

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp && tcp.port == 12345

No.	Time	Source	Destination	Protocol	Length	Info
10	1.693663915	192.168.1.236	192.168.1.234	TCP	76	54988 → 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=...
12	1.804941138	192.168.1.234	192.168.1.236	TCP	76	12345 → 54988 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460...
13	1.805000455	192.168.1.236	192.168.1.234	TCP	68	54988 → 12345 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1491228...
14	1.805133389	192.168.1.236	192.168.1.234	TCP	91	54988 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=23 TSval=1...
15	1.807739794	192.168.1.234	192.168.1.236	TCP	68	12345 → 54988 [ACK] Seq=1 Ack=24 Win=65152 Len=0 TSval=157993...
16	1.807740067	192.168.1.234	192.168.1.236	TCP	91	12345 → 54988 [PSH, ACK] Seq=1 Ack=24 Win=65152 Len=23 TSval=...
17	1.807776443	192.168.1.236	192.168.1.234	TCP	68	54988 → 12345 [ACK] Seq=24 Ack=24 Win=64256 Len=0 TSval=14912...
18	1.807939764	192.168.1.236	192.168.1.234	TCP	87	54988 → 12345 [PSH, ACK] Seq=24 Ack=24 Win=64256 Len=19 TSval=...
19	1.809540290	192.168.1.234	192.168.1.236	TCP	68	12345 → 54988 [ACK] Seq=24 Ack=43 Win=65152 Len=0 TSval=15799...
20	1.809975341	192.168.1.234	192.168.1.236	TCP	87	12345 → 54988 [PSH, ACK] Seq=24 Ack=43 Win=65152 Len=19 TSval=...
21	1.809986876	192.168.1.236	192.168.1.234	TCP	68	54988 → 12345 [ACK] Seq=43 Ack=43 Win=64256 Len=0 TSval=14912...
22	1.810150047	192.168.1.236	192.168.1.234	TCP	68	54988 → 12345 [FIN, ACK] Seq=43 Ack=43 Win=64256 Len=0 TSval=...
23	1.811806095	192.168.1.234	192.168.1.236	TCP	68	12345 → 54988 [FIN, ACK] Seq=43 Ack=44 Win=65152 Len=0 TSval=...
24	1.811825516	192.168.1.236	192.168.1.234	TCP	68	54988 → 12345 [ACK] Seq=44 Ack=44 Win=64256 Len=0 TSval=14912...

Frame 14: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface any, id 0
 Linux cooked capture
 Internet Protocol Version 4, Src: 192.168.1.236, Dst: 192.168.1.234
 Transmission Control Protocol, Src Port: 54988, Dst Port: 12345, Seq: 1, Ack: 1, Len: 23
 Data (23 bytes)

```

0000 00 04 00 01 00 06 d8 3b bf e7 00 31 00 00 08 00  ....1....
0010 45 00 00 4b c8 84 40 00 40 06 ed 01 c0 a8 01 ec  E-K-@-@-...
0020 c0 a8 01 ea d6 cc 30 39 60 d3 3d 12 60 75 32 62  ....09-=-u2b
0030 80 18 01 f6 85 64 00 00 01 01 08 0a 58 e2 58 6c  ....d-...X-X1
0040 5e 2b ef b9 48 61 64 61 72 20 50 69 6e 74 6f 20  ^+..Hada r Pinto
0050 44 76 69 72 20 50 6f 6c 6c 61 6b                Dvir Pol lak

```

wireshark_any_20211118171850_nh6DgT.pcapng

Packets: 69 · Displayed: 14 (20.3%) · Dropped: 0 (0.0%) Profile: Default

מורה נבוכים:

server port: 12345 server ip: 192.168.1.234
 client port: 54988 client ip : 192.168.1.236

ניתן לראות בצילום המסך, את התעבורה בין שני המחשבים הריצים את קודי השרת והלקוח, כאשר אנחנו מעבירים שני מסרים – הראשונה היא השמות שלנו, והמסר השני הוא מספרי תעודת הזהות שלנו.
 כפי שרואים בשורות הראשונות, שני המחשבים צריכים לבצע סנכרון ביניהם – "לחיצת ידיים". הדבר מתבטא בשורות (מסומן באדום). ניתן לראות כי הכיתוב [סין] מרמז על החיבור כפי שלמדנו בכיתה 1,2.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp && tcp.port == 12345

No.	Time	Source	Destination	Protocol	Length	Info
10	1.693663915	192.168.1.236	192.168.1.234	TCP	76	54988 → 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=...
12	1.804941138	192.168.1.234	192.168.1.236	TCP	76	12345 → 54988 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460...
13	1.805000455	192.168.1.236	192.168.1.234	TCP	68	54988 → 12345 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1491228...
14	1.805133389	192.168.1.236	192.168.1.234	TCP	91	54988 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=23 TSval=1...
15	1.807739794	192.168.1.234	192.168.1.236	TCP	68	12345 → 54988 [ACK] Seq=1 Ack=24 Win=65152 Len=0 TSval=157993...
16	1.807740067	192.168.1.234	192.168.1.236	TCP	91	12345 → 54988 [PSH, ACK] Seq=1 Ack=24 Win=65152 Len=23 TSval=...
17	1.807776443	192.168.1.236	192.168.1.234	TCP	68	54988 → 12345 [ACK] Seq=24 Ack=24 Win=64256 Len=0 TSval=14912...
18	1.807939764	192.168.1.236	192.168.1.234	TCP	87	54988 → 12345 [PSH, ACK] Seq=24 Ack=24 Win=64256 Len=19 TSval=...
19	1.809540290	192.168.1.234	192.168.1.236	TCP	68	12345 → 54988 [ACK] Seq=24 Ack=43 Win=65152 Len=0 TSval=15799...
20	1.809975341	192.168.1.234	192.168.1.236	TCP	87	12345 → 54988 [PSH, ACK] Seq=24 Ack=43 Win=65152 Len=19 TSval=...
21	1.809986876	192.168.1.236	192.168.1.234	TCP	68	54988 → 12345 [ACK] Seq=43 Ack=43 Win=64256 Len=0 TSval=14912...
22	1.810150047	192.168.1.236	192.168.1.234	TCP	68	54988 → 12345 [FIN, ACK] Seq=43 Ack=43 Win=64256 Len=0 TSval=...
23	1.811806095	192.168.1.234	192.168.1.236	TCP	68	12345 → 54988 [FIN, ACK] Seq=43 Ack=44 Win=65152 Len=0 TSval=...
24	1.811825516	192.168.1.236	192.168.1.234	TCP	68	54988 → 12345 [ACK] Seq=44 Ack=44 Win=64256 Len=0 TSval=14912...

[Stream index: 0]
 [TCP Segment Len: 0]
 Sequence number: 1 (relative sequence number)
 Sequence number (raw): 1624456466
 [Next sequence number: 1 (relative sequence number)]
 Acknowledgment number: 1 (relative ack number)
 Acknowledgment number (raw): 1618293346
 1000 = Header Length: 32 bytes (8)
 Flags: 0x010 (ACK)
 Window size value: 502
 [Calculated window size: 64256]
 [Window size scaling factor: 128]
 Checksum: 0x854d [unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0
 Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 [SEQ/ACK analysis]
 [Timestamps]

```

0000 00 04 00 01 00 06 d8 3b bf e7 00 31 00 00 08 00  ....1....
0010 45 00 00 34 c8 83 40 00 40 06 ed 19 c0 a8 01 ec  ..4-@-@-...
0020 c0 a8 01 ea d6 cc 30 39 60 d3 3d 12 60 75 32 62  ....09-=-u2b
0030 80 18 01 f6 85 64 00 00 01 01 08 0a 58 e2 58 6c  ....M-...X-X1
0040 5e 2b ef b9                ^+..

```

Acknowledgment number (tcp.ack), 4 bytes

Packets: 69 · Displayed: 14 (20.3%) · Dropped: 0 (0.0%) Profile: Default

נתייחס בתמונה זו לסקוואנס ולאק. ניתן לראות בתחילת התעבורה כי הסרבר שולח את האק הראשון על מנת להראות כי כפי 1אכן השרת והלקוח מסונכרנים בתקשורת. נביט בנוסף, בסקוונס, כי אנחנו מקבלים את הסקוונס הקודם בתוספת שלמדנו בכיתה

יש ציין כי המספרים הרשומים בסקוונס ובא"ק הינם מספרים רלטיביים ביחס לתחילת התקשורת שלנו. בסימון הכחול ניתן לראות את המספר הרלטיבי של הא"ק, ומתחתיו את המספר האמיתי שהמחשבים עובדים איתם.
 נציין, כי כל שליחה של תעבורה מלקוח לשרת וכדומה, גורמת לעדכון הסקוונס בכך שכמות הבייטים הנשלחים מתווספים לערך הסקוונס, וכאשר חוזר אק על קבלת המסר, נשלח בחזרה הסקוונס פלוס אחד. דוגמה לתרחיש שפורט לעיל מסומן בירוק

לסיום, כמה מילים על ניתוק התעבורה

ניתן לראות כי קיימת התנתקות "משולשת", כלומר, הלקוח שולח כי ברצונו לסגור את התקשורת בינו לבין השרת, ומכך השרת מאשר כי הוא קיבל את הרצון להתנתק, ושולחן פין בעצמו על מנת להתנתק. הלקוח מסיים את תהליך ההתנתקות בכך שהוא שולח לשרת כי הוא קיבל את הפין שלו ונסגר הסוקט