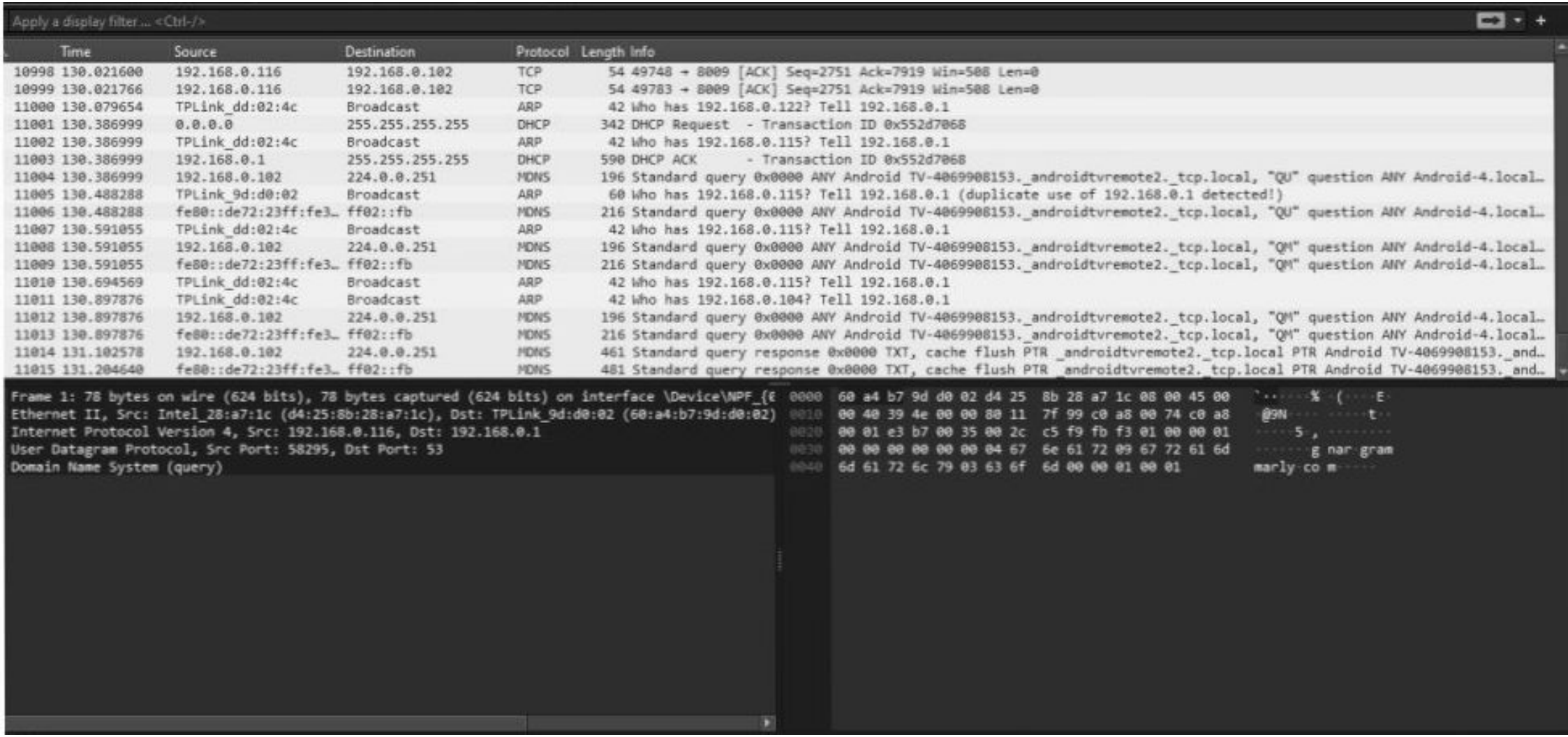
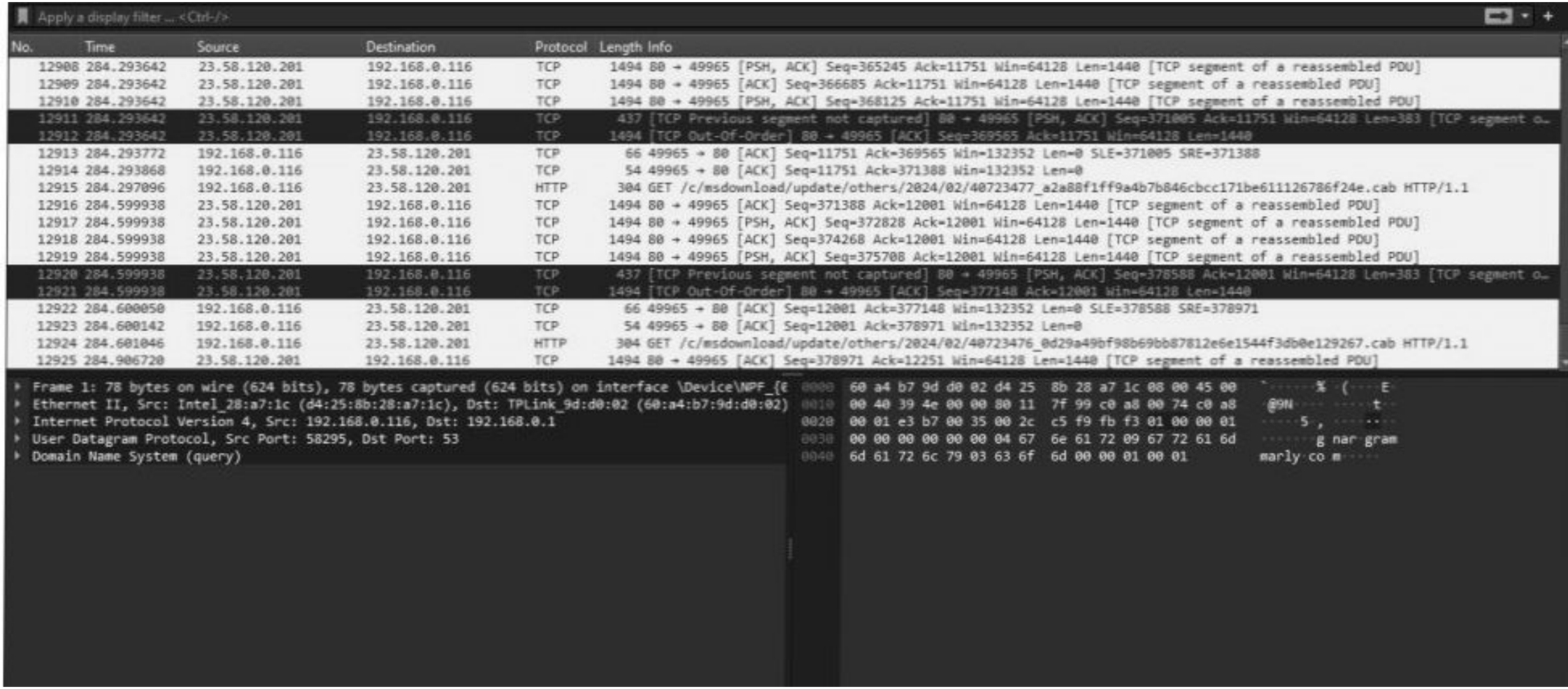
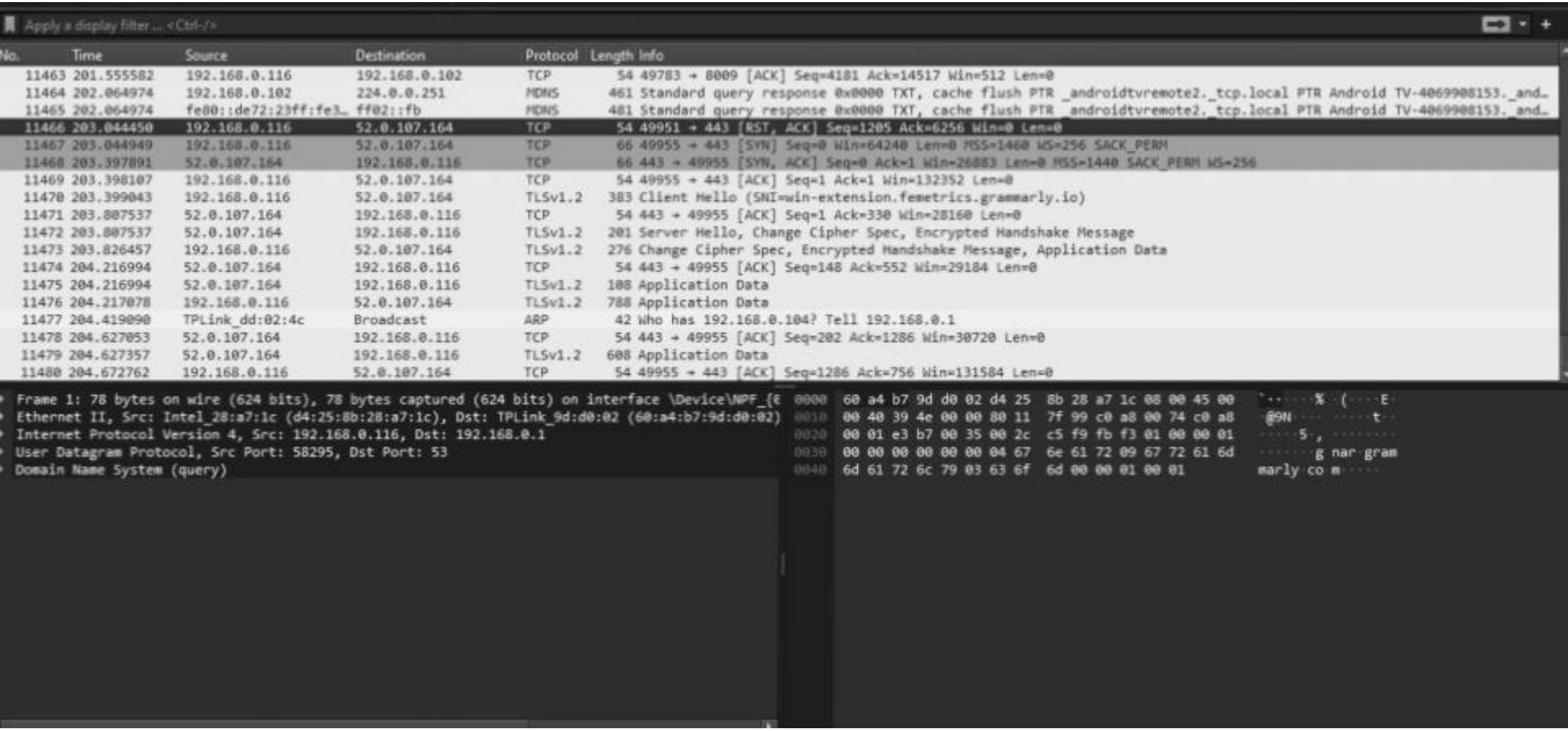
Wireshark

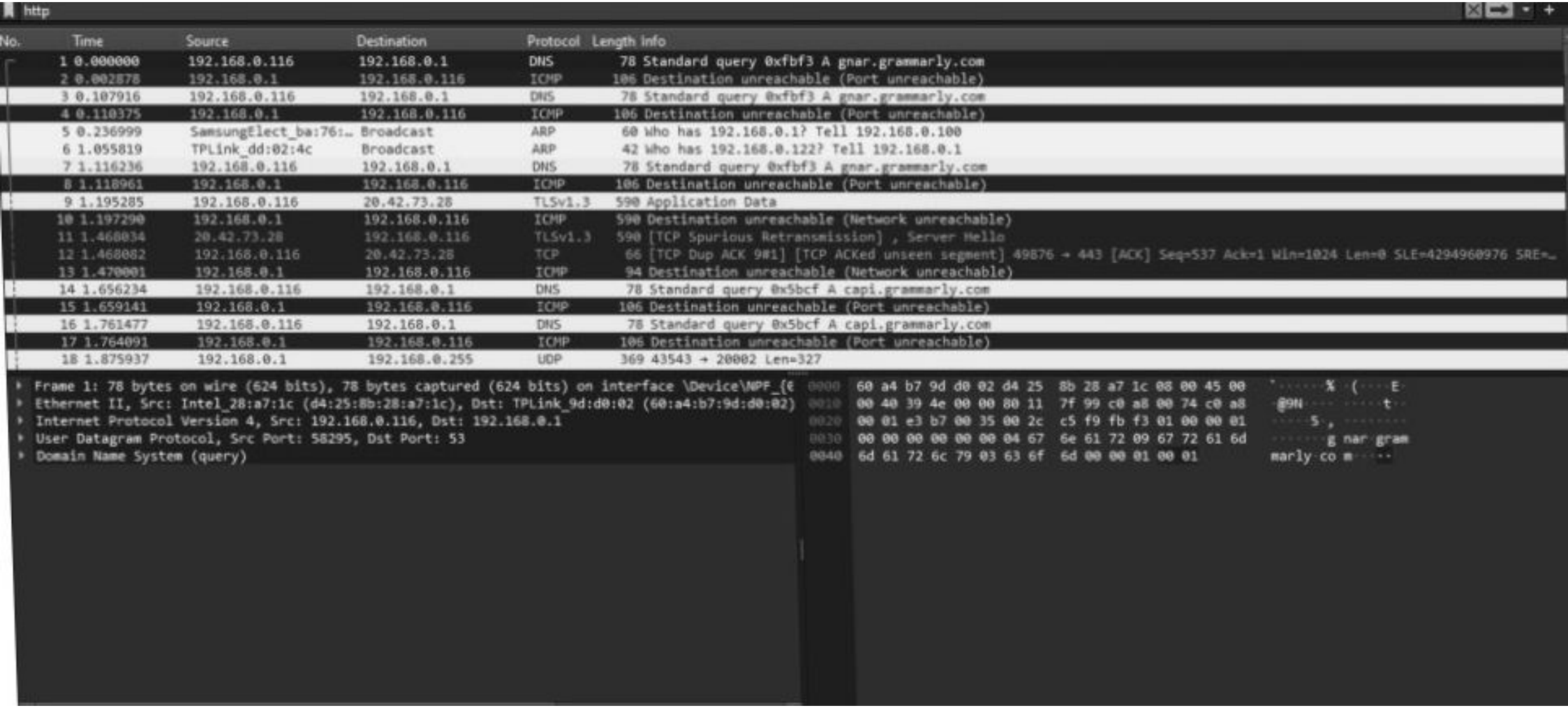
Submitted by

Zahed Hosen
MC 223104


Apply a display filter ... <Ctrl-/>
Time Source Destination Protocol Length Info
10998 130.021600 192.168.0.116 192.168.0.102 TCP 54 49748 → 8009 [ACK] Seq=2751 Ack=7919 Win=508 Len=0
10999 130.021766 192.168.0.116 192.168.0.102 TCP 54 49783 → 8009 [ACK] Seq=2751 Ack=7919 Win=508 Len=0
11000 130.079654 TPLink_dd:02:4c Broadcast ARP 42 Who has 192.168.0.122? Tell 192.168.0.1
11001 130.386999 0.0.0.0 255.255.255.255 DHCP 342 DHCP Request - Transaction ID 0x552d7068
11002 130.386999 TPLink_dd:02:4c Broadcast ARP 42 Who has 192.168.0.115? Tell 192.168.0.1
11003 130.386999 192.168.0.1 255.255.255.255 DHCP 590 DHCP ACK - Transaction ID 0x552d7068
11004 130.386999 192.168.0.102 224.0.0.251 MDNS 196 Standard query 0x0000 ANY Android TV-4069908153._androidtvremote2._tcp.local, "QU" question ANY Android-4.local…
11005 130.488288 TPLink_9d:d0:02 Broadcast ARP 60 Who has 192.168.0.115? Tell 192.168.0.1 (duplicate use of 192.168.0.1 detected!)
11006 130.488288 fe80::de72:23ff:fe3… ff02::fb MDNS 216 Standard query 0x0000 ANY Android TV-4069908153._androidtvremote2._tcp.local, "QU" question ANY Android-4.local…
11007 130.591055 TPLink_dd:02:4c Broadcast ARP 42 Who has 192.168.0.115? Tell 192.168.0.1
11008 130.591055 192.168.0.102 224.0.0.251 MDNS 196 Standard query 0x0000 ANY Android TV-4069908153._androidtvremote2._tcp.local, "QM" question ANY Android-4.local…
11009 130.591055 fe80::de72:23ff:fe3… ff02::fb MDNS 216 Standard query 0x0000 ANY Android TV-4069908153._androidtvremote2._tcp.local, "QM" question ANY Android-4.local…
11010 130.694569 TPLink_dd:02:4c Broadcast ARP 42 Who has 192.168.0.115? Tell 192.168.0.1
11011 130.897876 TPLink_dd:02:4c Broadcast ARP 42 Who has 192.168.0.104? Tell 192.168.0.1
11012 130.897876 192.168.0.102 224.0.0.251 MDNS 196 Standard query 0x0000 ANY Android TV-4069908153._androidtvremote2._tcp.local, "QM" question ANY Android-4.local…
11013 130.897876 fe80::de72:23ff:fe3… ff02::fb MDNS 216 Standard query 0x0000 ANY Android TV-4069908153._androidtvremote2._tcp.local, "QM" question ANY Android-4.local…
11014 131.102578 192.168.0.102 224.0.0.251 MDNS 461 Standard query response 0x0000 TXT, cache flush PTR _androidtvremote2._tcp.local PTR Android TV-4069908153._and…
11015 131.204640 fe80::de72:23ff:fe3… ff02::fb MDNS 481 Standard query response 0x0000 TXT, cache flush PTR _androidtvremote2._tcp.local PTR Android TV-4069908153._and…
Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{E
Ethernet II, Src: Intel_28:a7:1c (d4:25:8b:28:a7:1c), Dst: TPLink_9d:d0:02 (60:a4:b7:9d:d0:02)
Internet Protocol Version 4, Src: 192.168.0.116, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 58295, Dst Port: 53
Domain Name System (query)
0000 60 a4 b7 9d d0 02 d4 25 8b 28 a7 1c 08 00 45 00
0010 00 40 39 4e 00 00 80 11 7f 99 c0 a8 00 74 c0 a8
0020 00 01 e3 b7 00 35 00 2c c5 f9 fb f3 01 00 00 01
0030 00 00 00 00 00 00 04 67 6e 61 72 09 67 72 61 6d
0040 6d 61 72 6c 79 03 63 6f 6d 00 00 01 00 01


Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
12908 284.293642 23.58.120.201 192.168.0.116 TCP 1494 80 → 49965 [PSH, ACK] Seq=365245 Ack=11751 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
12909 284.293642 23.58.120.201 192.168.0.116 TCP 1494 80 → 49965 [ACK] Seq=366685 Ack=11751 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
12910 284.293642 23.58.120.201 192.168.0.116 TCP 1494 80 → 49965 [PSH, ACK] Seq=368125 Ack=11751 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
12911 284.293642 23.58.120.201 192.168.0.116 TCP 437 [TCP Previous segment not captured] 80 → 49965 [PSH, ACK] Seq=371005 Ack=11751 Win=64128 Len=383 [TCP segment o…
12912 284.293642 23.58.120.201 192.168.0.116 TCP 1494 [TCP Out-Of-Order] 80 → 49965 [ACK] Seq=369565 Ack=11751 Win=64128 Len=1440
12913 284.293772 192.168.0.116 23.58.120.201 TCP 66 49965 → 80 [ACK] Seq=11751 Ack=369565 Win=132352 Len=0 SLE=371005 SRE=371388
12914 284.293868 192.168.0.116 23.58.120.201 TCP 54 49965 → 80 [ACK] Seq=11751 Ack=371388 Win=132352 Len=0
12915 284.297096 192.168.0.116 23.58.120.201 HTTP 304 GET /c/msdownload/update/others/2024/02/40723477_a2a88f1ff9a4b7b846cbcc171be611126786f24e.cab HTTP/1.1
12916 284.599938 23.58.120.201 192.168.0.116 TCP 1494 80 → 49965 [ACK] Seq=371388 Ack=12001 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
12917 284.599938 23.58.120.201 192.168.0.116 TCP 1494 80 → 49965 [PSH, ACK] Seq=372828 Ack=12001 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
12918 284.599938 23.58.120.201 192.168.0.116 TCP 1494 80 → 49965 [ACK] Seq=374268 Ack=12001 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
12919 284.599938 23.58.120.201 192.168.0.116 TCP 1494 80 → 49965 [PSH, ACK] Seq=375708 Ack=12001 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
12920 284.599938 23.58.120.201 192.168.0.116 TCP 437 [TCP Previous segment not captured] 80 → 49965 [PSH, ACK] Seq=378588 Ack=12001 Win=64128 Len=383 [TCP segment o…
12921 284.599938 23.58.120.201 192.168.0.116 TCP 1494 [TCP Out-Of-Order] 80 → 49965 [ACK] Seq=377148 Ack=12001 Win=64128 Len=1440
12922 284.600050 192.168.0.116 23.58.120.201 TCP 66 49965 → 80 [ACK] Seq=12001 Ack=377148 Win=132352 Len=0 SLE=378588 SRE=378971
12923 284.600142 192.168.0.116 23.58.120.201 TCP 54 49965 → 80 [ACK] Seq=12001 Ack=378971 Win=132352 Len=0
12924 284.601046 192.168.0.116 23.58.120.201 HTTP 304 GET /c/msdownload/update/others/2024/02/40723476_0d29a49bf98b69bb87812e6e1544f3db0e129267.cab HTTP/1.1
12925 284.906720 23.58.120.201 192.168.0.116 TCP 1494 80 → 49965 [ACK] Seq=378971 Ack=12251 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{E
Ethernet II, Src: Intel_28:a7:1c (d4:25:8b:28:a7:1c), Dst: TPLink_9d:d0:02 (60:a4:b7:9d:d0:02)
Internet Protocol Version 4, Src: 192.168.0.116, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 58295, Dst Port: 53
Domain Name System (query)
0000 60 a4 b7 9d d0 02 d4 25 8b 28 a7 1c 08 00 45 00
0010 00 40 39 4e 00 00 80 11 7f 99 c0 a8 00 74 c0 a8
0020 00 01 e3 b7 00 35 00 2c c5 f9 fb f3 01 00 00 01
0030 00 00 00 00 00 00 04 67 6e 61 72 09 67 72 61 6d
0040 6d 61 72 6c 79 03 63 6f 6d 00 00 01 00 01


Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
11463 201.555582 192.168.0.116 192.168.0.102 TCP 54 49783 → 8009 [ACK] Seq=4181 Ack=14517 Win=512 Len=0
11464 202.064974 192.168.0.102 224.0.0.251 MDNS 461 Standard query response 0x0000 TXT, cache flush PTR _androidtvremote2._tcp.local PTR Android TV-4069908153._and…
11465 202.064974 fe80::de72:23ff:fe3… ff02::fb MDNS 481 Standard query response 0x0000 TXT, cache flush PTR _androidtvremote2._tcp.local PTR Android TV-4069908153._and…
11466 203.044450 192.168.0.116 52.0.107.164 TCP 54 49951 → 443 [RST, ACK] Seq=1205 Ack=6256 Win=0 Len=0
11467 203.044949 192.168.0.116 52.0.107.164 TCP 66 49955 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
11468 203.397891 52.0.107.164 192.168.0.116 TCP 66 443 → 49955 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1440 SACK_PERM WS=256
11469 203.398107 192.168.0.116 52.0.107.164 TCP 54 49955 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
11470 203.399043 192.168.0.116 52.0.107.164 TLSv1.2 383 Client Hello (SNI=win-extension.femetrics.grammarly.io)
11471 203.807537 52.0.107.164 192.168.0.116 TCP 54 443 → 49955 [ACK] Seq=1 Ack=330 Win=28160 Len=0
11472 203.807537 52.0.107.164 192.168.0.116 TLSv1.2 201 Server Hello, Change Cipher Spec, Encrypted Handshake Message
11473 203.826457 192.168.0.116 52.0.107.164 TLSv1.2 276 Change Cipher Spec, Encrypted Handshake Message, Application Data
11474 204.216994 52.0.107.164 192.168.0.116 TCP 54 443 → 49955 [ACK] Seq=148 Ack=552 Win=29184 Len=0
11475 204.216994 52.0.107.164 192.168.0.116 TLSv1.2 108 Application Data
11476 204.217078 192.168.0.116 52.0.107.164 TLSv1.2 788 Application Data
11477 204.419090 TPLink_dd:02:4c Broadcast ARP 42 Who has 192.168.0.104? Tell 192.168.0.1
11478 204.627053 52.0.107.164 192.168.0.116 TCP 54 443 → 49955 [ACK] Seq=202 Ack=1286 Win=30720 Len=0
11479 204.627357 52.0.107.164 192.168.0.116 TLSv1.2 608 Application Data
11480 204.672762 192.168.0.116 52.0.107.164 TCP 54 49955 → 443 [ACK] Seq=1286 Ack=756 Win=131584 Len=0
Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{E
Ethernet II, Src: Intel_28:a7:1c (d4:25:8b:28:a7:1c), Dst: TPLink_9d:d0:02 (60:a4:b7:9d:d0:02)
Internet Protocol Version 4, Src: 192.168.0.116, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 58295, Dst Port: 53
Domain Name System (query)
0000 60 a4 b7 9d d0 02 d4 25 8b 28 a7 1c 08 00 45 00
0010 00 40 39 4e 00 00 80 11 7f 99 c0 a8 00 74 c0 a8
0020 00 01 e3 b7 00 35 00 2c c5 f9 fb f3 01 00 00 01
0030 00 00 00 00 00 00 04 67 6e 61 72 09 67 72 61 6d
0040 6d 61 72 6c 79 03 63 6f 6d 00 00 01 00 01


http
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.0.116 192.168.0.1 DNS 78 Standard query 0xfbf3 A gnar.grammarly.com
2 0.002878 192.168.0.1 192.168.0.116 ICMP 106 Destination unreachable (Port unreachable)
3 0.107916 192.168.0.116 192.168.0.1 DNS 78 Standard query 0xfbf3 A gnar.grammarly.com
4 0.110375 192.168.0.1 192.168.0.116 ICMP 106 Destination unreachable (Port unreachable)
5 0.236999 SamsungElect_ba:76:… Broadcast ARP 60 Who has 192.168.0.1? Tell 192.168.0.100
6 1.055819 TPLink_dd:02:4c Broadcast ARP 42 Who has 192.168.0.122? Tell 192.168.0.1
7 1.116236 192.168.0.116 192.168.0.1 DNS 78 Standard query 0xfbf3 A gnar.grammarly.com
8 1.118961 192.168.0.1 192.168.0.116 ICMP 106 Destination unreachable (Port unreachable)
9 1.195285 192.168.0.116 20.42.73.28 TLSv1.3 590 Application Data
10 1.197290 192.168.0.1 192.168.0.116 ICMP 590 Destination unreachable (Network unreachable)
11 1.460034 20.42.73.28 192.168.0.116 TLSv1.3 590 [TCP Spurious Retransmission] , Server Hello
12 1.460082 192.168.0.116 20.42.73.28 TCP 66 [TCP Dup ACK 9#1] [TCP ACKed unseen segment] 49876 → 443 [ACK] Seq=537 Ack=1 Win=1024 Len=0 SLE=4294960976 SRE=…
13 1.470001 192.168.0.1 192.168.0.116 ICMP 94 Destination unreachable (Network unreachable)
14 1.656234 192.168.0.116 192.168.0.1 DNS 78 Standard query 0x5bcf A capi.grammarly.com
15 1.659141 192.168.0.1 192.168.0.116 ICMP 106 Destination unreachable (Port unreachable)
16 1.761477 192.168.0.116 192.168.0.1 DNS 78 Standard query 0x5bcf A capi.grammarly.com
17 1.764091 192.168.0.1 192.168.0.116 ICMP 106 Destination unreachable (Port unreachable)
18 1.875937 192.168.0.1 192.168.0.255 UDP 369 43543 → 20002 Len=327
Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{
Ethernet II, Src: Intel_28:a7:1c (d4:25:8b:28:a7:1c), Dst: TPLink_9d:d0:02 (60:a4:b7:9d:d0:02)
Internet Protocol Version 4, Src: 192.168.0.116, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 58295, Dst Port: 53
Domain Name System (query)
0000 60 a4 b7 9d d0 02 d4 25 8b 28 a7 1c 08 00 45 00
0010 00 40 39 4e 00 00 80 11 7f 99 c0 a8 00 74 c0 a8
0020 00 01 e3 b7 00 35 00 2c c5 f9 fb f3 01 00 00 01
0030 00 00 00 00 00 00 04 67 6e 61 72 09 67 72 61 6d
0040 6d 61 72 6c 79 03 63 6f 6d 00 00 01 00 01