Module 07: Linux and Mac Forensics

Lab Scenario

The cyber police department of a US district received information about an online scam occurring in a particular cybercafé of that district. They searched that place and seized computers that were running on Linux and Mac operating systems (OSes). Jason, a forensic expert, was appointed to examine these Linux and Mac systems and gather artifacts related to the case.

In order to analyze Linux and Mac OSes, you must be able to collect and analyze evidence from victims' or attackers' systems. The attacker can manipulate the system configuration and delete the attack data from victims' systems. As an investigator, you must be aware of Linux and Mac system configurations and their file systems to conduct forensic investigation.

Lab Objectives

The objective of this lab is to provide expert knowledge on finding pieces of evidence from Linux OS. Accomplishing this task will include:

- Performing memory forensics on Linux machine
- Recovering data from a Linux RAM dump

Overview of Linux and Mac Forensics

Linux and Mac Forensics refers to the investigation of cyber-crimes involving Linux and Mac machines. To find artifacts pertaining to cyber-crime on Linux and Mac systems, investigators must have knowledge of the Linux file system as well as various directories and commands through which they can find evidentiary data.

Lab Tasks

The following are the recommended labs that will assist you in Linux Forensics:

- Forensic investigation on a Linux memory dump
- Recovering data from a Linux memory dump

Lab 1: Forensic Investigation on a Linux Memory Dump

Lab Scenario

A reputed product-based technology firm that was about to launch its new artificial intelligence-driven product has discovered that confidential data pertaining to the

development and marketing strategy of the product was breached and deleted by unknown persons. The firm uses Linux workstations and consulted an expert forensic investigator to determine how the data breach was performed and the source of the attack as well as to recover the deleted data. The forensic investigator must perform volatile memory acquisition on a Linux machine and examine the memory dumps to find any form of malicious activity and recover the deleted/lost data.

As a forensic expert, you should know how to perform forensic investigation on memory dump acquired from a Linux machine.

Lab Objectives

Analyzing the RAM dump of a system helps investigators retrieve valuable evidence pertaining to a case of cyber-crime.

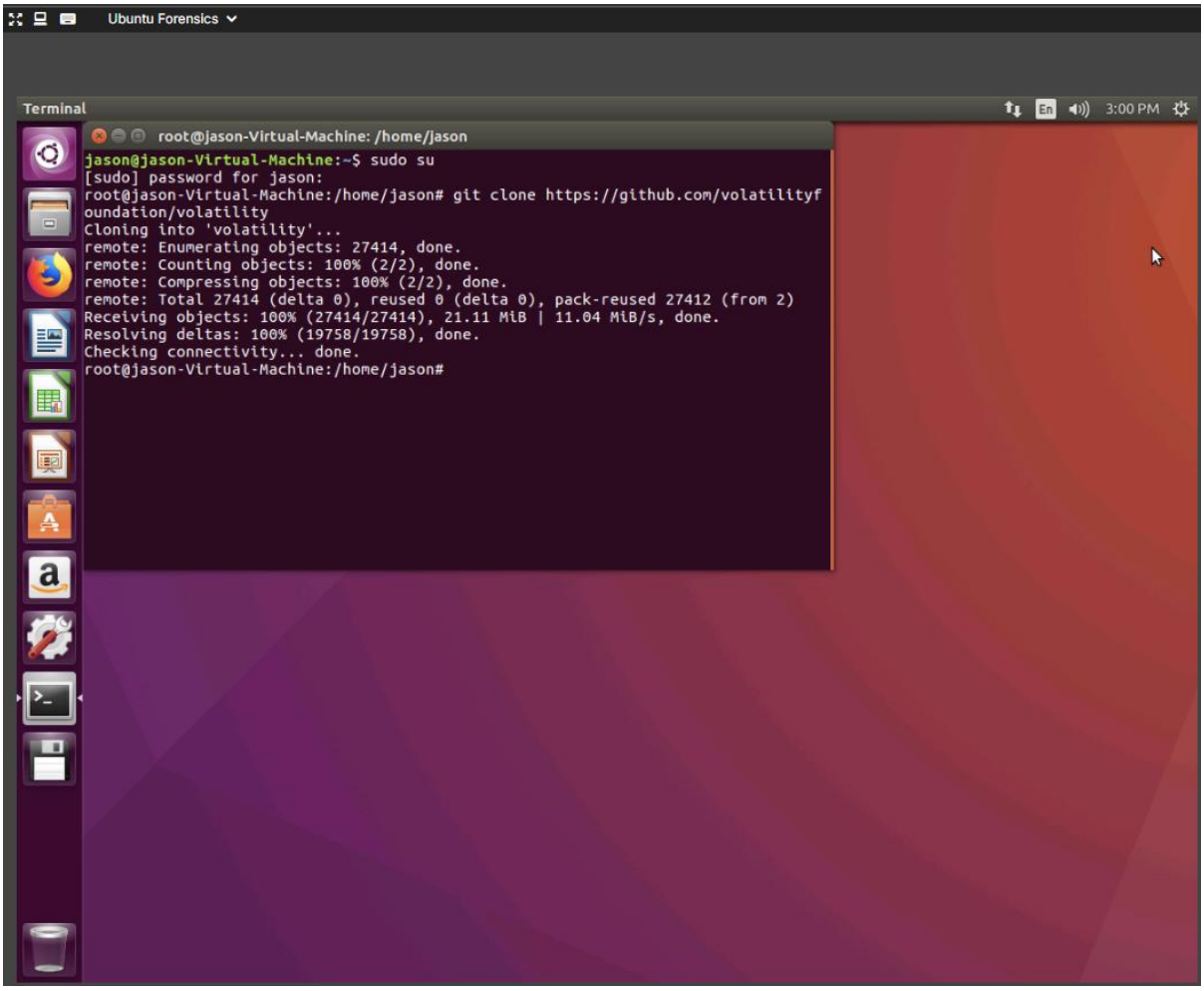
The objective of this lab is as follows:

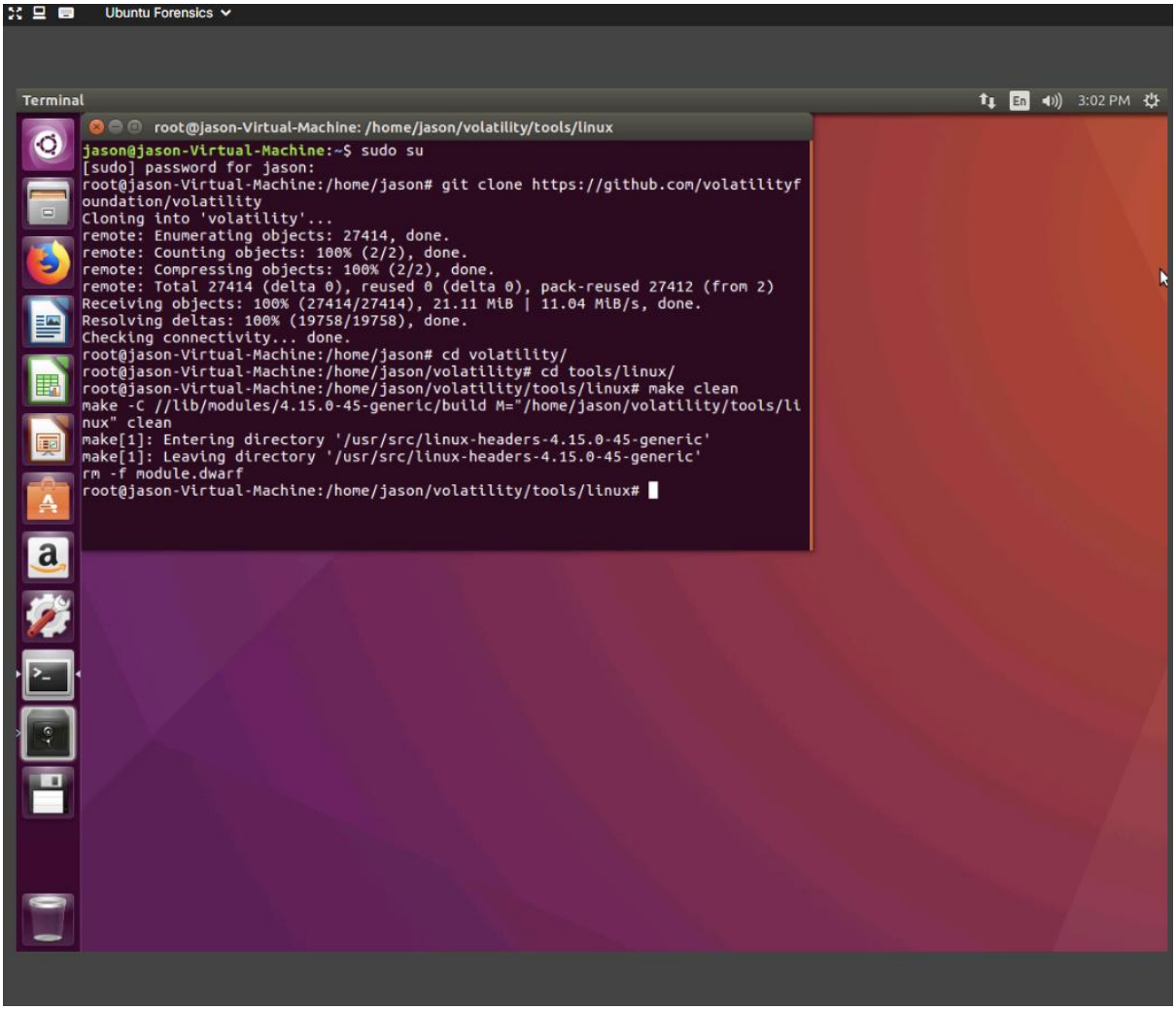
- Creating a Linux kernel profile for memory analysis
- Examining a RAM dump for potential evidence

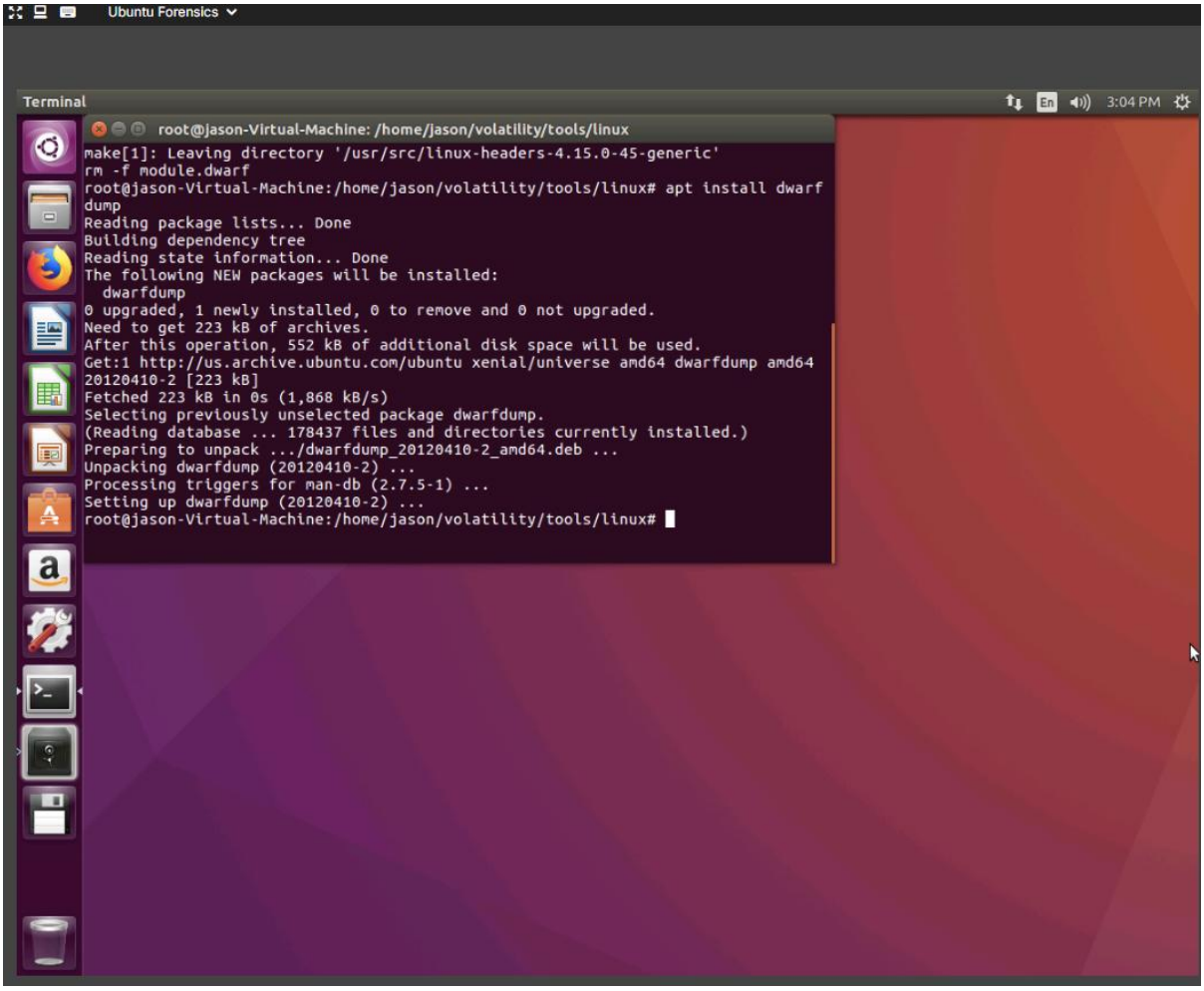
Overview of the Lab

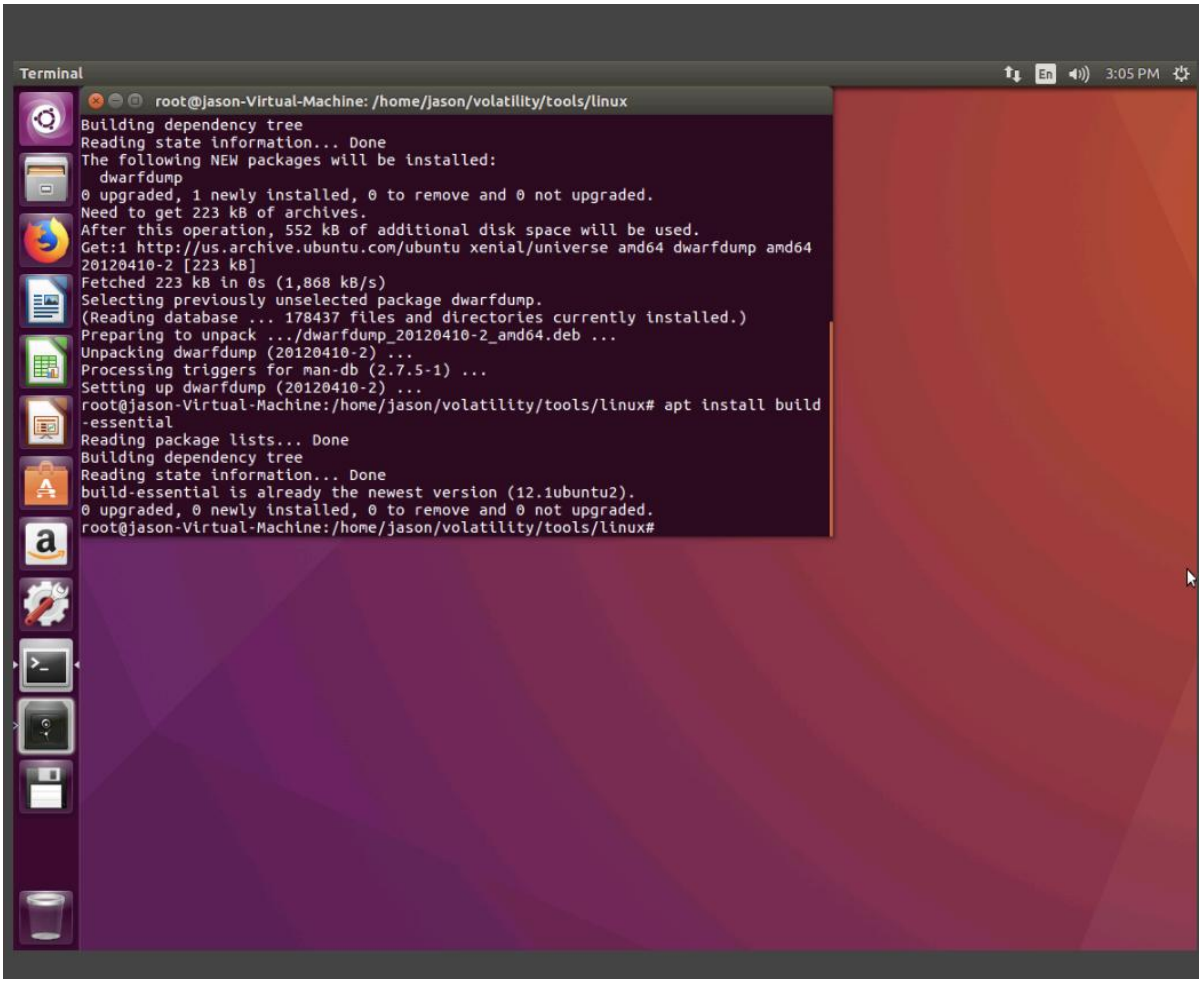
This lab familiarizes you with building Linux kernel profiles for memory forensics and examining the RAM dump acquired from a Linux machine using the Volatility Framework to gather the required evidence pertaining to an incidence of cyber-crime.

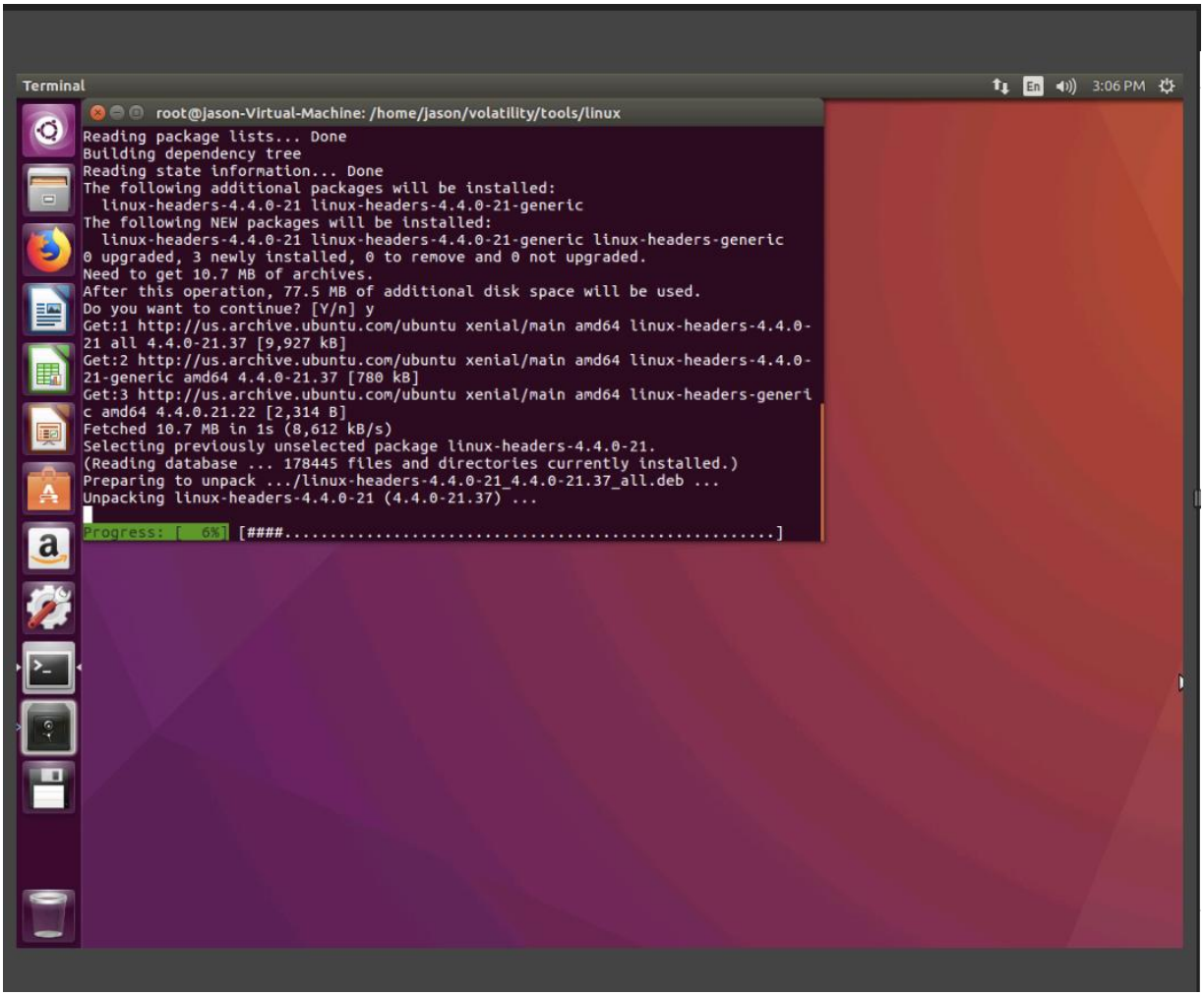
In this lab, we are going to examine a Linux RAM dump on Volatility and extract information that can be useful for investigation. However, to examine this file, we need to initially create a Linux Kernel profile, which allows the Volatility Framework to locate and parse critical information.

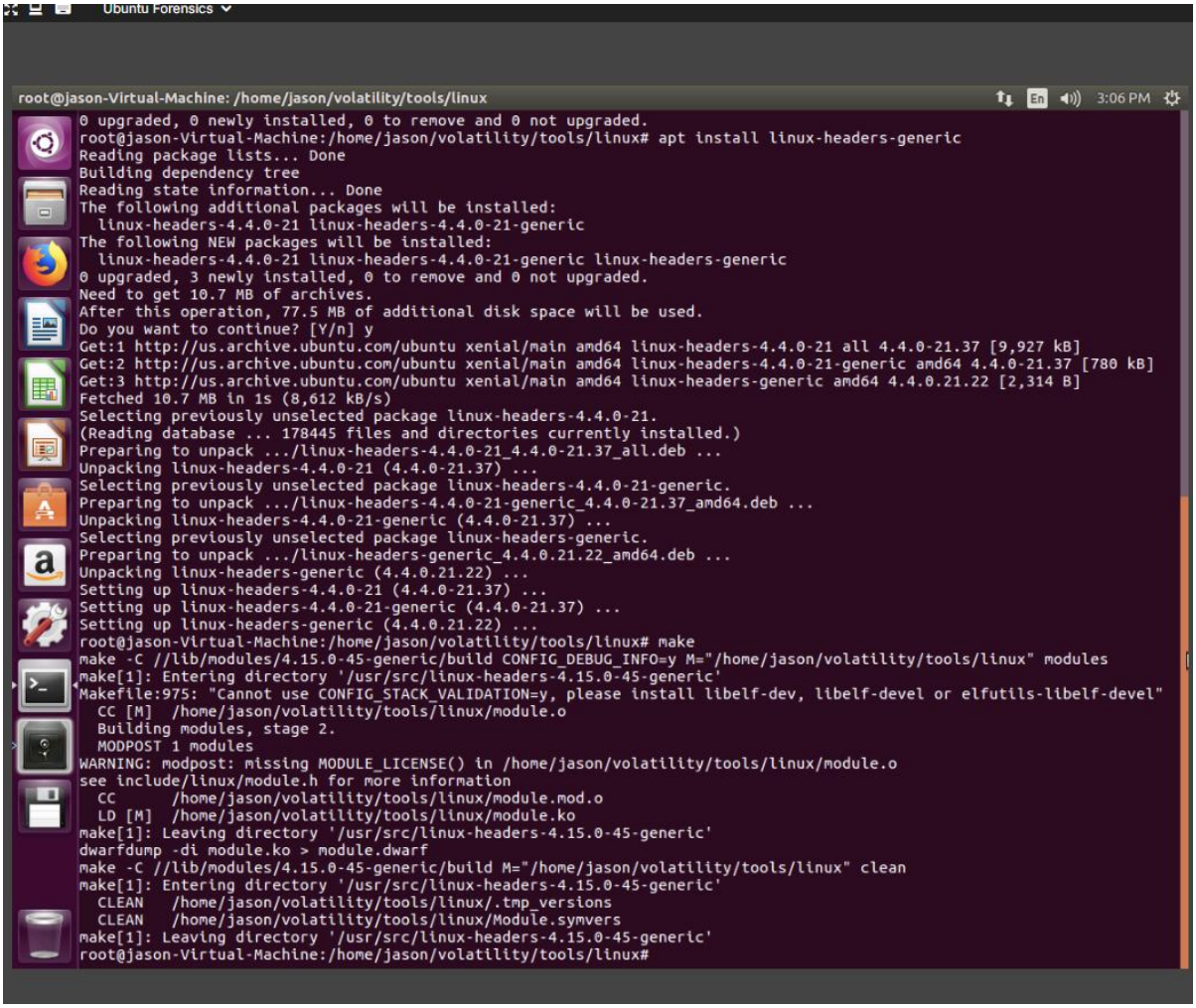

Ubuntu Forensics
Terminal
En
3:00 PM
root@jason-Virtual-Machine: /home/jason
jason@jason-Virtual-Machine:~$ sudo su
[sudo] password for jason:
root@jason-Virtual-Machine:/home/jason# git clone https://github.com/volatilityfoundation/volatility
Cloning into 'volatility'...
remote: Enumerating objects: 27414, done.
remote: Counting objects: 100% (2/2), done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 27414 (delta 0), reused 0 (delta 0), pack-reused 27412 (from 2)
Receiving objects: 100% (27414/27414), 21.11 MiB | 11.04 MiB/s, done.
Resolving deltas: 100% (19758/19758), done.
Checking connectivity... done.
root@jason-Virtual-Machine:/home/jason#

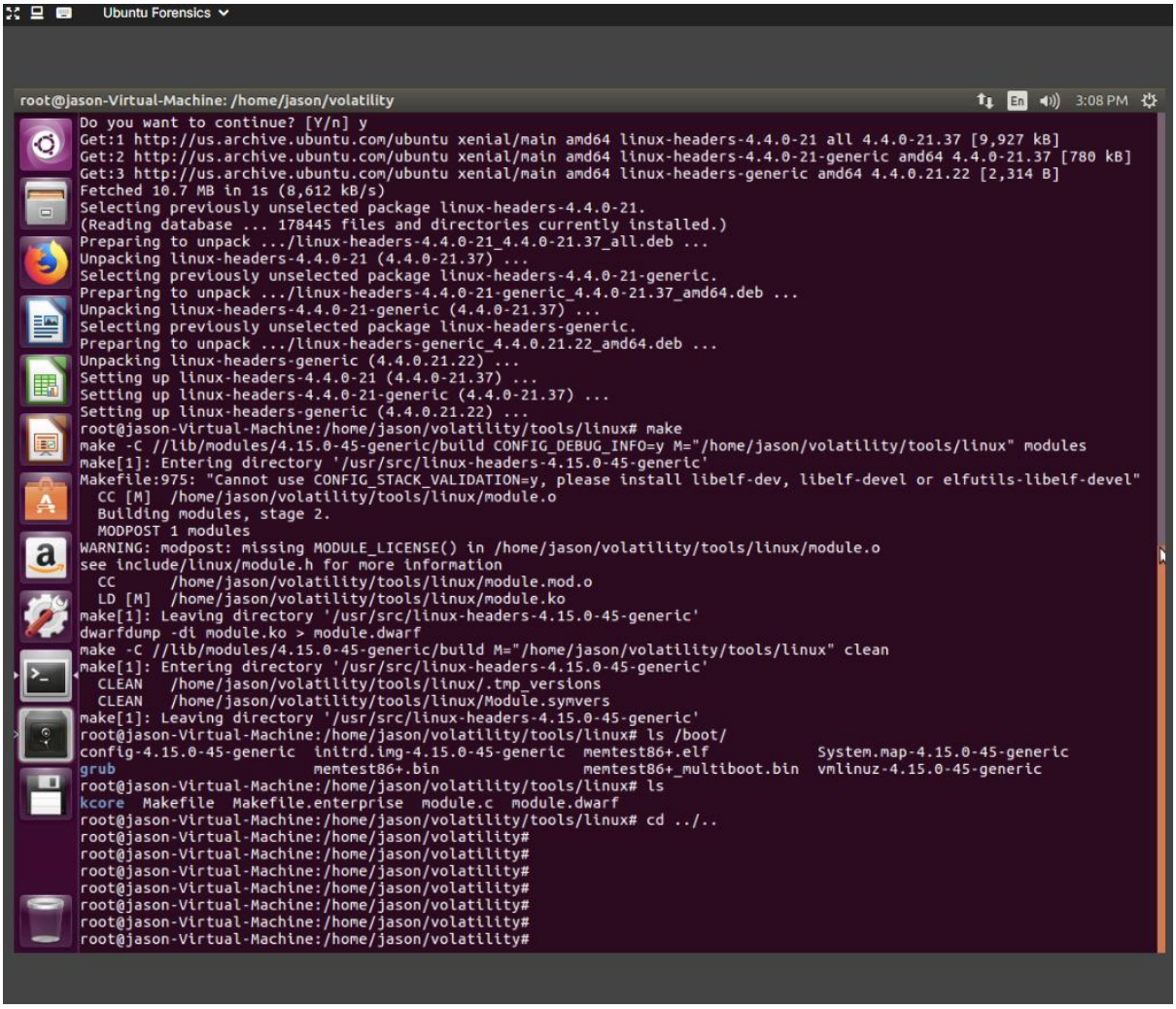

Ubuntu Forensics
Terminal
En
3:02 PM
root@jason-Virtual-Machine: /home/jason/volatility/tools/linux
jason@jason-Virtual-Machine:~$ sudo su
[sudo] password for jason:
root@jason-Virtual-Machine:/home/jason# git clone https://github.com/volatilityfoundation/volatility
Cloning into 'volatility'...
remote: Enumerating objects: 27414, done.
remote: Counting objects: 100% (2/2), done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 27414 (delta 0), reused 0 (delta 0), pack-reused 27412 (from 2)
Receiving objects: 100% (27414/27414), 21.11 MiB | 11.04 MiB/s, done.
Resolving deltas: 100% (19758/19758), done.
Checking connectivity... done.
root@jason-Virtual-Machine:/home/jason# cd volatility/
root@jason-Virtual-Machine:/home/jason/volatility# cd tools/linux/
root@jason-Virtual-Machine:/home/jason/volatility/tools/linux# make clean
make -C //lib/modules/4.15.0-45-generic/build M="/home/jason/volatility/tools/linux" clean
make[1]: Entering directory '/usr/src/linux-headers-4.15.0-45-generic'
make[1]: Leaving directory '/usr/src/linux-headers-4.15.0-45-generic'
rm -f module.dwarf
root@jason-Virtual-Machine:/home/jason/volatility/tools/linux#

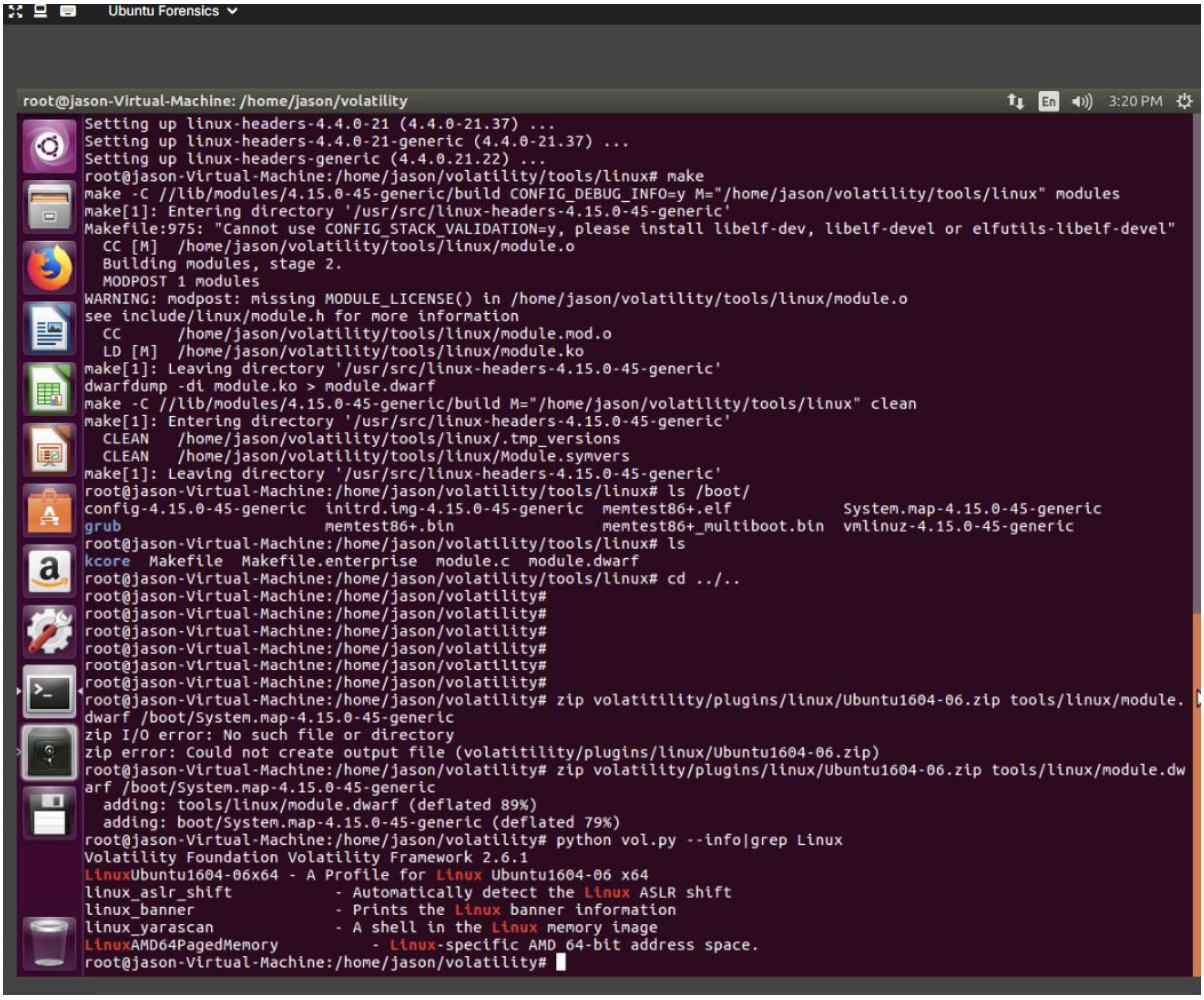

Ubuntu Forensics
Terminal
En
3:04 PM
root@jason-Virtual-Machine: /home/jason/volatility/tools/linux
make[1]: Leaving directory '/usr/src/linux-headers-4.15.0-45-generic'
rm -f module.dwarf
root@jason-Virtual-Machine:/home/jason/volatility/tools/linux# apt install dwarf
dump
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
dwarfdump
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 223 kB of archives.
After this operation, 552 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu xenial/universe amd64 dwarfdump amd64
20120410-2 [223 kB]
Fetched 223 kB in 0s (1,868 kB/s)
Selecting previously unselected package dwarfdump.
(Reading database ... 178437 files and directories currently installed.)
Preparing to unpack .../dwarfdump_20120410-2_amd64.deb ...
Unpacking dwarfdump (20120410-2) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up dwarfdump (20120410-2) ...
root@jason-Virtual-Machine:/home/jason/volatility/tools/linux#

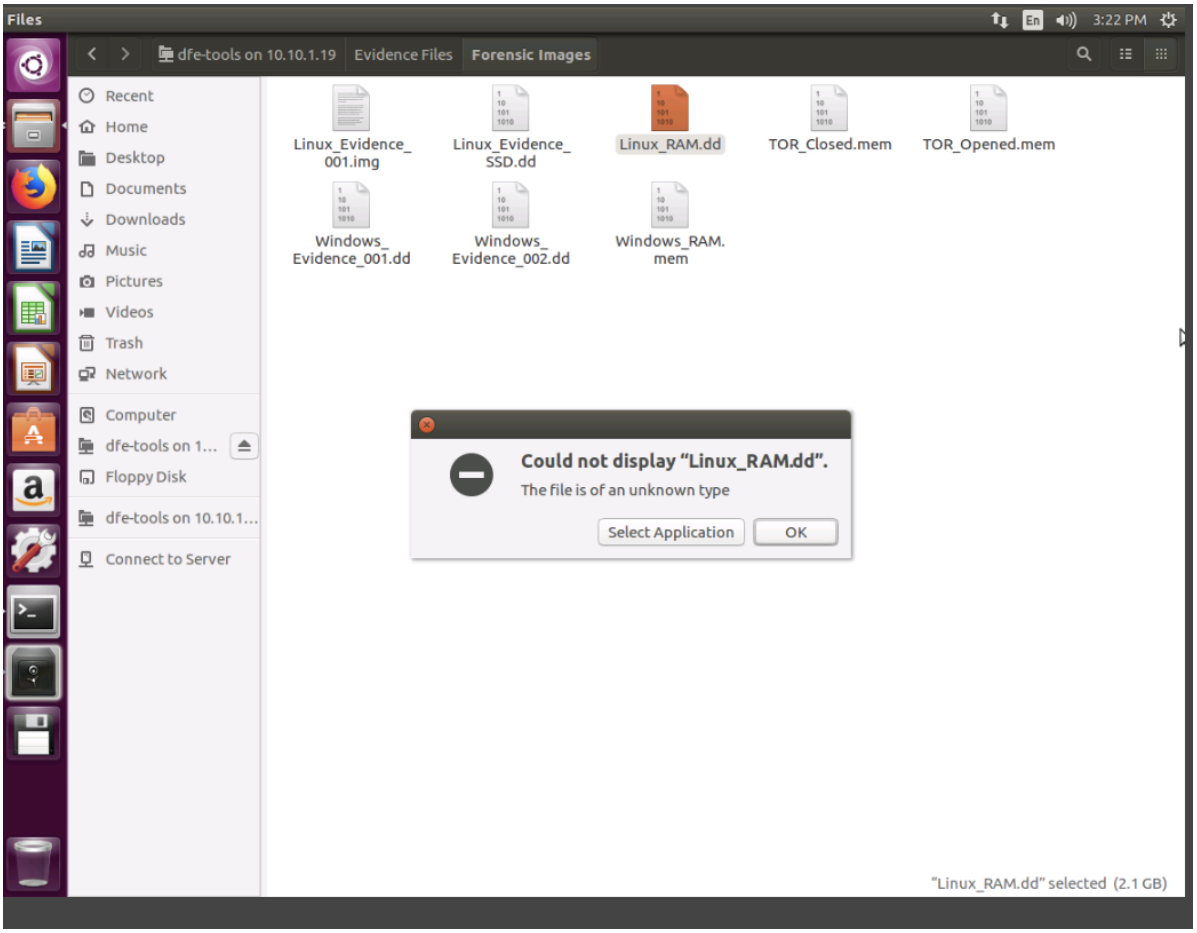

Terminal
En
3:05 PM
root@jason-Virtual-Machine: /home/jason/volatility/tools/linux
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
dwarfdump
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 223 kB of archives.
After this operation, 552 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu xenial/universe amd64 dwarfdump amd64
20120410-2 [223 kB]
Fetched 223 kB in 0s (1,868 kB/s)
Selecting previously unselected package dwarfdump.
(Reading database ... 178437 files and directories currently installed.)
Preparing to unpack .../dwarfdump_20120410-2_amd64.deb ...
Unpacking dwarfdump (20120410-2) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up dwarfdump (20120410-2) ...
root@jason-Virtual-Machine:/home/jason/volatility/tools/linux# apt install build
-essential
Reading package lists... Done
Building dependency tree
Reading state information... Done
build-essential is already the newest version (12.1ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@jason-Virtual-Machine:/home/jason/volatility/tools/linux#

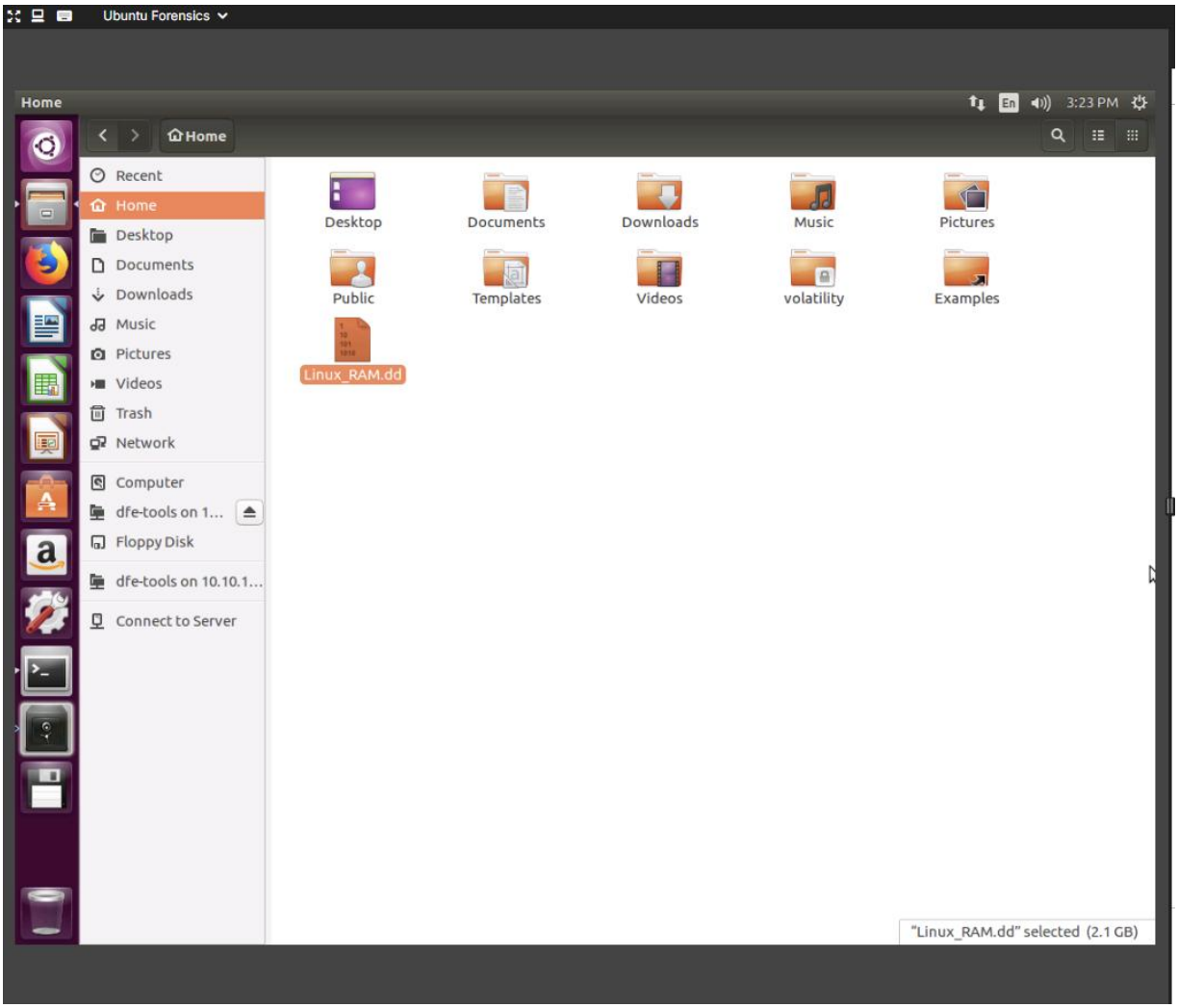

Terminal
En
3:06 PM
root@jason-Virtual-Machine: /home/jason/volatility/tools/linux
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
linux-headers-4.4.0-21 linux-headers-4.4.0-21-generic
The following NEW packages will be installed:
linux-headers-4.4.0-21 linux-headers-4.4.0-21-generic linux-headers-generic
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 10.7 MB of archives.
After this operation, 77.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 linux-headers-4.4.0-21 all 4.4.0-21.37 [9,927 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 linux-headers-4.4.0-21-generic amd64 4.4.0-21.37 [780 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 linux-headers-generic amd64 4.4.0.21.22 [2,314 B]
Fetched 10.7 MB in 1s (8,612 kB/s)
Selecting previously unselected package linux-headers-4.4.0-21.
(Reading database ... 178445 files and directories currently installed.)
Preparing to unpack .../linux-headers-4.4.0-21_4.4.0-21.37_all.deb ...
Unpacking linux-headers-4.4.0-21 (4.4.0-21.37) ...
Progress: [6%] [####.....]

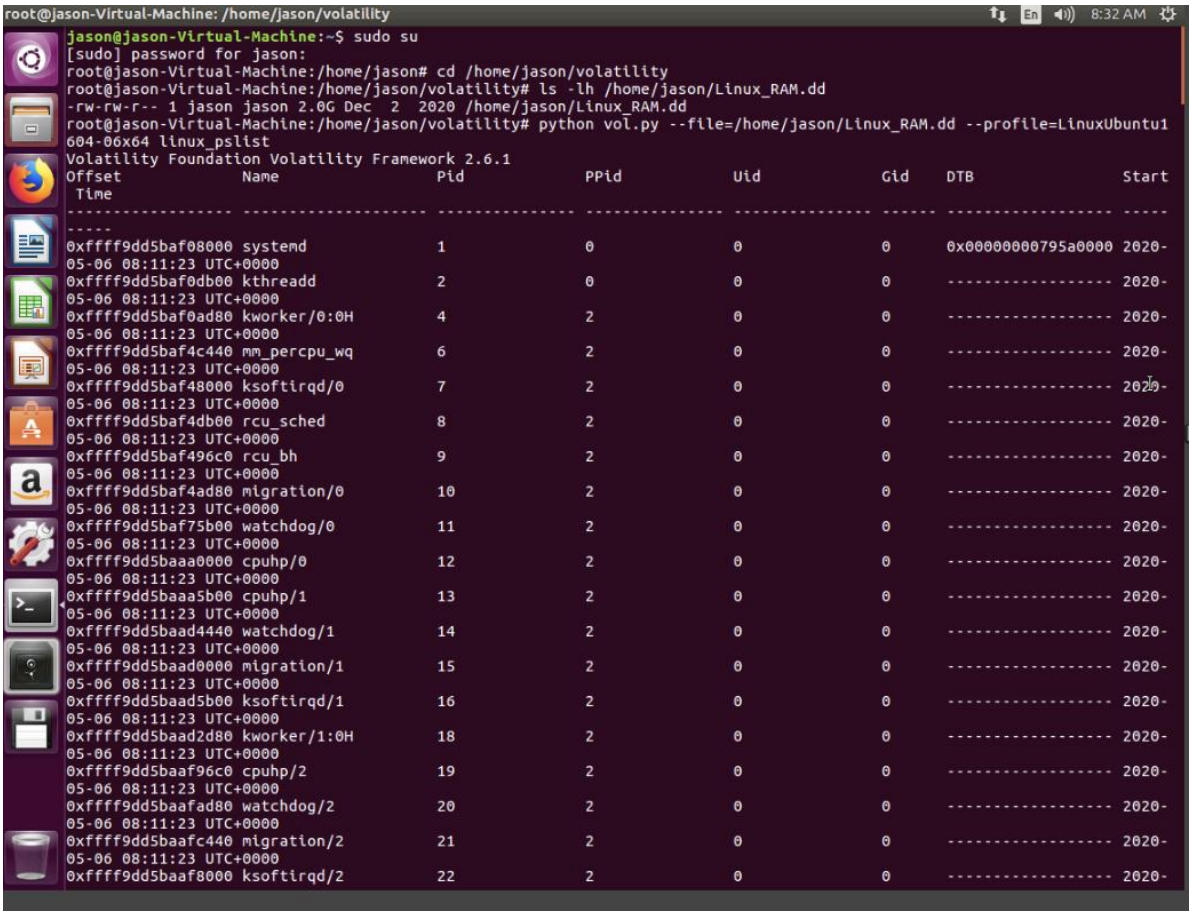

Ubuntu Forensics
root@jason-Virtual-Machine: /home/jason/volatility/tools/linux
En
3:06 PM
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@jason-Virtual-Machine:/home/jason/volatility/tools/linux# apt install linux-headers-generic
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
linux-headers-4.4.0-21 linux-headers-4.4.0-21-generic
The following NEW packages will be installed:
linux-headers-4.4.0-21 linux-headers-4.4.0-21-generic linux-headers-generic
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 10.7 MB of archives.
After this operation, 77.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 linux-headers-4.4.0-21 all 4.4.0-21.37 [9,927 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 linux-headers-4.4.0-21-generic amd64 4.4.0-21.37 [780 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 linux-headers-generic amd64 4.4.0.21.22 [2,314 B]
Fetched 10.7 MB in 1s (8,612 kB/s)
Selecting previously unselected package linux-headers-4.4.0-21.
(Reading database ... 178445 files and directories currently installed.)
Preparing to unpack .../linux-headers-4.4.0-21_4.4.0-21.37_all.deb ...
Unpacking linux-headers-4.4.0-21 (4.4.0-21.37) ...
Selecting previously unselected package linux-headers-4.4.0-21-generic.
Preparing to unpack .../linux-headers-4.4.0-21-generic_4.4.0-21.37_amd64.deb ...
Unpacking linux-headers-4.4.0-21-generic (4.4.0-21.37) ...
Selecting previously unselected package linux-headers-generic.
Preparing to unpack .../linux-headers-generic_4.4.0.21.22_amd64.deb ...
Unpacking linux-headers-generic (4.4.0.21.22) ...
Setting up linux-headers-4.4.0-21 (4.4.0-21.37) ...
Setting up linux-headers-4.4.0-21-generic (4.4.0-21.37) ...
Setting up linux-headers-generic (4.4.0.21.22) ...
root@jason-Virtual-Machine:/home/jason/volatility/tools/linux# make
make -C //lib/modules/4.15.0-45-generic/build CONFIG_DEBUG_INFO=y M="/home/jason/volatility/tools/linux" modules
make[1]: Entering directory '/usr/src/linux-headers-4.15.0-45-generic'
Makefile:975: "Cannot use CONFIG_STACK_VALIDATION=y, please install libelf-dev, libelf-devel or elfutils-libelf-devel"
CC [M] /home/jason/volatility/tools/linux/module.o
Building modules, stage 2.
MODPOST 1 modules
WARNING: modpost: missing MODULE_LICENSE() in /home/jason/volatility/tools/linux/module.o
see include/linux/module.h for more information
CC /home/jason/volatility/tools/linux/module.mod.o
LD [M] /home/jason/volatility/tools/linux/module.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.15.0-45-generic'
dwarfdump -di module.ko > module.dwarf
make -C //lib/modules/4.15.0-45-generic/build M="/home/jason/volatility/tools/linux" clean
make[1]: Entering directory '/usr/src/linux-headers-4.15.0-45-generic'
CLEAN /home/jason/volatility/tools/linux/.tmp_versions
CLEAN /home/jason/volatility/tools/linux/Module.symvers
make[1]: Leaving directory '/usr/src/linux-headers-4.15.0-45-generic'
root@jason-Virtual-Machine:/home/jason/volatility/tools/linux#

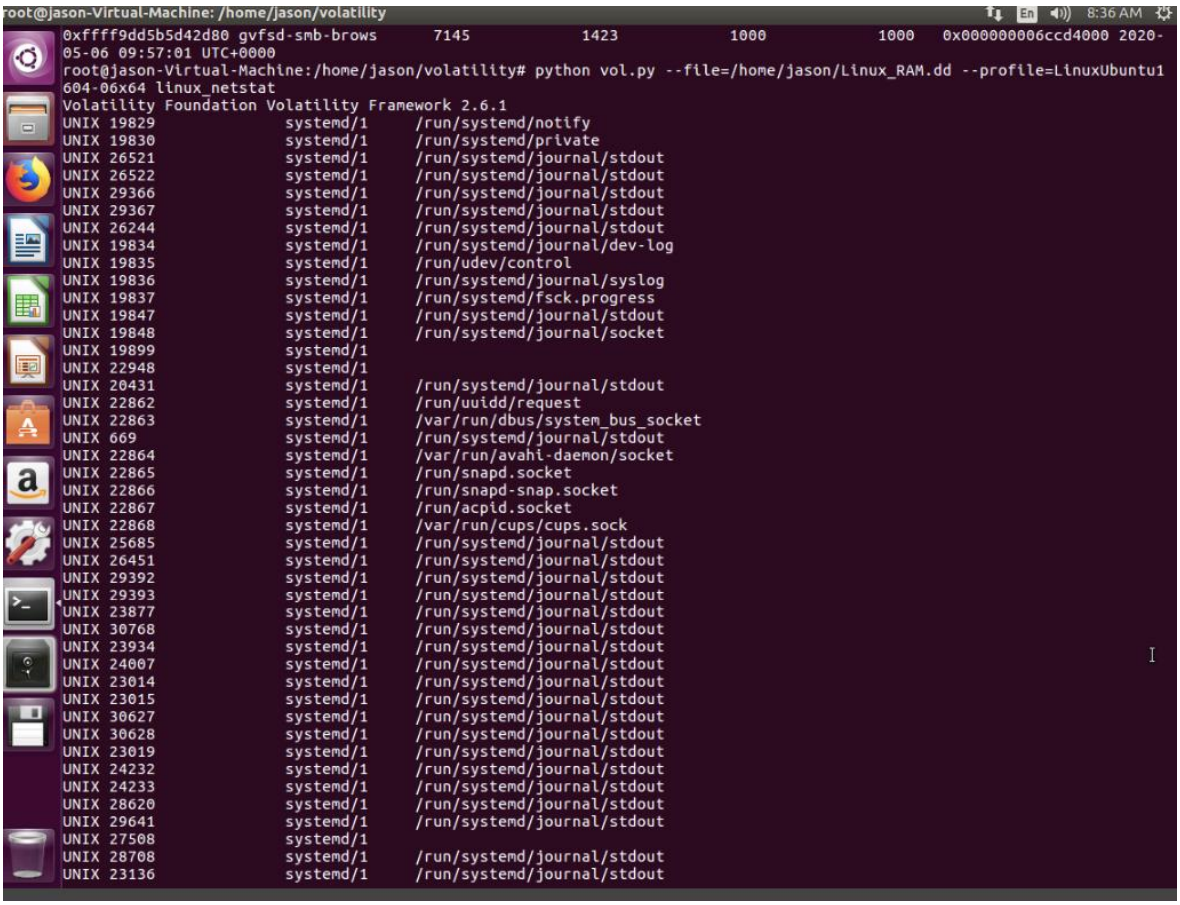

Ubuntu Forensics
root@jason-Virtual-Machine: /home/jason/volatility
En
3:08 PM
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 linux-headers-4.4.0-21 all 4.4.0-21.37 [9,927 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 linux-headers-4.4.0-21-generic amd64 4.4.0-21.37 [780 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 linux-headers-generic amd64 4.4.0.21.22 [2,314 B]
Fetched 10.7 MB in 1s (8,612 kB/s)
Selecting previously unselected package linux-headers-4.4.0-21.
(Reading database ... 178445 files and directories currently installed.)
Preparing to unpack .../linux-headers-4.4.0-21_4.4.0-21.37_all.deb ...
Unpacking linux-headers-4.4.0-21 (4.4.0-21.37) ...
Selecting previously unselected package linux-headers-4.4.0-21-generic.
Preparing to unpack .../linux-headers-4.4.0-21-generic_4.4.0-21.37_amd64.deb ...
Unpacking linux-headers-4.4.0-21-generic (4.4.0-21.37) ...
Selecting previously unselected package linux-headers-generic.
Preparing to unpack .../linux-headers-generic_4.4.0.21.22_amd64.deb ...
Unpacking linux-headers-generic (4.4.0.21.22) ...
Setting up linux-headers-4.4.0-21 (4.4.0-21.37) ...
Setting up linux-headers-4.4.0-21-generic (4.4.0-21.37) ...
Setting up linux-headers-generic (4.4.0.21.22) ...
root@jason-Virtual-Machine:/home/jason/volatility/tools/linux# make
make -C //lib/modules/4.15.0-45-generic/build CONFIG_DEBUG_INFO=y M="/home/jason/volatility/tools/linux" modules
make[1]: Entering directory '/usr/src/linux-headers-4.15.0-45-generic'
Makefile:975: "Cannot use CONFIG_STACK_VALIDATION=y, please install libelf-dev, libelf-devel or elfutils-libelf-devel"
CC [M] /home/jason/volatility/tools/linux/module.o
Building modules, stage 2.
MODPOST 1 modules
WARNING: modpost: missing MODULE_LICENSE() in /home/jason/volatility/tools/linux/module.o
see include/linux/module.h for more information
CC /home/jason/volatility/tools/linux/module.mod.o
LD [M] /home/jason/volatility/tools/linux/module.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.15.0-45-generic'
dwarfdump -di module.ko > module.dwarf
make -C //lib/modules/4.15.0-45-generic/build M="/home/jason/volatility/tools/linux" clean
make[1]: Entering directory '/usr/src/linux-headers-4.15.0-45-generic'
CLEAN /home/jason/volatility/tools/linux/.tmp_versions
CLEAN /home/jason/volatility/tools/linux/Module.symvers
make[1]: Leaving directory '/usr/src/linux-headers-4.15.0-45-generic'
root@jason-Virtual-Machine:/home/jason/volatility/tools/linux# ls /boot/
config-4.15.0-45-generic initrd.img-4.15.0-45-generic memtest86+.elf System.map-4.15.0-45-generic
grub memtest86+.bin memtest86+_multiboot.bin vmlinuz-4.15.0-45-generic
root@jason-Virtual-Machine:/home/jason/volatility/tools/linux# ls
kcore Makefile Makefile.enterprise module.c module.dwarf
root@jason-Virtual-Machine:/home/jason/volatility/tools/linux# cd ../..
root@jason-Virtual-Machine:/home/jason/volatility#
root@jason-Virtual-Machine:/home/jason/volatility#
root@jason-Virtual-Machine:/home/jason/volatility#
root@jason-Virtual-Machine:/home/jason/volatility#
root@jason-Virtual-Machine:/home/jason/volatility#
root@jason-Virtual-Machine:/home/jason/volatility#
root@jason-Virtual-Machine:/home/jason/volatility#

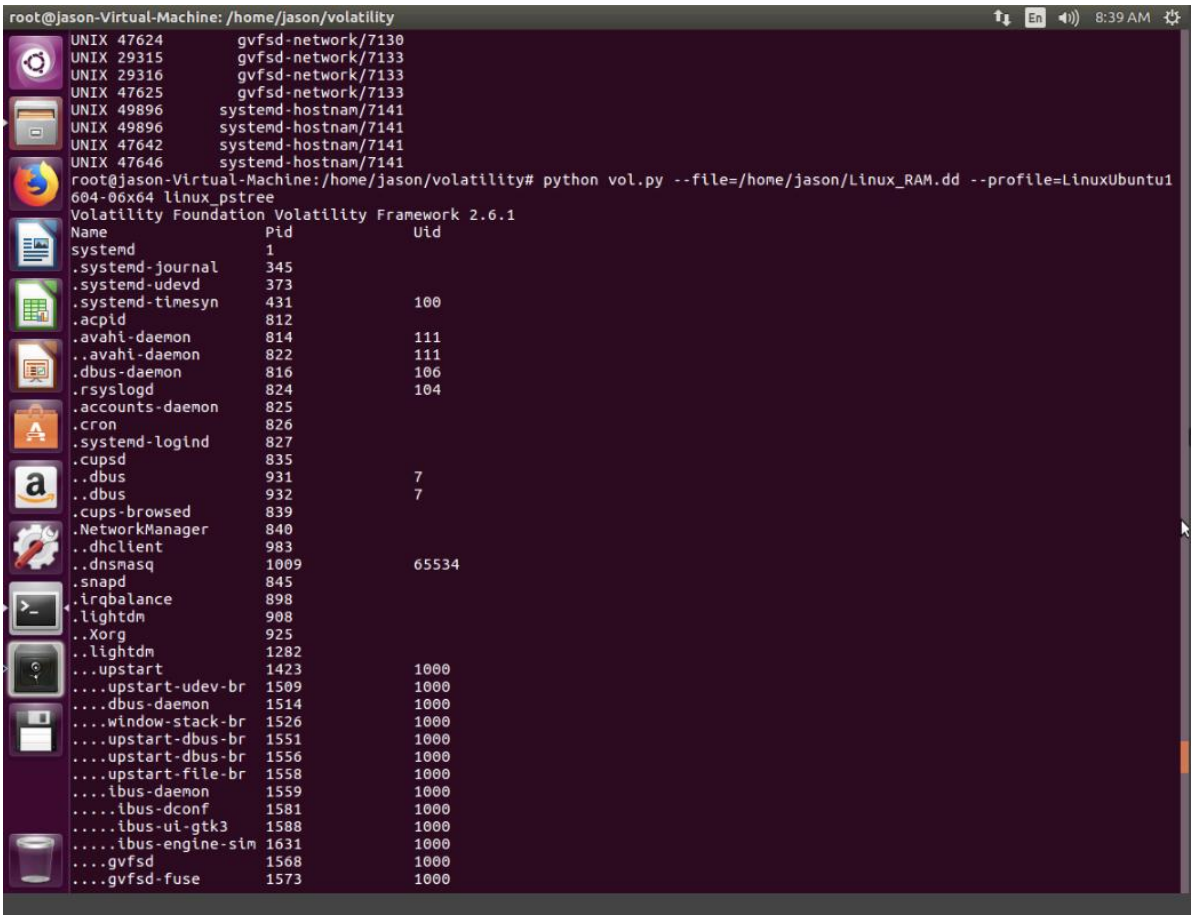

Ubuntu Forensics
root@jason-Virtual-Machine: /home/jason/volatility
En
3:20 PM
Setting up linux-headers-4.4.0-21 (4.4.0-21.37) ...
Setting up linux-headers-4.4.0-21-generic (4.4.0-21.37) ...
Setting up linux-headers-generic (4.4.0.21.22) ...
root@jason-Virtual-Machine:/home/jason/volatility/tools/linux# make
make -C //lib/modules/4.15.0-45-generic/build CONFIG_DEBUG_INFO=y M="/home/jason/volatility/tools/linux" modules
make[1]: Entering directory '/usr/src/linux-headers-4.15.0-45-generic'
Makefile:975: "Cannot use CONFIG_STACK_VALIDATION=y, please install libelf-dev, libelf-devel or elfutils-libelf-devel"
CC [M] /home/jason/volatility/tools/linux/module.o
Building modules, stage 2.
MODPOST 1 modules
WARNING: modpost: missing MODULE_LICENSE() in /home/jason/volatility/tools/linux/module.o
see include/linux/module.h for more information
CC /home/jason/volatility/tools/linux/module.mod.o
LD [M] /home/jason/volatility/tools/linux/module.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.15.0-45-generic'
dwarfdump -di module.ko > module.dwarf
make -C //lib/modules/4.15.0-45-generic/build M="/home/jason/volatility/tools/linux" clean
make[1]: Entering directory '/usr/src/linux-headers-4.15.0-45-generic'
CLEAN /home/jason/volatility/tools/linux/.tmp_versions
CLEAN /home/jason/volatility/tools/linux/Module.symvers
make[1]: Leaving directory '/usr/src/linux-headers-4.15.0-45-generic'
root@jason-Virtual-Machine:/home/jason/volatility/tools/linux# ls /boot/
config-4.15.0-45-generic initrd.img-4.15.0-45-generic memtest86+.elf System.map-4.15.0-45-generic
grub memtest86+.bin memtest86+_multiboot.bin vmlinuz-4.15.0-45-generic
root@jason-Virtual-Machine:/home/jason/volatility/tools/linux# ls
kcore Makefile Makefile.enterprise module.c module.dwarf
root@jason-Virtual-Machine:/home/jason/volatility/tools/linux# cd ../..
root@jason-Virtual-Machine:/home/jason/volatility#
root@jason-Virtual-Machine:/home/jason/volatility#
root@jason-Virtual-Machine:/home/jason/volatility#
root@jason-Virtual-Machine:/home/jason/volatility#
root@jason-Virtual-Machine:/home/jason/volatility#
root@jason-Virtual-Machine:/home/jason/volatility#
root@jason-Virtual-Machine:/home/jason/volatility# zip volatitility/plugins/linux/Ubuntu1604-06.zip tools/linux/module.
dwarf /boot/System.map-4.15.0-45-generic
zip I/O error: No such file or directory
zip error: Could not create output file (volatitility/plugins/linux/Ubuntu1604-06.zip)
root@jason-Virtual-Machine:/home/jason/volatility# zip volatility/plugins/linux/Ubuntu1604-06.zip tools/linux/module.dw
arf /boot/System.map-4.15.0-45-generic
adding: tools/linux/module.dwarf (deflated 89%)
adding: boot/System.map-4.15.0-45-generic (deflated 79%)
root@jason-Virtual-Machine:/home/jason/volatility# python vol.py --info|grep Linux
Volatility Foundation Volatility Framework 2.6.1
LinuxUbuntu1604-06x64 - A Profile for Linux Ubuntu1604-06 x64
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
LinuxAMD64PagedMemory - Linux-specific AMD 64-bit address space.
root@jason-Virtual-Machine:/home/jason/volatility#

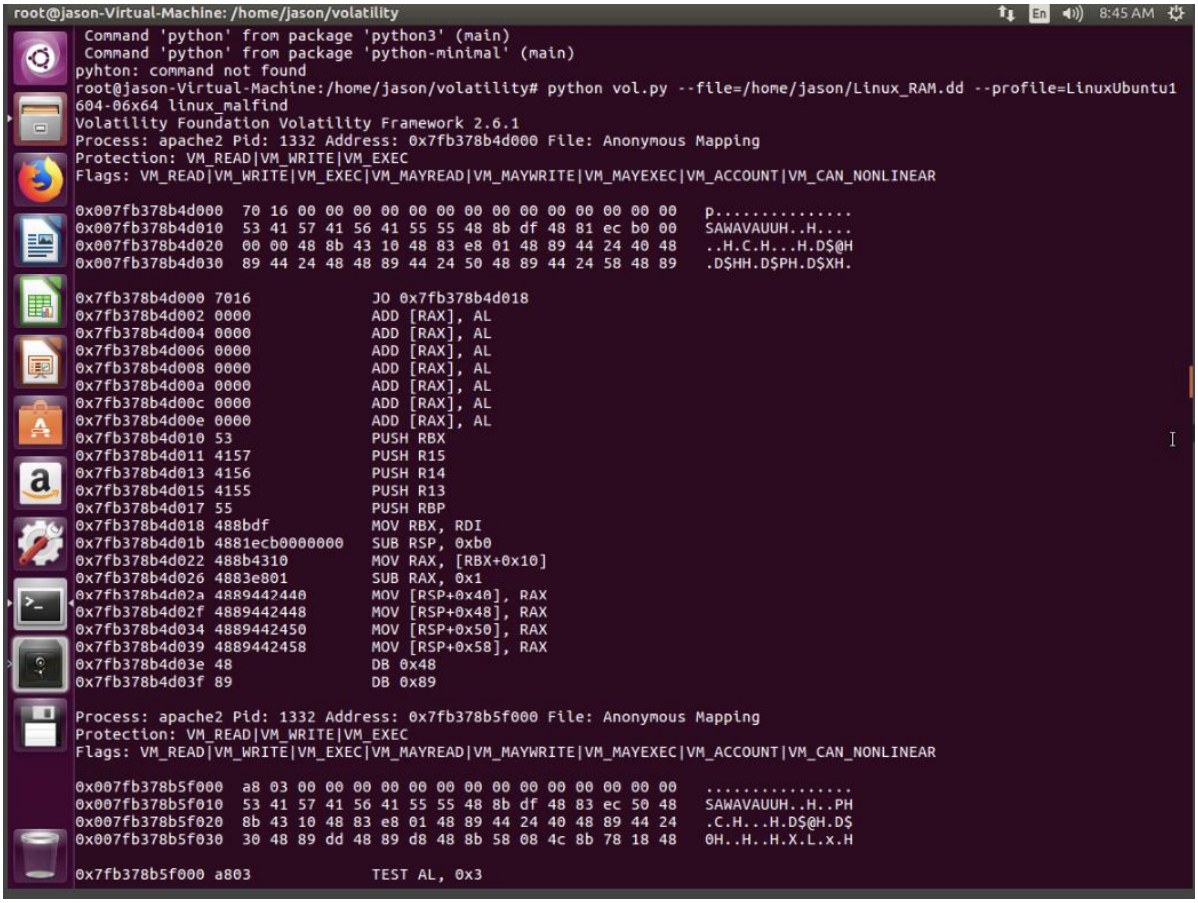

Files
3:22 PM
dfe-tools on 10.10.1.19
Evidence Files
Forensic Images
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Network
Computer
dfe-tools on 1...
Floppy Disk
dfe-tools on 10.10.1...
Connect to Server
Linux_Evidence_001.img
Linux_Evidence_SSD.dd
Linux_RAM.dd
TOR_Closed.mem
TOR_Opened.mem
Windows_Evidence_001.dd
Windows_Evidence_002.dd
Windows_RAM.mem
Could not display "Linux_RAM.dd".
The file is of an unknown type
Select Application
OK
"Linux_RAM.dd" selected (2.1 GB)

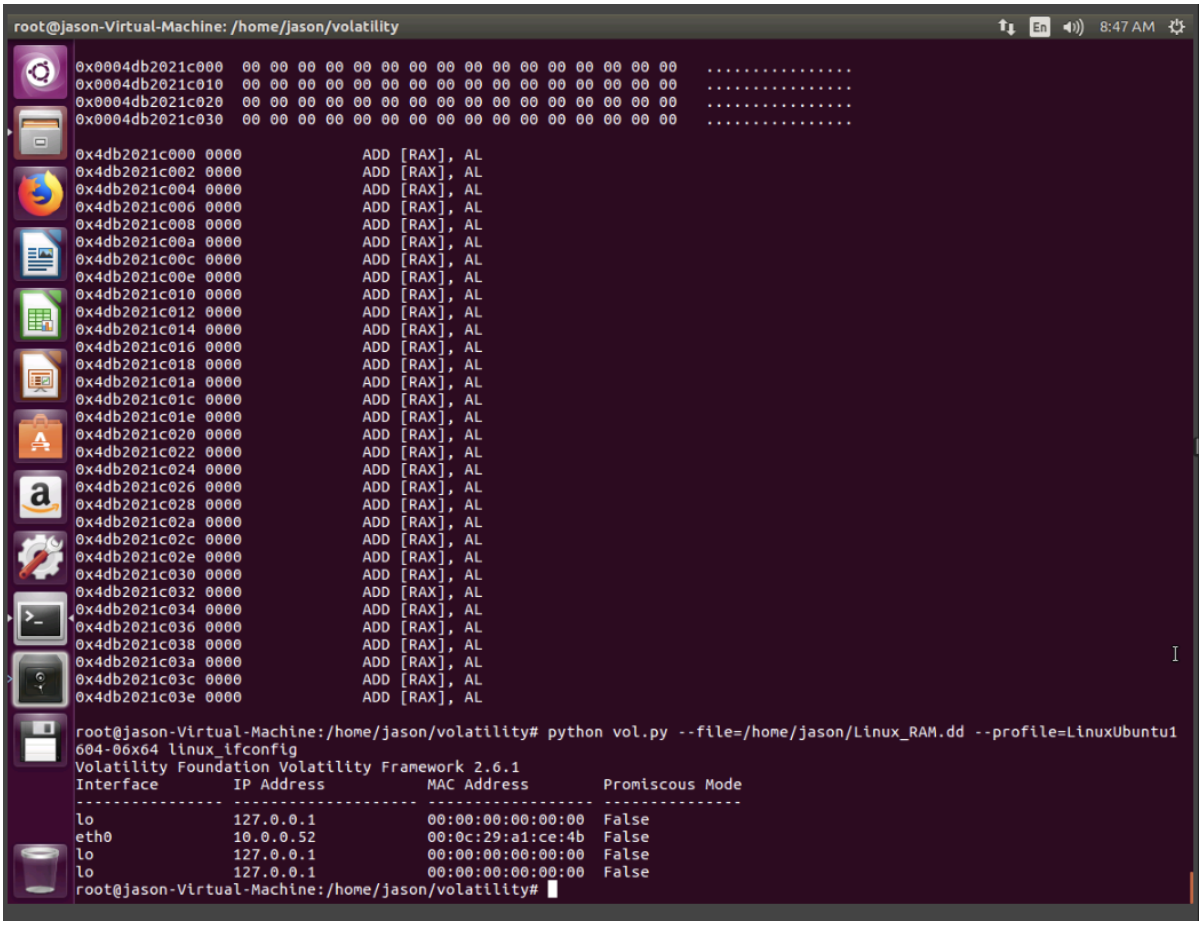

Ubuntu Forensics
Home
En
3:23 PM
Home
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Network
Computer
dfe-tools on 1...
Floppy Disk
dfe-tools on 10.10.1...
Connect to Server
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
volatility
Examples
Linux_RAM.dd
"Linux_RAM.dd" selected (2.1 GB)

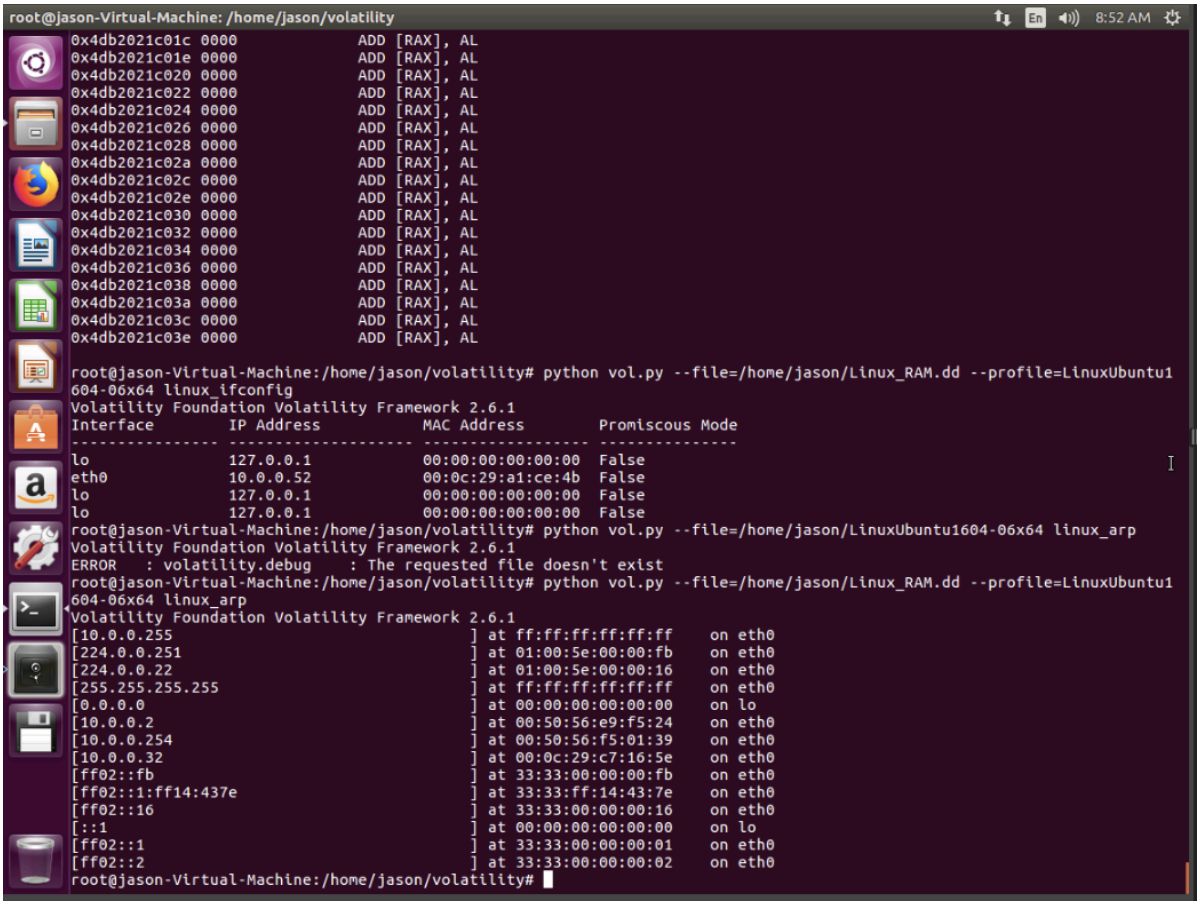

root@jason-Virtual-Machine: /home/jason/volatility
En
8:32 AM
jason@jason-Virtual-Machine:~$ sudo su
[sudo] password for jason:
root@jason-Virtual-Machine:/home/jason# cd /home/jason/volatility
root@jason-Virtual-Machine:/home/jason/volatility# ls -lh /home/jason/Linux_RAM.dd
-rw-rw-r-- 1 jason jason 2.0G Dec 2 2020 /home/jason/Linux_RAM.dd
root@jason-Virtual-Machine:/home/jason/volatility# python vol.py --file=/home/jason/Linux_RAM.dd --profile=LinuxUbuntu1604-06x64 linux_pslist
Volatility Foundation Volatility Framework 2.6.1
Offset Name Pid PPid Uid Gid DTB Start Time
0xffff9dd5baf08000 systemd 1 0 0 0 0x00000000795a0000 2020-05-06 08:11:23 UTC+0000
0xffff9dd5baf0db00 kthreadd 2 0 0 0 ---------- 2020-05-06 08:11:23 UTC+0000
0xffff9dd5baf0ad80 kworker/0:0H 4 2 0 0 ---------- 2020-05-06 08:11:23 UTC+0000
0xffff9dd5baf4c440 mm_percpu_wq 6 2 0 0 ---------- 2020-05-06 08:11:23 UTC+0000
0xffff9dd5baf48000 ksoftirqd/0 7 2 0 0 ---------- 2020-05-06 08:11:23 UTC+0000
0xffff9dd5baf4db00 rcu_sched 8 2 0 0 ---------- 2020-05-06 08:11:23 UTC+0000
0xffff9dd5baf496c0 rcu_bh 9 2 0 0 ---------- 2020-05-06 08:11:23 UTC+0000
0xffff9dd5baf4ad80 migration/0 10 2 0 0 ---------- 2020-05-06 08:11:23 UTC+0000
0xffff9dd5baf75b00 watchdog/0 11 2 0 0 ---------- 2020-05-06 08:11:23 UTC+0000
0xffff9dd5baaa0000 cpuhp/0 12 2 0 0 ---------- 2020-05-06 08:11:23 UTC+0000
0xffff9dd5baaa5b00 cpuhp/1 13 2 0 0 ---------- 2020-05-06 08:11:23 UTC+0000
0xffff9dd5baad4440 watchdog/1 14 2 0 0 ---------- 2020-05-06 08:11:23 UTC+0000
0xffff9dd5baad0000 migration/1 15 2 0 0 ---------- 2020-05-06 08:11:23 UTC+0000
0xffff9dd5baad5b00 ksoftirqd/1 16 2 0 0 ---------- 2020-05-06 08:11:23 UTC+0000
0xffff9dd5baad2d80 kworker/1:0H 18 2 0 0 ---------- 2020-05-06 08:11:23 UTC+0000
0xffff9dd5baaf96c0 cpuhp/2 19 2 0 0 ---------- 2020-05-06 08:11:23 UTC+0000
0xffff9dd5baafad80 watchdog/2 20 2 0 0 ---------- 2020-05-06 08:11:23 UTC+0000
0xffff9dd5baafc440 migration/2 21 2 0 0 ---------- 2020-05-06 08:11:23 UTC+0000
0xffff9dd5baaf8000 ksoftirqd/2 22 2 0 0 ---------- 2020-

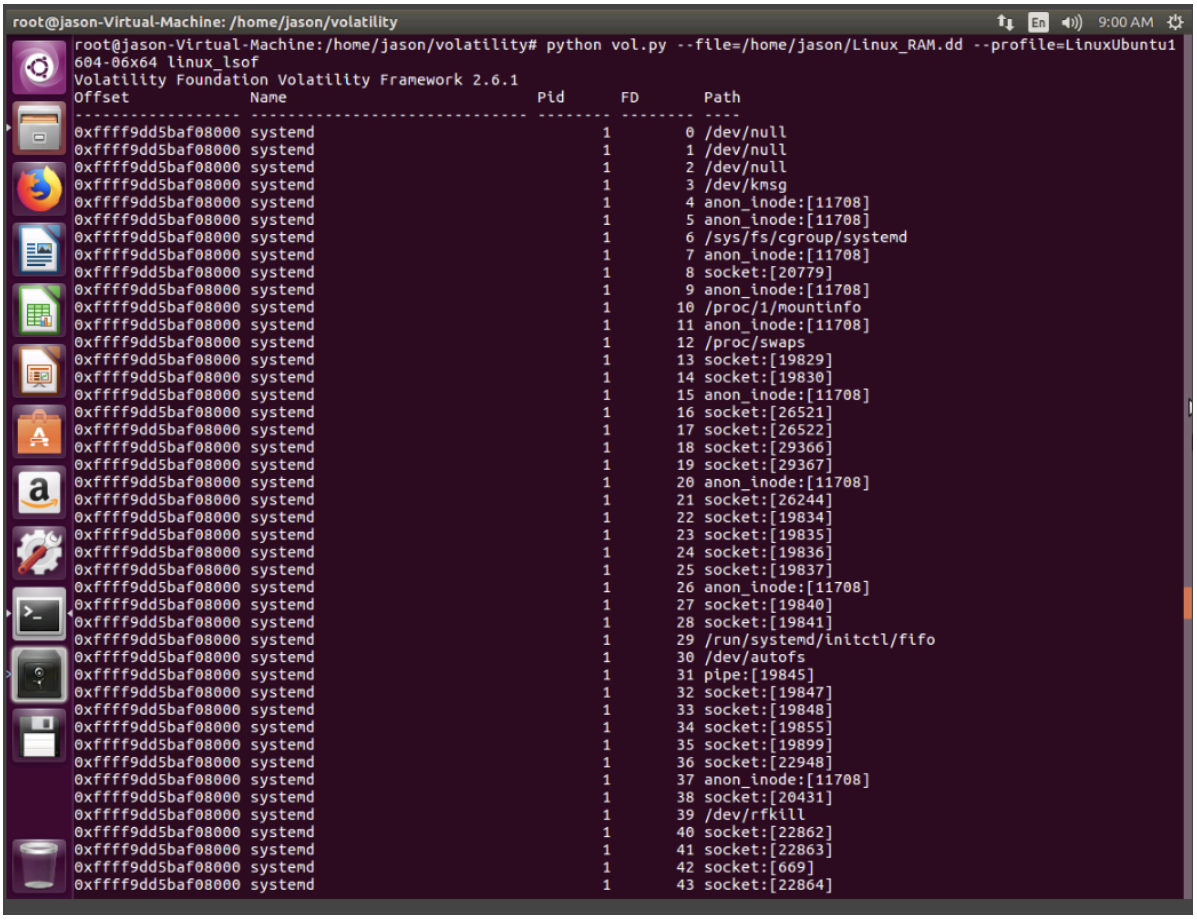

root@jason-Virtual-Machine: /home/jason/volatility
8:36 AM
0xffff9dd5b5d42d80 gvfsd-smb-brows 7145 1423 1000 1000 0x000000006ccd4000 2020-05-06 09:57:01 UTC+0000
root@jason-Virtual-Machine:/home/jason/volatility# python vol.py --file=/home/jason/Linux_RAM.dd --profile=LinuxUbuntu1604-06x64 linux_netstat
Volatility Foundation Volatility Framework 2.6.1
UNIX 19829 systemd/1 /run/systemd/notify
UNIX 19830 systemd/1 /run/systemd/private
UNIX 26521 systemd/1 /run/systemd/journal/stdout
UNIX 26522 systemd/1 /run/systemd/journal/stdout
UNIX 29366 systemd/1 /run/systemd/journal/stdout
UNIX 29367 systemd/1 /run/systemd/journal/stdout
UNIX 26244 systemd/1 /run/systemd/journal/stdout
UNIX 19834 systemd/1 /run/systemd/journal/dev-log
UNIX 19835 systemd/1 /run/udev/control
UNIX 19836 systemd/1 /run/systemd/journal/syslog
UNIX 19837 systemd/1 /run/systemd/fsck.progress
UNIX 19847 systemd/1 /run/systemd/journal/stdout
UNIX 19848 systemd/1 /run/systemd/journal/socket
UNIX 19899 systemd/1
UNIX 22948 systemd/1
UNIX 20431 systemd/1 /run/systemd/journal/stdout
UNIX 22862 systemd/1 /run/uuidd/request
UNIX 22863 systemd/1 /var/run/dbus/system_bus_socket
UNIX 669 systemd/1 /run/systemd/journal/stdout
UNIX 22864 systemd/1 /var/run/avahi-daemon/socket
UNIX 22865 systemd/1 /run/snapd.socket
UNIX 22866 systemd/1 /run/snapd-snap.socket
UNIX 22867 systemd/1 /run/acpid.socket
UNIX 22868 systemd/1 /var/run/cups/cups.sock
UNIX 25685 systemd/1 /run/systemd/journal/stdout
UNIX 26451 systemd/1 /run/systemd/journal/stdout
UNIX 29392 systemd/1 /run/systemd/journal/stdout
UNIX 29393 systemd/1 /run/systemd/journal/stdout
UNIX 23877 systemd/1 /run/systemd/journal/stdout
UNIX 30768 systemd/1 /run/systemd/journal/stdout
UNIX 23934 systemd/1 /run/systemd/journal/stdout
UNIX 24007 systemd/1 /run/systemd/journal/stdout
UNIX 23014 systemd/1 /run/systemd/journal/stdout
UNIX 23015 systemd/1 /run/systemd/journal/stdout
UNIX 30627 systemd/1 /run/systemd/journal/stdout
UNIX 30628 systemd/1 /run/systemd/journal/stdout
UNIX 23019 systemd/1 /run/systemd/journal/stdout
UNIX 24232 systemd/1 /run/systemd/journal/stdout
UNIX 24233 systemd/1 /run/systemd/journal/stdout
UNIX 28620 systemd/1 /run/systemd/journal/stdout
UNIX 29641 systemd/1 /run/systemd/journal/stdout
UNIX 27508 systemd/1
UNIX 28708 systemd/1 /run/systemd/journal/stdout
UNIX 23136 systemd/1 /run/systemd/journal/stdout

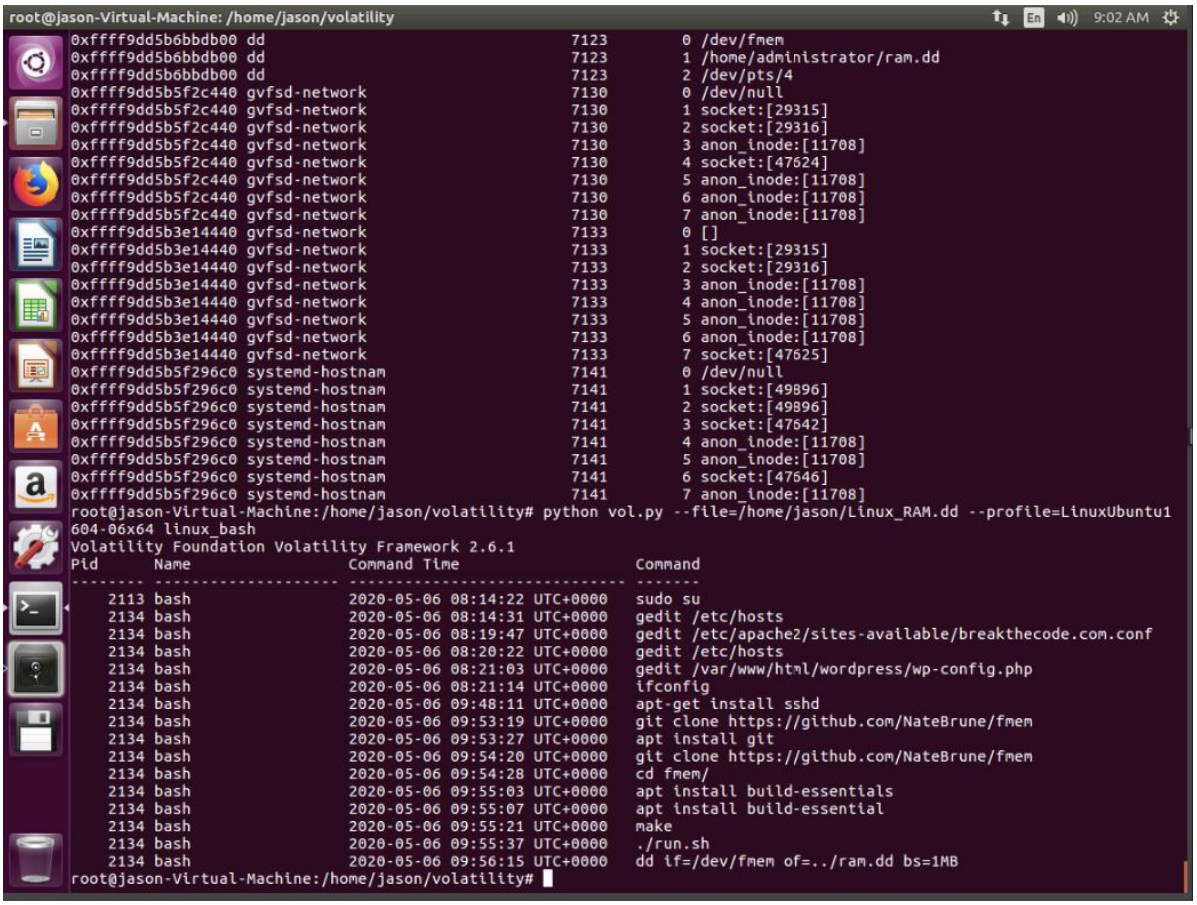

root@jason-Virtual-Machine: /home/jason/volatility
En
8:39 AM
UNIX 47624 gvfsd-network/7130
UNIX 29315 gvfsd-network/7133
UNIX 29316 gvfsd-network/7133
UNIX 47625 gvfsd-network/7133
UNIX 49896 systemd-hostnam/7141
UNIX 49896 systemd-hostnam/7141
UNIX 47642 systemd-hostnam/7141
UNIX 47646 systemd-hostnam/7141
root@jason-Virtual-Machine:/home/jason/volatility# python vol.py --file=/home/jason/Linux_RAM.dd --profile=LinuxUbuntu1
604-06x64 linux_pstree
Volatility Foundation Volatility Framework 2.6.1
Name Pid Uid
systemd 1
.systemd-journal 345
.systemd-udevd 373
.systemd-timesyn 431 100
.acpid 812
.avahi-daemon 814 111
..avahi-daemon 822 111
.dbus-daemon 816 106
.rsyslogd 824 104
.accounts-daemon 825
.cron 826
.systemd-logind 827
.cupsd 835
..dbus 931 7
..dbus 932 7
.cups-browsed 839
.NetworkManager 840
..dhclient 983
..dnsmasq 1009 65534
.snapd 845
.irqbalance 898
.lightdm 908
..Xorg 925
..lightdm 1282
...upstart 1423 1000
....upstart-udev-br 1509 1000
....dbus-daemon 1514 1000
....window-stack-br 1526 1000
....upstart-dbus-br 1551 1000
....upstart-dbus-br 1556 1000
....upstart-file-br 1558 1000
....ibus-daemon 1559 1000
.....ibus-dconf 1581 1000
.....ibus-ui-gtk3 1588 1000
.....ibus-engine-sim 1631 1000
....gvfsd 1568 1000
....gvfsd-fuse 1573 1000

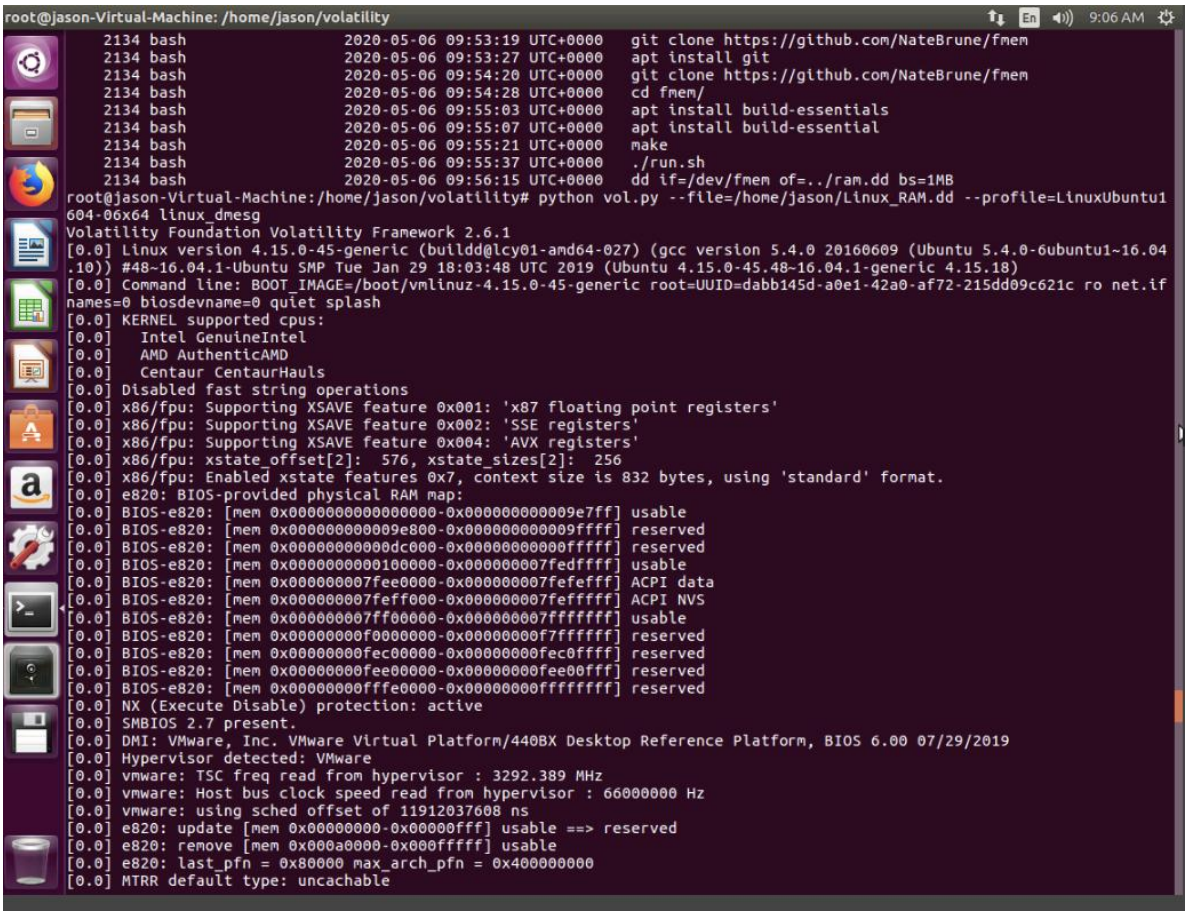

root@jason-Virtual-Machine: /home/jason/volatility
8:45 AM
Command 'python' from package 'python3' (main)
Command 'python' from package 'python-minimal' (main)
pyhton: command not found
root@jason-Virtual-Machine:/home/jason/volatility# python vol.py --file=/home/jason/Linux_RAM.dd --profile=LinuxUbuntu1
604-06x64 linux_malfind
Volatility Foundation Volatility Framework 2.6.1
Process: apache2 Pid: 1332 Address: 0x7fb378b4d000 File: Anonymous Mapping
Protection: VM_READ|VM_WRITE|VM_EXEC
Flags: VM_READ|VM_WRITE|VM_EXEC|VM_MAYREAD|VM_MAYWRITE|VM_MAYEXEC|VM_ACCOUNT|VM_CAN_NONLINEAR
0x007fb378b4d000 70 16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 p...............
0x007fb378b4d010 53 41 57 41 56 41 55 55 48 8b df 48 81 ec b0 00 SAWAVAUUH..H....
0x007fb378b4d020 00 00 48 8b 43 10 48 83 e8 01 48 89 44 24 40 48 ..H.C.H...H.D$@H
0x007fb378b4d030 89 44 24 48 48 89 44 24 50 48 89 44 24 58 48 89 .D$HH.D$PH.D$XH.
0x7fb378b4d000 7016 JO 0x7fb378b4d018
0x7fb378b4d002 0000 ADD [RAX], AL
0x7fb378b4d004 0000 ADD [RAX], AL
0x7fb378b4d006 0000 ADD [RAX], AL
0x7fb378b4d008 0000 ADD [RAX], AL
0x7fb378b4d00a 0000 ADD [RAX], AL
0x7fb378b4d00c 0000 ADD [RAX], AL
0x7fb378b4d00e 0000 ADD [RAX], AL
0x7fb378b4d010 53 PUSH RBX
0x7fb378b4d011 4157 PUSH R15
0x7fb378b4d013 4156 PUSH R14
0x7fb378b4d015 4155 PUSH R13
0x7fb378b4d017 55 PUSH RBP
0x7fb378b4d018 488bdf MOV RBX, RDI
0x7fb378b4d01b 4881ecb0000000 SUB RSP, 0xb0
0x7fb378b4d022 488b4310 MOV RAX, [RBX+0x10]
0x7fb378b4d026 4883e801 SUB RAX, 0x1
0x7fb378b4d02a 4889442440 MOV [RSP+0x40], RAX
0x7fb378b4d02f 4889442448 MOV [RSP+0x48], RAX
0x7fb378b4d034 4889442450 MOV [RSP+0x50], RAX
0x7fb378b4d039 4889442458 MOV [RSP+0x58], RAX
0x7fb378b4d03e 48 DB 0x48
0x7fb378b4d03f 89 DB 0x89
Process: apache2 Pid: 1332 Address: 0x7fb378b5f000 File: Anonymous Mapping
Protection: VM_READ|VM_WRITE|VM_EXEC
Flags: VM_READ|VM_WRITE|VM_EXEC|VM_MAYREAD|VM_MAYWRITE|VM_MAYEXEC|VM_ACCOUNT|VM_CAN_NONLINEAR
0x007fb378b5f000 a8 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x007fb378b5f010 53 41 57 41 56 41 55 55 48 8b df 48 83 ec 50 48 SAWAVAUUH..H..PH
0x007fb378b5f020 8b 43 10 48 83 e8 01 48 89 44 24 40 48 89 44 24 .C.H...H.D$@H.D$
0x007fb378b5f030 30 48 89 dd 48 89 d8 48 8b 58 08 4c 8b 78 18 48 0H..H..H.X.L.x.H
0x7fb378b5f000 a803 TEST AL, 0x3

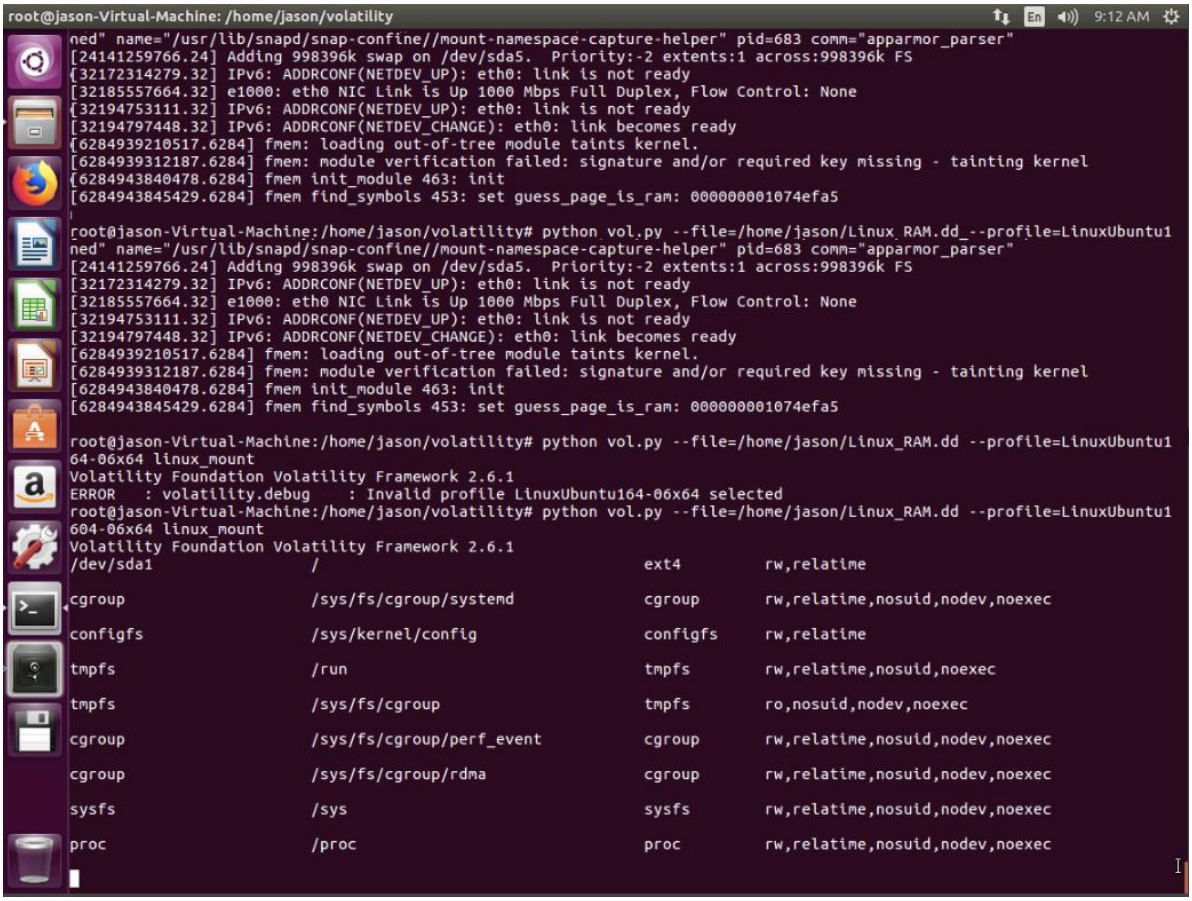

root@jason-Virtual-Machine: /home/jason/volatility
8:47 AM
0x0004db2021c000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x0004db2021c010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x0004db2021c020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x0004db2021c030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x4db2021c000 0000 ADD [RAX], AL
0x4db2021c002 0000 ADD [RAX], AL
0x4db2021c004 0000 ADD [RAX], AL
0x4db2021c006 0000 ADD [RAX], AL
0x4db2021c008 0000 ADD [RAX], AL
0x4db2021c00a 0000 ADD [RAX], AL
0x4db2021c00c 0000 ADD [RAX], AL
0x4db2021c00e 0000 ADD [RAX], AL
0x4db2021c010 0000 ADD [RAX], AL
0x4db2021c012 0000 ADD [RAX], AL
0x4db2021c014 0000 ADD [RAX], AL
0x4db2021c016 0000 ADD [RAX], AL
0x4db2021c018 0000 ADD [RAX], AL
0x4db2021c01a 0000 ADD [RAX], AL
0x4db2021c01c 0000 ADD [RAX], AL
0x4db2021c01e 0000 ADD [RAX], AL
0x4db2021c020 0000 ADD [RAX], AL
0x4db2021c022 0000 ADD [RAX], AL
0x4db2021c024 0000 ADD [RAX], AL
0x4db2021c026 0000 ADD [RAX], AL
0x4db2021c028 0000 ADD [RAX], AL
0x4db2021c02a 0000 ADD [RAX], AL
0x4db2021c02c 0000 ADD [RAX], AL
0x4db2021c02e 0000 ADD [RAX], AL
0x4db2021c030 0000 ADD [RAX], AL
0x4db2021c032 0000 ADD [RAX], AL
0x4db2021c034 0000 ADD [RAX], AL
0x4db2021c036 0000 ADD [RAX], AL
0x4db2021c038 0000 ADD [RAX], AL
0x4db2021c03a 0000 ADD [RAX], AL
0x4db2021c03c 0000 ADD [RAX], AL
0x4db2021c03e 0000 ADD [RAX], AL
root@jason-Virtual-Machine:/home/jason/volatility# python vol.py --file=/home/jason/Linux_RAM.dd --profile=LinuxUbuntu1
604-06x64 linux_ifconfig
Volatility Foundation Volatility Framework 2.6.1
Interface IP Address MAC Address Promiscous Mode
lo 127.0.0.1 00:00:00:00:00:00 False
eth0 10.0.0.52 00:0c:29:a1:ce:4b False
lo 127.0.0.1 00:00:00:00:00:00 False
lo 127.0.0.1 00:00:00:00:00:00 False
root@jason-Virtual-Machine:/home/jason/volatility#

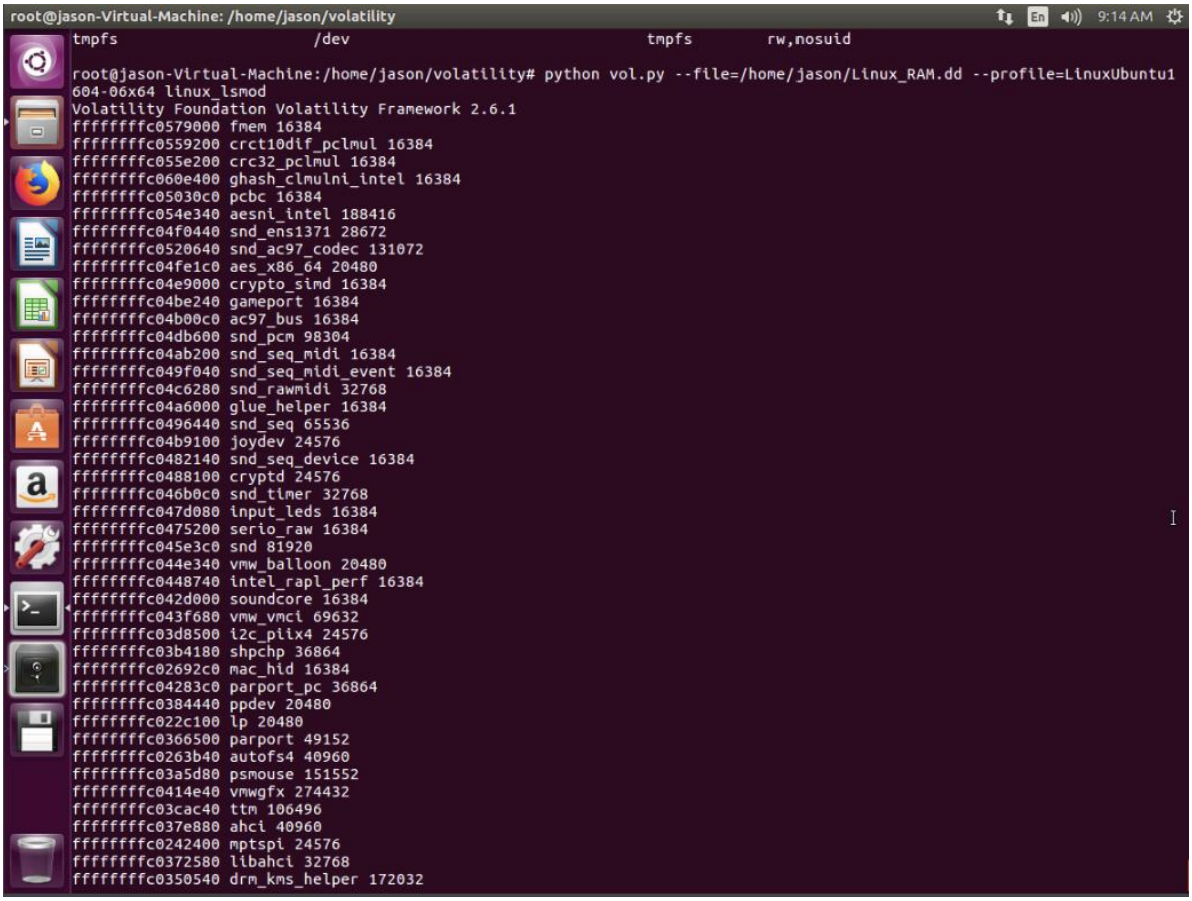

root@jason-Virtual-Machine: /home/jason/volatility
En
8:52 AM
0x4db2021c01c 0000 ADD [RAX], AL
0x4db2021c01e 0000 ADD [RAX], AL
0x4db2021c020 0000 ADD [RAX], AL
0x4db2021c022 0000 ADD [RAX], AL
0x4db2021c024 0000 ADD [RAX], AL
0x4db2021c026 0000 ADD [RAX], AL
0x4db2021c028 0000 ADD [RAX], AL
0x4db2021c02a 0000 ADD [RAX], AL
0x4db2021c02c 0000 ADD [RAX], AL
0x4db2021c02e 0000 ADD [RAX], AL
0x4db2021c030 0000 ADD [RAX], AL
0x4db2021c032 0000 ADD [RAX], AL
0x4db2021c034 0000 ADD [RAX], AL
0x4db2021c036 0000 ADD [RAX], AL
0x4db2021c038 0000 ADD [RAX], AL
0x4db2021c03a 0000 ADD [RAX], AL
0x4db2021c03c 0000 ADD [RAX], AL
0x4db2021c03e 0000 ADD [RAX], AL
root@jason-Virtual-Machine:/home/jason/volatility# python vol.py --file=/home/jason/Linux_RAM.dd --profile=LinuxUbuntu1604-06x64 linux_ifconfig
Volatility Foundation Volatility Framework 2.6.1
Interface IP Address MAC Address Promiscous Mode
lo 127.0.0.1 00:00:00:00:00:00 False
eth0 10.0.0.52 00:0c:29:a1:ce:4b False
lo 127.0.0.1 00:00:00:00:00:00 False
lo 127.0.0.1 00:00:00:00:00:00 False
root@jason-Virtual-Machine:/home/jason/volatility# python vol.py --file=/home/jason/LinuxUbuntu1604-06x64 linux_arp
Volatility Foundation Volatility Framework 2.6.1
ERROR : volatility.debug : The requested file doesn't exist
root@jason-Virtual-Machine:/home/jason/volatility# python vol.py --file=/home/jason/Linux_RAM.dd --profile=LinuxUbuntu1604-06x64 linux_arp
Volatility Foundation Volatility Framework 2.6.1
[10.0.0.255] at ff:ff:ff:ff:ff:ff on eth0
[224.0.0.251] at 01:00:5e:00:00:fb on eth0
[224.0.0.22] at 01:00:5e:00:00:16 on eth0
[255.255.255.255] at ff:ff:ff:ff:ff:ff on eth0
[0.0.0.0] at 00:00:00:00:00:00 on lo
[10.0.0.2] at 00:50:56:e9:f5:24 on eth0
[10.0.0.254] at 00:50:56:f5:01:39 on eth0
[10.0.0.32] at 00:0c:29:c7:16:5e on eth0
[ff02::fb] at 33:33:00:00:00:fb on eth0
[ff02::1:ff14:437e] at 33:33:ff:14:43:7e on eth0
[ff02::16] at 33:33:00:00:00:16 on eth0
[::1] at 00:00:00:00:00:00 on lo
[ff02::1] at 33:33:00:00:00:01 on eth0
[ff02::2] at 33:33:00:00:00:02 on eth0
root@jason-Virtual-Machine:/home/jason/volatility#


root@jason-Virtual-Machine: /home/jason/volatility
En
9:00 AM
root@jason-Virtual-Machine:/home/jason/volatility# python vol.py --file=/home/jason/Linux_RAM.dd --profile=LinuxUbuntu1
604-06x64 linux_lsof
Volatility Foundation Volatility Framework 2.6.1
Offset Name Pid FD Path
0xffff9dd5baf08000 systemd 1 0 /dev/null
0xffff9dd5baf08000 systemd 1 1 /dev/null
0xffff9dd5baf08000 systemd 1 2 /dev/null
0xffff9dd5baf08000 systemd 1 3 /dev/kmsg
0xffff9dd5baf08000 systemd 1 4 anon_inode:[11708]
0xffff9dd5baf08000 systemd 1 5 anon_inode:[11708]
0xffff9dd5baf08000 systemd 1 6 /sys/fs/cgroup/systemd
0xffff9dd5baf08000 systemd 1 7 anon_inode:[11708]
0xffff9dd5baf08000 systemd 1 8 socket:[20779]
0xffff9dd5baf08000 systemd 1 9 anon_inode:[11708]
0xffff9dd5baf08000 systemd 1 10 /proc/1/mountinfo
0xffff9dd5baf08000 systemd 1 11 anon_inode:[11708]
0xffff9dd5baf08000 systemd 1 12 /proc/swaps
0xffff9dd5baf08000 systemd 1 13 socket:[19829]
0xffff9dd5baf08000 systemd 1 14 socket:[19830]
0xffff9dd5baf08000 systemd 1 15 anon_inode:[11708]
0xffff9dd5baf08000 systemd 1 16 socket:[26521]
0xffff9dd5baf08000 systemd 1 17 socket:[26522]
0xffff9dd5baf08000 systemd 1 18 socket:[29366]
0xffff9dd5baf08000 systemd 1 19 socket:[29367]
0xffff9dd5baf08000 systemd 1 20 anon_inode:[11708]
0xffff9dd5baf08000 systemd 1 21 socket:[26244]
0xffff9dd5baf08000 systemd 1 22 socket:[19834]
0xffff9dd5baf08000 systemd 1 23 socket:[19835]
0xffff9dd5baf08000 systemd 1 24 socket:[19836]
0xffff9dd5baf08000 systemd 1 25 socket:[19837]
0xffff9dd5baf08000 systemd 1 26 anon_inode:[11708]
0xffff9dd5baf08000 systemd 1 27 socket:[19840]
0xffff9dd5baf08000 systemd 1 28 socket:[19841]
0xffff9dd5baf08000 systemd 1 29 /run/systemd/initctl/fifo
0xffff9dd5baf08000 systemd 1 30 /dev/autofs
0xffff9dd5baf08000 systemd 1 31 pipe:[19845]
0xffff9dd5baf08000 systemd 1 32 socket:[19847]
0xffff9dd5baf08000 systemd 1 33 socket:[19848]
0xffff9dd5baf08000 systemd 1 34 socket:[19855]
0xffff9dd5baf08000 systemd 1 35 socket:[19899]
0xffff9dd5baf08000 systemd 1 36 socket:[22948]
0xffff9dd5baf08000 systemd 1 37 anon_inode:[11708]
0xffff9dd5baf08000 systemd 1 38 socket:[20431]
0xffff9dd5baf08000 systemd 1 39 /dev/rfkill
0xffff9dd5baf08000 systemd 1 40 socket:[22862]
0xffff9dd5baf08000 systemd 1 41 socket:[22863]
0xffff9dd5baf08000 systemd 1 42 socket:[669]
0xffff9dd5baf08000 systemd 1 43 socket:[22864]


root@jason-Virtual-Machine: /home/jason/volatility
9:02 AM
0xffff9dd5b6bbdb00 dd 7123 0 /dev/fmem
0xffff9dd5b6bbdb00 dd 7123 1 /home/administrator/ram.dd
0xffff9dd5b6bbdb00 dd 7123 2 /dev/pts/4
0xffff9dd5b5f2c440 gvfsd-network 7130 0 /dev/null
0xffff9dd5b5f2c440 gvfsd-network 7130 1 socket:[29315]
0xffff9dd5b5f2c440 gvfsd-network 7130 2 socket:[29316]
0xffff9dd5b5f2c440 gvfsd-network 7130 3 anon_inode:[11708]
0xffff9dd5b5f2c440 gvfsd-network 7130 4 socket:[47624]
0xffff9dd5b5f2c440 gvfsd-network 7130 5 anon_inode:[11708]
0xffff9dd5b5f2c440 gvfsd-network 7130 6 anon_inode:[11708]
0xffff9dd5b5f2c440 gvfsd-network 7130 7 anon_inode:[11708]
0xffff9dd5b3e14440 gvfsd-network 7133 0 []
0xffff9dd5b3e14440 gvfsd-network 7133 1 socket:[29315]
0xffff9dd5b3e14440 gvfsd-network 7133 2 socket:[29316]
0xffff9dd5b3e14440 gvfsd-network 7133 3 anon_inode:[11708]
0xffff9dd5b3e14440 gvfsd-network 7133 4 anon_inode:[11708]
0xffff9dd5b3e14440 gvfsd-network 7133 5 anon_inode:[11708]
0xffff9dd5b3e14440 gvfsd-network 7133 6 anon_inode:[11708]
0xffff9dd5b3e14440 gvfsd-network 7133 7 socket:[47625]
0xffff9dd5b5f296c0 systemd-hostnam 7141 0 /dev/null
0xffff9dd5b5f296c0 systemd-hostnam 7141 1 socket:[49896]
0xffff9dd5b5f296c0 systemd-hostnam 7141 2 socket:[49896]
0xffff9dd5b5f296c0 systemd-hostnam 7141 3 socket:[47642]
0xffff9dd5b5f296c0 systemd-hostnam 7141 4 anon_inode:[11708]
0xffff9dd5b5f296c0 systemd-hostnam 7141 5 anon_inode:[11708]
0xffff9dd5b5f296c0 systemd-hostnam 7141 6 socket:[47646]
0xffff9dd5b5f296c0 systemd-hostnam 7141 7 anon_inode:[11708]
root@jason-Virtual-Machine:/home/jason/volatility# python vol.py --file=/home/jason/Linux_RAM.dd --profile=LinuxUbuntu1
604-06x64 linux_bash
Volatility Foundation Volatility Framework 2.6.1
Pid Name Command Time Command
2113 bash 2020-05-06 08:14:22 UTC+0000 sudo su
2134 bash 2020-05-06 08:14:31 UTC+0000 gedit /etc/hosts
2134 bash 2020-05-06 08:19:47 UTC+0000 gedit /etc/apache2/sites-available/breakthecode.com.conf
2134 bash 2020-05-06 08:20:22 UTC+0000 gedit /etc/hosts
2134 bash 2020-05-06 08:21:03 UTC+0000 gedit /var/www/html/wordpress/wp-config.php
2134 bash 2020-05-06 08:21:14 UTC+0000 ifconfig
2134 bash 2020-05-06 09:48:11 UTC+0000 apt-get install sshd
2134 bash 2020-05-06 09:53:19 UTC+0000 git clone https://github.com/NateBrune/fmem
2134 bash 2020-05-06 09:53:27 UTC+0000 apt install git
2134 bash 2020-05-06 09:54:20 UTC+0000 git clone https://github.com/NateBrune/fmem
2134 bash 2020-05-06 09:54:28 UTC+0000 cd fmem/
2134 bash 2020-05-06 09:55:03 UTC+0000 apt install build-essentials
2134 bash 2020-05-06 09:55:07 UTC+0000 apt install build-essential
2134 bash 2020-05-06 09:55:21 UTC+0000 make
2134 bash 2020-05-06 09:55:37 UTC+0000 ./run.sh
2134 bash 2020-05-06 09:56:15 UTC+0000 dd if=/dev/fmem of=../ram.dd bs=1MB
root@jason-Virtual-Machine:/home/jason/volatility#


root@jason-Virtual-Machine: /home/jason/volatility
En
9:06 AM
2134 bash 2020-05-06 09:53:19 UTC+0000 git clone https://github.com/NateBrune/fmem
2134 bash 2020-05-06 09:53:27 UTC+0000 apt install git
2134 bash 2020-05-06 09:54:20 UTC+0000 git clone https://github.com/NateBrune/fmem
2134 bash 2020-05-06 09:54:28 UTC+0000 cd fmem/
2134 bash 2020-05-06 09:55:03 UTC+0000 apt install build-essentials
2134 bash 2020-05-06 09:55:07 UTC+0000 apt install build-essential
2134 bash 2020-05-06 09:55:21 UTC+0000 make
2134 bash 2020-05-06 09:55:37 UTC+0000 ./run.sh
2134 bash 2020-05-06 09:56:15 UTC+0000 dd if=/dev/fmem of=../ram.dd bs=1MB
root@jason-Virtual-Machine:/home/jason/volatility# python vol.py --file=/home/jason/Linux_RAM.dd --profile=LinuxUbuntu1604-06x64 linux_dmesg
Volatility Foundation Volatility Framework 2.6.1
[0.0] Linux version 4.15.0-45-generic (buildd@lcy01-amd64-027) (gcc version 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.10)) #48~16.04.1-Ubuntu SMP Tue Jan 29 18:03:48 UTC 2019 (Ubuntu 4.15.0-45.48~16.04.1-generic 4.15.18)
[0.0] Command line: BOOT_IMAGE=/boot/vmlinuz-4.15.0-45-generic root=UUID=dabb145d-a0e1-42a0-af72-215dd09c621c ro net.ifnames=0 biosdevname=0 quiet splash
[0.0] KERNEL supported cpus:
[0.0] Intel GenuineIntel
[0.0] AMD AuthenticAMD
[0.0] Centaur CentaurHauls
[0.0] Disabled fast string operations
[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] e820: BIOS-provided physical RAM map:
[0.0] BIOS-e820: [mem 0x0000000000000000-0x000000000009e7ff] usable
[0.0] BIOS-e820: [mem 0x000000000009e800-0x000000000009ffff] reserved
[0.0] BIOS-e820: [mem 0x00000000000dc000-0x00000000000fffff] reserved
[0.0] BIOS-e820: [mem 0x0000000000100000-0x00000007fedfffff] usable
[0.0] BIOS-e820: [mem 0x00000007fee0000-0x00000007fefeffff] ACPI data
[0.0] BIOS-e820: [mem 0x00000007feff000-0x00000007fefffff] ACPI NVS
[0.0] BIOS-e820: [mem 0x00000007ff00000-0x00000007ffffffff] usable
[0.0] BIOS-e820: [mem 0x00000000f0000000-0x00000000f7ffffff] reserved
[0.0] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] reserved
[0.0] BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
[0.0] BIOS-e820: [mem 0x00000000fffe0000-0x00000000ffffffff] reserved
[0.0] NX (Execute Disable) protection: active
[0.0] SMBIOS 2.7 present.
[0.0] DMI: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 07/29/2019
[0.0] Hypervisor detected: VMware
[0.0] vmware: TSC freq read from hypervisor : 3292.389 MHz
[0.0] vmware: Host bus clock speed read from hypervisor : 66000000 Hz
[0.0] vmware: using sched offset of 11912037608 ns
[0.0] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
[0.0] e820: remove [mem 0x000a0000-0x000fffff] usable
[0.0] e820: last_pfn = 0x80000 max_arch_pfn = 0x400000000
[0.0] MTRR default type: uncachable


root@jason-Virtual-Machine: /home/jason/volatility
9:12 AM
ned" name="/usr/lib/snapd/snap-confine//mount-namespace-capture-helper" pid=683 comm="apparmor_parser"
[24141259766.24] Adding 998396k swap on /dev/sda5. Priority:-2 extents:1 across:998396k FS
[32172314279.32] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[32185557664.32] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
[32194753111.32] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[32194797448.32] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[6284939210517.6284] fmem: loading out-of-tree module taints kernel.
[6284939312187.6284] fmem: module verification failed: signature and/or required key missing - tainting kernel
[6284943840478.6284] fmem init_module 463: init
[6284943845429.6284] fmem find_symbols 453: set guess_page_is_ram: 000000001074efa5
root@jason-Virtual-Machine:/home/jason/volatility# python vol.py --file=/home/jason/Linux_RAM.dd_--profile=LinuxUbuntu1
ned" name="/usr/lib/snapd/snap-confine//mount-namespace-capture-helper" pid=683 comm="apparmor_parser"
[24141259766.24] Adding 998396k swap on /dev/sda5. Priority:-2 extents:1 across:998396k FS
[32172314279.32] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[32185557664.32] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
[32194753111.32] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[32194797448.32] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[6284939210517.6284] fmem: loading out-of-tree module taints kernel.
[6284939312187.6284] fmem: module verification failed: signature and/or required key missing - tainting kernel
[6284943840478.6284] fmem init_module 463: init
[6284943845429.6284] fmem find_symbols 453: set guess_page_is_ram: 000000001074efa5
root@jason-Virtual-Machine:/home/jason/volatility# python vol.py --file=/home/jason/Linux_RAM.dd --profile=LinuxUbuntu1
64-06x64 linux_mount
Volatility Foundation Volatility Framework 2.6.1
ERROR   : volatility.debug   : Invalid profile LinuxUbuntu164-06x64 selected
root@jason-Virtual-Machine:/home/jason/volatility# python vol.py --file=/home/jason/Linux_RAM.dd --profile=LinuxUbuntu1
604-06x64 linux_mount
Volatility Foundation Volatility Framework 2.6.1
/dev/sda1 / ext4 rw,relatime
cgroup /sys/fs/cgroup/systemd cgroup rw,relatime,nosuid,nodev,noexec
configfs /sys/kernel/config configfs rw,relatime
tmpfs /run tmpfs rw,relatime,nosuid,noexec
tmpfs /sys/fs/cgroup tmpfs ro,nosuid,nodev,noexec
cgroup /sys/fs/cgroup/perf_event cgroup rw,relatime,nosuid,nodev,noexec
cgroup /sys/fs/cgroup/rdma cgroup rw,relatime,nosuid,nodev,noexec
sysfs /sys sysfs rw,relatime,nosuid,nodev,noexec
proc /proc proc rw,relatime,nosuid,nodev,noexec



Lab 2: Recovering Data from a Linux Memory Dump

Lab Scenario

In an FBI-led operation, 7 people who were involved in a drug smuggling case were arrested, and drugs worth $1,00,000 were seized, along with a computer. The police suspect that investigating the computer can provide them important leads in the case; hence, they called a forensic expert to investigate the seized computer and retrieve recently accessed web pages, chats, and communications made by the accused via social networks. In order to do so, the investigator must obtain and examine a memory dump of the computer to retrieve useful data that could help during the investigation.

As a forensic expert, you must have sound knowledge of how to retrieve data from Linux memory dumps

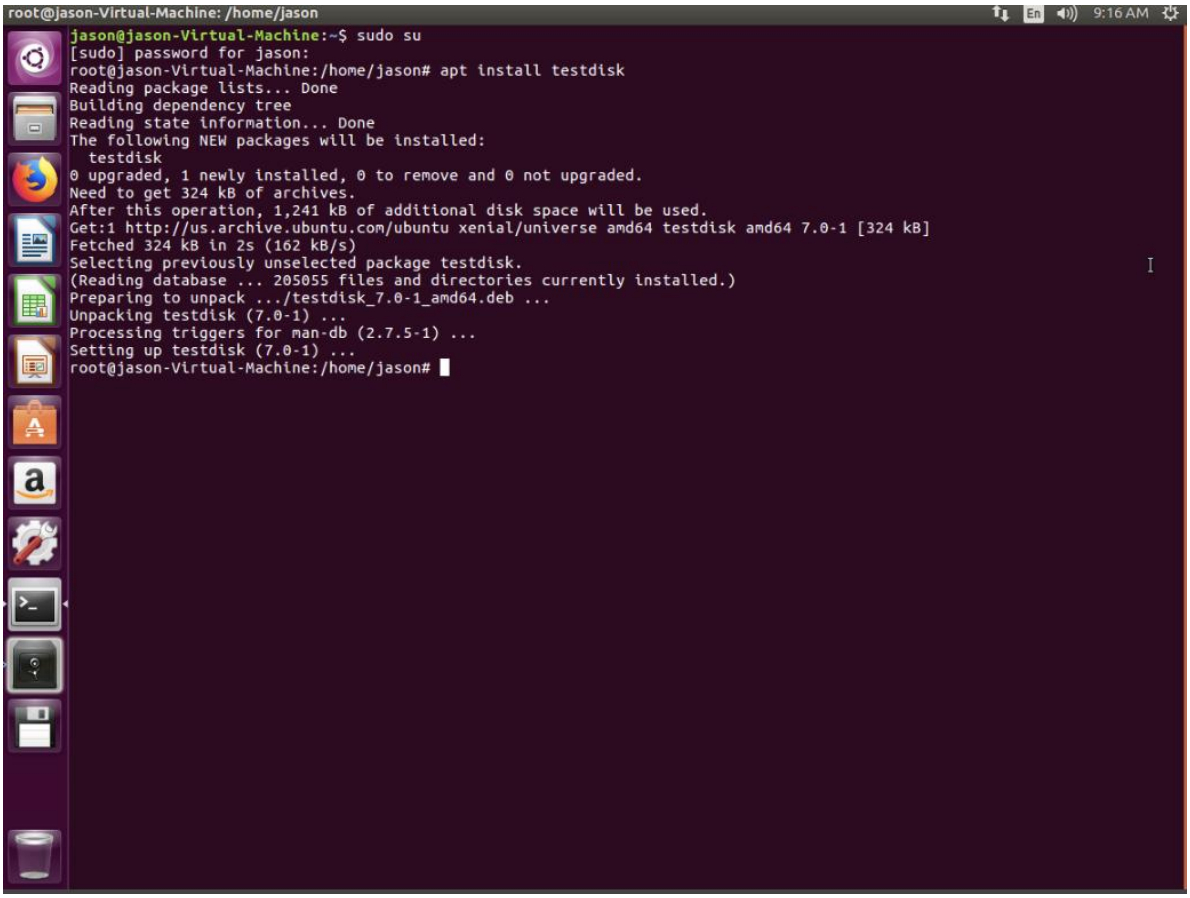
Lab Objectives

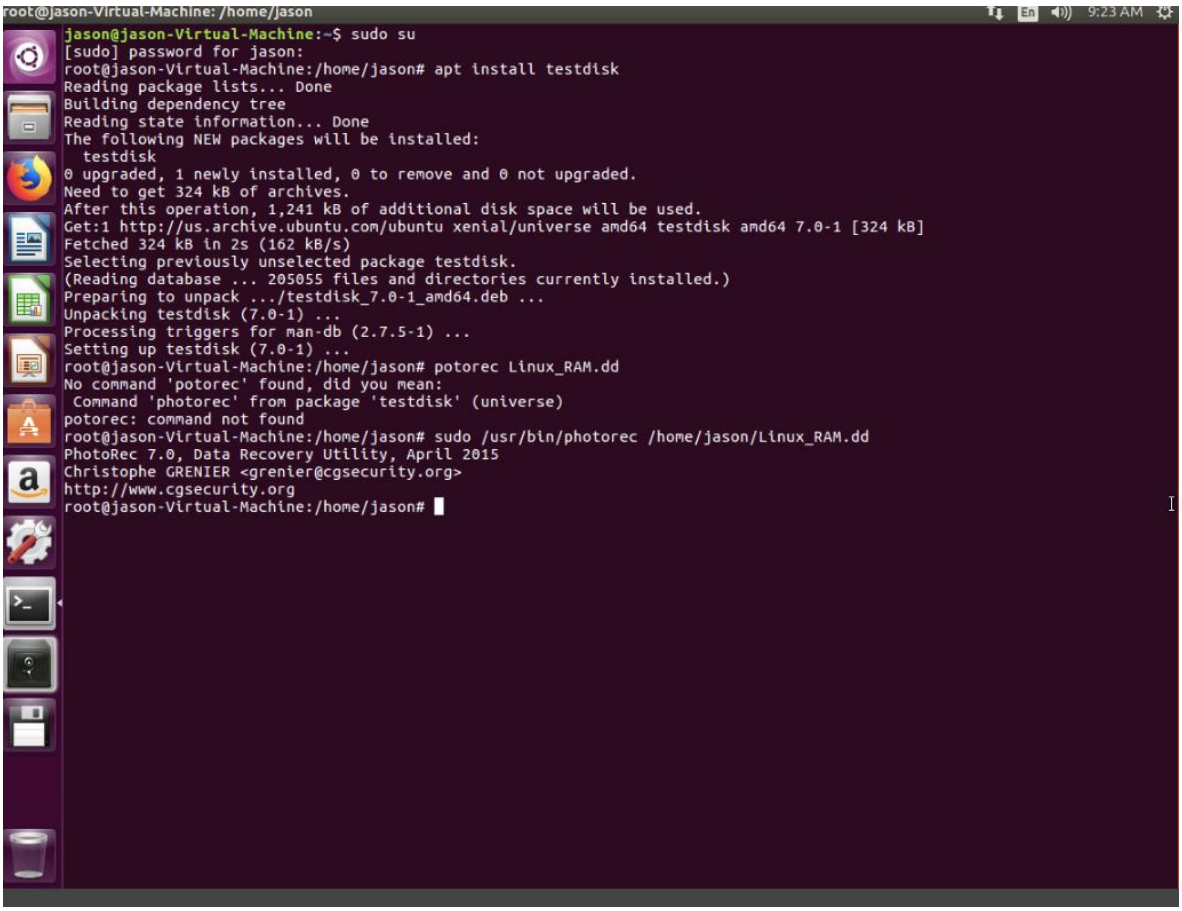
Analyzing the RAM dump of a system helps investigators retrieve valuable evidence pertaining to a case of cybercrime.

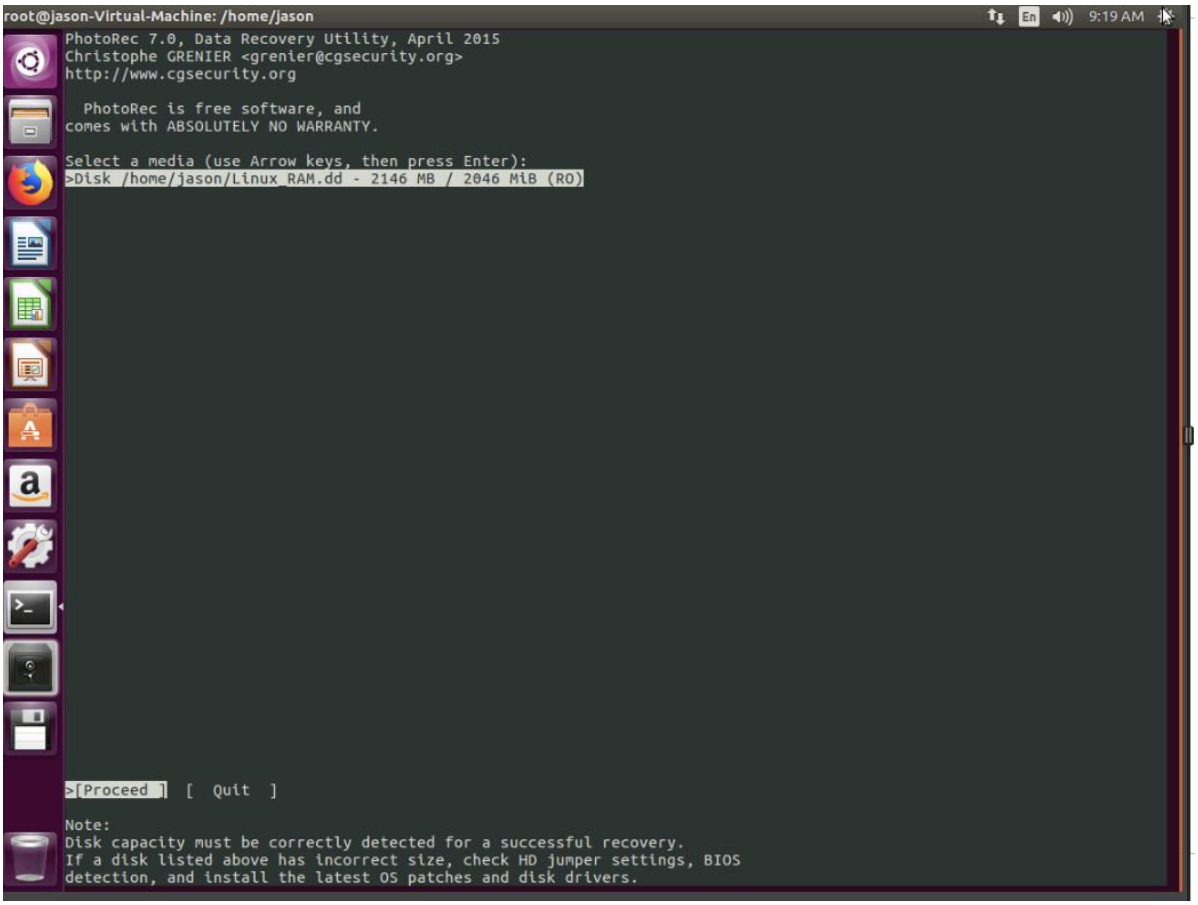
The objective of this lab is to understand how to retrieve data from a memory dump acquired on a Linux machine.

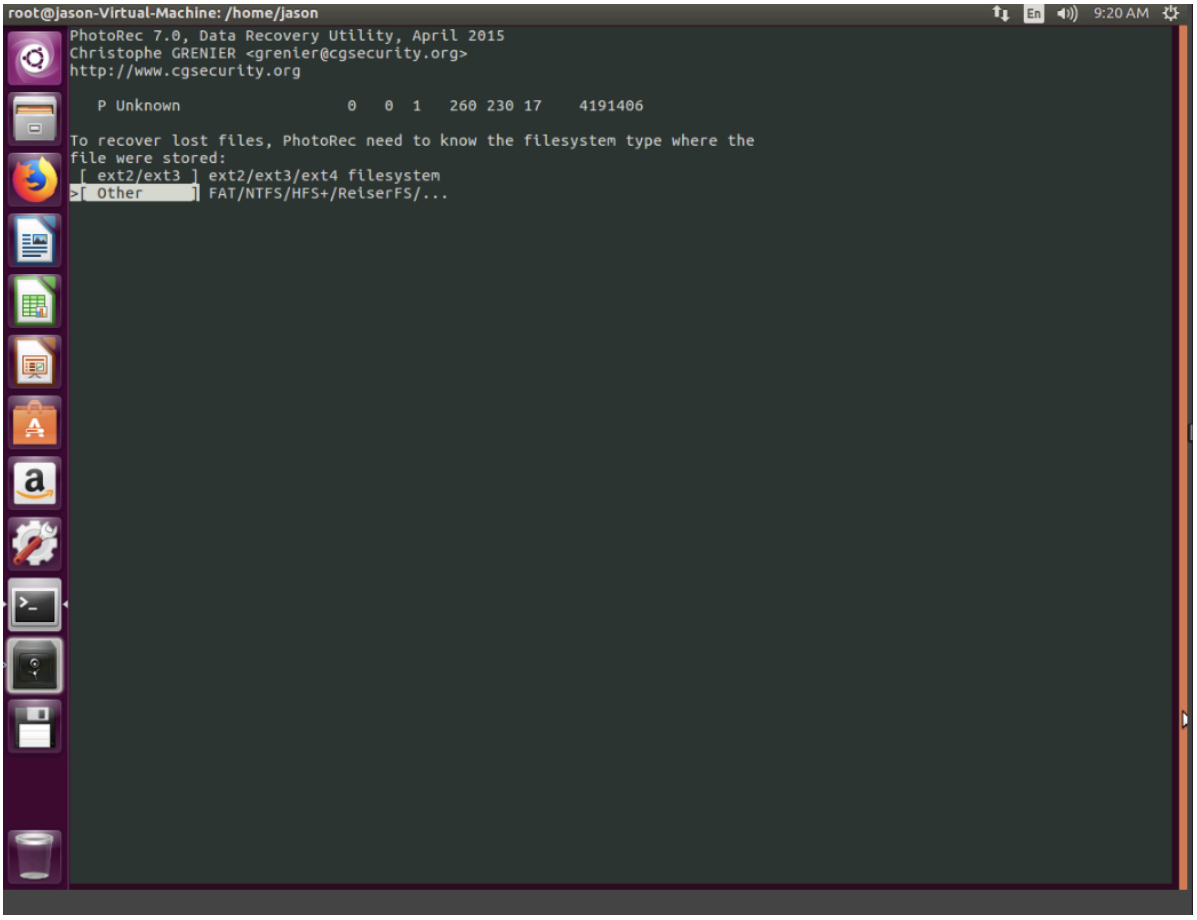
Overview of the Lab

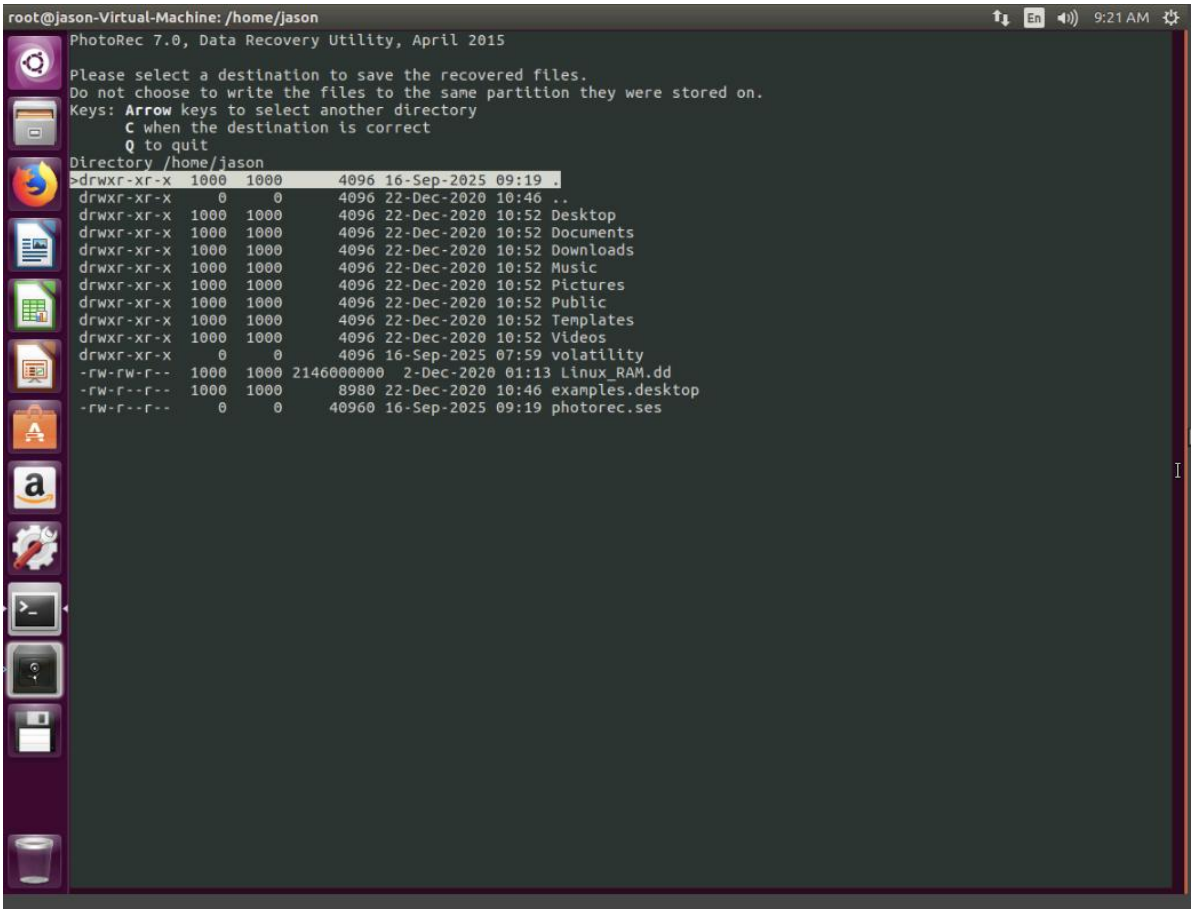
This lab familiarizes you with installing the PhotoRec tool on a Linux machine and recovering data from its memory dump.

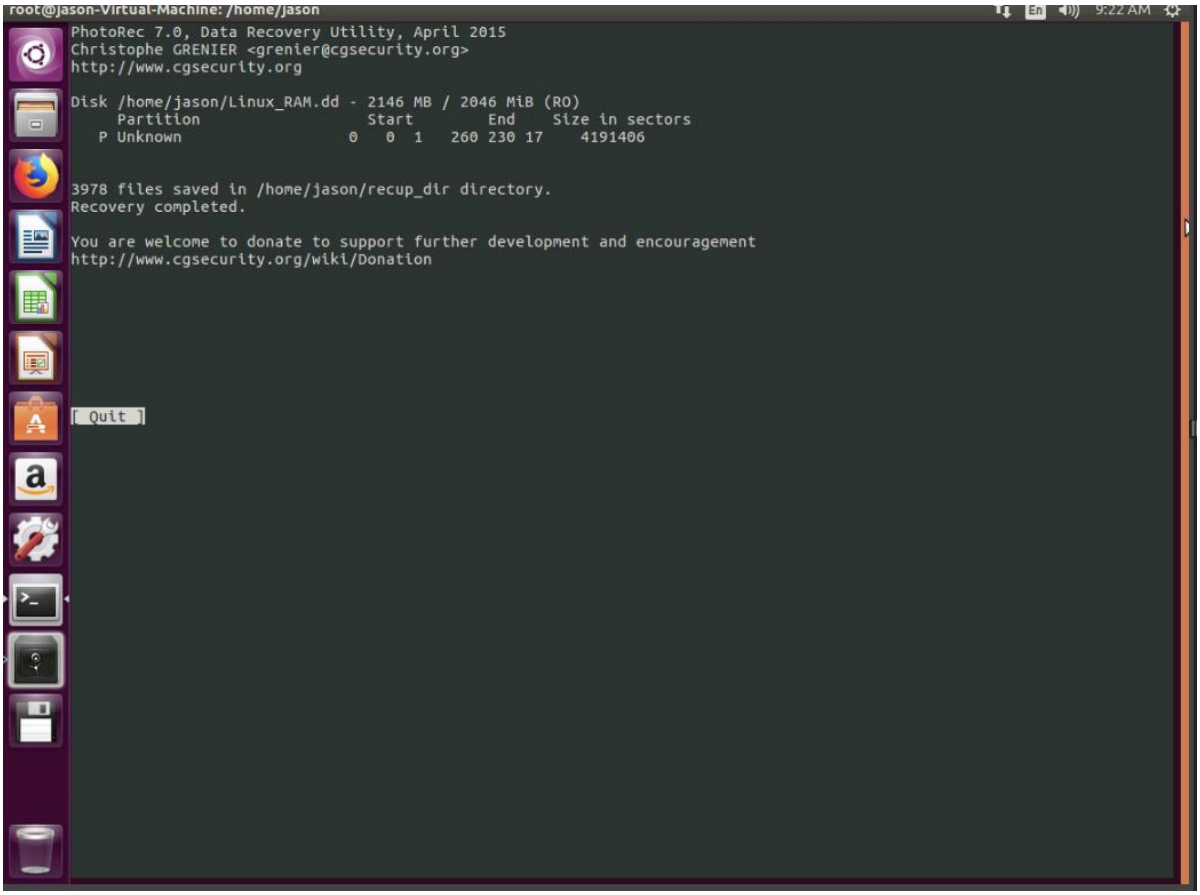


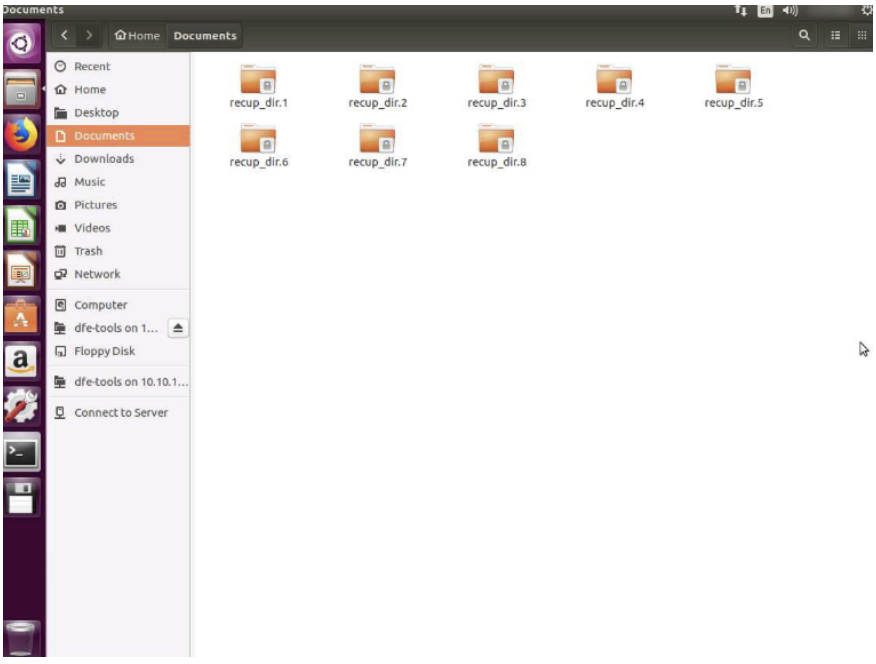

root@jason-Virtual-Machine: /home/jason
En
9:23 AM
jason@jason-Virtual-Machine:~$ sudo su
[sudo] password for jason:
root@jason-Virtual-Machine:/home/jason# apt install testdisk
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
testdisk
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 324 kB of archives.
After this operation, 1,241 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu xenial/universe amd64 testdisk amd64 7.0-1 [324 kB]
Fetched 324 kB in 2s (162 kB/s)
Selecting previously unselected package testdisk.
(Reading database ... 205055 files and directories currently installed.)
Preparing to unpack .../testdisk_7.0-1_amd64.deb ...
Unpacking testdisk (7.0-1) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up testdisk (7.0-1) ...
root@jason-Virtual-Machine:/home/jason# potorec Linux_RAM.dd
No command 'potorec' found, did you mean:
Command 'photorec' from package 'testdisk' (universe)
potorec: command not found
root@jason-Virtual-Machine:/home/jason# sudo /usr/bin/photorec /home/jason/Linux_RAM.dd
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
root@jason-Virtual-Machine:/home/jason#


root@jason-Virtual-Machine: /home/jason
En
9:19 AM
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.
Select a media (use Arrow keys, then press Enter):
>Disk /home/jason/Linux_RAM.dd - 2146 MB / 2046 MiB (RO)
>[Proceed] [Quit]
Note:
Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has incorrect size, check HD jumper settings, BIOS
detection, and install the latest OS patches and disk drivers.


root@jason-Virtual-Machine: /home/jason
En
9:20 AM
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
P Unknown 0 0 1 260 230 17 4191406
To recover lost files, PhotoRec need to know the filesystem type where the
file were stored:
[ext2/ext3] ext2/ext3/ext4 filesystem
>[Other] FAT/NTFS/HFS+/ReiserFS/...


root@jason-Virtual-Machine: /home/jason
En
9:21 AM
PhotoRec 7.0, Data Recovery Utility, April 2015
Please select a destination to save the recovered files.
Do not choose to write the files to the same partition they were stored on.
Keys: Arrow keys to select another directory
C when the destination is correct
Q to quit
Directory /home/jason
>drwxr-xr-x 1000 1000 4096 16-Sep-2025 09:19 .
drwxr-xr-x 0 0 4096 22-Dec-2020 10:46 ..
drwxr-xr-x 1000 1000 4096 22-Dec-2020 10:52 Desktop
drwxr-xr-x 1000 1000 4096 22-Dec-2020 10:52 Documents
drwxr-xr-x 1000 1000 4096 22-Dec-2020 10:52 Downloads
drwxr-xr-x 1000 1000 4096 22-Dec-2020 10:52 Music
drwxr-xr-x 1000 1000 4096 22-Dec-2020 10:52 Pictures
drwxr-xr-x 1000 1000 4096 22-Dec-2020 10:52 Public
drwxr-xr-x 1000 1000 4096 22-Dec-2020 10:52 Templates
drwxr-xr-x 1000 1000 4096 22-Dec-2020 10:52 Videos
drwxr-xr-x 0 0 4096 16-Sep-2025 07:59 volatility
-rw-rw-r-- 1000 1000 2146000000 2-Dec-2020 01:13 Linux_RAM.dd
-rw-r--r-- 1000 1000 8980 22-Dec-2020 10:46 examples.desktop
-rw-r--r-- 0 0 40960 16-Sep-2025 09:19 photorec.ses


root@jason-Virtual-Machine: /home/jason
En
9:22 AM
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
Disk /home/jason/Linux_RAM.dd - 2146 MB / 2046 MiB (RO)
Partition Start End Size in sectors
P Unknown 0 0 1 260 230 17 4191406
3978 files saved in /home/jason/recup_dir directory.
Recovery completed.
You are welcome to donate to support further development and encouragement
http://www.cgsecurity.org/wiki/Donation
[Quit]


Documents
En
Home
Documents
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Network
Computer
dfe-tools on 1...
Floppy Disk
dfe-tools on 10.10.1...
Connect to Server
recup_dir.1
recup_dir.2
recup_dir.3
recup_dir.4
recup_dir.5
recup_dir.6
recup_dir.7
recup_dir.8

Module 07: Linux and Mac Forensics – Lab 1 Summary

This lab focused on performing forensic analysis on a Linux memory dump to investigate a data breach at a technology firm. Using the Volatility Framework, the objectives were to create a Linux kernel profile for memory analysis and examine a RAM dump for malicious activity or deleted data. During the lab, several challenges were encountered, including difficulties with cloning the Volatility repository, building the kernel profile, handling file path and syntax issues, and ensuring proper recognition of the RAM dump. Despite these obstacles, the lab reinforced skills in memory forensics, Linux system analysis, and evidence extraction from volatile memory, while emphasizing careful attention to file locations, command syntax, and troubleshooting common Linux environment issues.