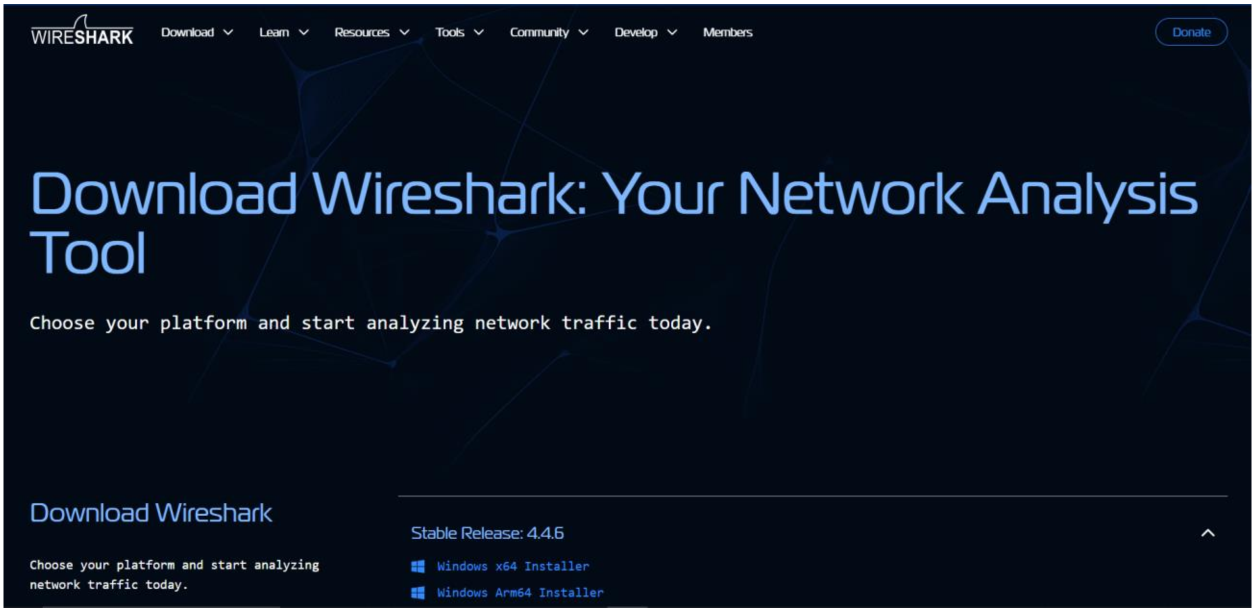
Task 5: Capture and Analyze Network Traffic Using Wireshark.

- Download Wireshark



Download Wireshark: Your Network Analysis Tool

Choose your platform and start analyzing network traffic today.

Download Wireshark

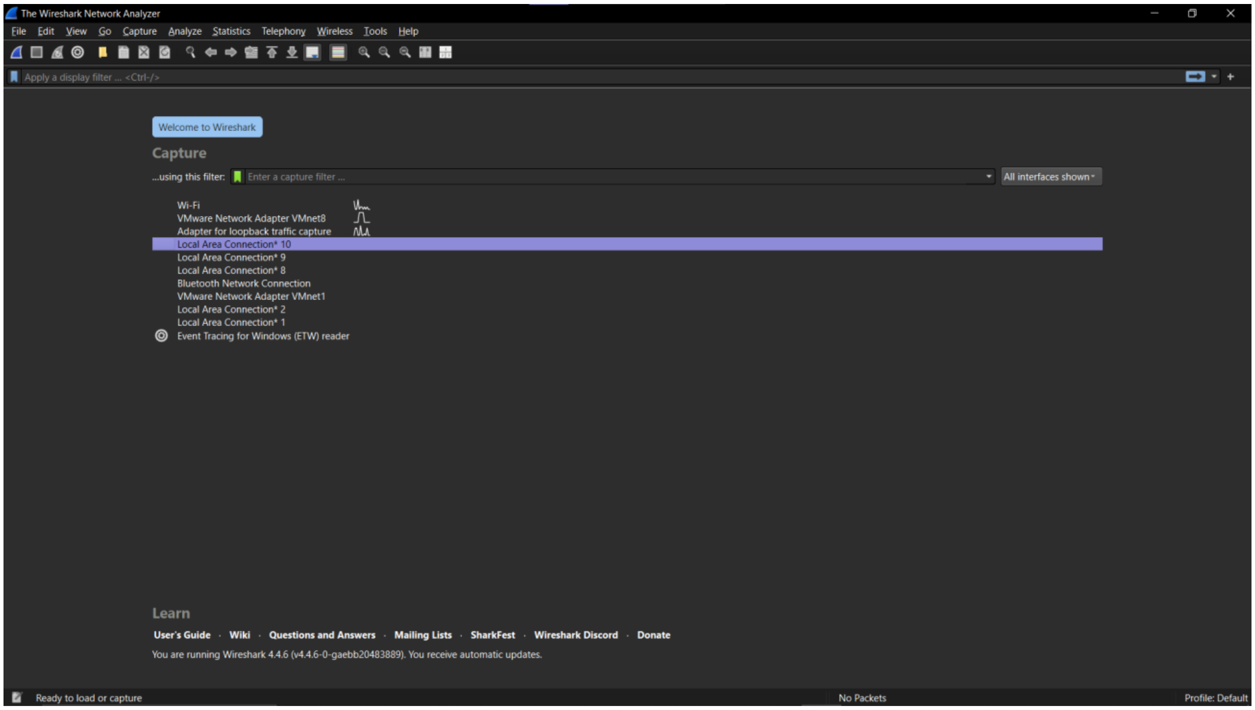
Choose your platform and start analyzing network traffic today.

Stable Release: 4.4.6

Windows x64 Installer

Windows Arm64 Installer

- Open Wireshark after installing

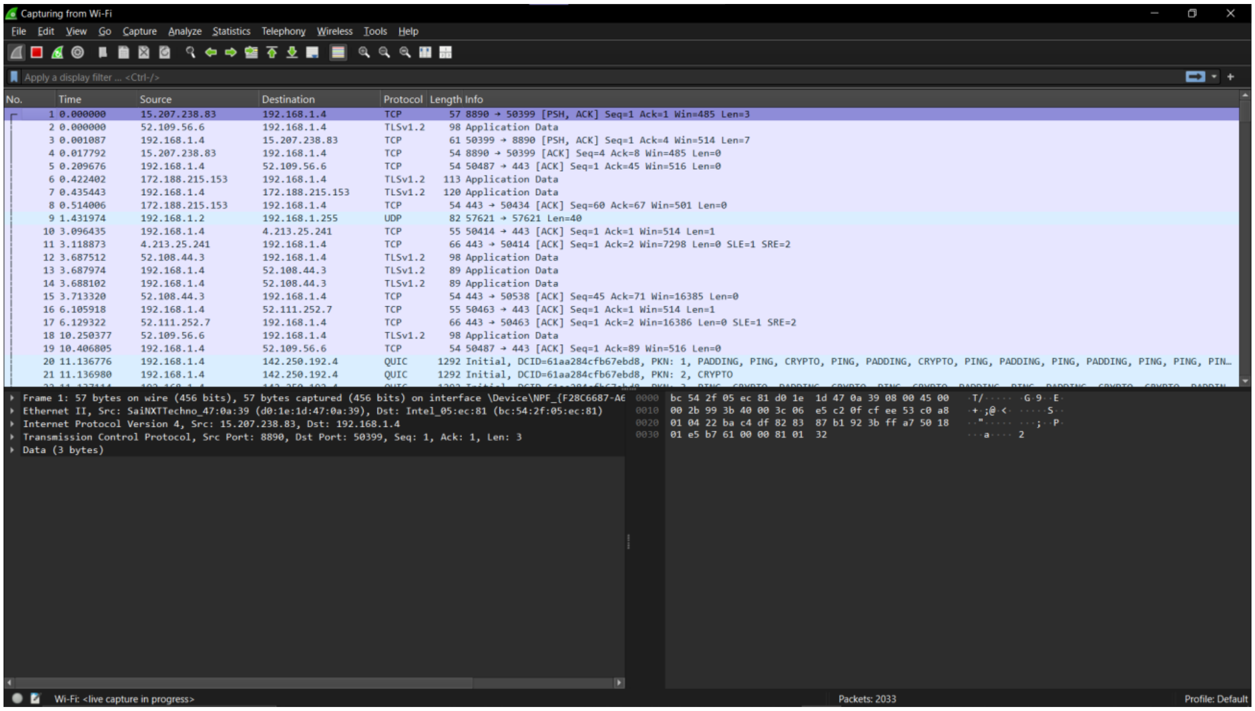

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown

Wi-Fi
VMware Network Adapter VMnet8
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
VMware Network Adapter VMnet1
Local Area Connection* 2
Local Area Connection* 1
Event Tracing for Windows (ETW) reader

Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.4.6 (v4.4.6-0-gaebb20483889). You receive automatic updates.

- Start scanning

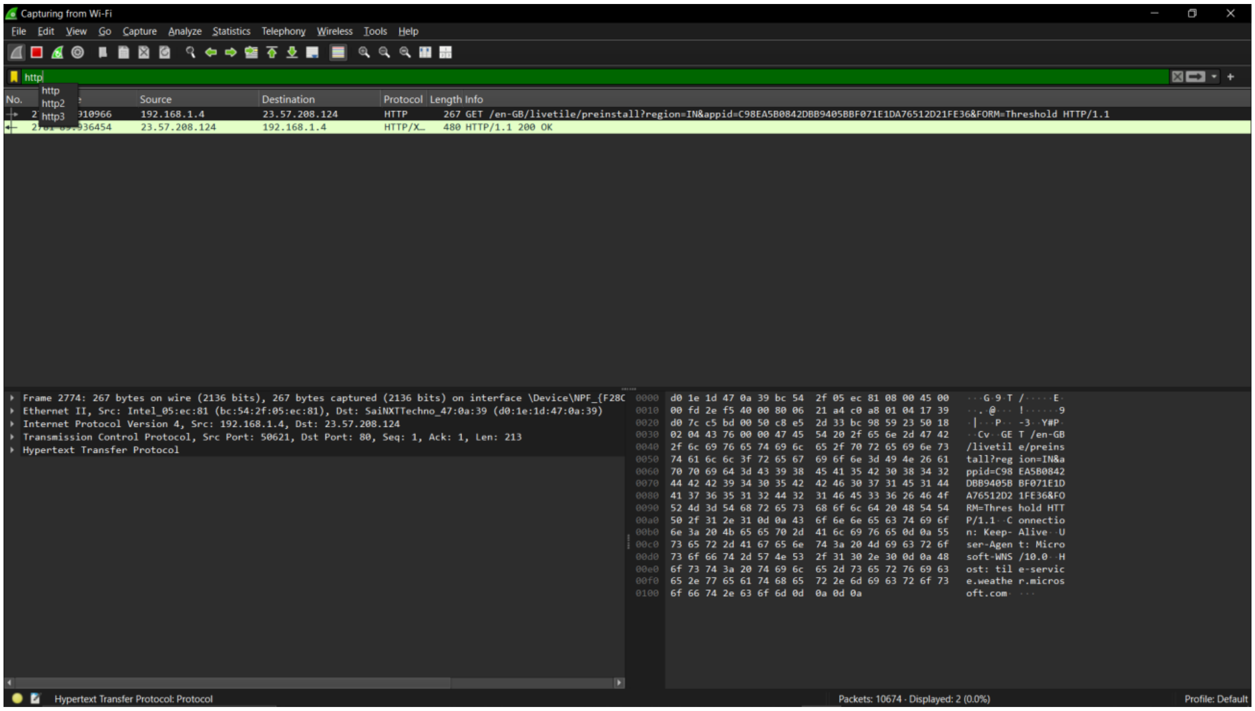

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source            Destination       Protocol Length Info
    1 0.000000    15.207.238.83     192.168.1.4       TCP        57 8890 → 50399 [PSH, ACK] Seq=1 Ack=1 Win=485 Len=3
    2 0.000000    52.109.56.6       192.168.1.4       TLSv1.2    98 Application Data
    3 0.001087    192.168.1.4       15.207.238.83     TCP        61 50399 → 8890 [PSH, ACK] Seq=1 Ack=4 Win=514 Len=7
    4 0.017792    15.207.238.83     192.168.1.4       TCP        54 8890 → 50399 [ACK] Seq=4 Ack=8 Win=485 Len=0
    5 0.209676    192.168.1.4       52.109.56.6       TCP        54 50487 → 443 [ACK] Seq=1 Ack=45 Win=516 Len=0
    6 0.422402    172.188.215.153   192.168.1.4       TLSv1.2   113 Application Data
    7 0.435443    192.168.1.4       172.188.215.153   TLSv1.2   120 Application Data
    8 0.514006    172.188.215.153   192.168.1.4       TCP        54 443 → 50434 [ACK] Seq=60 Ack=67 Win=501 Len=0
    9 1.431974    192.168.1.2       192.168.1.255     UDP        82 57621 → 57621 Len=40
   10 3.096435    192.168.1.4       4.213.25.241      TCP        55 50414 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1
   11 3.118873    4.213.25.241      192.168.1.4       TCP        66 443 → 50414 [ACK] Seq=1 Ack=2 Win=7298 Len=0 SLE=1 SRE=2
   12 3.687512    52.108.44.3       192.168.1.4       TLSv1.2    98 Application Data
   13 3.687974    192.168.1.4       52.108.44.3       TLSv1.2    89 Application Data
   14 3.688102    192.168.1.4       52.108.44.3       TLSv1.2    89 Application Data
   15 3.713320    52.108.44.3       192.168.1.4       TCP        54 443 → 50538 [ACK] Seq=45 Ack=71 Win=16385 Len=0
   16 6.105918    192.168.1.4       52.111.252.7      TCP        55 50463 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1
   17 6.129322    52.111.252.7      192.168.1.4       TCP        66 443 → 50463 [ACK] Seq=1 Ack=2 Win=16386 Len=0 SLE=1 SRE=2
   18 10.250377   52.109.56.6       192.168.1.4       TLSv1.2    98 Application Data
   19 10.406805   192.168.1.4       52.109.56.6       TCP        54 50487 → 443 [ACK] Seq=1 Ack=89 Win=516 Len=0
   20 11.136776   192.168.1.4       142.250.192.4     QUIC     1292 Initial, DCID=61aa284cfb67ebd8, PKN: 1, PADDING, PING, CRYPTO, PING, PADDING, CRYPTO, PING, PADDING, PING, PADDING, PING, PING, PIN…
   21 11.136980   192.168.1.4       142.250.192.4     QUIC     1292 Initial, DCID=61aa284cfb67ebd8, PKN: 2, CRYPTO
```

```
Frame 1: 57 bytes on wire (456 bits), 57 bytes captured (456 bits) on interface \Device\NPF_{F28C6687-A6
Ethernet II, Src: SaiNXTTechno_47:0a:39 (d0:1e:1d:47:0a:39), Dst: Intel_05:ec:81 (bc:54:2f:05:ec:81)
Internet Protocol Version 4, Src: 15.207.238.83, Dst: 192.168.1.4
Transmission Control Protocol, Src Port: 8890, Dst Port: 50399, Seq: 1, Ack: 1, Len: 3
Data (3 bytes)
```

```
0000  bc 54 2f 05 ec 81 d0 1e  1d 47 0a 39 08 00 45 00   ·T/·····  ·G·9··E·
0010  00 2b 99 3b 40 00 3c 06  e5 c2 0f cf ee 53 c0 a8   ·+·;@·<·  ·····S··
0020  01 04 22 ba c4 df 82 83  87 b1 92 3b ff a7 50 18   ··"·····  ···;··P·
0030  01 e5 b7 61 00 00 81 01  32                        ···a····  2
```

- HTTP Scan:


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
http2
http3

http

```
No.   Time        Source          Destination     Protocol Length Info
2…    …910966     192.168.1.4     23.57.208.124   HTTP      267 GET /en-GB/livetile/preinstall?region=IN&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1
2…    …936454     23.57.208.124   192.168.1.4     HTTP/X…   480 HTTP/1.1 200 OK
```

```
▸ Frame 2774: 267 bytes on wire (2136 bits), 267 bytes captured (2136 bits) on interface \Device\NPF_{F28C
▸ Ethernet II, Src: Intel_05:ec:81 (bc:54:2f:05:ec:81), Dst: SaiNXTTechno_47:0a:39 (d0:1e:1d:47:0a:39)
▸ Internet Protocol Version 4, Src: 192.168.1.4, Dst: 23.57.208.124
▸ Transmission Control Protocol, Src Port: 50621, Dst Port: 80, Seq: 1, Ack: 1, Len: 213
▸ Hypertext Transfer Protocol
```

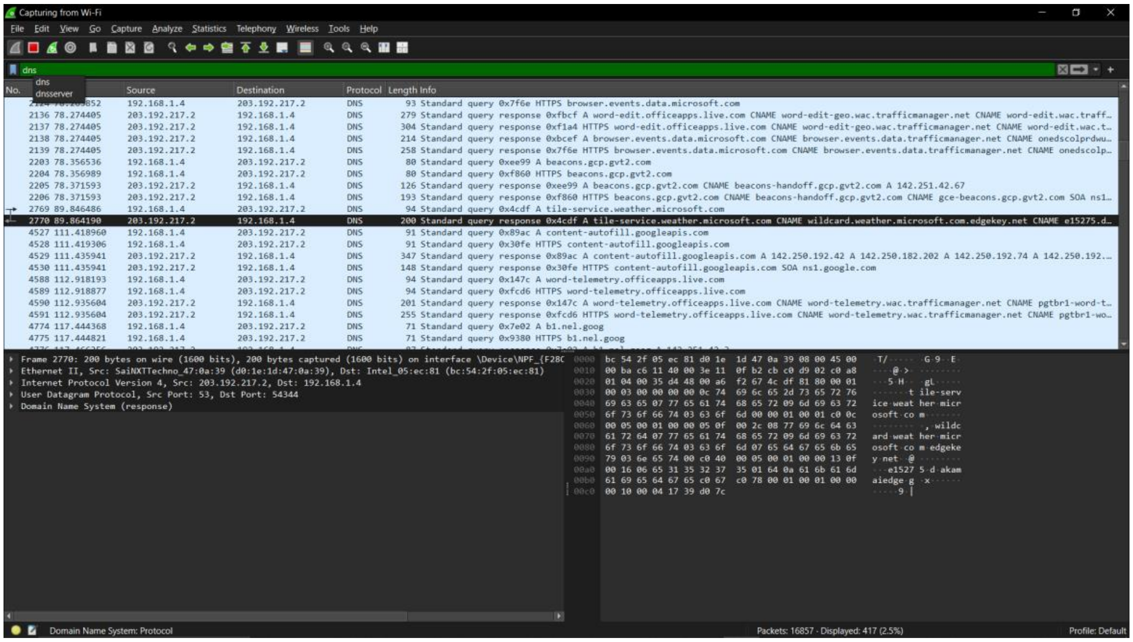
```
0000  d0 1e 1d 47 0a 39 bc 54  2f 05 ec 81 08 00 45 00   ···G·9·T /·····E·
0010  00 fd 2e f5 40 00 80 06  21 a4 c0 a8 01 04 17 39   ···.@··· !······9
0020  d0 7c c5 bd 00 50 c8 e5  2d 33 bc 98 59 23 50 18   ·|···P·· -3··Y#P·
0030  02 04 43 76 00 00 47 45  54 20 2f 65 6e 2d 47 42   ··Cv··GE T /en-GB
0040  2f 6c 69 76 65 74 69 6c  65 2f 70 72 65 69 6e 73   /livetil e/preins
0050  74 61 6c 6c 3f 72 65 67  69 6f 6e 3d 49 4e 26 61   tall?reg ion=IN&a
0060  70 70 69 64 3d 43 39 38  45 41 35 42 30 38 34 32   ppid=C98 EA5B0842
0070  44 42 42 39 34 30 35 42  42 46 30 37 31 45 31 44   DBB9405B BF071E1D
0080  41 37 36 35 31 32 44 32  31 46 45 33 36 26 46 4f   A76512D2 1FE36&FO
0090  52 4d 3d 54 68 72 65 73  68 6f 6c 64 20 48 54 54   RM=Thres hold HTT
00a0  50 2f 31 2e 31 0d 0a 43  6f 6e 6e 65 63 74 69 6f   P/1.1··C onnectio
00b0  6e 3a 20 4b 65 65 70 2d  41 6c 69 76 65 0d 0a 55   n: Keep- Alive··U
00c0  73 65 72 2d 41 67 65 6e  74 3a 20 4d 69 63 72 6f   ser-Agen t: Micro
00d0  73 6f 66 74 2d 57 4e 53  2f 31 30 2e 30 0d 0a 48   soft-WNS /10.0··H
00e0  6f 73 74 3a 20 74 69 6c  65 2d 73 65 72 76 69 63   ost: til e-servic
00f0  65 2e 77 65 61 74 68 65  72 2e 6d 69 63 72 6f 73   e.weathe r.micros
0100  6f 66 74 2e 63 6f 6d 0d  0a 0d 0a                  oft.com· ···
```

Hypertext Transfer Protocol: Protocol

Packets: 10674 · Displayed: 2 (0.0%)

Profile: Default

- DNS Scan:



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

```
No.                Source          Destination     Protocol Length Info
        852        192.168.1.4     203.192.217.2   DNS        93 Standard query 0x7f6e HTTPS browser.events.data.microsoft.com
   2136 78.274405  203.192.217.2   192.168.1.4     DNS       279 Standard query response 0xfbcf A word-edit.officeapps.live.com CNAME word-edit-geo.wac.trafficmanager.net CNAME word-edit.wac.traff…
   2137 78.274405  203.192.217.2   192.168.1.4     DNS       304 Standard query response 0xf1a4 HTTPS word-edit.officeapps.live.com CNAME word-edit-geo.wac.trafficmanager.net CNAME word-edit.wac.t…
   2138 78.274405  203.192.217.2   192.168.1.4     DNS       214 Standard query response 0xbcef A browser.events.data.microsoft.com CNAME browser.events.data.trafficmanager.net CNAME onedscolprdwu…
   2139 78.274405  203.192.217.2   192.168.1.4     DNS       258 Standard query response 0x7f6e HTTPS browser.events.data.microsoft.com CNAME browser.events.data.trafficmanager.net CNAME onedscolp…
   2203 78.356536  192.168.1.4     203.192.217.2   DNS        80 Standard query 0xee99 A beacons.gcp.gvt2.com
   2204 78.356989  192.168.1.4     203.192.217.2   DNS        80 Standard query 0xf860 HTTPS beacons.gcp.gvt2.com
   2205 78.371593  203.192.217.2   192.168.1.4     DNS       126 Standard query response 0xee99 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 142.251.42.67
   2206 78.371593  203.192.217.2   192.168.1.4     DNS       193 Standard query response 0xf860 HTTPS beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com CNAME gce-beacons.gcp.gvt2.com SOA ns1…
   2769 89.846486  192.168.1.4     203.192.217.2   DNS        94 Standard query 0x4cdf A tile-service.weather.microsoft.com
   2770 89.864190  203.192.217.2   192.168.1.4     DNS       200 Standard query response 0x4cdf A tile-service.weather.microsoft.com CNAME wildcard.weather.microsoft.com.edgekey.net CNAME e15275.d…
   4527 111.418960 192.168.1.4     203.192.217.2   DNS        91 Standard query 0x89ac A content-autofill.googleapis.com
   4528 111.419306 192.168.1.4     203.192.217.2   DNS        91 Standard query 0x30fe HTTPS content-autofill.googleapis.com
   4529 111.435941 203.192.217.2   192.168.1.4     DNS       347 Standard query response 0x89ac A content-autofill.googleapis.com A 142.250.192.42 A 142.250.182.202 A 142.250.192.74 A 142.250.192.…
   4530 111.435941 203.192.217.2   192.168.1.4     DNS       148 Standard query response 0x30fe HTTPS content-autofill.googleapis.com SOA ns1.google.com
   4588 112.918193 192.168.1.4     203.192.217.2   DNS        94 Standard query 0x147c A word-telemetry.officeapps.live.com
   4589 112.918877 192.168.1.4     203.192.217.2   DNS        94 Standard query 0xfcd6 HTTPS word-telemetry.officeapps.live.com
   4590 112.935604 203.192.217.2   192.168.1.4     DNS       201 Standard query response 0x147c A word-telemetry.officeapps.live.com CNAME word-telemetry.wac.trafficmanager.net CNAME pgtbr1-word-t…
   4591 112.935604 203.192.217.2   192.168.1.4     DNS       255 Standard query response 0xfcd6 HTTPS word-telemetry.officeapps.live.com CNAME word-telemetry.wac.trafficmanager.net CNAME pgtbr1-wo…
   4774 117.444368 192.168.1.4     203.192.217.2   DNS        71 Standard query 0x7e02 A b1.nel.goog
   4775 117.444821 192.168.1.4     203.192.217.2   DNS        71 Standard query 0x9380 HTTPS b1.nel.goog
```

```
▸ Frame 2770: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface \Device\NPF_{F28C
▸ Ethernet II, Src: SaiNXTTechno_47:0a:39 (d0:1e:1d:47:0a:39), Dst: Intel_05:ec:81 (bc:54:2f:05:ec:81)
▸ Internet Protocol Version 4, Src: 203.192.217.2, Dst: 192.168.1.4
▸ User Datagram Protocol, Src Port: 53, Dst Port: 54344
▸ Domain Name System (response)
```

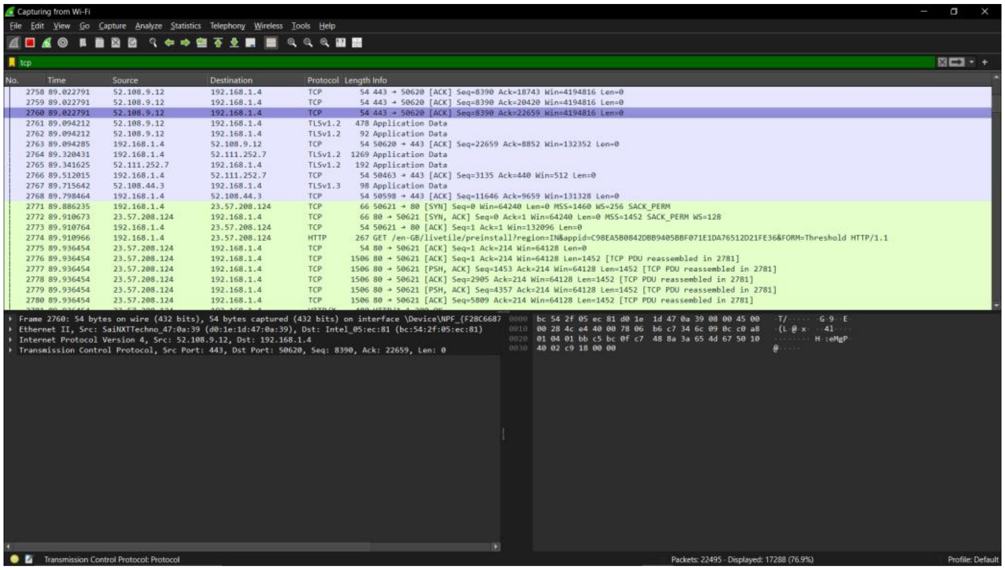
```
0000  bc 54 2f 05 ec 81 d0 1e  1d 47 0a 39 08 00 45 00   ·T/·····  ·G·9··E·
0010  00 ba c6 11 40 00 3e 11  0f b2 cb c0 d9 02 c0 a8   ····@·>·  ········
0020  01 04 00 35 d4 48 00 a6  f2 67 4c df 81 80 00 01   ···5·H··  ·gL·····
0030  00 03 00 00 00 00 0c 74  69 6c 65 2d 73 65 72 76   ·······t  ile-serv
0040  69 63 65 07 77 65 61 74  68 65 72 09 6d 69 63 72   ice·weat  her·micr
0050  6f 73 6f 66 74 03 63 6f  6d 00 00 01 00 01 c0 0c   osoft·co  m·······
0060  00 05 00 01 00 00 05 0f  00 2c 08 77 69 6c 64 63   ········  ·,·wildc
0070  61 72 64 07 77 65 61 74  68 65 72 09 6d 69 63 72   ard·weat  her·micr
0080  6f 73 6f 66 74 03 63 6f  6d 07 65 64 67 65 6b 65   osoft·co  m·edgeke
0090  79 03 6e 65 74 00 c0 40  00 05 00 01 00 00 13 0f   y·net··@  ········
00a0  00 16 06 65 31 35 32 37  35 01 64 0a 61 6b 61 6d   ···e1527  5·d·akam
00b0  61 69 65 64 67 65 c0 67  c0 78 00 01 00 01 00 00   aiedge·g  ·x······
00c0  00 10 00 04 17 39 d0 7c                            ·····9·|
```

Domain Name System: Protocol

Packets: 16857 · Displayed: 417 (2.5%)

Profile: Default

- TCP scan:



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

```
No.    Time       Source          Destination     Protocol Length Info
  2758 89.022791  52.108.9.12     192.168.1.4     TCP        54 443 → 50620 [ACK] Seq=8390 Ack=18743 Win=4194816 Len=0
  2759 89.022791  52.108.9.12     192.168.1.4     TCP        54 443 → 50620 [ACK] Seq=8390 Ack=20420 Win=4194816 Len=0
  2760 89.022791  52.108.9.12     192.168.1.4     TCP        54 443 → 50620 [ACK] Seq=8390 Ack=22659 Win=4194816 Len=0
  2761 89.094212  52.108.9.12     192.168.1.4     TLSv1.2   478 Application Data
  2762 89.094212  52.108.9.12     192.168.1.4     TLSv1.2    92 Application Data
  2763 89.094285  192.168.1.4     52.108.9.12     TCP        54 50620 → 443 [ACK] Seq=22659 Ack=8852 Win=132352 Len=0
  2764 89.320431  192.168.1.4     52.111.252.7    TLSv1.2  1269 Application Data
  2765 89.341625  52.111.252.7    192.168.1.4     TLSv1.2   192 Application Data
  2766 89.512015  192.168.1.4     52.111.252.7    TCP        54 50463 → 443 [ACK] Seq=3135 Ack=440 Win=512 Len=0
  2767 89.715642  52.108.44.3     192.168.1.4     TLSv1.3    98 Application Data
  2768 89.798464  192.168.1.4     52.108.44.3     TCP        54 50598 → 443 [ACK] Seq=11646 Ack=9659 Win=131328 Len=0
  2771 89.886235  192.168.1.4     23.57.208.124   TCP        66 50621 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  2772 89.910673  23.57.208.124   192.168.1.4     TCP        66 80 → 50621 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM WS=128
  2773 89.910764  192.168.1.4     23.57.208.124   TCP        54 50621 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
  2774 89.910966  192.168.1.4     23.57.208.124   HTTP      267 GET /en-GB/livetile/preinstall?region=IN&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1
  2775 89.936454  23.57.208.124   192.168.1.4     TCP        54 80 → 50621 [ACK] Seq=1 Ack=214 Win=64128 Len=0
  2776 89.936454  23.57.208.124   192.168.1.4     TCP      1506 80 → 50621 [ACK] Seq=1 Ack=214 Win=64128 Len=1452 [TCP PDU reassembled in 2781]
  2777 89.936454  23.57.208.124   192.168.1.4     TCP      1506 80 → 50621 [PSH, ACK] Seq=1453 Ack=214 Win=64128 Len=1452 [TCP PDU reassembled in 2781]
  2778 89.936454  23.57.208.124   192.168.1.4     TCP      1506 80 → 50621 [ACK] Seq=2905 Ack=214 Win=64128 Len=1452 [TCP PDU reassembled in 2781]
  2779 89.936454  23.57.208.124   192.168.1.4     TCP      1506 80 → 50621 [PSH, ACK] Seq=4357 Ack=214 Win=64128 Len=1452 [TCP PDU reassembled in 2781]
  2780 89.936454  23.57.208.124   192.168.1.4     TCP      1506 80 → 50621 [ACK] Seq=5809 Ack=214 Win=64128 Len=1452 [TCP PDU reassembled in 2781]
```

```
› Frame 2760: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{F28C6687
› Ethernet II, Src: SaiNXTTechno_47:0a:39 (d0:1e:1d:47:0a:39), Dst: Intel_05:ec:81 (bc:54:2f:05:ec:81)
› Internet Protocol Version 4, Src: 52.108.9.12, Dst: 192.168.1.4
› Transmission Control Protocol, Src Port: 443, Dst Port: 50620, Seq: 8390, Ack: 22659, Len: 0
```

```
0000  bc 54 2f 05 ec 81 d0 1e  1d 47 0a 39 08 00 45 00   ·T/·····  ·G·9··E·
0010  00 28 4c e4 40 00 78 06  b6 c7 34 6c 09 0c c0 a8   ·(L·@·x·  ··4l····
0020  01 04 01 bb c5 bc 0f c7  48 8a 3a 65 4d 67 50 10   ········  H·:eMgP·
0030  40 02 c9 18 00 00                                  @·····
```

Transmission Control Protocol: Protocol

Packets: 22495 · Displayed: 17288 (76.9%)

Profile: Default