

מבוא לרשתות תקשורת – תרגיל 2

סעיף א

תהליך הhandshake מתחיל עם העברת פקטת SYN – Synchronize מהקליינט המעוניין בחיבור, העברת Syn-Ack מהשרת על הפקטה ולבסוף העברת Ack מהקליינט שמכריע שהחיבור בוצע בהצלחה.

נראה זאת בהסנפת התעבורה בWireshark:

נתחיל עם הלקוח הראשון – מאזין לפורט 49600

שליחת הבקשה לסנכרון – Syn (כאשר 10.0.0.10 הוא אייפי הלקוח, 10.0.0.7 אייפי השרת)

The image shows a Wireshark packet capture of a TCP handshake. The packet list at the top shows several packets, with packet 6 (No. 6, Time 3.903925182) being the SYN packet from 10.0.0.10 to 10.0.0.7. The packet details pane shows the following information:

- Source Port: 49600
- Destination Port: 12345
- [Stream index: 0]
- [TCP Segment Len: 0]
- Sequence number: 1489256066
- [Next sequence number: 1489256066]
- Acknowledgment number: 0
- 1010 = Header Length: 40 bytes (10)
- Flags: 0x0c2 (SYN, ECN, CWR)
- Window size value: 29200

The packet bytes pane shows the raw data of the packet, including the header and the payload. The header is highlighted in blue, and the payload is shown in hexadecimal and ASCII.

Flags (12 bits) (tcp.flags), 2 bytes

Packets: 62 · Displayed: 15 (24.2%) · Dropped: 0 (0.0%) Profile: Default

לאחר מכן ניתן לראות שהשרת שולח בחזרה Ack על הsyn

The screenshot shows a Wireshark packet capture on interface *enp0s3. The packet list displays a series of TCP segments. The selected packet (No. 8) is a SYN-ACK from 10.0.0.10 to 10.0.0.7. The packet details pane shows the following information:

- Destination Port: 49600
- [Stream index: 0]
- [TCP Segment Len: 0]
- Sequence number: 764343584
- [Next sequence number: 764343584]
- Acknowledgment number: 1489256067
- 1000 ... = Header Length: 32 bytes (8)
- Flags: 0x012 (SYN, ACK)
- Window size value: 65535

The packet bytes pane shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates: Packets: 62 · Displayed: 15 (24.2%) · Dropped: 0 (0.0%) Profile: Default.

ולבסוף הקליינט שולח Ack ותהליך לחיצת הידיים מסתיים

The screenshot shows a Wireshark packet capture on interface *enp0s3. The packet list displays a series of TCP segments. The selected packet (No. 41) is an ACK from 10.0.0.10 to 10.0.0.7. The packet details pane shows the following information:

- Destination Port: 12345
- [Stream index: 0]
- [TCP Segment Len: 0]
- Sequence number: 1489256067
- [Next sequence number: 1489256067]
- Acknowledgment number: 764343585
- 0101 ... = Header Length: 20 bytes (5)
- Flags: 0x010 (ACK)
- Window size value: 229
- [Calculated window size: 29312]

The packet bytes pane shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates: Packets: 62 · Displayed: 15 (24.2%) · Dropped: 0 (0.0%) Profile: Default.

אפשר גם כן לראות את תהליך לחיצת הידיים מתבצע בתוך Flow Graph של התקשורת:

Wireshark · Flow · enp0s3

Time	10.0.0.10	10.0.0.7	Comment
3.903925182	49600	49600 → 12345 [SYN, ECN, CWR] Seq=14892560...	TCP: 49600 → 12345 [SYN, ECN, CWR] Seq=14892560...
3.904143307	49600	12345 → 49600 [SYN, ACK] Seq=764343584 Ack=...	TCP: 12345 → 49600 [SYN, ACK] Seq=764343584 Ack=...
3.904161918	49600	49600 → 12345 [ACK] Seq=1489256067 Ack=76...	TCP: 49600 → 12345 [ACK] Seq=1489256067 Ack=76...
6.266237149	49600	49600 → 12345 [PSH, ACK] Seq=1489256067 Ac...	TCP: 49600 → 12345 [PSH, ACK] Seq=1489256067 Ac...
6.266415943	49600	12345 → 49600 [ACK] Seq=764343585 Ack=148...	TCP: 12345 → 49600 [ACK] Seq=764343585 Ack=148...
6.267561597	49600	12345 → 49600 [PSH, ACK] Seq=764343585 Ack=...	TCP: 12345 → 49600 [PSH, ACK] Seq=764343585 Ack=...
6.267567832	49600	49600 → 12345 [ACK] Seq=1489256072 Ack=76...	TCP: 49600 → 12345 [ACK] Seq=1489256072 Ack=76...
14.507279605	49600	49600 → 12345 [PSH, ACK] Seq=1489256072 Ac...	TCP: 49600 → 12345 [PSH, ACK] Seq=1489256072 Ac...
14.507413258	49600	12345 → 49600 [ACK] Seq=764343590 Ack=148...	TCP: 12345 → 49600 [ACK] Seq=764343590 Ack=148...
14.508887744	49600	12345 → 49600 [PSH, ACK] Seq=764343590 Ack=...	TCP: 12345 → 49600 [PSH, ACK] Seq=764343590 Ack=...
14.508894980	49600	49600 → 12345 [ACK] Seq=1489256077 Ack=76...	TCP: 49600 → 12345 [ACK] Seq=1489256077 Ack=76...
16.700242139	49600	49600 → 12345 [FIN, ACK] Seq=1489256077 Ack=...	TCP: 49600 → 12345 [FIN, ACK] Seq=1489256077 Ack=...
16.700442716	49600	12345 → 49600 [ACK] Seq=764343595 Ack=148...	TCP: 12345 → 49600 [ACK] Seq=764343595 Ack=148...
19.486971840	49600	12345 → 49600 [FIN, ACK] Seq=764343595 Ack=...	TCP: 12345 → 49600 [FIN, ACK] Seq=764343595 Ack=...
19.486982603	49600	49600 → 12345 [ACK] Seq=1489256078 Ack=76...	TCP: 49600 → 12345 [ACK] Seq=1489256078 Ack=76...

Packet 7: TCP: 12345 → 49600 [SYN, ACK] Seq=764343...6067 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1

☒ Limit to display filter Flow type: All Flows Addresses: Any

כעת נעבור ללוקוח השני – מאזין לפורט 49602
 ניתן לראות את שלושת שלבי לחיצת הידיים, רק שכעת הפורט של הקליינט השתנה (הפורט של ה שרת כמובן נשאר קבוע)
 Client -> Syn -> Server
 Client <- Syn,Ack <- Server
 Client -> Ack -> Server

tcp.stream eq 1

No.	Time	Source	Destination	Protocol	Length	Source Port	Dest. Port	Info
37	19.486502223	10.0.0.10	10.0.0.7	TCP	74	49602	12345	49602 → 12345 [SYN, ECN, CWR] Seq=2721584261 Win=0 Len=0
38	19.486709843	10.0.0.7	10.0.0.10	TCP	66	12345	49602	12345 → 49602 [SYN, ACK] Seq=310404142 Ack=2721584261 Win=0 Len=0
39	19.486732819	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345 [ACK] Seq=2721584262 Ack=310404143 Win=0 Len=0
44	21.537238494	10.0.0.10	10.0.0.7	TCP	59	49602	12345	49602 → 12345 [PSH, ACK] Seq=2721584267 Ack=310404143 Win=0 Len=0
45	21.537373610	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602 [ACK] Seq=310404143 Ack=2721584267 Win=0 Len=0
46	21.538328394	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602 [PSH, ACK] Seq=310404143 Ack=2721584267 Win=0 Len=0
47	21.538360854	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345 [ACK] Seq=2721584267 Ack=310404143 Win=0 Len=0
51	24.702338621	10.0.0.10	10.0.0.7	TCP	59	49602	12345	49602 → 12345 [PSH, ACK] Seq=2721584267 Ack=310404143 Win=0 Len=0
52	24.702569504	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602 [ACK] Seq=310404148 Ack=2721584267 Win=0 Len=0
53	24.703769107	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602 [PSH, ACK] Seq=310404148 Ack=2721584267 Win=0 Len=0
54	24.703788962	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345 [ACK] Seq=2721584272 Ack=310404148 Win=0 Len=0
58	27.294905667	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345 [FIN, ACK] Seq=2721584272 Ack=310404148 Win=0 Len=0
59	27.295106364	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602 [ACK] Seq=310404153 Ack=2721584272 Win=0 Len=0

Source Port: 49602
 Destination Port: 12345
 [Stream index: 1]
 [TCP Segment Len: 0]
 Sequence number: 2721584261
 [Next sequence number: 2721584261]
 Acknowledgment number: 0
 1010 = Header Length: 40 bytes (10)
 Flags: 0x0c2 (SYN, ECN, CWR)
 Window size value: 29200

Flags (12 bits) (tcp.flags, 2 bytes)

Packets: 62 · Displayed: 13 (21.0%) · Dropped: 0 (0.0%) · Profile: Default

:Flow Graph

Wireshark · Flow · enp0s3

Time	10.0.0.10	10.0.0.7	Comment
19.486502223	49602	12345	TCP: 49602 → 12345 [SYN, ECN, CWR] Seq=2721584261 Win=0 Len=0
19.486709843	12345	49602	TCP: 12345 → 49602 [SYN, ACK] Seq=310404142 Ack=2721584261 Win=0 Len=0
19.486732819	49602	12345	TCP: 49602 → 12345 [ACK] Seq=2721584262 Ack=310404143 Win=0 Len=0
21.537238494	49602	12345	TCP: 49602 → 12345 [PSH, ACK] Seq=2721584267 Ack=310404143 Win=0 Len=0
21.537373610	49602	12345	TCP: 12345 → 49602 [ACK] Seq=310404143 Ack=2721584267 Win=0 Len=0
21.538328394	49602	12345	TCP: 12345 → 49602 [PSH, ACK] Seq=310404143 Ack=2721584267 Win=0 Len=0
21.538360854	49602	12345	TCP: 49602 → 12345 [ACK] Seq=2721584267 Ack=310404143 Win=0 Len=0
24.702338621	49602	12345	TCP: 49602 → 12345 [PSH, ACK] Seq=2721584267 Ack=310404143 Win=0 Len=0
24.702569504	49602	12345	TCP: 12345 → 49602 [ACK] Seq=310404148 Ack=2721584267 Win=0 Len=0
24.703769107	49602	12345	TCP: 12345 → 49602 [PSH, ACK] Seq=310404148 Ack=2721584267 Win=0 Len=0
24.703788962	49602	12345	TCP: 49602 → 12345 [ACK] Seq=2721584272 Ack=310404148 Win=0 Len=0
27.294905667	49602	12345	TCP: 49602 → 12345 [FIN, ACK] Seq=2721584272 Ack=310404148 Win=0 Len=0
27.295106364	49602	12345	TCP: 12345 → 49602 [ACK] Seq=310404153 Ack=2721584272 Win=0 Len=0

Packet 44: TCP: 49602 → 12345 [PSH, ACK] Seq=2721584262 Ack=310404143 Win=29312 Len=5

☒ Limit to display filter

Flow type: All Flows

Addresses: Any

Reset

Close Save As...

סעיף ב

כעת נעבור על החבילות ששלחו את ההדעות עצמן (Worldi Hello) מצד הלקוחות:
החבילה שנשלחה לאחר חבילתה Ack על Syn, Ack היא החבילה שהעבירה את hello:

The image shows a Wireshark packet capture analysis of a TCP connection. The packet list at the top shows a sequence of packets, with packet 44 selected. The packet details pane shows the Transmission Control Protocol (TCP) segment with Source Port 49602, Destination Port 12345, Sequence Number 2721584262, and Acknowledgment Number 310404143. The packet length is 59 bytes. The packet bytes pane shows the raw data, including the 'hello' string.

נעבור על כל רכיב בהדר של החבילה:

Source Port – כמובן שפורט המקור שלנו הוא הפורט שהקליינט מאזין לו – 49602

Destination Port – ופורט היעד הוא הפורט שהשרת מאזין לו – 12345

Sequence Number – הSequence Number שנשלח גדול ב1 מהמספר (שנבחר באופן רנדומלי) כאשר נשלחה חבילת הSyn, כעת הוא 2721584262, והוא היה 2721584261. הוא עלה ב1 כיוון שהשרת קיבל בAck והעלה את הAck Number ב1. (פקטות SYN מעלות ב1).

Ack Number – מתחיל ב0, ואז מתחיל Offset ממספר רנדומלי גם כן, במקרה שלנו 310404143.

Length – גודל החבילה, במקרה שלנו 5 בתים (hello) + ההדר

מוטב לציין כי בכל חבילה אחרי הSyn, פרוטוקול הTCP שולח את דגל הAck דלוק כיוון שכל חבילה שולחת את מספר הAck העדכני ביותר.

כעת נוכל לראות את ה Ack של השרת להודעת hello

The image shows a Wireshark capture of a TCP connection. The packet list at the top shows several packets, including a SYN packet (No. 37) and several ACK packets. The packet details for packet 45 show a TCP ACK segment with Seq=310404143 and Ack=2721584267. The packet bytes at the bottom show the raw data of the ACK segment.

No.	Time	Source	Destination	Protocol	Length	Source Port	Dest. Port	Info
37	19.486502223	10.0.0.10	10.0.0.7	TCP	74	49602	12345	49602 → 12345 [SYN, ECN, CWR] Seq=27215842
38	19.486709843	10.0.0.7	10.0.0.10	TCP	66	12345	49602	49602 → 12345 [SYN, ACK] Seq=310404142 Ack=
39	19.486732819	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345 [ACK] Seq=2721584262 Ack=310
44	21.537238494	10.0.0.10	10.0.0.7	TCP	59	49602	12345	49602 → 12345 [PSH, ACK] Seq=2721584262 Ac
45	21.537373610	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602 [ACK] Seq=310404143 Ack=2721
46	21.538328394	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602 [PSH, ACK] Seq=310404143 Ack
47	21.538360854	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345 [ACK] Seq=2721584267 Ack=310
51	24.702338621	10.0.0.10	10.0.0.7	TCP	59	49602	12345	49602 → 12345 [PSH, ACK] Seq=2721584267 Ac
52	24.702569504	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602 [ACK] Seq=310404148 Ack=2721
53	24.703769107	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602 [PSH, ACK] Seq=310404148 Ack
54	24.703788962	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345 [ACK] Seq=2721584272 Ack=310
58	27.294905667	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345 [FIN, ACK] Seq=2721584272 Ac
59	27.295106364	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602 [ACK] Seq=310404153 Ack=2721

Frame 45: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 Ethernet II, Src: Giga-Byt_54:ec:28 (40:8d:5c:54:ec:28), Dst: PcsCompu_7d:1b:f7 (08:00:27:7d:1b:f7)
 Internet Protocol Version 4, Src: 10.0.0.7, Dst: 10.0.0.10
 Transmission Control Protocol, Src Port: 12345, Dst Port: 49602, Seq: 310404143, Ack: 2721584267, Len: 0
 Source Port: 12345
 Destination Port: 49602
 [Stream index: 1]
 [TCP Segment Len: 0]
 Sequence number: 310404143
 [Next sequence number: 310404143]
 Acknowledgment number: 2721584267
 0101 = Header Length: 20 bytes (5)
 Flags: 0x010 (ACK)
 Window size value: 2053
 [Calculated window size: 525568]
 [Window size scaling factor: 256]
 Checksum: 0x7450 [unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0
 [SEQ/ACK analysis]
 [Timestamps]

0000 08 00 27 7d 1b f7 40 8d 5c 54 ec 28 08 00 45 00 ..'.@. \T.(.E.
 0010 00 28 65 af 40 00 80 06 81 10 0a 00 00 07 0a 00 .(e.@.....
 0020 00 0a 30 39 c1 c2 12 80 64 2f a2 38 14 8b 50 10 ..09.... d/.B. P.
 0030 08 05 74 50 00 00 00 00 00 00 00 00 00 00 00 ..tP.....

הפורטים כמובן הפוכים, היעד הוא 49602 (הלקוח) והמקור הוא 12345 (השרת)
 הוא עושה Ack על ה Seq Number שהתקבל מהלקוח + 5 הבתים של גודל החבילה ושולח את ה
 Seq Num שעליו הלקוח עשה Ack (כיוון שהוא לא שלח הודעה לפני כן)
 גודל החבילה הוא 0 ללא ההדר כיוון שאין בעצם payload, החבילה היא רק Ack על חבילת hello.

נסתכל על החבילה שהשרת שולח ללקוח לאחר מכן, החבילה עם HELLO

The image shows a Wireshark packet capture on interface `enp0s3`. The filter is `tcp.stream eq 1`. The selected packet is packet 46, a TCP segment from source `10.0.0.10` to destination `10.0.0.7`. The details pane shows the following information:

- Frame 46: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- Ethernet II, Src: Giga-Byt_54:ec:28 (40:8d:5c:54:ec:28), Dst: PcsCompu_7d:1b:f7 (08:00:27:7d:1b:f7)
- Internet Protocol Version 4, Src: 10.0.0.7, Dst: 10.0.0.10
- Transmission Control Protocol, Src Port: 12345, Dst Port: 49602, Seq: 310404143, Ack: 2721584267, Len: 5
 - Source Port: 12345
 - Destination Port: 49602
 - [Stream index: 1]
 - [TCP Segment Len: 5]
 - Sequence number: 310404143
 - [Next sequence number: 310404148]
 - Acknowledgment number: 2721584267
 - 0101 = Header Length: 20 bytes (5)
 - Flags: 0x018 (PSH, ACK)
 - Window size value: 2053
 - [Calculated window size: 525568]
 - [Window size scaling factor: 256]
 - Checksum: 0x90b1 [unverified]
 - [Checksum Status: Unverified]
 - Urgent pointer: 0
 - [SEQ/ACK analysis]
 - [Timestamps]
 - TCP payload (5 bytes)
- Data (5 bytes)
 - Data: 48454c4cf
 - [Length: 5]

The packet bytes pane shows the raw data in hexadecimal and ASCII. The ASCII representation shows the string `HELLO`.

הפורטים זהים לחבילה הקודמת, מהשרת ללקוח, כיוון שלא התקבלה שום חבילה מהלקוח וה Sequence Number ו Ack Number נשארים זהים. גודל החבילה יהיה 5 בתים בעקבות הודעת ה HELLO לא כולל ההדר הלקוח כעת שולח Ack על החבילה שהתקבלה.

Wireshark interface showing a packet capture on interface *enp0s3. The filter is set to tcp.stream eq 1.

No.	Time	Source	Destination	Protocol	Length	Source Port	Dest. Port	Info
37	19.486502223	10.0.0.10	10.0.0.7	TCP	74	49602	12345	49602 → 12345 [SYN, ECN, CWR] Seq=2721584267
38	19.486709843	10.0.0.7	10.0.0.10	TCP	66	12345	49602	49602 → 12345 [SYN, ACK] Seq=310404142 Ack=2721584267
39	19.486732819	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345 [ACK] Seq=2721584267 Ack=310404142
44	21.537238494	10.0.0.10	10.0.0.7	TCP	59	49602	12345	49602 → 12345 [PSH, ACK] Seq=2721584267 Ack=310404142
45	21.537373610	10.0.0.7	10.0.0.10	TCP	60	12345	49602	49602 → 12345 [ACK] Seq=310404143 Ack=2721584267
46	21.538328394	10.0.0.7	10.0.0.10	TCP	60	12345	49602	49602 → 12345 [PSH, ACK] Seq=310404143 Ack=2721584267
47	21.538360854	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345 [ACK] Seq=2721584267 Ack=310404143
51	24.702338621	10.0.0.10	10.0.0.7	TCP	59	49602	12345	49602 → 12345 [PSH, ACK] Seq=2721584267 Ack=310404148
52	24.702569504	10.0.0.7	10.0.0.10	TCP	60	12345	49602	49602 → 12345 [ACK] Seq=310404148 Ack=2721584267
53	24.703769107	10.0.0.7	10.0.0.10	TCP	60	12345	49602	49602 → 12345 [PSH, ACK] Seq=310404148 Ack=2721584267
54	24.703789962	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345 [ACK] Seq=2721584272 Ack=310404148
58	27.204905667	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345 [FIN, ACK] Seq=2721584272 Ack=310404153
59	27.295106364	10.0.0.7	10.0.0.10	TCP	60	12345	49602	49602 → 12345 [ACK] Seq=310404153 Ack=2721584272

Frame 47: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
 Ethernet II, Src: PcsCompu_7d:1b:f7 (08:00:27:7d:1b:f7), Dst: Giga-Byt_54:ec:28 (40:8d:5c:54:ec:28)
 Internet Protocol Version 4, Src: 10.0.0.10, Dst: 10.0.0.7
 Transmission Control Protocol, Src Port: 49602, Dst Port: 12345, Seq: 2721584267, Ack: 310404148, Len: 0
 Destination Port: 12345
 [Stream index: 1]
 [TCP Segment Len: 0]
 Sequence number: 2721584267
 [Next sequence number: 2721584267]
 Acknowledgment number: 310404148
 0101 = Header Length: 20 bytes (5)
 Flags: 0x010 (ACK)
 Window size value: 229
 [Calculated window size: 29312]
 [Window size scaling factor: 128]
 Checksum: 0x142b [unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0
 [SEQ/ACK analysis]
 [Timestamps]

0000 40 8d 5c 54 ec 28 08 00 27 7d 1b f7 08 00 45 00 @.\T.(..')....E-
 0010 00 28 1e 1f 40 00 40 06 08 a1 0a 00 00 0a 0a 00 -(.-@.@.....
 0020 00 07 c1 c2 30 39 a2 38 14 8b 12 80 64 34 50 1009.8d4P
 0030 00 e5 14 2b 00 00+..

Wireshark enp0s3_20181213115721_x4NG3A.pcapng Packets: 62 - Displayed: 13 (21.0%) - Dropped: 0 (0.0%) Profile: Default

הלקוח מאשר את הSEQ שנשלח מהשרת + 5 (גודל החבילה)
 שולח את Seq שלו + 5 מההודעה הקודמת שהוא שלח (הhello הרגיל)

נעבור להודעת הworld של הקליינט:

tcp.stream eq 1

No.	Time	Source	Destination	Protocol	Length	Source Port	Dest. Port	Info
37	19.486592223	10.0.0.10	10.0.0.7	TCP	74	49602	12345	49602 → 12345 [SYN, ECN, CWR] Seq=2721584267
38	19.486709843	10.0.0.7	10.0.0.10	TCP	66	12345	49602	49602 → 12345 [SYN, ACK] Seq=310404142 Ack=2721584267
39	19.486732819	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345 [ACK] Seq=2721584262 Ack=310404142
44	21.537238494	10.0.0.10	10.0.0.7	TCP	59	49602	12345	49602 → 12345 [PSH, ACK] Seq=2721584262 Ack=310404142
45	21.537373610	10.0.0.7	10.0.0.10	TCP	60	12345	49602	49602 → 12345 [ACK] Seq=310404143 Ack=2721584262
46	21.538328394	10.0.0.7	10.0.0.10	TCP	60	12345	49602	49602 → 12345 [PSH, ACK] Seq=310404143 Ack=2721584262
47	21.538360854	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345 [ACK] Seq=2721584267 Ack=310404143
51	24.702338621	10.0.0.10	10.0.0.7	TCP	59	49602	12345	49602 → 12345 [PSH, ACK] Seq=2721584267 Ack=310404148
52	24.702569504	10.0.0.7	10.0.0.10	TCP	60	12345	49602	49602 → 12345 [ACK] Seq=310404148 Ack=2721584267
53	24.703769107	10.0.0.7	10.0.0.10	TCP	60	12345	49602	49602 → 12345 [PSH, ACK] Seq=310404148 Ack=2721584267
54	24.703788962	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345 [ACK] Seq=2721584272 Ack=310404148
58	27.294905667	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345 [FIN, ACK] Seq=2721584272 Ack=310404153
59	27.295106364	10.0.0.7	10.0.0.10	TCP	60	12345	49602	49602 → 12345 [ACK] Seq=310404153 Ack=2721584272

Frame 51: 59 bytes on wire (472 bits), 59 bytes captured (472 bits) on interface 0
 Ethernet II, Src: PcsCompu_7d:1b:f7 (08:00:27:7d:1b:f7), Dst: Giga-Byt_54:ec:28 (40:8d:5c:54:ec:28)
 Internet Protocol Version 4, Src: 10.0.0.10, Dst: 10.0.0.7
 Transmission Control Protocol, Src Port: 49602, Dst Port: 12345, Seq: 2721584267, Ack: 310404148, Len: 5
 Source Port: 49602
 Destination Port: 12345
 [Stream index: 1]
 [TCP Segment Len: 5]
 Sequence number: 2721584267
 [Next sequence number: 2721584272]
 Acknowledgment number: 310404148
 0101 ... = Header Length: 20 bytes (5)
 Flags: 0x018 (PSH, ACK)
 Window size value: 229
 [Calculated window size: 29312]
 [Window size scaling factor: 128]
 Checksum: 0x1430 [unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0
 [SEQ/ACK analysis]
 [Timestamps]
 TCP payload (5 bytes)
 Data (5 bytes)
 Data: 776f726c64
 [Length: 5]

0000 40 8d 5c 54 ec 28 08 00 27 7d 1b f7 08 00 45 00 @.T(..'):...E.
 0010 00 2d 1e 20 40 00 40 06 08 9b 0a 00 00 0a 0a 00 ... @ @
 0020 00 07 c1 c2 30 39 a2 38 14 8b 12 80 64 34 50 18 ...09.8...d4P.
 0030 00 e5 14 30 00 00 77 6f 72 6c 64 ...0-wo.rld

Data (data.data), 5 bytes

Packets: 62 · Displayed: 13 (21.0%) · Dropped: 0 (0.0%) · Profile: Default

ה Ack וה Seq נשארים זהים כי לא הייתה תעבורה שהתקבלה מהשרת. גודל החבילה הוא 5 (world) ללא ההדר הפורטים הם מהלקוח (49602) לשרת (12345)

והAck מהשרת על הודעת הworld:

Wireshark packet capture analysis of a TCP stream. The packet list shows a sequence of packets from source 10.0.0.10 to destination 10.0.0.7. Packet 52 is highlighted, showing a TCP ACK segment with sequence number 310404148 and acknowledgment number 2721584272. The packet details pane shows the structure of the TCP header and the ACK flag. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Source Port	Dest. Port	Info
37	19.486502223	10.0.0.10	10.0.0.7	TCP	74	49602	12345	49602 → 12345 [SYN, ECN, CWR] Seq=27215842
38	19.486709843	10.0.0.7	10.0.0.10	TCP	66	12345	49602	49602 → 12345 [SYN, ACK] Seq=310404142 Ack=
39	19.486732819	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345 [ACK] Seq=2721584262 Ack=310
44	21.537238494	10.0.0.10	10.0.0.7	TCP	59	49602	12345	49602 → 12345 [PSH, ACK] Seq=2721584262 Ac
45	21.537373610	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602 [ACK] Seq=310404143 Ack=2721
46	21.538328394	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602 [PSH, ACK] Seq=310404143 Ack
47	21.538360854	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345 [ACK] Seq=2721584267 Ack=310
51	24.702338621	10.0.0.10	10.0.0.7	TCP	59	49602	12345	49602 → 12345 [PSH, ACK] Seq=2721584267 Ac
52	24.702569504	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602 [ACK] Seq=310404148 Ack=2721
53	24.703769107	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602 [PSH, ACK] Seq=310404148 Ack
54	24.703788962	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345 [ACK] Seq=2721584272 Ack=310
58	27.294905667	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345 [FIN, ACK] Seq=2721584272 Ac
59	27.295106364	10.0.0.7	10.0.0.10	TCP	60	12345	49602	49602 → 12345 [ACK] Seq=310404153 Ack=2721

Frame 52: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Giga-Byt_54:ec:28 (40:8d:5c:54:ec:28), Dst: PcsCompu_7d:1b:f7 (08:00:27:7d:1b:f7)
Internet Protocol Version 4, Src: 10.0.0.7, Dst: 10.0.0.10
Transmission Control Protocol, Src Port: 12345, Dst Port: 49602, Seq: 310404148, Ack: 2721584272, Len: 0
Source Port: 12345
Destination Port: 49602
[Stream index: 1]
[TCP Segment Len: 0]
Sequence number: 310404148
[Next sequence number: 310404148]
Acknowledgment number: 2721584272
0101 ... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window size value: 2053
[Calculated window size: 525568]
[Window size scaling factor: 256]
Checksum: 0x7446 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]

0000 08 00 27 7d 1b f7 40 8d 5c 54 ec 28 08 00 45 00 ...')...@... \T... (..E..
0010 00 28 65 b4 40 00 80 06 81 0b 0a 00 00 07 0a 00 ... (e@... ..
0020 00 0a 30 39 c1 c2 12 80 64 34 a2 38 14 90 50 10 ...09... d4.8..P..
0030 08 05 74 46 00 00 00 00 00 00 00 00 ...tF... ..

wireshark_enp0s3_20181213115721_x4NG3A.pcapng Packets: 62 · Displayed: 13 (21.0%) · Dropped: 0 (0.0%) Profile: Default

הוא שולח Ack Num של Seq שהלקוח שלח + 5 (גודל ההודעה), ושולח Seq של אותו המספר שהלקוח עשה לו Ack פעם שעברה כי הוא לא שלח שום הודעה מאז שהלקוח קיבל את ההודעה הקודמת

נעבור לשליחת ההודעה WORLD מצד השרת

tcp.stream eq 1

No.	Time	Source	Destination	Protocol	Length	Source Port	Dest. Port	Info
44	21.537238494	10.0.0.10	10.0.0.7	TCP	59	49602	12345	12345 → 49602
45	21.537373610	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602
46	21.538328394	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602
47	21.538360854	10.0.0.10	10.0.0.7	TCP	54	49602	12345	12345 → 49602
51	24.702338621	10.0.0.10	10.0.0.7	TCP	59	49602	12345	12345 → 49602
52	24.702569504	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602
53	24.703769107	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602
54	24.703788962	10.0.0.10	10.0.0.7	TCP	54	49602	12345	12345 → 49602
58	27.294905667	10.0.0.10	10.0.0.7	TCP	54	49602	12345	12345 → 49602
59	27.295106364	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602

Frame 53: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 Ethernet II, Src: Giga-Byt_54:ec:28 (40:8d:5c:54:ec:28), Dst: PcsCompu_7d:1b:f7 (08:00:27:7d:1b:f7)
 Internet Protocol Version 4, Src: 10.0.0.7, Dst: 10.0.0.10
 Transmission Control Protocol, Src Port: 12345, Dst Port: 49602, Seq: 310404148, Ack: 2721584272, Len: 5
 Source Port: 12345
 Destination Port: 49602
 [Stream index: 1]
 [TCP Segment Len: 5]
 Sequence number: 310404148
 [Next sequence number: 310404153]
 Acknowledgment number: 2721584272
 0101 = Header Length: 20 bytes (5)
 Flags: 0x018 (PSH, ACK)
 Window size value: 2053
 [Calculated window size: 525568]
 [Window size scaling factor: 256]
 Checksum: 0x869d [unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0
 [SEQ/ACK analysis]
 [Timestamps]
 TCP payload (5 bytes)
 Data (5 bytes)
 Data: 574f524c44
 0000 08 00 27 7d 1b f7 40 8d 5c 54 ec 28 08 00 45 00 ..'}...@. \T.(...E.
 0010 00 2d 65 b5 40 00 80 06 81 05 0a 00 00 07 0a 00 ..-e.@... ..
 0020 00 0a 30 39 c1 c2 12 80 64 34 a2 38 14 90 50 18 ..09.... d4.8..P.
 0030 08 05 86 9d 00 00 57 4f 52 4c 44 00WORLD..

The window size scaling factor (---window_size_scalefactor), 2 byte: Packets: 62 · Displayed: 13 (21.0%) · Dropped: 0 (0.0%) Profile: Default

השרת שולח אותו SEQ NUMBER כיוון ששליחת הACK לא העלתה אותו, וכן אותו ACK NUMBER כיוון שהלקוח לא שלח משהו חדש מאז.
 הפורטים הם מצד השרת 12345 ללקוח 49602, גודל החבילה הוא 5 (WORLD)

ולבסוף הלקוח שולח ACK על הודעת הWORLD

The image displays a Wireshark packet capture analysis of a TCP stream. The top pane shows a list of packets, with packet 54 selected. The middle pane shows the details of packet 54, highlighting the 'Window size scaling factor: 128' field. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Source Port	Dest. Port	Info
44	21.537238494	10.0.0.10	10.0.0.7	TCP	59	49602	12345	49602 → 12345
45	21.537373610	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602
46	21.538328394	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602
47	21.538360854	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345
51	24.702338621	10.0.0.10	10.0.0.7	TCP	59	49602	12345	49602 → 12345
52	24.702569504	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602
53	24.703769107	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602
54	24.703788962	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345
58	27.294905667	10.0.0.10	10.0.0.7	TCP	54	49602	12345	49602 → 12345
59	27.295106364	10.0.0.7	10.0.0.10	TCP	60	12345	49602	12345 → 49602

Frame 54: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
 Ethernet II, Src: PcsCompu_7d:1b:f7 (08:00:27:7d:1b:f7), Dst: Giga-Byt_54:ec:28 (40:8d:5c:54:ec:28)
 Internet Protocol Version 4, Src: 10.0.0.10, Dst: 10.0.0.7
 Transmission Control Protocol, Src Port: 49602, Dst Port: 12345, Seq: 2721584272, Ack: 310404153, Len: 0
 Source Port: 49602
 Destination Port: 12345
 [Stream index: 1]
 [TCP Segment Len: 0]
 Sequence number: 2721584272
 [Next sequence number: 2721584272]
 Acknowledgment number: 310404153
 0101 = Header Length: 20 bytes (5)
 Flags: 0x010 (ACK)
 Window size value: 229
 [Calculated window size: 29312]
 [Window size scaling factor: 128]
 Checksum: 0x142b [unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0
 [SEQ/ACK analysis]
 [Timestamps]

0000 40 8d 5c 54 ec 28 08 00 27 7d 1b f7 08 00 45 00 @. \T. (. ') E.
 0010 00 28 1e 21 40 00 40 06 08 9f 0a 00 00 0a 0a 00 . (. ! @ . @
 0020 00 07 c1 c2 30 39 a2 38 14 90 12 80 64 39 50 10 09 . 8 d9 P.
 0030 00 e5 14 2b 00 00 + . . .

The window size scaling factor (....window size scalefactor), 2 byte Packets: 62 · Displayed: 13 (21.0%) · Dropped: 0 (0.0%) Profile: Default

הלקוח שולח ACK NUMBER עם SEQ NUMBER שהוא קיבל מהשרת + 5 בתים של גודל החבילה

וכן SEQ NUMBER שהוא שולח גדול ב 5 מאז החבילה האחרונה שהוא שלח (worldn הקטן שגודלו גם היה 5)

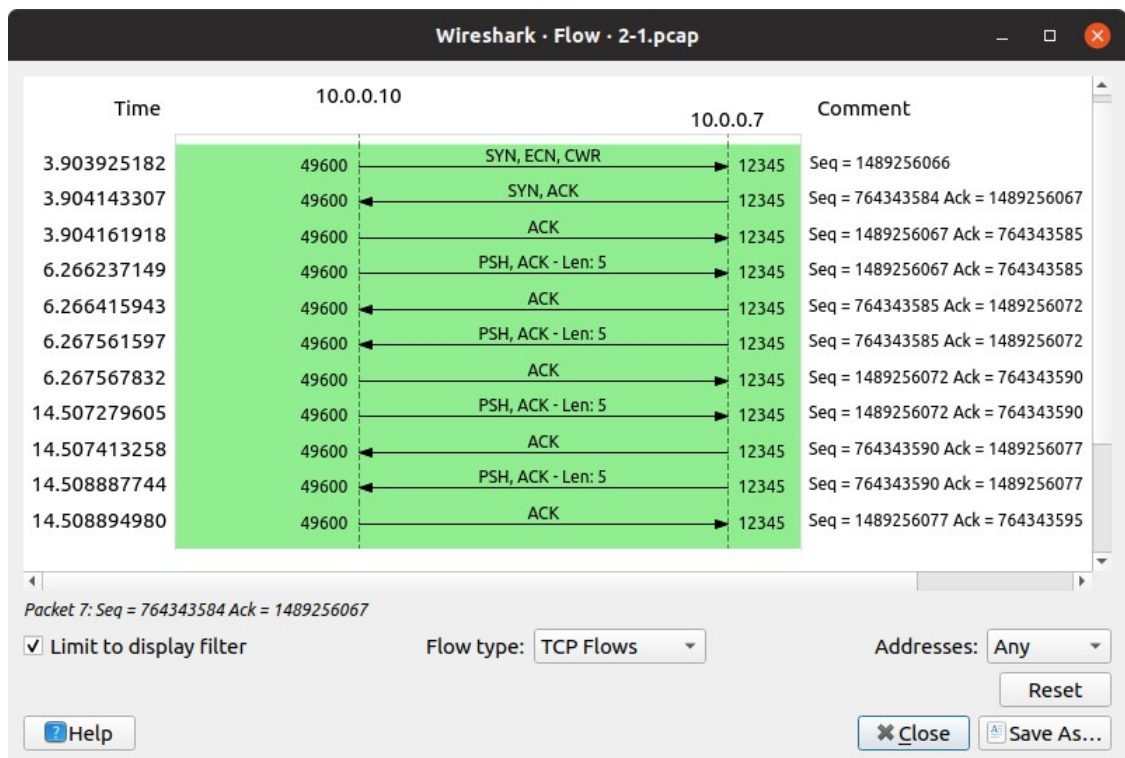
הפורטים הם מהלקוח 49602 לשרת 12345 וגודל החבילה כאומר הוא 5 ללא ההדר.

כעת נתבונן בקצרה על התעבורה של הלקוח הראשון מול השרת:

The image shows a Wireshark packet capture of a TCP connection establishment. The packet list at the top shows a SYN packet (No. 7) and its corresponding ACK (No. 8). The packet details for the ACK show the sequence number 764343584 and acknowledgment number 1489256067. The packet bytes show the raw data in hexadecimal and ASCII.

הלקוח שולח את החבילה הראשונה אחרי הקמת החיבור, נבחר מספר סידורי 1489256067, שהתחיל ב 1 פחות אבל עלה בעקבות הSYN לפני כן. השרת עשה ACK לאותו הSYN בהתחלה ובחר מספר סידורי גם כן (764343585) שהקליינט עשה לה ACK. לאחר שליחת הודעת הhello (בגודל כולל הדר של 59) השרת עושה ACK לחבילה, כלומר ACK לSEQ שהקליינט שלח + 5 בייטים כגודל התוכן. כעת השרת שולח (עם אותו SEQ של הPACKET הקודמת ששלח ואותו ACK) את ההודעה שלו (HELLO הקליינט מאשר את ההודעה, עושה ACK לSEQ שהשרת שלח + 5, שולח את הSEQ שלו + 5 מההודעה הקודמת ששלח (hello) השרת מקבל עם ACK, והתהליך חוזר חלילה באותם Offsets לגבי world.

ניתן לראות את התהליך מתבצע טוב ע"י Flow Chart

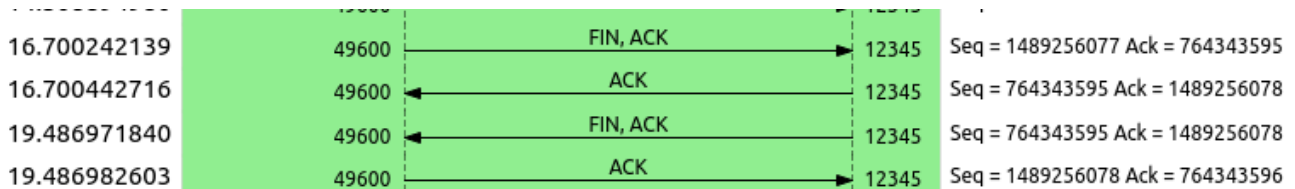


סעיף ג

כעת נסביר את תהליך ה־Teardown ע"י החבילות שלנו. תהליך ה־teardown הוא תהליך ניתוק החיבור בין שני הצדדים, והוא מתבצע בעזרת שימוש ה־fin flag שמעיד על רצון לסגור את החיבור.

Wireshark packet capture showing a TCP FIN, ACK sequence. The packet list shows a FIN, ACK packet from 10.0.0.10 to 10.0.0.7. The packet details show the flags as FIN, ACK and the sequence number as 1489256077. The packet bytes show the raw data.

ברגע שהלקוח רושם quit, במקום לשלוח את ההודעה התכונה של הקליינט שולחת בקשה לסגור את החיבור. הקליינט שולח חבילה עם הדגל FIN שמעיד על רצון לסגור את החיבור. לאחר מכן השרת מחזיר לו ACK על כך שהודעת ה־FIN התקבלה. אז השרת גם הוא יוזם את הליך הניתוק, ושולח הודעת FIN בעצמו אל הלקוח. הלקוח מקבל את ההודעה, שולח ACK וברגע שזה מתקבל השרת סוגר את החיבור וכך גם הלקוח.



נראה את תהליך הteardown בלקוח השני גם כן:

The image shows a Wireshark packet capture of a TCP connection teardown. The packet list shows a FIN segment from 10.0.0.10 to 10.0.0.7. The packet details show the segment's structure with flags and sequence numbers. The packet bytes show the raw data.

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
45	21.53...	10.0.0.10	10.0.0.7	TCP	60	12345	49602	[ACK] Seq=2721584262 Ack=310404143 Win=29312 Len=0
46	21.53...	10.0.0.7	10.0.0.10	TCP	60	49602	12345	[PSH, ACK] Seq=2721584262 Ack=310404143 Win=29312 Len=5
47	21.53...	10.0.0.10	10.0.0.7	TCP	60	12345	49602	[ACK] Seq=310404143 Ack=2721584267 Win=525568 Len=0
48	21.53...	10.0.0.7	10.0.0.10	TCP	60	49602	12345	[ACK] Seq=2721584267 Ack=310404148 Win=29312 Len=0
49	21.53...	10.0.0.10	10.0.0.7	TCP	60	12345	49602	[PSH, ACK] Seq=2721584267 Ack=310404148 Win=29312 Len=5
50	21.53...	10.0.0.7	10.0.0.10	TCP	60	49602	12345	[ACK] Seq=310404148 Ack=2721584272 Win=525568 Len=0
51	24.78...	10.0.0.10	10.0.0.7	TCP	60	12345	49602	[PSH, ACK] Seq=310404148 Ack=2721584272 Win=525568 Len=5
52	24.78...	10.0.0.7	10.0.0.10	TCP	60	49602	12345	[ACK] Seq=2721584272 Ack=310404153 Win=29312 Len=0
53	24.78...	10.0.0.10	10.0.0.7	TCP	60	12345	49602	[PSH, ACK] Seq=2721584272 Ack=310404153 Win=29312 Len=0
54	24.78...	10.0.0.7	10.0.0.10	TCP	60	49602	12345	[ACK] Seq=310404153 Ack=2721584273 Win=525568 Len=0
55	27.29...	10.0.0.10	10.0.0.7	TCP	54	49602	12345	[FIN, ACK] Seq=2721584272 Ack=310404153 Win=29312 Len=0
56	27.29...	10.0.0.7	10.0.0.10	TCP	60	12345	49602	[ACK] Seq=310404153 Ack=2721584273 Win=525568 Len=0

Frame 45: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 Ethernet II, Src: Giga-Byt_54:ec:28 (40:8d:5c:54:ec:28), Dst: PcsCompu_7d:1b:f7 (08:00:27:7d:1b:f7)
 Internet Protocol Version 4, Src: 10.0.0.10, Dst: 10.0.0.7
 Transmission Control Protocol, Src Port: 12345, Dst Port: 49602, Seq: 310404143, Ack: 2721584267, Len: 0
 Source Port: 12345
 Destination Port: 49602
 [Stream index: 1]
 [TCP Segment Len: 0]
 Sequence number: 310404143
 [Next sequence number: 310404143]
 Acknowledgment number: 2721584267
 0101 = Header Length: 20 bytes (5)
 Flags: 0x010 (ACK)
 Window size value: 2053
 [Calculated window size: 525568]
 [Window size scaling factor: 256]
 Checksum: 0x7450 [unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0
 [SEQ/ACK analysis]
 [Timestamps]

0000 08 00 27 7d 1b f7 40 8d 5c 54 ec 28 08 00 45 00@.. \T. (.E.
 0010 00 28 65 af 40 00 80 06 81 10 0a 00 00 07 0a 00 ... (e@.....
 0020 00 0a 30 39 c1 c2 12 80 64 2f a2 38 14 8b 50 10d/-8..P.
 0030 08 05 74 50 00 00 00 00 00 00 00 00 00 00 00LP.....

Transmission Control Protocol (tcp), 20 bytes Packets: 62 · Displayed: 13 (21.0%) · Dropped: 0 (0.0%) Profile: Default

כאן לעומת זאת ניתן לראות שאומנם הקליינט שלח FIN, והשרת קיבל ושלח Ack על הFin הזה, התעבורה הפסיקה ישר. (כלומר השרת לא שלח בעצמו Fin)
 לפי בדיקה באינטרנט המצב הזה נקרא Half Closed Connection, שבעצם מתאר מצב בו אומנם הלקוח מוכן לסגירת החיבור, אבל לשרת עדיין יש מידע לשלוח ללקוח ולכן הוא אינו שולח FIN. עם זאת, הלקוח עדיין סוגר את החיבור (בעקבות הquit)

