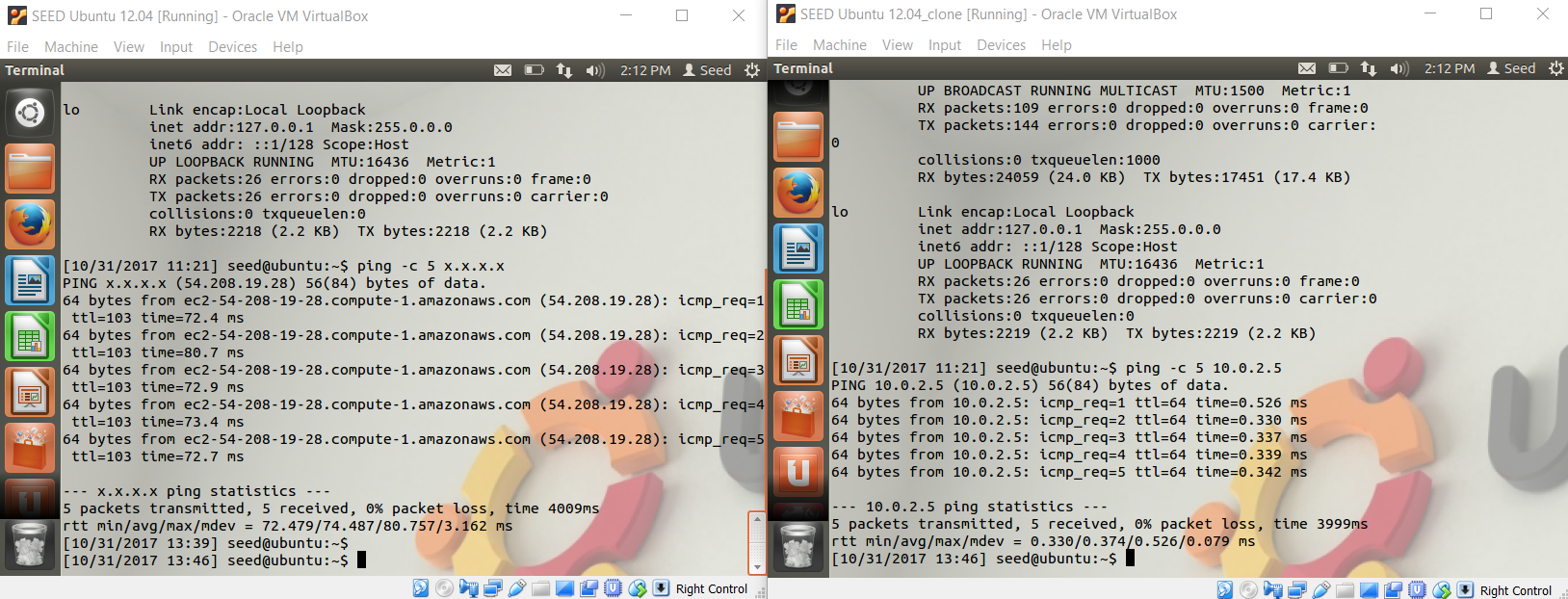
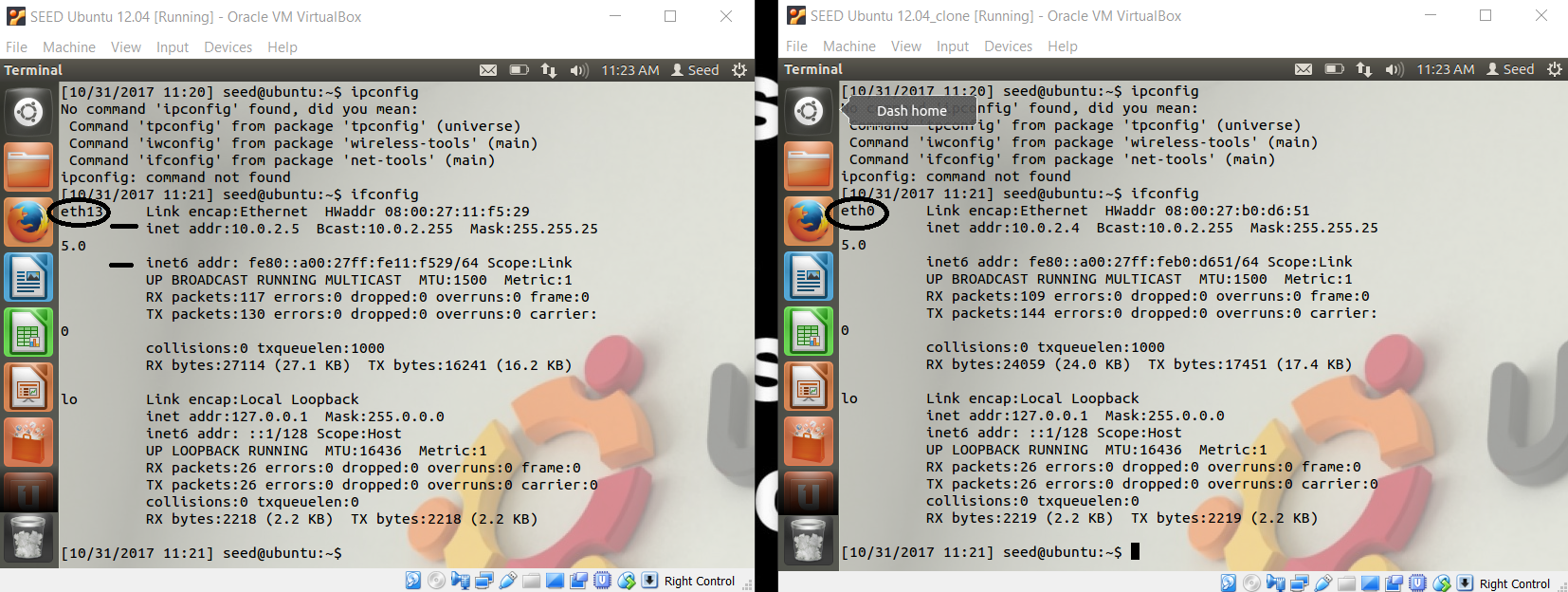
Jaeseung Lee

EX5\_Report

**1. ipconfig\_result**



**2.ping\_result**

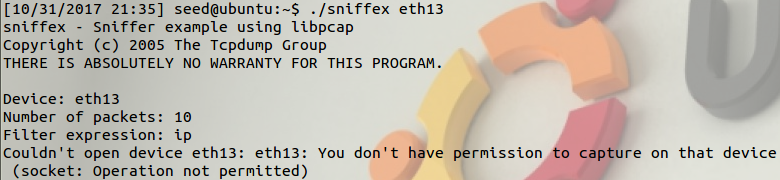


3. **Briefly summarize how the pcap-library is used**

It is packet capture consisting API for capturing network traffic. It is written in C and has the Unix-like environment.

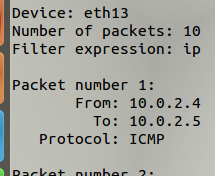
4. **After**

**[1] *gcc -o sniffex sniffex.c -lpcap* [2] *./sniffex eth13***



I am getting error because *tcpdump* needs permission that allows "raw packet captures", and "network interface manipulation"

**5. sudo ./sniffex eth13**



6. **While your sniffer is running on one machine, ping that machine from the second one. Document what happens.**

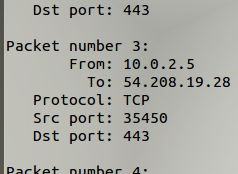
After I gave command to the original : sudo ./sniffex eth13, unless other(clone) machine pings, it doesn't print out the packet information, or wait really-really long time to print out one.

However, if I ping original one from clone, printing out package information gets executed immediately.

7. **Modify the filter expression in your packet sniffer source code so it only captures TCP packets. Redo; What has changed?**

"IP" used to print-out only: From, To, Protocol:ICMP;

Now "TCP" prints out Src\_port, Dst\_port with Protocol:TCP



8. Original VM was running server, Clone accessed to the server by logging in, and was able to create text file to the Original VM's desktop.



9. When I did the packet sniffling on the Clone's logging-in, I was able to see what the clone user was typing.

Interesting thing is although the clone doesn't take actions, the packet-sniffler recorder sometimes records it.

When I used Wireshark, it highlights when the clone is inputting. However, it doesn't printout the character of input, but rather shows the hex number.