Assignment 5

Part I:

1) What is the main difference between the transport layer protocols: TCP and UDP? [5 pts]

2) What is the main objective of the following application protocols: [5 pts]
    a. DHCP
    b. DNS

PART II - Wireshark Mini-Lab: Follow the following steps to answer the questions [35pts].

- Close all Internet applications (all browsers)
- Open Wireshark, select the interface used for Internet connection by double-clicking on it (e.g., double-click on "Wi-Fi: en0" if you use Wi-Fi), and start capturing packet (which starts automatically at first)
- Start a browser, and go to www.pitt.edu
- Stop capturing packet in Wireshark (by clicking on the stop button [red square button])

- In Wireshark, locate and examine the DNS query & response by searching the "Protocol" column for "DNS", or type dns in filter bar. Then, in the "info" column look for:
    - "standard query" for "A www.pitt.edu".
        - Right click on the query and select follow->UDP stream. You should be able to see the "standard query response".

1. Click on the DNS query response and look into the details of the message (middle portion in Wireshark). Click on the arrows to expand different fields. Are they sent over UDP or TCP? [3 pts]
   Hint: You can find this information next to source port (Src Port) and destination port numbers (Dst Port). This information is also in the IP header (next header field)

2. What is the destination port number for the DNS query message? What is the source port number of DNS response message? [5 pts]

3. Determine the IP address of your local DNS server. Is it the same address used in the destination address field of the DNS query, IP header? [3 pts]
    - ▪ Check your local DNS server –
        - MAC users:
            - o system preferences->network -> advanced -> DNS tab
        - Windows user:
            - o settings-> network connections -> Local Area Connection -> properties-> select TCP/IP-> Properties
            - o OR command prompt type ipconfig/all

4. Is DNS Query Multicast or Unicast packet? If unicast, how did your device get the IP address of local DNS server? [5 pts]

5. Is DNS Response Multicast or Unicast packet? [3 pts]

6. Examine the DNS response message. What is the IP address of the URL you typed in your browser (www.pitt.edu)? [3 pts]
   Hint: expand "Domain Name System (response), then expand "Answers", the IP address should be in the "Address field".

7. Find a Wireshark HTTP message to or from the address of wwww.pitt.edu you find from the DNS response

   Hints for the questions below:
    - *use can use filter by typing ip.addr == (type ip address)*
    - *Right click on the message and select follow -> TCP stream*
    - *Arrange the messages by time (by clicking on the time column in the main Wireshark window). Check the first three messages.*

   a. Provide a screenshot. What is the purpose of the first 3 TCP messages between your device and www.pitt.edu? [3 pts]
   b. What are the sequence and acknowledgement numbers of the three TCP packets performing the three-way handshake? [6 pts]
      i. Note that you may get relative numbers (sequence number 0, 1). For exact numbers, you need to go to Edit → Preferences → Protocols → TCP, and uncheck "Relative sequence numbers and window scaling."
   c. Right-click an HTTP packet captured in Wireshark and select "Follow HTTP stream". [4pt]
   d. What is the request line? What is the corresponding Response Status?
      (Choose any of the HTTP request and response)