	3		

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

Artifact	Records	Hostname	Origin URL	Submit URL	Username	Date Created	Last Used	Password Changed	Times Used	Web Browser (Profile)
Bookmarks	21	https://www.facebook.com	https://www.facebook.com	https://www.facebook.com		31/07/2023 14:01:32			0	Edge (Default)
Browser Settings	14	https://www.e-cisco.com	https://www.e-cisco.com	https://www.e-cisco.com		13/03/2023 15:20:31			0	Edge (Default)
Cached Files	21	https://accounts.google.com	https://accounts.google.com	https://accounts.google.com		29/04/2024 21:46:40			0	Edge (Default)
Cached Images	14	android://xUJTz; android://xUJTz;	android://xUJTz; android://xUJTz;	android://xUJTz; android://xUJTz;		13/03/2023 15:20:31			0	Edge (Default)
Cached Web Pages	18	https://www.facebook.com	https://www.facebook.com	https://www.facebook.com		13/03/2023 15:20:31			3	Edge (Default)
Cookies	0	android://zQxbE; android://zQxbE;	android://zQxbE; android://zQxbE;	android://zQxbE; android://zQxbE;		13/03/2023 15:20:31			0	Edge (Default)
Downloads	6	https://secure.iknowit.com	https://secure.iknowit.com	https://secure.iknowit.com		13/03/2023 15:20:31			0	Edge (Default)
Email Addresses	22	https://id.cisco.com	https://id.cisco.com	https://id.cisco.com		06/12/2021 08:14:22			0	Edge (Default)
Extensions	3	https://app.jointheREALworld.com	https://app.jointheREALworld.com	https://app.jointheREALworld.com		21/07/2024 21:47:38			0	Edge (Default)
Favicons	1	android://iT6tH; android://iT6tH;	android://iT6tH; android://iT6tH;	android://iT6tH; android://iT6tH;		13/03/2023 15:20:31			0	Edge (Default)
Form History	24	https://signup.e-cisco.com	https://signup.e-cisco.com	https://signup.e-cisco.com		13/03/2023 15:20:31			0	Edge (Default)
Logins	25	android://79xEc; android://79xEc;	android://79xEc; android://79xEc;	android://79xEc; android://79xEc;		13/03/2023 15:20:31			0	Edge (Default)
Searches	20	android://BnX9M; android://BnX9M;	android://BnX9M; android://BnX9M;	android://BnX9M; android://BnX9M;		13/03/2023 15:20:31			0	Edge (Default)
Session Tabs	0	android://19HC1; android://19HC1;	android://19HC1; android://19HC1;	android://19HC1; android://19HC1;		13/03/2023 15:20:31			0	Edge (Default)
Site Settings	16	https://signin.rocks	https://signin.rocks	https://signin.rocks		13/03/2023 15:20:31			0	Edge (Default)
Site Storage	22	https://accounts.google.com	https://accounts.google.com	https://accounts.google.com		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		

Viewing 20/25 records

Page size 50

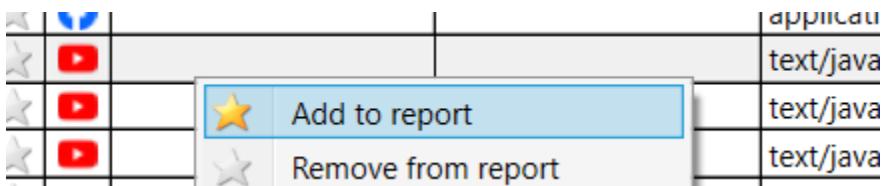
Firefox vs Edge Comparison

- 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.

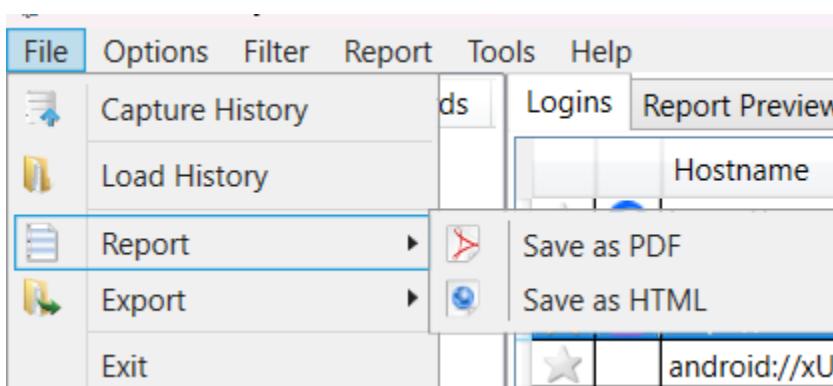
Let's now try and configure pdf and html reports:

Pdf:

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



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

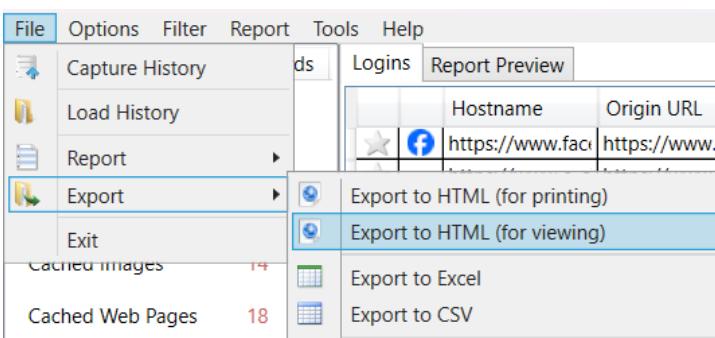


Here we go, we got our Web browser history Report:

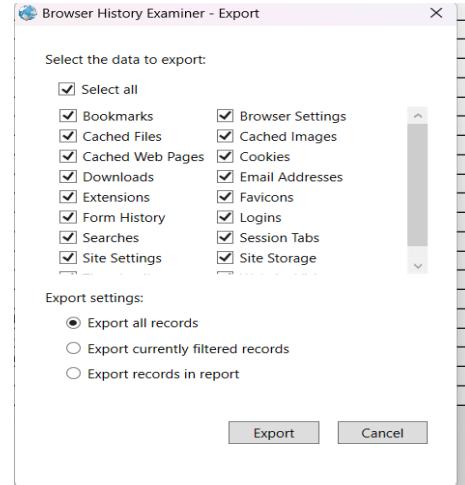
The screenshot displays a web browser window with several panels open, illustrating a history report. The top-left panel shows a 'Web Browser History Report' with details like 'Creation date: 2023-09-12' and 'Server: https://www.infoblox.com'. Below it is a 'Cached Images' panel showing a thumbnail of a webpage titled 'INFORIS PARTENAIRE DE L'OBSERVATOIRE DES DÉLAIS DE PAIEMENT'. The bottom-left panel shows a 'Downloads' section with a single entry for a file named 'infoblox_observatoire_des_delaix_de_paiement_v1.0.1.zip'. To the right of these are two smaller panels: one showing a 'Cached Web Pages' thumbnail and another showing a dark interface.

Html:

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



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 :

Browser History Examiner - Export Viewer							Time zone: UTC
Cached Files							
Show 50 entries <input style="width: 100px;" type="text" value="Search:"/>							
Last Fetched	Server Time	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser (Profile)	
		text/javascript	https://www.youtube.com/s/desktop/7b6077e9jsbin/desktop_polymer.vflset/desktop_polymer.js	5	18751357	Firefox (48hy4g.default-release)	
		text/javascript	r.js				
		application/xoctet-stream	https://edgedl.me.gvt1.com/edgedl/release2/chrome_component/accobt6wwsvpxzpb4hojn/dwkqq.4.10.2830.0/oimompccagnajdegrnijjobabeigek.4.10.2830.0_win64_dldxogwi36swpr.57ta4lg57z4.crx3	1	14507539	Firefox (48hy4g.default-release)	
		text/javascript	https://static.liecdn.com/aero-v1/sc/h/aqShd6kqrdsbj8fe5mfvu0		3400670	Edge (Default)	
		text/javascript	ipt				
		text/javascript	https://static.liecdn.com/aero-v1/sc/h/f5b36kgvtyjyzh9oqq4e2w7b3		3394954	Edge (Default)	
		text/javascript	ipt				
		text/javascript	https://static.liecdn.com/aero-v1/sc/h/4uyr0wnncwzgzasptwaxe1438		3369345	Edge (Default)	
		text/javascript	ipt				
		text/javascript	https://static.liecdn.com/aero-v1/sc/h/6detpy3gio42zzuzhps4weuya		3369012	Edge (Default)	
		text/javascript	ipt				
		text/javascript	https://static.liecdn.com/aero-v1/sc/h/5yq4xempw18gq7e53029blyfm		2449816	Edge (Default)	
		text/javascript	ipt				
		text/javascript	https://static.liecdn.com/aero-v1/sc/h/4fscjwfkvglx6bk0k3en4enim		2445690	Edge (Default)	
		text/javascript	ipt				

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](#)