***Submission - LAB 2: TCP***

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

***Student name:\_Alexander Stradnic\_\_\_\_\_\_ Student ID:\_119377263\_\_\_\_\_\_\_***

***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?

Source: 192.168.19.1:65344

Destination: 192.168.19.140:25

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

- ID 57913 → HELO [CS3506.ucc.ie]

- ID 59689 → MAIL [FROM: labsmaster@cs3506.ucc.ie]

- ID 49255 → RCPT [TO:[itsomp@localhost](mailto:itsomp@localhost)]

- ID 27178 → DATA [<datastream>]

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

- ID 8050 → 220 Service Ready

- ID 8052 → 250 Requested Mail Action okay, completed

- ID 8055 → 354 Start mail input; end with <CRLF>

- ID 8064 → 221 Service closing transmission channel

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

It is known as a Three-way Handshake. First, a TCP packet with the SYN flag is sent to the server from the client. The server then receives this and sends a packet with the flags SYN and ACK. Finally, the client sends a packet with the ACK flag.

1. 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?

TCP Sequence Number: 21

It contains 37 bytes of TCP payload.

1. Packets No. 9 and 10 have the same sequence numbers. How do you explain this?
2. 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”?
3. View Statistics – Capture File Properties. What is the throughput (bytes transferred per time unit) for the TCP connection? Explain how Wireshark calculates this value.

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

2**. TCP - HTTP trace**

1. What are the client and server TCP ports used for downloading over HTTP and HTTPS?
2. Based on reviewing the trace provided what are the risks associated with HTTP traffic as opposed to the use of TLS based HTTPS.
3. How much overhead does encryption incur (how many more Bytes are being transmitted) in the HTTPS case? How did you compute this?