



**National University of Computer and Emerging Sciences
Islamabad Campus**

CY2002

Digital Forensics

Semester Project

Browser Artifacts Forensics Tool for
Privacy-Focused Browsers

Submitted by:

Javeriah Faheem, Sabreena Azhar

Abubakar Sharif, Umar Zeb

Roll number: 22i-7421, 22i-1751, 22i-1575, 22i-1700

Date: 17-11-2024

Table of Contents

Project Title.....	2
Browser Artifacts Forensics Tool for Privacy-Focused Browsers	2
1. Introduction.....	2
Overview	2
Usage Scenario.....	2
2. Requirements:	2
System Requirements	2
Software Requirements	2
3. Installation and Scenario Setup	3
Step-by-Step Instructions.....	3
4. Features.....	3
5. Workflow.....	5
.....	12
6. FAQs.....	12
7. Conclusion	13
8. References.....	14

Project Title:

Browser Artifacts Forensics Tool for Privacy-Focused Browsers

1. Introduction:

Overview

The tool is command-line and a python script which is a comprehensive browser data extractor, capable of retrieving various types of information such as saved passwords, bookmarks, browsing history, accessed URLs, cache data, downloads, extensions, and installation dates from Chromium-based (like Brave) and non-Chromium-based (like Firefox and LibreWolf) browsers. It explores the registry entry and pre-fetch files for installation dates and other functionalities.

Usage Scenario

This tool can be used by Digital Forensics investigator to investigate the privacy focused browsers installed on a suspect's computer/laptop and to monitor their activities on such browsers, extract important passwords, check browsing and download histories and check cache in detail to view any suspicious activity done by the suspect. The tool offers the hex view of all the important databases and files like cache, browsing history and downloads history extra so the investigator can also view the files in hex format to study their bytes and to see if there are any corrupted files. This tool should not be used for personal purposes as it goes against the rules and regulations of someone's privacy.

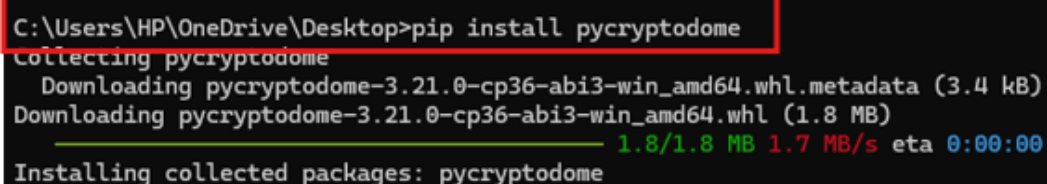
2. Requirements:

System Requirements

There are no as such system requirements to run this script, it can work on any system with basic RAM and storage available but it's only for windows and administrator privileges while running the script are recommended for full functionality (e.g., accessing protected files).

Software Requirements:

- Python 3.x installed. It can be installed from the following link: <https://www.python.org/downloads/>. After installing it make sure to run the command "python" on command prompt to check its installation. Some important python libraries that are pre-requisite to run this script and are not built-in are:
Crypto: "pip install pycryptodome"



```
C:\Users\HP\OneDrive\Desktop>pip install pycryptodome
Collecting pycryptodome
  Downloading pycryptodome-3.21.0-cp36-abi3-win_amd64.whl.metadata (3.4 kB)
  Downloading pycryptodome-3.21.0-cp36-abi3-win_amd64.whl (1.8 MB)
    ----- 1.8/1.8 MB 1.7 MB/s eta 0:00:00
Installing collected packages: pycryptodome
```

(Highlighted part is the command used to install it on your system)

Pywin32: “pip install pywin32”

```
C:\Users\HP\OneDrive\Desktop>pip install pywin32
Collecting pywin32
  Downloading pywin32-308-cp313-cp313-win_amd64.whl.metadata (8.3 kB)
  Downloading pywin32-308-cp313-cp313-win_amd64.whl (6.5 MB)
    ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 6.5/6.5 MB 1.2 MB/s eta 0:00:00
Installing collected packages: pywin32
Successfully installed pywin32-308
```

It's recommended to install the latest versions of these libraries so if there's an 'update to latest version' option then proceed with it.

Built-in libraries included:

CDLL, Structure, c_int, c_uint, c_void_p, c_char_p, c_ubyte, cast, byref, string_at, sys, os, winreg, glob, base64, time, getopt, getpass, json, base64, sqlite3, shutil, datetime.

3. Installation and Scenario Setup:

Step-by-Step Instructions:

1. Download or clone the script to a folder on your computer.
2. Download the required browsers (Brave, Firefox and LibreWolf) from app store/google. (Or the browsers must be installed already on the suspect's computer if an investigation is being carried out for privacy focused browsers).
3. Fill some artifacts/credentials like dummy passwords and browsing histories/downloads on the downloaded browsers for the scenario.
4. Recheck the required Python libraries are installed.
5. Close the Brave browser to avoid file locks.
6. Navigate to the script directory in the terminal (under administrative rights)
7. Run the script with “python script.py” command.

note: No paths need to be changed inside the script since all the paths are given dynamically for chromium-based browser and for non-chromium based the paths are always same if the installation is done without any changings to the path.

4. Features:

Each feature of the script should have its section with an explanation and examples of usage.

Hex Viewer:

- Describe how users can view the binary data of files in hex format.
- Example use: Analyzing files like bookmarks, cache, or manifest files for deeper insights.

Decryption Key Retrieval:

- Explain how the script retrieves and decrypts AES encryption keys from Local State file using win32crypt.

Password Decryption:

- How the script decrypts saved passwords using the encryption key and Brave's Login Data database.

Bookmarks:

- Describe how the script parses and displays bookmarks, allowing optional hex viewing of the raw bookmarks file.

Browsing History:

- Explain how the script retrieves URLs, titles, and timestamps from the History database.
- Highlight the timestamp conversion process for better readability.

Cache Files:

- Mention that the script lists all cache files and allows users to view any file in hex format.

Downloads:

- Detail how the script retrieves information about downloaded files, including file paths, sizes, and timestamps.

Extensions:

- Explain how the script scans for installed extensions, retrieves details from manifest.json, and optionally allows hex viewing of the manifest.

Installation Date Retrieval:

- Describe how the script queries the Windows Registry to find the installation date of Brave Browser.

Profile Detection:

- Mention the script's ability to detect and list available profiles in Brave's user data directory.

5. Workflow:

Pre-requisite: if this tool is not being used in a professional environment or on suspect's device where the browsers might already have a lot of artifacts, make sure to feed in some artifacts to the downloaded browsers to get the desired results.

- Run the script:

```
C:\Users\HP\OneDrive\Desktop\df_project>python script.py
=====
Welcome to Browser Data Extractor!
=====

Choose browser type:
1. Chromium-based browsers (e.g., Brave)
2. Non-Chromium-based browsers (e.g., Firefox, LibreWolf)

Enter your choice (1 or 2):
```

- Choose the browser that you're trying to fetch the artifacts for (choosing Brave):

```
C:\Users\HP\OneDrive\Desktop\df_project>python script.py
=====
Welcome to Browser Data Extractor!
=====

Choose browser type:
1. Chromium-based browsers (e.g., Brave)
2. Non-Chromium-based browsers (e.g., Firefox, LibreWolf)

Enter your choice (1 or 2): 1
👾 Brave Artifact Manager 👾

=====

Available profiles for Brave:
1. Default

Select the profile number to extract data from: 1

✓Selected profile: Default
```

- Now different prompts will show up asking if the user wants to view the features(history, cache, password files etc in hex or not), choose them according to what you wish to view according to your investigation and the program will flow like following:

Hex view of password file (512 bytes):

[illegible]

note: number of hex bytes to be viewed can be changed in the script 'hex_viewer' function, we've initially set them to 512 bytes

decrypted passwords obtained:

```

🔑 Decryption key obtained successfully.

🔑 Saved Passwords:

```

Origin URL	Username	Password
https://youtube.com/	umar	1234
https://twitter.com/	sabreena	Gj04938
https://instagram.com/	jaaveriaa.fm	multiple8374
https://facebook.com/	abubakkar	duo8394

Bookmarks obtained:

```

📌 Bookmarks:
1. googleclassroom (url): https://classroom.google.com/
2. Surah Ad-Duha (24 Times) | By Ridjaal Ahmed | قُرْآنُكَرِيمٌ | Arabic And English Translation -
No bookmarks found.

```

Hex view of bookmarks file (512 bytes):

```

C:\Brave Bookmarks File Found!
Would you like to view the bookmarks file in hex? (y/n): y

Hex View of C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Bookmarks:
-----
7B 0D 0A 20 20 20 22 63 68 65 63 6B 73 75 6D 22 {.. "checksum"
3A 20 22 36 62 32 61 66 36 62 64 33 36 65 64 62 : "6b2af6bd36edb
35 64 35 36 32 61 67 31 61 61 32 31 35 37 65 37 5d569a71aa2157e7
39 39 64 22 2C 0D 0A 20 20 22 72 6F 6F 74 73 99d",.. "roots
22 3A 20 7B 0D 0A 20 20 20 20 20 22 62 6F 6F ": {.. "boo
6B 6D 61 72 6B 5F 62 61 72 22 3A 20 7B 0D 0A 20 kmark_bar": {..
20 20 20 20 20 20 22 63 68 69 6C 64 72 65 "childre
6E 22 3A 20 5B 20 20 5D 2C 0D 0A 20 20 20 20 20 n": [ ],...
20 20 20 20 22 64 61 74 65 5F 61 64 64 65 64 22 "date_added"
3A 20 22 31 33 37 36 31 37 35 36 37 33 35 30 : "1337617567350
35 39 38 36 22 2C 0D 0A 20 20 20 20 20 20 20 20 5986",...
20 22 64 61 74 65 5F 6C 61 73 74 5F 75 73 65 64 "date_last_used
22 3A 20 22 30 22 2C 0D 0A 20 20 20 20 20 20 20 "": "0",...
20 20 22 64 61 74 65 5F 6D 6F 64 69 66 69 65 64 "date_modified
22 3A 20 22 30 22 2C 0D 0A 20 20 20 20 20 20 20 "": "0",...
20 20 22 67 75 69 64 22 3A 20 22 30 62 63 35 64 "guid": "0bc5d
31 33 66 2D 32 63 62 61 2D 35 64 37 34 2D 39 35 13f-2cba-5d74-95
31 66 2D 33 66 32 33 33 66 65 36 63 39 30 38 22 1f-3f233fe6c908"
2C 0D 0A 20 20 20 20 20 20 20 20 22 69 64 22 ,.. "id"
3A 20 22 31 22 2C 0D 0A 20 20 20 20 20 20 20 20 : "1",...
20 22 6E 61 6D 65 22 3A 20 22 42 6F 6F 6B 6D 61 "name": "Bookma
72 6B 73 20 62 61 72 22 2C 0D 0A 20 20 20 20 20 rks_bar",..
20 20 20 20 22 74 79 70 65 22 3A 20 22 66 6F 6C "type": "fol
64 65 72 22 0D 0A 20 20 20 20 20 20 20 20 7D 2C 0D 0A der".. },...
20 20 20 20 20 20 22 6F 74 68 65 72 22 3A 20 7B "other": {
0D 0A 20 20 20 20 20 20 20 20 22 63 68 69 6C .. "chil
64 72 65 6E 22 3A 20 5B 20 7B 0D 0A 20 20 20 20 dren": [ {..
20 20 20 20 20 20 20 20 22 64 61 74 65 5F 61 64 "date_ad
64 65 64 22 3A 20 22 31 33 33 37 36 31 37 36 30 ded": "133761760
37 32 37 39 33 32 37 31 22 2C 0D 0A 20 20 20 20 72793271",...
20 20 20 20 20 20 20 20 22 64 61 74 65 5F 6C 61 "date_la
73 74 5F 75 73 65 64 22 3A 20 22 30 22 2C 0D 0A st used": "0",...

```

Hex view of browsing history database (512 bytes):

[illegible]

Browsing history obtained:

URL	Title	Last Visit Time
https://www.google.com/search?q=googleclassroom&oq=googlec	googleclassroom - Google Sea	2024-11-15 20:24:16
https://sites.google.com/view/classroom-workspace/	Google Classroom	2024-11-15 20:24:21
https://sites.google.com/view/classroom-workspace/login	Google Classroom - Login	2024-11-15 20:24:25
https://classroom.google.com/u/0/	Classroom Management Tools &	2024-11-15 20:24:37
https://accounts.google.com/ServiceLogin?service=classroom	Classroom Management Tools &	2024-11-15 20:24:37
https://edu.google.com/intl/en-US/workspace-for-education/	Classroom Management Tools &	2024-11-16 16:33:37
https://accounts.google.com/ServiceLogin?continue=https%3A	Sign in - Google Accounts	2024-11-15 20:27:12
https://accounts.google.com/InteractiveLogin?continue=http	Sign in - Google Accounts	2024-11-15 20:27:12
https://accounts.google.com/v3/signin/identifier?continue=	Sign in - Google Accounts	2024-11-15 20:27:13
https://accounts.google.com/v3/signin/challenge/pwd?TL=AKO	Sign in - Google Accounts	2024-11-15 20:27:23
https://accounts.google.com/CheckCookie?continue=https://c	Home	2024-11-15 20:27:32
https://accounts.youtube.com/accounts/SetSID?ssdc=1&sidt=A	Home	2024-11-15 20:27:32
https://accounts.google.com.pk/accounts/SetSID?ssdc=1&sidt	Home	2024-11-15 20:27:32
https://classroom.google.com/	Home	2024-11-16 16:33:39
https://youtube.com/	YouTube	2024-11-15 23:34:28
https://www.youtube.com/	YouTube	2024-11-15 23:34:33
https://www.youtube.com/?themeRefresh=1	YouTube	2024-11-15 23:34:31
https://www.youtube.com/watch?v=hs2nBs0LkuM	Surah Ad-Duha (24 Times) B	2024-11-16 20:35:34
https://www.google.com/search?q=credit+card+numbers&oq=cre	credit card numbers - Google	2024-11-16 16:34:22
https://www.google.com/search?scas_esv=2ed73cc1c03bd200&q=c	credit card numbers - Google	2024-11-16 20:35:33
https://www.google.com/search?q=cat.png&oq=cat.png&gs_lcrp	cat.png - Google Search	2024-11-16 20:35:47
https://www.google.com/search?q=cat.png&oq=cat.png&gs_lcrp	cat.png - Google Search	2024-11-16 20:35:52
https://www.google.com/search?q=cat.png&oq=cat.png&gs_lcrp	cat.png - Google Search	2024-11-16 20:36:09
https://www.google.com/search?q=weapons+png&scas_esv=9ea83b	weapons png - Google Search	2024-11-16 20:36:28
https://www.google.com/search?q=weapons+pdf&scas_esv=9ea83b	weapons pdf - Google Search	2024-11-16 20:36:31
https://www.smallarmsurvey.org/sites/default/files/resour	SAS-HB-06-Weapons-ID-ch3.pdf	2024-11-16 21:39:57
https://www.google.com/search?q=extensions&oq=extensions&g	extensions - Google Search	2024-11-16 21:38:15
https://chromewebstore.google.com/category/extensions	Chrome Web Store - Extension	2024-11-16 21:38:25
https://accounts.google.com/ServiceLogin?passive=1209600&o	Chrome Web Store - Extension	2024-11-16 21:38:25
https://chromewebstore.google.com/accounts/SetOSID?authuse	Chrome Web Store - Extension	2024-11-16 21:38:25
https://chromewebstore.google.com/category/extensions?pli=	Chrome Web Store - Extension	2024-11-16 21:39:58
https://chromewebstore.google.com/detail/retro-games/cildk	Retro Games - Chrome Web Sto	2024-11-16 21:38:37
https://chromewebstore.google.com/detail/happy-dog-virtual	Happy dog - virtual pet for	2024-11-16 21:38:51
https://acrobat.adobe.com/dc-chrome-extension/mv/en_GB/Acr		2024-11-16 21:40:29
chrome-extension://efaidnbmninnbpcadjpcglclefindmkaj/viewer	Acrobat-for-Chrome.pdf	2024-11-16 21:40:30
chrome-extension://efaidnbmninnbpcadjpcglclefindmkaj/https:	chrome-extension://efaidnbmn	2024-11-16 21:40:30

Cache files obtained:

```
Cache Files:
Cache Files Found:
1. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\data_0
2. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\data_1
3. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\data_2
4. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\data_3
5. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000001
6. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000002
7. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000003
8. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000004
9. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000005
10. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000006
11. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000007
12. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000008
13. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000009
14. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_00000a
15. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_00000b
16. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_00000c
17. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_00000d
18. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_00000e
19. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_00000f
20. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000010
21. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000011
22. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000012
23. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000013
24. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000014
25. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000015
26. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000016
27. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000017
28. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000018
29. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000019
30. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_00001a
31. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_00001b
32. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_00001c
33. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_00001d
34. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_00001e
35. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_00001f
36. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000020
37. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000021
38. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000022
39. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000023
40. C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_000024
```

The cache file numbers are given at the start of every line, from there user can see the file number and select any file that user wants to view in hex format as follows:

```

Enter the file number to view in hex (or 0 to skip): 35
Hex View of C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Cache\Cache_Data\f_00001f:
-----
77 4F 46 32 00 01 00 00 00 00 40 0C 00 0F 00 00  wOF2.....@.....
00 00 A5 B0 00 00 3F AD 00 01 00 00 00 00 00 00  .....?.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
1A 81 3C 1B E7 6C 1C 94 3A 06 60 00 85 3A 11 08  ..<..l...:~...
0A 81 A3 00 81 82 64 0B 85 16 00 01 36 02 24 03  ....d.....6.$
8A 28 04 20 05 83 18 07 8E 4E 0C 07 1B F6 91 35  .(. ....N.....5
78 D3 2D E4 76 80 3F BB B5 2C 7F 81 DC 3C 53 6E  x.-.v.?.....<Sn
C7 D2 4F 2F AF 3C 0A 81 8D 83 20 80 FE 11 B3 FF  ..O/.<.....
FF 7B 72 32 44 21 76 40 D4 B6 9B 3F 04 8B 0C C1  .{r2D!v@...?....
22 93 C8 46 E4 CE 5C 33 98 DA DB 2D 35 42 A6 9D  "...F...\3....-5B..
BB D1 78 8C 29 AC 78 DB 24 7A 65 19 5F 63 DE 6C  ..x.)x.$ze._c.l
F8 29 7E 59 85 D7 59 45 E0 4A 7F 65 9E 75 57 FE  .)~Y..YE.J.e.uW.
25 29 FE 3F 2E F5 54 A9 5D AE 71 5F 37 79 B1 34  (%)?.T.].q_7y.4
FA AA B4 24 12 AB 8A D8 2A 74 0B 46 20 23 74 38  ...$....*t.F #t8
BA 6A BF D4 BE A0 47 4F BF 1F 6B 1C 9D 26 0F 45  .j....GO..k..&.E
63 62 B1 58 D7 9C 81 6D 23 7F 92 93 97 E7 E1 F7  cb.X...m#.....
C7 7F 6B EF 73 1F 46 72 02 98 8C 3C 71 7E 1E 40  ..k.s.Fr...<q~.@
5D 8A 50 48 4E 3F 0D 80 77 8F 68 CE 66 F7 2E 17  ].PHN?...w.h.f...
21 68 04 0F 41 2C 48 0C 82 88 D4 8D D6 1F 2A 48  !h..A,H.....*H
A8 52 C7 BD 54 8C 52 D1 A7 2A 88 07 DA EF F3 90  .R..T.R.*.....
BA E5 29 B5 E1 F9 6D F6 8C 7D 75 A2 18 8D 22 B0  .)....m..}u...".
29 28 4A E6 87 FF E1 03 82 C0 07 3E 21 AD 20 08  )(J.....>!..
56 2D E3 D2 9B EB EF 45 5E EC 62 51 B7 8B 9E D7  V-.....E^,bQ....
DB 55 EC A2 8A FF FF B8 E7 75 ED 73 3F 24 33 F1  .U.....u.s?.$3.
4C 24 84 01 AD 79 B5 86 85 A2 96 EC 1D E9 D5 4C  L$...y.....L
70 42 D5 48 E5 3D DD 07 DC CB 22 52 5D 7C 3D 80  pB.H.=...."R]|=.
87 BF 5F FD 6F F6 DD 57 A0 AA 0F B3 4E B2 6A 32  ..._o..W....N.j2
02 4C B2 44 9F 88 C2 EF E5 7B D5 3C F2 F3 73 ED  .L.D....{.<...s.
96 57 31 49 D0 20 7A 48 78 3A AB 1D 49 A4 89 9F  .W1I. zHx:...I...
DA DC DE FE 47 A0 7F 7E BF 36 BB CB 45 1E 26 49  ....G...~.6...E.&I
34 89 4A 86 9F 68 E6 59 AD 05 9A 75 4D 2E 89 44  4.J..h.Y...uM..D
C8 7A 16 75 2A AF AA 29 8A A3 12 E2 F3 DD 3C EE  .z.u*..).....<.
-----

```

Downloads obtained:

```

👉 Brave Downloads:
👉 Downloads Found:
1. File: C:\Users\HP\Downloads\images.jpeg
   Current Path: C:\Users\HP\Downloads\images.jpeg
   Total Size: 7158 bytes
   Received: 7158 bytes
   Start Time: 2024-11-17 01:36:00
   End Time: 2024-11-17 01:36:05
2. File: C:\Users\HP\Downloads\pngtree-isolated-cat-on-white-background-png-image_7094927.png
   Current Path: C:\Users\HP\Downloads\pngtree-isolated-cat-on-white-background-png-image_7094927.png
   Total Size: 126375 bytes
   Received: 126375 bytes
   Start Time: 2024-11-17 01:36:12
   End Time: 2024-11-17 01:36:16
3. File: C:\Users\HP\Downloads\SAS-HB-06-Weapons-ID-ch3.pdf
   Current Path: C:\Users\HP\Downloads\SAS-HB-06-Weapons-ID-ch3.pdf
   Total Size: 6388055 bytes
   Received: 6388055 bytes
   Start Time: 2024-11-17 01:36:59
   End Time: 2024-11-17 01:37:03

File Path                                     Received      Total Size    Start Time      End Time
-----
C:\Users\HP\Downloads\images.jpeg            7158          7158          2024-11-17 01:36:00  2024-11-17 01:36:05
C:\Users\HP\Downloads\pngtree-isolated-cat-on-white-backgr 126375        126375        2024-11-17 01:36:12  2024-11-17 01:36:16
C:\Users\HP\Downloads\SAS-HB-06-Weapons-ID-ch3.pdf 6388055       6388055       2024-11-17 01:36:59  2024-11-17 01:37:03

Enter the number of the download to view in hex (or 0 to skip):

```

similar as cache, any downloaded file can be viewed in its hex format by selecting the number of file (index starts at 1).

Hex format of a downloaded file:

```
File Path                                     Received      Total Size    Start Time      End Time
-----
C:\Users\HP\Downloads\images.jpeg            7158          7158         2024-11-17 01:36:00 2024-11-17 01:36:05
C:\Users\HP\Downloads\pngtree-isolated-cat-on-white-backgr 126375       126375       2024-11-17 01:36:12 2024-11-17 01:36:16
C:\Users\HP\Downloads\SAS-HB-06-Weapons-ID-ch3.pdf 6388055      6388055      2024-11-17 01:36:59 2024-11-17 01:37:03

Enter the number of the download to view in hex (or 0 to skip): 3

Hex View of C:\Users\HP\Downloads\SAS-HB-06-Weapons-ID-ch3.pdf:

25 50 44 46 2D 31 2E 35 0A 25 A7 E3 F1 F1 0A 32 %PDF-1.5%....2
20 30 20 6F 62 6A 0A 3C 3C 0A 2F 54 79 70 65 20 0 obj.<<./Type
2F 43 61 74 61 6C 6F 67 0A 2F 56 65 72 73 69 6F /Catalog./Versio
6E 20 2F 31 23 32 45 35 0A 2F 50 61 67 65 73 20 n /1#2E5./Pages
34 20 30 20 52 0A 2F 50 69 65 63 65 49 6E 66 6F 4 0 R./PieceInfo
20 35 20 30 20 52 0A 2F 56 69 65 77 65 72 50 72 5 0 R./ViewerPr
65 66 65 72 65 6E 63 65 73 20 36 20 30 20 52 0A eferences 6 0 R.
2F 50 61 67 65 4C 61 79 6F 75 74 20 2F 53 69 6E /PageLayout /Sin
67 6C 65 50 61 67 65 0A 2F 50 61 67 65 4D 6F 64 gilePage./PageMod
65 20 2F 55 73 65 4E 6F 6E 65 0A 2F 4C 61 6E 67 e /UseNone./Lang
20 28 65 6E 2D 47 42 29 0A 3E 3E 0A 65 6E 64 6F (en-GB).>>.endo
46 6A 0A 37 38 20 30 20 6F 62 6A 0A 3C 3C 0A 2F bj.78 0 obj.<<./
62 69 6C 74 65 72 20 2F 46 6C 61 74 65 44 65 63 Filter /FlateDec
6F 64 65 0A 2F 4C 65 6E 67 74 68 20 32 30 31 0A ode./Length 201.
3E 3E 0A 73 74 72 65 61 6D 0D 0A 48 89 4C 8F C1 >>.stream..H.L...
6E C2 40 0C 44 7F 65 8E C9 81 ED 3A DE 6C 36 BD n.@.D.e.....l6.
41 8B DA 72 42 C5 52 0F 80 AA 08 02 A2 25 A1 22 A..R.R.....%.
48 FC 3E 36 55 A5 5E 6C 6B 3C F3 2C 7B 47 65 80 H.>6U.^lk<.,{Ge.
77 05 8C 56 1F 0B 7C E3 E1 65 E1 B1 1F 54 09 85 w..V..|.e...T..
28 0B 04 AA B5 25 94 A4 3E 8E 38 B7 D8 61 22 BA +....%...8..a".
27 CD 44 B6 78 6D 39 11 93 64 07 0A 86 B3 46 3E '.D.xm9..d...F>
B8 94 A8 06 27 76 B1 2A 23 A4 43 F6 F4 3A 9E CB ....'v.*#.C.....
F4 1D 9C CB D7 DD 69 C7 D3 1D 41 9F 7F 8C F4 CB .....i...A.....
48 FF 18 21 39 E6 CA 10 CB EC 23 D7 29 68 9B 9F H..!9.....#.k..
53 3F E0 6D D8 F6 97 C3 CA 73 B5 69 2E 87 53 FF S?.m.....s.i..S.
88 7C 2D 33 8C F4 25 F3 5F 15 34 22 CD 32 E4 19 .|-3..%...4"..2..
D9 A2 68 8E 47 8C CF DD 60 F7 A7 82 9B 00 03 00 ..k.G.....
A5 B0 3B CC 0D 0A 65 6E 64 73 74 72 65 61 6D 0A ;;...endstream.
65 6E 64 6F 62 6A 0A 38 31 20 30 20 6F 62 6A 0A endobj.81 0 obj.
3C 3C 0A 2F 46 69 6C 74 65 72 20 2F 46 6C 61 74 <<./Filter /Flat
65 44 65 63 6F 64 65 0A 2F 4C 65 6E 67 74 68 20 eDecode./Length
33 37 30 37 0A 3E 3E 0A 73 74 72 65 61 6D 0D 0A 3707.>>.stream..
```

Extensions obtained:

```
Fetching Brave Extensions...

Installed Brave Extensions:
Extension Name                               Version      Description
-----
MSG_web2pdfExtnName__                       24.10.2.0   MSG_web2pdfExtnDescriptionChrome__
MSG_extensionName__                         3.10        MSG_extensionDescription__

Available extensions for hex view:
1. MSG_web2pdfExtnName__
2. MSG_extensionName__

Enter the number of the extension to view its manifest.json in hex (or 0 to skip): 1

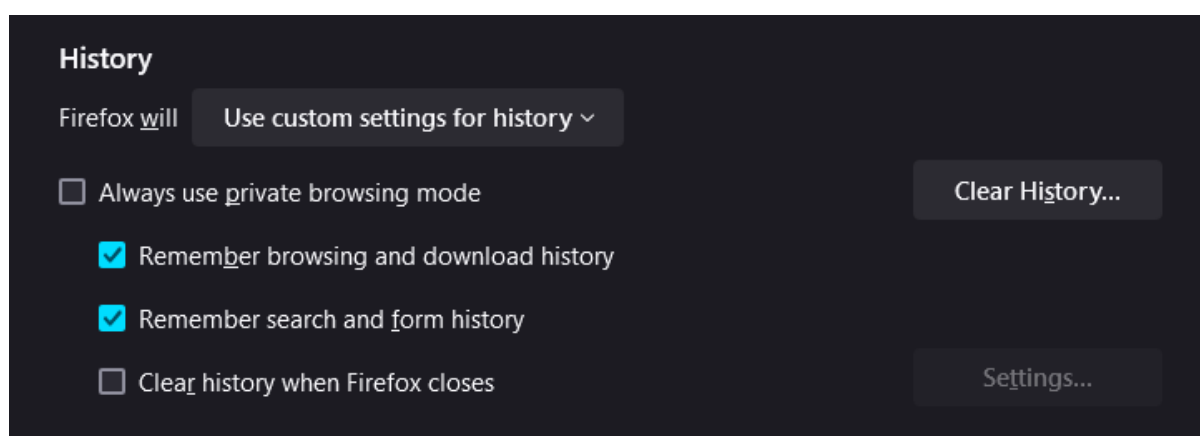
Hex View of C:\Users\HP\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Extensions\efaidnbmnmnibpcajpcglclef
7B 0D 0A 20 20 20 22 61 63 74 69 6F 6E 22 3A 20 {... "action":
7B 0D 0A 20 20 20 20 20 22 64 65 66 61 75 6C {... "defaul
74 5F 69 63 6F 6E 22 3A 20 22 62 72 6F 77 73 65 t icon": "browse
72 2F 69 6D 61 67 65 73 2F 61 63 72 6F 62 61 74 r/images/acrobat
5F 64 63 5F 61 70 70 69 63 6F 6E 5F 32 34 2E 70 _dc_appicon_24.p
6E 67 22 2C 0D 0A 20 20 20 20 20 20 22 64 65 66 ng",... "def
61 75 6C 74 5F 70 6F 70 75 70 22 3A 20 22 62 72 ault_popup": "br
6F 77 73 65 72 2F 6A 73 2F 70 6F 70 75 70 2E 68 owser/js/popup.h
74 6D 6C 22 2C 0D 0A 20 20 20 20 20 20 22 64 65 tml",... "de
66 61 75 6C 74 5F 74 69 74 6C 65 22 3A 20 22 5F fault_title": "_
5F 4D 53 47 5F 65 78 74 65 6E 73 69 6F 6E 4D 65 _MSG_extensionMe
6E 75 54 69 74 6C 65 5F 5F 22 0D 0A 20 20 20 7D nuTitle__"... }
2C 0D 0A 20 20 20 22 62 61 63 6B 67 72 6F 75 6E ,... "backgroun
64 22 3A 20 7B 0D 0A 20 20 20 20 20 20 22 73 65 d": {... "se
72 76 69 63 65 5F 77 6F 72 6B 65 72 22 3A 20 22 rvice_worker": "
73 65 72 76 69 63 65 2D 77 6F 72 6B 65 72 2E 6A service-worker.j
73 22 2C 0D 0A 20 20 20 20 20 20 22 74 79 70 65 s"... "type
22 3A 20 22 6D 6F 64 75 6C 65 22 0D 0A 20 20 20 ": "module"...
7D 2C 0D 0A 20 20 20 22 63 6F 6E 74 65 6E 74 5F },... "content_
73 63 72 69 70 74 73 22 3A 20 5B 20 7B 0D 0A 20 scripts": [ {...
20 20 20 20 20 22 6A 73 22 3A 20 5B 20 22 6C 69 "js": [ "li
62 73 2F 6A 71 75 65 72 79 2D 33 2E 31 2E 31 2E bs/jquery-3.1.1.
6D 69 6E 2E 6A 73 22 2C 20 22 62 72 6F 77 73 65 min.js", "browse
72 2F 6A 73 2F 63 68 2D 73 65 74 74 69 6E 67 73 r/js/ch-settings
```

A few differences in nonchromium based browsers artifacts fetching:

1- Downloads:

Nonchromium based browsers uses the places.sqlite database to store browsing history, bookmarks, and sometimes download history. Download URLs are stored in the moz_places table, and associated metadata (like visit dates) is stored in the moz_historyvisits table while chromium bases browsers (brave) uses a database named History in the user profile directory. The download information is stored in a separate table called downloads.

For the given scenario first make sure that these are unchecked in the firefox browser privacy settings first or else the downloads will not be visible at all:



Before applying these changes, the tool was giving the output that 'no downloads found' and after the changes we got the downloads history: (**for firefox**)

```
📄 Download Data:
Would you like to view the places.sqlite database in hex? (y/n): n

📄 Firefox Downloads:
File Name                                     Source URL                                     Download Time
-----
Unknown                                     https://www.mozilla.org/privacy/firefox/      2024-11-16 00:38:51
Firefox Privacy Notice - Mozilla             https://www.mozilla.org/en-US/privacy/firefox/ 2024-11-16 00:38:51
Continue to your Mozilla account              https://accounts.firefox.com/?context=fx_desktop_v3&entryp 2024-11-16 01:14:52
Continue to your Mozilla account              https://accounts.firefox.com/signup?context=fx_desktop_v3& 2024-11-16 01:15:20
Mozilla accounts                             https://accounts.firefox.com/signup?showReactApp=true&devi 2024-11-16 01:15:21
Enter confirmation code | Mozilla a           https://accounts.firefox.com/confirm_signup_code?showReact 2024-11-16 01:15:48
Connect another device: Sync your Fire        https://accounts.firefox.com/pair?showReactApp=true&device 2024-11-16 01:16:24
Connect another device: Sync your Fire        https://accounts.firefox.com/settings?showReactApp=true&de 2024-11-16 01:16:30
Mozilla accounts                             https://accounts.firefox.com/settings?deviceId=1d5b9b8f8ea 2024-11-16 01:16:30
Mozilla accounts                             https://accounts.firefox.com/settings?deviceId=1d5b9b8f8ea 2024-11-16 01:16:55
calculus.pdf - Google Search                  https://www.google.com/search?client=firefox-b-d&q=calculu 2024-11-17 01:45:34
Unknown                                       https://3lihandam69.files.wordpress.com/2018/10/calculus-1 2024-11-17 01:45:37
calculus-10th-edition-anton.pdf               https://3lihandam69.wordpress.com/wp-content/uploads/2018/ 2024-11-17 01:45:38
digitalforensics pdf - Google Search          https://www.google.com/search?q=digitalforensics+pdf&clien 2024-11-17 01:46:19
FORC Book 1.pdf                              https://ec.europa.eu/programmes/erasmus-plus/project-resul 2024-11-17 01:46:25
Module 01 Introduction to Digital Fore         https://www.cemca.org/ckfinder/userfiles/files/Module%2001 2024-11-17 01:46:46
Cyber Forensics.pdf                          https://annamalaiuniversity.ac.in/studport/download/engg/i 2024-11-17 02:04:04
Cyber Forensics.pdf                          https://annamalaiuniversity.ac.in/studport/download/engg/i 2024-11-17 02:04:04
dog.png - Google Search                      https://www.google.com/search?client=firefox-b-d&q=dog.png 2024-11-17 02:03:30
cat.jpg - Google Search                      https://www.google.com/search?client=firefox-b-d&q=cat.jpg 2024-11-17 02:11:26
cat.jpg - Google Search                      https://www.google.com/search?client=firefox-b-d&q=cat.jpg 2024-11-17 02:04:29
digital forensics pdf - Google Search         https://www.google.com/search?q=cyber+pdf&client=firefox-b 2024-11-17 02:11:38
cyber pdf - Google Search                    https://mrcet.com/pdf/Lab%20Manuals/IT/CYBER%20SECURITY%20 2024-11-17 02:11:44
CYBER SECURITY (R18A0521).pdf                 https://mrcet.com/pdf/Lab%20Manuals/IT/CYBER%20SECURITY%20 2024-11-17 15:09:20
cat - Google Search                          https://www.google.com/search?client=firefox-b-d&q=cat     2024-11-17 15:09:22
cat - Google Search                          https://www.google.com/search?client=firefox-b-d&sca_esv=8 2024-11-17 15:09:29
cat - Google Search                          https://www.google.com/search?client=firefox-b-d&sca_esv=8 2024-11-17 15:09:37
mano.jpg                                     https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTOMx 2024-11-17 15:15:54
cat - Google Search                          https://www.google.com/search?client=firefox-b-d&sca_esv=8 2024-11-17 15:15:59
secret.jpg                                   https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRlhx 2024-11-17 15:16:06

Enter the number of the download to view in hex (or 0 to skip):
```


For LibreWolf:

```
Download Data:
Would you like to view the places.sqlite database in hex? (y/n): n

Firefox Downloads:
File Name                                     Source URL                                     Download Time
-----
youtube at DuckDuckGo                        https://duckduckgo.com/?t=ffab&q=youtube      2024-11-16 07:54:44
youtube at DuckDuckGo                        https://duckduckgo.com/?t=ffab&q=youtube&ia=web 2024-11-16 07:54:45
YouTube                                     https://www.youtube.com/                     2024-11-16 07:54:48
YouTube                                     https://www.youtube.com/                     2024-11-16 07:55:24
Unknown                                     https://accounts.google.com/ServiceLogin?service=youtube&u 2024-11-16 07:54:56
Unknown                                     https://accounts.google.com/InteractiveLogin?continue=http 2024-11-16 07:54:56
Unknown                                     https://accounts.google.com/v3/signin/identifier?continue= 2024-11-16 07:54:56
YouTube                                     https://accounts.google.com/v3/signin/identifier?continue= 2024-11-16 07:54:57
YouTube                                     https://accounts.google.com/v3/signin/challenge/pwd?TL=AKO 2024-11-16 07:55:14
Unknown                                     https://accounts.google.com/CheckCookie?continue=https://w 2024-11-16 07:55:22
Unknown                                     https://accounts.youtube.com/accounts/SetSID?ssdc=1&sid=A 2024-11-16 07:55:22
Unknown                                     https://accounts.google.com.pk/accounts/SetSID?ssdc=1&sidt 2024-11-16 07:55:23
Unknown                                     https://www.youtube.com/signin?action_handle_signin=true&a 2024-11-16 07:55:23
The Wazuh File Integrity Monitoring (F       https://www.youtube.com/watch?v=a02jU0Fa9Hs 2024-11-16 07:55:46
Cybersecurity SOC Analyst Lab - PDF An      https://www.youtube.com/watch?v=k32X5gWsiqU 2024-11-16 07:56:01
CyberDefenders SOC Analyst Lab - Web S     https://www.youtube.com/watch?v=j-Bb3xQffJA 2024-11-16 07:56:06
you need this FREE CyberSecurity tool      https://www.youtube.com/watch?v=3CaG2GI1kn0 2024-11-16 07:56:16
what to feed a dog pdf at DuckDuckGo        https://duckduckgo.com/?t=ffab&q=what+to+feed+a+dog+pdf 2024-11-17 14:56:35
what to feed a dog pdf at DuckDuckGo        https://duckduckgo.com/?t=ffab&q=what+to+feed+a+dog+pdf&ia 2024-11-17 14:56:36
How Much Should I Feed My Dog? Vet-App      https://www.dogster.com/dog-nutrition/how-much-should-i-fe 2024-11-17 14:56:39
How Much Should I Feed My Dog? Vet-App      https://www.dogster.com/dog-nutrition/how-much-should-i-fe 2024-11-17 14:56:48
dog_nutrition_final_fix.pdf                 https://nap.nationalacademies.org/resource/10668/dog_nutri 2024-11-17 14:56:55
cat.jpg at DuckDuckGo                       https://duckduckgo.com/?q=cat.jpg&t=ffab      2024-11-17 14:57:27
cat.jpg at DuckDuckGo                       https://duckduckgo.com/?q=cat.jpg&t=ffab&ia=web 2024-11-17 14:57:29
cat.jpg at DuckDuckGo                       https://duckduckgo.com/?q=cat.jpg&t=ffab&iax=images&ia=ima 2024-11-17 14:57:31
cat.jpg at DuckDuckGo                       https://duckduckgo.com/?q=cat.jpg&t=ffab&iax=images&ia=ima 2024-11-17 14:57:35
kitten.jpg                                  https://external-content.duckduckgo.com/iu/?u=https%3A%2F% 2024-11-17 14:57:45
cat.jpg at DuckDuckGo                       https://duckduckgo.com/?q=cat.jpg&t=ffab&iax=images&ia=ima 2024-11-17 14:57:51
Unknown                                     http://images6.fanpop.com/image/photos/39000000/Cat-cats-3 2024-11-17 14:57:58
cat000jpg.jpg                              https://external-content.duckduckgo.com/iu/?u=http%3A%2F%2 2024-11-17 14:58:19

Enter the number of the download to view in hex (or 0 to skip):
```

Choosing a downloaded file won't give any hex output and it'll show 'the file no longer exists at that path' or 'URL isn't a local file' because the url field in the moz_places table is the web URL of the resource downloaded (e.g., <https://example.com/file.pdf>).

It does not store the local file path where the downloaded file resides on your machine.

Local File Path is Not Available in places.sqlite:

- Firefox does not store the downloaded file's local file path in places.sqlite.
- This information is typically stored in **other files** (like downloads.json or handlers.json), but Firefox has moved away from those formats in recent updates.

2- Cache:

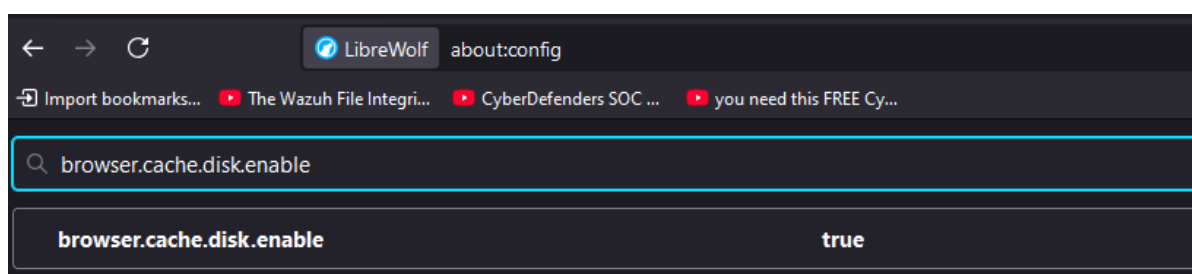
Although the non-chromium browsers show the path of the cache files to be the following under 'about:cache' but the cache directory is sometimes not created on the disk due to various reasons



Corrupted Profile: The profile may be corrupted or not fully functional, which can prevent the cache2 folder from being created. You can try creating a new profile and check if the cache2 folder is created in the new one.

Browser Settings: Ensure that the settings for disk cache are properly enabled:

- Open the **about** page in the browser (type about:config in the address bar).
- Look for browser.cache.disk.enable and ensure it is set to true.



Permissions: Ensure that the browser has the appropriate permissions to write to the cache directory. If there are permission issues, the folder might not be created.

Reinstall or Refresh: If none of the above works, consider resetting the profile or reinstalling the browser. This might help recreate any missing folders or reset configuration settings that are causing the issue.

6. FAQs

- **What is the purpose of this tool?**

The Browser Artifacts Forensics Tool helps digital forensic investigators analyze privacy-focused browsers. It extracts critical data such as browsing history, saved passwords, and cached files, which can be used to identify suspicious activities on a suspect's machine.

- **Which browsers are supported?**

The tool supports both Chromium-based browsers like Brave and non-Chromium browsers like Firefox and LibreWolf. It can be extended for other browsers as well.

- **What types of artifacts can this tool extract?**

This tool retrieves saved passwords, browsing history, bookmarks, cache data, download histories, and installation dates. It also allows for hex viewing of key files for deeper analysis.

- **Is the tool compatible with operating systems other than Windows?**

Currently, the tool only supports Windows. Future updates may include support for other operating systems depending on demand and feasibility.

- **What permissions are required to run the tool?**

Administrative privileges are recommended to access protected files and directories fully. This ensures all artifacts can be retrieved without restrictions.

- **How can I install and set up the tool?**

A separate section for this is already given above

- **Can this tool be used on encrypted browser profiles?**

Yes, the tool can retrieve and decrypt artifacts from encrypted profiles, provided it has access to the necessary decryption keys (e.g., for saved passwords in Chromium-based browsers).

- **How is user data protected during an investigation?**

The tool does not alter or delete any data on the suspect's machine. Investigators are encouraged to work on copies of the data to maintain integrity and follow ethical and legal guidelines strictly.

- **What should I do if an artifact is missing or corrupted?**

Ensure that the browser settings allow for artifact creation (e.g., cache and download history). If artifacts are still missing, check for potential profile corruption or permissions issues, and consider refreshing or reinstalling the browser.

- **Is it possible to extend this tool for other browsers?**

Yes, the tool is modular and can be extended to support additional browsers. Developers can add new modules for unsupported browsers by mapping their respective artifact storage locations.

7. Conclusion

Hence, our tool covers all the artifacts that a digital forensics investigator might need to analyze during an investigation of the suspect's machine, the artifacts includes: browsing history, cache data files, all the saved passwords and credentials, downloads history, bookmarks and any other stored fillable data.

8. References

- *Windows Registry Reference*. Retrieved from <https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry>
- *Chromium Project Documentation*. Retrieved from <https://www.chromium.org/developers>
- *Firefox Data Storage*. Retrieved from https://developer.mozilla.org/en-US/docs/Mozilla/Firefox/Data_storage
- **Casey, E. (2011).** *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*.