

Wireshark 抓包分析

骆继祥

UDP 抓包分析：

实验：

```
▼ Frame 515: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on interface \Device\NPF_{18A477C5-5DE8-4478-9608-B22608F0B26F}, id 0
  > Interface id: 0 (\Device\NPF_{18A477C5-5DE8-4478-9608-B22608F0B26F})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 25, 2020 17:38:30.381736000 中国标准时间
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1603618710.381736000 seconds
    [Time delta from previous captured frame: 0.000094000 seconds]
    [Time delta from previous displayed frame: 0.000094000 seconds]
    [Time since reference or first frame: 15.608380000 seconds]
    Frame Number: 515
    Frame Length: 305 bytes (2440 bits)
    Capture Length: 305 bytes (2440 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:data]

0000  ff ff ff ff ff ff 38 ba f8 e7 d3 30 08 00 45 00  ....8. ...0..E-
0010  01 23 81 f2 00 00 80 11 33 16 c0 a8 01 72 c0 a8  .#..... 3....r..
0020  01 ff d6 83 d6 83 01 0f 9c cb 00 4c 41 50 54 4f  .....LAPTO
0030  50 2d 44 4a 36 38 33 41 54 42 00 b6 1f 8a 9e 00  P-DJ683A TB.....
0040  00 00 80 b6 1f 8a 9e 00 00 00 64 b6 1f 8a 9e 00  .....d.....
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0060  00 00 f0 9d d4 ca 7e 02 00 00 e0 b5 1f 8a 9e 00  .....
0070  00 00 00 00 c2 c6 05 00 00 00 33 27 00 00 00 00  .....3'....
0080  00 00 e0 9d d4 ca 7e 02 00 00 30 ea c3 c6 7e 02  .....~...0....~
0090  00 00 01 00 00 00 00 00 00 00 01 00 00 00 00  .....
00a0  00 00 d6 86 86 e1 fc 7f 00 00 07 a7 03 7b 39 36  .....{96
00b0  62 66 64 33 37 35 2d 37 66 32 32 2d 34 63 31 37  bfd375-7 f22-4c17
00c0  2d 61 62 39 39 2d 37 65 61 31 33 36 35 30 66 31  -ab99-7e a13650f1
00d0  39 34 7d 00 1f 8a 9e 00 00 00 64 b6 1f 8a 9e 00  94}.....d.....
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00f0  00 00 00 00 c2 c6 7e 02 00 00 c0 b7 1f 8a 1c 00  .....~.....
0100  00 00 00 00 00 00 00 00 00 00 01 00 00 00 00  .....
0110  00 00 60 b6 1f 8a 9e 00 00 00 00 00 00 00 00 00  ..~.....
```

图一：总体图（数据帧结构的基本信息，帧数，帧长，时间等）

```
Frame Number: 515
Frame Length: 305 bytes (2440 bits)
Capture Length: 305 bytes (2440 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:data]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
▼ Ethernet II, Src: IntelCor_e7:d3:30 (38:ba:f8:e7:d3:30), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: IntelCor_e7:d3:30 (38:ba:f8:e7:d3:30)
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 192.168.1.114, Dst: 192.168.1.255
  > User Datagram Protocol, Src Port: 54915, Dst Port: 54915
  > Data (263 bytes)

0000  ff ff ff ff ff ff 38 ba f8 e7 d3 30 08 00 45 00  ....8. ...0..E-
0010  01 23 81 f2 00 00 80 11 33 16 c0 a8 01 72 c0 a8  .#..... 3....r..
0020  01 ff d6 83 d6 83 01 0f 9c cb 00 4c 41 50 54 4f  .....LAPTO
0030  50 2d 44 4a 36 38 33 41 54 42 00 b6 1f 8a 9e 00  P-DJ683A TB.....
0040  00 00 80 b6 1f 8a 9e 00 00 00 64 b6 1f 8a 9e 00  .....d.....
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0060  00 00 f0 9d d4 ca 7e 02 00 00 e0 b5 1f 8a 9e 00  .....
0070  00 00 00 00 c2 c6 05 00 00 00 33 27 00 00 00 00  .....3'....
0080  00 00 e0 9d d4 ca 7e 02 00 00 30 ea c3 c6 7e 02  .....~...0....~
0090  00 00 01 00 00 00 00 00 00 00 01 00 00 00 00  .....
00a0  00 00 d6 86 86 e1 fc 7f 00 00 07 a7 03 7b 39 36  .....{96
00b0  62 66 64 33 37 35 2d 37 66 32 32 2d 34 63 31 37  bfd375-7 f22-4c17
00c0  2d 61 62 39 39 2d 37 65 61 31 33 36 35 30 66 31  -ab99-7e a13650f1
00d0  39 34 7d 00 1f 8a 9e 00 00 00 64 b6 1f 8a 9e 00  94}.....d.....
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00f0  00 00 00 00 c2 c6 7e 02 00 00 c0 b7 1f 8a 1c 00  .....~.....
0100  00 00 00 00 00 00 00 00 00 00 01 00 00 00 00  .....
0110  00 00 60 b6 1f 8a 9e 00 00 00 00 00 00 00 00 00  ..~.....
```

图二：以太网协议字段（Destination 和 Source，以及网络类型）

| | |
|---|-------------------|
| Internet Protocol Version 4, Src: 192.168.1.114, Dst: 192.168.1.255 | |
| 0100 = Version: 4 | |
| 0101 = Header Length: 20 bytes (5) | |
| > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) | |
| Total Length: 291 | |
| Identification: 0x81f2 (33266) | |
| > Flags: 0x0000 | |
| Fragment offset: 0 | |
| Time to live: 128 | |
| Protocol: UDP (17) | |
| Header checksum: 0x3316 [validation disabled] | |
| [Header checksum status: Unverified] | |
| Source: 192.168.1.114 | |
| Destination: 192.168.1.255 | |
| > User Datagram Protocol, Src Port: 54915, Dst Port: 54915 | |
| 0000 ff ff ff ff ff ff 38 ba f8 e7 d3 30 08 00 45 00 |8....0...E.. |
| 0010 01 23 81 f2 00 00 80 11 33 16 c0 a8 01 72 c0 a8 | .#.....3.....r.. |
| 0020 01 ff d6 83 d6 83 01 0f 9c cb 00 4c 41 50 54 4f | ..LAPTO |
| 0030 50 2d 44 4a 36 38 33 41 54 42 00 b6 1f 8a 9e 00 | P-DJ683A TB..... |
| 0040 00 00 80 b6 1f 8a 9e 00 00 00 64 b6 1f 8a 9e 00 |d..... |
| 0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | |
| 0060 00 00 f0 9d d4 ca 7e 02 00 00 e0 b5 1f 8a 9e 00 |~..... |
| 0070 00 00 00 00 c2 c6 05 00 00 00 33 27 00 00 00 00 |3'..... |
| 0080 00 00 e0 9d d4 ca 7e 02 00 00 30 ea c3 c6 7e 02 |~..0..... |
| 0090 00 00 01 00 00 00 00 00 00 00 01 00 00 00 00 00 | |
| 00a0 00 00 d6 86 86 e1 fc 7f 00 00 07 a7 03 7b 39 36 |{96 |
| 00b0 62 66 64 33 37 35 2d 37 66 32 32 2d 34 63 31 37 | bfd375-7 f22-4c17 |
| 00c0 2d 61 62 39 39 2d 37 65 61 31 33 36 35 30 66 31 | -ab99-7e a13650f1 |
| 00d0 39 34 7d 00 1f 8a 9e 00 00 00 64 b6 1f 8a 9e 00 | 94}.....d..... |
| 00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | |
| 00f0 00 00 00 00 c2 c6 7e 02 00 00 c0 b7 1f 8a 1c 00 |~..... |
| 0100 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 | |
| 0110 00 00 60 b6 1f 8a 9e 00 00 00 00 00 00 00 00 00 | ..`..... |

图三：网络协议层字段（版本，头长度，DSCP（长度和身份），符号位，偏移为 0 不占位，时间 128，协议，头部检验未开启，最后依次是源地址和目的地址）

| |
|---|
| > Frame 515: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on |
| > Ethernet II, Src: IntelCor_e7:d3:30 (38:ba:f8:e7:d3:30), Dst: Broadcast (f |
| > Internet Protocol Version 4, Src: 192.168.1.114, Dst: 192.168.1.255 |
| > User Datagram Protocol, Src Port: 54915, Dst Port: 54915 |
| Source Port: 54915 |
| Destination Port: 54915 |
| Length: 271 |
| Checksum: 0x9ccb [unverified] |
| [Checksum Status: Unverified] |
| [Stream index: 3] |
| > [Timestamps] |
| > Data (263 bytes) |

| | |
|--|-------------------|
| 0020 01 ff d6 83 d6 83 01 0f 9c cb 00 4c 41 50 54 4f | ..LAPTO |
| 0030 50 2d 44 4a 36 38 33 41 54 42 00 b6 1f 8a 9e 00 | P-DJ683A TB..... |
| 0040 00 00 80 b6 1f 8a 9e 00 00 00 64 b6 1f 8a 9e 00 |d..... |
| 0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | |
| 0060 00 00 f0 9d d4 ca 7e 02 00 00 e0 b5 1f 8a 9e 00 |~..... |
| 0070 00 00 00 00 c2 c6 05 00 00 00 33 27 00 00 00 00 |3'..... |
| 0080 00 00 e0 9d d4 ca 7e 02 00 00 30 ea c3 c6 7e 02 |~..0..... |
| 0090 00 00 01 00 00 00 00 00 00 00 01 00 00 00 00 00 | |
| 00a0 00 00 d6 86 86 e1 fc 7f 00 00 07 a7 03 7b 39 36 |{96 |
| 00b0 62 66 64 33 37 35 2d 37 66 32 32 2d 34 63 31 37 | bfd375-7 f22-4c17 |
| 00c0 2d 61 62 39 39 2d 37 65 61 31 33 36 35 30 66 31 | -ab99-7e a13650f1 |
| 00d0 39 34 7d 00 1f 8a 9e 00 00 00 64 b6 1f 8a 9e 00 | 94}.....d..... |
| 00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | |
| 00f0 00 00 00 00 c2 c6 7e 02 00 00 c0 b7 1f 8a 1c 00 |~..... |
| 0100 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 | |
| 0110 00 00 60 b6 1f 8a 9e 00 00 00 00 00 00 00 00 00 | ..`..... |
| 0120 00 00 7a 99 bb d1 fc 7f 00 00 00 00 00 60 7f d1 | ..z..... |
| 0130 07 | . |

图四：UDP 层数据协议（源端口，目的端口，长度，校验位未开启，数据流索引为 3，时间戳）

▸ Data (263 bytes)

| | | |
|------|---|-------------------|
| 0020 | 01 ff d6 83 d6 83 01 0f 9c cb 00 4c 41 50 54 4f |-LAPTO |
| 0030 | 50 2d 44 4a 36 38 33 41 54 42 00 b6 1f 8a 9e 00 | P-DJ683A TB..... |
| 0040 | 00 00 80 b6 1f 8a 9e 00 00 00 64 b6 1f 8a 9e 00 |-d..... |
| 0050 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | |
| 0060 | 00 00 f0 9d d4 ca 7e 02 00 00 e0 b5 1f 8a 9e 00 |~..... |
| 0070 | 00 00 00 00 c2 c6 05 00 00 00 33 27 00 00 00 00 |-3'.... |
| 0080 | 00 00 e0 9d d4 ca 7e 02 00 00 30 ea c3 c6 7e 02 |~..0..... |
| 0090 | 00 00 01 00 00 00 00 00 00 00 01 00 00 00 00 | |
| 00a0 | 00 00 d6 86 86 e1 fc 7f 00 00 07 a7 03 7b 39 36 |{96 |
| 00b0 | 62 66 64 33 37 35 2d 37 66 32 32 2d 34 63 31 37 | bfd375-7 f22-4c17 |
| 00c0 | 2d 61 62 39 39 2d 37 65 61 31 33 36 35 30 66 31 | -ab99-7e a13650f1 |
| 00d0 | 39 34 7d 00 1f 8a 9e 00 00 00 64 b6 1f 8a 9e 00 | 94}.....-d..... |
| 00e0 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | |
| 00f0 | 00 00 00 00 c2 c6 7e 02 00 00 c0 b7 1f 8a 1c 00 |~..... |
| 0100 | 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 | |
| 0110 | 00 00 60 b6 1f 8a 9e 00 00 00 00 00 00 00 00 | ..~..... |
| 0120 | 00 00 7a 99 bb d1 fc 7f 00 00 00 00 00 60 7f d1 | ..z.....~.. |
| 0130 | 07 | . |

图五：UDP 数据

TCP 抓包分析：

实验：

| | | |
|--|---|---------------------|
| ▼ Frame 293: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{18A477C5-5DE8-4478-9608-B22608F0B26F}, id 0 | | |
| > Interface id: 0 (\Device\NPF_{18A477C5-5DE8-4478-9608-B22608F0B26F}) | | |
| Encapsulation type: Ethernet (1) | | |
| Arrival Time: Oct 25, 2020 17:38:30.163867000 中国标准时间 | | |
| [Time shift for this packet: 0.000000000 seconds] | | |
| Epoch Time: 1603618710.163867000 seconds | | |
| [Time delta from previous captured frame: 0.000093000 seconds] | | |
| [Time delta from previous displayed frame: 0.000093000 seconds] | | |
| [Time since reference or first frame: 15.390511000 seconds] | | |
| Frame Number: 293 | | |
| Frame Length: 1514 bytes (12112 bits) | | |
| Capture Length: 1514 bytes (12112 bits) | | |
| [Frame is marked: False] | | |
| [Frame is ignored: False] | | |
| [Protocols in frame: eth:ethertype:ip:tcp] | | |
| [Coloring Rule Name: TCP] | | |
| [Coloring Rule String: tcp] | | |
| 0000 | 54 bf 64 83 7d c6 74 05 a5 8b 79 59 08 00 45 14 | T-d.)-t-..yY..E.. |
| 0010 | 05 dc ae 2f 40 00 2d 06 4e 44 65 c8 23 af c0 a8 | .../@... NDe.#... |
| 0020 | 01 75 01 bb c6 2e c2 f8 a3 0c 5b 7c 77 0d 50 10 | -u..... [[wP.. |
| 0030 | 01 5f 24 76 00 00 e0 49 e9 9a ea e3 41 10 59 13 | - \$v...I ...A-V.. |
| 0040 | 7d 7a 5b 9f 93 5f a7 e3 52 6c ef 0e 56 d8 8c f0 |]Z[...- R1..V...- |
| 0050 | d2 fa ed 0f 1a 6f a6 44 c7 27 18 18 02 a4 e2 76 |QD ..-.....v |
| 0060 | cc 1e 3c 52 1c 13 fd 95 1f 3f c4 59 6b 56 68 a8 | -<<R...-?YkVh... |
| 0070 | e9 32 84 6e 80 b5 48 c5 ef c5 1e 89 59 7c 36 22 | -2.n...H...-Y[6" |
| 0080 | 56 bc 69 ea dc b1 d7 3a be 3c d9 25 a2 3d 8b 75 | V-i-...: <%->u |
| 0090 | 01 da de ed ff 6f 80 03 d4 ab f9 8e 94 be 7b 43 |o-{C |
| 00a0 | 23 78 e5 dc 2f 22 9c 2e 4c f4 a3 ba 48 66 a3 df | #x.../".. L...Hf... |
| 00b0 | 05 3f 90 45 70 32 9e 00 bf 20 39 0e 9a 43 07 45 | -?..Ep2...- 9...C-E |
| 00c0 | 88 47 b3 e6 14 55 40 fb 9b fa 0d 9d ea 99 30 0e | -G...U0...-.....0- |
| 00d0 | 45 01 2d 16 98 eb 59 5a 7c 78 23 98 df 89 0c 67 | E-....YZ x#....g |
| 00e0 | cb 0d 58 24 a4 40 d2 6f ff 96 df 5c ff b0 a2 29 | ..X\$.@-o ...\\...) |
| 00f0 | 3e 5c 1a 6b 37 3f 41 8b db 4d 66 61 0b e7 88 83 | >.\-k7?A...Mfa.... |
| 0100 | bc 4d e6 54 b6 62 9b 4b af b1 96 90 5f 7e 4a fa | -M-T.b-K~J.. |
| 0110 | d7 8e 56 2e fe 3a 60 95 4c 51 a4 7e 42 a4 c7 9c | ..V..:.. LQ...B... |
| 0120 | e5 cd f9 de 62 3b 42 a1 65 12 a7 e2 10 58 17 92 |b;B...e...-X... |
| 0130 | ac 82 57 2f b9 9b 51 08 0d db 4c ea 64 00 08 01 | ..W/-Q...-L-d... |
| 0140 | 5c 25 b5 95 e4 2f b9 25 e6 31 fa a9 6c 37 df 88 | \X.../-X -L-17... |

图六：总体图（数据帧结构的基本信息，帧数，帧长，时间等）

| | | | | | |
|-------|-------------|---------------|---------------|---------|---|
| 25013 | 1373.433640 | 192.168.1.117 | 182.61.200.6 | TCP | 66 51056 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 25014 | 1373.461979 | 182.61.200.6 | 192.168.1.117 | TCP | 66 443 → 51056 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1452 WS=32 SACK_PERM=1 |
| 25015 | 1373.461979 | 182.61.200.6 | 192.168.1.117 | TCP | 60 443 → 51056 [ACK] Seq=1032 Ack=5202 Win=39680 Len=0 |
| 25016 | 1373.462131 | 192.168.1.117 | 182.61.200.6 | TCP | 54 51056 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0 |
| 25017 | 1373.462684 | 192.168.1.117 | 182.61.200.6 | TLSv1.2 | 571 Client Hello |
| 25018 | 1373.489377 | 182.61.200.6 | 192.168.1.117 | TLSv1.2 | 933 Application Data |
| 25019 | 1373.491402 | 182.61.200.6 | 192.168.1.117 | TCP | 60 443 → 51056 [ACK] Seq=1 Ack=518 Win=30336 Len=0 |
| 25020 | 1373.491488 | 182.61.200.6 | 192.168.1.117 | TLSv1.2 | 150 Server Hello |
| 25021 | 1373.491488 | 182.61.200.6 | 192.168.1.117 | TLSv1.2 | 60 Change Cipher Spec |
| 25022 | 1373.491545 | 192.168.1.117 | 182.61.200.6 | TCP | 54 51056 → 443 [ACK] Seq=518 Ack=103 Win=131840 Len=0 |
| 25023 | 1373.491579 | 182.61.200.6 | 192.168.1.117 | TLSv1.2 | 99 Encrypted Handshake Message |

Sequence number (raw): 2722702923
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 0
Acknowledgment number (raw): 0
1000 = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
Window size value: 64240
[Calculated window size: 64240]
Checksum: 0x4088 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
Timestamps
[Time since first frame in this TCP stream: 0.000000000 seconds]
[Time since previous frame in this TCP stream: 0.000000000 seconds]

000 74 05 a5 8b 79 59 54 bf 64 83 7d c6 08 00 45 00 t...yT. d...E-
010 00 28 c1 09 40 00 24 06 55 65 b6 3d c8 06 c0 a8 -(.@.\$: Ue=....
020 c8 06 c7 70 01 bb a2 49 26 4b 00 00 00 00 00 02 ...p...I &K-----
030 fa f0 40 88 00 00 02 04 05 b4 01 03 03 08 01 01 ..@.....
040 04 02 ..

图七：TCP 三次握手-SYN

| | | | | | |
|-------|-------------|---------------|---------------|---------|---|
| 25014 | 1373.461979 | 182.61.200.6 | 192.168.1.117 | TCP | 66 443 → 51056 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1452 WS=32 SACK_PERM=1 |
| 25015 | 1373.461979 | 182.61.200.6 | 192.168.1.117 | TCP | 60 443 → 51056 [ACK] Seq=1032 Ack=5202 Win=39680 Len=0 |
| 25016 | 1373.462131 | 192.168.1.117 | 182.61.200.6 | TCP | 54 51056 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0 |
| 25017 | 1373.462684 | 192.168.1.117 | 182.61.200.6 | TLSv1.2 | 571 Client Hello |
| 25018 | 1373.489377 | 182.61.200.6 | 192.168.1.117 | TLSv1.2 | 933 Application Data |
| 25019 | 1373.491402 | 182.61.200.6 | 192.168.1.117 | TCP | 60 443 → 51056 [ACK] Seq=1 Ack=518 Win=30336 Len=0 |
| 25020 | 1373.491488 | 182.61.200.6 | 192.168.1.117 | TLSv1.2 | 150 Server Hello |
| 25021 | 1373.491488 | 182.61.200.6 | 192.168.1.117 | TLSv1.2 | 60 Change Cipher Spec |
| 25022 | 1373.491545 | 192.168.1.117 | 182.61.200.6 | TCP | 54 51056 → 443 [ACK] Seq=518 Ack=103 Win=131840 Len=0 |
| 25023 | 1373.491579 | 182.61.200.6 | 192.168.1.117 | TLSv1.2 | 99 Encrypted Handshake Message |

1000 = Header Length: 32 bytes (8)
Flags: 0x012 (SYN, ACK)
Window size value: 8192
[Calculated window size: 8192]
Checksum: 0xcdeb [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
SEQ/ACK analysis
[This is an ACK to the segment in frame: 25013]
[The RTT to ACK the segment was: 0.028339000 seconds]
[IRTT: 0.028491000 seconds]
Timestamps
[Time since first frame in this TCP stream: 0.028339000 seconds]
[Time since previous frame in this TCP stream: 0.028339000 seconds]

图八：TCP 三次握手-[SYN,ACK]

| | | | | | |
|-------|-------------|---------------|---------------|---------|---|
| 25013 | 1373.433640 | 192.168.1.117 | 182.61.200.6 | TCP | 66 51056 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 25014 | 1373.461979 | 182.61.200.6 | 192.168.1.117 | TCP | 66 443 → 51056 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1452 WS=32 SACK_PERM=1 |
| 25015 | 1373.461979 | 182.61.200.6 | 192.168.1.117 | TCP | 60 443 → 51056 [ACK] Seq=1032 Ack=5202 Win=39680 Len=0 |
| 25016 | 1373.462131 | 192.168.1.117 | 182.61.200.6 | TCP | 54 51056 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0 |
| 25017 | 1373.462684 | 192.168.1.117 | 182.61.200.6 | TLSv1.2 | 571 Client Hello |
| 25018 | 1373.489377 | 182.61.200.6 | 192.168.1.117 | TLSv1.2 | 933 Application Data |
| 25019 | 1373.491402 | 182.61.200.6 | 192.168.1.117 | TCP | 60 443 → 51056 [ACK] Seq=1 Ack=518 Win=30336 Len=0 |
| 25020 | 1373.491488 | 182.61.200.6 | 192.168.1.117 | TLSv1.2 | 150 Server Hello |
| 25021 | 1373.491488 | 182.61.200.6 | 192.168.1.117 | TLSv1.2 | 60 Change Cipher Spec |
| 25022 | 1373.491545 | 192.168.1.117 | 182.61.200.6 | TCP | 54 51056 → 443 [ACK] Seq=518 Ack=103 Win=131840 Len=0 |
| 25023 | 1373.491579 | 182.61.200.6 | 192.168.1.117 | TLSv1.2 | 99 Encrypted Handshake Message |

0101 = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window size value: 1240
[Calculated window size: 39680]
[Window size scaling factor: 32]
Checksum: 0xa329 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
SEQ/ACK analysis
[This is an ACK to the segment in frame: 25012]
[The RTT to ACK the segment was: 0.028939000 seconds]
[IRTT: 0.028052000 seconds]
Timestamps
[Time since first frame in this TCP stream: 2.013059000 seconds]
[Time since previous frame in this TCP stream: 0.028939000 seconds]

0000 54 bf 64 83 7d c6 74 05 a5 8b 79 59 08 00 45 00 T.d.}.t. ...yY...E-
0010 00 28 c1 09 40 00 24 06 55 65 b6 3d c8 06 c0 a8 -(.@.\$: Ue=....
0020 01 75 01 bb c7 6a f3 c3 b9 45 d9 ec 77 55 50 10 -u...j...E...uUP-
0030 04 d8 a3 29 00 00 00 00 c5 e1 23 31 ...}....-#1

图九：TCP 三次握手-ACK

| | | | | | | |
|-------|-------------|---------------|---------------|-----|----|--|
| 25884 | 1430.737036 | 182.61.200.6 | 192.168.1.117 | TCP | 66 | [TCP Keep-Alive ACK] 443 → 51060 [ACK] Seq=578 Ack=3016 Win=35968 Len=0 SLE=3015 |
| 25885 | 1430.737873 | 182.61.200.6 | 192.168.1.117 | TCP | 66 | [TCP Keep-Alive ACK] 443 → 51061 [ACK] Seq=526 Ack=2445 Win=33920 Len=0 SLE=2444 |
| 25887 | 1430.744457 | 192.168.1.117 | 182.61.200.6 | TCP | 55 | [TCP Keep-Alive] 51050 → 443 [ACK] Seq=25631 Ack=53016 Win=131328 Len=1 |
| 25890 | 1430.772821 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | [TCP Keep-Alive ACK] 443 → 51050 [ACK] Seq=53016 Ack=25632 Win=84480 Len=0 |
| 25976 | 1443.276338 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | 443 → 51056 [FIN, ACK] Seq=11262 Ack=23589 Win=76288 Len=0 |
| 25977 | 1443.276412 | 192.168.1.117 | 182.61.200.6 | TCP | 54 | 51056 → 443 [ACK] Seq=23589 Ack=11263 Win=131072 Len=0 |
| 26004 | 1445.747816 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | 443 → 51050 [FIN, ACK] Seq=53016 Ack=25632 Win=84480 Len=0 |
| 26005 | 1445.747854 | 192.168.1.117 | 182.61.200.6 | TCP | 54 | 51050 → 443 [ACK] Seq=25632 Ack=53017 Win=131328 Len=0 |
| 26006 | 1445.764160 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | [TCP Keep-Alive] 443 → 51061 [ACK] Seq=525 Ack=2445 Win=33920 Len=0 |
| 26007 | 1445.764194 | 192.168.1.117 | 182.61.200.6 | TCP | 54 | [TCP Keep-Alive ACK] 51061 → 443 [ACK] Seq=2445 Ack=526 Win=131584 Len=0 |
| 26010 | 1445.793985 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | [TCP Keep-Alive] 443 → 51060 [ACK] Seq=577 Ack=3016 Win=35968 Len=0 |
| 26011 | 1445.794002 | 192.168.1.117 | 182.61.200.6 | TCP | 54 | [TCP Keep-Alive ACK] 51060 → 443 [ACK] Seq=3016 Ack=578 Win=131328 Len=0 |
| 26013 | 1446.303457 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | 443 → 51056 [RST] Seq=11263 Win=0 Len=0 |
| 26045 | 1448.782118 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | 443 → 51050 [RST] Seq=53017 Win=0 Len=0 |

Sequence number (raw): 2692627068

[Next sequence number: 11263 (relative sequence number)]

Acknowledgment number: 23589 (relative ack number)

Acknowledgment number (raw): 2722726512

0101 = Header Length: 20 bytes (5)

> Flags: 0x011 (FIN, ACK)

Window size value: 2384

[Calculated window size: 76288]

[Window size scaling factor: 32]

Checksum: 0x9d41 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

v [Timestamps]

[Time since first frame in this TCP stream: 69.842698000 seconds]

[Time since previous frame in this TCP stream: 14.973494000 seconds]

| | | | | |
|------|-------------------------|-------------------------|-------------------|--|
| 0000 | 54 bf 64 83 7d c6 74 05 | a5 8b 79 59 08 00 45 00 | T-d-)-t-...yY-E- | |
| 0010 | 00 28 ba dc 40 00 24 06 | 5b 92 b6 3d c8 06 c0 a8 | -(.-@.\$- .-=.... | |
| 0020 | 01 75 01 bb c7 70 a0 7e | 3a 7c a2 49 82 70 50 11 | -u-...p-~ I-pP- | |
| 0030 | 09 50 9d 41 00 00 00 00 | 23 c3 9e 19 | -P-A-...#-... | |

图十：TCP 四次握手-[FIN,ACK]

| | | | | | | |
|-------|-------------|---------------|---------------|-----|----|--|
| 25884 | 1430.737036 | 182.61.200.6 | 192.168.1.117 | TCP | 66 | [TCP Keep-Alive ACK] 443 → 51060 [ACK] Seq=578 Ack=3016 Win=35968 Len=0 SLE=3015 |
| 25885 | 1430.737873 | 182.61.200.6 | 192.168.1.117 | TCP | 66 | [TCP Keep-Alive ACK] 443 → 51061 [ACK] Seq=526 Ack=2445 Win=33920 Len=0 SLE=2444 |
| 25887 | 1430.744457 | 192.168.1.117 | 182.61.200.6 | TCP | 55 | [TCP Keep-Alive] 51050 → 443 [ACK] Seq=25631 Ack=53016 Win=131328 Len=1 |
| 25890 | 1430.772821 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | [TCP Keep-Alive ACK] 443 → 51050 [ACK] Seq=53016 Ack=25632 Win=84480 Len=0 |
| 25976 | 1443.276338 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | 443 → 51056 [FIN, ACK] Seq=11262 Ack=23589 Win=76288 Len=0 |
| 25977 | 1443.276412 | 192.168.1.117 | 182.61.200.6 | TCP | 54 | 51056 → 443 [ACK] Seq=23589 Ack=11263 Win=131072 Len=0 |
| 26004 | 1445.747816 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | 443 → 51050 [FIN, ACK] Seq=53016 Ack=25632 Win=84480 Len=0 |
| 26005 | 1445.747854 | 192.168.1.117 | 182.61.200.6 | TCP | 54 | 51050 → 443 [ACK] Seq=25632 Ack=53017 Win=131328 Len=0 |
| 26006 | 1445.764160 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | [TCP Keep-Alive] 443 → 51061 [ACK] Seq=525 Ack=2445 Win=33920 Len=0 |
| 26007 | 1445.764194 | 192.168.1.117 | 182.61.200.6 | TCP | 54 | [TCP Keep-Alive ACK] 51061 → 443 [ACK] Seq=2445 Ack=526 Win=131584 Len=0 |
| 26010 | 1445.793985 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | [TCP Keep-Alive] 443 → 51060 [ACK] Seq=577 Ack=3016 Win=35968 Len=0 |
| 26011 | 1445.794002 | 192.168.1.117 | 182.61.200.6 | TCP | 54 | [TCP Keep-Alive ACK] 51060 → 443 [ACK] Seq=3016 Ack=578 Win=131328 Len=0 |
| 26013 | 1446.303457 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | 443 → 51056 [RST] Seq=11263 Win=0 Len=0 |
| 26045 | 1448.782118 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | 443 → 51050 [RST] Seq=53017 Win=0 Len=0 |

0101 = Header Length: 20 bytes (5)

> Flags: 0x010 (ACK)

Window size value: 512

[Calculated window size: 131072]

[Window size scaling factor: 256]

Checksum: 0x407c [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

v [SEQ/ACK analysis]

[This is an ACK to the segment in frame: 25976]

[The RTT to ACK the segment was: 0.000074000 seconds]

[RTT: 0.028491000 seconds]

v [Timestamps]

[Time since first frame in this TCP stream: 69.842772000 seconds]

[Time since previous frame in this TCP stream: 0.000074000 seconds]

| | | | |
|------|-------------------------|-------------------------|-------------------|
| 0000 | 74 05 a5 8b 79 59 54 bf | 64 83 7d c6 08 00 45 00 | t-...yYT-d-)...E- |
| 0010 | 00 28 f6 11 40 00 00 06 | 00 00 c0 a0 01 75 b6 3d | -(.-@-...-...u-=- |
| 0020 | c8 06 c7 70 01 bb a2 49 | 82 70 a0 7e 3a 7d 50 10 | -...p-~I-p-~ P- |
| 0030 | 02 00 40 7c 00 00 00 00 | | --@ ... |

图十一：TCP 四次握手-ACK

| | | | | | | |
|-------|-------------|---------------|---------------|-----|----|--|
| 25884 | 1430.737036 | 182.61.200.6 | 192.168.1.117 | TCP | 66 | [TCP Keep-Alive ACK] 443 → 51060 [ACK] Seq=578 Ack=3016 Win=35968 Len=0 SLE=3015 |
| 25885 | 1430.737873 | 182.61.200.6 | 192.168.1.117 | TCP | 66 | [TCP Keep-Alive ACK] 443 → 51061 [ACK] Seq=526 Ack=2445 Win=33920 Len=0 SLE=2444 |
| 25887 | 1430.744457 | 192.168.1.117 | 182.61.200.6 | TCP | 55 | [TCP Keep-Alive] 51050 → 443 [ACK] Seq=25631 Ack=53016 Win=131328 Len=1 |
| 25890 | 1430.772821 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | [TCP Keep-Alive ACK] 443 → 51050 [ACK] Seq=53016 Ack=25632 Win=84480 Len=0 |
| 25976 | 1443.276338 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | 443 → 51056 [FIN, ACK] Seq=11262 Ack=23589 Win=76288 Len=0 |
| 25977 | 1443.276412 | 192.168.1.117 | 182.61.200.6 | TCP | 54 | 51056 → 443 [ACK] Seq=23589 Ack=11263 Win=131072 Len=0 |
| 26004 | 1445.747816 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | 443 → 51050 [FIN, ACK] Seq=53016 Ack=25632 Win=84480 Len=0 |
| 26005 | 1445.747854 | 192.168.1.117 | 182.61.200.6 | TCP | 54 | 51050 → 443 [ACK] Seq=25632 Ack=53017 Win=131328 Len=0 |
| 26006 | 1445.764160 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | [TCP Keep-Alive] 443 → 51061 [ACK] Seq=525 Ack=2445 Win=33920 Len=0 |
| 26007 | 1445.764194 | 192.168.1.117 | 182.61.200.6 | TCP | 54 | [TCP Keep-Alive ACK] 51061 → 443 [ACK] Seq=2445 Ack=526 Win=131584 Len=0 |
| 26010 | 1445.793985 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | [TCP Keep-Alive] 443 → 51060 [ACK] Seq=577 Ack=3016 Win=35968 Len=0 |
| 26011 | 1445.794002 | 192.168.1.117 | 182.61.200.6 | TCP | 54 | [TCP Keep-Alive ACK] 51060 → 443 [ACK] Seq=3016 Ack=578 Win=131328 Len=0 |
| 26013 | 1446.303457 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | 443 → 51056 [RST] Seq=11263 Win=0 Len=0 |
| 26045 | 1448.782118 | 182.61.200.6 | 192.168.1.117 | TCP | 60 | 443 → 51050 [RST] Seq=53017 Win=0 Len=0 |

Sequence number (raw): 4089742421

[Next sequence number: 53017 (relative sequence number)]

Acknowledgment number: 25632 (relative ack number)

Acknowledgment number (raw): 3656173347

0101 = Header Length: 20 bytes (5)

> Flags: 0x011 (FIN, ACK)

Window size value: 2640

[Calculated window size: 84480]

[Window size scaling factor: 32]

Checksum: 0x82d1 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

▼ [Timestamps]

[Time since first frame in this TCP stream: 74.298896000 seconds]

[Time since previous frame in this TCP stream: 14.974955000 seconds]

图十二：TCP 四次握手-[FIN,ACK]

| | | | | | |
|-------|-------------|---------------|---------------|-----|---|
| 25976 | 1443.276338 | 182.61.200.6 | 192.168.1.117 | TCP | 60 443 → 51056 [FIN, ACK] Seq=11262 Ack=23589 Win=76288 Len=0 |
| 25977 | 1443.276412 | 192.168.1.117 | 182.61.200.6 | TCP | 54 51056 → 443 [ACK] Seq=23589 Ack=11263 Win=131072 Len=0 |
| 26004 | 1445.747816 | 182.61.200.6 | 192.168.1.117 | TCP | 60 443 → 51050 [FIN, ACK] Seq=53016 Ack=25632 Win=84480 Len=0 |
| 26005 | 1445.747854 | 192.168.1.117 | 182.61.200.6 | TCP | 54 51050 → 443 [ACK] Seq=25632 Ack=53017 Win=131328 Len=0 |
| 26006 | 1445.764160 | 182.61.200.6 | 192.168.1.117 | TCP | 60 [TCP Keep-Alive] 443 → 51061 [ACK] Seq=525 Ack=2445 Win=33920 Len=0 |
| 26007 | 1445.764194 | 192.168.1.117 | 182.61.200.6 | TCP | 54 [TCP Keep-Alive ACK] 51061 → 443 [ACK] Seq=2445 Ack=526 Win=131584 Len=0 |
| 26010 | 1445.793985 | 182.61.200.6 | 192.168.1.117 | TCP | 60 [TCP Keep-Alive] 443 → 51060 [ACK] Seq=577 Ack=3016 Win=35968 Len=0 |
| 26011 | 1445.794002 | 192.168.1.117 | 182.61.200.6 | TCP | 54 [TCP Keep-Alive ACK] 51060 → 443 [ACK] Seq=3016 Ack=578 Win=131328 Len=0 |
| 26013 | 1446.303457 | 182.61.200.6 | 192.168.1.117 | TCP | 60 443 → 51056 [RST] Seq=11263 Win=0 Len=0 |
| 26045 | 1448.782118 | 182.61.200.6 | 192.168.1.117 | TCP | 60 443 → 51050 [RST] Seq=53017 Win=0 Len=0 |

```

0101 ... = Header Length: 20 bytes (5)
> Flags: 0x010 (ACK)
Window size value: 513
[Calculated window size: 131328]
[Window size scaling factor: 256]
Checksum: 0x407c [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
▼ [SEQ/ACK analysis]
  [This is an ACK to the segment in frame: 26004]
  [The RTT to ACK the segment was: 0.000038000 seconds]
  [iRTT: 0.028052000 seconds]
▼ [Timestamps]
  [Time since first frame in this TCP stream: 74.298934000 seconds]
  [Time since previous frame in this TCP stream: 0.000038000 seconds]
0000 74 05 a5 8b 79 59 54 bf 64 83 7d c6 08 00 45 00  t...yY.T. d.}...E.
0010 00 28 f6 12 40 00 80 36 00 00 c0 a8 01 75 b6 3d  .(.@.  .....u.=
0020 c8 06 c7 6a 01 bb d9 ec c7 23 f3 c4 84 56 50 10  ...}....-#...VP.
0030 02 01 40 7c 00 00                                .@|..

```

图十三：TCP 四次握手 ACK

ICMP 抓包分析：

实验：

| | | | | | | |
|---|--------|----------|--------------|------|------------------------|---|
| 1 | 0.0... | 192.1... | 106.11.43... | ICMP | 74 Echo (ping) request | id=0x0001, seq=23/5888, ttl=128 (reply in 2) |
| 2 | 0.0... | 106.1... | 192.168.1... | ICMP | 74 Echo (ping) reply | id=0x0001, seq=23/5888, ttl=82 (request in 1) |
| 3 | 1.0... | 192.1... | 106.11.43... | ICMP | 74 Echo (ping) request | id=0x0001, seq=24/6144, ttl=128 (reply in 4) |
| 4 | 1.0... | 106.1... | 192.168.1... | ICMP | 74 Echo (ping) reply | id=0x0001, seq=24/6144, ttl=82 (request in 3) |
| 5 | 2.0... | 192.1... | 106.11.43... | ICMP | 74 Echo (ping) request | id=0x0001, seq=25/6400, ttl=128 (reply in 6) |
| 6 | 2.0... | 106.1... | 192.168.1... | ICMP | 74 Echo (ping) reply | id=0x0001, seq=25/6400, ttl=82 (request in 5) |
| 7 | 3.0... | 192.1... | 106.11.43... | ICMP | 74 Echo (ping) request | id=0x0001, seq=26/6656, ttl=128 (reply in 8) |
| 8 | 3.0... | 106.1... | 192.168.1... | ICMP | 74 Echo (ping) reply | id=0x0001, seq=26/6656, ttl=82 (request in 7) |

```

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{18A477C5-5DE8-447
> Ethernet II, Src: Dell_83:7d:c6 (54:bf:64:83:7d:c6), Dst: Tp-LinkT_8b:79:59 (74:05:a5:8b:79:59)
> Internet Protocol Version 4, Src: 192.168.1.117, Dst: 106.11.43.183
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4d44 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence number (BE): 23 (0x0017)
  Sequence number (LE): 5888 (0x1700)
<
0000 74 05 a5 8b 79 59 54 bf 64 83 7d c6 08 00 45 00  t...yY.T. d.}...E.
0010 00 3c 78 ff 00 00 80 01 00 00 c0 a8 01 75 6a 0b  .<X.....u.j.
0020 2b b7 08 00 4d 44 00 01 00 17 61 62 63 64 65 66  +...MD...abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69                    wabcdegh i

```

图十四：ICMP 抓包分析（前述帧结构，物理层协议，网络层协议不在详细解释，主要不同的是网络控制信息协议相关内容（类型，编码，校验和经校验正确，windows 下的 BE（大数端），LE（小数端）等）