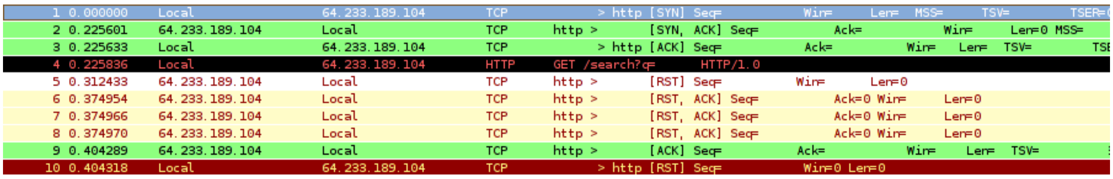
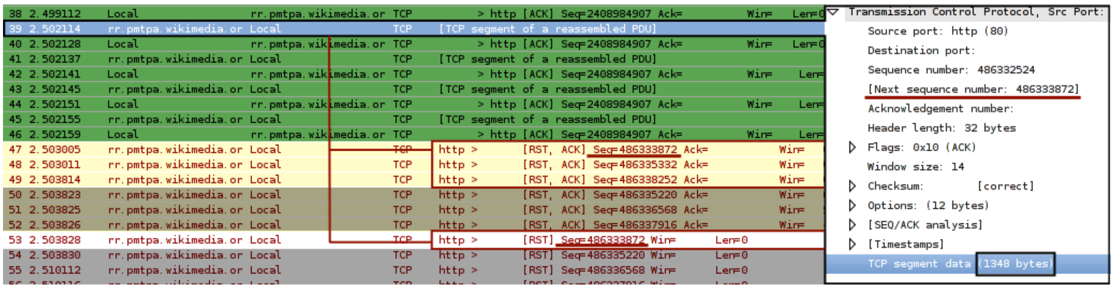
```
-- gfw protocol
do
 ip_id_f = Field.new("ip.id");
 ip_df_f = Field.new("ip.flags.df");
 tcp_win_f = Field.new("tcp.window_size");
 gfw_proto = Proto("gfw", "GFW Postdissector")
 type_F = ProtoField.uint8("gfw.type", "Type")
 gfw_proto.fields = { type_F }
 function gfw_proto.dissector(buffer, pinfo, tree)
   local _ip_id = ip_id_f()
   local _tcp_win = tcp_win_f()
   local _ip_df = ip_df_f()
   local ip_id = tonumber(tostring(_ip_id))
   local tcp_win = tonumber(tostring(_tcp_win))
   local ip_df = tonumber(tostring(_ip_df))
   if (tcp_win ~= nil) and (ip_id ~= nil) and (ip_df ~= nil) then
     local type1, type2
     if (ip_id == 64) and (tcp_win % 17 == 0) and (ip_df == 0) then
       type1 = true
     end
     local id = 65535 - tcp_win * 13;
     if id < 0 then id = id + 65536 end
     if (id == ip_id) and ip_df then
       type2 = true
     end
     if type1 or type2 then
       local subtree = tree:add(gfw_proto, "GFW Protocol Info")
       if type1 then subtree:add(type_F, 1)
       else subtree:add(type_F, 2) end
     end
   end
 end
 register_postdissector(gfw_proto)
end
```

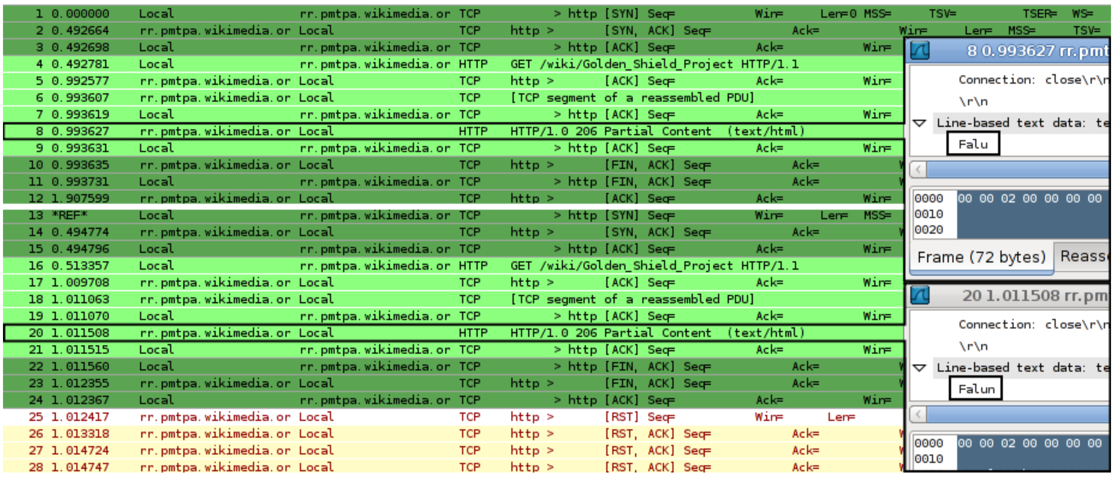


```
 1 0.000000  Local           64.233.189.104  TCP            > http [SYN] Seq=           Win=    Len=  MSS=    TSV=       TSER=
 2 0.225601  64.233.189.104  Local           TCP   http >        [SYN, ACK] Seq=         Ack=          Win=    Len=0 MSS=
 3 0.225633  Local           64.233.189.104  TCP            > http [ACK] Seq=           Ack=          Win=   Len=  TSV=       TSE
 4 0.225836  Local           64.233.189.104  HTTP  GET /search?q=       HTTP/1.0
 5 0.312433  64.233.189.104  Local           TCP   http >        [RST] Seq=          Win=      Len=0
 6 0.374954  64.233.189.104  Local           TCP   http >        [RST, ACK] Seq=         Ack=0 Win=     Len=0
 7 0.374966  64.233.189.104  Local           TCP   http >        [RST, ACK] Seq=         Ack=0 Win=     Len=0
 8 0.374970  64.233.189.104  Local           TCP   http >        [RST, ACK] Seq=         Ack=0 Win=     Len=0
 9 0.404289  64.233.189.104  Local           TCP   http >        [ACK] Seq=          Ack=          Win=    Len=  TSV=
10 0.404318  Local           64.233.189.104  TCP            > http [RST] Seq=           Win=0 Len=0
```



```
38 2.499112  Local                 rr.pmtpa.wikimedia.or TCP       > http [ACK] Seq=2408984907 Ack=        Win=   Len=0
39 2.502114  rr.pmtpa.wikimedia.or Local                 TCP  [TCP segment of a reassembled PDU]
40 2.502128  Local                 rr.pmtpa.wikimedia.or TCP       > http [ACK] Seq=2408984907 Ack=        Win=   Len=0
41 2.502137  rr.pmtpa.wikimedia.or Local                 TCP  [TCP segment of a reassembled PDU]
42 2.502141  Local                 rr.pmtpa.wikimedia.or TCP       > http [ACK] Seq=2408984907 Ack=        Win=    Len=
43 2.502145  rr.pmtpa.wikimedia.or Local                 TCP  [TCP segment of a reassembled PDU]
44 2.502151  Local                 rr.pmtpa.wikimedia.or TCP       > http [ACK] Seq=2408984907 Ack=        Win=    Len=
45 2.502155  rr.pmtpa.wikimedia.or Local                 TCP  [TCP segment of a reassembled PDU]
46 2.502159  Local                 rr.pmtpa.wikimedia.or TCP       > http [ACK] Seq=2408984907 Ack=        Win=    Len=
47 2.503005  rr.pmtpa.wikimedia.or Local                 TCP  http >     [RST, ACK] Seq=486333872 Ack=        Win=
48 2.503011  rr.pmtpa.wikimedia.or Local                 TCP  http >     [RST, ACK] Seq=486335332 Ack=        Win=
49 2.503814  rr.pmtpa.wikimedia.or Local                 TCP  http >     [RST, ACK] Seq=486338252 Ack=        Win=
50 2.503823  rr.pmtpa.wikimedia.or Local                 TCP  http >     [RST, ACK] Seq=486335220 Ack=        Win=
51 2.503825  rr.pmtpa.wikimedia.or Local                 TCP  http >     [RST, ACK] Seq=486336568 Ack=        Win=
52 2.503826  rr.pmtpa.wikimedia.or Local                 TCP  http >     [RST, ACK] Seq=486337916 Ack=        Win=
53 2.503828  rr.pmtpa.wikimedia.or Local                 TCP  http >     [RST] Seq=486333872 Win=      Len=0
54 2.503830  rr.pmtpa.wikimedia.or Local                 TCP  http >     [RST] Seq=486335220 Win=      Len=0
55 2.510112  rr.pmtpa.wikimedia.or Local                 TCP  http >     [RST] Seq=486336568 Win=      Len=0
56 2.510116  rr.pmtpa.wikimedia.or Local                 TCP  http >     [RST] Seq=486337916 Win=      Len=0
```

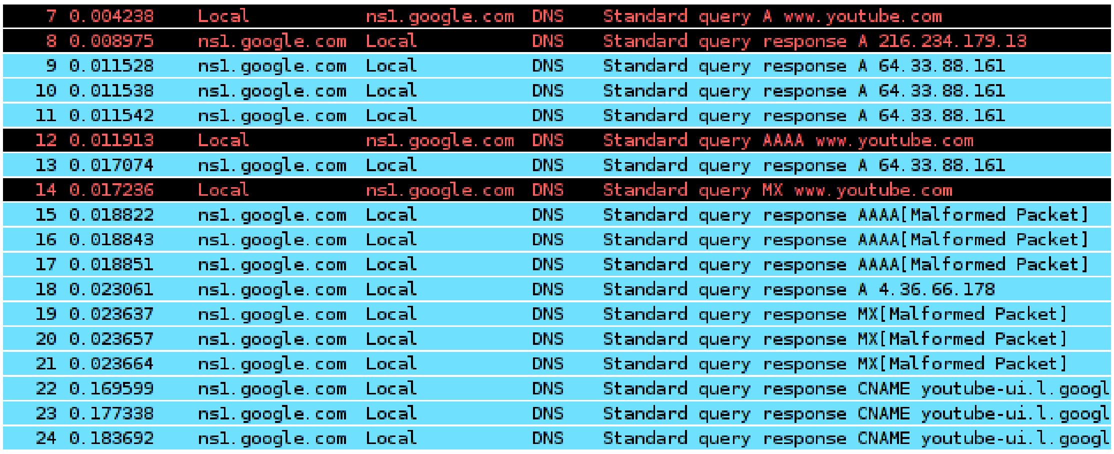
```
▽ Transmission Control Protocol, Src Port:
      Source port: http (80)
      Destination port:
      Sequence number: 486332524
      [Next sequence number: 486333872]
      Acknowledgement number:
      Header length: 32 bytes
  ▷ Flags: 0x10 (ACK)
      Window size: 14
  ▷ Checksum:          [correct]
  ▷ Options: (12 bytes)
  ▷ [SEQ/ACK analysis]
  ▷ [Timestamps]
      TCP segment data (1348 bytes)
```



```
 1 0.000000  Local                 rr.pmtpa.wikimedia.or TCP        > http [SYN] Seq=         Win=     Len=0 MSS=     TSV=         TSER=   WS=
 2 0.492664  rr.pmtpa.wikimedia.or Local                 TCP   http >      [SYN, ACK] Seq=         Ack=          Win=     Len=  MSS=     TSV=
 3 0.492698  Local                 rr.pmtpa.wikimedia.or TCP        > http [ACK] Seq=         Ack=          Win=
 4 0.492781  Local                 rr.pmtpa.wikimedia.or HTTP  GET /wiki/Golden_Shield_Project HTTP/1.1
 5 0.992577  rr.pmtpa.wikimedia.or Local                 TCP   http >      [ACK] Seq=         Ack=          Win=
 6 0.993607  rr.pmtpa.wikimedia.or Local                 TCP   [TCP segment of a reassembled PDU]
 7 0.993619  Local                 rr.pmtpa.wikimedia.or TCP        > http [ACK] Seq=         Ack=          Win=
 8 0.993627  rr.pmtpa.wikimedia.or Local                 HTTP  HTTP/1.0 206 Partial Content  (text/html)
 9 0.993631  Local                 rr.pmtpa.wikimedia.or TCP        > http [ACK] Seq=         Ack=          Win=
10 0.993635  rr.pmtpa.wikimedia.or Local                 TCP   http >      [FIN, ACK] Seq=         Ack=
11 0.993731  Local                 rr.pmtpa.wikimedia.or TCP        > http [FIN, ACK] Seq=         Ack=
12 1.907599  rr.pmtpa.wikimedia.or Local                 TCP   http >      [ACK] Seq=         Ack=          Win=
13 *REF*     Local                 rr.pmtpa.wikimedia.or TCP        > http [SYN] Seq=         Win=     Len=   MSS=
14 0.494774  rr.pmtpa.wikimedia.or Local                 TCP   http >      [SYN, ACK] Seq=         Ack=
15 0.494796  Local                 rr.pmtpa.wikimedia.or TCP        > http [ACK] Seq=         Ack=          Win=
16 0.513357  Local                 rr.pmtpa.wikimedia.or HTTP  GET /wiki/Golden_Shield_Project HTTP/1.1
17 1.009708  rr.pmtpa.wikimedia.or Local                 TCP   http >      [ACK] Seq=         Ack=          Win=
18 1.011063  rr.pmtpa.wikimedia.or Local                 TCP   [TCP segment of a reassembled PDU]
19 1.011070  Local                 rr.pmtpa.wikimedia.or TCP        > http [ACK] Seq=         Ack=          Win=
20 1.011508  rr.pmtpa.wikimedia.or Local                 HTTP  HTTP/1.0 206 Partial Content  (text/html)
21 1.011515  Local                 rr.pmtpa.wikimedia.or TCP        > http [ACK] Seq=         Ack=          Win=
22 1.011560  Local                 rr.pmtpa.wikimedia.or TCP        > http [FIN, ACK] Seq=         Ack=
23 1.012355  rr.pmtpa.wikimedia.or Local                 TCP   http >      [FIN, ACK] Seq=         Ack=
24 1.012367  Local                 rr.pmtpa.wikimedia.or TCP        > http [ACK] Seq=         Ack=          Win=
25 1.012417  rr.pmtpa.wikimedia.or Local                 TCP   http >      [RST] Seq=         Win=     Len=
26 1.013318  rr.pmtpa.wikimedia.or Local                 TCP   http >      [RST, ACK] Seq=         Ack=
27 1.014724  rr.pmtpa.wikimedia.or Local                 TCP   http >      [RST, ACK] Seq=         Ack=
28 1.014747  rr.pmtpa.wikimedia.or Local                 TCP   http >      [RST, ACK] Seq=         Ack=
```

```
8 0.993627 rr.pmt
      Connection: close\r\n
      \r\n
▽ Line-based text data: te
      Falu
0000  00 00 02 00 00 00 00
0010
0020
Frame (72 bytes)   Reass
```

```
20 1.011508 rr.pm
      Connection: close\r\n
      \r\n
▽ Line-based text data: te
      Falun
0000  00 00 02 00 00 00 00
0010
```



```
 7 0.004238  Local           ns1.google.com  DNS  Standard query A www.youtube.com
 8 0.008975  ns1.google.com  Local           DNS  Standard query response A 216.234.179.13
 9 0.011528  ns1.google.com  Local           DNS  Standard query response A 64.33.88.161
10 0.011538  ns1.google.com  Local           DNS  Standard query response A 64.33.88.161
11 0.011542  ns1.google.com  Local           DNS  Standard query response A 64.33.88.161
12 0.011913  Local           ns1.google.com  DNS  Standard query AAAA www.youtube.com
13 0.017074  ns1.google.com  Local           DNS  Standard query response A 64.33.88.161
14 0.017236  Local           ns1.google.com  DNS  Standard query MX www.youtube.com
15 0.018822  ns1.google.com  Local           DNS  Standard query response AAAA[Malformed Packet]
16 0.018843  ns1.google.com  Local           DNS  Standard query response AAAA[Malformed Packet]
17 0.018851  ns1.google.com  Local           DNS  Standard query response AAAA[Malformed Packet]
18 0.023061  ns1.google.com  Local           DNS  Standard query response A 4.36.66.178
19 0.023637  ns1.google.com  Local           DNS  Standard query response MX[Malformed Packet]
20 0.023657  ns1.google.com  Local           DNS  Standard query response MX[Malformed Packet]
21 0.023664  ns1.google.com  Local           DNS  Standard query response MX[Malformed Packet]
22 0.169599  ns1.google.com  Local           DNS  Standard query response CNAME youtube-ui.l.googl
23 0.177338  ns1.google.com  Local           DNS  Standard query response CNAME youtube-ui.l.googl
24 0.183692  ns1.google.com  Local           DNS  Standard query response CNAME youtube-ui.l.googl
```