William George
CS 372
Lab 1 WireShark Intro

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

   HTTP
   SSL
   TCP
   QUIC

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*.)**

   GET 273 11:55:27.030437
   OK 280 11:55:27.107289

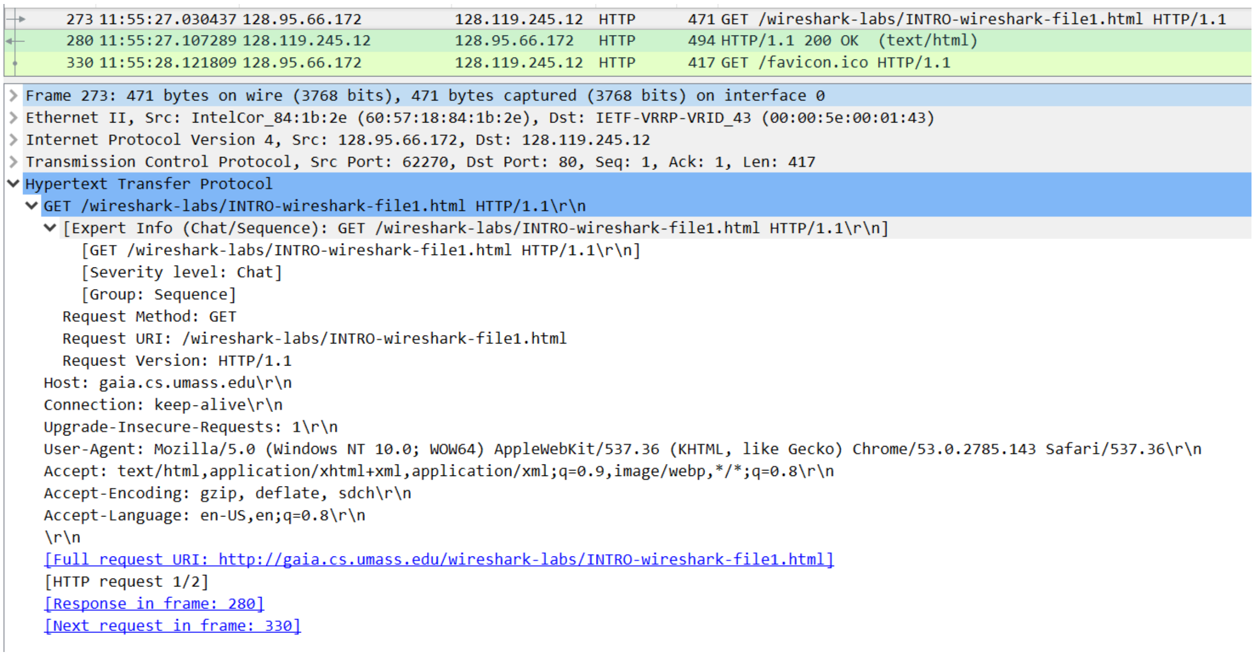
   Difference: .076852 Seconds

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?**

   gaia.cs.umass.edu IPv4 128.95.66.172
   Destination/My Computer 128.119.245.12

4. **Screenshot the two HTTP messages (GET and OK) referred to in question 2 above. Make sure to include all pertinent information in the screenshot (Time field, Internet addresses, etc). Paste these screenshots into your lab report.**

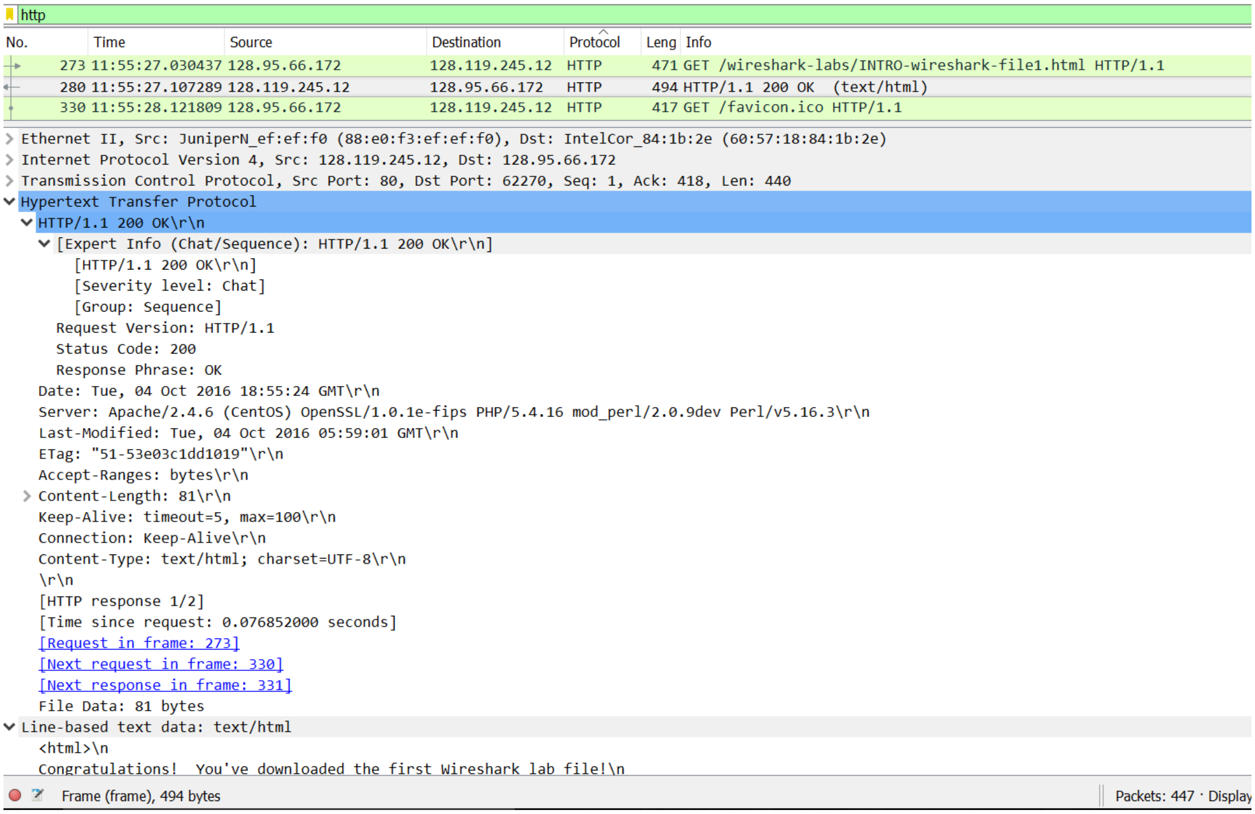
GET REQUEST:



```
273 11:55:27.030437 128.95.66.172      128.119.245.12  HTTP   471 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
280 11:55:27.107289 128.119.245.12     128.95.66.172   HTTP   494 HTTP/1.1 200 OK  (text/html)
330 11:55:28.121809 128.95.66.172      128.119.245.12  HTTP   417 GET /favicon.ico HTTP/1.1

> Frame 273: 471 bytes on wire (3768 bits), 471 bytes captured (3768 bits) on interface 0
> Ethernet II, Src: IntelCor_84:1b:2e (60:57:18:84:1b:2e), Dst: IETF-VRRP-VRID_43 (00:00:5e:00:01:43)
> Internet Protocol Version 4, Src: 128.95.66.172, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 62270, Dst Port: 80, Seq: 1, Ack: 1, Len: 417
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; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;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]
    [Response in frame: 280]
    [Next request in frame: 330]
```

OK RESPONSE:



```
No.   Time            Source          Destination     Protocol  Leng Info
  273 11:55:27.030437 128.95.66.172   128.119.245.12  HTTP       471 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  280 11:55:27.107289 128.119.245.12  128.95.66.172   HTTP       494 HTTP/1.1 200 OK  (text/html)
  330 11:55:28.121809 128.95.66.172   128.119.245.12  HTTP       417 GET /favicon.ico HTTP/1.1

> Ethernet II, Src: JuniperN_ef:ef:f0 (88:e0:f3:ef:ef:f0), Dst: IntelCor_84:1b:2e (60:57:18:84:1b:2e)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 128.95.66.172
> Transmission Control Protocol, Src Port: 80, Dst Port: 62270, Seq: 1, Ack: 418, Len: 440
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]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Date: Tue, 04 Oct 2016 18:55:24 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
    Last-Modified: Tue, 04 Oct 2016 05:59:01 GMT\r\n
    ETag: "51-53e03c1dd1019"\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: 0.076852000 seconds]
    [Request in frame: 273]
    [Next request in frame: 330]
    [Next response in frame: 331]
    File Data: 81 bytes
v Line-based text data: text/html
    <html>\n
    Congratulations!  You've downloaded the first Wireshark lab file!\n
```