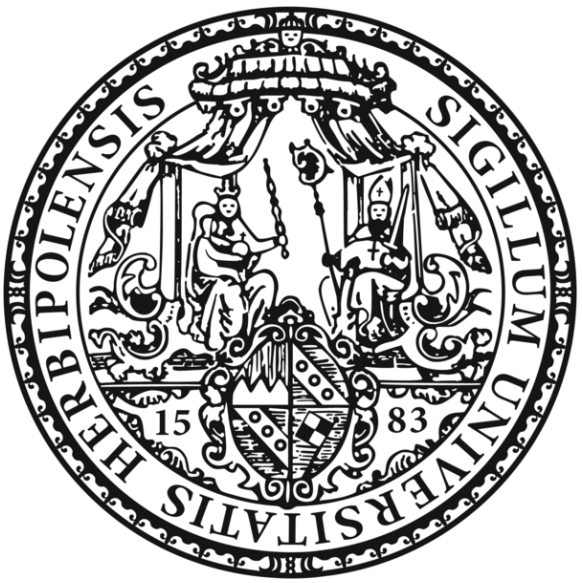
Hardwarepraktikum Internet-Technologien

Task 4: Transmission of the sens



Julius-Maximilians-Universität Würzburg

Chair of Computer Science III

A project report submitted by **group 11**

Enrique Mesonero Ronco

Manuel Calvo Martín

Pablo E. Ortega Ureña

Summer term 2022

May, 2022

Contents

4. Transmission of sensor data

4.1. TCP server at the end device

For the realization of this exercise, the first thing we have done has been to make the .py corresponding to the server, in this case, our PC, which will be responsible for receiving the information through the TCP protocol of our temperature sensor, sent through our Raspberry Pi.

4.2. TCP client on the Raspberry Pi

Next, we have made the necessary .py file for the Raspberry, in this case, the client that will send the information from the temperature sensor connected to it, and we have uploaded it from our PC to the Raspberry via scp, as shown in Figure 4.1.

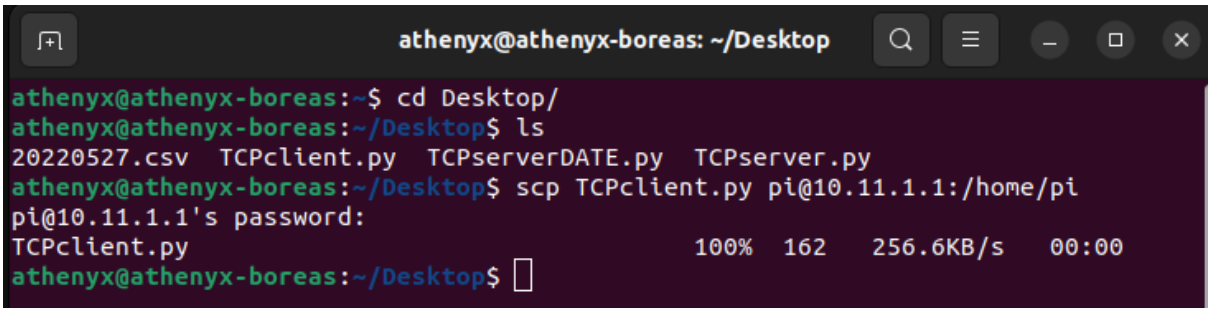


Figure 4.1: Uploading TCPclient.py via scp

Once all the files had been created and uploaded to their corresponding devices, we checked their correct operation, as shown in Figure 4.2.

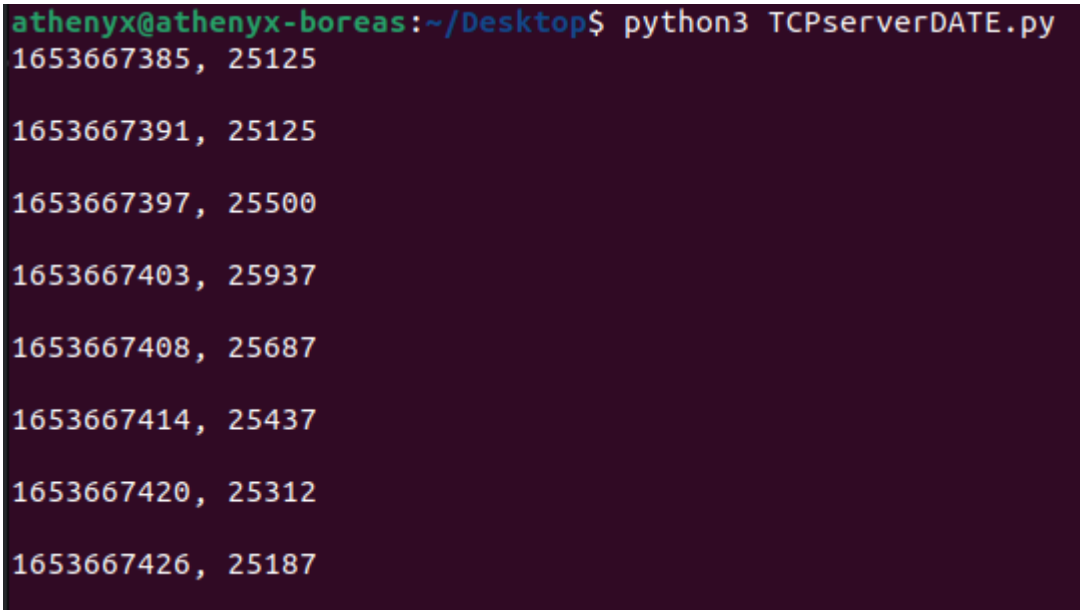


Figure 4.2.: Sending the temperature information

4.3. Presentation in the browser

For the presentation of the information, we created a .py file to generate the corresponding HTML files, using the .csv files resulting from the processing of the information from the temperature sensor by the server, and to show us a graph, the conclusion of the information obtained, as shown in Figure 4.3.

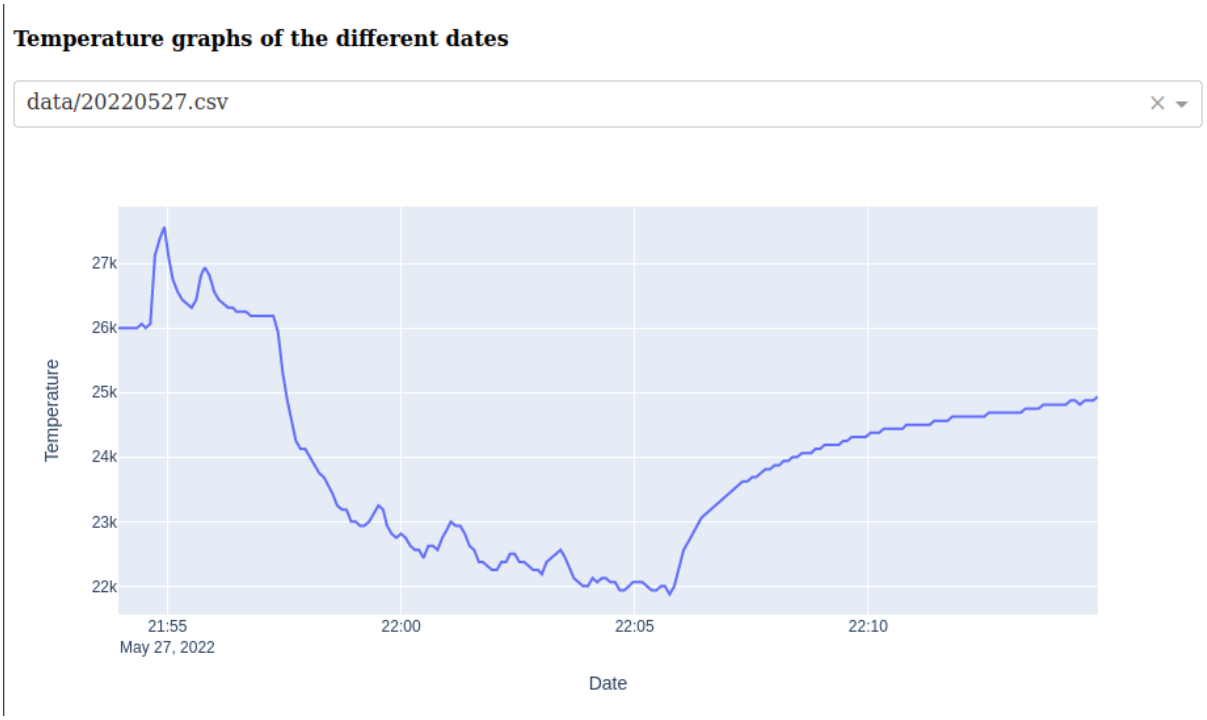
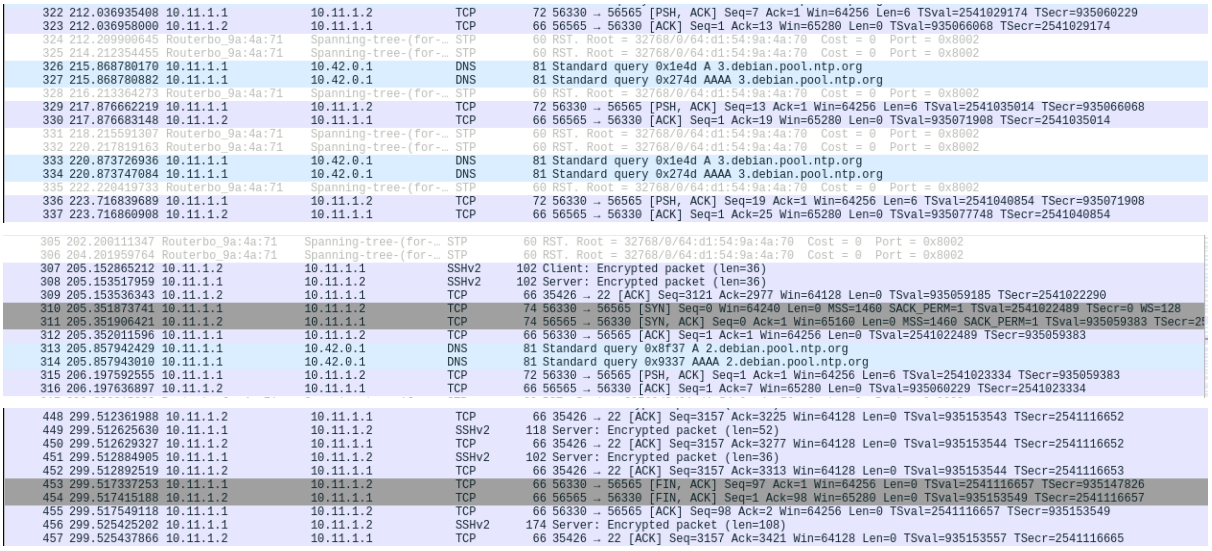


Figure 4.3.: Graphic of temperature

(Note: all scripts are available in our git repository.)

4.3. Monitoring of website views

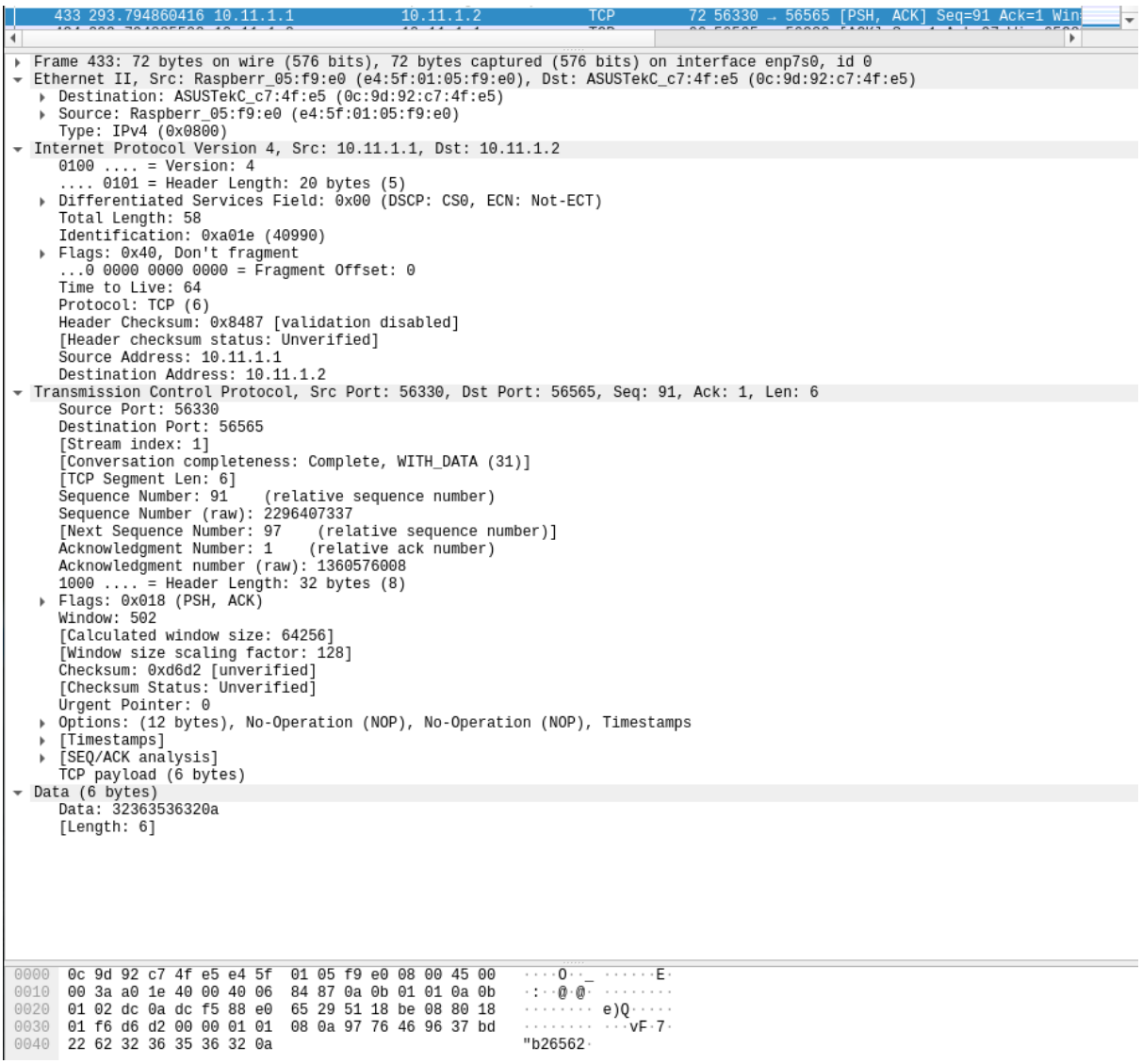
Finally, in order to perform the activities required in section 4.5 of the instruction sheet, we used WireShark to monitor and control the packets sent, as can be seen in the resulting figures.

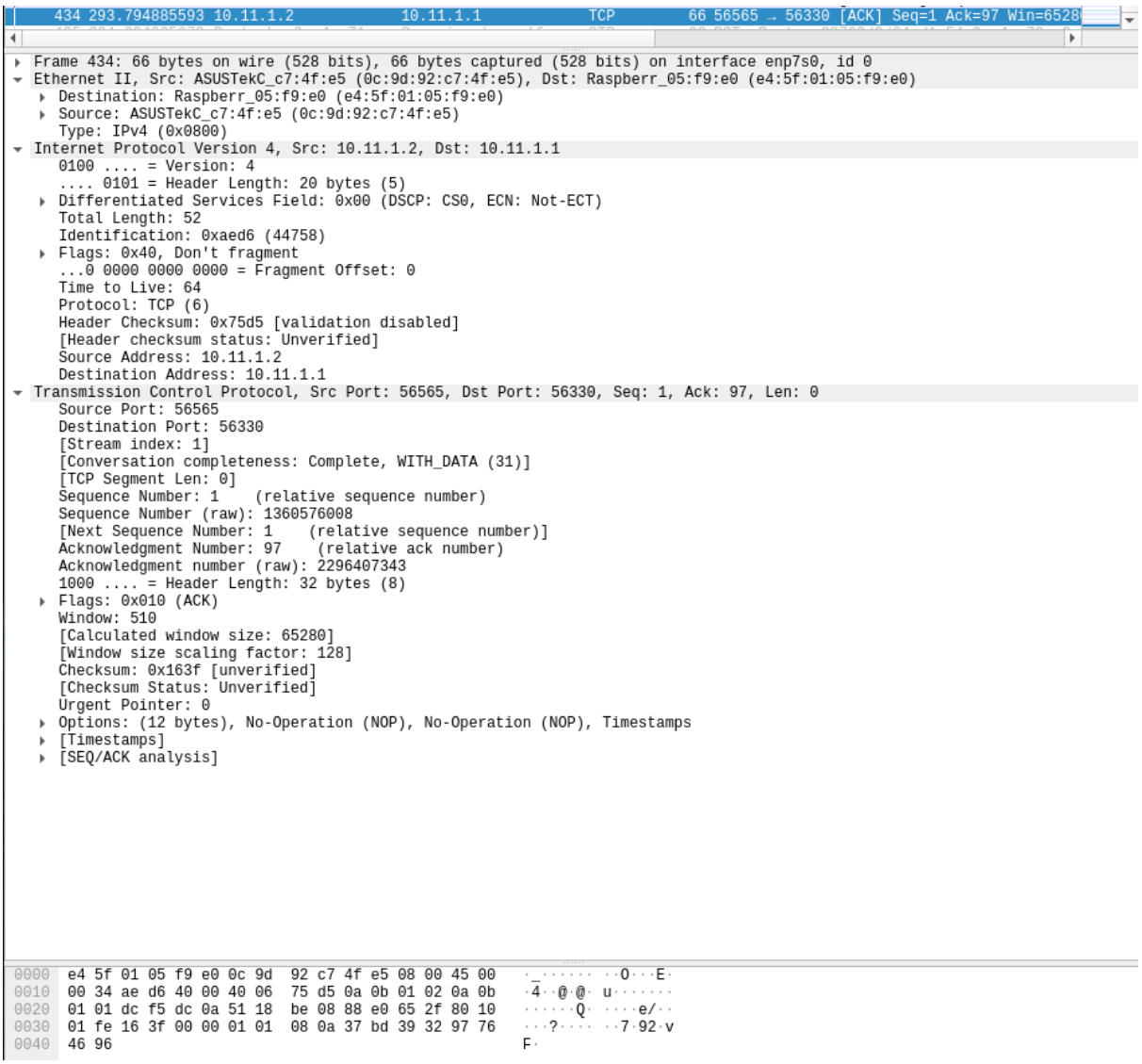


322	212.036935408	10.11.1.1	10.11.1.2	TCP	72 56330 → 56565 [PSH, ACK] Seq=7 Ack=1 Win=64256 Len=6 TSval=2541029174 TSecr=935060229
323	212.036958000	10.11.1.2	10.11.1.1	TCP	66 56565 → 56330 [ACK] Seq=1 Ack=13 Win=65280 Len=0 TSval=935066068 TSecr=2541029174
324	212.209900645	Routerbo_9a:4a:71	Spanning-tree-(for-…	STP	60 RST. Root = 32768/0/64:d1:54:9a:4a:70 Cost = 0 Port = 0x8002
325	214.212354455	Routerbo_9a:4a:71	Spanning-tree-(for-…	STP	60 RST. Root = 32768/0/64:d1:54:9a:4a:70 Cost = 0 Port = 0x8002
326	215.868780170	10.11.1.1	10.42.0.1	DNS	81 Standard query 0x1e4d A 3.debian.pool.ntp.org
327	215.868780882	10.11.1.1	10.42.0.1	DNS	81 Standard query 0x274d AAAA 3.debian.pool.ntp.org
328	216.213364273	Routerbo_9a:4a:71	Spanning-tree-(for-…	STP	60 RST. Root = 32768/0/64:d1:54:9a:4a:70 Cost = 0 Port = 0x8002
329	217.876662219	10.11.1.1	10.11.1.2	TCP	72 56330 → 56565 [PSH, ACK] Seq=13 Ack=1 Win=64256 Len=6 TSval=2541035014 TSecr=935066068
330	217.876683148	10.11.1.2	10.11.1.1	TCP	66 56565 → 56330 [ACK] Seq=1 Ack=19 Win=65280 Len=0 TSval=935071908 TSecr=2541035014
331	218.215591307	Routerbo_9a:4a:71	Spanning-tree-(for-…	STP	60 RST. Root = 32768/0/64:d1:54:9a:4a:70 Cost = 0 Port = 0x8002
332	220.217819163	Routerbo_9a:4a:71	Spanning-tree-(for-…	STP	60 RST. Root = 32768/0/64:d1:54:9a:4a:70 Cost = 0 Port = 0x8002
333	220.873726936	10.11.1.1	10.42.0.1	DNS	81 Standard query 0x1e4d A 3.debian.pool.ntp.org
334	220.873747084	10.11.1.1	10.42.0.1	DNS	81 Standard query 0x274d AAAA 3.debian.pool.ntp.org
335	222.220419733	Routerbo_9a:4a:71	Spanning-tree-(for-…	STP	60 RST. Root = 32768/0/64:d1:54:9a:4a:70 Cost = 0 Port = 0x8002
336	223.716839689	10.11.1.1	10.11.1.2	TCP	72 56330 → 56565 [PSH, ACK] Seq=19 Ack=1 Win=64256 Len=6 TSval=2541040854 TSecr=935071908
337	223.716860908	10.11.1.2	10.11.1.1	TCP	66 56565 → 56330 [ACK] Seq=1 Ack=25 Win=65280 Len=0 TSval=935077748 TSecr=2541040854

305	202.200111347	Routerbo_9a:4a:71	Spanning-tree-(for-…	STP	60 RST. Root = 32768/0/64:d1:54:9a:4a:70 Cost = 0 Port = 0x8002
306	204.201959764	Routerbo_9a:4a:71	Spanning-tree-(for-…	STP	60 RST. Root = 32768/0/64:d1:54:9a:4a:70 Cost = 0 Port = 0x8002
307	205.152865212	10.11.1.2	10.11.1.1	SSHv2	102 Client: Encrypted packet (len=36)
308	205.153517959	10.11.1.1	10.11.1.2	SSHv2	102 Server: Encrypted packet (len=36)
309	205.153536343	10.11.1.2	10.11.1.1	TCP	66 35426 → 22 [ACK] Seq=3121 Ack=2977 Win=64128 Len=0 TSval=935059185 TSecr=2541022290
310	205.351873741	10.11.1.1	10.11.1.2	TCP	74 56330 → 56565 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2541022489 TSecr=0 WS=128
311	205.351906421	10.11.1.2	10.11.1.1	TCP	74 56565 → 56330 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=935059383 TSecr=25
312	205.352011596	10.11.1.1	10.11.1.2	TCP	66 56330 → 56565 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2541022489 TSecr=935059383
313	205.857942429	10.11.1.1	10.42.0.1	DNS	81 Standard query 0x8f37 A 2.debian.pool.ntp.org
314	205.857943010	10.11.1.1	10.42.0.1	DNS	81 Standard query 0x9337 AAAA 2.debian.pool.ntp.org
315	206.197592555	10.11.1.1	10.11.1.2	TCP	72 56330 → 56565 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=6 TSval=2541023334 TSecr=935059383
316	206.197636897	10.11.1.2	10.11.1.1	TCP	66 56565 → 56330 [ACK] Seq=1 Ack=7 Win=65280 Len=0 TSval=935060229 TSecr=2541023334

448	299.512361988	10.11.1.2	10.11.1.1	TCP	66 35426 → 22 [ACK] Seq=3157 Ack=3225 Win=64128 Len=0 TSval=935153543 TSecr=2541116652
449	299.512625630	10.11.1.1	10.11.1.2	SSHv2	118 Server: Encrypted packet (len=52)
450	299.512629327	10.11.1.2	10.11.1.1	TCP	66 35426 → 22 [ACK] Seq=3157 Ack=3277 Win=64128 Len=0 TSval=935153544 TSecr=2541116652
451	299.512884905	10.11.1.1	10.11.1.2	SSHv2	102 Server: Encrypted packet (len=36)
452	299.512892519	10.11.1.2	10.11.1.1	TCP	66 35426 → 22 [ACK] Seq=3157 Ack=3313 Win=64128 Len=0 TSval=935153544 TSecr=2541116653
453	299.517337253	10.11.1.1	10.11.1.2	TCP	66 56330 → 56565 [FIN, ACK] Seq=97 Ack=1 Win=64256 Len=0 TSval=2541116657 TSecr=935147826
454	299.517415188	10.11.1.2	10.11.1.1	TCP	66 56565 → 56330 [FIN, ACK] Seq=1 Ack=98 Win=65280 Len=0 TSval=935153549 TSecr=2541116657
455	299.517549118	10.11.1.1	10.11.1.2	TCP	66 56330 → 56565 [ACK] Seq=98 Ack=2 Win=64256 Len=0 TSval=2541116657 TSecr=935153549
456	299.525425202	10.11.1.1	10.11.1.2	SSHv2	174 Server: Encrypted packet (len=108)
457	299.525437866	10.11.1.2	10.11.1.1	TCP	66 35426 → 22 [ACK] Seq=3157 Ack=3421 Win=64128 Len=0 TSval=935153557 TSecr=2541116665


433 293.794860416 10.11.1.1 10.11.1.2 TCP 72 56330 → 56565 [PSH, ACK] Seq=91 Ack=1 Win
Frame 433: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface enp7s0, id 0
Ethernet II, Src: Raspberr_05:f9:e0 (e4:5f:01:05:f9:e0), Dst: ASUSTekC_c7:4f:e5 (0c:9d:92:c7:4f:e5)
Destination: ASUSTekC_c7:4f:e5 (0c:9d:92:c7:4f:e5)
Source: Raspberr_05:f9:e0 (e4:5f:01:05:f9:e0)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.11.1.1, Dst: 10.11.1.2
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 58
Identification: 0xa01e (40990)
Flags: 0x40, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x8487 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.11.1.1
Destination Address: 10.11.1.2
Transmission Control Protocol, Src Port: 56330, Dst Port: 56565, Seq: 91, Ack: 1, Len: 6
Source Port: 56330
Destination Port: 56565
[Stream index: 1]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 6]
Sequence Number: 91 (relative sequence number)
Sequence Number (raw): 2296407337
[Next Sequence Number: 97 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1360576008
1000 .... = Header Length: 32 bytes (8)
Flags: 0x018 (PSH, ACK)
Window: 502
[Calculated window size: 64256]
[Window size scaling factor: 128]
Checksum: 0xd6d2 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[Timestamps]
[SEQ/ACK analysis]
TCP payload (6 bytes)
Data (6 bytes)
Data: 32363536320a
[Length: 6]
0000 0c 9d 92 c7 4f e5 e4 5f 01 05 f9 e0 08 00 45 00
0010 00 3a a0 1e 40 00 40 06 84 87 0a 0b 01 01 0a 0b
0020 01 02 dc 0a dc f5 88 e0 65 29 51 18 be 08 80 18
0030 01 f6 d6 d2 00 00 01 01 08 0a 97 76 46 96 37 bd
0040 22 62 32 36 35 36 32 0a


434 293.794885593 10.11.1.2 10.11.1.1 TCP 66 56565 → 56330 [ACK] Seq=1 Ack=97 Win=6528
Frame 434: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface enp7s0, id 0
Ethernet II, Src: ASUSTekC_c7:4f:e5 (0c:9d:92:c7:4f:e5), Dst: Raspberr_05:f9:e0 (e4:5f:01:05:f9:e0)
Destination: Raspberr_05:f9:e0 (e4:5f:01:05:f9:e0)
Source: ASUSTekC_c7:4f:e5 (0c:9d:92:c7:4f:e5)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.11.1.2, Dst: 10.11.1.1
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0xaed6 (44758)
Flags: 0x40, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x75d5 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.11.1.2
Destination Address: 10.11.1.1
Transmission Control Protocol, Src Port: 56565, Dst Port: 56330, Seq: 1, Ack: 97, Len: 0
Source Port: 56565
Destination Port: 56330
[Stream index: 1]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1360576008
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 97 (relative ack number)
Acknowledgment number (raw): 2296407343
1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
Window: 510
[Calculated window size: 65280]
[Window size scaling factor: 128]
Checksum: 0x163f [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[Timestamps]
[SEQ/ACK analysis]
0000 e4 5f 01 05 f9 e0 0c 9d 92 c7 4f e5 08 00 45 00
0010 00 34 ae d6 40 00 40 06 75 d5 0a 0b 01 02 0a 0b
0020 01 01 dc f5 dc 0a 51 18 be 08 88 e0 65 2f 80 10
0030 01 fe 16 3f 00 00 01 01 08 0a 37 bd 39 32 97 76
0040 46 96