בס"ד

מגישים: אלמוג יעקב, טל סומך

מטלה 4 תקשורת

חלק א'

בחלק זה מימשנו קובץ myping.cpp השולח הודעת ICMP ECHO REQUEST ומקבל הודעת ICMP-ECHO-REPLY.

תיעוד הרצת הפקודה:

```
home@ubuntu:~/Documents/vscode/c/tikshoret-Task4/Ex4$ sudo ./myping
[sudo] password for home:
-------------------------------
The echo request was sent successfully!
-------------------------------
ECHO REQUEST DETAILS:
ECHO REQUEST type: 8
ECHO REQUEST code: 0
ECHO REQUEST identifier: 18
ECHO REQUEST sequence: 0
ECHO REQUEST message: "This is the ping."
-------------------------------
The echo reply was received successfully!
RTT = 55.965390 milliseconds (0.055965 microseconds).
-------------------------------
ECHO REPLY DETAILS:
ECHO REPLY type: 0
ECHO REPLY code: 0
ECHO REPLY sequence: 18
ECHO REPLY sequence: 0
ECHO REPLY message: "This is the ping."
```

פירוט הודעת השליחה:

נבחין בהיידר של ה-IP תחת הלשונית "Internet Protocal Version 4":

נזכיר כי ע"פ ההנחיות ההיידר של ה-IP נוצר ע"י ה-KERNEL.

השליחה מתבצעת לכתובת 8.8.8.8 תחת כתובת ה-IP של המחשב בנוכחי.

ההודעה נשלחת עם Identification (מזהה) ללא פרגמנטציה (פירוק ההודעה).

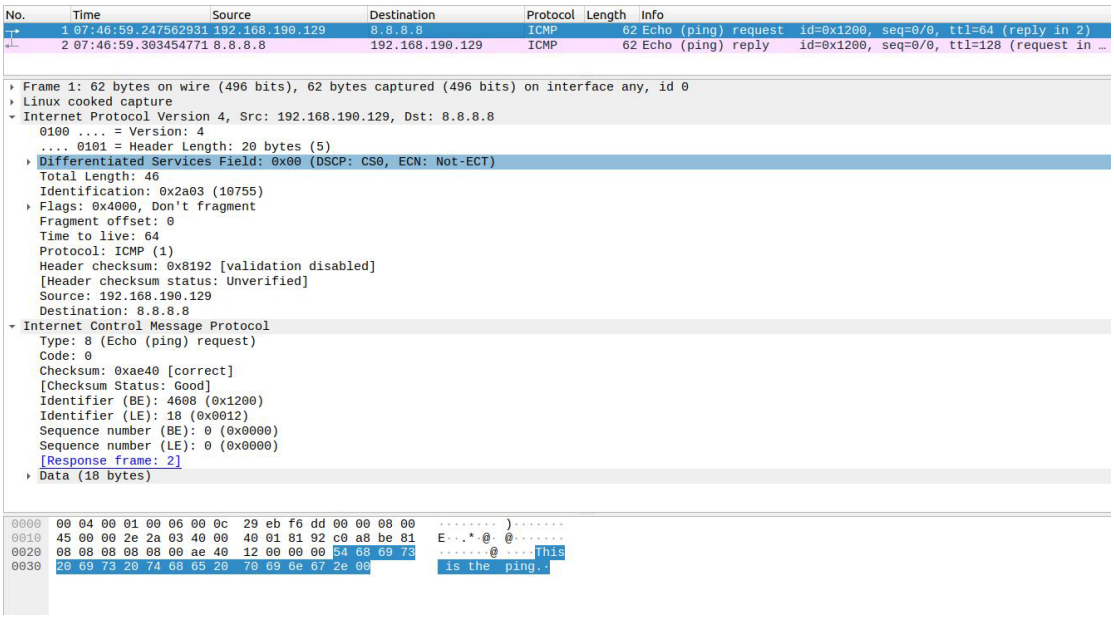
פרוטוקול ההודעה הינו ICMP עם מכסה של 64TTL (מספר ה-HOPS).

נבחין בהיידר של ה-ICMP תחת הלשונית "Internet Control Message Protocol":

ה-Type הינו 8 וה-Code הינו 0 (ה-Type וה-Code המתאימים להודעת Echo Request)

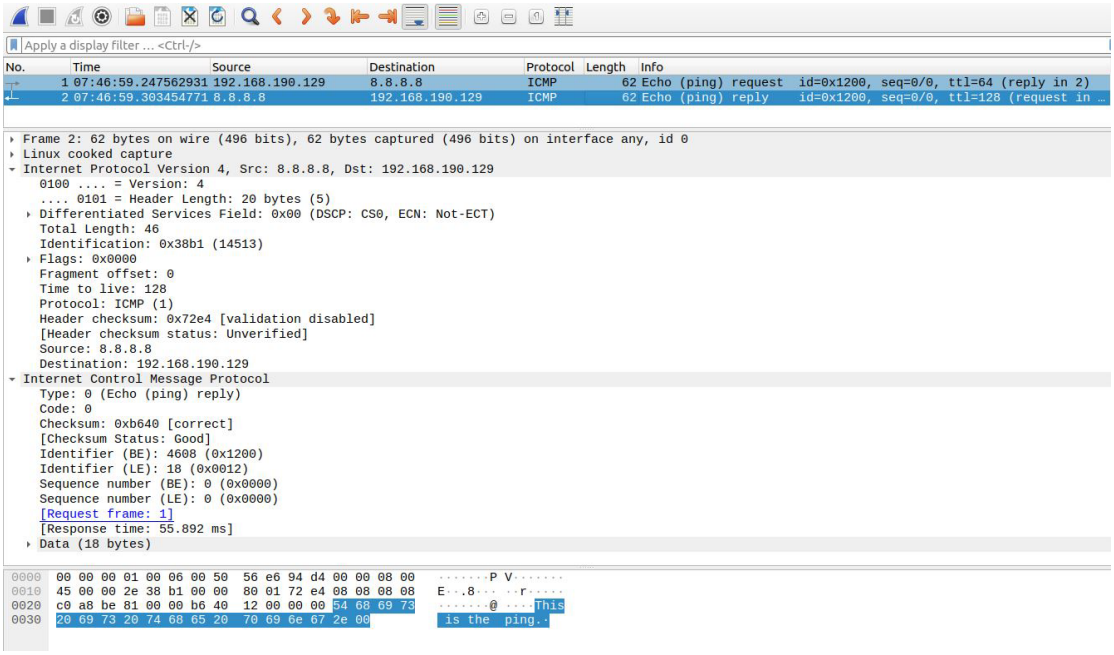
ההודעה נשלחה עם checksum ועם Identifier המוגדר להיות 18 לצורך זיהוי הודעת Echo Reply (הודעת ההחזרה המתאימה להודעה זו).

תוכן ההודעה הינו "This is the ping.".



<u>פירוט הודעת ההחזרה:</u>

נבחין בהיידר של ה-IP תחת הלשונית "Internet Protocal Version 4":
ההחזרה מתבצעת לכתובת הנוכחית מהכתובת 8.8.8.8.
ההודעה נשלחת עם Identification (מזהה) ללא פרגמנטציה (פירוק ההודעה).
פרוטוקול ההודעה הינו ICMP עם מכסה של 128TTL (מספר ה-HOPS).
נבחין בהיידר של ה-ICMP תחת הלשונית "Internet Control Message Protocol":
ה-Type הינו 0 וה-Code הינו 0 (ה-Type וה-Code המתאימים להודעת Echo Reply)
ההודעה נשלחה עם checksum ועם Identifier המוגדר להיות 18 לצורך זיהוי הודעת Echo Reply זו.
תוכן ההודעה הינו "This is the ping.".



No.	Time	Source	Destination	Protocol	Length	Info
1	07:46:59.247562931	192.168.190.129	8.8.8.8	ICMP	62	Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 2)
2	07:46:59.303454771	8.8.8.8	192.168.190.129	ICMP	62	Echo (ping) reply id=0x1200, seq=0/0, ttl=128 (request in …

```
▸ Frame 2: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface any, id 0
▸ Linux cooked capture
▾ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.190.129
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 46
    Identification: 0x38b1 (14513)
  ▸ Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x72e4 [validation disabled]
    [Header checksum status: Unverified]
    Source: 8.8.8.8
    Destination: 192.168.190.129
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xb640 [correct]
    [Checksum Status: Good]
    Identifier (BE): 4608 (0x1200)
    Identifier (LE): 18 (0x0012)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    [Request frame: 1]
    [Response time: 55.892 ms]
  ▸ Data (18 bytes)

0000  00 00 00 01 00 06 00 50  56 e6 94 d4 00 00 08 00   ·····P V·····
0010  45 00 00 2e 38 b1 00 00  80 01 72 e4 08 08 08 08   E···8··· ··r·····
0020  c0 a8 be 81 00 00 b6 40  12 00 00 00 54 68 69 73   ·····@ ····This
0030  20 69 73 20 74 68 65 20  70 69 6e 67 2e 00          is the  ping.·
```

חלק ב'

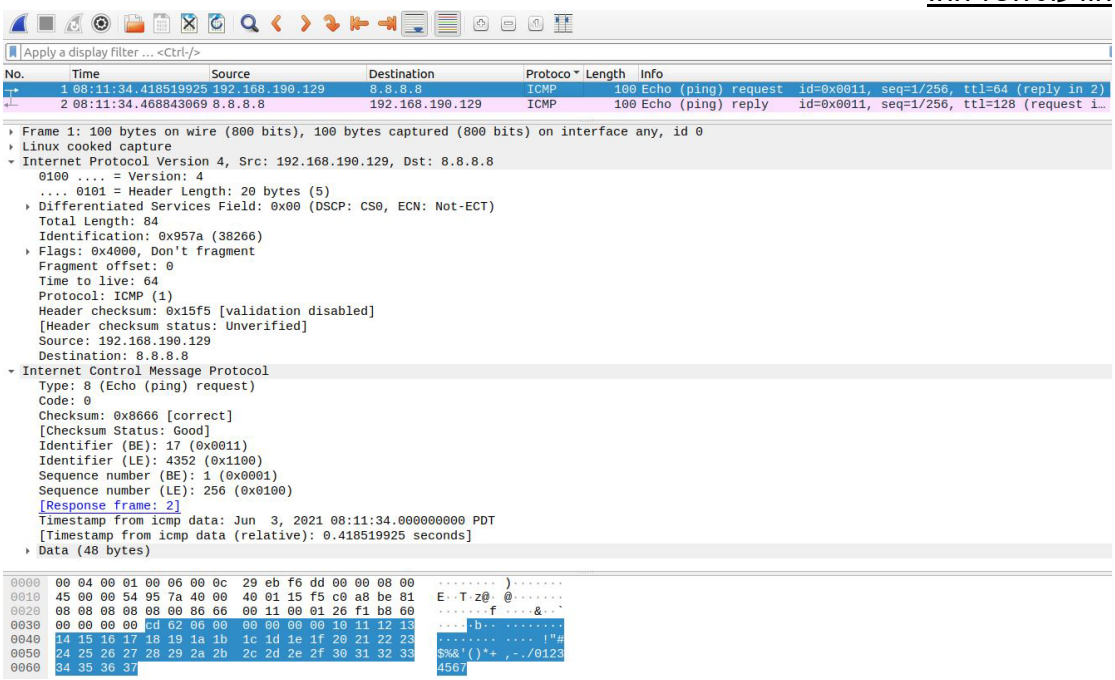
בחלק זה מימשנו קובץ sniffer.c שהוא כלי "להסנפת" פקטות (Sniffer). כלי זה מסניף תעבורת ICMP ברשת שלנו ומציג למסך את IP_SRC, IP_DST, TYPE, CODE (שדות ICMP) עבור כל פקטה רלוונטית העוברת ברשת שאנו מחוברים אליה.

תיעוד הרצת הפקודה:

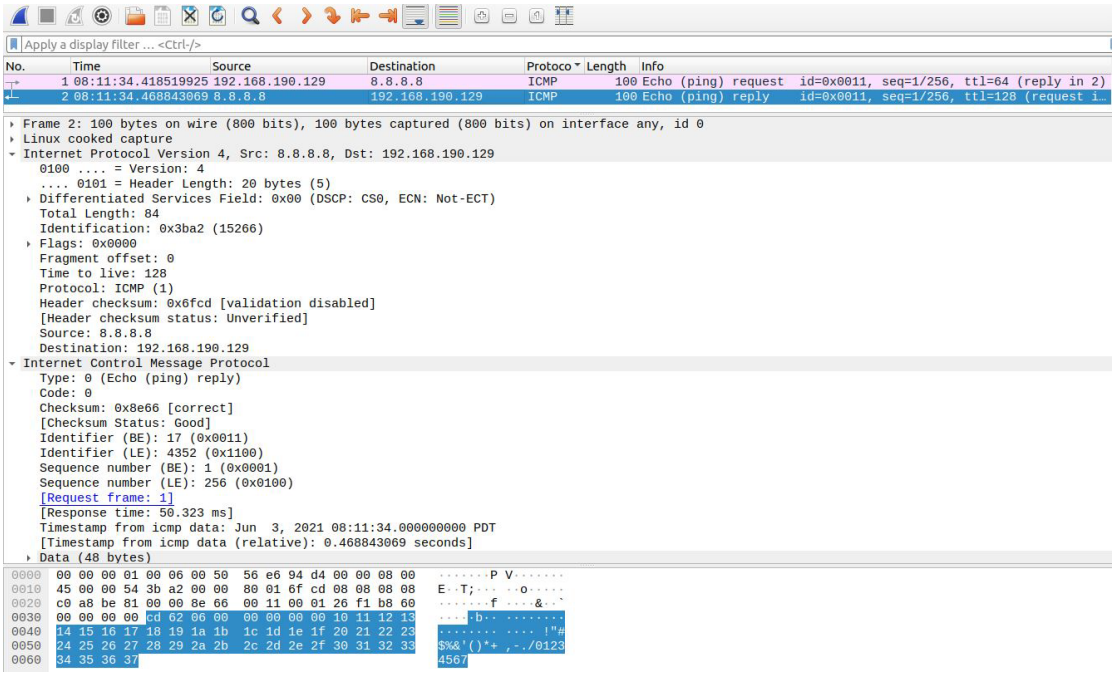
```
home@ubuntu:~/Documents/vscode/c/tikshoret-Task4/Ex4$ sudo ./sniffer
-------------------------------
IP DETAILS:
Source:  192.168.190.129
Destination: 8.8.8.8
ICMP DETAILS:
Type: 8
Code: 0
Id: 6656
Seq: 256
Data : ◆◆◆`
-------------------------------
IP DETAILS:
Source:  8.8.8.8
Destination: 192.168.190.129
ICMP DETAILS:
Type: 0
Code: 0
Id: 6656
Seq: 256
Data : ◆◆◆`
```

מכיוון שאנו מסניפים תעבורת ICMP ניתן להסניף את הפקטה שאנו שולחים ומקבלים בחלק א'.
בין היתר ניתן להסניף כל הודעת ICMP כמו לדוגמא לאחר שליחת פינג כפי שמתועד בתמונה לעיל (לאחר שליחת הודעת פינג לכתובת 8.8.8.8).
הסבר ההודעות המתועדות ב-Wireshark בחלק זה הינן זהות להודעות אותן הסברנו בחלק א' פרט לתוכן ה-Data (ונתונים אקראיים כדוגמת Sequence, Identifier).

הודעת השליחה:



הודעת ההחזרה:



No.	Time	Source	Destination	Protoco	Length	Info
1	08:11:34.418519925	192.168.190.129	8.8.8.8	ICMP	100	Echo (ping) request id=0x0011, seq=1/256, ttl=64 (reply in 2)
2	08:11:34.468843069	8.8.8.8	192.168.190.129	ICMP	100	Echo (ping) reply id=0x0011, seq=1/256, ttl=128 (request i…

```
▸ Frame 2: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
▸ Linux cooked capture
▾ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.190.129
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x3ba2 (15266)
  ▸ Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x6fcd [validation disabled]
    [Header checksum status: Unverified]
    Source: 8.8.8.8
    Destination: 192.168.190.129
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x8e66 [correct]
    [Checksum Status: Good]
    Identifier (BE): 17 (0x0011)
    Identifier (LE): 4352 (0x1100)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Request frame: 1]
    [Response time: 50.323 ms]
    Timestamp from icmp data: Jun  3, 2021 08:11:34.000000000 PDT
    [Timestamp from icmp data (relative): 0.468843069 seconds]
  ▸ Data (48 bytes)
```

```
0000  00 00 00 01 00 06 00 50  56 e6 94 d4 00 00 08 00   ·····P V·····
0010  45 00 00 54 3b a2 00 00  80 01 6f cd 08 08 08 08   E··T;··· ··o·····
0020  c0 a8 be 81 00 00 8e 66  00 11 00 01 26 f1 b8 60   ·····f ····&··`
0030  00 00 00 00 cd 62 06 00  00 00 00 00 10 11 12 13   ·····b·· ********
0040  14 15 16 17 18 19 1a 1b  1c 1d 1e 1f 20 21 22 23   ******** **** !"#
0050  24 25 26 27 28 29 2a 2b  2c 2d 2e 2f 30 31 32 33   $%&'()*+ ,-./0123
0060  34 35 36 37                                        4567
```