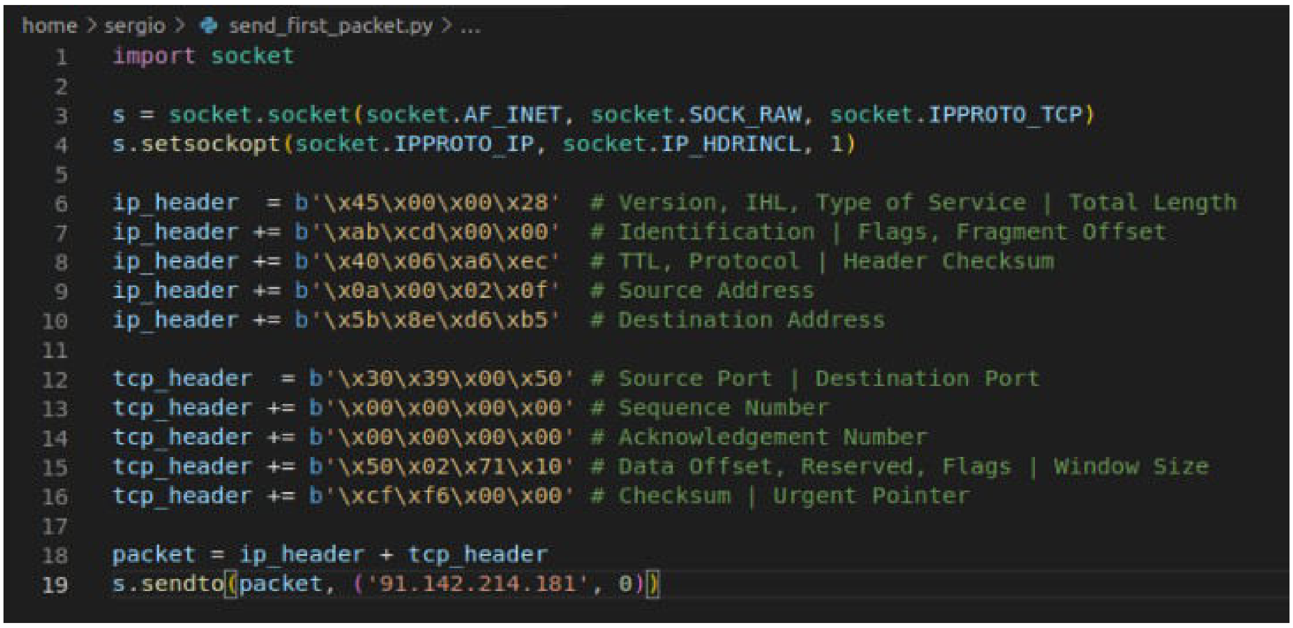
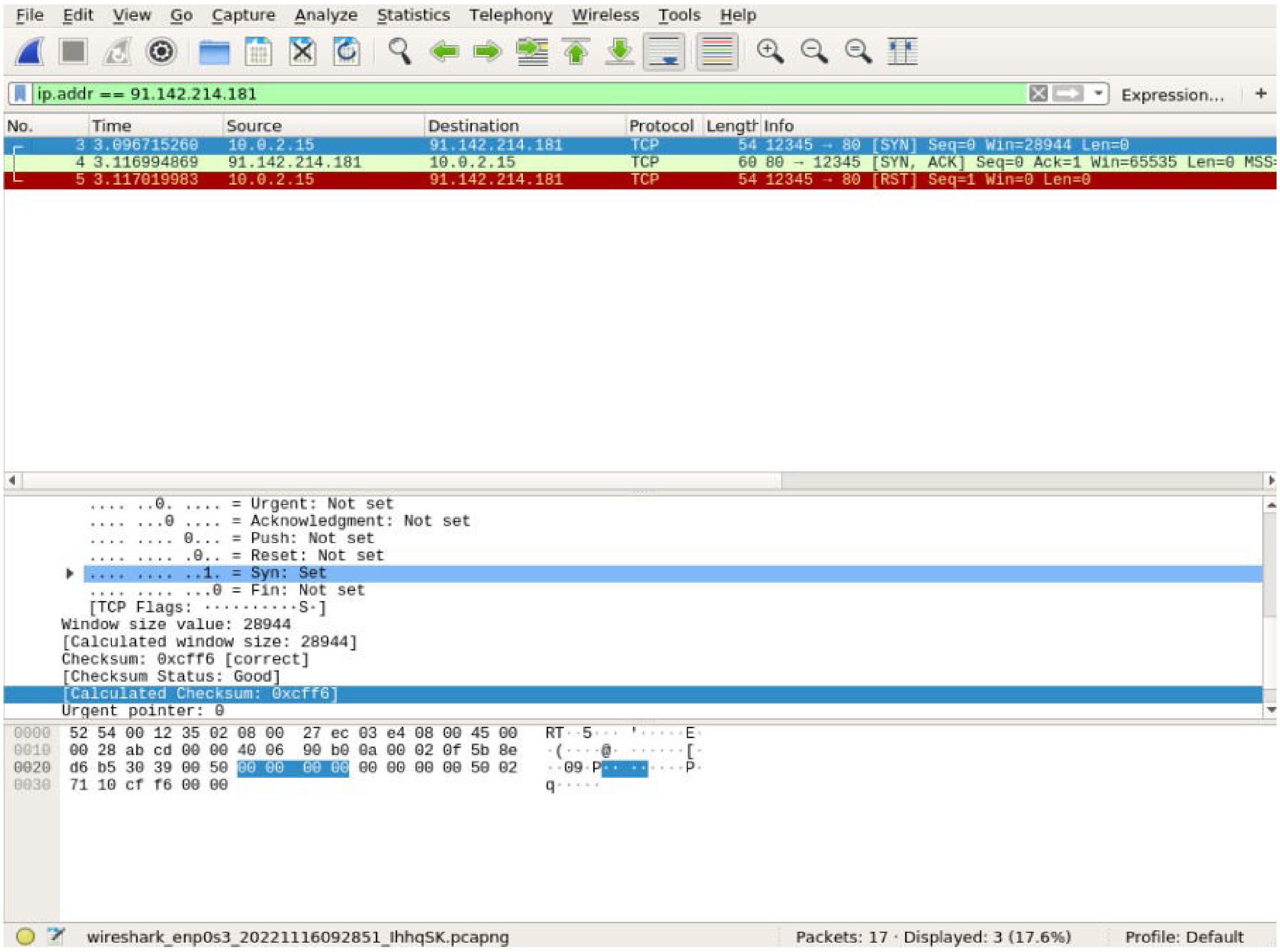
Creación manual de paquete TCP/IP

1-Crea un pantallazo de lo mostrado en Wireshark



home > sergio > send_first_packet.py > ...

```python
import socket

s = socket.socket(socket.AF_INET, socket.SOCK_RAW, socket.IPPROTO_TCP)
s.setsockopt(socket.IPPROTO_IP, socket.IP_HDRINCL, 1)

ip_header  = b'\x45\x00\x00\x28'  # Version, IHL, Type of Service | Total Length
ip_header += b'\xab\xcd\x00\x00'  # Identification | Flags, Fragment Offset
ip_header += b'\x40\x06\xa6\xec'  # TTL, Protocol | Header Checksum
ip_header += b'\x0a\x00\x02\x0f'  # Source Address
ip_header += b'\x5b\x8e\xd6\xb5'  # Destination Address

tcp_header  = b'\x30\x39\x00\x50' # Source Port | Destination Port
tcp_header += b'\x00\x00\x00\x00' # Sequence Number
tcp_header += b'\x00\x00\x00\x00' # Acknowledgement Number
tcp_header += b'\x50\x02\x71\x10' # Data Offset, Reserved, Flags | Window Size
tcp_header += b'\xcf\xf6\x00\x00' # Checksum | Urgent Pointer

packet = ip_header + tcp_header
s.sendto(packet, ('91.142.214.181', 0))
```



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

ip.addr == 91.142.214.181

```
No.   Time          Source           Destination      Protocol Length Info
    3 3.096715260   10.0.2.15        91.142.214.181   TCP        54 12345 → 80 [SYN] Seq=0 Win=28944 Len=0
    4 3.116994869   91.142.214.181   10.0.2.15        TCP        60 80 → 12345 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
    5 3.117019983   10.0.2.15        91.142.214.181   TCP        54 12345 → 80 [RST] Seq=1 Win=0 Len=0
```

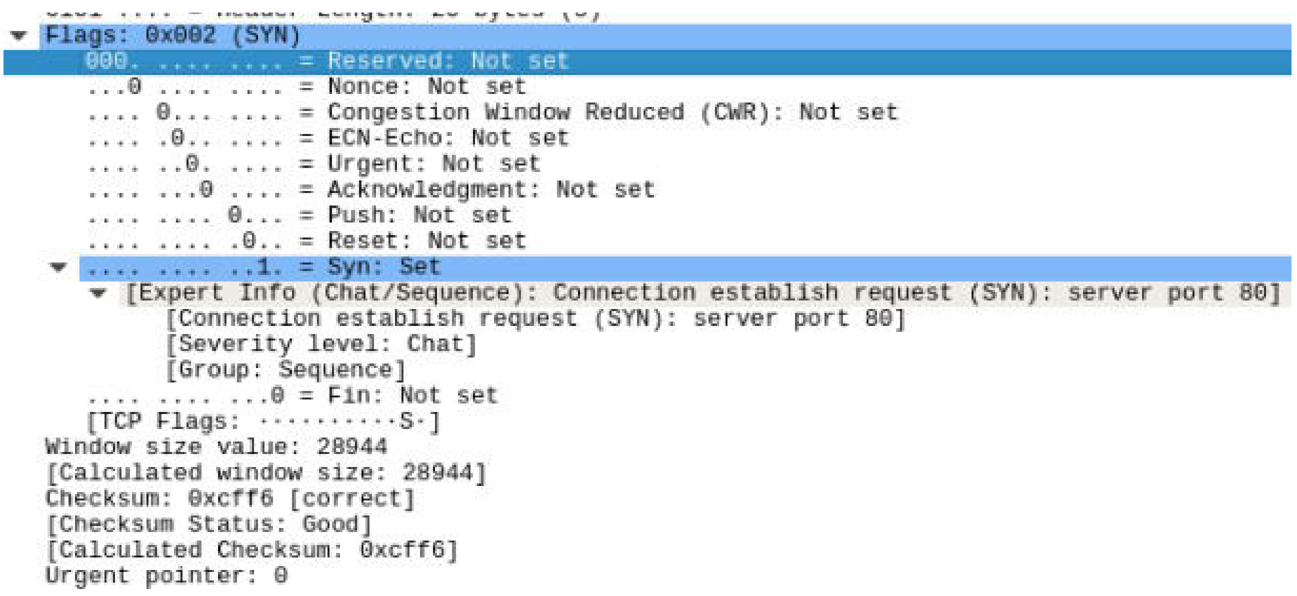
```
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    ▸ .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ··········S·]
  Window size value: 28944
  [Calculated window size: 28944]
  Checksum: 0xcff6 [correct]
  [Checksum Status: Good]
  [Calculated Checksum: 0xcff6]
  Urgent pointer: 0
```

```
0000  52 54 00 12 35 02 08 00  27 ec 03 e4 08 00 45 00   RT··5···'·····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 cf f6 00 00                                  q·····
```

wireshark_enp0s3_20221116092851_IhhqSK.pcapng   Packets: 17 · Displayed: 3 (17.6%)   Profile: Default

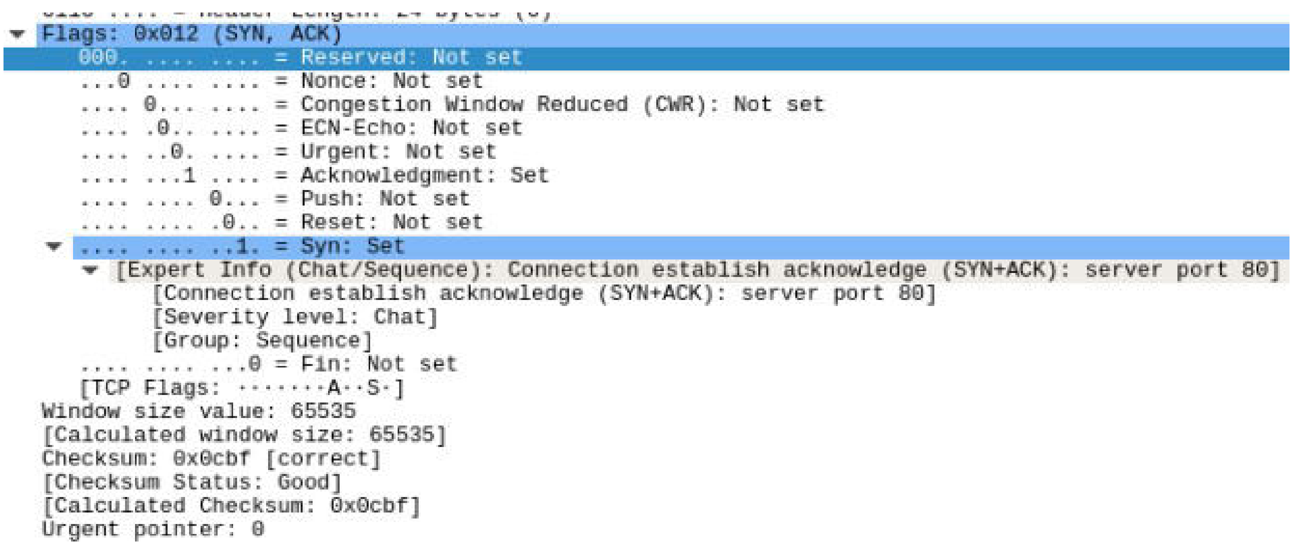
2-¿Qué flags tiene "encendidos" tu paquete?, ¿y el de vuelta?

Paquete de ida:



```
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
        [Expert Info (Chat/Sequence): Connection establish request (SYN): server port 80]
            [Connection establish request (SYN): server port 80]
            [Severity level: Chat]
            [Group: Sequence]
    .... .... ...0 = Fin: Not set
    [TCP Flags: ··········S·]
Window size value: 28944
[Calculated window size: 28944]
Checksum: 0xcff6 [correct]
[Checksum Status: Good]
[Calculated Checksum: 0xcff6]
Urgent pointer: 0
```

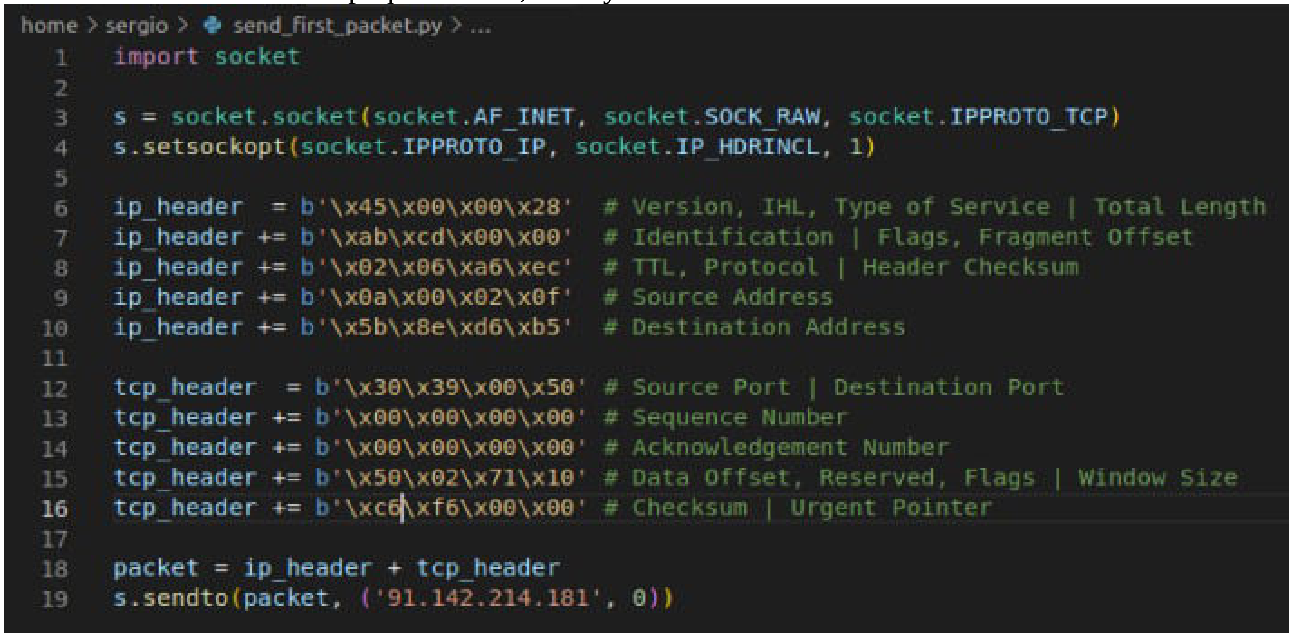
Paquete de vuelta:



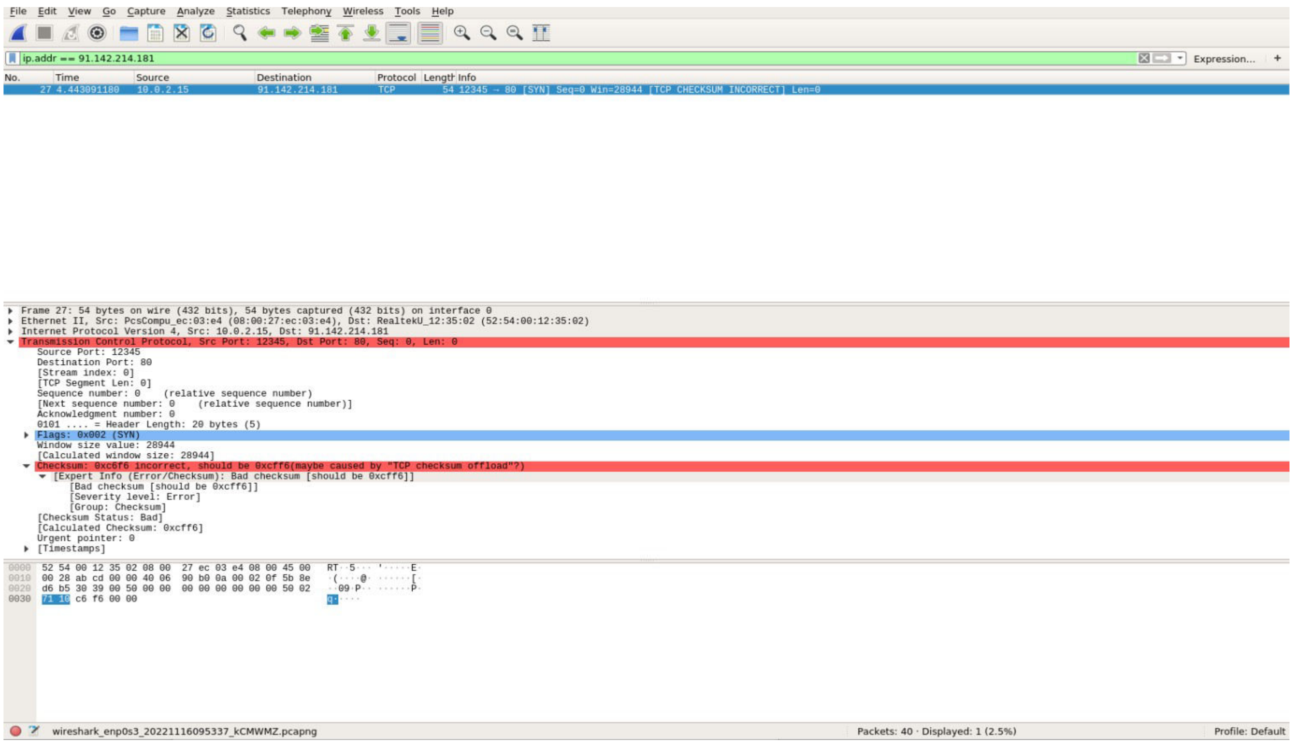
```
Flags: 0x012 (SYN, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..1. = Syn: Set
        [Expert Info (Chat/Sequence): Connection establish acknowledge (SYN+ACK): server port 80]
            [Connection establish acknowledge (SYN+ACK): server port 80]
            [Severity level: Chat]
            [Group: Sequence]
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·······A··S·]
Window size value: 65535
[Calculated window size: 65535]
Checksum: 0x0cbf [correct]
[Checksum Status: Good]
[Calculated Checksum: 0x0cbf]
Urgent pointer: 0
```

3-Pon mal el checksum y observa qué pasa

El servidor no devuelve el paquete SYN,ACK y wireshark nos avisa de un error con el checksum:



```python
import socket

s = socket.socket(socket.AF_INET, socket.SOCK_RAW, socket.IPPROTO_TCP)
s.setsockopt(socket.IPPROTO_IP, socket.IP_HDRINCL, 1)

ip_header  = b'\x45\x00\x00\x28'  # Version, IHL, Type of Service | Total Length
ip_header += b'\xab\xcd\x00\x00'  # Identification | Flags, Fragment Offset
ip_header += b'\x02\x06\xa6\xec'  # TTL, Protocol | Header Checksum
ip_header += b'\x0a\x00\x02\x0f'  # Source Address
ip_header += b'\x5b\x8e\xd6\xb5'  # Destination Address

tcp_header  = b'\x30\x39\x00\x50' # Source Port | Destination Port
tcp_header += b'\x00\x00\x00\x00' # Sequence Number
tcp_header += b'\x00\x00\x00\x00' # Acknowledgement Number
tcp_header += b'\x50\x02\x71\x10' # Data Offset, Reserved, Flags | Window Size
tcp_header += b'\xc6\xf6\x00\x00' # Checksum | Urgent Pointer

packet = ip_header + tcp_header
s.sendto(packet, ('91.142.214.181', 0))
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression... +

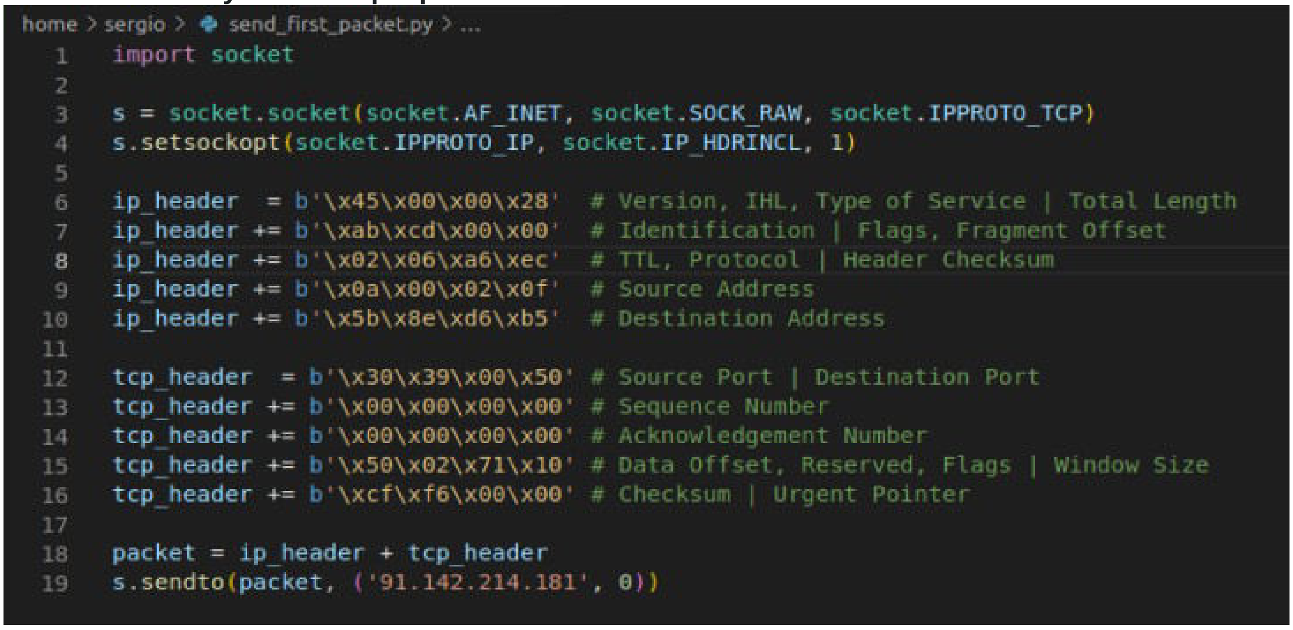
```
ip.addr == 91.142.214.181

No.    Time          Source       Destination      Protocol Length Info
    27 4.443091180   10.0.2.15    91.142.214.181   TCP         54 12345 → 80 [SYN] Seq=0 Win=28944 [TCP CHECKSUM INCORRECT] Len=0
```

```
▸ Frame 27: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_ec:03:e4 (08:00:27:ec:03:e4), 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: 0xc6f6 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]
    [Checksum Status: Bad]
    [Calculated Checksum: 0xcff6]
    Urgent pointer: 0
  ▸ [Timestamps]
```

```
0000  52 54 00 12 35 02 08 00  27 ec 03 e4 08 00 45 00   RT··5···'·····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 c6 f6 00 00                                  q·····
```

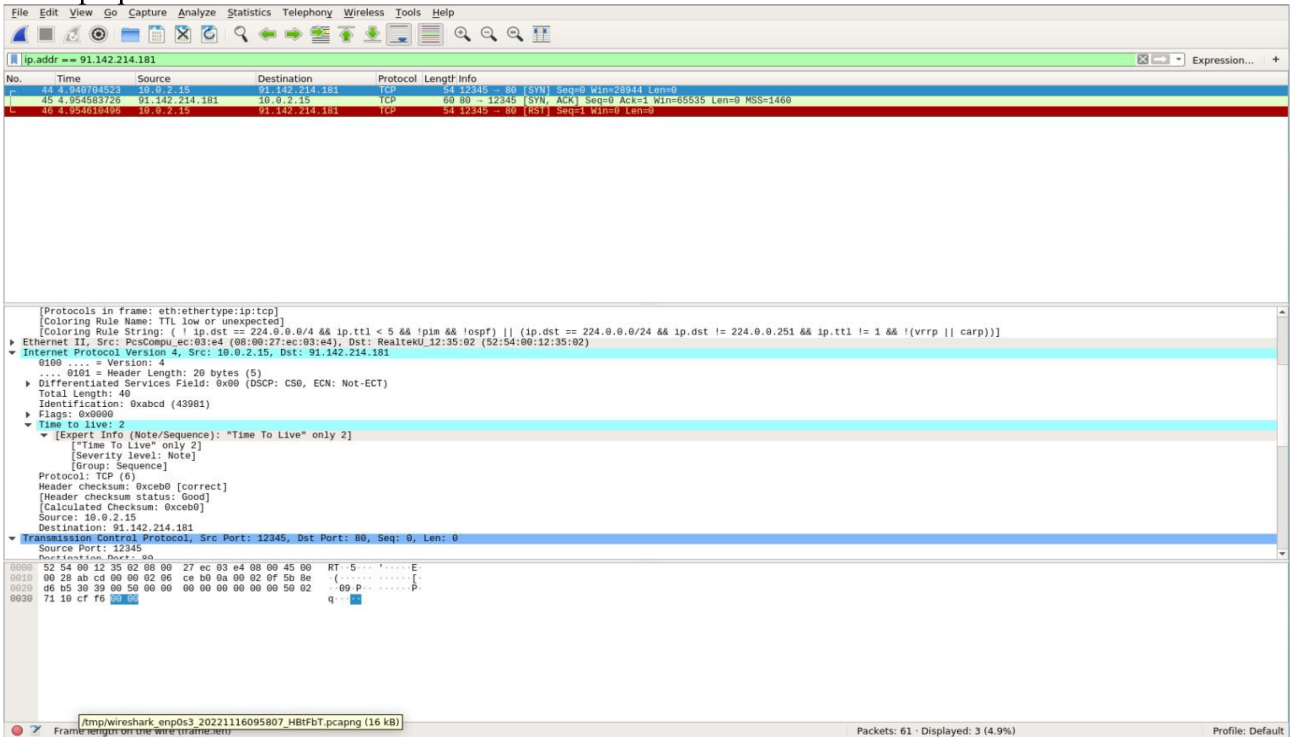
```
wireshark_enp0s3_20221116095337_kCMWMZ.pcapng     Packets: 40 · Displayed: 1 (2.5%)     Profile: Default
```

4-Pon un TTL=2 y observa qué pasa



```
home > sergio > send_first_packet.py > ...
import socket

s = socket.socket(socket.AF_INET, socket.SOCK_RAW, socket.IPPROTO_TCP)
s.setsockopt(socket.IPPROTO_IP, socket.IP_HDRINCL, 1)

ip_header  = b'\x45\x00\x00\x28'  # Version, IHL, Type of Service | Total Length
ip_header += b'\xab\xcd\x00\x00'  # Identification | Flags, Fragment Offset
ip_header += b'\x02\x06\xa6\xec'  # TTL, Protocol | Header Checksum
ip_header += b'\x0a\x00\x02\x0f'  # Source Address
ip_header += b'\x5b\x8e\xd6\xb5'  # Destination Address

tcp_header  = b'\x30\x39\x00\x50' # Source Port | Destination Port
tcp_header += b'\x00\x00\x00\x00' # Sequence Number
tcp_header += b'\x00\x00\x00\x00' # Acknowledgement Number
tcp_header += b'\x50\x02\x71\x10' # Data Offset, Reserved, Flags | Window Size
tcp_header += b'\xcf\xf6\x00\x00' # Checksum | Urgent Pointer

packet = ip_header + tcp_header
s.sendto(packet, ('91.142.214.181', 0))
```

En el paquete de ida tenemos:



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

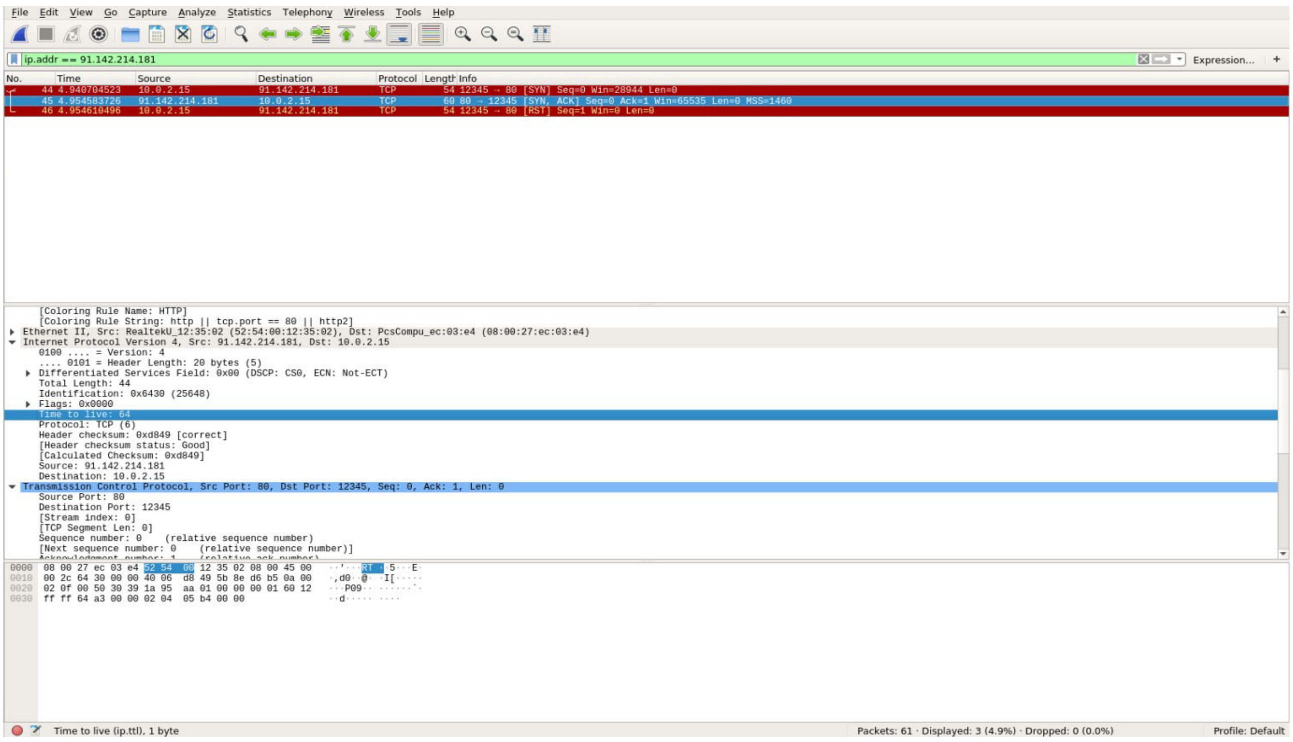
```
ip.addr == 91.142.214.181

No.   Time         Source          Destination     Protocol Length Info
   44 4.940704523  10.0.2.15       91.142.214.181  TCP      54 12345 → 80 [SYN] Seq=0 Win=28944 Len=0
   45 4.954583726  91.142.214.181  10.0.2.15       TCP      60 80 → 12345 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
   46 4.954610496  10.0.2.15       91.142.214.181  TCP      54 12345 → 80 [RST] Seq=1 Win=0 Len=0
```

```
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: TTL low or unexpected]
    [Coloring Rule String: ( ! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp || carp))]
▸ Ethernet II, Src: PcsCompu_ec:03:e4 (08:00:27:ec:03:e4), 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 [correct]
    [Header checksum status: Good]
    [Calculated Checksum: 0xceb0]
    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
```

```
0000  52 54 00 12 35 02 08 00  27 ec 03 e4 08 00 45 00   RT··5···'·····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·····
```

```
/tmp/wireshark_enp0s3_20221116095807_HBtFbT.pcapng (16 kB)
Packets: 61 · Displayed: 3 (4.9%)                Profile: Default
```

En el paquete de vuelta tenemos:


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

```
ip.addr == 91.142.214.181

No.   Time          Source           Destination      Protocol Length Info
   44 4.940704523   10.0.2.15        91.142.214.181   TCP      54 12345 → 80 [SYN] Seq=0 Win=28944 Len=0
   45 4.954583726   91.142.214.181   10.0.2.15        TCP      60 80 → 12345 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
   46 4.954610496   10.0.2.15        91.142.214.181   TCP      54 12345 → 80 [RST] Seq=1 Win=0 Len=0

    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
▸ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_ec:03:e4 (08:00:27:ec:03:e4)
▾ Internet Protocol Version 4, Src: 91.142.214.181, Dst: 10.0.2.15
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 44
    Identification: 0x6430 (25648)
  ▸ Flags: 0x0000
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xd849 [correct]
    [Header checksum status: Good]
    [Calculated Checksum: 0xd849]
    Source: 91.142.214.181
    Destination: 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)

0000  08 00 27 ec 03 e4 52 54  00 12 35 02 08 00 45 00   ··'···RT ··5···E·
0010  00 2c 64 30 00 00 40 06  d8 49 5b 8e d6 b5 0a 00   ·,d0··@· ·I[····
0020  02 0f 00 50 30 39 1a 95  aa 01 00 00 00 01 60 12   ···P09·· ······`·
0030  ff ff 64 a3 00 00 02 04  05 b4 00 00               ··d····· ····

Time to live (ip.ttl), 1 byte     Packets: 61 · Displayed: 3 (4.9%) · Dropped: 0 (0.0%)     Profile: Default
```