# Cyber Taster - Web Browser Forensics

This practical explores artefacts left behind by Web Browsing, exploring Firefox (Part A) and Chrome (Part B). A forensic analyst must be able to analyse artefacts from a variety of different applications, in this case different Web browsers. We will explore two different browsers to get an idea of how they are similar, and where they differ.

A bonus exercise at the end of the practical will look at artefacts left behind by the Skype chat application, which stores data using similar databases to Firefox and Chrome.

**The resources for this practical session can be downloaded from** [**https://github.com/smck1/taste\_of\_cyber/tree/master/05\_digital\_forensics**](https://github.com/smck1/taste_of_cyber/tree/master/05_digital_forensics)

**Download** and **unzip** the **morning\_evidence.zip** to somewhere convenient, such as the desktop.

We will use the **DB Browser for SQLite** utility. This utility allows for SQLite database files to be explored, which is a common storage format used by applications such as Web browsers and chat applications.

**If the DB Browser is not already installed on your PC you can download it from**: [**https://sqlitebrowser.org/dl/**](https://sqlitebrowser.org/dl/)

# Part A – Firefox

Many forensic investigations use Web browsing history, either directly or indirectly. In some cases the traces left behind by the browser are incriminating, such as searching for illegal content, in others they may simply help the investigator piece together a timeline of events. These traces are therefore incredibly important to many types of investigation.

This workshop will not contain any real evidence of a crime, however it is important to remember that something as simple as a bookmark or search query can make a huge difference in an investigation.

## Firefox Webpages

Firefox stores its browsing data separately for each user. On Windows 10 this is located at:

C:\Users\***[username]***\AppData\Local\Mozilla\Firefox\Profiles\***XXXXXXXX***.default\

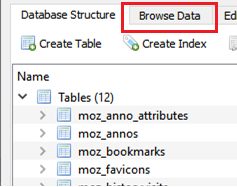
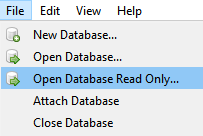
Where ***[username]*** is the name of the Windows user and ***XXXXXXXX*** is a random serious of characters forming a profile ID for the browser.

The Firefox evidence for this practical came from the path:

C:\Users\Arnie\AppData\Roaming\Mozilla\Firefox\Profiles\na6pxjnm.default

From this we can determine that the username is Arnie, and that we are using the default profile, but not much else.

1. From the **zip** file you downloaded earlier, open the **Firefox folder then open the na6pxjnm.default** subfolder.
   * Notice that Firefox makes use of many files to store its history. We are mainly interested in places.sqlite
2. **Start the** **DB Browser** application and **select “Open Database Read Only…” to open place.sqlite** from the **na6pxjnm.default folder**
3. You should now see a list of tables which are contained within the SQLite database. Click on the “Browse Data” tab to begin exploring the evidence.



* There are many tables in the database, but we will focus on using just a few to extract forensic artefacts:
  + moz\_places – contains history information for websites, such as page title, URL and the date of the visit.
  + moz\_bookmarks – contains Firefox bookmark information. This table does not actually contain the page URLs, which are stored in the moz\_places table
* We can ignore the other tables for this workshop. Use the above tables to answer the questions below.
  + Take note of the column headings in each table, the names are often very useful, such as “title” or “url”.

Questions:

Q1: Why did we open the database in Read Only mode?

Q2: What is the name of the game which has been bookmarked?

Q3: When was the game bookmarked?   
Note: You will need to convert the timestamp into human readable format using this tool: <https://www.epochconverter.com/>

The bookmark with the title “Gumtree toyota celica” has an “fk” value of 146. “fk” stands for “foreign key”, which is a reference to the ID of an entry in another table. In this case, the “fk” value from moz\_bookmarks refers to the “id” value of the same item in moz\_places.

Q4: Using the above information, what is the full URL of the bookmark “Gumtree toyota celica”?

Q5: A search was performed on **atgtickets.com**, which is visible in one of the URLs. Which show was being searched for, and in which city?

## Firefox Cache

Browsers often store media files, such as images, videos and sounds, to the local disk so that they don’t have to be downloaded again every time the same page is visited.

The Firefox cache is located in a separate directory from the Web history we used previously, and is found at:

C:\Users\***[username]***\AppData\Local\Mozilla\Firefox\Profiles\***XXXXXXXX***.default\cache2\

We’ll have a quick look at what was cached for the Arnie user.

1. From the zip file you extracted earlier open the **Firefox\cache\na6pxjnm.default\caches2\entries** folder
   * Notice that all of the filenames appear to be random hexadecimal characters (0-9, A-F), with no file extensions
   * This folder contains many different types of files.  
     For example: 3BE95930D1C6922ADC42FB42D72F21DCE83F7DD6 is a JPEG file, while 462CB53629E716A114514D05224E1510C308816F is an MP4 file.
   * Many of these files are media files which can be opened with a media playing application, such as Windows Media Player, VLC, or Media Player Classic (MPC).
2. **Try opening some files in one of the above applications to see what they are.**   
   Don’t worry if you get an error message, some files won’t open.
   * This is a little tedious, but forensics tools normally offer a “preview” which lets you see the content of the file whether the file has an extension or not. FTK Imager is useful for browsing directories of images, for example.

**Note:** You may also wish to try using dedicated tools for viewing the Firefox cache, such as:

<https://www.nirsoft.net/utils/mozilla_cache_viewer.html>

Questions:

Q6: What is the number of the yellow and black car in the centre of the file **136062B1EDF7116FDD097C870FF614499DD71B8C**?

Q7: When was **136062B1EDF7116FDD097C870FF614499DD71B8C** last modified? (This will be the creation date of the file in the cache)

Q8: The four largest files are all playable video files. What is the common theme that they all share?

# Part B – Google Chrome

## Browsing History

We will start with the browsing history for Chrome, which is again stored in the SQLite format.

Chrome stores all browsing data, including its cache at:

C:\Users\**[username]**\AppData\Local\Google\Chrome\User Data\Default

However, unlike Firefox, Chrome stores data in multiple SQLite databases. For this workshop we will focus on the follow files:

* Login\_Data – saved credentials from login forms
  + Contains the “stats” and “logins” tables
* History – Details of stored webpages, URLs, etc, similar to places.sqlite from Firefox.
  + Contains the “downloads”, “urls”,

1. Open the **Chrome folder** from the **zip file** and find the **Login\_Data** database. Open it in **DB Browser**. For questions **11-14, switch to the History database**.

Use the appropriate databases, and the DB Browser, to answer the following questions:

Q9: In the **stats** **table** of the **Login\_Data** **database**, which email address has been used to login to Google, Facebook and live.com?

Q10: A password has been saved for the Google account [sirmorgenchutzpah@gmail.com](mailto:sirmorgenchutzpah@gmail.com), what is it?

Q11: The **urls table** of the **History database** has a “visit\_count” column. What is the title of the most visited URL in Chrome?

Q12: When was outlook.com last visited? (You will need to use a different converter than last time as Chrome uses webkit timestamps, not Unix epoch: <https://www.epochconverter.com/webkit>)

Q13: The biggest download recorded is 9476678 bytes. What is the filename of the download?

Q14: DB Browser allows filter terms to be typed in at the top of the column. How many searches in the “keyword\_search\_terms” table contain   
the word “encrypt”?

**Note:** You may also wish to explore the Chrome cache using:

<https://www.nirsoft.net/utils/chrome_cache_view.html>

# Bonus: Skype Forensics

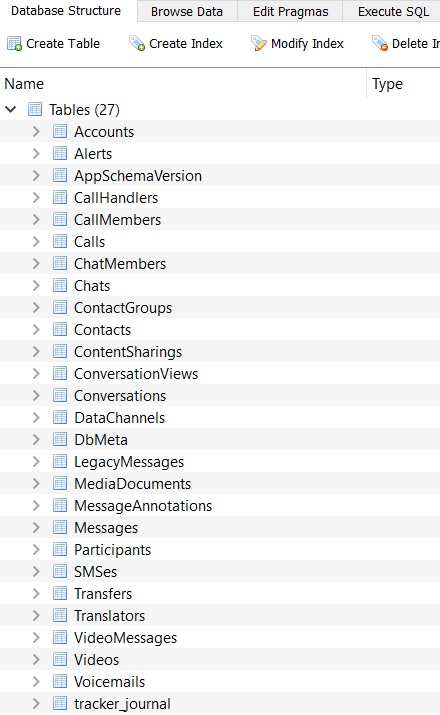
Chat applications also store relevant traces which can be of use to a forensic examiner.

Skype 7 stores logs of user activity and accounts at:

C:\Users\**[username]**\AppData\Roaming\Skype\**[skypeusername]**

The primary storage mechanism is the SQLite file **main.db**.

1. **Open the Skype\live#3ac.guzman88\main.db file in DB Browser** and answer the following questions.



|  |
| --- |
| Which email was used to login to the account?    What is the skype name of the account?    What is the full name of the user, as it is listed in Skype? |

Let’s first look at the Accounts table.

Questions:

Now use your judgement to determine which tables contain the data for the following questions.

Questions:

Which version of Skype was used?

Who are the people on the contacts list?

Which person on the contacts list has specified an avatar/profile picture? What is in the picture?

How many outgoing calls were made? Who to?

When did the call(s) begin (human readable date/time)?