TCP WireShark 抓包实验

09017423 杨彬

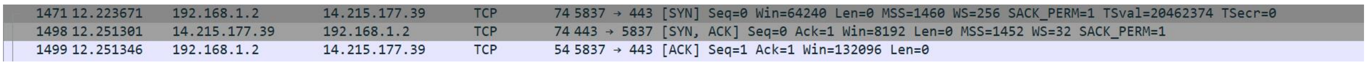
操作步骤

本次利用 wireshark进行抓包，我抓的是和 baidu.com进行通信的TCP数据报

1. 用 nslookup 查询 www.baidu.com 的 ip 为 14.215.177.39
2. 在 wireshark过滤器上添加 ip.dst == 14.215.177.39
3. 执行网络的打开关闭操作
4. 抓到包之后选择 TCP数据流
5. 对TCP数据流进行分析

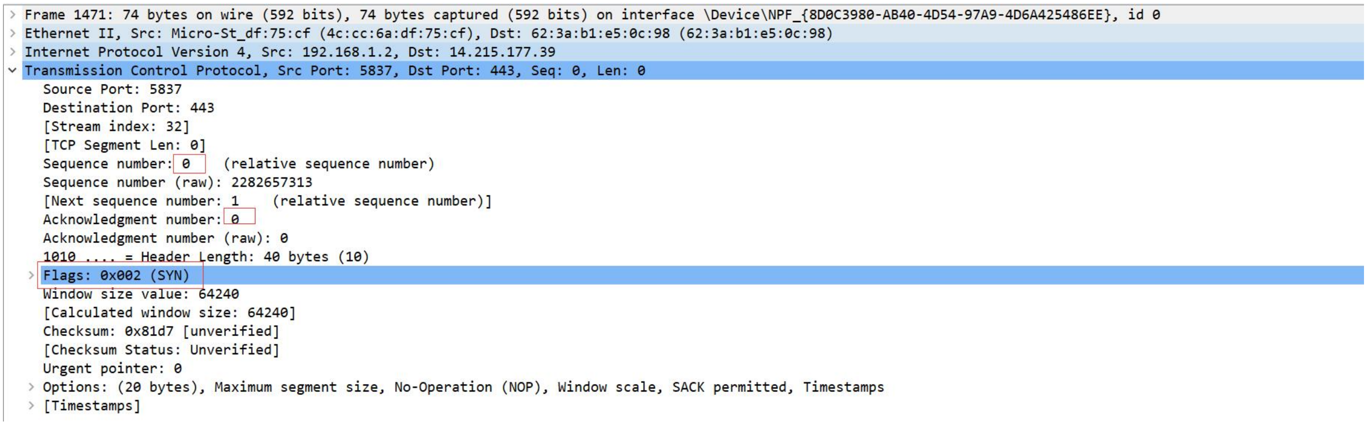
结果

TCP 三次握手



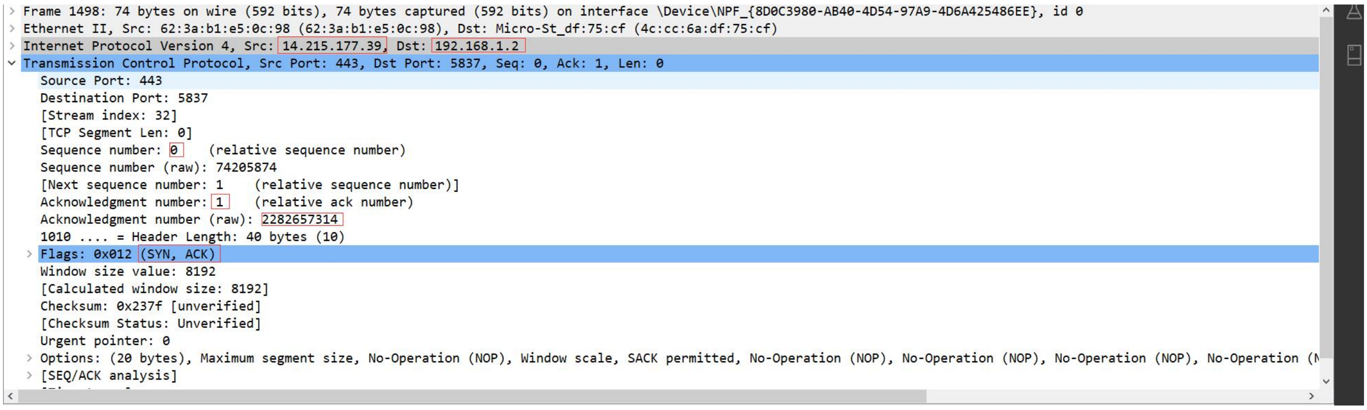
```
1471 12.223671   192.168.1.2     14.215.177.39   TCP   74 5837 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=20462374 TSecr=0
1498 12.251301   14.215.177.39   192.168.1.2     TCP   74 443 → 5837 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1452 WS=32 SACK_PERM=1
1499 12.251346   192.168.1.2     14.215.177.39   TCP   54 5837 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0
```

第一次握手



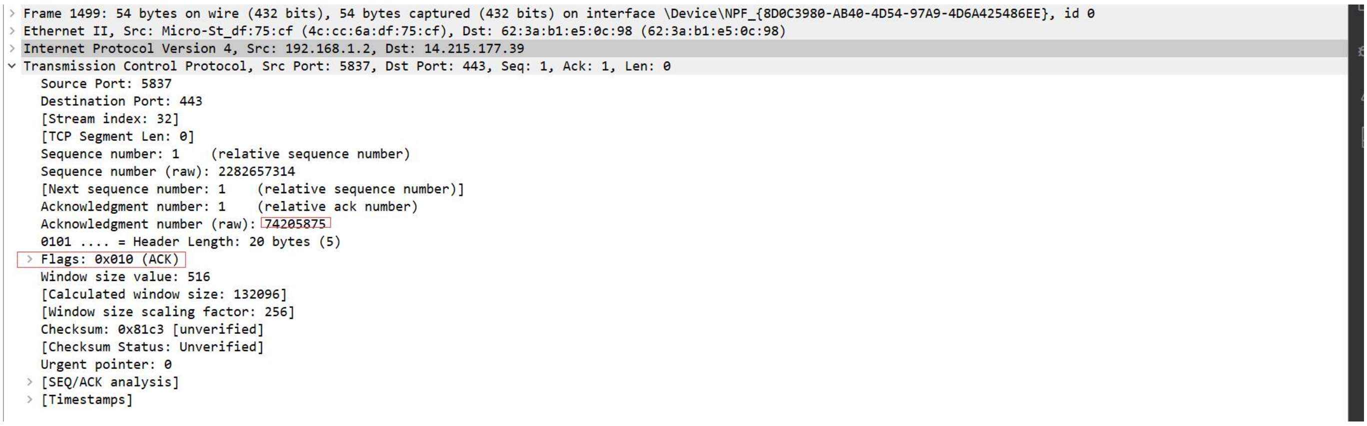
```
> Frame 1471: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{8D0C3980-AB40-4D54-97A9-4D6A425486EE}, id 0
> Ethernet II, Src: Micro-St_df:75:cf (4c:cc:6a:df:75:cf), Dst: 62:3a:b1:e5:0c:98 (62:3a:b1:e5:0c:98)
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 14.215.177.39
v Transmission Control Protocol, Src Port: 5837, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 5837
    Destination Port: 443
    [Stream index: 32]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 2282657313
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 0
    Acknowledgment number (raw): 0
    1010 .... = Header Length: 40 bytes (10)
  > Flags: 0x002 (SYN)
    Window size value: 64240
    [Calculated window size: 64240]
    Checksum: 0x81d7 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > Options: (20 bytes), Maximum segment size, No-Operation (NOP), Window scale, SACK permitted, Timestamps
  > [Timestamps]
```

第二次握手



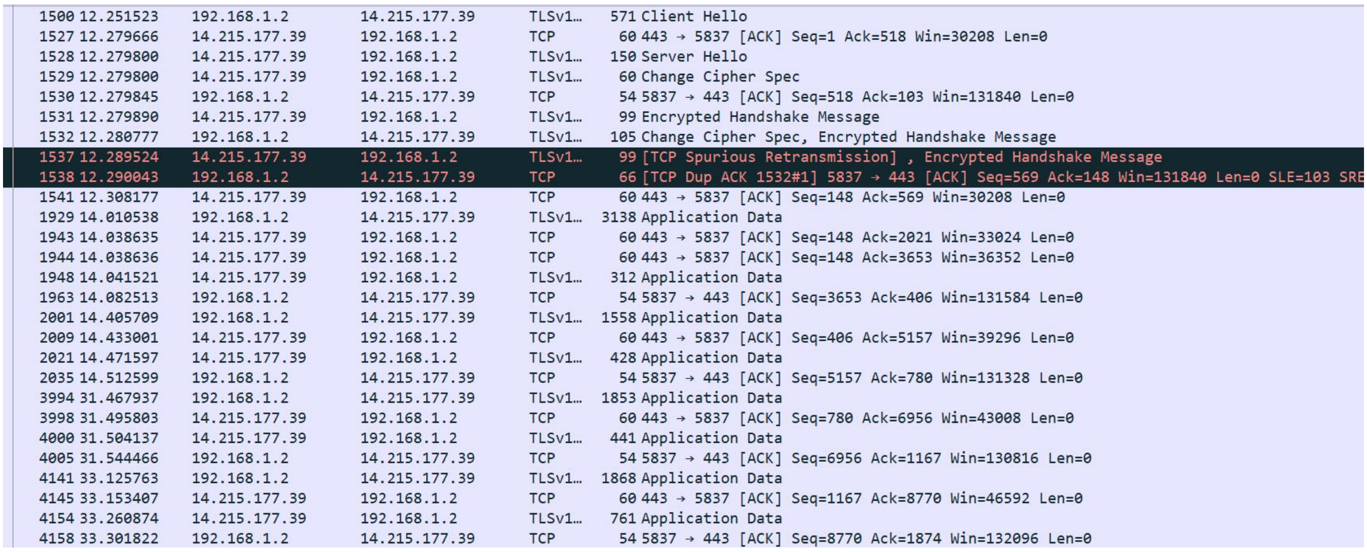
```
> Frame 1498: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{8D0C3980-AB40-4D54-97A9-4D6A425486EE}, id 0
> Ethernet II, Src: 62:3a:b1:e5:0c:98 (62:3a:b1:e5:0c:98), Dst: Micro-St_df:75:cf (4c:cc:6a:df:75:cf)
> Internet Protocol Version 4, Src: 14.215.177.39, Dst: 192.168.1.2
v Transmission Control Protocol, Src Port: 443, Dst Port: 5837, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 5837
    [Stream index: 32]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 74205874
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 2282657314
    1010 .... = Header Length: 40 bytes (10)
  > Flags: 0x012 (SYN, ACK)
    Window size value: 8192
    [Calculated window size: 8192]
    Checksum: 0x237f [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > Options: (20 bytes), Maximum segment size, No-Operation (NOP), Window scale, SACK permitted, No-Operation (NOP), No-Operation (NOP), No-Operation (NOP), No-Operation (N
  > [SEQ/ACK analysis]
```

第三次握手



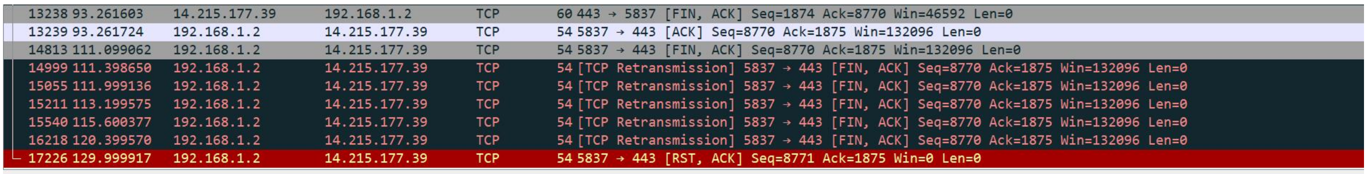
```
> Frame 1499: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{8D0C3980-AB40-4D54-97A9-4D6A425486EE}, id 0
> Ethernet II, Src: Micro-St_df:75:cf (4c:cc:6a:df:75:cf), Dst: 62:3a:b1:e5:0c:98 (62:3a:b1:e5:0c:98)
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 14.215.177.39
v Transmission Control Protocol, Src Port: 5837, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
    Source Port: 5837
    Destination Port: 443
    [Stream index: 32]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 2282657314
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 74205875
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window size value: 516
    [Calculated window size: 132096]
    [Window size scaling factor: 256]
    Checksum: 0x81c3 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
```

数据传输



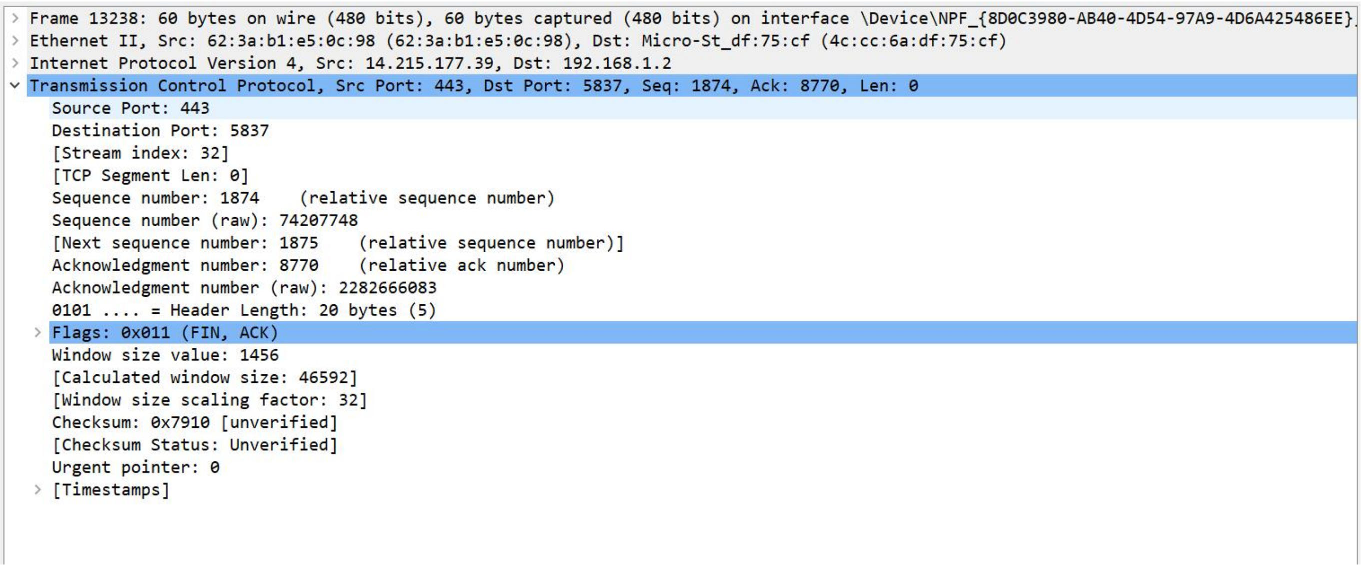
```
1500 12.251523   192.168.1.2     14.215.177.39   TLSv1…   571 Client Hello
1527 12.279666   14.215.177.39   192.168.1.2     TCP       60 443 → 5837 [ACK] Seq=1 Ack=518 Win=30208 Len=0
1528 12.279800   14.215.177.39   192.168.1.2     TLSv1…   150 Server Hello
1529 12.279800   14.215.177.39   192.168.1.2     TLSv1…    60 Change Cipher Spec
1530 12.279845   192.168.1.2     14.215.177.39   TCP       54 5837 → 443 [ACK] Seq=518 Ack=103 Win=131840 Len=0
1531 12.279890   14.215.177.39   192.168.1.2     TLSv1…    99 Encrypted Handshake Message
1532 12.280777   192.168.1.2     14.215.177.39   TLSv1…   105 Change Cipher Spec, Encrypted Handshake Message
1537 12.289524   14.215.177.39   192.168.1.2     TLSv1…    99 [TCP Spurious Retransmission] , Encrypted Handshake Message
1538 12.290043   192.168.1.2     14.215.177.39   TCP       66 [TCP Dup ACK 1532#1] 5837 → 443 [ACK] Seq=569 Ack=148 Win=131840 Len=0 SLE=103 SRE
1541 12.308177   14.215.177.39   192.168.1.2     TCP       60 443 → 5837 [ACK] Seq=148 Ack=569 Win=30208 Len=0
1929 14.010538   192.168.1.2     14.215.177.39   TLSv1…  3138 Application Data
1943 14.038635   14.215.177.39   192.168.1.2     TCP       60 443 → 5837 [ACK] Seq=148 Ack=2021 Win=33024 Len=0
1944 14.038636   14.215.177.39   192.168.1.2     TCP       60 443 → 5837 [ACK] Seq=148 Ack=3653 Win=36352 Len=0
1948 14.041521   14.215.177.39   192.168.1.2     TLSv1…   312 Application Data
1963 14.082513   192.168.1.2     14.215.177.39   TCP       54 5837 → 443 [ACK] Seq=3653 Ack=406 Win=131584 Len=0
2001 14.405709   192.168.1.2     14.215.177.39   TLSv1…  1558 Application Data
2009 14.433001   14.215.177.39   192.168.1.2     TCP       60 443 → 5837 [ACK] Seq=406 Ack=5157 Win=39296 Len=0
2021 14.471597   14.215.177.39   192.168.1.2     TLSv1…   428 Application Data
2035 14.512599   192.168.1.2     14.215.177.39   TCP       54 5837 → 443 [ACK] Seq=5157 Ack=780 Win=131328 Len=0
3994 31.467937   192.168.1.2     14.215.177.39   TLSv1…  1853 Application Data
3998 31.495803   14.215.177.39   192.168.1.2     TCP       60 443 → 5837 [ACK] Seq=780 Ack=6956 Win=43008 Len=0
4000 31.504137   14.215.177.39   192.168.1.2     TLSv1…   441 Application Data
4005 31.544466   192.168.1.2     14.215.177.39   TCP       54 5837 → 443 [ACK] Seq=6956 Ack=1167 Win=130816 Len=0
4141 33.125763   192.168.1.2     14.215.177.39   TLSv1…  1868 Application Data
4145 33.153407   14.215.177.39   192.168.1.2     TCP       60 443 → 5837 [ACK] Seq=1167 Ack=8770 Win=46592 Len=0
4154 33.260874   14.215.177.39   192.168.1.2     TLSv1…   761 Application Data
4158 33.301822   192.168.1.2     14.215.177.39   TCP       54 5837 → 443 [ACK] Seq=8770 Ack=1874 Win=132096 Len=0
```

TCP挥手



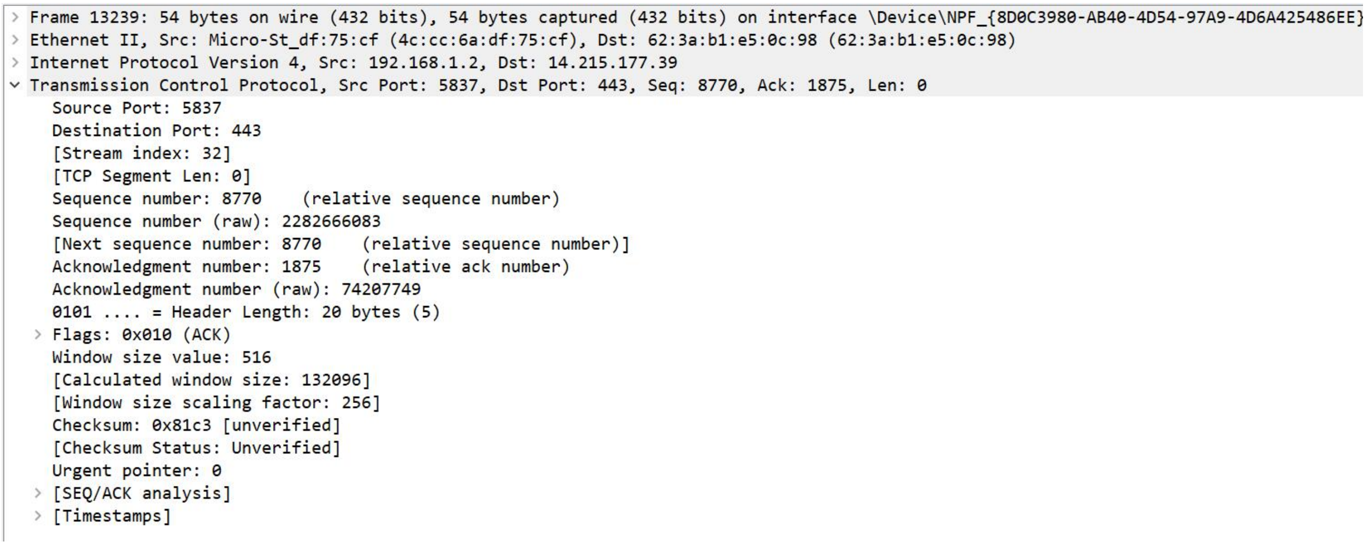
```
13238 93.261603    14.215.177.39   192.168.1.2     TCP    60 443 → 5837 [FIN, ACK] Seq=1874 Ack=8770 Win=46592 Len=0
13239 93.261724    192.168.1.2     14.215.177.39   TCP    54 5837 → 443 [ACK] Seq=8770 Ack=1875 Win=132096 Len=0
14813 111.099062   192.168.1.2     14.215.177.39   TCP    54 5837 → 443 [FIN, ACK] Seq=8770 Ack=1875 Win=132096 Len=0
14999 111.398650   192.168.1.2     14.215.177.39   TCP    54 [TCP Retransmission] 5837 → 443 [FIN, ACK] Seq=8770 Ack=1875 Win=132096 Len=0
15055 111.999136   192.168.1.2     14.215.177.39   TCP    54 [TCP Retransmission] 5837 → 443 [FIN, ACK] Seq=8770 Ack=1875 Win=132096 Len=0
15211 113.199575   192.168.1.2     14.215.177.39   TCP    54 [TCP Retransmission] 5837 → 443 [FIN, ACK] Seq=8770 Ack=1875 Win=132096 Len=0
15540 115.600377   192.168.1.2     14.215.177.39   TCP    54 [TCP Retransmission] 5837 → 443 [FIN, ACK] Seq=8770 Ack=1875 Win=132096 Len=0
16218 120.399570   192.168.1.2     14.215.177.39   TCP    54 [TCP Retransmission] 5837 → 443 [FIN, ACK] Seq=8770 Ack=1875 Win=132096 Len=0
17226 129.999917   192.168.1.2     14.215.177.39   TCP    54 5837 → 443 [RST, ACK] Seq=8771 Ack=1875 Win=0 Len=0
```

第一次挥手



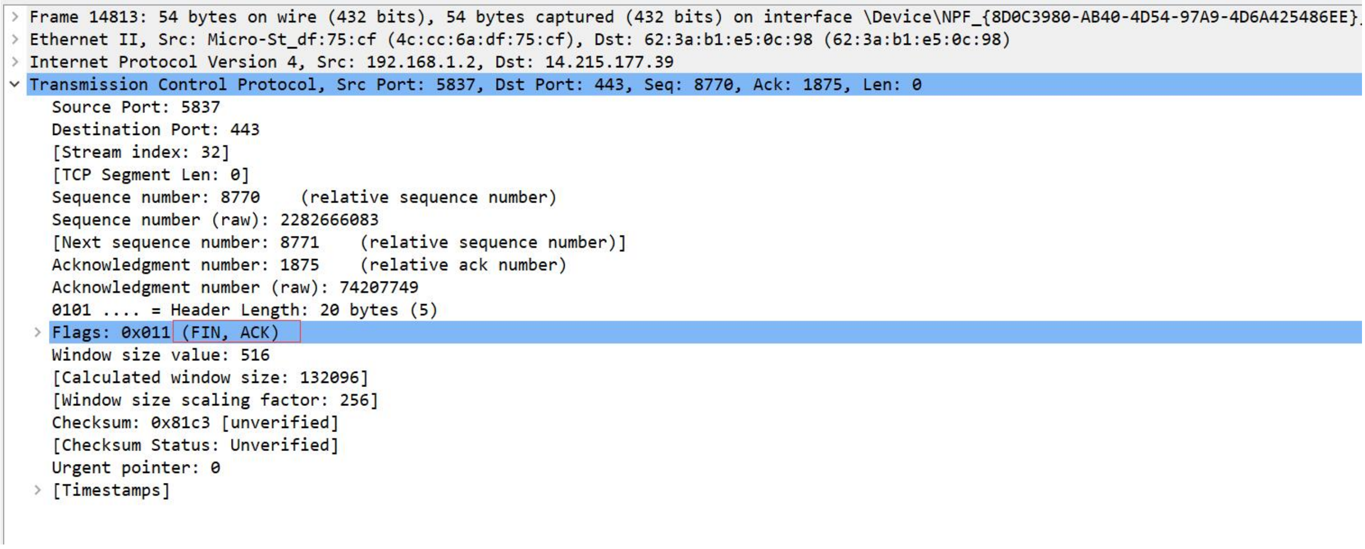
```
Frame 13238: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{8D0C3980-AB40-4D54-97A9-4D6A425486EE}
Ethernet II, Src: 62:3a:b1:e5:0c:98 (62:3a:b1:e5:0c:98), Dst: Micro-St_df:75:cf (4c:cc:6a:df:75:cf)
Internet Protocol Version 4, Src: 14.215.177.39, Dst: 192.168.1.2
Transmission Control Protocol, Src Port: 443, Dst Port: 5837, Seq: 1874, Ack: 8770, Len: 0
  Source Port: 443
  Destination Port: 5837
  [Stream index: 32]
  [TCP Segment Len: 0]
  Sequence number: 1874    (relative sequence number)
  Sequence number (raw): 74207748
  [Next sequence number: 1875    (relative sequence number)]
  Acknowledgment number: 8770    (relative ack number)
  Acknowledgment number (raw): 2282666083
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x011 (FIN, ACK)
  Window size value: 1456
  [Calculated window size: 46592]
  [Window size scaling factor: 32]
  Checksum: 0x7910 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  [Timestamps]
```

第二次挥手



```
Frame 13239: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{8D0C3980-AB40-4D54-97A9-4D6A425486EE}
Ethernet II, Src: Micro-St_df:75:cf (4c:cc:6a:df:75:cf), Dst: 62:3a:b1:e5:0c:98 (62:3a:b1:e5:0c:98)
Internet Protocol Version 4, Src: 192.168.1.2, Dst: 14.215.177.39
Transmission Control Protocol, Src Port: 5837, Dst Port: 443, Seq: 8770, Ack: 1875, Len: 0
  Source Port: 5837
  Destination Port: 443
  [Stream index: 32]
  [TCP Segment Len: 0]
  Sequence number: 8770    (relative sequence number)
  Sequence number (raw): 2282666083
  [Next sequence number: 8770    (relative sequence number)]
  Acknowledgment number: 1875    (relative ack number)
  Acknowledgment number (raw): 74207749
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x010 (ACK)
  Window size value: 516
  [Calculated window size: 132096]
  [Window size scaling factor: 256]
  Checksum: 0x81c3 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  [SEQ/ACK analysis]
  [Timestamps]
```

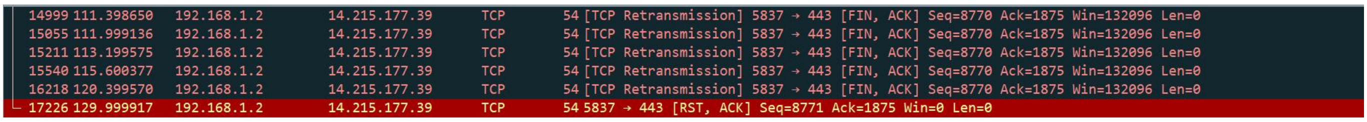
第三次挥手



```
Frame 14813: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{8D0C3980-AB40-4D54-97A9-4D6A425486EE}
Ethernet II, Src: Micro-St_df:75:cf (4c:cc:6a:df:75:cf), Dst: 62:3a:b1:e5:0c:98 (62:3a:b1:e5:0c:98)
Internet Protocol Version 4, Src: 192.168.1.2, Dst: 14.215.177.39
Transmission Control Protocol, Src Port: 5837, Dst Port: 443, Seq: 8770, Ack: 1875, Len: 0
  Source Port: 5837
  Destination Port: 443
  [Stream index: 32]
  [TCP Segment Len: 0]
  Sequence number: 8770    (relative sequence number)
  Sequence number (raw): 2282666083
  [Next sequence number: 8771    (relative sequence number)]
  Acknowledgment number: 1875    (relative ack number)
  Acknowledgment number (raw): 74207749
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x011 (FIN, ACK)
  Window size value: 516
  [Calculated window size: 132096]
  [Window size scaling factor: 256]
  Checksum: 0x81c3 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  [Timestamps]
```

第四次挥手

第四次挥手没有收到 ACK包，(挥手由百度服务器发器)，所以后面不断重传，最后自动关闭了。



```
14999 111.398650   192.168.1.2      14.215.177.39    TCP       54 [TCP Retransmission] 5837 → 443 [FIN, ACK] Seq=8770 Ack=1875 Win=132096 Len=0
15055 111.999136   192.168.1.2      14.215.177.39    TCP       54 [TCP Retransmission] 5837 → 443 [FIN, ACK] Seq=8770 Ack=1875 Win=132096 Len=0
15211 113.199575   192.168.1.2      14.215.177.39    TCP       54 [TCP Retransmission] 5837 → 443 [FIN, ACK] Seq=8770 Ack=1875 Win=132096 Len=0
15540 115.600377   192.168.1.2      14.215.177.39    TCP       54 [TCP Retransmission] 5837 → 443 [FIN, ACK] Seq=8770 Ack=1875 Win=132096 Len=0
16218 120.399570   192.168.1.2      14.215.177.39    TCP       54 [TCP Retransmission] 5837 → 443 [FIN, ACK] Seq=8770 Ack=1875 Win=132096 Len=0
17226 129.999917   192.168.1.2      14.215.177.39    TCP       54 5837 → 443 [RST, ACK] Seq=8771 Ack=1875 Win=0 Len=0
```

分析

握手分析

从上图抓包的结果我们看到，完整经历了3个挥手过程

seq是相对的序号

1. 本地->百度服务器。 seq =0 , flag=[SYN]
2. 百度服务器->本地。 seq =0, **ack=1** flag=[SYN,ACK]
3. 本地->百度服务器。 seq =1, **ack=1** flag=[ACK]

和我们所学习的 TCP握手过程相同，同时在详细信息内我们可以看到源端口，目的端口，raw sequence 等信息。

挥手分析

本次抓包，挥手由服务器发器

1. baidi->本地 flags=[FIN,ACK], seq = 1874 Ack=8770 (这一个 ack应该是对上一个数据报的回复)
2. 本地->baidu flags=[ACK], seq=8770, ack=1875 （1875=1874+1） 告知 服务器，客户端知道连接要关闭了
3. 本地->baidu flags=[FIN,ACK], seq=8770, Ack=1875. 告知服务器客户端也准备关闭连接
4. 服务器没有 ACK响应。(或许是服务器傲娇吧)

再经过数次重传之后，定时器时间到了，自动关闭连接。