Questions:

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

TCP,DNS, HTTP are among multiple protocols that appear in the protocol column. Others I discovered are also QUIC and TLSv1.2.

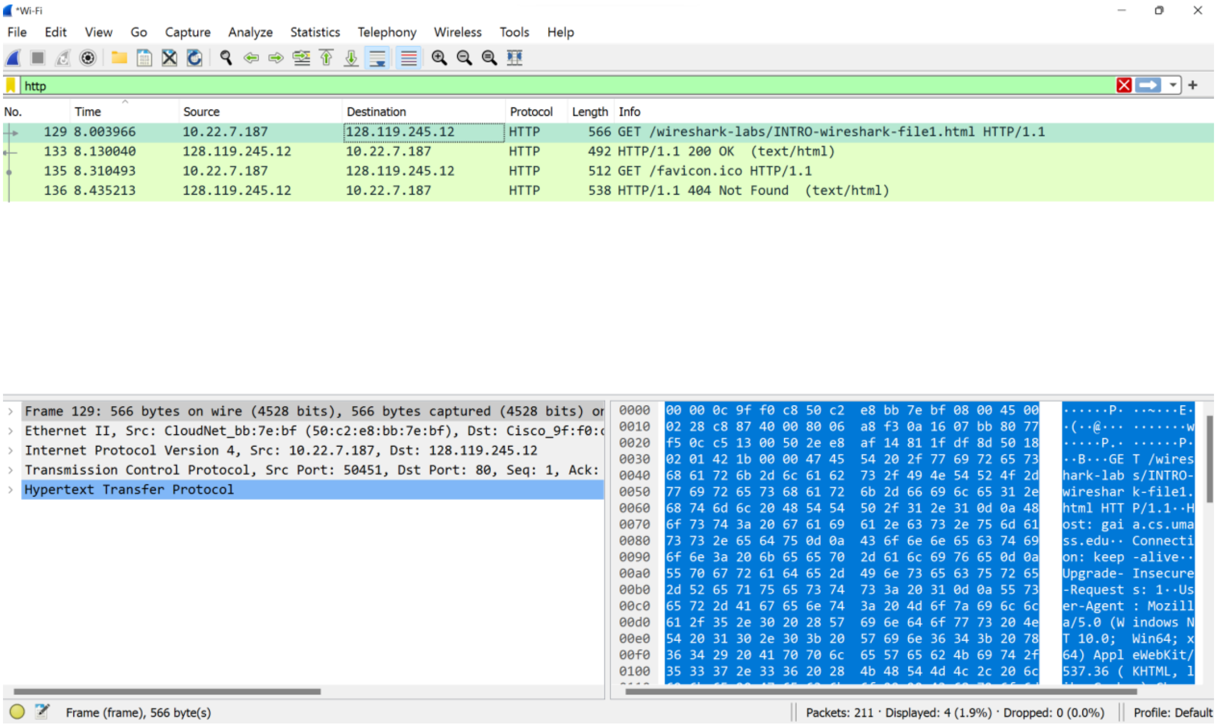
2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark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

It took 8.003966 seconds from when I started capturing In wireshark until I clicked the link and the GET message was sent, and at the time 8.130040, the ok reply was received. Which means it took 0,126074 seconds or 126ms from sending the GET message until the OK reply was received.

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

By looking at the source and destination columns, we can see the IP addresses of where information is sending and where it is receiving. If we look at where the GET message Is sent from my computer, we will see that the source IP is: 10.22.7.187, which is my computer as it is sending the request for information, therefore the source of the message. The destination would then of course be the website which we requested, where the IP is: 128.119.245.12. We could also look at other columns, however we see here that it is changing between which of the IPs are the destination and source. This is due to the communication going both ways, and different information are sent and received by different sources. Keeping in mind that the website also has to send some information back to the user, for the user being able to display the information. Therefore, having the OK reply, which switches destination and source address, as the information there is sent from website to user.

4. Take screenshots of the two HTTP messages (GET and OK) referred to in question 2 above. The screenshots should include the packet-header window for these messages and the packet list window (see the beginning of this tutorial for the descriptions of the different windows).



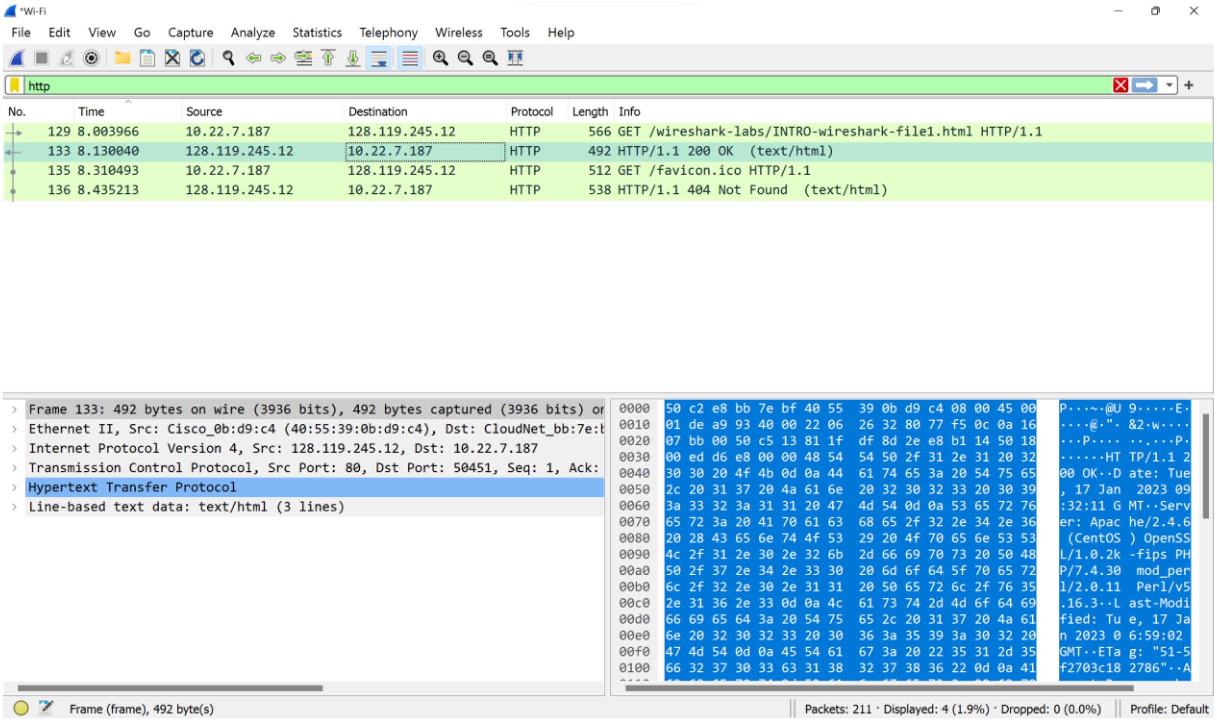
http

```
No.   Time        Source           Destination      Protocol  Length  Info
  129 8.003966    10.22.7.187      128.119.245.12   HTTP       566 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  133 8.130040    128.119.245.12   10.22.7.187      HTTP       492 HTTP/1.1 200 OK  (text/html)
  135 8.310493    10.22.7.187      128.119.245.12   HTTP       512 GET /favicon.ico HTTP/1.1
  136 8.435213    128.119.245.12   10.22.7.187      HTTP       538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 129: 566 bytes on wire (4528 bits), 566 bytes captured (4528 bits) or
> Ethernet II, Src: CloudNet_bb:7e:bf (50:c2:e8:bb:7e:bf), Dst: Cisco_9f:f0:c
> Internet Protocol Version 4, Src: 10.22.7.187, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50451, Dst Port: 80, Seq: 1, Ack:
> Hypertext Transfer Protocol
```

```
0000  00 00 0c 9f f0 c8 50 c2  e8 bb 7e bf 08 00 45 00   ······P· ··~···E·
0010  02 28 c8 87 40 00 80 06  a8 f3 0a 16 07 bb 80 77   ·(··@··· ·······w
0020  f5 0c c5 13 00 50 2e e8  af 14 81 1f df 8d 50 18   ·····P.· ······P·
0030  02 01 42 1b 00 00 47 45  54 20 2f 77 69 72 65 73   ··B···GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 49 4e 54 52 4f 2d   hark-lab s/INTRO-
0050  77 69 72 65 73 68 61 72  6b 2d 66 69 6c 65 31 2e   wireshar k-file1.
0060  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31 0d 0a 48   html HTT P/1.1··H
0070  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e 75 6d 61   ost: gai a.cs.uma
0080  73 73 2e 65 64 75 0d 0a  43 6f 6e 6e 65 63 74 69   ss.edu·· Connecti
0090  6f 6e 3a 20 6b 65 65 70  2d 61 6c 69 76 65 0d 0a   on: keep -alive··
00a0  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade- Insecure
00b0  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a 55 73   -Request s: 1··Us
00c0  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
00d0  61 2f 35 2e 30 20 28 57  69 6e 64 6f 77 73 20 4e   a/5.0 (W indows N
00e0  54 20 31 30 2e 30 3b 20  57 69 6e 36 34 3b 20 78   T 10.0;  Win64; x
00f0  36 34 29 20 41 70 70 6c  65 57 65 62 4b 69 74 2f   64) Appl eWebKit/
0100  35 33 37 2e 33 36 20 28  4b 48 54 4d 4c 2c 20 6c   537.36 ( KHTML, l
```

Frame (frame), 566 byte(s)   Packets: 211 · Displayed: 4 (1.9%) · Dropped: 0 (0.0%)   Profile: Default



http

```
No.   Time        Source           Destination      Protocol  Length  Info
  129 8.003966    10.22.7.187      128.119.245.12   HTTP       566 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  133 8.130040    128.119.245.12   10.22.7.187      HTTP       492 HTTP/1.1 200 OK  (text/html)
  135 8.310493    10.22.7.187      128.119.245.12   HTTP       512 GET /favicon.ico HTTP/1.1
  136 8.435213    128.119.245.12   10.22.7.187      HTTP       538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 133: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) or
> Ethernet II, Src: Cisco_0b:d9:c4 (40:55:39:0b:d9:c4), Dst: CloudNet_bb:7e:b
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.22.7.187
> Transmission Control Protocol, Src Port: 80, Dst Port: 50451, Seq: 1, Ack:
> Hypertext Transfer Protocol
> Line-based text data: text/html (3 lines)
```

```
0000  50 c2 e8 bb 7e bf 40 55  39 0b d9 c4 08 00 45 00   P···~·@U 9·····E·
0010  01 de a9 93 40 00 22 06  26 32 80 77 f5 0c 0a 16   ····@·"· &2·w····
0020  07 bb 00 50 c5 13 81 1f  df 8d 2e e8 b1 14 50 18   ···P···· ··.···P·
0030  00 ed d6 e8 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 54 75 65   00 OK··D ate: Tue
0050  2c 20 31 37 20 4a 61 6e  20 32 30 32 33 20 30 39   , 17 Jan  2023 09
0060  3a 33 32 3a 31 31 20 47  4d 54 0d 0a 53 65 72 76   :32:11 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS ) OpenSS
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2k -fips PH
00a0  50 2f 37 2e 34 2e 33 30  20 6d 6f 64 5f 70 65 72   P/7.4.30  mod_per
00b0  6c 2f 32 2e 30 2e 31 31  20 50 65 72 6c 2f 76 35   l/2.0.11  Perl/v5
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
00d0  66 69 65 64 3a 20 54 75  65 2c 20 31 37 20 4a 61   fied: Tu e, 17 Ja
00e0  6e 20 32 30 32 33 20 30  36 3a 35 39 3a 30 32 20   n 2023 0 6:59:02
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 35 31 2d 35   GMT··ETa g: "51-5
0100  66 32 37 30 33 63 31 38  32 37 38 36 22 0d 0a 41   f2703c18 2786"··A
```

Frame (frame), 492 byte(s)   Packets: 211 · Displayed: 4 (1.9%) · Dropped: 0 (0.0%)   Profile: Default