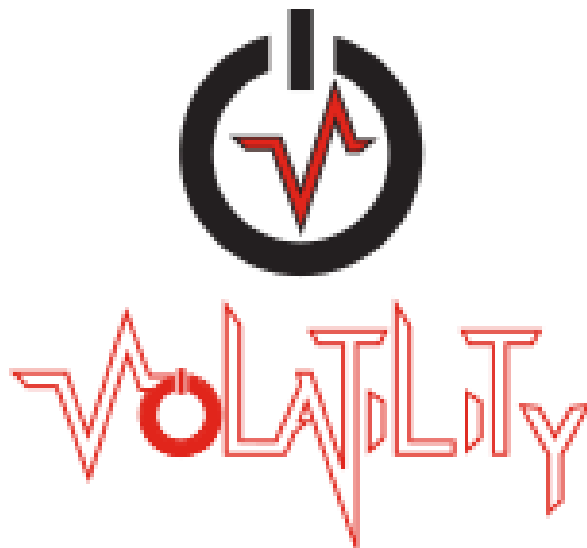


## **Tarea 2.2 - Instalación de Volatility 2 y Volatility 3 sobre un contenedor LXC**



Trabajo realizado por:

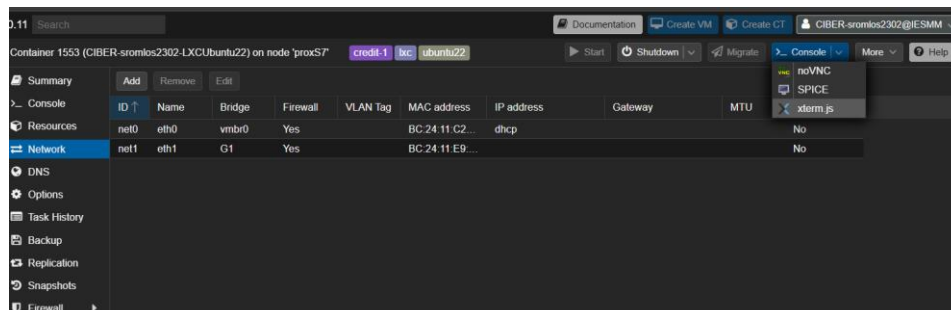
## Índice

|   |   |
|---|---|
| 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:

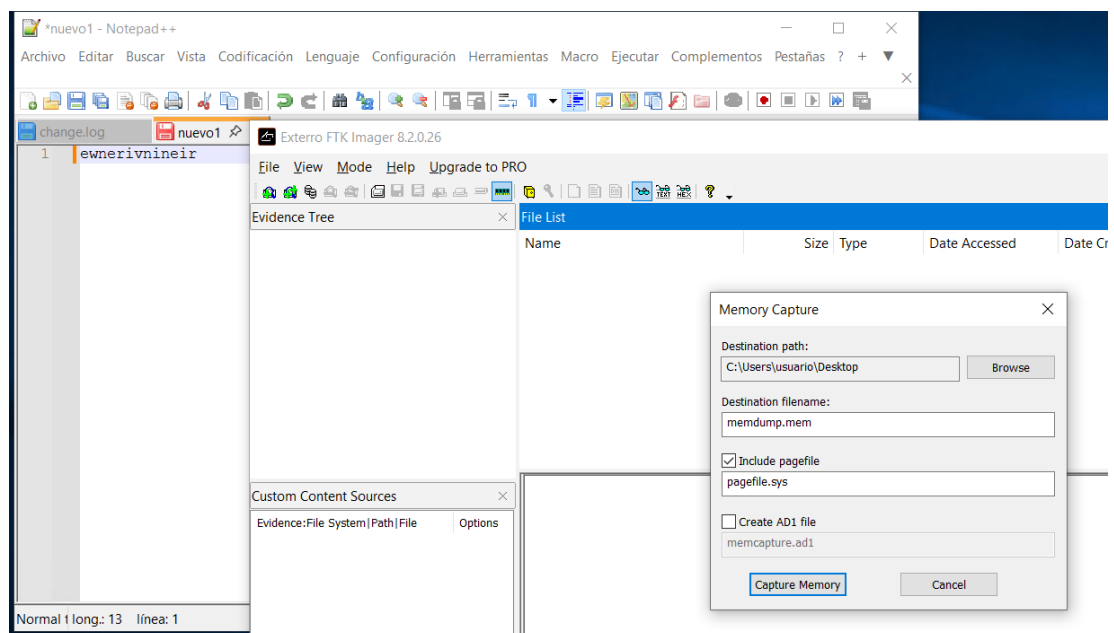
```
sudo ln -sf ~/volatility3/venv/bin/vol /usr/local/bin/vol3
```

## 2.- Uso de Volatility 2 y 3

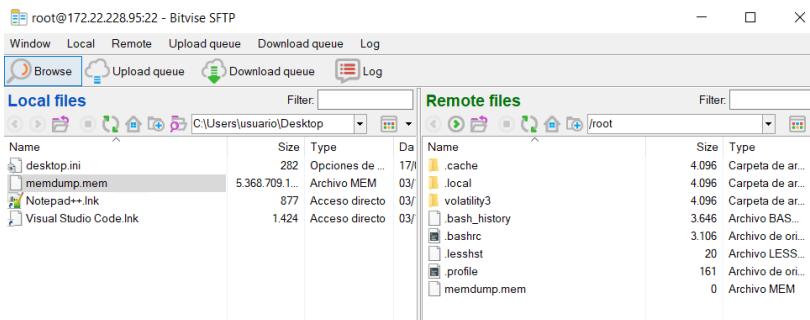
Instalo NotePad++ y CodeBlocks.



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@CI8BR-stromios2302-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/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 TimeDateStamp Tue Nov 11 22:23:06 2081
```

Para ver el listado de procesos:

vol3 -f memdump.mem windows.pslist

```
root@CI8BR-stromios2302-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 18:34:51.000000 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 0xc283523870c0 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 csrss.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
672 536 services.exe 0xc2835245f0c0 7 - 0 False 2025-11-03 18:34:56.000000 UTC N/A Disabled
680 672 lsass.exe 0xc2835245d0c0 9 - 0 False 2025-11-03 18:34:56.000000 UTC N/A Disabled
784 672 svchost.exe 0xc283524e30c0 1 - 0 False 2025-11-03 18:34:56.000000 UTC N/A Disabled
792 632 fontdrvhost.exe 0xc283525020c0 5 - 1 False 2025-11-03 18:34:56.000000 UTC N/A Disabled
800 536 fontdrvhost.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 0xc283536df0c0 11 - 0 False 2025-11-03 18:34:57.000000 UTC N/A Disabled
960 672 svchost.exe 0xc2835b1fa0c0 7 - 0 False 2025-11-03 18:34:57.000000 UTC N/A Disabled
8 672 svchost.exe 0xc2835b8ec0c0 35 - 0 False 2025-11-03 18:34:57.000000 UTC N/A Disabled
744 672 svchost.exe 0xc2835aff40c0 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 0xc2835b9f40c0 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 0xc283527ac0c0 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 0xc283527f00c0 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 0xc283528d80c0 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 0xc283529db0c0 6 - 0 False 2025-11-03 18:34:57.000000 UTC N/A Disabled
1752 672 svchost.exe 0xc283529db0c0 6 - 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

```
root@CIBER-sromlos2302-LXCUbuntu22:~# vol3 -f memdump.mem windows.pstree > pstree.txt
root@CIBER-sromlos2302-LXCUbuntu22:~# cat pstree.txt
Volatility 3 Framework 2.27.0

PID      PPID      ImageFileName      Offset(V)      Threads Handles SessionId      Wow64      CreateTime      ExitTime      Audit      Cmd      Path
4         0         System              0xc2834d864240 136           -         N/A      False      2025-11-03 18:34:51.000000 UTC N/A      -         -
* 88      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 \
456      444      csrss.exe            0xc28352370c0 11            -         N/A      False      2025-11-03 18:34:56.000000 UTC N/A      \Device\HarddiskVolume2\Windows\System32\csrss.exe \
SystemRoot\System32\smss.exe SystemRoot\System32\smss.exe
456      444      csrss.exe            0xc28352370c0 11            -         N/A      False      2025-11-03 18:34:56.000000 UTC N/A      \Device\HarddiskVolume2\Windows\System32\csrss.exe \
SystemRoot\System32\csrss.exe SystemRoot\System32\csrss.exe
ObjectDirectory=Windows SharedSection=1024,20480,768 Windows-On SubSystemType=Windows ServerDll=baseerv,1 ServerDll=winarv>UserServerDllIni
tialization,3 ServerDll=ssasrv,4 ProfileControl=Off MaxRequestThreads=16
536      444      wininit.exe          0xc283524190c0 1             -         False      2025-11-03 18:34:56.000000 UTC N/A      \Device\HarddiskVolume2\Windows\System32\wininit.ex
e
wininit.exe C:\Windows\System32\wininit.exe
536      536      services.exe         0xc283524570c0 7             -         False      2025-11-03 18:34:56.000000 UTC N/A      \Device\HarddiskVolume2\Windows\System32\services.e
xe
C:\Windows\System32\services.exe C:\Windows\System32\services.exe
** 8      672      svchost.exe          0xc2835b8ec0c0 35            -         False      2025-11-03 18:34:57.000000 UTC N/A      \Device\HarddiskVolume2\Windows\System32\svchost.exe
C:\Windows\System32\svchost.exe -s TermService
C:\Windows\System32\svchost.exe -k NetworkService -s TermService
*** 5308   8      rdclip.exe           0xc283528e8080 10            -         False      2025-11-03 18:35:41.000000 UTC N/A      \Device\HarddiskVolume2\Windows\System32\rd
clip.exe
rdclip.exe C:\Windows\System32\rdclip.exe
** 7176   672      svchost.exe          0xc28353827240 9             -         False      2025-11-03 18:35:46.000000 UTC N/A      \Device\HarddiskVolume2\Windows\System32\svchost.exe
```

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

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

```
6692      smartscreen.ex 0x7ffc92500000 0x35000 smartscreens.dll C:\Windows\System32\smartscreens.dll 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc4a200000 0xe1000 Windows.Security.Authentication.OnlineId.dll C:\Windows\System32\Windows.Security.Authentication.OnlineId.dll
2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc7b760000 0xa000 DPAPI.DLL C:\Windows\System32\DPAPI.DLL 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc48600000 0xe000 tbs.dll C:\Windows\System32\tbs.dll 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc7b700000 0x1d000 imagehlp.dll C:\Windows\System32\imagehlp.dll 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc45300000 0x18000 wksc.dll C:\Windows\System32\wksc.dll 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc9e800000 0x4e2000 WININET.dll C:\Windows\System32\WININET.dll 1 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc77700000 0x2f000 SspiCli.dll C:\Windows\System32\SspiCli.dll 1 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc2a400000 0x16000 ondemandconnroutehelper.dll C:\Windows\SYSTEM32\ondemandconnroutehelper.dll 6 2025-11-03 18:35:46.000000 UTC
abled
6692      smartscreen.ex 0x7ffc95000000 0xf0000 winhttp.dll C:\Windows\SYSTEM32\winhttp.dll 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc70600000 0x67000 mswsock.dll C:\Windows\System32\mswsock.dll 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc67e00000 0x95000 firewallapi.dll C:\Windows\System32\firewallapi.dll 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc6d900000 0xc6000 DNSAPI.dll C:\Windows\System32\DNSAPI.dll 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc7b700000 0x00000 NSI.dll C:\Windows\System32\NSI.dll 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc6d500000 0x3d000 IPHLPAPI.DLL C:\Windows\SYSTEM32\IPHLPAPI.DLL 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc67b00000 0x2d000 fwbase.dll C:\Windows\System32\fwbase.dll 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc25d00000 0xb0000 WINNSI.DLL C:\Windows\SYSTEM32\WINNSI.DLL 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc7b7a0000 0x1b000 CRYPTSP.dll C:\Windows\System32\CRYPTSP.dll 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc6b800000 0x33000 rsaenh.dll C:\Windows\System32\rsaenh.dll 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc4f300000 0xa000 rasadhlp.dll C:\Windows\System32\rasadhlp.dll 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc4e200000 0x79000 fwpucnt.dll C:\Windows\System32\fwpucnt.dll 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc6a000000 0x8c000 schannel.DLL C:\Windows\System32\channel.DLL 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc41900000 0x15000 mskeyprotect.dll C:\Windows\SYSTEM32\mskeyprotect.dll 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc77300000 0x2c000 ncrypt.dll C:\Windows\System32\ncrypt.dll 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc772f0000 0x3c000 NTASN1.dll C:\Windows\System32\NTASN1.dll 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc40e30000 0x2f000 cryptnet.dll C:\Windows\System32\cryptnet.dll 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc0c900000 0x16000 dhcpcsvc6.DLL C:\Windows\SYSTEM32\dhcpcsvc6.DLL 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc0c700000 0x1c000 dhcpcsvc.DLL C:\Windows\SYSTEM32\dhcpcsvc.DLL 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc7b700000 0x99000 webio.dll C:\Windows\SYSTEM32\webio.dll 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc41e00000 0x24000 ncryptssp.dll C:\Windows\System32\ncryptssp.dll 6 2025-11-03 18:35:46.000000 UTC Disabled
6692      smartscreen.ex 0x7ffc0d400000 0x31d000 certenroll.dll C:\Windows\System32\certenroll.dll 6 2025-11-03 18:35:46.000000 UTC Disabledroot@CIBER-sromlos2302-LXCUbuntu22:~# vol3 -f memdump.mem windows.netstat
```

```
sromlos2302-LXCUbuntu22:~# vol3 -f memdump.mem windows.netstat
Volatility 3 Framework 2.27.0
Progress: 100.00 PDB scanning finished
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

```
root@CIBER-sromlos2302-LXCUbuntu22:~# vol3 -f memdump.mem windows.netscan
```

| Volatility 3 Framework 2.27.0          |       |           |           |             |             |           |      |                |                                |  |
|--|-------|-----------|-----------|-------------|-------------|-----------|------|----------------|--------------------------------|--|
| Progress: 100.00 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 |  |
| 0xc2834da934f0                         | UDPv4 | 0.0.0.0   | 0         | *           | 0           |           | 2084 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da934f0                         | UDPv6 | ::        | 0         | *           | 0           |           | 2084 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da93660                         | UDPv4 | 0.0.0.0   | 0         | *           | 0           |           | 2084 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da93660                         | UDPv6 | ::        | 0         | *           | 0           |           | 2084 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da947a0                         | UDPv4 | 0.0.0.0   | 0         | *           | 0           |           | 4    | System         | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da94910                         | UDPv4 | 0.0.0.0   | 0         | *           | 0           |           | 2084 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da95bc0                         | UDPv4 | 0.0.0.0   | 0         | *           | 0           |           | 4    | System         | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da962f0                         | UDPv4 | 0.0.0.0   | 0         | *           | 0           |           | 4064 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da962f0                         | UDPv6 | ::        | 0         | *           | 0           |           | 4064 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da96e70                         | UDPv4 | 0.0.0.0   | 0         | *           | 0           |           | 2084 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da972c0                         | UDPv4 | 0.0.0.0   | 0         | *           | 0           |           | 2084 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da972c0                         | UDPv6 | ::        | 0         | *           | 0           |           | 2084 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da97880                         | UDPv4 | 0.0.0.0   | 0         | *           | 0           |           | 4064 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da97880                         | UDPv6 | ::        | 0         | *           | 0           |           | 4064 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da979f0                         | UDPv4 | 0.0.0.0   | 0         | *           | 0           |           | 4064 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da97cd0                         | UDPv4 | 0.0.0.0   | 0         | *           | 0           |           | 4064 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da98850                         | UDPv4 | 0.0.0.0   | 0         | *           | 0           |           | 4500 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da989c0                         | UDPv4 | 0.0.0.0   | 0         | *           | 0           |           | 4500 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da989c0                         | UDPv6 | ::        | 0         | *           | 0           |           | 4500 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da98b30                         | UDPv4 | 0.0.0.0   | 0         | *           | 0           |           | 4500 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da98b30                         | UDPv6 | ::        | 0         | *           | 0           |           | 4500 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da98ca0                         | UDPv4 | 0.0.0.0   | 0         | *           | 0           |           | 4500 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da99820                         | UDPv4 | 0.0.0.0   | 0         | *           | 0           |           | 4064 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da99820                         | UDPv6 | ::        | 0         | *           | 0           |           | 4064 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da99b00                         | UDPv4 | 0.0.0.0   | 0         | *           | 0           |           | 4064 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da99c70                         | UDPv4 | 0.0.0.0   | 0         | *           | 0           |           | 4500 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da9aad0                         | UDPv4 | 0.0.0.0   | 0         | *           | 0           |           | 4064 | svchost.exe    | 2025-11-03 18:35:09.000000 UTC |  |
| 0xc2834da9aad0                         | 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

|      |                  |                |          |                      |  |    |                                |          |
|------|------------------|----------------|----------|----------------------|--|----|--------------------------------|----------|
| 3392 | comhost.exe      | 0x7ffc78e00000 | 0x5d000  | powrprof.dll         | C:\Windows\System32\powrprof.dll         | 6  | 2025-11-03 18:47:44.000000 UTC | Disabled |
| 3392 | comhost.exe      | 0x7ffc78e00000 | 0x52000  | shlwapi.dll          | C:\Windows\System32\shlwapi.dll          | 6  | 2025-11-03 18:47:44.000000 UTC | Disabled |
| 3392 | comhost.exe      | 0x7ffc78e00000 | 0x11000  | kernel.appcore.dll   | C:\Windows\System32\kernel.appcore.dll   | 6  | 2025-11-03 18:47:44.000000 UTC | Disabled |
| 3392 | comhost.exe      | 0x7ffc78e00000 | 0x1b000  | cryptsp.dll          | C:\Windows\System32\cryptsp.dll          | 6  | 2025-11-03 18:47:44.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc7e1c0000 | 0x3f000  | SearchFilterHost.exe | C:\Windows\system32\SearchFilterHost.exe | -1 | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc7e1c0000 | 0x1ee000 | ntdll.dll            | C:\Windows\SYSTEM32\ntdll.dll            | -1 | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc7e1c0000 | 0x03000  | KERNEL32.DLL         | C:\Windows\System32\KERNEL32.DLL         | -1 | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc7e1c0000 | 0x294000 | KERNELBASE.dll       | C:\Windows\System32\KERNELBASE.dll       | -1 | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc79780000 | 0x9e000  | msvcrt.dll           | C:\Windows\System32\msvcrt.dll           | 6  | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc78ae0000 | 0xc4000  | OLEAUT32.dll         | C:\Windows\System32\OLEAUT32.dll         | 6  | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc770d0000 | 0xa0000  | msvcrt_win.dll       | C:\Windows\System32\msvcrt_win.dll       | 6  | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc77a00000 | 0x2af000 | ucrtbase.dll         | C:\Windows\System32\ucrtbase.dll         | 6  | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc78e00000 | 0x32a000 | combase.dll          | C:\Windows\System32\combase.dll          | 6  | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc79a10000 | 0x118000 | RPCRT4.dll           | C:\Windows\System32\RPCRT4.dll           | 6  | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc79700000 | 0x82000  | bcryptPrimitives.dll | C:\Windows\System32\bcryptPrimitives.dll | 6  | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc79e20000 | 0xa8000  | advapi32.dll         | C:\Windows\System32\advapi32.dll         | 6  | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc79ca0000 | 0xa2000  | sechost.dll          | C:\Windows\System32\sechost.dll          | 6  | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc79400000 | 0x26000  | bcrypt.dll           | C:\Windows\System32\bcrypt.dll           | 6  | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc7a3d0000 | 0x334000 | TQUERY.DLL           | C:\Windows\system32\TQUERY.DLL           | 6  | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc770d0000 | 0x15900  | cryptdll.dll         | C:\Windows\system32\cryptdll.dll         | 6  | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc79410000 | 0x2e000  | imm32.dll            | C:\Windows\System32\imm32.dll            | 6  | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc78e00000 | 0x197000 | USER32.dll           | C:\Windows\System32\USER32.dll           | 6  | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc7f700000 | 0x20000  | win32u.dll           | C:\Windows\System32\win32u.dll           | 6  | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc79570000 | 0x29000  | GDI32.dll            | C:\Windows\System32\GDI32.dll            | 6  | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc77dc0000 | 0x1a8000 | gdi32full.dll        | C:\Windows\System32\gdi32full.dll        | 6  | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc77890000 | 0x11000  | kernel.appcore.dll   | C:\Windows\System32\kernel.appcore.dll   | 6  | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc79360000 | 0xa8000  | clbcatq.dll          | C:\Windows\System32\clbcatq.dll          | 6  | 2025-11-03 18:47:47.000000 UTC | Disabled |
| 7712 | SearchFilterHost | 0x7ffc7ed00000 | 0x28000  | masprxy.dll          | C:\Windows\system32\masprxy.dll          | 6  | 2025-11-03 18:47:47.000000 UTC | Disabled |

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-sromlos2302-1XUbuntu22:~# 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=baserv,1 ServerDll=winlsrv:UserServerDllInitialization,3 ServerDll=ssxsr,4 ProfileControl=Off MaxRequestThreads=16
536 wininit.exe wininit.exe
548 csrss.exe \SystemRoot\System32\csrss.exe ObjectDirectory=Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=baserv,1 ServerDll=winlsrv:UserServerDllInitialization,3 ServerDll=ssxsr,4 ProfileControl=Off MaxRequestThreads=16
632 winlogon.exe 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.exe "fontdrvhost.exe"
800 fontdrvhost.exe "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 LSM
8 svchost.exe C:\Windows\System32\svchost.exe -k NetworkService -s TermService
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
1186 svchost.exe C:\Windows\System32\svchost.exe -k netsvcs -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 netsvcs -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 netsvcs -p -s Schedule
1428 MemCompression -
1456 svchost.exe C:\Windows\System32\svchost.exe -k netsvcs -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.