Chapter 6

Lab 5: Analyze TCP connection and segmentation when downloading large file from a web-server using Wireshark

6.1 Objective

We download a large object from a web server and analyze the following: TCP connection establishment, message segmentation, usage of sequence numbers and acknowledgement numbers and TCP connection closing. We want to see how the TCP segments are reassembled at the client to display the whole webpage.

6.2 Procedure

1 Start up your web browser, and make sure your browser's cache is cleared.

2 Start up the Wireshark packet sniffer

3 Enter the following URL into your browser http://gaia.cs.umass.edu/wiresharklabs/alice.txt.

4 Your browser should display the rather lengthy Alice's Adventures In Wonderland

5 Stop Wireshark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed.

6 Note the source port number (e.g., xxxx) used by the host to send the HTTP GET message. Then enter "tcp.port == xxxx" in the display-filter-specification window, so that the entire TCP session is displayed.

6.3 Analyses

Answer the following questions:

1. Fill the following table:

Frame Type	Frame No	Source Port No	Destination Port No
SYN			
SYNACK			
ACK			
HTTP Request			
First segment of object			
Last segment of			

object			
FIN			
ACK for FIN			

2. What are the sizes of the TCP header in the SYN and SYNACK segments? How does it compare to the TCP header size of the data-carrying TCP segments?
3. Identify the TCP segment which carried the HTTP GET message. Write the corresponding relative sequence number and the actual sequence number. [Note: Actual segments can be viewed by right clicking on sequence number, selecting protocol preferences and un-ticking the relative sequence numbers]
4. What are the actual sequence number and acknowledgement numbers of the segments used in the connection establishment?
5. What are the actual sequence number and acknowledgement numbers of the segments used in the connection closing?
6. How much time did it take to fully download the requested object? What is the throughput of the TCP session?
7. Plot the Round Trip Time Graph. Note: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the "listing of captured packets" window that is being sent from the client to the gaia.cs.umass.edu server. Then select: Statistics→TCP Stream Graph→Round Trip Time Graph.

Provide screenshot of the RTT graph. Provide screenshot of the packet listing window showing SYN, SYNACK and ACK segments. Provide screenshot of the packet listing window showing the segments meant for closing the TCP connection.