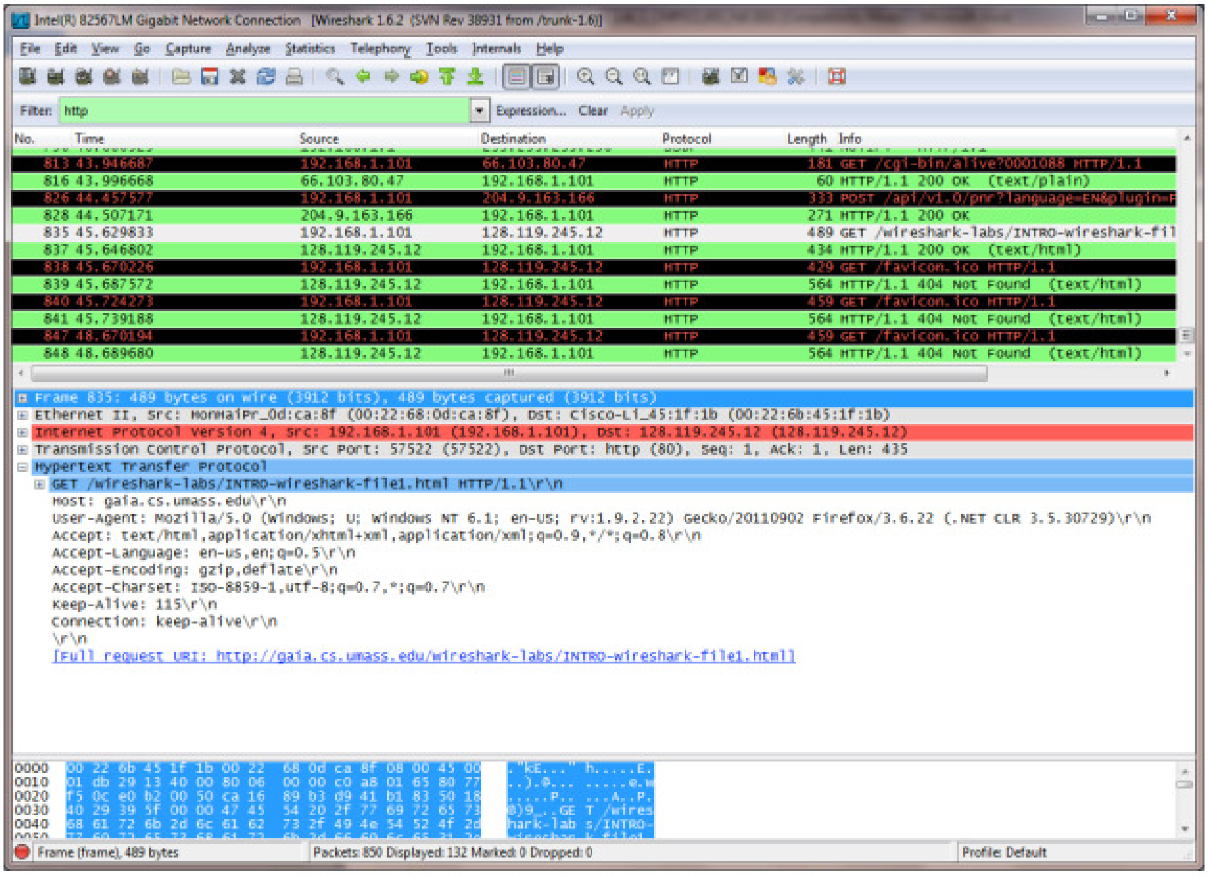

Intel(R) 82567LM Gigabit Network Connection [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply
Profile: Default

```
No.   Time        Source            Destination       Protocol   Length  Info
  813 43.946687   192.168.1.101     66.103.80.47      HTTP       181 GET /cgi-bin/alive?0001088 HTTP/1.1
  816 43.996668   66.103.80.47      192.168.1.101     HTTP        60 HTTP/1.1 200 OK  (text/plain)
  826 44.457577   192.168.1.101     204.9.163.166     HTTP       333 POST /api/v1.0/pnr?language=EN&plugin=F
  828 44.507171   204.9.163.166     192.168.1.101     HTTP       271 HTTP/1.1 200 OK
  835 45.629833   192.168.1.101     128.119.245.12    HTTP       489 GET /wireshark-labs/INTRO-wireshark-fil
  837 45.646802   128.119.245.12    192.168.1.101     HTTP       434 HTTP/1.1 200 OK  (text/html)
  838 45.670226   192.168.1.101     128.119.245.12    HTTP       429 GET /favicon.ico HTTP/1.1
  839 45.687572   128.119.245.12    192.168.1.101     HTTP       564 HTTP/1.1 404 Not Found  (text/html)
  840 45.724273   192.168.1.101     128.119.245.12    HTTP       459 GET /favicon.ico HTTP/1.1
  841 45.739188   128.119.245.12    192.168.1.101     HTTP       564 HTTP/1.1 404 Not Found  (text/html)
  847 48.670194   192.168.1.101     128.119.245.12    HTTP       459 GET /favicon.ico HTTP/1.1
  848 48.689680   128.119.245.12    192.168.1.101     HTTP       564 HTTP/1.1 404 Not Found  (text/html)
```

```
⊞ Frame 835: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
⊞ Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
⊞ Internet Protocol Version 4, Src: 192.168.1.101 (192.168.1.101), Dst: 128.119.245.12 (128.119.245.12)
⊞ Transmission Control Protocol, Src Port: 57522 (57522), Dst Port: http (80), Seq: 1, Ack: 1, Len: 435
⊟ Hypertext Transfer Protocol
  ⊞ GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.22) Gecko/20110902 Firefox/3.6.22 (.NET CLR 3.5.30729)\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 115\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

```
0000  00 22 6b 45 1f 1b 00 22  68 0d ca 8f 08 00 45 00   ."kE..." h.....E.
0010  01 db 29 13 40 00 80 06  00 00 c0 a8 01 65 80 77   ..).@... .....e.w
0020  f5 0c e0 b2 00 50 ca 16  89 b3 d9 41 b1 83 50 18   .....P.. ...A..P.
0030  40 29 39 5f 00 00 47 45  54 20 2f 77 69 72 65 73   @)9_..GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 49 4e 54 52 4f 2d   hark-lab s/INTRO-
```

Frame (frame), 489 bytes
Packets: 850 Displayed: 132 Marked: 0 Dropped: 0

Figure 5: Wireshark window after step 9

Questions for the Lab

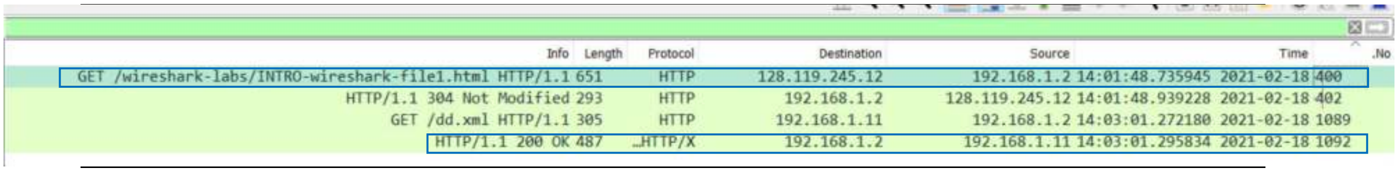
The goal of this first lab was primarily to introduce you to Wireshark. The following questions will demonstrate that you've been able to get Wireshark up and running, and have explored some of its capabilities. Answer the following questions, based on your Wireshark experimentation:

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

   HTTP protocol, TCP protocol, SSDP protocol, MDNS protocol

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.)



Info	Length	Protocol	Destination	Source	Time	.No
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1	651	HTTP	128.119.245.12	192.168.1.2	14:01:48.735945 2021-02-18	400
HTTP/1.1 304 Not Modified	293	HTTP	192.168.1.2	128.119.245.12	14:01:48.939228 2021-02-18	402
GET /dd.xml HTTP/1.1	305	HTTP	192.168.1.11	192.168.1.2	14:03:01.272180 2021-02-18	1089
HTTP/1.1 200 OK	487	..HTTP/X	192.168.1.2	192.168.1.11	14:03:01.295834 2021-02-18	1092

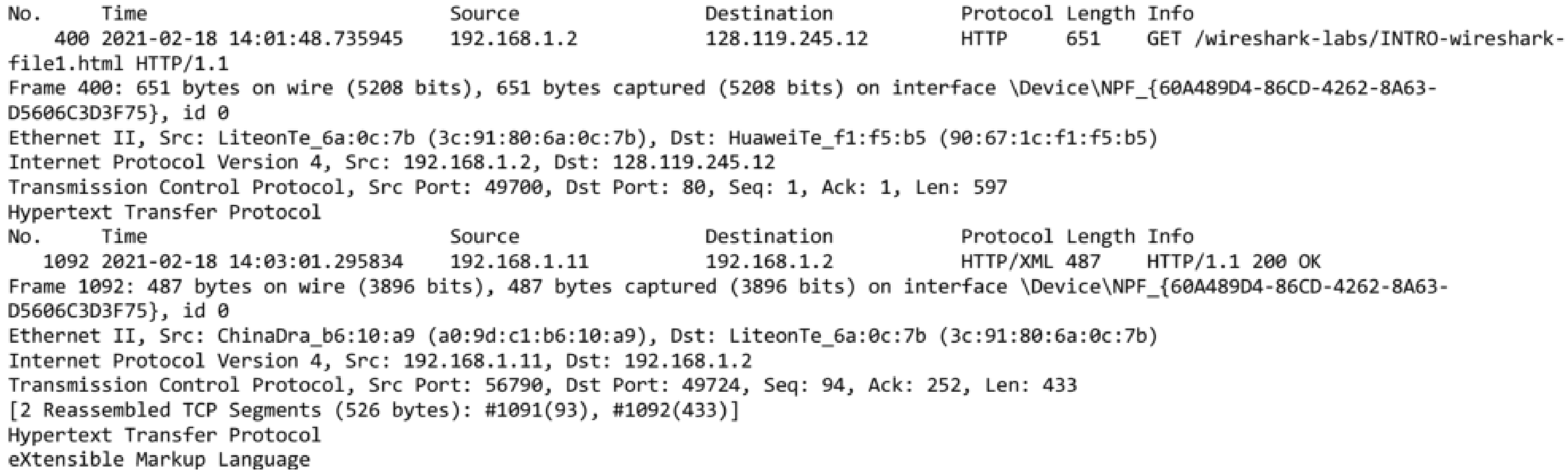
different between time response and time request is 0:01:12.559889

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?

Internet address of destination = 128.119.245.12

Internet address of my computer (source) = 192.168.1.2

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.



```
No.     Time                          Source                Destination           Protocol Length Info
    400 2021-02-18 14:01:48.735945    192.168.1.2           128.119.245.12        HTTP     651    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 400: 651 bytes on wire (5208 bits), 651 bytes captured (5208 bits) on interface \Device\NPF_{60A489D4-86CD-4262-8A63-
D5606C3D3F75}, id 0
Ethernet II, Src: LiteonTe_6a:0c:7b (3c:91:80:6a:0c:7b), Dst: HuaweiTe_f1:f5:b5 (90:67:1c:f1:f5:b5)
Internet Protocol Version 4, Src: 192.168.1.2, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49700, Dst Port: 80, Seq: 1, Ack: 1, Len: 597
Hypertext Transfer Protocol
No.     Time                          Source                Destination           Protocol Length Info
   1092 2021-02-18 14:03:01.295834    192.168.1.11          192.168.1.2           HTTP/XML 487    HTTP/1.1 200 OK
Frame 1092: 487 bytes on wire (3896 bits), 487 bytes captured (3896 bits) on interface \Device\NPF_{60A489D4-86CD-4262-8A63-
D5606C3D3F75}, id 0
Ethernet II, Src: ChinaDra_b6:10:a9 (a0:9d:c1:b6:10:a9), Dst: LiteonTe_6a:0c:7b (3c:91:80:6a:0c:7b)
Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.1.2
Transmission Control Protocol, Src Port: 56790, Dst Port: 49724, Seq: 94, Ack: 252, Len: 433
[2 Reassembled TCP Segments (526 bytes): #1091(93), #1092(433)]
Hypertext Transfer Protocol
eXtensible Markup Language
```