LINUX FORENSICS FUNDAMENTALS

A report submitted by group NWB for Cyber Security and Digital Forensics

Student Name	Registration No.
Aashish Kumar Ojha	317506408001
Arshatullah Mohammed	317506408005
Bindu Priya Bugatha	317506408007
Dakshit Raj Pediredla	317506408009
Mona Choudhrani	317506408024
Sai Abhiram Edupuganti	317506408039
Sandeep Tammineni	317506408044
Satya Venkata Lakshmi Supriya Cha	317506408046
Sri Rammanikanta Garapati	317506408050
Uma Basaveswara Rao Kurra	317506408055
Veda Upasan Pedagadi	317506408057

Course Teacher: Prof. V. Valli Kumari

01.02.2021

4/6 Integrated BTech/MTech NW

Department of Computer Science and Systems Engineering, AUCE(A), Andhra University

INTRODUCTION

"Over the last quarter century, legal requirements have increased the prevalence of and reliance upon computer forensics."

For forensic investigation, LINUX is a powerful tool. It helps in maintaining the integrity of evidence, chain of custody and also for memory acquisition.

Memory acquisition is becoming an armory for the incident response teams, forensic investigators and examiners. It is the procedure of copying the contents of physical memory to another storage device for preservation and investigation without interrupting the main memory. For modern systems it uses Kernel modules / objects. It also known as capturing, dumping, sampling.

PROBLEM STATEMENT

Memory acquisition on LINUX system

- On a partition-hard disk using *fdisk* command
- On volatile memory using LiME tool

PRE-REQUISITES AND TOOLS

1. Linux System (UBUNTU)
2. LiME (Linux Memory Extractor) Tool
3. Hashing Tools

PROCEDURE

For creating memory image of Disk

1. Open the Terminal. Use *fdisk* commands for view, create, delete, change, resize, copy and move partitions on a hard drive.
    a. *fdisk -h* (To see the help message and listing of all options)
    b. *fdisk -l* (to list the partitions on the system)
2. Use *dd* command for creating a memory image of a disk partition.

    dd if=/dev/sbd2 of=image.001 bs=1M status=progress

For creating memory image of volatile memory (RAM)

1. Clone the LiME (Linux Memory Extractor) tool from GitHub. (*sudo git clone https://github.com/504ensicsLabs/LiME.git*)
2. Change the directory (*cd LiME/src/*).
3. Using *make* command create the Kernel object.
4. Now create the memory image (*sudo insmod ./lime-5.8.0-38-generic.ko "path=../memo.mem format=raw"*)
5. Using hashing methods generate a hash value (*md5sum memo.mem*)
6. These hash values are used as evidence in the court in place huge memory files.
7. These memory files are analyzed using tools like FATKit, WMFT, Volatility Framework.

RESULTS

```
veda@Ubuntu-VEDA:~$ fdisk -h

Usage:
 fdisk [options] <disk>      change partition table
 fdisk [options] -l [<disk>] list partition table(s)

Display or manipulate a disk partition table.

Options:
 -b, --sector-size <size>      physical and logical sector size
 -B, --protect-boot            don't erase bootbits when creating a new label
 -c, --compatibility[=<mode>]  mode is 'dos' or 'nondos' (default)
 -L, --color[=<when>]          colorize output (auto, always or never)
                                 colors are enabled by default
 -l, --list                    display partitions and exit
 -o, --output <list>           output columns
 -t, --type <type>             recognize specified partition table type only
 -u, --units[=<unit>]          display units: 'cylinders' or 'sectors' (default)
 -s, --getsz                   display device size in 512-byte sectors [DEPRECATED]
     --bytes                   print SIZE in bytes rather than in human readable format
 -w, --wipe <mode>             wipe signatures (auto, always or never)
 -W, --wipe-partitions <mode>  wipe signatures from new partitions (auto, always or never)

 -C, --cylinders <number>      specify the number of cylinders
 -H, --heads <number>          specify the number of heads
 -S, --sectors <number>        specify the number of sectors per track

 -h, --help                    display this help
 -V, --version                 display version

Available output columns:
 gpt: Device Start End Sectors Size Type Type-UUID Attrs Name UUID
 dos: Device Start End Sectors Cylinders Size Type Id Attrs Boot End-C/H/S
      Start-C/H/S
 bsd: Slice Start End Sectors Cylinders Size Type Bsize Cpg Fsize
 sgi: Device Start End Sectors Cylinders Size Type Id Attrs
 sun: Device Start End Sectors Cylinders Size Type Id Flags

For more details see fdisk(8).
```

Fig 1. *fdisk -h* (To see the help message and listing of all options)

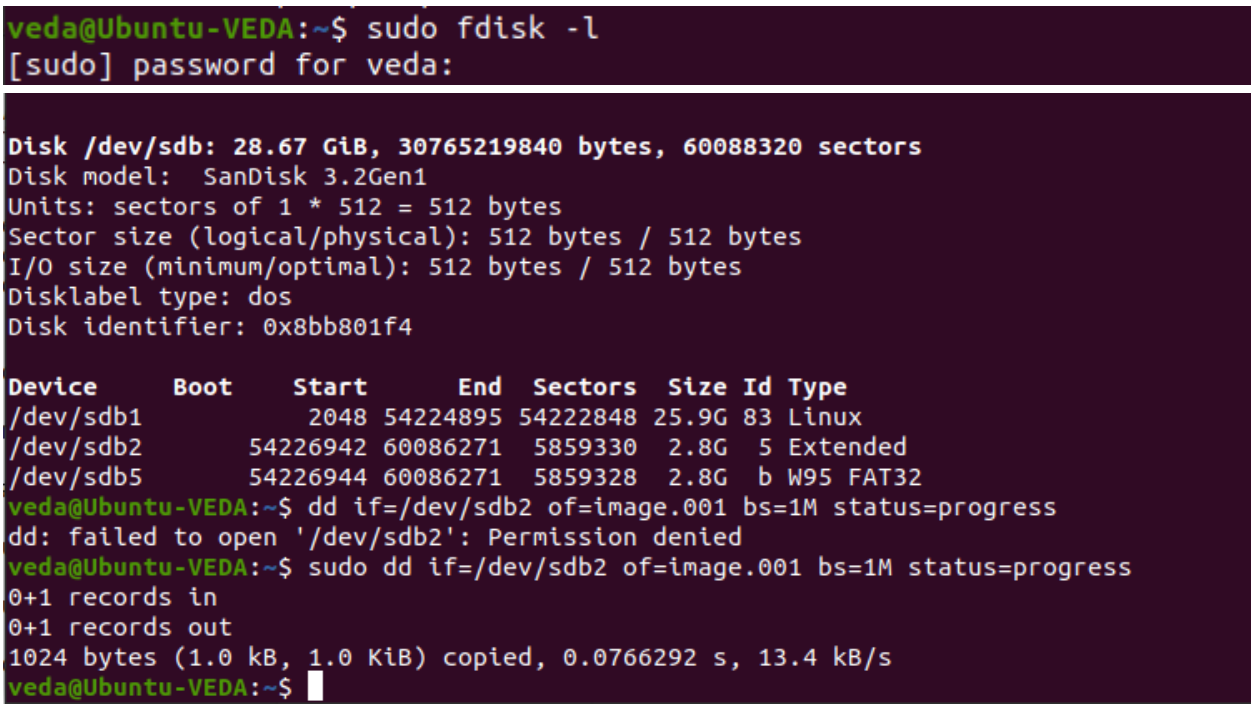

Fig 2. List of the partitions and creating memory image

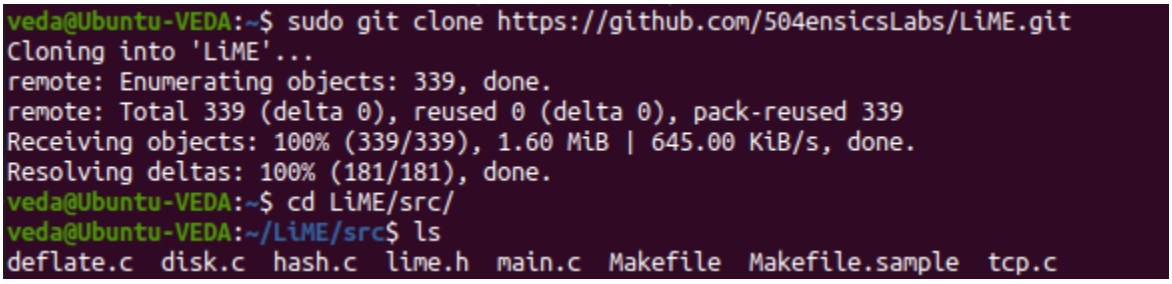

Fig 3. Cloning the *LiME* tool

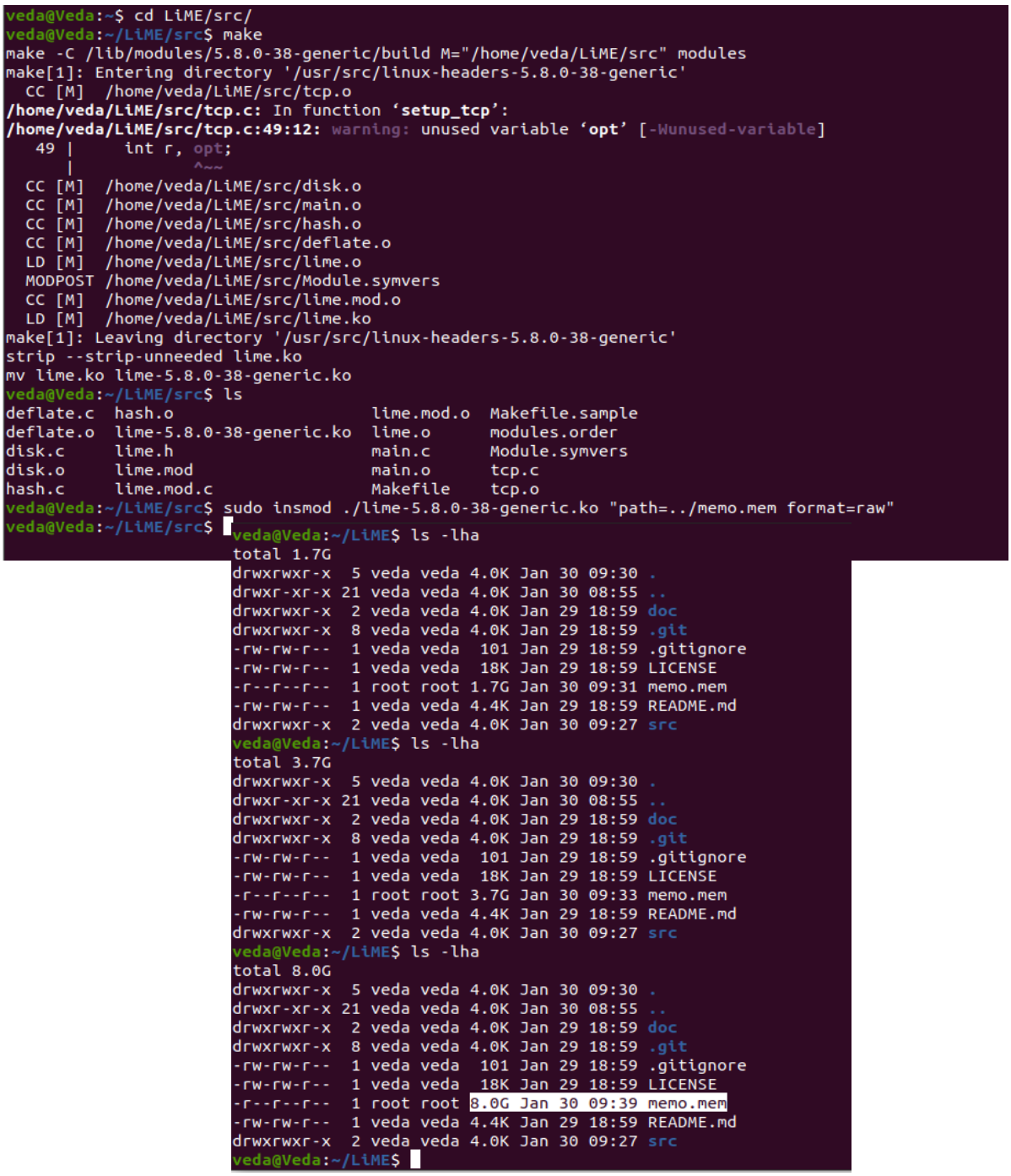

Fig 4. Creating Kernel object and memory image.

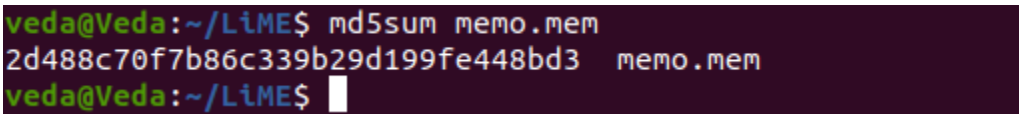

Fig 5. Creating hash value

CONCLUSION

Forensics professional should use these methods to investigate and identify attacks or malicious behaviors that do not leave detectable traces on hard drive. For further analyzing of the memory files, some tools like FATKit, WMFT, Volatility Framework must be used.

REFERENCES

1. https://www.oreilly.com/library/view/the-art-of/9781118824993/c04.xhtml
2. https://en.wikipedia.org/wiki/Fdisk
3. https://www.youtube.com/watch?v=_7Tq8dcmP0k
4. https://www.sans.org/reading-room/whitepapers/forensics/techniques-tools-recovering-analyzing-data-volatile-memory-33049