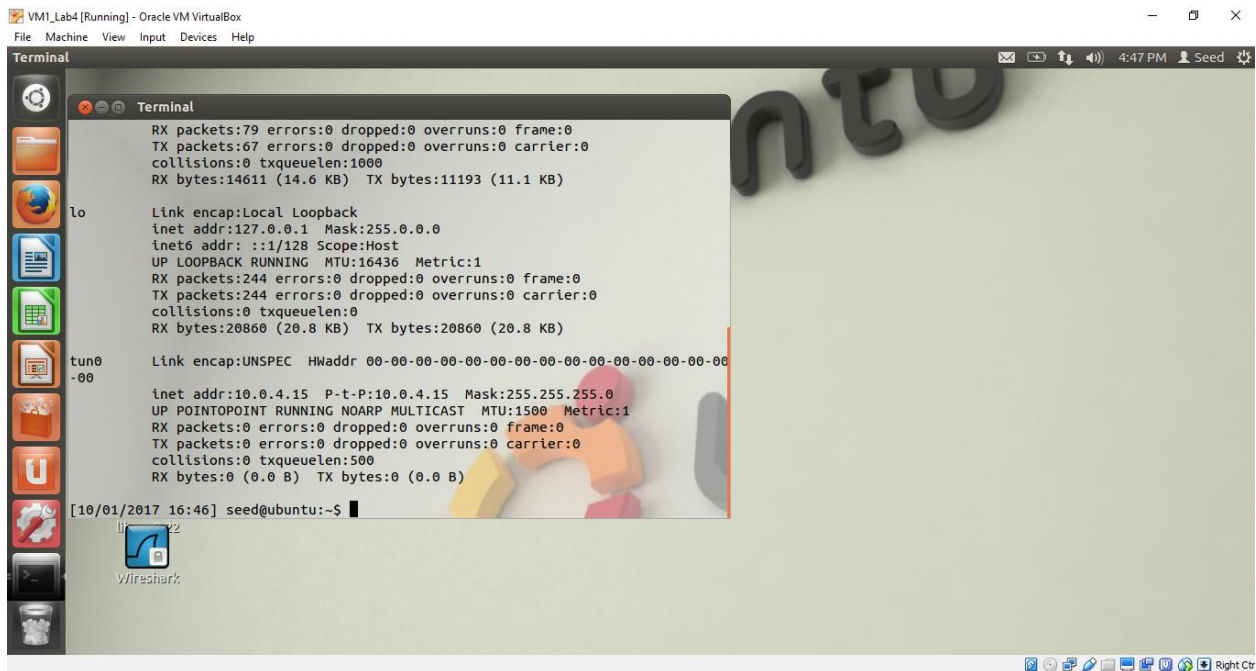


LAB ASSIGNMENT 4

SJSU ID: 012018487 NAME: NIVEDHITHA RAMARATHNAM KRISHNA

TASK 1: VM1 has tun0 interface setup complete.



The screenshot shows a terminal window titled "Terminal" within an Oracle VM VirtualBox environment. The terminal displays the output of the `ifconfig` command for the `tun0` interface. The output shows that the interface is up and running, with a link encap of UNSPEC, HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00, and IP address 10.0.4.15. The interface is connected to the local loopback interface `lo`. The terminal also shows the output of the `ifconfig` command for the `lo` interface, which is up and running with a link encap of Local Loopback, HWaddr 00:00:00:00:00:00, and IP address 127.0.0.1. The terminal prompt is `seed@ubuntu:~$`.

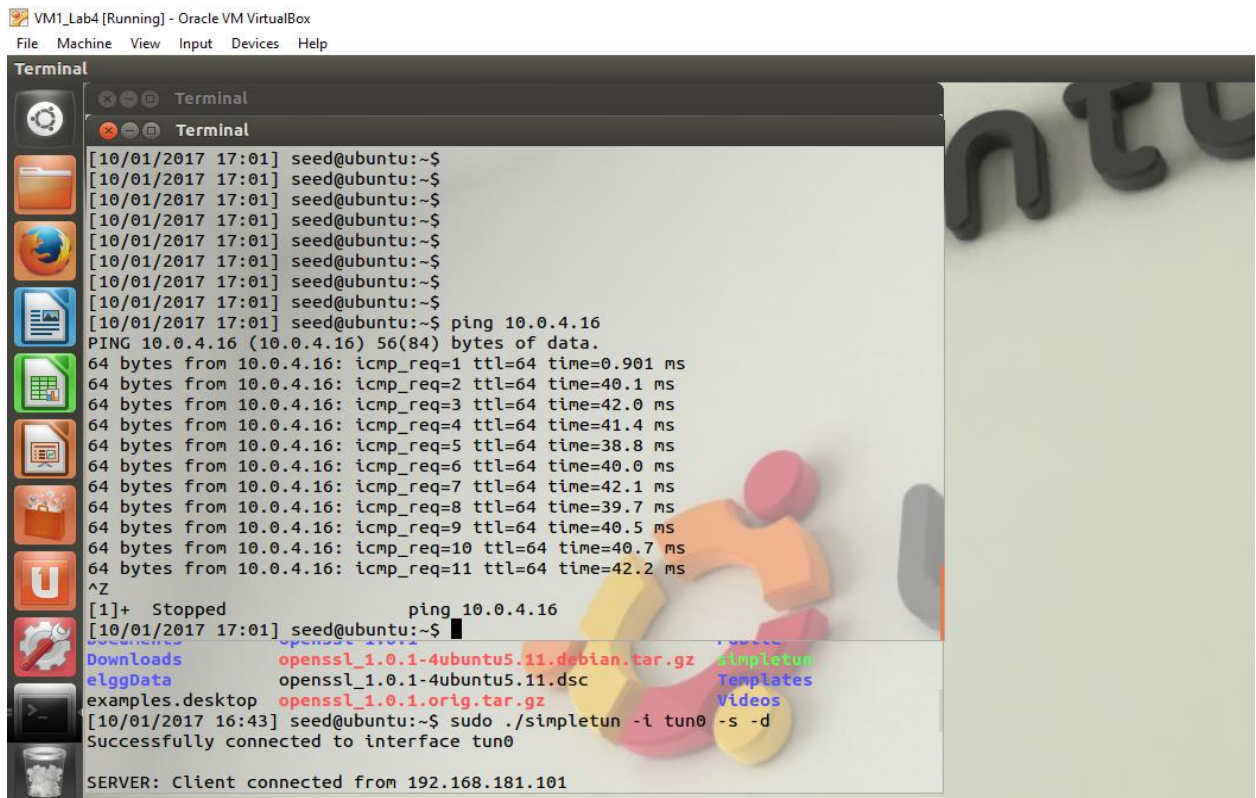
```
lo
RX packets:79 errors:0 dropped:0 overruns:0 frame:0
TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:14611 (14.6 KB) TX bytes:11193 (11.1 KB)

Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:244 errors:0 dropped:0 overruns:0 frame:0
TX packets:244 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:20860 (20.8 KB) TX bytes:20860 (20.8 KB)

tun0
Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet addr:10.0.4.15 P-t-P:10.0.4.15 Mask:255.255.255.0
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:500
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

[10/01/2017 16:46] seed@ubuntu:~$
```

Figure shows ifconfig on VM1 showing 10.0.4.15 as tunnel tun0 IP.



The screenshot shows a terminal window titled "Terminal" within an Oracle VM VirtualBox environment. The terminal displays the output of the `ping` command, showing successful results for the IP address 10.0.4.16. The output shows that the ping was successful, with 11 requests and 11 replies, all with a time of 40.1 ms. The terminal also shows the output of the `sudo ./simpletun -i tun0 -s -d` command, which successfully connects the interface `tun0` to the interface `tun0` on the host. The terminal prompt is `seed@ubuntu:~$`.

```
[10/01/2017 17:01] seed@ubuntu:~$ ping 10.0.4.16
PING 10.0.4.16 (10.0.4.16) 56(84) bytes of data:
64 bytes from 10.0.4.16: icmp_req=1 ttl=64 time=40.1 ms
64 bytes from 10.0.4.16: icmp_req=2 ttl=64 time=42.0 ms
64 bytes from 10.0.4.16: icmp_req=3 ttl=64 time=41.4 ms
64 bytes from 10.0.4.16: icmp_req=4 ttl=64 time=38.8 ms
64 bytes from 10.0.4.16: icmp_req=5 ttl=64 time=40.0 ms
64 bytes from 10.0.4.16: icmp_req=6 ttl=64 time=42.1 ms
64 bytes from 10.0.4.16: icmp_req=7 ttl=64 time=39.7 ms
64 bytes from 10.0.4.16: icmp_req=8 ttl=64 time=40.5 ms
64 bytes from 10.0.4.16: icmp_req=9 ttl=64 time=40.7 ms
64 bytes from 10.0.4.16: icmp_req=10 ttl=64 time=42.2 ms
64 bytes from 10.0.4.16: icmp_req=11 ttl=64 time=40.1 ms
^Z
[1]+  Stopped                  ping 10.0.4.16
[10/01/2017 17:01] seed@ubuntu:~$ sudo ./simpletun -i tun0 -s -d
Successfully connected to interface tun0
SERVER: Client connected from 192.168.181.101
```

Figure shows Ping sent successfully from VM1 to VM2.

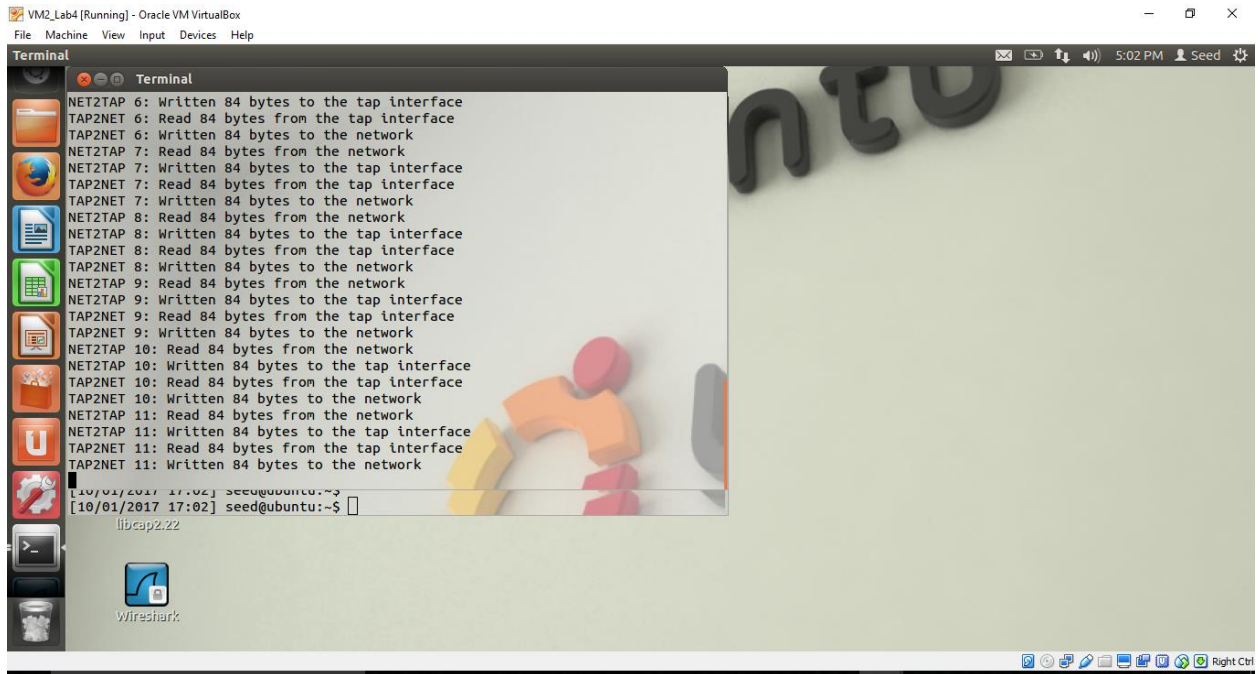


Figure shows Ping received successfully at VM2 from VM1.

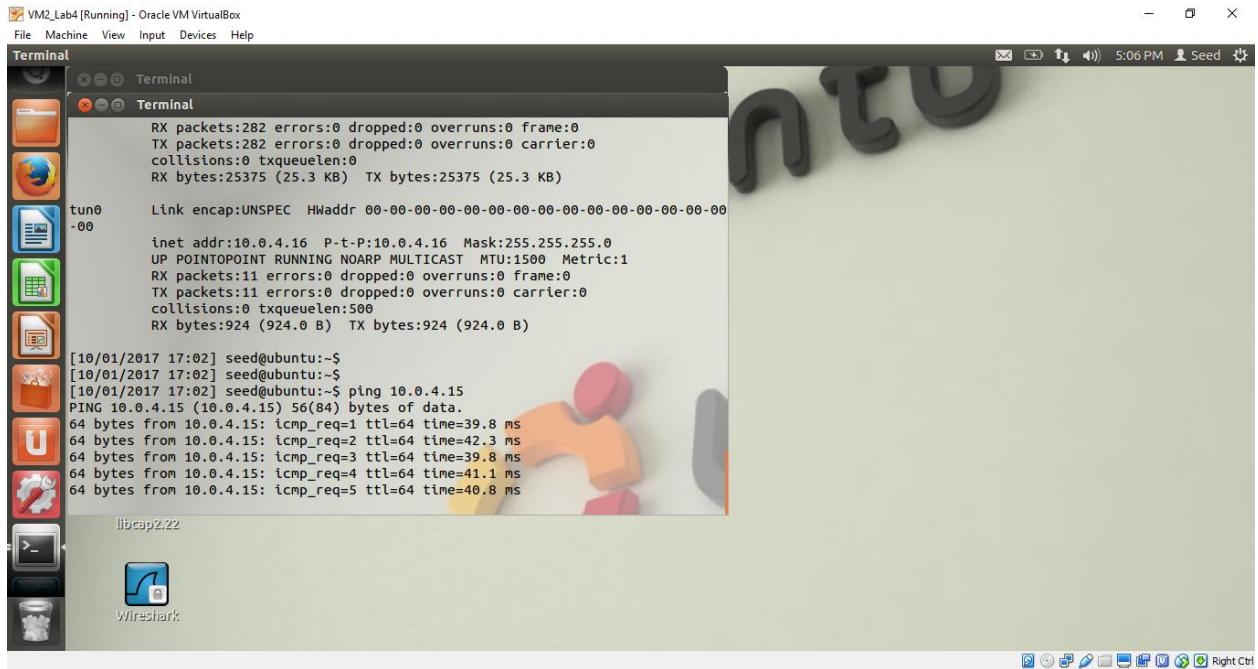


Figure shows Ping sent successfully from VM2 to VM1.



Figure shows Ping received successfully at VM1 from VM2.



Figure shows that SSH is successful from VM1 to VM2.

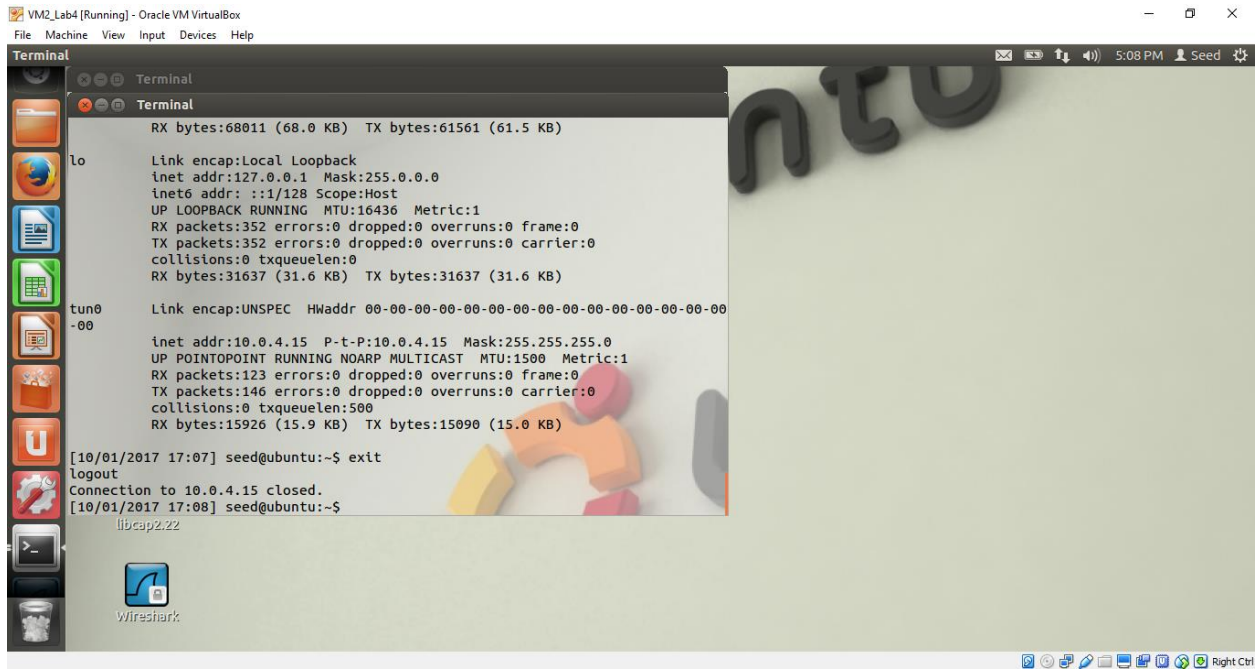


Figure shows that SSH successful from VM2 to VM1.

TASK 2:

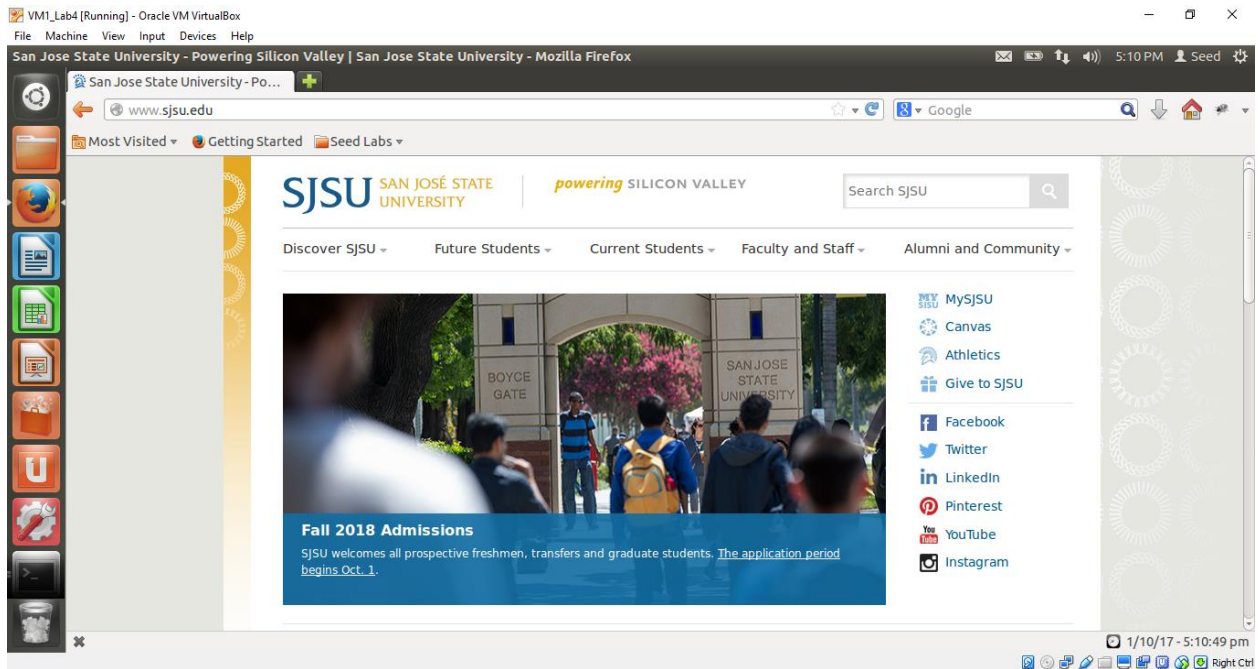


Figure shows that the website www.sjsu.edu is accessible before firewall configuration is setup on VM1.

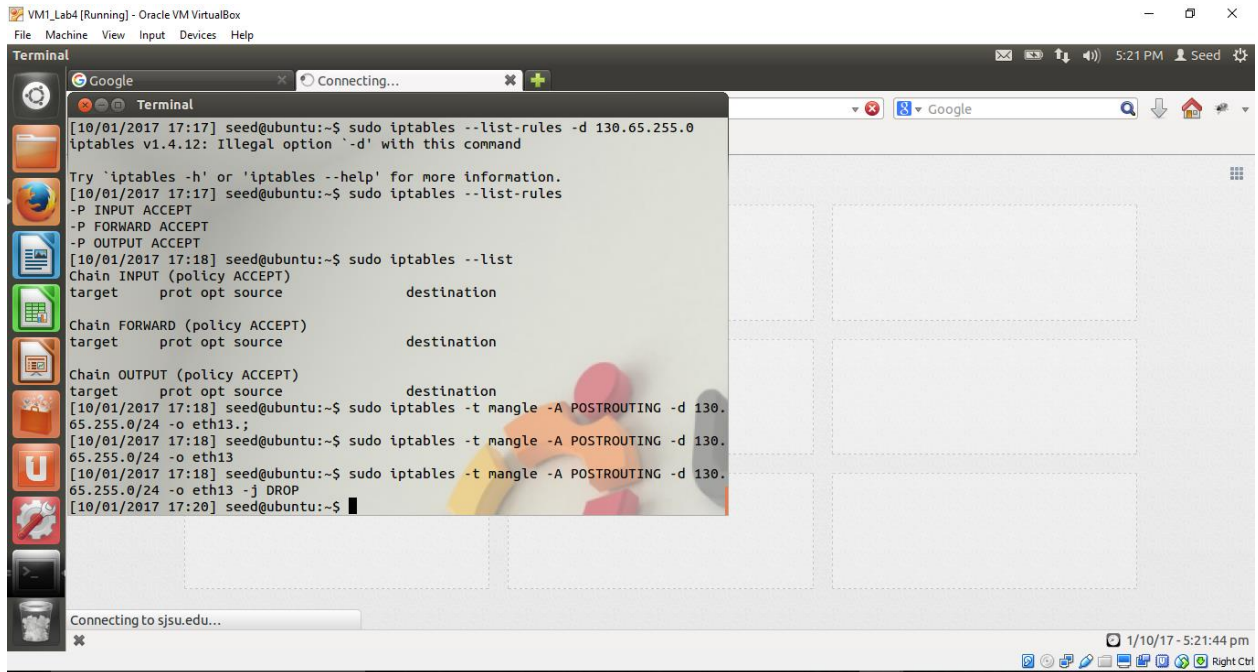


Figure shows that the website www.sjsu.edu is “dropped” from iptables at eth13 at VM1. Meaning the website is blocked at VM1.

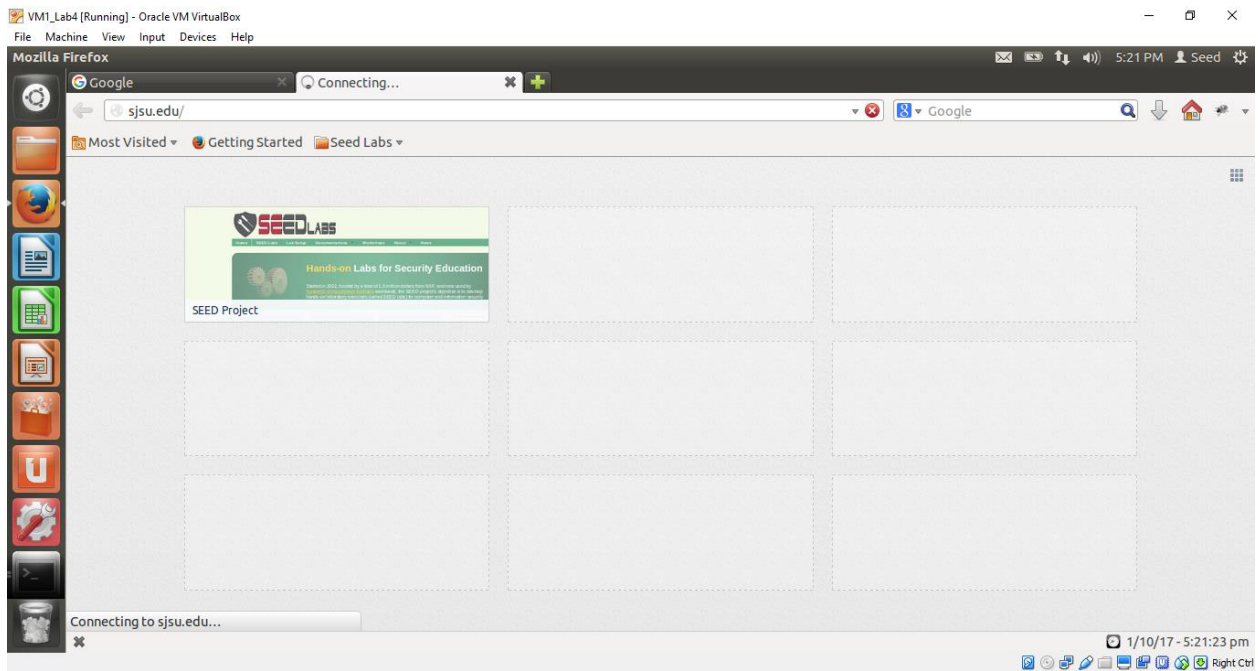


Figure shows that the site takes more time to load now at VM1.

- In this case the following IP address: 130.65.255.0/24 is added to iptables list under “DROP” target. This will stop the NAT connection between the machine (here VM1) and the IP address at given NAT port in this case eth13. Hence when trying to access the website from firefox it loads for a long time as the site is blocked. Finally, a “Connection timed out” error is received which says to check the system’s firewall settings. This shows that Firewall setup is successful.

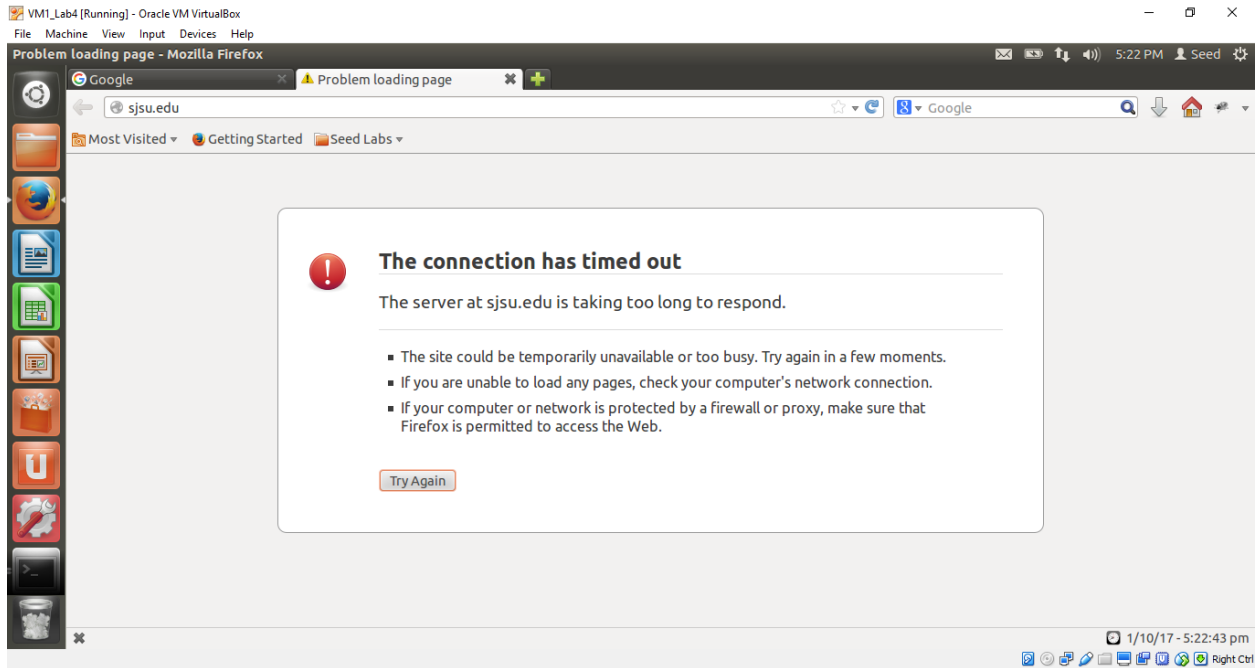


Figure shows that the website www.sjsu.edu is no more accessible on VM1 because of the firewall configuration is setup.

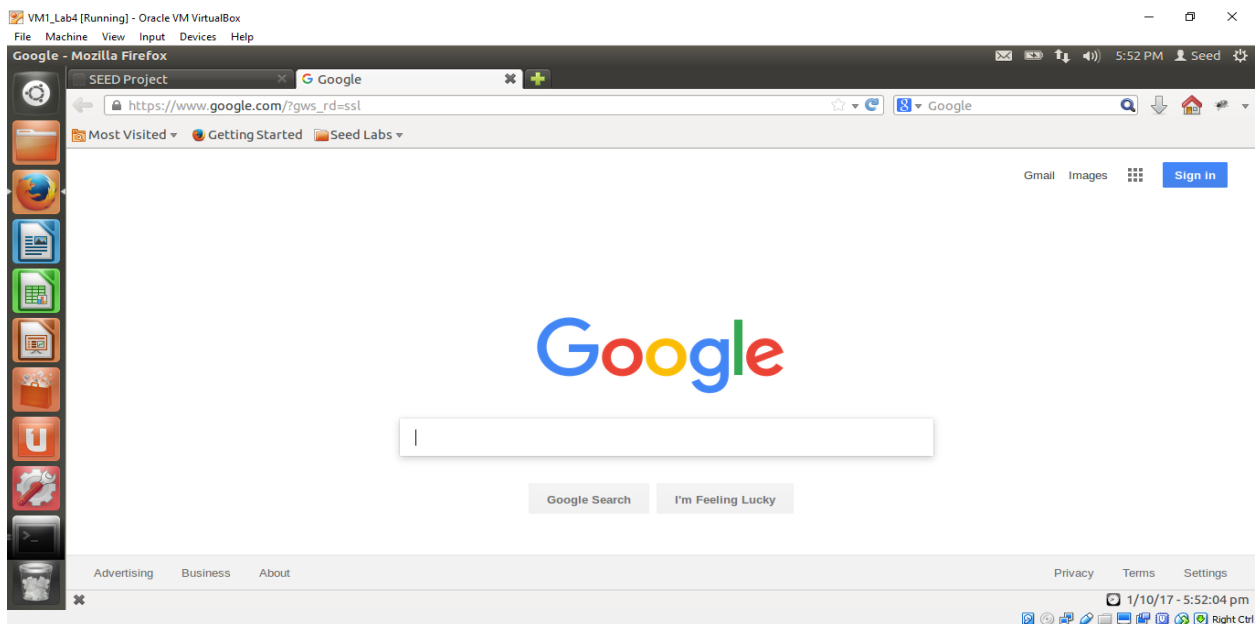
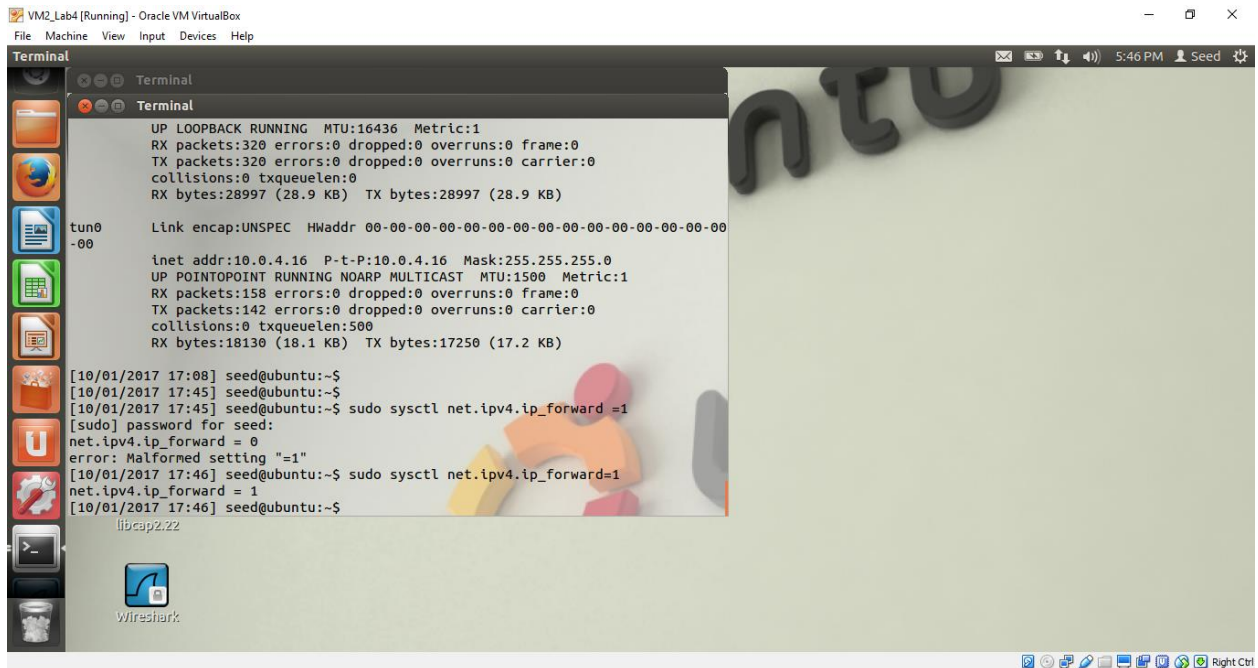


Figure shows that the other websites (www.google.com) is accessible in VM1 because it is not blocked.

TASK 3:



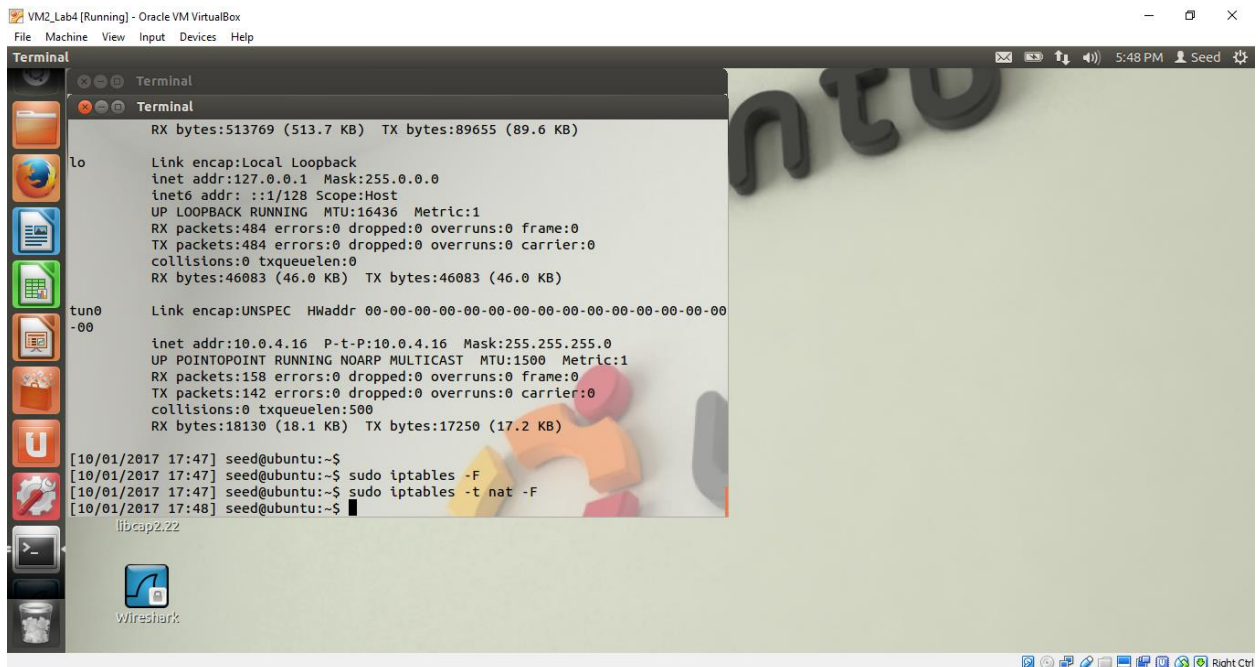
```
VM2_Lab4 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminal
Terminal
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:320 errors:0 dropped:0 overruns:0 frame:0
TX packets:320 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:28997 (28.9 KB) TX bytes:28997 (28.9 KB)

tun0
Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet addr:10.0.4.16 P-t-P:10.0.4.16 Mask:255.255.255.0
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
RX packets:158 errors:0 dropped:0 overruns:0 frame:0
TX packets:142 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:500
RX bytes:18130 (18.1 KB) TX bytes:17250 (17.2 KB)

[10/01/2017 17:08] seed@ubuntu:~$
[10/01/2017 17:45] seed@ubuntu:~$
[10/01/2017 17:45] seed@ubuntu:~$ sudo sysctl net.ipv4.ip_forward=1
[sudo] password for seed:
net.ipv4.ip_forward = 0
error: Malformed setting "=1"
[10/01/2017 17:46] seed@ubuntu:~$ sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
[10/01/2017 17:46] seed@ubuntu:~$
libcap2.22
Wireshark
```

Figure shows that the IP Port forwarding is enabled in VM2.



```
VM2_Lab4 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminal
Terminal
RX bytes:513769 (513.7 KB) TX bytes:89655 (89.6 KB)

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:484 errors:0 dropped:0 overruns:0 frame:0
TX packets:484 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:46083 (46.0 KB) TX bytes:46083 (46.0 KB)

tun0
Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet addr:10.0.4.16 P-t-P:10.0.4.16 Mask:255.255.255.0
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
RX packets:158 errors:0 dropped:0 overruns:0 frame:0
TX packets:142 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:500
RX bytes:18130 (18.1 KB) TX bytes:17250 (17.2 KB)

[10/01/2017 17:47] seed@ubuntu:~$
[10/01/2017 17:47] seed@ubuntu:~$ sudo iptables -F
[10/01/2017 17:47] seed@ubuntu:~$ sudo iptables -t nat -F
[10/01/2017 17:48] seed@ubuntu:~$
libcap2.22
Wireshark
```

Figure shows that the iptables are flushed and NAT iptables are flushed on VM2.

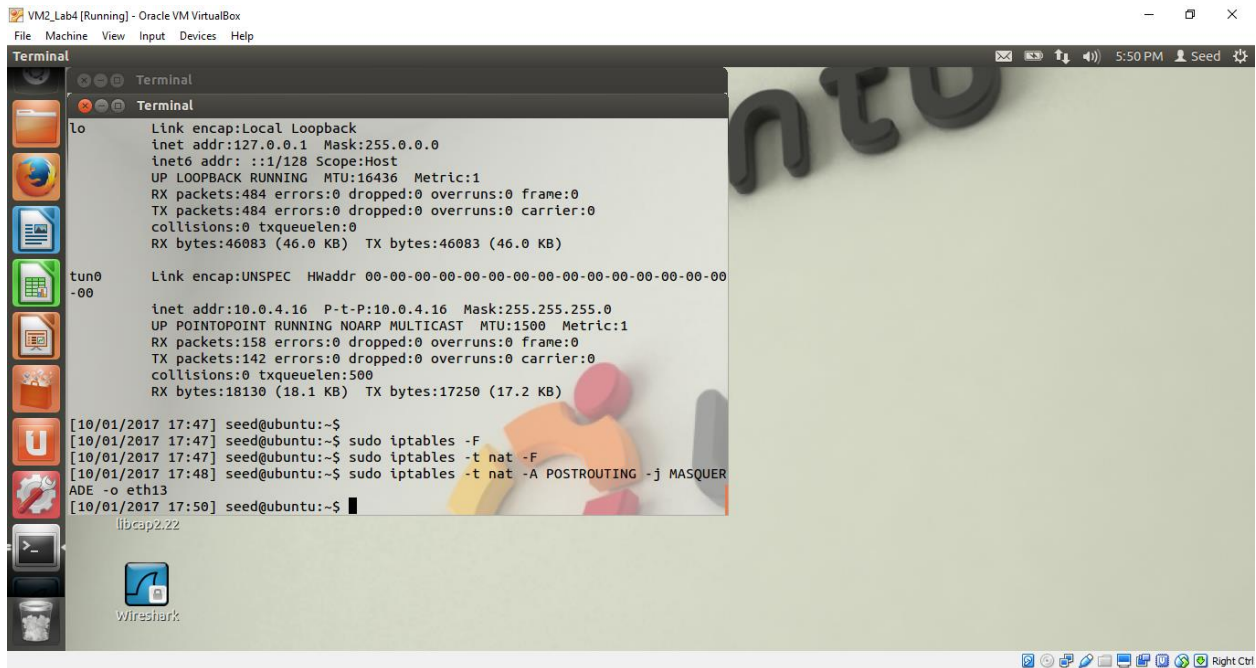


Figure shows that masquerade on NAT adapter is being performed on VM2.

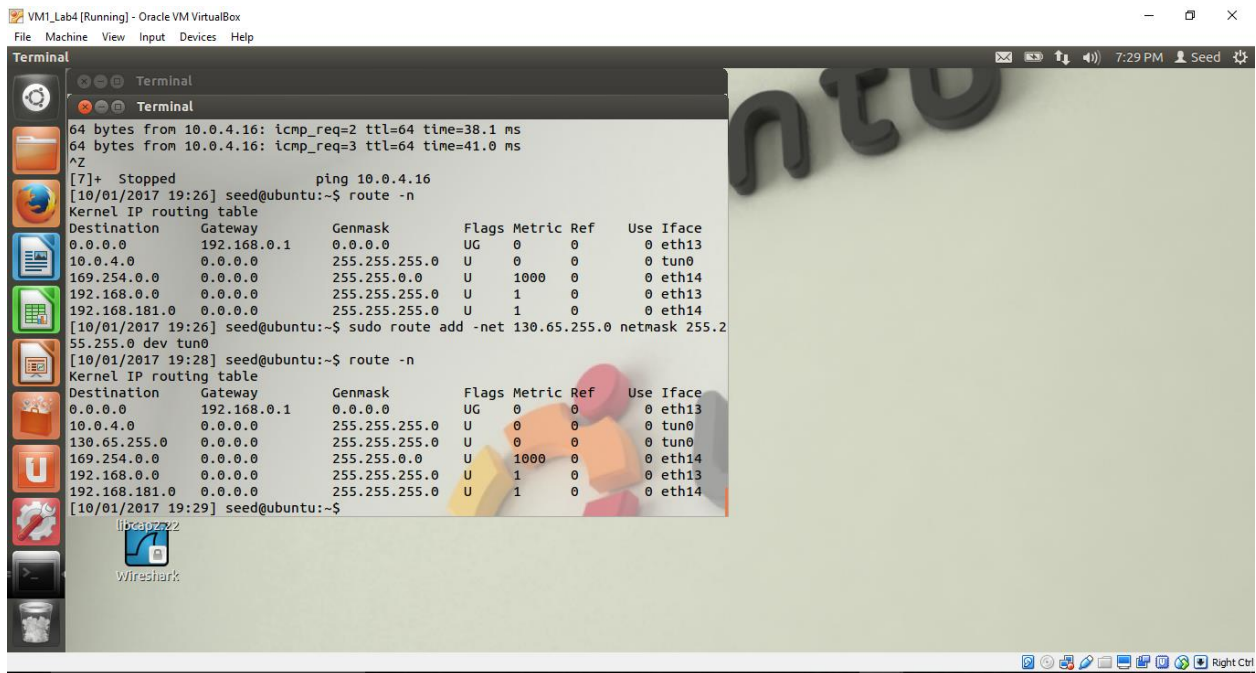


Figure shows a record created in routing table in VM1 where the request destination packets for 130.65.255.0/24 are routed to tun0 instead of NAT adapter eth13.



Figure shows that the www.sjsu.edu is accessible again on VM1 through tunneling and hence firewall has been bypassed.

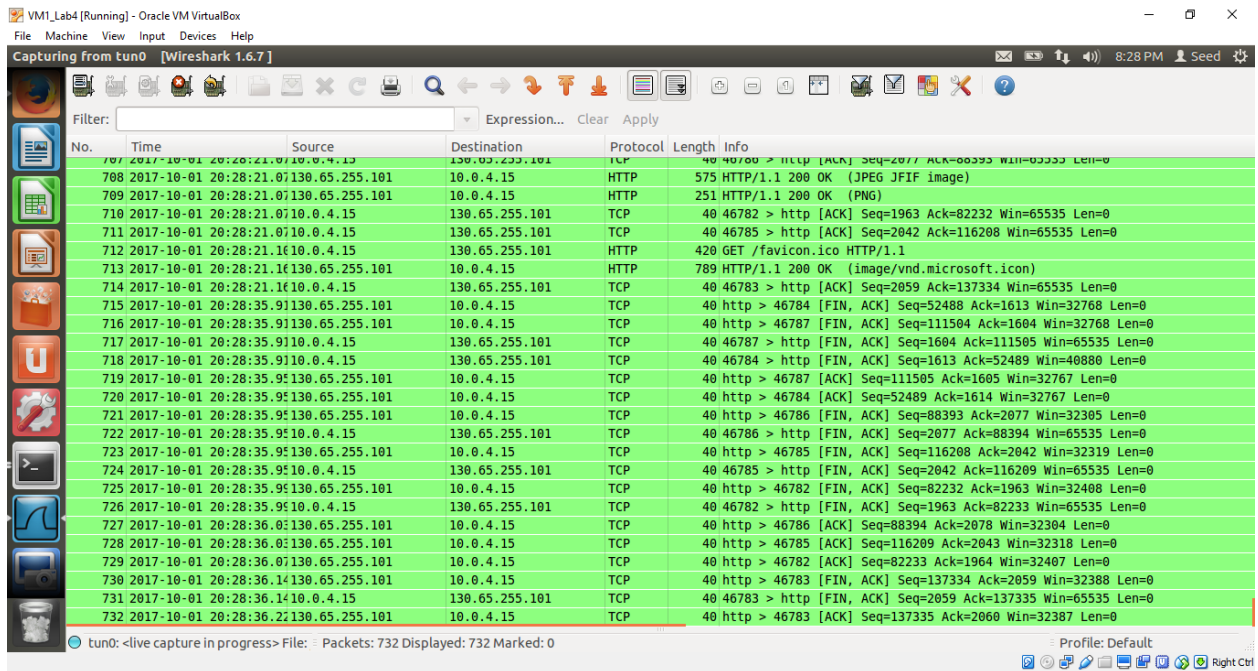


Figure shows that Wireshark analysis of packets being forwarded through `tun0` and shows connection to `10.0.4.16` to "sjsu website". Hence VM2 acts as a gateway here.