Computer Network Lab
CS359

Tanishq Malu | Lab1: Wireshark Intro | 1901CS63

Questions

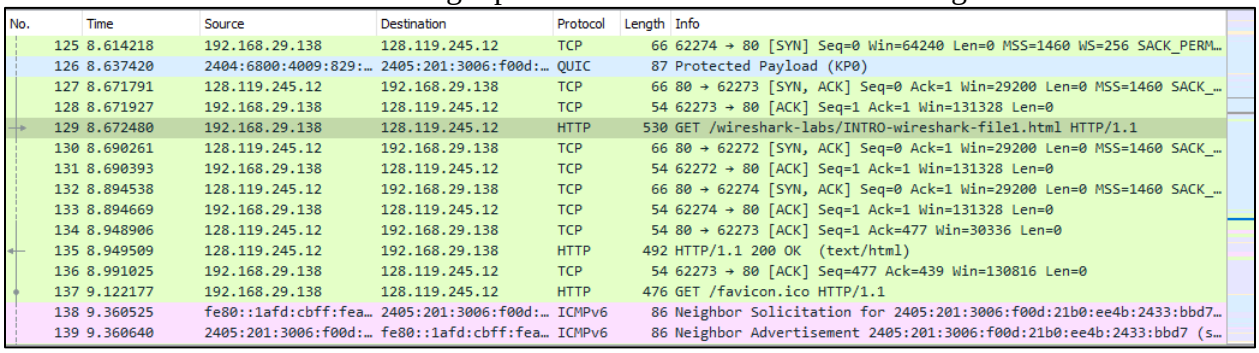
1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

Ans: Three Different protocols which I received while capturing the packets are:

a. TCP: The Transmission Control Protocol (TCP) is a transport protocol that is used on top of IP to ensure reliable transmission of packets.

b. QUIC: QUIC (Quick UDP Internet Connections, pronounced quick) is a general-purpose transport layer network.

c. ICMPv6: Internet Control Message Protocol version 6 is a protocol which acts as a communication messenger protocol between the communicating devices in IP network



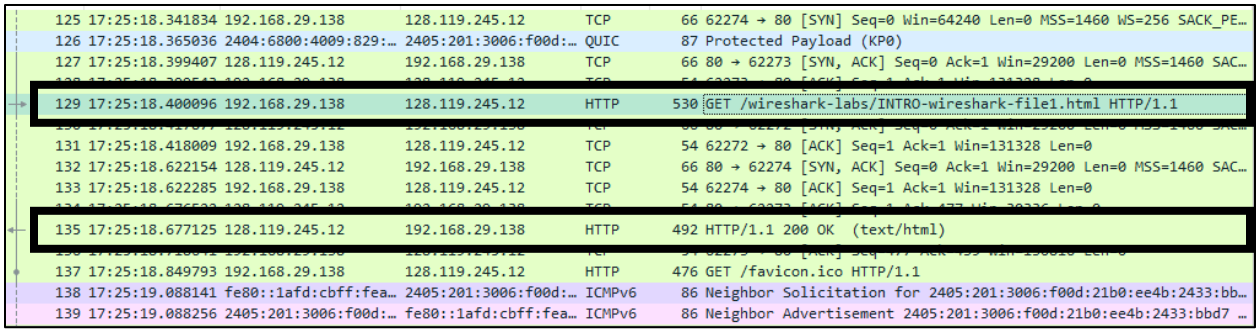
No.	Time	Source	Destination	Protocol	Length	Info
125	8.614218	192.168.29.138	128.119.245.12	TCP	66	62274 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM…
126	8.637420	2404:6800:4009:829:…	2405:201:3006:f00d:…	QUIC	87	Protected Payload (KP0)
127	8.671791	128.119.245.12	192.168.29.138	TCP	66	80 → 62273 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_…
128	8.671927	192.168.29.138	128.119.245.12	TCP	54	62273 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
129	8.672480	192.168.29.138	128.119.245.12	HTTP	530	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
130	8.690261	128.119.245.12	192.168.29.138	TCP	66	80 → 62272 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_…
131	8.690393	192.168.29.138	128.119.245.12	TCP	54	62272 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
132	8.894538	128.119.245.12	192.168.29.138	TCP	66	80 → 62274 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_…
133	8.894669	192.168.29.138	128.119.245.12	TCP	54	62274 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
134	8.948906	128.119.245.12	192.168.29.138	TCP	54	80 → 62273 [ACK] Seq=1 Ack=477 Win=30336 Len=0
135	8.949509	128.119.245.12	192.168.29.138	HTTP	492	HTTP/1.1 200 OK (text/html)
136	8.991025	192.168.29.138	128.119.245.12	TCP	54	62273 → 80 [ACK] Seq=477 Ack=439 Win=130816 Len=0
137	9.122177	192.168.29.138	128.119.245.12	HTTP	476	GET /favicon.ico HTTP/1.1
138	9.360525	fe80::1afd:cbff:fea…	2405:201:3006:f00d:…	ICMPv6	86	Neighbor Solicitation for 2405:201:3006:f00d:21b0:ee4b:2433:bbd7…
139	9.360640	2405:201:3006:f00d:…	fe80::1afd:cbff:fea…	ICMPv6	86	Neighbor Advertisement 2405:201:3006:f00d:21b0:ee4b:2433:bbd7 (s…

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: Time when HTTP Get request was sent: 17:25:18.400096

Time when HTTP OK reply was received: 17:25:18.677125

Time Difference = 0.277029 seconds



125	17:25:18.341834	192.168.29.138	128.119.245.12	TCP	66 62274 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PE…
126	17:25:18.365036	2404:6800:4009:829:…	2405:201:3006:f00d:…	QUIC	87 Protected Payload (KP0)
127	17:25:18.399407	128.119.245.12	192.168.29.138	TCP	66 80 → 62273 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SAC…
129	17:25:18.400096	192.168.29.138	128.119.245.12	HTTP	530 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
131	17:25:18.418009	192.168.29.138	128.119.245.12	TCP	54 62272 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
132	17:25:18.622154	128.119.245.12	192.168.29.138	TCP	66 80 → 62274 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SAC…
133	17:25:18.622285	192.168.29.138	128.119.245.12	TCP	54 62274 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
135	17:25:18.677125	128.119.245.12	192.168.29.138	HTTP	492 HTTP/1.1 200 OK (text/html)
137	17:25:18.849793	192.168.29.138	128.119.245.12	HTTP	476 GET /favicon.ico HTTP/1.1
138	17:25:19.088141	fe80::1afd:cbff:fea…	2405:201:3006:f00d:…	ICMPv6	86 Neighbor Solicitation for 2405:201:3006:f00d:21b0:ee4b:2433:bb…
139	17:25:19.088256	2405:201:3006:f00d:…	fe80::1afd:cbff:fea…	ICMPv6	86 Neighbor Advertisement 2405:201:3006:f00d:21b0:ee4b:2433:bbd7 …

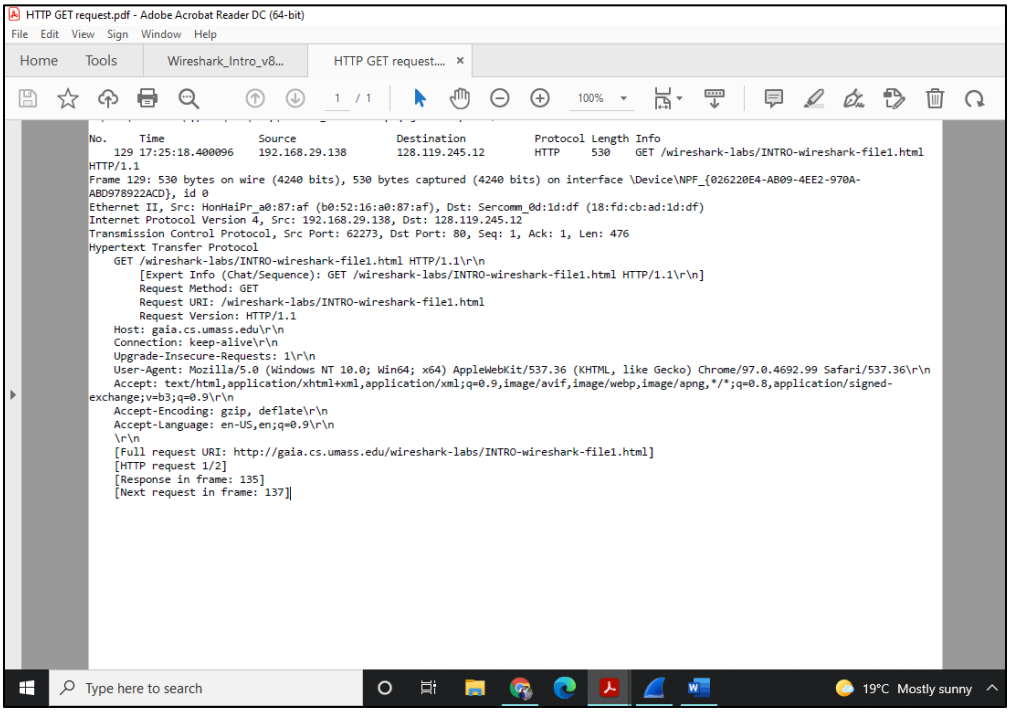
3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?

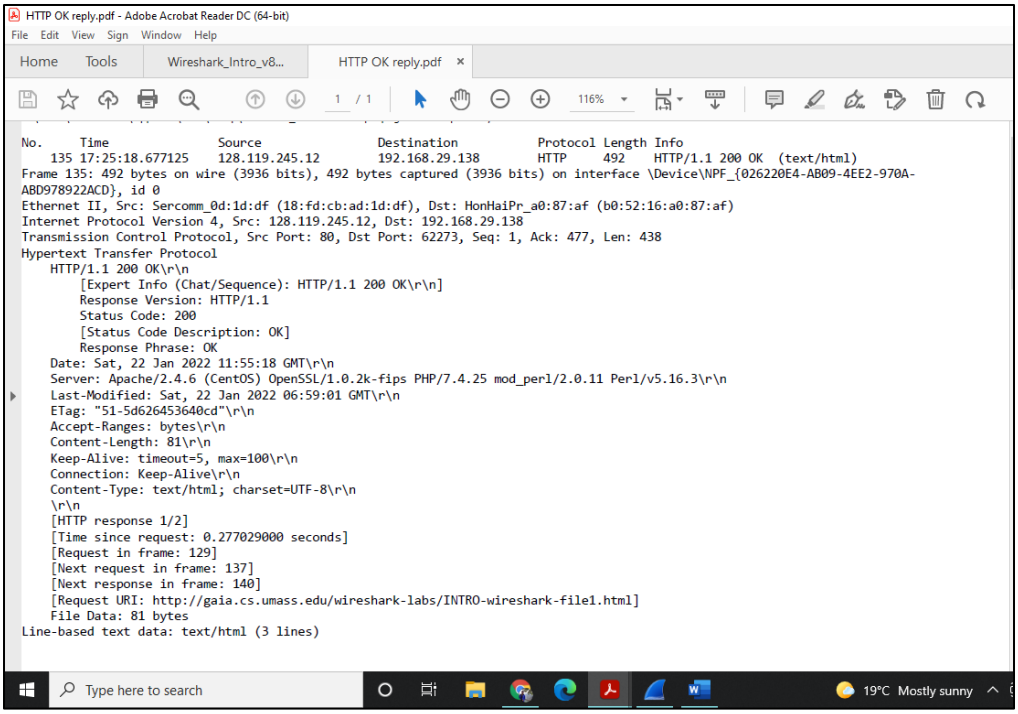
Ans: IP address of gaia.cs.umass.edu : 128.119.245.12

IP address of my computer : 192.168.29.138

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:




HTTP OK reply.pdf - Adobe Acrobat Reader DC (64-bit)
File Edit View Sign Window Help
Home Tools Wireshark_Intro_v8... HTTP OK reply.pdf
No. Time Source Destination Protocol Length Info
135 17:25:18.677125 128.119.245.12 192.168.29.138 HTTP 492 HTTP/1.1 200 OK (text/html)
Frame 135: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{026220E4-AB09-4EE2-970A-ABD978922ACD}, id 0
Ethernet II, Src: Sercomm_0d:1d:df (18:fd:cb:ad:1d:df), Dst: HonHaiPr_a0:87:af (b0:52:16:a0:87:af)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.29.138
Transmission Control Protocol, Src Port: 80, Dst Port: 62273, Seq: 1, Ack: 477, Len: 438
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Sat, 22 Jan 2022 11:55:18 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Sat, 22 Jan 2022 06:59:01 GMT\r\n
ETag: "51-5d626453640cd"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 81\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.277029000 seconds]
[Request in frame: 129]
[Next request in frame: 137]
[Next response in frame: 140]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
File Data: 81 bytes
Line-based text data: text/html (3 lines)
Type here to search
19°C Mostly sunny

The End