

Tarea 2.2 - Instalación de Volatility 2 y Volatility 3 sobre un contenedor LXC



Trabajo realizado por:

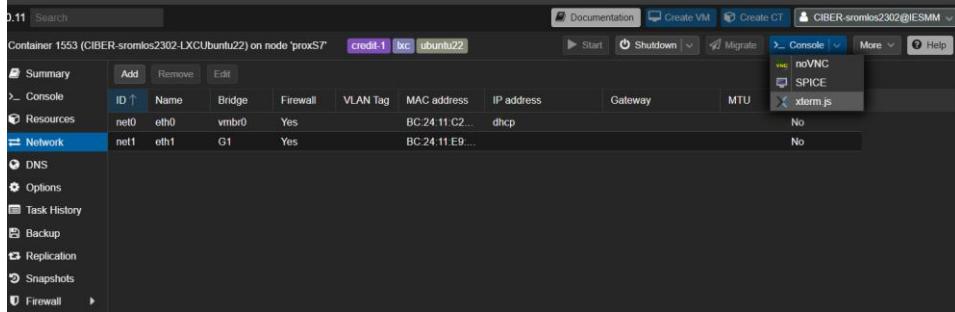
Índice

1.- Instalación Volatility 2 y 3	2
1.1.- Creación del contenedor	2
1.2.- Instalación Volatility2.....	3
1.3.- Instalación de Volatility3	3
2.- Uso de Volatility 2 y 3	5
3.- Comparativa entre Volatility 2 y 3	9

1.- Instalación Volatility 2 y 3

1.1.- Creación del contenedor

Primero, creamos el contenedor y lo abrimos con xterm.js.



1.2.- Instalación Volatility2

Después, instalamos Python2 y pip:

```
sudo apt update
```

```
sudo apt install -y python2 python-pip
```

Verificamos con el siguiente comando que esté todo bien:

```
python2 --version
```

```
pip2 --version
```

Instalamos Volatility 2:

```
sudo pip2 install
```

```
https://github.com/volatilityfoundation/volatility/archive/refs/heads/master.zip
```

Para que todos los plugins funcionen (malware, crypto, YARA, etc.):

```
sudo apt install -y build-essential python2-dev libyara-dev
```

```
sudo pip2 install -U "pip==20.3.4" "setuptools==44.1.1" "wheel==0.37.1"
```

```
sudo pip2 install pycrypto==2.6.1 distorm3==3.4.4 yara-python==3.10.0  
pefile==2019.4.18 pytz==2021.3
```

Y comprobamos que funciona:

```
vol.py -h
```

1.3.- Instalación de Volatility3

Ahora para instalar Volatility 3, primero instalamos Python3 y pip:

```
sudo apt update
```

```
sudo apt install -y python3 python3-venv python3-pip git build-essential libyara-dev
```

Verificamos que se haya instalado correctamente:

```
python3 --version
```

```
pip3 --version
```

Clonamos el repositorio oficial:

```
cd ~
```

```
git clone https://github.com/volatilityfoundation/volatility3.git
```

```
cd volatility3
```

Creamos un entorno virtual:

```
python3 -m venv venv
```

```
source venv/bin/activate
```

Instalamos Volatility3:

```
python3 -m pip install -U pip setuptools wheel
```

```
python3 -m pip install -e
```

Instalamos algunas dependencias opcionales:

```
python3 -m pip install pycryptodome impacket capstone pefile yara-python
```

Y probamos que funcione:

```
vol -h
```

Para acceder desde cualquier carpeta:

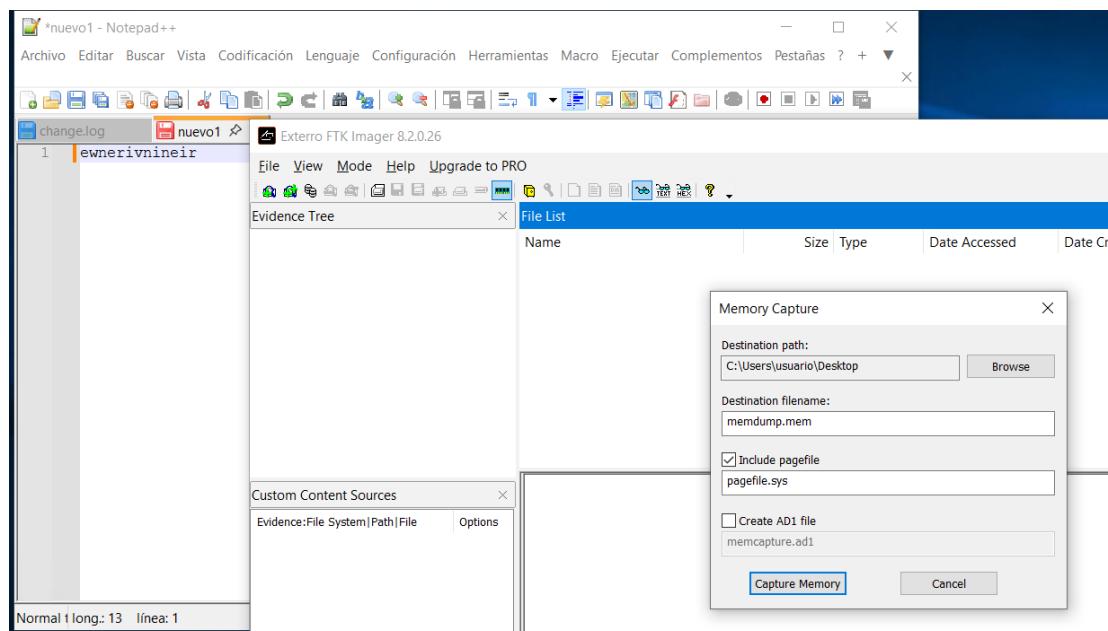
```
sudo ln -sf ~/volatility3/venv/bin/vol /usr/local/bin/vol3
```

2.- Uso de Volatility 2 y 3

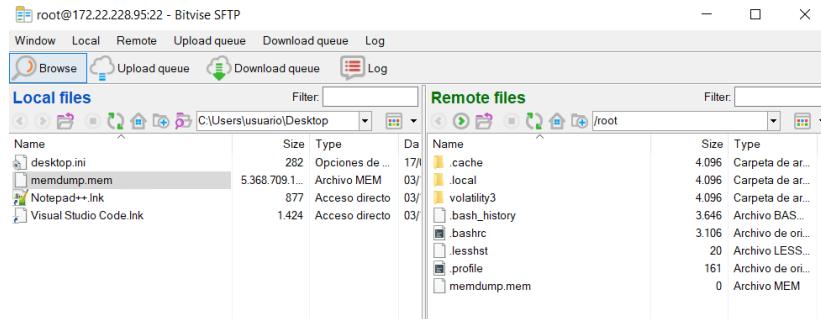
Instalo NotePad++ y CodeBlocks.



Ahora dejándolos abiertos, hago una copia de la ram.



Ahora mediante Bitvise me paso el archivo.



Y empezamos a usar Volatility 3. Primero con información del sistema operativo:

`vol3 -f memdump.mem windows.info`

```
root@CIBER-SROMIOS2302-LXCUbuntu22:~# vol3 -f memdump.mem windows.info
Volatility 3 Framework 2.27.0
Progress: 100.00          PDB scanning finished
Variable           Value

Kernel Base        0xf8023801c000
DTB              0x1aa000
Symbols file:///root/volatility3/symbols/windows/ntkrnlmp.pdb/80A68472D8B6D17786B0E6177FD0A6B7-1.json.xz
Is64Bit True
IsPAE False
layer_name         0 WindowsIntel32e
memory_layer       1 FileLayer
KdVersionBlock    0xf8023841df40
Major/Minor        15.17763
MachineType       34404
KeNumberProcessors 2
SystemTime         2025-11-03 18:48:42+00:00
NtSystemRoot      C:\Windows
NtProductType     NtProductWinNt
NtMajorVersion    10
NtMinorVersion    0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine        34404
PE TimeStamp       Tue Nov 11 22:23:06 2081
```

Para ver el listado de procesos:

`vol3 -f memdump.mem windows.pslist`

```
root@CIBER-SROMIOS2302-LXCUbuntu22:~# vol3 -f memdump.mem windows.pslist
Volatility 3 Framework 2.27.0
Progress: 100.00          PDB scanning finished
PID   PPID  ImageFileName          Offset(V)  Threads Handles SessionId  Wow64  CreateTime          ExitTime          File output
4     0      System               0xc2834d864240 136   -      N/A   False   2025-11-03 18:34:51.000000 UTC  N/A   Disabled
88    4      Registry             0xc2834d99d040 4     -      N/A   False   2025-11-03 18:34:49.000000 UTC  N/A   Disabled
348   4      smss.exe             0xc28350a22040 2     -      N/A   False   2025-11-03 18:34:51.000000 UTC  N/A   Disabled
456   444    csrss.exe            0xc283523f70c0 11    -      0     False   2025-11-03 18:34:56.000000 UTC  N/A   Disabled
536   444    wininit.exe          0xc283524190c0 1     -      0     False   2025-11-03 18:34:56.000000 UTC  N/A   Disabled
548   528    svchost.exe          0xc283552f9140 11    -      1     False   2025-11-03 18:34:56.000000 UTC  N/A   Disabled
632   528    winlogon.exe         0xc2835248d0c0 3     -      1     False   2025-11-03 18:34:56.000000 UTC  N/A   Disabled
680   536    services.exe         0xc28352570c0 9     -      0     False   2025-11-03 18:34:56.000000 UTC  N/A   Disabled
680   536    lsass.exe             0xc28352540c0 9     -      0     False   2025-11-03 18:34:56.000000 UTC  N/A   Disabled
680   536    cryptui.exe          0xc283525430c0 1     -      0     False   2025-11-03 18:34:56.000000 UTC  N/A   Disabled
792   632    fontdryhost.exe      0xc28352520c0 5     -      1     False   2025-11-03 18:34:56.000000 UTC  N/A   Disabled
800   536    fontdryhost.exe      0xc2835502b100 5     -      0     False   2025-11-03 18:34:56.000000 UTC  N/A   Disabled
868   672    svchost.exe          0xc2835254e0c0 15    -      0     False   2025-11-03 18:34:56.000000 UTC  N/A   Disabled
916   672    svchost.exe          0xc283516df0c0 11    -      0     False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
960   672    svchost.exe          0xc28351fa0c0 7     -      0     False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
8     672    svchost.exe          0xc283508fec0c0 35   -      0     False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
744   672    svchost.exe          0xc2835aff4f0c0 1     -      0     False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
1104  672    svchost.exe          0xc2835b8f1240 4     -      0     False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
1156  672    svchost.exe          0xc28359f4f0c0 5     -      0     False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
1192  672    svchost.exe          0xc283526ee0c0 3     -      0     False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
1216  672    svchost.exe          0xc2835270a0c0 3     -      0     False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
1340  672    svchost.exe          0xc2835b8fa2c0 3     -      0     False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
1348  672    svchost.exe          0xc2835272a0c0 9     -      0     False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
1356  672    svchost.exe          0xc283527b00c0 10    -      0     False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
1368  672    svchost.exe          0xc283527b60c0 10    -      0     False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
1428   4      MemCompression      0xc283527c9080 30   -      N/A   False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
1456  672    svchost.exe          0xc283527ff0c0 5     -      0     False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
1516  672    svchost.exe          0xc2835284a0c0 4     -      0     False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
1592  672    svchost.exe          0xc283528d0c0 2     -      0     False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
1628  632    dwm.exe              0xc2835291d0c0 13   -      1     False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
1644  632    LogonUI.exe          0xc2835293a0c0 14   -      1     False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
1704  672    svchost.exe          0xc283552142c0 4     -      0     False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
1740  672    svchost.exe          0xc283529d0c0 6     -      0     False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
1752  672    svchost.exe          0xc283529d0c0 7     -      0     False   2025-11-03 18:34:57.000000 UTC  N/A   Disabled
```

Para ver el listado de procesos en forma de árbol:

vol3 -f memdump.mem windows.pstree > pstree.txt

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Ww64	CreateTime	ExitTime	Audit	Cmd	Path
4	0	System	0xc2834d864240	136	-	N/A	False	2025-11-03 18:34:51.000000 UTC	N/A	-	-	-
89	4	Registry	0xc2834d99d040	4	-	N/A	False	2025-11-03 18:34:49.000000 UTC	N/A	Registry	-	-
1428	4	MemCompression	0xc283527c9080	30	-	N/A	False	2025-11-03 18:34:57.000000 UTC	N/A	MemCompression	-	-
348	4	smss.exe	0xc28350a22040	2	-	N/A	False	2025-11-03 18:34:51.000000 UTC	N/A	\Device\HarddiskVolume2\Windows\System32\smss.exe	\Device\HarddiskVolume2\Windows\System32\smss.exe	\SystemRoot\System32\smss.exe
456	444	csrss.exe	0xc283523870c0	11	-	0	False	2025-11-03 18:34:56.000000 UTC	N/A	\Device\HarddiskVolume2\Windows\System32\csrss.exe	\Device\HarddiskVolume2\Windows\System32\csrss.exe	\SystemRoot\System32\csrss.exe
536	444	wininit.exe	0xc283524190c0	1	-	0	False	2025-11-03 18:34:56.000000 UTC	N/A	\Device\HarddiskVolume2\Windows\System32\wininit.exe	\Device\HarddiskVolume2\Windows\System32\wininit.exe	\SystemRoot\System32\wininit.exe
672	536	services.exe	0xc283524570c0	7	-	0	False	2025-11-03 18:34:56.000000 UTC	N/A	\Device\HarddiskVolume2\Windows\System32\services.exe	\Device\HarddiskVolume2\Windows\System32\services.exe	\SystemRoot\System32\services.exe
** 8	672	svchost.exe	0xc2835b8e0c00	35	-	0	False	2025-11-03 18:34:57.000000 UTC	N/A	\Device\HarddiskVolume2\Windows\System32\svchost.exe	\Device\HarddiskVolume2\Windows\System32\svchost.exe	\SystemRoot\System32\svchost.exe
*** 5308	8	rdpclip.exe	0xc283528e0800	10	-	2	False	2025-11-03 18:35:41.000000 UTC	N/A	\Device\HarddiskVolume2\Windows\System32\rdpclip.exe	\Device\HarddiskVolume2\Windows\System32\rdpclip.exe	\SystemRoot\System32\rdpclip.exe
** 7176	672	svchost.exe	0xc28353027240	9	-	0	False	2025-11-03 18:35:46.000000 UTC	N/A	\Device\HarddiskVolume2\Windows\System32\svchost.exe	\Device\HarddiskVolume2\Windows\System32\svchost.exe	\SystemRoot\System32\svchost.exe

Ahora, para ver las librerías del sistema que se están utilizando:

vol3 -f memdump.mem windows.dlllist > dlllist.txt

abled												
6692	smartscreen.ex	0x7ffc92500000	0x35000	smartscreenps.dll	C:\Windows\System32\smartscreenps.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffca42c0000	0xe1000	Windows.Security.Authentication.OnlineId.dll	C:\Windows\System32\Windows.Security.Authentication.OnlineId.dll							
025-11-03 18:35:46.000000 UTC	Disabled											
6692	smartscreen.ex	0x7ffcb76e0000	0x0a000	DPAPI.DLL	C:\Windows\System32\DPAPI.DLL	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcb48e0000	0x0e000	tbs.dll	C:\Windows\System32\tbs.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcb790000	0x1d000	imagehlp.dll	C:\Windows\System32\imagehlp.dll	6	2025-11-03 18:35:46.000000 UTC	disabled				
6692	smartscreen.ex	0x7ffcb4530000	0x18000	wkscli.dll	C:\Windows\System32\wkscli.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcae08d000	0x4e2000	WININET.dll	C:\Windows\System32\WININET.dll	-1	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcb770000	0x2f000	Sspicli.dll	C:\Windows\System32\Sspicli.dll	-1	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffca240000	0x16000	ondemandconroutehelper.dll	C:\Windows\SYSTEM32\ondemandconroutehelper.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
abled												
6692	smartscreen.ex	0x7ffcb5000000	0xfd000	winhttp.dll	C:\Windows\System32\winhttp.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcb7060000	0x67000	mswsock.dll	C:\Windows\System32\mswsock.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcb67e0000	0x95000	firewallapi.dll	C:\Windows\System32\firewallapi.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcb6d90000	0xc6000	DNSAPI.dll	C:\Windows\System32\DNSAPI.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcb76b0000	0x80000	NSI.dll	C:\Windows\System32\NSI.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcb6d95000	0x3d000	IIPHLPAPI.DLL	C:\Windows\System32\IIPHLPAPI.DLL	6	2025-11-03 18:35:46.000000 UTC	disabled				
6692	smartscreen.ex	0x7ffcb6d95000	0x3d000	fwbase.dll	C:\Windows\System32\fwbase.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcb25d0000	0xb0000	WINNSI.dll	C:\Windows\System32\WINNSI.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcb7b40000	0x1b000	CRYPTSP.dll	C:\Windows\System32\CRYPTSP.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcb6880000	0x33000	rsaenh.dll	C:\Windows\System32\rsaenh.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcaf380000	0xa0000	rasadnlp.dll	C:\Windows\System32\rasadnlp.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcaf200000	0x79000	fvpuclnt.dll	C:\Windows\System32\fvpuclnt.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcaf6a60000	0x8c000	schannel.dll	C:\Windows\System32\schannel.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcaf1190000	0x15000	mskeyprotect.dll	C:\Windows\SYSTEM32\mskeyprotect.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcb7330000	0x2c000	ncrypt.dll	C:\Windows\SYSTEM32\ncrypt.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcb72f0000	0x3c000	NTASN1.dll	C:\Windows\SYSTEM32\NTASN1.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcaf0e30000	0x2f000	cryptnet.dll	C:\Windows\System32\cryptnet.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcb0c90000	0x16000	dhcpcsvc6.dll	C:\Windows\SYSTEM32\dhcpcsvc6.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcb0c70000	0x1c000	dhcpcsvc.dll	C:\Windows\SYSTEM32\dhcpcsvc.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcab70000	0x99000	webio.dll	C:\Windows\System32\webio.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcall0e0000	0x24000	ncryptts1p.dll	C:\Windows\System32\ncryptts1p.dll	6	2025-11-03 18:35:46.000000 UTC	Disabled				
6692	smartscreen.ex	0x7ffcaf0d0000	0x31d000	certenroll.dll	C:\Windows\System32\certenroll.dll	6	2025-11-03 18:35:46.000000 UTC	Disabledroot@CI				

Vemos la dirección IP que tenía el equipo:

vol3 -f memdump.mem windows.netstat

Volatility 3 Framework 2.27.0												
Offset	Proto	LocalAddr	LocalPort	ForeignAddr	ForeignPort	State	PID	Owner	Created			
0xc2835d8f9710	TCPv4	127.0.0.1	50278	127.0.0.1	5985	CLOSED	6924	svchost.exe	2025-11-03 18:48:45.000000 UTC			
0xc283530c49a0	TCPv4	172.22.254.24	49701	4.207.247.137	443	ESTABLISHED	2992	svchost.exe	2025-11-03 18:35:19.000000 UTC			
0xc283530839a0	TCPv4	172.22.254.24	3389	172.22.231.79	52710	ESTABLISHED	8	svchost.exe	2025-11-03 18:35:38.000000 UTC			

Para ver las conexiones de red realizadas (puertos y servicios):

```
vol3 -f memdump.mem windows.netscan
```

PDB scanning finished									
Offset	Proto	LocalAddr	LocalPort	ForeignAddr	ForeignPort	State	PID	Owner	Created
0xc2834d871590	TCPv4	127.0.0.1	22352	0.0.0.0	0	LISTENING	400	CmWebAdmin.exe	2025-11-03 18:43:05.000000 UTC
0xc2834d8716e0	TCPv4	0.0.0.0	49669	0.0.0.0	0	LISTENING	672	services.exe	2025-11-03 18:34:58.000000 UTC
0xc2834d8716e0	TCPv6	::	49669	::	0	LISTENING	672	services.exe	2025-11-03 18:34:58.000000 UTC
0xc2834d871c20	TCPv4	0.0.0.0	49669	0.0.0.0	0	LISTENING	672	services.exe	2025-11-03 18:34:58.000000 UTC
0xc2834d934700	UDPV4	0.0.0.0	0	*	0	2084	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d934700	UDPV6	::	0	*	0	2084	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d93660	UDPV4	0.0.0.0	0	*	0	2084	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d93660	UDPV6	::	0	*	0	2084	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d947a00	UDPV4	0.0.0.0	0	*	0	4	System	2025-11-03 18:35:09.000000 UTC	
0xc2834d949100	UDPV4	0.0.0.0	0	*	0	2084	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d95bco	UDPV4	0.0.0.0	0	*	0	4	System	2025-11-03 18:35:09.000000 UTC	
0xc2834d962f0	UDPV4	0.0.0.0	0	*	0	4064	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d962f0	UDPV6	::	0	*	0	4064	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d967e0	UDPV4	0.0.0.0	0	*	0	2084	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d972c0	UDPV4	0.0.0.0	0	*	0	2084	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d972c0	UDPV6	::	0	*	0	2084	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d97880	UDPV4	0.0.0.0	0	*	0	4064	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d97880	UDPV6	::	0	*	0	4064	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d979f0	UDPV4	0.0.0.0	0	*	0	4064	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d97cd0	UDPV4	0.0.0.0	0	*	0	4064	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d98850	UDPV4	0.0.0.0	0	*	0	4500	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d989c0	UDPV4	0.0.0.0	0	*	0	4500	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d989c0	UDPV6	::	0	*	0	4500	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d98b30	UDPV4	0.0.0.0	0	*	0	4500	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d98b30	UDPV6	::	0	*	0	4500	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d98ca0	UDPV4	0.0.0.0	0	*	0	4500	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d99820	UDPV4	0.0.0.0	0	*	0	4064	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d99820	UDPV6	::	0	*	0	4064	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d99b00	UDPV4	0.0.0.0	0	*	0	4064	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834d99c70	UDPV4	0.0.0.0	0	*	0	4500	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834da9acd0	UDPV4	0.0.0.0	0	*	0	4064	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834da9acd0	UDPV6	::	0	*	0	4064	svchost.exe	2025-11-03 18:35:09.000000 UTC	
0xc2834da9b370	UDPV4	0.0.0.0	0	*	0	4064	svchost.exe	2025-11-03 18:35:09.000000 UTC	

Para extraer una librería del sistema y subirla a VirusTotal, primero extraemos las librerías:

```
vol3 -f memdump.mem windows.dlllist
```

Una vez identificada una librería, escribimos lo siguiente:

```
mkdir -p extracted
```

```
vol3 -f memdump.mem -o extracted/ windows.dumpfiles --name IQUERY.DLL
```

Para ver un listado de comandos ejecutados:

```
vol3 -f memdump.mem windows.cmdline
```

```
root@CIBER-srmios2302-LXCUbuntu22:~# vol3 -f memdump.mem windows.cmdline
Volatility 3 Framework 2.27.0
Progress: 100.00          PDB scanning finished
PID  Process Args
4      System -
88     Registry -
348    smss.exe   \SystemRoot\System32\smss.exe
456    csrss.exe  \SystemRoot\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 Server01
1=winrv:1=userServer!Initialization,3 ServerDll=ssxrv,4 ProfileControl=Off MaxRequestThreads=16
536    wininit.exe
608    csrss.exe  \SystemRoot\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 Server01
1=winrv:1=userServer!Initialization,3 ServerDll=ssxrv,4 ProfileControl=Off MaxRequestThreads=16
632    winlogon.exe
672    services.exe C:\Windows\system32\services.exe
680    lsass.exe   C:\Windows\system32\lsass.exe
784    svchost.exe C:\Windows\system32\svchost.exe -k DcomLaunch -p -s PlugPlay
792    fontdrvhost.ex "fontdrvhost.exe"
800    fontdrvhost.ex "fontdrvhost.exe"
868    svchost.exe C:\Windows\system32\svchost.exe -k DcomLaunch -p
916    svchost.exe C:\Windows\system32\svchost.exe -k RPCSS -p
960    svchost.exe C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSN
964    svchost.exe C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TomService
744    svchost.exe C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
1104    svchost.exe C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s UmRdpService
1156    svchost.exe C:\Windows\system32\svchost.exe -k netwsvcs -p -s ProfSvc
1192    svchost.exe C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s SysMain
1216    svchost.exe C:\Windows\system32\svchost.exe -k netwsvcs -p -s Themes
1340    svchost.exe C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
1348    svchost.exe C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
1356    svchost.exe C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
1368    svchost.exe C:\Windows\system32\svchost.exe -k netwsvcs -p -s Schedule
1428    MemCompression -
1456    svchost.exe C:\Windows\system32\svchost.exe -k netwsvcs -s CertPropSvc
```

Tres pluggins adicionales:

```
vol3 -f memdump.mem windows.Sockets
```

```
vol3 -f memdump.mem windows.malfind
```

```
vol3 -f memdump.mem windows.clipboard
```

windows.sockets muestra todos los sockets (conexiones de red activas) abiertos por los procesos en el momento del volcado de memoria. Es especialmente útil para descubrir comunicaciones activas o sospechosas que podrían indicar conexión con servidores de comando y control (C2), túneles o exfiltración de datos.

windows.malfind busca inyecciones de código malicioso en la memoria de los procesos. Detecta regiones de memoria con permisos de lectura, escritura y ejecución simultáneos (RWX), típicos de malware que se oculta o ejecuta directamente en memoria.

`windows.clipboard` extrae el contenido del portapapeles (`clipboard`) que estaba almacenado en la memoria en el momento del volcado. Puede contener texto, comandos, contraseñas, URLs, o información sensible copiada por el usuario o un atacante.

3.- Comparativa entre Volatility 2 y 3

Volatility 2 se basa en Python 2.7, lo que limita su compatibilidad con sistemas actuales, aunque sigue siendo ampliamente usada por su amplio catálogo de plugins, su salida en texto estructurado y su madurez. Permite trabajar fácilmente con perfiles de sistemas (por ejemplo, Win7SP1x64) y ofrece una representación más visual, como en pstree, donde el árbol de procesos es claro y jerárquico. Sin embargo, su dependencia de perfiles predefinidos hace que analizar sistemas nuevos o sin perfil oficial sea más complicado.

Por otro lado, Volatility 3 representa una reescritura completa en Python 3, enfocada en modularidad, rendimiento y extensibilidad. Ya no depende de perfiles específicos, sino que detecta automáticamente la estructura de memoria del sistema, lo que la hace más flexible y moderna. Además, introduce una arquitectura de plugins más limpia, mejor soporte multiplataforma y una base de código más mantenible.

No obstante, algunos plugins de Volatility 2 aún no están disponibles en la versión 3, y la salida es menos visual por defecto, requiriendo redirecciones a archivos o tratamiento adicional para informes legibles.