

## 1. Find some tcp packet received by your laptop and explore it.

I found a tcp packet in the list of incoming packets

The screenshot shows the Wireshark interface with a list of captured packets. The selected packet is a TLSv1.2 packet from source 10.91.54.148 to destination 188.138.155.250, with length 97 bytes. The packet details pane shows the following structure:

- Frame 19: 728 bytes on wire (5824 bits), 728 bytes captured (5824 bits) on interface wlo1, id 0
- Ethernet II, Src: IntelCor\_b7:d3:4c (14:4f:8a:b7:d3:4c), Dst: Routerbo\_ac:1a:f5 (48:8f:5a:ac:1a:f5)
- Internet Protocol Version 4, Src: 10.91.54.148, Dst: 64.233.164.139
- Transmission Control Protocol, Src Port: 43764, Dst Port: 443, Seq: 1, Ack: 1, Len: 662
- Transport Layer Security

The packet bytes pane shows the raw data of the packet, including the TLS alert structure.

## 2. Which protocols are used inside the tcp packet?

Inside the given packet the following protocols are used

- Internet Protocol Version 4
- Transmission Control Protocol

The screenshot shows the Wireshark interface with the details pane expanded for the selected packet. The details pane shows the following structure:

- Frame 19: 728 bytes on wire (5824 bits), 728 bytes captured (5824 bits) on interface wlo1, id 0
- Ethernet II, Src: IntelCor\_b7:d3:4c (14:4f:8a:b7:d3:4c), Dst: Routerbo\_ac:1a:f5 (48:8f:5a:ac:1a:f5)
- Internet Protocol Version 4, Src: 10.91.54.148, Dst: 64.233.164.139
- Transmission Control Protocol, Src Port: 43764, Dst Port: 443, Seq: 1, Ack: 1, Len: 662
- Transport Layer Security

The packet bytes pane shows the raw data of the packet, including the TLS alert structure.

## 3. Who sent this package? What is the ip address and port of source host?

The packet was sent by 10.91.54.148 as is stated besides Internet Protocol Version 4

The port of the packet is 43764 as is stated besides Transmission Control Protocol

No.	Time	Source	Destination	Protocol	Length	Info
10	0.000000000	10.91.54.148	18.66.97.124	TLSv1.2	165	Application Data
3	0.057649477	10.91.54.148	18.66.97.124	TCP	66	59346 → 443 [ACK] Seq=40 Ack=40 Win=501 Len=0 TSval=194565967
10	0.385986561	10.91.54.148	64.233.164.139	TCP	74	43764 → 443 [SYN] Seq=0 Win=64256 Len=0 MSS=1460 SACK_PERM=1
16	0.389708467	10.91.54.148	64.233.164.139	TCP	66	43764 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=411026759
19	0.398384277	10.91.54.148	64.233.164.139	TLSv1.3	728	Client Hello
20	0.398958381	10.91.54.148	64.233.164.139	TLSv1.3	242	Change Cipher Spec, Application Data
27	0.432496280	10.91.54.148	64.233.164.139	TCP	66	43764 → 443 [ACK] Seq=839 Ack=763 Win=63616 Len=0 TSval=41102
29	0.433198559	10.91.54.148	64.233.164.139	TCP	66	43764 → 443 [ACK] Seq=839 Ack=825 Win=63616 Len=0 TSval=41102
31	0.433220730	10.91.54.148	64.233.164.139	TCP	66	43764 → 443 [ACK] Seq=839 Ack=856 Win=63616 Len=0 TSval=41102
32	0.433825435	10.91.54.148	64.233.164.139	TLSv1.3	150	Application Data, Application Data
33	0.435948496	10.91.54.148	64.233.164.139	TLSv1.3	97	Application Data
36	2.622980827	10.91.54.148	188.138.155.250	TCP	66	47618 → 443 [ACK] Seq=1 Ack=1 Win=1877 Len=0 TSval=3177084286
39	5.722867380	10.91.54.148	188.138.155.250	TLSv1.2	97	[TCP Previous segment not captured] Encrypted Alert
40	5.799941203	10.91.54.148	188.138.155.250	TCP	66	47618 → 443 [FIN, ACK] Seq=33 Ack=1 Win=1877 Len=0 TSval=3177
45	5.863518282	10.91.54.148	188.138.155.250	TCP	66	47618 → 443 [ACK] Seq=34 Ack=2 Win=1877 Len=0 TSval=317708746

Frame 19: 728 bytes on wire (5824 bits), 728 bytes captured (5824 bits) on interface wlo1, id 6  
Ethernet II, Src: IntelCor b7:d3:4c (14:df:8a:b7:d3:4c), Dst: Routerbo ac:1a:f5 (48:8f:5a:ac:1a:f5)  
Internet Protocol Version 4, Src: 10.91.54.148, Dst: 64.233.164.139  
Transmission Control Protocol, Src Port: 43764, Dst Port: 443, Seq: 1, Ack: 1, Len: 662  
Transport Layer Security

0000 48 8f 5a ac 1a f5 14 4f 8a b7 d3 4c 08 00 45 06 H Z...O...L...  
0010 32 ca 8b 08 40 80 40 00 86 c2 0a 5b 36 94 48 e9 ...0...[0-0...  
0020 1a 5a aa f4 01 b0 3f 41 7d 47 ca 7d 15 60 80 10 ...FA]g...  
0030 01 f6 49 ae 00 00 01 01 08 0a f4 fd b4 d5 94 5e IN...  
0040 4e 6e 16 03 01 02 01 01 00 02 8d 03 03 a7 d3 b7 Nn...  
0050 ad 2b ad a1 b5 e5 22 21 74 bd 16 c8 2b 49 b5 57 ...P t...+1W  
0060 9e 0a 51 98 fa 7b a9 1b ae 0c 8c d2 bd 20 01 d4 ...Q...  
0070 80 38 63 10 b1 66 ab 6d 8e 02 bf d5 9d c8 11 c0 ...c...Km...  
0080 1d b0 c5 16 ae a8 23 c0 e7 95 a1 2d ff c0 00 22 ...#...  
0090 13 01 13 03 13 02 c0 2b c0 2f cc a9 cc a8 c0 2c ...+...  
00a0 c0 30 c0 0a c0 09 c0 13 c0 14 00 9c 00 9d 00 2f ...  
00b0 00 35 01 00 02 22 00 00 00 19 00 17 00 00 14 74 ...P...t...  
00c0 72 61 6e 73 6c 61 74 65 2e 67 ef ef 67 6c 65 2e ranslate...google...  
00d0 63 6f 6d 00 17 00 00 ff 01 00 01 00 00 0a 00 0e com...  
00e0 00 0c 00 1d 00 17 00 18 00 19 01 00 01 01 00 0b ...  
00f0 00 02 01 00 00 10 00 0e 00 0c 02 68 32 00 68 74 ...h2 ht  
0100 74 70 2f 31 2e 31 00 05 00 05 01 00 00 00 00 00 tp/1.1...

#### 4. How do we filter out packets containing the tcp protocol?

In the upper corner there is a bar where filters can be applied. For example, if only TCP packets are needed, tcp can be typed in that bar.

No.	Time	Source	Destination	Protocol	Length	Info
10	0.000000000	10.91.54.148	18.66.97.124	TLSv1.2	165	Application Data
3	0.057649477	10.91.54.148	18.66.97.124	TCP	66	59346 → 443 [ACK] Seq=40 Ack=40 Win=501 Len=0 TSval=194565967
10	0.385986561	10.91.54.148	64.233.164.139	TCP	74	43764 → 443 [SYN] Seq=0 Win=64256 Len=0 MSS=1460 SACK_PERM=1
16	0.389708467	10.91.54.148	64.233.164.139	TCP	66	43764 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=411026759
19	0.398384277	10.91.54.148	64.233.164.139	TLSv1.3	728	Client Hello
20	0.398958381	10.91.54.148	64.233.164.139	TLSv1.3	242	Change Cipher Spec, Application Data
27	0.432496280	10.91.54.148	64.233.164.139	TCP	66	43764 → 443 [ACK] Seq=839 Ack=763 Win=63616 Len=0 TSval=41102
29	0.433198559	10.91.54.148	64.233.164.139	TCP	66	43764 → 443 [ACK] Seq=839 Ack=825 Win=63616 Len=0 TSval=41102
31	0.433220730	10.91.54.148	64.233.164.139	TCP	66	43764 → 443 [ACK] Seq=839 Ack=856 Win=63616 Len=0 TSval=41102
32	0.433825435	10.91.54.148	64.233.164.139	TLSv1.3	150	Application Data, Application Data
33	0.435948496	10.91.54.148	64.233.164.139	TLSv1.3	97	Application Data
36	2.622980827	10.91.54.148	188.138.155.250	TCP	66	47618 → 443 [ACK] Seq=1 Ack=1 Win=1877 Len=0 TSval=3177084286
39	5.722867380	10.91.54.148	188.138.155.250	TLSv1.2	97	[TCP Previous segment not captured] Encrypted Alert
40	5.799941203	10.91.54.148	188.138.155.250	TCP	66	47618 → 443 [FIN, ACK] Seq=33 Ack=1 Win=1877 Len=0 TSval=3177
45	5.863518282	10.91.54.148	188.138.155.250	TCP	66	47618 → 443 [ACK] Seq=34 Ack=2 Win=1877 Len=0 TSval=317708746

Frame 19: 728 bytes on wire (5824 bits), 728 bytes captured (5824 bits) on interface wlo1, id 6  
Ethernet II, Src: IntelCor b7:d3:4c (14:df:8a:b7:d3:4c), Dst: Routerbo ac:1a:f5 (48:8f:5a:ac:1a:f5)  
Internet Protocol Version 4, Src: 10.91.54.148, Dst: 64.233.164.139  
Transmission Control Protocol, Src Port: 43764, Dst Port: 443, Seq: 1, Ack: 1, Len: 662  
Transport Layer Security

0000 48 8f 5a ac 1a f5 14 4f 8a b7 d3 4c 08 00 45 06 H Z...O...L...  
0010 32 ca 8b 08 40 80 40 00 86 c2 0a 5b 36 94 48 e9 ...0...[0-0...  
0020 1a 5a aa f4 01 b0 3f 41 7d 47 ca 7d 15 60 80 10 ...FA]g...  
0030 01 f6 49 ae 00 00 01 01 08 0a f4 fd b4 d5 94 5e IN...  
0040 4e 6e 16 03 01 02 01 01 00 02 8d 03 03 a7 d3 b7 Nn...  
0050 ad 2b ad a1 b5 e5 22 21 74 bd 16 c8 2b 49 b5 57 ...P t...+1W  
0060 9e 0a 51 98 fa 7b a9 1b ae 0c 8c d2 bd 20 01 d4 ...Q...  
0070 80 38 63 10 b1 66 ab 6d 8e 02 bf d5 9d c8 11 c0 ...c...Km...  
0080 1d b0 c5 16 ae a8 23 c0 e7 95 a1 2d ff c0 00 22 ...#...  
0090 13 01 13 03 13 02 c0 2b c0 2f cc a9 cc a8 c0 2c ...+...  
00a0 c0 30 c0 0a c0 09 c0 13 c0 14 00 9c 00 9d 00 2f ...  
00b0 00 35 01 00 02 22 00 00 00 19 00 17 00 00 14 74 ...P...t...  
00c0 72 61 6e 73 6c 61 74 65 2e 67 ef ef 67 6c 65 2e ranslate...google...  
00d0 63 6f 6d 00 17 00 00 ff 01 00 01 00 00 0a 00 0e com...  
00e0 00 0c 00 1d 00 17 00 18 00 19 01 00 01 01 00 0b ...  
00f0 00 02 01 00 00 10 00 0e 00 0c 02 68 32 00 68 74 ...h2 ht  
0100 74 70 2f 31 2e 31 00 05 00 05 01 00 00 00 00 00 tp/1.1...

#### 5. How do we filter out packets from some specific host?

To filter out packets from a specific host, we can write down the following in the filter bar

ip.src == 10.91.54.148 or ip.addr == 10.91.54.148

Applications Mon, Jan 17 15:36

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 10.91.54.148 or ip.addr == 10.91.54.148

No.	Time	Source	Destination	Protocol	Length	Info
1834	66.392617241	10.91.54.148	91.108.56.163	TCP	66	50516 → 443 [ACK] Seq=1004 Ack=144076 Win=303872 Len=0 TSval=...
1832	66.392591630	10.91.54.148	91.108.56.163	TCP	66	50516 → 443 [ACK] Seq=1004 Ack=142848 Win=301056 Len=0 TSval=...
1838	66.392247060	10.91.54.148	91.108.56.163	TCP	66	50516 → 443 [ACK] Seq=1004 Ack=141620 Win=298112 Len=0 TSval=...
1828	66.392210563	10.91.54.148	91.108.56.163	TCP	66	50516 → 443 [ACK] Seq=1004 Ack=148392 Win=295168 Len=0 TSval=...
1826	66.391028047	10.91.54.148	91.108.56.163	TCP	66	50516 → 443 [ACK] Seq=1004 Ack=139164 Win=292352 Len=0 TSval=...
1824	66.391011533	10.91.54.148	91.108.56.163	TCP	66	50516 → 443 [ACK] Seq=1004 Ack=137936 Win=289408 Len=0 TSval=...
1822	66.390681086	10.91.54.148	91.108.56.163	TCP	66	50516 → 443 [ACK] Seq=1004 Ack=136708 Win=286464 Len=0 TSval=...
1820	66.390664026	10.91.54.148	91.108.56.163	TCP	66	50516 → 443 [ACK] Seq=1004 Ack=135480 Win=283648 Len=0 TSval=...
1818	66.389652040	10.91.54.148	91.108.56.163	TCP	66	50516 → 443 [ACK] Seq=1004 Ack=134252 Win=280784 Len=0 TSval=...
1816	66.389634483	10.91.54.148	91.108.56.163	TCP	66	50516 → 443 [ACK] Seq=1004 Ack=133024 Win=277888 Len=0 TSval=...
1814	66.389607351	10.91.54.148	91.108.56.163	TCP	66	50516 → 443 [ACK] Seq=1004 Ack=131796 Win=274944 Len=0 TSval=...
1812	66.389592644	10.91.54.148	91.108.56.163	TCP	66	50516 → 443 [ACK] Seq=1004 Ack=130568 Win=272000 Len=0 TSval=...
1810	66.388331193	10.91.54.148	91.108.56.163	TCP	66	50516 → 443 [ACK] Seq=1004 Ack=129340 Win=269184 Len=0 TSval=...
1808	66.388303873	10.91.54.148	91.108.56.163	TCP	66	50516 → 443 [ACK] Seq=1004 Ack=128112 Win=266240 Len=0 TSval=...
1806	66.387355893	10.91.54.148	91.108.56.163	TCP	66	50516 → 443 [ACK] Seq=1004 Ack=126884 Win=263296 Len=0 TSval=...

Arrival Time: Jan 17, 2022 15:15:14.392911431 EAT  
[Time shift for this packet: 0.000000000 seconds]  
Epoch Time: 1642421714.392911431 seconds  
[Time delta from previous captured frame: 0.000032159 seconds]  
[Time delta from previous displayed frame: 0.000032159 seconds]  
[Time since reference or first frame: 66.389652040 seconds]  
Frame Number: 1818  
Frame Length: 66 bytes (528 bits)  
Capture Length: 66 bytes (528 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ethertype:ip:tcp]  
[Coloring Rule Name: TCP]  
[Coloring Rule String: tcp]

Ethernet II, Src: IntelCor\_b7:d3:4c (14:4f:8a:b7:d3:4c), Dst: Routerbo\_ac:1a:f5 (48:8f:5a:ac:1a:f5)

Internet Protocol Version 4, Src: 10.91.54.148, Dst: 91.108.56.163

```

0000  48 8f 5a ac 1a f5 14 4f 8a b7 d3 4c 08 00 45 0e  H.Z...O...L...
0010  08 34 9d 00 20 00 00 00 c7 f0 00 5b 5c 94 50 0e  .L.B.O...[G.L
0020  55 54 c5 54 d1 b0 df 3f de 8a 9f 26 ad 9d 80 10  S.T.?...&
0030  08 91 e3 d1 00 00 01 01 08 0a 01 0b 08 ef f6 f8  ..a....
0040  8f ca

```

Internet Protocol Version 4 (ip), 20 bytes

Packets: 12793 · Displayed: 12775 (99.9%)

Profile: Default