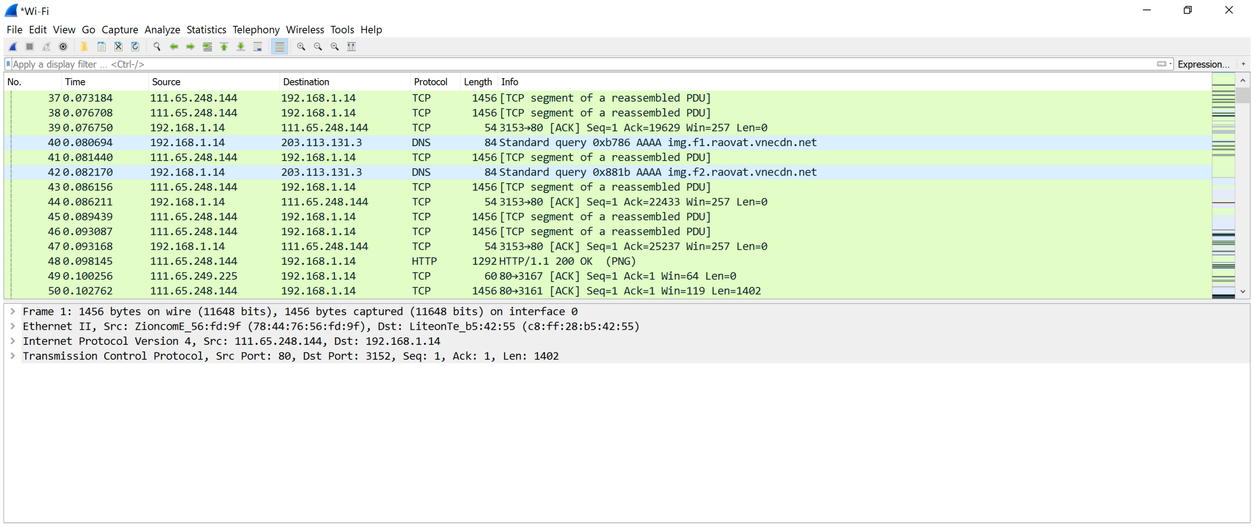
Wireshark Intro

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

   TCP, DNS, HTTP

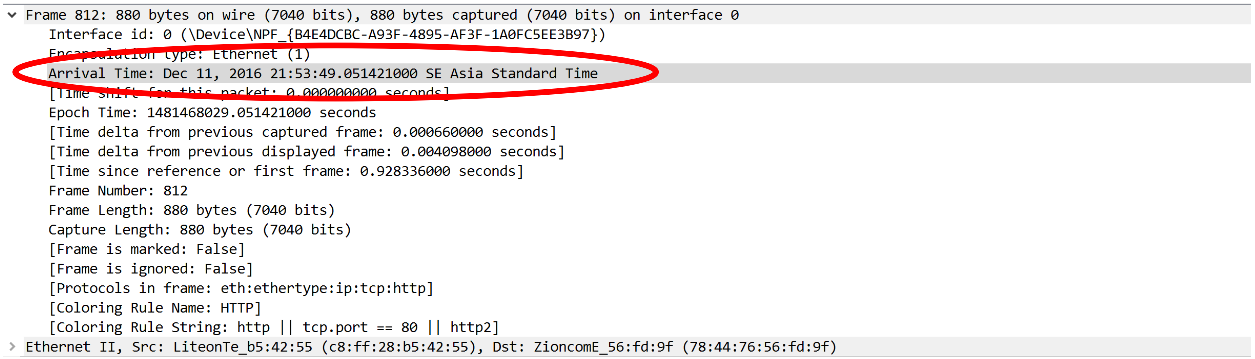

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.     Time      Source          Destination     Protocol Length Info
     37 0.073184  111.65.248.144  192.168.1.14    TCP      1456 [TCP segment of a reassembled PDU]
     38 0.076708  111.65.248.144  192.168.1.14    TCP      1456 [TCP segment of a reassembled PDU]
     39 0.076750  192.168.1.14    111.65.248.144  TCP        54 3153→80 [ACK] Seq=1 Ack=19629 Win=257 Len=0
     40 0.080694  192.168.1.14    203.113.131.3   DNS        84 Standard query 0xb786 AAAA img.f1.raovat.vnecdn.net
     41 0.081440  111.65.248.144  192.168.1.14    TCP      1456 [TCP segment of a reassembled PDU]
     42 0.082170  192.168.1.14    203.113.131.3   DNS        84 Standard query 0x881b AAAA img.f2.raovat.vnecdn.net
     43 0.086156  111.65.248.144  192.168.1.14    TCP      1456 [TCP segment of a reassembled PDU]
     44 0.086211  192.168.1.14    111.65.248.144  TCP        54 3153→80 [ACK] Seq=1 Ack=22433 Win=257 Len=0
     45 0.089439  111.65.248.144  192.168.1.14    TCP      1456 [TCP segment of a reassembled PDU]
     46 0.093087  111.65.248.144  192.168.1.14    TCP      1456 [TCP segment of a reassembled PDU]
     47 0.093168  192.168.1.14    111.65.248.144  TCP        54 3153→80 [ACK] Seq=1 Ack=25237 Win=257 Len=0
     48 0.098145  111.65.248.144  192.168.1.14    HTTP     1292 HTTP/1.1 200 OK  (PNG)
     49 0.100256  111.65.249.225  192.168.1.14    TCP        60 80→3167 [ACK] Seq=1 Ack=1 Win=64 Len=0
     50 0.102762  111.65.248.144  192.168.1.14    TCP      1456 80→3161 [ACK] Seq=1 Ack=1 Win=119 Len=1402

> Frame 1: 1456 bytes on wire (11648 bits), 1456 bytes captured (11648 bits) on interface 0
> Ethernet II, Src: ZioncomE_56:fd:9f (78:44:76:56:fd:9f), Dst: LiteonTe_b5:42:55 (c8:ff:28:b5:42:55)
> Internet Protocol Version 4, Src: 111.65.248.144, Dst: 192.168.1.14
> Transmission Control Protocol, Src Port: 80, Dst Port: 3152, Seq: 1, Ack: 1, Len: 1402
```

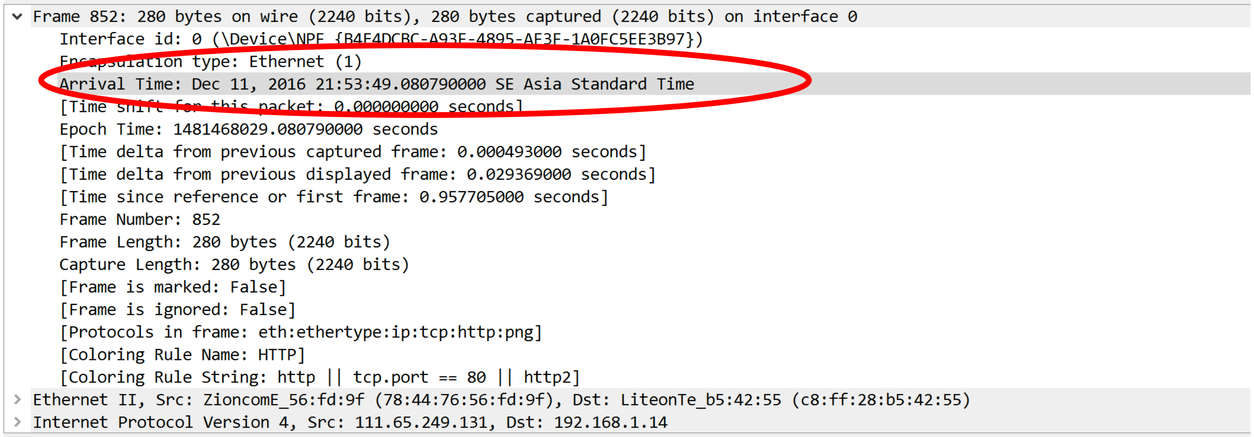
2. **How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the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

   GET request: the packet arrived at Arrival Time: Dec 11, 2016 21:53:49.051421000 SE Asia Standard Time



```
v Frame 812: 880 bytes on wire (7040 bits), 880 bytes captured (7040 bits) on interface 0
    Interface id: 0 (\Device\NPF_{B4E4DCBC-A93F-4895-AF3F-1A0FC5EE3B97})
    Encapsulation type: Ethernet (1)
    Arrival Time: Dec 11, 2016 21:53:49.051421000 SE Asia Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1481468029.051421000 seconds
    [Time delta from previous captured frame: 0.000660000 seconds]
    [Time delta from previous displayed frame: 0.004098000 seconds]
    [Time since reference or first frame: 0.928336000 seconds]
    Frame Number: 812
    Frame Length: 880 bytes (7040 bits)
    Capture Length: 880 bytes (7040 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: LiteonTe_b5:42:55 (c8:ff:28:b5:42:55), Dst: ZioncomE_56:fd:9f (78:44:76:56:fd:9f)
```

   HTTP OK: arrived at Arrival Time: Arrival Time: Dec 11, 2016 21:53:49.080790000 SE Asia Standard Time



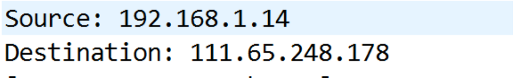
```
v Frame 852: 280 bytes on wire (2240 bits), 280 bytes captured (2240 bits) on interface 0
    Interface id: 0 (\Device\NPF_{B4E4DCBC-A93F-4895-AF3F-1A0FC5EE3B97})
    Encapsulation type: Ethernet (1)
    Arrival Time: Dec 11, 2016 21:53:49.080790000 SE Asia Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1481468029.080790000 seconds
    [Time delta from previous captured frame: 0.000493000 seconds]
    [Time delta from previous displayed frame: 0.029369000 seconds]
    [Time since reference or first frame: 0.957705000 seconds]
    Frame Number: 852
    Frame Length: 280 bytes (2240 bits)
    Capture Length: 280 bytes (2240 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:png]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: ZioncomE_56:fd:9f (78:44:76:56:fd:9f), Dst: LiteonTe_b5:42:55 (c8:ff:28:b5:42:55)
> Internet Protocol Version 4, Src: 111.65.249.131, Dst: 192.168.1.14
```

   The time differrence: . 080790000 - . 051421000 = 0.029369 sec

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?**

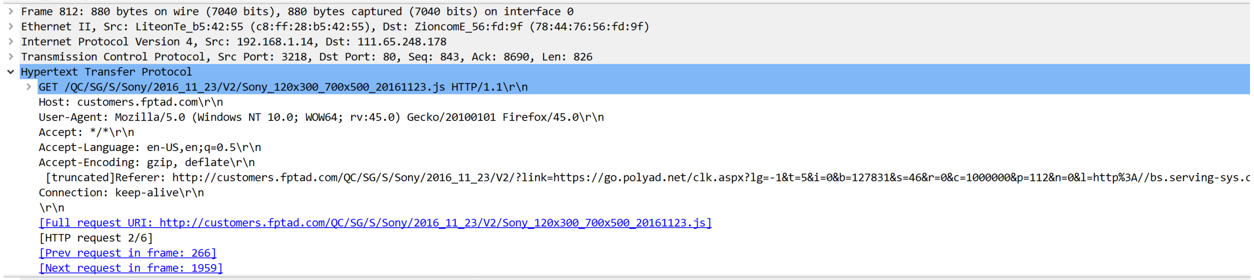
   IP address of my computer: 192.168.1.14

   www net.cs.umass.edu: 111.65.248.178

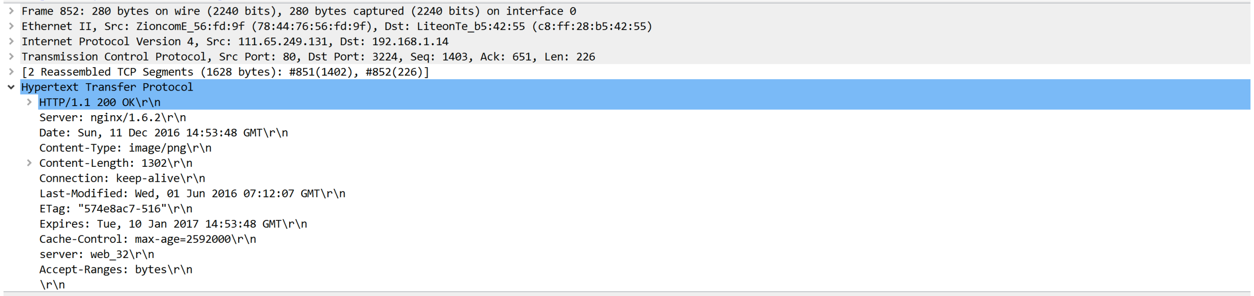


```
Source: 192.168.1.14
Destination: 111.65.248.178
```

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.**



```
Frame 812: 880 bytes on wire (7040 bits), 880 bytes captured (7040 bits) on interface 0
Ethernet II, Src: LiteonTe_b5:42:55 (c8:ff:28:b5:42:55), Dst: ZioncomE_56:fd:9f (78:44:76:56:fd:9f)
Internet Protocol Version 4, Src: 192.168.1.14, Dst: 111.65.248.178
Transmission Control Protocol, Src Port: 3218, Dst Port: 80, Seq: 843, Ack: 8690, Len: 826
Hypertext Transfer Protocol
  GET /QC/SG/S/Sony/2016_11_23/V2/Sony_120x300_700x500_20161123.js HTTP/1.1\r\n
  Host: customers.fptad.com\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0\r\n
  Accept: */*\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
   [truncated]Referer: http://customers.fptad.com/QC/SG/S/Sony/2016_11_23/V2/?link=https://go.polyad.net/clk.aspx?lg=-1&t=5&i=0&b=127831&s=46&r=0&c=1000000&p=112&n=0&l=http%3A//bs.serving-sys.c
  Connection: keep-alive\r\n
  \r\n
  [Full request URI: http://customers.fptad.com/QC/SG/S/Sony/2016_11_23/V2/Sony_120x300_700x500_20161123.js]
  [HTTP request 2/6]
  [Prev request in frame: 266]
  [Next request in frame: 1959]
```



```
Frame 852: 280 bytes on wire (2240 bits), 280 bytes captured (2240 bits) on interface 0
Ethernet II, Src: ZioncomE_56:fd:9f (78:44:76:56:fd:9f), Dst: LiteonTe_b5:42:55 (c8:ff:28:b5:42:55)
Internet Protocol Version 4, Src: 111.65.249.131, Dst: 192.168.1.14
Transmission Control Protocol, Src Port: 80, Dst Port: 3224, Seq: 1403, Ack: 651, Len: 226
[2 Reassembled TCP Segments (1628 bytes): #851(1402), #852(226)]
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Server: nginx/1.6.2\r\n
  Date: Sun, 11 Dec 2016 14:53:48 GMT\r\n
  Content-Type: image/png\r\n
  Content-Length: 1302\r\n
  Connection: keep-alive\r\n
  Last-Modified: Wed, 01 Jun 2016 07:12:07 GMT\r\n
  ETag: "574e8ac7-516"\r\n
  Expires: Tue, 10 Jan 2017 14:53:48 GMT\r\n
  Cache-Control: max-age=2592000\r\n
  server: web_32\r\n
  Accept-Ranges: bytes\r\n
  \r\n
```