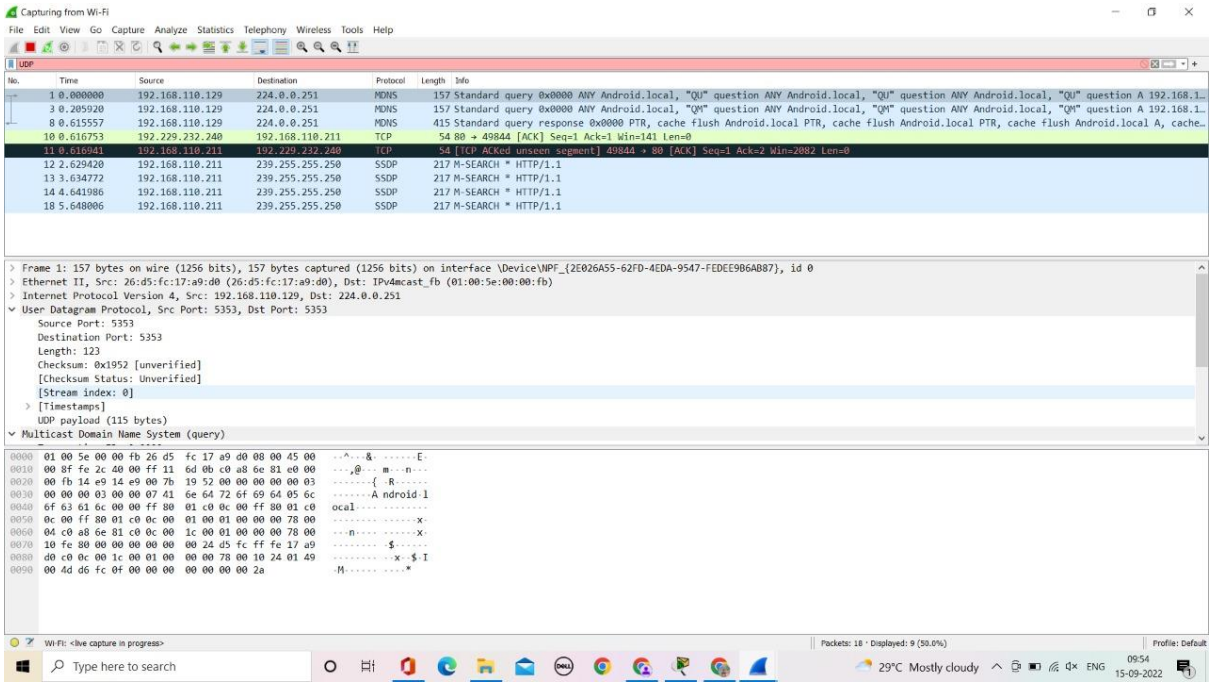
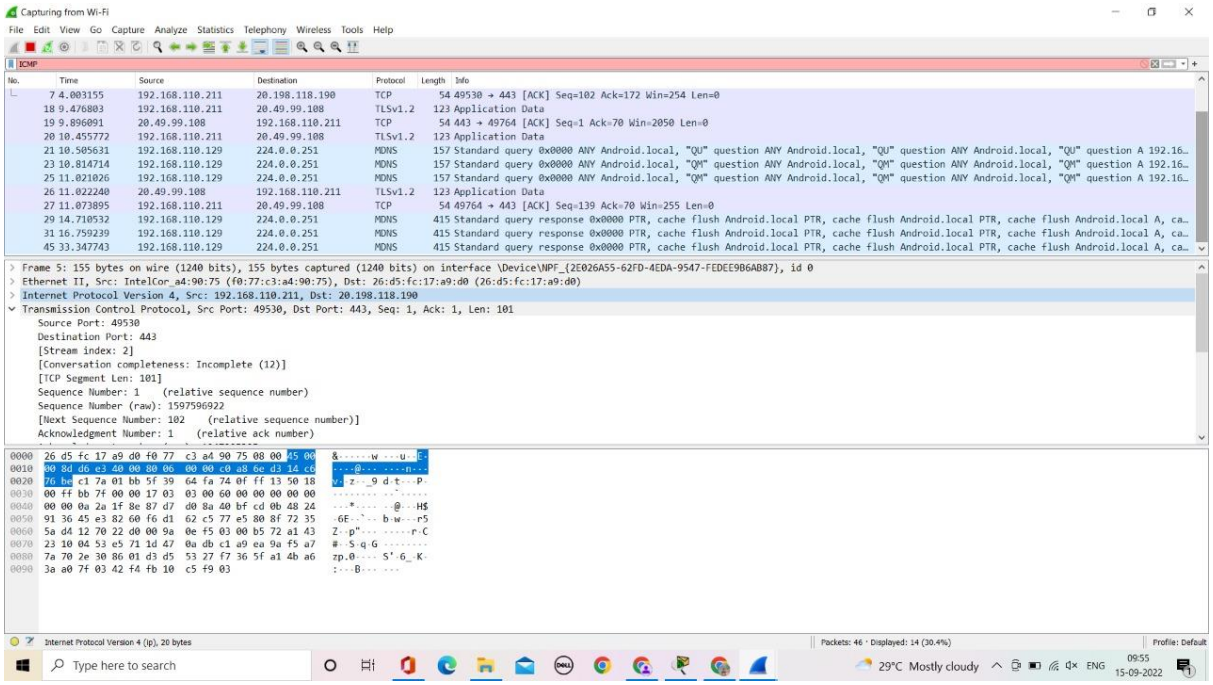
Computer networks - lab manual using wireshark

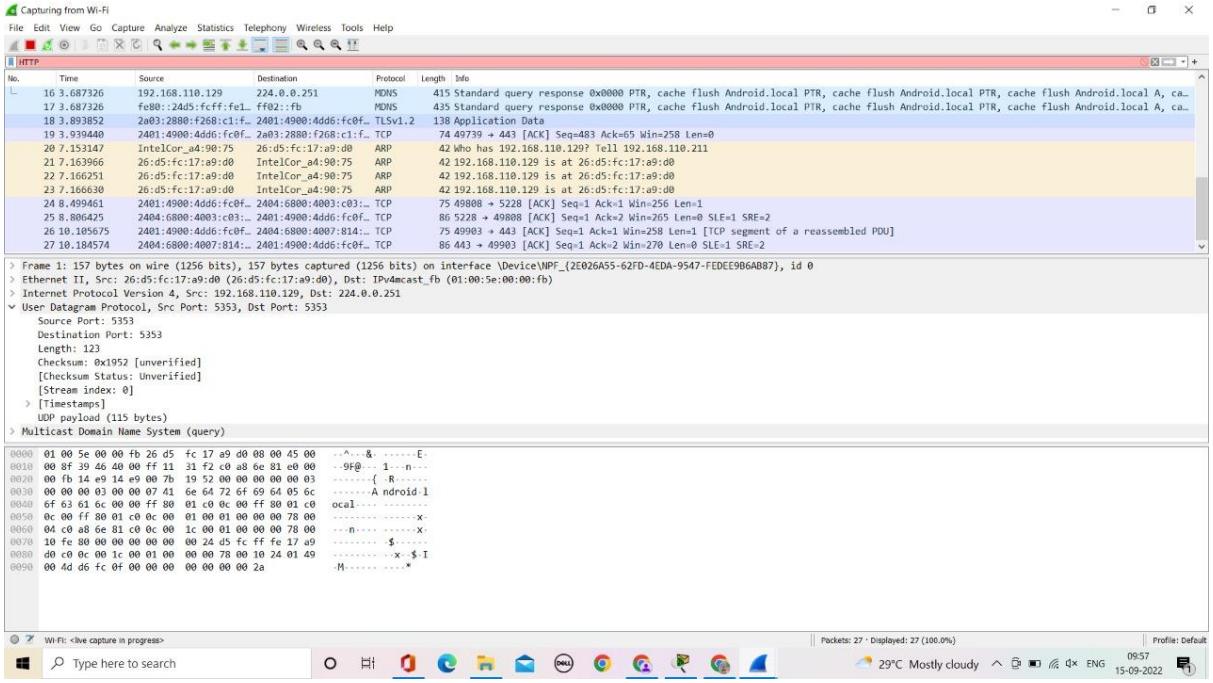
1.UDP:



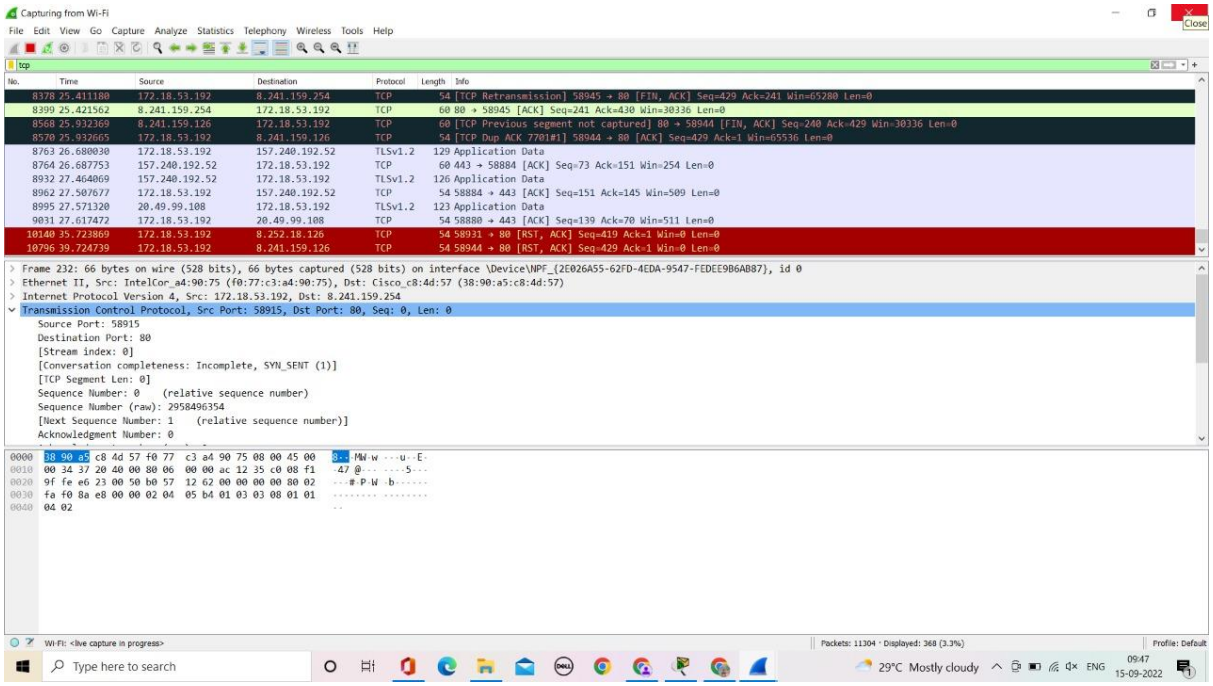
2.ICMP:



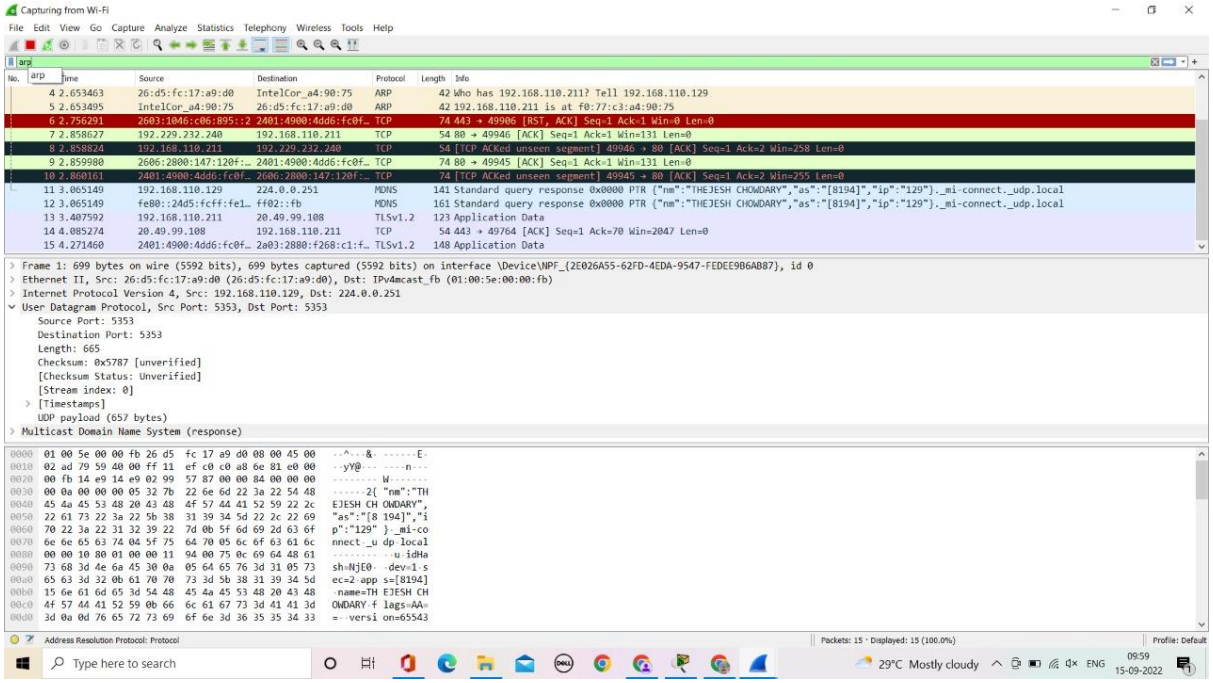
3.HTTP:


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
HTTP
No. Time Source Destination Protocol Length Info
16 3.687326 192.168.110.129 224.0.0.251 MDNS 415 Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local PTR, cache flush Android.local A, ca…
17 3.687326 fe80::24d5:fcff:fe1… ff02::fb MDNS 435 Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local PTR, cache flush Android.local A, ca…
18 3.893852 2a03:2880:f268:c1:f… 2401:4900:4dd6:fc0f… TLSv1.2 138 Application Data
19 3.939440 2401:4900:4dd6:fc0f… 2a03:2880:f268:c1:f… TCP 74 49739 → 443 [ACK] Seq=483 Ack=65 Win=258 Len=0
20 7.153147 IntelCor_a4:90:75 26:d5:fc:17:a9:d0 ARP 42 Who has 192.168.110.129? Tell 192.168.110.211
21 7.163966 26:d5:fc:17:a9:d0 IntelCor_a4:90:75 ARP 42 192.168.110.129 is at 26:d5:fc:17:a9:d0
22 7.166251 26:d5:fc:17:a9:d0 IntelCor_a4:90:75 ARP 42 192.168.110.129 is at 26:d5:fc:17:a9:d0
23 7.166630 26:d5:fc:17:a9:d0 IntelCor_a4:90:75 ARP 42 192.168.110.129 is at 26:d5:fc:17:a9:d0
24 8.499461 2401:4900:4dd6:fc0f… 2404:6800:4003:c03:… TCP 75 49808 → 5228 [ACK] Seq=1 Ack=1 Win=256 Len=1
25 8.806425 2404:6800:4003:c03:… 2401:4900:4dd6:fc0f… TCP 86 5228 → 49808 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
26 10.105675 2401:4900:4dd6:fc0f… 2404:6800:4007:814:… TCP 75 49903 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a reassembled PDU]
27 10.184574 2404:6800:4007:814:… 2401:4900:4dd6:fc0f… TCP 86 443 → 49903 [ACK] Seq=1 Ack=2 Win=270 Len=0 SLE=1 SRE=2
Frame 1: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface \Device\NPF_{2E026A55-62FD-4EDA-9547-FEDEE9B6AB87}, id 0
Ethernet II, Src: 26:d5:fc:17:a9:d0 (26:d5:fc:17:a9:d0), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
Internet Protocol Version 4, Src: 192.168.110.129, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Source Port: 5353
Destination Port: 5353
Length: 123
Checksum: 0x1952 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
UDP payload (115 bytes)
Multicast Domain Name System (query)
0000 01 00 5e 00 00 fb 26 d5 fc 17 a9 d0 08 00 45 00
0010 00 8f 39 46 40 00 ff 11 31 f2 c0 a8 6e 81 e0 00
0020 00 fb 14 e9 14 e9 00 7b 19 52 00 00 00 00 00 03
0030 00 00 00 03 00 00 07 41 6e 64 72 6f 69 64 05 6c
0040 6f 63 61 6c 00 00 ff 80 01 c0 0c 00 ff 80 01 c0
0050 0c 00 ff 80 01 c0 0c 00 01 00 01 00 00 00 78 00
0060 04 c0 a8 6e 81 c0 0c 00 1c 00 01 00 00 00 78 00
0070 10 fe 80 00 00 00 00 00 00 24 d5 fc ff fe 17 a9
0080 d0 c0 0c 00 1c 00 01 00 00 00 78 00 10 24 01 49
0090 00 4d d6 fc 0f 00 00 00 00 00 00 00 2a
Wi-Fi: <live capture in progress>
Packets: 27 · Displayed: 27 (100.0%)
Profile: Default
Type here to search
29°C Mostly cloudy
ENG
09:57
15-09-2022

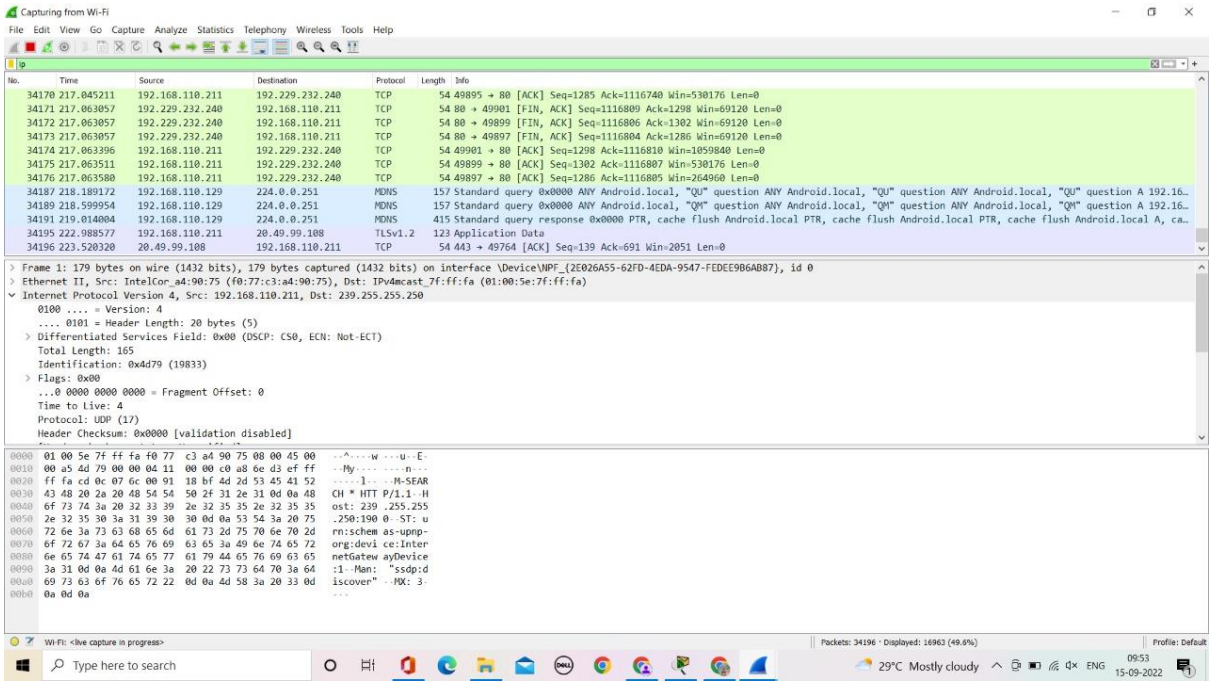
4.TCP:


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Close
tcp
No. Time Source Destination Protocol Length Info
8378 25.411180 172.18.53.192 8.241.159.254 TCP 54 [TCP Retransmission] 58945 → 80 [FIN, ACK] Seq=429 Ack=241 Win=65280 Len=0
8399 25.421562 8.241.159.254 172.18.53.192 TCP 60 80 → 58945 [ACK] Seq=241 Ack=430 Win=30336 Len=0
8568 25.932369 8.241.159.126 172.18.53.192 TCP 60 [TCP Previous segment not captured] 80 → 58944 [FIN, ACK] Seq=240 Ack=429 Win=30336 Len=0
8570 25.932665 172.18.53.192 8.241.159.126 TCP 54 [TCP Dup ACK 7701#1] 58944 → 80 [ACK] Seq=429 Ack=1 Win=65536 Len=0
8763 26.680030 172.18.53.192 157.240.192.52 TLSv1.2 129 Application Data
8764 26.687753 157.240.192.52 172.18.53.192 TCP 60 443 → 58884 [ACK] Seq=73 Ack=151 Win=254 Len=0
8932 27.464069 157.240.192.52 172.18.53.192 TLSv1.2 126 Application Data
8962 27.507677 172.18.53.192 157.240.192.52 TCP 54 58884 → 443 [ACK] Seq=151 Ack=145 Win=509 Len=0
8995 27.571320 20.49.99.108 172.18.53.192 TLSv1.2 123 Application Data
9031 27.617472 172.18.53.192 20.49.99.108 TCP 54 58880 → 443 [ACK] Seq=139 Ack=70 Win=511 Len=0
10140 35.723869 172.18.53.192 8.252.18.126 TCP 54 58931 → 80 [RST, ACK] Seq=419 Ack=1 Win=0 Len=0
10796 39.724739 172.18.53.192 8.241.159.126 TCP 54 58944 → 80 [RST, ACK] Seq=429 Ack=1 Win=0 Len=0
Frame 232: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{2E026A55-62FD-4EDA-9547-FEDEE9B6AB87}, id 0
Ethernet II, Src: IntelCor_a4:90:75 (f0:77:c3:a4:90:75), Dst: Cisco_c8:4d:57 (38:90:a5:c8:4d:57)
Internet Protocol Version 4, Src: 172.18.53.192, Dst: 8.241.159.254
Transmission Control Protocol, Src Port: 58915, Dst Port: 80, Seq: 0, Len: 0
Source Port: 58915
Destination Port: 80
[Stream index: 0]
[Conversation completeness: Incomplete, SYN_SENT (1)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2958496354
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
0000 38 90 a5 c8 4d 57 f0 77 c3 a4 90 75 08 00 45 00
0010 00 34 37 20 40 00 80 06 00 00 ac 12 35 c0 08 f1
0020 9f fe e6 23 00 50 b0 57 12 62 00 00 00 00 80 02
0030 fa f0 8a e8 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02
Wi-Fi: <live capture in progress>
Packets: 11304 · Displayed: 368 (3.3%)
Profile: Default
Type here to search
29°C Mostly cloudy
ENG
09:47
15-09-2022

5.ARP:


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
No. Time Source Destination Protocol Length Info
4 2.653463 26:d5:fc:17:a9:d0 IntelCor_a4:90:75 ARP 42 Who has 192.168.110.211? Tell 192.168.110.129
5 2.653495 IntelCor_a4:90:75 26:d5:fc:17:a9:d0 ARP 42 192.168.110.211 is at f0:77:c3:a4:90:75
6 2.756291 2603:1046:c06:895::2 2401:4900:4dd6:fc0f… TCP 74 443 → 49906 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7 2.858627 192.229.232.240 192.168.110.211 TCP 54 80 → 49946 [ACK] Seq=1 Ack=1 Win=131 Len=0
8 2.858824 192.168.110.211 192.229.232.240 TCP 54 [TCP ACKed unseen segment] 49946 → 80 [ACK] Seq=1 Ack=2 Win=258 Len=0
9 2.859980 2606:2800:147:120f:… 2401:4900:4dd6:fc0f… TCP 74 80 → 49945 [ACK] Seq=1 Ack=1 Win=131 Len=0
10 2.860161 2401:4900:4dd6:fc0f… 2606:2800:147:120f:… TCP 74 [TCP ACKed unseen segment] 49945 → 80 [ACK] Seq=1 Ack=2 Win=255 Len=0
11 3.065149 192.168.110.129 224.0.0.251 MDNS 141 Standard query response 0x0000 PTR {"nm":"THEJESH CHOWDARY","as":"[8194]","ip":"129"}._mi-connect._udp.local
12 3.065149 fe80::24d5:fcff:fe1… ff02::fb MDNS 161 Standard query response 0x0000 PTR {"nm":"THEJESH CHOWDARY","as":"[8194]","ip":"129"}._mi-connect._udp.local
13 3.407592 192.168.110.211 20.49.99.108 TLSv1.2 123 Application Data
14 4.085274 20.49.99.108 192.168.110.211 TCP 54 443 → 49764 [ACK] Seq=1 Ack=70 Win=2047 Len=0
15 4.271460 2401:4900:4dd6:fc0f… 2a03:2880:f268:c1:f… TLSv1.2 148 Application Data
Frame 1: 699 bytes on wire (5592 bits), 699 bytes captured (5592 bits) on interface \Device\NPF_{2E026A55-62FD-4EDA-9547-FEDEE9B6AB87}, id 0
Ethernet II, Src: 26:d5:fc:17:a9:d0 (26:d5:fc:17:a9:d0), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
Internet Protocol Version 4, Src: 192.168.110.129, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Source Port: 5353
Destination Port: 5353
Length: 665
Checksum: 0x5787 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
UDP payload (657 bytes)
Multicast Domain Name System (response)
0000 01 00 5e 00 00 fb 26 d5 fc 17 a9 d0 08 00 45 00
0010 02 ad 79 59 40 00 ff 11 ef c0 c0 a8 6e 81 e0 00
0020 00 fb 14 e9 14 e9 02 99 57 87 00 00 84 00 00 00
0030 00 0a 00 00 00 05 32 7b 22 6e 6d 22 3a 22 54 48
0040 45 4a 45 53 48 20 43 48 4f 57 44 41 52 59 22 2c
0050 22 61 73 22 3a 22 5b 38 31 39 34 5d 22 2c 22 69
0060 70 22 3a 22 31 32 39 22 7d 0b 5f 6d 69 2d 63 6f
0070 6e 6e 65 63 74 04 5f 75 64 70 05 6c 6f 63 61 6c
0080 00 00 10 80 01 00 00 11 94 00 75 0c 69 64 48 61
0090 73 68 3d 4e 6a 45 30 0a 05 64 65 76 3d 31 05 73
00a0 65 63 3d 32 0b 61 70 70 73 3d 5b 38 31 39 34 5d
00b0 15 6e 61 6d 65 3d 54 48 45 4a 45 53 48 20 43 48
00c0 4f 57 44 41 52 59 0b 66 6c 61 67 73 3d 41 41 3d
00d0 3d 0a 0d 76 65 72 73 69 6f 6e 3d 36 35 35 34 33
Address Resolution Protocol: Protocol
Packets: 15 · Displayed: 15 (100.0%)
Profile: Default
Type here to search
29°C Mostly cloudy
ENG
09:59
15-09-2022

6.IP:


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip
No. Time Source Destination Protocol Length Info
34170 217.045211 192.168.110.211 192.229.232.240 TCP 54 49895 → 80 [ACK] Seq=1285 Ack=1116740 Win=530176 Len=0
34171 217.063057 192.229.232.240 192.168.110.211 TCP 54 80 → 49901 [FIN, ACK] Seq=1116809 Ack=1298 Win=69120 Len=0
34172 217.063057 192.229.232.240 192.168.110.211 TCP 54 80 → 49899 [FIN, ACK] Seq=1116806 Ack=1302 Win=69120 Len=0
34173 217.063057 192.229.232.240 192.168.110.211 TCP 54 80 → 49897 [FIN, ACK] Seq=1116804 Ack=1286 Win=69120 Len=0
34174 217.063396 192.168.110.211 192.229.232.240 TCP 54 49901 → 80 [ACK] Seq=1298 Ack=1116810 Win=1059840 Len=0
34175 217.063511 192.168.110.211 192.229.232.240 TCP 54 49899 → 80 [ACK] Seq=1302 Ack=1116807 Win=530176 Len=0
34176 217.063580 192.168.110.211 192.229.232.240 TCP 54 49897 → 80 [ACK] Seq=1286 Ack=1116805 Win=264960 Len=0
34187 218.189172 192.168.110.129 224.0.0.251 MDNS 157 Standard query 0x0000 ANY Android.local, "QU" question ANY Android.local, "QU" question ANY Android.local, "QU" question A 192.16…
34189 218.599954 192.168.110.129 224.0.0.251 MDNS 157 Standard query 0x0000 ANY Android.local, "QM" question ANY Android.local, "QM" question ANY Android.local, "QM" question A 192.16…
34191 219.014004 192.168.110.129 224.0.0.251 MDNS 415 Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local PTR, cache flush Android.local A, ca…
34195 222.988577 192.168.110.211 20.49.99.108 TLSv1.2 123 Application Data
34196 223.520320 20.49.99.108 192.168.110.211 TCP 54 443 → 49764 [ACK] Seq=139 Ack=691 Win=2051 Len=0
Frame 1: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on interface \Device\NPF_{2E026A55-62FD-4EDA-9547-FEDEE9B6AB87}, id 0
Ethernet II, Src: IntelCor_a4:90:75 (f0:77:c3:a4:90:75), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.110.211, Dst: 239.255.255.250
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 165
Identification: 0x4d79 (19833)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 4
Protocol: UDP (17)
Header Checksum: 0x0000 [validation disabled]
0000 01 00 5e 7f ff fa f0 77 c3 a4 90 75 08 00 45 00
0010 00 a5 4d 79 00 00 04 11 00 00 c0 a8 6e d3 ef ff
0020 ff fa cd 0c 07 6c 00 91 18 bf 4d 2d 53 45 41 52
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48
0040 6f 73 74 3a 20 32 33 39 2e 32 35 35 2e 32 35 35
0050 2e 32 35 30 3a 31 39 30 0d 0a 53 54 3a 20 75
0060 72 6e 3a 73 63 68 65 6d 61 73 2d 75 70 6e 70 2d
0070 6f 72 67 3a 64 65 76 69 63 65 3a 49 6e 74 65 72
0080 6e 65 74 47 61 74 65 77 61 79 44 65 76 69 63 65
0090 3a 31 0d 0a 4d 61 6e 3a 20 22 73 73 64 70 3a 64
00a0 69 73 63 6f 76 65 72 22 0d 0a 4d 58 3a 20 33 0d
00b0 0a 0d 0a
Wi-Fi: <live capture in progress>
Packets: 34196 · Displayed: 16963 (49.6%)
Profile: Default
Type here to search
29°C Mostly cloudy
ENG
09:53
15-09-2022