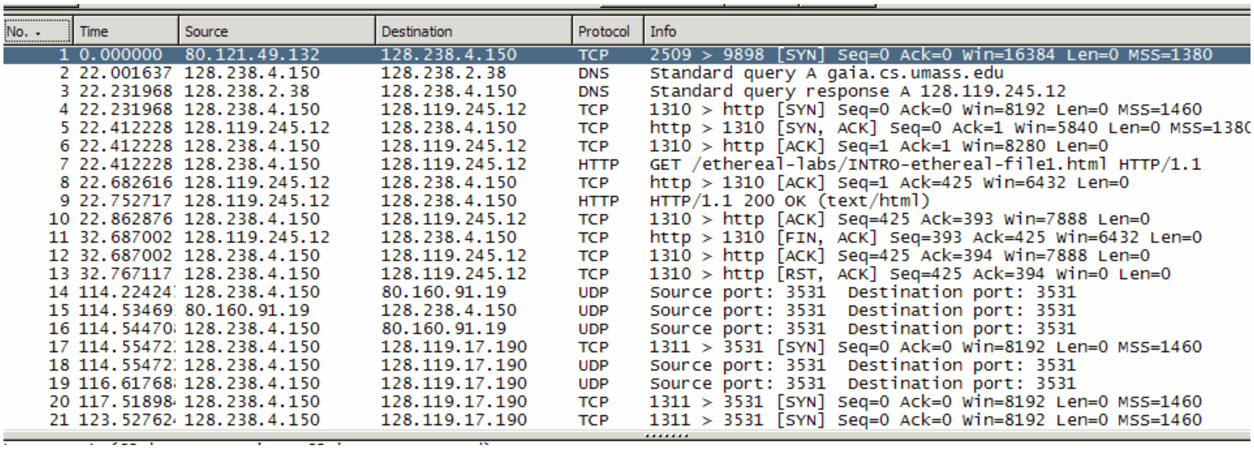
WIRESHARK LAB#1 SOLUTION

Answers were taken from students with correct lab reports and show what should be the ideal format of your lab report.

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

Answer:

The following protocols appeared in the protocol column in the unfiltered packet listing window after downloading a webpage: TCP, UDP, HTTP, DNS.

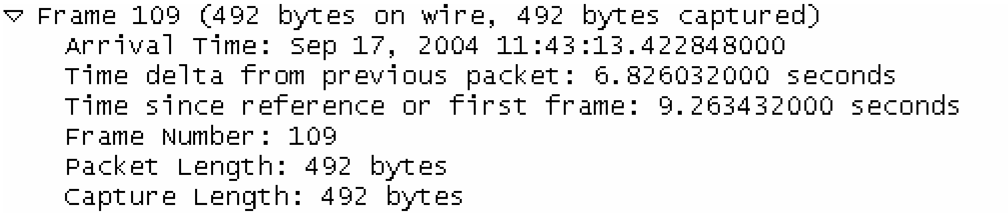


No.	Time	Source	Destination	Protocol	Info
1	0.000000	80.121.49.132	128.238.4.150	TCP	2509 > 9898 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1380
2	22.001637	128.238.4.150	128.238.2.38	DNS	Standard query A gaia.cs.umass.edu
3	22.231968	128.238.2.38	128.238.4.150	DNS	Standard query response A 128.119.245.12
4	22.231968	128.238.4.150	128.119.245.12	TCP	1310 > http [SYN] Seq=0 Ack=0 Win=8192 Len=0 MSS=1460
5	22.412228	128.119.245.12	128.238.4.150	TCP	http > 1310 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=138
6	22.412228	128.238.4.150	128.119.245.12	TCP	1310 > http [ACK] Seq=1 Ack=1 Win=8280 Len=0
7	22.412228	128.238.4.150	128.119.245.12	HTTP	GET /ethereal-labs/INTRO-ethereal-file1.html HTTP/1.1
8	22.682616	128.119.245.12	128.238.4.150	TCP	http > 1310 [ACK] Seq=1 Ack=425 Win=6432 Len=0
9	22.752717	128.119.245.12	128.238.4.150	HTTP	HTTP/1.1 200 OK (text/html)
10	22.862876	128.238.4.150	128.119.245.12	TCP	1310 > http [ACK] Seq=425 Ack=393 Win=7888 Len=0
11	32.687002	128.119.245.12	128.238.4.150	TCP	http > 1310 [FIN, ACK] Seq=393 Ack=425 Win=6432 Len=0
12	32.687002	128.238.4.150	128.119.245.12	TCP	1310 > http [ACK] Seq=425 Ack=394 Win=7888 Len=0
13	32.767117	128.238.4.150	128.119.245.12	TCP	1310 > http [RST, ACK] Seq=425 Ack=394 Win=0 Len=0
14	114.22424	128.238.4.150	80.160.91.19	UDP	Source port: 3531 Destination port: 3531
15	114.53469	80.160.91.19	128.238.4.150	UDP	Source port: 3531 Destination port: 3531
16	114.54470	128.238.4.150	80.160.91.19	UDP	Source port: 3531 Destination port: 3531
17	114.55472	128.238.4.150	128.119.17.190	TCP	1311 > 3531 [SYN] Seq=0 Ack=0 Win=8192 Len=0 MSS=1460
18	114.55472	128.238.4.150	128.119.17.190	UDP	Source port: 3531 Destination port: 3531
19	116.61768	128.238.4.150	128.119.17.190	UDP	Source port: 3531 Destination port: 3531
20	117.51898	128.238.4.150	128.119.17.190	TCP	1311 > 3531 [SYN] Seq=0 Ack=0 Win=8192 Len=0 MSS=1460
21	123.52762	128.238.4.150	128.119.17.190	TCP	1311 > 3531 [SYN] Seq=0 Ack=0 Win=8192 Len=0 MSS=1460

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*.)

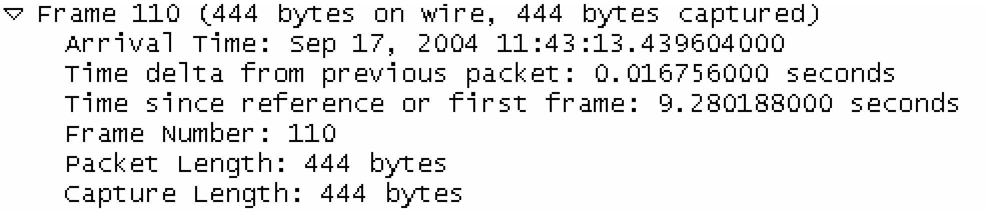
Answer:

If we look at the frame section of the GET request we see that the time the packet arrived is 11:43:13.422848000



```
▽ Frame 109 (492 bytes on wire, 492 bytes captured)
    Arrival Time: Sep 17, 2004 11:43:13.422848000
    Time delta from previous packet: 6.826032000 seconds
    Time since reference or first frame: 9.263432000 seconds
    Frame Number: 109
    Packet Length: 492 bytes
    Capture Length: 492 bytes
```

The same section for the HTTP OK shows an arrival time of 11:43:13.43960400



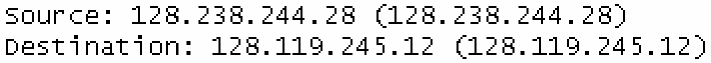
```
▽ Frame 110 (444 bytes on wire, 444 bytes captured)
    Arrival Time: Sep 17, 2004 11:43:13.439604000
    Time delta from previous packet: 0.016756000 seconds
    Time since reference or first frame: 9.280188000 seconds
    Frame Number: 110
    Packet Length: 444 bytes
    Capture Length: 444 bytes
```

The difference of these 2 times gives
.43960400 - .426032000 = **0.013572 seconds**

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

<u>Answer:</u>

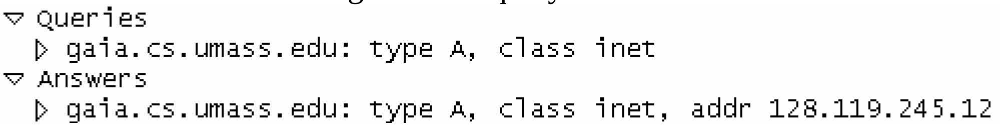
If we look at the IP section of the GET request, the source and destination are shown



```
Source: 128.238.244.28 (128.238.244.28)
Destination: 128.119.245.12 (128.119.245.12)
```

The source is the local machine's address and the destination is the web server's public
My (local machine's) address = 128.238.244.28
IP address 128.119.245.12 = www-net.cs.umass.edu.

This can also be seen during the DNS query



```
▽ Queries
  ▷ gaia.cs.umass.edu: type A, class inet
▽ Answers
  ▷ gaia.cs.umass.edu: type A, class inet, addr 128.119.245.12
```

4. Print the two HTTP messages displayed in step 9 above. To do so, select *Print* from the Wireshark *File* command menu, and select *"Selected Packet Only"* and *"Print as displayed"* and then click OK.

<u>Answer:</u>

Here is the information for the HTTP GET and OK packets:

HTTP GET:

```
Frame 4 (862 bytes on wire, 862 bytes captured)
Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: WestellT_9f:92:b9
(00:0f:db:9f:92:b9)
Internet Protocol, Src: 192.168.1.46 (192.168.1.46), Dst: 128.119.245.12
(128.119.245.12)
Transmission Control Protocol, Src Port: 1474 (1474), Dst Port: http (80), Seq: 1,
Ack: 1, Len: 808
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.4)
    Gecko/20070515 Firefox/2.0.0.4\r\n
    Accept:
    text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,im
    age/png,*/*;q=0.5\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
```

HTTP OK:

```
Frame 6 (439 bytes on wire, 439 bytes captured)
Ethernet II, Src: WestellT_9f:92:b9 (00:0f:db:9f:92:b9), Dst: Netgear_61:8e:6d
(00:09:5b:61:8e:6d)
Internet Protocol, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.46
(192.168.1.46)
Transmission Control Protocol, Src Port: http (80), Dst Port: 1474 (1474), Seq: 1,
Ack: 809, Len: 385
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Thu, 07 Jun 2007 18:09:01 GMT\r\n
    Server: Apache/2.0.52 (CentOS)\r\n
    Last-Modified: Thu, 07 Jun 2007 18:08:01 GMT\r\n
    ETag: "d6c69-50-cb94a240"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 80
    Keep-Alive: timeout=10, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=ISO-8859-1\r\n
    \r\n
Line-based text data: text/html
```