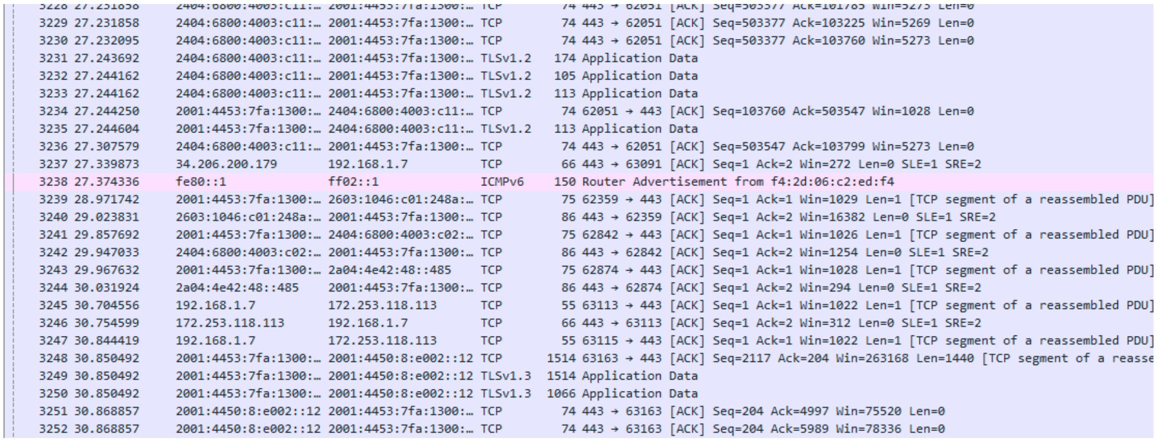
Name: Zuriel G. Montallana

Year/Block: BSIT3-B1

LabAct1

1. List 3 protocols appearing in the protocol column in the unfiltered packet-listing window in step 7 above. Then, briefly describe the function of each protocol. (5pts)



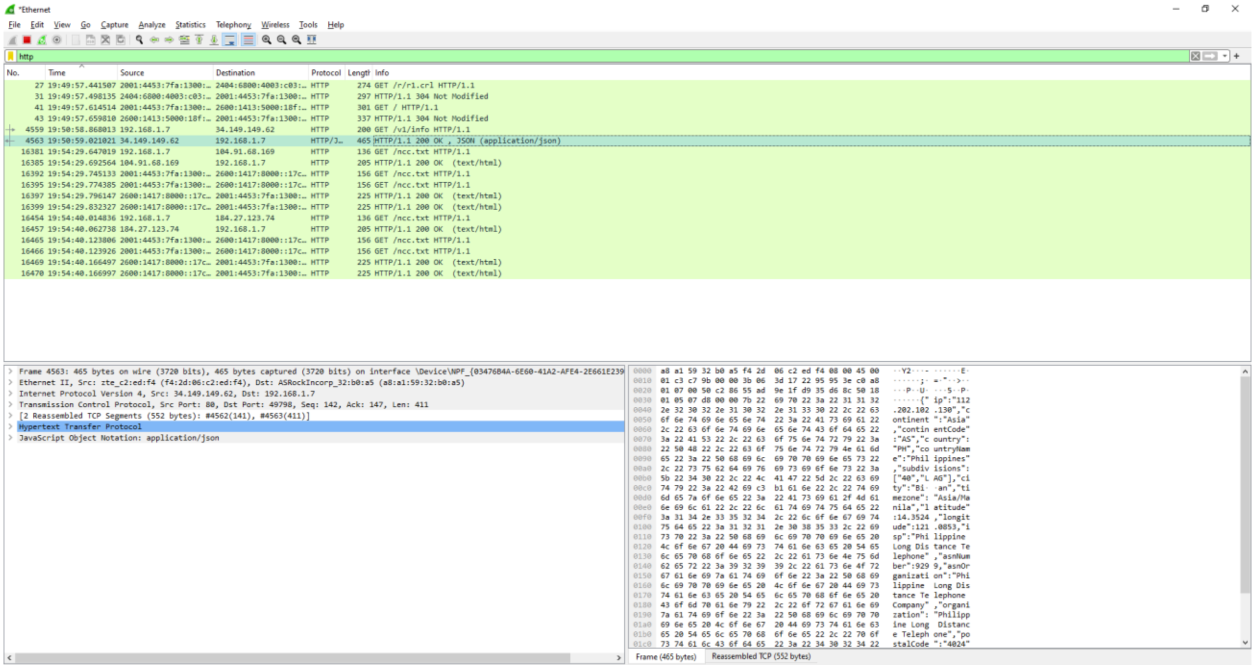
```
3228 27.231858   2404:6800:4003:c11:… 2001:4453:7fa:1300:… TCP       74 443 → 62051 [ACK] Seq=503377 Ack=101785 Win=5273 Len=0
3229 27.231858   2404:6800:4003:c11:… 2001:4453:7fa:1300:… TCP       74 443 → 62051 [ACK] Seq=503377 Ack=103225 Win=5269 Len=0
3230 27.232095   2404:6800:4003:c11:… 2001:4453:7fa:1300:… TCP       74 443 → 62051 [ACK] Seq=503377 Ack=103760 Win=5273 Len=0
3231 27.243692   2404:6800:4003:c11:… 2001:4453:7fa:1300:… TLSv1.2  174 Application Data
3232 27.244162   2404:6800:4003:c11:… 2001:4453:7fa:1300:… TLSv1.2  105 Application Data
3233 27.244162   2404:6800:4003:c11:… 2001:4453:7fa:1300:… TLSv1.2  113 Application Data
3234 27.244250   2001:4453:7fa:1300:… 2404:6800:4003:c11:… TCP       74 62051 → 443 [ACK] Seq=103760 Ack=503547 Win=1028 Len=0
3235 27.244604   2001:4453:7fa:1300:… 2404:6800:4003:c11:… TLSv1.2  113 Application Data
3236 27.307579   2404:6800:4003:c11:… 2001:4453:7fa:1300:… TCP       74 443 → 62051 [ACK] Seq=503547 Ack=103799 Win=5273 Len=0
3237 27.339873   34.206.200.179       192.168.1.7          TCP       66 443 → 63091 [ACK] Seq=1 Ack=2 Win=272 Len=0 SLE=1 SRE=2
3238 27.374336   fe80::1              ff02::1              ICMPv6   150 Router Advertisement from f4:2d:06:c2:ed:f4
3239 28.971742   2001:4453:7fa:1300:… 2603:1046:c01:248a:… TCP       75 62359 → 443 [ACK] Seq=1 Ack=1 Win=1029 Len=1 [TCP segment of a reassembled PDU]
3240 29.023831   2603:1046:c01:248a:… 2001:4453:7fa:1300:… TCP       86 443 → 62359 [ACK] Seq=1 Ack=2 Win=16382 Len=0 SLE=1 SRE=2
3241 29.857692   2001:4453:7fa:1300:… 2404:6800:4003:c02:… TCP       75 62842 → 443 [ACK] Seq=1 Ack=1 Win=1026 Len=1 [TCP segment of a reassembled PDU]
3242 29.947033   2404:6800:4003:c02:… 2001:4453:7fa:1300:… TCP       86 443 → 62842 [ACK] Seq=1 Ack=2 Win=1254 Len=0 SLE=1 SRE=2
3243 29.967632   2001:4453:7fa:1300:… 2a04:4e42:48::485    TCP       75 62874 → 443 [ACK] Seq=1 Ack=1 Win=1028 Len=1 [TCP segment of a reassembled PDU]
3244 30.031924   2a04:4e42:48::485    2001:4453:7fa:1300:… TCP       86 443 → 62874 [ACK] Seq=1 Ack=2 Win=294 Len=0 SLE=1 SRE=2
3245 30.704556   192.168.1.7          172.253.118.113      TCP       55 63113 → 443 [ACK] Seq=1 Ack=1 Win=1022 Len=1 [TCP segment of a reassembled PDU]
3246 30.754599   172.253.118.113      192.168.1.7          TCP       66 443 → 63113 [ACK] Seq=1 Ack=2 Win=312 Len=0 SLE=1 SRE=2
3247 30.844419   192.168.1.7          172.253.118.113      TCP       55 63115 → 443 [ACK] Seq=1 Ack=1 Win=1022 Len=1 [TCP segment of a reassembled PDU]
3248 30.850492   2001:4453:7fa:1300:… 2001:4450:8:e002::12 TCP     1514 63163 → 443 [ACK] Seq=2117 Ack=204 Win=263168 Len=1440 [TCP segment of a reasse
3249 30.850492   2001:4453:7fa:1300:… 2001:4450:8:e002::12 TLSv1.3 1514 Application Data
3250 30.850492   2001:4453:7fa:1300:… 2001:4450:8:e002::12 TLSv1.3 1066 Application Data
3251 30.868857   2001:4450:8:e002::12 2001:4453:7fa:1300:… TCP       74 443 → 63163 [ACK] Seq=204 Ack=4997 Win=75520 Len=0
3252 30.868857   2001:4450:8:e002::12 2001:4453:7fa:1300:… TCP       74 443 → 63163 [ACK] Seq=204 Ack=5989 Win=78336 Len=0
```

1. TLSv1.2 - Secures communication via encryption, widely used but supports older, less secure cryptographic methods.

2. ICMPv6 - Handles error reporting, diagnostics, and essential network operations in IPv6.

3. TLSv1.3 - Provides secure, encrypted communication with faster performance and stronger security than previous versions.

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the Time column value in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark Viewpull down menu, select Time Display Format, then select Time-of-day.) (5 pts)


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

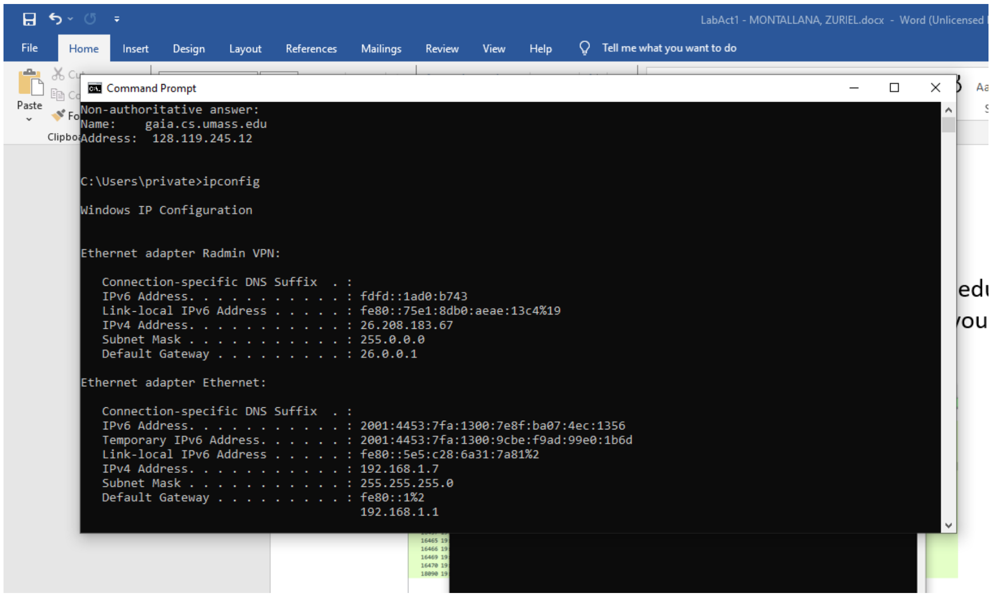
No.	Time	Source	Destination	Protocol	Length	Info
27	19:49:57.441507	2001:4453:7fa:1300:…	2404:6800:4003:c03:…	HTTP	274	GET /r/r1.crl HTTP/1.1
31	19:49:57.498135	2404:6800:4003:c03:…	2001:4453:7fa:1300:…	HTTP	297	HTTP/1.1 304 Not Modified
41	19:49:57.614514	2001:4453:7fa:1300:…	2600:1413:5000:18f:…	HTTP	301	GET / HTTP/1.1
43	19:49:57.659810	2600:1413:5000:18f:…	2001:4453:7fa:1300:…	HTTP	337	HTTP/1.1 304 Not Modified
4559	19:50:58.868013	192.168.1.7	34.149.149.62	HTTP	200	GET /v1/info HTTP/1.1
4563	19:50:59.021021	34.149.149.62	192.168.1.7	HTTP/J…	465	HTTP/1.1 200 OK , JSON (application/json)
16381	19:54:29.647019	192.168.1.7	104.91.68.169	HTTP	136	GET /ncc.txt HTTP/1.1
16385	19:54:29.692564	104.91.68.169	192.168.1.7	HTTP	205	HTTP/1.1 200 OK (text/html)
16392	19:54:29.745133	2001:4453:7fa:1300:…	2600:1417:8000::17c…	HTTP	156	GET /ncc.txt HTTP/1.1
16395	19:54:29.774385	2001:4453:7fa:1300:…	2600:1417:8000::17c…	HTTP	156	GET /ncc.txt HTTP/1.1
16397	19:54:29.796147	2600:1417:8000::17c…	2001:4453:7fa:1300:…	HTTP	225	HTTP/1.1 200 OK (text/html)
16399	19:54:29.832327	2600:1417:8000::17c…	2001:4453:7fa:1300:…	HTTP	225	HTTP/1.1 200 OK (text/html)
16454	19:54:40.014836	192.168.1.7	184.27.123.74	HTTP	136	GET /ncc.txt HTTP/1.1
16457	19:54:40.062738	184.27.123.74	192.168.1.7	HTTP	205	HTTP/1.1 200 OK (text/html)
16465	19:54:40.123806	2001:4453:7fa:1300:…	2600:1417:8000::17c…	HTTP	156	GET /ncc.txt HTTP/1.1
16466	19:54:40.123926	2001:4453:7fa:1300:…	2600:1417:8000::17c…	HTTP	156	GET /ncc.txt HTTP/1.1
16469	19:54:40.166497	2600:1417:8000::17c…	2001:4453:7fa:1300:…	HTTP	225	HTTP/1.1 200 OK (text/html)
16470	19:54:40.166997	2600:1417:8000::17c…	2001:4453:7fa:1300:…	HTTP	225	HTTP/1.1 200 OK (text/html)

```
> Frame 4563: 465 bytes on wire (3720 bits), 465 bytes captured (3720 bits) on interface \Device\NPF_{03476B4A-6E60-41A2-AFE4-2E661E239
> Ethernet II, Src: zte_c2:ed:f4 (f4:2d:06:c2:ed:f4), Dst: ASRockIncorp_32:b0:a5 (a8:a1:59:32:b0:a5)
> Internet Protocol Version 4, Src: 34.149.149.62, Dst: 192.168.1.7
> Transmission Control Protocol, Src Port: 80, Dst Port: 49798, Seq: 142, Ack: 147, Len: 411
> [2 Reassembled TCP Segments (552 bytes): #4562(141), #4563(411)]
> Hypertext Transfer Protocol
> JavaScript Object Notation: application/json
```

```
0000  a8 a1 59 32 b0 a5 f4 2d  06 c2 ed f4 08 00 45 00   ··Y2···- ······E·
0010  01 c3 c7 9b 00 00 3b 06  3d 17 22 95 95 3e c0 a8   ······;· =·"··>··
0020  01 07 00 50 c2 86 55 ad  9e 1f d9 35 d6 8c 50 18   ···P··U· ···5··P·
0030  01 05 07 d8 00 00 7b 22  69 70 22 3a 22 31 31 32   ······{" ip":"112
0040  2e 32 30 32 2e 31 30 32  2e 31 33 30 22 2c 22 63   .202.102 .130","c
0050  6f 6e 74 69 6e 65 6e 74  22 3a 22 41 73 69 61 22   ontinent ":"Asia"
0060  2c 22 63 6f 6e 74 69 6e  65 6e 74 43 6f 64 65 22   ,"contin entCode"
0070  3a 22 41 53 22 2c 22 63  6f 75 6e 74 72 79 22 3a   :"AS","c ountry":
0080  22 50 48 22 2c 22 63 6f  75 6e 74 72 79 4e 61 6d   "PH","co untryNam
0090  65 22 3a 22 50 68 69 6c  69 70 70 69 6e 65 73 22   e":"Phil ippines"
00a0  2c 22 73 75 62 64 69 76  69 73 69 6f 6e 73 22 3a   ,"subdiv isions":
00b0  5b 22 34 30 22 2c 22 4c  41 47 22 5d 2c 22 63 69   ["40","L AG"],"ci
00c0  74 79 22 3a 22 42 69 c3  b1 61 6e 22 2c 22 74 69   ty":"Bi· ·an","ti
00d0  6d 65 7a 6f 6e 65 22 3a  22 41 73 69 61 2f 4d 61   mezone": "Asia/Ma
00e0  6e 69 6c 61 22 2c 22 6c  61 74 69 74 75 64 65 22   nila","l atitude"
00f0  3a 31 34 2e 33 35 32 34  2c 22 6c 6f 6e 67 69 74   :14.3524 ,"longit
0100  75 64 65 22 3a 31 32 31  2e 30 38 35 33 2c 22 69   ude":121 .0853,"i
0110  73 70 22 3a 22 50 68 69  6c 69 70 70 69 6e 65 20   sp":"Phi lippine 
0120  4c 6f 6e 67 20 44 69 73  74 61 6e 63 65 20 54 65   Long Dis tance Te
0130  6c 65 70 68 6f 6e 65 22  2c 22 61 73 6e 4e 75 6d   lephone" ,"asnNum
0140  62 65 72 22 3a 39 32 39  39 2c 22 61 73 6e 4f 72   ber":929 9,"asnOr
0150  67 61 6e 69 7a 61 74 69  6f 6e 22 3a 22 50 68 69   ganizati on":"Phi
0160  6c 69 70 70 69 6e 65 20  4c 6f 6e 67 20 44 69 73   lippine  Long Dis
0170  74 61 6e 63 65 20 54 65  6c 65 70 68 6f 6e 65 20   tance Te lephone 
0180  43 6f 6d 70 61 6e 79 22  2c 22 6f 72 67 61 6e 69   Company" ,"organi
0190  7a 61 74 69 6f 6e 22 3a  22 50 68 69 6c 69 70 70   zation": "Philipp
01a0  69 6e 65 20 4c 6f 6e 67  20 44 69 73 74 61 6e 63   ine Long  Distanc
01b0  65 20 54 65 6c 65 70 68  6f 6e 65 22 2c 22 70 6f   e Teleph one","po
01c0  73 74 61 6c 43 6f 64 65  22 3a 22 34 30 32 34 22   stalCode ":"4024"
```

The HTTP GET request was sent at 19:49:57.615328, and the server responded with an HTTP 200 OK at 19:49:57.690143. This means it took about 0.075 seconds for the server to process the request and send back the response.

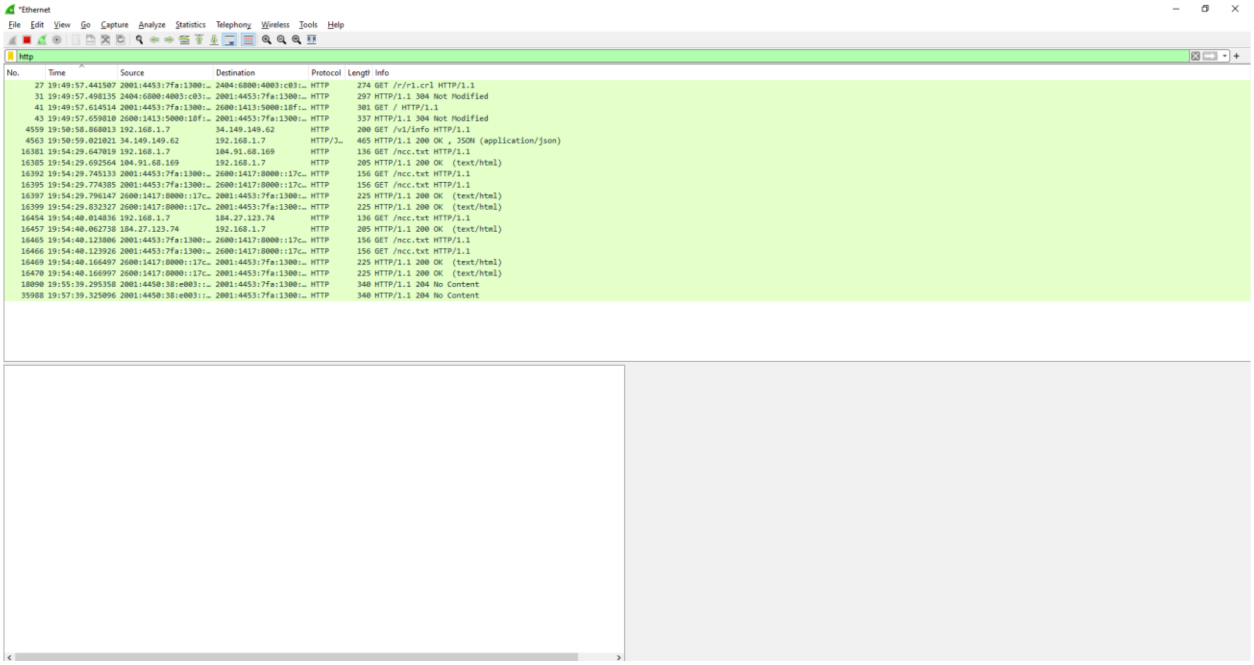
3. What is the Internet address of (also known as www-net.cs.umass.edu)? What is the Internet address of your computer? (5 pts)



```
Non-authoritative answer:
Name:    gaia.cs.umass.edu
Address:  128.119.245.12


C:\Users\private>ipconfig

Windows IP Configuration


Ethernet adapter Radmin VPN:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : fdfd::1ad0:b743
   Link-local IPv6 Address . . . . . : fe80::75e1:8db0:aeae:13c4%19
   IPv4 Address. . . . . . . . . . . : 26.208.183.67
   Subnet Mask . . . . . . . . . . . : 255.0.0.0
   Default Gateway . . . . . . . . . : 26.0.0.1

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:4453:7fa:1300:7e8f:ba07:4ec:1356
   Temporary IPv6 Address. . . . . . : 2001:4453:7fa:1300:9cbe:f9ad:99e0:1b6d
   Link-local IPv6 Address . . . . . : fe80::5e5:c28:6a31:7a81%2
   IPv4 Address. . . . . . . . . . . : 192.168.1.7
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%2
                                       192.168.1.1
```

I opened cmd and then first type “nslookup gaia.cs.umass.edu”. The Internet address of gaia.cs.umass.edu is 128.119.245.12, While my computer's IP address is 192.168.1.7 with an IPv6 address of 2001:4453:7f8a:1300:9ecb:fp04:99e0:1b6d using ipconfig on the command.

4. Filter the traffic to show only HTTP requests. How many HTTP GET requests are present? (5pts)


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
27	19:49:57.441507	2001:4453:7fa:1300:…	2404:6800:4003:c03:…	HTTP	274	GET /r/r1.crl HTTP/1.1
31	19:49:57.498135	2404:6800:4003:c03:…	2001:4453:7fa:1300:…	HTTP	297	HTTP/1.1 304 Not Modified
41	19:49:57.614514	2001:4453:7fa:1300:…	2600:1413:5000:18f:…	HTTP	301	GET / HTTP/1.1
43	19:49:57.659810	2600:1413:5000:18f:…	2001:4453:7fa:1300:…	HTTP	337	HTTP/1.1 304 Not Modified
4559	19:50:58.868013	192.168.1.7	34.149.149.62	HTTP	200	GET /v1/info HTTP/1.1
4563	19:50:59.021021	34.149.149.62	192.168.1.7	HTTP/J…	465	HTTP/1.1 200 OK , JSON (application/json)
16381	19:54:29.647019	192.168.1.7	104.91.68.169	HTTP	136	GET /ncc.txt HTTP/1.1
16385	19:54:29.692564	104.91.68.169	192.168.1.7	HTTP	205	HTTP/1.1 200 OK (text/html)
16392	19:54:29.745133	2001:4453:7fa:1300:…	2600:1417:8000::17c…	HTTP	156	GET /ncc.txt HTTP/1.1
16395	19:54:29.774385	2001:4453:7fa:1300:…	2600:1417:8000::17c…	HTTP	156	GET /ncc.txt HTTP/1.1
16397	19:54:29.796147	2600:1417:8000::17c…	2001:4453:7fa:1300:…	HTTP	225	HTTP/1.1 200 OK (text/html)
16399	19:54:29.832327	2600:1417:8000::17c…	2001:4453:7fa:1300:…	HTTP	225	HTTP/1.1 200 OK (text/html)
16454	19:54:40.014836	192.168.1.7	184.27.123.74	HTTP	136	GET /ncc.txt HTTP/1.1
16457	19:54:40.062738	184.27.123.74	192.168.1.7	HTTP	205	HTTP/1.1 200 OK (text/html)
16465	19:54:40.123806	2001:4453:7fa:1300:…	2600:1417:8000::17c…	HTTP	156	GET /ncc.txt HTTP/1.1
16466	19:54:40.123926	2001:4453:7fa:1300:…	2600:1417:8000::17c…	HTTP	156	GET /ncc.txt HTTP/1.1
16469	19:54:40.166497	2600:1417:8000::17c…	2001:4453:7fa:1300:…	HTTP	225	HTTP/1.1 200 OK (text/html)
16470	19:54:40.166997	2600:1417:8000::17c…	2001:4453:7fa:1300:…	HTTP	225	HTTP/1.1 200 OK (text/html)
18090	19:55:39.295358	2001:4450:38:e003::…	2001:4453:7fa:1300:…	HTTP	340	HTTP/1.1 204 No Content
35988	19:57:39.325096	2001:4450:38:e003::…	2001:4453:7fa:1300:…	HTTP	340	HTTP/1.1 204 No Content

After typing “http” on the filter bar, it displayed all protocols which are only http and there are four HTTP GET requests present. These are shown in packets numbered 2, 5, 11, and 31.