TSN2201 COMPUTER NETWORKS

Tri 1, 2017/2018

Group Assignment (20%, max. 2 students)

Main task: To study network protocols by capturing network traffics using **Wireshark**. The tutor will assign you 2 protocols (1 Protocol must be from the application layer, 1 from either transport layer, network layer or data link layer).

Setting up prior using Wireshark to capture data

Depending on the assigned protocol, you probably need (or need not) to install the network application related to the main protocol in computers.

Ex 1: File Transfer Protocol (FTP). You need to install FTP server in a machine, FTP client in another machine. Then, you capture the traffics between these two machines.

Ex 2: HTTP. No need to install any extra network application. Because what you need is a web browser which is already in your machine. Web servers are also everywhere in the Internet.

Analyze the packets you captured and answer the following questions:

Part A (4 marks, each 1 mark). Shared by all members.

i) Port number(s) used by the network application protocol

ii) IP address that the network application used (your laptop's IP address)

iii) IP address of the remote machine your network application was communicating to

iv) Port number of the remote machine the network application was communicating to

Part B (16 marks). Each member in a group will get different mark based on his/her efforts.
Each member should select a protocol and answer the following questions.

i) State the functions of the protocol. (2 marks)

ii) Show the packets captured by Wireshark, explain the entire process of the protocol occurred between the sender and receiver. (4 marks)

iii) Based on the Wireshark capture, give the header format for the protocol. Explain the function of the fields inside the header. (4 marks)

- You can also use the help of books or Internet, but you need to show where you find the header format by providing references. Do not copy figures from the references. Draw the header yourself.

v) Referring to your Wireshark capture, what is the content of the application data (1)? What are the values for the fields in the headers (2) – (4)? Explain the meaning of the values (as many as possible, try your best). Do not make up values. (6 marks)
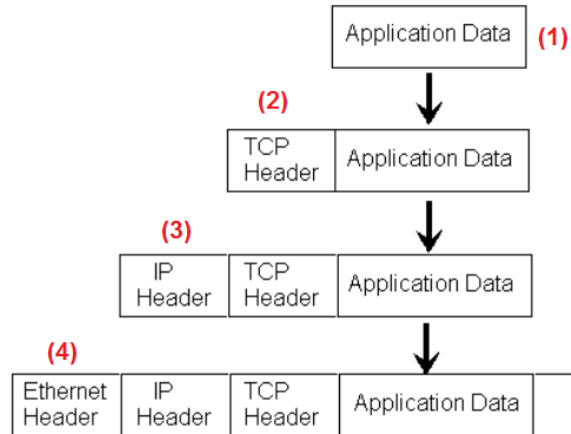
Presentation & Submission
i) The deadline for the assignment submission is on 24 Sept 2017. You have to submit the assignment to the MMLS.
ii) Your submission for the assignment shall include the softcopy of the report and the Wireshark capture.
ii) Presentation on Week 13 & 14. Proof your answer with Wireshark in your laptop. Zero mark for absentee.

In your report
i) Attach screenshots of Wireshark captures as proof for each answer. ***only Wireshark.
ii) Provide explanation for each answer.
***Zero mark for plagiarism.