INSTALACIÓN DE VOLATILITY 2 Y VOLATILITY 3 SOBRE UN CONTENEDOR LXC

ANALISIS FORENSE EN CIBERSEGURIDAD INFORMÁTICA

28 DE OCTUBRE DE 2023

IES MARITINEZ MONTAÑES

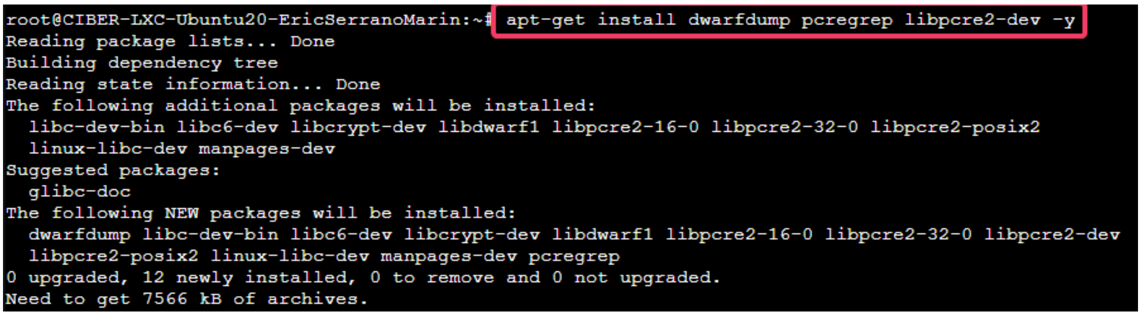
ERIC SERRANO MARÍN

INDICE

INSTALACIÓN VOLATILITY 2

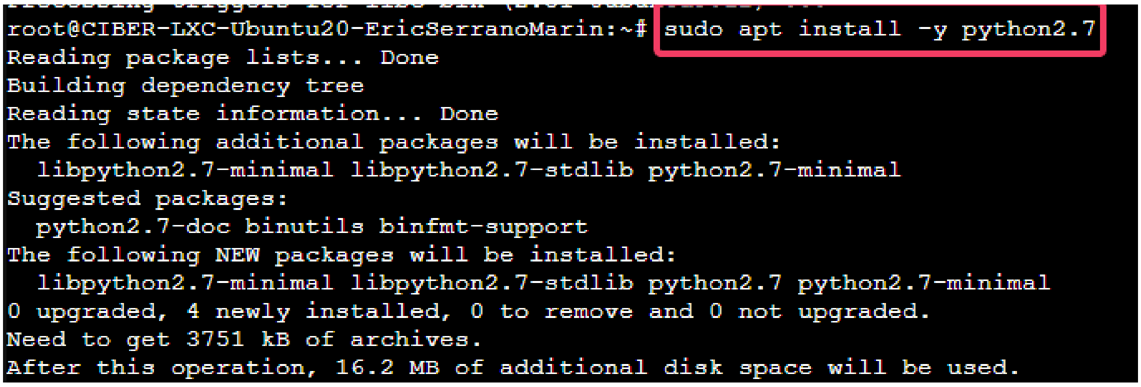
Primero actualizaremos los paquetes con los siguientes comandos **apt update** y **apt dist-upgrade.**

Vamos a instalar los paquetes dependientes de Python. **apt-get install dwarfdump pcregrep libpcre2-dev -y**:



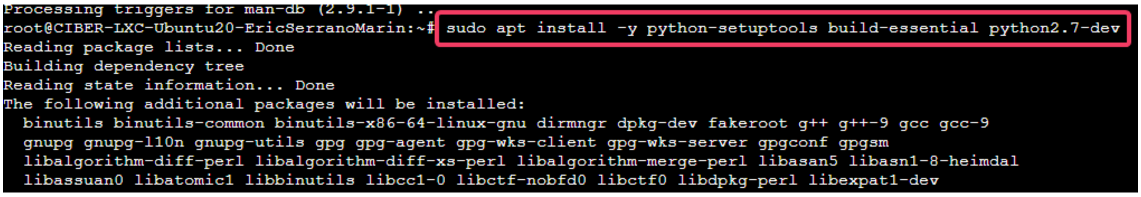
```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# apt-get install dwarfdump pcregrep libpcre2-dev -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libc-dev-bin libc6-dev libcrypt-dev libdwarf1 libpcre2-16-0 libpcre2-32-0 libpcre2-posix2
  linux-libc-dev manpages-dev
Suggested packages:
  glibc-doc
The following NEW packages will be installed:
  dwarfdump libc-dev-bin libc6-dev libcrypt-dev libdwarf1 libpcre2-16-0 libpcre2-32-0 libpcre2-dev
  libpcre2-posix2 linux-libc-dev manpages-dev pcregrep
0 upgraded, 12 newly installed, 0 to remove and 0 not upgraded.
Need to get 7566 kB of archives.
```

Instalaremos la última versión de Python:



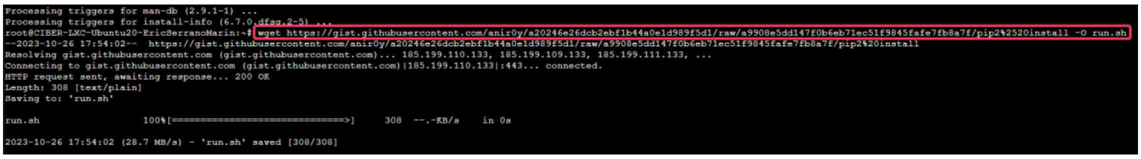
```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# sudo apt install -y python2.7
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libpython2.7-minimal libpython2.7-stdlib python2.7-minimal
Suggested packages:
  python2.7-doc binutils binfmt-support
The following NEW packages will be installed:
  libpython2.7-minimal libpython2.7-stdlib python2.7 python2.7-minimal
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 3751 kB of archives.
After this operation, 16.2 MB of additional disk space will be used.
```

Más dependencias de Python:



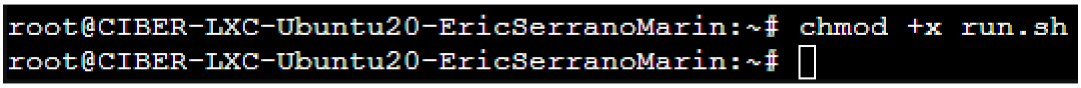
```
Processing triggers for man-db (2.9.1-1) ...
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# sudo apt install -y python-setuptools build-essential python2.7-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu dirmngr dpkg-dev fakeroot g++ g++-9 gcc gcc-9
  gnupg gnupg-l10n gnupg-utils gpg gpg-agent gpg-wks-client gpg-wks-server gpgconf gpgsm
  libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan5 libasn1-8-heimdal
  libassuan0 libatomic1 libbinutils libcc1-0 libctf-nobfd0 libctf0 libdpkg-perl libexpat1-dev
```

Descargamos de GitHub el siguiente repositorio:



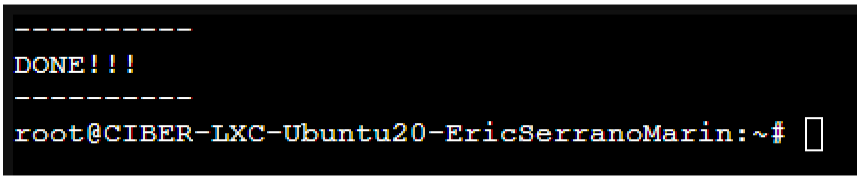
```
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for install-info (6.7.0.dfsg.2-5) ...
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# wget https://gist.githubusercontent.com/anir0y/a20246e26dcb2ebf1b44a0e1d989f5d1/raw/a9908e5dd147f0b6eb71ec51f9845fafe7fb8a7f/pip2%2520install -O run.sh
--2023-10-26 17:54:02--  https://gist.githubusercontent.com/anir0y/a20246e26dcb2ebf1b44a0e1d989f5d1/raw/a9908e5dd147f0b6eb71ec51f9845fafe7fb8a7f/pip2%20install
Resolving gist.githubusercontent.com (gist.githubusercontent.com)... 185.199.110.133, 185.199.109.133, 185.199.111.133, ...
Connecting to gist.githubusercontent.com (gist.githubusercontent.com)|185.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 308 [text/plain]
Saving to: 'run.sh'

run.sh                  100%[===================================>]     308  --.-KB/s    in 0s

2023-10-26 17:54:02 (28.7 MB/s) - 'run.sh' saved [308/308]
```

Le damos permisos de ejecución a run.sh



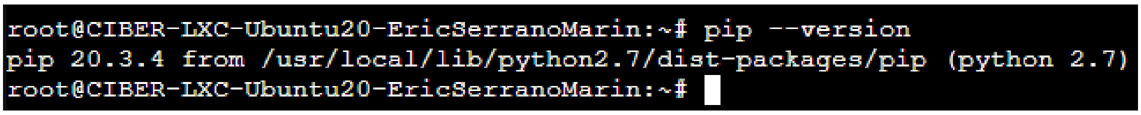
```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# chmod +x run.sh
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~#
```

Y acto seguido ejecutamos el archivo**: ./run.sh**



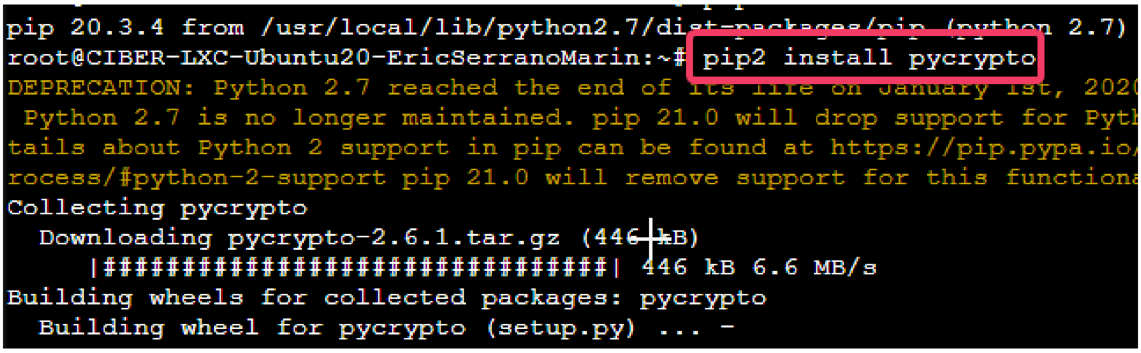
```
----------
DONE!!!
----------
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# 
```

Comprobación de versión de pip: **pip --version**



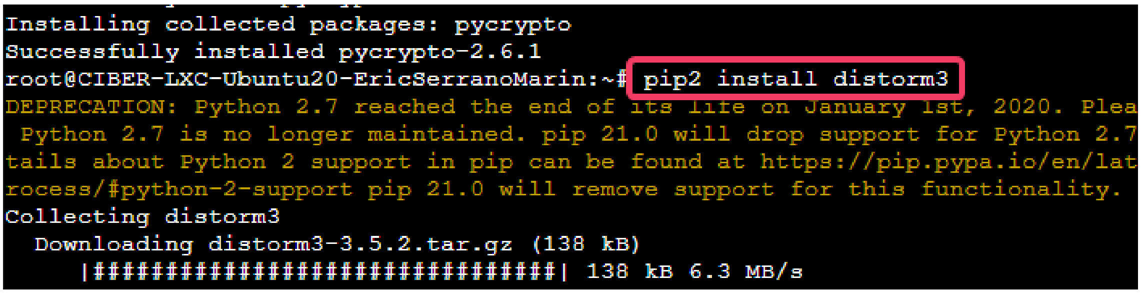
```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# pip --version
pip 20.3.4 from /usr/local/lib/python2.7/dist-packages/pip (python 2.7)
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# 
```

Instalación pycrypto: **pip2 install pycrypto**



```
pip 20.3.4 from /usr/local/lib/python2.7/dist-packages/pip (python 2.7)
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# pip2 install pycrypto
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 202
 Python 2.7 is no longer maintained. pip 21.0 will drop support for Pyth
tails about Python 2 support in pip can be found at https://pip.pypa.io/
rocess/#python-2-support pip 21.0 will remove support for this functiona
Collecting pycrypto
  Downloading pycrypto-2.6.1.tar.gz (446 kB)
     |████████████████████████████████| 446 kB 6.6 MB/s
Building wheels for collected packages: pycrypto
  Building wheel for pycrypto (setup.py) ... -
```

Instalación distorm3: **pip2 install distorm3**

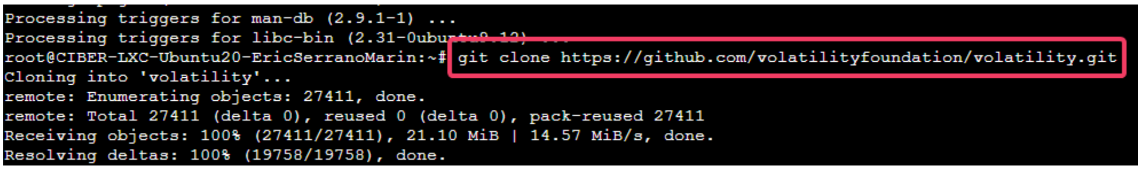


```
Installing collected packages: pycrypto
Successfully installed pycrypto-2.6.1
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# pip2 install distorm3
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Plea
 Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7
tails about Python 2 support in pip can be found at https://pip.pypa.io/en/lat
rocess/#python-2-support pip 21.0 will remove support for this functionality.
Collecting distorm3
  Downloading distorm3-3.5.2.tar.gz (138 kB)
     |████████████████████████████████| 138 kB 6.3 MB/s
```

Ahora estamos preparados para instalar volatility.

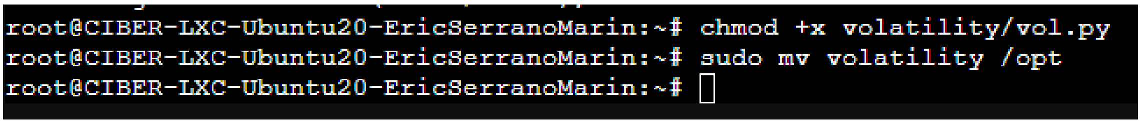
Empezaremos instalando git, para poder clonar el repositorio. **apt install git**

Para clonarlo usaremos **git clone**:



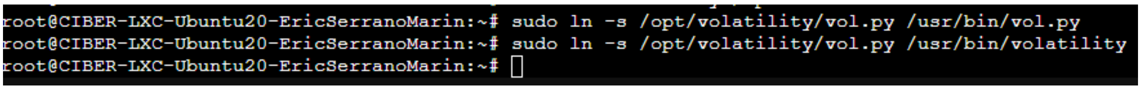
```
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.12) ...
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# git clone https://github.com/volatilityfoundation/volatility.git
Cloning into 'volatility'...
remote: Enumerating objects: 27411, done.
remote: Total 27411 (delta 0), reused 0 (delta 0), pack-reused 27411
Receiving objects: 100% (27411/27411), 21.10 MiB | 14.57 MiB/s, done.
Resolving deltas: 100% (19758/19758), done.
```

Daremos permisos y después lo moveremos: **chmod +x volatility/vol.py** y sudo **mv volatility /opt.**



```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# chmod +x volatility/vol.py
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# sudo mv volatility /opt
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# 
```

Vamos a crear enlaces simbólicos:

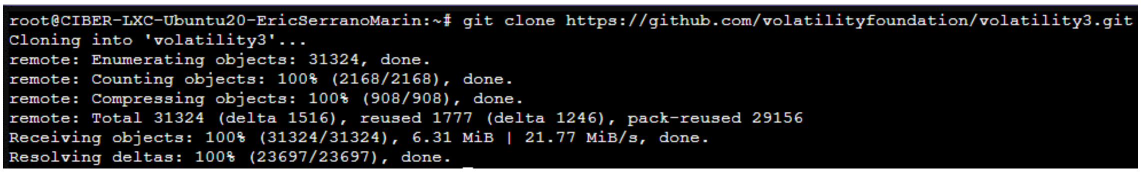


```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# sudo ln -s /opt/volatility/vol.py /usr/bin/vol.py
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# sudo ln -s /opt/volatility/vol.py /usr/bin/volatility
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# 
```

Por último, comprobaremos con los comandos **vol.py --info** y **volatility --info**. En mi caso todo salió correctamente.

INSTALACIÓN VOLATILITY 3

Clonamos repositorio: **git clone** https://github.com/volatilityfoundation/volatility3.git

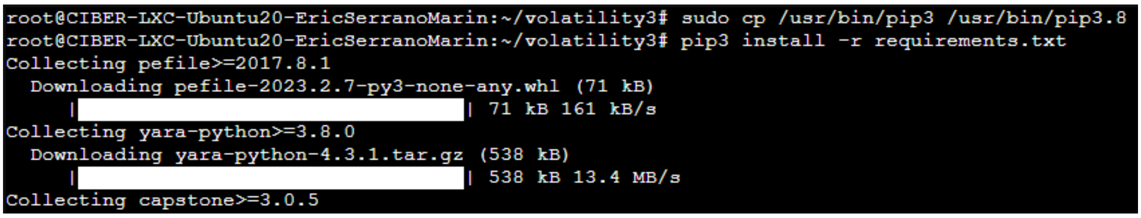


```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# git clone https://github.com/volatilityfoundation/volatility3.git
Cloning into 'volatility3'...
remote: Enumerating objects: 31324, done.
remote: Counting objects: 100% (2168/2168), done.
remote: Compressing objects: 100% (908/908), done.
remote: Total 31324 (delta 1516), reused 1777 (delta 1246), pack-reused 29156
Receiving objects: 100% (31324/31324), 6.31 MiB | 21.77 MiB/s, done.
Resolving deltas: 100% (23697/23697), done.
```

Instalamos las dependencias de volatility3, pip3, compiladores C y librería SSL.

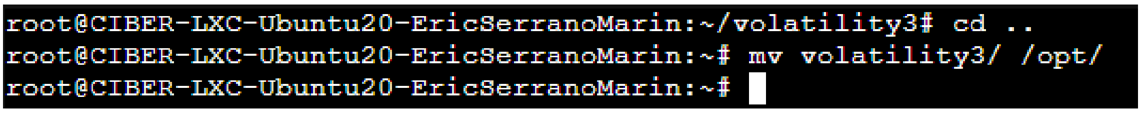
apt install python3-pip, apt-get install c++ build-essentials gcc g++, apt-get install libssl-dev.

Después de estas instalaciones sencillas, copiaremos pip3 para que se llame pip3.8.



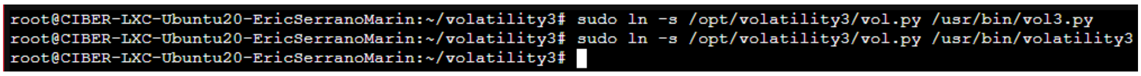
```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~/volatility3# sudo cp /usr/bin/pip3 /usr/bin/pip3.8
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~/volatility3# pip3 install -r requirements.txt
Collecting pefile>=2017.8.1
  Downloading pefile-2023.2.7-py3-none-any.whl (71 kB)
     |████████████████████████████████| 71 kB 161 kB/s
Collecting yara-python>=3.8.0
  Downloading yara-python-4.3.1.tar.gz (538 kB)
     |████████████████████████████████| 538 kB 13.4 MB/s
Collecting capstone>=3.0.5
```

Movemos volatility3 al path:



```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~/volatility3# cd ..
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# mv volatility3/ /opt/
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# 
```

Creamos los enlaces simbólicos:

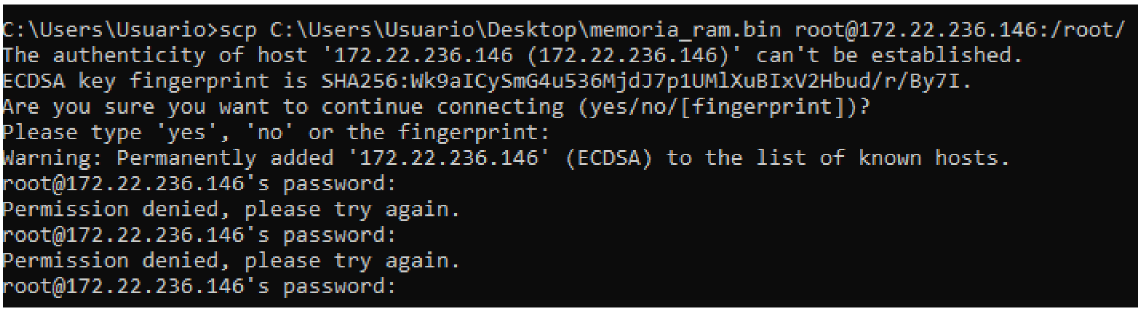


```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~/volatility3# sudo ln -s /opt/volatility3/vol.py /usr/bin/vol3.py
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~/volatility3# sudo ln -s /opt/volatility3/vol.py /usr/bin/volatility3
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~/volatility3# 
```

Probamos vol.py y vol3.py y funcionan correctamente.

PASANDO COPIA DE LA MEMORIA RAM DE UNA MV WINDOWS A CONTENEDOR LINUX

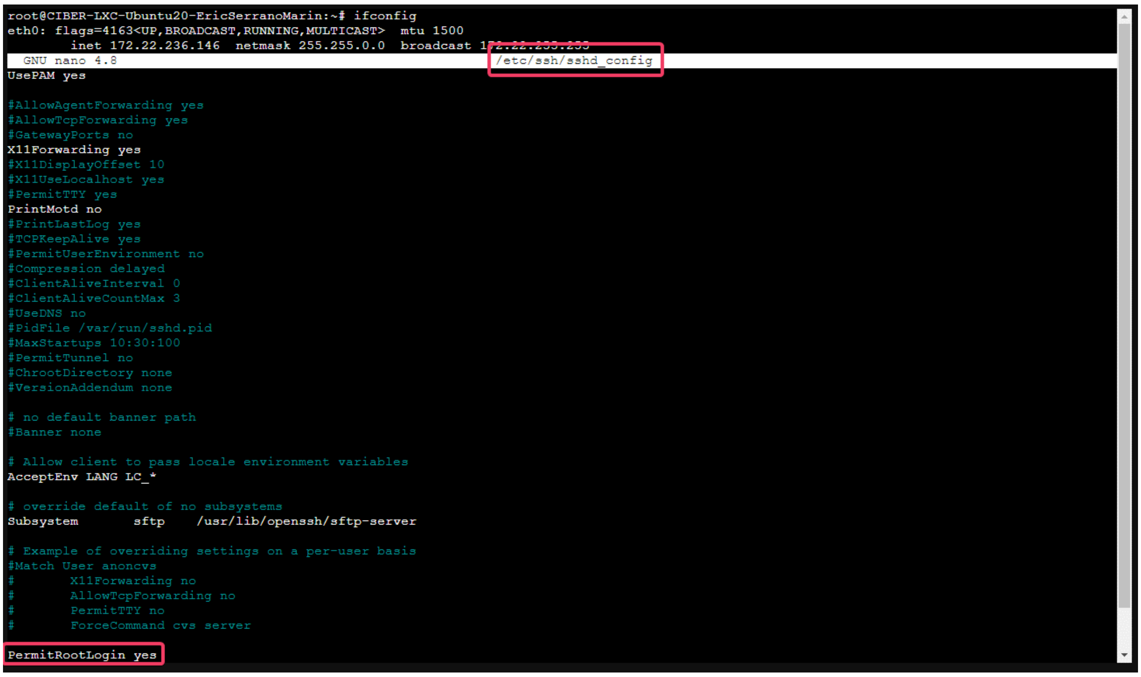
Como podemos observar nos deniega el permiso al poner la contraseña.



```
C:\Users\Usuario>scp C:\Users\Usuario\Desktop\memoria_ram.bin root@172.22.236.146:/root/
The authenticity of host '172.22.236.146 (172.22.236.146)' can't be established.
ECDSA key fingerprint is SHA256:Wk9aICySmG4u536MjdJ7p1UMlXuBIxV2Hbud/r/By7I.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Please type 'yes', 'no' or the fingerprint:
Warning: Permanently added '172.22.236.146' (ECDSA) to the list of known hosts.
root@172.22.236.146's password:
Permission denied, please try again.
root@172.22.236.146's password:
Permission denied, please try again.
root@172.22.236.146's password:
```

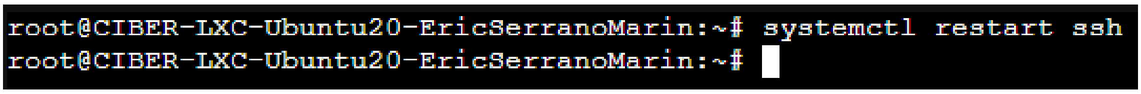
Para ello vamos a habilitar ssh root.

sudo nano **/etc/ssh/sshd_config**, después añadiremos **PermitRootLogin yes** abajo del todo.



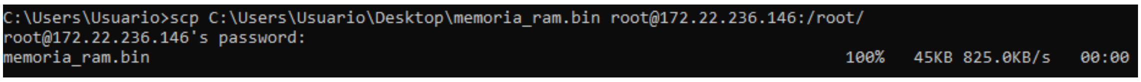
```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.22.236.146  netmask 255.255.0.0  broadcast 172.22.255.255
  GNU nano 4.8                                              /etc/ssh/sshd_config
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem       sftp    /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server

PermitRootLogin yes
```

Seguirá sin funcionar, ya que tendremos que reiniciar ssh. **systemctl restart ssh**.



```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# systemctl restart ssh
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~#
```

Aquí podemos ver como ya hemos podido pasar el archivo.



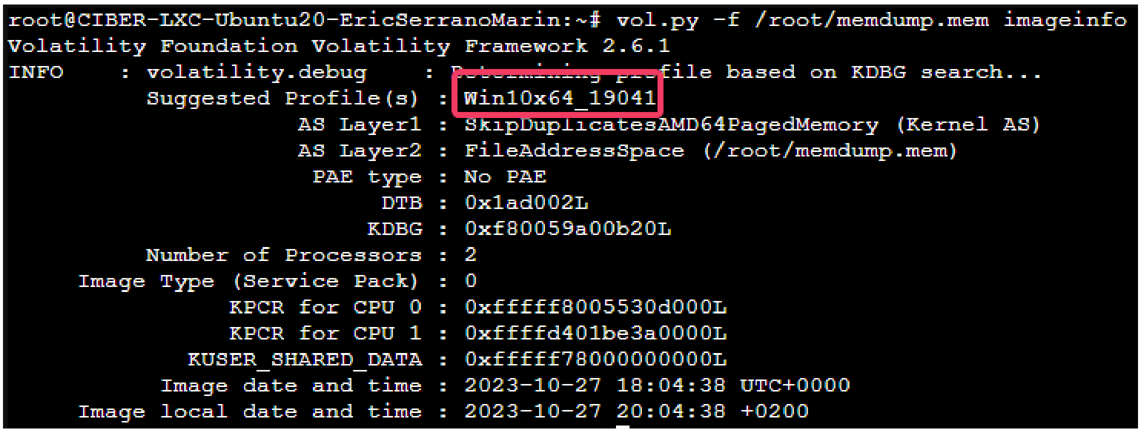
```
C:\Users\Usuario>scp C:\Users\Usuario\Desktop\memoria_ram.bin root@172.22.236.146:/root/
root@172.22.236.146's password:
memoria_ram.bin                                                     100%   45KB 825.0KB/s   00:00
```

Nota: El archivo de memoria RAM usado anteriormente no funcionaba, así que he pasado otro siguiente exactamente el mismo proceso.

INFORMACIÓN DEL SISTEMA OPERATIVO

VOLATILITY 2

vol.py -f /root/memdump.mem imageinfo



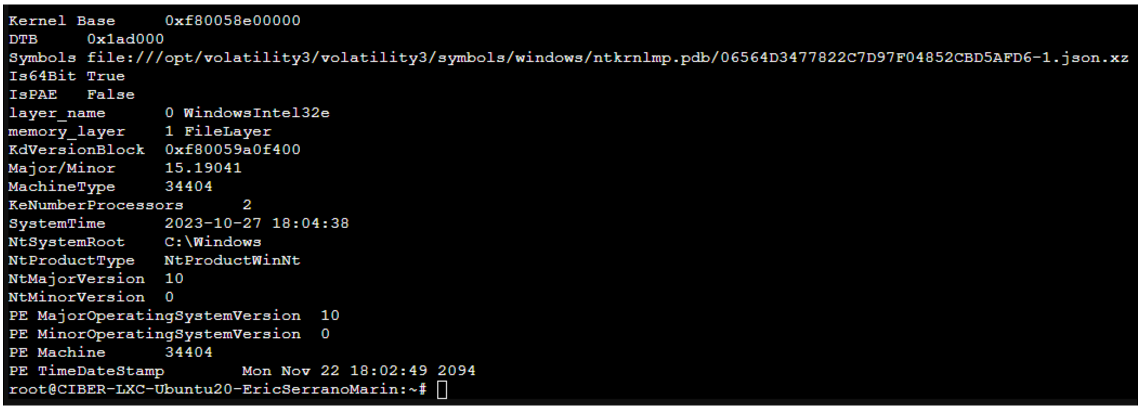
```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol.py -f /root/memdump.mem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win10x64_19041
                     AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/memdump.mem)
                      PAE type : No PAE
                           DTB : 0x1ad002L
                          KDBG : 0xf80059a00b20L
          Number of Processors : 2
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0xfffff8005530d000L
                KPCR for CPU 1 : 0xffffd401be3a0000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2023-10-27 18:04:38 UTC+0000
     Image local date and time : 2023-10-27 20:04:38 +0200
```

Win10: Indica que la imagen de RAM pertenece a una versión de Windows 10.

X64: Indica que se trata de una versión de 64bits.

19041: Indica la versión específica de Windows 10.

VOLATILITY 3



```
Kernel Base     0xf80058e00000
DTB     0x1ad000
Symbols file:///opt/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/06564D3477822C7D97F04852CBD5AFD6-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf80059a0f400
Major/Minor     15.19041
MachineType     34404
KeNumberProcessors      2
SystemTime      2023-10-27 18:04:38
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Mon Nov 22 18:02:49 2094
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# 
```

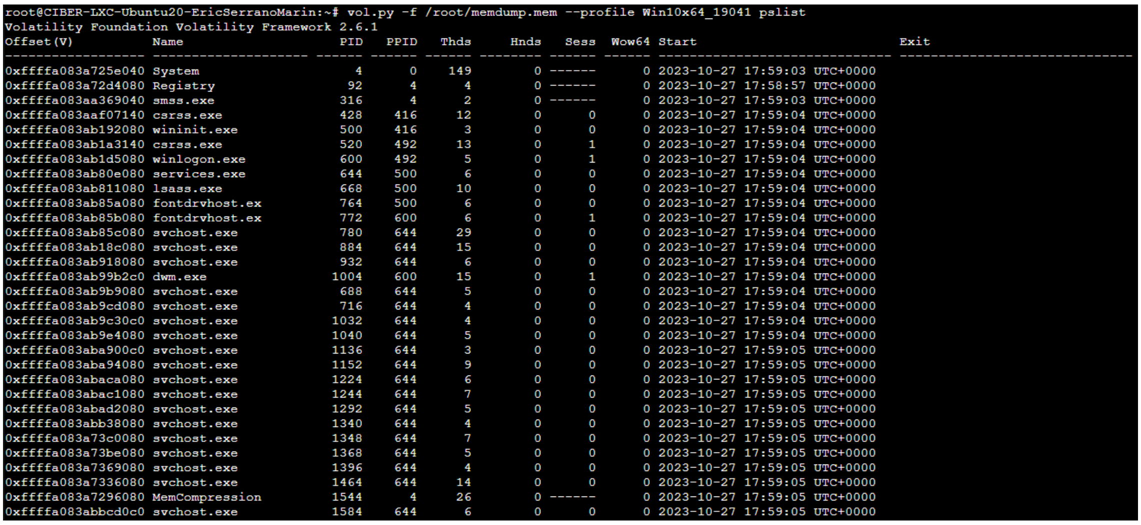
LISTADO DE PROCESOS

VOLATILITY 2

LISTADO DE PROCESOS

vol.py -f “/path/to/file” --profile <profile> pslist -> | <profile> será Suggested Profile(s) de la captura anterior.

vol.py -f /root/memdump.mem –profile Win10x64_19041 pslist.

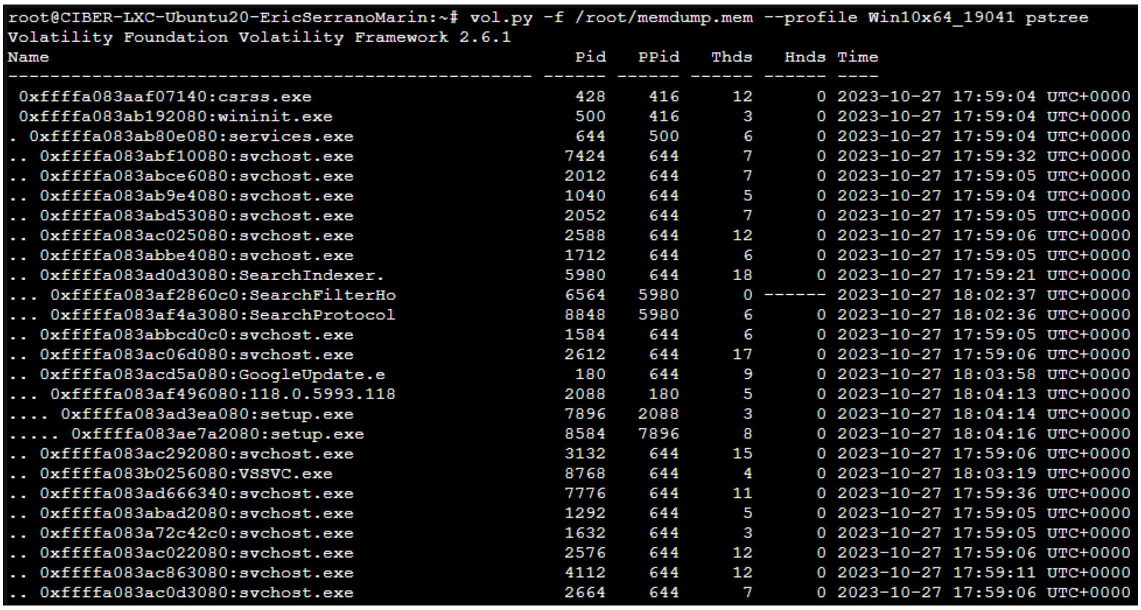


```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol.py -f /root/memdump.mem --profile Win10x64_19041 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xffffa083a725e040 System                    4      0    149        0 ------      0 2023-10-27 17:59:03 UTC+0000
0xffffa083a72d4080 Registry                 92      4      4        0 ------      0 2023-10-27 17:58:57 UTC+0000
0xffffa083aa369040 smss.exe                316      4      2        0 ------      0 2023-10-27 17:59:03 UTC+0000
0xffffa083aaf07140 csrss.exe               428    416     12        0      0      0 2023-10-27 17:59:04 UTC+0000
0xffffa083ab192080 wininit.exe             500    416      3        0      0      0 2023-10-27 17:59:04 UTC+0000
0xffffa083ab1a3140 csrss.exe               520    492     13        0      1      0 2023-10-27 17:59:04 UTC+0000
0xffffa083ab1d5080 winlogon.exe            600    492      5        0      1      0 2023-10-27 17:59:04 UTC+0000
0xffffa083ab80e080 services.exe            644    500      6        0      0      0 2023-10-27 17:59:04 UTC+0000
0xffffa083ab811080 lsass.exe               668    500     10        0      0      0 2023-10-27 17:59:04 UTC+0000
0xffffa083ab85a080 fontdrvhost.ex          764    500      6        0      0      0 2023-10-27 17:59:04 UTC+0000
0xffffa083ab85b080 fontdrvhost.ex          772    600      6        0      1      0 2023-10-27 17:59:04 UTC+0000
0xffffa083ab85c080 svchost.exe             780    644     29        0      0      0 2023-10-27 17:59:04 UTC+0000
0xffffa083ab18c080 svchost.exe             884    644     15        0      0      0 2023-10-27 17:59:04 UTC+0000
0xffffa083ab918080 svchost.exe             932    644      6        0      0      0 2023-10-27 17:59:04 UTC+0000
0xffffa083ab99b2c0 dwm.exe                1004    600     15        0      1      0 2023-10-27 17:59:04 UTC+0000
0xffffa083ab9b9080 svchost.exe             688    644      5        0      0      0 2023-10-27 17:59:04 UTC+0000
0xffffa083ab9cd080 svchost.exe             716    644      4        0      0      0 2023-10-27 17:59:04 UTC+0000
0xffffa083ab9c30c0 svchost.exe            1032    644      4        0      0      0 2023-10-27 17:59:04 UTC+0000
0xffffa083ab9e4080 svchost.exe            1040    644      5        0      0      0 2023-10-27 17:59:04 UTC+0000
0xffffa083aba900c0 svchost.exe            1136    644      3        0      0      0 2023-10-27 17:59:05 UTC+0000
0xffffa083aba94080 svchost.exe            1152    644      9        0      0      0 2023-10-27 17:59:05 UTC+0000
0xffffa083abaca080 svchost.exe            1224    644      6        0      0      0 2023-10-27 17:59:05 UTC+0000
0xffffa083abac1080 svchost.exe            1244    644      7        0      0      0 2023-10-27 17:59:05 UTC+0000
0xffffa083abad2080 svchost.exe            1292    644      5        0      0      0 2023-10-27 17:59:05 UTC+0000
0xffffa083abb38080 svchost.exe            1340    644      4        0      0      0 2023-10-27 17:59:05 UTC+0000
0xffffa083a73c0080 svchost.exe            1348    644      7        0      0      0 2023-10-27 17:59:05 UTC+0000
0xffffa083a73be080 svchost.exe            1368    644      5        0      0      0 2023-10-27 17:59:05 UTC+0000
0xffffa083a7369080 svchost.exe            1396    644      4        0      0      0 2023-10-27 17:59:05 UTC+0000
0xffffa083a7336080 svchost.exe            1464    644     14        0      0      0 2023-10-27 17:59:05 UTC+0000
0xffffa083a7296080 MemCompression         1544      4     26        0 ------      0 2023-10-27 17:59:05 UTC+0000
0xffffa083abbcd0c0 svchost.exe            1584    644      6        0      0      0 2023-10-27 17:59:05 UTC+0000
```

LISTADO DE PROCESOS EN FORMA DE ÁRBOL

Igual que el anterior, pero añadiendo al final **pstree**

vol.py -f /root/memdump.mem –profile Win10x64_19041 pstree.

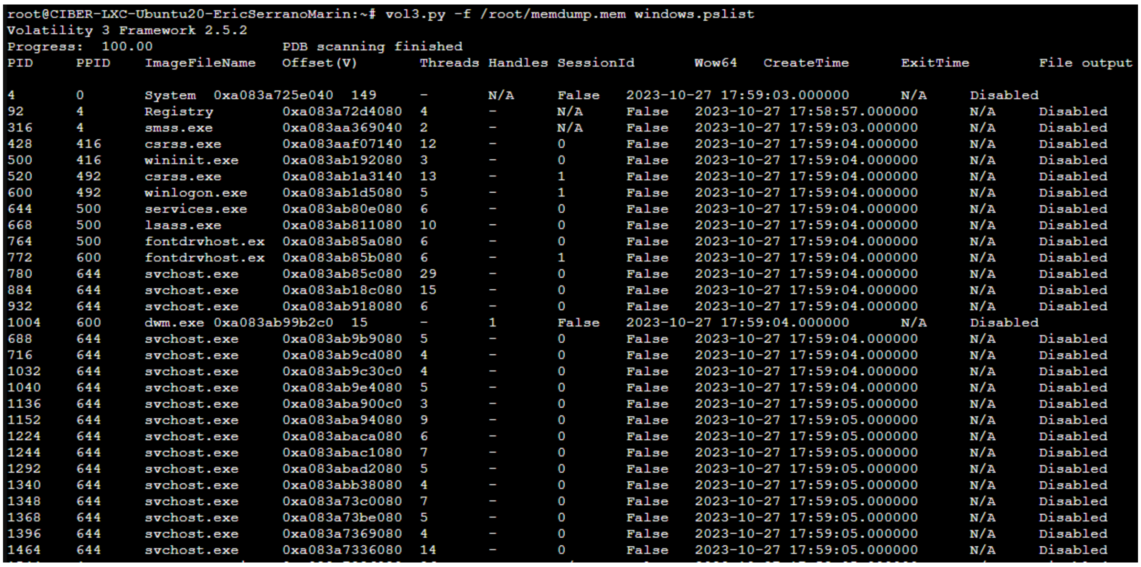


```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol.py -f /root/memdump.mem --profile Win10x64_19041 pstree
Volatility Foundation Volatility Framework 2.6.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xffffa083aaf07140:csrss.exe                         428    416     12      0 2023-10-27 17:59:04 UTC+0000
 0xffffa083ab192080:wininit.exe                       500    416      3      0 2023-10-27 17:59:04 UTC+0000
. 0xffffa083ab80e080:services.exe                     644    500      6      0 2023-10-27 17:59:04 UTC+0000
.. 0xffffa083abf10080:svchost.exe                    7424    644      7      0 2023-10-27 17:59:32 UTC+0000
.. 0xffffa083abce6080:svchost.exe                    2012    644      7      0 2023-10-27 17:59:05 UTC+0000
.. 0xffffa083ab9e4080:svchost.exe                    1040    644      5      0 2023-10-27 17:59:04 UTC+0000
.. 0xffffa083abd53080:svchost.exe                    2052    644      7      0 2023-10-27 17:59:05 UTC+0000
.. 0xffffa083ac025080:svchost.exe                    2588    644     12      0 2023-10-27 17:59:06 UTC+0000
.. 0xffffa083abbe4080:svchost.exe                    1712    644      6      0 2023-10-27 17:59:05 UTC+0000
.. 0xffffa083ad0d3080:SearchIndexer.                 5980    644     18      0 2023-10-27 17:59:21 UTC+0000
... 0xffffa083af2860c0:SearchFilterHo                6564   5980      0 ------ 2023-10-27 18:02:37 UTC+0000
... 0xffffa083af4a3080:SearchProtocol                8848   5980      6      0 2023-10-27 18:02:36 UTC+0000
.. 0xffffa083abbcd0c0:svchost.exe                    1584    644      6      0 2023-10-27 17:59:05 UTC+0000
.. 0xffffa083ac06d080:svchost.exe                    2612    644     17      0 2023-10-27 17:59:06 UTC+0000
.. 0xffffa083acd5a080:GoogleUpdate.e                  180    644      9      0 2023-10-27 18:03:58 UTC+0000
... 0xffffa083af496080:118.0.5993.118                2088    180      5      0 2023-10-27 18:04:13 UTC+0000
.... 0xffffa083ad3ea080:setup.exe                    7896   2088      3      0 2023-10-27 18:04:14 UTC+0000
..... 0xffffa083ae7a2080:setup.exe                   8584   7896      8      0 2023-10-27 18:04:16 UTC+0000
.. 0xffffa083ac292080:svchost.exe                    3132    644     15      0 2023-10-27 17:59:06 UTC+0000
.. 0xffffa083b0256080:VSSVC.exe                      8768    644      4      0 2023-10-27 18:03:19 UTC+0000
.. 0xffffa083ad666340:svchost.exe                    7776    644     11      0 2023-10-27 17:59:36 UTC+0000
.. 0xffffa083abad2080:svchost.exe                    1292    644      5      0 2023-10-27 17:59:05 UTC+0000
.. 0xffffa083a72c42c0:svchost.exe                    1632    644      3      0 2023-10-27 17:59:05 UTC+0000
.. 0xffffa083ac022080:svchost.exe                    2576    644     12      0 2023-10-27 17:59:06 UTC+0000
.. 0xffffa083ac863080:svchost.exe                    4112    644     12      0 2023-10-27 17:59:11 UTC+0000
.. 0xffffa083ac0d3080:svchost.exe                    2664    644      7      0 2023-10-27 17:59:06 UTC+0000
```

VOLATILITY 3

LISTADO DE PROCESOS

vol3.py -f /root/memdump.mem windows.pslist

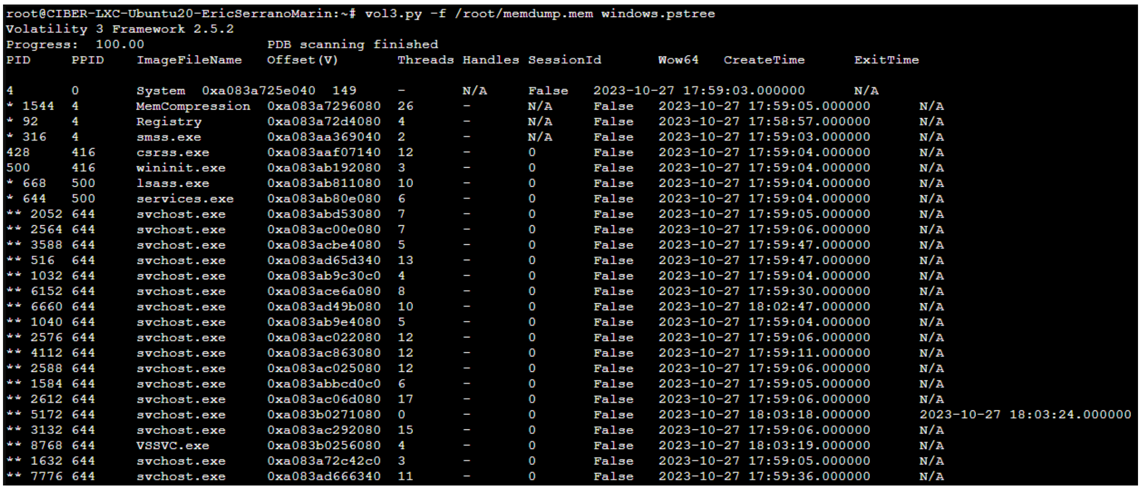


```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol3.py -f /root/memdump.mem windows.pslist
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xa083a725e040  149     -       N/A     False   2023-10-27 17:59:03.000000      N/A     Disabled
92      4       Registry        0xa083a72d4080  4       -       N/A     False   2023-10-27 17:58:57.000000      N/A     Disabled
316     4       smss.exe        0xa083aa369040  2       -       N/A     False   2023-10-27 17:59:03.000000      N/A     Disabled
428     416     csrss.exe       0xa083aaf07140  12      -       0       False   2023-10-27 17:59:04.000000      N/A     Disabled
500     416     wininit.exe     0xa083ab192080  3       -       0       False   2023-10-27 17:59:04.000000      N/A     Disabled
520     492     csrss.exe       0xa083ab1a3140  13      -       1       False   2023-10-27 17:59:04.000000      N/A     Disabled
600     492     winlogon.exe    0xa083ab1d5080  5       -       1       False   2023-10-27 17:59:04.000000      N/A     Disabled
644     500     services.exe    0xa083ab80e080  6       -       0       False   2023-10-27 17:59:04.000000      N/A     Disabled
668     500     lsass.exe       0xa083ab811080  10      -       0       False   2023-10-27 17:59:04.000000      N/A     Disabled
764     500     fontdrvhost.ex  0xa083ab85a080  6       -       0       False   2023-10-27 17:59:04.000000      N/A     Disabled
772     600     fontdrvhost.ex  0xa083ab85b080  6       -       1       False   2023-10-27 17:59:04.000000      N/A     Disabled
780     644     svchost.exe     0xa083ab85c080  29      -       0       False   2023-10-27 17:59:04.000000      N/A     Disabled
884     644     svchost.exe     0xa083ab18c080  15      -       0       False   2023-10-27 17:59:04.000000      N/A     Disabled
932     644     svchost.exe     0xa083ab918080  6       -       0       False   2023-10-27 17:59:04.000000      N/A     Disabled
1004    600     dwm.exe 0xa083ab99b2c0  15      -       1       False   2023-10-27 17:59:04.000000      N/A     Disabled
688     644     svchost.exe     0xa083ab9b9080  5       -       0       False   2023-10-27 17:59:04.000000      N/A     Disabled
716     644     svchost.exe     0xa083ab9cd080  4       -       0       False   2023-10-27 17:59:04.000000      N/A     Disabled
1032    644     svchost.exe     0xa083ab9c30c0  4       -       0       False   2023-10-27 17:59:04.000000      N/A     Disabled
1040    644     svchost.exe     0xa083ab9e4080  5       -       0       False   2023-10-27 17:59:04.000000      N/A     Disabled
1136    644     svchost.exe     0xa083aba900c0  3       -       0       False   2023-10-27 17:59:05.000000      N/A     Disabled
1152    644     svchost.exe     0xa083aba94080  9       -       0       False   2023-10-27 17:59:05.000000      N/A     Disabled
1224    644     svchost.exe     0xa083abaca080  6       -       0       False   2023-10-27 17:59:05.000000      N/A     Disabled
1244    644     svchost.exe     0xa083abac1080  7       -       0       False   2023-10-27 17:59:05.000000      N/A     Disabled
1292    644     svchost.exe     0xa083abad2080  5       -       0       False   2023-10-27 17:59:05.000000      N/A     Disabled
1340    644     svchost.exe     0xa083abb38080  4       -       0       False   2023-10-27 17:59:05.000000      N/A     Disabled
1348    644     svchost.exe     0xa083a73c0080  7       -       0       False   2023-10-27 17:59:05.000000      N/A     Disabled
1368    644     svchost.exe     0xa083a73be080  5       -       0       False   2023-10-27 17:59:05.000000      N/A     Disabled
1396    644     svchost.exe     0xa083a7369080  4       -       0       False   2023-10-27 17:59:05.000000      N/A     Disabled
1464    644     svchost.exe     0xa083a7336080  14      -       0       False   2023-10-27 17:59:05.000000      N/A     Disabled
```

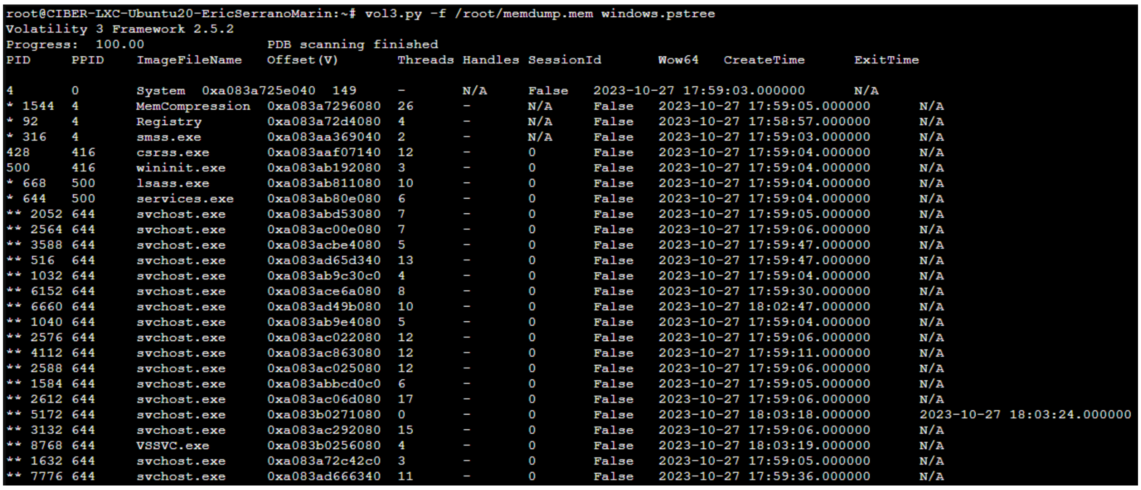
LISTADO DE PROCESOS EN ÁRBOL

Será igual que el anterior, pero con **pstree**.

vol3.py -f /root/memdump.mem windows.pstree.



```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol3.py -f /root/memdump.mem windows.pstree
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime

4       0       System  0xa083a725e040  149     -       N/A     False   2023-10-27 17:59:03.000000      N/A
* 1544  4       MemCompression  0xa083a7296080  26      -       N/A     False   2023-10-27 17:59:05.000000      N/A
* 92    4       Registry        0xa083a72d4080  4       -       N/A     False   2023-10-27 17:58:57.000000      N/A
* 316   4       smss.exe        0xa083aa369040  2       -       N/A     False   2023-10-27 17:59:03.000000      N/A
428     416     csrss.exe       0xa083aaf07140  12      -       0       False   2023-10-27 17:59:04.000000      N/A
500     416     wininit.exe     0xa083ab192080  3       -       0       False   2023-10-27 17:59:04.000000      N/A
* 668   500     lsass.exe       0xa083ab811080  10      -       0       False   2023-10-27 17:59:04.000000      N/A
* 644   500     services.exe    0xa083ab80e080  6       -       0       False   2023-10-27 17:59:04.000000      N/A
** 2052 644     svchost.exe     0xa083abd53080  7       -       0       False   2023-10-27 17:59:05.000000      N/A
** 2564 644     svchost.exe     0xa083ac00e080  7       -       0       False   2023-10-27 17:59:06.000000      N/A
** 3588 644     svchost.exe     0xa083acbe4080  5       -       0       False   2023-10-27 17:59:47.000000      N/A
** 516  644     svchost.exe     0xa083ad65d340  13      -       0       False   2023-10-27 17:59:47.000000      N/A
** 1032 644     svchost.exe     0xa083ab9c30c0  4       -       0       False   2023-10-27 17:59:04.000000      N/A
** 6152 644     svchost.exe     0xa083ace6a080  8       -       0       False   2023-10-27 17:59:30.000000      N/A
** 6660 644     svchost.exe     0xa083ad49b080  10      -       0       False   2023-10-27 18:02:47.000000      N/A
** 1040 644     svchost.exe     0xa083ab9e4080  5       -       0       False   2023-10-27 17:59:04.000000      N/A
** 2576 644     svchost.exe     0xa083ac022080  12      -       0       False   2023-10-27 17:59:06.000000      N/A
** 4112 644     svchost.exe     0xa083ac863080  12      -       0       False   2023-10-27 17:59:11.000000      N/A
** 2588 644     svchost.exe     0xa083ac025080  12      -       0       False   2023-10-27 17:59:06.000000      N/A
** 1584 644     svchost.exe     0xa083abbcd0c0  6       -       0       False   2023-10-27 17:59:05.000000      N/A
** 2612 644     svchost.exe     0xa083ac06d080  17      -       0       False   2023-10-27 17:59:06.000000      N/A
** 5172 644     svchost.exe     0xa083b0271080  0       -       0       False   2023-10-27 18:03:18.000000      2023-10-27 18:03:24.000000
** 3132 644     svchost.exe     0xa083ac292080  15      -       0       False   2023-10-27 17:59:06.000000      N/A
** 8768 644     VSSVC.exe       0xa083b0256080  4       -       0       False   2023-10-27 18:03:19.000000      N/A
** 1632 644     svchost.exe     0xa083a72c42c0  3       -       0       False   2023-10-27 17:59:05.000000      N/A
** 7776 644     svchost.exe     0xa083ad666340  11      -       0       False   2023-10-27 17:59:36.000000      N/A
```

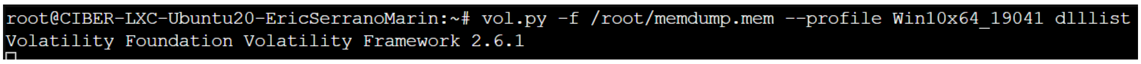


```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol3.py -f /root/memdump.mem windows.pstree
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime

4       0       System  0xa083a725e040  149     -       N/A     False   2023-10-27 17:59:03.000000      N/A
* 1544  4       MemCompression  0xa083a7296080  26      -       N/A     False   2023-10-27 17:59:05.000000      N/A
* 92    4       Registry        0xa083a72d4080  4       -       N/A     False   2023-10-27 17:58:57.000000      N/A
* 316   4       smss.exe        0xa083aa369040  2       -       N/A     False   2023-10-27 17:59:03.000000      N/A
428     416     csrss.exe       0xa083aaf07140  12      -       0       False   2023-10-27 17:59:04.000000      N/A
500     416     wininit.exe     0xa083ab192080  3       -       0       False   2023-10-27 17:59:04.000000      N/A
* 668   500     lsass.exe       0xa083ab811080  10      -       0       False   2023-10-27 17:59:04.000000      N/A
* 644   500     services.exe    0xa083ab80e080  6       -       0       False   2023-10-27 17:59:04.000000      N/A
** 2052 644     svchost.exe     0xa083abd53080  7       -       0       False   2023-10-27 17:59:05.000000      N/A
** 2564 644     svchost.exe     0xa083ac00e080  7       -       0       False   2023-10-27 17:59:06.000000      N/A
** 3588 644     svchost.exe     0xa083acbe4080  5       -       0       False   2023-10-27 17:59:47.000000      N/A
** 516  644     svchost.exe     0xa083ad65d340  13      -       0       False   2023-10-27 17:59:47.000000      N/A
** 1032 644     svchost.exe     0xa083ab9c30c0  4       -       0       False   2023-10-27 17:59:04.000000      N/A
** 6152 644     svchost.exe     0xa083ace6a080  8       -       0       False   2023-10-27 17:59:30.000000      N/A
** 6660 644     svchost.exe     0xa083ad49b080  10      -       0       False   2023-10-27 18:02:47.000000      N/A
** 1040 644     svchost.exe     0xa083ab9e4080  5       -       0       False   2023-10-27 17:59:04.000000      N/A
** 2576 644     svchost.exe     0xa083ac022080  12      -       0       False   2023-10-27 17:59:06.000000      N/A
** 4112 644     svchost.exe     0xa083ac863080  12      -       0       False   2023-10-27 17:59:11.000000      N/A
** 2588 644     svchost.exe     0xa083ac025080  12      -       0       False   2023-10-27 17:59:06.000000      N/A
** 1584 644     svchost.exe     0xa083abbcd0c0  6       -       0       False   2023-10-27 17:59:05.000000      N/A
** 2612 644     svchost.exe     0xa083ac06d080  17      -       0       False   2023-10-27 17:59:06.000000      N/A
** 5172 644     svchost.exe     0xa083b0271080  0       -       0       False   2023-10-27 18:03:18.000000      2023-10-27 18:03:24.000000
** 3132 644     svchost.exe     0xa083ac292080  15      -       0       False   2023-10-27 17:59:06.000000      N/A
** 8768 644     VSSVC.exe       0xa083b0256080  4       -       0       False   2023-10-27 18:03:19.000000      N/A
** 1632 644     svchost.exe     0xa083a72c42c0  3       -       0       False   2023-10-27 17:59:05.000000      N/A
** 7776 644     svchost.exe     0xa083ad666340  11      -       0       False   2023-10-27 17:59:36.000000      N/A
```

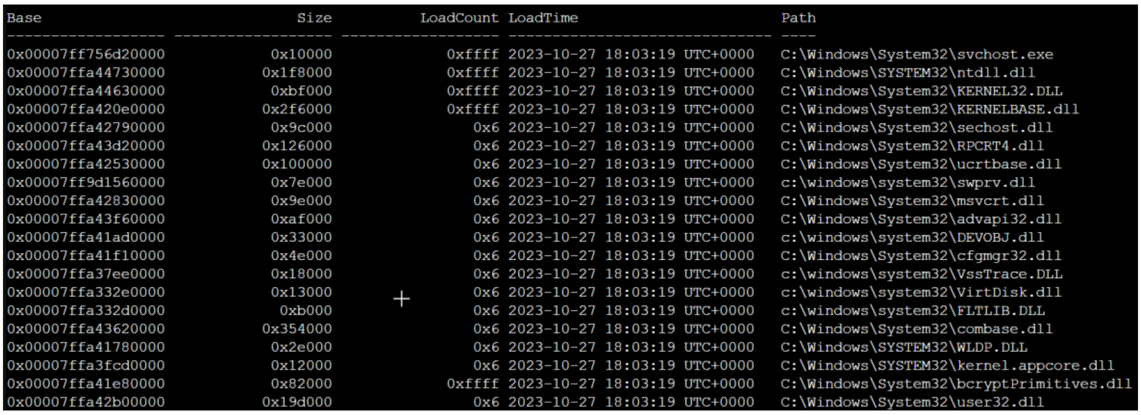
LIBRERÍAS DEL SISTEMA QUE SE ESTÁN UTILIZANDO

VOLATILITY 2

vol.py -f /root/memdump.mem –profile Win10x64_19041 dlllist.



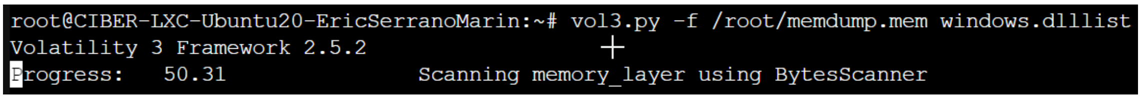
```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol.py -f /root/memdump.mem --profile Win10x64_19041 dlllist
Volatility Foundation Volatility Framework 2.6.1
```



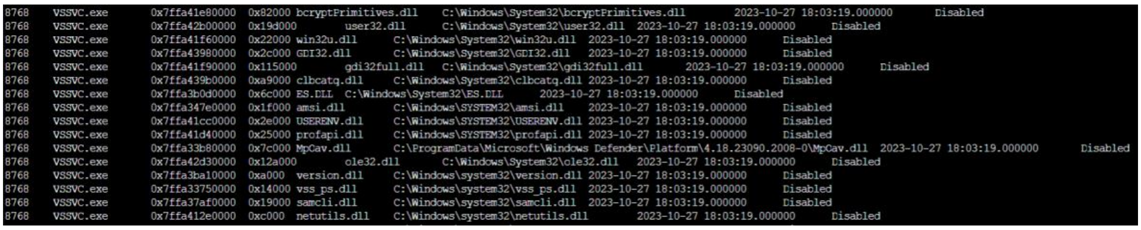
```
Base                             Size          LoadCount LoadTime                       Path
------------------ ------------------ ------------------ ------------------------------ ----
0x00007ff756d20000            0x10000             0xffff 2023-10-27 18:03:19 UTC+0000   C:\Windows\System32\svchost.exe
0x00007ffa44730000           0x1f8000             0xffff 2023-10-27 18:03:19 UTC+0000   C:\Windows\SYSTEM32\ntdll.dll
0x00007ffa44630000            0xbf000             0xffff 2023-10-27 18:03:19 UTC+0000   C:\Windows\System32\KERNEL32.DLL
0x00007ffa420e0000           0x2f6000             0xffff 2023-10-27 18:03:19 UTC+0000   C:\Windows\System32\KERNELBASE.dll
0x00007ffa42790000            0x9c000                0x6 2023-10-27 18:03:19 UTC+0000   C:\Windows\System32\sechost.dll
0x00007ffa43d20000           0x126000                0x6 2023-10-27 18:03:19 UTC+0000   C:\Windows\System32\RPCRT4.dll
0x00007ffa42530000           0x100000                0x6 2023-10-27 18:03:19 UTC+0000   C:\Windows\System32\ucrtbase.dll
0x00007ff9d1560000            0x7e000                0x6 2023-10-27 18:03:19 UTC+0000   c:\windows\system32\swprv.dll
0x00007ffa42830000            0x9e000                0x6 2023-10-27 18:03:19 UTC+0000   C:\Windows\System32\msvcrt.dll
0x00007ffa43f60000            0xaf000                0x6 2023-10-27 18:03:19 UTC+0000   C:\Windows\System32\advapi32.dll
0x00007ffa41ad0000            0x33000                0x6 2023-10-27 18:03:19 UTC+0000   c:\windows\system32\DEVOBJ.dll
0x00007ffa41f10000            0x4e000                0x6 2023-10-27 18:03:19 UTC+0000   C:\Windows\System32\cfgmgr32.dll
0x00007ffa37ee0000            0x18000                0x6 2023-10-27 18:03:19 UTC+0000   c:\windows\system32\VssTrace.DLL
0x00007ffa332e0000            0x13000                0x6 2023-10-27 18:03:19 UTC+0000   c:\windows\system32\VirtDisk.dll
0x00007ffa332d0000             0xb000                0x6 2023-10-27 18:03:19 UTC+0000   c:\windows\system32\FLTLIB.DLL
0x00007ffa43620000           0x354000                0x6 2023-10-27 18:03:19 UTC+0000   C:\Windows\System32\combase.dll
0x00007ffa41780000            0x2e000                0x6 2023-10-27 18:03:19 UTC+0000   C:\Windows\SYSTEM32\WLDP.DLL
0x00007ffa3fcd0000            0x12000                0x6 2023-10-27 18:03:19 UTC+0000   C:\Windows\SYSTEM32\kernel.appcore.dll
0x00007ffa41e80000            0x82000             0xffff 2023-10-27 18:03:19 UTC+0000   C:\Windows\System32\bcryptPrimitives.dll
0x00007ffa42b00000           0x19d000                0x6 2023-10-27 18:03:19 UTC+0000   C:\Windows\System32\user32.dll
```

VOLATILITY 3

vol3.py -f /root/memdump.mem windows.dlllist

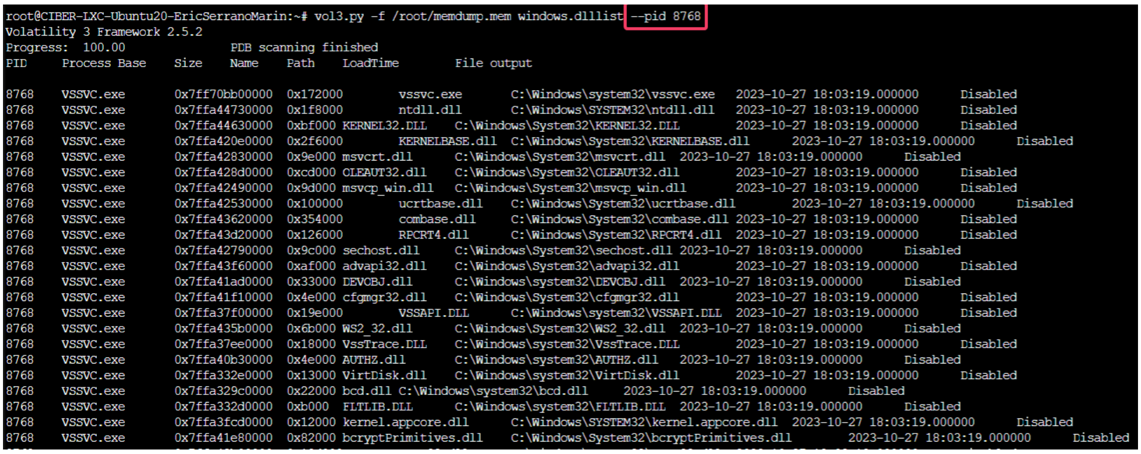


```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol3.py -f /root/memdump.mem windows.dlllist
Volatility 3 Framework 2.5.2
Progress:   50.31               Scanning memory_layer using BytesScanner
```



```
8768    VSSVC.exe       0x7ffa41e80000  0x82000 bcryptPrimitives.dll    C:\Windows\System32\bcryptPrimitives.dll        2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa42b00000  0x19d000        user32.dll      C:\Windows\System32\user32.dll  2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa41f60000  0x22000 win32u.dll      C:\Windows\System32\win32u.dll  2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa43980000  0x2c000 GDI32.dll       C:\Windows\System32\GDI32.dll   2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa41f90000  0x115000        gdi32full.dll   C:\Windows\System32\gdi32full.dll       2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa439b0000  0xa9000 clbcatq.dll     C:\Windows\System32\clbcatq.dll 2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa3b0d0000  0x6c000 ES.DLL  C:\Windows\System32\ES.DLL      2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa347e0000  0x1f000 amsi.dll        C:\Windows\SYSTEM32\amsi.dll    2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa41cc0000  0x2e000 USERENV.dll     C:\Windows\SYSTEM32\USERENV.dll 2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa41d40000  0x25000 profapi.dll     C:\Windows\SYSTEM32\profapi.dll 2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa33b80000  0x7c000 MpCav.dll       C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.23090.2008-0\MpCav.dll  2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa42d30000  0x12a000        ole32.dll       C:\Windows\System32\ole32.dll   2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa3ba10000  0xa000  version.dll     C:\Windows\system32\version.dll 2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa33750000  0x14000 vss_ps.dll      C:\Windows\system32\vss_ps.dll  2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa37af0000  0x19000 samcli.dll      C:\Windows\system32\samcli.dll  2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa412e0000  0xc000  netutils.dll    C:\Windows\system32\netutils.dll        2023-10-27 18:03:19.000000      Disabled
```

También podemos añadir -–pid y el número de identificación de proceso, en mi caso he usado el que he puesto en la captura anterior (8768)

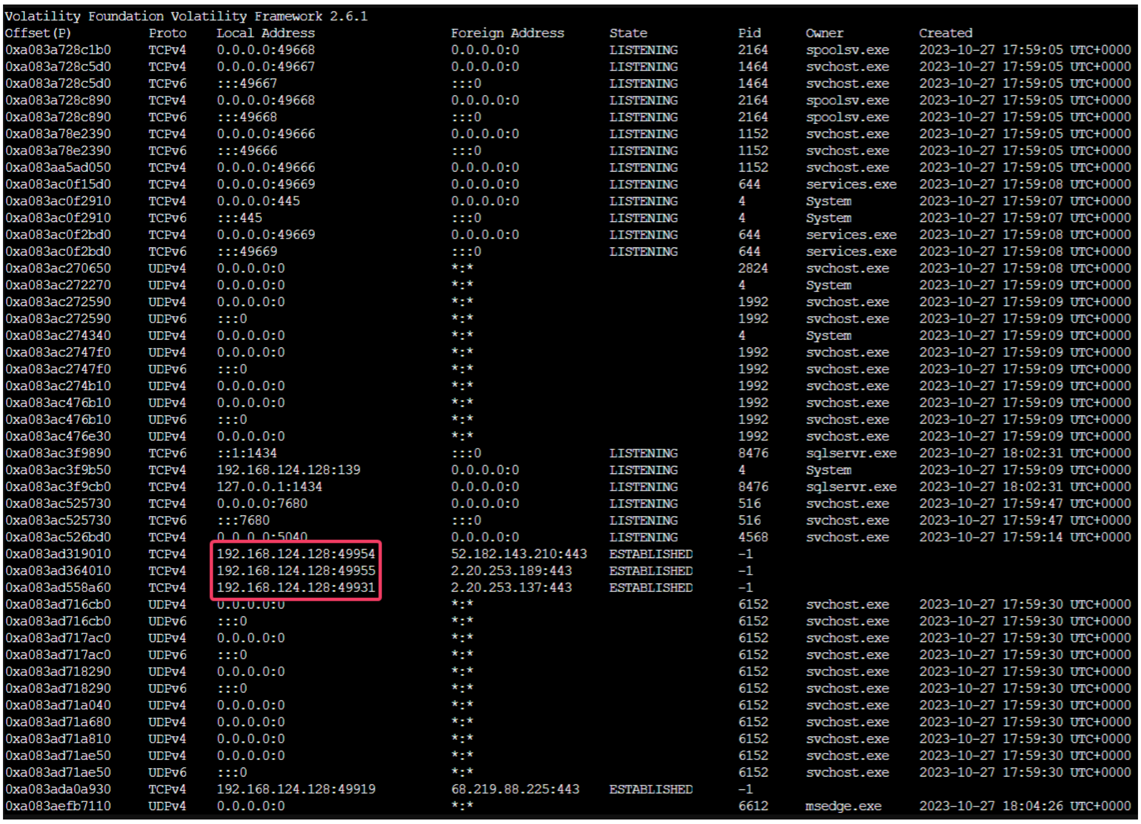


```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol3.py -f /root/memdump.mem windows.dlllist --pid 8768
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
PID     Process Base    Size    Name    Path    LoadTime        File output

8768    VSSVC.exe       0x7ff70bb00000  0x172000        vssvc.exe       C:\Windows\system32\vssvc.exe   2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa44730000  0x1f8000        ntdll.dll       C:\Windows\SYSTEM32\ntdll.dll   2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa44630000  0xbf000 KERNEL32.DLL    C:\Windows\System32\KERNEL32.DLL        2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa420e0000  0x2f6000        KERNELBASE.dll  C:\Windows\System32\KERNELBASE.dll      2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa42830000  0x9e000 msvcrt.dll      C:\Windows\System32\msvcrt.dll  2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa428d0000  0xcd000 CLEAUT32.dll    C:\Windows\System32\CLEAUT32.dll        2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa42490000  0x9d000 msvcp_win.dll   C:\Windows\System32\msvcp_win.dll       2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa42530000  0x100000        ucrtbase.dll    C:\Windows\System32\ucrtbase.dll        2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa43620000  0x354000        combase.dll     C:\Windows\System32\combase.dll 2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa43d20000  0x126000        RPCRT4.dll      C:\Windows\System32\RPCRT4.dll  2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa42790000  0x9c000 sechost.dll     C:\Windows\System32\sechost.dll 2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa43f60000  0xaf000 advapi32.dll    C:\Windows\System32\advapi32.dll        2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa41ad0000  0x33000 DEVCBJ.dll      C:\Windows\system32\DEVCBJ.dll  2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa41f10000  0x4e000 cfgmgr32.dll    C:\Windows\System32\cfgmgr32.dll        2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa37f00000  0x19e000        VSSAPI.DLL      C:\Windows\system32\VSSAPI.DLL  2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa435b0000  0x6b000 WS2_32.dll      C:\Windows\System32\WS2_32.dll  2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa37ee0000  0x18000 VssTrace.DLL    C:\Windows\system32\VssTrace.DLL        2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa40b30000  0x4e000 AUTHZ.dll       C:\Windows\system32\AUTHZ.dll   2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa332e0000  0x13000 VirtDisk.dll    C:\Windows\system32\VirtDisk.dll        2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa329c0000  0x22000 bcd.dll C:\Windows\system32\bcd.dll     2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa332d0000  0xb000  FLTLIB.DLL      C:\Windows\system32\FLTLIB.DLL  2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa3fcd0000  0x12000 kernel.appcore.dll      C:\Windows\SYSTEM32\kernel.appcore.dll  2023-10-27 18:03:19.000000      Disabled
8768    VSSVC.exe       0x7ffa41e80000  0x82000 bcryptPrimitives.dll    C:\Windows\System32\bcryptPrimitives.dll        2023-10-27 18:03:19.000000      Disabled
```

CONEXIONES DE RED REALIZADAS (PUERTOS Y SERVICIOS) Y IP DEL EQUIPO

VOLATILITY 2

vol.py -f /root/memdump.mem –-profile Win10x64_19041 netscan

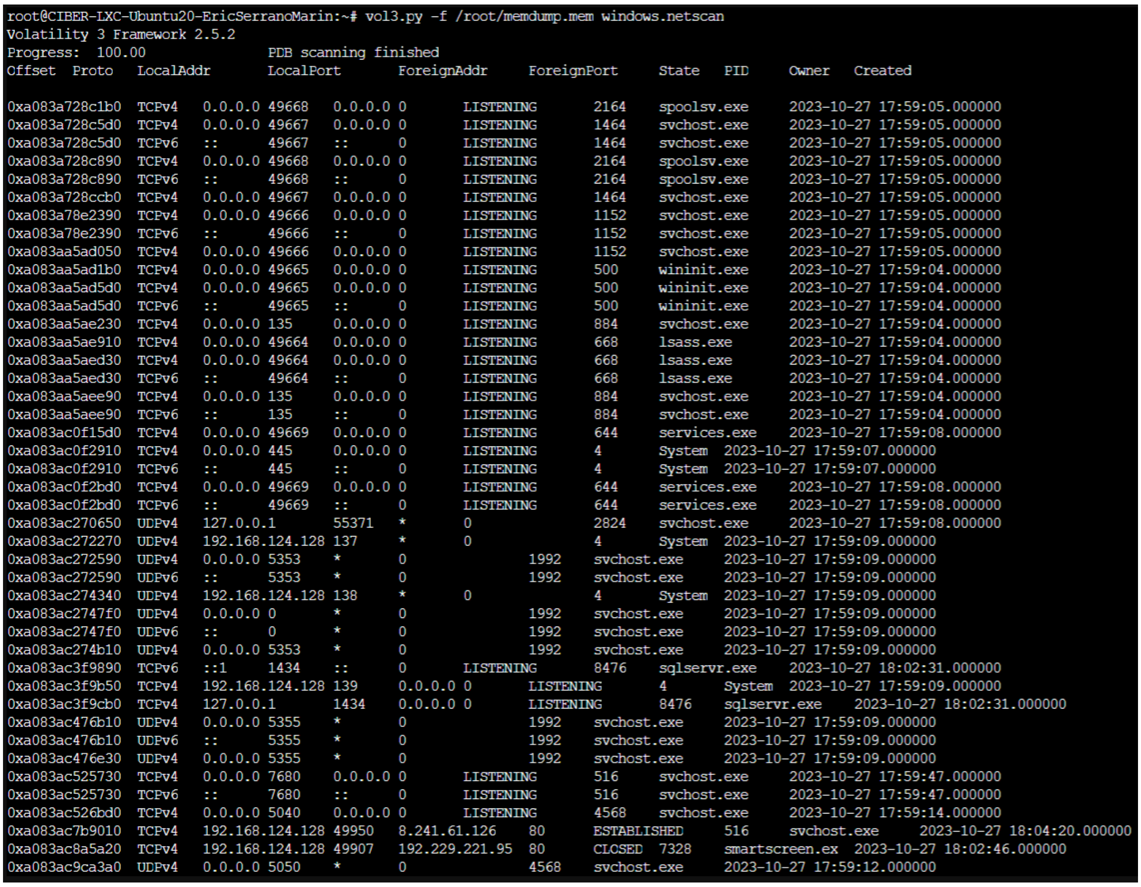


```
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0xa083a728c1b0     TCPv4    0.0.0.0:49668                  0.0.0.0:0            LISTENING        2164     spoolsv.exe    2023-10-27 17:59:05 UTC+0000
0xa083a728c5d0     TCPv4    0.0.0.0:49667                  0.0.0.0:0            LISTENING        1464     svchost.exe    2023-10-27 17:59:05 UTC+0000
0xa083a728c5d0     TCPv6    :::49667                       :::0                 LISTENING        1464     svchost.exe    2023-10-27 17:59:05 UTC+0000
0xa083a728c890     TCPv4    0.0.0.0:49668                  0.0.0.0:0            LISTENING        2164     spoolsv.exe    2023-10-27 17:59:05 UTC+0000
0xa083a728c890     TCPv6    :::49668                       :::0                 LISTENING        2164     spoolsv.exe    2023-10-27 17:59:05 UTC+0000
0xa083a78e2390     TCPv4    0.0.0.0:49666                  0.0.0.0:0            LISTENING        1152     svchost.exe    2023-10-27 17:59:05 UTC+0000
0xa083a78e2390     TCPv6    :::49666                       :::0                 LISTENING        1152     svchost.exe    2023-10-27 17:59:05 UTC+0000
0xa083aa5ad050     TCPv4    0.0.0.0:49666                  0.0.0.0:0            LISTENING        1152     svchost.exe    2023-10-27 17:59:05 UTC+0000
0xa083ac0f15d0     TCPv4    0.0.0.0:49669                  0.0.0.0:0            LISTENING        644      services.exe   2023-10-27 17:59:08 UTC+0000
0xa083ac0f2910     TCPv4    0.0.0.0:445                    0.0.0.0:0            LISTENING        4        System         2023-10-27 17:59:07 UTC+0000
0xa083ac0f2910     TCPv6    :::445                         :::0                 LISTENING        4        System         2023-10-27 17:59:07 UTC+0000
0xa083ac0f2bd0     TCPv4    0.0.0.0:49669                  0.0.0.0:0            LISTENING        644      services.exe   2023-10-27 17:59:08 UTC+0000
0xa083ac0f2bd0     TCPv6    :::49669                       :::0                 LISTENING        644      services.exe   2023-10-27 17:59:08 UTC+0000
0xa083ac270650     UDPv4    0.0.0.0:0                      *:*                                   2824     svchost.exe    2023-10-27 17:59:08 UTC+0000
0xa083ac272270     UDPv4    0.0.0.0:0                      *:*                                   4        System         2023-10-27 17:59:09 UTC+0000
0xa083ac272590     UDPv4    0.0.0.0:0                      *:*                                   1992     svchost.exe    2023-10-27 17:59:09 UTC+0000
0xa083ac272590     UDPv6    :::0                           *:*                                   1992     svchost.exe    2023-10-27 17:59:09 UTC+0000
0xa083ac274340     UDPv4    0.0.0.0:0                      *:*                                   4        System         2023-10-27 17:59:09 UTC+0000
0xa083ac2747f0     UDPv4    0.0.0.0:0                      *:*                                   1992     svchost.exe    2023-10-27 17:59:09 UTC+0000
0xa083ac2747f0     UDPv6    :::0                           *:*                                   1992     svchost.exe    2023-10-27 17:59:09 UTC+0000
0xa083ac274b10     UDPv4    0.0.0.0:0                      *:*                                   1992     svchost.exe    2023-10-27 17:59:09 UTC+0000
0xa083ac476b10     UDPv4    0.0.0.0:0                      *:*                                   1992     svchost.exe    2023-10-27 17:59:09 UTC+0000
0xa083ac476b10     UDPv6    :::0                           *:*                                   1992     svchost.exe    2023-10-27 17:59:09 UTC+0000
0xa083ac476e30     UDPv4    0.0.0.0:0                      *:*                                   1992     svchost.exe    2023-10-27 17:59:09 UTC+0000
0xa083ac3f9890     TCPv6    ::1:1434                       :::0                 LISTENING        8476     sqlservr.exe   2023-10-27 18:02:31 UTC+0000
0xa083ac3f9b50     TCPv4    192.168.124.128:139            0.0.0.0:0            LISTENING        4        System         2023-10-27 17:59:09 UTC+0000
0xa083ac3f9cb0     TCPv4    127.0.0.1:1434                 0.0.0.0:0            LISTENING        8476     sqlservr.exe   2023-10-27 18:02:31 UTC+0000
0xa083ac525730     TCPv4    0.0.0.0:7680                   0.0.0.0:0            LISTENING        516      svchost.exe    2023-10-27 17:59:47 UTC+0000
0xa083ac525730     TCPv6    :::7680                        :::0                 LISTENING        516      svchost.exe    2023-10-27 17:59:47 UTC+0000
0xa083ac526bd0     TCPv4    0.0.0.0:5040                   0.0.0.0:0            LISTENING        4568     svchost.exe    2023-10-27 17:59:14 UTC+0000
0xa083ad319010     TCPv4    192.168.124.128:49954          52.182.143.210:443   ESTABLISHED      -1
0xa083ad364010     TCPv4    192.168.124.128:49955          2.20.253.189:443     ESTABLISHED      -1
0xa083ad558a60     TCPv4    192.168.124.128:49931          2.20.253.137:443     ESTABLISHED      -1
0xa083ad716cb0     UDPv4    0.0.0.0:0                      *:*                                   6152     svchost.exe    2023-10-27 17:59:30 UTC+0000
0xa083ad716cb0     UDPv6    :::0                           *:*                                   6152     svchost.exe    2023-10-27 17:59:30 UTC+0000
0xa083ad717ac0     UDPv4    0.0.0.0:0                      *:*                                   6152     svchost.exe    2023-10-27 17:59:30 UTC+0000
0xa083ad717ac0     UDPv6    :::0                           *:*                                   6152     svchost.exe    2023-10-27 17:59:30 UTC+0000
0xa083ad718290     UDPv4    0.0.0.0:0                      *:*                                   6152     svchost.exe    2023-10-27 17:59:30 UTC+0000
0xa083ad718290     UDPv6    :::0                           *:*                                   6152     svchost.exe    2023-10-27 17:59:30 UTC+0000
0xa083ad71a040     UDPv4    0.0.0.0:0                      *:*                                   6152     svchost.exe    2023-10-27 17:59:30 UTC+0000
0xa083ad71a680     UDPv4    0.0.0.0:0                      *:*                                   6152     svchost.exe    2023-10-27 17:59:30 UTC+0000
0xa083ad71a810     UDPv4    0.0.0.0:0                      *:*                                   6152     svchost.exe    2023-10-27 17:59:30 UTC+0000
0xa083ad71ae50     UDPv4    0.0.0.0:0                      *:*                                   6152     svchost.exe    2023-10-27 17:59:30 UTC+0000
0xa083ad71ae50     UDPv6    :::0                           *:*                                   6152     svchost.exe    2023-10-27 17:59:30 UTC+0000
0xa083ada0a930     TCPv4    192.168.124.128:49919          68.219.88.225:443    ESTABLISHED      -1
0xa083aefb7110     UDPv4    0.0.0.0:0                      *:*                                   6612     msedge.exe     2023-10-27 18:04:26 UTC+0000
```

La IP sería 192.168.124.128, ya que la IP se repite, pero no el puerto.

VOLATILITY 3

vol3.py -f /root/memdump.mem windows.netscan



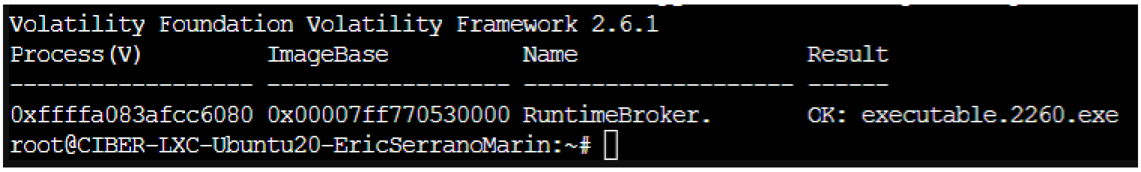
```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol3.py -f /root/memdump.mem windows.netscan
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0xa083a728c1b0  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       2164    spoolsv.exe     2023-10-27 17:59:05.000000
0xa083a728c5d0  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       1464    svchost.exe     2023-10-27 17:59:05.000000
0xa083a728c5d0  TCPv6   ::      49667   ::      0       LISTENING       1464    svchost.exe     2023-10-27 17:59:05.000000
0xa083a728c890  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       2164    spoolsv.exe     2023-10-27 17:59:05.000000
0xa083a728c890  TCPv6   ::      49668   ::      0       LISTENING       2164    spoolsv.exe     2023-10-27 17:59:05.000000
0xa083a728ccb0  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       1464    svchost.exe     2023-10-27 17:59:05.000000
0xa083a78e2390  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1152    svchost.exe     2023-10-27 17:59:05.000000
0xa083a78e2390  TCPv6   ::      49666   ::      0       LISTENING       1152    svchost.exe     2023-10-27 17:59:05.000000
0xa083aa5ad050  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1152    svchost.exe     2023-10-27 17:59:05.000000
0xa083aa5ad1b0  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       500     wininit.exe     2023-10-27 17:59:04.000000
0xa083aa5ad5d0  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       500     wininit.exe     2023-10-27 17:59:04.000000
0xa083aa5ad5d0  TCPv6   ::      49665   ::      0       LISTENING       500     wininit.exe     2023-10-27 17:59:04.000000
0xa083aa5ae230  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       884     svchost.exe     2023-10-27 17:59:04.000000
0xa083aa5ae910  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       668     lsass.exe       2023-10-27 17:59:04.000000
0xa083aa5aed30  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       668     lsass.exe       2023-10-27 17:59:04.000000
0xa083aa5aed30  TCPv6   ::      49664   ::      0       LISTENING       668     lsass.exe       2023-10-27 17:59:04.000000
0xa083aa5aee90  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       884     svchost.exe     2023-10-27 17:59:04.000000
0xa083aa5aee90  TCPv6   ::      135     ::      0       LISTENING       884     svchost.exe     2023-10-27 17:59:04.000000
0xa083ac0f15d0  TCPv4   0.0.0.0 49669   0.0.0.0 0       LISTENING       644     services.exe    2023-10-27 17:59:08.000000
0xa083ac0f2910  TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  2023-10-27 17:59:07.000000
0xa083ac0f2910  TCPv6   ::      445     ::      0       LISTENING       4       System  2023-10-27 17:59:07.000000
0xa083ac0f2bd0  TCPv4   0.0.0.0 49669   0.0.0.0 0       LISTENING       644     services.exe    2023-10-27 17:59:08.000000
0xa083ac0f2bd0  TCPv6   ::      49669   ::      0       LISTENING       644     services.exe    2023-10-27 17:59:08.000000
0xa083ac270650  UDPv4   127.0.0.1       55371   *       0               2824    svchost.exe     2023-10-27 17:59:08.000000
0xa083ac272270  UDPv4   192.168.124.128 137     *       0               4       System  2023-10-27 17:59:09.000000
0xa083ac272590  UDPv4   0.0.0.0 5353    *       0               1992    svchost.exe     2023-10-27 17:59:09.000000
0xa083ac272590  UDPv6   ::      5353    *       0               1992    svchost.exe     2023-10-27 17:59:09.000000
0xa083ac274340  UDPv4   192.168.124.128 138     *       0               4       System  2023-10-27 17:59:09.000000
0xa083ac2747f0  UDPv4   0.0.0.0 0       *       0               1992    svchost.exe     2023-10-27 17:59:09.000000
0xa083ac2747f0  UDPv6   ::      0       *       0               1992    svchost.exe     2023-10-27 17:59:09.000000
0xa083ac274b10  UDPv4   0.0.0.0 5353    *       0               1992    svchost.exe     2023-10-27 17:59:09.000000
0xa083ac3f9890  TCPv6   ::1     1434    ::      0       LISTENING       8476    sqlservr.exe    2023-10-27 18:02:31.000000
0xa083ac3f9b50  TCPv4   192.168.124.128 139     0.0.0.0 0       LISTENING       4       System  2023-10-27 17:59:09.000000
0xa083ac3f9cb0  TCPv4   127.0.0.1       1434    0.0.0.0 0       LISTENING       8476    sqlservr.exe    2023-10-27 18:02:31.000000
0xa083ac476b10  UDPv4   0.0.0.0 5355    *       0               1992    svchost.exe     2023-10-27 17:59:09.000000
0xa083ac476b10  UDPv6   ::      5355    *       0               1992    svchost.exe     2023-10-27 17:59:09.000000
0xa083ac476e30  UDPv4   0.0.0.0 5355    *       0               1992    svchost.exe     2023-10-27 17:59:09.000000
0xa083ac525730  TCPv4   0.0.0.0 7680    0.0.0.0 0       LISTENING       516     svchost.exe     2023-10-27 17:59:47.000000
0xa083ac525730  TCPv6   ::      7680    ::      0       LISTENING       516     svchost.exe     2023-10-27 17:59:47.000000
0xa083ac526bd0  TCPv4   0.0.0.0 5040    0.0.0.0 0       LISTENING       4568    svchost.exe     2023-10-27 17:59:14.000000
0xa083ac7b9010  TCPv4   192.168.124.128 49950   8.241.61.126    80      ESTABLISHED     516     svchost.exe     2023-10-27 18:04:20.000000
0xa083ac8a5a20  TCPv4   192.168.124.128 49907   192.229.221.95  80      CLOSED  7328    smartscreen.ex  2023-10-27 18:02:46.000000
0xa083ac9ca3a0  UDPv4   0.0.0.0 5050    *       0               4568    svchost.exe     2023-10-27 17:59:12.000000
```

EXTRAIGA UN EJECUTABLE Y SÚBALA A VIRUSTOTAL

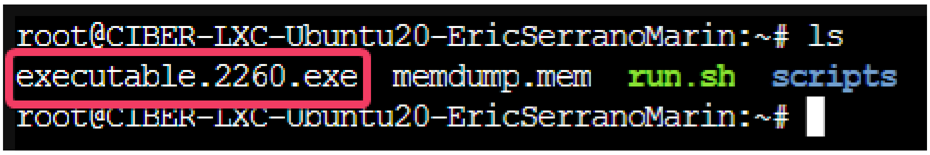
VOLATILITY 2

vol.py -f /root/memdump.mem --profile Win10x64_19041 procdump -p 2260 --dump-dir="/root/"

Siendo 2260 el pid de la librería que quiero.

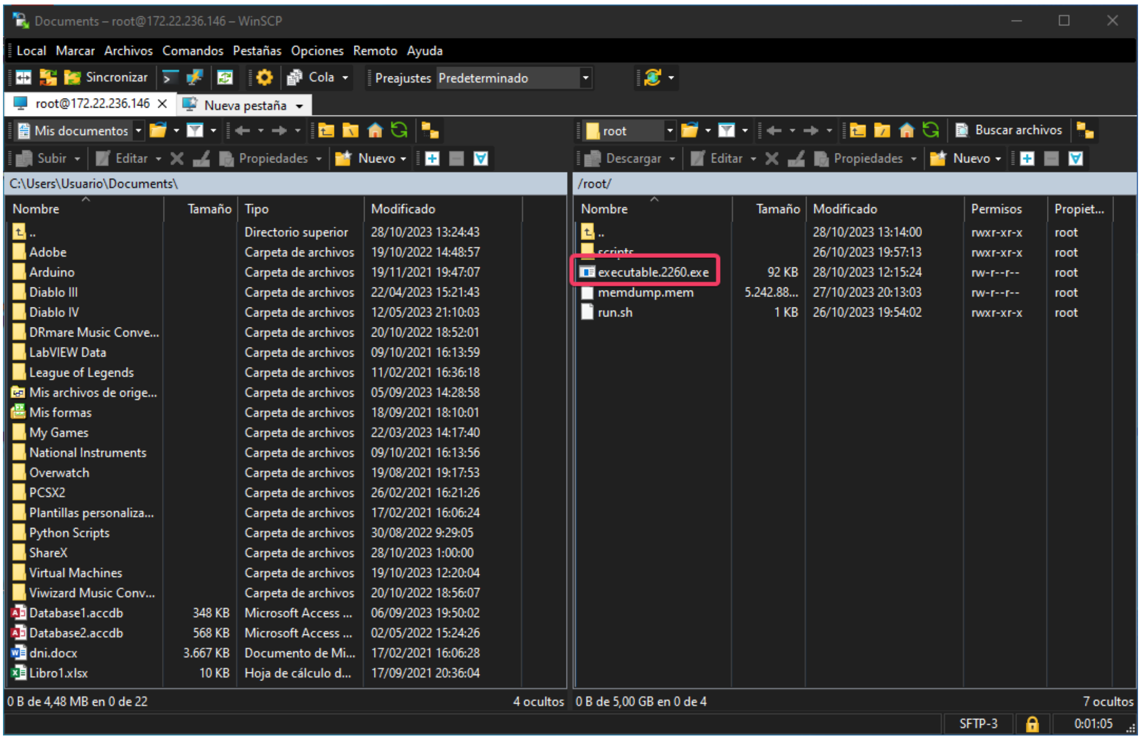


```
Volatility Foundation Volatility Framework 2.6.1
Process(V)         ImageBase          Name                 Result
------------------ ------------------ -------------------- ------
0xffffa083afcc6080 0x00007ff770530000 RuntimeBroker.       OK: executable.2260.exe
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# 
```



```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# ls
executable.2260.exe  memdump.mem  run.sh  scripts
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# 
```

Para pasar el archivo a mi Windows he usado WinSCP, ya que he estado un rato peleando con los comandos scp para pasármelo mediante comando, pero no he podido.



C:\Users\Usuario\Documents\

Nombre	Tamaño	Tipo	Modificado
..		Directorio superior	28/10/2023 13:24:43
Adobe		Carpeta de archivos	19/10/2022 14:48:57
Arduino		Carpeta de archivos	19/11/2021 19:47:07
Diablo III		Carpeta de archivos	22/04/2023 15:21:43
Diablo IV		Carpeta de archivos	12/05/2023 21:10:03
DRmare Music Conve...		Carpeta de archivos	20/10/2022 18:52:01
LabVIEW Data		Carpeta de archivos	09/10/2021 16:13:59
League of Legends		Carpeta de archivos	11/02/2021 16:36:18
Mis archivos de orige...		Carpeta de archivos	05/09/2023 14:28:58
Mis formas		Carpeta de archivos	18/09/2021 18:10:01
My Games		Carpeta de archivos	22/03/2023 14:17:40
National Instruments		Carpeta de archivos	09/10/2021 16:13:56
Overwatch		Carpeta de archivos	19/08/2021 19:17:53
PCSX2		Carpeta de archivos	26/02/2021 16:21:26
Plantillas personaliza...		Carpeta de archivos	17/02/2021 16:06:24
Python Scripts		Carpeta de archivos	30/08/2022 9:29:05
ShareX		Carpeta de archivos	28/10/2023 1:00:00
Virtual Machines		Carpeta de archivos	19/10/2023 12:20:04
Viwizard Music Conv...		Carpeta de archivos	20/10/2022 18:56:07
Database1.accdb	348 KB	Microsoft Access ...	06/09/2023 19:50:02
Database2.accdb	568 KB	Microsoft Access ...	02/05/2022 15:24:26
dni.docx	3.667 KB	Documento de Mi...	17/02/2021 16:06:28
Libro1.xlsx	10 KB	Hoja de cálculo d...	17/09/2021 20:36:04

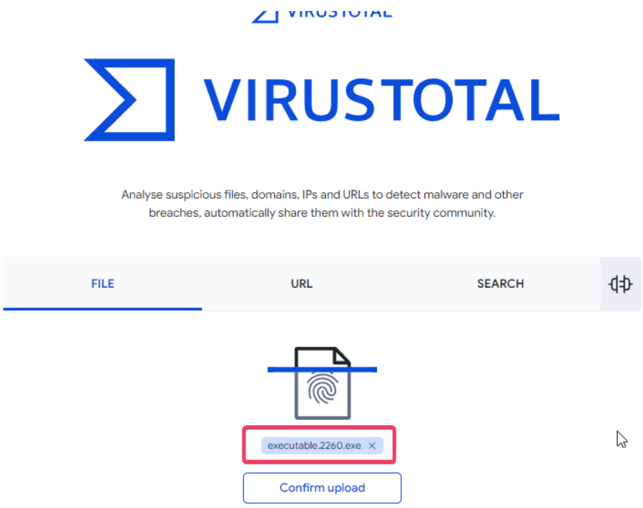
0 B de 4,48 MB en 0 de 22 — 4 ocultos

/root/

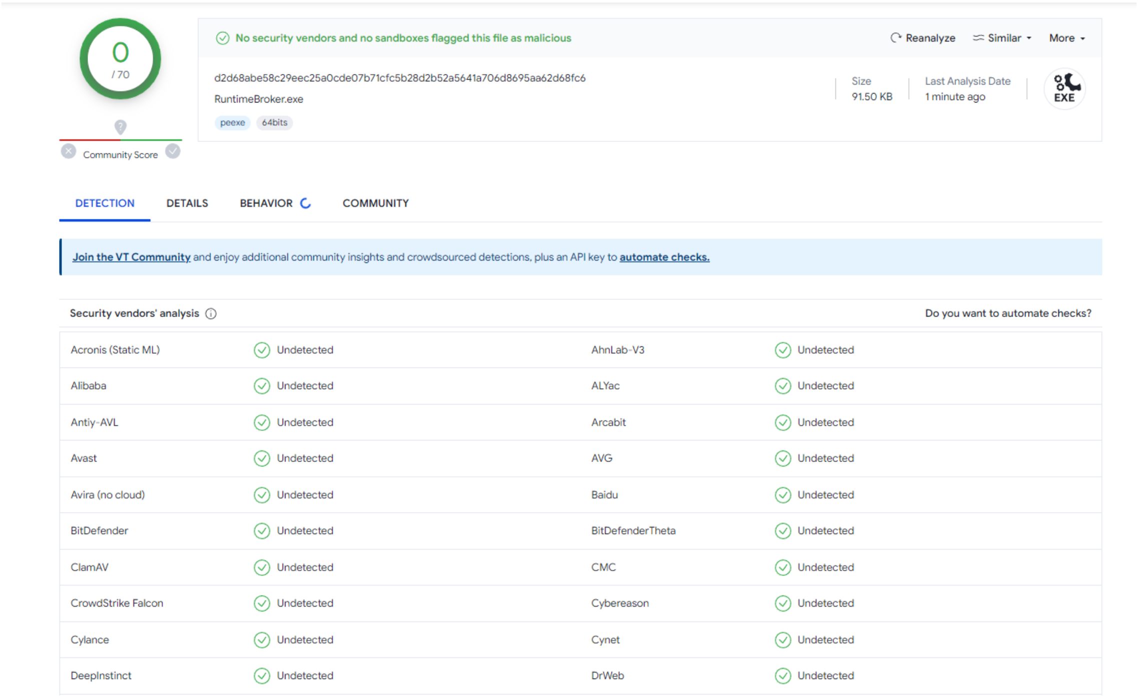
Nombre	Tamaño	Modificado	Permisos	Propiet...
..		28/10/2023 13:14:00	rwxr-xr-x	root
scripts		26/10/2023 19:57:13	rwxr-xr-x	root
executable.2260.exe	92 KB	28/10/2023 12:15:24	rw-r--r--	root
memdump.mem	5.242.88...	27/10/2023 20:13:03	rw-r--r--	root
run.sh	1 KB	26/10/2023 19:54:02	rwxr-xr-x	root

0 B de 5,00 GB en 0 de 4 — 7 ocultos

SFTP-3 0:01:05



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.



No security vendors and no sandboxes flagged this file as malicious

d2d68abe58c29eec25a0cde07b71cfc5b28d2b52a5641a706d8695aa62d68fc6

RuntimeBroker.exe

peexe 64bits

Size 91.50 KB

Last Analysis Date 1 minute ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

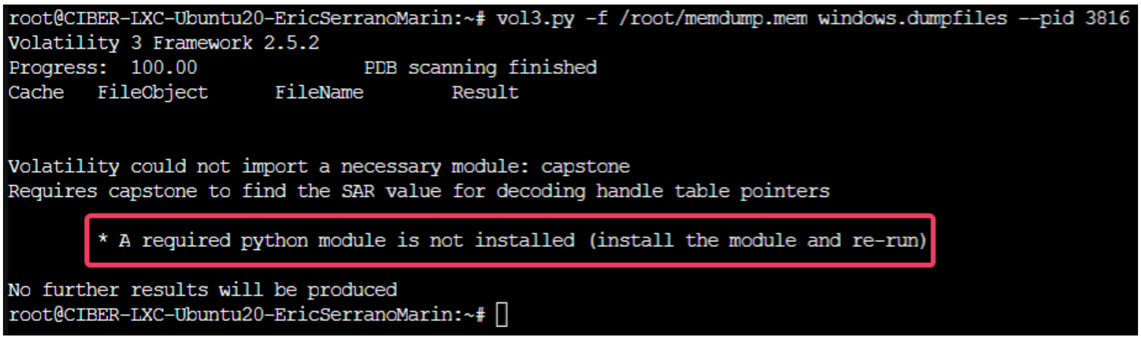
Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
Alibaba	✓ Undetected	ALYac	✓ Undetected
Antiy-AVL	✓ Undetected	Arcabit	✓ Undetected
Avast	✓ Undetected	AVG	✓ Undetected
Avira (no cloud)	✓ Undetected	Baidu	✓ Undetected
BitDefender	✓ Undetected	BitDefenderTheta	✓ Undetected
ClamAV	✓ Undetected	CMC	✓ Undetected
CrowdStrike Falcon	✓ Undetected	Cybereason	✓ Undetected
Cylance	✓ Undetected	Cynet	✓ Undetected
DeepInstinct	✓ Undetected	DrWeb	✓ Undetected

VOLATILITY 3

Nos dice que necesitamos un módulo que no tenemos llamado capstone.



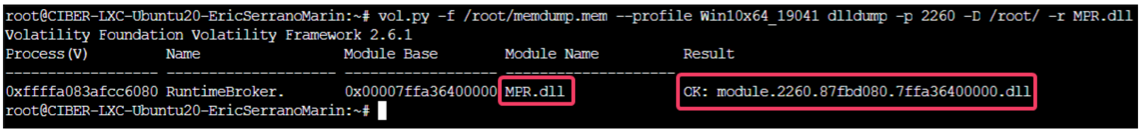
```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol3.py -f /root/memdump.mem windows.dumpfiles --pid 3816
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result


Volatility could not import a necessary module: capstone
Requires capstone to find the SAR value for decoding handle table pointers

         * A required python module is not installed (install the module and re-run)

No further results will be produced
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# 
```

EXTRAIGA UNA LIBRERÍA DEL SISTEMA Y SÚBALA A VIRUS TOTAL

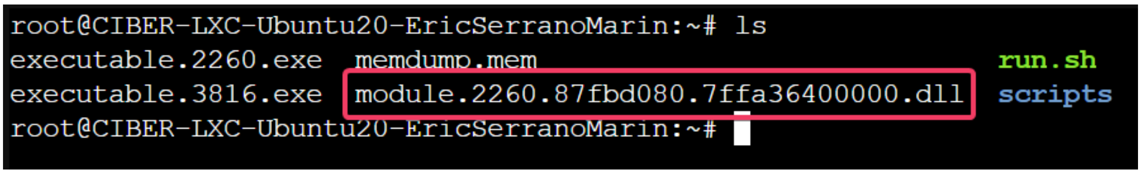
VOLATILITY 2

Obviamente para elegir PID y el .dll que queremos hemos buscado antes con **vol3.py -f /root/memdump.mem windows.dlllist.**

vol.py -f /root/memdump.mem --profile Win10x64_19041 dlldump -p 2260 -D /root/ -r MPR.dll

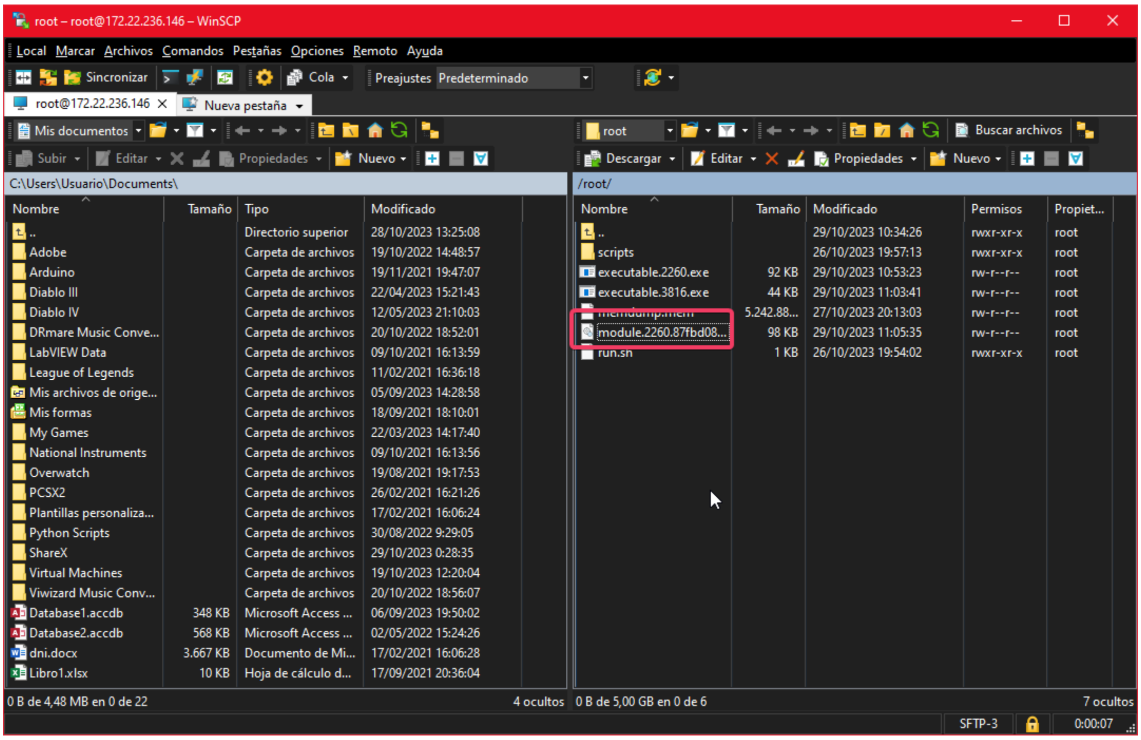


```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol.py -f /root/memdump.mem --profile Win10x64_19041 dlldump -p 2260 -D /root/ -r MPR.dll
Volatility Foundation Volatility Framework 2.6.1
Process(V)         Name                 Module Base        Module Name          Result
------------------ -------------------- ------------------ --------------------
0xffffa083afcc6080 RuntimeBroker.       0x00007ffa36400000 MPR.dll              OK: module.2260.87fbd080.7ffa36400000.dll
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# 
```



```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# ls
executable.2260.exe  memdump.mem                         run.sh
executable.3816.exe  module.2260.87fbd080.7ffa36400000.dll  scripts
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# 
```

Vamos a guardarlo en nuestra máquina Windows.



C:\Users\Usuario\Documents\

Nombre	Tamaño	Tipo	Modificado
..		Directorio superior	28/10/2023 13:25:08
Adobe		Carpeta de archivos	19/10/2022 14:48:57
Arduino		Carpeta de archivos	19/11/2021 19:47:07
Diablo III		Carpeta de archivos	22/04/2023 15:21:43
Diablo IV		Carpeta de archivos	12/05/2023 21:10:03
DRmare Music Conve...		Carpeta de archivos	20/10/2022 18:52:01
LabVIEW Data		Carpeta de archivos	09/10/2021 16:13:59
League of Legends		Carpeta de archivos	11/02/2021 16:36:18
Mis archivos de orige...		Carpeta de archivos	05/09/2023 14:28:58
Mis formas		Carpeta de archivos	18/09/2021 18:10:01
My Games		Carpeta de archivos	22/03/2023 14:17:40
National Instruments		Carpeta de archivos	09/10/2021 16:13:56
Overwatch		Carpeta de archivos	19/08/2021 19:17:53
PCSX2		Carpeta de archivos	26/02/2021 16:21:26
Plantillas personaliza...		Carpeta de archivos	17/02/2021 16:06:24
Python Scripts		Carpeta de archivos	30/08/2022 9:29:05
ShareX		Carpeta de archivos	29/10/2023 0:28:35
Virtual Machines		Carpeta de archivos	19/10/2023 12:20:04
Viwizard Music Conv...		Carpeta de archivos	20/10/2022 18:56:07
Database1.accdb	348 KB	Microsoft Access ...	06/09/2023 19:50:02
Database2.accdb	568 KB	Microsoft Access ...	02/05/2022 15:24:26
dni.docx	3.667 KB	Documento de Mi...	17/02/2021 16:06:28
Libro1.xlsx	10 KB	Hoja de cálculo d...	17/09/2021 20:36:04

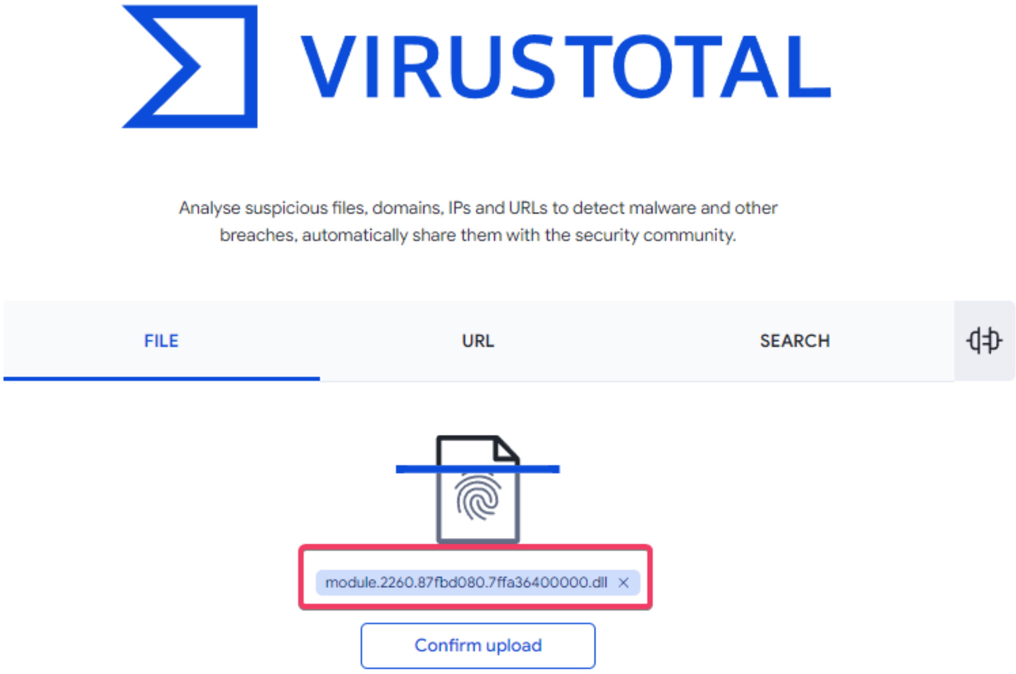
0 B de 4,48 MB en 0 de 22 4 ocultos

/root/

Nombre	Tamaño	Modificado	Permisos	Propiet...
..		29/10/2023 10:34:26	rwxr-xr-x	root
scripts		26/10/2023 19:57:13	rwxr-xr-x	root
executable.2260.exe	92 KB	29/10/2023 10:53:23	rw-r--r--	root
executable.3816.exe	44 KB	29/10/2023 11:03:41	rw-r--r--	root
memdump.mem	5.242.88...	27/10/2023 20:13:03	rw-r--r--	root
module.2260.87fbd08...	98 KB	29/10/2023 11:05:35	rw-r--r--	root
run.sh	1 KB	26/10/2023 19:54:02	rwxr-xr-x	root

0 B de 5,00 GB en 0 de 6 7 ocultos

SFTP-3 0:00:07

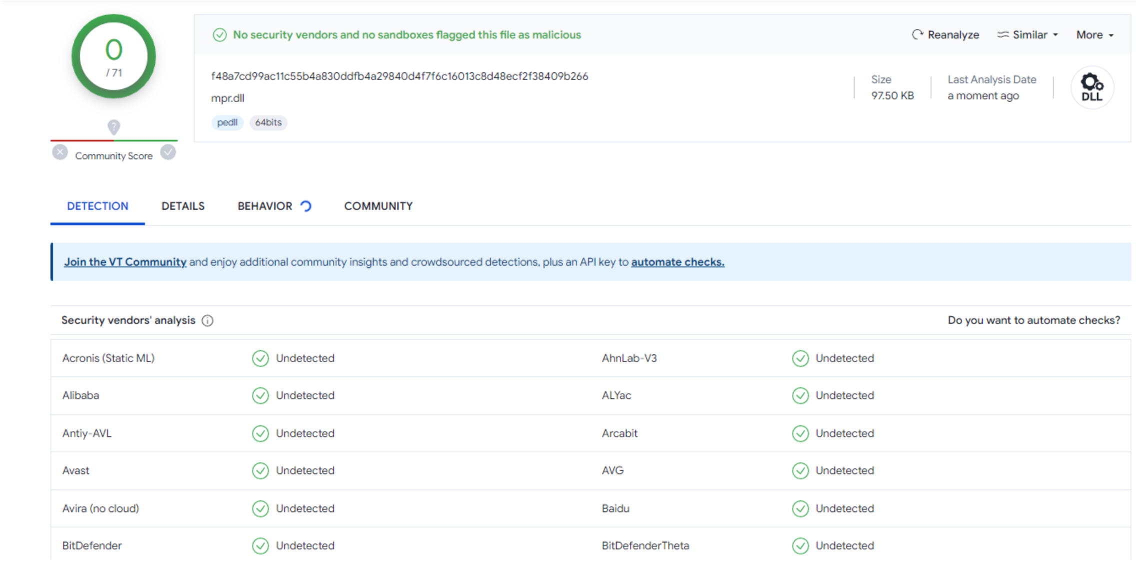


VIRUSTOTAL

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

module.2260.87fbd080.7ffa36400000.dll ×

Confirm upload



No security vendors and no sandboxes flagged this file as malicious

f48a7cd99ac11c55b4a830ddfb4a29840d4f7f6c16013c8d48ecf2f38409b266

mpr.dll

pedll 64bits

Size
97.50 KB

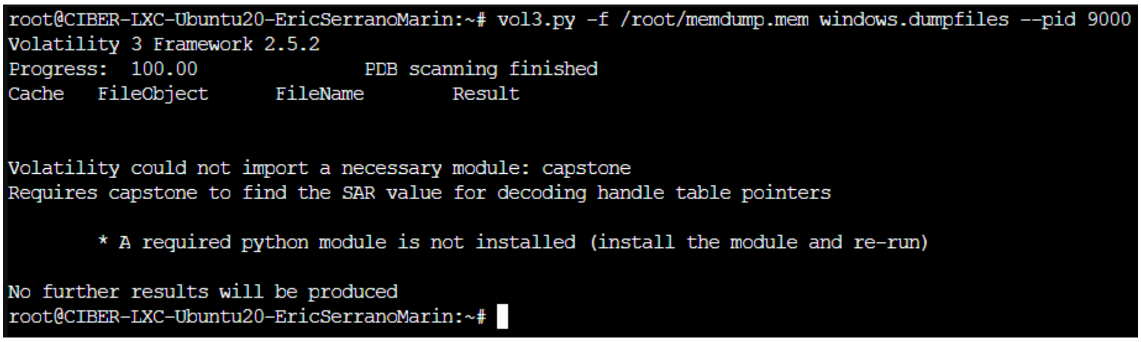
Last Analysis Date
a moment ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘ — Do you want to automate checks?

Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
Alibaba	✓ Undetected	ALYac	✓ Undetected
Antiy-AVL	✓ Undetected	Arcabit	✓ Undetected
Avast	✓ Undetected	AVG	✓ Undetected
Avira (no cloud)	✓ Undetected	Baidu	✓ Undetected
BitDefender	✓ Undetected	BitDefenderTheta	✓ Undetected

VOLATILITY 3



```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol3.py -f /root/memdump.mem windows.dumpfiles --pid 9000
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result


Volatility could not import a necessary module: capstone
Requires capstone to find the SAR value for decoding handle table pointers

        * A required python module is not installed (install the module and re-run)

No further results will be produced
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# 
```

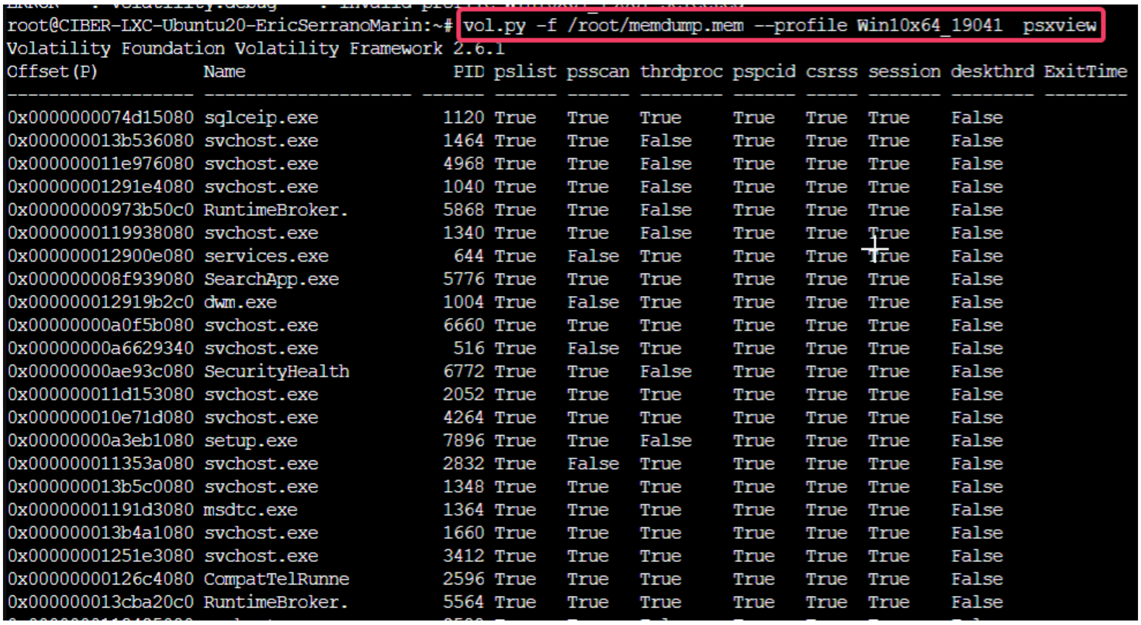
LISTADO DE COMANDOS CMD EJECUTADOS

Ya que serían muchas capturas, he hecho un gif. https://i.imgur.com/6xe2nOl.gif

ELIJA 3 PLUGINS ADICIONALES, EXPLÍQUELOS Y PRUÉBELOS

VOLATILITY 2: PSXVIEW

Se utiliza para mostrar información sobre los procesos. Es útil para detectar procesos ocultos o maliciosos que pueden estar tratando de evadir la detección.

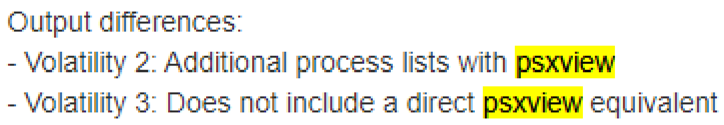


```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol.py -f /root/memdump.mem --profile Win10x64_19041  psxview
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
------------------ -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x0000000074d15080 sqlceip.exe            1120 True   True   True     True   True  True    False
0x000000013b536080 svchost.exe            1464 True   True   False    True   True  True    False
0x000000011e976080 svchost.exe            4968 True   True   False    True   True  True    False
0x00000001291e4080 svchost.exe            1040 True   True   False    True   True  True    False
0x00000000973b50c0 RuntimeBroker.         5868 True   True   False    True   True  True    False
0x0000000119938080 svchost.exe            1340 True   True   False    True   True  True    False
0x000000012900e080 services.exe            644 True   False  True     True   True  True    False
0x000000008f939080 SearchApp.exe          5776 True   True   True     True   True  True    False
0x000000012919b2c0 dwm.exe                1004 True   False  True     True   True  True    False
0x00000000a0f5b080 svchost.exe            6660 True   True   True     True   True  True    False
0x00000000a6629340 svchost.exe             516 True   False  True     True   True  True    False
0x00000000ae93c080 SecurityHealth         6772 True   True   False    True   True  True    False
0x000000011d153080 svchost.exe            2052 True   True   True     True   True  True    False
0x000000010e71d080 svchost.exe            4264 True   True   True     True   True  True    False
0x00000000a3eb1080 setup.exe              7896 True   True   False    True   True  True    False
0x000000011353a080 svchost.exe            2832 True   False  True     True   True  True    False
0x000000013b5c0080 svchost.exe            1348 True   True   True     True   True  True    False
0x00000001191d3080 msdtc.exe              1364 True   True   True     True   True  True    False
0x000000013b4a1080 svchost.exe            1660 True   True   True     True   True  True    False
0x00000001251e3080 svchost.exe            3412 True   True   True     True   True  True    False
0x00000000126c4080 CompatTelRunne         2596 True   True   True     True   True  True    False
0x000000013cba20c0 RuntimeBroker.         5564 True   True   True     True   True  True    False
```

Por lo que he podido entender mediante la siguiente página https://medium.com/@theumar9/memory-analysis-using-volatility-for-beginners-part-i-a6d37c0a1db6, si miramos las columnas pslist y psscan y tenemos alguna respuesta en False, esto indica que es un proceso que estaba escondido en nuestro escáner inicial.

VOLATILITY 3: PSXVIEW

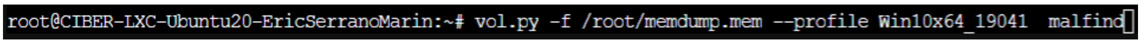
Volatility 3 no incluye PSXVIEW. Sus equivalentes serían: pslist, psscan, pstree.



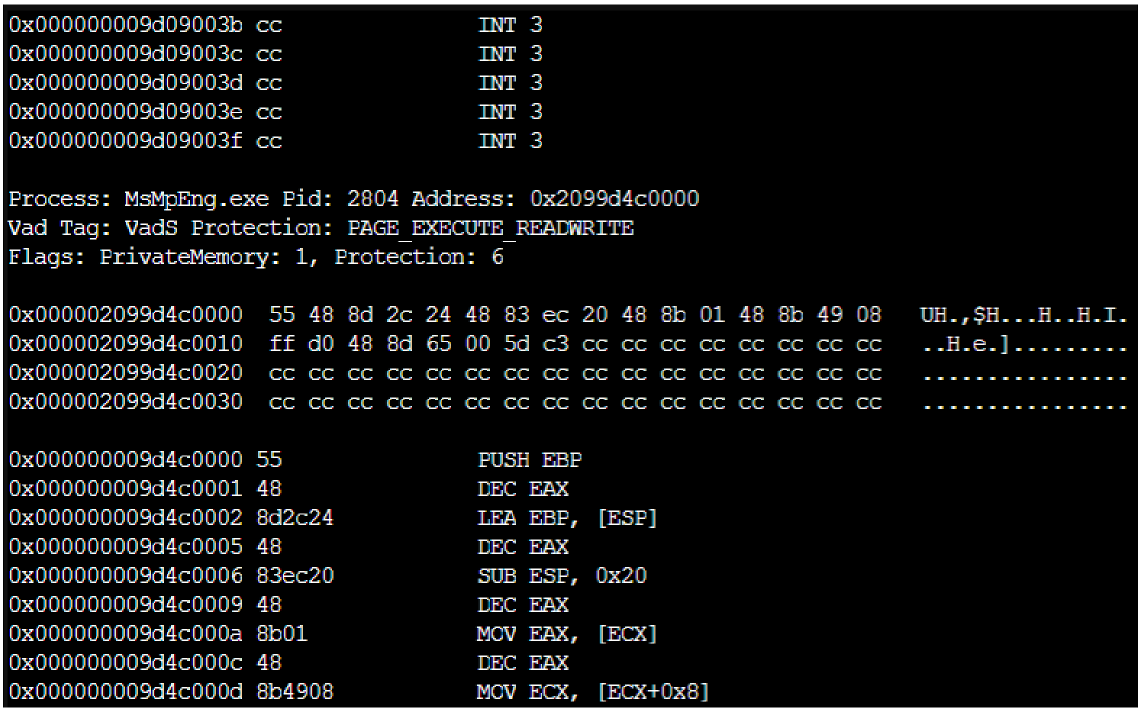
Output differences:
- Volatility 2: Additional process lists with psxview
- Volatility 3: Does not include a direct psxview equivalent

VOLATILITY 2: MALFIND

Se utiliza para identificar procesos que pueden ser maliciosos en función de su comportamiento, como la ejecución de código desde regiones de memoria inusuales.



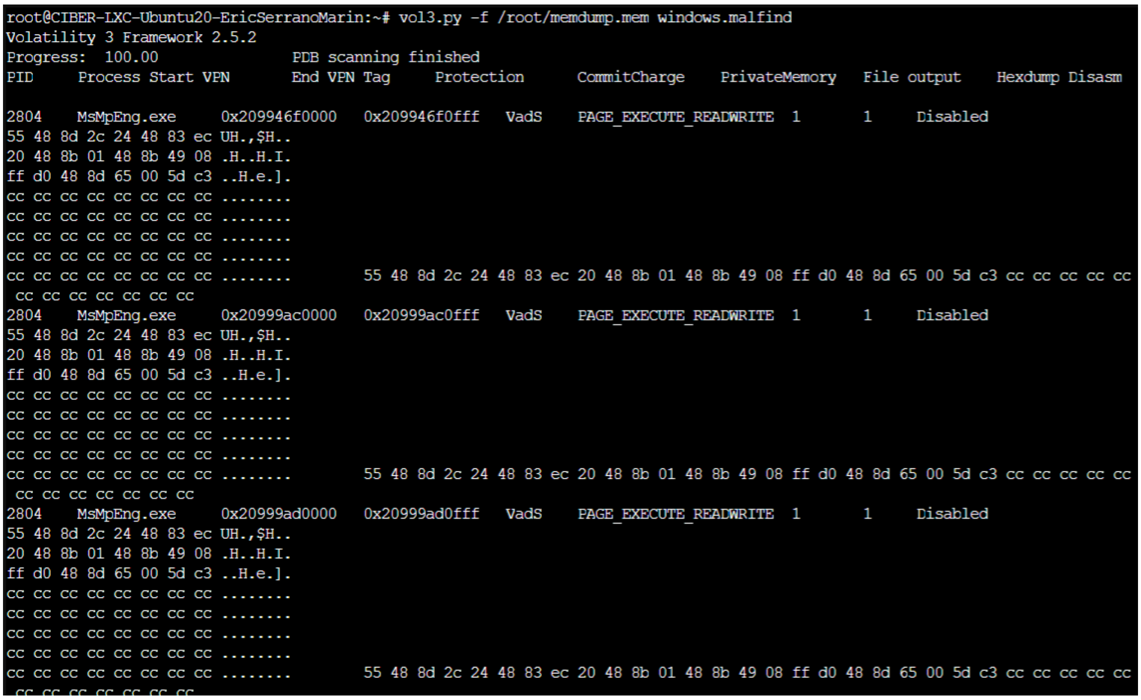
```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol.py -f /root/memdump.mem --profile Win10x64_19041  malfind
```



```
0x000000009d09003b cc               INT 3
0x000000009d09003c cc               INT 3
0x000000009d09003d cc               INT 3
0x000000009d09003e cc               INT 3
0x000000009d09003f cc               INT 3

Process: MsMpEng.exe Pid: 2804 Address: 0x2099d4c0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: PrivateMemory: 1, Protection: 6

0x000002099d4c0000  55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08   UH.,$H...H..H.I.
0x000002099d4c0010  ff d0 48 8d 65 00 5d c3 cc cc cc cc cc cc cc cc   ..H.e.].........
0x000002099d4c0020  cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc   ................
0x000002099d4c0030  cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc   ................

0x000000009d4c0000 55               PUSH EBP
0x000000009d4c0001 48               DEC EAX
0x000000009d4c0002 8d2c24           LEA EBP, [ESP]
0x000000009d4c0005 48               DEC EAX
0x000000009d4c0006 83ec20           SUB ESP, 0x20
0x000000009d4c0009 48               DEC EAX
0x000000009d4c000a 8b01             MOV EAX, [ECX]
0x000000009d4c000c 48               DEC EAX
0x000000009d4c000d 8b4908           MOV ECX, [ECX+0x8]
```

VOLATILITY 3: MALFIND

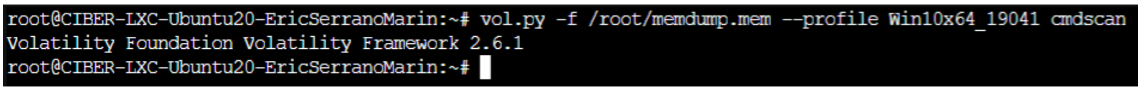
vol3.py -f /root/memdump.mem windows.malfind



```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol3.py -f /root/memdump.mem windows.malfind
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Hexdump Disasm

2804    MsMpEng.exe     0x209946f0000   0x209946f0fff   VadS    PAGE_EXECUTE_READWRITE  1       1       Disabled
55 48 8d 2c 24 48 83 ec UH.,$H..
20 48 8b 01 48 8b 49 08 .H..H.I.
ff d0 48 8d 65 00 5d c3 ..H.e.].
cc cc cc cc cc cc cc cc ........
cc cc cc cc cc cc cc cc ........
cc cc cc cc cc cc cc cc ........
cc cc cc cc cc cc cc cc ........
cc cc cc cc cc cc cc cc ........        55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08 ff d0 48 8d 65 00 5d c3 cc cc cc cc cc
 cc cc cc cc cc cc cc
2804    MsMpEng.exe     0x20999ac0000   0x20999ac0fff   VadS    PAGE_EXECUTE_READWRITE  1       1       Disabled
55 48 8d 2c 24 48 83 ec UH.,$H..
20 48 8b 01 48 8b 49 08 .H..H.I.
ff d0 48 8d 65 00 5d c3 ..H.e.].
cc cc cc cc cc cc cc cc ........
cc cc cc cc cc cc cc cc ........
cc cc cc cc cc cc cc cc ........
cc cc cc cc cc cc cc cc ........
cc cc cc cc cc cc cc cc ........        55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08 ff d0 48 8d 65 00 5d c3 cc cc cc cc cc
 cc cc cc cc cc cc cc
2804    MsMpEng.exe     0x20999ad0000   0x20999ad0fff   VadS    PAGE_EXECUTE_READWRITE  1       1       Disabled
55 48 8d 2c 24 48 83 ec UH.,$H..
20 48 8b 01 48 8b 49 08 .H..H.I.
ff d0 48 8d 65 00 5d c3 ..H.e.].
cc cc cc cc cc cc cc cc ........
cc cc cc cc cc cc cc cc ........
cc cc cc cc cc cc cc cc ........
cc cc cc cc cc cc cc cc ........
cc cc cc cc cc cc cc cc ........        55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08 ff d0 48 8d 65 00 5d c3 cc cc cc cc cc
 cc cc cc cc cc cc cc
```

VOLATILITY 2: CMDSCAN

El plugin cmdscan se utiliza para recuperar comandos ejecutados por procesos a través de la línea de comandos o terminal. Esto puede ser útil para investigar la actividad del sistema y la ejecución de comandos en una investigación forense.



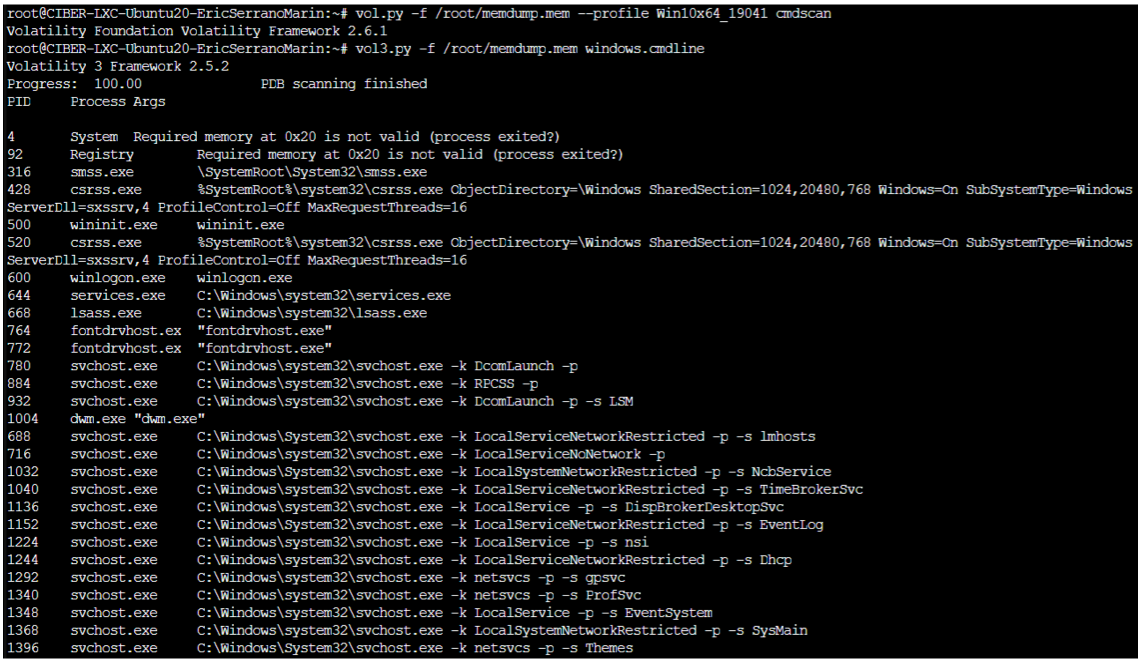
```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol.py -f /root/memdump.mem --profile Win10x64_19041 cmdscan
Volatility Foundation Volatility Framework 2.6.1
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# 
```

Como se puede observar me coge bien el comando, pero no da salida.

VOLATILITY 3: CMDSCAN

No es CMDSCAN como tal, pero hay una alternativa, que se llama CMDLINE.

vol3.py -f /root/memdump.mem windows.cmdline



```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol.py -f /root/memdump.mem --profile Win10x64_19041 cmdscan
Volatility Foundation Volatility Framework 2.6.1
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol3.py -f /root/memdump.mem windows.cmdline
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
PID     Process Args

4       System  Required memory at 0x20 is not valid (process exited?)
92      Registry        Required memory at 0x20 is not valid (process exited?)
316     smss.exe        \SystemRoot\System32\smss.exe
428     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows
ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
500     wininit.exe     wininit.exe
520     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows
ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
600     winlogon.exe    winlogon.exe
644     services.exe    C:\Windows\system32\services.exe
668     lsass.exe       C:\Windows\system32\lsass.exe
764     fontdrvhost.ex  "fontdrvhost.exe"
772     fontdrvhost.ex  "fontdrvhost.exe"
780     svchost.exe     C:\Windows\system32\svchost.exe -k DcomLaunch -p
884     svchost.exe     C:\Windows\system32\svchost.exe -k RPCSS -p
932     svchost.exe     C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
1004    dwm.exe "dwm.exe"
688     svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
716     svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
1032    svchost.exe     C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
1040    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
1136    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s DispBrokerDesktopSvc
1152    svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
1224    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
1244    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
1292    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
1340    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
1348    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
1368    svchost.exe     C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s SysMain
1396    svchost.exe     C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
```

CONCLUSIÓN FINAL

Lo que he visto durante la práctica de ambas herramientas es que Volatility 2 presenta salidas de comandos más claras y ordenadas, lo que me ha facilitado más ver los resultados. Sin embargo, también es verdad que es más complejo a la hora de escribir comandos, ya que hay que añadir detalles como el perfil del sistema operativo. (--profile Win10x64_19041).

Por otro lado Volatility 3 simplifica la escritura de comandos al tener atajos más intuitivos como windows.cmdline, windows.malfind, etc.. también es más rápido, sin embargo, las salidas me parecen menos estructuradas en comparación con Volatility 2.