**COMP 535 Computer Networks 1**

**Assignment 3**

**Guidelines:**

Please remember that the assignment must be solved individually. A pdf file with your solutions to the different exercises needs to be uploaded in the "Assignment 3" folder. This .pdf must be named A3_IDi.pdf, where IDi is your McGill id number. Inside the pdf file indicate your name and student id also in the header. **Due date: April 10, 11:59 PM**.

**Exercise 1: TCP congestion control**

Consider that only a single TCP (Reno) connection uses one 10Mbps link which does not buffer any data. Suppose that this link is the only congested link between the sending and receiving hosts. Assume that the TCP sender has a huge file to send to the receiver, and the receiver's receive buffer is much larger than the congestion window. We also make the following assumptions: each TCP segment size is 1,500 bytes; the two-way propagation delay of this connection is 150 msec; and this TCP connection is always in congestion avoidance phase, that is, ignore slow start.

a. What is the maximum window size (in segments) that this TCP connection can achieve?

b. What is the average window size (in segments) and average throughput (in bps) of this TCP connection?

c. How long would it take for this TCP connection to reach its maximum window again after recovering from a packet loss?

**Exercise 2: HTTP protocol**

This hands-on exercise aims at further investigating the HTTP protocol using the wireshark tool. You will need to cover the wireshark HTTP lab uploaded to myCourses and provide answers to the questions indicated in the document: Wireshark_HTTP_v6.1.pdf

**Notes:**

- You can download directly the traces from the link provided in the document and work on them with wireshark, instead of making a capture by yourself.
- The document includes 4 mandatory sections and one optional section.

**Exercise 3: Whois database**

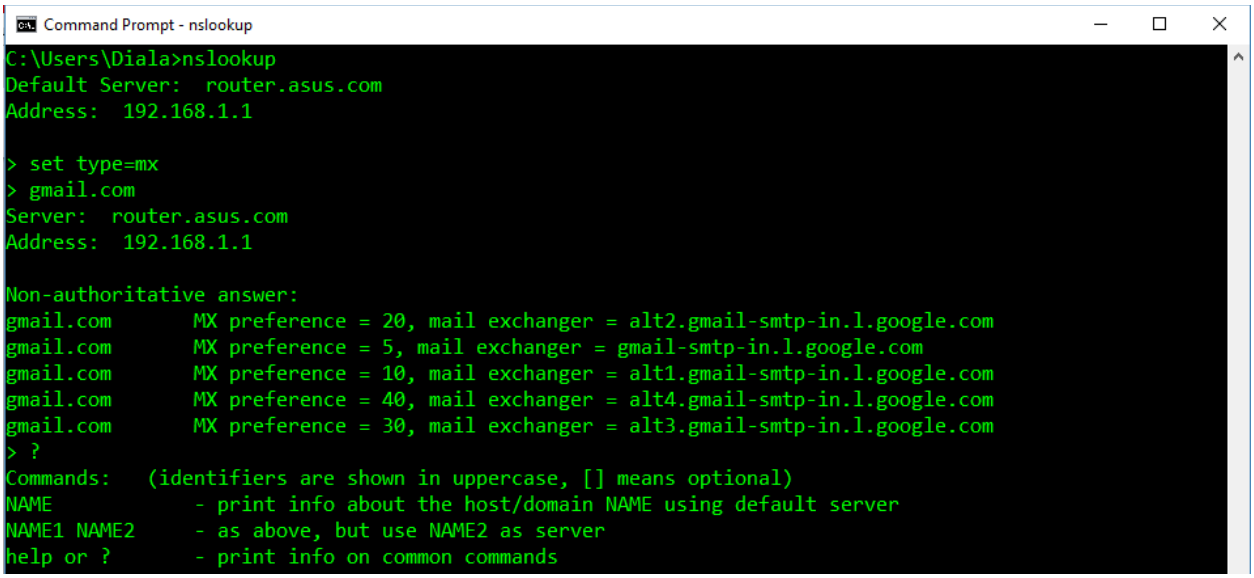
Perform a quick online research on whois database.

a) What is a whois database?

b) Use a whois database on the Internet (you can use for example: https://whois.net/) to obtain the names of DNS servers for two specific domain names of your choice (for example for domain name: yahoo.com). Indicate which whois database you used.

c) Use nslookup on your local host to send DNS queries. Try querying for Type A, NS, and MX reports. Present your findings.

**Note:** For that, launch the nslookup tool on your terminal. To change the type of query, use the set type command. For more details, you can hit "?" inside nslookup. An example is provided in the figure below.




d) Use nslookup to find a Web server that has multiple IP addresses. Does the Web server of mcgill have multiple IP addresses?

e) Use the ARIN whois database to determine the IP address range used by google.

f) Search online for reconnaissance. Describe how an attacker can use whois databases and the nslookup tool to perform reconnaissance on an institution.

g) Discuss reasons why whois databases should be publicly available.