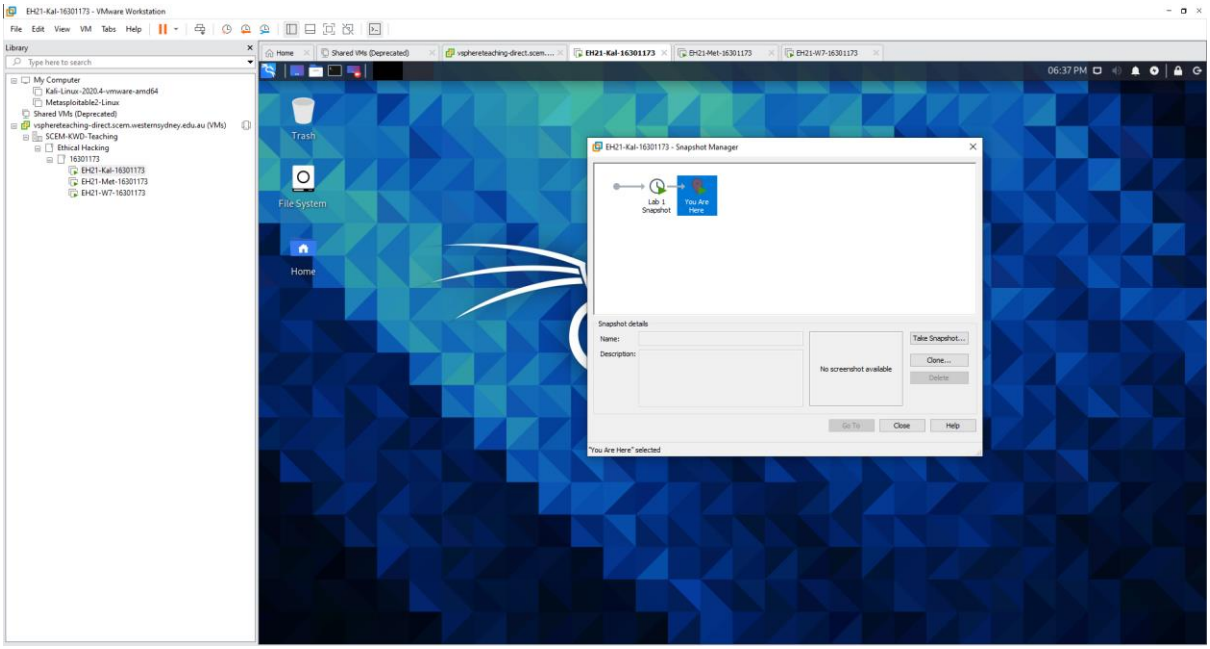
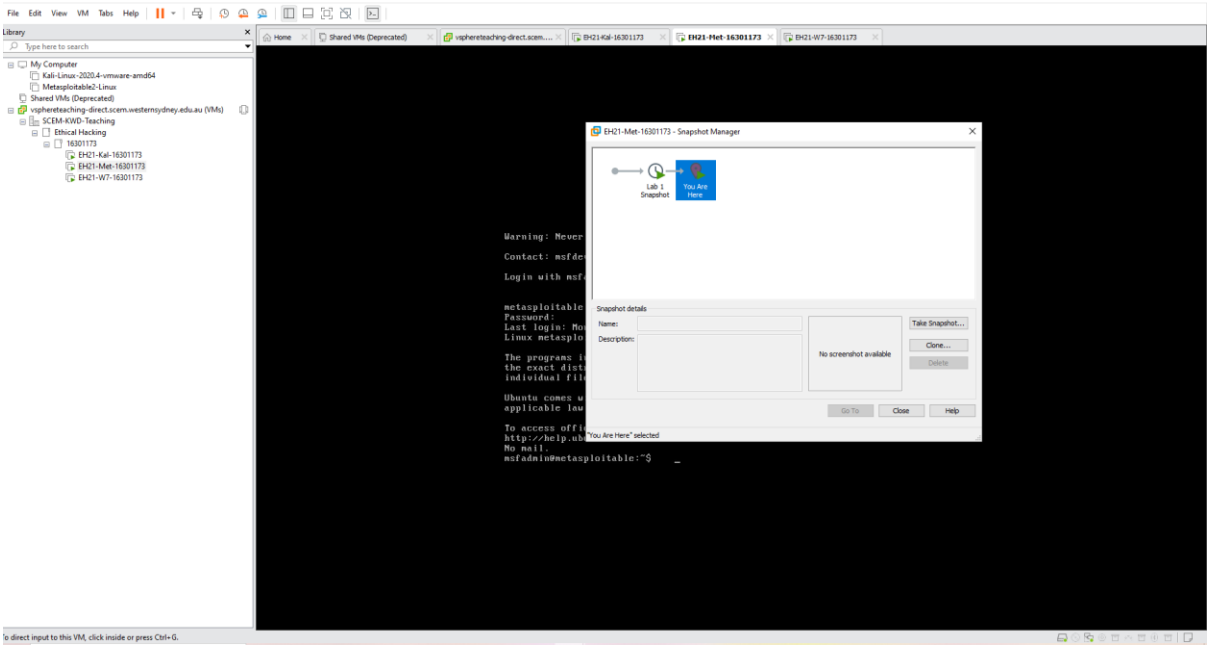
Part 1:

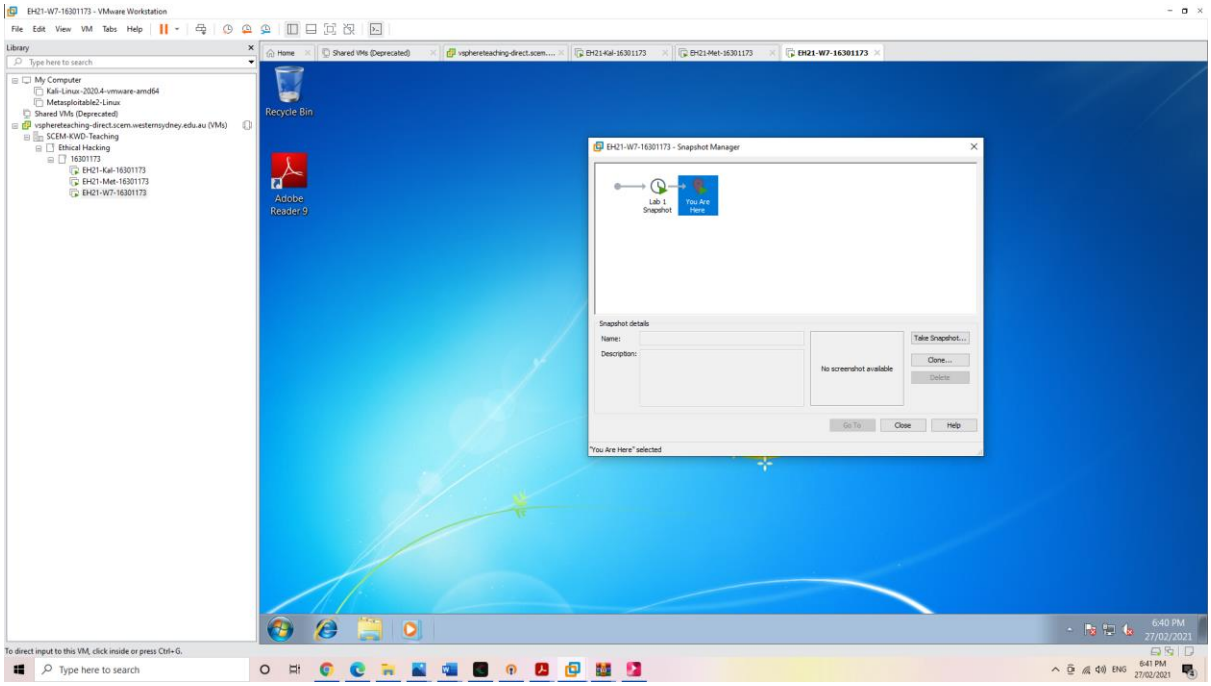
1.1 Screenshot KALI snapshot



1.2 Screenshot Metasploitable2 snapshot



1.3 Screenshot Windows 7 snapshot



PART 2: WINDOWS

2.1 Use the command 'ipconfig' to determine the IP address of this VM. Write the result to your lab report.

192.168.1.101

2.2 If you need the MAC address of the VM as well, what option you should add to the 'ipconfig' command?

Ipconfig /all [/all added to ipconfig]

2.3 Use the command 'netstat -an -p tcp' to determine which TCP ports are in a listening state. Write the result to your lab report.

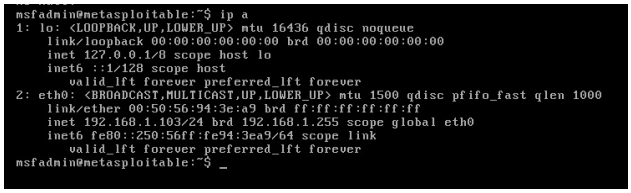
```
C:\Users\admin>netstat -an -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:23             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:554            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:10243          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49157          0.0.0.0:0              LISTENING
  TCP    192.168.1.101:139      0.0.0.0:0              LISTENING
  TCP    192.168.1.101:49163    104.119.96.124:443     ESTABLISHED
```

2.4 In your report, also explain the meanings of the options '-a' and '-n'. You can use the command ‘netstat /?’ to find out the answer. (Note: although ‘netstat’ is deprecated in Linux, it is not in Windows)

“-a” : Displays all connections and listening ports
“-n” : Displays addresses and port numbers in numerical form

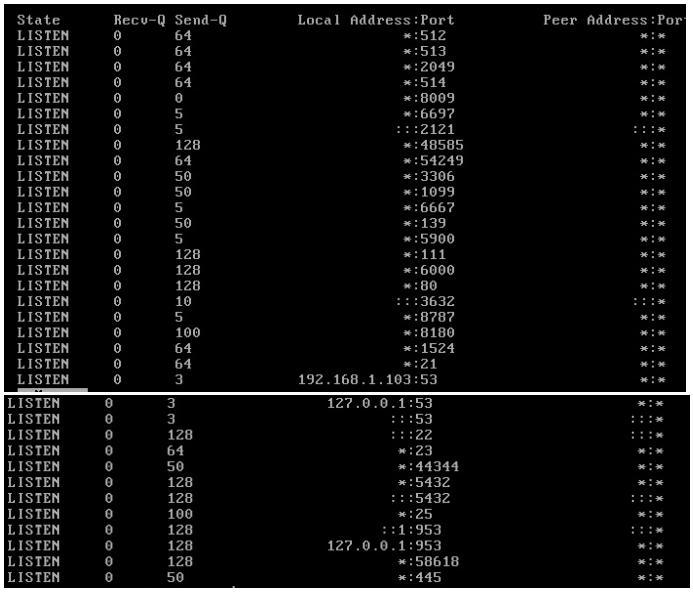
PART 3: MET

3.1 Use the 'ip a' command to show the IP address and MAC address of this VM. Write the result to your lab report. (Hint: look for the result from the output for Ethernet interface ‘eth0’)



IP Address: 192.168.1.103
MAC Address: 00:50:56:94:3e:a9

3.2 Use the command 'ss -ant | more' to determine which TCP ports are listening. Write the result to your lab report.



3.3 In your report, also explain the meanings of the options '-a', '-n', and the operator ‘|’.

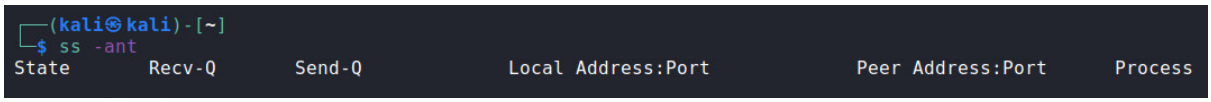
“-a”: display all sockets
“-n”: Do not try to resolve service names.
“|” : This is a pipe which connects standard out of “ss” command to the standard in of more which is another program [not a file]; and thus you can get a slower report of the command rather than it jamming the screen all at once.

PART 4: KALI

4.1 Use the 'ip a' command to show the IP address and MAC address of this VM. Write the result to your lab report. (Hint: look for the result from the output for Ethernet interface ‘eth0’)

IP Address: 192.168.1.102/24
MAC Address: 00:50:56:94:30:0d

4.2 Use the command 'ss -ant' to determine which TCP ports are listening. Write the result to your lab report.



4.3 Here you will notice that the result is very different from those of the previous two VMs. Explain this difference in your report after reading the Kali Network Service Policy, which can be found at:

https://www.kali.org/docs/policy/kali-linux-network-service-policies/. (This site may be blocked in campus network, but accessible in your home network.) You only need to read the first paragraph of this policy.

Kali Linux is a penetration testing toolkit and may potentially be used in “hostile” environments. Accordingly, Kali Linux deals with network services in a very different way than typical Linux distributions. Specifically, Kali does not enable any externally listening services by default with the goal of minimizing exposure when in a default state.

4.4 Use the command 'ip r' to determine the default gateway for this VM. Write the result to your lab report.

Default Gateway: 192.168.1.1

4.5 Ping the Win7 VM. Press 'Ctrl + C' to stop the ping. Note: In Linux, if you want to limit the number of pings, use 'ping -c <count> <destination IP>', where <count> is the number of ping probes (Eg, ping -c 6 192.16.0.2). Write the result to your lab report. If you cannot reach the Win7 VM, try to fix the problem.

```
┌──(kali㉿kali)-[~]
└─$ ping -c 10 192.168.1.101
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data.
64 bytes from 192.168.1.101: icmp_seq=1 ttl=128 time=1.42 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=128 time=0.703 ms
64 bytes from 192.168.1.101: icmp_seq=3 ttl=128 time=0.743 ms
64 bytes from 192.168.1.101: icmp_seq=4 ttl=128 time=0.787 ms
64 bytes from 192.168.1.101: icmp_seq=5 ttl=128 time=0.681 ms
64 bytes from 192.168.1.101: icmp_seq=6 ttl=128 time=0.730 ms
64 bytes from 192.168.1.101: icmp_seq=7 ttl=128 time=0.700 ms
64 bytes from 192.168.1.101: icmp_seq=8 ttl=128 time=0.666 ms
64 bytes from 192.168.1.101: icmp_seq=9 ttl=128 time=0.672 ms
64 bytes from 192.168.1.101: icmp_seq=10 ttl=128 time=0.707 ms

--- 192.168.1.101 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9162ms
rtt min/avg/max/mdev = 0.666/0.780/1.416/0.214 ms
```

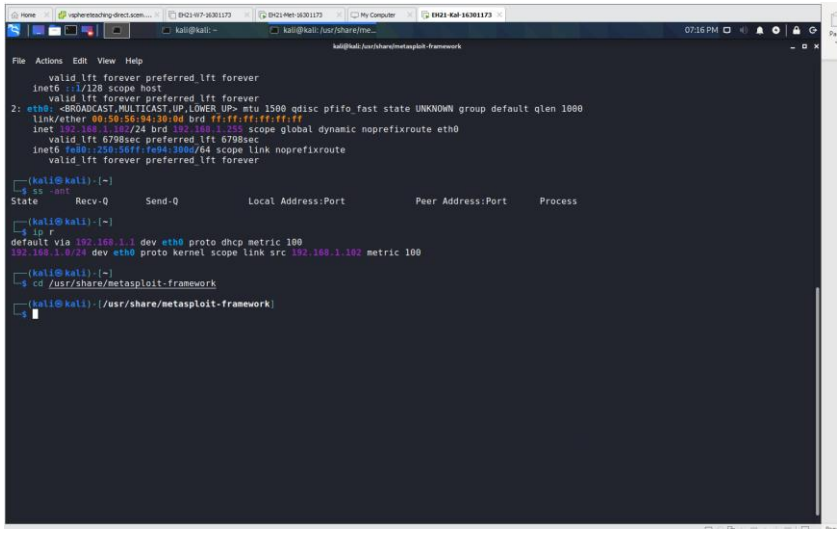
4.6 Ping the Metasploitable2 VM. Press 'Ctrl + C' to stop the ping. Write the result to your lab report. If you cannot reach the Metasploitable2 VM, try to fix the problem.

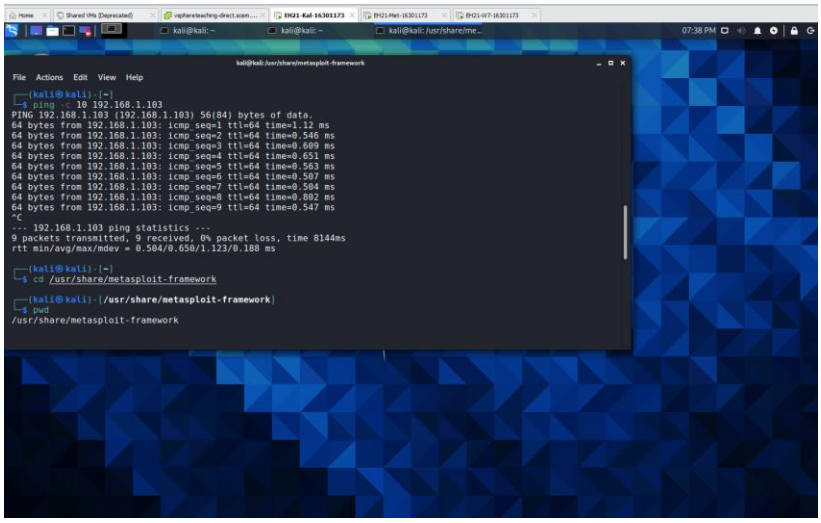
```
┌──(kali㉿kali)-[~]
└─$ ping -c 10 192.168.1.103
PING 192.168.1.103 (192.168.1.103) 56(84) bytes of data.
64 bytes from 192.168.1.103: icmp_seq=1 ttl=64 time=1.12 ms
64 bytes from 192.168.1.103: icmp_seq=2 ttl=64 time=0.546 ms
64 bytes from 192.168.1.103: icmp_seq=3 ttl=64 time=0.609 ms
64 bytes from 192.168.1.103: icmp_seq=4 ttl=64 time=0.651 ms
64 bytes from 192.168.1.103: icmp_seq=5 ttl=64 time=0.563 ms
64 bytes from 192.168.1.103: icmp_seq=6 ttl=64 time=0.507 ms
64 bytes from 192.168.1.103: icmp_seq=7 ttl=64 time=0.504 ms
64 bytes from 192.168.1.103: icmp_seq=8 ttl=64 time=0.802 ms
64 bytes from 192.168.1.103: icmp_seq=9 ttl=64 time=0.547 ms
^C
--- 192.168.1.103 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8144ms
rtt min/avg/max/mdev = 0.504/0.650/1.123/0.188 ms
```

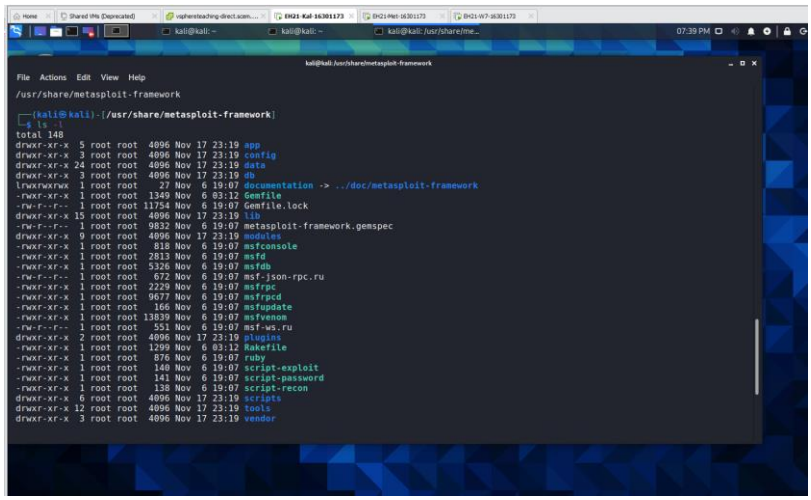
PART 5:

5.1 Grab a screenshot for the results of these three commands respectively, and save the screenshots to your lab report.

'cd /usr/share/metasploit-framework', 'pwd', and 'ls -l '.





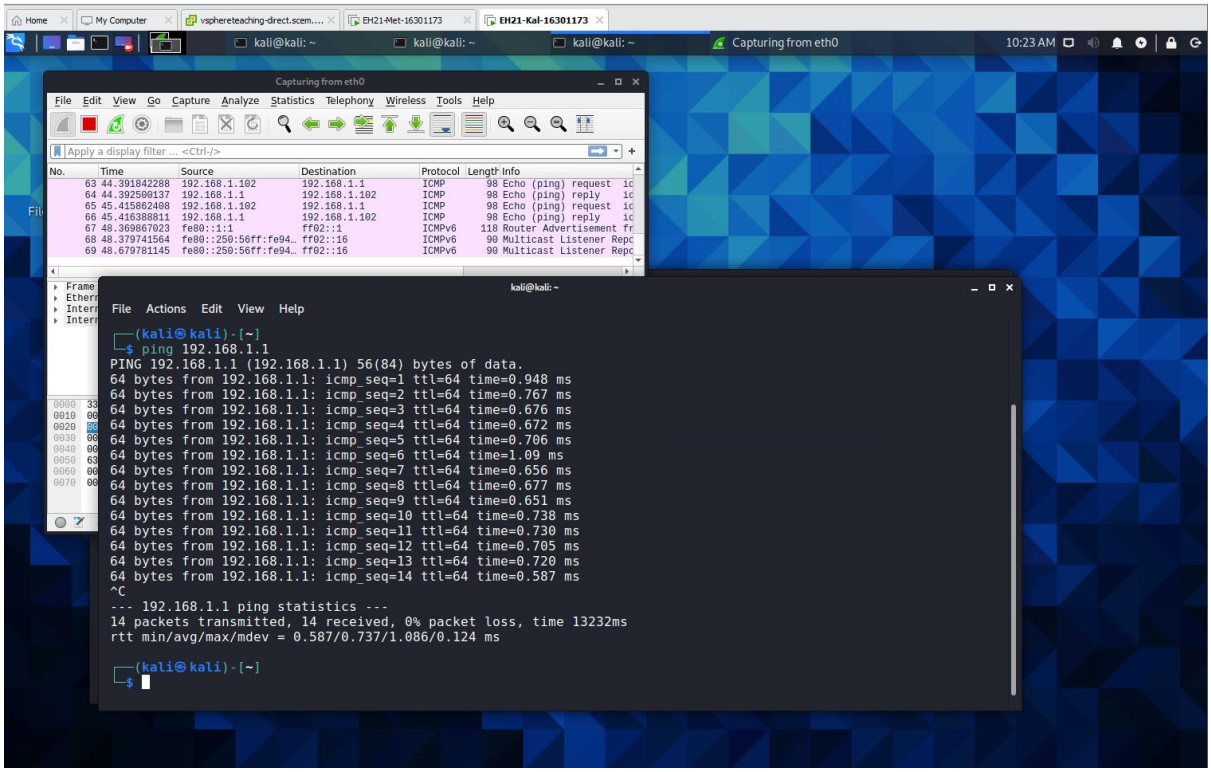


5.2 In your report, also explain the meanings of these three commands, especially, the option '-l' in 'ls -l '. (Hint: you can execute 'man ls ' to find out)

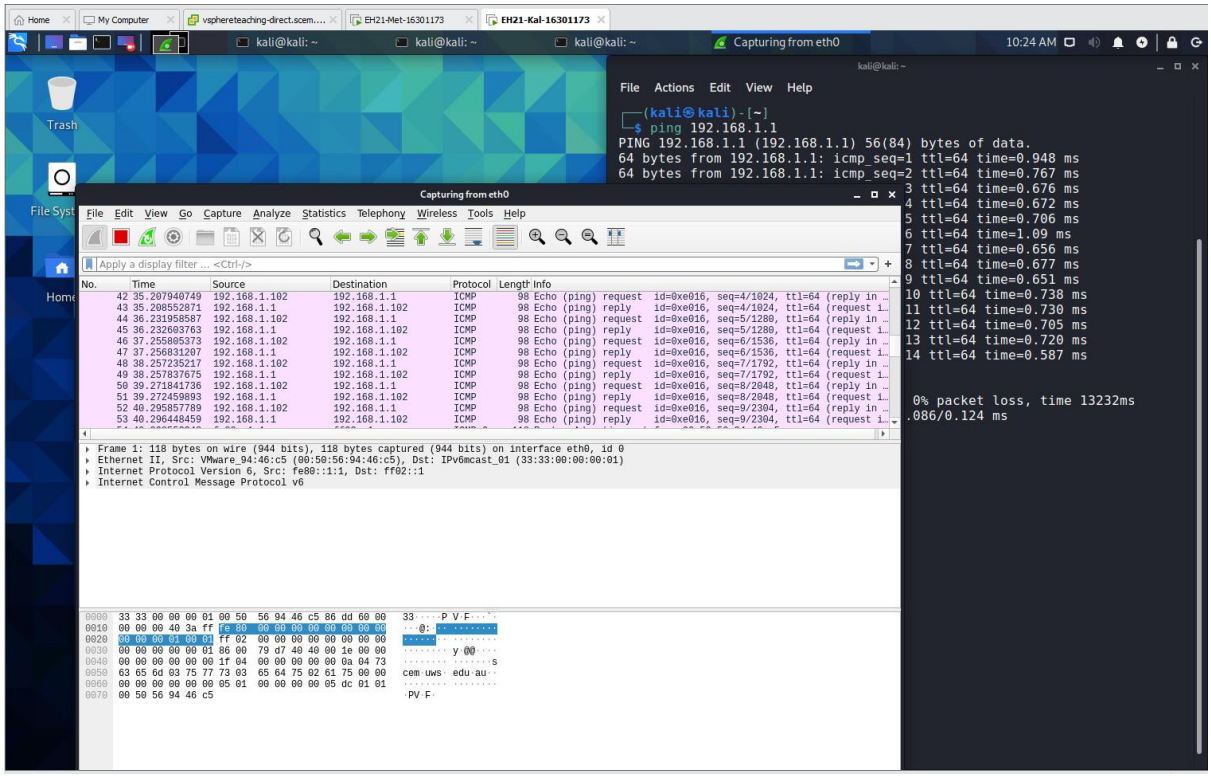
"cd" : Change directory to the directory specified
"pwd": print the name of the current working director
"ls" : list the files and folders in the current directory
"ls -l": gives a long listing with extra information about each file and their corresponding attributes; permissions, time, date and size.

PART 6:

6.1 Switch to a terminal to ping the default gateway. Press 'Ctrl + C' to stop the ping. Include a screenshot for this in your lab report.



6.2 Stop the Wireshark capture and observe the captured ping traffic. Include a screenshot about this in your lab report.



PART 7:

7.1 In your lab report, give your answer to the following cryptogram. Since you cannot play it using the website (you have to use paper and pencil instead), we offer you a hint that the first letter is ‘L’.

LOVE IS LIKE QUICKSILVER IN THE HAND LEAVE THE FINGERS OPEN AND IT STAYS CLUTCH IT AND IT DARTS AWAY

7.2 Describe at least two techniques you use for finding out the answer quickly.

- **Start with small words first [two letter ones]**
- **Looked at repetition**
- **Trial and Error**
- **Frequency analysis**