EECS 563
Network Protocol Analysis: TCP
Project 4

Provide your results in the form of a technical report using the provided format.
See: **Technical Report Format**
Also see this paper for advice on writing technical reports.
See: **Paper on writing technical reports**
Do not pad your reports, all figures and tables must be discussed in the text.

The purpose of this assignment is to use Wireshark to examine http and TCP packets involved in connection establishment, data transfer, and connection termination. In this class you must run Wireshark with the promiscuous mode turned off. The goal is to have you collect your own data, first attempt to collect your own Wireshark files. However, there can be issues with caching with the result that Wireshark may not capture the desired data. If you can not collect your own Wireshark files then use Wireshark file for small file transfer and Wireshark file for large file transfer. Note for the large file case the trace file will be large and you will need to wait for operations to complete.

Process-Small File:

a) Start Wireshark
b) Click start
c) Click on Hello World (if you need to repeat accessing the file be sure to clear your web cache and cookies and other site data)
d) Click on back
e) Stop Wireshark (be sure to wait long enough for the session to close)
f) Save the trace file.

1. Set filter to http & wait 30 sec for filter to be applied.
2. Right click on packet that has a Get in the Info field, it should look something like: GET …. Hello-world.txt HTTP/1.1
3. Go to Follow TCP Stream
4. Confirm that the source of the SYN packet is your computer and the destination of the SYN packet is the remote server.
5. Identify the sequence of session establishment or set-up packets.
    a. Does the connection establishment packet sequence match your expectations?
    b. What is the destination port number in the first packet? Why is this port number used in this case?
    c. What is the source port number in the first packet? Why is this port number used in this case?
    d. What flags are set?
    e. Explain the values of the relative sequence and ack numbers in the session establishment packets.

6. Identify the sequence of TCP session tear down packets.
    a. Discuss the sequence and Ack numbers used in the sequence of TCP session tear down packets
    b. Does the session tear down packet sequence match your expectations? If not verify that the sequence is valid.
7. Show the http packet that contains the requested data, i.e., Hello World. What is the File Data length in bytes and how does that relate to the message?
8. Statistics click on Flow Graph, Check "Limit to display filter" Discuss the flow Graph.
9. Does the TCP congestion control mechanism come into play in this session? Explain.
10. What is the TTL in the first packet that set up the TCP connection? Describe what happens to the TTL as the packet transverses the Internet. What layer of the protocol stack did you examine to obtain this number.
11. What is the source Ethernet address of the first packet that set up the TCP connection? Is this the expected address? What layer of the protocol stack did you examine to obtain this number?
12. Were there any other http GET messages in your TCP stream, if so report the site and explain what that extra GET is doing.
13. How does Wireshark demonstrate protocol layering and encapsulation? How does the Flow Graph assist in understanding the TCP connection establishment, data transfer, and connection termination processes?

Process-Large File:

a) Start Wireshark
b) Click start
c) Click on Video. Download the file, you do not need to collect while playing the video. (if you need to repeat accessing the file be sure to clear your web cache and cookies and other site data)
d) After the file has been downloaded click on back.
e) Stop Wireshark (be sure to wait long enough for the session to close)
f) Save the trace file. Note this will be a large trace file and you will need to wait for operations to complete.

1. Set filter to http
2. Right click on packet that has a Get in the Info field
3. Go to Follow TCP Stream
4. Does the connection establishment packet sequence match your expectations?
5. After the session establishment is completed how many connective packets are transmitted from the server to your host before the first ack is sent from your host to the server. How many bytes were in flight from the server to your host?
6. What is the length of these packets? Why do they all have this same length?
7. Open the last transmitted packet from the server to your host before the first ack is sent from your host to the server. Open the tcp part of the packet and under SEQ/ACK analysis note the Bytes in flight and compare to the result from part 5.

8. After the first ack is sent from your host to the server how many connective packets are transmitted from the server to your host before the second ack is sent from your host to the server.
9. Why are the number of packets from the server to your host between acks different?
10. Does the TCP congestion control mechanism come into play in this session? Examine the number of consecutive ACK packets and how they change with time. Explain.
11. Explain the relative sequence and ack numbers in the last packet before the first ack is sent from your host to the server and all the packets sent from your host back to the server before the next TCP packet containing video data is transmitted from the server to your host.
12. Click on Statistics→TCP Stream Graphs→Time Sequence (Stevens) zoom in on the first about 0.1-0.5 sec. "Here, each dot represents a TCP segment sent, plotting the sequence number of the segment versus the time at which it was sent. Note that a set of dots stacked above each other represents a series of packets (sometimes called a "fleet" of packets) that were sent back-to-back by the sender" Report your result and explain why the sequence number (b) sometimes decreases.
13. In the lower right of the controls, change the plot from Time Sequence (Stevens) to Round Trip Time, report the result.
14. In the lower right of the controls, change the plot to Throughput report the result. Discuss why there is an increase of throughput with time. Also comment on the average throughput compared to the result in part 7 above.
15. In the lower right of the controls, change the plot to Window Scaling report the result and comment on why the window size changes with time.
16. Find the first TCP Window Full packet. Why is this packet generated?

References:

[1] Wireshark Lab: TCP v8.1 Supplement to Computer Networking: A Top-Down Approach, 8th ed., J.F. Kurose and K.W. Ross.