EXPERIMENT NO. 7

Aim: Use Wireshark to understand the operation of TCP/IP layers.

Requirements: Linux/Windows O.S, Compatible version of Wireshark.

Theory:

What is 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.

Some intended purposes

Here are some reasons people use Wireshark:

- Network administrators use it to *troubleshoot network problems*
- Network security engineers use it to *examine security problems*
- QA engineers use it to *verify network applications*
- Developers use it to *debug protocol implementations*
- People use it to *learn network protocol* internals

Wireshark can also be helpful in many other situations.

Features:

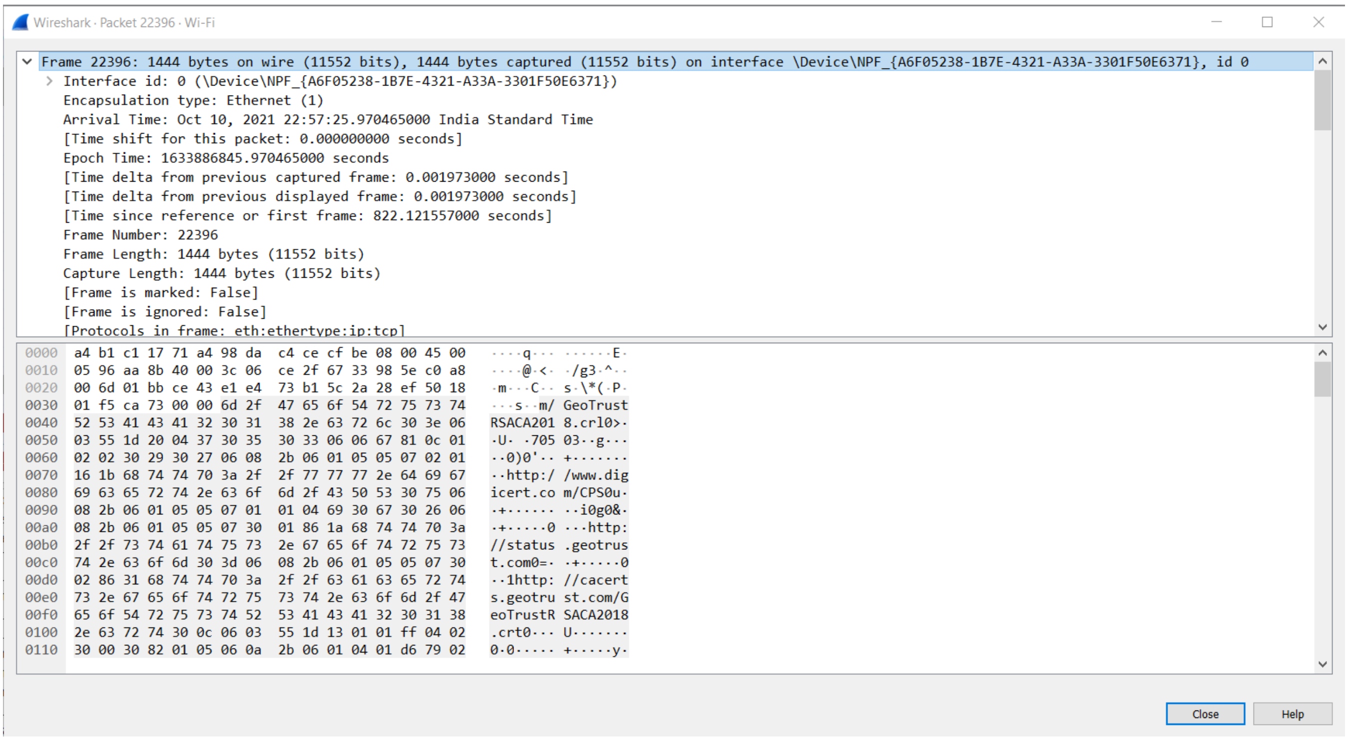
The following are some of the many features Wireshark provides:

- Available for *UNIX* and *Windows*.
- *Capture* live packet data from a network interface.
- *Open* files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.
- *Import* packets from text files containing hex dumps of packet data.
- Display packets with *very detailed protocol information*.
- *Save* packet data captured.
- *Export* some or all packets in a number of capture file formats.
- *Filter packets* on many criteria.
- *Search* for packets on many criteria.
- *Colorize* packet display based on filters.

- Create various *statistics*.
- …And *a lot more!*

Wireshark Output:

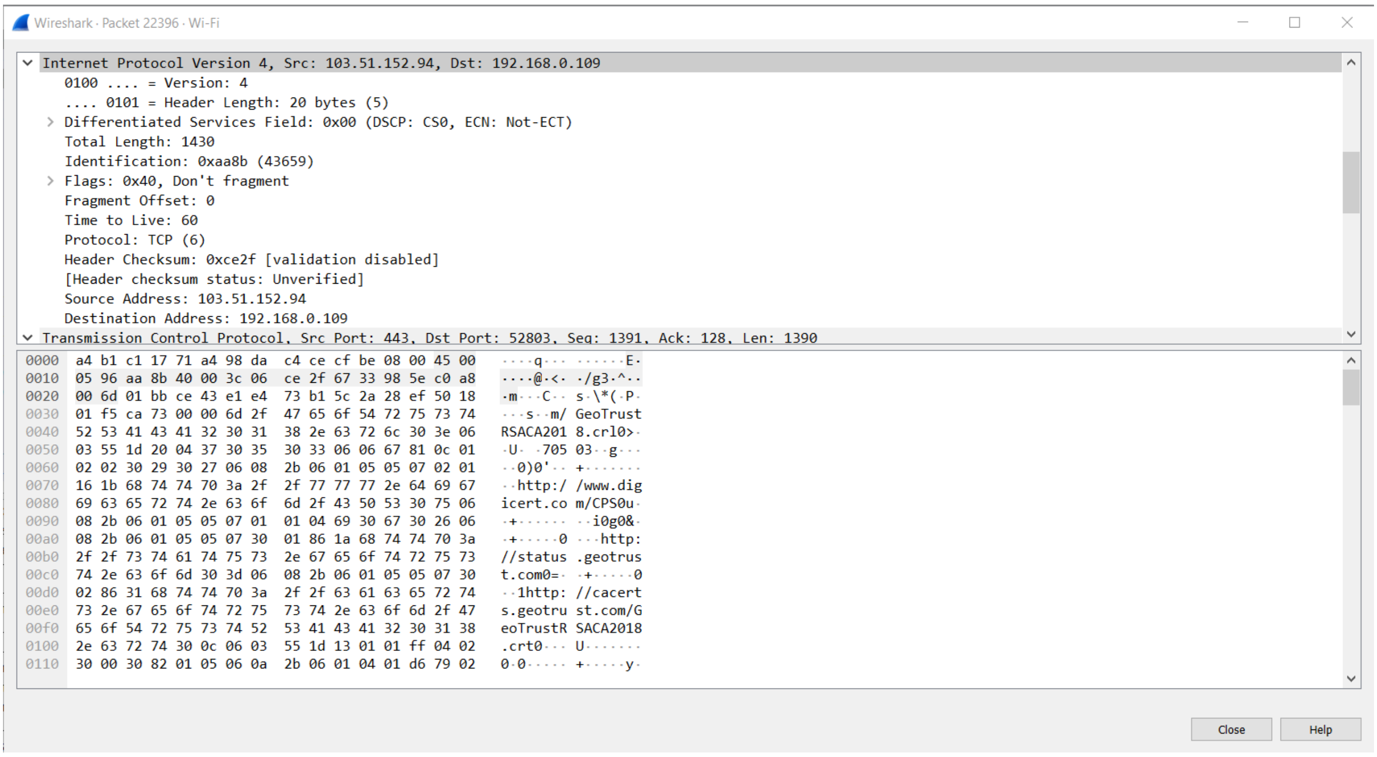
Frame Header and Frame Size:



```
Frame 22396: 1444 bytes on wire (11552 bits), 1444 bytes captured (11552 bits) on interface \Device\NPF_{A6F05238-1B7E-4321-A33A-3301F50E6371}, id 0
  > Interface id: 0 (\Device\NPF_{A6F05238-1B7E-4321-A33A-3301F50E6371})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 10, 2021 22:57:25.970465000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1633886845.970465000 seconds
    [Time delta from previous captured frame: 0.001973000 seconds]
    [Time delta from previous displayed frame: 0.001973000 seconds]
    [Time since reference or first frame: 822.121557000 seconds]
    Frame Number: 22396
    Frame Length: 1444 bytes (11552 bits)
    Capture Length: 1444 bytes (11552 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
```

```
0000  a4 b1 c1 17 71 a4 98 da  c4 ce cf be 08 00 45 00   ····q··· ······E·
0010  05 96 aa 8b 40 00 3c 06  ce 2f 67 33 98 5e c0 a8   ····@·<· ·/g3·^··
0020  00 6d 01 bb ce 43 e1 e4  73 b1 5c 2a 28 ef 50 18   ·m···C·· s·\*(·P·
0030  01 f5 ca 73 00 00 6d 2f  47 65 6f 54 72 75 73 74   ···s··m/ GeoTrust
0040  52 53 41 43 41 32 30 31  38 2e 63 72 6c 30 3e 06   RSACA201 8.crl0>·
0050  03 55 1d 20 04 37 30 35  30 33 06 06 67 81 0c 01   ·U· ·705 03··g···
0060  02 02 30 29 30 27 06 08  2b 06 01 05 05 07 02 01   ··0)0'·· +·······
0070  16 1b 68 74 74 70 3a 2f  2f 77 77 77 2e 64 69 67   ··http:/ /www.dig
0080  69 63 65 72 74 2e 63 6f  6d 2f 43 50 53 30 75 06   icert.co m/CPS0u·
0090  08 2b 06 01 05 05 07 01  01 04 69 30 67 30 26 06   ·+······ ··i0g0&·
00a0  08 2b 06 01 05 05 07 30  01 86 1a 68 74 74 70 3a   ·+·····0 ···http:
00b0  2f 2f 73 74 61 74 75 73  2e 67 65 6f 74 72 75 73   //status .geotrus
00c0  74 2e 63 6f 6d 30 3d 06  08 2b 06 01 05 05 07 30   t.com0=· ·+·····0
00d0  02 86 31 68 74 74 70 3a  2f 2f 63 61 63 65 72 74   ··1http: //cacert
00e0  73 2e 67 65 6f 74 72 75  73 74 2e 63 6f 6d 2f 47   s.geotru st.com/G
00f0  65 6f 54 72 75 73 74 52  53 41 43 41 32 30 31 38   eoTrustR SACA2018
0100  2e 63 72 74 30 0c 06 03  55 1d 13 01 01 ff 04 02   .crt0··· U·······
0110  30 00 30 82 01 05 06 0a  2b 06 01 04 01 d6 79 02   0·0····· +·····y·
```

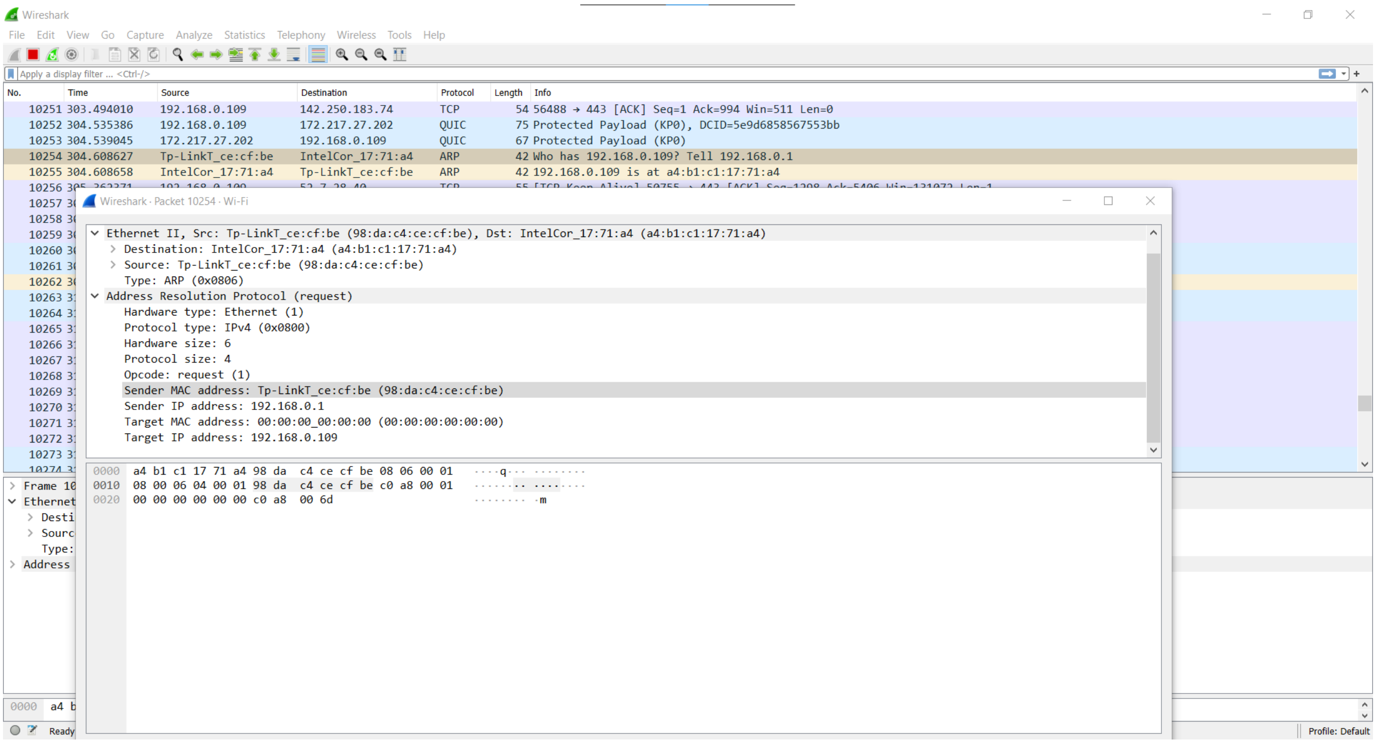
IP header:



```
Internet Protocol Version 4, Src: 103.51.152.94, Dst: 192.168.0.109
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1430
    Identification: 0xaa8b (43659)
  > Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 60
    Protocol: TCP (6)
    Header Checksum: 0xce2f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 103.51.152.94
    Destination Address: 192.168.0.109
Transmission Control Protocol, Src Port: 443, Dst Port: 52803, Seq: 1391, Ack: 128, Len: 1390
```

```
0000  a4 b1 c1 17 71 a4 98 da  c4 ce cf be 08 00 45 00   ····q··· ······E·
0010  05 96 aa 8b 40 00 3c 06  ce 2f 67 33 98 5e c0 a8   ····@·<· ·/g3·^··
0020  00 6d 01 bb ce 43 e1 e4  73 b1 5c 2a 28 ef 50 18   ·m···C·· s·\*(·P·
0030  01 f5 ca 73 00 00 6d 2f  47 65 6f 54 72 75 73 74   ···s··m/ GeoTrust
0040  52 53 41 43 41 32 30 31  38 2e 63 72 6c 30 3e 06   RSACA201 8.crl0>·
0050  03 55 1d 20 04 37 30 35  30 33 06 06 67 81 0c 01   ·U· ·705 03··g···
0060  02 02 30 29 30 27 06 08  2b 06 01 05 05 07 02 01   ··0)0'·· +·······
0070  16 1b 68 74 74 70 3a 2f  2f 77 77 77 2e 64 69 67   ··http:/ /www.dig
0080  69 63 65 72 74 2e 63 6f  6d 2f 43 50 53 30 75 06   icert.co m/CPS0u·
0090  08 2b 06 01 05 05 07 01  01 04 69 30 67 30 26 06   ·+······ ··i0g0&·
00a0  08 2b 06 01 05 05 07 30  01 86 1a 68 74 74 70 3a   ·+·····0 ···http:
00b0  2f 2f 73 74 61 74 75 73  2e 67 65 6f 74 72 75 73   //status .geotrus
00c0  74 2e 63 6f 6d 30 3d 06  08 2b 06 01 05 05 07 30   t.com0=· ·+·····0
00d0  02 86 31 68 74 74 70 3a  2f 2f 63 61 63 65 72 74   ··1http: //cacert
00e0  73 2e 67 65 6f 74 72 75  73 74 2e 63 6f 6d 2f 47   s.geotru st.com/G
00f0  65 6f 54 72 75 73 74 52  53 41 43 41 32 30 31 38   eoTrustR SACA2018
0100  2e 63 72 74 30 0c 06 03  55 1d 13 01 01 ff 04 02   .crt0··· U·······
0110  30 00 30 82 01 05 06 0a  2b 06 01 04 01 d6 79 02   0·0····· +·····y·
```

MAC Address and ARP:

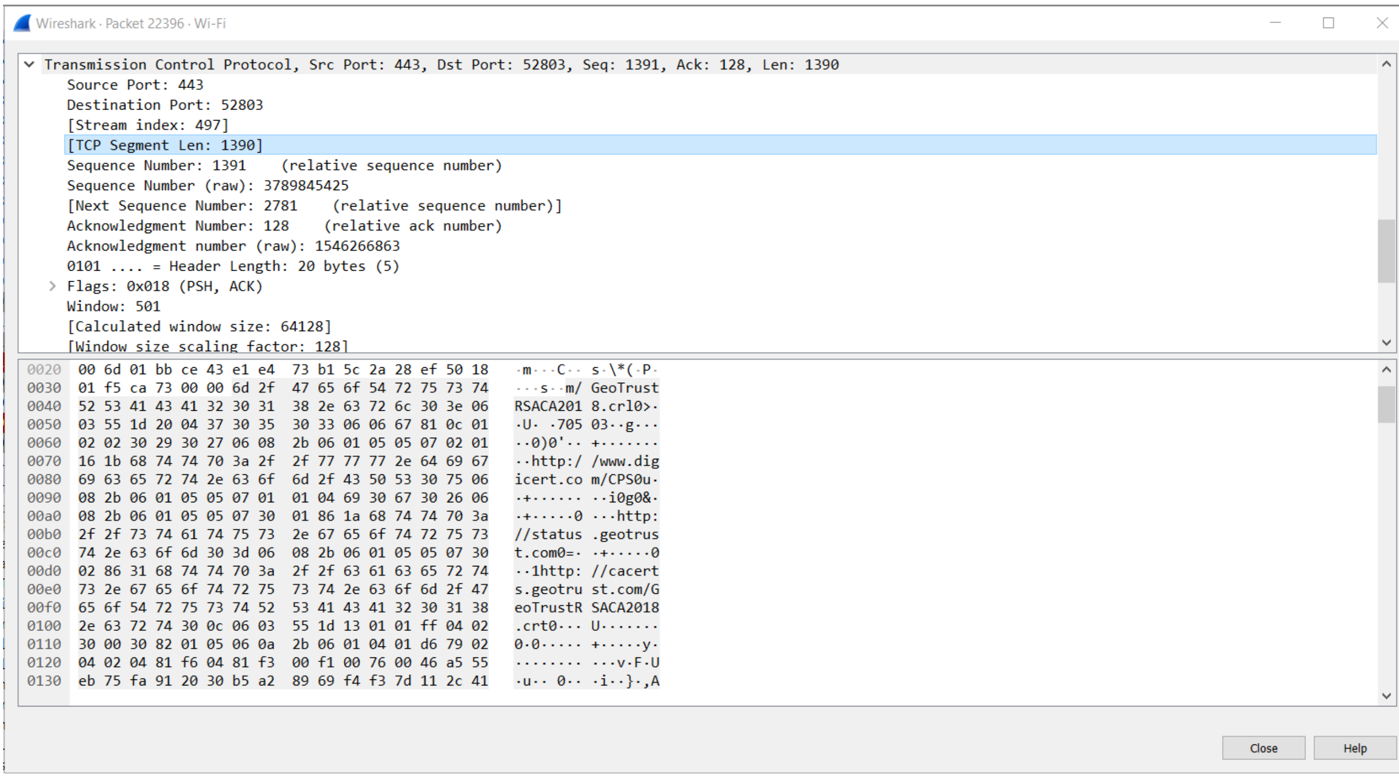

Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireshark · Packet 10254 · Wi-Fi
Ready
Profile: Default

```
No.   Time       Source             Destination        Protocol Length Info
10251 303.494010 192.168.0.109      142.250.183.74     TCP        54 56488 → 443 [ACK] Seq=1 Ack=994 Win=511 Len=0
10252 304.535386 192.168.0.109      172.217.27.202     QUIC       75 Protected Payload (KP0), DCID=5e9d6858567553bb
10253 304.539045 172.217.27.202     192.168.0.109      QUIC       67 Protected Payload (KP0)
10254 304.608627 Tp-LinkT_ce:cf:be  IntelCor_17:71:a4  ARP        42 Who has 192.168.0.109? Tell 192.168.0.1
10255 304.608658 IntelCor_17:71:a4  Tp-LinkT_ce:cf:be  ARP        42 192.168.0.109 is at a4:b1:c1:17:71:a4
10256 305.362371 192.168.0.109      52.7.28.40         TCP        55 [TCP Keep-Alive] 50755 → 443 [ACK] Seq=1298 Ack=5406 Win=131072 Len=1
```

```
v Ethernet II, Src: Tp-LinkT_ce:cf:be (98:da:c4:ce:cf:be), Dst: IntelCor_17:71:a4 (a4:b1:c1:17:71:a4)
  > Destination: IntelCor_17:71:a4 (a4:b1:c1:17:71:a4)
  > Source: Tp-LinkT_ce:cf:be (98:da:c4:ce:cf:be)
    Type: ARP (0x0806)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Tp-LinkT_ce:cf:be (98:da:c4:ce:cf:be)
    Sender IP address: 192.168.0.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.0.109
```

```
0000  a4 b1 c1 17 71 a4 98 da  c4 ce cf be 08 06 00 01   ····q··· ········
0010  08 00 06 04 00 01 98 da  c4 ce cf be c0 a8 00 01   ········ ········
0020  00 00 00 00 00 00 c0 a8  00 6d                     ········ ·m
```

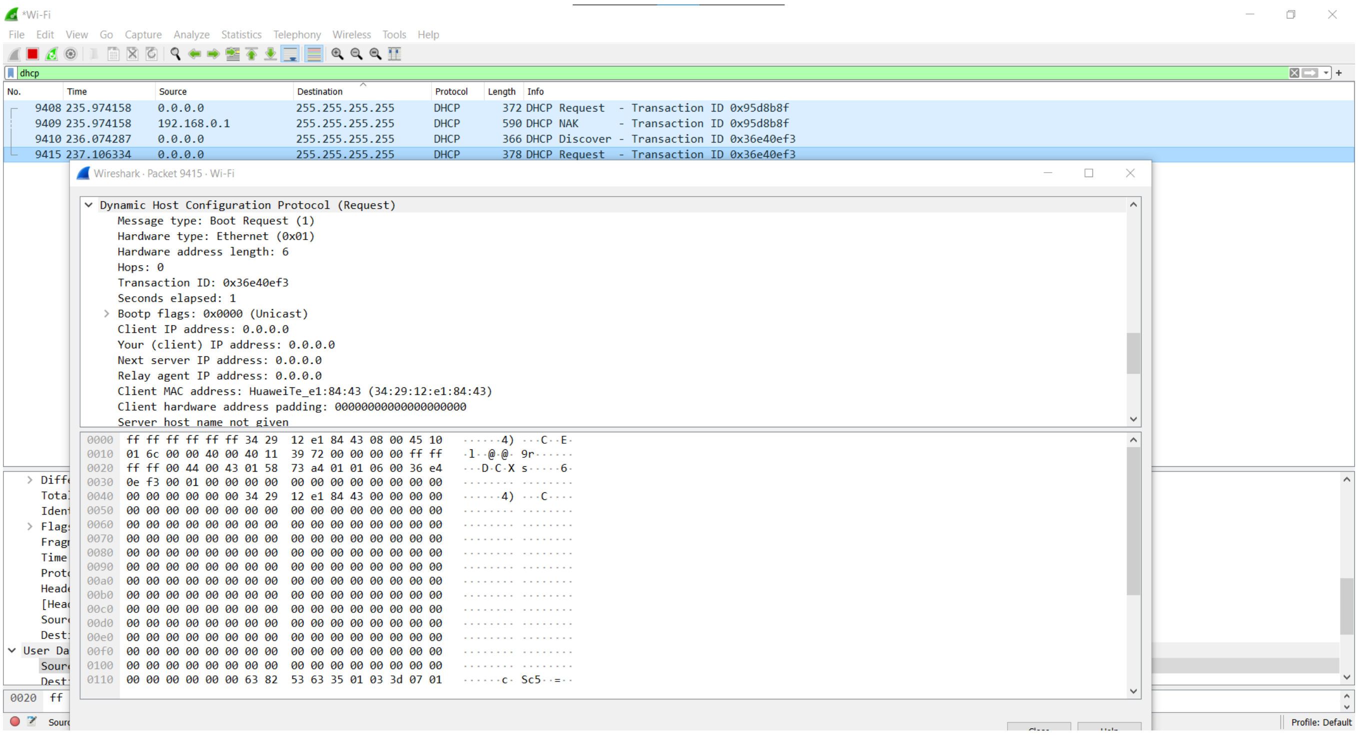
TCP Header:



```
v Transmission Control Protocol, Src Port: 443, Dst Port: 52803, Seq: 1391, Ack: 128, Len: 1390
    Source Port: 443
    Destination Port: 52803
    [Stream index: 497]
    [TCP Segment Len: 1390]
    Sequence Number: 1391    (relative sequence number)
    Sequence Number (raw): 3789845425
    [Next Sequence Number: 2781    (relative sequence number)]
    Acknowledgment Number: 128    (relative ack number)
    Acknowledgment number (raw): 1546266863
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 501
    [Calculated window size: 64128]
    [Window size scaling factor: 128]
```

```
0020  00 6d 01 bb ce 43 e1 e4  73 b1 5c 2a 28 ef 50 18   ·m···C·· s·\*(·P·
0030  01 f5 ca 73 00 00 6d 2f  47 65 6f 54 72 75 73 74   ···s··m/ GeoTrust
0040  52 53 41 43 41 32 30 31  38 2e 63 72 6c 30 3e 06   RSACA201 8.crl0>·
0050  03 55 1d 20 04 37 30 35  30 33 06 06 67 81 0c 01   ·U· ·705 03··g···
0060  02 02 30 29 30 27 06 08  2b 06 01 05 05 07 02 01   ··0)0'·· +·······
0070  16 1b 68 74 74 70 3a 2f  2f 77 77 77 2e 64 69 67   ··http:/ /www.dig
0080  69 63 65 72 74 2e 63 6f  6d 2f 43 50 53 30 75 06   icert.co m/CPS0u·
0090  08 2b 06 01 05 05 07 01  01 04 69 30 67 30 26 06   ·+······ ··i0g0&·
00a0  08 2b 06 01 05 05 07 30  01 86 1a 68 74 74 70 3a   ·+·····0 ···http:
00b0  2f 2f 73 74 61 74 75 73  2e 67 65 6f 74 72 75 73   //status .geotrus
00c0  74 2e 63 6f 6d 30 3d 06  08 2b 06 01 05 05 07 30   t.com0=· ·+·····0
00d0  02 86 31 68 74 74 70 3a  2f 2f 63 61 63 65 72 74   ··1http: //cacert
00e0  73 2e 67 65 6f 74 72 75  73 74 2e 63 6f 6d 2f 47   s.geotru st.com/G
00f0  65 6f 54 72 75 73 74 52  53 41 43 41 32 30 31 38   eoTrustR SACA2018
0100  2e 63 72 74 30 0c 06 03  55 1d 13 01 01 ff 04 02   .crt0··· U·······
0110  30 00 30 82 01 05 06 0a  2b 06 01 04 01 d6 79 02   0·0····· +·····y·
0120  04 02 04 81 f6 04 81 f3  00 f1 00 76 00 46 a5 55   ········ ···v·F·U
0130  eb 75 fa 91 20 30 b5 a2  89 69 f4 f3 7d 11 2c 41   ·u·· 0·· ·i··}·,A
```

DHCP:

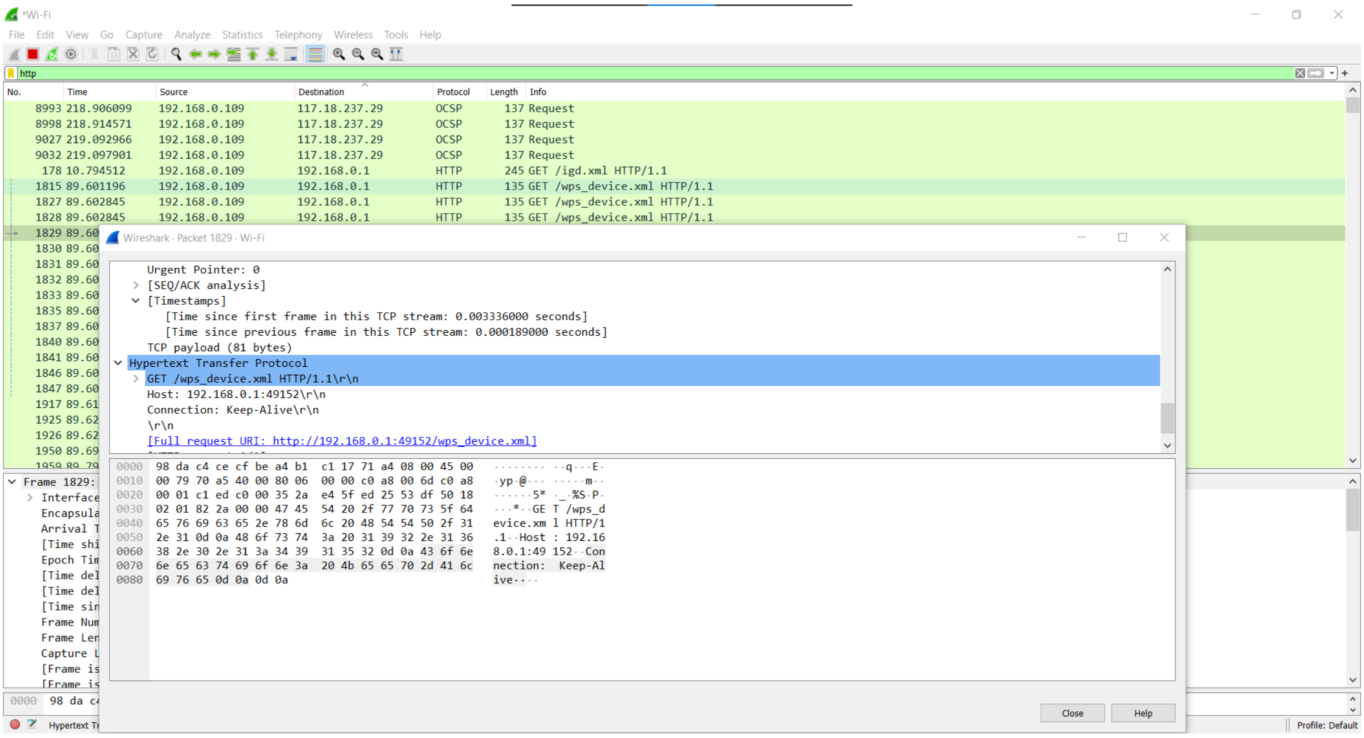

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp
Wireshark · Packet 9415 · Wi-Fi
Profile: Default

```
No.   Time        Source       Destination      Protocol Length Info
 9408 235.974158  0.0.0.0      255.255.255.255  DHCP     372 DHCP Request  - Transaction ID 0x95d8b8f
 9409 235.974158  192.168.0.1  255.255.255.255  DHCP     590 DHCP NAK      - Transaction ID 0x95d8b8f
 9410 236.074287  0.0.0.0      255.255.255.255  DHCP     366 DHCP Discover - Transaction ID 0x36e40ef3
 9415 237.106334  0.0.0.0      255.255.255.255  DHCP     378 DHCP Request  - Transaction ID 0x36e40ef3
```

```
Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x36e40ef3
    Seconds elapsed: 1
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: HuaweiTe_e1:84:43 (34:29:12:e1:84:43)
    Client hardware address padding: 00000000000000000000
    Server host name not given
```

```
0000  ff ff ff ff ff ff 34 29  12 e1 84 43 08 00 45 10   ······4) ···C··E·
0010  01 6c 00 00 40 00 40 11  39 72 00 00 00 00 ff ff   ·l··@·@· 9r······
0020  ff ff 00 44 00 43 01 58  73 a4 01 01 06 00 36 e4   ···D·C·X s·····6·
0030  0e f3 00 01 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 34 29  12 e1 84 43 00 00 00 00   ······4) ···C····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 03 3d 07 01   ······c· Sc5··=··
```

HTTP:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Wireshark · Packet 1829 · Wi-Fi
Close
Help
Profile: Default

```
No.   Time        Source         Destination    Protocol Length Info
 8993 218.906099  192.168.0.109  117.18.237.29  OCSP     137 Request
 8998 218.914571  192.168.0.109  117.18.237.29  OCSP     137 Request
 9027 219.092966  192.168.0.109  117.18.237.29  OCSP     137 Request
 9032 219.097901  192.168.0.109  117.18.237.29  OCSP     137 Request
  178 10.794512   192.168.0.109  192.168.0.1    HTTP     245 GET /igd.xml HTTP/1.1
 1815 89.601196   192.168.0.109  192.168.0.1    HTTP     135 GET /wps_device.xml HTTP/1.1
 1827 89.602845   192.168.0.109  192.168.0.1    HTTP     135 GET /wps_device.xml HTTP/1.1
 1828 89.602845   192.168.0.109  192.168.0.1    HTTP     135 GET /wps_device.xml HTTP/1.1
 1829 89.60
 1830 89.60
 1831 89.60
 1832 89.60
 1833 89.60
 1835 89.60
 1837 89.60
 1840 89.60
 1841 89.60
 1846 89.60
 1847 89.60
 1917 89.61
 1925 89.62
 1926 89.62
 1950 89.69
```

```
    Urgent Pointer: 0
  > [SEQ/ACK analysis]
  v [Timestamps]
      [Time since first frame in this TCP stream: 0.003336000 seconds]
      [Time since previous frame in this TCP stream: 0.000189000 seconds]
    TCP payload (81 bytes)
v Hypertext Transfer Protocol
  > GET /wps_device.xml HTTP/1.1\r\n
    Host: 192.168.0.1:49152\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://192.168.0.1:49152/wps_device.xml]
```

```
0000  98 da c4 ce cf be a4 b1  c1 17 71 a4 08 00 45 00   ········ ··q···E·
0010  00 79 70 a5 40 00 80 06  00 00 c0 a8 00 6d c0 a8   ·yp·@··· ·····m··
0020  00 01 c1 ed c0 00 35 2a  e4 5f ed 25 53 df 50 18   ······5* ·_·%S·P·
0030  02 01 82 2a 00 00 47 45  54 20 2f 77 70 73 5f 64   ···*··GE T /wps_d
0040  65 76 69 63 65 2e 78 6d  6c 20 48 54 54 50 2f 31   evice.xm l HTTP/1
0050  2e 31 0d 0a 48 6f 73 74  3a 20 31 39 32 2e 31 36   .1··Host : 192.16
0060  38 2e 30 2e 31 3a 34 39  31 35 32 0d 0a 43 6f 6e   8.0.1:49 152··Con
0070  6e 65 63 74 69 6f 6e 3a  20 4b 65 65 70 2d 41 6c   nection:  Keep-Al
0080  69 76 65 0d 0a 0d 0a                               ive····
```

Conclusion: We have successfully use Wireshark to understand the operation of TCP/IP layers and use it to get different header formats of packets.