Examining web browser histories – Firefox

Introduction

Browser histories contain valuable information for many types of investigations. The navigation and search history can help forensic experts to trace down the source of malware or phishing attacks. When criminals search for weapons, chemicals, or instructions in the web before a terroristic attack or a murder the browser history can be used as evidence in court. This also the case for other crimes such as copyright violations (illegal downloads of films or music) and child pornography.

Retrieving the browser history

Firefox stores all data in his profile. On windows folders containing all the profiles data are located under the following path ([user] must be replaced with the real name):

```
C:\Users\[user]\AppData\Roaming\Mozilla\Firefox\Profile
```

If you have multiple profiles and don't know what is the right one, or are on a different operating system, you can also find a link to your profiles folder on the about:support page of firefox.
When performing a forensic analysis of Firefox you should make a copy (or zip archive) of the folder and only work on that copy. If you only care about the browser history, it's enough to just copy `places.sqlite` file.
The file contains an SQLite database with all the browsers visited sites, search queries and more.

About SQLite

SQlite is a library that implements a small and self-contained SQL database engine. Unlike client-server database management systems like MariaDB or PostgreSQL it has no standalone processes with which the application communicates. Instead, it is used by firefox as a linked library. The entire database is stored with all definitions, tables, indices, and data in a single file. The server-less design reduces the amount of configuration needed to set up the database to a minimum and allows very low latencies. On the other hand, it allows very little concurrency as it only relies on file-system locks to control reading and writing from multiple processes. Also, the only access control for the database are file-system permissions.
All these properties make sqlite a perfect tool for browsers to store their browse history.

Investigating places.sqlite

To get a overview of places.sqlite we can run the following sql statement which returns an overview of all tables contained by the database:

```
SELECT * FROM sqlite_master WHERE type = "table";
```

	type	name	tbl_name	r...	sql
1	table	moz_places	moz_places	2	CREATE TABLE moz_places (id I…
2	table	moz_historyvisits	moz_historyvisits	3	CREATE TABLE moz_historyvisits (…
3	table	moz_inputhistory	moz_inputhistory	4	CREATE TABLE moz_inputhistory (…
4	table	moz_hosts	moz_hosts	6	CREATE TABLE moz_hosts (id INT…
5	table	moz_bookmarks	moz_bookmarks	8	CREATE TABLE moz_bookmarks (id…
6	table	moz_keywords	moz_keywords	9	CREATE TABLE moz_keywords (id …
7	table	sqlite_sequence	sqlite_sequence	11	CREATE TABLE sqlite_sequence(nam…
8	table	moz_anno_attributes	moz_anno_attributes	12	CREATE TABLE moz_anno_attributes…
9	table	moz_annos	moz_annos	14	CREATE TABLE moz_annos (id INT…
10	table	moz_items_annos	moz_items_annos	15	CREATE TABLE moz_items_annos (…
11	table	sqlite_stat1	sqlite_stat1	16	CREATE TABLE sqlite_stat1(tbl,id…
12	table	moz_bookmarks_deleted	moz_bookmarks_deleted	17	CREATE TABLE moz_bookmarks_delet…
13	table	moz_meta	moz_meta	19	CREATE TABLE moz_meta (key TEXT …
14	table	moz_origins	moz_origins	20	CREATE TABLE moz_origins (id IN…
15	table	moz_places_metadata	moz_places_metadata	22	CREATE TABLE moz_places_metadata…
16	table	moz_places_metadata_search_queries	moz_places_metadata_search_queries	23	CREATE TABLE moz_places_metadata…
17	table	moz_places_metadata_snapshots	moz_places_metadata_snapshots	25	CREATE TABLE moz_places_metadata…
18	table	moz_places_metadata_snapshots_extra	moz_places_metadata_snapshots_extra	26	CREATE TABLE moz_places_metadata…
19	table	moz_places_metadata_snapshots_groups	moz_places_metadata_snapshots_groups	27	CREATE TABLE moz_places_metadata…
20	table	moz_places_metadata_groups_to_snapshots	moz_places_metadata_groups_to_snapshots	28	CREATE TABLE moz_places_metadata…
21	table	moz_session_metadata	moz_session_metadata	29	CREATE TABLE moz_session_metadat…
22	table	moz_session_to_places	moz_session_to_places	31	CREATE TABLE moz_session_to_plac…
23	table	moz_previews_tombstones	moz_previews_tombstones	32	CREATE TABLE moz_previews_tombst…

Most interesting are `moz_places` which contains a list of all ever visited sites and `moz_historyvisits` contains a history when which place was visited. If this does not provide enough data, have a look at `moz_bookmarks` (all of the user's bookmarks) and `moz_inputhistory` (all searches typed by the user into the browsers url input field).

SQL allows us to do all sorts of useful queries, for example we can easily search for references to hacks but only related to the DIFO topic:

```
SELECT * FROM moz_places
      WHERE lower(title) LIKE "%hack%"
      AND lower(title) LIKE "%difo%";
```

	id	url	title	frecency	last_visit_date	visit_count
1	322824	https://moodle-thu.de/pluginfile.php/122070/mod_resource/c…	Zielstellung - 2022 DIFO FirstHacks.pdf	26	1649192786731000	2
2	326423	https://moodle-thu.de/pluginfile.php/122070/mod_resource/c…	Zielstellung - 2022 DIFO FirstHacks.pdf	50	1649752066616000	2
3	330392	https://moodle-thu.de/mod/forum/discuss.php?d=18811#p23225	DIFO: Save your date for your first hack …	20	1651043387249000	2
4	332733	https://moodle-thu.de/mod/resource/view.php?id=94312&force…	DIFO: List of chosen hacks (round#1)	555	1652080844932000	3
5	332734	https://moodle-thu.de/mod/forum/discuss.php?d=18918#p23355	DIFO: First Round of hacks starts tomorro…	49	1652086049138000	2
6	334617	https://moodle-thu.de/mod/assign/view.php?id=56254	DIFO: Task #5 Upload a PDF and a DOCX fil…	561	1655719629694000	18
7	334646	https://moodle-thu.de/pluginfile.php/122070/mod_resource/c…	Zielstellung - 2022 DIFO FirstHacks.pdf	53	1652080846275000	2
8	334863	https://moodle-thu.de/mod/forum/discuss.php?d=19040#p23498	DIFO: Updated agenda for Hack#1 presentat…	110	1652127409404000	3
9	334864	https://moodle-thu.de/pluginfile.php/122070/mod_resource/c…	Zielstellung - 2022 DIFO FirstHacks.pdf	74	1652123911319000	2
10	334865	https://moodle-thu.de/mod/folder/view.php?id=99419	DIFO: Download the reports for Hacks#1	330	1653563126426000	10
11	334996	https://moodle-thu.de/mod/assign/view.php?id=56254&action=…	DIFO: Task #5 Upload a PDF and a DOCX fil…	144	1652696598624000	4
12	334997	https://moodle-thu.de/mod/assign/view.php?id=56254&action=…	DIFO: Task #5 Upload a PDF and a DOCX fil…	116	1652696598649000	3
13	335349	https://moodle-thu.de/pluginfile.php/123332/mod_resource/c…	Zielstellung - 2022 DIFO SecondHacks.pdf	51	1652350195219000	2
14	335498	https://moodle-thu.de/mod/forum/discuss.php?d=19109#p23573	DIFO: Completing the hack#1 presentations…	59	1652706307547000	2
15	336380	https://moodle-thu.de/pluginfile.php/122070/mod_resource/c…	Zielstellung - 2022 DIFO FirstHacks.pdf	46	1652696631656000	1
16	336417	https://moodle-thu.de/mod/forum/discuss.php?d=19040	DIFO: Updated agenda for Hack#1 presentat…	46	1652706317435000	1
17	336418	https://moodle-thu.de/mod/assign/view.php?id=56255	DIFO: Task #6: Upload a PDF and a DOCX fi…	291	1655820197789000	4
18	336655	https://moodle-thu.de/pluginfile.php/122070/mod_resource/c…	Zielstellung - 2022 DIFO FirstHacks.pdf	47	1652788949528000	1
19	337279	https://moodle-thu.de/mod/forum/discuss.php?d=19229#p23728	DIFO: Upload your hack#1 report and selec…	20	1653048172278000	1
20	338069	https://moodle-thu.de/pluginfile.php/123332/mod_resource/c…	Zielstellung - 2022 DIFO SecondHacks.pdf	50	1653423835159000	1
21	338554	https://moodle-thu.de/pluginfile.php/123332/mod_resource/c…	Zielstellung - 2022 DIFO SecondHacks.pdf	52	1653563123317000	1
22	340019	https://moodle-thu.de/mod/forum/discuss.php?d=19340#p23855	DIFO: Hack#2 presentations will start aft…	56	1653932068998000	1
23	347760	https://moodle-thu.de/pluginfile.php/123332/mod_resource/c…	Zielstellung - 2022 DIFO SecondHacks.pdf	88	1655719641429000	1
24	347987	https://moodle-thu.de/pluginfile.php/123332/mod_resource/c…	Zielstellung - 2022 DIFO SecondHacks.pdf	110	1655832998384000	2

Column order of the output has been changed to provide more valuable information

As moz_places table only provides a timestamp of the last visit and moz_historyvisits does only contain a places id but not the url or description you need a little more knowledge if you want to find what websites were visited at a specific point in time. This can be done by joining the two tables:

```
SELECT * FROM moz_historyvisits
    LEFT JOIN moz_places ON moz_historyvisits.place_id = moz_places.id
        WHERE visit_date > 1655812800000000  --after  21.06.22 14:00
          AND visit_date < 1655823600000000; --before 21.06.22 17:00
```

Unfortunately, all timestamps are in microseconds since 1. January 1970 00:00:00, which makes querying for specific dates & times quite tedious.

Here you can see the joined output, containing both place and visit information:

	...	from_visit	visit_date	url	1	title
21	415743	415741	1655820214103000	https://moodle-thu.de/mod/resource/view.php?id=1…		Wahl 2022: Johannes Lasi
22	415742	415741	1655820212904000	https://moodle-thu.de/mod/resource/view.php?id=1…		Wahl 2022: Tim Eichler
23	415747	0	1655820788761000	https://musikschule-k-w.de/veranstaltungen/konze…		Konzertnacht der Vereine - Musikschule Köngen/Wendlingen
24	415709	415708	1655813986685000	https://netzpolitik.org/2018/digitale-forensik-m…		Digitale Forensik: Mit diesen sieben Programmen liest die Polizei …
25	415720	415719	1655818008116000	https://ppulm.polizei-bw.de/stellenangebote/cybe…		Cyberkriminalist/-in in Sonderlaufbahn (m/w/d) - Polizeipräsidium …
26	415716	415715	1655816519432000	https://support.magnetforensics.com/s/		Home
27	415717	415716	1655816528090000	https://support.magnetforensics.com/s/axiom-cyber		Magnet AXIOM Cyber
28	415715	415714	1655816485340000	https://support.magnetforensics.com/s/cyber-soft…		AXIOM Cyber Software and Downloads
29	415718	415717	1655816542102000	https://support.magnetforensics.com/s/cyber-soft…		AXIOM Cyber Software and Downloads
30	415725	0	1655819936645000	https://thu.webex.com/join/markus.schaeffter		<null>
31	415713	0	1655816481371000	https://thu.webex.com/thu-en/url.php?gourl=https…		Externer Standort
32	415708	0	1655813984903000	https://thu.webex.com/thu-en/url.php?gourl=https…		Externer Standort
33	415714	0	1655816482283000	https://thu.webex.com/thu-en/url.php?gourl=https…		Externer Standort
34	415711	0	1655816040347000	https://thu.webex.com/thu-en/url.php?gourl=https…		Externer Standort
35	415726	415725	1655819936702000	https://thu.webex.com/wbxmjs/joinservice/sites/t…		Cisco Webex Meetings
36	415727	415726	1655819940903000	https://thu.webex.com/webappng/sites/thu/dashboa…		Cisco Webex Meetings - persönlicher Raum
37	415730	415729	1655820096942000	https://webapps.verwaltung.hs-ulm.de/polyasauth		<null>
38	415731	415730	1655820109210000	https://webapps.verwaltung.hs-ulm.de/polyasauth/		Anmeldung THU
39	415724	0	1655818149398000	https://www.ausbildung.de/berufe/duales-studium-…		Gehalt und Verdienst für das duale Studium bei der Polizei
40	415721	0	1655818124706000	https://www.google.com/search?channel=nrow5&clie…		Kriminalkommissar/-in im gehobenen Polizeivollzugsdienst bw besold…
41	415722	415721	1655818132705000	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&…		<null>
42	415712	415711	1655816043288000	https://www.heise.de/download/product/x-ways-for…		X-Ways Forensics | heise Download
43	415719	0	1655817992196000	https://www.polizei-bw.de/karriere/		Karriere - Polizei Baden-Württemberg
44	415723	415722	1655818133291000	https://www.polizei-der-beruf.de/gehobener-dienst/		Gehobener Dienst - Polizei Nachwuchs BW
45	415729	415728	1655820096763000	https://www.thu.de/gremienwahlen-abstimmung		<null>
46	415710	0	1655815155214000	https://www.youtube.com/feed/subscriptions		Abos - YouTube
47	415754	0	1655822611135000	https://www.youtube.com/feed/subscriptions		Abos - YouTube
48	415755	415754	1655822630786000	https://www.youtube.com/watch?v=qVOCTOGnyDI		Prozessbeginn nach mutmaßlichen Polizistenmorden bei Kusel - YouTu…

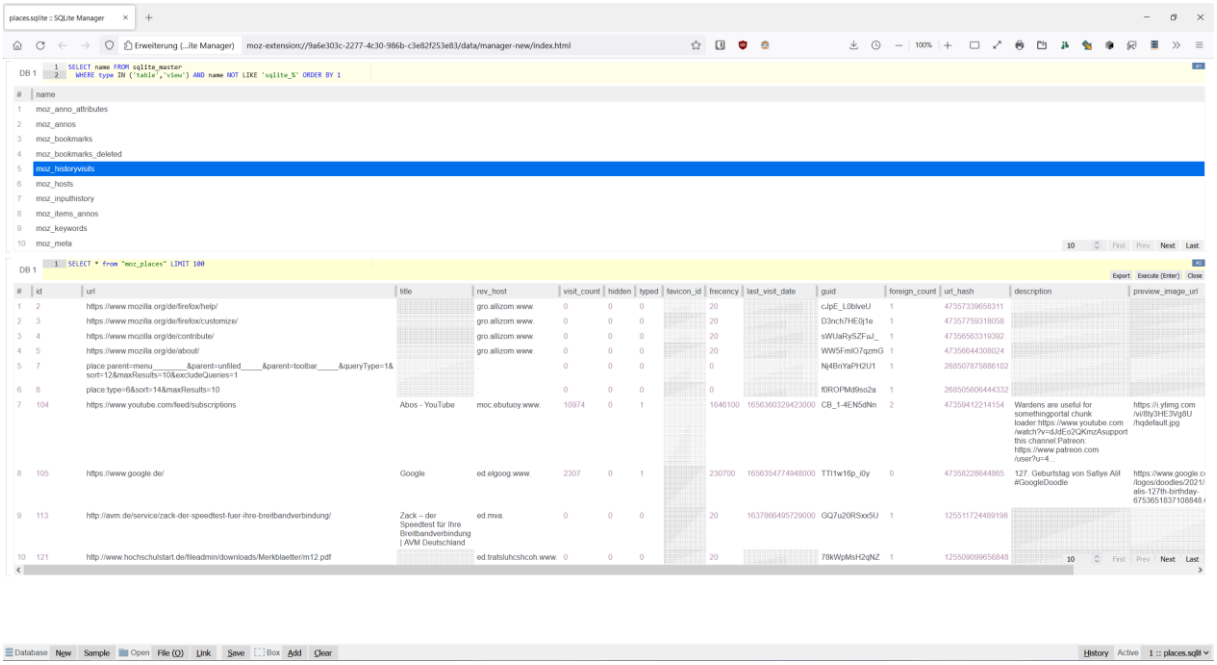
Column order of the output has been changed to provide more valuable information

Forensic tools

Basically, any application that is capable of querying data from an SQLite database can be used to examine browser histories.

SQLite Manager Browser Extension

The possibly simplest way to investigate the sqlite table containing all the visited places is by installing a firefox extension that can view the contents of sqlite databases. SQLite Manager is such an extension. No further software is required.



Sqlite3

Sqlite3 comes with a command line interface and is preinstalled on kali-linux. Many cyber forensic experts prefer command line applications over graphical user interfaces as its very easy to protocol all your inputs. This is important when using findings in court as every step of the forensic experts must be reproduceable. When working with sqlite command line the following inputs are particularly helpful:

```
.open --readonly places.sqlite
.output /mnt/d/Desktop/examination.txt
.mode table
```

`.open` opens the database with the given file name, `--readonly` makes access read-only so nothing can be accidentally overwritten.

`.output` will write all output from the sql statements to the given file

`.mode` will alter how the output is formatted. csv is quite useful if you want to open it in excel or json to exchange data with other applications.

Dumpzilla

Dumpzilla is a small command line application written in python that simplifies the process of searching for evidence in browser data and exporting it. It is included in kali-linux but does only work with Firefox, Iceweasel and Seamonkey browsers.

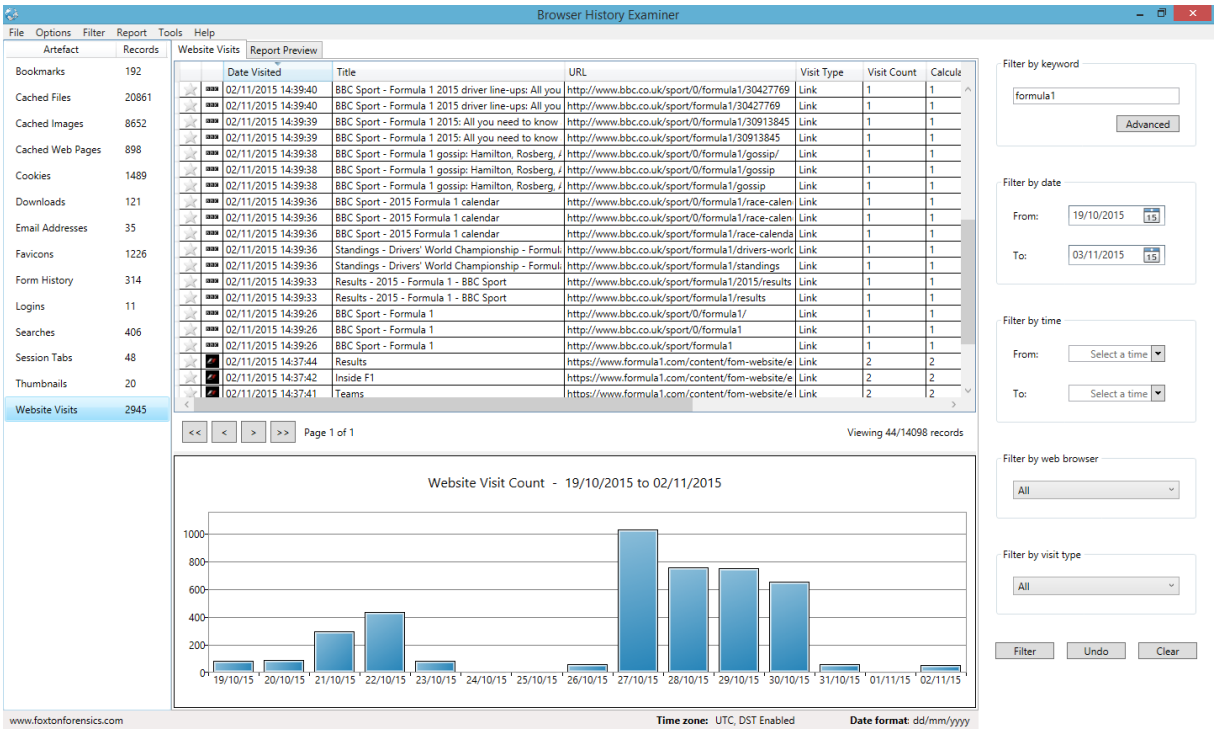
```
┌──(joblo㉿PC-J0B10)-[~]
└─$ dumpzilla --help
usage: python dumpzilla.py PROFILE_DIR [OPTIONS]

Options:

 --Addons
 --Search
 --Bookmarks [-bm_create_range <start> <end>][-bm_last_range <start> <end>]
 --Certoverride
 --Cookies [-showdom] [-domain <string>] [-name <string>] [-hostcookie <string>] [-access <date>]
[-create <date>]
          [-secure <0|1>] [-httponly <0|1>] [-last_range <start> <end>] [-create_range <start> <e
nd>]
 --Downloads [-range <start> <end>]
 --Export <directory> (export data as json)
 --Forms [-value <string>] [-forms_range <start> <end>]
 --Help (shows this help message and exit)
 --History [-url <string>] [-title <string>] [-date <date>] [-history_range <start> <end>] [-frequ
ency]
 --Keypinning [-entry_type <HPKP|HSTS>]
 --OfflineCache [-cache_range <start> <end> -extract <directory>]
 --Preferences
 --Passwords
 --Permissions [-host <string>] [-modif <date>] [-modif_range <start> <end>]
 --RegExp (use Regular Expresions for string type filters instead of Wildcards)
```

Foxton Browser History Examiner

Foxton forensics is a company that has specialized on providing tools for browser history examination. The Browser History Examiner (BHE) runs only on windows computers but is capable of investigating histories of all major web browsers: Chrome, Edge, Firefox and Internet Explorer are all supported. It



provides an easy user interface to visualize all browser data and easily search for keywords, dates or other metadata.

Magnet AXIOM Cyber

Axiom Cyber is a program by Magnet Forensics to acquire and analyze a wide range of evidence from computers, mobile devices, and cloud sources. The company advertises with “point-to-point remote acquisition, a covert on-demand agent, acquisition from cloud services, and automatically resumed collection”.

[redacted]

Sources

https://support.mozilla.org/en-US/kb/profiles-where-firefox-stores-user-data

https://www.sqlite.org/

https://support.magnetforensics.com/s/cyber-software-and-downloads