Computer Networks Lab 3

CS F303

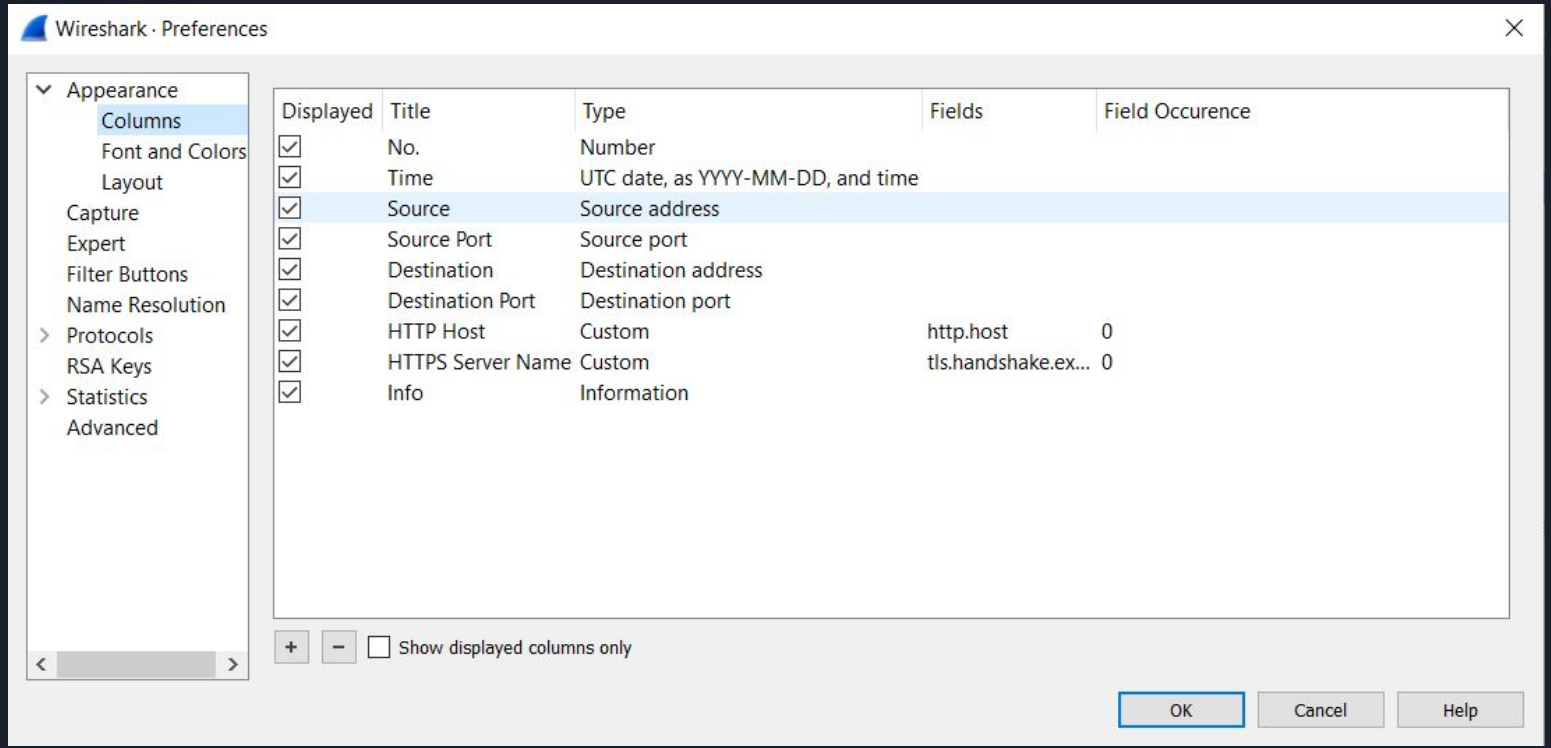
Susmit Wani 2018A7PS0116G

Question 1

Q1. Customize your Wireshark - (6 marks)
Generally, WireShark columns are arranged in the following order (which you can observe on your machine) - No. , Time, Source, Destination, Protocol, Length. etc. Being a security expert you have to arrange the WireShark display in such a way that it must have only the following items (1 mark per correct display item with the correct filter/field value and a screenshot).

a. Date & time in UTC
b. Source IP and source port
c. Destination IP and destination port
d. HTTP host
e. HTTPS server
f. Info

Names and fields of columns used to answer Q1



Question 2

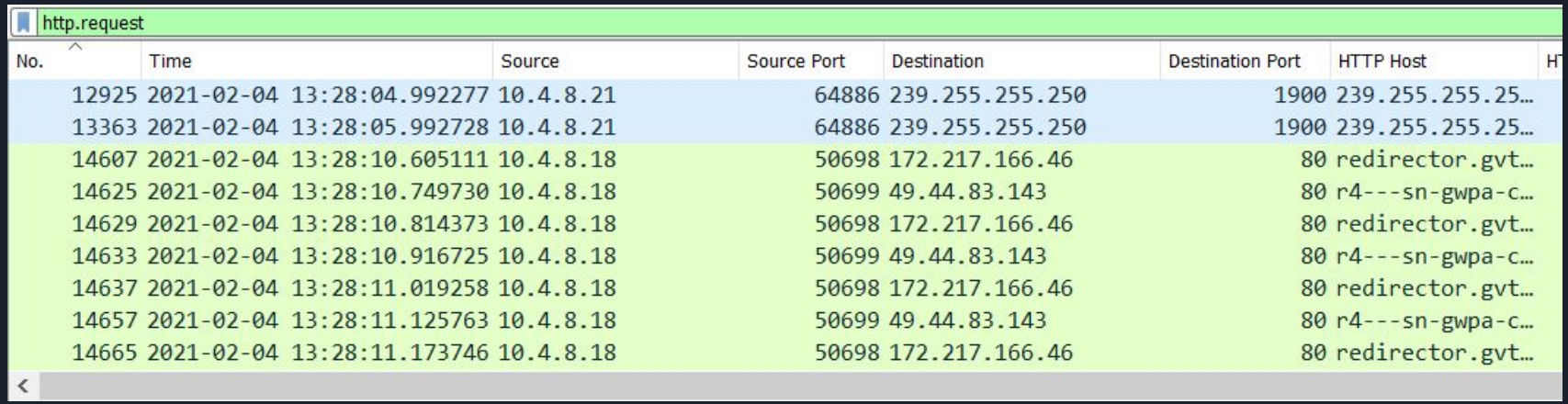
Q2. Wireshark dump analysis - (24 marks)
Using the given Lab3-Q2.pcapng, file answer the following questions. You have to write down the filter you have used (2 marks) and attach a screenshot and explain your output (2 marks).
a. Identify the http request packet
b. Identify the http response packet
c. Display the statistics of the TCP and UDP packets
d. List out the TCP packets whose syn. and ack. Flags are on.
e. List out the TCP and UDP packets where destination port=80.
f. List out the ARP packets.

a. Identify the http request packet

Use the command: http.request

Some columns are omitted from the screenshot due to clarity issues.

This command lists all the packets which were requested from the server by the client using http



http.request

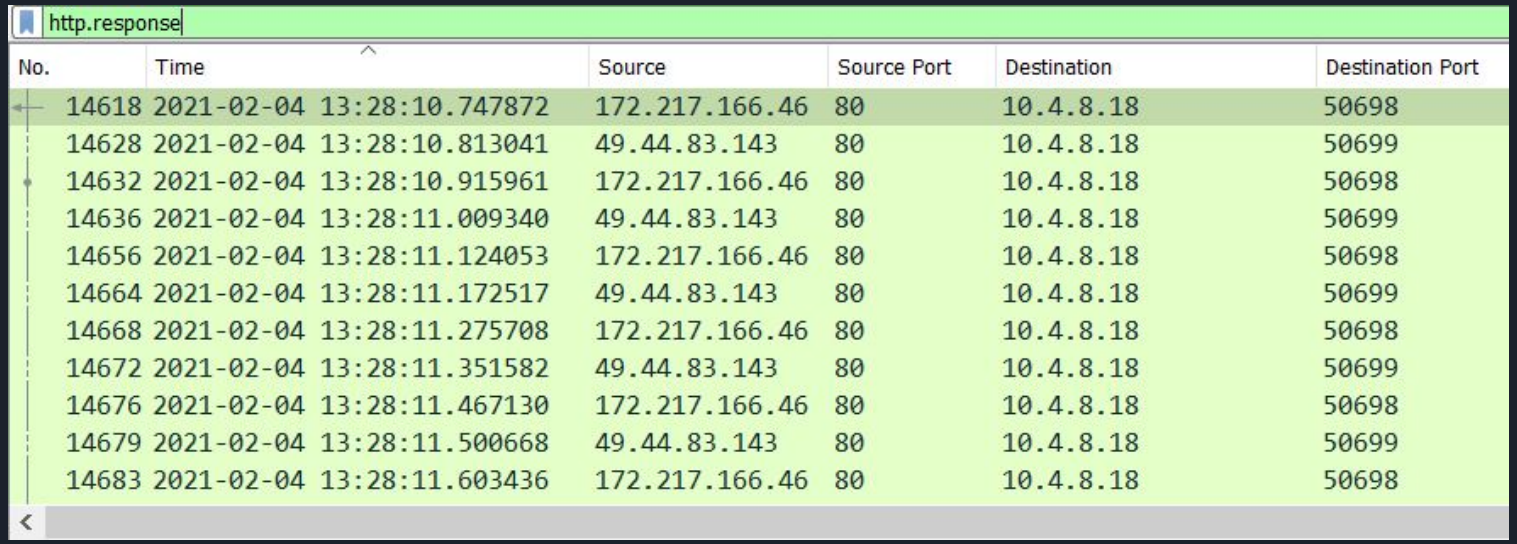
No.	Time	Source	Source Port	Destination	Destination Port	HTTP Host	HT
12925	2021-02-04 13:28:04.992277	10.4.8.21	64886	239.255.255.250	1900	239.255.255.25…	
13363	2021-02-04 13:28:05.992728	10.4.8.21	64886	239.255.255.250	1900	239.255.255.25…	
14607	2021-02-04 13:28:10.605111	10.4.8.18	50698	172.217.166.46	80	redirector.gvt…	
14625	2021-02-04 13:28:10.749730	10.4.8.18	50699	49.44.83.143	80	r4---sn-gwpa-c…	
14629	2021-02-04 13:28:10.814373	10.4.8.18	50698	172.217.166.46	80	redirector.gvt…	
14633	2021-02-04 13:28:10.916725	10.4.8.18	50699	49.44.83.143	80	r4---sn-gwpa-c…	
14637	2021-02-04 13:28:11.019258	10.4.8.18	50698	172.217.166.46	80	redirector.gvt…	
14657	2021-02-04 13:28:11.125763	10.4.8.18	50699	49.44.83.143	80	r4---sn-gwpa-c…	
14665	2021-02-04 13:28:11.173746	10.4.8.18	50698	172.217.166.46	80	redirector.gvt…	

a. Identify the http response packet

Use the command: http.response

Some columns are omitted from the screenshot due to clarity issues.

This command lists all the packets which were sent to the server by the client using http



c. Display the statistics of the TCP and UDP packets

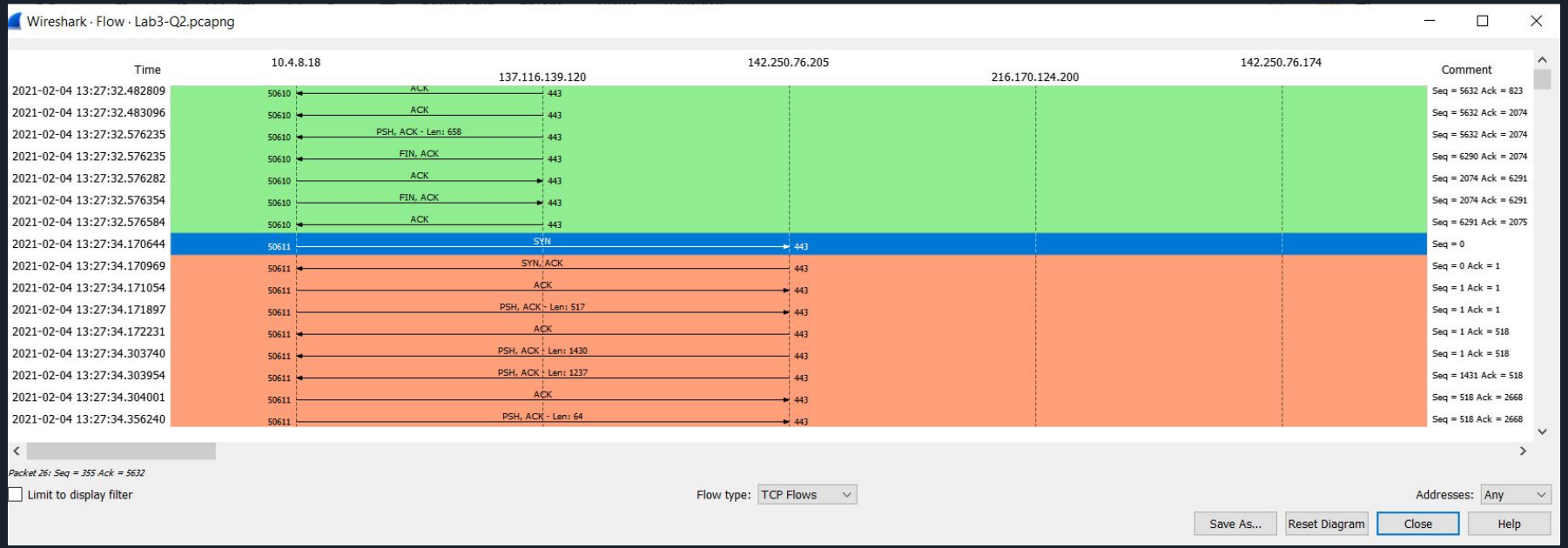
From the statistics tab, we can get the flow graph with the tcp filter which describes the tcp packets. We can also use the Protocol Hierarchy Statistics to see the statistics of tcp packets. This option too is under the statistics tab of the wireshark app.

From the statistics tab, we can also get the UDP multicast streams which shows the source and destination addresses and ports, average bandwidth, packets, packets/sec and other statistics

Images are on next two pages

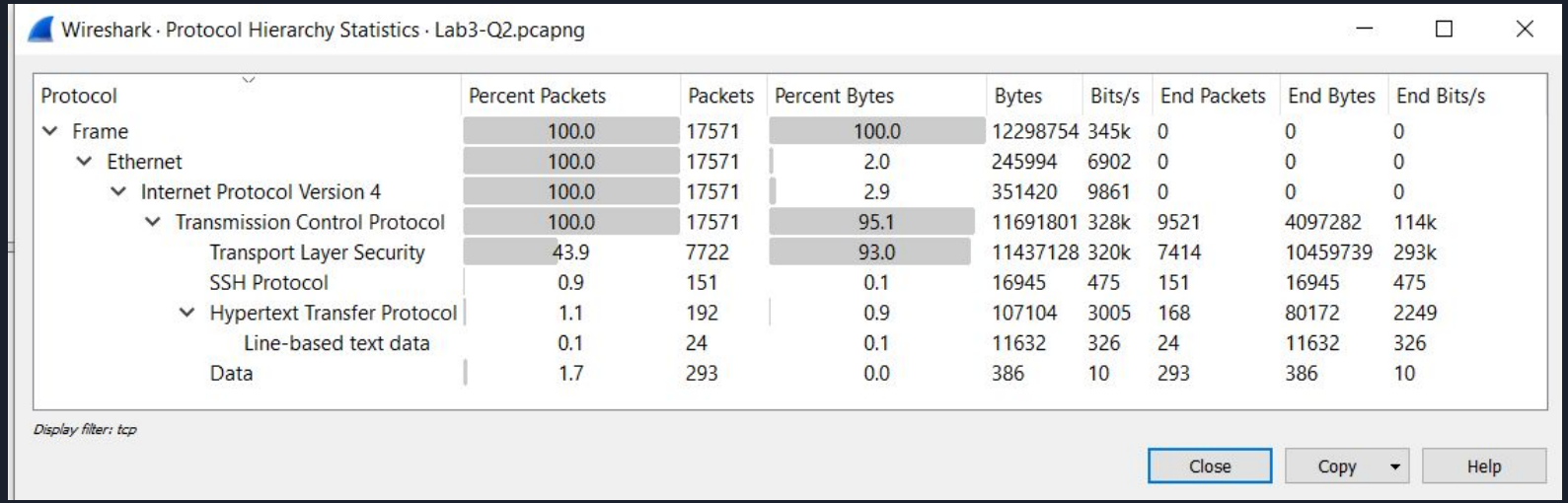
TCP statistics I:

This is the flow graph which describes all the flags as statistics in comment tab and gives source and destination addresses and port numbers.



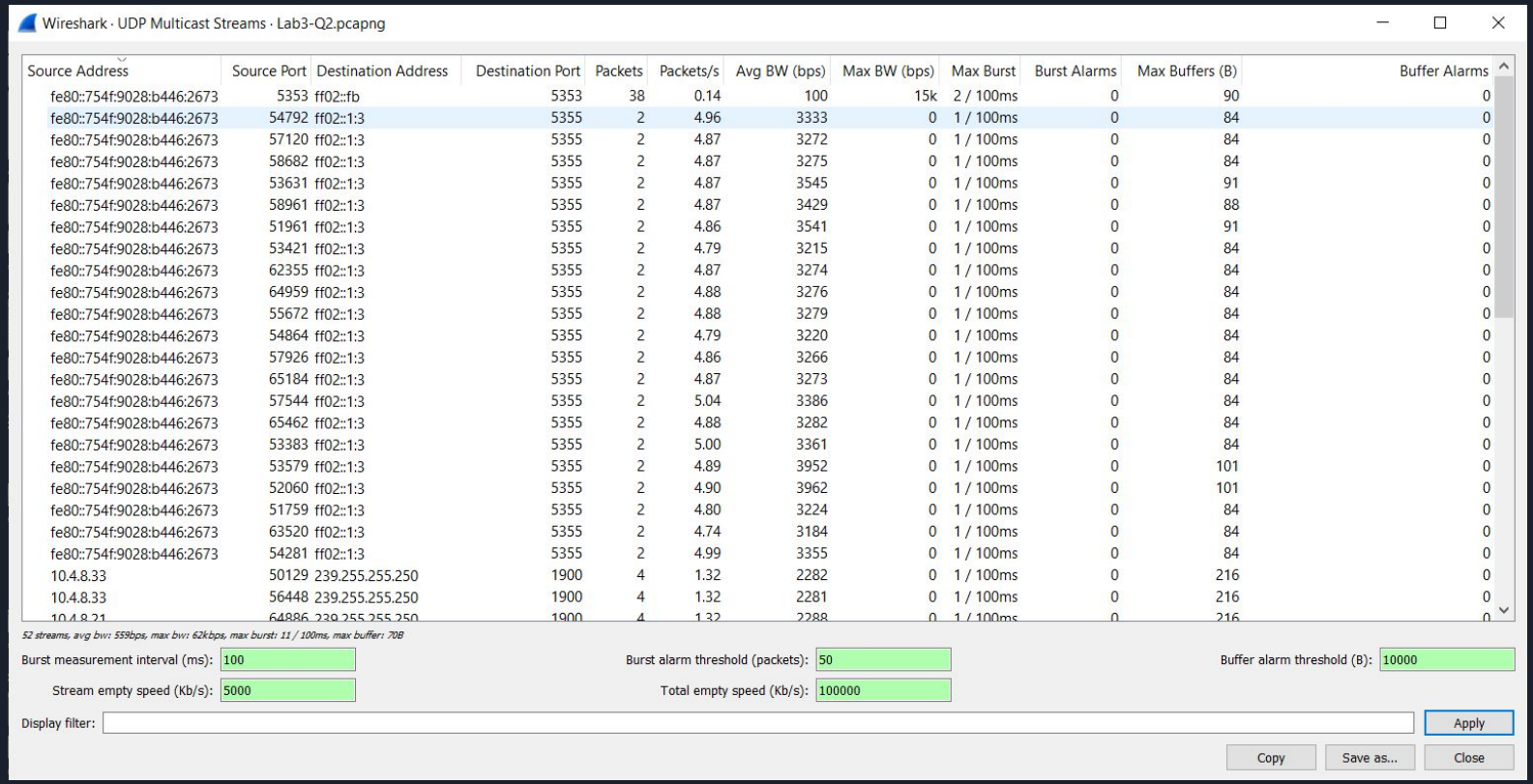
TCP Statistics II:

This is the Protocol Hierarchy Statistics with the tcp filter. It shows stats like size, speed of transfer and number of packets



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	17571	100.0	12298754	345k	0	0	0
Ethernet	100.0	17571	2.0	245994	6902	0	0	0
Internet Protocol Version 4	100.0	17571	2.9	351420	9861	0	0	0
Transmission Control Protocol	100.0	17571	95.1	11691801	328k	9521	4097282	114k
Transport Layer Security	43.9	7722	93.0	11437128	320k	7414	10459739	293k
SSH Protocol	0.9	151	0.1	16945	475	151	16945	475
Hypertext Transfer Protocol	1.1	192	0.9	107104	3005	168	80172	2249
Line-based text data	0.1	24	0.1	11632	326	24	11632	326
Data	1.7	293	0.0	386	10	293	386	10

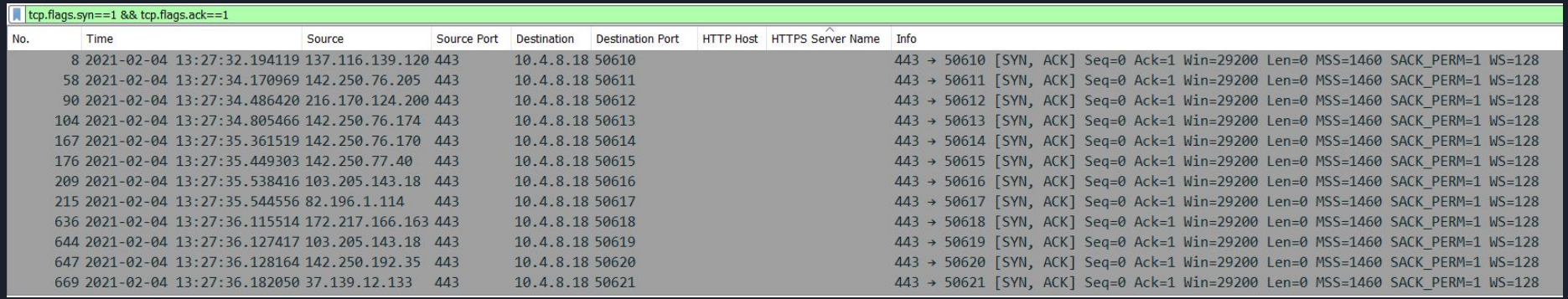
UDP statistics: UDP Multicast Streams



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

Use the command: tcp.flags.syn==1 && tcp.flags.ack==1

This command checks all the tcp packets which have ack and syn flags set to on. We use the AND operator here. SYN stands for synchronization and ack stands for acknowledgement.



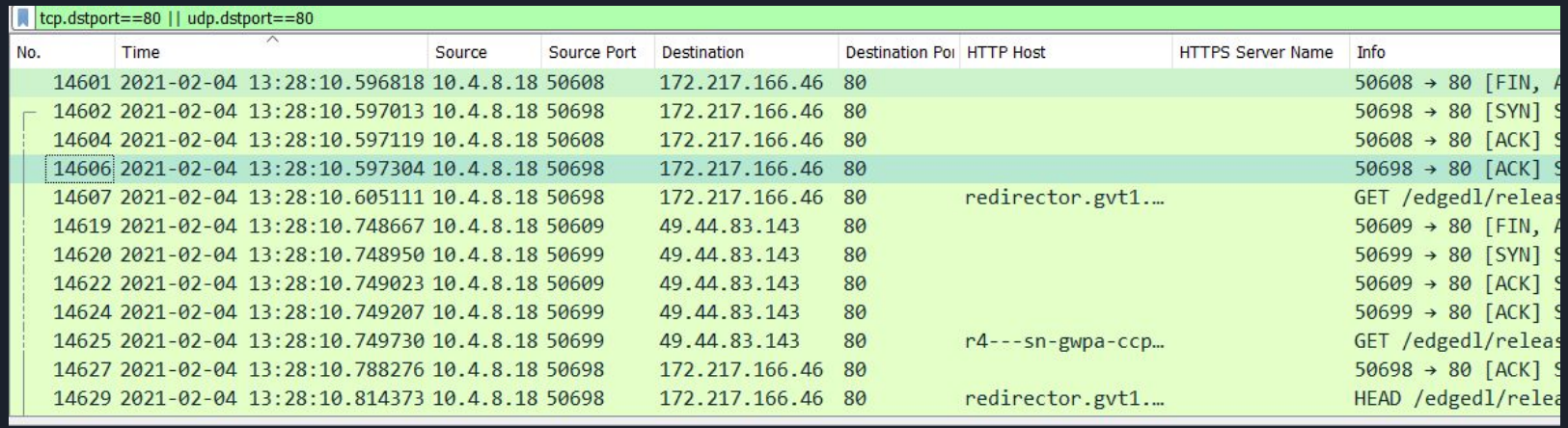
tcp.flags.syn==1 && tcp.flags.ack==1

No.	Time	Source	Source Port	Destination	Destination Port	HTTP Host	HTTPS Server Name	Info
8	2021-02-04 13:27:32.194119	137.116.139.120	443	10.4.8.18	50610			443 → 50610 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
58	2021-02-04 13:27:34.170969	142.250.76.205	443	10.4.8.18	50611			443 → 50611 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
90	2021-02-04 13:27:34.486420	216.170.124.200	443	10.4.8.18	50612			443 → 50612 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
104	2021-02-04 13:27:34.805466	142.250.76.174	443	10.4.8.18	50613			443 → 50613 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
167	2021-02-04 13:27:35.361519	142.250.76.170	443	10.4.8.18	50614			443 → 50614 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
176	2021-02-04 13:27:35.449303	142.250.77.40	443	10.4.8.18	50615			443 → 50615 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
209	2021-02-04 13:27:35.538416	103.205.143.18	443	10.4.8.18	50616			443 → 50616 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
215	2021-02-04 13:27:35.544556	82.196.1.114	443	10.4.8.18	50617			443 → 50617 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
636	2021-02-04 13:27:36.115514	172.217.166.163	443	10.4.8.18	50618			443 → 50618 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
644	2021-02-04 13:27:36.127417	103.205.143.18	443	10.4.8.18	50619			443 → 50619 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
647	2021-02-04 13:27:36.128164	142.250.192.35	443	10.4.8.18	50620			443 → 50620 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
669	2021-02-04 13:27:36.182050	37.139.12.133	443	10.4.8.18	50621			443 → 50621 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128

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

Use the command: tcp.dstport==80 || udp.dstport==80

This command lists all TCP and UDP packets with destination port number 80. We use the OR operator here


tcp.dstport==80 || udp.dstport==80

No.	Time	Source	Source Port	Destination	Destination Por	HTTP Host	HTTPS Server Name	Info
14601	2021-02-04 13:28:10.596818	10.4.8.18	50608	172.217.166.46	80			50608 → 80 [FIN, A
14602	2021-02-04 13:28:10.597013	10.4.8.18	50698	172.217.166.46	80			50698 → 80 [SYN] S
14604	2021-02-04 13:28:10.597119	10.4.8.18	50608	172.217.166.46	80			50608 → 80 [ACK] S
14606	2021-02-04 13:28:10.597304	10.4.8.18	50698	172.217.166.46	80			50698 → 80 [ACK] S
14607	2021-02-04 13:28:10.605111	10.4.8.18	50698	172.217.166.46	80	redirector.gvt1.…		GET /edgedl/releas
14619	2021-02-04 13:28:10.748667	10.4.8.18	50609	49.44.83.143	80			50609 → 80 [FIN, A
14620	2021-02-04 13:28:10.748950	10.4.8.18	50699	49.44.83.143	80			50699 → 80 [SYN] S
14622	2021-02-04 13:28:10.749023	10.4.8.18	50609	49.44.83.143	80			50609 → 80 [ACK] S
14624	2021-02-04 13:28:10.749207	10.4.8.18	50699	49.44.83.143	80			50699 → 80 [ACK] S
14625	2021-02-04 13:28:10.749730	10.4.8.18	50699	49.44.83.143	80	r4---sn-gwpa-ccp…		GET /edgedl/releas
14627	2021-02-04 13:28:10.788276	10.4.8.18	50698	172.217.166.46	80			50698 → 80 [ACK] S
14629	2021-02-04 13:28:10.814373	10.4.8.18	50698	172.217.166.46	80	redirector.gvt1.…		HEAD /edgedl/relea

f. List out the ARP packets.

Use the command: arp

This command is used to find the MAC address associated with an IPv4 address