CP372 – Computer Networks – Winter 2023
Wireshark Assignment 1: TCP

Due Feb 10th 2023, 11:59 pm

***Late penalty: 10% deduction per day**

Objective

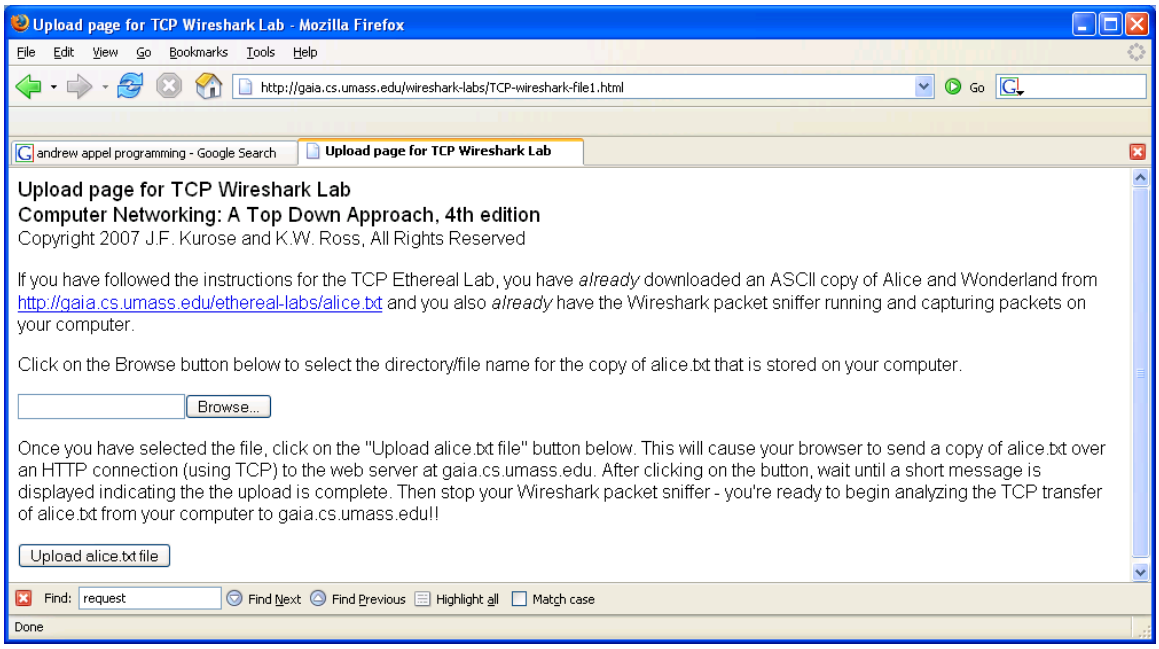
In this lab, you will capture a bulk TCP segment transfer from your computer to a remote server to explore the TCP protocol.

Whenever possible, when answering a question, you should hand in a printout or a screenshot of the packet(s) within the trace that you used to answer the question asked. Annotate the printout or screenshot to explain your answer. To print a packet, use *File->Print*, choose *Selected packet only*, choose *Packet summary line*, and select the minimum amount of packet detail that you need to answer the question (or take a screenshot showing this minimum amount of packet detail).

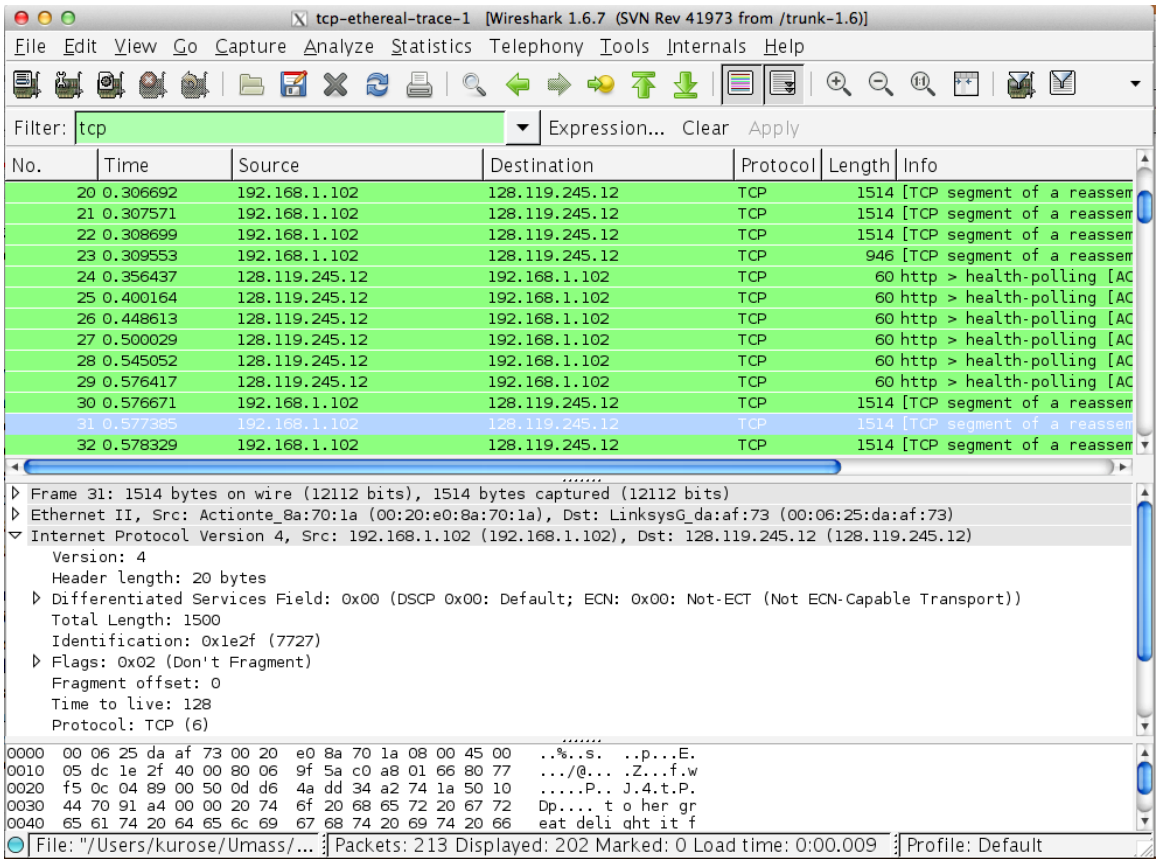
Capturing a bulk of TCP Segment Transfer

Do the following:

- Start up your web browser. Go the http://gaia.cs.umass.edu/wireshark-labs/alice.txt and retrieve an ASCII copy of Alice in Wonderland. Store this file somewhere on your computer.
- Next go to http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html
- You should see a screen that looks like:



- Use the Browse button in this form to enter the name of the file (full path name) on your computer containing Alice in Wonderland (or do so manually). Don't yet press the "Upload alice.txt file" button.
- Now start up Wireshark and begin packet capture (Capture->Start) and then press OK on the Wireshark Packet Capture Options screen (we'll not need to select any options here).
- Returning to your browser, press the "Upload alice.txt file" button to upload the file to the gaia.cs.umass.edu server. Once the file has been uploaded, a short congratulations message will be displayed in your browser window.
- Stop Wireshark packet capture. Your Wireshark window should look similar to the window shown below.



If you face any problems with the aforementioned method, please do the following:
Download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract. The traces in this zip file were collected by Wireshark running on the author's computers. Please load the trace tcp-ethereal-trace-1 into Wireshark and view the trace using the File pull down menu, choosing Open, and then selecting the tcp-ethereal-trace-1 trace file.

What you should see is a series of TCP and HTTP messages between your computer and gaia.cs.umass.edu. You should see the initial three-way handshake containing a SYN message. You should see an HTTP POST message being sent from your computer to gaia.cs.umass.edu. You should also see TCP ACK segments being returned from gaia.cs.umass.edu to your computer.

Recall that you can filter the packets displayed in the Wireshark window based on protocol, so you can enter "tcp" for example (or "http") to view these packets.

Please answer the following questions based on the displayed trace:

Important Notes:

- Answers might differ from one student to another. Screenshots should reflect the answers provided by students.
- For each question, half the point is deducted if no screenshot is provided.

1. What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu? (Please include a screenshot and highlight your answer on that screenshot). (2 points total, 1 point for each address))

2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection? (Please include a screenshot and highlight your answer on that screenshot) (2 points total, 1 point on IP address and 1 point on port number)

3. 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 (Please include a screenshot and highlight your answer on that screenshot)? What is it in the segment that identifies the segment as a SYN segment? (2 points total, 1 point on Sequence number of the TCP SYN segment and 1 point on what identifies the segment as a SYN segment)

4. 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? (Please include a screenshot and highlight your answer on that screenshot) What is it in the segment that identifies the segment as a SYNACK segment? (3 points total, 1 point on each question)

5. What is the sequence number of the TCP segment containing the HTTP POST command? (Please include a screenshot and highlight your answer on that screenshot). (0.5 point)

6. What is the minimum amount of available buffer space advertised at the receiver for the entire trace? (Please include a screenshot and highlight your answer on that screenshot). (1 point)

7. How much data does the receiver typically acknowledge in an ACK? To answer this question, please record the acknowledgment number and the acknowledged data of the first 12 acknowledgments generated by the receiver in the table below and state the data size that appears the most? (Please include a screenshot and highlight your answer on that screenshot) (3.5 points) [0.25 point for each row in the table and 0.5 point for the final answer]

	acknowledged sequence number	acknowledged data
ACK 1		
ACK 2		
ACK 3		
ACK 4		
ACK 5		
ACK 6		
ACK 7		
ACK 8		
ACK 9		
ACK 10		
ACK 11		
ACK 12		