

**SI430: Lab 04 --- Lab Title**

Names: ­**Brendan Lewis, Ian Coffey**

Alphas: 263708

External source(s)   
(“I referred to this site for x,” etc.)

Honor

We wrote the code on our own except the help from the external source(s) listed above. Moreover, we didn’t copy any part of the code from other midshipmen.

Initials: BL and IC

Challenges

(e.g., it was difficult to figure out how to x)

It was difficult understanding the relative positions of different values such as the tcp\_header length. However, upon learning how to see these in wireshark it made the task much simpler.

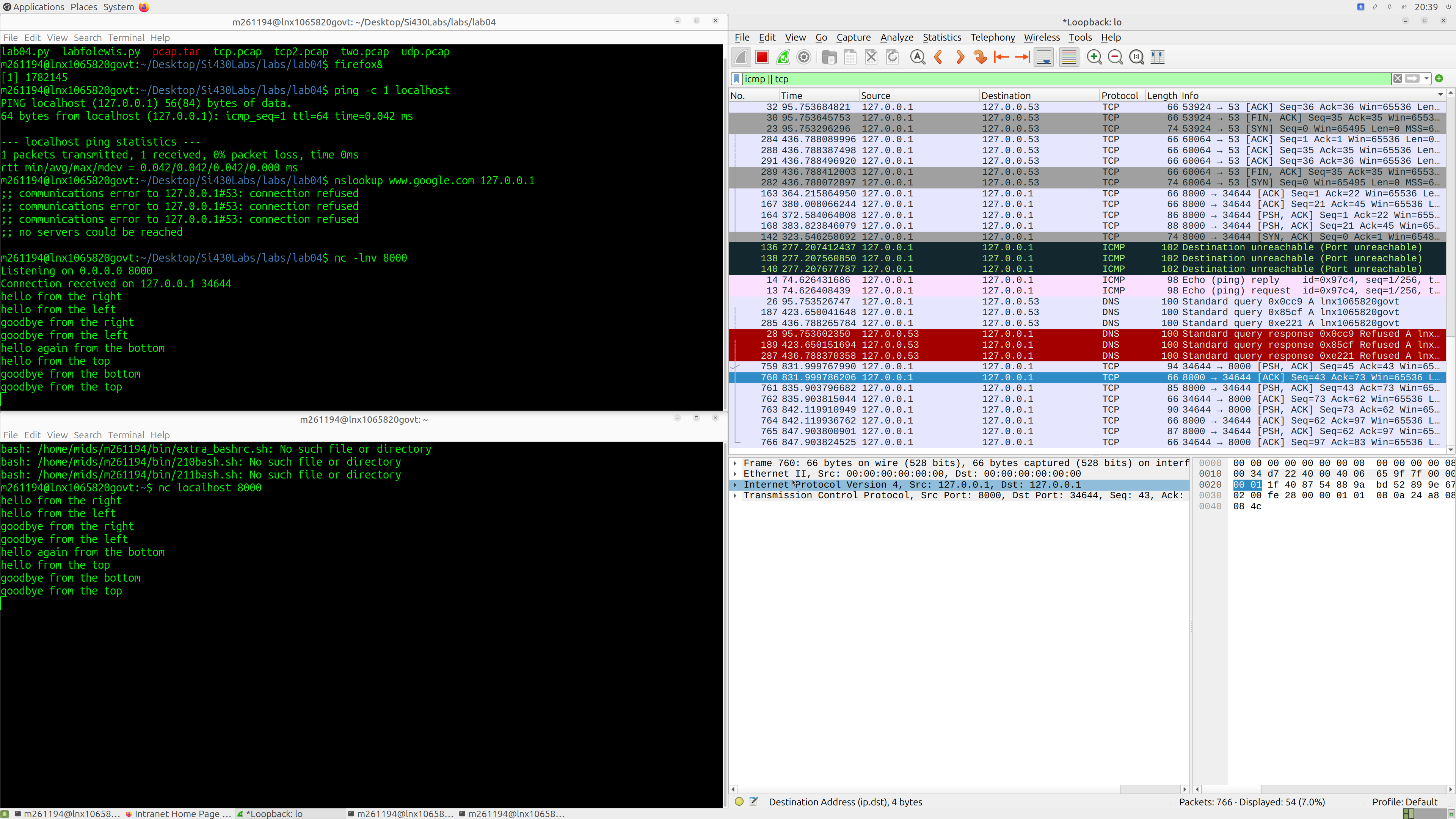
What we learned and what was interesting to us

(Specify what you learned and what was interesting to you)

We learned a lot about how to use wireshark and how useful it can be when you are trying to use it to parse through pcap files.

# **Part 1**

(For each part of the lab, give your work -- attach code, screen captures, explanations and answers as necessary)

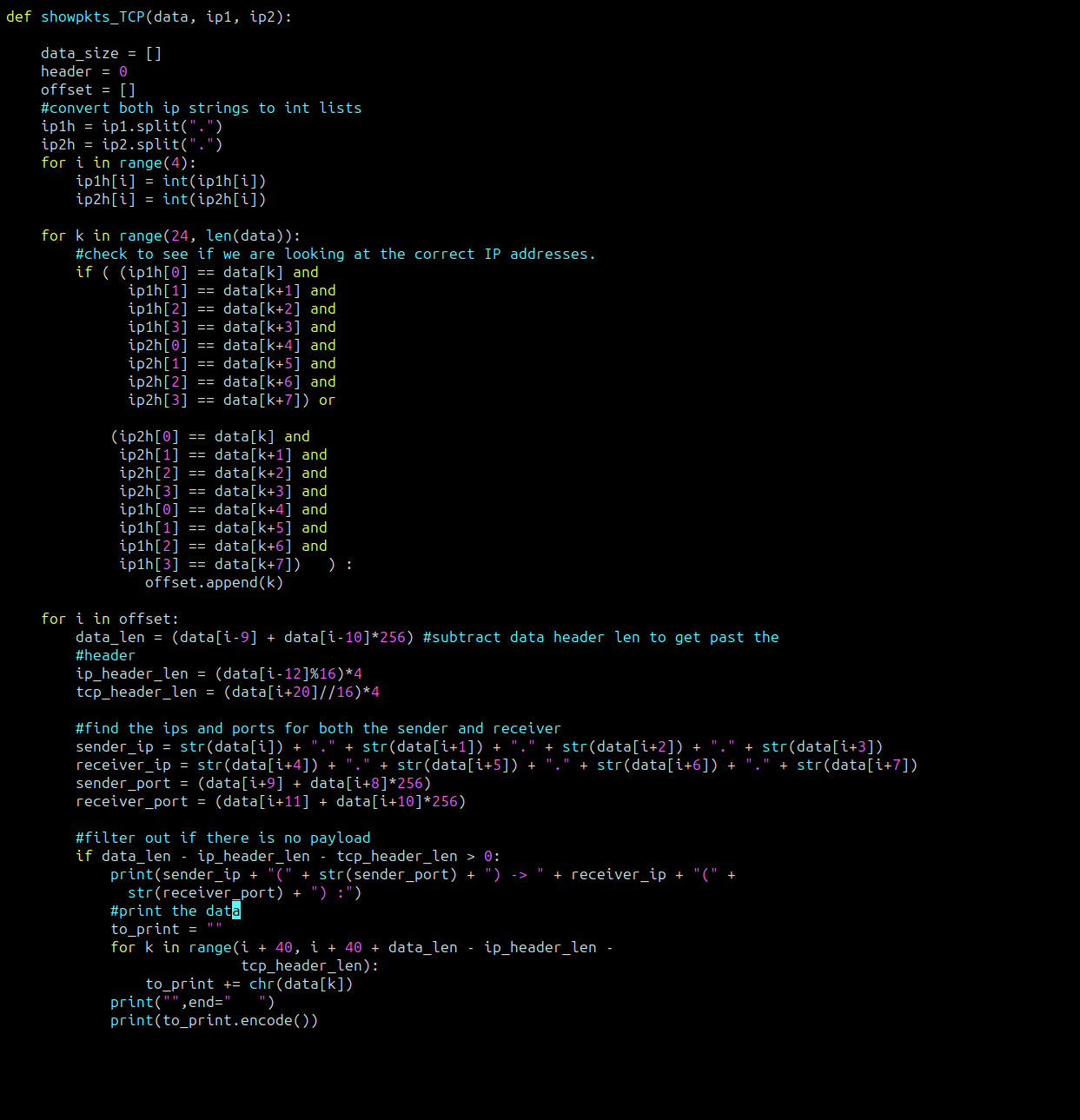


**PART 2**



showpkts\_IP works to parse through data in order to print all of the Ethernet and IP headers. The initial for loop excludes the global header and then loops through data in order to save pointers to the beginning of each packet in the list called offset. The second for loop then utilizes each offset as it’s loop variable ‘i’ i is then used to get the offset and each desired piece of data is extracted utilizing offsets from the beginning of the header.

***PART 3***



showpkts\_TCP first converts the string IPs into int lists so that they can then be used to compare the hex data that is being read to the IPs the user desires. This filters out the undesired packets. Once a packet fits the desired bounds, it is added to an offset list. Each offset is then used in a for loop where that value is used to find the ports, header lengths and locations of the payload so that it can be printed. It is very similar in it’s solution to showpkts\_IP.

aa