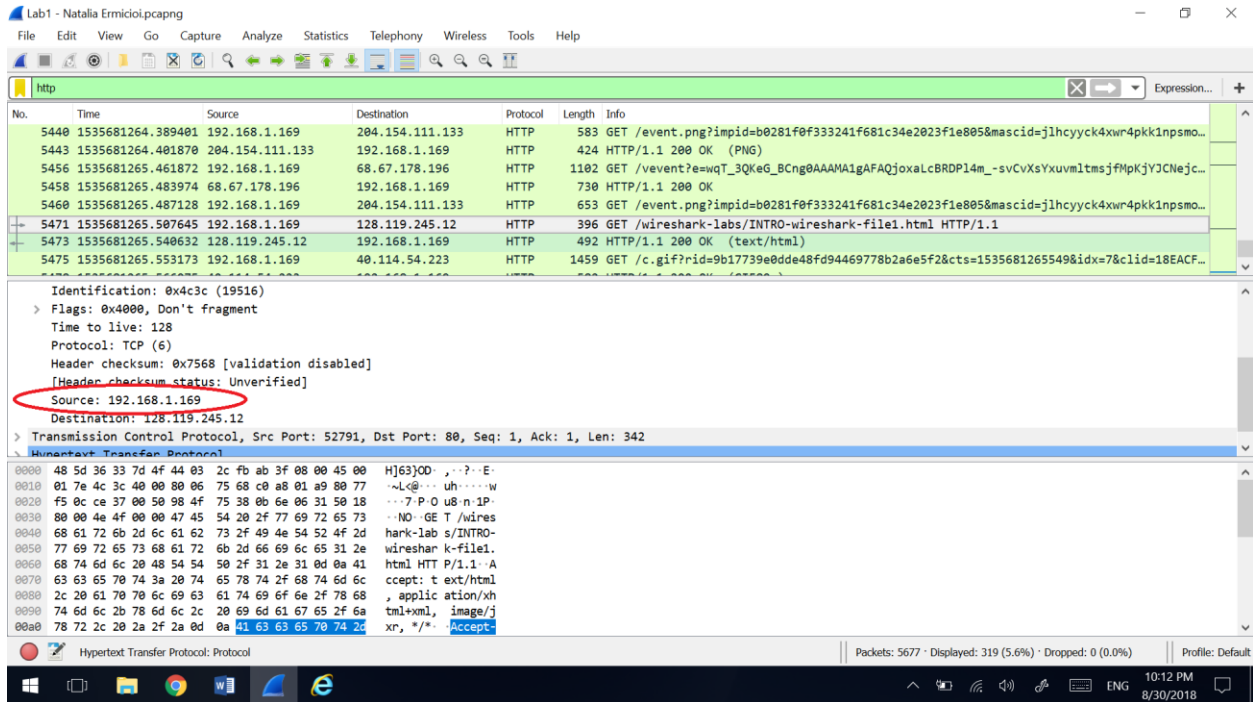


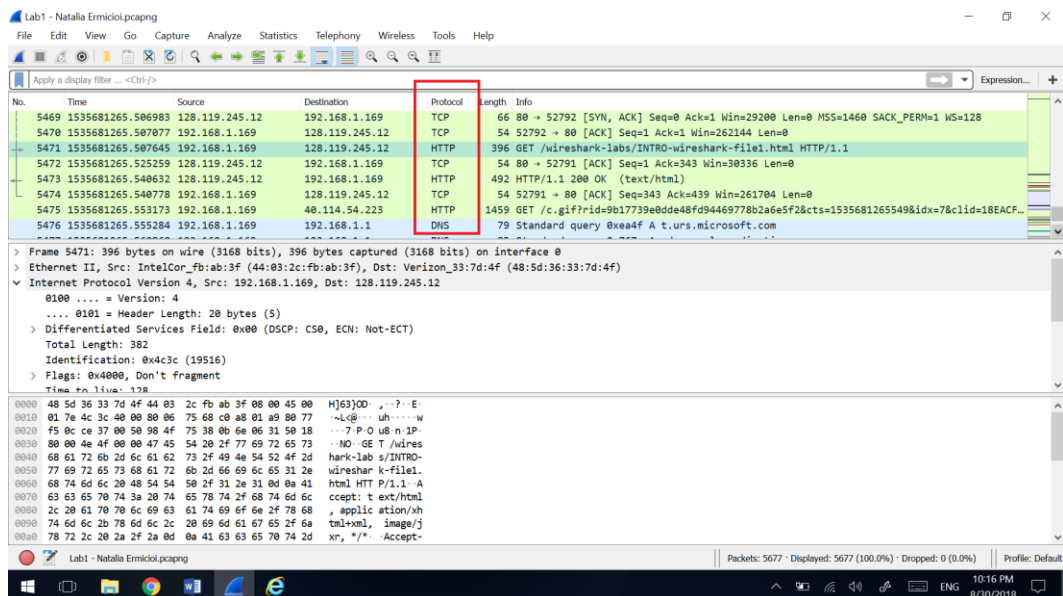
1. What is the Internet address of your computer?

Answer: 192.168.1.169



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.



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.)

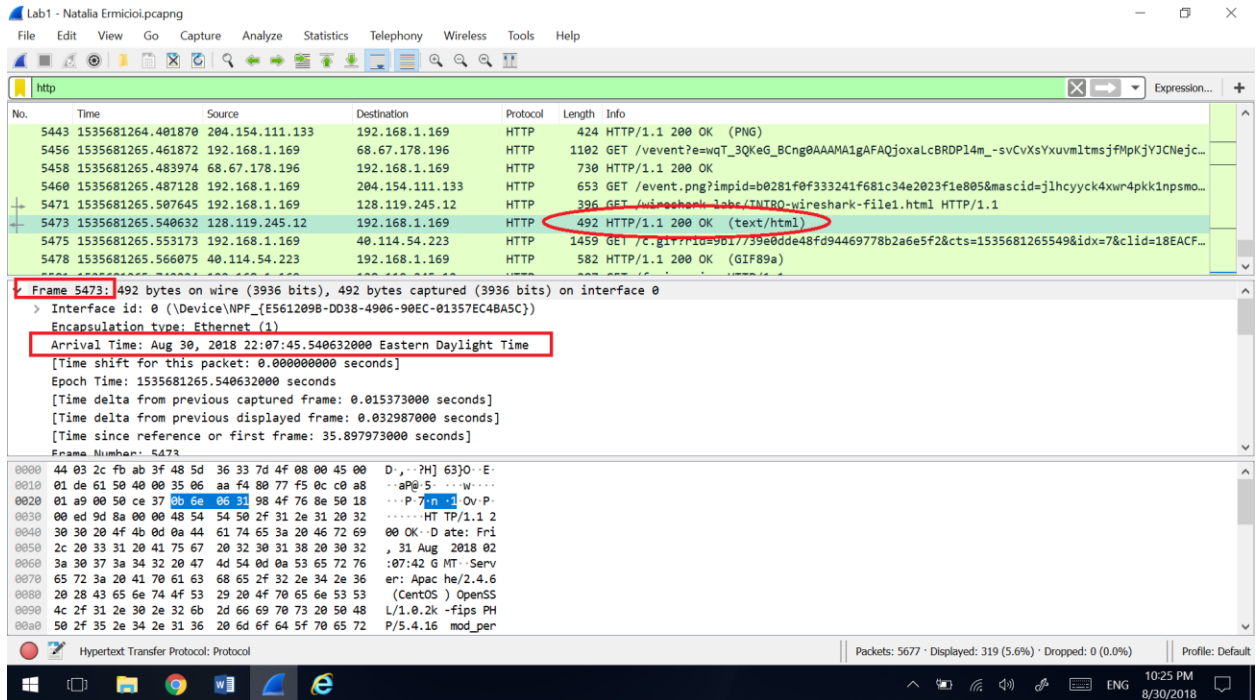
Answer:

- Arrival time of GET request is: Aug 30, 2018 22:07:45.507645000
 - Arrival time of HTTP OK is: Aug 30, 2018 22:07:45.540632000
- Difference: 0.540632-0.507645=0.032987 sec.

The image shows a Wireshark packet capture analysis. The packet list on the left shows several HTTP packets. Packet 5471 is highlighted, showing a GET request for `/wireshark-labs/INTRO-wireshark-file1.html`. The packet details pane on the right shows the arrival time of this packet as `Aug 30, 2018 22:07:45.507645000 Eastern Daylight Time`. The packet bytes pane at the bottom shows the raw data of the packet, including the HTTP request line `GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1`.

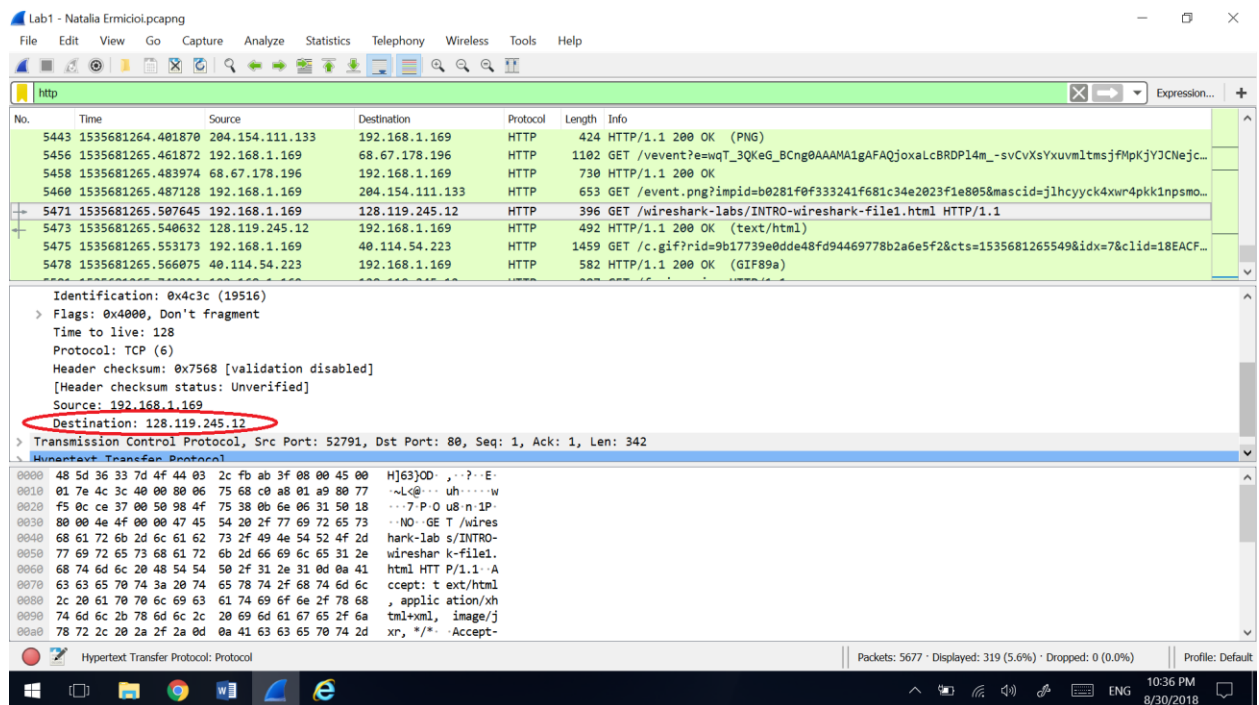
No.	Time	Source	Destination	Protocol	Length	Info
5443	1535681264.481870	204.154.111.133	192.168.1.169	HTTP	424	HTTP/1.1 200 OK (PNG)
5456	1535681265.461872	192.168.1.169	68.67.178.196	HTTP	1102	GET /event?e=wqT_3QKeG_BCng0AAAIAIgaFAQjoxaLcBRDP14m_-svCvXsYxuvmltmsjFMpKjYJCNejc...
5458	1535681265.483974	68.67.178.196	192.168.1.169	HTTP	730	HTTP/1.1 200 OK
5460	1535681265.487128	192.168.1.169	204.154.111.133	HTTP	653	GET /event.one?impid=b0281f0f333241f681c34e2023fle805&masid=jlhcyck4xwr4pk1npsmo...
5471	1535681265.507645	192.168.1.169	128.119.245.12	HTTP	396	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
5473	1535681265.540632	128.119.245.12	192.168.1.169	HTTP	482	HTTP/1.1 200 OK (text/html)
5475	1535681265.553173	192.168.1.169	40.114.54.223	HTTP	1459	GET /c.gif?rid=9b17739e0dde48fd94469778b2a6e5f2&cts=1535681265549&idx=7&clid=18EACF...
5478	1535681265.566075	40.114.54.223	192.168.1.169	HTTP	582	HTTP/1.1 200 OK (GIF89a)

Frame 5471: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits) on interface 0
> Interface id: 0 (\Device\NPF_{E5612098-DD38-4906-90EC-01357EC48A5C})
Encapsulation type: Ethernet (1)
Arrival Time: Aug 30, 2018 22:07:45.507645000 Eastern Daylight Time
[Time shift for this packet: 0.00000000 seconds]
Epoch Time: 1535681265.507645000 seconds
[Time delta from previous captured frame: 0.000568000 seconds]
[Time delta from previous displayed frame: 0.020517000 seconds]
[Time since reference or first frame: 35.864986000 seconds]
Frame Number: 5471
0000 48 5d 36 33 7d 4f 44 03 2c fb ab 3f 08 00 45 00 H]63]00: ,...?..E.
0010 01 7e 4c 3c 40 00 80 06 75 68 c0 a8 01 a9 80 77 ..L@... uh.....w
0020 f5 0c ce 37 00 50 98 4f 75 38 0b 6e 06 31 50 18 ...7.P.O u8-n.1P
0030 80 00 4e 4f 00 00 47 45 54 20 2f 77 69 72 65 73 ...NO.GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d hark-lab s/INTRO-
0050 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e wireshar k-file1.
0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 41 html HTTP/1.1..A
0070 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c ccept: t ext/html
0080 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 , applic ation/xh
0090 74 6d 6c 2b 78 6d 6c 2c 20 69 6d 61 67 65 2f 6a tml+xml, image/j
00a0 78 72 2c 20 2a 2f 2a 0d 0a 41 63 63 65 70 74 2d xr, /*: -Accept-



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

Answer: 128.119.245.12



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.

C:\Users\Natalia\Desktop\Lab1 - Natalia Ermidol.pcapng 5677 total packets, 319 shown

No.	Time	Source	Destination	Protocol	Length	Info
5471	1535681265.507645	192.168.1.169	128.119.245.12	HTTP	396	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 5471: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits) on interface 0
Ethernet II, Src: IntelCor_fb:ab:3f (44:03:2c:fb:ab:3f), Dst: Verizon_33:7d:4f (48:5d:36:33:7d:4f)
Internet Protocol Version 4, Src: 192.168.1.169, Dst: 128.119.245.12
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 382
 Identification: 0x4c3c (19516)
 Flags: 0x4000, Don't fragment
 Time to live: 128
 Protocol: TCP (6)
 Header checksum: 0x7568 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.169
 Destination: 128.119.245.12
Transmission Control Protocol, Src Port: 52791, Dst Port: 80, Seq: 1, Ack: 1, Len: 342
Hypertext Transfer Protocol

C:\Users\Natalia\Desktop\Lab1 - Natalia Ermicloi.pcapng 5677 total packets, 319 shown

No.	Time	Source	Destination	Protocol	Length	Info
5473	1535681265.540632	128.119.245.12	192.168.1.169	HTTP	492	HTTP/1.1 200 OK (text/html)

Frame 5473: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0
Ethernet II, Src: Verizon_33:7d:4f (48:5d:36:33:7d:4f), Dst: IntelCor_fb:ab:3f (44:03:2c:fb:ab:3f)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.169
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 478
Identification: 0x6150 (24912)
Flags: 0x4000, Don't fragment
Time to live: 53
Protocol: TCP (6)
Header checksum: 0xaaf4 [validation disabled]
[Header checksum status: Unverified]
Source: 128.119.245.12
Destination: 192.168.1.169
Transmission Control Protocol, Src Port: 80, Dst Port: 52791, Seq: 1, Ack: 343, Len: 438
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)