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.

dns.qry.name==www.gmail.com

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?

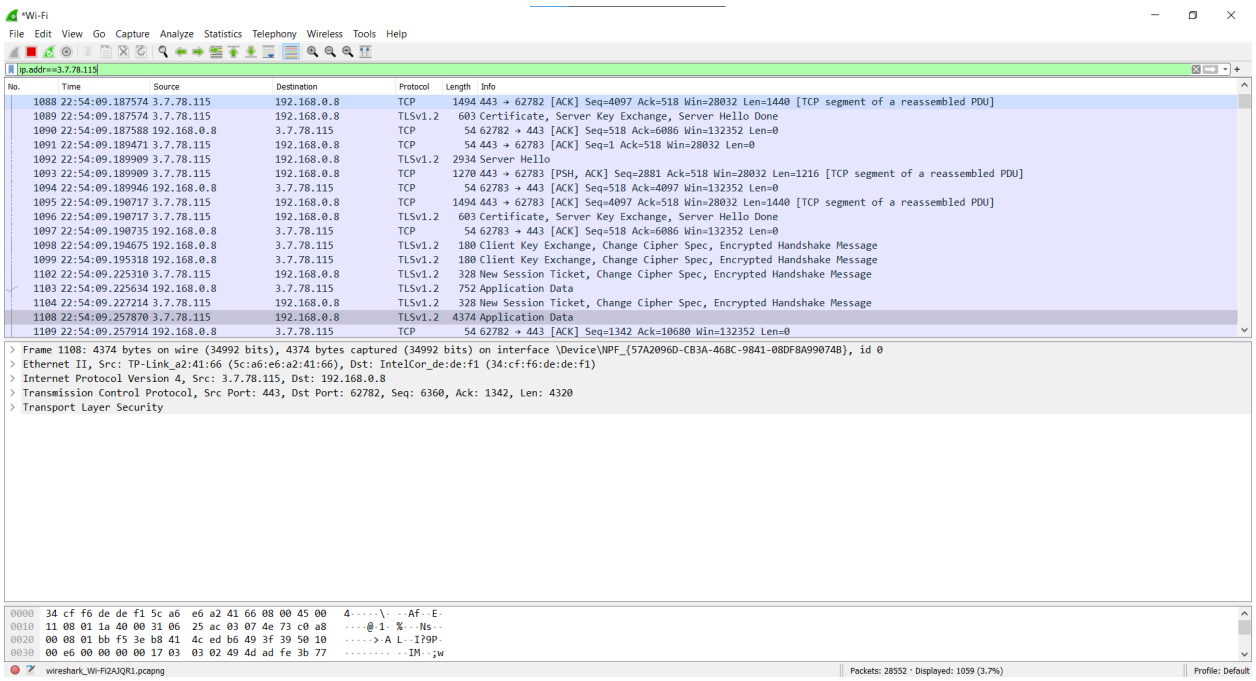
Were all the replies OK? Did you find anything else interesting? Ensure you have examined this packet capture in detail, using appropriate Wireshark functionality. Write up what you saw (yes, please include screen captures where you think they are necessary).

Ans :-

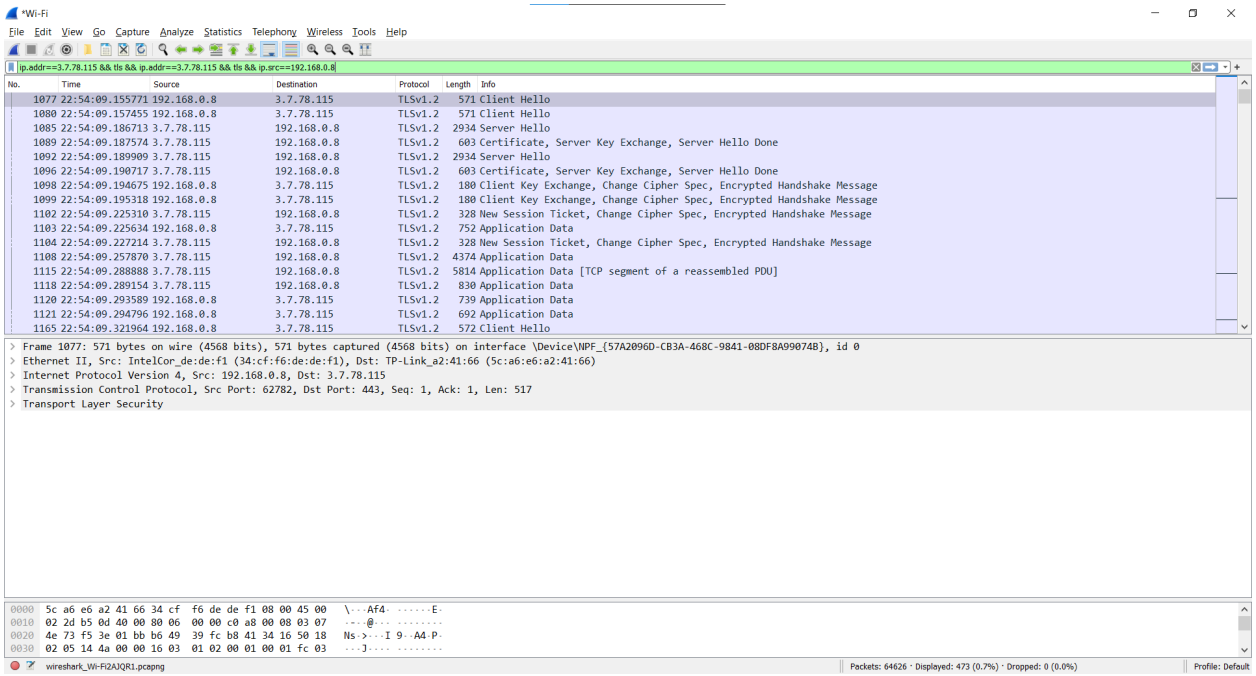
I have captured 1059 packets. No, there are packets other than TLS and I make 81 TLS requests and replies are not always OK.

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/ .



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



To find the number of TLS packets made by me.