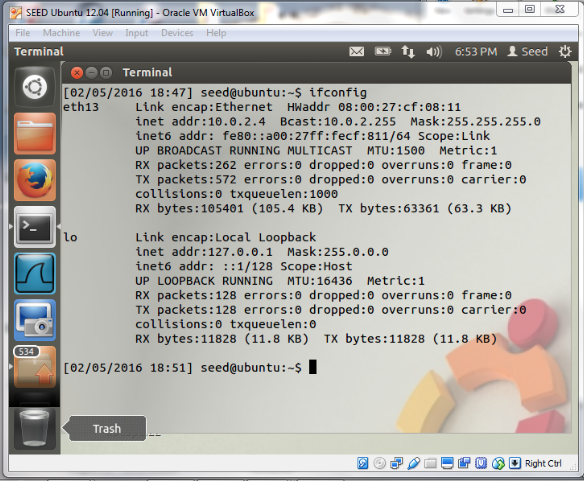
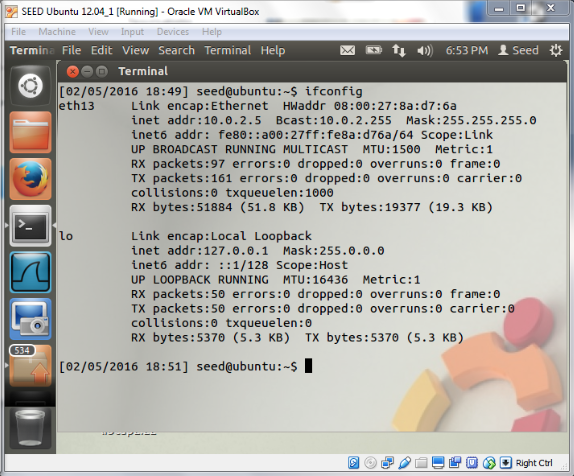
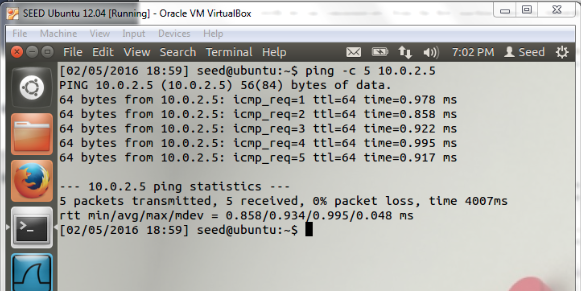
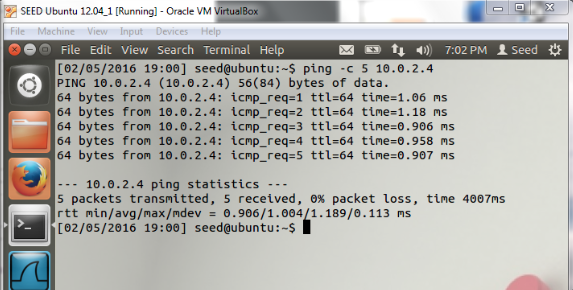
**CS380 Exercise 3 Kyle Turchik**

**Problem 3.1**





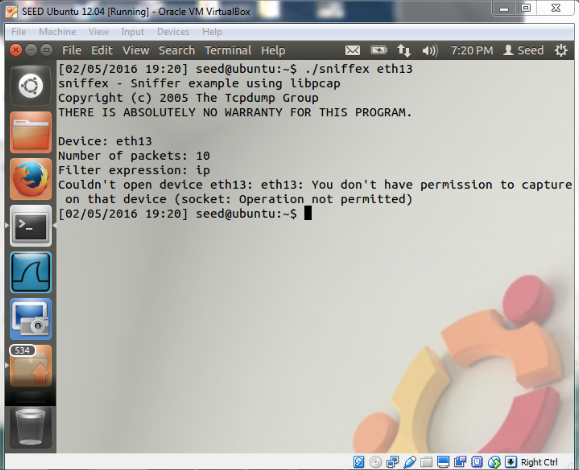




**Problem 3.2**

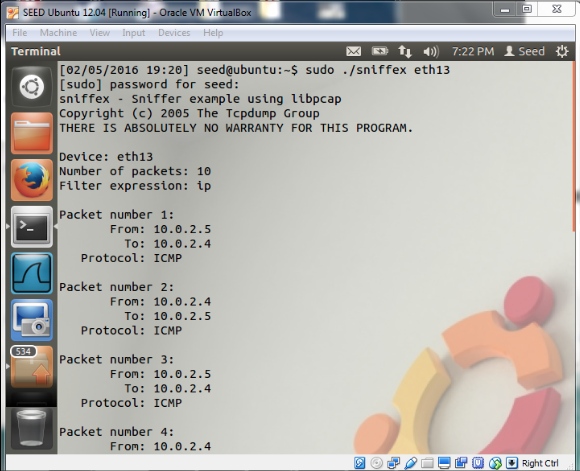
*Summarize how the pcap library is used.*

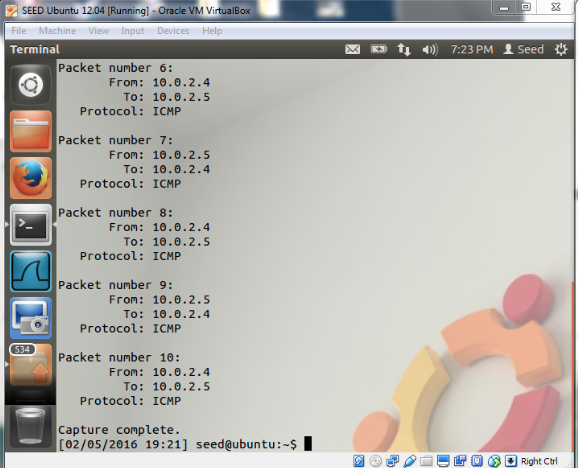
The pcap library determines the interface to use for packet sniffing. It initializes the library with a target device or multiple devices, filters which traffic to sniff (TCP, IP, etc.), then loops until a specified number of packets have been sniffed.

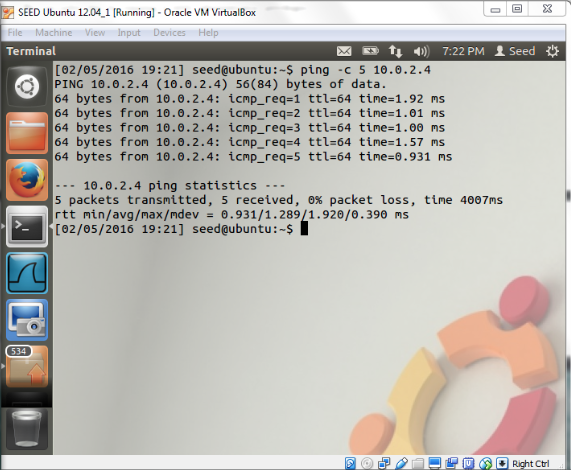


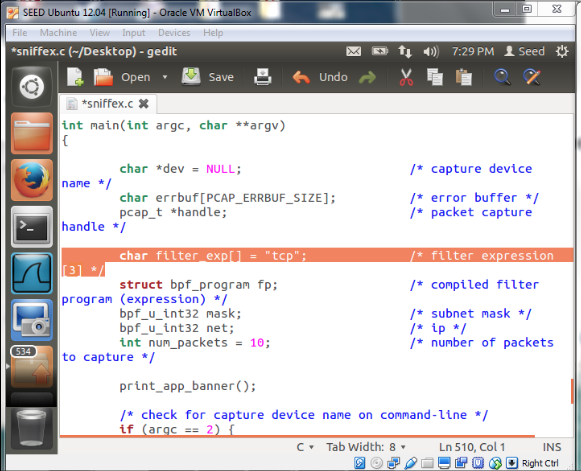
*What happens? Why does the program fail to start properly?*

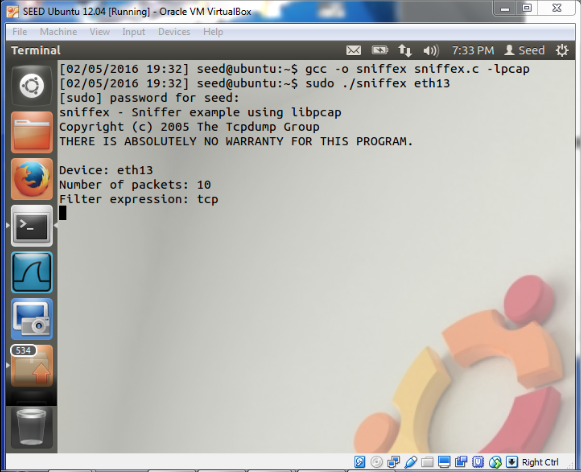
The user requires additional privileges.







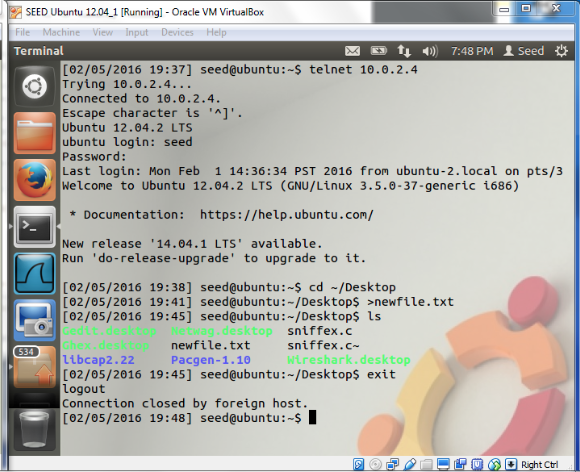


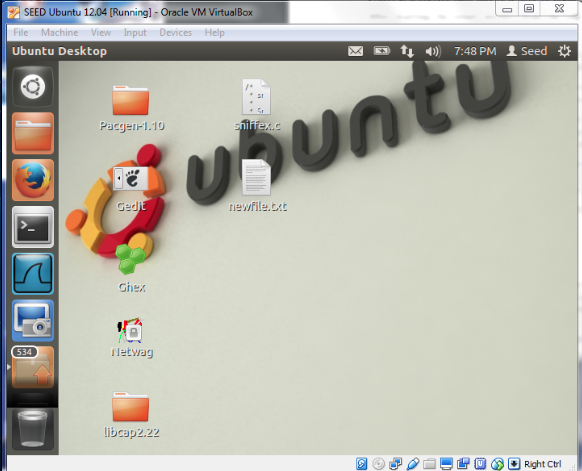


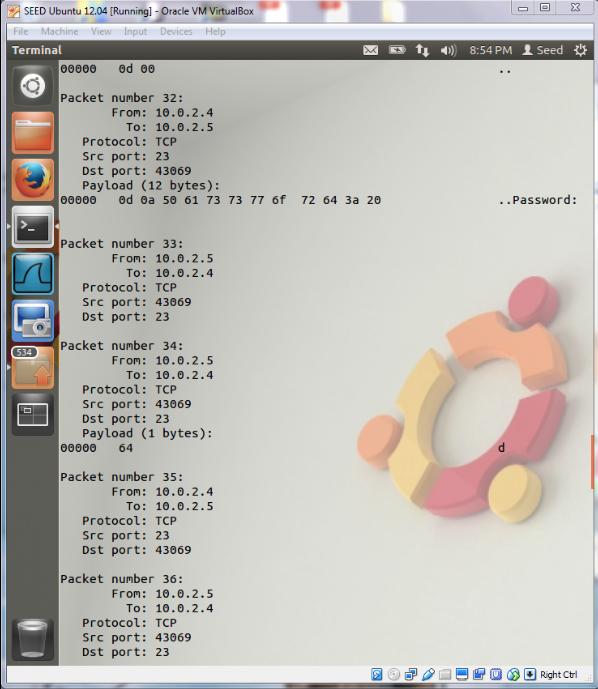
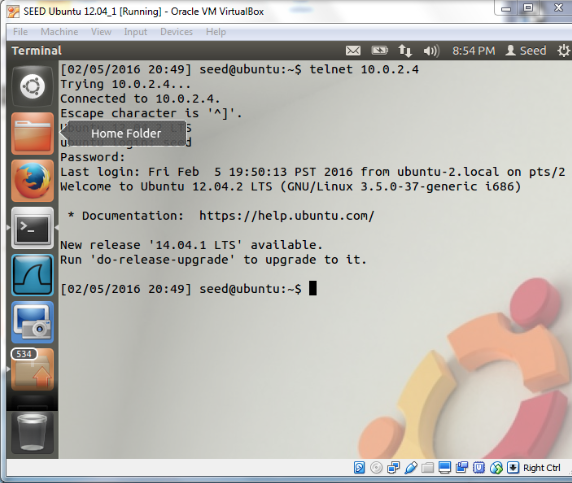
*What has changed?*

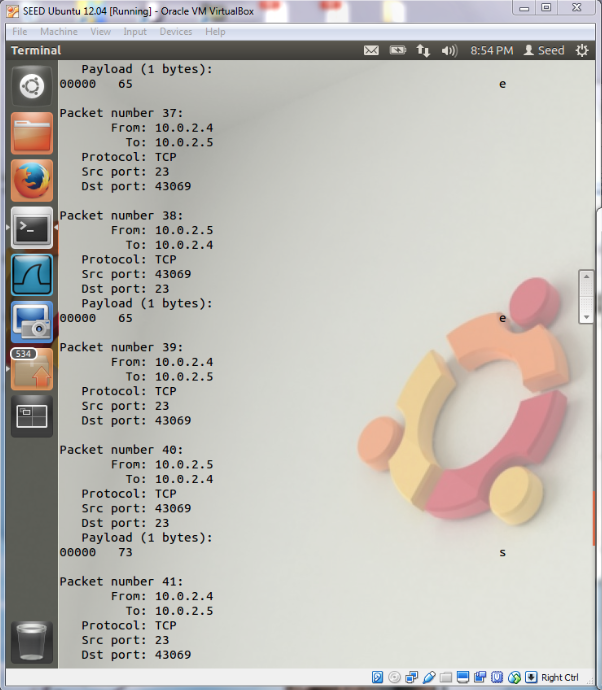
After modifying the sniffer code to only capture TCP packets, the program did not record any data. The pings are not TCP traffic.

**Problem 3.3**









*Discuss your thoughts about the security of using telnet as a method of remotely using* ***telnet*** *a system.*

The user’s username and password were both visible in the telnet sniffer and Wireshark captures.

Since telnet sends login information in plaintext, it is a very insecure system.

**Problem 3.4**

*Can you find the user’s password?*

The user’s username and password were NOT visible in the Wireshark packet capture.

Using SSH is more secure than using telnet since it is an encrypted system.