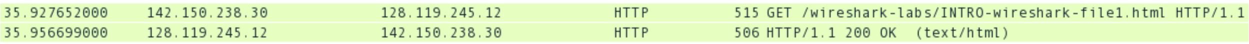
CSC358 Wireshark Assignment 1 Solution

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

Solution:
TCP, UDP, HTTP, DNS, ARP, IMAP, TLSV1.2, ……
(Any 3 possible protocols will be accepted.)

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.)

Solution:



```
35.927652000    142.150.238.30          128.119.245.12          HTTP        515 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
35.956699000    128.119.245.12          142.150.238.30          HTTP        506 HTTP/1.1 200 OK  (text/html)
```

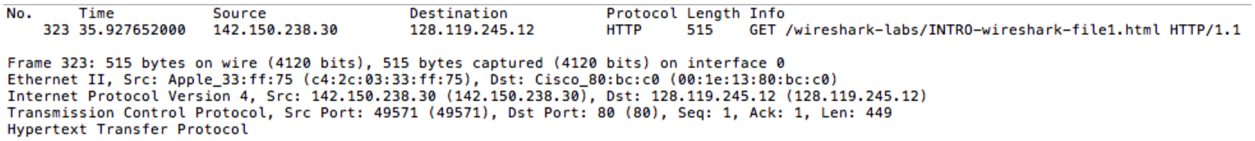
According to the screenshot, the time interval between the HTTP GET message and HTTP OK message is
35.956699000s - 35.927652000s = 0.029049s
(The time interval in the range of 0.015 ~ 0.040 will be accepted.)

3.What is the Internet address of the gaia.cs.umass.edu? What is the Internet address of your computer?

Solution:
gaia.cs.umass.edu: 128.119.245.12
my computer: xxx.xxx.xxx.xxx

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.

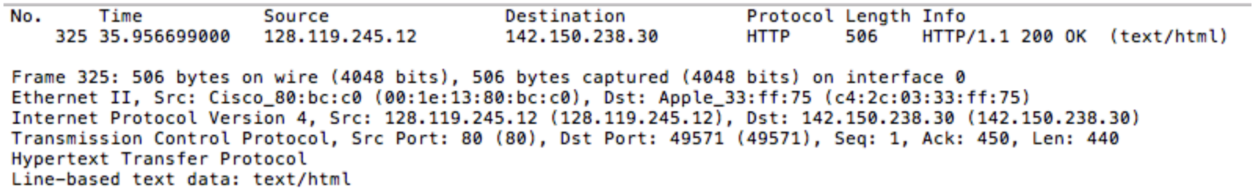
Solution:
The screenshot of HTTP GET message:



```
No.     Time           Source                Destination           Protocol Length Info
    323 35.927652000   142.150.238.30        128.119.245.12        HTTP     515    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 323: 515 bytes on wire (4120 bits), 515 bytes captured (4120 bits) on interface 0
Ethernet II, Src: Apple_33:ff:75 (c4:2c:03:33:ff:75), Dst: Cisco_80:bc:c0 (00:1e:13:80:bc:c0)
Internet Protocol Version 4, Src: 142.150.238.30 (142.150.238.30), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 49571 (49571), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 449
Hypertext Transfer Protocol
```

The screenshot of HTTP OK message:



```
No.     Time           Source                Destination           Protocol Length Info
    325 35.956699000   128.119.245.12        142.150.238.30        HTTP     506    HTTP/1.1 200 OK  (text/html)

Frame 325: 506 bytes on wire (4048 bits), 506 bytes captured (4048 bits) on interface 0
Ethernet II, Src: Cisco_80:bc:c0 (00:1e:13:80:bc:c0), Dst: Apple_33:ff:75 (c4:2c:03:33:ff:75)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 142.150.238.30 (142.150.238.30)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49571 (49571), Seq: 1, Ack: 450, Len: 440
Hypertext Transfer Protocol
Line-based text data: text/html
```