



Análisis Forense

Análisis de evidencias

María Andrea Ugarte Valencia

Marcos Villar Avión

Contents

1		3
1.1	3
1.2	3
1.3	4
2		6
2.1	6
2.2	7
3		7
3.1	7
3.1.1	7
3.1.2	9
3.1.3	13
3.1.4	14
3.1.5	16
3.1.6	17
3.1.7	25
3.1.8	26
3.1.9	29
3.1.10	31
3.1.11	33
3.2	34

1

1.1

Abrimos nuestro Autopsy instalado previamente en la resolución del caso forense "Trabajador traidor a su empresa" y creamos un nuevo caso:

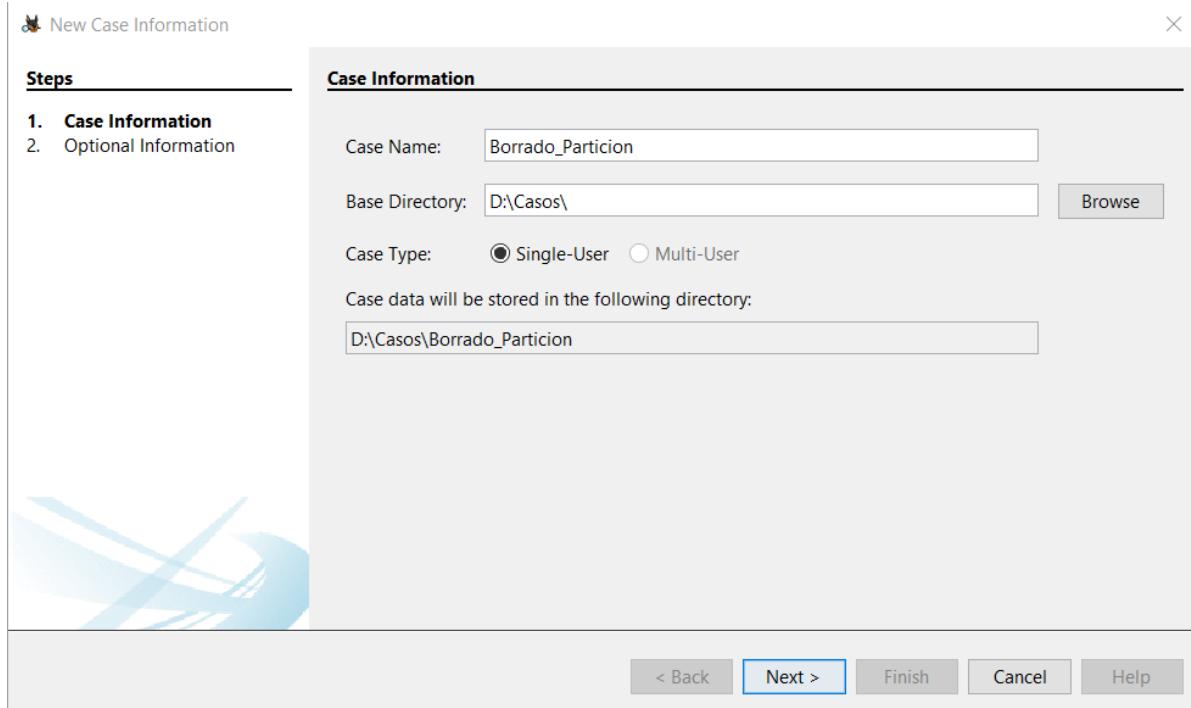


Figure 1: Creación de un nuevo caso

1.2

Cuando primeramente añadimos la imagen generada en la práctica anterior como fuente de datos, nos dimos cuenta de que no teníamos acceso a la segunda partición ya que hicimos la copia únicamente del tamaño de la primera, por lo que volvimos a seguir los pasos de la práctica y generamos una nueva imagen. Una vez listo, cargamos la fuente de datos.

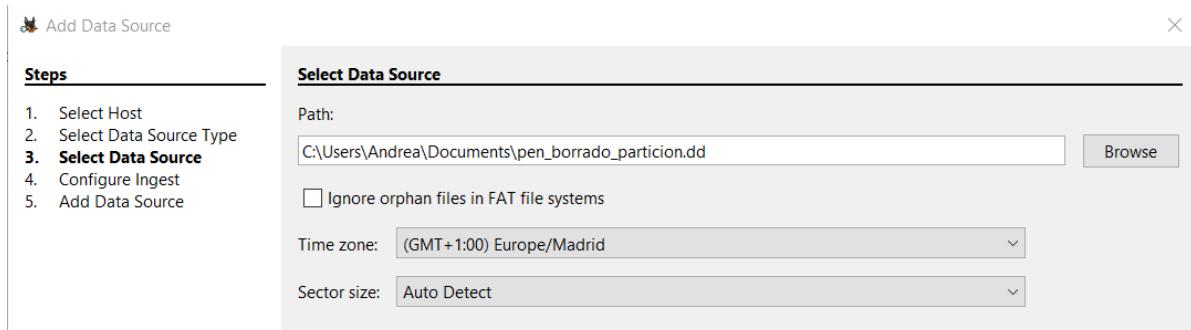


Figure 2: Añadiendo la fuente de datos

1.3

Una vez cargada la fuente de datos, en nuestro caso personal, no hemos necesitado ningún módulo para recuperar la información eliminada, ya que nos ha dado los datos directamente. Sin embargo, para otros casos parecidos, sería interesante seleccionar los siguientes módulos:

- **Recent Activity:** se utiliza para analizar la actividad reciente en un sistema informático.
- **File Type Identification:** se usa para identificar y categorizar los distintos tipos de archivos presentes.
- **Embedded File Extractor:** se utiliza para extraer archivos incrustados dentro de otros archivos.
- **Interesting Files Identifier:** este módulo busca archivos considerados como interesantes como pueden ser archivos de contraseñas, de configuración, imágenes sensibles,...
- **PhotoRec Carver:** se usa para recuperar archivos perdidos o borrados de medios de almacenamiento. De todas las opciones, esta sería la más interesante para este apartado.

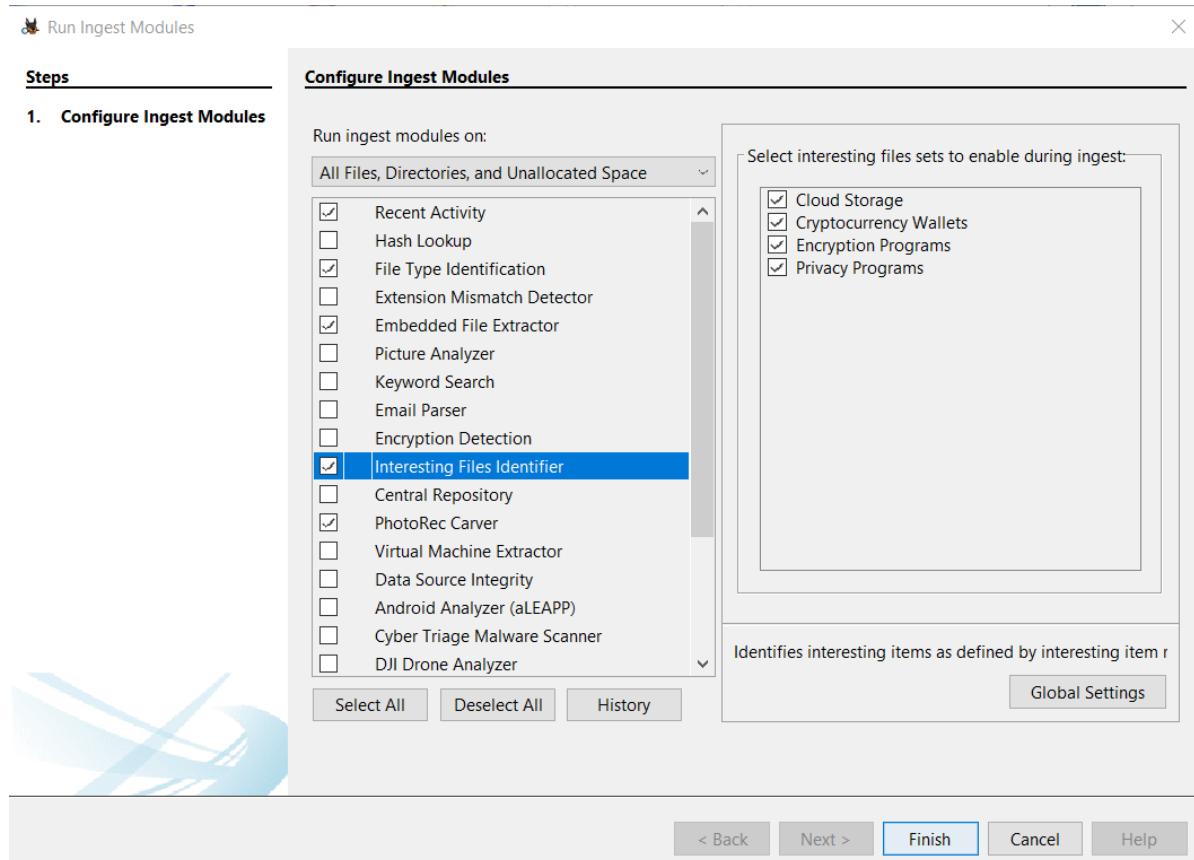


Figure 3: Módulos interesantes

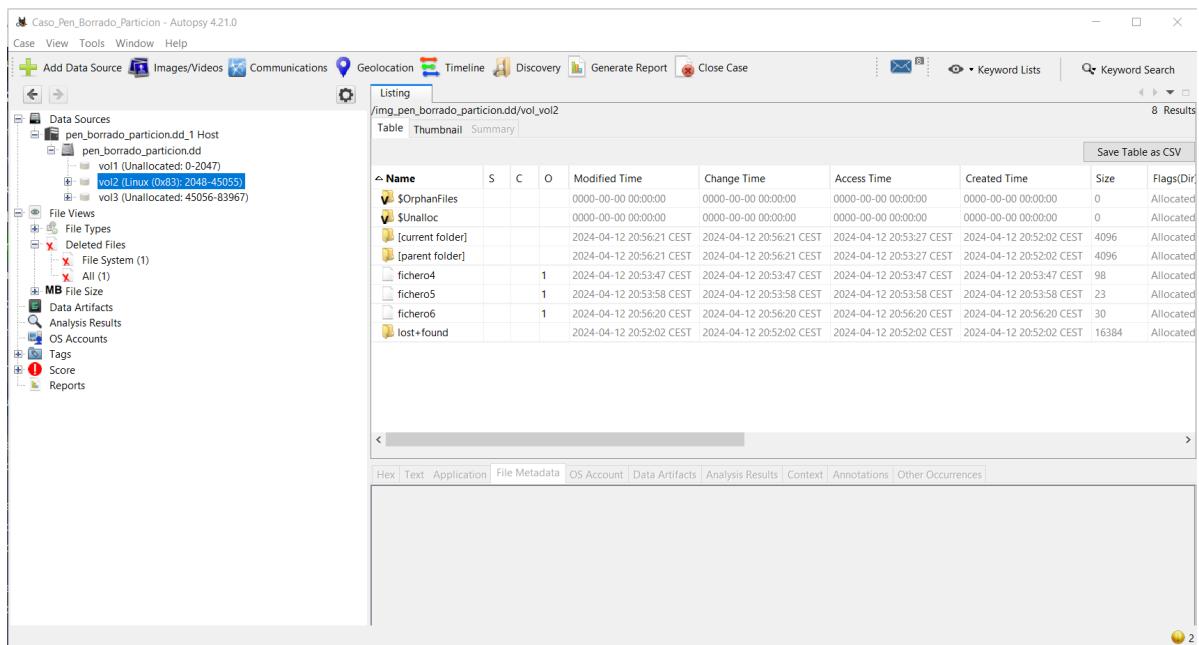


Figure 4: Archivos recuperados de una de las particiones

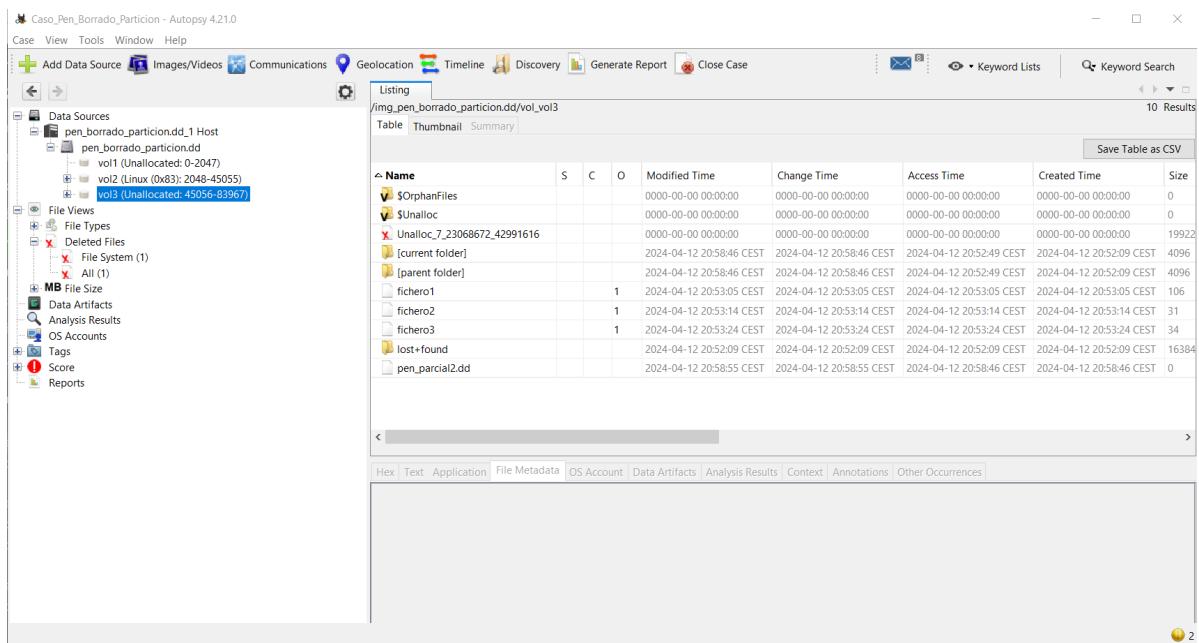


Figure 5: Archivos recuperados de la otra partición

2

2.1

Si ejecutamos la opción **imageinfo** de Volatility se nos mostrará información básica de la imagen de memoria. Entre ella, nos saldrán los sistemas operativos a los que puede pertenecer. Viendo la salida todo indica a que el sistema operativo es **Windows XP con Service Pack 2 en una arquitectura de 32 bits**. A partir de ahora lo usaremos de perfil. Esto lo hemos probado tanto en la versión de Volatility 3 como en la versión 2.6.1.

```
PS D:\volatility-master\volatility-master> py -2 vol.py -f memory.img imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug      : Determining profile based on KDBG search...
Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                      AS Layer1 : IA32PagedMemory (Kernel AS)
                      AS Layer2 : FileAddressSpace (D:\volatility-master\volatility-master\memory.img)
                      PAE type : No PAE
                        DTB : 0x39000L
                        KDBG : 0x8054c060L
Number of Processors : 1
Image Type (Service Pack) : 2
                      KPCR for CPU 0 : 0xffffd0000L
                      KUSER_SHARED_DATA : 0xffffdf0000L
Image date and time : 2005-07-04 18:30:32 UTC+0000
Image local date and time : 2005-07-04 14:30:32 -0400
```

Figure 6: imageinfo en Volatility 2.6.1

```
[(kali㉿kali)-[~/volatility3]]
└─$ python3 vol.py -f memory.img windows.info.Info
Volatility 3 Framework 2.7.0
Progress: 100.00          PDB scanning finished
Variable      Value
Kernel Base      0x804d7000
DTB      0x39000
Symbols file:///home/kali/volatility3/volatility3/symbols/windows/ntoskrnl.pdb/32962337F0F646388B39535CD8DD70E8-2.json.xz
Is64Bit False
IsPAE  False
layer_name      0 WindowsIntel
memory_layer     1 FileLayer
KdDebuggerDataBlock  0x8054c060
NTBuildLab     2600.xpsp_sp2_gdr.050301-1519
CSVersion       2
KdVersionBlock  0x8054c038
Major/Minor     15.2600
MachineType     332
KeNumberProcessors 1
SystemTime      2005-07-04 18:30:32
NtSystemRoot    C:\WINDOWS
NtProductType   NtProductWinNt
NtMajorVersion  5
NtMinorVersion  1
PE MajorOperatingSystemVersion 5
PE MinorOperatingSystemVersion 1
PE Machine      332
PE TimeStamp     Wed Mar  2 00:59:37 2005
```

Figure 7: imageinfo en Volatility 3

2.2

Para obtener los nombres de usuario junto con los hashes de sus contraseñas usamos la opción **hivelist** para identificar las ubicaciones de los archivos correspondientes a diferentes partes del registro de Windows. Así, podemos localizar la tabla SAM, que contiene los hashes de las contraseñas de los usuarios locales del sistema.

```
PS D:\volatility-master\volatility-master> py -2 vol.py -f memory.img --profile=WinXPSP2x86 hivelist
Volatility Foundation Volatility Framework 2.6.1
Virtual Physical Name
-----
0xe2610b60 0x14a99b60 \Device\HarddiskVolume1\Documents and Settings\Sarah\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe25f0578 0x17141578 \Device\HarddiskVolume1\Documents and Settings\Sarah\NTUSER.DAT
0xe1d33008 0x0f12c008 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1c73888 0x0fc5888 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe1c04688 0x0e88e688 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1b70b60 0x0dff5b60 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe1658b60 0x0c748b60 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe1a5a7e8 0x094bf7e8 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe165cb60 0x0c6ecb60 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe1a4f770 0x0948c770 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0xe1559b38 0x02d64b38 [no name]
0xe1035b60 0x0283db60 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe102e008 0x02837008 [no name]
```

Figure 8: Uso de la opción hivelist

Una vez que hemos identificado la ubicación de la tabla SAM (0xe165cb60), podemos extraer los hashes de las contraseñas y los nombres de usuario con la opción **hashdump**, que escanea la memoria volátil en busca de las áreas donde se almacenan los hashes de contraseñas y los extrae para su visualización. Estos hashes son útiles ya que se podrían usar para intentar crackear las contraseñas.

```
PS D:\volatility-master\volatility-master> py -2 vol.py -f memory.img --profile=WinXPSP2x86 hashdump -y 0xe165cb60
Volatility Foundation Volatility Framework 2.6.1
Administrator:500:08f3a52bdd35f179c81667e9d738c5d9:ed88ccbc08d1c18bcded317112555f4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:ddd4c9c883a8ecb2078f88d729ba2e67:e78d693bc40f92a534197dc1d3a6d34f:::
SUPPORT_388945a:1002:aad3b435b51404eeaad3b435b51404ee:8bfd47482583168a0ae5ab020e1186a9:::
phoenix:1003:07b8418e83fad948aad3b435b51404ee:53905140b80b6d8cbe1ab5953f7c1c51:::
ASPNET:1004:2b5f618079400df84f9346ce3e830467:aef73a8bb65a0f01d9470fadcc55a411c:::
Sarah:1006:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Figure 9: Uso de la opción hashdump

3

Para este apartado usaremos la versión 2.6.1 de Volatility y la versión 4.21.0 de Autopsy. Se han usado los plugins por defecto de Autopsy además de algunos a mayores para tratar de recopilar toda la información posible. Cabe destacar el uso del módulo PhotoRec Carver para recuperar archivos eliminados.

3.1

3.1.1

Al igual que en el apartado 2.a, hemos usado la opción **imageinfo** de Volatility para ver el sistema operativo usado para el ataque:

```

PS D:\> cd D:\volatility-master\volatility-master
PS D:\volatility-master\volatility-master> py -2 vol.py -f memory.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418,
Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (D:\volatility-master\volatility-master\memory.raw)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf800027fd0a0L
Number of Processors : 2
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffffff800027fed000L
KPCR for CPU 1 : 0xfffffff880009ea000L
KUSER_SHARED_DATA : 0xfffffff78000000000L
Image date and time : 2024-03-21 09:42:22 UTC+0000
Image local date and time : 2024-03-21 10:42:22 +0100

```

Figure 10: Uso de la opción imageinfo

Sin embargo, podemos ver que nos muestra demasiadas posibilidades, por lo que intentaremos reducirlas con Autopsy. Para ello, consultaremos la información del sistema operativo:

The screenshot shows the Autopsy 4.21 interface. The left sidebar lists various data sources and artifacts. The main pane displays 'Operating System Information' for a host named 'diskimg_1 Host'. A table provides details about the operating system, including:

Source Name	S	C	O	Name	Program Name	Processor Architecture	Temporary Files Directory	Path	Product ID
diskimg				JARVIS	Windows 7 Enterprise Service Pack 1	AMD64	%SystemRoot%\TEMP	C:\Windows	00392-918-5000C

Figure 11: Información del sistema operativo en Autopsy

Podemos afirmar que el sistema operativo es **Windows 7 con Service Pack 1 en una arquitectura de 64 bits**. Ahora sabemos que los perfiles que podremos usar en Volatility serán: Win7SP1x64, Win7SP1x64_24000 o Win7SP1x64_23418. Nos da igual cuál usar ya que solo cambia en ciertos módulos.

3.1.2

En Autopsy podemos ver los usuarios del sistema en el apartado **Users**.

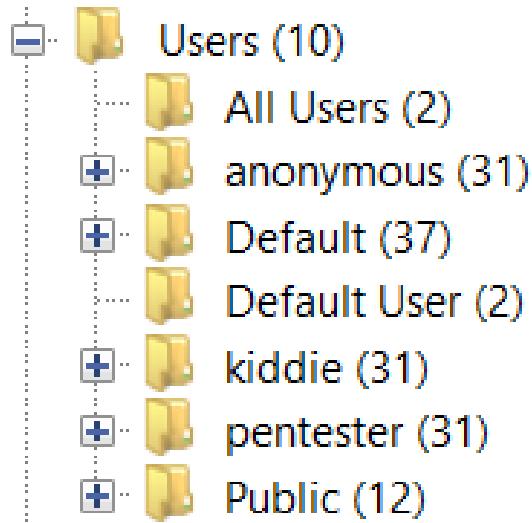


Figure 12: Usuarios del sistema en Autopsy

Si nos vamos a **OS Accounts**, las cuentas del sistema operativo, también los podemos encontrar:

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-18				SYSTEM	diskimg_1.. Local		NT AUTHORITY	
S-1-5-80-95600885-341852649-1831038044-185	1				diskimg_1.. Local		NT SERVICE	
S-1-5-19				LOCAL SERVICE	diskimg_1.. Local		NT AUTHORITY	
S-1-5-21-527521925-1815409902-1655353942-10C	0			kiddie	diskimg_1.. Domain			2024-02-29 01:56:55 CET
S-1-5-21-527521925-1815409902-1655353942-10C	0			anonymous	diskimg_1.. Domain			2024-02-29 01:47:43 CET
S-1-5-21-527521925-1815409902-1655353942-10C	0			pentester	diskimg_1.. Domain			2024-02-29 01:58:31 CET
S-1-5-20					NETWORK SERVICE	diskimg_1.. Local	NT SERVICE	
S-1-5-21-527521925-1815409902-1655353942-501	1			Invitado	diskimg_1.. Domain			2024-02-29 01:46:52 CET
S-1-5-21-527521925-1815409902-1655353942-501	0			Administrador	diskimg_1.. Domain			2024-02-29 01:46:52 CET

Figure 13: Usuarios del sistema en Autopsy

En Volatility, podríamos acceder a los usuarios y sus contraseñas encriptadas de la misma forma que en el apartado 2.b

```

PS D:\volatility-master\volatility-master> py -2 vol.py -f memory.raw --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6.1
Virtual          Physical          Name
-----
0xfffff8a0029e1010 0x0000000d4610010 \?\C:\Users\pentester\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a003229010 0x0000000a53e2010 \SystemRoot\System32\Config\DEFAULT
0xfffff8a0075b4010 0x00000006e149010 \?\C:\Users\pentester\ntuser.dat
0xfffff8a00000c010 0x0000000aa4c7010 [no name]
0xfffff8a000024010 0x0000000a9514010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a00004320 0x0000000a953e320 \REGISTRY\MACHINE\HARDWARE
0xfffff8a0005fc010 0x000000080203010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a0009fe010 0x000000083cb8010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a000f97170 0x0000000a85d1170 \SystemRoot\System32\Config\SECURITY
0xfffff8a00102e010 0x0000000a8961010 \SystemRoot\System32\Config\SAM
0xfffff8a001109010 0x0000000559f8010 \?\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a0011ad010 0x000000054d94010 \?\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a001501010 0x00000008c041010 \?\C:\Users\kiddie\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a001502410 0x00000004b840410 \?\C:\Users\kiddie\ntuser.dat
0xfffff8a00265c010 0x0000000104519010 \?\C:\System Volume Information\Syscache.hve
PS D:\volatility-master\volatility-master>

```

Figure 14: Uso de la opción hivelist

```

PS D:\volatility-master\volatility-master> py -2 vol.py -f memory.raw --profile=Win7SP1x64 hashdump -y 0xfffff8a00102e010
Volatility Foundation Volatility Framework 2.6.1
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
anonymous:1000:aad3b435b51404eeaad3b435b51404ee:3bf8787c73729d592047a8ff57f181bd:::
kiddie:1001:aad3b435b51404eeaad3b435b51404ee:4ec43f01fd703a75c984bfd88b24011:::
pentester:1002:aad3b435b51404eeaad3b435b51404ee:bc4a3605f88a0547f0e2ca855b5c9a40:::

```

Figure 15: Uso de la opción hashdump

Por tanto, podemos saber que los usuarios del sistema son: Administrador, Invitado, anonymous, kiddie y pentester

Podemos intentar buscar más información sobre las contraseñas con la opción **lsadump**, que escanea la memoria volátil en busca de la estructura de datos que contiene la Base de Datos de Autorización de Seguridad Local para así extraer información relevante como los usuarios y sus contraseñas.

```

PS D:\volatility-master\volatility-master> py -2 vol.py -f memory.raw --profile=Win7SP1x64 lsadump
Volatility Foundation Volatility Framework 2.6.1
DefaultPassword
0x00000000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0x00000010 66 5e 29 9e 9c ca 1d 3d 6e ab e7 3d 58 58 ba 63 f^)....=n..=XX.c

DPAPI_SYSTEM
0x00000000 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ,.... .
0x00000010 01 00 00 00 f9 c3 44 96 cc e5 54 f1 9e e9 9c 23 .....D...T....#
0x00000020 32 ab 7c 8b e4 d6 5f 22 34 b5 cc 20 24 a1 fa 00 2.|...."4...$...
0x00000030 4c 33 5b bb c2 97 9a d4 40 de 74 76 00 00 00 00 L3[.....@.tv....
```

Figure 16: Uso de la opción lsadump

La sección DefaultPassword nos muestra la contraseña que se usa como predeterminada en el sistema. Sin embargo, la salida no parece mostrar información de interés.

Por otro lado, la sección DPAPI_SYSTEM revela las credenciales que están protegidas utilizando un sistema llamado DPAPI, que es una forma de proteger información confidencial en Windows, como contraseñas. De nuevo, los datos no parecen revelar nada nuevo.

Para intentar conseguir las contraseñas en claro, se ha usado el plugin **mimikatz**, que ayuda a la extracción de las mismas en sistemas Windows. Una vez ejecutado, se han obtenido las contraseñas de dos de los usuarios: pentester y kiddie.

```
PS D:\volatility-master\volatility-master> py -2 vol.py --plugins=.\\plugins -f memory.raw --profile=Win7SP1x64 mimikatz
Volatility Foundation Volatility Framework 2.6.1
Module User Domain Password
-----
wdigest pentester jarvis Pw:lnQL04,
wdigest kiddie jarvis AnW9.s2Nmwl!
wdigest JARVIS$ WORKGROUP
```

Figure 17: Uso del plugin mimikatz

La contraseña del usuario anonymous también ha sido encontrada en claro. Esto se explica en el apartado vi de la memoria.

Por tanto, las credenciales que tenemos son:

- pentester: Pw:lnQL04,
- kiddie: AnW9.s2Nmwl!
- anonymous: Ñ4p4:)

En cuanto a qué usuario realizó el ataque informático, primero consultamos si en Autopsy podíamos encontrar alguna pista. Investigando, pudimos ver en el historial web que el usuario kiddie ha hecho búsquedas relacionadas con ataques informáticos.

The screenshot shows the Autopsy 4.21 interface with the 'Web History' tab selected. The main pane displays a table of search results with columns: Source Name, S, C, O, URL, Date Accessed, and Title. The results show various Google search queries related to hacking and malware, such as 'hacker sitereedit.com - Buscar con Google', 'Se acuerdan de este HACKER : r/CallOfDutyMobileES', and 'keepass - Reddit Search!'. The left sidebar shows a tree view of the forensic analysis, including sections like 'Installed Programs', 'Operating System Information', and 'Analysis Results'. The bottom pane shows detailed properties for a selected item, including 'Basic Properties' like Login: kiddie and Full Name: kiddie, and 'Host Details' like Last Login: 2024-03-21 09:59:59 CET and Login Count: 9.

Figure 18: Historial web en Autopsy

places.sqlite		google.com	como hacer un ataque informatico	FireFox Analyzer	2024-03-21 10:01:20 CET	disk.img
places.sqlite		google.com	el lado del mal	FireFox Analyzer	2024-03-21 10:01:34 CET	disk.img
places.sqlite		google.com	ataques de red site:elladodelmal.com	FireFox Analyzer	2024-03-21 10:01:42 CET	disk.img
places.sqlite		google.com	vulnerabilidades servidores	FireFox Analyzer	2024-03-21 10:02:41 CET	diskimg

Figure 19: Búsquedas en Google

Buscando pistas más contundentes, ejecutamos la opción **getsids** de Volatility, que se utiliza para extraer y listar los SIDs (Identificadores de Seguridad) presentes en la memoria volátil, que son identificadores únicos asignados a cada cuenta de usuario, grupo y objeto de seguridad en un sistema Windows.

```
PS D:\> cd D:\volatility-master\volatility-master
PS D:\volatility-master\volatility-master> py -2 vol.py -f memory.raw --profile=Win7SP1x64 getsids
Volatility Foundation Volatility Framework 2.6.1
```

Figure 20: Uso de la opción getsids

Analizamos la salida y vemos que el usuario kiddie está asociado a los procesos de la consola de comandos:

```
cmd.exe (5132): S-1-5-21-527521925-1815409902-1655353942-1001 (kiddie)
```

Figure 21: Salida interesante getsids

```
conhost.exe (6676): S-1-5-21-527521925-1815409902-1655353942-1001 (kiddie)
```

Figure 22: Salida interesante getsids

Ahora, si ejecutamos la opción **consoles** de Volatility podremos ver el ataque realizado, que se explicará con más detalle en el apartado viii. Si nos fijamos, podemos ver que los PIDs coinciden con los del usuario kiddie mostrados gracias a la opción **getsids**. Por tanto, podemos decir que el usuario que realizó el ataque fue kiddie.

```
PS D:\volatility-master\volatility-master> py -2 vol.py -f memory.raw --profile=Win7SP1x64 consoles
Volatility Foundation Volatility Framework 2.6.1
*****
ConsoleProcess: conhost.exe Pid: 6676
Console: 0xff286200 CommandHistorySize: 50
HistoryBufferCount: 4 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\System32\cmd.exe
Title: C:\Windows\System32\cmd.exe
AttachedProcess: cmd.exe Pid: 5132 Handle: 0x64
```

Figure 23: Uso de la opción consoles

3.1.3

Primero, se obtendrán todas las cadenas de texto legibles en el archivo con la herramienta **strings** para buscar nombres de persona.

```
D:\volatility-master\volatility-master>strings.exe memory.raw > salida.txt
>
Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com
```

Figure 24: Uso de la herramienta strings

Tras hacer varias búsquedas en el archivo de salida, no se ha encontrado ningún nombre relevante.

Sabiendo que el usuario que realizó el ataque fue el usuario kiddie, vamos a intentar encontrar su nombre con Autopsy mirando entre sus archivos. Si nos vamos a la carpeta de **Documentos** del usuario kiddie nos encontramos la siguiente imagen:



Figure 25: Foto encontrada en los archivos de kiddie

Si consultamos con una herramienta los metadatos del archivo podemos encontrar un nombre, **Judith Santamaria Morales**. Para hacer esto, se ha usado la herramienta **exiftool**.

```
D:\exiftool-12.84>exiftool linkedin.png
ExifTool Version Number      : 12.84
File Name                   : linkedin.png
Directory                   : .
File Size                    : 170 kB
File Modification Date/Time : 2024:05:09 18:23:08+02:00
File Access Date/Time       : 2024:05:09 18:31:06+02:00
File Creation Date/Time    : 2024:05:09 18:27:36+02:00
File Permissions            : -rw-rw-rw-
File Type                   : PNG
File Type Extension         : png
MIME Type                   : image/png
Image Width                 : 328
Image Height                : 320
Bit Depth                   : 8
Color Type                  : RGB with Alpha
Compression                 : Deflate/Inflate
Filter                      : Adaptive
Interlace                   : Noninterlaced
Exif Byte Order             : Big-endian (Motorola, MM)
Camera Model Name           : Samsung Galaxy Z Flip 5 de Judith Santamaría Morales
Resolution Unit              : inches
Y Cb Cr Positioning        : Centered
Image Size                  : 328x320
Megapixels                  : 0.105
```

Figure 26: Metadatos de la imagen

3.1.4

Si nos vamos a los archivos eliminados, nos encontramos una foto que parece ser sacada por algún usuario del dispositivo.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags
IMG-3405893082345.jpg				2024-03-21 10:17:45 CET	2024-03-21 10:17:45 CET	2024-03-21 10:17:40 CET	2024-03-21 10:17:40 CET	0	Unalloc
Codigo de Derecho de la Ciberseguridad.pdf				2024-03-21 10:40:39 CET	2024-03-21 10:40:39 CET	2024-03-21 10:40:39 CET	2024-03-21 10:40:39 CET	0	Unalloc
ufti-master.zip				2024-03-21 10:40:39 CET	2024-03-21 10:40:39 CET	2024-03-21 10:40:38 CET	2024-03-21 10:40:38 CET	3632949	Unalloc
rocyoutxt				2024-03-21 10:17:45 CET	2024-03-21 10:17:45 CET	2024-03-21 10:17:40 CET	2024-03-21 10:17:40 CET	139921497	Unalloc
IMG-3405893082345.jpg				2024-03-21 10:17:45 CET	2024-03-21 10:17:45 CET	2024-03-21 10:17:40 CET	2024-03-21 10:17:40 CET	0	Unalloc
Codigo de Derecho de la Ciberseguridad.pdf				2024-03-21 10:40:39 CET	2024-03-21 10:40:39 CET	2024-03-05 23:07:47 CET	2024-03-05 23:07:47 CET	7738389	Unalloc
ufti-master.zip				2024-03-21 10:40:39 CET	2024-03-21 10:40:39 CET	2024-03-21 10:40:38 CET	2024-03-21 10:40:38 CET	3632949	Unalloc
rocyoutxt				2024-03-21 10:40:39 CET	2024-03-21 10:40:39 CET	2024-03-21 10:40:38 CET	2024-03-21 10:40:38 CET	139921497	Unalloc
IMG-3405893082345.jpg				2024-03-21 10:17:45 CET	2024-03-21 10:17:45 CET	2024-03-21 10:17:40 CET	2024-03-21 10:17:40 CET	0	Unalloc
Codigo de Derecho de la Ciberseguridad.pdf				2024-03-21 10:40:39 CET	2024-03-21 10:40:39 CET	2024-03-05 23:07:47 CET	2024-03-05 23:07:47 CET	7738389	Unalloc
ufti-master.zip				2024-03-21 10:40:39 CET	2024-03-21 10:40:39 CET	2024-03-21 10:40:38 CET	2024-03-21 10:40:38 CET	3632949	Unalloc
rocyoutou.txt				2024-03-21 10:40:39 CET	2024-03-21 10:40:39 CET	2024-03-21 10:40:38 CET	2024-03-21 10:40:38 CET	139921497	Unalloc
IMG-3405893082345.jpg				2024-03-21 10:17:45 CET	2024-03-21 10:17:45 CET	2024-03-21 10:17:40 CET	2024-03-21 10:17:40 CET	0	Unalloc
Codigo de Derecho de la Ciberseguridad.pdf				2024-03-21 10:40:39 CET	2024-03-21 10:40:39 CET	2024-03-05 23:07:47 CET	2024-03-05 23:07:47 CET	7738389	Unalloc
ufti-master.zip				2024-03-21 10:40:39 CET	2024-03-21 10:40:39 CET	2024-03-21 10:40:38 CET	2024-03-21 10:40:38 CET	3632949	Unalloc
rocyoutou.txt				2024-03-21 10:40:39 CET	2024-03-21 10:40:39 CET	2024-03-21 10:40:38 CET	2024-03-21 10:40:38 CET	139921497	Unalloc

Figure 27: Imagen encontrada en los archivos eliminados

Es más, si nos vamos a la carpeta Pictures del usuario kiddie, nos la encontramos otra vez, por lo que pertenece a ese usuario.

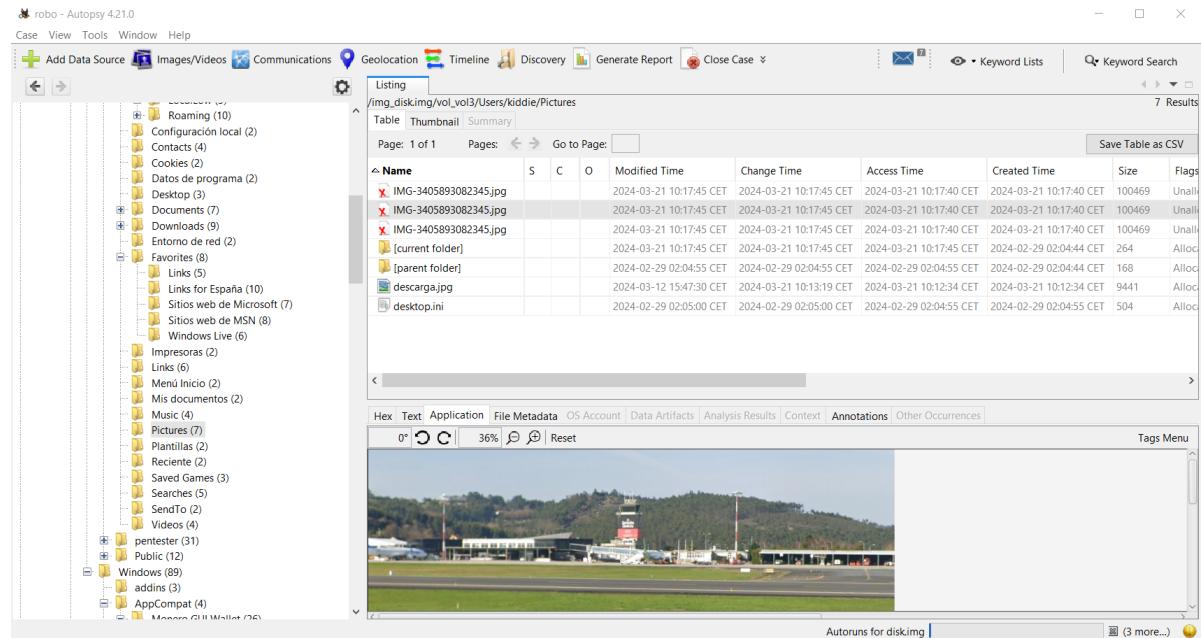


Figure 28: Imagen encontrada en la carpeta Pictures del usuario kiddie

Si geolocalizamos la foto podemos ver que se hizo desde el aeropuerto de Coruña. Por lo que el ataque pudo haber sido realizado desde esa ubicación.

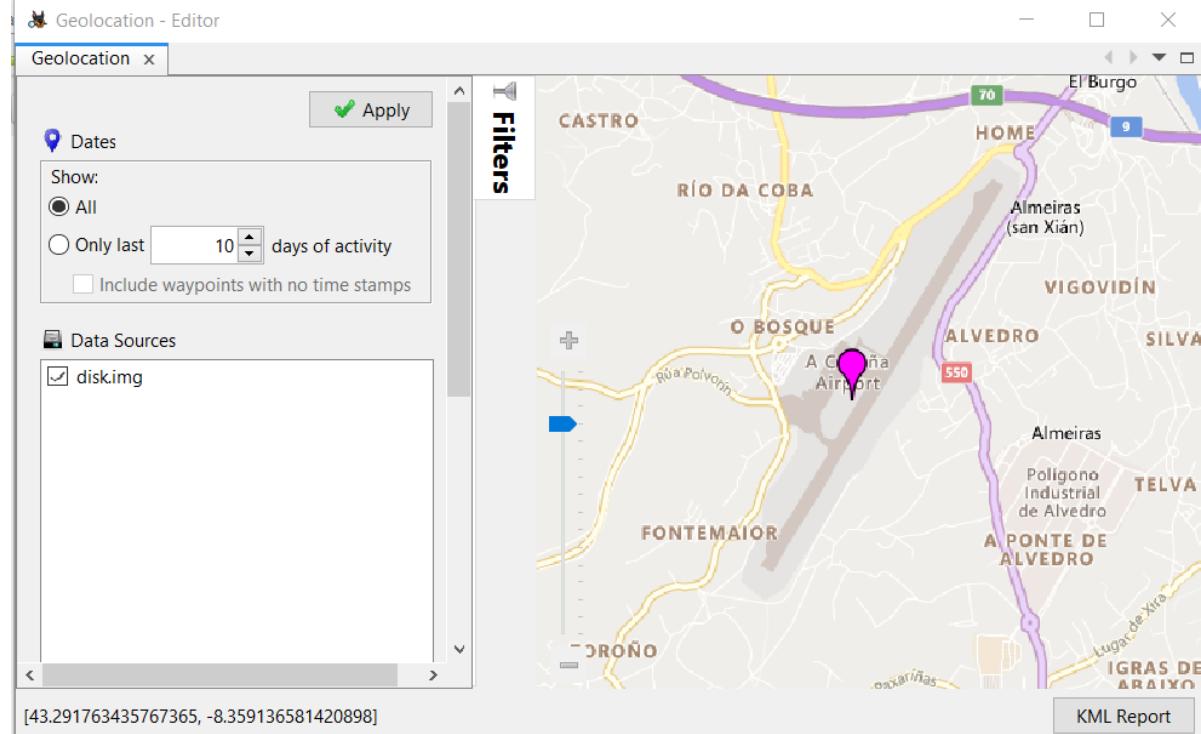


Figure 29: Geolocalización de la imagen

En los metadatos de la imagen podemos ver la fecha y hora en la que se realizó.

Metadata

Name:	/img_disk.img/vol_vo13/Users/kiddie/Pictures/IMG-3405893082345.jpg
Type:	File System
MIME Type:	image/jpeg
Size:	100469
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2024-03-21 10:17:45 CET
Accessed:	2024-03-21 10:17:40 CET
Created:	2024-03-21 10:17:40 CET
Changed:	2024-03-21 10:17:45 CET

Figure 30: Fecha y hora de la imagen

En la salida de consoles aparece una hora próxima a la de la fotografía del aeropuerto encontrada.

```
E:\>"C:\Program Files (x86)\Nmap\nmap.exe" --unprivileged -sV -T5 -p21 --script=**ftp* acme-university.pri
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-21 10:19 Hora est?ndar romanc
e
```

Figure 31: Hora en la que se realizó el ataque

3.1.5

Si ejecutamos la opción de Volatility **cmdscan** podemos extraer información sobre los comandos ejecutados en la línea de comandos, lo cual nos puede revelar información de la información extraída ya que lo más probable es que haya accedido al sistema con la información mediante comandos.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Users\Andrea> D:
PS D:\> cd D:\volatility-master\volatility-master
PS D:\volatility-master\volatility-master> py -2 vol.py -f memory.raw --profile=Win7SP1x64 cmdscan
Volatility Foundation Volatility Framework 2.6.1
*****
CommandProcess: conhost.exe Pid: 6676
CommandHistory: 0xb6540 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 3 LastAdded: 2 LastDisplayed: 2
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x64
Cmd #0 @ 0xa730: "C:\Program Files (x86)\Nmap\nmap.exe" --unprivileged -sV -T5 -p21 --script=**ftp* acme-university.pri
Cmd #1 @ 0xa6540: ftp acme-university.pri
Cmd #2 @ 0xfcfd0: "C:\Program Files\7-Zip\7z.exe" a archivos-robados.7z Estudiantes.xlsx Examen.pdf -p
Cmd #15 @ 0x60158: d
Cmd #16 @ 0xbde70: q
*****
CommandProcess: conhost.exe Pid: 4864
CommandHistory: 0x296550 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #15 @ 0x240158: )
Cmd #16 @ 0x294e60: )
PS D:\volatility-master\volatility-master>
```

Figure 32: Uso de la opción cmdscan

En la salida hay una línea que llama la atención:

```
Cmd #2 @ 0xbfc0d0: "C:\Program Files\7-zip\7z.exe" a archivos-robados.7z Estudiantes.xlsx  
Examen.pdf -p
```

Esta línea nos dice que el culpable creó un archivo comprimido llamado **archivos-robados.7z** con los archivos **Estudiantes.xlsx** y **Examen.pdf**. Por lo que es muy probable que haya robado un examen que iba a tener próximo a la fecha del ataque, junto a un listado de alumnos. Otra cosa a destacar es que con la opción **-p** se indica que ese fichero se proteja con contraseña.

3.1.6

Suponemos que esa información se encuentra en ese archivo comprimido. Así que lo vamos a instalar en nuestro ordenador. Para ello, primero ejecutamos la opción **filescan** de Volatility, que realiza un análisis en busca de archivos abiertos en el momento del volcado de memoria.

```
PS D:\volatility-master\volatility-master> py -2 vol.py -f memory.raw --profile=Win7SP1x64 filescan > filescan_salida.txt  
Volatility Foundation Volatility Framework 2.6.1
```

Figure 33: Uso de la opción filescan

Si buscamos entre la salida encontraremos el archivo y su dirección en memoria: 0x000000011faf9a0

```
0x000000011faf9a0      16      0 -W-r-- \Device\HarddiskVolume6\archivos-robados.7z
```

Figure 34: Archivo encontrado

Ahora recuperaremos el archivo con la opción **dumpfiles** de Volatility.

```
PS D:\volatility-master\volatility-master> py -2 vol.py -f memory.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000011faf9a0 --dump-dir .  
Volatility Foundation Volatility Framework 2.6.1
```

Figure 35: Uso de la opción dumpfiles

Como bien hemos mencionado en el apartado anterior, se encuentra protegido con contraseña y de momento no tenemos acceso a ella.

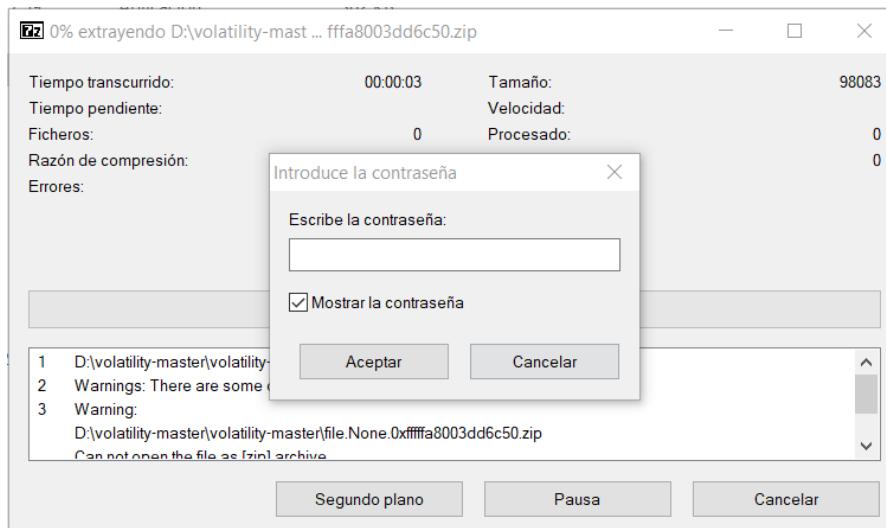


Figure 36: Archivo protegido con contraseña

Mirando en las carpetas del usuario kiddie, vemos que tiene instalado KeePass

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
[current folder]				2024-03-04 03:13:56 CET	2024-03-04 03:13:56 CET	2024-03-04 03:13:56 CET	2024-02-29 02:04:44 CET	56	Allocated	Allocated	unkno
[parent folder]				2024-02-29 02:04:45 CET	2024-02-29 02:04:45 CET	2024-02-29 02:04:45 CET	2024-02-29 02:04:44 CET	344	Allocated	Allocated	unkno
BurpSuite				2024-03-04 03:09:30 CET	2024-03-04 03:09:30 CET	2024-03-04 03:09:30 CET	2024-03-04 03:08:55 CET	56	Allocated	Allocated	unkno
Identities				2024-02-29 02:04:49 CET	2024-02-29 02:04:49 CET	2024-02-29 02:04:49 CET	2024-02-29 02:04:49 CET	312	Allocated	Allocated	unkno
KeePassXC				2024-03-04 03:19:01 CET	2024-03-04 03:19:01 CET	2024-03-04 03:19:01 CET	2024-03-04 03:13:56 CET	56	Allocated	Allocated	unkno
Media Center Programs				2011-04-12 11:12:11 CES	2024-02-29 02:04:45 CET	2024-02-29 02:04:44 CET	2024-02-29 02:04:44 CET	48	Allocated	Allocated	unkno
Microsoft				2024-03-04 03:04:52 CET	2024-03-04 03:04:52 CET	2024-03-04 03:04:52 CET	2024-02-29 02:04:44 CET	56	Allocated	Allocated	unkno
Mozilla				2024-02-29 02:25:32 CET	2024-02-29 02:25:32 CET	2024-02-29 02:25:32 CET	2024-02-29 02:25:32 CET	352	Allocated	Allocated	unkno
Telegram Desktop				2024-03-04 02:38:51 CET	2024-03-04 02:38:51 CET	2024-03-04 02:38:51 CET	2024-03-04 02:38:51 CET	584	Allocated	Allocated	unkno
Zoom				2024-03-04 03:02:35 CET	2024-03-04 03:02:35 CET	2024-03-04 03:02:35 CET	2024-03-04 03:01:11 CET	56	Allocated	Allocated	unkno

Figure 37: Muestra de que KeePass está instalado

Rebuscando en el disco dado, hemos encontrado un archivo llamado f0030720.kdbx, informándonos sabemos que es un archivo de KeePass que puede contener contraseñas importantes para la investigación, sin embargo, tambien se encuentra protegido.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
f0030720.kdbx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	842596352	Unallocated	Unallocated	unknown	/img_disk.img/vol_vo4/\$CarvedF
f0030720.kdbx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	842596352	Unallocated	Unallocated	unknown	/img_disk.img/vol_vo4/\$CarvedF
f0030592.txt				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	223	Unallocated	Unallocated	unknown	/img_disk.img/vol_vo4/\$CarvedF

Figure 38: Archivo de KeePass encontrado

Continuando la búsqueda en el pendrive, nos encontramos con un archivo denominado "keyfile.pdf". Es probable que este archivo sea el complemento utilizado como método adicional de autenticación, junto con una clave, para desbloquear las contraseñas almacenadas en KeePass.

Name	S	C	O	Modified Time	Change Time
keyfile.pdf				2024-03-12 12:09:23 CET	0000-00-00 00:00:00

Figure 39: Archivo keyfile.pdf encontrado

A lo largo de la investigación nos ha llamado la atención en Autopsy que el usuario anonymous, en la sección de pista de la contraseña, tiene puesto "la de siempre", lo que nos da a pensar que es una contraseña que reutiliza.

disk.img_1 Host Details	
Last Login:	2024-02-29 02:24:50 CET
Login Count:	2
Administrator:	True
Password Hint:	La de siempre
Password Fail Date:	2024-02-29 01:58:31 CET

Figure 40: Pista de la contraseña del usuario anonymous

Es por ello que vamos a tratar de crackear su contraseña para ver si puede tratarse de la misma del KeePass. Para esto usaremos la herramienta hashcat, disponible en kali linux. En concreto, hemos utilizado el siguiente comando:

```
hashcat -m 1000 -a 3 3bf8787c73729d592047a8ff57f181bd -1
/usr/share/hashcat/charsets/standard/Castilian/es-ES_ISO-8859-1.hcchr -2 ?l?d?u?s
-3 ?1?2 ?3?3?3?3?3?3 --potfile-disable
```

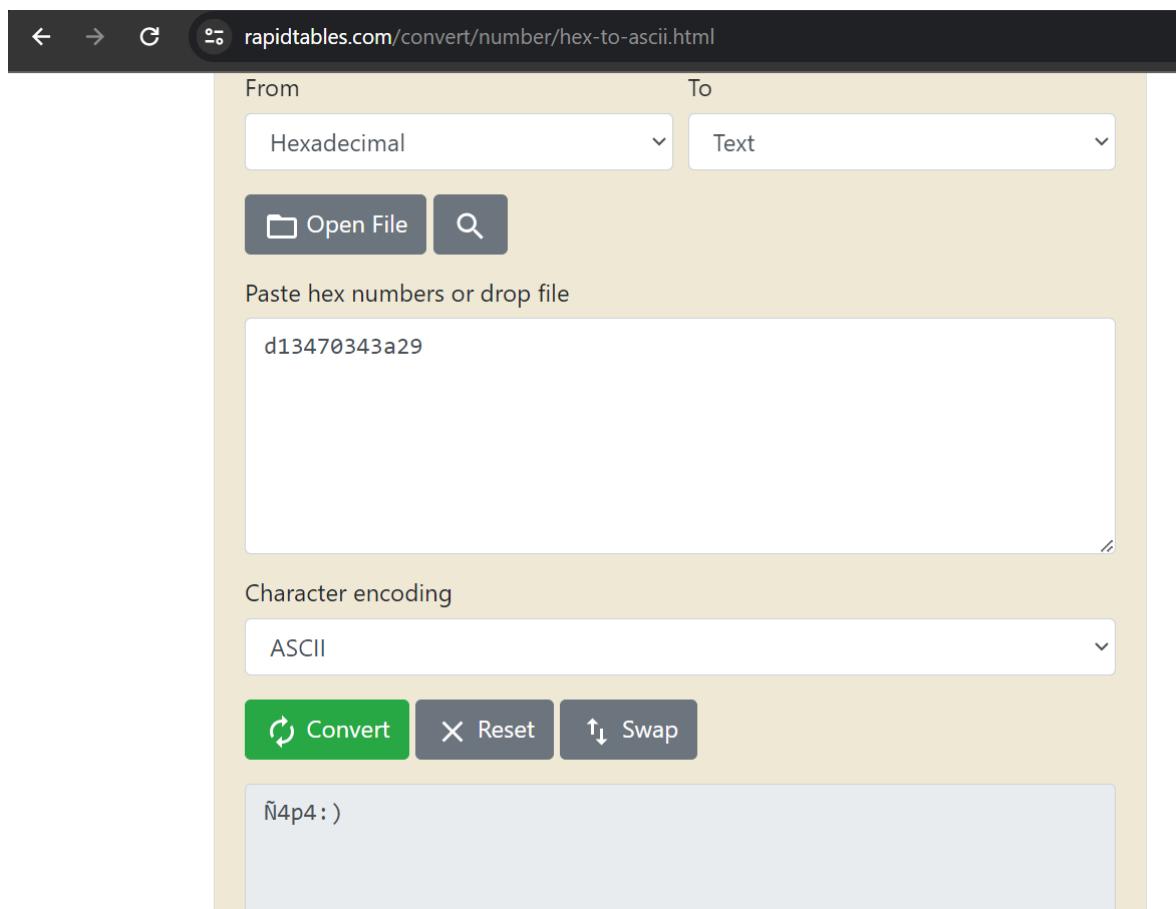
Este comando quiere decir: hashcat -m 1000 (Modo de hash: bcrypt) -a 3 (Tipo de ataque: combinación) 3bf8787c73729d592047a8ff57f181bd (Hash a descifrar) -1 /usr/share/hashcat/charsets/standard/Castilian/es-ES_ISO-8859-1.hcchr (Conjunto de caracteres en castellano) -2 ?l?d?u?s (Conjunto de caracteres incluyendo minúsculas, dígitos, mayúsculas y caracteres especiales) -3 ?1?2 ?3?3?3?3?3?3 (Conjunto de caracteres incluyendo caracteres específicos) --potfile-disable (Desactivar guardar hashes resueltos en un archivo de tabla hash).

En resumen, con este comando intentaremos descifrar el hash de la contraseña de anonymous usando un ataque de combinación. Para las combinaciones, incluiremos letras minúsculas, dígitos, letras mayúsculas, caracteres especiales y caracteres específicos.

```
3bf8787c73729d592047a8ff57f181bd:$HEX[d13470343a29]
Session.....: hashcat
Status.....: Cracked
Hash.Mode...: 1000 (NTLM)
Hash.Target.: 3bf8787c73729d592047a8ff57f181bd
Time.Started.: Wed May  8 13:21:19 2024 (7 mins, 53 secs)
Time.Estimated.: Wed May  8 13:29:12 2024 (0 secs)
Kernel.Feature.: Pure Kernel
Guess.Mask....: ?3?3?3?3?3?3 [6]
Guess.Charset...: -l /usr/share/hashcat/charsets/standard/Castilian/es-ES_ISO-8859-1.hcchr, -2 ?l?d?u?s, -3 ?1?2, -4 Undefine
d
Guess.Queue....: 1/1 (100.00%)
Speed.#1.....: 60025.9 kh/s (7.48ms) @ Accel:256 Loops:1024 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 29026300416/1870414552161 (1.55%)
Rejected.....: 0/29026300416 (0.00%)
Restore.Point...: 2355712/151807041 (1.55%)
Restore.Sub.#1.: Salt:0 Amplifier:2048-3072 Iteration:0-1024
Candidate.Engine.: Device Generator
Candidates.#1...: NS$H()1 → /\^f^%
Hardware.Mon.#1.: Util: 98%
Started: Wed May  8 13:21:14 2024
Stopped: Wed May  8 13:29:13 2024
```

Figure 41: Crackeo de la contraseña

Como podemos ver, hemos tenido éxito en el crackeo de la contraseña, que se nos devuelve en formato hexadecimal. Ahora simplemente tendremos que pasarlala a texto ASCII. Nosotros lo hemos hecho con la herramienta online [rapidtables](#)



The screenshot shows a web-based hex-to-ASCII converter. At the top, the URL is rapidtables.com/convert/number/hex-to-ascii.html. The interface has two dropdown menus: "From" set to "Hexadecimal" and "To" set to "Text". Below these are buttons for "Open File" and a search icon. A text input field contains the hex string "d13470343a29". A large text area below shows the converted ASCII output: "Ñ4p4:)". There are also buttons for "Convert" (green), "Reset" (grey), and "Swap" (grey).

Figure 42: Convirtiendo la contraseña a ASCII con rapidtables

Una vez convertida podemos ver que la contraseña es **Ñ4p4:)**. Vamos a probar a usarla en el KeyPass junto al keyfile.

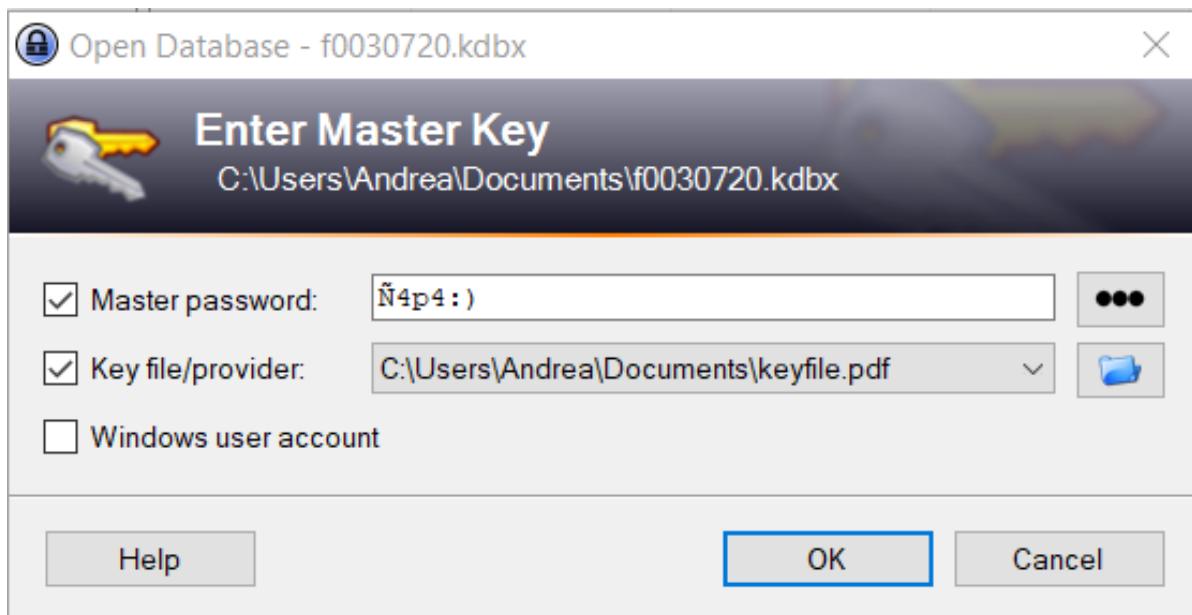


Figure 43: Uso de la contraseña junto al keyfile en KeePass

Como podemos ver, hemos tenido éxito. Una de las contraseñas que incluye este fichero es la de los ficheros robados, tras copiarla podemos ver que es **JfBop3sPeNU6i1AgCzJp**. Además, obtuvimos otra contraseña titulada Pruebas, NX47FNX04c, que es la contraseña para acceder al contenido de la siguiente url: <https://pastebin.com/hLi9xadZ>

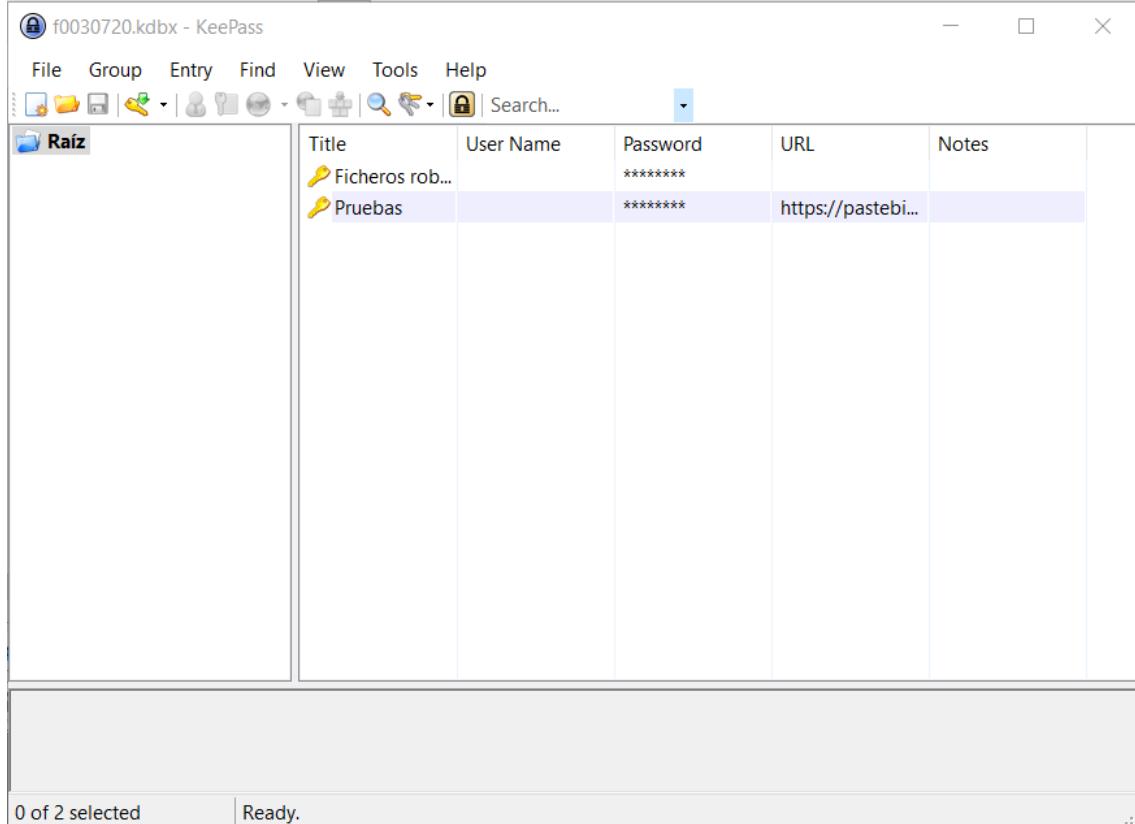


Figure 44: Contraseñas en KeePass

Tras obtener la contraseña del zip pudimos acceder a los archivos "Estudiantes.xlsx" y "Examen.pdf". En el primer archivo se nos muestran los nombres de los estudiantes de la asignatura. El número de alumnos que la cursan es 19.

	A	B	C	D	E	F	G
1	DNI	Correo Electrónico	Nombre	Primer apellido	Segundo apellido	Nota de prácticas	Grupo de prácticas
2	12345678A	12345678@acme-university.pri	Joaquín	López	Gil	7,5	A
3	23456789B	23456789@acme-university.pri	Laura	González	Pérez	6,8	A
4	34567890C	34567890@acme-university.pri	Fernando	Rodríguez	García	8,2	A
5	45678901D	45678901@acme-university.pri	Ana	Fernández	Santos	5,4	A
6	56789012E	56789012@acme-university.pri	Javier	Sánchez	Ríos	9,1	A
7	67890123F	67890123@acme-university.pri	Sofía	García	Castro	7,9	B
8	78901234G	78901234@acme-university.pri	Carlos	Pérez	Ruiz	6,7	B
9	89012345H	89012345@acme-university.pri	Marta	Fernández	Fernández	8,3	B
10	90123456I	90123456@acme-university.pri	Paula	Álvarez	Gómez	4,6	B
11	01234567J	01234567@acme-university.pri	Luis	Romero	Blanco	9,2	B
12	12345678K	12345678@acme-university.pri	Irene	Martínez	Molina	7,1	C
13	23456789L	23456789@acme-university.pri	David	Ortiz	Soto	6,9	C
14	34567890M	34567890@acme-university.pri	Nuria	Fernández	Ruiz	8,7	C
15	45678901N	45678901@acme-university.pri	Manuel	Díaz	García	5,8	C
16	56789012O	56789012@acme-university.pri	Leire	Santos	Martín	9,3	C
17	67890123P	67890123@acme-university.pri	Jaime	González	Gil	7,2	D
18	78901234Q	78901234@acme-university.pri	Patricia	García	Pérez	6,4	D
19	89012345R	89012345@acme-university.pri	Mario	Rivera	Sánchez	8,1	D

Figure 45: Listado de alumnos de la asignatura

En cuanto a la asignatura, se trata de "Investigaciones Forenses Avanzadas". El contenido es un examen para el día 2 de mayo.

Investigaciones Forenses Avanzadas

Examen del 2 de mayo

Instrucciones: Elige la respuesta correcta y márcala con una "X" en la casilla correspondiente.

1. ¿Qué es el análisis forense informático?

- Un método para acceder a sistemas informáticos sin autorización.
- Una técnica que se utiliza para recopilar y analizar evidencia digital en una investigación.
- Un método para eliminar todo rastro de actividad digital en un equipo.

2. ¿Qué es un hash MD5?

- Una función criptográfica que se utiliza para verificar la integridad de un archivo.
- Una técnica para acceder a sistemas informáticos sin ser detectado.
- Un protocolo de red utilizado para transferir archivos.

3. ¿Qué es el registro de eventos de Windows?

- Un archivo de registro que se utiliza para almacenar contraseñas.
- Un archivo de registro que almacena información sobre la actividad del sistema operativo y las aplicaciones instaladas.
- Una herramienta utilizada para limpiar el historial de navegación web.

4. ¿Qué es la esteganografía?

- Una técnica utilizada para ocultar información dentro de un archivo, como una imagen o un audio.

Figure 46: Examen de la asignatura

Si vemos las propiedades del archivo Estudiantes.xlsx podemos encontrar el autor del mismo, **Faustino Mateo Reina**, que debe ser uno de los profesores que imparten la materia. Si la parte práctica de la asignatura la imparte un profesor y la parte teórica otro, este señor seguramente sea el profesor de la parte práctica.

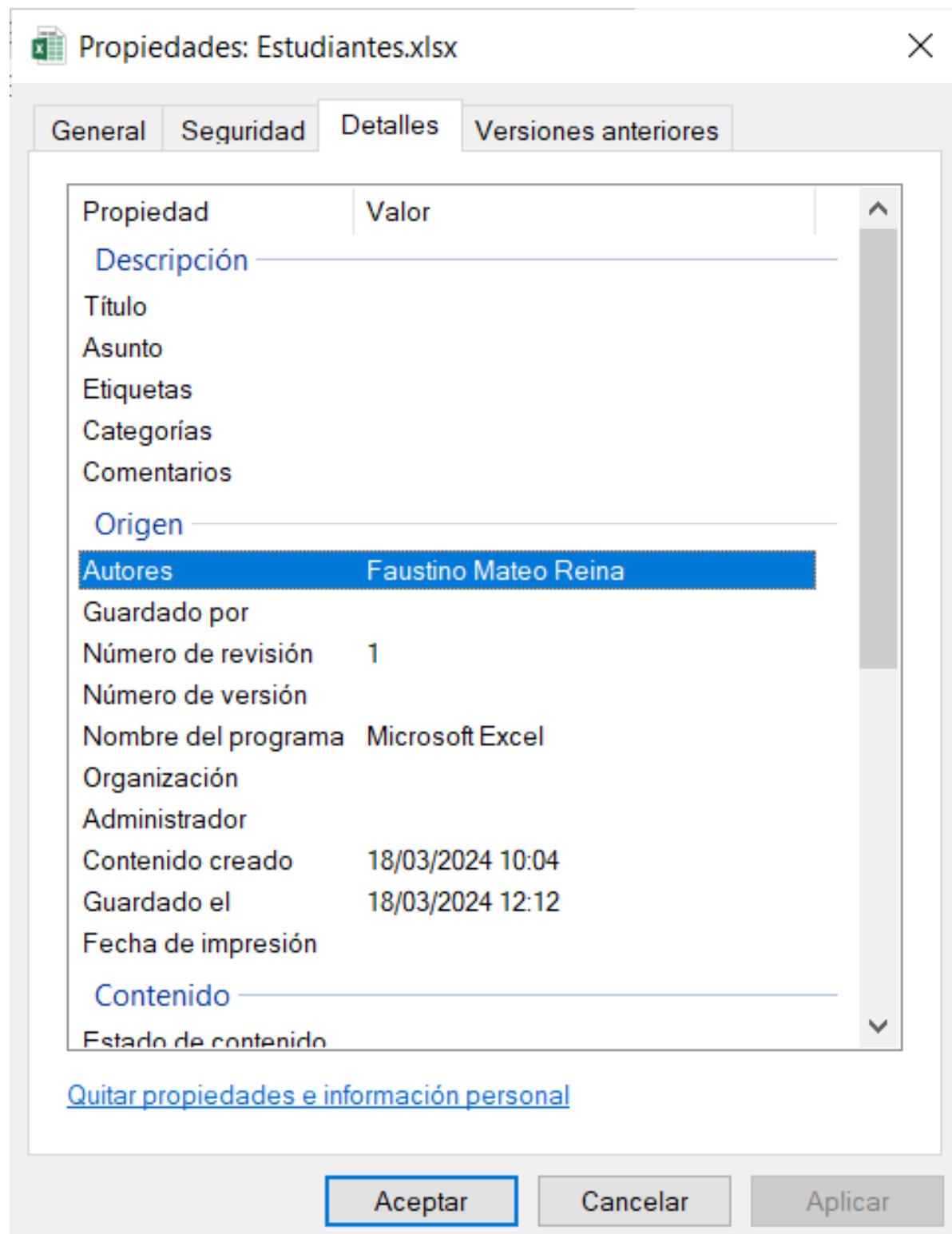


Figure 47: Propiedades del archivo Estudiantes.xlsx

Si consultamos los metadatos del archivo Examen.pdf con alguna herramienta nos sale el nombre del autor, Juan Antonio Cuadrado Domingo, este profesor tal vez imparte la parte teórica de la asignatura. Para sacar esta información hemos usado una herramienta online llamada [Groupdocs](#)

	Metadata
File Format Info	
FILEFORMAT	Pdf
MIMETYPE	application/pdf
PDFVERSION	1.6
PDF Properties	
AUTHOR	Juan Antonio Cuadrado Domi...
CREATIONDATE	10-04-2023 17:00:17
CREATOR	Word
MODDATE	18-03-2024 12:50:56
PRODUCER	Microsoft Writer
TITLE	Examen del 2 de mayo
Document Statistics	
CHARACTERCOUNT	3070
PAGECOUNT	2
WORDCOUNT	442
Xmp	
DC:CREATOR	[Juan Antonio Cuadrado Domi...

Figure 48: Metadatos del archivo Examen.pdf

3.1.7

Para este apartado hemos usado la opción **netscan** de Volatility, que nos da información relacionada con las conexiones de red que guarda el volcado de memoria. Así podremos ver la actividad de red en el sistema durante el momento en que se realizó el volcado.

Analizando la salida podemos llegar a la conclusión de que la IP de la máquina víctima es **172.20.20.2**, ya que es la única que nos muestra con el puerto 21, correspondiente a FTP, el servicio que aprovechó para robar previamente la información el atacante.

Offset(P)	Proto	Local Address	Foreign Address	State	Pid	Owner	Created
0x2b7c9d0	TCPv4	-:26520	172.20.20.2:21	CLOSED	1808	ftp.exe	
0x2c51cf0	TCPv4	-:26500	-:443	CLOSED	1180	firefox.exe	
0x2cb0200	TCPv4	-:26481	-:443	CLOSED	1180	firefox.exe	
0x2cd2350	TCPv4	-:26456	0.1.77.3:443	CLOSED	1180	firefox.exe	
0x37be7740	UDPv4	0.0.0.0:50195	*:*	*	1180	firefox.exe	2024-03-21 09:36:18 UTC+0000
0x11cb90010	UDPv4	0.0.0.0:62318	*:*	*	1180	firefox.exe	2024-03-21 09:36:18 UTC+0000
0x11cc76bc0	TCPv4	0.0.0.0:1028	0.0.0.0:0	LISTENING	516	services.exe	
0x11cc7d010	TCPv6	0.0.0.0:445	0.0.0.0:0	LISTENING	4	System	
0x11cef7d40	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	784	svchost.exe	
0x11cef7d40	TCPv6	:::135	:::0	LISTENING	784	svchost.exe	
0x11cef9ce0	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	784	svchost.exe	
0x11cf2b4e0	TCPv4	0.0.0.0:1026	0.0.0.0:0	LISTENING	856	svchost.exe	
0x11cf2ca90	TCPv4	0.0.0.0:1026	0.0.0.0:0	LISTENING	856	svchost.exe	
0x11cf2ca90	TCPv6	:::1026	:::0	LISTENING	856	svchost.exe	
0x11cf86640	TCPv4	0.0.0.0:1029	0.0.0.0:0	LISTENING	536	lsass.exe	
0x11fcf18e0	TCPv4	0.0.0.0:1029	0.0.0.0:0	LISTENING	536	lsass.exe	
0x11fcf18e0	TCPv6	:::1029	:::0	LISTENING	536	lsass.exe	
0x11caa1a90	TCPv4	-:26487	-:443	CLOSED	1180	firefox.exe	
0x11cb06700	TCPv4	-:1031	0.0.0.0:1030	CLOSED	1180	firefox.exe	
0x11cb3ca10	TCPv4	-:29698	-:443	CLOSED	1180	firefox.exe	
0x11cbabb90	TCPv4	:::0	104.48.73.4:0	CLOSED	1180	firefox.exe	
0x11c95840	TCPv6	:::0	826:8406:80fa:ffff:a808:8004:80fa:ffff::0	CLOSED	1	►P]♦?????	
0x11cef6390	TCPv4	:::0	120.84.142.6:0	CLOSED	1	►P]♦?????	
0x11cefbcf0	TCPv4	:::0	120.84.142.6:0	CLOSED	1	►P]♦?????	
0x11cf74270	TCPv4	-:58888	-:443	CLOSED	1180	firefox.exe	
0x11d394d10	UDPv4	127.0.0.1:55751	*:*	*	2120	svchost.exe	2024-03-21 09:01:08 UTC+0000
0x11d36bb40	TCPv4	0.0.0.0:1028	0.0.0.0:0	LISTENING	516	services.exe	
0x11d36bb40	TCPv6	:::1028	:::0	LISTENING	516	services.exe	
0x11d393470	TCPv4	0.0.0.0:1027	0.0.0.0:0	LISTENING	980	svchost.exe	
0x11d394480	TCPv4	0.0.0.0:1027	0.0.0.0:0	LISTENING	980	svchost.exe	
0x11d394480	TCPv6	:::1027	:::0	LISTENING	980	svchost.exe	
0x11d03f930	TCPv4	:::0	104.48.73.4:0	CLOSED	1180	firefox.exe	
0x11d3e6cf0	TCPv4	-:1030	0.0.0.0:1031	CLOSED	1180	firefox.exe	
0x11e935b40	TCPv4	0.0.0.0:1025	0.0.0.0:0	LISTENING	412	wininit.exe	
0x11eda0ad0	TCPv4	0.0.0.0:1025	0.0.0.0:0	LISTENING	412	wininit.exe	
0x11eda0ad0	TCPv6	:::1025	:::0	LISTENING	412	wininit.exe	
0x11e9703d0	TCPv4	-:26499	188.36.200.0:443	CLOSED	1180	firefox.exe	
0x11f2a72f0	UDPv4	0.0.0.0:51438	*:*	*	1180	firefox.exe	2024-03-21 09:30:25 UTC+0000
0x11f5a9ec0	UDPv4	0.0.0.0:50194	*:*	*	1180	firefox.exe	2024-03-21 09:36:18 UTC+0000
0x11f5e1ec0	UDPv4	0.0.0.0:64230	*:*	*	1180	firefox.exe	2024-03-21 09:36:50 UTC+0000
0x11f5f0010	UDPv4	0.0.0.0:5355	*:*	*	1124	svchost.exe	2024-03-21 10:01:05 UTC+0000
0x11f60b010	UDPv4	0.0.0.0:0	*:*	*	724	VBoxService.exe	2024-03-21 10:03:39 UTC+0000
0x11f7aca0	UDPv4	0.0.0.0:56162	*:*	*	1180	firefox.exe	2024-03-21 09:36:17 UTC+0000
0x11ee3d700	TCPv4	-:26402	0.3.12.3:21	CLOSED	6708	mscorsvw.exe	
0x11ef1d010	TCPv4	-:26534	172.20.20.2:20	CLOSED	1808	ftp.exe	
0x11f013cf0	TCPv4	-:26517	34.128.208.123:443	CLOSED	1180	firefox.exe	
0x11f164010	TCPv4	-:26524	192.228.79.201:443	CLOSED	1180	firefox.exe	
0x11f16d350	TCPv4	-:26490	-:443	CLOSED	1180	firefox.exe	
0x11f202290	TCPv4	-:26498	8.72.137.0:443	CLOSED	1180	firefox.exe	

Figure 49: Uso de la opción netscan

Siguiendo con el análisis de la salida, podemos ver que la única otra IP de la red es **172.20.20.101**, por lo que podemos decir que esa sería la IP del atacante.

0x11f29f010	TCPv4	-:26509	-:443	CLOSED	1180	firefox.exe
0x11f2a9cf0	TCPv4	-:26533	172.20.20.2:20	CLOSED	1808	ftp.exe
0x11f2d19e0	TCPv4	-:26514	-:443	CLOSED	1180	firefox.exe
0x11f392bf0	TCPv4	-:26523	224.0.0.252:443	CLOSED	1180	firefox.exe
0x11f3f1010	TCPv4	-:26474	0.3.12.3:21	CLOSED	6708	mscorsvw.exe
0x11f49dc30	TCPv4	-:29915	-:443	CLOSED	1180	firefox.exe
0x11f650ba0	TCPv4	-:26513	194.226.130.226:443	CLOSED	1180	firefox.exe
0x11f7564e0	TCPv4	-:26495	-:443	CLOSED	1180	firefox.exe
0x11f7c2530	TCPv4	-:58994	59.207.73.15:443	CLOSED	1180	firefox.exe
0x11f86bec0	UDPv4	0.0.0.0:0	*:*		724	VBoxService.exe
0x11fa07700	UDPv4	0.0.0.0:5355	*:*		1124	svchost.exe
0x11fa07700	UDPv6	:::5355	*:*		1124	svchost.exe
0x11fb4d9c0	UDPv4	0.0.0.0:53301	*:*		1180	firefox.exe
0x11fb9a5c0	UDPv4	0.0.0.0:50196	*:*		1180	firefox.exe
0x11fc44ec0	UDPv4	0.0.0.0:0	*:*		1124	svchost.exe
0x11fc44ec0	UDPv6	:::0	*:*		1124	svchost.exe
0x11fc49610	UDPv4	127.0.0.1:1900	*:*		2120	svchost.exe
0x11fc76e00	UDPv4	18.0.2.15:138	*:*		4	System
0x11fc8ee20	UDPv4	172.20.20.101:138	*:*		4	System
0x11fcab2d0	UDPv6	fe80::90b3:d51d:d003:7775:1900	*:*		2120	svchost.exe
0x11fcc0d70	UDPv4	172.20.20.101:1900	*:*		2120	svchost.exe
0x11fcc1890	UDPv6	::1:1900	*:*		2120	svchost.exe
0x11feb5bf0	UDPv4	18.0.2.15:1900	*:*		2120	svchost.exe
0x11ff0d9c0	UDPv6	fe80::d519:c157:9a80:3ff8:1900	*:*		2120	svchost.exe
0x11ff9d4c0	UDPv6	::1:55750	*:*		2120	svchost.exe
0x11ffa2c40	UDPv4	172.20.20.101:137	*:*		4	System
0x11ffad2c0	UDPv4	18.0.2.15:137	*:*		4	System
0x11ff623c0	TCPv4	18.0.2.15:139	0.0.0.0:0	LISTENING	4	System
0x11ff85350	TCPv4	172.20.20.101:139	0.0.0.0:0	LISTENING	4	System
0x11ff8cf380	TCPv4	-:26502	-:443	CLOSED	1180	firefox.exe
0x11f902940	TCPv4	-:26480	-:443	CLOSED	1180	firefox.exe
0x11f9ec5a0	TCPv4	-:26527	34.117.188.166:443	CLOSED	1180	firefox.exe
0x11f9f6010	TCPv4	-:29626	-:443	CLOSED	1180	firefox.exe
0x11fa3f010	TCPv4	-:26516	-:443	CLOSED	1180	firefox.exe
0x11fc20cf0	TCPv4	-:26531	174.137.133.49:443	CLOSED	1180	firefox.exe
0x11fc97cf0	TCPv4	-:26515	104.19.231.122:443	CLOSED	1180	firefox.exe
0x11fe7a010	TCPv4	-:1032	0.0.0.0:1033	CLOSED	2212	firefox.exe
0x11fe93540	TCPv4	-:1033	0.0.0.0:1032	CLOSED	2212	firefox.exe

Figure 50: Uso de la opción netscan

3.1.8

Como hemos visto anteriormente, el atacante se aprovechó de una vulnerabilidad FTP para robar la información. Esto lo podemos ver gracias a la opción **consoles** de Volatility.

```
Cmd #0 @ 0xba730: "C:\Program Files (x86)\Nmap\nmap.exe" --unprivileged -sV -T5 -p21 --script="*ftp*" acme-university.pri
Cmd #1 @ 0xa6540: ftp acme-university.pri
```

Figure 51: Aprovechamiento de la vulnerabilidad FTP

Además, con esa opción, podemos recuperar información sobre las consolas que estaban abiertas en el sistema en el momento del volcado de memoria.

```

PS D:\volatility-master\volatility-master> py -2 vol.py -f memory.raw --profile=Win7SP1x64 consoles
Volatility Foundation Volatility Framework 2.6.1
*****
ConsoleProcess: conhost.exe Pid: 6676
Console: 0xff286200 CommandHistorySize: 50
HistoryBufferCount: 4 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\System32\cmd.exe
Title: C:\Windows\System32\cmd.exe
AttachedProcess: cmd.exe Pid: 5132 Handle: 0x64
----
CommandHistory: 0xbef0 Application: 7z.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
----
CommandHistory: 0xbbee0 Application: ftp.exe Flags: Reset
CommandCount: 5 LastAdded: 4 LastDisplayed: 4
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
Cmd #0 at 0xb51b0: anonymous
Cmd #1 at 0xb3a40: ls
Cmd #2 at 0xa6500: get Estudiantes.xlsx
Cmd #3 at 0xb2510: get Examen.pdf
Cmd #4 at 0xb51d0: quit
----
CommandHistory: 0xbac20 Application: nmap.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
----
CommandHistory: 0xb6540 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 3 LastAdded: 2 LastDisplayed: 2
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x64
Cmd #0 at 0xba730: "C:\Program Files (x86)\Nmap\nmap.exe" --unprivileged -sV -T5 -p21 --script="*ftp*" acme-university.pri
Cmd #1 at 0xa6540: ftp acme-university.pri
Cmd #2 at 0xbfcfd0: "C:\Program Files\7-Zip\7z.exe" a archivos-robaros.7z Estudiantes.xlsx Examen.pdf -p
----
Screen 0x93000 X:80 Y:300
Dump:
Microsoft Windows [Versi?n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

E:\>"C:\Program Files (x86)\Nmap\nmap.exe" --unprivileged -sV -T5 -p21 --script=
"*ftp*" acme-university.pri
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-21 10:19 Hora est?ndar romanc
e
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for acme-university.pri (172.20.20.86)
Host is up (0.00s latency).

```

Figure 52: Uso de la opción consoles

```

PORT      STATE SERVICE      VERSION
21/tcp    open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 611.48 seconds

E:\>"C:\Program Files (x86)\Nmap\nmap.exe" --unprivileged -sV -T5 -p21 --script=**ftp* acme-university.pri
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-21 10:30 Hora est?ndar romanc
e
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
NSE: [ftp-brute] usernames: Time limit 3m00s exceeded.
NSE: [ftp-brute] usernames: Time limit 3m00s exceeded.
NSE: [ftp-brute] passwords: Time limit 3m00s exceeded.
Nmap scan report for acme-university.pri (172.20.20.86)
Host is up (0.00s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.5
|_ ftp-brute:
|   Accounts: No valid accounts found
|_ Statistics: Performed 922 guesses in 183 seconds, average tps: 4.3
|_ ftp-syst:
|   STAT:
|     FTP server status:
|       Connected to ::ffff:172.20.20.101
|       Logged in as ftp
|       TYPE: ASCII
|       No session bandwidth limit
|       Session timeout in seconds is 300
|       Control connection is plain text
|       Data connections will be plain text
|       At session startup, client count was 4
|       vsFTPD 3.0.5 - secure, fast, stable
|_End of status
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rwxr-xr-x  1 0          0          11010 Mar 19 11:55 Estudiantes.xlsx
|_ -rwxr-xr-x  1 0          0          87073 Mar 19 11:55 Examen.pdf
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 200.56 seconds

E:\>"C:\Program Files (x86)\Nmap\nmap.exe" --unprivileged -sV -T5 -p21 --script=**ftp* acme-university.pri

E:\>ftp acme-university.pri
Conectado a acme-university.pri.
220 (vsFTPD 3.0.5)

```

Figure 53: Uso de la opción consoles

La salida nos muestra como claramente se aprovechó de una vulnerabilidad en el servicio FTP para descargarse los archivos de su interés. Esto lo hizo gracias a un usuario llamado **anonymous**, que permite el acceso en las versiones vulnerables de FTP. Una vez dentro, robó la información.

3.1.9

Cuando ejecutamos la opción **consoles** de Volatility, vimos que el usuario usó la herramienta nmap.

```
E:\>"C:\Program Files (x86)\Nmap\nmap.exe" --unprivileged -sV -T5 -p21 --script=**ftp** acme-university.pri
```

Figure 54: Uso de la opción consoles

Miramos los procesos en ejecución del sistema con la opción pslist para ver si hay alguna herramienta de hacking ejecutándose. Sin embargo, no encontramos nada relevante.

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0xfffffa800316d2040	System	4	0	93	649	-	-	2024-03-21 08:59:30 UTC+0000	
0xfffffa800458350	smsvc.exe	276	4	2	30	-	-	2024-03-21 08:59:30 UTC+0000	
0xfffffa8004706060	crssrv.exe	368	356	9	379	0	0	2024-03-21 08:59:35 UTC+0000	
0xfffffa80067b720b	wininit.exe	412	356	3	77	0	0	2024-03-21 08:59:35 UTC+0000	
0xfffffa80067b5a50	crssrv.exe	432	420	12	301	1	0	2024-03-21 08:59:35 UTC+0000	
0xfffffa8006526900	winlogon.exe	484	420	3	108	1	0	2024-03-21 08:59:35 UTC+0000	
0xfffffa8006533910	services.exe	516	412	9	197	0	0	2024-03-21 08:59:35 UTC+0000	
0xfffffa8006542400	lsass.exe	536	412	8	571	0	0	2024-03-21 08:59:36 UTC+0000	
0xfffffa8006541300	lsass.exe	544	412	13	345	0	0	2024-03-21 08:59:36 UTC+0000	
0xfffffa8004190e30	svchost.exe	660	16	10	346	0	0	2024-03-21 08:59:36 UTC+0000	
0xfffffa80065ce30	VBoxService.exe	724	516	13	115	0	0	2024-03-21 08:59:36 UTC+0000	
0xfffffa80065e470	svchost.exe	784	516	6	261	0	0	2024-03-21 08:59:36 UTC+0000	
0xfffffa8004121b30	svchost.exe	856	516	18	496	0	0	2024-03-21 08:59:36 UTC+0000	
0xfffffa80065b2890	svchost.exe	924	516	20	519	0	0	2024-03-21 08:59:36 UTC+0000	
0xfffffa800655230	svchost.exe	988	516	27	1077	0	0	2024-03-21 08:59:37 UTC+0000	
0xfffffa80065a9490	svchost.exe	888	516	14	327	0	0	2024-03-21 08:59:37 UTC+0000	
0xfffffa80065dd310	svchost.exe	1124	516	15	474	0	0	2024-03-21 08:59:37 UTC+0000	
0xfffffa8006a15430	spools.exe	1256	516	12	271	0	0	2024-03-21 08:59:38 UTC+0000	
0xfffffa8006a3e30	svchost.exe	1297	516	17	311	0	0	2024-03-21 08:59:38 UTC+0000	
0xfffffa8006b330	svchost.exe	1520	516	8	159	1	0	2024-03-21 09:00:00 UTC+0000	
0xfffffa800653050	dmoc.exe	1988	516	3	301	1	0	2024-03-21 09:00:00 UTC+0000	
0xfffffa80065b2920	explorer.exe	2012	1988	24	902	1	0	2024-03-21 09:00:00 UTC+0000	
0xfffffa8006c4d6a0	VBoxTray.exe	1448	2012	13	140	1	0	2024-03-21 09:00:00 UTC+0000	
0xfffffa80065ac480	SearchIndexer.	1152	516	13	748	0	0	2024-03-21 09:00:06 UTC+0000	
0xfffffa8006559060	firefox.exe	1188	1892	0	-	1	0	2024-03-21 09:00:35 UTC+0000	2024-03-21 09:37:13 UTC+0000
0xfffffa8006d17630	svchost.exe	2128	516	9	204	0	0	2024-03-21 09:00:37 UTC+0000	
0xfffffa8003c52180	spsvc.exe	3328	516	4	158	0	0	2024-03-21 09:01:39 UTC+0000	
0xfffffa8003c5b30	svchost.exe	3364	516	8	306	0	0	2024-03-21 09:01:39 UTC+0000	
0xfffffa80048d0660	notepad.exe	7924	3284	1	62	1	0	2024-03-21 09:11:15 UTC+0000	
0xfffffa80045cc430	WUDHost.exe	5588	924	9	245	0	0	2024-03-21 09:15:49 UTC+0000	
0xfffffa8005146000	cmed.exe	5132	2012	1	21	1	0	2024-03-21 09:17:24 UTC+0000	
0xfffffa800453d10	Dumpit.exe	6676	432	53	53	1	0	2024-03-21 09:18:10 UTC+0000	
0xfffffa800453d10	Dumpit.exe	5669	2012	2	46	1	1	2024-03-21 09:42:20 UTC+0000	
0xfffffa8003b7e060	host.exe	4864	432	2	54	1	0	2024-03-21 09:42:20 UTC+0000	

Figure 55: Uso de la opción pslist

Realizamos también un psscan en busca de procesos que ya no están en la lista de procesos activos pero tampoco encontramos uso de ninguna nueva herramienta.

Offset(V)	Name	PID	PPID	PDW	Time created	Time exited
0x00000000002c9ab0	WmiPrvSE.exe	7344	668	0x00000000000014160000	2024-03-21 09:41:18 UTC+0000	2024-03-21 09:37:11 UTC+0000
0x00000000002c9bd30	firefox.exe	4428	1188	0x00000000000034640000	2024-03-21 09:21:41 UTC+0000	
0x00000000002d4f30	firefox.exe	8180	1188	0x00000000000035570000	2024-03-21 09:21:38 UTC+0000	2024-03-21 09:37:11 UTC+0000
0x00000000002d4f30	firefox.exe	4266	1188	0x00000000000071300000	2024-03-21 09:21:38 UTC+0000	2024-03-21 09:37:11 UTC+0000
0x00000000002d4f30	firefox.exe	4224	1188	0x00000000000032730000	2024-03-21 09:21:33 UTC+0000	2024-03-21 09:37:11 UTC+0000
0x0000000000702040	System	4	0	0x00000000000018700000	2024-03-21 08:59:38 UTC+0000	
0x0000000000702040	firefox.exe	2212	1188	0x000000000000841fdb0000	2024-03-21 09:00:37 UTC+0000	2024-03-21 09:37:13 UTC+0000
0x0000000000702040	firefox.exe	1148	1188	0x00000000000025dd0000	2024-03-21 09:32:21 UTC+0000	2024-03-21 09:37:10 UTC+0000
0x0000000000702040	fireFox.exe	1148	2012	0x000000000000f9a90000	2024-03-21 09:00:00 UTC+0000	
0x0000000000702040	svchost.exe	2128	1188	0x000000000000687f0000	2024-03-21 09:00:37 UTC+0000	
0x0000000000702040	svchost.exe	6792	1188	0x000000000000549e0000	2024-03-21 09:00:35 UTC+0000	2024-03-21 09:37:04 UTC+0000
0x0000000000702040	ping.exe	7148	1188	0x00000000000030770000	2024-03-21 09:37:12 UTC+0000	2024-03-21 09:37:15 UTC+0000
0x0000000000702040	firefox.exe	3080	1188	0x000000000000a3530000	2024-03-21 09:21:38 UTC+0000	2024-03-21 09:37:11 UTC+0000
0x0000000000702040	firefox.exe	6024	1188	0x0000000000003273f0000	2024-03-21 09:21:40 UTC+0000	2024-03-21 09:37:11 UTC+0000
0x0000000000702040	host.exe	6676	432	0x0000000000d3110000	2024-03-21 09:18:24 UTC+0000	
0x0000000000702040	spoolsv.exe	1256	516	0x000000000047f030000	2024-03-21 08:59:38 UTC+0000	
0x0000000000702040	svchost.exe	1292	516	0x000000000048920000	2024-03-21 08:59:38 UTC+0000	
0x0000000000702040	svchost.exe	1360	516	0x000000000049000000	2024-03-21 09:00:35 UTC+0000	
0x0000000000702040	firefox.exe	1180	1188	0x0000000000003a5e0000	2024-03-21 09:00:35 UTC+0000	2024-03-21 09:37:13 UTC+0000
0x0000000000702040	fireFox.exe	1180	1188	0x000000000000277f0000	2024-03-21 09:00:00 UTC+0000	
0x0000000000702040	taskhost.exe	1920	516	0x000000000000421760000	2024-03-21 09:00:00 UTC+0000	
0x0000000000702040	wlansvc.exe	484	428	0x00000000000058560000	2024-03-21 08:59:35 UTC+0000	
0x0000000000702040	services.exe	516	412	0x00000000000087f00000	2024-03-21 08:59:35 UTC+0000	
0x0000000000702040	lsass.exe	536	412	0x00000000000059310000	2024-03-21 08:59:36 UTC+0000	
0x0000000000702040	VMwareTray.exe	7224	516	0x00000000000055690000	2024-03-21 08:59:36 UTC+0000	
0x0000000000702040	audiodg.exe	784	516	0x00000000000055690000	2024-03-21 08:59:36 UTC+0000	
0x0000000000702040	svchost.exe	924	516	0x00000000000052b10000	2024-03-21 08:59:36 UTC+0000	
0x0000000000702040	firefox.exe	5724	1188	0x00000000000001c370000	2024-03-21 09:21:17 UTC+0000	2024-03-21 09:37:09 UTC+0000
0x0000000000702040	audiodg.exe	320	516	0x00000000000050130000	2024-03-21 08:59:37 UTC+0000	2024-03-21 09:47:02 UTC+0000
0x0000000000702040	svchost.exe	888	516	0x0000000000004e5c0000	2024-03-21 08:59:37 UTC+0000	
0x0000000000702040	lsm.exe	1124	516	0x000000000000549e0000	2024-03-21 08:59:37 UTC+0000	
0x0000000000702040	wininit.exe	412	516	0x00000000000054d40000	2024-03-21 08:59:35 UTC+0000	
0x0000000000702040	svrsv.exe	432	420	0x00000000000055900000	2024-03-21 08:59:35 UTC+0000	
0x0000000000702040	SearchIndexer.	1152	516	0x00000000000094c50000	2024-03-21 09:00:06 UTC+0000	
0x0000000000702040	svchost.exe	856	516	0x00000000000057a00000	2024-03-21 08:59:36 UTC+0000	
0x0000000000702040	svchost.exe	660	516	0x00000000000057490000	2024-03-21 08:59:36 UTC+0000	
0x0000000000702040	lsm.exe	544	412	0x00000000000055920000	2024-03-21 08:59:36 UTC+0000	
0x0000000000702040	fireFox.exe	7505	1188	0x00000000000001f3cc430	2024-03-21 08:59:33 UTC+0000	2024-03-21 09:37:10 UTC+0000
0x0000000000702040	services.exe	576	516	0x00000000000056000000	2024-03-21 08:59:33 UTC+0000	
0x0000000000702040	sethc.exe	3204	0x00000000000023427000	2024-03-21 09:11:15 UTC+0000		
0x0000000000702040	notepad.exe	7524	1188	0x00000000000001f06710000	2024-03-21 09:22:11 UTC+0000	2024-03-21 09:37:11 UTC+0000
0x0000000000702040	firefox.exe	7408	1188	0x00000000000001f06710000	2024-03-21 09:22:11 UTC+0000	
0x0000000000702040	Dumpit.exe	5660	2012	0x000000000000198a0000	2024-03-21 09:42:20 UTC+0000	
0x0000000000702040	firefox.exe	2912	1188	0x00000000000019850000	2024-03-21 09:21:24 UTC+0000	2024-03-21 09:37:11 UTC+0000
0x0000000000702040	svrsv.exe	368	516	0x000000000000503e0000	2024-03-21 08:59:35 UTC+0000	
0x0000000000702040	lsm.exe	612	516	0x000000000000503f0000	2024-03-21 08:59:35 UTC+0000	
0x0000000000702040	fireFox.exe	5588	324	0x00000000000001f3fd780	2024-03-21 09:15:49 UTC+0000	
0x0000000000702040	fireFox.exe	6536	1188	0x00000000000001f3fd780	2024-03-21 09:22:01 UTC+0000	2024-03-21 09:37:11 UTC+0000
0x0000000000702040	fireFox.exe	7200	1188	0x00000000000001f6f15b30	2024-03-21 09:21:37 UTC+0000	2024-03-21 09:37:11 UTC+0000

Figure 56: Uso de la opción psscan

En las carpetas de kiddie encontramos la herramienta BurpSuite, dedicada al pentesting, pero puede usarse para malos fines como pie de ser la realización de diversos ataques: fuerza bruta, explotación de vulnerabilidades,...

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Know
📁 [current folder]				2024-03-04 03:13:56 CET	2024-03-04 03:13:56 CET	2024-03-04 03:13:56 CET	2024-02-29 02:04:44 CET	56	Allocated	Allocated	unkno
📁 [parent folder]				2024-02-29 02:04:45 CET	2024-02-29 02:04:45 CET	2024-02-29 02:04:45 CET	2024-02-29 02:04:44 CET	344	Allocated	Allocated	unkno
📁 BurpSuite				2024-03-04 03:09:30 CET	2024-03-04 03:09:30 CET	2024-03-04 03:09:30 CET	2024-03-04 03:08:55 CET	56	Allocated	Allocated	unkno
📁 Identities				2024-02-29 02:04:49 CET	2024-02-29 02:04:49 CET	2024-02-29 02:04:49 CET	2024-02-29 02:04:49 CET	312	Allocated	Allocated	unkno
📁 KeePassXC			▼	2024-03-04 03:19:01 CET	2024-03-04 03:19:01 CET	2024-03-04 03:19:01 CET	2024-03-04 03:13:56 CET	56	Allocated	Allocated	unkno
📁 Media Center Programs				2011-04-12 11:21:11 CET	2024-02-29 02:04:45 CET	2024-02-29 02:04:44 CET	2024-02-29 02:04:44 CET	48	Allocated	Allocated	unkno
📁 Microsoft				2024-03-04 03:04:52 CET	2024-03-04 03:04:52 CET	2024-03-04 03:04:52 CET	2024-02-29 02:04:44 CET	56	Allocated	Allocated	unkno
📁 Mozilla				2024-02-29 02:25:32 CET	2024-02-29 02:25:32 CET	2024-02-29 02:25:32 CET	2024-02-29 02:25:32 CET	352	Allocated	Allocated	unkno
📁 Telegram Desktop				2024-03-04 02:38:51 CET	2024-03-04 02:38:51 CET	2024-03-04 02:38:51 CET	2024-03-04 02:38:41 CET	584	Allocated	Allocated	unkno
📁 Zoom				2024-03-04 03:02:35 CET	2024-03-04 03:02:35 CET	2024-03-04 03:02:35 CET	2024-03-04 03:01:11 CET	56	Allocated	Allocated	unkno

Figure 57: Herramienta BurpSuite encontrada

También se ha encontrado la herramienta **Npcap**, usada para capturar paquetes. Esta herramienta se puede usar para interceptar el tráfico de red y capturar información sensible.

/img_disk.img/vol_vol3/Program Files/Npcap											
15 Results											
Table		Thumbnail		Summary							
Page:	1 of 1	Pages:	◀	▶	Go to Page:	█	Save Table as CSV	Flags(Dir)	Flags(Meta)	Alloc	Alloc
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Alloc
📁 [current folder]				2024-03-04 02:48:35 CET	2024-03-04 02:48:35 CET	2024-03-04 02:48:35 CET	2024-03-04 02:47:16 CET	56	Allocated	Allocated	Alloc
📁 [parent folder]				2024-03-04 02:59:37 CET	2024-03-04 02:59:37 CET	2024-03-04 02:59:37 CET	2009-07-14 05:20:08 CEST	192	Allocated	Allocated	Alloc
CheckStatus.bat				2022-11-22 20:25:50 CET	2024-03-04 02:48:35 CET	2024-03-04 02:48:35 CET	2022-11-22 20:25:50 CET	815	Allocated	Allocated	Alloc
DiagReport.bat				2022-11-22 20:25:50 CET	2024-03-04 02:48:26 CET	2024-03-04 02:48:26 CET	2022-11-22 20:25:50 CET	1073	Allocated	Allocated	Alloc
DiagReport.ps1	▼			2022-11-22 20:25:50 CET	2024-03-04 02:48:26 CET	2024-03-04 02:48:26 CET	2022-11-22 20:25:50 CET	18078	Allocated	Allocated	Alloc
FixInstall.bat				2022-11-22 20:25:50 CET	2024-03-04 02:48:26 CET	2024-03-04 02:48:26 CET	2022-11-22 20:25:50 CET	2513	Allocated	Allocated	Alloc
install.log	▼			2024-03-04 02:48:38 CET	2024-03-04 02:48:38 CET	2024-03-04 02:47:16 CET	2024-03-04 02:47:16 CET	33734	Allocated	Allocated	Alloc
LICENSE	▼			2022-11-22 20:25:50 CET	2024-03-04 02:48:26 CET	2024-03-04 02:48:26 CET	2022-11-22 20:25:50 CET	11784	Allocated	Allocated	Alloc
npcap.cat	▼			2021-04-09 06:40:52 CEST	2024-03-04 02:48:26 CET	2024-03-04 02:48:26 CET	2021-04-09 06:40:52 CEST	9889	Allocated	Allocated	Alloc
npcap.inf				2021-04-09 06:28:22 CEST	2024-03-04 02:48:26 CET	2024-03-04 02:48:26 CET	2021-04-09 06:28:22 CEST	8562	Allocated	Allocated	Alloc
npcap.sys	▼			2021-04-09 06:41:12 CEST	2024-03-04 02:48:26 CET	2024-03-04 02:48:26 CET	2021-04-09 06:41:12 CEST	66008	Allocated	Allocated	Alloc
npcap_wfp.inf				2021-04-09 06:28:22 CEST	2024-03-04 02:48:26 CET	2024-03-04 02:48:26 CET	2021-04-09 06:28:22 CEST	2404	Allocated	Allocated	Alloc
NPFInstall.exe	▼			2023-04-26 23:54:54 CEST	2024-03-04 02:48:26 CET	2024-03-04 02:48:26 CET	2023-04-26 23:54:54 CEST	308688	Allocated	Allocated	Alloc
NPFInstall.log				2024-03-04 02:48:33 CET	2024-03-04 02:48:33 CET	2024-03-04 02:48:26 CET	2024-03-04 02:48:26 CET	5660	Allocated	Allocated	Alloc

Figure 58: Herramienta Npcap encontrada

3.1.10

Podemos ver que el atacante tiene instalado tanto **Telegram** como **Zoom**, ambas herramientas de comunicación.

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
[current folder]	2024-03-04 03:13:56 CET	2024-03-04 03:13:56 CET	2024-02-29 02:04:44 CET	2024-02-29 02:04:44 CET	56	Allocated
[parent folder]	2024-02-29 02:04:45 CET	2024-02-29 02:04:45 CET	2024-02-29 02:04:44 CET	2024-02-29 02:04:44 CET	344	Allocated
BurpSuite	2024-03-04 03:09:30 CET	2024-03-04 03:09:30 CET	2024-03-04 03:09:30 CET	2024-03-04 03:08:55 CET	56	Allocated
Identities	2024-02-29 02:04:49 CET	2024-02-29 02:04:49 CET	2024-02-29 02:04:49 CET	2024-02-29 02:04:49 CET	312	Allocated
KeePassXC	2024-03-04 03:19:01 CET	2024-03-04 03:19:01 CET	2024-03-04 03:19:01 CET	2024-03-04 03:13:56 CET	56	Allocated
Media Center Programs	2011-04-12 11:12:11 EST	2024-02-29 02:04:45 CET	2024-02-29 02:04:44 CET	2024-02-29 02:04:44 CET	48	Allocated
Microsoft	2024-03-04 03:04:52 CET	2024-03-04 03:04:52 CET	2024-02-29 02:04:44 CET	2024-02-29 02:04:44 CET	56	Allocated
Mozilla	2024-02-29 02:25:32 CET	2024-02-29 02:25:32 CET	2024-02-29 02:25:32 CET	2024-02-29 02:25:32 CET	352	Allocated
Telegram Desktop	2024-03-04 02:38:51 CET	2024-03-04 02:38:51 CET	2024-03-04 02:38:51 CET	2024-03-04 02:38:41 CET	584	Allocated
Zoom	2024-03-04 03:02:35 CET	2024-03-04 03:02:35 CET	2024-03-04 03:02:35 CET	2024-03-04 03:01:11 CET	56	Allocated

Figure 59: Aplicaciones Telegram y Zoom encontradas

También se ha encontrado Windows Mail:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
wabmig.exe				2009-07-14 03:39:50 CEST	2024-02-29 01:36:42 CET	2009-07-14 01:57:58 CEST	2009-07-14 01:57:58 CEST	67584	Allocated	Allocated	unknown	/img_disk/img/vol_
wabimp.dll				2009-07-14 03:41:56 CEST	2024-02-29 01:36:42 CET	2009-07-14 01:57:59 CEST	2009-07-14 01:57:59 CEST	50176	Allocated	Allocated	unknown	/img_disk/img/vol_
wabfind.dll				2009-07-14 03:41:56 CEST	2024-02-29 01:36:42 CET	2009-07-14 01:57:58 CEST	2009-07-14 01:57:58 CEST	35328	Allocated	Allocated	unknown	/img_disk/img/vol_
wab.exe				2010-11-21 04:24:32 CET	2024-02-29 01:36:42 CET	2010-11-21 04:24:32 CET	2010-11-21 04:24:32 CET	516096	Allocated	Allocated	unknown	/img_disk/img/vol_
oimport.dll				2010-11-21 04:24:48 CET	2024-02-29 01:36:42 CET	2010-11-21 04:24:48 CET	2010-11-21 04:24:48 CET	93184	Allocated	Allocated	unknown	/img_disk/img/vol_
mse.dll	V			2010-11-21 04:24:48 CET	2024-02-29 01:36:42 CET	2010-11-21 04:24:48 CET	2010-11-21 04:24:48 CET	2080256	Allocated	Allocated	unknown	/img_disk/img/vol_
es-ES				2011-04-12 11:05:26 CEST	2024-02-29 01:38:48 CET	2011-04-12 11:05:34 CEST	2011-04-12 11:05:26 CEST	272	Allocated	Allocated	unknown	/img_disk/img/vol_
[parent folder]				2024-03-04 02:59:37 CET	2024-03-04 02:59:37 CET	2024-03-04 02:59:37 CET	2009-07-14 05:20:08 CEST	192	Allocated	Allocated	unknown	/img_disk/img/vol_
[current folder]				2011-04-12 11:05:26 CEST	2024-02-29 01:38:48 CET	2011-04-12 11:05:26 CEST	2009-07-14 05:20:08 CEST	56	Allocated	Allocated	unknown	/img_disk/img/vol_
WinMail.exe				2009-07-14 03:39:53 CEST	2024-02-29 01:36:42 CET	2009-07-14 01:58:02 CEST	2009-07-14 01:58:02 CEST	398848	Allocated	Allocated	unknown	/img_disk/img/vol_
MSOERES.dll				2009-07-14 03:29:51 CEST	2024-02-29 01:36:42 CET	2009-07-14 01:58:20 CEST	2009-07-14 01:58:20 CEST	2836992	Allocated	Allocated	unknown	/img_disk/img/vol_

Figure 60: Enter Caption

Con el fin de buscar rastros de uso, se han usado las opciones pslist y psscan de Volatility. Sin embargo, no se ha encontrado nada relevante.

Revisando en los strings, se han encontrado las siguientes cadenas de texto, que podrían indicar algún uso de la aplicación Zoom.

```

-->
text="Su dispositivo se est
quedando sin almacenamiento. Libere espacio para evitar interrupciones mientras utiliza Zoom.">/ID12544>
<ID12545 text="Eliminar"></ID12545>
<ID12546 text="Esta es una acci
n unilateral. El mensaje completo no ser
visible para los miembros nuevos de este grupo.
Continuar?">/ID12546>
<ID12547 text="Eliminar"></ID12547>
<ID12548 text="% recuper
un %s">/ID12548>
<ID12549 text="mensaje"></ID12549>
<ID12550 text="No se pudo cargar
archivo en uso">/ID12550>
<ID12551 text="El archivo no se puede subir porque no es posible encontrarlo"></ID12551>
<ID12552 text="Compartido con %s">/ID12552>
<ID12553 text="A
adir a adhesivos">/ID12553>
<ID12554 text="Eliminar adhesivos"></ID12554>
<ID12555 text="Cargar adhesivos">/ID12555>
<ID12556 text="Guardar emojis de cualquier chat">/ID12556>
<ID12557 text="Clic derecho en una imagen en la ventana de chat,&#xD;&#xA;luego elegir "%s""></ID12557>
<ID12558 text="Cargue su propio adhesivo">/ID12558>
<ID12559 text="Hacer clic en el men
en la esquina inferior derecha">/ID12559>
<ID12560 text="Eliminar Seleccionado">/ID12560>
<ID12561 text="(f 2)Ya ha bloqueado a @1 y no puede enviar ni recibir mensajes de esa persona. Puede desbloquear a @1 desde @2{/f}."></ID12561>
<ID12562 text="

Est
seguro de que desea bloquear %s?">/ID12562>
<ID12563 text="%1 no podr
ponerse en contacto con usted.
Desea bloquear a %2?">/ID12563>
<ID12564 text="Bloquear contacto">/ID12564>
<ID12565 text="Desbloquear contacto">/ID12565>
<ID12566 text="Seleccionar usuarios debajo para desbloquear:">/ID12566>
<ID12567 text="Desbloquear">/ID12567>
<ID12568 text="otros">/ID12568>

```

Figure 61: Strings relacionados con Zoom

También se han encontrado strings relacionados con Telegram, por ejemplo:

```

-->
<a id="launchsupporturl">https://desktop.telegram.org</a>
<a id="launchhelpurl">https://desktop.telegram.org</a>
C:\Users\kiddie\AppData\Roaming\Telegram Desktop\
<a id="launchupdateurl">https://desktop.telegram.org</a>
Telegram FZ-LLC

```

Figure 62: Strings relacionados con Telegram

3.1.11

En Autopsy, tenemos un apartado llamado **Interesting Items** que, nada más entrar nos muestra una billetera de criptomonedas de Monero, por lo que podemos intuir que es la criptomoneda con la que opera.

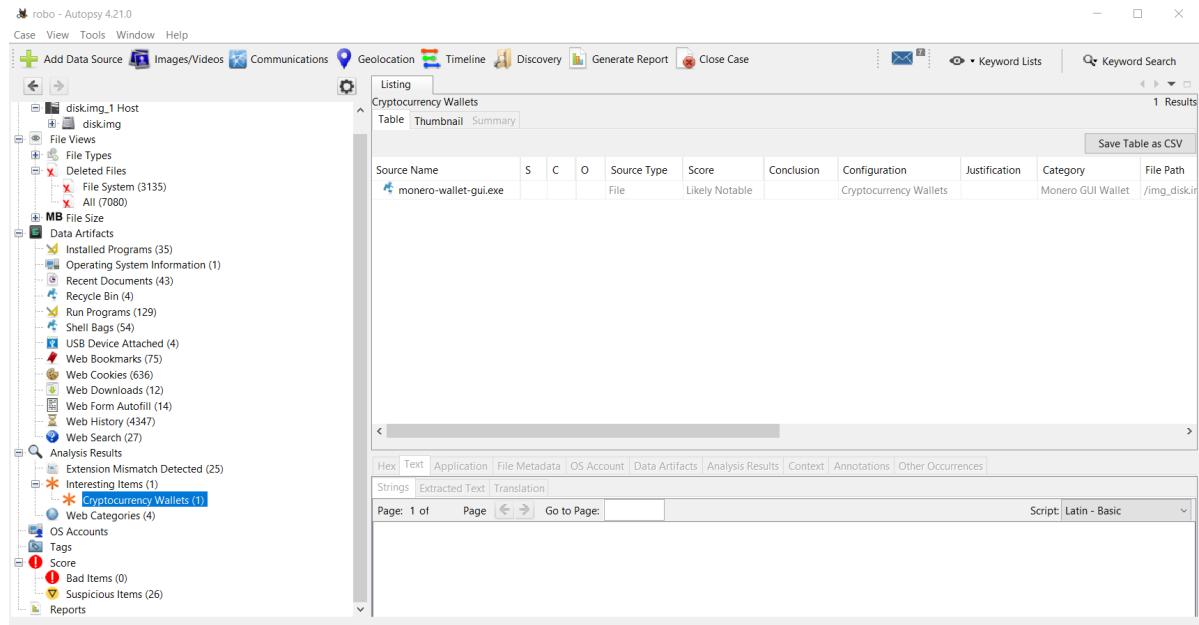


Figure 63: Billetera de criptomonedas de Monero

Es más, hasta hemos podido encontrar una carpeta llamada "Monero GUI Wallet", donde incluso hay una guía de uso.

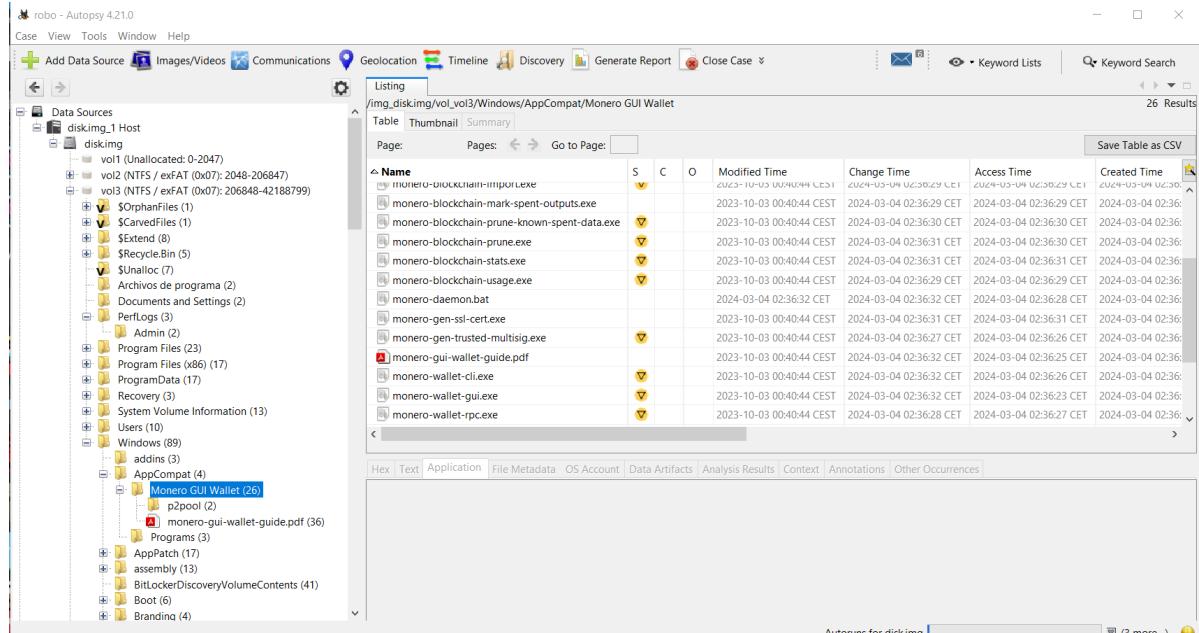


Figure 64: Contenido de la carpeta Monero GUI Wallet

3.2

El informe forense se ha incluído aparte.