CS 315: Computer Networks Lab
Spring 2024-25, IIT Dharwad
Assignment-5

Wireshark Lab: TCP

February 3, 2025

Lab Instructions

- Login to the Ubuntu OS on your machine. The login credentials are as follows:
  - Username: user
  - Password: 123456
- Mark your attendance in the attendance sheet before leaving the lab.
- Handle the lab resources with utmost care.
- Please go through the following exercises in today's lab.
- It is recommended that you complete all the following exercises during the lab slot itself.
- If you face any difficulties, please feel free to seek help online or from your peers or TAs.
- After finishing all exercises, please carry your solutions (via email/pen drive) for future reference, and delete the files from the desktop.

Introduction

In this lab, we'll investigate the behavior of the celebrated TCP protocol in detail. We'll analyze a trace of the TCP segments sent and received in transferring a 150 KB file (containing the text of Lewis Carrol's *Alice's Adventures in Wonderland*) from your computer to a remote server. We'll study TCP's use of sequence and acknowledgment numbers for reliable data transfer; we'll see TCP's congestion control algorithm – slow start and congestion avoidance – in action; and we'll look at TCP's receiver-advertised flow control mechanism. We'll also briefly consider TCP connection setup and investigate the performance (throughput and round-trip time) of the TCP connection between your computer and the server.

Part 0: Paste a screenshot of your system IP address, using `ipconfig` (on Windows) or `ifconfig` (on Mac and Linux), and fill out this Google form to submit the details of your system. The same system must be used to attempt all exercises of this lab.

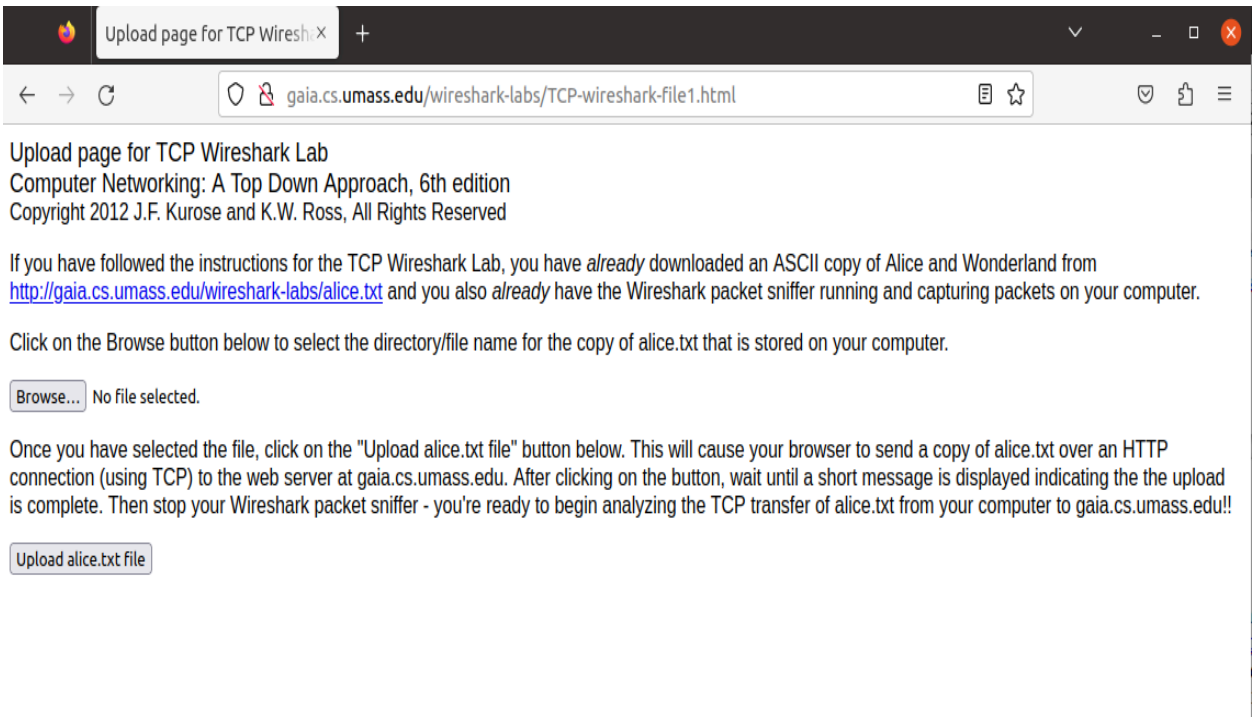
Part 1: Capturing a bulk TCP transfer from your computer to a remote server

Before beginning our exploration of TCP, we'll need to use Wireshark to obtain a packet trace of the TCP transfer of a file from your computer to a remote server. You'll do so by accessing a Web page that will allow you to enter the name of a file stored on your computer (which contains

the ASCII text of *Alice in Wonderland*), and then transfer the file to a Web server using the HTTP POST method. We're using the POST rather than the GET method as we'd like to transfer a large amount of data from your computer to another. Of course, we'll be running Wireshark during this time to obtain the trace of the TCP segments sent and received from your computer.

Do the following:

- Start up your web browser. Go the http://gaia.cs.umass.edu/wireshark-labs/alice.txt and retrieve an ASCII copy of *Alice in Wonderland*. Store this as a .txt file somewhere on your computer.
- Next go to http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html
- You should see a screen that looks like the Figure below.



- Use the ***Browse*** button in this form to the file on your computer that you just created containing *Alice in Wonderland*. Don't press the "*Upload alice.txt file*" button yet.
- Now start up Wireshark and begin packet capture (see the earlier Wireshark labs if you need a refresher on how to do this).
- Returning to your browser, press the "*Upload alice.txt file*" button to upload the file to the gaia.cs.umass.edu server. Once the file has been uploaded, a short congratulations message will be displayed in your browser window.
- Stop Wireshark packet capture.

Answer the following questions

1. State the number of `GET` and `POST` requests to the `gaia.cs.umass` website.
2. State the different type(s) of `http` status code(s) observed in this connection to `gaia.cs.umass` website.
3. Expand the TCP conversation stream for this connection to `gaia.cs.umass` website and answer the following questions.
    a. What are the source and destination IP addresses in the HTTP GET/POST requests?
    b. What are the source and destination port numbers used in this TCP stream?
    c. How many packets are exchanged to establish a TCP connection between your system and the `gaia.cs.umass` website, and what are these packets' specifications?
    d. What are the `Sequence Number` and `Acknowledgment Number` for the `SYN`, `SYN-ACK`, and `ACK` packets?
    e. Which field in the 3 TCP packets – used to establish a connection with the `gaia.cs.umass` website – confirms that the packets are actually the `SYN`, `SYN-ACK`, and `ACK` packets? Provide the screenshots for the same.
    f. How many reassembled TCP segments are present for the first HTTP request?
4. What is the round trip time (RTT) taken to establish the 3-way handshake?

Part 2: Analysing the POST packet contents

Answer the following questions based on the traces in the HTTP POST request and its corresponding response packets.

1. What does the `Reassembled TCP Segments` field in the HTTP POST packet indicate about how the file was uploaded?
2. Why do the first and last segments matter in verifying the integrity of the file uploaded? Does it contain any information regarding the file?
3. In which TCP segment can you find the beginning of the actual file contents?
4. What is the total size of the Reassembled TCP segments, and what does it represent?
5. What is the length of each TCP segment?

Part 3: Analysing the window scaling

1. What is the Maximum Segment Size value considered in this connection? (HINT: You will find this information in one of the packets of the 3-way handshake)

Instruction: Select the following two fields in any of the packets of the TCP stream and right-click and select “Add as column” option, these two fields will be visible as columns in the Wireshark.

2. What is the value of the `Calculated window size` and the `Bytes in flight` for the `HTTP POST` packet (the last TCP segment)? Does any of these two field values change in comparison to the first TCP segment?

3. What is the value of the `Window size scaling factor`?

Submission Details

- Write your answers in a single doc/tex file, and submit its PDF named after your IIT Dharwad roll number, which contains all answers.
- Attach the screenshots for all the answers.