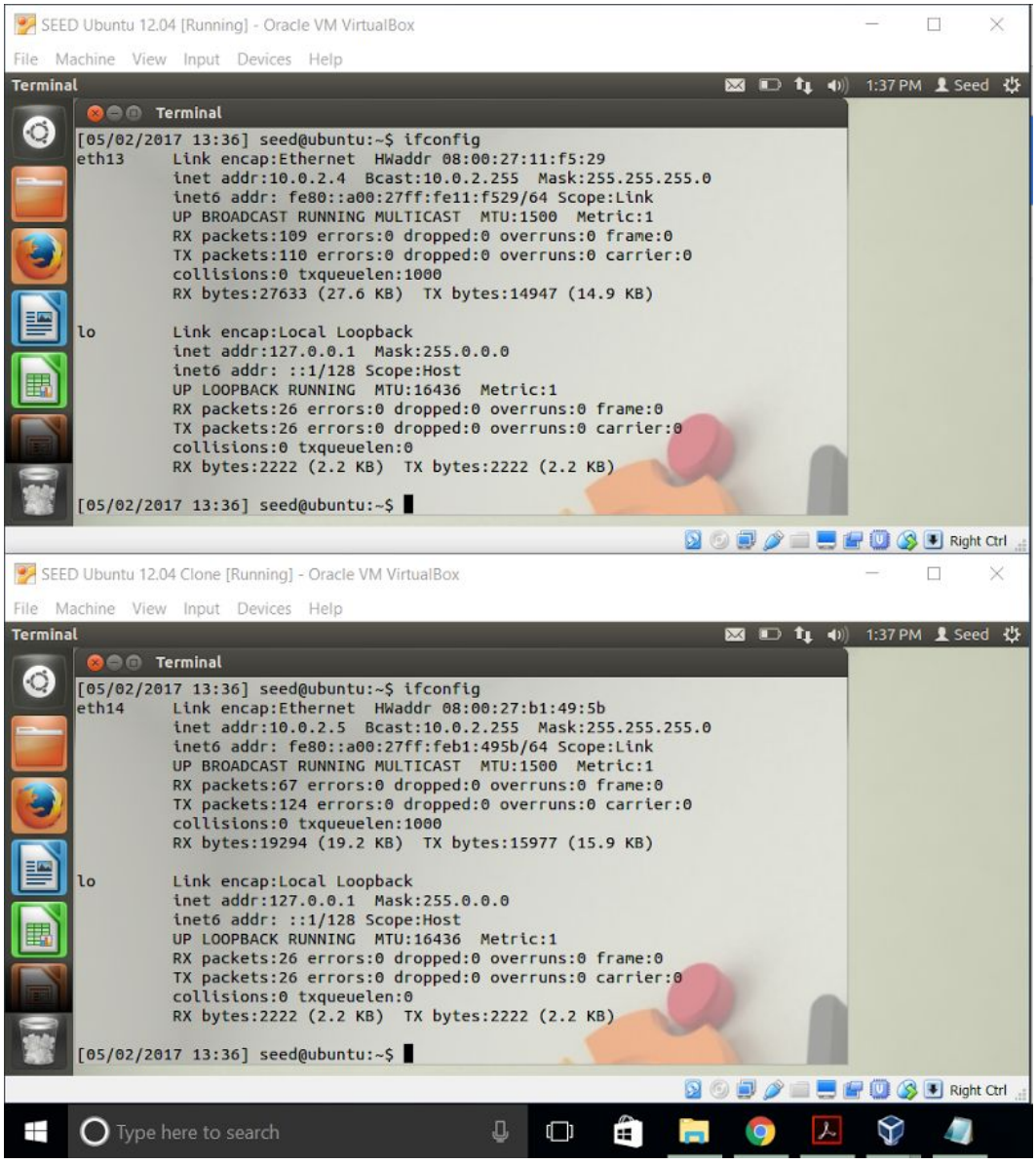
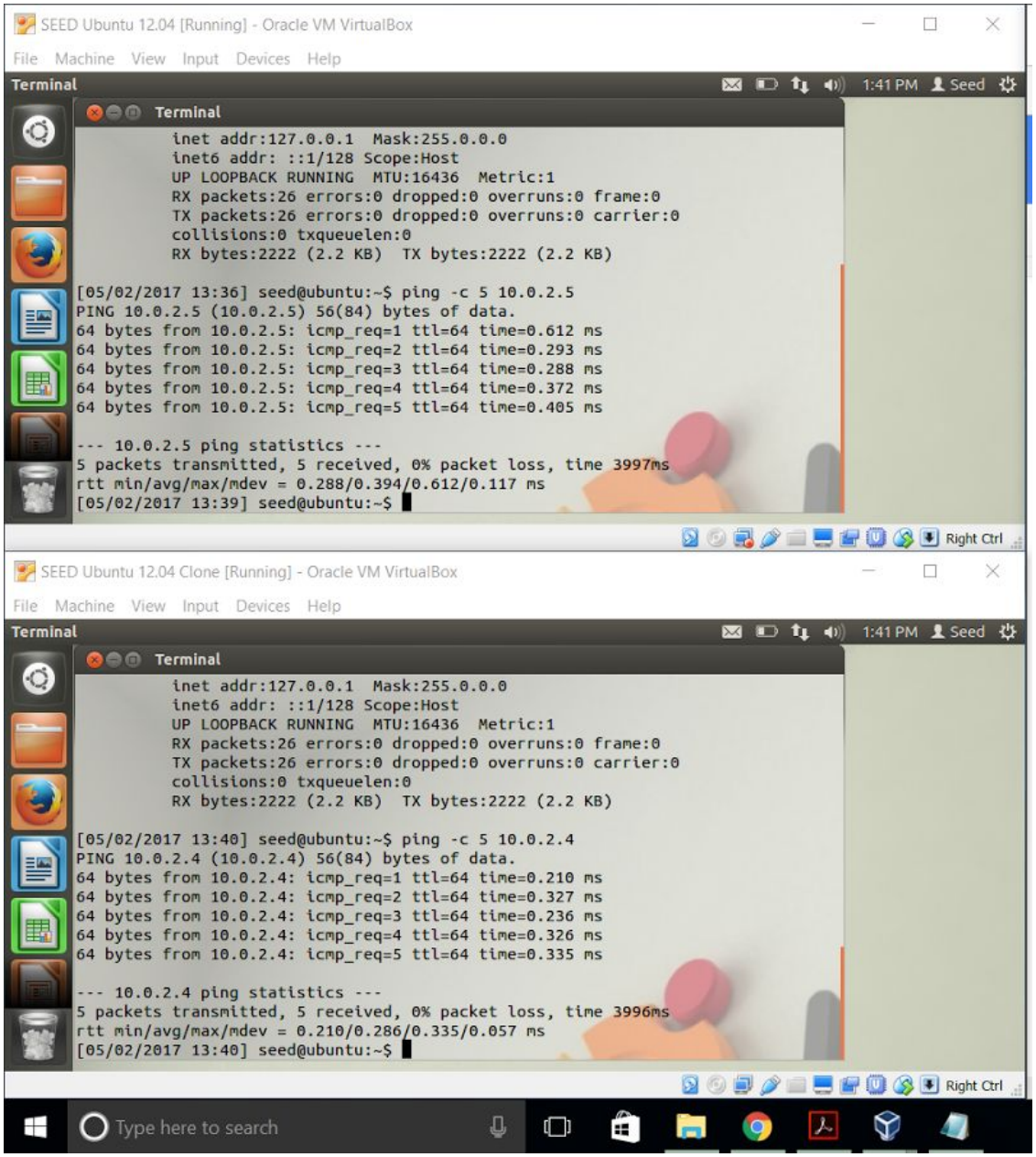
Pedro Ruelas

Exercise 5
3.1 Problem 1: Verifying the Network
Output for terminal command:
$ ifconfig



Output for terminal command:
$ ping -c 5 x.x.x.x

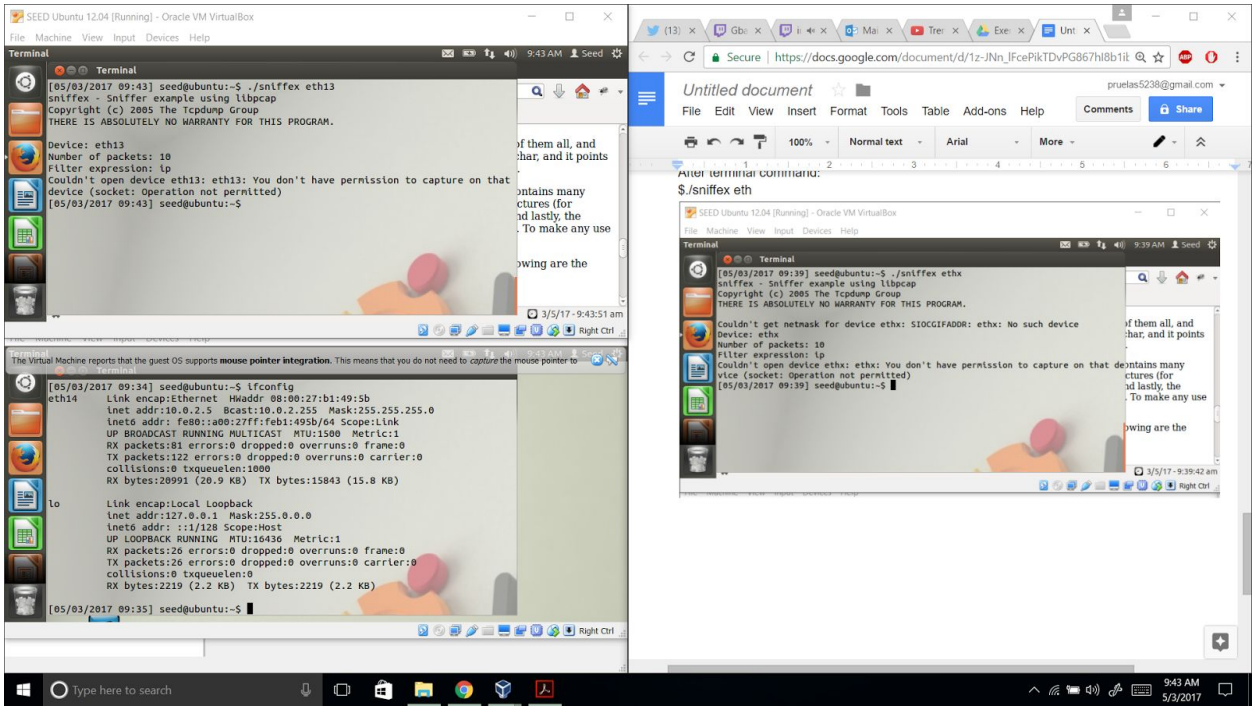


3.2 Problem 2: Writing a Packet Sniffer

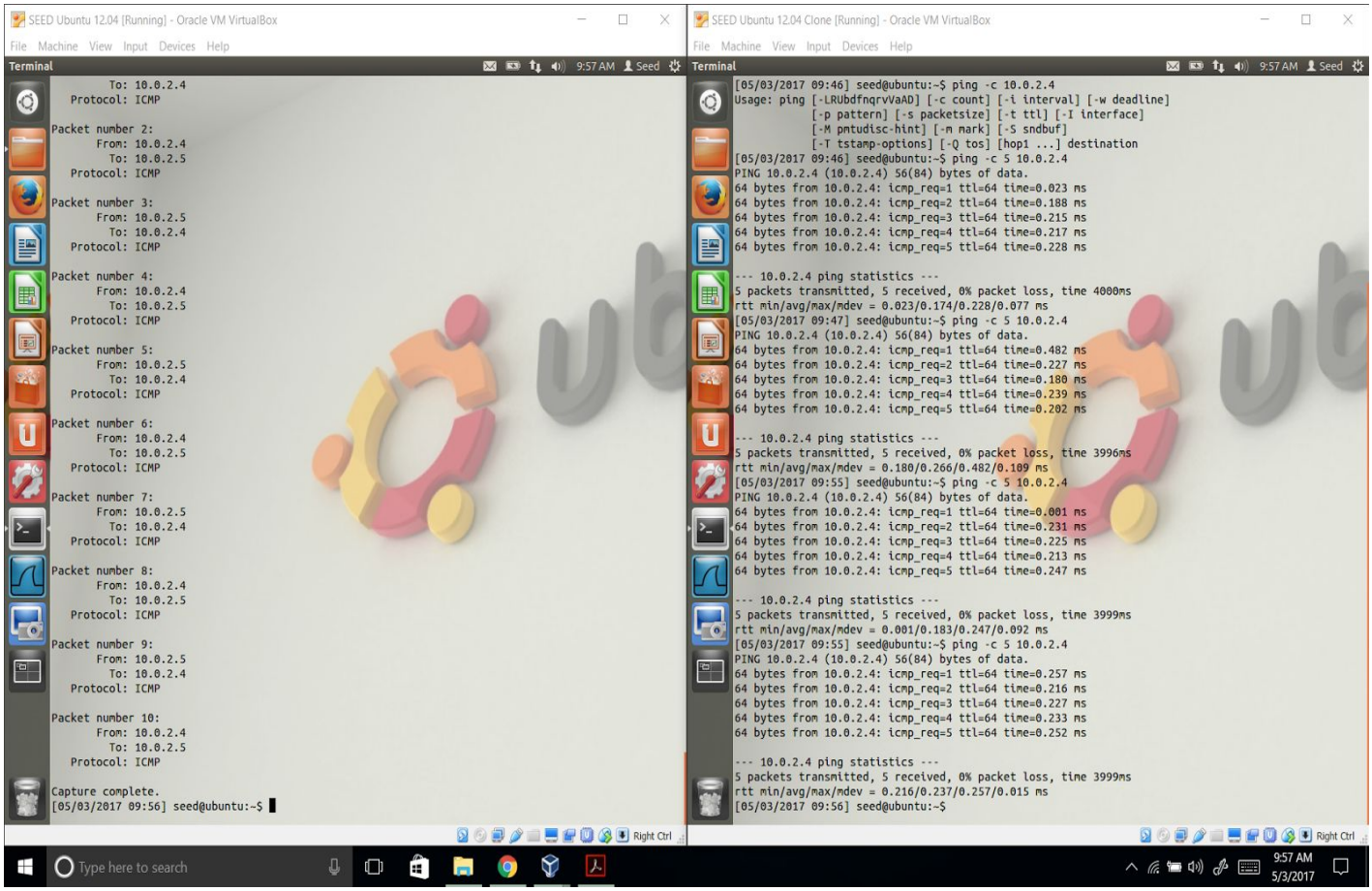
Summary of the PCAP Library

- The pcap library is used to view the traffic that is passing on an interface. One must inform the pcap on which device it will be viewing the traffic and inform what types of traffic it will be viewing. After running the pcap, it will view the traffic until it has received a set amount of packets specified by the user.

After terminal command:
$./sniffex eth13



Results for running the sniffer program in the first machine and pinging from the second.

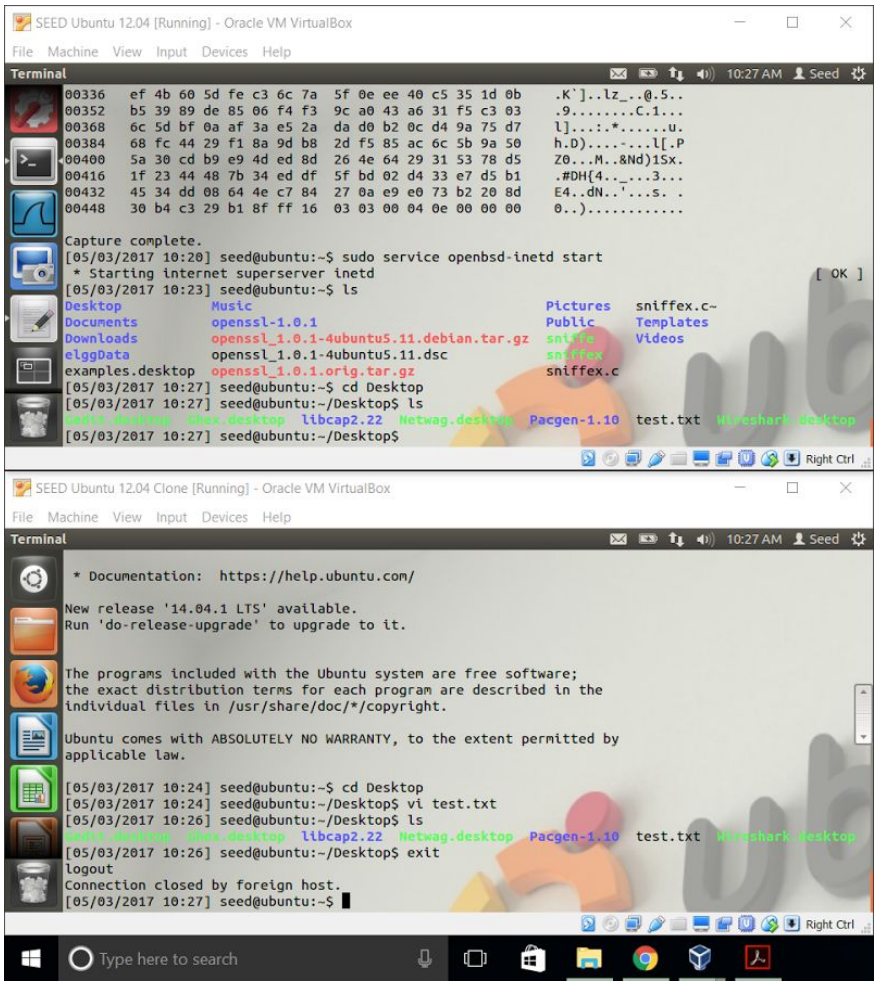


After modifying the filter in the packet sniffer source code so that it captures TCP packets, the pings from the second machined are not being captured by the machine running the sniffer.

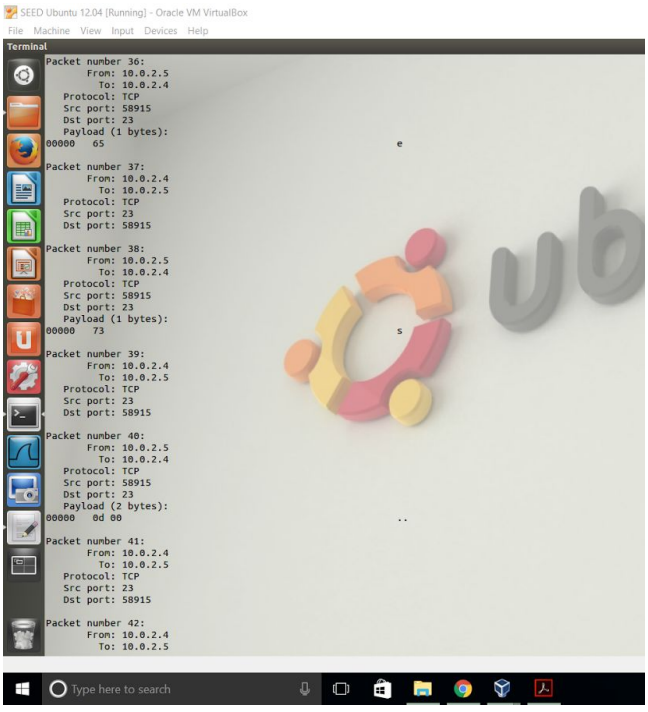
3.3 Problem 3: Password Sniffing

After running the terminal command below on the first machine
$ sudo service openbsd-inetd start
And using the terminal command below on the second machine
$ telnet 10.0.2.4

I logged from the second machine into the first and created a text file called “test.txt.” After logging out, the text file was present on the first machine.



Trying to find the password of the user logging in.
The password was visible.



Using Wireshark

- When using wireshark instead of my own packet sniffer, I am still able to locate the user's password by looking at the telnet data segments present in wireshark.

After these experiments it appears that using telnet as a method of remotely accessing a system is not secure and should be avoided since the password of a user can be retrieved without much difficulty.

3.4 Problem 4: SSH

When using SSH to login to the first virtual machine, I am unable to find the password entered at the second virtual machine through wireshark. When one looks through the packets, it appears impossible to determine the password.