Project 1

Wireshark Lab: Ethernet

Puja Shah

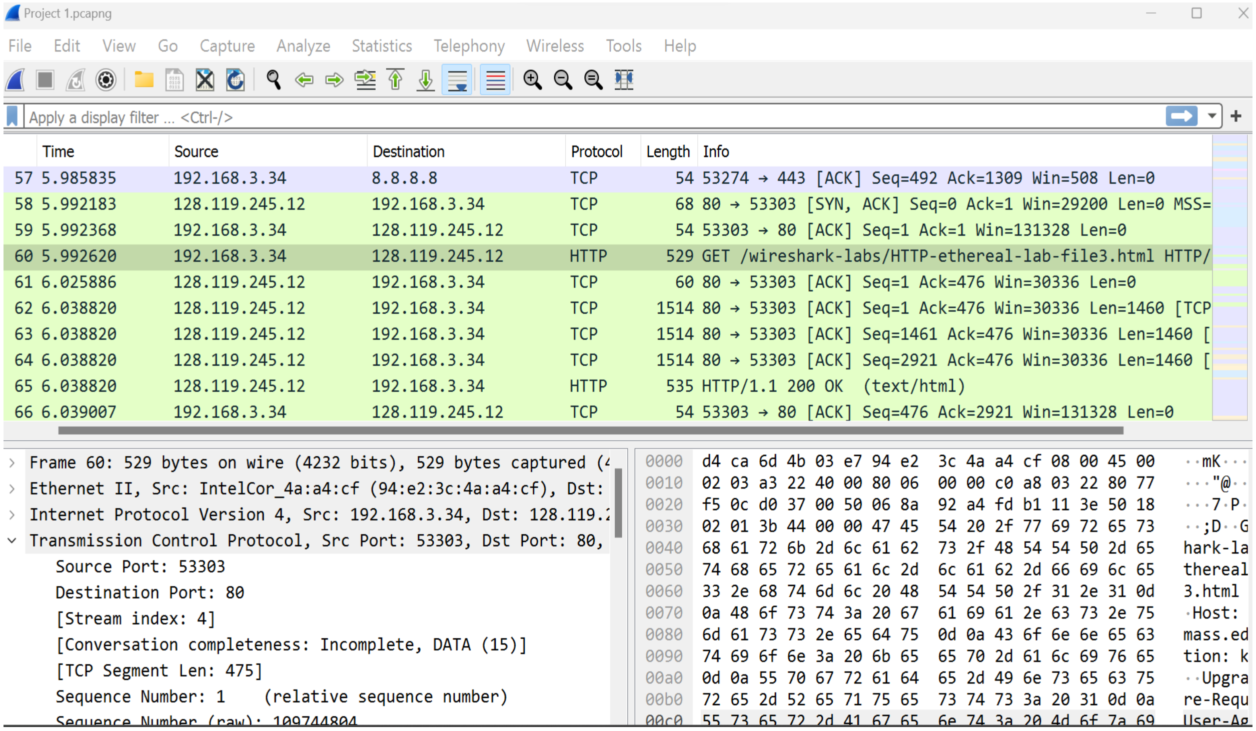
CSIT-340-11 Computer Networks

Summer 2023

Dr. Murtadha Aldeer

Capturing and analyzing ethernet frames:

In my test, the HTTP GET request is at packet 60.

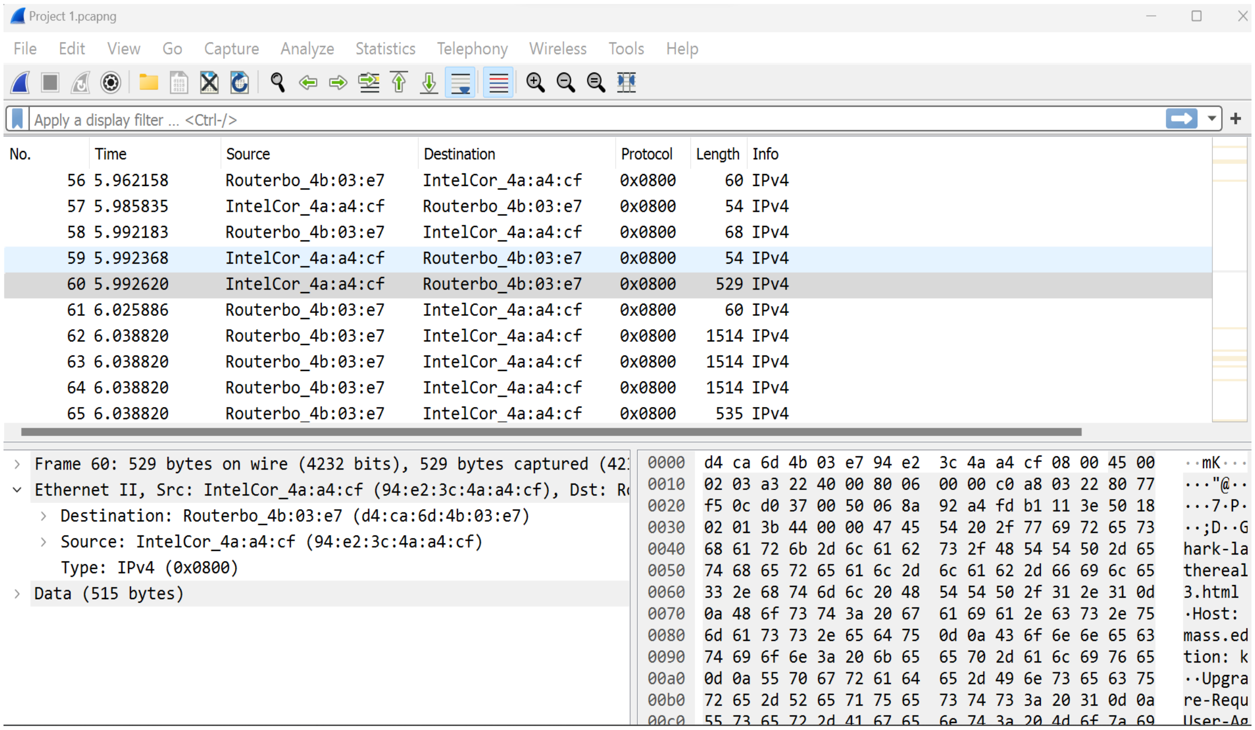

Project 1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
   Time        Source            Destination      Protocol  Length Info
57 5.985835    192.168.3.34      8.8.8.8          TCP        54 53274 → 443 [ACK] Seq=492 Ack=1309 Win=508 Len=0
58 5.992183    128.119.245.12    192.168.3.34     TCP        68 80 → 53303 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=
59 5.992368    192.168.3.34      128.119.245.12   TCP        54 53303 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
60 5.992620    192.168.3.34      128.119.245.12   HTTP      529 GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/
61 6.025886    128.119.245.12    192.168.3.34     TCP        60 80 → 53303 [ACK] Seq=1 Ack=476 Win=30336 Len=0
62 6.038820    128.119.245.12    192.168.3.34     TCP      1514 80 → 53303 [ACK] Seq=1 Ack=476 Win=30336 Len=1460 [TCP
63 6.038820    128.119.245.12    192.168.3.34     TCP      1514 80 → 53303 [ACK] Seq=1461 Ack=476 Win=30336 Len=1460 [
64 6.038820    128.119.245.12    192.168.3.34     TCP      1514 80 → 53303 [ACK] Seq=2921 Ack=476 Win=30336 Len=1460 [
65 6.038820    128.119.245.12    192.168.3.34     HTTP      535 HTTP/1.1 200 OK  (text/html)
66 6.039007    192.168.3.34      128.119.245.12   TCP        54 53303 → 80 [ACK] Seq=476 Ack=2921 Win=131328 Len=0
```

```
> Frame 60: 529 bytes on wire (4232 bits), 529 bytes captured (4
> Ethernet II, Src: IntelCor_4a:a4:cf (94:e2:3c:4a:a4:cf), Dst:
> Internet Protocol Version 4, Src: 192.168.3.34, Dst: 128.119.2
v Transmission Control Protocol, Src Port: 53303, Dst Port: 80,
    Source Port: 53303
    Destination Port: 80
    [Stream index: 4]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 475]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 109744804
```

```
0000  d4 ca 6d 4b 03 e7 94 e2  3c 4a a4 cf 08 00 45 00   ··mK···
0010  02 03 a3 22 40 00 80 06  00 00 c0 a8 03 22 80 77   ···"@··
0020  f5 0c d0 37 00 50 06 8a  92 a4 fd b1 11 3e 50 18   ···7·P·
0030  02 01 3b 44 00 00 47 45  54 20 2f 77 69 72 65 73   ··;D··G
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 65   hark-la
0050  74 68 65 72 65 61 6c 2d  6c 61 62 2d 66 69 6c 65   thereal
0060  33 2e 68 74 6d 6c 20 48  54 54 50 2f 31 2e 31 0d   3.html
0070  0a 48 6f 73 74 3a 20 67  61 69 61 2e 63 73 2e 75   ·Host:
0080  6d 61 73 73 2e 65 64 75  0d 0a 43 6f 6e 6e 65 63   mass.ed
0090  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: k
00a0  0d 0a 55 70 67 72 61 64  65 2d 49 6e 73 65 63 75   ··Upgra
00b0  72 65 2d 52 65 71 75 65  73 74 73 3a 20 31 0d 0a   re-Requ
00c0  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 69   User-Ag
```

Wireshark without IP analysis:


Project 1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source               Destination          Protocol  Length Info
   56 5.962158    Routerbo_4b:03:e7    IntelCor_4a:a4:cf    0x0800      60 IPv4
   57 5.985835    IntelCor_4a:a4:cf    Routerbo_4b:03:e7    0x0800      54 IPv4
   58 5.992183    Routerbo_4b:03:e7    IntelCor_4a:a4:cf    0x0800      68 IPv4
   59 5.992368    IntelCor_4a:a4:cf    Routerbo_4b:03:e7    0x0800      54 IPv4
   60 5.992620    IntelCor_4a:a4:cf    Routerbo_4b:03:e7    0x0800     529 IPv4
   61 6.025886    Routerbo_4b:03:e7    IntelCor_4a:a4:cf    0x0800      60 IPv4
   62 6.038820    Routerbo_4b:03:e7    IntelCor_4a:a4:cf    0x0800    1514 IPv4
   63 6.038820    Routerbo_4b:03:e7    IntelCor_4a:a4:cf    0x0800    1514 IPv4
   64 6.038820    Routerbo_4b:03:e7    IntelCor_4a:a4:cf    0x0800    1514 IPv4
   65 6.038820    Routerbo_4b:03:e7    IntelCor_4a:a4:cf    0x0800     535 IPv4
```

```
> Frame 60: 529 bytes on wire (4232 bits), 529 bytes captured (42
v Ethernet II, Src: IntelCor_4a:a4:cf (94:e2:3c:4a:a4:cf), Dst: Ro
  > Destination: Routerbo_4b:03:e7 (d4:ca:6d:4b:03:e7)
  > Source: IntelCor_4a:a4:cf (94:e2:3c:4a:a4:cf)
    Type: IPv4 (0x0800)
> Data (515 bytes)
```

```
0000  d4 ca 6d 4b 03 e7 94 e2  3c 4a a4 cf 08 00 45 00   ··mK···
0010  02 03 a3 22 40 00 80 06  00 00 c0 a8 03 22 80 77   ···"@··
0020  f5 0c d0 37 00 50 06 8a  92 a4 fd b1 11 3e 50 18   ···7·P·
0030  02 01 3b 44 00 00 47 45  54 20 2f 77 69 72 65 73   ··;D··G
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 65   hark-la
0050  74 68 65 72 65 61 6c 2d  6c 61 62 2d 66 69 6c 65   thereal
0060  33 2e 68 74 6d 6c 20 48  54 54 50 2f 31 2e 31 0d   3.html
0070  0a 48 6f 73 74 3a 20 67  61 69 61 2e 63 73 2e 75   ·Host:
0080  6d 61 73 73 2e 65 64 75  0d 0a 43 6f 6e 6e 65 63   mass.ed
0090  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: k
00a0  0d 0a 55 70 67 72 61 64  65 2d 49 6e 73 65 63 75   ··Upgra
00b0  72 65 2d 52 65 71 75 65  73 74 73 3a 20 31 0d 0a   re-Requ
00c0  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 69   User-Ag
```

1. **What is the 48-bit Ethernet address of your computer?**

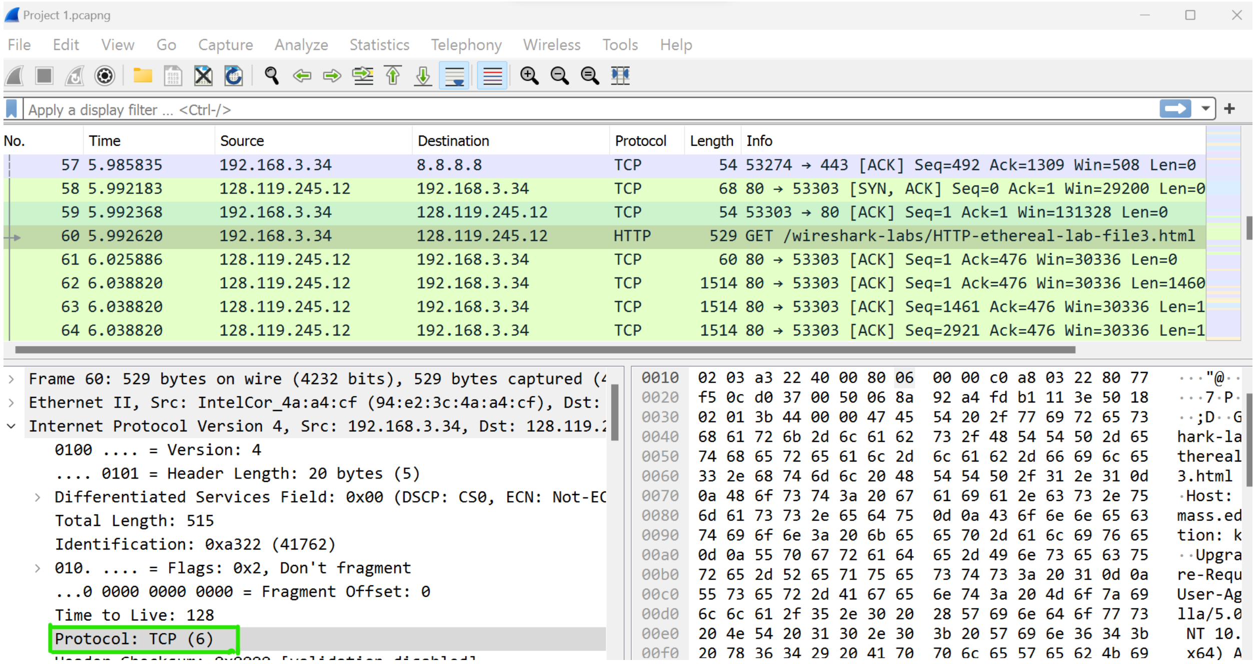
   The 48-bit Ethernet address of my computer is 94:e2:3c:4a:a4:cf

2. **What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]**

   The 48-bit destination address is d4:ca:6d:4b:03:e7. This is not the Ethernet address of gaia.cs.umass.edu.Rather, it is the Ethernet address of the router to which my computer is connected.

3. **Which transport protocol is used between your machine and the web server?**

   The Transmission Control Protocol (TCP) was used between my machine and the web server.



```
No.   Time      Source          Destination     Protocol Length Info
   57 5.985835  192.168.3.34    8.8.8.8         TCP        54 53274 → 443 [ACK] Seq=492 Ack=1309 Win=508 Len=0
   58 5.992183  128.119.245.12  192.168.3.34    TCP        68 80 → 53303 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
   59 5.992368  192.168.3.34    128.119.245.12  TCP        54 53303 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
   60 5.992620  192.168.3.34    128.119.245.12  HTTP      529 GET /wireshark-labs/HTTP-ethereal-lab-file3.html
   61 6.025886  128.119.245.12  192.168.3.34    TCP        60 80 → 53303 [ACK] Seq=1 Ack=476 Win=30336 Len=0
   62 6.038820  128.119.245.12  192.168.3.34    TCP      1514 80 → 53303 [ACK] Seq=1 Ack=476 Win=30336 Len=1460
   63 6.038820  128.119.245.12  192.168.3.34    TCP      1514 80 → 53303 [ACK] Seq=1461 Ack=476 Win=30336 Len=1
   64 6.038820  128.119.245.12  192.168.3.34    TCP      1514 80 → 53303 [ACK] Seq=2921 Ack=476 Win=30336 Len=1
```

```
> Frame 60: 529 bytes on wire (4232 bits), 529 bytes captured (4
> Ethernet II, Src: IntelCor_4a:a4:cf (94:e2:3c:4a:a4:cf), Dst:
v Internet Protocol Version 4, Src: 192.168.3.34, Dst: 128.119.2
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-EC
     Total Length: 515
     Identification: 0xa322 (41762)
   > 010. .... = Flags: 0x2, Don't fragment
     ...0 0000 0000 0000 = Fragment Offset: 0
     Time to Live: 128
     Protocol: TCP (6)
     Header Checksum: 0x0000 [validation disabled]
```

```
0010  02 03 a3 22 40 00 80 06  00 00 c0 a8 03 22 80 77   ···"@··
0020  f5 0c d0 37 00 50 06 8a  92 a4 fd b1 11 3e 50 18   ···7·P·
0030  02 01 3b 44 00 00 47 45  54 20 2f 77 69 72 65 73   ··;D··G
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 65   hark-la
0050  74 68 65 72 65 61 6c 2d  6c 61 62 2d 66 69 6c 65   thereal
0060  33 2e 68 74 6d 6c 20 48  54 54 50 2f 31 2e 31 0d   3.html
0070  0a 48 6f 73 74 3a 20 67  61 69 61 2e 63 73 2e 75   ·Host:
0080  6d 61 73 73 2e 65 64 75  0d 0a 43 6f 6e 6e 65 63   mass.ed
0090  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: k
00a0  0d 0a 55 70 67 72 61 64  65 2d 49 6e 73 65 63 75   ··Upgra
00b0  72 65 2d 52 65 71 75 65  73 74 73 3a 20 31 0d 0a   re-Requ
00c0  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 69   User-Ag
00d0  6c 6c 61 2f 35 2e 30 20  28 57 69 6e 64 6f 77 73   lla/5.0
00e0  20 4e 54 20 31 30 2e 30  3b 20 57 69 6e 36 34 3b    NT 10.
00f0  20 78 36 34 29 20 41 70  70 6c 65 57 65 62 4b 69    x64) A
```

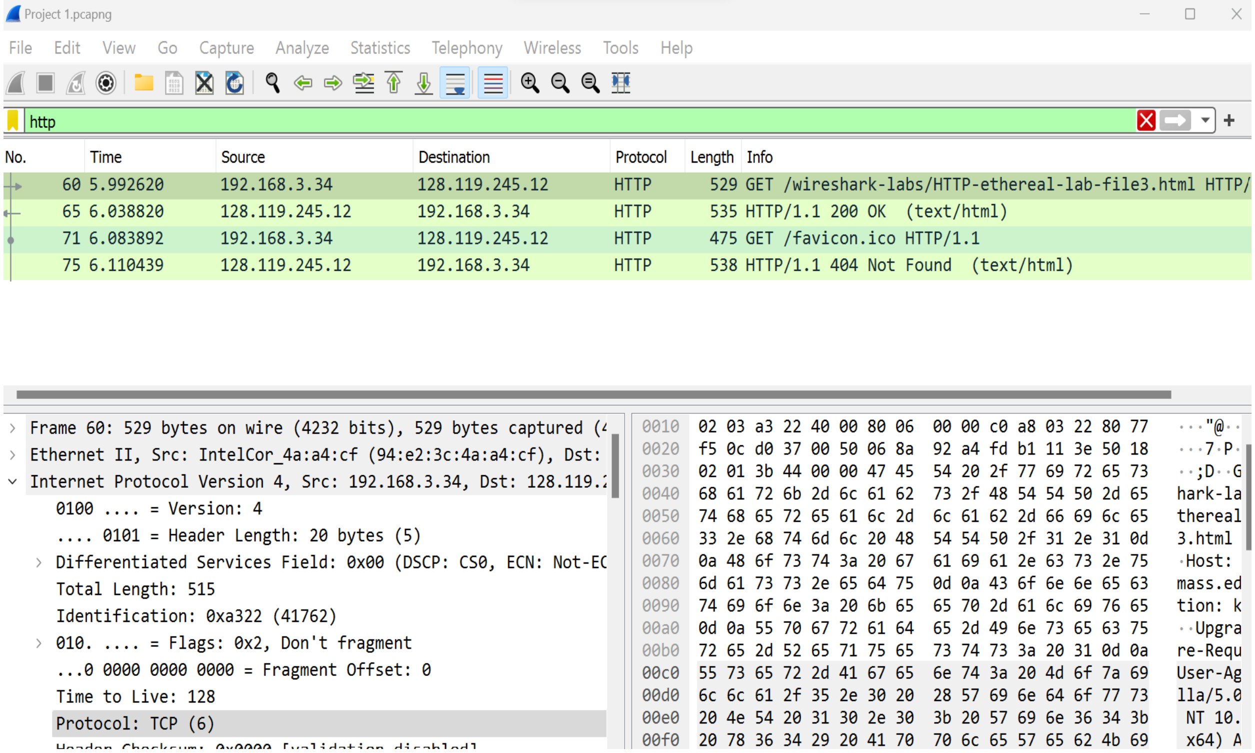
4. **You will see that other protocols are captured in your trace. One such protocol is HTTP. What is the relationship between the transport protocol you identified and HTTP?**

   The relationship between the transport protocol identified as TCP and the HTTP protocol is that TCP is used as the underlying transport protocol for HTTP communication. HTTP is an application layer protocol that governs the communication between web clients and web servers. It defines the structure and format of the messages exchanged between the client and server, including requests and responses for accessing and transferring resources. TCP, on the other hand, operates at the transport layer of the network protocol stack. It provides reliable, connection-oriented communication between hosts. TCP ensures that data sent over the network is delivered in the correct order, without loss, and with error checking. It establishes a connection between the client and server, segments data into packets, manages flow control, and handles retransmission of lost packets. In the context of HTTP, TCP is responsible for ensuring the reliable delivery of HTTP messages. When a client sends an HTTP request to a server or receives an HTTP response, TCP handles the encapsulation, segmentation, and reliable delivery of the HTTP message across the network. It establishes a connection, manages the transmission of HTTP packets, and guarantees the ordered delivery of those packets. Therefore, TCP serves as the transport protocol that facilitates the reliable transport of HTTP messages between the client and the server, ensuring the integrity and orderly delivery of the HTTP communication.

5. **Type in “http” (without the quotes, and in lowercase - all protocol names are in lowercase in Wireshark) into the display filter specification window at the top of the**

main Wireshark window. Then select Apply (to the right of where you entered "http"). This will cause only HTTP messages to be displayed in the packet-listing window. To see the exchange of HTTP messages with the web server, click statistics - flow graph - then check the "limit to display filter" box. Take a snapshot or copy/paste the packets displayed on the monitor (no need to scroll down and copy all).

HTTP packet-listing window:

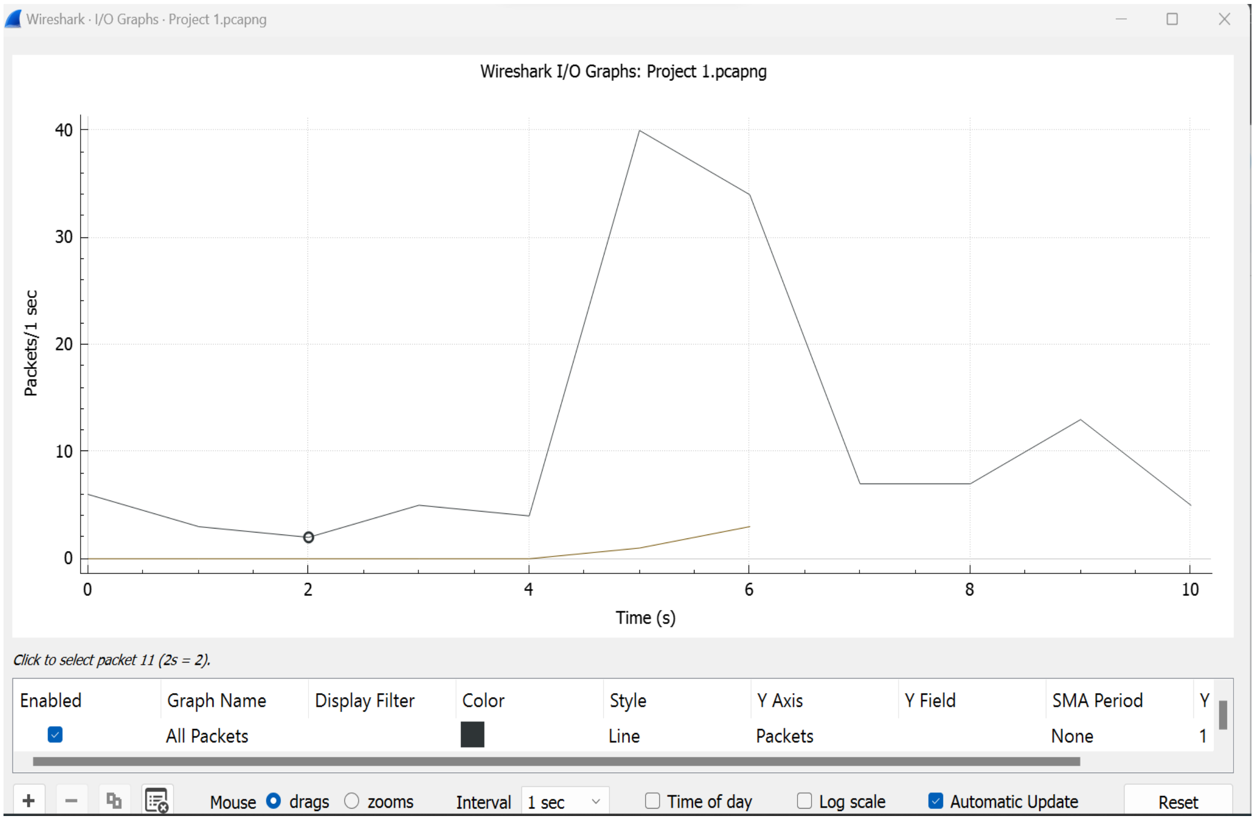

Project 1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.  Time      Source          Destination     Protocol Length Info
 60 5.992620   192.168.3.34    128.119.245.12  HTTP      529 GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/
 65 6.038820   128.119.245.12  192.168.3.34    HTTP      535 HTTP/1.1 200 OK  (text/html)
 71 6.083892   192.168.3.34    128.119.245.12  HTTP      475 GET /favicon.ico HTTP/1.1
 75 6.110439   128.119.245.12  192.168.3.34    HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 60: 529 bytes on wire (4232 bits), 529 bytes captured (4
> Ethernet II, Src: IntelCor_4a:a4:cf (94:e2:3c:4a:a4:cf), Dst:
v Internet Protocol Version 4, Src: 192.168.3.34, Dst: 128.119.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-EC
    Total Length: 515
    Identification: 0xa322 (41762)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
```

```
0010  02 03 a3 22 40 00 80 06  00 00 c0 a8 03 22 80 77   ···"@··
0020  f5 0c d0 37 00 50 06 8a  92 a4 fd b1 11 3e 50 18   ···7·P·
0030  02 01 3b 44 00 00 47 45  54 20 2f 77 69 72 65 73   ··;D··G
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 65   hark-la
0050  74 68 65 72 65 61 6c 2d  6c 61 62 2d 66 69 6c 65   thereal
0060  33 2e 68 74 6d 6c 20 48  54 54 50 2f 31 2e 31 0d   3.html
0070  0a 48 6f 73 74 3a 20 67  61 69 61 2e 63 73 2e 75   ·Host:
0080  6d 61 73 73 2e 65 64 75  0d 0a 43 6f 6e 6e 65 63   mass.ed
0090  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: k
00a0  0d 0a 55 70 67 72 61 64  65 2d 49 6e 73 65 63 75   ··Upgra
00b0  72 65 2d 52 65 71 75 65  73 74 73 3a 20 31 0d 0a   re-Requ
00c0  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 69   User-Ag
00d0  6c 6c 61 2f 35 2e 30 20  28 57 69 6e 64 6f 77 73   lla/5.0
00e0  20 4e 54 20 31 30 2e 30  3b 20 57 69 6e 36 34 3b    NT 10.
00f0  20 78 36 34 29 20 41 70  70 6c 65 57 65 62 4b 69    x64) A
```

Statistics:


Wireshark · I/O Graphs · Project 1.pcapng
Wireshark I/O Graphs: Project 1.pcapng
Packets/1 sec
40
30
20
10
0
0
2
4
6
8
10
Time (s)
+
−
Reset

Click to select packet 11 (2s = 2).

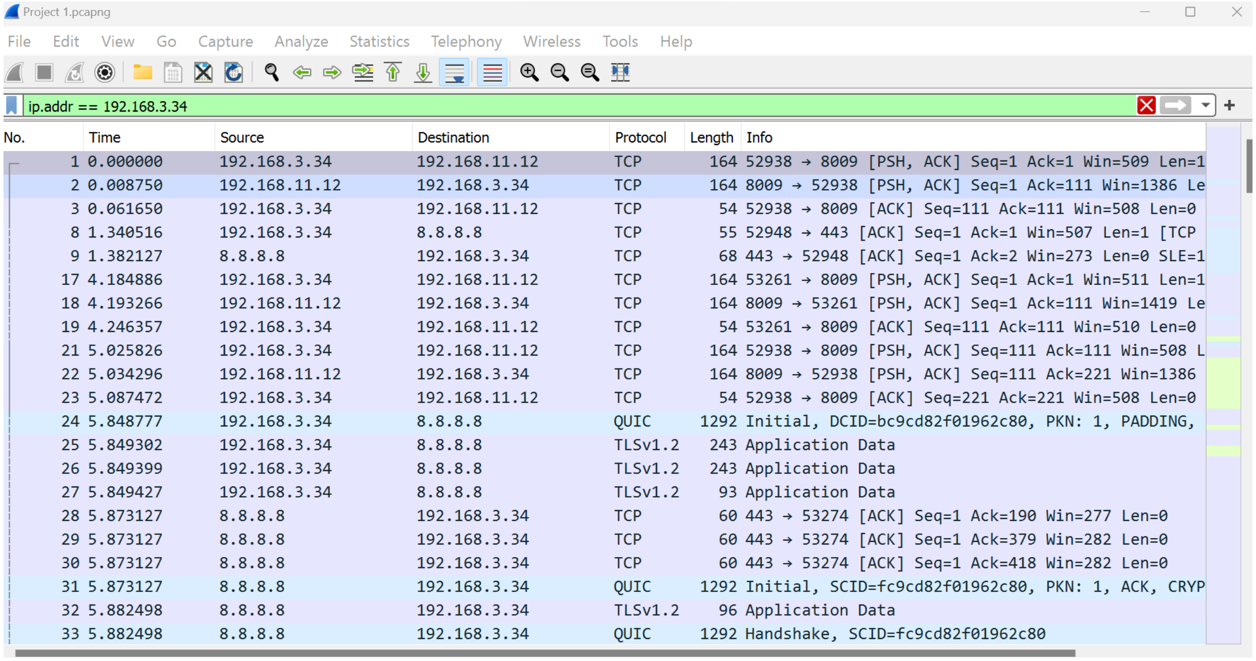
Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y
☑	All Packets		■	Line	Packets		None	1

Mouse ● drags ○ zooms Interval 1 sec □ Time of day □ Log scale ☑ Automatic Update

6. **Find an example packet in the trace where the IP address associated with your machine is present. Provide this example packet with your submission (take a screen dump or cut and paste the packet).**

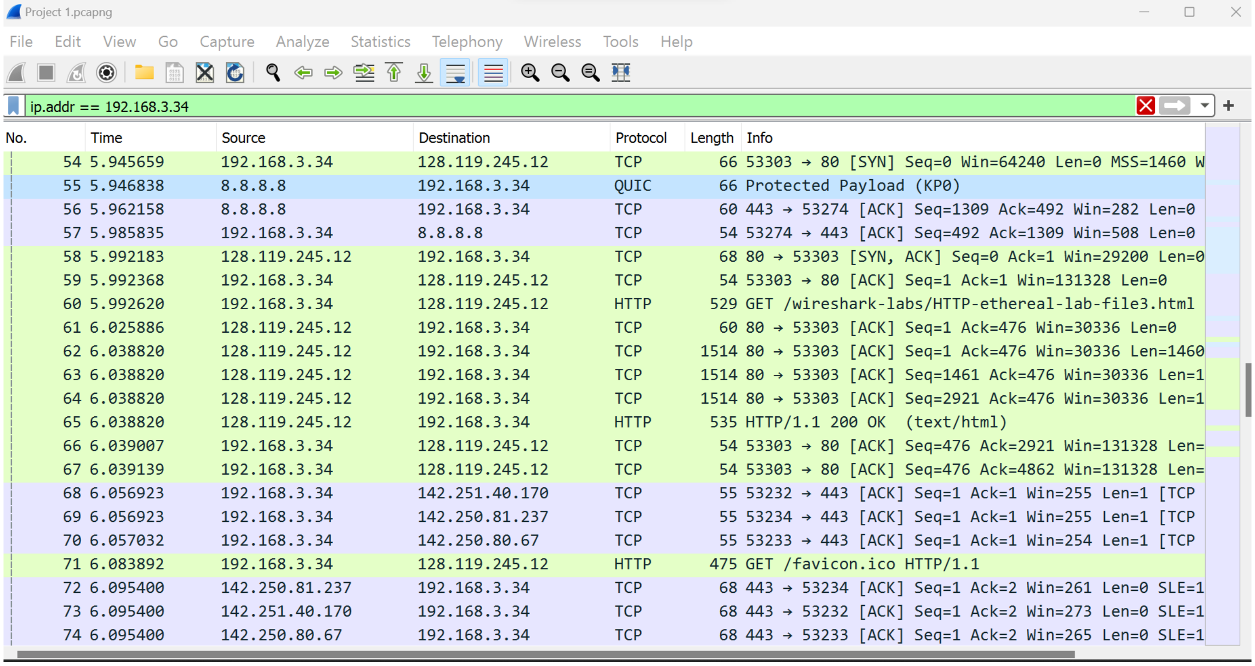
IP address of my machine is 192.168.3.34

The filter "ip.addr == 192.168.3.34" to filter packets where my machine's IP address appears either as the source or destination:



ip.addr == 192.168.3.34

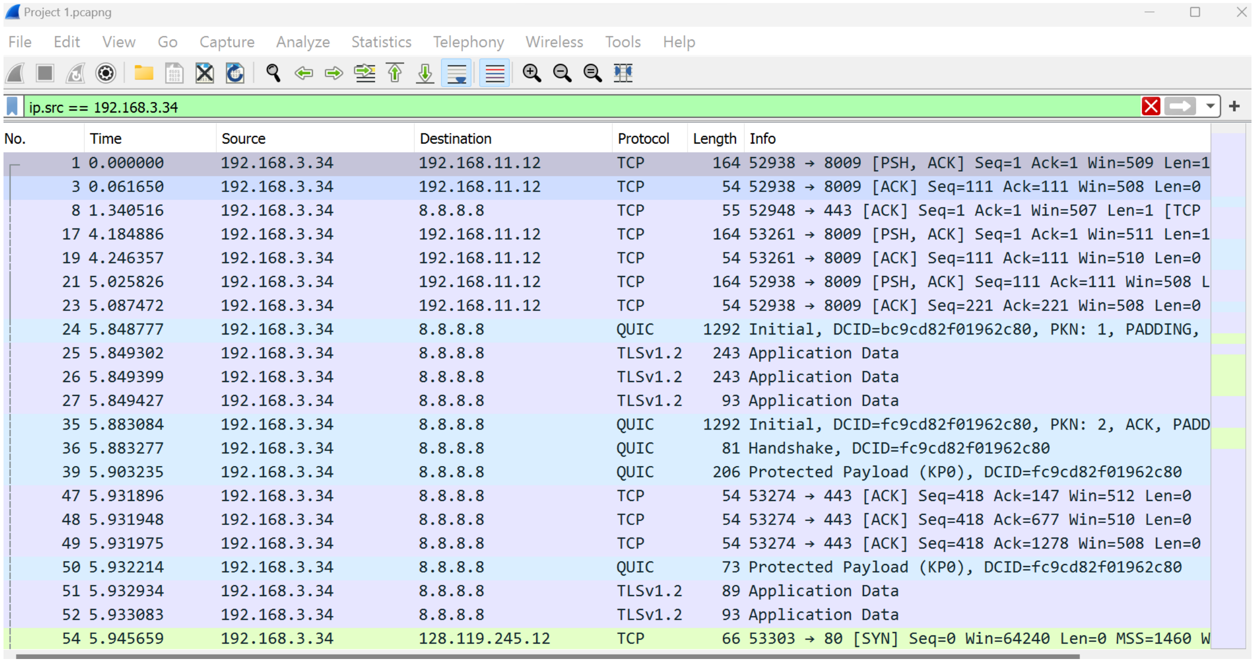
```
No.   Time       Source          Destination     Protocol Length Info
    1 0.000000   192.168.3.34    192.168.11.12   TCP       164 52938 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=509 Len=1
    2 0.008750   192.168.11.12   192.168.3.34    TCP       164 8009 → 52938 [PSH, ACK] Seq=1 Ack=111 Win=1386 Le
    3 0.061650   192.168.3.34    192.168.11.12   TCP        54 52938 → 8009 [ACK] Seq=111 Ack=111 Win=508 Len=0
    8 1.340516   192.168.3.34    8.8.8.8         TCP        55 52948 → 443 [ACK] Seq=1 Ack=1 Win=507 Len=1 [TCP
    9 1.382127   8.8.8.8         192.168.3.34    TCP        68 443 → 52948 [ACK] Seq=1 Ack=2 Win=273 Len=0 SLE=1
   17 4.184886   192.168.3.34    192.168.11.12   TCP       164 53261 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=511 Len=1
   18 4.193266   192.168.11.12   192.168.3.34    TCP       164 8009 → 53261 [PSH, ACK] Seq=1 Ack=111 Win=1419 Le
   19 4.246357   192.168.3.34    192.168.11.12   TCP        54 53261 → 8009 [ACK] Seq=111 Ack=111 Win=510 Len=0
   21 5.025826   192.168.3.34    192.168.11.12   TCP       164 52938 → 8009 [PSH, ACK] Seq=111 Ack=111 Win=508 L
   22 5.034296   192.168.11.12   192.168.3.34    TCP       164 8009 → 52938 [PSH, ACK] Seq=111 Ack=221 Win=1386
   23 5.087472   192.168.3.34    192.168.11.12   TCP        54 52938 → 8009 [ACK] Seq=221 Ack=221 Win=508 Len=0
   24 5.848777   192.168.3.34    8.8.8.8         QUIC     1292 Initial, DCID=bc9cd82f01962c80, PKN: 1, PADDING,
   25 5.849302   192.168.3.34    8.8.8.8         TLSv1.2   243 Application Data
   26 5.849399   192.168.3.34    8.8.8.8         TLSv1.2   243 Application Data
   27 5.849427   192.168.3.34    8.8.8.8         TLSv1.2    93 Application Data
   28 5.873127   8.8.8.8         192.168.3.34    TCP        60 443 → 53274 [ACK] Seq=1 Ack=190 Win=277 Len=0
   29 5.873127   8.8.8.8         192.168.3.34    TCP        60 443 → 53274 [ACK] Seq=1 Ack=379 Win=282 Len=0
   30 5.873127   8.8.8.8         192.168.3.34    TCP        60 443 → 53274 [ACK] Seq=1 Ack=418 Win=282 Len=0
   31 5.873127   8.8.8.8         192.168.3.34    QUIC     1292 Initial, SCID=fc9cd82f01962c80, PKN: 1, ACK, CRYP
   32 5.882498   8.8.8.8         192.168.3.34    TLSv1.2    96 Application Data
   33 5.882498   8.8.8.8         192.168.3.34    QUIC     1292 Handshake, SCID=fc9cd82f01962c80
```



ip.addr == 192.168.3.34

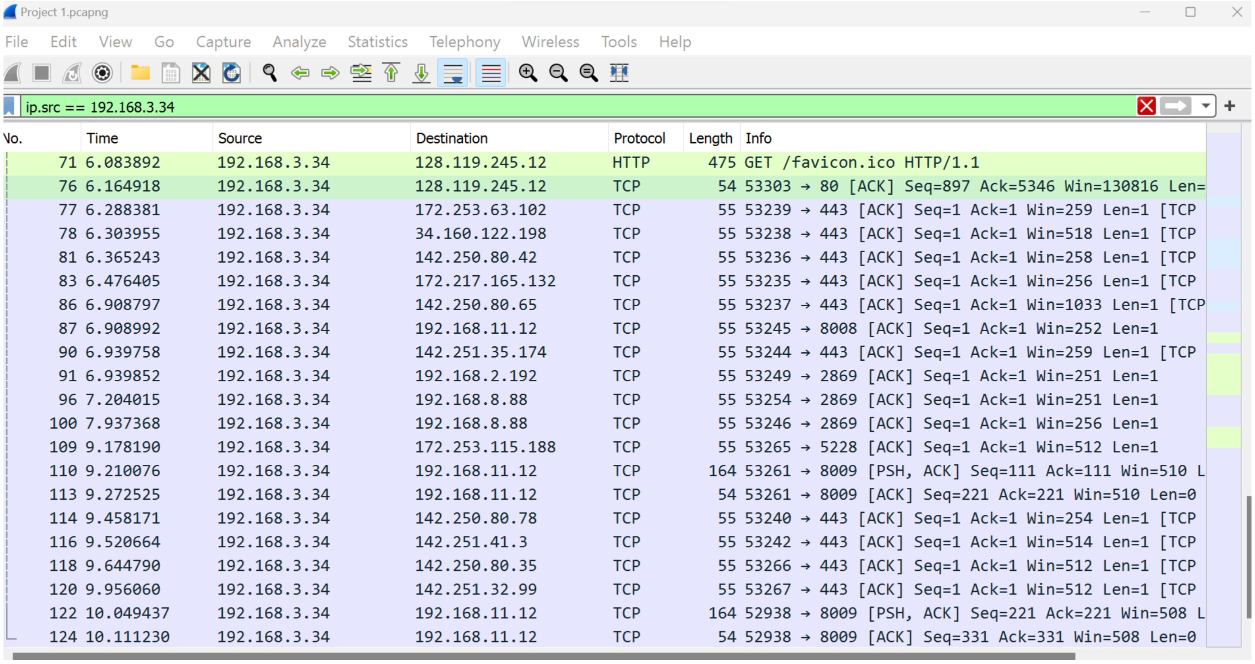
```
No.   Time       Source          Destination     Protocol Length Info
   54 5.945659   192.168.3.34    128.119.245.12  TCP        66 53303 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
   55 5.946838   8.8.8.8         192.168.3.34    QUIC       66 Protected Payload (KP0)
   56 5.962158   8.8.8.8         192.168.3.34    TCP        60 443 → 53274 [ACK] Seq=1309 Ack=492 Win=282 Len=0
   57 5.985835   192.168.3.34    8.8.8.8         TCP        54 53274 → 443 [ACK] Seq=492 Ack=1309 Win=508 Len=0
   58 5.992183   128.119.245.12  192.168.3.34    TCP        68 80 → 53303 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
   59 5.992368   192.168.3.34    128.119.245.12  TCP        54 53303 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
   60 5.992620   192.168.3.34    128.119.245.12  HTTP      529 GET /wireshark-labs/HTTP-ethereal-lab-file3.html
   61 6.025886   128.119.245.12  192.168.3.34    TCP        60 80 → 53303 [ACK] Seq=1 Ack=476 Win=30336 Len=0
   62 6.038820   128.119.245.12  192.168.3.34    TCP      1514 80 → 53303 [ACK] Seq=1 Ack=476 Win=30336 Len=1460
   63 6.038820   128.119.245.12  192.168.3.34    TCP      1514 80 → 53303 [ACK] Seq=1461 Ack=476 Win=30336 Len=1
   64 6.038820   128.119.245.12  192.168.3.34    TCP      1514 80 → 53303 [ACK] Seq=2921 Ack=476 Win=30336 Len=1
   65 6.038820   128.119.245.12  192.168.3.34    HTTP      535 HTTP/1.1 200 OK  (text/html)
   66 6.039007   192.168.3.34    128.119.245.12  TCP        54 53303 → 80 [ACK] Seq=476 Ack=2921 Win=131328 Len=
   67 6.039139   192.168.3.34    128.119.245.12  TCP        54 53303 → 80 [ACK] Seq=476 Ack=4862 Win=131328 Len=
   68 6.056923   192.168.3.34    142.251.40.170  TCP        55 53232 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP
   69 6.056923   192.168.3.34    142.250.81.237  TCP        55 53234 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP
   70 6.057032   192.168.3.34    142.250.80.67   TCP        55 53233 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1 [TCP
   71 6.083892   192.168.3.34    128.119.245.12  HTTP      475 GET /favicon.ico HTTP/1.1
   72 6.095400   142.250.81.237  192.168.3.34    TCP        68 443 → 53234 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1
   73 6.095400   142.251.40.170  192.168.3.34    TCP        68 443 → 53232 [ACK] Seq=1 Ack=2 Win=273 Len=0 SLE=1
   74 6.095400   142.250.80.67   192.168.3.34    TCP        68 443 → 53233 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1
```

The filter “ip.src == 192.168.3.34” to filter packets where my machine’s IP address is specifying the source:


Project 1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 192.168.3.34

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.3.34	192.168.11.12	TCP	164	52938 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=509 Len=1
3	0.061650	192.168.3.34	192.168.11.12	TCP	54	52938 → 8009 [ACK] Seq=111 Ack=111 Win=508 Len=0
8	1.340516	192.168.3.34	8.8.8.8	TCP	55	52948 → 443 [ACK] Seq=1 Ack=1 Win=507 Len=1 [TCP
17	4.184886	192.168.3.34	192.168.11.12	TCP	164	53261 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=511 Len=1
19	4.246357	192.168.3.34	192.168.11.12	TCP	54	53261 → 8009 [ACK] Seq=111 Ack=111 Win=510 Len=0
21	5.025826	192.168.3.34	192.168.11.12	TCP	164	52938 → 8009 [PSH, ACK] Seq=111 Ack=111 Win=508 L
23	5.087472	192.168.3.34	192.168.11.12	TCP	54	52938 → 8009 [ACK] Seq=221 Ack=221 Win=508 Len=0
24	5.848777	192.168.3.34	8.8.8.8	QUIC	1292	Initial, DCID=bc9cd82f01962c80, PKN: 1, PADDING,
25	5.849302	192.168.3.34	8.8.8.8	TLSv1.2	243	Application Data
26	5.849399	192.168.3.34	8.8.8.8	TLSv1.2	243	Application Data
27	5.849427	192.168.3.34	8.8.8.8	TLSv1.2	93	Application Data
35	5.883084	192.168.3.34	8.8.8.8	QUIC	1292	Initial, DCID=fc9cd82f01962c80, PKN: 2, ACK, PADD
36	5.883277	192.168.3.34	8.8.8.8	QUIC	81	Handshake, DCID=fc9cd82f01962c80
39	5.903235	192.168.3.34	8.8.8.8	QUIC	206	Protected Payload (KP0), DCID=fc9cd82f01962c80
47	5.931896	192.168.3.34	8.8.8.8	TCP	54	53274 → 443 [ACK] Seq=418 Ack=147 Win=512 Len=0
48	5.931948	192.168.3.34	8.8.8.8	TCP	54	53274 → 443 [ACK] Seq=418 Ack=677 Win=510 Len=0
49	5.931975	192.168.3.34	8.8.8.8	TCP	54	53274 → 443 [ACK] Seq=418 Ack=1278 Win=508 Len=0
50	5.932214	192.168.3.34	8.8.8.8	QUIC	73	Protected Payload (KP0), DCID=fc9cd82f01962c80
51	5.932934	192.168.3.34	8.8.8.8	TLSv1.2	89	Application Data
52	5.933083	192.168.3.34	8.8.8.8	TLSv1.2	93	Application Data
54	5.945659	192.168.3.34	128.119.245.12	TCP	66	53303 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W


Project 1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 192.168.3.34

No.	Time	Source	Destination	Protocol	Length	Info
71	6.083892	192.168.3.34	128.119.245.12	HTTP	475	GET /favicon.ico HTTP/1.1
76	6.164918	192.168.3.34	128.119.245.12	TCP	54	53303 → 80 [ACK] Seq=897 Ack=5346 Win=130816 Len=
77	6.288381	192.168.3.34	172.253.63.102	TCP	55	53239 → 443 [ACK] Seq=1 Ack=1 Win=259 Len=1 [TCP
78	6.303955	192.168.3.34	34.160.122.198	TCP	55	53238 → 443 [ACK] Seq=1 Ack=1 Win=518 Len=1 [TCP
81	6.365243	192.168.3.34	142.250.80.42	TCP	55	53236 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP
83	6.476405	192.168.3.34	172.217.165.132	TCP	55	53235 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [TCP
86	6.908797	192.168.3.34	142.250.80.65	TCP	55	53237 → 443 [ACK] Seq=1 Ack=1 Win=1033 Len=1 [TCP
87	6.908992	192.168.3.34	192.168.11.12	TCP	55	53245 → 8008 [ACK] Seq=1 Ack=1 Win=252 Len=1
90	6.939758	192.168.3.34	142.251.35.174	TCP	55	53244 → 443 [ACK] Seq=1 Ack=1 Win=259 Len=1 [TCP
91	6.939852	192.168.3.34	192.168.2.192	TCP	55	53249 → 2869 [ACK] Seq=1 Ack=1 Win=251 Len=1
96	7.204015	192.168.3.34	192.168.8.88	TCP	55	53254 → 2869 [ACK] Seq=1 Ack=1 Win=251 Len=1
100	7.937368	192.168.3.34	192.168.8.88	TCP	55	53246 → 2869 [ACK] Seq=1 Ack=1 Win=256 Len=1
109	9.178190	192.168.3.34	172.253.115.188	TCP	55	53265 → 5228 [ACK] Seq=1 Ack=1 Win=512 Len=1
110	9.210076	192.168.3.34	192.168.11.12	TCP	164	53261 → 8009 [PSH, ACK] Seq=111 Ack=111 Win=510 L
113	9.272525	192.168.3.34	192.168.11.12	TCP	54	53261 → 8009 [ACK] Seq=221 Ack=221 Win=510 Len=0
114	9.458171	192.168.3.34	142.250.80.78	TCP	55	53240 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1 [TCP
116	9.520664	192.168.3.34	142.251.41.3	TCP	55	53242 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1 [TCP
118	9.644790	192.168.3.34	142.250.80.35	TCP	55	53266 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP
120	9.956060	192.168.3.34	142.251.32.99	TCP	55	53267 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP
122	10.049437	192.168.3.34	192.168.11.12	TCP	164	52938 → 8009 [PSH, ACK] Seq=221 Ack=221 Win=508 L
124	10.111230	192.168.3.34	192.168.11.12	TCP	54	52938 → 8009 [ACK] Seq=331 Ack=331 Win=508 Len=0

7. **We discussed protocol layers in class. Which layer is the IP associated with? Which layer is the transport protocol you identified in sec. 2 a is associated with? Which layer is the HTTP protocol associated with?**

Make sure to provide your answer in the required sequence. You may use a table like this to answer this section:

Layer	**Protocol**
Network Layer	IP (Internet Protocol)
Transport Layer	TCP (Transmission Control Protocol)
Application Layer	HTTP (Hypertext Transfer Protocol)