Lab 1: Preparation and Warm-up[1]

(Total: 5 points)

OBJECTIVE:

The objective of this lab is to explore the course website at D2L, install the basic software and have some warm-up exercises to get ready for the future course work.

LAB ACTIVITIES:

1. Explore the course website at D2L and get familiar with various sections and tools provided by D2L. For example, you should know where to find lecture slides and videos, lab manuals, and dropboxes for lab submissions, where to check your grades, and so on. Download a copy of the course syllabus and read it carefully.
2. We will have in-person labs. However, in case you could not attend the in-person labs for medical or other legitimate reasons, it would be good to install some important software on your home computer. Note that this is only optional.
    1) To install **Java**, some help information is listed at https://www.cs.unb.ca/help/students/java-install.shtml. You can download and install your favorite Java IDE such as Eclipse and IntelliJ IDEA.
    2) **Wireshark** is a free software and can be downloaded at https://www.wireshark.org/download.html.
    3) The instructions for **UNB VPN** setup can be found at https://www.cs.unb.ca/help/vpn/. In order to use SSH or remote desktop to access the lab computers on campus, you need to first connect to the UNB's VPN.
    4) For MacOS, Linux or the latest Windows 10/11, **SSH** is likely already installed. If not, you can follow the instructions at https://www.cs.unb.ca/help/ssh-help.shtml to install SSH on your computer. In addition to the built-in SSH tool, you can also use other SSH clients like Putty.
    5) The licensed software (including Microsoft Office) for the UNB community can be accessed at https://unbcloud.sharepoint.com/sites/ITServices/SitePages/Software.aspx. Note that authentication is needed to access this website. **Microsoft Word** will be needed to edit answers for the assignments and exams. You can also use some alternatives such as Apache OpenOffice Writer or LibreOffice Writer.
    6) For **Microsoft Teams**, a desktop copy is available for download at https://www.microsoft.com/en-ca/microsoft-365/microsoft-teams/download-app. Or you can use the Web version at https://teams.microsoft.com/.
    7) Download and install **Acrobat Reader** so that you can read the lecture slides and convert your assignments and exams to PDF files before submission. You can download a free version of Acrobat Reader at https://get.adobe.com/reader/.
    8) Download and install other required software such as your favorite Web browser, and make sure they support D2L and video conferencing on Teams well.

[1] The lab materials are adapted from the textbooks "Computer Networking – A Top-Down Approach" by James Kurose and Keith Ross and the materials provided with them. They can only be used by students who registered for this course. Reproduction outside of this course use is prohibited.

Once you set up your home computer, test the software. For example, edit a report using some word processing software (e.g., Microsoft Word, OpenOffice, Google Doc, etc.), and convert the file into PDF.

3. In this course, we will use Wireshark to study important network protocols used on the Internet. Next, please work through each of the tasks discussed below and get familiar with Wireshark. To get started please read the attached basic introduction on Wireshark.

4. Get your first capture with Wireshark:

   a. After you login to Linux in the lab, make sure you start Windows VM from Applications -> FCS VMs -> Windows 11 Lab VM. Then, start Wireshark from bottom menu. Select the Capture pull down menu and select Options. Select the network interface (i.e., the physical connection) that your computer has. Click "Start".

   b. Before performing the steps below, make sure your browser's cache is empty. Start up your favourite Web browser and display the webpage[2] http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html. In order to display this page, your browser will contact the HTTP server and exchange HTTP messages with the server in order to download this page. The Ethernet or Ethernet II frames containing these HTTP messages will be captured by Wireshark.

   c. After your browser has displayed the webpage, stop Wireshark packet capture by selecting stop in the Wireshark capture window. This will cause the Wireshark capture window to disappear and the main Wireshark window to display all packets captured since you began packet capture. Please go to "File" and select save file (e.g., call it a ***trace***).

5. Examine the trace which contains live packet data exchanged between your machine and the Web server (the host providing the webpage to your machine).

   a. Even though the only action you took was to download a webpage, there were evidently many other protocols running on your computer that are unseen by the user. We'll learn much more about these protocols as we progress through the text! In the trace you can see many protocols listed. Choose three of these protocols from your list and use Google or go to the IETF site to find out what they are being used to support.

   b. The protocol used to exchange messages between a Web browser and Web server is HTTP. Type in "http" (without the quotes, and in lowercase - all protocol names are in lower case in Wireshark) into the display filter specification window at the top of the main Wireshark window. Then apply the filter (to the right of where you entered "http"). This will cause only HTTP message to be displayed in the packet-listing window. By clicking on '+' and '-' and right-pointing and down-pointing arrowheads to the left side of the packet details window, maximize the amount information displayed about the HTTP messages. Now, export the two HTTP messages (GET and 200 OK), specifically related to the requested webpage in item 4. To do so, select *Export Packet Dissections … As Plain Text* from the Wireshark *File* command menu and select the "*Selected Packet Only*" and "*Print as displayed*" radial buttons, and then click *OK*. Copy and paste the messages in the exported files in your report.

6. Based on the above trace, answer the following questions. Note that some questions will touch on the fundamental networking concepts that we have not yet fully covered in class. For this senior course we expect you will consult the textbook, the Internet and other courses to guide you. Please note, as

[2] Check the URL carefully and make sure it does NOT begin with "https". Also, you cannot use VPN while capturing the trace.

always, citations must be provided with your answers if you consult any external source for information.

a. Select the first HTTP message shown in the packet-listing window. This should be the HTTP GET message that was sent from your computer to the HTTP server to the above requested webpage in item 4. When you select the HTTP GET message, the Ethernet or Ethernet II frame, IPv4 datagram, TCP segment, and HTTP message header information will be displayed in the packet-header window. How long did it take from when the HTTP GET message was sent until the first HTTP response (200 OK reply) was received? (By default, the value of the Time column in the packet listing window is the amount of time, in seconds, since Wireshark tracing began.)

b. In the trace you will find IPv4 addresses within the packets. Find an example packet in the trace where the IPv4 address associated with your machine is present. Compare this address with the IPv4 address you can find by using the following command: *ipconfig /all* on Windows, or *ifconfig* on MacOS or Linux. If you use Windows VM for the above capture, make sure you run the command on the terminal within the VM. Running this command also gives a 48-bit physical address for the network interference. This is the MAC (medium access control) address (not discussed in class yet) of your machine. Can you find the MAC address of the packet in the trace? Is it the same as the physical address returned by the above command?

   If you use your personal computer, you can mask selected digits of your MAC address and IPv4 address in your answers to protect your private information.

LAB SUBMISSION:

Go through the above lab activities and write a report **answering the questions listed in items 5-6**.

- **Please follow the lab report template in Microsoft Word posted on D2L.** The template includes one example answer for a question listed in item 6. Once you are done, convert your Word document into **a single PDF file** and submit it to the corresponding dropbox on D2L by the due time.
- In your report, you need to explain where you find the answer to each question. You can print out a packet using Wireshark if requested or use screen capture software to take a screenshot of the displayed packet in Wireshark, and then annotate the output packet with color markups to show the information related to your answers.