

מטלה מס' 2 – אילאי בן יהושע ונועם ליבוביץ

ראשית נתאים ונשנה את הקוד כך שישלח את שמותינו לשרת, באופן הבא –

```
tcp_server.py X
tcp_server.py > ...
1 import socket
2 server = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
3 server.bind(('', 12345))
4 server.listen(5)
5
6 while True:
7     client_socket, client_address = server.accept()
8     print('Connection from: ', client_address)
9     data = client_socket.recv(100)
10    print('Received: ', data)
11    client_socket.send(data.upper())
12    client_socket.close()
13    print('Client disconnected')
```

```
tcp_client.py X
tcp_client.py > ...
1 import socket
2 s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
3 s.connect(('192.168.135.1', 12345))
4 s.send(b'Noam and Elay')
5 data = s.recv(100)
6 print("Server sent: ", data)
7 s.close()
```

כעת נריץ את הקודים המעודכנים הנ"ל, נסניף את המידע בעזרת "כריש-הכבל" (בלעז – Wireshark), מעתה והילך כאשר נכתוב 'כריש' בקיצור נתייחס למינוח הזה), וננתח את מה שקרה פה בהתאם לעקרונות TCP שראינו בהרצאה ובתרגול.

זה מה שמוצג לנו בכריש לאחר הרצת הקודים -

No.	Time	Source	Destination	Proto	Length	Info
1	0.0000	192.168.13...	192.168.13...	TCP	74	52970 → 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2648340298 TSecr=0 WS=128
2	0.0002	192.168.13...	192.168.13...	TCP	74	12345 → 52970 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM TSval=5376432 TSecr=264834
3	0.0006	192.168.13...	192.168.13...	TCP	66	52970 → 12345 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2648340299 TSecr=5376432
4	0.0008	192.168.13...	192.168.13...	TCP	79	52970 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=13 TSval=2648340299 TSecr=5376432
5	0.0015	192.168.13...	192.168.13...	TCP	79	12345 → 52970 [PSH, ACK] Seq=1 Ack=14 Win=1049600 Len=13 TSval=5376433 TSecr=2648340299
6	0.0015	192.168.13...	192.168.13...	TCP	66	12345 → 52970 [FIN, ACK] Seq=14 Ack=14 Win=1049600 Len=0 TSval=5376434 TSecr=2648340299
7	0.0018	192.168.13...	192.168.13...	TCP	66	52970 → 12345 [ACK] Seq=14 Ack=14 Win=64256 Len=0 TSval=2648340300 TSecr=5376433
8	0.0021	192.168.13...	192.168.13...	TCP	66	52970 → 12345 [FIN, ACK] Seq=14 Ack=15 Win=64256 Len=0 TSval=2648340300 TSecr=5376434
9	0.0026	192.168.13...	192.168.13...	TCP	66	12345 → 52970 [ACK] Seq=15 Ack=15 Win=1049600 Len=0 TSval=5376435 TSecr=2648340300

נעבור על כל חבילה וחבילה על מנת לתאר במדויק כל שלב בתקשורת.

חבילה מס' 1 –

The image shows a Wireshark packet capture of a TCP connection. The first packet (No. 1) is a SYN packet from 192.168.135.1 to 192.168.135.128 on port 52970. The packet details show the following information:

- Source Port: 52970
- Destination Port: 12345
- Sequence Number (raw): 1035627461
- Next Sequence Number: 1 (relative sequence number)
- Acknowledgment Number: 0
- Acknowledgment number (raw): 0
- Flags: 0x0002 (SYN)
- Window: 64240
- Checksum: 0xff73 [unverified]
- Checksum Status: Unverified
- Urgent Pointer: 0
- Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window s...

אנו רואים פניה שמתבצעת לPORT - 12345 (אשר אותו נתנו ידנית לשרת), אשר מגיעה מפורט מקור 52970 אשר ניתן דינאמית ללקוח ע"י מ"ה (כיוון שלא צמדנו אותו לפורט ספציפי). הפנייה היא מסוג syn (ניתן לראות את הדגל הדלוק), כלומר הלקוח מבקש להסתנכרן עם השרת וזוהי תפקידה של החבילה הנ"ל עם דגל החס, אשר מהווה את השלב הראשון בטקס 'לחיצת הידיים המשולשת'. בנוסף לכך אנו רואים את ערך האופסט הגולמי (= raw) של הseq

שבחר הלקוח, כאשר ניתן לראות שהוא החליט שתחילת התקשורת תתחיל מאופסט '1305627461', ואילו ברור לנו שערך הack שלו כרגע יהיה '0', כיוון שהack שלו, זה הseq של השרת (אשר טרם נבחר..). כמובן שהlen הוא 0 שהרי אין דאטא בהודעת syn.

דבר מעניין נוסף ניתן לראות כאשר נפתח את הoptions –

```
Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
TCP Option - Maximum segment size: 1460 bytes
TCP Option - SACK permitted
TCP Option - Timestamps: TSval 2648340298, TSecr 0
TCP Option - No-Operation (NOP)
TCP Option - Window scale: 7 (multiply by 128)
[Timestamps]
```

ובו, הלקוח מציין בפני השרת – "רק שתדע, המss שלי הוא 1460b".

חבילה מס' 2 –

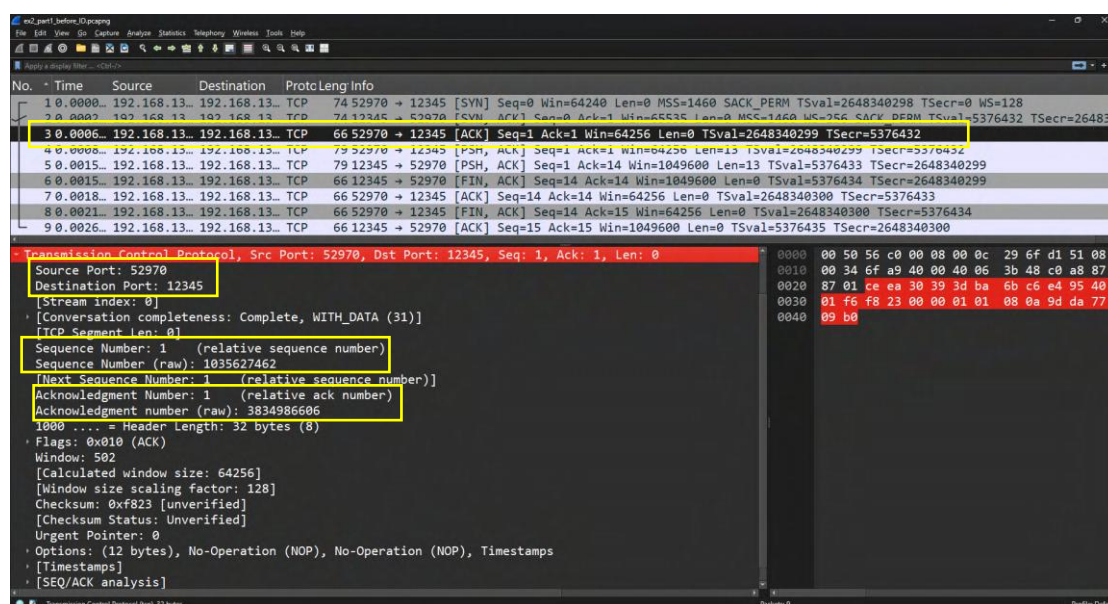
The image shows a Wireshark packet capture of a TCP SYN-ACK packet. The packet list shows a packet from 192.168.13 to 192.168.13 on port 52970. The packet details pane shows the following information:

- Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{ED60E847...}
- Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: VMware_6f:d1:51 (00:0c:29:6f:d1:51)
- Internet Protocol Version 4, Src: 192.168.135.1, Dst: 192.168.135.128
- Transmission Control Protocol, Src Port: 12345, Dst Port: 52970, Seq: 0, Ack: 1, Len: 0
 - Source Port: 12345
 - Destination Port: 52970
 - [Stream index: 0]
 - [Conversation completeness: Complete, WITH_DATA (31)]
 - [TCP Segment Len: 0]
 - Sequence Number: 0 (relative sequence number)
 - Sequence Number (raw): 3834986605
 - Max Sequence Number: 1 (relative sequence number)
 - Acknowledgment Number: 1 (relative ack number)
 - Acknowledgment number (raw): 1035627462
 - 1010
 - Header Length: 40 bytes (10)
 - Flags: 0x012 (SYN, ACK)
 - Window: 65535
 - [Calculated window size: 65535]
 - Checksum: 0xcbbd [unverified]
 - [Checksum Status: Unverified]
 - Urgent Pointer: 0
 - Options: (20 bytes), Maximum segment size, No-Operation (NOP), Window scale, SACK permitted, Timestamps

אנו רואים פניה שמתבצעת הפעם בכיוון ההפוך מ-PORT 12345 (השרת), אשר מיודעת לפורט 52970 (הלקוח). הפניה (או יותר נכון 'תגובה') מצד השרת הינה מסוג syn, ack (גם פה ניתן לראות את שני הדגלים דלוקים), כלומר השרת ראשית מכיר בסכרון של הלקוח איתו, אך בנוסף הוא מבקש להסתנכרן גם הוא עם הלקוח. זוהי למעשה תפקידה של החבילה הנ"ל עם דגלי הack, syn, אשר מהווה את השלב השני בטקס 'לחיצת הידיים המשולשת'. ראוי לציין כי השלב הנ"ל עשוי להתבצע לעיתים ב2 חבילות שונות (1 לack ואחת לsyn) אך כמו שאנו רואים כאן, אלו יכולות להישלח גם כן יחדיו בחבילה אחת. בנוסף לכך אנו רואים את ערך האופסט הגולמי (= raw) של הseq שבחר השרת, כאשר ניתן לראות שהוא החליט שתחילת התקשורת תתחיל מאופסט '3834986605', ואילו נשים לב שערך הack שלו יהיה '1305627462', שזה 1 יותר משהיה הseq של הלקוח בגלל phantom-bit. גם כאן הlen הוא 0 שהרי אנחנו עדיין לא בשלב של העברת דאטא, אך מאוד מתקרבים לשם. אם נפתח את הoptions נשים לב שגם השרת מציין בפני הלקוח מהו המss שלו – 1460b, כדי שזה ידע את הנתון כאשר הוא שולח אליו הודעות.

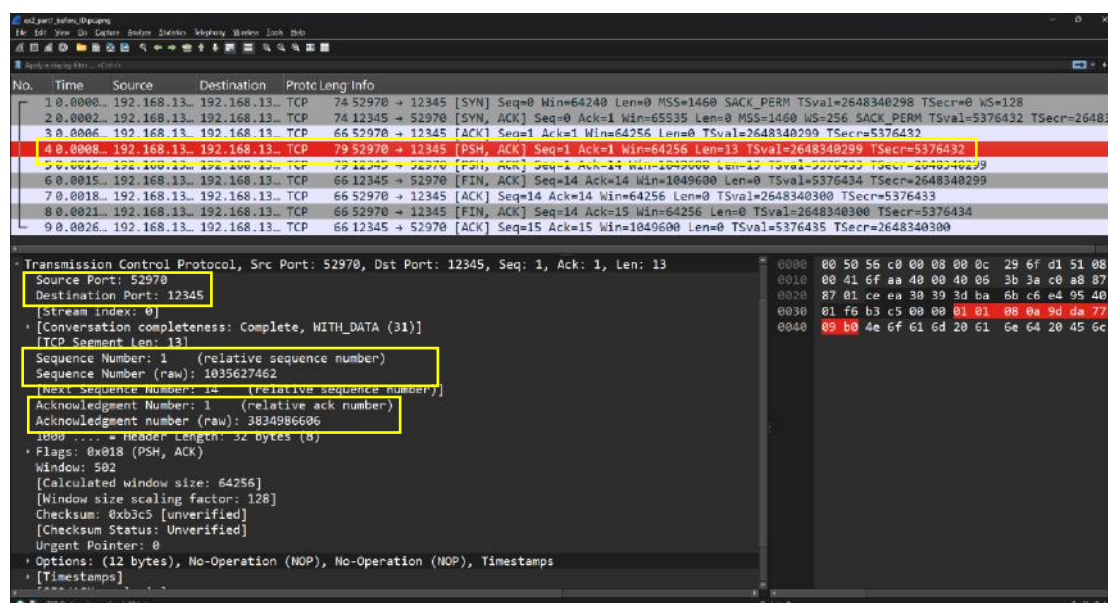
```
Options: (20 bytes), Maximum segment size, No-Operation (NOP), Window scale, SACK permitted, Timestamps
TCP Option - Maximum segment size: 1460 bytes
TCP Option - No-Operation (NOP)
TCP Option - Window scale: 8 (multiply by 256)
TCP Option - SACK permitted
TCP Option - Timestamps: TSval 5376432, TSecr 2648340298
[Timestamps]
[SEQ/ACK analysis]
```


חבילה מס' 3 –



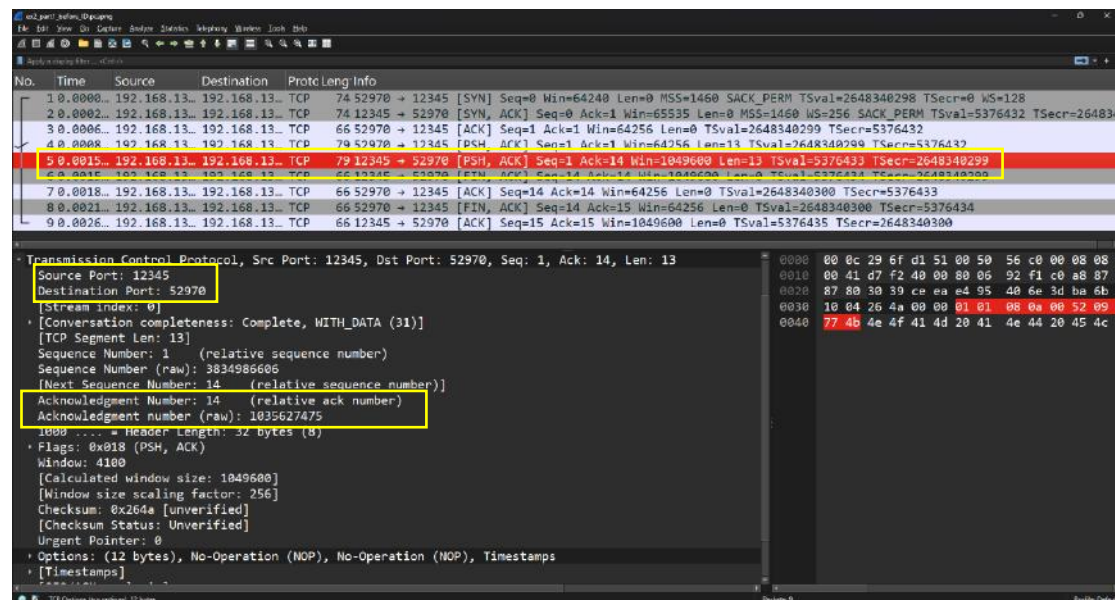
כעת ניתן לראות פניה נוספת מהלקוח 52970 (הלקוח), אל השרת. הפניה מצד השרת הינה מסוג ack (שוב הדגל דלוק ולמעשה מעתה והילך הוא יהיה דלוק עד סוף התקשורת, אז נפסיק לציין זאת...), דהיינו הלקוח גם הוא מכיר בהכרת השרת בסנכרון שלו, ולמעשה תפקידה של החבילה הזו מהווה את השלב השלישי והאחרון בטקס 'לחיצת הידיים המשולשת', שכן שני הצדדים הסתנכרנו אחד עם השני, וכל אחד מהם הכיר בסנכרון המשותף, ומכאן והילך הקשר שריר וניתן להעביר דרכו הודעות. שוב אנו רואים את ערך האופסט הגולמי (= raw) של האקט ששולח הלקוח, והוא – '3834986606', באופן לא מפתיע זה 1 יותר מהseq שבחר השרת (שוב אנחנו מגדילים בגלל הפאנטום ביט של האקט). הseq לעומת זאת לא השתנה שכן לא נשלח עוד דאטא, וכתוצאה מכך שוב החל הוא 0 (אך לא לעוד הרבה זמן). אם נפתח את הoptions נשים לב שהמס' שלו לא נשלח, שכן שני הצדדים כבר יודעים ומודעים למגבלות כל אחד של השני.

חבילה מס' 4 –



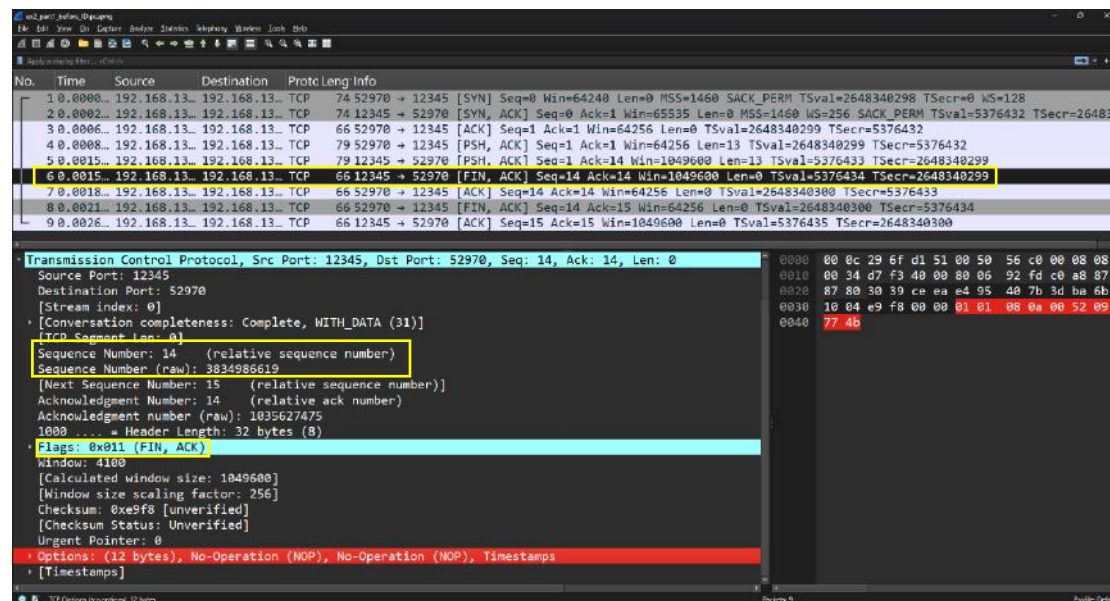
סוף כל סוף הגענו לחלק המעניין ('פסגת הקורס' לפי חלק מהשיטות), אנו רואים הודעה מהלקוח (לפי הפורט 52970 שראינו קודם שהוא הפורט של הלקוח), השולח 13 בתים (לפי ההנחה), שאנחנו יודעים שהם הבתים של המחרוזת 'Noam and Elay' (כנדרש במטלה), ובנוסף לדגל האק (שאמרנו שמעתה והילך תמיד יהיה דלוק), גם כן דלוק דגל הpush שכאילו אומר להעביר בדחיפות לאפליקציה את המידע שהגיע. נשים לב שעכשיו יש לנו גם את שכבת datan בהודעה (הבתים ששלחנו מאופן מקודד).

חבילה מס' 5 –



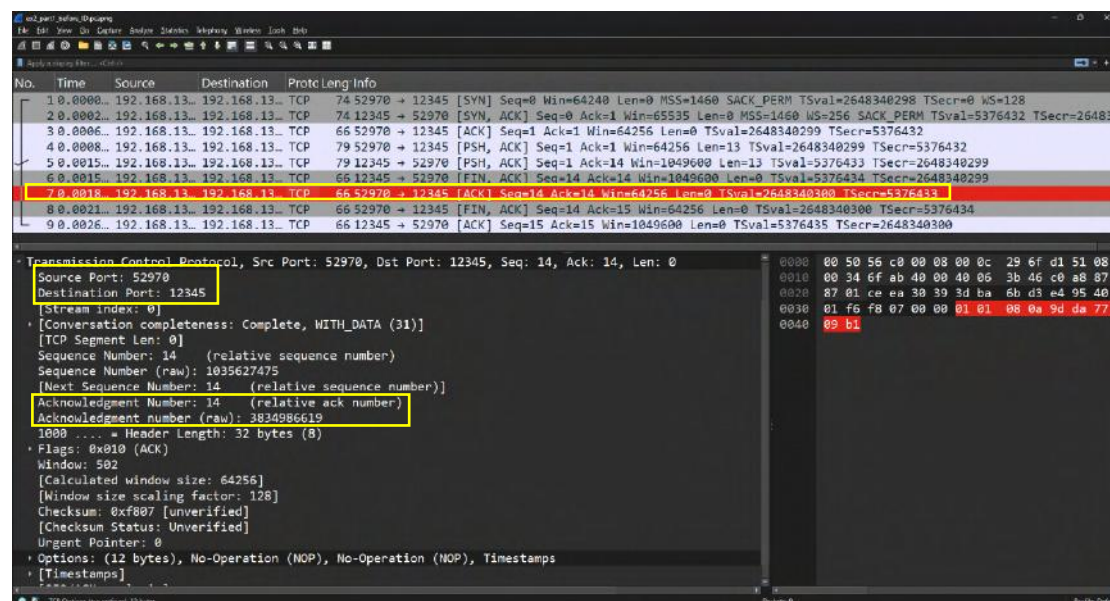
כעת נראה את תגובת השרת להודעה שקיבל מהלקוח בחבילה הקודמת שסקרנו. השרת ראשית מעדכן את המספר בשדה האק להיות 13 יותר משהיה – '1035627475' שכן עכשיו הוא אומר ללקוח – "שומע?! קיבלתי כבר עד בית מס' 1035627475 תן לי ממנו והלאה". אמנם seq לא משתנה כיוון שהוא טרם שלח דאטא משל עצמו ללקוח, אך כעת הוא מצרף להודעת האק את התוכן שקיבל בupper (ושוב אנו לא מופתעים שהלח הוא 13).

חבילה מס' 6 –



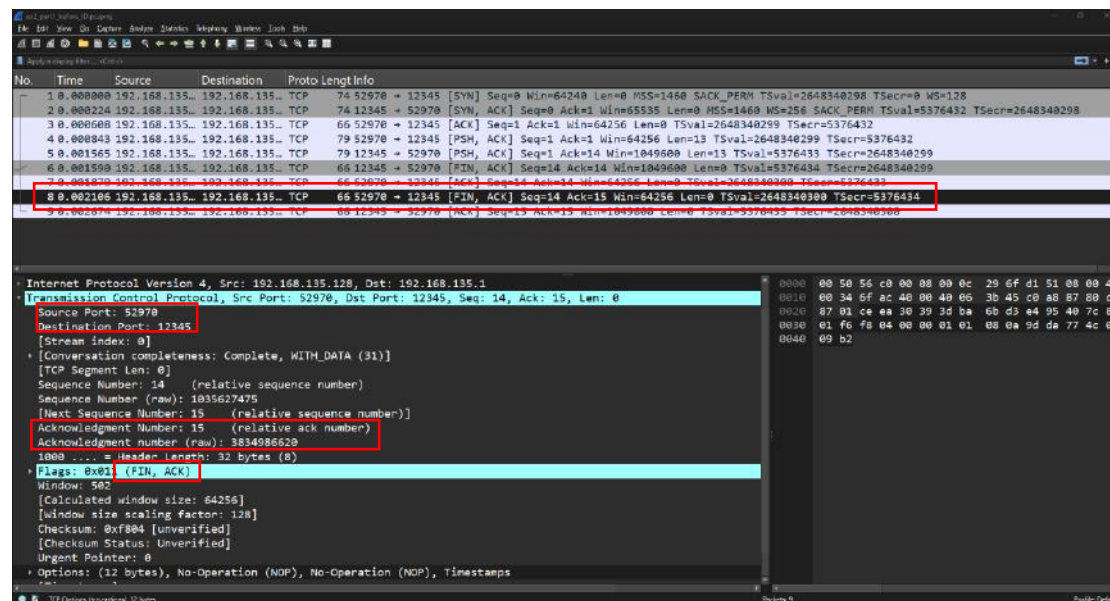
מיד לאחר שהשרת שולח את הודעת האקס עם התוכן upper, הוא שולח הודעת חס (ניתן לראות דגל דולק), שכן הוא עשה את שלו, ותפקיד ההודעה הזו להודיע על כך שהוא מעוניין לסיים את מערכת היחסים עם הלקוח. נשים לב שעכשיו הseq של השרת גדל ב13 גם הוא לערך – '3834986619'.

חבילה מס' 7 –



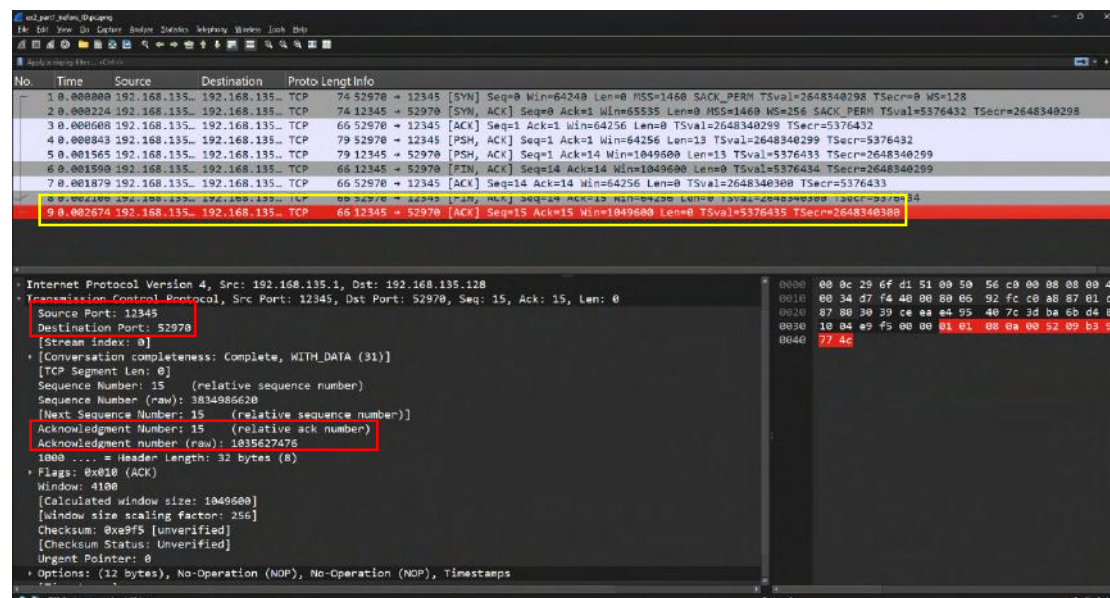
הלקוח מקבל את הדאטא חזרה מהשרת בupper, בהתאמה הוא מגדיל את ערך הacked ב13 בתים נוספים לערך – '3834986619'. כמו כן נשים לב שגם ערך הseq המצוין בהודעה גדל ב-13 מהפעם האחרונה בה ראינו חבילה נשלחת מהלקוח, וכעת הוא עומד על – '1035627475' (שוקינג זה האקס של השרת..).

חבילה מס' 8 –



הלקוח כעת שולח הודעת ack לשרת, ולמעשה מעדכן שהוא קיבל את ההודעה שלו בנוגע לסיום ההתקשרות עימו. כיוון שהוא הבין שנגמר הקשר, הוא מסיים אותו גם מבחינתו ומצרף זאת להודעה (דגל החיף דלוק בה). דהיינו תפקיד ההודעה לומר לשרת שהסיום הינו הדדי. מעבר לזה אין מידע מעניין למעט העובדה שערך האck של הלקוח גדל ב-1 כתוצאה מהפאנטום ביט של הודעה החיף שמוכרת רק עכשיו.

חבילה מס' 9 –



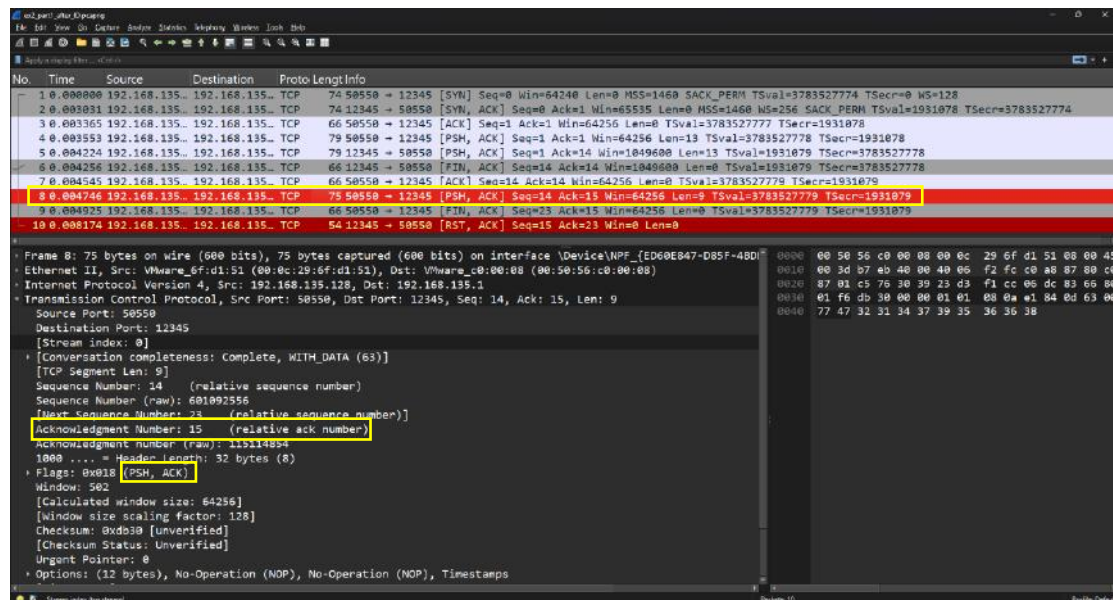
בחבילה האחרונה (🙄) שלנו אנו רואים את השרת מכיר בסיום ההתקשרות מצד הלקוח גם הוא בהודעת ack, ובאופן פרקטי תפקיד ההודעה הינו לסיים לחלוטין בהחלט את ערוץ התקשורת שהיה ביניהם. נשים לב שרגע לפני שהוא אומר "ביי", הוא מגדיל גם הוא את ערך האck כתוצאה מהפאנטום ביט של החיף שהגיע מהלקוח, סה"כ ערך האck של השרת בסיום התקשורת עומד על – '1035627476'.

סיימנו לנתח את התקשורת בחלק הראשון. נסיף כעת את שליחת ה-t.z. של אילאי לאחר שהשרת משיב את תשובתו ונראה את השינויים.

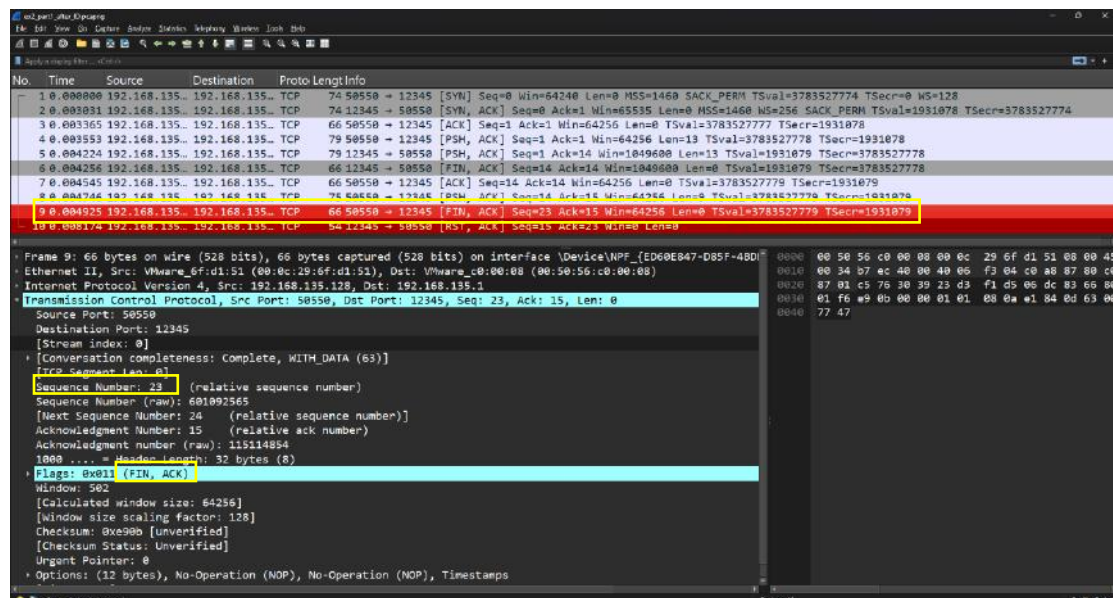
```
tcp_server.py
1 import socket
2 server = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
3 server.bind(('', 12345))
4 server.listen(5)
5
6 while True:
7     client_socket, client_address = server.accept()
8     print('Connection from: ', client_address)
9     data = client_socket.recv(100)
10    print('Received: ', data)
11    client_socket.send(data.upper())
12    client_socket.close()
13    print('Client disconnected')
```

```
tcp_client.py
1 import socket
2 s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
3 s.connect(('192.168.135.1', 12345))
4 s.send(b'Noam and Elay')
5 data = s.recv(100)
6 print("Server sent: ", data)
7 s.send(b'214795668')
8 s.close()
```

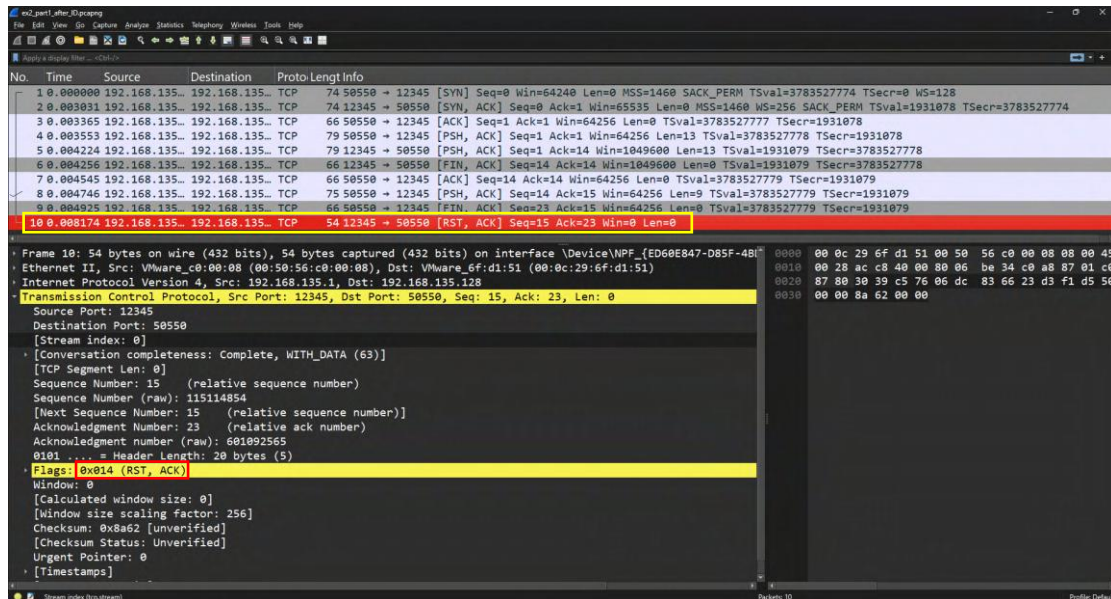
כל ההודעות בהתחלה תתנהגנה באופן זהה (לכן נחסוך ונתחיל רק מהמקום בו השינוי קורה), אבל עכשיו נשים לב –



לאחר שהלקוח החזיר ack על הfin של השרת (פאנטום ביט מגדיל ב1 את הacked), במקום לשלוח גם הוא fin (כמו שקרה קודם), הוא מנסה לשלוח הודעה נוספת לעשות לה psh לאפליקציה (הלוא היא ה-t.z.), ורק לאחר שההודעה הזו נשלחת, הוא שולח גם כן fin מצידו –



seq שלו גדל ב-9, והוא מסכים עכשיו לסיים את התקשורת. אלא שבגלל שהשרת לא ידע שעליו לצפות לחבילה נוספת הוא כבר סיים וסגר את העניין, ולכן נקבל ממנו הודעת rst –



כאילו רוצה לומר – "חדש אח שלי, חדש. מה שהיה אני כבר לא שם, ואין מי שישמע ויקבל את מה שיש לך לשלוח. אם אתה רוצה בוא נתחיל מההתחלה, ומשם נשתמע הלאה..".

ובכך סיימנו לנתח גם את המקרה בו הודעה נשלחת לאחר שהשרת עושה קלוז קודם לרגע בו היא מגיעה.

סעיף 2:

כעת, ננתח בקצרה את הקודים של הגרסאות השונות ואת התעבורה בהן:

גרסה v1:

The first screenshot shows the code for server.py. It imports socket and sys, sets TCP_IP to '0.0.0.0' and TCP_PORT to 5798. It binds a socket to these values and listens. In a while loop, it accepts connections, prints the address, receives data, and sends it back. It also handles a second connection. The second screenshot shows client.py, which imports socket, sys, and time. It takes command-line arguments for TCP_IP, TCP_PORT, and a message. It connects to the server and sends the message. The third screenshot is a Wireshark capture showing a TCP connection from 192.168.135.1 to 192.168.135.128. It highlights the first packet, a SYN packet, and shows the packet details, including the source and destination ports and the sequence number.

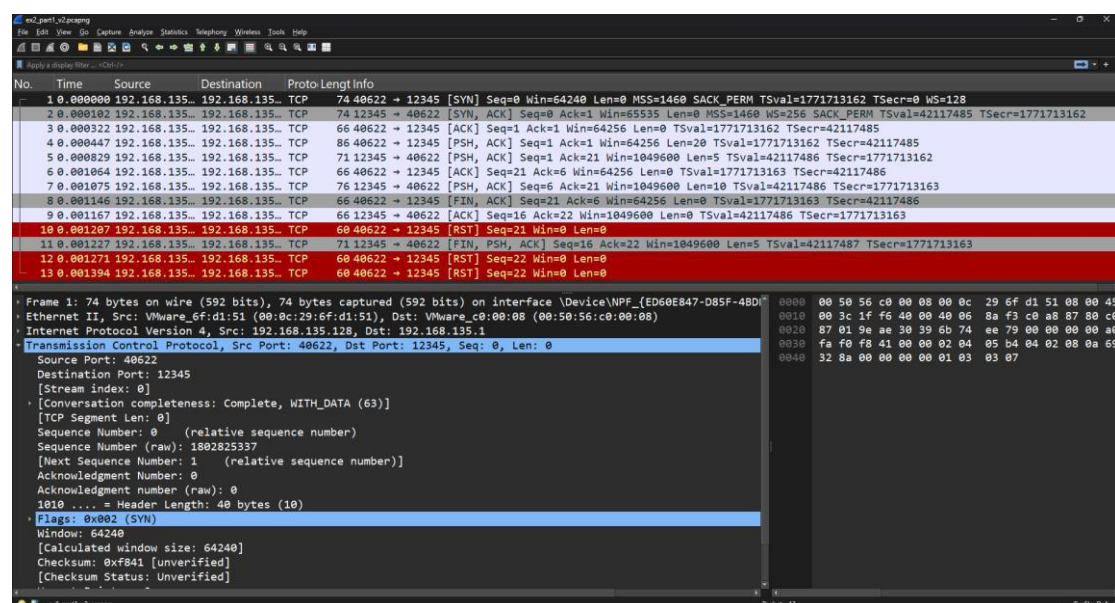
הלקוח מקבל את הIP והפורט מהארגומנטים לתוכנית, לאחר מכן הוא מתחבר בשני חיבורים נפרדים בעזרת שני סוקטים נפרדים (שורות 4 עד 9). הלקוח תחילה שולח הודעה דרך החיבור השני, מחכה 5 שניות ושולח הודעה אחרת דרך החיבור הראשון. לבסוף, הלקוח מקבל את שתי ההודעות מהסוקט בסדר הפוך לסדר בו התבצעה השליחה, ולאחר מכן סוגר את החיבורים. צד שני, השרת מאזין לכל החיבורים כיוון שהוא בחר בכתובת 0.0.0.0 ומקבל פורט כקלט. הוא מרים את השרת לאוויר כאשר הוא מוכן שיהיו ברגע נתון לכל היותר חיבור 1 בהמתנה (ליסטן שווה 0). הוא עושה accept לשני חיבורים (מדפיס מי הם), מקצר את ההודעה השנייה ל-7 תווים הראשונים שנקלטו ושולח אותה לחיבור הראשון, ואת ההודעה הראשונה ל-5 תווים הראשונים שנקלטו ושולח אותה לחיבור השני. לבסוף, יוזם ניתוק רק עם החיבור הראשון שהוא פתח.

נשים לב שבפועל בכריש קרה משהו מעניין. לאחר האתחול עד שורה 9, נשלחת ההודעה מהסוקט שנוצר שני בלקוח, והשרת לפני שהוא מחזיר עליה ack לאותו סוקט שני, קודם שולח את ההודעה המקוצרת (7 בתים), לחיבור הראשון (שורה 11). יתרה מזאת, הוא מקבל מהחיבור הראשון ack על ההודעה המקוצרת (שורה 12), ורק אז מחזיר ack על עצם זה שהוא קיבל את ההודעה המקורית מהחיבור השני. לאחר מכן השרת מקבל את ההודעה מהסוקט שנוצר ראשון בקליינט, ובאופן דומה לפני שהוא מחזיר עליה ack, הוא מעביר את 5 הבתים הראשונים מההודעה לחיבור סוקט השני. בשלב הזה מגיעה הודעת fin מהחיבור הראשון, אשר נענית בחיבור מצד השרת, ועל הדרך הוא גם נותן לו ack (רק בשלב הזה) על החבילה שנשלחה על ידו, ומיד הודעה נוספת של ack על החיבור עם הפאנטום ביט. החיבור השני מחזיר ack רק עכשיו על ההודעה שהוא קיבל (5 הבתים), החיבור הראשון מחזיר ack על הודעות החיבור שקיבל מהשרת (שוב פאנטום ביט), ולבסוף השרת מקבל fin מהחיבור השני ומשיב על כך באק (הוא לא שולח לו fin שכן בקוד החיבור השרת הינו עבור החיבור הראשון, שכבר נסגר מיוזמתו קודם לכן..).

גרסה v2:

```
server.py > ...
1 import socket,sys
2
3 TCP_IP = '0.0.0.0'
4 TCP_PORT = int(sys.argv[1])
5 BUFFER_SIZE = 5
6
7 s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
8 s.bind((TCP_IP, TCP_PORT))
9 s.listen(1)
10
11 while True:
12     conn, addr = s.accept()
13     print("New connection from:", addr)
14     while True:
15         data = conn.recv(BUFFER_SIZE)
16         if not data: break
17         print("received:", data)
18         conn.send(data.upper())
19     conn.close()
20
21
```

```
client.py > ...
1 import socket,sys
2
3 TCP_IP = sys.argv[1]
4 TCP_PORT = int(sys.argv[2])
5 BUFFER_SIZE = 1024
6 MESSAGE = b'World! Hello, World!'
7
8 s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
9 s.connect((TCP_IP, TCP_PORT))
10 s.send(MESSAGE)
11 data = s.recv(BUFFER_SIZE)
12 s.close()
13
14 print("received data:", data)
15
16
```



כמו בתוכנית הקודמת, הלקוח מקבל את IP והפורט מהארגומנטים לתוכנית, לאחר מכן הוא מתחבר לשרת ושולח לו את ההודעה המצוינת. הוא עושה recv מהשרת, ולאחר שקיבל את ההודעה שהגיעה חזרה מהשרת הוא מדפיס אותה. מצד שני, כמו בתוכנית הקודמת, השרת מאזין לכל החיבורים כיוון שהוא בחר בכתובת 0.0.0.0 ומקבל פורט קקלט. הוא פותח חיבור, מקבל את ההודעה בצאנקים של בתים 5 (כגודל הבאפר), עד שבתים מפסיקים להגיע, מדפיס כל צאנק, ושולח אותו חזרה ללקוח באופן של upper. לבסוף, הוא סוגר את החיבור.

כמו התפיסה האחרונה, ניתן לראות את לחיצת הידיים בין הלקוח לשרת (שורות 4 5 6). אך בשונה מהתפיסה האחרונה, השרת קולט את המידע שמגיע אליו מחיבור אחד בחתיכות של 5 תווים. לכן רואים בכריש את הצאנק הראשון מגיע ומוחזר מהשרת (בupper כמובן), ולפני שאנו רואים את המשך קבלת הצאנקים בשרת, אנו רואים את האק שהלקוח החזיר על הצאנק הראשון. משום מה השרת מאחד את 2 הצאנקים הבאים ושולח אותם יחדיו ללקוח, כאשר האחרון מחזיר עליהם ack. עם זאת, מכיוון שיש רק recv אחד בלקוח, הוא ממשיך בשלו ולאחר קבלת הצאנק הראשון הוא שולח fin כדי לסיים את ההתקשרות. השרת מקבל את fin ומחזיר עליה ack, אולם מעתה והילך שאר הצאנקים שהשרת שולח זוכים למענה של rst כיוון שאין אף אחד בצד השני ששומע וזמין לקבל. כנל לfin שהשרת שולח – הכל מקבל rst, שכן הלקוח ניתק בצד השני...

גרסה v3:

```

server.py
1 import socket,sys
2
3 TCP_IP = '0.0.0.0'
4 TCP_PORT = int(sys.argv[1])
5 BUFFER_SIZE = 1024
6
7 s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
8 s.bind((TCP_IP, TCP_PORT))
9 s.listen(1)
10
11 while True:
12     conn, addr = s.accept()
13     print('New connection from:', addr)
14     while True:
15         data = conn.recv(BUFFER_SIZE)
16         if not data: break
17         print("received:", data)
18         conn.send(data.upper()*1000)
19     conn.close()

```

```

client.py > ...
1 import socket,sys
2
3 TCP_IP = sys.argv[1]
4 TCP_PORT = int(sys.argv[2])
5 BUFFER_SIZE = 1024
6 MESSAGE = b'Hello, World!'
7
8 s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
9 s.connect((TCP_IP, TCP_PORT))
10 s.send(MESSAGE)
11 data = s.recv(BUFFER_SIZE)
12 print("received data:", data)
13 data = s.recv(BUFFER_SIZE)
14 print("received data:", data)
15 s.close()
16
17
18
19

```

The Wireshark capture shows the following details for the selected packet (No. 15):

- Ethernet II, Src: VMware_6f:d1:51 (08:0c:29:6f:d1:51), Dst: VMware_c8:00:08 (00:50:56:c8:00:08)**
- Internet Protocol Version 4, Src: 192.168.135.128, Dst: 192.168.135.1**
- Transmission Control Protocol, Src Port: 44550, Dst Port: 12345, Seq: 0, Len: 0**
- TCP Segment Len: 0**
- Sequence Number: 0 (relative sequence number)**
- Sequence Number (raw): 377262953**
- Next Sequence Number: 1 (relative sequence number)**
- Acknowledgment Number: 0**
- Acknowledgment number (raw): 0**
- 1010 ... = Header Length: 40 bytes (10)**
- Flags: 0x002 (SYN)**
- Window: 64240**
- [Calculated window size: 64240]**

כמו בתוכנית הקודמת, הקוד לא השתנה המון – הלקוח מקבל את התוכנית, לאחר מכן הוא מתחבר לשרת ושולח לו הודעה, אך בשונה מהתוכנית הקודמת, לאחר שקיבל את ההודעה חזרה מהשרת הוא מושך ומדפיס את ה-1024 בתים הראשונים ולאחר מכן שוב הוא מנסה למשוך עוד 1024 בתים. כמו כן בצד שני, כמו בתוכנית הקודמת, השרת מאזין לכל החיבורים כיוון שהוא בחר בכתובת 0.0.0.0 ומקבל פורט קקלט. הוא פותח חיבור, מקבל את 1024 הבתים הראשונים ושולח אותם חזרה ללקוח באותיות גדולות בהכפלה של 1000 פעמים הקלט. לבסוף, סוגר את החיבור.

כמו בתפיסה האחרונה, ניתן לראות את לחיצת הידיים בין הלקוח לשרת. מיד לאחר מכן את 13 הבתים שהלקוח שולח, ואז השרת קולט את כל המידע שמגיע אליו, ושולח אותו באותיות גדולות כפול 1000 פעמים, לכן יש הרבה שליחות של 12345 (השרת) ל-44550 (הלקוח). השרת שולח את החבילה הראשונה, ולאחר מכן עוד מלא חבילות. הלקוח מאשר את קבלת החבילה הראשונה (1024 הבתים הראשונים) וכן את השנייה (אלו שבאים אחרי), מחזיר ack באופן מאוחד על 13000 הבתים שהגיעו, וסוגר את החיבור. אבל יש עוד חבילות בבאפר שלא נקראו ע"י האפליקציה כאשר היא נסגרת, לכן נשלחת הודעת rst לשרת שידע שהלקוח ניתק מבלי לקרוא עד הסוף.

גרסה v4:

```
server.py > ...
1 import socket,sys,time
2
3 TCP_IP = '0.0.0.0'
4 TCP_PORT = int(sys.argv[1])
5 BUFFER_SIZE = 1024
6
7 s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
8 s.bind((TCP_IP, TCP_PORT))
9 s.listen(1)
10
11 while True:
12     conn, addr = s.accept()
13     print('New connection from:', addr)
14     while True:
15         time.sleep(5)
16         data = conn.recv(BUFFER_SIZE)
17         if not data: break
18         print("received:", data)
19         conn.send(data.upper())
20     conn.close()
```

```
client.py > ...
1 import socket,sys
2
3 TCP_IP = sys.argv[1]
4 TCP_PORT = int(sys.argv[2])
5 BUFFER_SIZE = 1024
6 MESSAGE = b'Hello, World!'
7
8 s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
9 s.connect((TCP_IP, TCP_PORT))
10 s.send(MESSAGE*10)
11 s.send(MESSAGE*10)
12 s.send(MESSAGE*10)
13 s.send(MESSAGE*10)
14 data = s.recv(BUFFER_SIZE)
15 s.close()
16
17 print("received data:", data)
```

The image shows a Wireshark packet capture of a TCP connection. The packet list shows several segments, including a SYN exchange and data transmission. The packet details pane for a selected segment shows the following information:

- Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{ED60E847-D85F-48D0-8000-000000000000}
- Ethernet II, Src: VMware_6f:d1:51 (00:0c:29:6f:d1:51), Dst: VMware_c8:00:08 (00:50:56:c0:00:08)
- Internet Protocol Version 4, Src: 192.168.135.128, Dst: 192.168.135.1
- Transmission Control Protocol, Src Port: 38542, Dst Port: 12345, Seq: 0, Len: 0
- Source Port: 38542
- Destination Port: 12345
- [Stream index: 0]
- [Conversation completeness: Complete, WITH_DATA (31)]
- [TCP Segment Len: 0]
- Sequence Number: 0 (relative sequence number)
- Sequence Number (raw): 2833201009
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 0
- Acknowledgment number (raw): 0
- 1010 = Header Length: 40 bytes (10)
- Flags: 0x002 (SYN)
- Window: 64240
- [Calculated window size: 64240]
- Checksum: 0xa136 [unverified]
- [Checksum Status: Unverified]

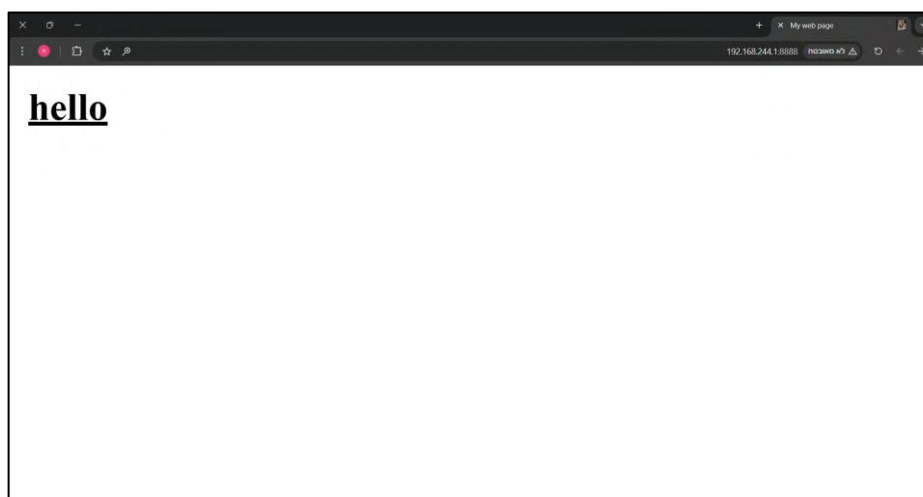
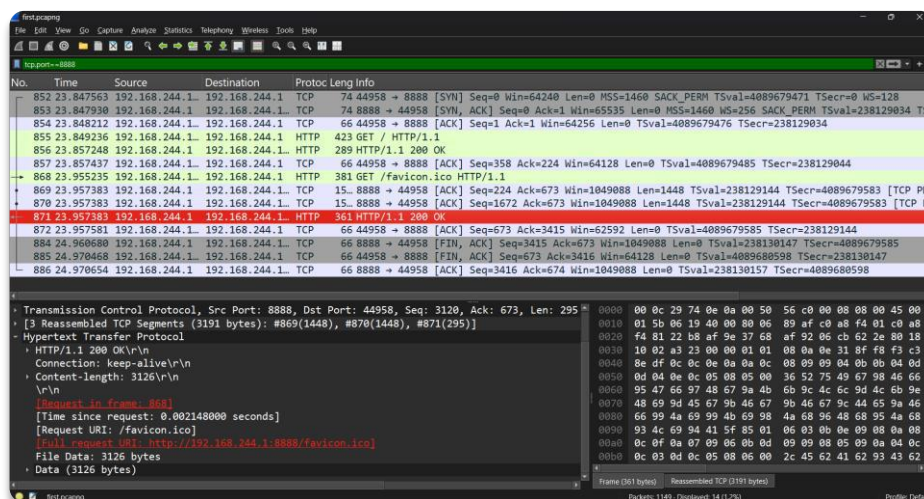
כרגיל הלקוח מקבל את ה-IP והפורט מהארגומנטים לתוכנית, לאחר מכן הוא מתחבר לשרת ושולח לו 4 הודעות שכל הודעה היא 10 פעמים "Hello, World", השוני הפעם מהתוכנית הקודמת, הוא שלאחר שקיבל את ההודעה חזרה מהשרת הוא מדפיס את ה-1024 בתים הראשונים. בצד שני, כרגיל השרת מאזין לכל החיבורים כיוון שהוא בחר בכתובת 0.0.0.0 ומקבל פורט כקלט. הוא פותח חיבור מחכה 5 שניות, מקבל את ה-1024 הבתים הראשונים ושולח אותם חזרה ללקוח באותיות גדולות. הוא חוזר על התהליך עד שהוא מפסיק לקבל מידע מהלקוח ולבסוף סוגר את החיבור.

בכריש אנו רואים תחילה את לחיצת הידיים בין הלקוח לשרת. אך בשונה מהתפיסה האחרונה, השרת מחכה 5 שניות ולכן התגובה שלו מתעכבת. ניתן לראות כי השליחה (של הלקוח) והתגובה (של השרת) קורית פה 2 פעמים (כנראה 3 השליחות האחרונות אוחדו בעת שליחתן). בכל פעם השרת (שנמצא ב-timeout באפליקציה ולכן לא קורא מהבאפר), מחזיר ack שהוא קיבל את ההודעה. השרת שולח את כל ה-520 בתים בחזרה בפעם אחת (מאוחדת) באותיות גדולות, ומקבל ack עליו מהשרת. מכאן והילך טקס הפרידה הסטנדרטי של fin-ack-ack הייתה בעיה של rst בשל העובדה שכל המידע נקרא מהבאפר בטרם האפליקציה סיימה את הריצה.

חלק ב' -

נסיים חלק זה של התרגיל בהצגת הכריש בזמן ריצת קוד השרת שלנו, כאשר האחרון מקבל בקשות מהדפדפן (אשר רץ בVM).

<http://192.168.244.1:8888/>



הכתובת פונה ומבקשת מהשרת את דף הבית, והוא מחזיר בתמורה את index.html. ניתן לראות בתמונה שהדפדפן עושה מס' פניות מאותו פורט (44958), כאשר תחילה הוא שולח את הבקשה של הקובץ, ומקבל אליו חזרה את ה אס 200, מיד לאחר שהם מחליפים ack ביניהם אודות מעבר הקובץ באופן תקין, הדפדפן שולח בקשת get נוספת עבור הקובץ favicon.ico הלוא הוא האייקון של "האתר" שלנו שאנו רואים בקצה הכרטיסייה בדפדפן, גם על בקשה זו מתקבלת הודעת אס 200 (בתמונה רואים את הקובץ עליו הוחזר אס למטה בbody), והתקשורת נסגרת באופן הדדי בחינים משני הצדדים. ניתן לראות שנשלח המון מידע עם הודעת get מדפדפן, כמו סוג הדפדפן, הגרסה שלו, סטטוס connection, עדיפות ועוד. מעבר לget, ההחזרה של המידע מהשרת – אס 200, ואז הבקשה לאייקון אין משהו מיוחד, ואין בקשה נוספת מאותו פורט.

<http://192.168.244.129:8888/c/Footube.html>

Time	Source	Destination	Proto	Length	Info
0.0003...	192.168.24...	192.168.24...	TCP	66	54010 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
0.0005...	192.168.24...	192.168.24...	TCP	66	8888 → 54010 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
0.0006...	192.168.24...	192.168.24...	TCP	54	54010 → 8888 [ACK] Seq=1 Ack=1 Win=131328 Len=0
0.0007...	192.168.24...	192.168.24...	HTTP	524	GET /c/Footube.html HTTP/1.1
0.0008...	192.168.24...	192.168.24...	TCP	60	8888 → 54010 [ACK] Seq=1 Ack=471 Win=64128 Len=0
0.0010...	192.168.24...	192.168.24...	TCP	15	8888 → 54010 [ACK] Seq=1 Ack=471 Win=64128 Len=1460 [TCP PDU reassembled in 14]
0.0010...	192.168.24...	192.168.24...	TCP	15	8888 → 54010 [ACK] Seq=1461 Ack=471 Win=64128 Len=1460 [TCP PDU reassembled in 14]
0.0010...	192.168.24...	192.168.24...	TCP	15	8888 → 54010 [ACK] Seq=2921 Ack=471 Win=64128 Len=1460 [TCP PDU reassembled in 14]
0.0010...	192.168.24...	192.168.24...	TCP	15	8888 → 54010 [ACK] Seq=4381 Ack=471 Win=64128 Len=1460 [TCP PDU reassembled in 14]
0.0010...	192.168.24...	192.168.24...	HTTP	360	HTTP/1.1 200 OK
0.0011...	192.168.24...	192.168.24...	TCP	54	54010 → 8888 [ACK] Seq=471 Ack=6147 Win=131328 Len=0
0.0047...	192.168.24...	192.168.24...	TCP	66	54011 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
0.0053...	192.168.24...	192.168.24...	TCP	66	8888 → 54011 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
0.0054...	192.168.24...	192.168.24...	TCP	54	54011 → 8888 [ACK] Seq=1 Ack=1 Win=131328 Len=0
0.0223...	192.168.24...	192.168.24...	TCP	66	54012 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
0.0226...	192.168.24...	192.168.24...	TCP	66	8888 → 54012 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
0.0229...	192.168.24...	192.168.24...	TCP	54	54012 → 8888 [ACK] Seq=1 Ack=1 Win=131328 Len=0
0.0230...	192.168.24...	192.168.24...	TCP	66	54013 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
0.0231...	192.168.24...	192.168.24...	TCP	66	8888 → 54013 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
0.0235...	192.168.24...	192.168.24...	TCP	54	54013 → 8888 [ACK] Seq=1 Ack=1 Win=131328 Len=0
0.0239...	192.168.24...	192.168.24...	TCP	66	54014 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
0.0240...	192.168.24...	192.168.24...	TCP	66	8888 → 54014 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
0.0242...	192.168.24...	192.168.24...	TCP	54	54014 → 8888 [ACK] Seq=1 Ack=1 Win=131328 Len=0
0.0242...	192.168.24...	192.168.24...	HTTP	429	GET /c/footube.css HTTP/1.1
0.0242...	192.168.24...	192.168.24...	HTTP	473	GET /c/img/1.jpg HTTP/1.1

Transmission Control Protocol, Src Port: 54010, Dst Port: 8888, Seq: 1, Ack: 1, Len: 470

Hypertext Transfer Protocol

GET /c/Footube.html HTTP/1.1\r\n\r\nHost: 192.168.244.129:8888\r\n\r\nConnection: keep-alive\r\n\r\nUpgrade-Insecure-Requests: 1\r\n\r\n

0039 02 01 ec 17 00 00 47 45 54 20 2f 63 2f 0040 74 75 02 65 2e 68 74 6d 6c 20 48 54 540050 2e 31 0d 0a 48 6f 73 74 3a 20 31 39 320060 38 2e 32 34 34 2e 31 32 39 3a 38 38 380070 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b0080 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61

Time	Source	Destination	Proto	Length	Info
5.0647...	192.168.24...	192.168.24...	TCP	15	8888 → 54015 [ACK] Seq=511001 Ack=420 Win=64128 Len=1460 [TCP PDU reassembled in 2491]
5.0647...	192.168.24...	192.168.24...	TCP	15	8888 → 54015 [ACK] Seq=512461 Ack=420 Win=64128 Len=1460 [TCP PDU reassembled in 2491]
5.0647...	192.168.24...	192.168.24...	TCP	15	8888 → 54015 [ACK] Seq=513921 Ack=420 Win=64128 Len=1460 [TCP PDU reassembled in 2491]
5.0647...	192.168.24...	192.168.24...	TCP	15	8888 → 54015 [ACK] Seq=515381 Ack=420 Win=64128 Len=1460 [TCP PDU reassembled in 2491]
5.0647...	192.168.24...	192.168.24...	TCP	15	8888 → 54015 [ACK] Seq=516841 Ack=420 Win=64128 Len=1460 [TCP PDU reassembled in 2491]
5.0647...	192.168.24...	192.168.24...	TCP	15	8888 → 54015 [ACK] Seq=518301 Ack=420 Win=64128 Len=1460 [TCP PDU reassembled in 2491]
5.0647...	192.168.24...	192.168.24...	TCP	15	8888 → 54015 [ACK] Seq=519761 Ack=420 Win=64128 Len=1460 [TCP PDU reassembled in 2491]
5.0647...	192.168.24...	192.168.24...	TCP	15	8888 → 54015 [ACK] Seq=521221 Ack=420 Win=64128 Len=1460 [TCP PDU reassembled in 2491]
5.0647...	192.168.24...	192.168.24...	TCP	15	8888 → 54015 [ACK] Seq=522681 Ack=420 Win=64128 Len=1460 [TCP PDU reassembled in 2491]
5.0648...	192.168.24...	192.168.24...	TCP	15	8888 → 54015 [ACK] Seq=524141 Ack=420 Win=64128 Len=1460 [TCP PDU reassembled in 2491]
5.0648...	192.168.24...	192.168.24...	TCP	15	8888 → 54015 [ACK] Seq=525601 Ack=420 Win=64128 Len=1460 [TCP PDU reassembled in 2491]
5.0648...	192.168.24...	192.168.24...	TCP	15	8888 → 54015 [ACK] Seq=527061 Ack=420 Win=64128 Len=1460 [TCP PDU reassembled in 2491]
5.0648...	192.168.24...	192.168.24...	TCP	15	8888 → 54015 [ACK] Seq=528521 Ack=420 Win=64128 Len=1460 [TCP PDU reassembled in 2491]
5.0648...	192.168.24...	192.168.24...	TCP	15	8888 → 54015 [ACK] Seq=529981 Ack=420 Win=64128 Len=1460 [TCP PDU reassembled in 2491]
5.0648...	192.168.24...	192.168.24...	HTTP	604	HTTP/1.1 200 OK (image/png)
5.0648...	192.168.24...	192.168.24...	TCP	54	54015 → 8888 [ACK] Seq=420 Ack=432161 Win=131328 Len=0
5.0648...	192.168.24...	192.168.24...	TCP	54	54015 → 8888 [ACK] Seq=420 Ack=446761 Win=131328 Len=0
5.0649...	192.168.24...	192.168.24...	TCP	54	54015 → 8888 [ACK] Seq=420 Ack=461361 Win=131328 Len=0
5.0650...	192.168.24...	192.168.24...	TCP	54	54015 → 8888 [ACK] Seq=420 Ack=475961 Win=131328 Len=0
5.0651...	192.168.24...	192.168.24...	TCP	54	54015 → 8888 [ACK] Seq=420 Ack=490561 Win=131328 Len=0
5.0652...	192.168.24...	192.168.24...	TCP	54	54015 → 8888 [ACK] Seq=420 Ack=505161 Win=131328 Len=0
5.0653...	192.168.24...	192.168.24...	TCP	54	54015 → 8888 [ACK] Seq=420 Ack=519761 Win=131328 Len=0
5.0655...	192.168.24...	192.168.24...	TCP	54	54015 → 8888 [ACK] Seq=420 Ack=531991 Win=131328 Len=0
6.0635...	192.168.24...	192.168.24...	TCP	60	8888 → 54015 [FIN, ACK] Seq=531991 Ack=420 Win=64128 Len=0
6.0637...	192.168.24...	192.168.24...	TCP	54	54015 → 8888 [ACK] Seq=420 Ack=531992 Win=131328 Len=0

Frame 2491: 604 bytes on wire (4832 bits), 604 bytes captured (4832 bits) on interface \Device\NPF_{c...} Ethernet II, Src: VMware 74:0e:0a (00:0c:29:74:0e:0a), Dst: VMware 00:00:00 (00:50:56:c0:00:00)

Internet Protocol Version 4, Src: 192.168.244.129, Dst: 192.168.244.1

Transmission Control Protocol, Src Port: 8888, Dst Port: 54015, Seq: 531441, Ack: 420, Len: 550

[365 Reassembled TCP Segments (531990 bytes): #2095(1460), #2096(1460), #2097(1460), #2098(1460), #2099(1460), #2100(1460), #2101(1460), #2102(1460), #2103(1460), #2104(1460), #2105(1460), #2106(1460), #2107(1460), #2108(1460), #2109(1460), #2110(1460), #2111(1460), #2112(1460), #2113(1460), #2114(1460), #2115(1460), #2116(1460), #2117(1460), #2118(1460), #2119(1460), #2120(1460), #2121(1460), #2122(1460), #2123(1460), #2124(1460), #2125(1460), #2126(1460), #2127(1460), #2128(1460), #2129(1460), #2130(1460), #2131(1460), #2132(1460), #2133(1460), #2134(1460), #2135(1460), #2136(1460), #2137(1460), #2138(1460), #2139(1460), #2140(1460), #2141(1460), #2142(1460), #2143(1460), #2144(1460), #2145(1460), #2146(1460), #2147(1460), #2148(1460), #2149(1460), #2150(1460), #2151(1460), #2152(1460), #2153(1460), #2154(1460), #2155(1460), #2156(1460), #2157(1460), #2158(1460), #2159(1460), #2160(1460), #2161(1460), #2162(1460), #2163(1460), #2164(1460), #2165(1460), #2166(1460), #2167(1460), #2168(1460), #2169(1460), #2170(1460), #2171(1460), #2172(1460), #2173(1460), #2174(1460), #2175(1460), #2176(1460), #2177(1460), #2178(1460), #2179(1460), #2180(1460), #2181(1460), #2182(1460), #2183(1460), #2184(1460), #2185(1460), #2186(1460), #2187(1460), #2188(1460), #2189(1460), #2190(1460), #2191(1460), #2192(1460), #2193(1460), #2194(1460), #2195(1460), #2196(1460), #2197(1460), #2198(1460), #2199(1460), #2200(1460), #2201(1460), #2202(1460), #2203(1460), #2204(1460), #2205(1460), #2206(1460), #2207(1460), #2208(1460), #2209(1460), #2210(1460), #2211(1460), #2212(1460), #2213(1460), #2214(1460), #2215(1460), #2216(1460), #2217(1460), #2218(1460), #2219(1460), #2220(1460), #2221(1460), #2222(1460), #2223(1460), #2224(1460), #2225(1460), #2226(1460), #2227(1460), #2228(1460), #2229(1460), #2230(1460), #2231(1460), #2232(1460), #2233(1460), #2234(1460), #2235(1460), #2236(1460), #2237(1460), #2238(1460), #2239(1460), #2240(1460), #2241(1460), #2242(1460), #2243(1460), #2244(1460), #2245(1460), #2246(1460), #2247(1460), #2248(1460), #2249(1460), #2250(1460), #2251(1460), #2252(1460), #2253(1460), #2254(1460), #2255(1460), #2256(1460), #2257(1460), #2258(1460), #2259(1460), #2260(1460), #2261(1460), #2262(1460), #2263(1460), #2264(1460), #2265(1460), #2266(1460), #2267(1460), #2268(1460), #2269(1460), #2270(1460), #2271(1460), #2272(1460), #2273(1460), #2274(1460), #2275(1460), #2276(1460), #2277(1460), #2278(1460), #2279(1460), #2280(1460), #2281(1460), #2282(1460), #2283(1460), #2284(1460), #2285(1460), #2286(1460), #2287(1460), #2288(1460), #2289(1460), #2290(1460), #2291(1460), #2292(1460), #2293(1460), #2294(1460), #2295(1460), #2296(1460), #2297(1460), #2298(1460), #2299(1460), #2300(1460), #2301(1460), #2302(1460), #2303(1460), #2304(1460), #2305(1460), #2306(1460), #2307(1460), #2308(1460), #2309(1460), #2310(1460), #2311(1460), #2312(1460), #2313(1460), #2314(1460), #2315(1460), #2316(1460), #2317(1460), #2318(1460), #2319(1460), #2320(1460), #2321(1460), #2322(1460), #2323(1460), #2324(1460), #2325(1460), #2326(1460), #2327(1460), #2328(1460), #2329(1460), #2330(1460), #2331(1460), #2332(1460), #2333(1460), #2334(1460), #2335(1460), #2336(1460), #2337(1460), #2338(1460), #2339(1460), #2340(1460), #2341(1460), #2342(1460), #2343(1460), #2344(1460), #2345(1460), #2346(1460), #2347(1460), #2348(1460), #2349(1460), #2350(1460), #2351(1460), #2352(1460), #2353(1460), #2354(1460), #2355(1460), #2356(1460), #2357(1460), #2358(1460), #2359(1460), #2360(1460), #2361(1460), #2362(1460), #2363(1460), #2364(1460), #2365(1460), #2366(1460), #2367(1460), #2368(1460), #2369(1460), #2370(1460), #2371(1460), #2372(1460), #2373(1460), #2374(1460), #2375(1460), #2376(1460), #2377(1460), #2378(1460), #2379(1460), #2380(1460), #2381(1460), #2382(1460), #2383(1460), #2384(1460), #2385(1460), #2386(1460), #2387(1460), #2388(1460), #2389(1460), #2390(1460), #2391(1460), #2392(1460), #2393(1460), #2394(1460), #2395(1460), #2396(1460), #2397(1460), #2398(1460), #2399(1460), #2400(1460), #2401(1460), #2402(1460), #2403(1460), #2404(1460), #2405(1460), #2406(1460), #2407(1460), #2408(1460), #2409(1460), #2410(1460), #2411(1460), #2412(1460), #2413(1460), #2414(1460), #2415(1460), #2416(1460), #2417(1460), #2418(1460), #2419(1460), #2420(1460), #2421(1460), #2422(1460), #2423(1460), #2424(1460), #2425(1460), #2426(1460), #2427(1460), #2428(1460), #2429(1460), #2430(1460), #2431(1460), #2432(1460), #2433(1460), #2434(1460), #2435(1460), #2436(1460), #2437(1460), #2438(1460), #2439(1460), #2440(1460), #2441(1460), #2442(1460), #2443(1460), #2444(1460), #2445(1460), #2446(1460), #2447(1460), #2448(1460), #2449(1460), #2450(1460), #2451(1460), #2452(1460), #2453(1460), #2454(1460), #2455(1460), #2456(1460), #2457(1460), #2458(1460), #2459(1460), #2460(1460), #2461(1460), #2462(1460), #2463(1460), #2464(1460), #2465(1460), #2466(1460), #2467(1460), #2468(1460), #2469(1460), #2470(1460), #2471(1460), #2472(1460), #2473(1460), #2474(1460), #2475(1460), #2476(1460), #2477(1460), #2478(1460), #2479(1460), #2480(1460), #2481(1460), #2482(1460), #2483(1460), #2484(1460), #2485(1460), #2486(1460), #2487(1460), #2488(1460), #2489(1460), #2490(1460), #2491(1460), #2492(1460), #2493(1460), #2494(1460), #2495(1460), #2496(1460), #2497(1460), #2498(1460), #2499(1460), #2500(1460), #2501(1460), #2502(1460), #2503(1460), #2504(1460), #2505(1460), #2506(1460), #2507(1460), #2508(1460), #2509(1460), #2510(1460), #2511(1460), #2512(1460), #2513(1460), #2514(1460), #2515(1460), #2516(1460), #2517(1460), #2518(1460), #2519(1460), #2520(1460), #2521(1460), #2522(1460), #2523(1460), #2524(1460), #2525(1460), #2526(1460), #2527(1460), #2528(1460), #2529(1460), #2530(1460), #2531(1460), #2532(1460), #2533(1460), #2534(1460), #2535(1460), #2536(1460), #2537(1460), #2538(1460), #2539(1460), #2540(1460), #2541(1460), #2542(1460), #2543(1460), #2544(1460), #2545(1460), #2546(1460), #2547(1460), #2548(1460), #2549(1460), #2550(1460), #2551(1460), #2552(1460), #2553(1460), #2554(1460), #2555(1460), #2556(1460), #2557(1460), #2558(1460), #2559(1460), #2560(1460), #2561(1460), #2562(1460), #2563(1460), #2564(1460), #2565(1460), #2566(1460), #2567(1460), #2568(1460), #2569(1460), #2570(1460), #2571(1460), #2572(1460), #2573(1460), #2574(1460), #2575(1460), #2576(1460), #2577(1460), #2578(1460), #2579(1460), #2580(1460), #2581(1460), #2582(1460), #2583(1460), #2584(1460), #2585(1460), #2586(1460), #2587(1460), #2588(1460), #2589(1460), #2590(1460), #2591(1460), #2592(1460), #2593(1460), #2594(1460), #2595(1460), #2596(1460), #2597(1460), #2598(1460), #2599(1460), #2600(1460), #2601(1460), #2602(1460), #2603(1460), #2604(1460), #2605(1460), #2606(1460), #2607(1460), #2608(1460), #2609(1460), #2610(1460), #2611(1460), #2612(1460), #2613(1460), #2614(1460), #2615(1460), #2616(1460), #2617(1460), #2618(1460), #2619(1460), #2620(1460), #2621(1460), #2622(1460), #2623(1460), #2624(1460), #2625(1460), #2626(1460), #2627(1460), #2628(1460), #2629(1460), #2630(1460), #2631(1460), #2632(1460), #2633(1460), #2634(1460), #2635(1460), #2636(1460), #2637(1460), #2638(1460), #2639(1460), #2640(1460), #2641(1460), #2642(1460), #2643(1460), #2644(1460), #2645(1460), #2646(1460), #2647(1460), #2648(1460), #2649(1460), #2650(1460), #2651(1460), #2652(1460), #2653(1460), #2654(1460), #2655(1460), #2656(1460), #2657(1460), #2658(1460), #2659(1460), #2660(1460), #2661(1460), #2662(1460), #2663(1460), #2664(1460), #2665(1460), #2666(1460), #2667(1460), #2668(1460), #266

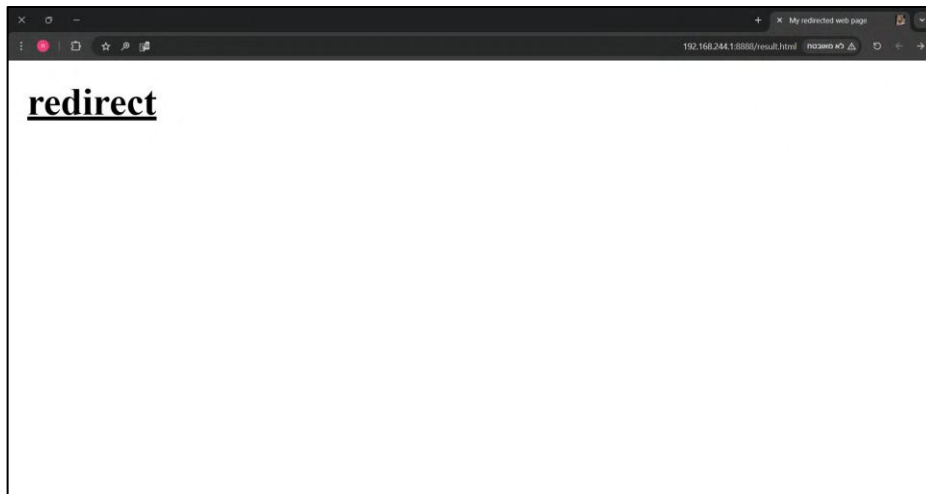
כעת מבקש הדפדפן את קובץ `/c/Footube.html` אשר מכיל בתוכו מס' קבצים (תמונות) נוספים. ניתן לראות שהפעם הוא פותח מס' חיבורים (כ-חמישה) דרך כמה פורטים (תמונה ראשונה), אבל בפועל בשלב הראשון רק דרך החיבור הראשון עוברת התקשורת של הבקשה מהשרת. לאחר שהוא מבקש את הדף הראשון (זה שביקשנו בכתובת), הוא מקבל אותו ומתחיל ברצף בקשות כבדות מאוד של התמונות המופיעות באותו קובץ. נשים לב שהתמונה מועברת בהמון צאנקים, אך לאחר כמה זמן הוא מנסה לבקש דרך אחד הפורטים האחרים שהוא פתח תמונה נוספת שונה מזו שביקש דרך הפורט הראשי, אך למרות זאת עדיין התקשורת ממשיכה להגיע דרכו. לאחר שמס' תמונות הגיעו מהפורט הראשי – הוא נסגר, ואז אנו רואים כיצד התמונה שנתבקשה בפורט השונה (54636) מתחילה להגיע גם היא. אותו דפוס פעולה חוזר על עצמו, כאשר מס' תמונות מגיעות דרך כמה פורטים שונים, אך אין ערבוב והכל מתבצע בצאנקים, דהיינו רק לאחר שפורט קיבל את התמונות שלו ונסגר (בחפץ `fin` כמובן), אנחנו רואים שהתמונות שביקש פורט אחר מתחילות להגיע (זה וודאי נובע מהמחסור במקביליות באופן שבו בנינו את השרת, ובשל כך שאר הפורטים תקועים ב`listen` כאשר האחד מקבל שירותים מהשרת). התמונות שהן די גדולות מועברות בהמון צאנקים (כנראה בגלל שאנחנו עובדים מחשב-VM), ואחת לכמה זמן אנו רואים במהלך התקשורת `ack` שחוזר עליהן מהלקוח לשרת, כאשר בסיום העברה של כל קובץ תמונה נראה שמגיע `get` "מאסף". שוב בקשות `get` מכילות באותו מידע יבש על הדפדפן ושאר התשתיות. כך זה מתבצע באופן איטרטיבי עד שבסופו של דבר הפורט האחרון שביקש את התמונה האחרונה נסגר גם הוא, והדפדפן מציג את הדף בשלמותו (תמונה חמישית). ניתן לראות בקובץ `pcap` המלא את כלל ההסברים שכתבנו כאן באופן ממשי (אנחנו גבוליים עם גודל הזיפ לכן מצמצמים בתמונות מחילה). יש לציין שבתחתית כל חבילה המכילה קובץ `PNG` ישנם נתונים בהקשר הזה אשר אנו מניחים שעוזרים לפענח את התמונה (לפי הטייפ שלה, גודל וכדו').

<http://192.168.244.1:8888/redirect>

The image shows a Wireshark packet capture of an HTTP 301 redirect. The packet list on the left shows a GET request to /redirect on port 8888, followed by a 301 Moved Permanently response. The packet details pane on the right shows the response status and headers. The packet bytes pane on the right shows the raw data of the response.

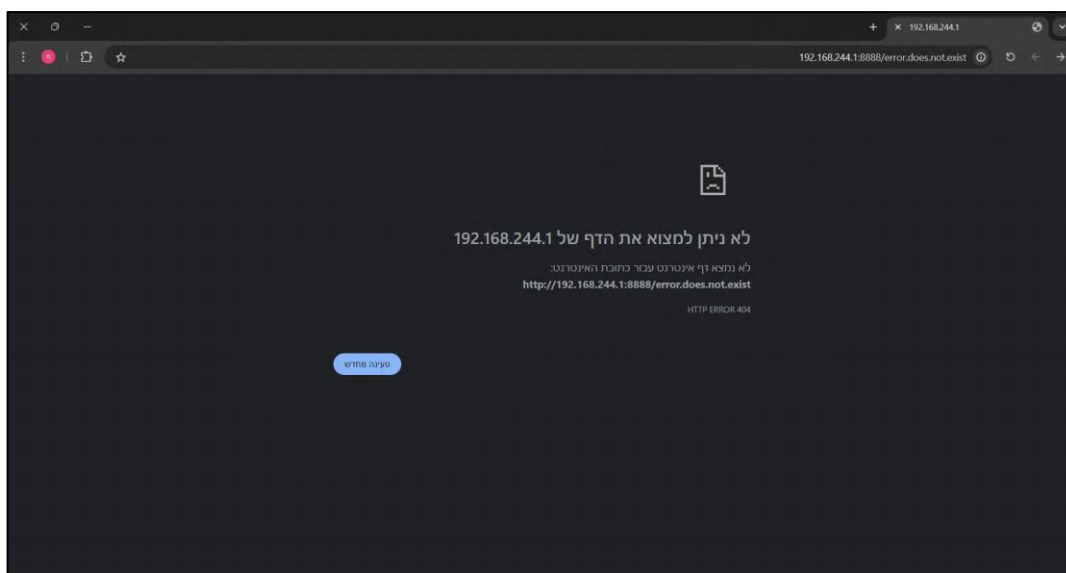
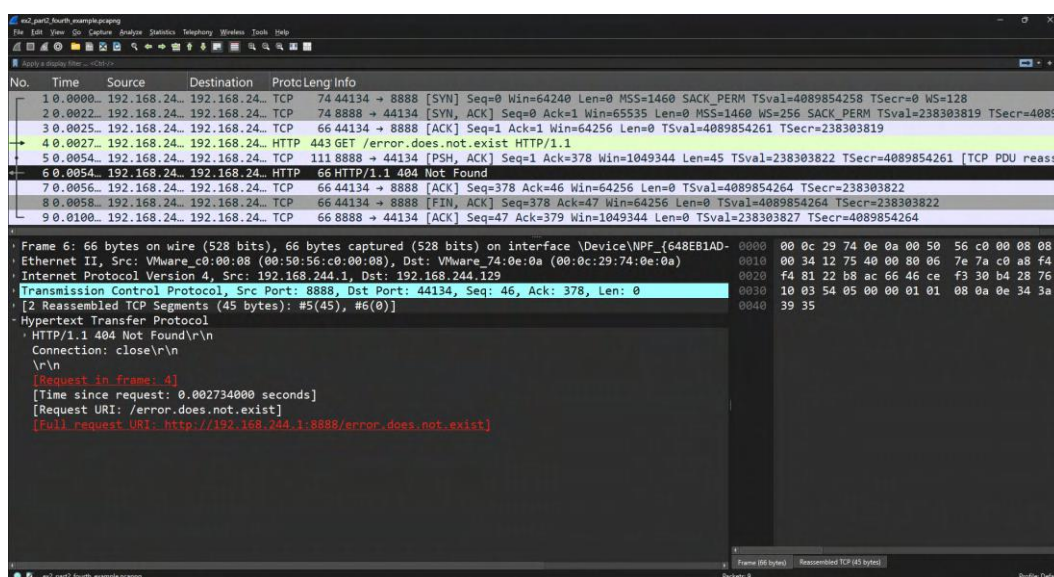
No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000	192.168.24.1	192.168.24.1	TCP	74	52298 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4089810494 TSecr=0 WS=128
2	0.0026	192.168.24.1	192.168.24.1	TCP	74	8888 → 52298 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM TSval=238260055 TSecr=4089810494
3	0.0029	192.168.24.1	192.168.24.1	TCP	66	52298 → 8888 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4089810497 TSecr=238260055
4	0.0030	192.168.24.1	192.168.24.1	HTTP	431	GET /redirect HTTP/1.1
5	0.0056	192.168.24.1	192.168.24.1	TCP	143	8888 → 52298 [PSH, ACK] Seq=1 Ack=366 Win=1049344 Len=77 TSval=238260058 TSecr=4089810497 [TCP PDU reassemble]
6	0.0056	192.168.24.1	192.168.24.1	HTTP	66	HTTP/1.1 301 Moved Permanently
7	0.0058	192.168.24.1	192.168.24.1	TCP	66	52298 → 8888 [ACK] Seq=366 Ack=78 Win=64256 Len=0 TSval=4089810500 TSecr=238260058
8	0.0059	192.168.24.1	192.168.24.1	TCP	66	52298 → 8888 [FIN, ACK] Seq=366 Ack=79 Win=64256 Len=0 TSval=4089810500 TSecr=238260058
9	0.0058	192.168.24.1	192.168.24.1	TCP	66	8888 → 52298 [ACK] Seq=79 Ack=367 Win=1049344 Len=0 TSval=238260062 TSecr=4089810500
10	0.0223	192.168.24.1	192.168.24.1	TCP	74	52306 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4089810517 TSecr=0 WS=128
11	0.0237	192.168.24.1	192.168.24.1	TCP	74	8888 → 52306 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM TSval=238260076 TSecr=4089810517
12	0.0241	192.168.24.1	192.168.24.1	TCP	66	52306 → 8888 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4089810519 TSecr=238260076
13	0.0266	192.168.24.1	192.168.24.1	HTTP	434	GET /result.html HTTP/1.1
14	0.0300	192.168.24.1	192.168.24.1	HTTP	244	HTTP/1.1 200 OK
15	0.0302	192.168.24.1	192.168.24.1	TCP	66	52306 → 8888 [ACK] Seq=369 Ack=179 Win=64128 Len=0 TSval=4089810525 TSecr=238260083
16	1.0444	192.168.24.1	192.168.24.1	TCP	66	8888 → 52306 [FIN, ACK] Seq=179 Ack=369 Win=1049344 Len=0 TSval=238261097 TSecr=4089810525
17	1.0450	192.168.24.1	192.168.24.1	TCP	66	52306 → 8888 [FIN, ACK] Seq=369 Ack=180 Win=64128 Len=0 TSval=4089811539 TSecr=238261097
18	1.0452	192.168.24.1	192.168.24.1	TCP	66	8888 → 52306 [ACK] Seq=180 Ack=370 Win=1049344 Len=0 TSval=238261098 TSecr=4089811539

Transmission Control Protocol, Src Port: 8888, Dst Port: 52298, Seq: 78, Ack: 366, Len: 0
Source Port: 8888
Destination Port: 52298
[Stream index: 0]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 78 (relative sequence number)
Sequence Number (raw): 2271379029
[Next Sequence Number: 79 (relative sequence number)]
[Next Sequence Number (raw): 2271379030]
Acknowledgment Number: 366 (relative ack number)
Acknowledgment Number (raw): 1137864124
1000 = Header Length: 32 bytes (8)
Flags: 0x01 (FIN, ACK)



הדפדפן פונה כעת אל הנתיב `/redirect` של השרת שלנו. ניתן לראות שהפעם הוא פותח תחילה חיבור יחיד של פורט אחד, אשר דרכו הוא שולח את הפניה (שורה צהובה עליונה). השרת שולח לו תשובה חזרה של 'moved permanently', מצרף לתשובה שלו את ההפניה/הכתובת של מקום החדש, והחיבור נסגר (תמונה ראשונה). מיד לאחר מכן מוקם חיבור חדש מצד הדפדפן, אשר דרכו מתבצעת הבקשה לאותו location-מיקום חדש שהחזיר השרת לדפדפן בבקשה הקודמת (שורה צהובה שלישית). השרת מקבל את הבקשה השנייה, מחזיר את הקובץ שביקש בדפדפן – `result.html`, ואחר כך שוב פעם אנו רואים את הסגירה של התקשורת בfin שמגיע משני הכיוונים. ברמת המטא-דאטא אין שוני יוצא דופן משראינו כבר.

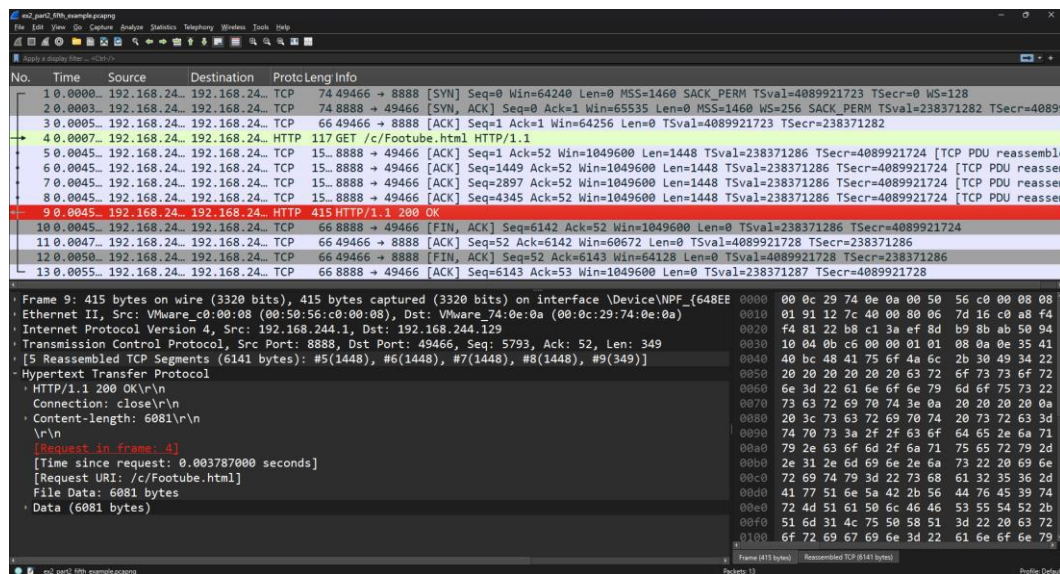
<http://192.168.244.1:8888/error.does.not.exist>



אנו רואים כעת ניסיון של הדפדפן לפנות לכתובת אשר לא קיימת מבחינת השרת שלנו. אנו רואים שנפתח שוב חיבור יחיד של פורט אחד, אשר דרכו נשלחת הבקשה (השורה בצהוב). השרת אשר שולח ack על כך שקיבל את הבקשה, ומיד מחזיר לדפדפן תשובה חזרה של שנותנת אינדיקציה לדפדפן שהדף לא נמצא – '404 not found' (תמונה שנייה). לאחר שהתשובה מוחזרת, התקשורת נסגרת ב-finish. ברמת המטא-דאטא שוב אין שוני 'יוצא דופן' משראינו כבר.

נסיים בכך שנראה מס' בקשות בכריש אשר התבצעו אל השרת אך הפעם לא מהדפדפן אלא מקוד הקליינט שאנחנו כתבנו –

[/c/Footube.html](http://c/Footube.html)



הלקוח מבקש את הקובץ /c/Footube.html אשר מכיל "עמוד אינטרנטי עם של תמונות וקבצים המוכלים בו, אולם כאן אנו רואים פורט יחיד אשר נפתח ע"י הלקוח ופונה לשרת, ויתרה מזאת לאחר שמתקבל הקובץ אנו לא רואים שרשרת של בקשות בדומה למה שראינו כאשר הפניה הגיעה מהדפדפן, כיוון שפה הלקוח רק מבקש את הקובץ ולא מנסה להציגו, אולם לו היה מנסה היה נתקל בכל מיני קבצים ומשאבים אשר אין, ובאמת היינו רואים שרשרת בקשות המנסה לייבא את כל המשאבים המוחזקים באופן כזה או אחר אצל השרת, אשר אלו דרושים באופן חיוני על מנת להציג את הקובץ במלואו. לאחר שהקובץ מגיע התקשורת נסגרת בfin הדדי. יש לציין שניתן לראות שהheader הרבה יותר דליל מזה שראינו בבקשות שהגיעו מהדפדפן, שכן שאנחנו בקוד הקליינט כתבנו בפניה רק את – סוג הפניה, שוב הקובץ המבוקש, הפרוטוקול בו אנו משתמשים, וכן סטטוס הconnection.

/favicon.ico

The image shows a Wireshark packet capture of an HTTP transaction. The packet list on the left shows a GET request for /favicon.ico (No. 4) and a 200 OK response (No. 7). The packet details pane for packet 7 shows the following information:

- Frame 7: 356 bytes on wire (2848 bits), 356 bytes captured (2848 bits) on interface \Device\NPF_{648E...}
- Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: VMware_74:0e:0a (00:0c:29:74:0e:0a)
- Internet Protocol Version 4, Src: 192.168.244.1, Dst: 192.168.244.129
- Transmission Control Protocol, Src Port: 8888, Dst Port: 47648, Seq: 2897, Ack: 49, Len: 290
 - Source Port: 8888
 - Destination Port: 47648
 - [Stream index: 0]
 - [Conversation completeness: Complete, WITH_DATA (31)]
 - [TCP Segment Len: 290]
 - Sequence Number: 2897 (relative sequence number)
 - Sequence Number (raw): 1648570390
 - [Next Sequence Number: 3187 (relative sequence number)]
 - Acknowledgment Number: 49 (relative ack number)
 - Acknowledgment number (raw): 3350907590
 - 1000 = Header Length: 32 bytes (8)
 - Flags: 0x018 (PSH, ACK)
 - Window: 4100
 - [Calculated window size: 1049600]
 - [Window size scaling factor: 256]
 - Character set: ASCII (UTF-8)

The packet bytes pane on the right shows the raw data of the packet, including the TCP header and the body of the response.

דוג' פשוטה ואחרונה בה הלקוח מבקש את הקובץ של האייקון של השרת (התמונה הקטנה המופיעה בראש הכרטיסייה), אנו רואים שהשרת מחזיר את התוכן ב2 חבילות שונות (מפאת גודלו), ומאסף זאת בהודעת 200. לאחר שמעבר ההודעה נשלם, אנו רואים את הסגירה של התקשורת.