CSCI 4311/5311

Wireshark

Programming Assignment 3

Due Date: April 25, 2024, 11:59 PM

Goal of the assignment

In this assignment, we learn how to use Wireshark.

The basic tool for observing the messages exchanged between executing protocol entities is called a packet sniffer. As the name suggests, a packet sniffer captures (“sniffs”) messages being sent/received from/by your computer; it will also typically store and/or display the contents of the various protocol fields in these captured messages. The second component of a packet sniffer is the packet analyzer, which displays the contents of all fields within a protocol message.

We will be using the Wireshark packet sniffer [http://www.wireshark.org/] for this assignment, allowing us to display the contents of messages being sent/received from/by protocols at different levels of the protocol stack.

I will upload 12 pdf file which covers all topics in this class. However, you will be responsible for only 3 of them as I describe below. You can check other pdf files for practice. Each pdf file explains what you need to do step-by-step. Follow the instructions in the pdf files.

For each question, you need to **show your results by screenshot.** If screenshot is not necessary, explain your answer with details.

Rules:

- We have 33 questions. Each question is 3 points.
- 1 point is bonus to everyone who submits the assignment.
- You need to provide a screenshot for each question. Also, you need to briefly explain your screenshot.
- Save your report in PDF format.
- Without the report, you don’t get any points.

Part 1 – Wireshark Introduction

Check: 01 - Wireshark_Intro_v8.0.pdf file

This file shows you how to setup Wireshark step by step. You need to answer **4 questions** at the last page of the file **(Page 10)**.

Part 2 – Wireshark TCP

Check: 04 - Wireshark_TCP_v8.0.pdf file

This part investigates the behavior of the celebrated TCP protocol in detail. You need to answer the following questions.

Page 4 – Q1, Q2, Q3.

Pages 5 and 6 – all questions from Q4 to Q12

Page 8 – Q13, Q14

Part 3 – Wireshark IP

Check: 06 - Wireshark_IP_v8.0.pdf file

This part investigates the IP protocol. You need to answer the following questions.

Page 4, 5 and 6 – Q1 to Q15