How many bytes are in the TCP header? its different fields? How are values set? verify in Wireshark.

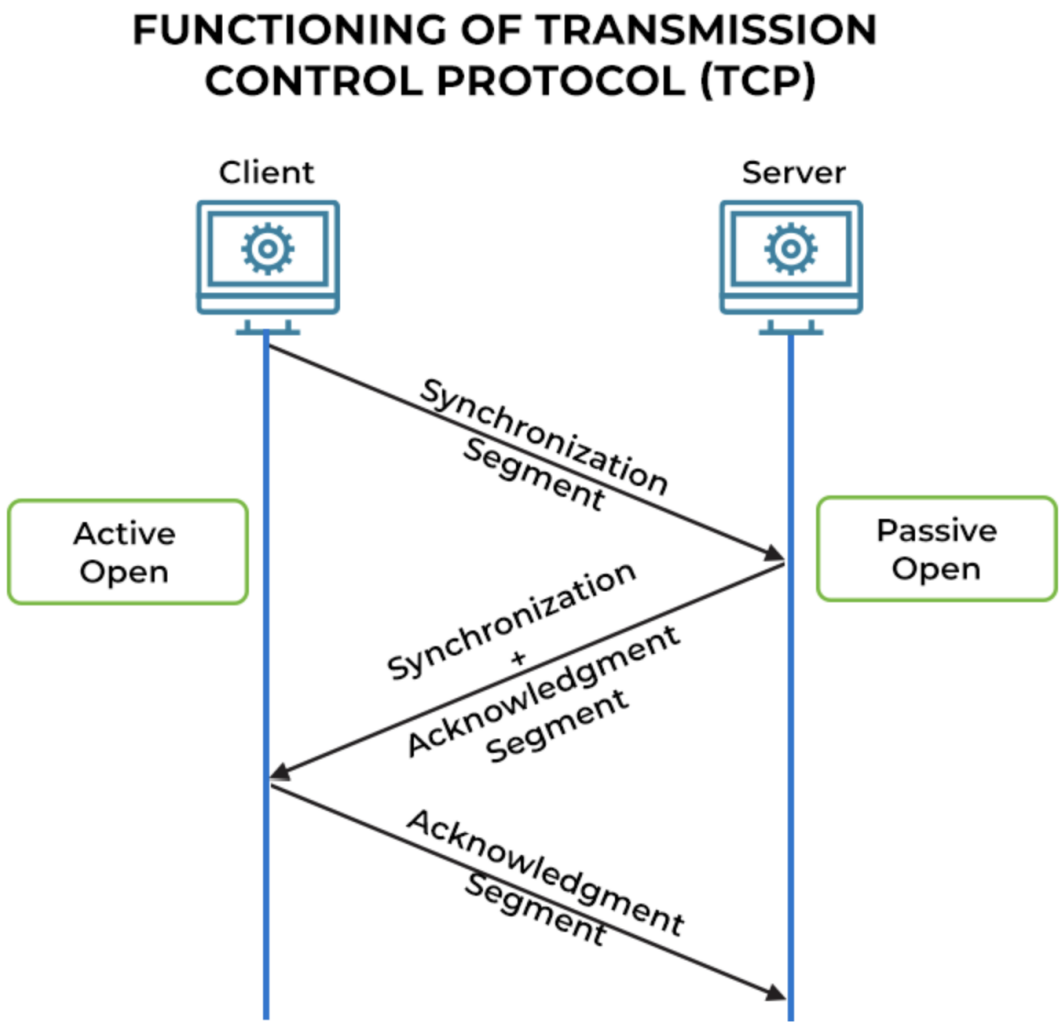
Let’s first talk about TCP.

Transmission Control Protocol

- a communication protocol that allows computing devices and applications to send data over a network and also verify its delivery
- carries packets across the internet and ensures successful delivery of the messages and data across the networks

It operates with the internet protocol.

- **IP** sends each packet to the destination
- **TCP** guarantees the bytes are transmitted in the order they are sent with no errors.



How it works?

- As it is connection-based, it creates and maintains the connection between a sender and receiver while data is passed between them.
- At first, communication must be established between a client and a server.
- It relies on a three-way handshake
- **SYN (The client sends the server a SYN packet (a connection request from its source port to a server's destination port) to initiate a connection)**
- **SYN-ACK (Server responds with a SYN/ACK packet)**

- **ACK (Client receives the SYN/ACK packet and responds with an ACK packet of its own)**
- Once the connection is established, data and messages can be sent between client and server in both directions.
- Here, the transmitted data is divided into segments, each of which is packaged into a datagram and sent to its destination.
- After successful transmission of the messages, the connection is terminated through a four-step process involving **FIN(finish)** and **ACK** packets from both client and server.

Real-life use cases

- Email (**SMTP** protocol for email transmission uses **TCP**)
- File transfer (**FTP** relies on **TCP**)
- Web browsing (**HTTP/HTTPS** protocols use **TCP**)

The **TCP** wraps each data packet with a header containing 10 fields which is typically 20 bytes long.

Each header holds information about the connection and the current data being sent.

The 10 header fields are explained below:

a) **Source port** (sending device's port) **16bits**

b) **Destination port** (receiving device's port) **16bits**

c) **Sequence number** (A device initiating a TCP connection must choose a random initial sequence number which is incremented according to the number of transmitted bytes) **32bits**

d) **Acknowledgment number** (receiving device maintains an acknowledgment number starting with zero which is incremented according to the number of bytes received) **32bits**

e) **TCP data offset** (specifies the size of the TCP header in 32-bit words) **4bits**

f) **Reserved data** (the reserved field is always set to zero) **3bits**

g) **Control flags** (nine control flags to manage data flow in specific situations such as initiating a reset) **9bits**

h) **Checksum** (sender generates a checksum and transmits it in every packet header, the receiving device can use this checksum to check for errors in the receiver header) **16bits**

i) **Urgent pointer** (If URG control flag is set, this value indicates an offset from the sequence number, indicating the last urgent data byte) **16bits**

j) **mTCP optional data** (optional fields for setting maximum segment sizes)

k) **Window size** (specifies the size of the sender's receive window) **16bits**

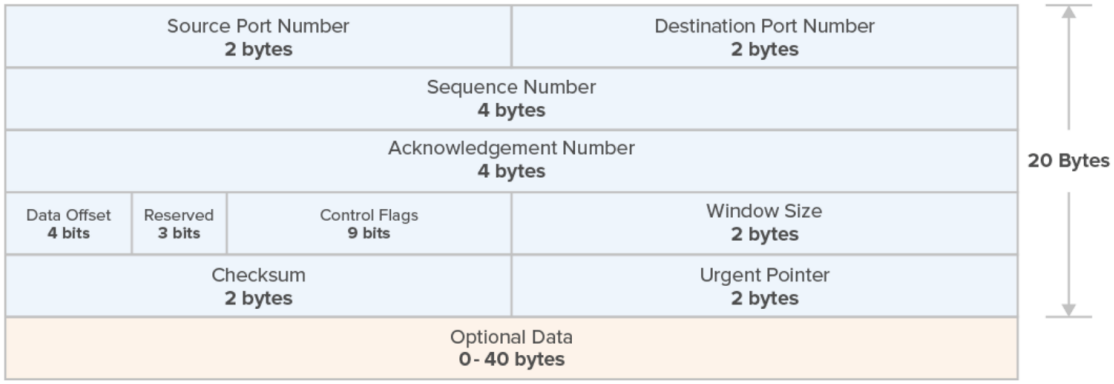
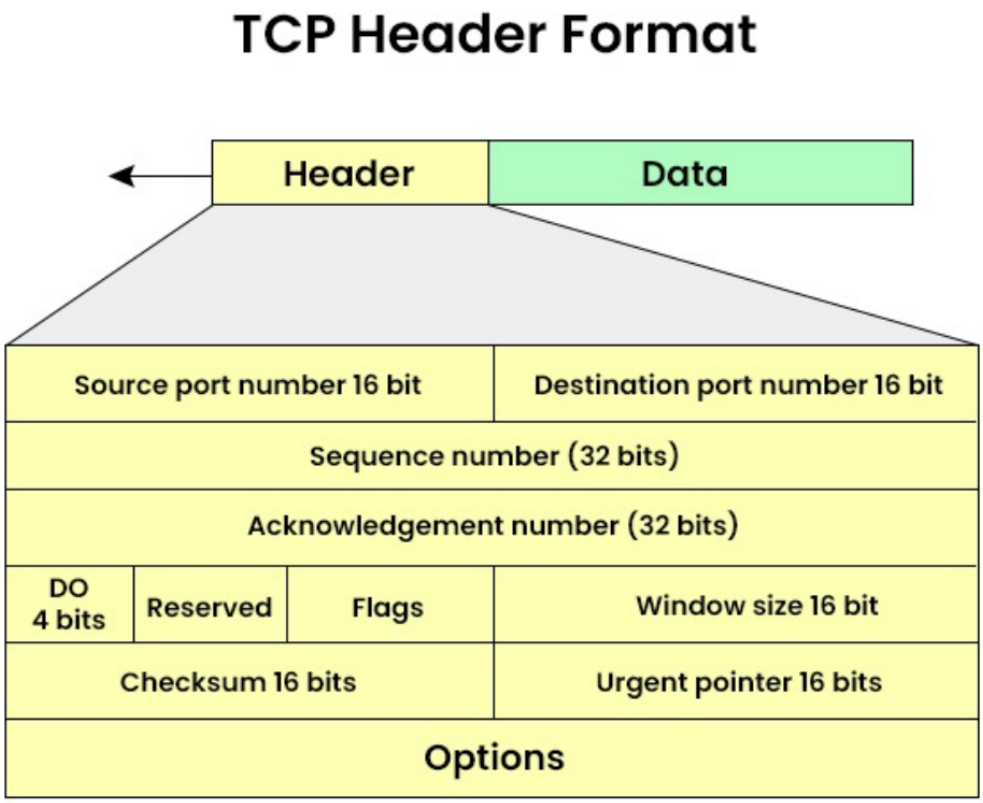


Figure 1 – **TCP Header Model**



How are values set?

a) **Source and Destination port** (set by the application initiating the application and the server applications)

b) **Sequence Number** (set by the sender to indicate the byte sequence in the segment)

c) **Acknowledgment Number** (set by the receiver to acknowledge receipt of data)

d) **Data offset** (set to the size of TCP header (32-bit words)

e) **Reserved** (should be set to 0)

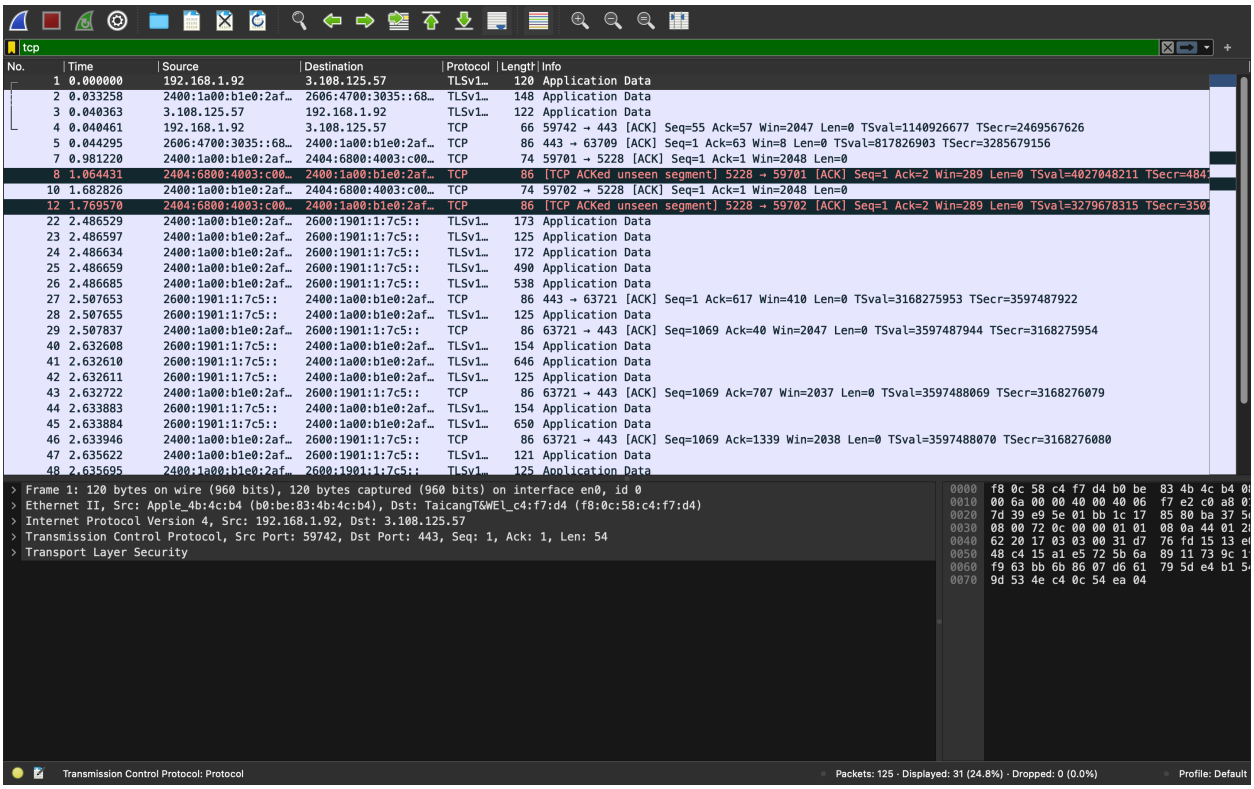
f) **Flags** (set according to the connection state and purpose)

g) **Window size** (set by sender)

h) **Checksum** (computed and set by the sender to check errors)

i) **Urgent pointer** (set if URG flag is used, indicating urgent data)

I captured packets on my network interface using Wireshark and obtained the following results:



tcp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.92	3.108.125.57	TLSv1…	120	Application Data
2	0.033258	2400:1a00:b1e0:2af…	2606:4700:3035::68…	TLSv1…	148	Application Data
3	0.040363	3.108.125.57	192.168.1.92	TLSv1…	122	Application Data
4	0.040461	192.168.1.92	3.108.125.57	TCP	66	59742 → 443 [ACK] Seq=55 Ack=57 Win=2047 Len=0 TSval=1140926677 TSecr=2469567626
5	0.044295	2606:4700:3035::68…	2400:1a00:b1e0:2af…	TCP	86	443 → 63709 [ACK] Seq=1 Ack=63 Win=8 Len=0 TSval=817826903 TSecr=3285679156
7	0.981220	2400:1a00:b1e0:2af…	2404:6800:4003:c00…	TCP	74	59701 → 5228 [ACK] Seq=1 Ack=1 Win=2048 Len=0
8	1.064431	2404:6800:4003:c00…	2400:1a00:b1e0:2af…	TCP	86	[TCP ACKed unseen segment] 5228 → 59701 [ACK] Seq=1 Ack=2 Win=289 Len=0 TSval=4027048211 TSecr=4841
10	1.682826	2400:1a00:b1e0:2af…	2404:6800:4003:c00…	TCP	74	59702 → 5228 [ACK] Seq=1 Ack=1 Win=2048 Len=0
12	1.769570	2404:6800:4003:c00…	2400:1a00:b1e0:2af…	TCP	86	[TCP ACKed unseen segment] 5228 → 59702 [ACK] Seq=1 Ack=2 Win=289 Len=0 TSval=3279678315 TSecr=3507
22	2.486529	2400:1a00:b1e0:2af…	2600:1901:1:7c5::	TLSv1…	173	Application Data
23	2.486597	2400:1a00:b1e0:2af…	2600:1901:1:7c5::	TLSv1…	125	Application Data
24	2.486634	2400:1a00:b1e0:2af…	2600:1901:1:7c5::	TLSv1…	172	Application Data
25	2.486659	2400:1a00:b1e0:2af…	2600:1901:1:7c5::	TLSv1…	490	Application Data
26	2.486685	2400:1a00:b1e0:2af…	2600:1901:1:7c5::	TLSv1…	538	Application Data
27	2.507653	2600:1901:1:7c5::	2400:1a00:b1e0:2af…	TCP	86	443 → 63721 [ACK] Seq=1 Ack=617 Win=410 Len=0 TSval=3168275953 TSecr=3597487922
28	2.507655	2600:1901:1:7c5::	2400:1a00:b1e0:2af…	TLSv1…	125	Application Data
29	2.507837	2400:1a00:b1e0:2af…	2600:1901:1:7c5::	TCP	86	63721 → 443 [ACK] Seq=1069 Ack=40 Win=2047 Len=0 TSval=3597487944 TSecr=3168275954
40	2.632608	2600:1901:1:7c5::	2400:1a00:b1e0:2af…	TLSv1…	154	Application Data
41	2.632610	2600:1901:1:7c5::	2400:1a00:b1e0:2af…	TLSv1…	646	Application Data
42	2.632611	2600:1901:1:7c5::	2400:1a00:b1e0:2af…	TLSv1…	125	Application Data
43	2.632722	2400:1a00:b1e0:2af…	2600:1901:1:7c5::	TCP	86	63721 → 443 [ACK] Seq=1069 Ack=707 Win=2037 Len=0 TSval=3597488069 TSecr=3168276079
44	2.633883	2600:1901:1:7c5::	2400:1a00:b1e0:2af…	TLSv1…	154	Application Data
45	2.633884	2600:1901:1:7c5::	2400:1a00:b1e0:2af…	TLSv1…	650	Application Data
46	2.633946	2400:1a00:b1e0:2af…	2600:1901:1:7c5::	TCP	86	63721 → 443 [ACK] Seq=1069 Ack=1339 Win=2038 Len=0 TSval=3597488070 TSecr=3168276080
47	2.635622	2400:1a00:b1e0:2af…	2600:1901:1:7c5::	TLSv1…	121	Application Data
48	2.635695	2400:1a00:b1e0:2af…	2600:1901:1:7c5::	TLSv1…	125	Application Data

```
> Frame 1: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface en0, id 0
> Ethernet II, Src: Apple_4b:4c:b4 (b0:be:83:4b:4c:b4), Dst: TaicangT&WEl_c4:f7:d4 (f8:0c:58:c4:f7:d4)
> Internet Protocol Version 4, Src: 192.168.1.92, Dst: 3.108.125.57
v Transmission Control Protocol, Src Port: 59742, Dst Port: 443, Seq: 1, Ack: 1, Len: 54
    Source Port: 59742
    Destination Port: 443
    [Stream index: 0]
  v [Conversation completeness: Incomplete (12)]
      ..0. .... = RST: Absent
      ...0 .... = FIN: Absent
      .... 1... = Data: Present
      .... .1.. = ACK: Present
      .... ..0. = SYN-ACK: Absent
      .... ...0 = SYN: Absent
      [Completeness Flags: ··DA··]
    [TCP Segment Len: 54]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 471303552
```

```
0000  f8 0c 58 c4 f7 d4 b0 be  83 4b 4c b4 08
0010  00 6a 00 00 40 00 40 06  f7 e2 c0 a8 01
0020  7d 39 e9 5e 01 bb 1c 17  85 80 ba 37 50
0030  08 00 72 0c 00 00 01 01  08 0a 44 01 2d
0040  62 20 17 03 03 00 31 d7  76 fd 15 13 e6
0050  48 c4 15 a1 e5 72 5b 6a  89 11 73 9c 17
0060  f9 63 bb 6b 86 07 d6 61  79 5d e4 b1 54
0070  9d 53 4e c4 0c 54 ea 04
```

Transmission Control Protocol: Protocol · Packets: 125 · Displayed: 31 (24.8%) · Dropped: 0 (0.0%) · Profile: Default


```
> Frame 1: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface en0, id 0
> Ethernet II, Src: Apple_4b:4c:b4 (b0:be:83:4b:4c:b4), Dst: TaicangT&WEl_c4:f7:d4 (f8:0c:58:c4:f7:d4)
> Internet Protocol Version 4, Src: 192.168.1.92, Dst: 3.108.125.57
v Transmission Control Protocol, Src Port: 59742, Dst Port: 443, Seq: 1, Ack: 1, Len: 54
    Source Port: 59742
    Destination Port: 443
    [Stream index: 0]
  v [Conversation completeness: Incomplete (12)]
      ..0. .... = RST: Absent
      ...0 .... = FIN: Absent
      .... 1... = Data: Present
      .... .1.. = ACK: Present
      .... ..0. = SYN-ACK: Absent
      .... ...0 = SYN: Absent
      [Completeness Flags: ··DA··]
    [TCP Segment Len: 54]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 471303552
```

```
0000  f8 0c 58 c4 f7 d4 b0 be  83 4b 4c b4 08
0010  00 6a 00 00 40 00 40 06  f7 e2 c0 a8 01
0020  7d 39 e9 5e 01 bb 1c 17  85 80 ba 37 50
0030  08 00 72 0c 00 00 01 01  08 0a 44 01 2d
0040  62 20 17 03 03 00 31 d7  76 fd 15 13 e6
0050  48 c4 15 a1 e5 72 5b 6a  89 11 73 9c 17
0060  f9 63 bb 6b 86 07 d6 61  79 5d e4 b1 54
0070  9d 53 4e c4 0c 54 ea 04
```

Transmission Control Protocol: Protocol · Packets: 125 · Displayed: 31 (24.8%) · Dropped: 0 (0.0%) · Profile: Default


```
    Sequence Number (raw): 1371006846
    [Next Sequence Number: 1339    (relative sequence number)]
    Acknowledgment Number: 1069    (relative ack number)
    Acknowledgment number (raw): 298642064
    1000 .... = Header Length: 32 bytes (8)
  v Flags: 0x018 (PSH, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 1... = Push: Set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·····AP···]
    Window: 421
```

```
0040  ea 90 80 18 01 a5 eb b9  00 00 01 01 08
0050  0e 70 d6 6d 4f 48 17 03  03 02 2f 93 15
0060  a9 f2 20 12 eb 94 76 0d  54 ae b5 82 2f
0070  db 0f a9 1d 66 27 fb 89  1c c0 d4 df 9e
0080  86 49 48 ea 11 d5 a3 f7  82 b1 e7 55 9a
0090  85 8f ab eb b8 5e 19 1e  b0 a9 02 2c 6b
00a0  5a 4a 9f bf 13 33 3f c1  72 19 92 d3 11
00b0  03 6f 60 24 a8 90 d7 70  a2 55 1c 6f d8
00c0  c2 b6 4b 95 3b 18 fa 05  6a 02 7b 6a ae
00d0  49 1a c1 66 15 5b 34 01  97 48 be 29 3e
00e0  81 ef bf 65 59 e1 d3 6e  d6 bd 76 51 33
00f0  e9 e9 d1 b8 fd 62 9d d5  ec fb 1e 48 7b
0100  87 a4 4e 25 4c 1e 89 e1  59 26 ef d9 74
0110  cb 65 c6 80 8e 54 7f 8c  5f 2c a1 ce 3f
0120  ef ca e0 19 60 73 12 36  34 74 48 e6 c0
0130  46 aa 3b f1 f8 c7 82 1a  2f a0 0e 9e 8d
0140  b3 8c fd 46 20 7f cc 72  ca c0 5c 46 f5
0150  fa ec a2 1e 24 00 36 da  3f 64 19 3b d9
0160  1b ad 60 49 bc b3 32 ca  f7 e5 63 90 c5
0170  35 f2 ad 11 e5 16 27 95  24 c6 f2 f0 e5
0180  71 ac eb 69 cd aa 6b b6  87 a0 b1 3a b5
```

TCP Flags (tcp.flags.str), 2 bytes · Packets: 125 · Displayed: 31 (24.8%) · Dropped: 0 (0.0%) · Profile: Default

```
    Window: 421
    [Calculated window size: 421]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0xebb9 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ⌄ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    > TCP Option - No-Operation (NOP)
    > TCP Option - No-Operation (NOP)
    > TCP Option - Timestamps: TSval 3168276080, TSecr 3597487944
  ⌄ [Timestamps]
      [Time since first frame in this TCP stream: 0.147355000 seconds]
      [Time since previous frame in this TCP stream: 0.000001000 seconds]
  ⌄ [SEQ/ACK analysis]
      [Bytes in flight: 632]
      [Bytes sent since last PSH flag: 564]
    TCP payload (564 bytes)
⌄ Transport Layer Security
```

```
0040  ea 90 80 18 01 a5 eb b9  00 00 01 01 08
0050  0e 70 d6 6d 4f 48 17 03  03 02 2f 93 15
0060  a9 f2 20 12 eb 94 76 0d  54 ae b5 82 23
0070  db 0f a9 1d 66 27 fb 89  1c c0 d4 df 94
0080  86 49 48 ea 11 d5 a3 f7  82 b1 e7 55 9a
0090  85 8f ab eb b8 5e 19 1e  b0 a9 02 2c 67
00a0  5a 4a 9f bf 13 33 3f c1  72 19 92 d3 11
00b0  03 6f 60 24 a8 90 d7 70  a2 55 1c 6f db
00c0  c2 b6 4b 95 3b 18 fa 05  6a 02 7b 6a ae
00d0  49 1a c1 66 15 5b 34 01  97 48 be 29 3d
00e0  81 ef bf 65 59 e1 d3 6e  d6 bd 76 51 33
00f0  e9 e9 d1 b8 fd 62 9d d5  ec fb 1e 48 7b
0100  87 a4 4e 25 4c 1e 89 e1  59 26 ef d9 74
0110  cb 65 c6 80 8e 54 7f 8c  5f 2c a1 ce 31
0120  ef ca e0 19 60 73 12 36  34 74 48 e6 cc
0130  46 aa 3b f1 f8 c7 82 1a  2f a0 0e 9e 84
0140  b3 8c fd 46 20 7f cc 72  ca c0 5c 46 f5
0150  fa ec a2 1e 24 00 36 da  3f 64 19 3b d9
0160  1b ad 60 49 bc b3 32 ca  f7 e5 63 90 c5
0170  35 f2 ad 11 e5 16 27 95  24 c6 f2 f0 e5
0180  71 ac eb 69 cd aa 6b b6  87 a0 b1 3a b3
```

TCP Flags (tcp.flags.str), 2 bytes · Packets: 125 · Displayed: 31 (24.8%) · Dropped: 0 (0.0%) · Profile: Default