

רשתות תקשורת תרגיל 2 - חלק א'

ביצענו בקובץ client את השינויים הנדרשים (הוספנו עוד שורה לפני סגירת הסוקט, של שליחת מספרי תעודות הזהות שלנו: '206821258, 319024600' ועדכנו את ההודעה הראשונה שהלקוח שולח לשרת להיות השמות שלנו – 'IdanSimai, IdoAharon').

בנוסף, סגרנו את השרת לאחר קבלת הודעה שנייה מהלקוח ולא אחרי הודעה אחת).

הרצנו את הלקוח על מחשב אחד ואת השרת על מחשב אחר כך ששני המחשבים באותה הרשת(שניהם מכונות וירטואליות שונות עם כתובות IP שונות).

כתובת לקוח – 192.168.100.5, כתובת שרת - 192.168.100.4).

הסנפנו ב wireshark את התעבורה על ידי סינון לפי כתובות ה ip של הלקוח והשרת ולפי הפרוטוקול שבו השתמשנו שהוא TCP בצורה הבאה:

```
tcp && ((ip.src == 192.168.100.4 && ip.dst == 192.168.100.5) || (ip.src == 192.168.100.5 && ip.dst == 192.168.100.4))
```

השתמשנו בכרטיס רשת enp2s0 לצורך הסינון בwireshark. זהו כרטיס רשת המיועד לתקשורת בין מחשבים שונים.

ביצענו סינון לחבילות שנשלחו מהשרת ללקוח וגם להפך. סה"כ קיבלנו 12 חבילות.

No.	Time	Source	Destination	Protocol	Length	Info
50	48.789799251	192.168.100.5	192.168.100.4	TCP	74	60692 → 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2697910841 TSecr=0 WS=128
51	48.789837218	192.168.100.4	192.168.100.5	TCP	74	12345 → 60692 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=264552587 TSecr=2697910841 WS=128
52	48.790979355	192.168.100.5	192.168.100.4	TCP	66	60692 → 12345 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2697910844 TSecr=264552587
53	48.819572219	192.168.100.5	192.168.100.4	TCP	86	60692 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=20 TSval=2697910870 TSecr=264552587
54	48.819638208	192.168.100.4	192.168.100.5	TCP	66	12345 → 60692 [ACK] Seq=1 Ack=21 Win=65152 Len=0 TSval=264552616 TSecr=2697910870
55	48.822636831	192.168.100.4	192.168.100.5	TCP	86	12345 → 60692 [PSH, ACK] Seq=1 Ack=21 Win=65152 Len=20 TSval=264552619 TSecr=2697910870
56	48.825660500	192.168.100.5	192.168.100.4	TCP	66	60692 → 12345 [ACK] Seq=21 Ack=21 Win=64256 Len=0 TSval=2697910878 TSecr=264552619
57	48.828597287	192.168.100.5	192.168.100.4	TCP	86	60692 → 12345 [PSH, ACK] Seq=21 Ack=21 Win=64256 Len=20 TSval=2697910889 TSecr=264552619
58	48.830162180	192.168.100.4	192.168.100.5	TCP	66	12345 → 60692 [FIN, ACK] Seq=21 Ack=41 Win=65152 Len=0 TSval=264552627 TSecr=2697910888
59	48.830895734	192.168.100.5	192.168.100.4	TCP	66	60692 → 12345 [FIN, ACK] Seq=41 Ack=21 Win=64256 Len=0 TSval=2697910882 TSecr=264552619
60	48.830924780	192.168.100.4	192.168.100.5	TCP	66	12345 → 60692 [ACK] Seq=22 Ack=42 Win=65152 Len=0 TSval=264552628 TSecr=2697910882
61	48.833263683	192.168.100.5	192.168.100.4	TCP	66	60692 → 12345 [ACK] Seq=42 Ack=22 Win=64256 Len=0 TSval=2697910886 TSecr=264552627

בניגוד לפרוטוקול UDP אנו מבצעים תהליך לחיצת ידיים, הקמת חיבור. בשלב זה מתבצע סנכרון בין שני הצדדים - השרת והלקוח. שלוש החבילות הראשונות, אשר מוצגות בצילום המסך לעיל מייצגות תהליך זה.

שלוש החבילות הללו יהיו ללא שכבת אפליקציה, יכילו את ה-TCP header ומטה(ACK, SYN ACK, SYN).

החבילה הרביעית מייצגת את שליחת ההודעה הראשונה של הלקוח לשרת(PSH ACK).

אחריה נראה את חבילת ה ACK המגיעה מהשרת ללקוח כאישור.

כתשובה ללקוח, השרת שולח הודעה בחזרה (PSH ACK) שבמקרה שלנו זה השמות ב-UPPER CASE.

לאחר מכן, הלקוח מחזיר לו ACK כאישור, כחבילה ה-7.

לאחר מכן, הלקוח שולח הודעה נוספת לשרת (PSH ACK), במקרה שלנו עם תעודות הזהות.

החבילה הבאה היא חבלת ה-FIN ACK שהשרת שולח ללקוח, אשר מדברת על סיום התקשורת ביניהם.

לאחר מכן, גם הלקוח שולח חזרה FIN ACK.

השרת מחזיר לו ACK כאישור (אישור שכולל גם אישור על החבילה של העברת מספרי תעודת הזהות, שכן ACK = 42 מה שאומר שכל המידע התקבל).

והלקוח מחזיר חזרה ACK אישור.

כעת ננתח חבילה חבילה:

חבילה (50):1

```

Ethernet II, Src: PcsCompu_3a:39:47 (08:00:27:3a:39:47), Dst: PcsCompu_3a:39:47 (08:00:27:3a:39:47)
Internet Protocol Version 4, Src: 192.168.100.5, Dst: 192.168.100.4
Transmission Control Protocol, Src Port: 60692, Dst Port: 12345, Seq: 0, Len: 0
  Source Port: 60692
  Destination Port: 12345
  [Stream index: 2]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 984980523
  [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: 0x947d [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  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 2697910841, TSecr 0
    TCP Option - No-Operation (NOP)
    TCP Option - Window scale: 7 (multiply by 128)
  [Timestamps]

```

אנו יכולים לראות ב-wireshark שפורט המקור הוא 60692 ופורט היעד 12345.

חבילה זו נשלחה מהלקוח לשרת.

בנוסף לכך, ה Sequence number שמופיע בחבילה זו הוא 984980523.

מספר זה הוא המספר הסידורי שממנו הלקוח מתחיל.
 רואים גם את השדה של Acknowledgement number שערכו הוא אפס מכיוון
 שדגל ה ACK כבוי ואין עדיין משמעות לערך זה.
 לאחר מכן אנו רואים את השדה Header length שאורכו 40 בתים.
 הדגל SYN דולק, זה מתבטא בצילום המסך בכך שבלשונית flags בשורה של
 SYN הביט דלוק.
 SYN - מלשון המילה סינכרוניזציה.
 כאשר נשלחת חבילה עם ביט זה דולק, המשמעות היא - שהלקוח רוצה
 להסתנכרן מול השרת.
 לאחר הדגלים, מצוין לנו גודל החלון שהוא 64240, שזוהי כמות המידע
 שהלקוח יכול לקבל מהשרת בבת אחת מבלי צורך ב ACK.
 יש לנו את השדה Checksum, כשהחבילה מגיעה לשרת, שכבת התעבורה
 מבצעת בעצמה את חישוב ה Checksum על החבילה.
 אם ערך זה שונה מהערך שמוצג בשדה ה Checksum אנו יודעים שהחבילה לא
 תקינה, כלומר חלק מהביטים השתבשו בדרך.
 אם Checksum לא תקין - זורקים את החבילה, ובעתיד תשלח חבילה
 חדשה(מכיוון שזה TCP).
 יש לנו לשונית של Options ששם מופיע הMSS, כלומר גודל ה data בשכבת
 האפליקציה לא יכול לעבור ערך זה(לכל חבילה), שערכו הוא 1460 בתים.
 מעכשיו לא נפרט יותר על הפורטים ושאר המידע שלא רלוונטי.

חבילה (51):2

```

> Ethernet II, Src: PcsCompu_3a:39:47 (08:00:27:3a:39:47), Dst: PcsCompu_3a:39:47 (08:00:27:3a:39:47)
> Internet Protocol Version 4, Src: 192.168.100.4, Dst: 192.168.100.5
- Transmission Control Protocol, Src Port: 12345, Dst Port: 60692, Seq: 0, Ack: 1, Len: 0
  Source Port: 12345
  Destination Port: 60692
  [Stream index: 2]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 334909424
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 984980524
  1010 .... = Header Length: 40 bytes (10)
- Flags: 0x012 (SYN, ACK)
  Window: 65160
  [Calculated window size: 65160]
  Checksum: 0x4989 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
- 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 264552587, TSecr 2697910841
  > TCP Option - No-Operation (NOP)
  > TCP Option - Window scale: 7 (multiply by 128)
  > [Timestamps]

```

ה Sequence number שמופיע בחבילה זו הוא 334909424.
מספר זה הוא המספר הסידורי שממנו השרת מתחיל.
Acknowledgement number הוא 984980524 כך שניתן לראות
שהוא באמת ה number sequence של חבילה 1 בתוספת ביט אחד.
בכך הוא יודיע ללקוח שהוא קיבל ממנו את החבילה.
הפעם, שני הדגלים דולקים - ACK וגם דגל SYN.
הביט הדלוק של SYN מציין כי השרת רוצה להסתנכרן מול הלקוח הפעם(שכן
הוא השולח של ההודעה הזו) ואילו הביט הדלוק של ACK מציין שהערך שמופיע
בשדה Acknowledgment number הוא בעל משמעות(גדול מ0).
החל מחבילה זו בכל החבילות הביט של ACK דולק.

חבילה (52):3

```

> Ethernet II, Src: PcsCompu_3a:39:47 (08:00:27:3a:39:47), Dst: PcsCompu_3a:39:47 (08:00:27:3a:39:47)
> Internet Protocol Version 4, Src: 192.168.100.5, Dst: 192.168.100.4
- Transmission Control Protocol, Src Port: 60692, Dst Port: 12345, Seq: 1, Ack: 1, Len: 0
  Source Port: 60692
  Destination Port: 12345
  [Stream index: 2]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 984980524
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 334909425
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x010 (ACK)
  Window: 502
  [Calculated window size: 64256]
  [Window size scaling factor: 128]
  Checksum: 0x87fa [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
- Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > TCP Option - No-Operation (NOP)
  > TCP Option - No-Operation (NOP)
  > TCP Option - Timestamps: TSval 2697910844, TSecr 264552587
  > [Timestamps]
  > [SEQ/ACK analysis]

```

חבילה זו היא החבילה האחרונה בתהליך הקמת החיבור, חבילה זו נשלחת
מהלקוח לשרת, כדי לאשר שחבילת השרת התקבלה אצל הלקוח.
ה Sequence number בחבילה זו הוא 984980524, כך שהוא גדל ב1 ביחס
לחבילה הקודמת שנשלחה מהלקוח לשרת.
מספר זה הוא המספר הסידורי שהשרת מצפה לו כפי שראינו בחבילה הקודמת
דרך ה Acknowledgment number.
רואים גם את השדה של Acknowledgment number שערכו הוא
334909425, זה המספר הסידורי שהלקוח אומר בעזרתו שאם השרת ישלח
חבילה, הוא מצפה שהיא תהיה עם מספר סידורי זה.

חבילה (53) 4:

```
▶ Ethernet II, Src: PcsCompu_3a:39:47 (08:00:27:3a:39:47), Dst: PcsCompu_3a:39:47 (08:00:27:3a:39:47)
▶ Internet Protocol Version 4, Src: 192.168.100.5, Dst: 192.168.100.4
▼ Transmission Control Protocol, Src Port: 60692, Dst Port: 12345, Seq: 1, Ack: 1, Len: 20
  Source Port: 60692
  Destination Port: 12345
  [Stream index: 2]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 20]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 984980524
  [Next Sequence Number: 21 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 334909425
  1000 .... = Header Length: 32 bytes (8)
▶ Flags: 0x018 (PSH, ACK)
  Window: 502
  [Calculated window size: 64256]
  [Window size scaling factor: 128]
  Checksum: 0x1bf9 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
▼ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▶ TCP Option - No-Operation (NOP)
  ▶ TCP Option - No-Operation (NOP)
  ▶ TCP Option - Timestamps: TSval 2697910870, TSecr 264552587
▶ [Timestamps]
▶ [SEQ/ACK analysis]
```

הלקוח שולח את ההודעה הראשונה לשרת, ההודעה מכילה את הטקסט הבא:
"IdanSimai, IdoAharon".

חבילה זו מייצגת את ההודעה הנ"ל כאשר הפעם כוללת בתוכה שכבת אפליקציה המכילה את תוכן ההודעה.

מספר הבתים בשכבת האפליקציה הוא כגודל הטקסט - 20 בתים.

ה Sequence number בחבילה זו הוא 984980524.

המספר לא השתנה מהחבילה הקודמת, כיוון שהלקוח לא שלח מידע בשכבת האפליקציה והשרת לא שלח ACK שמצפה לקבל מידע מהלקוח עבור Sequence number גבוה יותר.

רואים גם את השדה של Acknowledgement number שערכו הוא 334909425, זהה להודעה הקודמת.

חבילה (54) 5:

```
▶ Ethernet II, Src: PcsCompu_3a:39:47 (08:00:27:3a:39:47), Dst: PcsCompu_3a:39:47 (08:00:27:3a:39:47)
▶ Internet Protocol Version 4, Src: 192.168.100.4, Dst: 192.168.100.5
▼ Transmission Control Protocol, Src Port: 12345, Dst Port: 60692, Seq: 1, Ack: 21, Len: 0
  Source Port: 12345
  Destination Port: 60692
  [Stream index: 2]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 334909425
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 21 (relative ack number)
  Acknowledgment number (raw): 984980544
  1000 .... = Header Length: 32 bytes (8)
▶ Flags: 0x010 (ACK)
  Window: 509
  [Calculated window size: 65152]
  [Window size scaling factor: 128]
  Checksum: 0x4981 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
▼ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▶ TCP Option - No-Operation (NOP)
  ▶ TCP Option - No-Operation (NOP)
  ▶ TCP Option - Timestamps: TSval 264552616, TSecr 2697910870
▶ [Timestamps]
▶ [SEQ/ACK analysis]
```

השרת שולח חבילת ACK ללקוח, ע"מ לאשר שקיבל את החבילה שהלקוח שלח לו.

עבור חבילה זו אין שכבת אפליקציה, (אין הודעה בפועל אלא רק ACK).
ה Sequence number בחבילה זו הוא 334909425, זה המספר הסיידורי שהלקוח מצפה לקבל, כמו שראינו ב Acknowledgement number של החבילה הקודמת.

רואים גם את השדה של Acknowledgement number שערכו הוא 984980544.

בעזרת ערך זה, אנו רואים שהשרת באמת קיבל את המידע שהלקוח שלח לו, שהרי הערך גדל ב20 בתים, שזה בעצם גודל המידע שנשלח.

חבילה (55) 6:

```

Ethernet II, Src: PcsCompu_3a:39:47 (08:00:27:3a:39:47), Dst: PcsCompu_3a:39:47 (08:00:27:3a:39:47)
Internet Protocol Version 4, Src: 192.168.100.4, Dst: 192.168.100.5
Transmission Control Protocol, Src Port: 12345, Dst Port: 60692, Seq: 1, Ack: 21, Len: 20
  Source Port: 12345
  Destination Port: 60692
  [Stream index: 2]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 20]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 334909425
  [Next Sequence Number: 21 (relative sequence number)]
  Acknowledgment Number: 21 (relative ack number)
  Acknowledgment number (raw): 984980544
  1000 ... = Header Length: 32 bytes (8)
  Flags: 0x018 (PSH, ACK)
  Window: 509
  [Calculated window size: 65152]
  [Window size scaling factor: 128]
  Checksum: 0x4995 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    TCP Option - No-Operation (NOP)
    TCP Option - No-Operation (NOP)
    TCP Option - Timestamps: TSval 264552619, TSecr 2697910870
  [Timestamps]
  [SEQ/ACK analysis]
```

בנוסף לחבילת ה ACK שהשרת שולח הוא שולח ללקוח חבילה עם מידע כפי שהוגדר לו לעשות בקוד (להחזיר את השמות ב UPPERCASE).

ההודעה שהשרת שולח מכילה את הטקסט הבא: "IDANSIMAI, IDOAHARON"

גם במקרה זה, גודל שכבת האפליקציה (ההודעה שנשלחה) הוא 20 בתים. ה Sequence number בחבילה זו הוא 334909425.

רואים גם את השדה של Acknowledgement number שערכו הוא 984980544.

שני הערכים לא השתנו מאז החבילה הקודמת, מכיוון שבחבילה הקודמת הלקוח לא שלח חבילה עם Acknowledgement number שונה.

חבילה (56) :7

```

> Ethernet II, Src: PcsCompu_3a:39:47 (08:00:27:3a:39:47), Dst: PcsCompu_3a:39:47 (08:00:27:3a:39:47)
> Internet Protocol Version 4, Src: 192.168.100.5, Dst: 192.168.100.4
> Transmission Control Protocol, Src Port: 60692, Dst Port: 12345, Seq: 21, Ack: 21, Len: 0
  Source Port: 60692
  Destination Port: 12345
  [Stream index: 2]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 21 (relative sequence number)
  Sequence Number (raw): 984980544
  [Next Sequence Number: 21 (relative sequence number)]
  Acknowledgment Number: 21 (relative ack number)
  Acknowledgment number (raw): 334909445
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x010 (ACK)
  Window: 502
  [Calculated window size: 64256]
  [Window size scaling factor: 128]
  Checksum: 0x8790 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    > TCP Option - No-Operation (NOP)
    > TCP Option - No-Operation (NOP)
    > TCP Option - Timestamps: TSval 2697910878, TSecr 264552619
  > [Timestamps]
  > [SEQ/ACK analysis]

```

הלקוח מחזיר לשרת הודעת ACK.

ה Sequence number בחבילה זו הוא 984980544, שינוי של 20 יותר מההודעה הקודמת שהלקוח שלח, וזהה ל Acknowledgement number של החבילה הקודמת שהשרת שלח ללקוח. רואים גם את השדה של Acknowledgement number שערכו הוא 334909445, שוב שינוי של 20 יותר מההודעה הקודמת שהלקוח שלח, וזהה ל Sequence number של החבילה הקודמת שהשרת שלח (שכן אנו מעלים ב 20 בתים את המקום ממנו אנו אומרים לצד השני להתחיל לקרוא, וקיבלנו גם עוד 20 מהשרת חזרה).

חבילה (57) :8

```

> Frame 57: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface enp0s3, id 0
> Ethernet II, Src: PcsCompu_3a:39:47 (08:00:27:3a:39:47), Dst: PcsCompu_3a:39:47 (08:00:27:3a:39:47)
> Internet Protocol Version 4, Src: 192.168.100.5, Dst: 192.168.100.4
> Transmission Control Protocol, Src Port: 60692, Dst Port: 12345, Seq: 21, Ack: 21, Len: 20
  Source Port: 60692
  Destination Port: 12345
  [Stream index: 2]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 20]
  Sequence Number: 21 (relative sequence number)
  Sequence Number (raw): 984980544
  [Next Sequence Number: 41 (relative sequence number)]
  Acknowledgment Number: 21 (relative ack number)
  Acknowledgment number (raw): 334909445
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
  Window: 502
  [Calculated window size: 64256]
  [Window size scaling factor: 128]
  Checksum: 0x9c72 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
  > [SEQ/ACK analysis]
  TCP payload (20 bytes)
> Data (20 bytes)

```


זוהי החבילה השנייה שהלקוח שולח לשרת ("206821258, 319024600").
גודל החבילה הוא שוב 20 בתים.
ה Sequence number בחבילה זו הוא 984980544, ללא שינוי מההודעה הקודמת, שכן נרצה שהשרת עדיין יקרא מאותו המקום.
רואים גם את השדה של Acknowledgement number שערכו הוא 334909445, שוב ללא שינוי כיוון שהשרת לא שלח כלום.

חבילה (58) 9:

```

> Frame 58: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface enp0s3, id 0
> Ethernet II, Src: PcsCompu_3a:39:47 (08:00:27:3a:39:47), Dst: PcsCompu_3a:39:47 (08:00:27:3a:39:47)
> Internet Protocol Version 4, Src: 192.168.100.4, Dst: 192.168.100.5
> Transmission Control Protocol, Src Port: 12345, Dst Port: 60692, Seq: 21, Ack: 41, Len: 0
  Source Port: 12345
  Destination Port: 60692
  [Stream index: 2]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 21 (relative sequence number)
  Sequence Number (raw): 334909445
  [Next Sequence Number: 22 (relative sequence number)]
  Acknowledgment Number: 41 (relative ack number)
  Acknowledgment number (raw): 984980564
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x011 (FIN, ACK)
  Window: 509
  [Calculated window size: 65152]
  [Window size scaling factor: 128]
  Checksum: 0x4981 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
  > [SEQ/ACK analysis]

```

בחבילה הזו, השרת שולח ללקוח שהוא סיים את התקשורת מהצד שלו.
זה מסומן על ידי ביט דולק בדגל FIN.
הלקוח עדיין יכול לשלוח הודעות לשרת.
ה Sequence number בחבילה זו הוא 334909445, יותר מהפעם הקודמת שכן השרת החזיר הודעה ללקוח שאורכה 20 בתים.
רואים גם את השדה של Acknowledgement number שערכו הוא 984980564, יותר ב 20 מהפעם הקודמת עקב 20 הבתים שהתקבלו מהלקוח עקב ההודעה השנייה שהוא שלח.

חבילה (59) 10:

```

> Frame 59: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface enp0s3, id 0
> Ethernet II, Src: PcsCompu_3a:39:47 (08:00:27:3a:39:47), Dst: PcsCompu_3a:39:47 (08:00:27:3a:39:47)
> Internet Protocol Version 4, Src: 192.168.100.5, Dst: 192.168.100.4
> Transmission Control Protocol, Src Port: 60692, Dst Port: 12345, Seq: 41, Ack: 21, Len: 0
  Source Port: 60692
  Destination Port: 12345
  [Stream index: 2]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 41 (relative sequence number)
  Sequence Number (raw): 984980564
  [Next Sequence Number: 42 (relative sequence number)]
  Acknowledgment Number: 21 (relative ack number)
  Acknowledgment number (raw): 334909445
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x011 (FIN, ACK)
  Window: 502
  [Calculated window size: 64256]
  [Window size scaling factor: 128]
  Checksum: 0x8777 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]

```


בחבילה הזו, הלקוח שולח לשרת שהוא סיים את התקשורת מהצד שלו.
זה מסומן על ידי ביט דולק בדגל FIN.

Sequence number בחבילה זו הוא 984980564, 20 יותר מהפעם הקודמת
שכן הלקוח שלח הודעה נוספת לשרת שאורכה 20 בתים.
רואים גם את השדה של Acknowledgement number שערכו הוא
334909445, זהה לפעם הקודמת כיוון שהשרת לא שלח כלום.

חבילה (60): 11:

```
Frame 60: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_3a:39:47 (08:00:27:3a:39:47), Dst: PcsCompu_3a:39:47 (08:00:27:3a:39:47)
Internet Protocol Version 4, Src: 192.168.100.4, Dst: 192.168.100.5
Transmission Control Protocol, Src Port: 12345, Dst Port: 60692, Seq: 22, Ack: 42, Len: 0
  Source Port: 12345
  Destination Port: 60692
  [Stream index: 2]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 22 (relative sequence number)
  Sequence Number (raw): 334909446
  [Next Sequence Number: 22 (relative sequence number)]
  Acknowledgment Number: 42 (relative ack number)
  Acknowledgment number (raw): 984980565
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x010 (ACK)
  Window: 509
  [Calculated window size: 65152]
  [Window size scaling factor: 128]
  Checksum: 0x4981 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  [Timestamps]
  [SEQ/ACK analysis]
```

השרת מחזיר ACK ללקוח על בקשת סיום ההתקשרות שלו.
עבור חבילה זו אין שכבת אפליקציה, השרת לא שולח הודעה אלא רק שולח
ACK.

Sequence number בחבילה זו הוא 334909446, 1 יותר מהפעם הקודמת
שכן השרת החזיר הודעה ללקוח שאורכה 1 בתים (ACK).
רואים גם את השדה של Acknowledgement number שערכו הוא
984980565, זהה לפעם הקודמת שכן הלקוח לא שלח כלום.

חבילה (61): 12:

```
Frame 61: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_3a:39:47 (08:00:27:3a:39:47), Dst: PcsCompu_3a:39:47 (08:00:27:3a:39:47)
Internet Protocol Version 4, Src: 192.168.100.5, Dst: 192.168.100.4
Transmission Control Protocol, Src Port: 60692, Dst Port: 12345, Seq: 42, Ack: 22, Len: 0
  Source Port: 60692
  Destination Port: 12345
  [Stream index: 2]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 42 (relative sequence number)
  Sequence Number (raw): 984980565
  [Next Sequence Number: 42 (relative sequence number)]
  Acknowledgment Number: 22 (relative ack number)
  Acknowledgment number (raw): 334909446
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x010 (ACK)
  Window: 502
  [Calculated window size: 64256]
  [Window size scaling factor: 128]
  Checksum: 0x876a [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  [Timestamps]
  [SEQ/ACK analysis]
```

הלקוח מחזיר ACK ללקוח על בקשת סיום ההתקשרות שלו.
עבור חבילה זו אין שכבת אפליקציה, הלקוח לא שולח הודעה אלא רק שולח ACK.
Sequence number בחבילה זו הוא 984980565, 1 יותר מהפעם הקודמת
שכן הלקוח החזיר הודעה ללקוח שאורכה 1 בתים (ACK).
רואים גם את השדה של Acknowledgement number שערכו הוא
334909446, 1 יותר מהפעם הקודמת עקב הACK שהשרת שלח וקראנו
בהצלחה.

הסבר עבור V1:

קוד השרת:

כתובת הIP המוגדרת היא '0.0.0.0' כלומר, כל כתובת IP, כל עוד הוא Port המתאים לסוקט.
את הפורט אנחנו מקבלים כארגומנט בשורת הפקודה.
בנוסף ניתן לראות כי הבאפר לכל אורך של הודעה הוא 1024 בתים.
השרת מאזין ללקוח 1 כל פעם.
הsocket של השרת לא נסגר והשרת רץ בלולאה אינסופית, שבלולאה זו הוא מקבל לקוח.
בפונק' accept, אנו מקבלים זוג של conn, addr שconn הוא אובייקט מסוג סוקט שיכול לקבל data בחיבור, addr הוא כתובת הIP של הלקוח.
לאחר יצירת התקשורת עם הלקוח הספציפי, מודפסת הודעה עם מי התבצעה התקשורת ומתחיל תהליך של שליחת הודעות בין השרת ל לקוח בתוך לולאה נוספת, בתוכה השרת משתמש ב socket הייעודי (conn) על מנת לקבל מידע מהלקוח.
אם הוא קיבל מידע, הוא מדפיס אותו ושולח הודעה בחזרה ללקוח עם אותו המידע באותיות גדולות.
אחרת - לא התקבל מידע מהלקוח, אנו יוצאים מהלולאה הפנימית והתקשורת ביניהם תסתיים ע"י סגירת הסוקט.

קוד הלקוח:

הלקוח מקבל כארגומנטים בשורת הפקודה את כתובת הIP של השרת ואת מספר Port שלו.
גודל הבאפר, כלומר גודל ההודעה שאפשר לקרוא בכל פעם הוא 1024 בתים.
יוצרים socket של פרוטוקול TCP ומתחברים לשרת לפי ה IP וה Port שהוגדרו.
לאחר מכן הלקוח שולח את ההודעה לשרת:
"Hello, World"

והלוקח מקבל תשובה מהשרת ע"י פקודת recv ומכניס את המידע למשתנה data.
לאחר מכן סוגרים את החיבור, ובזאת מסיים הלוקח את התקשורת מהצד שלו.
לאחר מכן הלוקח מדפיס את המידע שנשלח מהשרת(המשתנה data).

ניתוח החבילות באWireshark:

180	384.343408734	192.168.100.5	192.168.100.4	TCP	74	33670 → 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=311087744 TSecr=0 WS=128
181	384.343470194	192.168.100.4	192.168.100.5	TCP	74	12345 → 33670 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=1372051349 TSecr=311087744 WS=128
182	384.345196009	192.168.100.5	192.168.100.4	TCP	66	33670 → 12345 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=311087746 TSecr=1372051349
183	384.345196352	192.168.100.5	192.168.100.4	TCP	79	33670 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=13 TSval=311087746 TSecr=1372051349
184	384.345372017	192.168.100.4	192.168.100.5	TCP	66	12345 → 33670 [ACK] Seq=1 Ack=14 Win=65152 Len=0 TSval=1372051350 TSecr=311087746
185	384.346041368	192.168.100.4	192.168.100.5	TCP	79	12345 → 33670 [PSH, ACK] Seq=1 Ack=14 Win=65152 Len=13 TSval=1372051351 TSecr=311087746
186	384.347415700	192.168.100.5	192.168.100.4	TCP	66	33670 → 12345 [ACK] Seq=14 Ack=14 Win=64256 Len=0 TSval=311087748 TSecr=1372051351
187	384.348210614	192.168.100.5	192.168.100.4	TCP	66	33670 → 12345 [FIN, ACK] Seq=14 Ack=14 Win=64256 Len=0 TSval=311087749 TSecr=1372051351
188	384.348622762	192.168.100.4	192.168.100.5	TCP	66	12345 → 33670 [FIN, ACK] Seq=14 Ack=15 Win=65152 Len=0 TSval=1372051354 TSecr=311087749
189	384.349960605	192.168.100.5	192.168.100.4	TCP	66	33670 → 12345 [ACK] Seq=15 Ack=15 Win=64256 Len=0 TSval=311087751 TSecr=1372051354

החבילה הראשונה נשלחת מהלוקח לשרת עם הדגל SYN ע"מ להסתנכרן מולו.
לאחר מכן גם השרת שולח ללוקח חבילה עם הדגל SYN דלוק ע"מ להסתנכרן מול הלוקח ושולח גם ACK לאישור באותה החבילה.
בחבילה השלישית הלוקח שולח לשרת חבילת ACK ע"מ לאשר את קבלת החבילה שנשלחה אליו ע"י השרת.
כאן הסתיים תהליך הקמת החיבור.
מיד לאחר מכן הוא שולח חבילה נוספת ובה כולל את ההודעה "hello world"
כלומר חבילה זו כוללת את שכבת האפליקציה.
החבילה החמישית - חבילה שהשרת שולח ללוקח בה הוא מאשר את קבלת החבילה שהלוקח שלח באמצעות ACK.
לאחר מכן, השרת שולח ללוקח חבילה נוספת הכוללת מידע בשכבת האפליקציה(PSH ACK).
הודעה זו היא ההודעה שהלוקח שלח באותיות גדולות.
החבילה השביעית היא חבילת ACK שהלוקח שולח לשרת ע"מ להודיע לו שקיבל את ההודעה שלו.
לאחר מכן, הלוקח שולח חבילה עם הדגל FIN ע"מ לבשר לשרת שסיים את התקשורת מהצד שלו.
השרת שולח ללוקח גם כן חבילת FIN שיש בה גם ACK כאישור(גם הלוקח שלח ACK מקודם יחד עם ה-FIN).
החבילה האחרונה היא חבילת ACK שהלוקח שולח לשרת ע"מ לומר לו שהוא קיבל את חבילת ה-FIN שלו.

הסבר עבור V2:

קוד השרת:

זהה לחלוטין לV1, למעט שכאן גודל הבאפר הוא 5 בתים.

קוד הלקוח:

זהה לחלוטין לV1, למעט שכאן תוכן ההודעה שונה וגודל הבאפר הוא 5 בתים.

ניתוח החבילות בwireshark:

111	17.962487783	192.168.100.5	192.168.100.4	TCP	74	52474 → 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=312538643 TSecr=0 WS=128
112	17.962514828	192.168.100.4	192.168.100.5	TCP	74	12345 → 52474 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=1373502249 TSecr=312538643 WS=128
113	17.963501745	192.168.100.5	192.168.100.4	TCP	66	52474 → 12345 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=312538646 TSecr=1373502249
114	17.963501955	192.168.100.5	192.168.100.4	TCP	86	52474 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=20 TSval=312538646 TSecr=1373502249
115	17.963614300	192.168.100.4	192.168.100.5	TCP	66	12345 → 52474 [ACK] Seq=1 Ack=21 Win=65152 Len=0 TSval=1373502250 TSecr=312538646
116	17.964145710	192.168.100.4	192.168.100.5	TCP	71	12345 → 52474 [PSH, ACK] Seq=1 Ack=21 Win=65152 Len=5 TSval=1373502250 TSecr=312538646
117	17.964819008	192.168.100.5	192.168.100.4	TCP	66	52474 → 12345 [ACK] Seq=21 Ack=6 Win=64256 Len=0 TSval=312538647 TSecr=1373502250
118	17.964831832	192.168.100.4	192.168.100.5	TCP	81	12345 → 52474 [PSH, ACK] Seq=6 Ack=21 Win=65152 Len=15 TSval=1373502251 TSecr=312538647
119	17.966435517	192.168.100.5	192.168.100.4	TCP	66	52474 → 12345 [FIN, ACK] Seq=21 Ack=6 Win=64256 Len=0 TSval=312538648 TSecr=1373502250
120	17.966435650	192.168.100.5	192.168.100.4	TCP	60	52474 → 12345 [RST] Seq=21 Win=0 Len=0

החבילה הראשונה נשלחת מהלקוח לשרת עם הדגל SYN ע"מ להסתנכר מולו.
לאחר מכן גם השרת שולח ללקוח חבילה עם הדגל SYN דלוק ע"מ להסתנכר
מול הלקוח, יחד עם ACK באותה החבילה כדי לאשר את קבלת החבילה
הקודמת.

בחבילה השלישית הלקוח שולח לשרת חבילת ACK ע"מ לאשר את קבלת
החבילה שנשלחה אליו.

כאן מסתיים תהליך הקמת החיבור.

לאחר מכן הלקוח שולח חבילה נוספת ובה כולל את ההודעה:
"!World! Hello, World"

כלומר חבילה זו כוללת את שכבת האפליקציה.

החבילה החמישית היא חבילה שהשרת שולח ללקוח בה הוא מאשר את קבלת
החבילה שהלקוח שלח באמצעות ACK.

לאחר מכן השרת שולח ללקוח חבילה נוספת הכוללת מידע בשכבת
האפליקציה (5 הבתים הראשונים שהלקוח שלח באותיות גדולות).

החבילה הבאה היא חבילה שהלקוח שולח עם הדגל ACK ע"מ לאשר לשרת
שהוא קיבל את ההודעה.

החבילה הבאה היא חבילה שהשרת שולח ללקוח עם יתרת ההודעה של הלקוח
באותיות גדולות, ובאותה החבילה הוא מחזיר ACK גם כן.

לאחר מכן הלקוח מכריז שהוא סיים את התקשורת ע"י שליחת חבילה לשרת עם הדגל FIN דלוק.
 החבילה האחרונה היא חבילה שהלקוח שולח לשרת גם כן, חבילה זו עם דגל RST דלוק נשלחת כתוצאה מכך שהשרת המשיך לשלוח חבילות לאחר שהלקוח סגר את התקשורת(השרת לא שלח FIN).

הסבר עבור V3:

קוד השרת:

זהה לחלוטין ל V1, למעט שהמידע שנשלח ללקוח הוא 1000 פעמים המידע שנשלח ללקוח ב V1 .

קוד הלקוח:

זהה לחלוטין ל V1, למעט שכאן מקבלים מידע מהבאפר פעמיים ולא פעם אחת באמצעות הפקודה recv, ומכיוון שמקבלים מידע פעמיים גם מדפיסים פעמיים.

ניתוח החבילות ב wireshark:

340	28.372398977	192.168.100.5	192.168.100.4	TCP	74	38088 → 12345 [SYN, Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=315833301 TSecr=0 WS=128
341	28.372424313	192.168.100.4	192.168.100.5	TCP	74	12345 → 38088 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=1376797117 TSecr=315833301 WS=128
342	28.374343075	192.168.100.5	192.168.100.4	TCP	66	38088 → 12345 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=315833304 TSecr=1376797117
343	28.375373799	192.168.100.5	192.168.100.4	TCP	79	38088 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=13 TSval=315833304 TSecr=1376797117
344	28.375389574	192.168.100.4	192.168.100.5	TCP	66	12345 → 38088 [ACK] Seq=1 Ack=14 Win=65152 Len=0 TSval=1376797120 TSecr=315833304
345	28.376068184	192.168.100.4	192.168.100.5	TCP	7306	12345 → 38088 [PSH, ACK] Seq=1 Ack=14 Win=65152 Len=7240 TSval=1376797121 TSecr=315833304
346	28.376378395	192.168.100.4	192.168.100.5	TCP	5826	12345 → 38088 [PSH, ACK] Seq=7241 Ack=14 Win=65152 Len=5760 TSval=1376797121 TSecr=315833304
347	28.377143773	192.168.100.5	192.168.100.4	TCP	66	38088 → 12345 [ACK] Seq=14 Ack=7241 Win=60672 Len=0 TSval=315833307 TSecr=1376797121
348	28.377143868	192.168.100.5	192.168.100.4	TCP	66	38088 → 12345 [ACK] Seq=14 Ack=13001 Win=56832 Len=0 TSval=315833307 TSecr=1376797121
349	28.377143888	192.168.100.5	192.168.100.4	TCP	66	38088 → 12345 [RST, ACK] Seq=14 Ack=13001 Win=64128 Len=0 TSval=315833307 TSecr=1376797121

החבילה הראשונה נשלחת מהלקוח לשרת עם הדגל SYN ע"מ להסתנכרן מול השרת.

לאחר מכן גם השרת שולח ללקוח חבילה עם הדגל SYN דלוק ע"מ להסתנכרן מול הלקוח, בנוסף מאשר את קבלת חבילת הלקוח ע"י ACK באותה החבילה. בחבילה השלישית הלקוח שולח לשרת חבילת ACK לאישור קבלה. כאן מסתיים תהליך הקמת החיבור.

לאחר מכן הלקוח שולח חבילה נוספת ובה ההודעה: "Hello, World"

כלומר חבילה זו כוללת את שכבת האפליקציה.

החבילה החמישית - חבילה שהשרת שולח ללקוח בה הוא מאשר את קבלת החבילה שהלקוח שלח באמצעות ACK.

לאחר מכן השרת שולח ללקוח חבילה נוספת הכוללת מידע בשכבת האפליקציה, מידע זה הוא ההודעה שהלקוח שלח באותיות גדולות אלף פעמים. גם בחבילה השביעית, יש את שאר הפעמים הנותרות מתוך 1000.

לאחר מכן, הלקוח שולח לשרת חבילת ACK המאשרת שקיבל ממנו את כל 13,000 הבתים, בשתי חבילות ACK שונות כפי שהשרת שלח לו בשתי חבילות.

החבילה האחרונה היא חבילת RST לשרת שבעצם אומרת שהלקוח חייב לסיים את הקשר ולא קרא את כל מה שהשרת שלח לו.
מה שקורה הוא שגודל ה buffer של הלקוח הוא 1024, ובכל קריאה של ה Data מה buffer הוא בעצם קורא 1024 בתים.
מכיוון שמתבצעות רק 2 קריאות של recv, נקראים סה"כ 2048 בתים, מה שמשאיר 10952 בתים עדיין בבאפר, מידע שהלקוח לא מתכוון לקרוא(טיפה יותר מ13000 סה"כ, אך זה בעקבות הקידוד).
לכן נשלחת חבילת RST.

הסבר עבור V4:

קוד השרת:

זהה לחלוטין לV1, למעט שלפני קריאת המידע שנמצא בבאפר, השרת מחכה 5 שניות(בעזרת sleep).

קוד הלקוח:

זהה לחלוטין לV1, למעט שכאן מבצעים 4 פעמים send ובכל אחת מהן שולחים 10 פעמים את ההודעה.

ניתוח החבילות בwireshark:

80	13.518319175	192.168.100.5	192.168.100.4	TCP	74	57958 → 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=316970460 TSecr=0 WS=128
81	13.518350114	192.168.100.4	192.168.100.5	TCP	74	12345 → 57958 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=1377934047 TSecr=316970460 WS=128
82	13.520880101	192.168.100.5	192.168.100.4	TCP	66	57958 → 12345 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=316970463 TSecr=1377934047
83	13.525503132	192.168.100.5	192.168.100.4	TCP	196	57958 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=130 TSval=316970469 TSecr=1377934047
84	13.525522870	192.168.100.4	192.168.100.5	TCP	66	12345 → 57958 [ACK] Seq=1 Ack=131 Win=65152 Len=0 TSval=1377934054 TSecr=316970469
85	13.527285414	192.168.100.5	192.168.100.4	TCP	456	57958 → 12345 [PSH, ACK] Seq=131 Ack=1 Win=64256 Len=390 TSval=316970470 TSecr=1377934054
86	13.527296629	192.168.100.4	192.168.100.5	TCP	66	12345 → 57958 [ACK] Seq=1 Ack=521 Win=64768 Len=0 TSval=1377934056 TSecr=316970470
110	18.529054028	192.168.100.4	192.168.100.5	TCP	586	12345 → 57958 [PSH, ACK] Seq=1 Ack=521 Win=64768 Len=520 TSval=1377939058 TSecr=316970470
111	18.534588016	192.168.100.5	192.168.100.4	TCP	66	57958 → 12345 [ACK] Seq=521 Ack=521 Win=64128 Len=0 TSval=316975475 TSecr=1377939058
112	18.534588711	192.168.100.5	192.168.100.4	TCP	66	57958 → 12345 [FIN, ACK] Seq=521 Ack=521 Win=64128 Len=0 TSval=316975476 TSecr=1377939058
113	18.579905636	192.168.100.4	192.168.100.5	TCP	66	12345 → 57958 [ACK] Seq=521 Ack=522 Win=64768 Len=0 TSval=1377939109 TSecr=316975476
124	23.536057806	192.168.100.4	192.168.100.5	TCP	66	12345 → 57958 [FIN, ACK] Seq=521 Ack=522 Win=64768 Len=0 TSval=1377944065 TSecr=316975476
125	23.537066478	192.168.100.5	192.168.100.4	TCP	66	57958 → 12345 [ACK] Seq=522 Ack=522 Win=64128 Len=0 TSval=316980481 TSecr=1377944065

החבילה הראשונה נשלחת מהלקוח לשרת עם הדגל SYN ע"מ להסתנכר מולו.
לאחר מכן גם השרת שולח ללקוח חבילה עם הדגל SYN דלוק ע"מ להסתנכר מול הלקוח, בנוסף מאשר את קבלת חבילת הלקוח ע"י ACK באותה החבילה.

בחבילה השלישית הלקוח שולח לשרת חבילת ACK ע"מ לאשר את קבלת החבילה.

כאן מסתיים תהליך הקמת החיבור.
לאחר מכן הוא שולח חבילה נוספת ובה כולל את

ההודעה:

Hello, World!Hello, World!Hello, World!Hello, World!Hello, “
,World!Hello, World!Hello, World!Hello

!“World!Hello, World!Hello, World

כלומר חבילה זו כוללת את שכבת האפליקציה.
החבילה החמישית - חבילה שהשרת שולח ללקוח בה הוא מאשר את קבלת החבילה שהלקוח שלח באמצעות ACK.
לאחר מכן הלקוח שולח לשרת חבילה נוספת באורך 456 עם שאר התוכן, כלומר חבילה עם שכבת אפליקציה.
לאחר מכן השרת שלח ללקוח חבילת ACK המאשרת את קבלת המידע מהלקוח.

כעת, בחבילה הבאה אנו רואים פעם ראשונה שהשרת שולח מידע ללקוח, המידע נאסף בבאפר ונשלח באופן מרוכז לאחר 5 שניות באותיות גדולות. זה נגרם כתוצאה מהטיימר שהיה בקוד, ניתן גם לראות שעברו 5 שניות ב-wireshark.

החבילה הבאה היא חבילת ACK שהלקוח שולח לשרת המאשרת את קבלת המידע.

לאחר מכן הלקוח שולח חבילה עם הדגל FIN ע"מ לבשר לשרת שמבחינתו סיים את התקשורת. כתוצאה מכך, השרת שולח חבילת ACK המאשרת שקיבל את חבילת ה-FIN.

לאחר מכן, שולח השרת חבילה נוספת המבשרת שגם הוא סיים את התקשורת עם הלקוח, והוא מבצע זאת על ידי הדלקת הדגל FIN גם כן.
החבילה האחרונה היא חבילת ACK שהלקוח שולח לשרת המאשרת את קבלת חבילת ה-FIN שלו.

הרצה של

הכל



No.	Time	Source	Destination	Protocol	Length	Info
9	16.02082622	127.0.0.1	127.0.0.1	TCP	60	60824 → 12345 [Syn] Seq=1 Min=65495 Len=0 MS=65495 SACK PERM=1 Tsvail=185143425 TSecr=185143425
10	16.02302222	127.0.0.1	127.0.0.1	TCP	74	12345 → 60284 [ACK] Seq=1 Seq=1 Ack=1 Len=65483 Len=0 MS=65495 SACK PERM=1 Tsvail=185143425 TSecr=185143425 MS=128
11	16.26301522	127.0.0.1	127.0.0.1	TCP	60	60824 → 12345 [ACK] Seq=1 Seq=1 Ack=1 Len=65536 Len=0 Tsvail=185143425 TSecr=185143425
12	16.00162968	127.0.0.1	127.0.0.1	TCP	60	12345 → 60284 [FIN] Seq=1 Seq=1 Ack=1 Len=65536 Len=0 Tsvail=1851434963 TSecr=1851433992
13	17.00000000	127.0.0.1	127.0.0.1	TCP	60	60826 → 12345 [FIN] Seq=1 Seq=1 Ack=1 Len=65536 Len=0 Tsvail=1851434963 TSecr=1851434963
14	17.00175955	127.0.0.1	127.0.0.1	TCP	60	12345 → 60286 [ACK] Seq=1 Seq=1 Ack=1 Len=65536 Len=0 Tsvail=1851434993 TSecr=1851434993
15	16.81248086	127.0.0.1	127.0.0.1	TCP	3284	12345 → 60284 [ACK] Seq=1 Ack=708 Min=65536 Len=32768 Tsvail=1851435087 TSecr=1851433992 [TCP segment of a reassembled PDU]
16	16.81543590	127.0.0.1	127.0.0.1	TCP	60	60824 → 12345 [ACK] Seq=1 Seq=1 Ack=1 Len=65536 Len=0 Tsvail=1851435087 TSecr=1851435087
17	17.01505346	127.0.0.1	127.0.0.1	TCP	3284	12345 → 60284 [PSH, ACK] Seq=32768 Ack=708 Min=65536 Len=32768 Tsvail=1851435087 TSecr=1851433992 [TCP segment of a reassembled PDU]
18	16.81555398	127.0.0.1	127.0.0.1	TCP	60	60824 → 12345 [ACK] Seq=708 Ack=55537 Min=85236 Len=0 Tsvail=1851435087 TSecr=1851435087
19	16.81557606	127.0.0.1	127.0.0.1	TCP	3284	12345 → 60284 [ACK] Seq=55537 Ack=708 Min=65536 Len=32768 Tsvail=1851435087 TSecr=1851435087 [TCP segment of a reassembled PDU]
20	17.01505346	127.0.0.1	127.0.0.1	TCP	3284	12345 → 60284 [PSH, ACK] Seq=55537 Ack=708 Min=65536 Len=32768 Tsvail=1851435087 TSecr=1851435087 [TCP segment of a reassembled PDU]
21	16.81562298	127.0.0.1	127.0.0.1	TCP	60	60824 → 12345 [ACK] Seq=708 Ack=38309 Min=65536 Len=0 Tsvail=1851435087 TSecr=1851435087
22	16.81562606	127.0.0.1	127.0.0.1	TCP	60	60824 → 12345 [ACK] Seq=708 Ack=11073 Min=16640 Len=0 Tsvail=1851435087 TSecr=1851435087
23	16.81564046	127.0.0.1	127.0.0.1	TCP	3284	12345 → 60284 [ACK] Seq=708 Ack=11073 Min=65536 Len=32768 Tsvail=1851435087 TSecr=1851435087 [TCP segment of a reassembled PDU]
24	16.81565398	127.0.0.1	127.0.0.1	TCP	60	60824 → 12345 [ACK] Seq=708 Ack=16341 Min=72552 Len=0 Tsvail=1851435087 TSecr=1851435087
25	16.81567246	127.0.0.1	127.0.0.1	TCP	3284	12345 → 60284 [PSH, ACK] Seq=16341 Ack=708 Min=65536 Len=32768 Tsvail=1851435087 TSecr=1851435087 [TCP segment of a reassembled PDU]
26	16.81567628	127.0.0.1	127.0.0.1	TCP	60	60824 → 12345 [ACK] Seq=708 Ack=19609 Min=58466 Len=0 Tsvail=1851435087 TSecr=1851435087
27	16.81568296	127.0.0.1	127.0.0.1	HTTP	2475	HTTP/1.1 200 OK (JPEG image)
28	16.81568786	127.0.0.1	127.0.0.1	TCP	60	60824 → 12345 [ACK] Seq=708 Ack=20818 Min=58466 Len=0 Tsvail=1851435087 TSecr=1851435087
29	16.81569572	127.0.0.1	127.0.0.1	TCP	60	12345 → 60284 [FIN, ACK] Seq=1 Seq=1 Ack=1 Min=65536 Len=0 Tsvail=1851436069 TSecr=1851435087
30	16.81569572	127.0.0.1	127.0.0.1	TCP	60	60824 → 12345 [ACK] Seq=1 Seq=1 Ack=1 Min=65536 Len=0 Tsvail=1851436069 TSecr=1851435087
31	16.81569572	127.0.0.1	127.0.0.1	TCP	60	12345 → 60284 [ACK] Seq=22019 Ack=708 Min=65536 Len=0 Tsvail=1851436069 TSecr=1851436069
32	16.81569572	127.0.0.1	127.0.0.1	TCP	60	12345 → 60284 [ACK] Seq=22019 Ack=708 Min=65536 Len=0 Tsvail=1851436069 TSecr=1851436069
33	16.81569572	127.0.0.1	127.0.0.1	TCP	60	12345 → 60284 [ACK] Seq=22019 Ack=708 Min=65536 Len=0 Tsvail=1851436069 TSecr=1851436069
34	16.81569572	127.0.0.1	127.0.0.1	TCP	60	12345 → 60284 [ACK] Seq=22019 Ack=708 Min=65536 Len=0 Tsvail=1851436069 TSecr=1851436069
35	16.81569572	127.0.0.1	127.0.0.1	TCP	60	12345 → 60284 [ACK] Seq=22019 Ack=708 Min=65536 Len=0 Tsvail=1851436069 TSecr=1851436069
36	16.81569572	127.0.0.1	127.0.0.1	TCP	60	12345 → 60284 [ACK] Seq=22019 Ack=708 Min=65536 Len=0 Tsvail=1851436069 TSecr=1851436069
37	16.81569572	127.0.0.1	127.0.0.1	TCP	60	

ניתן לראות כי יש כאן חיבור יחיד שבו הדפדפן שולח בקשה
לשרת לקבל את הקובץ 5.jpg שהוא קובץ של תמונת עוגת

וניל טעימה וקריספית. מפני שתוכן התמונה גדול (תמונה שוקלת יותר מסתם מחרוזת) כמו בבקשות אחרות שנראה פה השרת מחלק את החבילה לסגמנטים, הוא לא יכול לשלוח את כל התמונה בבת אחת כי גודלה הוא גדול יותר מהMSS ולכן הוא מחלק אותה לחתיכות ושולח אותן אחת-אחת. הלקוח מקבל את כל אחד מהחלקים האלה, מחזיר ACK עליהם ואחר כך התקשורת נסגרת משני הצדדים ע"י FIN הדדי.

הרצה של /a/b/ref.html :

הכל

tcp.port == 12345						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	TCP	74	51899 → 12345 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1853322848 TSecr=0 WS=128
2	0.000000160	127.0.0.1	127.0.0.1	TCP	74	51899 → 12345 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1853322848 TSecr=0 WS=128
3	0.000000000	127.0.0.1	127.0.0.1	TCP	74	12345 → 51899 [SYN, ACK] Seq=0 Ack=1 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1853322848 TSecr=1853322848 WS=128
4	0.000000000	127.0.0.1	127.0.0.1	TCP	74	12345 → 51899 [SYN, ACK] Seq=0 Ack=1 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1853322848 TSecr=1853322848 WS=128
5	0.000000000	127.0.0.1	127.0.0.1	TCP	66	51899 → 12345 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1853322848 TSecr=1853322848
6	0.000000000	127.0.0.1	127.0.0.1	TCP	66	51899 → 12345 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1853322848 TSecr=1853322848
7	0.000027700	127.0.0.1	127.0.0.1	HTTP	778	GET /a/b/ref.html HTTP/1.1
8	0.000332800	127.0.0.1	127.0.0.1	TCP	66	12345 → 51899 [ACK] Seq=1 Ack=713 Win=64896 Len=0 TSval=1853322848 TSecr=1853322848
9	0.010242499	127.0.0.1	127.0.0.1	HTTP	733	HTTP/1.1 200 OK
10	0.010266199	127.0.0.1	127.0.0.1	TCP	66	51899 → 12345 [ACK] Seq=713 Ack=668 Win=64896 Len=0 TSval=1853322864 TSecr=1853322864
11	0.034409599	127.0.0.1	127.0.0.1	HTTP	701	GET /a/1.jpg HTTP/1.1
12	0.046033599	127.0.0.1	127.0.0.1	HTTP	703	GET /a/0/1.jpg HTTP/1.1
13	0.047181599	127.0.0.1	127.0.0.1	TCP	66	12345 → 51899 [ACK] Seq=1 Ack=038 Win=64896 Len=0 TSval=1853322883 TSecr=1853322883
14	0.051618099	127.0.0.1	127.0.0.1	TCP	32834	12345 → 51899 [ACK] Seq=668 Ack=1348 Win=65536 Len=32768 TSval=1853322899 TSecr=1853322882 [TCP segment of a reassembled PDU]
15	0.051655599	127.0.0.1	127.0.0.1	TCP	32834	12345 → 51899 [ACK] Seq=668 Ack=1348 Win=65536 Len=32768 TSval=1853322899 TSecr=1853322882 [TCP segment of a reassembled PDU]
16	0.051701599	127.0.0.1	127.0.0.1	TCP	66	51899 → 12345 [ACK] Seq=1348 Ack=66204 Win=65536 Len=0 TSval=1853322899 TSecr=1853322899
17	0.051707599	127.0.0.1	127.0.0.1	TCP	32834	12345 → 51899 [ACK] Seq=66204 Ack=1348 Win=65536 Len=32768 TSval=1853322899 TSecr=1853322899 [TCP segment of a reassembled PDU]
18	0.051722599	127.0.0.1	127.0.0.1	TCP	32834	[TCP Window Full] 12345 → 51899 [PSH, ACK] Seq=98977 Ack=1348 Win=65536 Len=32768 TSval=1853322899 TSecr=1853322899 [TCP segment of a reassembled PDU]
19	0.051728599	127.0.0.1	127.0.0.1	TCP	66	51899 → 12345 [ACK] Seq=1348 Ack=98977 Win=65536 Len=0 TSval=1853322899 TSecr=1853322899
20	0.051763599	127.0.0.1	127.0.0.1	TCP	66	51899 → 12345 [ACK] Seq=1348 Ack=131740 Win=65536 Len=0 TSval=1853322899 TSecr=1853322899
21	0.051769599	127.0.0.1	127.0.0.1	TCP	32834	12345 → 51899 [ACK] Seq=131740 Ack=1348 Win=65536 Len=32768 TSval=1853322899 TSecr=1853322899 [TCP segment of a reassembled PDU]
22	0.051774599	127.0.0.1	127.0.0.1	TCP	32834	[TCP Window Full] 12345 → 51899 [PSH, ACK] Seq=161568 Ack=1348 Win=65536 Len=32768 TSval=1853322899 TSecr=1853322899 [TCP segment of a reassembled PDU]
23	0.051782599	127.0.0.1	127.0.0.1	TCP	66	51899 → 12345 [ACK] Seq=1348 Ack=161276 Win=65536 Len=0 TSval=1853322899 TSecr=1853322899
24	0.051787599	127.0.0.1	127.0.0.1	TCP	32834	12345 → 51899 [ACK] Seq=161276 Ack=1348 Win=65536 Len=32768 TSval=1853322899 TSecr=1853322899 [TCP segment of a reassembled PDU]
25	0.051791599	127.0.0.1	127.0.0.1	TCP	32834	12345 → 51899 [PSH, ACK] Seq=230944 Ack=1348 Win=65536 Len=32768 TSval=1853322899 TSecr=1853322899 [TCP segment of a reassembled PDU]
26	0.051813599	127.0.0.1	127.0.0.1	TCP	32834	12345 → 51899 [ACK] Seq=262812 Ack=1348 Win=65536 Len=32768 TSval=1853322899 TSecr=1853322899 [TCP segment of a reassembled PDU]
27	0.051813599	127.0.0.1	127.0.0.1	TCP	32834	12345 → 51899 [ACK] Seq=262812 Ack=1348 Win=65536 Len=32768 TSval=1853322899 TSecr=1853322899 [TCP segment of a reassembled PDU]

* Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface lo, id 8
* Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
* Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
* Transmission Control Protocol, Src Port: 51899, Dst Port: 12345, Seq: 0, Len: 8

פקטה

203	2.280074158	127.0.0.1	127.0.0.1	TCP	66	51900	-	12345	[ACK] Seq=636 Ack=458753 Win=1375230 Len=0 TSval=1853325137 TSrcr=1853325137
204	2.280978176	127.0.0.1	127.0.0.1	TCP	66	51900	-	12345	[ACK] Seq=636 Ack=458753 Win=1375230 Len=0 TSval=1853325137 TSrcr=1853325137
205	2.280978156	127.0.0.1	127.0.0.1	TCP	66	51900	-	12345	[ACK] Seq=636 Ack=458753 Win=1375230 Len=0 TSval=1853325137 TSrcr=1853325137
206	2.280978156	127.0.0.1	127.0.0.1	TCP	66	51900	-	12345	[ACK] Seq=636 Ack=458753 Win=1375230 Len=0 TSval=1853325137 TSrcr=1853325137
207	2.280980328	127.0.0.1	127.0.0.1	TCP	7668	11701	1	208 OK	[CPEX GET] image1
208	2.280980328	127.0.0.1	127.0.0.1	TCP	66	51900	-	12345	[ACK] Seq=636 Ack=511991 Win=1748064 Len=0 TSval=1853325137 TSrcr=1853325137
209	2.280912530	127.0.0.1	127.0.0.1	TCP	66	12345	-	51900	[FIN, ACK] Seq=515091 Ack=458 Win=65536 Len=0 TSval=1853326138 TSrcr=1853325137
210	2.283141319	127.0.0.1	127.0.0.1	TCP	66	51900	-	12345	[ACK] Seq=636 Ack=511991 Win=1748064 Len=0 TSval=1853326138 TSrcr=1853326138
211	2.283621139	127.0.0.1	127.0.0.1	TCP	66	12345	-	51900	[ACK] Seq=515092 Ack=637 Win=65536 Len=0 TSval=1853326138 TSrcr=1853326138
212	2.283621139	127.0.0.1	127.0.0.1	TCP	66	12345	-	51900	[ACK] Seq=515092 Ack=637 Win=65536 Len=0 TSval=1853326138 TSrcr=1853326138
213	2.283621139	127.0.0.1	127.0.0.1	TCP	66	12345	-	51900	[ACK] Seq=515092 Ack=637 Win=65536 Len=0 TSval=1853326138 TSrcr=1853326138
214	2.291442921	127.0.0.1	127.0.0.1	TCP	66	12345	-	51900	[ACK] Seq=515092 Ack=637 Win=65536 Len=0 TSval=1853327139 TSrcr=1853327139
215	2.291442921	127.0.0.1	127.0.0.1	TCP	66	12345	-	51900	[ACK] Seq=515092 Ack=637 Win=65536 Len=0 TSval=1853327139 TSrcr=1853327139
216	2.291501021	127.0.0.1	127.0.0.1	TCP	66	12345	-	51900	[ACK] Seq=515092 Ack=637 Win=65536 Len=0 TSval=1853327139 TSrcr=1853327139
217	2.292641983	127.0.0.1	127.0.0.1	TCP	66	12345	-	51918	[ACK] Seq=515092 Ack=637 Win=65536 Len=0 TSval=1853328140 TSrcr=1853328140
218	2.292641983	127.0.0.1	127.0.0.1	TCP	66	12345	-	51918	[ACK] Seq=515092 Ack=637 Win=65536 Len=0 TSval=1853328140 TSrcr=1853328140
219	2.292641983	127.0.0.1	127.0.0.1	TCP	66	12345	-	51918	[ACK] Seq=515092 Ack=637 Win=65536 Len=0 TSval=1853328140 TSrcr=1853328140
220	2.292641983	127.0.0.1	127.0.0.1	TCP	66	12345	-	51918	[ACK] Seq=515092 Ack=637 Win=65536 Len=0 TSval=1853328140 TSrcr=1853328140
221	2.292641983	127.0.0.1	127.0.0.1	TCP	66	12345	-	51918	[ACK] Seq=515092 Ack=637 Win=65536 Len=0 TSval=1853328140 TSrcr=1853328140
222	2.292641983	127.0.0.1	127.0.0.1	TCP	66	12345	-	51918	[ACK] Seq=515092 Ack=637 Win=65536 Len=0 TSval=1853328140 TSrcr=1853328140
223	2.292641983	127.0.0.1	127.0.0.1	TCP	66	12345	-	51918	[ACK] Seq=515092 Ack=637 Win=65536 Len=0 TSval=1853328140 TSrcr=1853328140
224	2.292641983	127.0.0.1	127.0.0.1	TCP	66	12345	-	51918	[ACK] Seq=515092 Ack=637 Win=65536 Len=0 TSval=1853328140 TSrcr=1853328140
225	2.292641983	127.0.0.1	127.0.0.1	TCP	66	12345	-	51918	[ACK] Seq=515092 Ack=637 Win=65536 Len=0 TSval=1853328140 TSrcr=1853328140
226	2.292641983	127.0.0.1	127.0.0.1	TCP	66	12345	-	51918	[ACK] Seq=515092 Ack=637 Win=65536 Len=0 TSval=1853328140 TSrcr=1853328140
227	2.292641983	127.0.0.1	127.0.0.1	TCP	66	12345	-	51918	[ACK] Seq=515092 Ack=637 Win=65536 Len=0 TSval=1853328140 TSrcr=1853328140
228	2.292641983	127.0.0.1	127.0.0.1	TCP	66	12345	-	51918	[ACK] Seq=515092 Ack=637 Win=65536 Len=0 TSval=1853328140 TSrcr=1853328140
229	2.292641983	127.0.0.1	127.0.0.1	TCP	66	12345	-	51918	[ACK] Seq=515092 Ack=637 Win=65536 Len=0 TSval=1853328140 TSrcr=1853

כפי שניתן לראות מאורך הבקשה, שהדפדפן שלנו (הלקוח) פונה לשרת בבקשה לקבל את הקובץ <a/b/ref.html> שזה קובץ html שבתוכו יש ייחוסים לקבצים אחרים, לכן השרת מוריד את הקבצים הנוספים הללו דרך אותו החיבור ובמקביל

הוא פותח חיבורים נוספים שאיתם הוא יכול להוריד במקביל את הקבצים כדי לחסוך בזמן. כלומר, הדפדפן שואף לפתוח מספר חיבורים במקביל מול השרת ולא רק אחד, כי הדבר חוסך זמן. לכן, במקרה זה השרת פתח מספר חיבורים שבהם הוא טיפל אחד אחרי השני, כך שכל חיבור מבקש את התמונה המתאימה מהשרת והוא בתגובה מחזיר את תוכן התמונה או הקובץ המבוקש. השורות השורות שכתוב בהן Window Full באדום אומר שהחלון TCP שלמדנו עליו בהרצאה מלא ולכן הוא לא ימשיך לשלוח בקשות עד שהוא יקבל Ack ויתפנה מקום בחלון.

הרצה של /not_found :

פקטה

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	TCP	74	42500 → 12346 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 SACK_PERM=1 TSval=1858709430 TSecr=0 WS=128
2	0.000001200	127.0.0.1	127.0.0.1	TCP	74	42506 → 12346 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1858709430 TSecr=0 WS=128
3	0.000002600	127.0.0.1	127.0.0.1	TCP	74	12346 → 42508 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=1858709430 TSecr=1858709430 WS=128
4	0.000002700	127.0.0.1	127.0.0.1	TCP	74	12346 → 42508 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=1858709430 TSecr=1858709430 WS=128
5	0.000005500	127.0.0.1	127.0.0.1	TCP	66	42506 → 12346 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1858709430 TSecr=1858709430
6	0.000005700	127.0.0.1	127.0.0.1	TCP	66	42506 → 12346 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1858709430 TSecr=1858709430
7	0.000444800	127.0.0.1	127.0.0.1	HTTP	801	GET /not_found HTTP/1.1
8	0.000453800	127.0.0.1	127.0.0.1	TCP	66	12346 → 42506 [ACK] Seq=1 Ack=736 Win=64768 Len=0 TSval=1858709430 TSecr=1858709430
9	0.259478611	127.0.0.1	127.0.0.1	TCP	74	42522 → 12346 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1858709689 TSecr=0 WS=128
10	0.259491111	127.0.0.1	127.0.0.1	TCP	74	12346 → 42522 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=1858709689 TSecr=1858709689 WS=128
11	0.259502611	127.0.0.1	127.0.0.1	TCP	66	42522 → 12346 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1858709689 TSecr=1858709689
12	1.001729642	127.0.0.1	127.0.0.1	TCP	66	12346 → 42508 [FIN, ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1858710431 TSecr=1858709430
13	1.001872642	127.0.0.1	127.0.0.1	TCP	66	42508 → 12346 [FIN, ACK] Seq=2 Ack=2 Win=65536 Len=0 TSval=1858710431 TSecr=1858710431
14	1.001883342	127.0.0.1	127.0.0.1	TCP	66	12346 → 42508 [ACK] Seq=2 Ack=2 Win=65536 Len=0 TSval=1858710431 TSecr=1858710431
15	1.005916242	127.0.0.1	127.0.0.1	TCP	111	12346 → 42506 [PSH, ACK] Seq=1 Ack=736 Win=65536 Len=45 TSval=1858710435 TSecr=1858709430 [TCP segment of a reassembled PDU]
16	1.005958142	127.0.0.1	127.0.0.1	TCP	66	42506 → 12346 [ACK] Seq=736 Ack=46 Win=65536 Len=0 TSval=1858710435 TSecr=1858710435
17	1.005991942	127.0.0.1	127.0.0.1	HTTP	66	HTTP/1.1 404 Not Found
18	1.006115542	127.0.0.1	127.0.0.1	TCP	66	42506 → 12346 [FIN, ACK] Seq=736 Ack=47 Win=65536 Len=0 TSval=1858710435 TSecr=1858710435
19	1.005112442	127.0.0.1	127.0.0.1	TCP	66	12346 → 42506 [ACK] Seq=47 Ack=737 Win=65536 Len=0 TSval=1858710435 TSecr=1858710435
20	2.006824585	127.0.0.1	127.0.0.1	TCP	66	12346 → 42522 [FIN, ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1858711436 TSecr=1858709689
21	2.007129985	127.0.0.1	127.0.0.1	TCP	66	42522 → 12346 [FIN, ACK] Seq=1 Ack=2 Win=65536 Len=0 TSval=1858711437 TSecr=1858711436
22	2.007156185	127.0.0.1	127.0.0.1	TCP	66	12346 → 42522 [ACK] Seq=2 Ack=2 Win=65536 Len=0 TSval=1858711437 TSecr=1858711437

בבקשה זו ביקשנו מהשרת קובץ שלא קיים, ולכן ציפינו לקבל בתור תשובה את 404 Not Found. הלקוח ביקש בקשה של קובץ not_found שלא קיים בצד השרת, שכתוצאה מכך השרת ראה שאין בצד שלו קובץ כזה ולכן החזיר את הודעת השגיאה 404. לאחר מכן, הלקוח לא ביקש בקשות נוספות ולכן החיבור הסתיים.

הרצה של /redirect :

פקטה

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	TCP	74	38828 → 12346 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1859894305 TSecr=0 WS=128
2	0.000020808	127.0.0.1	127.0.0.1	TCP	74	12346 → 38828 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=1859894305 TSecr=1859894305 WS=128
3	0.000101600	127.0.0.1	127.0.0.1	TCP	66	38828 → 12346 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1859894305 TSecr=1859894305
4	0.000191000	127.0.0.1	127.0.0.1	TCP	74	38830 → 12346 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1859894305 TSecr=0 WS=128
5	0.000335008	127.0.0.1	127.0.0.1	TCP	74	12346 → 38830 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=1859894305 TSecr=1859894305 WS=128
6	0.000335008	127.0.0.1	127.0.0.1	TCP	66	38830 → 12346 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1859894305 TSecr=1859894305
7	0.000662508	127.0.0.1	127.0.0.1	HTTP	774	GET /redirect HTTP/1.1
8	0.000662508	127.0.0.1	127.0.0.1	TCP	66	12346 → 38830 [ACK] Seq=1 Ack=709 Win=64896 Len=0 TSval=1859894306 TSecr=1859894306
9	0.263092015	127.0.0.1	127.0.0.1	TCP	74	48932 → 12346 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1859894568 TSecr=0 WS=128
10	0.263266715	127.0.0.1	127.0.0.1	TCP	74	12346 → 48932 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=1859894568 TSecr=1859894568 WS=128
11	0.263368615	127.0.0.1	127.0.0.1	TCP	66	48932 → 12346 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1859894568 TSecr=1859894568
12	1.002401275	127.0.0.1	127.0.0.1	TCP	66	12346 → 38828 [FIN, ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1859895307 TSecr=1859894305
13	1.002629875	127.0.0.1	127.0.0.1	TCP	66	38828 → 12346 [FIN, ACK] Seq=1 Ack=2 Win=65536 Len=0 TSval=1859895308 TSecr=1859895307
14	1.002635075	127.0.0.1	127.0.0.1	TCP	66	12346 → 38828 [ACK] Seq=2 Ack=2 Win=65536 Len=0 TSval=1859895308 TSecr=1859895308
15	1.003236775	127.0.0.1	127.0.0.1	TCP	143	12346 → 38830 [PSH, ACK] Seq=1 Ack=709 Win=65536 Len=77 TSval=1859895308 TSecr=1859894306 [TCP segment of a reassembled PDU]
16	1.003295975	127.0.0.1	127.0.0.1	TCP	66	38830 → 12346 [ACK] Seq=709 Ack=78 Win=65536 Len=0 TSval=1859895308 TSecr=1859895308
17	1.003329475	127.0.0.1	127.0.0.1	HTTP	66	HTTP/1.1 301 Moved Permanently
18	1.003374775	127.0.0.1	127.0.0.1	TCP	66	38830 → 12346 [FIN, ACK] Seq=709 Ack=79 Win=65536 Len=0 TSval=1859895308 TSecr=1859895308
19	1.003464075	127.0.0.1	127.0.0.1	TCP	66	12346 → 38830 [ACK] Seq=79 Ack=710 Win=65536 Len=0 TSval=1859895308 TSecr=1859895308
20	1.018598872	127.0.0.1	127.0.0.1	HTTP	777	GET /result.html HTTP/1.1
21	1.018639972	127.0.0.1	127.0.0.1	TCP	66	12346 → 48932 [ACK] Seq=1 Ack=712 Win=64896 Len=0 TSval=1859895316 TSecr=1859895316
22	1.031278666	127.0.0.1	127.0.0.1	HTTP	252	HTTP/1.1 200 OK
23	1.031269466	127.0.0.1	127.0.0.1	TCP	66	48932 → 12346 [ACK] Seq=712 Ack=187 Win=65408 Len=0 TSval=1859895336 TSecr=1859895336
24	2.032517411	127.0.0.1	127.0.0.1	TCP	66	12346 → 48932 [FIN, ACK] Seq=187 Ack=712 Win=65536 Len=0 TSval=1859896327 TSecr=1859895336
25	2.032845411	127.0.0.1	127.0.0.1	TCP	66	48932 → 12346 [FIN, ACK] Seq=712 Ack=188 Win=65536 Len=0 TSval=1859896328 TSecr=1859896327
26	2.032861411	127.0.0.1	127.0.0.1	TCP	66	12346 → 48932 [ACK] Seq=188 Ack=713 Win=65536 Len=0 TSval=1859896328 TSecr=1859896328

כפי שניתן לראות בבקשה הזו מתבצעים שני חיבורים עם השרת, מתבצעות שתי בקשות לשרת ומתקבלות שתי תשובות מהשרת ביחד עם שתי בקשות FIN. בחיבור הראשון הלקוח (דפדפן הכרום) מבקש בקשת של redirect, עבורה מוחזרת התשובה 301 Moved Permanently. ביחד עם אותה תשובה הוא מוסיף את סימן ה-FIN כדי להגיד ללקוח שהוא סיים את העבודה מהצד שלו ורוצה לסיים את התקשורת. הלקוח מתגובה מסיים את התקשורת ומיד לאחר מכן מבקש את הקובץ result.html ולכן תהליך החיבור עם השרת מתבצע מחדש והשרת שולח ללקוח את הקובץ שהוא ביקש. אנו רואים שערך ה connection היה keep-alive מפני שבבקשה השניה השרת ממשיך להאזין ורק לאחר שעוברת שניה (ניתן לראות בזמן קפיצה של מ1 שניות ל2 שניות) שולח בקשת FIN ללקוח שנענית בבקשת FIN חוזרת והחיבור נסגר.

הרצה של /index.html :

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	TCP	74	33610 → 12346 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1859540286 TSecr=0 WS=128
2	0.000018998	127.0.0.1	127.0.0.1	TCP	74	12346 → 33610 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=1859540287 TSecr=1859540286 WS=128
3	0.000033200	127.0.0.1	127.0.0.1	TCP	66	33610 → 12346 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1859540287 TSecr=1859540287
4	0.0000541900	127.0.0.1	127.0.0.1	HTTP	776	GET /index.html HTTP/1.1
5	0.000590100	127.0.0.1	127.0.0.1	TCP	66	12346 → 33610 [ACK] Seq=1 Ack=711 Win=64896 Len=0 TSval=1859540207 TSecr=1859540207
6	0.001884399	127.0.0.1	127.0.0.1	TCP	74	33612 → 12346 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1859540288 TSecr=0 WS=128
7	0.001899299	127.0.0.1	127.0.0.1	TCP	74	12346 → 33612 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=1859540288 TSecr=1859540288 WS=128
8	0.001911199	127.0.0.1	127.0.0.1	TCP	66	33612 → 12346 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1859540288 TSecr=1859540288
9	0.016768198	127.0.0.1	127.0.0.1	HTTP	298	HTTP/1.1 200 OK
10	0.016864698	127.0.0.1	127.0.0.1	TCP	66	33610 → 12346 [ACK] Seq=711 Ack=233 Win=65408 Len=0 TSval=1859540223 TSecr=1859540223
11	0.247875375	127.0.0.1	127.0.0.1	TCP	74	33624 → 12346 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1859540454 TSecr=0 WS=128
12	0.247885175	127.0.0.1	127.0.0.1	TCP	74	12346 → 33624 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=1859540454 TSecr=1859540454 WS=128
13	0.247893375	127.0.0.1	127.0.0.1	TCP	66	33624 → 12346 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1859540454 TSecr=1859540454
14	0.018065000	127.0.0.1	127.0.0.1	TCP	66	12346 → 33610 [FIN, ACK] Seq=233 Ack=711 Win=65536 Len=0 TSval=1859541225 TSecr=1859540223
15	0.018351000	127.0.0.1	127.0.0.1	TCP	66	33610 → 12346 [FIN, ACK] Seq=711 Ack=234 Win=65536 Len=0 TSval=1859541225 TSecr=1859541225
16	0.018372800	127.0.0.1	127.0.0.1	TCP	66	12346 → 33610 [ACK] Seq=234 Ack=712 Win=65536 Len=0 TSval=1859541225 TSecr=1859541225
17	0.019864103	127.0.0.1	127.0.0.1	TCP	66	12346 → 33612 [FIN, ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1859542226 TSecr=1859540208
18	0.020022803	127.0.0.1	127.0.0.1	TCP	66	33612 → 12346 [FIN, ACK] Seq=1 Ack=2 Win=65536 Len=0 TSval=1859542227 TSecr=1859542226
19	0.020035303	127.0.0.1	127.0.0.1	TCP	66	12346 → 33612 [ACK] Seq=2 Ack=2 Win=65536 Len=0 TSval=1859542227 TSecr=1859542227
20	0.021405905	127.0.0.1	127.0.0.1	TCP	66	12346 → 33624 [FIN, ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1859543228 TSecr=1859540454
21	0.021613605	127.0.0.1	127.0.0.1	TCP	66	33624 → 12346 [FIN, ACK] Seq=1 Ack=2 Win=65536 Len=0 TSval=1859543228 TSecr=1859543228
22	0.021628505	127.0.0.1	127.0.0.1	TCP	66	12346 → 33624 [ACK] Seq=2 Ack=2 Win=65536 Len=0 TSval=1859543228 TSecr=1859543228

הלקוח שולח בקשת GET לקובץ בשם index.html, מתבצע חיבור בין הלקוח לשרת והשרת מחזיר ללקוח (הדפדפן של כרום) את הקובץ אותו ביקש. כמו במקרה דומה שפירטנו פה, השרת שולח לדפדפן בקשת FIN באופן מפורש מפני שהדפדפן הכיל בבקשתו את השדה connection: keep-alive מה שגרם לשרת להשאר מחובר ורק לאחר שניה שלא קרה בה כלום השרת שלח בקשת FIN מפורשת ללקוח, הלקוח שולח בקשת FIN בחזרה והחיבור נסגר.

הרצה של /c/Footube.html :

פקטה

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	TCP	74	58174 → 12346 [SYN] Seq=0 Win=0 Len=0 MSS=65536 SACK_PERM=1 TSval=1860125282 TSecr=0 WS=128
2	0.000000000	127.0.0.1	127.0.0.1	TCP	74	58175 → 12346 [SYN] Seq=0 Win=0 Len=0 MSS=65536 SACK_PERM=1 TSval=1860125282 TSecr=0 WS=128
3	0.000026000	127.0.0.1	127.0.0.1	TCP	74	12346 → 58176 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=65536 SACK_PERM=1 TSval=1860125282 TSecr=1860125282 WS=128
4	0.000039000	127.0.0.1	127.0.0.1	TCP	66	58176 → 12346 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1860125282 TSecr=1860125282
5	0.000078300	127.0.0.1	127.0.0.1	TCP	74	12346 → 58176 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=65536 SACK_PERM=1 TSval=1860125282 TSecr=1860125282 WS=128
6	0.000096300	127.0.0.1	127.0.0.1	TCP	66	58174 → 12346 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1860125282 TSecr=1860125282
7	0.000272300	127.0.0.1	127.0.0.1	HTTP	789	GET /c/Footube.html HTTP/1.1
8	0.000577900	127.0.0.1	127.0.0.1	TCP	66	12346 → 58174 [ACK] Seq=1 Ack=715 Win=6896 Len=0 TSval=1860125282 TSecr=1860125282
9	0.251179421	127.0.0.1	127.0.0.1	TCP	74	58180 → 12346 [SYN] Seq=0 Win=0 Len=0 MSS=65536 SACK_PERM=1 TSval=1860125543 TSecr=0 WS=128
10	0.261332921	127.0.0.1	127.0.0.1	TCP	74	12346 → 58180 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=65536 SACK_PERM=1 TSval=1860125543 TSecr=1860125543 WS=128
11	0.261346521	127.0.0.1	127.0.0.1	TCP	66	58180 → 12346 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1860125543 TSecr=1860125543
12	0.001969079	127.0.0.1	127.0.0.1	TCP	66	12346 → 58176 [FIN, ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1860125282 TSecr=1860125282
13	0.002138279	127.0.0.1	127.0.0.1	TCP	66	58176 → 12346 [FIN, ACK] Seq=1 Ack=2 Win=65536 Len=0 TSval=1860126284 TSecr=1860126284
14	0.002266879	127.0.0.1	127.0.0.1	TCP	66	12346 → 58176 [ACK] Seq=2 Ack=2 Win=65536 Len=0 TSval=1860126284 TSecr=1860126284
15	0.048059302	127.0.0.1	127.0.0.1	HTTP	6336	HTTP/1.1 200 OK
16	0.048060782	127.0.0.1	127.0.0.1	TCP	66	58174 → 12346 [ACK] Seq=725 Ack=0271 Win=0 Len=0 TSval=1860126322 TSecr=1860126322
17	0.055549983	127.0.0.1	127.0.0.1	HTTP	663	GET /c/footube.css HTTP/1.1
18	0.055588763	127.0.0.1	127.0.0.1	TCP	66	12346 → 58174 [ACK] Seq=0271 Ack=1312 Win=5924 Len=0 TSval=1860126337 TSecr=1860126337
19	0.089065202	127.0.0.1	127.0.0.1	HTTP	478	HTTP/1.1 200 OK
20	0.105653682	127.0.0.1	127.0.0.1	HTTP	648	GET /c/footube.js HTTP/1.1
21	0.105654382	127.0.0.1	127.0.0.1	HTTP	787	GET /c/img/1.jpg HTTP/1.1
22	0.105930882	127.0.0.1	127.0.0.1	TCP	66	12346 → 58180 [ACK] Seq=1 Ack=642 Win=6496 Len=0 TSval=1860126388 TSecr=1860126388
23	0.121158682	127.0.0.1	127.0.0.1	HTTP	872	HTTP/1.1 200 OK
24	0.122570182	127.0.0.1	127.0.0.1	HTTP	787	GET /c/img/2.jpg HTTP/1.1
25	0.141557282	127.0.0.1	127.0.0.1	TCP	32834	12346 → 58174 [ACK] Seq=7489 Ack=2535 Win=65536 Len=32768 TSval=1860126423 TSecr=1860126404 [TCP segment of a reassembled PDU]
26	0.141577982	127.0.0.1	127.0.0.1	TCP	32834	TCP Window Full] 12346 → 58174 [PSH, ACK] Seq=40157 Ack=2535 Win=65536 Len=32768 TSval=1860126423 TSecr=1860126404 [TCP segment of a reassembled PDU]
27	0.141664882	127.0.0.1	127.0.0.1	TCP	66	58174 → 12346 [ACK] Seq=2535 Ack=7025 Win=65536 Len=0 TSval=1860126423 TSecr=1860126423
28	0.141825982	127.0.0.1	127.0.0.1	TCP	32834	12346 → 58174 [ACK] Seq=28015 Ack=2535 Win=65536 Len=32768 TSval=1860126424 TSecr=1860126423 [TCP segment of a reassembled PDU]
29	0.141931182	127.0.0.1	127.0.0.1	TCP	32834	TCP Window Full] 12346 → 58174 [PSH, ACK] Seq=100191 Ack=2535 Win=65536 Len=32768 TSval=1860126424 TSecr=1860126423 [TCP segment of a reassembled PDU]
30	0.141972482	127.0.0.1	127.0.0.1	TCP	66	58174 → 12346 [ACK] Seq=2535 Ack=185793 Win=65536 Len=0 TSval=1860126424 TSecr=1860126424
31	0.141981482	127.0.0.1	127.0.0.1	TCP	32834	TCP Window Full] 12346 → 58174 [PSH, ACK] Seq=28015 Ack=2535 Win=65536 Len=32768 TSval=1860126424 TSecr=1860126423 [TCP segment of a reassembled PDU]
32	0.141988882	127.0.0.1	127.0.0.1	TCP	66	58174 → 12346 [ACK] Seq=2535 Ack=185851 Win=65536 Len=0 TSval=1860126424 TSecr=1860126424
33	0.141994282	127.0.0.1	127.0.0.1	TCP	32834	TCP Window Full] 12346 → 58174 [PSH, ACK] Seq=71320 Ack=2535 Win=65536 Len=32768 TSval=1860126424 TSecr=1860126424 [TCP segment of a reassembled PDU]
34	0.141993882	127.0.0.1	127.0.0.1	TCP	66	58174 → 12346 [ACK] Seq=2535 Ack=171329 Win=65536 Len=0 TSval=1860126424 TSecr=1860126424
35	0.141911382	127.0.0.1	127.0.0.1	TCP	32834	12346 → 58174 [ACK] Seq=284097 Ack=2535 Win=65536 Len=32768 TSval=1860126424 TSecr=1860126424 [TCP segment of a reassembled PDU]
36	0.141914382	127.0.0.1	127.0.0.1	TCP	66	58174 → 12346 [ACK] Seq=2535 Ack=284097 Win=65536 Len=0 TSval=1860126424 TSecr=1860126424
37	0.141926382	127.0.0.1	127.0.0.1	TCP	32834	12346 → 58174 [PSH, ACK] Seq=236065 Ack=2535 Win=65536 Len=32768 TSval=1860126424 TSecr=1860126424 [TCP segment of a reassembled PDU]
38	0.141926882	127.0.0.1	127.0.0.1	TCP	66	58174 → 12346 [ACK] Seq=2535 Ack=286933 Win=65536 Len=0 TSval=1860126424 TSecr=1860126424
39	0.141929582	127.0.0.1	127.0.0.1	TCP	32834	12346 → 58174 [ACK] Seq=260633 Ack=2535 Win=65536 Len=32768 TSval=1860126424 TSecr=1860126424 [TCP segment of a reassembled PDU]
40	0.141937082	127.0.0.1	127.0.0.1	TCP	32834	12346 → 58174 [PSH, ACK] Seq=302401 Ack=2535 Win=65536 Len=32768 TSval=1860126424 TSecr=1860126424 [TCP segment of a reassembled PDU]
41	0.141941882	127.0.0.1	127.0.0.1	TCP	66	58174 → 12346 [ACK] Seq=2535 Ack=335169 Win=65536 Len=0 TSval=1860126424 TSecr=1860126424
42	0.141956882	127.0.0.1	127.0.0.1	TCP	32834	12346 → 58174 [ACK] Seq=335169 Ack=2535 Win=65536 Len=32768 TSval=1860126424 TSecr=1860126424 [TCP segment of a reassembled PDU]
43	0.141978782	127.0.0.1	127.0.0.1	TCP	32834	12346 → 58174 [PSH, ACK] Seq=367937 Ack=2535 Win=65536 Len=32768 TSval=1860126424 TSecr=1860126424 [TCP segment of a reassembled PDU]

* Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface lo, id 0
* Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
* Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
* Transmission Control Protocol, Src Port: 58174, Dst Port: 12346, Seq: 0, Len: 0

No.	Time	Source	Destination	Protocol	Length	Info
43	1.14197872	127.0.0.1	127.0.0.1	TCP	32834	12346 - 58374 [ACK] Seq=367937 Ack=2535 Win=65536 Len=32768 TSval=1860126424 TSecr=1860126424 [TCP segment of a reassembled PDU]
44	1.14198392	127.0.0.1	127.0.0.1	TCP	66	58374 - 12346 [ACK] Seq=2535 Ack=400705 Win=111334 Len=0 TSval=1860126424 TSecr=1860126424
45	1.14198602	127.0.0.1	127.0.0.1	TCP	32834	12346 - 58374 [ACK] Seq=460785 Ack=2535 Win=65536 Len=32768 TSval=1860126424 TSecr=1860126424 [TCP segment of a reassembled PDU]
46	1.14198802	127.0.0.1	127.0.0.1	TCP	32834	12346 - 58374 [ACK] Seq=43473 Ack=2535 Win=65536 Len=32768 TSval=1860126424 TSecr=1860126424 [TCP segment of a reassembled PDU]
47	1.14200132	127.0.0.1	127.0.0.1	TCP	66	58374 - 12346 [ACK] Seq=2535 Ack=466241 Win=1375232 Len=0 TSval=1860126424 TSecr=1860126424
48	1.14200992	127.0.0.1	127.0.0.1	TCP	32834	12346 - 58374 [ACK] Seq=460241 Ack=2535 Win=65536 Len=32768 TSval=1860126424 TSecr=1860126424 [TCP segment of a reassembled PDU]
49	1.18227521	127.0.0.1	127.0.0.1	TCP	66	58374 - 12346 [ACK] Seq=2535 Ack=499009 Win=1506176 Len=0 TSval=1860126464 TSecr=1860126424
50	1.18235181	127.0.0.1	127.0.0.1	HTTP	40936	HTTP/1.1 200 OK (JPEG JFIF image)
51	1.18243951	127.0.0.1	127.0.0.1	TCP	66	58374 - 12346 [ACK] Seq=2535 Ack=530479 Win=1637128 Len=0 TSval=1860126464 TSecr=1860126464
52	1.18607481	127.0.0.1	127.0.0.1	HTTP	767	GET /c/img/3.jpg HTTP/1.1
53	1.21653250	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=539479 Ack=3176 Win=65536 Len=65483 TSval=1860126500 TSecr=1860126468 [TCP segment of a reassembled PDU]
54	1.21663200	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=494982 Ack=3176 Win=65536 Len=65483 TSval=1860126500 TSecr=1860126468 [TCP segment of a reassembled PDU]
55	1.21665100	127.0.0.1	127.0.0.1	TCP	66	58374 - 12346 [ACK] Seq=3176 Ack=570445 Win=1899136 Len=0 TSval=1860126500 TSecr=1860126500
56	1.21665900	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=678445 Ack=3176 Win=65536 Len=65483 TSval=1860126500 TSecr=1860126500 [TCP segment of a reassembled PDU]
57	1.21668370	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=755928 Ack=3176 Win=65536 Len=65483 TSval=1860126500 TSecr=1860126468 [TCP segment of a reassembled PDU]
58	1.21669430	127.0.0.1	127.0.0.1	TCP	66	58374 - 12346 [ACK] Seq=3176 Ack=801411 Win=2161824 Len=0 TSval=1860126500 TSecr=1860126500
59	1.21671450	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=480141 Ack=3176 Win=65536 Len=65483 TSval=1860126500 TSecr=1860126468 [TCP segment of a reassembled PDU]
60	1.21674120	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=866894 Ack=3176 Win=65536 Len=65483 TSval=1860126500 TSecr=1860126468 [TCP segment of a reassembled PDU]
61	1.21674780	127.0.0.1	127.0.0.1	TCP	66	58374 - 12346 [ACK] Seq=3176 Ack=932377 Win=2422656 Len=0 TSval=1860126500 TSecr=1860126500
62	1.21677230	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=932377 Ack=3176 Win=65536 Len=65483 TSval=1860126500 TSecr=1860126468 [TCP segment of a reassembled PDU]
63	1.21680610	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=990760 Ack=3176 Win=65536 Len=65483 TSval=1860126501 TSecr=1860126468 [TCP segment of a reassembled PDU]
64	1.21681350	127.0.0.1	127.0.0.1	HTTP	8192	HTTP/1.1 200 OK (JPEG JFIF image)
65	1.21930750	127.0.0.1	127.0.0.1	TCP	66	58374 - 12346 [ACK] Seq=3176 Ack=1071460 Win=2422656 Len=0 TSval=1860126581 TSecr=1860126580
66	1.22257380	127.0.0.1	127.0.0.1	HTTP	767	GET /c/img/4.jpg HTTP/1.1
67	1.24361880	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=1071460 Ack=3817 Win=65536 Len=65483 TSval=1860126525 TSecr=1860126584 [TCP segment of a reassembled PDU]
68	1.24366190	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=136952 Ack=3817 Win=65536 Len=65483 TSval=1860126525 TSecr=1860126584 [TCP segment of a reassembled PDU]
69	1.24367870	127.0.0.1	127.0.0.1	TCP	66	58374 - 12346 [ACK] Seq=3817 Ack=1202435 Win=2422656 Len=0 TSval=1860126525 TSecr=1860126525
70	1.24368740	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=1224245 Ack=3817 Win=65536 Len=65483 TSval=1860126525 TSecr=1860126584 [TCP segment of a reassembled PDU]
71	1.24370780	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=122719 Ack=3817 Win=65536 Len=65483 TSval=1860126525 TSecr=1860126584 [TCP segment of a reassembled PDU]
72	1.24371430	127.0.0.1	127.0.0.1	TCP	66	58374 - 12346 [ACK] Seq=3817 Ack=1333401 Win=2717952 Len=0 TSval=1860126525 TSecr=1860126525
73	1.24373480	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=1335481 Ack=3817 Win=65536 Len=65483 TSval=1860126525 TSecr=1860126584 [TCP segment of a reassembled PDU]
74	1.24375150	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=1398884 Ack=3817 Win=65536 Len=65483 TSval=1860126525 TSecr=1860126584 [TCP segment of a reassembled PDU]
75	1.24376100	127.0.0.1	127.0.0.1	TCP	66	58374 - 12346 [ACK] Seq=3817 Ack=1464367 Win=2422656 Len=0 TSval=1860126525 TSecr=1860126525
76	1.24378140	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=1464367 Ack=3817 Win=65536 Len=65483 TSval=1860126525 TSecr=1860126584 [TCP segment of a reassembled PDU]
77	1.24380960	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=1529850 Ack=3817 Win=65536 Len=65483 TSval=1860126526 TSecr=1860126584 [TCP segment of a reassembled PDU]
78	1.24381660	127.0.0.1	127.0.0.1	TCP	66	58374 - 12346 [ACK] Seq=3817 Ack=1595335 Win=3012224 Len=0 TSval=1860126526 TSecr=1860126525
79	1.24382400	127.0.0.1	127.0.0.1	HTTP	8192	HTTP/1.1 200 OK (JPEG JFIF image)
80	1.24681470	127.0.0.1	127.0.0.1	HTTP	767	GET /c/img/5.jpg HTTP/1.1
81	1.29233979	127.0.0.1	127.0.0.1	TCP	66	12346 - 58374 [ACK] Seq=1683459 Ack=458 Win=65536 Len=0 TSval=1860126574 TSecr=1860126528
82	1.29513789	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=1683459 Ack=458 Win=65536 Len=65483 TSval=1860126577 TSecr=1860126528 [TCP segment of a reassembled PDU]
83	1.29524599	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=168942 Ack=458 Win=65536 Len=65483 TSval=1860126577 TSecr=1860126528 [TCP segment of a reassembled PDU]
84	1.29525759	127.0.0.1	127.0.0.1	TCP	66	58374 - 12346 [ACK] Seq=458 Ack=1734425 Win=3112448 Len=0 TSval=1860126577 TSecr=1860126528 [TCP segment of a reassembled PDU]
85	1.29528579	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=1734425 Ack=458 Win=65536 Len=65483 TSval=1860126577 TSecr=1860126528 [TCP segment of a reassembled PDU]

* Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface lo, id 0
 * Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
 * Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
 * Transmission Control Protocol, Src Port: 58374, Dst Port: 12346, Seq: 0, Len: 0

No.	Time	Source	Destination	Protocol	Length	Info
85	1.29529879	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=1734425 Ack=458 Win=65536 Len=65483 TSval=1860126577 TSecr=1860126528 [TCP segment of a reassembled PDU]
86	1.29530719	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=1799908 Ack=458 Win=65536 Len=65483 TSval=1860126577 TSecr=1860126528 [TCP segment of a reassembled PDU]
87	1.29537879	127.0.0.1	127.0.0.1	TCP	66	58374 - 12346 [ACK] Seq=458 Ack=1805191 Win=3112448 Len=0 TSval=1860126577 TSecr=1860126577
88	1.29544370	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=1805191 Ack=458 Win=65536 Len=65483 TSval=1860126577 TSecr=1860126528 [TCP segment of a reassembled PDU]
89	1.29549109	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=1908874 Ack=458 Win=65536 Len=65483 TSval=1860126577 TSecr=1860126528 [TCP segment of a reassembled PDU]
90	1.29549879	127.0.0.1	127.0.0.1	TCP	66	58374 - 12346 [ACK] Seq=458 Ack=1908757 Win=3112448 Len=0 TSval=1860126577 TSecr=1860126577
91	1.29553709	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=1908317 Ack=458 Win=65536 Len=65483 TSval=1860126577 TSecr=1860126528 [TCP segment of a reassembled PDU]
92	1.29555979	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=2061840 Ack=458 Win=65536 Len=65483 TSval=1860126577 TSecr=1860126528 [TCP segment of a reassembled PDU]
93	1.29557189	127.0.0.1	127.0.0.1	HTTP	8192	HTTP/1.1 200 OK (JPEG JFIF image)
94	1.29560470	127.0.0.1	127.0.0.1	TCP	66	58374 - 12346 [ACK] Seq=458 Ack=2135449 Win=3112448 Len=0 TSval=1860126577 TSecr=1860126577
95	1.30064970	127.0.0.1	127.0.0.1	HTTP	767	GET /c/img/6.jpg HTTP/1.1
96	1.32606270	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=2135449 Ack=5099 Win=65536 Len=65483 TSval=1860126600 TSecr=1860126582 [TCP segment of a reassembled PDU]
97	1.32613407	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=2208932 Ack=5099 Win=65536 Len=65483 TSval=1860126600 TSecr=1860126582 [TCP segment of a reassembled PDU]
98	1.32615710	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=2268415 Ack=5099 Win=65536 Len=65483 TSval=1860126600 TSecr=1860126582 [TCP segment of a reassembled PDU]
99	1.32618270	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=2316615 Ack=5099 Win=65536 Len=65483 TSval=1860126600 TSecr=1860126582 [TCP segment of a reassembled PDU]
100	1.32620670	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=2373811 Ack=5099 Win=65536 Len=65483 TSval=1860126600 TSecr=1860126582 [TCP segment of a reassembled PDU]
101	1.32621970	127.0.0.1	127.0.0.1	TCP	66	58374 - 12346 [ACK] Seq=5099 Ack=2397381 Win=3045342 Len=0 TSval=1860126600 TSecr=1860126600
102	1.32624670	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=2397381 Ack=5099 Win=65536 Len=65483 TSval=1860126600 TSecr=1860126582 [TCP segment of a reassembled PDU]
103	1.32628870	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=2528247 Ack=5099 Win=65536 Len=65483 TSval=1860126600 TSecr=1860126582 [TCP segment of a reassembled PDU]
104	1.32631070	127.0.0.1	127.0.0.1	TCP	65549	12346 - 58374 [ACK] Seq=2593830 Ack=5099 Win=65536 Len=65483 TSval=1860126600 TSecr=1860126582 [TCP segment of a reassembled PDU]
105	1.32632470	127.0.0.1	127.0.0.1	HTTP	8192	HTTP/1.1 200 OK (JPEG JFIF image)
106	1.32640570	127.0.0.1	127.0.0.1	TCP	66	58374 - 12346 [ACK] Seq=5099 Ack=3007619 Win=3007616 Len=0 TSval=1860126600 TSecr=1860126600
107	1.40815477	127.0.0.1	127.0.0.1	TCP	74	58002 - 12346 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1860126690 TSecr=0 WS=128
108	1.40816177	127.0.0.1	127.0.0.1	TCP	74	12346 - 58002 [ACK] Seq=0 Ack=1 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1860126690 TSecr=1860126690 WS=128
109	1.40817777	127.0.0.1	127.0.0.1	TCP	66	58002 - 12346 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1860126690 TSecr=1860126690
110	1.40818477	127.0.0.1	127.0.0.1	TCP	74	58002 - 12346 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1860126690 TSecr=0 WS=128
111	1.40819277	127.0.0.1	127.0.0.1	TCP	74	12346 - 58002 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1860126690 TSecr=1860126690
112	1.40819777	127.0.0.1	127.0.0.1	TCP	66	58002 - 12346 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1860126690 TSecr=1860126690
113	1.40820777	127.0.0.1	127.0.0.1	TCP	74	12346 - 58002 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1860126690 TSecr=0 WS=128
114	1.40821577	127.0.0.1	127.0.0.1	TCP	74	12346 - 58002 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1860126690 TSecr=1860126690
115	1.40821577	127.0.0.1	127.0.0.1	TCP	66	58002 - 12346 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1860126690 TSecr=1860126690
116	1.40821577	127.0.0.1	127.0.0.1	TCP	74	58002 - 12346 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1860126690 TSecr=0 WS=128
117	1.40821577	127.0.0.1	127.0.0.1	TCP	74	12346 - 58002 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1860126690 TSecr=1860126690
118	1.40821577	127.0.0.1	127.0.0.1	TCP	66	58002 - 12346 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1860126690 TSecr=1860126690
119	1.40821577	127.0.0.1	127.0.0.1	TCP	74	12346 - 58002 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1860126690 TSecr=0 WS=128
120	1.40821577	127.0.0.1	127.0.0.1	TCP	66	58002 - 12346 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1860126690 TSecr=1860126690
121	1.40821577	127.0.0.1	127.0.0.1	TCP	74	12346 - 58002 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1860126690 TSecr=0 WS=128
122	1.40821577	127.0.0.1	127.0.0.1	TCP	66	58002 - 12346 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1860126690 TSecr=1860126690
123	1.40821577	127.0.0.1	127.0.0.1	TCP	74	12346 - 58002 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1860126690 TSecr=0 WS=128
124	1.40821577	127.0.0.1	127.0.0.1	TCP	66	58002 - 12346 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1860126690 TSecr=1860126690
125	1.40821577	127.0.0.1	127.0.0.1	TCP	74	12346 - 58002 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1860126690 TSecr=0 WS=128
126	1.40821577	127.0.0.1	127.0.0.1	TCP	66	58002 - 12346 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1860126690 TSecr=1860126690

164	5.353201606	127.0.0.1	127.0.0.1	TCP	66	12346 → 58418 [ACK] Seq=2 Ack=2 Win=65536 Len=0 TSval=1860130635 TSecr=1860130635
165	6.354372388	127.0.0.1	127.0.0.1	TCP	66	12346 → 58426 [FIN, ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1860131636 TSecr=1860126691
166	6.354541688	127.0.0.1	127.0.0.1	TCP	66	58426 → 12346 [FIN, ACK] Seq=1 Ack=2 Win=65536 Len=0 TSval=1860131636 TSecr=1860131636
167	6.354554008	127.0.0.1	127.0.0.1	TCP	66	12346 → 58426 [ACK] Seq=2 Ack=2 Win=65536 Len=0 TSval=1860131636 TSecr=1860131636
168	7.355760776	127.0.0.1	127.0.0.1	TCP	66	12346 → 58442 [FIN, ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1860132637 TSecr=1860126691
169	7.355941976	127.0.0.1	127.0.0.1	TCP	66	58442 → 12346 [FIN, ACK] Seq=1 Ack=2 Win=65536 Len=0 TSval=1860132638 TSecr=1860132637
170	7.355954076	127.0.0.1	127.0.0.1	TCP	66	12346 → 58442 [ACK] Seq=2 Ack=2 Win=65536 Len=0 TSval=1860132638 TSecr=1860132638

▶ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface lo, id 0
 ▶ Ethernet II, Src: 08:00:00:00:00:00 (08:00:00:00:00:00), Dst: 08:00:00:00:00:00 (08:00:00:00:00:00)
 ▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
 ▶ Transmission Control Protocol, Src Port: 58374, Dst Port: 12346, Seq: 0, Len: 0

גם במקרה הזה אנו רואים שיש חיבורים רבים לשרת מפני שבתוך דף ה html שביקשנו יש בקשות רבות לקבצים אחרים כגון תמונות, קבצי JS CSS ועוד, לכן באופן דומה לקובץ html האחר שפתחנו השרת פותח מספר חיבורים במקביל כדי לחסוך בזמן שלוקח לו להחזיר את התשובה למשתמש ובכל בקשה כזו הוא מעביר ללקוח את אחד הקבצים הקשורים לקובץ html. ניתן לראות שהצד הלקוח מתמלא (אפילו כמה פעמים) ולכן לא ממשיך לקבל בקשות עד לקבל ACK שלאחריה הוא ממשיך. עבור כל חבילה כזו שנשלחת ניתן לראות את הACKים העוברים מהלקוח כדי להודיע לשרת שהקבצים הגיעו. אפשר לראות גם פאקטות שמתחלקות לחלקים מפני שהן גדולות מהMSS (משהו ששכיח בהעברת תמונות שהן בדרך כלל כבדות, ויותר כבדות ממחרוזות ומקבצי טקסט) ולכן הן נשלחות בחלקים ולא בבת אחת. לאחר שכל הקבצים עברו ניתן לראות שליחת הFINים הדדיים בין השרת ללקוח בכל החיבורים והחיבורים מסתיימים.