Gabriel Emerson

ELEC 5220 - Lab 1

8/26/21

Questions

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

Besides the HTTP there is also TCP, UDP, ARP, DNS, MDNS and more!

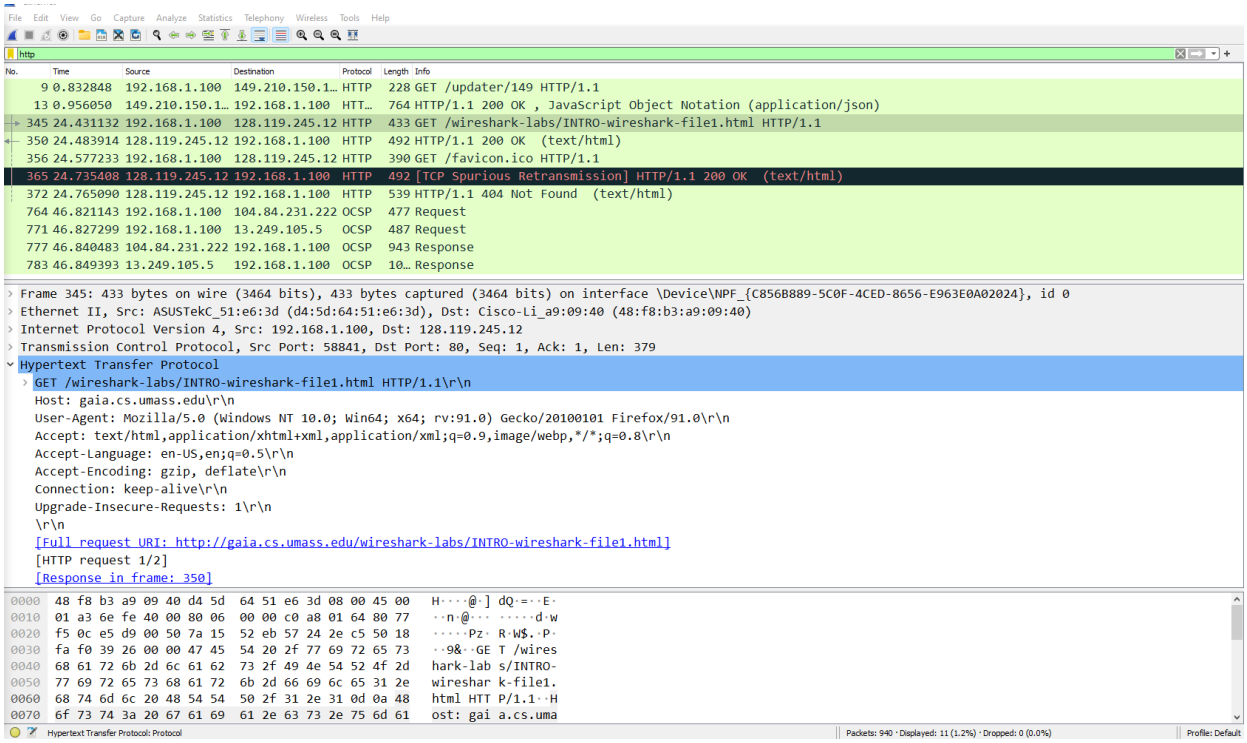
2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

GET started at 17:25:33, and OK was at 17:25:33. It was at the same time for calling GET on both HTTP updater (I assume is called when launching a browser) and when going to the wireshark website

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?

The address of the website is 128.119.245.12 and my computer is 192.168.1.100

Attached below is also a screenshot of the Wireshark page just in case any numbers did not make sense.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
9 0.832848 192.168.1.100 149.210.150.1… HTTP 228 GET /updater/149 HTTP/1.1
13 0.956050 149.210.150.1… 192.168.1.100 HTT… 764 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
345 24.431132 192.168.1.100 128.119.245.12 HTTP 433 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
350 24.483914 128.119.245.12 192.168.1.100 HTTP 492 HTTP/1.1 200 OK (text/html)
356 24.577233 192.168.1.100 128.119.245.12 HTTP 390 GET /favicon.ico HTTP/1.1
365 24.735408 128.119.245.12 192.168.1.100 HTTP 492 [TCP Spurious Retransmission] HTTP/1.1 200 OK (text/html)
372 24.765090 128.119.245.12 192.168.1.100 HTTP 539 HTTP/1.1 404 Not Found (text/html)
764 46.821143 192.168.1.100 104.84.231.222 OCSP 477 Request
771 46.827299 192.168.1.100 13.249.105.5 OCSP 487 Request
777 46.840483 104.84.231.222 192.168.1.100 OCSP 943 Response
783 46.849393 13.249.105.5 192.168.1.100 OCSP 10… Response
Frame 345: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on interface \Device\NPF_{C856B889-5C0F-4CED-8656-E963E0A02024}, id 0
Ethernet II, Src: ASUSTekC_51:e6:3d (d4:5d:64:51:e6:3d), Dst: Cisco-Li_a9:09:40 (48:f8:b3:a9:09:40)
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 58841, Dst Port: 80, Seq: 1, Ack: 1, Len: 379
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 NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 1/2]
[Response in frame: 350]
0000 48 f8 b3 a9 09 40 d4 5d 64 51 e6 3d 08 00 45 00 H····@·] dQ·=··E·
0010 01 a3 6e fe 40 00 80 06 00 00 c0 a8 01 64 80 77 ··n·@··· ·····d·w
0020 f5 0c e5 d9 00 50 7a 15 52 eb 57 24 2e c5 50 18 ·····Pz· R·W$.·P·
0030 fa f0 39 26 00 00 47 45 54 20 2f 77 69 72 65 73 ··9&··GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d hark-lab s/INTRO-
0050 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e wireshar k-file1.
0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 html HTT P/1.1··H
0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 ost: gai a.cs.uma
Hypertext Transfer Protocol: Protocol
Packets: 940 · Displayed: 11 (1.2%) · Dropped: 0 (0.0%)
Profile: Default