

Lab 1: Wireshark Assignment

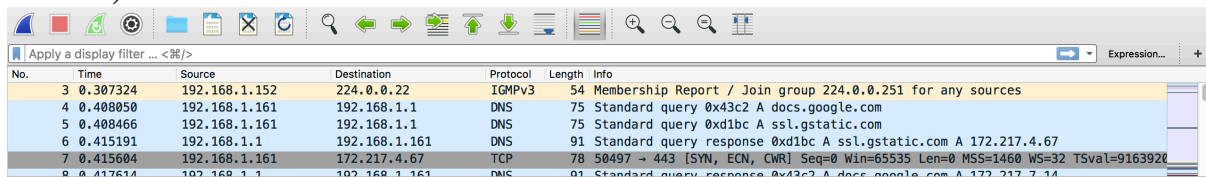
By: Monil Shah (mds747)

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

Ans 1) 1) TCP

2) DNS

3) IGMPv3



No.	Time	Source	Destination	Protocol	Length	Info
3	0.307324	192.168.1.152	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
4	0.408050	192.168.1.161	192.168.1.1	DNS	75	Standard query 0x43c2 A docs.google.com
5	0.408466	192.168.1.161	192.168.1.1	DNS	75	Standard query 0xd1bc A ssl.gstatic.com
6	0.415191	192.168.1.1	192.168.1.161	DNS	91	Standard query response 0xd1bc A ssl.gstatic.com A 172.217.4.67
7	0.415604	192.168.1.161	172.217.4.67	TCP	78	50497 -> 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=9163920
8	0.417614	192.168.1.1	192.168.1.161	DNS	91	Standard query response 0x43c2 A docs.google.com A 172.217.7.14

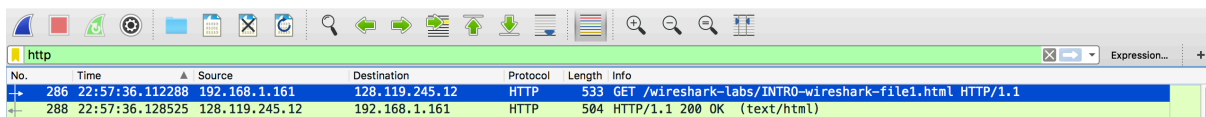
2)

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 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.)

Ans) HTTP GET: Time: 22:57:36.112288

HTTP OK: Time: 22:57:36.128525

Time Taken: 16237 milliseconds



No.	Time	Source	Destination	Protocol	Length	Info
286	22:57:36.112288	192.168.1.161	128.119.245.12	HTTP	533	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
288	22:57:36.128525	128.119.245.12	192.168.1.161	HTTP	504	HTTP/1.1 200 OK (text/html)

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?

Ans) **gaia.cs.umass.edu**

Internet address: 128.119.245.12

My Computer

Internet address: 192.168.1.161

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.

Ans)

```
/var/folders/9w/3sz6p5916gd99qwlyxj6__zw0000gn/T//wireshark_en0_20170203233854_WygzNI.pcapng 85 total packets, 2 shown

    33 23:39:05.258577    192.168.1.161          128.119.245.12          HTTP      493    GET /
wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 33: 493 bytes on wire (3944 bits), 493 bytes captured (3944 bits) on interface 0
Ethernet II, Src: Apple_9c:a6:65 (4c:32:75:9c:a6:65), Dst: Verizon_f1:47:66 (48:5d:36:f1:47:66)
Internet Protocol Version 4, Src: 192.168.1.161, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50875, Dst Port: 80, Seq: 1, Ack: 1, Len: 427
Hypertext Transfer Protocol
    37 23:39:05.275016    128.119.245.12          192.168.1.161          HTTP      504    HTTP/1.1
200 OK (text/html)
Frame 37: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface 0
Ethernet II, Src: Verizon_f1:47:66 (48:5d:36:f1:47:66), Dst: Apple_9c:a6:65 (4c:32:75:9c:a6:65)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.161
Transmission Control Protocol, Src Port: 80, Dst Port: 50875, Seq: 1, Ack: 428, Len: 438
Hypertext Transfer Protocol
Line-based text data: text/html
```