



Curso de Ciberseguridad

Análisis Forense en Windows

Análisis Forense Informático



Internet Explorer.....	3
Internet Explorer 11	3
Cache	6
Cookies	8
Historial de ficheros descargados	10
Historial de navegación	12
Typed URLs.....	15
Edge.....	16
Firefox	18
Historial de navegación	18
Historial de ficheros descargados	22
Cookies.....	22
Cache.....	23
Chrome.....	25
Historial de navegación	25
Historial de ficheros descargados	30
Cache.....	31
Cookie	33
Recuperando registros bases de datos SQLITE.....	34



Los navegadores son una parte también importante dentro de las investigaciones, ya que pueden ayudarnos a investigar desde una fuga de información hasta el vector de ataque de una brecha de seguridad.

INTERNET EXPLORER

Internet Explorer es uno de los navegadores más conocidos, debido a su principal inclusión por defecto en los sistemas operativos Windows. Es verdad que en la actualidad no es uno de los mayormente usados, pero siempre es importante conocerlo.

¿Qué información nos proporciona Internet Explorer?

- ◆ Qué sitios han sido visitados en los últimos X días
- ◆ Qué ficheros han sido accedidos en el sistema en los últimos días
- ◆ Cuantas veces cada sitio ha sido visitado
- ◆ Si la cuenta de usuario ha sido utilizada para visitar el sitio (información dentro el perfil)
- ◆ Hora concreta del último acceso
- ◆ Esta información es almacenada en los ficheros Index.dat (IE4-IE9) o WebcacheV.dat (IE10+)

Dentro de Internet Explorer podemos encontrar distintas versiones, que afectaran donde se localizan los artefactos forenses, dado que este curso se quiere presentar lo más actual de artefactos forenses, analizaremos las versiones más actuales.

INTERNET EXPLORER 11

Internet Explorer tiene la particularidad de almacenar los datos y los metadatos por separado. Tenemos que diferenciar entre los metadatos y los datos. Los metadatos van a ser la información que nos va a permitir encontrar los datos en sí.

¿Dónde se encuentra estos metadatos?

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

El siguiente paso sería extraer este artefacto mediante FTK Imager para que sea analizado.

¿Qué contienen los metadatos? Información de donde se encuentra:

- ◆ Cookies
- ◆ Cache
- ◆ Historial de Navegación
- ◆ Descargas

File List			
Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	18/11/2018 17:47:23
V01.chk	8	Regular File	18/11/2018 17:47:33
V01.log	512	Regular File	18/11/2018 17:47:23
V01000AA.log	512	Regular File	17/11/2018 9:01:12
V01000AB.log	512	Regular File	17/11/2018 9:01:13
V01000EA.log	512	Regular File	18/11/2018 17:46:58
V01000EB.log	512	Regular File	18/11/2018 17:46:58
V01000EC.log	512	Regular File	18/11/2018 17:46:58
V01000ED.log	512	Regular File	18/11/2018 17:46:58
V01000EE.log	512	Regular File	18/11/2018 17:46:58
V01000EF.log	512	Regular File	18/11/2018 17:46:58
V01000F0.log	512	Regular File	18/11/2018 17:46:58
V01000F1.log	512	Regular File	18/11/2018 17:46:58
V01000F2.log	512	Regular File	18/11/2018 17:46:58
V01000F3.log	512	Regular File	18/11/2018 17:47:00
V01000F4.log	512	Regular File	18/11/2018 17:47:23
V01000F5.log	512	Regular File	18/11/2018 17:47:23
V01res00001.jrs	512	Regular File	07/04/2018 16:29:17
V01res00002.jrs	512	Regular File	07/04/2018 16:29:17
WebCacheV01.dat	38.976	Regular File	18/11/2018 10:26:24
WebCacheV01.tmp	512	Regular File	18/11/2018 10:26:24
WebCacheV01.tmp	512	Regular File	17/11/2018 8:32:37
WebCacheV01.tmp	512	Regular File	17/11/2018 9:00:35

La base de datos ESE puede contener los siguientes nombres:

- ◆ WebcacheV01.dat
- ◆ WebcacheV16.dat
- ◆ WebcacheV24.dat

Si identificamos el fichero **V01.log**, más reciente (como el de la imagen superior) que el fichero **WebcacheV01.dat** debemos recuperar la base de datos ESE mediante el siguiente comando:

```
Esentutl /r V01 /d
```

Es muy importante que extraigamos todos los ficheros de la carpeta Webcache, ya que serán utilizados para recuperar la base de datos:

```
C:\Windows\system32\cmd.exe

C:\Users\usuario>cd C:\Users\usuario\Desktop\Browsers\WebCache
C:\Users\usuario\Desktop\Browsers\WebCache>esentutl /r V01 /d

Extensible Storage Engine Utilities for Microsoft(R) Windows(R)
Version 6.1
Copyright (C) Microsoft Corporation. All Rights Reserved.

Initiating RECOVERY mode...
  Logfile base name: V01
    Log files: <current directory>
    System files: <current directory>
    Database Directory: <current directory>

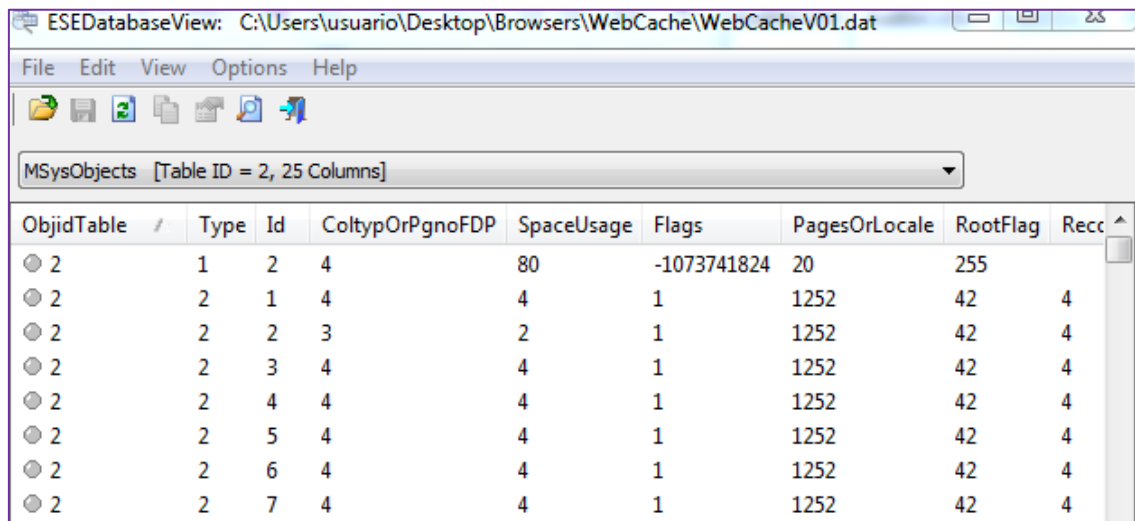
Performing soft recovery...
      Restore Status (% complete)

      0   10   20   30   40   50   60   70   80   90  100
      |---|---|---|---|---|---|---|---|---|---|
      .....

Operation completed successfully in 0.702 seconds.
```

Al ser una base de datos ESE, dispone de cabeceras específicas que permitirían recuperar la misma, mediante técnicas de carving, en caso de borrado. [Photorec](#) lo permite, mediante la opción Exchange Database (EDB).

Es una Base de datos ESE, por lo que podemos utilizar el programa ESEDatabaseView de Nirsoft para abrirlo:



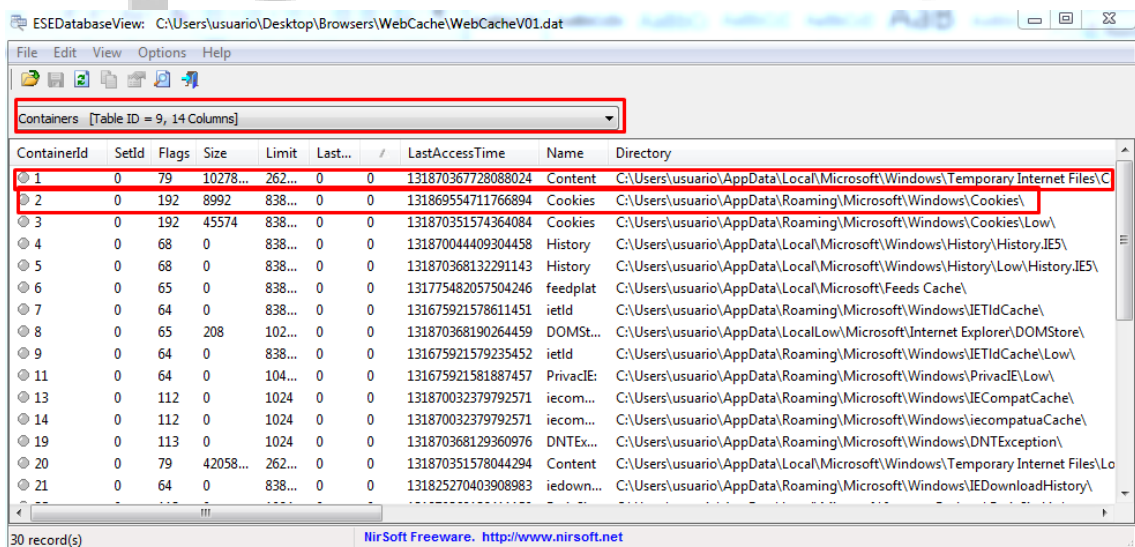
ESEDatabaseView: C:\Users\usuario\Desktop\Browsers\WebCache\WebCacheV01.dat

File Edit View Options Help

MSysObjects [Table ID = 2, 25 Columns]

ObjidTable	Type	Id	ColtypOrPgnoFDP	SpaceUsage	Flags	PagesOrLocale	RootFlag	Recc
2	1	2	4	80	-1073741824	20	255	
2	2	1	4	4	1	1252	42	4
2	2	2	3	2	1	1252	42	4
2	2	3	4	4	1	1252	42	4
2	2	4	4	4	1	1252	42	4
2	2	5	4	4	1	1252	42	4
2	2	6	4	4	1	1252	42	4
2	2	7	4	4	1	1252	42	4

Seleccionamos el Objeto Containers para ver la información de los metadatos y sus rutas:



ESEDatabaseView: C:\Users\usuario\Desktop\Browsers\WebCache\WebCacheV01.dat

File Edit View Options Help

Containers [Table ID = 9, 14 Columns]

ContainerId	SetId	Flags	Size	Limit	Last...	LastAccessTime	Name	Directory
1	0	79	10278...	262...	0	0	131870367728088024	Content C:\Users\usuario\AppData\Local\Microsoft\Windows\Temporary Internet Files\...
2	0	192	8992	838...	0	0	131869554711766894	Cookies C:\Users\usuario\AppData\Roaming\Microsoft\Windows\Cookies\
3	0	192	45574	838...	0	0	131870351574364084	Cookies C:\Users\usuario\AppData\Roaming\Microsoft\Windows\Cookies\Low\
4	0	68	0	838...	0	0	131870044409304458	History C:\Users\usuario\AppData\Local\Microsoft\Windows\History\History.IE5\
5	0	68	0	838...	0	0	131870368132291143	History C:\Users\usuario\AppData\Local\Microsoft\Windows\History\Low\History.IE5\
6	0	65	0	838...	0	0	131775482057504246	feedplat C:\Users\usuario\AppData\Local\Microsoft\Feeds Cache\
7	0	64	0	838...	0	0	131675921578611451	ietId C:\Users\usuario\AppData\Roaming\Microsoft\Windows\IETIdCache\
8	0	65	208	102...	0	0	131870368190264459	DOMSt... C:\Users\usuario\AppData\Local\Low\Microsoft\Internet Explorer\DOMStore\
9	0	64	0	838...	0	0	131675921579235452	ietId C:\Users\usuario\AppData\Roaming\Microsoft\Windows\IETIdCache\Low\
11	0	64	0	104...	0	0	131675921581887457	PrivacIE... C:\Users\usuario\AppData\Roaming\Microsoft\Windows\PrivacIE\Low\
13	0	112	0	1024	0	0	131870032379792571	iecom... C:\Users\usuario\AppData\Roaming\Microsoft\Windows\IECompatCache\
14	0	112	0	1024	0	0	131870032379792571	iecom... C:\Users\usuario\AppData\Roaming\Microsoft\Windows\iecompatuaCache\
19	0	113	0	1024	0	0	131870368129360976	DNTE... C:\Users\usuario\AppData\Roaming\Microsoft\Windows\DNTEException\
20	0	79	42058...	262...	0	0	131870351578044294	Content C:\Users\usuario\AppData\Local\Microsoft\Windows\Temporary Internet Files\Lo
21	0	64	0	838...	0	0	131825270403908983	iedown... C:\Users\usuario\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\

30 record(s) NirSoft Freeware. <http://www.nirsoft.net>

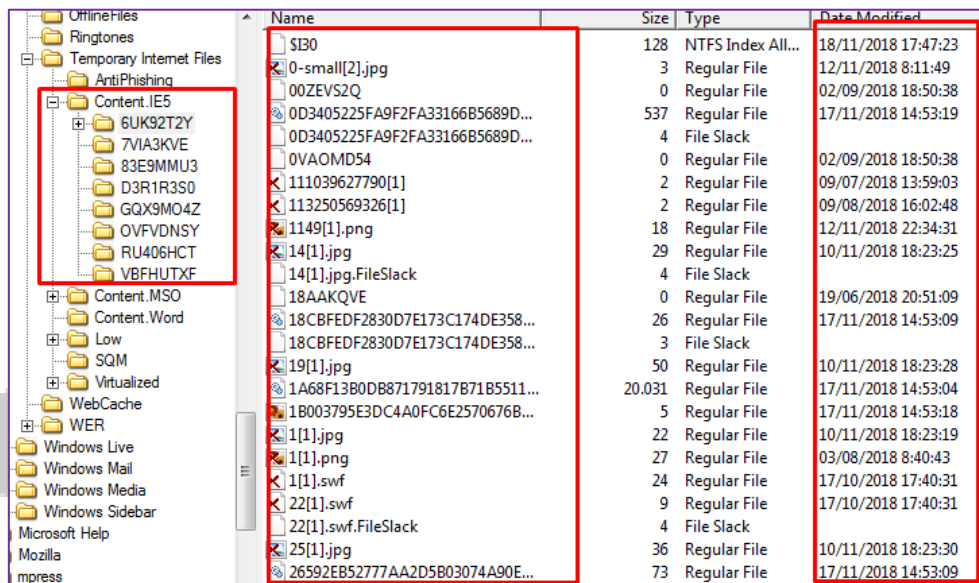
De aquí podemos obtener la siguiente información:

CACHE

La cache es el lugar donde están los componentes de la página web son almacenados localmente para acelerar siguientes visitas.

- ◆ %userprofile%\Appdata\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5 -> Container 1
- ◆ %userprofile%\Appdata\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5 -> Container 20

Si vamos dentro de nuestra evidencia con FTK Imager, a las siguientes rutas podremos encontrar los objetos que han sido descargados:



Name	Size	Type	Date Modified
\$I30	128	NTFS Index All...	18/11/2018 17:47:23
0-small[2].jpg	3	Regular File	12/11/2018 8:11:49
00ZEV52Q	0	Regular File	02/09/2018 18:50:38
0D3405225FA9F2FA33166B5689D...	537	Regular File	17/11/2018 14:53:19
0D3405225FA9F2FA33166B5689D...	4	File Slack	
0VAOMD54	0	Regular File	02/09/2018 18:50:38
111039627790[1]	2	Regular File	09/07/2018 13:59:03
113250569326[1]	2	Regular File	09/08/2018 16:02:48
1149[1].png	18	Regular File	12/11/2018 22:34:31
14[1].jpg	29	Regular File	10/11/2018 18:23:25
14[1].jpg.FileSlack	4	File Slack	
18AAKQVE	0	Regular File	19/06/2018 20:51:09
18CBFEDF2830D7E173C174DE358...	26	Regular File	17/11/2018 14:53:09
18CBFEDF2830D7E173C174DE358...	3	File Slack	
19[1].jpg	50	Regular File	10/11/2018 18:23:28
1A68F13B0DB871791817B71B5511...	20.031	Regular File	17/11/2018 14:53:04
1B003795E3DC4A0FC6E2570676B...	5	Regular File	17/11/2018 14:53:18
1[1].jpg	22	Regular File	10/11/2018 18:23:19
1[1].png	27	Regular File	03/08/2018 8:40:43
1[1].swf	24	Regular File	17/10/2018 17:40:31
22[1].swf	9	Regular File	17/10/2018 17:40:31
22[1].swf.FileSlack	4	File Slack	
25[1].jpg	36	Regular File	10/11/2018 18:23:30
26592EB52777AA2D5B03074A90E...	73	Regular File	17/11/2018 14:53:09

Proporciona al investigador un snapshot de que es lo que estaba mirando un usuario:

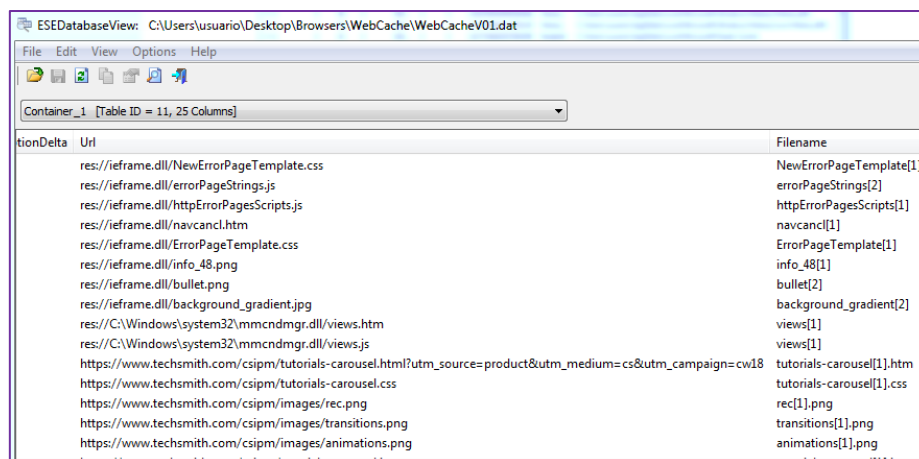
- ◆ La cache por defecto almacena 250 MB
- ◆ Los timestamps muestran cuando el sitio fue visitado:
 - Por primera vez: fecha de creación NTFS
 - Última vez: fecha de modificación NTFS

Estas fechas también se pueden obtener del análisis de MFT con la herramienta MFT2CSV.

Cache Metadata

Se encuentra en el Container 1 / 20 y podemos obtener la siguiente información:

- ◆ Nombre del archivo que existe en el disco
- ◆ SecureDirectory localización del fichero dentro los directorios de la cache
- ◆ AccessCount: número de veces que se ha usado la caché
- ◆ URL: origen que cacheó el contenido.



The screenshot shows a window titled 'ESEDatabaseView' with the file path 'C:\Users\usuario\Desktop\Browsers\WebCache\WebCacheV01.dat'. The window displays a table with columns 'Url' and 'Filename'. The table contains various entries including local resources (e.g., 'res://ieframe.dll/NewErrorPageTemplate.css') and external URLs (e.g., 'https://www.techsmith.com/csipm/tutorials-carousel.html?utm_source=product&utm_medium=cs&utm_campaign=cw18').

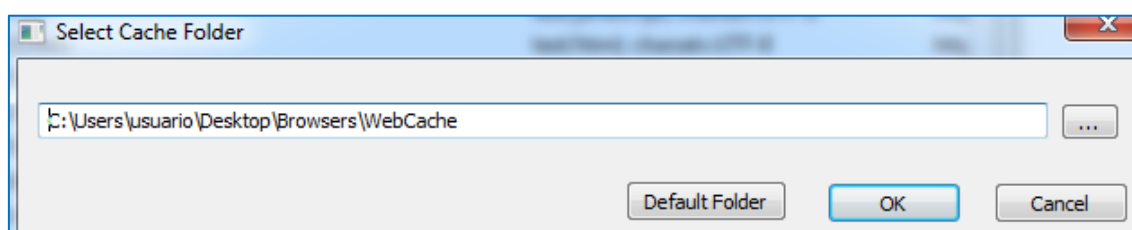
Url	Filename
res://ieframe.dll/NewErrorPageTemplate.css	NewErrorPageTemplate[1]
res://ieframe.dll/errorPageStrings.js	errorPageStrings[2]
res://ieframe.dll/httpErrorPagesScripts.js	httpErrorPagesScripts[1]
res://ieframe.dll/navcancel.htm	navcancel[1]
res://ieframe.dll/ErrorPageTemplate.css	ErrorPageTemplate[1]
res://ieframe.dll/info_48.png	info_48[1]
res://ieframe.dll/bullet.png	bullet[2]
res://ieframe.dll/background_gradient.jpg	background_gradient[2]
res://C:\Windows\system32\mmcndmgr.dll/views.htm	views[1]
res://C:\Windows\system32\mmcndmgr.dll/views.js	views[1]
https://www.techsmith.com/csipm/tutorials-carousel.html?utm_source=product&utm_medium=cs&utm_campaign=cw18	tutorials-carousel[1].htm
https://www.techsmith.com/csipm/tutorials-carousel.css	tutorials-carousel[1].css
https://www.techsmith.com/csipm/images/rec.png	rec[1].png
https://www.techsmith.com/csipm/images/transitions.png	transitions[1].png
https://www.techsmith.com/csipm/images/animations.png	animations[1].png

Los timestamps que hay dentro del container indican lo siguiente

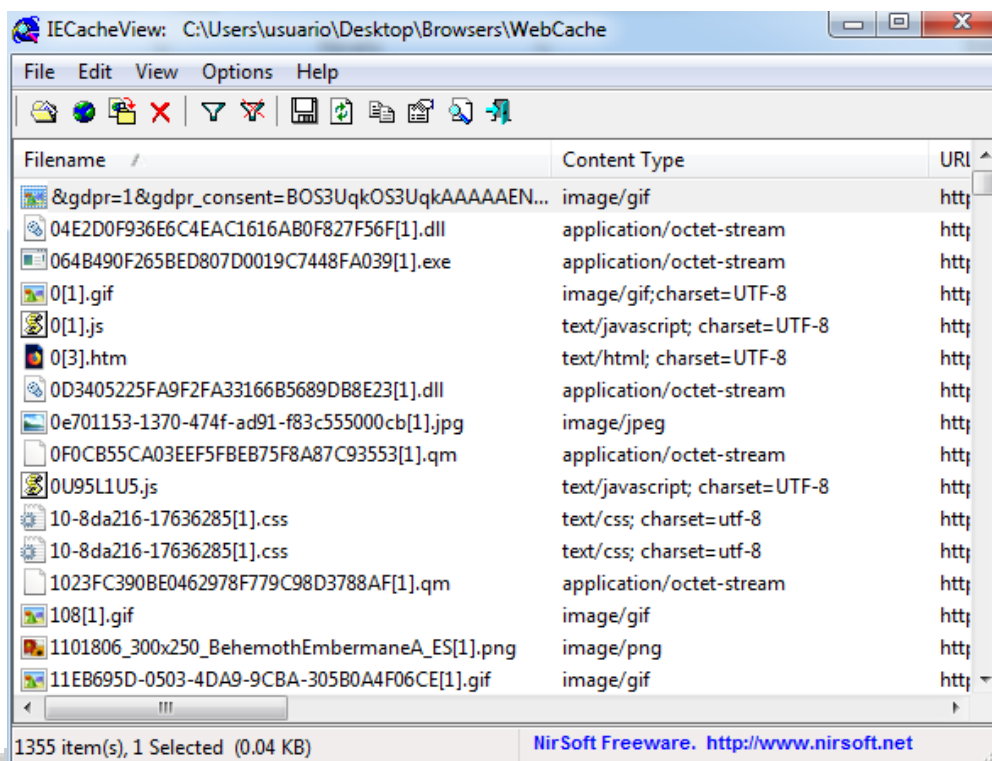
- ◆ CreationTime: cuando fue cacheado el fichero que fue guardado al disco, la primera vez que el contenido fue visto.
- ◆ AccessedTime: Proporciona el timestamp donde el cache fue requerido y visto por el usuario.
- ◆ ModifiedTime: Indica la última versión de la página si el fichero fue modificado en servidor web. Los servidores web siempre devuelven un timestamp como parte de las cabeceras HTTP
- ◆ ExpiryTime: establecido por la web que proporciona el contenido, permitiendo saber cuándo debe ser borrado.

Podemos utilizar el programa IECacheView, que tenemos dentro de la carpeta Browsers donde automáticamente nos interpretaría la base de datos **WebcacheV01.dat**.

Para ello, seleccionamos "File -> Select Cache Folder" para indicar el directorio que contiene **WebcacheV01.dat** que hemos extraído mediante FTK:



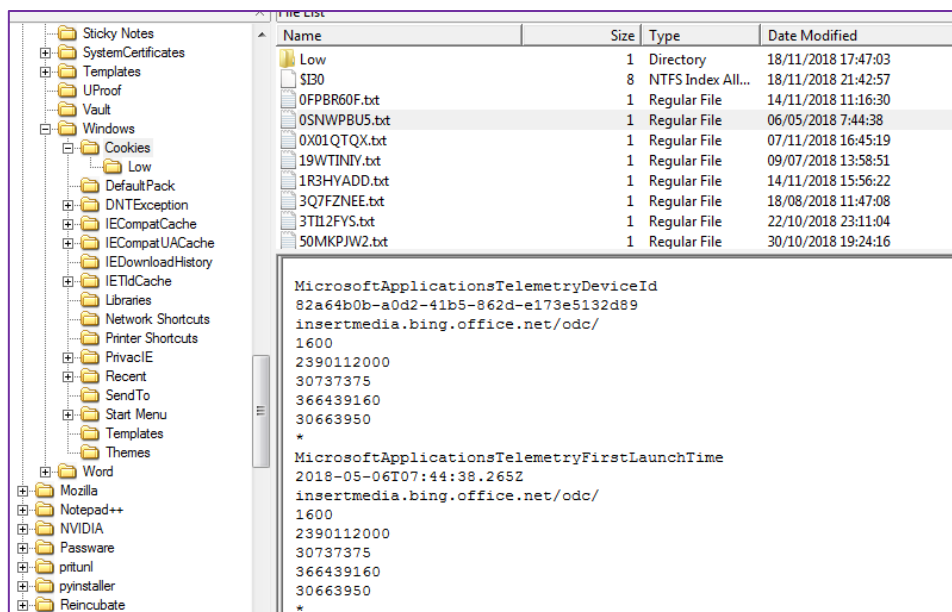
Una vez leído nos muestra toda la información:



COOKIES

De la base de datos WebcacheV01.dat podemos obtener las siguientes rutas de donde se encuentran las rutas:

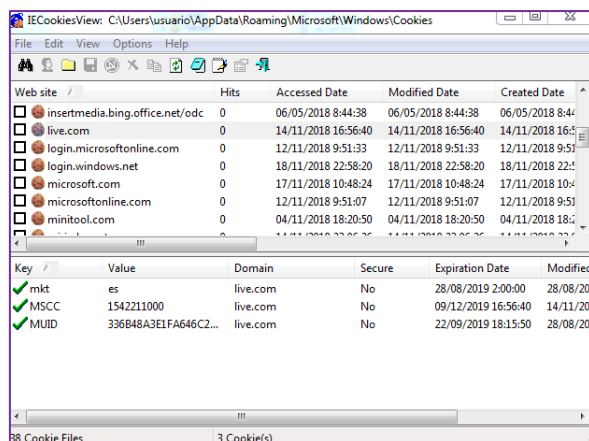
- ◆ %userprofile%\Appdata\Roaming\Microsoft\Windows\Cookies -> Container 2
- ◆ %userprofile%\Appdata\Roaming\Microsoft\Windows\Cookies\Low -> Container 3



Las cookies no superan los 4kbs de tamaño y nos proporcionan la siguiente información:

- ◆ Emisor de la web
- ◆ Cuenta local
- ◆ Fechas de sistemas del sistema de archivos
- ◆ Las cookies persistentes se almacenan en el disco. Las cookies de sesión en memoria.

Un visor de cookies, es decir, uno que pueda analizar los ficheros de cookies que estén las rutas que hemos visto más arriba, sería IECookiesViewer de Nirsoft. Para ello debemos indicarle donde tenemos el directorio que previamente hemos extraído con FTK, mediante "File-> Select Cookies Folder"



¿Qué información podemos tener de los metadatos localizados en **WebcacheV01.dat** de las cookies?

- ◆ Nombre de la cookie en el sistema de archivos
- ◆ URL que proporciona la cookie
- ◆ AccessCount: cuantas veces la cookie ha sido pasada al sitio
- ◆ CreationTime: primera vez que la cookie se guardo en el sistema (UTC)
- ◆ ModifiedTime: última vez que el website modificó la cookie.(UTC)
- ◆ AccessedTime: última vez que la cookie fue pasada al sitio. (UTC)
- ◆ ExpiryTime: fecha a partir que la cookie no será aceptada. (UTC)

Container_2 [Table ID = 12, 25 Columns]							
	CreationTime	ExpiryTime	ModifiedTime	AccessedTime	P..	Sync...	Url
1450	131675716543872141	131675717740000000	131675716543870000	131675921577831450	0	0	Cookie:usuario@www.geforce.com/
9031	131866677900099031	132497397980000000	131866677900099031	131866677900099031	0	0	Cookie:usuario@adobe.com/
6514	131675974627136514	131831494620000000	131675974627136514	131675974627136514	0	0	Cookie:usuario@demdex.net/
9677	131678395403559677	131993719470000000	131678395403559677	131678395403559677	0	0	Cookie:usuario@programacion.net/
7945	131856972886637943	137990417510000000	131856972886637941	131856972886707945	0	0	Cookie:usuario@github.com/
1324	131680310825861323	131995634970000000	131680310825841322	131680310825881324	0	0	Cookie:usuario@contextis.com/
1329	131680310825951328	131995634970000000	131680310825951328	131680310825961329	0	0	Cookie:usuario@www.contextis.com/
0415	131681291826410413	131996616010000000	131681291826400413	131866971697968391	0	0	Cookie:usuario@wireshark.org/
9738	131689695119139738	131689803130000000	131689695119139738	131689695119139738	0	0	Cookie:usuario@formacionoea-ihacklabs.talentlms.com/
0353	131700662778250353	132037622770000000	131700662778250353	131700665876754151	0	0	Cookie:usuario@insertmedia.bing.office.net/
8360	131700662782618360	132016022780000000	131700662782618360	131700665876754151	0	0	Cookie:usuario@insertmedia.bing.office.net/odc/
1103	131860827194571103	132491547190000000	131860827194571103	131860827194671103	0	0	Cookie:usuario@win-rar.com/
9655	131858256503439654	132488976500000000	131858256503439654	131858256503539655	0	0	Cookie:usuario@minitool.com/
5329	13173915733889329	141739157350000000	13173915733889329	131739157334045329	0	0	Cookie:usuario@clickability.com/
4366	131869217043104366	132145940190000000	131869217043104366	131870368431118235	0	0	Cookie:usuario@microsoft.com/

HISTORIAL DE FICHEROS DESCARGADOS

Según el análisis de la base de datos ESE WebcacheV01.dat obtenemos lo siguiente:

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

ESEDatabaseView: C:\Users\usuario\Desktop\Browsers\nueva\WebCache\WebCacheV01....					
File Edit View Options Help					
Container_21 [Table ID = 53, 25 Columns]					
Delta	Url	Filename	FileExtension	RequestHeaders	Response
	iedownload:{AF7E874C-EB83-11E8-B2FA-A9288F69D456}				89 00 0

Esta tabla contiene las siguientes columnas:

- ◆ Nombre del fichero
- ◆ Tamaño
- ◆ URL Original
- ◆ URL Referrer
- ◆ Destino de la descarga
- ◆ Tiempo en descargarse

El campo ResponseHeaders podemos analizarlo mediante [CyberChef](#):

Extension	RequestHeaders	ResponseHeaders	RedirectUrl	Group
		89 00 00 00 0B 00 00 00 00 00 00 00 00 00 00 00 E9 F...		

Copiamos el campo ResponseHeader a Cyberchef con las recetas que veremos en la siguiente captura:

Recipe

From Hex

Delimiter
Auto

Remove null bytes

Input

length: 3071
lines: 1

```

00 32 00 38 00 2E 00 78 00 6C 00 73 00 78 00 26 00 75 00 73 00 67 00 3D 00 41 00
4F 00 76 00 56 00 61 00 77 00 32 00 74 00 38 00 48 00 35 00 62 00 75 00 62 00 53
00 63 00 55 00 59 00 35 00 45 00 4C 00 64 00 39 00 38 00 7A 00 50 00 64 00 37 00
00 00 61 00 70 00 70 00 6C 00 69 00 63 00 61 00 74 00 69 00 6F 00 6E 00 2F 00 76
00 6E 00 64 00 2E 00 6F 00 70 00 65 00 6E 00 78 00 6D 00 6C 00 66 00 6F 00 72 00
6D 00 61 00 74 00 73 00 2D 00 6F 00 66 00 66 00 69 00 63 00 65 00 64 00 6F 00 63
00 75 00 6D 00 65 00 6E 00 74 00 2E 00 73 00 70 00 72 00 65 00 61 00 64 00 73 00
68 00 65 00 65 00 74 00 6D 00 6C 00 2E 00 73 00 68 00 65 00 65 00 74 00 00 00 43
00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 75 00 73 00 75 00 61 00 72 00
69 00 6F 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63
00 61 00 6C 00 5C 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 5C 00
57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 5C 00 54 00 65 00 6D 00 70 00 6F 00 72
00 61 00 72 00 79 00 20 00 49 00 6E 00 74 00 65 00 72 00 6E 00 65 00 74 00

```

Output

time: 2ms
length: 476
lines: 3

```

..éý^ w..èè.²ú@(.iôVp02r..ô.....LO...{.²EÈ.Ç.LwäÈàv".Æ.Àdè
.ù¹. T.upT.uÀdè
ø.L Ý*.ù¹.@.Eu°ù¹.qvEu Ý*.ø.ó.Èù¹.À;LT.L Ý*.òù¹.ÛN.upèI.http://www.google.es
/url?sa=t&nct=j&q=&esrc=s&source=web&cd=4&
ved=2ahUKEwjDyJLIgt_eAhUF3RoKHcoGAHAQFjADegQICRAC&url=http%3A%2F
%2Fmstskheta.gov.ge%2Fpublic%2Fimg%2F1530793528.xlsx&
usg=AOvVaw2t8K5bubScUY5ELd98zPd7application/vnd.openxmlformats-
officedocument.spreadsheetml.sheetC:\Users\usuario\AppData\Local\Microsoft\Windows
\Temporary Internet

```

Podemos obtener claramente la información de descarga, donde ha sido descargado, el tipo de fichero y la ruta:

http://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=2ahUKEwjDyJLlgt_eAhUF3RoKHcoGAHAQFjADegQICRAC&url=http%3A%2F%2Fmstkheta.gov.ge%2Fpublic%2Fimg%2F1530793528.xlsx&usq=A0vVaw2t8K5bubScUY5ELd98zPd7

application/vnd.openxmlformats-officedocument.spreadsheetml.sheet

C:\Users\usuario\AppData\Local\Microsoft\Windows\Temporary Internet

HISTORIAL DE NAVEGACIÓN

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

- %userprofile%\Appdata\Local\Microsoft\Windows\History\History.IE5 -> Container 4
- %userprofile%\Appdata\Local\Microsoft\Windows\History\Low\History.IE5 -> Container 5

ContainerId	SetId	Flags	Size	Limit	La...	E...	LastAccessTime	Name	PartitionId	Directory
6	0	65	0	8388608	0	0	131775482057504246	feedplat	M	C:\Users\usuario\AppData\Local\Microsoft\Feeds\Cache\
5	0	68	0	8388608	0	0	131870368132291143	History	L	C:\Users\usuario\AppData\Local\Microsoft\Windows\History\Low\History.IE5\
4	0	68	0	8388608	0	0	13187004409304458	History	M	C:\Users\usuario\AppData\Local\Microsoft\Windows\History\History.IE5\
13	0	112	0	1024	0	0	131870032379792571	iecompat	M	C:\Users\usuario\AppData\Roaming\Microsoft\Windows\IECompatCache\
14	0	112	0	1024	0	0	131870032379792571	iecompatua	M	C:\Users\usuario\AppData\Roaming\Microsoft\Windows\iecompatuaCache\
21	0	64	0	8388608	0	0	131825270403908983	iedownload	M	C:\Users\usuario\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\
9	0	64	0	8388608	0	0	131675921579235452	ietld	L	C:\Users\usuario\AppData\Roaming\Microsoft\Windows\IETldCache\Low\
7	0	64	0	8388608	0	0	131675921578611451	ietld	M	C:\Users\usuario\AppData\Roaming\Microsoft\Windows\IETldCache\
213	0	64	0	8388608	0	0	131860832311487562	MSHist0120181...	L	C:\Users\usuario\AppData\Local\Microsoft\Windows\History\Low\History.IE5\M
209	0	64	0	8388608	0	0	131858805297583250	MSHist0120181...	M	C:\Users\usuario\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist
220	0	64	0	8388608	0	0	131864826369153473	MSHist0120181...	M	C:\Users\usuario\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist
214	0	64	0	8388608	0	0	131860832311767567	MSHist0120181...	L	C:\Users\usuario\AppData\Local\Microsoft\Windows\History\Low\History.IE5\M
218	0	64	0	8388608	0	0	131863567155813709	MSHist0120181...	L	C:\Users\usuario\AppData\Local\Microsoft\Windows\History\Low\History.IE5\M
221	0	64	0	8388608	0	0	131864826370563481	MSHist0120181...	M	C:\Users\usuario\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist
222	0	64	0	8388608	0	0	131865373843423182	MSHist0120181...	M	C:\Users\usuario\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist

Dentro del Container 4 podemos localizar lo siguiente:

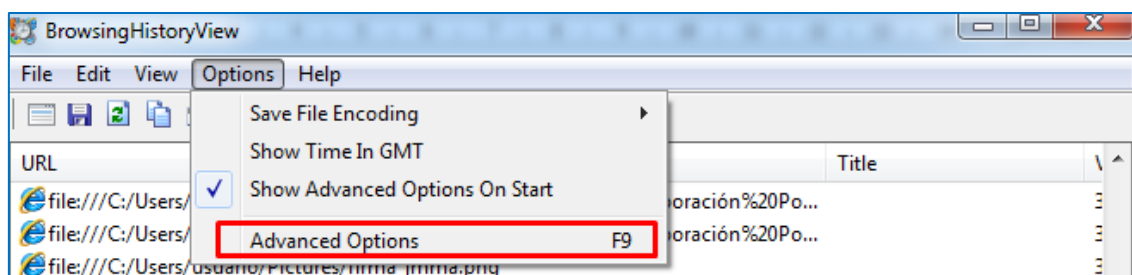
- ModifiedTime: primera vez que se referencia al objeto en una URL
- AccessedTime: última vez que se referencia al objeto en una URL
- AccessCount: número de vez de la URL visitado



Container_4 [Table ID = 14, 25 Columns]									
gs	AccessCount	SyncTime	CreationTime	ExpiryTime	ModifiedTime	AccessedTime	P.	SyncCount	Url
3	131856355958503365	0	131878819958508595	131856355958503365	131856355958503365	131856355958503365	0	0	Visited: usuario@file:///C:/Users/usuario/Desk
3	131856355491676494	0	131878819491681724	131856355491676494	131856355491676494	131856355491676494	0	0	Visited: usuario@file:///C:/Users/usuario/Desk
3	131859092604649909	0	131881556604650139	131859092604649909	131859092604649909	131859092604649909	0	0	Visited: usuario@file:///C:/Users/usuario/Desk
2	131855028167079676	0	131877492167084906	131855028167079676	131855028167079676	131855028167079676	0	0	Visited: usuario@file:///C:/Mio/Trabajo/thack
183	131869498092910884	0	131891962092916114	131869498092910884	131869498092910884	131869498092910884	0	0	Visited: usuario@file:///C:/Mio/Trabajo/thack
11	131866671998355132	0	131889135998360362	131866671998355132	131866671998355132	131866671998355132	0	0	Visited: usuario@file:///C:/Mio/Trabajo/thack
20	131867703851065269	0	131890167851070499	131867703851065269	131867703851065269	131867703851065269	0	0	Visited: usuario@file:///C:/Mio/Trabajo/thack
48	131866823688567310	0	131889287688562539	131866823688567309	131866823688567309	131866823688567310	0	0	Visited: usuario@file:///C:/Mio/Trabajo/thack
14	131868444393116357	0	131890904098154291	131868444393116357	131868444393116357	131868444393116357	0	0	Visited: usuario@file:///C:/Mio/Trabajo/thack
2	131858919259381599	0	131881383259381828	131858919259376598	131858919259381599	131858919259381599	0	0	Visited: usuario@file:///C:/Mio/Trabajo/thack
4	131866706075733669	0	131889170075738899	131866706075733669	131866706075733669	131866706075733669	0	0	Visited: usuario@file:///C:/Mio/Trabajo/thack
2	131857193825822708	0	131879657825827938	131857193825822708	131857193825822708	131857193825822708	0	0	Visited: usuario@file:///C:/Users/usuario/Drop
2	131854720761256065	0	131877184761261295	131854720761256065	131854720761256065	131854720761256065	0	0	Visited: usuario@file:///C:/Users/usuario/Drop
3	131858936149986433	0	131881395855024367	131858936149986433	131858936149986433	131858936149986433	0	0	Visited: usuario@file:///C:/Mio/Trabajo/thack
4	131863496217734828	0	13188595922727262	131863496217734828	131863496217734828	131863496217734828	0	0	Visited: usuario@file:///C:/Mio/Trabajo/thack

También Podemos utilizar el programa de Nirsoft **BrowsingHistoryView** para analizar la base de datos directamente, para ello, primeramente, debemos seleccionar Options-> Advanced Options

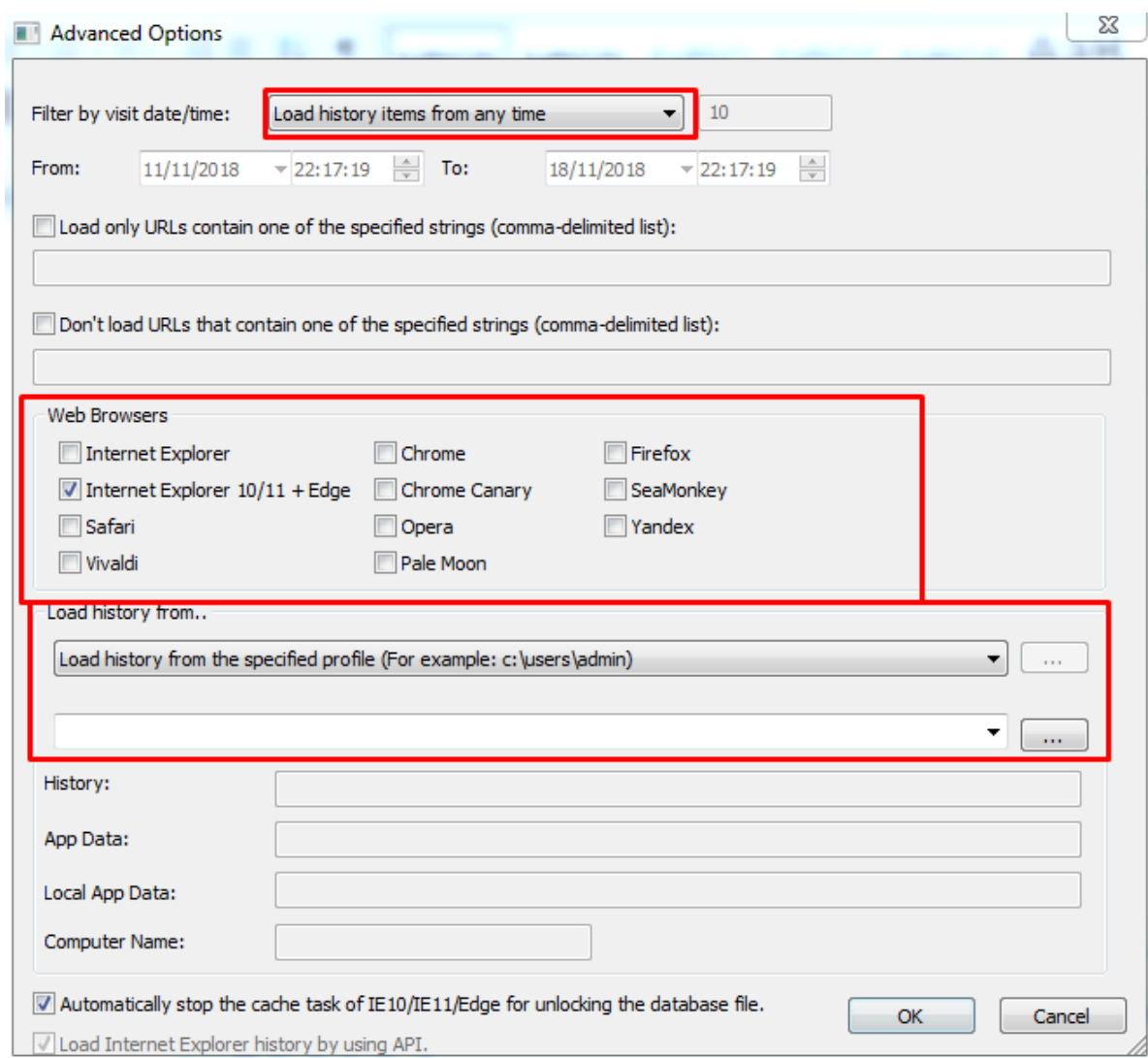
QUANTIKA¹⁴



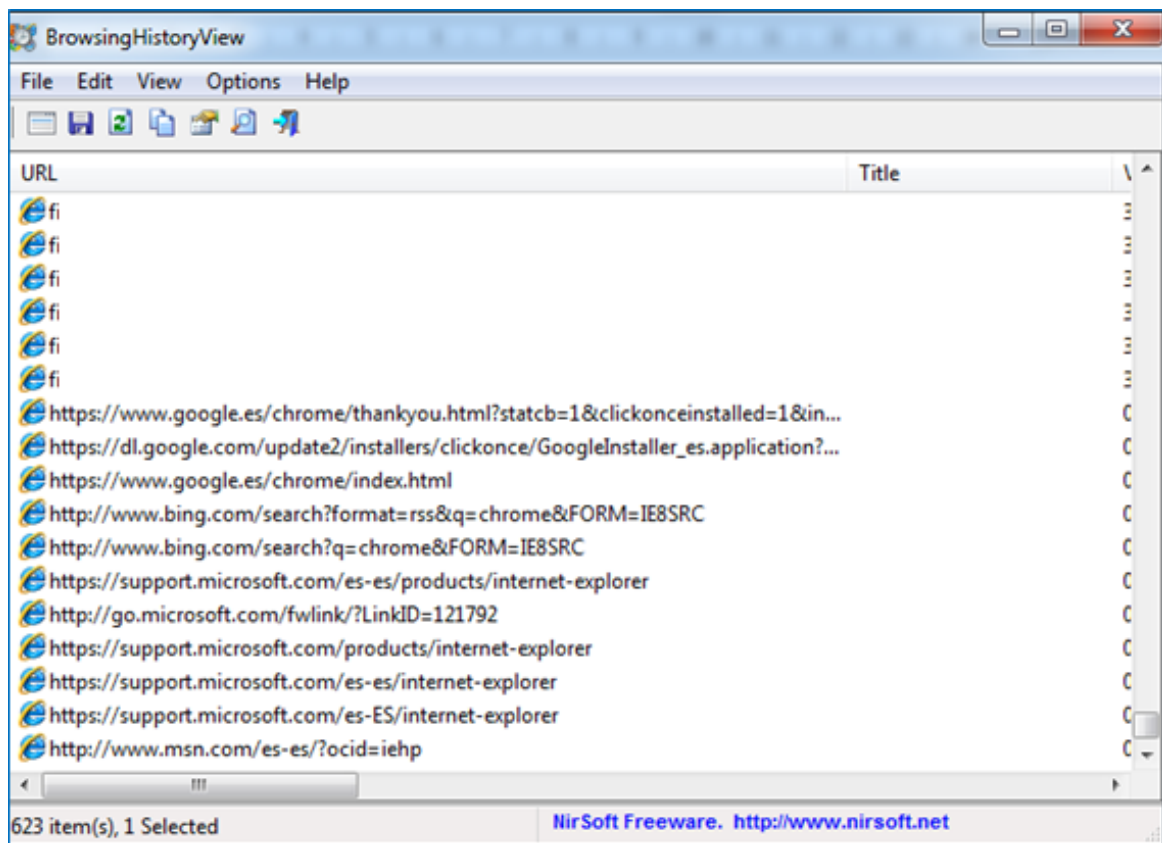
A continuación, nos muestra las opciones que debemos seleccionar:

- El periodo de tiempo del histórico
- Qué Web Browsers va a analizar
- Cargar el historial ¿desde?

Para cargar el historial desde, lo más cómodo sería montar la imagen forense mediante Arsenal Imagen Mounter, con permisos de escritura, verificar los permisos sobre el usuario que vayamos a investigar y seleccionar la ruta en la opción de Browsing History View



Una vez hecho, ya tenemos los resultados de navegación:



TYPED URLS

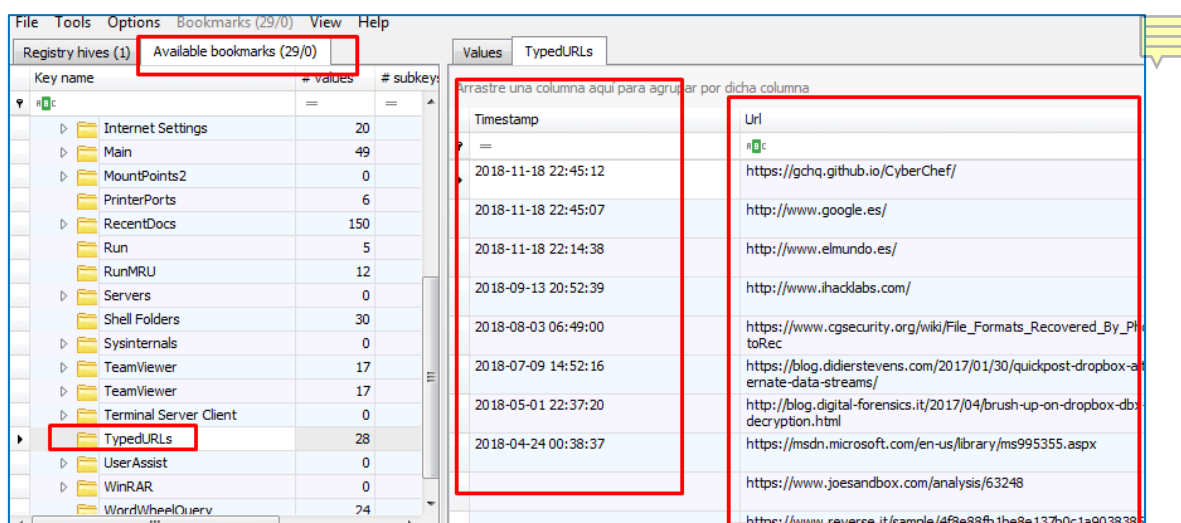
Las Typed URL es el historial de las urls que han sido tecleadas, se almacena en el registro del usuario NTUSER.DAT, en la siguiente ruta:

- ◆ **Software\Microsoft\InternetExplorer\TypedURLs**
 - ◆ Registra las últimas 25 (IE9)
 - ◆ Incrementado a las 50 últimas direcciones (IE10+)

A partir de Internet Explorer 10 también se registra la última vez que fue utilizada la TypedURL

- ◆ **Software\Microsoft\InternetExplorer\TypedURLsTime**

Para analizar este artefacto, previamente deberemos extraer el registro NTUSER.DAT mediante FTK del usuario a investigar para posteriormente utilizar Registry Explorer y en la solapa de Bookmarks, seleccionar TypeUrls:



EDGE

Con la llegada de Windows 10, se introdujo un nuevo navegador que a nivel forense es el mismo que hemos analizado en la versión de IE11. El fichero que contiene todos los metadatos es WebCacheVX.dat y dispone de:

- ◆ **Cache**
- ◆ **Historial**
- ◆ **Descarga de Ficheros**
- ◆ **Cookies**

Containers [Table ID = 9, 14 Columns]		
Contain...	Name /	Directory
15	BackgroundTr...	C:\Users\ismis\AppData\Local\Packages\microsoft.windows.contentdeliverymanager_cw5n1h2byewy\AC\NetHistory\BackgroundTransferA...
28	BackgroundTr...	C:\Users\ismis\AppData\Local\Packages\microsoft.microsoftskydrive_8wekyb3d8bbwe\AC\NetHistory\BackgroundTransferApi\
33	BackgroundTr...	C:\Users\ismis\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\AC\NetHistory\BackgroundTransferApi\
19	BackgroundTr...	C:\Users\ismis\AppData\Local\Packages\microsoft.windows.cortana_cw5n1h2byewy\AC\NetHistory\BackgroundTransferApi\
20	BackgroundTr...	C:\Users\ismis\AppData\Local\Packages\microsoft.windows.cortana_cw5n1h2byewy\AC\NetHistory\BackgroundTransferApiGroup\
34	Content	C:\Users\ismis\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\AC\NetCache\
35	Content	C:\Users\ismis\AppData\Local\Packages\microsoft.windows.authhost.a_8wekyb3d8bbwe\AC\NetCache\
8	Content	C:\Users\ismis\AppData\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\MicrosoftEdge\Cache\
4	Content	C:\Users\ismis\AppData\Local\Packages\microsoft.windows.cortana_cw5n1h2byewy\AC\NetCache\
30	Content	C:\Users\ismis\AppData\Local\Packages\microsoft.skypeapp_kzf8qxf38zg5c\AC\NetCache\
29	Content	C:\Users\ismis\AppData\Local\Packages\microsoft.microsoftskydrive_8wekyb3d8bbwe\AC\NetCache\
3	Content	C:\Users\ismis\AppData\Local\Packages\microsoft.windows.contentdeliverymanager_cw5n1h2byewy\AC\NetCache\
13	Content	C:\Users\ismis\AppData\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\#1002\MicrosoftEdge\Cache\
24	Content	C:\Users\ismis\AppData\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\#1001\MicrosoftEdge\Cache\
39	Content	C:\Users\ismis\AppData\Local\Packages\microsoft.windows.cloudexperiencehost_cw5n1h2byewy\AC\NetCache\
21	Content	C:\Users\ismis\AppData\Local\Packages\microsoft.windowsstore_8wekyb3d8bbwe\AC\NetCache\
31	Content	C:\Users\ismis\AppData\Local\Packages\microsoft.officehub_8wekyb3d8bbwe\AC\NetCache\
1	Content	C:\Users\ismis\AppData\Local\Microsoft\Windows\NetCache\IE\
36	Cookies	C:\Users\ismis\AppData\Local\Packages\microsoft.windows.authhost.a_8wekyb3d8bbwe\AC\NetCookies\
32	DOMStore	C:\Users\ismis\AppData\Local\Packages\microsoft.skypeapp_kzf8qxf38zg5c\AC\Microsoft\Internet Explorer\DOMStore\
40	DOMStore	C:\Users\ismis\AppData\Local\Packages\microsoft.windows.cloudexperiencehost_cw5n1h2byewy\AC\Microsoft\Internet Explorer\DOMStore\
38	DOMStore	C:\Users\ismis\AppData\Local\Packages\microsoft.windows.authhost.a_8wekyb3d8bbwe\AC\Microsoft\Internet Explorer\DOMStore\
23	DOMStore	C:\Users\ismis\AppData\Local\Packages\microsoft.windowsstore_8wekyb3d8bbwe\AC\Microsoft\Internet Explorer\DOMStore\
14	DOMStore	C:\Users\ismis\AppData\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\#1002\MicrosoftEdge\User\Default\DOMStore\
25	DOMStore	C:\Users\ismis\AppData\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\#1001\MicrosoftEdge\User\Default\DOMStore\
5	DOMStore	C:\Users\ismis\AppData\Local\Packages\microsoft.windows.cortana_cw5n1h2byewy\AC\Microsoft\Internet Explorer\DOMStore\
37	History	C:\Users\ismis\AppData\Local\Packages\microsoft.windows.authhost.a_8wekyb3d8bbwe\AC\NetHistory\
16	History	C:\Users\ismis\AppData\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\#1002\MicrosoftEdge\History\
2	History	C:\Users\ismis\AppData\Local\Microsoft\Windows\History\History.IE5\
27	History	C:\Users\ismis\AppData\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\#1121\MicrosoftEdge\History\
26	History	C:\Users\ismis\AppData\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\#1001\MicrosoftEdge\History\
6	History	C:\Users\ismis\AppData\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\MicrosoftEdge\History\
18	iedownload	C:\Users\ismis\AppData\Local\Packages\microsoft.microsoftedge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\DownloadHistory\
7	MicrosoftEdge...	C:\Users\ismis\AppData\Local\MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_DIN1Exception\
11	MicrosoftEdge...	C:\Users\ismis\AppData\Local\MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_EmieSiteList\
12	MicrosoftEdge...	C:\Users\ismis\AppData\Local\MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_EmieUserList\
9	MicrosoftEdge...	C:\Users\ismis\AppData\Local\MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_iecompat\
10	MicrosoftEdge...	C:\Users\ismis\AppData\Local\MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_iecompatua\
17	MicrosoftEdge...	C:\Users\ismis\AppData\Local\MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_ieflipahead\
22	MSHist012018...	C:\Users\ismis\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012018100320181004\

De la imagen superior podemos obtener las rutas físicas de donde encuentran los artefactos. El procedimiento es el mismo que en Internet Explorer, pero en Windows10 se trabaja en la siguiente ruta:

◆ %userprofile%\Appdata\Local\Packages\

Será siempre obligatorio analizar esta base de datos para identificar donde están las localizaciones físicas.

**Ver video: 001/MÓD. 6 -Internet Explorer*

FIREFOX

Firefox es un navegador web open-source que es capaz de funcionar en variedad de plataformas, incluyendo 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**

Lo primero de que deberemos hacer es extraer esta carpeta mediante FTK Imager de la evidencia para poder analizar los siguientes artefactos:

HISTORIAL DE NAVEGACIÓN

Se encuentra en la base de datos en formato SQLite **places.sqlite**, para leerla bastaría con abrir el programa SQLite Studio, pinchar en "Databases -> Add Database" y seleccionarla. Mas información de como añadir una base de datos SQLITE:

https://github.com/pawelsalawa/sqlitestudio/wiki/User_Manual#using-existing-database

En la Tabla **moz_places** encontraremos el historial de navegación y podríamos lanzar una query de esta manera para obtener todo el historial.

Se puede consultar la siguiente url para ver cómo se lanza una consulta:

https://github.com/pawelsalawa/sqlitestudio/wiki/User_Manual#executing-sql-queries

```
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
```

Nos devolverá el historial en UTC junto con el tipo de visita:



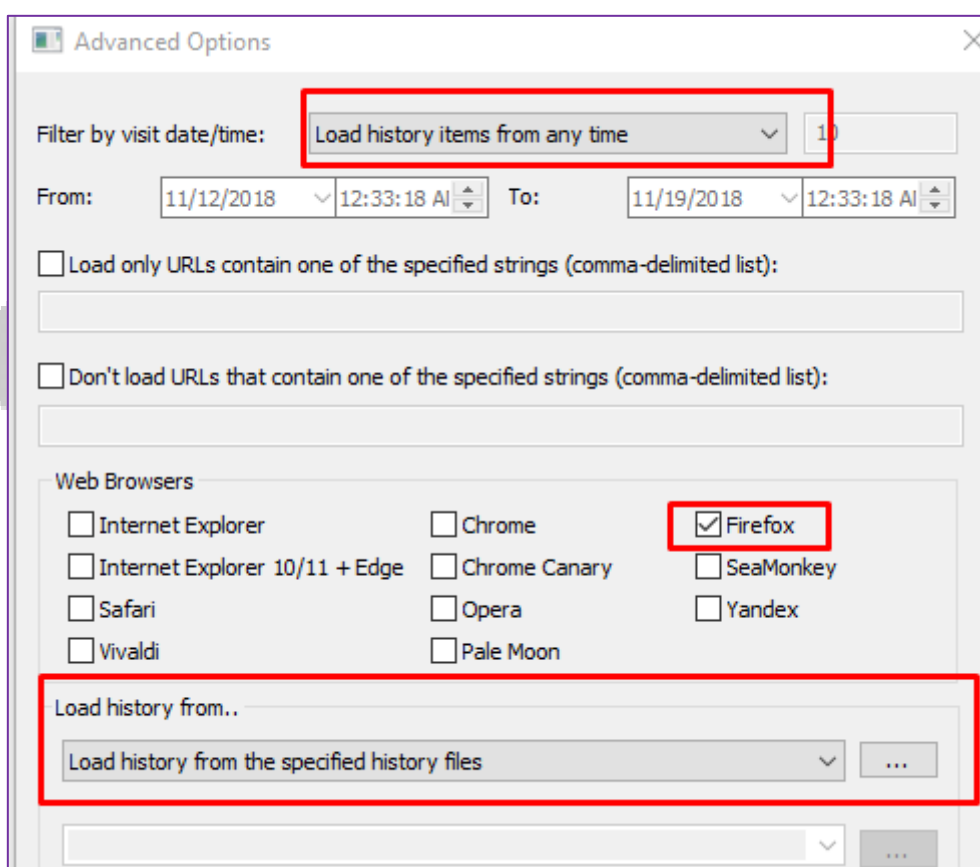
	visit_date	url	title	visit_count	visit_type
1	2018-10-03 17:45:24	https://www.mozilla.org/privacy/firefox/	NULL	1	1
2	2018-10-03 17:45:24	https://www.mozilla.org/es-ES/privacy/firefox/	Aviso de privacidad de Firefox — Mozilla	1	5
3	2018-10-03 17:46:15	https://www.google.com/search?q=dropbox&ie=...	dropbox - Buscar con Google	2	2
4	2018-10-03 17:45:57	https://www.google.com/sorry/index?continue=ht...	https://www.google.com/search?q=dropbox&ie=utf-8&oe=utf-8&client=firefox-b-ab	1	6
5	2018-10-03 17:46:15	https://www.google.com/search?q=dropbox&ie=...	NULL	1	1
6	2018-10-03 17:46:15	https://www.google.com/search?q=dropbox&ie=...	dropbox - Buscar con Google	2	6
7	2018-10-03 17:46:17	https://www.googleadservices.com/pagead/ack?...	NULL	1	1
8	2018-10-03 17:46:18	https://www.dropbox.com/business/landing-t61f?...	Dropbox - Dropbox Business	1	6
9	2018-10-03 17:46:42	https://www.dropbox.com/plans?trigger=sem	Choose the right Dropbox for you and your business	1	1
10	2018-10-03 17:46:59	https://www.dropbox.com/plus	NULL	1	1
11	2018-10-03 17:46:59	https://www.dropbox.com/plus?cid=f321260c1f7f5...	Accede a todas tus cosas en cualquier parte con 1 TB de almacenamiento - Dropbox P...	1	6
12	2018-10-03 17:47:08	https://www.google.com/search?q=dropbox+free...	dropbox free - Buscar con Google	1	2
13	2018-10-03 17:47:11	https://www.dropbox.com/es/	Dropbox	1	1
14	2018-10-03 17:48:22	https://www.dropbox.com/find_plan?signup_tag=i...	Busca el plan de Dropbox apropiado para ti - Dropbox	1	1
15	2018-10-03 17:48:37	https://www.dropbox.com/install?_tk=uj_merlin	Instalar - Dropbox	1	1
16	2018-10-03 17:48:40	https://www.dropbox.com/install?_tk=uj_merlin#d...	Instalar - Dropbox	1	1
17	2018-10-03 17:48:40	https://www.dropbox.com/download?os=win	NULL	1	1
18	2018-10-03 17:48:46	https://dl-web.dropbox.com/installer?authenticod...	DropboxInstaller.exe	0	7
19	2018-10-03 17:48:46	https://dl-web.dropbox.com/installer?authenticod...	DropboxInstaller.exe	0	7
20	2018-10-03 17:52:28	https://www.dropbox.com/complete_setup?plat=...	Te damos la bienvenida a Dropbox - Dropbox	1	1
21	2018-10-03 17:52:49	https://www.dropbox.com/home?client=1	Dropbox	1	1
22	2018-10-03 17:52:51	https://www.dropbox.com/home	Archivos - Dropbox	1	1
23	2018-10-03 18:18:29	https://www.google.com/search?q=nist&ie=utf-8...	nist - Buscar con Google	1	2

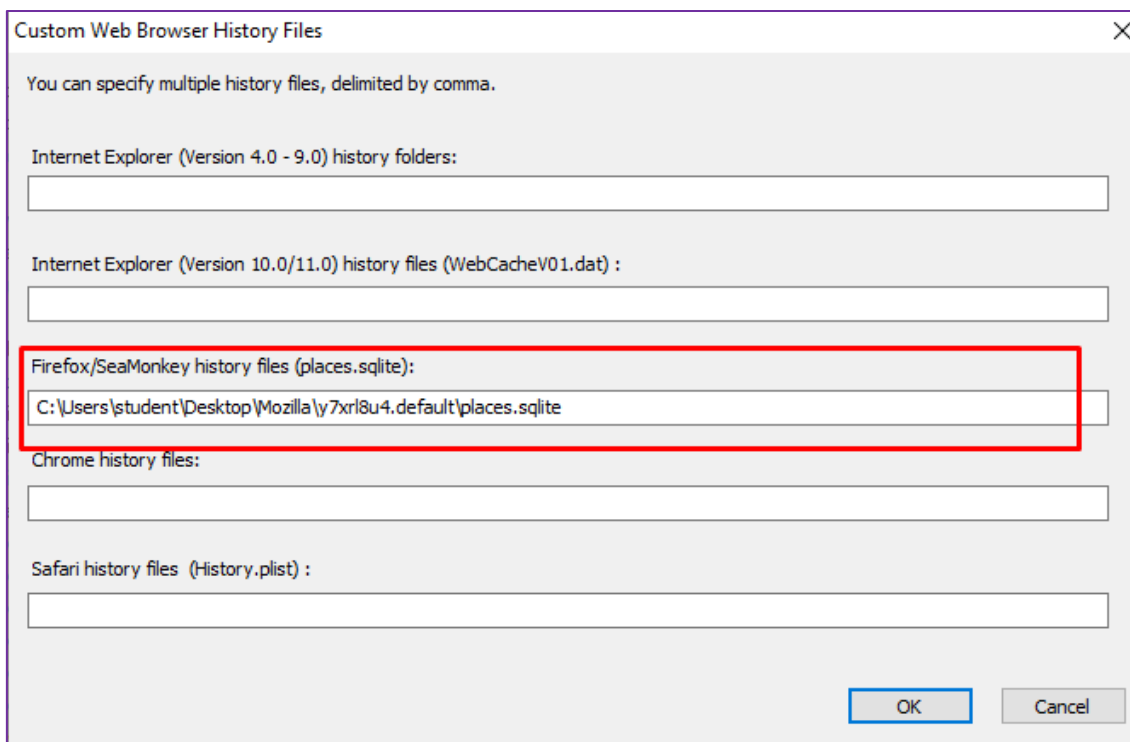
QUANTIKA¹⁴

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

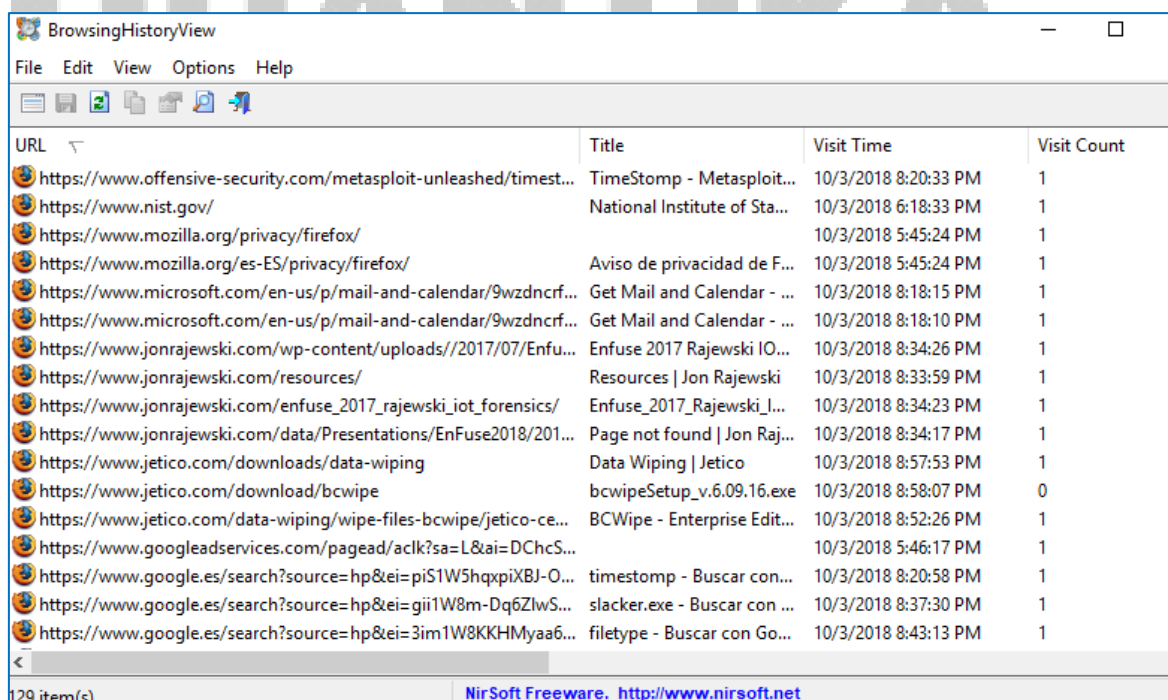
- ◆ 1: el usuario siguió un link
- ◆ 2: el usuario escribió la url
- ◆ 3: el usuario utilizó un favorito
- ◆ 4: fue cargado desde un iframe
- ◆ 5: página accedida debido a HTTP redirect 301
- ◆ 6: página accedida debido a HTTP redirect 302
- ◆ 7: Fichero descargado
- ◆ 8: el usuario siguió un link de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

También podemos utilizar herramienta de Nirsoft Browsing History View, pero en este caso seleccionaremos Firefox y el fichero places.sqlite





QUANTIKA 14



Esta herramienta no indica el tipo de visita.

HISTORIAL DE FICHEROS DESCARGADOS

Seguimos con la base de datos **Places.Sqlite** pero esta vez en la tabla **moz_annos** que contiene las descargas realizadas, por lo que podemos realizar la consulta de esta manera en SQLite Studio:

```
SELECT datetime(lastModified/1000000,'unixepoch') AS
Fecha_Descarga, content as Fichero, url as URL
FROM moz_places, moz_annos
WHERE moz_places.id = moz_annos.place_id
```

Resultado de la query:

Fecha_Descarga	Fichero	URL
2018-10-03 17:48:46	file:///C:/Users/ismis/Downloads/DropboxInstaller.exe	https://dl-web.dropbox.com/installer?authenticcode_sign=True&build_no=58.4.92&juno=True&juno_use_p...
2018-10-03 17:48:46	("state":1,"endTime":1538588926647,"fileSize":696096)	https://dl-web.dropbox.com/installer?authenticcode_sign=True&build_no=58.4.92&juno=True&juno_use_p...
2018-10-03 18:43:02	file:///C:/Users/ismis/Downloads/readerdc_es_xa_crd_install.exe	https://admdownload.adobe.com/bin/live/readerdc_es_xa_crd_install.exe
2018-10-03 18:43:02	("state":1,"endTime":1538592182589,"fileSize":1207800)	https://admdownload.adobe.com/bin/live/readerdc_es_xa_crd_install.exe
2018-10-03 20:06:26	file:///C:/Users/ismis/Downloads/didier.de.saint.pierre.es.ppt	http://www.un.org/en/ecosoc/newfunct/pdf/didier.de.saint.pierre.es.ppt
2018-10-03 20:07:09	("state":1,"endTime":1538597229348,"fileSize":3721216)	http://www.un.org/en/ecosoc/newfunct/pdf/didier.de.saint.pierre.es.ppt
2018-10-03 20:42:26	file:///C:/Users/ismis/Downloads/slacker.exe	https://raw.githubusercontent.com/codejanus/ToolSuite/master/slacker.exe
2018-10-03 20:42:26	("state":1,"endTime":1538599346556,"fileSize":53248)	https://raw.githubusercontent.com/codejanus/ToolSuite/master/slacker.exe
2018-10-03 20:44:17	file:///C:/Users/ismis/OneDrive/Escritorio/Tools/know-your-file-ty...	https://blogmedia.whoishostingthis.com/wp-content/uploads/2014/12/know-your-file-types.jpg
2018-10-03 20:44:17	("state":1,"endTime":1538599457347,"fileSize":117888)	https://blogmedia.whoishostingthis.com/wp-content/uploads/2014/12/know-your-file-types.jpg
2018-10-03 20:58:09	file:///C:/Users/ismis/Downloads/bcwipeSetup_v.6.09.16.exe	https://www.jetico.com/download/bcwipe
2018-10-03 20:58:44	("state":1,"endTime":1538600324024,"fileSize":8342880)	https://www.jetico.com/download/bcwipe

COOKIES

Para extraer las cookies, ahora trabajaremos con la base de datos SQLite **cookies.sqlite**.

Abrimos el programa SQLite Studio, a continuación, pinchamos en "Database->AddDatabase", seleccionamos la ruta donde tenemos el fichero **cookies.sqlite**, desplegamos la base de datos y ya podemos obtener directamente todas las cookies y veremos las siguientes columnas:

- ◆ Name: nombre de la cookie
- ◆ Value: valor que contiene la cookie
- ◆ Host: para que host es la cookie
- ◆ Expiry: cuando expira la cookie
- ◆ lastAccessed: ultimo acceso que el servidor la utilizó (epoch)
- ◆ CreationTime: cuando fue la cookie creada (epoch)
- ◆ isSecure: ¿fue firmada en una conexión segura?

id	baseDomain	ginAttribut	name	value	host
1	mozilla.org		moz-stub-attribution-code	c291cmNPkd3dy5tb3ppbGxhM9yZyZtZWVpdW09KG5vbmUpJmNhbXBhaWduPSHub3Qgc...	www.mozilla.org
2	mozilla.org		moz-stub-attribution-sig	24f20c1791256511cbb5047975f1f4003fc1cb8cd216aba0cb34f9baa206a5f9	www.mozilla.org
3	mozilla.org		_ga	GA1.2.1686524305.1538588728	.mozilla.org
4	mozilla.org		_gid	GA1.2.787796716.1538588728	.mozilla.org
5	mozilla.org		_gat_UA-36116321-1	1	.mozilla.org
11	google.com		GOOGLE_ABUSE_EXEMPTION	ID=e713fb5a7284c3a0:TM=1538588758:C=r:IP=217.182.232.207:-S=APGng0slq3pPewFnndCjv...	.google.com
14	google.com		SNID	ADy17Zx8MpmNVZSuC7x870WXL_XGhVdFjhmVh49aW0Tat0j1Y20aUWjy_taJruuzbZ81ydGTO...	.google.com
19	google.ru		NID	140-ks3JE4VlPu3EazjJm9YR0gWo40_W0oCspQfavSUm6y1B8sHk9WABSDkalprLk3E3xa5FxF...	.google.ru
20	googleservices.com		Conversion	EhM2ub57Onq3QVmfdrCh2qyQw7GAEGsczt4zCpMDIAUgBkAhkkoXthQeYAQCgAQCoA...	www.googleservices.com
21	dropbox.com		traffic_source	c2Vt	.www.dropbox.com
24	dropbox.com		gvc	MTA2NDAwODM0Ng2MTU3MDY0OTkyMjE5ZmZlZmJlMTZc5Mjgy	www.dropbox.com
27	dropboxstatic.com		__cfduid	d8040236d6bed0c193a1eef8d0521d0ee1538588779	.dropboxstatic.com
28	dropbox.com		_gcl_au	1.1.1291265815.1538588780	.dropbox.com
32	mathtag.com		uuid	55c25bb4-f684-4200-9596-46ffb3de4ced	.mathtag.com
33	6sc.co		6suuid	ef497b5c706c00006c00b55b2c030000fb3e0000	.6sc.co
34	dropbox.com		_gd_visitor	660976c9-d13f-4585-8b0f-f19a466d12c0	marketing.dropbox.com
35	dropbox.com		_gd_session	971032d0-83ca-48e2-8717-257039dbd83e	marketing.dropbox.com
37	abmr.net		01AI	2-2-54BAF63583150F61CD8773CAF65430F2C37A86AE45255673A411414B74E1831-9261ECDA...	.abmr.net
39	mathtag.com		uudc	3iv3CIPduwIQInrYpKx0L8Y8eBj8dQzmlj8TUEIFR+M6LBwBDr6UOA22c/kJ5Fud4aszkQ4F...	.mathtag.com
40	dropbox.com		_gd_visitor	ef497b5c706c00006c00b55b2c030000fb3e0000	marketing.dropbox.com
41	dropbox.com		SnapABugRef	https%3A%2F%2Fsnapengage.dropbox.com%2Fbusiness%2Flanding-161f1%3F_ad%3D24466...	.dropbox.com
42	dropbox.com		SnapABugHistory	1#	.dropbox.com
51	doubleclick.net		IDF	AHWqUTnTL778GfMnGNEUo0q6lF5oCVZYH6hFITi6u-6BoX3v-XHpWNxg2yGLj	.doubleclick.net
53	linkedin.com		BizID	2a5054a2-da89-4a42-8be9-4b0b605c5582	.ads.linkedin.com
54	linkedin.com		lidc	"b=VGST07:gb=925:u=1:i=1538588782:t=1538675182:s=AQGCOnX9YlAZkV2Glin49NyR3Jw9f1"	.linkedin.com
55	twitter.com		personalization_id	"v1_XNHDIvYbYHDooQMxtzc5VA=="	.twitter.com
59	linkedin.com		UserMatchHistory	AQIvq1Ayc2upHwAAAVYCa_RRvTdsPv6CjqrSjRlDvXb-7Heph1H6aWg9ghVWZ3bztKG...	.ads.linkedin.com
63	yahoo.co.jp		B	5ah6c7tdra03e8b=38s=bc	.yahoo.co.jp
65	facebook.com		fr	07d7r1aeDSMwmtO7V.BbtQBv...1.0.8btQBv.	.facebook.com
66	linkedin.com		bcookie	"v=2&6b99a71e-d55c-40f0-8164-935015f1c15"	.linkedin.com
67	linkedin.com		bscookie	"v=1&20181003174623b86cd2ca-54e2-4ef4-80ba-5cdf30d9d69aAQG6PKMcIPdqJqQ57Cowl...	.www.linkedin.com
68	mathtag.com		HRL8	3f3G8B7QYFUp29HzeQf5cPo00zXXDuUv4S_BufCdAl22bEkvoTWvSRQ	.mathtag.com
75	bidswitch.net		tuuid	71c08ac4-00e6-4c0f-9808-111e17167277	.bidswitch.net
76	bidswitch.net		tuuid_lu	1538588786	.bidswitch.net
77	bidswitch.net		c	1538588786	.bidswitch.net
79	360yield.com		tuuid	70f8df51-a954-4ec7-9508-cfe7d6406819	ad.360yield.com
80	360yield.com		tuuid_lu	1538588786	ad.360yield.com
83	bluekai.com		bkdc	iad	.bluekai.com
85	pubmatic.com		KRTBCOOKIE_27	16735-uid:55c25bb4-f684-4200-9596-46ffb3de4ced&RTB&23019-uid:55c25bb4-f684-4200-9...	.pubmatic.com
92	360yield.com		um	15,MW5Wt4NcC9gDQVD1UvYDzQvAQNdAAT7vGPIAXvpeJDXSmqCulq.m0mZWvflm-Efs#...	ad.360yield.com
93	360yield.com		umeh	15,0,370039586,-1	ad.360yield.com
95	crwdcntrl.net		_cc_dc	1	.crwdcntrl.net

CACHE

La cache tiene un tamaño aproximado de 350mb y se almacena la siguiente ruta:

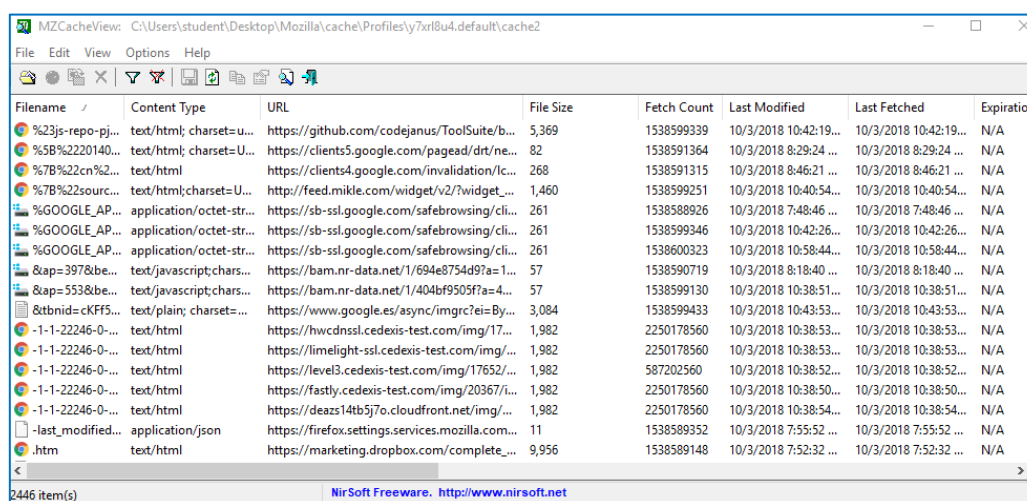
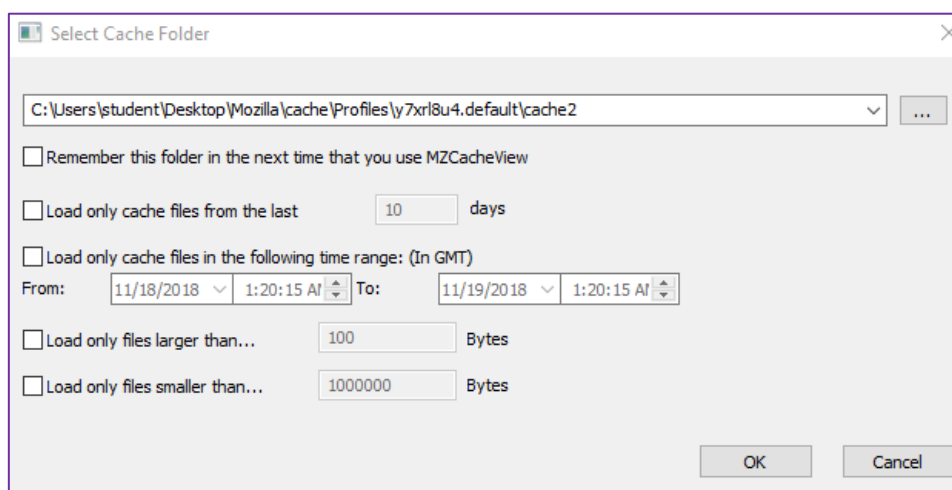
◆ %userprofile%\Appdata\Local\Mozilla\Firefox\Profiles\<random>.default\Cache2

Los formatos de fichero tienen la siguiente cabecera y se encuentra en \Cache2\entries

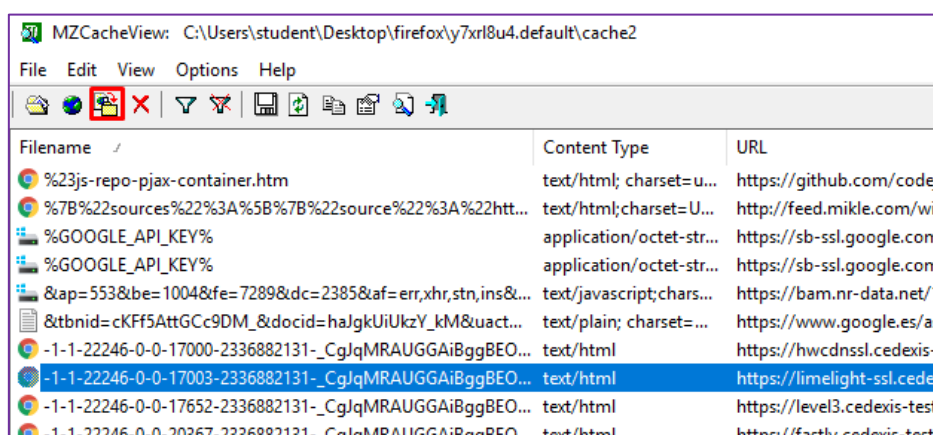
47	49	46	38	39	61	01	00	01	00	80	00	00	E0	E0	E0	GIF89a....€..ààà
00	00	00	21	F9	04	01	00	00	00	00	2C	00	00	00	00	...!u.....,
01	00	01	00	00	02	02	44	01	00	3B	B5	0D	E8	A1	EBD.:;u.è;ë
EC	00	00	00	03	00	00	00	01	5B	9B	E7	04	5B	9B	E7	ì.....[>ç.[>ç
04	3F	7F	9E	BA	00	00	00	00	00	00	01	C8	00	00	00	.?.ž°.....È...
00	3A	68	74	74	70	3A	2F	2F	61	6E	61	70	69	78	65	.:http://anapixe
6C	2E	65	6C	6D	75	6E	64	6F	2E	65	73	2F	74	65	72	l.elmundo.es/ter
2E	67	69	66	3F	63	61	6D	70	61	69	67	6E	3D	7A	7A	.gif?campaign=zz
5F	62	69	67	64	61	74	61	26	67	72	6F	75	70	3D	7A	_bigdata&group=z
7A	5F	62	69	67	64	61	74	61	26	70	61	67	65	3D	7A	z_bigdata&page=z
7A	5F	62	69	67	64	61	74	61	26	63	72	65	61	74	69	z_bigdata&creati
76	69	74	79	3D	7A	7A	5F	62	69	67	64	61	74	61	26	vity=zz_bigdata&
65	65	64	70	61	72	74	60	61	6C	74	60	6D	65	73	74	ondpartialtime

Al tener una cabecera conocida "GIF89a", se podría recuperar mediante técnicas de Carving.

Para abrir los ficheros cache, vamos a utilizar la herramienta **MozillaCacheView** y vamos a indicarle mediante "File -> Select Cache Folder" y seleccionamos la carpeta "Cache2" del profile.



La herramienta permite extraer los ficheros, pulsando en el botón en rojo:



¿Qué Podemos obtener de aquí?

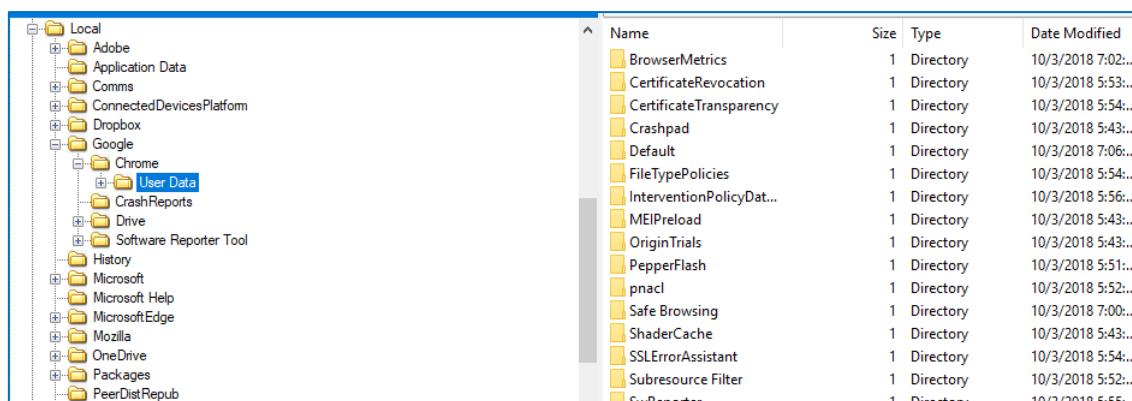
- ◆ URL: cual fue la web que tenía el contenido
- ◆ Fetch Count: que frecuencia es usado el contenido cacheado
- ◆ Filename: nombre del fichero cacheado
- ◆ Content Type: tipo del fichero cacheado
- ◆ File Size: tamaño del fichero cacheado
- ◆ Last modified time: última vez que el contenido fue almacenado en la cache (se puede seleccionar en las opciones para verlo en UTC)
- ◆ Last Fetched Time: cuando fue por última vez visitada la cache (se puede seleccionar en las opciones para verlo en UTC)
- ◆ Server Last Modified: indica cuando el contenido en el servidor fue cambiado
- ◆ Server Response: código HTTP de respuesta del servidor.

**Ver video: 002/MÓD. 6 -Firefox*

CHROME

Chrome es otro de los navegadores a tener en cuenta para realizar una investigación forense. Su información es organizada en un perfil, como hace Firefox, pero Chrome lo almacena en la siguiente ruta:

- ◆ **%UserProfile%\AppData\Local\Google\Chrome\User Data\Default**



HISTORIAL DE NAVEGACIÓN

El primer paso que tenemos que hacer, es obtener el fichero **History** que se encuentra dentro del perfil visto anteriormente. Este fichero es una base de datos SQLITE que podremos analizar con la herramienta que hemos visto: SQLITE Studio

El historial lo podremos encontrar en las tablas:

- ◆ **Urls**
- ◆ **Visits**

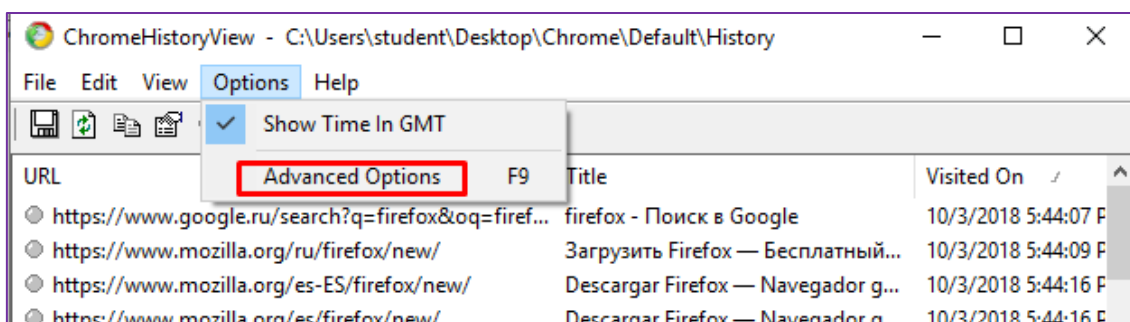
Podemos lanzar la siguiente query, que nos devolverá los visitas en UTC:

```
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
```

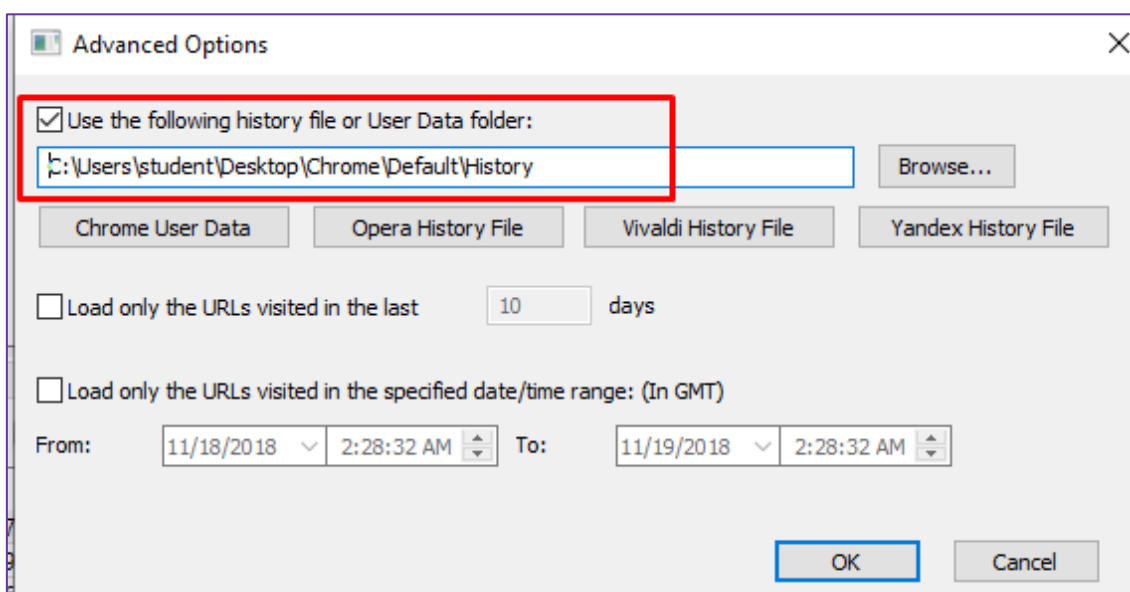
Resultado de la query;

ultima_visita	url	title	typed_count	transition
2018-10-03 17:44:07	https://www.google.ru/search?q=firefox&aq=firefox&aqs=chrome..69l57j0l5.5843j0j4&sourceid=ch...	firefox - Поиск в Google	0	838860805
2018-10-03 17:44:09	https://www.mozilla.org/ru/firefox/new/	Загрузить Firefox — Бесплатный веб-браузер	0	805306368
2018-10-03 17:44:16	https://www.mozilla.org/es-es/firefox/new/	Descargar Firefox — Navegador gratuito	1	268435457
2018-10-03 17:44:16	https://www.mozilla.org/es-ES/firefox/new/	Descargar Firefox — Navegador gratuito	0	-1610612735
2018-10-03 17:44:18	https://www.mozilla.org/es-ES/firefox/download/thanks/	Descargar Firefox — Navegador gratuito	0	1610612736
2018-10-03 17:55:22	https://accounts.google.com/signin/chrome/sync?ssp=1&continue=https%3A%2F%2Fwww.googl...	Inicia sesión: Cuentas de Google	0	805306370
2018-10-03 17:55:22	https://accounts.google.com/signin/chrome/sync?ssp=1&continue=https%3A%2F%2Fwww.googl...	Inicia sesión: Cuentas de Google	0	805306368
2018-10-03 17:55:22	https://accounts.google.com/signin/chrome/sync?ssp=1&continue=https%3A%2F%2Fwww.googl...	Inicia sesión: Cuentas de Google	0	805306368
2018-10-03 17:55:22	https://accounts.google.com/signin/chrome/sync/identifier?ssp=1&continue=https%3A%2F%2Fw...	Inicia sesión: Cuentas de Google	0	805306368
2018-10-03 17:56:48	http://www.gmail.com/	Gmail: espacio de almacenamiento y correo gratuitos de Google	0	268435457
2018-10-03 17:56:48	https://www.gmail.com/	Gmail: espacio de almacenamiento y correo gratuitos de Google	1	-2147483647
2018-10-03 17:56:48	https://www.google.com/gmail/	Gmail: espacio de almacenamiento y correo gratuitos de Google	0	-2147483647
2018-10-03 17:56:48	https://mail.google.com/mail/	Gmail: espacio de almacenamiento y correo gratuitos de Google	0	-2147483647
2018-10-03 17:56:48	https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&continue=https...	Gmail: espacio de almacenamiento y correo gratuitos de Google	0	-2147483647
2018-10-03 17:56:48	https://mail.google.com/intl/es/mail/help/about.html#	Gmail: espacio de almacenamiento y correo gratuitos de Google	0	-2147483647
2018-10-03 17:56:48	https://www.google.com/intl/es/mail/help/about.html#	Gmail: espacio de almacenamiento y correo gratuitos de Google	0	-2147483647
2018-10-03 17:56:48	https://www.google.com/intl/es/gmail/about/#	Gmail: espacio de almacenamiento y correo gratuitos de Google	0	-1610612735
2018-10-03 17:56:51	https://accounts.google.com/AccountChooser?service=mail&continue=https://mail.google.com/...	Gmail	0	268435456
2018-10-03 17:56:52	https://accounts.google.com/ServiceLogin?continue=https%3A%2F%2Fmail.google.com%2Fmail%...	Gmail	0	-1610612736
2018-10-03 17:56:52	https://accounts.google.com/ServiceLogin?continue=https%3A%2F%2Fmail.google.com%2Fmail%...	Gmail	0	805306368
2018-10-03 17:56:52	https://accounts.google.com/ServiceLogin?continue=https%3A%2F%2Fmail.google.com%2Fmail%...	Gmail	0	805306368

También podríamos utilizar la herramienta de Nirsoft Chrome History View, que nos permite seleccionar directamente la base de datos Sqlite, en “Options -> Advanced Options”



Seleccionamos la base de datos History:



Resultado de abrir con ChromeHistoryView:



ChromeHistoryView - C:\Users\student\Desktop\Chrome\Default\History

File Edit View Options Help

URL	Title	Visited On
https://www.google.ru/search?q=firefox&oq=firef...	firefox - Поиск в Google	10/3/2018 5:44:07 PM
https://www.mozilla.org/ru/firefox/new/	Загрузить Firefox — Бесплатный...	10/3/2018 5:44:09 PM
https://www.mozilla.org/es/firefox/new/	Descargar Firefox — Navegador g...	10/3/2018 5:44:16 PM
https://www.mozilla.org/es-ES/firefox/new/	Descargar Firefox — Navegador g...	10/3/2018 5:44:16 PM
https://www.mozilla.org/es-ES/firefox/download/t...	Descargar Firefox — Navegador g...	10/3/2018 5:44:18 PM
https://accounts.google.com/signin/chrome/sync...	Inicia sesión: Cuentas de Google	10/3/2018 5:55:22 PM
https://accounts.google.com/signin/chrome/sync...	Inicia sesión: Cuentas de Google	10/3/2018 5:55:22 PM
https://accounts.google.com/signin/chrome/sync...	Inicia sesión: Cuentas de Google	10/3/2018 5:55:22 PM
https://accounts.google.com/signin/chrome/sync...	Inicia sesión: Cuentas de Google	10/3/2018 5:55:22 PM
http://www.gmail.com/	Gmail: espacio de almacenamient...	10/3/2018 5:56:48 PM
https://www.gmail.com/	Gmail: espacio de almacenamient...	10/3/2018 5:56:48 PM
https://www.google.com/gmail/	Gmail: espacio de almacenamient...	10/3/2018 5:56:48 PM
https://mail.google.com/mail/	Gmail: espacio de almacenamient...	10/3/2018 5:56:48 PM
https://accounts.google.com/ServiceLogin?servic...	Gmail: espacio de almacenamient...	10/3/2018 5:56:48 PM
https://mail.google.com/intl/es/mail/help/about....	Gmail: espacio de almacenamient...	10/3/2018 5:56:48 PM
https://www.google.com/intl/es/mail/help/about....	Gmail: espacio de almacenamient...	10/3/2018 5:56:48 PM
https://www.google.com/intl/es/gmail/about/#	Gmail: espacio de almacenamient...	10/3/2018 5:56:48 PM

<

QUANTIKA¹⁴

Hay una columna muy parecida a la que vimos en Firefox, para identificar de donde provenía la navegación, el campo “Transition Type”:

Visit ID	Profile	URL Length	Transition Type	Transition Qualifiers
1	Default	105	Generated	Chain Start,Chain End
2	Default	39	Link	Chain Start,Chain End
3	Default	39	Typed	Chain Start
4	Default	42	Typed	Chain End,Server Redirect
5	Default	54	Link	Chain End,Client Redirect
6	Default	92	Auto Bookmark	Chain Start,Chain End
7	Default	92	Link	Chain Start,Chain End
8	Default	92	Link	Chain Start,Chain End
9	Default	134	Link	Chain Start,Chain End
10	Default	21	Typed	Chain Start
11	Default	22	Typed	Server Redirect
12	Default	29	Typed	Server Redirect
13	Default	29	Typed	Server Redirect
14	Default	166	Typed	Server Redirect
15	Default	53	Typed	Server Redirect
16	Default	52	Typed	Server Redirect
17	Default	44	Typed	Chain End,Server Redirect

Tipos de Transition Type:

- ◆ **Link:** usuario ha clickado un link
- ◆ **Typed:** la url ha sido escrita en la url
- ◆ **Auto Bookmark:** sugerido por Chrome
- ◆ **Auto Subframe:** Anuncio
- ◆ **Start Page:** home page
- ◆ **Form Submit:** el usuario insertó información
- ◆ **Reloade:** página recargada



HISTORIAL DE FICHEROS DESCARGADOS

Se encuentran dentro de la misma base de datos “History” pero en la tabla “downloads”

History (SQLite3)		
<div> <div>Tables (11)</div> <ul style="list-style-type: none"> downloads downloads_slices downloads_url_chains keyword_search_terms meta segment_usage segments typed_url_sync_metadata urls visit_source visits Views </div>		
id	guid	current_path
1	3b008a1a-4eb4-463c-ae4f-62442c74e404	C:\Users\student\Desktop\cyberchef.htm
2	584cc71e-099f-4df4-9117-78551a54fc7c	C:\Users\student\Downloads\Unconfirmed 581577.crdownload
3	4c40b192-81fa-4196-95e2-44961f1a8001	C:\Users\student\Downloads\010EditorWin64Installer801.exe
4	7da7ac82-66be-4a4b-b80d-2355cbff22c	
5	3e850725-22a2-4bd8-9dc9-122df4dbb8d7	C:\Users\student\Downloads\HxDSetup.zip
6	6d42b1b8-24bf-47fb-828d-141fd2a11477	C:\Users\student\Downloads\npp.7.5.8.Installer.exe
7	9dd8a4ff-3327-46ff-bb42-fa33fc47a9f0	
8	3519d567-f04b-4948-a29d-f40ff594d8c	C:\Users\student\Downloads\vccredist_x64.exe
9	c698b096-37ee-4772-b2d5-d2324b660880	C:\Users\student\Downloads\adobe.exe
10	7b6c194f-6759-4c72-a3b7-7c4d901d15f3	C:\Users\student\Downloads\Apache_OpenOffice_4.1.5_Win_x86_install_es.exe
11	0b27fd8a-c950-4187-8b66-b12a91d5e3a5	C:\Users\student\Downloads\readerdc_en_xa_crd_install.exe
12	019484d0-7396-4069-8fc2-44ab6aa74c1f	C:\Users\student\Downloads\jre-8u181-windows-x64.exe
13	ed9f1033-9ab6-4022-b469-0ad35dd2d8c3	C:\Users\student\Downloads\autopsy-4.9.0-64bit.msi
14	b6be5bdb-6d1f-4398-8b7f-0e344f10fa26	C:\Users\student\Downloads\python-2.7.15.amd64.msi
15	d990e219-2ad3-4ec5-9cd1-c9041e706862	C:\Digital Forensics\Applications\recentfilecache-parser-master.zip
16	673cb67d-91c1-4505-8ce8-f599d793f46f	C:\Users\student\Desktop\New folder\recentfilecache-parser-master (1).zip
17	0aea6394-0bde-493e-8bf5-c6615e930a2c	C:\Users\student\Downloads\bulk_extractor-1.6.0-dev-rec03-windowsinstaller_x64.exe
18	11e1245a-7a3d-45b6-bba7-90e615a0188b	C:\Users\student\Downloads\fulleventlogview-x64.zip
19	40800c7a-75e7-40e9-b1e7-2f38040a9129	C:\Users\student\Desktop\Mozilla\mzcv-x64.zip
20	aee6126-b39a-49f9-b426-14a256121673	C:\Users\student\Desktop\Chrome\chromecookiesview.zip

Dispone de las siguientes columnas:

- ◆ Ruta del fichero donde se guarda
- ◆ Tamaño del fichero (total_bytes)
- ◆ Fecha de cuando comenzó la descarga (start_time)
- ◆ Fecha de cuando terminó la descarga (end_time)
- ◆ Referer
- ◆ URL de descarga
- ◆ Tipo de fichero (mime_type)

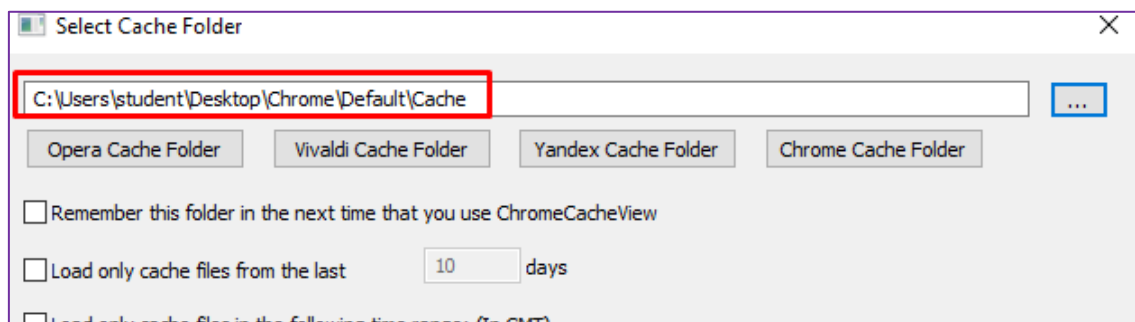
CACHE

La cache de Chrome se encuentra en la siguiente ruta:

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

\$I30	96	NTFS Index All...	10/3/2018 7:04:...
data_0	80	Regular File	10/3/2018 7:07:...
data_0.FileSlack	20	File Slack	
data_1	776	Regular File	10/3/2018 7:07:...
data_1.FileSlack	36	File Slack	
data_2	2,056	Regular File	10/3/2018 7:07:...
data_2.FileSlack	148	File Slack	
data_3	16,392	Regular File	10/3/2018 7:04:...
data_3.FileSlack	4,040	File Slack	
f_000001	17	Regular File	10/3/2018 5:44:...
f_000001.FileSlack	4	File Slack	
f_000002	117	Regular File	10/3/2018 5:44:...
f_000002.FileSlack	4	File Slack	
f_000003	153	Regular File	10/3/2018 5:44:...
f_000004	76	Regular File	10/3/2018 5:44:...
f_000005	47	Regular File	10/3/2018 5:44:...
f_000005.FileSlack	2	File Slack	
f_000006	48	Regular File	10/3/2018 5:44:...
f_000006.FileSlack	1	File Slack	
f_000007	67	Regular File	10/3/2018 5:44:...
f_000007.FileSlack	2	File Slack	
f_000008	38	Regular File	10/3/2018 5:44:...
f_000008.FileSlack	3	File Slack	
f_000009	47	Regular File	10/3/2018 5:44:...
f_000009.FileSlack	2	File Slack	
f_000010	52	Regular File	10/3/2018 5:44:...

Para analizar la Cache, utilizaremos la herramienta de Nirsoft Chrome CacheView, pinchando en "File-> Select Cache Folder":

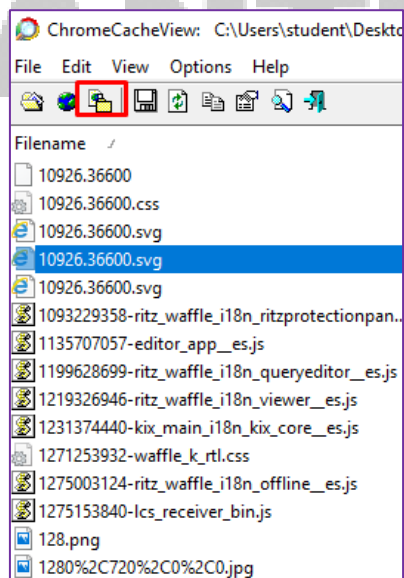


ChromeCacheView: C:\Users\student\Desktop\Chrome\Default\Cache

File Edit View Options Help

Filename	URL	Content Type
%5B%2220140509-01%22%2Cnull%2C0%5D.h...	https://clients5.google.com/pagead/drt/ne?di=%5B%2220140509-01...	text/html
&atyp=i&biw=1024&bih=657&ei=3Am1W7z...	https://www.google.ru/client_204?&atyp=i&biw=1024&bih=657&ei...	text/html
&atyp=i&biw=1024&bih=657&ei=5Am1W_G...	https://www.google.es/client_204?&atyp=i&biw=1024&bih=657&ei...	text/html
&atyp=i&biw=1920&bih=921&ei=bxG1W5S8...	https://www.google.es/client_204?&atyp=i&biw=1920&bih=921&ei...	text/html
&atyp=i&biw=1920&bih=969&ei=gAS1W-j5F...	https://www.google.ru/client_204?&atyp=i&biw=1920&bih=969&ei...	text/html
&atyp=i&biw=1920&bih=969&ei=hxK1W8b0...	https://www.google.ru/client_204?&atyp=i&biw=1920&bih=969&ei...	text/html
&atyp=i&biw=1920&bih=969&ei=YhK1W4vD...	https://www.google.es/client_204?&atyp=i&biw=1920&bih=969&ei...	text/html
&atyp=i&biw=1920&bih=969&ei=zQS1W4P8...	https://www.google.es/client_204?&atyp=i&biw=1920&bih=969&ei...	text/html
&atyp=i&biw=988&bih=620&ei=5_-0W4q2G...	https://www.google.ru/client_204?&atyp=i&biw=988&bih=620&ei=...	text/html
-638352429.jpg	https://avatar.skype.com/v1/avatars/juan_manuel_martinez_alcala?a...	image/jpeg
.	https://skyapi.onedrive.live.com/xmlproxy.js?	text/javascript
.htm	https://docs.google.com/offline/extension/frame?ouid=	text/html
0.htm	https://docs.google.com/presentation/u/0/preload?authuser=0	text/html
0.htm	https://docs.google.com/drawings/u/0/preload?authuser=0	text/html
0.htm	https://docs.google.com/document/u/0/preload?authuser=0	text/html
0.htm	https://drive.google.com/file/u/0/preload?authuser=0	text/html
0.htm	https://docs.google.com/spreadsheets/u/0/preload?authuser=0	text/html

Podemos exportar la cache pinchando en el botón en rojo:

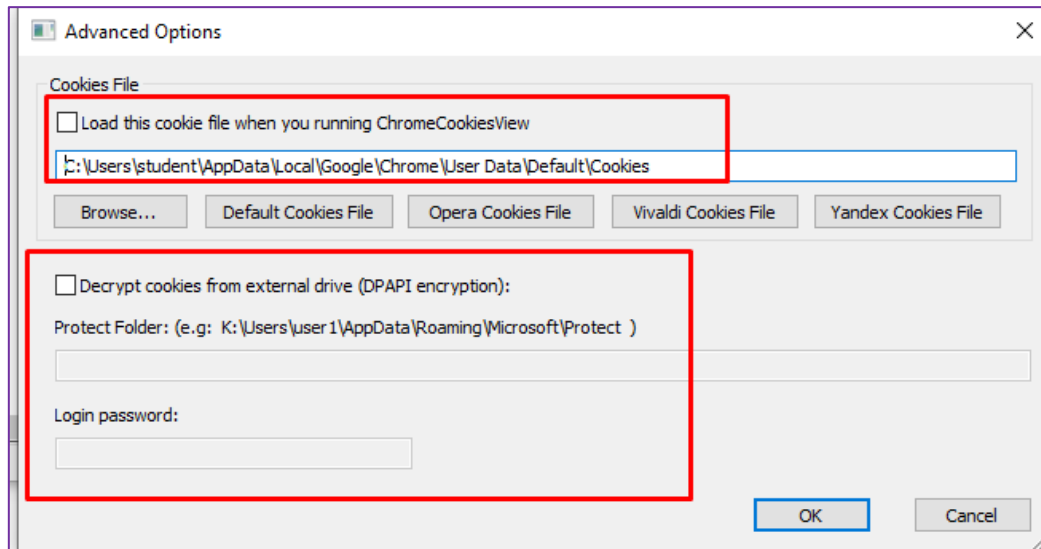


COOKIE

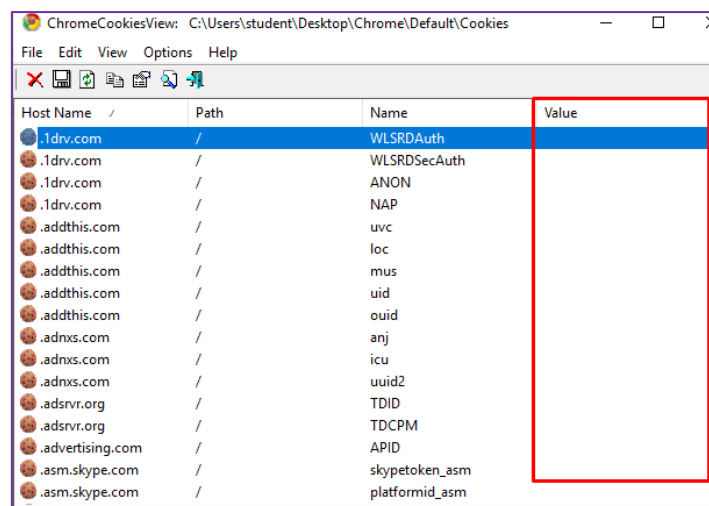
El fichero que contiene las cookies, es nuevamente una base de datos SQLITE que se encuentra en el perfil de Chrome

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

Vamos a utilizar ChromeCookies view para analizarlas, para ello seleccionaremos en Options y nos aparecerá la siguiente pantalla:



En la primera sección deberemos insertar la base de datos y en la segunda parte nos pide las credenciales de Windows del usuario que utilizó Chrome y la carpeta protect. Si no lo insertamos nos aparecerán las cookies sin valor como en la siguiente captura:

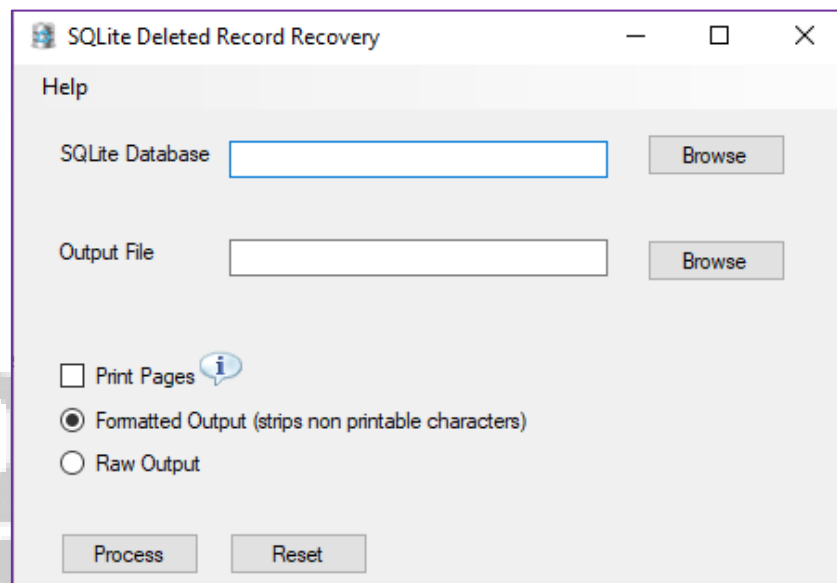


**Ver video: 003/MÓD. 6 -Chrome*

RECUPERANDO REGISTROS BASES DE DATOS SQLITE

Como hemos visto tanto para Firefox como para Chrome, el funcionamiento de almacenar el historial y las descargas está basado en SQLITE.

Los registros que sean borrados de una tabla dentro de una base de datos se pueden recuperar con la herramienta sqlparse_GUI



Tan solo habría que proporcionarle la base de datos SQLITE e indicarle un fichero de salida donde se guardaran los registros que haya podido encontrar. El éxito de la recuperación vendrá dado por el uso del browser sobre la base de datos y sobre el comando vacuum.

Más información del comando vacuum:

<https://people.cs.umass.edu/~mikkau/assets/pubs/sigmod2007LMS/stahlberg07forensicDB.pdf>

**Ver Video: 004/MÓD. 6 -Sqlite*