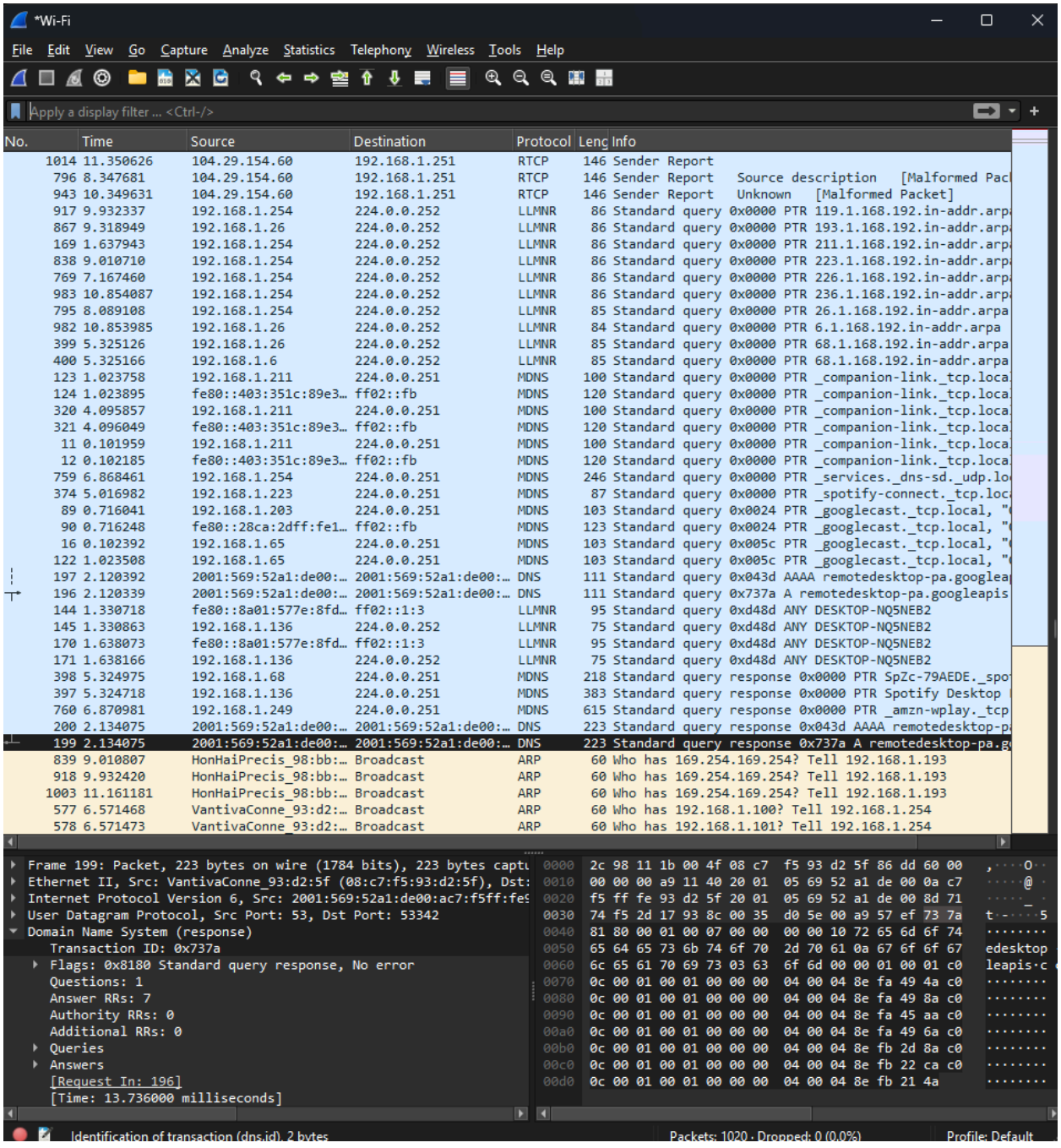
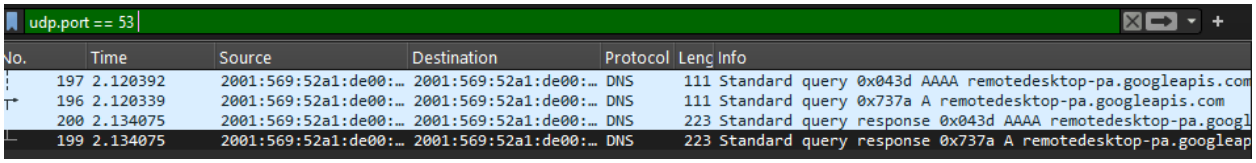
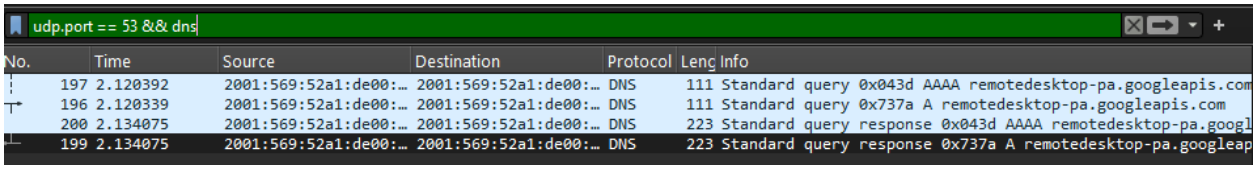
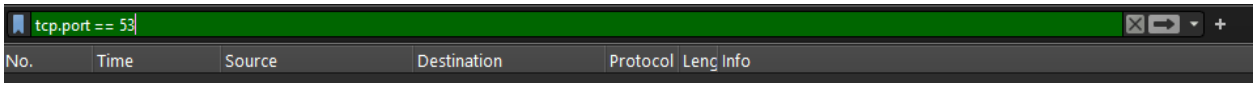
# Section 1

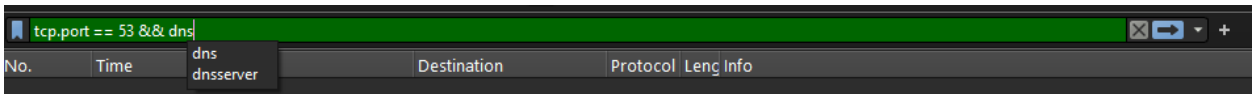

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Leng Info
1014 11.350626 104.29.154.60 192.168.1.251 RTCP 146 Sender Report
796 8.347681 104.29.154.60 192.168.1.251 RTCP 146 Sender Report Source description [Malformed Pac
943 10.349631 104.29.154.60 192.168.1.251 RTCP 146 Sender Report Unknown [Malformed Packet]
917 9.932337 192.168.1.254 224.0.0.252 LLMNR 86 Standard query 0x0000 PTR 119.1.168.192.in-addr.arp
867 9.318949 192.168.1.26 224.0.0.252 LLMNR 86 Standard query 0x0000 PTR 193.1.168.192.in-addr.arp
169 1.637943 192.168.1.254 224.0.0.252 LLMNR 86 Standard query 0x0000 PTR 211.1.168.192.in-addr.arp
838 9.010710 192.168.1.254 224.0.0.252 LLMNR 86 Standard query 0x0000 PTR 223.1.168.192.in-addr.arp
769 7.167460 192.168.1.254 224.0.0.252 LLMNR 86 Standard query 0x0000 PTR 226.1.168.192.in-addr.arp
983 10.854087 192.168.1.254 224.0.0.252 LLMNR 86 Standard query 0x0000 PTR 236.1.168.192.in-addr.arp
795 8.089108 192.168.1.254 224.0.0.252 LLMNR 85 Standard query 0x0000 PTR 26.1.168.192.in-addr.arpa
982 10.853985 192.168.1.26 224.0.0.252 LLMNR 84 Standard query 0x0000 PTR 6.1.168.192.in-addr.arpa
399 5.325126 192.168.1.26 224.0.0.252 LLMNR 85 Standard query 0x0000 PTR 68.1.168.192.in-addr.arpa
400 5.325166 192.168.1.6 224.0.0.252 LLMNR 85 Standard query 0x0000 PTR 68.1.168.192.in-addr.arpa
123 1.023758 192.168.1.211 224.0.0.251 MDNS 100 Standard query 0x0000 PTR _companion-link._tcp.loca
124 1.023895 fe80::403:351c:89e3… ff02::fb MDNS 120 Standard query 0x0000 PTR _companion-link._tcp.loca
320 4.095857 192.168.1.211 224.0.0.251 MDNS 100 Standard query 0x0000 PTR _companion-link._tcp.loca
321 4.096049 fe80::403:351c:89e3… ff02::fb MDNS 120 Standard query 0x0000 PTR _companion-link._tcp.loca
11 0.101959 192.168.1.211 224.0.0.251 MDNS 100 Standard query 0x0000 PTR _companion-link._tcp.loca
12 0.102185 fe80::403:351c:89e3… ff02::fb MDNS 120 Standard query 0x0000 PTR _companion-link._tcp.loca
759 6.868461 192.168.1.254 224.0.0.251 MDNS 246 Standard query 0x0000 PTR _services._dns-sd._udp.lo
374 5.016982 192.168.1.223 224.0.0.251 MDNS 87 Standard query 0x0000 PTR _spotify-connect._tcp.loc
89 0.716041 192.168.1.203 224.0.0.251 MDNS 103 Standard query 0x0024 PTR _googlecast._tcp.local, "
90 0.716248 fe80::28ca:2dff:fe1… ff02::fb MDNS 123 Standard query 0x0024 PTR _googlecast._tcp.local, "
16 0.102392 192.168.1.65 224.0.0.251 MDNS 103 Standard query 0x005c PTR _googlecast._tcp.local, "
122 1.023508 192.168.1.65 224.0.0.251 MDNS 103 Standard query 0x005c PTR _googlecast._tcp.local, "
197 2.120392 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 111 Standard query 0x043d AAAA remotedesktop-pa.googlea
196 2.120339 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 111 Standard query 0x737a A remotedesktop-pa.googleapis
144 1.330718 fe80::8a01:577e:8fd… ff02::1:3 LLMNR 95 Standard query 0xd48d ANY DESKTOP-NQ5NEB2
145 1.330863 192.168.1.136 224.0.0.252 LLMNR 75 Standard query 0xd48d ANY DESKTOP-NQ5NEB2
170 1.638073 fe80::8a01:577e:8fd… ff02::1:3 LLMNR 95 Standard query 0xd48d ANY DESKTOP-NQ5NEB2
171 1.638166 192.168.1.136 224.0.0.252 LLMNR 75 Standard query 0xd48d ANY DESKTOP-NQ5NEB2
398 5.324975 192.168.1.68 224.0.0.251 MDNS 218 Standard query response 0x0000 PTR SpZc-79AEDE._spo
397 5.324718 192.168.1.136 224.0.0.251 MDNS 383 Standard query response 0x0000 PTR Spotify Desktop
760 6.870981 192.168.1.249 224.0.0.251 MDNS 615 Standard query response 0x0000 PTR _amzn-wplay._tcp
200 2.134075 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 223 Standard query response 0x043d AAAA remotedesktop-p
199 2.134075 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 223 Standard query response 0x737a A remotedesktop-pa.g
839 9.010807 HonHaiPrecis_98:bb:… Broadcast ARP 60 Who has 169.254.169.254? Tell 192.168.1.193
918 9.932420 HonHaiPrecis_98:bb:… Broadcast ARP 60 Who has 169.254.169.254? Tell 192.168.1.193
1003 11.161181 HonHaiPrecis_98:bb:… Broadcast ARP 60 Who has 169.254.169.254? Tell 192.168.1.193
577 6.571468 VantivaConne_93:d2:… Broadcast ARP 60 Who has 192.168.1.100? Tell 192.168.1.254
578 6.571473 VantivaConne_93:d2:… Broadcast ARP 60 Who has 192.168.1.101? Tell 192.168.1.254
Frame 199: Packet, 223 bytes on wire (1784 bits), 223 bytes captu
Ethernet II, Src: VantivaConne_93:d2:5f (08:c7:f5:93:d2:5f), Dst:
Internet Protocol Version 6, Src: 2001:569:52a1:de00:ac7:f5ff:fe
User Datagram Protocol, Src Port: 53, Dst Port: 53342
Domain Name System (response)
Transaction ID: 0x737a
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 7
Authority RRs: 0
Additional RRs: 0
Queries
Answers
[Request In: 196]
[Time: 13.736000 milliseconds]
0000 2c 98 11 1b 00 4f 08 c7 f5 93 d2 5f 86 dd 60 00 ,....O.. ....._..`.
0010 00 00 00 a9 11 40 20 01 05 69 52 a1 de 00 0a c7 .....@ . .iR.....
0020 f5 ff fe 93 d2 5f 20 01 05 69 52 a1 de 00 8d 71 ....._ . .iR....q
0030 74 f5 2d 17 93 8c 00 35 d0 5e 00 a9 57 ef 73 7a t.-....5 .^..W.sz
0040 81 80 00 01 00 07 00 00 00 00 10 72 65 6d 6f 74 ........ ...remot
0050 65 64 65 73 6b 74 6f 70 2d 70 61 0a 67 6f 6f 67 edesktop -pa.goog
0060 6c 65 61 70 69 73 03 63 6f 6d 00 00 01 00 01 c0 leapis.c om......
0070 0c 00 01 00 01 00 00 00 04 00 04 8e fa 49 4a c0 ........ .....IJ.
0080 0c 00 01 00 01 00 00 00 04 00 04 8e fa 49 8a c0 ........ .....I..
0090 0c 00 01 00 01 00 00 00 04 00 04 8e fa 45 aa c0 ........ .....E..
00a0 0c 00 01 00 01 00 00 00 04 00 04 8e fa 49 6a c0 ........ .....Ij.
00b0 0c 00 01 00 01 00 00 00 04 00 04 8e fb 2d 8a c0 ........ .....-..
00c0 0c 00 01 00 01 00 00 00 04 00 04 8e fb 22 ca c0 ........ ....."..
00d0 0c 00 01 00 01 00 00 00 04 00 04 8e fb 21 4a ........ .....!J
Identification of transaction (dns.id), 2 bytes
Packets: 1020 · Dropped: 0 (0.0%)
Profile: Default

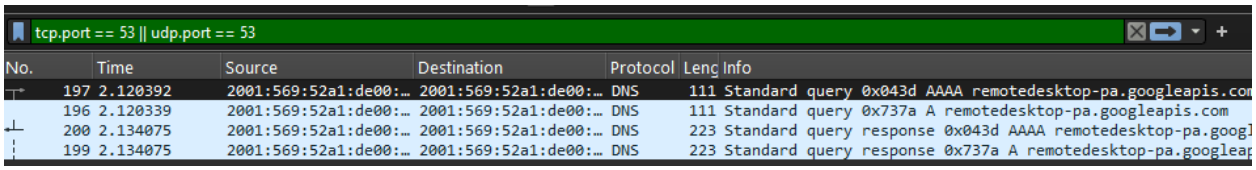
# Section 2

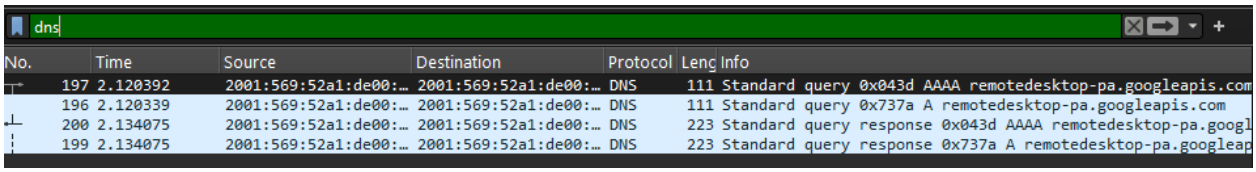

udp.port == 53
No. Time Source Destination Protocol Leng Info
197 2.120392 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 111 Standard query 0x043d AAAA remotedesktop-pa.googleapis.com
196 2.120339 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 111 Standard query 0x737a A remotedesktop-pa.googleapis.com
200 2.134075 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 223 Standard query response 0x043d AAAA remotedesktop-pa.googl
199 2.134075 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 223 Standard query response 0x737a A remotedesktop-pa.googleap

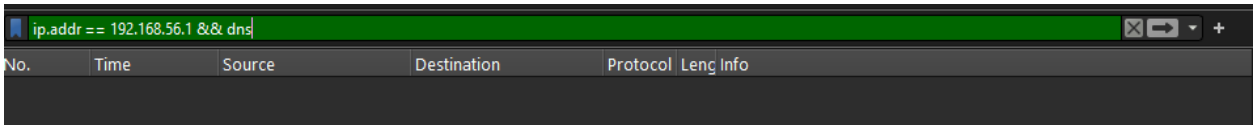

udp.port == 53 && dns
No. Time Source Destination Protocol Leng Info
197 2.120392 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 111 Standard query 0x043d AAAA remotedesktop-pa.googleapis.com
196 2.120339 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 111 Standard query 0x737a A remotedesktop-pa.googleapis.com
200 2.134075 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 223 Standard query response 0x043d AAAA remotedesktop-pa.googl
199 2.134075 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 223 Standard query response 0x737a A remotedesktop-pa.googleap

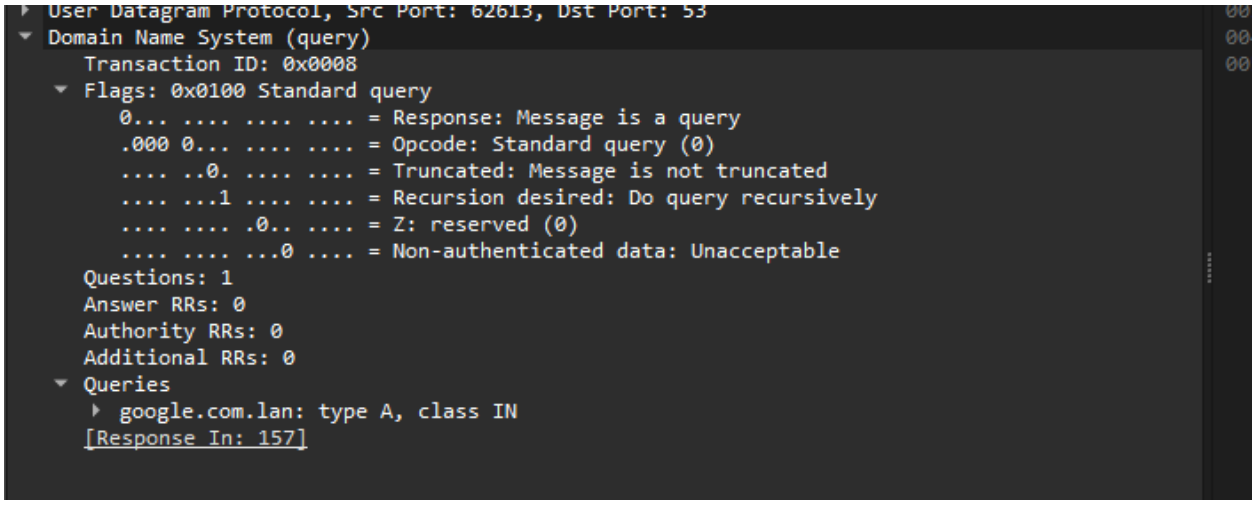

tcp.port == 53
No. Time Source Destination Protocol Leng Info


tcp.port == 53 && dns
dns
dnsserver
No. Time Destination Protocol Leng Info

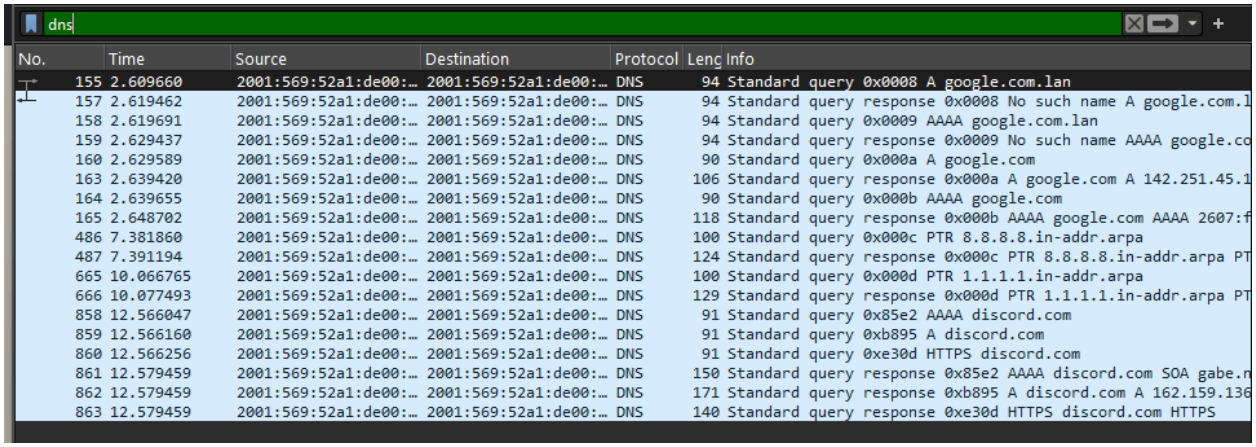

tcp.port == 53 || udp.port == 53
No. Time Source Destination Protocol Leng Info
197 2.120392 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 111 Standard query 0x043d AAAA remotedesktop-pa.googleapis.com
196 2.120339 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 111 Standard query 0x737a A remotedesktop-pa.googleapis.com
200 2.134075 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 223 Standard query response 0x043d AAAA remotedesktop-pa.googl
199 2.134075 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 223 Standard query response 0x737a A remotedesktop-pa.googleap

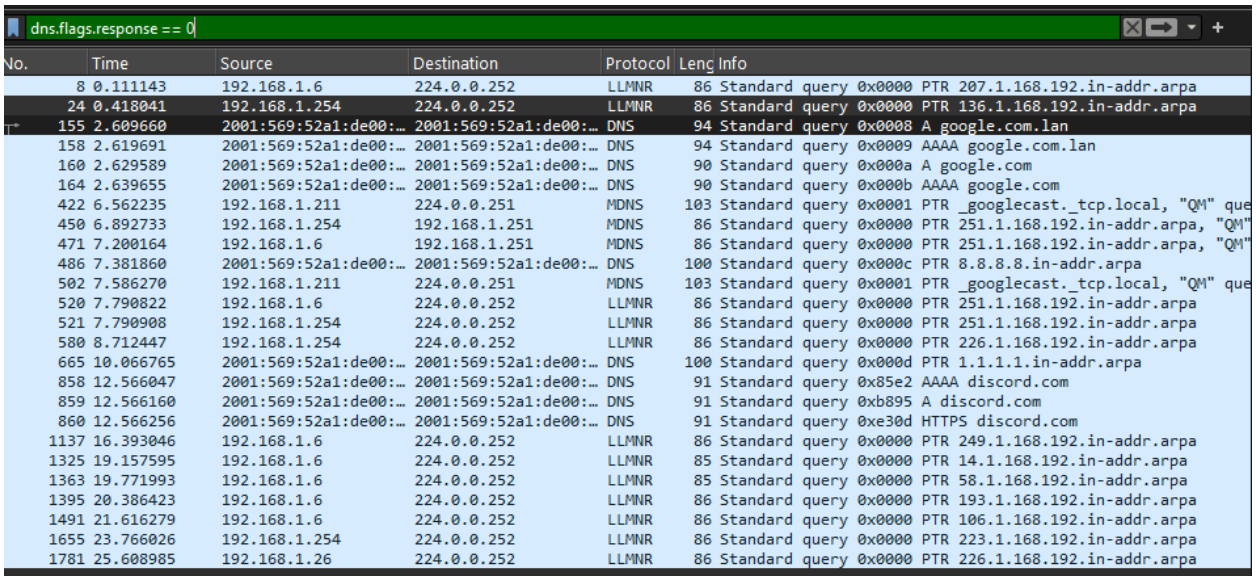

dns
No. Time Source Destination Protocol Leng Info
197 2.120392 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 111 Standard query 0x043d AAAA remotedesktop-pa.googleapis.com
196 2.120339 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 111 Standard query 0x737a A remotedesktop-pa.googleapis.com
200 2.134075 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 223 Standard query response 0x043d AAAA remotedesktop-pa.googl
199 2.134075 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 223 Standard query response 0x737a A remotedesktop-pa.googleap

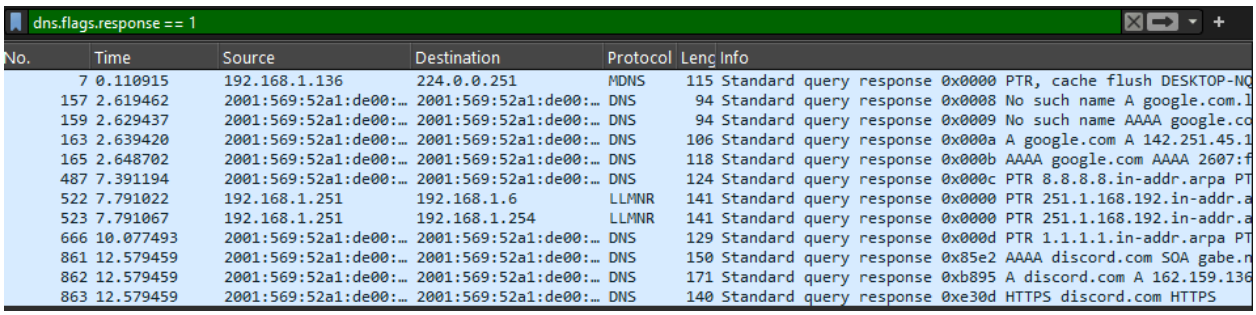

ip.addr == 192.168.56.1 && dns
No. Time Source Destination Protocol Leng Info

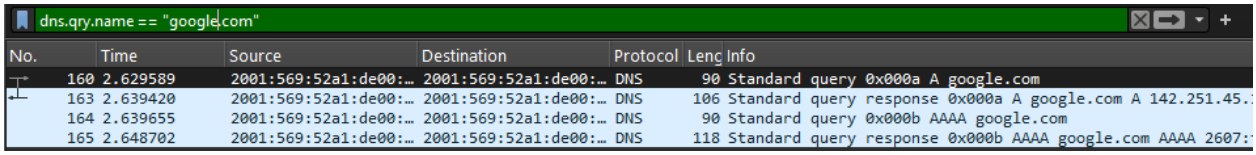

User Datagram Protocol, Src Port: 62613, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x0008
Flags: 0x0100 Standard query
0... .... .... .... = Response: Message is a query
.000 0... .... .... = Opcode: Standard query (0)
.... ..0. .... .... = Truncated: Message is not truncated
.... ...1 .... .... = Recursion desired: Do query recursively
.... .... .0.. .... = Z: reserved (0)
.... .... ...0 .... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
google.com.lan: type A, class IN
[Response In: 157]

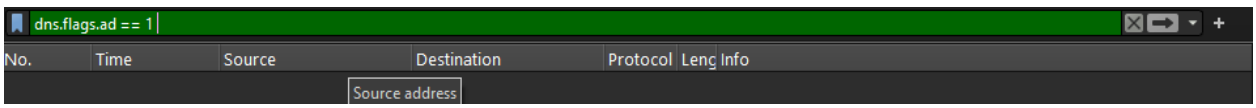
# Section 3


dns
No. Time Source Destination Protocol Leng Info
155 2.609660 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 94 Standard query 0x0008 A google.com.lan
157 2.619462 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 94 Standard query response 0x0008 No such name A google.com.l
158 2.619691 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 94 Standard query 0x0009 AAAA google.com.lan
159 2.629437 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 94 Standard query response 0x0009 No such name AAAA google.co
160 2.629589 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 90 Standard query 0x000a A google.com
163 2.639420 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 106 Standard query response 0x000a A google.com A 142.251.45.1
164 2.639655 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 90 Standard query 0x000b AAAA google.com
165 2.648702 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 118 Standard query response 0x000b AAAA google.com AAAA 2607:f
486 7.381860 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 100 Standard query 0x000c PTR 8.8.8.8.in-addr.arpa
487 7.391194 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 124 Standard query response 0x000c PTR 8.8.8.8.in-addr.arpa PT
665 10.066765 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 100 Standard query 0x000d PTR 1.1.1.1.in-addr.arpa
666 10.077493 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 129 Standard query response 0x000d PTR 1.1.1.1.in-addr.arpa PT
858 12.566047 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 91 Standard query 0x85e2 AAAA discord.com
859 12.566160 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 91 Standard query 0xb895 A discord.com
860 12.566256 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 91 Standard query 0xe30d HTTPS discord.com
861 12.579459 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 150 Standard query response 0x85e2 AAAA discord.com SOA gabe.n
862 12.579459 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 171 Standard query response 0xb895 A discord.com A 162.159.136
863 12.579459 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 140 Standard query response 0xe30d HTTPS discord.com HTTPS


dns.flags.response == 0
No. Time Source Destination Protocol Leng Info
8 0.111143 192.168.1.6 224.0.0.252 LLMNR 86 Standard query 0x0000 PTR 207.1.168.192.in-addr.arpa
24 0.418041 192.168.1.254 224.0.0.252 LLMNR 86 Standard query 0x0000 PTR 136.1.168.192.in-addr.arpa
155 2.609660 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 94 Standard query 0x0008 A google.com.lan
158 2.619691 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 94 Standard query 0x0009 AAAA google.com.lan
160 2.629589 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 90 Standard query 0x000a A google.com
164 2.639655 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 90 Standard query 0x000b AAAA google.com
422 6.562235 192.168.1.211 224.0.0.251 MDNS 103 Standard query 0x0001 PTR _googlecast._tcp.local, "QM" que
450 6.892733 192.168.1.254 192.168.1.251 MDNS 86 Standard query 0x0000 PTR 251.1.168.192.in-addr.arpa, "QM"
471 7.200164 192.168.1.6 192.168.1.251 MDNS 86 Standard query 0x0000 PTR 251.1.168.192.in-addr.arpa, "QM"
486 7.381860 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 100 Standard query 0x000c PTR 8.8.8.8.in-addr.arpa
502 7.586270 192.168.1.211 224.0.0.251 MDNS 103 Standard query 0x0001 PTR _googlecast._tcp.local, "QM" que
520 7.790822 192.168.1.6 224.0.0.252 LLMNR 86 Standard query 0x0000 PTR 251.1.168.192.in-addr.arpa
521 7.790908 192.168.1.254 224.0.0.252 LLMNR 86 Standard query 0x0000 PTR 251.1.168.192.in-addr.arpa
580 8.712447 192.168.1.254 224.0.0.252 LLMNR 86 Standard query 0x0000 PTR 226.1.168.192.in-addr.arpa
665 10.066765 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 100 Standard query 0x000d PTR 1.1.1.1.in-addr.arpa
858 12.566047 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 91 Standard query 0x85e2 AAAA discord.com
859 12.566160 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 91 Standard query 0xb895 A discord.com
860 12.566256 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 91 Standard query 0xe30d HTTPS discord.com
1137 16.393046 192.168.1.6 224.0.0.252 LLMNR 86 Standard query 0x0000 PTR 249.1.168.192.in-addr.arpa
1325 19.157595 192.168.1.6 224.0.0.252 LLMNR 85 Standard query 0x0000 PTR 14.1.168.192.in-addr.arpa
1363 19.771993 192.168.1.6 224.0.0.252 LLMNR 85 Standard query 0x0000 PTR 58.1.168.192.in-addr.arpa
1395 20.386423 192.168.1.6 224.0.0.252 LLMNR 86 Standard query 0x0000 PTR 193.1.168.192.in-addr.arpa
1491 21.616279 192.168.1.6 224.0.0.252 LLMNR 86 Standard query 0x0000 PTR 106.1.168.192.in-addr.arpa
1655 23.766026 192.168.1.254 224.0.0.252 LLMNR 86 Standard query 0x0000 PTR 223.1.168.192.in-addr.arpa
1781 25.608985 192.168.1.26 224.0.0.252 LLMNR 86 Standard query 0x0000 PTR 226.1.168.192.in-addr.arpa


dns.flags.response == 1
No. Time Source Destination Protocol Leng Info
7 0.110915 192.168.1.136 224.0.0.251 MDNS 115 Standard query response 0x0000 PTR, cache flush DESKTOP-NQ
157 2.619462 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 94 Standard query response 0x0008 No such name A google.com.l
159 2.629437 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 94 Standard query response 0x0009 No such name AAAA google.co
163 2.639420 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 106 Standard query response 0x000a A google.com A 142.251.45.1
165 2.648702 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 118 Standard query response 0x000b AAAA google.com AAAA 2607:f
487 7.391194 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 124 Standard query response 0x000c PTR 8.8.8.8.in-addr.arpa PT
522 7.791022 192.168.1.251 192.168.1.6 LLMNR 141 Standard query response 0x0000 PTR 251.1.168.192.in-addr.a
523 7.791067 192.168.1.251 192.168.1.254 LLMNR 141 Standard query response 0x0000 PTR 251.1.168.192.in-addr.a
666 10.077493 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 129 Standard query response 0x000d PTR 1.1.1.1.in-addr.arpa PT
861 12.579459 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 150 Standard query response 0x85e2 AAAA discord.com SOA gabe.n
862 12.579459 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 171 Standard query response 0xb895 A discord.com A 162.159.136
863 12.579459 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 140 Standard query response 0xe30d HTTPS discord.com HTTPS


dns.qry.name == "google.com"
No. Time Source Destination Protocol Leng Info
160 2.629589 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 90 Standard query 0x000a A google.com
163 2.639420 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 106 Standard query response 0x000a A google.com A 142.251.45.
164 2.639655 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 90 Standard query 0x000b AAAA google.com
165 2.648702 2001:569:52a1:de00:… 2001:569:52a1:de00:… DNS 118 Standard query response 0x000b AAAA google.com AAAA 2607:


dns.flags.ad == 1
No. Time Source Destination Protocol Leng Info
Source address

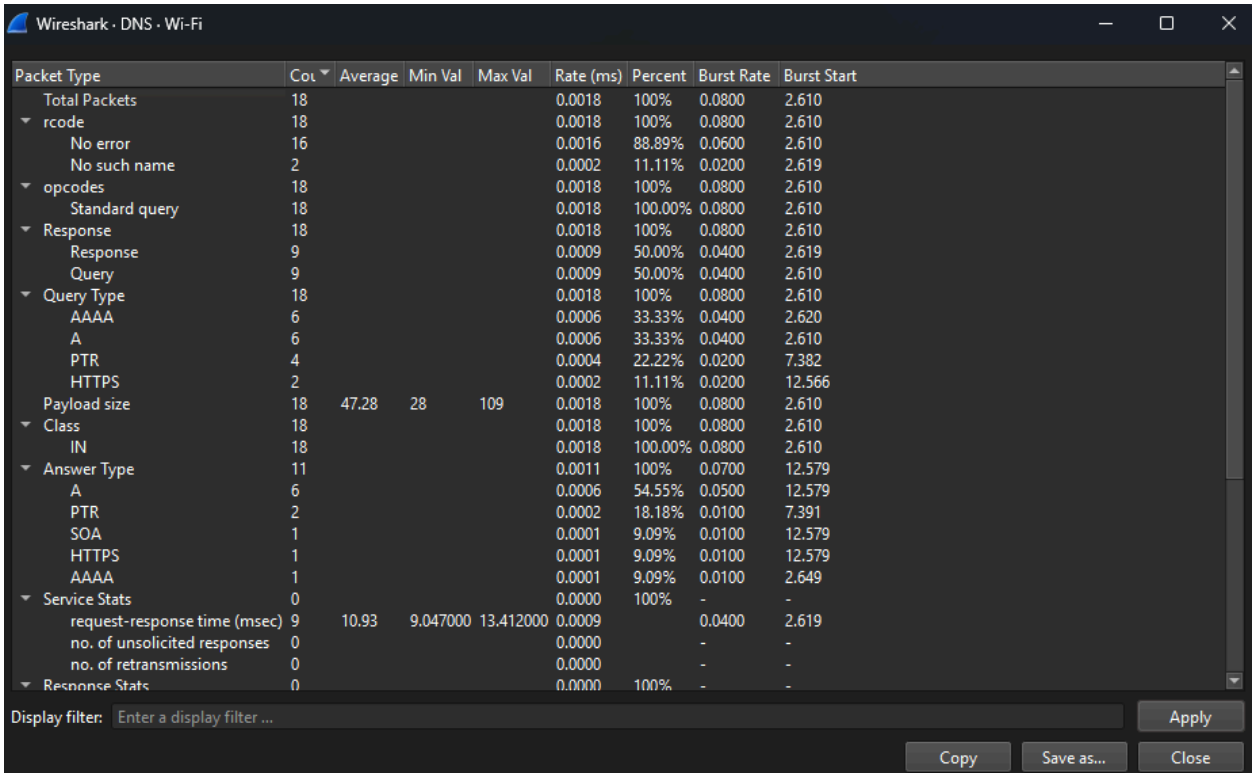
udp.srcport != 53 && dns

| No. | Time | Source | Destination | Protocol | Leng | Info |
|---|---|---|---|---|---|---|
| 155 | 2.609660 | 2001:569:52a1:de00:… | 2001:569:52a1:de00:… | DNS | 94 | Standard query 0x0008 A google.com.lan |
| 158 | 2.619691 | 2001:569:52a1:de00:… | 2001:569:52a1:de00:… | DNS | 94 | Standard query 0x0009 AAAA google.com.lan |
| 160 | 2.629589 | 2001:569:52a1:de00:… | 2001:569:52a1:de00:… | DNS | 90 | Standard query 0x000a A google.com |
| 164 | 2.639655 | 2001:569:52a1:de00:… | 2001:569:52a1:de00:… | DNS | 90 | Standard query 0x000b AAAA google.com |
| 486 | 7.381860 | 2001:569:52a1:de00:… | 2001:569:52a1:de00:… | DNS | 100 | Standard query 0x000c PTR 8.8.8.8.in-addr.arpa |
| 665 | 10.066765 | 2001:569:52a1:de00:… | 2001:569:52a1:de00:… | DNS | 100 | Standard query 0x000d PTR 1.1.1.1.in-addr.arpa |
| 858 | 12.566047 | 2001:569:52a1:de00:… | 2001:569:52a1:de00:… | DNS | 91 | Standard query 0x85e2 AAAA discord.com |
| 859 | 12.566160 | 2001:569:52a1:de00:… | 2001:569:52a1:de00:… | DNS | 91 | Standard query 0xb895 A discord.com |
| 860 | 12.566256 | 2001:569:52a1:de00:… | 2001:569:52a1:de00:… | DNS | 91 | Standard query 0xe30d HTTPS discord.com |

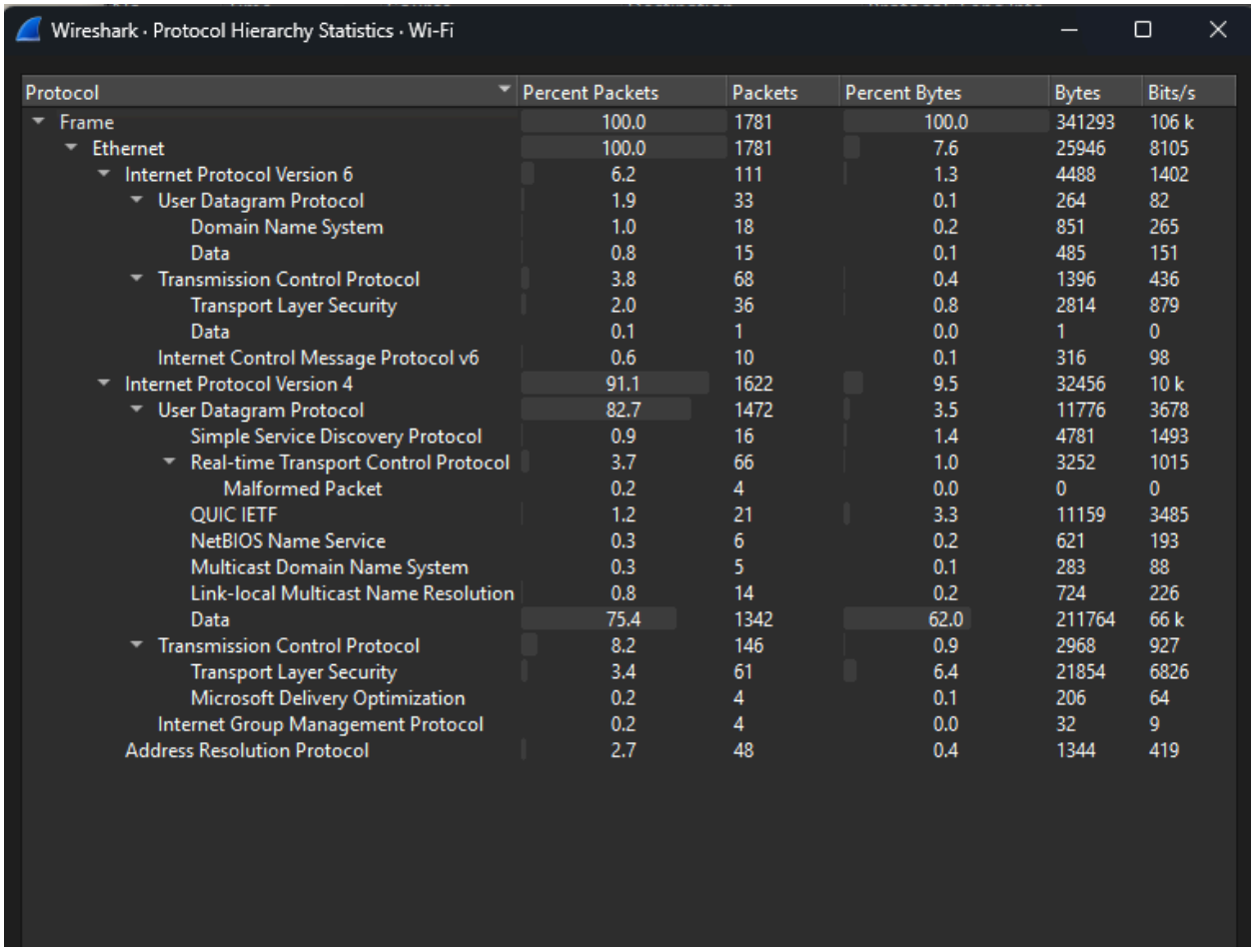
dns.count.answers > 0

| No. | Time | Source | Destination | Protocol | Leng | Info |
|---|---|---|---|---|---|---|
| 7 | 0.110915 | 192.168.1.136 | 224.0.0.251 | MDNS | 115 | Standard query response 0x0000 PTR, cache flush DESKTOP-NQ |
| 163 | 2.639420 | 2001:569:52a1:de00:… | 2001:569:52a1:de00:… | DNS | 106 | Standard query response 0x000a A google.com A 142.251.45.1 |
| 165 | 2.648702 | 2001:569:52a1:de00:… | 2001:569:52a1:de00:… | DNS | 118 | Standard query response 0x000b AAAA google.com AAAA 2607:f |
| 487 | 7.391194 | 2001:569:52a1:de00:… | 2001:569:52a1:de00:… | DNS | 124 | Standard query response 0x000c PTR 8.8.8.8.in-addr.arpa PT |
| 522 | 7.791022 | 192.168.1.251 | 192.168.1.6 | LLMNR | 141 | Standard query response 0x0000 PTR 251.1.168.192.in-addr.a |
| 523 | 7.791067 | 192.168.1.251 | 192.168.1.254 | LLMNR | 141 | Standard query response 0x0000 PTR 251.1.168.192.in-addr.a |
| 666 | 10.077493 | 2001:569:52a1:de00:… | 2001:569:52a1:de00:… | DNS | 129 | Standard query response 0x000d PTR 1.1.1.1.in-addr.arpa PT |
| 862 | 12.579459 | 2001:569:52a1:de00:… | 2001:569:52a1:de00:… | DNS | 171 | Standard query response 0xb895 A discord.com A 162.159.136 |
| 863 | 12.579459 | 2001:569:52a1:de00:… | 2001:569:52a1:de00:… | DNS | 140 | Standard query response 0xe30d HTTPS discord.com HTTPS |

# Section 4




| Packet Type | Cou | Average | Min Val | Max Val | Rate (ms) | Percent | Burst Rate | Burst Start |
|---|---|---|---|---|---|---|---|---|
| Total Packets | 18 | | | | 0.0018 | 100% | 0.0800 | 2.610 |
| rcode | 18 | | | | 0.0018 | 100% | 0.0800 | 2.610 |
| No error | 16 | | | | 0.0016 | 88.89% | 0.0600 | 2.610 |
| No such name | 2 | | | | 0.0002 | 11.11% | 0.0200 | 2.619 |
| opcodes | 18 | | | | 0.0018 | 100% | 0.0800 | 2.610 |
| Standard query | 18 | | | | 0.0018 | 100.00% | 0.0800 | 2.610 |
| Response | 18 | | | | 0.0018 | 100% | 0.0800 | 2.610 |
| Response | 9 | | | | 0.0009 | 50.00% | 0.0400 | 2.619 |
| Query | 9 | | | | 0.0009 | 50.00% | 0.0400 | 2.610 |
| Query Type | 18 | | | | 0.0018 | 100% | 0.0800 | 2.610 |
| AAAA | 6 | | | | 0.0006 | 33.33% | 0.0400 | 2.620 |
| A | 6 | | | | 0.0006 | 33.33% | 0.0400 | 2.610 |
| PTR | 4 | | | | 0.0004 | 22.22% | 0.0200 | 7.382 |
| HTTPS | 2 | | | | 0.0002 | 11.11% | 0.0200 | 12.566 |
| Payload size | 18 | 47.28 | 28 | 109 | 0.0018 | 100% | 0.0800 | 2.610 |
| Class | 18 | | | | 0.0018 | 100% | 0.0800 | 2.610 |
| IN | 18 | | | | 0.0018 | 100.00% | 0.0800 | 2.610 |
| Answer Type | 11 | | | | 0.0011 | 100% | 0.0700 | 12.579 |
| A | 6 | | | | 0.0006 | 54.55% | 0.0500 | 12.579 |
| PTR | 2 | | | | 0.0002 | 18.18% | 0.0100 | 7.391 |
| SOA | 1 | | | | 0.0001 | 9.09% | 0.0100 | 12.579 |
| HTTPS | 1 | | | | 0.0001 | 9.09% | 0.0100 | 12.579 |
| AAAA | 1 | | | | 0.0001 | 9.09% | 0.0100 | 2.649 |
| Service Stats | 0 | | | | 0.0000 | 100% | - | - |
| request-response time (msec) | 9 | 10.93 | 9.047000 | 13.412000 | 0.0009 | | 0.0400 | 2.619 |
| no. of unsolicited responses | 0 | | | | 0.0000 | | - | - |
| no. of retransmissions | 0 | | | | 0.0000 | | - | - |
| Response Stats | 0 | | | | 0.0000 | 100% | - | - |



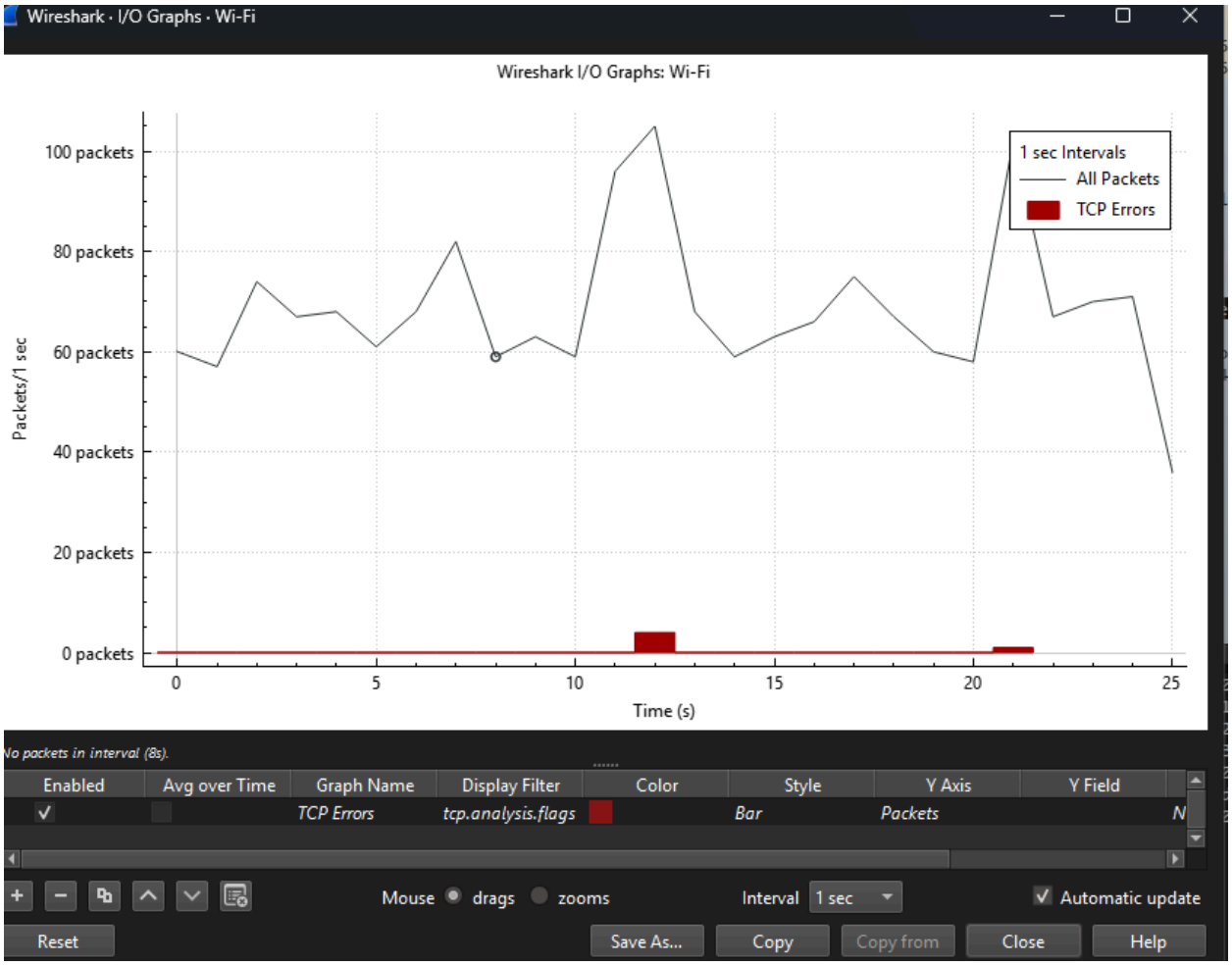

| Protocol | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s |
|---|---|---|---|---|---|
| Frame | 100.0 | 1781 | 100.0 | 341293 | 106 k |
| Ethernet | 100.0 | 1781 | 7.6 | 25946 | 8105 |
| Internet Protocol Version 6 | 6.2 | 111 | 1.3 | 4488 | 1402 |
| User Datagram Protocol | 1.9 | 33 | 0.1 | 264 | 82 |
| Domain Name System | 1.0 | 18 | 0.2 | 851 | 265 |
| Data | 0.8 | 15 | 0.1 | 485 | 151 |
| Transmission Control Protocol | 3.8 | 68 | 0.4 | 1396 | 436 |
| Transport Layer Security | 2.0 | 36 | 0.8 | 2814 | 879 |
| Data | 0.1 | 1 | 0.0 | 1 | 0 |
| Internet Control Message Protocol v6 | 0.6 | 10 | 0.1 | 316 | 98 |
| Internet Protocol Version 4 | 91.1 | 1622 | 9.5 | 32456 | 10 k |
| User Datagram Protocol | 82.7 | 1472 | 3.5 | 11776 | 3678 |
| Simple Service Discovery Protocol | 0.9 | 16 | 1.4 | 4781 | 1493 |
| Real-time Transport Control Protocol | 3.7 | 66 | 1.0 | 3252 | 1015 |
| Malformed Packet | 0.2 | 4 | 0.0 | 0 | 0 |
| QUIC IETF | 1.2 | 21 | 3.3 | 11159 | 3485 |
| NetBIOS Name Service | 0.3 | 6 | 0.2 | 621 | 193 |
| Multicast Domain Name System | 0.3 | 5 | 0.1 | 283 | 88 |
| Link-local Multicast Name Resolution | 0.8 | 14 | 0.2 | 724 | 226 |
| Data | 75.4 | 1342 | 62.0 | 211764 | 66 k |
| Transmission Control Protocol | 8.2 | 146 | 0.9 | 2968 | 927 |
| Transport Layer Security | 3.4 | 61 | 6.4 | 21854 | 6826 |
| Microsoft Delivery Optimization | 0.2 | 4 | 0.1 | 206 | 64 |
| Internet Group Management Protocol | 0.2 | 4 | 0.0 | 32 | 9 |
| Address Resolution Protocol | 2.7 | 48 | 0.4 | 1344 | 419 |

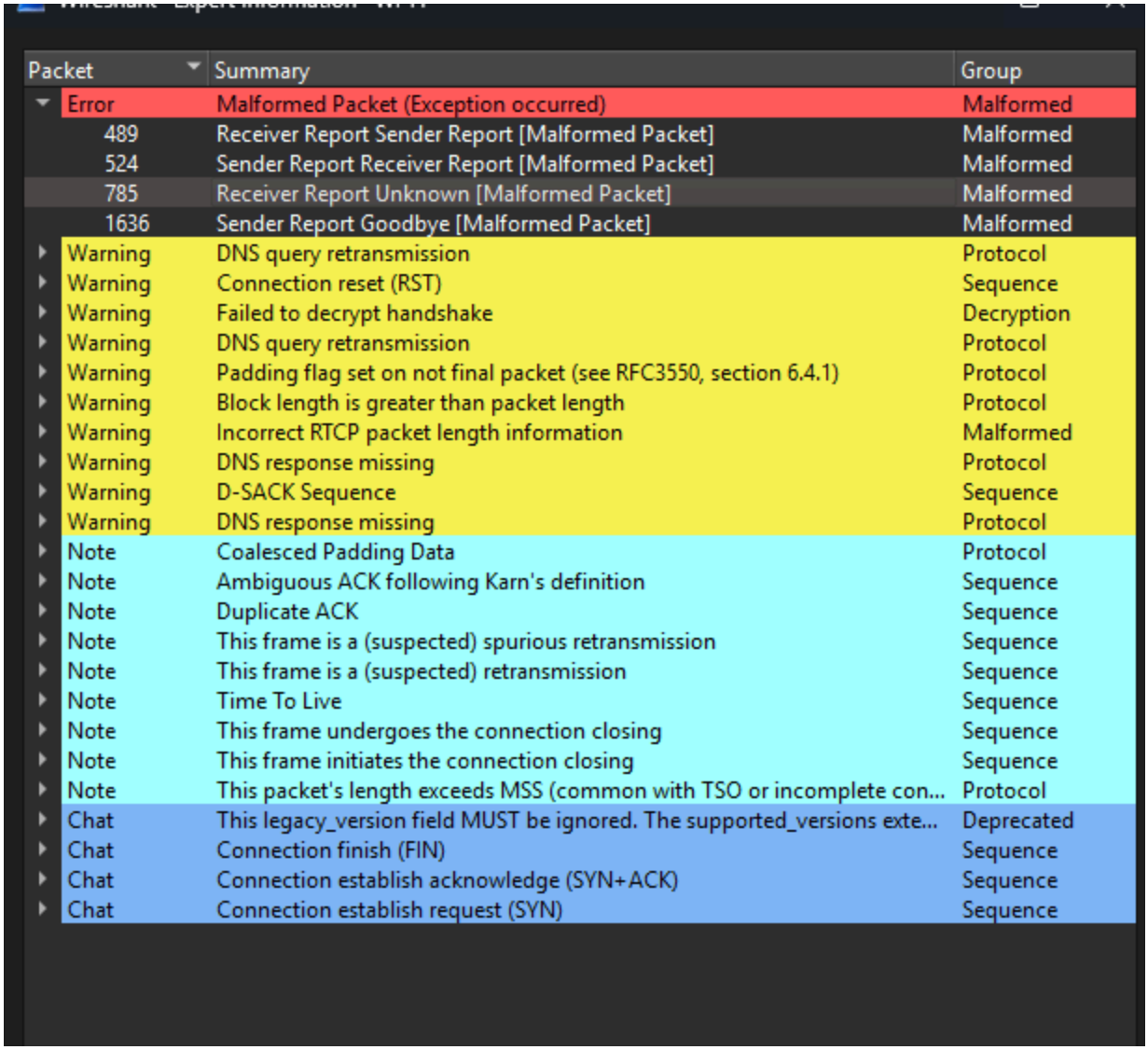
Ethernet · 23 | IPv4 · 30 | IPv6 · 18 | TCP · 21 | UDP · 35

| Address A | Port A | Address B | Port B | Packets | Bytes |
|---|---|---|---|---|---|
| 162.159.136.234 | 443 | 192.168.1.251 | 65289 | 74 | 10819 |
| 192.168.1.251 | 58149 | 3.233.44.150 | 443 | 6 | 399 |
| 192.168.1.251 | 58151 | 18.213.94.234 | 443 | 6 | 413 |
| 192.168.1.251 | 58160 | 34.107.243.93 | 443 | 3 | 240 |
| 192.168.1.251 | 53720 | 34.195.60.101 | 443 | 6 | 399 |
| 192.168.1.251 | 58144 | 34.239.10.16 | 443 | 6 | 399 |
| 192.168.1.251 | 58150 | 44.216.141.0 | 443 | 6 | 399 |
| 192.168.1.251 | 65438 | 54.205.201.147 | 443 | 26 | 14742 |
| 192.168.1.251 | 65437 | 192.168.1.193 | 7680 | 11 | 824 |
| 192.168.1.251 | 51115 | 205.196.6.132 | 443 | 2 | 168 |

Ethernet · 23 | IPv4 · 30 | IPv6 · 18 | TCP · 21 | UDP · 35

| Address A | Port A | Address B | Port B | Packets | Bytes |
|---|---|---|---|---|---|
| 104.29.154.60 | 19321 | 192.168.1.251 | 63132 | 69 | 8886 |
| 104.29.159.107 | 19309 | 192.168.1.251 | 50116 | 849 | 167778 |
| 192.168.1.6 | 36931 | 192.168.1.251 | 5353 | 1 | 86 |
| 192.168.1.6 | 45140 | 192.168.1.251 | 137 | 2 | 291 |
| 192.168.1.6 | 5355 | 224.0.0.252 | 5355 | 7 | 600 |
| 192.168.1.14 | 40901 | 239.255.255.250 | 8082 | 9 | 5310 |
| 192.168.1.26 | 47447 | 192.168.1.251 | 137 | 2 | 291 |
| 192.168.1.26 | 5355 | 224.0.0.252 | 5355 | 1 | 86 |
| 192.168.1.136 | 5353 | 224.0.0.251 | 5353 | 1 | 115 |
| 192.168.1.211 | 5353 | 224.0.0.251 | 5353 | 2 | 206 |
| 192.168.1.211 | 49842 | 239.255.255.250 | 1900 | 1 | 60 |
| 192.168.1.211 | 50593 | 239.255.255.250 | 1900 | 6 | 1002 |
| 192.168.1.211 | 63101 | 239.255.255.250 | 1900 | 1 | 60 |





| Packet | Summary | Group |
|---|---|---|
| Error | Malformed Packet (Exception occurred) | Malformed |
| 489 | Receiver Report Sender Report [Malformed Packet] | Malformed |
| 524 | Sender Report Receiver Report [Malformed Packet] | Malformed |
| 785 | Receiver Report Unknown [Malformed Packet] | Malformed |
| 1636 | Sender Report Goodbye [Malformed Packet] | Malformed |
| Warning | DNS query retransmission | Protocol |
| Warning | Connection reset (RST) | Sequence |
| Warning | Failed to decrypt handshake | Decryption |
| Warning | DNS query retransmission | Protocol |
| Warning | Padding flag set on not final packet (see RFC3550, section 6.4.1) | Protocol |
| Warning | Block length is greater than packet length | Protocol |
| Warning | Incorrect RTCP packet length information | Malformed |
| Warning | DNS response missing | Protocol |
| Warning | D-SACK Sequence | Sequence |
| Warning | DNS response missing | Protocol |
| Note | Coalesced Padding Data | Protocol |
| Note | Ambiguous ACK following Karn's definition | Sequence |
| Note | Duplicate ACK | Sequence |
| Note | This frame is a (suspected) spurious retransmission | Sequence |
| Note | This frame is a (suspected) retransmission | Sequence |
| Note | Time To Live | Sequence |
| Note | This frame undergoes the connection closing | Sequence |
| Note | This frame initiates the connection closing | Sequence |
| Note | This packet's length exceeds MSS (common with TSO or incomplete con... | Protocol |
| Chat | This legacy_version field MUST be ignored. The supported_versions exte... | Deprecated |
| Chat | Connection finish (FIN) | Sequence |
| Chat | Connection establish acknowledge (SYN+ACK) | Sequence |
| Chat | Connection establish request (SYN) | Sequence |

# Section 7-1

## dns_early_response

| Packet No | Type of Anomaly | Evidence in Packet | Suggested Mitigation |
|---|---|---|---|
| 2 | Early response | It is before the query | Enable DNSSEC validation |

## dns_poisoning

| Packet No | Type of Anomaly | Evidence in Packet | Suggested Mitigation |
|---|---|---|---|
| 2 | Response time over WAN is unrealistically fast | Response time is 800 micro seconds<br>Expert information highlights there is not DNS response | DNSSEC: cryptographic signatures for authenticity & integrity<br><br>Randomization of transaction IDs & source port<br><br>Restrict open resolvers<br><br>Deep Packet Inspection & TXT Volume Monitoring<br><br>Rate limiting & firewalls for suspicious DNS traffic |

## dns_suspicious_port

| Packet No | Type of Anomaly | Evidence in Packet | Suggested Mitigation |
|---|---|---|---|
| 2 | Wrong src port | Src port: 9999 instead of 53 | Block DNS response from non 53 ports, DNSSEC |

dns_txid_mismatch

| Packet No | Type of Anomaly | Evidence in Packet | Suggested Mitigation |
|---|---|---|---|
| 2 | Transaction ID mismatch | 0x0000 in query<br>0x9999 in response | Enable DNSSEC validation<br>Randomization of transaction IDs & source ports |

# Section 7-2

1. Using dns, how many DNS packets are in the capture?
    9
2. Apply dns.flags.response == 0. Which domains were queried?
    5
3. Apply dns.flags.response == 1. What were the responses?
    6
4. Look at the TXID values. Do all queries and responses match correctly?
    Packet 4 is mismatching
5. Use udp.srcport != 53 && dns. Which packets appear suspicious? Why?
    Packet 4
6. Which response looks like a DNS poisoning attempt? Explain.
    Packer 4 with a mismatch source ip to response to a DNS query
7. How could DNSSEC prevent this type of attack?
    DNSSEC ensures that
    The DNS data was created by the real domain owner
    The data was not modified in transit
    Forged responses are detected and rejected