CS2910 Exercise: TCP Handshake

Names: ____

TCP Handshake and Closing of TCP Connection

1. Throughout this exercise, make notes and record any questions you have in the (you guessed it) **Notes and Questions** section of this exercise report.

2. Fire up Wireshark. Since you may have quite a bit of network traffic that we are not interested in, create a capture filter for a particular host with which you would not normally communicate. I suggest a low-feature website such as craigslist.org (city of your choice). Avoid google.com or gmail.com as they may keep a connection open thus you will not capture the three-way handshake. Also avoid any website that bumps you to https and you will see a lot of additional traffic. If a server shows up at a variety of IP addresses due to load balancing, you may be able to see the traffic by filtering on the subnet: e.g. `ip.host contains "208.82.236."`

3. With the capture running, direct your browser to that source (or refresh it if you have it up already). The capture should collect a handful of packets.

4. Locate the three-way handshake. You will be able to spot this in Wireshark as three TCP packets with [SYN], [SYN, ACK], and [ACK] noted in the Info column. Note the Sequence and Acknowledgement numbers shown in the Info column. Be careful. You may see multiple SYN packets and possibly multiple SYN, ACK packets.

5. Expand the initiating SYN packet. Click on the “Sequence number: 0” line under the expanded TCP packet. This will highlight the corresponding field in the raw TCP packet. Write the numbers highlighted below and comment on the numbers in **Notes and Questions**:

Partner #1: _______________ Partner #2: ________________ Partner #3: _______________

6. Expand the corresponding SYNC, ACK packet. Click on the “Acknowledgement number: 1” line under the expanded TCP packet. This will highlight the corresponding field in the raw TCP packet. Write the numbers highlighted below and comment on the numbers in **Notes and Questions**:

Partner #1: _______________ Partner #2: ________________ Partner #3: _______________

7. Conduct a similar investigation of the sequence number in the SYN, ACK packet as well as the acknowledgement number in the ACK packet. **Comment in Notes and Questions**.

8. When a TCP connection closes, a slightly different transaction occurs. Locate the closure of the TCP connection in Wireshark. Sketch the transaction and comment on the sequence of packets. Note that the initial FIN flag may be in an http packet. Refer to Figure 3.40 in the book if needed. What can you infer from the sequence and acknowledgment numbers present in these packets?

Notes and questions and answers (to questions above)

Please record notes on your exercise activity here, along with any questions you have.

(Acknowledgement: Original exercise by Dr. Sebern/Dr. Rothe)