CS3506 - Wireshark Lab 2: TCP

In this lab, we'll explore several aspects of the Transport Control Protocol:

- TCP traffic generated by a POST HTTP message;
- the TCP ACK, slow start and congestion control mechanisms;
- the format and contents of a TCP packet.
- Data contents of a TCP packet

Ensure your PC is running Linux and remember that you have to run Wireshark as the administrative user, so at the command line type "**sudo wireshark**" (without the quotation marks).
You may first also need to run "**xhost +**" to ensure that the X Window System allows Wireshark access to the display.

TCP - E-mail trace

You have already managed to read the contents of the captured email. Keep the wireshark window open.
<u>Print and fill out this assignment</u>

- *<u>Now answer questions 1.1-1.10</u>*

Let's begin by loading the trace. Before analysing the behaviour of the TCP connection in detail, let's take a high level view of the trace.
You should see a series of TCP and SMTP messages between a client and an email server. It starts with the initial three-way handshake containing a SYN, a SYN-ACK and an ACK message.

TCP – HTTP

Start a new capture and filter the packets displayed in the Wireshark window by entering "**ip.addr == 143.239.75.241**" (lowercase, no quotes, and don't forget to press return after typing!) into the display filter specification window towards the top of the Wireshark window.

<u>Download File1 from the assignment site.</u>

The Web page will ask you for the user name and password. From the message you can see the user name while instructions are in the e-mail trace that you downloaded earlier. (**HINT**: you need to run two commands to generate password)
What you should see is a series of TCP and HTTP messages between a client and a web server. Make sure that the files are downloaded and that you did not capture a cache validation message (HTTP 304). Stop the capture.

Note: Wireshark's power lies in filters. You can create a filter for every field in a packet. You can select a field, right click on it and select "apply as a filter". Now Wireshark will only display the packets that have the same value for this field. Here are some filters that might be of use for this lab:

```
tcp.stream eq 0
tcp contains FROM
tcp contains BONUS
tcp.analysis.retransmission
ip.addr == 143.239.211.230 && tcp.port == 80
```

- *<u>Now answer questions 2.1-2.6</u>*

Submission - LAB 2: TCP

Please submit during this lab session or else at next week's lab session.

Student name:_________________________ Student ID:_____________________
Submission date:___________________________

1. TCP - Email trace

1. What are the pairs of IP addresses and TCP ports found in the email communication? Which IP and port belong to the email server and which to the client?

2. From the packet trace, find four different commands for SMTP. Write down packet ID containing those commands.

3. Write down four response codes for SMTP and their corresponding meaning and the packets containing them in the trace.

4. What are the TCP flags of the first three packets of the TCP connection? What is the name of this mechanism?

5. What is the sequence number of the TCP segment containing the mail FROM address? Note that in order to find specific payload, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with "FROM" within its DATA field. How many bytes of TCP payload does this packet contain? What is the FROM email address?

6. Packets No. 9 and 10 have the same sequence numbers. How do you explain this?

7. Select frame 14. What is its ACK number?
It acknowledges frame 13. Use the ACK number and segment information to explain why.
How does Wireshark compute “next Seq number”?

8. View Statistics – Summary. What is the throughput (bytes transferred per time unit) for the TCP connection? Explain how Wireshark calculates this value.

9. How many bytes of TCP payload were transferred in this transmission in total? How did you compute this?

10. Does TCP Header have fixed length? Explain. Verify using the packet trace.

2**. TCP - HTTP trace**

1. What are the client and server TCP ports used for downloading File1?

2. From the packet trace, find request command for HTTP. What is the purpose of this command?

3. Check the HTTP Standard (RFC 2616 for HTTP 1.1). Write down four other HTTP request commands.

4. Write down two response codes for HTTP and their corresponding meaning and the packets containing them in the trace.

5. Check the HTTP Standard (RFC 2616 for HTTP 1.1). Write down response codes for the following response: “Bad request”, “Not Found”, “HTTP Version not Supported”, “Unsupported Media Type”

6. What is the main difference between HTTP and HTTPS?