TCP Wireshark Analysis Instructions

1. Find the IP Address and TCP Port of the Client (Source)

- Open Wireshark and load the packet capture (.pcap file).

- Apply a filter for HTTP traffic: http

- Select an HTTP packet (e.g., GET or POST request).

- Expand the "Transmission Control Protocol (TCP)" section in the "Packet Details" pane.

- Note the Source IP and Source Port.

2. Find the IP Address and Port of gaia.cs.umass.edu

- In the selected HTTP packet, note the Destination IP and Destination Port (should be 80 for HTTP).

3. Find the Source IP and Port for File Transfer

- Repeat step 1 focusing on the file transfer request (usually a POST or GET).

4. Find the TCP SYN Sequence Number

- Apply filter: tcp.flags.syn==1 && tcp.flags.ack==0

- Select the first SYN packet from client to server.

- Expand "Transmission Control Protocol" section.

- Note the Sequence Number and Flags (should show [SYN]).

5. Find the SYN-ACK Sequence and Acknowledgment Number

- Apply filter: tcp.flags.syn==1 && tcp.flags.ack==1

- Select the SYN-ACK packet from gaia.cs.umass.edu.

- Expand "Transmission Control Protocol" section.

- Note the Sequence Number, Acknowledgment Number (Clients sequence number + 1), and Flags (should show [SYN, ACK]).

6. Find the Sequence Number of HTTP POST

- Use filter: http.request.method=="POST"

- Select the POST request packet.

- Expand "Transmission Control Protocol" section.

- Note the Sequence Number.

7. Find the Length of the First Six TCP Segments

- Start from the first TCP segment containing the HTTP POST.

- Look at the "Length" field in the TCP header.

- Repeat for the next five segments.

8. Plot the Estimated RTT

- Apply filter: tcp.stream eq 0 (change stream number if needed).

- Go to Statistics TCP Stream Graph Round Trip Time Graph.

- Observe RTT values after each ACK.