Justin Phillips

cs372 summer 2020

6/24/2020

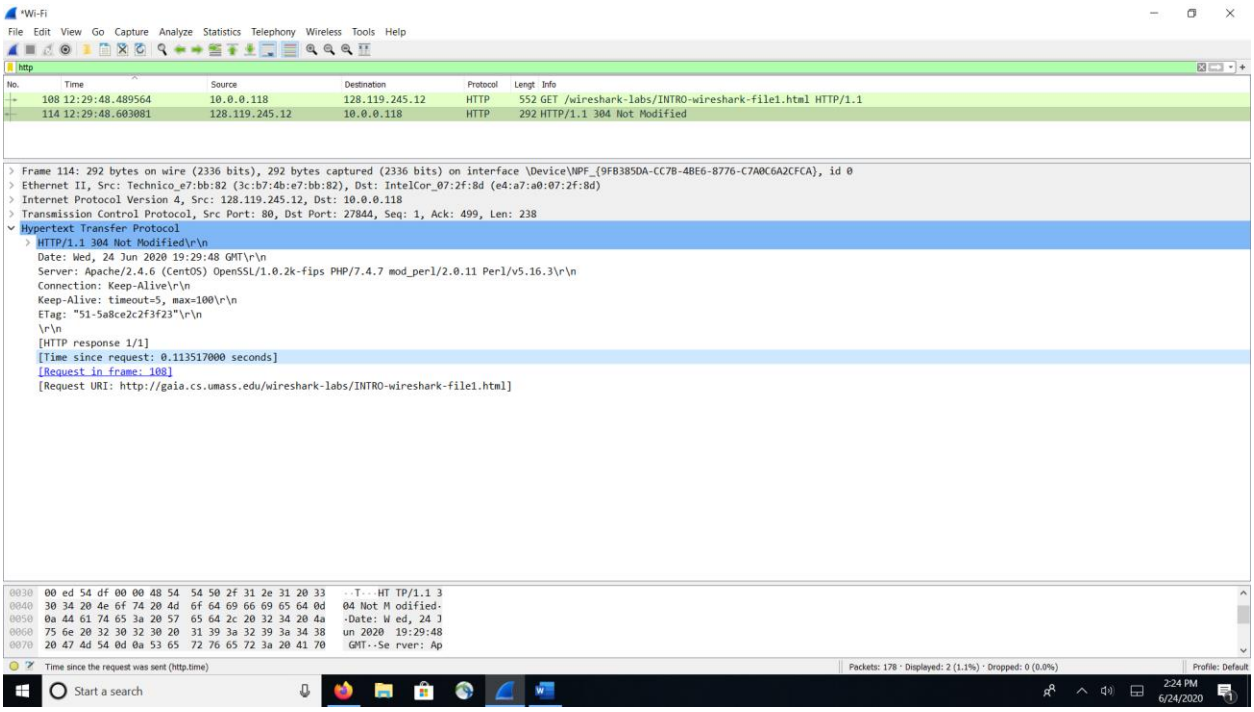
1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

Three different protocols that appear in the protocol column in the unfiltered packet-listing window are TCP, DNS and HTTP

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.)

The get request was made at 12:29:48.489564 and the ok reply was at 12:29:48.603081 so it took .113517 seconds

screen shot of the original values and the highlighted response ti



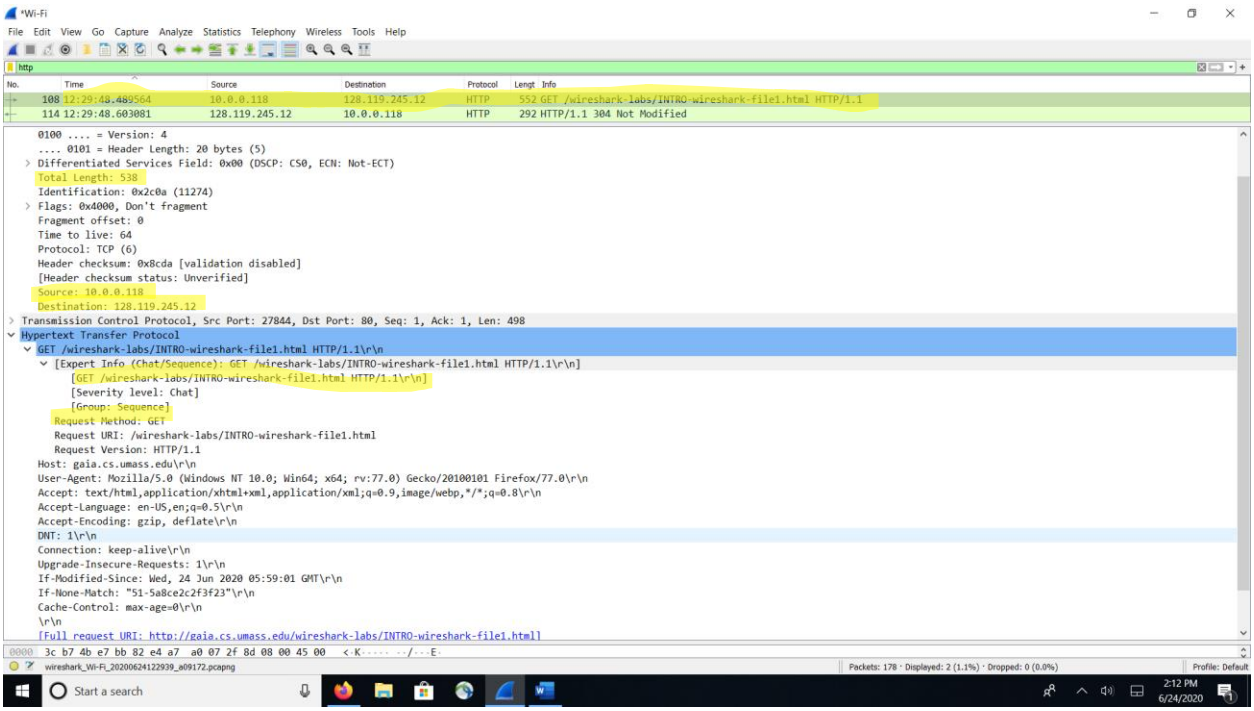
3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?

http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html : 128.119.245.12

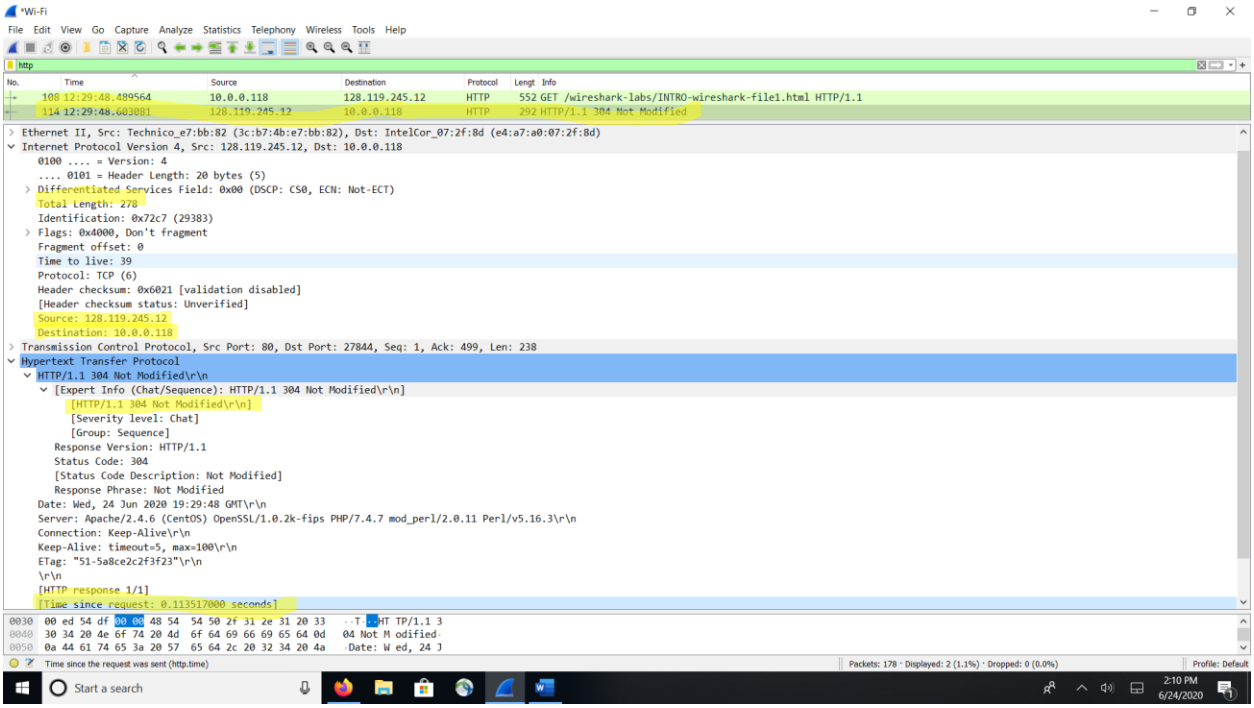
address of my pc 10.0.0.118

4. Screenshot the two HTTP messages (GET and OK) referred to in question 2 above. Make sure to include all pertinent information in the screenshot (Time field, Internet addresses, etc). Paste these screenshots into your lab report.

Get



Return OK


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Lengt Info
108 12:29:48.489564 10.0.0.118 128.119.245.12 HTTP 552 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
114 12:29:48.603081 128.119.245.12 10.0.0.118 HTTP 292 HTTP/1.1 304 Not Modified
Ethernet II, Src: Technico_e7:bb:82 (3c:b7:4b:e7:bb:82), Dst: IntelCor_07:2f:8d (e4:a7:a0:07:2f:8d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.118
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 278
Identification: 0x72c7 (29383)
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 39
Protocol: TCP (6)
Header checksum: 0x6021 [validation disabled]
[Header checksum status: Unverified]
Source: 128.119.245.12
Destination: 10.0.0.118
Transmission Control Protocol, Src Port: 80, Dst Port: 27844, Seq: 1, Ack: 499, Len: 238
Hypertext Transfer Protocol
HTTP/1.1 304 Not Modified\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
[HTTP/1.1 304 Not Modified\r\n]
[Severity level: Chat]
[Group: Sequence]
Response Version: HTTP/1.1
Status Code: 304
[Status Code Description: Not Modified]
Response Phrase: Not Modified
Date: Wed, 24 Jun 2020 19:29:48 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.7 mod_perl/2.0.11 Perl/v5.16.3\r\n
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=100\r\n
ETag: "51-5a8ce2c2f3f23"\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.113517000 seconds]
0030 00 ed 54 df 00 00 48 54 54 50 2f 31 2e 31 20 33
0040 30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65 64 0d
0050 0a 44 61 74 65 3a 20 57 65 64 2c 20 32 34 20 4a
Time since the request was sent (http.time)
Packets: 178 · Displayed: 2 (1.1%) · Dropped: 0 (0.0%)
Profile: Default
Start a search
2:10 PM
6/24/2020