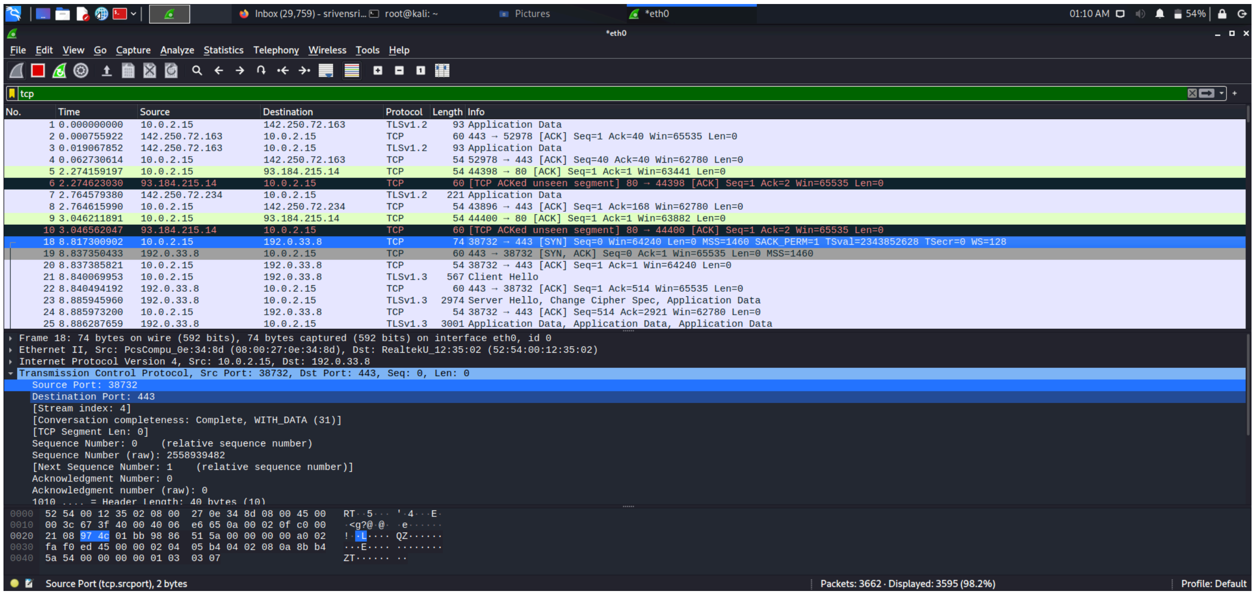
Objective: To understand how a TCP session is established and terminated, including the role of the three-way handshake and the process of closing a connection.

1. **Open Wireshark**: Launch Wireshark on your computer with the necessary administrative privileges. Choose your network interface eth0 or wifi. Browse a web server or streaming service to capture data.
2. Initiate a TCP Connection
3. **Apply TCP Filter**: In the Wireshark filter bar, type `tcp` to filter only TCP packets. This will narrow down the displayed packets to only those using the TCP protocol.
4. **Locate the Three-Way Handshake Packets**:

SYN: The synchronize packet is the first step in the TCP three-way handshake. It is sent from the client (your computer) to the server to initiate a new TCP connection.



Inbox (29,759) - srivensri...
root@kali: ~
Pictures
*eth0
01:10 AM
54%
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

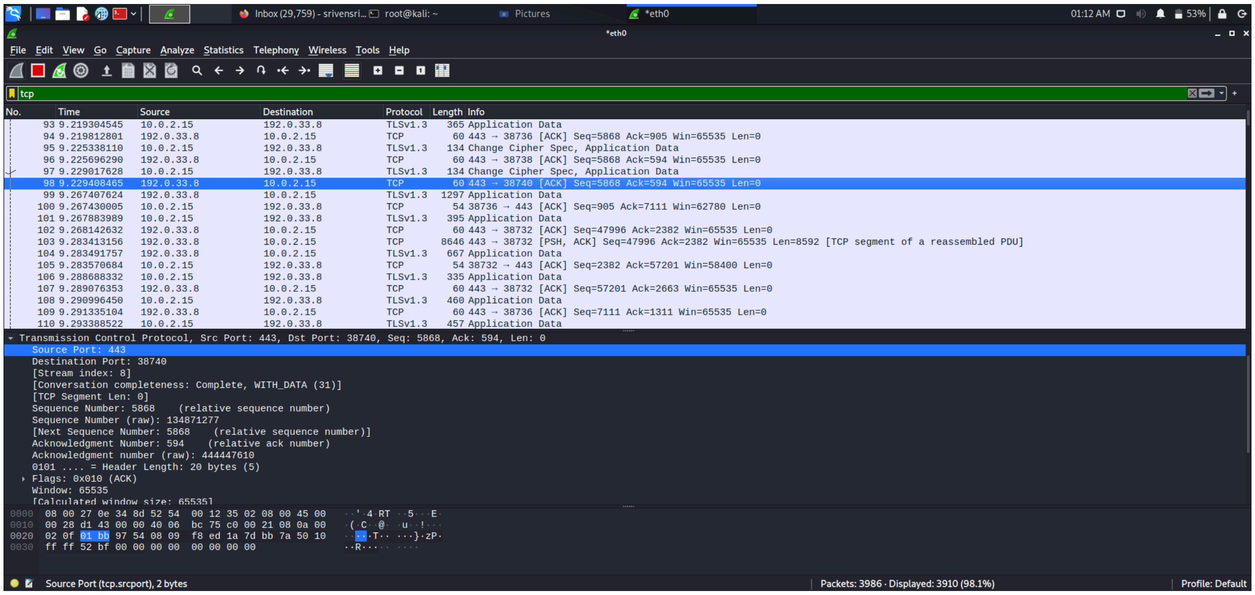
```
No.    Time          Source            Destination      Protocol  Length Info
     1 0.000000000   10.0.2.15         142.250.72.163   TLSv1.2     93 Application Data
     2 0.000755922   142.250.72.163    10.0.2.15        TCP         60 443 → 52978 [ACK] Seq=1 Ack=40 Win=65535 Len=0
     3 0.019067852   142.250.72.163    10.0.2.15        TLSv1.2     93 Application Data
     4 0.062730614   10.0.2.15         142.250.72.163   TCP         54 52978 → 443 [ACK] Seq=40 Ack=40 Win=62780 Len=0
     5 2.274159197   10.0.2.15         93.184.215.14    TCP         54 44398 → 80 [ACK] Seq=1 Ack=1 Win=63441 Len=0
     6 2.274623030   93.184.215.14     10.0.2.15        TCP         60 [TCP ACKed unseen segment] 80 → 44398 [ACK] Seq=1 Ack=2 Win=65535 Len=0
     7 2.764579380   142.250.72.234    10.0.2.15        TLSv1.2    221 Application Data
     8 2.764615990   10.0.2.15         142.250.72.234   TCP         54 43896 → 443 [ACK] Seq=1 Ack=168 Win=62780 Len=0
     9 3.046211891   10.0.2.15         93.184.215.14    TCP         54 44400 → 80 [ACK] Seq=1 Ack=1 Win=63882 Len=0
    10 3.046562047   93.184.215.14     10.0.2.15        TCP         60 [TCP ACKed unseen segment] 80 → 44400 [ACK] Seq=1 Ack=2 Win=65535 Len=0
    18 8.817300902   10.0.2.15         192.0.33.8       TCP         74 38732 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2343852628 TSecr=0 WS=128
    19 8.837350433   192.0.33.8        10.0.2.15        TCP         60 443 → 38732 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
    20 8.837385821   10.0.2.15         192.0.33.8       TCP         54 38732 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
    21 8.840069953   10.0.2.15         192.0.33.8       TLSv1.3    567 Client Hello
    22 8.840494192   192.0.33.8        10.0.2.15        TCP         60 443 → 38732 [ACK] Seq=1 Ack=514 Win=65535 Len=0
    23 8.885945960   192.0.33.8        10.0.2.15        TLSv1.3   2974 Server Hello, Change Cipher Spec, Application Data
    24 8.885973200   10.0.2.15         192.0.33.8       TCP         54 38732 → 443 [ACK] Seq=514 Ack=2921 Win=62780 Len=0
    25 8.886287659   192.0.33.8        10.0.2.15        TLSv1.3   3001 Application Data, Application Data, Application Data
```

```
› Frame 18: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
› Ethernet II, Src: PcsCompu_0e:34:8d (08:00:27:0e:34:8d), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.0.33.8
˅ Transmission Control Protocol, Src Port: 38732, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 38732
    Destination Port: 443
    [Stream index: 4]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2558939482
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1010 .... = Header Length: 40 bytes (10)
```

```
0000  52 54 00 12 35 02 08 00  27 0e 34 8d 08 00 45 00   RT··5··· '·4···E·
0010  00 3c 67 3f 40 00 40 06  e6 65 0a 00 02 0f c0 00   ·<g?@·@· ·e······
0020  21 08 97 4c 01 bb 98 86  51 5a 00 00 00 00 a0 02   !··L···· QZ······
0030  fa f0 ed 45 00 00 02 04  05 b4 04 02 08 0a 8b b4   ···E···· ········
0040  5a 54 00 00 00 00 01 03  03 07                     ZT······ ··
```

Source Port (tcp.srcport), 2 bytes | Packets: 3662 · Displayed: 3595 (98.2%) | Profile: Default

SYN-ACK:The synchronize-acknowledgment packet is the server's response to the SYN packet from the client. It acknowledges the receipt of the SYN packet and sends back its own SYN to synchronize the connection.



Inbox (29,759) - srivensri...
root@kali: ~
Pictures
*eth0
01:12 AM
53%
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

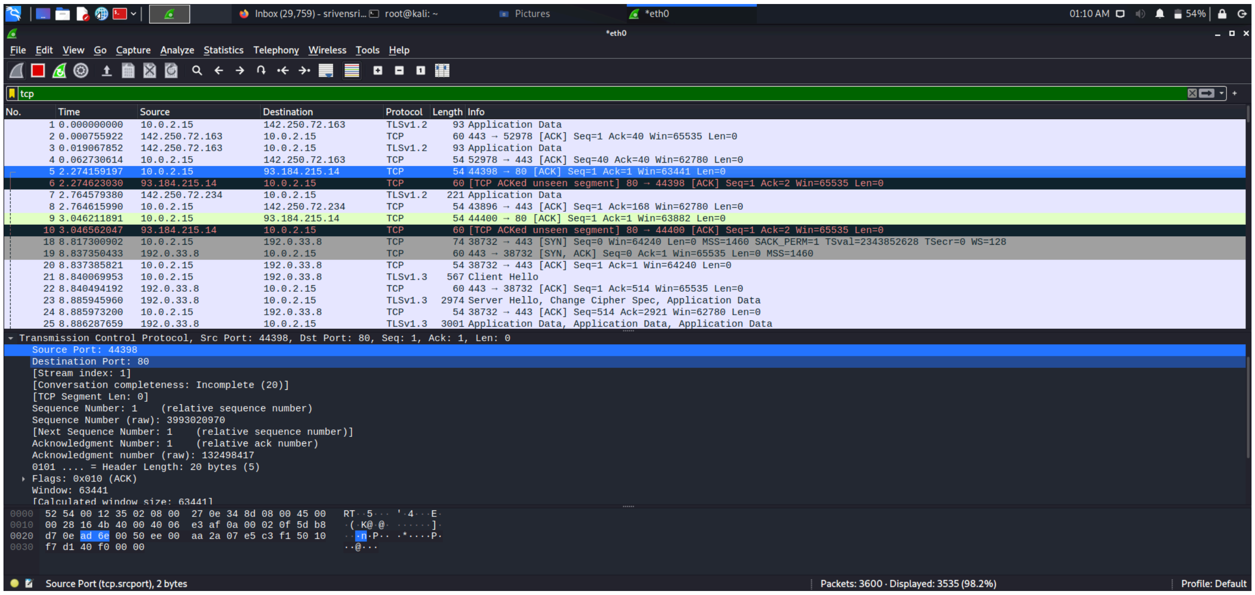
```
No.  Time          Source        Destination   Protocol Length Info
  93 9.219304545   10.0.2.15     192.0.33.8    TLSv1.3   365 Application Data
  94 9.219812801   192.0.33.8    10.0.2.15     TCP        60 443 → 38736 [ACK] Seq=5868 Ack=905 Win=65535 Len=0
  95 9.225338110   10.0.2.15     192.0.33.8    TLSv1.3   134 Change Cipher Spec, Application Data
  96 9.225696290   192.0.33.8    10.0.2.15     TCP        60 443 → 38738 [ACK] Seq=5868 Ack=594 Win=65535 Len=0
  97 9.229017628   10.0.2.15     192.0.33.8    TLSv1.3   134 Change Cipher Spec, Application Data
  98 9.229408465   192.0.33.8    10.0.2.15     TCP        60 443 → 38740 [ACK] Seq=5868 Ack=594 Win=65535 Len=0
  99 9.267407624   192.0.33.8    10.0.2.15     TLSv1.3  1297 Application Data
 100 9.267430005   10.0.2.15     192.0.33.8    TCP        54 38736 → 443 [ACK] Seq=905 Ack=7111 Win=62780 Len=0
 101 9.267883989   10.0.2.15     192.0.33.8    TLSv1.3   395 Application Data
 102 9.268142632   192.0.33.8    10.0.2.15     TCP        60 443 → 38732 [ACK] Seq=47996 Ack=2382 Win=65535 Len=0
 103 9.283413156   192.0.33.8    10.0.2.15     TCP      8646 443 → 38732 [PSH, ACK] Seq=47996 Ack=2382 Win=65535 Len=8592 [TCP segment of a reassembled PDU]
 104 9.283491757   192.0.33.8    10.0.2.15     TLSv1.3   667 Application Data
 105 9.283570684   10.0.2.15     192.0.33.8    TCP        54 38732 → 443 [ACK] Seq=2382 Ack=57201 Win=58400 Len=0
 106 9.288688332   10.0.2.15     192.0.33.8    TLSv1.3   335 Application Data
 107 9.289076353   192.0.33.8    10.0.2.15     TCP        60 443 → 38732 [ACK] Seq=57201 Ack=2663 Win=65535 Len=0
 108 9.290996450   10.0.2.15     192.0.33.8    TLSv1.3   460 Application Data
 109 9.291335104   192.0.33.8    10.0.2.15     TCP        60 443 → 38736 [ACK] Seq=7111 Ack=1311 Win=65535 Len=0
 110 9.293388522   10.0.2.15     192.0.33.8    TLSv1.3   457 Application Data
```

```
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 38740, Seq: 5868, Ack: 594, Len: 0
    Source Port: 443
    Destination Port: 38740
    [Stream index: 8]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 5868    (relative sequence number)
    Sequence Number (raw): 134871277
    [Next Sequence Number: 5868    (relative sequence number)]
    Acknowledgment Number: 594    (relative ack number)
    Acknowledgment number (raw): 444447610
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x010 (ACK)
    Window: 65535
    [Calculated window size: 65535]
```

```
0000  08 00 27 0e 34 8d 52 54  00 12 35 02 08 00 45 00   ··'·4·RT ··5···E·
0010  00 28 d1 43 00 00 40 06  bc 75 c0 00 21 08 0a 00   ·(·C··@· ·u··!···
0020  02 0f 01 bb 97 54 08 09  f8 ed 1a 7d bb 7a 50 10   ·····T·· ···}·zP·
0030  ff ff 52 bf 00 00 00 00  00 00 00 00               ··R····· ····
```

Source Port (tcp.srcport), 2 bytes | Packets: 3986 · Displayed: 3910 (98.1%) | Profile: Default

ACK: The (acknowledgment) packet is sent from the client to the server to acknowledge the receipt of the server's SYN-ACK packet, completing the three-way handshake.



Inbox (29,759) - srivensri...
root@kali: ~
Pictures
*eth0
01:10 AM
54%
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.  Time          Source          Destination     Protocol Length Info
   1 0.000000000   10.0.2.15       142.250.72.163  TLSv1.2    93 Application Data
   2 0.000755922   142.250.72.163  10.0.2.15       TCP        60 443 → 52978 [ACK] Seq=1 Ack=40 Win=65535 Len=0
   3 0.019067852   142.250.72.163  10.0.2.15       TLSv1.2    93 Application Data
   4 0.062730614   10.0.2.15       142.250.72.163  TCP        54 52978 → 443 [ACK] Seq=40 Ack=40 Win=62780 Len=0
   5 2.274159197   10.0.2.15       93.184.215.14   TCP        54 44398 → 80 [ACK] Seq=1 Ack=1 Win=63441 Len=0
   6 2.274623030   93.184.215.14   10.0.2.15       TCP        60 [TCP ACKed unseen segment] 80 → 44398 [ACK] Seq=1 Ack=2 Win=65535 Len=0
   7 2.764579380   142.250.72.234  10.0.2.15       TLSv1.2   221 Application Data
   8 2.764615990   10.0.2.15       142.250.72.234  TCP        54 43896 → 443 [ACK] Seq=1 Ack=168 Win=62780 Len=0
   9 3.046211891   10.0.2.15       93.184.215.14   TCP        54 44400 → 80 [ACK] Seq=1 Ack=1 Win=63882 Len=0
  10 3.046562047   93.184.215.14   10.0.2.15       TCP        60 [TCP ACKed unseen segment] 80 → 44400 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  18 8.817300902   10.0.2.15       192.0.33.8      TCP        74 38732 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2343852628 TSecr=0 WS=128
  19 8.837350433   192.0.33.8      10.0.2.15       TCP        60 443 → 38732 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
  20 8.837385821   10.0.2.15       192.0.33.8      TCP        54 38732 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  21 8.840069953   10.0.2.15       192.0.33.8      TLSv1.3   567 Client Hello
  22 8.840494192   192.0.33.8      10.0.2.15       TCP        60 443 → 38732 [ACK] Seq=1 Ack=514 Win=65535 Len=0
  23 8.885945960   192.0.33.8      10.0.2.15       TLSv1.3  2974 Server Hello, Change Cipher Spec, Application Data
  24 8.885973200   10.0.2.15       192.0.33.8      TCP        54 38732 → 443 [ACK] Seq=514 Ack=2921 Win=62780 Len=0
  25 8.886287659   192.0.33.8      10.0.2.15       TLSv1.3  3001 Application Data, Application Data, Application Data
```

```
▾ Transmission Control Protocol, Src Port: 44398, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 44398
    Destination Port: 80
    [Stream index: 1]
    [Conversation completeness: Incomplete (20)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3993020970
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 132498417
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x010 (ACK)
    Window: 63441
    [Calculated window size: 63441]
```

```
0000  52 54 00 12 35 02 08 00  27 0e 34 8d 08 00 45 00   RT··5··· '·4···E·
0010  00 28 16 4b 40 00 40 06  e3 af 0a 00 02 0f 5d b8   ·(·K@·@· ······]·
0020  d7 0e ad 6e 00 50 ee 00  aa 2a 07 e5 c3 f1 50 10   ···n·P·· ·*····P·
0030  f7 d1 40 f0 00 00                                  ··@···
```

Source Port (tcp.srcport), 2 bytes | Packets: 3600 · Displayed: 3535 (98.2%) | Profile: Default

Explain the Purpose of Each Step:

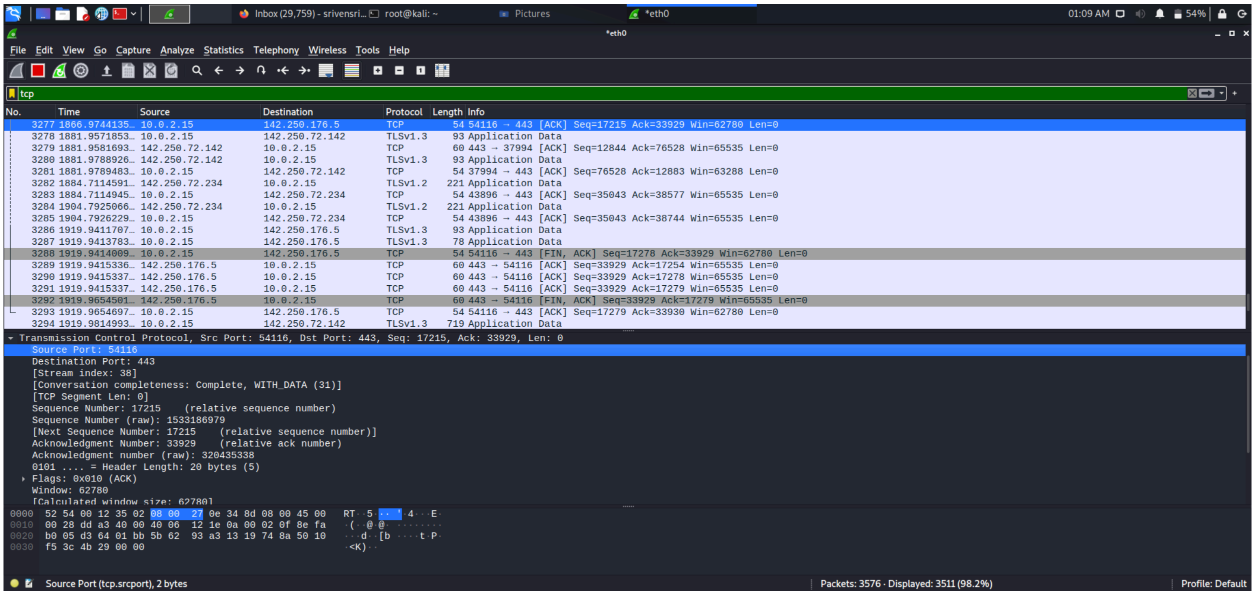
1. **SYN**: The client initiates the connection and synchronizes sequence numbers.
2. **SYN-ACK**: The server acknowledges the client’s SYN and sends its own SYN to establish a session.

3. **ACK**: The client acknowledges the server's SYN-ACK, completing the handshake and establishing a TCP session.

Include Key Fields Observed in Packets:

1. **Sequence Numbers**: They are initialized and keep incrementing at every step.
2. **Acknowledgment Numbers**: They confirm receipt of packets and ensure reliable communication.

Session Termination



tcp

```
No.  Time            Source          Destination     Protocol Length Info
3277 1866.9744135…   10.0.2.15       142.250.176.5   TCP       54 54116 → 443 [ACK] Seq=17215 Ack=33929 Win=62780 Len=0
3278 1881.9571853…   10.0.2.15       142.250.72.142  TLSv1.3   93 Application Data
3279 1881.9581693…   142.250.72.142  10.0.2.15       TCP       60 443 → 37994 [ACK] Seq=12844 Ack=76528 Win=65535 Len=0
3280 1881.9788926…   142.250.72.142  10.0.2.15       TLSv1.3   93 Application Data
3281 1881.9789483…   10.0.2.15       142.250.72.142  TCP       54 37994 → 443 [ACK] Seq=76528 Ack=12883 Win=63288 Len=0
3282 1884.7114591…   142.250.72.234  10.0.2.15       TLSv1.2  221 Application Data
3283 1884.7114945…   10.0.2.15       142.250.72.234  TCP       54 43896 → 443 [ACK] Seq=35043 Ack=38577 Win=65535 Len=0
3284 1904.7925066…   142.250.72.234  10.0.2.15       TLSv1.2  221 Application Data
3285 1904.7926229…   10.0.2.15       142.250.72.234  TCP       54 43896 → 443 [ACK] Seq=35043 Ack=38744 Win=65535 Len=0
3286 1919.9411707…   10.0.2.15       142.250.176.5   TLSv1.3   93 Application Data
3287 1919.9413783…   10.0.2.15       142.250.176.5   TLSv1.3   78 Application Data
3288 1919.9414009…   10.0.2.15       142.250.176.5   TCP       54 54116 → 443 [FIN, ACK] Seq=17278 Ack=33929 Win=62780 Len=0
3289 1919.9415336…   142.250.176.5   10.0.2.15       TCP       60 443 → 54116 [ACK] Seq=33929 Ack=17254 Win=65535 Len=0
3290 1919.9415337…   142.250.176.5   10.0.2.15       TCP       60 443 → 54116 [ACK] Seq=33929 Ack=17278 Win=65535 Len=0
3291 1919.9415337…   142.250.176.5   10.0.2.15       TCP       60 443 → 54116 [ACK] Seq=33929 Ack=17279 Win=65535 Len=0
3292 1919.9654501…   142.250.176.5   10.0.2.15       TCP       60 443 → 54116 [FIN, ACK] Seq=33929 Ack=17279 Win=65535 Len=0
3293 1919.9654697…   10.0.2.15       142.250.176.5   TCP       54 54116 → 443 [ACK] Seq=17279 Ack=33930 Win=62780 Len=0
3294 1919.9814993…   10.0.2.15       142.250.72.142  TLSv1.3  719 Application Data
```

```
▾ Transmission Control Protocol, Src Port: 54116, Dst Port: 443, Seq: 17215, Ack: 33929, Len: 0
    Source Port: 54116
    Destination Port: 443
    [Stream index: 38]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 17215    (relative sequence number)
    Sequence Number (raw): 1533186979
    [Next Sequence Number: 17215    (relative sequence number)]
    Acknowledgment Number: 33929    (relative ack number)
    Acknowledgment number (raw): 320435338
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x010 (ACK)
    Window: 62780
    [Calculated window size: 62780]
```

```
0000  52 54 00 12 35 02 08 00  27 0e 34 8d 08 00 45 00   RT··5···'·4···E·
0010  00 28 dd a3 40 00 40 06  12 1e 0a 00 02 0f 8e fa   ·(··@·@·········
0020  b0 05 d3 64 01 bb 5b 62  93 a3 13 19 74 8a 50 10   ···d··[b····t·P·
0030  f5 3c 4b 29 00 00                                  ·<K)··
```

Source Port (tcp.srcport), 2 bytes

Packets: 3576 · Displayed: 3511 (98.2%)

Profile: Default

1. The **FIN** (finish) packet is the first step in terminating a TCP session. It signals that the sender has finished sending data and wants to close the connection.
2. The **FIN-ACK** (finish-acknowledgement) packet is sent by the receiver of the initial FIN packet to acknowledge the request to terminate the connection and to indicate that it also agrees to close the connection.
3. The **ACK** (acknowledgment) packet is sent in response to the **FIN-ACK** to acknowledge the termination of the connection from both sides. This packet completes the TCP connection termination process.

Key Fields to Note:

1. **Source Port**: The ephemeral port chosen by the client. Mostly it is 443 or 80
2. **Destination Port**: The server port.
3. **Sequence Number**: This should match the acknowledgment number received in the server's SYN-ACK. **Acknowledgment Number**: The server's initial sequence number + 1.