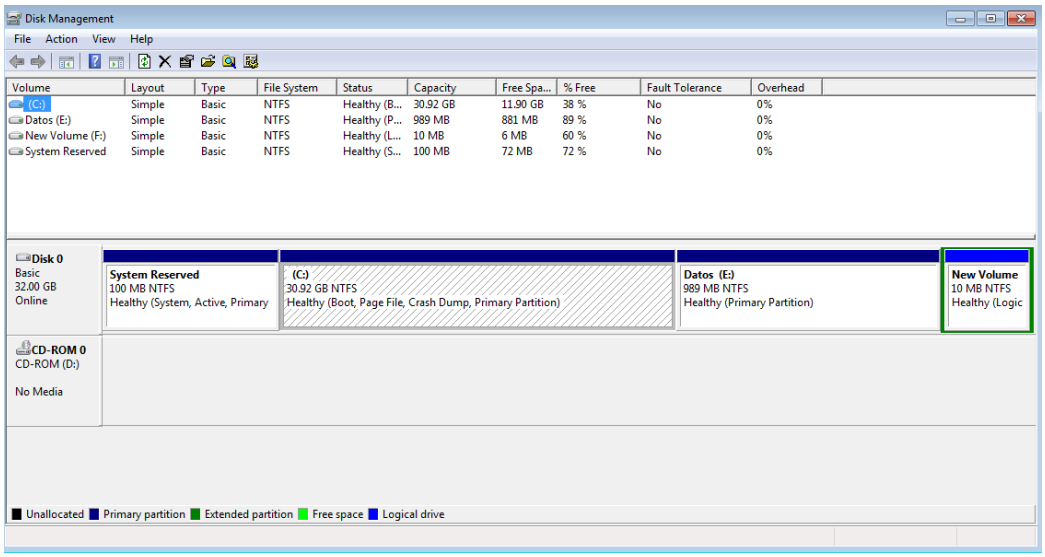
# ANALISIS FORENSE

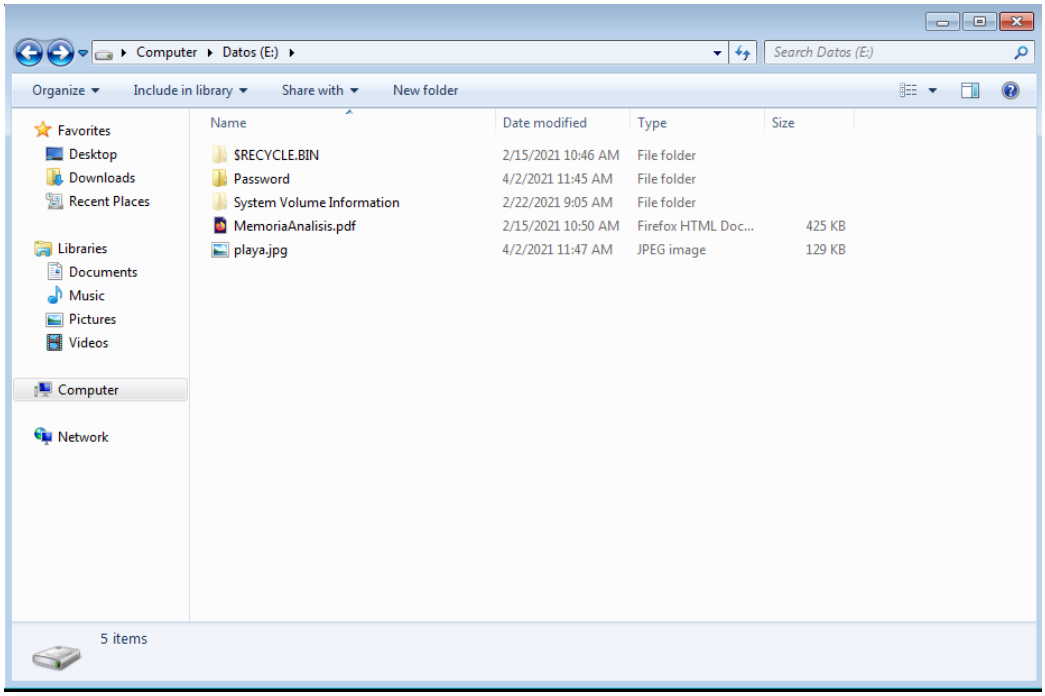
Practica 1 Ramón Rojas Soto

## Recuperar ficheros con File Carving de una partición.

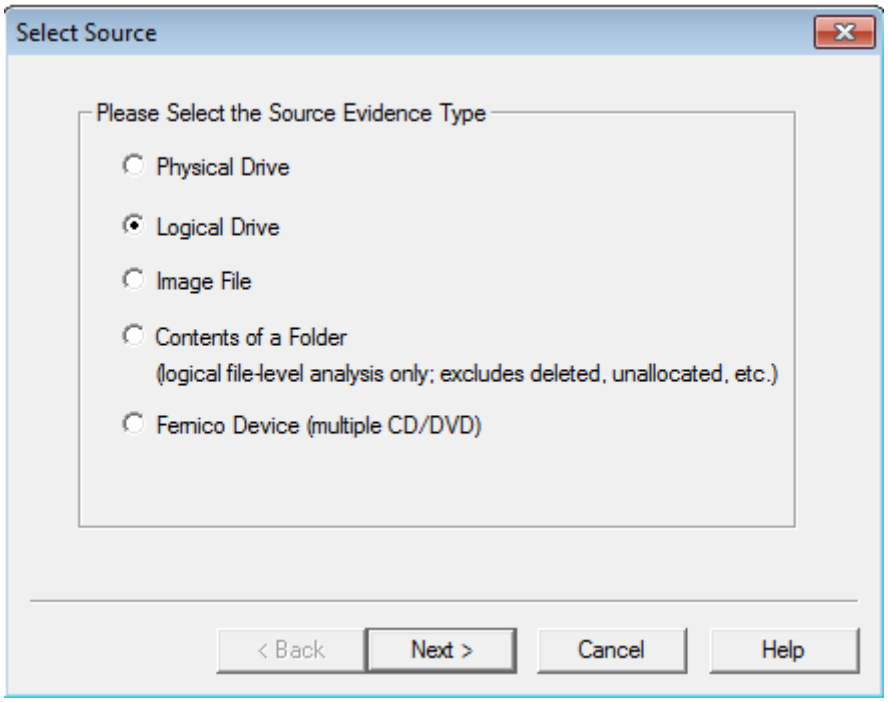
Tenemos varias partición ya creadas , en nuestro caso vamos a seleccionar la partición Datos (E:)



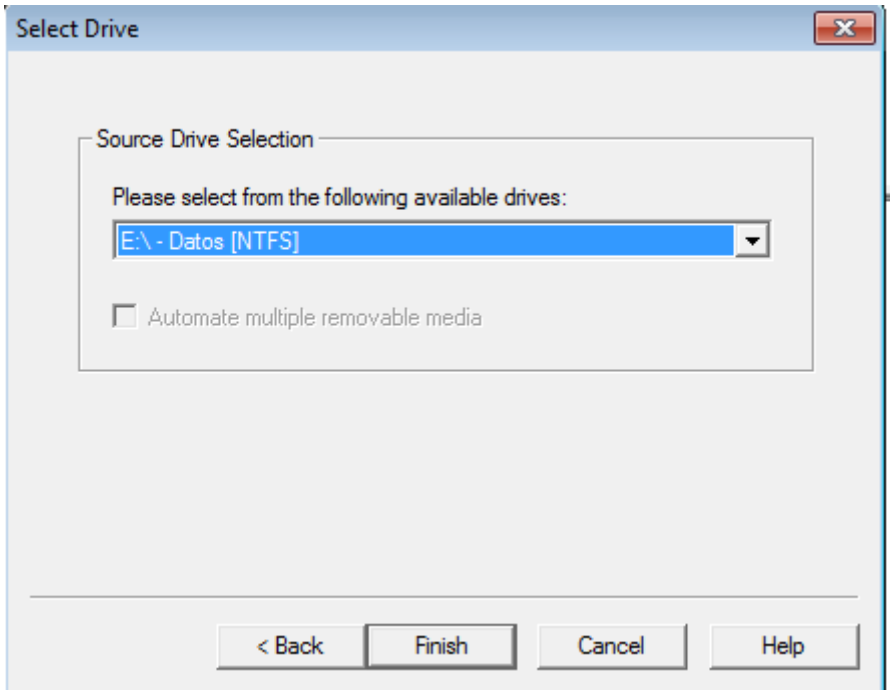

El contenido de la partición son un pdf, una imagen y dentro de la carpeta paswords un archivo txt con una contraseña



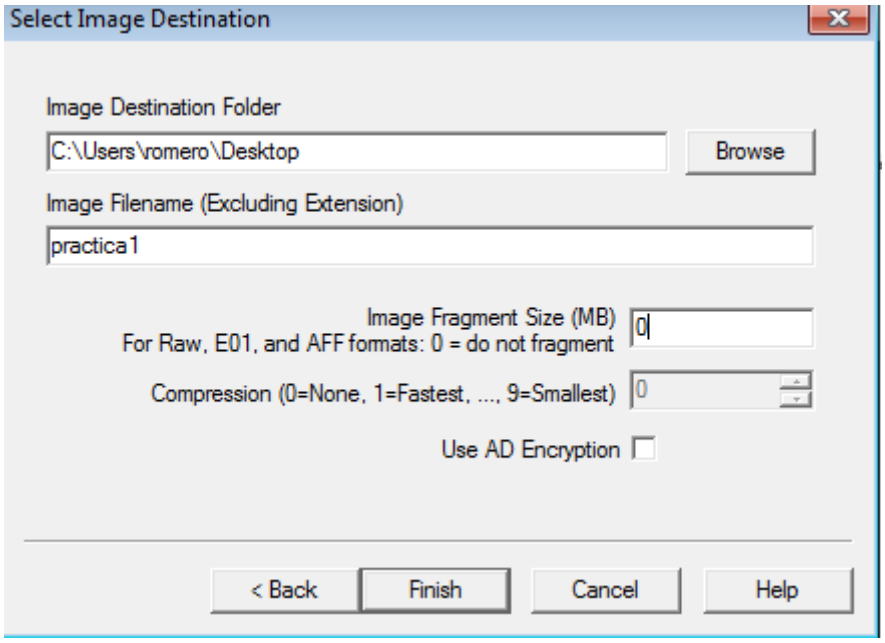
En el FTK imager File -> Create disk image cuando estamos en este menú seleccionamos la opción de Logical Drive



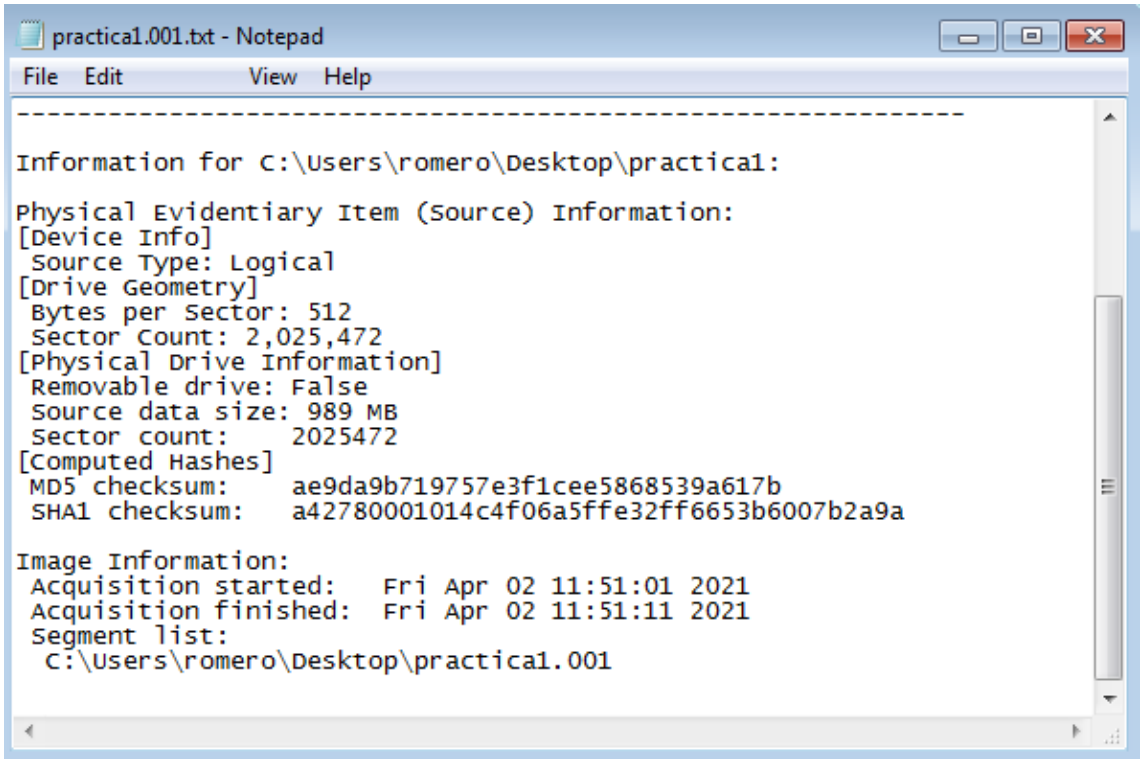

Marcamos la partición que queremos copiar



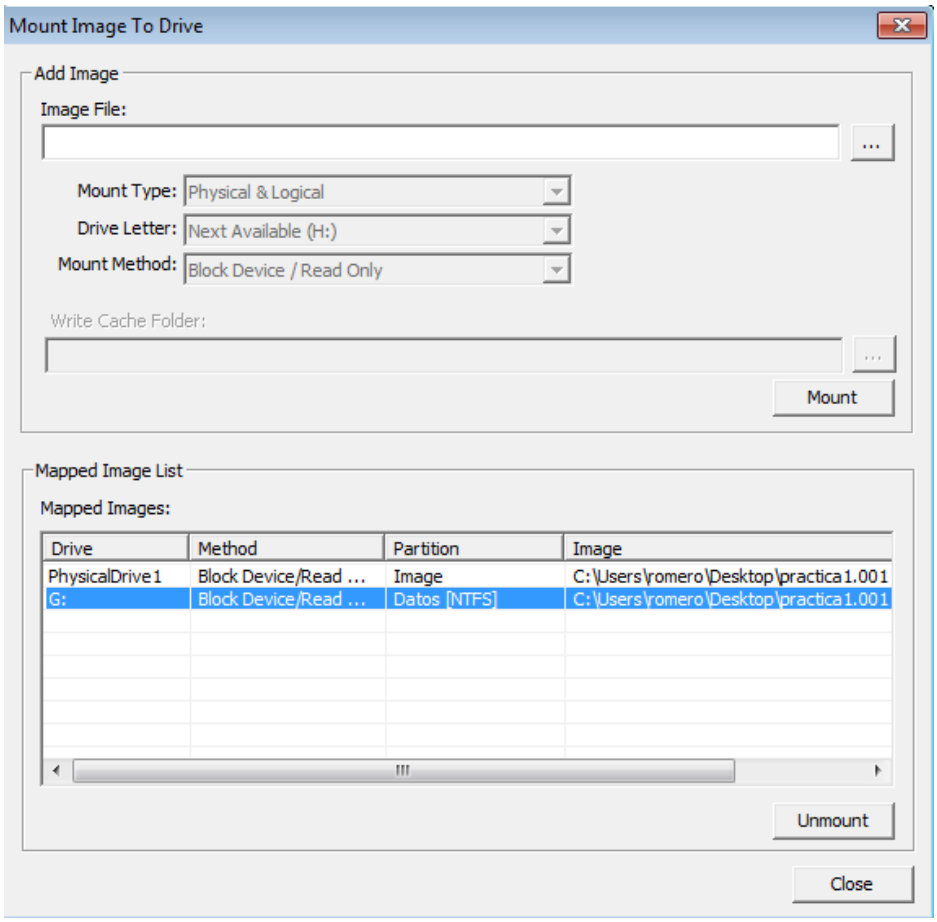

El nombre y donde la queremos guardar en mi caso yo la guardo en el escritorio



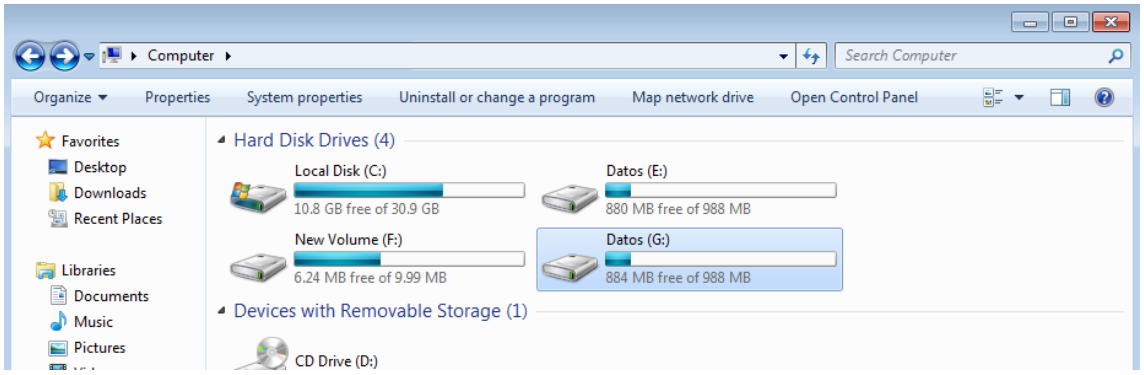

Una vez creada aparte de nuestra imagen se nos genera un archivo txt de informa




Tenemos un par de opciones para analizar la partición, una es con la opción de File -> Image Mounting

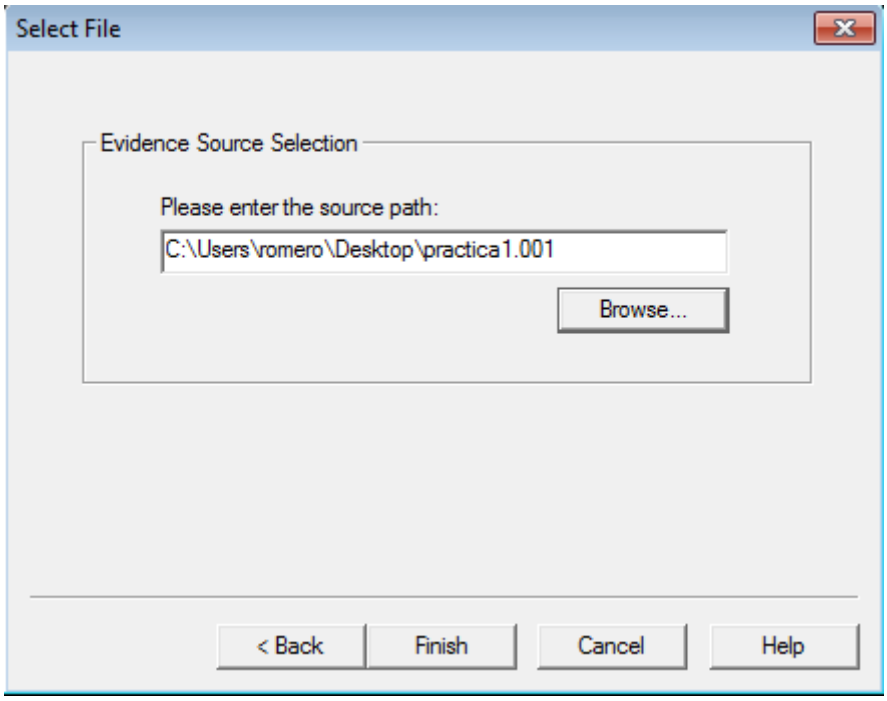



Que lo que hace es montarnos la copia que acabamos de crear como otro disco duro mas al que podemos acceder como haríamos normalmente

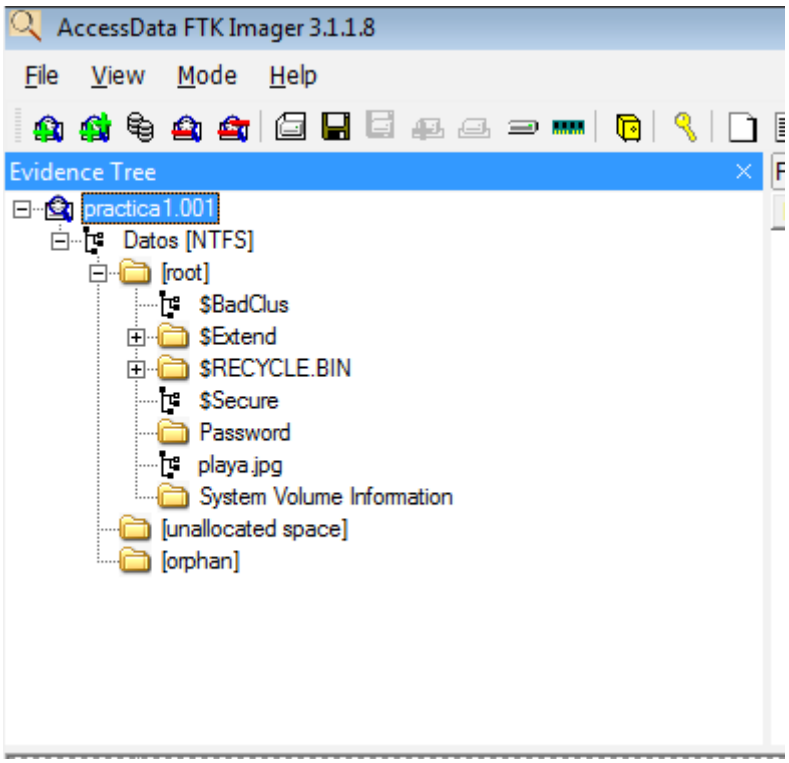



Y la otra que es mas visual para usar la herramienta es File -> Add evidence item -> Image File

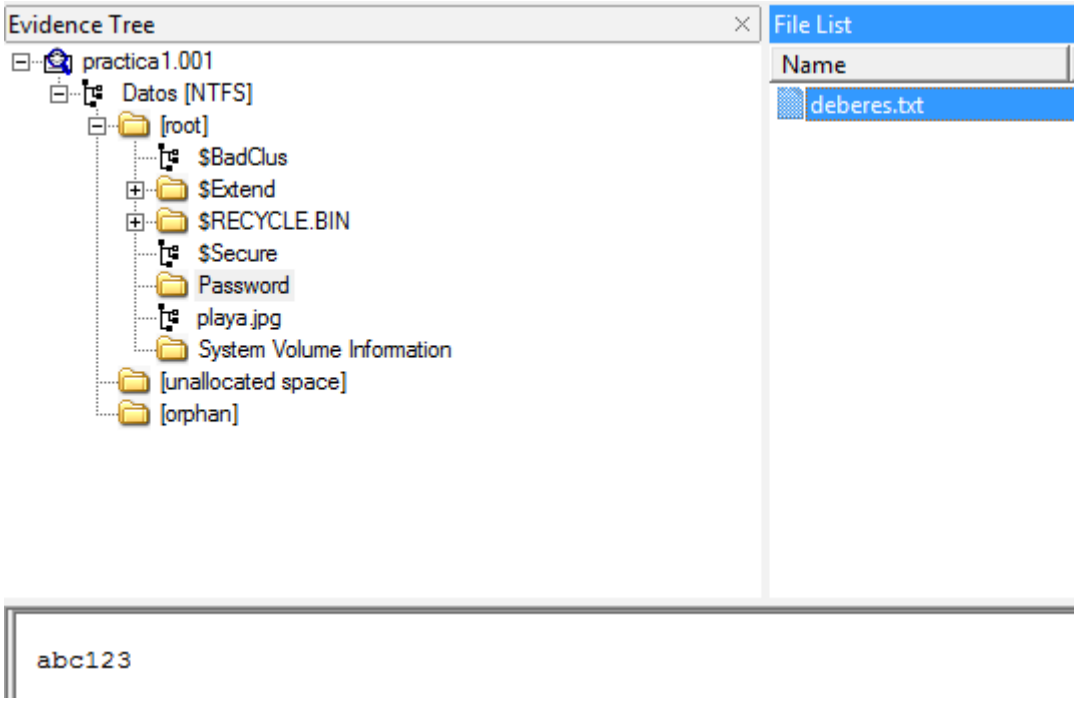
Seleccionamos nuestra imagen



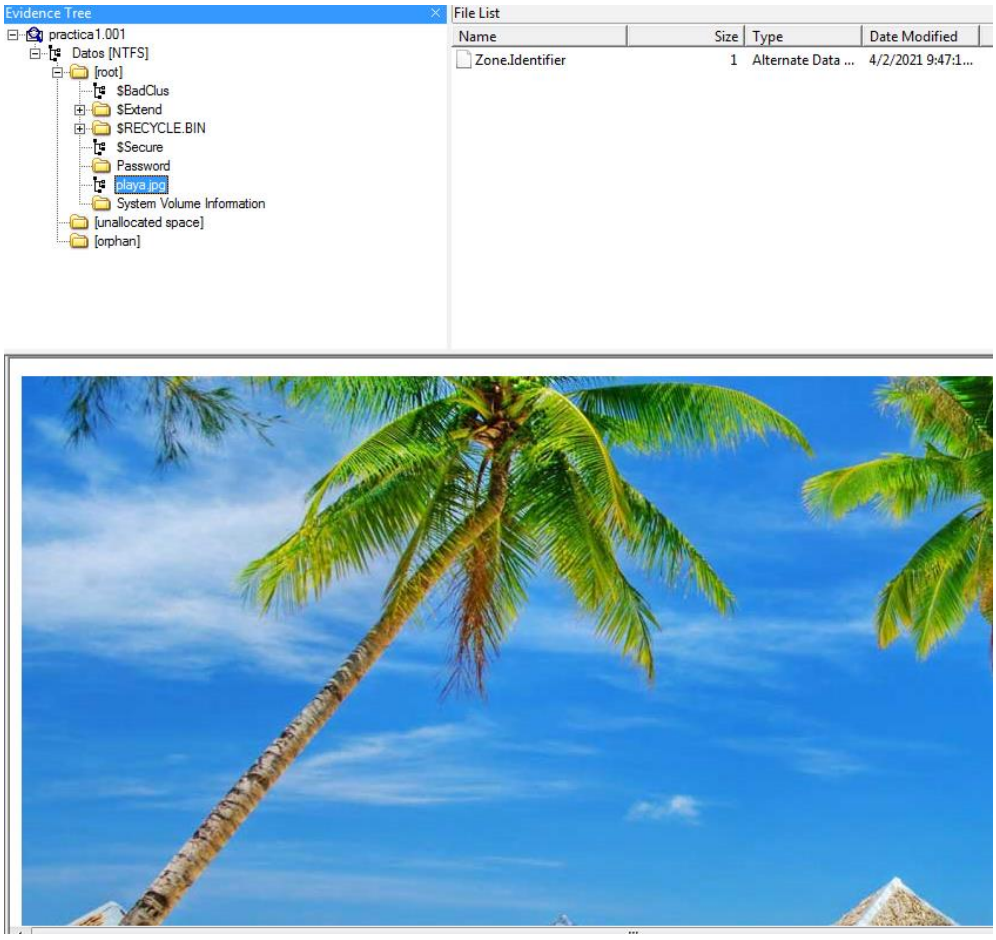

Y nos la despliega dentro de la herramienta




Aquí podemos ver el archivos con la contraseña dentro de nuestra carpeta password

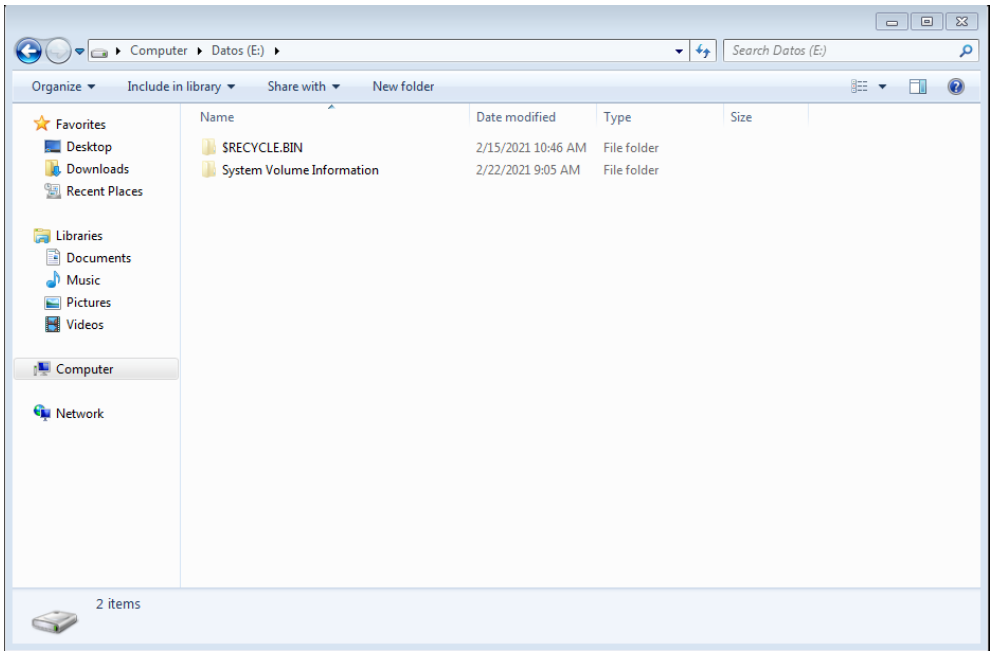



Incluso permite visualizar las imágenes que tenemos en la imagen del disco

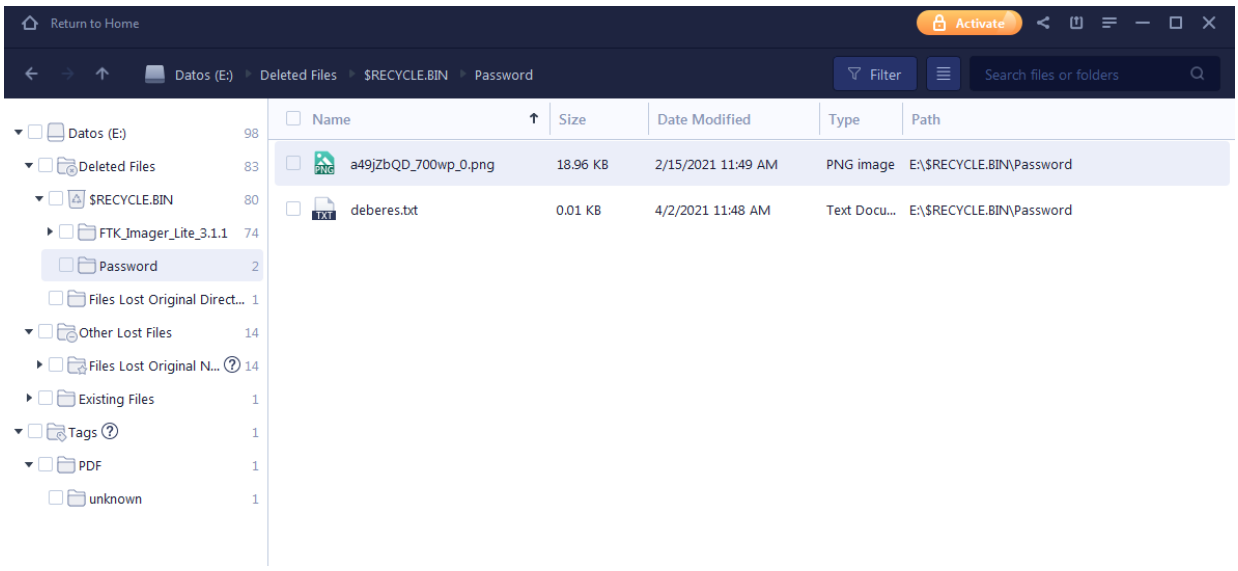


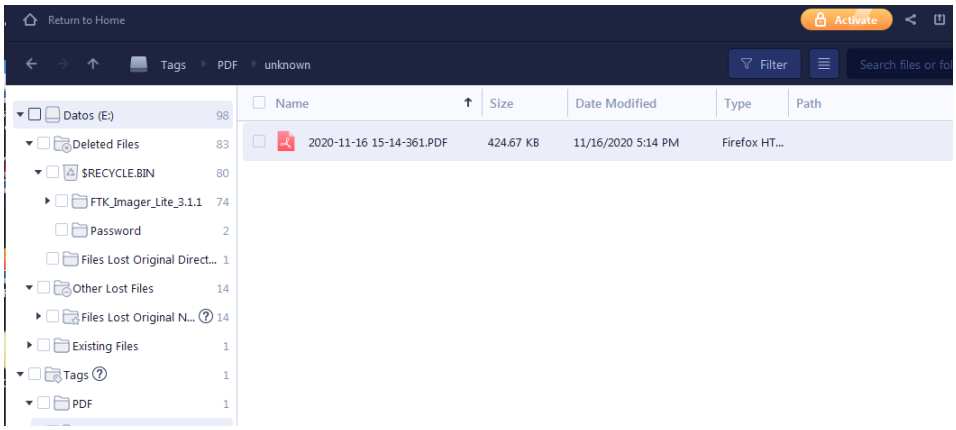
## EaseUS recovery

Ahora borramos todos los archivos para utilizar varias herramientas para recuperar nuestros datos una vez borrados del disco

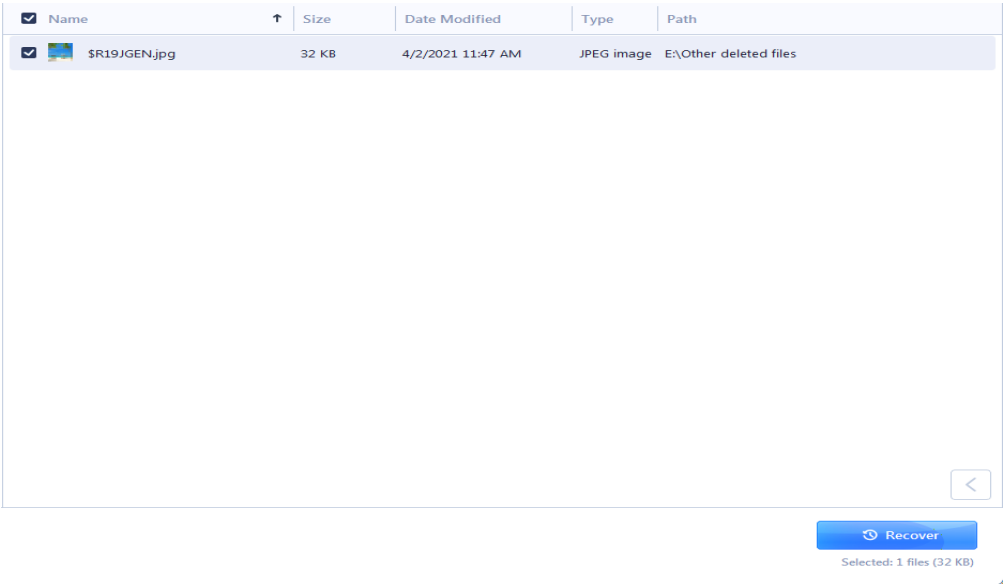



Una de ellas es **EaseUS recovery** una vez instalado podemos decir que nos analice nuestra partición de la que han sido eliminados los datos y vemos como nos recupera incluso más ficheros que habrían sido borrados anteriormente





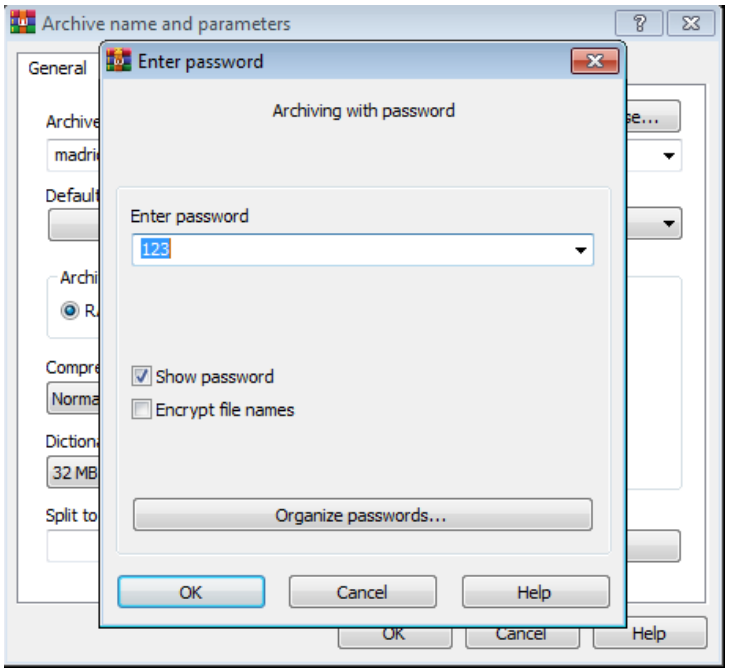

Esta herramienta también nos ofrece la posibilidad de recuperar el archivo eliminado



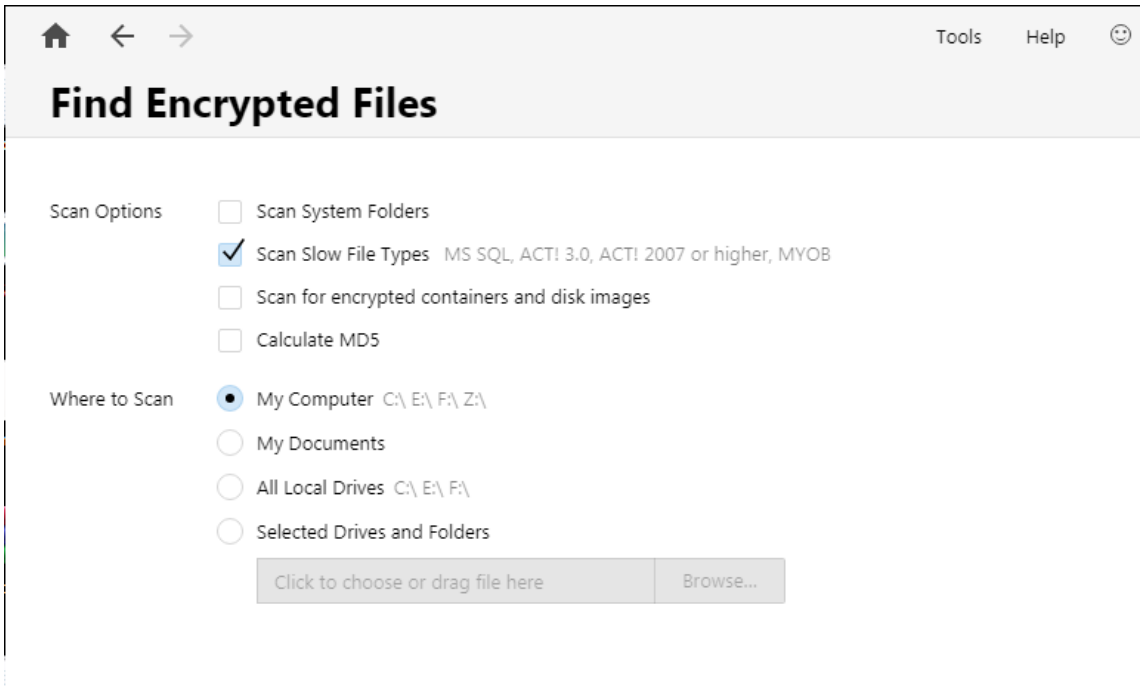

## Password Forensic Kit

Recuperar contraseñas con Password forensic Kit

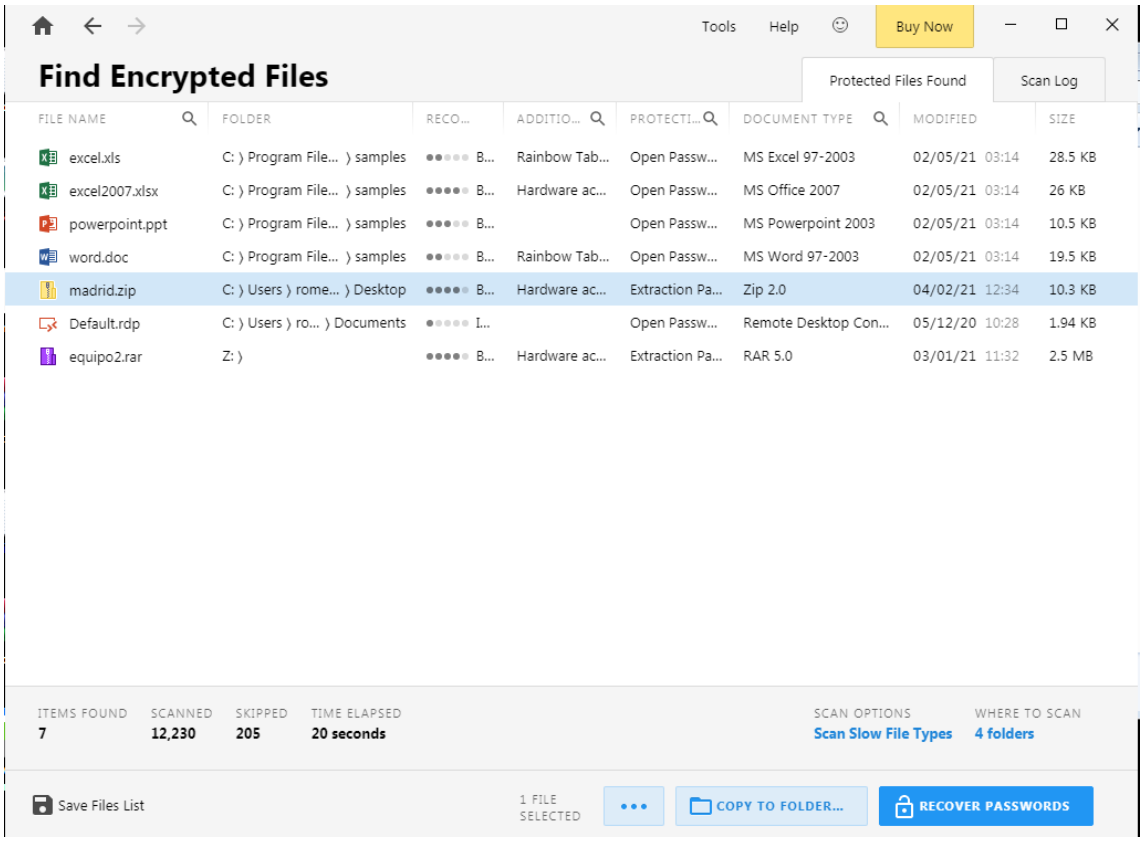
Primero creamos un archivo zip con una contraseña fácil para que nos la encuentre rápidamente

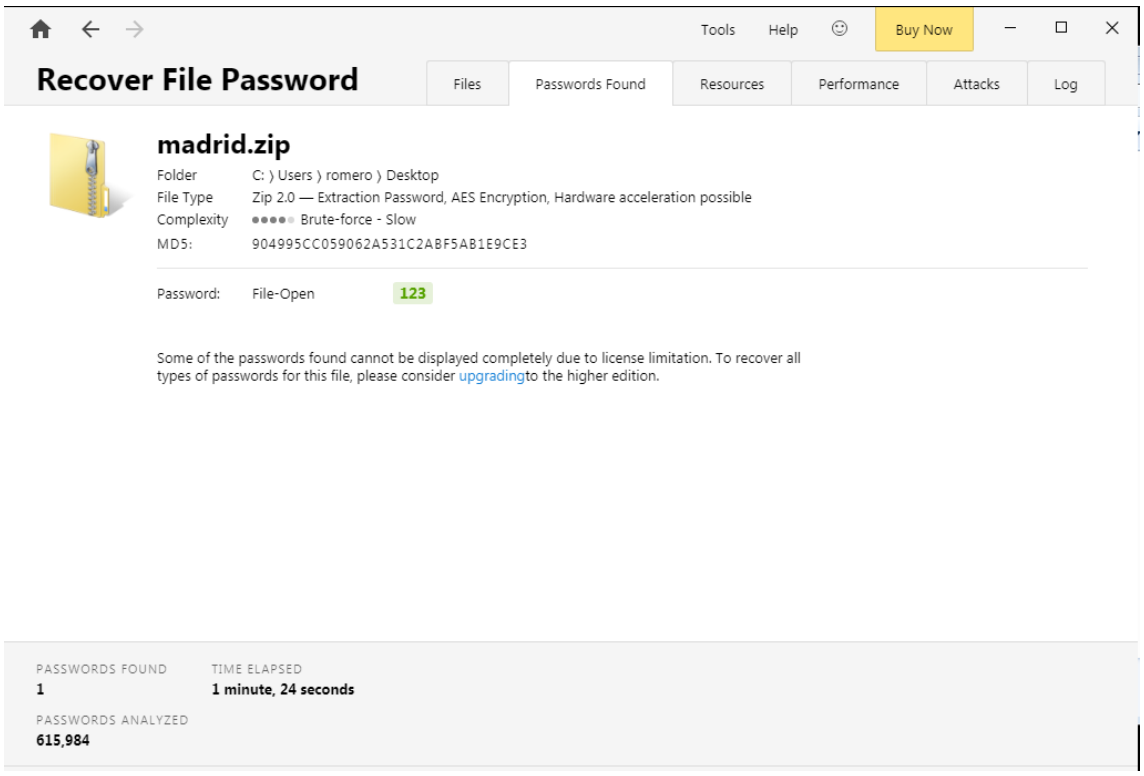



En la herramienta le decimos que analice todo nuestro ordenador para que sea lo mas real posible pues no vamos a saber dónde esconde la gente sus archivos



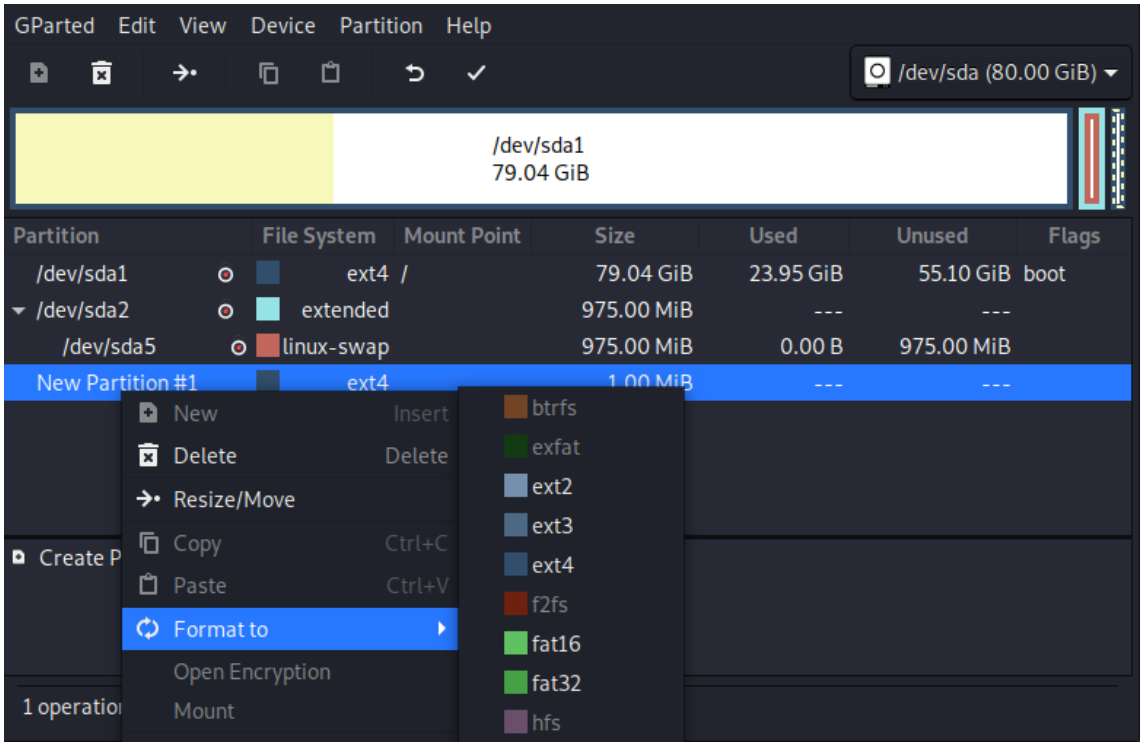

Nos encuentra varios ficheros de ejemplo y luego el que habíamos creado previamente

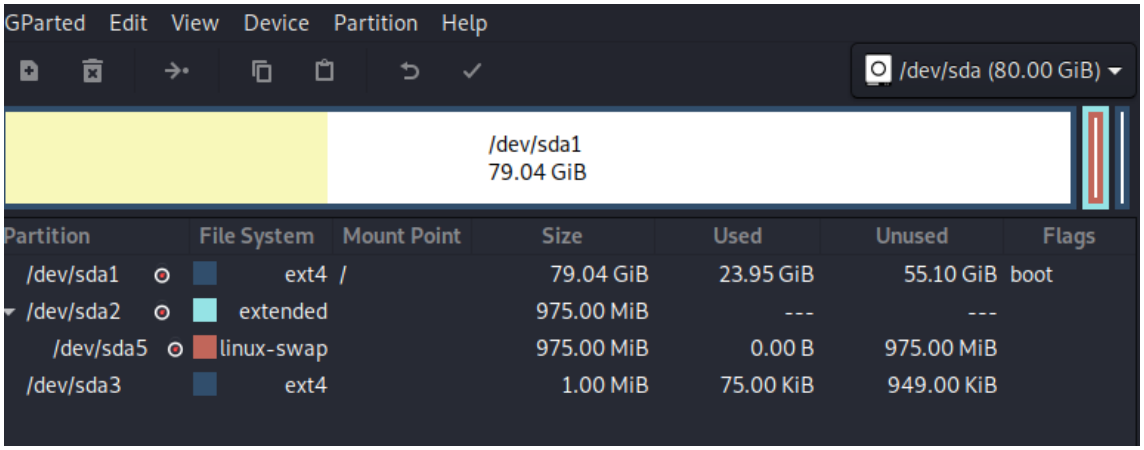

Tools
Help
Buy Now
Find Encrypted Files
Protected Files Found
Scan Log
FILE NAME
FOLDER
RECO...
ADDITIO...
PROTECTI...
DOCUMENT TYPE
MODIFIED
SIZE
excel.xls C: ) Program File... ) samples B... Rainbow Tab... Open Passw... MS Excel 97-2003 02/05/21 03:14 28.5 KB
excel2007.xlsx C: ) Program File... ) samples B... Hardware ac... Open Passw... MS Office 2007 02/05/21 03:14 26 KB
powerpoint.ppt C: ) Program File... ) samples B... Open Passw... MS Powerpoint 2003 02/05/21 03:14 10.5 KB
word.doc C: ) Program File... ) samples B... Rainbow Tab... Open Passw... MS Word 97-2003 02/05/21 03:14 19.5 KB
madrid.zip C: ) Users ) rome... ) Desktop B... Hardware ac... Extraction Pa... Zip 2.0 04/02/21 12:34 10.3 KB
Default.rdp C: ) Users ) ro... ) Documents I... Open Passw... Remote Desktop Con... 05/12/20 10:28 1.94 KB
equipo2.rar Z: ) B... Hardware ac... Extraction Pa... RAR 5.0 03/01/21 11:32 2.5 MB
ITEMS FOUND 7
SCANNED 12,230
SKIPPED 205
TIME ELAPSED 20 seconds
SCAN OPTIONS Scan Slow File Types
WHERE TO SCAN 4 folders
Save Files List
1 FILE SELECTED
COPY TO FOLDER...
RECOVER PASSWORDS


Tools
Help
Buy Now
Recover File Password
Files
Passwords Found
Resources
Performance
Attacks
Log
madrid.zip
Folder C: ) Users ) romero ) Desktop
File Type Zip 2.0 — Extraction Password, AES Encryption, Hardware acceleration possible
Complexity Brute-force - Slow
MD5: 904995CC059062A531C2ABF5AB1E9CE3
Password: File-Open 123
Some of the passwords found cannot be displayed completely due to license limitation. To recover all types of passwords for this file, please consider upgradingto the higher edition.
PASSWORDS FOUND 1
TIME ELAPSED 1 minute, 24 seconds
PASSWORDS ANALYZED 615,984

# FILE CARVING LINUX

Creamos una partición en Linux con Gparted




Para gestionar los clonados de discos en Linux usamos la herramienta "DD"

El comando se ordena : dd if=(origen) of=(destino)

```
kali@kali:~$ sudo dd if=/dev/sda3 of=/root/particion.dd status=progress
2048+0 records in
2048+0 records out
1048576 bytes (1.0 MB, 1.0 MiB) copied, 0.0137842 s, 76.1 MB/s
kali@kali:~$
```

Comprobamos que el md5 del disco y de la copia es exactamente igual , por lo que está bien clonado

```
kali@kali:~$ sudo md5sum /root/particion.dd
1c0937c4b1a441ec7f55a93fa7164465  /root/particion.dd
kali@kali:~$ sudo md5sum /dev/sda3
1c0937c4b1a441ec7f55a93fa7164465  /dev/sda3
kali@kali:~$
```

Una herramienta de Linux es Hexeditor para ver de forma hexadecimal el contenido del disco , en Windows también existe esta herramienta entre muchas otras

```
kali@kali:~$ sudo hexeditor /root/particion.dd
```

```
File    Actions    Edit    View    Help
File: /root/particion.dd
00000330  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00
00000340  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00
00000350  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00
00000360  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00
00000370  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00
00000380  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00
00000390  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00
000003A0  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00
000003B0  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00
000003C0  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00
000003D0  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00
000003E0  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00
000003F0  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00
00000400  80 00 00 00  00 04 00 00   33 00 00 00  DA 03 00 00
00000410  75 00 00 00  01 00 00 00   00 00 00 00  00 00 00 00
00000420  00 20 00 00  00 20 00 00   80 00 00 00  00 00 00 00
00000430  02 FD 66 60  00 00 FF FF   53 EF 01 00  01 00 00 00
00000440  02 FD 66 60  00 00 00 00   00 00 00 00  01 00 00 00
00000450  00 00 00 00  0B 00 00 00   80 00 00 00  38 00 00 00
00000460  42 02 00 00  6B 04 00 00   BF 35 AE 1E  72 72 4A 0F
00000470  8F 19 D3 96  02 43 D5 21   00 00 00 00  00 00 00 00
00000480  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00
00000490  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00
000004A0  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00
000004B0  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00
000004C0  00 00 00 00  00 00 00 00   00 00 00 00  00 00 03 00
000004D0  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00
000004E0  00 00 00 00  00 00 00 00   00 00 00 00  D5 90 17 49
000004F0  13 83 4B A2  89 BD 66 6E   C7 11 56 25  01 00 00 00
00000500  0C 00 00 00  00 00 00 00   02 FD 66 60  00 00 00 00
00000510  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00
00000520  00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00
```

Esto es interesante porque Linux incorpora unas opciones para llenar un disco de ceros o de bits con valor random

Los comandos para realizar estas acción son

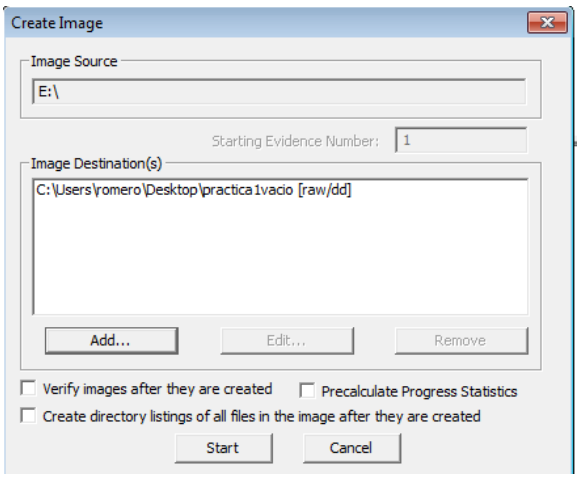
```
kali@kali:~$ sudo dd if=/dev/zero of=/dev/sda3 status=progress
```

```
kali@kali:~$ dd if=/dev/sda3 of=/root/particionRandom.dd
dd: failed to open '/dev/sda3': Permission denied
kali@kali:~$ sudo dd if=/dev/sda3 of=/root/particionRandom.dd
2048+0 records in
2048+0 records out
1048576 bytes (1.0 MB, 1.0 MiB) copied, 0.0121644 s, 86.2 MB/s
kali@kali:~$
```

```
File  Actions  Edit  View  Help
File: /root/particionRandom.dd
00000000  56 37 B4 81  2C 87 09 EE   28 A2 A0 E7  C9 3C CB A9
00000010  38 C7 5D 54  06 00 65 97   1A AE 62 FB  CB 29 BF C8
00000020  1D B5 34 D2  7E FD B5 9E   D2 69 2D 5E  B9 C3 04 53
00000030  17 B8 70 E6  AA 8B 55 93   64 6E 41 1F  9B B3 9D 49
00000040  72 67 51 3B  AE 5F 31 16   6D 7F C1 C6  02 3A 56 FF
00000050  CA 1B AD 16  7D 67 84 A1   AB E5 59 09  9F BE 5E AD
00000060  A9 97 3D 8C  5D D6 DC 66   16 14 4E 45  C7 10 CF 8D
00000070  4B 27 FF 56  6C D0 9A 14   19 6B 5D F9  AA 9D 53 0C
00000080  01 49 E6 FE  25 76 E3 BC   01 A9 0D FE  B9 57 B3 6C
00000090  9E 8C 54 56  82 D0 04 1D   F2 9F 7E F3  01 6F 36 C4
000000A0  F6 B8 57 60  1E 34 B6 DC   35 C5 0A 11  CE A5 69 4C
000000B0  9B 26 A5 BD  85 07 48 8A   C0 14 F3 DB  A7 29 8A 83
000000C0  F2 F7 95 34  80 45 58 02   85 DE 8C 9E  2B 41 41 B7
000000D0  DF 6F 36 2B  88 1B 14 96   2B 44 38 DC  3E 12 87 94
000000E0  03 63 3C 3B  F2 5E 7B 15   CA 0C BF C3  B2 19 0C EB
000000F0  AB B2 74 62  FC 1A 0A 3D   AA 2D E9 46  DE 79 A4 34
```

## FOREMOST

Con el disco aun vacío creamos otra copia para llevarla a Linux y realizar las acciones anteriores pero con la herramienta Foremost

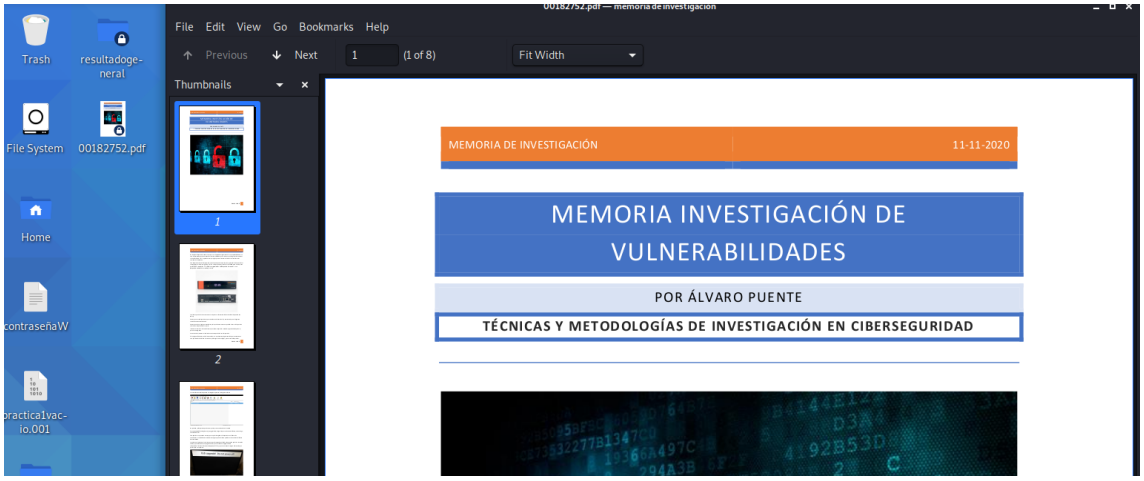


Primero hacemos una búsqueda solo de archivos pdf que puedan existir en el disco y vemos que nos encuentra dos

```
kali@kali:~/Desktop$ sudo foremost -t pdf -i practica1vacio.001 -o resultadopdf
Processing: practica1vacio.001
|**********|
kali@kali:~/Desktop$
```

```
root@kali:/home/kali/Desktop# cd resultadopdf/
root@kali:/home/kali/Desktop/resultadopdf# ls
audit.txt  pdf
root@kali:/home/kali/Desktop/resultadopdf# cd pdf/
root@kali:/home/kali/Desktop/resultadopdf/pdf# ls
00151488.pdf  00182752.pdf
root@kali:/home/kali/Desktop/resultadopdf/pdf#
```

```
root@kali:/home/kali/Desktop/resultadopdf/pdf# ls
00151488.pdf  00182752.pdf
root@kali:/home/kali/Desktop/resultadopdf/pdf# mv 00151488.pdf ../..
root@kali:/home/kali/Desktop/resultadopdf/pdf#
```



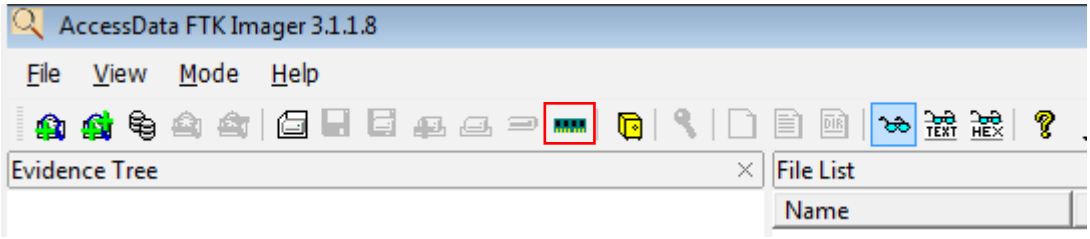

Si queremos que nos encuentre todos los posibles archivos solo debemos obviar el parámetro **-t** y entrando al archivo Audit.txt que nos crea vemos todos los tipos de archivo que nos ha encontrado.

```
root@kali:/home/kali/Desktop/resultadogeneral# ls
audit.txt  bmp  dll  exe  gif  jpg  pdf  png
root@kali:/home/kali/Desktop/resultadogeneral#
```

```
662 FILES EXTRACTED

jpg:= 10
gif:= 14
bmp:= 20
exe:= 85
png:= 531
pdf:= 2
```

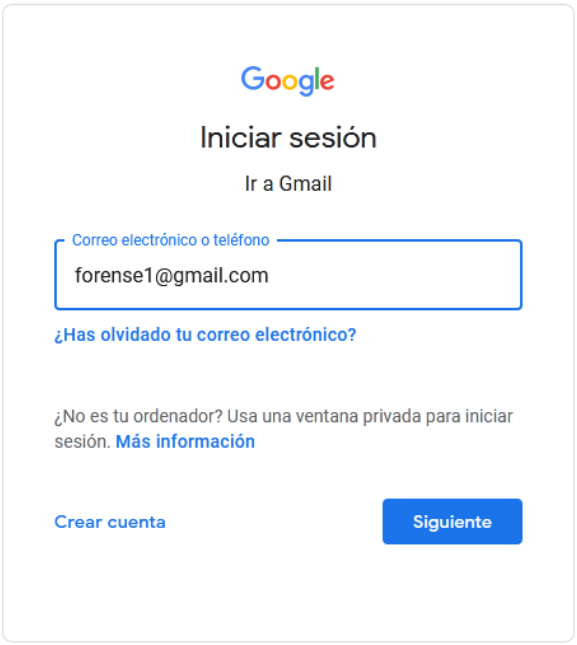
# Dumpear memoria RAM y extraer información en Windows

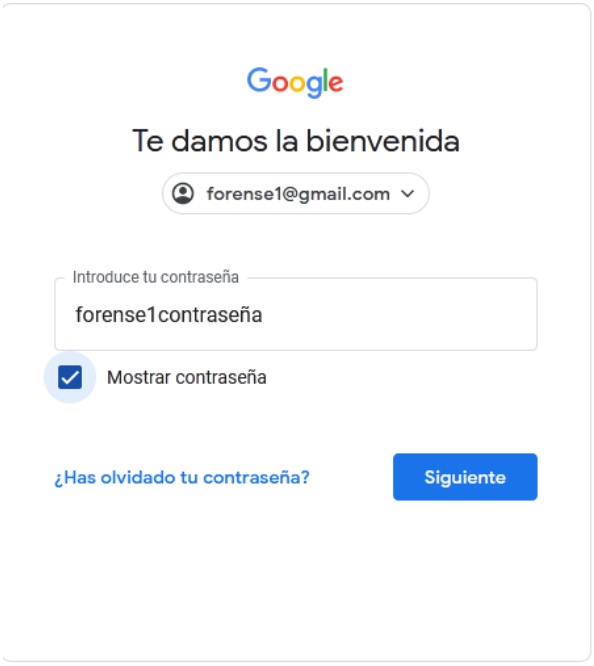
Para dumpear la memoria de un pc con FTK simplemente tenemos que hacer clic en el icono de la memoria RAM que tenemos en la barra superior



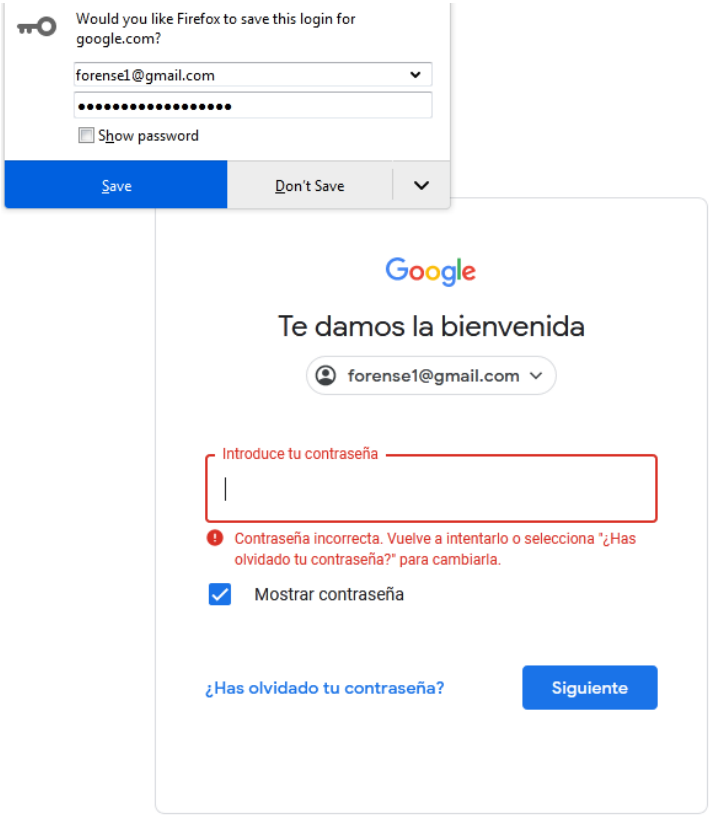

Esto nos extrae la memoria del pc de la cual podremos extraer toda la información que este en ese momento en la RAM, vamos a mostrar un ejemplo de lo que podemos extraer.

Vamos a introducir nuestras credenciales en una pagina web y a continuación dumpearemos la memoria para buscar dichas credenciales

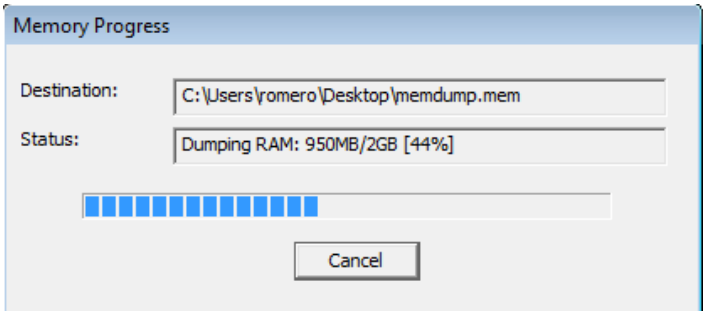


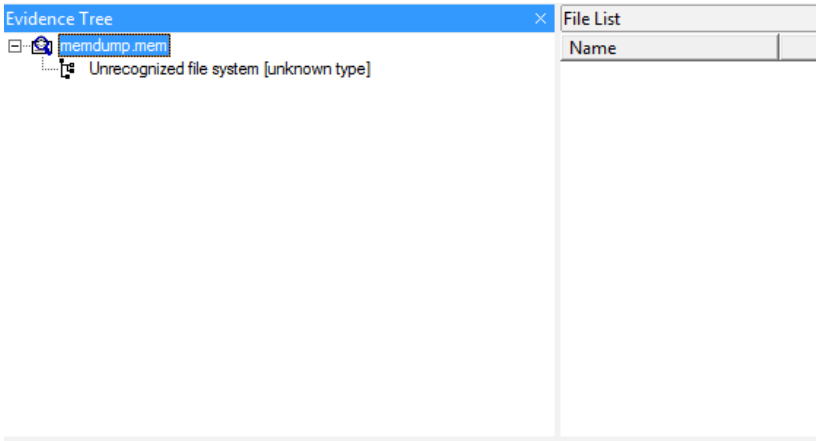




Estas credenciales no existen pero ya se han quedado en memoria

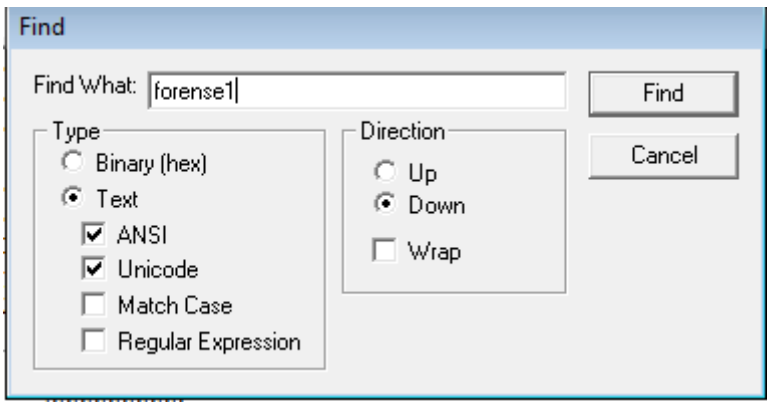



A continuación hacemos el volcado de memoria y pasamos a buscar esta contraseña en la RAM






```
0d01abd0 41 8B 4A 5C 4C 89 5C 24-20 FF 15 91 84 FA FF 83 A·J\L·\$ ÿ···úÿ·
0d01abe0 E8 02 78 0A 3B C7 75 09-83 7D 00 04 75 03 40 B7 è·x·;Çu··}··u·@·
0d01abf0 01 40 8A C7 48 8B 5C 24-40 48 8B 6C 24 48 48 8B ·@·ÇH·\$@H·l$HH·
0d01ac00 74 24 50 48 8B 7C 24 58-48 83 C4 30 41 5C C3 CC t$PH·|$XH·Ä0A\ÃÌ
0d01ac10 CC CC CC CC CC CC CC-48 8B C4 48 89 58 08 48 ÌÌÌÌÌÌÌÌH·ÄH·X·H
0d01ac20 89 68 10 48 89 70 18 57-41 54 41 55 48 83 EC 40 ·h·H·p·WATAUH·ì@
0d01ac30 83 60 C8 00 0F 29 70 D8-49 8B D8 48 8B F2 48 8B ·`È··)pØI·ØH·òH·
0d01ac40 F9 E8 9E 55 FF FF 8B E8-85 C0 78 1A 8B 43 30 89 ùè·Uÿÿ·è·Àx··C0·
0d01ac50 87 80 00 00 00 48 B8 9A-99 99 99 99 B9 3F 48 ·····H¸·····¹?H
0d01ac60 89 87 88 00 00 00 85 ED-0F 88 DB 00 00 00 8B 43 ·····íí··Û····C
0d01ac70 38 8B 57 20 48 8D 0D 65-F0 06 00 89 87 98 00 00 8·W H··eð·····
0d01ac80 00 48 83 7E 10 00 B8 04-00 00 00 48 0F 45 4E 10 ·H·~··¸····H·EN·
0d01ac90 48 F7 E2 48 C7 C2 FF FF-FF FF 4C 8B 01 48 0F 40 H÷âHÇÂÿÿÿÿL··H·@
0d01aca0 C2 8B D0 41 FF 50 08 48-89 87 90 00 00 00 48 85 Â·ÐAÿP·H·····H·
0d01acb0 C0 75 0A BD 0E 00 07 80-E9 8C 00 00 00 33 F6 39 Àu·½····é····3ö9
0d01acc0 77 20 0F 86 81 00 00 00-F2 0F 10 35 58 98 FB FF w ·····ò··5X·ûÿ
0d01acd0 45 33 E4 45 33 ED 48 8B-87 90 00 00 00 41 89 74 E3äE3íH·····A·t
0d01ace0 05 00 3B 77 20 73 0A 48-8B 47 18 49 8B 0C 04 EB ··;w s·H·G·I···ë
0d01acf0 02 33 C9 48 85 C9 74 42-3B 77 20 73 0A 48 8B 47 ·3ÉH·ÉtB;w s·H·G
0d01ad00 18 49 8B 0C 04 EB 02 33-C9 48 8B 01 FF 50 58 48 ·I···ë·3ÉH··ÿPXH
0d01ad10 8B CF 48 8B D8 48 8B 07-FF 50 60 48 8B D3 48 8B ·ÏH·ØH··ÿP`H·ÓH·
0d01ad20 C8 66 0F 28 DE 66 0F 28-D6 F2 0F 11 74 24 28 F2 Èf·(Þf·(Öò··t$(ò
0d01ad30 0F 11 74 24 20 E8 8A 78-FE FF FF C6 49 83 C5 04 ··t$ è·xþÿÿÆI·Å·
0d01ad40 49 83 C4 08 3B 77 20 72-8D 48 8B 5C 24 60 48 8B I·Ä·;w r·H·\$`H·
0d01ad50 74 24 70 0F 28 74 24 30-8B C5 48 8B 6C 24 68 48 t$p·(t$0·ÅH·l$hH
0d01ad60 83 C4 40 41 5D 41 5C 5F-C3 CC CC CC CC CC CC CC ·Ä@A]A\_ÃÌÌÌÌÌÌÌ
0d01ad70 48 8B C4 48 89 58 08 48-89 68 10 48 89 70 18 48 H·ÄH·X·H·h·H·p·H
0d01ad80 89 78 20 41 54 48 83 EC-20 41 8B 80 80 00 00 00 ·x ATH·ì A·····
0d01ad90 49 8B E8 4C 8B E2 89 81-80 00 00 00 49 8B 80 88 I·èL·â·····I···
0d01ada0 00 00 00 48 8B F9 48 89-81 88 00 00 00 E8 66 56 ···H·ùH·····èfV
0d01adb0 FF FF 33 DB 3B C3 8B F0-7C 72 8B 8D 98 00 00 00 ÿÿ3Û;Ã·ð|r·····
0d01adc0 8B 57 20 8D 43 04 89 8F-98 00 00 00 49 39 5C 24 ·W ·C·····I9\$
```




```
0cd21270 00 00 00 00 03 00 E5 E5-E5 E5 E5 E5 E5 E5 E5 E5 ·····åååååååååå
0cd21280 01 00 00 00 26 00 00 00-66 00 6F 00 72 00 65 00 ····&···f·o·r·e·
0cd21290 6E 00 73 00 65 00 31 00-63 00 6F 00 6E 00 74 00 n·s·e·1·c·o·n·t·
0cd212a0 72 00 61 00 73 00 65 00-F1 00 61 00 00 00 E5 E5 r·a·s·e·ñ·a···åå
```

# Obtener información volátil en LINUX

Todas las pruebas las hacemos con la herramienta **volatility**

Con el archivo de RAM en nuestro Kali lo primero que hacemos es obtener información de la imagen RAM

Con el comando: **sudo Python vol.py imageinfo -f ~/Desktop/memdump.mem**

```
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP0x64, Win7SP1x64, Win2008R2SP0x64, Win2008R2SP1x64
                     AS Layer1 : AMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/Desktop/memdump.mem)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80002a030a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002a04d00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2021-04-05 09:23:54 UTC+0000
     Image local date and time : 2021-04-05 11:23:54 +0200
kali@kali:~/volatility-kali-master$
```

Con esto lo principal es que obtenemos los principales perfiles de búsqueda recomendados por la herramienta , en mi caso la memoria ha sido volcada desde un W7SP1x64, la herramienta tiene muchas opciones vamos a mostrar algunas de las más comunes

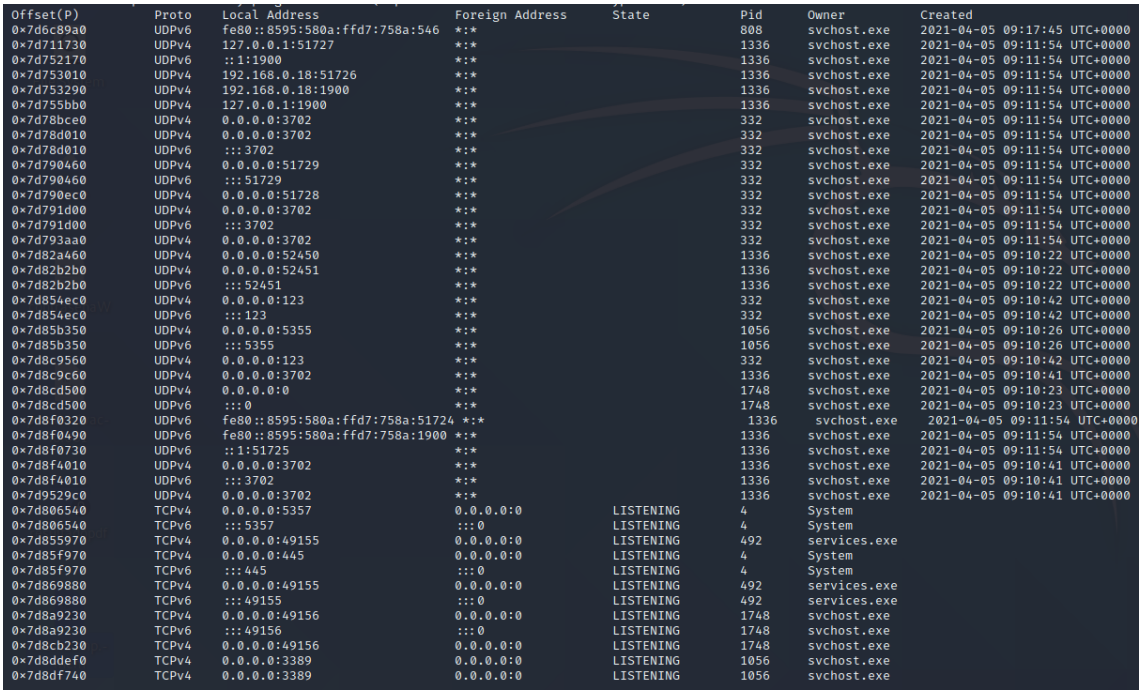
- **Obtener el listado de procesos**

  Con el comando: **sudo python vol.py --profile=Win7SP1x64 pslist -f ~/Desktop/memdump.mem**

| Offset(V) | Name | PID | PPID | Thds | Hnds | Sess | Wow64 | Start | Exit |
|---|---|---|---|---|---|---|---|---|---|
| 0xfffffa80018ad040 | System | 4 | 0 | 83 | 584 | ------ | 0 | 2021-04-05 09:10:18 UTC+0000 | |
| 0xfffffa800211eb00 | smss.exe | 248 | 4 | 2 | 29 | ------ | 0 | 2021-04-05 09:10:18 UTC+0000 | |
| 0xfffffa80038fbb30 | smss.exe | 328 | 248 | 0 | -------- | 0 | 0 | 2021-04-05 09:10:19 UTC+0000 | 2021-04-05 09:10:19 UTC+0000 |
| 0xfffffa80020226b0 | csrss.exe | 336 | 328 | 9 | 371 | 0 | 0 | 2021-04-05 09:10:19 UTC+0000 | |
| 0xfffffa80039a1630 | smss.exe | 380 | 248 | 0 | -------- | 1 | 0 | 2021-04-05 09:10:19 UTC+0000 | 2021-04-05 09:10:19 UTC+0000 |
| 0xfffffa80039a2280 | wininit.exe | 388 | 328 | 3 | 75 | 0 | 0 | 2021-04-05 09:10:19 UTC+0000 | |
| 0xfffffa80039aa790 | csrss.exe | 396 | 380 | 10 | 421 | 1 | 0 | 2021-04-05 09:10:19 UTC+0000 | |
| 0xfffffa8003a03060 | winlogon.exe | 432 | 380 | 3 | 111 | 1 | 0 | 2021-04-05 09:10:19 UTC+0000 | |
| 0xfffffa80039f8b30 | services.exe | 492 | 388 | 6 | 188 | 0 | 0 | 2021-04-05 09:10:19 UTC+0000 | |
| 0xfffffa8003a6a880 | lsass.exe | 500 | 388 | 8 | 621 | 0 | 0 | 2021-04-05 09:10:19 UTC+0000 | |
| 0xfffffa8003a6b660 | lsm.exe | 508 | 388 | 11 | 201 | 0 | 0 | 2021-04-05 09:10:19 UTC+0000 | |
| 0xfffffa8003b45b30 | svchost.exe | 600 | 492 | 9 | 352 | 0 | 0 | 2021-04-05 09:10:20 UTC+0000 | |
| 0xfffffa8003b6ab30 | VBoxService.ex | 660 | 492 | 13 | 137 | 0 | 0 | 2021-04-05 09:10:20 UTC+0000 | |
| 0xfffffa8003ba0b30 | svchost.exe | 728 | 492 | 7 | 254 | 0 | 0 | 2021-04-05 09:10:20 UTC+0000 | |
| 0xfffffa8003bfdb30 | svchost.exe | 808 | 492 | 21 | 475 | 0 | 0 | 2021-04-05 09:10:20 UTC+0000 | |
| 0xfffffa8003c389e0 | svchost.exe | 884 | 492 | 17 | 394 | 0 | 0 | 2021-04-05 09:10:21 UTC+0000 | |
| 0xfffffa8003c519e0 | svchost.exe | 916 | 492 | 37 | 1042 | 0 | 0 | 2021-04-05 09:10:21 UTC+0000 | |
| 0xfffffa8003d34b30 | svchost.exe | 332 | 492 | 18 | 464 | 0 | 0 | 2021-04-05 09:10:21 UTC+0000 | |
| 0xfffffa8003d5eb30 | svchost.exe | 1056 | 492 | 24 | 553 | 0 | 0 | 2021-04-05 09:10:21 UTC+0000 | |
| 0xfffffa8003b38060 | spoolsv.exe | 1200 | 492 | 12 | 276 | 0 | 0 | 2021-04-05 09:10:22 UTC+0000 | |
| 0xfffffa8003b70060 | svchost.exe | 1232 | 492 | 17 | 301 | 0 | 0 | 2021-04-05 09:10:22 UTC+0000 | |
| 0xfffffa8003b03350 | svchost.exe | 1336 | 492 | 14 | 242 | 0 | 0 | 2021-04-05 09:10:22 UTC+0000 | |
| 0xfffffa8003e7c580 | svchost.exe | 1748 | 492 | 5 | 98 | 0 | 0 | 2021-04-05 09:10:23 UTC+0000 | |
| 0xfffffa8001b9c680 | sppsvc.exe | 1500 | 492 | 4 | 145 | 0 | 0 | 2021-04-05 09:11:41 UTC+0000 | |
| 0xfffffa8003d6d790 | taskhost.exe | 988 | 492 | 9 | 143 | 1 | 0 | 2021-04-05 09:11:41 UTC+0000 | |
| 0xfffffa8003f81060 | userinit.exe | 1604 | 432 | 0 | -------- | 1 | 0 | 2021-04-05 09:11:45 UTC+0000 | 2021-04-05 09:12:20 UTC+0000 |
| 0xfffffa8003c36a10 | dwm.exe | 1652 | 884 | 3 | 87 | 1 | 0 | 2021-04-05 09:11:45 UTC+0000 | |
| 0xfffffa8003f7fb30 | explorer.exe | 1244 | 1604 | 28 | 778 | 1 | 0 | 2021-04-05 09:11:45 UTC+0000 | |
| 0xfffffa80040596e0 | VBoxTray.exe | 1712 | 1244 | 13 | 144 | 1 | 0 | 2021-04-05 09:11:46 UTC+0000 | |
| 0xfffffa80040a570 | SearchIndexer. | 1540 | 492 | 11 | 693 | 0 | 0 | 2021-04-05 09:11:53 UTC+0000 | |
| 0xfffffa8003f816b0 | wmpnetwk.exe | 1700 | 492 | 9 | 205 | 0 | 0 | 2021-04-05 09:11:53 UTC+0000 | |
| 0xfffffa8003cc0890 | audiodg.exe | 1784 | 808 | 4 | 122 | 0 | 0 | 2021-04-05 09:19:03 UTC+0000 | |
| 0xfffffa8003ecc060 | FTK Imager.exe | 2964 | 1244 | 16 | 308 | 1 | 1 | 2021-04-05 09:19:04 UTC+0000 | |
| 0xfffffa8004130b30 | taskeng.exe | 2932 | 916 | 4 | 83 | 1 | 0 | 2021-04-05 09:20:24 UTC+0000 | |
| 0xfffffa8001a84060 | firefox.exe | 2632 | 1244 | 0 | -------- | 1 | 0 | 2021-04-05 09:21:51 UTC+0000 | 2021-04-05 09:21:52 UTC+0000 |
| 0xfffffa8001f72b30 | firefox.exe | 1136 | 2632 | 0 | -------- | 1 | 0 | 2021-04-05 09:21:51 UTC+0000 | 2021-04-05 09:21:52 UTC+0000 |
| 0xfffffa8001a8fa30 | updater.exe | 2220 | 1136 | 0 | -------- | 1 | 0 | 2021-04-05 09:21:52 UTC+0000 | 2021-04-05 09:22:01 UTC+0000 |
| 0xfffffa8001b1b060 | firefox.exe | 2688 | 2220 | 0 | -------- | 1 | 0 | 2021-04-05 09:22:00 UTC+0000 | 2021-04-05 09:22:01 UTC+0000 |
| 0xfffffa8001b8d060 | firefox.exe | 2472 | 2688 | 74 | 1079 | 1 | 1 | 2021-04-05 09:22:00 UTC+0000 | |
| 0xfffffa8001be2b30 | firefox.exe | 1312 | 2472 | 8 | 267 | 1 | 1 | 2021-04-05 09:22:01 UTC+0000 | |
| 0xfffffa8001bb45d0 | firefox.exe | 2620 | 2472 | 0 | -------- | 1 | 0 | 2021-04-05 09:22:02 UTC+0000 | 2021-04-05 09:22:11 UTC+0000 |
| 0xfffffa8001c77b30 | firefox.exe | 1032 | 2472 | 0 | -------- | 1 | 0 | 2021-04-05 09:22:02 UTC+0000 | 2021-04-05 09:22:20 UTC+0000 |
| 0xfffffa8001c71740 | firefox.exe | 1216 | 2472 | 21 | 320 | 1 | 1 | 2021-04-05 09:22:02 UTC+0000 | |

- **Ver las conexiones de red**

Con el comando: **sudo python vol.py --profile=Win7SP1x64 netscan -f ~/Desktop/memdump.mem**

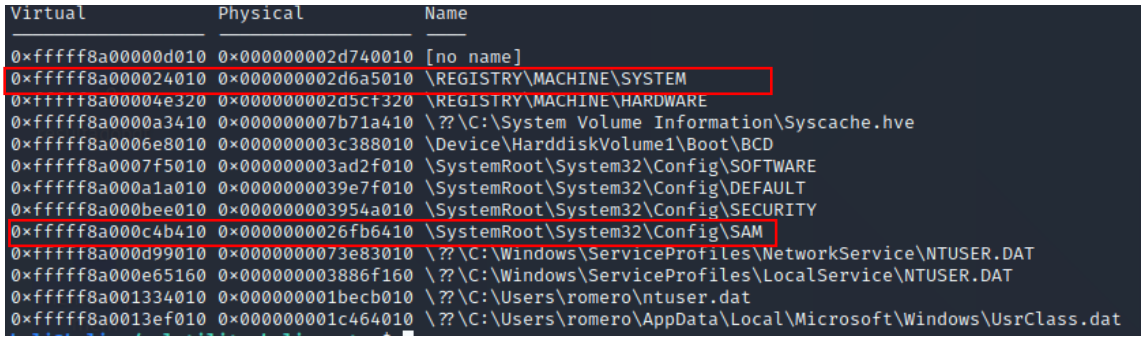


| Offset(P) | Proto | Local Address | Foreign Address | State | Pid | Owner | Created |
|---|---|---|---|---|---|---|---|
| 0x7d6c89a0 | UDPv6 | fe80::8595:580a:ffd7:758a:546 | *:* | | 808 | svchost.exe | 2021-04-05 09:17:45 UTC+0000 |
| 0x7d711730 | UDPv4 | 127.0.0.1:51727 | *:* | | 1336 | svchost.exe | 2021-04-05 09:11:54 UTC+0000 |
| 0x7d752170 | UDPv6 | ::1:1900 | *:* | | 1336 | svchost.exe | 2021-04-05 09:11:54 UTC+0000 |
| 0x7d753010 | UDPv4 | 192.168.0.18:51726 | *:* | | 1336 | svchost.exe | 2021-04-05 09:11:54 UTC+0000 |
| 0x7d753290 | UDPv4 | 192.168.0.18:1900 | *:* | | 1336 | svchost.exe | 2021-04-05 09:11:54 UTC+0000 |
| 0x7d755bb0 | UDPv4 | 127.0.0.1:1900 | *:* | | 1336 | svchost.exe | 2021-04-05 09:11:54 UTC+0000 |
| 0x7d78bce0 | UDPv4 | 0.0.0.0:3702 | *:* | | 332 | svchost.exe | 2021-04-05 09:11:54 UTC+0000 |
| 0x7d78d010 | UDPv4 | 0.0.0.0:3702 | *:* | | 332 | svchost.exe | 2021-04-05 09:11:54 UTC+0000 |
| 0x7d78d010 | UDPv6 | :::3702 | *:* | | 332 | svchost.exe | 2021-04-05 09:11:54 UTC+0000 |
| 0x7d790460 | UDPv4 | 0.0.0.0:51729 | *:* | | 332 | svchost.exe | 2021-04-05 09:11:54 UTC+0000 |
| 0x7d790460 | UDPv6 | :::51729 | *:* | | 332 | svchost.exe | 2021-04-05 09:11:54 UTC+0000 |
| 0x7d790ec0 | UDPv4 | 0.0.0.0:51728 | *:* | | 332 | svchost.exe | 2021-04-05 09:11:54 UTC+0000 |
| 0x7d791d00 | UDPv4 | 0.0.0.0:3702 | *:* | | 332 | svchost.exe | 2021-04-05 09:11:54 UTC+0000 |
| 0x7d791d00 | UDPv6 | :::3702 | *:* | | 332 | svchost.exe | 2021-04-05 09:11:54 UTC+0000 |
| 0x7d793aa0 | UDPv4 | 0.0.0.0:3702 | *:* | | 332 | svchost.exe | 2021-04-05 09:11:54 UTC+0000 |
| 0x7d82a460 | UDPv4 | 0.0.0.0:52450 | *:* | | 1336 | svchost.exe | 2021-04-05 09:10:22 UTC+0000 |
| 0x7d82b2b0 | UDPv4 | 0.0.0.0:52451 | *:* | | 1336 | svchost.exe | 2021-04-05 09:10:22 UTC+0000 |
| 0x7d82b2b0 | UDPv6 | :::52451 | *:* | | 1336 | svchost.exe | 2021-04-05 09:10:22 UTC+0000 |
| 0x7d854ec0 | UDPv4 | 0.0.0.0:123 | *:* | | 332 | svchost.exe | 2021-04-05 09:10:42 UTC+0000 |
| 0x7d854ec0 | UDPv6 | :::123 | *:* | | 332 | svchost.exe | 2021-04-05 09:10:42 UTC+0000 |
| 0x7d85b350 | UDPv4 | 0.0.0.0:5355 | *:* | | 1056 | svchost.exe | 2021-04-05 09:10:26 UTC+0000 |
| 0x7d85b350 | UDPv6 | :::5355 | *:* | | 1056 | svchost.exe | 2021-04-05 09:10:26 UTC+0000 |
| 0x7d8c9560 | UDPv4 | 0.0.0.0:123 | *:* | | 332 | svchost.exe | 2021-04-05 09:10:42 UTC+0000 |
| 0x7d8c9c60 | UDPv4 | 0.0.0.0:3702 | *:* | | 1336 | svchost.exe | 2021-04-05 09:10:41 UTC+0000 |
| 0x7d8cd500 | UDPv4 | 0.0.0.0:0 | *:* | | 1748 | svchost.exe | 2021-04-05 09:10:23 UTC+0000 |
| 0x7d8cd500 | UDPv6 | :::0 | *:* | | 1748 | svchost.exe | 2021-04-05 09:10:23 UTC+0000 |
| 0x7d8f0320 | UDPv6 | fe80::8595:580a:ffd7:758a:51724 | *:* | | 1336 | svchost.exe | 2021-04-05 09:11:54 UTC+0000 |
| 0x7d8f0490 | UDPv6 | fe80::8595:580a:ffd7:758a:1900 | *:* | | 1336 | svchost.exe | 2021-04-05 09:11:54 UTC+0000 |
| 0x7d8f0730 | UDPv6 | ::1:51725 | *:* | | 1336 | svchost.exe | 2021-04-05 09:11:54 UTC+0000 |
| 0x7d8f4010 | UDPv4 | 0.0.0.0:3702 | *:* | | 1336 | svchost.exe | 2021-04-05 09:10:41 UTC+0000 |
| 0x7d8f4010 | UDPv6 | :::3702 | *:* | | 1336 | svchost.exe | 2021-04-05 09:10:41 UTC+0000 |
| 0x7d9529c0 | UDPv4 | 0.0.0.0:3702 | *:* | | 1336 | svchost.exe | 2021-04-05 09:10:41 UTC+0000 |
| 0x7d806540 | TCPv4 | 0.0.0.0:5357 | 0.0.0.0:0 | LISTENING | 4 | System | |
| 0x7d806540 | TCPv6 | :::5357 | :::0 | LISTENING | 4 | System | |
| 0x7d855970 | TCPv4 | 0.0.0.0:49155 | 0.0.0.0:0 | LISTENING | 492 | services.exe | |
| 0x7d85f970 | TCPv4 | 0.0.0.0:445 | 0.0.0.0:0 | LISTENING | 4 | System | |
| 0x7d85f970 | TCPv6 | :::445 | :::0 | LISTENING | 4 | System | |
| 0x7d869880 | TCPv4 | 0.0.0.0:49155 | 0.0.0.0:0 | LISTENING | 492 | services.exe | |
| 0x7d869880 | TCPv6 | :::49155 | :::0 | LISTENING | 492 | services.exe | |
| 0x7d8a9230 | TCPv4 | 0.0.0.0:49156 | 0.0.0.0:0 | LISTENING | 1748 | svchost.exe | |
| 0x7d8a9230 | TCPv6 | :::49156 | :::0 | LISTENING | 1748 | svchost.exe | |
| 0x7d8cb230 | TCPv4 | 0.0.0.0:49156 | 0.0.0.0:0 | LISTENING | 1748 | svchost.exe | |
| 0x7d8ddef0 | TCPv4 | 0.0.0.0:3389 | 0.0.0.0:0 | LISTENING | 1056 | svchost.exe | |
| 0x7d8df740 | TCPv4 | 0.0.0.0:3389 | 0.0.0.0:0 | LISTENING | 1056 | svchost.exe | |

- **Extraer hashes almacenados en la memoria**

Primero con el comando: **sudo python vol.py --profile=Win7SP1x64 hivelist -f ~/Desktop/memdump.mem**

Obtenemos el registro , nos interesan las direcciones SAM y SYSTEM



| Virtual | Physical | Name |
|---|---|---|
| 0xfffff8a00000d010 | 0x000000002d740010 | [no name] |
| 0xfffff8a000024010 | 0x000000002d6a5010 | \REGISTRY\MACHINE\SYSTEM |
| 0xfffff8a00004e320 | 0x000000002d5cf320 | \REGISTRY\MACHINE\HARDWARE |
| 0xfffff8a0000a3410 | 0x000000007b71a410 | \??\C:\System Volume Information\Syscache.hve |
| 0xfffff8a0006e8010 | 0x000000003c388010 | \Device\HarddiskVolume1\Boot\BCD |
| 0xfffff8a0007f5010 | 0x000000003ad2f010 | \SystemRoot\System32\Config\SOFTWARE |
| 0xfffff8a000a1a010 | 0x0000000039e7f010 | \SystemRoot\System32\Config\DEFAULT |
| 0xfffff8a000bee010 | 0x000000003954a010 | \SystemRoot\System32\Config\SECURITY |
| 0xfffff8a000c4b410 | 0x0000000026fb6410 | \SystemRoot\System32\Config\SAM |
| 0xfffff8a000d99010 | 0x0000000073e83010 | \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT |
| 0xfffff8a000e65160 | 0x000000003886f160 | \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT |
| 0xfffff8a001334010 | 0x000000001becb010 | \??\C:\Users\romero\ntuser.dat |
| 0xfffff8a0013ef010 | 0x000000001c464010 | \??\C:\Users\romero\AppData\Local\Microsoft\Windows\UsrClass.dat |

Por último con el comando**: sudo python vol.py hashdump --profile=Win7SP1x64 sys-offset=0xfffff8a000024010 sam-offset=0xfffff8a000c4b410 -f ~/Desktop/memdump.mem > hashesmemoria.txt**

Otra forma de comando: **sudo python vol.py --profile=Win7SP1x64 hashdump -f ~/Desktop/memdump.mem -y 0xfffff8a000024010 -s 0xfffff8a000c4b410 > hashesmemoria.txt**

Debería extraer los hashes pero da un error y puede ser porque no tengo bien instalado volatility

Ejemplo de que debería salir

You will have to replace the two hexadecimal addresses with the correct virtual addresses of your hives, in this format:

-y SYSTEM -s SAM

```
volatility hashdump --profile=Win2008SP1x86 -f memdump.mem -y 0x86226008 -s 0x89c33450
```

When you get the command correct, you will see the login account names and hashed passwords, as shown below.

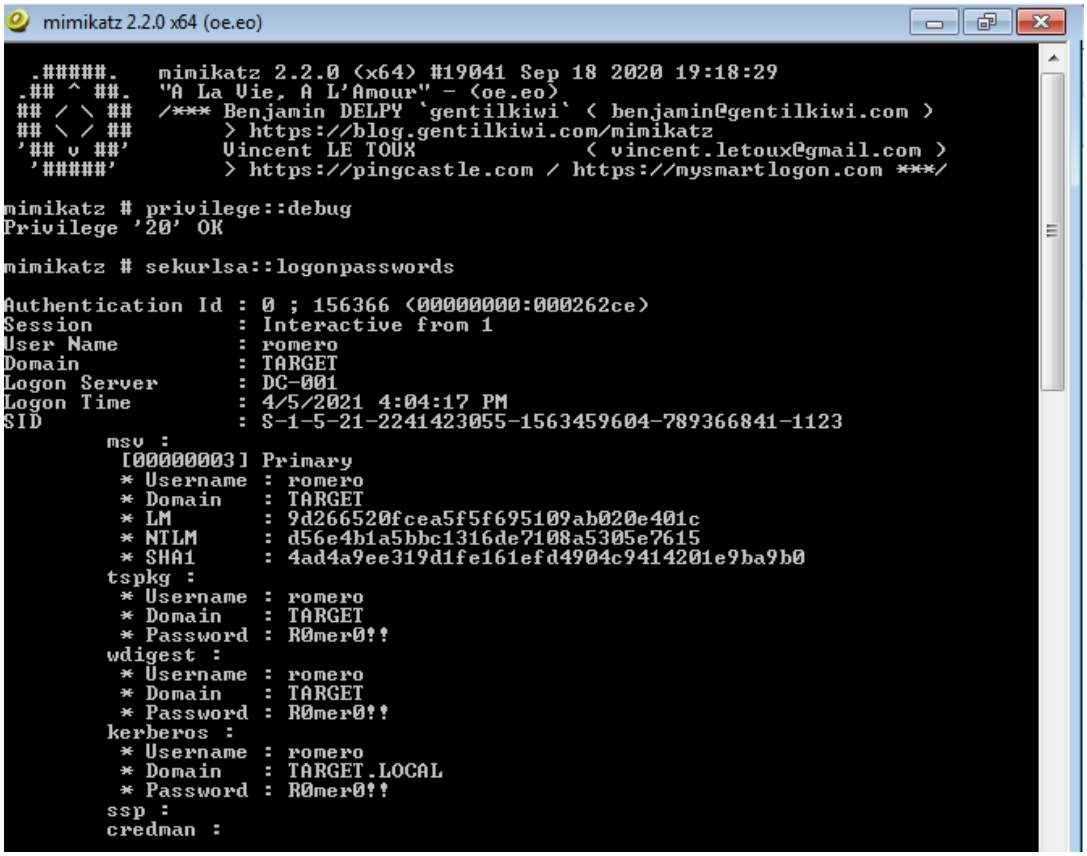
Windows stores two hashes with each password, delimited by colons. The first one is an extremely insecure, obsolete hash using the they are filled with a dummy value starting with "aad".

The second hash is the newer NTLM hash, which is much better than LANMAN hashes, but still extremely insecure and much more

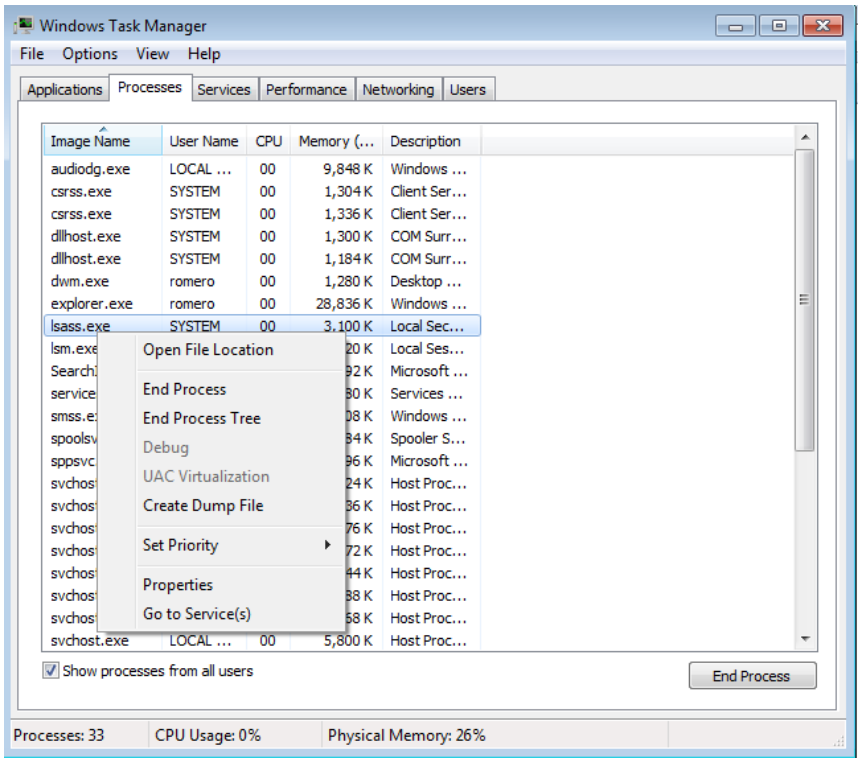
```
root@kali:~/152# volatility hashdump --profile=Win2008SP1x86 -f memdump.mem -y 0x86226008 -s 0x89c33450
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
student:1000:aad3b435b51404eeaad3b435b51404ee:e19c[redacted]:::
probe:1002:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
waldo:1004:aad3b435b51404eeaad3b435b51404ee:cfeac129dc5e61b2eb9b2e7131fc7e2b:::
YOUR-NAME:1005:aad3b435b51404eeaad3b435b51404ee:958c8526e4252b277d8d70adbd2ea2ce:::
```

# Parte Windows con SysInternals

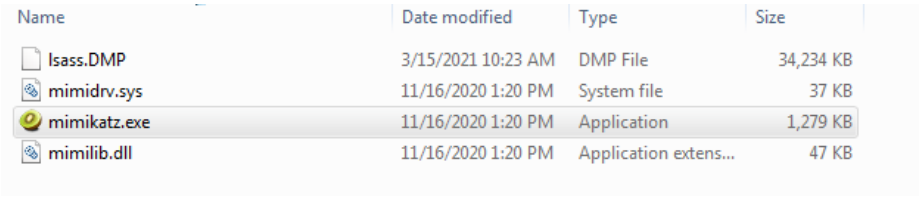
## Identificar contraseñas almacenadas en el equipo



Otra forma es con el fichero lsass

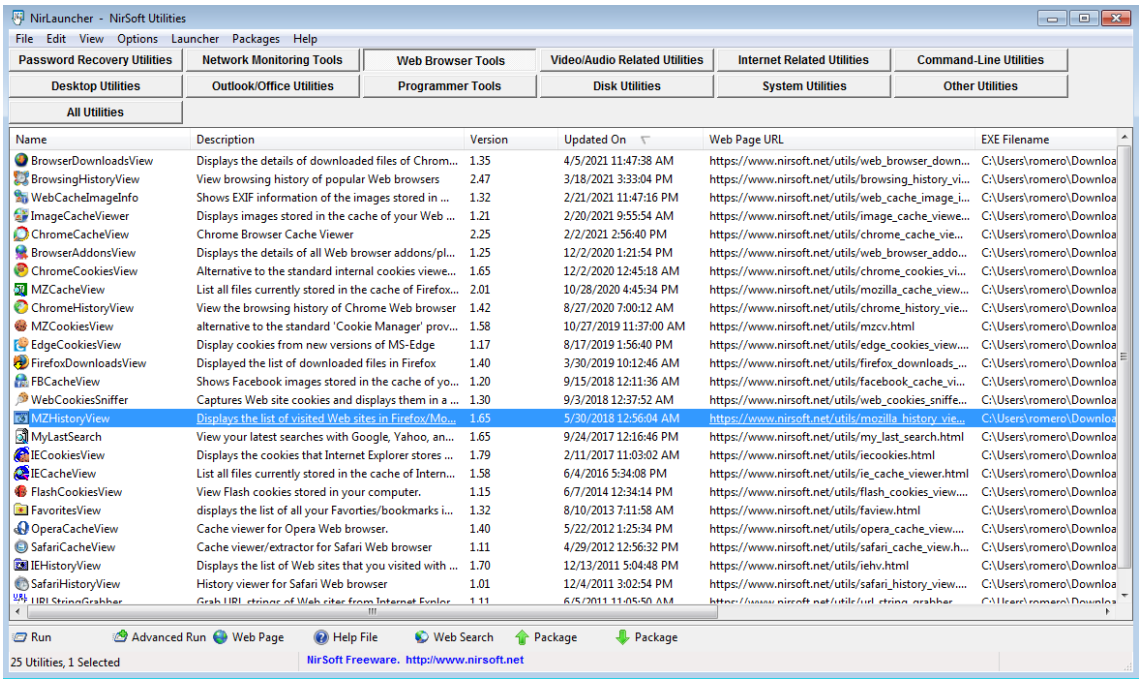


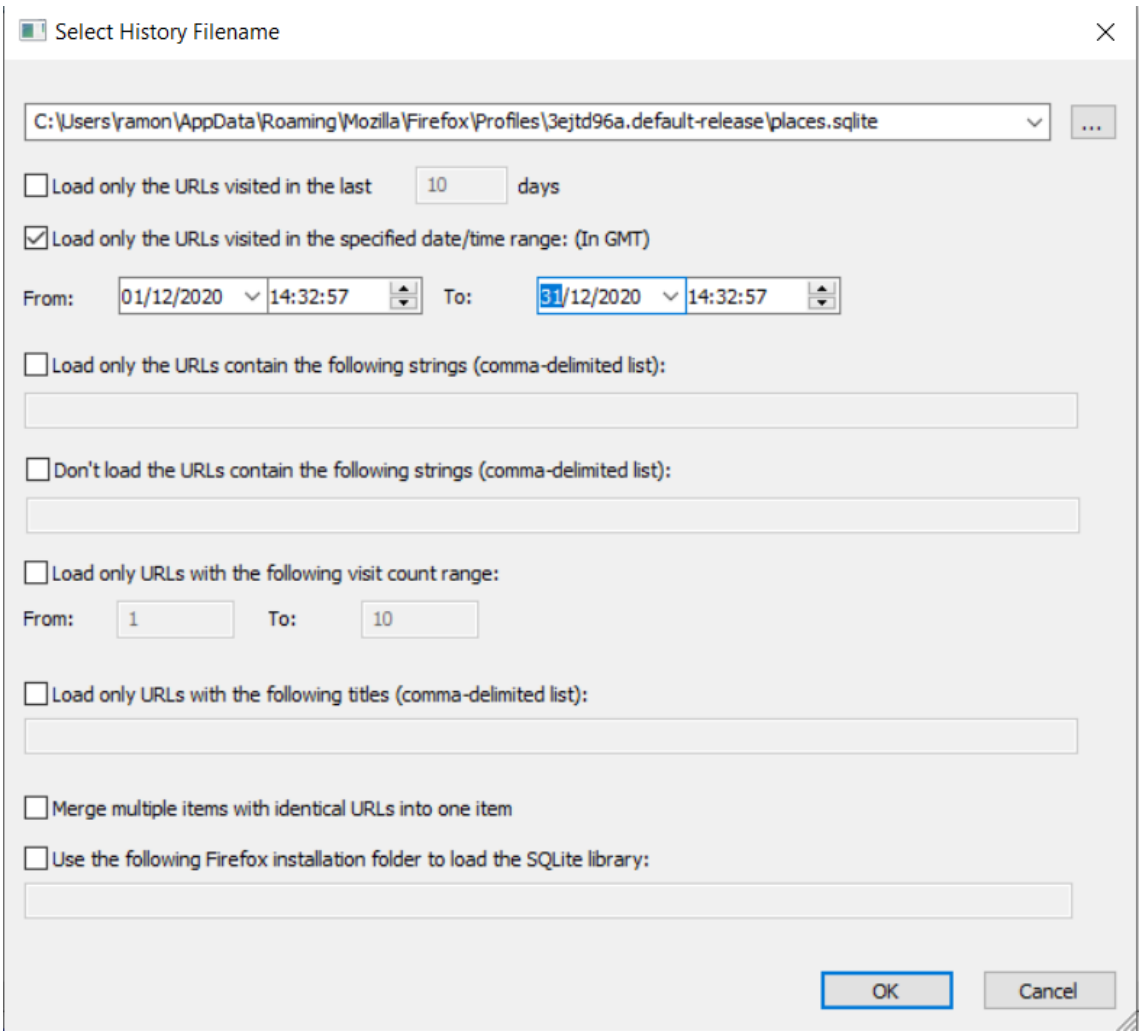

El archivo creado nos lo llevamos a la carpeta donde tengamos el ejecutable de Mimi Katz

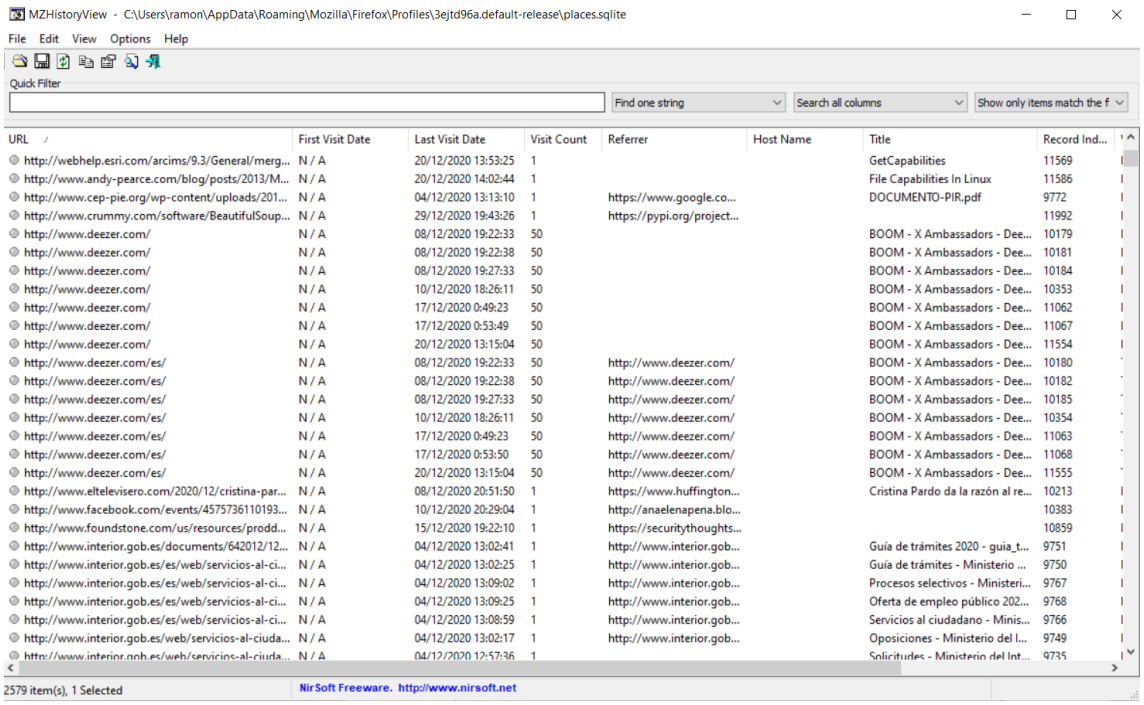



```
mimikatz # sekurlsa::minidump lsass.dmp
Switch to MINIDUMP : 'lsass.dmp'

mimikatz # sekurlsa::logonpasswords
Opening : 'lsass.dmp' file for minidump...

Authentication Id : 0 ; 108257 (00000000:0001a6e1)
Session           : Interactive from 1
User Name         : romero
Domain            : TARGET
Logon Server      : DC-001
Logon Time        : 3/15/2021 9:27:36 AM
SID               : S-1-5-21-2241423055-1563459604-789366841-1123
        msv :
         [00000003] Primary
         * Username : romero
         * Domain   : TARGET
         * LM       : 9d266520fcea5f5f695109ab020e401c
         * NTLM     : d56e4b1a5bbc1316de7108a5305e7615
         * SHA1     : 4ad4a9ee319d1fe161efd4904c9414201e9ba9b0
        tspkg :
         * Username : romero
         * Domain   : TARGET
         * Password : R0mer0!!
        wdigest :
         * Username : romero
         * Domain   : TARGET
         * Password : R0mer0!!
        kerberos :
         * Username : romero
         * Domain   : TARGET.LOCAL
```

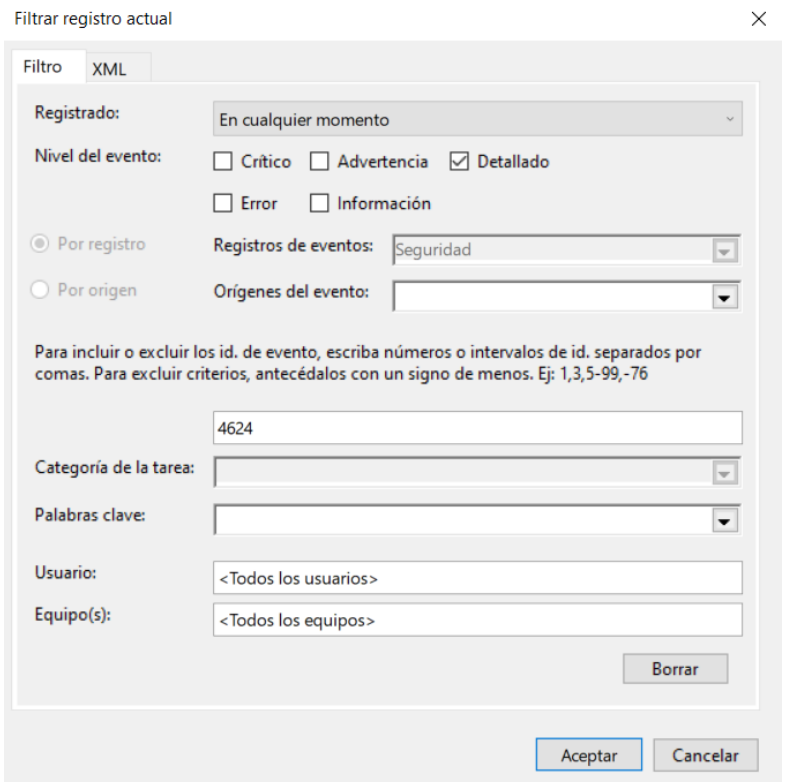
## Listado de webs accedidas en diciembre



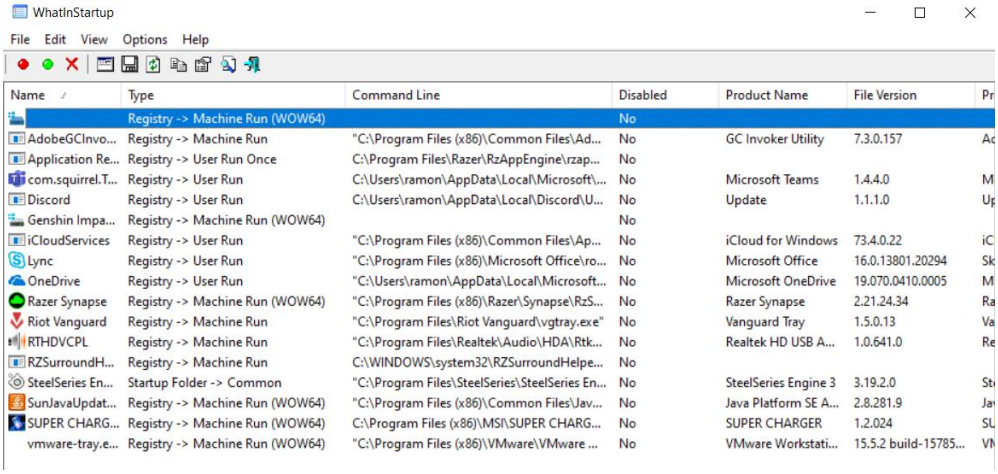



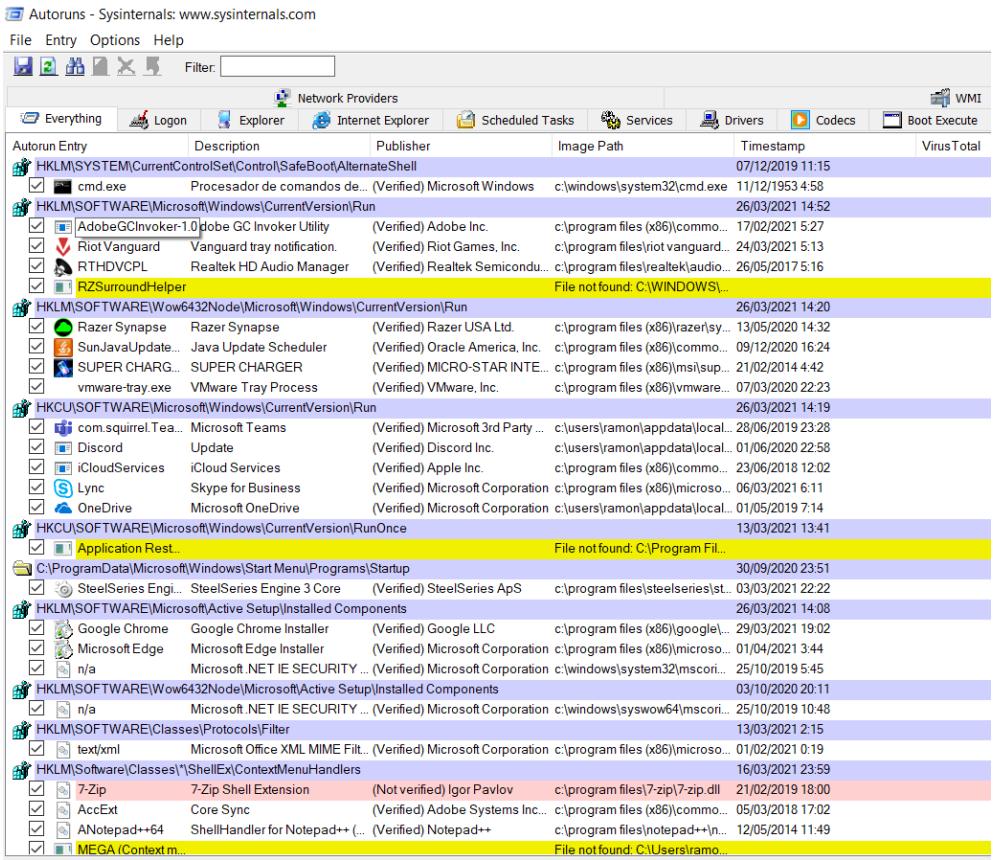


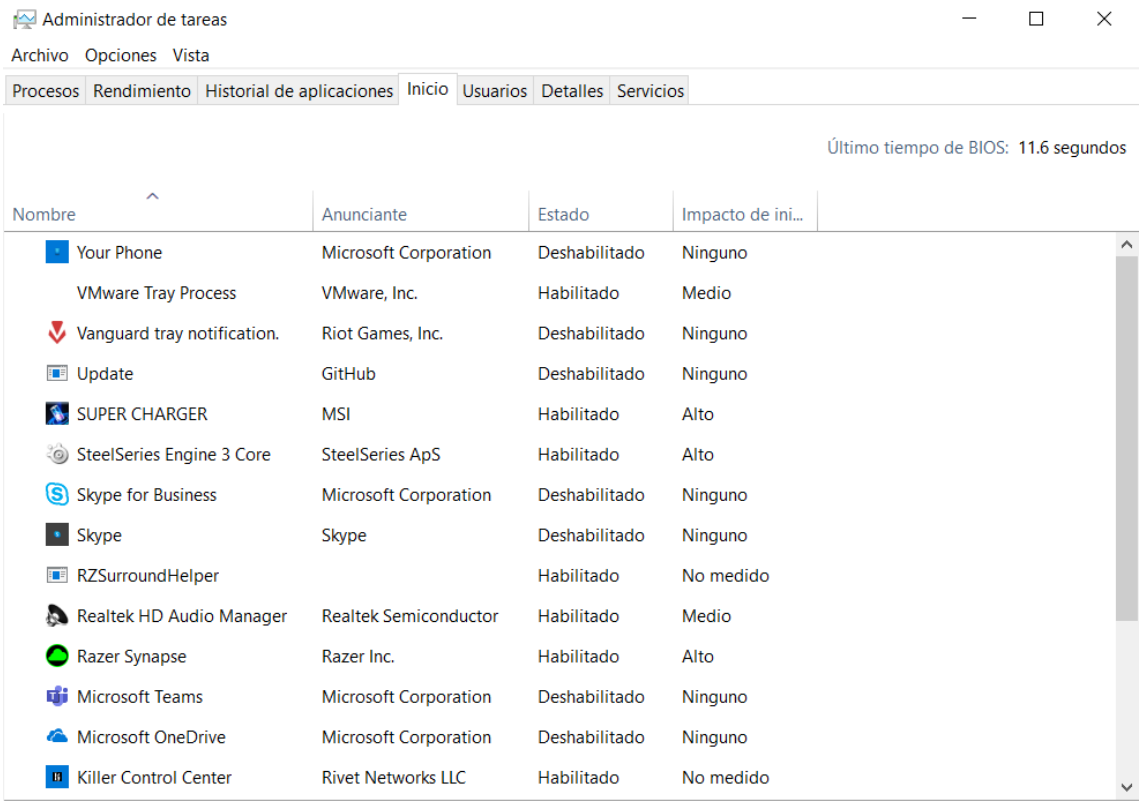

## Listado de autenticaciones con fecha y hora que se han realizado en el sistema



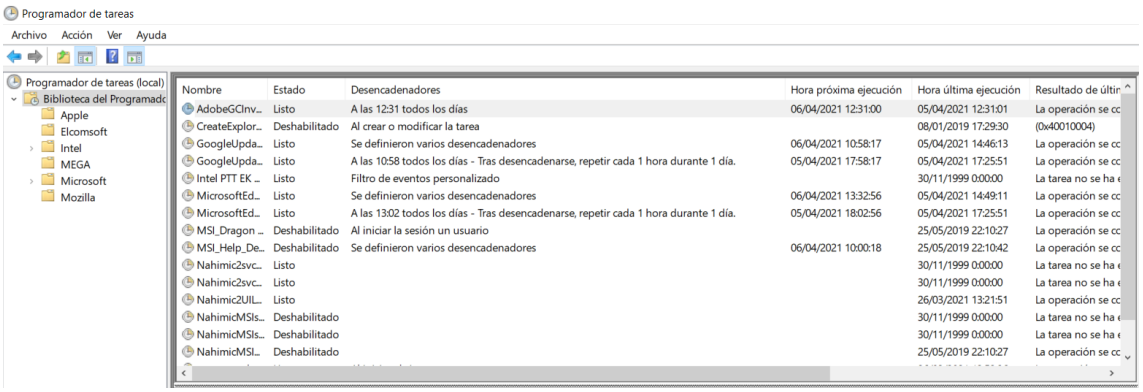

## Analizar herramientas que se ejecuten en el arranque

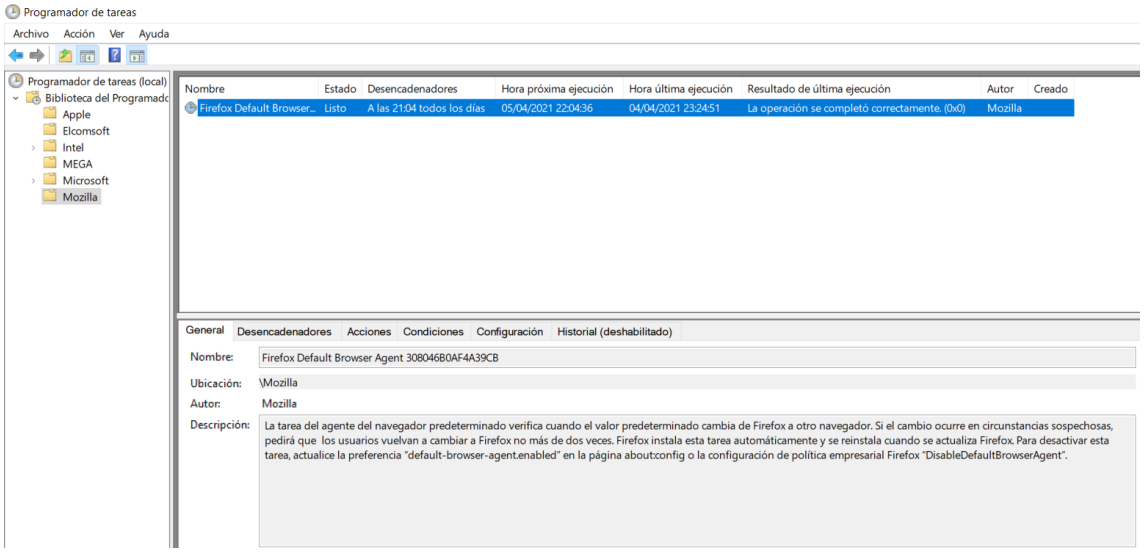


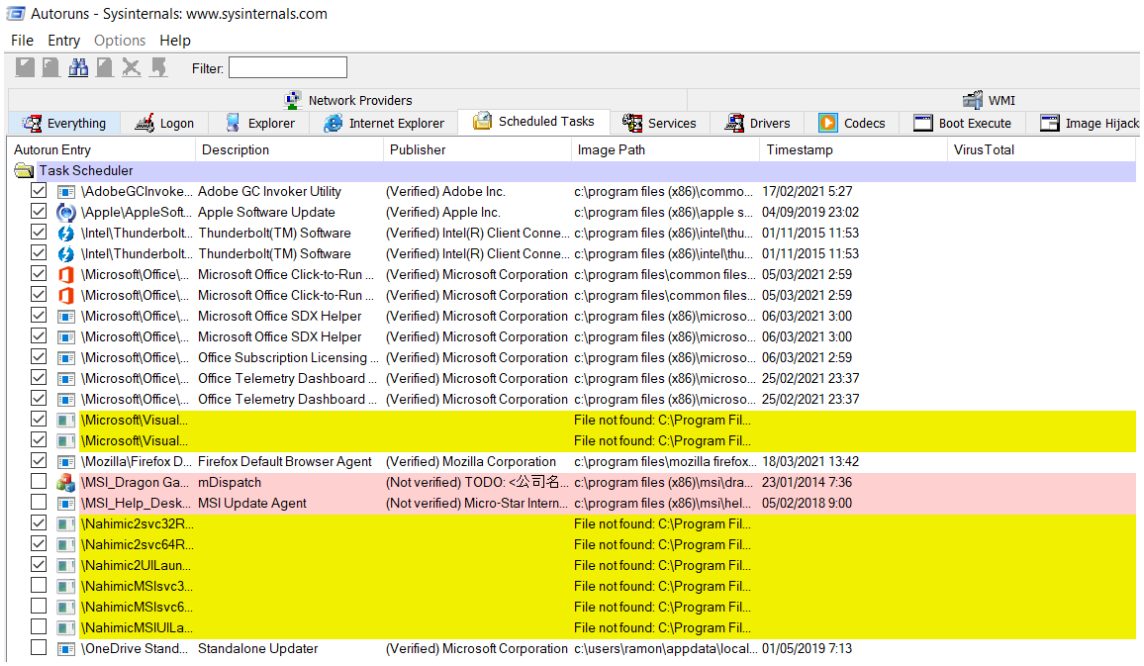



## Analizar tareas programadas en el equipo



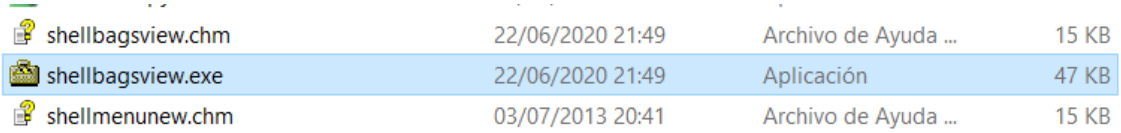


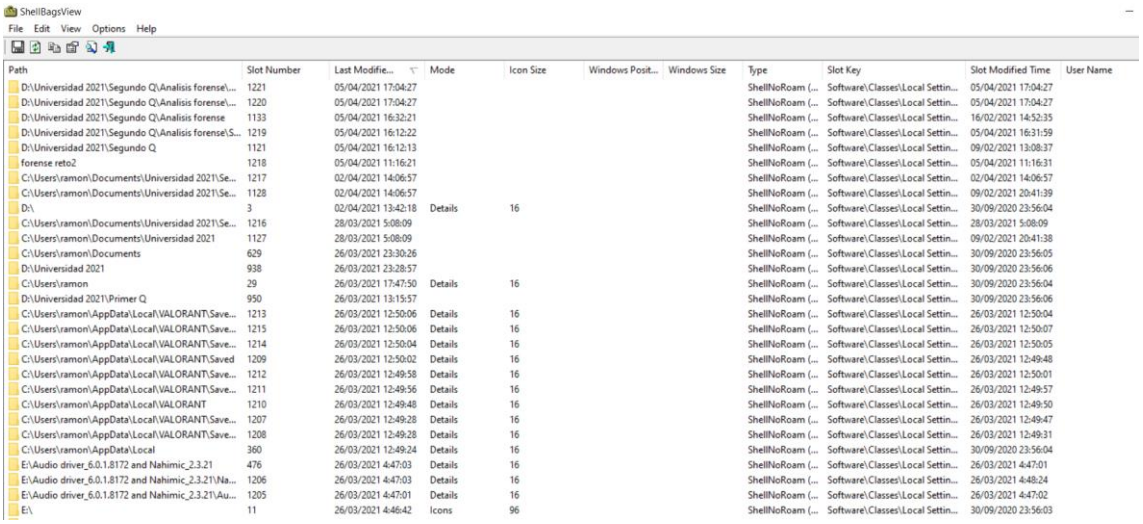

## Sysinternasl Autoruns Scheduled Tasks



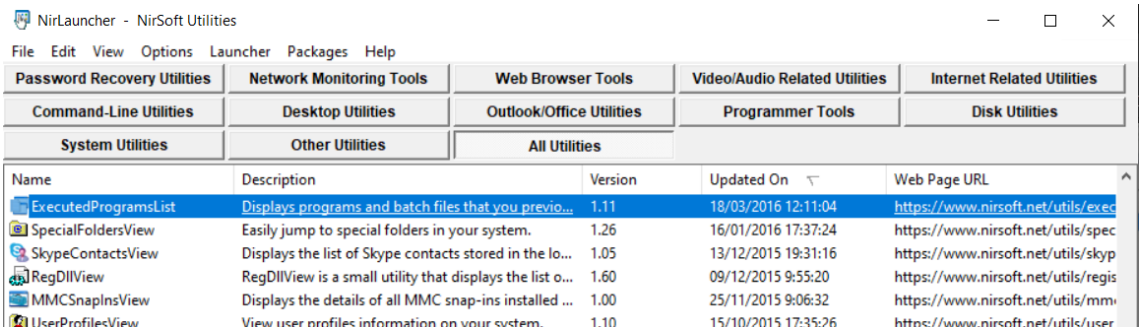

## Analizar shellbags en el equipo.

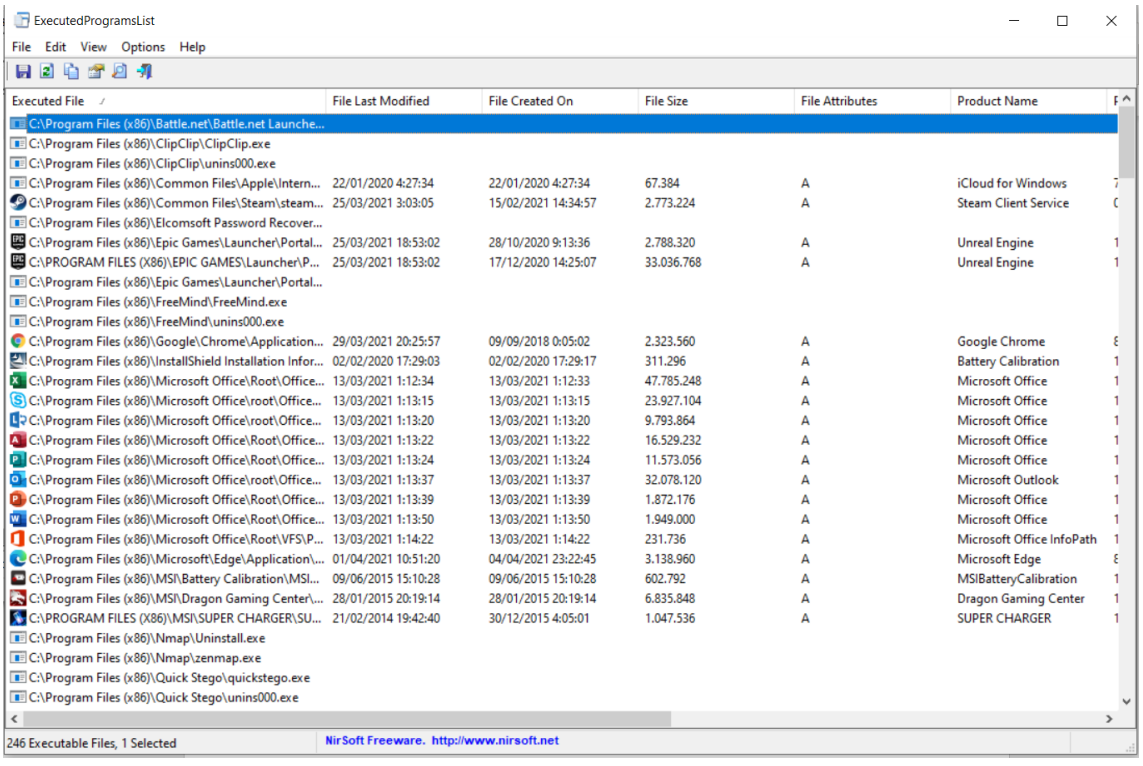
Para esto tenemos que ejecutar como administrador



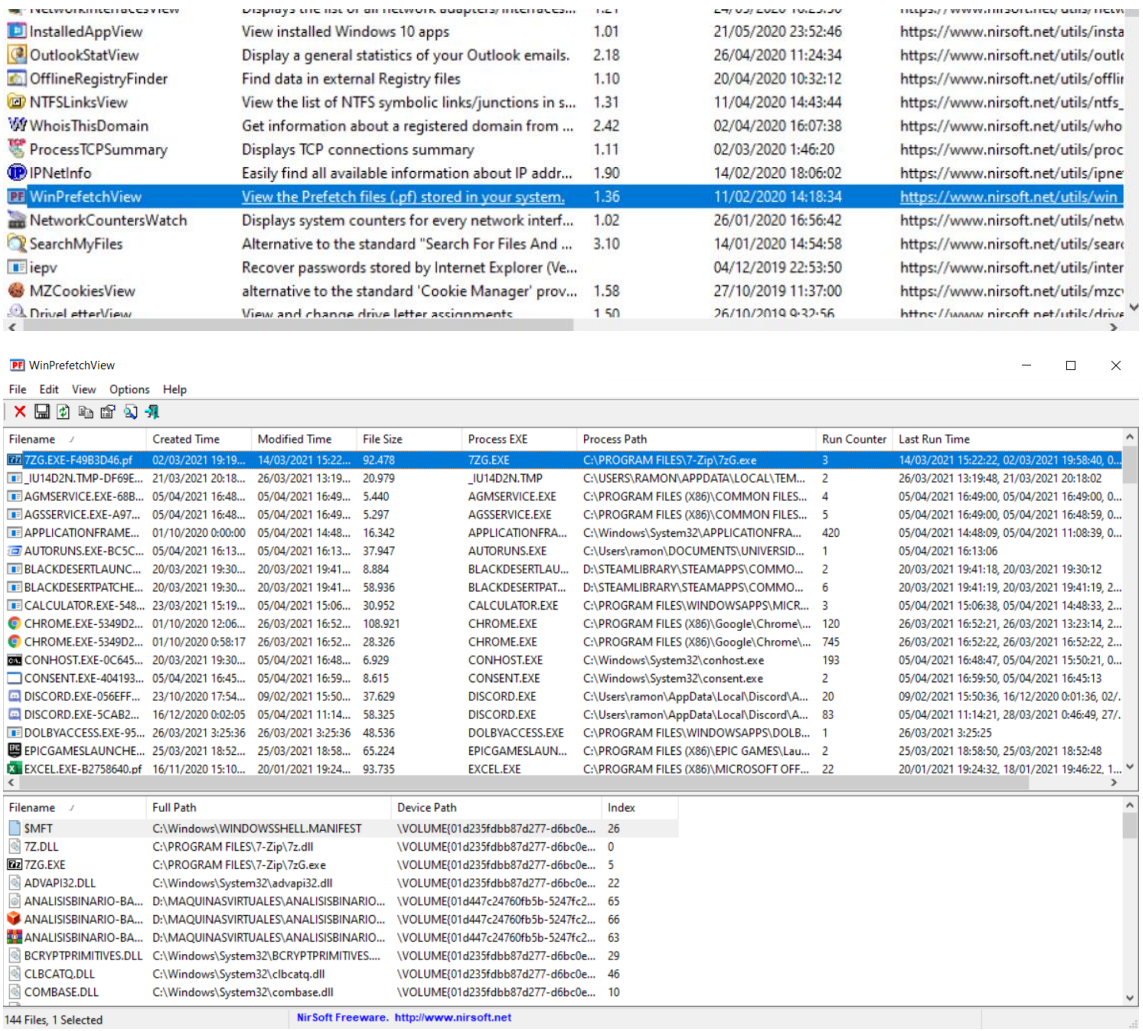



## Analizar ficheros prefetch en el equipo.



Otra utilidad de Nirsoft : **WinPrefetchView**



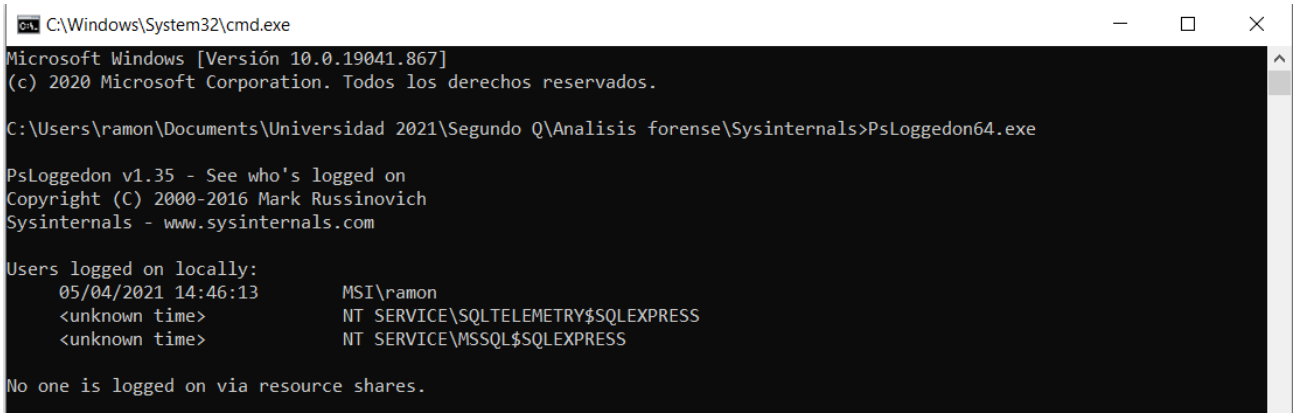
| | | | | |
|---|---|---|---|---|
| InstalledAppView | View installed Windows 10 apps | 1.01 | 21/05/2020 23:52:46 | https://www.nirsoft.net/utils/insta |
| OutlookStatView | Display a general statistics of your Outlook emails. | 2.18 | 26/04/2020 11:24:34 | https://www.nirsoft.net/utils/outl |
| OfflineRegistryFinder | Find data in external Registry files | 1.10 | 20/04/2020 10:32:12 | https://www.nirsoft.net/utils/offli |
| NTFSLinksView | View the list of NTFS symbolic links/junctions in s... | 1.31 | 11/04/2020 14:43:44 | https://www.nirsoft.net/utils/ntfs_ |
| WhoisThisDomain | Get information about a registered domain from ... | 2.42 | 02/04/2020 16:07:38 | https://www.nirsoft.net/utils/who |
| ProcessTCPSummary | Displays TCP connections summary | 1.11 | 02/03/2020 1:46:20 | https://www.nirsoft.net/utils/proc |
| IPNetInfo | Easily find all available information about IP addr... | 1.90 | 14/02/2020 18:06:02 | https://www.nirsoft.net/utils/ipne |
| WinPrefetchView | View the Prefetch files (.pf) stored in your system. | 1.36 | 11/02/2020 14:18:34 | https://www.nirsoft.net/utils/win |
| NetworkCountersWatch | Displays system counters for every network interf... | 1.02 | 26/01/2020 16:56:42 | https://www.nirsoft.net/utils/netw |
| SearchMyFiles | Alternative to the standard "Search For Files And ... | 3.10 | 14/01/2020 14:54:58 | https://www.nirsoft.net/utils/sear |
| iepv | Recover passwords stored by Internet Explorer (Ve... | | 04/12/2019 22:53:50 | https://www.nirsoft.net/utils/inter |
| MZCookiesView | alternative to the standard 'Cookie Manager' prov... | 1.58 | 27/10/2019 11:37:00 | https://www.nirsoft.net/utils/mzc |




## Otras utilidades de Sysinternals Suite

- **PsLoggedon.exe**

  Nos dice los usuarios logados en el sistema localmente donde el segundo y el tercero son cuentas de servicio



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Versión 10.0.19041.867]
(c) 2020 Microsoft Corporation. Todos los derechos reservados.

C:\Users\ramon\Documents\Universidad 2021\Segundo Q\Analisis forense\Sysinternals>PsLoggedon64.exe

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

Users logged on locally:
     05/04/2021 14:46:13        MSI\ramon
     <unknown time>             NT SERVICE\SQLTELEMETRY$SQLEXPRESS
     <unknown time>             NT SERVICE\MSSQL$SQLEXPRESS

No one is logged on via resource shares.
```

- **Logonsessions.exe**

```
C:\Users\ramon\Documents\Universidad 2021\Segundo Q\Analisis forense\Sysinternals>logonsessions.exe

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\MSI$
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          S-1-5-18
    Logon time:   26/03/2021 14:52:26
    Logon server:
    DNS Domain:
    UPN:
```

```
[12] Logon session 00000000:00abd8aa:
    User name:    MSI\ramon
    Auth package: CloudAP
    Logon type:   Interactive
    Session:      3
    Sid:          S-1-5-21-2175565578-157587113-1341888070-1001
    Logon time:   26/03/2021 23:24:47
    Logon server:
    DNS Domain:
    UPN:
```

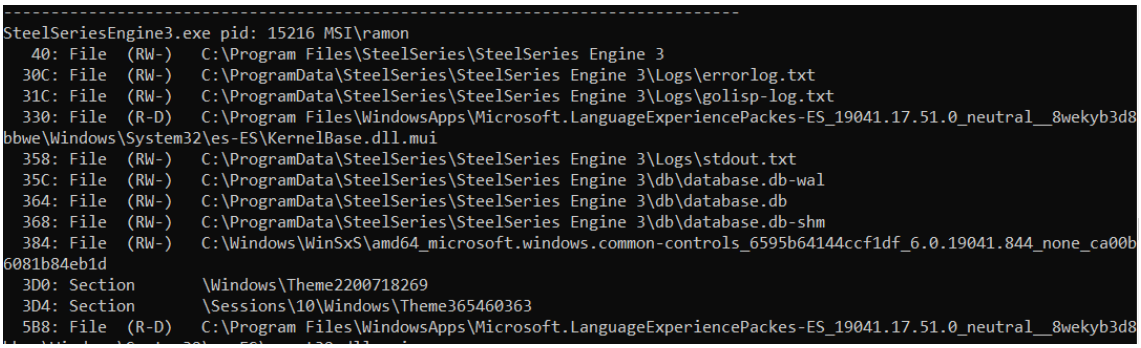
- **Listdlls.exe**

Las librerías que usa cada proceso en ejecución

```
------------------------------------------------------------------------------
VirtualBoxVM.exe pid: 11536
Command line: 60eaff78-4bdd-042d-2e72-669728efd737-suplib-3rdchild --comment "Windows Server 2008 r
-3355-4825-8ddc-ef4a70729581 --no-startvm-errormsgbox "--sup-hardening-log=D:\MaquinasVirtuales\Ret
8 r2\Logs\VBoxHardening.log"

Base               Size      Path
0x00000000e3680000  0x118000  C:\Program Files\Oracle\VirtualBox\VirtualBoxVM.exe
0x0000000026470000  0x1f5000  C:\WINDOWS\SYSTEM32\ntdll.dll
0x0000000025730000  0xbd000   C:\WINDOWS\System32\KERNEL32.DLL
0x0000000023bb0000  0x2c9000  C:\WINDOWS\System32\KERNELBASE.dll
0x00000000179d0000  0x5000    C:\Program Files\Oracle\VirtualBox\VBoxSupLib.DLL
0x0000000024290000  0x60000   C:\WINDOWS\System32\Wintrust.dll
0x00000000249b0000  0x9e000   C:\WINDOWS\System32\msvcrt.dll
0x0000000025450000  0x12b000  C:\WINDOWS\System32\RPCRT4.dll
0x0000000024100000  0x15f000  C:\WINDOWS\System32\CRYPT32.dll
0x00000000242f0000  0x100000  C:\WINDOWS\System32\ucrtbase.dll
0x00000000237a0000  0x12000   C:\WINDOWS\SYSTEM32\MSASN1.dll
```

- **Handle.exe**

Son los diferentes ficheros que utiliza un proceso


SteelSeriesEngine3.exe pid: 15216 MSI\ramon
40: File (RW-) C:\Program Files\SteelSeries\SteelSeries Engine 3
30C: File (RW-) C:\ProgramData\SteelSeries\SteelSeries Engine 3\Logs\errorlog.txt
31C: File (RW-) C:\ProgramData\SteelSeries\SteelSeries Engine 3\Logs\golisp-log.txt
330: File (R-D) C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackes-ES_19041.17.51.0_neutral__8wekyb3d8
bbwe\Windows\System32\es-ES\KernelBase.dll.mui
358: File (RW-) C:\ProgramData\SteelSeries\SteelSeries Engine 3\Logs\stdout.txt
35C: File (RW-) C:\ProgramData\SteelSeries\SteelSeries Engine 3\db\database.db-wal
364: File (RW-) C:\ProgramData\SteelSeries\SteelSeries Engine 3\db\database.db
368: File (RW-) C:\ProgramData\SteelSeries\SteelSeries Engine 3\db\database.db-shm
384: File (RW-) C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.844_none_ca00b
6081b84eb1d
3D0: Section \Windows\Theme2200718269
3D4: Section \Sessions\10\Windows\Theme365460363
5B8: File (R-D) C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackes-ES_19041.17.51.0_neutral__8wekyb3d8