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

HTTP, TCP TLSv1.3

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.)

I took 0.078823 seconds from when the HTTP GET message was sent until the HTTP OK reply was received.

```
165 11.551084 10.249.199.227      128.119.245.12      HTTP      539 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

174 11.629907 128.119.245.12      10.249.199.227      HTTP      492 HTTP/1.1 200 OK  (text/html)
```

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?
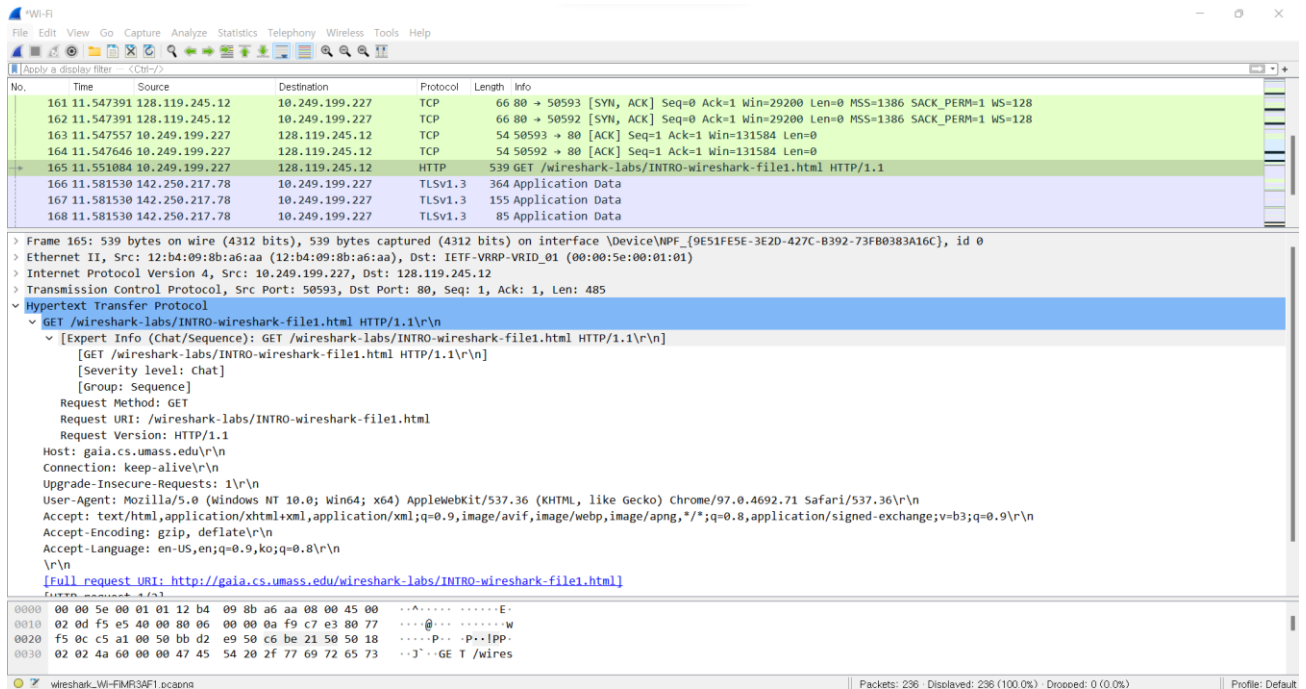
The internet address of the gaia.cs.umass.edu is 128.119.245.12.

The internet address of my computer is 10.249.199.227.

```
165 11.551084 10.249.199.227      128.119.245.12      HTTP      539 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

174 11.629907 128.119.245.12      10.249.199.227      HTTP      492 HTTP/1.1 200 OK  (text/html)
```

4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the "Selected Packet Only" and "Print as displayed" radial buttons, and then click OK.

\<HTTP GET message>

```
161 11.547391 128.119.245.12    10.249.199.227    TCP   66 80 → 50593 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1386 SACK_PERM=1 WS=128
162 11.547391 128.119.245.12    10.249.199.227    TCP   66 80 → 50592 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1386 SACK_PERM=1 WS=128
163 11.547557 10.249.199.227    128.119.245.12    TCP   54 50593 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
164 11.547646 10.249.199.227    128.119.245.12    TCP   54 50592 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
165 11.551084 10.249.199.227    128.119.245.12    HTTP  539 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
166 11.581530 142.250.217.78    10.249.199.227    TLSv1.3  364 Application Data
167 11.581530 142.250.217.78    10.249.199.227    TLSv1.3  155 Application Data
168 11.581530 142.250.217.78    10.249.199.227    TLSv1.3  85 Application Data
```

```
> Frame 165: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits) on interface \Device\NPF_{9E51FE5E-3E2D-427C-B392-73FB0383A16C}, id 0
> Ethernet II, Src: 12:b4:09:8b:a6:aa (12:b4:09:8b:a6:aa), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 10.249.199.227, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50593, Dst Port: 80, Seq: 1, Ack: 1, Len: 485
v Hypertext Transfer Protocol
  v GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
        [GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/INTRO-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\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/97.0.4692.71 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,ko;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
```

```
0000  00 00 5e 00 01 01 12 b4  09 8b a6 aa 08 00 45 00   ··^···· ······E·
0010  02 0d f5 e5 40 00 80 06  00 00 0a f9 c7 e3 80 77   ····@··· ·······w
0020  f5 0c c5 a1 00 50 bb d2  e9 50 c6 be 21 50 50 18   ·····P·· ·P··!PP·
0030  02 02 4a 60 00 00 47 45  54 20 2f 77 69 72 65 73   ··J`··GE T /wires
```

Packets: 236 · Displayed: 236 (100.0%) · Dropped: 0 (0.0%)   Profile: Default

\<HTTP OK message>

```
167 11.581530 142.250.217.78    10.249.199.227    TLSv1.3  155 Application Data
168 11.581530 142.250.217.78    10.249.199.227    TLSv1.3  85 Application Data
169 11.581530 142.250.217.78    10.249.199.227    TLSv1.3  93 Application Data
170 11.581738 10.249.199.227    142.250.217.78    TCP   54 50594 → 443 [ACK] Seq=1404 Ack=7755 Win=130304 Len=0
171 11.582883 10.249.199.227    142.250.217.78    TLSv1.3  93 Application Data
172 11.590662 142.250.217.78    10.249.199.227    TCP   56 443 → 50594 [ACK] Seq=7755 Ack=1443 Win=68864 Len=0
173 11.628478 128.119.245.12    10.249.199.227    TCP   56 80 → 50593 [ACK] Seq=1 Ack=486 Win=30336 Len=0
174 11.629907 128.119.245.12    10.249.199.227    HTTP  492 HTTP/1.1 200 OK  (text/html)
```

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 50593, Seq: 1, Ack: 486, Len: 438
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Tue, 11 Jan 2022 23:31:17 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 11 Jan 2022 06:59:02 GMT\r\n
    ETag: "51-5d548fcfa00be"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 81\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.078822000 seconds]
```

```
0000  12 b4 09 8b a6 aa 40 b9  3c 45 60 de 08 00 45 00   ······@· <E`···E·
0010  01 de 53 d4 40 00 25 06  b7 e5 80 77 f5 0c 0a f9   ··S·@·%· ···w····
0020  c7 e3 00 50 c5 a1 c6 be  21 50 bb d2 eb 35 50 18   ···P···· !P···5P·
0030  00 ed 42 87 00 00 48 54  54 50 2f 31 2e 31 20 32   ··B···HT TP/1.1 2
```

Packets: 236 · Displayed: 236 (100.0%) · Dropped: 0 (0.0%)   Profile: Default