Wireshark Packet Capture

Amrith M

April 9, 2018

1 About Wireshark

Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.[5]

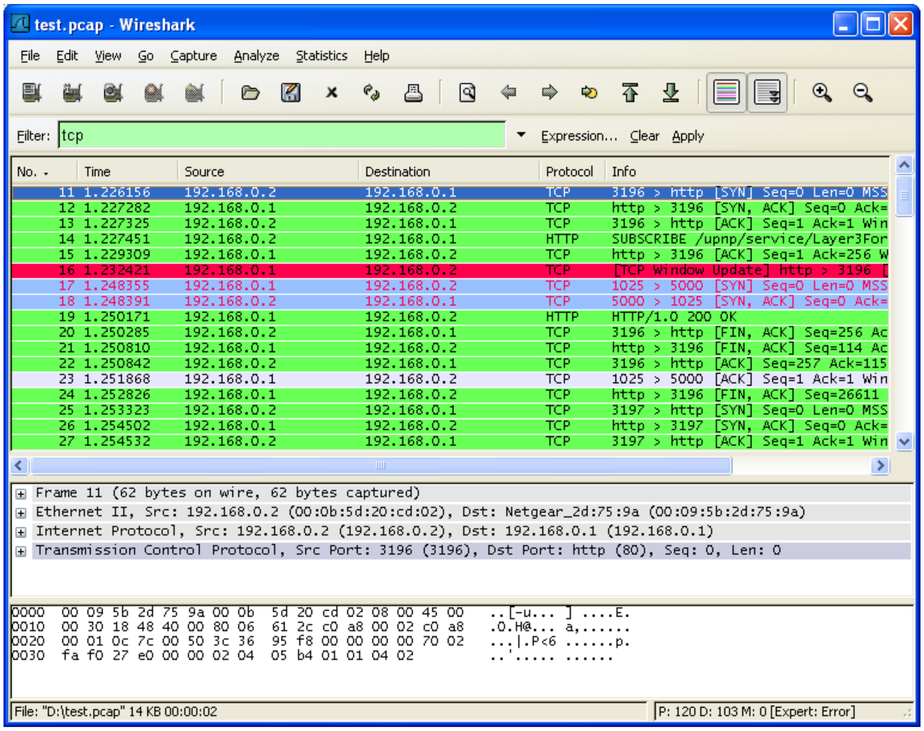
Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License.

2 TCP Packet Capture

TCP Packets are captured and 3-way handshake is observed. (figure below)

3 UDP Packet Capture

UDP packets are captured and sending datagrams in a connectionless service is observed. (figure below)



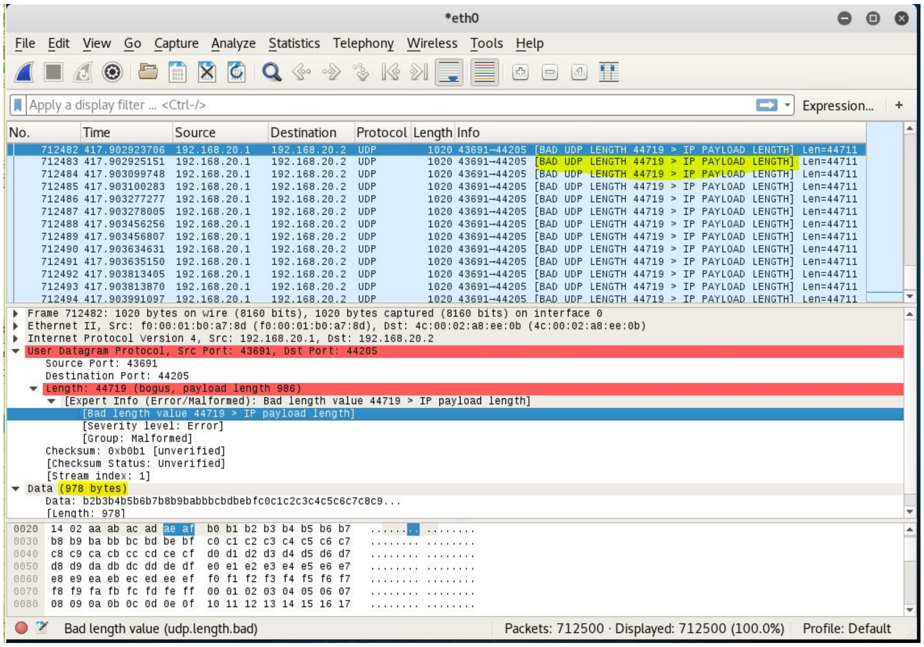
Filter: tcp

```
No.  Time       Source        Destination   Protocol  Info
  11 1.226156   192.168.0.2   192.168.0.1   TCP       3196 > http [SYN] Seq=0 Len=0 MSS
  12 1.227282   192.168.0.1   192.168.0.2   TCP       http > 3196 [SYN, ACK] Seq=0 Ack=
  13 1.227325   192.168.0.2   192.168.0.1   TCP       3196 > http [ACK] Seq=1 Ack=1 Win
  14 1.227451   192.168.0.2   192.168.0.1   HTTP      SUBSCRIBE /upnp/service/Layer3For
  15 1.229309   192.168.0.1   192.168.0.2   TCP       http > 3196 [ACK] Seq=1 Ack=256 W
  16 1.232421   192.168.0.1   192.168.0.2   TCP       [TCP Window Update] http > 3196 [
  17 1.248355   192.168.0.1   192.168.0.2   TCP       1025 > 5000 [SYN] Seq=0 Len=0 MSS
  18 1.248391   192.168.0.2   192.168.0.1   TCP       5000 > 1025 [SYN, ACK] Seq=0 Ack=
  19 1.250171   192.168.0.1   192.168.0.2   HTTP      HTTP/1.0 200 OK
  20 1.250285   192.168.0.2   192.168.0.1   TCP       3196 > http [FIN, ACK] Seq=256 Ac
  21 1.250810   192.168.0.1   192.168.0.2   TCP       http > 3196 [FIN, ACK] Seq=114 Ac
  22 1.250842   192.168.0.2   192.168.0.1   TCP       3196 > http [ACK] Seq=257 Ack=115
  23 1.251868   192.168.0.1   192.168.0.2   TCP       1025 > 5000 [ACK] Seq=1 Ack=1 Win
  24 1.252826   192.168.0.1   192.168.0.2   TCP       http > 3196 [FIN, ACK] Seq=26611
  25 1.253323   192.168.0.2   192.168.0.1   TCP       3197 > http [SYN] Seq=0 Len=0 MSS
  26 1.254502   192.168.0.1   192.168.0.2   TCP       http > 3197 [SYN, ACK] Seq=0 Ack=
  27 1.254532   192.168.0.2   192.168.0.1   TCP       3197 > http [ACK] Seq=1 Ack=1 Win
```

```
⊞ Frame 11 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
⊞ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
⊞ Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0
```

```
0000  00 09 5b 2d 75 9a 00 0b  5d 20 cd 02 08 00 45 00   ..[-u... ] ....E.
0010  00 30 18 48 40 00 80 06  61 2c c0 a8 00 02 c0 a8   .0.H@... a,......
0020  00 01 0c 7c 00 50 3c 36  95 f8 00 00 00 00 70 02   ...|.P<6 ......p.
0030  fa f0 27 e0 00 00 02 04  05 b4 01 01 04 02         ..'..... ......
```

```
File: "D:\test.pcap" 14 KB 00:00:02        P: 120 D: 103 M: 0 [Expert: Error]
```



```
No.     Time           Source        Destination   Protocol Length Info
 712482 417.902923706  192.168.20.1  192.168.20.2  UDP      1020 43691→44205 [BAD UDP LENGTH 44719 > IP PAYLOAD LENGTH] Len=44711
 712483 417.902925151  192.168.20.1  192.168.20.2  UDP      1020 43691→44205 [BAD UDP LENGTH 44719 > IP PAYLOAD LENGTH] Len=44711
 712484 417.903099748  192.168.20.1  192.168.20.2  UDP      1020 43691→44205 [BAD UDP LENGTH 44719 > IP PAYLOAD LENGTH] Len=44711
 712485 417.903100283  192.168.20.1  192.168.20.2  UDP      1020 43691→44205 [BAD UDP LENGTH 44719 > IP PAYLOAD LENGTH] Len=44711
 712486 417.903277277  192.168.20.1  192.168.20.2  UDP      1020 43691→44205 [BAD UDP LENGTH 44719 > IP PAYLOAD LENGTH] Len=44711
 712487 417.903278005  192.168.20.1  192.168.20.2  UDP      1020 43691→44205 [BAD UDP LENGTH 44719 > IP PAYLOAD LENGTH] Len=44711
 712488 417.903456256  192.168.20.1  192.168.20.2  UDP      1020 43691→44205 [BAD UDP LENGTH 44719 > IP PAYLOAD LENGTH] Len=44711
 712489 417.903456807  192.168.20.1  192.168.20.2  UDP      1020 43691→44205 [BAD UDP LENGTH 44719 > IP PAYLOAD LENGTH] Len=44711
 712490 417.903634631  192.168.20.1  192.168.20.2  UDP      1020 43691→44205 [BAD UDP LENGTH 44719 > IP PAYLOAD LENGTH] Len=44711
 712491 417.903635150  192.168.20.1  192.168.20.2  UDP      1020 43691→44205 [BAD UDP LENGTH 44719 > IP PAYLOAD LENGTH] Len=44711
 712492 417.903813405  192.168.20.1  192.168.20.2  UDP      1020 43691→44205 [BAD UDP LENGTH 44719 > IP PAYLOAD LENGTH] Len=44711
 712493 417.903813870  192.168.20.1  192.168.20.2  UDP      1020 43691→44205 [BAD UDP LENGTH 44719 > IP PAYLOAD LENGTH] Len=44711
 712494 417.903991097  192.168.20.1  192.168.20.2  UDP      1020 43691→44205 [BAD UDP LENGTH 44719 > IP PAYLOAD LENGTH] Len=44711
```

```
▶ Frame 712482: 1020 bytes on wire (8160 bits), 1020 bytes captured (8160 bits) on interface 0
▶ Ethernet II, Src: f0:00:01:b0:a7:8d (f0:00:01:b0:a7:8d), Dst: 4c:00:02:a8:ee:0b (4c:00:02:a8:ee:0b)
▶ Internet Protocol Version 4, Src: 192.168.20.1, Dst: 192.168.20.2
▼ User Datagram Protocol, Src Port: 43691, Dst Port: 44205
    Source Port: 43691
    Destination Port: 44205
  ▼ Length: 44719 (bogus, payload length 986)
    ▼ [Expert Info (Error/Malformed): Bad length value 44719 > IP payload length]
        [Bad length value 44719 > IP payload length]
        [Severity level: Error]
        [Group: Malformed]
    Checksum: 0xb0b1 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
▼ Data (978 bytes)
    Data: b2b3b4b5b6b7b8b9babbbcbdbebfc0c1c2c3c4c5c6c7c8c9...
    [Length: 978]
```

```
0020  14 02 aa ab ac ad ae af  b0 b1 b2 b3 b4 b5 b6 b7   ........ ........
0030  b8 b9 ba bb bc bd be bf  c0 c1 c2 c3 c4 c5 c6 c7   ........ ........
0040  c8 c9 ca cb cc cd ce cf  d0 d1 d2 d3 d4 d5 d6 d7   ........ ........
0050  d8 d9 da db dc dd de df  e0 e1 e2 e3 e4 e5 e6 e7   ........ ........
0060  e8 e9 ea eb ec ed ee ef  f0 f1 f2 f3 f4 f5 f6 f7   ........ ........
0070  f8 f9 fa fb fc fd fe ff  00 01 02 03 04 05 06 07   ........ ........
0080  08 09 0a 0b 0c 0d 0e 0f  10 11 12 13 14 15 16 17   ........ ........
```

```
Bad length value (udp.length.bad)      Packets: 712500 · Displayed: 712500 (100.0%)      Profile: Default
```