BLG433E
COMPUTER COMMUNICATIONS

OBJECTIVES

The purpose of this homework is to give you experience on network analyzing with the Wireshark tool. You will investigate different protocol types, offered services and performance metrics such as *Throughput*, *Round Trip Time (RTT)* and *Window Size*.

QUESTIONS

You are expected to prepare a report for the following questions by providing Wireshark screenshots for each of them separately:

1. **(15 Points) DHCP:**
   Use Wireshark to investigate DHCP protocol on your computer while getting an IP address from a DHCP server. Provide a sequence diagram and explain each of the messages included to show the communication between your computer and the DHCP server.

2. **(15 Points) DNS protocol:**
   Provide visual materials and explain DNS stages in Wireshark by typing the address of a previously unknown website in your browser. Indicate the IP address of the DNS server and the IP address of the website through screenshots.

3. **(35 Points) Transport Layer protocols:**
   a. **(15 Points)** Try to capture a session on your browser that uses TCP protocol. Using "Statistics" panel in Wireshark, provide drawings for *Throughput*, *RTT*, and *Window Size* parameters over the session. Interpret the change in *Window Size* parameter by referring TCP congestion control mechanism.
   b. **(15 Points)** Try to capture a session on your browser that uses UDP protocol and provide statistics for your UDP session. What does it mean to provide *best effort* service in UDP?
   c. **(5 Points)** Is there any other Transport Layer protocol that you observe during your sessions? Please, indicate and explain them.

4. **(15 Points) File transfer:**
   You are not able to observe any *ftp* packets over Wireshark while downloading a file from *Ninova* on your browser. What may be the reason for this situation? Try the download another file from the link given, "ftp://speedtest.tele2.net/", and take a screenshot of an ftp packet. Interpret the steps you covered during the file transfer process in both cases.

5. **(20 Points) Protocol analysis interpretation:**
    a. **(10 Points)** How many different protocols did you capture in Wireshark? Please, give them in a list. What are the specific protocol numbers of transport layer protocols (TCP, UDP, and ICMP) captured in Wireshark?
    b. **(10 Points)** Did you capture any packet retransmission during your analysis with Wireshark? If so, what is the transport layer protocol? Compare TCP and UDP protocols considering the retransmission mechanisms offered by them.