Lab Assignment - 5

TCP

Wireshark trace file **tcp-ethereal-trace-1** is provided here. This trace file is captured during uploading a 150 KB text file to a Web server through the HTTP POST method. Here transmission is happening between your computer and server. Run Wireshark and open the above trace file and answer the following.

1. Filter the TCP packets displayed in the Wireshark window.
2. Find out which packet contains the actual POST request.
3. What are the first and last packets for the POST request?
4. What is the IP address and the TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?
5. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?
6. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?
7. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the ACKnowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?
8. What is the sequence number of the TCP segment containing the HTTP POST command?
9. Analyze the amount of data sent per unit time from the client to the server through wireshark time-Sequence Graph.

UDP

1. Select one UDP packet named **udp-wireshark-trace**. From this packet, determine how many fields are there in the UDP header. Name these fields.
2. By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.
3. The value in the Length field is the length of what? What is the length of UDP payload for your selected packet?
4. What is the maximum number of bytes that can be included in a UDP payload?

5. What is the largest possible source port number?
6. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation.
7. Examine a pair of UDP packets in which the first packet is sent by your host and the second packet is a reply to the first packet. Describe the relationship between the port numbers in the two packets.