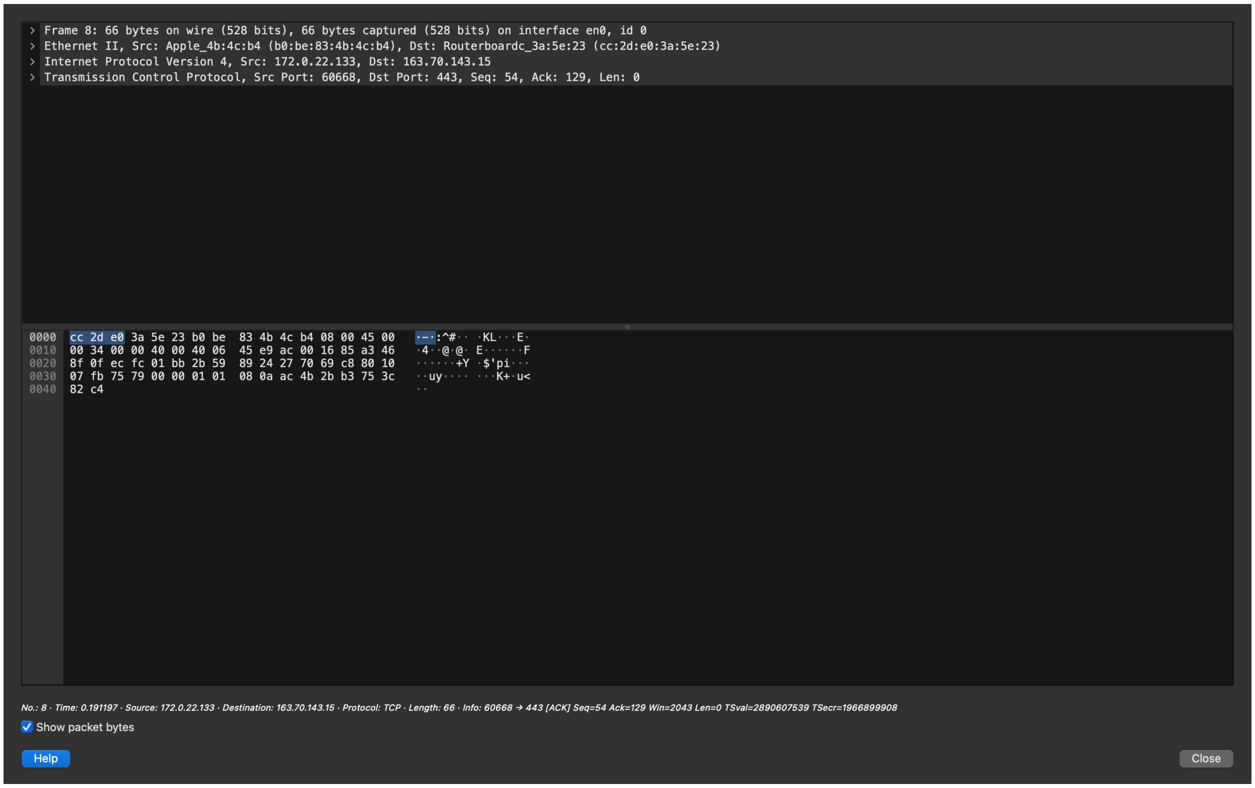
IP packet analysis

a) Packet capture



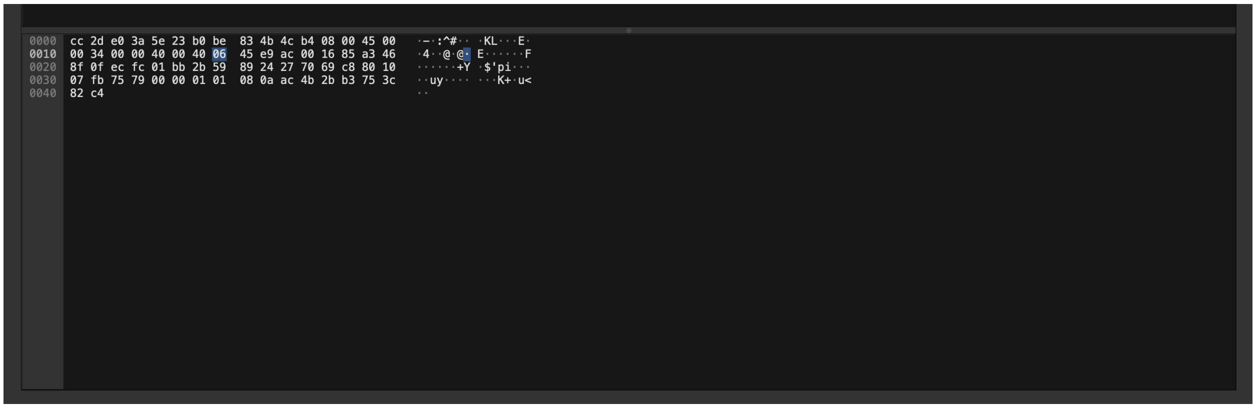
```
> Frame 8: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0
> Ethernet II, Src: Apple_4b:4c:b4 (b0:be:83:4b:4c:b4), Dst: Routerboardc_3a:5e:23 (cc:2d:e0:3a:5e:23)
> Internet Protocol Version 4, Src: 172.0.22.133, Dst: 163.70.143.15
> Transmission Control Protocol, Src Port: 60668, Dst Port: 443, Seq: 54, Ack: 129, Len: 0
```

```
0000  cc 2d e0 3a 5e 23 b0 be  83 4b 4c b4 08 00 45 00   ·-·:^#·· ·KL···E·
0010  00 34 00 00 40 00 40 06  45 e9 ac 00 16 85 a3 46   ·4··@·@· E······F
0020  8f 0f ec fc 01 bb 2b 59  89 24 27 70 69 c8 80 10   ······+Y ·$'pi···
0030  07 fb 75 79 00 00 01 01  08 0a ac 4b 2b b3 75 3c   ··uy···· ···K+·u<
0040  82 c4                                              ··
```

No.: 8 · Time: 0.191197 · Source: 172.0.22.133 · Destination: 163.70.143.15 · Protocol: TCP · Length: 66 · Info: 60668 → 443 [ACK] Seq=54 Ack=129 Win=2043 Len=0 TSval=2890607539 TSecr=1966899908

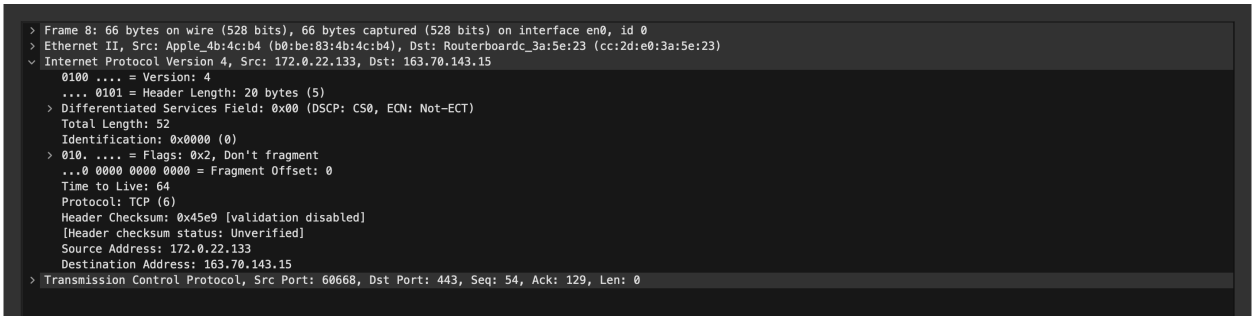
☑ Show packet bytes

b) Hexadecimal data



```
0000  cc 2d e0 3a 5e 23 b0 be  83 4b 4c b4 08 00 45 00   ·-·:^#·· ·KL···E·
0010  00 34 00 00 40 00 40 06  45 e9 ac 00 16 85 a3 46   ·4··@·@· E······F
0020  8f 0f ec fc 01 bb 2b 59  89 24 27 70 69 c8 80 10   ······+Y ·$'pi···
0030  07 fb 75 79 00 00 01 01  08 0a ac 4b 2b b3 75 3c   ··uy···· ···K+·u<
0040  82 c4                                              ··
```

c) IP header



```
> Frame 8: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0
> Ethernet II, Src: Apple_4b:4c:b4 (b0:be:83:4b:4c:b4), Dst: Routerboardc_3a:5e:23 (cc:2d:e0:3a:5e:23)
v Internet Protocol Version 4, Src: 172.0.22.133, Dst: 163.70.143.15
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x45e9 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.0.22.133
    Destination Address: 163.70.143.15
> Transmission Control Protocol, Src Port: 60668, Dst Port: 443, Seq: 54, Ack: 129, Len: 0
```

Here's the IP header fields explanation:

a) Version (4)

the IP version

b) Header Length (20 bytes)

length of IP header

c) Type of service (TOS) 0x00

indicates the quality of services

d) Total length (52 bytes)

the total length of IP packet (header + data)

e) Identification (0x0000)

sequential number that uniquely identifies the packet for reassembly if fragmentation occurs

f) Flags (0x2)

control or identity fragments

g) Fragment offset (0)

position of the fragment in the original packet

h) Time to live (64)

the maximum time the packet is allowed to remain in the network

i) Protocol : TCP (6)

protocol used in data portion of the packet

j) Header checksum (0x45e9)

error checking for the header

k) Source IP address (172.0.22.133)

l) Destination IP address (163.70.143.15)