How many bytes in TCP header? its different fields? how are values set? verify in wireshark.

Answer:

The TCP (Transmission Control Protocol) header is typically 20 bytes long, but it can be longer if options are used. The standard fields in a TCP header are as follows:

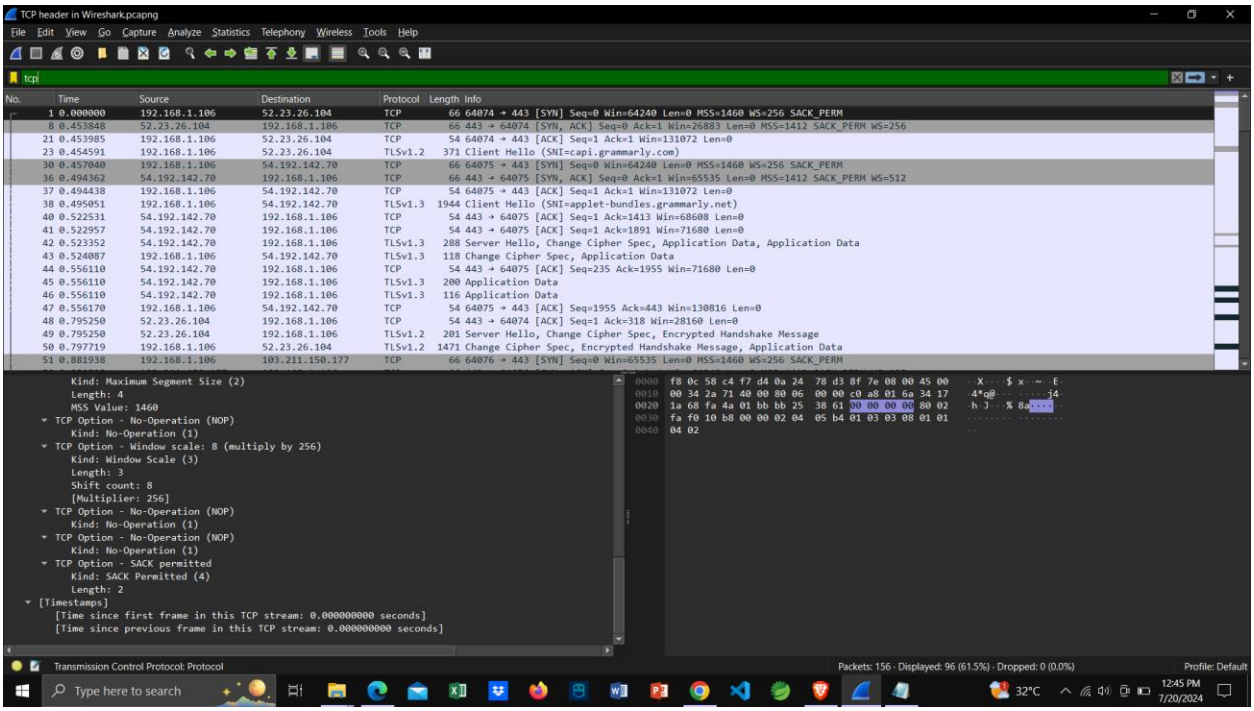
1. **Source Port (16 bits)**: Identifies the sending port.
2. **Destination Port (16 bits)**: Identifies the receiving port.
3. **Sequence Number (32 bits)**: Used for data ordering.
4. **Acknowledgment Number (32 bits)**: Indicates the next expected byte.
5. **Data Offset (4 bits)**: Specifies the size of the TCP header.
6. **Reserved (3 bits)**: Reserved for future use and should be set to zero.
7. **Flags (9 bits)**: Control flags (NS, CWR, ECE, URG, ACK, PSH, RST, SYN, FIN).
8. **Window Size (16 bits)**: Specifies the size of the sender's receive window.
9. **Checksum (16 bits)**: Used for error-checking the header and data.
10. **Urgent Pointer (16 bits)**: Indicates the end of urgent data.
11. **Options (variable length)**: Optional settings for TCP.

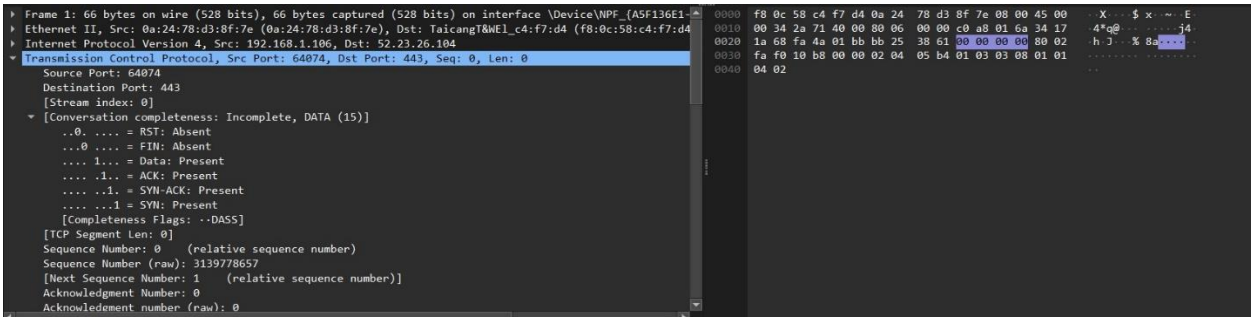
Values Setting:

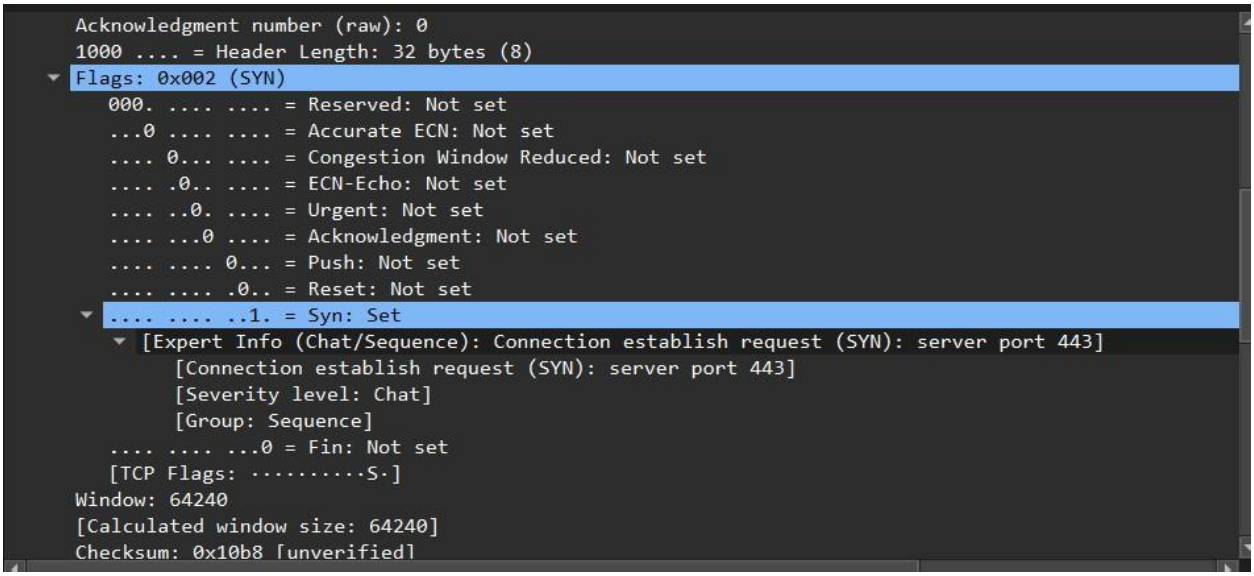
- **Source and Destination Port**: Set by the sending and receiving applications, respectively.

- **Sequence and Acknowledgment Numbers**: Used to ensure data is delivered in order and without duplicates.
- **Data Offset**: Indicates where the data begins in the TCP segment.
- **Flags**: Set based on the required control information (e.g., SYN for connection establishment).
- **Window Size**: Determines how much data can be sent before an acknowledgment is received.
- **Checksum**: Calculated by the sender and verified by the receiver.
- **Urgent Pointer**: Used if the URG flag is set.
- **Options**: Used for various extensions (e.g., Maximum Segment Size, Window Scaling).

I started Wireshark and captured packets on my network interface and found folllowing results:


TCP header in Wireshark.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.1.106 52.23.26.104 TCP 66 64074 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
8 0.453848 52.23.26.104 192.168.1.106 TCP 66 443 → 64074 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1412 SACK_PERM WS=256
21 0.453985 192.168.1.106 52.23.26.104 TCP 54 64074 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
23 0.454591 192.168.1.106 52.23.26.104 TLSv1.2 371 Client Hello (SNI=capi.grammarly.com)
30 0.457040 192.168.1.106 54.192.142.70 TCP 66 64075 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
36 0.494362 54.192.142.70 192.168.1.106 TCP 66 443 → 64075 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=512
37 0.494438 192.168.1.106 54.192.142.70 TCP 54 64075 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
38 0.495051 192.168.1.106 54.192.142.70 TLSv1.3 1944 Client Hello (SNI=applet-bundles.grammarly.net)
40 0.522531 54.192.142.70 192.168.1.106 TCP 54 443 → 64075 [ACK] Seq=1 Ack=1413 Win=68608 Len=0
41 0.522957 54.192.142.70 192.168.1.106 TCP 54 443 → 64075 [ACK] Seq=1 Ack=1891 Win=71680 Len=0
42 0.523352 54.192.142.70 192.168.1.106 TLSv1.3 288 Server Hello, Change Cipher Spec, Application Data, Application Data
43 0.524087 192.168.1.106 54.192.142.70 TLSv1.3 118 Change Cipher Spec, Application Data
44 0.556110 54.192.142.70 192.168.1.106 TCP 54 443 → 64075 [ACK] Seq=235 Ack=1955 Win=71680 Len=0
45 0.556110 54.192.142.70 192.168.1.106 TLSv1.3 200 Application Data
46 0.556110 54.192.142.70 192.168.1.106 TLSv1.3 116 Application Data
47 0.556170 192.168.1.106 54.192.142.70 TCP 54 64075 → 443 [ACK] Seq=1955 Ack=443 Win=130816 Len=0
48 0.795250 52.23.26.104 192.168.1.106 TCP 54 443 → 64074 [ACK] Seq=1 Ack=318 Win=28160 Len=0
49 0.795250 52.23.26.104 192.168.1.106 TLSv1.2 201 Server Hello, Change Cipher Spec, Encrypted Handshake Message
50 0.797719 192.168.1.106 52.23.26.104 TLSv1.2 1471 Change Cipher Spec, Encrypted Handshake Message, Application Data
51 0.881938 192.168.1.106 103.211.150.177 TCP 66 64076 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
Kind: Maximum Segment Size (2)
Length: 4
MSS Value: 1460
TCP Option - No-Operation (NOP)
Kind: No-Operation (1)
TCP Option - Window scale: 8 (multiply by 256)
Kind: Window Scale (3)
Length: 3
Shift count: 8
[Multiplier: 256]
TCP Option - No-Operation (NOP)
Kind: No-Operation (1)
TCP Option - No-Operation (NOP)
Kind: No-Operation (1)
TCP Option - SACK permitted
Kind: SACK Permitted (4)
Length: 2
[Timestamps]
[Time since first frame in this TCP stream: 0.000000000 seconds]
[Time since previous frame in this TCP stream: 0.000000000 seconds]
0000 f8 0c 58 c4 f7 d4 0a 24 78 d3 8f 7e 08 00 45 00
0010 00 34 2a 71 40 00 80 06 00 00 c0 a8 01 6a 34 17
0020 1a 68 fa 4a 01 bb bb 25 38 61 00 00 00 00 80 02
0030 fa f0 10 b8 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02
Transmission Control Protocol: Protocol
Packets: 156 · Displayed: 96 (61.5%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
32°C
12:45 PM
7/20/2024


Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A5F136E1-
Ethernet II, Src: 0a:24:78:d3:8f:7e (0a:24:78:d3:8f:7e), Dst: TaicangT&WEl_c4:f7:d4 (f8:0c:58:c4:f7:d4
Internet Protocol Version 4, Src: 192.168.1.106, Dst: 52.23.26.104
Transmission Control Protocol, Src Port: 64074, Dst Port: 443, Seq: 0, Len: 0
Source Port: 64074
Destination Port: 443
[Stream index: 0]
[Conversation completeness: Incomplete, DATA (15)]
..0. .... = RST: Absent
...0 .... = FIN: Absent
.... 1... = Data: Present
.... .1.. = ACK: Present
.... ..1. = SYN-ACK: Present
....1 = SYN: Present
[Completeness Flags: ··DASS]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 3139778657
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
0000 f8 0c 58 c4 f7 d4 0a 24 78 d3 8f 7e 08 00 45 00
0010 00 34 2a 71 40 00 80 06 00 00 c0 a8 01 6a 34 17
0020 1a 68 fa 4a 01 bb bb 25 38 61 00 00 00 00 80 02
0030 fa f0 10 b8 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02


Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....1. = Syn: Set
[Expert Info (Chat/Sequence): Connection establish request (SYN): server port 443]
[Connection establish request (SYN): server port 443]
[Severity level: Chat]
[Group: Sequence]
....0 = Fin: Not set
[TCP Flags: ··········S·]
Window: 64240
[Calculated window size: 64240]
Checksum: 0x10b8 [unverified]

```
Window: 64240
[Calculated window size: 64240]
Checksum: 0x10b8 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
▾ Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No
  ▾ TCP Option - Maximum segment size: 1460 bytes
      Kind: Maximum Segment Size (2)
      Length: 4
      MSS Value: 1460
  ▾ TCP Option - No-Operation (NOP)
      Kind: No-Operation (1)
  ▾ TCP Option - Window scale: 8 (multiply by 256)
      Kind: Window Scale (3)
      Length: 3
      Shift count: 8
      [Multiplier: 256]
  ▾ TCP Option - No-Operation (NOP)
      Kind: No-Operation (1)
  ▾ TCP Option - No-Operation (NOP)
      Kind: No-Operation (1)
```

```
      Kind: Maximum Segment Size (2)
      Length: 4
      MSS Value: 1460
  ▾ TCP Option - No-Operation (NOP)
      Kind: No-Operation (1)
  ▾ TCP Option - Window scale: 8 (multiply by 256)
      Kind: Window Scale (3)
      Length: 3
      Shift count: 8
      [Multiplier: 256]
  ▾ TCP Option - No-Operation (NOP)
      Kind: No-Operation (1)
  ▾ TCP Option - No-Operation (NOP)
      Kind: No-Operation (1)
  ▾ TCP Option - SACK permitted
      Kind: SACK Permitted (4)
      Length: 2
▾ [Timestamps]
    [Time since first frame in this TCP stream: 0.000000000 seconds]
    [Time since previous frame in this TCP stream: 0.000000000 seconds]
```