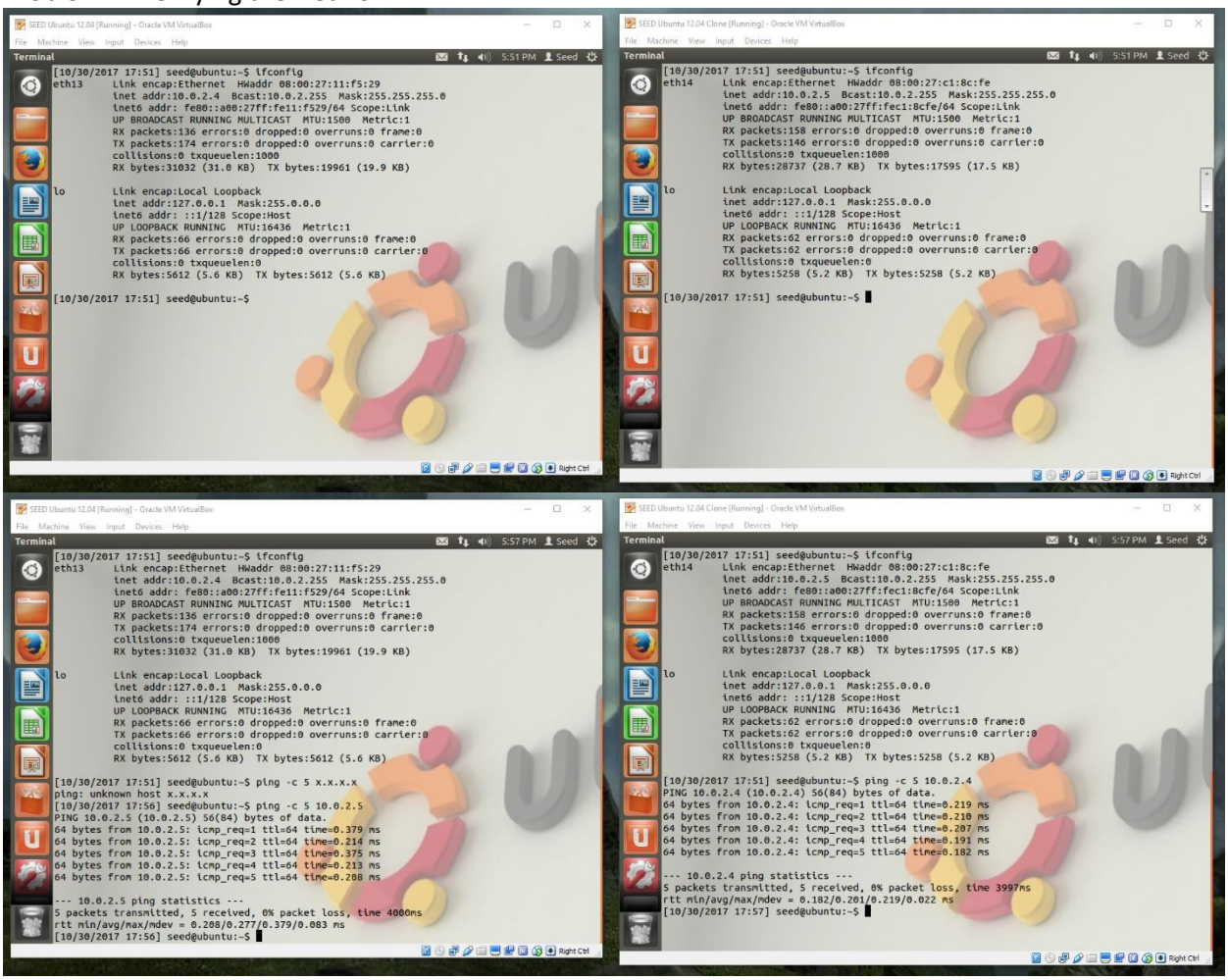
William Kenji Kiplinger
EX5
https://github.com/Kenjum/CS380-EX5/

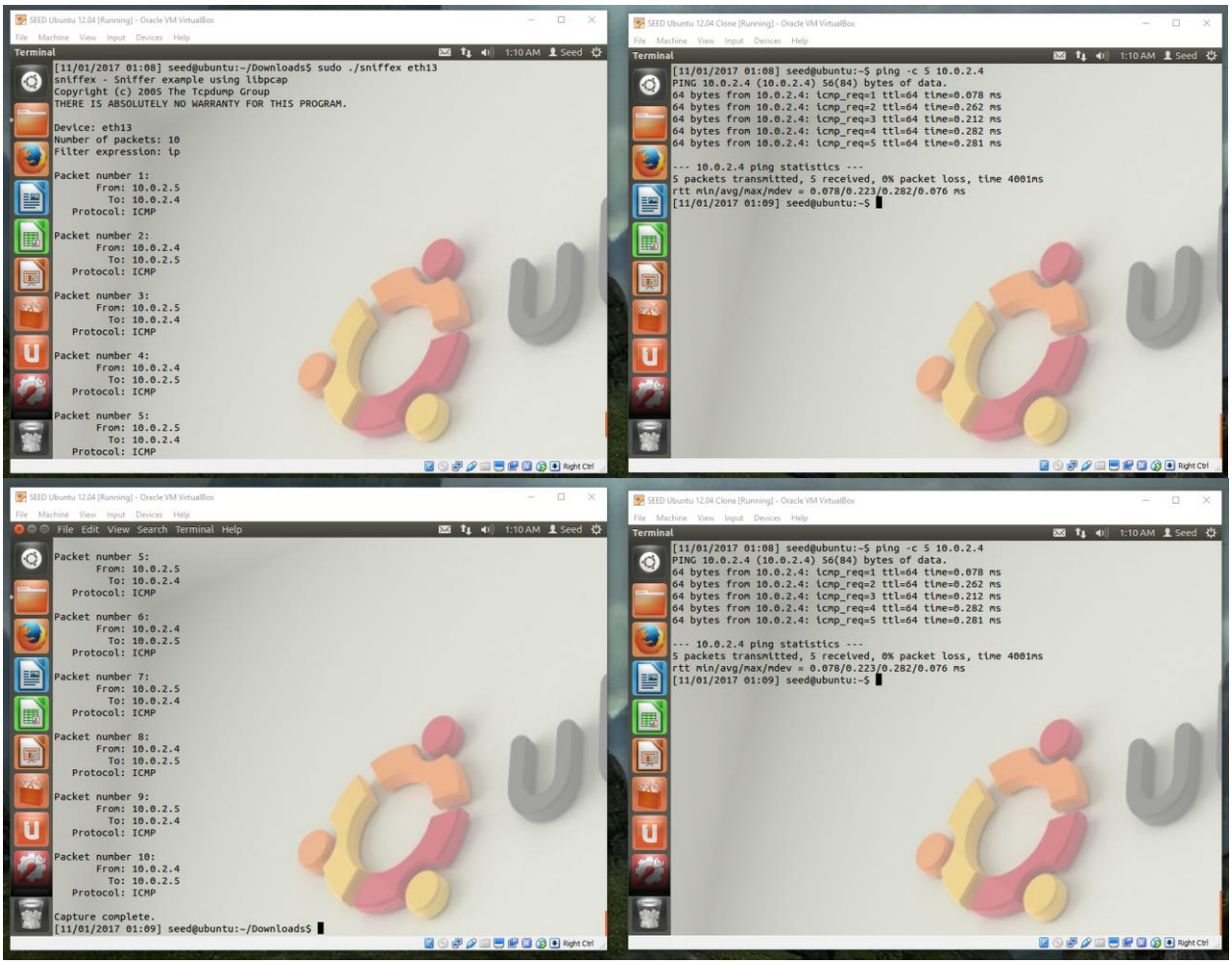
Problem 1: Verifying the Network

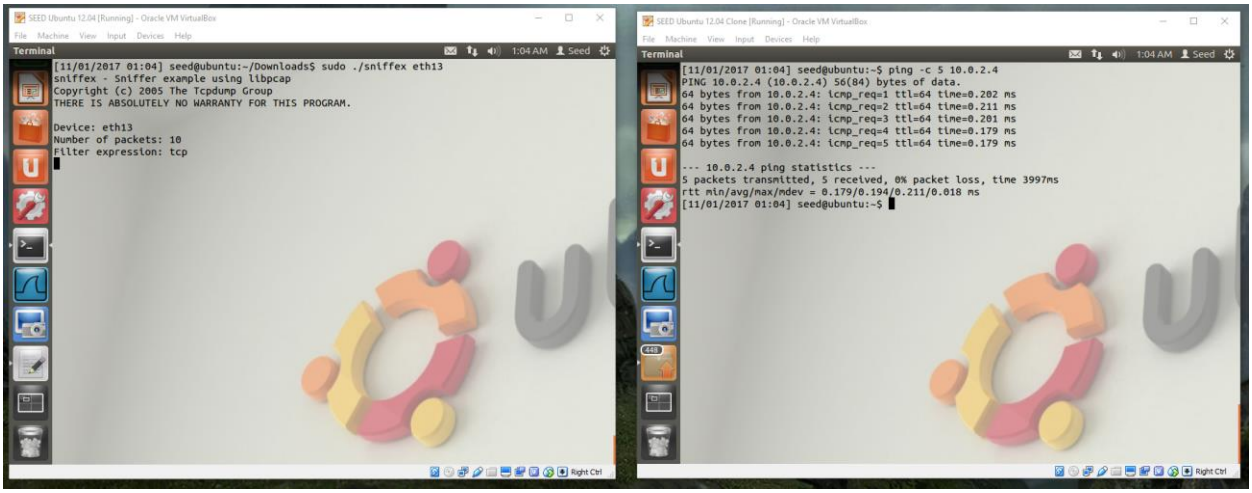


Problem 2: Writing a Packet Sniffer

Summary of pcap library use:

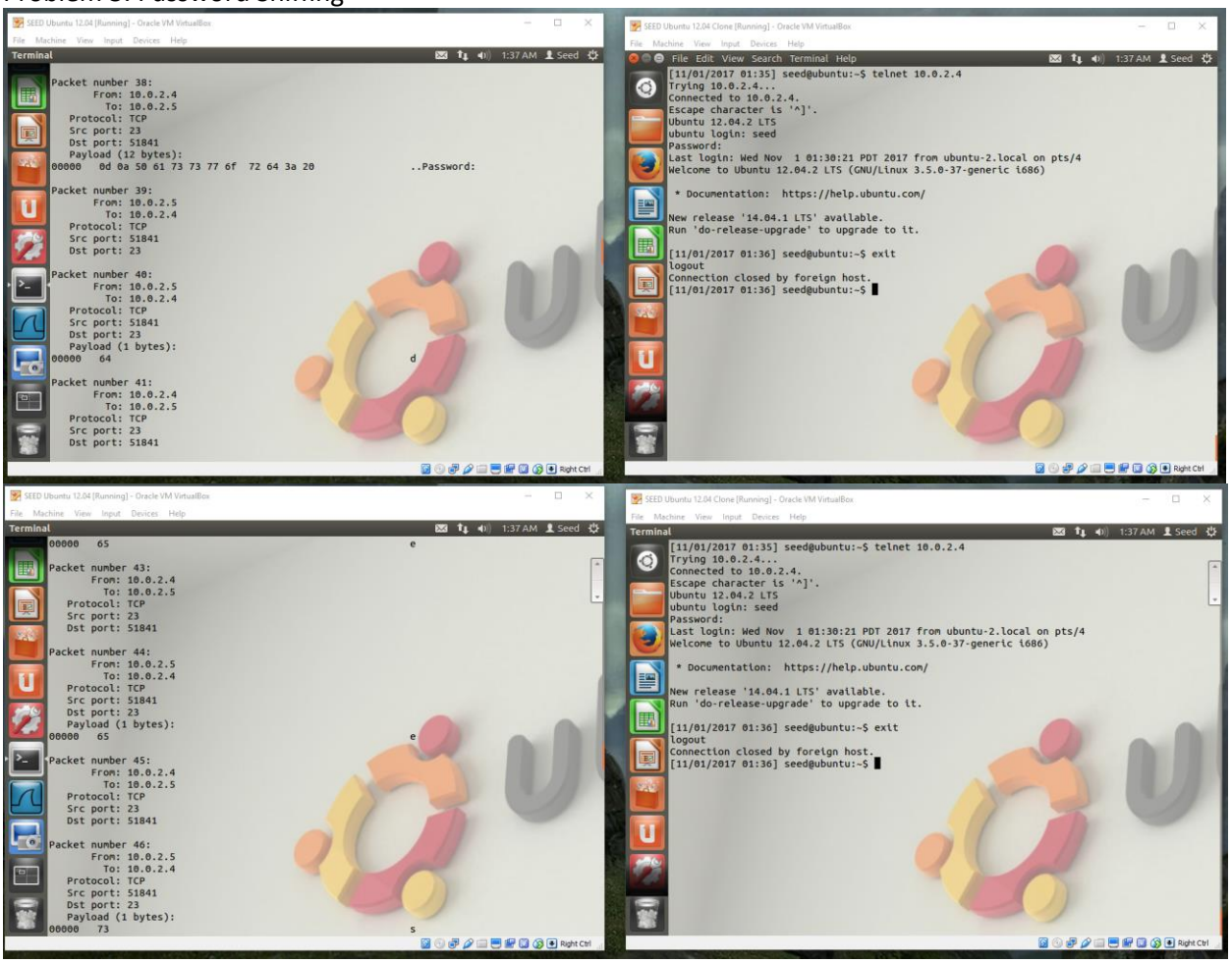
After the interface to be sniffed is chosen, either the device is defined in a string or we can ask pcap to provide the name of an interface that will do the job. Pcap is then initialized once it knows which device(s) it will be sniffing via file handles for sessions. If you want to get specific, you create a rule set, “compile” it, and apply it to whichever session that will be filtered. Lastly, pcap enters an execution loop where it waits until it has received however many packets desired. For every time, it gets a new packet in, it calls another function that we have already defined.





ICMP files are being sent over so with the tcp filter on, nothing appears.

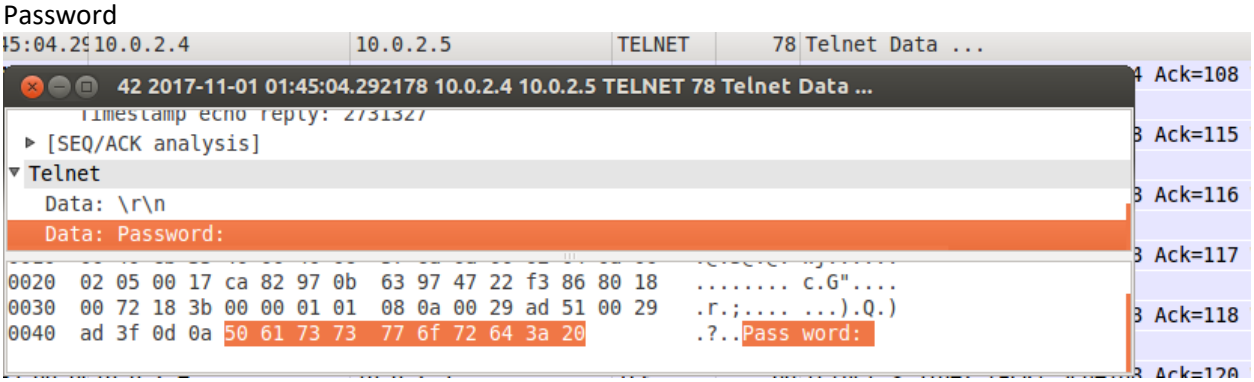
Problem 3: Password Sniffing



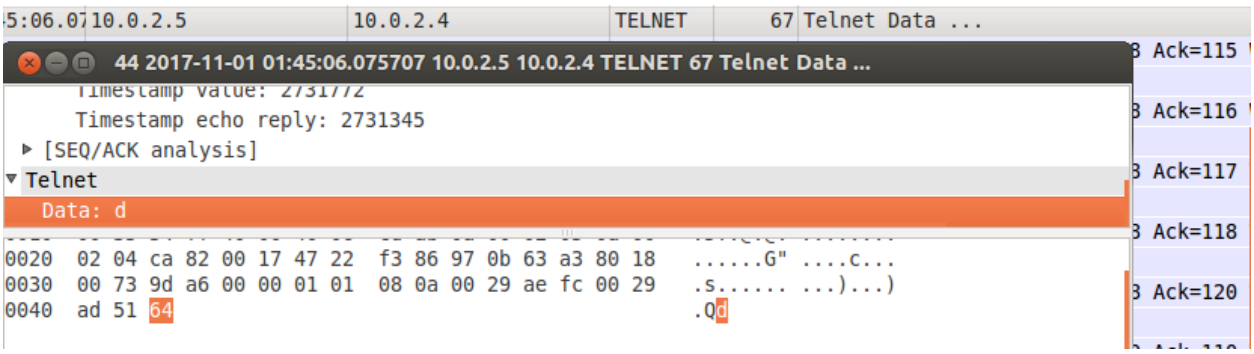
it recorded the password: “dees”

Using Wireshark

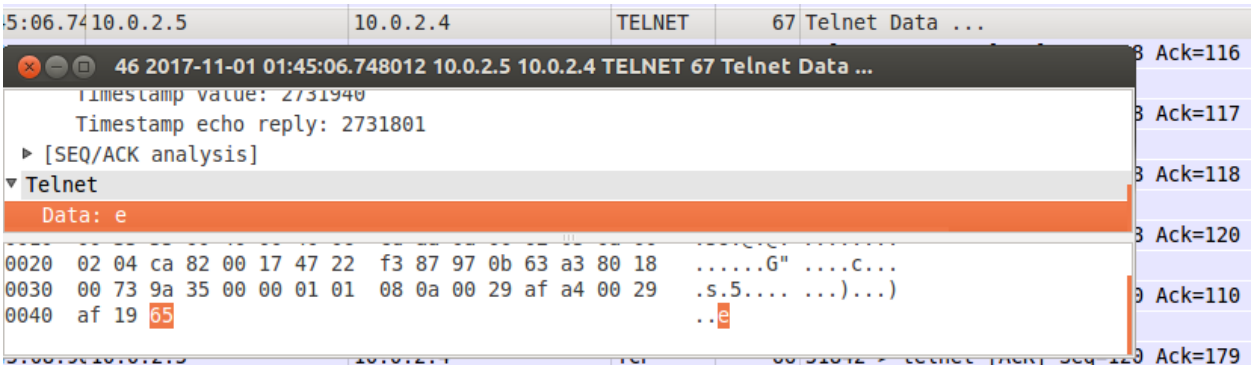
Password



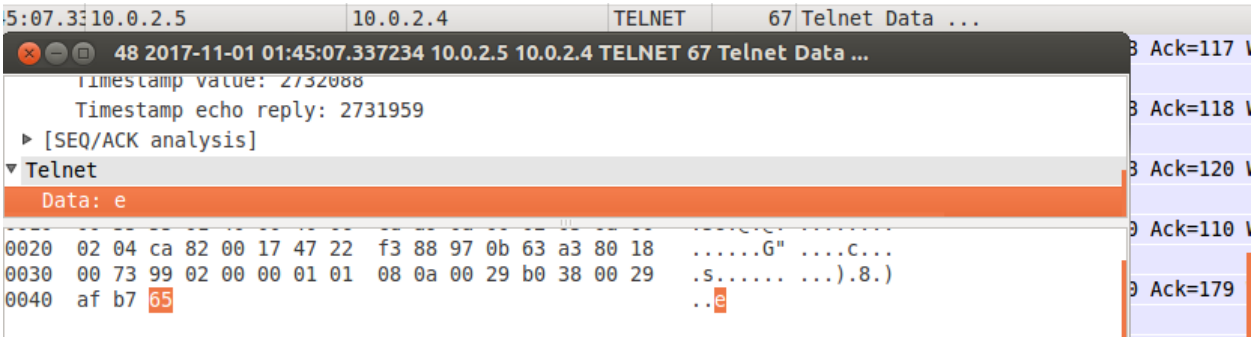
d



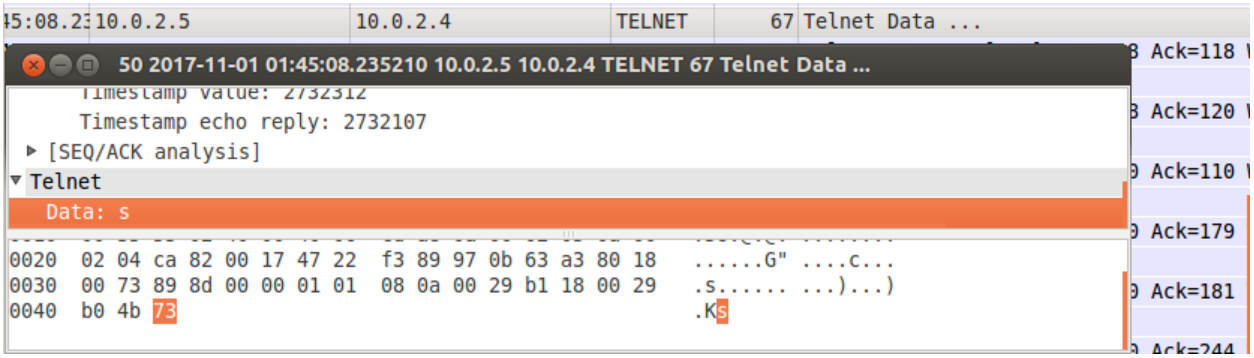
e



e

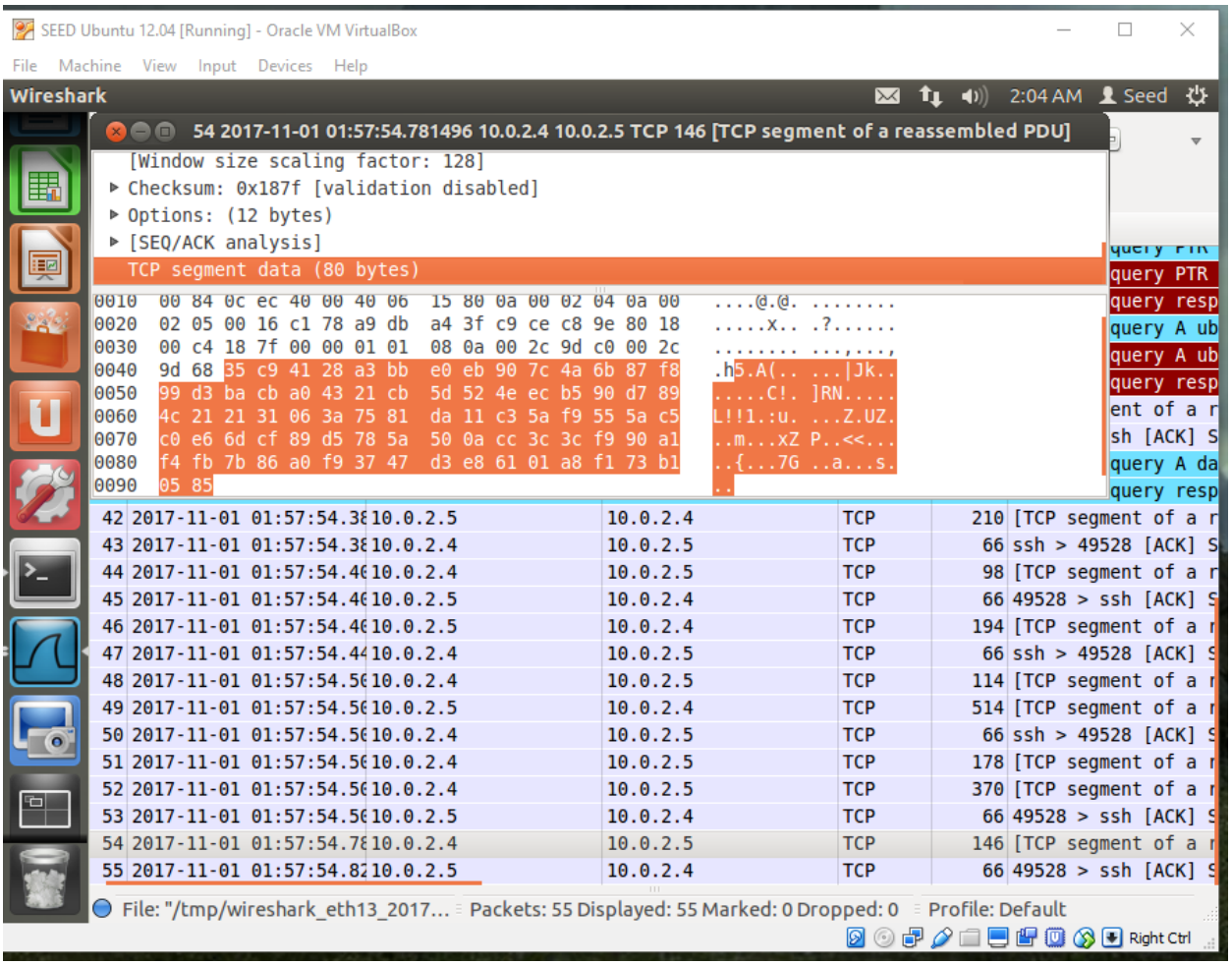


s



After doing these tests, it's surprising how easy it is to access information that is passing through. At the same time, it makes a lot of sense how this works and is possible. You're just simply taking a deeper look at the packets being transmitted. This really shows the importance of encryption.

Problem 4: SSH



Instead of Wireshark being able to pick up the user input key by key, SSH had everything come in as a chunk. The data is also encrypted and I currently don't have any means of deciphering it.