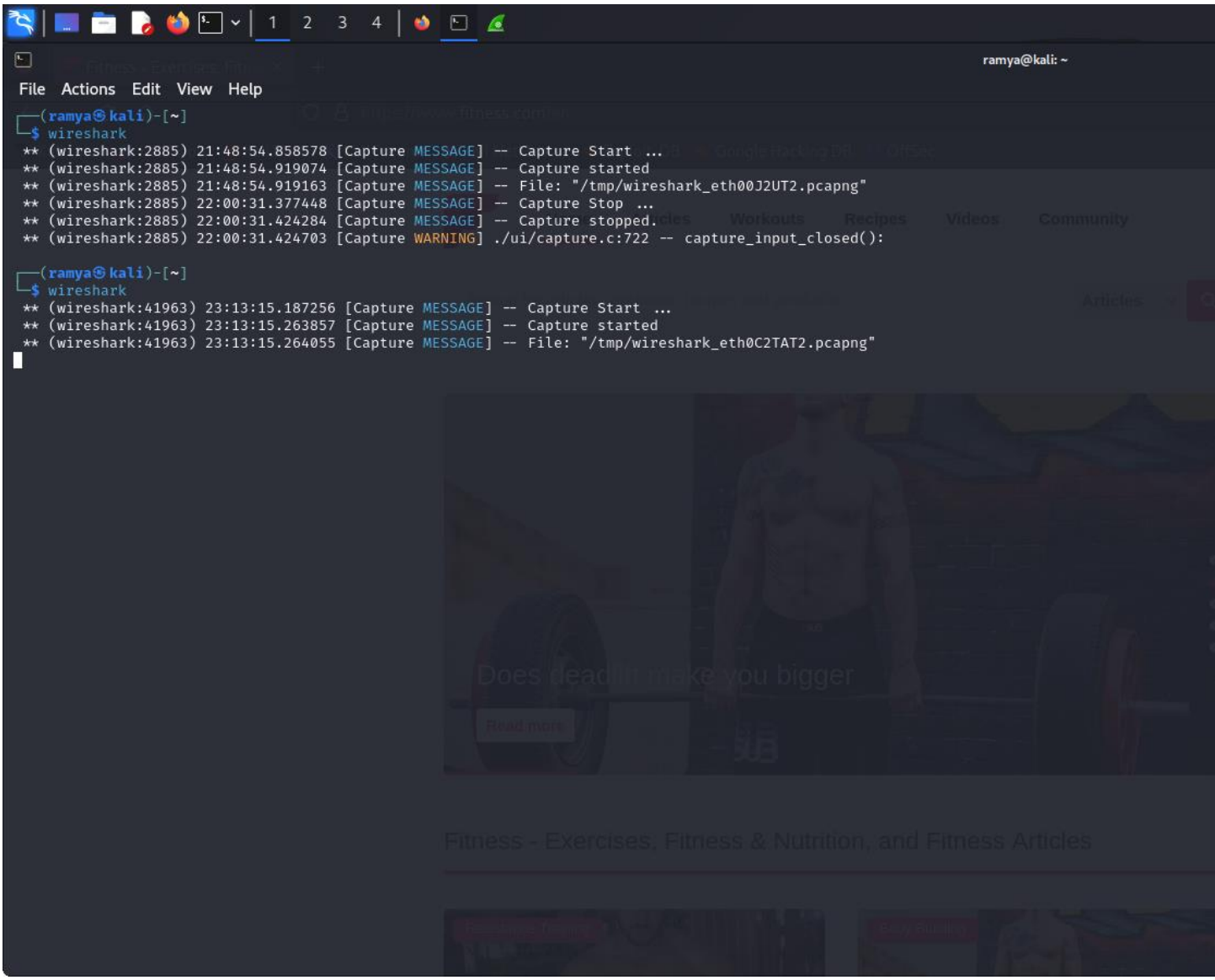
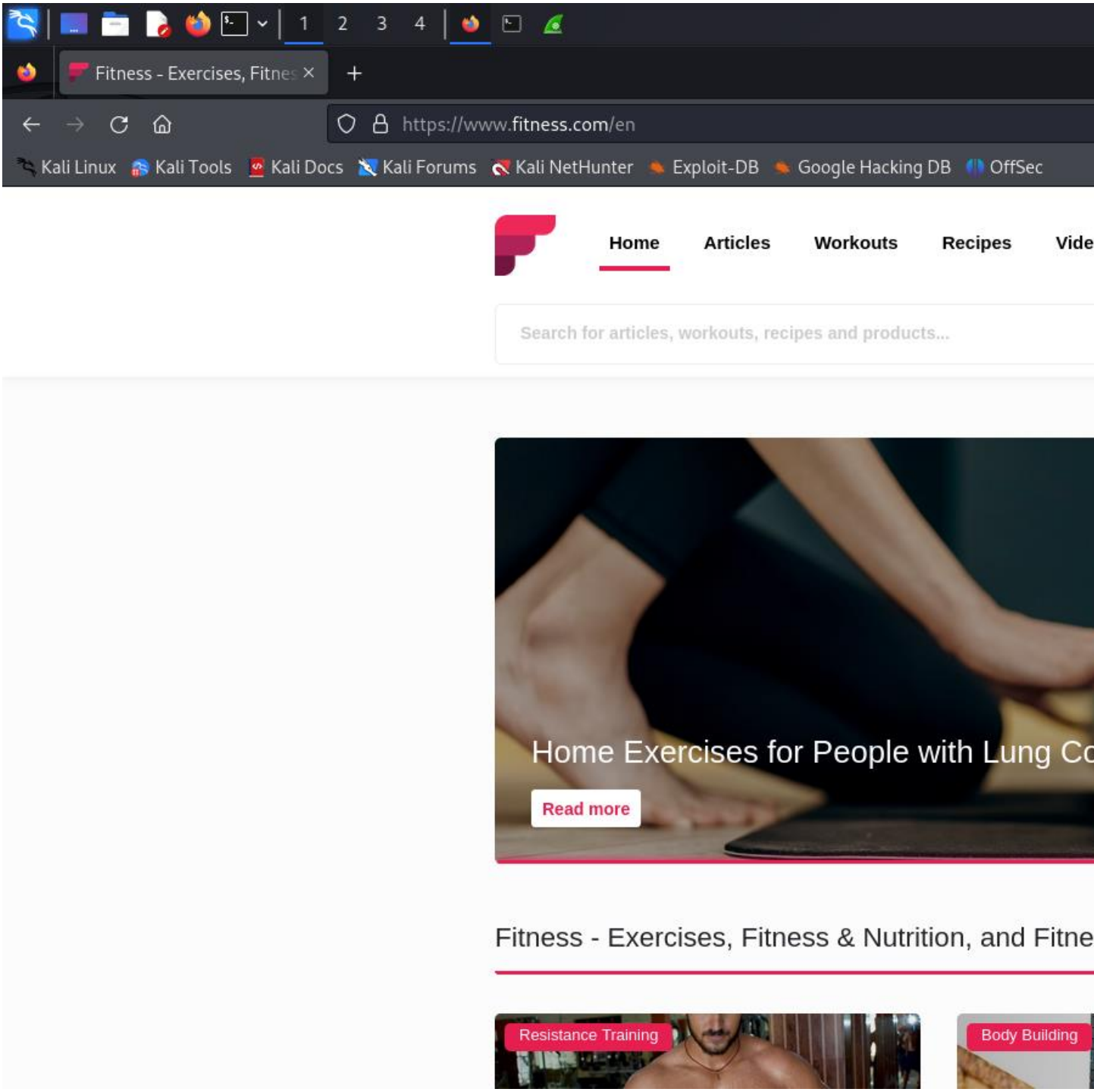
TCP Session Establishment and Termination

Bakka Ramyasree

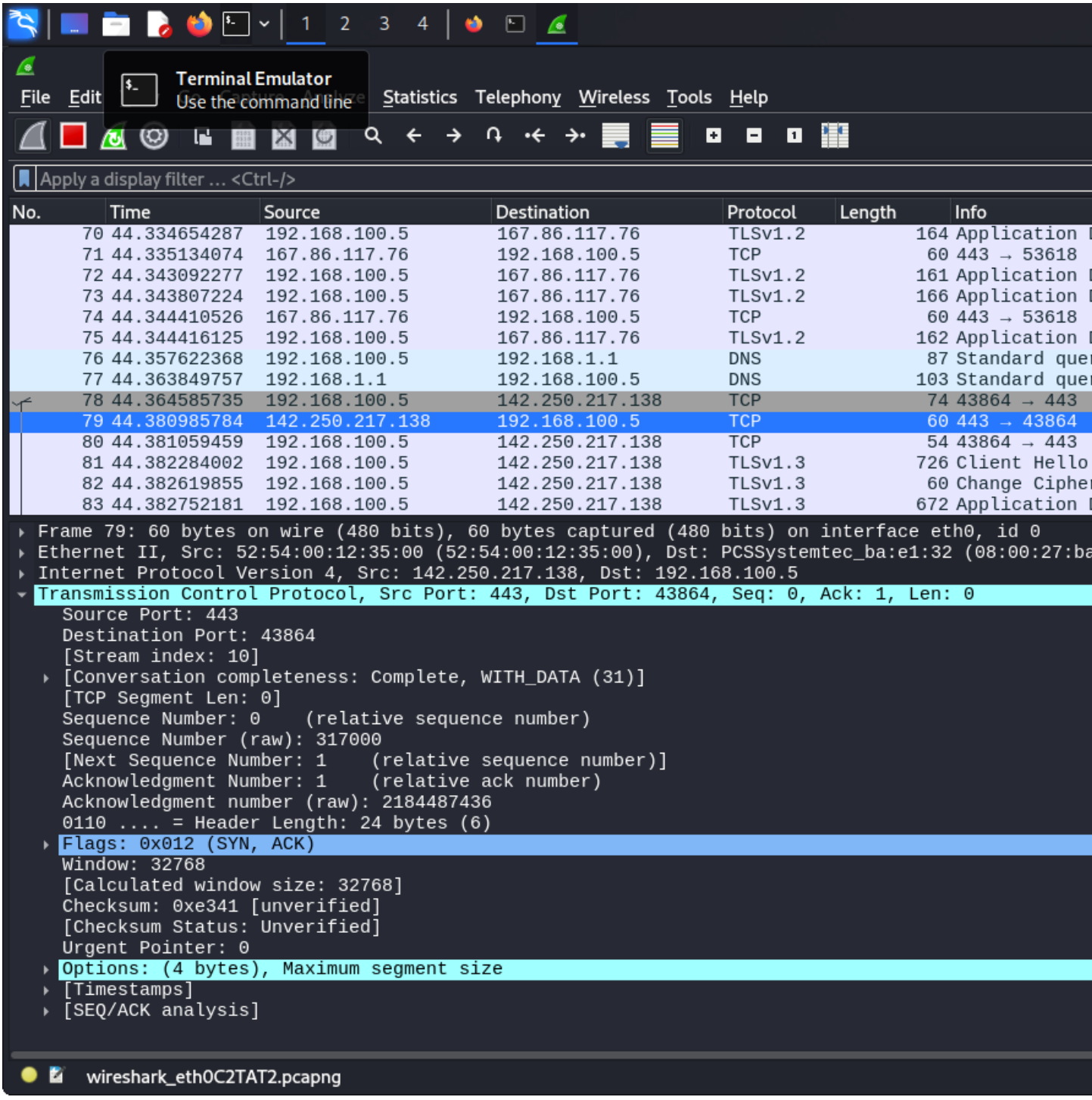
Open Wireshark and Start Capturing

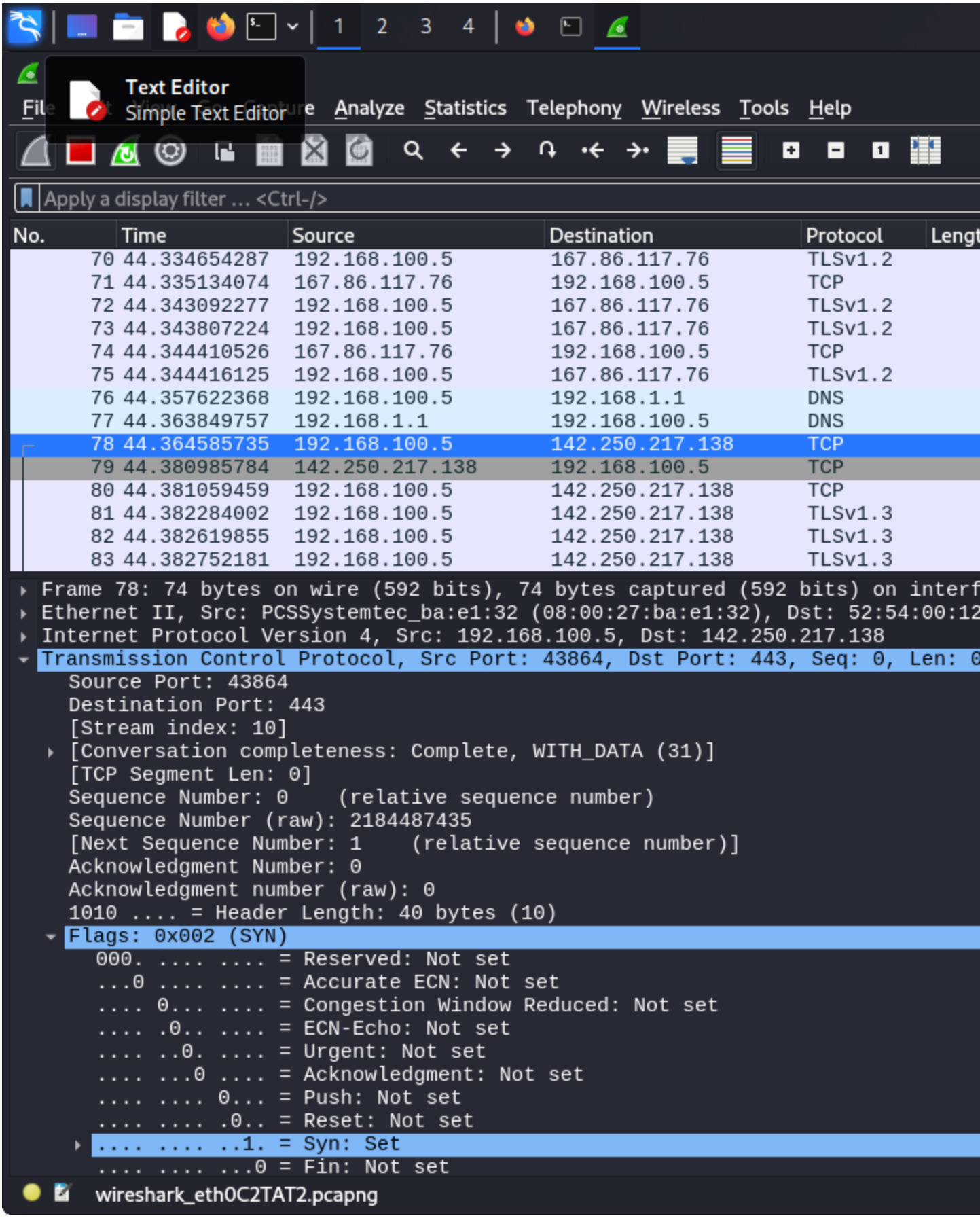


Initiate a TCP Connection:



Identify the Three-Way Handshake:




1 2 3 4
Text Editor
Simple Text Editor
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Lengt
70 44.334654287 192.168.100.5 167.86.117.76 TLSv1.2
71 44.335134074 167.86.117.76 192.168.100.5 TCP
72 44.343092277 192.168.100.5 167.86.117.76 TLSv1.2
73 44.343807224 192.168.100.5 167.86.117.76 TLSv1.2
74 44.344410526 167.86.117.76 192.168.100.5 TCP
75 44.344416125 192.168.100.5 167.86.117.76 TLSv1.2
76 44.357622368 192.168.100.5 192.168.1.1 DNS
77 44.363849757 192.168.1.1 192.168.100.5 DNS
78 44.364585735 192.168.100.5 142.250.217.138 TCP
79 44.380985784 142.250.217.138 192.168.100.5 TCP
80 44.381059459 192.168.100.5 142.250.217.138 TCP
81 44.382284002 192.168.100.5 142.250.217.138 TLSv1.3
82 44.382619855 192.168.100.5 142.250.217.138 TLSv1.3
83 44.382752181 192.168.100.5 142.250.217.138 TLSv1.3
Frame 78: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interf
Ethernet II, Src: PCSSystemtec_ba:e1:32 (08:00:27:ba:e1:32), Dst: 52:54:00:12
Internet Protocol Version 4, Src: 192.168.100.5, Dst: 142.250.217.138
Transmission Control Protocol, Src Port: 43864, Dst Port: 443, Seq: 0, Len: 0
Source Port: 43864
Destination Port: 443
[Stream index: 10]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2184487435
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1010 .... = Header Length: 40 bytes (10)
Flags: 0x002 (SYN)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: 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
wireshark_eth0C2TAT2.pcapng

Analyze the Handshake: A stable connection is established between a client and a server through the TCP three-way handshake, which synchronizes sequence numbers and verifies that both are prepared for communication.
SYN, SYN-ACK, and ACK are the three primary phases in the TCP three-way handshake.
By sending the server a SYN (synchronize) packet, the client starts the TCP connection.
This packet synchronizes the initial sequence number (ISN) for the connection and signals the client's desire to connect to the server.

Here 78 79 80 packets are the 3 packets

Step78: SYN .....First, sync (or SYN). Flags on a packet: ACK = 0 and SYN = 1.
SEQ (Sequence Number): Sequence number:21844874354 ACK=0

Step79: The second step is the SYN-ACK (Synchronize-Acknowledgment) packet.
The server replies with a SYN-ACK packet after receiving the SYN packet.
This packet accomplishes two goals:
Sets the ACK flag to indicate receipt of the SYN packet from the client.

gives its initial sequence number (ISN) and sends its own SYN to the client to let it know it is prepared to connect as well.
Information about the packet: SYN :317000 , ACK=1

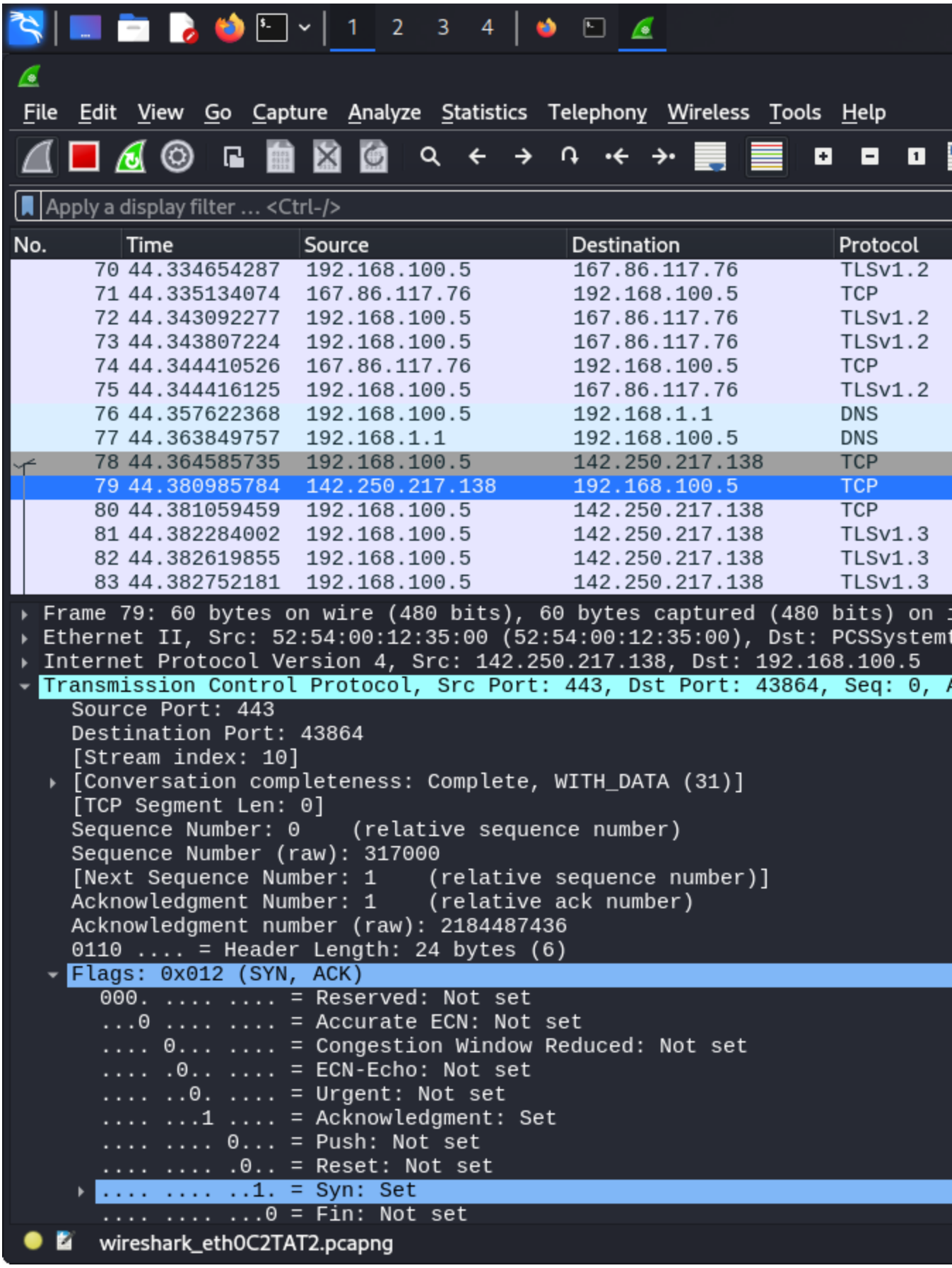
ACK (Acknowledgment) Packet

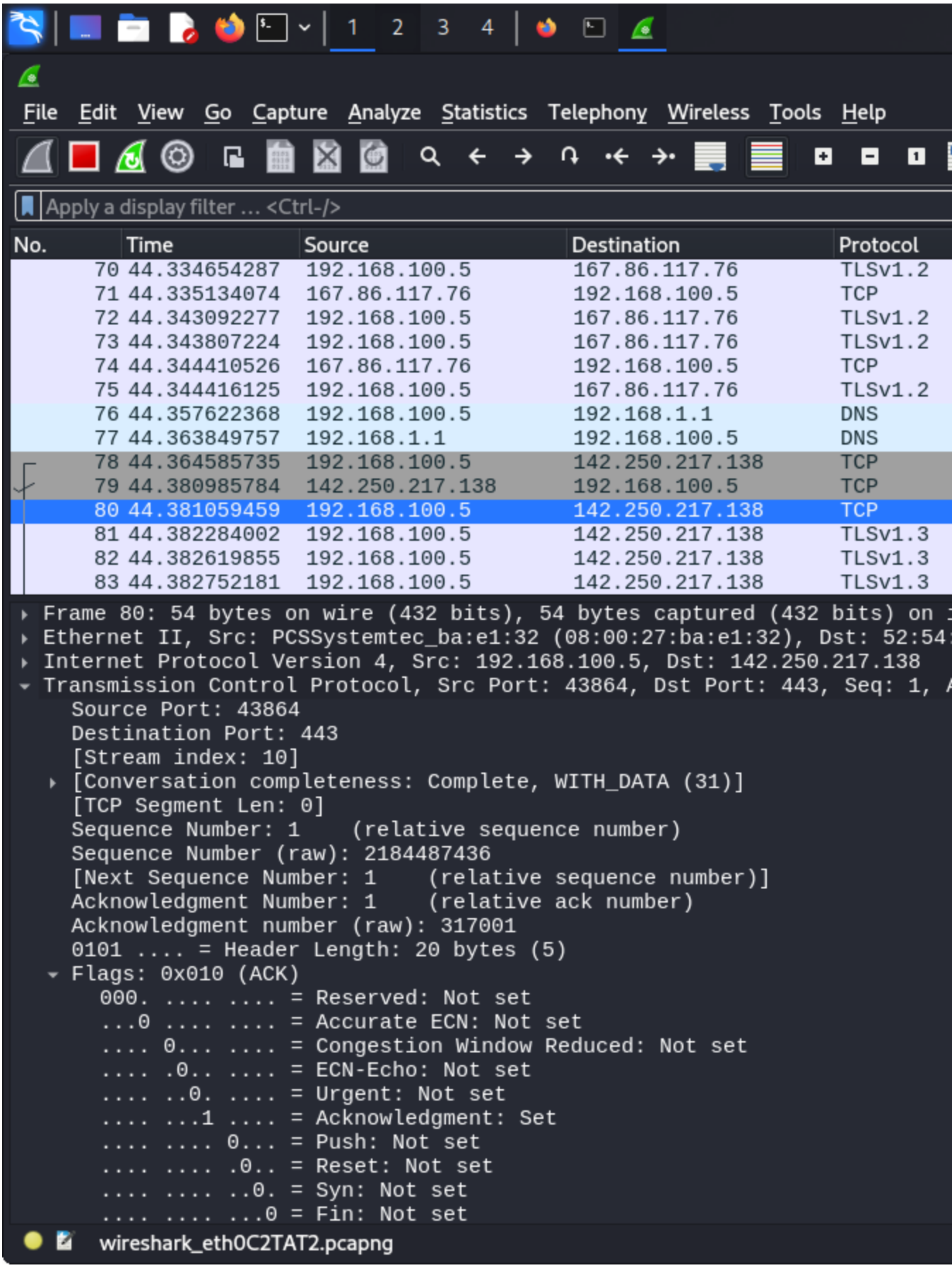
Purpose:

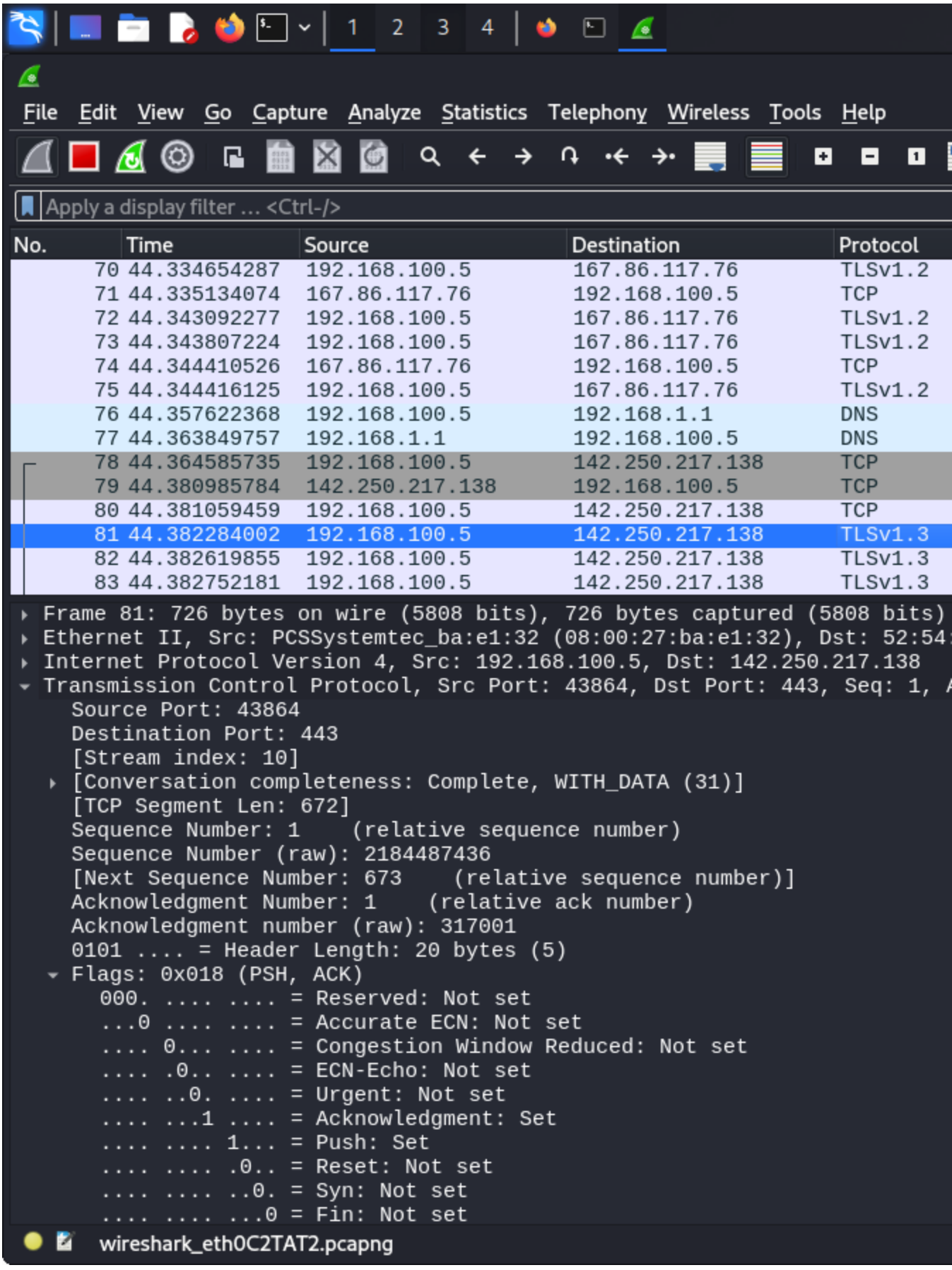
After receiving the SYN-ACK packet, the client sends an ACK packet back to the server.

This packet acknowledges the receipt of the server's SYN-ACK and completes the handshake process.

The connection is now established, and both sides are ready to exchange data Packet 80: SYN:2184487436, ACK=317001
Due to the fact that this is the first packet and there is no data to acknowledge yet, the acknowledgement number (ACK) is 0.

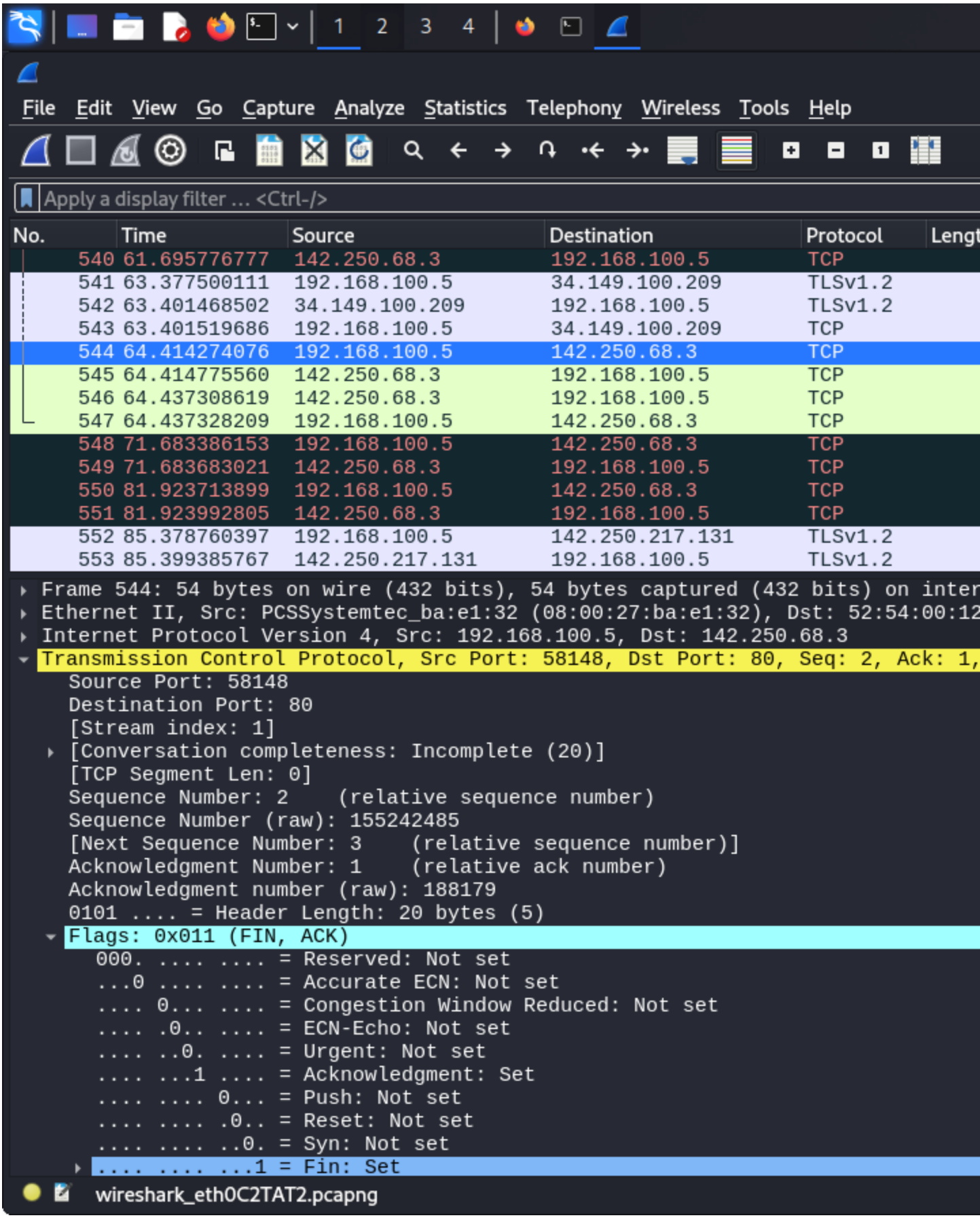

1 2 3 4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol
70 44.334654287 192.168.100.5 167.86.117.76 TLSv1.2
71 44.335134074 167.86.117.76 192.168.100.5 TCP
72 44.343092277 192.168.100.5 167.86.117.76 TLSv1.2
73 44.343807224 192.168.100.5 167.86.117.76 TLSv1.2
74 44.344410526 167.86.117.76 192.168.100.5 TCP
75 44.344416125 192.168.100.5 167.86.117.76 TLSv1.2
76 44.357622368 192.168.100.5 192.168.1.1 DNS
77 44.363849757 192.168.1.1 192.168.100.5 DNS
78 44.364585735 192.168.100.5 142.250.217.138 TCP
79 44.380985784 142.250.217.138 192.168.100.5 TCP
80 44.381059459 192.168.100.5 142.250.217.138 TCP
81 44.382284002 192.168.100.5 142.250.217.138 TLSv1.3
82 44.382619855 192.168.100.5 142.250.217.138 TLSv1.3
83 44.382752181 192.168.100.5 142.250.217.138 TLSv1.3
Frame 79: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on
Ethernet II, Src: 52:54:00:12:35:00 (52:54:00:12:35:00), Dst: PCSystem
Internet Protocol Version 4, Src: 142.250.217.138, Dst: 192.168.100.5
Transmission Control Protocol, Src Port: 443, Dst Port: 43864, Seq: 0,
Source Port: 443
Destination Port: 43864
[Stream index: 10]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 317000
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2184487436
0110 .... = Header Length: 24 bytes (6)
Flags: 0x012 (SYN, ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: 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
wireshark_eth0C2TAT2.pcapng

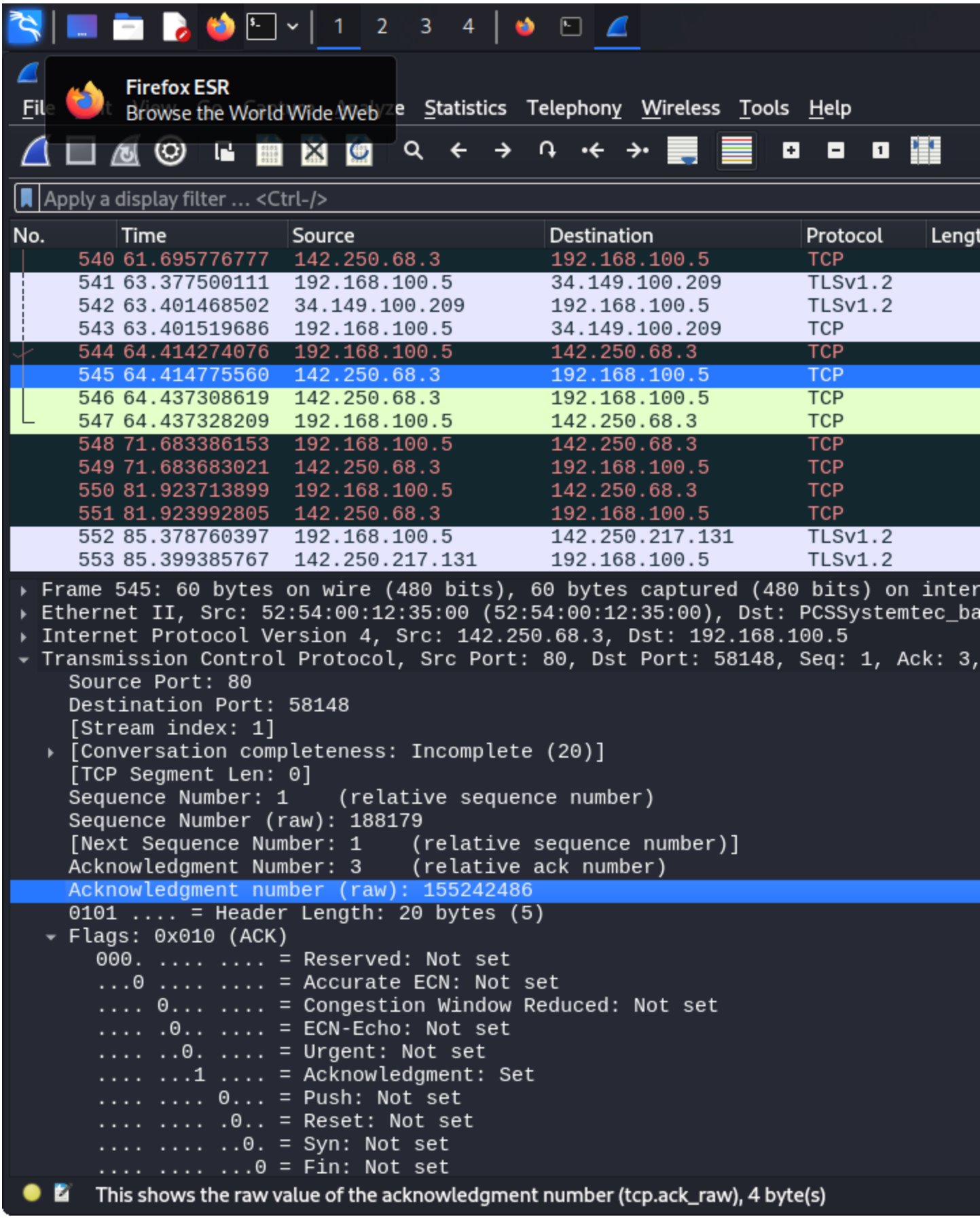

1 2 3 4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol
70 44.334654287 192.168.100.5 167.86.117.76 TLSv1.2
71 44.335134074 167.86.117.76 192.168.100.5 TCP
72 44.343092277 192.168.100.5 167.86.117.76 TLSv1.2
73 44.343807224 192.168.100.5 167.86.117.76 TLSv1.2
74 44.344410526 167.86.117.76 192.168.100.5 TCP
75 44.344416125 192.168.100.5 167.86.117.76 TLSv1.2
76 44.357622368 192.168.100.5 192.168.1.1 DNS
77 44.363849757 192.168.1.1 192.168.100.5 DNS
78 44.364585735 192.168.100.5 142.250.217.138 TCP
79 44.380985784 142.250.217.138 192.168.100.5 TCP
80 44.381059459 192.168.100.5 142.250.217.138 TCP
81 44.382284002 192.168.100.5 142.250.217.138 TLSv1.3
82 44.382619855 192.168.100.5 142.250.217.138 TLSv1.3
83 44.382752181 192.168.100.5 142.250.217.138 TLSv1.3
Frame 80: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on
Ethernet II, Src: PCSSystemtec_ba:e1:32 (08:00:27:ba:e1:32), Dst: 52:54
Internet Protocol Version 4, Src: 192.168.100.5, Dst: 142.250.217.138
Transmission Control Protocol, Src Port: 43864, Dst Port: 443, Seq: 1,
Source Port: 43864
Destination Port: 443
[Stream index: 10]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2184487436
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 317001
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....0 = Fin: Not set
wireshark_eth0C2TAT2.pcapng

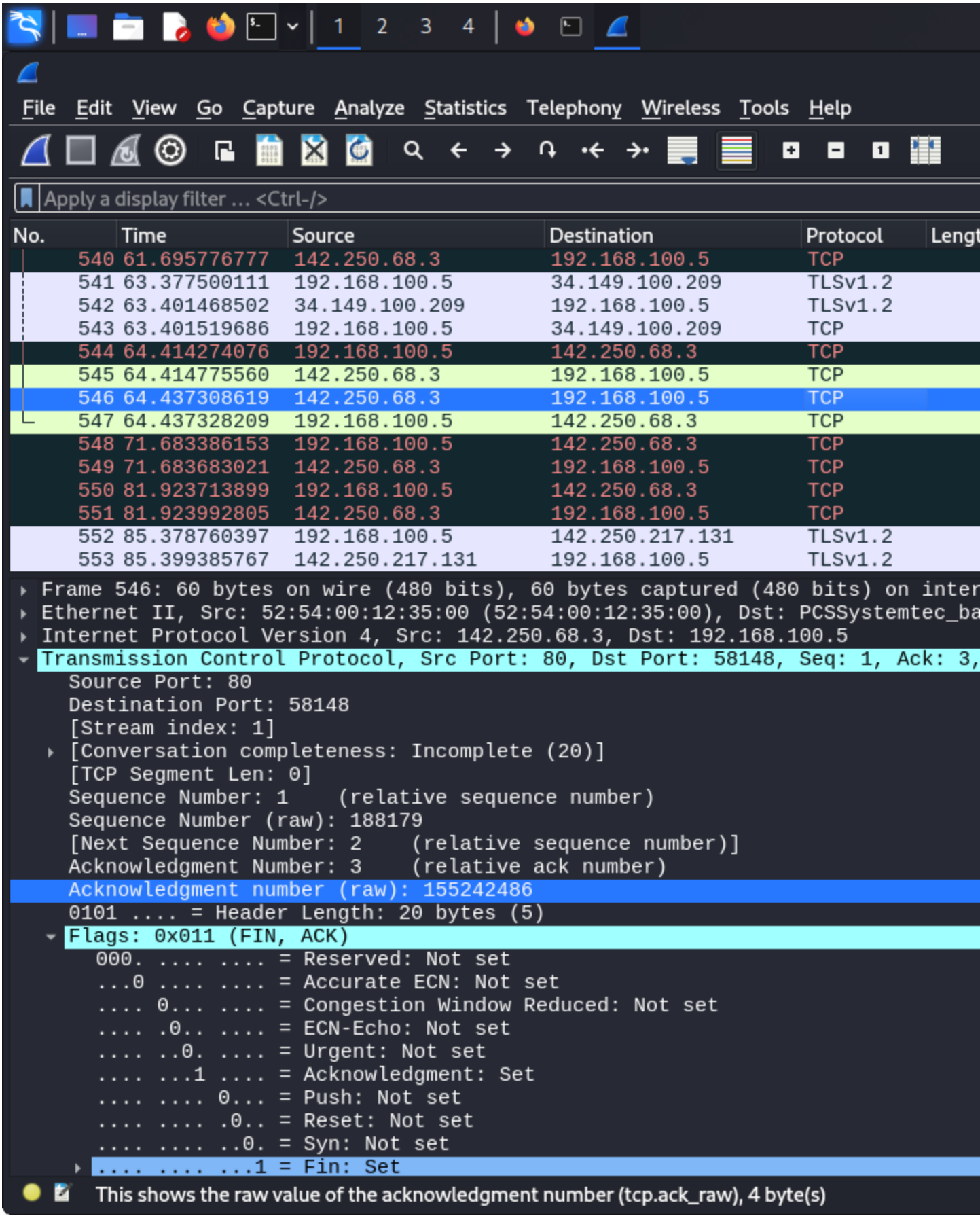

1 2 3 4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol
70 44.334654287 192.168.100.5 167.86.117.76 TLSv1.2
71 44.335134074 167.86.117.76 192.168.100.5 TCP
72 44.343092277 192.168.100.5 167.86.117.76 TLSv1.2
73 44.343807224 192.168.100.5 167.86.117.76 TLSv1.2
74 44.344410526 167.86.117.76 192.168.100.5 TCP
75 44.344416125 192.168.100.5 167.86.117.76 TLSv1.2
76 44.357622368 192.168.100.5 192.168.1.1 DNS
77 44.363849757 192.168.1.1 192.168.100.5 DNS
78 44.364585735 192.168.100.5 142.250.217.138 TCP
79 44.380985784 142.250.217.138 192.168.100.5 TCP
80 44.381059459 192.168.100.5 142.250.217.138 TCP
81 44.382284002 192.168.100.5 142.250.217.138 TLSv1.3
82 44.382619855 192.168.100.5 142.250.217.138 TLSv1.3
83 44.382752181 192.168.100.5 142.250.217.138 TLSv1.3
Frame 81: 726 bytes on wire (5808 bits), 726 bytes captured (5808 bits)
Ethernet II, Src: PCSSystemtec_ba:e1:32 (08:00:27:ba:e1:32), Dst: 52:54
Internet Protocol Version 4, Src: 192.168.100.5, Dst: 142.250.217.138
Transmission Control Protocol, Src Port: 43864, Dst Port: 443, Seq: 1,
Source Port: 43864
Destination Port: 443
[Stream index: 10]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 672]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2184487436
[Next Sequence Number: 673 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 317001
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....0 = Fin: Not set
wireshark_eth0C2TAT2.pcapng

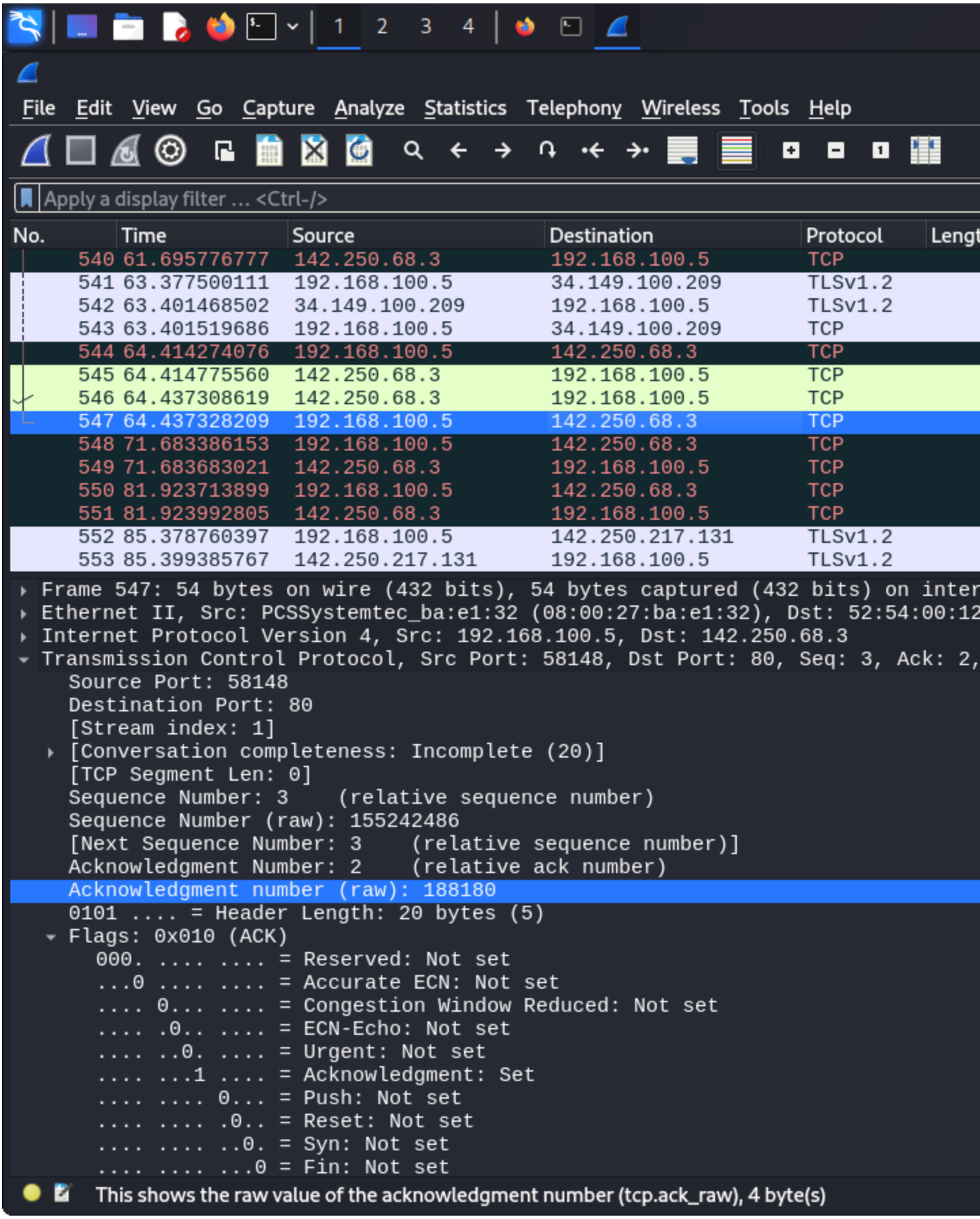
Session Termination: Identify the packets used to terminate the TCP session (FIN, FIN-ACK, ACK).

- **544,545,546,547 packets**


1 2 3 4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Lengt
540 61.695776777 142.250.68.3 192.168.100.5 TCP
541 63.377500111 192.168.100.5 34.149.100.209 TLSv1.2
542 63.401468502 34.149.100.209 192.168.100.5 TLSv1.2
543 63.401519686 192.168.100.5 34.149.100.209 TCP
544 64.414274076 192.168.100.5 142.250.68.3 TCP
545 64.414775560 142.250.68.3 192.168.100.5 TCP
546 64.437308619 142.250.68.3 192.168.100.5 TCP
547 64.437328209 192.168.100.5 142.250.68.3 TCP
548 71.683386153 192.168.100.5 142.250.68.3 TCP
549 71.683683021 142.250.68.3 192.168.100.5 TCP
550 81.923713899 192.168.100.5 142.250.68.3 TCP
551 81.923992805 142.250.68.3 192.168.100.5 TCP
552 85.378760397 192.168.100.5 142.250.217.131 TLSv1.2
553 85.399385767 142.250.217.131 192.168.100.5 TLSv1.2
Frame 544: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on inter
Ethernet II, Src: PCSSystemtec_ba:e1:32 (08:00:27:ba:e1:32), Dst: 52:54:00:12
Internet Protocol Version 4, Src: 192.168.100.5, Dst: 142.250.68.3
Transmission Control Protocol, Src Port: 58148, Dst Port: 80, Seq: 2, Ack: 1,
Source Port: 58148
Destination Port: 80
[Stream index: 1]
[Conversation completeness: Incomplete (20)]
[TCP Segment Len: 0]
Sequence Number: 2 (relative sequence number)
Sequence Number (raw): 155242485
[Next Sequence Number: 3 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 188179
0101 .... = Header Length: 20 bytes (5)
Flags: 0x011 (FIN, ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....1 = Fin: Set
wireshark_eth0C2TAT2.pcapng


1 2 3 4
Firefox ESR
Browse the World Wide Web
Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Lengt
540 61.695776777 142.250.68.3 192.168.100.5 TCP
541 63.377500111 192.168.100.5 34.149.100.209 TLSv1.2
542 63.401468502 34.149.100.209 192.168.100.5 TLSv1.2
543 63.401519686 192.168.100.5 34.149.100.209 TCP
544 64.414274076 192.168.100.5 142.250.68.3 TCP
545 64.414775560 142.250.68.3 192.168.100.5 TCP
546 64.437308619 142.250.68.3 192.168.100.5 TCP
547 64.437328209 192.168.100.5 142.250.68.3 TCP
548 71.683386153 192.168.100.5 142.250.68.3 TCP
549 71.683683021 142.250.68.3 192.168.100.5 TCP
550 81.923713899 192.168.100.5 142.250.68.3 TCP
551 81.923992805 142.250.68.3 192.168.100.5 TCP
552 85.378760397 192.168.100.5 142.250.217.131 TLSv1.2
553 85.399385767 142.250.217.131 192.168.100.5 TLSv1.2
Frame 545: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on inter
Ethernet II, Src: 52:54:00:12:35:00 (52:54:00:12:35:00), Dst: PCSSystemtec_ba
Internet Protocol Version 4, Src: 142.250.68.3, Dst: 192.168.100.5
Transmission Control Protocol, Src Port: 80, Dst Port: 58148, Seq: 1, Ack: 3,
Source Port: 80
Destination Port: 58148
[Stream index: 1]
[Conversation completeness: Incomplete (20)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 188179
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 3 (relative ack number)
Acknowledgment number (raw): 155242486
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....0 = Fin: Not set
This shows the raw value of the acknowledgment number (tcp.ack_raw), 4 byte(s)


1 2 3 4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Lengt
540 61.695776777 142.250.68.3 192.168.100.5 TCP
541 63.377500111 192.168.100.5 34.149.100.209 TLSv1.2
542 63.401468502 34.149.100.209 192.168.100.5 TLSv1.2
543 63.401519686 192.168.100.5 34.149.100.209 TCP
544 64.414274076 192.168.100.5 142.250.68.3 TCP
545 64.414775560 142.250.68.3 192.168.100.5 TCP
546 64.437308619 142.250.68.3 192.168.100.5 TCP
547 64.437328209 192.168.100.5 142.250.68.3 TCP
548 71.683386153 192.168.100.5 142.250.68.3 TCP
549 71.683683021 142.250.68.3 192.168.100.5 TCP
550 81.923713899 192.168.100.5 142.250.68.3 TCP
551 81.923992805 142.250.68.3 192.168.100.5 TCP
552 85.378760397 192.168.100.5 142.250.217.131 TLSv1.2
553 85.399385767 142.250.217.131 192.168.100.5 TLSv1.2
Frame 546: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on inter
Ethernet II, Src: 52:54:00:12:35:00 (52:54:00:12:35:00), Dst: PCSSystemtec_ba
Internet Protocol Version 4, Src: 142.250.68.3, Dst: 192.168.100.5
Transmission Control Protocol, Src Port: 80, Dst Port: 58148, Seq: 1, Ack: 3,
Source Port: 80
Destination Port: 58148
[Stream index: 1]
[Conversation completeness: Incomplete (20)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 188179
[Next Sequence Number: 2 (relative sequence number)]
Acknowledgment Number: 3 (relative ack number)
Acknowledgment number (raw): 155242486
0101 .... = Header Length: 20 bytes (5)
Flags: 0x011 (FIN, ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....1 = Fin: Set
This shows the raw value of the acknowledgment number (tcp.ack_raw), 4 byte(s)


1 2 3 4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Lengt
540 61.695776777 142.250.68.3 192.168.100.5 TCP
541 63.377500111 192.168.100.5 34.149.100.209 TLSv1.2
542 63.401468502 34.149.100.209 192.168.100.5 TLSv1.2
543 63.401519686 192.168.100.5 34.149.100.209 TCP
544 64.414274076 192.168.100.5 142.250.68.3 TCP
545 64.414775560 142.250.68.3 192.168.100.5 TCP
546 64.437308619 142.250.68.3 192.168.100.5 TCP
547 64.437328209 192.168.100.5 142.250.68.3 TCP
548 71.683386153 192.168.100.5 142.250.68.3 TCP
549 71.683683021 142.250.68.3 192.168.100.5 TCP
550 81.923713899 192.168.100.5 142.250.68.3 TCP
551 81.923992805 142.250.68.3 192.168.100.5 TCP
552 85.378760397 192.168.100.5 142.250.217.131 TLSv1.2
553 85.399385767 142.250.217.131 192.168.100.5 TLSv1.2
Frame 547: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on inter
Ethernet II, Src: PCSSystemtec_ba:e1:32 (08:00:27:ba:e1:32), Dst: 52:54:00:12
Internet Protocol Version 4, Src: 192.168.100.5, Dst: 142.250.68.3
Transmission Control Protocol, Src Port: 58148, Dst Port: 80, Seq: 3, Ack: 2,
Source Port: 58148
Destination Port: 80
[Stream index: 1]
[Conversation completeness: Incomplete (20)]
[TCP Segment Len: 0]
Sequence Number: 3 (relative sequence number)
Sequence Number (raw): 155242486
[Next Sequence Number: 3 (relative sequence number)]
Acknowledgment Number: 2 (relative ack number)
Acknowledgment number (raw): 188180
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....0 = Fin: Not set
This shows the raw value of the acknowledgment number (tcp.ack_raw), 4 byte(s)