GHARDA FOUNDATION’S

GHARDA INSTITUTE OF TECHNOLOGY

Department of Computer Engineering

Evaluation Sheet

Class: T.E Computer Engineering **Sem:** VI

Subject: Cryptography and System Security

Experiment No: 10

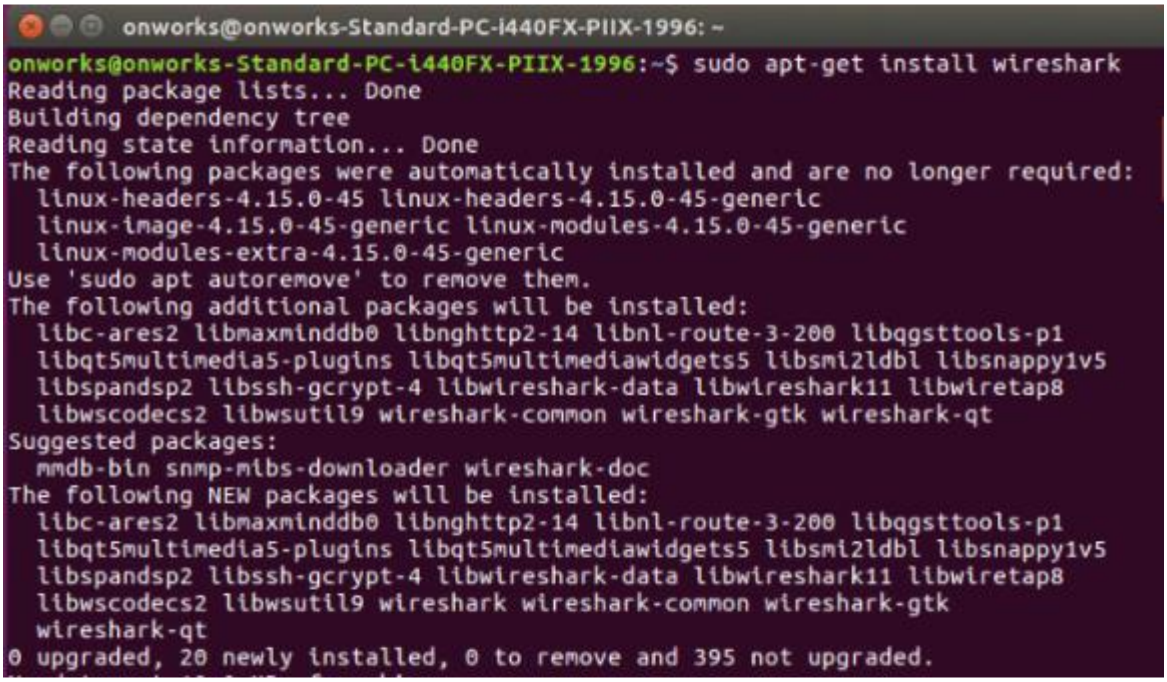
Date:

Title of Experiment: Study of packet sniffer wireshark: 1. Download and install wireshark and capture icmp, tcp, and http packets in promiscuous mode. 2. Explore how the packets can be traced based on dfferent filters.

Sr. No.	Evaluation Criteria	Max Marks	Marks Obtained
1	Practical Performance	12	
2	Oral	2	
3	Timely Submission	1	
	Total	15	

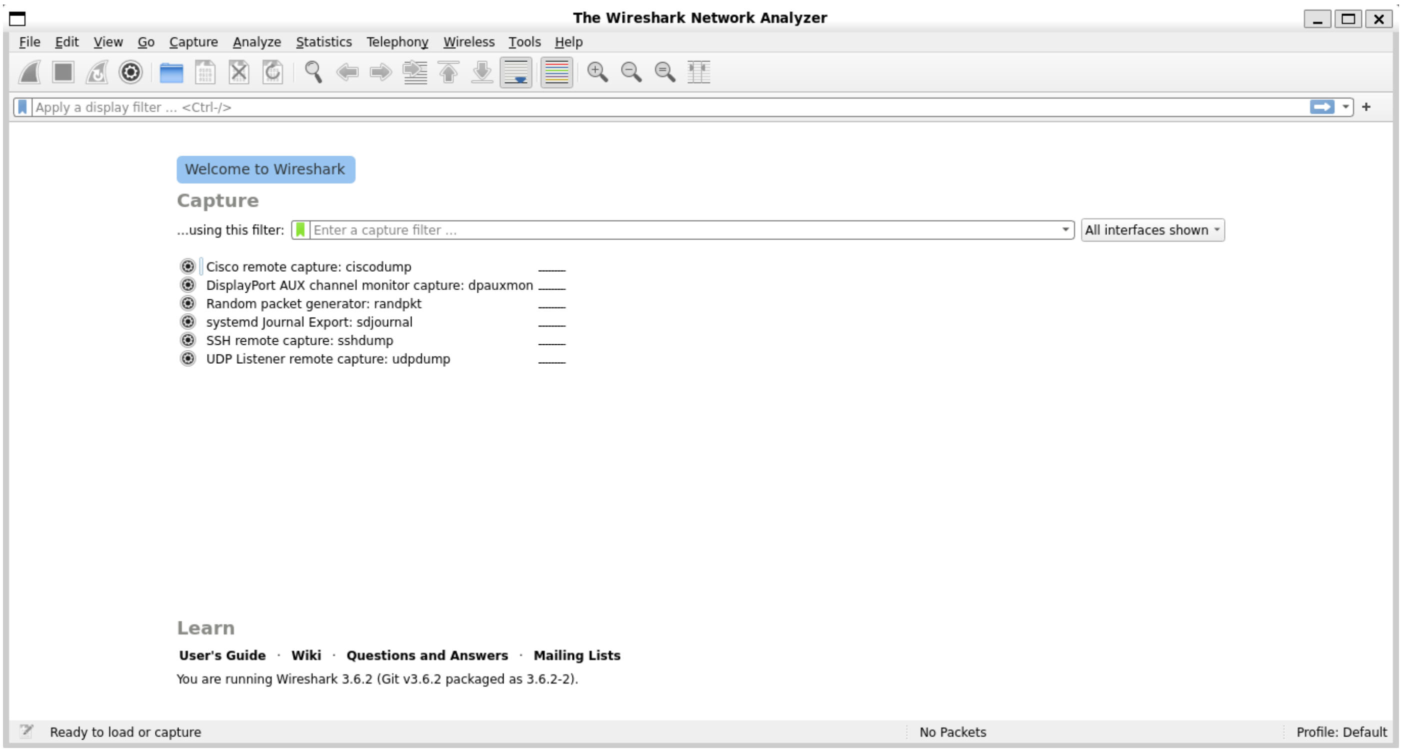
Signature of Subject Teacher
[Vijesh M.Nair]

Installation of wireshark



```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ sudo apt-get install wireshark
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-4.15.0-45 linux-headers-4.15.0-45-generic
  linux-image-4.15.0-45-generic linux-modules-4.15.0-45-generic
  linux-modules-extra-4.15.0-45-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libc-ares2 libmaxminddb0 libnghttp2-14 libnl-route-3-200 libqgsttools-p1
  libqt5multimedia5-plugins libqt5multimediawidgets5 libsmi2ldbl libsnappy1v5
  libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark11 libwiretap8
  libwscodecs2 libwsutil9 wireshark-common wireshark-gtk wireshark-qt
Suggested packages:
  mmdb-bin snmp-mibs-downloader wireshark-doc
The following NEW packages will be installed:
  libc-ares2 libmaxminddb0 libnghttp2-14 libnl-route-3-200 libqgsttools-p1
  libqt5multimedia5-plugins libqt5multimediawidgets5 libsmi2ldbl libsnappy1v5
  libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark11 libwiretap8
  libwscodecs2 libwsutil9 wireshark wireshark-common wireshark-gtk
  wireshark-qt
0 upgraded, 20 newly installed, 0 to remove and 395 not upgraded.
```

Running wireshark



Capture

...using this filter: Enter a capture filter ... All interfaces shown

- Cisco remote capture: ciscodump
- DisplayPort AUX channel monitor capture: dpauxmon
- Random packet generator: randpkt
- systemd Journal Export: sdjournal
- SSH remote capture: sshdump
- UDP Listener remote capture: udpdump

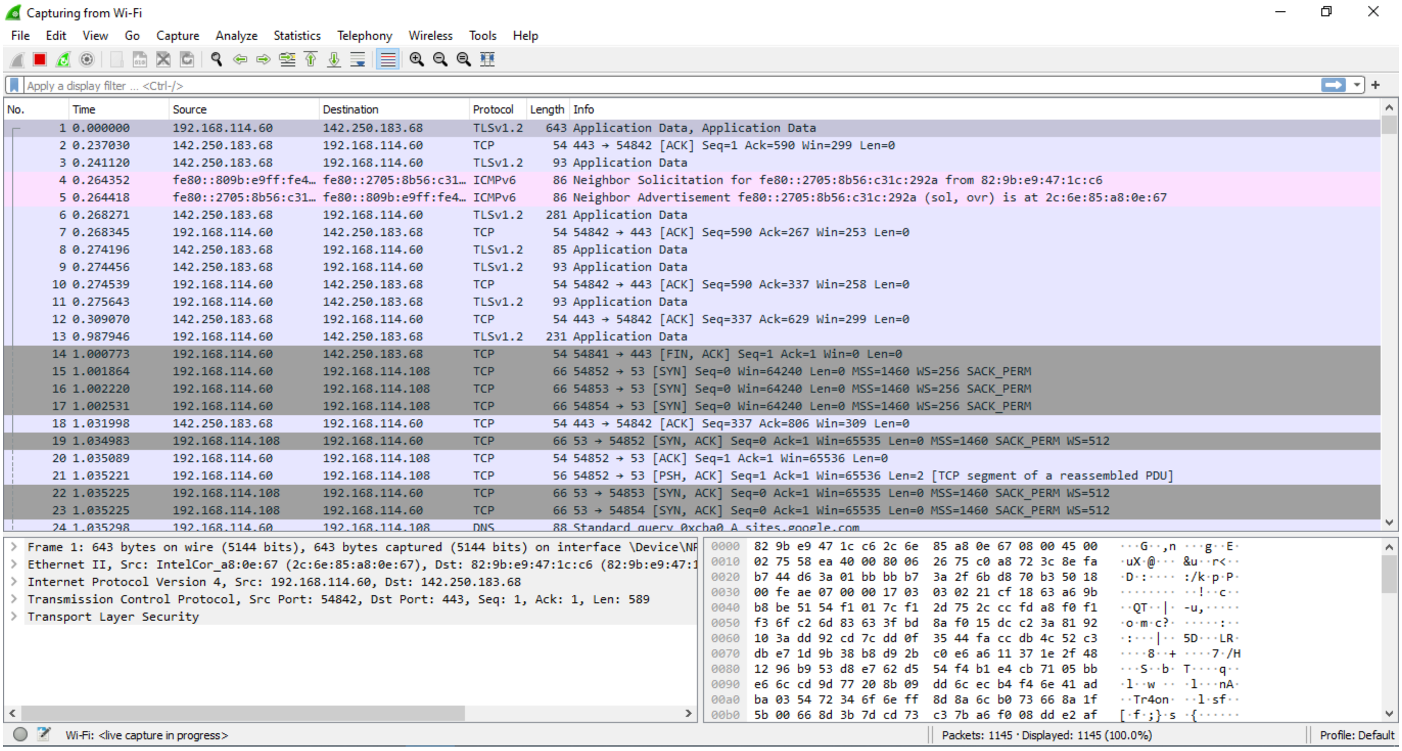
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.6.2 (Git v3.6.2 packaged as 3.6.2-2).

Ready to load or capture | No Packets | Profile: Default

Wireshark Packet Capturing Interface


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

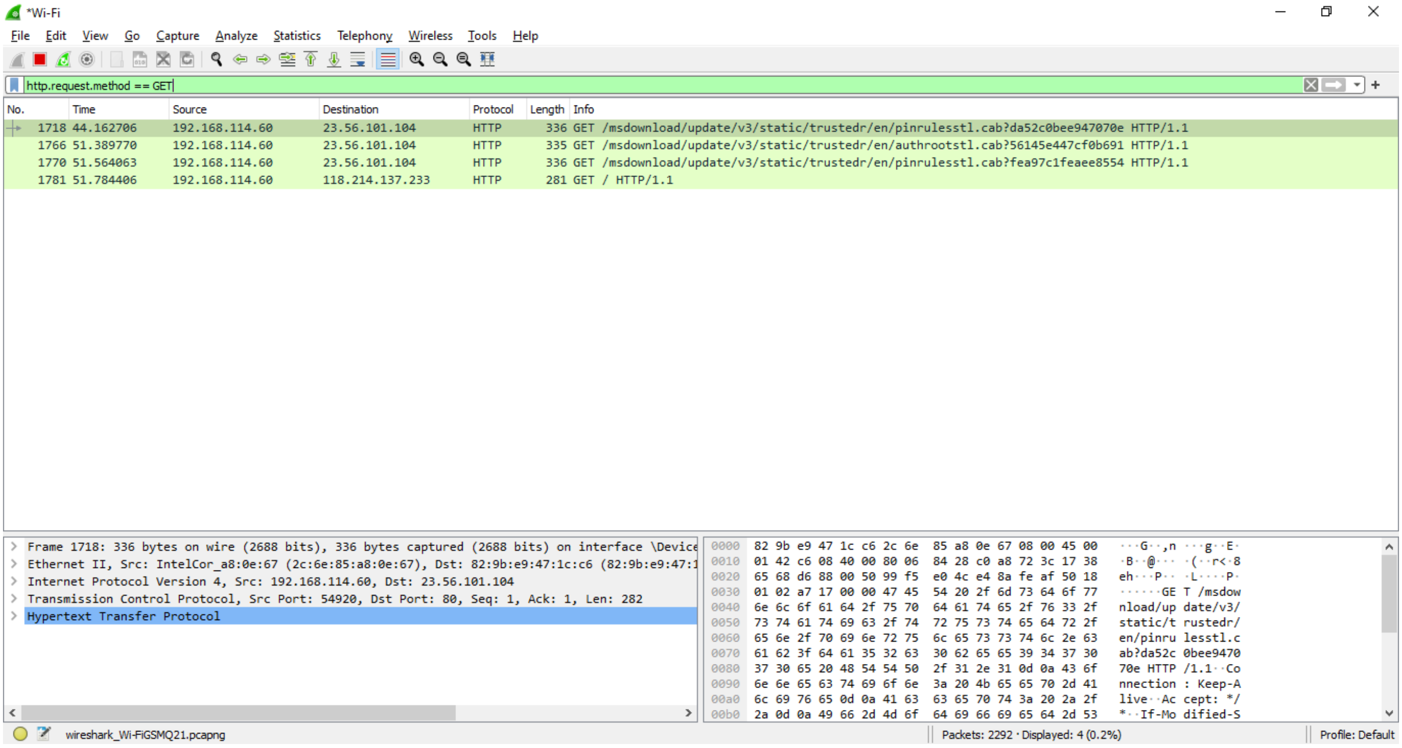
```
No.   Time        Source            Destination       Protocol  Length Info
    1 0.000000    192.168.114.60    142.250.183.68    TLSv1.2   643 Application Data, Application Data
    2 0.237030    142.250.183.68    192.168.114.60    TCP        54 443 → 54842 [ACK] Seq=1 Ack=590 Win=299 Len=0
    3 0.241120    142.250.183.68    192.168.114.60    TLSv1.2    93 Application Data
    4 0.264352    fe80::809b:e9ff:fe4… fe80::2705:8b56:c31… ICMPv6   86 Neighbor Solicitation for fe80::2705:8b56:c31c:292a from 82:9b:e9:47:1c:c6
    5 0.264418    fe80::2705:8b56:c31… fe80::809b:e9ff:fe4… ICMPv6   86 Neighbor Advertisement fe80::2705:8b56:c31c:292a (sol, ovr) is at 2c:6e:85:a8:0e:67
    6 0.268271    142.250.183.68    192.168.114.60    TLSv1.2   281 Application Data
    7 0.268345    192.168.114.60    142.250.183.68    TCP        54 54842 → 443 [ACK] Seq=590 Ack=267 Win=253 Len=0
    8 0.274196    142.250.183.68    192.168.114.60    TLSv1.2    85 Application Data
    9 0.274456    142.250.183.68    192.168.114.60    TLSv1.2    93 Application Data
   10 0.274539    192.168.114.60    142.250.183.68    TCP        54 54842 → 443 [ACK] Seq=590 Ack=337 Win=258 Len=0
   11 0.275643    192.168.114.60    142.250.183.68    TLSv1.2    93 Application Data
   12 0.309070    142.250.183.68    192.168.114.60    TCP        54 443 → 54842 [ACK] Seq=337 Ack=629 Win=299 Len=0
   13 0.987946    192.168.114.60    142.250.183.68    TLSv1.2   231 Application Data
   14 1.000773    192.168.114.60    142.250.183.68    TCP        54 54841 → 443 [FIN, ACK] Seq=1 Ack=1 Win=0 Len=0
   15 1.001864    192.168.114.60    192.168.114.108   TCP        66 54852 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   16 1.002220    192.168.114.60    192.168.114.108   TCP        66 54853 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   17 1.002531    192.168.114.60    192.168.114.108   TCP        66 54854 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   18 1.031998    142.250.183.68    192.168.114.60    TCP        54 443 → 54842 [ACK] Seq=337 Ack=806 Win=309 Len=0
   19 1.034983    192.168.114.108   192.168.114.60    TCP        66 53 → 54852 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
   20 1.035089    192.168.114.60    192.168.114.108   TCP        54 54852 → 53 [ACK] Seq=1 Ack=1 Win=65536 Len=0
   21 1.035221    192.168.114.60    192.168.114.108   TCP        56 54852 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=2 [TCP segment of a reassembled PDU]
   22 1.035225    192.168.114.108   192.168.114.60    TCP        66 53 → 54853 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
   23 1.035225    192.168.114.108   192.168.114.60    TCP        66 53 → 54854 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
   24 1.035298    192.168.114.60    192.168.114.108   DNS        88 Standard query 0xcba0 A sites.google.com
```

```
> Frame 1: 643 bytes on wire (5144 bits), 643 bytes captured (5144 bits) on interface \Device\NF
> Ethernet II, Src: IntelCor_a8:0e:67 (2c:6e:85:a8:0e:67), Dst: 82:9b:e9:47:1c:c6 (82:9b:e9:47:1
> Internet Protocol Version 4, Src: 192.168.114.60, Dst: 142.250.183.68
> Transmission Control Protocol, Src Port: 54842, Dst Port: 443, Seq: 1, Ack: 1, Len: 589
> Transport Layer Security
```

```
0000  82 9b e9 47 1c c6 2c 6e  85 a8 0e 67 08 00 45 00   ···G··,n ···g··E·
0010  02 75 58 ea 40 00 80 06  26 75 c0 a8 72 3c 8e fa   ·uX·@··· &u··r<··
0020  b7 44 d6 3a 01 bb bb b7  3a 2f 6b d8 70 b3 50 18   ·D·:···· :/k·p·P·
0030  00 fe ae 07 00 00 17 03  03 02 21 cf 18 63 a6 9b   ········ ··!··c··
0040  b8 be 51 54 f1 01 7c f1  2d 75 2c cc fd a8 f0 f1   ··QT··|· -u,·····
0050  f3 6f c2 6d 83 63 3f bd  8a f0 15 dc c2 3a 81 92   ·o·m·c?· ·····:··
0060  10 3a dd 92 cd 7c dd 0f  35 44 fa cc db 4c 52 c3   ·:···|·· 5D···LR·
0070  db e7 1d 9b 38 b8 d9 2b  c0 e6 a6 11 37 1e 2f 48   ····8··+ ····7·/H
0080  12 96 b9 53 d8 e7 62 d5  54 f4 b1 e4 cb 71 05 bb   ···S··b· T····q··
0090  e6 6c cd 9d 77 20 8b 09  dd 6c ec b4 f4 6e 41 ad   ·l··w ·· ·l···nA·
00a0  ba 03 54 72 34 6f 6e ff  8d 8a 6c b0 73 66 8a 1f   ··Tr4on· ··l·sf··
00b0  5b 00 66 8d 3b 7d cd 73  c3 7b a6 f0 08 dd e2 af   [·f·;}·s ·{······
```

Wi-Fi: <live capture in progress>   Packets: 1145 · Displayed: 1145 (100.0%)   Profile: Default

Capturing HTTP GET Requests


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

```
http.request.method == GET
```

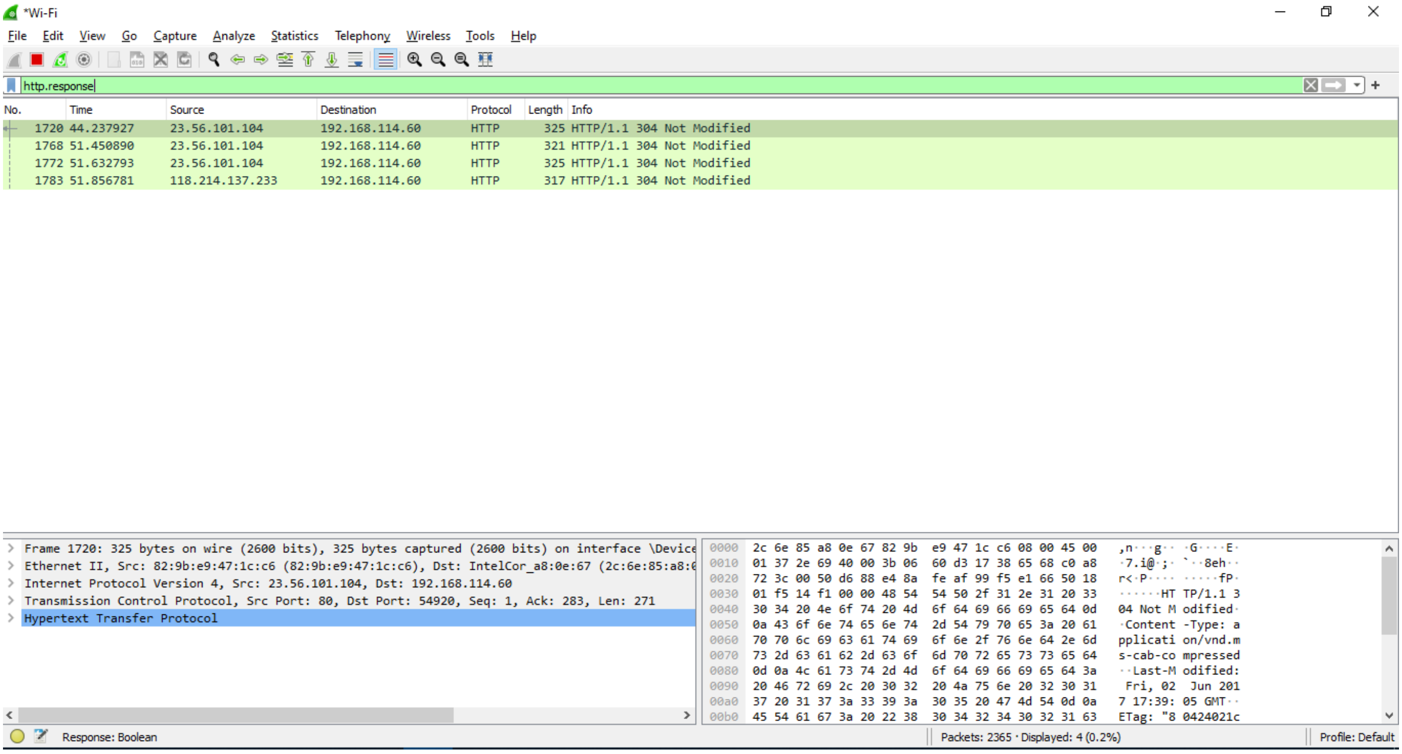
```
No.   Time         Source            Destination       Protocol  Length Info
 1718 44.162706    192.168.114.60    23.56.101.104     HTTP      336 GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?da52c0bee947070e HTTP/1.1
 1766 51.389770    192.168.114.60    23.56.101.104     HTTP      335 GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?56145e447cf0b691 HTTP/1.1
 1770 51.564063    192.168.114.60    23.56.101.104     HTTP      336 GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?fea97c1feaee8554 HTTP/1.1
 1781 51.784406    192.168.114.60    118.214.137.233   HTTP      281 GET / HTTP/1.1
```

```
> Frame 1718: 336 bytes on wire (2688 bits), 336 bytes captured (2688 bits) on interface \Device
> Ethernet II, Src: IntelCor_a8:0e:67 (2c:6e:85:a8:0e:67), Dst: 82:9b:e9:47:1c:c6 (82:9b:e9:47:1
> Internet Protocol Version 4, Src: 192.168.114.60, Dst: 23.56.101.104
> Transmission Control Protocol, Src Port: 54920, Dst Port: 80, Seq: 1, Ack: 1, Len: 282
> Hypertext Transfer Protocol
```

```
0000  82 9b e9 47 1c c6 2c 6e  85 a8 0e 67 08 00 45 00   ···G··,n ···g··E·
0010  01 42 c6 08 40 00 80 06  84 28 c0 a8 72 3c 17 38   ·B··@··· ·(··r<·8
0020  65 68 d6 88 00 50 99 f5  e0 4c e4 8a fe af 50 18   eh···P·· ·L····P·
0030  01 02 a7 17 00 00 47 45  54 20 2f 6d 73 64 6f 77   ······GE T /msdow
0040  6e 6c 6f 61 64 2f 75 70  64 61 74 65 2f 76 33 2f   nload/up date/v3/
0050  73 74 61 74 69 63 2f 74  72 75 73 74 65 64 72 2f   static/t rustedr/
0060  65 6e 2f 70 69 6e 72 75  6c 65 73 73 74 6c 2e 63   en/pinru lesstl.c
0070  61 62 3f 64 61 35 32 63  30 62 65 65 39 34 37 30   ab?da52c 0bee9470
0080  37 30 65 20 48 54 54 50  2f 31 2e 31 0d 0a 43 6f   70e HTTP /1.1··Co
0090  6e 6e 65 63 74 69 6f 6e  3a 20 4b 65 65 70 2d 41   nnection : Keep-A
00a0  6c 69 76 65 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   live··Ac cept: */
00b0  2a 0d 0a 49 66 2d 4d 6f  64 69 66 69 65 64 2d 53   *··If-Mo dified-S
```

wireshark_Wi-FiGSMQ21.pcapng   Packets: 2292 · Displayed: 4 (0.2%)   Profile: Default

Capturing HTTP Response


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

http.response

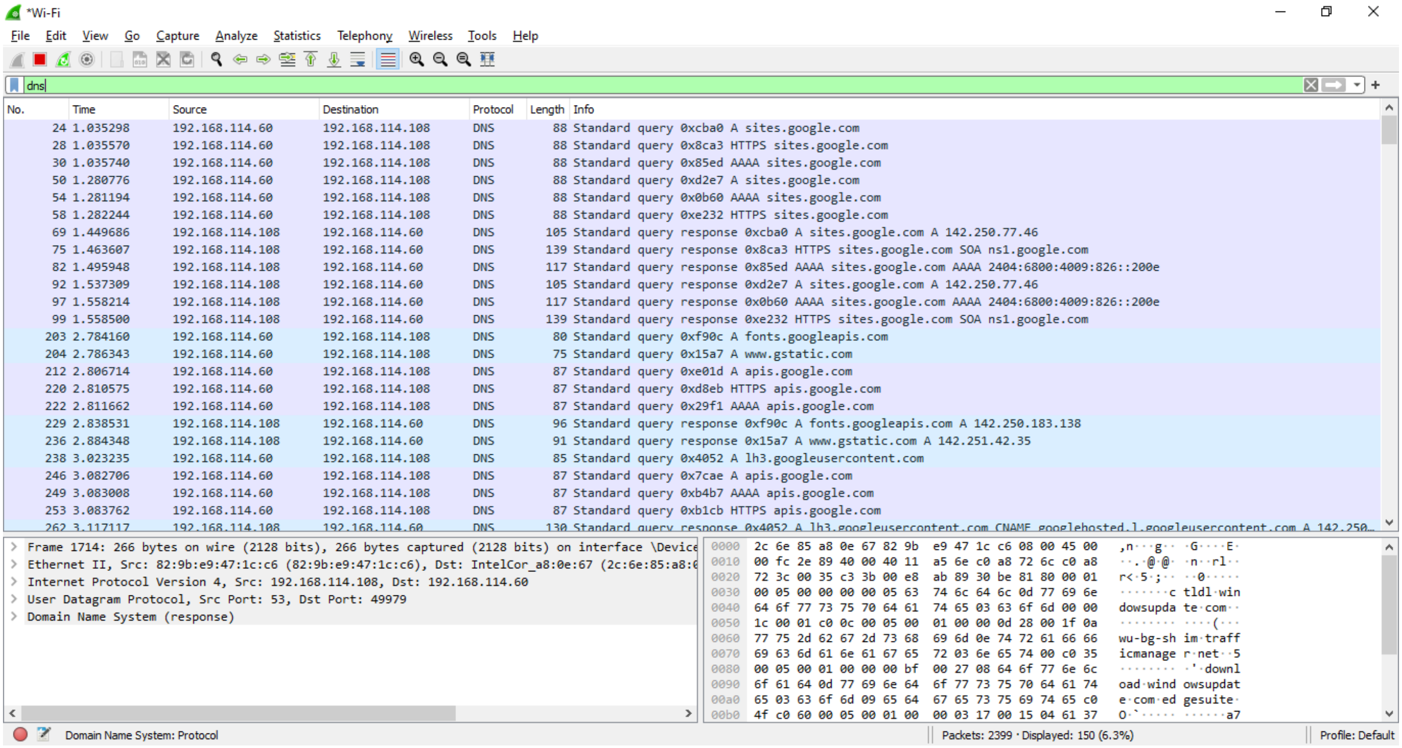
```
No.   Time       Source          Destination     Protocol Length Info
 1720 44.237927  23.56.101.104   192.168.114.60  HTTP     325 HTTP/1.1 304 Not Modified
 1768 51.450890  23.56.101.104   192.168.114.60  HTTP     321 HTTP/1.1 304 Not Modified
 1772 51.632793  23.56.101.104   192.168.114.60  HTTP     325 HTTP/1.1 304 Not Modified
 1783 51.856781  118.214.137.233 192.168.114.60  HTTP     317 HTTP/1.1 304 Not Modified
```

```
> Frame 1720: 325 bytes on wire (2600 bits), 325 bytes captured (2600 bits) on interface \Device
> Ethernet II, Src: 82:9b:e9:47:1c:c6 (82:9b:e9:47:1c:c6), Dst: IntelCor_a8:0e:67 (2c:6e:85:a8:0
> Internet Protocol Version 4, Src: 23.56.101.104, Dst: 192.168.114.60
> Transmission Control Protocol, Src Port: 80, Dst Port: 54920, Seq: 1, Ack: 283, Len: 271
> Hypertext Transfer Protocol
```

```
0000  2c 6e 85 a8 0e 67 82 9b  e9 47 1c c6 08 00 45 00   ,n···g·· ·G····E·
0010  01 37 2e 69 40 00 3b 06  60 d3 17 38 65 68 c0 a8   ·7.i@·;· `··8eh··
0020  72 3c 00 50 d6 88 e4 8a  fe af 99 f5 e1 66 50 18   r<·P···· ·····fP·
0030  01 f5 14 f1 00 00 48 54  54 50 2f 31 2e 31 20 33   ······HT TP/1.1 3
0040  30 34 20 4e 6f 74 20 4d  6f 64 69 66 69 65 64 0d   04 Not M odified·
0050  0a 43 6f 6e 74 65 6e 74  2d 54 79 70 65 3a 20 61   ·Content -Type: a
0060  70 70 6c 69 63 61 74 69  6f 6e 2f 76 6e 64 2e 6d   pplicati on/vnd.m
0070  73 2d 63 61 62 2d 63 6f  6d 70 72 65 73 73 65 64   s-cab-co mpressed
0080  0d 0a 4c 61 73 74 2d 4d  6f 64 69 66 69 65 64 3a   ··Last-M odified:
0090  20 46 72 69 2c 20 30 32  20 4a 75 6e 20 32 30 31    Fri, 02  Jun 201
00a0  37 20 31 37 3a 33 39 3a  30 35 20 47 4d 54 0d 0a   7 17:39: 05 GMT··
00b0  45 54 61 67 3a 20 22 38  30 34 32 34 30 32 31 63   ETag: "8 0424021c
```

Response: Boolean   Packets: 2365 · Displayed: 4 (0.2%)   Profile: Default

Capturing DNS Packets


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

dns

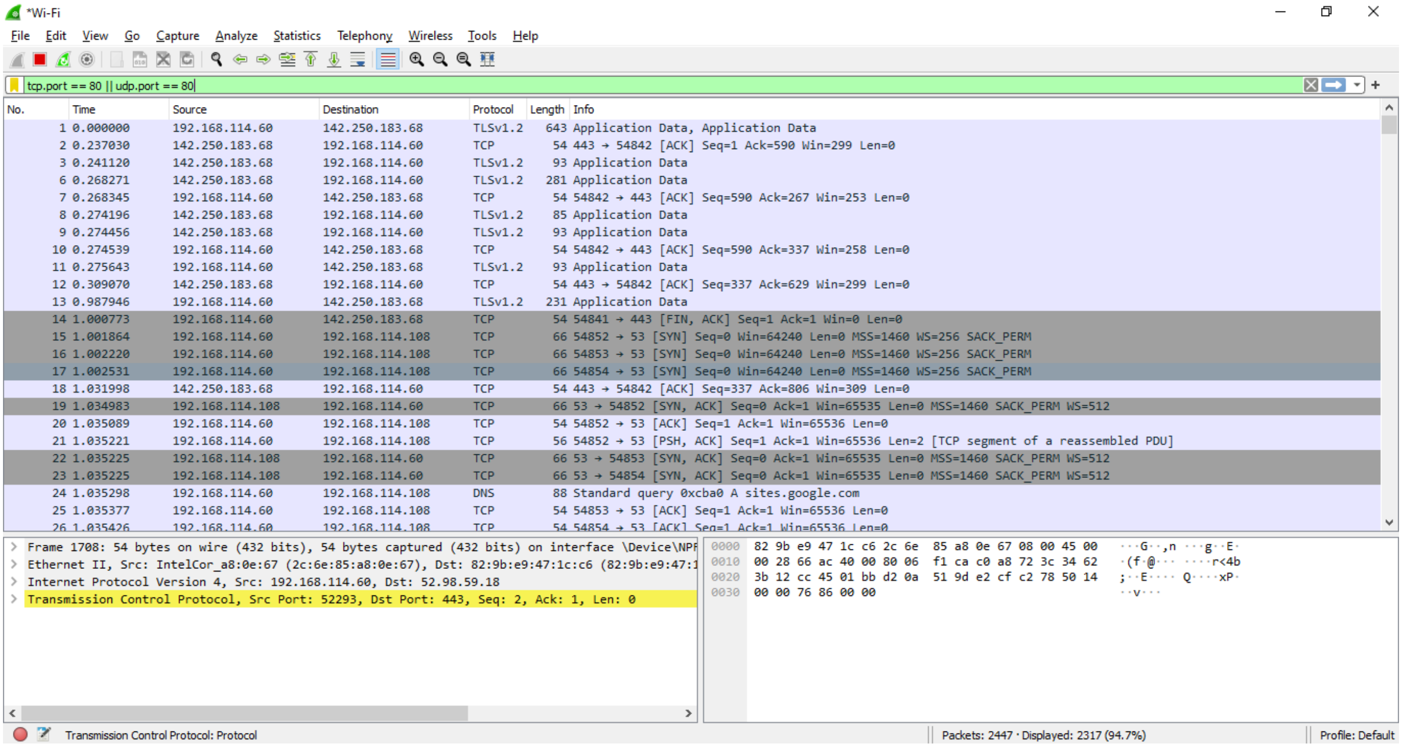
```
No.   Time      Source           Destination      Protocol Length Info
   24 1.035298  192.168.114.60   192.168.114.108  DNS       88 Standard query 0xcba0 A sites.google.com
   28 1.035570  192.168.114.60   192.168.114.108  DNS       88 Standard query 0x8ca3 HTTPS sites.google.com
   30 1.035740  192.168.114.60   192.168.114.108  DNS       88 Standard query 0x85ed AAAA sites.google.com
   50 1.280776  192.168.114.60   192.168.114.108  DNS       88 Standard query 0xd2e7 A sites.google.com
   54 1.281194  192.168.114.60   192.168.114.108  DNS       88 Standard query 0x0b60 AAAA sites.google.com
   58 1.282244  192.168.114.60   192.168.114.108  DNS       88 Standard query 0xe232 HTTPS sites.google.com
   69 1.449686  192.168.114.108  192.168.114.60   DNS      105 Standard query response 0xcba0 A sites.google.com A 142.250.77.46
   75 1.463607  192.168.114.108  192.168.114.60   DNS      139 Standard query response 0x8ca3 HTTPS sites.google.com SOA ns1.google.com
   82 1.495948  192.168.114.108  192.168.114.60   DNS      117 Standard query response 0x85ed AAAA sites.google.com AAAA 2404:6800:4009:826::200e
   92 1.537309  192.168.114.108  192.168.114.60   DNS      105 Standard query response 0xd2e7 A sites.google.com A 142.250.77.46
   97 1.558214  192.168.114.108  192.168.114.60   DNS      117 Standard query response 0x0b60 AAAA sites.google.com AAAA 2404:6800:4009:826::200e
   99 1.558500  192.168.114.108  192.168.114.60   DNS      139 Standard query response 0xe232 HTTPS sites.google.com SOA ns1.google.com
  203 2.784160  192.168.114.60   192.168.114.108  DNS       80 Standard query 0xf90c A fonts.googleapis.com
  204 2.786343  192.168.114.60   192.168.114.108  DNS       75 Standard query 0x15a7 A www.gstatic.com
  212 2.806714  192.168.114.60   192.168.114.108  DNS       87 Standard query 0xe01d A apis.google.com
  220 2.810575  192.168.114.60   192.168.114.108  DNS       87 Standard query 0xd8eb HTTPS apis.google.com
  222 2.811662  192.168.114.60   192.168.114.108  DNS       87 Standard query 0x29f1 AAAA apis.google.com
  229 2.838531  192.168.114.108  192.168.114.60   DNS       96 Standard query response 0xf90c A fonts.googleapis.com A 142.250.183.138
  236 2.884348  192.168.114.108  192.168.114.60   DNS       91 Standard query response 0x15a7 A www.gstatic.com A 142.251.42.35
  238 3.023235  192.168.114.60   192.168.114.108  DNS       85 Standard query 0x4052 A lh3.googleusercontent.com
  246 3.082706  192.168.114.60   192.168.114.108  DNS       87 Standard query 0x7cae A apis.google.com
  249 3.083008  192.168.114.60   192.168.114.108  DNS       87 Standard query 0xb4b7 AAAA apis.google.com
  253 3.083762  192.168.114.60   192.168.114.108  DNS       87 Standard query 0xb1cb HTTPS apis.google.com
  262 3.117117  192.168.114.108  192.168.114.60   DNS      130 Standard query response 0x4052 A lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 142.250…
```

```
> Frame 1714: 266 bytes on wire (2128 bits), 266 bytes captured (2128 bits) on interface \Device
> Ethernet II, Src: 82:9b:e9:47:1c:c6 (82:9b:e9:47:1c:c6), Dst: IntelCor_a8:0e:67 (2c:6e:85:a8:0
> Internet Protocol Version 4, Src: 192.168.114.108, Dst: 192.168.114.60
> User Datagram Protocol, Src Port: 53, Dst Port: 49979
> Domain Name System (response)
```

```
0000  2c 6e 85 a8 0e 67 82 9b  e9 47 1c c6 08 00 45 00   ,n···g·· ·G····E·
0010  00 fc 2e 89 40 00 40 11  a5 6e c0 a8 72 6c c0 a8   ··.·@·@· ·n··rl··
0020  72 3c 00 35 c3 3b 00 e8  ab 89 30 be 81 80 00 01   r<·5·;·· ··0·····
0030  00 05 00 00 00 00 05 63  74 6c 64 6c 0d 77 69 6e   ·······c tldl·win
0040  64 6f 77 73 75 70 64 61  74 65 03 63 6f 6d 00 00   dowsupda te·com··
0050  1c 00 01 c0 0c 00 05 00  01 00 00 0d 28 00 1f 0a   ········ ····(···
0060  77 75 2d 62 67 2d 73 68  69 6d 0e 74 72 61 66 66   wu-bg-sh im·traff
0070  69 63 6d 61 6e 61 67 65  72 03 6e 65 74 00 c0 35   icmanage r·net··5
0080  00 05 00 01 00 00 00 bf  00 27 08 64 6f 77 6e 6c   ········ ·'·downl
0090  6f 61 64 0d 77 69 6e 64  6f 77 73 75 70 64 61 74   oad·wind owsupdat
00a0  65 03 63 6f 6d 09 65 64  67 65 73 75 69 74 65 c0   e·com·ed gesuite·
00b0  4f c0 60 00 05 00 01 00  00 03 17 00 15 04 61 37   O·`····· ······a7
```

Domain Name System: Protocol   Packets: 2399 · Displayed: 150 (6.3%)   Profile: Default

Capturing TCP Port 80 and UDP Port 80



```
tcp.port == 80 || udp.port == 80
```

```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  192.168.114.60  142.250.183.68  TLSv1.2   643 Application Data, Application Data
   2 0.237030  142.250.183.68  192.168.114.60  TCP        54 443 → 54842 [ACK] Seq=1 Ack=590 Win=299 Len=0
   3 0.241120  142.250.183.68  192.168.114.60  TLSv1.2    93 Application Data
   6 0.268271  142.250.183.68  192.168.114.60  TLSv1.2   281 Application Data
   7 0.268345  192.168.114.60  142.250.183.68  TCP        54 54842 → 443 [ACK] Seq=590 Ack=267 Win=253 Len=0
   8 0.274196  142.250.183.68  192.168.114.60  TLSv1.2    85 Application Data
   9 0.274456  142.250.183.68  192.168.114.60  TLSv1.2    93 Application Data
  10 0.274539  192.168.114.60  142.250.183.68  TCP        54 54842 → 443 [ACK] Seq=590 Ack=337 Win=258 Len=0
  11 0.275643  192.168.114.60  142.250.183.68  TLSv1.2    93 Application Data
  12 0.309070  142.250.183.68  192.168.114.60  TCP        54 443 → 54842 [ACK] Seq=337 Ack=629 Win=299 Len=0
  13 0.987946  192.168.114.60  142.250.183.68  TLSv1.2   231 Application Data
  14 1.000773  192.168.114.60  142.250.183.68  TCP        54 54841 → 443 [FIN, ACK] Seq=1 Ack=1 Win=0 Len=0
  15 1.001864  192.168.114.60  192.168.114.108 TCP        66 54852 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  16 1.002220  192.168.114.60  192.168.114.108 TCP        66 54853 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  17 1.002531  192.168.114.60  192.168.114.108 TCP        66 54854 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  18 1.031998  142.250.183.68  192.168.114.60  TCP        54 443 → 54842 [ACK] Seq=337 Ack=806 Win=309 Len=0
  19 1.034983  192.168.114.108 192.168.114.60  TCP        66 53 → 54852 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
  20 1.035089  192.168.114.60  192.168.114.108 TCP        54 54852 → 53 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  21 1.035221  192.168.114.60  192.168.114.108 TCP        56 54852 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=2 [TCP segment of a reassembled PDU]
  22 1.035225  192.168.114.108 192.168.114.60  TCP        66 53 → 54853 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
  23 1.035225  192.168.114.108 192.168.114.60  TCP        66 53 → 54854 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
  24 1.035298  192.168.114.60  192.168.114.108 DNS        88 Standard query 0xcba0 A sites.google.com
  25 1.035377  192.168.114.60  192.168.114.108 TCP        54 54853 → 53 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  26 1.035426  192.168.114.60  192.168.114.108 TCP        54 54854 → 53 [ACK] Seq=1 Ack=1 Win=65536 Len=0
```

```
> Frame 1708: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF
> Ethernet II, Src: IntelCor_a8:0e:67 (2c:6e:85:a8:0e:67), Dst: 82:9b:e9:47:1c:c6 (82:9b:e9:47:1
> Internet Protocol Version 4, Src: 192.168.114.60, Dst: 52.98.59.18
> Transmission Control Protocol, Src Port: 52293, Dst Port: 443, Seq: 2, Ack: 1, Len: 0
```

```
0000  82 9b e9 47 1c c6 2c 6e  85 a8 0e 67 08 00 45 00   ···G··,n ···g··E·
0010  00 28 66 ac 40 00 80 06  f1 ca c0 a8 72 3c 34 62   ·(f·@··· ····r<4b
0020  3b 12 cc 45 01 bb d2 0a  51 9d e2 cf c2 78 50 14   ;··E···· Q····xP·
0030  00 00 76 86 00 00                                  ··v···
```

Transmission Control Protocol: Protocol | Packets: 2447 · Displayed: 2317 (94.7%) | Profile: Default