CIS*3210
Assignment 3
Deadline: Friday, November 16, 9:00pm
Weight: 10%

Description

This assignment is a series of labs aimed to support the material we have covered in the last three weeks - namely, transport layer and network layer protocols. **You can complete this assignment in teams of 2-3.**

This assignment is meant to make up for lack of labs in the course. As a result, it is ery lab-like in nature - and difficulty. It gives you a chance to examine "live" network traffic (other than as a small part of Assignment 1).

It is essentially a sequence of two labs to help you explore transport and network layer protocols using various software tools: traceroute, wireshark, etc..

Work through these the labs one by one and follow the lab steps carefully. As you do, complete a report document, answering the questions in each lab. Make sure that you create all the plots required by the labs, capture the relevant screenshots, and include them in your report.

Notes:
- The labs are labelled in the same sequence as they appear in the book: TCP, UDP, then IP. Part 0 helps you build some experience using Wireshark, which will come in handy in Parts 2 and 3.
- Make sure you also organize the report in this order.
- Part 2 will require the use of the Ping Plotter utility. You can download a free version here: https://www.pingplotter.com/products/free.html.

Part 0: learning the tools (TCP)

Complete the TCP lab from the textbook: https://gaia.cs.umass.edu/wireshark-labs/Wireshark_TCP_v7.0.pdf. This lab will **not** be graded, so you do not need to actually include anything in the report. It is listed here to help you learn the tools.

Part 1: UDP

Run Wireshark and capture some UDP packets for at least two application level protocols discussed in class (use the "udp" filter, possibly with a port number, to filter out other traffic). Attach a screen shot for each packet capture, along with your comments on how you triggered it.

In addition, do the following:

1. Include a small screenshot of one captured UDP packet from the trace. For that packet:
    1. Determine the length (in bytes) of each of the UDP header fields by consulting the displayed information in Wireshark's packet content field for this packet.
    2. The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.
    3. What is the protocol number for UDP? Give your answer in decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields).
2. In your capture, examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. Describe the relationship between the port numbers in the two packets. What protocol was this request-ACK sequence for?

Part 2: IP

Complete the IP lab described here: https://gaia.cs.umass.edu/wireshark-labs/Wireshark_IP_v7.0.pdf. You can get a free version of PingPlotter here: https://www.pingplotter.com/products/free.html

- You only need to answer questions 1-9.
- Include Wireshark and Ping Plotter screenshots that support your answers. However, please keep the number of screenshots small - you should only need a couple of Wireshark shots and one PingPlotter shot.
- You are welcome to play with the fragmentation section, but please do not include it in your report.

Submission

Submit the report as a PDF file. Make sure the report contains all the answers for Parts 1 - 2, as well as all the screenshots. If you are working as a team, submit one report per team and make sure you list all teammates in the report.