בס"ד

מטלה 6

דביר בהון 318765856

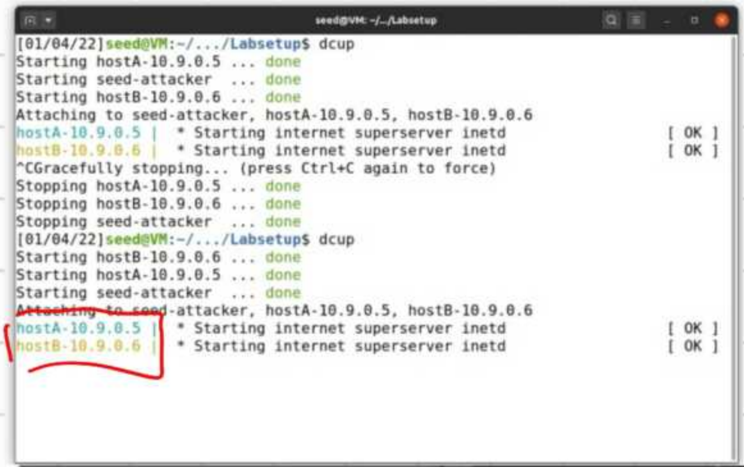
אהד שירצי - 318636693

1.1A

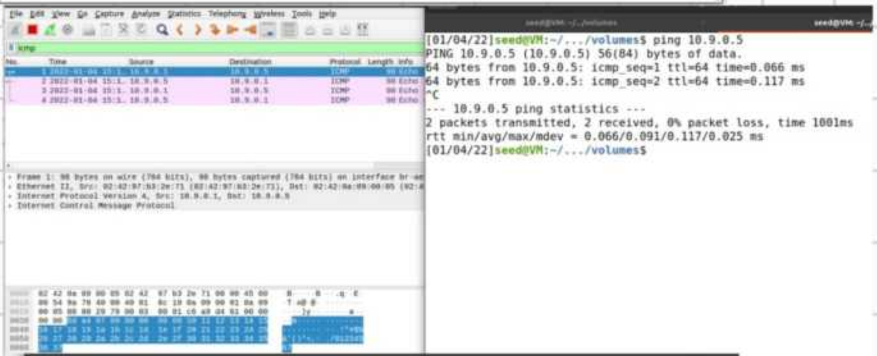
ה ip של HostA, HostB שלנו יהיו 10.9.0.5, 10.9.0.6

ו- 10.9.0.1 יהיה של התוקף.

לכן בכל המשך המטלה אנו נראה את התוקף מבוצע ממנו אל אחרים.

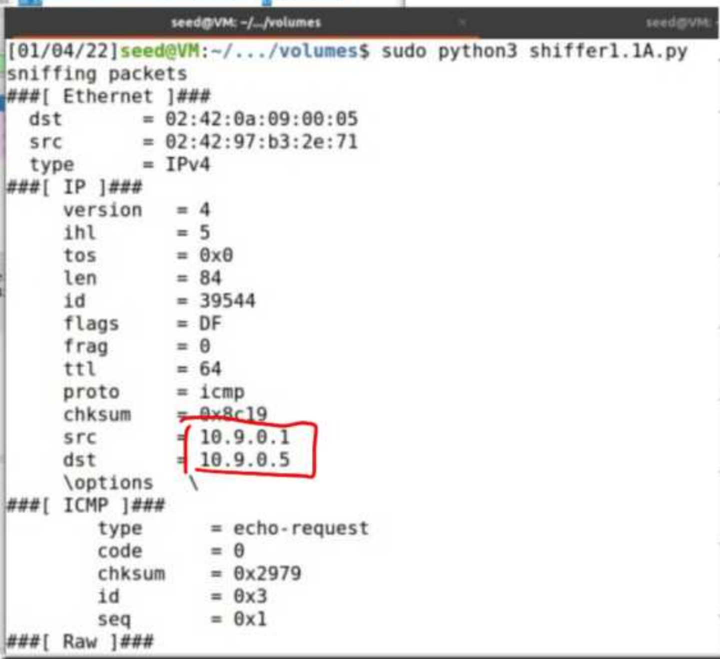


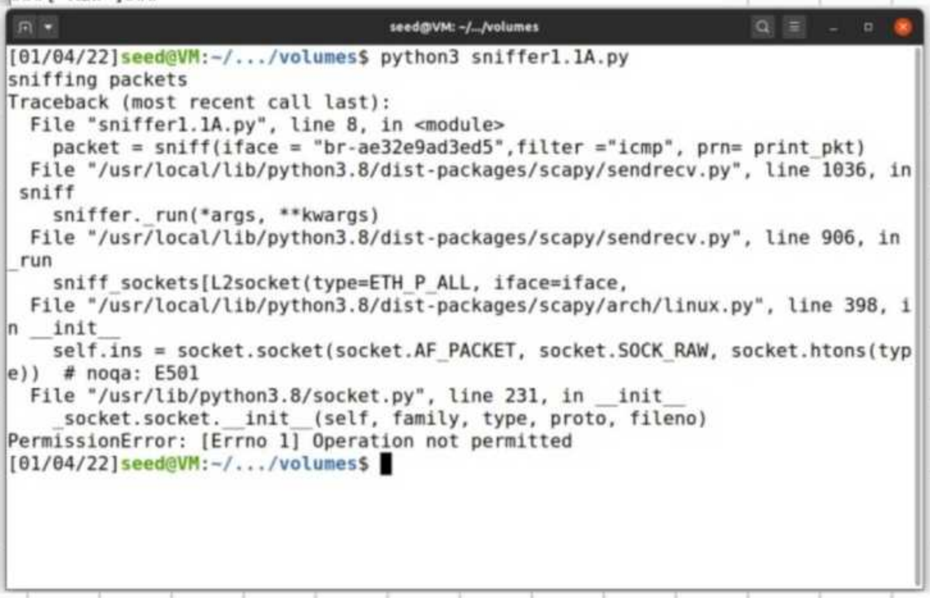
כמו שאפשר לראות בתמונה שלנו 2 הודעות פינג וקיבלנו 2 הודעות פונג (Replay) לכן בוושארק אפשר לראות 4 הודעות.



ואצלנו בקוד השני סניפר. אפשר לראות שאנו תופסים את src ו- Dest של הפינג.

כל זה באישור הפעלה של הרשאות מנהל. sudo.





בפעם השנייה שניסינו להפעיל ללא הרשאות זה לא ניתן לנו להפעיל כי אנחנו משתמשים פה ב Raw וכמו שאנו יודעים מתעלים קודמות זה קשור למערכת הפעלה ולכן חייב הרשאות מנהל.

1.1B

```
[01/04/22]seed@VM:~/.../volumes$ sudo python3 shiffer1.1A.py
sniffing packets
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:97:b3:2e:71
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 39544
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0x8c19
     src       = 10.9.0.1
     dst       = 10.9.0.5
     \options   \
###[ ICMP ]###
        type      = echo-request
        code      = 0
        chksum    = 0x2979
        id        = 0x3
        seq       = 0x1
###[ Raw ]###
```

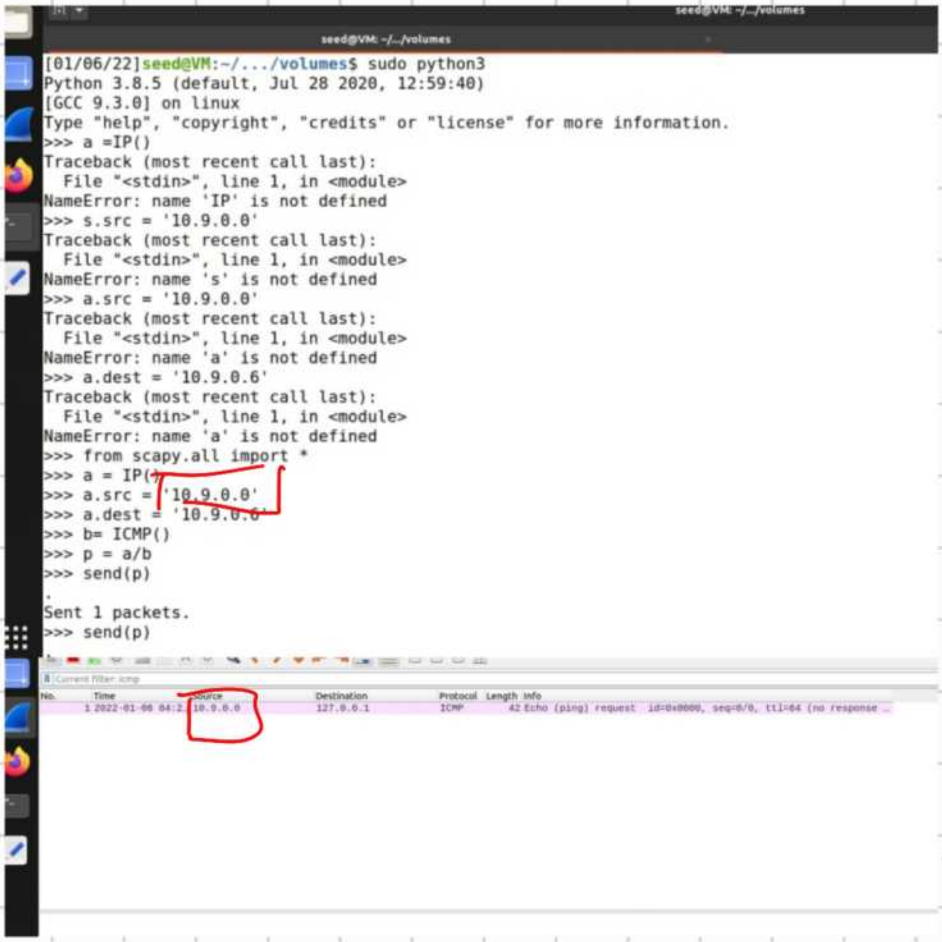
```
[01/06/22]seed@VM:~/.../volumes$ sudo python3 sniffer1.1B.py
sniffing packets
###[ Ethernet ]###
  dst       = 52:54:00:12:35:02
  src       = 08:00:27:04:01:83
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 28243
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0xb037
     src       = 10.0.2.15
     dst       = 8.8.8.8
     \options   \
###[ ICMP ]###
        type      = echo-request
        code      = 0
        chksum    = 0x9bc3
        id        = 0x5
        seq       = 0x1
###[ Raw ]###
           load      = 'G\x98\xd6a\x00\x00\x00\x00\x00si\x0c\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\
!"#$%&\'()*+,-./01234567'

###[ Ethernet ]###
```

```
1 from scapy.all import *
2 print("sniffing packets")
3
4 def print_pkt(pkt):
5     pkt.show()
6
7 #(filter = "icmp", prn= print_pkt)# part 1
8 packet = sniff(iface = "br-ae32e9ad3ed5", filter = "tcp", prn=
  print_pkt) #part 2
9 #packet = sniff(filter = "icmp and host 8.8.8.8", prn= print_pkt)
  #part 3
```

```
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0x3d85
     src       = 10.9.0.5
     dst       = 10.9.0.1
     \options   \
###[ TCP ]###
        sport     = telnet
        dport     = 41514
        seq       = 1784407128
        ack       = 1309346890
        dataofs   = 8
        reserved  = 0
        flags     = PA
        window    = 509
        chksum    = 0x1453
        urgptr    = 0
        options   = [('NOP', None), ('NOP', None)
53302453))]
###[ Raw ]###
           load      = 'seed@153b7cdbdd2e:~$ '
```

Task 1.2



כמו שאפשר לראות בתוכנית
אני מזייפים את src.
מציין שאני בכלל 10.9.0.1
ושיניתי ל-10.9.0.0.
אפשר לראות בוושארק
שלא התקבלה תשובה בגלל
שכתובת זה לא קיים.
ואין לו למי להשיב.
בתמונה האחרונה אפשר לראות
באמת שבפקטה ה src
שלי השתנה. מציין ששלחתי
ל- HostA. אך היינו צריכים
להאזין loopback.

```
Sent 1 packets.
>>> ls(a)
version    : BitField  (4 bits)          = 4             (4)
ihl        : BitField  (4 bits)          = None          (None)
tos        : XByteField                  = 0             (0)
len        : ShortField                  = None          (None)
id         : ShortField                  = 1             (1)
flags      : FlagsField  (3 bits)        = <Flag 0 ()>   (<Flag 0 ()>)
frag       : BitField  (13 bits)         = 0             (0)
ttl        : ByteField                   = 64            (64)
proto      : ByteEnumField               = 0             (0)
chksum     : XShortField                 = None          (None)
src        : SourceIPField               = '10.9.0.0'    (None)
dst        : DestIPField                 = '127.0.0.1'   (None)
options    : PacketListField             = []            ([])
>>> ls(a)
version    : BitField  (4 bits)          = 4             (4)
ihl        : BitField  (4 bits)          = None          (None)
tos        : XByteField                  = 0             (0)
len        : ShortField                  = None          (None)
id         : ShortField                  = 1             (1)
flags      : FlagsField  (3 bits)        = <Flag 0 ()>   (<Flag 0 ()>)
frag       : BitField  (13 bits)         = 0             (0)
ttl        : ByteField                   = 64            (64)
proto      : ByteEnumField               = 0             (0)
chksum     : XShortField                 = None          (None)
src        : SourceIPField               = '10.9.0.0'    (None)
dst        : DestIPField                 = '127.0.0.1'   (None)
options    : PacketListField             = []            ([])
>>> send(p)
```

Task 1.3

```python
from scapy.all import *

a = IP(dst = '172.217.171.206', ttl = 1)
b = ICMP()
p = a/b
ls(a)
send(p)
```

```python
from scapy.all import *

a = IP(dst = '172.217.171.206', ttl = 16)
b = ICMP()
p = a/b
ls(a)
send(p)
```

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-01-06 04:4…	PcsCompu_04:01:83	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
2	2022-01-06 04:4…	RealtekU_12:35:02	PcsCompu_04:01:83	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
3	2022-01-06 04:4…	10.0.2.15	172.217.171.206	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=1 (no response f…
4	2022-01-06 04:4…	10.0.2.2	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
5	2022-01-06 04:4…	PcsCompu_04:01:83	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
6	2022-01-06 04:4…	RealtekU_12:35:02	PcsCompu_04:01:83	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
7	2022-01-06 04:4…	10.0.2.15	172.217.171.206	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=2 (no response f…
8	2022-01-06 04:4…	31.168.13.77	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
9	2022-01-06 04:4…	PcsCompu_04:01:83	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
10	2022-01-06 04:4…	RealtekU_12:35:02	PcsCompu_04:01:83	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
11	2022-01-06 04:4…	10.0.2.15	172.217.171.206	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=4 (no response f…
12	2022-01-06 04:4…	10.250.88.11	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
13	2022-01-06 04:4…	PcsCompu_04:01:83	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
14	2022-01-06 04:4…	RealtekU_12:35:02	PcsCompu_04:01:83	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
15	2022-01-06 04:4…	10.0.2.15	172.217.171.206	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=8 (no response f…
16	2022-01-06 04:4…	216.239.50.123	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
17	2022-01-06 04:4…	PcsCompu_04:01:83	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
18	2022-01-06 04:4…	RealtekU_12:35:02	PcsCompu_04:01:83	ARP	60	10.0.2.2 is at 52:54:00:12:35:02

```
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_04:01:83 (08:00:27:04:01:83), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
```

No.	Time	Source	Destination	Protocol	Length	Info
24	2022-01-06 04:4…	208.67.220.220	10.0.2.15	DNS	161	Standard query response 0x58a1 AAAA connectivity-check.ubuntu…
25	2022-01-06 04:4…	PcsCompu_04:01:83	RealtekU_12:35:02	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
26	2022-01-06 04:4…	RealtekU_12:35:02	PcsCompu_04:01:83	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
27	2022-01-06 04:4…	PcsCompu_04:01:83	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
28	2022-01-06 04:4…	RealtekU_12:35:02	PcsCompu_04:01:83	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
29	2022-01-06 04:4…	10.0.2.15	172.217.171.206	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=12 (reply in 30)
30	2022-01-06 04:4…	172.217.171.206	10.0.2.15	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=115 (request in …
31	2022-01-06 04:4…	10.0.2.15	208.67.220.220	DNS	100	Standard query 0x4e53 AAAA connectivity-check.ubuntu.com OPT
32	2022-01-06 04:4…	208.67.220.220	10.0.2.15	DNS	161	Standard query response 0x4e53 AAAA connectivity-check.ubuntu…
33	2022-01-06 04:4…	PcsCompu_04:01:83	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
34	2022-01-06 04:4…	RealtekU_12:35:02	PcsCompu_04:01:83	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
35	2022-01-06 04:4…	10.0.2.15	172.217.171.206	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=10 (reply in 36)
36	2022-01-06 04:4…	172.217.171.206	10.0.2.15	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=115 (request in …
37	2022-01-06 04:4…	PcsCompu_04:01:83	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
38	2022-01-06 04:4…	RealtekU_12:35:02	PcsCompu_04:01:83	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
39	2022-01-06 04:4…	10.0.2.15	172.217.171.206	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=9 (reply in 40)
40	2022-01-06 04:4…	172.217.171.206	10.0.2.15	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=115 (request in …

```
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_04:01:83 (08:00:27:04:01:83), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
```

אפשר לראות בקוד כי אנחנו מתחילים ב-ttl=1 ואז מתחילים לעלות בקפיצות של 2 עד שנקבל תגובה. אחרי שקיבלנו תגובה ורדנו ב ttl בכדי למצוא את המדויק. (הגענו לכך שהוא שווה ל-9)

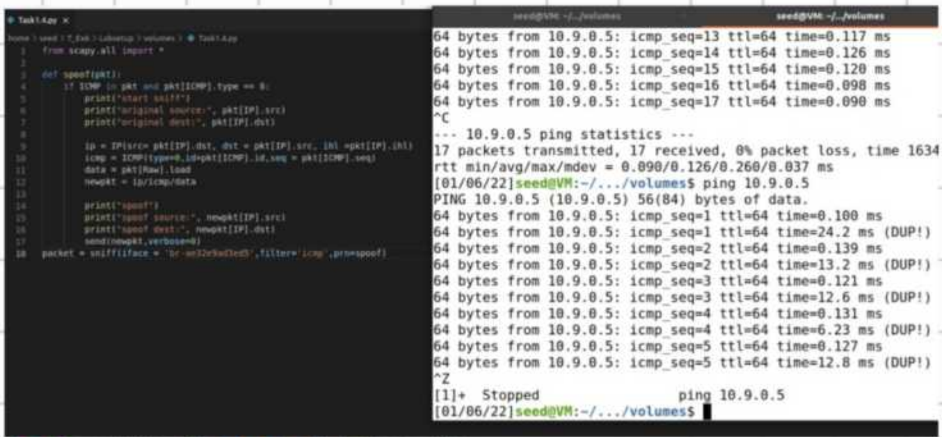
את הבדיקה עשינו מול גוגל. אפשר לראות בוויירשרק שבאיות בהתחלה לא קיבלנו תגובה כי ה ttl קטן מידי. ולאחר מכן אנו מקבלים תגובה.

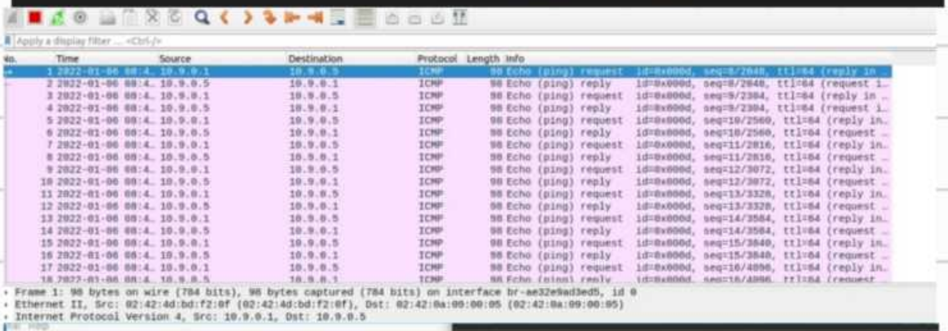
הוספנו שגם התוכנית תדפיס את הפקטה שנשלחה מה שאפשר לראות בתמונה האמורה.

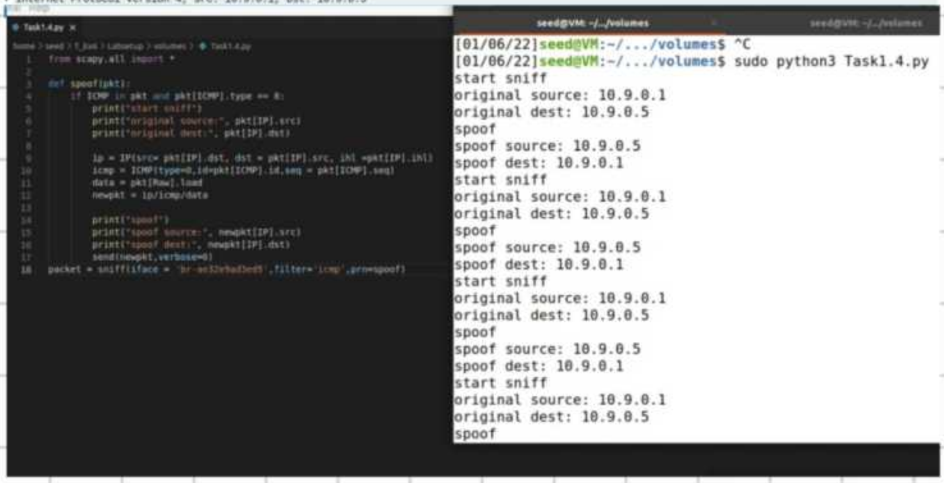
```
proto      : ByteEnumField                    = 0               (0)
chksum     : XShortField                      = None            (None)
src        : SourceIPField                    = '10.0.2.15'     (None)
dst        : DestIPField                      = '172.217.171.206' (None)
options    : PacketListField                  = []              ([])
.
Sent 1 packets.
[01/06/22]seed@VM:~/.../volumes$ sudo python3 Task1.3.py
version    : BitField  (4 bits)               = 4               (4)
ihl        : BitField  (4 bits)               = None            (None)
tos        : XByteField                       = 0               (0)
len        : ShortField                       = None            (None)
id         : ShortField                       = 1               (1)
flags      : FlagsField  (3 bits)             = <Flag 0 ()>     (<Flag 0 ()>)
frag       : BitField  (13 bits)              = 0               (0)
ttl        : ByteField                        = 9               (64)
proto      : ByteEnumField                    = 0               (0)
chksum     : XShortField                      = None            (None)
src        : SourceIPField                    = '10.0.2.15'     (None)
dst        : DestIPField                      = '172.217.171.206' (None)
options    : PacketListField                  = []              ([])
.
Sent 1 packets.
[01/06/22]seed@VM:~/.../volumes$
```

Task 1.4

אפשר להראות שאני שולחת ping ל- HostB.
ואני מזייפת בעצם אני מחליף בין השולח לנשלח.
אפשר להראות את זה בהדפסות וגם בקוד, שאני מסניפה לפקטות ובעקבות אותן שולחת תשובה ומחליפה בין src ל- dest.

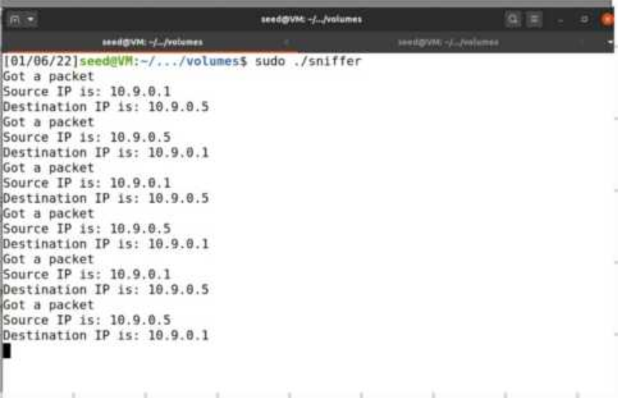






Task 2.1A

```
[01/06/22]seed@VM:~/.../volumes$ ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
64 bytes from 10.9.0.5: icmp_seq=1 ttl=64 time=0.052 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=64 time=0.060 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=64 time=0.058 ms
^Z
[1]+  Stopped                 ping 10.9.0.5
[01/06/22]seed@VM:~/.../volumes$
```



```
[01/06/22]seed@VM:~/.../volumes$ sudo ./sniffer
Got a packet
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.5
Got a packet
Source IP is: 10.9.0.5
Destination IP is: 10.9.0.1
Got a packet
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.5
Got a packet
Source IP is: 10.9.0.5
Destination IP is: 10.9.0.1
Got a packet
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.5
Got a packet
Source IP is: 10.9.0.5
Destination IP is: 10.9.0.1
```

Q1) בכדי שאוכל לקבל את src ip ו dst ip אני צריכה לשלוח פקטה אז שלחנו פקטה מסוג icmp. ואז אני מפלטרת אותה בכדי למצוא את src ip ו dst ip.

Q2) אני חייבת הרשאות מנהל מ-2 סיבות
1. בכדי להיות בפרומיסקוס מוד (מצב) ושונה לכולם.
2. להשתמש ב-Raw sock. ואני חלקים שבמערכת הפעלה אחראית עליהם. שזה Ethernet, ip, icmp (מערכת הפעלה).

Q3) אם אני אכבה את מצב פרומיסקוס מוד. אני אקבל רק את החבילות שאמורות להגיע אלי ישירות ולא כל הפקטות העוברות בכבלים ברשת שלי.

Task 2.1B

אפשר לראות כי הסנפני רק פקטות מסוג icmp בין 10.9.0.1 לבין 10.9.0.6, ושלחנו הודעת ping בכדי לראות אותה.

```
****************** ICMP Packet ******************
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
ICMP Echo type is: Type 8 Echo Request
ICMP Echo code is: 0
Got a packet

****************** ICMP Packet ******************
Source IP is: 10.9.0.6
Destination IP is: 10.9.0.1
ICMP Echo type is: Type 0  Echo Reply
ICMP Echo code is: 0
Got a packet

****************** ICMP Packet ******************
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
ICMP Echo type is: Type 8 Echo Request
ICMP Echo code is: 0
Got a packet

****************** ICMP Packet ******************
Source IP is: 10.9.0.6
Destination IP is: 10.9.0.1
ICMP Echo type is: Type 0  Echo Reply
ICMP Echo code is: 0
^Z
[2]+  Stopped                 ping 10.9.0.6
[01/06/22]seed@VM:~/.../volumes$
```

```
seed@VM: ~/.../volumes                    seed@VM: ~/.../volumes
******************* TCP Packet ******************
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59580
Destanation Port is: 23
Got a packet


******************* TCP Packet ******************
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59580
Destanation Port is: 23
Got a packet


******************* TCP Packet ******************
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59580
Destanation Port is: 23
Got a packet


******************* TCP Packet ******************
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59580
Destanation Port is: 23
```

```
seed@VM: ~/.../volumes                    seed@VM: ~/.../volumes
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Thu Jan  6 18:46:44 UTC 2022 from 10.9.0.1 on pts/2
seed@61faa7e1f08a:~$ exit
logout
Connection closed by foreign host.
[01/06/22]seed@VM:~/.../volumes$ telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
61faa7e1f08a login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Thu Jan  6 18:51:19 UTC 2022 from 10.9.0.1 on pts/2
seed@61faa7e1f08a:~$ exit
logout
Connection closed by foreign host.
[01/06/22]seed@VM:~/.../volumes$
```

```
******************* TCP Packet ******************
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59596
Destanation Port is: 23
Data:
D
Got a packet


******************* TCP Packet ******************
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59596
Destanation Port is: 23
Data:
`
Got a packet


******************* TCP Packet ******************
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59596
Destanation Port is: 23
Data:
Got a packet
```

```
Data:
C
Got a packet


******************* TCP Packet ******************
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59596
Destanation Port is: 23
Data:
C
Got a packet


******************* TCP Packet ******************
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59596
Destanation Port is: 23
Data:
s
Got a packet
```

שאלה לחשוב מדוע כי אנו מבקשים את החלק השני כאשר מיצגים בפורמט לא 100-101 אחסן בפורמט Tcp. ושאיתנו שלושה כדי לחשוב שאנו הסניפר שלנו מקבים את לב.

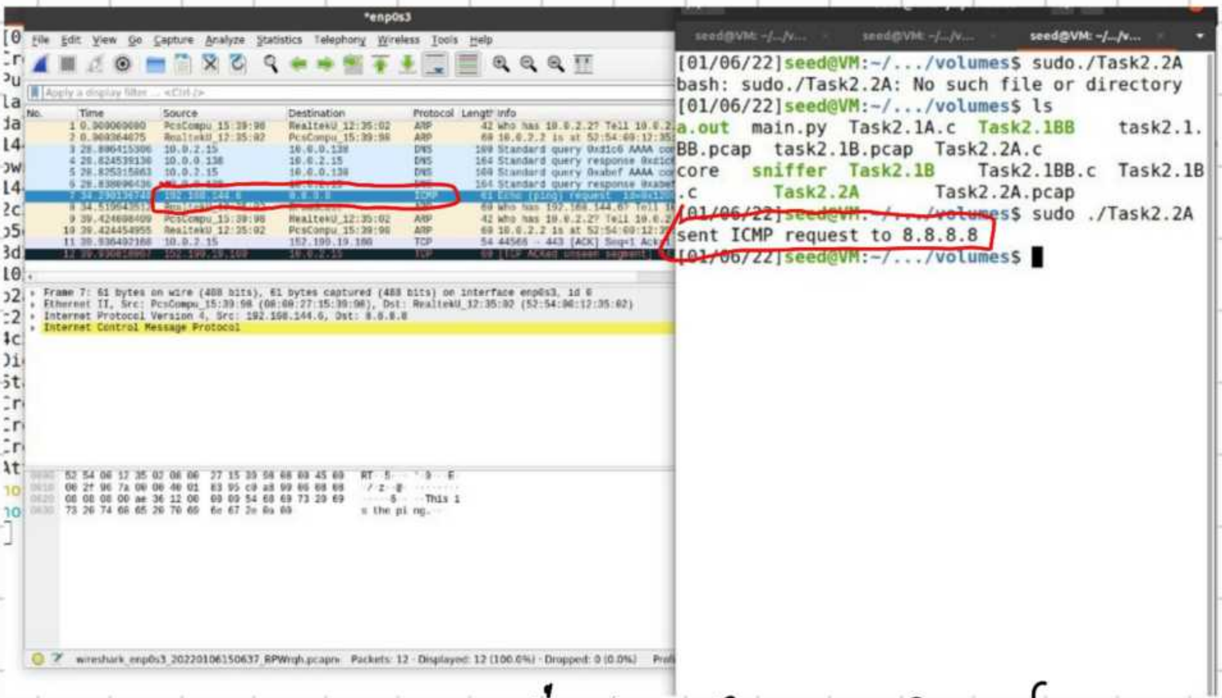
Task 2.1C

עקבנו אם את Tcp Data ושמם הצלחנו לחשוב את הסיסמה שאתה הקשנו.

Task2.2A

Task 2.2B

ענינו על שני המשימות
זייפנו ip אפשר לראות
בתמונה שאנחנו שולחים
לגוגל ping אך ה src
לא תואם לשלנו ולכן
גוגל לא משיב אך
הוא קיבל את הבקשה.

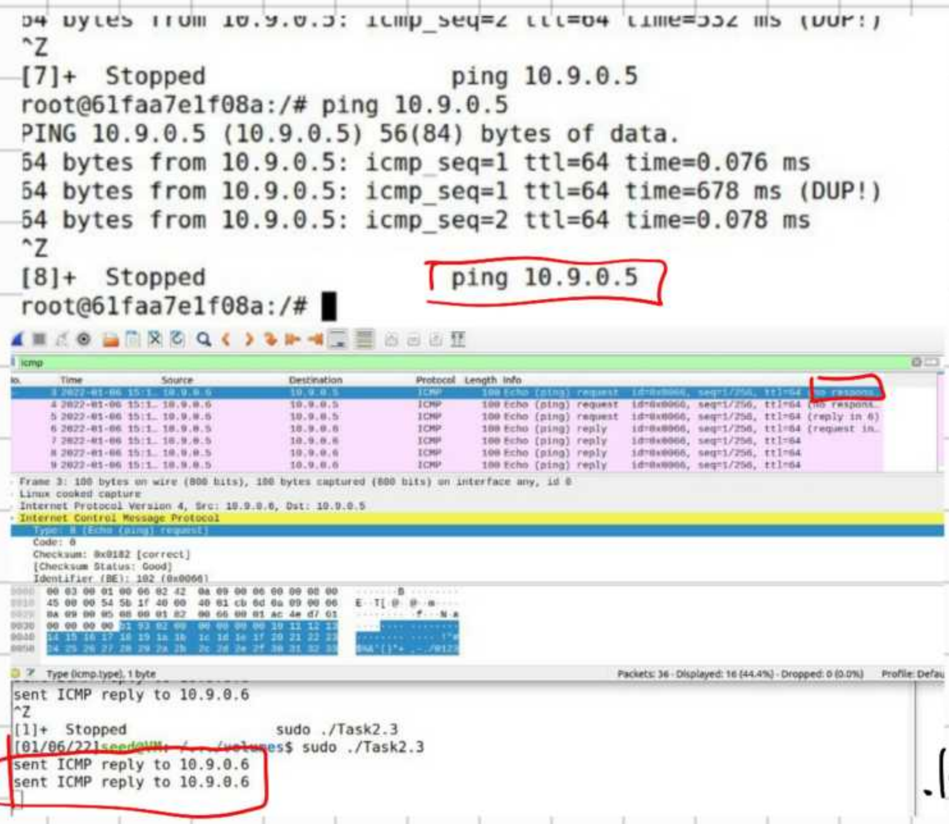


Q4 לא מבין שבגלל אם תשלח פקטה יותר קטנה הוא "ירפד" אותה באפסים על מנת שהיא תהיה בגודל הרצוי.

Q5 אני חייב לחשב את check sum כאשר אני משתמש ב- Raw Socket. בכדי שהוא יגיע למקום הרצוי של ip ולא לאבד (השתמשנו בדברים במטלה כך).

Q6 אני חייב להשתמש בהרשאות מנהל Ethernet, ip, icmp, Data מערכת הפעלה.
מכיוון שאני ניגשים לאיזור בו המערכת הפעלה שלי אחראית עליו אני חייב הרשאות מנהל Raw Sockets אומר שאני רוצים בעצמנו להגדיר את השדות.

Task 2.3



אפשר לראות כי אנחנו
שולחים מ HostA
ל- HostB את icmp
אך ה Atkker מסניף
ושולח את התשובה לפני
ומחליף את הבקשה בין
src ל- dst ולכן
אפשר לראות עם הוושארק
שאין תגובה לבקשת icmp.
שלחנו את הבקשות
מ- 10.9.06 ל- 10.9.05.