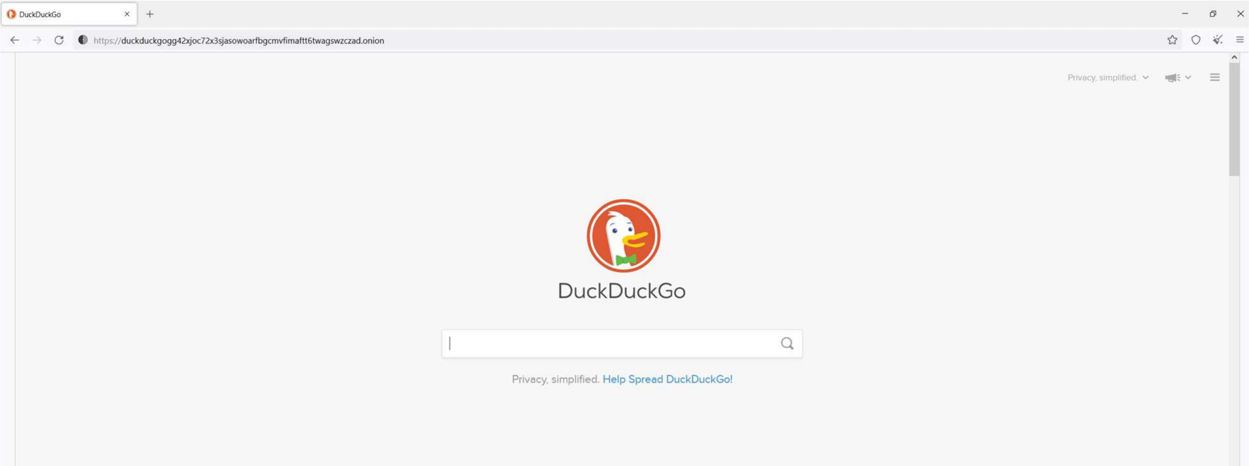
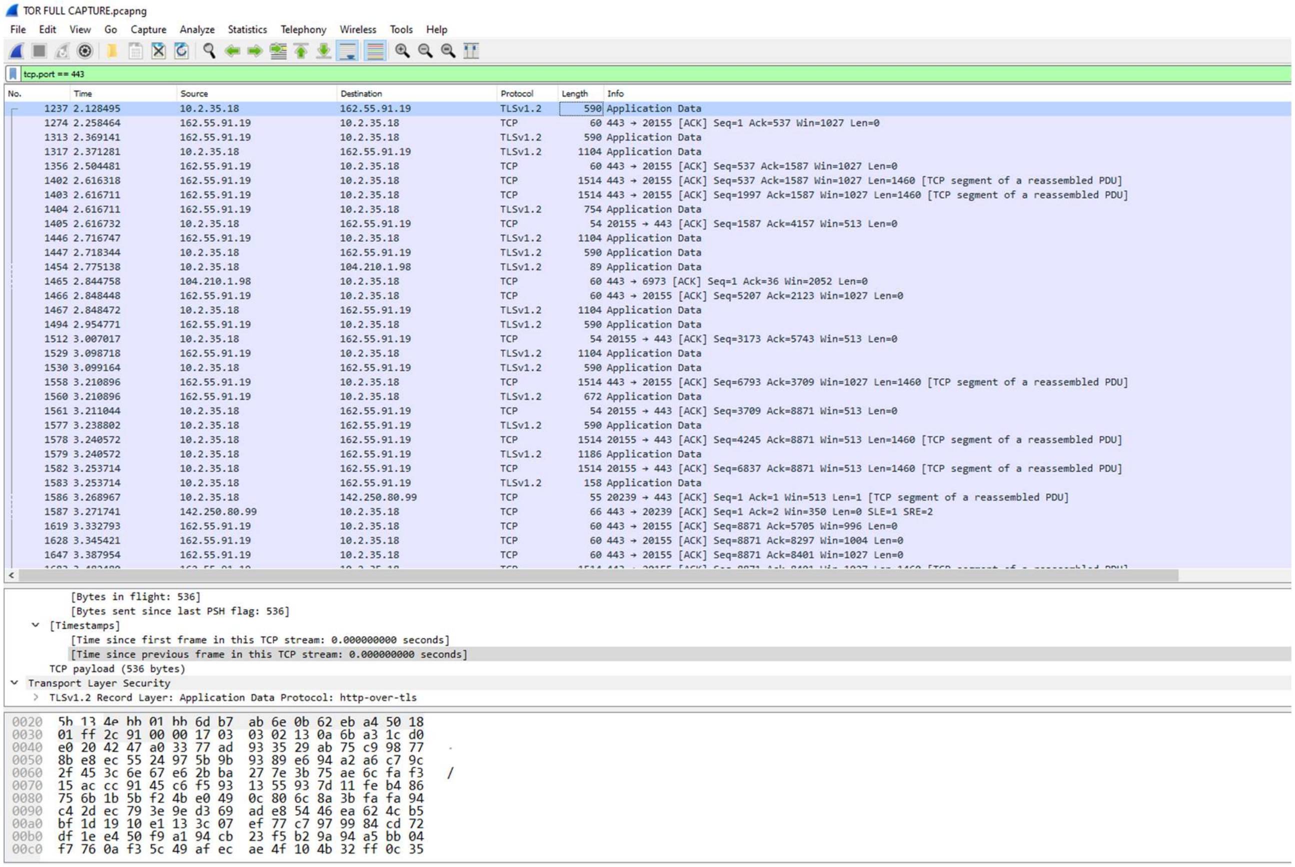
Brandon Vo

Homework 3


DuckDuckGo
https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion
Privacy, simplified.
DuckDuckGo
Privacy, simplified. Help Spread DuckDuckGo!



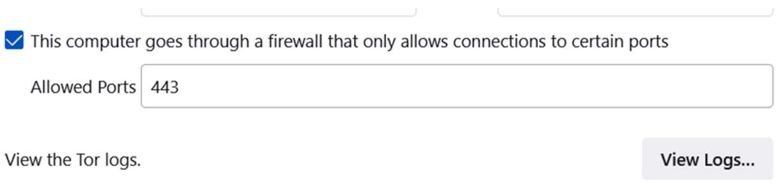
```
tcp.port == 443
```

```
No.     Time        Source          Destination     Protocol  Length Info
   1237 2.128495    10.2.35.18      162.55.91.19    TLSv1.2      590 Application Data
   1274 2.258464    162.55.91.19    10.2.35.18      TCP           60 443 → 20155 [ACK] Seq=1 Ack=537 Win=1027 Len=0
   1313 2.369141    162.55.91.19    10.2.35.18      TLSv1.2      590 Application Data
   1317 2.371281    10.2.35.18      162.55.91.19    TLSv1.2     1104 Application Data
   1356 2.504481    162.55.91.19    10.2.35.18      TCP           60 443 → 20155 [ACK] Seq=537 Ack=1587 Win=1027 Len=0
   1402 2.616318    162.55.91.19    10.2.35.18      TCP         1514 443 → 20155 [ACK] Seq=537 Ack=1587 Win=1027 Len=1460 [TCP segment of a reassembled PDU]
   1403 2.616711    162.55.91.19    10.2.35.18      TCP         1514 443 → 20155 [ACK] Seq=1997 Ack=1587 Win=1027 Len=1460 [TCP segment of a reassembled PDU]
   1404 2.616711    162.55.91.19    10.2.35.18      TLSv1.2      754 Application Data
   1405 2.616732    10.2.35.18      162.55.91.19    TCP           54 20155 → 443 [ACK] Seq=1587 Ack=4157 Win=513 Len=0
   1446 2.716747    162.55.91.19    10.2.35.18      TLSv1.2     1104 Application Data
   1447 2.718344    10.2.35.18      162.55.91.19    TLSv1.2      590 Application Data
   1454 2.775138    10.2.35.18      104.210.1.98    TLSv1.2       89 Application Data
   1465 2.844758    104.210.1.98    10.2.35.18      TCP           60 443 → 6973 [ACK] Seq=1 Ack=36 Win=2052 Len=0
   1466 2.848448    162.55.91.19    10.2.35.18      TCP           60 443 → 20155 [ACK] Seq=5207 Ack=2123 Win=1027 Len=0
   1467 2.848472    10.2.35.18      162.55.91.19    TLSv1.2     1104 Application Data
   1494 2.954771    162.55.91.19    10.2.35.18      TLSv1.2      590 Application Data
   1512 3.007017    10.2.35.18      162.55.91.19    TCP           54 20155 → 443 [ACK] Seq=3173 Ack=5743 Win=513 Len=0
   1529 3.098718    162.55.91.19    10.2.35.18      TLSv1.2     1104 Application Data
   1530 3.099164    10.2.35.18      162.55.91.19    TLSv1.2      590 Application Data
   1558 3.210896    162.55.91.19    10.2.35.18      TCP         1514 443 → 20155 [ACK] Seq=6793 Ack=3709 Win=1027 Len=1460 [TCP segment of a reassembled PDU]
   1560 3.210896    162.55.91.19    10.2.35.18      TLSv1.2      672 Application Data
   1561 3.211044    10.2.35.18      162.55.91.19    TCP           54 20155 → 443 [ACK] Seq=3709 Ack=8871 Win=513 Len=0
   1577 3.238802    10.2.35.18      162.55.91.19    TLSv1.2      590 Application Data
   1578 3.240572    10.2.35.18      162.55.91.19    TCP         1514 20155 → 443 [ACK] Seq=4245 Ack=8871 Win=513 Len=1460 [TCP segment of a reassembled PDU]
   1579 3.240572    10.2.35.18      162.55.91.19    TLSv1.2     1186 Application Data
   1582 3.253714    10.2.35.18      162.55.91.19    TCP         1514 20155 → 443 [ACK] Seq=6837 Ack=8871 Win=513 Len=1460 [TCP segment of a reassembled PDU]
   1583 3.253714    10.2.35.18      162.55.91.19    TLSv1.2      158 Application Data
   1586 3.268967    10.2.35.18      142.250.80.99   TCP           55 20239 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
   1587 3.271741    142.250.80.99   10.2.35.18      TCP           66 443 → 20239 [ACK] Seq=1 Ack=2 Win=350 Len=0 SLE=1 SRE=2
   1619 3.332793    162.55.91.19    10.2.35.18      TCP           60 443 → 20155 [ACK] Seq=8871 Ack=5705 Win=996 Len=0
   1628 3.345421    162.55.91.19    10.2.35.18      TCP           60 443 → 20155 [ACK] Seq=8871 Ack=8297 Win=1004 Len=0
   1647 3.387954    162.55.91.19    10.2.35.18      TCP           60 443 → 20155 [ACK] Seq=8871 Ack=8401 Win=1027 Len=0
```

```
        [Bytes in flight: 536]
        [Bytes sent since last PSH flag: 536]
    ⌄ [Timestamps]
        [Time since first frame in this TCP stream: 0.000000000 seconds]
        [Time since previous frame in this TCP stream: 0.000000000 seconds]
    TCP payload (536 bytes)
⌄ Transport Layer Security
    > TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
```

```
0020  5b 13 4e bb 01 bb 6d b7  ab 6e 0b 62 eb a4 50 18
0030  01 ff 2c 91 00 00 17 03  03 02 13 0a 6b a3 1c d0
0040  e0 20 42 47 a0 33 77 ad  93 35 29 ab 75 c9 98 77
0050  8b e8 ec 55 24 97 5b 9b  93 89 e6 94 a2 a6 c7 9c
0060  2f 45 3c 6e 67 e6 2b ba  27 7e 3b 75 ae 6c fa f3
0070  15 ac cc 91 45 c6 f5 93  13 55 93 7d 11 fe b4 86
0080  75 6b 1b 5b f2 4b e0 49  0c 80 6c 8a 3b fa fa 94
0090  c4 2d ec 79 3e 9e d3 69  ad e8 54 46 ea 62 4c b5
00a0  bf 1d 19 10 e1 13 3c 07  ef 77 c7 97 99 84 cd 72
00b0  df 1e e4 50 f9 a1 94 cb  23 f5 b2 9a 94 a5 bb 04
00c0  f7 76 0a f3 5c 49 af ec  ae 4f 10 4b 32 ff 0c 35
```

- 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



☑ This computer goes through a firewall that only allows connections to certain ports

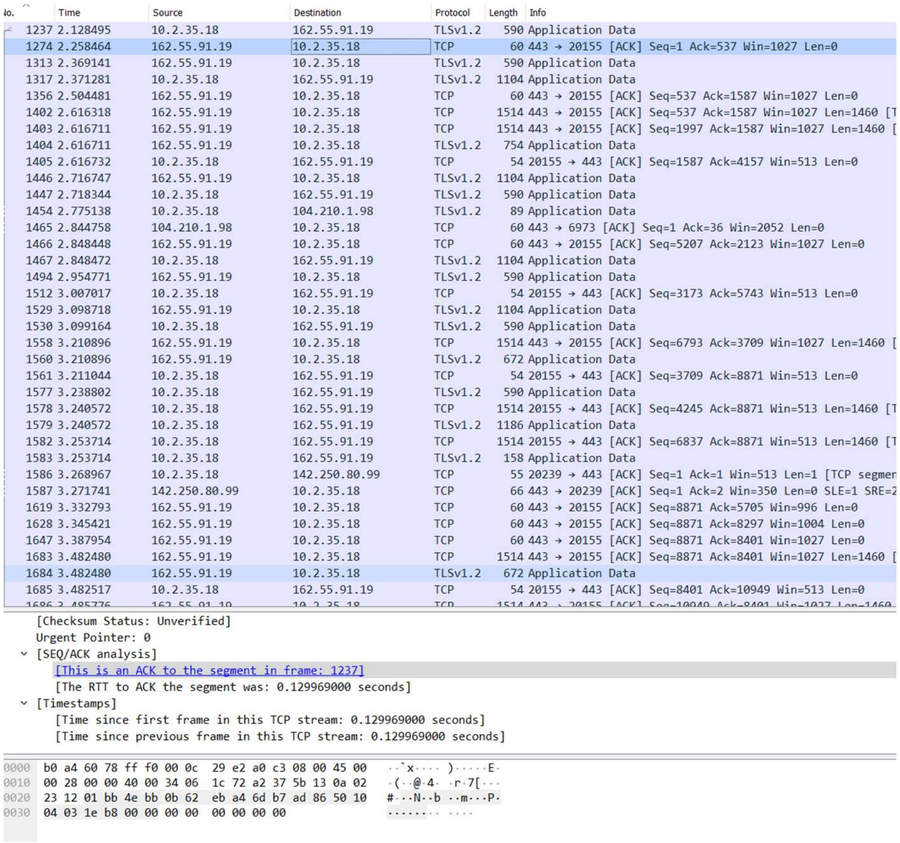
Allowed Ports 443

View the Tor logs.

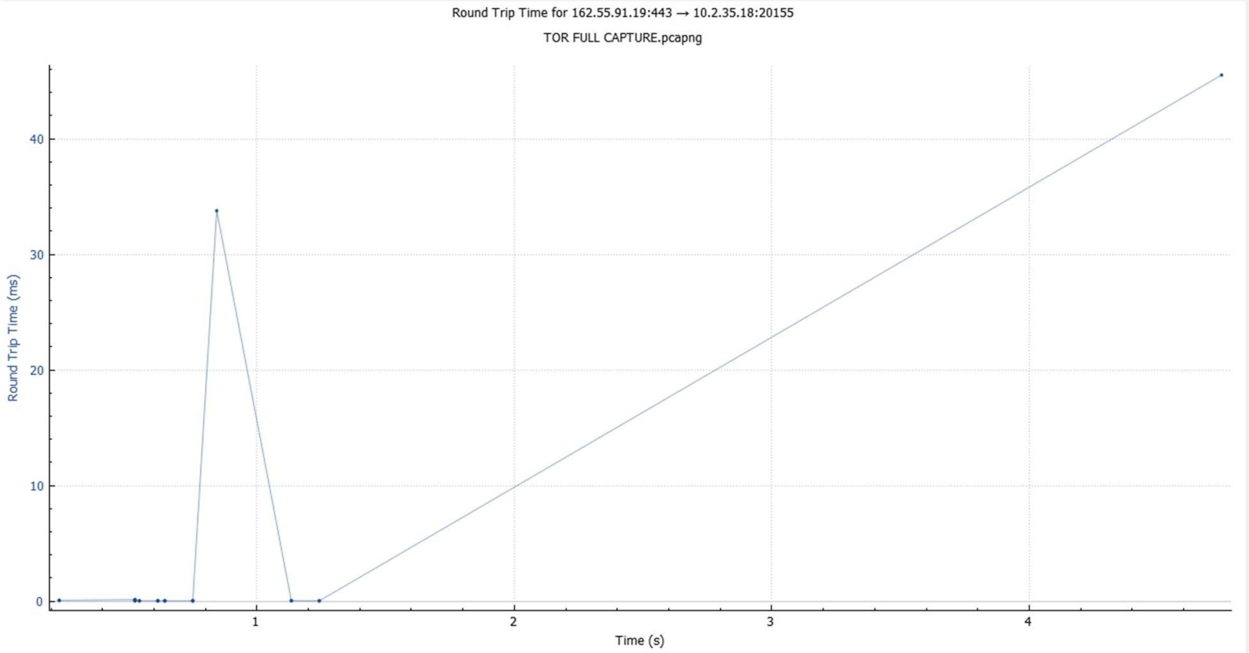
- To ensure that I didn't accidentally capture packets from other sources, I shut down any other browser or web application that required an internet connection.
    - After starting the capture, I waited before loading the web page to make sure there were no incoming or outgoing TCP packets prior to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

Packet Analysis:

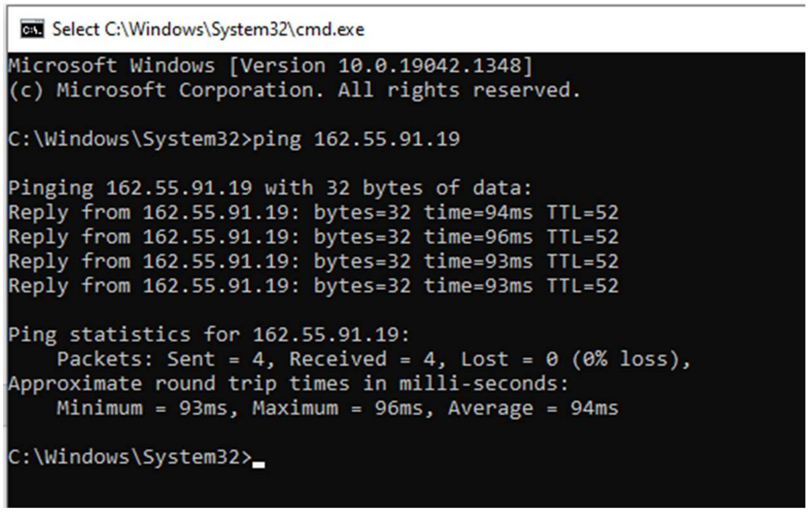
- For measurement, we're taking Packet No. 1237 which had a time since first frame of 2.128495 seconds
    - Epoch Time: 1637119225.708895000 seconds
- The matching ACK packet was Packet No. 1274 whose ACK number matches the previous packet's sequence number.
    - RTT to ACK the segment was: 0.129969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



```
No.  Time      Source         Destination    Protocol Length Info
1237 2.128495  10.2.35.18     162.55.91.19   TLSv1.2   590 Application Data
1274 2.258464  162.55.91.19   10.2.35.18     TCP        60 443 → 20155 [ACK] Seq=1 Ack=537 Win=1027 Len=0
1313 2.369141  162.55.91.19   10.2.35.18     TLSv1.2   590 Application Data
1317 2.371281  10.2.35.18     162.55.91.19   TLSv1.2  1104 Application Data
1356 2.504481  162.55.91.19   10.2.35.18     TCP        60 443 → 20155 [ACK] Seq=537 Ack=1587 Win=1027 Len=0
1402 2.616318  162.55.91.19   10.2.35.18     TCP      1514 443 → 20155 [ACK] Seq=537 Ack=1587 Win=1027 Len=1460 [T
1403 2.616711  162.55.91.19   10.2.35.18     TCP      1514 443 → 20155 [ACK] Seq=1997 Ack=1587 Win=1027 Len=1460 [
1404 2.616711  162.55.91.19   10.2.35.18     TLSv1.2   754 Application Data
1405 2.616732  10.2.35.18     162.55.91.19   TCP        54 20155 → 443 [ACK] Seq=1587 Ack=4157 Win=513 Len=0
1446 2.716747  162.55.91.19   10.2.35.18     TLSv1.2  1104 Application Data
1447 2.718344  10.2.35.18     162.55.91.19   TLSv1.2   590 Application Data
1454 2.775138  10.2.35.18     104.210.1.98   TLSv1.2    89 Application Data
1465 2.844758  104.210.1.98   10.2.35.18     TCP        60 443 → 6973 [ACK] Seq=1 Ack=36 Win=2052 Len=0
1466 2.848448  162.55.91.19   10.2.35.18     TCP        60 443 → 20155 [ACK] Seq=5207 Ack=2123 Win=1027 Len=0
1467 2.848472  10.2.35.18     162.55.91.19   TLSv1.2  1104 Application Data
1494 2.954771  162.55.91.19   10.2.35.18     TLSv1.2   590 Application Data
1512 3.007017  10.2.35.18     162.55.91.19   TCP        54 20155 → 443 [ACK] Seq=3173 Ack=5743 Win=513 Len=0
1529 3.098718  162.55.91.19   10.2.35.18     TLSv1.2  1104 Application Data
1530 3.099164  10.2.35.18     162.55.91.19   TLSv1.2   590 Application Data
1558 3.210896  162.55.91.19   10.2.35.18     TCP      1514 443 → 20155 [ACK] Seq=6793 Ack=3709 Win=1027 Len=1460 [
1560 3.210896  162.55.91.19   10.2.35.18     TLSv1.2   672 Application Data
1561 3.211044  10.2.35.18     162.55.91.19   TCP        54 20155 → 443 [ACK] Seq=3709 Ack=8871 Win=513 Len=0
1577 3.238802  10.2.35.18     162.55.91.19   TLSv1.2   590 Application Data
1578 3.240572  10.2.35.18     162.55.91.19   TCP      1514 20155 → 443 [ACK] Seq=4245 Ack=8871 Win=513 Len=1460 [T
1579 3.240572  10.2.35.18     162.55.91.19   TLSv1.2  1186 Application Data
1582 3.253714  10.2.35.18     162.55.91.19   TCP      1514 20155 → 443 [ACK] Seq=6837 Ack=8871 Win=513 Len=1460 [T
1583 3.253714  10.2.35.18     162.55.91.19   TLSv1.2   158 Application Data
1586 3.268967  10.2.35.18     142.250.80.99  TCP        55 20239 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segmen
1587 3.271741  142.250.80.99  10.2.35.18     TCP        66 443 → 20239 [ACK] Seq=1 Ack=2 Win=350 Len=0 SLE=1 SRE=2
1619 3.332793  162.55.91.19   10.2.35.18     TCP        60 443 → 20155 [ACK] Seq=8871 Ack=5705 Win=996 Len=0
1628 3.345421  162.55.91.19   10.2.35.18     TCP        60 443 → 20155 [ACK] Seq=8871 Ack=8297 Win=1004 Len=0
1647 3.387954  162.55.91.19   10.2.35.18     TCP        60 443 → 20155 [ACK] Seq=8871 Ack=8401 Win=1027 Len=0
1683 3.482480  162.55.91.19   10.2.35.18     TCP      1514 443 → 20155 [ACK] Seq=8871 Ack=8401 Win=1027 Len=1460 [
1684 3.482480  162.55.91.19   10.2.35.18     TLSv1.2   672 Application Data
1685 3.482517  10.2.35.18     162.55.91.19   TCP        54 20155 → 443 [ACK] Seq=8401 Ack=10949 Win=513 Len=0
1686 3.485776  162.55.91.19   10.2.35.18     TCP      1514 443 → 20155 [ACK] Seq=10949 Ack=8401 Win=1027 Len=1460

    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ˅ [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 1237]
      [The RTT to ACK the segment was: 0.129969000 seconds]
  ˅ [Timestamps]
      [Time since first frame in this TCP stream: 0.129969000 seconds]
      [Time since previous frame in this TCP stream: 0.129969000 seconds]

0000  b0 a4 60 78 ff f0 00 0c  29 e2 a0 c3 08 00 45 00   ··`x····)·····E·
0010  00 28 00 00 40 00 34 06  1c 72 a2 37 5b 13 0a 02   ·(··@·4··r·7[···
0020  23 12 01 bb 4e bb 0b 62  eb a4 6d b7 ad 86 50 10   #···N··b··m···P·
0030  04 03 1e b8 00 00 00 00  00 00 00 00               ············
```



The destination address of the first node is 162.55.91.19 which is a German server located in Gunzenhausen, Germany[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.

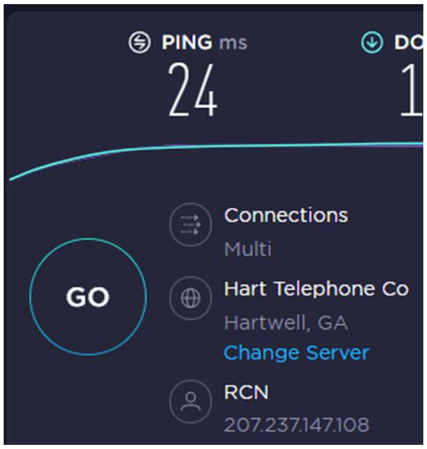


```
Microsoft Windows [Version 10.0.19042.1348]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>ping 162.55.91.19

Pinging 162.55.91.19 with 32 bytes of data:
Reply from 162.55.91.19: bytes=32 time=94ms TTL=52
Reply from 162.55.91.19: bytes=32 time=96ms TTL=52
Reply from 162.55.91.19: bytes=32 time=93ms TTL=52
Reply from 162.55.91.19: bytes=32 time=93ms TTL=52

Ping statistics for 162.55.91.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 93ms, Maximum = 96ms, Average = 94ms

C:\Windows\System32>_
```

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.

[1] https://www.whois.com/whois/162.55.91.19



PING ms
24

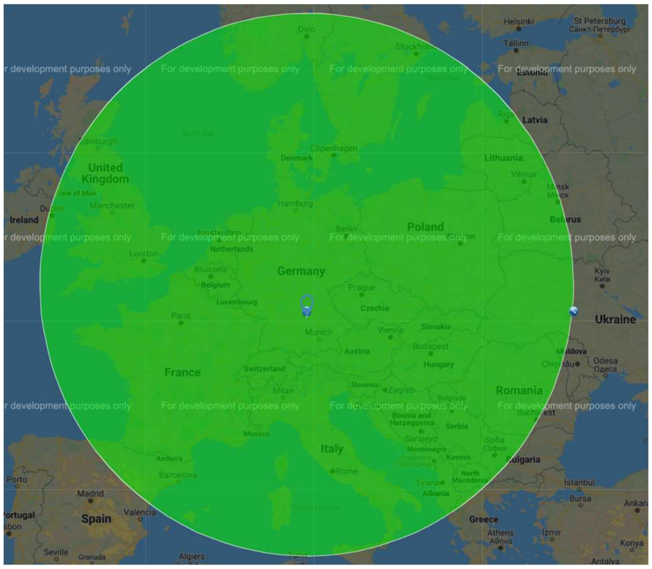
DO
1

Connections
Multi

Hart Telephone Co
Hartwell, GA

RCN
207.237.147.108

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.



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.