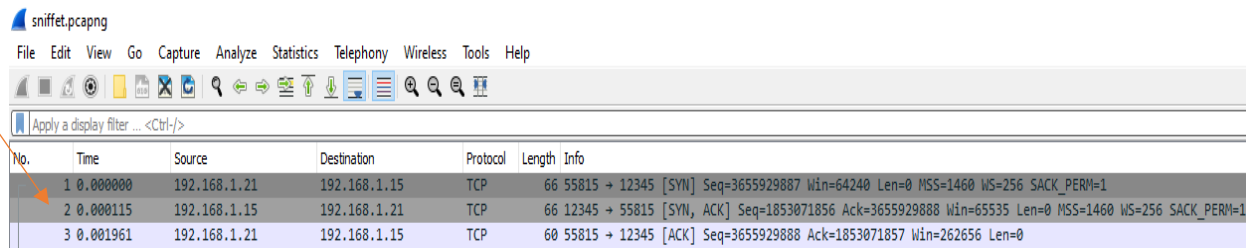


חלק א'

IP לקוח-192.168.1.21

IP שרת-192.168.1.15

הקמת החיבור :



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.21	192.168.1.15	TCP	66	55815 → 12345 [SYN] Seq=3655929887 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000115	192.168.1.15	192.168.1.21	TCP	66	12345 → 55815 [SYN, ACK] Seq=1853071856 Ack=3655929888 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
3	0.001961	192.168.1.21	192.168.1.15	TCP	60	55815 → 12345 [ACK] Seq=3655929888 Ack=1853071857 Win=262656 Len=0

תצלום 1.1 : הקמת חיבור

1 : הלקוח מנסה להתחבר לשרת, על ידי שליחת SYN, הוא מעביר לו את seq number שאליו אמור להתחיל להיכתב המידע.

2 : השרת מחזיר לו בהודעה המכילה שתי מטרות, הראשונה ACK על הודעת הSYN של הלקוח, שבעקבותיה הוא מצרף את הack number שעד אליו קיבל את המידע, שהוא seq+1 שהלקוח שלח.

בנוסף הוא שולח בהודעה SYN ללקוח בכך מודיע שרוצה לקיים אתו חיבור, כמו קודם לכן הוא מצרף seq כדי להגיד מאיפה להתחיל לכתוב את המידע.

3 : הלקוח מחזיר הודעת ACK כדי לסמן לשרת שאכן קיבל את הSYN שלו, הוא מצרף אליה number שעד אליו קיבל את המידע, שהוא seq+1 שהשרת שלח.

מהלך החיבור :

3	0.001961	192.168.1.21	192.168.1.15	TCP	60	55815 → 12345 [ACK] Seq=3655929888 Ack=1853071857 Win=262656 Len=0
4	0.001961	192.168.1.21	192.168.1.15	TCP	81	55815 → 12345 [PSH, ACK] Seq=3655929888 Ack=1853071857 Win=262656 Len=27
5	0.018627	192.168.1.15	192.168.1.21	TCP	81	12345 → 55815 [PSH, ACK] Seq=1853071857 Ack=3655929915 Win=65536 Len=27
6	0.074018	192.168.1.21	192.168.1.15	TCP	60	55815 → 12345 [ACK] Seq=3655929915 Ack=1853071884 Win=262656 Len=0
7	0.080125	192.168.1.21	192.168.1.15	TCP	74	55815 → 12345 [PSH, ACK] Seq=3655929915 Ack=1853071884 Win=262656 Len=20
8	0.080187	192.168.1.15	192.168.1.21	TCP	74	12345 → 55815 [PSH, ACK] Seq=1853071884 Ack=3655929935 Win=65536 Len=20

תצלום 1.2 : מהלך החיבור

4 : הלקוח שולח לשרת את השמות שלנו ומצרף את הseq והlen כדי שהשרת ידע מאיפה להתחיל לכתוב את המידע recv buffer ואת אורכו הוא גם מעביר את הack number.

¹ כשאנו מסבירים לפי מספר מסוים הכוונה לפי מספר ההודעה (ראה חץ כתום)

0000	58 fb 84 c6 4b 02 fc aa	14 86 f8 86 08 00 45 00	X...K... ..E.
0010	00 43 3c 35 40 00 80 06	3b 0b c0 a8 01 15 c0 a8	.C<5@... ;.....
0020	01 0f da 07 30 39 d9 e9	10 20 6e 73 a1 f1 50 18	...09... ns...P.
0030	04 02 31 ff 00 00 59 6f	67 65 76 20 41 62 61 72	..1...Yo gev Abar
0040	62 61 6e 65 6c 2c 20 49	64 6f 20 42 61 72 6b 61	banel, I do Barka
0050	69		i

תצלום 1.3 : תוכן הפקטה שנשלחה ע"י הלקוח המכילה את השמות

5 : השרת מחזיר את המידע בהודעה משולבת, הוא גם מודיע שקיבל את המידע ניתן לראות זאת כי ה ack number גדל בדיוק באורך המידע שהלקוח שלח (ביחס להודעה 3), ובנוסף הוא מחזיר ללקוח את מה ששלח לכן הוא מצרף את ה seq, len שתפקידם כפי שתיארתי קודם.

0000	fc aa 14 86 f8 86 58 fb	84 c6 4b 02 08 00 45 00X. .K...E.
0010	00 43 d4 ce 40 00 40 06	e2 71 c0 a8 01 0f c0 a8	.C...@...@. .q.....
0020	01 15 30 39 da 07 6e 73	a1 f1 d9 e9 10 3b 50 18	..09...ns;P.
0030	01 00 76 07 00 00 59 4f	47 45 56 20 41 42 41 52	..v...YO GEV ABAR
0040	42 41 4e 45 4c 2c 20 49	44 4f 20 42 41 52 4b 41	BANEL, I DO BARKA
0050	49		I

תצלום 1.4 : תוכן הפקטה שחזרה מן השרת

6 : הלקוח מחזיר ACK על המידע שהשרת שלח, שוב ניתן לראות זאת כי ה ack number גדל בדיוק באורך המידע שנשלח.

7 : כעת, הלקוח שולח שוב לשרת הפעם את התז שלנו, כמו עם השמות seq מייצג מאיפה לרשום את המידע ב buffer וה len את גודלו.

0000	58 fb 84 c6 4b 02 fc aa	14 86 f8 86 08 00 45 00	X...K... ..E.
0010	00 3c 3c 37 40 00 80 06	3b 10 c0 a8 01 15 c0 a8	.<<7@... ;.....
0020	01 0f da 07 30 39 d9 e9	10 3b 6e 73 a2 0c 50 18	...09... ;ns...P.
0030	04 02 25 59 00 00 33 32	36 31 31 36 39 31 30 2c	..%Y...32 6116910,
0040	20 33 32 36 36 32 39 39	38 37	3266299 87

תצלום 1.5 : תוכן הפקטה שנשלחה ע"י הלקוח המכילה תז

8 : השרת מחזיר כמובן ack על המידע (ניתן לראות שגדל בכאורך המידע אשר נשלח), בנוסף הוא מחזיר seq, len מתאימים כי הוא מחזיר ללקוח את התז.

0000	fc aa 14 86 f8 86 58 fb 84 c6 4b 02 08 00 45 00X. .K...E.
0010	00 3c d4 cf 40 00 40 06 e2 77 c0 a8 01 0f c0 a8	<...@.@. .w.....
0020	01 15 30 39 da 07 6e 73 a2 0c d9 e9 10 4f 50 18	..09...nsOP.
0030	01 00 28 47 00 00 33 32 36 31 31 36 39 31 30 2c	..(G...32 6116910,
0040	20 33 32 36 36 32 39 39 38 37	3266299 87

תצלום 1.6 : תוכן הפקטה שחזרה בתגובה מהשרת

סיום החיבור:

7 0.080125	192.168.1.21	192.168.1.15	TCP	74 55815 → 12345 [PSH, ACK] Seq=3655929915 Ack=1853071884 Win=262656 Len=20
8 0.080187	192.168.1.15	192.168.1.21	TCP	74 12345 → 55815 [PSH, ACK] Seq=1853071884 Ack=3655929935 Win=65536 Len=20
9 0.080261	192.168.1.15	192.168.1.21	TCP	54 12345 → 55815 [FIN, ACK] Seq=1853071904 Ack=3655929935 Win=65536 Len=0
10 0.080844	192.168.1.21	192.168.1.15	TCP	60 55815 → 12345 [FIN, ACK] Seq=3655929935 Ack=1853071884 Win=262656 Len=0
11 0.080864	192.168.1.15	192.168.1.21	TCP	54 12345 → 55815 [ACK] Seq=1853071905 Ack=3655929936 Win=65536 Len=0
12 0.082154	192.168.1.21	192.168.1.15	TCP	60 55815 → 12345 [RST, ACK] Seq=3655929936 Ack=1853071904 Win=0 Len=0

תצלום 1.7 : סיום החיבור

9 : השרת שולח ללקוח שהוא רוצה להתנתק בעזרת הודעת FIN

10 : הלקוח שולח לשרת שהוא רוצה להתנתק על ידי הודעת FIN (הוא לא קיבל עדיין את שלו- נסיק זאת כי ack number לא גדל מהודעה 7)

11 : השרת מאשר את הודעת ה-FIN של הלקוח (נסיק זאת כי ה-ack גדל מאז הודעה 9)

12 : הלקוח מאשר את הודעת ה-FIN של השרת (נראה שהשרת כבר סגר את החיבור כי הוא רצה לסגור וגם קיבל הודעת FIN מהלקוח לכן הוא סגר את החיבור מה שגרם לכך שהודעת ה-ACK של הלקוח על הסגירה לא להגיע)