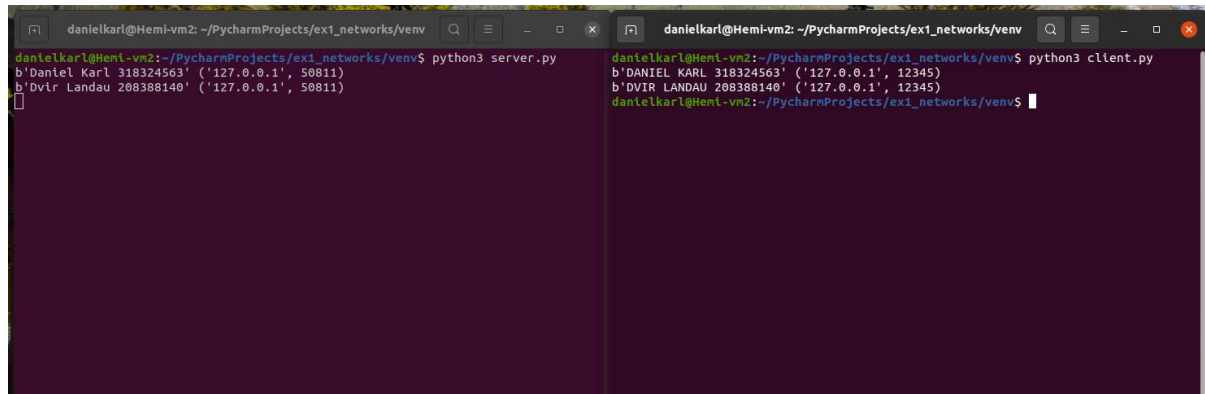


שמות המגישים: דניאל מאיר קרל 318324563

דביר לנדאו 208388140

חלק א

1. להלן ההתקשרות בין השרת ללקוח כאשר צד שמאל זהו השרת ומצד ימין זהו הלקוח. ניתן לראות כי השרת מקבל בחזרה את שמות המגישים ותעודות הזהות שלהם באותיות גדולות, כפי שהתקבל מן השרת. בנוסף, ניתן לראות שצד השרת הדפיס את ההודעה שקיבל מהלקוח ואת תשובת ה־קו והפורט של הלקוח שהתחבר אליו.



```
danielkarl@Hemi-vm2: ~/PycharmProjects/ex1_networks/venv$ python3 server.py
b'Daniel Karl 318324563' ('127.0.0.1', 50811)
b'Dvir Landau 208388140' ('127.0.0.1', 50811)

danielkarl@Hemi-vm2: ~/PycharmProjects/ex1_networks/venv$ python3 client.py
b'DANIEL KARL 318324563' ('127.0.0.1', 12345)
b'DVIR LANDAU 208388140' ('127.0.0.1', 12345)
danielkarl@Hemi-vm2: ~/PycharmProjects/ex1_networks/venv$
```

2. מצ"ב קובץ trace1 ובו קובץ שבו מפורטות החבילות שהלקוח שלח לשרת והשרת שלח ללקוח. סינונו את החבילות באמצעות הסינון "udp && udp.port==12345" בעזרת סינון זה נוכל לראות רק את החבילות שנשלחו ע"י UDP ובנוסף שפורט השולח/נשלח הוא 12345. (יש לשים לב שמכיוון שהתקשורת כאן היא מקומית – דהיינו בתוך אותו ip של 127.0.0.1 אז כל החבילות נשלחו דרך כרטיס הרשת LOOPBACK שאחראי על התקשורת בתוך הרשת עצמה)
  3. בקוד השרת כאשר הוא עושה bind הוא קובע באיזה פורט הוא מאזין. מכיוון שהגדרנו שהוא עושה bind לפורט 12345, אז מי שירצה לפנות אליו יהיה חייב לציין את מס פורט זה. בניגוד לכך, בקוד הלקוח אין כלל פעולת bind ולכן מערכת ההפעלה תבחר מס פורט אקראי עבור הקליינט. בנוסף, קוד הלקוח מציין ב sendto את מס הפורט ומס ה־IP של השרת.
- ב Wireshark מס הפורט המקור ומס פורט היעד מצוין בכל חבילה ב User Datagram Protocol. זהו בעצם הייצוג של שכבת התעבורה שבה מצוין מאיזה פורט הגיעה החבילה, ולאיזה פורט החבילה מיועדת. להלן צילום מסך לכך:

| No. | Time        | Source    | Destination | Protocol | Length | Info                 |
|-----|-------------|-----------|-------------|----------|--------|----------------------|
| 1   | 0.000000000 | 127.0.0.1 | 127.0.0.1   | UDP      | 63     | 50811 → 12345 Len=21 |
| 2   | 0.000141417 | 127.0.0.1 | 127.0.0.1   | UDP      | 63     | 12345 → 50811 Len=21 |
| 3   | 0.000218913 | 127.0.0.1 | 127.0.0.1   | UDP      | 63     | 50811 → 12345 Len=21 |
| 4   | 0.000258496 | 127.0.0.1 | 127.0.0.1   | UDP      | 63     | 12345 → 50811 Len=21 |

```
Frame 1: 63 bytes on wire (504 bits), 63 bytes captured (504 bits) on interface lo, id
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
User Datagram Protocol, Src Port: 50811, Dst Port: 12345
Source Port: 50811
Destination Port: 12345
Length: 29
Checksum: 0xfe30 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
UDP payload (21 bytes)
Data (21 bytes)
```

שכבת התעבורה.  
מצוין בה הפורטים  
של היעד ושל המקור



4. ניתן לראות ב wireshark כי כתובת ה IP של הלקוח והשרת היא זהה (127.0.0.1). דבר זה מוגדר ב Internet Protocol Version 4, כך שניתן לראות מאיזו IP נשלחה החבילה, ולאיזה IP החבילה נועדה. נשים לב, שכתובות ה IP נמצאות בשכבת הרשת. בנוסף, ניתן לראות לפי פקודת ifconfig כתובת ה IP של כרטיס הרשת עבור LOOPBACK הינו 127.0.0.1, ואילו כתובת ה IP עבור כרטיס הרשת הוא 10.0.2.4 מכיוון שהתקשורת היא פנימית אז ב wireshark יופיעו רק כתובות ה local host להלן צילום מסך:

| No. | Time        | Source    | Destination | Protocol | Length | Info                 |
|-----|-------------|-----------|-------------|----------|--------|----------------------|
| 1   | 0.000000000 | 127.0.0.1 | 127.0.0.1   | UDP      | 63     | 50811 → 12345 Len=21 |
| 2   | 0.000141417 | 127.0.0.1 | 127.0.0.1   | UDP      | 63     | 12345 → 50811 Len=21 |
| 3   | 0.000218913 | 127.0.0.1 | 127.0.0.1   | UDP      | 63     | 50811 → 12345 Len=21 |
| 4   | 0.000258496 | 127.0.0.1 | 127.0.0.1   | UDP      | 63     | 12345 → 50811 Len=21 |

### שכבת הרשת.

Contains the source and destination ip



```
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
  0100 ... = Version: 4
  ... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 49
  Identification: 0x7fe5 (32741)
  Flags: 0x40, Don't fragment
  ... 0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header checksum: 0xbcd4 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 127.0.0.1
  Destination Address: 127.0.0.1
  User Datagram Protocol, Src Port: 50811, Dst Port: 12345
  Data (21 bytes)

danielkarl@Heni-vm2:~/PycharmProjects/ex1_networks/venv$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.4 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::73f8:e11d:7cd5:4361 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:33:49:2a txqueuelen 1000 (Ethernet)
    RX packets 4149 bytes 5038142 (5.0 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2574 bytes 242156 (242.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 426 bytes 36794 (36.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 426 bytes 36794 (36.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

danielkarl@Heni-vm2:~/PycharmProjects/ex1_networks/venv$
```

## חלק ב'

מגישים: דניאל מאיר קרל 318324563, דביר לנדאו 208388140

נראה שלוש חבילות מתעבורת השרת והלקוחות:

1) הצטרפות של לקוח בשם dvir לקבוצה ע"י הפקודה 1 בצירוף שמו:

The image shows a Wireshark packet capture of a network traffic. The top pane displays a list of captured packets, with packet 57 selected. The middle pane shows the details of packet 57, which is a User Datagram Protocol (UDP) packet. The packet is from source 127.0.0.1:37584 to destination 127.0.0.1:12345. The bottom pane shows the raw data of the packet, which is a hexadecimal string representing the message 'dvir'.

| No. | Time          | Source    | Destination | Protocol  | Length | Info                 |
|-----|---------------|-----------|-------------|-----------|--------|----------------------|
| 57  | 233.400395396 | 127.0.0.1 | 127.0.0.1   | UDP       | 48     | 37584 → 12345 Len=6  |
| 58  | 233.400633145 | 127.0.0.1 | 127.0.0.1   | UDP       | 42     | 12345 → 37584 Len=0  |
| 59  | 242.092417066 | 127.0.0.1 | 127.0.0.1   | UDP       | 50     | 33710 → 12345 Len=8  |
| 60  | 242.092677039 | 127.0.0.1 | 127.0.0.1   | UDP       | 46     | 12345 → 33710 Len=4  |
| 61  | 261.506108740 | 127.0.0.1 | 127.0.0.1   | UDP       | 53     | 37584 → 12345 Len=11 |
| 62  | 261.506361313 | 127.0.0.1 | 127.0.0.1   | UDP       | 59     | 12345 → 37584 Len=17 |
| 64  | 275.038340763 | 127.0.0.1 | 127.0.0.1   | UDP       | 55     | 33710 → 12345 Len=13 |
| 65  | 275.038726333 | 127.0.0.1 | 127.0.0.1   | UDP       | 57     | 12345 → 33710 Len=15 |
| 66  | 285.375790435 | 127.0.0.1 | 127.0.0.1   | UDP       | 47     | 33710 → 12345 Len=5  |
| 67  | 285.376141069 | 127.0.0.1 | 127.0.0.1   | UDP       | 42     | 12345 → 33710 Len=0  |
| 68  | 293.167212884 | 127.0.0.1 | 127.0.0.1   | UDP       | 45     | 37584 → 12345 Len=3  |
| 69  | 293.167610529 | 127.0.0.1 | 127.0.0.1   | UDP       | 57     | 12345 → 37584 Len=15 |
| 70  | 302.960265143 | 127.0.0.1 | 127.0.0.1   | UDP       | 43     | 37584 → 12345 Len=1  |
| 71  | 302.960372313 | 127.0.0.1 | 127.0.0.1   | UDP       | 92     | 12345 → 37584 Len=50 |
| 72  | 319.610590600 | 127.0.0.1 | 127.0.0.1   | UDP       | 43     | 33710 → 12345 Len=1  |
| 73  | 327.610302237 | 127.0.0.1 | 127.0.0.1   | UDP       | 43     | 37584 → 12345 Len=1  |
| 74  | 327.610411431 | 127.0.0.1 | 127.0.0.1   | ADwin ... | 64     |                      |
| 75  | 333.331830735 | 127.0.0.1 | 127.0.0.1   | UDP       | 43     | 37584 → 12345 Len=1  |

Details of packet 57:

- 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)
- Destination: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Source: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Address: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Type: IPv4 (0x0000)
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
- User Datagram Protocol, Src Port: 37584, Dst Port: 12345
- Source Port: 37584
- Destination Port: 12345
- Length: 14
- Checksum: 0xfe21 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 7]
- [Timestamps]
- Data (6 bytes): 312064766972

Raw data (hex): 0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 ...E-  
0010 00 22 db 10 40 00 00 11 61 b8 7f 00 00 01 7f 00 ..."-@. a:.....  
0020 00 01 92 d0 30 39 00 0e fe 21 31 20 64 76 69 72 ...-09- :!1 dvir

ניתן לראות בחלק העליון של המסך את החבילה המסומנת כאשר התקשורת מתבצעת בפרוטוקול UDP מהלקוח הראשון שהפורט שלו 37584 לשרת בפורט 12345, בחלק האמצעי ניתן לראות את הפרטים על שכבות התעבורה והרשת בהן כתובות המקור והיעד, כאשר בחלק התחתון ניתן לראות את תוכן ההודעה שהלקוח מעביר לשרת, במקרה שלנו **dvir 1**.

2) שליחת הודעה מהלקוח dvir בפורט 37584 לשאר חברי הקבוצה ע"י הפקודה 2 כאשר תוכן

ההודעה הוא: "from dvir" ניתן לראות בתמונה המצורפת בעמוד הבא את החבילה המסומנת בה הלקוח dvir משתמש בפקודה 2 ולאחריה שולח את ההודעה "from dvir", גם כאן ניתן לראות את פרטי המקור והיעד גם בשכבת התעבורה בה נראה את הפורטים של השרת (12345) והלקוח (37584) וגם בשכבת הרשת בה נראה את כתובות ה-IP שבמקרה שלנו שתיהן קבועות כ- 127.0.0.1 כיוון שכל תעבורת הרשת במקרה שלנו היא מקומית.

בתחתית המסך ניתן לראות את תוכן ההודעה.

נראה את שליחת ההודעה שהתקבלה בשרת ממנו אל שאר החברים בקבוצה, במקרה שלנו משתתף שני בשם daniel:

|    |               |           |           |           |    |               |        |
|----|---------------|-----------|-----------|-----------|----|---------------|--------|
| 58 | 233.400633145 | 127.0.0.1 | 127.0.0.1 | UDP       | 42 | 12345 → 37584 | Len=0  |
| 59 | 242.092417066 | 127.0.0.1 | 127.0.0.1 | UDP       | 50 | 33710 → 12345 | Len=8  |
| 60 | 242.092677039 | 127.0.0.1 | 127.0.0.1 | UDP       | 46 | 12345 → 33710 | Len=4  |
| 61 | 261.506108740 | 127.0.0.1 | 127.0.0.1 | UDP       | 53 | 37584 → 12345 | Len=11 |
| 62 | 261.506361313 | 127.0.0.1 | 127.0.0.1 | UDP       | 59 | 12345 → 37584 | Len=17 |
| 64 | 275.038340763 | 127.0.0.1 | 127.0.0.1 | UDP       | 55 | 33710 → 12345 | Len=13 |
| 65 | 275.038726333 | 127.0.0.1 | 127.0.0.1 | UDP       | 57 | 12345 → 33710 | Len=15 |
| 66 | 285.375790435 | 127.0.0.1 | 127.0.0.1 | UDP       | 47 | 33710 → 12345 | Len=5  |
| 67 | 285.376141069 | 127.0.0.1 | 127.0.0.1 | UDP       | 42 | 12345 → 33710 | Len=0  |
| 68 | 293.167212884 | 127.0.0.1 | 127.0.0.1 | UDP       | 45 | 37584 → 12345 | Len=3  |
| 69 | 293.167610529 | 127.0.0.1 | 127.0.0.1 | UDP       | 57 | 12345 → 37584 | Len=15 |
| 70 | 302.960265143 | 127.0.0.1 | 127.0.0.1 | UDP       | 43 | 37584 → 12345 | Len=1  |
| 71 | 302.960372313 | 127.0.0.1 | 127.0.0.1 | UDP       | 92 | 12345 → 37584 | Len=50 |
| 72 | 319.610059060 | 127.0.0.1 | 127.0.0.1 | UDP       | 43 | 33710 → 12345 | Len=1  |
| 73 | 327.610302237 | 127.0.0.1 | 127.0.0.1 | UDP       | 43 | 37584 → 12345 | Len=1  |
| 74 | 327.610411431 | 127.0.0.1 | 127.0.0.1 | ADwin ... | 64 |               |        |
| 75 | 333.331830735 | 127.0.0.1 | 127.0.0.1 | UDP       | 43 | 37584 → 12345 | Len=1  |

|   |   |
|---|---|
| Frame Length: 53 bytes (424 bits)   |   |
| Capture Length: 53 bytes (424 bits)   |   |
| [Frame is marked: False]  |   |
| [Frame is ignored: False]   |   |
| [Protocols in Frame: eth:ethertype:ip:udp:data]   |   |
| [Coloring Rule Name: UDP]   |   |
| [Coloring Rule String: udp]   |   |
| ▼ 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) |   |
| ▼ Destination: 00:00:00:00:00:00 (00:00:00:00:00:00)  |   |
| Address: 00:00:00:00:00:00 (00:00:00:00:00:00)  |   |
| .....0..... = LG bit: Globally unique address (factory default)                                       |   |
| .....0..... = IG bit: Individual address (unicast)  |   |
| ▼ Source: 00:00:00:00:00:00 (00:00:00:00:00:00)   |   |
| Address: 00:00:00:00:00:00 (00:00:00:00:00:00)  |   |
| .....0..... = LG bit: Globally unique address (factory default)                                       |   |
| .....0..... = IG bit: Individual address (unicast)  |   |
| Type: IPv4 (0x0800)   |   |
| ► Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1   |   |
| ▼ User Datagram Protocol, Src Port: 37584, Dst Port: 12345  |   |
| Source Port: 37584  |   |
| Destination Port: 12345   |   |
| Length: 19  |   |
| Checksum: 0xfe26 [unverified]   |   |
| [Checksum Status: Unverified]   |   |
| [Stream index: 7]   |   |
| ► [Timestamps]  |   |
| ▼ Data (11 bytes)   |   |
| Data: 322066726f6d2064766972  |   |
| [Length: 11]  |   |
| 0000  | 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 .....E:     |
| 0010  | 00 27 e8 03 40 00 40 11 54 c0 7f 00 00 01 7f 00 ...@.T..... |
| 0020  | 00 01 92 d0 30 39 00 13 fe 26 32 20 66 72 6f 60 ....&2 from |
| 0030  | 20 64 76 69 72 dvir   |

|    |               |           |           |     |    |               |        |
|----|---------------|-----------|-----------|-----|----|---------------|--------|
| 61 | 261.506108740 | 127.0.0.1 | 127.0.0.1 | UDP | 53 | 37584 → 12345 | Len=11 |
| 62 | 261.506361313 | 127.0.0.1 | 127.0.0.1 | UDP | 59 | 12345 → 37584 | Len=17 |
| 64 | 275.038340763 | 127.0.0.1 | 127.0.0.1 | UDP | 55 | 33710 → 12345 | Len=13 |
| 65 | 275.038726333 | 127.0.0.1 | 127.0.0.1 | UDP | 57 | 12345 → 33710 | Len=15 |
| 66 | 285.375790435 | 127.0.0.1 | 127.0.0.1 | UDP | 47 | 33710 → 12345 | Len=5  |
| 67 | 285.376141069 | 127.0.0.1 | 127.0.0.1 | UDP | 42 | 12345 → 33710 | Len=0  |
| 68 | 293.167212884 | 127.0.0.1 | 127.0.0.1 | UDP | 45 | 37584 → 12345 | Len=3  |
| 69 | 293.167610529 | 127.0.0.1 | 127.0.0.1 | UDP | 57 | 12345 → 37584 | Len=15 |
| 70 | 302.960265143 | 127.0.0.1 | 127.0.0.1 | UDP | 43 | 37584 → 12345 | Len=1  |
| 71 | 302.960372313 | 127.0.0.1 | 127.0.0.1 | UDP | 92 | 12345 → 37584 | Len=50 |

ניתן לראות בחבילה המסומנת הודעה מפורט 12345 כלומר השרת לפורט 33710 שזהו הפורט של הקליינט daniel .

|   |  |
|---|--|
| [Coloring Rule Name: UDP]   |  |
| [Coloring Rule String: udp]   |  |
| 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   |  |
| User Datagram Protocol, Src Port: 12345, Dst Port: 33710  |  |
| Source Port: 12345  |  |
| Destination Port: 33710   |  |
| Length: 23  |  |
| Checksum: 0xfe2a [unverified]   |  |
| [Checksum Status: Unverified]   |  |
| [Stream index: 8]   |  |
| ► [Timestamps]  |  |
| Data (15 bytes)   |  |
| Data: 647669723a2066726f6d2064766972  |  |
| 300   | 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 .....E:      |
| 310   | 00 2b f2 13 40 00 40 11 4a ac 7f 00 00 01 7f 00 ...+@.J..... |
| 320   | 00 01 30 39 83 ae 00 17 fe 2a 64 76 69 72 3a 20 ....*dvir:   |
| 330   | 66 72 6f 6d 20 64 76 69 72 from dvi r                        |

כאן ניתן לראות את הפורטים של המקור והיעד ואת ההודעה כפי שהתקבלה אצל daniel : dvir" . from dvir"

3) הזנת פקודה שגויה ע"י הלקוח dvir שמזין לטרמינל את הפקודה "foo" ניתן לראות בצילום כי השרת יקבל את ההודעה כאשר הוא מסווג אותה כלא חוקית ויחזיר הודעה בהתאם כפי שנראה בתמונות הבאות.

| No. | Time          | Source    | Destination | Protocol  | Length | Info                 |
|-----|---------------|-----------|-------------|-----------|--------|----------------------|
| 57  | 233.400395396 | 127.0.0.1 | 127.0.0.1   | UDP       | 48     | 37584 → 12345 Len=6  |
| 58  | 233.400633145 | 127.0.0.1 | 127.0.0.1   | UDP       | 42     | 12345 → 37584 Len=0  |
| 59  | 242.092417066 | 127.0.0.1 | 127.0.0.1   | UDP       | 50     | 33710 → 12345 Len=8  |
| 60  | 242.092677039 | 127.0.0.1 | 127.0.0.1   | UDP       | 46     | 12345 → 33710 Len=4  |
| 61  | 261.506108740 | 127.0.0.1 | 127.0.0.1   | UDP       | 53     | 37584 → 12345 Len=11 |
| 62  | 261.506361313 | 127.0.0.1 | 127.0.0.1   | UDP       | 59     | 12345 → 37584 Len=17 |
| 64  | 275.038340763 | 127.0.0.1 | 127.0.0.1   | UDP       | 55     | 33710 → 12345 Len=13 |
| 65  | 275.038726333 | 127.0.0.1 | 127.0.0.1   | UDP       | 57     | 12345 → 33710 Len=15 |
| 66  | 285.375790435 | 127.0.0.1 | 127.0.0.1   | UDP       | 47     | 33710 → 12345 Len=5  |
| 67  | 285.376141069 | 127.0.0.1 | 127.0.0.1   | UDP       | 42     | 12345 → 33710 Len=0  |
| 68  | 293.167212884 | 127.0.0.1 | 127.0.0.1   | UDP       | 45     | 37584 → 12345 Len=3  |
| 69  | 293.167610529 | 127.0.0.1 | 127.0.0.1   | UDP       | 57     | 12345 → 37584 Len=15 |
| 70  | 302.960265143 | 127.0.0.1 | 127.0.0.1   | UDP       | 43     | 37584 → 12345 Len=1  |
| 71  | 302.960372313 | 127.0.0.1 | 127.0.0.1   | UDP       | 92     | 12345 → 37584 Len=50 |
| 72  | 319.610059060 | 127.0.0.1 | 127.0.0.1   | UDP       | 43     | 33710 → 12345 Len=1  |
| 73  | 327.610302237 | 127.0.0.1 | 127.0.0.1   | UDP       | 43     | 37584 → 12345 Len=1  |
| 74  | 327.610411431 | 127.0.0.1 | 127.0.0.1   | ADwin ... | 64     |                      |
| 75  | 333.331830735 | 127.0.0.1 | 127.0.0.1   | UDP       | 43     | 37584 → 12345 Len=1  |

Frame 68: 45 bytes on wire (360 bits), 45 bytes captured (360 bits) on interface lo, id 0

Interface id: 0 (lo)

Encapsulation type: Ethernet (1)

Arrival Time: Nov 14, 2022 12:02:50.947746970 PST

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1668456170.947746970 seconds

[Time delta from previous captured frame: 7.791071815 seconds]

[Time delta from previous displayed frame: 7.791071815 seconds]

[Time since reference or first frame: 293.167212884 seconds]

Frame Number: 68

Frame Length: 45 bytes (360 bits)

Capture Length: 45 bytes (360 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:udp:data]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

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

User Datagram Protocol, Src Port: 37584, Dst Port: 12345

Source Port: 37584

Destination Port: 12345

Length: 11

Checksum: 0xfe1e [unverified]

[Checksum Status: Unverified]

[Stream index: 7]

[Timestamps]

Data (3 bytes)

Data: 666f6f

0000 .....E
0010 00 1f fd c4 40 00 40 11 3f 07 7f 00 00 01 7f 00 ....@. ?.....
0020 00 01 92 d0 30 39 00 0b fe 1e 66 6f 6f ....09...foo

ניתן לראות כי החבילה המסומנת בחלק העליון של המסך עוברת מפורט 37584 שהוא הפורט של dvir כפי שציינו קודם אל הפורט 12345 של השרת, בתחתית המסך נוכל לראות את תוכן ההודעה "foo" כפי שהיא תועבר לשרת.

כעת נראה את החבילה הבאה שבה השרת משיב ל– dvir כי הפקודה איננה חוקית:

|    |               |           |           |           |    |                      |
|----|---------------|-----------|-----------|-----------|----|----------------------|
| 65 | 275.038726333 | 127.0.0.1 | 127.0.0.1 | UDP       | 57 | 12345 → 33710 Len=15 |
| 66 | 285.375790435 | 127.0.0.1 | 127.0.0.1 | UDP       | 47 | 33710 → 12345 Len=5  |
| 67 | 285.376141069 | 127.0.0.1 | 127.0.0.1 | UDP       | 42 | 12345 → 33710 Len=0  |
| 68 | 293.167212884 | 127.0.0.1 | 127.0.0.1 | UDP       | 45 | 37584 → 12345 Len=3  |
| 69 | 293.167610529 | 127.0.0.1 | 127.0.0.1 | UDP       | 57 | 12345 → 37584 Len=15 |
| 70 | 302.960265143 | 127.0.0.1 | 127.0.0.1 | UDP       | 43 | 37584 → 12345 Len=1  |
| 71 | 302.960372313 | 127.0.0.1 | 127.0.0.1 | UDP       | 92 | 12345 → 37584 Len=50 |
| 72 | 319.610059060 | 127.0.0.1 | 127.0.0.1 | UDP       | 43 | 33710 → 12345 Len=1  |
| 73 | 327.610302237 | 127.0.0.1 | 127.0.0.1 | UDP       | 43 | 37584 → 12345 Len=1  |
| 74 | 327.610411431 | 127.0.0.1 | 127.0.0.1 | ADwin ... | 64 |                      |
| 75 | 333.331830735 | 127.0.0.1 | 127.0.0.1 | UDP       | 43 | 37584 → 12345 Len=1  |

ניתן לראות את חבילה המסומנת מפורט 12345 של השרת חזרה לפורט 37584 של הלקוח dvir

|   |  |  |  |  |  |  |
|---|--|--|--|--|--|--|
| [Protocols in frame: eth:ethertype:ip:udp:data]   |  |  |  |  |  |  |
| [Coloring Rule Name: UDP]   |  |  |  |  |  |  |
| [Coloring Rule String: udp]   |  |  |  |  |  |  |
| 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   |  |  |  |  |  |  |
| User Datagram Protocol, Src Port: 12345, Dst Port: 37584  |  |  |  |  |  |  |
| Source Port: 12345  |  |  |  |  |  |  |
| Destination Port: 37584   |  |  |  |  |  |  |
| Length: 23  |  |  |  |  |  |  |
| Checksum: 0xfe2a [unverified]   |  |  |  |  |  |  |
| [Checksum Status: Unverified]   |  |  |  |  |  |  |
| [Stream index: 7]   |  |  |  |  |  |  |
| [Timestamps]  |  |  |  |  |  |  |
| Data (15 bytes)   |  |  |  |  |  |  |
| Data: 496c6c6567616c2072657175657374  |  |  |  |  |  |  |
| 0000 .....E |  |  |  |  |  |  |
| 0010 00 2b fd c5 40 00 40 11 3e fa 7f 00 00 01 7f 00 +..@. >.....                                     |  |  |  |  |  |  |
| 0020 00 01 30 39 92 d0 00 17 fe 2a 49 6c 6c 65 67 61 ..09....*Illega                                  |  |  |  |  |  |  |
| 0030 6c 20 72 65 71 75 65 73 74 1 request   |  |  |  |  |  |  |

wireshark\_lo\_20221114115740\_ucLuwV.pcapng

Packets: 79 · Displayed: 18 (22.8%) · Dropped: 0 (0.0%) · Profile: Default

ניתן לראות את פרטי התעבורה של השרת והלקוח ובתחתית התמונה נראה את תוכן ההודעה:  
"Illegal request" כפי שנשלחה מהשרת את הלקוח כתגובה לפקודה הבלתי חוקית שהועברה  
בחבילה הקודמת.