Name and Section: _____

1 Lab Preparation

- Download the following trace files to your working directory:
  - transport.pcapng
- At this point you should know how to setup filters in wireshark and tshark. With your knowledge of these tools, filters, and network protocols you are expected to derive the filter syntax and use problem solving to complete the analysis of the capture.

Submission

Submit all of your work in **neatly hand-written** format.

What to turn in:
- The completed lab packet

2 Lab Assignment

- Open the packet capture 'transport.pcapng' in Wireshark
- Create a profile with the following columns displayed:

  frame.number, time, ip.src, ip.dst, ip.proto, Protocol, and info

- Turn off all name resolution

1. List the frame numbers of at least three different 3-way handshakes.

2. List two frame numbers where the FIN flag was set to 1. What was the TCP well known port number associated with these? What application protocol is associated with these port numbers?

3. What is the well known port number and the associated application protocol seen in frame 7?

4. Select frame 4, right click and select 'Follow TCP Stream'. What does this do? Close the pop-up window. Copy the filter syntax that was created, use this to create a tshark command that will output the sequence and acknowledgement numbers from each packet in the stream. Save the output to a file named 'seq_ack_numbers.txt'

5. Using both the output you saved to the text file and the `tcp stream` you have filtered in wireshark, draw a diagram depicting the flow of traffic *You may stop once you have reached frame 40.* In great detail, explain the values of the sequence and acknowledgment numbers. You must include within the diagram how the size/length of the messages are related to the sequence and acknowledgement numbers.

Review Questions

1. What is the size of a TCP header? How do you know how big the header is for a given TCP segment?

2. Explain the use of 'well-known' port numbers and their usage within the client-server model. How are port numbers related to UDP, TCP and encapsulation?

3. In detail, explain why TCP is considered a 'reliable' transport layer protocol.

4. Are packets any less likely to be lost when using TCP compared to UDP?

5. Draw out the TCP/IP stack. List all protocols we have learned thus far at the appropriate layers. Annotate support protocols as needed. For each layer list the addressing type used at that layer. Lastly, list the network device type for each layer.