Análisis Forense

Volatility en Linux.

Jennifer Galván Bejarano

Índice

Introducción

Proceso completo de **análisis forense de memoria volátil en sistemas Linux**, utilizando las herramientas **Volatility 2 y Volatility 3**

Volatility: Es un software opensource para la extracción de artefactos digitales de la memoria volátil (RAM). Está desarrollado y respaldado por The Volatility Foundation.

Requisitos del entorno

Sistema base

Máquina virtual con Debian 12

Acceso a usuario con privilegios de superusuario

Software necesario

Python 2.7 y Python 3

Python 2.7.18 compilado manualmente

pip para Python 2 (get-pip.py)

Herramientas de compilación

build-essential, zlib1g-dev, libffi-dev, libssl-dev, libbz2-dev, etc.

Volatility 2

Repositorio oficial: https://github.com/volatilityfoundation/volatility.git

Dependencias: distorm3, yara-python, pycrypto

Volatility 3

Repositorio oficial: https://github.com/volatilityfoundation/volatility3.git

Dependencias: capstone, distorm3, yara-python

Uso de entorno virtual (venv)

Archivos necesarios

Volcado de memoria RAM (ram.lime)

Perfiles para Volatility 2: .zip con System.map y module.dwarf

Perfiles para Volatility 3: .json y .xz generados con dwarf2json

Herramientas adicionales

LiME: Para generar volcados de memoria en formato .lime

dwarfdump: Para extraer DWARF de vmlinux

dwarf2json + golang-go: Para generar perfiles en JSON para Volatility 3

linux-headers-$(uname -r) y linux-image-$(uname -r)-dbg

Instalación Volatility 2.

Para ello instale python2 porque no lo tiene en el sistema:

1. Edite el repositorio sources.list agregando las líneas
   deb http://deb.debian.org/debian buster main contrib non-free
   deb http://security.debian.org/debian-security buster/updates main
   Actualice
   $ sudo apt update
2. Instale Dependencias para Compilar Python 2.7

**sudo apt install -y build-essential zlib1g-dev libffi-dev libssl-dev **
**libbz2-dev libreadline-dev libsqlite3-dev libncurses5-dev **
liblzma-dev tk-dev uuid-dev wget curl

3. Descargar y Compilar Python 2.7 con Soporte SSL
   $ cd /usr/src
   $ sudo wget https://www.python.org/ftp/python/2.7.18/Python-2.7.18.tgz
   $ sudo tar -xvzf Python-2.7.18.tgz
   $ cd Python-2.7.18

```
jenny@destforense:/usr/src$ sudo wget https://www.python.org/ftp/python/2.7.18/Python-2.7.18.t
gz
--2025-02-05 12:08:59--  https://www.python.org/ftp/python/2.7.18/Python-2.7.18.tgz
Resolviendo www.python.org (www.python.org)... 151.101.132.223
Conectando con www.python.org (www.python.org)[151.101.132.223]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 17539408 (17M) [application/octet-stream]
Grabando a: «Python-2.7.18.tgz»

Python-2.7.18.tgz       100%[=============================>]  16,73M  27,4MB/s    en 0,6s

2025-02-05 12:08:59 (27,4 MB/s) - «Python-2.7.18.tgz» guardado [17539408/17539408]

jenny@destforense:/usr/src$ sudo tar -xvzf Python-2.7.18.tgz
Python-2.7.18/
Python-2.7.18/Include/
Python-2.7.18/Include/tupleobject.h
Python-2.7.18/Include/compile.h
```

Configura la compilación para que use OpenSSL correctamente:

$ sudo ./configure

```
jenny@destforense:/usr/src$ cd Python-2.7.18
jenny@destforense:/usr/src/Python-2.7.18$ sudo ./configure
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking for python2.7... no
checking for python3... python3
checking for --enable-universalsdk... no
checking for --with-universal-archs... no
```

$ sudo make -j$(nproc)

```
jenny@destforense:/usr/src/Python-2.7.18$ sudo make -j$(nproc)
gcc -c -fno-strict-aliasing -g -O2 -DNDEBUG -g -fwrapv -O3 -Wall -Wstrict-prototypes  -I. -IIn
clude -I./Include   -DPy_BUILD_CORE -o Modules/python.o ./Modules/python.c
gcc -c -fno-strict-aliasing -g -O2 -DNDEBUG -g -fwrapv -O3 -Wall -Wstrict-prototypes  -I. -IIn
clude -I./Include   -DPy_BUILD_CORE -o Parser/acceler.o Parser/acceler.c
gcc -c -fno-strict-aliasing -g -O2 -DNDEBUG -g -fwrapv -O3 -Wall -Wstrict-prototypes  -I. -IIn
clude -I./Include   -DPy_BUILD_CORE -o Parser/grammar1.o Parser/grammar1.c
gcc -c -fno-strict-aliasing -g -O2 -DNDEBUG -g -fwrapv -O3 -Wall -Wstrict-prototypes  -I. -IIn
clude -I./Include   -DPy_BUILD_CORE -o Parser/listnode.o Parser/listnode.c
gcc -c -fno-strict-aliasing -g -O2 -DNDEBUG -g -fwrapv -O3 -Wall -Wstrict-prototypes  -I. -IIn
clude -I./Include   -DPy_BUILD_CORE -o Parser/node.o Parser/node.c
```

$ sudo make install

```
jenny@destforense:/usr/src/Python-2.7.18$ sudo make install
/usr/bin/install -c python /usr/local/bin/python2.7
if test -f libpython2.7.a; then \
        if test -n "" ; then \
                /usr/bin/install -c -m 555  /usr/local/bin; \
        else \
                /usr/bin/install -c -m 555 libpython2.7.a /usr/local/lib/libpython2.7.a; \
                if test libpython2.7.a != libpython2.7.a; then \
                        (cd /usr/local/lib; ln -sf libpython2.7.a libpython2.7.a) \
                fi \
        fi; \
else    true; \
fi
```

4. Instalar pip para Python 2

$ wget https://bootstrap.pypa.io/pip/2.7/get-pip.py

$ python2 get-pip.py

```
jenny@destforense:/usr/src/Python-2.7.18$ python2 --version
Python 2.7.18
jenny@destforense:/usr/src/Python-2.7.18$ wget https://bootstrap.pypa.io/pip/2.7/get-pip.py
--2025-02-05 12:12:10--  https://bootstrap.pypa.io/pip/2.7/get-pip.py
Resolviendo bootstrap.pypa.io (bootstrap.pypa.io)... 151.101.132.175
Conectando con bootstrap.pypa.io (bootstrap.pypa.io)[151.101.132.175]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 1908226 (1,8M) [text/x-python]
Grabando a: «get-pip.py»

get-pip.py              100%[=============================>]   1,82M  --.-KB/s    en 0,09s

2025-02-05 12:12:11 (20,0 MB/s) - «get-pip.py» guardado [1908226/1908226]

jenny@destforense:/usr/src/Python-2.7.18$ python2 get-pip.py
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your
Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in Jan
uary 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/l
atest/development/release-process/#python-2-support pip 21.0 will remove support for this func
tionality.
Defaulting to user installation because normal site-packages is not writeable
Collecting pip<21.0
  Downloading pip-20.3.4-py2.py3-none-any.whl (1.5 MB)
     |████████████████████████████████| 1.5 MB 3.8 MB/s
Collecting setuptools<45
  Downloading setuptools-44.1.1-py2.py3-none-any.whl (583 kB)
     |████████████████████████████████| 583 kB 17.8 MB/s
Collecting wheel
  Downloading wheel-0.37.1-py2.py3-none-any.whl (35 kB)
Installing collected packages: pip, setuptools, wheel
  WARNING: The scripts pip, pip2 and pip2.7 are installed in '/home/jenny/.local/bin' which is
 not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-
warn-script-location.
  WARNING: The scripts easy_install and easy_install-2.7 are installed in '/home/jenny/.local/
bin' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-
warn-script-location.
  WARNING: The script wheel is installed in '/home/jenny/.local/bin' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-
warn-script-location.
Successfully installed pip-20.3.4 setuptools-44.1.1 wheel-0.37.1
jenny@destforense:/usr/src/Python-2.7.18$
```

Agrego la carpeta de pip en el PATH y verifico que si se puede usar

$ echo 'export PATH=$HOME/.local/bin:$PATH' >> ~/.bashrc

$ source ~/.bashrc

$ pip -- version

```
jenny@destforense:~$ echo 'export PATH=$HOME/.local/bin:$PATH' >> ~/.bashrc
jenny@destforense:~$ source ~/.bashrc
jenny@destforense:~$ pip --version
pip 20.3.4 from /home/jenny/.local/lib/python2.7/site-packages/pip (python 2.7)
jenny@destforense:~$
```

5. Instalado volatility 2

   $ git clone https://github.com/volatilityfoundation/volatility.git

```
jenny@destforense:~$ git clone https://github.com/volatilityfoundation/volatility.git
Clonando en 'volatility'...
remote: Enumerating objects: 27411, done.
remote: Total 27411 (delta 0), reused 0 (delta 0), pack-reused 27411 (from 1)
Recibiendo objetos: 100% (27411/27411), 21.10 MiB | 7.33 MiB/s, listo.
Resolviendo deltas: 100% (19758/19758), listo.
jenny@destforense:~$ ls
kali-linux-2024.3-live-amd64.iso  respaldos  velociraptor  volatility
jenny@destforense:~$
```

6. Instale dependencias de python2 para que funcione volatility

   $ pip2 install distorm3 yara-python pycrypto

```
jenny@destforense:~$ pip install distorm3 yara-python pycrypto
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your
Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in Jan
uary 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/l
atest/development/release-process/#python-2-support pip 21.0 will remove support for this func
tionality.
Defaulting to user installation because normal site-packages is not writeable
Collecting distorm3
  Downloading distorm3-3.5.2.tar.gz (138 kB)
     |████████████████████████████████| 138 kB 1.9 MB/s
Collecting yara-python
  Downloading yara_python-4.5.1.tar.gz (550 kB)
     |████████████████████████████████| 550 kB 12.3 MB/s
Collecting pycrypto
  Downloading pycrypto-2.6.1.tar.gz (446 kB)
     |████████████████████████████████| 446 kB 33.3 MB/s
Building wheels for collected packages: distorm3, yara-python, pycrypto
  Building wheel for distorm3 (setup.py) ... done
  Created wheel for distorm3: filename=distorm3-3.5.2-cp27-cp27m-linux_x86_64.whl size=122385
sha256=be23f0334627a035cee79f0773d08830bf544180ea32a9918d5212887bdc282b
  Stored in directory: /home/jenny/.cache/pip/wheels/83/31/73/653b4e3e3bbb8db3495ba943e3192fbd
9f8f3015fae69886dd
  Building wheel for yara-python (setup.py) ... done
  Created wheel for yara-python: filename=yara_python-4.5.1-cp27-cp27m-linux_x86_64.whl size=8
53867 sha256=0e1a76b9c8d70825f1c0db26db764dbefe8f38312c2d3595687b84540e0d44bc
  Stored in directory: /home/jenny/.cache/pip/wheels/8c/7a/c2/066bf11071f8c193bc6ba84cb1c5886a
d886cb58c9858dd7fc
  Building wheel for pycrypto (setup.py) ... done
  Created wheel for pycrypto: filename=pycrypto-2.6.1-cp27-cp27m-linux_x86_64.whl size=490567
sha256=3f78aebc17ac12e98d6decda9121d2ce338e31c52a1a3345ae8209a0217fdf90
  Stored in directory: /home/jenny/.cache/pip/wheels/b6/e6/c8/d1eca13628952ceec1d40d96e0a7a138
0460d2349ce0b85312
Successfully built distorm3 yara-python pycrypto
Installing collected packages: distorm3, yara-python, pycrypto
Successfully installed distorm3-3.5.2 pycrypto-2.6.1 yara-python-4.5.1
jenny@destforense:~$
```

7. Cree un script de bash para facilitar la ejecución de volatility y le doy permisos

   $ chmod +x vol.sh

```
  GNU nano 7.2                                    vol2.sh
#!/bin/bash

python2 /home/jenny/volatility/vol.py "$@"
```

8. Verificar que funciona

```
jenny@destforense:~/volatility$ ./vol2.sh -h
Volatility Foundation Volatility Framework 2.6.1
Usage: Volatility - A memory forensics analysis platform.

Options:
  -h, --help            list all available options and their default values.
                        Default values may be set in the configuration file
                        (/etc/volatilityrc)
  --conf-file=/home/jenny/.volatilityrc
```

Preparar Volatility 2 para trabajar con determinados perfiles Linux (linux overlays)

● Descarga perfil de Volatility que se ajusta al volcado del apartado y copialo en el lugar adecuado (overlays/linux) para poder utilizarlo con volatility 2.

$ sudo mv /home/jenny/debian10-4.19.0-23-686.zip /home/jenny/volatility/volatility/plugins/overlays/linux/

```
jenny@destforense:~$ ls
debian10-4.19.0-23-686.zip        ram.lime   velociraptor
kali-linux-2024.3-live-amd64.iso  respaldos  volatility
jenny@destforense:~$ sudo mv /home/jenny/debian10-4.19.0-23-686.zip /home/jenny/volatility/vol
atility/plugins/overlays/linux/
```

Verifico los perfiles que ahora tiene volatility

$ ./vol2.sh --info | grep Linux

```
jenny@destforense:~/volatility$ ./vol2.sh --info | grep Linux
Volatility Foundation Volatility Framework 2.6.1
Linuxdebian10-4_19_0-23-686x86 - A Profile for Linux debian10-4.19.0-23-686 x86
LinuxAMD64PagedMemory          - Linux-specific AMD 64-bit address space.
linux_aslr_shift           - Automatically detect the Linux ASLR shift
linux_banner               - Prints the Linux banner information
linux_yarascan             - A shell in the Linux memory image
jenny@destforense:~/volatility$
```

Verificó que puedo ejecutar volatility conociendo la información del volcado de memoria que me dieron

$ ./vol2.sh -f ram.lime --profile=Linuxdebian10-4_19_0-23-686x86 linux_banner

```
jenny@destforense:~/volatility$ ./vol2.sh -f ram.lime --profile=Linuxdebian10-4_19_0-23-686x86
 linux_banner
Volatility Foundation Volatility Framework 2.6.1
Linux version 4.19.0-23-686 (debian-kernel@lists.debian.org) (gcc version 8.3.0 (Debian 8.3.0-
6)) #1 SMP Debian 4.19.269-1 (2022-12-20)
jenny@destforense:~/volatility$
```

Realizar análisis básico de los volcados de memoria en Linux.

Utiliza el comando “vol.py” y el volcado de memoria del apartado anterior para describir qué información podemos obtener usando los modificadores siguientes:

- **Análisis de procesos**

linux_pslist:

$ ./vol2.sh -f ram.lime --profile=Linuxdebian10-4_19_0-23-686x86 linux_pslist > /home/jenny/rV/pslist.txt

```
jenny@destforense:~/volatility$ cat /home/jenny/rV/pslist.txt
Offset     Name                 Pid             PPid            Uid
 Gid    DTB        Start Time
---------- -------------------- --------------- --------------- ---------
------- ---------- ----------
0xf491cb40 systemd              1               0               0
 0      0x34a8e000 0
0xf4918ac0 kthreadd             2               0               0
 0      ---------- 0
0xf4919580 rcu_gp               3               2               0
 0      ---------- 0
0xf491b5c0 rcu_par_gp           4               2               0
 0      ---------- 0
0xf4918000 kworker/0:0H         6               2               0
 0      ---------- 0
0xf491a040 mm_percpu_wq         8               2               0
 0      ---------- 0
0xf491e0c0 ksoftirqd/0          9               2               0
 0      ---------- 0
0xf491eb80 rcu_sched            10              2               0
 0      ---------- 0
0xf491ab00 rcu_bh               11              2               0
 0      ---------- 0
0xf493cb40 migration/0          12              2               0
 0      ---------- 0
0xf493b5c0 cpuhp/0              14              2               0
 0      ---------- 0
0xf493c080 cpuhp/1              15              2               0
 0      ---------- 0
0xf4938000 migration/1          16              2               0
 0      ---------- 0
0xf493d600 ksoftirqd/1          17              2               0
 0      ---------- 0
0xf493e0c0 kworker/1:0H         19              2               0
```

linux_psaux:

$ ./vol2.sh -f ram.lime --profile=Linuxdebian10-4_19_0-23-686x86 linux_psaux > /home/jenny/rV/psaux.txt

```
jenny@destforense:~/rV$ cat psaux.txt
Pid     Uid     Gid     Arguments
1       0       0       /sbin/init
2       0       0       [kthreadd]
3       0       0       [rcu_gp]
4       0       0       [rcu_par_gp]
6       0       0       [kworker/0:0H]
8       0       0       [mm_percpu_wq]
9       0       0       [ksoftirqd/0]
10      0       0       [rcu_sched]
11      0       0       [rcu_bh]
12      0       0       [migration/0]
14      0       0       [cpuhp/0]
15      0       0       [cpuhp/1]
16      0       0       [migration/1]
17      0       0       [ksoftirqd/1]
19      0       0       [kworker/1:0H]
20      0       0       [kdevtmpfs]
21      0       0       [netns]
22      0       0       [kauditd]
23      0       0       [khungtaskd]
24      0       0       [oom_reaper]
25      0       0       [writeback]
26      0       0       [kcompactd0]
27      0       0       [ksmd]
28      0       0       [khugepaged]
```

linux_pstree:

$ ./vol2.sh -f ram.lime --profile=Linuxdebian10-4_19_0-23-686x86 linux_pstree > /home/jenny/rV/pstree.txt

```
jenny@destforense:~/rV$ cat ps
psaux.txt   pslist.txt  pstree.txt
jenny@destforense:~/rV$ cat pstree.txt
Name                 Pid             Uid
systemd              1
.systemd-journal     202
.systemd-udevd       219
.systemd-timesyn     241             101
.systemd-logind      330
.rsyslogd            332
.dbus-daemon         335             104
.cron                339
.sshd                350
..sshd               392
...sshd              409             1000
....bash             410             1000
.....su              606             1000
......bash           607
.......insmod        11218
.login               351
..bash               385
.dhclient            348
.systemd             374
..(sd-pam)           375
.systemd             395             1000
..(sd-pam)           396             1000
[kthreadd]           2
.[rcu_gp]            3
.[rcu_par_gp]        4
.[kworker/0:0H]      6
.[mm_percpu_wq]      8
```

linux_cpuinfo:

$ ./vol2.sh -f ram.lime --profile=Linuxdebian10-4_19_0-23-686x86 linux_cpuinfo > /home/jenny/rV/cpuinfo.txt

```
jenny@destforense:~/rV$ cat cpuinfo.txt
Processor    Vendor            Model
------------ ----------------- -----
0            GenuineIntel      Intel(R) Core(TM) i3-4130T CPU @ 2.90GHz
1            GenuineIntel      Intel(R) Core(TM) i3-4130T CPU @ 2.90GHz
jenny@destforense:~/rV$
```

- **Análisis de red**

linux_arp:

$ ./vol2.sh -f ram.lime --profile=Linuxdebian10-4_19_0-23-686x86 linux_arp> /home/jenny/rV/arp.txt

```
jenny@destforense:~/rV$ cat arp.txt
[192.168.10.1                          ] at 64:d1:54:ec:e9:9d    on enp0s3
[192.168.10.8                          ] at 08:00:27:3f:5c:82    on enp0s3
[192.168.10.20                         ] at f8:32:e4:72:f8:c6    on enp0s3
[fe80::66d1:54ff:feec:e99d             ] at 64:d1:54:ec:e9:9d    on enp0s3
[ff02::1:ffba:fc21                     ] at 33:33:ff:ba:fc:21    on enp0s3
[ff02::2                               ] at 33:33:00:00:00:02    on enp0s3
[ff02::16                              ] at 33:33:00:00:00:16    on enp0s3
jenny@destforense:~/rV$
```

linux_ifconfig:

$ ./vol2.sh -f ram.lime --profile=Linuxdebian10-4_19_0-23-686x86 linux_ifconfig > /home/jenny/rV/ifconfig.txt

```
jenny@destforense:~/rV$ cat cpuinfo.txt
Processor    Vendor          Model
---------- --------------- -----
0           GenuineIntel     Intel(R) Core(TM) i3-4130T CPU @ 2.90GHz
1           GenuineIntel     Intel(R) Core(TM) i3-4130T CPU @ 2.90GHz
jenny@destforense:~/rV$ cat arp.txt
[192.168.10.1                          ] at 64:d1:54:ec:e9:9d    on enp0s3
[192.168.10.8                          ] at 08:00:27:3f:5c:82    on enp0s3
[192.168.10.20                         ] at f8:32:e4:72:f8:c6    on enp0s3
[fe80::66d1:54ff:feec:e99d             ] at 64:d1:54:ec:e9:9d    on enp0s3
[ff02::1:ffba:fc21                     ] at 33:33:ff:ba:fc:21    on enp0s3
[ff02::2                               ] at 33:33:00:00:00:02    on enp0s3
[ff02::16                              ] at 33:33:00:00:00:16    on enp0s3
jenny@destforense:~/rV$ cat ifconfig.txt
Interface        IP Address           MAC Address        Promiscous Mode
---------------- -------------------- ------------------ ---------------
lo               127.0.0.1            00:00:00:00:00:00  False
enp0s3           192.168.10.226       08:00:27:ba:fc:21  False
jenny@destforense:~/rV$
ort MobaXterm by subscribing to the professional edition here:  https://mobaxterm.mobatek.net
```

linux_route_cache:

$ ./vol2.sh -f ram.lime --profile=Linuxdebian10-4_19_0-23-686x86 linux_route_cache > /home/jenny/rV/route_cache.txt

```
jenny@destforense:~/rV$ cat route_cache.txt
Interface        Destination          Gateway
---------------- -------------------- -------
jenny@destforense:~/rV$
```

linux_netstat:

$ ./vol2.sh -f ram.lime --profile=Linuxdebian10-4_19_0-23-686x86 linux_netstat> /home/jenny/rV/netstat.txt

```
jenny@destforense:~/volatility$ ./vol2.sh -f ram.lime --profile=Linuxdebian10-4_19_0-23-686x86 linux_route_cache > /home/jenny/rV/
route_cache.txt
Volatility Foundation Volatility Framework 2.6.1
ERROR   : volatility.debug    : This plugin does not support this profile. The Linux routing cache was deleted in 3.6.x. See: http
s://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=89aef8921bfbac22f00e04f8450f6e447db13e42
jenny@destforense:~/volatility$
```

- **Ficheros y análisis del kernel**

linux_enumerate_files:

$ ./vol2.sh -f ram.lime --profile=Linuxdebian10-4_19_0-23-686x86 linux_enumerate_files > /home/jenny/rV/enumerate_files.txt

```
jenny@destforense:~/rV$ cat enumerate_files.txt
Inode Address Inode Number              Path
------------ ------------------------ ----
   0xf600b840                    10328 /sys/fs/cgroup
   0xf61fd4d0                    10363 /sys/fs/cgroup/rdma
   0xf61fcfa8                    10362 /sys/fs/cgroup/cpuset
   0xf61fc3a0                    10361 /sys/fs/cgroup/pids
   0xf61fd688                    10360 /sys/fs/cgroup/memory
   0xf61fdd68                    10359 /sys/fs/cgroup/freezer
   0xf61fd9f8                    10358 /sys/fs/cgroup/perf_event
   0xf61fcc38                    10357 /sys/fs/cgroup/net_cls
   0xf66cec38                    10356 /sys/fs/cgroup/net_prio
   0xf66ce558                    10355 /sys/fs/cgroup/net_cls,net_prio
   0xf66cea80                    10354 /sys/fs/cgroup/devices
   0xf66cf9f8                    10353 /sys/fs/cgroup/cpuacct
   0xf604fbb0                    10352 /sys/fs/cgroup/cpu
   0xf604e030                    10351 /sys/fs/cgroup/cpu,cpuacct
   0xf65da558                    10350 /sys/fs/cgroup/blkio
   0xf600a8c8                    10330 /sys/fs/cgroup/systemd
   0xf600b318                    10329 /sys/fs/cgroup/unified
   0xf413f3e8                        1 /sys
   0xf41bc620                        5 /sys/dev
   0xf42ebd18                        7 /sys/dev/char
   0xf3d42f50                     7691 /sys/dev/char/4:64
   0xf3d43260                     7789 /sys/dev/char/4:66
   0xf3d43570                     7740 /sys/dev/char/4:65
   0xf3d42620                     7838 /sys/dev/char/4:67
   0xf3c29a08                    13481 /sys/dev/char/13:33
```

linux_find_file:

$ ./vol2.sh -f ram.lime --profile=Linuxdebian10-4_19_0-23-686x86 linux_find_file -F 'etc/passwd' > /home/jenny/rV2/find_file.txt

linux_recover_filesystem:

$ sudo ./vol2.sh -f ram.lime --profile=Linuxdebian10-4_19_0-23-686x86 linux_filesystem > /home/jenny/rV/filesystem.txt

$ ./vol2.sh -f ram.lime --profile=Linuxdebian10-4_19_0-23-686x86 linux_lsof > /home/jenny/rV/linux_lsof.txt

```
jenny@destforense:~/rV$ cat linux_lsof.txt
Offset             Name                           Pid      FD       Path
------------------ ------------------------------ -------- -------- ----
0x00000000f491cb40 systemd                             1        0 /dev/null
0x00000000f491cb40 systemd                             1        1 /dev/null
0x00000000f491cb40 systemd                             1        2 /dev/null
0x00000000f491cb40 systemd                             1        3 /dev/kmsg
0x00000000f491cb40 systemd                             1        4 anon_inode:[8319]
0x00000000f491cb40 systemd                             1        5 anon_inode:[8319]
0x00000000f491cb40 systemd                             1        6 anon_inode:[8319]
0x00000000f491cb40 systemd                             1        7 /sys/fs/cgroup/unified
0x00000000f491cb40 systemd                             1        8 anon_inode:[8319]
0x00000000f491cb40 systemd                             1        9 socket:[10496]
0x00000000f491cb40 systemd                             1       10 anon_inode:[8319]
0x00000000f491cb40 systemd                             1       11 anon_inode:[8319]
0x00000000f491cb40 systemd                             1       13 /proc/1/mountinfo
0x00000000f491cb40 systemd                             1       14 anon_inode:[8319]
0x00000000f491cb40 systemd                             1       15 /proc/swaps
0x00000000f491cb40 systemd                             1       16 socket:[10498]
0x00000000f491cb40 systemd                             1       17 socket:[10500]
0x00000000f491cb40 systemd                             1       18 socket:[10501]
0x00000000f491cb40 systemd                             1       19 socket:[10502]
0x00000000f491cb40 systemd                             1       23 socket:[13866]
0x00000000f491cb40 systemd                             1       24 anon_inode:[8319]
0x00000000f491cb40 systemd                             1       25 anon_inode:[8319]
0x00000000f491cb40 systemd                             1       26 socket:[10509]
0x00000000f491cb40 systemd                             1       27 socket:[10512]
0x00000000f491cb40 systemd                             1       28 socket:[10516]
0x00000000f491cb40 systemd                             1       29 anon_inode:[8319]
```

linux_mount:

$ ./vol2.sh -f ram.lime --profile=Linuxdebian10-4_19_0-23-686x86 linux_mount > /home/jenny/rV/mount.txt

```
jenny@destforense:~/rV$ cat mount.txt
tmpfs                /sys/fs/cgroup                tmpfs       ro,nosuid,nodev,noexec
sysfs                /sys                          sysfs       ro,relatime,nosuid,nodev,noexec
tmpfs                /home                         tmpfs       ro,relatime,nosuid,noexec
debugfs              /sys/kernel/debug             debugfs     ro,relatime
/dev/sda1            /                             ext4        ro,relatime
tmpfs                /dev                          tmpfs       ro,nosuid,noexec
udev                 /dev                          devtmpfs    rw,relatime,nosuid
cgroup               /sys/fs/cgroup/blkio          cgroup      ro,relatime,nosuid,nodev,noexec
cgroup               /sys/fs/cgroup/pids           cgroup      rw,relatime,nosuid,nodev,noexec
proc                 /proc                         proc        rw,relatime,nosuid,nodev,noexec
systemd-1            /proc/sys/fs/binfmt_misc      autofs      rw,relatime
cgroup               /sys/fs/cgroup/net_cls,net_prio cgroup    rw,relatime,nosuid,nodev,noexec
cgroup               /sys/fs/cgroup/perf_event     cgroup      rw,relatime,nosuid,nodev,noexec
hugetlbfs            /dev/hugepages                hugetlbfs   rw,relatime
tmpfs                /dev/shm                      tmpfs       rw,nosuid,nodev
securityfs           /sys/kernel/security          securityfs  rw,relatime,nosuid,nodev,noexec
cgroup               /sys/fs/cgroup/cpuset         cgroup      rw,relatime,nosuid,nodev,noexec
cgroup               /sys/fs/cgroup/devices        cgroup      rw,relatime,nosuid,nodev,noexec
tmpfs                /run/user/0                   tmpfs       rw,relatime,nosuid,nodev
pstore               /sys/fs/pstore                pstore      rw,relatime,nosuid,nodev,noexec
mqueue               /dev/mqueue                   mqueue      rw,relatime
```

linux_mount_cache:

$ ./vol2.sh -f ram.lime --profile=Linuxdebian10-4_19_0-23-686x86 linux_mount_cache > /home/jenny/rV/mount_cache.txt

linux_bash:

$ ./vol2.sh -f ram.lime --profile=Linuxdebian10-4_19_0-23-686x86 linux_bash > /home/jenny/rV/bash.txt

```
jenny@destforense:~/rV$ cat bash.txt
Pid      Name                 Command Time                   Command
-------- -------------------- ------------------------------ -------
     385 bash                 2023-03-15 13:25:03 UTC+0000   find . -name "linux"
     385 bash                 2023-03-15 13:25:03 UTC+0000   apt install linux-headers-$(uname -a)
     385 bash                 2023-03-15 13:25:03 UTC+0000   apt install linux-headers-$(uname -r)
     385 bash                 2023-03-15 13:25:03 UTC+0000   ip address
     385 bash                 2023-03-15 13:25:03 UTC+0000   ls
     385 bash                 2023-03-15 13:25:03 UTC+0000   cd tools/
     385 bash                 2023-03-15 13:25:03 UTC+0000   make
     385 bash                 2023-03-15 13:25:03 UTC+0000   S??u?????
     385 bash                 2023-03-15 13:25:03 UTC+0000   uname -a
     385 bash                 2023-03-15 13:25:03 UTC+0000   uname -r
     385 bash                 2023-03-15 13:25:03 UTC+0000   uname -a
     385 bash                 2023-03-15 13:25:03 UTC+0000   cd plugins/linux/
     385 bash                 2023-03-15 13:25:03 UTC+0000   ls
     385 bash                 2023-03-15 13:25:03 UTC+0000   ls
     385 bash                 2023-03-15 13:25:03 UTC+0000   cd volatility/
     385 bash                 2023-03-15 13:25:03 UTC+0000   apt search linux-headers | grep headers
     385 bash                 2023-03-15 13:25:03 UTC+0000   apt search linux-headers | grep headers | more
     385 bash                 2023-03-15 13:25:03 UTC+0000   ls
     385 bash                 2023-03-15 13:25:03 UTC+0000   make
     385 bash                 2023-03-15 13:25:03 UTC+0000   apt update
     385 bash                 2023-03-15 13:25:03 UTC+0000   cd linux
     385 bash                 2023-03-15 13:25:03 UTC+0000   git clone https://github.com/volatilityfoundation/volatility.git
     385 bash                 2023-03-15 13:25:03 UTC+0000   apt install build-essential
     385 bash                 2023-03-15 13:25:03 UTC+0000   make
     385 bash                 2023-03-15 13:25:03 UTC+0000   cd ..
     385 bash                 2023-03-15 13:25:03 UTC+0000   rm -R volatility/
     385 bash                 2023-03-15 13:25:03 UTC+0000   apt install linux-headers-$(uname -a)
     385 bash                 2023-03-15 13:25:03 UTC+0000   apt install volatility
     385 bash                 2023-03-15 13:25:03 UTC+0000   cd ..
     385 bash                 2023-03-15 13:25:03 UTC+0000   apt install build-essential
     385 bash                 2023-03-15 13:25:03 UTC+0000   cd ..
     385 bash                 2023-03-15 13:25:03 UTC+0000   apt install linux-headers-$(uname -r)
     385 bash                 2023-03-15 13:25:03 UTC+0000   cd ..
     385 bash                 2023-03-15 13:25:03 UTC+0000   dwarfdump
```

linux_dmesg:

$ ./vol2.sh -f ram.lime --profile=Linuxdebian10-4_19_0-23-686x86 linux_dmesg > /home/jenny/rV/dmesg.txt

```
jenny@destforense:~/rV$ cat dmesg.txt
[0.0] Linux version 4.19.0-23-686 (debian-kernel@lists.debian.org) (gcc version 8.3.0 (Debian 8.3.0-6)) #1 SMP Debian 4.19.269-1
2022-12-20)
[0.0] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
[0.0] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
[0.0] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
[0.0] x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
[0.0] x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard' format.
[0.0] BIOS-provided physical RAM map:
[0.0] BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
[0.0] BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
[0.0] BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
[0.0] BIOS-e820: [mem 0x0000000000100000-0x00000003ffefffff] usable
[0.0] BIOS-e820: [mem 0x00000003fff0000-0x00000003ffffffff] ACPI data
[0.0] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
[0.0] BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
[0.0] BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
[0.0] Notice: NX (Execute Disable) protection cannot be enabled: non-PAE kernel!
[0.0] SMBIOS 2.5 present.
[0.0] DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
[0.0] Hypervisor detected: KVM
[0.0] kvm-clock: Using msrs 4b564d01 and 4b564d00
[831.0] kvm-clock: cpu 0, msr 9a30001, primary cpu clock
[904.0] kvm-clock: using sched offset of 7370052075 cycles
[3395.0] clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 881590591483 ns
[5981.0] tsc: Detected 2893.298 MHz processor
[1780280.0] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
[1782221.0] e820: remove [mem 0x000a0000-0x000fffff] usable
[1786001.0] last_pfn = 0x3fff0 max_arch_pfn = 0x100000
[1797223.0] MTRR default type: uncachable
[1797967.0] MTRR variable ranges disabled:
[1798647.0] Disabled
[1799773.0] x86/PAT: MTRRs disabled, skipping PAT initialization too.
[1802657.0] CPU MTRRs all blank - virtualized system.
[1805082.0] x86/PAT: Configuration [0-7]: WB  WT  UC- UC  WB  WT  UC- UC
[1835283.0] found SMP MP-table at [mem 0x0009fff0-0x0009ffff]
[68949783.0] initial memory mapped: [mem 0x00000000-0x09ffffff]
[69017833.0] RAMDISK: [mem 0x3568b000-0x36b3cfff]
[69022980.0] ACPI: Early table checksum verification disabled
[69046561.0] ACPI: RSDP 0x00000000000E0000 000024 (v02 VBOX  )
[69050763.0] ACPI: XSDT 0x00000003FFF0030 00003C (v01 VBOX   VBOXXSDT 00000001 ASL  00000061)
[69056389.0] ACPI: FACP 0x00000003FFF00F0 0000F4 (v04 VBOX   VBOXFACP 00000001 ASL  00000061)
[69062049.0] ACPI: DSDT 0x00000003FFF0610 002353 (v02 VBOX   VBOXBIOS 00000002 INTL 20100528)
[69065546.0] ACPI: FACS 0x00000003FFF0200 000040
```

Generar perfiles específicos para Volatility.

Antes de continuar, necesitamos asegurarnos de que tu sistema tiene las herramientas adecuadas.

1. Instalar las herramientas necesarias:

dwarfdump: Este paquete es una herramienta para examinar información de depuración en formato DWARF, que se encuentra en los binarios compilados (como el kernel de Linux).
Es fundamental porque nos permite extraer los símbolos de depuración desde vmlinux y generar el archivo module.dwarf, que Volatility necesita para analizar estructuras internas de la memoria.
build-essential: Es un metapaquete que instala las herramientas básicas para compilar software en Debian/Ubuntu.
linux-headers-$(uname -r): Instala los archivos de cabecera (headers) del kernel que coinciden con la versión del sistema.
Estos archivos son esenciales para compilar módulos del kernel y entender sus estructuras de datos. Volatility necesita esta información para interpretar correctamente la memoria.
$ sudo apt install -y dwarfdump build-essential
$ sudo apt install -y linux-headers-$(uname -r)

Ahora necesitamos obtener la versión exacta del kernel y descargar los archivos de símbolos necesarios.
$ uname -r
verifique si el archivo de configuración del kernel está presente con el siguiente comando:
$ ls -l /boot/config-$(uname -r)

```
jenny@destforense:/usr/src$ uname -r
6.1.0-30-amd64
jenny@destforense:/usr/src$ ls -l /boot/config-$(uname -r)
-rw-r--r-- 1 root root 259624 ene 12 20:58 /boot/config-6.1.0-30-amd64
```

2. descargar System.map

Es crucial en la generación del perfil de Volatility 2 porque proporciona los símbolos de depuración del kernel, que incluyen información detallada sobre sus estructuras de datos y funciones.
$ sudo apt install linux-image-$(uname -r)-dbg
Buscar la ruta del paquete de depuración
$ ls -l /usr/lib/debug/boot/System.map-$(uname -r)

```
jenny@destforense:/usr/src$ sudo apt install linux-image-$(uname -r)-dbg
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
linux-image-6.1.0-30-amd64-dbg ya está en su versión más reciente (6.1.124-1).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
jenny@destforense:/usr/src$ sudo find /usr/src -name "System.map*"
jenny@destforense:/usr/src$ ls -l /usr/lib/debug/boot/System.map-$(uname -r)
-rw-r--r-- 1 root root 3894030 ene 12 20:58 /usr/lib/debug/boot/System.map-6.1.0-30-amd64
```

3. Generar el archivo DWARF

Ahora vamos a generar el archivo DWARF, que contiene la información de depuración necesaria para construir el perfil de Volatility.

Primero verifique la presencia del archivo vmlinux:

$ ls -l /usr/lib/debug/boot/vmlinux-$(uname -r)

Extraje la información DWARF de esta manera funciona correctamente, el problema es que vuelca el module.dwarf es muy pesado

dwarfdump /usr/lib/debug/boot/vmlinux-$(uname -r) > module.dwarf

```
jenny@destforense:/usr/src$ ls -l /usr/lib/debug/boot/vmlinux-$(uname -r)
-rw-r--r-- 1 root root 627917752 ene 12 20:58 /usr/lib/debug/boot/vmlinux-6.1.0-30-amd64
jenny@destforense:/usr/src$ cd
jenny@destforense:~$ dwarfdump /usr/lib/debug/boot/vmlinux-$(uname -r) > module.dwarf
jenny@destforense:~$ ls -l module.dwarf
-rw-r--r-- 1 jenny jenny 3464527872 feb  6 11:05 module.dwarf
jenny@destforense:~$ ls -lh module.dwarf
-rw-r--r-- 1 jenny jenny 3,3G feb  6 11:05 module.dwarf
```

4. Cree el perfil para Volatility 2

$ zip Debian12-6.1.0-30-amd64.zip module.dwarf /usr/lib/debug/boot/System.map-$(uname -r)

ls -lh Debian12-6.1.0-30-amd64.zip

Muevo el fichero a la ruta que le corresponde

$ sudo mv /home/jenny/Debian12-6.1.0-30-amd64.zip /home/jenny/volatility/volatility/plugins/overlays/linux/

```
jenny@destforense:~$ zip Debian12-6.1.0-30-amd64.zip module.dwarf /usr/lib/debug/boot/Syst
em.map-$(uname -r)
  adding: module.dwarf (deflated 94%)
  adding: usr/lib/debug/boot/System.map-6.1.0-30-amd64 (deflated 79%)
jenny@destforense:~$ ls
Debian12-6.1.0-30-amd64.zip  module.dwarf  rV2  volatility
jenny@destforense:~$ sudo mv /home/jenny/volatility/volatility/plugins/overlays/linux/
mv: falta el fichero de destino después de '/home/jenny/volatility/volatility/plugins/over
lays/linux/'
```

5. Comprobe el perfil en volatility2

$ ./vol2.sh --info | grep Linux

```
jenny@destforense:~/volatility$ ./vol2.sh --info | grep Linux
Volatility Foundation Volatility Framework 2.6.1
LinuxDebian12-6_1_0-30-amd64x64 - A Profile for Linux Debian12-6.1.0-30-amd64 x64
Linuxdebian10-4_19_0-23-686x86  - A Profile for Linux debian10-4.19.0-23-686 x86
LinuxAMD64PagedMemory          - Linux-specific AMD 64-bit address space.
linux_aslr_shift           - Automatically detect the Linux ASLR shift
linux_banner               - Prints the Linux banner information
linux_yarascan             - A shell in the Linux memory image
jenny@destforense:~/volatility$
```

También se hace instalando **dwarfdump** dentro de **/home/jenny/volatility/tools/linux** y después se ejecuta **make** el archivo que se crea es mucho menos pesado y es lo ideal se guarda en zip y se agrega en la ruta, **/home/jenny/volatility/volatility/plugins/overlays/linux/**

Para ello y para que me funcionara correctamente instale los headers

 # apt reinstall linux-headers-6.1.0-30-common

verifique en donde se encuentra la ruta

 # ls -l /usr/src/linux-headers-6.1.0-30-common

```
root@destforense:/home/jenny/volatility2/tools/linux# apt reinstall linux-headers-6.1.0-30-c
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
  linux-image-6.1.0-26-amd64
Utilice «sudo apt autoremove» para eliminarlo.
0 actualizados, 0 nuevos se instalarán, 1 reinstalados, 0 para eliminar y 0 no actualizados.
Se necesita descargar 10,1 MB de archivos.
Se utilizarán 0 B de espacio de disco adicional después de esta operación.
Des:1 http://deb.debian.org/debian bookworm-updates/main amd64 linux-headers-6.1.0-30-common
.124-1 [10,1 MB]
Descargados 10,1 MB en 6s (1.695 kB/s)
(Leyendo la base de datos ... 88398 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../linux-headers-6.1.0-30-common_6.1.124-1_all.deb ...
Desempaquetando linux-headers-6.1.0-30-common (6.1.124-1) sobre (6.1.124-1) ...
Configurando linux-headers-6.1.0-30-common (6.1.124-1) ...
root@destforense:/home/jenny/volatility2/tools/linux# ls -l /usr/src/linux-headers-6.1.0-30-
total 80
drwxr-xr-x 15 root root  4096 feb  8 20:28 arch
drwxr-xr-x 31 root root  4096 feb  8 20:28 include
-rw-r--r--  1 root root 71990 ene 12 20:58 Makefile
lrwxrwxrwx  1 root root    34 ene 12 20:58 scripts -> ../../lib/linux-kbuild-6.1/scripts
lrwxrwxrwx  1 root root    32 ene 12 20:58 tools -> ../../lib/linux-kbuild-6.1/tools
```

Edite el module.c agregando esta regla al final

 # nano /home/jenny/volatility2/tools/linux/module.c

MODULE_LICENSE("GPL");

```
 GNU nano 7.2                  /home/jenny/volatility2/tools/linux/module.c
        atomic_t count;          /* use count */
        atomic_t in_use;         /* number of callers into module in progress; */
                                 /* negative -> it's going away RSN */
        struct completion *pde_unload_completion;
        struct list_head pde_openers;   /* who did ->open, but not ->release */
        spinlock_t pde_unload_lock; /* proc_fops checks and pde_users bumps */
        u8 namelen;
        char name[];
    };
#else
    struct proc_dir_entry {
        unsigned int low_ino;
        umode_t mode;
        nlink_t nlink;
        kuid_t uid;
        kgid_t gid;
        loff_t size;
        const struct inode_operations *proc_iops;
        const struct file_operations *proc_fops;
        struct proc_dir_entry *parent;
        struct rb_root subdir;
        struct rb_node subdir_node;
        void *data;
        atomic_t count;     /* use count */
        atomic_t in_use;    /* number of callers into module in progress; */
                /* negative -> it's going away RSN */
        struct completion *pde_unload_completion;
        struct list_head pde_openers;   /* who did ->open, but not ->release */
        spinlock_t pde_unload_lock; /* proc_fops checks and pde_users bumps */
        u8 namelen;
        char name[];
    };
#endif
#endif

struct resource resource;

MODULE_LICENSE("GPL");
```

Compilo con **make** y listo se crea el archivo **module.dwarf**

```
root@destforense:/home/jenny/volatility2/tools/linux# make
make -C //lib/modules/6.1.0-30-amd64/build CONFIG_DEBUG_INFO=y M="/home/jenny/volatility2/tools/linu
x" modules
make[1]: se entra en el directorio '/usr/src/linux-headers-6.1.0-30-amd64'
  CC [M]  /home/jenny/volatility2/tools/linux/module.o
  MODPOST /home/jenny/volatility2/tools/linux/Module.symvers
  CC [M]  /home/jenny/volatility2/tools/linux/module.mod.o
  LD [M]  /home/jenny/volatility2/tools/linux/module.ko
  BTF [M] /home/jenny/volatility2/tools/linux/module.ko
Skipping BTF generation for /home/jenny/volatility2/tools/linux/module.ko due to unavailability of v
mlinux
make[1]: se sale del directorio '/usr/src/linux-headers-6.1.0-30-amd64'
dwarfdump -di module.ko > module.dwarf
make -C //lib/modules/6.1.0-30-amd64/build M="/home/jenny/volatility2/tools/linux" clean
make[1]: se entra en el directorio '/usr/src/linux-headers-6.1.0-30-amd64'
  CLEAN   /home/jenny/volatility2/tools/linux/Module.symvers
make[1]: se sale del directorio '/usr/src/linux-headers-6.1.0-30-amd64'
root@destforense:/home/jenny/volatility2/tools/linux# ls
kcore  Makefile  Makefile.enterprise  module.c  module.dwarf
root@destforense:/home/jenny/volatility2/tools/linux# history
```

Creo el archivo zip con el nombre que le quiera poner

 # zip Debian12-6.1.0-30-amd64.zip module.dwarf /usr/lib/debug/boot/System.map-$(uname -r)

```
root@destforense:/home/jenny/volatility2/tools/linux# zip Debian12-6.1.0-30-amd64.zip module.dwarf /
usr/lib/debug/boot/System.map-$(uname -r)
  adding: module.dwarf (deflated 91%)
  adding: usr/lib/debug/boot/System.map-6.1.0-30-amd64 (deflated 79%)
root@destforense:/home/jenny/volatility2/tools/linux# ls
Debian12-6.1.0-30-amd64.zip  kcore  Makefile  Makefile.enterprise  module.c  module.dwarf
root@destforense:/home/jenny/volatility2/tools/linux# mv Debian12-6.1.0-30-amd64.zip /home/jenny/vol
atility2/volatility/plugins/overlays/linux/
root@destforense:/home/jenny/volatility2/tools/linux# exit
exit
```

Reviso que volatility reconozca el perfil

$ ./vol2.sh --info | grep Linux

```
jenny@destforense:~/volatility2$ ./vol2.sh --info | grep Linux
Volatility Foundation Volatility Framework 2.6.1
LinuxDebian12-6_1_0-30-amd6411x64 - A Profile for Linux Debian12-6.1.0-30-amd6411 x64
LinuxDebian12-6_1_0-30-amd64x64   - A Profile for Linux Debian12-6.1.0-30-amd64 x64
Linuxdebian10-4_19_0-23-686x86    - A Profile for Linux debian10-4.19.0-23-686 x86
LinuxAMD64PagedMemory          - Linux-specific AMD 64-bit address space.
linux_aslr_shift           - Automatically detect the Linux ASLR shift
linux_banner               - Prints the Linux banner information
linux_yarascan             - A shell in the Linux memory image
jenny@destforense:~/volatility2$
```

Instalación herramienta Volatility 3

Instale dependencias de python 3

$ sudo apt install -y python3-pip git

Clone el repositorio de volatility 3

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

$ cd volatility 3

```
jenny@destforense:~$ git clone https://github.com/volatilityfoundation/volatility3.git
Clonando en 'volatility3'...
remote: Enumerating objects: 42305, done.
remote: Counting objects: 100% (276/276), done.
remote: Compressing objects: 100% (133/133), done.
remote: Total 42305 (delta 215), reused 154 (delta 143), pack-reused 42029 (from 2)
Recibiendo objetos: 100% (42305/42305), 8.29 MiB | 5.37 MiB/s, listo.
Resolviendo deltas: 100% (32550/32550), listo.
jenny@destforense:~$ ls
module.dwarf  rV2  volatility2  volatility3
jenny@destforense:~$ cd volatility3
jenny@destforense:~/volatility3$ ls
API_CHANGES.md  doc          pyproject.toml  volatility3  volshell.spec
CITATION.cff    LICENSE.txt  README.md       vol.py       vol.spec
development     MANIFEST.in  test            volshell.py
```

Cree un entorno virtual para Volatility 3

$ python3 -m venv venv

$ source venv/bin/activate

```
jenny@destforense:~/volatility3$ python3 -m venv venv
jenny@destforense:~/volatility3$ source venv/bin/activate
```

Instale las dependencias que volatility 3 necesita

$ pip install capstone distorm3 yara-python

Pruebo que funcione volatility 3

$ python3 vol.py -h

```
(venv) jenny@destforense:~/volatility3$ pip install capstone distorm3 yara-python
Collecting capstone
  Downloading capstone-5.0.5-py3-none-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (1.5
MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1.5/1.5 MB 9.8 MB/s eta 0:00:00
Collecting distorm3
  Using cached distorm3-3.5.2.tar.gz (138 kB)
  Preparing metadata (setup.py) ... done
Collecting yara-python
  Downloading yara_python-4.5.1-cp311-cp311-manylinux_2_17_x86_64.manylinux2014_x86_64.whl
 (2.3 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 2.3/2.3 MB 19.8 MB/s eta 0:00:00
Installing collected packages: yara-python, distorm3, capstone
  DEPRECATION: distorm3 is being installed using the legacy 'setup.py install' method, bec
ause it does not have a 'pyproject.toml' and the 'wheel' package is not installed. pip 23.
1 will enforce this behaviour change. A possible replacement is to enable the '--use-pep51
7' option. Discussion can be found at https://github.com/pypa/pip/issues/8559
  Running setup.py install for distorm3 ... done
Successfully installed capstone-5.0.5 distorm3-3.5.2 yara-python-4.5.1
(venv) jenny@destforense:~/volatility3$ python3 vol.py -h
Volatility 3 Framework 2.20.0
usage: vol.py [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND]
              [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q]
              [-r RENDERER] [-f FILE] [--write-config] [--save-config SAVE_CONFIG]
              [--clear-cache] [--cache-path CACHE_PATH] [--offline | -u URL]
```

Creo un alias permanente para que pueda ejecutarlo en cualquier momento y cualquier parte sin necesidad de activar el entorno virtual de python 3

$ echo "alias vol3='~/volatility3/venv/bin/python3 ~/volatility3/vol.py'" >> ~/.bashrc

$ source ~/.bashrc

Pruebo que funcione volatility 3

vol3 -h

```
(venv) jenny@destforense:~/volatility3$ echo "alias vol3='~/volatility3/venv/bin/python3 ~
/volatility3/vol.py'" >> ~/.bashrc
(venv) jenny@destforense:~/volatility3$ source ~/.bashrc
jenny@destforense:~/volatility3$ vol3 -h
Volatility 3 Framework 2.20.0
usage: vol.py [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND]
              [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q]
              [-r RENDERER] [-f FILE] [--write-config] [--save-config SAVE_CONFIG]
              [--clear-cache] [--cache-path CACHE_PATH] [--offline | -u URL]
              [--filters FILTERS] [--hide-columns [HIDE_COLUMNS ...]]
              [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]]
              [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
              PLUGIN ...
```

Preparar Volatility 3 para trabajar con determinados perfiles Linux

● Descarga perfil de Volatility que se ajusta al volcado del punto y copialo en el directorio SYMBOLS de Volatility 3.

```
jenny@destforense:~$ ls -lh /home/jenny/volatility3/volatility3/symbols/
total 1,4M
-rw-r--r-- 1 jenny jenny 1,4M feb  6 12:36 debian10-4.19.0-23-686.json.xz
drwxr-xr-x 3 jenny jenny 4,0K feb  6 12:01 generic
-rw-r--r-- 1 jenny jenny  415 feb  6 12:01 __init__.py
drwxr-xr-x 2 jenny jenny 4,0K feb  6 12:07 __pycache__
jenny@destforense:~$
```

Realizar análisis básico de los volcados de memoria en Linux:

banners.Banners:

$ vol3 -f ram.lime -s /home/jenny/volatility3/volatility3/symbols banners.Banners > /home/jenny/rV3/banner.txt

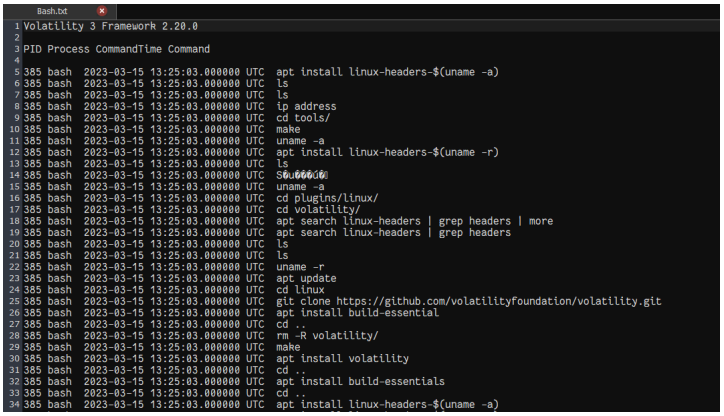
```
jenny@destforense:~/rV3$ cat banner.txt
Volatility 3 Framework 2.20.0

Offset  Banner

0x9687160       Linux version 4.19.0-23-686 (debian-kernel@lists.debian.org) (gcc version
8.3.0 (Debian 8.3.0-6)) #1 SMP Debian 4.19.269-1 (2022-12-20)
0x9a379e4       Linux version 4.19.0-23-686 (debian-kernel@lists.debian.org) (gcc version
8.3.0 (Debian 8.3.0-6)) #1 SMP Debian 4.19.269-1 (2022-12-20)
0x3788f624      Linux version 4.19.0-23-686 (debian-kernel@lists.debian.org) (gcc version
8.3.0 (Debian 8.3.0-6)) #1 SMP Debian 4.19.269-1 (2022-12-20)
0x3942e7df      Linux version 4.19.0-23-686 (debian-kernel@lists.debian.org) (gcc version
8.3.0 (Debian 8.3.0-6)) #1 SMP Debian 4.19.269-1 (2022-12-20)
0x3a300264      Linux version 4.19.0-23-686 (debian-kernel@lists.debian.org) (gcc version
8.3.0 (Debian 8.3.0-6)) #1 SMP Debian 4.19.269-1 (2022-12-20)
0x3b2037a8      Linux version 4.19.0-23-686 (debian-kernel@lists.debian.org) (gcc version
8.3.0 (Debian 8.3.0-6)) #1 SMP Debian 4.19.269-1 (2022-12-20)
0x3c275ea4      Linux version 4.19.0-23-686 (debian-kernel@lists.debian.org) (gcc version
8.3.0 (Debian 8.3.0-6)) #1 SMP Debian 4.19.269-1 (2022-12-20)
0x3d895ae4      Linux version 4.19.0-23-686 (debian-kernel@lists.debian.org) (gcc version
8.3.0 (Debian 8.3.0-6)) #1 SMP Debian 4.19.269-1 (2022-12-20)
0x3da173e8      Linux version 4.19.0-23-686 (debian-kernel@lists.debian.org) (gcc version
8.3.0 (Debian 8.3.0-6)) #1 SMP Debian 4.19.269-1 (2022-12-20)
jenny@destforense:~/rV3$
```

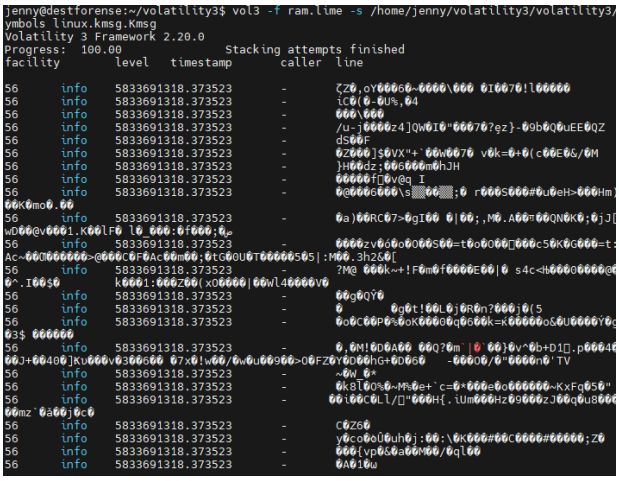
linux.bash.Bash:

$ vol3 -f ram.lime -s /home/jenny/volatility3/volatility3/symbols linux.bash.Bash > /home/jenny/rV3/Bash.txt



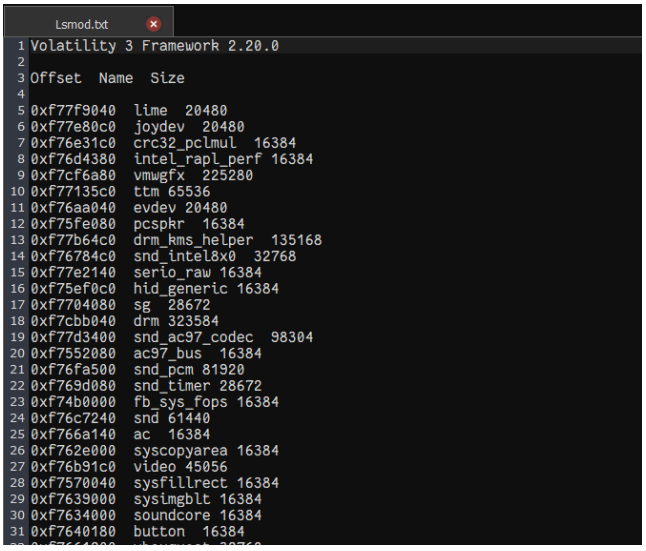
linux.kmsg.Kmsg:

$ vol3 -f ram.lime -s /home/jenny/volatility3/volatility3/symbols linux.kmsg.Kmsg



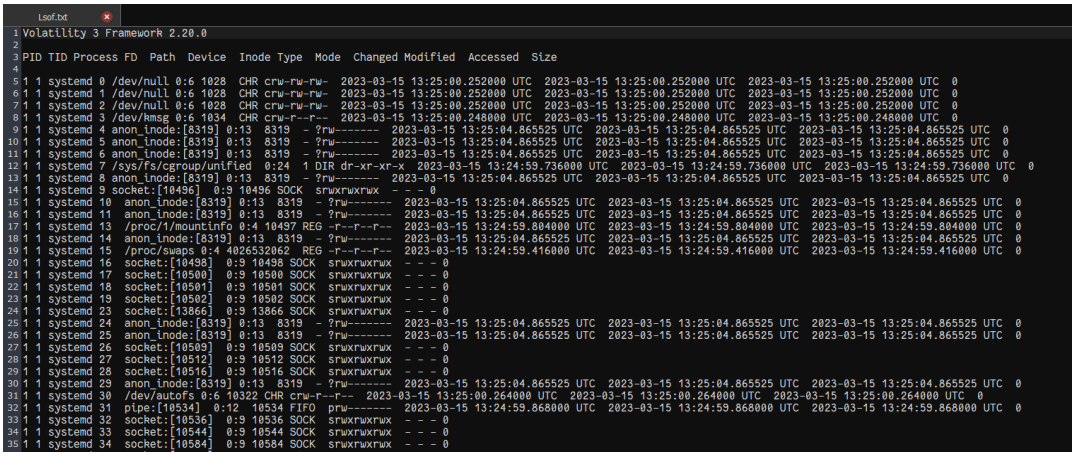
linux.lsmod.Lsmod:

$ vol3 -f ram.lime -s /home/jenny/volatility3/volatility3/symbols linux.lsmod.Lsmod > /home/jenny/rV3/Lsmod.txt



linux.lsof.Lsof:

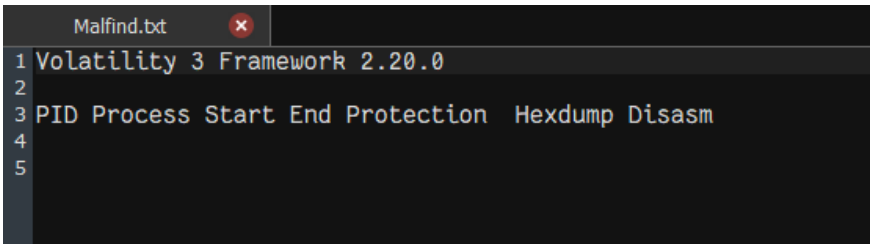
$ vol3 -f ram.lime -s /home/jenny/volatility3/volatility3/symbols linux.lsof.Lsof > /home/jenny/rV3/Lsof.txt



```
Lsof.txt
1 Volatility 3 Framework 2.20.0
2
3 PID TID Process FD  Path  Device  Inode Type  Mode  Changed Modified  Accessed  Size
4
5 1 1 systemd 0 /dev/null 0:6 1028  CHR crw-rw-rw-  2023-03-15 13:25:00.252000 UTC  2023-03-15 13:25:00.252000 UTC  2023-03-15 13:25:00.252000 UTC  0
6 1 1 systemd 1 /dev/null 0:6 1028  CHR crw-rw-rw-  2023-03-15 13:25:00.252000 UTC  2023-03-15 13:25:00.252000 UTC  2023-03-15 13:25:00.252000 UTC  0
7 1 1 systemd 2 /dev/null 0:6 1028  CHR crw-rw-rw-  2023-03-15 13:25:00.252000 UTC  2023-03-15 13:25:00.252000 UTC  2023-03-15 13:25:00.252000 UTC  0
8 1 1 systemd 3 /dev/kmsg 0:6 1034  CHR crw-r--r--  2023-03-15 13:25:00.248000 UTC  2023-03-15 13:25:00.248000 UTC  2023-03-15 13:25:00.248000 UTC  0
9 1 1 systemd 4 anon_inode:[8319] 0:13  8319  - ?rw-------  2023-03-15 13:25:04.865525 UTC  2023-03-15 13:25:04.865525 UTC  2023-03-15 13:25:04.865525 UTC  0
10 1 1 systemd 5 anon_inode:[8319] 0:13  8319  - ?rw-------  2023-03-15 13:25:04.865525 UTC  2023-03-15 13:25:04.865525 UTC  2023-03-15 13:25:04.865525 UTC  0
11 1 1 systemd 6 anon_inode:[8319] 0:13  8319  - ?rw-------  2023-03-15 13:25:04.865525 UTC  2023-03-15 13:25:04.865525 UTC  2023-03-15 13:25:04.865525 UTC  0
12 1 1 systemd 7 /sys/fs/cgroup/unified  0:24  1 DIR dr-xr-xr-x  2023-03-15 13:24:59.736000 UTC  2023-03-15 13:24:59.736000 UTC  2023-03-15 13:24:59.736000 UTC  0
13 1 1 systemd 8 anon_inode:[8319] 0:13  8319  - ?rw-------  2023-03-15 13:25:04.865525 UTC  2023-03-15 13:25:04.865525 UTC  2023-03-15 13:25:04.865525 UTC  0
14 1 1 systemd 9 socket:[10496]  0:9 10496 SOCK  srwxrwxrwx  - - - 0
15 1 1 systemd 10  anon_inode:[8319] 0:13  8319  - ?rw-------  2023-03-15 13:25:04.865525 UTC  2023-03-15 13:25:04.865525 UTC  2023-03-15 13:25:04.865525 UTC  0
16 1 1 systemd 11  anon_inode:[8319] 0:13  8319  - ?rw-------  2023-03-15 13:25:04.865525 UTC  2023-03-15 13:25:04.865525 UTC  2023-03-15 13:25:04.865525 UTC  0
17 1 1 systemd 13  /proc/1/mountinfo 0:4 10497 REG -r--r--r--  2023-03-15 13:24:59.804000 UTC  2023-03-15 13:24:59.804000 UTC  2023-03-15 13:24:59.804000 UTC  0
18 1 1 systemd 14  anon_inode:[8319] 0:13  8319  - ?rw-------  2023-03-15 13:25:04.865525 UTC  2023-03-15 13:25:04.865525 UTC  2023-03-15 13:25:04.865525 UTC  0
19 1 1 systemd 15  /proc/swaps 0:4 4026532062  REG -r--r--r--  2023-03-15 13:24:59.416000 UTC  2023-03-15 13:24:59.416000 UTC  2023-03-15 13:24:59.416000 UTC  0
20 1 1 systemd 16  socket:[10498]  0:9 10498 SOCK  srwxrwxrwx  - - - 0
21 1 1 systemd 17  socket:[10500]  0:9 10500 SOCK  srwxrwxrwx  - - - 0
22 1 1 systemd 18  socket:[10501]  0:9 10501 SOCK  srwxrwxrwx  - - - 0
23 1 1 systemd 19  socket:[10502]  0:9 10502 SOCK  srwxrwxrwx  - - - 0
24 1 1 systemd 23  socket:[13866]  0:9 13866 SOCK  srwxrwxrwx  - - - 0
25 1 1 systemd 24  anon_inode:[8319] 0:13  8319  - ?rw-------  2023-03-15 13:25:04.865525 UTC  2023-03-15 13:25:04.865525 UTC  2023-03-15 13:25:04.865525 UTC  0
26 1 1 systemd 25  anon_inode:[8319] 0:13  8319  - ?rw-------  2023-03-15 13:25:04.865525 UTC  2023-03-15 13:25:04.865525 UTC  2023-03-15 13:25:04.865525 UTC  0
27 1 1 systemd 26  socket:[10509]  0:9 10509 SOCK  srwxrwxrwx  - - - 0
28 1 1 systemd 27  socket:[10512]  0:9 10512 SOCK  srwxrwxrwx  - - - 0
29 1 1 systemd 28  socket:[10516]  0:9 10516 SOCK  srwxrwxrwx  - - - 0
30 1 1 systemd 29  anon_inode:[8319] 0:13  8319  - ?rw-------  2023-03-15 13:25:04.865525 UTC  2023-03-15 13:25:04.865525 UTC  2023-03-15 13:25:04.865525 UTC  0
31 1 1 systemd 30  /dev/autofs 0:6 10322 CHR crw-r--r--  2023-03-15 13:25:00.264000 UTC  2023-03-15 13:25:00.264000 UTC  2023-03-15 13:25:00.264000 UTC  0
32 1 1 systemd 31  pipe:[10534]  0:12  10534 FIFO  prw-------  2023-03-15 13:24:59.868000 UTC  2023-03-15 13:24:59.868000 UTC  2023-03-15 13:24:59.868000 UTC  0
33 1 1 systemd 32  socket:[10536]  0:9 10536 SOCK  srwxrwxrwx  - - - 0
34 1 1 systemd 33  socket:[10544]  0:9 10544 SOCK  srwxrwxrwx  - - - 0
35 1 1 systemd 34  socket:[10584]  0:9 10584 SOCK  srwxrwxrwx  - - - 0
```

linux.malfind.Malfind:

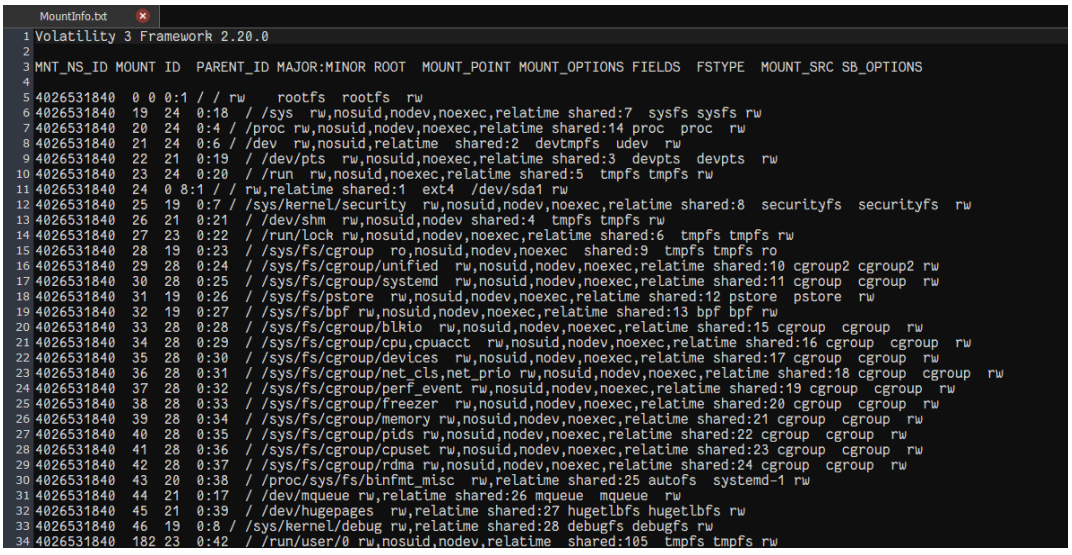
$ vol3 -f ram.lime -s /home/jenny/volatility3/volatility3/symbols linux.malfind.Malfind > /home/jenny/rV3/Malfind.txt



```
Malfind.txt
1 Volatility 3 Framework 2.20.0
2
3 PID Process Start End Protection  Hexdump Disasm
4
5
```

linux.mountinfo.MountInfo:

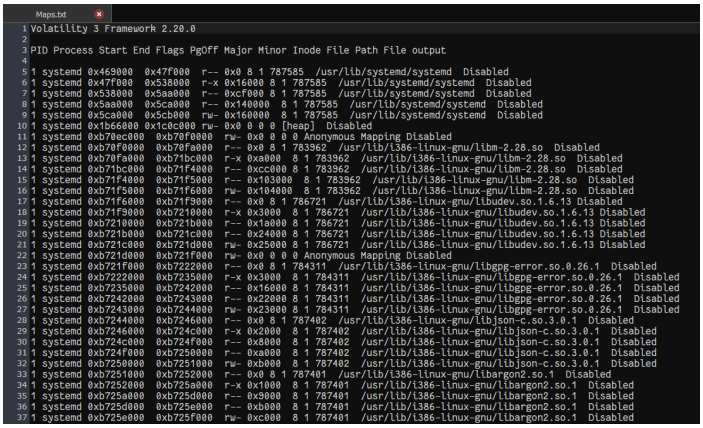
$ vol3 -f ram.lime -s /home/jenny/volatility3/volatility3/symbols linux.mountinfo.MountInfo > /home/jenny/rV3/MountInfo.txt



```
MountInfo.txt
1 Volatility 3 Framework 2.20.0
2
3 MNT_NS_ID MOUNT ID  PARENT_ID MAJOR:MINOR ROOT  MOUNT_POINT MOUNT_OPTIONS FIELDS  FSTYPE  MOUNT_SRC SB_OPTIONS
4
5 4026531840  0 0 0:1 / / rw    rootfs  rootfs  rw
6 4026531840  19  24  0:18  / /sys  rw,nosuid,nodev,noexec,relatime shared:7  sysfs sysfs rw
7 4026531840  20  24  0:4 / /proc rw,nosuid,nodev,noexec,relatime shared:14 proc  proc  rw
8 4026531840  21  24  0:6 / /dev  rw,nosuid,relatime  shared:2  devtmpfs  udev  rw
9 4026531840  22  21  0:19  / /dev/pts  rw,nosuid,noexec,relatime shared:3  devpts  devpts  rw
10 4026531840  23  24  0:20  / /run  rw,nosuid,noexec,relatime shared:5  tmpfs tmpfs rw
11 4026531840  24  0 8:1 / / rw,relatime shared:1  ext4  /dev/sda1 rw
12 4026531840  25  19  0:7 / /sys/kernel/security  rw,nosuid,nodev,noexec,relatime shared:8  securityfs  securityfs  rw
13 4026531840  26  21  0:21  / /dev/shm  rw,nosuid,nodev shared:4  tmpfs tmpfs rw
14 4026531840  27  23  0:22  / /run/lock rw,nosuid,nodev,noexec,relatime shared:6  tmpfs tmpfs rw
15 4026531840  28  19  0:23  / /sys/fs/cgroup  ro,nosuid,nodev,noexec  shared:9  tmpfs tmpfs ro
16 4026531840  29  28  0:24  / /sys/fs/cgroup/unified  rw,nosuid,nodev,noexec,relatime shared:10 cgroup2 cgroup2 rw
17 4026531840  30  28  0:25  / /sys/fs/cgroup/systemd  rw,nosuid,nodev,noexec,relatime shared:11 cgroup  cgroup  rw
18 4026531840  31  19  0:26  / /sys/fs/pstore  rw,nosuid,nodev,noexec,relatime shared:12 pstore  pstore  rw
19 4026531840  32  19  0:27  / /sys/fs/bpf rw,nosuid,nodev,noexec,relatime shared:13 bpf bpf rw
20 4026531840  33  28  0:28  / /sys/fs/cgroup/blkio  rw,nosuid,nodev,noexec,relatime shared:15 cgroup  cgroup  rw
21 4026531840  34  28  0:29  / /sys/fs/cgroup/cpu,cpuacct  rw,nosuid,nodev,noexec,relatime shared:16 cgroup  cgroup  rw
22 4026531840  35  28  0:30  / /sys/fs/cgroup/devices  rw,nosuid,nodev,noexec,relatime shared:17 cgroup  cgroup  rw
23 4026531840  36  28  0:31  / /sys/fs/cgroup/net_cls,net_prio rw,nosuid,nodev,noexec,relatime shared:18 cgroup  cgroup  rw
24 4026531840  37  28  0:32  / /sys/fs/cgroup/perf_event rw,nosuid,nodev,noexec,relatime shared:19 cgroup  cgroup  rw
25 4026531840  38  28  0:33  / /sys/fs/cgroup/freezer  rw,nosuid,nodev,noexec,relatime shared:20 cgroup  cgroup  rw
26 4026531840  39  28  0:34  / /sys/fs/cgroup/memory rw,nosuid,nodev,noexec,relatime shared:21 cgroup  cgroup  rw
27 4026531840  40  28  0:35  / /sys/fs/cgroup/pids rw,nosuid,nodev,noexec,relatime shared:22 cgroup  cgroup  rw
28 4026531840  41  28  0:36  / /sys/fs/cgroup/cpuset rw,nosuid,nodev,noexec,relatime shared:23 cgroup  cgroup  rw
29 4026531840  42  28  0:37  / /sys/fs/cgroup/rdma rw,nosuid,nodev,noexec,relatime shared:24 cgroup  cgroup  rw
30 4026531840  43  20  0:38  / /proc/sys/fs/binfmt_misc  rw,relatime shared:25 autofs  systemd-1 rw
31 4026531840  44  21  0:17  / /dev/mqueue rw,relatime shared:26 mqueue  mqueue  rw
32 4026531840  45  21  0:39  / /dev/hugepages  rw,relatime shared:27 hugetlbfs hugetlbfs rw
33 4026531840  46  19  0:8 / /sys/kernel/debug rw,relatime shared:28 debugfs debugfs rw
34 4026531840  182 23  0:42  / /run/user/0 rw,nosuid,nodev,relatime  shared:105  tmpfs tmpfs rw
```

linux.proc.Maps:

$ vol3 -f ram.lime -s /home/jenny/volatility3/volatility3/symbols linux.proc.Maps> /home/jenny/rV3/Maps.txt



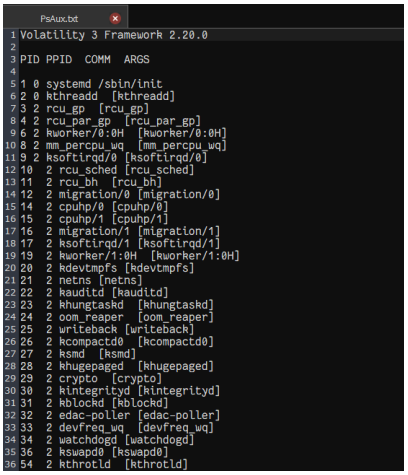
```
Maps.txt
Volatility 3 Framework 2.20.0

PID Process Start End Flags PgOff Major Minor Inode File Path File output

1 systemd 0x469000  0x47f000  r-- 0x0 8 1 787585  /usr/lib/systemd/systemd  Disabled
1 systemd 0x47f000  0x538000  r-x 0x16000 8 1 787585  /usr/lib/systemd/systemd  Disabled
1 systemd 0x538000  0x5aa000  r-- 0xcf000 8 1 787585  /usr/lib/systemd/systemd  Disabled
1 systemd 0x5aa000  0x5ca000  r-- 0x140000  8 1 787585  /usr/lib/systemd/systemd  Disabled
1 systemd 0x5ca000  0x5cb000  rw- 0x160000  8 1 787585  /usr/lib/systemd/systemd  Disabled
1 systemd 0x1b66000 0x1c0c000 rw- 0x0 0 0 0 [heap]  Disabled
1 systemd 0xb70ec000  0xb70f0000  rw- 0x0 0 0 0 Anonymous Mapping Disabled
1 systemd 0xb70f0000  0xb70fa000  r-- 0x0 8 1 783962  /usr/lib/i386-linux-gnu/libm-2.28.so  Disabled
1 systemd 0xb70fa000  0xb71bc000  r-x 0xa000  8 1 783962  /usr/lib/i386-linux-gnu/libm-2.28.so  Disabled
1 systemd 0xb71bc000  0xb71f4000  r-- 0xcc000 8 1 783962  /usr/lib/i386-linux-gnu/libm-2.28.so  Disabled
1 systemd 0xb71f4000  0xb71f5000  r-- 0x103000  8 1 783962  /usr/lib/i386-linux-gnu/libm-2.28.so  Disabled
1 systemd 0xb71f5000  0xb71f6000  rw- 0x104000  8 1 783962  /usr/lib/i386-linux-gnu/libm-2.28.so  Disabled
1 systemd 0xb71f6000  0xb71f3000  r-- 0x0 8 1 786721  /usr/lib/i386-linux-gnu/libudev.so.1.6.13 Disabled
1 systemd 0xb71f3000  0xb7210000  r-x 0x3000  8 1 786721  /usr/lib/i386-linux-gnu/libudev.so.1.6.13 Disabled
1 systemd 0xb7210000  0xb721b000  r-- 0x1a000 8 1 786721  /usr/lib/i386-linux-gnu/libudev.so.1.6.13 Disabled
1 systemd 0xb721b000  0xb721c000  r-- 0x24000 8 1 786721  /usr/lib/i386-linux-gnu/libudev.so.1.6.13 Disabled
1 systemd 0xb721c000  0xb721d000  rw- 0x25000 8 1 786721  /usr/lib/i386-linux-gnu/libudev.so.1.6.13 Disabled
1 systemd 0xb721d000  0xb721f000  rw- 0x0 0 0 0 Anonymous Mapping Disabled
1 systemd 0xb721f000  0xb7222000  r-- 0x0 8 1 784311  /usr/lib/i386-linux-gnu/libgpg-error.so.0.26.1  Disabled
1 systemd 0xb7222000  0xb7235000  r-x 0x3000  8 1 784311  /usr/lib/i386-linux-gnu/libgpg-error.so.0.26.1  Disabled
1 systemd 0xb7235000  0xb7242000  r-- 0x16000 8 1 784311  /usr/lib/i386-linux-gnu/libgpg-error.so.0.26.1  Disabled
1 systemd 0xb7242000  0xb7243000  r-- 0x22000 8 1 784311  /usr/lib/i386-linux-gnu/libgpg-error.so.0.26.1  Disabled
1 systemd 0xb7243000  0xb7244000  rw- 0x23000 8 1 784311  /usr/lib/i386-linux-gnu/libgpg-error.so.0.26.1  Disabled
1 systemd 0xb7244000  0xb7246000  r-- 0x0 8 1 787402  /usr/lib/i386-linux-gnu/libjson-c.so.3.0.1  Disabled
1 systemd 0xb7246000  0xb724c000  r-x 0x2000  8 1 787402  /usr/lib/i386-linux-gnu/libjson-c.so.3.0.1  Disabled
1 systemd 0xb724c000  0xb724f000  r-- 0x8000  8 1 787402  /usr/lib/i386-linux-gnu/libjson-c.so.3.0.1  Disabled
1 systemd 0xb724f000  0xb7250000  r-- 0xa000  8 1 787402  /usr/lib/i386-linux-gnu/libjson-c.so.3.0.1  Disabled
1 systemd 0xb7250000  0xb7251000  rw- 0xb000  8 1 787402  /usr/lib/i386-linux-gnu/libjson-c.so.3.0.1  Disabled
1 systemd 0xb7251000  0xb7252000  r-- 0x0 8 1 787401  /usr/lib/i386-linux-gnu/libargon2.so.1  Disabled
1 systemd 0xb7252000  0xb725a000  r-x 0x1000  8 1 787401  /usr/lib/i386-linux-gnu/libargon2.so.1  Disabled
1 systemd 0xb725a000  0xb725d000  r-- 0x9000  8 1 787401  /usr/lib/i386-linux-gnu/libargon2.so.1  Disabled
1 systemd 0xb725d000  0xb725e000  r-- 0xb000  8 1 787401  /usr/lib/i386-linux-gnu/libargon2.so.1  Disabled
1 systemd 0xb725e000  0xb725f000  rw- 0xc000  8 1 787401  /usr/lib/i386-linux-gnu/libargon2.so.1  Disabled
```

linux.psaux.PsAux:

$ vol3 -f ram.lime -s /home/jenny/volatility3/volatility3/symbols linux.psaux.PsAux> /home/jenny/rV3/PsAux.txt



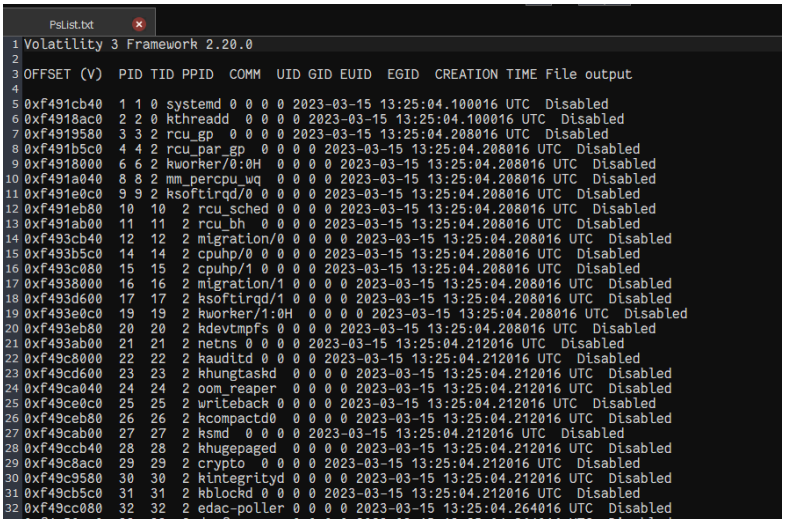
```
PsAux.txt
Volatility 3 Framework 2.20.0

PID PPID  COMM  ARGS

1 0 systemd /sbin/init
2 0 kthreadd  [kthreadd]
3 2 rcu_gp  [rcu_gp]
4 2 rcu_par_gp  [rcu_par_gp]
6 2 kworker/0:0H  [kworker/0:0H]
8 2 mm_percpu_wq  [mm_percpu_wq]
9 2 ksoftirqd/0 [ksoftirqd/0]
10  2 rcu_sched [rcu_sched]
11  2 rcu_bh  [rcu_bh]
12  2 migration/0 [migration/0]
14  2 cpuhp/0 [cpuhp/0]
15  2 cpuhp/1 [cpuhp/1]
16  2 migration/1 [migration/1]
17  2 ksoftirqd/1 [ksoftirqd/1]
19  2 kworker/1:0H  [kworker/1:0H]
20  2 kdevtmpfs [kdevtmpfs]
21  2 netns [netns]
22  2 kauditd [kauditd]
23  2 khungtaskd  [khungtaskd]
24  2 oom_reaper  [oom_reaper]
25  2 writeback [writeback]
26  2 kcompactd0  [kcompactd0]
27  2 ksmd  [ksmd]
28  2 khugepaged  [khugepaged]
29  2 crypto  [crypto]
30  2 kintegrityd [kintegrityd]
31  2 kblockd [kblockd]
32  2 edac-poller [edac-poller]
33  2 devfreq_wq  [devfreq_wq]
34  2 watchdogd [watchdogd]
36  2 kswapd0 [kswapd0]
54  2 kthrotld  [kthrotld]
```

linux.pslist.PsList:

$ vol3 -f ram.lime -s /home/jenny/volatility3/volatility3/symbols linux.pslist.PsList> /home/jenny/rV3/PsList.txt



PsList.txt

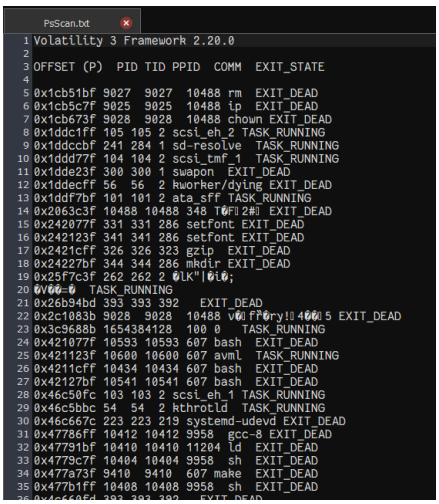
```
Volatility 3 Framework 2.20.0

OFFSET (V)  PID TID PPID  COMM  UID GID EUID  EGID  CREATION TIME File output

0xf491cb40  1 1 0 systemd 0 0 0 0 2023-03-15 13:25:04.100016 UTC  Disabled
0xf4918ac0  2 2 0 kthreadd  0 0 0 0 2023-03-15 13:25:04.100016 UTC  Disabled
0xf4919580  3 3 2 rcu_gp  0 0 0 0 2023-03-15 13:25:04.208016 UTC  Disabled
0xf491b5c0  4 4 2 rcu_par_gp  0 0 0 0 2023-03-15 13:25:04.208016 UTC  Disabled
0xf4918000  6 6 2 kworker/0:0H  0 0 0 0 2023-03-15 13:25:04.208016 UTC  Disabled
0xf491a040  8 8 2 mm_percpu_wq  0 0 0 0 2023-03-15 13:25:04.208016 UTC  Disabled
0xf491e0c0  9 9 2 ksoftirqd/0 0 0 0 0 2023-03-15 13:25:04.208016 UTC  Disabled
0xf491eb80  10  10  2 rcu_sched 0 0 0 0 2023-03-15 13:25:04.208016 UTC  Disabled
0xf491ab00  11  11  2 rcu_bh  0 0 0 0 2023-03-15 13:25:04.208016 UTC  Disabled
0xf493cb40  12  12  2 migration/0 0 0 0 0 2023-03-15 13:25:04.208016 UTC  Disabled
0xf493b5c0  14  14  2 cpuhp/0 0 0 0 0 2023-03-15 13:25:04.208016 UTC  Disabled
0xf493c080  15  15  2 cpuhp/1 0 0 0 0 2023-03-15 13:25:04.208016 UTC  Disabled
0xf4938000  16  16  2 migration/1 0 0 0 0 2023-03-15 13:25:04.208016 UTC  Disabled
0xf493d600  17  17  2 ksoftirqd/1 0 0 0 0 2023-03-15 13:25:04.208016 UTC  Disabled
0xf493e0c0  19  19  2 kworker/1:0H  0 0 0 0 2023-03-15 13:25:04.208016 UTC  Disabled
0xf493eb80  20  20  2 kdevtmpfs 0 0 0 0 2023-03-15 13:25:04.208016 UTC  Disabled
0xf493ab00  21  21  2 netns 0 0 0 0 2023-03-15 13:25:04.212016 UTC  Disabled
0xf49c8000  22  22  2 kauditd 0 0 0 0 2023-03-15 13:25:04.212016 UTC  Disabled
0xf49cd600  23  23  2 khungtaskd  0 0 0 0 2023-03-15 13:25:04.212016 UTC  Disabled
0xf49ca040  24  24  2 oom_reaper  0 0 0 0 2023-03-15 13:25:04.212016 UTC  Disabled
0xf49ce0c0  25  25  2 writeback 0 0 0 0 2023-03-15 13:25:04.212016 UTC  Disabled
0xf49ceb80  26  26  2 kcompactd0  0 0 0 0 2023-03-15 13:25:04.212016 UTC  Disabled
0xf49cab00  27  27  2 ksmd  0 0 0 0 2023-03-15 13:25:04.212016 UTC  Disabled
0xf49ccb40  28  28  2 khugepaged  0 0 0 0 2023-03-15 13:25:04.212016 UTC  Disabled
0xf49c8ac0  29  29  2 crypto  0 0 0 0 2023-03-15 13:25:04.212016 UTC  Disabled
0xf49c9580  30  30  2 kintegrityd 0 0 0 0 2023-03-15 13:25:04.212016 UTC  Disabled
0xf49cb5c0  31  31  2 kblockd 0 0 0 0 2023-03-15 13:25:04.212016 UTC  Disabled
0xf49cc080  32  32  2 edac-poller 0 0 0 0 2023-03-15 13:25:04.264016 UTC  Disabled
```

linux.psscan.PsScan:

$ vol3 -f ram.lime -s /home/jenny/volatility3/volatility3/symbols linux.psscan.PsScan > /home/jenny/rV3/PsScan.txt



PsScan.txt

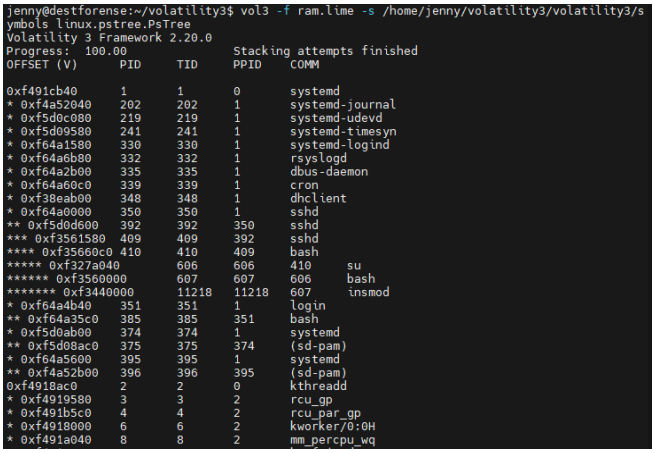
```
Volatility 3 Framework 2.20.0

OFFSET (P)  PID TID PPID  COMM  EXIT_STATE

0x1cb51bf 9027  9027  10488 rm  EXIT_DEAD
0x1cb5c7f 9025  9025  10488 ip  EXIT_DEAD
0x1cb673f 9028  9028  10488 chown EXIT_DEAD
0x1ddc1ff 105 105 2 scsi_eh_2 TASK_RUNNING
0x1ddccbf 241 284 1 sd-resolve  TASK_RUNNING
0x1ddd77f 104 104 2 scsi_tmf_1  TASK_RUNNING
0x1dde23f 300 300 1 swapon  EXIT_DEAD
0x1ddecff 56  56  2 kworker/dying EXIT_DEAD
0x1ddf7bf 101 101 2 ata_sff TASK_RUNNING
0x2063c3f 10488 10488 348 T@F2# EXIT_DEAD
0x242077f 331 331 286 setfont EXIT_DEAD
0x242123f 341 341 286 setfont EXIT_DEAD
0x2421cff 326 326 323 gzip  EXIT_DEAD
0x24227bf 344 344 286 mkdir EXIT_DEAD
0x25f7c3f 262 262 2 @LK"|@i@;
0V@@=@  TASK_RUNNING
0x26b94bd 393 393 392   EXIT_DEAD
0x2c1083b 9028  9028  10488 v@f?@ry!@4@@5 EXIT_DEAD
0x3c9688b 1654384128  100 0   TASK_RUNNING
0x421077f 10593 10593 607 bash  EXIT_DEAD
0x421123f 10600 10600 607 avml  TASK_RUNNING
0x4211cff 10434 10434 607 bash  EXIT_DEAD
0x42127bf 10541 10541 607 bash  EXIT_DEAD
0x46c50fc 103 103 2 scsi_eh_1 TASK_RUNNING
0x46c5bbc 54  54  2 kthrotld  TASK_RUNNING
0x46c667c 223 223 219 systemd-udevd EXIT_DEAD
0x47786ff 10412 10412 9958  gcc-8 EXIT_DEAD
0x47791bf 10410 10410 11204 ld  EXIT_DEAD
0x4779c7f 10404 10404 9958  sh  EXIT_DEAD
0x477a73f 9410  9410  607 make  EXIT_DEAD
0x477b1ff 10408 10408 9958  sh  EXIT_DEAD
```

linux.pstree.PsTree:

$ vol3 -f ram.lime -s /home/jenny/volatility3/volatility3/symbols linux.pstree.PsTree > /home/jenny/rV3/PsTree.txt

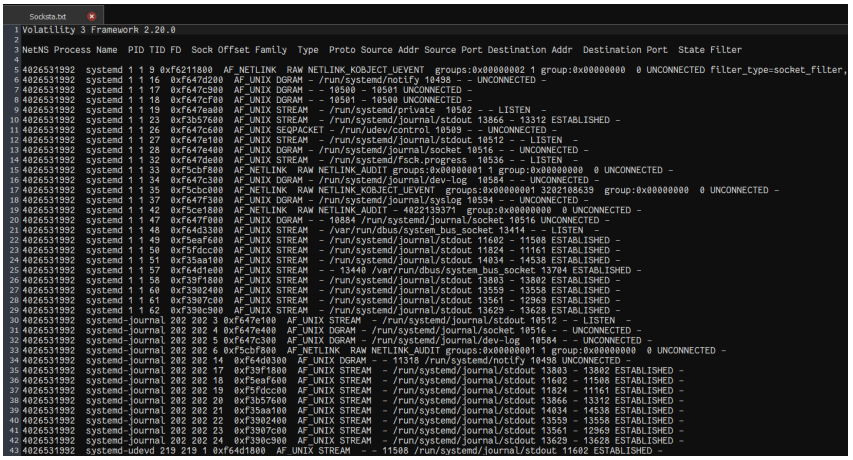


```
jenny@destforense:~/volatility3$ vol3 -f ram.lime -s /home/jenny/volatility3/volatility3/s
ymbols linux.pstree.PsTree
Volatility 3 Framework 2.20.0
Progress:  100.00               Stacking attempts finished
OFFSET (V)      PID     TID     PPID    COMM

0xf491cb40      1       1       0       systemd
* 0xf4a52040    202     202     1       systemd-journal
* 0xf5d0c080    219     219     1       systemd-udevd
* 0xf5d09580    241     241     1       systemd-timesyn
* 0xf64a1580    330     330     1       systemd-logind
* 0xf64a6b80    332     332     1       rsyslogd
* 0xf64a2b00    335     335     1       dbus-daemon
* 0xf64a60c0    339     339     1       cron
* 0xf38eab00    348     348     1       dhclient
* 0xf64a0000    350     350     1       sshd
** 0xf5d0d600   392     392     350     sshd
*** 0xf3561580  409     409     392     sshd
**** 0xf35660c0 410     410     409     bash
***** 0xf327a040        606     606     410     su
****** 0xf3560000       607     607     606     bash
******* 0xf3440000      11218   11218   607     insmod
* 0xf64a4b40    351     351     1       login
** 0xf64a35c0   385     385     351     bash
* 0xf5d0ab00    374     374     1       systemd
** 0xf5d08ac0   375     375     374     (sd-pam)
* 0xf64a5600    395     395     1       systemd
** 0xf4a52b00   396     396     395     (sd-pam)
0xf4918ac0      2       2       0       kthreadd
* 0xf4919580    3       3       2       rcu_gp
* 0xf491b5c0    4       4       2       rcu_par_gp
* 0xf4918000    6       6       2       kworker/0:0H
* 0xf491a040    8       8       2       mm_percpu_wq
```

linux.sockstat.Sockstat:

$ vol3 -f ram.lime -s /home/jenny/volatility3/volatility3/symbols linux.sockstat.Socksta > /home/jenny/rV3/Socksta.txt



Generar perfiles específicos para Volatility.

Primero veré la versión que tengo del kernel

$ uname -r

Luego instalo y extraigo el archivo vmlinux que lo hicimos en el ejercicio de volatility 2 y busco que el archivo para conocer la ruta

$ sudo apt install linux-image-$(uname -r)-dbg

$ find /usr/lib/debug/ -name "vmlinux"

```
jenny@destforense:~/volatility3$ uname -r
6.1.0-30-amd64
jenny@destforense:~/volatility3$ find /usr/lib/debug/ -name "vmlinux"
/usr/lib/debug/lib/modules/6.1.0-30-amd64/vmlinux
jenny@destforense:~/volatility3$
```

Obtengo la ruta del archivo System.map

$ find /boot -name "System.map-*"

```
jenny@destforense:~/volatility3$ find /boot -name "System.map-*"
/boot/System.map-6.1.0-30-amd64
jenny@destforense:~/volatility3$
```

Instale dwarf2json es una herramienta que extrae información de depuración del kernel para Volatility.

$ git clone https://github.com/volatilityfoundation/dwarf2json.git

Instale golang es un compilador

$ sudo apt install golang-go

```
jenny@destforense:~$ git clone https://github.com/volatilityfoundation/dwarf2json.git
Clonando en 'dwarf2json'...
remote: Enumerating objects: 165, done.
remote: Counting objects: 100% (94/94), done.
remote: Compressing objects: 100% (46/46), done.
remote: Total 165 (delta 47), reused 69 (delta 38), pack-reused 71 (from 1)
Recibiendo objetos: 100% (165/165), 65.12 KiB | 1.12 MiB/s, listo.
Resolviendo deltas: 100% (66/66), listo.
jenny@destforense:~$ sudo apt install golang-go
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  golang-1.19-go golang-1.19-src golang-src
```

Entre en la carpeta dwarf2json y lo ejecute

$ cd dwarf2json

$ go build .

```
jenny@destforense:~/dwarf2json$ go build .
go: downloading github.com/spf13/pflag v1.0.5
jenny@destforense:~/dwarf2json$
```

Genere el JSON del kermel y reviso que se creó correctamente

$ ./dwarf2json linux --elf /usr/lib/debug/lib/modules/6.1.0-30-amd64/vmlinux > debian12-kernel.json

$ ls -lh debian12-kernel.json

```
jenny@destforense:~/dwarf2json$ ls
dwarf2json  go.mod  go.sum  LICENSE.txt  main.go  README.md
jenny@destforense:~/dwarf2json$ ./dwarf2json linux --elf /usr/lib/debug/lib/modules/6.1.0-30-amd64/vmlinux > debian12-kernel.json
jenny@destforense:~/dwarf2json$ ls -lh debian12-kernel.json
-rw-r--r-- 1 jenny jenny 37M feb  6 13:48 debian12-kernel.json
jenny@destforense:~/dwarf2json$
```

Creamos el mapa de memoria del kernel y reviso que se creó correctamente

$ ./dwarf2json linux --elf /usr/lib/debug/lib/modules/6.1.0-30-amd64/vmlinux --system-map /boot/System.map-6.1.0-30-amd64 > linux-image-6.1.0-30-amd64-memmap.json.xz

$ ls -lh linux-image-6.1.0-30-amd64-memmap.json.xz

```
jenny@destforense:~/dwarf2json$ ./dwarf2json linux --elf /usr/lib/debug/lib/modules/6.1.0-30-amd64/vmlinux --system-map /boot/System.map-6.1.0-30-amd64 > linux-image-6.1.0-30-amd64-memmap.json.xz
jenny@destforense:~/dwarf2json$ ls -lh debian12-kernel.json
-rw-r--r-- 1 jenny jenny 37M feb  6 13:48 debian12-kernel.json
jenny@destforense:~/dwarf2json$ ls -lh linux-image-6.1.0-30-amd64-memmap.json.xz
-rw-r--r-- 1 jenny jenny 37M feb  6 13:55 linux-image-6.1.0-30-amd64-memmap.json.xz
jenny@destforense:~/dwarf2json$
```

Muvi el archivo en la carpeta correspondiente

$ sudo mv linux-image-6.1.0-30-amd64-memmap.json.xz ~/volatility3/volatility3/symbols/

Verifique que esta en la carpeta correspondiente

$ ls -lh ~/volatility3/volatility3/symbols/

```
jenny@destforense:~$ ls -lh ~/volatility3/volatility3/symbols/
total 38M
-rw-r--r-- 1 jenny jenny 1,4M feb  6 12:36 debian10-4.19.0-23-686.json.xz
drwxr-xr-x 3 jenny jenny 4,0K feb  6 12:01 generic
-rw-r--r-- 1 jenny jenny  415 feb  6 12:01 __init__.py
-rw-r--r-- 1 jenny jenny  37M feb  6 13:55 linux-image-6.1.0-30-amd64-memmap.json.xz
drwxr-xr-x 2 jenny jenny 4,0K feb  6 12:07 __pycache__
jenny@destforense:~$
```

Comprobación del perfil

$ vol3 -f debian12.dd -s /home/jenny/volatility3/volatility3/symbols/ banners.Banners