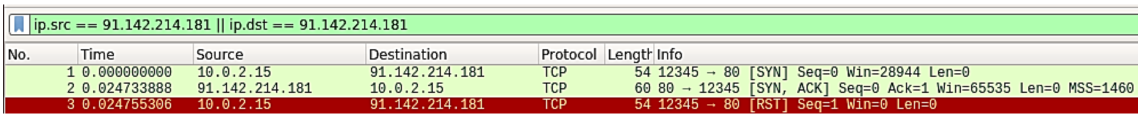
https://inc0x0.com/tcp-ip-packets-introduction/tcp-ip-packets-3-manually-create-and-send-raw-tcp-ip-packets/

Crea un paquete TCP SYN que vaya a 91.142.214.181, escucha con Wireshark y observa si obtienes la respuesta.

1-Crea un pantallazo de lo mostrado en Wireshark

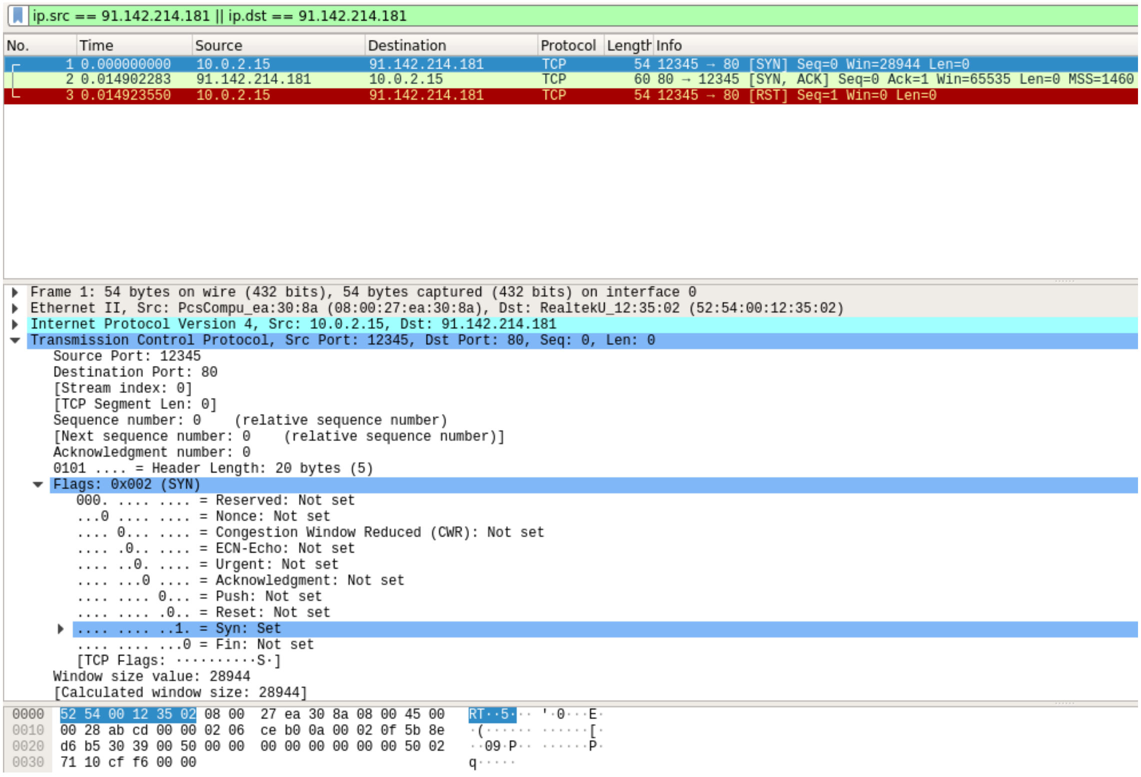


```
ip.src == 91.142.214.181 || ip.dst == 91.142.214.181

No.   Time          Source            Destination       Protocol Length Info
    1 0.000000000   10.0.2.15         91.142.214.181    TCP          54 12345 → 80 [SYN] Seq=0 Win=28944 Len=0
    2 0.024733888   91.142.214.181    10.0.2.15         TCP          60 80 → 12345 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
    3 0.024755306   10.0.2.15         91.142.214.181    TCP          54 12345 → 80 [RST] Seq=1 Win=0 Len=0
```

2- ¿Qué flags tiene "encendidos" tu paquete?, ¿y el de vuelta?

Ida:



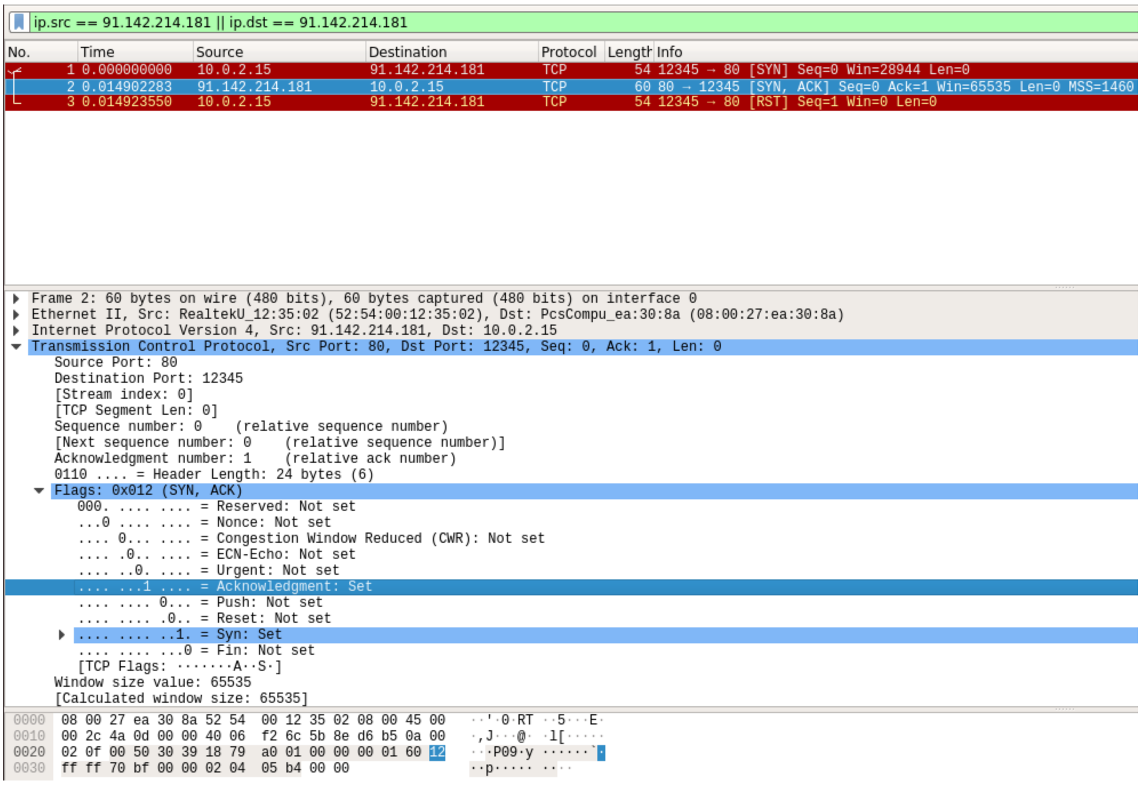
```
ip.src == 91.142.214.181 || ip.dst == 91.142.214.181

No.   Time          Source            Destination       Protocol Length Info
    1 0.000000000   10.0.2.15         91.142.214.181    TCP          54 12345 → 80 [SYN] Seq=0 Win=28944 Len=0
    2 0.014902283   91.142.214.181    10.0.2.15         TCP          60 80 → 12345 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
    3 0.014923550   10.0.2.15         91.142.214.181    TCP          54 12345 → 80 [RST] Seq=1 Win=0 Len=0
```

```
▶ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
▶ Ethernet II, Src: PcsCompu_ea:30:8a (08:00:27:ea:30:8a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 91.142.214.181
▼ Transmission Control Protocol, Src Port: 12345, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 12345
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    0101 .... = Header Length: 20 bytes (5)
  ▼ Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): 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
      .... .... ...0 = Fin: Not set
      [TCP Flags: ··········S·]
    Window size value: 28944
    [Calculated window size: 28944]
```

```
0000  52 54 00 12 35 02 08 00  27 ea 30 8a 08 00 45 00   RT··5··· '·0···E·
0010  00 28 ab cd 00 00 02 06  ce b0 0a 00 02 0f 5b 8e   ·(······ ······[·
0020  d6 b5 30 39 00 50 00 00  00 00 00 00 00 00 50 02   ··09·P·· ······P·
0030  71 10 cf f6 00 00                                  q·····
```

Vuelta:



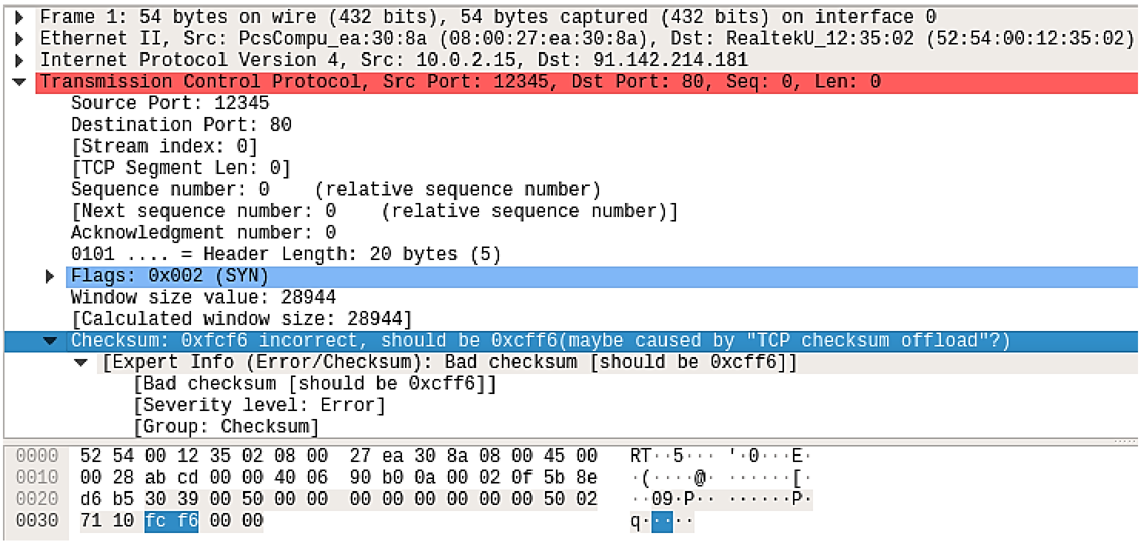
```
ip.src == 91.142.214.181 || ip.dst == 91.142.214.181

No.  Time         Source          Destination     Protocol Length Info
   1 0.000000000  10.0.2.15       91.142.214.181  TCP      54 12345 → 80 [SYN] Seq=0 Win=28944 Len=0
   2 0.014902283  91.142.214.181  10.0.2.15       TCP      60 80 → 12345 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
   3 0.014923550  10.0.2.15       91.142.214.181  TCP      54 12345 → 80 [RST] Seq=1 Win=0 Len=0

▶ Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▶ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_ea:30:8a (08:00:27:ea:30:8a)
▶ Internet Protocol Version 4, Src: 91.142.214.181, Dst: 10.0.2.15
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 12345, Seq: 0, Ack: 1, Len: 0
     Source Port: 80
     Destination Port: 12345
     [Stream index: 0]
     [TCP Segment Len: 0]
     Sequence number: 0    (relative sequence number)
     [Next sequence number: 0    (relative sequence number)]
     Acknowledgment number: 1    (relative ack number)
     0110 .... = Header Length: 24 bytes (6)
   ▼ Flags: 0x012 (SYN, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
      ▶ .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······A··S·]
     Window size value: 65535
     [Calculated window size: 65535]

0000  08 00 27 ea 30 8a 52 54  00 12 35 02 08 00 45 00   ··'·0·RT ··5···E·
0010  00 2c 4a 0d 00 00 40 06  f2 6c 5b 8e d6 b5 0a 00   ·,J···@· ·l[·····
0020  02 0f 00 50 30 39 18 79  a0 01 00 00 00 01 60 12   ···P09·y ······`·
0030  ff ff 70 bf 00 00 02 04  05 b4 00 00               ··p····· ····
```

3-Pon mal el checksum y observa qué pasa

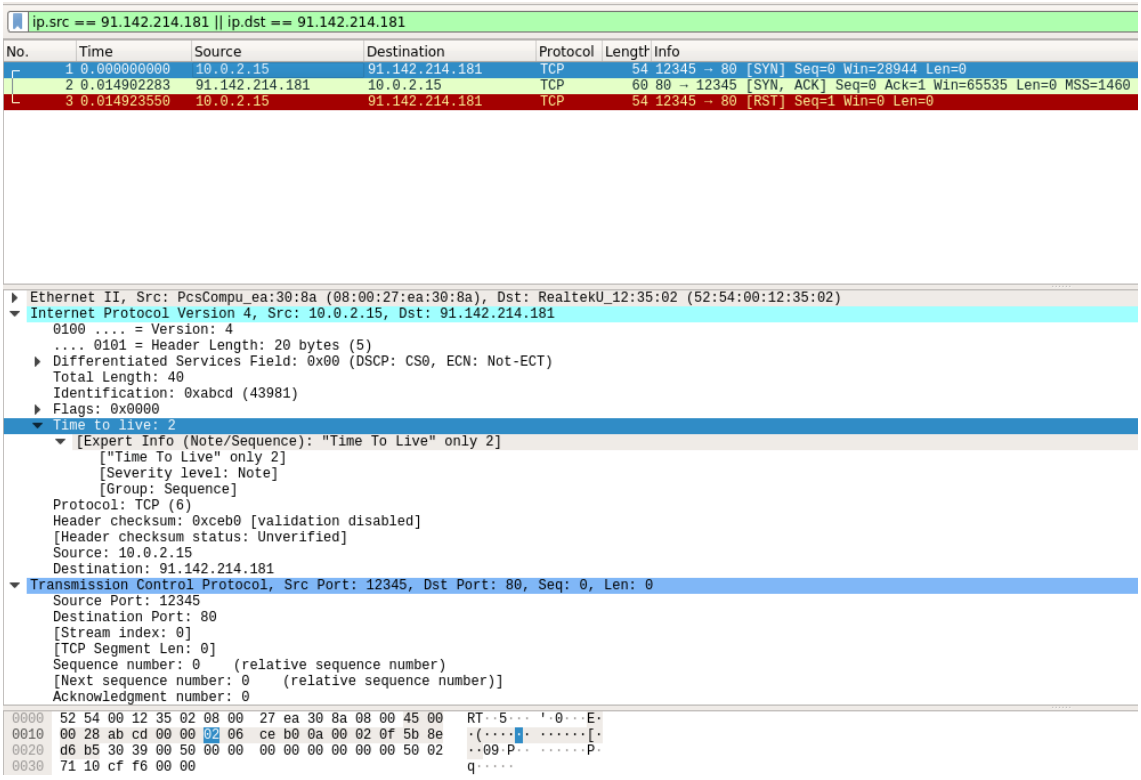


```
▶ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
▶ Ethernet II, Src: PcsCompu_ea:30:8a (08:00:27:ea:30:8a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 91.142.214.181
▼ Transmission Control Protocol, Src Port: 12345, Dst Port: 80, Seq: 0, Len: 0
     Source Port: 12345
     Destination Port: 80
     [Stream index: 0]
     [TCP Segment Len: 0]
     Sequence number: 0    (relative sequence number)
     [Next sequence number: 0    (relative sequence number)]
     Acknowledgment number: 0
     0101 .... = Header Length: 20 bytes (5)
   ▶ Flags: 0x002 (SYN)
     Window size value: 28944
     [Calculated window size: 28944]
   ▼ Checksum: 0xfcf6 incorrect, should be 0xcff6(maybe caused by "TCP checksum offload"?)
      ▼ [Expert Info (Error/Checksum): Bad checksum [should be 0xcff6]]
           [Bad checksum [should be 0xcff6]]
           [Severity level: Error]
           [Group: Checksum]

0000  52 54 00 12 35 02 08 00  27 ea 30 8a 08 00 45 00   RT··5··· '·0···E·
0010  00 28 ab cd 00 00 40 06  90 b0 0a 00 02 0f 5b 8e   ·(····@· ······[·
0020  d6 b5 30 39 00 50 00 00  00 00 00 00 00 00 50 02   ··09·P·· ······P·
0030  71 10 fc f6 00 00                                  q·····
```

El wireshark te dice el ckecksum que debería tener

4-Pon un TTL=2 y observa qué pasa



```
ip.src == 91.142.214.181 || ip.dst == 91.142.214.181
```

```
No.    Time         Source          Destination     Protocol Length Info
     1 0.000000000  10.0.2.15       91.142.214.181  TCP          54 12345 → 80 [SYN] Seq=0 Win=28944 Len=0
     2 0.014902283  91.142.214.181  10.0.2.15       TCP          60 80 → 12345 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
     3 0.014923550  10.0.2.15       91.142.214.181  TCP          54 12345 → 80 [RST] Seq=1 Win=0 Len=0
```

```
▸ Ethernet II, Src: PcsCompu_ea:30:8a (08:00:27:ea:30:8a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 91.142.214.181
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0xabcd (43981)
  ▸ Flags: 0x0000
  ▾ Time to live: 2
    ▾ [Expert Info (Note/Sequence): "Time To Live" only 2]
          ["Time To Live" only 2]
          [Severity level: Note]
          [Group: Sequence]
    Protocol: TCP (6)
    Header checksum: 0xceb0 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.15
    Destination: 91.142.214.181
▾ Transmission Control Protocol, Src Port: 12345, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 12345
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
```

```
0000  52 54 00 12 35 02 08 00  27 ea 30 8a 08 00 45 00   RT··5··· '·0···E·
0010  00 28 ab cd 00 00 02 06  ce b0 0a 00 02 0f 5b 8e   ·(······ ······[·
0020  d6 b5 30 39 00 50 00 00  00 00 00 00 00 00 50 02   ··09·P·· ······P·
0030  71 10 cf f6 00 00                                  q·····
```