**Homework 3**

Graphical user interface, application

Description automatically generated

Graphical user interface, application, table

Description automatically generated

* This was the packet trace used when loading DuckDuckGo on Tor Browser. It was filtered to check for any ports using 443 on TCP which is marked as HTTPS.
* Tor was set to use only port 443 to make it easier to identify Tor Browser’s traffic

Graphical user interface, text, application

Description automatically generated

* To ensure that I didn’t accidentally capture packets from other sources, I shut down any other browser or web application that required an internet connection.
  + After starting the capture, I waited before loading the web page to make sure there were no incoming or outgoing TCP packets prior to initializing the web page.

Packet Analysis:

* For measurement, we’re taking Packet No. 1237 which had a time since first frame of 2.128495 seconds
  + Epoch Time: 1637119225.708895000 seconds
* The matching ACK packet was Packet No. 1274 whose ACK number matches the previous packet’s sequence number.
  + RTT to ACK the segment was: 0.129969 seconds
  + Epoch Time: 1637119225.838864000 seconds
* Measured RTT Time based off Epoch Time: 1637119225.838864000 - 1637119225.708895000 = 0.12996912002 seconds

Graphical user interface, application, table

Description automatically generated

Chart, line chart

Description automatically generated

The destination address of the first node is 162.55.91.19 which is a German server located in Gunzenhausen, Germany[[1]](#footnote-1). Sending a ping command directly to the server shows a latency delay of about 95 milliseconds on average. With the measured RTT time from Tor Browser being about 120~130 ms, there is an additional 25~30 milliseconds of delay used to connect to the other Tor Relay Networks.

A picture containing text

Description automatically generated

Results of the ping test to the German server

To measure the maximum possible range, a network test was used on SpeedTest to measure the ping latency to a server that would match the additional 25 ms of delay. The server with the matching latency time was a server located in Hartwell, Georgia which is located approximately 800 miles from New York City. This would mean that there is a total distance of at most 800 miles from Gunzenhausen to wherever the second Tor Relay server is located at.

Graphical user interface, application

Description automatically generated

With the maximum total range being about an additional 800 miles, the Tor Relay nodes can be located within most of central Europe. The figure below shows the where the second Tor Relay node could be located at for the possibility of retaining that additional 25 ms worth of RTT.

Chart, map

Description automatically generated

The 800-mile radius of where the second Tor Relay nodes could be placed relative to the first Tor server

Upon inspecting the rest of the packets, they either had an RTT time of less than 2 ms or they had an RTT time of over 100 ms. Most of the packets had an average RTT time of around 130 ms which is consistent with the RTT measured for the first packet response. This means the first, second and third Tor Relay nodes are communicating with each other somewhere within central Europe before having to carry the connection from my computer and to DuckDuckGo’s server.

1. https://www.whois.com/whois/162.55.91.19 [↑](#footnote-ref-1)