

Análisis Forense Windows

Este va a ser un taller para obtener información de windows

Análisis Forense Windows

Este va a ser un taller para obtener información de windows

Podremos encontrar la cookies del ordenador

Lo primero será ejecutar una consola de Windows y desde la raiz de C con el comando:

```
dir cookie*.**.* /s/p
```

Usualmente tendremos bastantes cookies y por lo tanto buscaremos las que no interesen. En mi caso utilizaré las de Google Chrome.

```
Directorio de C:\Users\betog\AppData\Local\Google\Chrome\User Data\Default\Extensions\ahmpjcflkgiildlgicmcieglgoilbfdp
.0.57_0
                             942 cookiemgr.js
1/10/2019 13:08
              1 archivos
                                      942 bytes
Directorio de C:\Users\betog\AppData\Local\Google\Chrome\User Data\Default\Extensions\oocalimimngaihdkbihfgmpkcpnmlaoa
.1.0_0\img\icons\General
              :15 3.296 Cookie.svg
1 archivos 3.206 b.
3/02/2023 13:15
Directorio de C:\Users\betog\AppData\Local\Google\Chrome\User Data\Default\Network
5/04/2023 21:20
5/04/2023 21:20
                        1.507.328 Cookies
                                 0 Cookies-journal
             1:20 0 Cookies-jo
2 archivos 1.507.328 bytes
esione una tecla para continuar . .
Directorio de C:\Users\betog\AppData\Local\Google\Chrome\User Data\Guest Profile\Network
```

Podremos entrar a ese directorio en donde habrá un archivo cookies que podremos pasar por un desempaquetador online

https://filext.com/online-file-viewer.html.

```
cookies (3243 rows)
  SELECT * FROM 'cookies' where host_key LIKE "%drop%"
creation utc
                   host key
                                    top frame site key
                                                      name
                                                                          valu
13317924723447916 www.dropbox.com
                                                       __Host-js_csrf
13317924722868336 www.dropbox.com
                                                       gvc
13317924722830248 .dropbox.com
                                                       locale
13317924723447816 .dropbox.com
13322220966519260 .pxdrop.lijit.com
                                                       lijitPage_14day_c026
```

Con esa sentencia podremos buscar cualquier página o lugar.

SITIOS DONDE SE HAN NAVEGADO

```
dir index.dat /s /p /a
```

Se podría utilizar el mismo proceso anterior.

APLICACIONES QUE SE HAN EJECUTADO

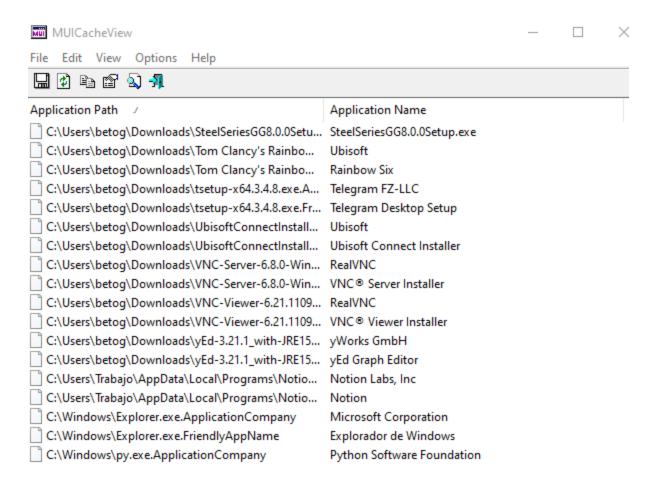
```
dir *.pf /s /a
```

Mostrará un listado de todos lo programas ejecutados.

MUICacheView

https://www.nirsoft.net/utils/muicache view.html

Una vez decargada la abriremos.



Aquí podremos ver todos los programas ejecutados desde el primer uso.

Ver todas las imágenes borradas

dir thumb*.db /s /p /a

```
\>dir thumb*.db /s /p /a
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: C201-A643
Directorio de C:\Users\betog\AppData\Local\Microsoft\Windows\Explorer
25/04/2023 19:38
                                              24 thumbcache 1280.db
25/04/2023 19:38 1.048.576 thumbcache_1260.db

25/04/2023 19:38 24 thumbcache_1920.db

25/04/2023 19:38 1.048.576 thumbcache_256.db

25/04/2023 19:38 1.048.576 thumbcache_2560.db

25/04/2023 19:38 1.048.576 thumbcache_32.db
1.048.576 thumbcache_32.db

25/04/2023 19:38 1.048.576 thumbcache_48.db

25/04/2023 19:38 1.048.576 thumbcache_768.db

25/04/2023 19:38 1.048.576 thumbcache_96.db

25/04/2023 19:38 24 thumbcache custom
                                             24 thumbcache_custom_stream.db
                                          24 thumbcache_exif.db
25/04/2023 19:38
                                     14.688 thumbcache idx.db
25/04/2023 19:38
25/04/2023 19:38
25/04/2023 19:38
25/04/2023 19:38
                                           24 thumbcache_sr.db
                                           24 thumbcache_wide.db
                                             24 thumbcache wide alternate.db
                   15 archivos 7.354.888 bytes
Directorio de C:\Users\betog\Documents\Clase\Lenguaje Marcas\ejercicio_maquetacion\media
23/07/2014 04:24
                                        25.088 Thumbs.db
                    1 archivos
                                             25.088 bytes
Directorio de C:\Users\Trabajo\AppData\Local\Microsoft\Windows\Explorer
```

Con una aplicación con WFA podremos abrir el archivo y ver su contenido.

Capturar toda la memoria

Descargando DumpIt podremos ver la memoria. La ejecutamos esperamos y usamos una herramienta de analizado de volcado de datos.

Volcado de memoria de paginacion

Instalaremos ShadowCopy: http://shadowcopy.findmysoft.com/.

Ver usuarios logeados

Con PsLogedOn ejectuado desde cmd. https://learn.microsoft.com/es-es/sysinternals/downloads/psloggedon

Podremos encontrar la cookies del ordenador

Lo primero será ejecutar una consola de Windows y desde la raiz de C

Con el comando:

```
dir cookie*.*. /s/p
```

Usualmente tendremos bastantes cookies y por lo tanto buscaremos las que no interesen

En mi caso utilizaré las de Google Chrome

Podremos entrar a ese directorio en donde habrá un archivo cookies que podremos pasar por un desempaquetador online https://filext.com/online-file-viewer.html

cookies (3243 rows) SELECT * FROM 'cookies' where host_key LIKE "%drop%" creation utc host key top frame site key name valu 13317924723447916 www.dropbox.com Host-js csrf 13317924722868336 www.dropbox.com qvc 13317924722830248 .dropbox.com locale 13317924723447816 .dropbox.com 13322220966519260 .pxdrop.lijit.com lijitPage 14day c026

Con esa sentencia podremos buscar cualquier página o lugar

SITIOS DONDE SE HAN NAVEGADO

dir index.dat /s /p /a Se podría utilizar el mismo proceso anterior

APLICACIONES QUE SE HAN EJECUTADO

dir *.pf /s /a

Mostrará un listado de todos lo programas ejecutados

MUICacheView

https://www.nirsoft.net/utils/muicache view.html

Una vez decargada la abriremos

MUICacheView	- □ ×
File Edit View Options Help	
Application Path /	Application Name
C:\Users\betog\Downloads\SteelSeriesGG8.0.0Setu	SteelSeriesGG8.0.0Setup.exe
C:\Users\betog\Downloads\Tom Clancy's Rainbo	Ubisoft
C:\Users\betog\Downloads\Tom Clancy's Rainbo	Rainbow Six
C:\Users\betog\Downloads\tsetup-x64.3.4.8.exe.A	Telegram FZ-LLC
C:\Users\betog\Downloads\tsetup-x64.3.4.8.exe.Fr	Telegram Desktop Setup
C:\Users\betog\Downloads\UbisoftConnectInstall	Ubisoft
C:\Users\betog\Downloads\UbisoftConnectInstall	Ubisoft Connect Installer
C:\Users\betog\Downloads\VNC-Server-6.8.0-Win	RealVNC
C:\Users\betog\Downloads\VNC-Server-6.8.0-Win	VNC® Server Installer
C:\Users\betog\Downloads\VNC-Viewer-6.21.1109	RealVNC
C:\Users\betog\Downloads\VNC-Viewer-6.21.1109	VNC® Viewer Installer
C:\Users\betog\Downloads\yEd-3.21.1_with-JRE15	yWorks GmbH
C:\Users\betog\Downloads\yEd-3.21.1_with-JRE15	yEd Graph Editor
C:\Users\Trabajo\AppData\Local\Programs\Notio	Notion Labs, Inc
C:\Users\Trabajo\AppData\Local\Programs\Notio	Notion
C:\Windows\Explorer.exe.ApplicationCompany	Microsoft Corporation
C:\Windows\Explorer.exe.FriendlyAppName	Explorador de Windows
C:\Windows\py.exe.ApplicationCompany	Python Software Foundation

Aquí podremos ver todos los programas ejecutados desde el primer uso

Ver todas las imágenes borradas

dir thumb*.db /s /p /a

```
:\>dir thumb*.db /s /p /a
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: C201-A643
 Directorio de C:\Users\betog\AppData\Local\Microsoft\Windows\Explorer
25/04/2023 19:38 24 thumbcache_1280.db

25/04/2023 19:38 1.048.576 thumbcache_16.db

25/04/2023 19:38 24 thumbcache_1920.db

25/04/2023 19:38 1.048.576 thumbcache_256.db

25/04/2023 19:38 1.048.576 thumbcache_2560.db

25/04/2023 19:38 1.048.576 thumbcache_32.db

25/04/2023 19:38 1.048.576 thumbcache_48.db

25/04/2023 19:38 1.048.576 thumbcache_768.db

25/04/2023 19:38 1.048.576 thumbcache_96.db

25/04/2023 19:38 24 thumbcache_custom_s
25/04/2023 19:38
                                                     24 thumbcache_1280.db
                                                    24 thumbcache_custom_stream.db
                                                   24 thumbcache_exif.db
 25/04/2023 19:38
25/04/2023 19:38
25/04/2023 19:38
25/04/2023 19:38
25/04/2023 19:38
                                           14.688 thumbcache_idx.db
                                                  24 thumbcache_sr.db
                                                  24 thumbcache_wide.db
24 thumbcache_wide_alternate.db
                      15 archivos 7.354.888 bytes
 Directorio de C:\Users\betog\Documents\Clase\Lenguaje Marcas\ejercicio_maquetacion\media
23/07/2014 04:24
                                              25.088 Thumbs.db
                        1 archivos
                                                    25.088 bytes
 Directorio de C:\Users\Trabajo\AppData\Local\Microsoft\Windows\Explorer
```

Con una aplicación con WFA podremos abrir el archivo y ver su contenido

Capturar toda la memoria

Descargando DumpIt podremos ver la memoria

La ejecutamos esperamos y usamos una herramienta de analizado de volcado de datos

Volcado de memoria de paginacion

Instalaremos ShadowCopy

http://shadowcopy.findmysoft.com/

Ver usuarios logeados

Con PsLogedOn ejectuado desde cmd

https://learn.microsoft.com/eses/sysinternals/downloads/psloggedon

```
C:\Users\betog\Desktop>PsLoggedon.exe

PsLoggedon v1.35 - See who's logged on
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
25/04/2023 19:36:41 DESKTOP-3PN0T45\betog
<unknown time> NT SERVICE\MariaDB

Users\betog\Desktop>_
C:\Users\betog\Desktop>_
```