Assignment 3

Nathan Ketterlinus   
*Fisher College of Science and Mathematics*  
*Towson University*Towson, United States  
[nketter1@students.towson.edu](mailto:nketter1@students.towson.edu)

Assignment 4.1

Step 2.4

A screenshot of a computer

Description automatically generated

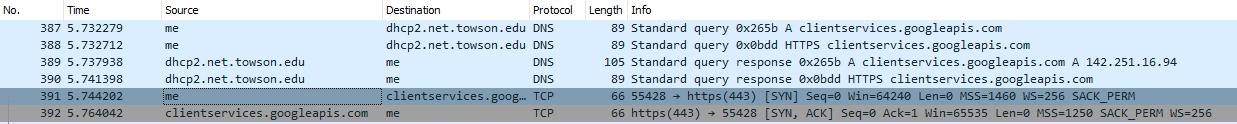
A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

Step 3.1



The first packet sent to the google server (no. 391 above) has the following info:

Source: 10.128.189.79

Destination: 142.251.16.94



Step 3.2

The destination IP address from 3.1 is assigned to GOOGLE

A screenshot of a computer

Description automatically generated

Step 3.3

The protocols used to establish the connection to the web server and deliver the web page to my local host are DNS and TCP, while TCP, TLSv1.3, DNS, and QUIC were used during the window of time that I had google.com open.

Step 3.4

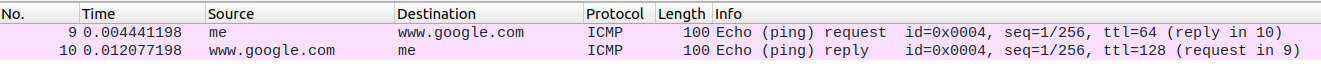
Most traffic between me and google used a light purple color, although some traffic was colored gray or black

Step 4.1.2

Pinging google.com results in network traffic that uses DNS and ICMP protocols

Step 4.1.4

With the icmp filter in use, the only traffic displayed is a ping request and a ping reply



Step 4.2.1

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

The transport protocols used for web traffic include TCP, UDP, and QUIC

4.2.2

This info is found in the 9th IP header field, designated for defining protocol.

4.2.3

TCP is represented by 6, while QUIC and UCP is represented by 17,

4.2.4

Web traffic uses the DNS, TLS, and HTTP protocols.

4.2.5

Computers use information contained in the packet header about IP destinations and port destinations to determine which application should receive an incoming packet.

4.2.6

There are so many inbound and outbound packets when clicking on a link because the host server must send a bunch of packets back to the end user so that they can successfully rebuild the website on their machine. It is important to wait 20 seconds before ending a capture so that any communication that the end user is doing has time to finish, or at the very least all critical communication is finished in time.