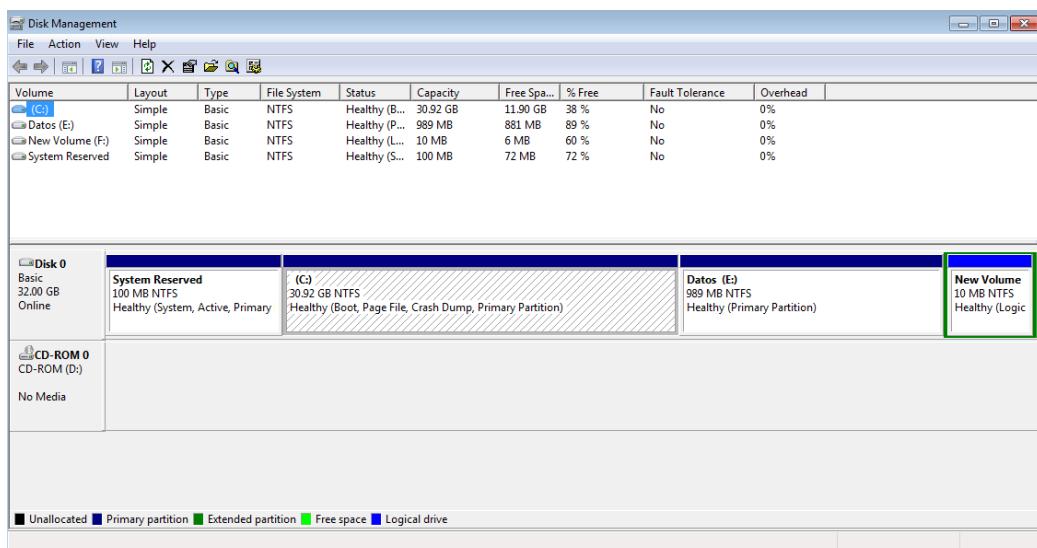


ANALISIS FORENSE

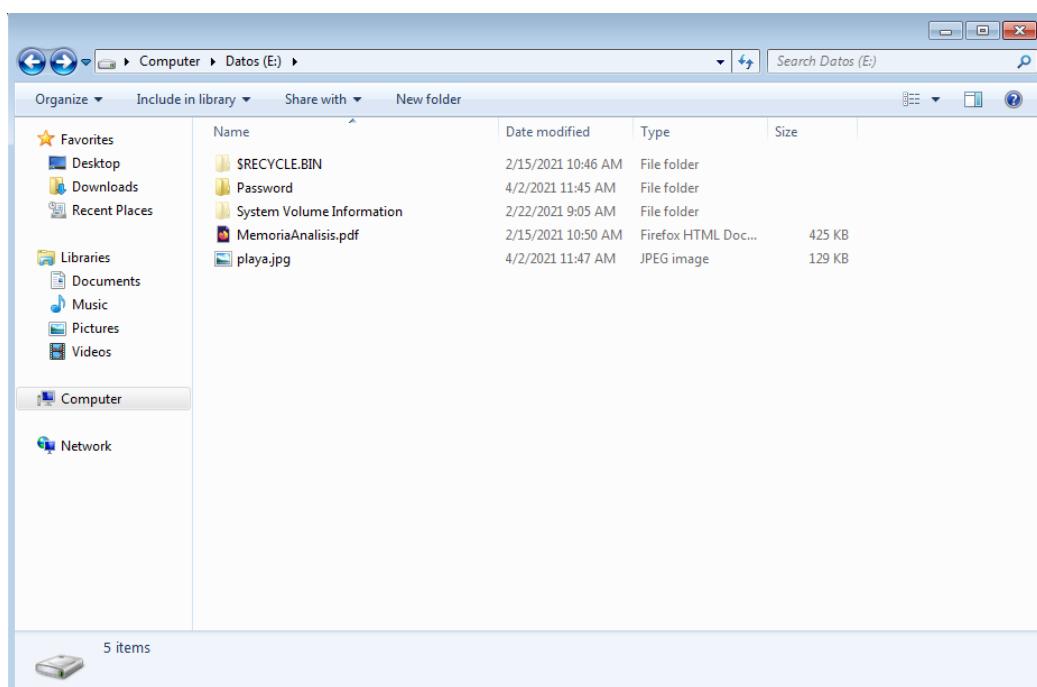
Practica 1 Ramón Rojas Soto

Recuperar ficheros con File Carving de una partición.

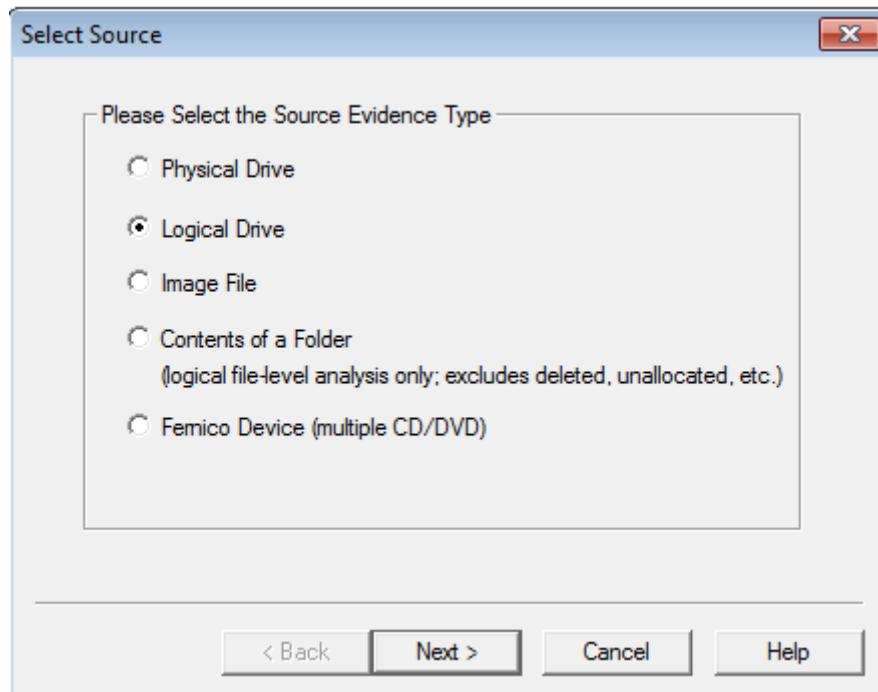
Tenemos varias partición ya creadas , en nuestro caso vamos a seleccionar la partición Datos (E:)



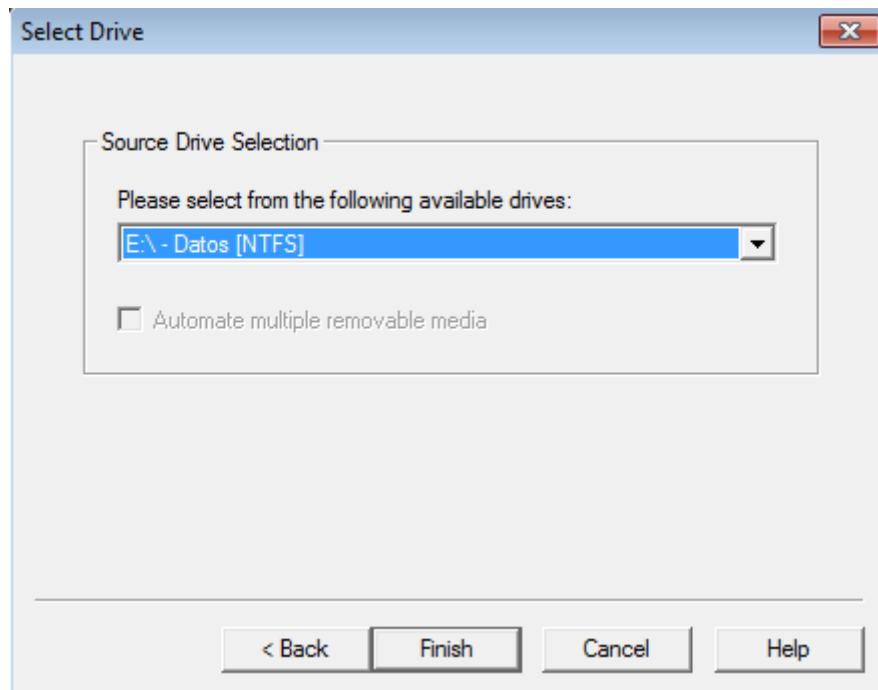
El contenido de la partición son un pdf, una imagen y dentro de la carpeta passwords un archivo txt con una contraseña



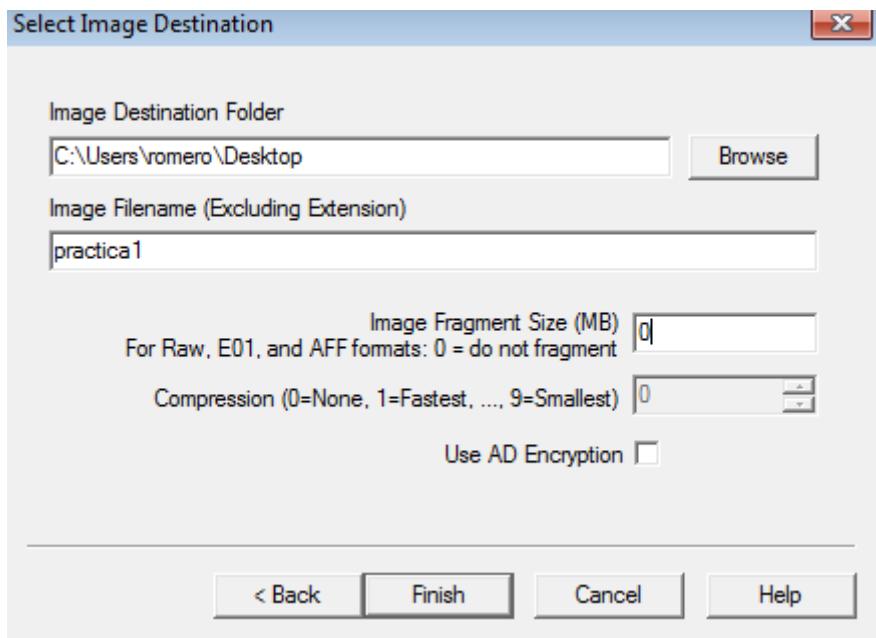
En el FTK imager File -> Create disk image cuando estamos en este menú seleccionamos la opción de Logical Drive



Marcamos la partición que queremos copiar



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

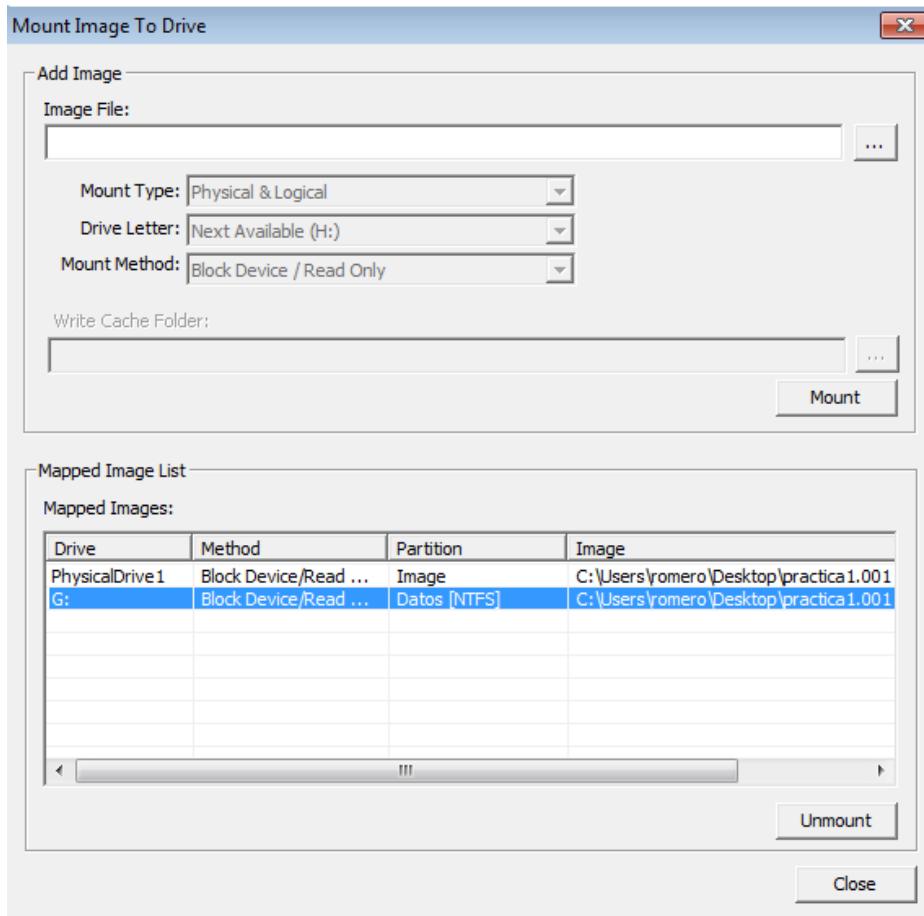


Una vez creada aparte de nuestra imagen se nos genera un archivo txt de informa

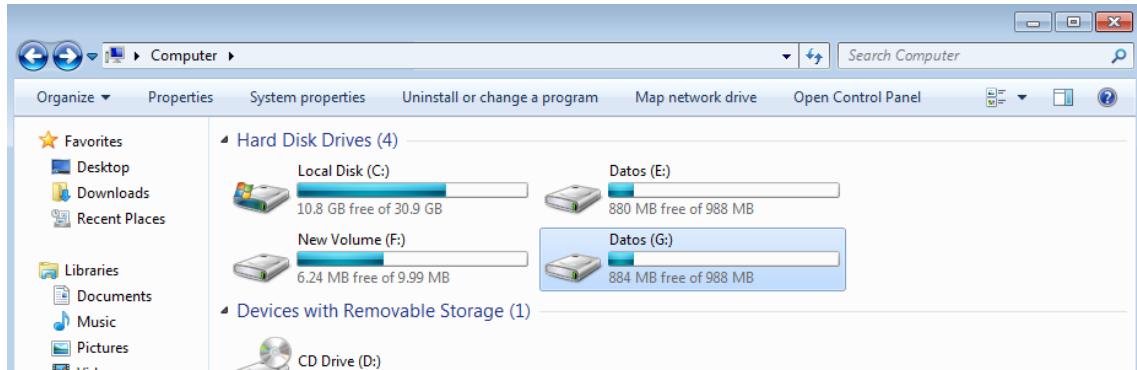
```
practica1.001.txt - Notepad
File Edit View Help
-----
Information for c:\users\romero\Desktop\practica1:
Physical Evidentiary Item (source) Information:
[Device Info]
Source Type: Logical
[Drive Geometry]
Bytes per Sector: 512
Sector Count: 2,025,472
[Physical Drive Information]
Removable drive: False
Source data size: 989 MB
Sector count: 2025472
[Computed Hashes]
MD5 checksum: ae9da9b719757e3f1cee5868539a617b
SHA1 checksum: a42780001014c4f06a5ffe32ff6653b6007b2a9a

Image Information:
Acquisition started: Fri Apr 02 11:51:01 2021
Acquisition finished: Fri Apr 02 11:51:11 2021
Segment list:
C:\Users\romero\Desktop\practica1.001
```

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

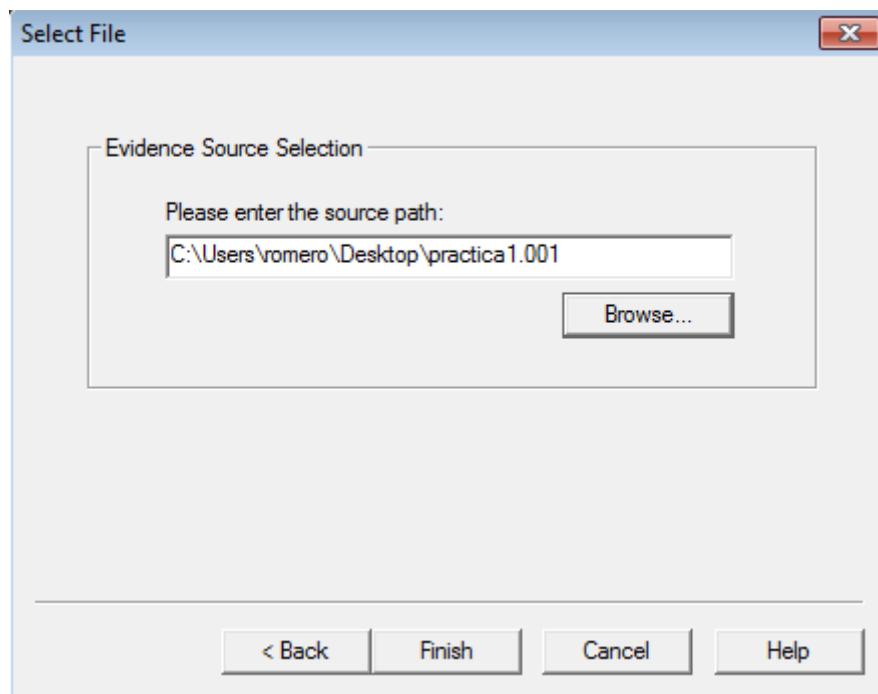


Que lo que hace es montarnos la copia que acabamos de crear como otro disco duro mas al que podemos acceder como haríamos normalmente

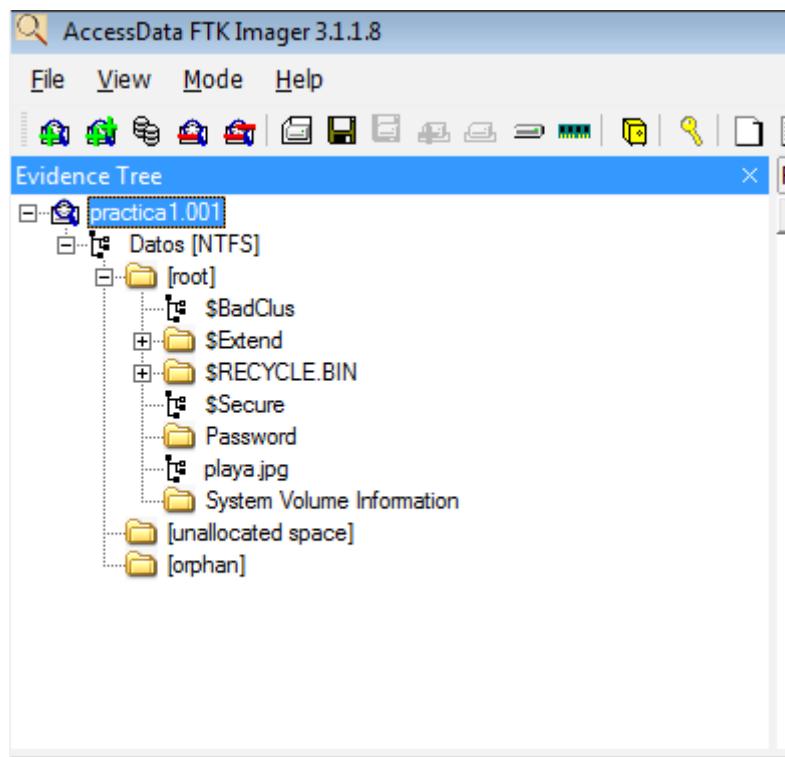


Y la otra que es mas visual para usar la herramienta es File -> Add evidence item -> Image File

Seleccionamos nuestra imagen



Y nos la despliega dentro de la herramienta



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

Evidence Tree

practica1.001

Datos [NTFS]

[root]

- \$BadClus
- \$Extend
- \$RECYCLE.BIN
- \$Secure
- Password
- playa.jpg
- System Volume Information
- [unallocated space]
- [orphan]

File List

Name
deberes.txt

abc123

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

Evidence Tree

practica1.001

Datos [NTFS]

[root]

- \$BadClus
- \$Extend
- \$RECYCLE.BIN
- \$Secure
- Password
- playa.jpg
- System Volume Information
- [unallocated space]
- [orphan]

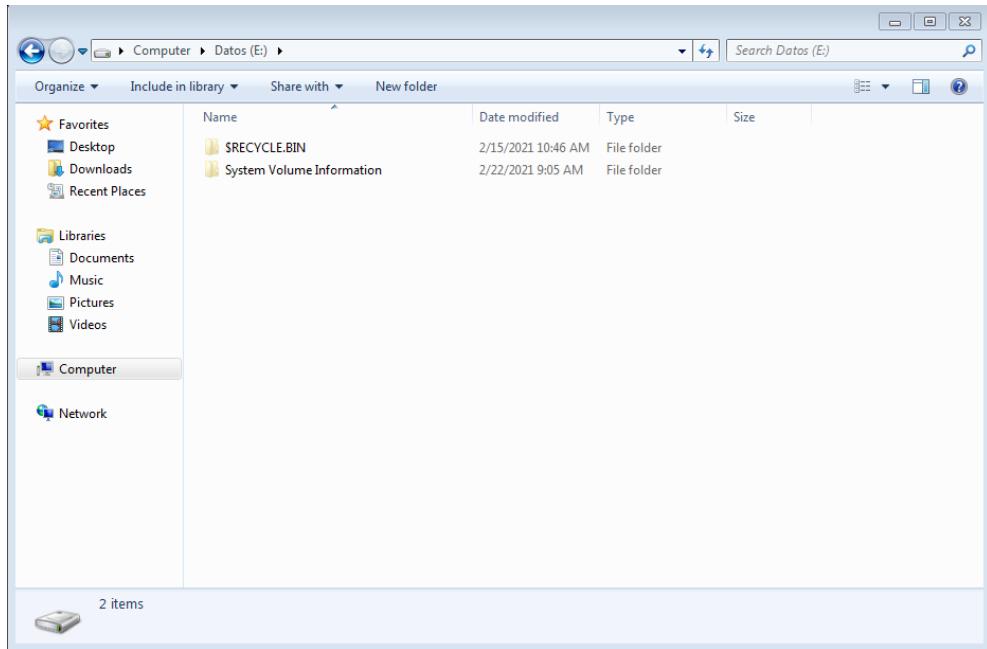
File List

Name	Size	Type	Date Modified
Zone.Identifier	1	Alternate Data ...	4/2/2021 9:47:1...

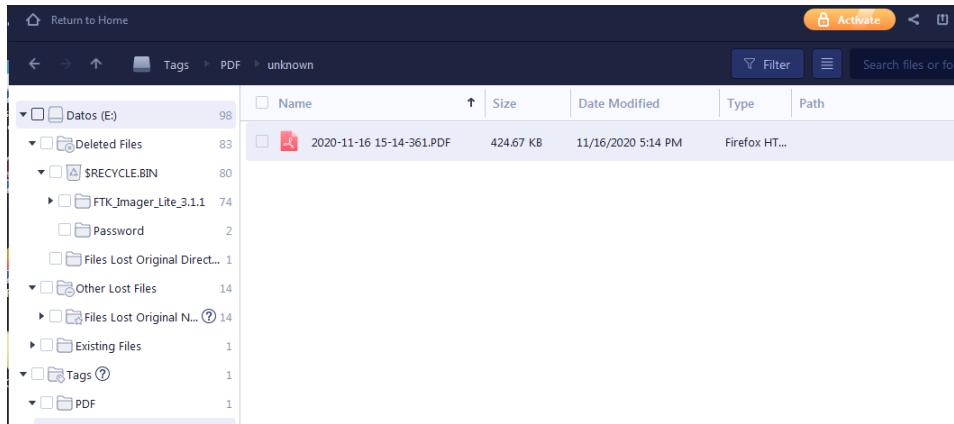


EaseUS recovery

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



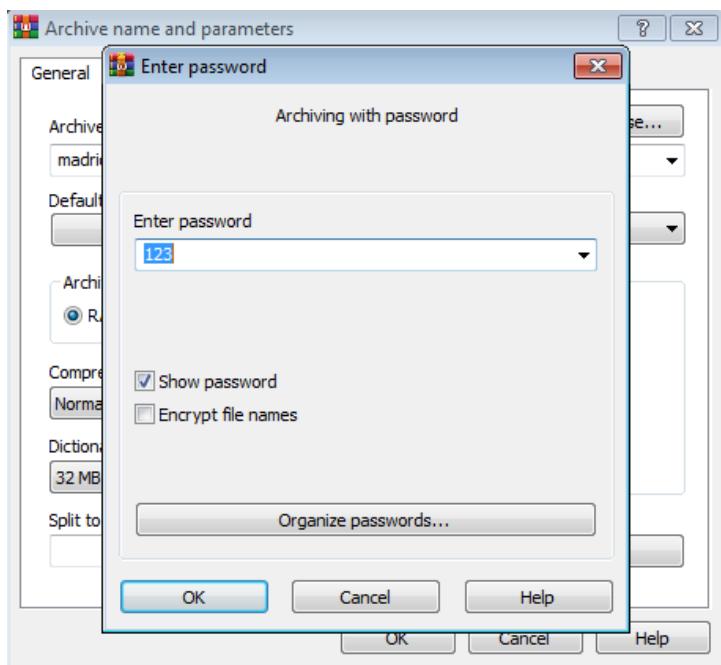
Esta herramienta también nos ofrece la posibilidad de recuperar el archivo eliminado

The screenshot shows a file recovery interface. A single file, '\$R19JGEN.jpg', is selected in a list. The list includes columns: Name, Size, Date Modified, Type, and Path. The file '\$R19JGEN.jpg' has a size of 32 KB, was modified on 4/2/2021 11:47 AM, is a JPEG image, and is located in E:\Other deleted files. A 'Recover' button is visible at the bottom right, along with the text 'Selected: 1 files (32 KB)'.

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

Find Encrypted Files

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\romeo... \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 SCANNED SKIPPED TIME ELAPSED
7 12,230 205 20 seconds

SCAN OPTIONS WHERE TO SCAN
[Scan Slow File Types](#) [4 folders](#)

[Save Files List](#) 1 FILE SELECTED [...](#) [COPY TO FOLDER...](#) [RECOVER PASSWORDS](#)

Recover File Password

madrid.zip

Folder: C:\Users\romeo\Desktop
 File Type: Zip 2.0 — Extraction Password, AES Encryption, Hardware acceleration possible
 Complexity: ••••• Brute-force - Slow
 MD5: 904995CC059062A531C2ABF5AB1E9CE3

Password: File-Open **123**

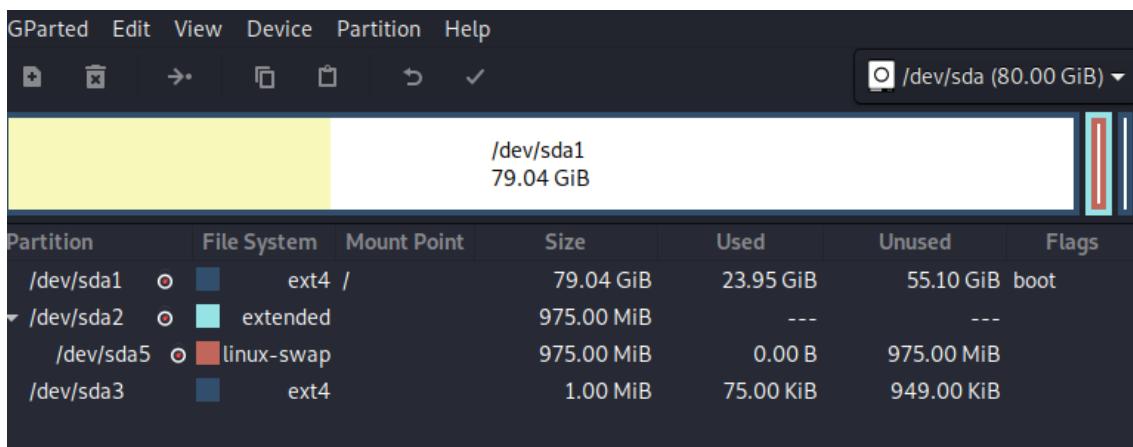
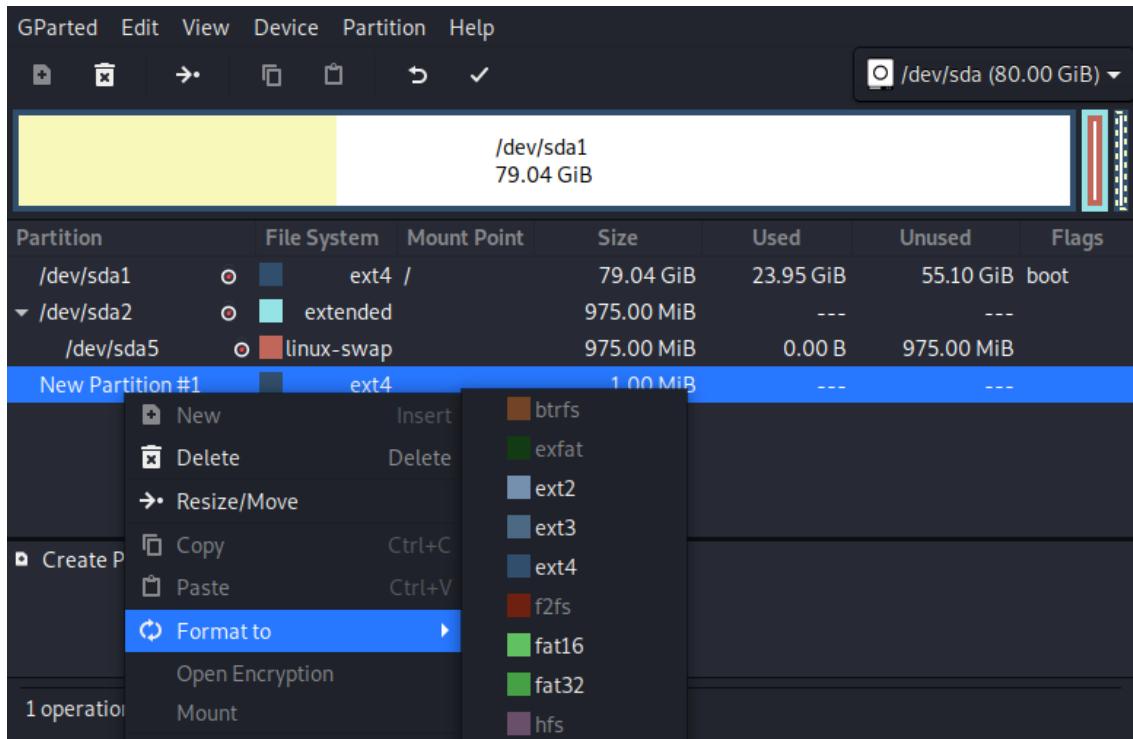
Some of the passwords found cannot be displayed completely due to license limitation. To recover all types of passwords for this file, please consider [upgrading](#) to the higher edition.

PASSWORDS FOUND TIME ELAPSED
1 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
```

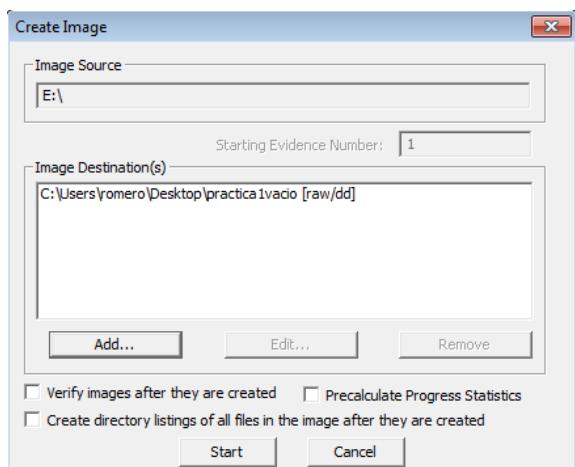
```
kali㉿kali:~$ dd if=/dev/sda3 of=/root/particionRandom.dd
dd: failed to open '/dev/sda3': Permission denied
kali㉿kali:~$ sudo dd if=/dev/sda3 of=/root/particionRandom.dd
2048+0 records in
2048+0 records out
1048576 bytes (1.0 MB, 1.0 MiB) copied, 0.0121644 s, 86.2 MB/s
kali㉿kali:~$
```

The screenshot shows a hex editor window with the following details:

- File:** /root/particionRandom.dd
- Content:** A grid of hex values representing random data. The columns are labeled with addresses from 00000000 to 00000100.
- Hex Values:** The values are mostly random, such as 56 37 B4 81, 2C 87 09 EE, etc.

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 practicavacio.001 -o resultadopdf
Processing: practicavacio.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#
```



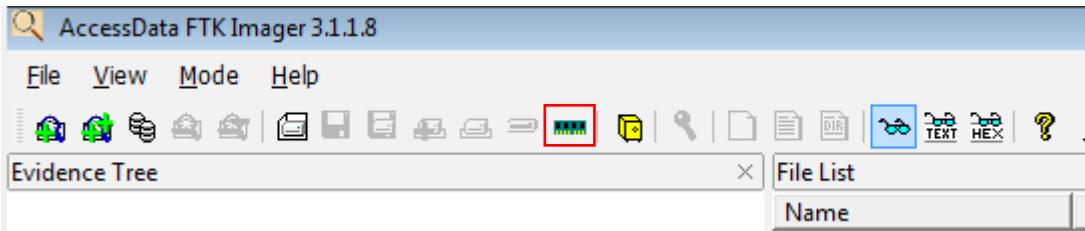
Si queremos que nos encuentre todos los posibles archivos solo debemos obviar el parámetro **-t** y entrando al archivo Audit.txt que nos crea vemos todos los tipos de archivo que nos ha encontrado.

```
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
```

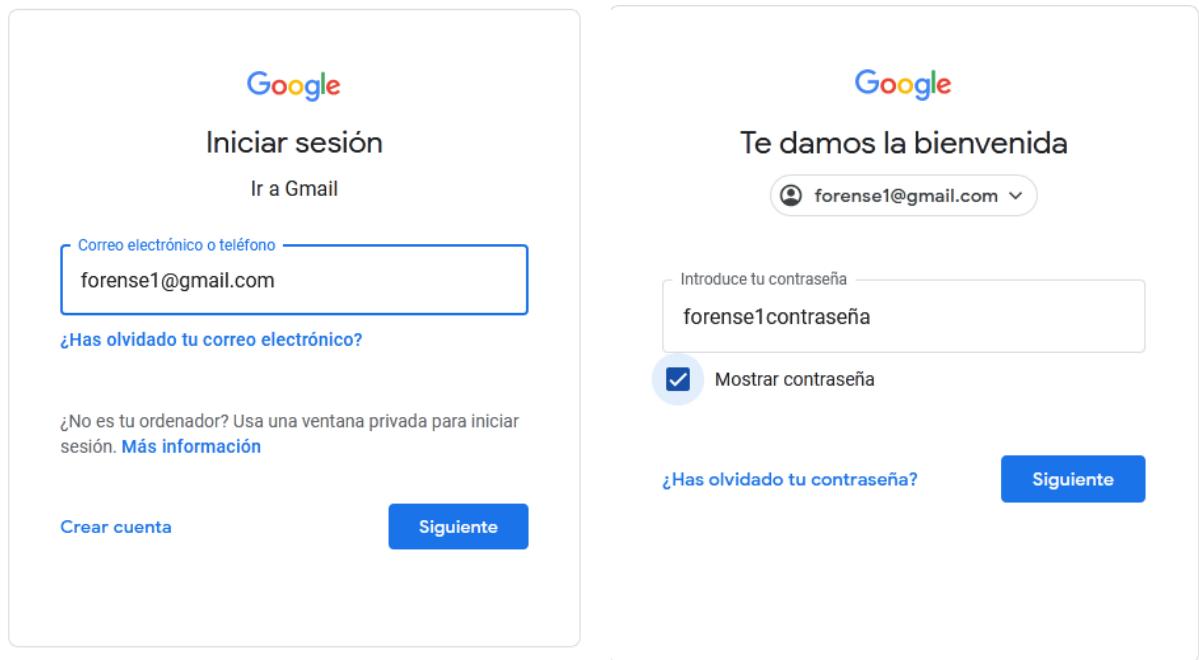
Dumppear memoria RAM y extraer información en Windows

Para dumppear 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



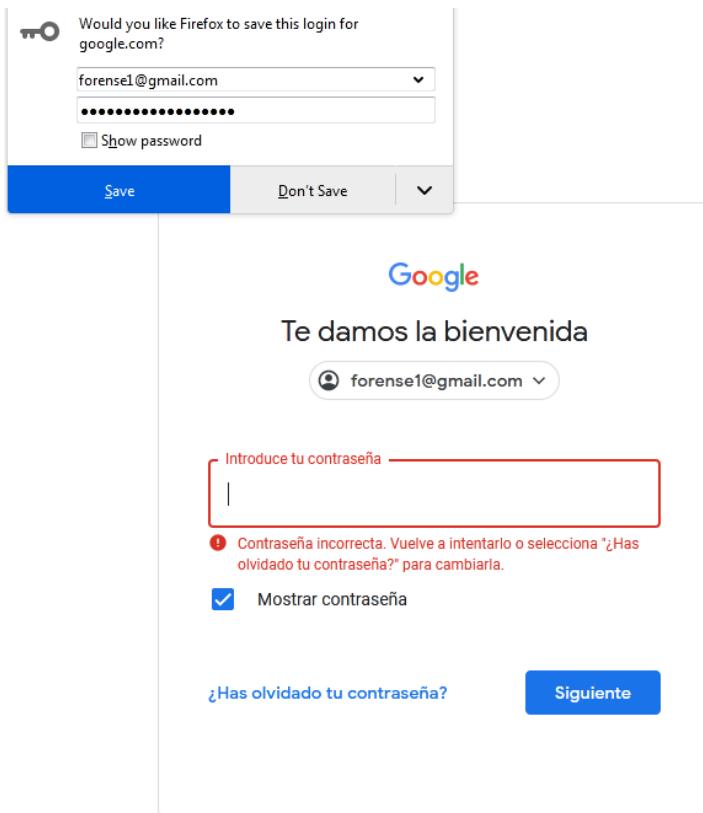
Esto nos extrae la memoria del pc de la cual podremos extraer toda la información que este en ese momento en la RAM, vamos a mostrar un ejemplo de lo que podemos extraer.

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

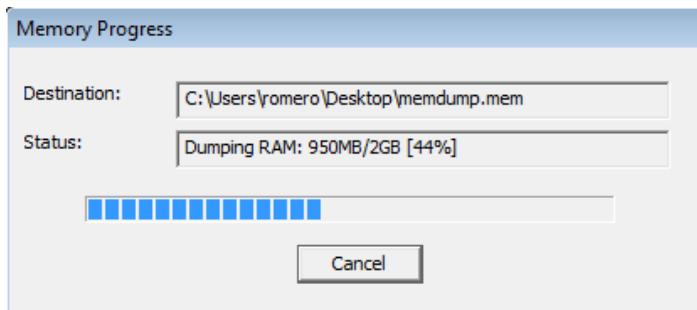


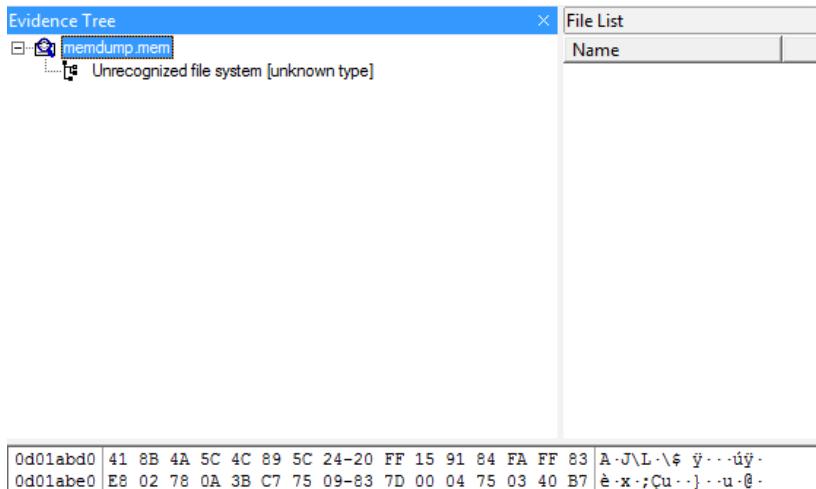
The image consists of two side-by-side screenshots of a web-based sign-in process. The left screenshot shows the 'Iniciar sesión' (Sign in) step, where the user has entered their email address 'forense1@gmail.com' into the 'Correo electrónico o teléfono' (Email or phone number) input field. The right screenshot shows the 'Te damos la bienvenida' (Welcome) step, where the user has entered their password 'forense1contraseña' into the 'Introduce tu contraseña' (Enter your password) input field. Both screenshots include a 'Mostrar contraseña' (Show password) checkbox, which is checked in the right screenshot. The overall interface is clean and modern, typical of a Google account sign-in page.

Estas credenciales no existen pero ya se han quedado en memoria

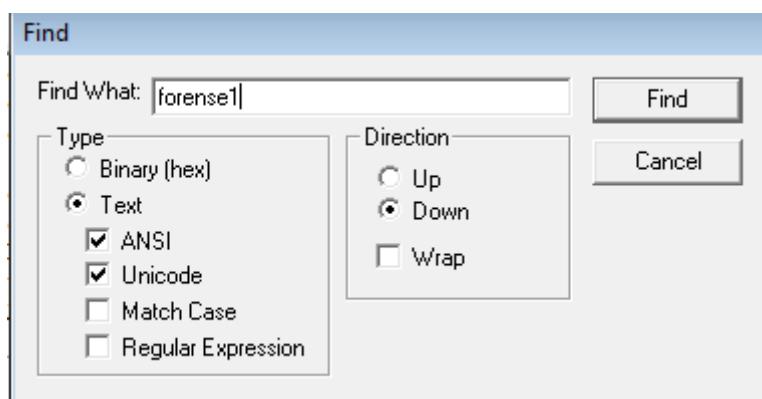


A continuación hacemos el volcado de memoria y pasamos a buscar esta contraseña en la RAM





0d01abd0	41 8B 4A 5C 4C 89 5C 24-20 FF 15 91 84 FA FF 83	A-J\L\\$\ ý..úý.
0d01abe0	E8 02 78 0A 3B C7 75 09-83 7D 00 04 75 03 40 B7	è-x.;Cu..}..u.ø.
0d01abf0	01 40 8A C7 48 8B 5C 24-40 48 8B 6C 24 48 48 8B	@.CH.\\$@H.l\$HH.
0d01ac00	74 24 50 48 8B 7C 24 58-48 83 C4 30 41 5C C3 CC	téPH-!\$XH-ÀO\Àí
0d01ac10	CC CC CC CC CC CC CC-48 8B C4 48 89 58 08 48	iiiiiiih-ÀH-X-H
0d01ac20	89 68 10 48 89 70 18 57-41 54 41 55 48 83 EC 40	.h-H.p-WATAUH-iØ
0d01ac30	83 60 C8 00 0F 29 70 D8-49 8B D8 48 8B F2 48 8B	.È..)pØI-OH-òH-
0d01ac40	F9 E8 9E 55 FF FF 8B E8-85 C0 78 1A 8B 43 30 89	ùè-Uyy-è-Àx-CO-
0d01ac50	87 80 00 00 00 48 B8 9A-99 99 99 99 B9 3F 48H,...,...,...?H
0d01ac60	89 87 88 00 00 00 85 ED-OF 88 DB 00 00 00 8B 43i.Û....C
0d01ac70	38 8B 57 20 48 8D 0D 65-FO 06 00 89 87 98 00 00	8-W H..eØ.....
0d01ac80	00 48 83 7E 10 00 B8 04-00 00 00 48 OF 45 4E 10	.H~...,...H-EN-
0d01ac90	48 F7 E2 48 C7 C2 FF FF-FF FF 4C 8B 01 48 OF 40	H-ÀHCÀÝÝÝL..H-Ø
0d01aca0	C2 8B D0 41 FF 50 08 48-89 87 90 00 00 00 48 85	À-DAyP-H.....H-
0d01acb0	C0 75 0A BD 0E 00 07 80-E9 8C 00 00 00 33 F6 39	Àu-à...-é...-3Ø9
0d01acc0	77 20 OF 86 81 00 00 00-F2 OF 10 35 58 98 FB FF	wò...-5X-ûý
0d01acd0	45 33 E4 45 33 ED 48 8B-87 90 00 00 00 41 89 74	E3àE3iH.....A-t
0d01ace0	05 00 38 77 20 73 0A 48-8B 47 18 49 8B 0C 04 EB	;w s-H-G-I...-é
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...-é-3ÉH-..ýPXH
0d01ad10	8B CF 48 8B D8 48 8B 07-FF 50 60 48 8B D3 48 8B	.-IH-ØH..-ýP`H-ØH-
0d01ad20	C8 66 0F 28 DE 66 0F 28-D6 F2 OF 11 74 24 28 F2	Éf-(bf.(Øo.-tø(ø
0d01ad30	0F 11 74 24 20 E8 0A 78-FF FF FF C6 49 83 C5 04	..-tø è .xpÿýEI-À-
0d01ad40	49 83 C4 08 3B 77 20 72-8D 48 8B 5C 24 60 48 8B	I-À.;w r-H-à`H-
0d01ad50	74 24 70 OF 28 74 24 30-8B C5 48 8B 6C 24 68 48	tøp-(tøo.ÀH.l\$H
0d01ad60	83 C4 40 41 5D 41 5C 5F-C3 CC CC CC CC CC CC	-ÀØA]A\._iiiiiiii
0d01ad70	48 8B C4 48 89 58 08 48-89 68 10 48 89 70 18 48	H-ÀH-X-H-h-H-p-H
0d01ad80	89 78 20 41 54 48 83 EC-20 41 8B 80 80 00 00	.x ATH-i A.....
0d01ad90	49 8B E8 4C 8B E2 89 81-80 00 00 00 49 8B 80 88	I-ÈL.à.....I...
0d01ada0	00 00 00 48 8B F9 48 89-81 88 00 00 00 E8 66 56	..H-ÛH.....èfV
0d01adb0	FF FF 33 DB 3B C3 8B F0-7C 72 8B 8D 98 00 00 00	yy3Û;À-Ø 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 E5aaaaaaaaaa
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-n-a...åä

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
practicalvacuum:~/Desktop/memdump.mem
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	
0xfffffa80038fb30	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	
0xfffffa80039a7a79	cssrss.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	
0xfffffa8003fb830	services.exe	492	388	6	188	0	0	2021-04-05 09:10:19 UTC+0000	
0xfffffa8003a0a800	lsass.exe	500	388	8	621	0	0	2021-04-05 09:10:19 UTC+0000	
0xfffffa8003b4b60	lsm.exe	508	388	11	201	0	0	2021-04-05 09:10:19 UTC+0000	
0xfffffa8003b4b30	svchost.exe	600	492	9	352	0	0	2021-04-05 09:10:20 UTC+0000	
0xfffffa8003b0b30	VboxService.exe	660	492	13	137	0	0	2021-04-05 09:10:20 UTC+0000	
0xfffffa8003b0b30	svchost.exe	728	492	7	254	0	0	2021-04-05 09:10:20 UTC+0000	
0xfffffa8003b0fd30	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	
0xfffffa8003d34030	svchost.exe	332	492	18	464	0	0	2021-04-05 09:10:21 UTC+0000	
0xfffffa8003d5e6b0	svchost.exe	1056	492	24	553	0	0	2021-04-05 09:10:21 UTC+0000	
0xfffffa8003d8060	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	
0xfffffa8001b0c680	sppsvc.exe	1500	492	4	145	0	0	2021-04-05 09:11:41 UTC+0000	
0xfffffa8003dd6d790	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	
0xfffffa8003f7fd30	explorer.exe	1244	1604	28	778	1	0	2021-04-05 09:11:45 UTC+0000	
0xfffffa80040596e0	VBoxIRay.exe	1712	1244	13	144	1	0	2021-04-05 09:11:46 UTC+0000	
0xfffffa800408a570	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	
0xfffffa8003cc0894	audiogd.exe	1784	808	4	122	0	0	2021-04-05 09:19:03 UTC+0000	
0xfffffa8003ecc064	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	
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
0xfffffa8001b6d060	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
0xfffffa8001c7b30	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::8:595:580a: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	UDPv6	127.0.0.1:1900	***	1336	svchost.exe		2021-04-05 09:11:54 UTC+0000
0x7d78bc00	UDPv4	0.0.0.0:13702	***	332	svchost.exe		2021-04-05 09:11:54 UTC+0000
0x7d78d010	UDPv6	::1:3702	***	332	svchost.exe		2021-04-05 09:11:54 UTC+0000
0x7d790460	UDPv4	0.0.0.0:151729	***	332	svchost.exe		2021-04-05 09:11:54 UTC+0000
0x7d790460	UDPv6	::1:51729	***	332	svchost.exe		2021-04-05 09:11:54 UTC+0000
0x7d790ec0	UDPv4	0.0.0.0:151728	***	332	svchost.exe		2021-04-05 09:11:54 UTC+0000
0x7d791d00	UDPv4	0.0.0.0:13702	***	332	svchost.exe		2021-04-05 09:11:54 UTC+0000
0x7d791d00	UDPv6	::1:3702	***	332	svchost.exe		2021-04-05 09:11:54 UTC+0000
0x7d793aa0	UDPv4	0.0.0.0:13702	***	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	::1:52451	***	1336	svchost.exe		2021-04-05 09:10:22 UTC+0000
0x7d854e00	UDPv4	0.0.0.0:123	***	332	svchost.exe		2021-04-05 09:10:42 UTC+0000
0x7d854e00	UDPv6	::1:123	***	332	svchost.exe		2021-04-05 09:10:42 UTC+0000
0x7d85b350	UDPv4	0.0.0.0:15355	***	1056	svchost.exe		2021-04-05 09:10:26 UTC+0000
0x7d85b350	UDPv6	::1:5355	***	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	0.0.0.0:13702	***	1336	svchost.exe		2021-04-05 09:10:41 UTC+0000
0x7d8cd500	UDPv4	0.0.0.0:10	***	1748	svchost.exe		2021-04-05 09:10:23 UTC+0000
0x7d8cd500	UDPv6	::1:10	***	1748	svchost.exe		2021-04-05 09:10:23 UTC+0000
0x7df0f320	UDPv6	fe80::8:595:580a:ffd7:758a:51724	***	1336	svchost.exe		2021-04-05 09:11:54 UTC+0000
0x7df0f490	UDPv6	fe80::8:595:580a:ffd7:758a:1900	***	1336	svchost.exe		2021-04-05 09:11:54 UTC+0000
0x7df0f730	UDPv6	::1:151725	***	1336	svchost.exe		2021-04-05 09:11:54 UTC+0000
0x7df4010	UDPv4	0.0.0.0:13702	***	1336	svchost.exe		2021-04-05 09:10:41 UTC+0000
0x7df4010	UDPv6	::1:3702	***	1336	svchost.exe		2021-04-05 09:10:41 UTC+0000
0x7d9529c0	UDPv4	0.0.0.0:13702	***	1336	svchost.exe		2021-04-05 09:10:41 UTC+0000
0x7d806540	TCPv4	0.0.0.0:15357	0.0.0.0:0	LISTENING	4	System	
0x7d806540	TCPv6	::1:5357	::0	LISTENING	4	System	
0x7d855970	TCPv4	0.0.0.0:9155	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	::1:445	::0	LISTENING	4	System	
0x7d869880	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	492	services.exe	
0x7d869880	TCPv6	::1:49155	::0	LISTENING	492	services.exe	
0x7d8a9230	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	1748	svchost.exe	
0x7d8a9230	TCPv6	::1:49156	::0	LISTENING	1748	svchost.exe	
0x7d8cb230	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	1748	svchost.exe	
0x7dddef0	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	0x0000000002d740010	[no name]
0xfffff8a000024010	0x0000000002d6a5010	\REGISTRY\MACHINE\SYSTEM
0xfffff8a00004e320	0x0000000002d5cf320	\REGISTRY\MACHINE\HARDWARE
0xfffff8a0000a3410	0x0000000007b71a410	\?\C:\System Volume Information\Syscache.hve
0xfffff8a0006e8010	0x0000000003c388010	\Device\HarddiskVolume1\Boot\BCD
0xfffff8a0007f5010	0x0000000003ad2f010	\SystemRoot\System32\Config\SOFTWARE
0xfffff8a000a1a010	0x00000000039e7f010	\SystemRoot\System32\Config\DEFAULT
0xfffff8a000bee010	0x0000000003954a010	\SystemRoot\System32\Config\SECURITY
0xfffff8a000c4b410	0x00000000026fb6410	\SystemRoot\System32\Config\SAM
0xfffff8a000d99010	0x00000000073e83010	\?\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a000e65160	0x0000000003886f160	\?\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a001334010	0x0000000001becb010	\?\C:\Users\romero\ntuser.dat
0xfffff8a0013ef010	0x0000000001c464010	\?\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.

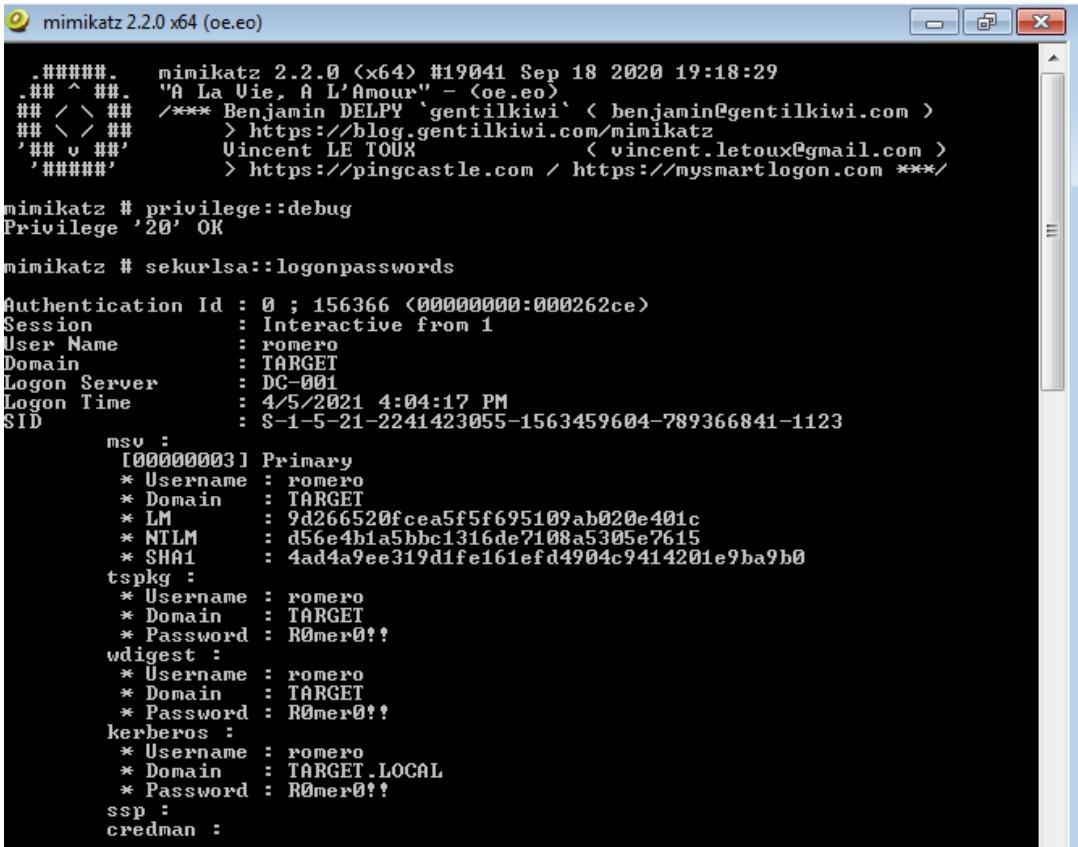
Windows stores two hashes with each password, delimited by colons. The first one is an extremely insecure, obsolete hash using the they are filled with a dummy value starting with "aad".

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:e19ccf75ea54e06b06a5907af13cef42:::
probe:1002:aad3b435b51404eeaad3b435b51404ee:e19ccf75ea54e06b06a5907af13cef42:::
waldo:1004:aad3b435b51404eeaad3b435b51404ee:cfeac129dc5e61b2eb9b2e7131fc7e2b:::
YOUR-NAME:1005:aad3b435b51404eeaad3b435b51404ee:958c8526e4252b277d8d70adbd2ea2ce:::
```

Parte Windows con SysInternals

Identificar contraseñas almacenadas en el equipo



```
mimikatz 2.2.0 x64 (oe.eo)

#####
. mimikatz 2.2.0 <x64> #19041 Sep 18 2020 19:18:29
.## ^ ##. "A La Vie, A L'Amour" - <oe.eo>
## /> ## /*** Benjamin DELPY `gentilkiwi` <benjamin@gentilkiwi.com>
## \ / ## > https://blog.gentilkiwi.com/mimikatz
## v ##' Vincent LE TOUX <vincent.letoux@gmail.com>
## ##### > https://pingcastle.com / https://mysmartlogon.com ***
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 156366 <00000000:000262ce>
Session : Interactive from 1
User Name : romero
Domain : TARGET
Logon Server : DC-001
Logon Time : 4/5/2021 4:04:17 PM
SID : S-1-5-21-2241423055-1563459604-789366841-1123

msv :
[00000003] Primary
* Username : romero
* Domain : TARGET
* LM : 9d266520fceaa5f5f695109ab020e401c
* NTLM : d56e4b1a5bbc1316de7108a5305e7615
* SHA1 : 4ad4a9ee319d1fe161efd4904c9414201e9ba9b0

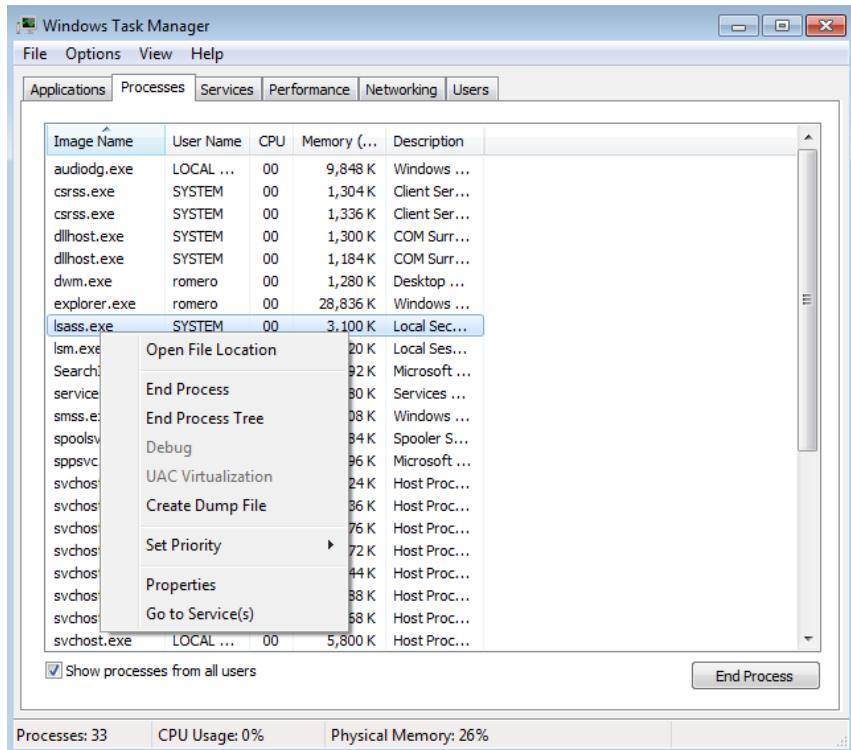
tspkg :
* Username : romero
* Domain : TARGET
* Password : R0mer0!?

wdigest :
* Username : romero
* Domain : TARGET
* Password : R0mer0!?

kerberos :
* Username : romero
* Domain : TARGET.LOCAL
* Password : R0mer0!?

ssp :
credman :
```

Otra forma es con el fichero lsass



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

Name	Date modified	Type	Size
lsass.DMP	3/15/2021 10:23 AM	DMP File	34,234 KB
mimidrv.sys	11/16/2020 1:20 PM	System file	37 KB
mimikatz.exe	11/16/2020 1:20 PM	Application	1,279 KB
mimilib.dll	11/16/2020 1:20 PM	Application extens...	47 KB

```
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       : 9d266520fceaa5f5f695109ab020e401c
* 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

NirLauncher - NirSoft Utilities

Name	Description	Version	Updated On	Web Page URL	EXE Filename
BrowserDownloadsView	Displays the details of downloaded files of Chrome...	1.35	4/5/2021 11:47:38 AM	https://www.nirsoft.net/utils/web_browser_down...	C:\Users\romero\Download...
BrowsingHistoryView	View browsing history of popular Web browsers	2.47	3/18/2021 3:33:04 PM	https://www.nirsoft.net/utils/browsing_history.v...	C:\Users\romero\Download...
WebCacheImageInfo	Shows EXIF information of the images stored in ...	1.32	2/21/2021 11:47:16 PM	https://www.nirsoft.net/utils/web_cache_image_i...	C:\Users\romero\Download...
ImageCacheViewer	Displays images stored in the cache of your Web ...	1.21	2/20/2021 9:55:54 AM	https://www.nirsoft.net/utils/image_cache_viewe...	C:\Users\romero\Download...
ChromeCacheView	Chrome Browser Cache Viewer	2.25	2/2/2021 2:56:40 PM	https://www.nirsoft.net/utils/chrome_cache_vie...	C:\Users\romero\Download...
BrowserAddonsView	Displays the details of all Web browser addons/plu...	1.25	12/2/2020 1:21:54 PM	https://www.nirsoft.net/utils/web_browser_addon...	C:\Users\romero\Download...
ChromeCookiesView	Alternative to the standard internal cookies view...	1.65	12/2/2020 12:45:18 AM	https://www.nirsoft.net/utils/chrome_cookies_v...	C:\Users\romero\Download...
MZCacheView	List all files currently stored in the cache of Firefo...	2.01	10/28/2020 4:45:34 PM	https://www.nirsoft.net/utils/mozilla_cache_view...	C:\Users\romero\Download...
ChromeHistoryView	View the browsing history of Chrome Web browser	1.42	8/27/2020 7:00:12 AM	https://www.nirsoft.net/utils/chrome_history_vie...	C:\Users\romero\Download...
MZCookiesView	alternative to the standard 'Cookie Manager' prov...	1.58	10/27/2019 11:37:00 AM	https://www.nirsoft.net/utils/mzcv.html	C:\Users\romero\Download...
EdgeCookiesView	Display cookies from new versions of MS-Edge	1.17	8/17/2019 1:56:40 PM	https://www.nirsoft.net/utils/edge_cookies_view...	C:\Users\romero\Download...
FirefoxDownloadsView	Displayed the list of downloaded files in Firefox	1.40	3/30/2019 10:12:46 AM	https://www.nirsoft.net/utils/firefox_downloads_...	C:\Users\romero\Download...
FBCacheView	Shows Facebook images stored in the cache of yo...	1.20	9/15/2018 12:11:36 AM	https://www.nirsoft.net/utils/facebook_cache_v...	C:\Users\romero\Download...
WebCookiesSniffer	Captures Web site cookies and displays them in a ...	1.30	9/3/2018 12:37:52 AM	https://www.nirsoft.net/utils/web_cookies_sniffe...	C:\Users\romero\Download...
MZHISTORYVIEW	Displays the list of visited Web sites in Firefox/Moz...	1.65	5/30/2018 12:56:04 AM	https://www.nirsoft.net/utils/mozilla_history_vie...	C:\Users\romero\Download...
MyLastSearch	View your latest searches with Google, Yahoo, an...	1.65	9/24/2017 12:16:46 PM	https://www.nirsoft.net/utils/my_last_search.html	C:\Users\romero\Download...
IECookiesView	Displays the cookies that Internet Explorer stores ...	1.79	2/11/2017 11:03:02 AM	https://www.nirsoft.net/utils/iecookies.html	C:\Users\romero\Download...
IECacheView	List all files currently stored in the cache of Intern...	1.58	6/4/2016 9:34:08 PM	https://www.nirsoft.net/utils/ie_cache_viewer.html	C:\Users\romero\Download...
FlashCookiesView	View Flash cookies stored in your computer.	1.15	6/7/2014 12:34:14 PM	https://www.nirsoft.net/utils/flash_cookies_view...	C:\Users\romero\Download...
FavoritesView	displays the list of all your Favorites/bookmarks i...	1.32	8/10/2013 7:11:58 AM	https://www.nirsoft.net/utils/favview.html	C:\Users\romero\Download...
OperaCacheView	Cache viewer for Opera Web browser.	1.40	5/22/2012 1:25:34 PM	https://www.nirsoft.net/utils/opera_cache_viewe...	C:\Users\romero\Download...
SafariCacheView	Cache viewer/extractor for Safari Web browser	1.11	4/29/2012 12:56:32 PM	https://www.nirsoft.net/utils/safari_cache_viewe...	C:\Users\romero\Download...
IEHistoryView	Displays the list of Web sites that you visited with ...	1.70	12/13/2011 5:04:48 PM	https://www.nirsoft.net/utils/iehistory.html	C:\Users\romero\Download...
SafariHistoryView	History viewer for Safari Web browser	1.01	12/4/2011 3:02:54 PM	https://www.nirsoft.net/utils/safari_history_view...	C:\Users\romero\Download...
URLStringGrabber	Grab URLs strings of Web sites from Internet Explor...	1.11	6/5/2011 11:05:50 AM	https://www.nirsoft.net/utils/url_string_grabber...	C:\Users\romero\Download...

Run Advanced Run Web Page Help File Web Search Package Package

25 Utilities, 1 Selected

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

Select History Filename

Load only the URLs visited in the last days

Load only the URLs visited in the specified date/time range: (In GMT)

From: To:

Load only the URLs contain the following strings (comma-delimited list):

Don't load the URLs contain the following strings (comma-delimited list):

Load only URLs with the following visit count range:
From: To:

Load only URLs with the following titles (comma-delimited list):

Merge multiple items with identical URLs into one item

Use the following Firefox installation folder to load the SQLite library:

MZHistoryView - C:\Users\ramon\AppData\Roaming\Mozilla\Firefox\Profiles\3ejtd96a.default-release\places.sqlite

File Edit View Options Help

Quick Filter Find one string Search all columns Show only items match the f

URL	First Visit Date	Last Visit Date	Visit Count	Referrer	Host Name	Title	Record Ind...
① http://webhelp.esri.com/arcims/9.3/General/merg...	N / A	20/12/2020 13:53:25	1			GetCapabilities	11569
② http://www.andy-pearse.com/blog/posts/2013/M...	N / A	20/12/2020 14:02:44	1			File Capabilities In Linux	11586
③ http://www.cepii.org/wp-content/uploads/201...	N / A	04/12/2020 13:13:10	1	https://www.google.co...		DOCUMENTO-PIR.pdf	9772
④ http://www.crummy.com/software/BeautifulSoup...	N / A	29/12/2020 19:43:26	1	https://pypi.org/project/...			11992
⑤ http://www.deezer.com/	N / A	08/12/2020 19:22:33	50			BOOM - X Ambassadors - Dee...	10179
⑥ http://www.deezer.com/	N / A	08/12/2020 19:22:38	50			BOOM - X Ambassadors - Dee...	10181
⑦ http://www.deezer.com/	N / A	08/12/2020 19:22:38	50			BOOM - X Ambassadors - Dee...	10184
⑧ http://www.deezer.com/	N / A	08/12/2020 19:27:33	50			BOOM - X Ambassadors - Dee...	10353
⑨ http://www.deezer.com/	N / A	10/12/2020 18:26:11	50			BOOM - X Ambassadors - Dee...	10354
⑩ http://www.deezer.com/	N / A	17/12/2020 0:49:23	50			BOOM - X Ambassadors - Dee...	11062
⑪ http://www.deezer.com/	N / A	17/12/2020 0:53:49	50			BOOM - X Ambassadors - Dee...	11067
⑫ http://www.deezer.com/	N / A	20/12/2020 13:15:04	50			BOOM - X Ambassadors - Dee...	11554
⑬ http://www.deezer.com/es/	N / A	08/12/2020 19:22:33	50	http://www.deezer.com/		BOOM - X Ambassadors - Dee...	10180
⑭ http://www.deezer.com/es/	N / A	08/12/2020 19:22:38	50	http://www.deezer.com/		BOOM - X Ambassadors - Dee...	10182
⑮ http://www.deezer.com/es/	N / A	08/12/2020 19:27:33	50	http://www.deezer.com/		BOOM - X Ambassadors - Dee...	10185
⑯ http://www.deezer.com/es/	N / A	10/12/2020 18:26:11	50	http://www.deezer.com/		BOOM - X Ambassadors - Dee...	10354
⑰ http://www.deezer.com/es/	N / A	17/12/2020 0:49:23	50	http://www.deezer.com/		BOOM - X Ambassadors - Dee...	11063
⑱ http://www.deezer.com/es/	N / A	17/12/2020 0:53:50	50	http://www.deezer.com/		BOOM - X Ambassadors - Dee...	11068
⑲ http://www.deezer.com/es/	N / A	20/12/2020 13:15:04	50	http://www.deezer.com/		BOOM - X Ambassadors - Dee...	11555
⑳ http://www.deezer.com/par...	N / A	08/12/2020 20:51:50	1	https://www.huffington...		Cristina Pardo da la razón al re...	10213
㉑ http://www.facebook.com/events/4575736110193...	N / A	10/12/2020 20:29:04	1	https://anelenapena.blo...			10383
㉒ http://www.foundstone.com/us/resources/prodd...	N / A	15/12/2020 19:22:10	1	https://securitythoughts...			10859
㉓ http://www.interior.gob.es/documents/642012/12...	N / A	04/12/2020 13:02:41	1	http://www.interior.gob...		Guía de trámites 2020 - guía_t...	9751
㉔ http://www.interior.gob.es/web/servicios-al-ci...	N / A	04/12/2020 13:02:25	1	http://www.interior.gob...		Guía de trámites - Ministerio ...	9750
㉕ http://www.interior.gob.es/es/web/servicios-al-ci...	N / A	04/12/2020 13:09:02	1	http://www.interior.gob...		Procesos selectivos - Ministeri...	9767
㉖ http://www.interior.gob.es/es/web/servicios-al-ci...	N / A	04/12/2020 13:09:25	1	http://www.interior.gob...		Oferta de empleo público 202...	9768
㉗ http://www.interior.gob.es/web/servicios-al-ci...	N / A	04/12/2020 13:08:59	1	http://www.interior.gob...		Servicios al ciudadano - Minis...	9766
㉘ http://www.interior.gob.es/web/servicios-al-ciuda...	N / A	04/12/2020 13:02:17	1	http://www.interior.gob...		Oposiciones - Ministerio del I...	9749
㉙ http://www.interior.mnn.es/webs/cericircn-al-riurta...	N / A	04/12/2020 12:57:36	1			Sinlitudes - Ministerio del Int...	9735

2579 item(s), 1 Selected

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

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

Filtrar registro actual X

Filtro XML

Registrado:	En cualquier momento
Nivel del evento:	<input type="checkbox"/> Crítico <input type="checkbox"/> Advertencia <input checked="" type="checkbox"/> Detallado <input type="checkbox"/> Error <input type="checkbox"/> Información
Por registro	Registros de eventos: <select>Seguridad</select>
Por origen	Orígenes del evento: <select></select>
Para incluir o excluir los id. de evento, escriba números o intervalos de id. separados por comas. Para excluir criterios, antecédalos con un signo de menos. Ej: 1,3,5-99,-76	
<input type="text" value="4624"/>	
Categoría de la tarea:	<select></select>
Palabras clave:	<select></select>
Usuario:	<Todos los usuarios>
Equipo(s):	<Todos los equipos>
<input type="button" value="Borrar"/>	
<input type="button" value="Aceptar"/> <input type="button" value="Cancelar"/>	

Visor de eventos (local)

Vistas personalizadas

Registros de Windows

- Aplicación
- Seguridad
- Instalación
- Sistema
- Eventos reenviados
- Registros de aplicaciones y servicios
- Suscripciones

Seguridad Número de eventos: 32.837

Filtrados: Registro: Security; Origen: ; Id. del evento: 4624. Número de eventos: 2.461

Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Auditoría correcta	05/04/2021 17:27:28	Microsoft Windows security au...	4624	Logon
Auditoría correcta	05/04/2021 17:25:38	Microsoft Windows security au...	4624	Logon
Auditoría correcta	05/04/2021 17:25:38	Microsoft Windows security au...	4624	Logon
Auditoría correcta	05/04/2021 17:24:44	Microsoft Windows security au...	4624	Logon
Auditoría correcta	05/04/2021 17:23:21	Microsoft Windows security au...	4624	Logon
Auditoría correcta	05/04/2021 17:19:21	Microsoft Windows security au...	4624	Logon
Auditoría correcta	05/04/2021 17:19:20	Microsoft Windows security au...	4624	Logon
Auditoría correcta	05/04/2021 17:14:03	Microsoft Windows security au...	4624	Logon
Auditoría correcta	05/04/2021 17:13:36	Microsoft Windows security au...	4624	Logon
Auditoría correcta	05/04/2021 17:13:36	Microsoft Windows security au...	4624	Logon
Auditoría correcta	05/04/2021 17:13:34	Microsoft Windows security au...	4624	Logon
Auditoría correcta	05/04/2021 17:13:34	Microsoft Windows security au...	4624	Logon

Anализar herramientas que se ejecuten en el arranque

WhatinStartup

File Edit View Options Help

Name	Type	Command Line	Disabled	Product Name	File Version	Pr
Registry -> Machine Run (WOW64)			No			
AdobeGCInvo...	Registry -> Machine Run	"C:\Program Files (x86)\Common Files\Ad...	No	GC Invoker Utility	7.3.0.157	Ac
Application Re...	Registry -> User Run Once	C:\Program Files\Razer\RzAppEngine\rzap...	No			
com.squirrel.T...	Registry -> User Run	C:\Users\ramon\AppData\Local\Microsoft\...	No	Microsoft Teams	1.4.4.0	M
Discord	Registry -> User Run	C:\Users\ramon\AppData\Local\Discord\U...	No	Update	1.1.1.0	Up
Genshin Impa...	Registry -> Machine Run (WOW64)		No			
iCloudServices	Registry -> User Run	"C:\Program Files (x86)\Common Files\Ap...	No	iCloud for Windows	73.4.0.22	iC
Lync	Registry -> User Run	"C:\Program Files (x86)\Microsoft Office\ro...	No	Microsoft Office	16.0.13801.20294	Sk
OneDrive	Registry -> User Run	"C:\Users\ramon\AppData\Local\Microsoft\...	No	Microsoft OneDrive	19.070.0410.0005	M
Razer Synapse	Registry -> Machine Run (WOW64)	"C:\Program Files (x86)\Razer\Synapse\RzS...	No	Razer Synapse	2.21.24.34	Ra
Riot Vanguard	Registry -> Machine Run	"C:\Program Files\Riot Vanguard\vgtray.exe"	No	Vanguard Tray	1.50.13	Va
RTHDVCP...	Registry -> Machine Run	"C:\Program Files\Realtek\Audio\HDA\Rtk...	No	Realtek HD USB A...	1.0.641.0	Re
RZSurroundH...	Registry -> Machine Run	C:\WINDOWS\system32\RZsurroundHelp...	No			
SteelSeries En...	Startup Folder -> Common	"C:\Program Files\SteelSeries\SteelSeries En...	No	SteelSeries Engine 3	3.19.2.0	St
SunJavaUpdat...	Registry -> Machine Run (WOW64)	"C:\Program Files (x86)\Common Files\Jav...	No	Java Platform SE A...	2.8.281.9	Ja
SUPER CHARG...	Registry -> Machine Run (WOW64)	C:\Program Files (x86)\MSI\SUPER CHARG...	No	SUPER CHARGER	1.2.024	SL
vmware-tray.e...	Registry -> Machine Run (WOW64)	"C:\Program Files (x86)\VMware\VMware ...	No	VMware Workstati...	15.5.2 build-15785...	VM

Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

Network Providers					
Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				07/12/2019 11:15	
cmd.exe	Procesador de comandos de... (Verified) Microsoft Windows	c:\windows\system32\cmd.exe		11/12/1953 4:58	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				26/03/2021 14:52	
AdobeGCInvoker	Adobe GC Invoker Utility (Verified) Adobe Inc.	c:\program files (x86)\commo...		17/02/2021 5:27	
Riot Vanguard	Riot Vanguard tray notification (Verified) Riot Games, Inc.	c:\program files\riot vanguard...		24/03/2021 5:13	
RTHDVCP...	Realtek HD Audio Manager (Verified) Realtek Semiconductor...	c:\program files\realtek\audio\...		26/05/2017 5:16	
RZSurroundHelper			File not found: C:\WINDOWS\...		
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				26/03/2021 14:20	
Razer Synapse	Razer Synapse (Verified) Razer USA Ltd.	c:\program files (x86)\razer\sy...		13/05/2020 14:32	
SunJavaUpdate...	Java Update Scheduler (Verified) Oracle America, Inc.	c:\program files (x86)\commo...		09/12/2020 16:24	
SUPER CHARG...	SUPER CHARGER (Verified) MICRO-STAR INTE...	c:\program files (x86)\msi\sup...		21/02/2014 4:42	
vmware-tray.exe	VMware Tray Process (Verified) VMware, Inc.	c:\program files (x86)\vmware\...		07/03/2020 22:23	
HKCU\Software\Microsoft\Windows\CurrentVersion\Run				26/03/2021 14:19	
com.squirrel.Tea...	Microsoft Teams (Verified) Microsoft 3rd Party...	c:\users\ramon\appdata\local\...		28/06/2019 23:28	
Discord	Update (Verified) Discord Inc.	c:\users\ramon\appdata\local\...		01/06/2020 22:58	
iCloudServices	iCloud Services (Verified) Apple Inc.	c:\program files (x86)\commo...		23/06/2018 12:02	
Lync	Skype for Business (Verified) Microsoft Corporation	c:\program files (x86)\micros...		06/03/2021 6:11	
OneDrive	Microsoft OneDrive (Verified) Microsoft Corporation	c:\users\ramon\appdata\local\...		01/05/2019 7:14	
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce				13/03/2021 13:41	
Application Rest...			File not found: C:\Program Fil...		
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup				30/09/2020 23:51	
SteelSeries Eng...	SteelSeries Engine 3 Core (Verified) SteelSeries ApS	c:\program files\steelseries\st...		03/03/2021 22:22	
HKLM\Software\Microsoft\Active Setup\Installed Components				26/03/2021 14:08	
Google Chrome	Google Chrome Installer (Verified) Google LLC	c:\program files (x86)\google\...		29/03/2021 19:02	
Microsoft Edge	Microsoft Edge Installer (Verified) Microsoft Corporation	c:\program files (x86)\micros...		01/04/2021 3:44	
n/a	Microsoft .NET IE SECURITY... (Verified) Microsoft Corporation	c:\windows\system32\mscori...		25/10/2019 5:45	
HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed Components				03/10/2020 20:11	
n/a	Microsoft.NET SECURITY... (Verified) Microsoft Corporation	c:\windows\syswow64\mscori...		25/10/2019 10:48	
HKLM\Software\Classes\Protocols\Filter				13/03/2021 2:15	
text/xml	Microsoft Office XML MIME Filt... (Verified) Microsoft Corporation	c:\program files (x86)\micros...		01/02/2021 0:19	
HKLM\Software\Classes\^ShellEx\ContextMenuHandlers				16/03/2021 23:59	
7-Zip	7-Zip Shell Extension (Not verified) Igor Pavlov	c:\program files\7-zip\7zip.dll		21/02/2019 18:00	
AccExt	Core Sync (Verified) Adobe Systems Inc.	c:\program files (x86)\commo...		05/03/2018 17:02	
ANotePad++64	ShellHandler for Notepad++... (Verified) NotePad++	c:\program files\notepad++\n...		12/05/2014 11:49	
MEGA Context m...			File not found: C:\Users\ramo...		

Administrador de tareas

Archivo Opciones Vista

Procesos Rendimiento Historial de aplicaciones Inicio Usuarios Detalles Servicios

Último tiempo de BIOS: 11.6 segundos

Nombre	Anunciante	Estado	Impacto de ini...
Your Phone	Microsoft Corporation	Deshabilitado	Ninguno
VMware Tray Process	VMware, Inc.	Habilitado	Medio
Vanguard tray notification.	Riot Games, Inc.	Deshabilitado	Ninguno
Update	GitHub	Deshabilitado	Ninguno
SUPER CHARGER	MSI	Habilitado	Alto
SteelSeries Engine 3 Core	SteelSeries ApS	Habilitado	Alto
Skype for Business	Microsoft Corporation	Deshabilitado	Ninguno
Skype	Skype	Deshabilitado	Ninguno
RZSurroundHelper		Habilitado	No medido
Realtek HD Audio Manager	Realtek Semiconductor	Habilitado	Medio
Razer Synapse	Razer Inc.	Habilitado	Alto
Microsoft Teams	Microsoft Corporation	Deshabilitado	Ninguno
Microsoft OneDrive	Microsoft Corporation	Deshabilitado	Ninguno
Killer Control Center	Rivet Networks LLC	Habilitado	No medido

Analizar tareas programadas en el equipo

Programador de tareas

Archivo Acción Ver Ayuda

Programador de tareas (local)

Biblioteca del Programador

- Apple
- Elcomsoft
- Intel
- MEGA
- Microsoft
- Mozilla

Nombre	Estado	Desencadenadores	Hora próxima ejecución	Hora última ejecución	Resultado de últi...
AdobeGCInv...	Listo	A las 12:31 todos los días	06/04/2021 12:31:00	05/04/2021 12:31:01	La operación se cc...
CreateExplor...	Deshabilitado	Al crear o modificar la tarea		08/01/2019 17:29:30	(0x40010004)
GoogleUpda...	Listo	Se definieron varios desencadenadores	06/04/2021 10:58:17	05/04/2021 14:46:13	La operación se cc...
GoogleUpda...	Listo	A las 10:58 todos los días - Tras desencadenarse, repetir cada 1 hora durante 1 día.	05/04/2021 17:58:17	05/04/2021 17:55:51	La operación se cc...
Intel PIT EK...	Listo	Filtro de eventos personalizado		30/11/1999 00:00:00	La tarea no se ha e...
MicrosoftEd...	Listo	Se definieron varios desencadenadores	06/04/2021 13:32:56	05/04/2021 14:49:11	La operación se cc...
MicrosoftEd...	Listo	A las 13:02 todos los días - Tras desencadenarse, repetir cada 1 hora durante 1 día.	05/04/2021 18:02:56	05/04/2021 17:25:51	La operación se cc...
MSL_Dragon_...	Deshabilitado	Al iniciar la sesión un usuario		25/05/2019 22:10:27	La operación se cc...
MSL_Help_De...	Deshabilitado	Se definieron varios desencadenadores	06/04/2021 10:00:18	25/05/2019 22:10:42	La operación se cc...
Nahimic2sv...	Listo			30/11/1999 00:00:00	La tarea no se ha e...
Nahimic2sv...	Listo			30/11/1999 00:00:00	La tarea no se ha e...
Nahimic2UL...	Listo			26/03/2021 13:21:51	La operación se cc...
NahimicMSI_...	Deshabilitado			30/11/1999 00:00:00	La tarea no se ha e...
NahimicMSI_...	Deshabilitado			30/11/1999 00:00:00	La tarea no se ha e...
NahimicMSL...	Deshabilitado			25/05/2019 22:10:27	La operación se cc...

The screenshot shows the Windows Task Scheduler interface. On the left, there's a tree view under 'Programador de tareas (local)' with nodes like 'Biblioteca del Programador', 'Apple', 'Elcomsoft', 'Intel', 'MEGA', 'Microsoft', and 'Mozilla'. A task named 'Firefox Default Browser Agent' is selected. The main pane displays the task details:

Nombre	Estado	Desencadenadores	Hora próxima ejecución	Hora última ejecución	Resultado de última ejecución	Autor	Creado
Firefox Default Browser Agent	Listo	A las 21:04 todos los días	05/04/2021 22:04:36	04/04/2021 23:24:51	La operación se completó correctamente. (0x0)	Mozilla	

Below the table, tabs for 'General', 'Desencadenadores', 'Acciones', 'Condiciones', 'Configuración', and 'Historial (deshabilitado)' are visible. The 'General' tab shows the task name as 'Firefox Default Browser Agent 308046B0AF4A39CB', located at '\Mozilla' by 'Mozilla', and a detailed description about Firefox changing to another browser.

Sysinternals Autoruns Scheduled Tasks

The screenshot shows the Sysinternals Autoruns tool interface. The top menu includes File, Entry, Options, Help, and a toolbar with icons for Network Providers, WMI, Everything, Logon, Explorer, Internet Explorer, Scheduled Tasks, Services, Drivers, Codecs, Boot Execute, and Image Hijack. The main window lists scheduled tasks with columns for Autorun Entry, Description, Publisher, Image Path, Timestamp, and VirusTotal. A yellow highlight covers several entries, including 'Mozilla\Firefox D...', 'MSL_Dragon Ga...', 'MSL_Help_Desk...', and multiple entries for 'Nahimic' services.

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
Task Scheduler					
<input checked="" type="checkbox"/> \AdobeGCInvoke...	Adobe GC Invoker Utility	(Verified) Adobe Inc.	c:\program files (x86)\commo...	17/02/2021 5:27	
<input checked="" type="checkbox"/> \AppleAppleSoft...	Apple Software Update	(Verified) Apple Inc.	c:\program files (x86)\apple s...	04/09/2019 23:02	
<input checked="" type="checkbox"/> \Intel\Thunderbolt...	Thunderbolt(TM) Software	(Verified) Intel(R) Client Conne...	c:\program files (x86)\intel\thu...	01/11/2015 11:53	
<input checked="" type="checkbox"/> \Intel\Thunderbolt...	Thunderbolt(TM) Software	(Verified) Intel(R) Client Conne...	c:\program files (x86)\intel\thu...	01/11/2015 11:53	
<input checked="" type="checkbox"/> \Microsoft\Office\...	Microsoft Office Click-to-Run ...	(Verified) Microsoft Corporation	c:\program files\common files...	05/03/2021 2:59	
<input checked="" type="checkbox"/> \Microsoft\Office\...	Microsoft Office Click-to-Run ...	(Verified) Microsoft Corporation	c:\program files\common files...	05/03/2021 2:59	
<input checked="" type="checkbox"/> \Microsoft\Office\...	Microsoft Office SDX Helper	(Verified) Microsoft Corporation	c:\program files (x86)\microso...	06/03/2021 3:00	
<input checked="" type="checkbox"/> \Microsoft\Office\...	Microsoft Office SDX Helper	(Verified) Microsoft Corporation	c:\program files (x86)\microso...	06/03/2021 3:00	
<input checked="" type="checkbox"/> \Microsoft\Office\...	Office Subscription Licensing ...	(Verified) Microsoft Corporation	c:\program files (x86)\microso...	06/03/2021 2:59	
<input checked="" type="checkbox"/> \Microsoft\Office\...	Office Telemetry Dashboard ...	(Verified) Microsoft Corporation	c:\program files (x86)\microso...	25/02/2021 23:37	
<input checked="" type="checkbox"/> \Microsoft\Office\...	Office Telemetry Dashboard ...	(Verified) Microsoft Corporation	c:\program files (x86)\microso...	25/02/2021 23:37	
<input checked="" type="checkbox"/> \Microsoft\Visual...			File not found: C:\Program Fil...		
<input checked="" type="checkbox"/> \Microsoft\Visual...			File not found: C:\Program Fil...		
<input checked="" type="checkbox"/> Mozilla\Firefox D...	Firefox Default Browser Agent	(Verified) Mozilla Corporation	c:\program files\mozilla firefo...	18/03/2021 13:42	
<input type="checkbox"/> \MSL_Dragon Ga...	mDispatch	(Not verified) TODO: <公司名>	c:\program files (x86)\msl\dra...	23/01/2014 7:36	
<input type="checkbox"/> \MSL_Help_Desk...	MSI Update Agent	(Not verified) Micro-Star Intern...	c:\program files (x86)\msi\hel...	05/02/2018 9:00	
<input checked="" type="checkbox"/> \Nahimic2svc32...			File not found: C:\Program Fil...		
<input checked="" type="checkbox"/> \Nahimic2svc64R...			File not found: C:\Program Fil...		
<input checked="" type="checkbox"/> \Nahimic2UILaun...			File not found: C:\Program Fil...		
<input type="checkbox"/> \NahimicMSIsvc3...			File not found: C:\Program Fil...		
<input type="checkbox"/> \NahimicMSIsvc6...			File not found: C:\Program Fil...		
<input checked="" type="checkbox"/> \NahimicMSIUILa...			File not found: C:\Program Fil...		
<input type="checkbox"/> \OneDrive Stand...	Standalone Updater	(Verified) Microsoft Corporation	c:\users\ramon\appdata\local...	01/05/2019 7:13	

Analizar shellbags en el equipo.

Para esto tenemos que ejecutar como administrador

	shellbagsview.chm	22/06/2020 21:49	Archivo de Ayuda ...	15 KB
	shellbagsview.exe	22/06/2020 21:49	Aplicación	47 KB
	shellmenunew.chm	03/07/2013 20:41	Archivo de Ayuda ...	15 KB

ShellBagsView										
Path	Slot Number	Last Modified...	Mode	Icon Size	Windows Posit...	Windows Size	Type	Slot Key	Slot Modified Time	User Name
D:\Universidad 2021\Segundo Q\Análisis forense...	1221	05/04/2021 17:04:27		Small	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	05/04/2021 17:04:27	
D:\Universidad 2021\Segundo Q\Análisis forense...	1220	05/04/2021 17:04:27		Small	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	05/04/2021 17:04:27	
D:\Universidad 2021\Segundo Q\Análisis forense...	1133	05/04/2021 16:32:21		Small	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	16/02/2021 14:52:35	
D:\Universidad 2021\Segundo Q\Análisis forense...	1219	05/04/2021 16:12:22		Small	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	05/04/2021 16:31:59	
D:\Universidad 2021\Segundo Q	1121	05/04/2021 16:12:13		Small	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	09/02/2021 13:08:37	
forense reto2	1218	05/04/2021 11:16:21		Small	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	05/04/2021 11:16:31	
C:\Users\ramon\Documents\Universidad 2021\Se...	1217	02/04/2021 14:06:57		Small	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	02/04/2021 14:06:57	
C:\Users\ramon\Documents\Universidad 2021\Se...	1128	02/04/2021 14:06:57		Small	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	09/02/2021 20:41:39	
D:\	3	02/04/2021 13:42:18	Details	Medium	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	30/09/2020 23:56:04	
C:\Users\ramon\Documents\Universidad 2021\Se...	1216	28/03/2021 5:08:09		Small	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	28/03/2021 5:08:09	
C:\Users\ramon\Documents\Universidad 2021	1127	28/03/2021 5:08:09		Small	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	09/02/2021 20:41:38	
C:\Users\ramon\Documents	629	26/03/2021 23:30:26		Small	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	30/09/2020 23:56:05	
D:\Universidad 2021	938	26/03/2021 23:28:57		Small	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	30/09/2020 23:56:06	
C:\Users\ramon	29	26/03/2021 17:47:50	Details	Medium	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	30/09/2020 23:56:04	
D:\Universidad 2021\Primer Q	950	26/03/2021 13:15:57		Small	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	30/09/2020 23:56:06	
C:\Users\ramon\AppData\Local\VALORANT\Save...	1213	26/03/2021 12:50:06	Details	Medium	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	26/03/2021 12:50:04	
C:\Users\ramon\AppData\Local\VALORANT\Save...	1215	26/03/2021 12:50:06	Details	Medium	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	26/03/2021 12:50:07	
C:\Users\ramon\AppData\Local\VALORANT\Save...	1214	26/03/2021 12:50:04	Details	Medium	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	26/03/2021 12:50:05	
C:\Users\ramon\AppData\Local\VALORANT\Save...	1209	26/03/2021 12:50:02	Details	Medium	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	26/03/2021 12:49:48	
C:\Users\ramon\AppData\Local\VALORANT\Save...	1212	26/03/2021 12:49:58	Details	Medium	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	26/03/2021 12:50:01	
C:\Users\ramon\AppData\Local\VALORANT\Save...	1211	26/03/2021 12:49:56	Details	Medium	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	26/03/2021 12:49:57	
C:\Users\ramon\AppData\Local\VALORANT	1210	26/03/2021 12:49:48	Details	Medium	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	26/03/2021 12:49:50	
C:\Users\ramon\AppData\Local\VALORANT\Save...	1207	26/03/2021 12:49:28	Details	Medium	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	26/03/2021 12:49:47	
C:\Users\ramon\AppData\Local\VALORANT\Save...	1208	26/03/2021 12:49:28	Details	Medium	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	26/03/2021 12:49:31	
C:\Users\ramon\AppData\Local	360	26/03/2021 12:49:24	Details	Medium	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	30/09/2020 23:56:04	
E:\Audio driver_6.0.1.8172 and Nahmic_2.3.2.1	476	26/03/2021 4:47:03	Details	Medium	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	26/03/2021 4:47:01	
E:\Audio driver_6.0.1.8172 and Nahmic_2.3.2.1\Na...	1206	26/03/2021 4:47:03	Details	Medium	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	26/03/2021 4:48:24	
E:\Audio driver_6.0.1.8172 and Nahmic_2.3.2.1\Au...	1205	26/03/2021 4:47:01	Details	Medium	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	26/03/2021 4:47:02	
E:\	11	26/03/2021 4:46:42	Icons	Large	Top Left	192x144	ShellNoRoam (...)	Software\Classes\Local Settin...	30/09/2020 23:56:03	

Analizar ficheros prefetch en el equipo.

NirLauncher - NirSoft Utilities					
File	Edit	View	Options	Launcher	Packages Help
Password Recovery Utilities					
Command-Line Utilities				Network Monitoring Tools	
System Utilities					
Name	Description	Version	Updated On	Web Page URL	
ExecutedProgramsList	Displays programs and batch files that you previou...	1.11	18/03/2016 12:11:04	https://www.nirsoft.net/utils/exec	
SpecialFoldersView	Easily jump to special folders in your system.	1.26	16/01/2016 17:37:24	https://www.nirsoft.net/utils/spec	
SkypeContactsView	Displays the list of Skype contacts stored in the lo...	1.05	13/12/2015 19:31:16	https://www.nirsoft.net/utils/skyp	
RegDllView	RegDllView is a small utility that displays the list o...	1.60	09/12/2015 9:55:20	https://www.nirsoft.net/utils/regis	
MMCSnapInsView	Displays the details of all MMC snap-ins installed ...	1.00	25/11/2015 9:06:32	https://www.nirsoft.net/utils/mmc	
UserProfilesView	View user profiles information on your system.	1.10	15/10/2015 17:35:26	https://www.nirsoft.net/utils/user	

ExecutedProgramsList						
File	Edit	View	Options	Help		
Executed File		File Last Modified	File Created On	File Size	File Attributes	Product Name
C:\Program Files (x86)\Battle.net\Battle.net Launc...						
C:\Program Files (x86)\ClipClip\ClipClip.exe						
C:\Program Files (x86)\ClipClip\unins000.exe						
C:\Program File (x86)\Common Files\Apple\Intern...	22/01/2020 4:27:34	22/01/2020 4:27:34	67.384	A		iCloud for Windows
C:\Program Files (x86)\Common Files\Steam\steam...	25/03/2021 3:03:05	15/02/2021 14:34:57	2.773.224	A		Steam Client Service
C:\Program File (x86)\Elcomsoft Password Recover...						
C:\Program Files (x86)\Epic Games\Launcher\Porta...	25/03/2021 18:53:02	28/10/2020 9:13:36	2.788.320	A		Unreal Engine
C:\PROGRAM FILES (X86)\EPIC GAMES\Launcher\P...	25/03/2021 18:53:02	17/12/2020 14:25:07	33.036.768	A		Unreal Engine
C:\Program Files (x86)\Epic Games\Launcher\Porta...						
C:\Program Files (x86)\FreeMind\FreeMind.exe						
C:\Program Files (x86)\Google\Chrome\Application...	29/03/2021 20:25:57	09/09/2018 0:05:02	2.323.560	A		Google Chrome
C:\Program File (x86)\InstallShield Installation Infor...	02/02/2020 17:29:03	02/02/2020 17:29:17	311.296	A		Battery Calibration
C:\Program Files (x86)\Microsoft Office\Root\Office...	13/03/2021 1:12:34	13/03/2021 1:12:33	47.785.248	A		Microsoft Office
C:\Program Files (x86)\Microsoft Office\root\Office...	13/03/2021 1:13:15	13/03/2021 1:13:15	23.927.104	A		Microsoft Office
C:\Program Files (x86)\Microsoft Office\root\Office...	13/03/2021 1:13:20	13/03/2021 1:13:20	9.793.864	A		Microsoft Office
C:\Program Files (x86)\Microsoft Office\Root\Office...	13/03/2021 1:13:22	13/03/2021 1:13:22	16.529.232	A		Microsoft Office
C:\Program File (x86)\Microsoft Office\Root\Office...	13/03/2021 1:13:24	13/03/2021 1:13:24	11.573.056	A		Microsoft Office
C:\Program Files (x86)\Microsoft Office\root\Office...	13/03/2021 1:13:37	13/03/2021 1:13:37	32.078.120	A		Microsoft Outlook
C:\Program Files (x86)\Microsoft Office\Root\Office...	13/03/2021 1:13:39	13/03/2021 1:13:39	1.872.176	A		Microsoft Office
C:\Program File (x86)\Microsoft Office\Root\Office...	13/03/2021 1:13:50	13/03/2021 1:13:50	1.949.000	A		Microsoft Office
C:\Program Files (x86)\Microsoft Office\Root\VFS\P...	13/03/2021 1:14:22	13/03/2021 1:14:22	231.736	A		Microsoft Office InfoPath
C:\Program File (x86)\Microsoft Edge\Application...	01/04/2021 10:51:20	04/04/2021 23:22:45	3.138.960	A		Microsoft Edge
C:\Program Files (x86)\MSI\Battery Calibration\MSI...	09/06/2015 15:10:28	09/06/2015 15:10:28	602.792	A		MSIBatteryCalibration
C:\Program Files (x86)\MSI\Dragon Gaming Center\...	28/01/2015 20:19:14	28/01/2015 20:19:14	6.835.848	A		Dragon Gaming Center
C:\PROGRAM FILES (X86)\MSI\SUPER CHARGER\SU...	21/02/2014 19:42:40	30/12/2015 4:05:01	1.047.536	A		SUPER CHARGER
C:\Program Files (x86)\Nmap\Uninstall.exe						
C:\Program Files (x86)\Nmap\zenmap.exe						
C:\Program Files (x86)\Quick Stego\quickstego.exe						
C:\Program Files (x86)\Quick Stego\unins000.exe						

246 Executable Files, 1 Selected

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

Otra utilidad de Nirsoft : WinPrefetchView

NetworkInterfaceView	Displays the list of all network adapters/interfaces...	NET	24/03/2020 16:23:59		https://www.nirsoft.net/utils/networkinterfaceview.htm
InstalledAppView	View installed Windows 10 apps	1.01	21/05/2020 23:52:46		https://www.nirsoft.net/utils/installedappview.htm
OutlookStatView	Display a general statistics of your Outlook emails.	2.18	26/04/2020 11:24:34		https://www.nirsoft.net/utils/outlookstatview.htm
OfflineRegistryFinder	Find data in external Registry files	1.10	20/04/2020 10:32:12		https://www.nirsoft.net/utils/offlineregistryfinder.htm
NTFSLinksView	View the list of NTFS symbolic links/junctions in s...	1.31	11/04/2020 14:43:44		https://www.nirsoft.net/utils/ntfslinksview.htm
WhoIsThisDomain	Get information about a registered domain from ...	2.42	02/04/2020 16:07:38		https://www.nirsoft.net/utils/whoisthisdomain.htm
ProcessTCPSummary	Displays TCP connections summary	1.11	02/03/2020 1:46:20		https://www.nirsoft.net/utils/procsummary.htm
IPNetInfo	Easily find all available information about IP addr...	1.90	14/02/2020 18:06:02		https://www.nirsoft.net/utils/ipnetinfo.htm
WinPrefetchView	View the Prefetch files (.pf) stored in your system.	1.36	11/02/2020 14:18:34		https://www.nirsoft.net/utils/winprefetchview.htm
NetworkCountersWatch	Displays system counters for every network interf...	1.02	26/01/2020 16:56:42		https://www.nirsoft.net/utils/networkcounterswatch.htm
SearchMyFiles	Alternative to the standard "Search For Files And ...	3.10	14/01/2020 14:54:58		https://www.nirsoft.net/utils/searchmyfiles.htm
iepv	Recover passwords stored by Internet Explorer (V...		04/12/2019 22:53:50		https://www.nirsoft.net/utils/iepv.htm
MZCookiesView	alternative to the standard 'Cookie Manager' prov...	1.58	27/10/2019 11:37:00		https://www.nirsoft.net/utils/mzcookiesview.htm
DriveLetterView	View and change drive letter assignments	1.50	26/10/2019 9:32:56		https://www.nirsoft.net/utils/driveletterview.htm

WinPrefetchView								
File	Edit	View	Options	Help				
Filename	/	Created Time	Modified Time	File Size	Process EXE	Process Path	Run Counter	Last Run Time
Z7G.EXE-F4983D46.pf		02/03/2021 19:19...	14/03/2021 15:22...	92.478	Z7G.EXE	C:\PROGRAM FILES\7-Zip\7z.exe	3	14/03/2021 15:22:22, 02/03/2021 19:58:40, 0...
JU14D2N.TMP-DF69E...		21/03/2021 20:18...	26/03/2021 13:19...	20.979	_JU14D2N.TMP	C:\USERS\RAMON\APPDATA\LOCAL\TEM...	2	26/03/2021 13:19:48, 21/03/2021 20:18:02
AGMSERVICE.EXE-68B...	05/04/2021 16:48...	05/04/2021 16:49...	5.440	AGMSERVICE.EXE	C:\PROGRAM FILES (X86)\COMMON FILE...	4	05/04/2021 16:49:00, 05/04/2021 16:49:00, 0...	
AGSSERVICE.EXE-A97...	05/04/2021 16:48...	05/04/2021 16:49...	5.297	AGSSERVICE.EXE	C:\PROGRAM FILES (X86)\COMMON FILE...	5	05/04/2021 16:49:00, 05/04/2021 16:48:59, 0...	
APPLICATIONFRAME...	01/10/2020 0:00:00	05/04/2021 14:48...	16.342	APPLICATIONFRA...	C:\Windows\System32\APPLICATIONFRA...	420	05/04/2021 14:48:09, 05/04/2021 11:08:39, 0...	
AUTORUNS.EXE-B5C5...	05/04/2021 16:13...	05/04/2021 16:13...	37.947	AUTORUNS.EXE	C:\Windows\System32\autoruns...	1	05/04/2021 16:13:06	
BLACKDESERTLAUNC...	20/03/2021 19:30...	20/03/2021 19:41...	8.884	BLACKDESERTLAU...	D:\STEAMLIBRARY\STEAMAPPS\COMM...	2	20/03/2021 19:41:18, 20/03/2021 19:30:12	
BLACKDESERTPAT...	20/03/2021 19:30...	20/03/2021 19:41...	58.936	BLACKDESERTPAT...	D:\STEAMLIBRARY\STEAMAPPS\COMM...	6	20/03/2021 19:41:19, 20/03/2021 19:41:19, 2...	
CALCULATOR.EXE-548...	23/03/2021 15:19...	05/04/2021 15:06...	30.952	CALCULATOR.EXE	C:\PROGRAM FILES\WINDOWSAPPS\MICR...	3	05/04/2021 15:06:38, 05/04/2021 14:48:33, 2...	
CHROME.EXE-5349D02...	01/10/2020 12:06...	26/03/2021 16:52...	108.921	CHROME.EXE	C:\PROGRAM FILES (X86)\Google\Chrom...	120	26/03/2021 16:52:21, 26/03/2021 13:23:14, 2...	
CHROME.EXE-5349D02...	01/10/2020 12:06...	26/03/2021 16:52...	28.326	CHROME.EXE	C:\PROGRAM FILES (X86)\Google\Chrom...	745	26/03/2021 16:52:22, 26/03/2021 16:52:22, 2...	
CONHOST.EXE-0C645...	20/03/2021 19:30...	05/04/2021 16:48...	6.929	CONHOST.EXE	C:\Windows\System32\conhost.exe	193	05/04/2021 16:48:47, 05/04/2021 15:50:21, 0...	
CONSENT.EXE-404193...	05/04/2021 16:45...	05/04/2021 16:59...	8.615	CONSENT.EXE	C:\Windows\System32\consent.exe	2	05/04/2021 16:59:50, 05/04/2021 16:45:13	
DISCORD.EXE-056EF...	23/10/2020 17:54...	09/02/2021 15:50...	37.629	DISCORD.EXE	C:\Users\ramon\AppData\Discord\A...	20	09/02/2021 15:50:36, 16/12/2020 0:01:36, 0/...	
DISCORD.EXE-5CAB2...	16/12/2020 0:02:05...	05/04/2021 11:14...	58.325	DISCORD.EXE	C:\Users\ramon\AppData\Local\Discord\A...	83	05/04/2021 11:14:21, 28/03/2021 0:46:49, 27/...	
DOLBYACCESS.EXE-95...	26/03/2021 3:25:36...	26/03/2021 3:25:36...	48.536	DOLBYACCESS.EXE	C:\PROGRAM FILES\WINDOWSAPPS\DOB...	1	26/03/2021 3:25:25	
EPICGAMESLAUNCHER...	25/03/2021 18:52...	25/03/2021 18:58...	65.224	EPICGAMESLAUN...	C:\PROGRAM FILES (X86)\EPIC GAMES\La...	2	25/03/2021 18:58:50, 25/03/2021 18:52:48	
EXCEL.EXE-B2758640.pf	16/11/2020 15:10...	20/01/2021 19:24...	93.735	EXCEL.EXE	C:\PROGRAM FILES (X86)\MICROSOFT OFF...	22	20/01/2021 19:24:32, 18/01/2021 19:46:22, 1...	

144 Files, 1 Selected NirSoft Freeware. <http://www.nirsoft.net>

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 r2 SP1 Evaluation Edition" --sup-hardenin
g-log=D:\MaquinasVirtuales\Retencion\Logs\VBoxHardening.log

Base          Size      Path
0x00000000e3680000 0x118000  C:\Program Files\Oracle\VirtualBox\VirtualBoxVM.exe
0x0000000026470000 0x1f5000  C:\WINDOWS\SYSTEM32\ntdll.dll
0x0000000025730000 0xb000   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
588: File  (R-D)  C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackes-ES_19041.17.51.0_neutral_8wekyb3d8
-----
```