CS372
Lab1, Eric Rouse

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

ARP, HTTP, NBNS, SNMP, TCP

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.)

Approximately 2.3 seconds.

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

128.119.245.12

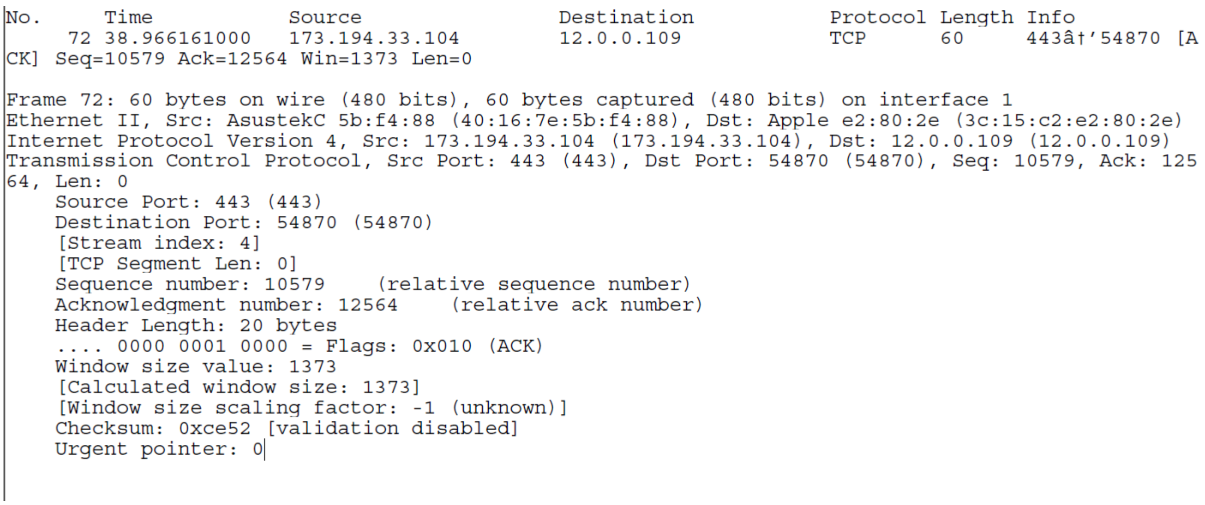
What is the Internet address of your computer?

IP address: 12.0.0.10; Internet address: 74.125.28.147

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.

There was not HTTP GET, which, according to wireshark help is because my browser defaults to HTTPS and so it is encrypted, I have a TCP packet on port 443 which is the equivalent of GET.

HTTP GET (ENCRYPTED)

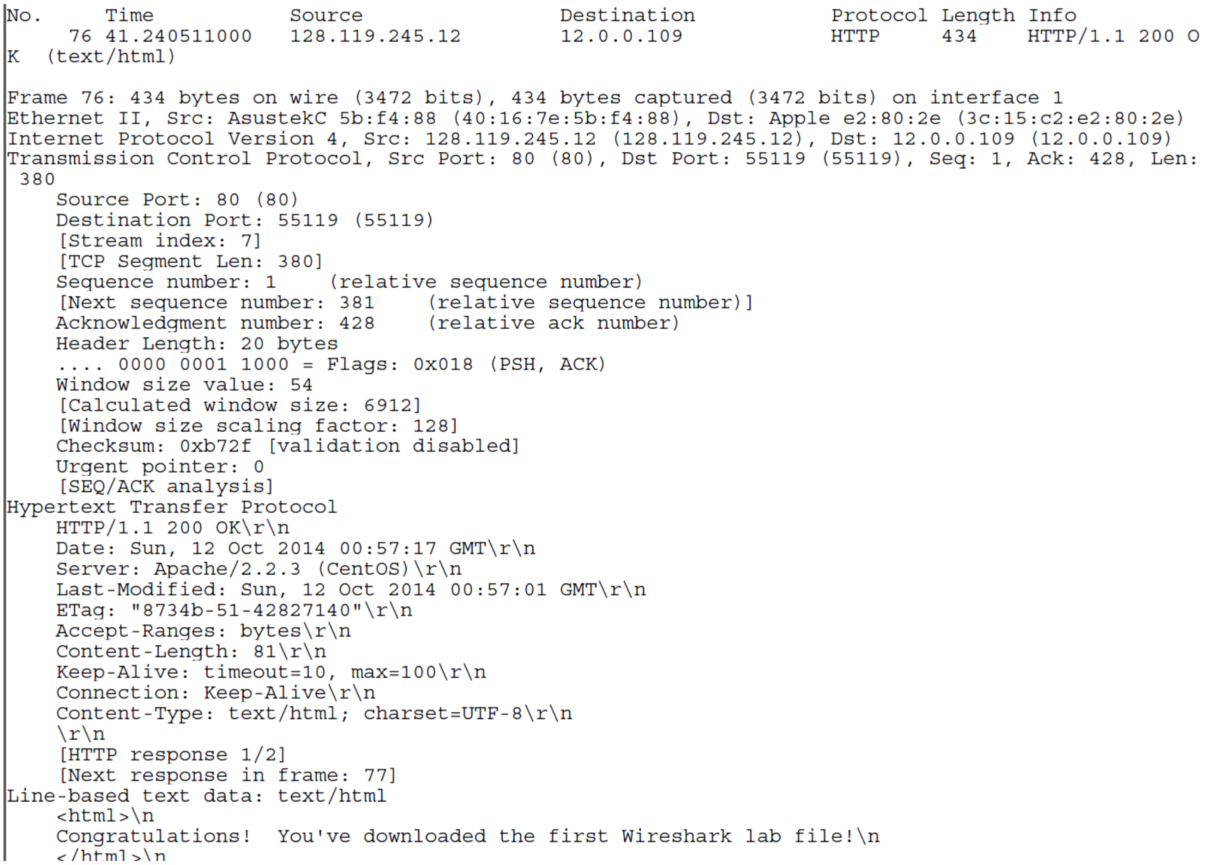


```
No.     Time           Source                Destination           Protocol Length Info
     72 38.966161000   173.194.33.104        12.0.0.109            TCP      60     443â†’54870 [A
CK] Seq=10579 Ack=12564 Win=1373 Len=0

Frame 72: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 1
Ethernet II, Src: AsustekC 5b:f4:88 (40:16:7e:5b:f4:88), Dst: Apple e2:80:2e (3c:15:c2:e2:80:2e)
Internet Protocol Version 4, Src: 173.194.33.104 (173.194.33.104), Dst: 12.0.0.109 (12.0.0.109)
Transmission Control Protocol, Src Port: 443 (443), Dst Port: 54870 (54870), Seq: 10579, Ack: 125
64, Len: 0
    Source Port: 443 (443)
    Destination Port: 54870 (54870)
    [Stream index: 4]
    [TCP Segment Len: 0]
    Sequence number: 10579    (relative sequence number)
    Acknowledgment number: 12564    (relative ack number)
    Header Length: 20 bytes
    .... 0000 0001 0000 = Flags: 0x010 (ACK)
    Window size value: 1373
    [Calculated window size: 1373]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0xce52 [validation disabled]
    Urgent pointer: 0
```

CS372
Lab1, Eric Rouse

HTTP OK



```
No.     Time           Source                Destination           Protocol Length Info
     76 41.240511000   128.119.245.12        12.0.0.109            HTTP     434    HTTP/1.1 200 O
K  (text/html)

Frame 76: 434 bytes on wire (3472 bits), 434 bytes captured (3472 bits) on interface 1
Ethernet II, Src: AsustekC 5b:f4:88 (40:16:7e:5b:f4:88), Dst: Apple e2:80:2e (3c:15:c2:e2:80:2e)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 12.0.0.109 (12.0.0.109)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 55119 (55119), Seq: 1, Ack: 428, Len:
 380
    Source Port: 80 (80)
    Destination Port: 55119 (55119)
    [Stream index: 7]
    [TCP Segment Len: 380]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 381    (relative sequence number)]
    Acknowledgment number: 428    (relative ack number)
    Header Length: 20 bytes
    .... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
    Window size value: 54
    [Calculated window size: 6912]
    [Window size scaling factor: 128]
    Checksum: 0xb72f [validation disabled]
    Urgent pointer: 0
    [SEQ/ACK analysis]
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Sun, 12 Oct 2014 00:57:17 GMT\r\n
    Server: Apache/2.2.3 (CentOS)\r\n
    Last-Modified: Sun, 12 Oct 2014 00:57:01 GMT\r\n
    ETag: "8734b-51-42827140"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
    Keep-Alive: timeout=10, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Next response in frame: 77]
Line-based text data: text/html
    <html>\n
    Congratulations!  You've downloaded the first Wireshark lab file!\n
    </html>\n
```