Browser and Internet Forensics

Objective

1. To retrieve the websites visited by the user through firefox browser by investigating the SQLlite databases
2. Retrieving users browser history using pasco
3. Retrieving cookie information stored by Internet Explorer using Galleta

In Browser Forensics, forensic investigator can find information about the activities of the suspect in their web browser. It’s important to note that this information will vary by operating system and browser.

Internet Explorer:-

Let’s begin with Microsoft’s Internet Explorer. It is installed on every single Windows system as the default browser (except on newer versions of Window 10 where Edge is default, though IE is still installed), so it is widely used. In many Institutional and Corporate environments, it is the only browser allowed.

IE places its records in different places depending upon the version of Windows. Let’s look at its recent versions since 2000 first.

Windows 2000 & XP:-

We can get evidence of the user’s internet activity in the following locations:

%systemdir%\Documents and Settings\%username%\Local Settings\Temporary Internet Files\Content.ie5

%systemdir%\Documents and Settings\%username%\Cookies

%systemdir%\Documents and Settings\%username%\Local Settings\History\history.ie5

Windows Vista & 7:-

The path of the files is slightly different beginning with Windows Vista and 7. We can find IE’s files at:

%systemdir%\Users\%username%\AppData\Local\Microsoft\Windows\Temporary Internet Files\

%systemdir%\Users\%username%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\

Please note that AppData and Temporary Internet Files are hidden files.

Mozilla Firefox:-

With Mozilla Firefox and its many variations (IceWeasel in Kali Linux is one), most of the information is stored in SQLite databases. We can find those databases at different locations based upon the operating system.

Below is the path to the database in Windows (XP, Vista, and 7), Linux, and Mac OS X:

Windows XP:-

C:\Documents and Settings\<username>\Application Data\Mozilla\Firefox\Profiles\<profile folder>\places.sqlite

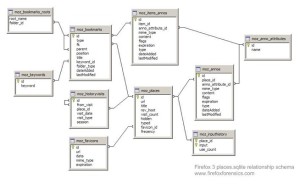
GNU/Linux:-

/home/<user>/.mozilla/firefox/<profile folder>/places.sqlite

Mac OS X:-

/Users/<user>/Library/Application Support/Firefox/Profiles/default.lov/places.sqlite

Mozilla uses a relational database to store the user’s data, which has a structure like that below:



Browser Basics

The most prevalent software applications in use today are probably Web browsers. They are used for viewing, retrieving, traversing, and presenting information resources obtained from the Web. Although browsers are complex software applications, they have common functionality regarding their main components. A simplified overview of their high level structure is as follows:

User Interface - the entire browser display except for its main window.

Browser Engine - takes the marked up content (XML, HTML, etc.) and formatting information (CSS, XSL, etc.) and displays it on the monitor’s screen.

Rendering Engine - responsible for displaying the requested content.

Networking - used for network calls (HTTP, etc.).

UI Backend - used for drawing widgets such as windows and combo boxes.

JavaScript Interpreter - software which interprets/executes JavaScript.

Data Storage - a persistence layer consisting of the data that the browser stores on the computer hard drive.

When a URL is entered into the address bar, the browser communicates with a name server to resolve it into an IP address. This allows the browser to connect to the appropriate Web server using HTTP. Once connected, HTTP commands then direct the Web server to retrieve and transmit data back to the browser. The browser reads the HTML and displays the information resources (HTML document, a .pdf file, an image, a video, etc.) which were identified by a Unified Resource Identifier (URI). The browser then saves the Web documents in its cache using Web caching technology. Caching of Web objects reduces the bandwidth usage and server load and allows the browser to retrieve the same Web page much faster when it is visited at a later time. It also allows recently viewed Web pages to be viewed offline and copied although some of the features such as Flash animations and “real time” objects found on the Web page may not function.

Task 1: Firefox web activity

To retrieve the websites visited by the user through firefox browser, investigate the SQLlite databases

Step 1: Using SQLite to Find Browser Evidence:-

SQLite is now being used by many browsers, applications, and mobile devices that require a small, lightweight relational database. Due to its lightweight nature, it is becoming increasingly popular among mobile devices and mobile apps. That being the case, it is critical that any competent forensic investigator become familiar with it as it is becoming very popular.

To view or query the data in these SQLite databases, SQLite Browser is used .

Step 2: Load the Database File into the SQLite Browser:-

Once you have installed the SQLite browser, navigate to the location specified above for the operating system you are investigating.

You will see many files ending with “sqlite.” These are the database tables that Mozilla uses to store the information on the user’s browsing activities.

Let’s open that database in the SQLite browser. Next, click on the “Database Structure” tab to the far left.

If we click on the “Browse Data” tab, the SQLite browser will display the data in the table we have selected.

Now that we have a basic knowledge of the database structure, let’s use some simple SQL queries to find specific and relevant data to our investigation.

Step 3: Querying the Database:-

Let’s look in the moz\_inputhistory table for input that the user entered into the browser. Click on the “Execute SQL” tab to open a SQL query window. We could then write a general SQL query to find all the input data by entering:

SELECT \* FROM moz\_inputhistory

After entering the query, click on the play (>) button to execute the query.

Step 4: Finding Specific User Input:-

Let’s assume that this was a case where the employee is suspected of having downloaded pirated files from a torrenting site (in many companies and institutions this is prohibited activity, and in many countries it is illegal). We could be very specific in our SQL query to find where the suspect may have input “tor.” We could find every occurrence where they typed “tor” querying the input history with:

SELECT \* FROM moz\_inputhistory WHERE input like ‘%tor%’

This query will provide us all columns (SELECT \*) from the input history table (FROM moz\_inputhistory) where the typed input is like “tor” (WHERE input like ‘%tor%’). Note the wildcards (%) before and after tor. This indicates that we are looking for anything before tor and anything after tor.

This query should provide us with results of any input by the user that has “tor” anywhere in it.

Task 2: Internet Explorer user activity:

The Index.dat File

Internet Explorer saves numerous files named “index.dat” within each user’s home directory on the computer system. Each user will generate multiple Index.dat files that may be found in multiple directories as indicated below. This file maps web sites visited to locally saved cache files in randomly named directories so that the next time the user visits the same web site, he will not have to download the same graphics and web pages all over again.

The following table lists additional areas of the file system where other index.dat files may be located for Internet Explorer running on different versions of Windows:

OperatingSystem File Path(s)

Windows 95/98/Me \Windows\Temporary Internet Files\Content.IE5\

\Windows\Cookies\ \Windows\History\History.IE5\

Windows NT \Winnt\Profiles\<username>\Local Settings\Temporary Internet Files\Content.IE5\

\Winnt\Profiles\<username>\Cookies\

\Winnt\Profiles\<username>\Local Settings\History\History.IE5\

Windows 2K/XP \Documents and Settings\<username>\Local Settings\Temporary Internet Files\Content.IE5\

\Documents and Settings\<username>\Cookies\ \Document and Settings\<username>\Local Settings\History\History.IE5\

C:\WINDOWS\system32\config\systemprofile\LocalSettings\History\History.IE5

Table 1 - Locations of Index.dat Files

Index.dat File Structure

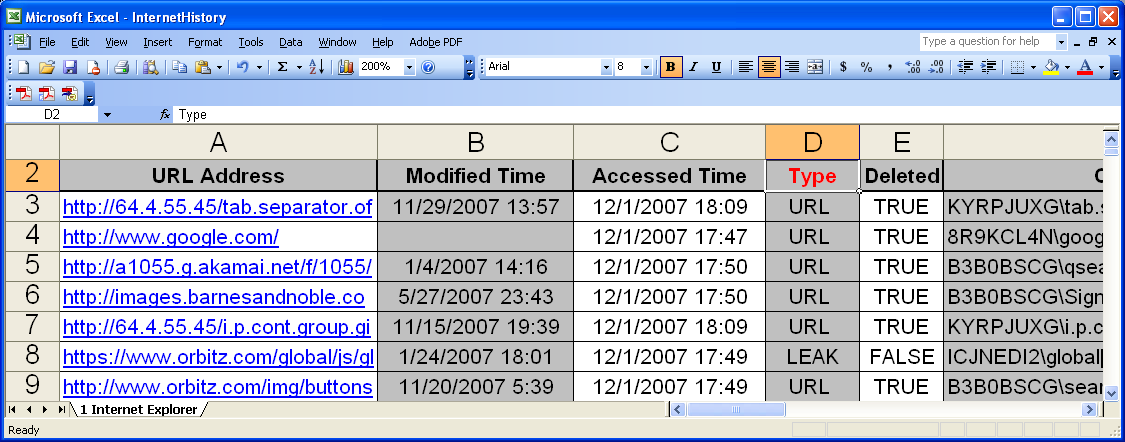
A forensic investigator may use the information found in the index.dat file to retrace the web activity of a suspect. The structures identified during forensic analysis of Index.dat that are relevant to constructing internet activity include the following types of Internet Explorer activity records:

• REDR – The REDR type of activity record indicates when the subject’s browser was redirected to another site.

• URL – The URL activity record is a set of data that represents a URL, or website, a user visited.

• LEAK - The LEAK activity record also indicates the website that the user visited.

Examples of these are show in the figure below:



Pasco index.dat > index.xlsx

The above command is used to parse index.dat file using pasco tool and store the information in index.xlsx. These index.dat data types represent the most relevant information for analyzing a suspect’s web usage. These will be used to reconstruct suspects browsing habits.

Task 3: Internet Explorer Cookies

A cookie is a small file containing data that the web server places on a user’s computer so it may request back at a later date. During forensic analysis it is often relevant to parse the information in Internet Explorer’s cookie files into a human readable format. Cookies aid forensic analysts during the investigation by providing insight to a suspect’s internet activity.

But why are cookies necessary for browsing the internet? Cookies are necessary because HTTP is a stateless protocol therefore websites must place information on a user’s computer if it needs to save information about a web session. For instance, whenever a person purchases a book from amazon.com and adds it to his shopping cart, the information can be saved on the clients computer.

Structure of an Internet Explorer Cookie File

After visiting a website such as http://www.arstechnica.com, a cookie will be generated on the user’s computer that resembles the following:

atechnica

home

arstechnica.com/

0

1238799232

29570658

1484443312

29552553

\*

Contents of an Internet Explorer Cookie

This cookie contains the information meant to be saved on the client’s machine from the web server, the domain name that is responsible for this cookie, and the relevant time/date stamps. The file will be created in the user’s IE Cookie directory, typically located in the following places:

Operating System Cookie File Location

Windows 2000/XP C:\Documents and Settings\<username>\Cookies

Since the file is in ASCII format, it is easy to analyze the function of each line in the file.

• The first line contains the variable name. In this case, the variable is named atechnica.

• The second line contains the value for the variable. In this example, the variable atechnica has the value of home.

• The third line contains the website that issued the cookie.

• The fourth line contains flags, which are zero in this case.

• The next two lines (lines five and six) contain the expiration time for the cookie.

• The next two lines (lines 7 and 8) are the creation time for the cookie.

• The last line (line 9) will always contain a \* since it is the record delimiter when this text file contains more than one cookie. A new cookie would start on the next line (line 10)

Using Galleta

The commands for using Galleta are also relatively simple:

galleta administrator@arstechnica.txt > arstechnica\_galleta.txt

parses the cookie [administrator@arstechnica.txt](mailto:administrator@arstechnica.txt) and stores the information in the file arstechnica\_galleta.txt.

Task 4 : Parse Firefox cache

Firefox Cache Location

The Firefox cache contains both metadata (information about the various cache entries) and data (the cached items themselves) which can be of immense forensic importance. Cache files are located as follows in Windows 7 and 8:

• C:\Users\[User]\AppData\Local\Mozilla\Firefox\Profiles\xxxxxxxx.default\Cache

• C:\Users\[User]\AppData\Local\Mozilla\Firefox\Profiles\xxxxxxxx.default\jumplistCache

• C:\Users\[User]\AppData\Local\Mozilla\Firefox\Profiles\xxxxxxxx.default\OfflineCache

• C:\Users\[User]\AppData\Local\Mozilla\Firefox\Profiles\xxxxxxxx.default\startupCache

Which innovative new product has been a game-changer this year? Tell us & win! Learn More

In the C:\Users\[User]\AppData\Local\Mozilla\Firefox\Profiles\xxxxxxxx.default\Cache directory there are four primary internal files:

• \_CACHE\_001\_ - stores small metadata and data entries in 512-byte blocks.

• \_CACHE\_002\_ - stores medium-sized metadata and data items in 1024-byte blocks.

• \_CACHE\_003\_ - stores large metadata and data items in 4096-byte blocks.

• \_CACHE\_MAP\_ - contains the index to both the metadata and the data and links them together. A working copy is stored in memory when Firefox is running while the other cache files are continuously updated during Web browsing.

Additionally, there may be any number of external directories/files which are used to store very large metadata items or data.

Viewing the Firefox Cache

Firefox has a built-in feature which allows direct viewing access to cache files. With the Firefox browser running, entering “about:cache” into the address field and pressing the Enter key on the keyboard will load the “Information about the Cache Service” screen. Information concerning the memory cache device, disk cache device, and offline cache device will be displayed and appear as follows:

• Memory cache device

Number of entries

Maximum storage size

Storage in use

Inactive storage

List Cache Entries

• Disk cache device

Number of entries

Maximum storage size

Storage in use

Cache directory

List Cache Entries

• Offline cache device

Number of entries

Maximum storage size

Storage in use

Cache directory

Both “List Cache Entries” are hyperlinks. Clicking on either one will cause the cached files or objects to be displayed along with their original link location URLs. For instance, clicking on the link under “memory cache device” will display information regarding the key, data size, fetch count, last modified, and expires that is stored in memory. The information is searchable. Clicking on any of the entries will display the “Cache entry information” screen for that entry and provide a wealth of potential forensic information such as:

Key - the URL.

Fetch count – number of times accessed.

Last fetched – yyyy-mm-dd-hh:mm:ss.

Last modified – yyyy-mm-dd-hh:mm:ss.

Expires – yyyy-mm-dd-hh:mm:ss.

Data size – size of the file.

File on disk – none.

Security - document does not have any security information associated with it.

Client – HTTP.

Request method – GET (may or may not be present)

Response head – HTTP, server information, etc. (may or may not be present).

Charset - (may or may not be present).

Charset source - (may or may not be present).

Likewise, clicking on the link under “Disk cache device” and clicking on any of its entries will provide similar information. Clicking on one of the key entries should open the URL or provide other pertinent information. Note that the “File on disk” may point to the directory where it is stored on the hard drive!