Student Information

Full Name : Mehmet Rüçhan Yavuzdemir
Id Number: 2522159

Answer 1

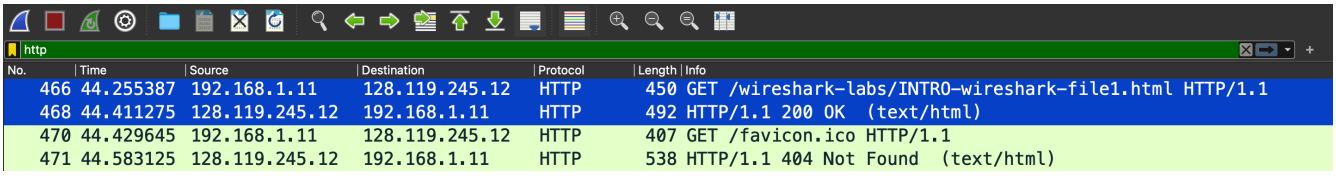
tcp || quic || http || dns || udp || tls

No.	Time	Source	Destination	Protocol	Length	Info
83	7.002934	192.168.1.11	34.117.65.55	TCP	66	63027 → 443 [ACK] Seq=1 Ack=25 Win=2047 Len=0 TSval=37565
84	7.003189	192.168.1.11	34.117.65.55	TLSv1.2	94	Application Data
85	7.055579	34.117.65.55	192.168.1.11	TCP	66	443 → 63027 [ACK] Seq=25 Ack=29 Win=285 Len=0 TSval=17341
86	7.099985	128.119.245.12	192.168.1.11	TCP	66	[TCP Retransmission] 80 → 63580 [SYN, ACK] Seq=0 Ack=1 Wi
87	7.100083	192.168.1.11	128.119.245.12	TCP	54	[TCP Dup ACK 68#1] 63580 → 80 [ACK] Seq=1 Ack=1 Win=26214
88	7.642358	192.168.1.11	128.119.245.12	TCP	78	[TCP Retransmission] 63581 → 80 [SYN] Seq=0 Win=65535 Len
89	7.807261	128.119.245.12	192.168.1.11	TCP	66	80 → 63581 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=145
90	7.807464	192.168.1.11	128.119.245.12	TCP	54	63581 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
92	8.538095	192.168.1.4	255.255.255.255	UDP	214	60447 → 6667 Len=172
100	11.712376	192.168.1.11	128.119.245.12	TCP	54	63580 → 80 [FIN, ACK] Seq=1 Ack=1 Win=262144 Len=0
102	12.394723	192.168.1.11	128.119.245.12	TCP	54	[TCP Retransmission] 63580 → 80 [FIN, ACK] Seq=1 Ack=1 Wi
103	12.559064	128.119.245.12	192.168.1.11	TCP	60	80 → 63580 [FIN, ACK] Seq=1 Ack=2 Win=29312 Len=0
104	12.559301	192.168.1.11	128.119.245.12	TCP	54	63580 → 80 [ACK] Seq=2 Ack=2 Win=262144 Len=0
105	13.555587	192.168.1.4	255.255.255.255	UDP	214	60447 → 6667 Len=172
106	13.715526	192.168.1.11	128.119.245.12	TCP	54	63581 → 80 [FIN, ACK] Seq=1 Ack=1 Win=262144 Len=0
107	13.885827	128.119.245.12	192.168.1.11	TCP	60	80 → 63581 [FIN, ACK] Seq=1 Ack=2 Win=29312 Len=0
108	13.886094	192.168.1.11	128.119.245.12	TCP	54	63581 → 80 [ACK] Seq=2 Ack=2 Win=262144 Len=0
112	16.786074	192.168.1.11	128.119.245.12	TCP	78	63584 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSv
113	16.791296	192.168.1.11	128.119.245.12	TCP	78	63585 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSv
114	16.979311	128.119.245.12	192.168.1.11	TCP	66	80 → 63584 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=145
115	16.979314	128.119.245.12	192.168.1.11	TCP	66	80 → 63585 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=145
116	16.979524	192.168.1.11	128.119.245.12	TCP	54	63584 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
117	16.979596	192.168.1.11	128.119.245.12	TCP	54	63585 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
119	18.371426	128.119.245.12	192.168.1.11	TCP	66	[TCP Retransmission] 80 → 63585 [SYN, ACK] Seq=0 Ack=1 Wi
120	18.371567	192.168.1.11	128.119.245.12	TCP	54	[TCP Dup ACK 117#1] 63585 → 80 [ACK] Seq=1 Ack=1 Win=2621
121	18.466548	192.168.1.4	255.255.255.255	UDP	214	60447 → 6667 Len=172
122	18.920942	2a02:e0:6791:9…	2a02:e0:4f10::1	DNS	116	Standard query 0x9ed2 HTTPS googlehosted.l.googleuserconte
123	18.947136	2a02:e0:4f10::1	2a02:e0:6791:9…	DNS	176	Standard query response 0x9ed2 HTTPS googlehosted.l.googl
124	18.952244	2a02:e0:6791:9…	2a00:1450:4017…	QUIC	12…	Initial, DCID=742a010a442a0341, PKN: 0, CRYPTO, PADDING
125	18.997663	2a00:1450:4017…	2a02:e0:6791:9…	QUIC	12…	Initial, SCID=f42a010a442a0341, PKN: 1, ACK, CRYPTO, PADD

Figure 1: Protocols

I made a query `tcp || quic || HTTP || DNS || udp || tls` to the table. I could gather all of them except HTTP, but I already have it in Figure 2. Hence, I have **TCP, QUIC, HTTP, DNS, UDP, and TLSv1.2** in my file.

Answer 2

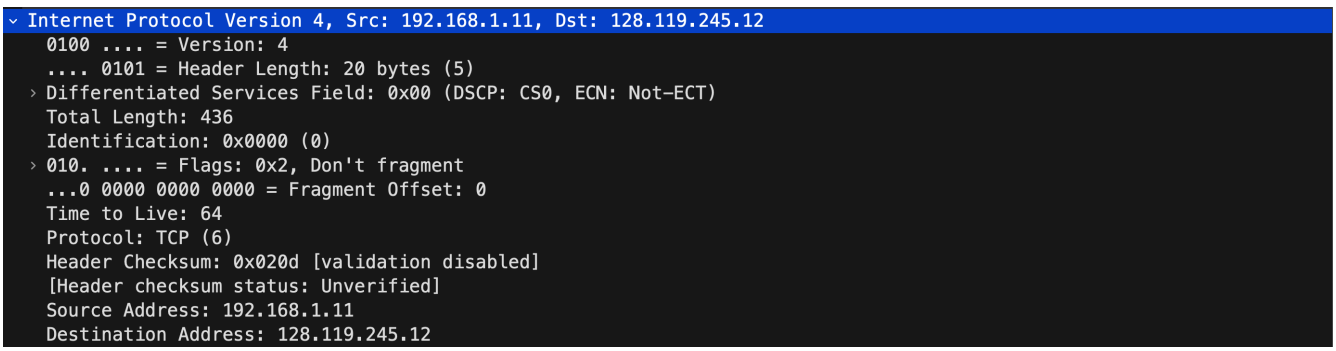


No.	Time	Source	Destination	Protocol	Length	Info
466	44.255387	192.168.1.11	128.119.245.12	HTTP	450	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
468	44.411275	128.119.245.12	192.168.1.11	HTTP	492	HTTP/1.1 200 OK (text/html)
470	44.429645	192.168.1.11	128.119.245.12	HTTP	407	GET /favicon.ico HTTP/1.1
471	44.583125	128.119.245.12	192.168.1.11	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Figure 2: HTTP Requests

The highlighted rows are the ones we are interested in this question. If we find the time between them, we can find how many seconds it took to get a response from the server. I subtracted 44.255387 from 44.411275 and got 0.155888. Finally, I rounded it to 0.156. It took **0.156** seconds to receive an HTTP 200 OK message after sending the request.

Answer 3



```
Internet Protocol Version 4, Src: 192.168.1.11, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 436
    Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x020d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.11
    Destination Address: 128.119.245.12
```

Figure 3: IP

The Internet address of `gaia.cs.umass.edu` is called the destination address, and the client's address is called the source address. It can be seen from Figure 3 that the destination address is `128.119.245.12` and the source address is `192.168.1.11`. Hence the Internet address of `gaia.cs.umass.edu` is `128.119.245.12` and the Internet address of my computer is `192.168.1.11`.

Answer 4

```
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 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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: 468]
    [Next request in frame: 470]
```

Figure 4: HTTP

Mozilla Firefox is mentioned in the User-Agent header information. Hence, the client uses Firefox Browser on the computer.

Answer 5

```
Transmission Control Protocol, Src Port: 63586, Dst Port: 80, Seq: 1, Ack: 1, Len: 396
    Source Port: 63586
    Destination Port: 80
    [Stream index: 12]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 396]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2469234203
    [Next Sequence Number: 397    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3719385537
    0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
    Window: 4096
    [Calculated window size: 262144]
    [Window size scaling factor: 64]
    Checksum: 0x4cf0 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  [Timestamps]
  [SEQ/ACK analysis]
    TCP payload (396 bytes)
```

Figure 5: TCP

It can be seen from the figure above that the destination port is `80`, to which the HTTP request is being sent.