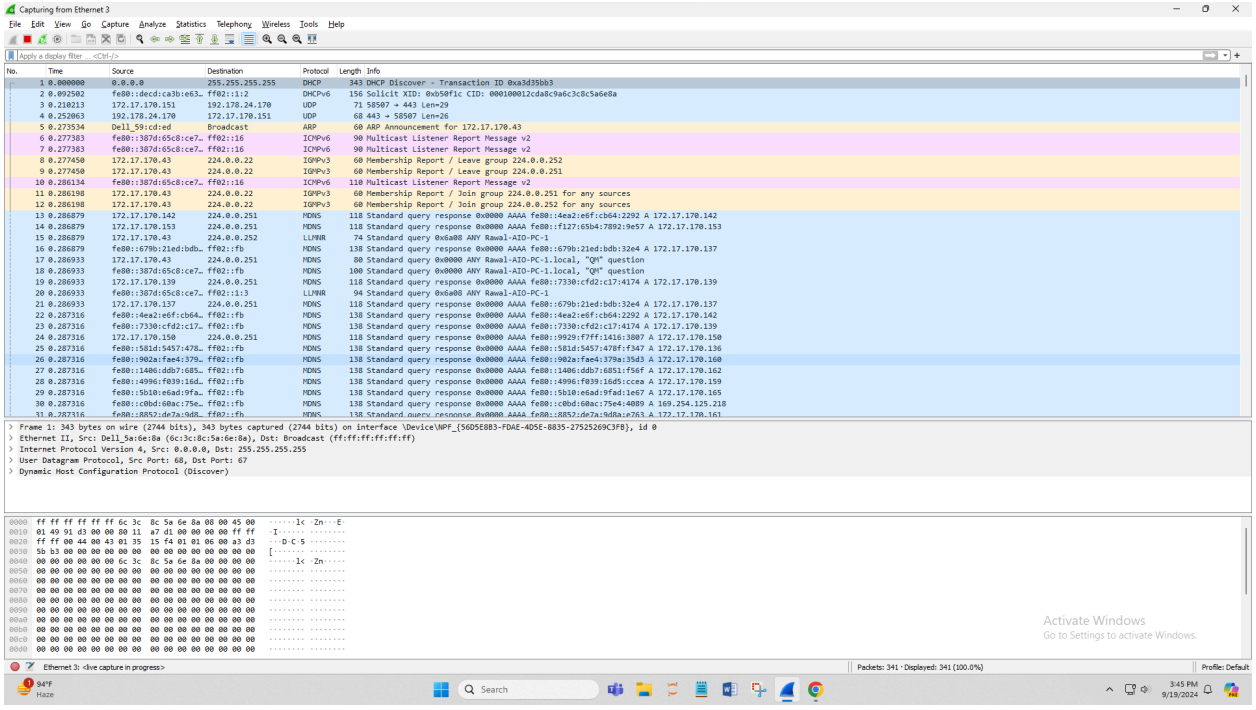
Lab #5
Computer Networks

Tasks :

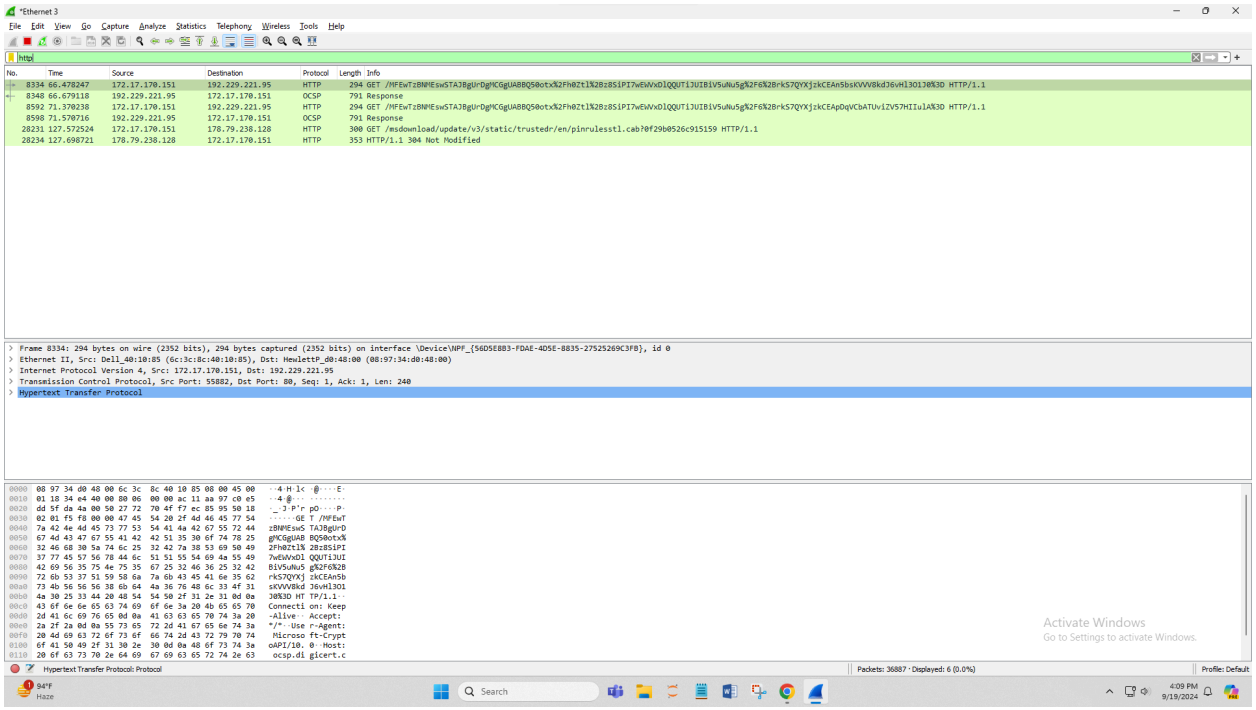
1. Open wireshark and start capturing the traffic.



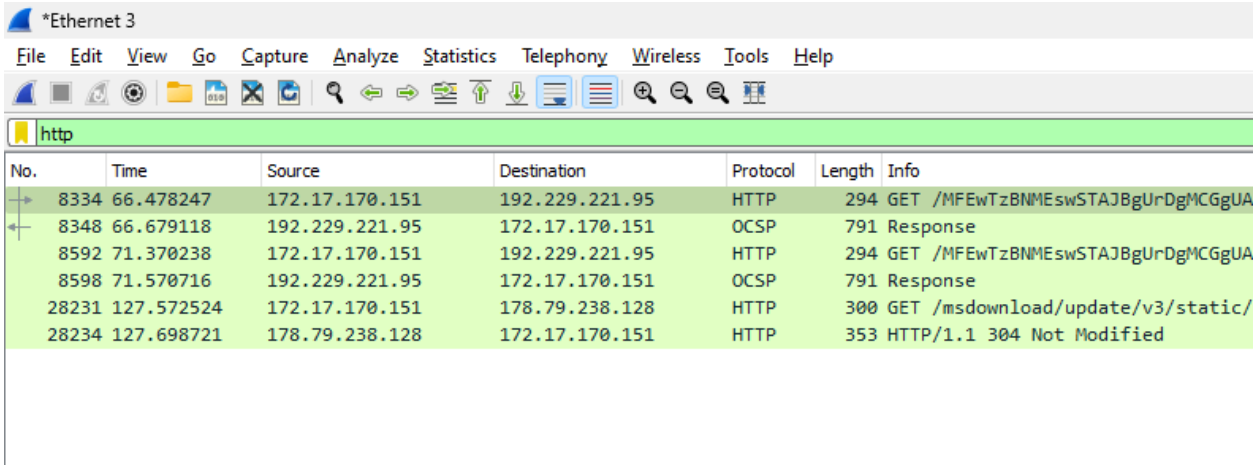
2. Search for 'gmail' on the internet and log in to your account.

Done

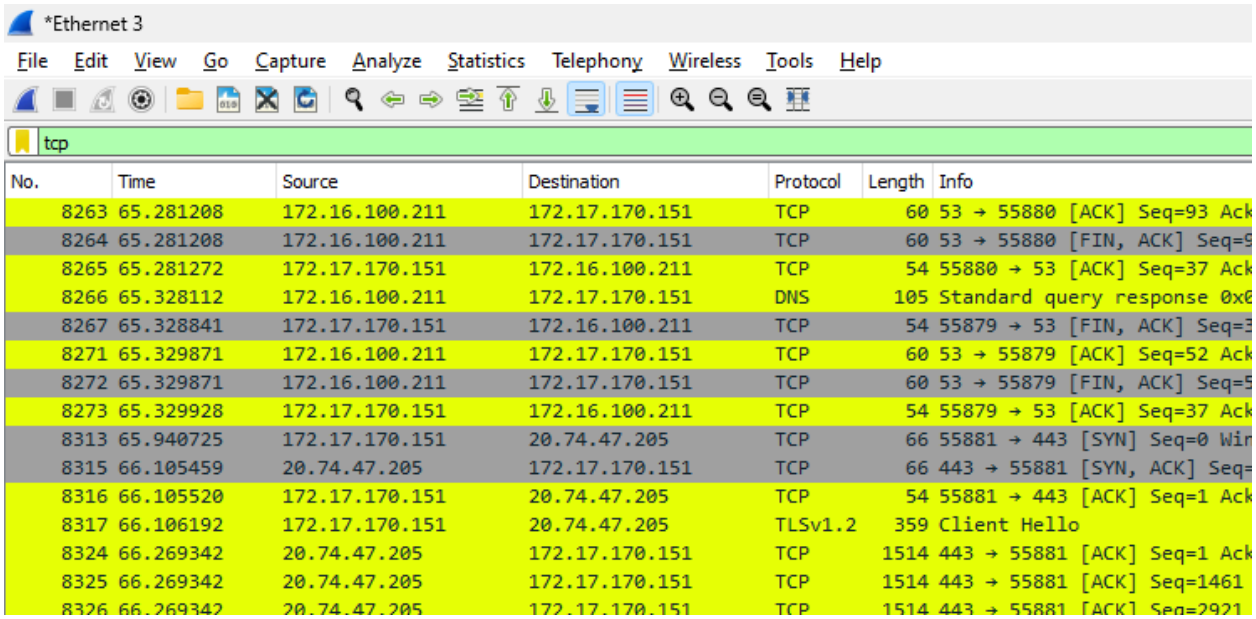
3. Stop capturing the traffic and display 'http' traffic. Then search for tcp and dns too.



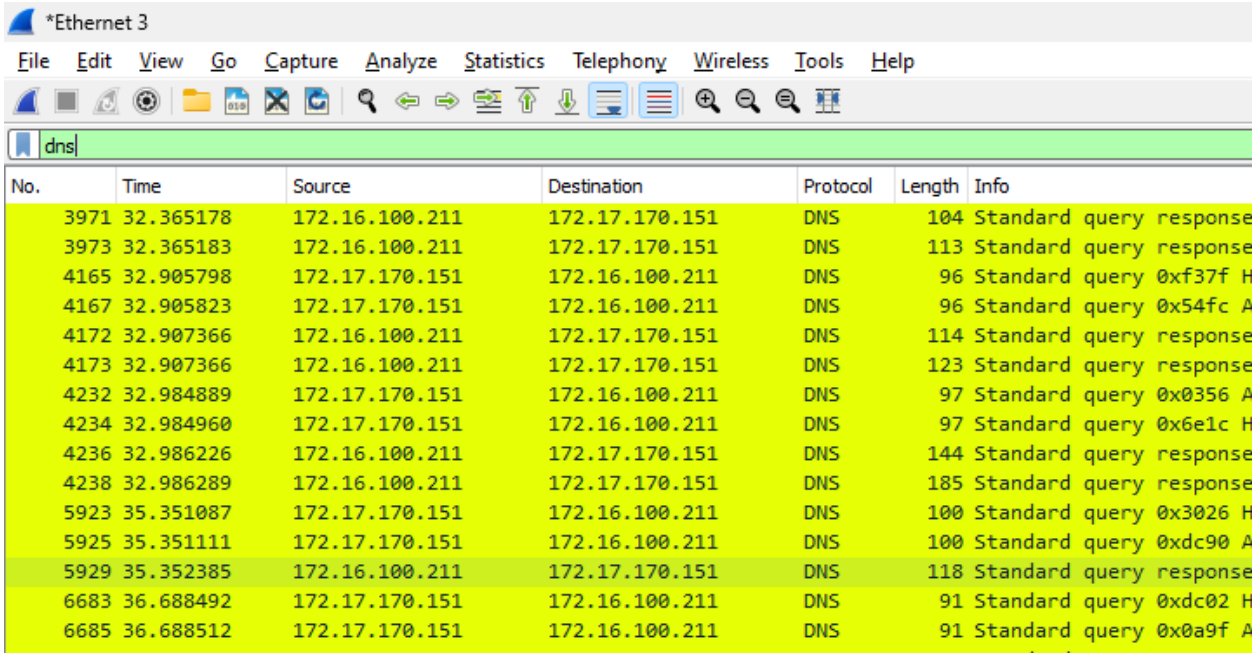
Http :


*Ethernet 3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
8334 66.478247 172.17.170.151 192.229.221.95 HTTP 294 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUA
8348 66.679118 192.229.221.95 172.17.170.151 OCSP 791 Response
8592 71.370238 172.17.170.151 192.229.221.95 HTTP 294 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUA
8598 71.570716 192.229.221.95 172.17.170.151 OCSP 791 Response
28231 127.572524 172.17.170.151 178.79.238.128 HTTP 300 GET /msdownload/update/v3/static/
28234 127.698721 178.79.238.128 172.17.170.151 HTTP 353 HTTP/1.1 304 Not Modified

TCP :

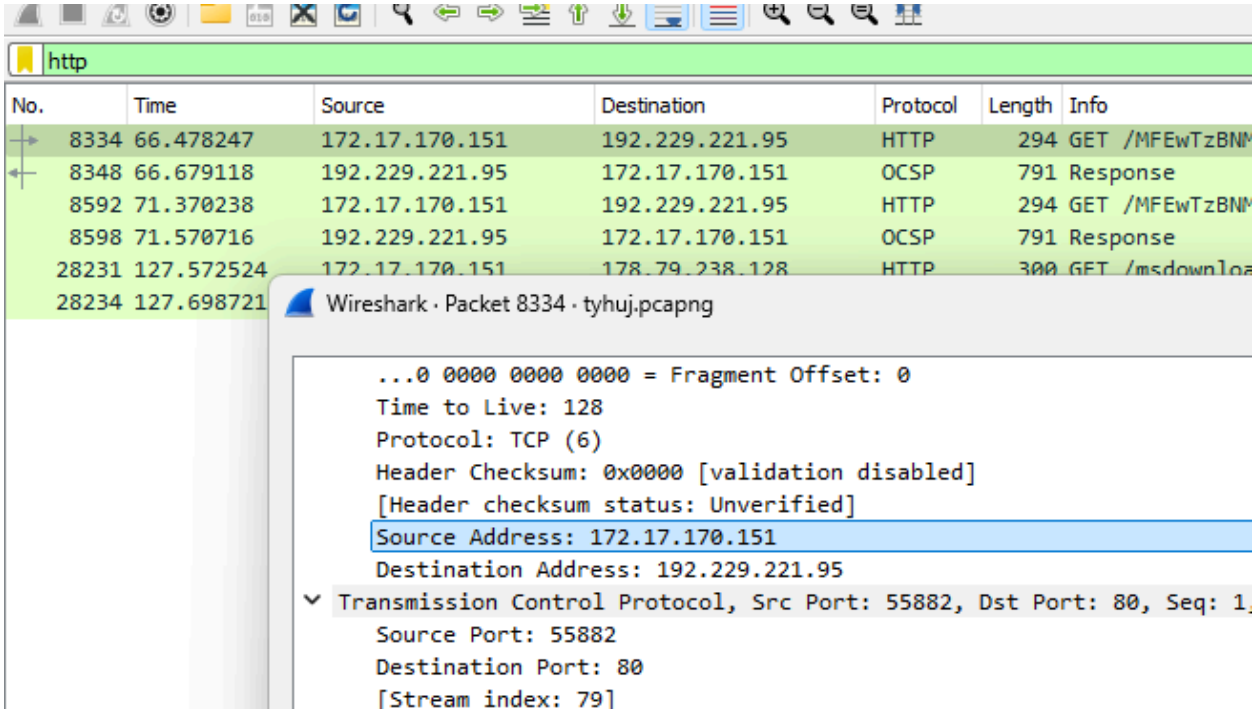

*Ethernet 3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
8263 65.281208 172.16.100.211 172.17.170.151 TCP 60 53 → 55880 [ACK] Seq=93 Ack
8264 65.281208 172.16.100.211 172.17.170.151 TCP 60 53 → 55880 [FIN, ACK] Seq=9
8265 65.281272 172.17.170.151 172.16.100.211 TCP 54 55880 → 53 [ACK] Seq=37 Ack
8266 65.328112 172.16.100.211 172.17.170.151 DNS 105 Standard query response 0x0
8267 65.328841 172.17.170.151 172.16.100.211 TCP 54 55879 → 53 [FIN, ACK] Seq=3
8271 65.329871 172.16.100.211 172.17.170.151 TCP 60 53 → 55879 [ACK] Seq=52 Ack
8272 65.329871 172.16.100.211 172.17.170.151 TCP 60 53 → 55879 [FIN, ACK] Seq=5
8273 65.329928 172.17.170.151 172.16.100.211 TCP 54 55879 → 53 [ACK] Seq=37 Ack
8313 65.940725 172.17.170.151 20.74.47.205 TCP 66 55881 → 443 [SYN] Seq=0 Win
8315 66.105459 20.74.47.205 172.17.170.151 TCP 66 443 → 55881 [SYN, ACK] Seq=
8316 66.105520 172.17.170.151 20.74.47.205 TCP 54 55881 → 443 [ACK] Seq=1 Ack
8317 66.106192 172.17.170.151 20.74.47.205 TLSv1.2 359 Client Hello
8324 66.269342 20.74.47.205 172.17.170.151 TCP 1514 443 → 55881 [ACK] Seq=1 Ack
8325 66.269342 20.74.47.205 172.17.170.151 TCP 1514 443 → 55881 [ACK] Seq=1461
8326 66.269342 20.74.47.205 172.17.170.151 TCP 1514 443 → 55881 [ACK] Seq=2921

DNS :



No.	Time	Source	Destination	Protocol	Length	Info
3971	32.365178	172.16.100.211	172.17.170.151	DNS	104	Standard query response
3973	32.365183	172.16.100.211	172.17.170.151	DNS	113	Standard query response
4165	32.905798	172.17.170.151	172.16.100.211	DNS	96	Standard query 0xf37f H
4167	32.905823	172.17.170.151	172.16.100.211	DNS	96	Standard query 0x54fc A
4172	32.907366	172.16.100.211	172.17.170.151	DNS	114	Standard query response
4173	32.907366	172.16.100.211	172.17.170.151	DNS	123	Standard query response
4232	32.984889	172.17.170.151	172.16.100.211	DNS	97	Standard query 0x0356 A
4234	32.984960	172.17.170.151	172.16.100.211	DNS	97	Standard query 0x6e1c H
4236	32.986226	172.16.100.211	172.17.170.151	DNS	144	Standard query response
4238	32.986289	172.16.100.211	172.17.170.151	DNS	185	Standard query response
5923	35.351087	172.17.170.151	172.16.100.211	DNS	100	Standard query 0x3026 H
5925	35.351111	172.17.170.151	172.16.100.211	DNS	100	Standard query 0xdc90 A
5929	35.352385	172.16.100.211	172.17.170.151	DNS	118	Standard query response
6683	36.688492	172.17.170.151	172.16.100.211	DNS	91	Standard query 0xdc02 H
6685	36.688512	172.17.170.151	172.16.100.211	DNS	91	Standard query 0x0a9f A

4. Write down the IP address of your machine and the IP address of destination server.



My machine IP :

172.17.170.151

Destination Server IP :

192.229.221.95

5. Write down source and destination port number of one http packet.

Source Port: 55882

Destination Port: 80