

Lab 3

Parmesh Mathur

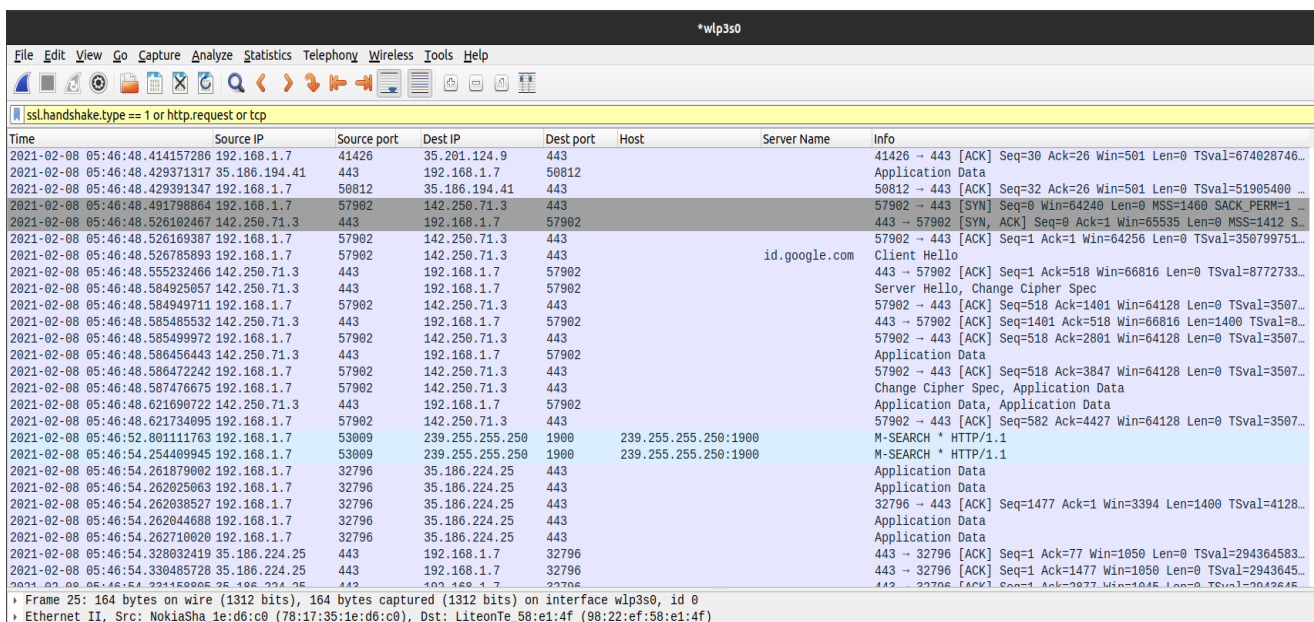
2018A7PS0133G

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		id.google.com	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			443 → 57902 [ACK] Seq=1 Ack=518 Win=66816 Len=0 TSval=8772733...
2021-02-08 05:46:48.555232466	142.250.71.3	443	192.168.1.7	57902			Server Hello, Change Cipher Spec
2021-02-08 05:46:48.584925057	142.250.71.3	443	192.168.1.7	57902			57902 → 443 [ACK] Seq=518 Ack=1401 Win=64128 Len=0 TSval=3507...
2021-02-08 05:46:48.584949711	192.168.1.7	57902	142.250.71.3	443			443 → 57902 [ACK] Seq=1401 Ack=518 Win=66816 Len=1400 TSval=8...
2021-02-08 05:46:48.585485532	142.250.71.3	443	192.168.1.7	57902			57902 → 443 [ACK] Seq=518 Ack=2801 Win=64128 Len=0 TSval=3507...
2021-02-08 05:46:48.585499972	192.168.1.7	57902	142.250.71.3	443			Application Data
2021-02-08 05:46:48.586456443	142.250.71.3	443	192.168.1.7	57902			57902 → 443 [ACK] Seq=518 Ack=3847 Win=64128 Len=0 TSval=3507...
2021-02-08 05:46:48.586472242	192.168.1.7	57902	142.250.71.3	443			Change Cipher Spec, Application Data
2021-02-08 05:46:48.587476675	192.168.1.7	57902	142.250.71.3	443			Application Data, Application Data
2021-02-08 05:46:48.621690722	142.250.71.3	443	192.168.1.7	57902			57902 → 443 [ACK] Seq=582 Ack=4427 Win=64128 Len=0 TSval=3507...
2021-02-08 05:46:48.621734095	192.168.1.7	57902	142.250.71.3	443			M-SEARCH * HTTP/1.1
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		Application Data
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...
2021-02-08 05:46:54.331558005	35.186.224.25	443	192.168.1.7	32796			443 → 32796 [ACK] Seq=1 Ack=2877 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.

The screenshot shows the Wireshark interface with the filter `http.request` applied. The packet list displays 18 HTTP requests. The packet details pane shows the structure of a selected packet (Frame 840), including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Simple Service Discovery Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Time	Source IP	Source port	Dest IP	Dest port	Host	Server Name Info
2021-02-04 13:27:33.506985	10.4.8.18	54793	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2021-02-04 13:27:34.509039	10.4.8.18	54793	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2021-02-04 13:27:35.509426	10.4.8.18	54793	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2021-02-04 13:27:36.509935	10.4.8.18	54793	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2021-02-04 13:28:02.972132	10.4.8.21	64886	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2021-02-04 13:28:03.972834	10.4.8.21	64886	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2021-02-04 13:28:04.992277	10.4.8.21	64886	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2021-02-04 13:28:05.992728	10.4.8.21	64886	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2021-02-04 13:28:10.605111	10.4.8.18	50698	172.217.166.46	80	redirector.gvt1.com	GET /edgedl/release2/chrome_component/A036Nr
2021-02-04 13:28:10.749730	10.4.8.18	50699	49.44.83.143	80	r4---sn-gwpa-ccpe.gvt1.com	GET /edgedl/release2/chrome_component/A036Nr
2021-02-04 13:28:10.814373	10.4.8.18	50698	172.217.166.46	80	redirector.gvt1.com	HEAD /edgedl/release2/chrome_component/A036Nr
2021-02-04 13:28:10.916725	10.4.8.18	50699	49.44.83.143	80	r4---sn-gwpa-ccpe.gvt1.com	HEAD /edgedl/release2/chrome_component/A036Nr
2021-02-04 13:28:11.019258	10.4.8.18	50698	172.217.166.46	80	redirector.gvt1.com	GET /edgedl/release2/chrome_component/A036Nr
2021-02-04 13:28:11.125763	10.4.8.18	50699	49.44.83.143	80	r4---sn-gwpa-ccpe.gvt1.com	GET /edgedl/release2/chrome_component/A036Nr
2021-02-04 13:28:11.173746	10.4.8.18	50698	172.217.166.46	80	redirector.gvt1.com	HEAD /edgedl/release2/chrome_component/A036Nr
2021-02-04 13:28:11.277241	10.4.8.18	50699	49.44.83.143	80	r4---sn-gwpa-ccpe.gvt1.com	HEAD /edgedl/release2/chrome_component/A036Nr
2021-02-04 13:28:11.362444	10.4.8.18	50698	172.217.166.46	80	redirector.gvt1.com	GET /edgedl/release2/chrome_component/A036Nr
2021-02-04 13:28:11.467934	10.4.8.18	50699	49.44.83.143	80	r4---sn-gwpa-ccpe.gvt1.com	GET /edgedl/release2/chrome_component/A036Nr

Frame 840: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AAB0D8657}, id 0
Ethernet II, Src: LOF0HeFe.41:a3:c8 (28:d2:44:a1:a3:c8), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 10.4.8.18, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 54793, Dst Port: 1900
Simple Service Discovery Protocol

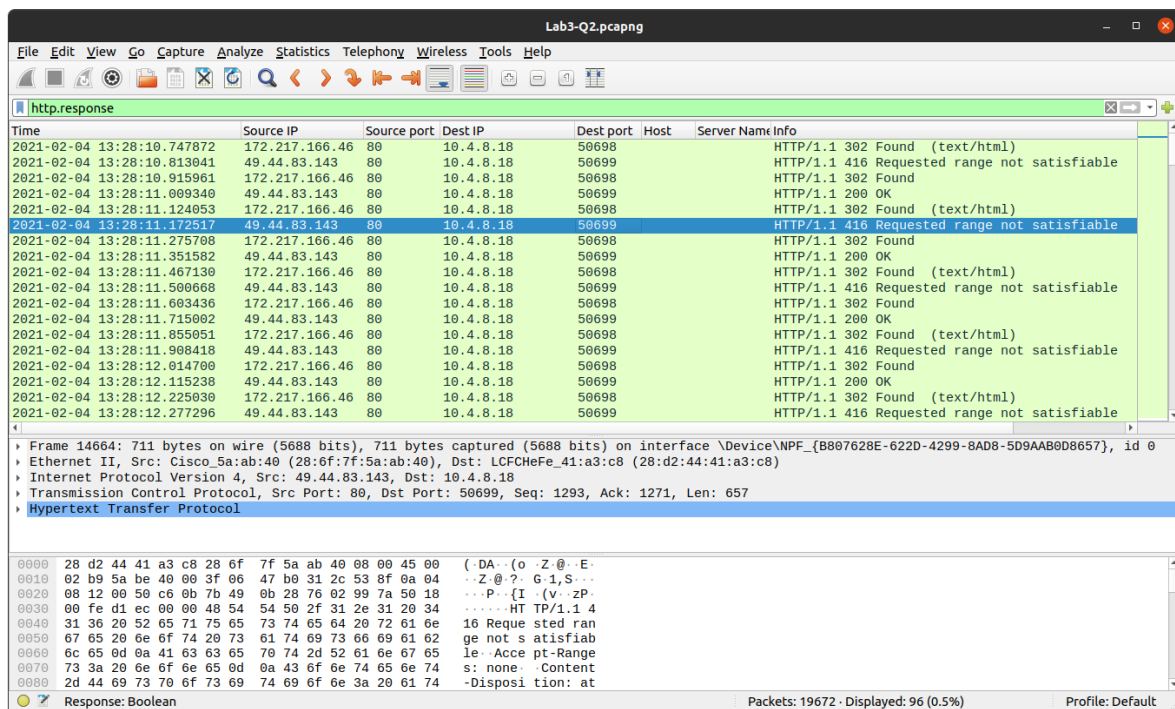
0000 01 00 5e 7f ff fa 28 d2 44 a1 a3 c8 08 00 45 00 --A---(DA---E-
0010 00 c9 29 ac 00 00 01 11 00 00 0a 04 08 12 ef ff --)---
0020 ff fa d6 09 07 6c 00 b5 d5 ba 4d 2d 53 45 41 52 ----1---M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTTP/1.1: H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239.255.255
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 ,250:190 0-MAN;
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 6d "ssdp:discover"
0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a .MX: 1--ST: urn:
0080 64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e dial-multiscreen

Request: Boolean Packets: 19672 - Displayed: 128 (0.7%) Profile: Default

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).



The image shows a Wireshark capture window titled "Lab3-Q2.pcapng". The filter bar at the top shows the filter `http.response`. The packet list pane displays a table of captured packets, all of which are HTTP responses. The packet details pane shows the structure of a selected packet (Frame 14664), including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol layers. The packet bytes pane shows the raw data of the selected packet.

Time	Source IP	Source port	Dest IP	Dest port	Host	Server Name Info
2021-02-04 13:28:10.747872	172.217.166.46	80	10.4.8.18	50698		HTTP/1.1 302 Found (text/html)
2021-02-04 13:28:10.813041	49.44.83.143	80	10.4.8.18	50699		HTTP/1.1 416 Requested range not satisfiable
2021-02-04 13:28:10.915961	172.217.166.46	80	10.4.8.18	50698		HTTP/1.1 302 Found
2021-02-04 13:28:11.009340	49.44.83.143	80	10.4.8.18	50699		HTTP/1.1 200 OK
2021-02-04 13:28:11.124653	172.217.166.46	80	10.4.8.18	50698		HTTP/1.1 302 Found (text/html)
2021-02-04 13:28:11.172517	49.44.83.143	80	10.4.8.18	50699		HTTP/1.1 416 Requested range not satisfiable
2021-02-04 13:28:11.275708	172.217.166.46	80	10.4.8.18	50698		HTTP/1.1 302 Found
2021-02-04 13:28:11.351582	49.44.83.143	80	10.4.8.18	50699		HTTP/1.1 200 OK
2021-02-04 13:28:11.467138	172.217.166.46	80	10.4.8.18	50698		HTTP/1.1 302 Found (text/html)
2021-02-04 13:28:11.500668	49.44.83.143	80	10.4.8.18	50699		HTTP/1.1 416 Requested range not satisfiable
2021-02-04 13:28:11.603436	172.217.166.46	80	10.4.8.18	50698		HTTP/1.1 302 Found
2021-02-04 13:28:11.715002	49.44.83.143	80	10.4.8.18	50699		HTTP/1.1 200 OK
2021-02-04 13:28:11.855051	172.217.166.46	80	10.4.8.18	50698		HTTP/1.1 302 Found (text/html)
2021-02-04 13:28:11.908418	49.44.83.143	80	10.4.8.18	50699		HTTP/1.1 416 Requested range not satisfiable
2021-02-04 13:28:12.014700	172.217.166.46	80	10.4.8.18	50698		HTTP/1.1 302 Found
2021-02-04 13:28:12.115238	49.44.83.143	80	10.4.8.18	50699		HTTP/1.1 200 OK
2021-02-04 13:28:12.225030	172.217.166.46	80	10.4.8.18	50698		HTTP/1.1 302 Found (text/html)
2021-02-04 13:28:12.277296	49.44.83.143	80	10.4.8.18	50699		HTTP/1.1 416 Requested range not satisfiable

Frame 14664: 711 bytes on wire (5688 bits), 711 bytes captured (5688 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AAB0D8657}, id 0
Ethernet II, Src: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40), Dst: LCfCHeFe_41:a3:c8 (28:d2:44:41:a3:c8)
Internet Protocol Version 4, Src: 49.44.83.143, Dst: 10.4.8.18
Transmission Control Protocol, Src Port: 80, Dst Port: 50699, Seq: 1293, Ack: 1271, Len: 657
Hypertext Transfer Protocol

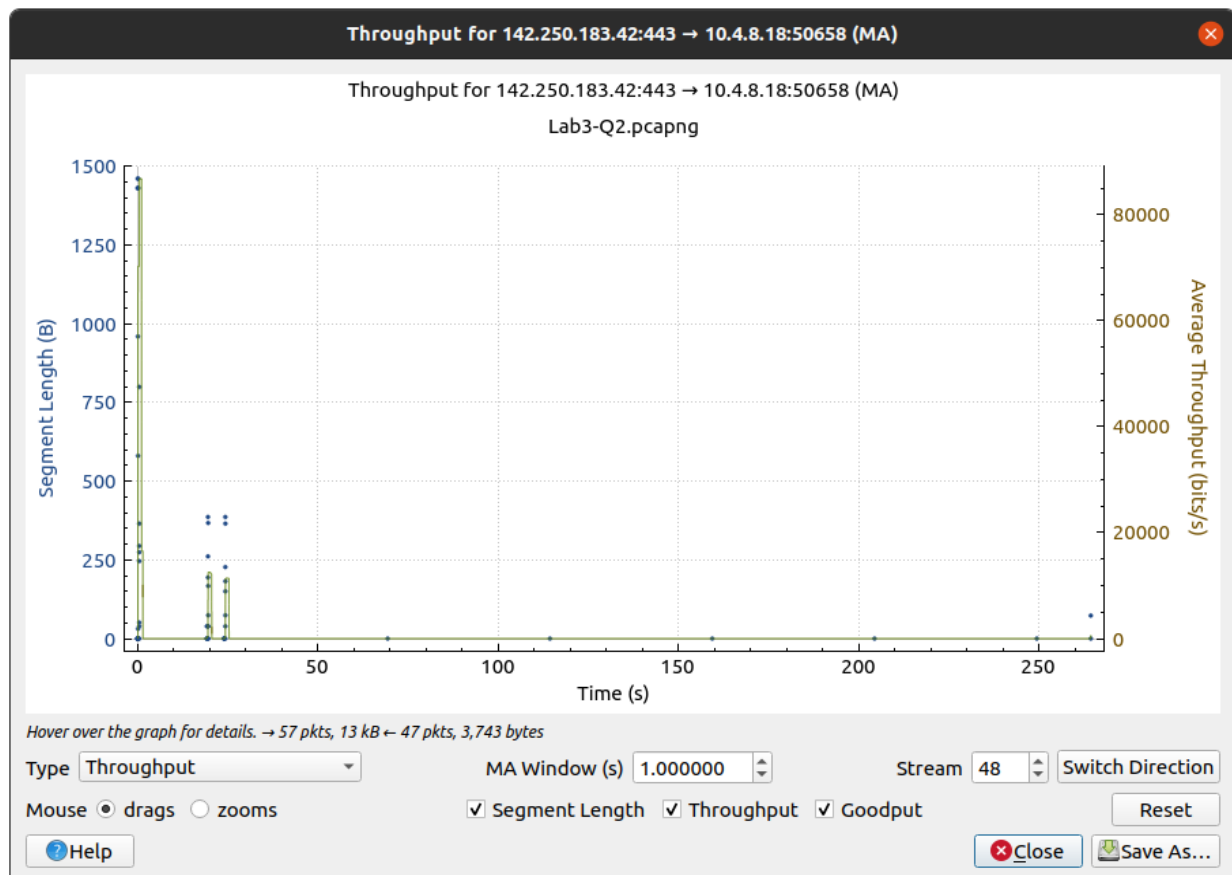
0000 28 d2 44 41 a3 c8 28 6f 7f 5a ab 40 08 00 45 00 (.DA..(o .Z.@..E
0010 02 b9 5a be 40 00 3f 06 47 b0 31 2c 53 8f 0a 04 ..Z.@.? G 1,S..
0020 08 12 00 50 c6 0b 7b 49 0b 28 76 02 99 7a 50 18 ...P...{I .(v .zP
0030 00 fe d1 ec 00 00 48 54 54 50 2f 31 2e 31 20 34HT TP/1.1 4
0040 31 36 20 52 65 71 75 05 73 74 05 64 20 72 61 6e 16 Requested ran
0050 67 65 20 6e 6f 74 20 73 61 74 69 73 66 69 61 62 ge not s atisfiab
0060 6c 65 0d 0a 41 63 63 65 70 74 2d 52 61 6e 67 65 le .Acce pt-Range
0070 73 3a 20 6e 6f 6e 65 0d 0a 43 6f 6e 74 65 6e 74 s: none .Content
0080 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 61 74 -Disposi tion: at

Response: Boolean Packets: 19672 · Displayed: 96 (0.5%) Profile: Default

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 statistics 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::754f9028:b446:2673	5353	ff02::fb	5353	38	0.14	100	15 k	2 / 100ms	0	90	0
fe80::754f9028:b446:2673	54792	ff02::13	5355	2	4.96	3,333	0	1 / 100ms	0	168	0
fe80::754f9028:b446:2673	57120	ff02::13	5355	2	4.87	3,272	0	1 / 100ms	0	168	0
fe80::754f9028:b446:2673	58682	ff02::13	5355	2	4.87	3,275	0	1 / 100ms	0	168	0
fe80::754f9028:b446:2673	53631	ff02::13	5355	2	4.87	3,545	0	1 / 100ms	0	91	0
fe80::754f9028:b446:2673	58961	ff02::13	5355	2	4.87	3,429	0	1 / 100ms	0	88	0
fe80::754f9028:b446:2673	51961	ff02::13	5355	2	4.86	3,541	0	1 / 100ms	0	91	0
fe80::754f9028:b446:2673	53421	ff02::13	5355	2	4.79	3,215	0	1 / 100ms	0	84	0
fe80::754f9028:b446:2673	62355	ff02::13	5355	2	4.87	3,274	0	1 / 100ms	0	84	0
fe80::754f9028:b446:2673	64959	ff02::13	5355	2	4.88	3,276	0	1 / 100ms	0	84	0
fe80::754f9028:b446:2673	55672	ff02::13	5355	2	4.88	3,279	0	1 / 100ms	0	84	0
fe80::754f9028:b446:2673	54864	ff02::13	5355	2	4.79	3,220	0	1 / 100ms	0	84	0
fe80::754f9028:b446:2673	57926	ff02::13	5355	2	4.86	3,266	0	1 / 100ms	0	84	0
fe80::754f9028:b446:2673	65184	ff02::13	5355	2	4.87	3,273	0	1 / 100ms	0	84	0
fe80::754f9028:b446:2673	57544	ff02::13	5355	2	5.04	3,386	0	1 / 100ms	0	84	0
fe80::754f9028:b446:2673	65462	ff02::13	5355	2	4.88	3,282	0	1 / 100ms	0	84	0
fe80::754f9028:b446:2673	53383	ff02::13	5355	2	5.00	3,361	0	1 / 100ms	0	84	0
fe80::754f9028:b446:2673	53579	ff02::13	5355	2	4.89	3,952	0	1 / 100ms	0	101	0
fe80::754f9028:b446:2673	52060	ff02::13	5355	2	4.90	3,962	0	1 / 100ms	0	101	0
fe80::754f9028:b446:2673	51759	ff02::13	5355	2	4.80	3,224	0	1 / 100ms	0	84	0
fe80::754f9028:b446:2673	63520	ff02::13	5355	2	4.74	3,184	0	1 / 100ms	0	84	0
fe80::754f9028:b446:2673	54281	ff02::13	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
10.4.8.18	51759	224.0.0.252	5355	2	4.80	2,457	0	1 / 100ms	0	64	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 successfully, respectively.

Lab3-Q2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

Time	Source IP	Source port	Dest IP	Dest port	Host	Server Name	Info
2021-02-04 13:27:45.320371	27.123.43.205	443	10.4.8.18	50645			443 → 50645 [SYN, ACK] Seq=0 Ack=1 Win=2
2021-02-04 13:27:45.774579	74.125.24.189	443	10.4.8.18	50646			443 → 50646 [SYN, ACK] Seq=0 Ack=1 Win=2
2021-02-04 13:27:46.312587	172.67.158.42	443	10.4.8.18	50647			443 → 50647 [SYN, ACK] Seq=0 Ack=1 Win=2
2021-02-04 13:27:46.544861	106.10.218.155	443	10.4.8.18	50648			443 → 50648 [SYN, ACK] Seq=0 Ack=1 Win=2
2021-02-04 13:27:46.546659	106.10.218.155	443	10.4.8.18	50649			443 → 50649 [SYN, ACK] Seq=0 Ack=1 Win=2
2021-02-04 13:27:46.547469	27.123.43.204	443	10.4.8.18	50650			443 → 50650 [SYN, ACK] Seq=0 Ack=1 Win=2
2021-02-04 13:27:46.872515	172.217.174.238	443	10.4.8.18	50651			443 → 50651 [SYN, ACK] Seq=0 Ack=1 Win=2
2021-02-04 13:27:47.133055	18.138.125.73	443	10.4.8.18	50652			443 → 50652 [SYN, ACK] Seq=0 Ack=1 Win=2
2021-02-04 13:27:47.917953	142.250.183.10	443	10.4.8.18	50653			443 → 50653 [SYN, ACK] Seq=0 Ack=1 Win=2
2021-02-04 13:27:48.203233	106.10.248.157	443	10.4.8.18	50654			443 → 50654 [SYN, ACK] Seq=0 Ack=1 Win=2
2021-02-04 13:27:48.387314	23.282.33.58	443	10.4.8.18	50655			443 → 50655 [SYN, ACK] Seq=0 Ack=1 Win=2
2021-02-04 13:27:48.465241	142.250.183.42	443	10.4.8.18	50656			443 → 50656 [SYN, ACK] Seq=0 Ack=1 Win=2
2021-02-04 13:27:48.776221	27.123.43.204	443	10.4.8.18	50657			443 → 50657 [SYN, ACK] Seq=0 Ack=1 Win=2
2021-02-04 13:27:48.930666	142.250.183.42	443	10.4.8.18	50658			443 → 50658 [SYN, ACK] Seq=0 Ack=1 Win=2
2021-02-04 13:27:50.095999	142.250.67.170	443	10.4.8.18	50659			443 → 50659 [SYN, ACK] Seq=0 Ack=1 Win=2
2021-02-04 13:27:50.209822	52.109.88.37	443	10.4.8.18	50660			443 → 50660 [SYN, ACK] Seq=0 Ack=1 Win=2
2021-02-04 13:27:50.628339	35.231.223.125	443	10.4.8.18	50661			443 → 50661 [SYN, ACK] Seq=0 Ack=1 Win=2
2021-02-04 13:27:50.685453	89.187.162.50	443	10.4.8.18	50662			443 → 50662 [SYN, ACK] Seq=0 Ack=1 Win=2

Frame 5011: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AAB0D8657}, id 0

Ethernet II, Src: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40), Dst: LCFChFe_41:a3:c8 (28:d2:44:41:a3:c8)

Internet Protocol Version 4, Src: 106.10.218.155, Dst: 10.4.8.18

Transmission Control Protocol, Src Port: 443, Dst Port: 50648, Seq: 0, Ack: 1, Len: 0

0000 28 d2 44 41 a3 c8 28 6f 7f 5a ab 40 08 00 45 00 (.DA.(o.Z.@.E.

0010 00 34 00 00 00 00 3f 06 e5 08 0a 0a da 9b 0a 04 .4.@.?..j]....

0020 08 12 01 bb c5 08 bd b3 fe 7c 25 a2 24 0d 00 12:|%.S...

0030 72 10 d8 c1 00 00 02 04 05 b4 01 01 04 02 01 03 r.....

0040 03 07 ..

Lab3-Q2.pcapng Packets: 19672 · Displayed: 115 (0.6%) Profile: Default

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 column, which displays both the Source and Destination port number.

Lab3-Q2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

Time	Source IP	Source port	Dest IP	Dest port	Host	Server Name	Info
2021-02-04 13:28:10.596818	10.4.8.18	50608	172.217.166.46	80			50608 → 80 [FIN, ACK] Seq=1 Ack=1 Win=4106 Len=0
2021-02-04 13:28:10.597013	10.4.8.18	50698	172.217.166.46	80			50698 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2021-02-04 13:28:10.597119	10.4.8.18	50608	172.217.166.46	80			50608 → 80 [ACK] Seq=2 Ack=2 Win=4106 Len=0
2021-02-04 13:28:10.597304	10.4.8.18	50698	172.217.166.46	80			50698 → 80 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
2021-02-04 13:28:10.748667	10.4.8.18	50609	49.44.83.143	80			50609 → 80 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
2021-02-04 13:28:10.748950	10.4.8.18	50699	49.44.83.143	80			50699 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2021-02-04 13:28:10.749023	10.4.8.18	50609	49.44.83.143	80			50609 → 80 [ACK] Seq=2 Ack=2 Win=513 Len=0
2021-02-04 13:28:10.749207	10.4.8.18	50699	49.44.83.143	80			50699 → 80 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
2021-02-04 13:28:10.788276	10.4.8.18	50698	172.217.166.46	80			50698 → 80 [ACK] Seq=305 Ack=1115 Win=1049856 L
2021-02-04 13:28:10.853555	10.4.8.18	50699	49.44.83.143	80			50699 → 80 [ACK] Seq=431 Ack=658 Win=1050368 Le
2021-02-04 13:28:10.957176	10.4.8.18	50698	172.217.166.46	80			50698 → 80 [ACK] Seq=589 Ack=1728 Win=1051136 L
2021-02-04 13:28:11.050444	10.4.8.18	50699	49.44.83.143	80			50699 → 80 [ACK] Seq=841 Ack=1293 Win=1049856 L
2021-02-04 13:28:11.164079	10.4.8.18	50698	172.217.166.46	80			50698 → 80 [ACK] Seq=893 Ack=2842 Win=1049856 L
2021-02-04 13:28:11.213658	10.4.8.18	50699	49.44.83.143	80			50699 → 80 [ACK] Seq=1271 Ack=1950 Win=1051136
2021-02-04 13:28:11.316923	10.4.8.18	50698	172.217.166.46	80			50698 → 80 [ACK] Seq=1177 Ack=3455 Win=1051136
2021-02-04 13:28:11.393018	10.4.8.18	50699	49.44.83.143	80			50699 → 80 [ACK] Seq=1681 Ack=2585 Win=1050368
2021-02-04 13:28:11.553213	10.4.8.18	50699	49.44.83.143	80			50699 → 80 [ACK] Seq=2123 Ack=3242 Win=1049856
2021-02-04 13:28:11.652999	10.4.8.18	50698	172.217.166.46	80			50698 → 80 [ACK] Seq=1765 Ack=5210 Win=1051136
2021-02-04 13:28:11.762429	10.4.8.18	50699	49.44.83.143	80			50699 → 80 [ACK] Seq=2533 Ack=3877 Win=1051136
2021-02-04 13:28:11.895051	10.4.8.18	50698	172.217.166.46	80			50698 → 80 [ACK] Seq=2069 Ack=6352 Win=1049856
2021-02-04 13:28:11.949110	10.4.8.18	50699	49.44.83.143	80			50699 → 80 [ACK] Seq=2975 Ack=4534 Win=1050368
2021-02-04 13:28:12.055182	10.4.8.18	50698	172.217.166.46	80			50698 → 80 [ACK] Seq=2353 Ack=6965 Win=1051136
2021-02-04 13:28:12.156863	10.4.8.18	50699	49.44.83.143	80			50699 → 80 [ACK] Seq=3385 Ack=5169 Win=1049856
2021-02-04 13:28:12.265588	10.4.8.18	50698	172.217.166.46	80			50698 → 80 [ACK] Seq=2657 Ack=8107 Win=1049856

Frame 14663: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AAB0D8657}, id 0

Ethernet II, Src: LcFChEFe_41:a3:c8 (28:d2:44:41:a3:c8), Dst: Cisco_5a:ab:40 (28:6f:7f:5a:ab:40)

Internet Protocol Version 4, Src: 10.4.8.18, Dst: 172.217.166.46

Transmission Control Protocol, Src Port: 50698, Dst Port: 80, Seq: 893, Ack: 2842, Len: 0

0000 28 f7 7f 5a ab 40 28 d2 44 41 a3 c8 08 00 45 00 (0 Z 6 [U A E .

0010 00 28 37 37 40 00 00 00 00 00 0a 04 08 12 ac d9 . (778

0020 a6 2e c6 8a 00 50 7f d1 cd f0 62 b3 8a 5e 50 10 P A P .

0030 10 05 65 38 00 00 . . e8 . .

Lab3-Q2.pcapng Packets: 19672 · Displayed: 207 (1.1%) Profile: Default

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.

The image shows a Wireshark packet capture window titled "Lab3-Q2.pcapng". The filter bar at the top contains the text "arp". The packet list pane shows a table of captured packets, with the 15th packet (Time: 13:27:51.615444) selected. The packet details pane shows the structure of the selected packet: Ethernet II, Src: LCFHeFe_41:a3:c8 (28:d2:44:41:a3:c8), Dst: Cisco_49:b4:1b (a0:e0:af:49:b4:1b), and Address Resolution Protocol (reply). The packet bytes pane shows the raw data in hexadecimal and ASCII.

Time	Source IP	Source port	Dest IP	Dest port	Host	Server Name	Info
2021-02-04 13:27:35.064012	00:0f:29:ce:87:01		ff:ff:ff:ff:ff:ff				Who has 10.20.0.1? Tell 10.4.8.21
2021-02-04 13:27:35.068952	00:0f:29:ce:87:01		ff:ff:ff:ff:ff:ff				Who has 10.4.8.1? Tell 10.4.8.21
2021-02-04 13:27:35.069133	00:0f:29:ce:87:01		ff:ff:ff:ff:ff:ff				Who has 10.4.8.1? Tell 10.4.8.21
2021-02-04 13:27:38.194242	00:17:e0:34:14:0e		a0:e0:af:49:b0:99				10.4.8.47 is at 00:17:e0:34:14:0e
2021-02-04 13:27:44.070653	a0:e0:af:49:b0:99		00:e0:d8:1b:ba:01				Who has 10.4.8.12? Tell 0.0.0.0
2021-02-04 13:27:51.615444	a0:e0:af:49:b4:1b		28:d2:44:41:a3:c8				Who has 10.4.8.18? Tell 0.0.0.0
2021-02-04 13:27:51.615456	28:d2:44:41:a3:c8		a0:e0:af:49:b4:1b				10.4.8.18 is at 28:d2:44:41:a3:c8
2021-02-04 13:28:05.035518	28:6f:7f:5a:ab:40		28:d2:44:41:a3:c8				Who has 10.4.8.18? Tell 10.4.8.1
2021-02-04 13:28:05.035518	28:6f:7f:5a:ab:40		fc:15:b4:e6:31:93				Who has 10.4.8.13? Tell 10.4.8.1
2021-02-04 13:28:05.035534	28:d2:44:41:a3:c8		28:6f:7f:5a:ab:40				10.4.8.18 is at 28:d2:44:41:a3:c8
2021-02-04 13:28:18.350939	00:e0:d8:1b:ba:01		a0:e0:af:49:b0:99				10.4.8.12 is at 00:e0:d8:1b:ba:01
2021-02-04 13:28:20.849004	a0:e0:af:49:b0:99		28:d2:44:41:a3:c8				Who has 10.4.8.18? Tell 0.0.0.0
2021-02-04 13:28:20.849032	28:d2:44:41:a3:c8		a0:e0:af:49:b0:99				10.4.8.18 is at 28:d2:44:41:a3:c8
2021-02-04 13:28:20.976936	a0:e0:af:49:b4:1b		28:d2:44:41:a3:c8				Who has 10.4.8.18? Tell 0.0.0.0
2021-02-04 13:28:20.976976	28:d2:44:41:a3:c8		a0:e0:af:49:b4:1b				10.4.8.18 is at 28:d2:44:41:a3:c8
2021-02-04 13:28:34.957658	28:d2:44:41:a3:c8		ff:ff:ff:ff:ff:ff				Who has 10.4.8.1? Tell 10.4.8.18
2021-02-04 13:28:34.959043	28:6f:7f:5a:ab:40		28:d2:44:41:a3:c8				10.4.8.1 is at 28:6f:7f:5a:ab:40
2021-02-04 13:28:34.968015	28:d2:44:41:a3:c8		ff:ff:ff:ff:ff:ff				Who has 10.4.8.1? Tell 10.4.8.18

Frame 7542: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AAB0D8657}, id 0
Ethernet II, Src: LCFHeFe_41:a3:c8 (28:d2:44:41:a3:c8), Dst: Cisco_49:b4:1b (a0:e0:af:49:b4:1b)
Address Resolution Protocol (reply)

0000 a0 e0 af 49 b4 1b 28 d2 44 41 a3 c8 08 06 00 01 ...I...DA.....
0010 08 00 06 04 00 02 28 d2 44 41 a3 c8 0a 04 08 12DA.....
0020 a0 e0 af 49 b4 1b 00 00 00 00 ...I.....

Address Resolution Protocol: Protocol Packets: 19672 · Displayed: 1273 (6.5%) Profile: Default