CSCD 330 – Computer Networks

Lab 5, TCP and Wireshark

Overview:

We've gone over lots of TCP specifics and learned how to associate them with what is going on in `wireshark` analyzing `pcap` files.

Today you will put together all the TCP and `wireshark` knowledge we have to analyze the file `mystery.pcap`.

Write up:

Analyze the `pcap` file and write up your report being sure to answer **all** the following questions in no more than 2 pages.

You must include supporting evidence for every claim. For example, if you answer question 1 and don't refer to a specific packet in the pcap you have not provided any evidence.

Questions:

1. What port numbers and IP addresses are used in this `pcap`?
2. Who is the client? Who is the server? Explain how you know this.
3. What network interface was probably used to take this `pcap`? Explain. (Ethernet is not a network interface!)
4. What is the `MSS` for the client and server?
5. Are any packets larger than the `MSS`? If so, which ones?
6. What causes retransmissions in general?
7. What might've caused the retransmissions in this `pcap`? Provide evidence.
8. What was the retransmission rate?
9. Can `tc` be used to cause retransmissions? If so, what rule might've been used when creating this `pcap`?
10. What `wireshark` filter shows only the retransmitted packets?
11. Does the packet loss appear to affect the transmission rate?
12. Can you tell what file type was sent? If so, what was it?
13. How can you reconstruct the sent data from the `pcap`? What was sent?
14. Do you see a DNS call, if so what port? If not, why not?

Note: `tc` is a program on your virtual machines that you can read about using the `man` pages or any online resources.

Turn in:

You must submit a PDF file with proper grammar. As discussed in class this is a technical document, be succinct and precise. You may include **relevant** figures or screenshots if necessary, but if we find them to be irrelevant you will be deducted points. Be sure to give evidence for any statements made and explain how the conclusion was determined. Do not go over the 2 page limit, we won't read it.

The 2 page limit is only for written text, the bibliography may extend to a third page.

Citations:

If you use **any** websites as references please cite them. You may also cite the book or slides when making statements. If you, for example, find a `tc` rule online that does what I ask, be sure to cite it.

Reminder:

This is an **individual assignment**. I want to see what you know, not your neighbor, and certainly not chatGPT. Your answers should be as specific as possible to the provided pcap.