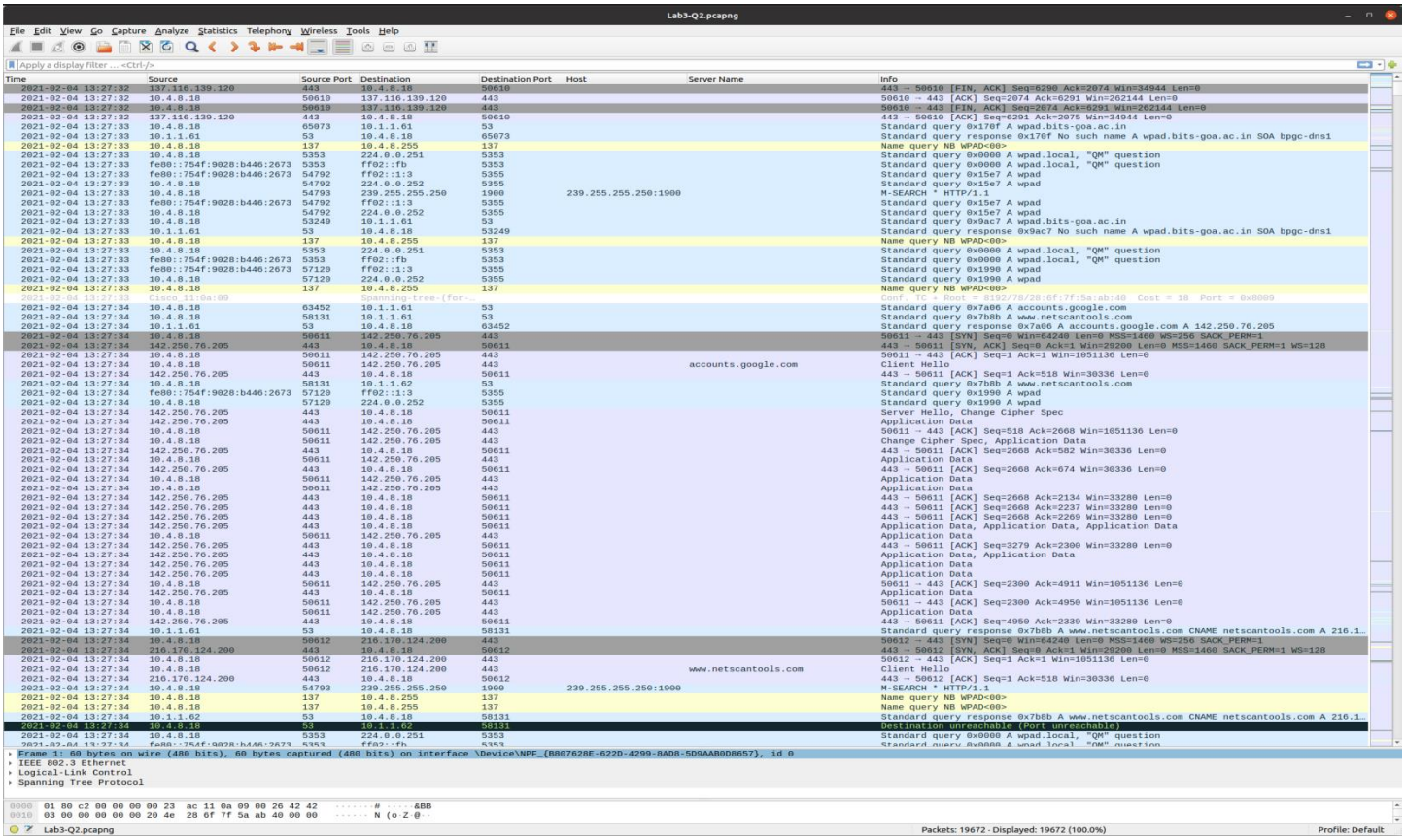
Computer Networks Lab 3

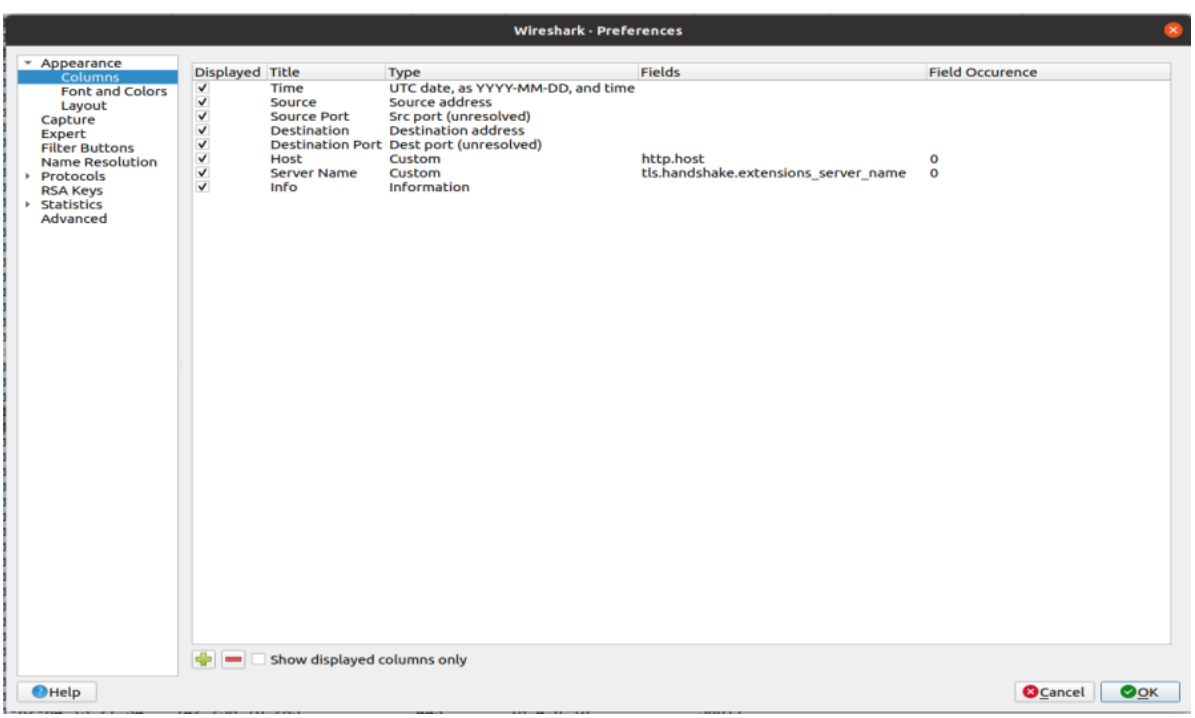
Name: Vaibhav Chaudhari

ID: 2017B5A70834G

Q1. Customize your Wireshark

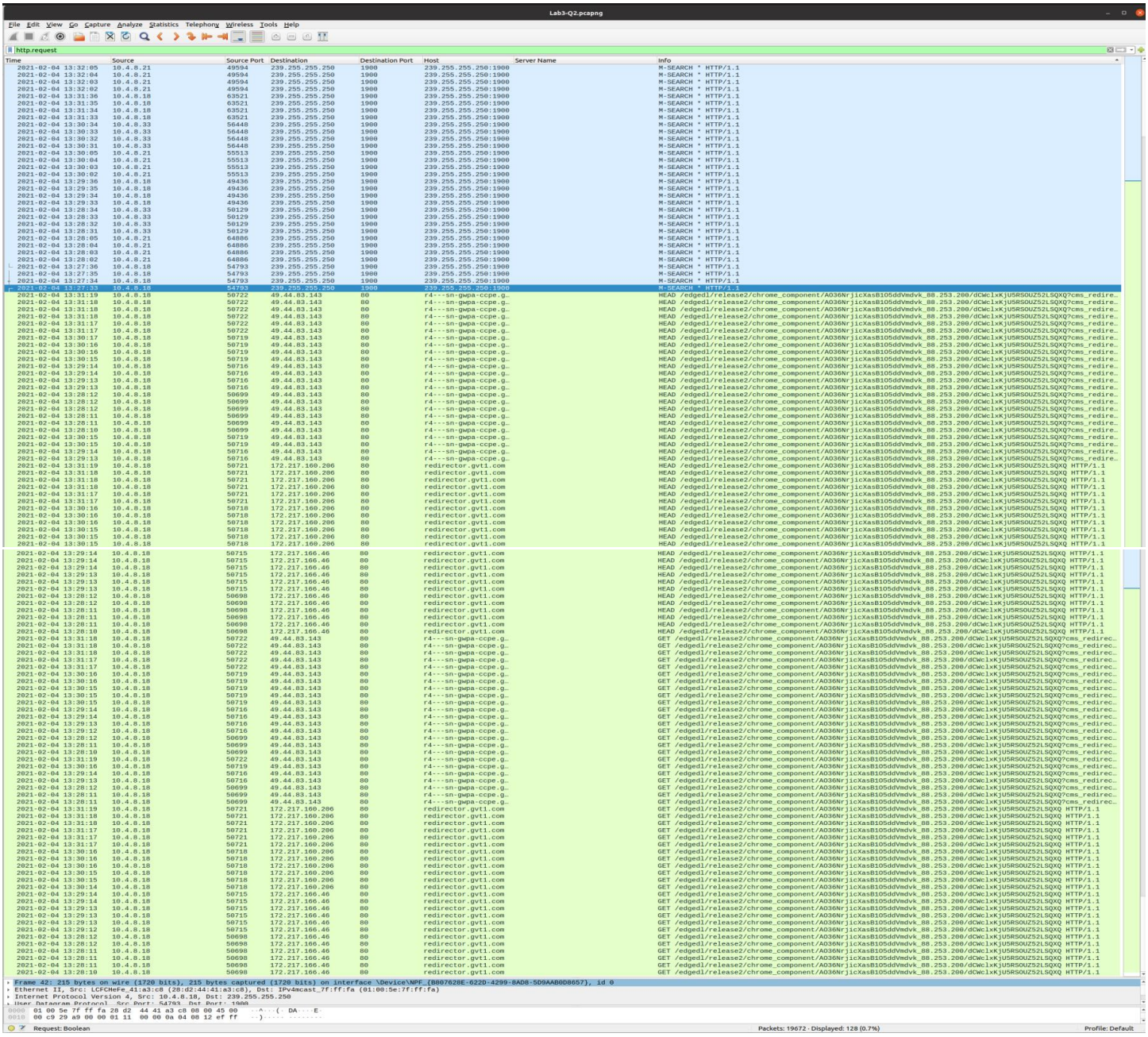


The preferences were set as follows:



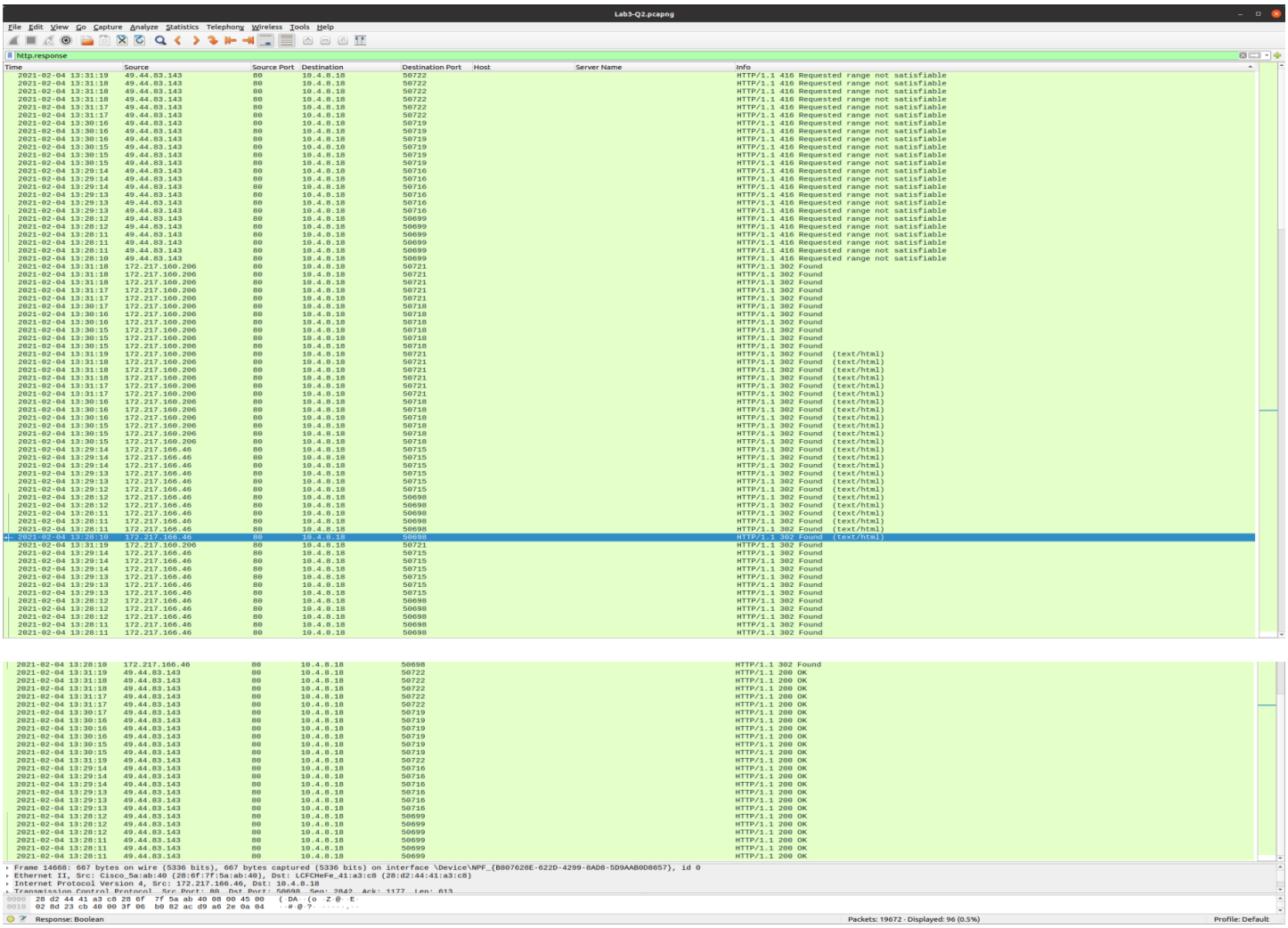
Q2. Wireshark dump analysis

a. Identify the http request packet



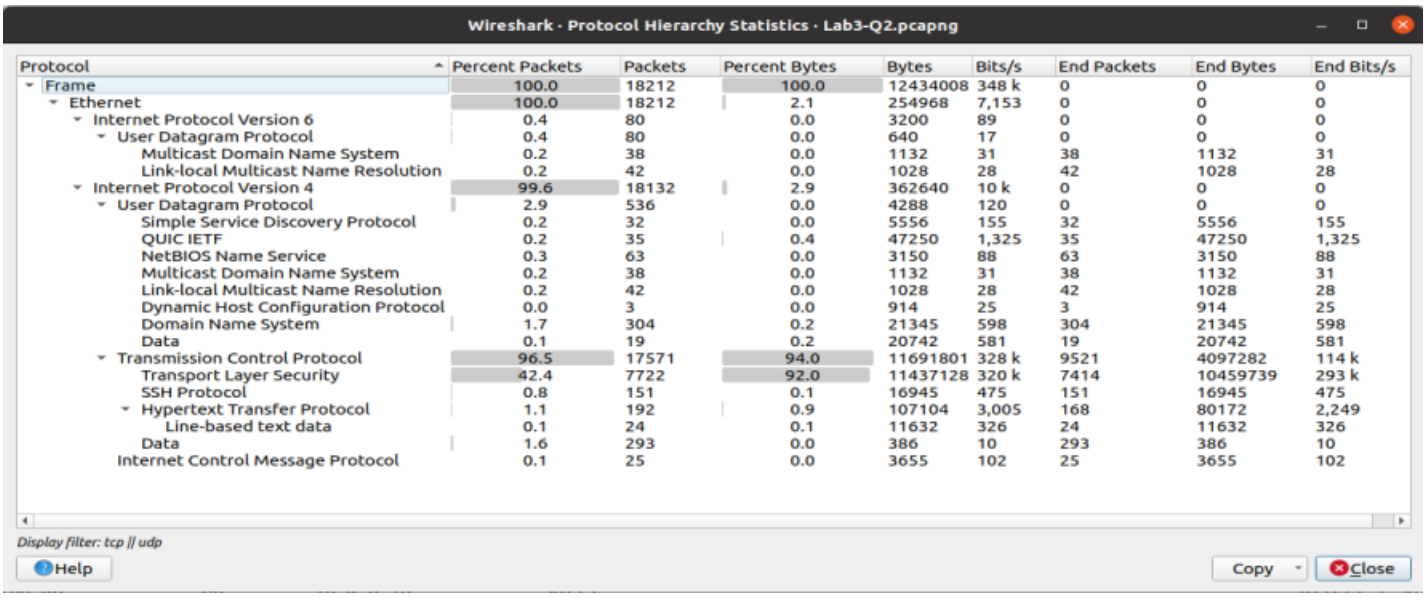
The filter used here is the **http.request.** This tells us the list of all requests that are made.

b. Identify the http response packet



The filter used here is **http.response.** This tells us the list of all the responses. We can see that the destination address for all the packets are the same.

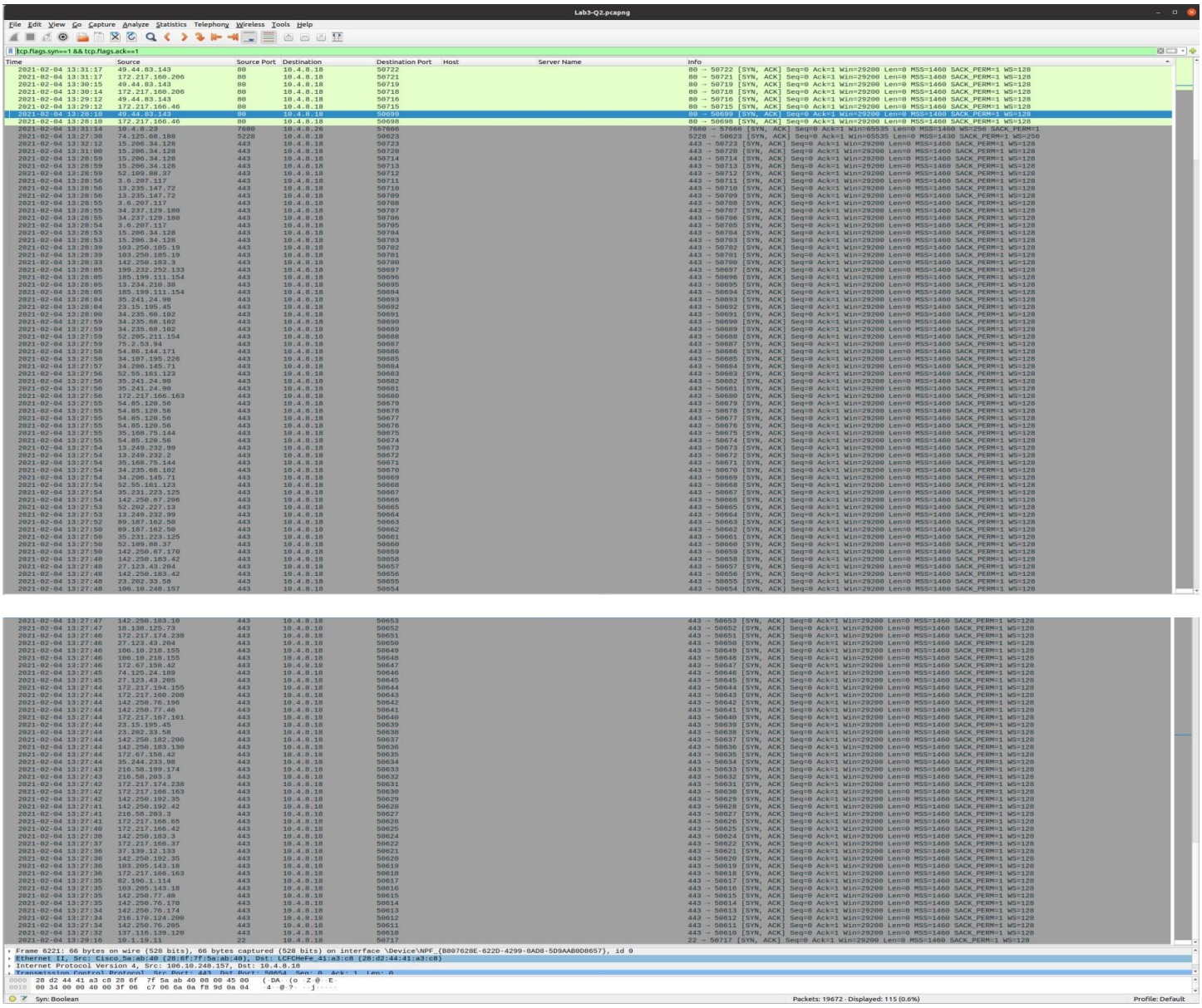
c. Display the statistics of the TCP and UDP packets



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	18212	100.0	12434008	348 k	0	0	0
Ethernet	100.0	18212	2.1	254968	7,153	0	0	0
Internet Protocol Version 6	0.4	80	0.0	3200	89	0	0	0
User Datagram Protocol	0.4	80	0.0	640	17	0	0	0
Multicast Domain Name System	0.2	38	0.0	1132	31	38	1132	31
Link-local Multicast Name Resolution	0.2	42	0.0	1028	28	42	1028	28
Internet Protocol Version 4	99.6	18132	2.9	362640	10 k	0	0	0
User Datagram Protocol	2.9	536	0.0	4288	120	0	0	0
Simple Service Discovery Protocol	0.2	32	0.0	5556	155	32	5556	155
QUIC IETF	0.2	35	0.4	47250	1,325	35	47250	1,325
NetBIOS Name Service	0.3	63	0.0	3150	88	63	3150	88
Multicast Domain Name System	0.2	38	0.0	1132	31	38	1132	31
Link-local Multicast Name Resolution	0.2	42	0.0	1028	28	42	1028	28
Dynamic Host Configuration Protocol	0.0	3	0.0	914	25	3	914	25
Domain Name System	1.7	304	0.2	21345	598	304	21345	598
Data	0.1	19	0.2	20742	581	19	20742	581
Transmission Control Protocol	96.5	17571	94.0	11691801	328 k	9521	4097282	114 k
Transport Layer Security	42.4	7722	92.0	11437128	320 k	7414	10459739	293 k
SSH Protocol	0.8	151	0.1	16945	475	151	16945	475
Hypertext Transfer Protocol	1.1	192	0.9	107104	3,005	168	80172	2,249
Line-based text data	0.1	24	0.1	11632	326	24	11632	326
Data	1.6	293	0.0	386	10	293	386	10
Internet Control Message Protocol	0.1	25	0.0	3655	102	25	3655	102

The filter used here is **udp || tcp**. We can get this by going to **Protocol Hierarchy** option in the **Statistics** Menu. This gives us a detailed report on the number of packets and their percentage.

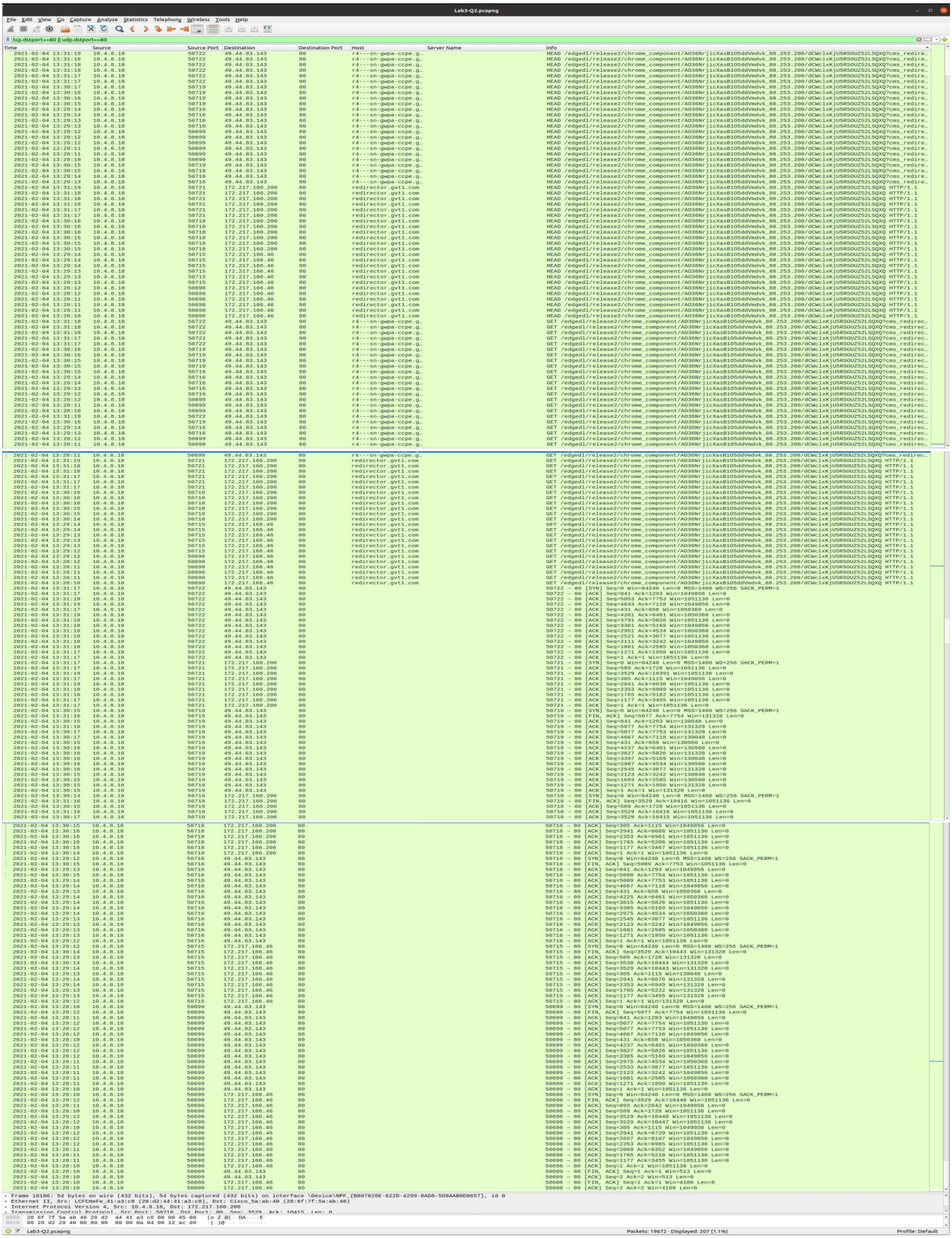
d. List out the TCP packets whose syn. and ack. Flags are on.



The filter used here is **tcp.flags.syn==1 && tcp.flags.ack==1**

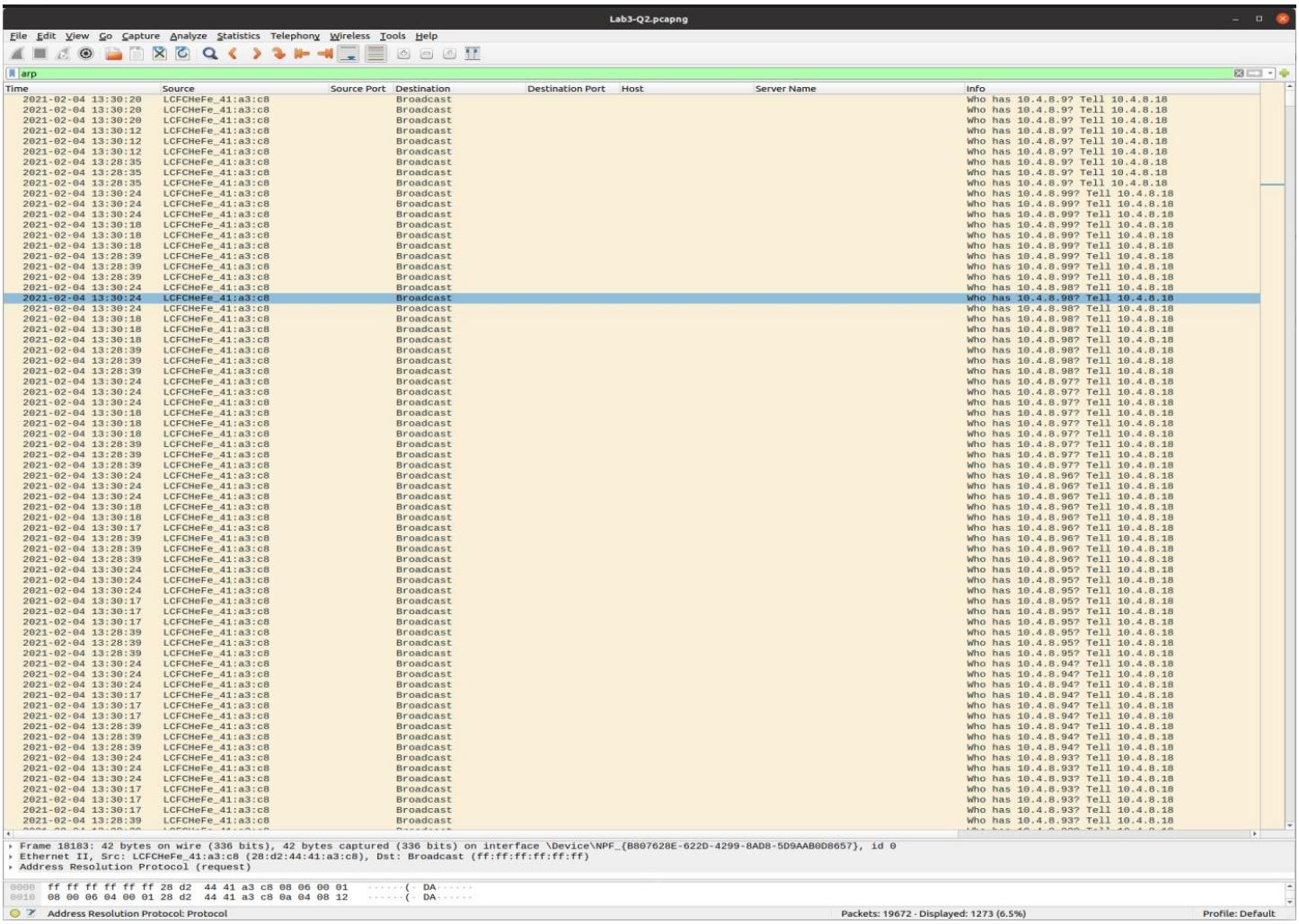
For the flags to be on, they have to be set to 1 so we check all the tcp packets whose syn. and ack. flags are set to 1.

e. List out the TCP and UDP packets where destination port=80.



The filter used here is **tcp.dstport==80 || udp.dstport==80.** We use dstport to check if the destination port is 80 for the tcp and udp connections.

f. List out the ARP packets.



The filter used here is **arp.** The ARP(Address Resolution Protocol) is used to see the mapping between a layer 3 (protocol) and a layer 2 (hardware) address.