

K. N. V. L. Manicharan
AP20110010143
Computer Networks Lab
Experiment 1

1. List up to 10 different protocols that appear in the protocol column in the unfiltered packet-listing window.

Ans :-

- TCP
- QUIC
- TLSv1.3
- DNS
- SSDP
- HTTP
- ICMP
- ARP
- Broadcast
- MDNS

2. How long did it take from when the HTTP (or TLS) GET message was sent until the HTTP OK reply was received? Include the screen shot.

Ans :-

It took approximately 0.146462 seconds to receive an HTTP OK reply, after sending a GET message.

32467	22:40:45.628246	192.168.0.8	115.247.40.229	HTTP	504 GET /moodle/ HTTP/1.1
32514	22:40:45.774708	115.247.40.229	192.168.0.8	HTTP	676 HTTP/1.1 200 OK (text/html)

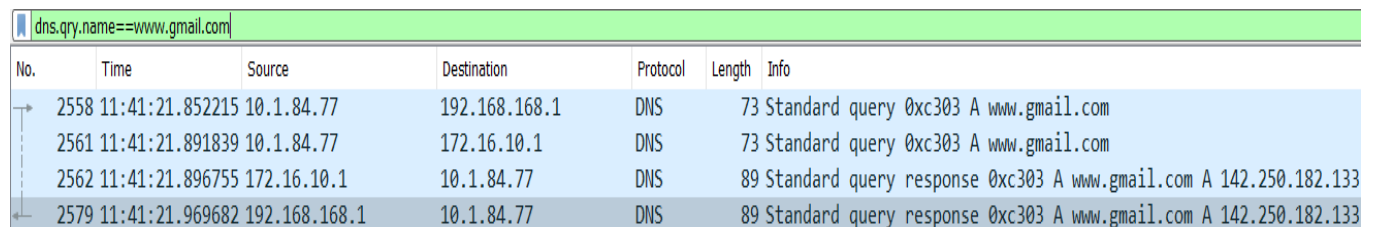
3. What is the Internet address (IP address) of www.gmail.com? What is the Internet address of your computer? Include a screenshot and describe where you got the data to answer this question.

Ans :-

IP address of your computer is 10.1.84.77

IP address of www.gmail.com is 142.250.182.133

I found the IP address of www.gmail.com with some help by searching through Google and I have used a display filter and it is `dns.qry.name == www.gmail.com`, and we can see that in the given screenshot below.



The screenshot shows a Wireshark packet capture with a display filter of `dns.qry.name==www.gmail.com`. The packet list contains four entries, all of which are DNS queries or responses for the domain www.gmail.com. The first two packets (2558 and 2561) are standard queries from source IP 10.1.84.77 to destination IP 192.168.168.1 and 172.16.10.1 respectively. The next two packets (2562 and 2579) are standard query responses from source IP 172.16.10.1 and 192.168.168.1 respectively, both returning the IP address 142.250.182.133 for the domain.

No.	Time	Source	Destination	Protocol	Length	Info
2558	11:41:21.852215	10.1.84.77	192.168.168.1	DNS	73	Standard query 0xc303 A www.gmail.com
2561	11:41:21.891839	10.1.84.77	172.16.10.1	DNS	73	Standard query 0xc303 A www.gmail.com
2562	11:41:21.896755	172.16.10.1	10.1.84.77	DNS	89	Standard query response 0xc303 A www.gmail.com A 142.250.182.133
2579	11:41:21.969682	192.168.168.1	10.1.84.77	DNS	89	Standard query response 0xc303 A www.gmail.com A 142.250.182.133

4. How many packets did you capture (total of all protocols, not just TLS)? Now, use display filters to determine how many packets contain your IP address (Hint: Use `ip.addr`). Now, reverse the filter to determine how many packets don't contain your IP address. See any problems here? If not, you've already figured out the point of this question, so explain how you did so. If so, how can this problem be fixed? What are the appropriate display filters to use? How does Wireshark warn you of such a problem?

Ans :-

Total number of packets captured = 64626

Total number of packets that contain my IP address = 57658

Total number of packets that does not contain my IP address
= 4497

Explanation :-

In the question we have been given a hint, it is ip.addr. I have used it find number of packets that contain my IP address, and to get number of packets that does not contain my IP address I used '!=' in place of '=='.

5. Use your newly acquired Wireshark skills to capture the process when your browser loads the front page of SRM's website (i.e. <https://srmap.edu.in/>). How many packets did you capture? Were all of them TLS? How many TLS requests did you make?

Were all the replies OK? Did you find anything else interesting? Ensure you have examined this packet capture in detail, using appropriate Wireshark functionality. Write up what you saw (yes, please include screen captures where you think they are necessary).

Ans :-

I have captured 1059 packets. No, there are packets other than TLS and I make 81 TLS requests and replies are not always OK.

1050	22:54:09.123388	192.168.0.1	192.168.0.8	DNS	88 Standard query response 0x9086 A srmap.edu.in A 3.7.78.115
1051	22:54:09.123388	192.168.0.1	192.168.0.8	DNS	88 Standard query response 0x9086 A srmap.edu.in A 3.7.78.115

To find the IP address of the <https://srmap.edu.in/> .

The image shows a Wireshark packet capture window. The top pane displays a list of packets. The selected packet (No. 1108) is a TLSv1.2 Application Data packet. The middle pane shows the packet details, including the TLSv1.2 structure and the application data. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1088	22:54:09.187574	3.7.78.115	192.168.0.8	TCP	1494	443 → 62782 [ACK] Seq=4097 Ack=518 Win=28032 Len=1440 [TCP segment of a reassembled PDU]
1089	22:54:09.187574	3.7.78.115	192.168.0.8	TLSv1.2	603	Certificate, Server Key Exchange, Server Hello Done
1090	22:54:09.187588	192.168.0.8	3.7.78.115	TCP	54	62782 → 443 [ACK] Seq=518 Ack=6086 Win=132352 Len=0
1091	22:54:09.189471	3.7.78.115	192.168.0.8	TCP	54	443 → 62783 [ACK] Seq=1 Ack=518 Win=28032 Len=0
1092	22:54:09.189909	3.7.78.115	192.168.0.8	TLSv1.2	2934	Server Hello
1093	22:54:09.189909	3.7.78.115	192.168.0.8	TCP	1270	443 → 62783 [PSH, ACK] Seq=2881 Ack=518 Win=28032 Len=1216 [TCP segment of a reassembled PDU]
1094	22:54:09.189946	192.168.0.8	3.7.78.115	TCP	54	62783 → 443 [ACK] Seq=518 Ack=4097 Win=132352 Len=0
1095	22:54:09.190717	3.7.78.115	192.168.0.8	TCP	1494	443 → 62783 [ACK] Seq=4097 Ack=518 Win=28032 Len=1440 [TCP segment of a reassembled PDU]
1096	22:54:09.190717	3.7.78.115	192.168.0.8	TLSv1.2	603	Certificate, Server Key Exchange, Server Hello Done
1097	22:54:09.190735	192.168.0.8	3.7.78.115	TCP	54	62783 → 443 [ACK] Seq=518 Ack=6086 Win=132352 Len=0
1098	22:54:09.194675	192.168.0.8	3.7.78.115	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1099	22:54:09.195318	192.168.0.8	3.7.78.115	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1100	22:54:09.225310	3.7.78.115	192.168.0.8	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1101	22:54:09.225634	192.168.0.8	3.7.78.115	TLSv1.2	752	Application Data
1102	22:54:09.227214	3.7.78.115	192.168.0.8	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1103	22:54:09.257870	3.7.78.115	192.168.0.8	TLSv1.2	4374	Application Data
1109	22:54:09.257914	192.168.0.8	3.7.78.115	TCP	54	62782 → 443 [ACK] Seq=1342 Ack=10680 Win=132352 Len=0

Frame 1108: 4374 bytes on wire (34992 bits), 4374 bytes captured (34992 bits) on interface \Device\NPF_{57A2096D-CB3A-468C-9841-08DF8A9074B}, id 0
 Ethernet II, Src: TP-Link a2:41:66 (Sc:a6:e6:a2:41:66), Dst: IntelCor_de:de:f1 (34:cf:f6:de:de:f1)
 Internet Protocol Version 4, Src: 3.7.78.115, Dst: 192.168.0.8
 Transmission Control Protocol, Src Port: 443, Dst Port: 62782, Seq: 6360, Ack: 1342, Len: 4320
 Transport Layer Security

0000 34 cf f6 de de f1 5c a6 e6 a2 41 66 08 00 45 00 4.....\..Af..E:
 0010 11 08 01 1a 40 00 31 06 25 ac 03 07 4e 73 c0 a8@.1.%.Ns..
 0020 00 08 01 bb f5 3e b8 41 4c ed b6 49 3f 39 50 10>A L..I79P..
 0030 00 e6 00 00 00 17 03 03 02 49 4d ad fe 3b 77IR..;w

wireshark_WF-F2A2QR1.pcapng Packets: 28352 - Displayed: 1059 (3.7%) Profile: Default

To find the number packets captured while loading the homepage of <https://srmap.edu.in/> .

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==3.7.78.115 && ts && ip.addr==3.7.78.115 && ts && ip.src==192.168.0.8

No.	Time	Source	Destination	Protocol	Length	Info
1077	22:54:09.155771	192.168.0.8	3.7.78.115	TLSv1.2	571	Client Hello
1080	22:54:09.157455	192.168.0.8	3.7.78.115	TLSv1.2	571	Client Hello
1085	22:54:09.186713	3.7.78.115	192.168.0.8	TLSv1.2	2934	Server Hello
1089	22:54:09.187574	3.7.78.115	192.168.0.8	TLSv1.2	603	Certificate, Server Key Exchange, Server Hello Done
1092	22:54:09.189909	3.7.78.115	192.168.0.8	TLSv1.2	2934	Server Hello
1096	22:54:09.190717	3.7.78.115	192.168.0.8	TLSv1.2	603	Certificate, Server Key Exchange, Server Hello Done
1098	22:54:09.194675	192.168.0.8	3.7.78.115	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1099	22:54:09.195318	192.168.0.8	3.7.78.115	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1102	22:54:09.225310	3.7.78.115	192.168.0.8	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1103	22:54:09.225634	192.168.0.8	3.7.78.115	TLSv1.2	752	Application Data
1104	22:54:09.227214	3.7.78.115	192.168.0.8	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1108	22:54:09.257070	3.7.78.115	192.168.0.8	TLSv1.2	4374	Application Data
1115	22:54:09.288888	3.7.78.115	192.168.0.8	TLSv1.2	5814	Application Data [TCP segment of a reassembled PDU]
1118	22:54:09.289154	3.7.78.115	192.168.0.8	TLSv1.2	830	Application Data
1120	22:54:09.293589	192.168.0.8	3.7.78.115	TLSv1.2	739	Application Data
1121	22:54:09.294796	192.168.0.8	3.7.78.115	TLSv1.2	692	Application Data
1165	22:54:09.321964	192.168.0.8	3.7.78.115	TLSv1.2	572	Client Hello

> Frame 1077: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Device\NPF_{57A2096D-CB3A-468C-9841-08DF8A99074B}, id 0

> Ethernet II, Src: IntelCor_de:de:f1 (34:cf:f6:de:de:f1), Dst: TP-Link_a2:41:66 (5c:a6:e6:a2:41:66)

> Internet Protocol Version 4, Src: 192.168.0.8, Dst: 3.7.78.115

> Transmission Control Protocol, Src Port: 62782, Dst Port: 443, Seq: 1, Ack: 1, Len: 517

> Transport Layer Security

```

0000  5c a6 e6 a2 41 66 34 cf f6 de de f1 00 00 45 00  \...Af4. ....E:
0010  02 2d b5 0d 40 00 80 06 00 00 c9 a8 00 08 03 07  --@- .....
0020  4e 73 f5 3e 01 bb b6 49 39 fc b8 41 34 16 50 18  Ns>...I 9--A4 P:
0030  02 05 14 4a 00 00 16 03 01 02 00 01 00 01 fc 03  --J.....

```

wireshark_Wi-Fi2AQR1.pcapng

Packets: 64626 - Displayed: 473 (0.7%) - Dropped: 0 (0.0%)

Profile: Default

To find the number of TLS packets made by me.