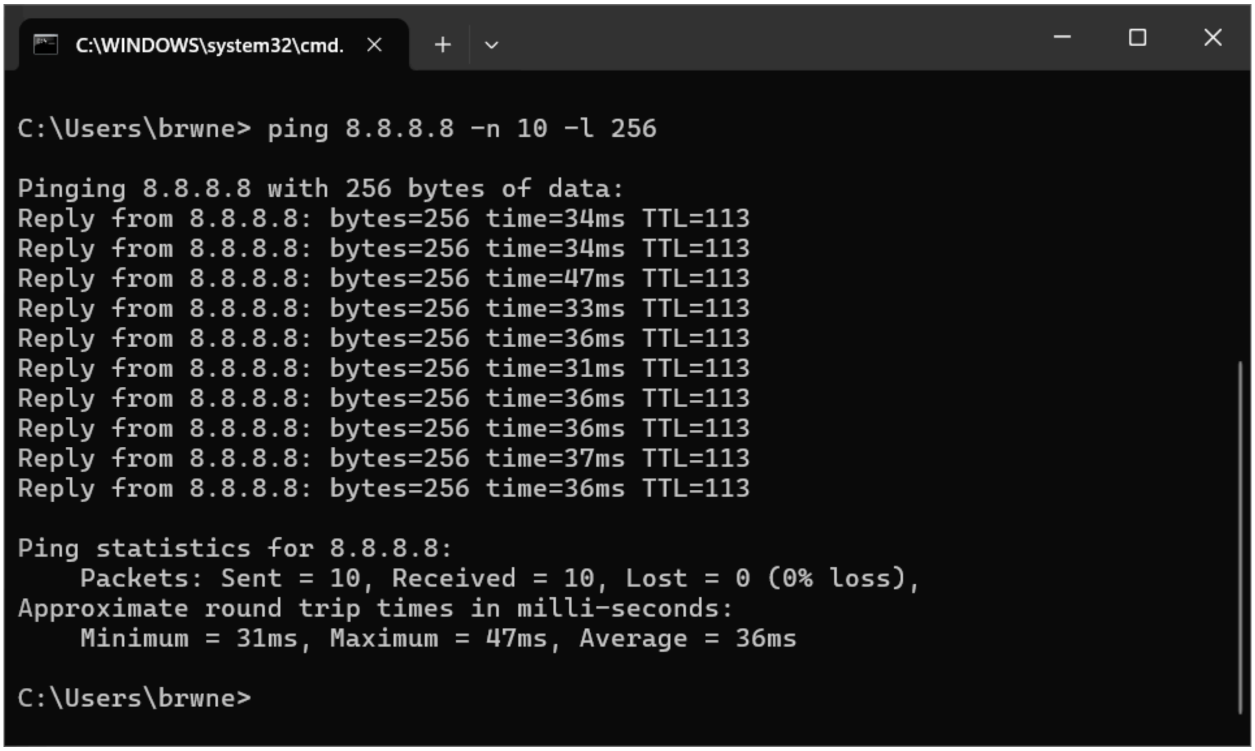
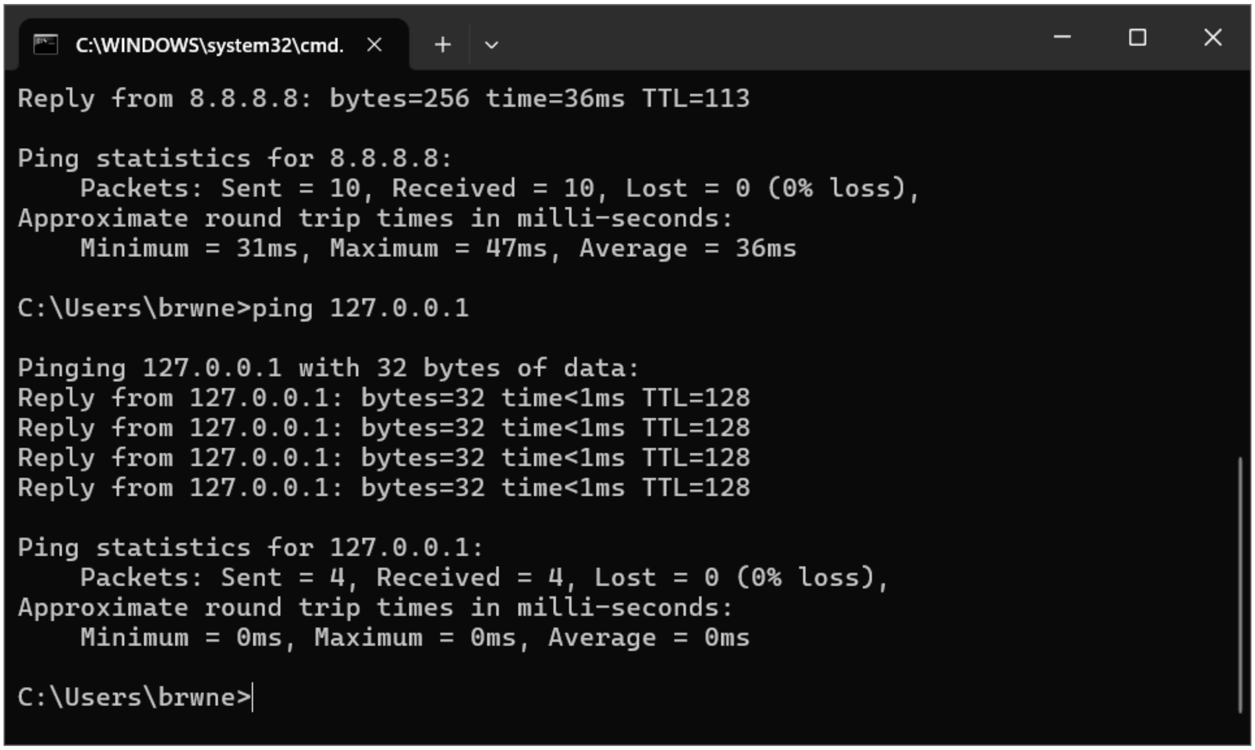
# Lab Assignment 1

The PING (Packet Internet Groper)command

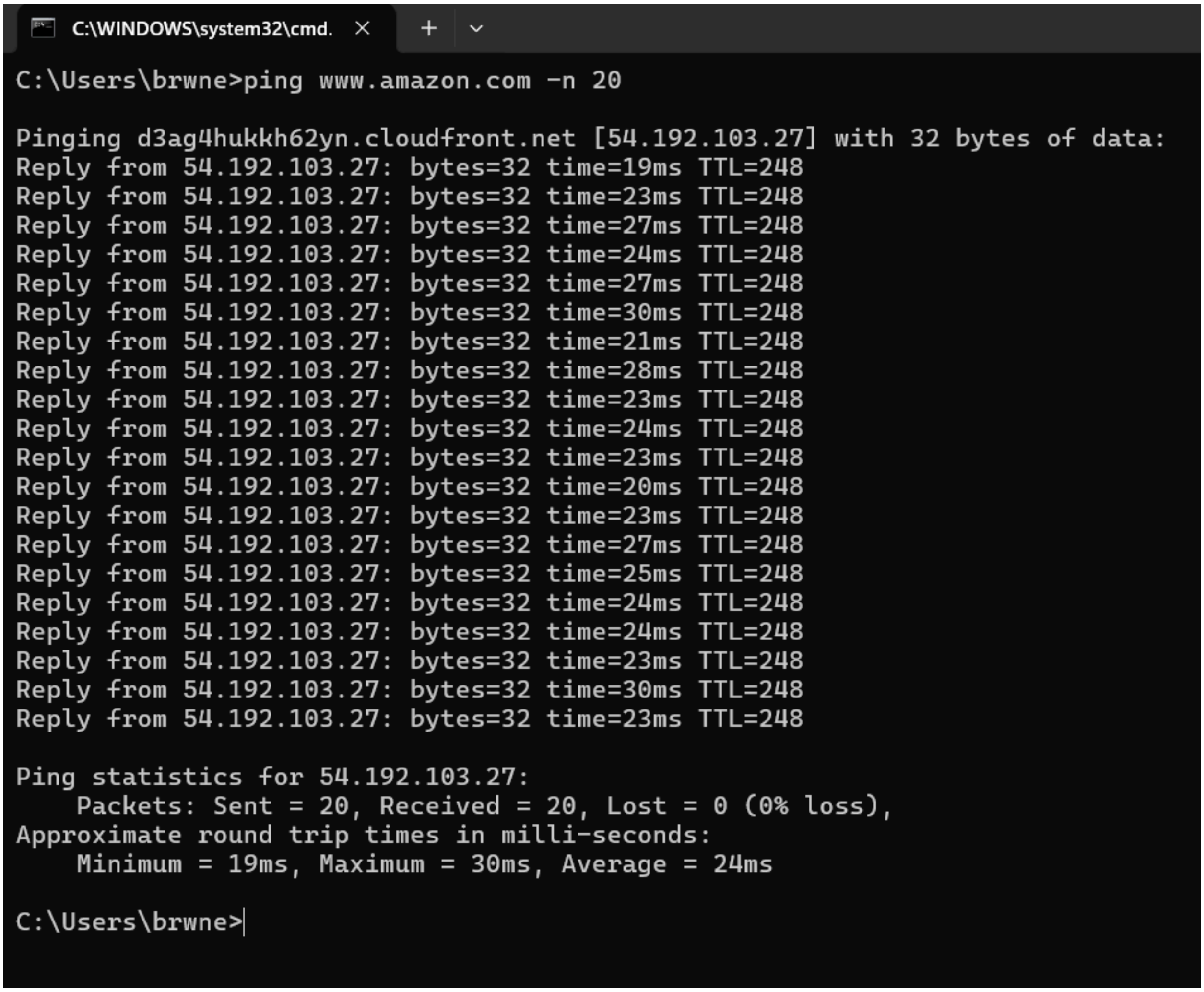


```
C:\Users\brwne> ping 8.8.8.8 -n 10 -l 256

Pinging 8.8.8.8 with 256 bytes of data:
Reply from 8.8.8.8: bytes=256 time=34ms TTL=113
Reply from 8.8.8.8: bytes=256 time=34ms TTL=113
Reply from 8.8.8.8: bytes=256 time=47ms TTL=113
Reply from 8.8.8.8: bytes=256 time=33ms TTL=113
Reply from 8.8.8.8: bytes=256 time=36ms TTL=113
Reply from 8.8.8.8: bytes=256 time=31ms TTL=113
Reply from 8.8.8.8: bytes=256 time=36ms TTL=113
Reply from 8.8.8.8: bytes=256 time=36ms TTL=113
Reply from 8.8.8.8: bytes=256 time=37ms TTL=113
Reply from 8.8.8.8: bytes=256 time=36ms TTL=113

Ping statistics for 8.8.8.8:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 31ms, Maximum = 47ms, Average = 36ms

C:\Users\brwne>
```



```
Reply from 8.8.8.8: bytes=256 time=36ms TTL=113

Ping statistics for 8.8.8.8:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 31ms, Maximum = 47ms, Average = 36ms

C:\Users\brwne>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\brwne>
```

A. Four packets were sent. The default size for each packet is 32 bytes.
B. Google accepted 256.
C. Average = 41ms
D. TTL value indicated is 113. TTL is Time To Live. It tells how many hops a packet can make before being discarded. A higher TTL means the packet can travel further.
E. By running: ping 127.0.0.1. My default TTL = 128.
F. Protocol used is Internet Control Message Protocol (ICMP).

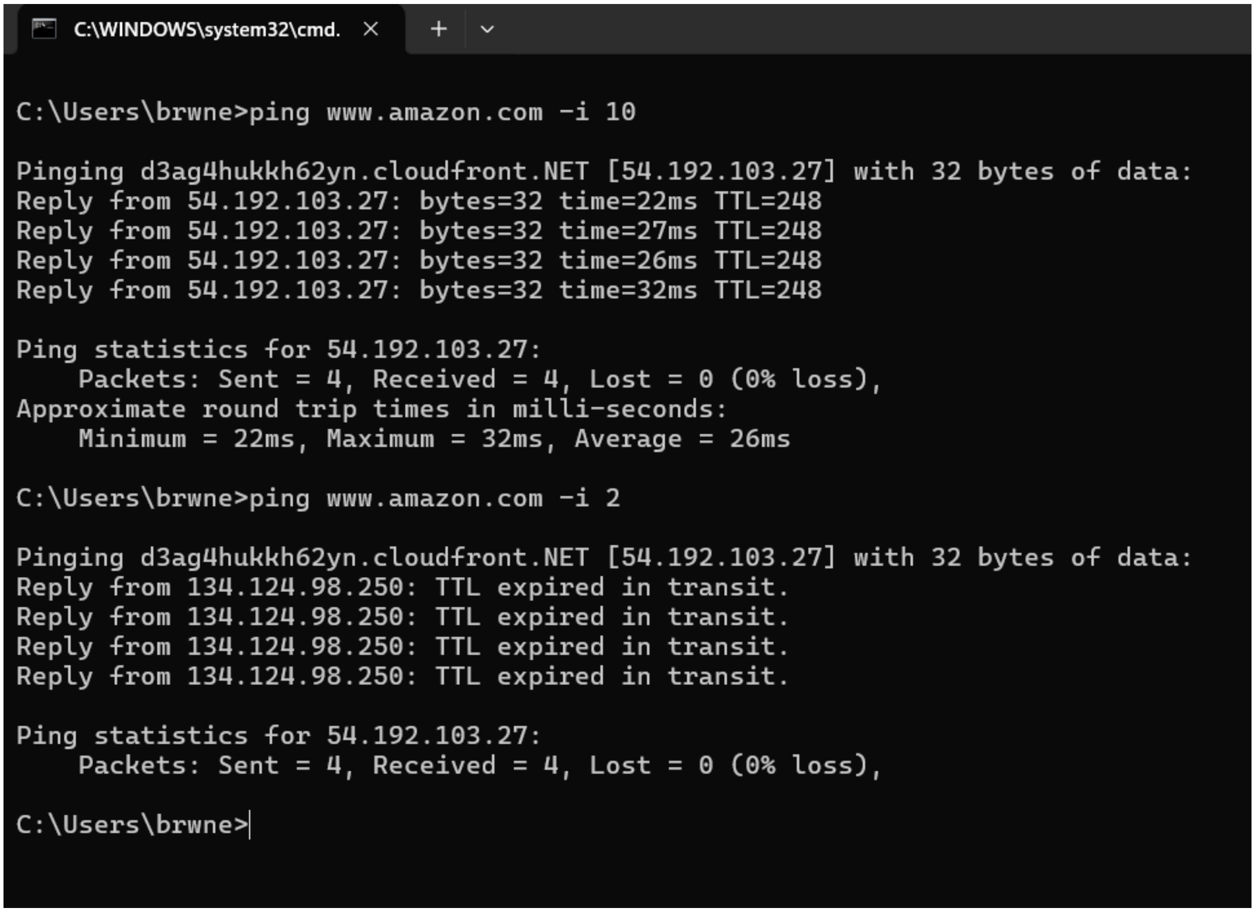


```
C:\Users\brwne>ping www.amazon.com -n 20

Pinging d3ag4hukkh62yn.cloudfront.net [54.192.103.27] with 32 bytes of data:
Reply from 54.192.103.27: bytes=32 time=19ms TTL=248
Reply from 54.192.103.27: bytes=32 time=23ms TTL=248
Reply from 54.192.103.27: bytes=32 time=27ms TTL=248
Reply from 54.192.103.27: bytes=32 time=24ms TTL=248
Reply from 54.192.103.27: bytes=32 time=27ms TTL=248
Reply from 54.192.103.27: bytes=32 time=30ms TTL=248
Reply from 54.192.103.27: bytes=32 time=21ms TTL=248
Reply from 54.192.103.27: bytes=32 time=28ms TTL=248
Reply from 54.192.103.27: bytes=32 time=23ms TTL=248
Reply from 54.192.103.27: bytes=32 time=24ms TTL=248
Reply from 54.192.103.27: bytes=32 time=23ms TTL=248
Reply from 54.192.103.27: bytes=32 time=20ms TTL=248
Reply from 54.192.103.27: bytes=32 time=23ms TTL=248
Reply from 54.192.103.27: bytes=32 time=27ms TTL=248
Reply from 54.192.103.27: bytes=32 time=25ms TTL=248
Reply from 54.192.103.27: bytes=32 time=24ms TTL=248
Reply from 54.192.103.27: bytes=32 time=24ms TTL=248
Reply from 54.192.103.27: bytes=32 time=23ms TTL=248
Reply from 54.192.103.27: bytes=32 time=30ms TTL=248
Reply from 54.192.103.27: bytes=32 time=23ms TTL=248

Ping statistics for 54.192.103.27:
    Packets: Sent = 20, Received = 20, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 30ms, Average = 24ms

C:\Users\brwne>
```

G. Amazon IP address is [54.192.103.27]

H. The TTL value is now 248. The TTL value differs because Amazon’s server and Google’s server use different operating systems and network configurations, which start with different default TTL values (e.g., 64, 128, or 255). Additionally, the number of hops (routers between my computer and the server) is different for each destination. Since each hop decreases the TTL by 1, the final TTL value reported by ping depends on both the server’s starting TTL and how many hops the packet traveled.

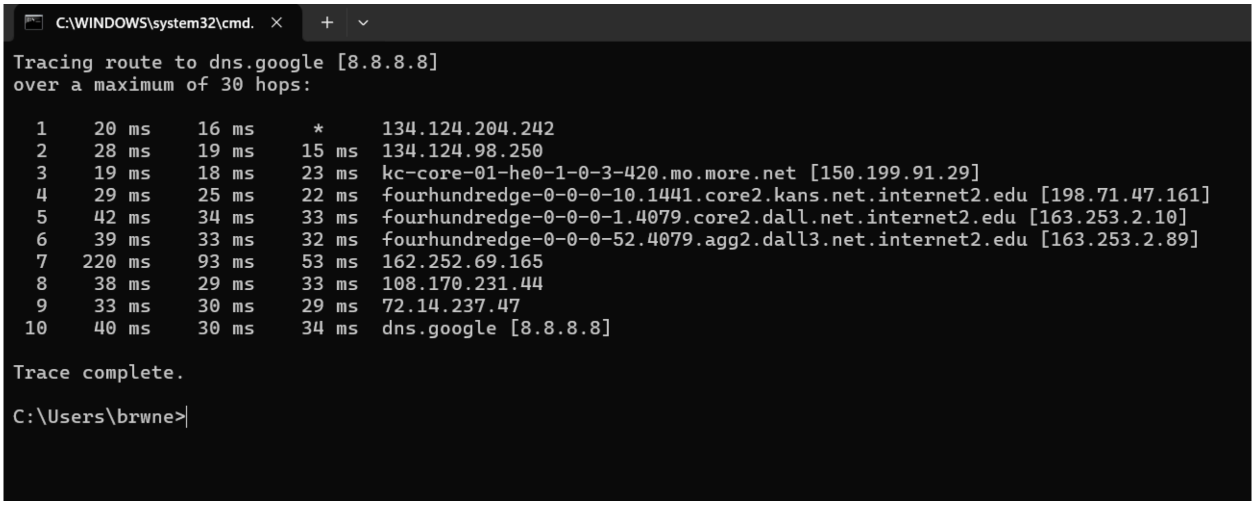
I. Amazon was not more than 10 hops away so the ping was still successful. So I set the TTL to 2, then the TTL expired in Transit. TTL is like a time limit on how far packets can travel.  Since Amazon was more than two hops away, it failed.



```
C:\Users\brwne>ping www.amazon.com -i 10

Pinging d3ag4hukkh62yn.cloudfront.NET [54.192.103.27] with 32 bytes of data:
Reply from 54.192.103.27: bytes=32 time=22ms TTL=248
Reply from 54.192.103.27: bytes=32 time=27ms TTL=248
Reply from 54.192.103.27: bytes=32 time=26ms TTL=248
Reply from 54.192.103.27: bytes=32 time=32ms TTL=248

Ping statistics for 54.192.103.27:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 32ms, Average = 26ms

C:\Users\brwne>ping www.amazon.com -i 2

Pinging d3ag4hukkh62yn.cloudfront.NET [54.192.103.27] with 32 bytes of data:
Reply from 134.124.98.250: TTL expired in transit.
Reply from 134.124.98.250: TTL expired in transit.
Reply from 134.124.98.250: TTL expired in transit.
Reply from 134.124.98.250: TTL expired in transit.

Ping statistics for 54.192.103.27:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\brwne>
```

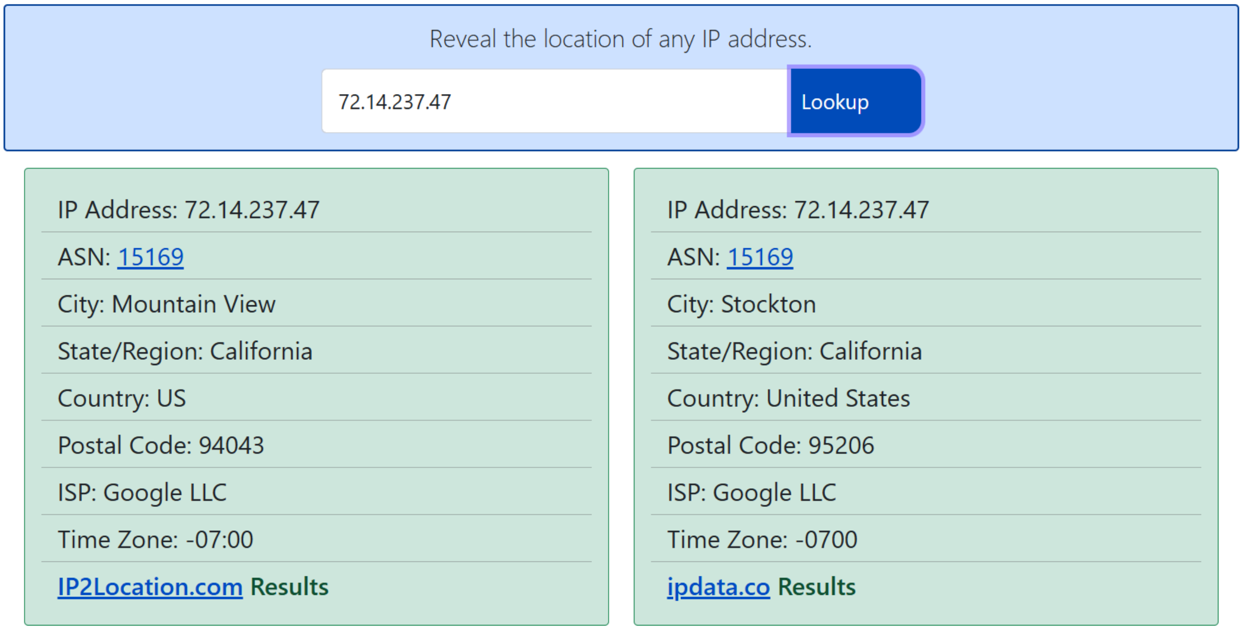
J. Two main factors are physical distance/propagation delay and network congestion and routing. Physical distance/propagation delay because signals travel at finite speed, so a server farther away = longer RTT. Network congestion & routing becasue busy links, number of hops, and path efficiency impact delay. Also there are processing delays at intermediate routers.

## The Traceroute/Tracert utility



```
Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  1    20 ms    16 ms     *     134.124.204.242
  2    28 ms    19 ms    15 ms  134.124.98.250
  3    19 ms    18 ms    23 ms  kc-core-01-he0-1-0-3-420.mo.more.net [150.199.91.29]
  4    29 ms    25 ms    22 ms  fourhundredge-0-0-0-10.1441.core2.kans.net.internet2.edu [198.71.47.161]
  5    42 ms    34 ms    33 ms  fourhundredge-0-0-0-1.4079.core2.dall.net.internet2.edu [163.253.2.10]
  6    39 ms    33 ms    32 ms  fourhundredge-0-0-0-52.4079.agg2.dall3.net.internet2.edu [163.253.2.89]
  7   220 ms    93 ms    53 ms  162.252.69.165
  8    38 ms    29 ms    33 ms  108.170.231.44
  9    33 ms    30 ms    29 ms  72.14.237.47
 10    40 ms    30 ms    34 ms  dns.google [8.8.8.8]

Trace complete.

C:\Users\brwne>
```

A. Routers = 9 ; Hops = 10
B. 30 is the default but it can be overridden or configured with -h up to 255 (max)
C. Minimum os 30ms ; maximum is 40 ms



Reveal the location of any IP address.

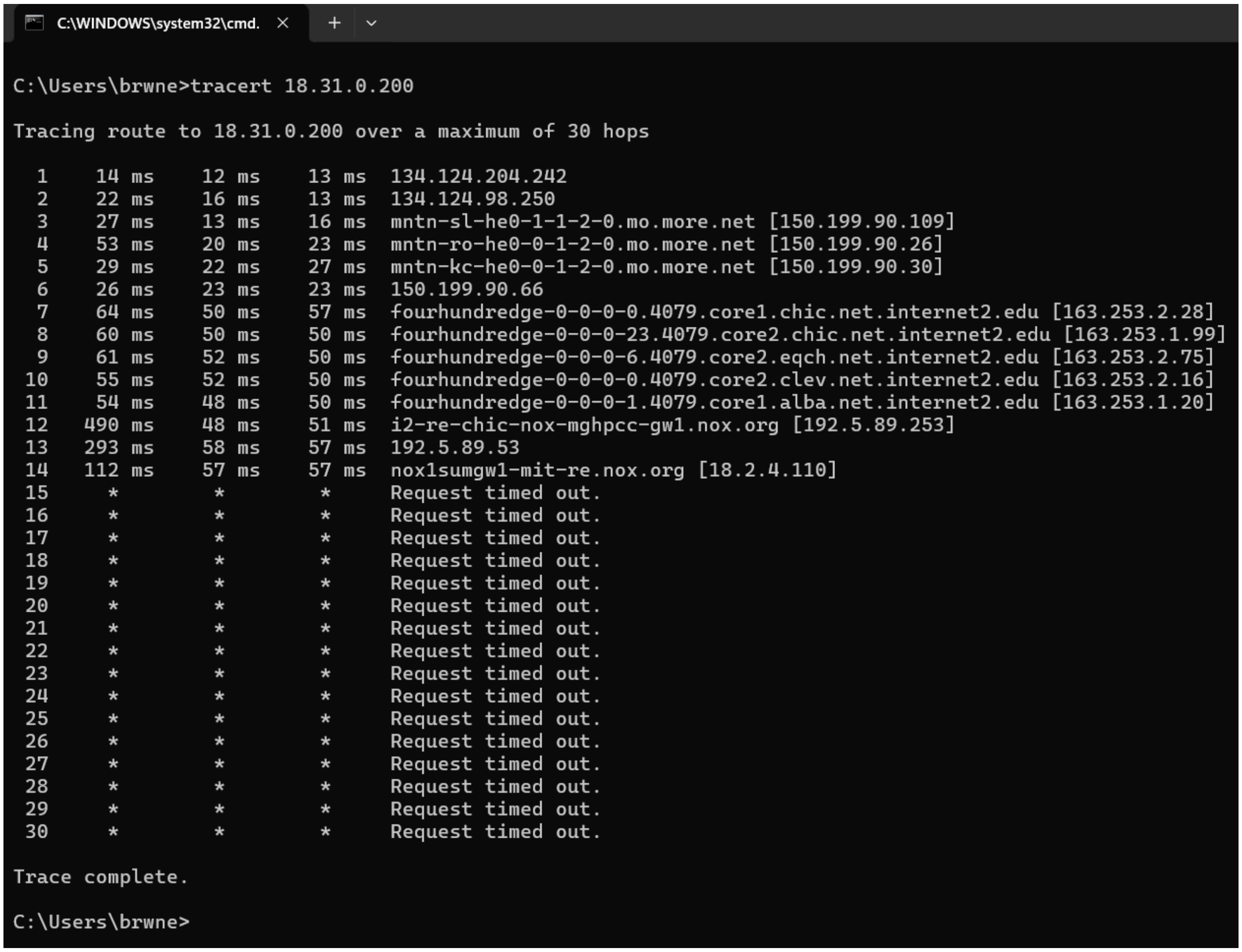
IP Address: 72.14.237.47
ASN: 15169
City: Mountain View
State/Region: California
Country: US
Postal Code: 94043
ISP: Google LLC
Time Zone: -07:00
IP2Location.com Results

IP Address: 72.14.237.47
ASN: 15169
City: Stockton
State/Region: California
Country: United States
Postal Code: 95206
ISP: Google LLC
Time Zone: -0700
ipdata.co Results

D.

E. The tracert command on Windows discovers the path by sending Internet Control Message Protocol (ICMP) Echo Request packets with a gradually increasing Time To Live (TTL) value. It begins with TTL set to 1, so the very first router decrements the TTL to 0 and then returns an ICMP Time Exceeded message, which reveals that router's IP address and response time. tracert then increases the TTL to 2, which allows the packet to pass through the first router and reach the second router before expiring. This process continues, with the TTL increasing by one for each set of probes, until the packet finally reaches the destination. At that point, the destination host responds with an ICMP Echo

Reply, completing the trace. In this way, tracert is able to map the sequence of routers (hops) between the source and the destination while also reporting the delay at each step.

F. 

```
C:\Users\brwne>tracert 18.31.0.200

Tracing route to 18.31.0.200 over a maximum of 30 hops

  1    14 ms    12 ms    13 ms  134.124.204.242
  2    22 ms    16 ms    13 ms  134.124.98.250
  3    27 ms    13 ms    16 ms  mntn-sl-he0-1-1-2-0.mo.more.net [150.199.90.109]
  4    53 ms    20 ms    23 ms  mntn-ro-he0-0-1-2-0.mo.more.net [150.199.90.26]
  5    29 ms    22 ms    27 ms  mntn-kc-he0-0-1-2-0.mo.more.net [150.199.90.30]
  6    26 ms    23 ms    23 ms  150.199.90.66
  7    64 ms    50 ms    57 ms  fourhundredge-0-0-0-0.4079.core1.chic.net.internet2.edu [163.253.2.28]
  8    60 ms    50 ms    50 ms  fourhundredge-0-0-0-23.4079.core2.chic.net.internet2.edu [163.253.1.99]
  9    61 ms    52 ms    50 ms  fourhundredge-0-0-0-6.4079.core2.eqch.net.internet2.edu [163.253.2.75]
 10    55 ms    52 ms    50 ms  fourhundredge-0-0-0-0.4079.core2.clev.net.internet2.edu [163.253.2.16]
 11    54 ms    48 ms    50 ms  fourhundredge-0-0-0-1.4079.core1.alba.net.internet2.edu [163.253.1.20]
 12   490 ms    48 ms    51 ms  i2-re-chic-nox-mghpcc-gw1.nox.org [192.5.89.253]
 13   293 ms    58 ms    57 ms  192.5.89.53
 14   112 ms    57 ms    57 ms  nox1sumgw1-mit-re.nox.org [18.2.4.110]
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.

C:\Users\brwne>
```

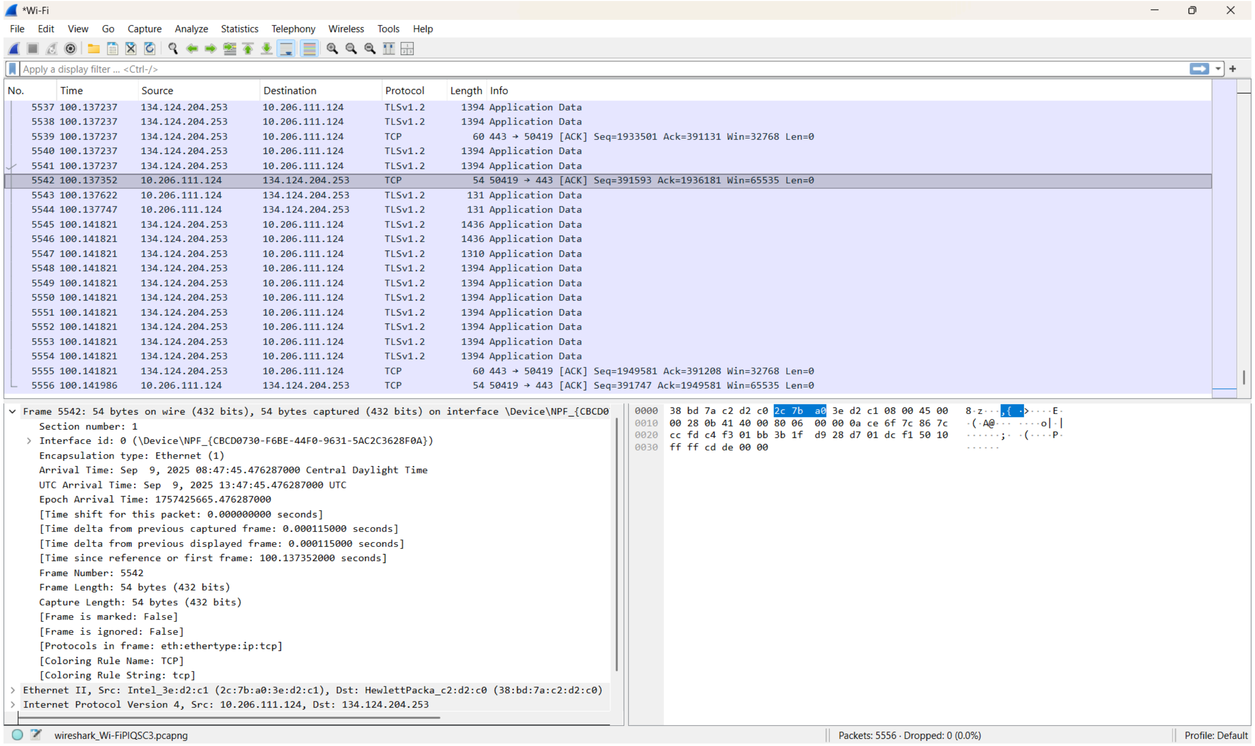
.When running tracert to the MIT server at 18.31.0.200, some hops may display asterisks (*) instead of times. These asterisks indicate that the probe packets did not receive a reply within the timeout period. This usually happens because certain routers are configured to block or rate-limit ICMP Time Exceeded messages, or because of temporary congestion or packet loss along the path. Even though asterisks appear, the trace may still continue successfully to later hops and ultimately reach the destination.

G. I am using UMSL's VPN at the moment so the packet begins in the Missouri Research and Education Network (MOREnet), which provides my university's Internet access, and then transitions into the Internet2 backbone, a high-speed academic research network. Toward the end of the route, the traffic is handed off to MIT's own network through the Northern Crossroads (NOX) exchange. The change in ISPs is visible as the route shifts from MOREnet to Internet2 and finally to MIT's local network.

# Wireshark

A. I am using UMSL's VPN, so I only see two: TCP and TLSv1.2. I stopped using UMSL's VPN and now I see DNS, QUIC, UDP, & IGMPv3.

B. When I select a packet in the packet-listing pane, the packet-details pane expands that packet into hierarchical protocol layers. For Frame 5542, the details pane shows the Ethernet II header, the Internet Protocol Version 4 (IPv4) header, and the Transmission Control Protocol (TCP) segment information. To the right of that, the packet-contents pane displays the same packet in raw form: hexadecimal values on the left and their ASCII representations on the right. The final encapsulation layer of the message being sent on the physical/wireless media is Ethernet II.

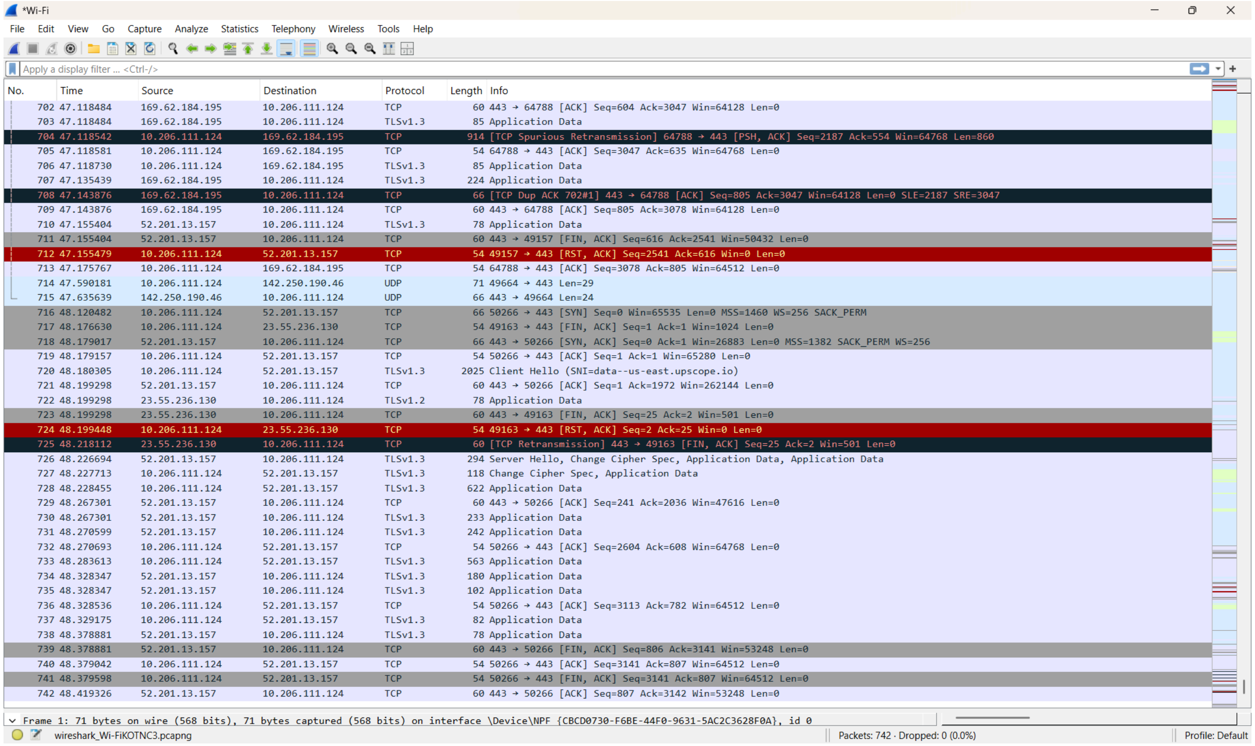

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 5537 | 100.137237 | 134.124.204.253 | 10.206.111.124 | TLSv1.2 | 1394 | Application Data |
| 5538 | 100.137237 | 134.124.204.253 | 10.206.111.124 | TLSv1.2 | 1394 | Application Data |
| 5539 | 100.137237 | 134.124.204.253 | 10.206.111.124 | TCP | 60 | 443 → 50419 [ACK] Seq=1933501 Ack=391131 Win=32768 Len=0 |
| 5540 | 100.137237 | 134.124.204.253 | 10.206.111.124 | TLSv1.2 | 1394 | Application Data |
| 5541 | 100.137237 | 134.124.204.253 | 10.206.111.124 | TLSv1.2 | 1394 | Application Data |
| 5542 | 100.137352 | 10.206.111.124 | 134.124.204.253 | TCP | 54 | 50419 → 443 [ACK] Seq=391593 Ack=1936181 Win=65535 Len=0 |
| 5543 | 100.137622 | 10.206.111.124 | 134.124.204.253 | TLSv1.2 | 131 | Application Data |
| 5544 | 100.137747 | 10.206.111.124 | 134.124.204.253 | TLSv1.2 | 131 | Application Data |
| 5545 | 100.141821 | 134.124.204.253 | 10.206.111.124 | TLSv1.2 | 1436 | Application Data |
| 5546 | 100.141821 | 134.124.204.253 | 10.206.111.124 | TLSv1.2 | 1436 | Application Data |
| 5547 | 100.141821 | 134.124.204.253 | 10.206.111.124 | TLSv1.2 | 1310 | Application Data |
| 5548 | 100.141821 | 134.124.204.253 | 10.206.111.124 | TLSv1.2 | 1394 | Application Data |
| 5549 | 100.141821 | 134.124.204.253 | 10.206.111.124 | TLSv1.2 | 1394 | Application Data |
| 5550 | 100.141821 | 134.124.204.253 | 10.206.111.124 | TLSv1.2 | 1394 | Application Data |
| 5551 | 100.141821 | 134.124.204.253 | 10.206.111.124 | TLSv1.2 | 1394 | Application Data |
| 5552 | 100.141821 | 134.124.204.253 | 10.206.111.124 | TLSv1.2 | 1394 | Application Data |
| 5553 | 100.141821 | 134.124.204.253 | 10.206.111.124 | TLSv1.2 | 1394 | Application Data |
| 5554 | 100.141821 | 134.124.204.253 | 10.206.111.124 | TLSv1.2 | 1394 | Application Data |
| 5555 | 100.141821 | 134.124.204.253 | 10.206.111.124 | TCP | 60 | 443 → 50419 [ACK] Seq=1949581 Ack=391208 Win=32768 Len=0 |
| 5556 | 100.141986 | 10.206.111.124 | 134.124.204.253 | TCP | 54 | 50419 → 443 [ACK] Seq=391747 Ack=1949581 Win=65535 Len=0 |

```
v Frame 5542: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{CBCD0
    Section number: 1
  > Interface id: 0 (\Device\NPF_{CBCD0730-F6BE-44F0-9631-5AC2C3628F0A})
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep  9, 2025 08:47:45.476287000 Central Daylight Time
    UTC Arrival Time: Sep  9, 2025 13:47:45.476287000 UTC
    Epoch Arrival Time: 1757425665.476287000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000115000 seconds]
    [Time delta from previous displayed frame: 0.000115000 seconds]
    [Time since reference or first frame: 100.137352000 seconds]
    Frame Number: 5542
    Frame Length: 54 bytes (432 bits)
    Capture Length: 54 bytes (432 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
> Ethernet II, Src: Intel_3e:d2:c1 (2c:7b:a0:3e:d2:c1), Dst: HewlettPacka_c2:d2:c0 (38:bd:7a:c2:d2:c0)
> Internet Protocol Version 4, Src: 10.206.111.124, Dst: 134.124.204.253
```

```
0000  38 bd 7a c2 d2 c0 2c 7b  a0 3e d2 c1 08 00 45 00   8·z···,{ ·>····E·
0010  00 28 0b 41 40 00 80 06  00 00 0a ce 6f 7c 86 7c   ·(·A@··· ····o|·|
0020  cc fd c4 f3 01 bb 3b 1f  d9 28 d7 01 dc f1 50 10   ······;· ·(····P·
0030  ff ff cd de 00 00                                  ······
```

wireshark_Wi-FiPIQSC3.pcapng
Packets: 5556 · Dropped: 0 (0.0%)
Profile: Default


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source          Destination     Protocol  Length Info
 702 47.118484  169.62.184.195  10.206.111.124  TCP          60 443 → 64788 [ACK] Seq=604 Ack=3047 Win=64128 Len=0
 703 47.118484  169.62.184.195  10.206.111.124  TLSv1.3      85 Application Data
 704 47.118542  10.206.111.124  169.62.184.195  TCP         914 [TCP Spurious Retransmission] 64788 → 443 [PSH, ACK] Seq=2187 Ack=554 Win=64768 Len=860
 705 47.118581  10.206.111.124  169.62.184.195  TCP          54 64788 → 443 [ACK] Seq=3047 Ack=635 Win=64768 Len=0
 706 47.118730  10.206.111.124  169.62.184.195  TLSv1.3      85 Application Data
 707 47.135439  169.62.184.195  10.206.111.124  TLSv1.3     224 Application Data
 708 47.143876  169.62.184.195  10.206.111.124  TCP          66 [TCP Dup ACK 702#1] 443 → 64788 [ACK] Seq=805 Ack=3047 Win=64128 Len=0 SLE=2187 SRE=3047
 709 47.143876  169.62.184.195  10.206.111.124  TCP          60 443 → 64788 [ACK] Seq=805 Ack=3078 Win=64128 Len=0
 710 47.155404  52.201.13.157   10.206.111.124  TLSv1.3      78 Application Data
 711 47.155404  52.201.13.157   10.206.111.124  TCP          60 443 → 49157 [FIN, ACK] Seq=616 Ack=2541 Win=50432 Len=0
 712 47.155479  10.206.111.124  52.201.13.157   TCP          54 49157 → 443 [RST, ACK] Seq=2541 Ack=616 Win=0 Len=0
 713 47.175767  10.206.111.124  169.62.184.195  TCP          54 64788 → 443 [ACK] Seq=3078 Ack=805 Win=64512 Len=0
 714 47.590181  10.206.111.124  142.250.190.46  UDP          71 49664 → 443 Len=29
 715 47.635639  142.250.190.46  10.206.111.124  UDP          66 443 → 49664 Len=24
 716 48.120482  10.206.111.124  52.201.13.157   TCP          66 50266 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 717 48.176630  10.206.111.124  23.55.236.130   TCP          54 49163 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
 718 48.179017  52.201.13.157   10.206.111.124  TCP          66 443 → 50266 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1382 SACK_PERM WS=256
 719 48.179157  10.206.111.124  52.201.13.157   TCP          54 50266 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
 720 48.180305  10.206.111.124  52.201.13.157   TLSv1.3    2025 Client Hello (SNI=data--us-east.upscope.io)
 721 48.199298  52.201.13.157   10.206.111.124  TCP          60 443 → 50266 [ACK] Seq=1 Ack=1972 Win=262144 Len=0
 722 48.199298  23.55.236.130   10.206.111.124  TLSv1.2      78 Application Data
 723 48.199298  23.55.236.130   10.206.111.124  TCP          60 443 → 49163 [FIN, ACK] Seq=25 Ack=2 Win=501 Len=0
 724 48.199448  10.206.111.124  23.55.236.130   TCP          54 49163 → 443 [RST, ACK] Seq=2 Ack=25 Win=0 Len=0
 725 48.218112  23.55.236.130   10.206.111.124  TCP          60 [TCP Retransmission] 443 → 49163 [FIN, ACK] Seq=25 Ack=2 Win=501 Len=0
 726 48.226694  52.201.13.157   10.206.111.124  TLSv1.3     294 Server Hello, Change Cipher Spec, Application Data, Application Data
 727 48.227713  10.206.111.124  52.201.13.157   TLSv1.3     118 Change Cipher Spec, Application Data
 728 48.228455  10.206.111.124  52.201.13.157   TLSv1.3     622 Application Data
 729 48.267301  52.201.13.157   10.206.111.124  TCP          60 443 → 50266 [ACK] Seq=241 Ack=2036 Win=47616 Len=0
 730 48.267301  52.201.13.157   10.206.111.124  TLSv1.3     233 Application Data
 731 48.270599  52.201.13.157   10.206.111.124  TLSv1.3     242 Application Data
 732 48.270693  10.206.111.124  52.201.13.157   TCP          54 50266 → 443 [ACK] Seq=2604 Ack=608 Win=64768 Len=0
 733 48.283613  10.206.111.124  52.201.13.157   TLSv1.3     563 Application Data
 734 48.328347  52.201.13.157   10.206.111.124  TLSv1.3     180 Application Data
 735 48.328347  52.201.13.157   10.206.111.124  TLSv1.3     102 Application Data
 736 48.328536  10.206.111.124  52.201.13.157   TCP          54 50266 → 443 [ACK] Seq=3113 Ack=782 Win=64512 Len=0
 737 48.329175  10.206.111.124  52.201.13.157   TLSv1.3      82 Application Data
 738 48.378881  52.201.13.157   10.206.111.124  TLSv1.3      78 Application Data
 739 48.378881  52.201.13.157   10.206.111.124  TCP          60 443 → 50266 [FIN, ACK] Seq=806 Ack=3141 Win=53248 Len=0
 740 48.379042  10.206.111.124  52.201.13.157   TCP          54 50266 → 443 [ACK] Seq=3141 Ack=807 Win=64512 Len=0
 741 48.379598  10.206.111.124  52.201.13.157   TCP          54 50266 → 443 [FIN, ACK] Seq=3141 Ack=807 Win=64512 Len=0
 742 48.419326  52.201.13.157   10.206.111.124  TCP          60 443 → 50266 [ACK] Seq=807 Ack=3142 Win=53248 Len=0

> Frame 1: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{CBCD0730-F6BE-44F0-9631-5AC2C3628F0A}, id 0
wireshark_Wi-FiKOTNC3.pcapng          Packets: 742 · Dropped: 0 (0.0%)          Profile: Default
```

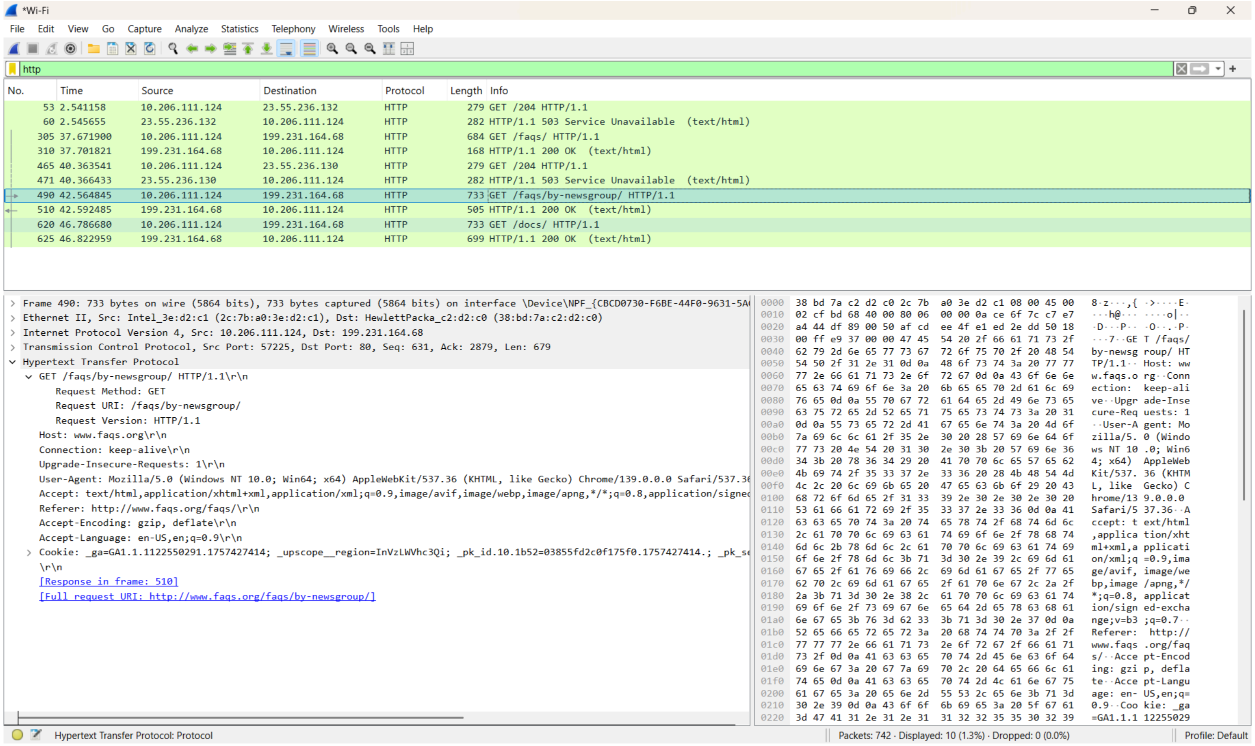
C.

i. GET

ii. HTTP/1.1

iii. Source Address (my computer): 10.206.111.124
Destination Address: 23.55.236.132

iv. Screenshots below of GET and OK with HTTP dropdown open


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time        Source           Destination      Protocol  Length Info
   53 2.541158    10.206.111.124   23.55.236.132    HTTP       279 GET /204 HTTP/1.1
   60 2.545655    23.55.236.132    10.206.111.124   HTTP       282 HTTP/1.1 503 Service Unavailable  (text/html)
  305 37.671900   10.206.111.124   199.231.164.68   HTTP       684 GET /faqs/ HTTP/1.1
  310 37.701821   199.231.164.68   10.206.111.124   HTTP       168 HTTP/1.1 200 OK  (text/html)
  465 40.363541   10.206.111.124   23.55.236.130    HTTP       279 GET /204 HTTP/1.1
  471 40.366433   23.55.236.130    10.206.111.124   HTTP       282 HTTP/1.1 503 Service Unavailable  (text/html)
  490 42.564845   10.206.111.124   199.231.164.68   HTTP       733 GET /faqs/by-newsgroup/ HTTP/1.1
  510 42.592485   199.231.164.68   10.206.111.124   HTTP       505 HTTP/1.1 200 OK  (text/html)
  620 46.786680   10.206.111.124   199.231.164.68   HTTP       733 GET /docs/ HTTP/1.1
  625 46.822959   199.231.164.68   10.206.111.124   HTTP       699 HTTP/1.1 200 OK  (text/html)
```

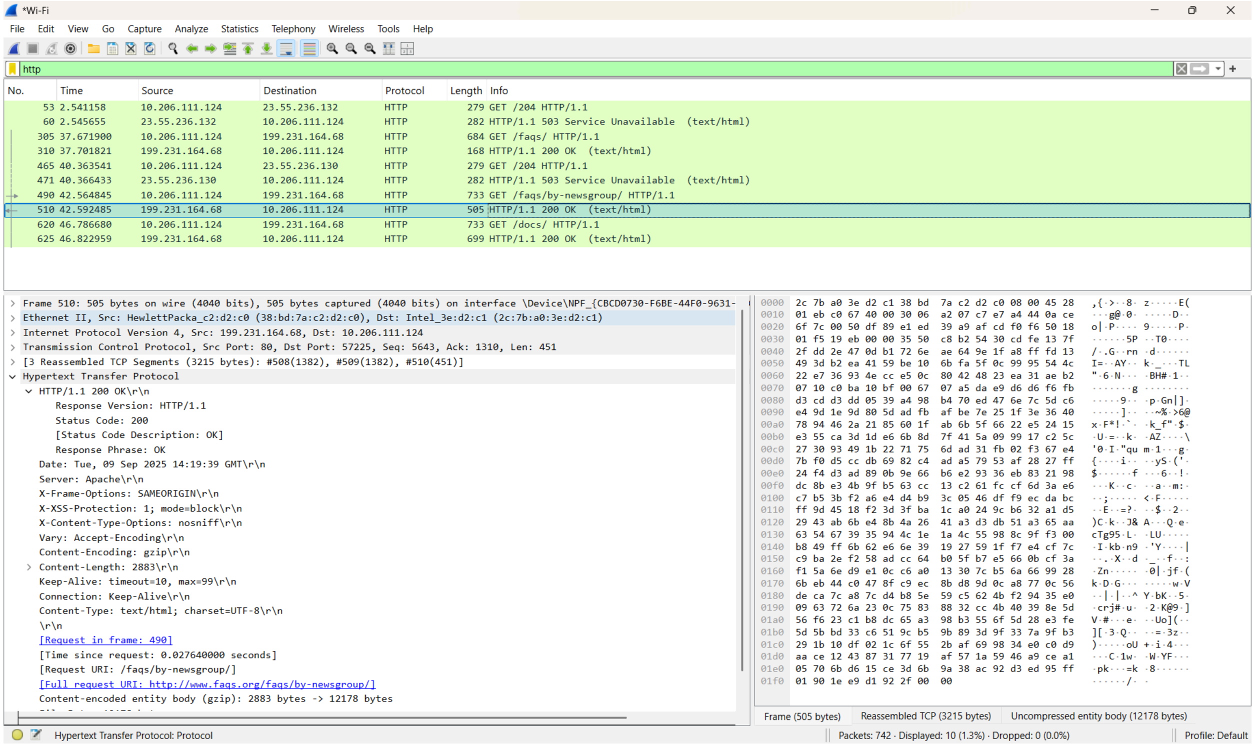
```
> Frame 490: 733 bytes on wire (5864 bits), 733 bytes captured (5864 bits) on interface \Device\NPF_{CBCD0730-F6BE-44F0-9631-5A
> Ethernet II, Src: Intel_3e:d2:c1 (2c:7b:a0:3e:d2:c1), Dst: HewlettPacka_c2:d2:c0 (38:bd:7a:c2:d2:c0)
> Internet Protocol Version 4, Src: 10.206.111.124, Dst: 199.231.164.68
> Transmission Control Protocol, Src Port: 57225, Dst Port: 80, Seq: 631, Ack: 2879, Len: 679
v Hypertext Transfer Protocol
  v GET /faqs/by-newsgroup/ HTTP/1.1\r\n
      Request Method: GET
      Request URI: /faqs/by-newsgroup/
      Request Version: HTTP/1.1
    Host: www.faqs.org\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed
    Referer: http://www.faqs.org/faqs/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
  > Cookie: _ga=GA1.1.1122550291.1757427414; _upscope__region=InVzLWVhc3Qi; _pk_id.10.1b52=03855fd2c0f175f0.1757427414.; _pk_se
    \r\n
    [Response in frame: 510]
    [Full request URI: http://www.faqs.org/faqs/by-newsgroup/]
```

```
0000  38 bd 7a c2 d2 c0 2c 7b  a0 3e d2 c1 08 00 45 00   8·z···,{ ·>····E·
0010  02 cf bd 68 40 00 80 06  00 00 0a ce 6f 7c c7 e7   ···h@··· ····o|··
0020  a4 44 df 89 00 50 af cd  ee 4f e1 ed 2e dd 50 18   ·D···P·· ·O···.·P·
0030  00 ff e9 37 00 00 47 45  54 20 2f 66 61 71 73 2f   ···7··GE T /faqs/
0040  62 79 2d 6e 65 77 73 67  72 6f 75 70 2f 20 48 54   by-newsg roup/ HT
0050  54 50 2f 31 2e 31 0d 0a  48 6f 73 74 3a 20 77 77   TP/1.1·· Host: ww
0060  77 2e 66 61 71 73 2e 6f  72 67 0d 0a 43 6f 6e 6e   w.faqs.o rg··Conn
0070  65 63 74 69 6f 6e 3a 20  6b 65 65 70 2d 61 6c 69   ection:  keep-ali
0080  76 65 0d 0a 55 70 67 72  61 64 65 2d 49 6e 73 65   ve··Upgr ade-Inse
0090  63 75 72 65 2d 52 65 71  75 65 73 74 73 3a 20 31   cure-Req uests: 1
00a0  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 6f   ··User-A gent: Mo
00b0  7a 69 6c 6c 61 2f 35 2e  30 20 28 57 69 6e 64 6f   zilla/5. 0 (Windo
00c0  77 73 20 4e 54 20 31 30  2e 30 3b 20 57 69 6e 36   ws NT 10 .0; Win6
00d0  34 3b 20 78 36 34 29 20  41 70 70 6c 65 57 65 62   4; x64)  AppleWeb
00e0  4b 69 74 2f 35 33 37 2e  33 36 20 28 4b 48 54 4d   Kit/537. 36 (KHTM
00f0  4c 2c 20 6c 69 6b 65 20  47 65 63 6b 6f 29 20 43   L, like  Gecko) C
0100  68 72 6f 6d 65 2f 31 33  39 2e 30 2e 30 2e 30 20   hrome/13 9.0.0.0
0110  53 61 66 61 72 69 2f 35  33 37 2e 33 36 0d 0a 41   Safari/5 37.36··A
0120  63 63 65 70 74 3a 20 74  65 78 74 2f 68 74 6d 6c   ccept: t ext/html
0130  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 68 74   ,applica tion/xht
0140  6d 6c 2b 78 6d 6c 2c 61  70 70 6c 69 63 61 74 69   ml+xml,a pplicati
0150  6f 6e 2f 78 6d 6c 3b 71  3d 30 2e 39 2c 69 6d 61   on/xml;q =0.9,ima
0160  67 65 2f 61 76 69 66 2c  69 6d 61 67 65 2f 77 65   ge/avif, image/we
0170  62 70 2c 69 6d 61 67 65  2f 61 70 6e 67 2c 2a 2f   bp,image /apng,*/
0180  2a 3b 71 3d 30 2e 38 2c  61 70 70 6c 69 63 61 74   *;q=0.8, applicat
0190  69 6f 6e 2f 73 69 67 6e  65 64 2d 65 78 63 68 61   ion/sign ed-excha
01a0  6e 67 65 3b 76 3d 62 33  3b 71 3d 30 2e 37 0d 0a   nge;v=b3 ;q=0.7··
01b0  52 65 66 65 72 65 72 3a  20 68 74 74 70 3a 2f 2f   Referer:  http://
01c0  77 77 77 2e 66 61 71 73  2e 6f 72 67 2f 66 61 71   www.faqs .org/faq
01d0  73 2f 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   s/··Acce pt-Encod
01e0  69 6e 67 3a 20 67 7a 69  70 2c 20 64 65 66 6c 61   ing: gzi p, defla
01f0  74 65 0d 0a 41 63 63 65  70 74 2d 4c 61 6e 67 75   te··Acce pt-Langu
0200  61 67 65 3a 20 65 6e 2d  55 53 2c 65 6e 3b 71 3d   age: en- US,en;q=
0210  30 2e 39 0d 0a 43 6f 6f  6b 69 65 3a 20 5f 67 61   0.9··Coo kie: _ga
0220  3d 47 41 31 2e 31 2e 31  31 32 32 35 35 30 32 39   =GA1.1.1 12255029
```

Hypertext Transfer Protocol: Protocol

Packets: 742 · Displayed: 10 (1.3%) · Dropped: 0 (0.0%)

Profile: Default


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time        Source           Destination      Protocol  Length Info
   53 2.541158    10.206.111.124   23.55.236.132    HTTP       279 GET /204 HTTP/1.1
   60 2.545655    23.55.236.132    10.206.111.124   HTTP       282 HTTP/1.1 503 Service Unavailable  (text/html)
  305 37.671900   10.206.111.124   199.231.164.68   HTTP       684 GET /faqs/ HTTP/1.1
  310 37.701821   199.231.164.68   10.206.111.124   HTTP       168 HTTP/1.1 200 OK  (text/html)
  465 40.363541   10.206.111.124   23.55.236.130    HTTP       279 GET /204 HTTP/1.1
  471 40.366433   23.55.236.130    10.206.111.124   HTTP       282 HTTP/1.1 503 Service Unavailable  (text/html)
  490 42.564845   10.206.111.124   199.231.164.68   HTTP       733 GET /faqs/by-newsgroup/ HTTP/1.1
  510 42.592485   199.231.164.68   10.206.111.124   HTTP       505 HTTP/1.1 200 OK  (text/html)
  620 46.786680   10.206.111.124   199.231.164.68   HTTP       733 GET /docs/ HTTP/1.1
  625 46.822959   199.231.164.68   10.206.111.124   HTTP       699 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 510: 505 bytes on wire (4040 bits), 505 bytes captured (4040 bits) on interface \Device\NPF_{CBCD0730-F6BE-44F0-9631-
> Ethernet II, Src: HewlettPacka_c2:d2:c0 (38:bd:7a:c2:d2:c0), Dst: Intel_3e:d2:c1 (2c:7b:a0:3e:d2:c1)
> Internet Protocol Version 4, Src: 199.231.164.68, Dst: 10.206.111.124
> Transmission Control Protocol, Src Port: 80, Dst Port: 57225, Seq: 5643, Ack: 1310, Len: 451
> [3 Reassembled TCP Segments (3215 bytes): #508(1382), #509(1382), #510(451)]
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Tue, 09 Sep 2025 14:19:39 GMT\r\n
    Server: Apache\r\n
    X-Frame-Options: SAMEORIGIN\r\n
    X-XSS-Protection: 1; mode=block\r\n
    X-Content-Type-Options: nosniff\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
  > Content-Length: 2883\r\n
    Keep-Alive: timeout=10, max=99\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [Request in frame: 490]
    [Time since request: 0.027640000 seconds]
    [Request URI: /faqs/by-newsgroup/]
    [Full request URI: http://www.faqs.org/faqs/by-newsgroup/]
    Content-encoded entity body (gzip): 2883 bytes -> 12178 bytes
```

```
0000  2c 7b a0 3e d2 c1 38 bd  7a c2 d2 c0 08 00 45 28   ,{·>··8· z·····E(
0010  01 eb c0 67 40 00 30 06  a2 07 c7 e7 a4 44 0a ce   ···g@·0· ·····D··
0020  6f 7c 00 50 df 89 e1 ed  39 a9 af cd f0 f6 50 18   o|·P···· 9·····P·
0030  01 f5 19 eb 00 00 35 50  c8 b2 54 30 cd fe 13 7f   ······5P ··T0····
0040  2f dd 2e 47 0d b1 72 6e  ae 64 9e 1f a8 ff fd 13   /·.G··rn ·d······
0050  49 3d b2 ea 41 59 be 10  6b fa 5f 0c 99 95 54 4c   I=··AY·· k·_···TL
0060  22 e7 36 93 4e cc e5 0c  80 42 48 23 ea 31 ae b2   "·6·N··· ·BH#·1··
0070  07 10 c0 ba 10 bf 00 67  07 a5 da e9 d6 d6 f6 fb   ·······g ········
0080  d3 cd d3 dd 05 39 a4 98  b4 70 ed 47 6e 7c 5d c6   ·····9·· ·p·Gn|]·
0090  e4 9d 1e 9d 80 5d ad fb  af be 7e 25 1f 3e 36 40   ·····]·· ··~%·>6@
00a0  78 94 46 2a 21 85 60 1f  ab 6b 5f 66 22 e5 24 15   x·F*!·`· ·k_f"·$·
00b0  e3 55 ca 3d 1d e6 6b 8d  7f 41 5a 09 99 17 c2 5c   ·U·=··k· ·AZ····\
00c0  27 30 93 49 1b 22 71 75  6d ad 31 fb 02 f3 67 e4   '0·I·"qu m·1···g·
00d0  7b f0 d5 cc db 69 82 c4  ad a5 79 53 af 28 27 ff   {····i·· ··yS·('·
00e0  24 f4 d3 ad 89 0b 9e 66  b6 e2 93 36 eb 83 21 98   $······f ···6··!·
00f0  dc 8b e3 4b 9f b5 63 cc  13 c2 61 fc cf 6d 3a e6   ···K··c· ··a··m:·
0100  c7 b5 3b f2 a6 e4 d4 b9  3c 05 46 df f9 ec da bc   ··;····· <·F·····
0110  ff 9d 45 18 f2 3d 3f ba  1c a0 24 9c b6 32 a1 d5   ··E··=?· ··$··2··
0120  29 43 ab 6b e4 8b 4a 26  41 a3 d3 db 51 a3 65 aa   )C·k··J& A···Q·e·
0130  63 54 67 39 35 94 4c 1e  1a 4c 55 98 8c 9f f3 00   cTg95·L· ·LU·····
0140  b8 49 ff 6b 62 e6 6e 39  19 27 59 1f f7 e4 cf 7c   ·I·kb·n9 ·'Y····|
0150  c9 ba 2e f2 58 ad cc 64  b0 5f b7 e5 66 0b cf 3a   ··.·X··d ·_··f··:
0160  f1 5a 6e d9 e1 0c c6 a0  13 30 7c b5 6a 66 99 28   ·Zn····· ·0|·jf·(
0170  6b eb 44 c0 47 8f c9 ec  8b d8 9d 0c a8 77 0c 56   k·D·G··· ·····w·V
0180  de ca 7c a8 7c d4 b8 5e  59 c5 62 4b f2 94 35 e0   ··|·|··^ Y·bK··5·
0190  09 63 72 6a 23 0c 75 83  88 32 cc 4b 40 39 8e 5d   ·crj#·u· ·2·K@9·]
01a0  56 f6 23 c1 b8 dc 65 a3  98 b3 55 6f 5d 28 e3 fe   V·#···e· ··Uo](··
01b0  5d 5b bd 33 c6 51 9c b5  9b 89 3d 9f 33 7a 9f b3   ][·3·Q·· ··=·3z··
01c0  29 1b 10 df 02 1c 6f 55  2b af 69 98 34 e0 c0 d9   )·····oU +·i·4···
01d0  aa ce 12 43 87 31 77 19  af 57 1a 59 46 a9 ce a1   ···C·1w· ·W·YF···
01e0  05 70 6b d6 15 ce 3d 6b  9a 38 ac 92 d3 ed 95 ff   ·pk···=k ·8······
01f0  01 90 1e e9 d1 92 2f 00  00                        ······/· ·
```

Frame (505 bytes) | Reassembled TCP (3215 bytes) | Uncompressed entity body (12178 bytes)

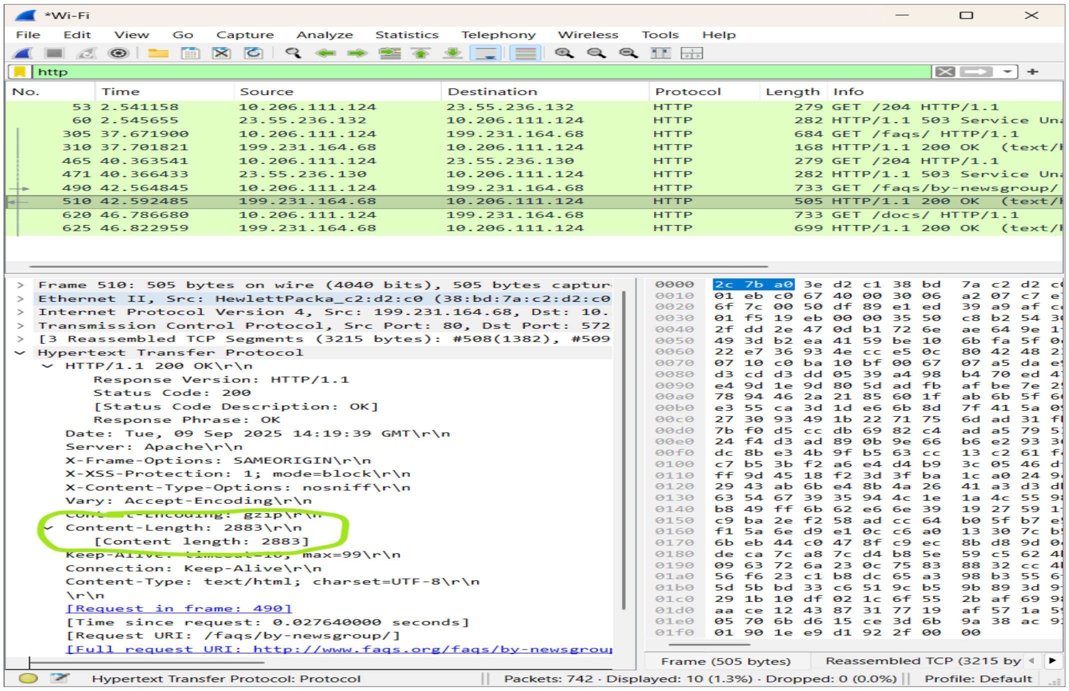
Hypertext Transfer Protocol: Protocol

Packets: 742 · Displayed: 10 (1.3%) · Dropped: 0 (0.0%)

Profile: Default

v) Packet 53 (GET): time = 2.541158
Packet 305 (HTTP/1.1 200 OK): time = 37.671998
37.671998 – 2.541158 = 35.13084 seconds

vi) Content lengths vary by 200 OK response but the specific one I am looking at is: 2883 bytes.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.    Time       Source           Destination      Protocol  Length Info
    53 2.541158   10.206.111.124   23.55.236.132    HTTP         279 GET /204 HTTP/1.1
    60 2.545655   23.55.236.132    10.206.111.124   HTTP         282 HTTP/1.1 503 Service Un
   305 37.671900  10.206.111.124   199.231.164.68   HTTP         684 GET /faqs/ HTTP/1.1
   310 37.701821  199.231.164.68   10.206.111.124   HTTP         168 HTTP/1.1 200 OK  (text/
   465 40.363541  10.206.111.124   23.55.236.130    HTTP         279 GET /204 HTTP/1.1
   471 40.366433  23.55.236.130    10.206.111.124   HTTP         282 HTTP/1.1 503 Service Un
   490 42.564845  10.206.111.124   199.231.164.68   HTTP         733 GET /faqs/by-newsgroup/
   510 42.592485  199.231.164.68   10.206.111.124   HTTP         505 HTTP/1.1 200 OK  (text/
   620 46.786680  10.206.111.124   199.231.164.68   HTTP         733 GET /docs/ HTTP/1.1
   625 46.822959  199.231.164.68   10.206.111.124   HTTP         699 HTTP/1.1 200 OK  (text/
```

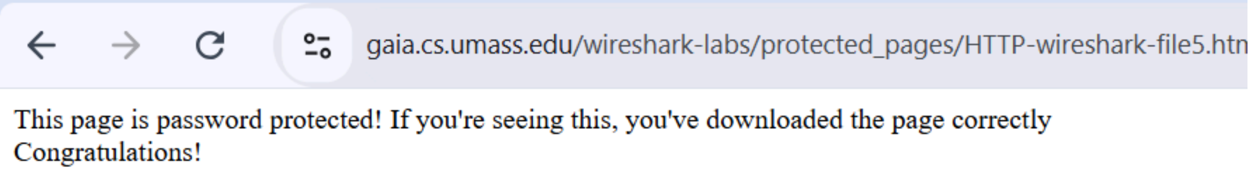
```
> Frame 510: 505 bytes on wire (4040 bits), 505 bytes captur
> Ethernet II, Src: HewlettPacka_c2:d2:c0 (38:bd:7a:c2:d2:c0
> Internet Protocol Version 4, Src: 199.231.164.68, Dst: 10.
> Transmission Control Protocol, Src Port: 80, Dst Port: 572
> [3 Reassembled TCP Segments (3215 bytes): #508(1382), #509
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Tue, 09 Sep 2025 14:19:39 GMT\r\n
    Server: Apache\r\n
    X-Frame-Options: SAMEORIGIN\r\n
    X-XSS-Protection: 1; mode=block\r\n
    X-Content-Type-Options: nosniff\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
  v Content-Length: 2883\r\n
        [Content length: 2883]
    Keep-Alive: timeout=10, max=99\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [Request in frame: 490]
    [Time since request: 0.027640000 seconds]
    [Request URI: /faqs/by-newsgroup/]
    [Full request URI: http://www.faqs.org/faqs/by-newsgrou
```

```
0000  2c 7b a0 3e d2 c1 38 bd  7a c2 d2
0010  01 eb c0 67 40 00 30 06  a2 07 c7
0020  6f 7c 00 50 df 89 e1 ed  39 a9 af
0030  01 f5 19 eb 00 00 35 50  c8 b2 54
0040  2f dd 2e 47 0d b1 72 6e  ae 64 9e
0050  49 3d b2 ea 41 59 be 10  6b fa 5f
0060  22 e7 36 93 4e cc e5 0c  80 42 48
0070  07 10 c0 ba 10 bf 00 67  07 a5 da
0080  d3 cd d3 dd 05 39 a4 98  b4 70 ed
0090  e4 9d 1e 9d 80 5d ad fb  af be 7e
00a0  78 94 46 2a 21 85 60 1f  ab 6b 5f
00b0  e3 55 ca 3d 1d e6 6b 8d  7f 41 5a
00c0  27 30 93 49 1b 22 71 75  6d ad 31
00d0  7b f0 d5 cc db 69 82 c4  ad a5 79
00e0  24 f4 d3 ad 89 0b 9e 66  b6 e2 93
00f0  dc 8b e3 4b 9f b5 63 cc  13 c2 61
0100  c7 b5 3b f2 a6 e4 d4 b9  3c 05 46
0110  ff 9d 45 18 f2 3d 3f ba  1c a0 24
0120  29 43 ab 6b e4 8b 4a 26  41 a3 d3
0130  63 54 67 39 35 94 4c 1e  1a 4c 55
0140  b8 49 ff 6b 62 e6 6e 39  19 27 59
0150  c9 ba 2e f2 58 ad cc 64  b0 5f b7
0160  f1 5a 6e d9 e1 0c c6 a0  13 30 7c
0170  6b eb 44 c0 47 8f c9 ec  8b d8 9d
0180  de ca 7c a8 7c d4 b8 5e  59 c5 62
0190  09 63 72 6a 23 0c 75 83  88 32 cc
01a0  56 f6 23 c1 b8 dc 65 a3  98 b3 55
01b0  5d 5b bd 33 c6 51 9c b5  9b 89 3d
01c0  29 1b 10 df 02 1c 6f 55  2b af 69
01d0  aa ce 12 43 87 31 77 19  af 57 1a
01e0  05 70 6b d6 15 ce 3d 6b  9a 38 ac
01f0  01 90 1e e9 d1 92 2f 00  00
```

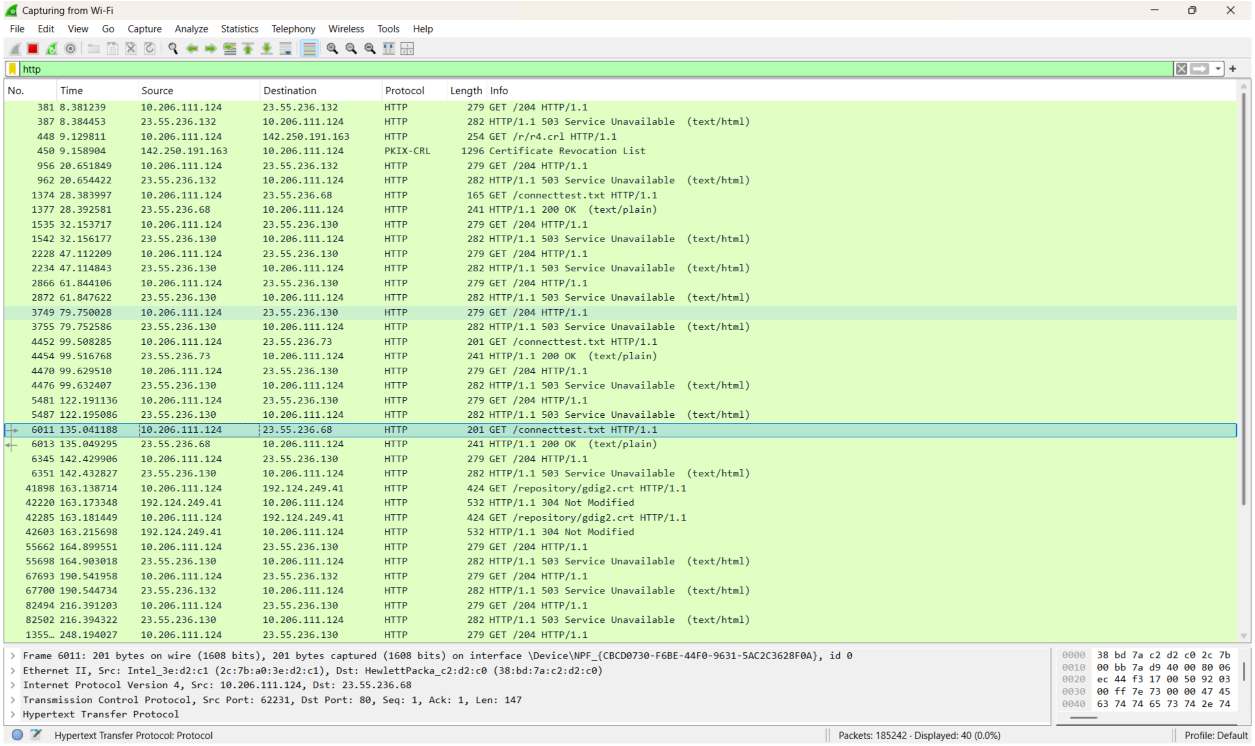
Hypertext Transfer Protocol: Protocol || Packets: 742 · Displayed: 10 (1.3%) · Dropped: 0 (0.0%) || Profile: Default

Part B: HTTP Authentication

1. HTTP/1.1 503 Service Unavailable
2. I am not sure (I don’t think I am seeing what I am supposed to see)
3. The Authorization: Basic value decodes to wireshark-students:network (format is username:password). Basic authentication over HTTP is not encrypted; the credentials are merely Base64-encoded. Anyone sniffing the network can recover the username and password (as Wireshark just did). Basic auth should only be used over HTTPS (so TLS encrypts the headers) or replaced with stronger schemes.


gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.htm

This page is password protected! If you're seeing this, you've downloaded the page correctly
Congratulations!



http

```
No.    Time        Source           Destination      Protocol  Length Info
  381 8.381239    10.206.111.124   23.55.236.132    HTTP       279 GET /204 HTTP/1.1
  387 8.384453    23.55.236.132    10.206.111.124   HTTP       282 HTTP/1.1 503 Service Unavailable  (text/html)
  448 9.129811    10.206.111.124   142.250.191.163  HTTP       254 GET /r/r4.crl HTTP/1.1
  450 9.158904    142.250.191.163  10.206.111.124   PKIX-CRL  1296 Certificate Revocation List
  956 20.651849   10.206.111.124   23.55.236.132    HTTP       279 GET /204 HTTP/1.1
  962 20.654422   23.55.236.132    10.206.111.124   HTTP       282 HTTP/1.1 503 Service Unavailable  (text/html)
 1374 28.383997   10.206.111.124   23.55.236.68     HTTP       165 GET /connecttest.txt HTTP/1.1
 1377 28.392581   23.55.236.68     10.206.111.124   HTTP       241 HTTP/1.1 200 OK  (text/plain)
 1535 32.153717   10.206.111.124   23.55.236.130    HTTP       279 GET /204 HTTP/1.1
 1542 32.156177   23.55.236.130    10.206.111.124   HTTP       282 HTTP/1.1 503 Service Unavailable  (text/html)
 2228 47.112209   10.206.111.124   23.55.236.130    HTTP       279 GET /204 HTTP/1.1
 2234 47.114843   23.55.236.130    10.206.111.124   HTTP       282 HTTP/1.1 503 Service Unavailable  (text/html)
 2866 61.844106   10.206.111.124   23.55.236.130    HTTP       279 GET /204 HTTP/1.1
 2872 61.847622   23.55.236.130    10.206.111.124   HTTP       282 HTTP/1.1 503 Service Unavailable  (text/html)
 3749 79.750028   10.206.111.124   23.55.236.130    HTTP       279 GET /204 HTTP/1.1
 3755 79.752586   23.55.236.130    10.206.111.124   HTTP       282 HTTP/1.1 503 Service Unavailable  (text/html)
 4452 99.508285   10.206.111.124   23.55.236.73     HTTP       201 GET /connecttest.txt HTTP/1.1
 4454 99.516768   23.55.236.73     10.206.111.124   HTTP       241 HTTP/1.1 200 OK  (text/plain)
 4470 99.629510   10.206.111.124   23.55.236.130    HTTP       279 GET /204 HTTP/1.1
 4476 99.632407   23.55.236.130    10.206.111.124   HTTP       282 HTTP/1.1 503 Service Unavailable  (text/html)
 5481 122.191136  10.206.111.124   23.55.236.130    HTTP       279 GET /204 HTTP/1.1
 5487 122.195086  23.55.236.130    10.206.111.124   HTTP       282 HTTP/1.1 503 Service Unavailable  (text/html)
 6011 135.041188  10.206.111.124   23.55.236.68     HTTP       201 GET /connecttest.txt HTTP/1.1
 6013 135.049295  23.55.236.68     10.206.111.124   HTTP       241 HTTP/1.1 200 OK  (text/plain)
 6345 142.429906  10.206.111.124   23.55.236.130    HTTP       279 GET /204 HTTP/1.1
 6351 142.432827  23.55.236.130    10.206.111.124   HTTP       282 HTTP/1.1 503 Service Unavailable  (text/html)
41898 163.138714  10.206.111.124   192.124.249.41   HTTP       424 GET /repository/gdig2.crt HTTP/1.1
42220 163.173348  192.124.249.41   10.206.111.124   HTTP       532 HTTP/1.1 304 Not Modified
42285 163.181449  10.206.111.124   192.124.249.41   HTTP       424 GET /repository/gdig2.crt HTTP/1.1
42603 163.215698  192.124.249.41   10.206.111.124   HTTP       532 HTTP/1.1 304 Not Modified
55662 164.899551  10.206.111.124   23.55.236.130    HTTP       279 GET /204 HTTP/1.1
55698 164.903018  23.55.236.130    10.206.111.124   HTTP       282 HTTP/1.1 503 Service Unavailable  (text/html)
67693 190.541958  10.206.111.124   23.55.236.132    HTTP       279 GET /204 HTTP/1.1
67700 190.544734  23.55.236.132    10.206.111.124   HTTP       282 HTTP/1.1 503 Service Unavailable  (text/html)
82494 216.391203  10.206.111.124   23.55.236.130    HTTP       279 GET /204 HTTP/1.1
82502 216.394322  23.55.236.130    10.206.111.124   HTTP       282 HTTP/1.1 503 Service Unavailable  (text/html)
1355… 248.194027  10.206.111.124   23.55.236.130    HTTP       279 GET /204 HTTP/1.1
```

```
> Frame 6011: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits) on interface \Device\NPF_{CBCD0730-F6BE-44F0-9631-5AC2C3628F0A}, id 0
> Ethernet II, Src: Intel_3e:d2:c1 (2c:7b:a0:3e:d2:c1), Dst: HewlettPacka_c2:d2:c0 (38:bd:7a:c2:d2:c0)
> Internet Protocol Version 4, Src: 10.206.111.124, Dst: 23.55.236.68
> Transmission Control Protocol, Src Port: 62231, Dst Port: 80, Seq: 1, Ack: 1, Len: 147
> Hypertext Transfer Protocol
```

```
0000  38 bd 7a c2 d2 c0 2c 7b
0010  00 bb 7a d9 40 00 80 06
0020  ec 44 f3 17 00 50 92 03
0030  00 ff 7e 73 00 00 47 45
0040  63 74 74 65 73 74 2e 74
```

Hypertext Transfer Protocol: Protocol

Packets: 185242 · Displayed: 40 (0.0%)

Profile: Default