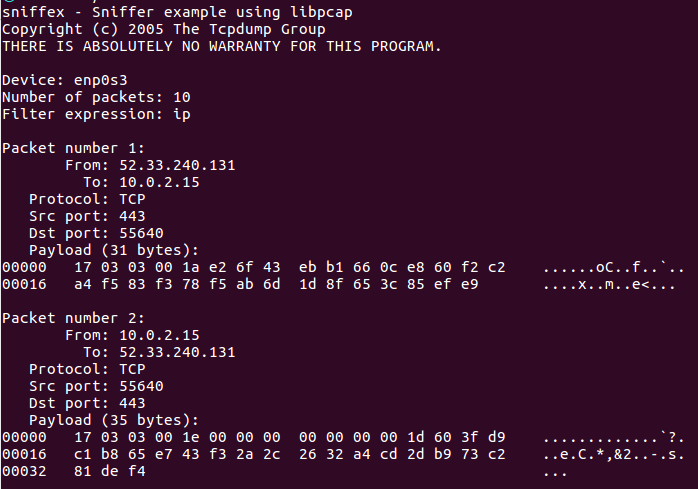
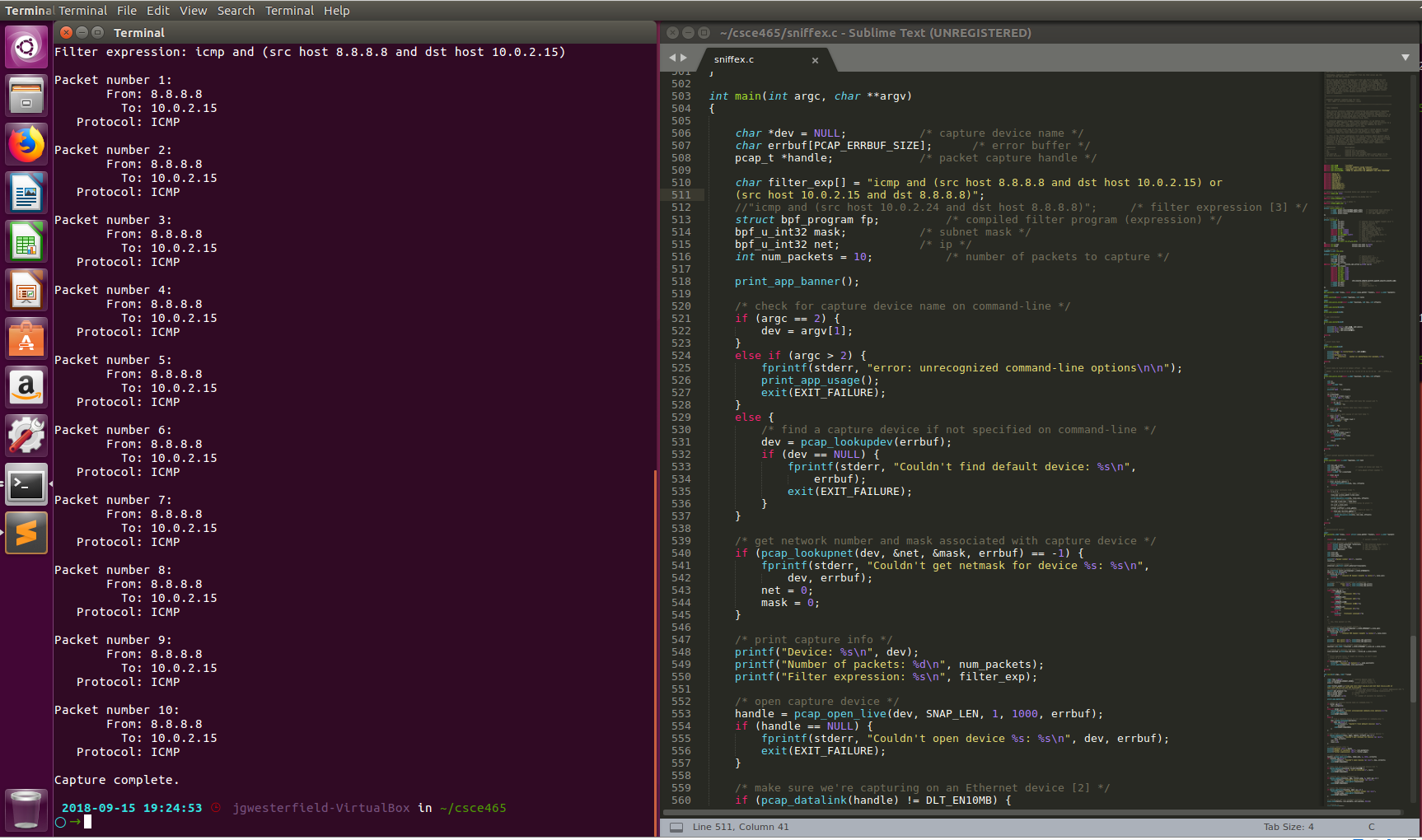
CSCE 465 Lab 1

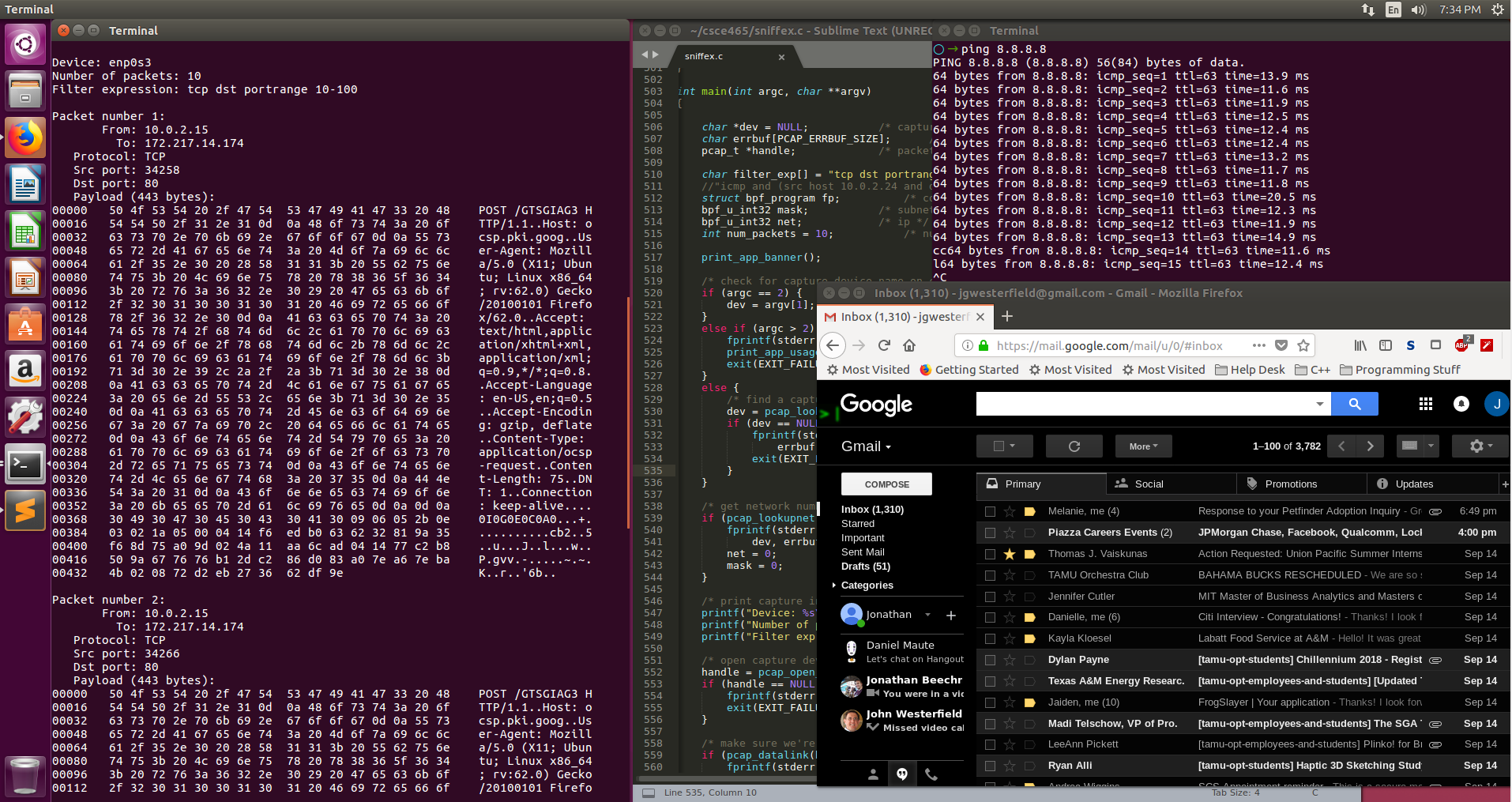
1. Please use your own words to desribe the squence of the library calls that are essential for sniffer programs.
   * First we have to find the capture device by finding the subnet (pca\_lookupnet), create a handle in order to open the device we are watching (pcap\_open\_live), check to see if we are actually reading data (pcap\_datalink), compile and set the filter expression to create a filter for the data (pcap\_compile, pcap\_setfilter), and finally set the call back function to loop through.
2. Why do yo uneed root privilege to run sniffex? Where does the program fail if executed without root privilege?
   * Without root privileges, you cannot access the networking sockets you need to look at.
   * Fails during pcap\_open\_live which is opening a capture device.
3. Turn on and off the promiscous mode in the sniffer. Can you demonstrate the difference when this mode is on and off?
   * Setting promisc to 0 shows the packet contents of every packet that is captured.



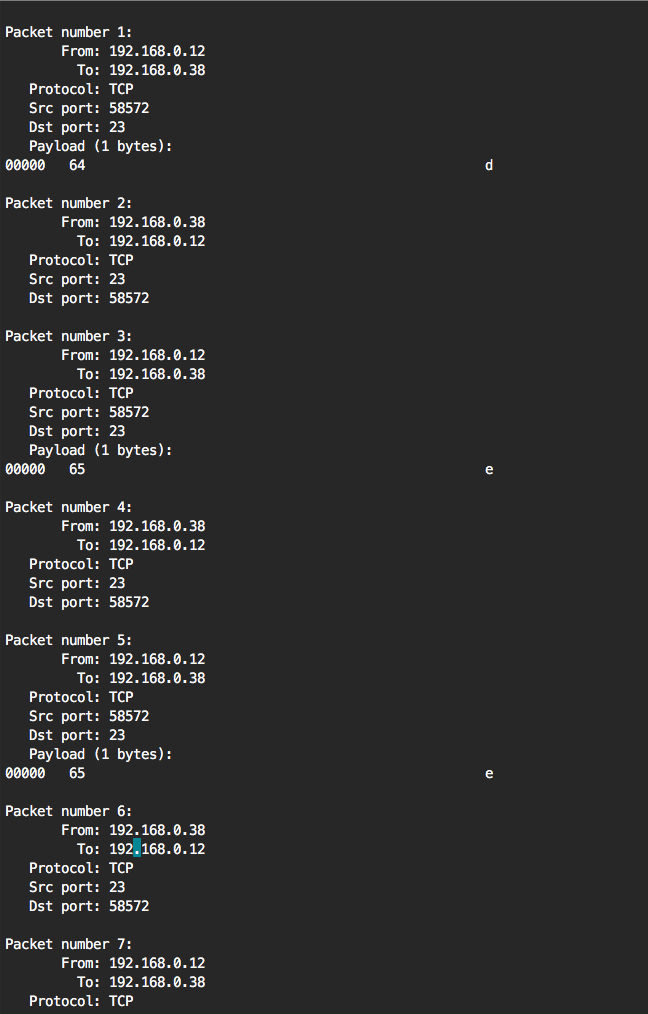
1.b) Changing the filter expression to "icmp and (src host 192.168.0.38 and dst host 8.8.8.8) or (src host 8.8.8.8 and dst host 192.168.0.38)" and we get the output below. Referenced this website to do this: http://www.tcpdump.org/manpages/pcap-filter.7.html



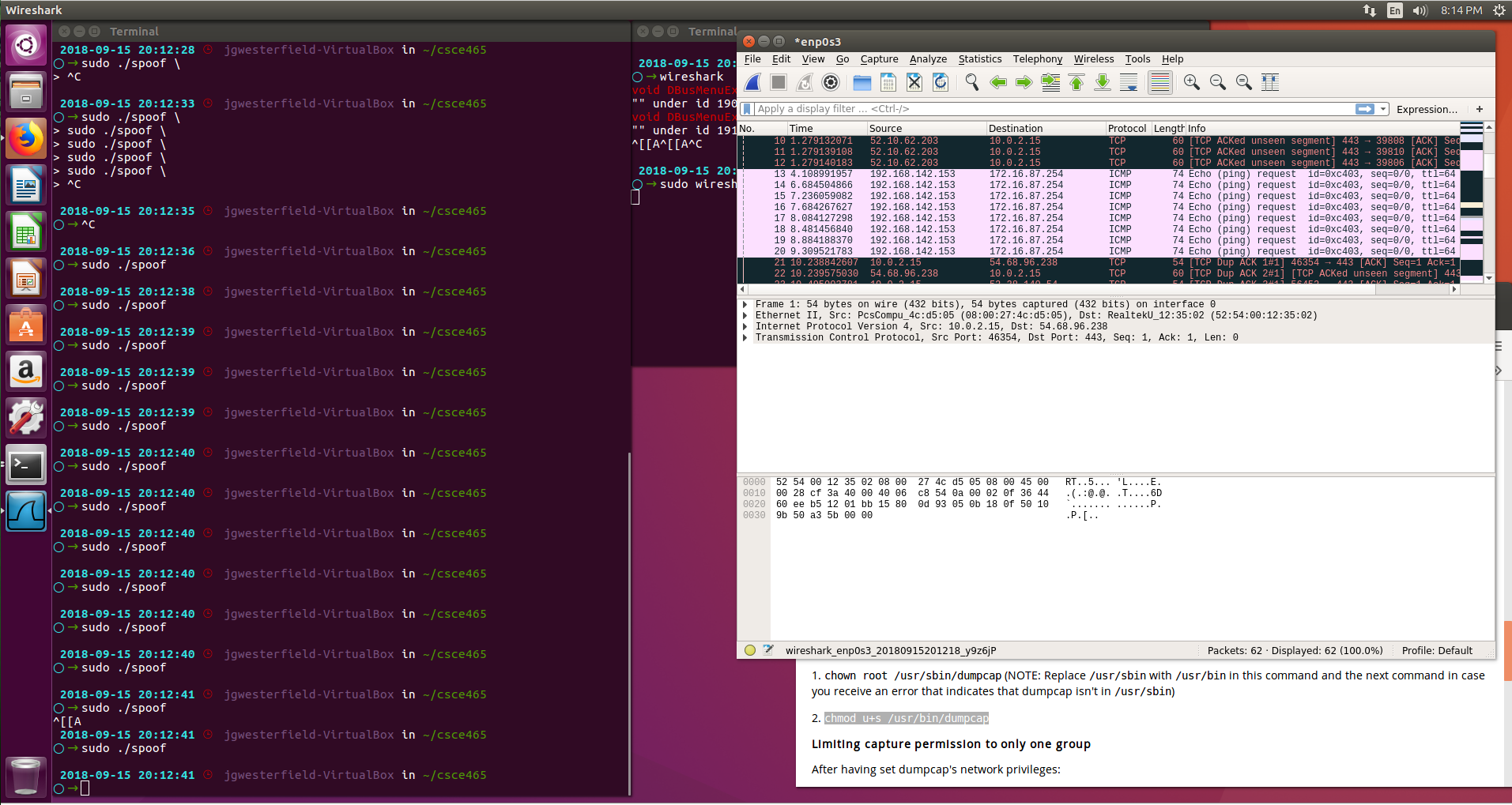
1.b) Changing the filter expression to "tcp dst portrange 10-100" gives the output below when navigating to a webpage using port 80:



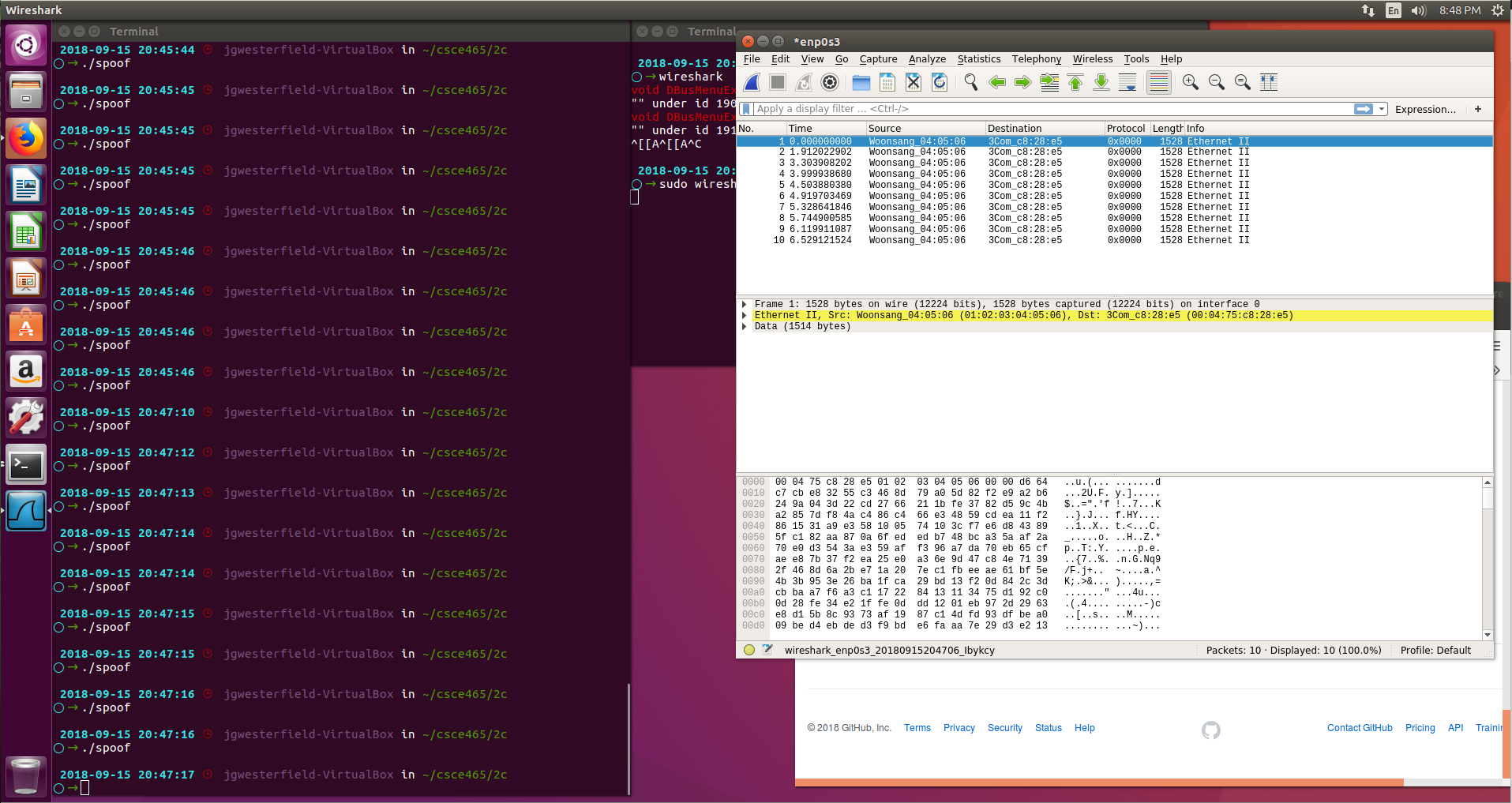
1.c) When changing the filter to "tcp port 23" and starting telnet on port 23, the output is shown below:



2.a/2.b) My spoofing program spoofs a packet saying that it is sent from 192.168.142.153 to 172.16.87.254. I accidentely skipped over this and went straight to 2b. The output is shown below from wireshark:



2.c) When setting 01:02:03:04:05:06 as the source and spoofing the ethernet frame, I get the traffic from wireshark below:



4) Can you set the IP packet length field to an arbitrary value, regardless of how big the actual packet is?

* Yes you can but it will not do anything. If the size is manually set to size smaller than the actual packet size, the system corrects this by calculating the actual size and resetting the length field to the correct value. However, if the value is set higher than the actual size, there shouldn’t be any issue as long as it is not larger than the maximum packet size.

5) Using the raw socket programming, do you have to calculate the checksum for the IP header?

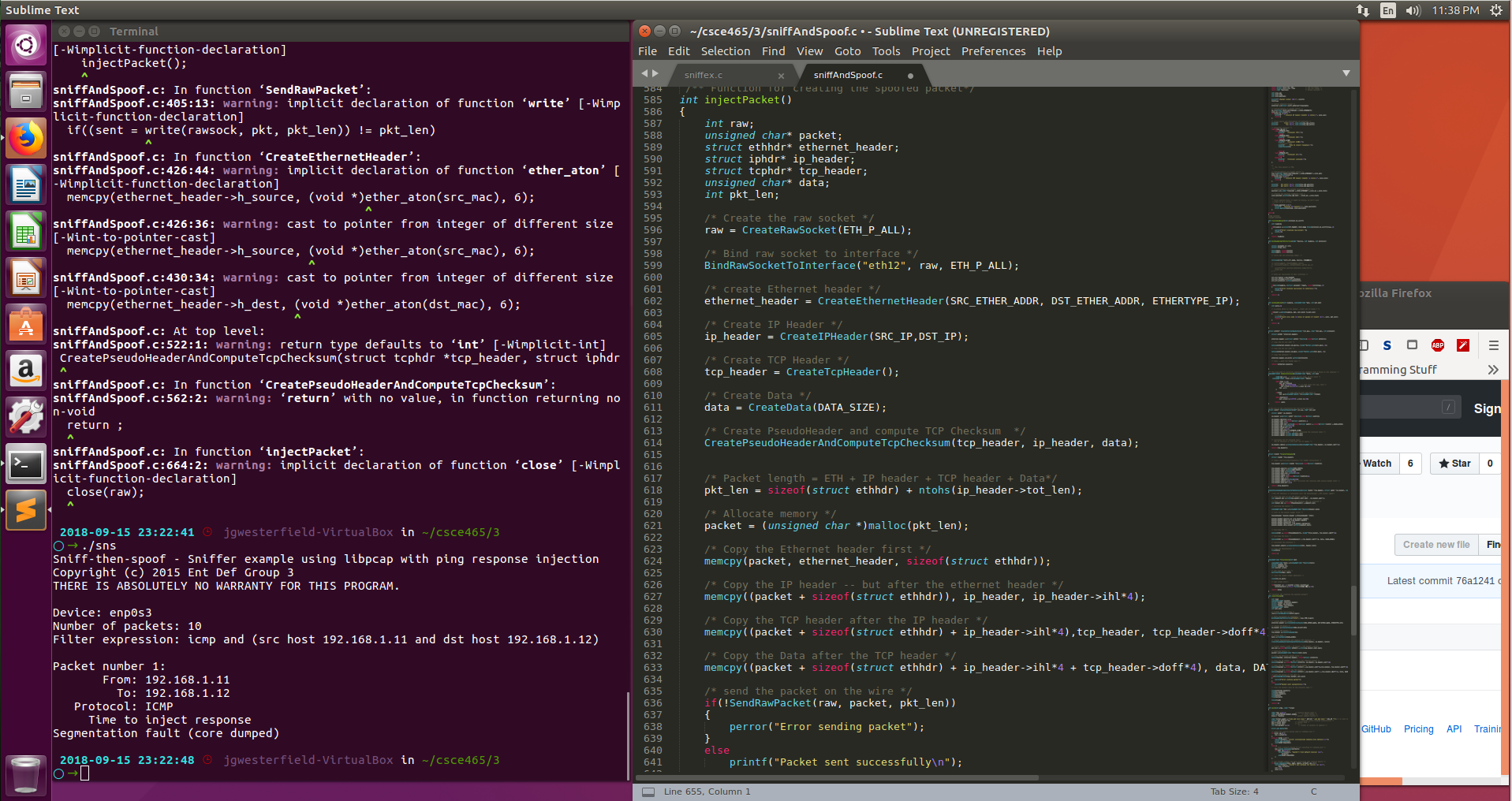
* Yes you do. Since we are creating the packet ourselves, we must calculate the correct checksum. If we don’t, the packet will get dropped once it reaches its destination because the checksum listed will be incorrect from the actual checksum.

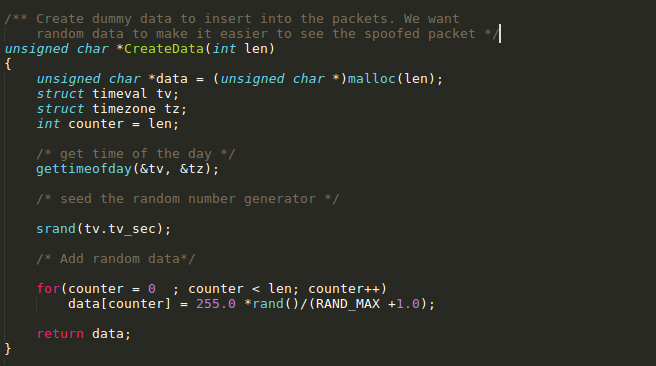
6) Why do you need the root privilege the run the programs that use raw sockets? Where does the program fail if executed without root privileges?

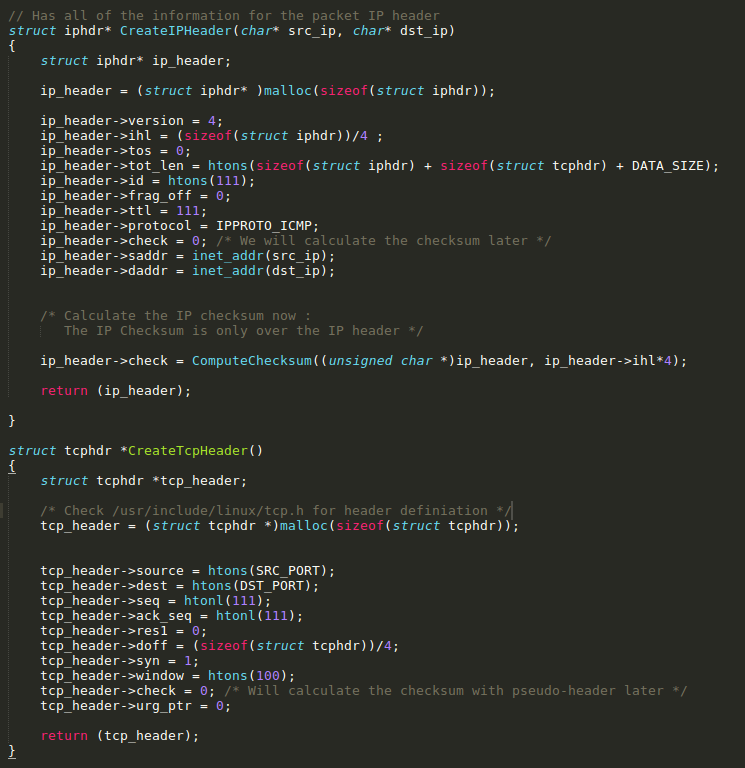
* It's because you can spoof custom packets, which may interfere with inbound traffic. It also can break other rules for networking that are in place

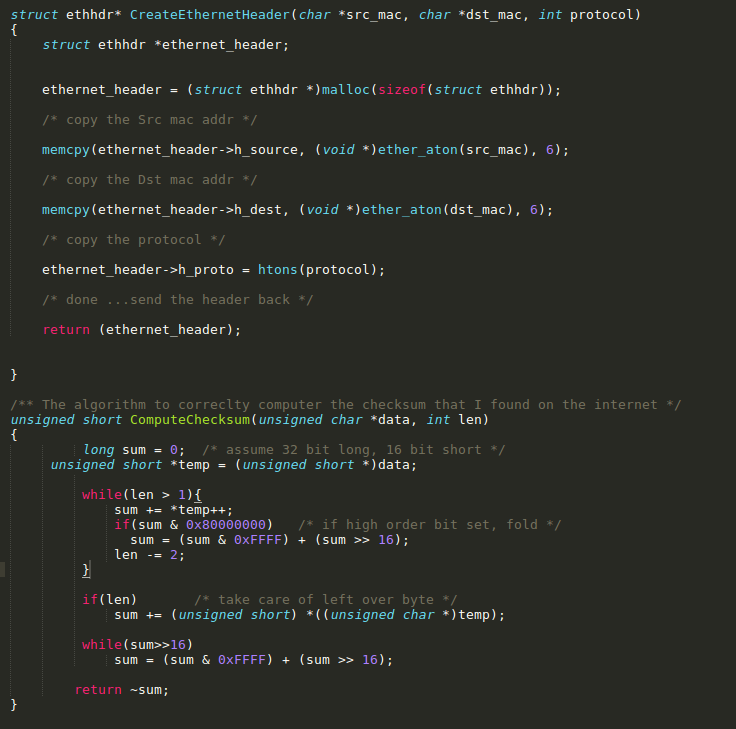
TASK 3)

Unfortunately, I could not get a working solution. Everytime I would try to run it, it would register that there was a ping, but it would seg fault and I couldn’t figure out a solution











This is where the code broke. For whatever reason, ioctl() returned -1 and would crash the program.