

# Creating Linux Profiles, Capturing Linux memory dump and running plugins using Volatility – 3

## Memory Forensics

Volatility, a forensic analysis tool, manages symbol tables in various formats. It can process files in pure JSON (.json), or compressed formats like .json.gz or .json.xz, automatically decompressing them when needed. These files, once used, are cached in a compressed format in the .cache/volatility3 directory within the user's home folder. This directory, which also stores other essential data, currently cannot be changed. By default, symbol table JSON files for Volatility are stored in the volatility3/symbols directory [1]

For Linux and Mac systems, symbol tables are created from DWARF files using the dwarf2json tool. The most comprehensive source for this data is a kernel equipped with debugging symbols, necessary for most Volatility plugins to retrieve all required information [1]

Volatility processes and analyzes the kernel's symbol table, storing this data in a specialized format called the Intermediate Symbol Format (ISF). This means that for analyzing a Linux memory dump, an ISF file is used instead of the traditional profile format [1]

```
rusheel@ubuntu:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:   Ubuntu 20.04.6 LTS
Release:      20.04
Codename:     focal
rusheel@ubuntu:~$ uname -a
Linux ubuntu 5.15.0-88-generic #98~20.04.1-Ubuntu SMP Mon Oct 9 16:43:45 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
rusheel@ubuntu:~$ uname -r
5.15.0-88-generic
```

So, we have got the OS and Kernel version:

- OS: *Ubuntu 22.04.6 LTS [focal]*
- Kernel: *Linux version 5.15.0-88-generic.*

### **Creating ISF (Intermediate Symbol Format):**

At this stage, the required needs are the **Linux kernel** and [dwarf2json](#) debug symbols.

### **Installing GO:**

```
# https://github.com/canha/golang-tools-install-script
```

```
$ wget -q -O - https://git.io/vQhTU | bash
```

```
$ source ~/.bashrc
```

```
$ go version
```

### **Installing dwarf2json:**

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

```
$ cd dwarf2json/
```

```
$ go build
```

### **Build a Linux Kernel DWARF File(vmlinux) and system.map[1]:**

```
$ echo "deb http://ddebs.ubuntu.com $(lsb_release -cs) main restricted
universe multiverse
deb http://ddebs.ubuntu.com $(lsb_release -cs)-updates main restricted
universe multiverse
deb http://ddebs.ubuntu.com $(lsb_release -cs)-proposed main restricted
universe multiverse" | \
sudo tee -a /etc/apt/sources.list.d/ddebs.list
```

```
$ sudo apt install ubuntu-dbgsym-keyring
```

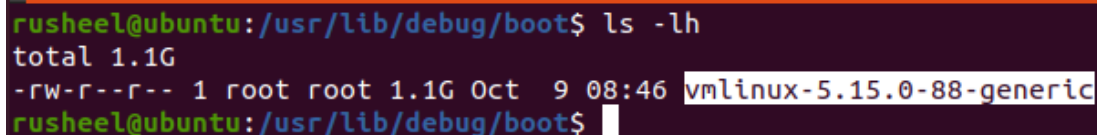
```
$ sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys
F2EDC64DC5AEE1F6B9C621F0C8CAB6595FDFF622
```

```
$ sudo apt-get update
```

```
$ sudo apt install linux-image-5.15.0-88-generic-dbgsym
```

```
$ cd /usr/lib/debug/boot
```

```
$ ls -lh
```

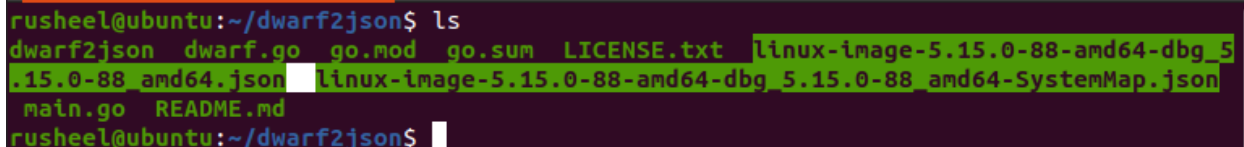


```
rusheel@ubuntu:/usr/lib/debug/boot$ ls -lh
total 1.1G
-rw-r--r-- 1 root root 1.1G Oct  9 08:46 vmlinux-5.15.0-88-generic
rusheel@ubuntu:/usr/lib/debug/boot$
```

Traverse to dwarf2json folder:

```
$ ./dwarf2json linux --elf /usr/lib/debug/boot/vmlinux-5.15.0-88-generic >
linux-image-5.15.0-88-amd64-dbg_5.15.0-88_amd64.json
```

```
$ ./dwarf2json linux --elf /usr/lib/debug/boot/vmlinux-5.15.0-79-generic --
system-map /boot/System.map-5.15.0-88-generic > linux-image-5.15.0-79-amd64-
dbg_5.15.0-79_amd64-SystemMap.json
```



```
rusheel@ubuntu:~/dwarf2json$ ls
dwarf2json  dwarf.go  go.mod  go.sum  LICENSE.txt  linux-image-5.15.0-88-amd64-dbg_5
.15.0-88_amd64.json  linux-image-5.15.0-88-amd64-dbg_5.15.0-88_amd64-SystemMap.json
main.go  README.md
rusheel@ubuntu:~/dwarf2json$
```

Copy the DWARF file and System Map files to the volatility3/symbols folder.

```
$ sudo cp -r linux-image-5.15.0-88-amd64-dbg_5.15.0-88_amd64*  
~/volatility3/volatility3/symbols/
```

```
rusheel@ubuntu:~$ cd volatility3/volatility3/symbols/  
rusheel@ubuntu:~/volatility3/volatility3/symbols$ ls  
__init__.py  
linux  
linux-image-5.15.0-88-amd64-dbg_5.15.0-88_amd64.json  
linux-image-5.15.0-88-amd64-dbg_5.15.0-88_amd64-SystemMap.json  
__pycache__
```

### Capturing the Linux memory dump:

Linux Memory Extractor (LiME) is a popular tool for acquiring memory on a Linux system [2]

```
$ sudo git clone https://github.com/504ensicsLabs/LiME.git
```

```
$ cd LiME/src/
```

```
$ ls
```

```
deflate.c  disk.c  hash.c  lime.h  main.c  Makefile  Makefile.sample  tcp.c
```

```
$ sudo make
```

This will compile and create an executable called “lime-5.15.0-88-generic.ko”

```
$ sudo insmod ./lime-5.15.0-88-generic.ko "path=/home/rusheel/ubuntu.lime  
format=lime"
```

Successful execution of this command will result in Linux memory dump acquisition.

```
rusheel@ubuntu:~/LiME/src$ ls  
deflate.c  disk.c  hash.c  lime-5.15.0-88-generic.ko  lime.mod  lime.mod.o  main.c  Makefile  modules.order  tcp.c  ubuntu.lime  
deflate.o  disk.o  hash.o  lime.h  lime.mod.c  lime.o  main.o  Makefile.sample  Module.symvers  tcp.o  
rusheel@ubuntu:~/LiME/src$
```

## Executing volatility 3 plugins on the acquired memory dump:

Plugin: **banners.Banners** : Attempts to identify potential linux banners in an image [3]

```
$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime banners.Banners
```

```
rusheel@ubuntu:~/volatility3$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime banners.Banners
[sudo] password for rusheel:
Volatility 3 Framework 2.5.2
Progress: 100.00 PDB scanning finished
Offset Banner
0x118c7ac88 Linux version 5.15.0-88-generic (buildd@lcy02-and64-011) (gcc (Ubuntu 9.4.0-1ubuntu1-20.04.2) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #98-20.04.1-Ubuntu SMP Mon Oct 9 16:43:45 UTC 2
023 (Ubuntu 5.15.0-88.98-20.04.1-generic 5.15.126)
0x136225c88 Linux version 5.15.0-88-generic (buildd@lcy02-and64-011) (gcc (Ubuntu 9.4.0-1ubuntu1-20.04.2) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #98-20.04.1-Ubuntu SMP Mon Oct 9 16:43:45 UTC 2
023 (Ubuntu 5.15.0-88.98-20.04.1-generic 5.15.126)
0x136480c88 Linux version 5.15.0-88-generic (buildd@lcy02-and64-011) (gcc (Ubuntu 9.4.0-1ubuntu1-20.04.2) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #98-20.04.1-Ubuntu SMP Mon Oct 9 16:43:45 UTC 2
023 (Ubuntu 5.15.0-88.98-20.04.1-generic 5.15.126)
0x13661ec88 Linux version 5.15.0-88-generic (buildd@lcy02-and64-011) (gcc (Ubuntu 9.4.0-1ubuntu1-20.04.2) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #98-20.04.1-Ubuntu SMP Mon Oct 9 16:43:45 UTC 2
023 (Ubuntu 5.15.0-88.98-20.04.1-generic 5.15.126)
0x13675cc88 Linux version 5.15.0-88-generic (buildd@lcy02-and64-011) (gcc (Ubuntu 9.4.0-1ubuntu1-20.04.2) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #98-20.04.1-Ubuntu SMP Mon Oct 9 16:43:45 UTC 2
023 (Ubuntu 5.15.0-88.98-20.04.1-generic 5.15.126)
```

Plugin: **linux.pslist.PsList** : Lists the processes present in a particular Linux memory image [3]

```
$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.pslist
```

```
rusheel@ubuntu:~/volatility3$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.pslist
[sudo] password for rusheel:
Sorry, try again.
[sudo] password for rusheel:
Volatility 3 Framework 2.5.2
Progress: 100.00 Stacking attempts finished
Offset (V) PID TID PPID COMM File output
0x93e380291980 1 1 0 systemd Disabled
0x93e380293300 2 2 0 kthreadd Disabled
0x93e380294c80 3 3 2 rcu_gp Disabled
0x93e380296600 4 4 2 rcu_par_gp Disabled
0x93e380290000 5 5 2 slub_flushwq Disabled
0x93e3802acc80 6 6 2 netns Disabled
0x93e3802ae600 7 7 2 kworker/0:0 Disabled
0x93e3802a8000 8 8 2 kworker/0:0H Disabled
0x93e3802a9980 9 9 2 kworker/u256:0 Disabled
0x93e3802ab300 10 10 2 mm_percpu_wq Disabled
0x93e3802b1980 11 11 2 rcu_tasks_rude_ Disabled
0x93e3802b3300 12 12 2 rcu_tasks_trace Disabled
0x93e3802b4c80 13 13 2 ksoftirqd/0 Disabled
0x93e3802b6600 14 14 2 rcu_sched Disabled
0x93e3802b0000 15 15 2 migration/0 Disabled
0x93e38037b300 16 16 2 idle_inject/0 Disabled
0x93e38037cc80 17 17 2 kworker/0:1 Disabled
0x93e380a68000 18 18 2 cpuhp/0 Disabled
0x93e380a7cc80 19 19 2 cpuhp/1 Disabled
0x93e380a7e600 20 20 2 idle_inject/1 Disabled
0x93e380a78000 21 21 2 migration/1 Disabled
0x93e380a79980 22 22 2 ksoftirqd/1 Disabled
0x93e380a7b300 23 23 2 kworker/1:0 Disabled
0x93e380b03300 24 24 2 kworker/1:0H Disabled
0x93e380b04c80 25 25 2 cpuhp/2 Disabled
0x93e380b06600 26 26 2 idle_inject/2 Disabled
0x93e380b00000 27 27 2 migration/2 Disabled
0x93e380b01980 28 28 2 ksoftirqd/2 Disabled
0x93e380b16600 29 29 2 kworker/2:0 Disabled
0x93e380b10000 30 30 2 kworker/2:0H Disabled
0x93e380b11980 31 31 2 cpuhp/3 Disabled
0x93e380b13300 32 32 2 idle_inject/3 Disabled
```

Plugin: *linux.psscan.PsScan* : Scans for processes present in a particular linux image [3]

```
$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.psscan
```

```
rusheel@ubuntu:~/volatility3$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.psscan
Volatility 3 Framework 2.5.2
Progress: 100.00 Stacking attempts finished
OFFSET (P) PID TID PPID COMM EXIT_STATE
0x100290000 5 5 2 slub_flushwq TASK_RUNNING
0x100291980 1 1 0 systemd TASK_RUNNING
0x100293300 2 2 0 kthreadd TASK_RUNNING
0x100294c80 3 3 2 rcu_gp TASK_RUNNING
0x100296600 4 4 2 rcu_par_gp TASK_RUNNING
0x1002a8000 8 8 2 kworker/0:0H TASK_RUNNING
0x1002a9980 9 9 2 kworker/u256:0 TASK_RUNNING
0x1002ab300 10 10 2 mm_percpu_wq TASK_RUNNING
0x1002acc80 6 6 2 netns TASK_RUNNING
0x1002ae600 7 7 2 kworker/0:0 TASK_RUNNING
0x1002b0000 15 15 2 migration/0 TASK_RUNNING
0x1002b1980 11 11 2 rcu_tasks_rude TASK_RUNNING
0x1002b3300 12 12 2 rcu_tasks_trace TASK_RUNNING
0x1002b4c80 13 13 2 ksoftirqd/0 TASK_RUNNING
0x1002b6600 14 14 2 rcu_sched TASK_RUNNING
0x10037b300 16 16 2 idle_inject/0 TASK_RUNNING
0x10037cc80 17 17 2 kworker/0:1 TASK_RUNNING
0x100a68000 18 18 2 cpuhp/0 TASK_RUNNING
0x100a78000 21 21 2 migration/1 TASK_RUNNING
0x100a79980 22 22 2 ksoftirqd/1 TASK_RUNNING
0x100a7b300 23 23 2 kworker/1:0 TASK_RUNNING
0x100a7cc80 19 19 2 cpuhp/1 TASK_RUNNING
0x100a7e600 20 20 2 idle_inject/1 TASK_RUNNING
0x100b00000 27 27 2 migration/2 TASK_RUNNING
0x100b01980 28 28 2 ksoftirqd/2 TASK_RUNNING
0x100b03300 24 24 2 kworker/1:0H TASK_RUNNING
0x100b04c80 25 25 2 cpuhp/2 TASK_RUNNING
0x100b06600 26 26 2 idle_inject/2 TASK_RUNNING
0x100b10000 30 30 2 kworker/2:0H TASK_RUNNING
0x100b11980 31 31 2 cpuhp/3 TASK_RUNNING
0x100b13300 32 32 2 idle_inject/3 TASK_RUNNING
0x100b14c80 33 33 2 migration/3 TASK_RUNNING
0x100b16600 29 29 2 kworker/2:0 TASK_RUNNING
0x100b18000 34 34 2 ksoftirqd/3 TASK_RUNNING
0x100b19980 35 35 2 kworker/3:0 TASK_RUNNING
0x100b1b300 36 36 2 kworker/3:0H TASK_RUNNING
```

Plugin: **linux.bash.Bash** : Recovers bash command history from memory [3]

```
$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.bash
```

```
rusheel@ubuntu:~/volatility3$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.bash
Volatility 3 Framework 2.5.2
Progress: 100.00 Stacking attempts finished
PID Process CommandTime Command
2219 bash 2023-11-12 23:11:54.000000 cd volatility3/
2219 bash 2023-11-12 23:11:54.000000 sudo rmmod line
2219 bash 2023-11-12 23:11:54.000000 ps aux | grep lime
2219 bash 2023-11-12 23:11:54.000000 sudo kill -9 6881
2219 bash 2023-11-12 23:11:54.000000 LESSOPEN
2219 bash 2023-11-12 23:11:54.000000 *I,*V
2219 bash 2023-11-12 23:11:54.000000 uname -r
2219 bash 2023-11-12 23:11:54.000000 LANG=en_US.UTF-8
2219 bash 2023-11-12 23:11:54.000000 cd ../
2219 bash 2023-11-12 23:11:54.000000 sudo rmmod line
2219 bash 2023-11-12 23:11:54.000000 sudo insmod ./lime-5.15.0-88-generic.ko "path=/home/rusheel"
2219 bash 2023-11-12 23:11:54.000000 **V
2219 bash 2023-11-12 23:11:54.000000 sudo rmmod lime-5.15.0-88-generic
2219 bash 2023-11-12 23:11:54.000000 rm sample.raw
2219 bash 2023-11-12 23:11:54.000000 ls
2219 bash 2023-11-12 23:11:54.000000 cd src/
2219 bash 2023-11-12 23:11:54.000000 ls -al
2219 bash 2023-11-12 23:11:54.000000 sudo insmod ./lime-5.15.0-88-generic.ko "path=/home/rusheel/sample.raw format=raw"
2219 bash 2023-11-12 23:11:54.000000 sudo insmod ./lime-5.15.0-88-generic.ko "path=/home/rusheel/ubuntu format=lime"
2219 bash 2023-11-12 23:11:54.000000 cd ../../
2219 bash 2023-11-12 23:11:54.000000 ls
2219 bash 2023-11-12 23:11:54.000000 locate sample.lime
2219 bash 2023-11-12 23:11:54.000000 lsmod | grep line
2219 bash 2023-11-12 23:11:54.000000 ls
2219 bash 2023-11-12 23:11:54.000000 ls
2219 bash 2023-11-12 23:11:54.000000 ls
2219 bash 2023-11-12 23:11:54.000000 ls
2219 bash 2023-11-12 23:11:54.000000 sudo rm ubuntu.raw
2219 bash 2023-11-12 23:11:54.000000 lsmod | grep lime
2219 bash 2023-11-12 23:11:54.000000 sudo ./dwarf2json linux --elf /usr/lib/debug/boot/vmlinux-5.15.0-88-generic --system-map /boot/vmlinux > linux-image-5.15.0-88-amd64-dbg_5.15.0-88-amd64-Sy
stemMap.json
2219 bash 2023-11-12 23:11:54.000000 sudo ./dwarf2json linux --elf /usr/lib/debug/boot/vmlinux-5.15.0-88-generic --system-map /boot/System.map-5.15.0-88-generic > linux-image-5.15.0-88-amd64-d
bg_5.15.0-88-amd64-SystemMap.json
2219 bash 2023-11-12 23:11:54.000000 cd ../
2219 bash 2023-11-12 23:11:54.000000 dmesg | tail
```

Plugin: **linux.check\_creds.Check\_creds** : Checks if any processes are sharing credential structures [3]

```
$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime
linux.check_creds.Check_creds
```

```
rusheel@ubuntu:~/volatility3$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.check_creds.Check_creds
Volatility 3 Framework 2.5.2
Progress: 100.00 Stacking attempts finished
PIDs
```

Plugin: *linux.check\_idt.Check\_idt* : Checks if the IDT has been altered [3]

```
$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.check_idt.Check_idt
```

```
rusheel@ubuntu:~/volatility3$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.check_idt.Check_idt
Volatility 3 Framework 2.5.2
Progress: 100.00 Stacking attempts finished
Index Address Module Symbol
0x0 0xffff88e00940 __kernel__ asm_exc_divide_error
0x1 0xffff88e00c60 __kernel__ asm_exc_debug
0x2 0xffff88e01620 __kernel__ asm_exc_nmi
0x3 0xffff88e00b50 __kernel__ asm_exc_int3
0x4 0xffff88e00960 __kernel__ asm_exc_overflow
0x5 0xffff88e00980 __kernel__ asm_exc_bounds
0x6 0xffff88e00b30 __kernel__ asm_exc_invalid_op
0x7 0xffff88e009a0 __kernel__ asm_exc_device_not_available
0x8 0xffff88e00cc0 __kernel__ asm_exc_double_fault
0x9 0xffff88e009c0 __kernel__ asm_exc_coproc_segment_overrun
0xa 0xffff88e00a40 __kernel__ asm_exc_invalid_tss
0xb 0xffff88e00a70 __kernel__ asm_exc_segment_not_present
0xc 0xffff88e00aa0 __kernel__ asm_exc_stack_segment
0xd 0xffff88e00ad0 __kernel__ asm_exc_general_protection
0xe 0xffff88e00b90 __kernel__ asm_exc_page_fault
0xf 0xffff88e009e0 __kernel__ asm_exc_spurious_interrupt_bug
0x10 0xffff88e00a00 __kernel__ asm_exc_coprocessor_error
0x11 0xffff88e00b00 __kernel__ asm_exc_alignment_check
0x12 0xffff88e00bc0 __kernel__ asm_exc_machine_check
0x13 0xffff88e00a20 __kernel__ asm_exc_simd_coprocessor_error
0x80 0xffff88e019f0 __kernel__ entry_INT80_compat
```

Plugin: *linux.check\_syscall.Check\_syscall* : Check system call table for hooks [3]

```
$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime
linux.check_syscall.Check_syscall
```

```
rusheel@ubuntu:~/volatility3$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.check_syscall.Check_syscall
Volatility 3 Framework 2.5.2
Progress: 100.00 Stacking attempts finished
Table Address Table Name Index Handler Address Handler Symbol
0xffff82200320 64bit 0 0xffff8838bf30 __x64_sys_read
0xffff82200320 64bit 1 0xffff8838c060 __x64_sys_write
0xffff82200320 64bit 2 0xffff88388790 __x64_sys_open
0xffff82200320 64bit 3 0xffff88385f30 __x64_sys_close
0xffff82200320 64bit 4 0xffff88391bb0 __x64_sys_newstat
0xffff82200320 64bit 5 0xffff883927e0 __x64_sys_newlstat
0xffff82200320 64bit 6 0xffff88391c70 __x64_sys_newlstat
0xffff82200320 64bit 7 0xffff883a89a0 __x64_sys_poll
0xffff82200320 64bit 8 0xffff88388dd0 __x64_sys_lseek
0xffff82200320 64bit 9 0xffff88045900 __x64_sys_mmap
0xffff82200320 64bit 10 0xffff88307440 __x64_sys_mprotect
0xffff82200320 64bit 11 0xffff883026a0 __x64_sys_munmap
0xffff82200320 64bit 12 0xffff88303a30 __x64_sys_brk
0xffff82200320 64bit 13 0xffff880d5a30 __x64_sys_rt_sigaction
0xffff82200320 64bit 14 0xffff880d14e0 __x64_sys_rt_sigprocmask
0xffff82200320 64bit 15 0xffff8803e510 __do_sys_rt_sigreturn
0xffff82200320 64bit 16 0xffff883a4f40 __x64_sys_ioctl
0xffff82200320 64bit 17 0xffff8838c140 __x64_sys_pread64
0xffff82200320 64bit 18 0xffff8838c240 __x64_sys_pwrite64
0xffff82200320 64bit 19 0xffff8838a340 __x64_sys_readv
0xffff82200320 64bit 20 0xffff8838acd0 __x64_sys_writev
0xffff82200320 64bit 21 0xffff88385b60 __x64_sys_access
0xffff82200320 64bit 22 0xffff88397e00 __x64_sys_plpe
0xffff82200320 64bit 23 0xffff883a8fb0 __x64_sys_select
0xffff82200320 64bit 24 0xffff880ffb60 __do_sys_sched_yield
0xffff82200320 64bit 25 0xffff88309440 __x64_sys_mremap
0xffff82200320 64bit 26 0xffff88309760 __x64_sys_msync
0xffff82200320 64bit 27 0xffff882fd180 __x64_sys_mincore
0xffff82200320 64bit 28 0xffff883258b0 __x64_sys_madvise
0xffff82200320 64bit 29 0xffff88512bb0 __x64_sys_shmget
0xffff82200320 64bit 30 0xffff885150e0 __x64_sys_shmat
0xffff82200320 64bit 31 0xffff88514750 __x64_sys_shmctl
0xffff82200320 64bit 32 0xffff883b2ad0 __x64_sys_dup
0xffff82200320 64bit 33 0xffff883b2de0 __x64_sys_dup2
```



Plugin: *linux.elfs.Elfs* : Lists all memory mapped ELF files for all processes [3]

```
$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.elfs.Elfs
```

```
rusheel@ubuntu:~/volatility3$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.elfs.Elfs
Volatility 3 Framework 2.5.2
Progress: 100.00 Stacking attempts finished
PID Process Start End File Path File Output
1 systemd 0x55b0887e9000 0x55b08881b000 /usr/lib/systemd/systemd Disabled
1 systemd 0x7f6d73ae1000 0x7f6d73aee000 /usr/lib/x86_64-linux-gnu/libm-2.31.so Disabled
1 systemd 0x7f6d73c30000 0x7f6d73c35000 /usr/lib/x86_64-linux-gnu/libudev.so.1.6.17 Disabled
1 systemd 0x7f6d73c5d000 0x7f6d73c6d000 /usr/lib/x86_64-linux-gnu/libunistring.so.2.1.0 Disabled
1 systemd 0x7f6d73ddfd00 0x7f6d73de3000 /usr/lib/x86_64-linux-gnu/libgpg-error.so.0.28.0 Disabled
1 systemd 0x7f6d73e02000 0x7f6d73e06000 /usr/lib/x86_64-linux-gnu/libjson-c.so.4.0.0 Disabled
1 systemd 0x7f6d73e16000 0x7f6d73e17000 /usr/lib/x86_64-linux-gnu/libargon2.so.1 Disabled
1 systemd 0x7f6d73e20000 0x7f6d73e2a000 /usr/lib/x86_64-linux-gnu/libdevmapper.so.1.02.1 Disabled
1 systemd 0x7f6d73e8b000 0x7f6d73e8d000 /usr/lib/x86_64-linux-gnu/libuuid.so.1.3.0 Disabled
1 systemd 0x7f6d73e94000 0x7f6d73f0c000 /usr/lib/x86_64-linux-gnu/libcrypto.so.1.1 Disabled
1 systemd 0x7f6d7416a000 0x7f6d7416e000 /usr/lib/x86_64-linux-gnu/libzstd.so.1.4.4 Disabled
1 systemd 0x7f6d74213000 0x7f6d74215000 /usr/lib/x86_64-linux-gnu/libcap-ng.so.0.0.0 Disabled
1 systemd 0x7f6d7421d000 0x7f6d7421e000 /usr/lib/x86_64-linux-gnu/libdl-2.31.so Disabled
1 systemd 0x7f6d74223000 0x7f6d74225000 /usr/lib/x86_64-linux-gnu/libpcre2-8.so.0.9.0 Disabled
1 systemd 0x7f6d742b4000 0x7f6d742ba000 /usr/lib/x86_64-linux-gnu/libpthread-2.31.so Disabled
1 systemd 0x7f6d742d7000 0x7f6d742da000 /usr/lib/x86_64-linux-gnu/liblzma.so.5.2.4 Disabled
1 systemd 0x7f6d74300000 0x7f6d74302000 /usr/lib/x86_64-linux-gnu/liblz4.so.1.9.2 Disabled
1 systemd 0x7f6d74323000 0x7f6d74325000 /usr/lib/x86_64-linux-gnu/libip4tc.so.2.0.0 Disabled
1 systemd 0x7f6d7432d000 0x7f6d7432f000 /usr/lib/x86_64-linux-gnu/libidn2.so.0.3.6 Disabled
1 systemd 0x7f6d7434e000 0x7f6d7435a000 /usr/lib/x86_64-linux-gnu/libgcrypt.so.20.2.5 Disabled
1 systemd 0x7f6d7446c000 0x7f6d74473000 /usr/lib/x86_64-linux-gnu/libcryptsetup.so.12.5.0 Disabled
1 systemd 0x7f6d744d3000 0x7f6d744d5000 /usr/lib/x86_64-linux-gnu/libcrypt.so.1.1.0 Disabled
1 systemd 0x7f6d7450e000 0x7f6d74510000 /usr/lib/x86_64-linux-gnu/libcap.so.2.32 Disabled
1 systemd 0x7f6d74519000 0x7f6d74523000 /usr/lib/x86_64-linux-gnu/libblkid.so.1.1.0 Disabled
1 systemd 0x7f6d74570000 0x7f6d74572000 /usr/lib/x86_64-linux-gnu/libacl.so.1.1.2253 Disabled
1 systemd 0x7f6d7457b000 0x7f6d7457e000 /usr/lib/x86_64-linux-gnu/libapparmor.so.1.6.1 Disabled
1 systemd 0x7f6d74590000 0x7f6d74594000 /usr/lib/x86_64-linux-gnu/libkmod.so.2.3.5 Disabled
1 systemd 0x7f6d745ad000 0x7f6d745b0000 /usr/lib/x86_64-linux-gnu/libaudit.so.1.0.0 Disabled
1 systemd 0x7f6d745d9000 0x7f6d745dc000 /usr/lib/x86_64-linux-gnu/libpam.so.0.84.2 Disabled
1 systemd 0x7f6d745ed000 0x7f6d745f8000 /usr/lib/x86_64-linux-gnu/libmount.so.1.1.0 Disabled
1 systemd 0x7f6d7464d000 0x7f6d74653000 /usr/lib/x86_64-linux-gnu/libselinux.so.1 Disabled
1 systemd 0x7f6d74678000 0x7f6d7467a000 /usr/lib/x86_64-linux-gnu/libseccomp.so.2.5.1 Disabled
1 systemd 0x7f6d7469a000 0x7f6d7469c000 /usr/lib/x86_64-linux-gnu/librt-2.31.so Disabled
1 systemd 0x7f6d746a4000 0x7f6d746ea000 /usr/lib/systemd/libsystemd-shared-245.so Disabled
```

Plugin: **linux.envvars.Envvars** : Lists processes with their environment variables [3].

```
$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.envvars.Envvars
```

```
rusheel@ubuntu:~/volatility3$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.envvars.Envvars
Volatility 3 Framework 2.5.2
Progress: 100.00 Stacking attempts finished
PID PPID COMM KEY VALUE
1 0 systemd find_preseed /preseed.cfg
1 0 systemd HOME /
1 0 systemd init /sbin/init
1 0 systemd NETWORK_SKIP_ENSLAVED
1 0 systemd locale en_US
1 0 systemd TERM linux
1 0 systemd BOOT_IMAGE /boot/vmlinuz-5.15.0-88-generic
1 0 systemd drop_caps
1 0 systemd PATH /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
1 0 systemd PWD /
1 0 systemd rootmnt /root
1 0 systemd priority critical
380 1 systemd-journal LANG en_US.UTF-8
380 1 systemd-journal PATH /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
380 1 systemd-journal NOTIFY_SOCKET /run/systemd/notify
380 1 systemd-journal LISTEN_PID 380
380 1 systemd-journal LISTEN_FDS 4
380 1 systemd-journal LISTEN_FDNAMES systemd-journald-dev-log.socket:systemd-journald-audit.socket:systemd-journald.socket:systemd-journald.socket
380 1 systemd-journal INVOCATION_ID add859e89cea4e8ea5d5d5c067ee2d5
380 1 systemd-journal RUNTIME_DIRECTORY /run/systemd/journal
429 1 systemd-udevd LANG en_US.UTF-8
429 1 systemd-udevd PATH /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
429 1 systemd-udevd NOTIFY_SOCKET /run/systemd/notify
429 1 systemd-udevd LISTEN_PID 429
429 1 systemd-udevd LISTEN_FDS 2
429 1 systemd-udevd LISTEN_FDNAMES systemd-udevd-kernel.socket:systemd-udevd-control.socket
429 1 systemd-udevd WATCHDOG_PID 429
429 1 systemd-udevd WATCHDOG_USEC 180000000
429 1 systemd-udevd INVOCATION_ID 9142d024241a48548ed2614812192d25
429 1 systemd-udevd JOURNAL_STREAM 8:19088
437 1 vmware-vmtoolsd HOME /root
437 1 vmware-vmtoolsd JOURNAL_STREAM 8:33181
437 1 vmware-vmtoolsd INVOCATION_ID 8f5618157ed1480597fc59e5914977c9
437 1 vmware-vmtoolsd LANG en_US.UTF-8
437 1 vmware-vmtoolsd PWD /
```

Plugin: **linux.lsmmod.Lsmmod** : Lists loaded kernel modules [3].

```
$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.lsmmod.Lsmmod
```

```
rusheel@ubuntu:~/volatility3$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.lsmmod.Lsmmod
Volatility 3 Framework 2.5.2
Progress: 100.00 Stacking attempts finished
Offset Name Size
0xfffffc0a1e040 lime 24576
0xfffffc0acc700 rfcomm 81920
0xfffffc09ac900 bnep 28672
0xfffffc098d140 vsock_loopback 16384
0xfffffc0999c00 vmw_vsock_virtio_transport_common 40960
0xfffffc09873c0 vmw_vsock_vmci_transport 32768
0xfffffc096f500 vsock 45056
0xfffffc0887100 nls_iso8859_1 16384
0xfffffc0882400 intel_rapl_msr 20480
0xfffffc08aa580 snd_ens1371 32768
0xfffffc09012c0 snd_ac97_codec 155648
0xfffffc07dd280 gameport 24576
0xfffffc07d70c0 ac97_bus 16384
0xfffffc08d8780 snd_pcm 135168
0xfffffc08bcd80 intel_rapl_common 40960
0xfffffc08b3500 vmw_balloon 24576
0xfffffc0810240 crct10dif_pclmul 16384
0xfffffc087c2c0 snd_seq_midi 20480
0xfffffc0876280 snd_seq_midi_event 16384
0xfffffc07b5440 ghash_clmulni_intel 16384
0xfffffc0866fc0 aesni_intel 376832
0xfffffc07f2440 binfmt_misc 24576
0xfffffc07e8040 crypto_simd 16384
0xfffffc080a180 cryptd 24576
0xfffffc0792d40 rapl 20480
0xfffffc07fd6c0 snd_rawmidi 49152
0xfffffc07d1940 btusb 61440
0xfffffc079b480 btrtl 24576
0xfffffc07bf0c0 btbcm 24576
0xfffffc07ac800 snd_seq 77824
0xfffffc08a1280 btintel 40960
0xfffffc06e1140 snd_seq_device 16384
0xfffffc06d86c0 joydev 32768
0xfffffc0892180 snd_timer 40960
0xfffffc06cf140 input_leds 16384
0xfffffc076a680 bluetooth 688128
```

Plugin: *linux.lsof.Lsof* : Lists all memory maps for all processes [1] .

```
$ sudo python3 vol.py ~/LiME/src/ubuntu.lime linux.lsof.Lsof
```

```
rusheel@ubuntu:~/volatility3$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.lsof.Lsof
Volatility 3 Framework 2.5.2
Progress: 100.00 Stacking attempts finished
PID Process FD Path
1 systemd 0 /dev/null
1 systemd 1 /dev/null
1 systemd 2 /dev/null
1 systemd 3 /dev/kmsg
1 systemd 4 anon_inode:[14611]
1 systemd 5 anon_inode:[14611]
1 systemd 6 anon_inode:[14611]
1 systemd 7 /sys/fs/cgroup/unified
1 systemd 8 anon_inode:[14611]
1 systemd 9 anon_inode:[14611]
1 systemd 10 /proc/1/mountinfo
1 systemd 11 anon_inode:[14611]
1 systemd 12 /dev/dri/card0
1 systemd 13 anon_inode:[14611]
1 systemd 14 /proc/swaps
1 systemd 15 socket:[26687]
1 systemd 16 socket:[26688]
1 systemd 17 socket:[26689]
1 systemd 18 socket:[26690]
1 systemd 19 socket:[26691]
1 systemd 20 socket:[26693]
1 systemd 21 socket:[52303]
1 systemd 22 socket:[52304]
1 systemd 23 socket:[52334]
1 systemd 24 socket:[52335]
1 systemd 25 anon_inode:[14611]
1 systemd 26 /dev/autofs
1 systemd 27 pipe:[26700]
1 systemd 28 anon_inode:[14611]
1 systemd 29 socket:[26702]
1 systemd 30 socket:[26704]
1 systemd 31 /run/initctl
1 systemd 32 socket:[26711]
1 systemd 33 socket:[26712]
1 systemd 34 socket:[26714]
1 systemd 35 socket:[26716]
```

```
$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.malfind.Malfind
```

Plugin: *linux.mountinfo.MountInfo* : Lists mount points on processes mount namespaces[4].

```
$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.mountinfo.MountInfo
```

```

root@kali:~/LHME/src/ubuntu.lhme linux.mountinfo MountInfo
Volatility 3 Framework 2.5.2
Progress: 100.00
Stacking attempts finished

```

MNT NS ID	MOUNT ID	PARENT ID	MAJOR:MINOR	ROOT	MOUNT POINT	MOUNT OPTIONS	FIELDS	FSTYPE	MOUNT SRC	SB OPTIONS
4026531841	1	0	2	/	/	rw,rofs none rw				
4026531841	1	29	0	22	/	/sys rw,nosuid,nodev,noexec,relatime shared:7	sysfs	sysfs	rw	
4026531841	25	29	0	23	/	/proc rw,nosuid,nodev,noexec,relatime shared:14	proc	proc	rw	
4026531841	26	29	0	15	/	/dev rw,nosuid,nodev,noexec,relatime shared:2	devtmpfs	devtmpfs	rw	
4026531841	27	26	0	24	/	/dev/pts rw,nosuid,nodev,noexec,relatime shared:3	devpts	devpts	rw	
4026531841	28	29	0	25	/	/run rw,nosuid,nodev,noexec,relatime shared:5	tmpfs	tmpfs	rw	
4026531841	29	1	8	15	/	rw,relatime shared:1 ext4 /dev/sda5	rw			
4026531841	30	24	0	16	/	/sys/kernel/security rw,nosuid,nodev,noexec,relatime shared:8	rw	securityfs	securityfs	rw
4026531841	31	26	0	26	/	/dev/shm rw,nosuid,nodev shared:4	tmpfs			
4026531841	32	28	0	27	/	/run/lock rw,nosuid,nodev,noexec,relatime shared:6	tmpfs	tmpfs	rw	
4026531841	33	24	0	28	/	/sys/fs/cgroup rw,nosuid,nodev,noexec,relatime shared:9	tmpfs	tmpfs	rw	
4026531841	34	33	0	29	/	/sys/fs/cgroup/unified rw,nosuid,nodev,noexec,relatime shared:10	cgroup2	cgroup2	rw	
4026531841	35	33	0	30	/	/sys/fs/cgroup/systemd rw,nosuid,nodev,noexec,relatime shared:11	cgroup	cgroup	rw	
4026531841	36	24	0	31	/	/sys/fs/pstore rw,nosuid,nodev,noexec,relatime shared:12	pstore	pstore	rw	
4026531841	37	24	0	32	/	/sys/fs/bpf rw,nosuid,nodev,noexec,relatime shared:13	bpf			
4026531841	38	33	0	33	/	/sys/fs/cgroup/bkrio rw,nosuid,nodev,noexec,relatime shared:15	cgroup	cgroup	rw	
4026531841	39	33	0	34	/	/sys/fs/cgroup/net_cls,nfs rw,nosuid,nodev,noexec,relatime shared:16	cgroup	cgroup	rw	
4026531841	40	33	0	35	/	/sys/fs/cgroup/misc rw,nosuid,nodev,noexec,relatime shared:17	cgroup	cgroup	rw	
4026531841	41	33	0	36	/	/sys/fs/cgroup/perf_event rw,nosuid,nodev,noexec,relatime shared:18	cgroup	cgroup	rw	
4026531841	42	33	0	37	/	/sys/fs/cgroup/devices rw,nosuid,nodev,noexec,relatime shared:19	cgroup	cgroup	rw	
4026531841	43	33	0	38	/	/sys/fs/cgroup/memory rw,nosuid,nodev,noexec,relatime shared:20	cgroup	cgroup	rw	
4026531841	44	33	0	39	/	/sys/fs/cgroup/freezer rw,nosuid,nodev,noexec,relatime shared:21	cgroup	cgroup	rw	
4026531841	45	33	0	40	/	/sys/fs/cgroup/cpu,cpuacct rw,nosuid,nodev,noexec,relatime shared:22	cgroup	cgroup	rw	
4026531841	46	33	0	41	/	/sys/fs/cgroup/cpuset rw,nosuid,nodev,noexec,relatime shared:23	cgroup	cgroup	rw	
4026531841	47	33	0	42	/	/sys/fs/cgroup/pids rw,nosuid,nodev,noexec,relatime shared:24	cgroup	cgroup	rw	
4026531841	48	33	0	43	/	/sys/fs/cgroup/hugetlb rw,nosuid,nodev,noexec,relatime shared:25	cgroup	cgroup	rw	
4026531841	49	33	0	44	/	/sys/fs/cgroup/rdma rw,nosuid,nodev,noexec,relatime shared:26	cgroup	cgroup	rw	
4026531841	50	25	0	45	/	/proc/sys/fs/binfmt_misc rw,relatime shared:27	autofs	systemd-1	rw	
4026531841	51	26	0	46	/	/dev/hugepages rw,nosuid,nodev,relatime shared:28	hugetlbfs			
4026531841	52	26	0	47	/	/dev/mqueue rw,nosuid,nodev,noexec,relatime shared:29	mqueue			
4026531841	53	24	0	48	/	/sys/kernel/debug rw,nosuid,nodev,noexec,relatime shared:30	debugfs	debugfs	rw	
4026531841	54	24	0	49	/	/sys/kernel/tracing rw,nosuid,nodev,noexec,relatime shared:31	tracefs	tracefs	rw	
4026531841	56	29	7	0	/	/snap/core20/2015 ro,nodev,relatime shared:32	squashfs	/dev/loop0	ro	
4026531841	57	29	7	1	/	/snap/gnome-3-38-2004/119 ro,nodev,relatime shared:33	squashfs	/dev/loop2	ro	
4026531841	58	29	7	1	/	/snap/bare/5 ro,nodev,relatime shared:34	squashfs	/dev/loop1	ro	
4026531841	59	29	7	1	/	/snap/core20/1828 ro,nodev,relatime shared:35	squashfs	/dev/loop4	ro	
4026531841	60	29	7	1	/	/snap/gnome-42-2204/141 ro,nodev,relatime shared:36	squashfs	/dev/loop3	ro	
4026531841	136	29	7	1	/	/snap/gnome-3-38-2004/143 ro,nodev,relatime shared:75	squashfs	/dev/loop5	ro	
4026531841	139	29	7	1	/	/snap/core22/1864 ro,nodev,relatime shared:77	squashfs	/dev/loop7	ro	



Plugin: **linux.proc.Maps** : Lists all memory maps for all processes [3] .

```
$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.proc.Maps
```

```
rusheel@ubuntu:~/volatility3$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.proc.Maps
Volatility 3 Framework 2.5.2
Progress: 100.00 Stacking attempts finished
```

PID	Process	Start	End	Flags	PgOff	Major	Minor	Inode	File Path	File output
1	systemd	0x55b0887e9000	0x55b08881b000	r--	0x0	8	5	1313208	/usr/lib/systemd/systemd	Disabled
1	systemd	0x55b08881b000	0x55b0888d9000	r-x	0x32000	8	5	1313208	/usr/lib/systemd/systemd	Disabled
1	systemd	0x55b0888d9000	0x55b08892f000	r--	0xf0000	8	5	1313208	/usr/lib/systemd/systemd	Disabled
1	systemd	0x55b08892f000	0x55b088975000	r--	0x145000	8	5	1313208	/usr/lib/systemd/systemd	Disabled
1	systemd	0x55b088975000	0x55b088976000	rw-	0x18b000	8	5	1313208	/usr/lib/systemd/systemd	Disabled
1	systemd	0x55b088a404000	0x55b088a656000	rw-	0x0	0	0	0	[heap]	Disabled
1	systemd	0x7f6d64000000	0x7f6d64021000	rw-	0x0	0	0	0	Anonymous Mapping	Disabled
1	systemd	0x7f6d64021000	0x7f6d68000000	---	0x0	0	0	0	Anonymous Mapping	Disabled
1	systemd	0x7f6d6c000000	0x7f6d6c021000	rw-	0x0	0	0	0	Anonymous Mapping	Disabled
1	systemd	0x7f6d6c021000	0x7f6d70000000	---	0x0	0	0	0	Anonymous Mapping	Disabled
1	systemd	0x7f6d72ad8000	0x7f6d72ad9000	---	0x0	0	0	0	Anonymous Mapping	Disabled
1	systemd	0x7f6d72ad9000	0x7f6d732d9000	rw-	0x0	0	0	0	Anonymous Mapping	Disabled
1	systemd	0x7f6d732d9000	0x7f6d732da000	---	0x0	0	0	0	Anonymous Mapping	Disabled
1	systemd	0x7f6d732da000	0x7f6d73ae1000	rw-	0x0	0	0	0	Anonymous Mapping	Disabled
1	systemd	0x7f6d73ae1000	0x7f6d73ae0000	r--	0x0	8	5	1312945	/usr/lib/x86_64-linux-gnu/libm-2.31.so	Disabled
1	systemd	0x7f6d73ae0000	0x7f6d73b95000	r-x	0xd000	8	5	1312945	/usr/lib/x86_64-linux-gnu/libm-2.31.so	Disabled
1	systemd	0x7f6d73b95000	0x7f6d73c2e000	r--	0xb4000	8	5	1312945	/usr/lib/x86_64-linux-gnu/libm-2.31.so	Disabled
1	systemd	0x7f6d73c2e000	0x7f6d73c2f000	r--	0x14c000	8	5	1312945	/usr/lib/x86_64-linux-gnu/libm-2.31.so	Disabled
1	systemd	0x7f6d73c2f000	0x7f6d73c30000	rw-	0x14d000	8	5	1312945	/usr/lib/x86_64-linux-gnu/libm-2.31.so	Disabled
1	systemd	0x7f6d73c30000	0x7f6d73c35000	r--	0x0	8	5	1310844	/usr/lib/x86_64-linux-gnu/libudev.so.1.6.17	Disabled
1	systemd	0x7f6d73c35000	0x7f6d73c51000	r-x	0x5000	8	5	1310844	/usr/lib/x86_64-linux-gnu/libudev.so.1.6.17	Disabled
1	systemd	0x7f6d73c51000	0x7f6d73c5b000	r--	0x21000	8	5	1310844	/usr/lib/x86_64-linux-gnu/libudev.so.1.6.17	Disabled
1	systemd	0x7f6d73c5b000	0x7f6d73c50000	r--	0x2a000	8	5	1310844	/usr/lib/x86_64-linux-gnu/libudev.so.1.6.17	Disabled
1	systemd	0x7f6d73c5c000	0x7f6d73c5d000	rw-	0x2b000	8	5	1310844	/usr/lib/x86_64-linux-gnu/libudev.so.1.6.17	Disabled
1	systemd	0x7f6d73c5d000	0x7f6d73c6d000	r--	0x0	8	5	1318464	/usr/lib/x86_64-linux-gnu/libunistring.so.2.1.0	Disabled
1	systemd	0x7f6d73c6d000	0x7f6d73ca3000	r-x	0x10000	8	5	1318464	/usr/lib/x86_64-linux-gnu/libunistring.so.2.1.0	Disabled
1	systemd	0x7f6d73ca3000	0x7f6d73dda000	r--	0x46000	8	5	1318464	/usr/lib/x86_64-linux-gnu/libunistring.so.2.1.0	Disabled
1	systemd	0x7f6d73dda000	0x7f6d73ddb000	---	0x17d000	8	5	1318464	/usr/lib/x86_64-linux-gnu/libunistring.so.2.1.0	Disabled
1	systemd	0x7f6d73ddb000	0x7f6d73dde000	r--	0x17d000	8	5	1318464	/usr/lib/x86_64-linux-gnu/libunistring.so.2.1.0	Disabled
1	systemd	0x7f6d73dde000	0x7f6d73ddf000	rw-	0x180000	8	5	1318464	/usr/lib/x86_64-linux-gnu/libunistring.so.2.1.0	Disabled
1	systemd	0x7f6d73ddf000	0x7f6d73de3000	r--	0x0	8	5	1317676	/usr/lib/x86_64-linux-gnu/libgpg-error.so.0.28.0	Disabled
1	systemd	0x7f6d73de3000	0x7f6d73df6000	r-x	0x4000	8	5	1317676	/usr/lib/x86_64-linux-gnu/libgpg-error.so.0.28.0	Disabled
1	systemd	0x7f6d73df6000	0x7f6d73e00000	r--	0x17000	8	5	1317676	/usr/lib/x86_64-linux-gnu/libgpg-error.so.0.28.0	Disabled
1	systemd	0x7f6d73e00000	0x7f6d73e01000	r--	0x20000	8	5	1317676	/usr/lib/x86_64-linux-gnu/libgpg-error.so.0.28.0	Disabled

Plugin: **linux.psaux.PsAux** : Lists processes with their command line arguments [3] .

```
$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.psaux.PsAux
```

```
rusheel@ubuntu:~/volatility3$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.psaux.PsAux
Volatility 3 Framework 2.5.2
Progress: 100.00 Stacking attempts finished
```

PID	PPID	COMM	ARGS
1	0	systemd /sbin/init	auto noprompt
2	0	kthreadd	[kthreadd]
3	2	rcu_gp	[rcu_gp]
4	2	rcu_par_gp	[rcu_par_gp]
5	2	slub_flushwq	[slub_flushwq]
6	2	netns	[netns]
7	2	kworker/0:0	[kworker/0:0]
8	2	kworker/0:0H	[kworker/0:0H]
9	2	kworker/u256:0	[kworker/u256:0]
10	2	mm_percpu_wq	[mm_percpu_wq]
11	2	rcu_tasks_rude	[rcu_tasks_rude]
12	2	rcu_tasks_trace	[rcu_tasks_trace]
13	2	ksoftirqd/0	[ksoftirqd/0]
14	2	rcu_sched	[rcu_sched]
15	2	migration/0	[migration/0]
16	2	idle_inject/0	[idle_inject/0]
17	2	kworker/0:1	[kworker/0:1]
18	2	cpuhp/0	[cpuhp/0]
19	2	cpuhp/1	[cpuhp/1]
20	2	idle_inject/1	[idle_inject/1]
21	2	migration/1	[migration/1]
22	2	ksoftirqd/1	[ksoftirqd/1]
23	2	kworker/1:0	[kworker/1:0]
24	2	kworker/1:0H	[kworker/1:0H]
25	2	cpuhp/2	[cpuhp/2]
26	2	idle_inject/2	[idle_inject/2]
27	2	migration/2	[migration/2]
28	2	ksoftirqd/2	[ksoftirqd/2]
29	2	kworker/2:0	[kworker/2:0]
30	2	kworker/2:0H	[kworker/2:0H]
31	2	cpuhp/3	[cpuhp/3]
32	2	idle_inject/3	[idle_inject/3]
33	2	migration/3	[migration/3]

Plugin: **linux.sockstat.Sockstat** : Lists all network connections for all processes [3] .

```
$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.sockstat.Sockstat
```

rusheel@ubuntu:~/volatility3\$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.sockstat.Sockstat													
Volatility 3 Framework 2.5.2													
Progress: 100.00													
Stacking attempts finished													
NetNS	Pid	FD	Sock Offset	Family	Type	Proto	Source Addr	Source Port	Destination Addr	Destination Port	State	Filter	
4026531840	1	15	0x93e3933a5800	AF_NETLINK	RAW	NETLINK_KOB3JECT_UEVENT	groups:0x00000002	1	group:0x00000000	0	UNCONNECTED	filter_type=socket_filter,b	
pf_filter_type=CBPF													
4026531840	1	16	0x93e384236e80	AF_UNIX	DGRAM	-	/run/systemd/notify	26688	-	-	UNCONNECTED	-	
4026531840	1	17	0x93e384236b80	AF_UNIX	DGRAM	-	-	26689	-	26690	CONNECTED	-	
4026531840	1	18	0x93e384232640	AF_UNIX	DGRAM	-	-	26690	-	26689	CONNECTED	-	
4026531840	1	19	0x93e384232200	AF_UNIX	STREAM	-	/run/systemd/private	26691	-	-	LISTEN	-	
4026531840	1	20	0x93e384232a80	AF_UNIX	STREAM	-	/run/systemd/userdb/io.systemd.DynamicUser	26693	-	-	LISTEN	-	
4026531840	1	21	0x93e389d42200	AF_UNIX	STREAM	-	/run/systemd/journal/stdout	52303	-	52301	ESTABLISHED	-	
4026531840	1	22	0x93e389d40440	AF_UNIX	STREAM	-	/run/systemd/journal/stdout	52304	-	52302	ESTABLISHED	-	
4026531840	1	23	0x93e389d41100	AF_UNIX	STREAM	-	/run/systemd/journal/stdout	52334	-	52333	ESTABLISHED	-	
4026531840	1	24	0x93e38ec9a640	AF_UNIX	STREAM	-	/run/systemd/journal/stdout	52335	-	53279	ESTABLISHED	-	
4026531840	1	29	0x93e384230440	AF_UNIX	DGRAM	-	/run/systemd/journal/syslog	26702	-	-	UNCONNECTED	-	
4026531840	1	30	0x93e384236a40	AF_UNIX	STREAM	-	/run/systemd/fsck.progress	26704	-	-	LISTEN	-	
4026531840	1	32	0x93e3933a7800	AF_NETLINK	RAW	NETLINK_AUDIT	groups:0x00000001	1	group:0x00000000	0	UNCONNECTED	-	
4026531840	1	33	0x93e384234400	AF_UNIX	DGRAM	-	/run/systemd/journal/dev-log	26712	-	-	UNCONNECTED	-	
4026531840	1	34	0x93e3842350c0	AF_UNIX	STREAM	-	/run/systemd/journal/stdout	26714	-	-	LISTEN	-	
4026531840	1	35	0x93e384231dc0	AF_UNIX	DGRAM	-	/run/systemd/journal/socket	26716	-	-	UNCONNECTED	-	
4026531840	1	36	0x93e3933a1000	AF_UNIX	SEQPACKET	-	/run/udev/control	26718	-	-	UNCONNECTED	-	
4026531840	1	37	0x93e3933a1000	AF_NETLINK	RAW	NETLINK_KOB3JECT_UEVENT	groups:0x00000001	3627223072	group:0x00000000	0	UNCONNECTED	-	
4026531840	1	40	0x93e3933a0000	AF_NETLINK	RAW	NETLINK_AUDIT	-	2183184094	group:0x00000000	0	UNCONNECTED	-	
4026531840	1	43	0x93e39307b800	AF_UNIX	DGRAM	-	-	34317	/run/systemd/journal/socket	26716	UNCONNECTED	-	
4026531840	1	46	0x93e3cf9d90c0	AF_UNIX	STREAM	-	/run/systemd/journal/stdout	59268	-	59868	ESTABLISHED	-	
4026531840	1	48	0x93e389fcd800	AF_UNIX	STREAM	-	/run/systemd/journal/stdout	52228	-	51560	ESTABLISHED	-	
4026531840	1	49	0x93e394c2a200	AF_UNIX	STREAM	-	/run/systemd/journal/stdout	36415	-	35700	ESTABLISHED	-	
4026531840	1	50	0x93e38423b0c0	AF_UNIX	STREAM	-	/run/systemd/journal/stdout	35764	-	35763	ESTABLISHED	-	
4026531840	1	51	0x93e392f2f5940	AF_UNIX	STREAM	-	/run/systemd/journal/stdout	36498	-	36399	ESTABLISHED	-	
4026531840	1	52	0x93e384234c80	AF_UNIX	STREAM	-	/run/systemd/journal/stdout	35513	-	36350	ESTABLISHED	-	
4026531840	1	53	0x93e384231980	AF_UNIX	STREAM	-	/run/acpid.socket	36459	-	-	LISTEN	-	
4026531840	1	54	0x93e384232ec0	AF_UNIX	STREAM	-	/run/avahi-daemon/socket	36461	-	-	LISTEN	-	
4026531840	1	55	0x93e384233fc0	AF_UNIX	STREAM	-	/run/cups/socket	36463	-	-	LISTEN	-	
4026531840	1	56	0x93e384235940	AF_UNIX	STREAM	-	/run/dbus/system_bus_socket	36465	-	-	LISTEN	-	
4026531840	1	57	0x93e384230c00	AF_UNIX	STREAM	-	/run/snapd.socket	36467	-	-	LISTEN	-	
4026531840	1	58	0x93e384233300	AF_UNIX	STREAM	-	/run/snapd-snap.socket	36469	-	-	LISTEN	-	
4026531840	1	59	0x93e384235500	AF_UNIX	STREAM	-	/run/uidd/request	36471	-	-	LISTEN	-	
4026531840	1	60	0x93e392f25500	AF_UNIX	STREAM	-	-	38401	/run/dbus/system_bus_socket	38512	ESTABLISHED	-	
4026531840	1	61	0x93e389d5a200	AF_UNIX	STREAM	-	/run/systemd/journal/stdout	59293	-	59292	ESTABLISHED	-	
4026531840	1	62	0x93e39307bfc0	AF_UNIX	STREAM	-	/run/systemd/journal/stdout	43976	-	42313	ESTABLISHED	-	
4026531840	1	65	0x93e394c2e600	AF_UNIX	STREAM	-	/run/systemd/journal/stdout	37342	-	39177	ESTABLISHED	-	
4026531840	770	9	0x93e380c98000	AF_NETLINK	RAW	NETLINK_ROUTE	groups:0x00000111	770	group:0x00000000	0	UNCONNECTED	-	
4026531840	770	12	0x93e396491f80	AF_INET	DGRAM	UDP	127.0.0.0.53	53	0.0.0.0.0	0	UNCONNECTED	-	
4026531840	770	13	0x93e38fe2b600	AF_INET	STREAM	TCP	127.0.0.0.53	53	0.0.0.0.0	0	LISTEN	-	
4026531840	770	14	0x93e392f21980	AF_UNIX	STREAM	-	-	38391	/run/dbus/system_bus_socket	38509	ESTABLISHED	-	
4026531840	771	1	0x93e384230880	AF_UNIX	STREAM	-	-	36350	/run/systemd/journal/stdout	35513	ESTABLISHED	-	
4026531840	771	2	0x93e384230880	AF_UNIX	STREAM	-	-	36350	/run/systemd/journal/stdout	35513	ESTABLISHED	-	
4026531840	771	3	0x93e387811980	AF_UNIX	DGRAM	-	-	37253	/run/systemd/journal/socket	26716	UNCONNECTED	-	
4026531840	771	7	0x93e387811100	AF_UNIX	DGRAM	-	-	37255	-	37256	CONNECTED	-	
4026531840	771	8	0x93e387817700	AF_UNIX	DGRAM	-	-	37256	-	37255	CONNECTED	-	
4026531840	771	9	0x93e387814840	AF_UNIX	DGRAM	-	-	37257	-	37258	CONNECTED	-	
4026531840	771	10	0x93e387813740	AF_UNIX	DGRAM	-	-	37258	-	37257	CONNECTED	-	
4026531840	771	15	0x93e387811dc0	AF_UNIX	STREAM	-	-	37341	/run/dbus/system_bus_socket	38508	ESTABLISHED	-	
4026531840	778	1	0x93e394c2aa80	AF_UNIX	STREAM	-	-	35700	/run/systemd/journal/stdout	36415	ESTABLISHED	-	
4026531840	778	2	0x93e394c2aa80	AF_UNIX	STREAM	-	-	35700	/run/systemd/journal/stdout	36415	ESTABLISHED	-	
4026531840	778	3	0x93e394c2dd80	AF_UNIX	DGRAM	-	-	35765	-	-	UNCONNECTED	-	
4026531840	778	7	0x93e394c2b740	AF_UNIX	STREAM	-	/var/run/vmware/guestServicePipe	39068	-	-	LISTEN	-	
4026531840	780	1	0x93e394c2a640	AF_UNIX	STREAM	-	-	35763	/run/systemd/journal/stdout	35764	ESTABLISHED	-	
4026531840	780	2	0x93e394c2a640	AF_UNIX	STREAM	-	-	35763	/run/systemd/journal/stdout	35764	ESTABLISHED	-	
4026531840	780	8	0x93e38fe68a00	AF_VSOCK	STREAM	-	-	-	-	-	CONNECTED	-	
4026531840	808	1	0x93e394c29100	AF_UNIX	STREAM	-	-	39177	/run/systemd/journal/stdout	37342	ESTABLISHED	-	
4026531840	808	2	0x93e394c29100	AF_UNIX	STREAM	-	-	39177	/run/systemd/journal/stdout	37342	ESTABLISHED	-	
4026531840	808	5	0x93e392f20000	AF_UNIX	STREAM	-	-	38392	/run/dbus/system_bus_socket	38510	ESTABLISHED	-	
4026531840	809	0	0x93e384231980	AF_UNIX	STREAM	-	/run/acpid.socket	36459	-	-	LISTEN	-	
4026531840	809	3	0x93e387815500	AF_UNIX	DGRAM	-	-	37406	/run/systemd/journal/dev-log	26712	UNCONNECTED	-	
4026531840	809	7	0x93e38da5c000	AF_NETLINK	RAW	NETLINK_GENERIC	groups:0x00000020	809	group:0x00000000	0	UNCONNECTED	-	
4026531840	812	1	0x93e3878150c0	AF_UNIX	STREAM	-	-	37471	/run/systemd/journal/stdout	39254	ESTABLISHED	-	
4026531840	812	2	0x93e3878150c0	AF_UNIX	STREAM	-	-	37471	/run/systemd/journal/stdout	39254	ESTABLISHED	-	
4026531840	812	3	0x93e384232ec0	AF_UNIX	STREAM	-	/run/avahi-daemon/socket	36461	-	-	LISTEN	-	
4026531840	812	4	0x93e384233740	AF_UNIX	DGRAM	-	-	36491	/run/systemd/journal/dev-log	26712	UNCONNECTED	-	
4026531840	812	5	0x93e3969cbfc0	AF_UNIX	STREAM	-	-	40433	-	40434	ESTABLISHED	-	
4026531840	812	10	0x93e3969c8000	AF_UNIX	STREAM	-	-	40438	/run/dbus/system_bus_socket	38673	ESTABLISHED	-	
4026531840	812	12	0x93e39316ad00	AF_INET	DGRAM	UDP	0.0.0.0.5353	0.0.0.0.0	0	UNCONNECTED	-		
4026531840	812	13	0x93e38abdd940	AF_INET6	DGRAM	UDP	:::5353	:::0	0	UNCONNECTED	-		
4026531840	812	14	0x93e39316a800	AF_INET	DGRAM	UDP	0.0.0.0.42869	0.0.0.0.0	0	UNCONNECTED	-		
4026531840	812	15	0x93e38abdd400	AF_INET6	DGRAM	UDP	:::52273	:::0	0	UNCONNECTED	-		
4026531840	812	16	0x93e388148000	AF_NETLINK	DGRAM	NETLINK_ROUTE	groups:0x00000111	812	group:0x00000000	0	UNCONNECTED	-	
4026531840	814	1	0x93e387816a40	AF_UNIX	STREAM	-	-	37536	/run/systemd/journal/stdout	39321	ESTABLISHED	-	
4026531840	814	2	0x93e387816a40	AF_UNIX	STREAM	-	-	37536	/run/systemd/journal/stdout	39321	ESTABLISHED	-	
4026531840	814	4	0x93e387812a80	AF_UNIX	DGRAM	-	-	37538	/run/systemd/notify	26688	UNCONNECTED	-	
4026531840	814	5	0x93e382fe6c00	AF_BLUETOOTH	RAW	-	-	-	-	-	UNCONNECTED	-	
4026531840	814	6	0x93e387812200	AF_UNIX	DGRAM	-	-	37540	/run/systemd/journal/dev-log	26712	UNCONNECTED	-	
4026531840	814	7	0x93e387812640	AF_UNIX	STREAM	-	-	37560	/run/dbus/system_bus_socket	38511	ESTABLISHED	-	
4026531840	814	8	0x93e382fe4800	AF_BLUETOOTH	RAW	-	-	-	-	-	UNCONNECTED	-	
4026531840	814	9	0x93e382fe7c00	AF_BLUETOOTH	SEQPACKET	-	-	-	-	-	UNCONNECTED	-	

Plugin: *linux.tty\_check.tty\_check* : Checks tty devices for hooks [3] .

```
$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.tty_check.tty_check
```

```
rusheel@ubuntu:~/volatility3$ sudo python3 vol.py -f ~/LiME/src/ubuntu.lime linux.tty_check.tty_check
Volatility 3 Framework 2.5.2
Progress: 100.00 Stacking attempts finished
Name Address Module Symbol
tty2 0xffff887eea70 __kernel__ n_tty_receive_buf
tty6 0xffff887eea70 __kernel__ n_tty_receive_buf
```

## References:

- [1]. <https://medium.com/@alirezataghikhani1998/build-a-custom-linux-profile-for-volatility3-640afdaf161b>.
- [2]. <https://opensource.com/article/21/4/linux-memory-forensics>
- [3]. <https://github.com/volatilityfoundation/volatility3>
- [4]. <https://medium.com/mii-cybersec/memory-forensic-linux-kernel-confusion-8f711a4ed4d1>
- [5]. <https://fahriguresci.com/create-specific-volatility-profile-and-symbol-table/>
- [6]. <https://github.com/504ensicsLabs/LiME>