

LAB 3 - More on Wireshark and Introduction to Network Programming

NAME - DEV GOEL

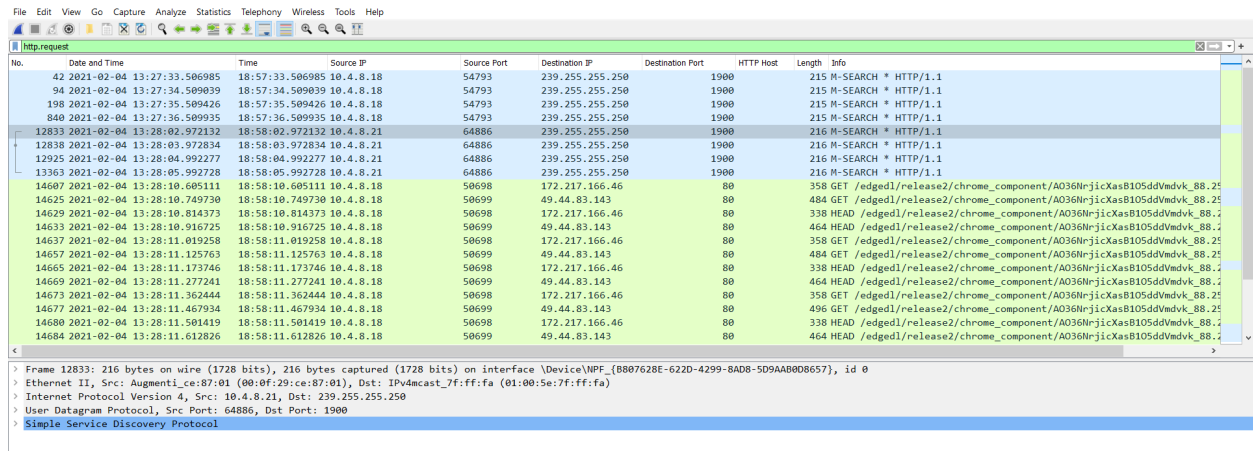
ID - 2019A7PS0236G

Q 2. Load the provided file into WireShark and then answer the following questions along with necessary screenshots (1 mark x 6 = 6 marks)

a. Identify the http request packet

Ans -

Filter applied => http.request



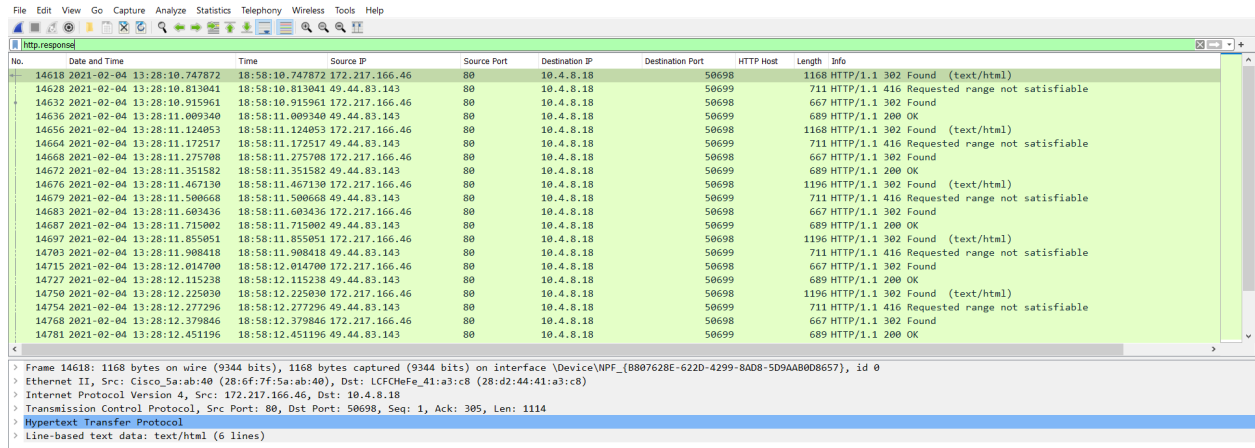
No.	Date and Time	Time	Source IP	Source Port	Destination IP	Destination Port	HTTP Host	Length	Info
42	2021-02-04 13:27:33.586985	18:57:33.586985	10.4.8.18	54793	239.255.255.250	1900	215 M-SEARCH * HTTP/1.1		
94	2021-02-04 13:27:34.589039	18:57:34.589039	10.4.8.18	54793	239.255.255.250	1900	215 M-SEARCH * HTTP/1.1		
198	2021-02-04 13:27:35.589426	18:57:35.589426	10.4.8.18	54793	239.255.255.250	1900	215 M-SEARCH * HTTP/1.1		
840	2021-02-04 13:27:36.589935	18:57:36.589935	10.4.8.18	54793	239.255.255.250	1900	215 M-SEARCH * HTTP/1.1		
12833	2021-02-04 13:28:02.972132	18:58:02.972132	10.4.8.21	64886	239.255.255.250	1900	216 M-SEARCH * HTTP/1.1		
12838	2021-02-04 13:28:03.972834	18:58:03.972834	10.4.8.21	64886	239.255.255.250	1900	216 M-SEARCH * HTTP/1.1		
12925	2021-02-04 13:28:04.992277	18:58:04.992277	10.4.8.21	64886	239.255.255.250	1900	216 M-SEARCH * HTTP/1.1		
13363	2021-02-04 13:28:05.992728	18:58:05.992728	10.4.8.21	64886	239.255.255.250	1900	216 M-SEARCH * HTTP/1.1		
14607	2021-02-04 13:28:10.605111	18:58:10.605111	10.4.8.18	50698	172.217.166.46	80	358 GET /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.2		
14625	2021-02-04 13:28:10.749730	18:58:10.749730	10.4.8.18	50699	49.44.83.143	80	484 GET /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.2		
14629	2021-02-04 13:28:10.814373	18:58:10.814373	10.4.8.18	50698	172.217.166.46	80	338 HEAD /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.2		
14633	2021-02-04 13:28:10.916725	18:58:10.916725	10.4.8.18	50699	49.44.83.143	80	464 HEAD /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.2		
14637	2021-02-04 13:28:11.019258	18:58:11.019258	10.4.8.18	50698	172.217.166.46	80	358 GET /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.2		
14657	2021-02-04 13:28:11.125763	18:58:11.125763	10.4.8.18	50699	49.44.83.143	80	484 GET /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.2		
14665	2021-02-04 13:28:11.173746	18:58:11.173746	10.4.8.18	50698	172.217.166.46	80	338 HEAD /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.2		
14669	2021-02-04 13:28:11.277241	18:58:11.277241	10.4.8.18	50699	49.44.83.143	80	464 HEAD /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.2		
14673	2021-02-04 13:28:11.362444	18:58:11.362444	10.4.8.18	50698	172.217.166.46	80	358 GET /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.2		
14677	2021-02-04 13:28:11.467934	18:58:11.467934	10.4.8.18	50699	49.44.83.143	80	496 GET /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.2		
14680	2021-02-04 13:28:11.501419	18:58:11.501419	10.4.8.18	50698	172.217.166.46	80	338 HEAD /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.2		
14684	2021-02-04 13:28:11.612826	18:58:11.612826	10.4.8.18	50699	49.44.83.143	80	464 HEAD /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.2		

< Frame 12833: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AAB0D8657}, id 0
> Ethernet II, Src: Augmentica:87:01 (00:0f:29:ce:87:01), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 10.4.8.21, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 64886, Dst Port: 1900
> Simple Service Discovery Protocol

b. Identify the http response packet

Ans -

Filter applied => http.response



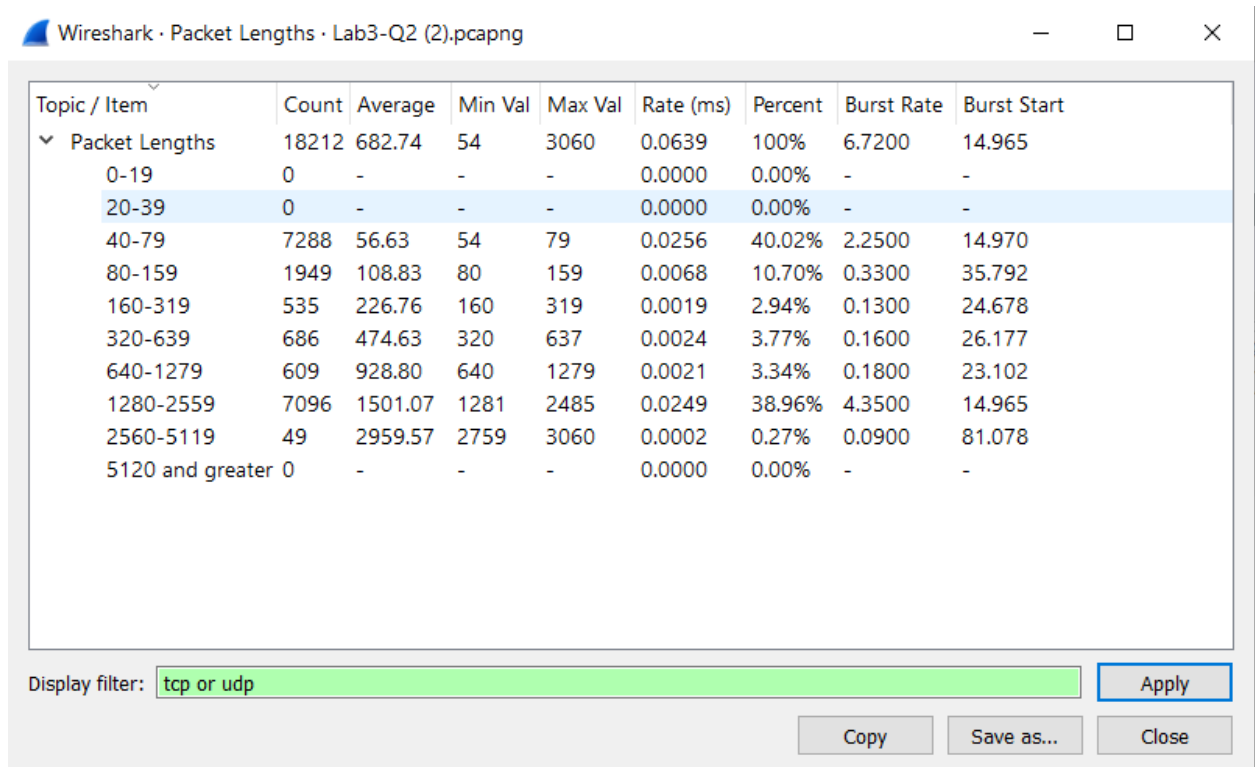
No.	Date and Time	Time	Source IP	Source Port	Destination IP	Destination Port	HTTP Host	Length	Info
14618	2021-02-04 13:28:10.747872	18:58:10.747872	172.217.166.46	80	10.4.8.18	50698	1168 HTTP/1.1 302 Found (text/html)		
14628	2021-02-04 13:28:10.813041	18:58:10.813041	49.44.83.143	80	10.4.8.18	50699	711 HTTP/1.1 416 Requested range not satisfiable		
14632	2021-02-04 13:28:10.915961	18:58:10.915961	172.217.166.46	80	10.4.8.18	50698	667 HTTP/1.1 302 Found		
14636	2021-02-04 13:28:11.009340	18:58:11.009340	49.44.83.143	80	10.4.8.18	50699	689 HTTP/1.1 200 OK		
14656	2021-02-04 13:28:11.124053	18:58:11.124053	172.217.166.46	80	10.4.8.18	50698	1168 HTTP/1.1 302 Found (text/html)		
14664	2021-02-04 13:28:11.172517	18:58:11.172517	49.44.83.143	80	10.4.8.18	50699	711 HTTP/1.1 416 Requested range not satisfiable		
14668	2021-02-04 13:28:11.275708	18:58:11.275708	172.217.166.46	80	10.4.8.18	50698	667 HTTP/1.1 302 Found		
14672	2021-02-04 13:28:11.351582	18:58:11.351582	49.44.83.143	80	10.4.8.18	50699	689 HTTP/1.1 200 OK		
14676	2021-02-04 13:28:11.467130	18:58:11.467130	172.217.166.46	80	10.4.8.18	50698	1196 HTTP/1.1 302 Found (text/html)		
14679	2021-02-04 13:28:11.500668	18:58:11.500668	49.44.83.143	80	10.4.8.18	50699	711 HTTP/1.1 416 Requested range not satisfiable		
14683	2021-02-04 13:28:11.603436	18:58:11.603436	172.217.166.46	80	10.4.8.18	50698	667 HTTP/1.1 302 Found		
14687	2021-02-04 13:28:11.715002	18:58:11.715002	49.44.83.143	80	10.4.8.18	50699	689 HTTP/1.1 200 OK		
14697	2021-02-04 13:28:11.855051	18:58:11.855051	172.217.166.46	80	10.4.8.18	50698	1196 HTTP/1.1 302 Found (text/html)		
14703	2021-02-04 13:28:11.908418	18:58:11.908418	49.44.83.143	80	10.4.8.18	50699	711 HTTP/1.1 416 Requested range not satisfiable		
14715	2021-02-04 13:28:12.014700	18:58:12.014700	172.217.166.46	80	10.4.8.18	50698	667 HTTP/1.1 302 Found		
14727	2021-02-04 13:28:12.115238	18:58:12.115238	49.44.83.143	80	10.4.8.18	50699	689 HTTP/1.1 200 OK		
14750	2021-02-04 13:28:12.225030	18:58:12.225030	172.217.166.46	80	10.4.8.18	50698	1196 HTTP/1.1 302 Found (text/html)		
14754	2021-02-04 13:28:12.277296	18:58:12.277296	49.44.83.143	80	10.4.8.18	50699	711 HTTP/1.1 416 Requested range not satisfiable		
14768	2021-02-04 13:28:12.379846	18:58:12.379846	172.217.166.46	80	10.4.8.18	50698	667 HTTP/1.1 302 Found		
14781	2021-02-04 13:28:12.451196	18:58:12.451196	49.44.83.143	80	10.4.8.18	50699	689 HTTP/1.1 200 OK		

> Frame 14618: 1168 bytes on wire (9344 bits), 1168 bytes captured (9344 bits) on interface \Device\NPF_{B807628E-6220-4299-8AD8-5D9AAB0D8657}, id 0
> Ethernet II, Src: Cisco_Sa:ab:40 (28:6f:7f:5a:ab:40), Dst: LCFMeFe_41:a3:c8 (28:d2:44:41:a3:c8)
> Internet Protocol Version 4, Src: 172.217.166.46, Dst: 10.4.8.18
> Transmission Control Protocol, Src Port: 80, Dst Port: 50698, Seq: 1, Ack: 305, Len: 1114
> Hypertext Transfer Protocol
> Line-based text data: text/html (6 lines)

c. Display the statistics of the TCP and UDP packets

Ans -

PACKET LENGTHS



Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	18212	682.74	54	3060	0.0639	100%	6.7200	14.965
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	7288	56.63	54	79	0.0256	40.02%	2.2500	14.970
80-159	1949	108.83	80	159	0.0068	10.70%	0.3300	35.792
160-319	535	226.76	160	319	0.0019	2.94%	0.1300	24.678
320-639	686	474.63	320	637	0.0024	3.77%	0.1600	26.177
640-1279	609	928.80	640	1279	0.0021	3.34%	0.1800	23.102
1280-2559	7096	1501.07	1281	2485	0.0249	38.96%	4.3500	14.965
2560-5119	49	2959.57	2759	3060	0.0002	0.27%	0.0900	81.078
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

Display filter: tcp or udp

Apply

Copy Save as... Close

CONVERSATIONS - TCP

Wireshark - Conversations - Lab3-Q2 (2).pcapng

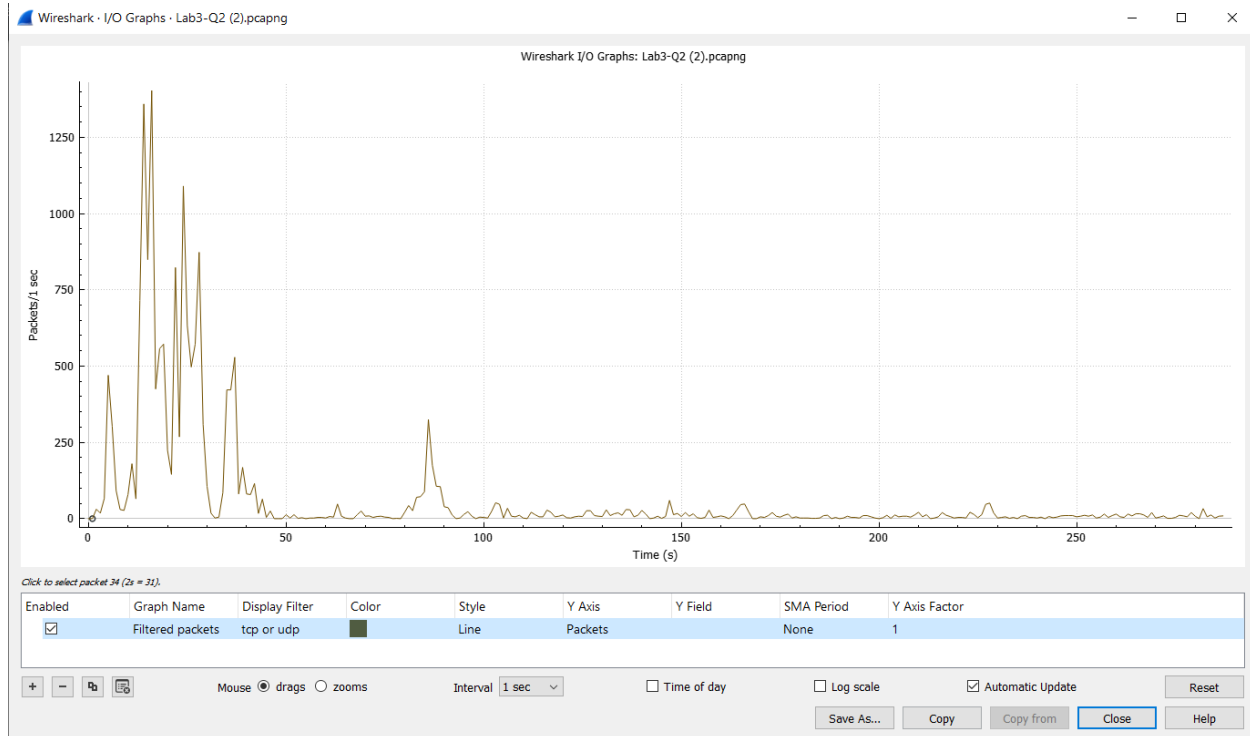
TCP - 120		UDP - 219													
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A		
10.4.8.18	50610	137.116.139.120	443	26	9826	13	2787	13	7039	2.205485	0.3827	58 k	147 k		
10.4.8.18	50611	142.250.76.205	443	71	15 k	31	5531	40	9545	4.182289	276.4751	160	276		
10.4.8.18	50612	216.170.124.200	443	211	183 k	77	6048	134	177 k	4.497732	63.6057	760	22 k		
10.4.8.18	50613	142.250.76.174	443	68	11 k	30	3430	38	7920	4.816755	259.5236	105	244		
10.4.8.18	50614	142.250.76.170	443	125	24 k	52	5168	73	19 k	5.372818	260.1008	158	607		
10.4.8.18	50615	142.250.77.40	443	79	49 k	31	2791	48	46 k	5.460585	240.2905	92	1547		
10.4.8.18	50616	103.205.143.18	443	293	228 k	112	9422	181	219 k	5.549672	30.4629	2474	57 k		
10.4.8.18	50617	82.196.1.114	443	26	9284	11	1724	15	7560	5.555903	39.0200	353	1549		
10.4.8.18	50618	172.217.166.163	443	40	7381	18	2035	22	5346	6.126857	240.4003	67	177		
10.4.8.18	50619	103.205.143.18	443	105	89 k	38	3231	67	85 k	6.138782	30.1823	856	22 k		
10.4.8.18	50620	142.250.192.35	443	405	344 k	146	10 k	259	334 k	6.139502	259.6193	308	10 k		
10.4.8.18	50621	37.159.12.153	443	26	9684	12	1826	14	8058	6.193397	19.5268	746	3301		
10.4.8.18	50622	172.217.166.37	443	111	54 k	45	6959	66	47 k	7.685107	245.6822	226	1557		
10.4.8.18	50623	74.125.68.198	5228	29	6903	14	1531	15	5372	8.667875	270.7917	45	158		
10.4.8.18	50624	142.250.183.3	443	41	11 k	18	4487	23	6610	8.885583	240.4139	149	219		
10.4.8.18	50625	172.217.166.42	443	83	16 k	36	6520	47	9902	10.861948	258.1350	202	306		
10.4.8.18	50626	172.217.166.65	443	86	57 k	34	3136	52	54 k	11.021920	240.2000	104	1812		
10.4.8.18	50627	216.58.203.3	443	220	91 k	88	7754	132	83 k	11.022091	268.1824	231	2489		
10.4.8.18	50628	142.250.192.42	443	116	15 k	48	5360	68	10 k	11.467656	265.3280	161	30		
10.4.8.18	50629	142.250.192.35	443	27	5539	13	1300	14	4239	12.377547	245.1690	42	138		
10.4.8.18	50630	172.217.166.163	443	1,198	1072 k	421	30 k	777	1041 k	12.383610	266.6657	916	31 k		
10.4.8.18	50631	172.217.174.238	443	190	94 k	75	22 k	115	72 k	12.475400	268.0954	658	2158		
10.4.8.18	50632	216.58.203.3	443	122	94 k	46	3495	76	91 k	13.446650	240.1726	116	3045		
10.4.8.18	50633	216.58.199.174	443	77	19 k	34	4770	43	14 k	13.800865	270.7700	140	429		
10.4.8.18	50634	35.244.233.98	443	2,380	2151 k	825	138 k	1,555	2012 k	14.041749	262.4346	4229	61 k		
10.4.8.18	50635	172.67.158.42	443	33	7817	17	1984	16	5833	16.043409	271.0402	58	172		
10.4.8.18	50636	142.250.192.150	443	27	5509	13	1300	14	4209	16.046660	245.1747	42	137		

CONVERSATIONS - UDP

Wireshark - Conversations - Lab3-Q2 (2).pcapng

TCP - 120		UDP - 219													
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A		
10.4.8.1	67	255.255.255.255	68	2	698	2	698	0	0	51.848121	0.0000	—	—		
10.4.8.18	64228	10.1.1.61	53	2	303	1	86	1	217	2.167155	0.0353	19 k	49 k		
10.4.8.18	64228	10.1.1.62	53	2	303	1	86	1	217	2.190227	0.0247	9211	23 k		
10.4.8.18	65073	10.1.1.61	53	2	227	1	79	1	148	3.180478	0.0007	—	—		
10.4.8.18	137	10.4.8.255	137	57	5244	57	5244	0	0	3.181517	280.4172	149	0		
10.4.8.18	5353	224.0.0.251	5353	38	2728	38	2728	0	0	3.181803	278.9071	78	0		
10.4.8.18	54792	224.0.0.252	5355	2	128	2	128	0	0	3.182767	0.4030	2540	0		
10.4.8.18	54793	239.255.255.250	1900	4	860	4	860	0	0	3.518630	3.0030	2291	0		
10.4.8.18	53249	10.1.1.61	53	2	227	1	79	1	148	3.812699	0.0006	—	—		
10.4.8.18	57120	224.0.0.252	5355	2	128	2	128	0	0	3.814462	0.4107	2493	0		
10.4.8.18	63452	10.1.1.61	53	2	174	1	79	1	95	4.178829	0.0007	—	—		
10.4.8.18	58131	10.1.1.61	53	2	190	1	80	1	110	4.179305	0.3170	2018	2775		
10.4.8.18	58131	10.1.1.62	53	2	190	1	80	1	110	4.223253	0.4986	1283	1764		
10.4.8.18	50689	10.1.1.61	53	2	201	1	83	1	118	4.814923	0.0007	—	—		
10.4.8.18	55582	10.1.1.61	53	2	227	1	79	1	148	5.124015	0.0008	—	—		
10.4.8.18	58682	224.0.0.252	5355	2	128	2	128	0	0	5.125896	0.4102	2496	0		
10.4.8.18	60912	10.1.1.61	53	2	176	1	80	1	96	5.370846	0.0008	—	—		
10.4.8.18	57812	10.1.1.61	53	2	180	1	82	1	98	5.371043	0.1782	3681	4399		
10.4.8.18	57812	10.1.1.62	53	2	180	1	82	1	98	5.402464	0.1649	3979	4755		
10.4.8.18	58465	10.1.1.61	53	2	230	1	83	1	147	5.455361	0.1001	6630	11 k		
10.4.8.18	64011	10.1.1.61	53	2	228	1	84	1	144	5.459367	0.0006	—	—		
10.4.8.18	64012	216.170.124.200	443	6	7098	6	7098	0	0	5.466922	4.0004	14 k	0		
10.4.8.18	58465	10.1.1.62	53	2	230	1	83	1	147	5.487085	0.0791	8399	14 k		
10.4.8.18	60966	10.1.1.61	53	2	206	1	77	1	129	5.620662	0.0008	—	—		
10.4.8.18	60967	142.250.192.35	443	5	6960	5	6960	0	0	5.630703	3.9995	13 k	0		
10.4.8.18	60968	103.205.143.18	443	6	7098	6	7098	0	0	5.850829	4.0013	14 k	0		
10.4.8.18	58718	10.1.1.61	53	2	194	1	89	1	105	6.125324	0.0007	—	—		
10.4.8.18	58719	103.205.143.18	443	6	7098	6	7098	0	0	6.138488	4.0015	14 k	0		
10.4.8.18	56741	10.1.1.61	53	2	202	1	77	1	125	6.152184	0.0407	15 k	24 k		
10.4.8.18	56741	10.1.1.62	53	2	202	1	77	1	125	6.183729	0.0728	8464	13 k		
10.4.8.18	49406	10.1.1.61	53	2	193	1	75	1	118	7.683625	0.0006	—	—		

I/O GRAPHS



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

Ans -

Filter applied => tcp.flags.syn and tcp.flags.ack

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.syn and tcp.flags.ack

No.	Time	Source	Destination	Protocol	Length	Info
7	18:57:32.193840	10.4.8.18	137.116.139.120	TCP	66	50610 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
8	18:57:32.194119	137.116.139.120	10.4.8.18	TCP	66	443 → 50610 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
9	18:57:32.194188	10.4.8.18	137.116.139.120	TCP	54	50610 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
10	18:57:32.196335	10.4.8.18	137.116.139.120	TLSv1.2	250	Client Hello
11	18:57:32.196613	137.116.139.120	10.4.8.18	TCP	60	443 → 50610 [ACK] Seq=1 Ack=197 Win=30336 Len=0
14	18:57:32.379240	137.116.139.120	10.4.8.18	TCP	1514	443 → 50610 [ACK] Seq=1 Ack=197 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
15	18:57:32.379277	10.4.8.18	137.116.139.120	TCP	54	50610 → 443 [ACK] Seq=197 Ack=1461 Win=262144 Len=0
16	18:57:32.379341	137.116.139.120	10.4.8.18	TCP	1514	443 → 50610 [PSH, ACK] Seq=1461 Ack=197 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
17	18:57:32.379360	10.4.8.18	137.116.139.120	TCP	54	50610 → 443 [ACK] Seq=197 Ack=2921 Win=262144 Len=0
18	18:57:32.379434	137.116.139.120	10.4.8.18	TCP	1514	443 → 50610 [ACK] Seq=2921 Ack=197 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
19	18:57:32.379450	10.4.8.18	137.116.139.120	TCP	54	50610 → 443 [ACK] Seq=197 Ack=4381 Win=262144 Len=0
20	18:57:32.379599	137.116.139.120	10.4.8.18	TLSv1.2	1254	Server Hello, Certificate, Server Key Exchange, Server Hello Done
21	18:57:32.379524	10.4.8.18	137.116.139.120	TCP	54	50610 → 443 [ACK] Seq=197 Ack=5581 Win=260864 Len=0
22	18:57:32.383875	10.4.8.18	137.116.139.120	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
23	18:57:32.384129	137.116.139.120	10.4.8.18	TCP	60	443 → 50610 [ACK] Seq=5581 Ack=355 Win=31360 Len=0
24	18:57:32.475968	137.116.139.120	10.4.8.18	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
25	18:57:32.476010	10.4.8.18	137.116.139.120	TCP	54	50610 → 443 [ACK] Seq=355 Ack=5632 Win=260864 Len=0
26	18:57:32.482683	10.4.8.18	137.116.139.120	TLSv1.2	522	Application Data
27	18:57:32.482649	10.4.8.18	137.116.139.120	TLSv1.2	1305	Application Data
28	18:57:32.482809	137.116.139.120	10.4.8.18	TCP	60	443 → 50610 [ACK] Seq=5632 Ack=823 Win=32512 Len=0
29	18:57:32.483096	137.116.139.120	10.4.8.18	TCP	60	443 → 50610 [ACK] Seq=5632 Ack=2074 Win=34944 Len=0
30	18:57:32.576235	137.116.139.120	10.4.8.18	TLSv1.2	712	Application Data

< >

> Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AA80D8657}, id 0
> Ethernet II, Src: LCFHeFe_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: 137.116.139.120
> Transmission Control Protocol, Src Port: 50610, Dst Port: 443, Seq: 0, Len: 0

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

Ans -

Filter applied => tcp.dstport == 80 || udp.dstport == 80

No.	Time	Source	Destination	Protocol	Length	Info
14601	18:58:10.596818	10.4.8.18	172.217.166.46	TCP	54	50608 → 80 [FIN, ACK] Seq=1 Ack=1 Win=4106 Len=0
14602	18:58:10.597013	10.4.8.18	172.217.166.46	TCP	66	50698 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
14604	18:58:10.597119	10.4.8.18	172.217.166.46	TCP	54	50608 → 80 [ACK] Seq=2 Ack=2 Win=4106 Len=0
14606	18:58:10.597304	10.4.8.18	172.217.166.46	TCP	54	50698 → 80 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
14607	18:58:10.605111	10.4.8.18	172.217.166.46	HTTP	358	GET /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.253.200/dCwC1xKjU5RSOUZ52LSQXQ HT
14619	18:58:10.748667	10.4.8.18	49.44.83.143	TCP	54	50609 → 80 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
14620	18:58:10.748950	10.4.8.18	49.44.83.143	TCP	66	50699 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
14622	18:58:10.749023	10.4.8.18	49.44.83.143	TCP	54	50609 → 80 [ACK] Seq=2 Ack=2 Win=513 Len=0
14624	18:58:10.749207	10.4.8.18	49.44.83.143	TCP	54	50699 → 80 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
14625	18:58:10.749730	10.4.8.18	49.44.83.143	HTTP	484	GET /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.253.200/dCwC1xKjU5RSOUZ52LSQXQ?cm
14627	18:58:10.788276	10.4.8.18	172.217.166.46	TCP	54	50698 → 80 [ACK] Seq=305 Ack=1115 Win=1049856 Len=0
14629	18:58:10.814373	10.4.8.18	172.217.166.46	HTTP	338	HEAD /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.253.200/dCwC1xKjU5RSOUZ52LSQXQ H
14631	18:58:10.853555	10.4.8.18	49.44.83.143	TCP	54	50699 → 80 [ACK] Seq=431 Ack=658 Win=1058368 Len=0
14633	18:58:10.916725	10.4.8.18	49.44.83.143	HTTP	464	HEAD /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.253.200/dCwC1xKjU5RSOUZ52LSQXQ?c
14635	18:58:10.957176	10.4.8.18	172.217.166.46	TCP	54	50698 → 80 [ACK] Seq=589 Ack=1728 Win=1051136 Len=0
14637	18:58:11.019258	10.4.8.18	172.217.166.46	HTTP	358	GET /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.253.200/dCwC1xKjU5RSOUZ52LSQXQ HT
14643	18:58:11.059444	10.4.8.18	49.44.83.143	TCP	54	50699 → 80 [ACK] Seq=841 Ack=1293 Win=1049856 Len=0
14657	18:58:11.125763	10.4.8.18	49.44.83.143	HTTP	484	GET /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.253.200/dCwC1xKjU5RSOUZ52LSQXQ?cm
14663	18:58:11.164079	10.4.8.18	172.217.166.46	TCP	54	50698 → 80 [ACK] Seq=893 Ack=2842 Win=1049856 Len=0
14665	18:58:11.173746	10.4.8.18	172.217.166.46	HTTP	338	HEAD /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.253.200/dCwC1xKjU5RSOUZ52LSQXQ H
14667	18:58:11.213658	10.4.8.18	49.44.83.143	TCP	54	50699 → 80 [ACK] Seq=1271 Ack=1950 Win=1051136 Len=0
14669	18:58:11.277241	10.4.8.18	49.44.83.143	HTTP	464	HEAD /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.253.200/dCwC1xKjU5RSOUZ52LSQXQ?c

> Frame 14601: 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: LCFHeFe_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: 50608, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

f. List out the ARP packets.

Ans -

Filter applied => arp

No.	Time	Source	Destination	Protocol	Length	Info
129	18:57:35.064012	AugmentI_ce:87:01	Broadcast	ARP	60	who has 10.20.0.1? Tell 10.4.8.21
136	18:57:35.068952	AugmentI_ce:87:01	Broadcast	ARP	60	who has 10.4.8.1? Tell 10.4.8.21
137	18:57:35.069133	AugmentI_ce:87:01	Broadcast	ARP	60	who has 10.4.8.1? Tell 10.4.8.21
992	18:57:38.194242	Cisco_34:14:0e	Cisco_49:b0:99	ARP	60	10.4.8.47 is at 00:17:e0:34:14:0e
2127	18:57:44.070653	Cisco_49:b0:99	LANBitCo_1b:ba:01	ARP	60	who has 10.4.8.12? Tell 0.0.0.0
7541	18:57:51.615444	Cisco_49:b4:1b	LCFHeFe_41:a3:c8	ARP	60	who has 10.4.8.18? Tell 0.0.0.0
7542	18:57:51.615456	LCFHeFe_41:a3:c8	Cisco_49:b4:1b	ARP	42	10.4.8.18 is at 28:d2:44:41:a3:c8
12937	18:58:05.035518	Cisco_5a:ab:40	LCFHeFe_41:a3:c8	ARP	60	who has 10.4.8.18? Tell 10.4.8.1
12938	18:58:05.035518	Cisco_5a:ab:40	HewlettP_e6:31:93	ARP	60	who has 10.4.8.13? Tell 10.4.8.1
12939	18:58:05.035534	LCFHeFe_41:a3:c8	Cisco_5a:ab:40	ARP	42	10.4.8.18 is at 28:d2:44:41:a3:c8
14945	18:58:18.350939	LANBitCo_1b:ba:01	Cisco_49:b0:99	ARP	60	10.4.8.12 is at 00:e0:8d:1b:ba:01
14960	18:58:20.849004	Cisco_49:b0:99	LCFHeFe_41:a3:c8	ARP	60	who has 10.4.8.18? Tell 0.0.0.0
14961	18:58:20.849032	LCFHeFe_41:a3:c8	Cisco_49:b0:99	ARP	42	10.4.8.18 is at 28:d2:44:41:a3:c8
14962	18:58:20.976936	Cisco_49:b4:1b	LCFHeFe_41:a3:c8	ARP	60	who has 10.4.8.18? Tell 0.0.0.0
14963	18:58:20.976976	LCFHeFe_41:a3:c8	Cisco_49:b4:1b	ARP	42	10.4.8.18 is at 28:d2:44:41:a3:c8
15073	18:58:34.957658	LCFHeFe_41:a3:c8	Broadcast	ARP	42	who has 10.4.8.1? Tell 10.4.8.18
15074	18:58:34.959043	Cisco_5a:ab:40	LCFHeFe_41:a3:c8	ARP	60	10.4.8.1 is at 28:6f:7f:5a:ab:40
15075	18:58:34.968015	LCFHeFe_41:a3:c8	Broadcast	ARP	42	who has 10.4.8.1? Tell 10.4.8.18
15076	18:58:34.968453	Cisco_5a:ab:40	LCFHeFe_41:a3:c8	ARP	60	10.4.8.1 is at 28:6f:7f:5a:ab:40
15077	18:58:34.978277	LCFHeFe_41:a3:c8	Broadcast	ARP	42	who has 10.4.8.1? Tell 10.4.8.18
15078	18:58:34.978719	Cisco_5a:ab:40	LCFHeFe_41:a3:c8	ARP	60	10.4.8.1 is at 28:6f:7f:5a:ab:40
15079	18:58:34.993594	LCFHeFe_41:a3:c8	Broadcast	ARP	42	who has 10.4.8.2? Tell 10.4.8.18

> Frame 12939: 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_5a:ab:40 (28:6f:7f:5a:ab:40)
> Address Resolution Protocol (reply)