תקשורת ומחשוב מטלה 6

חלק 1:

-1.1A

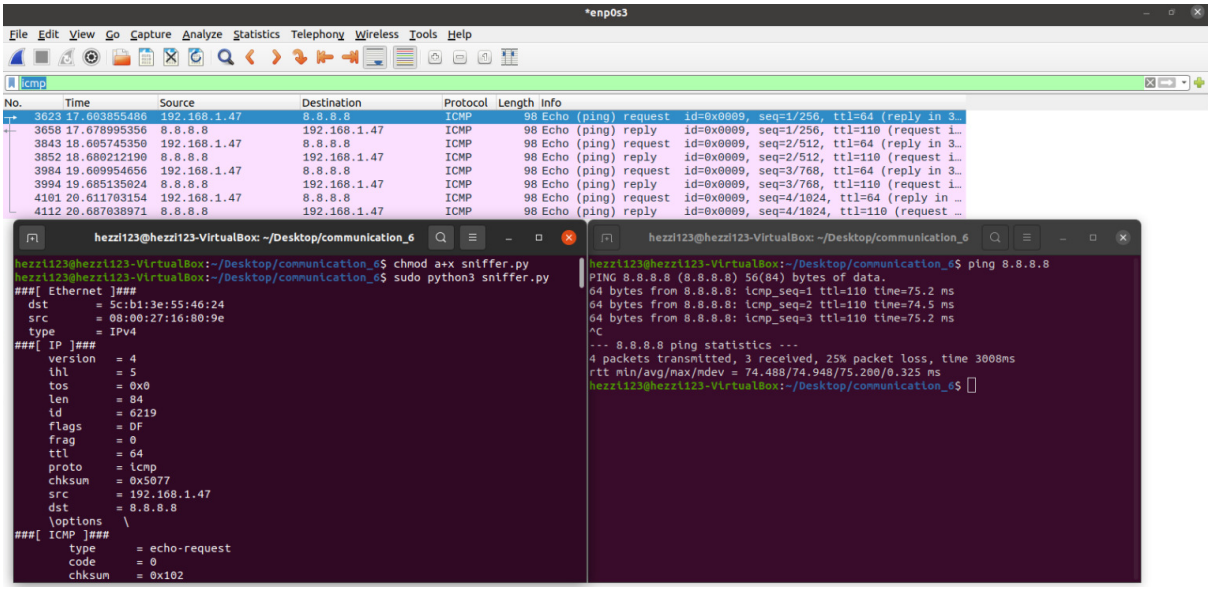
הקוד

```python
#!/usr/bin/env python3
from scapy.all import *

def print_pkt(pkt):
    pkt.show()

pkt = sniff(iface='enp0s3', filter='icmp', prn=print_pkt)
```

כשאנחנו מנסים להריץ ללא הפקודה sudo אנחנו מקבלים שגיאה, משום שאין לנו הרשאה להסניף פקטות.

```
hezzi123@hezzi123-VirtualBox: ~/Desktop/communication_6
hezzi123@hezzi123-VirtualBox:~/Desktop/communication_6$ python3 sniffer.py
Traceback (most recent call last):
  File "sniffer.py", line 7, in <module>
    pkt = sniff(iface='enp0s3', filter='icmp', prn=print_pkt)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 1263, in sn
iff
    sniffer._run(*args, **kwargs)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 1127, in _r
un
    sniff_sockets[L2socket(type=ETH_P_ALL, iface=iface,
  File "/usr/local/lib/python3.8/dist-packages/scapy/arch/linux.py", line 486, in _
_init__
    self.ins = socket.socket(
  File "/usr/lib/python3.8/socket.py", line 231, in __init__
    socket.socket.__init__(self, family, type, proto, fileno)
PermissionError: [Errno 1] Operation not permitted
hezzi123@hezzi123-VirtualBox:~/Desktop/communication_6$
```

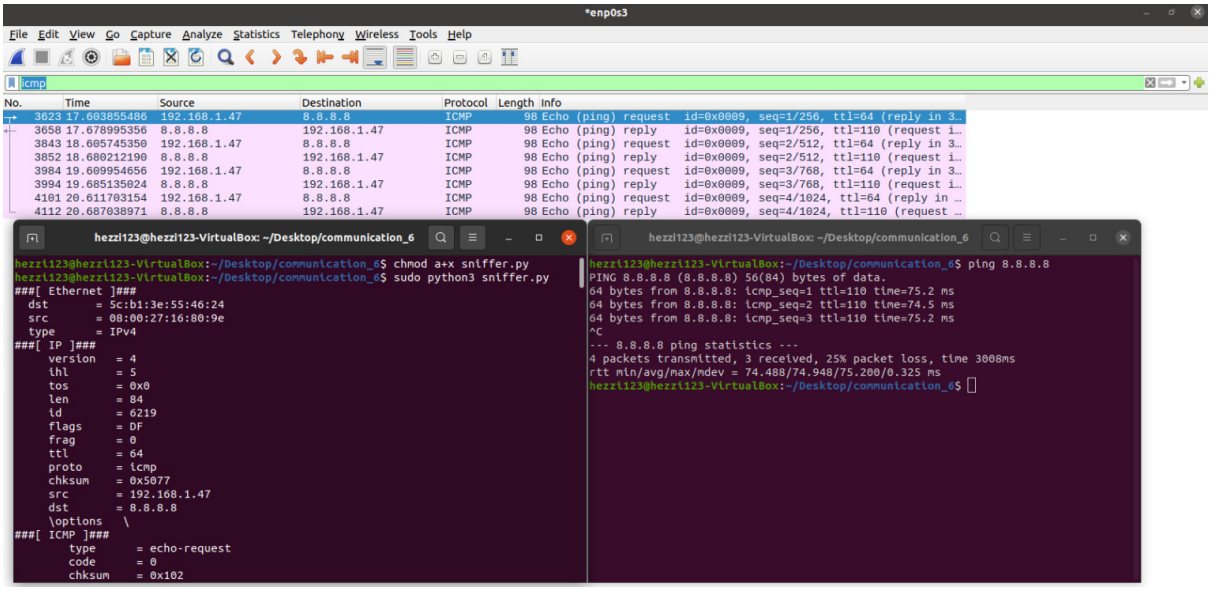
כשמריצים עם הפקודה sudo הקוד רץ (בגלל שהפקודה sudo נותנת למשתמש להריץ"as root") וניתן לראות בצד ימין בתמונה שעשינו פינג ל8.8.8.8 (google.com) ובצד שמאל בתמונה ניתן לראות את sniffer שלנו האזין לפקטות.



-1.1B

ICMP:

Capture only the ICMP packet

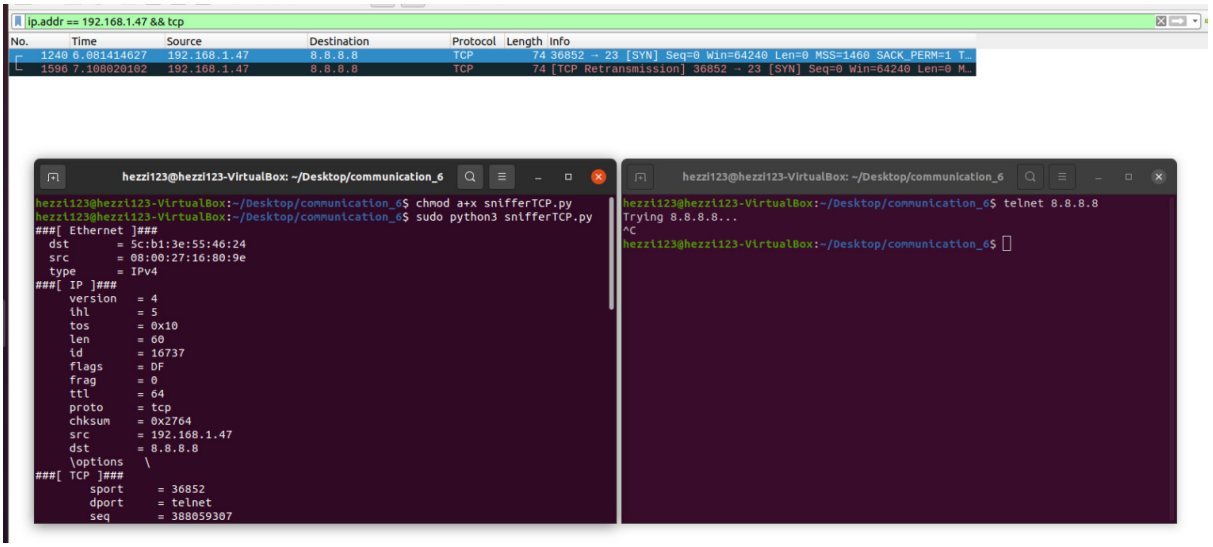


הקוד

```python
#!/usr/bin/env python3
from scapy.all import *

def print_pkt(pkt):
    pkt.show()

pkt = sniff(iface='enp0s3', filter='icmp', prn=print_pkt)
```

TCP:

Capture any TCP packet that comes from a particular IP and with a destination port number 23.

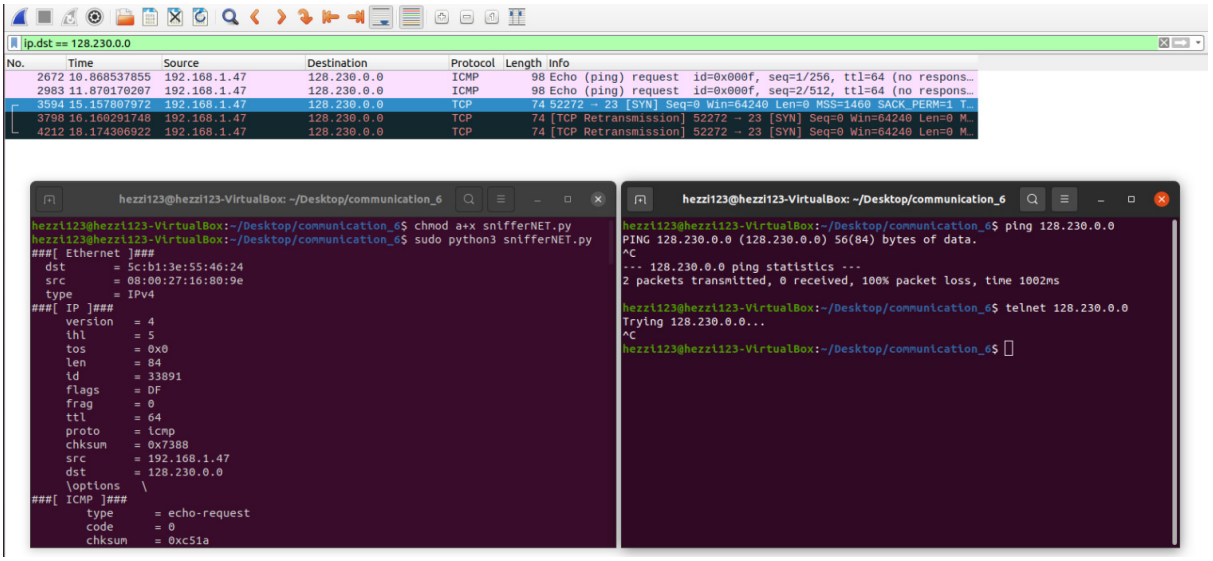


הקוד

```python
#!/usr/bin/env python3
from scapy.all import *

def print_pkt(pkt):
  pkt.show()

pkt = sniff(iface='enp0s3', filter='tcp and src host 192.168.1.47 and dst port 23', prn=print_pkt)
```

particular subnet(128.230.0.0):

Capture packets comes from or to go to a particular subnet.

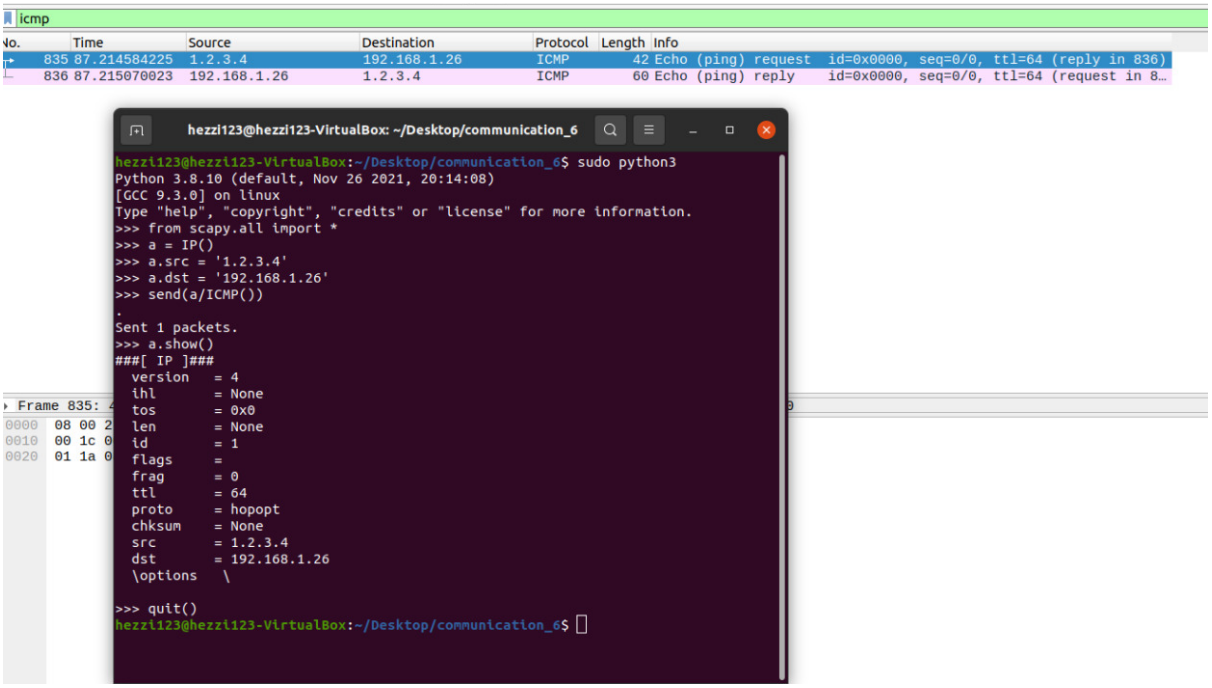


הקוד

```python
#!/usr/bin/env python3
from scapy.all import *

def print_pkt(pkt):
  pkt.show()

pkt = sniff(iface='enp0s3', filter='net 128.230.0.0/16', prn=print_pkt)
```

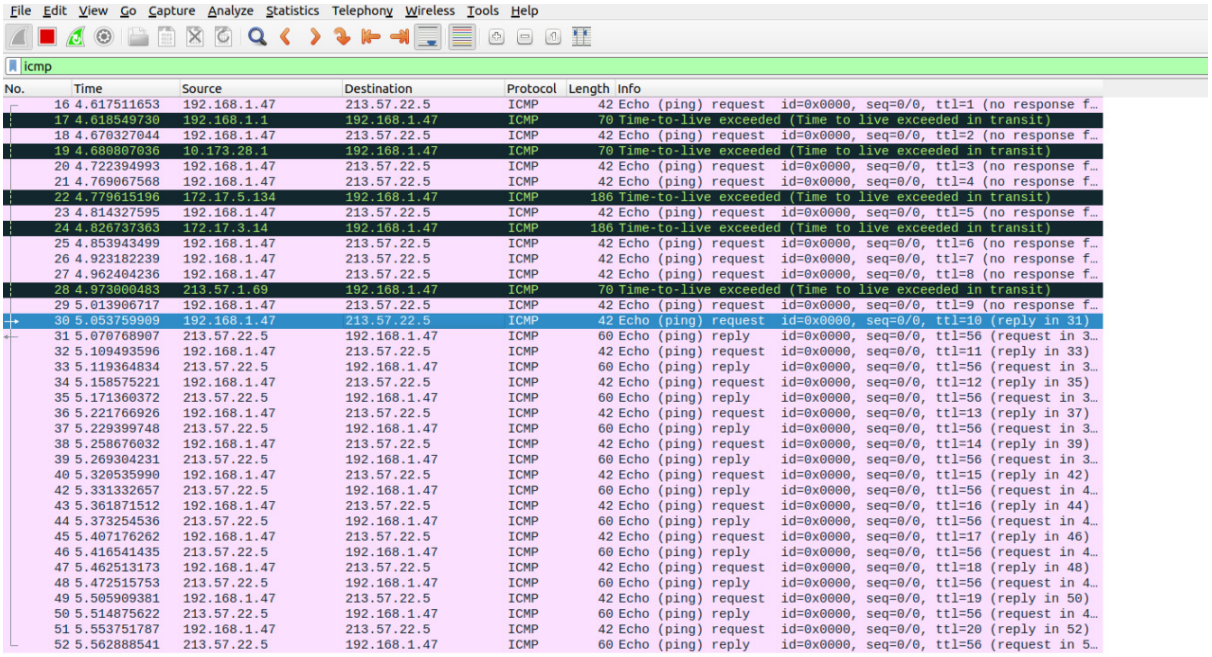
-1.2

פתחנו שני VM, הכתובת IP של המכונה הראשונה הינה 192.168.1.47 ושל השנייה הינה 192.169.1.26. השתמשנו במכונה השנייה כדי לשלוח ICMP packet עם ip מזויף (1.2.3.4). עשינו spoof ושלחנו למכונה הראשונה שנמצאת על אותה התת-רשת.

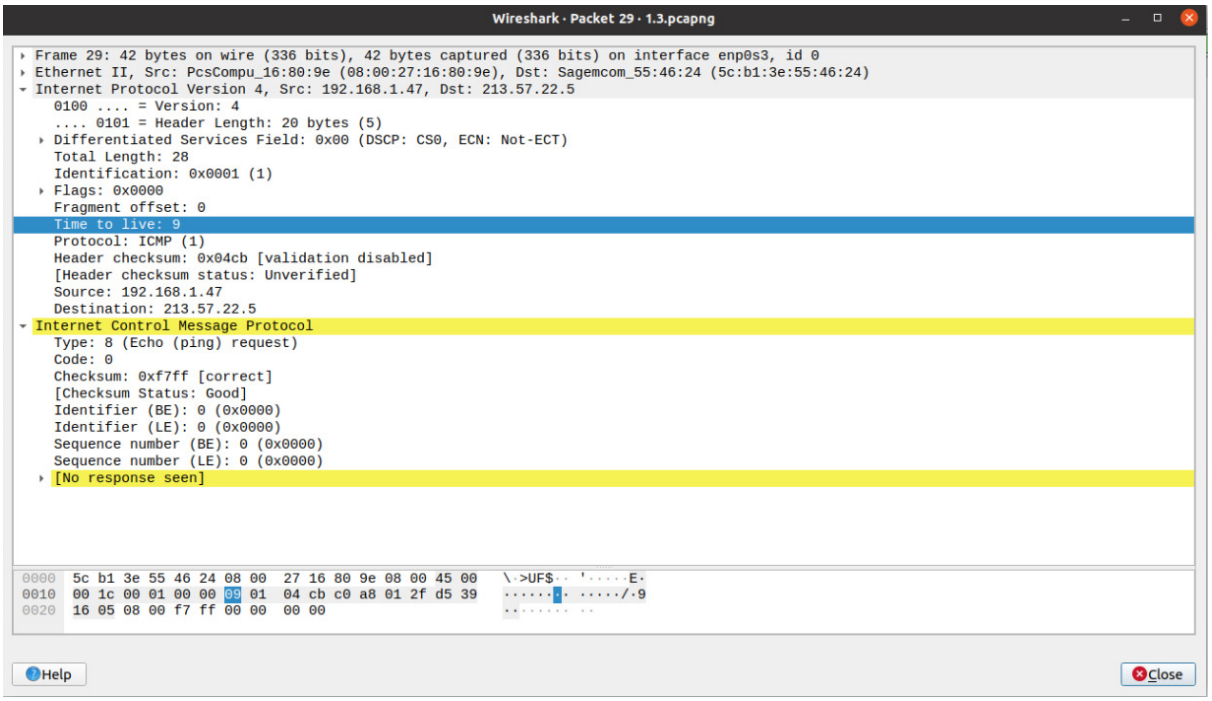


-1.3

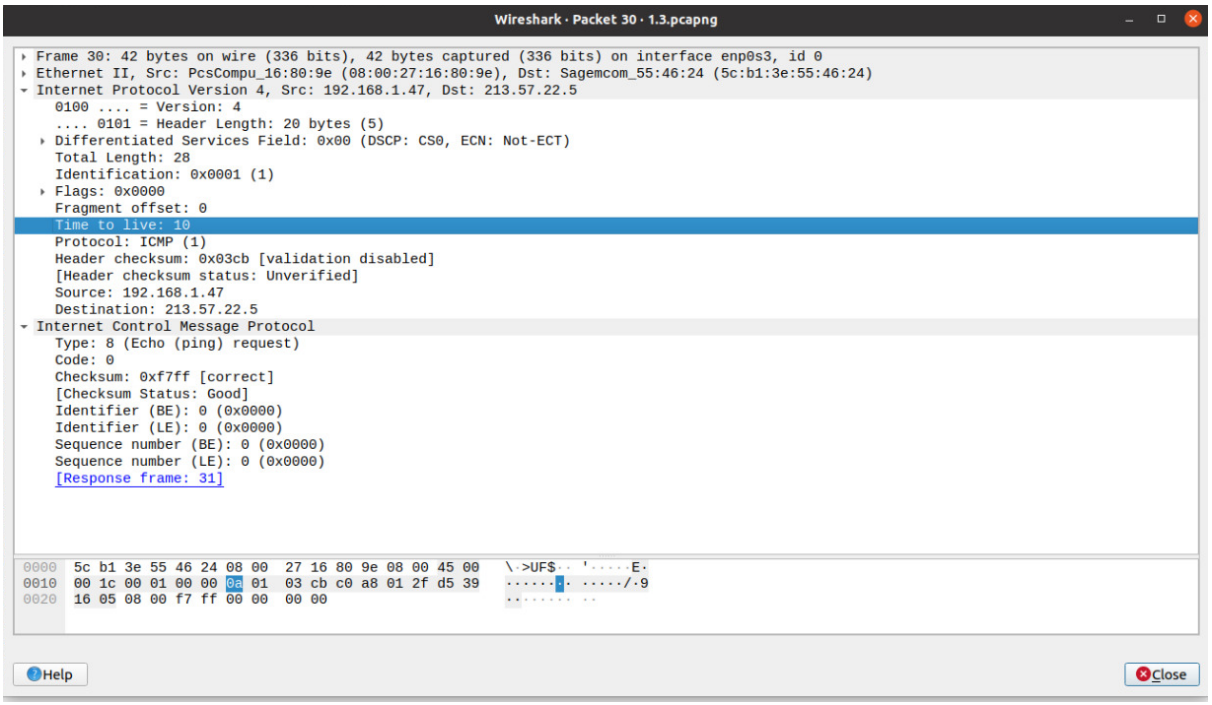
שלחנו 20 פעמים הודעת פינג עם TTL עם 1 עד 20 (כל הודעת פינג עם TTL שונה וגדול באחד מקודמו).



ב9=TTL לא קיבלנו reply.



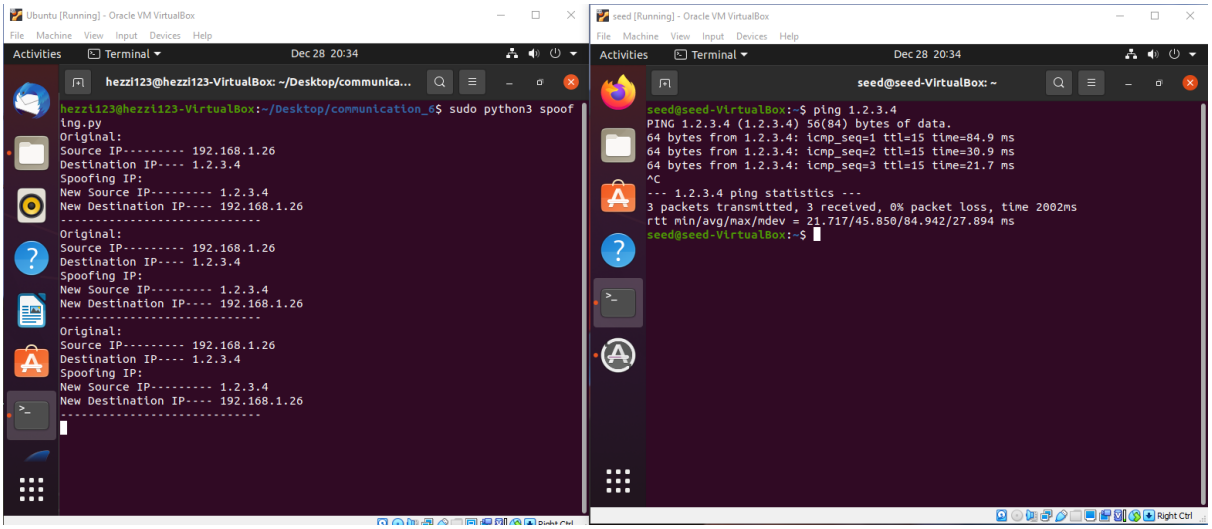
ב10=TTL קיבלנו reply.

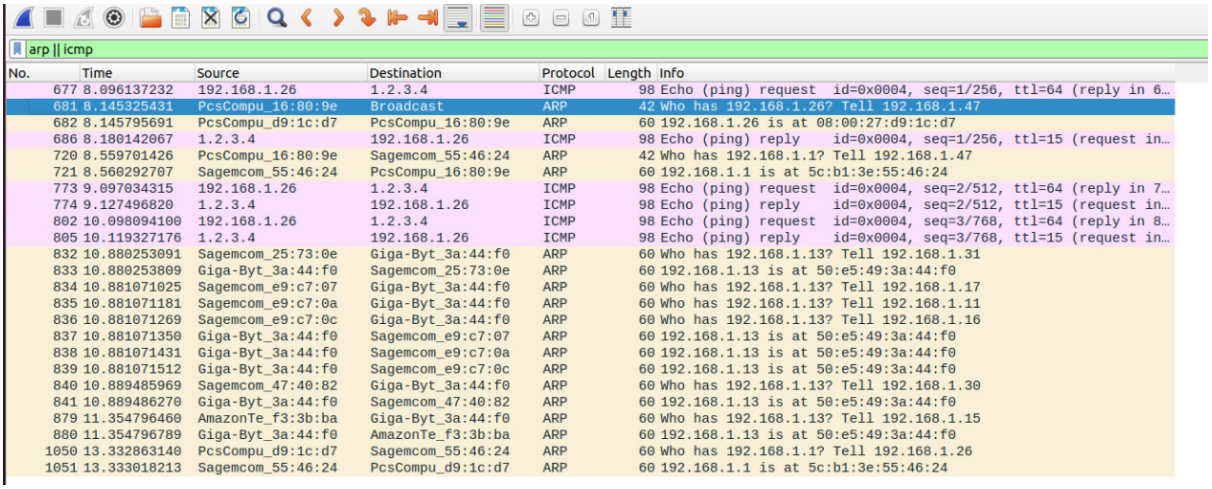


-1.4

ping 1.2.3.4:

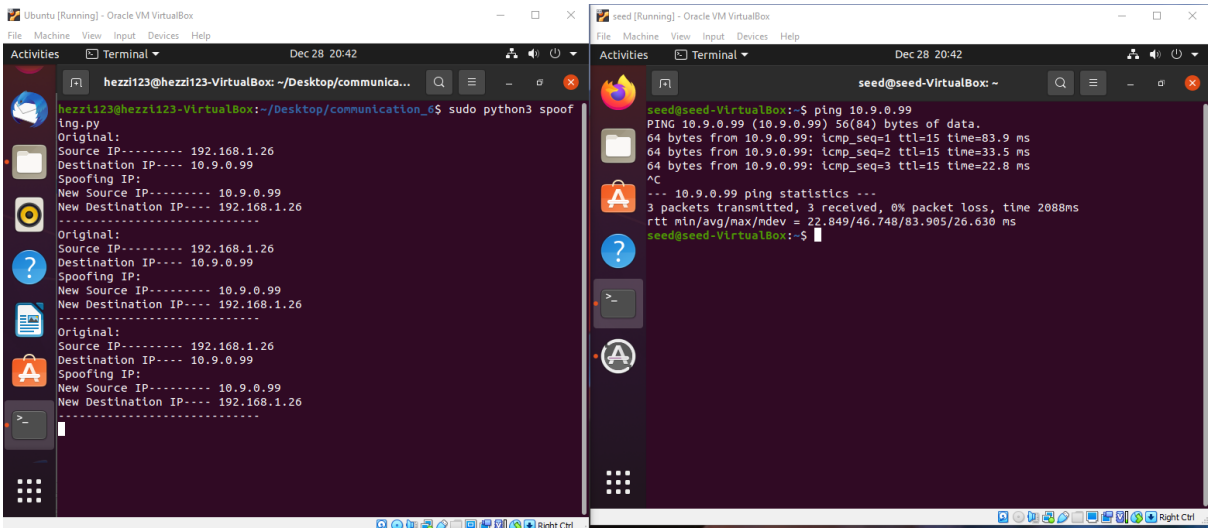
המVM השנייה שולחת פינג ל1.2.3.4 אבל בגלל שהכתובת לא קיימת ברשת האינטרנט הודעת ARP יוצאת מהרשת המקומית והVM הראשונה עושה sniff ואז spoof.

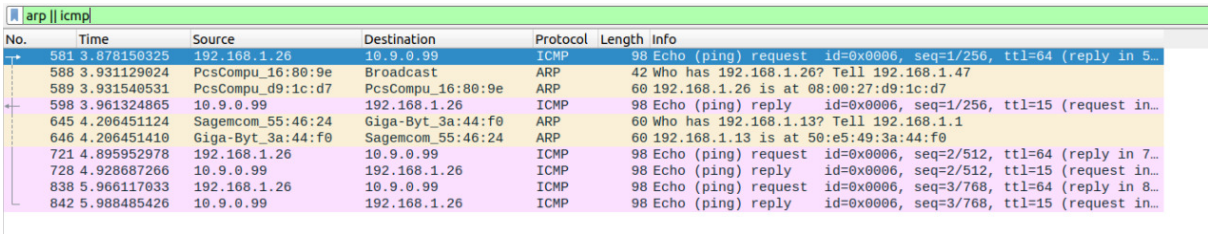




ping 10.9.0.99:

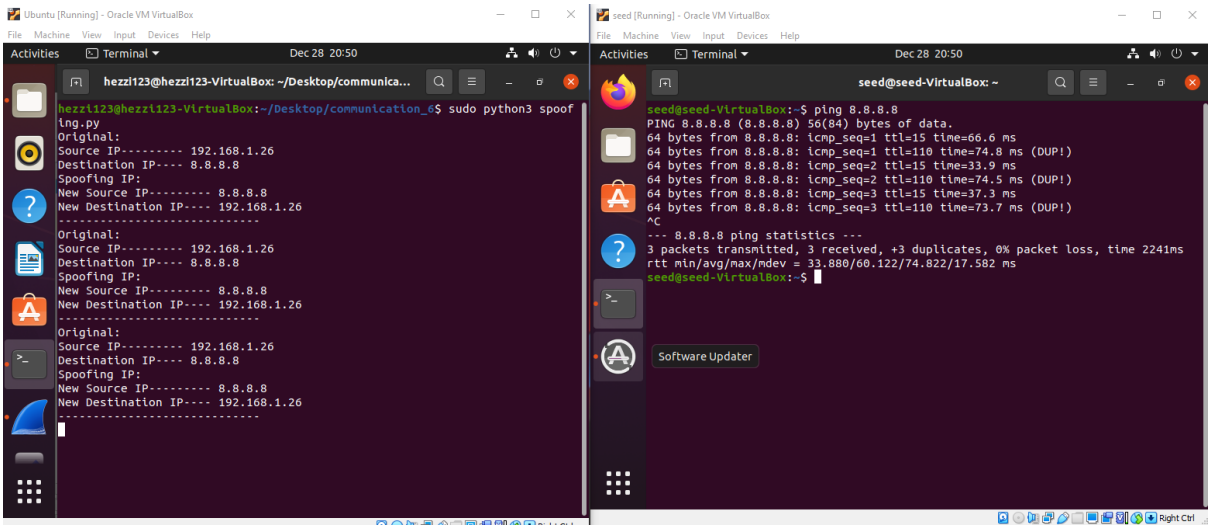
המVM השנייה שולחת פינג ל10.9.0.99 אבל בגלל שהכתובת לא קיימת ברשת המקומית ההודעת ARP יוצאת מהרשת המקומית והVM השנייה עושה sniff ואז spoof(בדומה לסעיף הקודם שבו שלחנו לכתובת שלא קיימת באינטרנט).

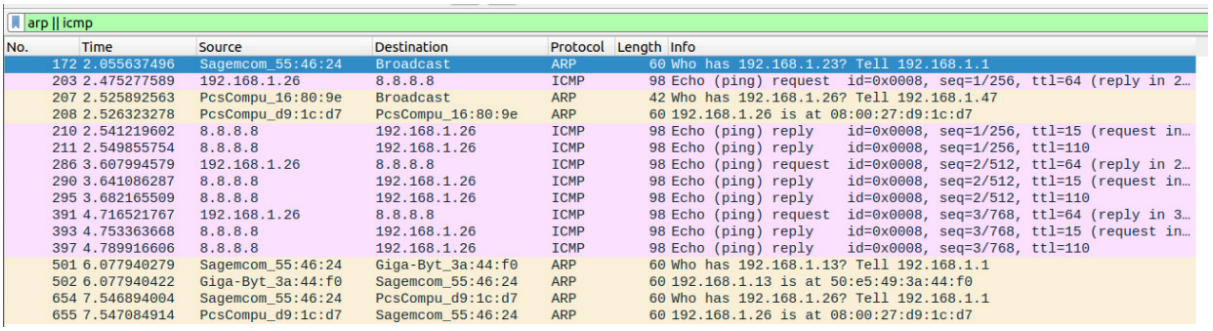




ping 8.8.8.8:

הVM השנייה שולחת פינג ל8.8.8.8 ובגלל שהכתובת הזאת קיימת אז בניגוד לכתובות שלא קיימות, פה אנחנו מקבלים כמה תשובות (אחד מהכתובת 8.8.8.8 ואחת מהVM השנייה). וזה בעצם הDUP! שניתן לראות בתמונה שצירפנו למטה.





חלק 2:

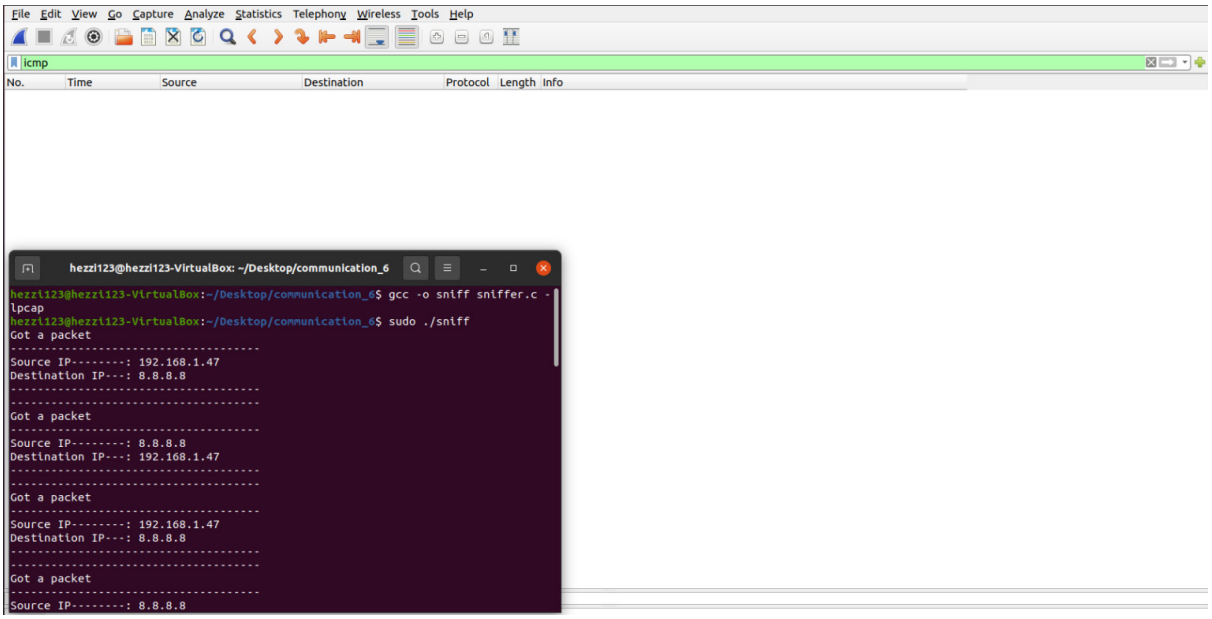
2.1A-

שאלה 1: פותחים סשן של pcap שיפתח לנו raw-socket דרכו נסניף. נגדיר את הממשק שנרצה, כמות הדאטא שנקבל, וכל כמה זמן נקבל דאטא ומבנה נתונים שיקבל שגיאות. בנוסף נגדיר שאנחנו נכנסים למצב מופקר כדי שנעשה sniff לכל התעבורה ולא רק מה שברשת שלנו. נגדיר את הפילטר הרצוי.

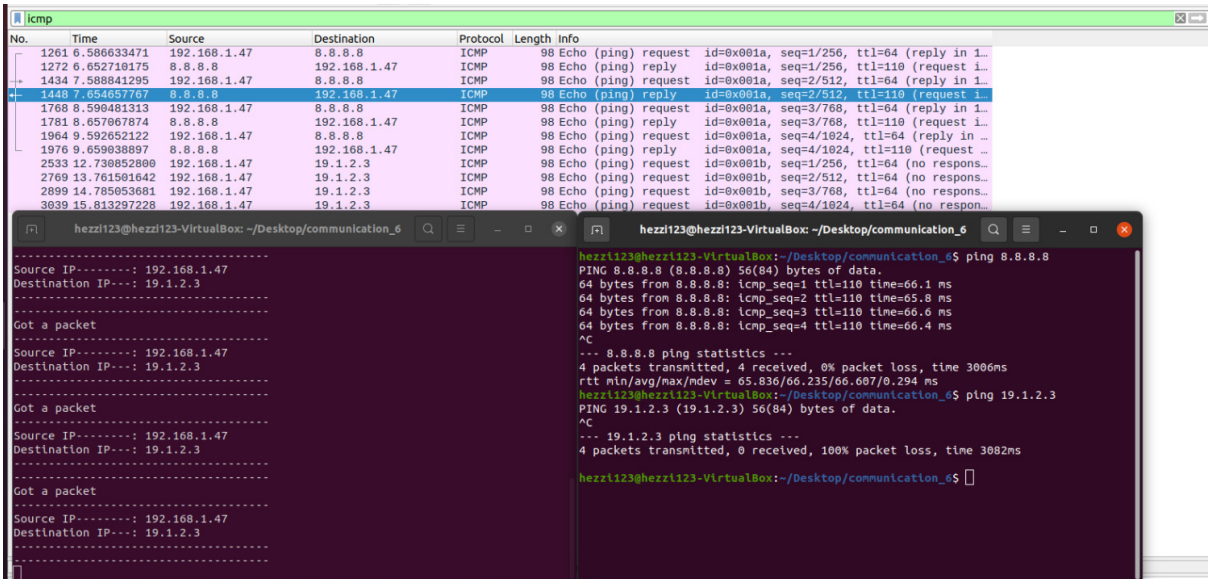
שאלה 2: נצטרך הרשאה בשביל לעשות sniff, אחרת נקבל שגיאה כמו בחלק אחד של המטלה.

שאלה 3: כאשר המספר הוא 0 אז אנחנו עושים sniff רק למה שנשלח אלינו ואילו כאשר המספר הוא 1 אז אנחנו עושים sniff לכל התעבורה ברשת.

כאן אנחנו עושים ping.



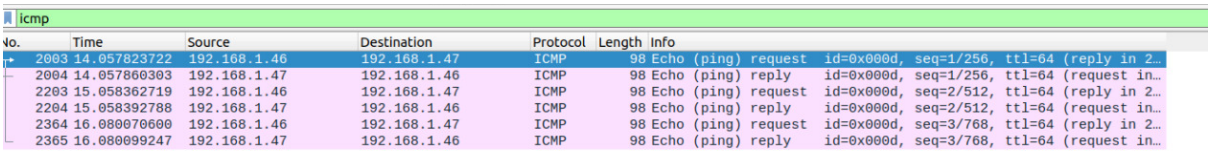
כאן ניתן לראות את התעבורה.

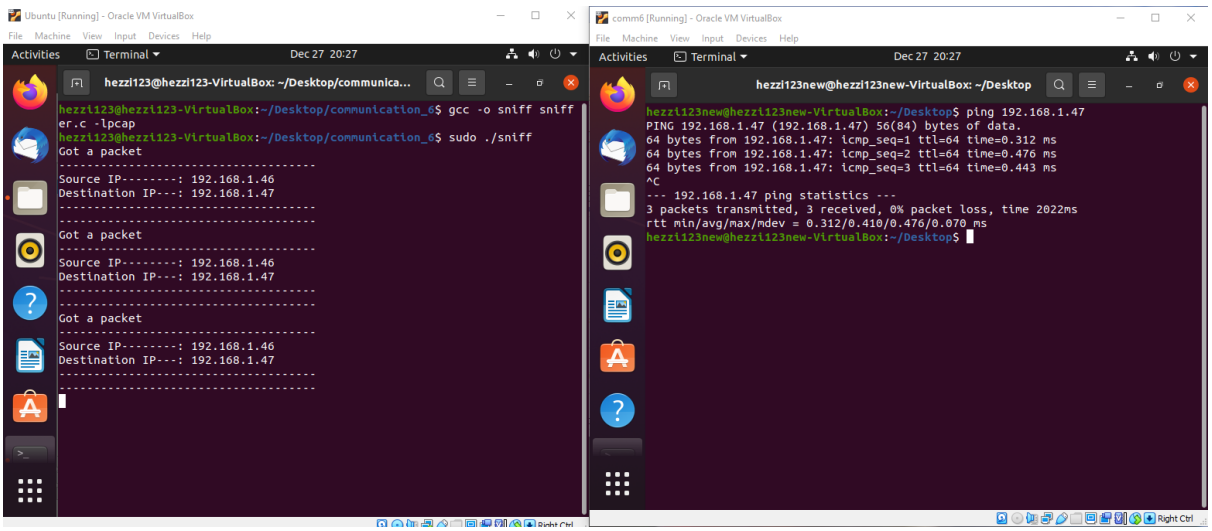


-2.1B

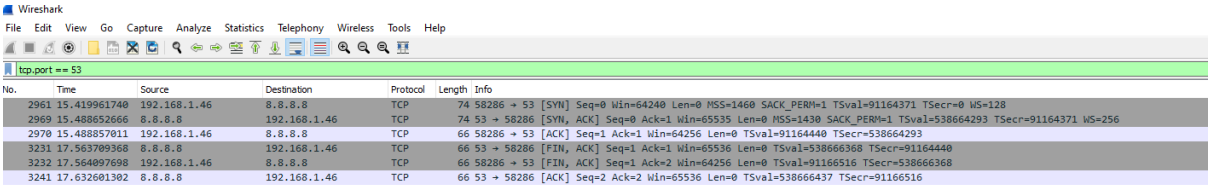
ההבדל בקוד הוא שורה אחת בmain: `char filter_exp[] =`
ובעזרת מכונה חדשה שכתובת הIP שלה הינה 192.168.1.46
כל פעם רוצים לפי מה שאנחנו רוצים להסניף.

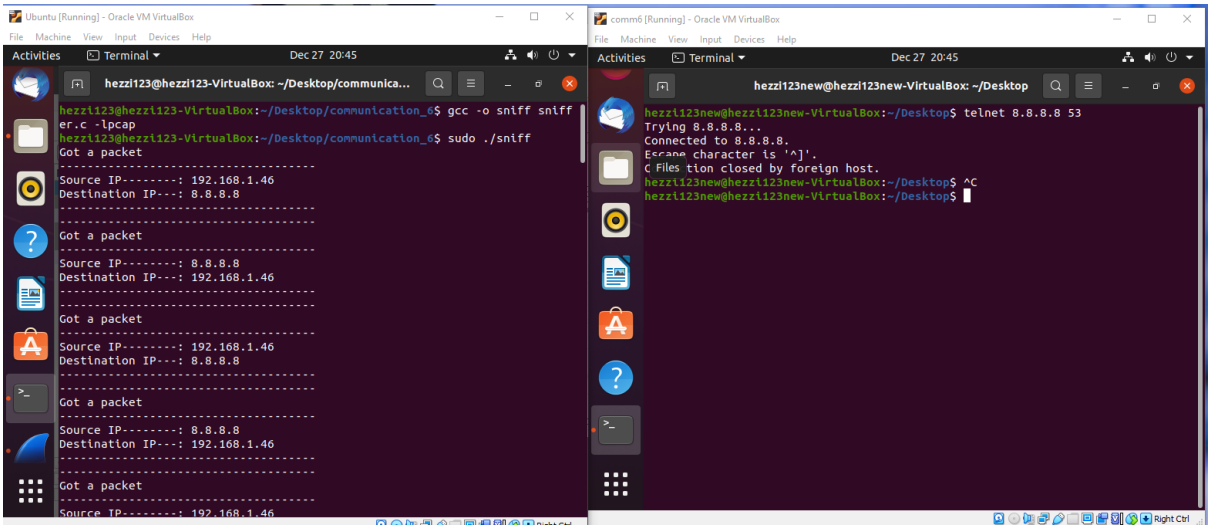
Between two specific hosts:



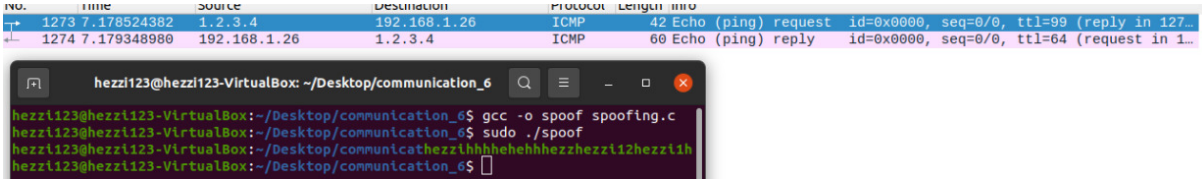


With a destination port number in the range from 10 to 100:





<u>2.2A&2.2B-</u> שלחנו פקטות ICMP מכתובת 192.168.1.47 לכתוב 192.168.1.26 אבל השתמשנו בכתובת מזויפת 1.2.3.4.



<u>שאלה 4-</u> כן,ניתן להגדיר את השדה במספר שרירותי, בגלל שלאחר מכן הגודל משתנה לגודל האמיתי, למרות מה שהגדרנו בשדה.

<u>שאלה 5-</u> לא, מערכת ההפעלה תעשה את זה בשבילנו אם ip_check = 0 בip header (זה הערך הדיפולטיבי).

שאלה 6- נצטרך root privilege בשביל לקבל הרשאה להריץ raw socket ולשנות מידע בתוך החבילות. אם נריץ ללא root privilege התוכנית תסתיים בשגיאה. הודעת השגיאה תהיה שאין לנו permission. השגיאה תהיה כאשר ננסה ליצור את הsocket.

2.3- הרצנו את התוכנית ממכונה אחת ועשינו sniffing ממכונה שנייה ואז spoofing (שינינו את כתובת הsrc לכתובת לא קיימת 1.2.3.4).