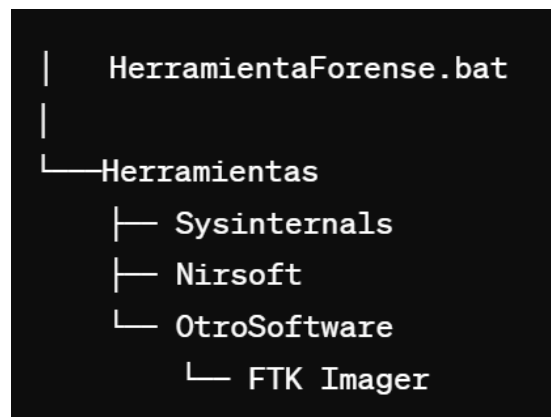


Practica 1

La volatilidad en Windows

Apartado A:

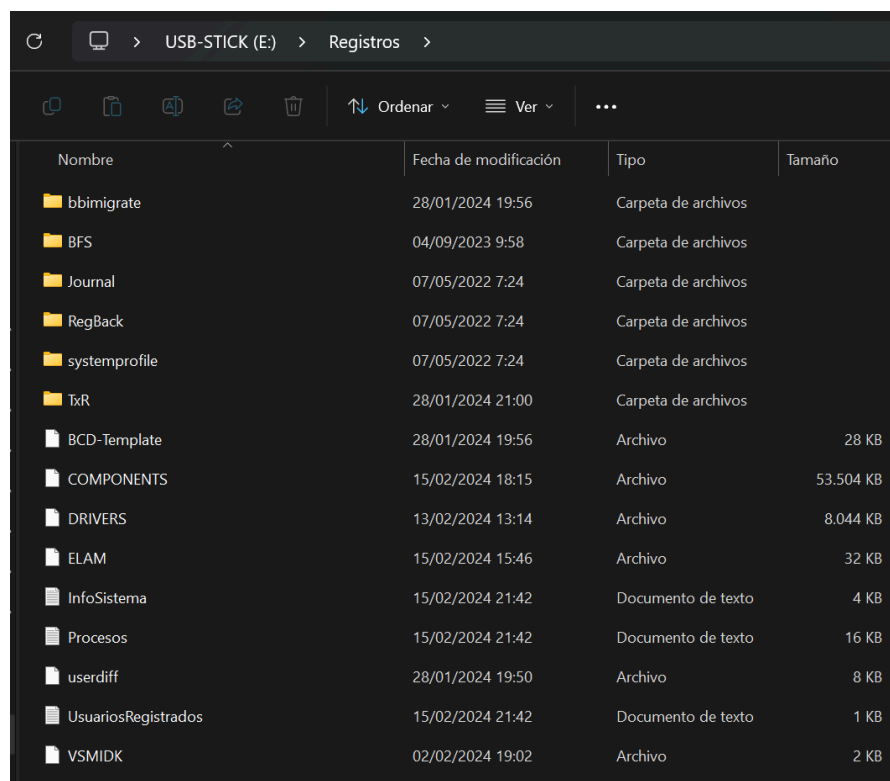
En esta sección, nos enfocaremos en la creación de un USB-STICK que contendrá herramientas y un archivo de procesamiento por lotes. El archivo BATCH se ejecutará en la máquina objetivo, llevando a cabo tareas como la copia de registros en la unidad USB externa y la recopilación de información clave, como fecha, hora, usuarios registrados, árbol de procesos y tiempo de actividad del sistema.



Este es el archivo por lotes que lleva a cabo la adquisición de registros e información, almacenados en un directorio llamado 'registros' en la misma unidad USB.

```
HerramientaForense.bat X
Procesamiento > HerramientaForense.bat
1  @echo off
2
3  set "destino=%~d0\Registros"
4
5  echo Extrayendo registros del sistema...
6  if not exist "%destino%" mkdir "%destino%"
7  xcopy C:\Windows\System32\config\*. * "%destino%" /E /C /H /R /Y
8
9  echo Recopilando información del sistema...
10 systeminfo > "%destino%\InfoSistema.txt"
11 tasklist > "%destino%\Procesos.txt"
12 net user > "%destino%\UsuariosRegistrados.txt"
13
14 echo Herramienta forense completada.
15 pause
16
```

Después de ejecutar este archivo, en el directorio tendríamos algo similar a esto, con la información recopilada.



The screenshot shows a Windows File Explorer window with the address bar set to 'USB-STICK (E:) > Registros >'. The window displays a list of files and folders. The files are organized into columns: 'Nombre' (Name), 'Fecha de modificación' (Date modified), 'Tipo' (Type), and 'Tamaño' (Size). The files include folders like 'bbimigrate', 'BFS', 'Journal', 'RegBack', 'systemprofile', and 'TxR', as well as individual files like 'BCD-Template', 'COMPONENTS', 'DRIVERS', 'ELAM', 'InfoSistema', 'Procesos', 'userdiff', 'UsuariosRegistrados', and 'VSMIDK'.

Nombre	Fecha de modificación	Tipo	Tamaño
bbimigrate	28/01/2024 19:56	Carpeta de archivos	
BFS	04/09/2023 9:58	Carpeta de archivos	
Journal	07/05/2022 7:24	Carpeta de archivos	
RegBack	07/05/2022 7:24	Carpeta de archivos	
systemprofile	07/05/2022 7:24	Carpeta de archivos	
TxR	28/01/2024 21:00	Carpeta de archivos	
BCD-Template	28/01/2024 19:56	Archivo	28 KB
COMPONENTS	15/02/2024 18:15	Archivo	53.504 KB
DRIVERS	13/02/2024 13:14	Archivo	8.044 KB
ELAM	15/02/2024 15:46	Archivo	32 KB
InfoSistema	15/02/2024 21:42	Documento de texto	4 KB
Procesos	15/02/2024 21:42	Documento de texto	16 KB
userdiff	28/01/2024 19:50	Archivo	8 KB
UsuariosRegistrados	15/02/2024 21:42	Documento de texto	1 KB
VSMIDK	02/02/2024 19:02	Archivo	2 KB

```

Nombre de host: JOSE
Nombre del sistema operativo: Microsoft Windows 11 Pro
Versi n del sistema operativo: 10.0.22631 N/D Compilaci n 22631
Fabricante del sistema operativo: Microsoft Corporation
Configuraci n del sistema operativo: Estaci n de trabajo independiente
Tipo de compilaci n del sistema operativo: Multiprocessor Free
Propiedad de: jose_016al@outlook.com
Organizaci n registrada:
Id. del producto: 00330-80000-00000-AA115
Fecha de instalaci n original: 28/01/2024, 21:00:48
Tiempo de arranque del sistema: 12/02/2024, 20:06:26
Fabricante del sistema: Micro-Star International Co., Ltd.
Modelo del sistema: PS42 Modern 8MO
Tipo de sistema: x64-based PC
Procesador(es): 1 Procesadores instalados.
[01]: Intel64 Family 6 Model 142 Stepping 11 GenuineIntel ~2001 Mhz
American Megatrends Inc. E14B3IMS.102, 25/01/2019
Versi n del BIOS:
Directorio de Windows: C:\WINDOWS
Directorio de sistema: C:\WINDOWS\system32
Dispositivo de arranque: \Device\HarddiskVolume1
Configuraci n regional del sistema: es;Espa ol (internacional)
Idioma de entrada: es;Espa ol (tradicional)
Zona horaria: (UTC+01:00) Bruselas, Copenhagen, Madrid, Paris
Cantidad total de memoria f sica: 16.228 MB
Memoria f sica disponible: 9.618 MB
Memoria virtual: tama o m ximo: 18.281 MB
Memoria virtual: disponible: 11.314 MB
Memoria virtual: en uso: 6.967 MB
Ubicaci n(es) de archivo de paginaci n: C:\pagefile.sys
Dominio: WORKGROUP

```

Apartado B:

En esta secci n, exploramos la adquisici n de memoria RAM con Volatility, adquiriendo habilidades en el manejo de esta herramienta forense

Perfil del sistema operativo

Para obtener el perfil del sistema operativo, emplearemos dos comandos: **'imageinfo'**, que nos proporcionar  informaci n b sica sobre la adquisici n; esto ser   til para obtener el **'profile'** necesario para realizar un an lisis m s profundo de la adquisici n. Adem s, podemos utilizar **'kdbgscan'**, que nos brindar  una cantidad considerablemente mayor de informaci n, con detalles m s espec ficos.

- ***vol.py -f practica1.raw imageinfo***
- ***vol.py -f practica1.raw kdbgscan***

```
(kali㉿kali)-[~/practica1]
$ vol.py -f practica1.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86
      AS Layer1 : IA32PagedMemoryPae (Kernel AS)
      AS Layer2 : FileAddressSpace (/home/kali/practica1/practica1.raw)
      PAE type : PAE
      DTB : 0x185000L
      KDBG : 0x82977be8L
      Number of Processors : 1
      Image Type (Service Pack) : 0
      KPCR for CPU 0 : 0x82978c00L
      KUSER_SHARED_DATA : 0xffdf0000L
      Image date and time : 2019-11-07 12:52:54 UTC+0000
      Image local date and time : 2019-11-07 13:52:54 +0100
```

Listado de procesos

Para enumerar los procesos activos durante la adquisición, contamos con varios parámetros. El comando **'pstree'** exhibe los procesos de manera jerárquica, **'pslist'** los presenta de forma directa y ordenada en formato de lista, mientras que **'psscan'** se concentra en aquellos procesos que consumían significativamente más recursos. Por último, **'psxview'** revisa la presencia de subprocesos sospechosos o malignos que podrían no haber sido detectados por **'pslist'** y **'psscan'**.

- ***vol.py -f practica1.raw --profile=Win7SP1x86_23418 pstree***
- ***vol.py -f practica1.raw --profile=Win7SP1x86_23418 pslist***
- ***vol.py -f practica1.raw --profile=Win7SP1x86_23418 psscan***
- ***vol.py -f practica1.raw --profile=Win7SP1x86_23418 psxview***

```
(kali㉿kali)-[~/practical1]
$ vol.py -f practical1.raw --profile=Win7SP1x86_23418 pstree
Volatility Foundation Volatility Framework 2.6.1
```

Name	Pid	PPid	Thds	Hnds	Time
0x8657a400:explorer.exe	1408	1356	39	804	2019-11-07 12:51:59 UTC+0000
. 0x865fdc28:vmtoolsd.exe	1648	1408	10	196	2019-11-07 12:51:59 UTC+0000
. 0x87cc79b8:notepad.exe	3112	1408	12	293	2019-11-07 12:52:11 UTC+0000
. 0x92549d40:MagnetRAMCaptu	3316	1408	13	296	2019-11-07 12:52:15 UTC+0000
0x86398148:wininit.exe	388	320	7	90	2019-11-07 12:51:57 UTC+0000
. 0x86407030:lsm.exe	508	388	11	153	2019-11-07 12:51:57 UTC+0000
. 0x863fe230:services.exe	492	388	21	248	2019-11-07 12:51:57 UTC+0000
.. 0x86479790:svchost.exe	776	492	25	528	2019-11-07 12:51:58 UTC+0000
... 0x864cd5c0:audiodg.exe	976	776	6	125	2019-11-07 12:51:58 UTC+0000
.. 0x87d11d40:VSVC.exe	2192	492	7	119	2019-11-07 12:52:04 UTC+0000
.. 0x87d094c0:msdtc.exe	644	492	15	155	2019-11-07 12:52:03 UTC+0000
.. 0x864f4510:svchost.exe	1052	492	37	783	2019-11-07 12:51:58 UTC+0000
.. 0x86444d40:vmacthlp.exe	672	492	5	55	2019-11-07 12:51:58 UTC+0000
.. 0x87dadd40:wmpnetwk.exe	2468	492	17	482	2019-11-07 12:52:06 UTC+0000
.. 0x925198d8:svchost.exe	2780	492	11	356	2019-11-07 12:52:07 UTC+0000
.. 0x87c73b38:dlhhost.exe	560	492	21	202	2019-11-07 12:52:01 UTC+0000
.. 0x87c7a548:dlhhost.exe	1724	492	18	207	2019-11-07 12:52:01 UTC+0000
.. 0x865f2140:vmtoolsd.exe	1824	492	9	293	2019-11-07 12:52:00 UTC+0000
.. 0x86563030:spoolsv.exe	1348	492	15	322	2019-11-07 12:51:59 UTC+0000

```
(kali㉿kali)-[~/practical1]
$ vol.py -f practical1.raw --profile=Win7SP1x86_23418 pslist
Volatility Foundation Volatility Framework 2.6.1
```

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0x84f4a8e8	System	4	0	85	507		0	2019-11-07 12:51:57 UTC+0000	
0x85aa8128	smss.exe	248	4	4	29		0	2019-11-07 12:51:57 UTC+0000	
0x85a7a030	csrss.exe	336	320	9	639	0	0	2019-11-07 12:51:57 UTC+0000	
0x86398148	wininit.exe	388	320	7	90	0	0	2019-11-07 12:51:57 UTC+0000	
0x863c3d40	csrss.exe	396	380	10	228	1	0	2019-11-07 12:51:57 UTC+0000	
0x863d1030	winlogon.exe	432	380	6	119	1	0	2019-11-07 12:51:57 UTC+0000	
0x863fe230	services.exe	492	388	21	248	0	0	2019-11-07 12:51:57 UTC+0000	
0x86404840	lsass.exe	500	388	10	792	0	0	2019-11-07 12:51:57 UTC+0000	
0x86407030	lsm.exe	508	388	11	153	0	0	2019-11-07 12:51:57 UTC+0000	
0x86429c40	svchost.exe	616	492	16	366	0	0	2019-11-07 12:51:58 UTC+0000	
0x86444d40	vmacthlp.exe	672	492	5	55	0	0	2019-11-07 12:51:58 UTC+0000	
0x864595e8	svchost.exe	716	492	11	314	0	0	2019-11-07 12:51:58 UTC+0000	
0x86479790	svchost.exe	776	492	25	528	0	0	2019-11-07 12:51:58 UTC+0000	
0x8648eb90	svchost.exe	848	492	32	518	0	0	2019-11-07 12:51:58 UTC+0000	

```
(kali㉿kali)-[~/practical1]
$ vol.py -f practical1.raw --profile=Win7SP1x86_23418 psscan
Volatility Foundation Volatility Framework 2.6.1
```

Offset(P)	Name	PID	PPID	PDB	Time created	Time exited
-----------	------	-----	------	-----	--------------	-------------

```
(kali@kali)-[~/practical1]
$ vol.py -f practical1.raw --profile=Win7SP1x86_23418 psxview
Volatility Foundation Volatility Framework 2.6.1
Offset(P)  Name                               PID  pslist  psscan  thrddproc  pspcid  csrss  session  deskthrd  ExitTime
-----
0x0e5cd400 SearchProtocol                      2336 True    False    True       True    True   True     True     True
0x0e844d40 vmacthlp.exe                        672  True    False    True       True    True   True     False    True
0x0a14d618 WmiPrvSE.exe                        2904 True    False    True       True    True   True     True     True
0x0e97cc88 svchost.exe                         1400 True    False    True       True    True   True     False    True
0x0e8f4510 svchost.exe                         1052 True    False    True       True    True   True     True     True
0x0e879790 svchost.exe                         776  True    False    True       True    True   True     True     True
0x0dbbb8d8 svchost.exe                         2780 True    False    True       True    True   True     False    True
0x019d1d40 wmpnetwk.exe                       2468 True    False    True       True    True   True     True     True
0x07ed5c98 SearchFilterHost            2356 True    False    True       True    True   True     True     True
0x0e9f2140 vmtoolsd.exe                      1824 True    False    True       True    True   True     False    True
0x0ebfe230 services.exe                  492  True    False    True       True    True   True     False    True
0x0ebd1030 winlogon.exe                   432  True    False    True       True    True   True     True     True
```

Historial de comandos

Con estos comandos podemos identificar los comandos que se han lanzado desde la cmd

- ***vol.py -f practica1.raw --profile=Win7SP1x86_23418 cmdscan***
- ***vol.py -f practica1.raw --profile=Win7SP1x86_23418 cmdline***
- ***vol.py -f practica1.raw --profile=Win7SP1x86_23418 consoles***

```
(kali@kali)-[~/practical1]
$ vol.py -f practical1.raw --profile=Win7SP1x86_23418 cmdline
Volatility Foundation Volatility Framework 2.6.1
*****
System pid: 4
*****
smss.exe pid: 248
Command line : \SystemRoot\System32\smss.exe
*****
csrss.exe pid: 336
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,12288,512 Windows=On SubSystemType=Windows ServerDll=baserv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
*****
wininit.exe pid: 388
Command line : wininit.exe
*****
csrss.exe pid: 396
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,12288,512 Windows=On SubSystemType=Windows ServerDll=baserv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
*****
```

Información detallada del sistema operativo

Habíamos mencionado previamente este comando; ofrece información más detallada del sistema operativo, complementando así la información proporcionada por 'imageinfo'.

- ***vol.py -f practica1.raw kdbgscan***

```

(kali@kali)-[~/practica1]
$ vol.py -f practica1.raw kdbgscan
Volatility Foundation Volatility Framework 2.6.1
*****
Instantiating KDBG using: /home/kali/practica1/practica1.raw WinXPSP2x86 (5.1.0 32bit)
Offset (P) : 0x2977be8
KDBG owner tag check : True
Profile suggestion (KDBGHeader): Win7SP1x86_23418
Version64 : 0x2977bc0 (Major: 15, Minor: 7600)
PsActiveProcessHead : 0x8298fe98
PsLoadedModuleList : 0x82997810
KernelBase : 0x8284f000

*****
Instantiating KDBG using: /home/kali/practica1/practica1.raw WinXPSP2x86 (5.1.0 32bit)
Offset (P) : 0x2977be8
KDBG owner tag check : True
Profile suggestion (KDBGHeader): Win7SP1x86
Version64 : 0x2977bc0 (Major: 15, Minor: 7600)
PsActiveProcessHead : 0x8298fe98

```

Ficheros cargados en memoria

Nos muestra todos los DLL que estan detras de cada proceso

vol.py -f practica1.raw --profile=Win7SP1x86_23418 dlllist

```

(kali@kali)-[~/practica1]
$ vol.py -f practica1.raw --profile=Win7SP1x86_23418 dlllist
Volatility Foundation Volatility Framework 2.6.1
*****
System pid: 4
Unable to read PEB for task.
*****
smss.exe pid: 248
Command line : \SystemRoot\System32\smss.exe

Base      Size  LoadCount LoadTime      Path
0x48260000 0x13000 0xffff 1970-01-01 00:00:00 UTC+0000 \SystemRoot\System32\smss.exe
0x76e90000 0x13c000 0xffff 1970-01-01 00:00:00 UTC+0000 C:\Windows\SYSTEM32\ntdll.dll
*****
csrss.exe pid: 336
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=Windows SharedSection=1024,12288,512 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16

Base      Size  LoadCount LoadTime      Path
0x49710000 0x5000 0xffff 1970-01-01 00:00:00 UTC+0000 C:\Windows\system32\csrss.exe
0x76e90000 0x13c000 0xffff 1970-01-01 00:00:00 UTC+0000 C:\Windows\SYSTEM32\ntdll.dll

```

Conexiones activas

Estos comandos proporcionan información útil sobre conexiones internas o externas, específicamente diseñados para un entorno Windows. En el caso de un entorno Linux, se utilizarían comandos distintos para obtener información similar.

- ***vol.py -f practica1.raw --profile=Win7SP1x86_23418 connscan***

- **`vol.py -f practica1.raw --profile=Win7SP1x86_23418 sockets`**
- **`vol.py -f practica1.raw --profile=Win7SP1x86_23418 netscan`**

```
(kali@kali)-[~/practica1]
$ vol.py -f practica1.raw --profile=Win7SP1x86_23418 netscan
Volatility Foundation Volatility Framework 2.6.1
```

Offset(P)	Proto	Local Address	Foreign Address	State	Pid	Owner	Created
0x259378	TCPv4	0.0.0.0:2869	0.0.0.0:0	LISTENING	4	System	
0x259378	TCPv6	:::2869	:::0	LISTENING	4	System	
0x10494b8	UDPv6	fe80::91bc:cd88:f2f4:736e:546	*		776	svchost.exe	2019-11-07 12:52:09 UTC+0000
0x13d7f50	UDPv4	0.0.0.0:0	*		2780	svchost.exe	2019-11-07 12:52:07 UTC+0000
0x13d7f50	UDPv6	:::0	*		2780	svchost.exe	2019-11-07 12:52:07 UTC+0000
0x13d7680	TCPv4	0.0.0.0:10243	0.0.0.0:0	LISTENING	4	System	
0x13d7680	TCPv6	:::10243	:::0	LISTENING	4	System	
0x19c8d28	UDPv6	:::1:54672	*		2552	svchost.exe	2019-11-07 12:52:07 UTC+0000
0x19c8e98	UDPv6	fe80::91bc:cd88:f2f4:736e:54671	*		2552	svchost.exe	2019-11-07 12:52:07 UTC+0000
0x1ff2638	UDPv4	0.0.0.0:0	*		2780	svchost.exe	2019-11-07 12:52:07 UTC+0000
0x1ff2638	UDPv6	:::0	*		2780	svchost.exe	2019-11-07 12:52:07 UTC+0000
0x2699a30	UDPv4	0.0.0.0:61257	*		1136	svchost.exe	2019-11-07 12:52:52 UTC+0000
0x4346960	UDPv4	0.0.0.0:3702	*		2552	svchost.exe	2019-11-07 12:52:28 UTC+0000
0x4346960	UDPv6	:::3702	*		2552	svchost.exe	2019-11-07 12:52:28 UTC+0000
0x4bf4750	UDPv4	0.0.0.0:3702	*		1052	svchost.exe	2019-11-07 12:52:28 UTC+0000
0x4e365c8	UDPv4	0.0.0.0:0	*		2780	svchost.exe	2019-11-07 12:52:18 UTC+0000
0x4e365c8	UDPv6	:::0	*		2780	svchost.exe	2019-11-07 12:52:18 UTC+0000
0x4f0fd90	UDPv4	0.0.0.0:3540	*		2780	svchost.exe	2019-11-07 12:52:18 UTC+0000