Step 1: Open the Wireshark

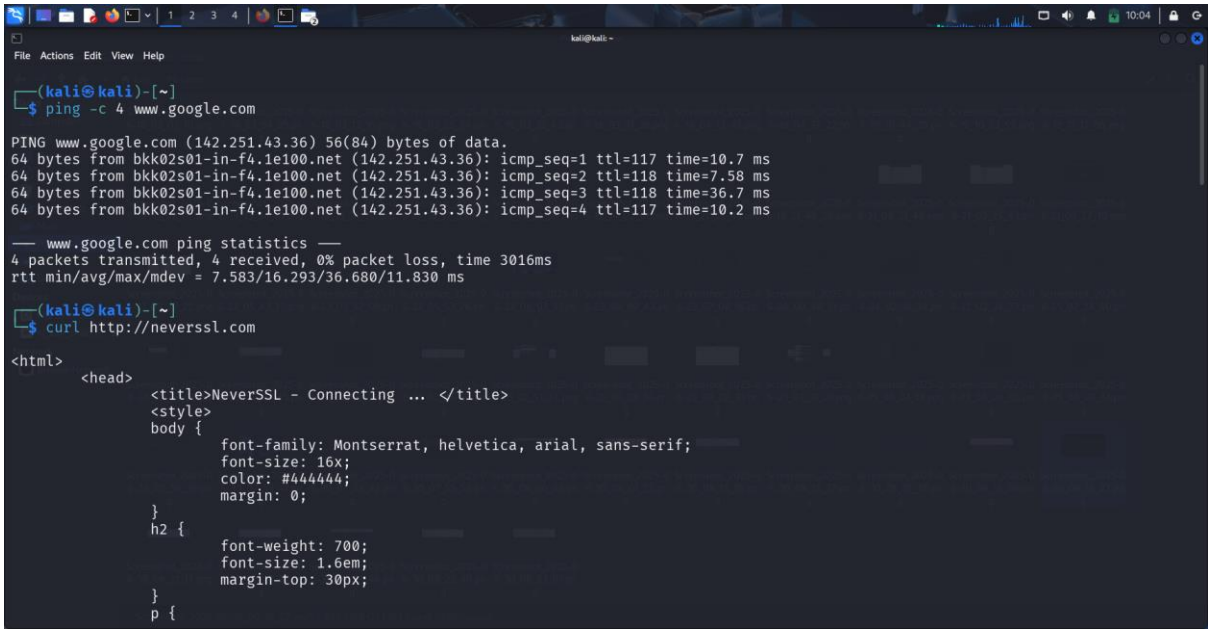
Step 2: Select the active network interface (ethO)

Step 3: Open a terminal and run:

ping google.com

http://neverssl.com

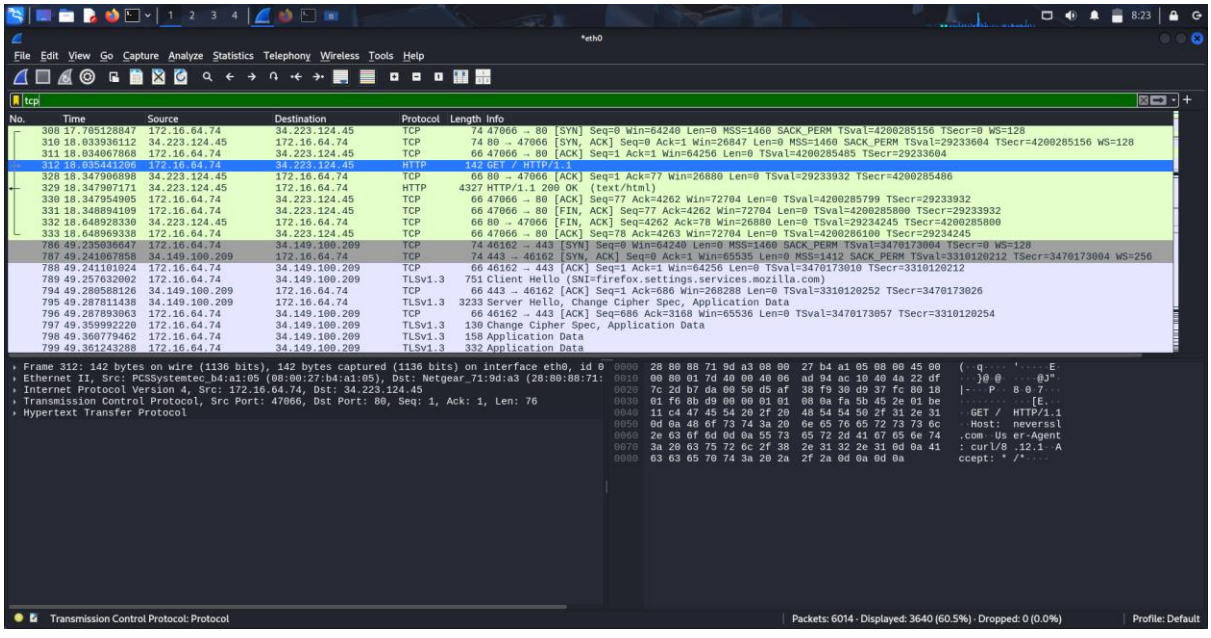
https://www.google.com

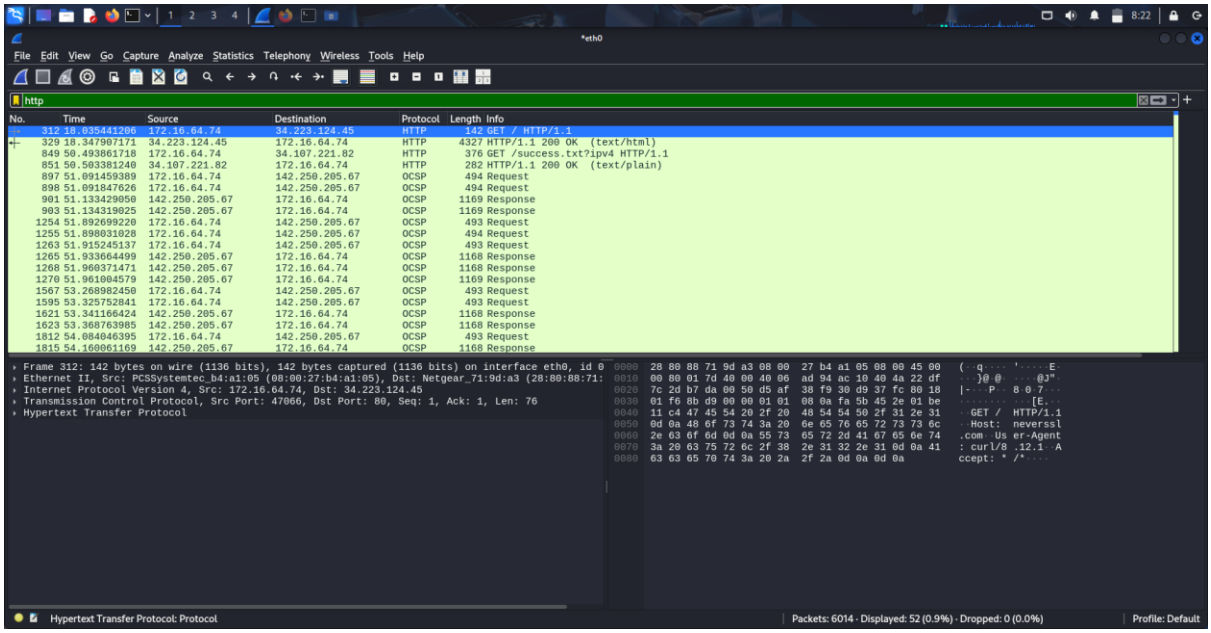


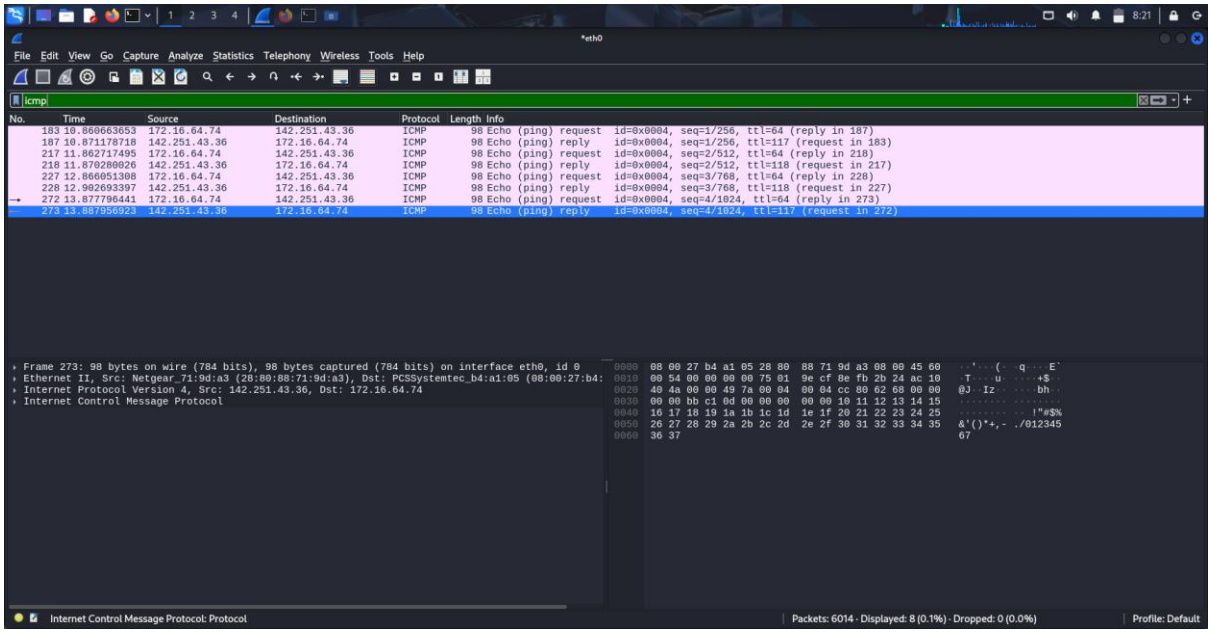
Step 4: Stop Packet Capture

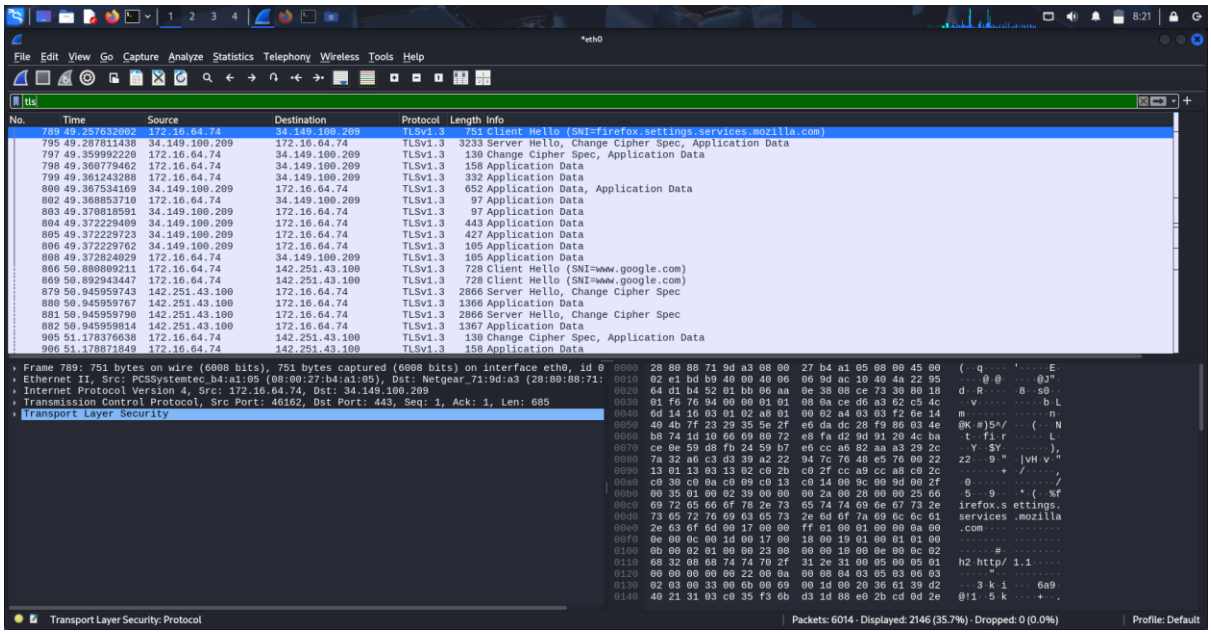
Step 5: Apply the Protocol Filter

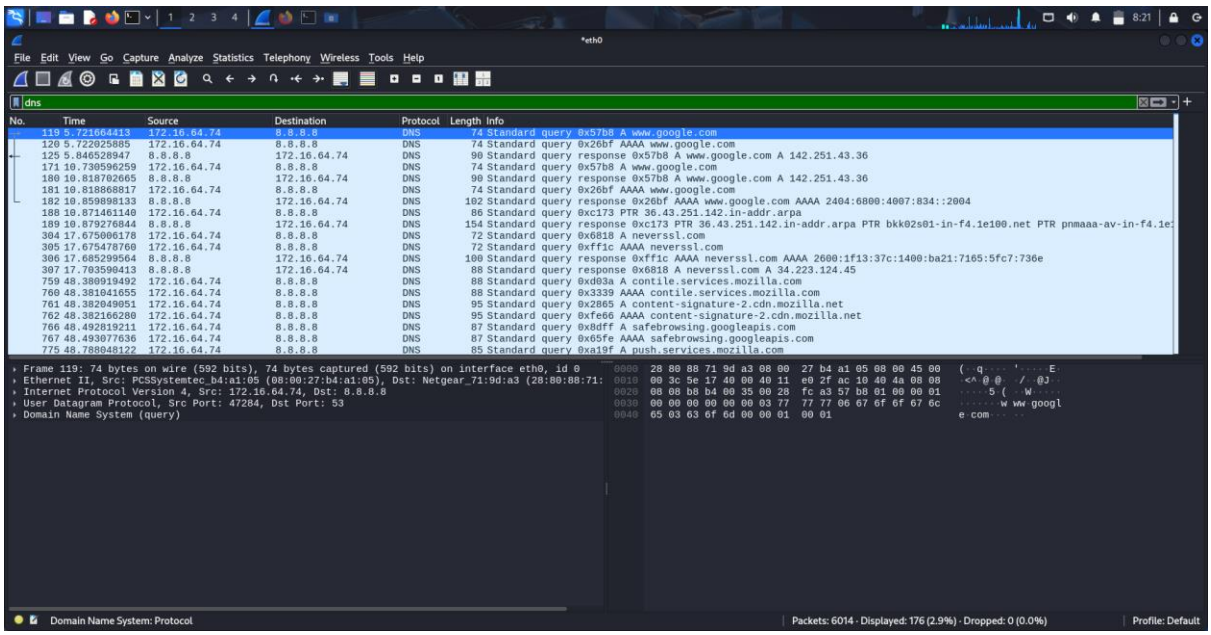
Use the **Display Filter Bar** at the top to filter traffic:




*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
312 18.035441206 172.16.64.74 34.223.124.45 HTTP 142 GET / HTTP/1.1
329 18.347907171 34.223.124.45 172.16.64.74 HTTP 4327 HTTP/1.1 200 OK (text/html)
849 50.493861718 172.16.64.74 34.107.221.82 HTTP 376 GET /success.txt?ipv4 HTTP/1.1
851 50.503381240 34.107.221.82 172.16.64.74 HTTP 282 HTTP/1.1 200 OK (text/plain)
897 51.091459389 172.16.64.74 142.250.205.67 OCSP 494 Request
898 51.091847626 172.16.64.74 142.250.205.67 OCSP 494 Request
901 51.133429050 142.250.205.67 172.16.64.74 OCSP 1169 Response
903 51.134319025 142.250.205.67 172.16.64.74 OCSP 1169 Response
1254 51.892699220 172.16.64.74 142.250.205.67 OCSP 493 Request
1255 51.898031028 172.16.64.74 142.250.205.67 OCSP 494 Request
1263 51.915245137 172.16.64.74 142.250.205.67 OCSP 493 Request
1265 51.933664499 142.250.205.67 172.16.64.74 OCSP 1168 Response
1268 51.960371471 142.250.205.67 172.16.64.74 OCSP 1168 Response
1270 51.961004579 142.250.205.67 172.16.64.74 OCSP 1169 Response
1567 53.268982450 172.16.64.74 142.250.205.67 OCSP 493 Request
1595 53.325752841 172.16.64.74 142.250.205.67 OCSP 493 Request
1621 53.341166424 142.250.205.67 172.16.64.74 OCSP 1168 Response
1623 53.368763985 142.250.205.67 172.16.64.74 OCSP 1168 Response
1812 54.084046395 172.16.64.74 142.250.205.67 OCSP 493 Request
1815 54.160061169 142.250.205.67 172.16.64.74 OCSP 1168 Response
Frame 312: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_b4:a1:05 (08:00:27:b4:a1:05), Dst: Netgear_71:9d:a3 (28:80:88:71:
Internet Protocol Version 4, Src: 172.16.64.74, Dst: 34.223.124.45
Transmission Control Protocol, Src Port: 47066, Dst Port: 80, Seq: 1, Ack: 1, Len: 76
Hypertext Transfer Protocol
0000 28 80 88 71 9d a3 08 00 27 b4 a1 05 08 00 45 00
0010 00 80 01 7d 40 00 40 06 ad 94 ac 10 40 4a 22 df
0020 7c 2d b7 da 00 50 d5 af 38 f9 30 d9 37 fc 80 18
0030 01 f6 8b d9 00 00 01 01 08 0a fa 5b 45 2e 01 be
0040 11 c4 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31
0050 0d 0a 48 6f 73 74 3a 20 6e 65 76 65 72 73 73 6c
0060 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74
0070 3a 20 63 75 72 6c 2f 38 2e 31 32 2e 31 0d 0a 41
0080 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 0d 0a
Hypertext Transfer Protocol: Protocol
Packets: 6014 · Displayed: 52 (0.9%) · Dropped: 0 (0.0%)
Profile: Default


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
183 10.860663653 172.16.64.74 142.251.43.36 ICMP 98 Echo (ping) request id=0x0004, seq=1/256, ttl=64 (reply in 187)
187 10.871178718 142.251.43.36 172.16.64.74 ICMP 98 Echo (ping) reply id=0x0004, seq=1/256, ttl=117 (request in 183)
217 11.862717495 172.16.64.74 142.251.43.36 ICMP 98 Echo (ping) request id=0x0004, seq=2/512, ttl=64 (reply in 218)
218 11.870280026 142.251.43.36 172.16.64.74 ICMP 98 Echo (ping) reply id=0x0004, seq=2/512, ttl=118 (request in 217)
227 12.866051308 172.16.64.74 142.251.43.36 ICMP 98 Echo (ping) request id=0x0004, seq=3/768, ttl=64 (reply in 228)
228 12.902693397 142.251.43.36 172.16.64.74 ICMP 98 Echo (ping) reply id=0x0004, seq=3/768, ttl=118 (request in 227)
272 13.877796441 172.16.64.74 142.251.43.36 ICMP 98 Echo (ping) request id=0x0004, seq=4/1024, ttl=64 (reply in 273)
273 13.887956923 142.251.43.36 172.16.64.74 ICMP 98 Echo (ping) reply id=0x0004, seq=4/1024, ttl=117 (request in 272)
Frame 273: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
Ethernet II, Src: Netgear_71:9d:a3 (28:80:88:71:9d:a3), Dst: PCSSystemtec_b4:a1:05 (08:00:27:b4:
Internet Protocol Version 4, Src: 142.251.43.36, Dst: 172.16.64.74
Internet Control Message Protocol
0000 08 00 27 b4 a1 05 28 80 88 71 9d a3 08 00 45 60
0010 00 54 00 00 00 00 75 01 9e cf 8e fb 2b 24 ac 10
0020 40 4a 00 00 49 7a 00 04 00 04 cc 80 62 68 00 00
0030 00 00 bb c1 0d 00 00 00 00 00 10 11 12 13 14 15
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
0060 36 37
Internet Control Message Protocol: Protocol
Packets: 6014 · Displayed: 8 (0.1%) · Dropped: 0 (0.0%)
Profile: Default


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls
No. Time Source Destination Protocol Length Info
789 49.257632002 172.16.64.74 34.149.100.209 TLSv1.3 751 Client Hello (SNI=firefox.settings.services.mozilla.com)
795 49.287811438 34.149.100.209 172.16.64.74 TLSv1.3 3233 Server Hello, Change Cipher Spec, Application Data
797 49.359992220 172.16.64.74 34.149.100.209 TLSv1.3 130 Change Cipher Spec, Application Data
798 49.360779462 172.16.64.74 34.149.100.209 TLSv1.3 158 Application Data
799 49.361243288 172.16.64.74 34.149.100.209 TLSv1.3 332 Application Data
800 49.367534169 34.149.100.209 172.16.64.74 TLSv1.3 652 Application Data, Application Data
802 49.368853710 172.16.64.74 34.149.100.209 TLSv1.3 97 Application Data
803 49.370818591 34.149.100.209 172.16.64.74 TLSv1.3 97 Application Data
804 49.372229409 34.149.100.209 172.16.64.74 TLSv1.3 443 Application Data
805 49.372229723 34.149.100.209 172.16.64.74 TLSv1.3 427 Application Data
806 49.372229762 34.149.100.209 172.16.64.74 TLSv1.3 105 Application Data
808 49.372824029 172.16.64.74 34.149.100.209 TLSv1.3 105 Application Data
866 50.880809211 172.16.64.74 142.251.43.100 TLSv1.3 728 Client Hello (SNI=www.google.com)
869 50.892943447 172.16.64.74 142.251.43.100 TLSv1.3 728 Client Hello (SNI=www.google.com)
879 50.945959743 142.251.43.100 172.16.64.74 TLSv1.3 2866 Server Hello, Change Cipher Spec
880 50.945959767 142.251.43.100 172.16.64.74 TLSv1.3 1366 Application Data
881 50.945959790 142.251.43.100 172.16.64.74 TLSv1.3 2866 Server Hello, Change Cipher Spec
882 50.945959814 142.251.43.100 172.16.64.74 TLSv1.3 1367 Application Data
905 51.178376638 172.16.64.74 142.251.43.100 TLSv1.3 130 Change Cipher Spec, Application Data
906 51.178871849 172.16.64.74 142.251.43.100 TLSv1.3 158 Application Data
Frame 789: 751 bytes on wire (6008 bits), 751 bytes captured (6008 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_b4:a1:05 (08:00:27:b4:a1:05), Dst: Netgear_71:9d:a3 (28:80:88:71:
Internet Protocol Version 4, Src: 172.16.64.74, Dst: 34.149.100.209
Transmission Control Protocol, Src Port: 46162, Dst Port: 443, Seq: 1, Ack: 1, Len: 685
Transport Layer Security
Transport Layer Security: Protocol
Packets: 6014 · Displayed: 2146 (35.7%) · Dropped: 0 (0.0%)
Profile: Default


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
119 5.721664413 172.16.64.74 8.8.8.8 DNS 74 Standard query 0x57b8 A www.google.com
120 5.722025885 172.16.64.74 8.8.8.8 DNS 74 Standard query 0x26bf AAAA www.google.com
125 5.846528947 8.8.8.8 172.16.64.74 DNS 90 Standard query response 0x57b8 A www.google.com A 142.251.43.36
171 10.730596259 172.16.64.74 8.8.8.8 DNS 74 Standard query 0x57b8 A www.google.com
180 10.818702665 8.8.8.8 172.16.64.74 DNS 90 Standard query response 0x57b8 A www.google.com A 142.251.43.36
181 10.818868817 172.16.64.74 8.8.8.8 DNS 74 Standard query 0x26bf AAAA www.google.com
182 10.859898133 8.8.8.8 172.16.64.74 DNS 102 Standard query response 0x26bf AAAA www.google.com AAAA 2404:6800:4007:834::2004
188 10.871461140 172.16.64.74 8.8.8.8 DNS 86 Standard query 0xc173 PTR 36.43.251.142.in-addr.arpa
189 10.879276844 8.8.8.8 172.16.64.74 DNS 154 Standard query response 0xc173 PTR 36.43.251.142.in-addr.arpa PTR bkk02s01-in-f4.1e100.net PTR pnmaaa-av-in-f4.1e
304 17.675006178 172.16.64.74 8.8.8.8 DNS 72 Standard query 0x6818 A neverssl.com
305 17.675478760 172.16.64.74 8.8.8.8 DNS 72 Standard query 0xff1c AAAA neverssl.com
306 17.685299564 8.8.8.8 172.16.64.74 DNS 100 Standard query response 0xff1c AAAA neverssl.com AAAA 2600:1f13:37c:1400:ba21:7165:5fc7:736e
307 17.703590413 8.8.8.8 172.16.64.74 DNS 88 Standard query response 0x6818 A neverssl.com A 34.223.124.45
759 48.380919492 172.16.64.74 8.8.8.8 DNS 88 Standard query 0xd03a A contile.services.mozilla.com
760 48.381041655 172.16.64.74 8.8.8.8 DNS 88 Standard query 0x3339 AAAA contile.services.mozilla.com
761 48.382049051 172.16.64.74 8.8.8.8 DNS 95 Standard query 0x2865 A content-signature-2.cdn.mozilla.net
762 48.382166280 172.16.64.74 8.8.8.8 DNS 95 Standard query 0xfe66 AAAA content-signature-2.cdn.mozilla.net
766 48.492819211 172.16.64.74 8.8.8.8 DNS 87 Standard query 0x8dff A safebrowsing.googleapis.com
767 48.493077636 172.16.64.74 8.8.8.8 DNS 87 Standard query 0x65fe AAAA safebrowsing.googleapis.com
775 48.788048122 172.16.64.74 8.8.8.8 DNS 85 Standard query 0xa19f A push.services.mozilla.com
Frame 119: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_b4:a1:05 (08:00:27:b4:a1:05), Dst: Netgear_71:9d:a3 (28:80:88:71:
Internet Protocol Version 4, Src: 172.16.64.74, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 47284, Dst Port: 53
Domain Name System (query)
Domain Name System: Protocol
Packets: 6014 · Displayed: 176 (2.9%) · Dropped: 0 (0.0%)
Profile: Default