

Computer Networks Lab 3

Name: Vaibhav Chaudhari

ID: 2017B5A70834G

Q1. Customize your Wireshark

The screenshot shows the Wireshark interface with the Lab3-Q2.pcapng file loaded. The packet list pane displays a series of packets, with the selected packet (No. 19672) showing details in the packet details pane. The packet details pane shows the following information:

- Frame 19672: 60 bytes on wire (480 bits) captured (480 bits) on interface 'DeviceNPF_{B097628C-6220-4299-BAD8-5D9AAB006657}', 14.9
- IEEE 802.3 Ethernet
- Logical-link control
- Spanning Tree Protocol

The packet details pane also shows the following information:

- Destination: 10.1.1.1
- Source: 10.1.1.1
- Type: 0x0000
- Standard query response 0x15e7 A www.netscantools.com A 216.1

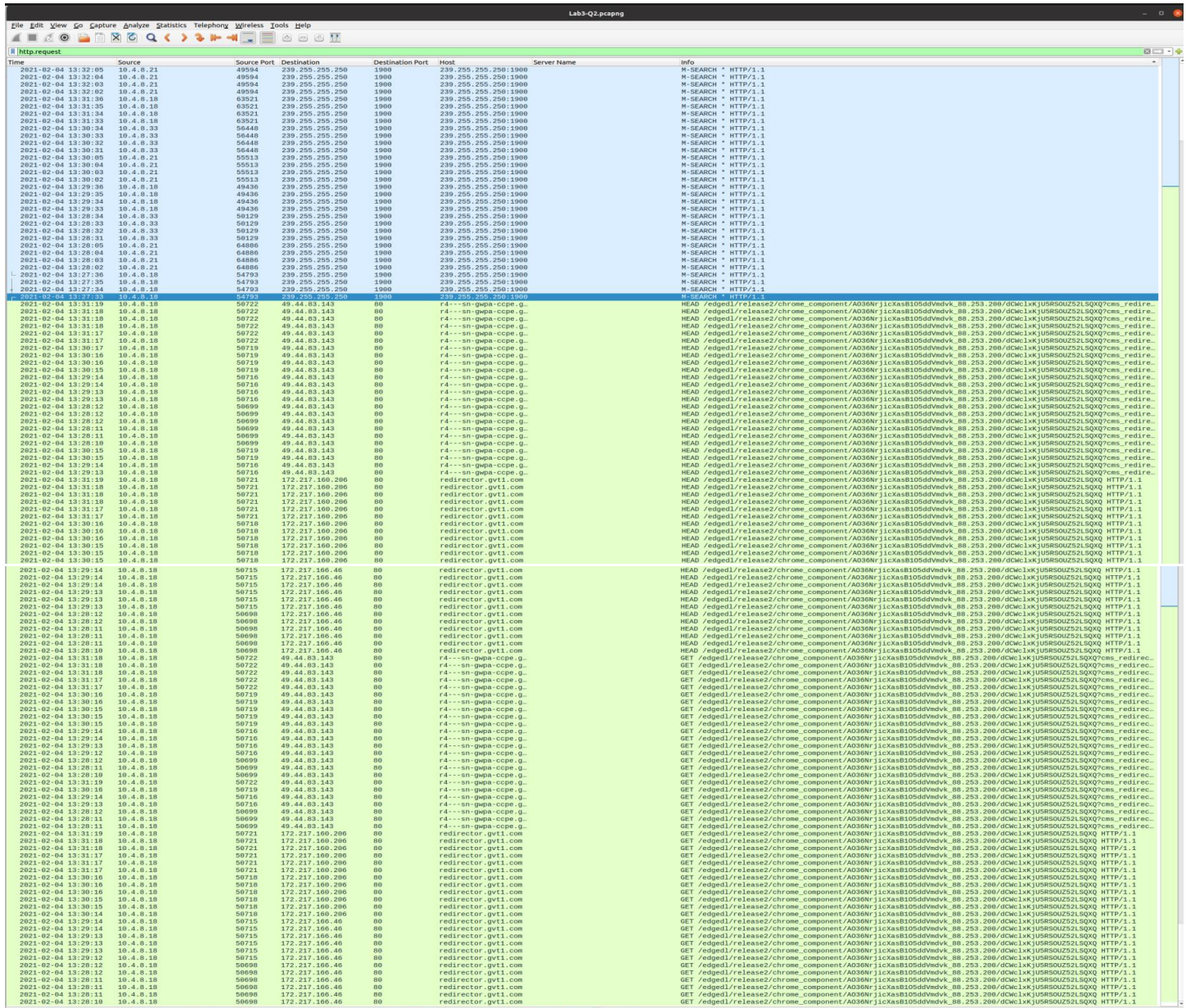
The preferences were set as follows:

The screenshot shows the Wireshark Preferences dialog box with the Appearance tab selected. The following preferences are shown:

- Columns: ☒ Displayed, ☒ Title, ☒ Type, ☒ Fields, ☒ Field Occurrence
- Font and Colors: ☒ Layout
- Capture: ☒ Expert
- Filter Buttons: ☒ Name Resolution
- Protocols: ☒ RSA Keys
- Statistics: ☒ Advanced

The packet list pane shows the following information:

- Time: 0.000000
- Source: 10.1.1.1
- Destination: 10.1.1.1
- Type: 0x0000
- Standard query response 0x15e7 A www.netscantools.com A 216.1



b. Identify the http response packet

The image shows a Wireshark packet capture of a network traffic. The filter applied is **http.response**. The packet list shows a series of HTTP responses, mostly 200 OK, with some 404 Not Found and 500 Internal Server Error. The selected packet is a 200 OK response from 10.4.8.10 to 10.4.8.10.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
2	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
3	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
4	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
5	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
6	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
7	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
8	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
9	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
10	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
11	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
12	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
13	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
14	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
15	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
16	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
17	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
18	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
19	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
20	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
21	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
22	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
23	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
24	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
25	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
26	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
27	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
28	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
29	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
30	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
31	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
32	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
33	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
34	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
35	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
36	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
37	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
38	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
39	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
40	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
41	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
42	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
43	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
44	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
45	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
46	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
47	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
48	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
49	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
50	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
51	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
52	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
53	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
54	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
55	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
56	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
57	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
58	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
59	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
60	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
61	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
62	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
63	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
64	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
65	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
66	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
67	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
68	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
69	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
70	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
71	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
72	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
73	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
74	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
75	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
76	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
77	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
78	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
79	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
80	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
81	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
82	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
83	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
84	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
85	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
86	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
87	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
88	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
89	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
90	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
91	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
92	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
93	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
94	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
95	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
96	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
97	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
98	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
99	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK
100	0.000000	10.4.8.10	10.4.8.10	HTTP	140	200 OK

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

The image shows the Wireshark Protocol Hierarchy Statistics for Lab3-Q2.pcapng. The statistics are displayed in a table format, showing the percentage of packets, the number of packets, and the percentage of bytes for each protocol.

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.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Lab-Q2.pcapng

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

100%

Time	Source	Destination	Host	Server Name	Info
2021-02-04 13:31:17	49.44.83.143	80	10.4.0.18	50722	80 -> 50722 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:31:17	172.217.166.296	80	10.4.0.18	50721	80 -> 50721 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:30:15	49.44.83.143	80	10.4.0.18	50719	80 -> 50719 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:30:14	172.217.166.296	80	10.4.0.18	50718	80 -> 50718 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:29:12	49.44.83.143	80	10.4.0.18	50710	80 -> 50710 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:29:12	172.217.166.296	80	10.4.0.18	50715	80 -> 50715 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:29:12	172.217.166.296	80	10.4.0.18	50699	80 -> 50699 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:29:12	172.217.166.296	80	10.4.0.18	50698	80 -> 50698 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:31:14	172.217.166.296	80	10.4.0.18	50722	80 -> 50722 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:31:14	172.217.166.296	80	10.4.0.18	50721	80 -> 50721 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:31:10	172.217.166.296	80	10.4.0.18	50720	80 -> 50720 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:31:00	172.217.166.296	80	10.4.0.18	50723	80 -> 50723 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:31:00	172.217.166.296	80	10.4.0.18	50724	80 -> 50724 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50713	80 -> 50713 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50712	80 -> 50712 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50711	80 -> 50711 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50710	80 -> 50710 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50709	80 -> 50709 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50708	80 -> 50708 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50707	80 -> 50707 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50706	80 -> 50706 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50705	80 -> 50705 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50704	80 -> 50704 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50703	80 -> 50703 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50702	80 -> 50702 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50701	80 -> 50701 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50700	80 -> 50700 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50699	80 -> 50699 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50698	80 -> 50698 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50697	80 -> 50697 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50696	80 -> 50696 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50695	80 -> 50695 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50694	80 -> 50694 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50693	80 -> 50693 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50692	80 -> 50692 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:28:59	172.217.166.296	80	10.4.0.18	50691	80 -> 50691 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:59	44.235.68.102	443	10.4.0.18	50689	443 -> 50689 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:59	44.235.68.102	443	10.4.0.18	50688	443 -> 50688 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:59	52.205.211.154	443	10.4.0.18	50687	443 -> 50687 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:59	52.205.211.154	443	10.4.0.18	50686	443 -> 50686 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:59	54.86.144.171	443	10.4.0.18	50685	443 -> 50685 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:59	34.107.195.226	443	10.4.0.18	50684	443 -> 50684 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:57	44.206.145.71	443	10.4.0.18	50683	443 -> 50683 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:56	92.55.161.123	443	10.4.0.18	50682	443 -> 50682 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:56	92.241.24.90	443	10.4.0.18	50681	443 -> 50681 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:56	92.241.24.90	443	10.4.0.18	50680	443 -> 50680 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:56	172.217.166.163	443	10.4.0.18	50679	443 -> 50679 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:55	54.85.126.56	443	10.4.0.18	50678	443 -> 50678 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:55	54.85.126.56	443	10.4.0.18	50677	443 -> 50677 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:55	54.85.126.56	443	10.4.0.18	50676	443 -> 50676 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:55	54.85.126.56	443	10.4.0.18	50675	443 -> 50675 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:55	54.85.126.56	443	10.4.0.18	50674	443 -> 50674 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:54	13.248.232.99	443	10.4.0.18	50673	443 -> 50673 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:54	13.248.232.2	443	10.4.0.18	50672	443 -> 50672 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:54	54.86.79.244	443	10.4.0.18	50671	443 -> 50671 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:54	34.235.68.102	443	10.4.0.18	50670	443 -> 50670 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:54	34.206.145.71	443	10.4.0.18	50669	443 -> 50669 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:54	52.55.161.123	443	10.4.0.18	50668	443 -> 50668 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:54	35.231.223.125	443	10.4.0.18	50667	443 -> 50667 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:53	52.292.127.13	443	10.4.0.18	50666	443 -> 50666 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:53	13.248.232.99	443	10.4.0.18	50665	443 -> 50665 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:52	89.187.162.58	443	10.4.0.18	50664	443 -> 50664 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:58	89.187.162.58	443	10.4.0.18	50663	443 -> 50663 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:58	89.187.162.58	443	10.4.0.18	50662	443 -> 50662 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:58	89.187.162.58	443	10.4.0.18	50661	443 -> 50661 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:58	89.187.162.58	443	10.4.0.18	50660	443 -> 50660 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:58	89.187.162.58	443	10.4.0.18	50659	443 -> 50659 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:48	142.250.183.42	443	10.4.0.18	50658	443 -> 50658 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:48	142.250.183.42	443	10.4.0.18	50657	443 -> 50657 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:48	142.250.183.42	443	10.4.0.18	50656	443 -> 50656 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:48	142.250.183.42	443	10.4.0.18	50655	443 -> 50655 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:48	142.250.183.42	443	10.4.0.18	50654	443 -> 50654 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:47	142.250.183.39	443	10.4.0.18	50653	443 -> 50653 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:47	142.250.183.39	443	10.4.0.18	50652	443 -> 50652 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:46	176.10.216.155	443	10.4.0.18	50651	443 -> 50651 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:46	176.10.216.155	443	10.4.0.18	50650	443 -> 50650 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:46	176.10.216.155	443	10.4.0.18	50649	443 -> 50649 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:46	176.10.216.155	443	10.4.0.18	50648	443 -> 50648 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:46	176.10.216.155	443	10.4.0.18	50647	443 -> 50647 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:46	176.10.216.155	443	10.4.0.18	50646	443 -> 50646 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:45	176.10.216.155	443	10.4.0.18	50645	443 -> 50645 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:45	176.10.216.155	443	10.4.0.18	50644	443 -> 50644 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:45	176.10.216.155	443	10.4.0.18	50643	443 -> 50643 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:44	176.10.216.155	443	10.4.0.18	50642	443 -> 50642 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:44	176.10.216.155	443	10.4.0.18	50641	443 -> 50641 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:44	176.10.216.155	443	10.4.0.18	50640	443 -> 50640 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:44	176.10.216.155	443	10.4.0.18	50639	443 -> 50639 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:44	176.10.216.155	443	10.4.0.18	50638	443 -> 50638 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:44	176.10.216.155	443	10.4.0.18	50637	443 -> 50637 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:44	176.10.216.155	443	10.4.0.18	50636	443 -> 50636 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2021-02-04 13:27:44	176.10.216.155	443	10.4.0.18	50635	443 -> 50635 [SYN, ACK] Seq=0 Ack=1 Win=29

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

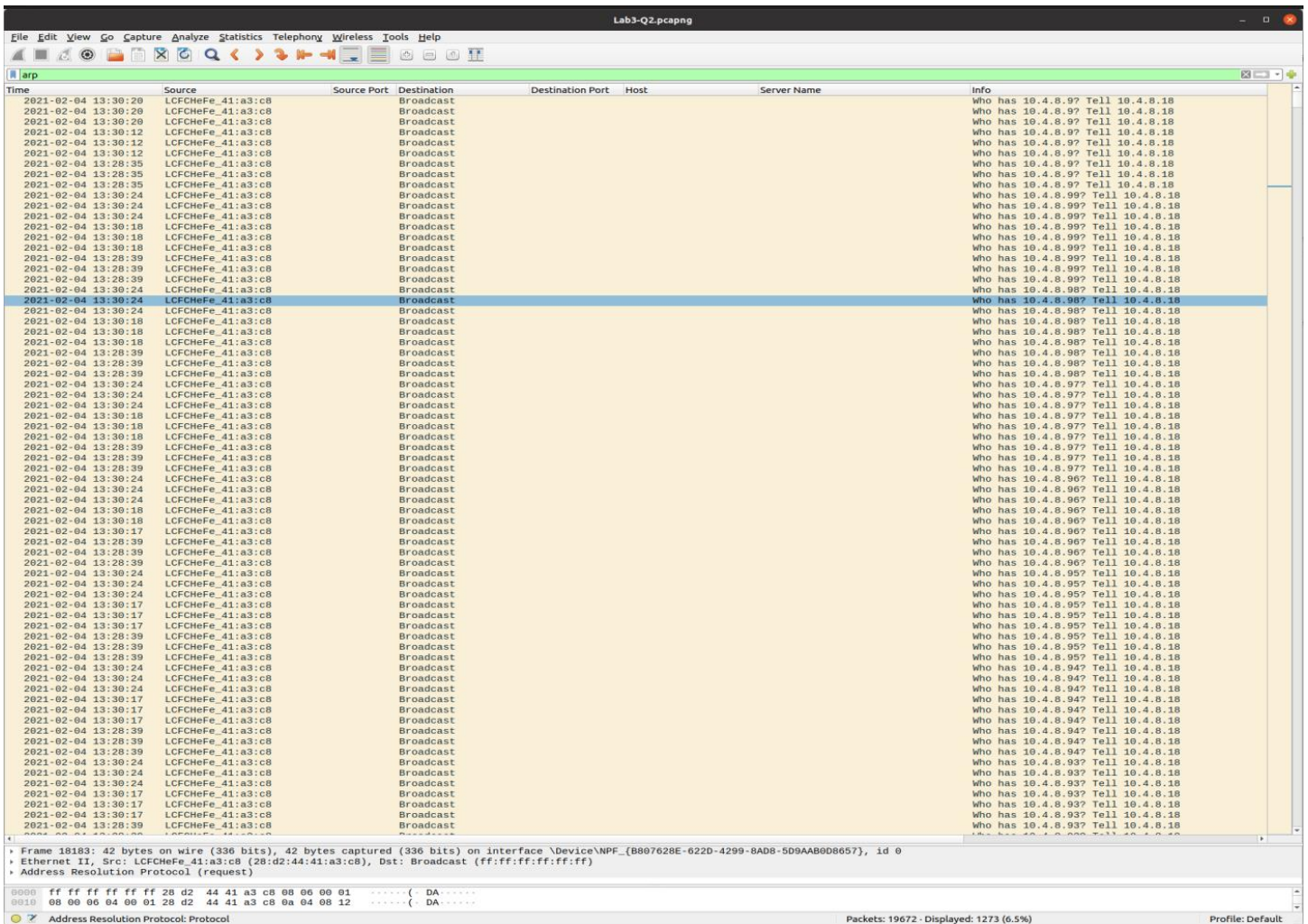
For the flags to be on, they have to be set to 1 so we check all the tcp packets whose syn. and ack. flags are set to 1.

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

[illegible]

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.



Time	Source	Source Port	Destination	Destination Port	Host	Server Name	Info
2021-02-04 13:30:20	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.97 Tell 10.4.8.18
2021-02-04 13:30:20	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.97 Tell 10.4.8.18
2021-02-04 13:30:20	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.97 Tell 10.4.8.18
2021-02-04 13:30:12	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.97 Tell 10.4.8.18
2021-02-04 13:30:12	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.97 Tell 10.4.8.18
2021-02-04 13:30:12	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.97 Tell 10.4.8.18
2021-02-04 13:28:35	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.97 Tell 10.4.8.18
2021-02-04 13:28:35	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.97 Tell 10.4.8.18
2021-02-04 13:30:24	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.997 Tell 10.4.8.18
2021-02-04 13:30:24	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.997 Tell 10.4.8.18
2021-02-04 13:30:18	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.997 Tell 10.4.8.18
2021-02-04 13:30:18	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.997 Tell 10.4.8.18
2021-02-04 13:28:39	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.997 Tell 10.4.8.18
2021-02-04 13:28:39	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.997 Tell 10.4.8.18
2021-02-04 13:28:39	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.997 Tell 10.4.8.18
2021-02-04 13:30:24	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.987 Tell 10.4.8.18
2021-02-04 13:30:24	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.987 Tell 10.4.8.18
2021-02-04 13:30:18	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.987 Tell 10.4.8.18
2021-02-04 13:30:18	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.987 Tell 10.4.8.18
2021-02-04 13:28:39	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.987 Tell 10.4.8.18
2021-02-04 13:28:39	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.987 Tell 10.4.8.18
2021-02-04 13:30:24	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.977 Tell 10.4.8.18
2021-02-04 13:30:24	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.977 Tell 10.4.8.18
2021-02-04 13:30:24	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.977 Tell 10.4.8.18
2021-02-04 13:30:18	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.977 Tell 10.4.8.18
2021-02-04 13:30:18	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.977 Tell 10.4.8.18
2021-02-04 13:28:39	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.977 Tell 10.4.8.18
2021-02-04 13:28:39	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.977 Tell 10.4.8.18
2021-02-04 13:28:39	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.977 Tell 10.4.8.18
2021-02-04 13:30:24	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.967 Tell 10.4.8.18
2021-02-04 13:30:24	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.967 Tell 10.4.8.18
2021-02-04 13:30:18	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.967 Tell 10.4.8.18
2021-02-04 13:30:17	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.967 Tell 10.4.8.18
2021-02-04 13:28:39	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.967 Tell 10.4.8.18
2021-02-04 13:28:39	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.967 Tell 10.4.8.18
2021-02-04 13:28:39	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.967 Tell 10.4.8.18
2021-02-04 13:30:24	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.957 Tell 10.4.8.18
2021-02-04 13:30:24	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.957 Tell 10.4.8.18
2021-02-04 13:30:17	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.957 Tell 10.4.8.18
2021-02-04 13:30:17	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.957 Tell 10.4.8.18
2021-02-04 13:28:39	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.957 Tell 10.4.8.18
2021-02-04 13:28:39	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.957 Tell 10.4.8.18
2021-02-04 13:30:24	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.947 Tell 10.4.8.18
2021-02-04 13:30:24	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.947 Tell 10.4.8.18
2021-02-04 13:30:17	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.947 Tell 10.4.8.18
2021-02-04 13:30:17	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.947 Tell 10.4.8.18
2021-02-04 13:28:39	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.947 Tell 10.4.8.18
2021-02-04 13:28:39	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.947 Tell 10.4.8.18
2021-02-04 13:30:24	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.937 Tell 10.4.8.18
2021-02-04 13:30:24	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.937 Tell 10.4.8.18
2021-02-04 13:30:17	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.937 Tell 10.4.8.18
2021-02-04 13:30:17	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.937 Tell 10.4.8.18
2021-02-04 13:28:39	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.937 Tell 10.4.8.18
2021-02-04 13:28:39	LCfCHeFe_41:a3:c8		Broadcast				who has 10.4.8.937 Tell 10.4.8.18

Frame 18183: 42 bytes captured (336 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9AAB8D8657}, id 0
Ethernet II, Src: LCfCHeFe_41:a3:c8 (28:d2:44:41:a3:c8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

0000 ff ff ff ff ff ff 28 d2 44 41 a3 c8 08 06 00 01(DA.....
0010 08 00 06 04 00 01 28 d2 44 41 a3 c8 0a 04 08 12(DA.....

Address Resolution Protocol: Protocol

Packets: 19672 - Displayed: 1273 (6.5%)

Profile: Default

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.