Name: Satya chaitanya

Email: satyachaitanya21@gmail.com

Objective: Capture live network packets and identify basic protocols and traffic types

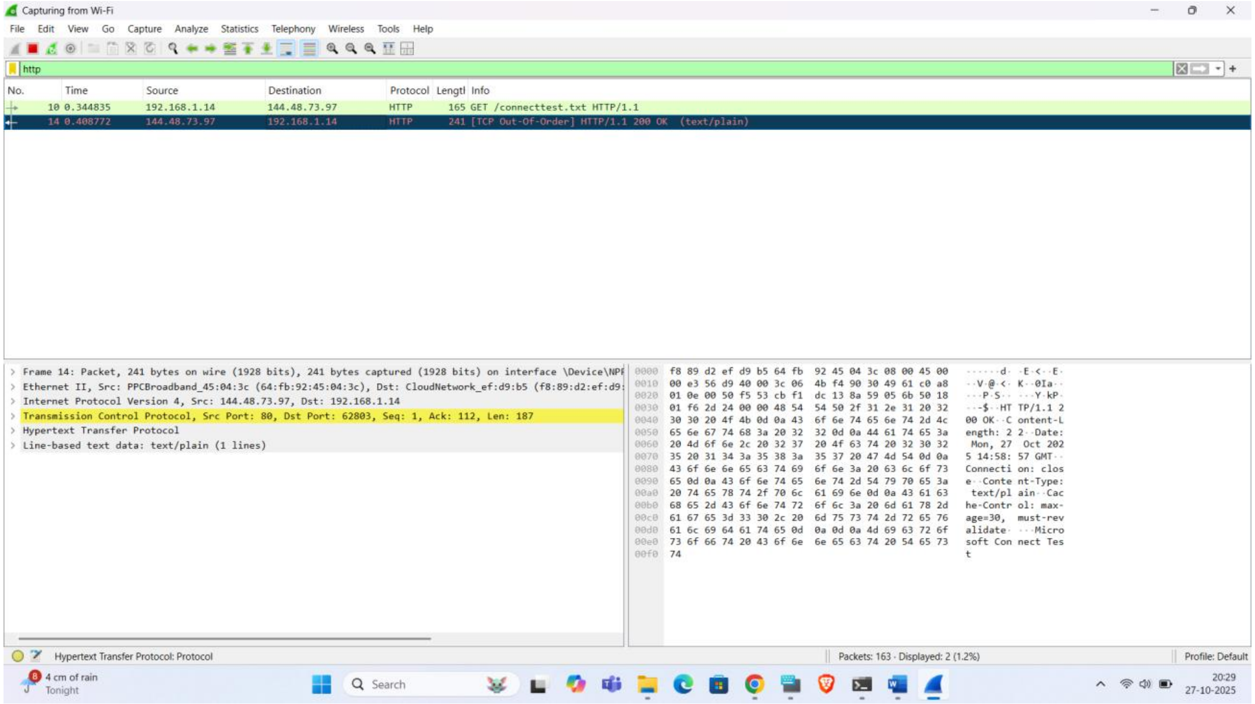
Target ip: 192.168.1.14

Wireshark

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible. You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

Target ports I did http tcp, dns

http packet inspection


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
4 cm of rain
Tonight
Search
20:29
27-10-2025

http

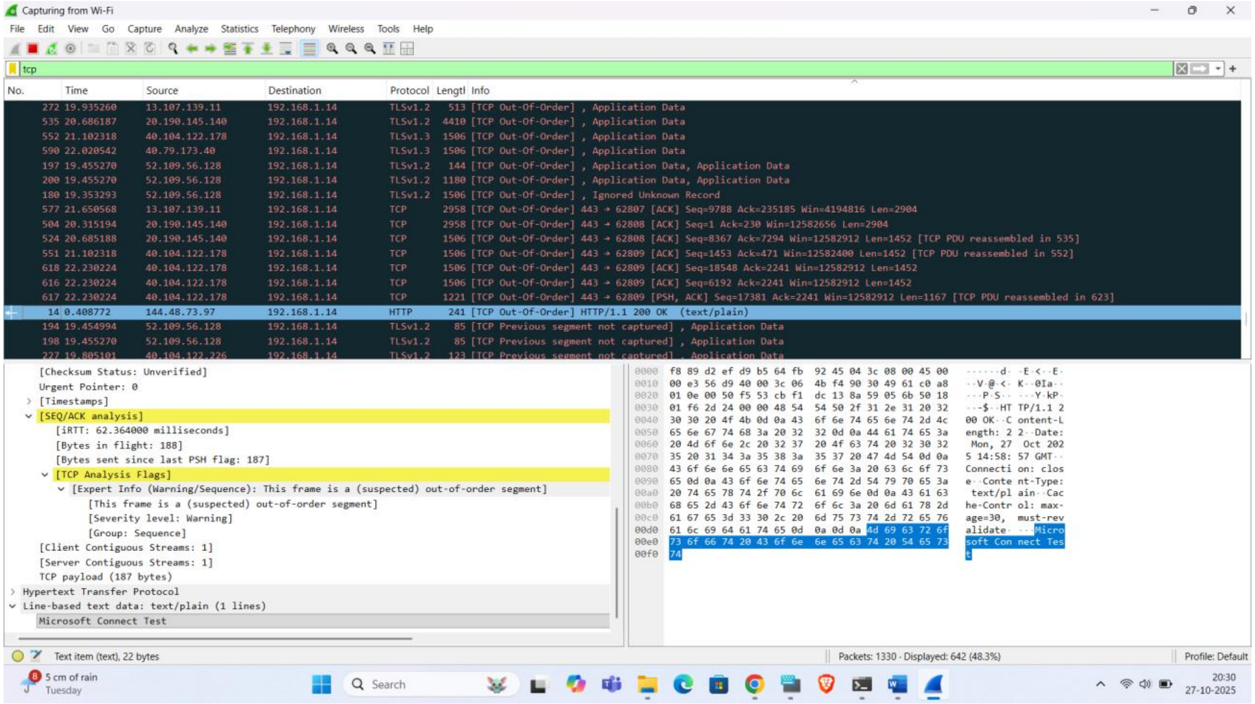
```
No.    Time        Source          Destination     Protocol  Lengtl  Info
  10   0.344835    192.168.1.14    144.48.73.97    HTTP      165     GET /connecttest.txt HTTP/1.1
  14   0.408772    144.48.73.97    192.168.1.14    HTTP      241     [TCP Out-Of-Order] HTTP/1.1 200 OK  (text/plain)
```

```
> Frame 14: Packet, 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits) on interface \Device\NPF
> Ethernet II, Src: PPCBroadband_45:04:3c (64:fb:92:45:04:3c), Dst: CloudNetwork_ef:d9:b5 (f8:89:d2:ef:d9:
> Internet Protocol Version 4, Src: 144.48.73.97, Dst: 192.168.1.14
> Transmission Control Protocol, Src Port: 80, Dst Port: 62803, Seq: 1, Ack: 112, Len: 187
> Hypertext Transfer Protocol
> Line-based text data: text/plain (1 lines)
```

```
0000  f8 89 d2 ef d9 b5 64 fb  92 45 04 3c 08 00 45 00   ······d· ·E·<··E·
0010  00 e3 56 d9 40 00 3c 06  4b f4 90 30 49 61 c0 a8   ··V·@·<· K··0Ia··
0020  01 0e 00 50 f5 53 cb f1  dc 13 8a 59 05 6b 50 18   ···P·S·· ···Y·kP·
0030  01 f6 2d 24 00 00 48 54  54 50 2f 31 2e 31 20 32   ··-$··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d 4c   00 OK··C ontent-L
0050  65 6e 67 74 68 3a 20 32  32 0d 0a 44 61 74 65 3a   ength: 2 2··Date:
0060  20 4d 6f 6e 2c 20 32 37  20 4f 63 74 20 32 30 32    Mon, 27  Oct 202
0070  35 20 31 34 3a 35 38 3a  35 37 20 47 4d 54 0d 0a   5 14:58: 57 GMT··
0080  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 63 6c 6f 73   Connecti on: clos
0090  65 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   e··Conte nt-Type:
00a0  20 74 65 78 74 2f 70 6c  61 69 6e 0d 0a 43 61 63    text/pl ain··Cac
00b0  68 65 2d 43 6f 6e 74 72  6f 6c 3a 20 6d 61 78 2d   he-Contr ol: max-
00c0  61 67 65 3d 33 30 2c 20  6d 75 73 74 2d 72 65 76   age=30,  must-rev
00d0  61 6c 69 64 61 74 65 0d  0a 0d 0a 4d 69 63 72 6f   alidate· ···Micro
00e0  73 6f 66 74 20 43 6f 6e  6e 65 63 74 20 54 65 73   soft Con nect Tes
00f0  74                                                 t
```

Hypertext Transfer Protocol: Protocol | Packets: 163 · Displayed: 2 (1.2%) | Profile: Default

tcp


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Text item (text), 22 bytes
Packets: 1330 · Displayed: 642 (48.3%)
Profile: Default
5 cm of rain
Tuesday
Search
20:30
27-10-2025

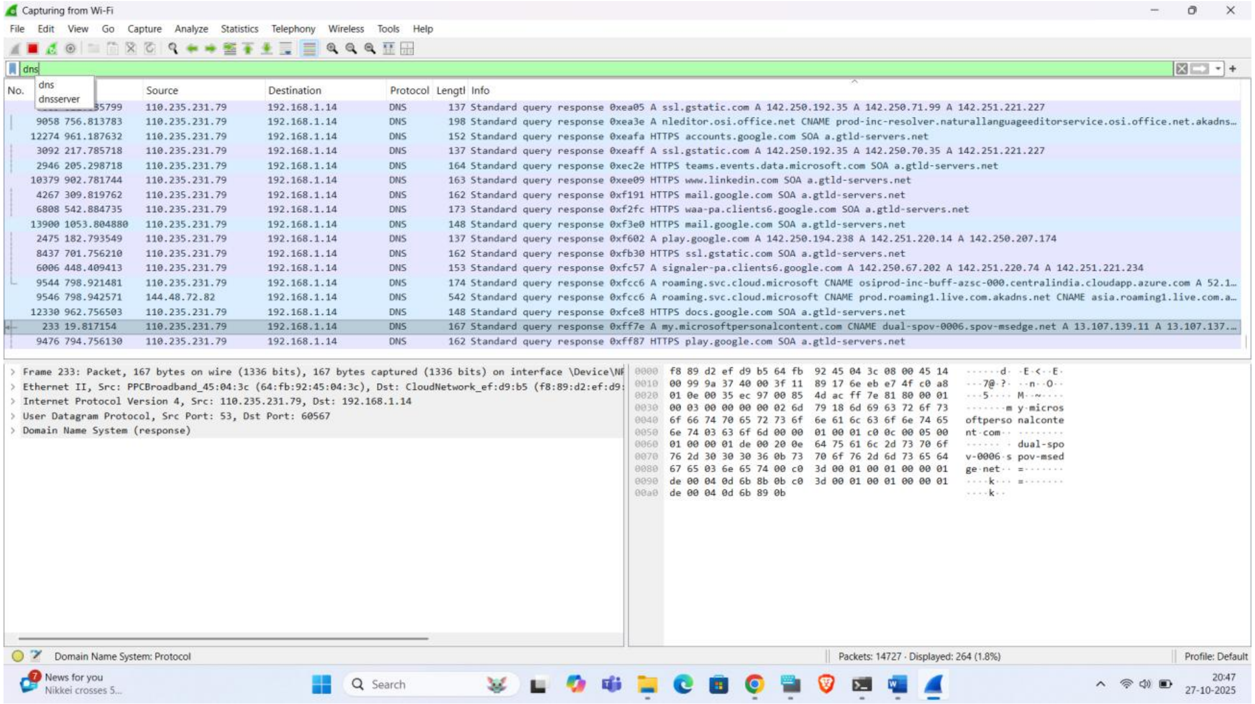
```
tcp

No.   Time         Source           Destination    Protocol Lengtl Info
  272 19.935260    13.107.139.11    192.168.1.14   TLSv1.2   513 [TCP Out-Of-Order] , Application Data
  535 20.686187    20.190.145.140   192.168.1.14   TLSv1.2  4410 [TCP Out-Of-Order] , Application Data
  552 21.102318    40.104.122.178   192.168.1.14   TLSv1.3  1506 [TCP Out-Of-Order] , Application Data
  590 22.020542    40.79.173.40     192.168.1.14   TLSv1.3  1506 [TCP Out-Of-Order] , Application Data
  197 19.455270    52.109.56.128    192.168.1.14   TLSv1.2   144 [TCP Out-Of-Order] , Application Data, Application Data
  200 19.455270    52.109.56.128    192.168.1.14   TLSv1.2  1180 [TCP Out-Of-Order] , Application Data, Application Data
  180 19.353293    52.109.56.128    192.168.1.14   TLSv1.2  1506 [TCP Out-Of-Order] , Ignored Unknown Record
  577 21.650568    13.107.139.11    192.168.1.14   TCP      2958 [TCP Out-Of-Order] 443 → 62807 [ACK] Seq=9788 Ack=235185 Win=4194816 Len=2904
  504 20.315194    20.190.145.140   192.168.1.14   TCP      2958 [TCP Out-Of-Order] 443 → 62808 [ACK] Seq=1 Ack=230 Win=12582656 Len=2904
  524 20.685188    20.190.145.140   192.168.1.14   TCP      1506 [TCP Out-Of-Order] 443 → 62808 [ACK] Seq=8367 Ack=7294 Win=12582912 Len=1452 [TCP PDU reassembled in 535]
  551 21.102318    40.104.122.178   192.168.1.14   TCP      1506 [TCP Out-Of-Order] 443 → 62809 [ACK] Seq=1453 Ack=471 Win=12582400 Len=1452 [TCP PDU reassembled in 552]
  618 22.230224    40.104.122.178   192.168.1.14   TCP      1506 [TCP Out-Of-Order] 443 → 62809 [ACK] Seq=18548 Ack=2241 Win=12582912 Len=1452
  616 22.230224    40.104.122.178   192.168.1.14   TCP      1506 [TCP Out-Of-Order] 443 → 62809 [ACK] Seq=6192 Ack=2241 Win=12582912 Len=1452
  617 22.230224    40.104.122.178   192.168.1.14   TCP      1221 [TCP Out-Of-Order] 443 → 62809 [PSH, ACK] Seq=17381 Ack=2241 Win=12582912 Len=1167 [TCP PDU reassembled in 623]
   14 0.408772     144.48.73.97     192.168.1.14   HTTP      241 [TCP Out-Of-Order] HTTP/1.1 200 OK  (text/plain)
  194 19.454994    52.109.56.128    192.168.1.14   TLSv1.2    85 [TCP Previous segment not captured] , Application Data
  198 19.455270    52.109.56.128    192.168.1.14   TLSv1.2    85 [TCP Previous segment not captured] , Application Data
  227 19.805101    40.104.122.226   192.168.1.14   TLSv1.2   123 [TCP Previous segment not captured] , Application Data
```

```
      [Checksum Status: Unverified]
      Urgent Pointer: 0
    > [Timestamps]
    v [SEQ/ACK analysis]
        [iRTT: 62.364000 milliseconds]
        [Bytes in flight: 188]
        [Bytes sent since last PSH flag: 187]
      v [TCP Analysis Flags]
        v [Expert Info (Warning/Sequence): This frame is a (suspected) out-of-order segment]
              [This frame is a (suspected) out-of-order segment]
              [Severity level: Warning]
              [Group: Sequence]
      [Client Contiguous Streams: 1]
      [Server Contiguous Streams: 1]
      TCP payload (187 bytes)
  > Hypertext Transfer Protocol
  v Line-based text data: text/plain (1 lines)
      Microsoft Connect Test
```

```
0000  f8 89 d2 ef d9 b5 64 fb  92 45 04 3c 08 00 45 00   ······d· ·E·<··E·
0010  00 e3 56 d9 40 00 3c 06  4b f4 90 30 49 61 c0 a8   ··V·@·<· K··0Ia··
0020  01 0e 00 50 f5 53 cb f1  dc 13 8a 59 05 6b 50 18   ···P·S·· ···Y·kP·
0030  01 f6 2d 24 00 00 48 54  54 50 2f 31 2e 31 20 32   ··-$··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d 4c   00 OK··C ontent-L
0050  65 6e 67 74 68 3a 20 32  32 0d 0a 44 61 74 65 3a   ength: 2 2··Date:
0060  20 4d 6f 6e 2c 20 32 37  20 4f 63 74 20 32 30 32    Mon, 27  Oct 202
0070  35 20 31 34 3a 35 38 3a  35 37 20 47 4d 54 0d 0a   5 14:58: 57 GMT··
0080  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 63 6c 6f 73   Connecti on: clos
0090  65 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   e··Conte nt-Type:
00a0  20 74 65 78 74 2f 70 6c  61 69 6e 0d 0a 43 61 63    text/pl ain··Cac
00b0  68 65 2d 43 6f 6e 74 72  6f 6c 3a 20 6d 61 78 2d   he-Contr ol: max-
00c0  61 67 65 3d 33 30 2c 20  6d 75 73 74 2d 72 65 76   age=30,  must-rev
00d0  61 6c 69 64 61 74 65 0d  0a 0d 0a 4d 69 63 72 6f   alidate· ···Micro
00e0  73 6f 66 74 20 43 6f 6e  6e 65 63 74 20 54 65 73   soft Con nect Tes
00f0  74                                                 t
```

dns

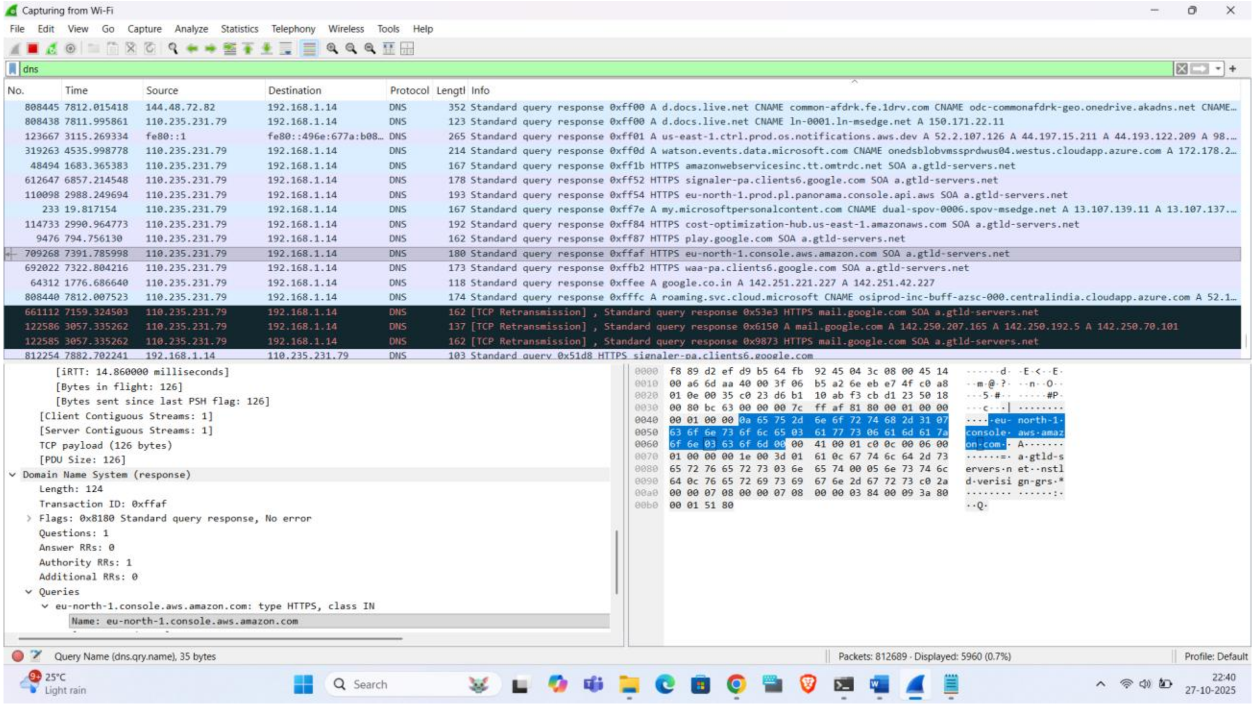

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
dnsserver
Domain Name System: Protocol
Packets: 14727 · Displayed: 264 (1.8%)
Profile: Default
News for you
Nikkei crosses 5...
Search
20:47
27-10-2025

```
dns

No.   Time         Source           Destination    Protocol Lengtl Info
      ...35799     110.235.231.79   192.168.1.14   DNS       137 Standard query response 0xea05 A ssl.gstatic.com A 142.250.192.35 A 142.250.71.99 A 142.251.221.227
 9058 756.813783   110.235.231.79   192.168.1.14   DNS       198 Standard query response 0xea3e A nleditor.osi.office.net CNAME prod-inc-resolver.naturallanguageeditorservice.osi.office.net.akadns…
12274 961.187632   110.235.231.79   192.168.1.14   DNS       152 Standard query response 0xeafa HTTPS accounts.google.com SOA a.gtld-servers.net
 3092 217.785718   110.235.231.79   192.168.1.14   DNS       137 Standard query response 0xeaff A ssl.gstatic.com A 142.250.192.35 A 142.250.70.35 A 142.251.221.227
 2946 205.298718   110.235.231.79   192.168.1.14   DNS       164 Standard query response 0xec2e HTTPS teams.events.data.microsoft.com SOA a.gtld-servers.net
10379 902.781744   110.235.231.79   192.168.1.14   DNS       163 Standard query response 0xee09 HTTPS www.linkedin.com SOA a.gtld-servers.net
 4267 309.819762   110.235.231.79   192.168.1.14   DNS       162 Standard query response 0xf191 HTTPS mail.google.com SOA a.gtld-servers.net
 6808 542.884735   110.235.231.79   192.168.1.14   DNS       173 Standard query response 0xf2fc HTTPS waa-pa.clients6.google.com SOA a.gtld-servers.net
13900 1053.804880  110.235.231.79   192.168.1.14   DNS       148 Standard query response 0xf3e0 HTTPS mail.google.com SOA a.gtld-servers.net
 2475 182.793549   110.235.231.79   192.168.1.14   DNS       137 Standard query response 0xf602 A play.google.com A 142.250.194.238 A 142.251.220.14 A 142.250.207.174
 8437 701.756210   110.235.231.79   192.168.1.14   DNS       162 Standard query response 0xfb30 HTTPS ssl.gstatic.com SOA a.gtld-servers.net
 6006 448.409413   110.235.231.79   192.168.1.14   DNS       153 Standard query response 0xfc57 A signaler-pa.clients6.google.com A 142.250.67.202 A 142.251.220.74 A 142.251.221.234
 9544 798.921481   110.235.231.79   192.168.1.14   DNS       174 Standard query response 0xfcc6 A roaming.svc.cloud.microsoft CNAME osiprod-inc-buff-azsc-000.centralindia.cloudapp.azure.com A 52.1…
 9546 798.942571   144.48.72.82     192.168.1.14   DNS       542 Standard query response 0xfcc6 A roaming.svc.cloud.microsoft CNAME prod.roaming1.live.com.akadns.net CNAME asia.roaming1.live.com.a…
12330 962.756503   110.235.231.79   192.168.1.14   DNS       148 Standard query response 0xfce8 HTTPS docs.google.com SOA a.gtld-servers.net
  233 19.817154    110.235.231.79   192.168.1.14   DNS       167 Standard query response 0xff7e A my.microsoftpersonalcontent.com CNAME dual-spov-0006.spov-msedge.net A 13.107.139.11 A 13.107.137.…
 9476 794.756130   110.235.231.79   192.168.1.14   DNS       162 Standard query response 0xff87 HTTPS play.google.com SOA a.gtld-servers.net
```

```
> Frame 233: Packet, 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface \Device\NF
> Ethernet II, Src: PPCBroadband_45:04:3c (64:fb:92:45:04:3c), Dst: CloudNetwork_ef:d9:b5 (f8:89:d2:ef:d9:
> Internet Protocol Version 4, Src: 110.235.231.79, Dst: 192.168.1.14
> User Datagram Protocol, Src Port: 53, Dst Port: 60567
> Domain Name System (response)
```

```
0000  f8 89 d2 ef d9 b5 64 fb  92 45 04 3c 08 00 45 14   ······d· ·E·<··E·
0010  00 99 9a 37 40 00 3f 11  89 17 6e eb e7 4f c0 a8   ···7@·?· ··n··O··
0020  01 0e 00 35 ec 97 00 85  4d ac ff 7e 81 80 00 01   ···5···· M··~····
0030  00 03 00 00 00 00 02 6d  79 18 6d 69 63 72 6f 73   ·······m y·micros
0040  6f 66 74 70 65 72 73 6f  6e 61 6c 63 6f 6e 74 65   oftperso nalconte
0050  6e 74 03 63 6f 6d 00 00  01 00 01 c0 0c 00 05 00   nt·com·· ········
0060  01 00 00 01 de 00 20 0e  64 75 61 6c 2d 73 70 6f   ······ · dual-spo
0070  76 2d 30 30 30 36 0b 73  70 6f 76 2d 6d 73 65 64   v-0006·s pov-msed
0080  67 65 03 6e 65 74 00 c0  3d 00 01 00 01 00 00 01   ge·net·· =·······
0090  de 00 04 0d 6b 8b 0b c0  3d 00 01 00 01 00 00 01   ····k··· =·······
00a0  de 00 04 0d 6b 89 0b                               ····k··
```



Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

```
No.     Time          Source           Destination          Protocol Lengtl Info
 808445 7812.015418   144.48.72.82     192.168.1.14         DNS      352 Standard query response 0xff00 A d.docs.live.net CNAME common-afdrk.fe.1drv.com CNAME odc-commonafdrk-geo.onedrive.akadns.net CNAME…
 808438 7811.995861   110.235.231.79   192.168.1.14         DNS      123 Standard query response 0xff00 A d.docs.live.net CNAME ln-0001.ln-msedge.net A 150.171.22.11
 123667 3115.269334   fe80::1          fe80::496e:677a:b08… DNS      265 Standard query response 0xff01 A us-east-1.ctrl.prod.os.notifications.aws.dev A 52.2.107.126 A 44.197.15.211 A 44.193.122.209 A 98.…
 319263 4535.998778   110.235.231.79   192.168.1.14         DNS      214 Standard query response 0xff0d A watson.events.data.microsoft.com CNAME onedsblobvmssprdwus04.westus.cloudapp.azure.com A 172.178.2…
  48494 1683.365383   110.235.231.79   192.168.1.14         DNS      167 Standard query response 0xff1b HTTPS amazonwebservicesinc.tt.omtrdc.net SOA a.gtld-servers.net
 612647 6857.214548   110.235.231.79   192.168.1.14         DNS      178 Standard query response 0xff52 HTTPS signaler-pa.clients6.google.com SOA a.gtld-servers.net
 110098 2988.249694   110.235.231.79   192.168.1.14         DNS      193 Standard query response 0xff54 HTTPS eu-north-1.prod.pl.panorama.console.api.aws SOA a.gtld-servers.net
    233 19.817154     110.235.231.79   192.168.1.14         DNS      167 Standard query response 0xff7e A my.microsoftpersonalcontent.com CNAME dual-spov-0006.spov-msedge.net A 13.107.139.11 A 13.107.137.…
 114733 2990.964773   110.235.231.79   192.168.1.14         DNS      192 Standard query response 0xff84 HTTPS cost-optimization-hub.us-east-1.amazonaws.com SOA a.gtld-servers.net
   9476 794.756130    110.235.231.79   192.168.1.14         DNS      162 Standard query response 0xff87 HTTPS play.google.com SOA a.gtld-servers.net
 709268 7391.785998   110.235.231.79   192.168.1.14         DNS      180 Standard query response 0xffaf HTTPS eu-north-1.console.aws.amazon.com SOA a.gtld-servers.net
 692022 7322.804216   110.235.231.79   192.168.1.14         DNS      173 Standard query response 0xffb2 HTTPS waa-pa.clients6.google.com SOA a.gtld-servers.net
  64312 1776.686640   110.235.231.79   192.168.1.14         DNS      118 Standard query response 0xffee A google.co.in A 142.251.221.227 A 142.251.42.227
 808440 7812.007523   110.235.231.79   192.168.1.14         DNS      174 Standard query response 0xfffc A roaming.svc.cloud.microsoft CNAME osiprod-inc-buff-azsc-000.centralindia.cloudapp.azure.com A 52.1…
 661112 7159.324503   110.235.231.79   192.168.1.14         DNS      162 [TCP Retransmission] , Standard query response 0x53e3 HTTPS mail.google.com SOA a.gtld-servers.net
 122586 3057.335262   110.235.231.79   192.168.1.14         DNS      137 [TCP Retransmission] , Standard query response 0x6150 A mail.google.com A 142.250.207.165 A 142.250.192.5 A 142.250.70.101
 122585 3057.335262   110.235.231.79   192.168.1.14         DNS      162 [TCP Retransmission] , Standard query response 0x9873 HTTPS mail.google.com SOA a.gtld-servers.net
 812254 7882.702241   192.168.1.14     110.235.231.79       DNS      103 Standard query 0x51d8 HTTPS signaler-pa.clients6.google.com
```

```
        [iRTT: 14.860000 milliseconds]
        [Bytes in flight: 126]
        [Bytes sent since last PSH flag: 126]
    [Client Contiguous Streams: 1]
    [Server Contiguous Streams: 1]
    TCP payload (126 bytes)
    [PDU Size: 126]
v Domain Name System (response)
    Length: 124
    Transaction ID: 0xffaf
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  v Queries
    v eu-north-1.console.aws.amazon.com: type HTTPS, class IN
          Name: eu-north-1.console.aws.amazon.com
```

```
0000  f8 89 d2 ef d9 b5 64 fb  92 45 04 3c 08 00 45 14   ······d· ·E·<··E·
0010  00 a6 6d aa 40 00 3f 06  b5 a2 6e eb e7 4f c0 a8   ··m·@·?· ··n··O··
0020  01 0e 00 35 c0 23 d6 b1  10 ab f3 cb d1 23 50 18   ···5·#·· ·····#P·
0030  00 80 bc 63 00 00 00 7c  ff af 81 80 00 01 00 00   ···c···| ········
0040  00 01 00 00 0a 65 75 2d  6e 6f 72 74 68 2d 31 07   ·····eu- north-1·
0050  63 6f 6e 73 6f 6c 65 03  61 77 73 06 61 6d 61 7a   console· aws·amaz
0060  6f 6e 03 63 6f 6d 00 00  41 00 01 c0 0c 00 06 00   on·com·· A·······
0070  01 00 00 00 1e 00 3d 01  61 0c 67 74 6c 64 2d 73   ······=· a·gtld-s
0080  65 72 76 65 72 73 03 6e  65 74 00 05 6e 73 74 6c   ervers·n et··nstl
0090  64 0c 76 65 72 69 73 69  67 6e 2d 67 72 73 c0 2a   d·verisi gn-grs·*
00a0  00 00 07 08 00 00 07 08  00 00 03 84 00 09 3a 80   ········ ······:·
00b0  00 01 51 80                                        ··Q·
```

Query Name (dns.qry.name), 35 bytes

Packets: 812689 · Displayed: 5960 (0.7%)

Profile: Default