

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above. Support your answer with an appropriate screenshot from your computer.

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

No.	Time	Source	Destination	Protocol	Length	Info
230	9.359570	104.194.123.158	216.47.143.106	DNS	77	Standard query 0xeace A gaia.cs.umass.edu
231	9.360112	104.194.123.158	216.47.143.106	DNS	77	Standard query 0xc1e1 AAAA gaia.cs.umass.edu
232	9.362117	216.47.143.106	104.194.123.158	DNS	147	Standard query response 0xeace A gaia.cs.umass.edu A 128.119.2
233	9.362118	216.47.143.106	104.194.123.158	DNS	130	Standard query response 0xc1e1 AAAA gaia.cs.umass.edu SOA uni
234	9.363460	104.194.123.158	128.119.245.12	TCP	66	50059 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE
235	9.379410	35.173.72.116	104.194.123.158	TCP	60	443 → 49973 [FIN, ACK] Seq=32 Ack=2 Win=110 Len=0
236	9.379411	35.173.72.116	104.194.123.158	TCP	85	[TCP Out-Of-Order] 443 → 49973 [PSH, ACK] Seq=1 Ack=2 Win=110
237	9.379464	104.194.123.158	35.173.72.116	TCP	54	[TCP Dup ACK 215#1] 49973 → 443 [ACK] Seq=2 Ack=1 Win=258 Len=
238	9.379545	104.194.123.158	35.173.72.116	TCP	54	49973 → 443 [RST, ACK] Seq=2 Ack=32 Win=0 Len=0
239	9.390786	128.119.245.12	104.194.123.158	TCP	66	80 → 50059 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1250 SA
240	9.390945	104.194.123.158	128.119.245.12	TCP	54	50059 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
241	9.391356	104.194.123.158	128.119.245.12	HTTP	513	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
242	9.418512	128.119.245.12	104.194.123.158	TCP	60	80 → 50059 [ACK] Seq=1 Ack=460 Win=30336 Len=0
243	9.419503	128.119.245.12	104.194.123.158	HTTP	492	HTTP/1.1 200 OK (text/html)
244	9.469094	104.194.123.158	128.119.245.12	TCP	54	50059 → 80 [ACK] Seq=460 Ack=439 Win=65792 Len=0
245	9.781465	104.194.123.158	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
246	10.232526	104.194.123.158	34.253.201.72	TCP	66	50061 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE
247	10.270863	104.194.123.158	162.247.242.21	TCP	1304	49945 → 443 [ACK] Seq=1 Ack=1 Win=64249 Len=1250 [TCP segment

> Frame 231: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0
 > Ethernet II, Src: IntelCor_98:15:cf (5c:e0:c5:98:15:cf), Dst: Cisco_9f:f0:93 (00:00:0c:9f:f0:93)
 > Internet Protocol Version 4, Src: 104.194.123.158, Dst: 216.47.143.106
 > User Datagram Protocol, Src Port: 53138, Dst Port: 53
 > Domain Name System (query)

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.)

Frame section of the GET request is 12:47:28.212674 and the same section for the HTTP OK shows an arrival time of 12:47:28.240821.

The difference of these two gives:

$$.240821 - .212674 = 0.028147 \text{ seconds}$$

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
241	12:47:28.212674	104.194.123.158	128.119.245.12	HTTP	513	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
243	12:47:28.240821	128.119.245.12	104.194.123.158	HTTP	492	HTTP/1.1 200 OK (text/html)
260	12:47:29.119623	104.194.123.158	128.119.245.12	HTTP	451	GET /favicon.ico HTTP/1.1
261	12:47:29.149711	128.119.245.12	104.194.123.158	HTTP	538	HTTP/1.1 404 Not Found (text/html)

<

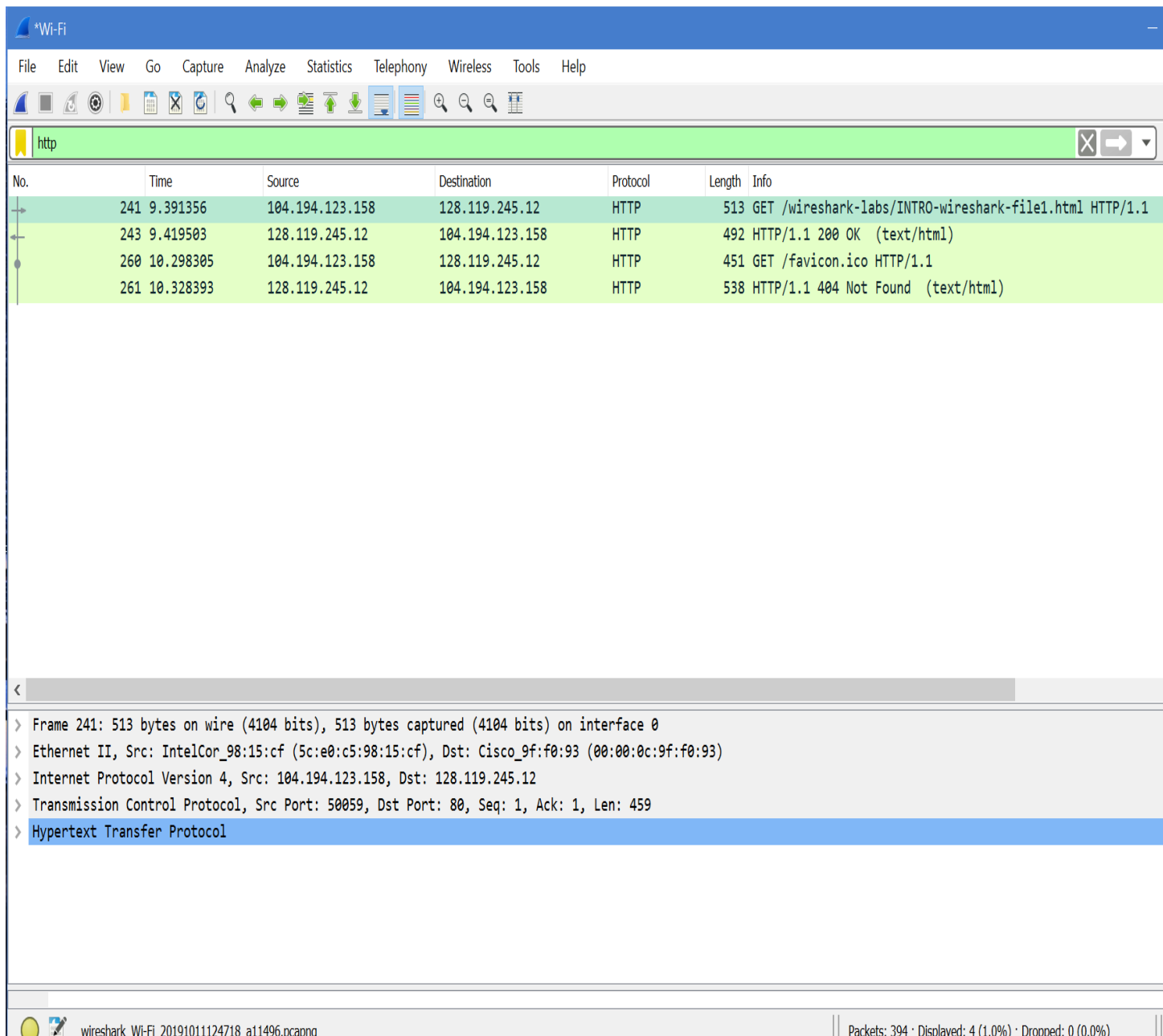
- > Frame 241: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface 0
- > Ethernet II, Src: IntelCor_98:15:cf (5c:e0:c5:98:15:cf), Dst: Cisco_9f:f0:93 (00:00:0c:9f:f0:93)
- > Internet Protocol Version 4, Src: 104.194.123.158, Dst: 128.119.245.12
- > Transmission Control Protocol, Src Port: 50059, Dst Port: 80, Seq: 1, Ack: 1, Len: 459
- > Hypertext Transfer Protocol

wireshark_Wi-Fi_20191011124718_a11496.pcapng

Packets: 394 · Displayed: 4 (1.0%) · Dropped: 0 (0.0%)

Profile: De

3. What is the Internet address of the gaia.cs.umass.edu? What is the Internet address of your computer? Support your answer with an appropriate screenshot from your computer.



IP section of the GET request, the source and destination are shown:

Source: 104.194.123.158

Destination: 128.119.245.12

Source is the local machine's address and destination is the web server's public address.

My address (local machine): 104.194.123.158

Destination IP address: 128.119.245.12

No.	Time	Source	Destination	Protocol	Length	Info
DSCP	243	12:47:28.240821	128.119.245.12	104.194.123.158	HTTP	492 HTTP/1.1 200 OK (text/html)
Default						
Frame 243: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0						
Ethernet II, Src: Cisco_0d:da:3f (78:0c:f0:0d:da:3f), Dst: IntelCor_98:15:cf (5c:e0:c5:98:15:cf)						
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 104.194.123.158						
Transmission Control Protocol, Src Port: 80, Dst Port: 50059, Seq: 1, Ack: 460, Len: 438						
Hypertext Transfer Protocol						
Line-based text data: text/html (3 lines)						