PRACTICAL-10

AIM

Perform Live / Memory Analysis on a Linux OS and prepare a detailed report.

IMPLEMENTATION

- Step 1: Download from https://github.com/504ensicsLabs/LiME

```
kali@kali:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
kali@kali:~$ git --version
git version 2.26.2
kali@kali:~$ git clone https://github.com/504ensicsLabs/LiME.git
Cloning into 'LiME' ...
remote: Enumerating objects: 31, done.
remote: Counting objects: 100% (31/31), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 323 (delta 12), reused 19 (delta 7), pack-reused 292
Receiving objects: 100% (323/323), 1.61 MiB | 71.00 KiB/s, done.
Resolving deltas: 100% (163/163), done.
```

- Step 2: Now go to src folder in LiME and view the contents.

```
kali@kali:~/Downloads$ cd LiME/
kali@kali:~/Downloads/LiME$ ls
doc  LICENSE  README.md  src
kali@kali:~/Downloads/LiME$ cd src
kali@kali:~/Downloads/LiME/src$ ls
deflate.c  disk.c  hash.c  lime.h  main.c  Makefile  Makefile.sample  tcp.c
```

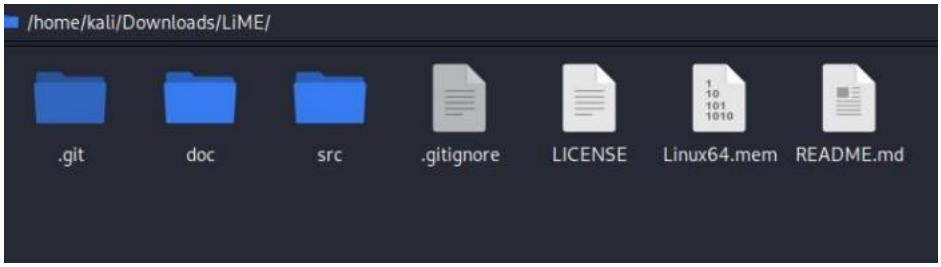
- Step 3: Now run the make command to compile it.

```
kali@kali:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
kali@kali:~$ git --version
git version 2.26.2
kali@kali:~$ git clone https://github.com/504ensicsLabs/LiME.git
Cloning into 'LiME' ...
remote: Enumerating objects: 31, done.
remote: Counting objects: 100% (31/31), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 323 (delta 12), reused 19 (delta 7), pack-reused 292
Receiving objects: 100% (323/323), 1.61 MiB | 71.00 KiB/s, done.
Resolving deltas: 100% (163/163), done.
kali@kali:~$ ls
Desktop  Documents  Downloads  LiME  Music  Pictures  Public  Templates  Videos
kali@kali:~$ cd LiME/
kali@kali:~/LiME$ ls
doc  LICENSE  README.md  src
kali@kali:~/LiME$ cd src
kali@kali:~/LiME/src$ ls
deflate.c  disk.c  hash.c  lime.h  main.c  Makefile  Makefile.sample  tcp.c
```

Step 4: Run the command “sudo insmod ./lime-5.5.0-kali2-amd64.ko “path= ../Linux64.mem format=raw”

```
kali@kali:~/LiME/src$ sudo insmod ./lime-5.5.0-kali2-amd64.ko "path=../Linux64.mem format=raw"
[sudo] password for kali:
```

Step 5: Creating a hash value for the memory image i.e., of Linux64.mem.



CONCLUSION

In this practical, we learnt to perform live analysis of memory in linux.