

Práctica 4

Evidencias de los navegadores web

Jose Almirón López

8 de Marzo del 2024



Tabla de contenidos

Introducción	3
Internet Explorer y Microsoft Edge	4
Cache	5
Cookies	6
Historial de ficheros descargados	6
Historial de navegación	6
Mozilla Firefox	7
Historial de navegación	7
Historial de ficheros descargados	10
Cookies	10
Cache	11
Google Chrome	11
Historial de navegación	11
Historial de ficheros descargados	13
Cache	14
Cookies	15

Introducción

En esta práctica, analizaremos las evidencias de los navegadores más comunes, como Microsoft Edge, Firefox y Google Chrome. Investigaremos las ubicaciones donde se almacenan las evidencias de cada uno, utilizando herramientas como SQLite Studio y varias herramientas de Nirsoft. El primer paso consistirá en extraer las evidencias mediante FTK Imager.

- **%userprofile%\Appdata\Local\Microsoft**
- **%userprofile%\Appdata\Roaming\Mozilla**
- **%userprofile%\AppData\Local\Google**

Como se puede apreciar, todas las evidencias están localizadas en el perfil del usuario. En consecuencia, he creado una imagen del perfil de usuario de la víctima.

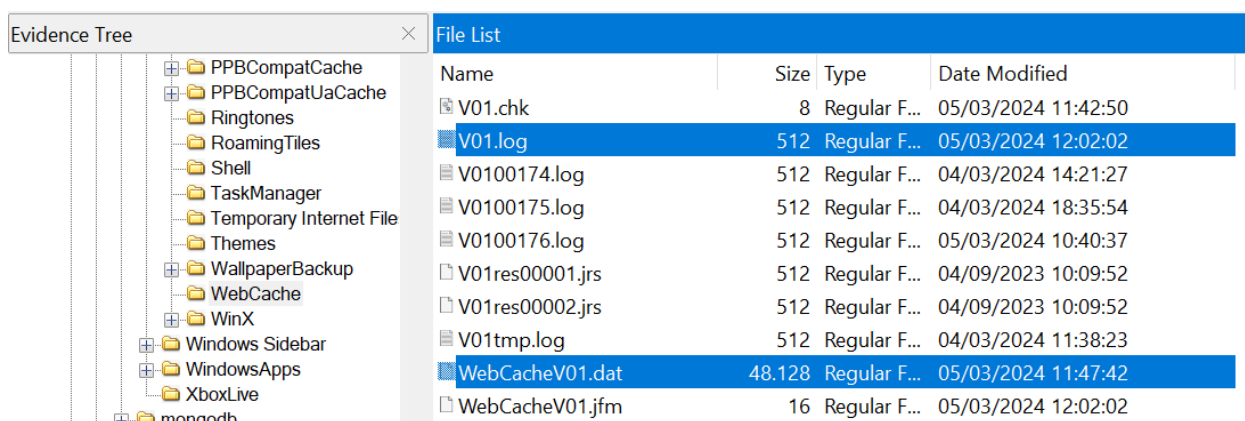
Forense > practica 4.4		Buscar en practica 4.4		
	Nombre	Fecha de modificación	Tipo	Tamaño
✚	win-10-profile.ad1	08/03/2024 13:54	Archivo AD1	1.536.000 KB
✚	win-10-profile.ad1	08/03/2024 15:14	Archivo de origen Diff	256 KB
✚	win-10-profile.ad1	08/03/2024 14:02	Documento de texto	20 KB
✚	win-10-profile.ad2	08/03/2024 13:55	Archivo AD2	1.536.000 KB
✚	win-10-profile.ad3	08/03/2024 13:55	Archivo AD3	1.536.000 KB
✚	win-10-profile.ad4	08/03/2024 13:55	Archivo AD4	1.536.000 KB
✚	win-10-profile.ad5	08/03/2024 13:55	Archivo AD5	1.536.000 KB
✚	win-10-profile.ad6	08/03/2024 13:55	Archivo AD6	125.498 KB

Una vez obtenidas las evidencias, emplearemos FTK Imager para montar las evidencias que necesitaremos analizar en cada caso.

Internet Explorer y Microsoft Edge

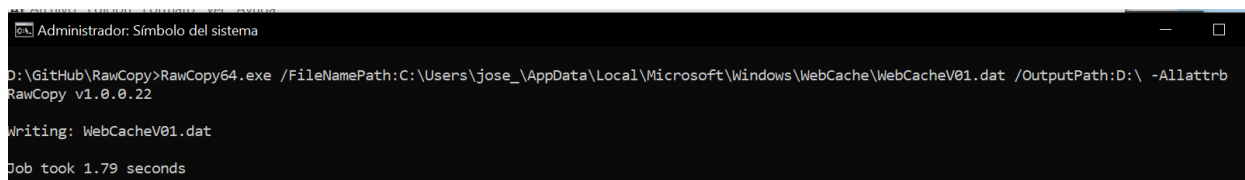
Internet Explorer es uno de los navegadores más conocidos, especialmente por su inclusión predeterminada en los sistemas operativos Windows. Aunque en Windows 10 fue reemplazado por Microsoft Edge, comparte la misma estructura. Internet Explorer presenta la peculiaridad de almacenar los datos y los metadatos de forma separada. Es crucial distinguir entre los metadatos y los datos, ya que los primeros proporcionan la información necesaria para localizar los datos reales. Estos metadatos se encuentran en:

%userprofile%\Appdata\Local\Microsoft\Windows\WebCache\WebcacheVx.dat



Name	Size	Type	Date Modified
V01.chk	8	Regular F...	05/03/2024 11:42:50
V01.log	512	Regular F...	05/03/2024 12:02:02
V0100174.log	512	Regular F...	04/03/2024 14:21:27
V0100175.log	512	Regular F...	04/03/2024 18:35:54
V0100176.log	512	Regular F...	05/03/2024 10:40:37
V01res00001.jrs	512	Regular F...	04/09/2023 10:09:52
V01res00002.jrs	512	Regular F...	04/09/2023 10:09:52
V01tmp.log	512	Regular F...	04/03/2024 11:38:23
WebCacheV01.dat	48.128	Regular F...	05/03/2024 11:47:42
WebCacheV01.jfm	16	Regular F...	05/03/2024 12:02:02

Necesitamos adquirir el archivo **WebCacheV01.dat**. Podemos intentar exportar el directorio **WebCache** desde FTK Imager, pero en mi caso, Windows bloquea por defecto estos archivos. Si esta opción no resulta, podemos emplear la herramienta [RawCopy](#) para obtener una copia del archivo y así poder trabajar con él.



```
D:\GitHub\RawCopy>RawCopy64.exe /FileNamePath:C:\Users\jose\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat /OutputPath:D:\ -Allattrb
RawCopy v1.0.0.22

Writing: WebCacheV01.dat

Job took 1.79 seconds
```

Una vez obtenido el fichero **WebCacheV01.dat**, podemos utilizar la herramienta [ESEDatabaseView](#) para identificar las rutas donde se encuentran los artefactos que buscamos.

ESEDatabaseView: D:\VirtualBox VMs\Carpeta-Compartida\Forens\practica 4.4\WebCacheV01.dat

File Edit View Options Help

Containers [Table ID = 9, 14 Columns]

C...	Setid	Flags	Size	Limit	Last...	E...	LastAccessTime	Name	PartitionId	Directory
1	0	79	21443	346030080	0	0	133543730717427317	Content	M	C:\Users\jose\AppData\Local\Microsoft\Windows\NetCache\IE\
2	0	68	0	1024	0	0	133543731922475965	History	M	C:\Users\jose\AppData\Local\Microsoft\Windows\History\History.IE5\
3	1	15	0	52428800	0	0	133543756586129565	Content	S-1-15-2...	C:\Users\jose\AppData\Local\Packages\microsoft.windows.contentdeliverymanager_cw5n1h2tyewy\AC\NetCache\
4	1	15	1295911	52428800	0	0	133543791260577652	Content	S-1-15-2...	C:\Users\jose\AppData\Local\Packages\microsoft.windows.search_cw5n1h2tyewy\AC\NetCache\
5	1	1	26	1024000	0	0	133543928070164276	DOMStore	S-1-15-2...	C:\Users\jose\AppData\Local\Packages\microsoft.windows.search_cw5n1h2tyewy\AC\Microsoft\Internet Explorer\DOMStore\
6	1	0	0	1024	0	0	133542866299840654	Backgroun...	S-1-15-2...	C:\Users\jose\AppData\Local\Packages\microsoft.windows.contentdeliverymanager_cw5n1h2tyewy\AC\NetHistory\BackgroundTr
7	1	0	0	1024	0	0	133542867296304043	Backgroun...	S-1-15-2...	C:\Users\jose\AppData\Local\Packages\microsoft.windows.search_cw5n1h2tyewy\AC\NetHistory\BackgroundTransferApi\
8	1	0	0	1024	0	0	133542867301173287	Backgroun...	S-1-15-2...	C:\Users\jose\AppData\Local\Packages\microsoft.windows.search_cw5n1h2tyewy\AC\NetHistory\BackgroundTransferApiGroup\
9	0	64	0	1024	0	0	133543942424174824	MSHist012...	M	C:\Users\jose\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012024030720240308\
10	1	15	2812390	52428800	0	0	133543965685212895	Content	S-1-15-2...	C:\Users\jose\AppData\Local\Packages\microsoft.windowsstore_8wekyb3d8bbwe\AC\NetCache\
11	1	0	0	1024	0	0	133542869976432069	Backgroun...	S-1-15-2...	C:\Users\jose\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\AC\NetHistory\BackgroundTr
12	1	15	0	52428800	0	0	133542870032410164	Content	S-1-15-2...	C:\Users\jose\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\AC\NetCache\
13	1	15	2373224	52428800	0	0	133543928112029396	Content	S-1-15-2...	C:\Users\jose\AppData\Local\Packages\microsoft.windows.cloudexperiencehost_cw5n1h2tyewy\AC\NetCache\
14	1	1	13	1024000	0	0	133543928112498040	DOMStore	S-1-15-2...	C:\Users\jose\AppData\Local\Packages\microsoft.windows.cloudexperiencehost_cw5n1h2tyewy\AC\Microsoft\Internet Explorer\D
15	1	0	0	1024	0	0	133543928122027025	Cookies	S-1-15-2...	C:\Users\jose\AppData\Local\Packages\microsoft.windows.cloudexperiencehost_cw5n1h2tyewy\AC\NetCookies\
31	1	15	0	52428800	0	0	133543971572684388	Content	S-1-15-2...	C:\Users\jose\AppData\Local\Packages\microsoft.windows.client.cbs_cw5n1h2tyewy\AC\NetCache\
32	1	79	0	346030080	0	0	133543044447322181	Content	S-1-15-2...	C:\Users\jose\AppData\Local\Packages\microsoft.officehub_8wekyb3d8bbwe\AC\NetCache\
33	1	1	13	1024000	0	0	133543044451747426	DOMStore	S-1-15-2...	C:\Users\jose\AppData\Local\Packages\microsoft.officehub_8wekyb3d8bbwe\AC\Microsoft\Internet Explorer\DOMStore\
35	0	112	0	1024	0	0	133543122224098975	iecompat	M	C:\Users\jose\AppData\Local\Microsoft\Windows\IECompatCache\
36	0	112	0	1024	0	0	133543122224098975	iecompatua	M	C:\Users\jose\AppData\Local\Microsoft\Windows\IECompatUaCache\
37	0	113	0	1024	0	0	133543122224411585	DNTExcepti...	M	C:\Users\jose\AppData\Local\Microsoft\Windows\NetCookies\DNTException\
45	0	64	0	1024	0	0	133543613825026821	MSHist012...	M	C:\Users\jose\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012024030820240309\

Este procedimiento debe ser seguido cada vez que llevemos a cabo un análisis forense de este navegador, ya que nos permitirá obtener las rutas de los datos.

Cache

La caché es el espacio donde los componentes de una página web se almacenan localmente para acelerar las visitas posteriores, podemos encontrarla en:

C:\Users\jose\AppData\Local\Packages\microsoft.windows.contentdeliverymanager_cw5n1h2tyewy\AC\NetCache\ -> Container 3

C:\Users\jose\AppData\Local\Packages\microsoft.windowsstore_8wekyb3d8bbwe\AC\NetCache\ -> Container 10

C:\Users\jose\AppData\Local\Packages\microsoft.windows.cloudexperiencehost_cw5n1h2tyewy\AC\NetCache\ -> Container 31

Podemos emplear el programa [IECacheView](#); para ello, seleccionamos 'File > Select Cache Folder' para indicar el directorio que contiene **WebCacheV01.dat**.

IECacheView: D:\VirtualBox VMs\Carpeta-Compartida\Forens\practica 4.4

File Edit View Options Help

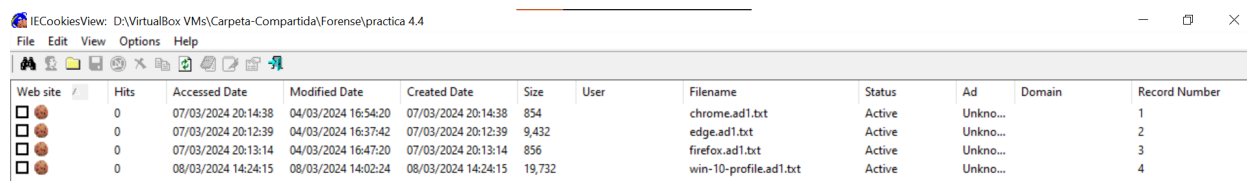
Filename	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hits	File Size	Subfolder Name
2RFgnacs6nPw...		https://r.bing.com/rs/7b/t5/jnc,nj/2RFgnacs6nP...	08/03/2024 19:35:59	08/03/2024 3:30:50	13/03/2024 13:18:28	N/A	2	308	SGDHIUD1
5S4e_l2wpLofAs...	text/javascript; ch...	https://www.bing.com/rp/5S4e_l2wpLofAsoMy4...	08/03/2024 19:35:59	17/08/2022 7:14:01	13/03/2024 19:35:59	N/A	2	1.203	EDLOOK14
7gjhvoh0czA9HP...		https://r.bing.com/rb/5u/jnc,nj/7gjhvoh0czA9HP...	08/03/2024 18:33:27	07/03/2024 21:46:45	13/03/2024 4:10:57	N/A	1	58.366	EDLOOK14
AppFramework...	text/javascript; ch...	https://sdx.microsoft.com/bundles/scripts/AppF...	08/03/2024 18:33:35	19/10/2023 12:20:27	18/10/2024 12:20:27	N/A	2	14.353	UXRJZBW6
apps.11608.1425...	image/png	https://sdx.microsoft.com/bundles/scripts/AppF...	08/03/2024 18:33:35	24/05/2023 20:50:31	23/05/2024 20:50:31	N/A	1	2.631	2HFC19ZX
apps.1277.14431...	image/jpeg	https://store-images.s-microsoft.com/image/ap...	08/03/2024 19:36:10	06/07/2021 21:07:00	06/06/2024 20:36:10	N/A	1	12.920	CW2T17FM
apps.13199.1351...	image/png	https://store-images.s-microsoft.com/image/ap...	08/03/2024 19:36:13	16/01/2020 12:08:19	06/06/2024 20:36:13	N/A	1	70.583	1EVPU9AS
apps.13320.1462...	image/jpeg	https://store-images.s-microsoft.com/image/ap...	08/03/2024 19:36:14	04/05/2016 12:20:18	06/06/2024 20:36:14	N/A	1	12.880	QLVP2VOS
		https://store-images.s-microsoft.com/image/ap...	08/03/2024 19:36:13	07/02/2020 21:04:31	06/06/2024 20:36:13	N/A	1	45.050	QLVP2VOS

Cookies

De la base de datos WebCacheV01.dat, podemos extraer la siguiente ruta que indica la ubicación de las cookies:

C:\Users\jose_\AppData\Local\Packages\microsoft.windows.cloudexperiencehost_cw5n1h2txyewy\AC\INETCookies\ -> Container 15

La herramienta que emplearemos para visualizarlas es [IECookiesViewer](#) de Nirsoft. Para hacerlo, debemos indicarle la ubicación del directorio que hemos extraído previamente mediante '**File > Select Cookies Folder**'.



IECookiesViewer: D:\VirtualBox VMs\Carpeta-Compartida\Forens\practica 4.4

Web site	Hits	Accessed Date	Modified Date	Created Date	Size	User	Filename	Status	Ad	Domain	Record Number
	0	07/03/2024 20:14:38	04/03/2024 16:54:20	07/03/2024 20:14:38	854		chrome.ad1.txt	Active		Unkno...	1
	0	07/03/2024 20:12:39	04/03/2024 16:37:42	07/03/2024 20:12:39	9,432		edge.ad1.txt	Active		Unkno...	2
	0	07/03/2024 20:13:14	04/03/2024 16:47:20	07/03/2024 20:13:14	856		firefox.ad1.txt	Active		Unkno...	3
	0	08/03/2024 14:24:15	08/03/2024 14:02:24	08/03/2024 14:24:15	19,732		win-10-profile.ad1.txt	Active		Unkno...	4

Historial de ficheros descargados

Tras examinar la base de datos ESE **WebcacheV01.dat**, no se han registrado descargas en este navegador. Sin embargo, en el caso de Microsoft Edge, la ruta potencial podría ser la siguiente:

%userprofile%\AppData\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\DownloadHistory

En versiones anteriores de Internet Explorer, una ruta posible para este caso podría ser:

%userprofile%\Appdata\Roaming\Microsoft\Windows\IEDownloadHistory -> Container 21

Historial de navegación

Analizando el WebcacheV01.dat podemos obtener las rutas de los historiales de navegación:

C:\Users\jose_\AppData\Local\Microsoft\Windows\History\History.IE5\ -> Container 2

C:\Users\jose_\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012024030720240308\ -> Container 9

C:\Users\jose_\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012024030820240309\ -> Container 45

Podemos emplear la aplicación [BrowsingHistoryView](#) de Nirsoft para analizar directamente la base de datos. Para ello, primero, seleccionamos '**Options > Advanced Options**'.

BrowsingHistoryView

File Edit View Options Help

URL	Visit Time	Visit Count	Visited From	Visit Type	Web Browser	User Profile
file:///C:/Users/jose_/Downloads/disco1.dd	08/03/2024 18:40:31	2			Internet Explorer 10/11 / ...	jose_
file:///C:/Users/jose_/Downloads/disco2.dd	08/03/2024 18:38:30	2			Internet Explorer 10/11 / ...	jose_
file:///C:/Users/jose_/Downloads/Five86-1/Five86-1.o...	07/03/2024 19:00:33	1			Internet Explorer 10/11 / ...	jose_
file:///C:/Users/jose_/Downloads/Practica%202_2%20Ataque%...	07/03/2024 18:59:24	1			Internet Explorer 10/11 / ...	jose_
file:///C:/Users/jose_/Downloads/q4os.ova	07/03/2024 18:53:36	1			Internet Explorer 10/11 / ...	jose_
file:///C:/Users/jose_/Downloads/windows-11-morado-abstrac...	07/03/2024 13:32:23	1			Internet Explorer 10/11 / ...	jose_
file:///C:/Users/jose_/OneDrive/Escritorio/Mozilla	08/03/2024 12:41:41	1			Internet Explorer 10/11 / ...	jose_
file:///C:/Users/jose_/OneDrive/Imágenes/Wallpapers/astronau...	07/03/2024 13:34:09	1			Internet Explorer 10/11 / ...	jose_
file:///C:/Users/jose_/OneDrive/Imágenes/Wallpapers/espacio-...	07/03/2024 16:03:54	1			Internet Explorer 10/11 / ...	jose_
file:///D:/	07/03/2024 20:03:04	7			Internet Explorer 10/11 / ...	jose_
file:///D:/Archivos%20de%20programa	07/03/2024 13:07:48	1			Internet Explorer 10/11 / ...	jose_
file:///D:/Edge.001	07/03/2024 20:47:08	1			Internet Explorer 10/11 / ...	jose_
file:///D:/Evansa	07/03/2024 20:03:04	1			Internet Explorer 10/11 / ...	jose_

Mozilla Firefox

Firefox es un navegador web de código abierto que puede ejecutarse en diversas plataformas, como Windows, Linux y MacOSX.

El directorio donde se almacena toda la información a nivel Forense del navegador Firefox:

%userprofile%\Appdata\Roaming\Mozilla\Firefox\Profiles\<random>.default

Historial de navegación

La información se almacena en la base de datos en formato SQLite llamada **places.sqlite**. Para acceder a ella, simplemente abre [SQLite Studio](#), haz clic en '**Databases > Add Database**' y selecciona el archivo. En la tabla **moz_places** se encuentra el historial de navegación, y puedes ejecutar una consulta de la siguiente manera para obtener todo el historial:

```
select datetime(last_visit_date/1000000,'unixepoch') as
visit_date, url, title, visit_count, visit_type FROM
moz_places,moz_historyvisits
WHERE moz_places.id = moz_historyvisits.place_id
```

Vista de rejilla Vista de formulario

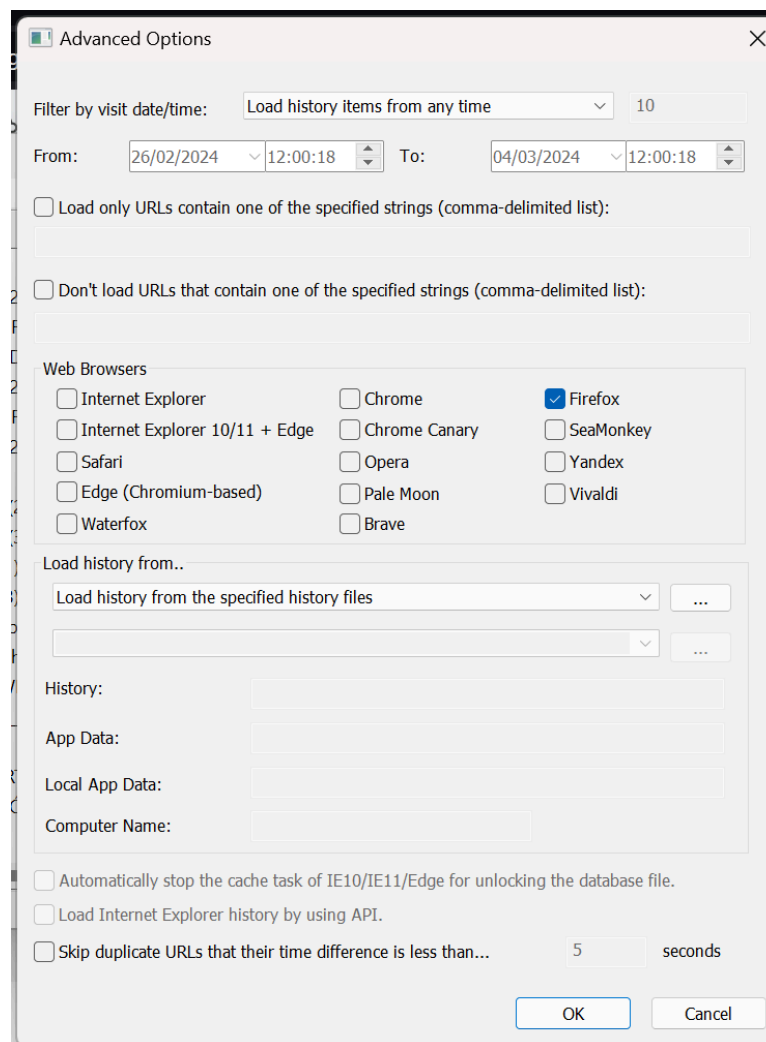
Total rows loaded: 127866

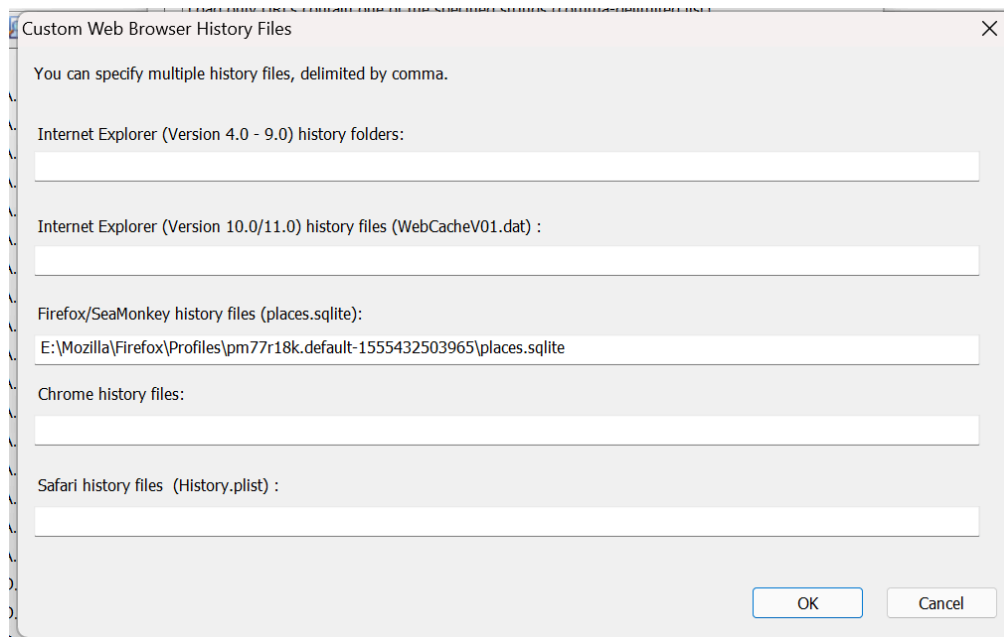
	visit_date	url	title	visit_count	visit_type
1	2017-06-11 10:07:20	http://aka.ms/wimup.	NULL	1	2
2	2018-04-13 08:41:24	https://www.google.com/	Google	130	2
3	2018-04-13 08:41:24	https://www.google.com/	Google	130	1
4	2018-04-13 08:41:24	https://www.google.com/	Google	130	1
5	2018-04-13 08:41:24	https://www.google.com/	Google	130	1
6	2018-04-13 08:41:24	https://www.google.com/	Google	130	1
7	2018-04-13 08:41:24	https://www.google.com/	Google	130	1
8	2018-04-13 08:41:24	https://www.google.com/	Google	130	1
9	2018-04-13 08:41:24	https://www.google.com/	Google	130	1
10	2018-04-13 08:41:24	https://www.google.com/	Google	130	1
11	2018-04-13 08:41:24	https://www.google.com/	Google	130	1

El tipo de visita lo podemos identificar de la siguiente manera:

- **1:** el usuario siguió un link
- **2:** el usuario escribió la url
- **3:** el usuario utilizó un favorito
- **4:** fue cargado desde un iframe
- **5:** página accedida debido a HTTP redirect 301
- **6:** página accedida debido a HTTP redirect 302
- **7:** Fichero descargado
- **8:** el usuario siguió un link de un iframe

También podemos utilizar la herramienta de Nirsoft [Browsing History View](#).





URL	Title	Visit Time	Visit Count	Visited From	Visit Type	Visit
file:///C:/Users/Jose/A...	IMG-20190327-WA0004[...	27/03/2019 14:57:01	1		Link	
file:///C:/Users/Jose/A...	PREGUNTAS FRECUENTE...	05/02/2020 13:13:48	1		Link	
file:///C:/Users/Jose/A...	adj-Res_Def_Destinos_Ad...	27/01/2020 14:33:35	1		Link	
file:///C:/Users/Jose/A...	IMG-20190327-WA0005[...	27/03/2019 14:56:41	1		Link	
file:///C:/Users/Jose/A...	PREGUNTAS FRECUENTE...	27/01/2020 14:34:25	1		Link	
file:///C:/Users/Jose/A...	IMG-20190327-WA0006[...	27/03/2019 14:46:52	1		Link	
file:///C:/Users/Jose/A...	1.PDF	09/04/2018 20:33:07	1		Link	
file:///C:/Users/Jose/A...	DNI delante (2).pdf	01/07/2018 20:16:30	1		Link	
file:///C:/Users/Jose/A...	DNI delante (3).pdf	01/07/2018 20:16:45	1		Link	
file:///C:/Users/Jose/A...	DNI detras (1).pdf	01/07/2018 20:15:26	1		Link	
file:///C:/Users/Jose/A...	DNI detras (3).pdf	01/07/2018 20:19:47	1		Link	
file:///C:/Users/Jose/A...	Documento.pdf	07/05/2018 13:52:36	1		Link	
file:///C:/Users/Jose/A...	Anuel AA - China (Letra_L...	10/01/2020 10:34:07	1		Link	
file:///C:/Users/Jose/A...	6-087 - C_WEB_SOS_PD...	22/02/2020 12:25:31	1		Link	
file:///C:/Users/Jose/A...	C_WEB_SOS_PDFS_Bene...	22/02/2020 12:26:05	1		Link	
file:///C:/Users/Jose/A...	Diapositiva 1 - C_WEB_S...	22/02/2020 12:25:45	1		Link	
file:///C:/Users/Jose/A...	MULTIDEPORTE.pdf	11/02/2019 13:44:07	1		Link	
file:///C:/Users/Jose/D...	AUTORIZACIÓN INCLUSI...	10/09/2019 11:00:53	1		Link	
file:///C:/Users/Jose/D...	2.pdf	10/09/2019 11:04:53	1		Link	

127866 item(s)

NirSoft Freeware. <https://www.nirsoft.net>

Page 10 of 10

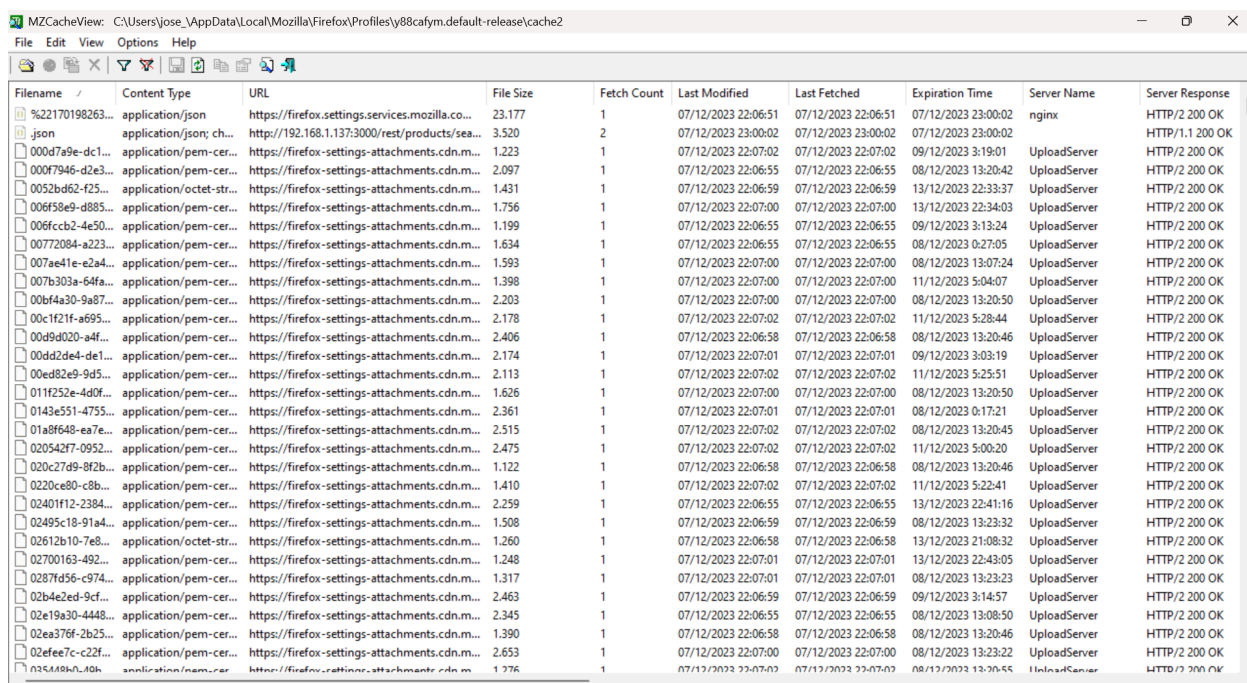
Fecha_Descarga		Fichero	URL
16	2017-09-07 10:47:18	file:///C:/Users/Jose/...	file:///D:/CARTA%20DE%20PAGO.pdf
17	2017-09-16 18:52:52	UTF-8	http://www.flvto.biz/es/downloads/mp3/yt_72U00v5ESUo/
18	2017-09-16 18:53:24	UTF-8	http://www.flvto.biz/es/
19	2017-09-23 18:40:01	UTF-8	https://www.airbnb.es/s/Vera--Espa%C3%B1a/homes?...
20	2017-10-15 10:02:51	file:///C:/Users/Jose/...	file:///C:/Users/Jose/Downloads/PR%C3%81CTICA%202.pdf
21	2017-10-15 10:04:13	file:///C:/Users/Jose/...	file:///C:/Users/Jose/Downloads/PR%C3%81CTICA%203.pdf
22	2017-12-10 20:10:16	file:///C:/Users/Jose/...	http://sitcadigital.com/tramitacion/PRESTACIONES%20DESEMPLEADOS/Declaracion_rentas_mayores_52.pdf
23	2017-12-10 20:10:17	{"state":1,"endTime":...	http://sitcadigital.com/tramitacion/PRESTACIONES%20DESEMPLEADOS/Declaracion_rentas_mayores_52.pdf
24	2018-01-08 07:45:02	file:///C:/Users/Jose/...	file:///C:/Users/Jose/Downloads/Declaracion_rentas_mayores_52.pdf
25	2018-01-08 07:45:02	{"state":1,"endTime":...	file:///C:/Users/Jose/Downloads/Declaracion_rentas_mayores_52.pdf
26	2018-03-17 20:00:35	UTF-8	https://www.bankia.es/oficina/particulares/#/posicion-global
27	2018-03-17 20:02:13	UTF-8	https://www.bankia.es/es/particulares
28	2018-07-17 15:53:12	UTF-8	https://clave-dninbrt.seg-social.gob.es/rss-gateway/AuthByLevelFormGateWayServlet?...
29	2018-07-25 15:28:55	UTF-8	https://clave-dninbrt.seg-social.gob.es/rss-gateway/AuthByLevelFormGateWayServlet?...

Cache

La caché se localiza en el directorio:

%userprofile%\Appdata\Local\Mozilla\Firefox\Profiles\default\Cache2

Para acceder a los archivos de la caché, utilizaremos la herramienta [MozillaCacheView](#). Abre la aplicación y selecciona la carpeta "**Cache2**" del perfil mediante la opción "**File > Select Cache Folder**".



The screenshot shows the MozillaCacheView application window. The title bar reads "MZCacheView: C:\Users\jose\AppData\Local\Mozilla\Firefox\Profiles\y88cafym.default-release\cache2". The menu bar includes "File", "Edit", "View", "Options", and "Help". The toolbar contains icons for file operations. The main window displays a table of cached files with the following columns: Filename, Content Type, URL, File Size, Fetch Count, Last Modified, Last Fetched, Expiration Time, Server Name, and Server Response. The table lists numerous files, mostly of type "application/json" or "application/pem-certificate", with URLs pointing to various services like mozilla.co and cdn.mozilla.org. The server response for all entries is "HTTP/2 200 OK".

Filename	Content Type	URL	File Size	Fetch Count	Last Modified	Last Fetched	Expiration Time	Server Name	Server Response
%2170198263...	application/json	https://firefox.settings.services.mozilla.co...	23.177	1	07/12/2023 22:06:51	07/12/2023 22:06:51	07/12/2023 23:00:02	nginx	HTTP/2 200 OK
.json	application/json; ch...	http://192.168.1.137:3000/rest/products/sea...	3.520	2	07/12/2023 23:00:02	07/12/2023 23:00:02	07/12/2023 23:00:02		HTTP/1.1 200 OK
000d7a9e-dc1...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	1.223	1	07/12/2023 22:07:02	07/12/2023 22:07:02	09/12/2023 3:19:01	UploadServer	HTTP/2 200 OK
000f7946-d2e3...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	2.097	1	07/12/2023 22:06:55	07/12/2023 22:06:55	08/12/2023 13:20:42	UploadServer	HTTP/2 200 OK
0052bd62-f25...	application/octet-str...	https://firefox-settings-attachments.cdn.m...	1.431	1	07/12/2023 22:06:59	07/12/2023 22:06:59	13/12/2023 22:33:37	UploadServer	HTTP/2 200 OK
006f58e9-d885...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	1.756	1	07/12/2023 22:07:00	07/12/2023 22:07:00	13/12/2023 22:34:03	UploadServer	HTTP/2 200 OK
006fccb2-4e50...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	1.199	1	07/12/2023 22:06:55	07/12/2023 22:06:55	09/12/2023 3:13:24	UploadServer	HTTP/2 200 OK
00772084-a223...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	1.634	1	07/12/2023 22:06:55	07/12/2023 22:06:55	08/12/2023 0:27:05	UploadServer	HTTP/2 200 OK
007ae41e-e2a4...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	1.593	1	07/12/2023 22:07:00	07/12/2023 22:07:00	08/12/2023 13:07:24	UploadServer	HTTP/2 200 OK
007b303a-64fa...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	1.398	1	07/12/2023 22:07:00	07/12/2023 22:07:00	11/12/2023 5:04:07	UploadServer	HTTP/2 200 OK
00bf4a30-9a87...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	2.203	1	07/12/2023 22:07:00	07/12/2023 22:07:00	08/12/2023 13:20:50	UploadServer	HTTP/2 200 OK
00cf12f1-a695...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	2.178	1	07/12/2023 22:07:02	07/12/2023 22:07:02	11/12/2023 5:28:44	UploadServer	HTTP/2 200 OK
00d9d020-a4f...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	2.406	1	07/12/2023 22:06:58	07/12/2023 22:06:58	08/12/2023 13:20:46	UploadServer	HTTP/2 200 OK
00dd2de4-de1...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	2.174	1	07/12/2023 22:07:01	07/12/2023 22:07:01	09/12/2023 3:03:19	UploadServer	HTTP/2 200 OK
00ed82e9-9d5...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	2.113	1	07/12/2023 22:07:02	07/12/2023 22:07:02	11/12/2023 5:25:51	UploadServer	HTTP/2 200 OK
011f252e-4d0f...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	1.626	1	07/12/2023 22:07:00	07/12/2023 22:07:00	08/12/2023 13:20:50	UploadServer	HTTP/2 200 OK
0143e551-4755...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	2.361	1	07/12/2023 22:07:01	07/12/2023 22:07:01	08/12/2023 0:17:21	UploadServer	HTTP/2 200 OK
01a8f648-ea7e...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	2.515	1	07/12/2023 22:07:02	07/12/2023 22:07:02	08/12/2023 13:20:45	UploadServer	HTTP/2 200 OK
020542f7-0952...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	2.475	1	07/12/2023 22:07:02	07/12/2023 22:07:02	11/12/2023 5:00:20	UploadServer	HTTP/2 200 OK
020c27d9-8f2b...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	1.122	1	07/12/2023 22:06:58	07/12/2023 22:06:58	08/12/2023 13:20:46	UploadServer	HTTP/2 200 OK
0220ce80-c8b...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	1.410	1	07/12/2023 22:07:02	07/12/2023 22:07:02	11/12/2023 5:22:41	UploadServer	HTTP/2 200 OK
0240f1f2-2384...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	2.259	1	07/12/2023 22:06:55	07/12/2023 22:06:55	13/12/2023 22:41:16	UploadServer	HTTP/2 200 OK
02495c18-91a4...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	1.508	1	07/12/2023 22:06:59	07/12/2023 22:06:59	08/12/2023 13:23:32	UploadServer	HTTP/2 200 OK
02612b10-7e8...	application/octet-str...	https://firefox-settings-attachments.cdn.m...	1.260	1	07/12/2023 22:06:58	07/12/2023 22:06:58	13/12/2023 21:08:32	UploadServer	HTTP/2 200 OK
02700163-492...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	1.248	1	07/12/2023 22:07:01	07/12/2023 22:07:01	13/12/2023 22:43:05	UploadServer	HTTP/2 200 OK
0287fd56-c974...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	1.317	1	07/12/2023 22:07:01	07/12/2023 22:07:01	08/12/2023 13:23:23	UploadServer	HTTP/2 200 OK
02b4e2ed-9cf...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	2.463	1	07/12/2023 22:06:59	07/12/2023 22:06:59	09/12/2023 3:14:57	UploadServer	HTTP/2 200 OK
02e19a30-4448...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	2.345	1	07/12/2023 22:06:55	07/12/2023 22:06:55	08/12/2023 13:08:50	UploadServer	HTTP/2 200 OK
02ea376f-2b25...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	1.390	1	07/12/2023 22:06:58	07/12/2023 22:06:58	08/12/2023 13:20:46	UploadServer	HTTP/2 200 OK
02fee7c-c22f...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	2.653	1	07/12/2023 22:07:00	07/12/2023 22:07:00	08/12/2023 13:23:22	UploadServer	HTTP/2 200 OK
n55448b0-f0h...	application/pem-cer...	https://firefox-settings-attachments.cdn.m...	1.276	1	07/12/2023 22:07:02	07/12/2023 22:07:02	08/12/2023 13:20:55	UploadServer	HTTP/2 200 OK

Google Chrome

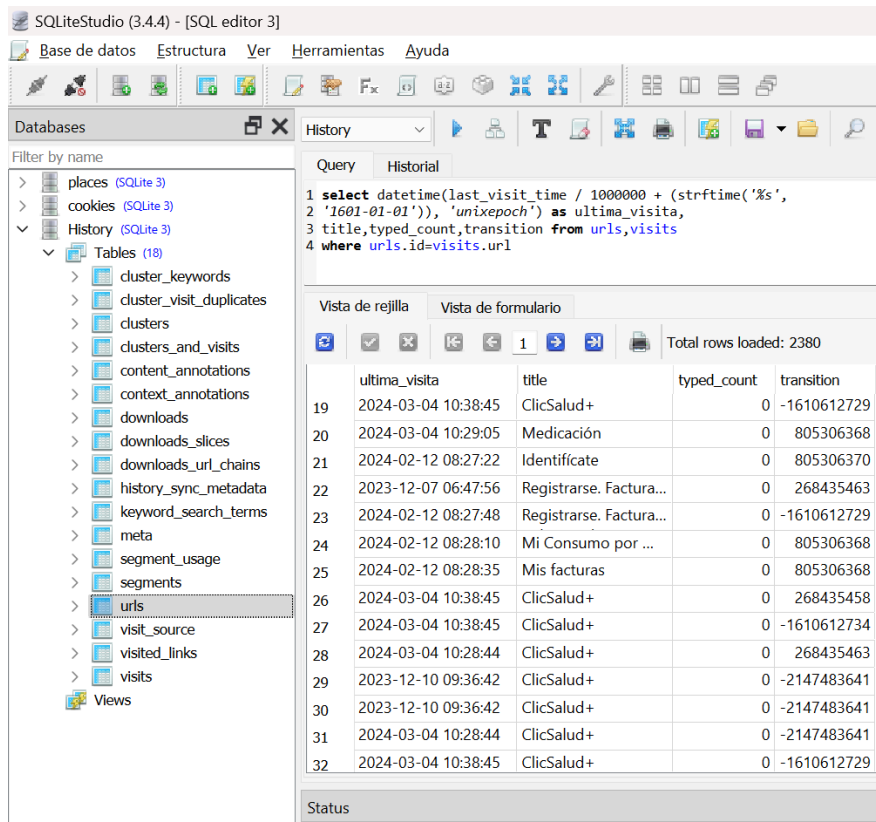
Chrome es otro navegador relevante para realizar investigaciones forenses. Al igual que Firefox, organiza su información en un perfil, pero Chrome guarda estos datos en la siguiente ruta:

%Users\<\$user>\AppData\Local\Google\Chrome\User Data\Default

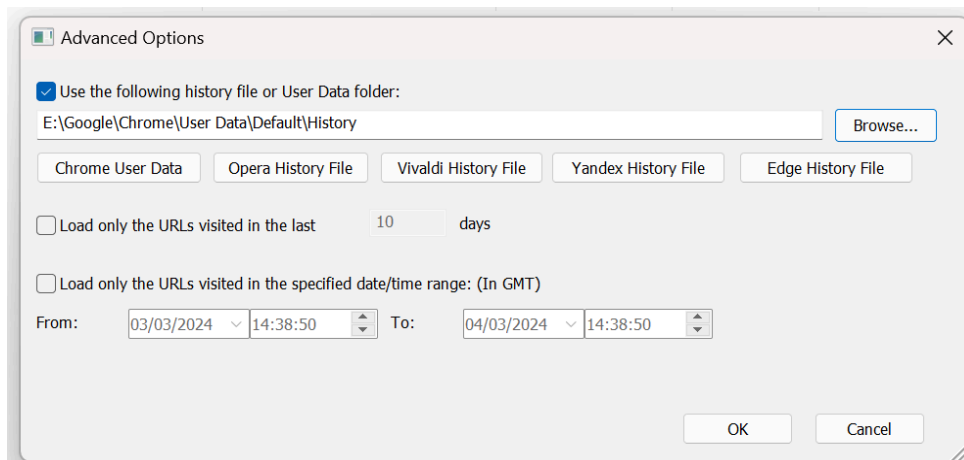
Historial de navegación

El primer paso que debemos realizar es obtener el archivo **History**, el cual se encuentra dentro del perfil mencionado anteriormente. Este archivo es una base de datos SQLite que podemos analizar con SQLite Studio. Ejecutaremos la siguiente consulta para obtener el historial:

```
select datetime(last_visit_time / 1000000 + (strftime('%s',
'1601-01-01')), 'unixepoch') as ultima_visita,
title,typed_count,transition from urls,visits
where urls.id=visits.url
```



Además, podemos emplear la herramienta [Chrome History View](#) de Nirsoft, la cual nos permite seleccionar directamente la base de datos SQLite a través de la opción '**Options > Advanced Options**'.



ChromeHistoryView - E:\Google\Chrome\User Data\Default\History

File Edit View Options Help

URL	Title	Visited On	Visit Count	Typed Count	Referrer
file:///C:/Users/Jose/Downloads/177874464_17787...	177874464_177873105_signed_82...	25/02/2024 12:18:56	1	0	
file:///C:/Users/Jose/Downloads/181816299_18181...	181816299_181814939_8245383_...	25/02/2024 12:24:59	1	0	
http://portal.lacaixa.es/low/descon_low.html	Banca online para Particulares Cai...	04/01/2024 9:11:38	1	0	
https://account.live.com/logout.aspx?chained=1&...	Iniciar sesión en la cuenta de Micro...	01/02/2024 13:39:56	1	0	https://login.live.co
https://accounts.google.com/AddSession?Email=j...	Inicia sesión: Cuentas de Google	05/02/2024 9:22:57	1	0	
https://accounts.google.com/CheckCookie?continu...	Google Account	05/02/2024 9:23:35	1	0	https://accounts.go
https://accounts.google.com/ServiceLogin?continu...	Google Account	05/02/2024 9:23:35	1	0	https://accounts.go
https://accounts.google.com/v3/signin/challenge/...	Inicia sesión: Cuentas de Google	05/02/2024 9:23:09	1	0	https://accounts.go
https://accounts.google.com/v3/signin/identifier?E...	Inicia sesión: Cuentas de Google	05/02/2024 9:22:57	1	0	https://accounts.go
https://ad.doubleclick.net/ddm/clk/540876258;349...	Alarmas Securitas Direct	06/02/2024 9:27:39	1	0	https://www.bing.c
https://apus20.cert.fnmt.es/DescargaCertificados/v...		06/02/2024 15:00:05	1	0	
https://checkout.microsoft365.com/acquire/purcha...	Finalización de la compra de Micro...	06/02/2024 9:26:34	2	0	https://go.microsof
https://checkout.microsoft365.com/acquire/purcha...	Finalización de la compra de Micro...	06/02/2024 9:26:41	2	0	https://login.live.co
https://clave-dninbrt-seg-social.gob.es/Autenticaci...	Pasarela Seguridad Social - Cl@ve ...	03/03/2024 10:21:14	1	0	https://clave-dninbr
https://clave-dninbrt-seg-social.gob.es/IPUC2/Login	Plataforma de Autenticación - Login	03/03/2024 10:21:12	1	0	https://sp.seg-socia
https://clave-dninbrt-seg-social.gob.es/rss-gateway...	Cl@ve Permanente	03/03/2024 10:21:14	1	0	https://clave-dninbr
https://clientes.mapfre.es/area-de-clientes/client-ar...	Área de clientes para Particulares y ...	01/02/2024 9:51:19	1	0	https://clientes.map
https://clientes.mapfre.es/area-de-clientes/login/pa...	Área de clientes para Particulares y ...	01/02/2024 9:50:41	1	0	
https://gds.google.com/web/chip?cardIndex=0&hl...	Cuenta de Google	05/02/2024 9:23:35	1	0	https://gds.google.

2380 item(s) NirSoft Freeware. <https://www.nirsoft.net>

Historial de ficheros descargados

Estos datos están ubicados en la misma base de datos llamada **'History'**, específicamente en la tabla **'downloads'**.

SQLiteStudio (3.4.4) - [SQL editor 4]

Base de datos Estructura Ver Herramientas Ayuda

Databases

Filter by name

- places (SQLite 3)
- cookies (SQLite 3)
- History (SQLite 3)
 - Tables (18)
 - cluster_keywords
 - cluster_visit_duplicates
 - clusters
 - clusters_and_visits
 - content_annotations
 - context_annotations
 - downloads
 - downloads_slices
 - downloads_url_chains
 - history_sync_metadata
 - keyword_search_terms
 - meta
 - segment_usage
 - segments
 - urls
 - visit_source
 - visited_links
 - visits
 - Views

Query Historial

Vista de rejilla Vista de formulario

Total rows loaded: 394

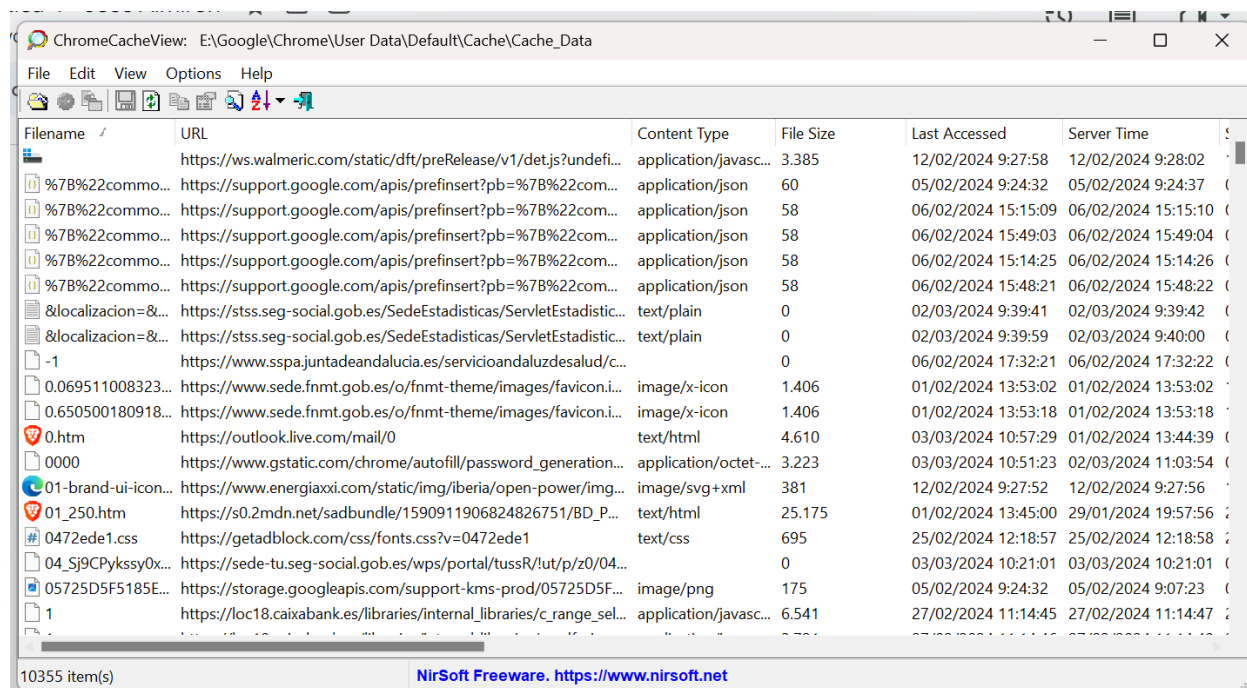
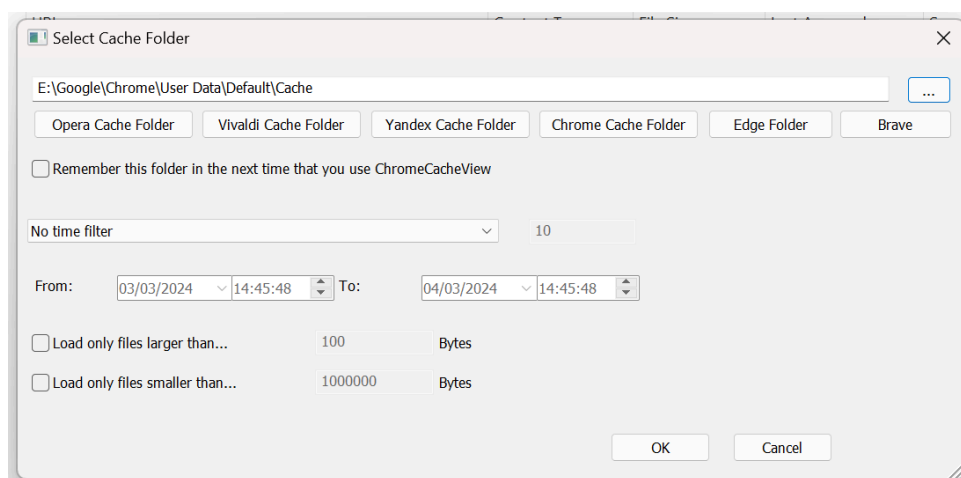
	id	guid	current_path	target_path
1	1	9D8F8D03-AA94-4E49-A52C-79780DC53031	C:\Users\Jose\Downloads\SUS_ENTRADAS_PARA_EL_10-08-2017_Ref1452681_889656.pdf	C:\Users\Jose\De
2	3	15E718B7-A14A-42E1-80E5-19130A7233B1	C:\Users\Jose\Downloads\VOSE.docx	C:\Users\Jose\De
3	4	98bd33c5-0089-4672-8c42-d8d446c52fd7	C:\Users\Jose\Downloads\Guion modulo1.doc	C:\Users\Jose\De
4	5	ecb053e3-b5ab-4244-9553-5685fadf0792	C:\Users\Jose\Downloads\77143144V.pdf	C:\Users\Jose\De
5	7	0b0e3d5a-9b79-44c5-ba88-70d700035bbc	C:\Users\Jose\Downloads\Informe - Almirón López, Inmaculada.pdf	C:\Users\Jose\De
6	9	640cf6c4-3934-4110-a329-3ccd7c803c5b	C:\Users\Jose\Downloads\Movimientos de la cuenta ES3520383508766000342346_CUENTA FACIL.pdf	C:\Users\Jose\De
7	10	0eac69a1-243e-4cc2-b8e9-b3e666309673	C:\Users\Jose\Downloads\Movimientos de la cuenta ES3520383508766000342346_CUENTA FACIL (1).pdf	C:\Users\Jose\De
8	11	4e7a9310-fbc5-415a-a6b8-835c6ba3ccb9	C:\Users\Jose\Downloads\1.PDF	C:\Users\Jose\De
9	13	2cd1480e-cc19-4976-a933-6d43310c8bc3	C:\Users\Jose\Downloads\Guion modulo 3.doc	C:\Users\Jose\De
10	14	0bd24763-9968-421f-9ef1-087bc041b178	C:\Users\Jose\Downloads\CUESTIONARIO 2.doc	C:\Users\Jose\De
11	15	529f278a-45f3-4919-8cbc-eb8a33ea3c30	C:\Users\Jose\Downloads\TEXTO 2.pdf	C:\Users\Jose\De
12	16	33bfc057-ef64-4ce6-a25f-cfadb8a863aa1	C:\Users\Jose\Downloads\solicitud grado superior oficial.pdf	C:\Users\Jose\De
13	17	3dbbeb6bb-51eb-47f7-a1dd-5d8681fe739b	C:\Users\Jose\Downloads\rau-w-alejandro-x-dalex-x-lenny-tavarez-x-dimelo-flow-elegi-video-oficial.mp3	C:\Users\Jose\De
14	18	83e47600-f8c2-46c3-8a30-e0a7a68aa2b2	C:\Users\Jose\Downloads\ozuna-x-willy-temporal-audio-oficial.mp3	C:\Users\Jose\De
15	19	3f7a94d6-a401-4d5e-b311-f53293effddc	C:\Users\Jose\Downloads\tbt-sebastian-yatra-rauw-alejandro-manuel-turizo-letra.mp3	C:\Users\Jose\De
16	21	742008a4-8281-4ae1-9b5b-e5e76baba86c	C:\Users\Jose\Downloads\1 (1).PDF	C:\Users\Jose\De
17	28	071b2798-9910-46a1-bb4d-959bb3dd74b0	C:\Users\Jose\Downloads\Uhon Pal 'El Increible' Ft. Adso Alejandro, Lary Over, Akapellah - Hookiao.mp3	C:\Users\Jose\De

Cache

La caché de Chrome se encuentra en la siguiente ruta:

Users\<\$user>\AppData\Local\Google\Chrome\User Data\Default\Cache

Para analizar la caché, emplearemos la herramienta [Chrome CacheView](#) de Nirsoft. Simplemente selecciona la opción **'File > Select Cache Folder'**:



Cookies

El archivo que almacena las cookies es, una vez más, una base de datos SQLite que se encuentra en el perfil de Chrome.

Users\<\$user>\AppData\Local\Google\Chrome\User Data\Default\Cookies

Utilizaremos [ChromeCookies](#) View para analizarlas. Aunque en mi caso no tengo ninguna cookie

