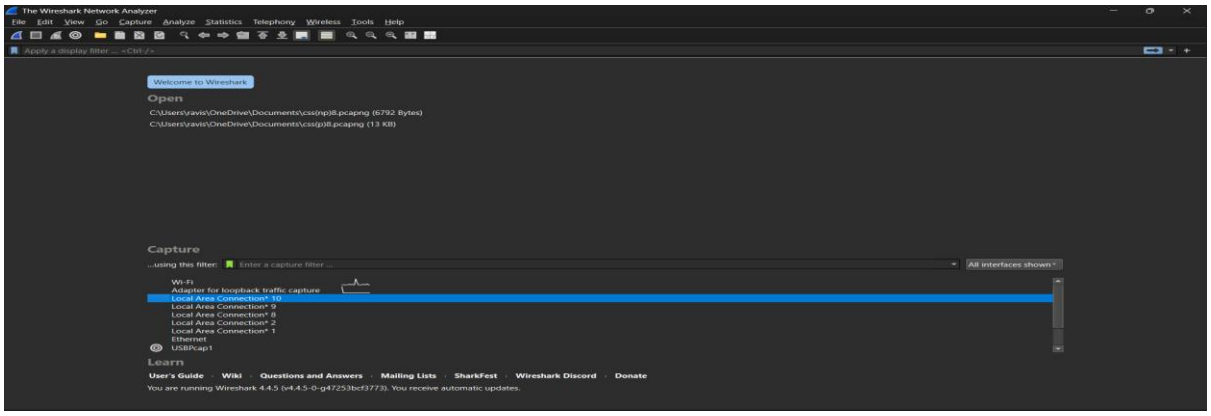
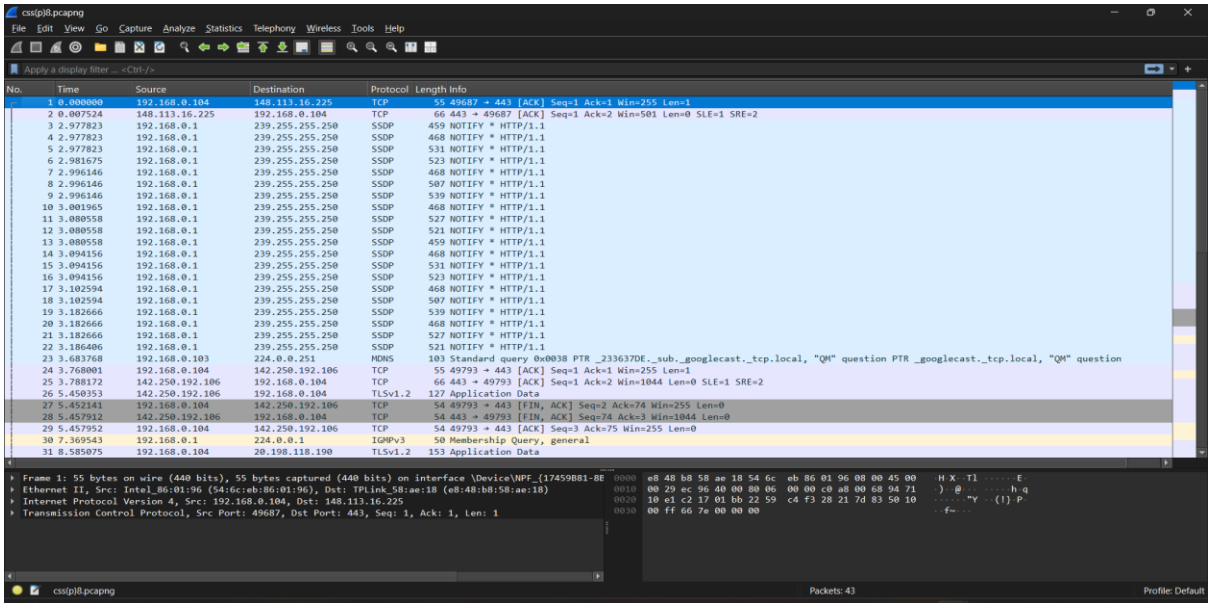
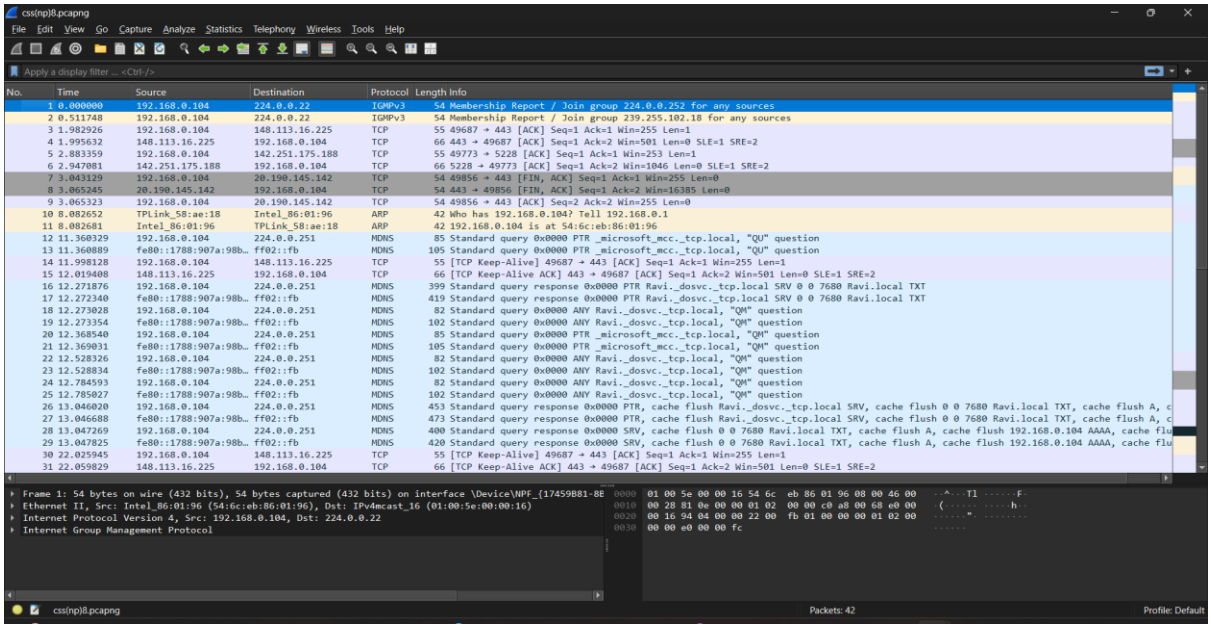
#CSS-8 for wireshark

1]WireShark display interface:-

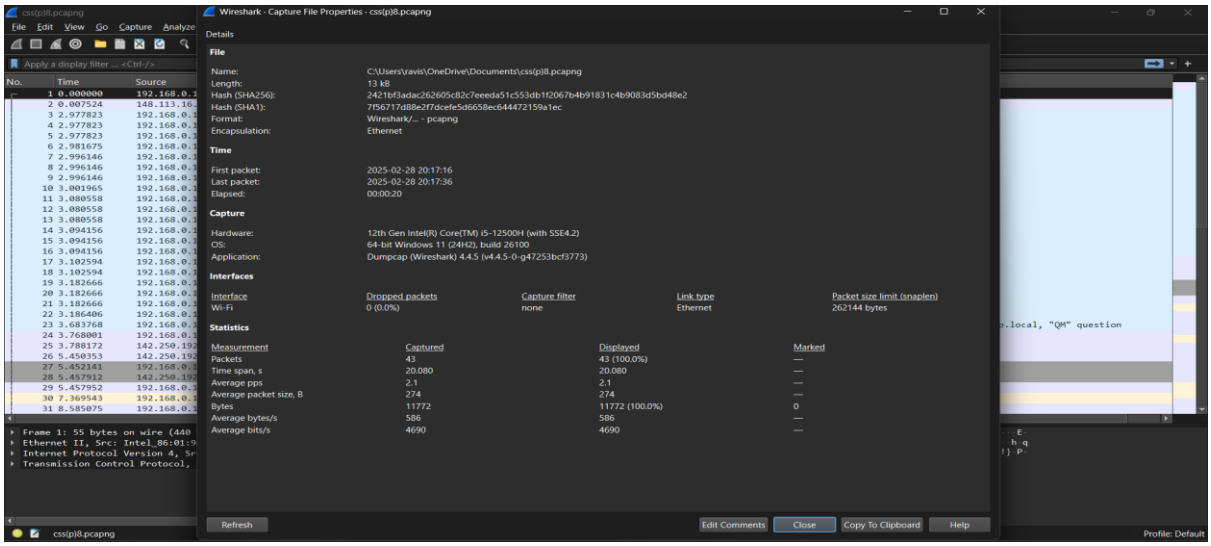


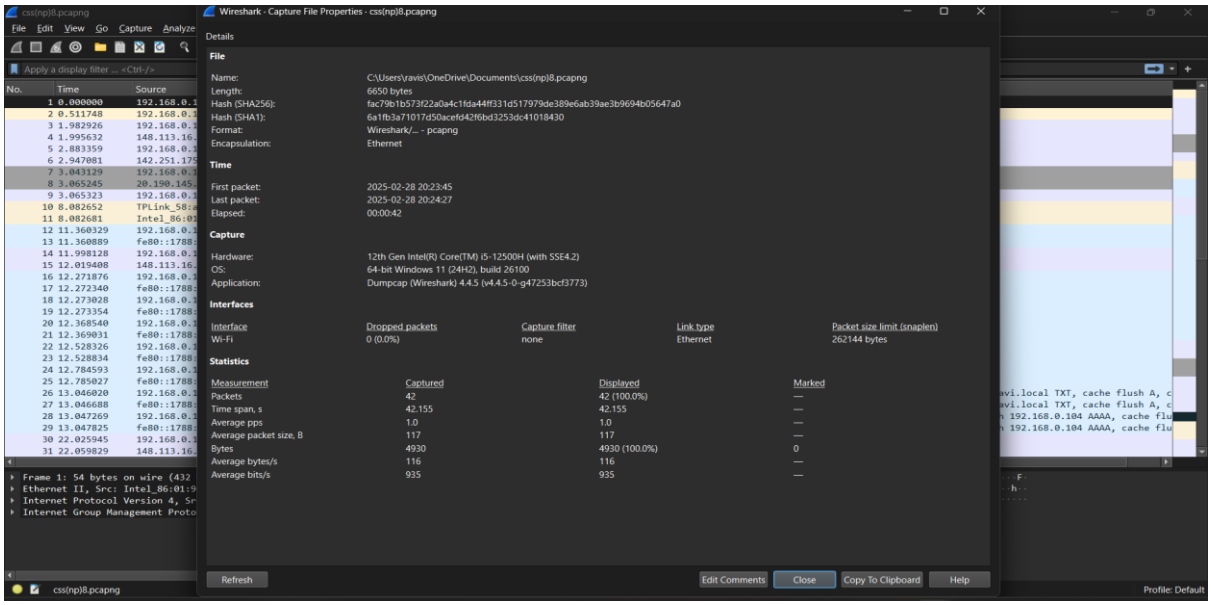
2] Observing Performance in Promiscuous and Non-Promiscuous Mode:-



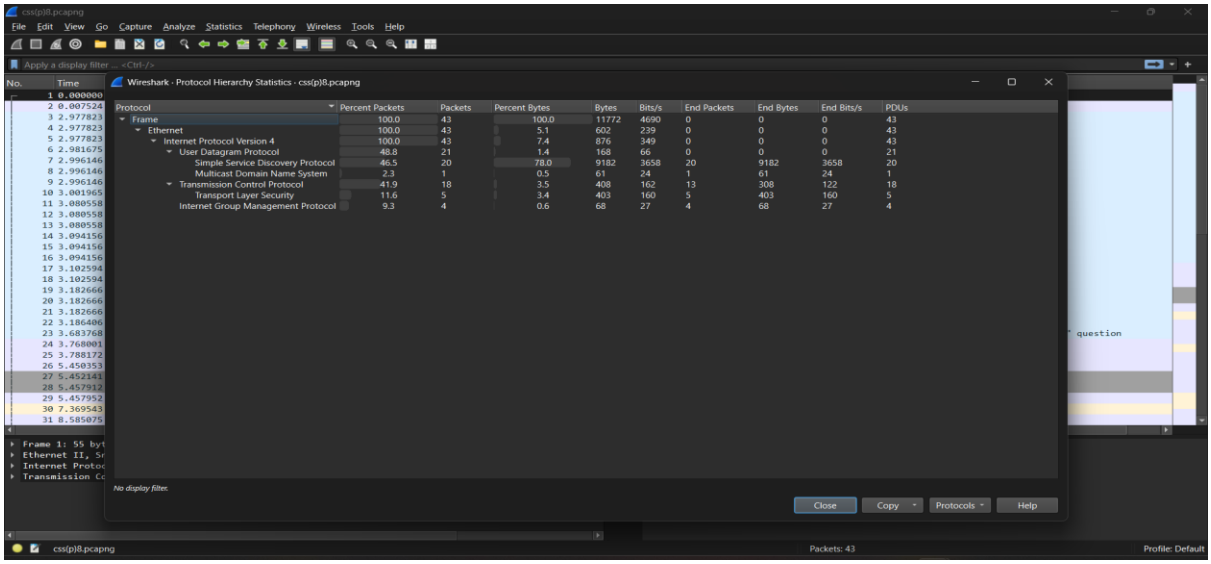


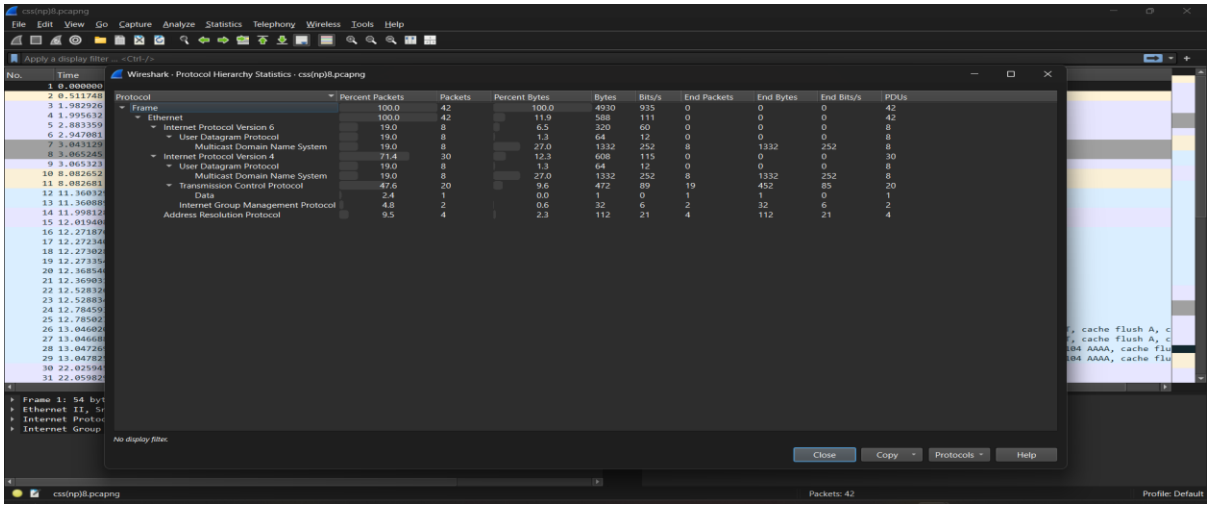
3] Compare Promiscuous vs. Non-Promiscuous Mode:-



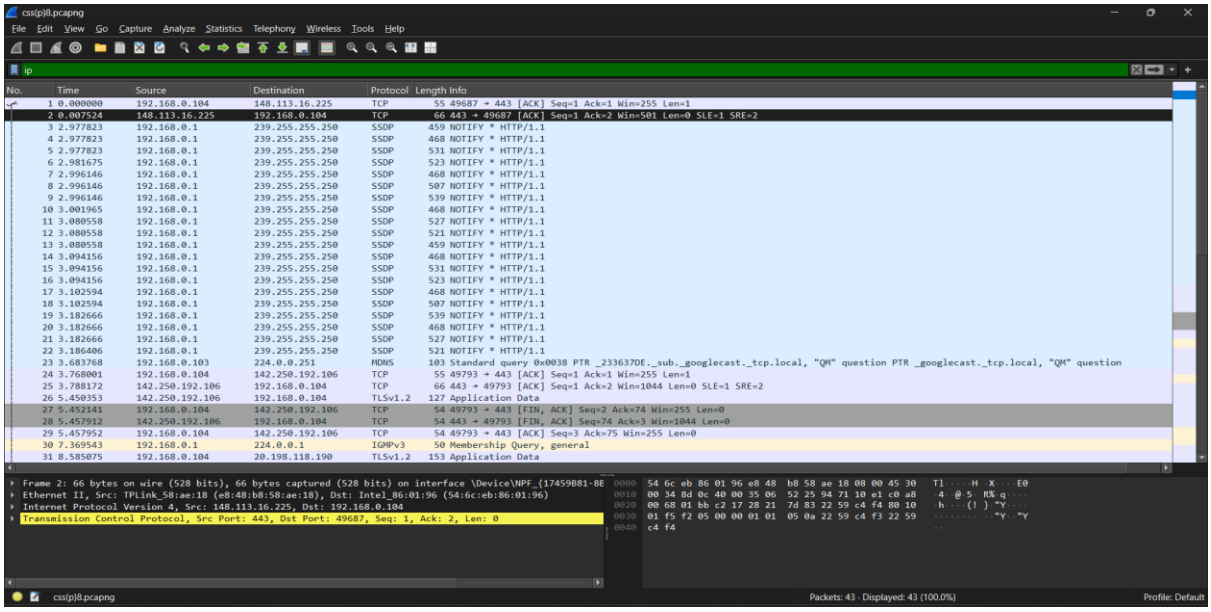


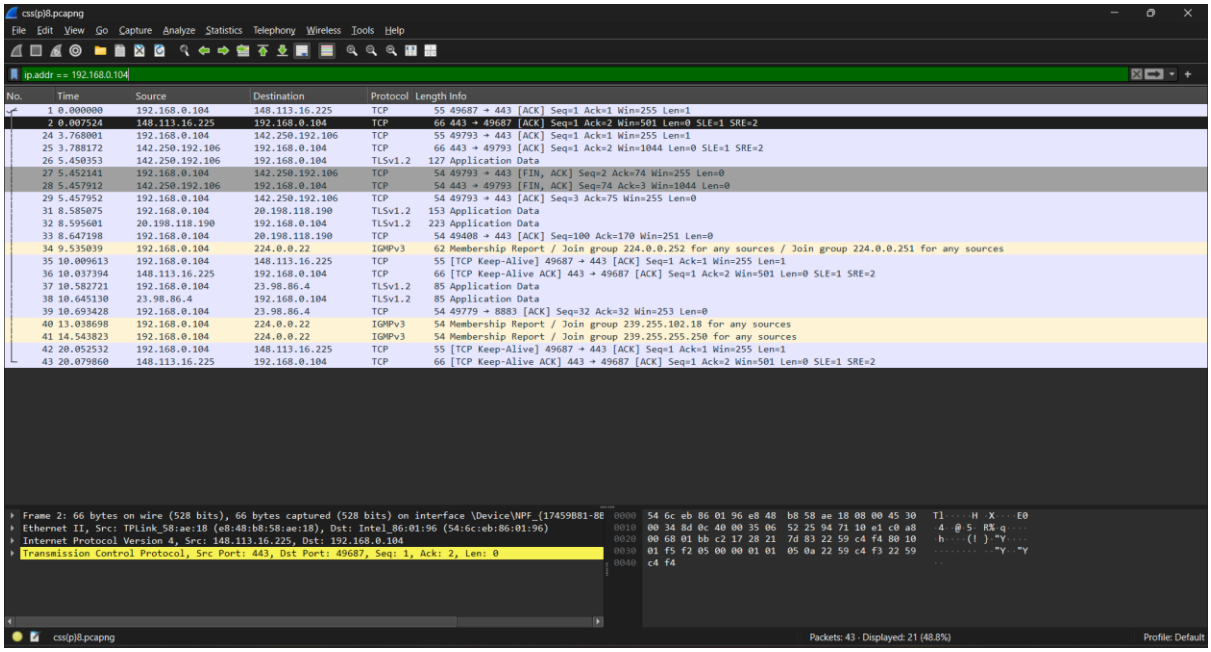
4] Protocol Hierarchy Statistics for Promiscuous vs. Non-Promiscuous Mode:-

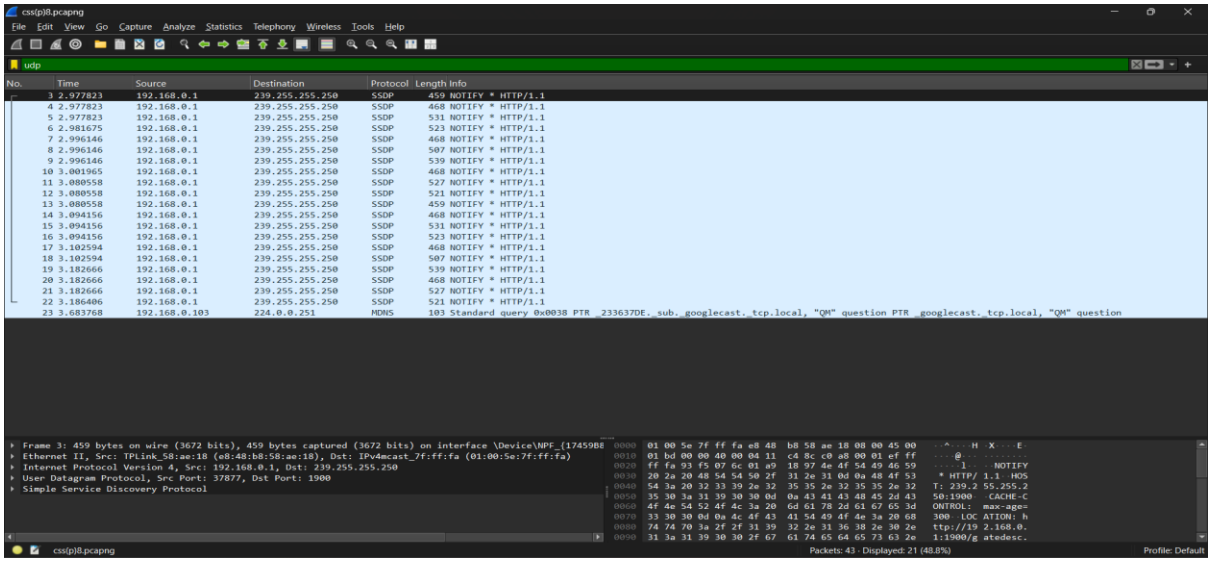


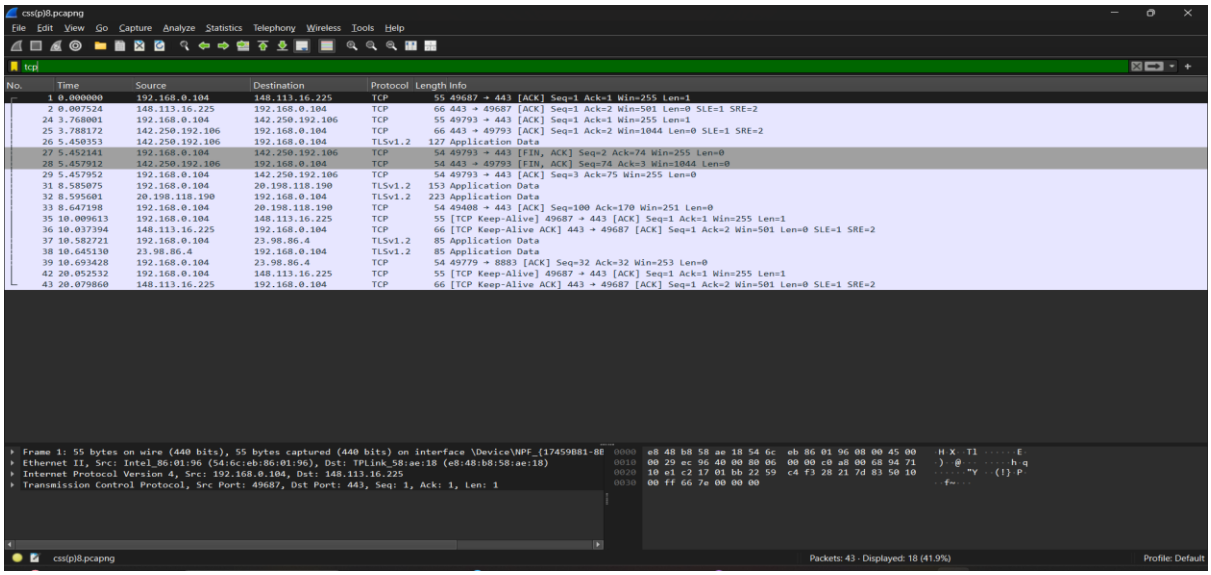


5] Commands to Run in Both (p and np) based on different filters:-

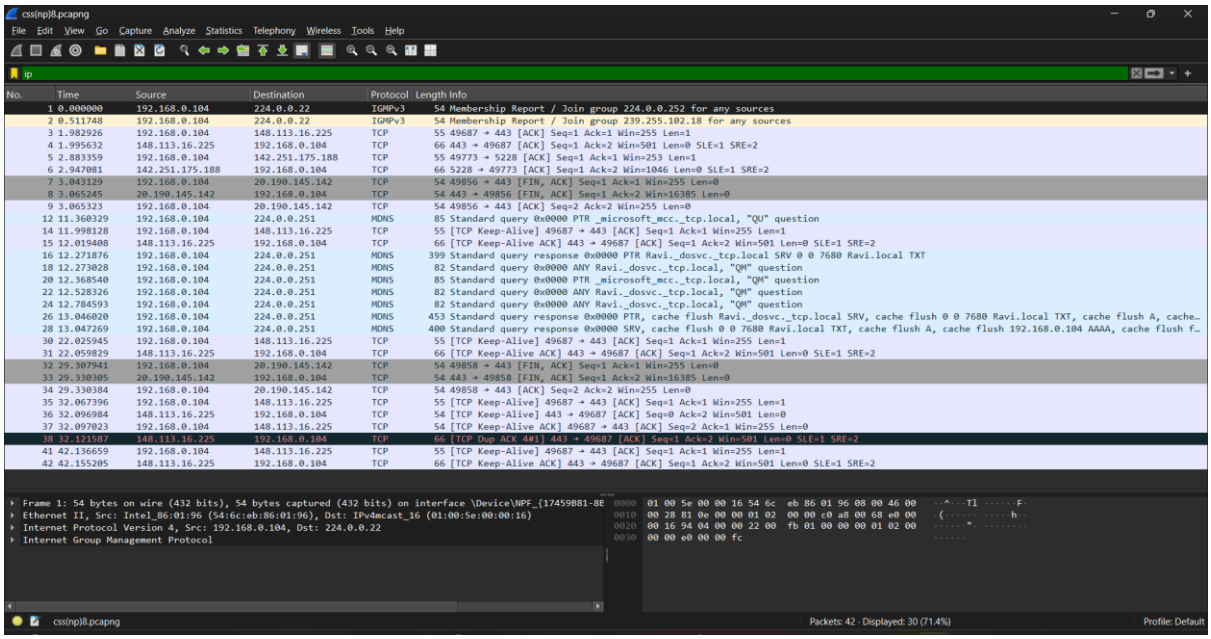


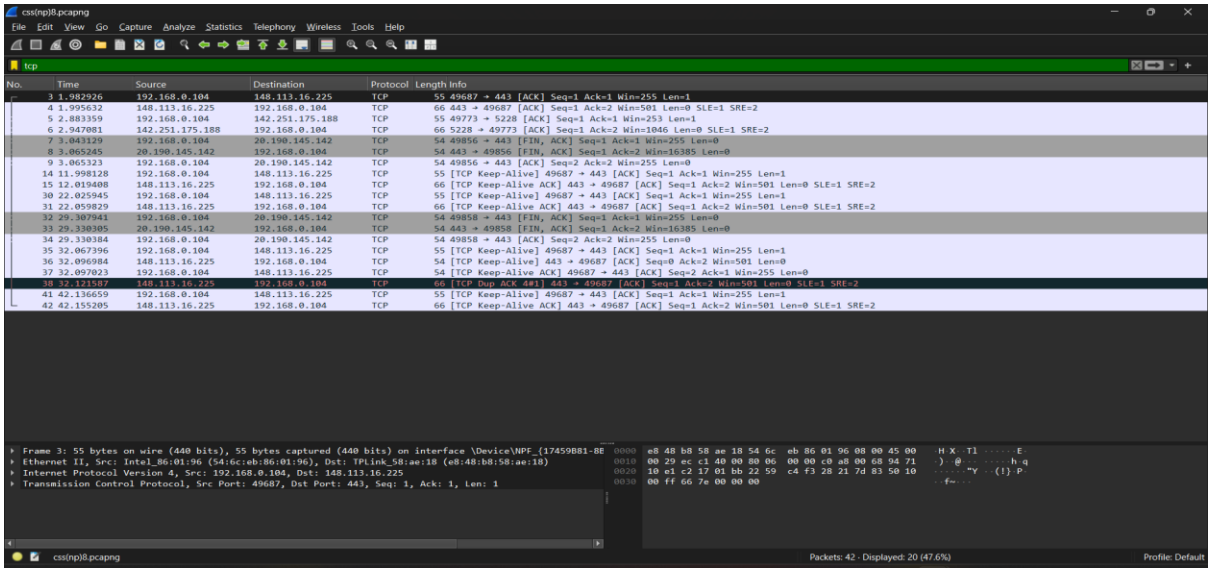


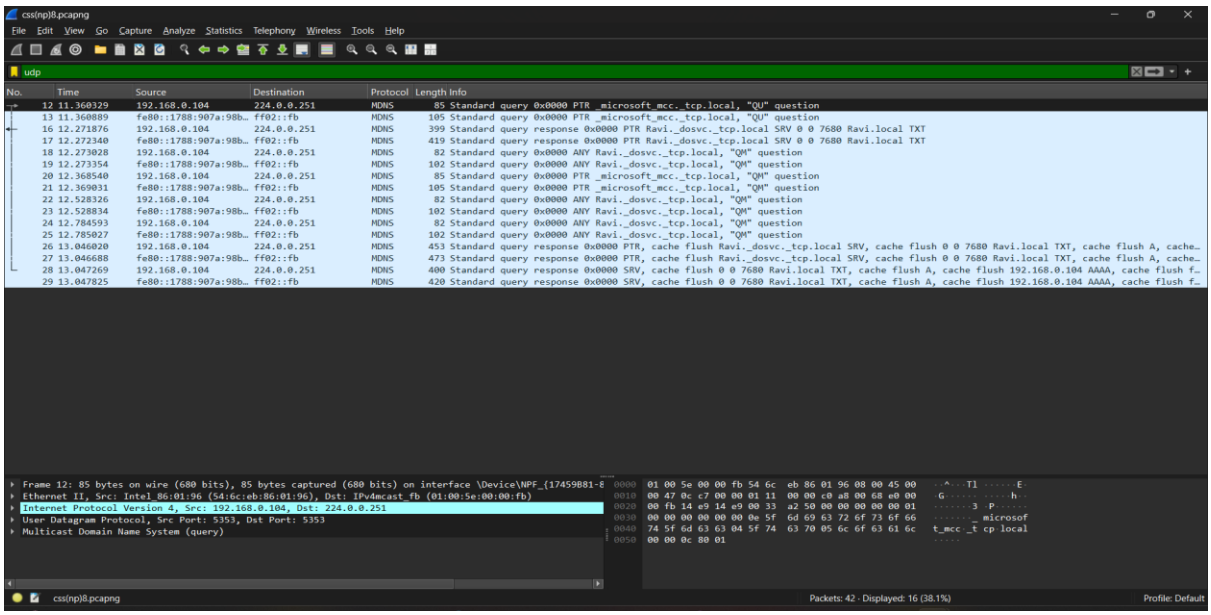

css(p)8.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
No. Time Source Destination Protocol Length Info
3 2.977823 192.168.0.1 239.255.255.250 SSDP 459 NOTIFY * HTTP/1.1
4 2.977823 192.168.0.1 239.255.255.250 SSDP 468 NOTIFY * HTTP/1.1
5 2.977823 192.168.0.1 239.255.255.250 SSDP 531 NOTIFY * HTTP/1.1
6 2.981675 192.168.0.1 239.255.255.250 SSDP 523 NOTIFY * HTTP/1.1
7 2.996146 192.168.0.1 239.255.255.250 SSDP 468 NOTIFY * HTTP/1.1
8 2.996146 192.168.0.1 239.255.255.250 SSDP 507 NOTIFY * HTTP/1.1
9 2.996146 192.168.0.1 239.255.255.250 SSDP 539 NOTIFY * HTTP/1.1
10 3.001965 192.168.0.1 239.255.255.250 SSDP 468 NOTIFY * HTTP/1.1
11 3.080558 192.168.0.1 239.255.255.250 SSDP 527 NOTIFY * HTTP/1.1
12 3.080558 192.168.0.1 239.255.255.250 SSDP 521 NOTIFY * HTTP/1.1
13 3.080558 192.168.0.1 239.255.255.250 SSDP 459 NOTIFY * HTTP/1.1
14 3.094156 192.168.0.1 239.255.255.250 SSDP 468 NOTIFY * HTTP/1.1
15 3.094156 192.168.0.1 239.255.255.250 SSDP 531 NOTIFY * HTTP/1.1
16 3.094156 192.168.0.1 239.255.255.250 SSDP 523 NOTIFY * HTTP/1.1
17 3.102594 192.168.0.1 239.255.255.250 SSDP 468 NOTIFY * HTTP/1.1
18 3.102594 192.168.0.1 239.255.255.250 SSDP 507 NOTIFY * HTTP/1.1
19 3.182666 192.168.0.1 239.255.255.250 SSDP 539 NOTIFY * HTTP/1.1
20 3.182666 192.168.0.1 239.255.255.250 SSDP 468 NOTIFY * HTTP/1.1
21 3.182666 192.168.0.1 239.255.255.250 SSDP 527 NOTIFY * HTTP/1.1
22 3.186406 192.168.0.1 239.255.255.250 SSDP 521 NOTIFY * HTTP/1.1
23 3.683768 192.168.0.103 224.0.0.251 MDNS 103 Standard query 0x0038 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
Frame 3: 459 bytes on wire (3672 bits), 459 bytes captured (3672 bits) on interface \Device\NPF_{17459B8
Ethernet II, Src: TPLink_58:ae:18 (e8:48:b8:58:ae:18), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 37877, Dst Port: 1900
Simple Service Discovery Protocol
0000 01 00 5e 7f ff fa e8 48 b8 58 ae 18 08 00 45 00
0010 01 bd 00 00 40 00 04 11 c4 8c c0 a8 00 01 ef ff
0020 ff fa 93 f5 07 6c 01 a9 18 97 4e 4f 54 49 46 59
0030 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 4f 53
0040 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 2e 32
0050 35 30 3a 31 39 30 30 0d 0a 43 41 43 48 45 2d 43
0060 4f 4e 54 52 4f 4c 3a 20 6d 61 78 2d 61 67 65 3d
0070 33 30 30 0d 0a 4c 4f 43 41 54 49 4f 4e 3a 20 68
0080 74 74 70 3a 2f 2f 31 39 32 2e 31 36 38 2e 30 2e
0090 31 3a 31 39 30 30 2f 67 61 74 65 64 65 73 63 2e
css(p)8.pcapng
Packets: 43 · Displayed: 21 (48.8%)
Profile: Default

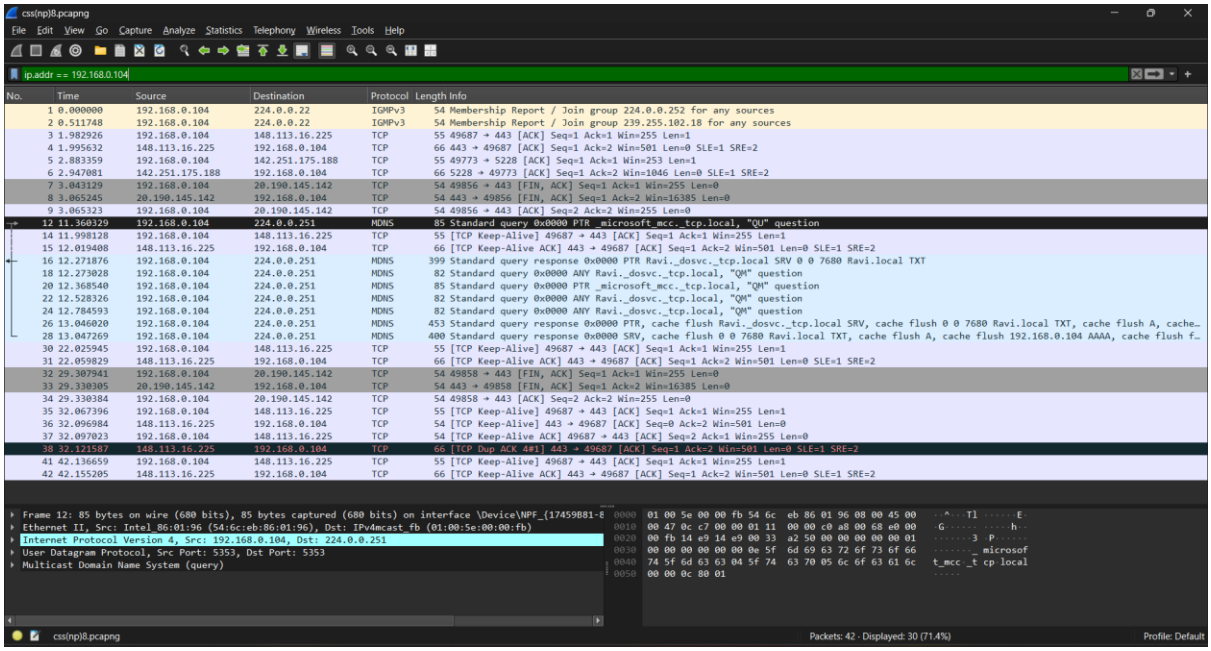

css(p)8.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.0.104 148.113.16.225 TCP 55 49687 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
2 0.007524 148.113.16.225 192.168.0.104 TCP 66 443 → 49687 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
24 3.768001 192.168.0.104 142.250.192.106 TCP 55 49793 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
25 3.788172 142.250.192.106 192.168.0.104 TCP 66 443 → 49793 [ACK] Seq=1 Ack=2 Win=1044 Len=0 SLE=1 SRE=2
26 5.450353 142.250.192.106 192.168.0.104 TLSv1.2 127 Application Data
27 5.452141 192.168.0.104 142.250.192.106 TCP 54 49793 → 443 [FIN, ACK] Seq=2 Ack=74 Win=255 Len=0
28 5.457912 142.250.192.106 192.168.0.104 TCP 54 443 → 49793 [FIN, ACK] Seq=74 Ack=3 Win=1044 Len=0
29 5.457952 192.168.0.104 142.250.192.106 TCP 54 49793 → 443 [ACK] Seq=3 Ack=75 Win=255 Len=0
31 8.585075 192.168.0.104 20.198.118.190 TLSv1.2 153 Application Data
32 8.595601 20.198.118.190 192.168.0.104 TLSv1.2 223 Application Data
33 8.647198 192.168.0.104 20.198.118.190 TCP 54 49408 → 443 [ACK] Seq=100 Ack=170 Win=251 Len=0
35 10.009613 192.168.0.104 148.113.16.225 TCP 55 [TCP Keep-Alive] 49687 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
36 10.037394 148.113.16.225 192.168.0.104 TCP 66 [TCP Keep-Alive ACK] 443 → 49687 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
37 10.582721 192.168.0.104 23.98.86.4 TLSv1.2 85 Application Data
38 10.645130 23.98.86.4 192.168.0.104 TLSv1.2 85 Application Data
39 10.693428 192.168.0.104 23.98.86.4 TCP 54 49779 → 8883 [ACK] Seq=32 Ack=32 Win=253 Len=0
42 20.052532 192.168.0.104 148.113.16.225 TCP 55 [TCP Keep-Alive] 49687 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
43 20.079860 148.113.16.225 192.168.0.104 TCP 66 [TCP Keep-Alive ACK] 443 → 49687 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{17459B81-8E
Ethernet II, Src: Intel_86:01:96 (54:6c:eb:86:01:96), Dst: TPLink_58:ae:18 (e8:48:b8:58:ae:18)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 148.113.16.225
Transmission Control Protocol, Src Port: 49687, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
0000 e8 48 b8 58 ae 18 54 6c eb 86 01 96 08 00 45 00
0010 00 29 ec 96 40 00 80 06 00 00 c0 a8 00 68 94 71
0020 10 e1 c2 17 01 bb 22 59 c4 f3 28 21 7d 83 50 10
0030 00 ff 66 7e 00 00 00
css(p)8.pcapng
Packets: 43 · Displayed: 18 (41.9%)
Profile: Default

Np:


css(np)8.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.0.104 224.0.0.22 IGMPv3 54 Membership Report / Join group 224.0.0.252 for any sources
2 0.511748 192.168.0.104 224.0.0.22 IGMPv3 54 Membership Report / Join group 239.255.102.18 for any sources
3 1.982926 192.168.0.104 148.113.16.225 TCP 55 49687 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
4 1.995632 148.113.16.225 192.168.0.104 TCP 66 443 → 49687 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
5 2.883359 192.168.0.104 142.251.175.188 TCP 55 49773 → 5228 [ACK] Seq=1 Ack=1 Win=253 Len=1
6 2.947081 142.251.175.188 192.168.0.104 TCP 66 5228 → 49773 [ACK] Seq=1 Ack=2 Win=1046 Len=0 SLE=1 SRE=2
7 3.043129 192.168.0.104 20.190.145.142 TCP 54 49856 → 443 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
8 3.065245 20.190.145.142 192.168.0.104 TCP 54 443 → 49856 [FIN, ACK] Seq=1 Ack=2 Win=16385 Len=0
9 3.065323 192.168.0.104 20.190.145.142 TCP 54 49856 → 443 [ACK] Seq=2 Ack=2 Win=255 Len=0
12 11.360329 192.168.0.104 224.0.0.251 MDNS 85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
14 11.998128 192.168.0.104 148.113.16.225 TCP 55 [TCP Keep-Alive] 49687 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
15 12.019408 148.113.16.225 192.168.0.104 TCP 66 [TCP Keep-Alive ACK] 443 → 49687 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
16 12.271876 192.168.0.104 224.0.0.251 MDNS 399 Standard query response 0x0000 PTR Ravi._dosvc._tcp.local SRV 0 0 7680 Ravi.local TXT
18 12.273028 192.168.0.104 224.0.0.251 MDNS 82 Standard query 0x0000 ANY Ravi._dosvc._tcp.local, "QM" question
20 12.368540 192.168.0.104 224.0.0.251 MDNS 85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
22 12.528326 192.168.0.104 224.0.0.251 MDNS 82 Standard query 0x0000 ANY Ravi._dosvc._tcp.local, "QM" question
24 12.784593 192.168.0.104 224.0.0.251 MDNS 82 Standard query 0x0000 ANY Ravi._dosvc._tcp.local, "QM" question
26 13.046020 192.168.0.104 224.0.0.251 MDNS 453 Standard query response 0x0000 PTR, cache flush Ravi._dosvc._tcp.local SRV, cache flush 0 0 7680 Ravi.local TXT, cache flush A, cache…
28 13.047269 192.168.0.104 224.0.0.251 MDNS 400 Standard query response 0x0000 SRV, cache flush 0 0 7680 Ravi.local TXT, cache flush A, cache flush 192.168.0.104 AAAA, cache flush f…
30 22.025945 192.168.0.104 148.113.16.225 TCP 55 [TCP Keep-Alive] 49687 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
31 22.059829 148.113.16.225 192.168.0.104 TCP 66 [TCP Keep-Alive ACK] 443 → 49687 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
32 29.307941 192.168.0.104 20.190.145.142 TCP 54 49858 → 443 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
33 29.330305 20.190.145.142 192.168.0.104 TCP 54 443 → 49858 [FIN, ACK] Seq=1 Ack=2 Win=16385 Len=0
34 29.330384 192.168.0.104 20.190.145.142 TCP 54 49858 → 443 [ACK] Seq=2 Ack=2 Win=255 Len=0
35 32.067396 192.168.0.104 148.113.16.225 TCP 55 [TCP Keep-Alive] 49687 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
36 32.096984 148.113.16.225 192.168.0.104 TCP 54 [TCP Keep-Alive] 443 → 49687 [ACK] Seq=0 Ack=2 Win=501 Len=0
37 32.097023 192.168.0.104 148.113.16.225 TCP 54 [TCP Keep-Alive ACK] 49687 → 443 [ACK] Seq=2 Ack=1 Win=255 Len=0
38 32.121587 148.113.16.225 192.168.0.104 TCP 66 [TCP Dup ACK 4#1] 443 → 49687 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
41 42.136659 192.168.0.104 148.113.16.225 TCP 55 [TCP Keep-Alive] 49687 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
42 42.155205 148.113.16.225 192.168.0.104 TCP 66 [TCP Keep-Alive ACK] 443 → 49687 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{17459B81-8E
Ethernet II, Src: Intel_86:01:96 (54:6c:eb:86:01:96), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 224.0.0.22
Internet Group Management Protocol
0000 01 00 5e 00 00 16 54 6c eb 86 01 96 08 00 46 00
0010 00 28 81 0e 00 00 01 02 00 00 c0 a8 00 68 e0 00
0020 00 16 94 04 00 00 22 00 fb 01 00 00 00 01 02 00
0030 00 00 e0 00 00 fc
css(np)8.pcapng
Packets: 42 · Displayed: 30 (71.4%)
Profile: Default


css(np)8.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
3 1.982926 192.168.0.104 148.113.16.225 TCP 55 49687 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
4 1.995632 148.113.16.225 192.168.0.104 TCP 66 443 → 49687 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
5 2.883359 192.168.0.104 142.251.175.188 TCP 55 49773 → 5228 [ACK] Seq=1 Ack=1 Win=253 Len=1
6 2.947081 142.251.175.188 192.168.0.104 TCP 66 5228 → 49773 [ACK] Seq=1 Ack=2 Win=1046 Len=0 SLE=1 SRE=2
7 3.043129 192.168.0.104 20.190.145.142 TCP 54 49856 → 443 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
8 3.065245 20.190.145.142 192.168.0.104 TCP 54 443 → 49856 [FIN, ACK] Seq=1 Ack=2 Win=16385 Len=0
9 3.065323 192.168.0.104 20.190.145.142 TCP 54 49856 → 443 [ACK] Seq=2 Ack=2 Win=255 Len=0
14 11.998128 192.168.0.104 148.113.16.225 TCP 55 [TCP Keep-Alive] 49687 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
15 12.019408 148.113.16.225 192.168.0.104 TCP 66 [TCP Keep-Alive ACK] 443 → 49687 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
30 22.025945 192.168.0.104 148.113.16.225 TCP 55 [TCP Keep-Alive] 49687 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
31 22.059829 148.113.16.225 192.168.0.104 TCP 66 [TCP Keep-Alive ACK] 443 → 49687 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
32 29.307941 192.168.0.104 20.190.145.142 TCP 54 49858 → 443 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
33 29.330305 20.190.145.142 192.168.0.104 TCP 54 443 → 49858 [FIN, ACK] Seq=1 Ack=2 Win=16385 Len=0
34 29.330384 192.168.0.104 20.190.145.142 TCP 54 49858 → 443 [ACK] Seq=2 Ack=2 Win=255 Len=0
35 32.067396 192.168.0.104 148.113.16.225 TCP 55 [TCP Keep-Alive] 49687 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
36 32.096984 148.113.16.225 192.168.0.104 TCP 54 [TCP Keep-Alive] 443 → 49687 [ACK] Seq=0 Ack=2 Win=501 Len=0
37 32.097023 192.168.0.104 148.113.16.225 TCP 54 [TCP Keep-Alive ACK] 49687 → 443 [ACK] Seq=2 Ack=1 Win=255 Len=0
38 32.121587 148.113.16.225 192.168.0.104 TCP 66 [TCP Dup ACK 4#1] 443 → 49687 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
41 42.136659 192.168.0.104 148.113.16.225 TCP 55 [TCP Keep-Alive] 49687 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
42 42.155205 148.113.16.225 192.168.0.104 TCP 66 [TCP Keep-Alive ACK] 443 → 49687 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
Frame 3: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{17459B81-8E
Ethernet II, Src: Intel_86:01:96 (54:6c:eb:86:01:96), Dst: TPLink_58:ae:18 (e8:48:b8:58:ae:18)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 148.113.16.225
Transmission Control Protocol, Src Port: 49687, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
0000 e8 48 b8 58 ae 18 54 6c eb 86 01 96 08 00 45 00
0010 00 29 ec c1 40 00 80 06 00 00 c0 a8 00 68 94 71
0020 10 e1 c2 17 01 bb 22 59 c4 f3 28 21 7d 83 50 10
0030 00 ff 66 7e 00 00 00
css(np)8.pcapng
Packets: 42 · Displayed: 20 (47.6%)
Profile: Default


css(np)8.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
No. Time Source Destination Protocol Length Info
12 11.360329 192.168.0.104 224.0.0.251 MDNS 85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
13 11.360889 fe80::1788:907a:98b… ff02::fb MDNS 105 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
16 12.271876 192.168.0.104 224.0.0.251 MDNS 399 Standard query response 0x0000 PTR Ravi._dosvc._tcp.local SRV 0 0 7680 Ravi.local TXT
17 12.272340 fe80::1788:907a:98b… ff02::fb MDNS 419 Standard query response 0x0000 PTR Ravi._dosvc._tcp.local SRV 0 0 7680 Ravi.local TXT
18 12.273028 192.168.0.104 224.0.0.251 MDNS 82 Standard query 0x0000 ANY Ravi._dosvc._tcp.local, "QM" question
19 12.273354 fe80::1788:907a:98b… ff02::fb MDNS 102 Standard query 0x0000 ANY Ravi._dosvc._tcp.local, "QM" question
20 12.368540 192.168.0.104 224.0.0.251 MDNS 85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
21 12.369031 fe80::1788:907a:98b… ff02::fb MDNS 105 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
22 12.528326 192.168.0.104 224.0.0.251 MDNS 82 Standard query 0x0000 ANY Ravi._dosvc._tcp.local, "QM" question
23 12.528834 fe80::1788:907a:98b… ff02::fb MDNS 102 Standard query 0x0000 ANY Ravi._dosvc._tcp.local, "QM" question
24 12.784593 192.168.0.104 224.0.0.251 MDNS 82 Standard query 0x0000 ANY Ravi._dosvc._tcp.local, "QM" question
25 12.785027 fe80::1788:907a:98b… ff02::fb MDNS 102 Standard query 0x0000 ANY Ravi._dosvc._tcp.local, "QM" question
26 13.046020 192.168.0.104 224.0.0.251 MDNS 453 Standard query response 0x0000 PTR, cache flush Ravi._dosvc._tcp.local SRV, cache flush 0 0 7680 Ravi.local TXT, cache flush A, cache…
27 13.046688 fe80::1788:907a:98b… ff02::fb MDNS 473 Standard query response 0x0000 PTR, cache flush Ravi._dosvc._tcp.local SRV, cache flush 0 0 7680 Ravi.local TXT, cache flush A, cache…
28 13.047269 192.168.0.104 224.0.0.251 MDNS 400 Standard query response 0x0000 SRV, cache flush 0 0 7680 Ravi.local TXT, cache flush A, cache flush 192.168.0.104 AAAA, cache flush f…
29 13.047825 fe80::1788:907a:98b… ff02::fb MDNS 420 Standard query response 0x0000 SRV, cache flush 0 0 7680 Ravi.local TXT, cache flush A, cache flush 192.168.0.104 AAAA, cache flush f…
Frame 12: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{17459B81-8
Ethernet II, Src: Intel_86:01:96 (54:6c:eb:86:01:96), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)
0000 01 00 5e 00 00 fb 54 6c eb 86 01 96 08 00 45 00
0010 00 47 0c c7 00 00 01 11 00 00 c0 a8 00 68 e0 00
0020 00 fb 14 e9 14 e9 00 33 a2 50 00 00 00 00 00 01
0030 00 00 00 00 00 00 0e 5f 6d 69 63 72 6f 73 6f 66
0040 74 5f 6d 63 63 04 5f 74 63 70 05 6c 6f 63 61 6c
0050 00 00 0c 80 01
css(np)8.pcapng
Packets: 42 · Displayed: 16 (38.1%)
Profile: Default


css(np)8.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.0.104
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.0.104 224.0.0.22 IGMPv3 54 Membership Report / Join group 224.0.0.252 for any sources
2 0.511748 192.168.0.104 224.0.0.22 IGMPv3 54 Membership Report / Join group 239.255.102.18 for any sources
3 1.982926 192.168.0.104 148.113.16.225 TCP 55 49687 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
4 1.995632 148.113.16.225 192.168.0.104 TCP 66 443 → 49687 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
5 2.883359 192.168.0.104 142.251.175.188 TCP 55 49773 → 5228 [ACK] Seq=1 Ack=1 Win=253 Len=1
6 2.947081 142.251.175.188 192.168.0.104 TCP 66 5228 → 49773 [ACK] Seq=1 Ack=2 Win=1046 Len=0 SLE=1 SRE=2
7 3.043129 192.168.0.104 20.190.145.142 TCP 54 49856 → 443 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
8 3.065245 20.190.145.142 192.168.0.104 TCP 54 443 → 49856 [FIN, ACK] Seq=1 Ack=2 Win=16385 Len=0
9 3.065323 192.168.0.104 20.190.145.142 TCP 54 49856 → 443 [ACK] Seq=2 Ack=2 Win=255 Len=0
12 11.360329 192.168.0.104 224.0.0.251 MDNS 85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
14 11.998128 192.168.0.104 148.113.16.225 TCP 55 [TCP Keep-Alive] 49687 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
15 12.019408 148.113.16.225 192.168.0.104 TCP 66 [TCP Keep-Alive ACK] 443 → 49687 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
16 12.271876 192.168.0.104 224.0.0.251 MDNS 399 Standard query response 0x0000 PTR Ravi._dosvc._tcp.local SRV 0 0 7680 Ravi.local TXT
18 12.273028 192.168.0.104 224.0.0.251 MDNS 82 Standard query 0x0000 ANY Ravi._dosvc._tcp.local, "QM" question
20 12.368540 192.168.0.104 224.0.0.251 MDNS 85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
22 12.528326 192.168.0.104 224.0.0.251 MDNS 82 Standard query 0x0000 ANY Ravi._dosvc._tcp.local, "QM" question
24 12.784593 192.168.0.104 224.0.0.251 MDNS 82 Standard query 0x0000 ANY Ravi._dosvc._tcp.local, "QM" question
26 13.046020 192.168.0.104 224.0.0.251 MDNS 453 Standard query response 0x0000 PTR, cache flush Ravi._dosvc._tcp.local SRV, cache flush 0 0 7680 Ravi.local TXT, cache flush A, cache…
28 13.047269 192.168.0.104 224.0.0.251 MDNS 400 Standard query response 0x0000 SRV, cache flush 0 0 7680 Ravi.local TXT, cache flush A, cache flush 192.168.0.104 AAAA, cache flush f…
30 22.025945 192.168.0.104 148.113.16.225 TCP 55 [TCP Keep-Alive] 49687 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
31 22.059829 148.113.16.225 192.168.0.104 TCP 66 [TCP Keep-Alive ACK] 443 → 49687 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
32 29.307941 192.168.0.104 20.190.145.142 TCP 54 49858 → 443 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
33 29.330305 20.190.145.142 192.168.0.104 TCP 54 443 → 49858 [FIN, ACK] Seq=1 Ack=2 Win=16385 Len=0
34 29.330384 192.168.0.104 20.190.145.142 TCP 54 49858 → 443 [ACK] Seq=2 Ack=2 Win=255 Len=0
35 32.067396 192.168.0.104 148.113.16.225 TCP 55 [TCP Keep-Alive] 49687 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
36 32.096984 148.113.16.225 192.168.0.104 TCP 54 [TCP Keep-Alive] 443 → 49687 [ACK] Seq=0 Ack=2 Win=501 Len=0
37 32.097023 192.168.0.104 148.113.16.225 TCP 54 [TCP Keep-Alive ACK] 49687 → 443 [ACK] Seq=2 Ack=1 Win=255 Len=0
38 32.121587 148.113.16.225 192.168.0.104 TCP 66 [TCP Dup ACK 4#1] 443 → 49687 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
41 42.136659 192.168.0.104 148.113.16.225 TCP 55 [TCP Keep-Alive] 49687 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
42 42.155205 148.113.16.225 192.168.0.104 TCP 66 [TCP Keep-Alive ACK] 443 → 49687 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
Frame 12: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{17459B81-8
Ethernet II, Src: Intel_86:01:96 (54:6c:eb:86:01:96), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)
0000 01 00 5e 00 00 fb 54 6c eb 86 01 96 08 00 45 00
0010 00 47 0c c7 00 00 01 11 00 00 c0 a8 00 68 e0 00
0020 00 fb 14 e9 14 e9 00 33 a2 50 00 00 00 00 00 01
0030 00 00 00 00 00 00 0e 5f 6d 69 63 72 6f 73 6f 66
0040 74 5f 6d 63 63 04 5f 74 63 70 05 6c 6f 63 61 6c
0050 00 00 0c 80 01
css(np)8.pcapng
Packets: 42 · Displayed: 30 (71.4%)
Profile: Default