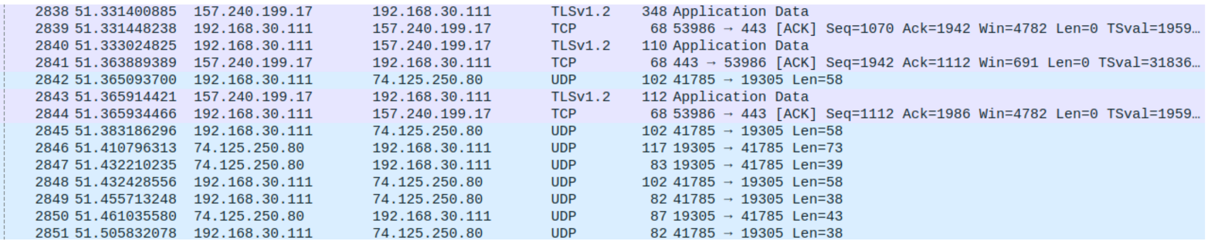
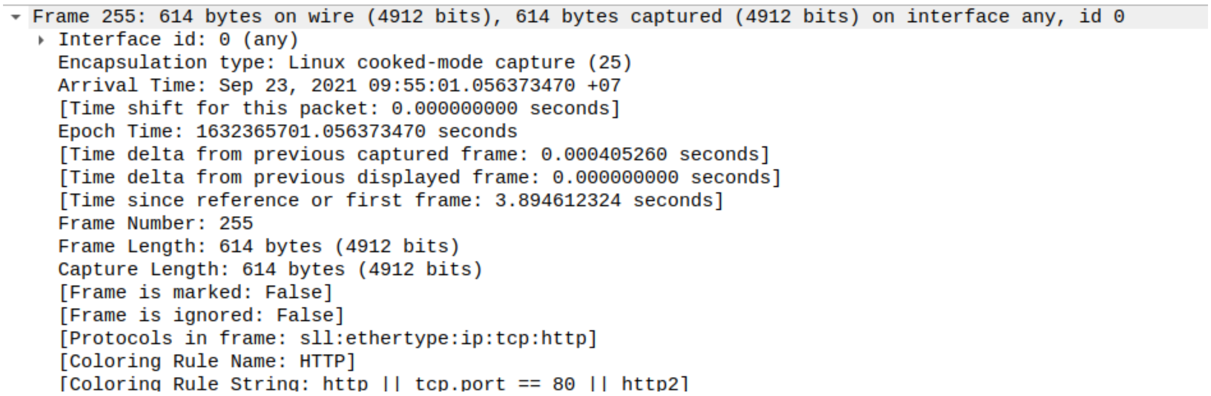
Câu 1: List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.



```
2838 51.331400885  157.240.199.17      192.168.30.111      TLSv1.2    348 Application Data
2839 51.331448238  192.168.30.111      157.240.199.17      TCP         68 53986 → 443 [ACK] Seq=1070 Ack=1942 Win=4782 Len=0 TSval=1959…
2840 51.333024825  192.168.30.111      157.240.199.17      TLSv1.2    110 Application Data
2841 51.363889389  157.240.199.17      192.168.30.111      TCP         68 443 → 53986 [ACK] Seq=1942 Ack=1112 Win=691 Len=0 TSval=31836…
2842 51.365093700  192.168.30.111      74.125.250.80       UDP        102 41785 → 19305 Len=58
2843 51.365914421  157.240.199.17      192.168.30.111      TLSv1.2    112 Application Data
2844 51.365934466  192.168.30.111      157.240.199.17      TCP         68 53986 → 443 [ACK] Seq=1112 Ack=1986 Win=4782 Len=0 TSval=1959…
2845 51.383186296  192.168.30.111      74.125.250.80       UDP        102 41785 → 19305 Len=58
2846 51.410796313  74.125.250.80       192.168.30.111      UDP        117 19305 → 41785 Len=73
2847 51.432210235  74.125.250.80       192.168.30.111      UDP         83 19305 → 41785 Len=39
2848 51.432428556  192.168.30.111      74.125.250.80       UDP        102 41785 → 19305 Len=58
2849 51.455713248  192.168.30.111      74.125.250.80       UDP         82 41785 → 19305 Len=38
2850 51.461035580  74.125.250.80       192.168.30.111      UDP         87 19305 → 41785 Len=43
2851 51.505832078  192.168.30.111      74.125.250.80       UDP         82 41785 → 19305 Len=38
```

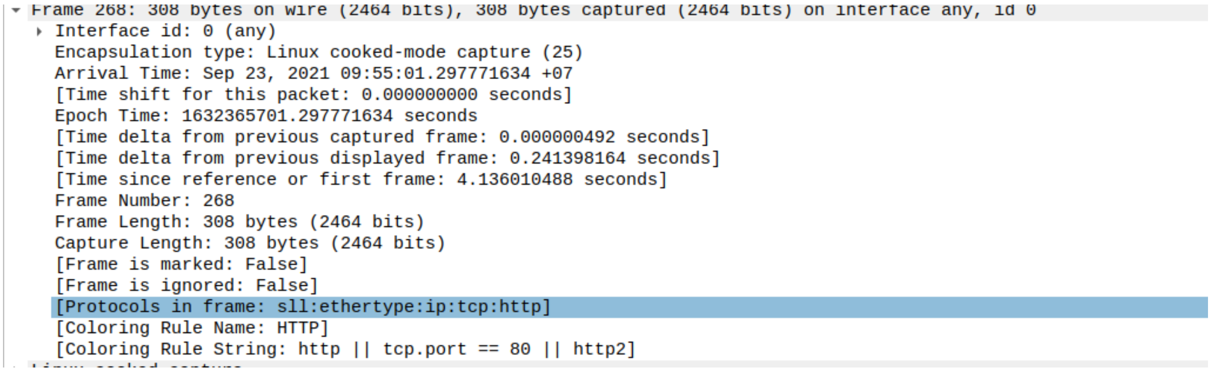
Câu 2: How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packetlisting window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the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

HTTP GET



```
▾ Frame 255: 614 bytes on wire (4912 bits), 614 bytes captured (4912 bits) on interface any, id 0
  ▸ Interface id: 0 (any)
    Encapsulation type: Linux cooked-mode capture (25)
    Arrival Time: Sep 23, 2021 09:55:01.056373470 +07
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1632365701.056373470 seconds
    [Time delta from previous captured frame: 0.000405260 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 3.894612324 seconds]
    Frame Number: 255
    Frame Length: 614 bytes (4912 bits)
    Capture Length: 614 bytes (4912 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: sll:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
```

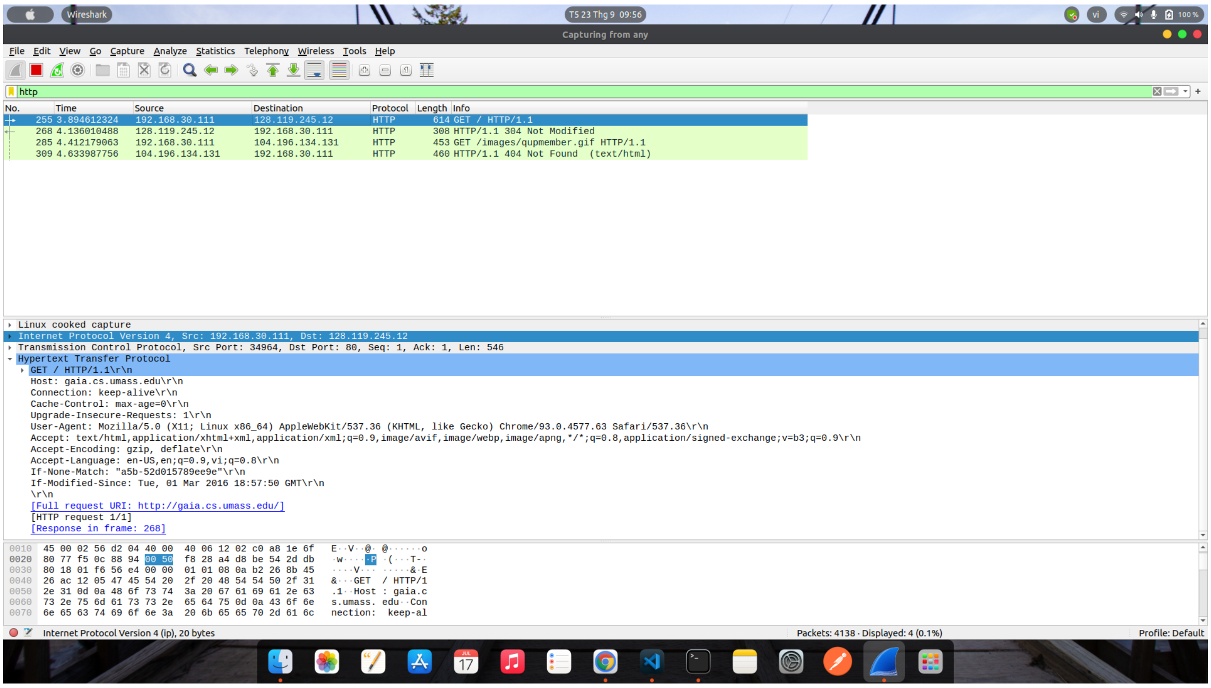
HTTP OK



```
▾ Frame 268: 308 bytes on wire (2464 bits), 308 bytes captured (2464 bits) on interface any, id 0
  ▸ Interface id: 0 (any)
    Encapsulation type: Linux cooked-mode capture (25)
    Arrival Time: Sep 23, 2021 09:55:01.297771634 +07
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1632365701.297771634 seconds
    [Time delta from previous captured frame: 0.000000492 seconds]
    [Time delta from previous displayed frame: 0.241398164 seconds]
    [Time since reference or first frame: 4.136010488 seconds]
    Frame Number: 268
    Frame Length: 308 bytes (2464 bits)
    Capture Length: 308 bytes (2464 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: sll:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
```

Time =.2977771634-.056373470 = 0.2414036934 (s)

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



Wireshark
T5 23 Thg 9 09:56
Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.     Time          Source            Destination       Protocol  Length  Info
255 3.894612324   192.168.30.111    128.119.245.12    HTTP      614 GET / HTTP/1.1
268 4.136010488   128.119.245.12    192.168.30.111    HTTP      308 HTTP/1.1 304 Not Modified
285 4.412179063   192.168.30.111    104.196.134.131   HTTP      453 GET /images/qupmember.gif HTTP/1.1
309 4.633987756   104.196.134.131   192.168.30.111    HTTP      460 HTTP/1.1 404 Not Found  (text/html)
```

```
› Linux cooked capture
› Internet Protocol Version 4, Src: 192.168.30.111, Dst: 128.119.245.12
› Transmission Control Protocol, Src Port: 34964, Dst Port: 80, Seq: 1, Ack: 1, Len: 546
⌄ Hypertext Transfer Protocol
  › GET / HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 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,vi;q=0.8\r\n
    If-None-Match: "a5b-52d015789ee9e"\r\n
    If-Modified-Since: Tue, 01 Mar 2016 18:57:50 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/]
    [HTTP request 1/1]
    [Response in frame: 268]
```

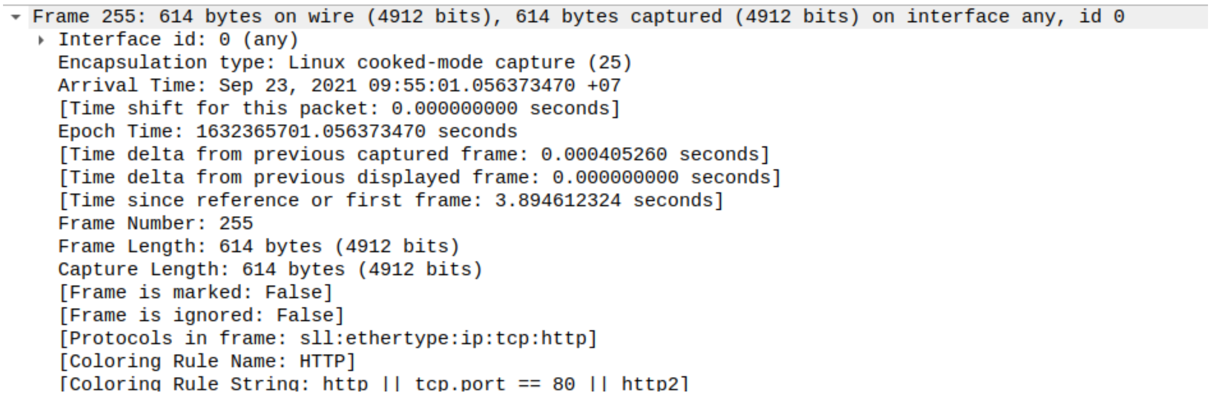
```
0010  45 00 02 56 d2 04 40 00  40 06 12 02 c0 a8 1e 6f   E··V··@· @······o
0020  80 77 f5 0c 88 94 00 50  f8 28 a4 d8 be 54 2d db   ·w·····P ·(···T-·
0030  80 18 01 f6 56 e4 00 00  01 01 08 0a b2 26 8b 45   ····V··· ·····&·E
0040  26 ac 12 05 47 45 54 20  2f 20 48 54 54 50 2f 31   &···GET  / HTTP/1
0050  2e 31 0d 0a 48 6f 73 74  3a 20 67 61 69 61 2e 63   .1··Host : gaia.c
0060  73 2e 75 6d 61 73 73 2e  65 64 75 0d 0a 43 6f 6e   s.umass. edu··Con
0070  6e 65 63 74 69 6f 6e 3a  20 6b 65 65 70 2d 61 6c   nection:  keep-al
```

Internet Protocol Version 4 (ip), 20 bytes
Packets: 4138 · Displayed: 4 (0.1%)
Profile: Default

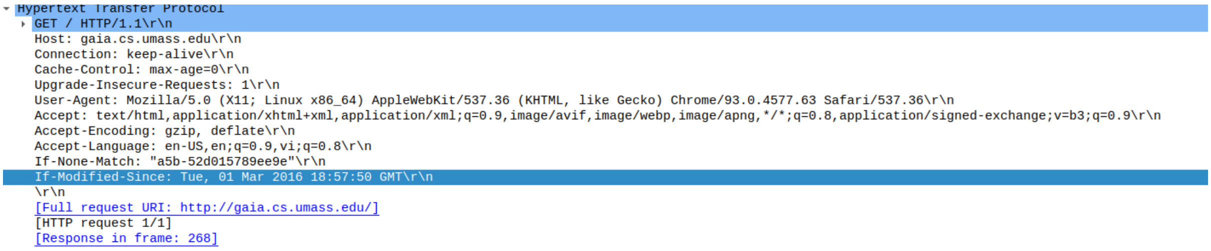
- Internet address of the gaia.cs.umass.edu: 128.119.245.12
- Internet address of my computer: 192.168.30.111

Câu 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

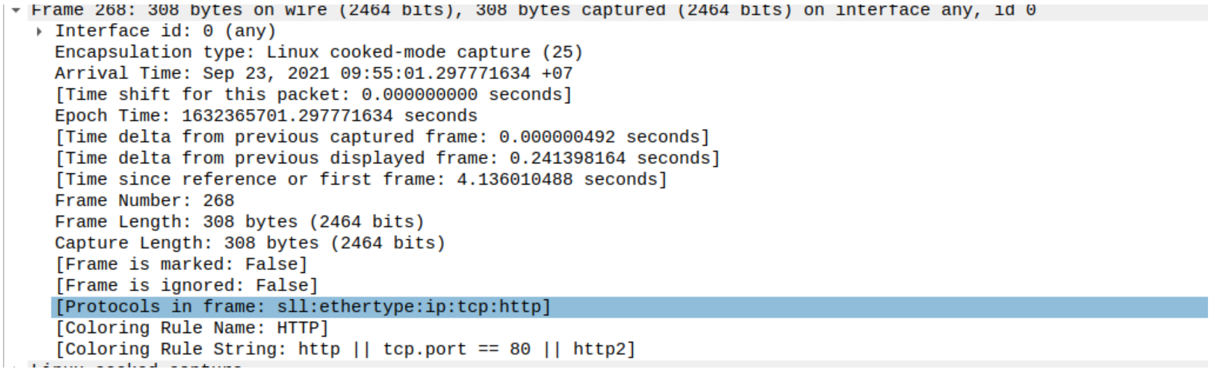


```
⌄ Frame 255: 614 bytes on wire (4912 bits), 614 bytes captured (4912 bits) on interface any, id 0
  › Interface id: 0 (any)
    Encapsulation type: Linux cooked-mode capture (25)
    Arrival Time: Sep 23, 2021 09:55:01.056373470 +07
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1632365701.056373470 seconds
    [Time delta from previous captured frame: 0.000405260 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 3.894612324 seconds]
    Frame Number: 255
    Frame Length: 614 bytes (4912 bits)
    Capture Length: 614 bytes (4912 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: sll:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
```

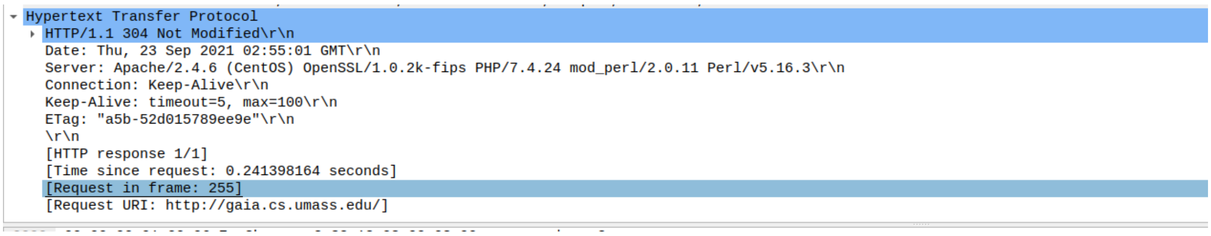


```
⌄ Hypertext Transfer Protocol
  › GET / HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36\r\n
    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,vi;q=0.8\r\n
    If-None-Match: "a5b-52d015789ee9e"\r\n
    If-Modified-Since: Tue, 01 Mar 2016 18:57:50 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/]
    [HTTP request 1/1]
    [Response in frame: 268]
```

HTTP OK



```
▾ Frame 268: 308 bytes on wire (2464 bits), 308 bytes captured (2464 bits) on interface any, id 0
  ▸ Interface id: 0 (any)
    Encapsulation type: Linux cooked-mode capture (25)
    Arrival Time: Sep 23, 2021 09:55:01.297771634 +07
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1632365701.297771634 seconds
    [Time delta from previous captured frame: 0.000000492 seconds]
    [Time delta from previous displayed frame: 0.241398164 seconds]
    [Time since reference or first frame: 4.136010488 seconds]
    Frame Number: 268
    Frame Length: 308 bytes (2464 bits)
    Capture Length: 308 bytes (2464 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: sll:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
  Linux cooked capture
```



```
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 304 Not Modified\r\n
    Date: Thu, 23 Sep 2021 02:55:01 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "a5b-52d015789ee9e"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.241398164 seconds]
    [Request in frame: 255]
    [Request URI: http://gaia.cs.umass.edu/]
```