FORENSICS
LAB SERIES

Lab 5: Obtaining & Analyzing Memory

Material in this Lab Aligns to the Following Certification Domains/Objectives	
GIAC Certified Forensics Examiner (GCFE) Domains	Certified Cyber Forensics Professional (CCFP) Objectives
2: Digital Forensics Fundamentals	4: Digital Forensics

Document Version: 2016-08-17

Contents

Introduction

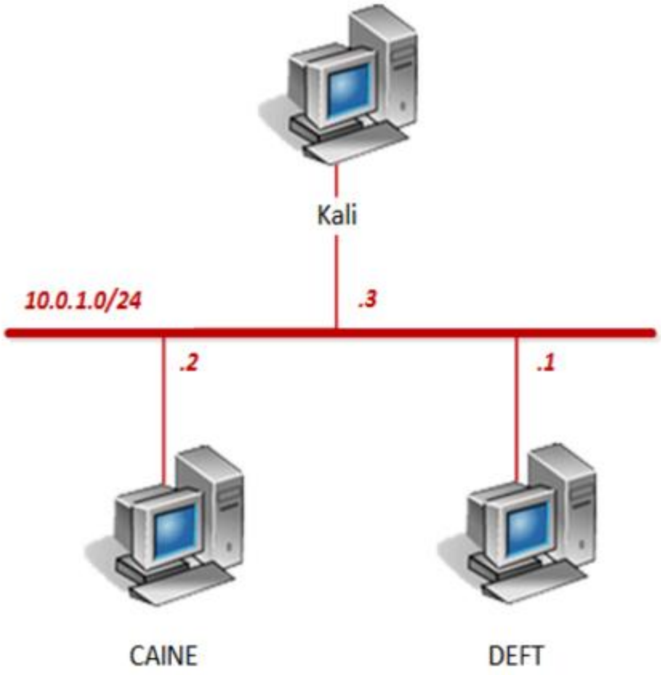
This lab will demonstrate live forensics on a Linux machine using the LiME Linux memory extractor tool, along with a Volatility tool to analyze the memory capture. Many artifacts exist in RAM and can be extracted directly from a capture.

Objective

In this lab, you will be conducting forensic practices using various tools. You will be performing the following tasks:

1. Extracting Live Memory
2. Create dcfldd Image Acquisition

Pod Topology



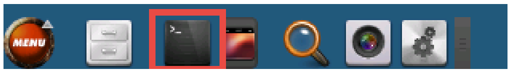
Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
DEFT	10.0.1.1	deft	password
CAINE	10.0.1.2	caine	
Kali	10.0.1.3	root	toor

1 Extracting Live Memory

1. Click on the **CAINE** graphic on the *topology page* to open the VM.
2. Open a new terminal by clicking on the **MATE Terminal** icon located on the bottom panel.

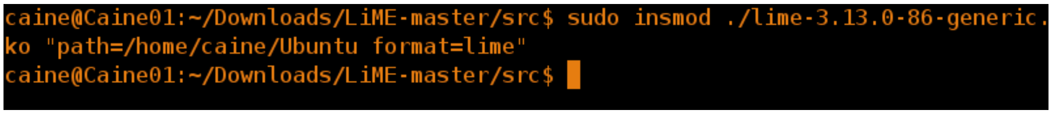


3. Using the terminal, change to the **/home/caine/Downloads/LiME-master/src** directory by entering the command below.

```
cd /home/caine/Downloads/LiME-master/src
```

4. Enter the command below to install LiME into the Kernel of the operating system so that it will be ready to extract live memory captures.

```
sudo insmod ./lime-3.13.0-86-generic.ko “path=/home/caine/Ubuntu
format=lime”
```



```
caine@Caine01:~/Downloads/LiME-master/src$ sudo insmod ./lime-3.13.0-86-generic.
ko "path=/home/caine/Ubuntu format=lime"
caine@Caine01:~/Downloads/LiME-master/src$
```

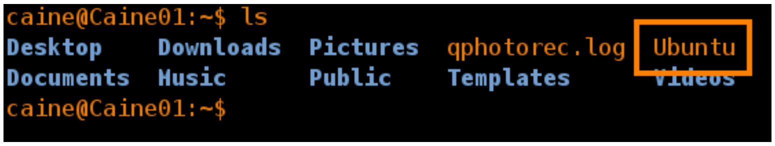
There may be a slight delay, wait 1 minute for the command to execute.

5. Change to the **/home/caine** directory by entering the command below.

```
cd
```

6. Enter the command below to list the files in the current directory and notice the *Ubuntu* memory dump.

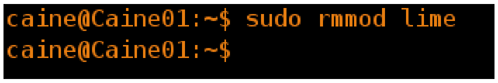
```
ls
```



```
caine@Caine01:~$ ls
Desktop    Downloads  Pictures  qphotorec.log  Ubuntu
Documents  Music      Public    Templates      Videos
caine@Caine01:~$
```

7. Remove the *LiME* module from the kernel. Enter the command below.

```
sudo rmmod lime
```

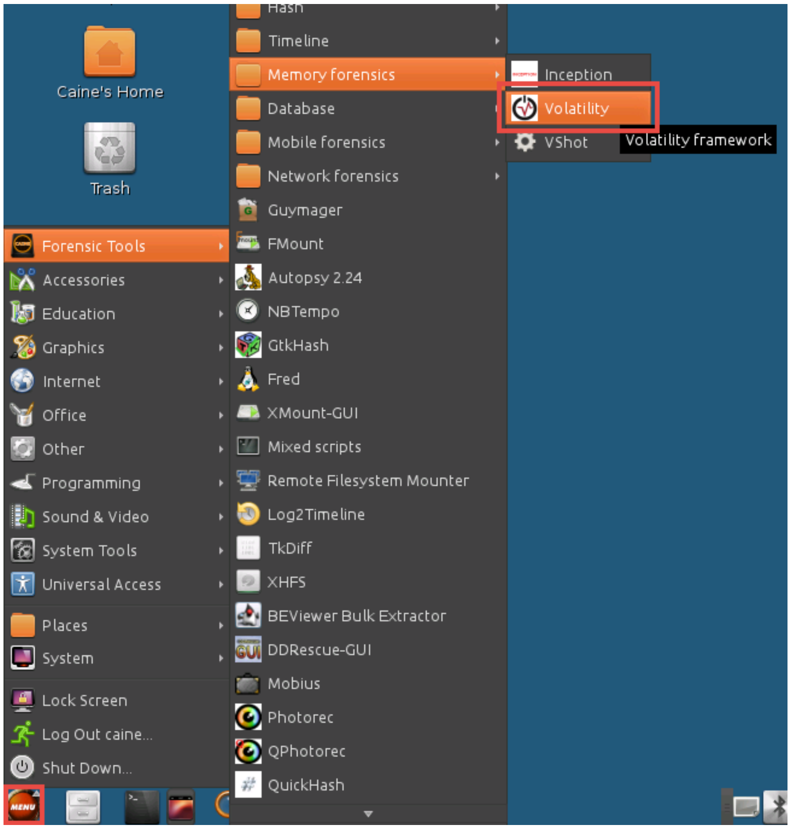


```
caine@Caine01:~$ sudo rmmod lime
caine@Caine01:~$
```

8. Close the terminal window.

2 Create dcfldd Image Acquisition

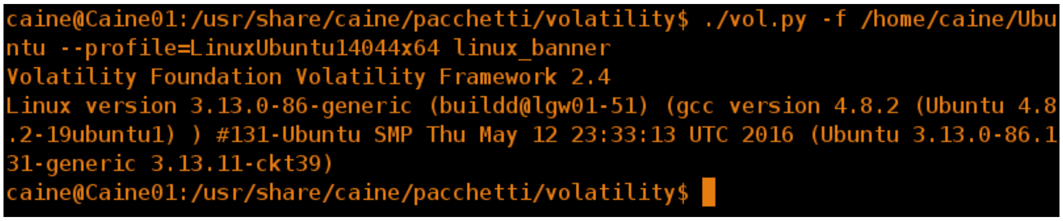
1. Navigate to **Start Menu > Forensic Tools > Memory forensics > Volatility** to launch the memory analyzer tool named *Volatility*.



2. Notice a new terminal window appears. Briefly review the *Volatility* command options and press the **spacebar** key repeatedly until a prompt is given. The prompt should show the current directory; */usr/share/caine/pacchetti/volatility$.*

3. Initiate a simple check of the version of Linux from the memory dump acquired from *Task 1*. Enter the command below into the same terminal window.

```
./vol.py -f /home/caine/Ubuntu --profile=LinuxUbuntu14044x64 linux_banner
```



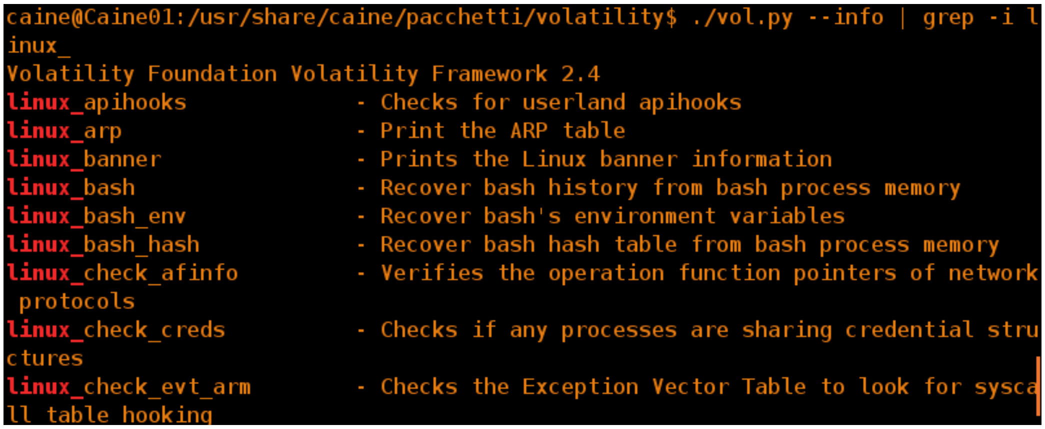
```
caine@Caine01:/usr/share/caine/pacchetti/volatility$ ./vol.py -f /home/caine/Ubu
ntu --profile=LinuxUbuntu14044x64 linux_banner
Volatility Foundation Volatility Framework 2.4
Linux version 3.13.0-86-generic (buildd@lgw01-51) (gcc version 4.8.2 (Ubuntu 4.8
.2-19ubuntu1) ) #131-Ubuntu SMP Thu May 12 23:33:13 UTC 2016 (Ubuntu 3.13.0-86.1
31-generic 3.13.11-ckt39)
caine@Caine01:/usr/share/caine/pacchetti/volatility$ 
```

Command Breakdown:

-f = memory dump file name
--profile = profile for version of OS that is being analyzed

4. Notice the memory that is being analyzed belongs to an *Ubuntu 3.13-0.86-generic* kernel. View all the *Linux* modules volatility has to analyze the image. Enter the command below.

```
./vol.py --info | grep -i linux_
```

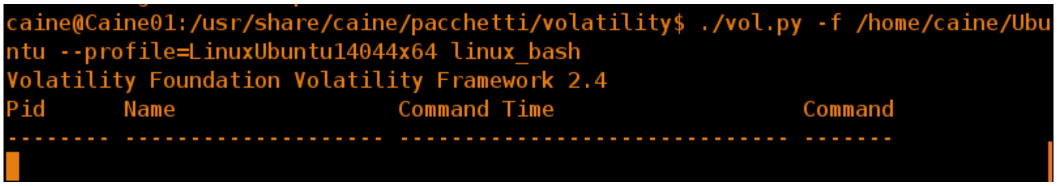


```
caine@Caine01:/usr/share/caine/pacchetti/volatility$ ./vol.py --info | grep -i l
inux_
Volatility Foundation Volatility Framework 2.4
linux_apihooks              - Checks for userland apihooks
linux_arp                   - Print the ARP table
linux_banner                - Prints the Linux banner information
linux_bash                  - Recover bash history from bash process memory
linux_bash_env              - Recover bash's environment variables
linux_bash_hash             - Recover bash hash table from bash process memory
linux_check_afinfo          - Verifies the operation function pointers of network
 protocols
linux_check_creds           - Checks if any processes are sharing credential stru
ctures
linux_check_evt_arm         - Checks the Exception Vector Table to look for sysca
ll table hooking
```

Notice how several modules are present that can be applied to the image for analysis.

5. View the bash history from the acquired memory dump image. Enter the command below.

```
./vol.py -f /home/caine/Ubuntu --profile=LinuxUbuntu14044x64 linux_bash
```

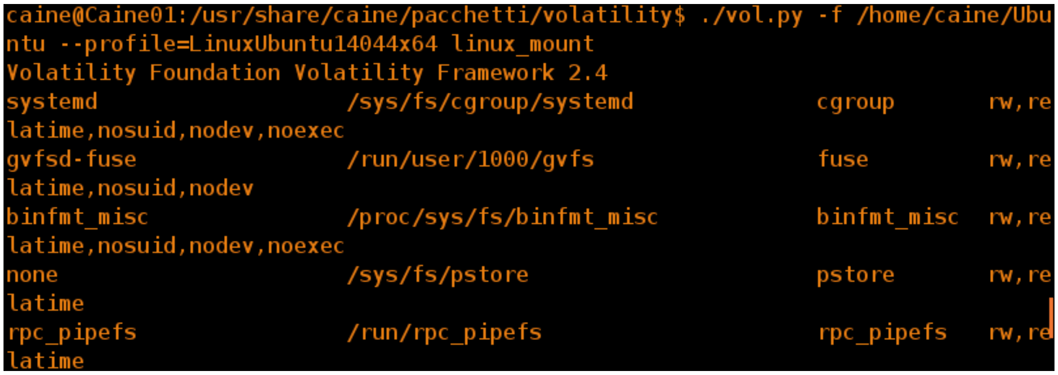


```
caine@Caine01:/usr/share/caine/pacchetti/volatility$ ./vol.py -f /home/caine/Ubu
ntu --profile=LinuxUbuntu14044x64 linux_bash
Volatility Foundation Volatility Framework 2.4
Pid      Name                 Command Time                   Command
-------- -------------------- ------------------------------ -------
```

The output will vary depending on set of commands were used during the time of capture.

6. View what has been mounted, based on analyzing the memory dump image. Enter the command below.

```
./vol.py -f /home/caine/Ubuntu --profile=LinuxUbuntu14044x64 linux_mount
```

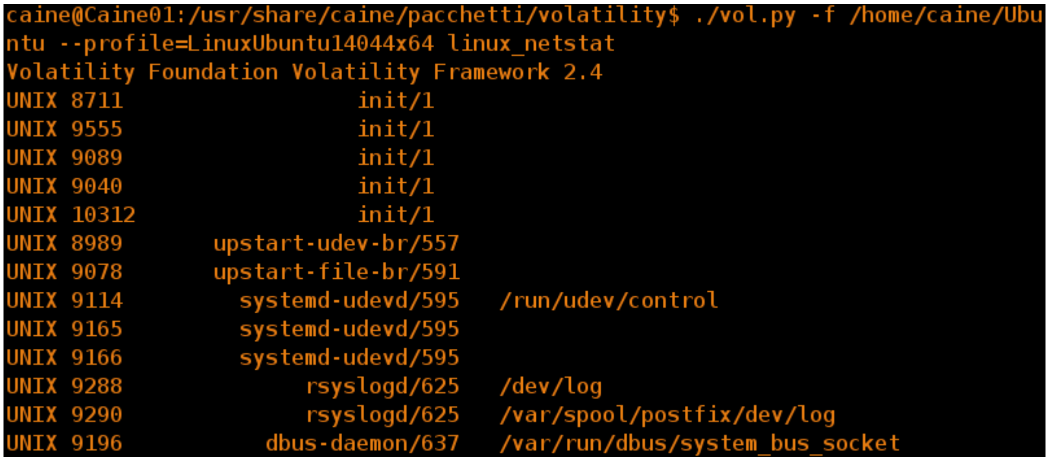


```
caine@Caine01:/usr/share/caine/pacchetti/volatility$ ./vol.py -f /home/caine/Ubu
ntu --profile=LinuxUbuntu14044x64 linux_mount
Volatility Foundation Volatility Framework 2.4
systemd                   /sys/fs/cgroup/systemd              cgroup       rw,re
latime,nosuid,nodev,noexec
gvfsd-fuse                /run/user/1000/gvfs                 fuse         rw,re
latime,nosuid,nodev
binfmt_misc               /proc/sys/fs/binfmt_misc            binfmt_misc  rw,re
latime,nosuid,nodev,noexec
none                      /sys/fs/pstore                      pstore       rw,re
latime
rpc_pipefs                /run/rpc_pipefs                     rpc_pipefs   rw,re
latime
```

These are all the mounted file systems.

7. View the network connections from analyzing the same memory dump image. Enter the command below.

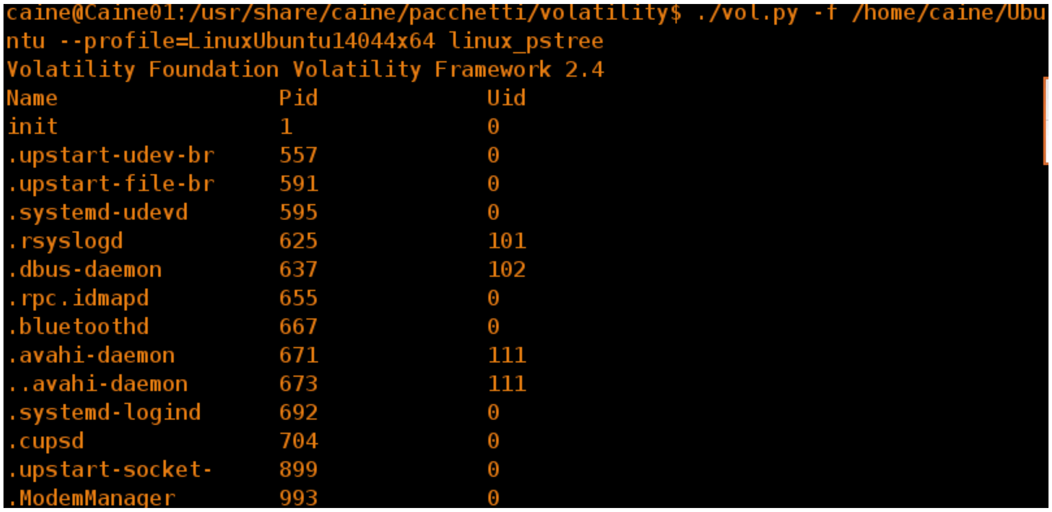
```
./vol.py -f /home/caine/Ubuntu --profile=LinuxUbuntu14044x64
linux_netstat
```



```
caine@Caine01:/usr/share/caine/pacchetti/volatility$ ./vol.py -f /home/caine/Ubu
ntu --profile=LinuxUbuntu14044x64 linux_netstat
Volatility Foundation Volatility Framework 2.4
UNIX 8711                  init/1
UNIX 9555                  init/1
UNIX 9089                  init/1
UNIX 9040                  init/1
UNIX 10312                 init/1
UNIX 8989       upstart-udev-br/557
UNIX 9078       upstart-file-br/591
UNIX 9114         systemd-udevd/595    /run/udev/control
UNIX 9165         systemd-udevd/595
UNIX 9166         systemd-udevd/595
UNIX 9288              rsyslogd/625    /dev/log
UNIX 9290              rsyslogd/625    /var/spool/postfix/dev/log
UNIX 9196           dbus-daemon/637    /var/run/dbus/system_bus_socket
```

8. View the processes that were running the system at the time of the memory capture. Enter the command below.

```
./vol.py -f /home/caine/Ubuntu --profile=LinuxUbuntu14044x64 linux_pstree
```



```
caine@Caine01:/usr/share/caine/pacchetti/volatility$ ./vol.py -f /home/caine/Ubu
ntu --profile=LinuxUbuntu14044x64 linux_pstree
Volatility Foundation Volatility Framework 2.4
Name                    Pid             Uid
init                    1               0
.upstart-udev-br        557             0
.upstart-file-br        591             0
.systemd-udevd          595             0
.rsyslogd               625             101
.dbus-daemon            637             102
.rpc.idmapd             655             0
.bluetoothd             667             0
.avahi-daemon           671             111
..avahi-daemon          673             111
.systemd-logind         692             0
.cupsd                  704             0
.upstart-socket-        899             0
.ModemManager           993             0
```

9. Close all **PC Viewers** and end the reservation to complete the lab.