

## רשתות תרגיל 2

מגישים: נועם כהן 209311620

ואופק ילוז 206666729

חלק א': הרצנו את קוד הקליינט והסרבר מהתרגול, הנה ניתוח התעבורה המתקבלת ב Wireshark:

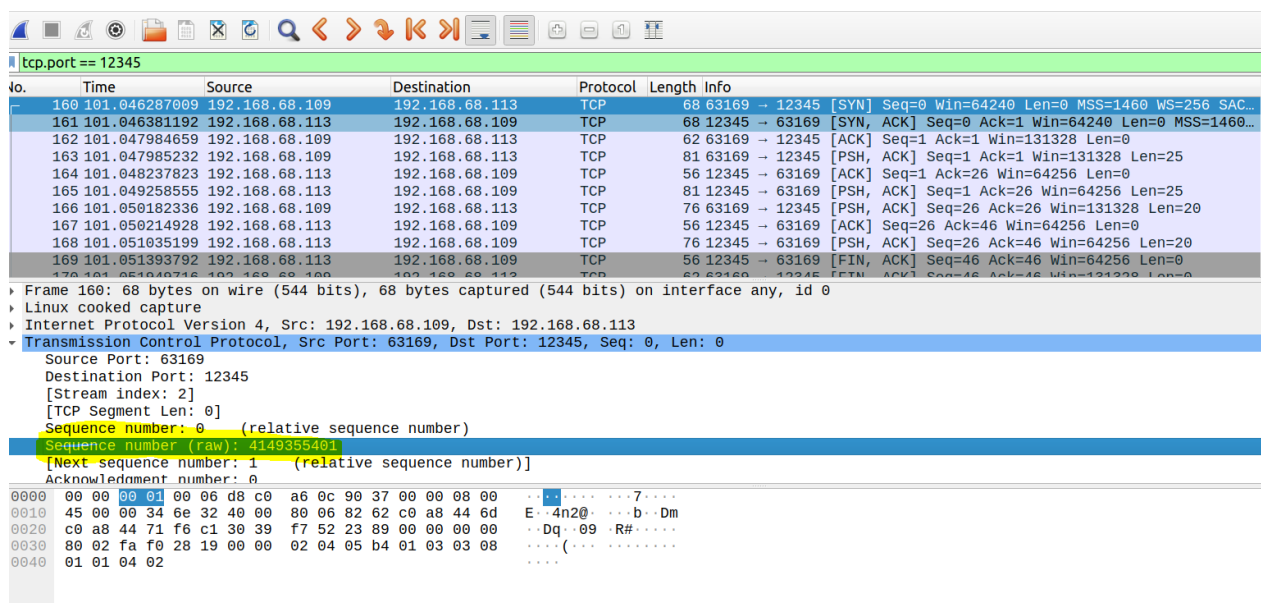
השרת (על מכונה וירטואלית – מערכת הפעלה Ubuntu) נמצא בפורט 12345 והלקוח נמצא ב 63169 (על מחשב ה Windows שמכיל את המכונה הוירטואלית)

להלן ניתוח התעבורה (בנוסף, בתוך הקובץ ClientServerWireshark.pcap מופיע קובץ ה pcap המלא):

בשניה 101 (מתחילת ה sniffing), הלקוח שלח לשרת הודעת SYN. שזה בקשה ליצור חיבור מולו, שזה התחלת ה Handshake. ה Sequence Number שמופיע ב Wireshark הוא

ה Wireshark מסמן את ה Sequence Number להיות 0, אבל בפועל הוא כותב בתוך ה raw שמוסמן בצהוב את מספר הסגמנט הראשון האמיתי שהוא מספר ארוך יותר.

מספר ה Seq האמיתי הוא: 4148355401.



No.	Time	Source	Destination	Protocol	Length	Info
160	101.046287009	192.168.68.109	192.168.68.113	TCP	68	63169 → 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SAC...
161	101.046381192	192.168.68.113	192.168.68.109	TCP	68	12345 → 63169 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460...
162	101.047984659	192.168.68.109	192.168.68.113	TCP	62	63169 → 12345 [ACK] Seq=1 Ack=1 Win=131328 Len=0
163	101.047985232	192.168.68.109	192.168.68.113	TCP	81	63169 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=25
164	101.048237823	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [ACK] Seq=1 Ack=26 Win=64256 Len=0
165	101.049258555	192.168.68.113	192.168.68.109	TCP	81	12345 → 63169 [PSH, ACK] Seq=1 Ack=26 Win=64256 Len=25
166	101.050182336	192.168.68.109	192.168.68.113	TCP	76	63169 → 12345 [PSH, ACK] Seq=26 Ack=26 Win=131328 Len=20
167	101.050214928	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [ACK] Seq=26 Ack=46 Win=64256 Len=0
168	101.051035199	192.168.68.113	192.168.68.109	TCP	76	12345 → 63169 [PSH, ACK] Seq=26 Ack=46 Win=64256 Len=20
169	101.051393792	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [FIN, ACK] Seq=46 Ack=46 Win=64256 Len=0

Frame 160: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface any, id 0

Linux cooked capture

Internet Protocol Version 4, Src: 192.168.68.109, Dst: 192.168.68.113

Transmission Control Protocol, Src Port: 63169, Dst Port: 12345, Seq: 0, Len: 0

Source Port: 63169

Destination Port: 12345

[Stream index: 2]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

Sequence number (raw): 4148355401

[Next sequence number: 1 (relative sequence number)]

Acknowledgment number: 0

0000 00 00 00 01 00 06 d8 c0 a6 0c 90 37 00 00 08 00 ...7...Dm

0010 45 00 00 34 6e 32 40 00 80 06 82 62 c0 a8 44 6d E...4n2...b...Dm

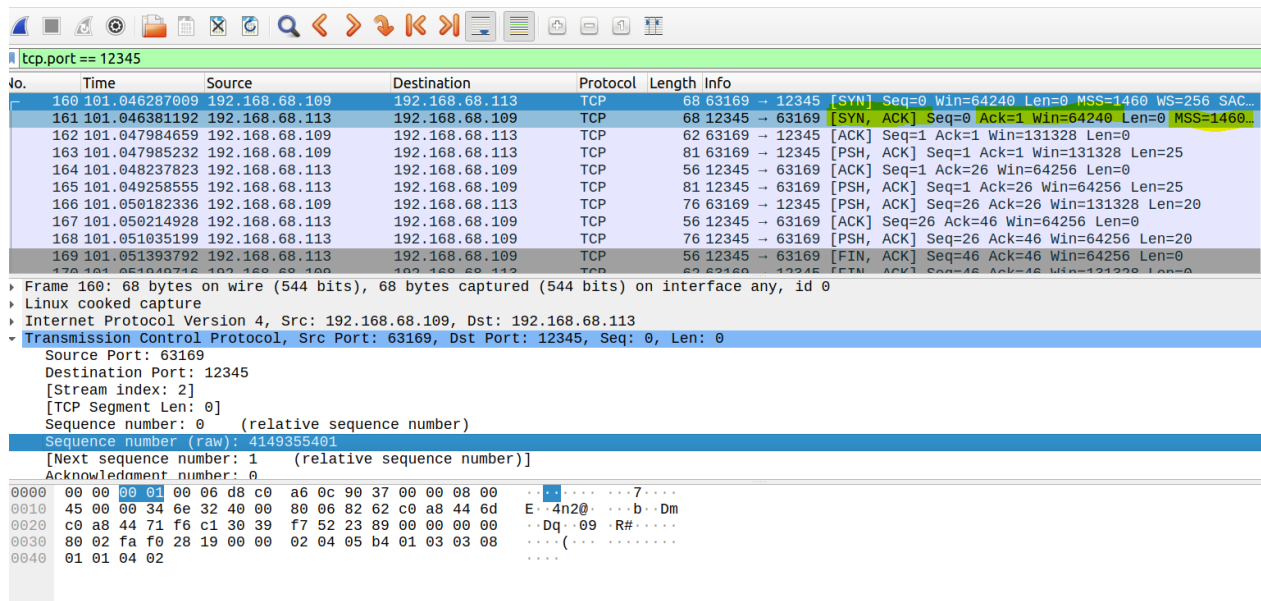
0020 c0 a8 44 71 f6 c1 30 39 f7 52 23 89 00 00 00 00 ...Dq...09...R#...

0030 80 02 fa f0 28 19 00 00 02 04 05 b4 01 03 03 08 ...(... ..)

0040 01 01 04 02 ...

לאחר מכן, השרת שולח הודעת SYN, ACK ללקוח, כאשר ה ACK Number הוא 0 וגודל החלון הוא 64240, כמו כן, ה MSS הוא 1460.

מספר ה Sequence Number האמיתי התעדכן להיות 4149355401. מספר ה ACK האמיתי הוא 2540863573.



No.	Time	Source	Destination	Protocol	Length	Info
160	101.046287009	192.168.68.109	192.168.68.113	TCP	68	63169 → 12345 [SYN, Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SAC...
161	101.046381192	192.168.68.113	192.168.68.109	TCP	68	12345 → 63169 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460...
162	101.047984659	192.168.68.109	192.168.68.113	TCP	62	63169 → 12345 [ACK] Seq=1 Ack=1 Win=131328 Len=0
163	101.047985232	192.168.68.109	192.168.68.113	TCP	81	63169 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=25
164	101.048237823	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [ACK] Seq=1 Ack=26 Win=64256 Len=0
165	101.049258555	192.168.68.113	192.168.68.109	TCP	81	12345 → 63169 [PSH, ACK] Seq=1 Ack=26 Win=64256 Len=25
166	101.050182336	192.168.68.109	192.168.68.113	TCP	76	63169 → 12345 [PSH, ACK] Seq=26 Ack=26 Win=131328 Len=20
167	101.050214928	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [ACK] Seq=26 Ack=46 Win=64256 Len=0
168	101.051035199	192.168.68.113	192.168.68.109	TCP	76	12345 → 63169 [PSH, ACK] Seq=26 Ack=46 Win=64256 Len=20
169	101.051393792	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [FIN, ACK] Seq=46 Ack=46 Win=131328 Len=0

Frame 160: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface any, id 0

Linux cooked capture

Internet Protocol Version 4, Src: 192.168.68.109, Dst: 192.168.68.113

Transmission Control Protocol, Src Port: 63169, Dst Port: 12345, Seq: 0, Len: 0

Source Port: 63169

Destination Port: 12345

[Stream index: 2]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

Sequence number (raw): 4149355401

[Next sequence number: 1 (relative sequence number)]

Acknowledgment number: 0

0000 00 00 00 01 00 06 d8 c0 a6 0c 90 37 00 00 08 00 .....7....

0010 45 00 00 34 6e 32 40 00 80 06 82 62 c0 a8 44 6d E..4n2@...b...Dm

0020 c0 a8 44 71 f6 c1 30 39 f7 52 23 89 00 00 00 00 ..Dq..09..R#....

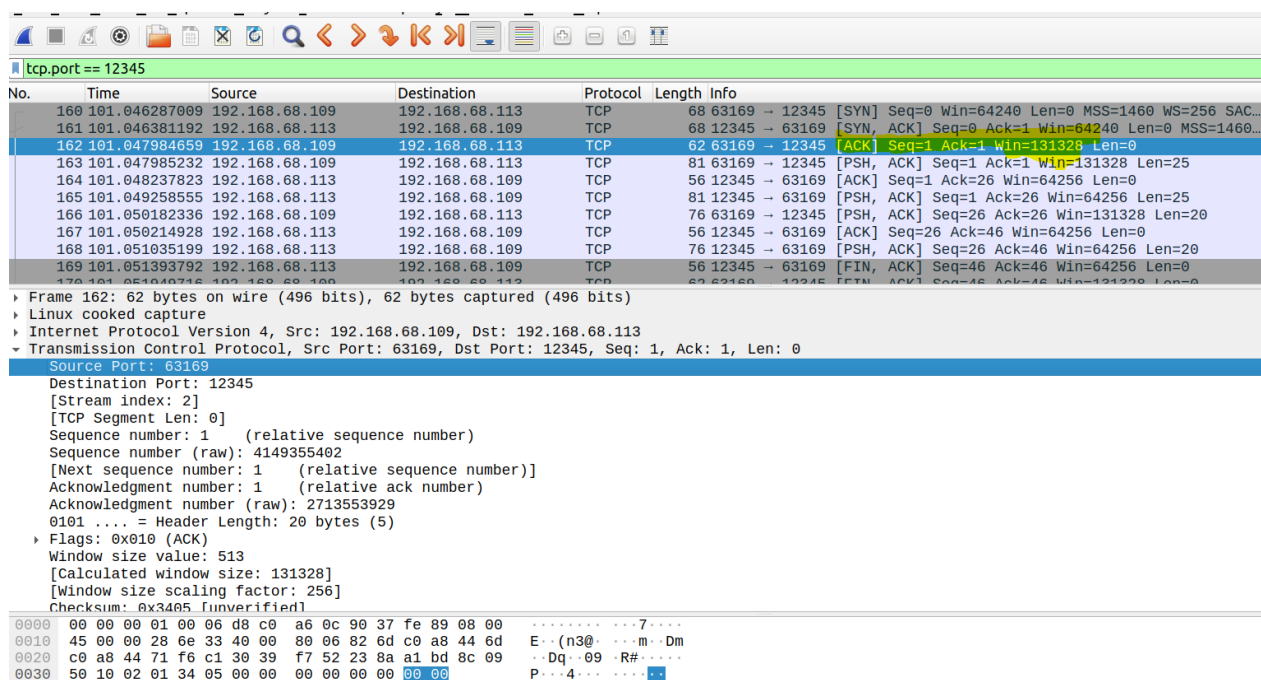
0030 80 02 fa f0 28 19 00 00 02 04 05 b4 01 03 03 08 ....(.....

0040 01 01 04 02 .....

לאחר מכן, הלקוח שולח לשרת הודעת ACK, כדי לסיים את ה handshake. מתקיים כי החלון של הלקוח הוא 131328, כמו כן, מספר ה Seq הפך ל 1, וגם ה ACK הפך ל 1 (שהרי הלקוח קיבל SYN-ACK מהשרת).

מספר ה Sequence Number האמיתי התעדכן להיות 4149355402. מספר ה ACK האמיתי הוא 2713553929

מספר ה ACK האמיתי התעדכן להיות 1.



No.	Time	Source	Destination	Protocol	Length	Info
160	101.046287009	192.168.68.109	192.168.68.113	TCP	68	63169 → 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SAC...
161	101.046381192	192.168.68.113	192.168.68.109	TCP	68	12345 → 63169 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460...
162	101.047984659	192.168.68.109	192.168.68.113	TCP	62	63169 → 12345 [ACK] Seq=1 Ack=1 Win=131328 Len=0
163	101.047985232	192.168.68.109	192.168.68.113	TCP	81	63169 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=25
164	101.048237823	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [ACK] Seq=1 Ack=26 Win=64256 Len=0
165	101.049258555	192.168.68.113	192.168.68.109	TCP	81	12345 → 63169 [PSH, ACK] Seq=1 Ack=26 Win=64256 Len=25
166	101.050182336	192.168.68.109	192.168.68.113	TCP	76	63169 → 12345 [PSH, ACK] Seq=26 Ack=26 Win=131328 Len=20
167	101.050214928	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [ACK] Seq=26 Ack=46 Win=64256 Len=0
168	101.051035199	192.168.68.113	192.168.68.109	TCP	76	12345 → 63169 [PSH, ACK] Seq=26 Ack=46 Win=64256 Len=20
169	101.051393792	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [FIN, ACK] Seq=46 Ack=46 Win=131328 Len=0

Frame 162: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)

Linux cooked capture

Internet Protocol Version 4, Src: 192.168.68.109, Dst: 192.168.68.113

Transmission Control Protocol, Src Port: 63169, Dst Port: 12345, Seq: 1, Ack: 1, Len: 0

Source Port: 63169

Destination Port: 12345

[Stream index: 2]

[TCP Segment Len: 0]

Sequence number: 1 (relative sequence number)

Sequence number (raw): 4149355402

[Next sequence number: 1 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Acknowledgment number (raw): 2713553929

0101 .... = Header Length: 20 bytes (5)

Flags: 0x010 (ACK)

Window size value: 513

[Calculated window size: 131328]

[Window size scaling factor: 256]

Checksum: 0x3405 (unverified)

0000 00 00 00 01 00 06 d8 c0 a6 0c 90 37 fe 89 08 00 .....7....

0010 45 00 00 28 6e 33 40 00 80 06 82 6d c0 a8 44 6d E..(n3@...m...Dm

0020 c0 a8 44 71 f6 c1 30 39 f7 52 23 8a a1 bd 8c 09 ..Dq..09..R#....

0030 50 10 02 01 34 05 00 00 00 00 00 00 00 00 00 P...4....

לאחר מכן, הלקוח שולח לשרת הודעת PSH-ACK שמכילה את השמות שלנו: Noam Cohen and Ofek Yaloz, מספר הסגמנט הוא 1, ומספר הACK הוא 1 (כי מקודם השרת החזיר ACK). כמו כן, גודל החלון של הלקוח הוא 131328, אורך החבילה הוא 25.

מספר ה Sequence Number האמיתי הוא: 419355402

מספר ה ACK האמיתי הוא: 2713553929.

162	101.047984659	192.168.68.109	192.168.68.113	TCP	62	63169 → 12345	[ACK] Seq=1 Ack=1 Win=131328 Len=0
163	101.047985232	192.168.68.109	192.168.68.113	TCP	81	63169 → 12345	[PSH, ACK] Seq=1 Ack=1 Win=131328 Len=25
164	101.048237823	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169	[ACK] Seq=1 Ack=26 Win=64256 Len=0
165	101.049258555	192.168.68.113	192.168.68.109	TCP	81	12345 → 63169	[PSH, ACK] Seq=1 Ack=26 Win=64256 Len=25
166	101.050182336	192.168.68.109	192.168.68.113	TCP	76	63169 → 12345	[PSH, ACK] Seq=26 Ack=26 Win=131328 Len=20
167	101.050214928	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169	[ACK] Seq=26 Ack=46 Win=64256 Len=0
168	101.051035199	192.168.68.113	192.168.68.109	TCP	76	12345 → 63169	[PSH, ACK] Seq=26 Ack=46 Win=64256 Len=20
169	101.051393792	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169	[FIN, ACK] Seq=46 Ack=46 Win=64256 Len=0
170	101.051940716	192.168.68.109	192.168.68.113	TCP	62	63169 → 12345	[ACK] Seq=46 Ack=46 Win=131328 Len=0
Frame 163: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)							
Linux cooked capture							
Internet Protocol Version 4, Src: 192.168.68.109, Dst: 192.168.68.113							
Transmission Control Protocol, Src Port: 63169, Dst Port: 12345, Seq: 1, Ack: 1, Len: 25							
Source Port: 63169							
Destination Port: 12345							
[Stream index: 2]							
[TCP Segment Len: 25]							
Sequence number: 1 (relative sequence number)							
Sequence number (raw): 4149355402							
[Next sequence number: 26 (relative sequence number)]							
Acknowledgment number: 1 (relative ack number)							
Acknowledgment number (raw): 2713553929							
0101 .... = Header Length: 20 bytes (5)							
Flags: 0x018 (PSH, ACK)							
Window size value: 513							
[Calculated window size: 131328]							
[Window size scaling factor: 256]							
Checksum: 0xcce81 [unverified]							
0020	c0 a8 44 71	f6 c1 30 39	f7 52 23 8a	a1 bd 8c 09	.....	09	R#.....
0030	50 18 02 01	ce 81 00 00	4e 6f 61 6d	20 43 6f 68	P.....	Noam Coh	
0040	65 6e 20 61	6e 64 20 4f	66 65 6b 20	59 61 6c 6f	en and 0	fek Yalo	
0050	7a				z		

השרת מחזיר ללקוח הודעת ACK, כאשר ה ACK=26, וזה כיוון שמקודם הוא ה Received Buffer הכיל בית אחד (על ה ACK בעת ה handshake), וכעת הוא קיבל הודעה שאורכה 25 בתים, ולכן  $26 = 1 + 25$  וזה מספר ה ACK העדכני.

מספר ה sequence האמיתי הוא 2713553929

מספר ה ACK האמיתי הוא 4149355427.

tcp.port == 12345							
No.	Time	Source	Destination	Protocol	Length	Info	
160	101.046287009	192.168.68.109	192.168.68.113	TCP	68	63169 → 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=2	
161	101.046381192	192.168.68.113	192.168.68.109	TCP	68	12345 → 63169 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MS	
162	101.047984659	192.168.68.109	192.168.68.113	TCP	62	63169 → 12345 [ACK] Seq=1 Ack=1 Win=131328 Len=0	
163	101.047985232	192.168.68.109	192.168.68.113	TCP	81	63169 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=25	
164	101.048237823	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [ACK] Seq=1 Ack=26 Win=64256 Len=0	
165	101.049258555	192.168.68.113	192.168.68.109	TCP	81	12345 → 63169 [PSH, ACK] Seq=1 Ack=26 Win=64256 Len=25	
166	101.050182336	192.168.68.109	192.168.68.113	TCP	76	63169 → 12345 [PSH, ACK] Seq=26 Ack=26 Win=131328 Len=20	
167	101.050214928	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [ACK] Seq=26 Ack=46 Win=64256 Len=0	
168	101.051035199	192.168.68.113	192.168.68.109	TCP	76	12345 → 63169 [PSH, ACK] Seq=26 Ack=46 Win=64256 Len=20	
169	101.051393792	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [FIN, ACK] Seq=46 Ack=46 Win=64256 Len=0	
170	101.051940716	192.168.68.109	192.168.68.113	TCP	62	63169 → 12345 [ACK] Seq=46 Ack=46 Win=131328 Len=0	
Frame 164: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)							
Linux cooked capture							
Internet Protocol Version 4, Src: 192.168.68.113, Dst: 192.168.68.109							
Transmission Control Protocol, Src Port: 12345, Dst Port: 63169, Seq: 1, Ack: 26, Len: 0							
Source Port: 12345							
Destination Port: 63169							
[Stream index: 2]							
[TCP Segment Len: 0]							
Sequence number: 1 (relative sequence number)							
Sequence number (raw): 2713553929							
[Next sequence number: 1 (relative sequence number)]							
Acknowledgment number: 26 (relative ack number)							
Acknowledgment number (raw): 4149355427							
0101 .... = Header Length: 20 bytes (5)							
Flags: 0x010 (ACK)							
Window size value: 502							
[Calculated window size: 64256]							
[Window size scaling factor: 128]							
Checksum: 0x0a4a [unverified]							
0000	00 04 00 01	00 06 08 00	27 48 5d eb	08 00 08 00	.....	'H].....	
0010	45 00 00 28	59 5d 40 00	40 06 d7 43	c0 a8 44 71	E..(Y]@..@..C..Dq		
0020	c0 a8 44 6d	30 39 f6 c1	a1 bd 8c 09	f7 52 23 a3	.....Dm09.....R#..		
0030	50 10 01 f6	0a 4a 00 00			P.....J..		

לאחר מכן, השרת מחזיר ללקוח הודעה שמכילה את השמות שלה – כשהם עתה ב UPPER CASE, אזי מתקיים כי מספר הסגמנט בשרת הוא 1, (כי הוא שלח בינתיים רק SYN-ACK בהתחלה), כמו כן, גודל החבילה הוא 25, בנוסף, גודל החלון נשאר 64256.

מספר ה Sequence Number האמיתי הוא: 2713553929

מספר ה ACK האמיתי הוא: 4149355427

No.	Time	Source	Destination	Protocol	Length	Info
160	101.046287009	192.168.68.109	192.168.68.113	TCP	68	63169 → 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SAC...
161	101.046381192	192.168.68.113	192.168.68.109	TCP	68	12345 → 63169 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460...
162	101.047984659	192.168.68.109	192.168.68.113	TCP	62	63169 → 12345 [ACK] Seq=1 Ack=1 Win=131328 Len=0
163	101.047985232	192.168.68.109	192.168.68.113	TCP	81	63169 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=25
164	101.048237823	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [ACK] Seq=1 Ack=26 Win=64256 Len=0
165	101.049258555	192.168.68.113	192.168.68.109	TCP	81	12345 → 63169 [PSH, ACK] Seq=1 Ack=26 Win=64256 Len=25
166	101.050182336	192.168.68.109	192.168.68.113	TCP	76	63169 → 12345 [PSH, ACK] Seq=26 Ack=26 Win=131328 Len=20
167	101.050214928	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [ACK] Seq=26 Ack=46 Win=64256 Len=0
168	101.051035199	192.168.68.113	192.168.68.109	TCP	76	12345 → 63169 [PSH, ACK] Seq=26 Ack=46 Win=64256 Len=20
169	101.051393792	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [FIN, ACK] Seq=46 Ack=46 Win=64256 Len=0

▶ Frame 165: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)  
 ▶ Linux cooked capture  
 ▶ Internet Protocol Version 4, Src: 192.168.68.113, Dst: 192.168.68.109  
 ▶ Transmission Control Protocol, Src Port: 12345, Dst Port: 63169, Seq: 1, Ack: 26, Len: 25  
     Source Port: 12345  
     Destination Port: 63169  
     [Stream index: 2]  
     [TCP Segment Len: 25]  
     Sequence number: 1 (relative sequence number)  
     Sequence number (raw): 2713553929  
     [Next sequence number: 26 (relative sequence number)]  
     Acknowledgment number: 26 (relative ack number)  
     Acknowledgment number (raw): 4149355427  
     0101 ... = Header Length: 20 bytes (5)  
     ▶ Flags: 0x018 (PSH, ACK)  
     Window size value: 502  
     [Calculated window size: 64256]  
     [Window size scaling factor: 128]  
     Checksum: 0x0a63 [unverified]

0020	c0 a8 44 6d 30 39 f6 c1 a1 bd 8c 09 f7 52 23 a3	...	Dm09	...	R#
0030	50 18 01 f6 0a 63 00 00 4e 4f 41 4d 20 43 4f 48	...	P	...	NOAM COH
0040	45 4e 20 41 4e 44 20 4f 46 45 4b 20 59 41 4c 4f	...	EN AND 0	FEK	YALO
0050	5a	...	2	...	

לאחר מכן, הלקוח שולח לשרת הודעה, כעת מספר הסגמנט הסידורי הוא 26 (כי מקודם הוא שלח הודעה עם השמות), מספר ה ACK הוא 26 (כי השרת שלח גם את השמות כשהם באותיות גדולות),

מספר ה Sequence Number הוא 4149355427

מספר ה ACK האמיתי הוא 2713553954

וגודל החלון שלו נשאר זהה – 131328, ואורך החבילה היא 20, בתוכן החבילה, ניתן לראות את תעודת הזהות שלנו:

160	101.046287009	192.168.68.109	192.168.68.113	TCP	68	63169 → 12345	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SAC...
161	101.046381192	192.168.68.113	192.168.68.109	TCP	68	12345 → 63169	[SYN, ACK]	Seq=0 Ack=1 Win=64240 Len=0 MSS=1460...
162	101.047984659	192.168.68.109	192.168.68.113	TCP	62	63169 → 12345	[ACK]	Seq=1 Ack=1 Win=131328 Len=0
163	101.047985232	192.168.68.109	192.168.68.113	TCP	81	63169 → 12345	[PSH, ACK]	Seq=1 Ack=1 Win=131328 Len=25
164	101.048237823	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169	[ACK]	Seq=1 Ack=26 Win=64256 Len=0
165	101.049258555	192.168.68.109	192.168.68.109	TCP	81	12345 → 63169	[PSH, ACK]	Seq=1 Ack=26 Win=64256 Len=25
166	101.050182336	192.168.68.109	192.168.68.113	TCP	76	63169 → 12345	[PSH, ACK]	Seq=26 Ack=26 Win=131328 Len=20
167	101.050214928	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169	[ACK]	Seq=26 Ack=46 Win=64256 Len=0
168	101.051035199	192.168.68.113	192.168.68.109	TCP	76	12345 → 63169	[PSH, ACK]	Seq=26 Ack=46 Win=64256 Len=20
169	101.051393792	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169	[FIN, ACK]	Seq=46 Ack=46 Win=64256 Len=0
170	101.051407716	192.168.68.109	192.168.68.113	TCP	60	63169 → 12345	[FIN, ACK]	Seq=46 Ack=46 Win=131328 Len=0

▶ Frame 166: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)  
 ▶ Linux cooked capture  
 ▶ Internet Protocol Version 4, Src: 192.168.68.109, Dst: 192.168.68.113  
 ▶ Transmission Control Protocol, Src Port: 63169, Dst Port: 12345, Seq: 26, Ack: 26, Len: 20  
 Source Port: 63169  
 Destination Port: 12345  
 [Stream index: 2]  
 [TCP Segment Len: 20]  
 Sequence number: 26 (relative sequence number)  
 Sequence number (raw): 4149355427  
 [Next sequence number: 46 (relative sequence number)]  
 Acknowledgment number: 26 (relative ack number)  
 Acknowledgment number (raw): 2713553954  
 0101 .... = Header Length: 20 bytes (5)  
 ▶ Flags: 0x018 (PSH, ACK)  
 Window size value: 513  
 [Calculated window size: 131328]  
 [Window size scaling factor: 256]  
 Checksum: 0x41b5 [unverified]

0010	45 00 00 3c 6e 35 40 00	80 06 82 57 c0 a8 44 6d	E...<n5@: ...W...Dm
0020	c0 a8 44 71 f6 c1 30 39	f7 52 23 a3 a1 bd 8c 22	...Dq...09...R#..."
0030	50 18 02 01 41 b5 00 00	32 30 39 33 31 31 36 32	P...A... 20931162
0040	30 2c 20 32 30 36 36 36	36 37 32 39	0, 20666 6729

עכשיו השרת מחזיר הודעת ACK כאשר ACK=46 שהוא קיבל את ההודעה עם תעודת הזרות, הסיבה שה ACK הוא 46, כי כבר השרת קיבל חבילות מהלקוח: של SYN (נספר כאחד) + שמות שלנו (25) תעודות זהות (20). כמו כן, גודל החלון נשאר זהה – 64256: מספר ה Sequence Number האמיתי הוא: 2713553954. מספר ה ACK האמיתי הוא: 4149355447

tcp.port == 12345									
No.	Time	Source	Destination	Protocol	Length	Info			
160	101.046287009	192.168.68.109	192.168.68.113	TCP	68	63169 → 12345	[SYN]	Seq=0 Win=64240 Len=0 MSS=1460 WS=256 S...	
161	101.046381192	192.168.68.113	192.168.68.109	TCP	68	12345 → 63169	[SYN, ACK]	Seq=0 Ack=1 Win=64240 Len=0 MSS=1460...	
162	101.047984659	192.168.68.109	192.168.68.113	TCP	62	63169 → 12345	[ACK]	Seq=1 Ack=1 Win=131328 Len=0	
163	101.047985232	192.168.68.109	192.168.68.113	TCP	81	63169 → 12345	[PSH, ACK]	Seq=1 Ack=1 Win=131328 Len=25	
164	101.048237823	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169	[ACK]	Seq=1 Ack=26 Win=64256 Len=0	
165	101.049258555	192.168.68.113	192.168.68.109	TCP	81	12345 → 63169	[PSH, ACK]	Seq=1 Ack=26 Win=64256 Len=25	
166	101.050182336	192.168.68.109	192.168.68.113	TCP	76	63169 → 12345	[PSH, ACK]	Seq=26 Ack=26 Win=131328 Len=20	
167	101.050214928	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169	[ACK]	Seq=26 Ack=46 Win=64256 Len=0	
168	101.051035199	192.168.68.113	192.168.68.109	TCP	76	12345 → 63169	[PSH, ACK]	Seq=26 Ack=46 Win=64256 Len=20	
169	101.051393792	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169	[FIN, ACK]	Seq=46 Ack=46 Win=64256 Len=0	
170	101.051407716	192.168.68.109	192.168.68.113	TCP	60	63169 → 12345	[FIN, ACK]	Seq=46 Ack=46 Win=131328 Len=0	

▶ Frame 167: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)  
 ▶ Linux cooked capture  
 ▶ Internet Protocol Version 4, Src: 192.168.68.113, Dst: 192.168.68.109  
 ▶ Transmission Control Protocol, Src Port: 12345, Dst Port: 63169, Seq: 26, Ack: 46, Len: 0  
 Source Port: 12345  
 Destination Port: 63169  
 [Stream index: 2]  
 [TCP Segment Len: 0]  
 Sequence number: 26 (relative sequence number)  
 Sequence number (raw): 2713553954  
 [Next sequence number: 26 (relative sequence number)]  
 Acknowledgment number: 46 (relative ack number)  
 Acknowledgment number (raw): 4149355447  
 0101 .... = Header Length: 20 bytes (5)  
 ▶ Flags: 0x010 (ACK)  
 Window size value: 502  
 [Calculated window size: 64256]  
 [Window size scaling factor: 128]  
 Checksum: 0x0a0a [unverified]

0000	00 04 00 01 00 06 08 00	27 48 5d eb 01 00 08 00	..... 'H'.....
0010	45 00 00 28 59 5f 40 00	40 06 d7 41 c0 a8 44 71	E... (Y_@_ @_ A_ Dq
0020	c0 a8 44 6d 30 39 f6 c1	a1 bd 8c 22 f7 52 23 b7	...Dm09... "...R#
0030	50 18 01 f6 0a 4a 00 00		P... J...

עכשיו השרת מחזיר הודעת ACK שהוא קיבל את תעודות הזרות, כמו שהן נשלחו אליו. לכן דגל ה PUSH דולק, כמו כן, מספר הסגמנט הסידורי הוא 26, וה ACK הוא 46 כמו בהודעה שלפני כן.



מספר ה Sequence Number האמיתי הוא 2713553954

מספר ה ACK האמיתי הוא: 4149355447

163	101.047985232	192.168.68.109	192.168.68.113	TCP	81	63169 → 12345	[PSH, ACK] Seq=1 Ack=1 Win=131328 Len=25
164	101.048237823	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169	[ACK] Seq=1 Ack=26 Win=64256 Len=0
165	101.049258555	192.168.68.113	192.168.68.109	TCP	81	12345 → 63169	[PSH, ACK] Seq=1 Ack=26 Win=64256 Len=25
166	101.050182336	192.168.68.109	192.168.68.113	TCP	76	63169 → 12345	[PSH, ACK] Seq=26 Ack=26 Win=131328 Len=20
167	101.050214928	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169	[ACK] Seq=26 Ack=46 Win=64256 Len=0
168	101.051035199	192.168.68.113	192.168.68.109	TCP	76	12345 → 63169	[PSH, ACK] Seq=26 Ack=46 Win=64256 Len=20
169	101.051393792	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169	[FIN, ACK] Seq=46 Ack=46 Win=64256 Len=0
170	101.051949716	192.168.68.109	192.168.68.113	TCP	62	63169 → 12345	[FIN, ACK] Seq=46 Ack=46 Win=131328 Len=0
171	101.052012960	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169	[ACK] Seq=47 Ack=47 Win=64256 Len=0
172	101.051949940	192.168.68.109	192.168.68.113	TCP	62	63169 → 12345	[ACK] Seq=47 Ack=47 Win=131328 Len=0

Frame 168: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)

Linux cooked capture

Internet Protocol Version 4, Src: 192.168.68.113, Dst: 192.168.68.109

Transmission Control Protocol, Src Port: 12345, Dst Port: 63169, Seq: 26, Ack: 46, Len: 20

Source Port: 12345

Destination Port: 63169

[Stream index: 2]

[TCP Segment Len: 20]

Sequence number: 26 (relative sequence number)

Sequence number (raw): 2713553954

[Next sequence number: 46 (relative sequence number)]

Acknowledgment number: 46 (relative ack number)

Acknowledgment number (raw): 4149355447

0101 .... = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

Window size value: 502

[Calculated window size: 64256]

[Window size scaling factor: 128]

Checksum: 0x0a5e [unverified]

0010	45 00 00 3c 59 60 40 00 40 06 d7 2c c0 a8 44 71	E...<Y@. @...Dq
0020	c0 a8 44 6d 30 39 f6 c1 a1 bd 8c 22 f7 52 23 b7	..Dm09...R#
0030	50 18 01 f6 0a 5e 00 00 32 30 39 33 31 31 36 32	P...A...20931162
0040	30 2c 20 32 30 36 36 36 36 37 32 39	0, 20666 6729

השרת, מבצע client.close(), וזה בא לידי ביטוי בכך שהוא שולח הודעה ללקוח של FYN-ACK, המספר הסידורי הוא 46 (כי מקודם הוא שלח את תעודות הזרות באורך 20 – 20+26=46), כמו כן, גודל החלון נשאר 64256.

מספר ה Sequence number האמיתי הוא 2713553974

מספר ה ACK האמיתי הוא 4149355447

tcp.port == 12345							
No.	Time	Source	Destination	Protocol	Length	Info	
163	101.047985232	192.168.68.109	192.168.68.113	TCP	81	63169 → 12345	[PSH, ACK] Seq=1 Ack=1 Win=131328 Len=25
164	101.048237823	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169	[ACK] Seq=1 Ack=26 Win=64256 Len=0
165	101.049258555	192.168.68.113	192.168.68.109	TCP	81	12345 → 63169	[PSH, ACK] Seq=1 Ack=26 Win=64256 Len=25
166	101.050182336	192.168.68.109	192.168.68.113	TCP	76	63169 → 12345	[PSH, ACK] Seq=26 Ack=26 Win=131328 Len=20
167	101.050214928	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169	[ACK] Seq=26 Ack=46 Win=64256 Len=0
168	101.051035199	192.168.68.113	192.168.68.109	TCP	76	12345 → 63169	[PSH, ACK] Seq=26 Ack=46 Win=64256 Len=20
169	101.051393792	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169	[FIN, ACK] Seq=46 Ack=46 Win=64256 Len=0
170	101.051949716	192.168.68.109	192.168.68.113	TCP	62	63169 → 12345	[FIN, ACK] Seq=46 Ack=46 Win=131328 Len=0
171	101.052012960	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169	[ACK] Seq=47 Ack=47 Win=64256 Len=0
172	101.051949940	192.168.68.109	192.168.68.113	TCP	62	63169 → 12345	[ACK] Seq=47 Ack=47 Win=131328 Len=0

Frame 169: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)

Linux cooked capture

Internet Protocol Version 4, Src: 192.168.68.113, Dst: 192.168.68.109

Transmission Control Protocol, Src Port: 12345, Dst Port: 63169, Seq: 46, Ack: 46, Len: 0

Source Port: 12345

Destination Port: 63169

[Stream index: 2]

[TCP Segment Len: 0]

Sequence number: 46 (relative sequence number)

Sequence number (raw): 2713553974

[Next sequence number: 47 (relative sequence number)]

Acknowledgment number: 46 (relative ack number)

Acknowledgment number (raw): 4149355447

0101 .... = Header Length: 20 bytes (5)

Flags: 0x011 (FIN, ACK)

Window size value: 502

[Calculated window size: 64256]

[Window size scaling factor: 128]

Checksum: 0x0a4a [unverified]

0000	00 04 00 01 00 06 08 00 27 48 5d eb 00 00 08 00	.....'H].....
0010	45 00 00 28 59 61 40 00 40 06 d7 3f c0 a8 44 71	E..(Ya@. @...?..Dq
0020	c0 a8 44 6d 30 39 f6 c1 a1 bd 8c 36 f7 52 23 b7	..Dm09...6.R#
0030	50 11 01 f6 0a 4a 00 00	P...J..

הלקוח מחזיר לשרת הודעת FYN-ACK עם מספר סגמנט 46, ומספר ACK של 46, אורך החלון נשאר 131328

מספר ה Sequence Number האמיתי הוא 4149355447

מספר ה ACK האמיתי הוא 2713553974

tcp.port == 12345						
No.	Time	Source	Destination	Protocol	Length	Info
163	101.047985232	192.168.68.109	192.168.68.113	TCP	81	63169 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=25
164	101.048237823	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [ACK] Seq=1 Ack=26 Win=64256 Len=0
165	101.049258555	192.168.68.113	192.168.68.109	TCP	81	12345 → 63169 [PSH, ACK] Seq=1 Ack=26 Win=64256 Len=25
166	101.050182336	192.168.68.109	192.168.68.113	TCP	76	63169 → 12345 [PSH, ACK] Seq=26 Ack=26 Win=131328 Len=20
167	101.050214928	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [ACK] Seq=26 Ack=46 Win=64256 Len=0
168	101.051035199	192.168.68.113	192.168.68.109	TCP	76	12345 → 63169 [PSH, ACK] Seq=26 Ack=46 Win=64256 Len=20
169	101.051393792	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [FIN, ACK] Seq=46 Ack=46 Win=131328 Len=0
170	101.051949716	192.168.68.109	192.168.68.113	TCP	62	63169 → 12345 [FIN, ACK] Seq=46 Ack=46 Win=131328 Len=0
171	101.052012960	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [ACK] Seq=47 Ack=47 Win=64256 Len=0
172	101.051949940	192.168.68.109	192.168.68.113	TCP	62	63169 → 12345 [ACK] Seq=47 Ack=47 Win=131328 Len=0

Frame 170: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)

Linux cooked capture

Internet Protocol Version 4, Src: 192.168.68.109, Dst: 192.168.68.113

Transmission Control Protocol, Src Port: 63169, Dst Port: 12345, Seq: 46, Ack: 46, Len: 0

Source Port: 63169

Destination Port: 12345

[Stream index: 2]

[TCP Segment Len: 0]

Sequence number: 46 (relative sequence number)

Sequence number (raw): 4149355447

[Next sequence number: 47 (relative sequence number)]

Acknowledgment number: 46 (relative ack number)

Acknowledgment number (raw): 2713553974

0101 .... = Header Length: 20 bytes (5)

Flags: 0x011 (FIN, ACK)

Window size value: 513

[Calculated window size: 131328]

[Window size scaling factor: 256]

Checksum: 0x33aa [unverified]

0000 00 00 00 01 00 06 d8 c0 a6 0c 90 37 00 00 08 00 .....7....  
0010 45 00 00 28 6e 36 40 00 80 06 82 6a c0 a8 44 6d E..(n6@...].Dm  
0020 c0 a8 44 71 f6 c1 30 39 f7 52 23 b7 a1 bd 8c 36 ..Dq..09..R#...6  
0030 50 11 02 01 33 aa 00 00 00 00 00 00 00 00 P...3... .....

השרת שולח הודעת ACK ללקוח- כעת מספר ה ACK הוא 47 (הודעת ה FYN-ACK נספרת כאחת), וגם מספר הסגמנט הסידורי הוא 47, וגודל החלון הוא 64256

מספר ה Sequence Number האמיתי הוא 2713553975

מספר ה ACK האמיתי הוא 4149355448

tcp.port == 12345						
No.	Time	Source	Destination	Protocol	Length	Info
163	101.047985232	192.168.68.109	192.168.68.113	TCP	81	63169 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=25
164	101.048237823	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [ACK] Seq=1 Ack=26 Win=64256 Len=0
165	101.049258555	192.168.68.113	192.168.68.109	TCP	81	12345 → 63169 [PSH, ACK] Seq=1 Ack=26 Win=64256 Len=25
166	101.050182336	192.168.68.109	192.168.68.113	TCP	76	63169 → 12345 [PSH, ACK] Seq=26 Ack=26 Win=131328 Len=20
167	101.050214928	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [ACK] Seq=26 Ack=46 Win=64256 Len=0
168	101.051035199	192.168.68.113	192.168.68.109	TCP	76	12345 → 63169 [PSH, ACK] Seq=26 Ack=46 Win=64256 Len=20
169	101.051393792	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [FIN, ACK] Seq=46 Ack=46 Win=131328 Len=0
170	101.051949716	192.168.68.109	192.168.68.113	TCP	62	63169 → 12345 [FIN, ACK] Seq=46 Ack=46 Win=131328 Len=0
171	101.052012960	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [ACK] Seq=47 Ack=47 Win=64256 Len=0
172	101.051949940	192.168.68.109	192.168.68.113	TCP	62	63169 → 12345 [ACK] Seq=47 Ack=47 Win=131328 Len=0

Frame 171: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)

Linux cooked capture

Internet Protocol Version 4, Src: 192.168.68.113, Dst: 192.168.68.109

Transmission Control Protocol, Src Port: 12345, Dst Port: 63169, Seq: 47, Ack: 47, Len: 0

Source Port: 12345

Destination Port: 63169

[Stream index: 2]

[TCP Segment Len: 0]

Sequence number: 47 (relative sequence number)

Sequence number (raw): 2713553975

[Next sequence number: 47 (relative sequence number)]

Acknowledgment number: 47 (relative ack number)

Acknowledgment number (raw): 4149355448

0101 .... = Header Length: 20 bytes (5)

Flags: 0x010 (ACK)

Window size value: 502

[Calculated window size: 64256]

[Window size scaling factor: 128]

Checksum: 0x0ada [unverified]

0000 00 04 00 01 00 06 08 00 27 48 5d eb 00 00 08 00 .....H]....  
0010 45 00 00 28 59 62 40 00 40 06 d7 3e c0 a8 44 71 E..(Yb@..@..Dq  
0020 c0 a8 44 6d 30 39 f6 c1 a1 bd 8c 37 f7 52 23 b8 ..Dm09...7..R#  
0030 50 10 01 f6 0a 4a 00 00 00 00 00 00 00 00 P...J... .....

Destination Port (tcp.dstport), 2 bytes

Packets: 237 · Displayed: 14

הלקוח שולח לשרת הודעת ACK כדי לסיים את החיבור.

כמו כן, עכשיו מספר הסגמנט הסידורי הוא 47, גודל החלון הוא 131328, וה ACK=47, כמו מקודם (הודעת ה FYN-ACK ממקודם נספרה כאחת).

מספר ה Sequence Number האמיתי הוא 414355448.

מספר ה ACK האמיתי הוא 2713553975

tcp.port == 12345						
No.	Time	Source	Destination	Protocol	Length	Info
163	101.047985232	192.168.68.109	192.168.68.113	TCP	81	63169 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=25
164	101.048237823	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [ACK] Seq=1 Ack=26 Win=64256 Len=0
165	101.049258555	192.168.68.113	192.168.68.109	TCP	81	12345 → 63169 [PSH, ACK] Seq=1 Ack=26 Win=64256 Len=25
166	101.050182336	192.168.68.109	192.168.68.113	TCP	76	63169 → 12345 [PSH, ACK] Seq=26 Ack=26 Win=131328 Len=2
167	101.050214928	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [ACK] Seq=26 Ack=46 Win=64256 Len=0
168	101.051035199	192.168.68.113	192.168.68.109	TCP	76	12345 → 63169 [PSH, ACK] Seq=26 Ack=46 Win=64256 Len=20
169	101.051393792	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [FIN, ACK] Seq=46 Ack=46 Win=64256 Len=0
170	101.051949716	192.168.68.109	192.168.68.113	TCP	62	63169 → 12345 [FIN, ACK] Seq=46 Ack=46 Win=131328 Len=0
171	101.052012960	192.168.68.113	192.168.68.109	TCP	56	12345 → 63169 [ACK] Seq=47 Ack=47 Win=64256 Len=0
172	101.051949940	192.168.68.109	192.168.68.113	TCP	62	63169 → 12345 [ACK] Seq=47 Ack=47 Win=131328 Len=0
Frame 172: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)						
Linux cooked capture						
Internet Protocol Version 4, Src: 192.168.68.109, Dst: 192.168.68.113						
Transmission Control Protocol, Src Port: 63169, Dst Port: 12345, Seq: 47, Ack: 47, Len: 0						
Source Port: 63169						
Destination Port: 12345						
[Stream index: 2]						
[TCP Segment Len: 0]						
Sequence number: 47 (relative sequence number)						
Sequence number (raw): 4149355448						
[Next sequence number: 47 (relative sequence number)]						
Acknowledgment number: 47 (relative ack number)						
Acknowledgment number (raw): 2713553975						
0101 .... = Header Length: 20 bytes (5)						
Flags: 0x010 (ACK)						
Window size value: 513						
[Calculated window size: 131328]						
[Window size scaling factor: 256]						
Checksum: 0x33a9 [unverified]						
0000	00 00 00 01 00 06 d8 c0	a6 0c 90 37 00 00 08 00	.....7....			
0010	45 00 00 28 6e 37 40 00	80 06 82 69 c0 a8 44 6d	E..(n70...i..Dm			
0020	c0 a8 44 71 f6 c1 50 39	f7 52 23 b8 a1 bd 8c 37	..Dq...09..R#...7			
0030	50 10 02 01 33 a9 00 00	00 00 00 00 00 00 00	P...3... .....			