FACULTY OF ENGINEERING,
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

ECE4436A–NETWORKING: PRINCIPLES, PROTOCOLS, AND ARCHITECTURES

Laboratory 2: Packet Sniffer using Wireshark

Objectives:
In this lab experiment, a packet sniffer software, namely Wireshark, is used to demonstrate the behaviour of several network protocols. You will see the protocols' message exchanges in real time.

Equipment: Windows workstation and Internet access.

Schedule:
You may complete it at home or at any lab at Western Engineering (i.e., there are **NO** lab checkpoints for this lab). TAs will be available to answer any question that you may have. The lab schedule is as follows:

- Monday from 9:30am to 11:30am at SEB-1012
- Monday from 12:30pm to 2:30am at TEB-244
- Wednesday from 10:30am to 12:30pm at SEB-1012
- Thursday from 1:30pm to 3:30pm at SEB-1012

Lab reports are **due Sunday October 25, 2015 at 11:55 pm**. Please submit **ONLY** a soft copy in the **ONLY PDF format** through the Lab2 link under the Assignments tab on the course website at OWL. Name your PDF file as "yourUWOid_lab2" (e.g., if your UWOID is aouda4 then the document name will be "aouda4_lab2".

Background:
The basic tool for observing the messages exchanged between executing protocol entities is called a packet sniffer. As the name suggests, a packet sniffer captures ("sniffs") messages being sent/received from/by your computer; it will also typically store and/or display the contents of the various protocol fields in these captured messages. A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself. Similarly, received packets are never explicitly addressed to the packet sniffer. Instead, a packet sniffer receives a copy of packets that are sent/received from/by applications and protocols executing on your machine.

Procedure:
Please refer to pages 9-22 of the Lab2_Attachment document. An introduction to Wireshark is given in pages 1-8 of the attachment. For those who are not familiar with Wireshark, please read the introduction before the lab session.

Lab Report:
Prepare a lab report and answer the following questions. Add snapshots of the Wireshark window, if necessary.

Part A - HTTP
Questions: Answer all 19 questions.

Part B - DNS
Questions: Answer all 23 questions.

Please have an introduction and conclusion for each part of the Lab.