Lab 2 - HTTP, DNS, and TCP:

Suggested Resources:

https://www.w3.org/Protocols/rfc2616/rfc2616-sec5.html
http://packetbomb.com/understanding-the-tcptrace-time-sequence-graph-in-wireshark/
https://wiki.linuxfoundation.org/networking/netem

Part 1: HTTP

In this section, we will observe how the HTTP protocol operates. We will do this by using the Mininet VM. Begin by opening Wireshark and listening on the 'any' interface.

Open Chromium and navigate to http://www.example.com (not **https**!):

1. (5) Find the packet that corresponds to the initial HTTP request that your computer issued. Take a screenshot of this packet. What HTTP method did your computer use to make this request? What URI did your computer request from the server, as present in the HTTP request? (note: NOT the URL). Explain.
2. (5) Find the packet that corresponds to the initial HTTP response the server issued in response to your request. Take a screenshot of this packet. What HTTP status code did the server return? What is the content type of the response the server is sending back? Explain.

Using Chromium, navigate to http://www.soe.ucsc.edu (not **https**!):

3. (10) Find the packets that correspond to the initial HTTP request and response that your computer issued/received. Take a screenshot of these packets. What's different? Explain.

Using Chromium (or any other Linux utility you are comfortable with), find a way to create an HTTP message using a method other than GET.

4. (10) Take a screenshot of your packet and explain what you did to create it.

Part 2: DNS

In this section, we will observe how the DNS protocol operates. We will do this by using the Mininet VM. Begin by opening Wireshark and listening on the 'any' interface.

Open Chromium and navigate to www.example.com.

5. (5) Were any steps taken by your computer before the web page was loaded? If so, using your captured packets in Wireshark, find the packets that allowed your computer to successfully load http://www.example.com. Take a screenshot of these packets, and explain why you think these are the correct packets. If not, explain why your computer did not need to take these steps.

In Chromium, navigate to http://216.58.193.68.

6. (5) Were any steps taken by your computer before the web page was loaded? If so, using your captured packets in Wireshark, find the packets that allowed your computer to successfully load http://216.58.193.68. Take a screenshot of these packets, and explain why you think these are the correct packets. If not, explain why your computer did not need to take these steps.

Open a terminal window. Using nslookup, find the ***A*** records for www.google.com.

7. (5) Take a screenshot of the packets corresponding to your request, and the response from the server. If the request was resolved, what is the IP address you were given for www.google.com?

8. (5) Did your computer want to complete the request recursively? How do you know? Take a screenshot proving your answer.

Using nslookup, find the ***A*** records for cmpe150.ucsc.edu.

9. (5) Take a screenshot of the packets corresponding to your request, and the response from the server. If the request was resolved, what is the IP address you were given for cmpe150.ucsc.edu?

10. (5) What is the authoritative name server for the ucsc.edu domain? How do you know? Take a screenshot proving your answer.

Part 3: TCP

In this section, we will observe how the TCP protocol operates. We will do this by using the Mininet VM. Begin by opening Wireshark and listening on the 'any' interface.

Open a terminal window. Using wget, download the file http://ipv4.download.thinkbroadband.com/10MB.zip

11. (15) Find the packets corresponding to the SYN, SYN-ACK, and ACK that initiated the TCP connection for this file transfer. Take a screenshot of these packets. What was the initial window size that your computer advertised to the server? What was the initial window size that the server advertised to you?

12. (10) Find a packet from the download whose source address is the server's address and the destination address is your computer's address. Using Wireshark, create a tcptrace graph with this packet selected. Take a screenshot of the graph and explain what it is showing. **Look into the Wireshark documentation if you need assistance making this graph.**

In the next section, we will be simulating loss using the command *tc qdisc*. When you first use the command you should use ***add dev*** for the device you plan on changing. It only needs to be set on the sender's side. After adding the device use ***change dev***. **Look into the suggested link on the top of this assignment if you need assistance using netem.**

```
sudo tc qdisc add dev eth0 root netem loss 0%
sudo tc qdisc change dev eth0 root netem loss 100%
```

Read through this paragraph before starting the next step. Open 2 terminals and have the commands typed and ready before you begin. In one terminal, download the 10MB.zip file again. While the download is in progress, change loss to 100%. After a few seconds, change loss to 0%.

13. (15) Find a packet from the download whose source address is the address of the server and destination address is your computer's address. Create a tcptrace graph with this packet selected. Take a screenshot of the graph and explain what it is showing. Using an image editing program, circle the areas where the 0% loss is shown, as well as where TCP is in slow-start and congestion-avoidance.