Lab 3

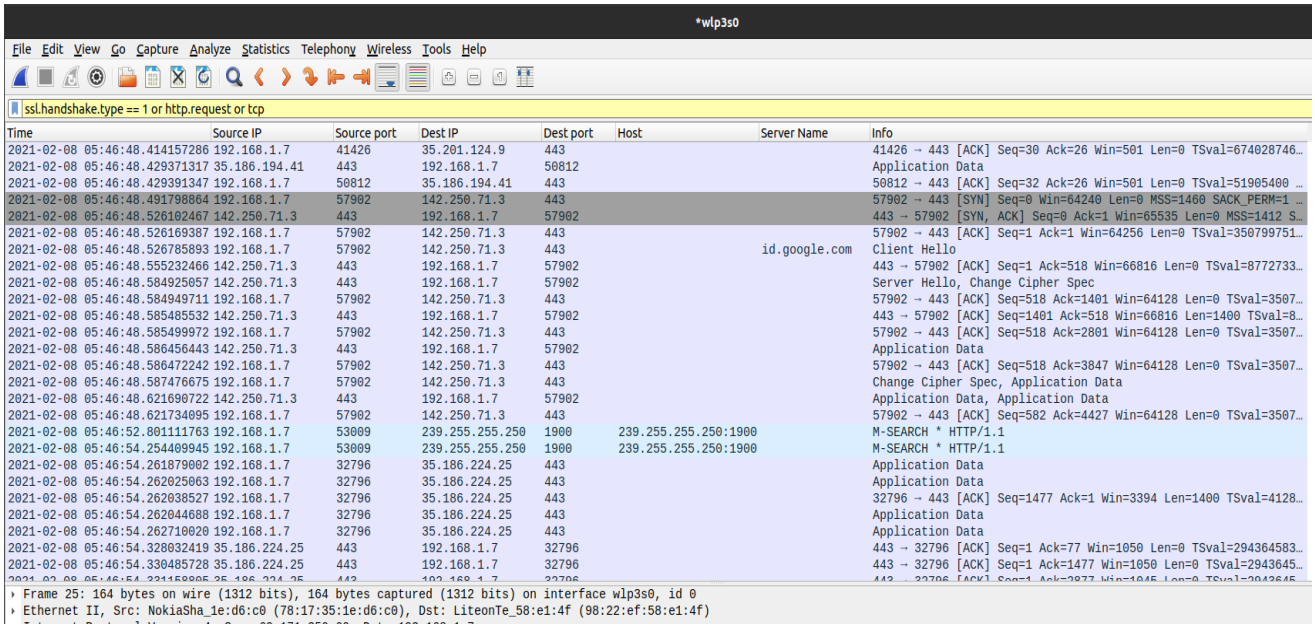
Parmesh Mathur **2018A7PS0133G**

1. Customizing Wireshark

Wireshark can be customized to suit our own needs. General customization in Wireshark includes adding, removing, hiding or editing details of columns in the viewing space.

Here, the No., Protocol and Length columns have been hidden. We have added columns for the Source and Destination ports, and those for HTTP hosts and HTTPS server names of packets (entries for which are empty in most cases as not all packets have HTTP either attribute).

The Time column has been changed to show in UTC.



Time	Source IP	Source port	Dest IP	Dest port	Host	Server Name	Info
2021-02-08 05:46:48.414157286	192.168.1.7	41426	35.201.124.9	443			41426 → 443 [ACK] Seq=30 Ack=26 Win=501 Len=0 TSval=674028746…
2021-02-08 05:46:48.429371317	35.186.194.41	443	192.168.1.7	50812			Application Data
2021-02-08 05:46:48.429391347	192.168.1.7	50812	35.186.194.41	443			50812 → 443 [ACK] Seq=32 Ack=26 Win=501 Len=0 TSval=51905400 …
2021-02-08 05:46:48.491798864	192.168.1.7	57902	142.250.71.3	443			57902 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 …
2021-02-08 05:46:48.526102467	142.250.71.3	443	192.168.1.7	57902			443 → 57902 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 S…
2021-02-08 05:46:48.526169387	192.168.1.7	57902	142.250.71.3	443			57902 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=350799751…
2021-02-08 05:46:48.526785893	192.168.1.7	57902	142.250.71.3	443		id.google.com	Client Hello
2021-02-08 05:46:48.555232466	142.250.71.3	443	192.168.1.7	57902			443 → 57902 [ACK] Seq=1 Ack=518 Win=66816 Len=0 TSval=8772733…
2021-02-08 05:46:48.584925057	142.250.71.3	443	192.168.1.7	57902			Server Hello, Change Cipher Spec
2021-02-08 05:46:48.584949711	192.168.1.7	57902	142.250.71.3	443			57902 → 443 [ACK] Seq=518 Ack=1401 Win=64128 Len=0 TSval=3507…
2021-02-08 05:46:48.585485532	142.250.71.3	443	192.168.1.7	57902			443 → 57902 [ACK] Seq=1401 Ack=518 Win=66816 Len=1400 TSval=8…
2021-02-08 05:46:48.585499972	192.168.1.7	57902	142.250.71.3	443			57902 → 443 [ACK] Seq=518 Ack=2801 Win=64128 Len=0 TSval=3507…
2021-02-08 05:46:48.586456443	142.250.71.3	443	192.168.1.7	57902			Application Data
2021-02-08 05:46:48.586472242	192.168.1.7	57902	142.250.71.3	443			57902 → 443 [ACK] Seq=518 Ack=3847 Win=64128 Len=0 TSval=3507…
2021-02-08 05:46:48.587476675	192.168.1.7	57902	142.250.71.3	443			Change Cipher Spec, Application Data
2021-02-08 05:46:48.621690722	142.250.71.3	443	192.168.1.7	57902			Application Data, Application Data
2021-02-08 05:46:48.621734095	192.168.1.7	57902	142.250.71.3	443			57902 → 443 [ACK] Seq=582 Ack=4427 Win=64128 Len=0 TSval=3507…
2021-02-08 05:46:52.801111763	192.168.1.7	53009	239.255.255.250	1900	239.255.255.250:1900		M-SEARCH * HTTP/1.1
2021-02-08 05:46:54.254409945	192.168.1.7	53009	239.255.255.250	1900	239.255.255.250:1900		M-SEARCH * HTTP/1.1
2021-02-08 05:46:54.261879002	192.168.1.7	32796	35.186.224.25	443			Application Data
2021-02-08 05:46:54.262025063	192.168.1.7	32796	35.186.224.25	443			Application Data
2021-02-08 05:46:54.262038527	192.168.1.7	32796	35.186.224.25	443			32796 → 443 [ACK] Seq=1477 Ack=1 Win=3394 Len=1400 TSval=4128…
2021-02-08 05:46:54.262044688	192.168.1.7	32796	35.186.224.25	443			Application Data
2021-02-08 05:46:54.262710020	192.168.1.7	32796	35.186.224.25	443			Application Data
2021-02-08 05:46:54.328032419	35.186.224.25	443	192.168.1.7	32796			443 → 32796 [ACK] Seq=1 Ack=77 Win=1050 Len=0 TSval=294364583…
2021-02-08 05:46:54.330485728	35.186.224.25	443	192.168.1.7	32796			443 → 32796 [ACK] Seq=1 Ack=1477 Win=1050 Len=0 TSval=2943645…

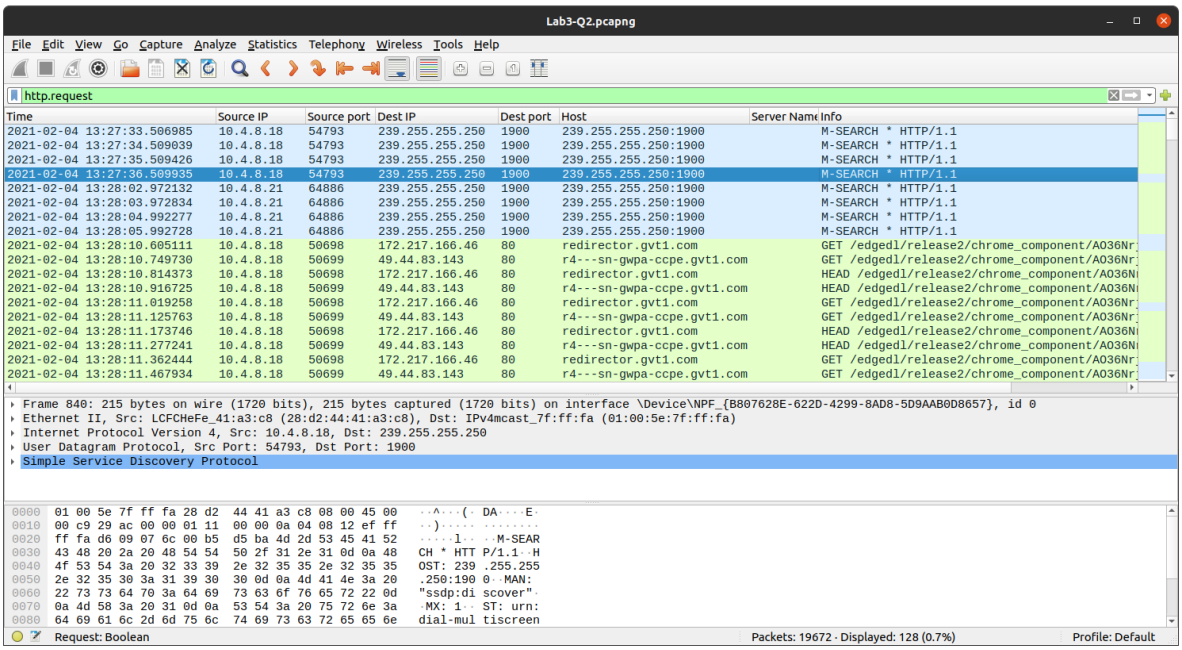
Note: A filter has been used here to shorten the output list. This was done to show frames with hosts and server names in one window of output of the application itself.

2. Wireshark dump analysis

a. Identify the HTTP request packets.

The `http.request` filter is used to list out HTTP request packets.

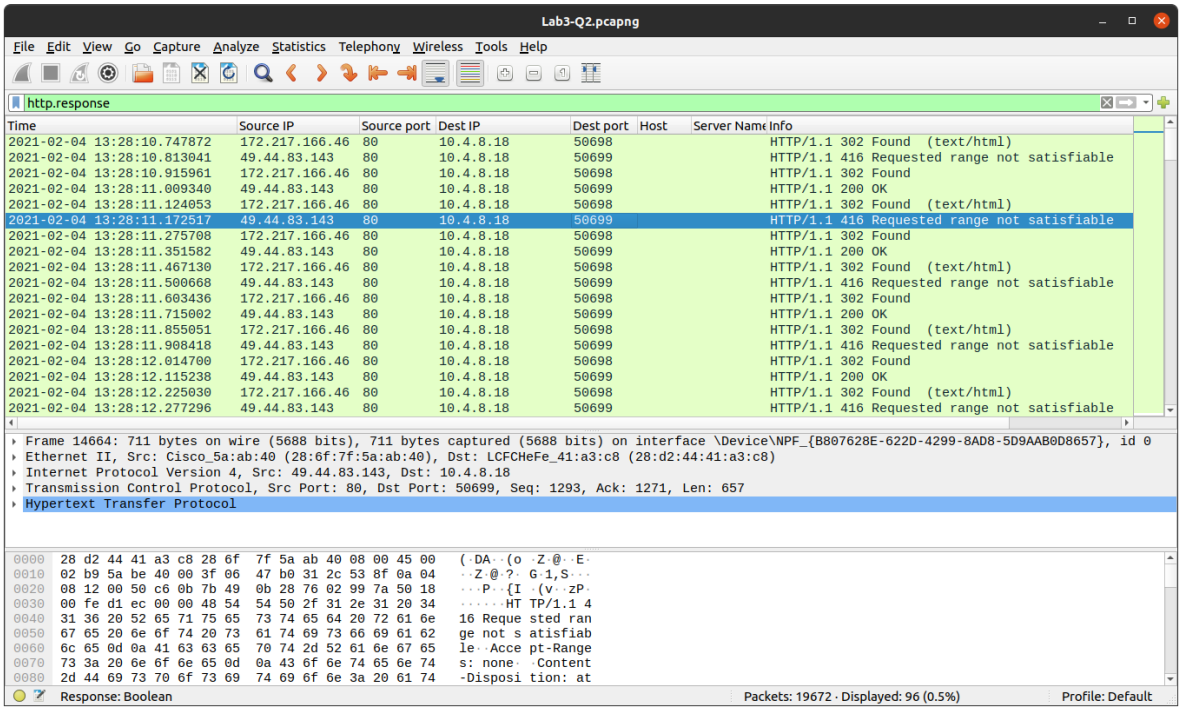
As shown in the information column, HTTP requests entail actions like GET (among others like PUT, WRITE). It is also noticeable that the Source IP for these requests do not vary a lot as these packets originate in the system itself.



b. Identify the HTTP response packets.

The `http.response` filter is used to identify HTTP response packets.

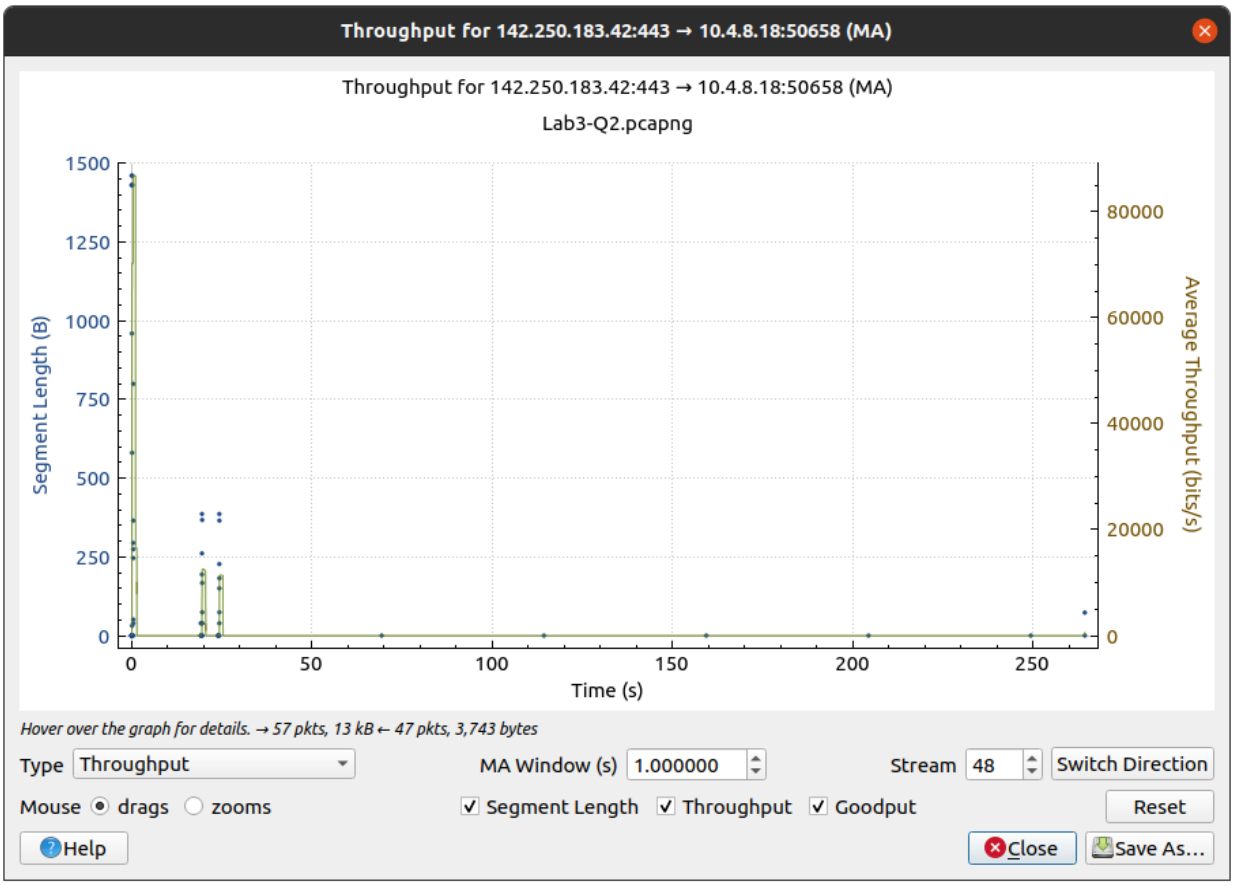
As is visible, a majority of these responses are in the form of acknowledgement messages (e.g. OK, Found), while some might be of the form of denial/rejection of requests. As shown, the Destination IP of these packets are the same, indicating they are addressed to a particular address (the particular system, in this case).



c. Display the statistics of the TCP and UDP packets

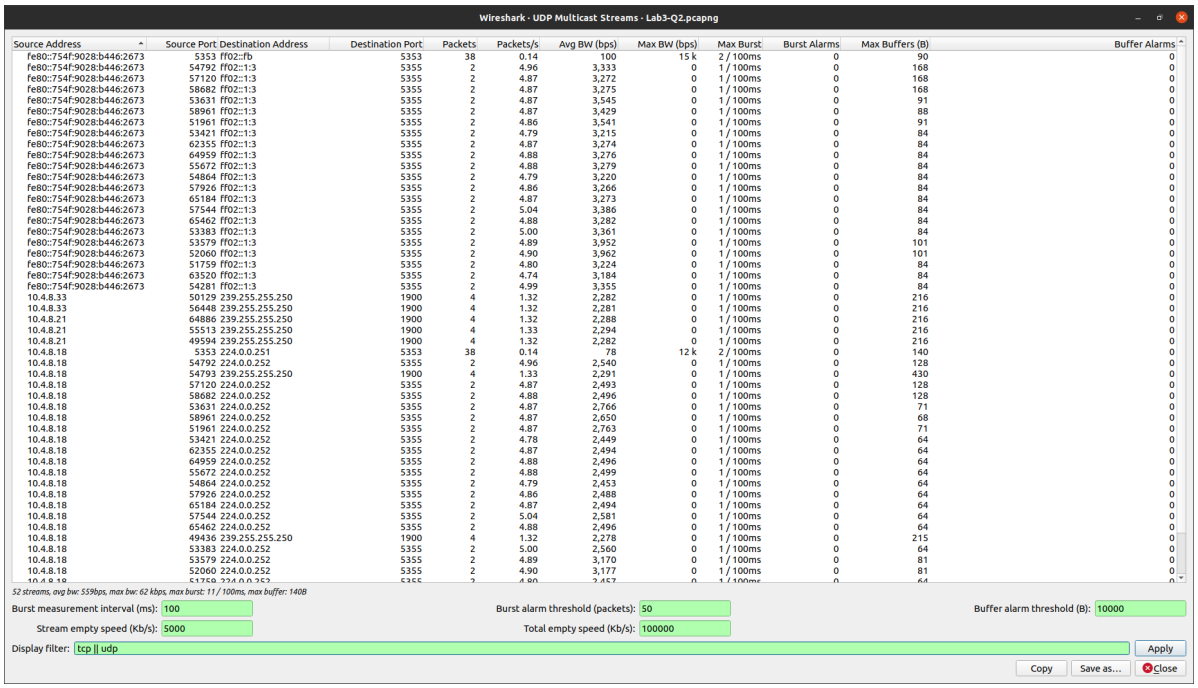
The filter used is `tcp || udp`, which is a logical or of the `tcp` and the `udp` filters.

To collect the staistics for these packets, we use the Statistics menu in Wireshark. From here some statistics to display are Throughput (from TCP Stream Graphs) and UDP Multicast Stream.



The Throughput Graph available in the TCP Stream Graphs option

P.T.O.



Wireshark · UDP Multicast Streams · Lab3-Q2.pcapng

Source Address	Source Port	Destination Address	Destination Port	Packets	Packets/s	Avg BW (bps)	Max BW (bps)	Max Burst	Burst Alarms	Max Buffers (B)	Buffer Alarms
fe80::754f:9028:b446:2673	5353	ff02::fb	5353	38	0.14	100	15 k	2 / 100ms	0	90	0
fe80::754f:9028:b446:2673	54792	ff02::1:3	5355	2	4.96	3,333	0	1 / 100ms	0	168	0
fe80::754f:9028:b446:2673	57120	ff02::1:3	5355	2	4.87	3,272	0	1 / 100ms	0	168	0
fe80::754f:9028:b446:2673	58682	ff02::1:3	5355	2	4.87	3,275	0	1 / 100ms	0	168	0
fe80::754f:9028:b446:2673	53631	ff02::1:3	5355	2	4.87	3,545	0	1 / 100ms	0	91	0
fe80::754f:9028:b446:2673	58961	ff02::1:3	5355	2	4.87	3,429	0	1 / 100ms	0	88	0
fe80::754f:9028:b446:2673	51961	ff02::1:3	5355	2	4.86	3,541	0	1 / 100ms	0	91	0
fe80::754f:9028:b446:2673	53421	ff02::1:3	5355	2	4.79	3,215	0	1 / 100ms	0	84	0
fe80::754f:9028:b446:2673	62355	ff02::1:3	5355	2	4.87	3,274	0	1 / 100ms	0	84	0
fe80::754f:9028:b446:2673	64959	ff02::1:3	5355	2	4.88	3,276	0	1 / 100ms	0	84	0
fe80::754f:9028:b446:2673	55672	ff02::1:3	5355	2	4.88	3,279	0	1 / 100ms	0	84	0
fe80::754f:9028:b446:2673	54864	ff02::1:3	5355	2	4.79	3,220	0	1 / 100ms	0	84	0
fe80::754f:9028:b446:2673	57926	ff02::1:3	5355	2	4.86	3,266	0	1 / 100ms	0	84	0
fe80::754f:9028:b446:2673	65184	ff02::1:3	5355	2	4.87	3,273	0	1 / 100ms	0	84	0
fe80::754f:9028:b446:2673	57544	ff02::1:3	5355	2	5.04	3,386	0	1 / 100ms	0	84	0
fe80::754f:9028:b446:2673	65462	ff02::1:3	5355	2	4.88	3,282	0	1 / 100ms	0	84	0
fe80::754f:9028:b446:2673	53383	ff02::1:3	5355	2	5.00	3,361	0	1 / 100ms	0	84	0
fe80::754f:9028:b446:2673	53579	ff02::1:3	5355	2	4.89	3,952	0	1 / 100ms	0	101	0
fe80::754f:9028:b446:2673	52060	ff02::1:3	5355	2	4.90	3,962	0	1 / 100ms	0	101	0
fe80::754f:9028:b446:2673	51759	ff02::1:3	5355	2	4.80	3,224	0	1 / 100ms	0	84	0
fe80::754f:9028:b446:2673	63520	ff02::1:3	5355	2	4.74	3,184	0	1 / 100ms	0	84	0
fe80::754f:9028:b446:2673	54281	ff02::1:3	5355	2	4.99	3,355	0	1 / 100ms	0	84	0
10.4.8.33	50129	239.255.255.250	1900	4	1.32	2,282	0	1 / 100ms	0	216	0
10.4.8.33	56448	239.255.255.250	1900	4	1.32	2,281	0	1 / 100ms	0	216	0
10.4.8.21	64886	239.255.255.250	1900	4	1.32	2,288	0	1 / 100ms	0	216	0
10.4.8.21	55513	239.255.255.250	1900	4	1.33	2,294	0	1 / 100ms	0	216	0
10.4.8.21	49594	239.255.255.250	1900	4	1.32	2,282	0	1 / 100ms	0	216	0
10.4.8.18	5353	224.0.0.251	5353	38	0.14	78	12 k	2 / 100ms	0	140	0
10.4.8.18	54792	224.0.0.252	5355	2	4.96	2,540	0	1 / 100ms	0	128	0
10.4.8.18	54793	239.255.255.250	1900	4	1.33	2,291	0	1 / 100ms	0	430	0
10.4.8.18	57120	224.0.0.252	5355	2	4.87	2,493	0	1 / 100ms	0	128	0
10.4.8.18	58682	224.0.0.252	5355	2	4.88	2,496	0	1 / 100ms	0	128	0
10.4.8.18	53631	224.0.0.252	5355	2	4.87	2,766	0	1 / 100ms	0	71	0
10.4.8.18	58961	224.0.0.252	5355	2	4.87	2,650	0	1 / 100ms	0	68	0
10.4.8.18	51961	224.0.0.252	5355	2	4.87	2,763	0	1 / 100ms	0	71	0
10.4.8.18	53421	224.0.0.252	5355	2	4.78	2,449	0	1 / 100ms	0	64	0
10.4.8.18	62355	224.0.0.252	5355	2	4.87	2,494	0	1 / 100ms	0	64	0
10.4.8.18	64959	224.0.0.252	5355	2	4.88	2,496	0	1 / 100ms	0	64	0
10.4.8.18	55672	224.0.0.252	5355	2	4.88	2,499	0	1 / 100ms	0	64	0
10.4.8.18	54864	224.0.0.252	5355	2	4.79	2,453	0	1 / 100ms	0	64	0
10.4.8.18	57926	224.0.0.252	5355	2	4.86	2,488	0	1 / 100ms	0	64	0
10.4.8.18	65184	224.0.0.252	5355	2	4.87	2,494	0	1 / 100ms	0	64	0
10.4.8.18	57544	224.0.0.252	5355	2	5.04	2,581	0	1 / 100ms	0	64	0
10.4.8.18	65462	224.0.0.252	5355	2	4.88	2,496	0	1 / 100ms	0	64	0
10.4.8.18	49436	239.255.255.250	1900	4	1.32	2,278	0	1 / 100ms	0	215	0
10.4.8.18	53383	224.0.0.252	5355	2	5.00	2,560	0	1 / 100ms	0	64	0
10.4.8.18	53579	224.0.0.252	5355	2	4.89	3,170	0	1 / 100ms	0	81	0
10.4.8.18	52060	224.0.0.252	5355	2	4.90	3,177	0	1 / 100ms	0	81	0

52 streams, avg bw: 559bps, max bw: 62 kbps, max burst: 11 / 100ms, max buffer: 140B

Burst measurement interval (ms): 100 | Burst alarm threshold (packets): 50 | Buffer alarm threshold (B): 10000

Stream empty speed (Kb/s): 5000 | Total empty speed (Kb/s): 100000

Display filter: tcp || udp | Apply

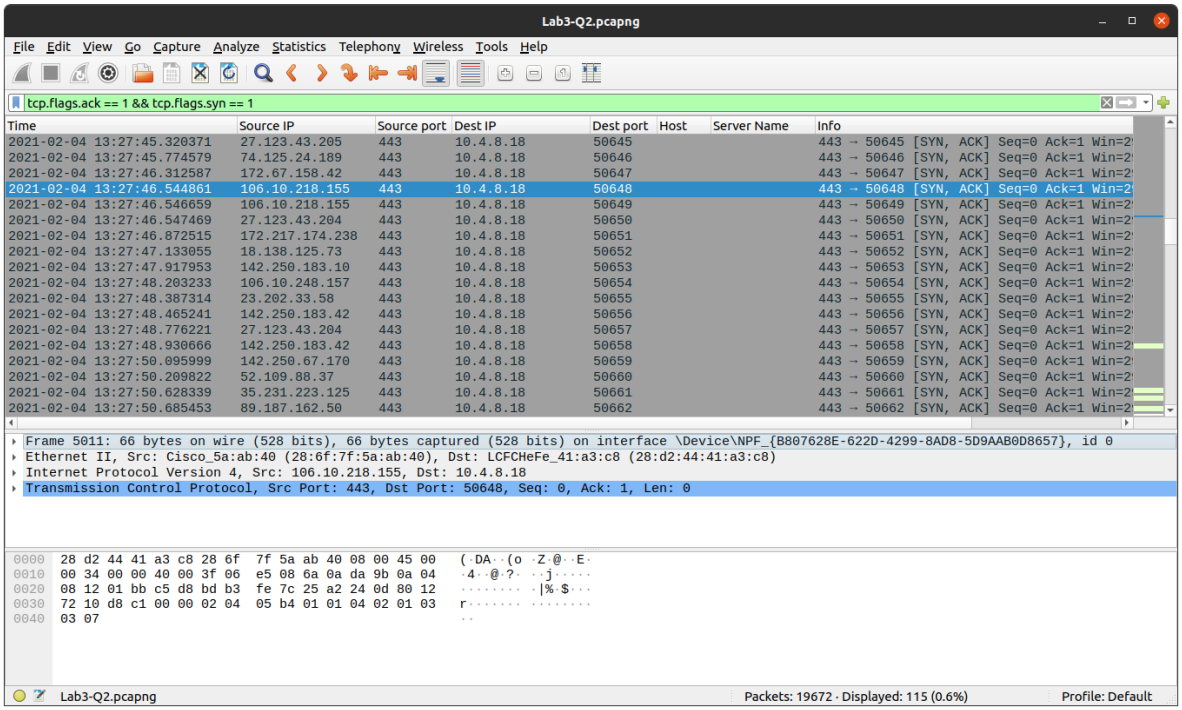
Copy | Save as… | Close

The UDP Multicast Streams statistics

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

The filter used here (`tcp.flags.ack==1 && tcp.flags.syn==1`) is a logical and of two separate filters (`tcp.flags.ack==1`) and (`tcp.flags.syn==1`).

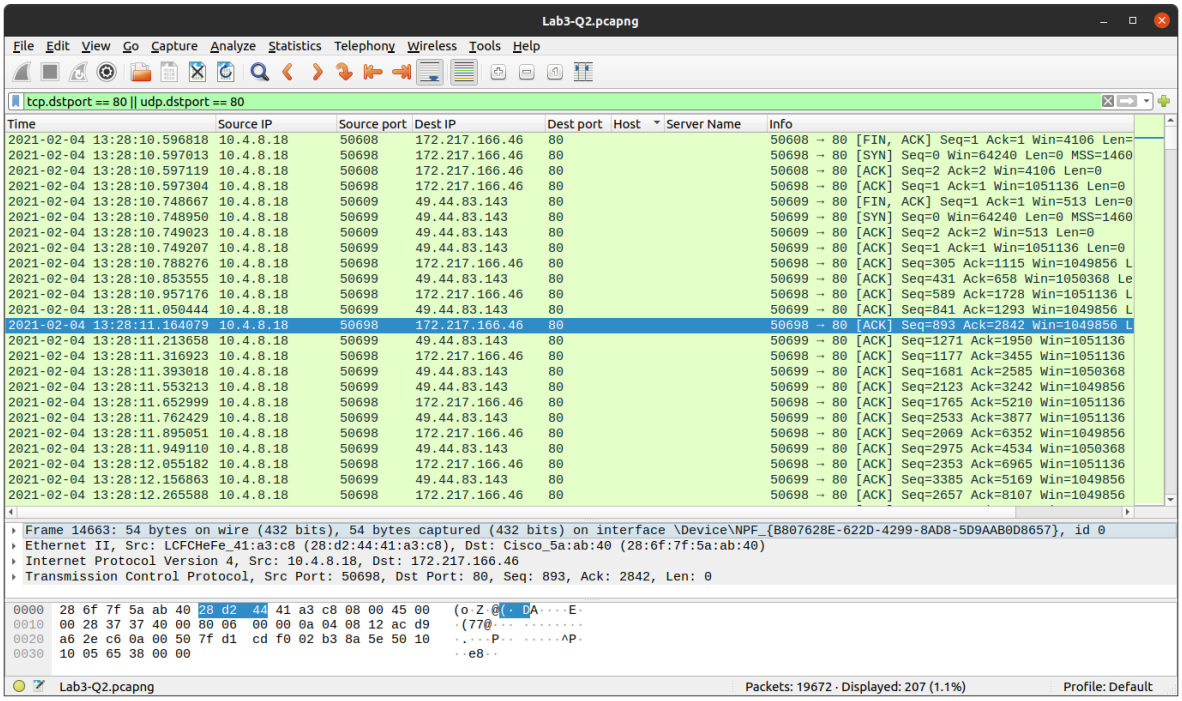
As is visible, the Info column shows both [SYN, ACK]; signifying a connection being initiated, and the packet has been received succesfully, respectively.



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

The filter used here, `tcp.dstport == 80 || udp.dstport == 80`, is also a logical combination of two separate filters.

As expected, the column for the Dest port shows number 80 for all the packets. This is also visible in the Info clumn, which displays both the Source and Destination port number.



f. List out the ARP packets

The `arp` filter is used here, to list out packets following the *Address Resolution Protocol.*

The Info column shows more information about the communication taking place with each packet.