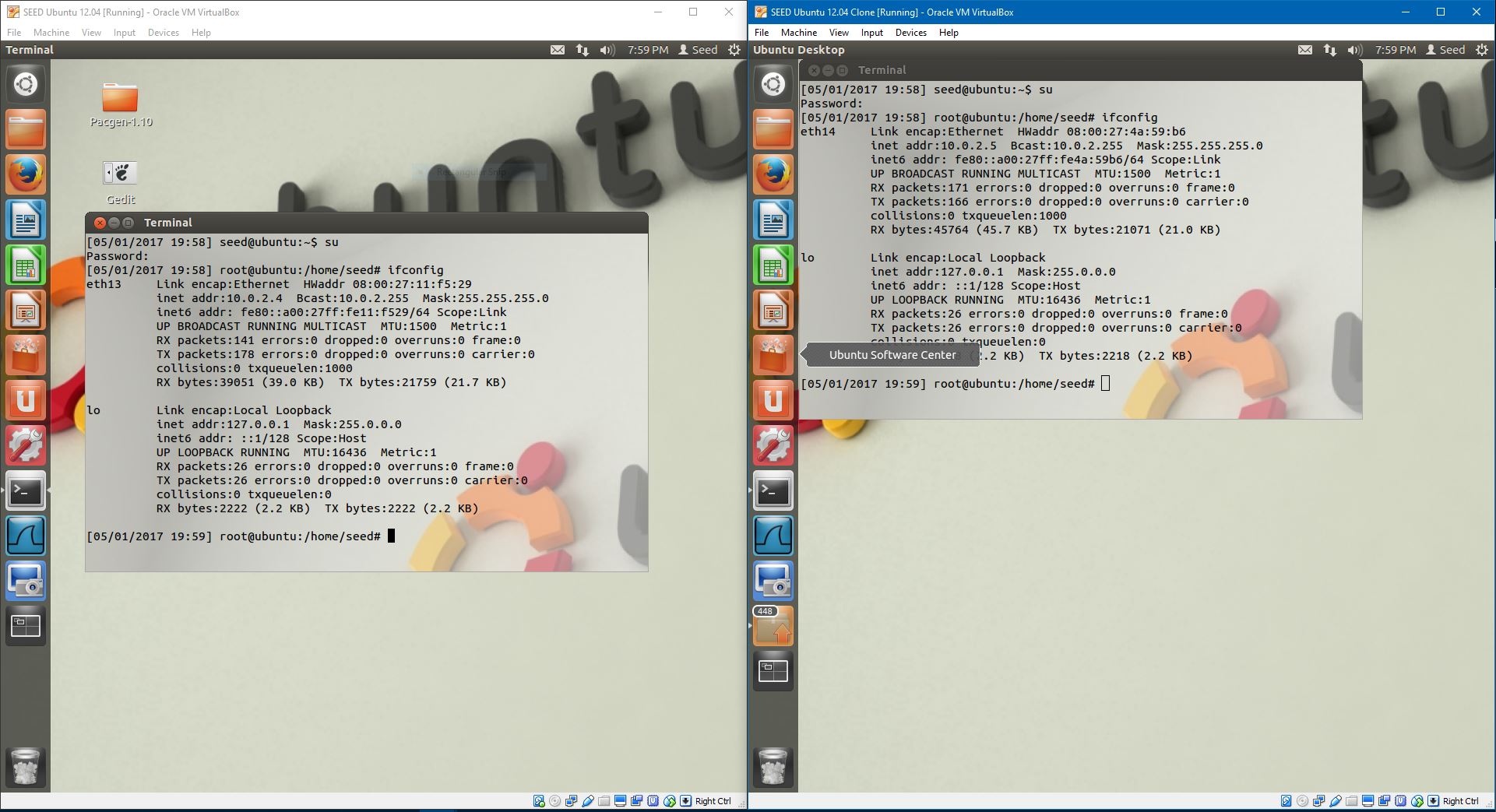
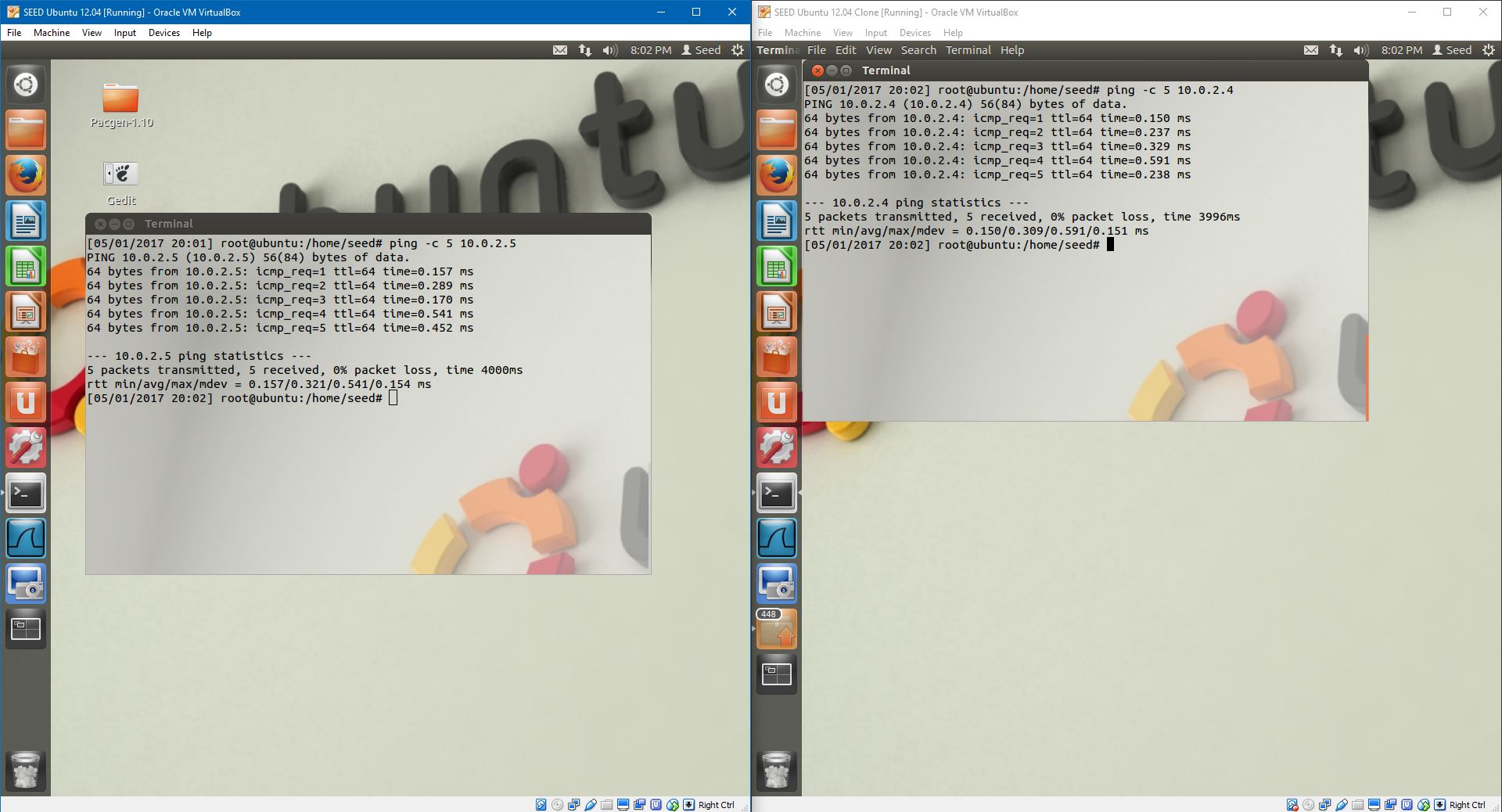
3.1:

Ifconfig on both:



ping on both:



3.2:

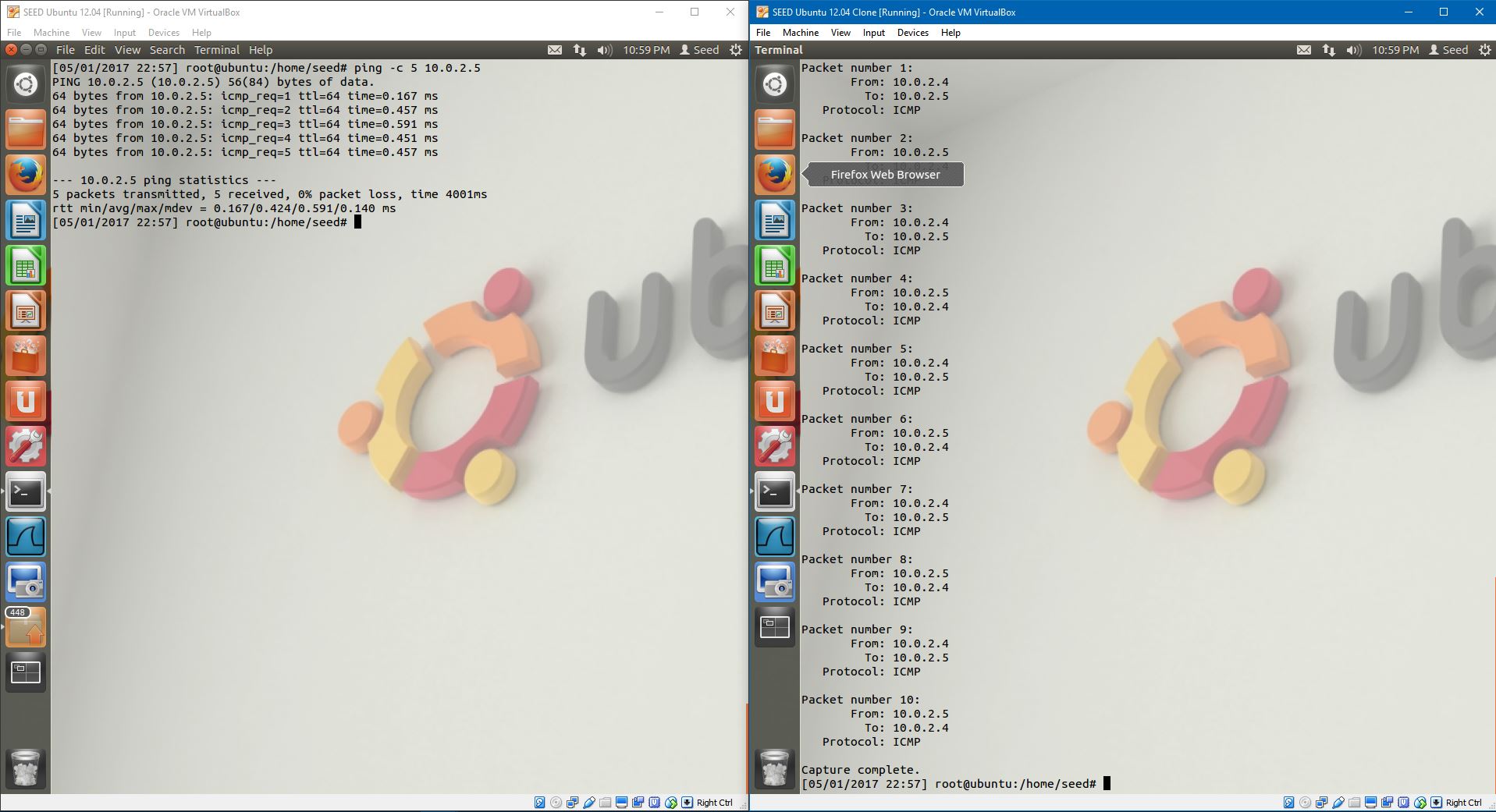
Pcap library:

You first give pcap an argument as to which adapter to use, then pcap\_open\_live() is used to sniff the device for packets. Program can also use pcap to filter any type of traffic.

./sniffex ethx:

Needs super user permissions to run the program. It closes as soon as it is opened.

su ./sniffex ethx:

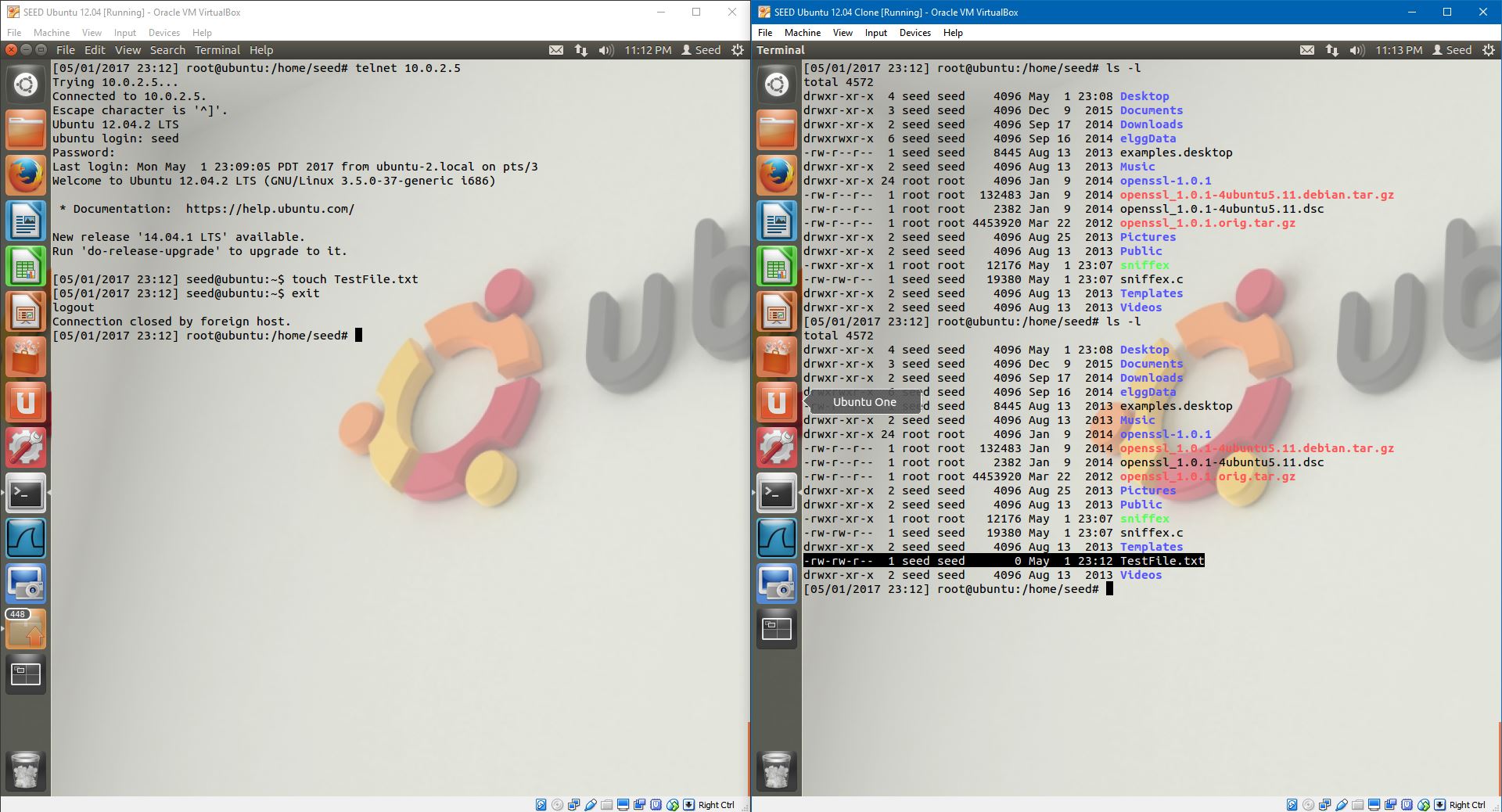


TCP Packets:

Change the filter\_exp[] to “tcp” and the program will filter tcp packets. And since the ping only sends UDP and ICMP packets, nothing happens in sniffex.

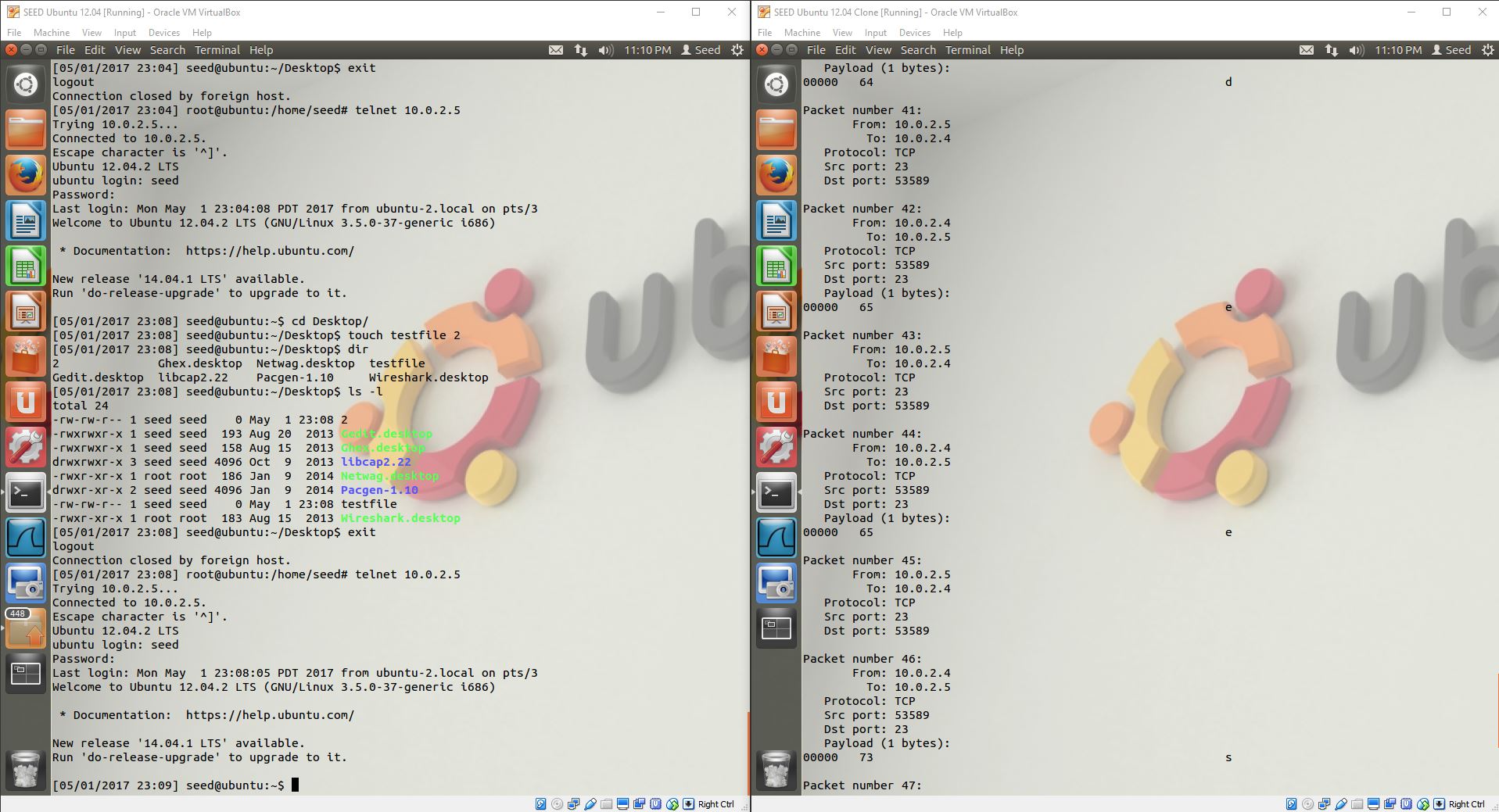
3.3:

Telenet:



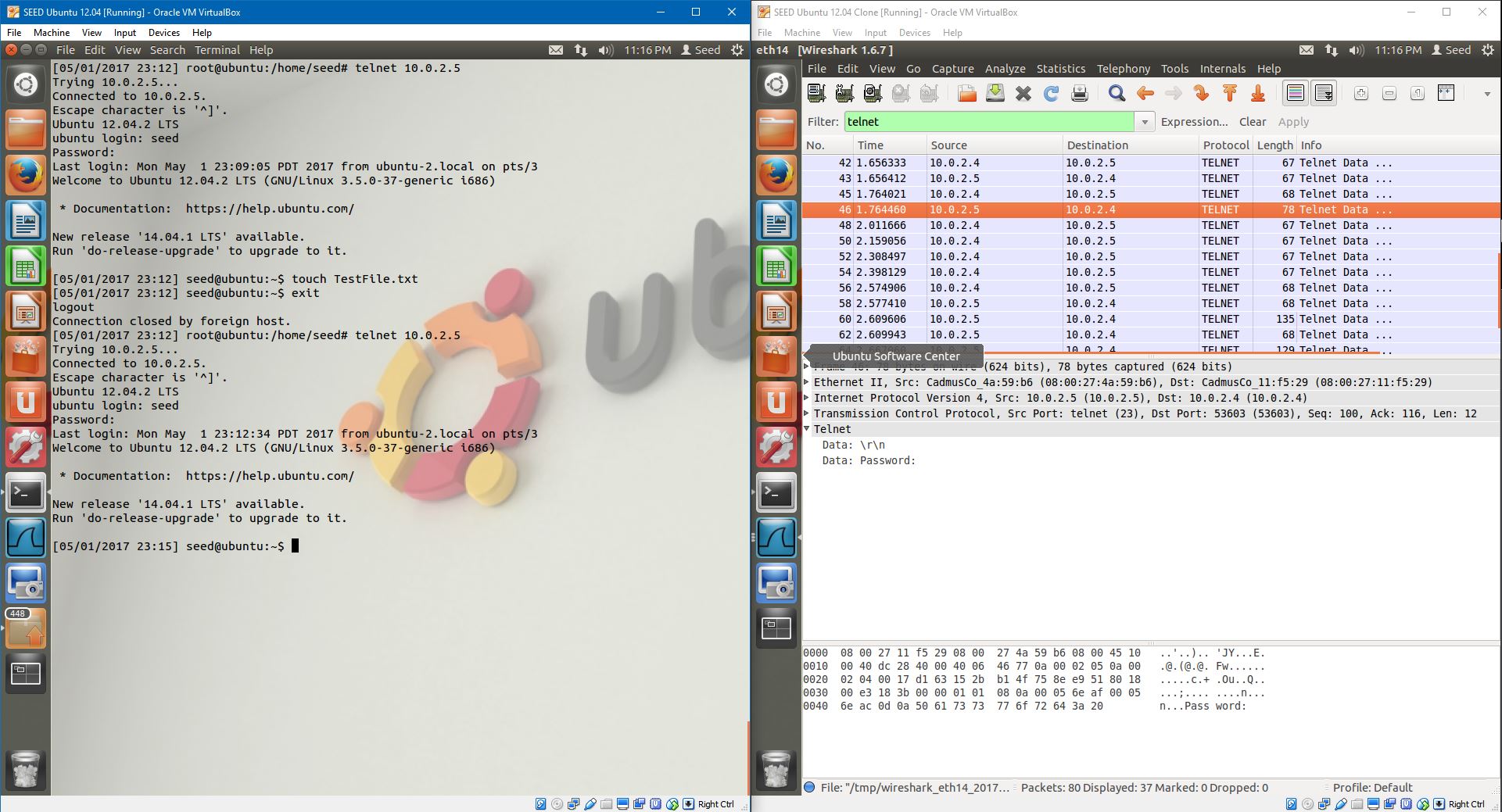
Created the testfile.txt

Password sniff:



User’s password using sniffex.

Wireshark:



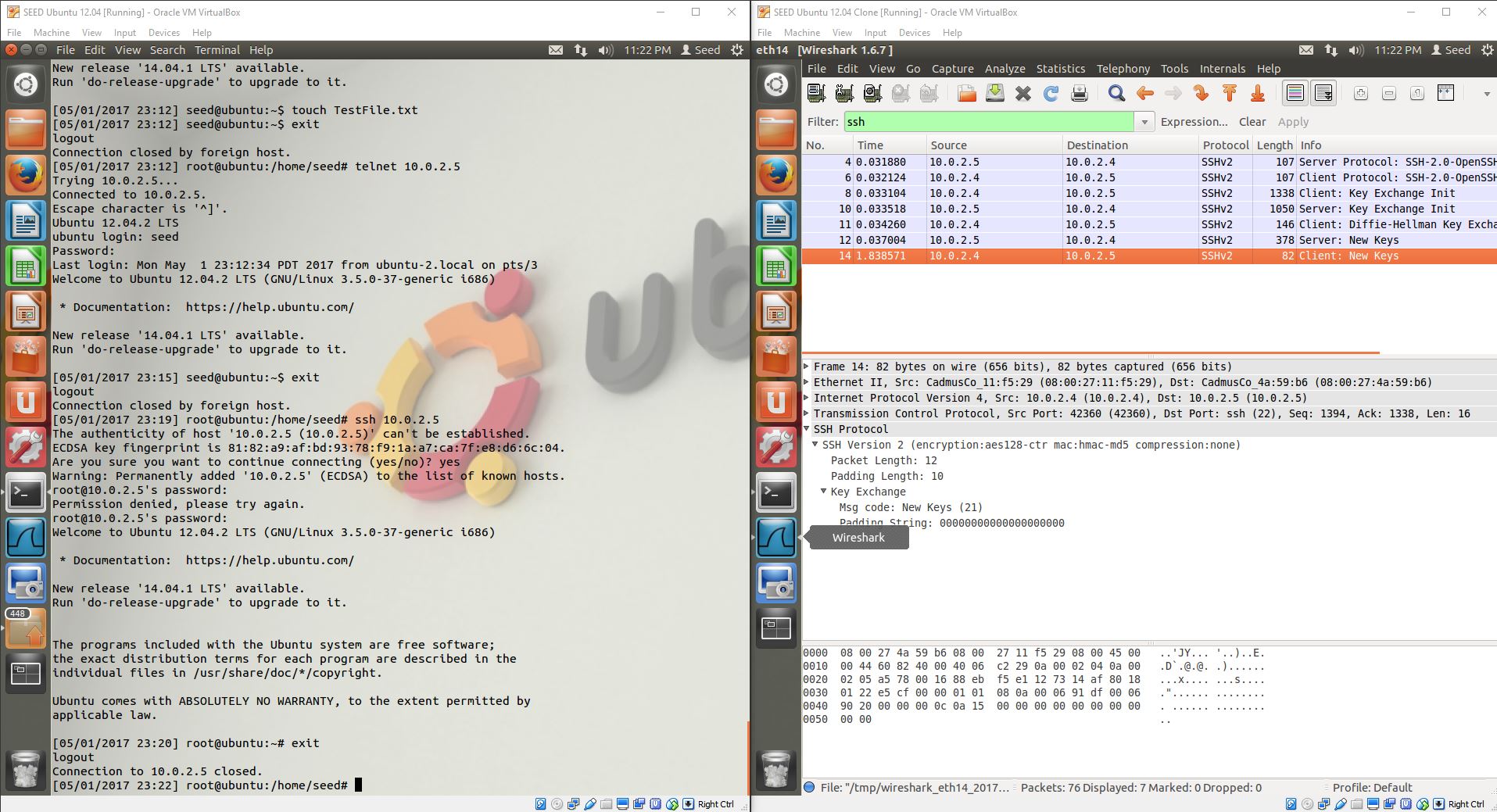
Password is viewable in wireshark.

My thoughts:

Telnet is very weak; it does not encrypt anything and should not be used to remotely access in any system.

3.4:

SSH:



The exchanged are encrypted and therefore not viewable in wireshark unless the keys are known.