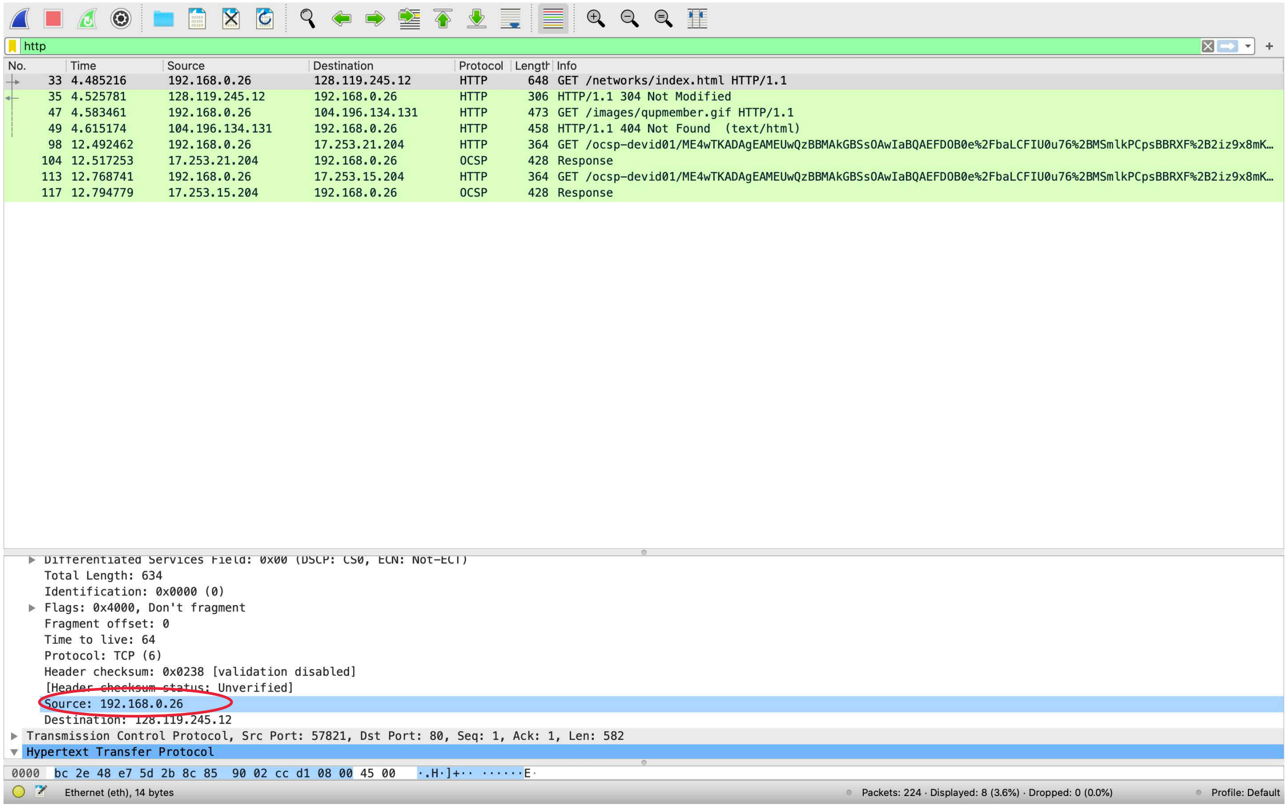
Zakaria Hilali

Course: IT-120

Lab 3

1. What is the Internet address of your computer?

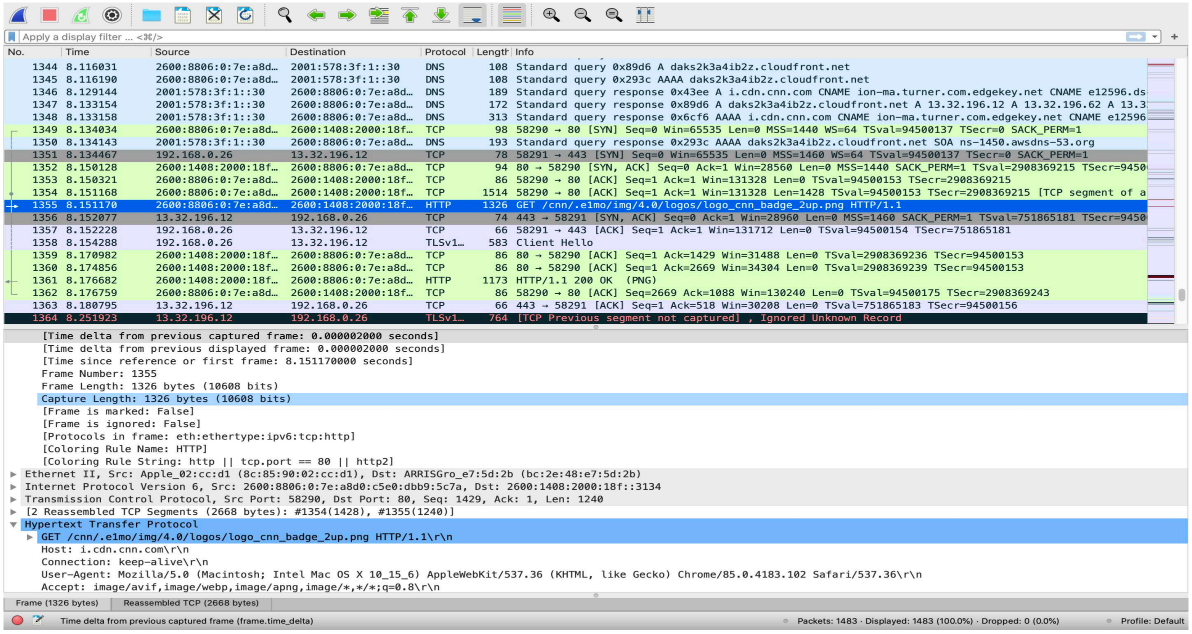
Answer: 192.168.0.26



```
http
No.   Time       Source           Destination      Protocol  Length Info
  33  4.485216   192.168.0.26     128.119.245.12   HTTP       648 GET /networks/index.html HTTP/1.1
  35  4.525781   128.119.245.12   192.168.0.26     HTTP       306 HTTP/1.1 304 Not Modified
  47  4.583461   192.168.0.26     104.196.134.131  HTTP       473 GET /images/qupmember.gif HTTP/1.1
  49  4.615174   104.196.134.131  192.168.0.26     HTTP       458 HTTP/1.1 404 Not Found  (text/html)
  98  12.492462  192.168.0.26     17.253.21.204    HTTP       364 GET /ocsp-devid01/ME4wTKADAgEAMEUwQzBBMAkGBSsOAwIaBQAEFDOB0e%2FbaLCFIU0u76%2BMSmlkPCpsBBRXF%2B2iz9x8mK…
 104  12.517253  17.253.21.204    192.168.0.26     OCSP       428 Response
 113  12.768741  192.168.0.26     17.253.15.204    HTTP       364 GET /ocsp-devid01/ME4wTKADAgEAMEUwQzBBMAkGBSsOAwIaBQAEFDOB0e%2FbaLCFIU0u76%2BMSmlkPCpsBBRXF%2B2iz9x8mK…
 117  12.794779  17.253.15.204    192.168.0.26     OCSP       428 Response

  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 634
    Identification: 0x0000 (0)
  ▶ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x0238 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.26
    Destination: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 57821, Dst Port: 80, Seq: 1, Ack: 1, Len: 582
▼ Hypertext Transfer Protocol

0000  bc 2e 48 e7 5d 2b 8c 85  90 02 cc d1 08 00 45 00   ·.H·]+·· ······E·

Ethernet (eth), 14 bytes        Packets: 224 · Displayed: 8 (3.6%) · Dropped: 0 (0.0%)        Profile: Default
```

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

Answer: TCP, HTTP, DNS.



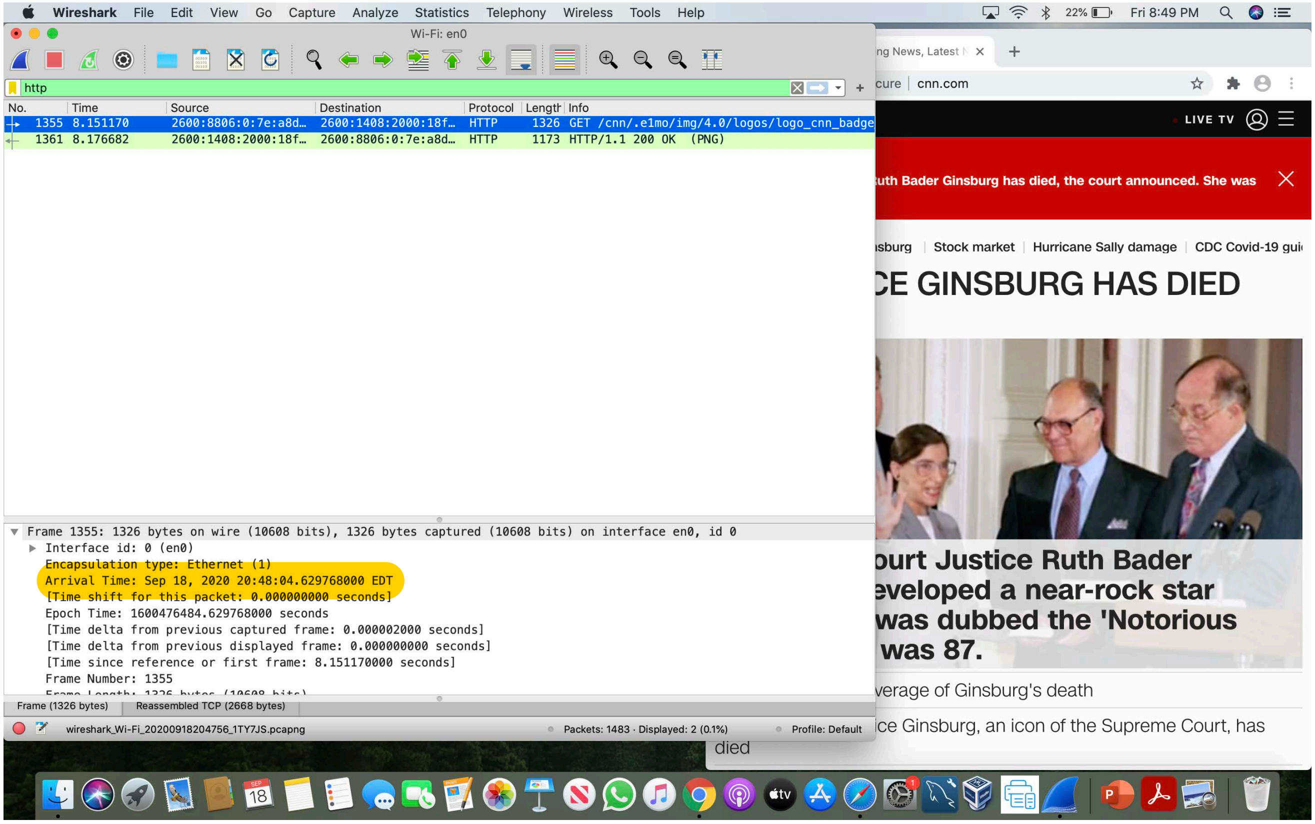
```
Apply a display filter ... <⌘/>
No.   Time      Source                Destination           Protocol  Length Info
1344  8.116031  2600:8806:0:7e:a8d…   2001:578:3f:1::30     DNS        108 Standard query 0x89d6 A daks2k3a4ib2z.cloudfront.net
1345  8.116190  2600:8806:0:7e:a8d…   2001:578:3f:1::30     DNS        108 Standard query 0x293c AAAA daks2k3a4ib2z.cloudfront.net
1346  8.129144  2001:578:3f:1::30     2600:8806:0:7e:a8d…   DNS        189 Standard query response 0x43ee A i.cdn.cnn.com CNAME ion-ma.turner.com.edgekey.net CNAME e12596.ds
1347  8.133154  2001:578:3f:1::30     2600:8806:0:7e:a8d…   DNS        172 Standard query response 0x89d6 A daks2k3a4ib2z.cloudfront.net A 13.32.196.12 A 13.32.196.62 A 13.3
1348  8.133158  2001:578:3f:1::30     2600:8806:0:7e:a8d…   DNS        313 Standard query response 0x6cf6 AAAA i.cdn.cnn.com CNAME ion-ma.turner.com.edgekey.net CNAME e12596
1349  8.134034  2600:8806:0:7e:a8d…   2600:1408:2000:18f…   TCP         98 58290 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=94500137 TSecr=0 SACK_PERM=1
1350  8.134143  2001:578:3f:1::30     2600:8806:0:7e:a8d…   DNS        193 Standard query response 0x293c AAAA daks2k3a4ib2z.cloudfront.net SOA ns-1450.awsdns-53.org
1351  8.134467  192.168.0.26          13.32.196.12          TCP         78 58291 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=94500137 TSecr=0 SACK_PERM=1
1352  8.150128  2600:1408:2000:18f…   2600:8806:0:7e:a8d…   TCP         94 80 → 58290 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=2908369215 TSecr=9450
1353  8.150321  2600:8806:0:7e:a8d…   2600:1408:2000:18f…   TCP         86 58290 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 TSval=94500153 TSecr=2908369215
1354  8.151168  2600:8806:0:7e:a8d…   2600:1408:2000:18f…   TCP       1514 58290 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=1428 TSval=94500153 TSecr=2908369215 [TCP segment of a
1355  8.151170  2600:8806:0:7e:a8d…   2600:1408:2000:18f…   HTTP      1326 GET /cnn/.e1mo/img/4.0/logos/logo_cnn_badge_2up.png HTTP/1.1
1356  8.152077  13.32.196.12          192.168.0.26          TCP         74 443 → 58291 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=751865181 TSecr=9450
1357  8.152228  192.168.0.26          13.32.196.12          TCP         66 58291 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=94500154 TSecr=751865181
1358  8.154288  192.168.0.26          13.32.196.12          TLSv1…     583 Client Hello
1359  8.170982  2600:1408:2000:18f…   2600:8806:0:7e:a8d…   TCP         86 80 → 58290 [ACK] Seq=1 Ack=1429 Win=31488 Len=0 TSval=2908369236 TSecr=94500153
1360  8.174856  2600:1408:2000:18f…   2600:8806:0:7e:a8d…   TCP         86 80 → 58290 [ACK] Seq=1 Ack=2669 Win=34304 Len=0 TSval=2908369239 TSecr=94500153
1361  8.176682  2600:1408:2000:18f…   2600:8806:0:7e:a8d…   HTTP      1173 HTTP/1.1 200 OK  (PNG)
1362  8.176759  2600:8806:0:7e:a8d…   2600:1408:2000:18f…   TCP         86 58290 → 80 [ACK] Seq=2669 Ack=1088 Win=130240 Len=0 TSval=94500175 TSecr=2908369243
1363  8.180795  13.32.196.12          192.168.0.26          TCP         66 443 → 58291 [ACK] Seq=1 Ack=518 Win=30208 Len=0 TSval=751865183 TSecr=94500156
1364  8.251923  13.32.196.12          192.168.0.26          TLSv1…     764 [TCP Previous segment not captured] , Ignored Unknown Record

    [Time delta from previous captured frame: 0.000002000 seconds]
    [Time delta from previous displayed frame: 0.000002000 seconds]
    [Time since reference or first frame: 8.151170000 seconds]
    Frame Number: 1355
    Frame Length: 1326 bytes (10608 bits)
    Capture Length: 1326 bytes (10608 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
▶ Ethernet II, Src: Apple_02:cc:d1 (8c:85:90:02:cc:d1), Dst: ARRISGro_e7:5d:2b (bc:2e:48:e7:5d:2b)
▶ Internet Protocol Version 6, Src: 2600:8806:0:7e:a8d0:c5e0:dbb9:5c7a, Dst: 2600:1408:2000:18f::3134
▶ Transmission Control Protocol, Src Port: 58290, Dst Port: 80, Seq: 1429, Ack: 1, Len: 1240
▶ [2 Reassembled TCP Segments (2668 bytes): #1354(1428), #1355(1240)]
▼ Hypertext Transfer Protocol
  ▶ GET /cnn/.e1mo/img/4.0/logos/logo_cnn_badge_2up.png HTTP/1.1\r\n
    Host: i.cdn.cnn.com\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36\r\n
    Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8\r\n

Frame (1326 bytes)   Reassembled TCP (2668 bytes)
Time delta from previous captured frame (frame.time_delta)   Packets: 1483 · Displayed: 1483 (100.0%) · Dropped: 0 (0.0%)   Profile: Default
```

3. 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.)

Answer:

- Arrival time of GET request is: Sep 18, 2020 20:48:04.629768000
- Arrival time of HTTP OK is: Sep 18, 2020 20:48:04.655280000

  Difference: 0.655280-0.629768=0.025512 sec.

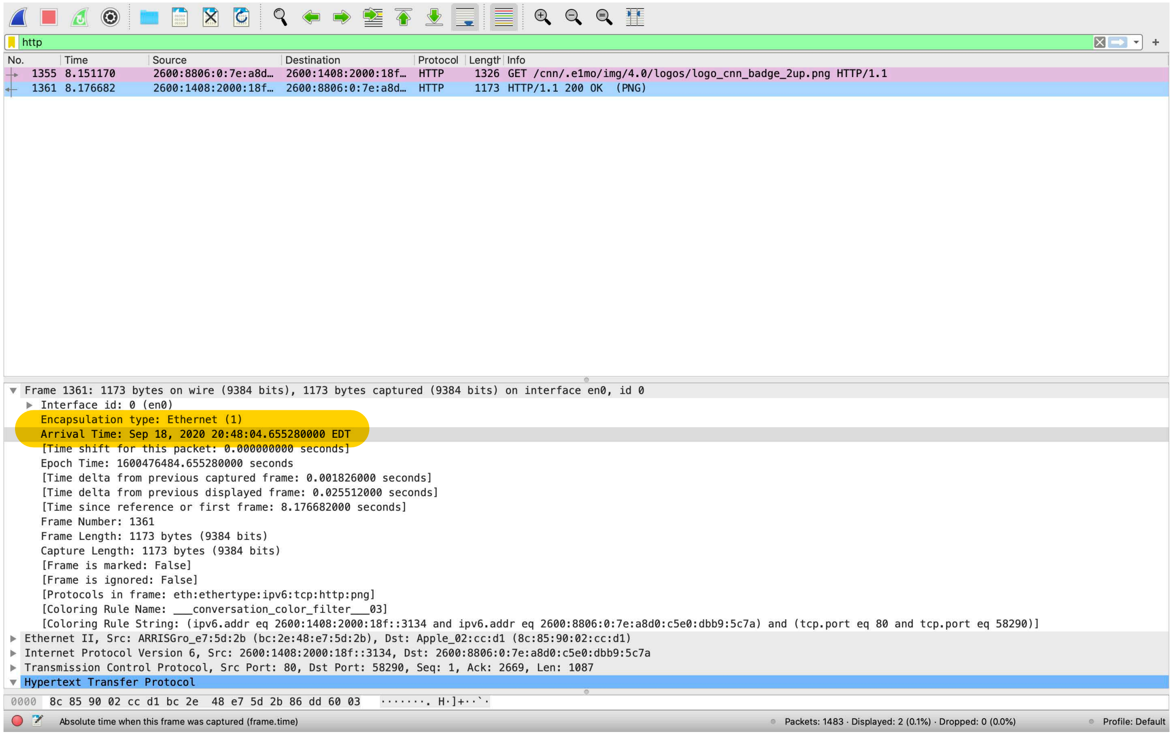


Wireshark
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
22%
Fri 8:49 PM
Wi-Fi: en0
ng News, Latest
cure
cnn.com
LIVE TV
uth Bader Ginsburg has died, the court announced. She was
sburg
Stock market
Hurricane Sally damage
CDC Covid-19 gui
CE GINSBURG HAS DIED
ourt Justice Ruth Bader
eveloped a near-rock star
was dubbed the 'Notorious
was 87.
verage of Ginsburg's death
ice Ginsburg, an icon of the Supreme Court, has
died
Frame (1326 bytes)
Reassembled TCP (2668 bytes)
wireshark_Wi-Fi_20200918204756_1TY7JS.pcapng
Packets: 1483 · Displayed: 2 (0.1%)
Profile: Default

http

```
No.   Time      Source               Destination          Protocol  Length  Info
1355  8.151170  2600:8806:0:7e:a8d…  2600:1408:2000:18f…  HTTP      1326    GET /cnn/.e1mo/img/4.0/logos/logo_cnn_badge
1361  8.176682  2600:1408:2000:18f…  2600:8806:0:7e:a8d…  HTTP      1173    HTTP/1.1 200 OK  (PNG)
```

```
▼ Frame 1355: 1326 bytes on wire (10608 bits), 1326 bytes captured (10608 bits) on interface en0, id 0
  ▶ Interface id: 0 (en0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 18, 2020 20:48:04.629768000 EDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1600476484.629768000 seconds
    [Time delta from previous captured frame: 0.000002000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 8.151170000 seconds]
    Frame Number: 1355
    Frame Length: 1326 bytes (10608 bits)
```

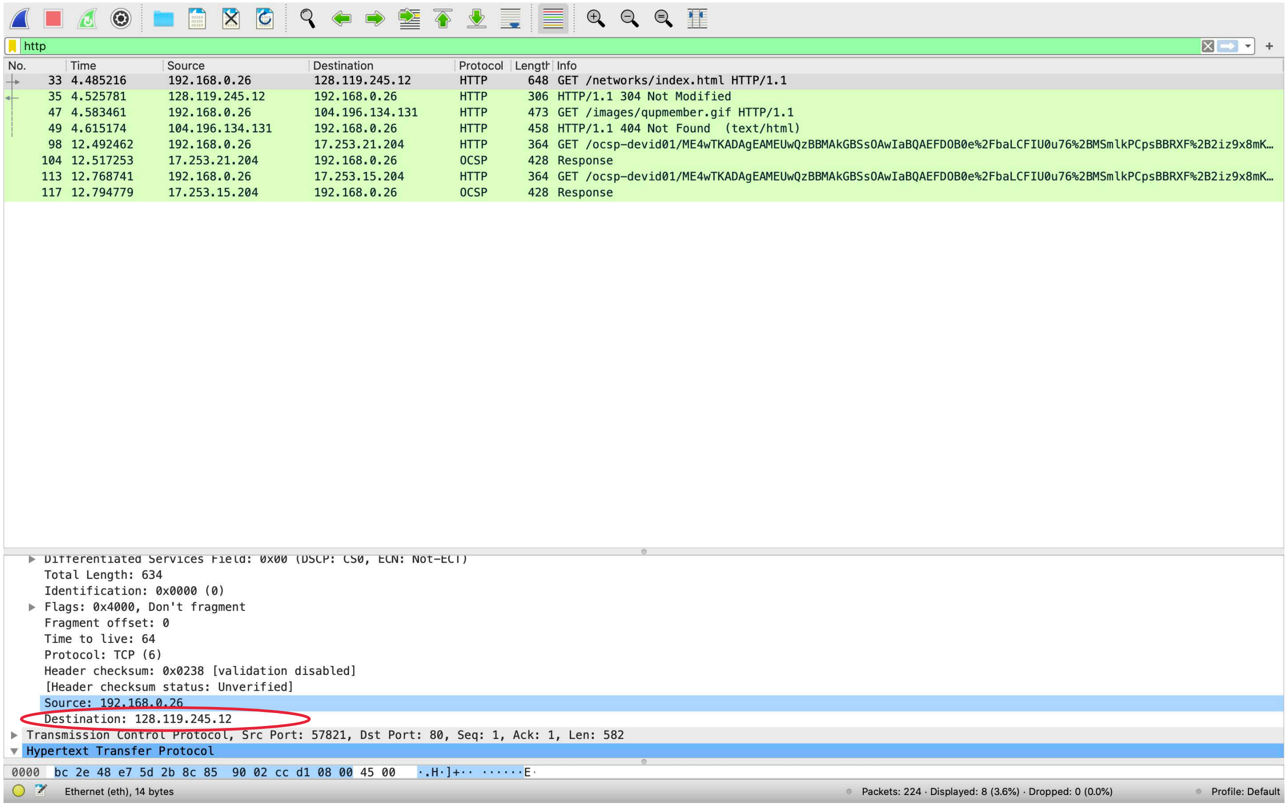


```
http
No.    Time      Source               Destination          Protocol Length Info
 1355  8.151170  2600:8806:0:7e:a8d…  2600:1408:2000:18f…  HTTP     1326   GET /cnn/.e1mo/img/4.0/logos/logo_cnn_badge_2up.png HTTP/1.1
 1361  8.176682  2600:1408:2000:18f…  2600:8806:0:7e:a8d…  HTTP     1173   HTTP/1.1 200 OK  (PNG)
```

```
▼ Frame 1361: 1173 bytes on wire (9384 bits), 1173 bytes captured (9384 bits) on interface en0, id 0
  ▶ Interface id: 0 (en0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 18, 2020 20:48:04.655280000 EDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1600476484.655280000 seconds
    [Time delta from previous captured frame: 0.001826000 seconds]
    [Time delta from previous displayed frame: 0.025512000 seconds]
    [Time since reference or first frame: 8.176682000 seconds]
    Frame Number: 1361
    Frame Length: 1173 bytes (9384 bits)
    Capture Length: 1173 bytes (9384 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:tcp:http:png]
    [Coloring Rule Name: ___conversation_color_filter___03]
    [Coloring Rule String: (ipv6.addr eq 2600:1408:2000:18f::3134 and ipv6.addr eq 2600:8806:0:7e:a8d0:c5e0:dbb9:5c7a) and (tcp.port eq 80 and tcp.port eq 58290)]
▶ Ethernet II, Src: ARRISGro_e7:5d:2b (bc:2e:48:e7:5d:2b), Dst: Apple_02:cc:d1 (8c:85:90:02:cc:d1)
▶ Internet Protocol Version 6, Src: 2600:1408:2000:18f::3134, Dst: 2600:8806:0:7e:a8d0:c5e0:dbb9:5c7a
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 58290, Seq: 1, Ack: 2669, Len: 1087
▼ Hypertext Transfer Protocol

0000  8c 85 90 02 cc d1 bc 2e  48 e7 5d 2b 86 dd 60 03   ·······. H·]+··`·

Absolute time when this frame was captured (frame.time)        Packets: 1483 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%)        Profile: Default
```

4. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)?

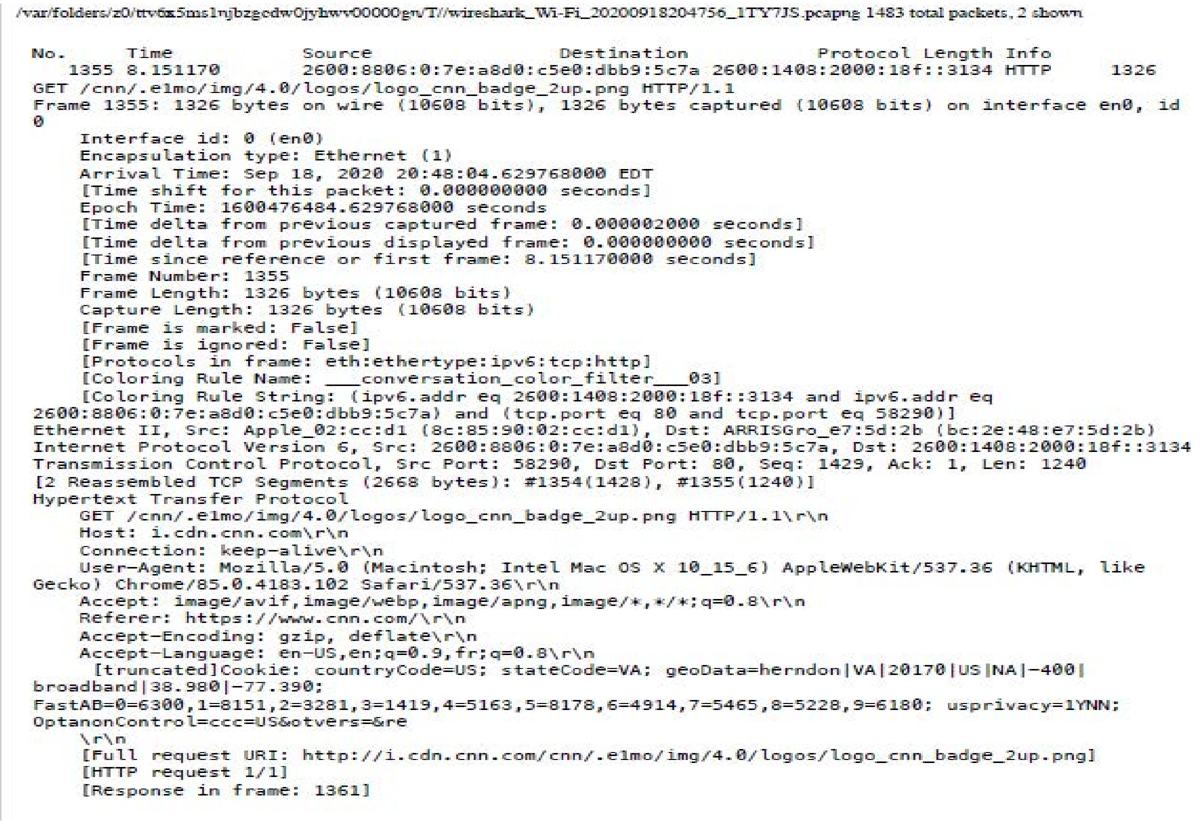
Answer: 128.119.245.12



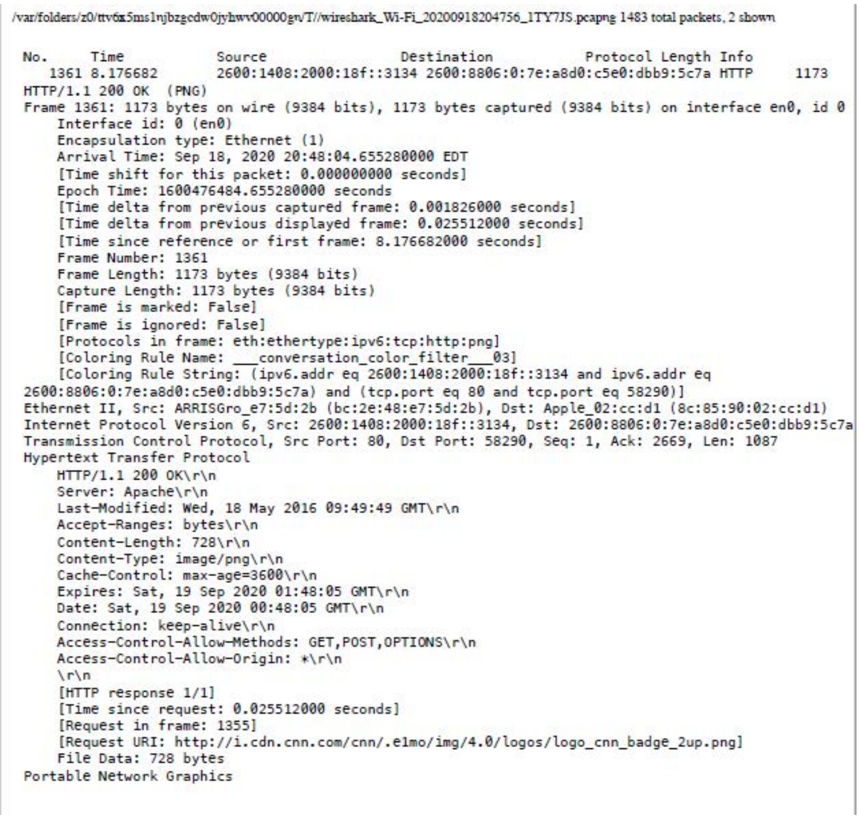
```
http
No.    Time       Source            Destination       Protocol Length Info
   33  4.485216   192.168.0.26      128.119.245.12    HTTP     648  GET /networks/index.html HTTP/1.1
   35  4.525781   128.119.245.12    192.168.0.26      HTTP     306  HTTP/1.1 304 Not Modified
   47  4.583461   192.168.0.26      104.196.134.131   HTTP     473  GET /images/qupmember.gif HTTP/1.1
   49  4.615174   104.196.134.131   192.168.0.26      HTTP     458  HTTP/1.1 404 Not Found  (text/html)
   98  12.492462  192.168.0.26      17.253.21.204     HTTP     364  GET /ocsp-devid01/ME4wTKADAgEAMEUwQzBBMAkGBSsOAwIaBQAEFDOB0e%2FbaLCFIU0u76%2BMSmlkPCpsBBRXF%2B2iz9x8mK…
  104  12.517253  17.253.21.204     192.168.0.26      OCSP     428  Response
  113  12.768741  192.168.0.26      17.253.15.204     HTTP     364  GET /ocsp-devid01/ME4wTKADAgEAMEUwQzBBMAkGBSsOAwIaBQAEFDOB0e%2FbaLCFIU0u76%2BMSmlkPCpsBBRXF%2B2iz9x8mK…
  117  12.794779  17.253.15.204     192.168.0.26      OCSP     428  Response
```

```
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 634
    Identification: 0x0000 (0)
  ▶ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x0238 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.26
    Destination: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 57821, Dst Port: 80, Seq: 1, Ack: 1, Len: 582
▼ Hypertext Transfer Protocol

0000  bc 2e 48 e7 5d 2b 8c 85  90 02 cc d1 08 00 45 00   ·.H·]+·· ······E·

Ethernet (eth), 14 bytes        Packets: 224 · Displayed: 8 (3.6%) · Dropped: 0 (0.0%)        Profile: Default
```

5. 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.



```
/var/folders/z0/ttv6x5ms1njbzgcdw0jyhwv00000gn/T//wireshark_Wi-Fi_20200918204756_1TY7JS.pcapng 1483 total packets, 2 shown

No.     Time           Source                Destination           Protocol Length Info
   1355 8.151170       2600:8806:0:7e:a8d0:c5e0:dbb9:5c7a 2600:1408:2000:18f::3134 HTTP     1326
GET /cnn/.e1mo/img/4.0/logos/logo_cnn_badge_2up.png HTTP/1.1
Frame 1355: 1326 bytes on wire (10608 bits), 1326 bytes captured (10608 bits) on interface en0, id
0
    Interface id: 0 (en0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 18, 2020 20:48:04.629768000 EDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1600476484.629768000 seconds
    [Time delta from previous captured frame: 0.000002000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 8.151170000 seconds]
    Frame Number: 1355
    Frame Length: 1326 bytes (10608 bits)
    Capture Length: 1326 bytes (10608 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:tcp:http]
    [Coloring Rule Name: ___conversation_color_filter___03]
    [Coloring Rule String: (ipv6.addr eq 2600:1408:2000:18f::3134 and ipv6.addr eq
2600:8806:0:7e:a8d0:c5e0:dbb9:5c7a) and (tcp.port eq 80 and tcp.port eq 58290)]
Ethernet II, Src: Apple_02:cc:d1 (8c:85:90:02:cc:d1), Dst: ARRISGro_e7:5d:2b (bc:2e:48:e7:5d:2b)
Internet Protocol Version 6, Src: 2600:8806:0:7e:a8d0:c5e0:dbb9:5c7a, Dst: 2600:1408:2000:18f::3134
Transmission Control Protocol, Src Port: 58290, Dst Port: 80, Seq: 1429, Ack: 1, Len: 1240
[2 Reassembled TCP Segments (2668 bytes): #1354(1428), #1355(1240)]
Hypertext Transfer Protocol
    GET /cnn/.e1mo/img/4.0/logos/logo_cnn_badge_2up.png HTTP/1.1\r\n
    Host: i.cdn.cnn.com\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/85.0.4183.102 Safari/537.36\r\n
    Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8\r\n
    Referer: https://www.cnn.com/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,fr;q=0.8\r\n
     [truncated]Cookie: countryCode=US; stateCode=VA; geoData=herndon|VA|20170|US|NA|-400|
broadband|38.980|-77.390;
FastAB=0=6300,1=8151,2=3281,3=1419,4=5163,5=8178,6=4914,7=5465,8=5228,9=6180; usprivacy=1YNN;
OptanonControl=ccc=US&otvers=&re
    \r\n
    [Full request URI: http://i.cdn.cnn.com/cnn/.e1mo/img/4.0/logos/logo_cnn_badge_2up.png]
    [HTTP request 1/1]
    [Response in frame: 1361]
```



/var/folders/z0/ttv6x5ms1njbzgcdw0jyhwv00000gn/T//wireshark_Wi-Fi_20200918204756_1TY7JS.pcapng 1483 total packets, 2 shown

```
No.     Time           Source                Destination           Protocol Length Info
   1361 8.176682       2600:1408:2000:18f::3134 2600:8806:0:7e:a8d0:c5e0:dbb9:5c7a HTTP     1173
HTTP/1.1 200 OK  (PNG)
Frame 1361: 1173 bytes on wire (9384 bits), 1173 bytes captured (9384 bits) on interface en0, id 0
    Interface id: 0 (en0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 18, 2020 20:48:04.655280000 EDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1600476484.655280000 seconds
    [Time delta from previous captured frame: 0.001826000 seconds]
    [Time delta from previous displayed frame: 0.025512000 seconds]
    [Time since reference or first frame: 8.176682000 seconds]
    Frame Number: 1361
    Frame Length: 1173 bytes (9384 bits)
    Capture Length: 1173 bytes (9384 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:tcp:http:png]
    [Coloring Rule Name: ___conversation_color_filter___03]
    [Coloring Rule String: (ipv6.addr eq 2600:1408:2000:18f::3134 and ipv6.addr eq
2600:8806:0:7e:a8d0:c5e0:dbb9:5c7a) and (tcp.port eq 80 and tcp.port eq 58290)]
Ethernet II, Src: ARRISGro_e7:5d:2b (bc:2e:48:e7:5d:2b), Dst: Apple_02:cc:d1 (8c:85:90:02:cc:d1)
Internet Protocol Version 6, Src: 2600:1408:2000:18f::3134, Dst: 2600:8806:0:7e:a8d0:c5e0:dbb9:5c7a
Transmission Control Protocol, Src Port: 80, Dst Port: 58290, Seq: 1, Ack: 2669, Len: 1087
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Server: Apache\r\n
    Last-Modified: Wed, 18 May 2016 09:49:49 GMT\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 728\r\n
    Content-Type: image/png\r\n
    Cache-Control: max-age=3600\r\n
    Expires: Sat, 19 Sep 2020 01:48:05 GMT\r\n
    Date: Sat, 19 Sep 2020 00:48:05 GMT\r\n
    Connection: keep-alive\r\n
    Access-Control-Allow-Methods: GET,POST,OPTIONS\r\n
    Access-Control-Allow-Origin: *\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.025512000 seconds]
    [Request in frame: 1355]
    [Request URI: http://i.cdn.cnn.com/cnn/.e1mo/img/4.0/logos/logo_cnn_badge_2up.png]
    File Data: 728 bytes
Portable Network Graphics
```