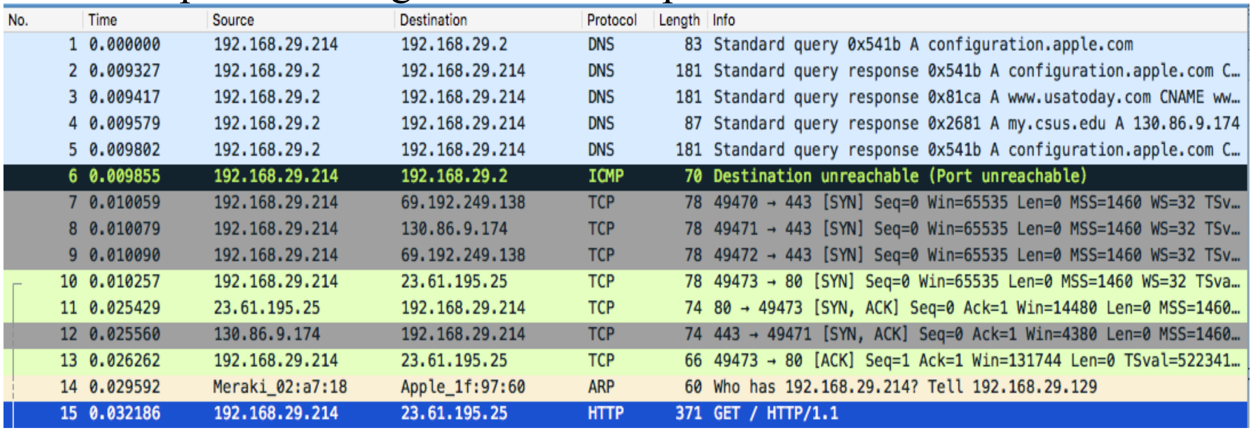
Jaskarn Jagpal
06/10/2016
CSc 138 T, TH 1240-410

Lab 1
Wireshark Introduction

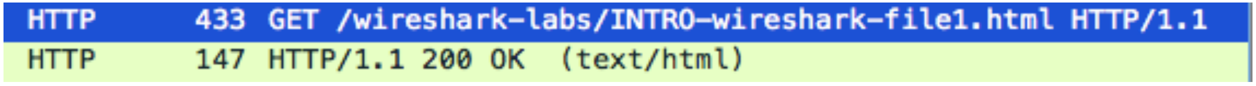
1) List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.29.214	192.168.29.2	DNS	83	Standard query 0x541b A configuration.apple.com
2	0.009327	192.168.29.2	192.168.29.214	DNS	181	Standard query response 0x541b A configuration.apple.com C…
3	0.009417	192.168.29.2	192.168.29.214	DNS	181	Standard query response 0x81ca A www.usatoday.com CNAME ww…
4	0.009579	192.168.29.2	192.168.29.214	DNS	87	Standard query response 0x2681 A my.csus.edu A 130.86.9.174
5	0.009802	192.168.29.2	192.168.29.214	DNS	181	Standard query response 0x541b A configuration.apple.com C…
6	0.009855	192.168.29.214	192.168.29.2	ICMP	70	Destination unreachable (Port unreachable)
7	0.010059	192.168.29.214	69.192.249.138	TCP	78	49470 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSv…
8	0.010079	192.168.29.214	130.86.9.174	TCP	78	49471 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSv…
9	0.010090	192.168.29.214	69.192.249.138	TCP	78	49472 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSv…
10	0.010257	192.168.29.214	23.61.195.25	TCP	78	49473 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSva…
11	0.025429	23.61.195.25	192.168.29.214	TCP	74	80 → 49473 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460…
12	0.025560	130.86.9.174	192.168.29.214	TCP	74	443 → 49471 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460…
13	0.026262	192.168.29.214	23.61.195.25	TCP	66	49473 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=522341…
14	0.029592	Meraki_02:a7:18	Apple_1f:97:60	ARP	60	Who has 192.168.29.214? Tell 192.168.29.129
15	0.032186	192.168.29.214	23.61.195.25	HTTP	371	GET / HTTP/1.1

a) TCP, ARP, and HTTP are 3 protocols that appear in the protocol column.

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*.)



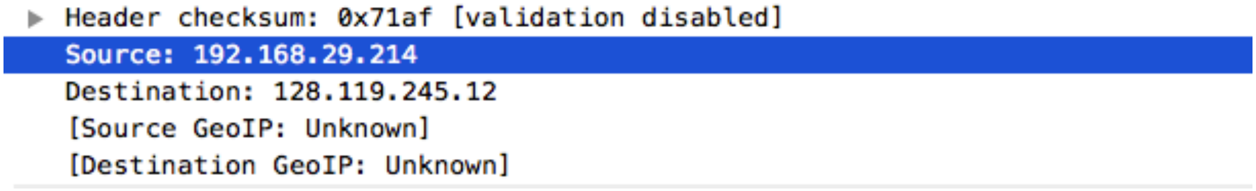
```
HTTP       433  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
HTTP       147  HTTP/1.1 200 OK  (text/html)
```

a) HTTP GET message sent: 17:49:07.324309

b) HTTP OK reply received: 17:49:07.527486

c) It took 0.203177 ms from when the HTTP GET message was sent until the HTTP OK reply was received.

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



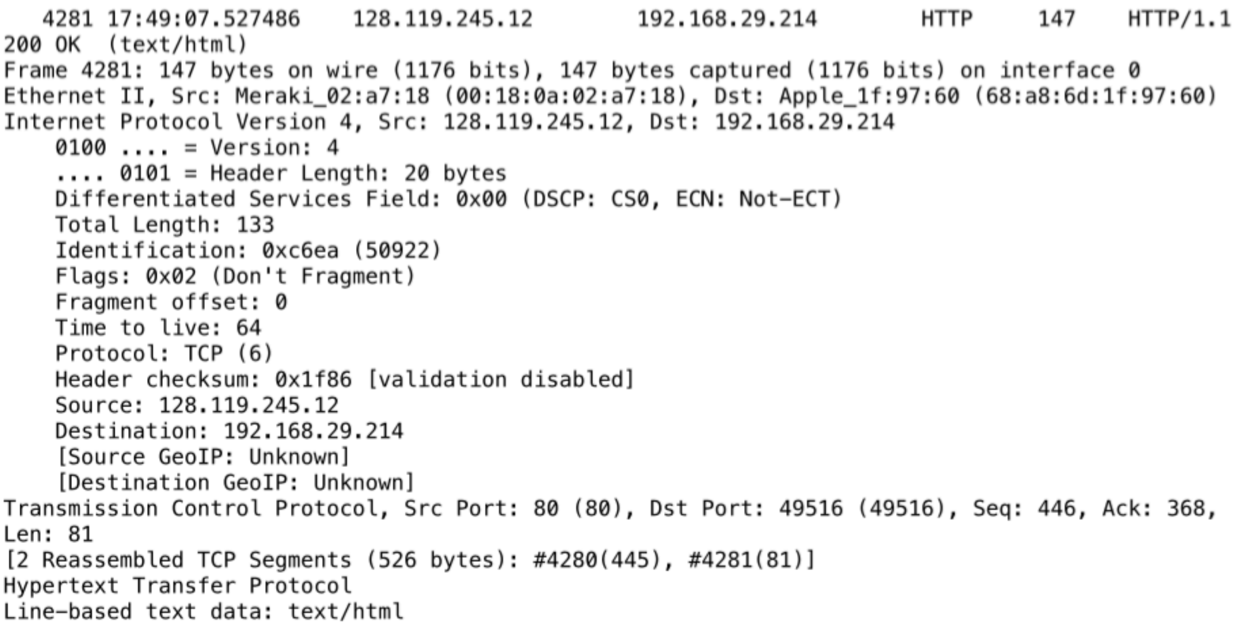
```
▶ Header checksum: 0x71af [validation disabled]
  Source: 192.168.29.214
  Destination: 128.119.245.12
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
```

a) Source: 192.168.29.214 – my computer

b) Destination: 128.119.245.12 – gaia.cs.umass.edu

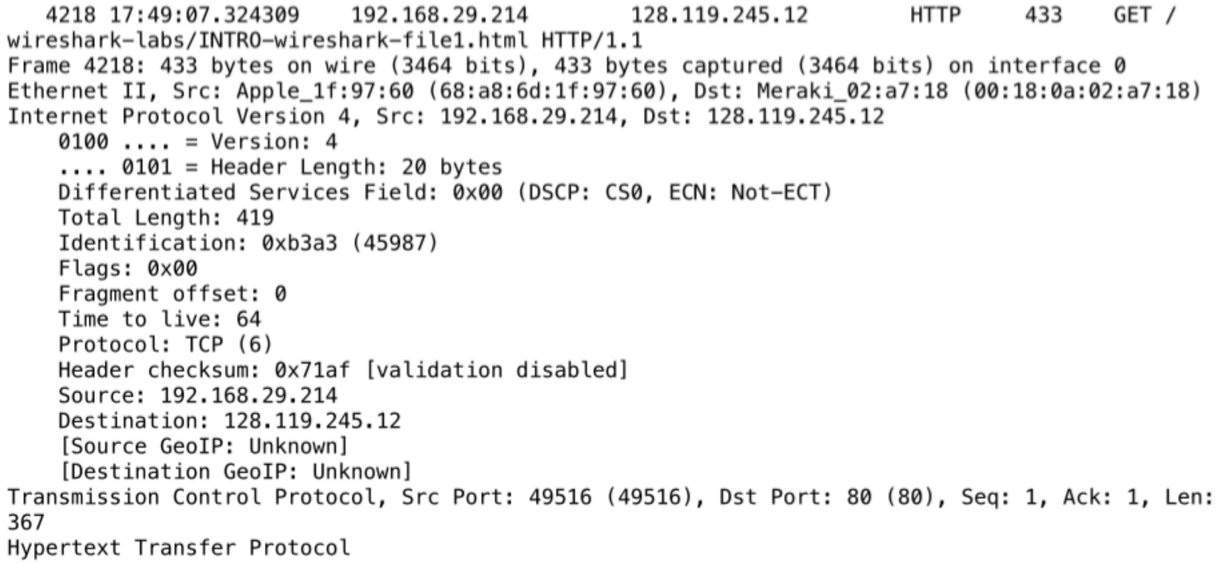
4) Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select *Print* from the Wireshark *File* command menu, and select the "*Selected Packet Only"* and *"Print as displayed"* radial buttons, and then click OK.

a) GET:



```
   4281 17:49:07.527486    128.119.245.12        192.168.29.214        HTTP     147    HTTP/1.1
200 OK  (text/html)
Frame 4281: 147 bytes on wire (1176 bits), 147 bytes captured (1176 bits) on interface 0
Ethernet II, Src: Meraki_02:a7:18 (00:18:0a:02:a7:18), Dst: Apple_1f:97:60 (68:a8:6d:1f:97:60)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.29.214
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 133
    Identification: 0xc6ea (50922)
    Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x1f86 [validation disabled]
    Source: 128.119.245.12
    Destination: 192.168.29.214
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49516 (49516), Seq: 446, Ack: 368,
Len: 81
[2 Reassembled TCP Segments (526 bytes): #4280(445), #4281(81)]
Hypertext Transfer Protocol
Line-based text data: text/html
```

OK:



```
   4218 17:49:07.324309    192.168.29.214        128.119.245.12        HTTP     433    GET /
wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 4218: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on interface 0
Ethernet II, Src: Apple_1f:97:60 (68:a8:6d:1f:97:60), Dst: Meraki_02:a7:18 (00:18:0a:02:a7:18)
Internet Protocol Version 4, Src: 192.168.29.214, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 419
    Identification: 0xb3a3 (45987)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x71af [validation disabled]
    Source: 192.168.29.214
    Destination: 128.119.245.12
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 49516 (49516), Dst Port: 80 (80), Seq: 1, Ack: 1, Len:
367
Hypertext Transfer Protocol
```