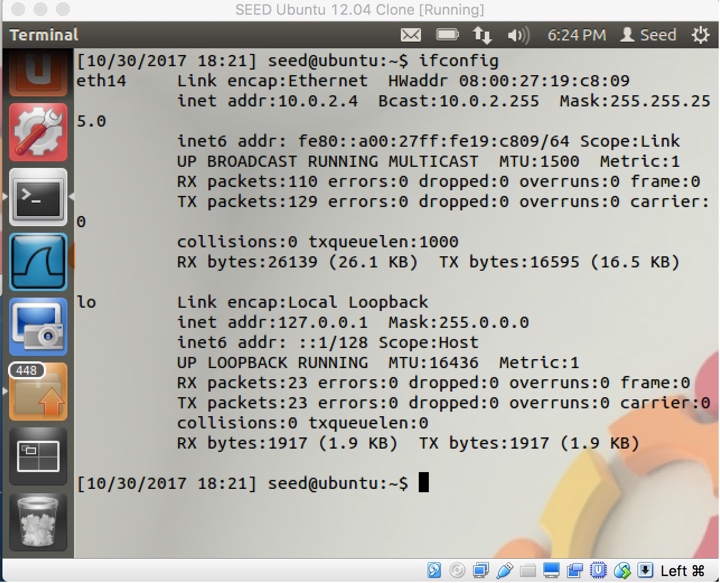
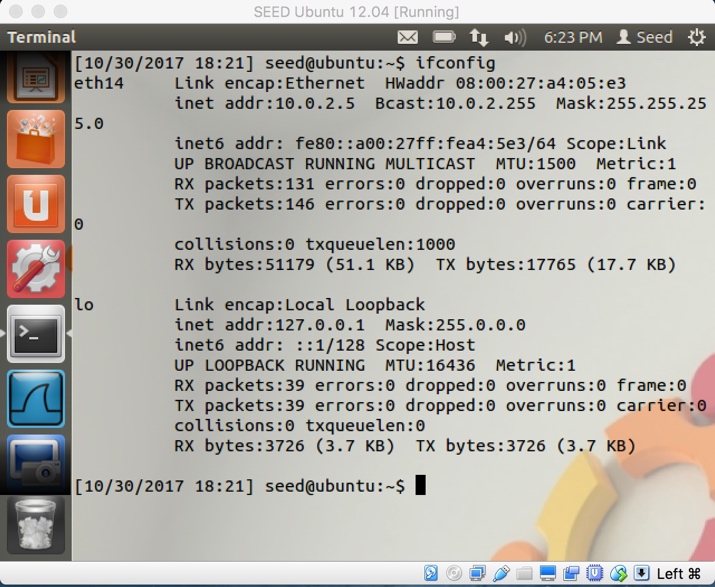
Jerahmeel Calma

[www.github.com/CS380-EX5](http://www.github.com/CS380-EX5)

3.1

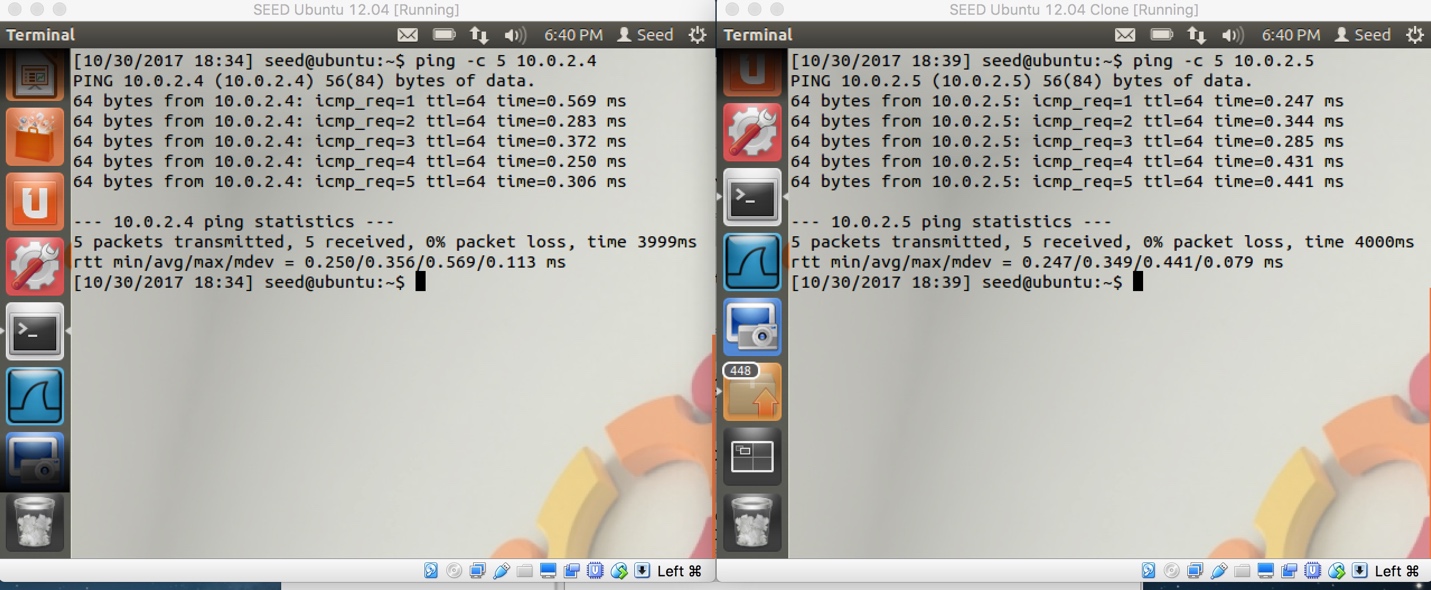
ifconfig

original clone



ping –c 5 x.x.x.x

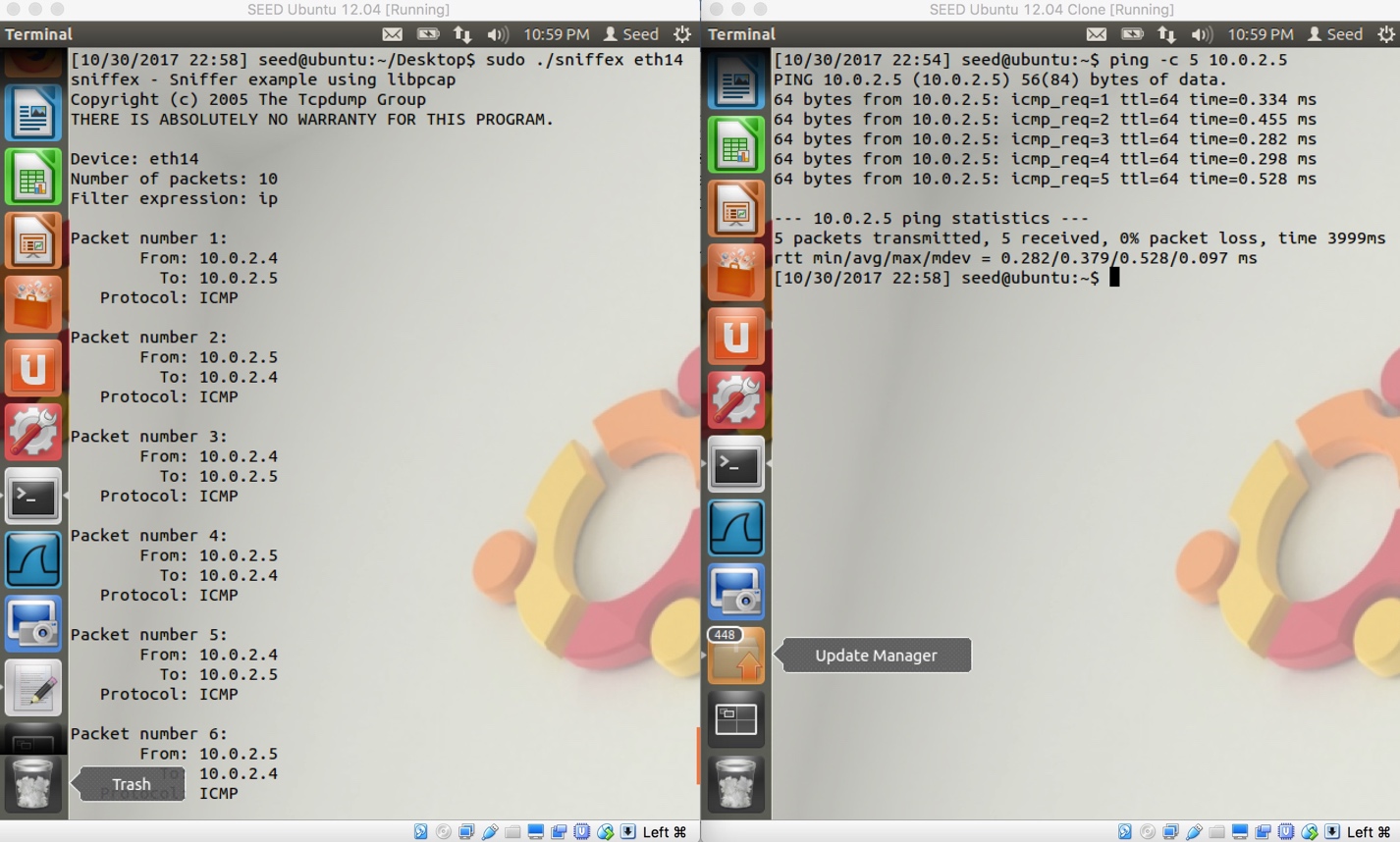
original clone



3.2

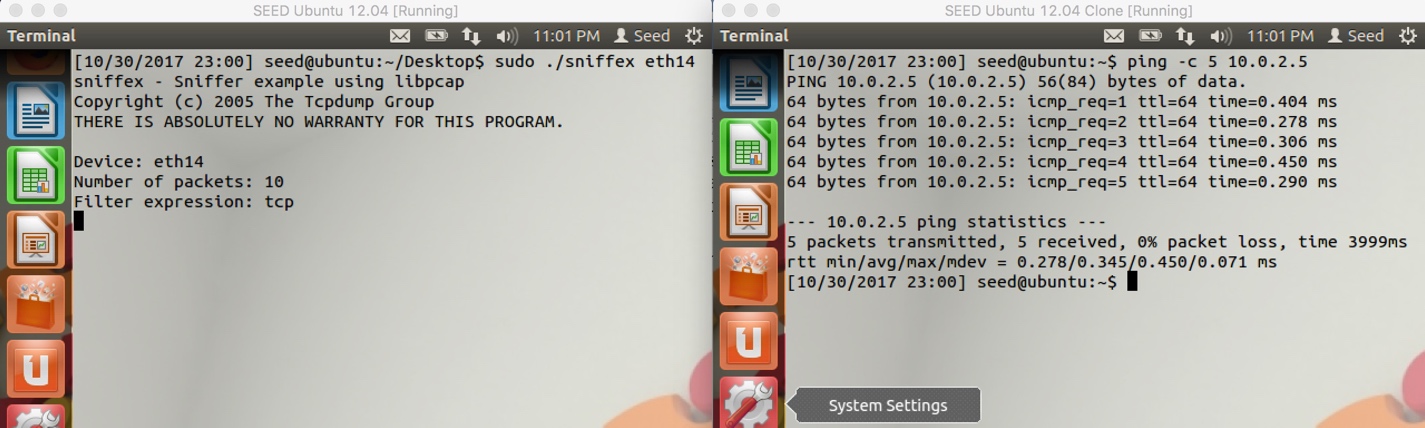
We first have to determine the interface we want to sniff on. Then we tell pcap what device we are sniffing on and we name the sniffing sessions so we can tell each sniffing sessions apart. If we want to sniff specific traffic, we must create a rule set which is saved as a string. The rule set is then converted into a format that pcap can read and then the rule set is applied to the desired sniffing session. Pcap will wait to receive all the packets we want it to receive. Every time it receives a new packet it will either dissect the packet and print it to the user, it can save it in a file, or it can do nothing at all.

sudo ./sniffex eth14





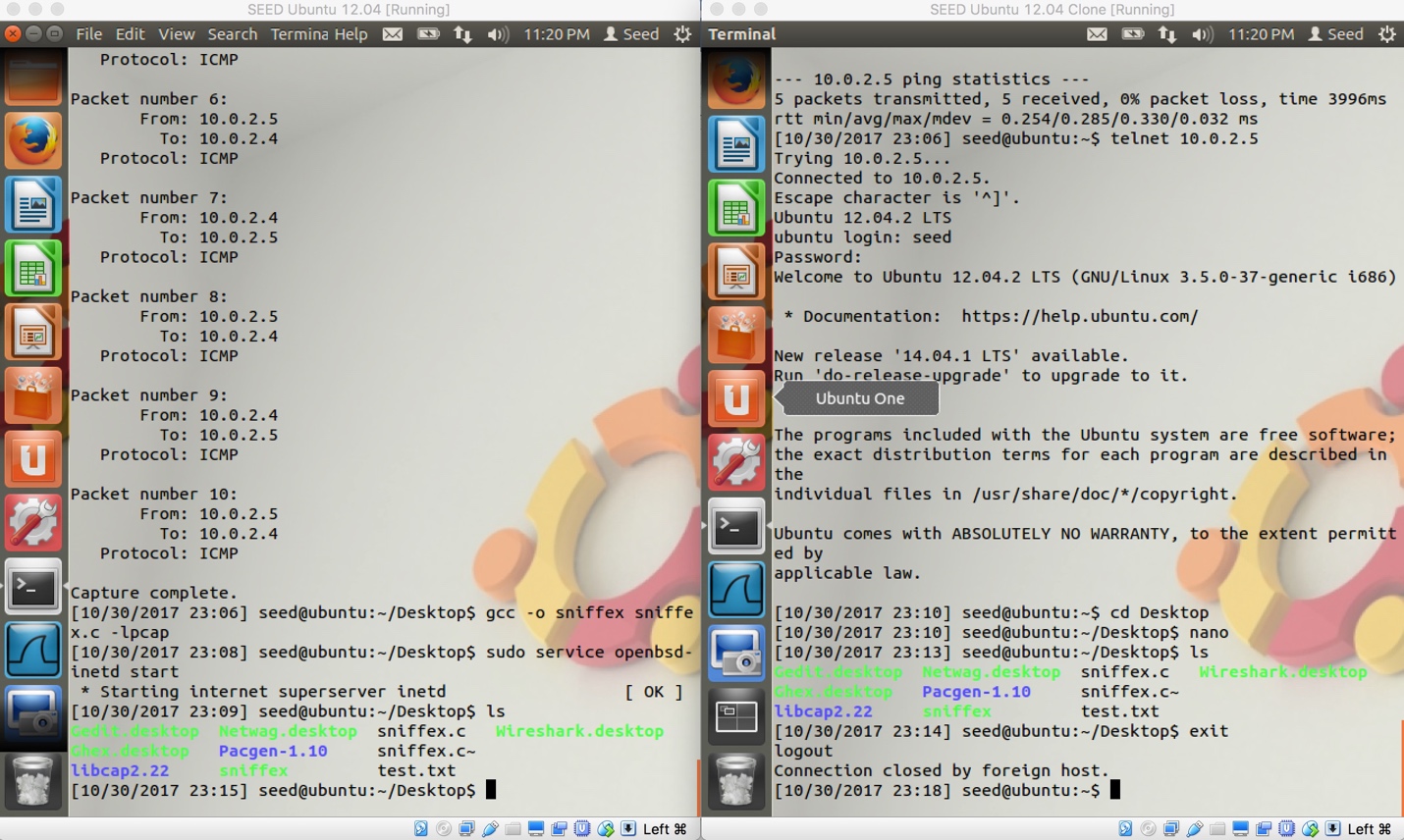
only TCP packets



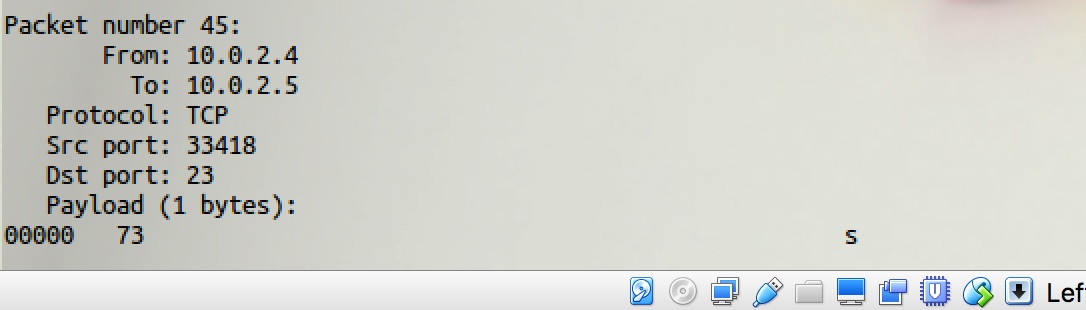
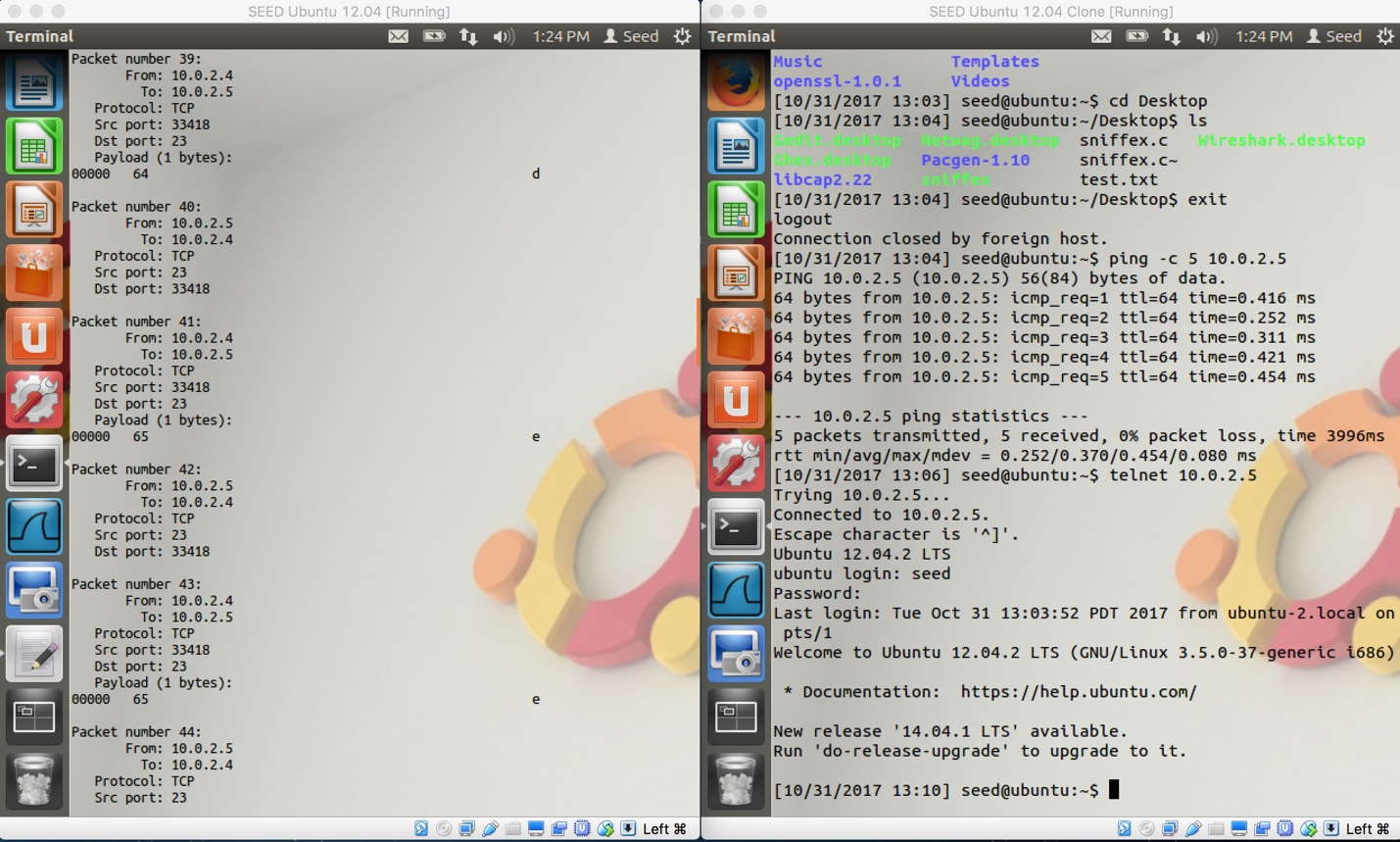
The packets being sent are ICMP packets so the sniffer just waits for TCP packets to be sent to it.

3.3

create a text file

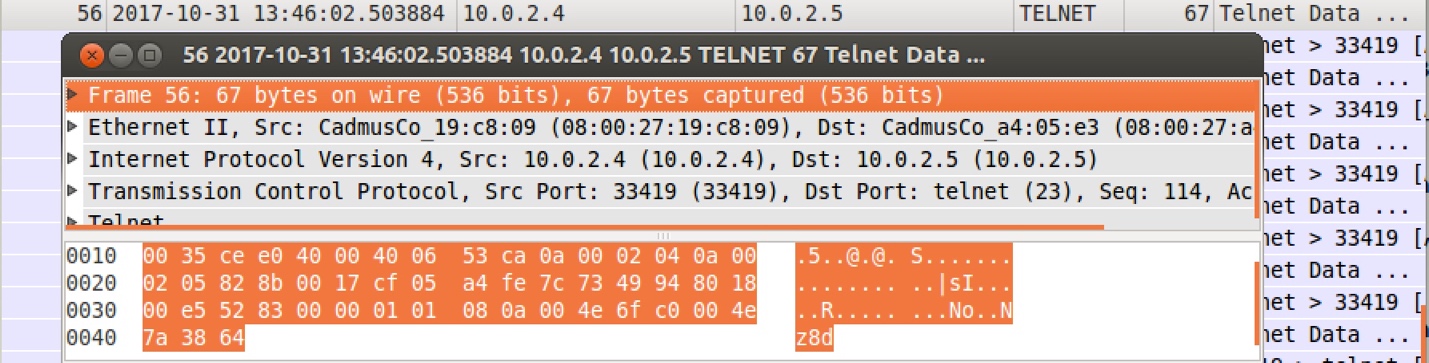


find password

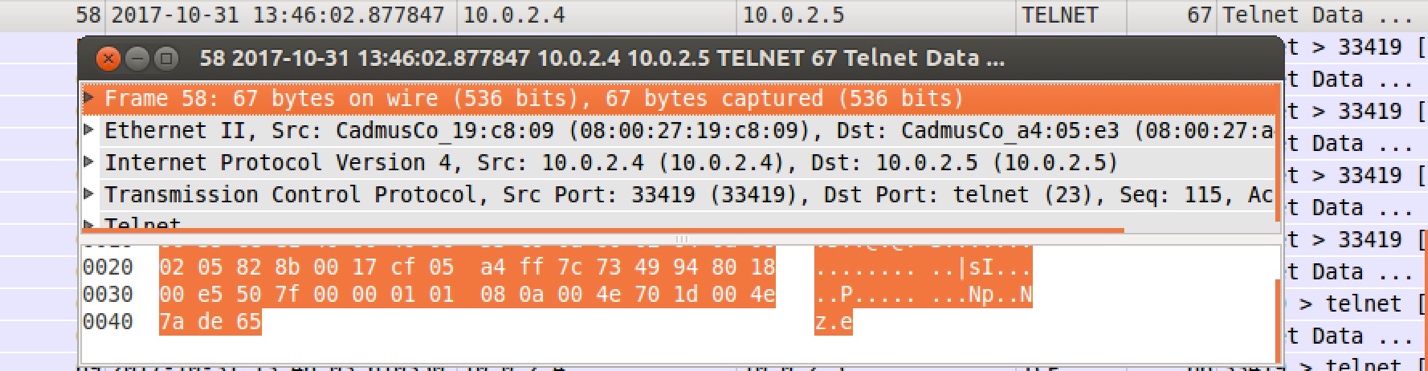


find password using Wireshark

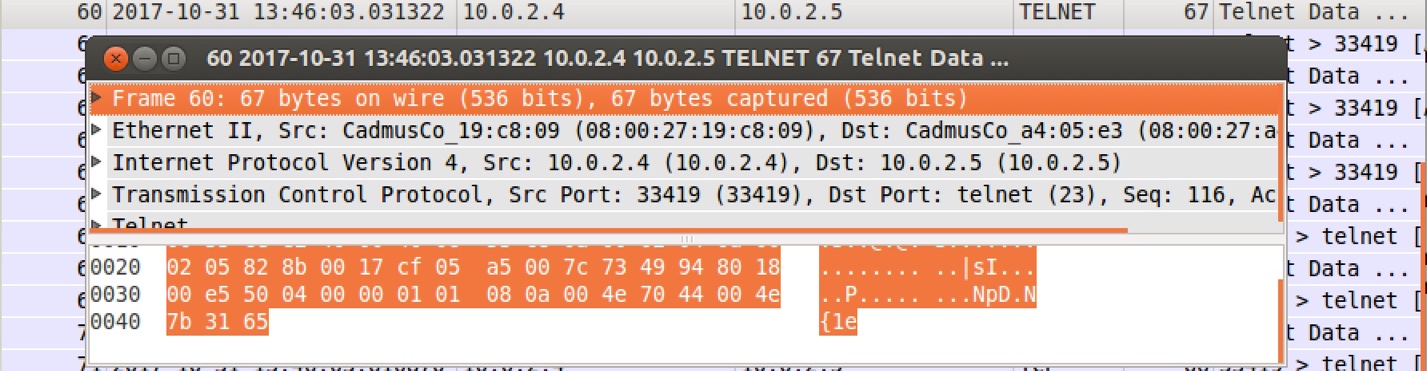
d



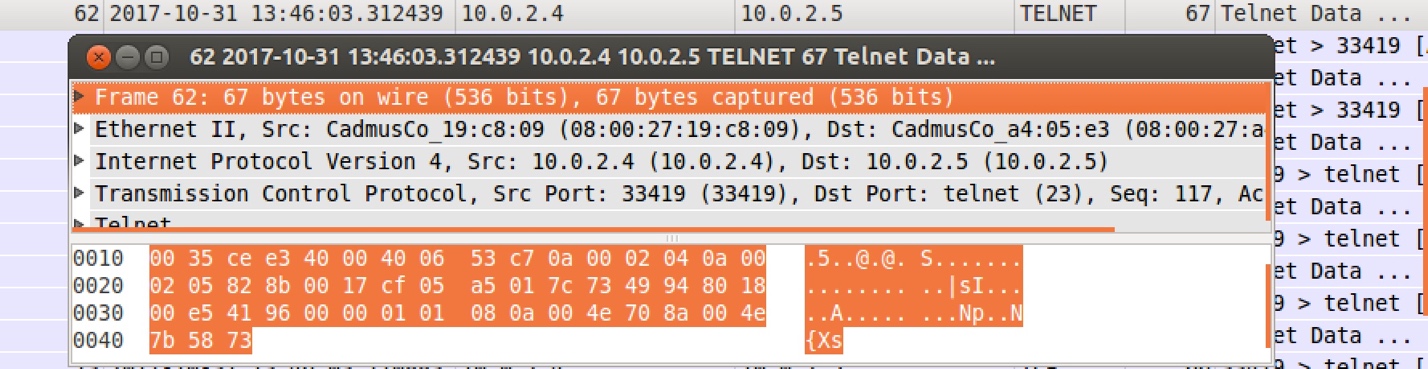
e



e



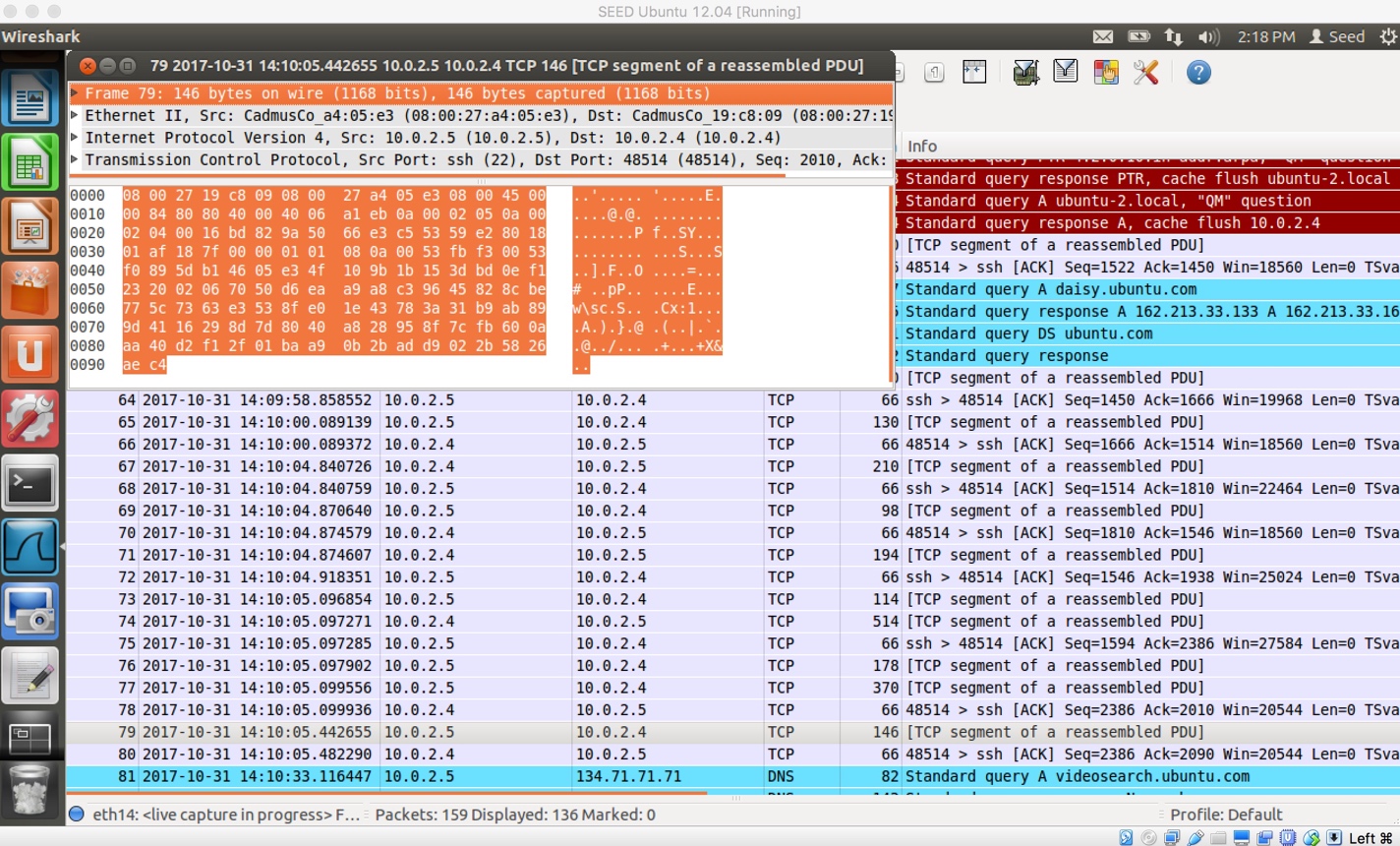
s



I can still locate the password but it does require more effort, than using sniffex.c in the terminal, to search for each letter of the password.

I think that using telnet as a method of remotely accessing a system is dangerous because even though it may take some time to sift through all the packets, as long as you know where to look, it is easy to see people’s passwords.

3.4



Even though I know which packets to look at, I am unable to find the password. The data is encrypted so I cannot understand the data just by directly looking at its contents.