Name and Section: McKenzie Eshleman

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.

   Fram numbers 4-6, 13-15, and 18-20 has a three way handshake

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?
   Frames 222, 224, and 6047 has a FIN flag set to 1, the TCP well know port number that is associted with these are 20 and 52,913. The application protocols that are associated with these port numbers is protocol 6, which is the Transmission Control Protocol

   Filter: tcp.flags.fin == 1

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

   The well known port number that is seen in frame 7 is 80 which is a well-known port which identifies HTTP traffic for a web server. The associated application protocol is protocol 6, which is the transmission control protocol.

4. Select frame 4, right click and select 'Follow TCP Stream'. What does this do?

   When you follow the TCP stream of frame 4 it displays the html code for the website that is being streamed and all the data of when the site was accessed, the website is for missing people.

5. Using 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?

   The size of a TCP header can range from 20-60 bytes, the 40 bytes are for different options if there are no options then the header is 20 bytes. We can determine the size of the header by subtracting the combination length of the segement header and the IP header from the total IP datagram length that is specified in the IP header.

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?

   The use of well know ports allows client applications to easily locate the corresponding server application processes on other host.
   Ports are related to UDP, TCP, and encapsulation by specifying the source and destination port numbers in their packet headers and that information, along with the source and destination IP addresses and the transport protocol (UDP/TCP) enables applications running on hosts on a TCP/IP network to communicate.

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

   The reason why TCP is considered 'reliable; is that the protocol itself checks to see if everything that was transmitted was delivered at the recieving end.

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

   TCP s comparatively slower than UDP, UDP is much faster, simpler, and efficient protocol, retransmission of lost data packets is only possible with TCP.

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.