

תקשורת ומחשב מטלה 6

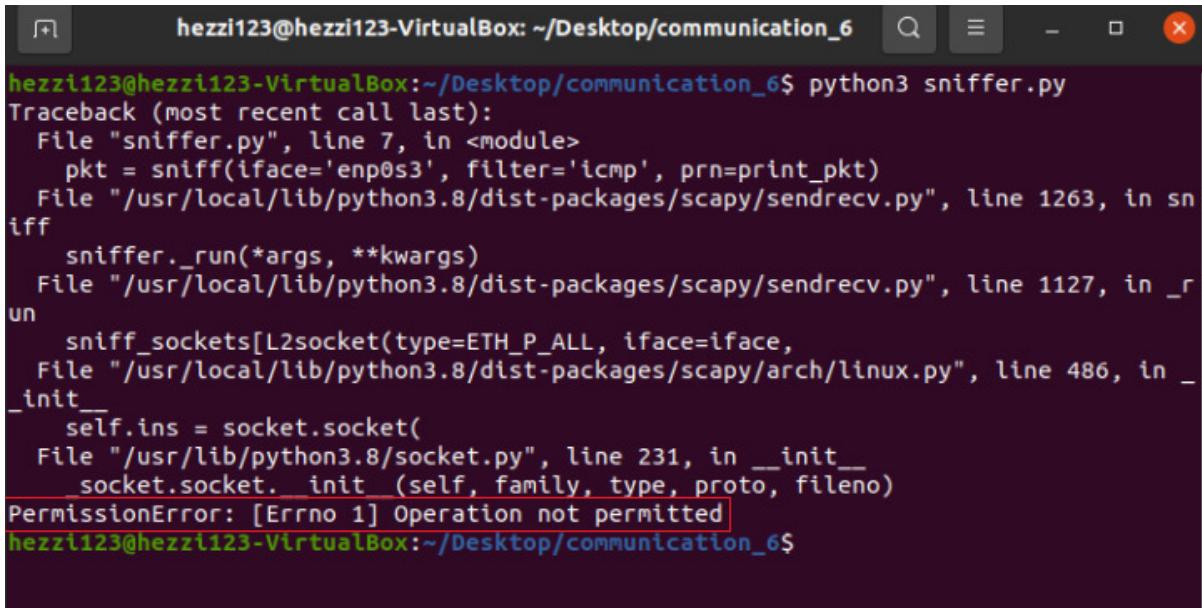
חלק 1

-1.1A

הקוד

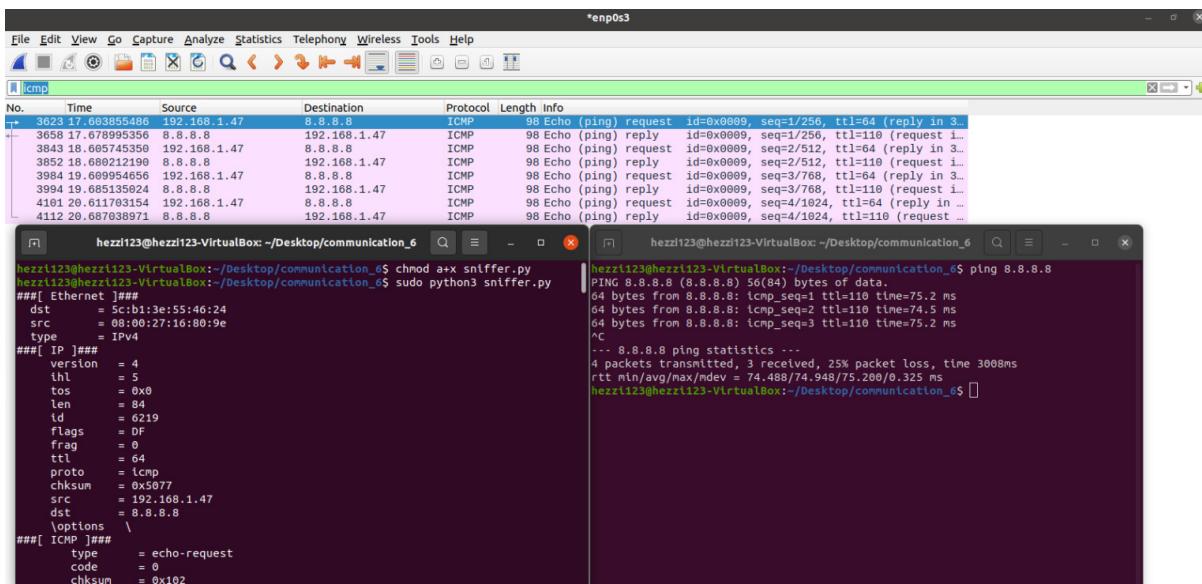
```
1 #!/usr/bin/env python3
2 from scapy.all import *
3
4 def print_pkt(pkt):
5     pkt.show()
6
7 pkt = sniff(iface='enp0s3', filter='icmp', prn=print_pkt)
```

כשאנחנו מנוטם להריץ ללא הפקודה sudo אנחנו מקבלים שגיאה, משום שאין לנו הרשות להסניף פקודות.



```
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 sniff
    sniff_.run(*args, **kwargs)
  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$
```

כשריצים עם הפקודה sudo הפקודה רץ (בגלל שהפקודה sudo נותנת למשתמש להריץ "as root") וניתן לראות בצד ימין בתמונה שעשינו פינג ל google.com 8.8.8.8 (ובצד שמאל בתמונה ניתן לראות את החומר שלחנו האין לפקות.

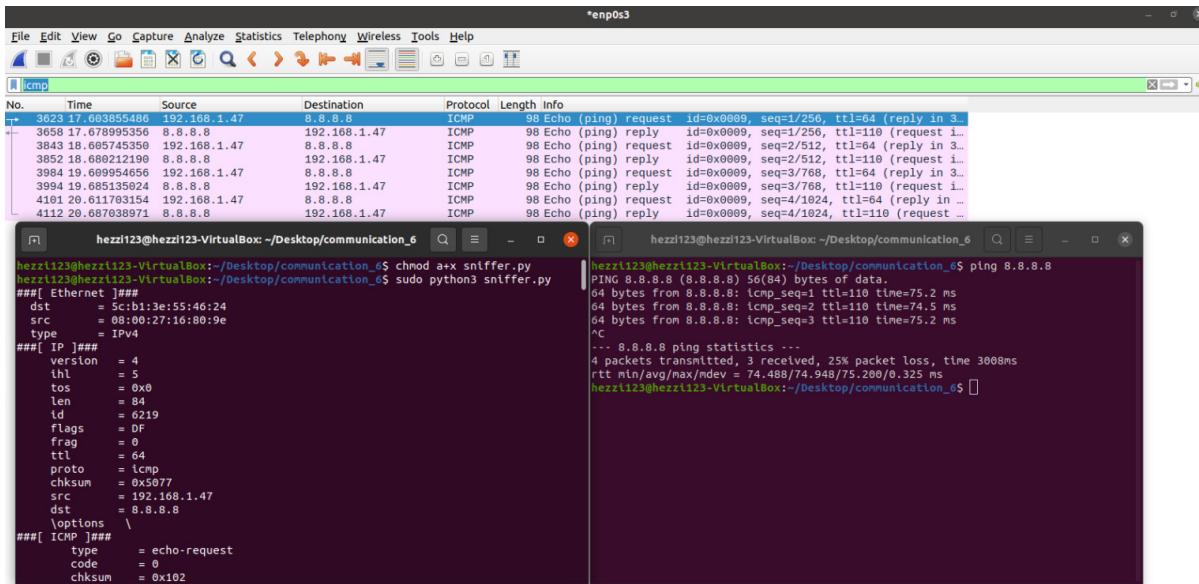


The Wireshark interface shows captured ICMP traffic between two hosts on the enp0s3 interface. The traffic consists of ICMP Echo requests (ping) from 192.168.1.47 to 8.8.8.8, and ICMP Echo replies from 8.8.8.8 back to 192.168.1.47. The terminal window shows the command `ping 8.8.8.8` being run, which returns statistics for 4 transmitted packets with 0% loss and a round-trip time of 3008ms.

-1.1B

ICMP:

Capture only the ICMP packet

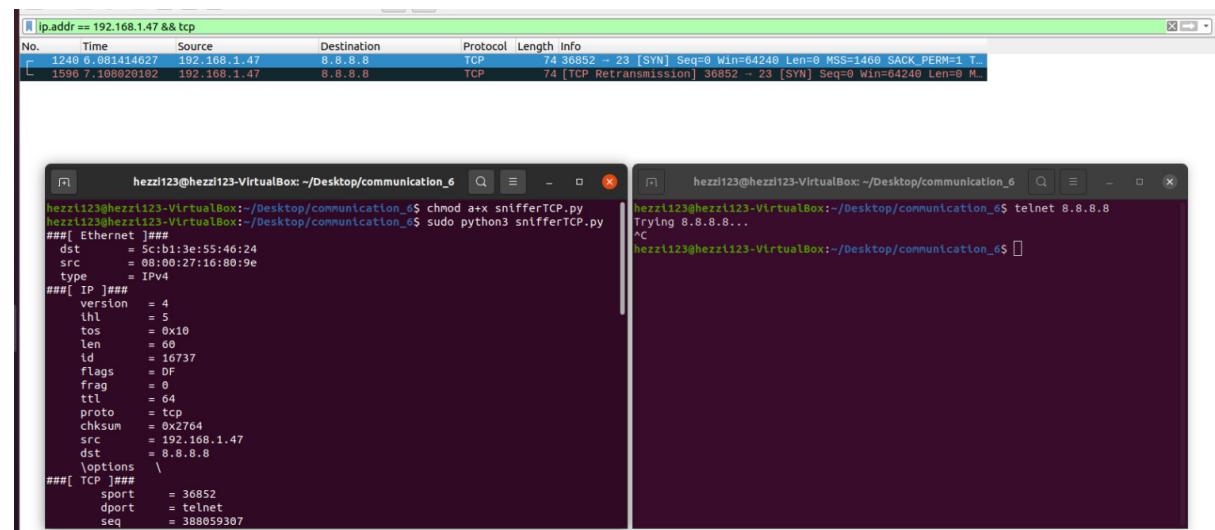


Tip

```
1#!/usr/bin/env python3
2from scapy.all import *
3
4def print_pkt(pkt):
5    pkt.show()
6
7pkt = 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.

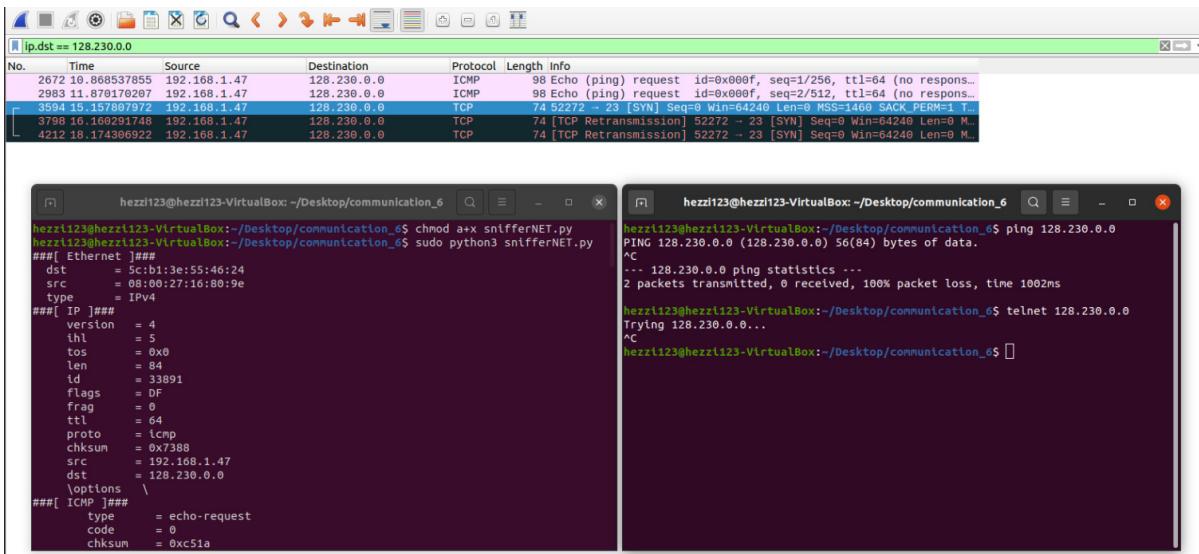


הקווד

```
1#!/usr/bin/env python3
2from scapy.all import *
3
4def print_pkt(pkt):
5    pkt.show()
6
7pkt = 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.

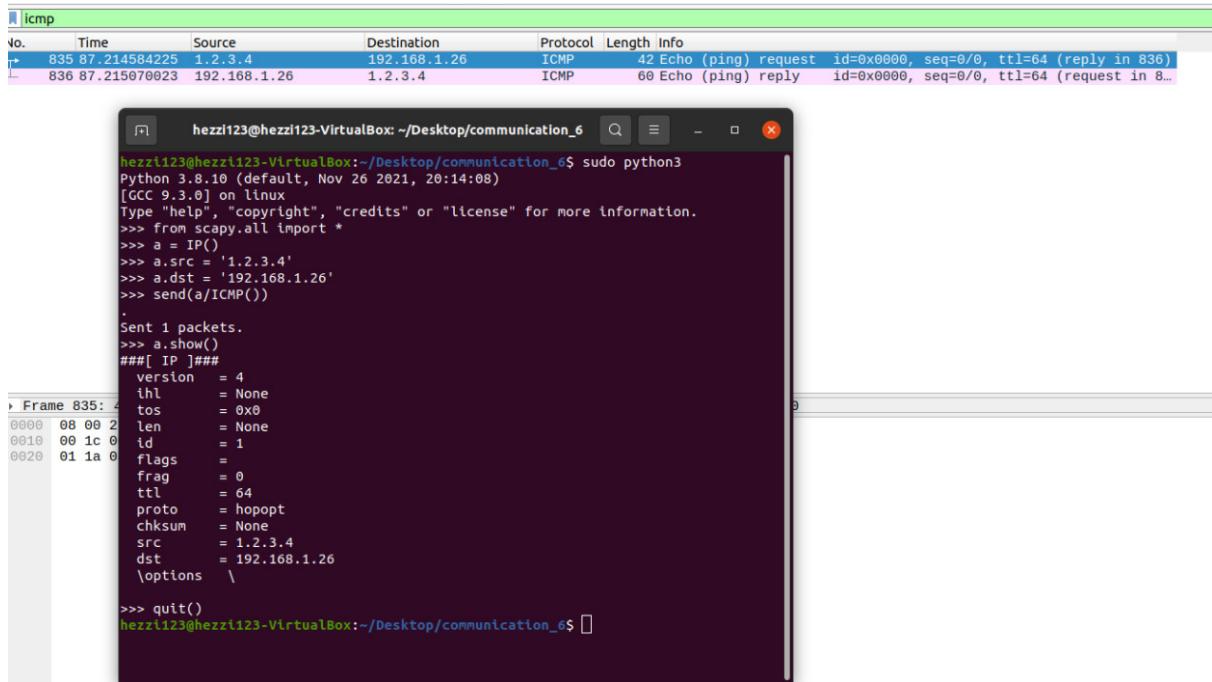


הקווד

```
1#!/usr/bin/env python3
2from scapy.all import *
3
4def print_pkt(pkt):
5    pkt.show()
6
7pkt = sniff(iface='enp0s3', filter='net 128.230.0.0/16', prn=print_pkt)
```

-1.2

פתחנו שני VM, הכתובת IP של המcona 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 התח-רשת.



-1.3

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

No.	Time	Source	Destination	Protocol	Length	Info
16	4.617511653	192.168.1.47	213.57.22.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=1 (no response f...
17	4.618549738	192.168.1.1	192.168.1.47	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
18	4.670327044	192.168.1.47	213.57.22.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=2 (no response f...
19	4.680867036	10.173.28.1	192.168.1.47	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
20	4.722394993	192.168.1.47	213.57.22.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=3 (no response f...
21	4.769067568	192.168.1.47	213.57.22.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=4 (no response f...
22	4.779615196	172.17.5.134	192.168.1.47	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
23	4.814327595	192.168.1.47	213.57.22.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=5 (no response f...
24	4.828737363	172.17.3.14	192.168.1.47	ICMP	186	Time-to-live exceeded (Time to live exceeded in transit)
25	4.853943499	192.168.1.47	213.57.22.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=6 (no response f...
26	4.923182239	192.168.1.47	213.57.22.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=7 (no response f...
27	4.962464236	192.168.1.47	213.57.22.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=8 (no response f...
28	4.973000483	213.57.1.69	192.168.1.47	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
29	5.013906717	192.168.1.47	213.57.22.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=9 (no response f...
30	5.053759999	192.168.1.47	213.57.22.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=10 (reply in 31)
31	5.070768907	213.57.22.5	192.168.1.47	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=56 (request in 3...
32	5.109493596	192.168.1.47	213.57.22.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=11 (reply in 33)
33	5.119364834	213.57.22.5	192.168.1.47	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=56 (request in 3...
34	5.158575221	192.168.1.47	213.57.22.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=12 (reply in 35)
35	5.171366372	213.57.22.5	192.168.1.47	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=56 (request in 3...
36	5.221766926	192.168.1.47	213.57.22.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=13 (reply in 37)
37	5.229399748	213.57.22.5	192.168.1.47	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=56 (request in 3...
38	5.258670632	192.168.1.47	213.57.22.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=14 (reply in 39)
39	5.269304231	213.57.22.5	192.168.1.47	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=56 (request in 3...
40	5.320535990	192.168.1.47	213.57.22.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=15 (reply in 42)
42	5.331332657	213.57.22.5	192.168.1.47	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=56 (request in 4...
43	5.361871512	192.168.1.47	213.57.22.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=16 (reply in 44)
44	5.373254536	213.57.22.5	192.168.1.47	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=56 (request in 4...
45	5.407176262	192.168.1.47	213.57.22.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=17 (reply in 46)
46	5.416541435	213.57.22.5	192.168.1.47	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=56 (request in 4...
47	5.462513173	192.168.1.47	213.57.22.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=18 (reply in 48)
48	5.472515753	213.57.22.5	192.168.1.47	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=56 (request in 4...
49	5.505909381	192.168.1.47	213.57.22.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=19 (reply in 50)
50	5.514875622	213.57.22.5	192.168.1.47	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=56 (request in 4...
51	5.553751787	192.168.1.47	213.57.22.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=20 (reply in 52)
52	5.562888541	213.57.22.5	192.168.1.47	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=56 (request in 5...

ב9=TTL לא קיבלנו reply.

Wireshark - Packet 29 · 1.3.pcapng

Frame 29: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_16:80:9e (08:00:27:16:80:9e), Dst: Sagemcom_55:46:24 (5c:b1:3e:55:46:24)
Internet Protocol Version 4, Src: 192.168.1.47, Dst: 213.57.22.5
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 28
Identification: 0x0001 (1)
Flags: 0x0000
Fragment offset: 0
Time to live: 9
Protocol: ICMP (1)
Header checksum: 0x04cb [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.47
Destination: 213.57.22.5
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf7ff [correct]
[Checksum Status: Good]
Identifier (BE): 0 (0x0000)
Identifier (LE): 0 (0x0000)
Sequence number (BE): 0 (0x0000)
Sequence number (LE): 0 (0x0000)
[No response seen]

0000 5c b1 3e 55 46 24 08 00 27 16 80 9e 08 00 45 00 \->UF\$.. '.....E.
0010 00 1c 00 01 00 00 0a 01 04 cb c0 a8 01 2f d5 39#...../.9
0020 16 05 08 00 f7 ff 00 00 00 00

Help Close

ב10=TTL קיבלנו reply.

Wireshark - Packet 30 · 1.3.pcapng

Frame 30: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_16:80:9e (08:00:27:16:80:9e), Dst: Sagemcom_55:46:24 (5c:b1:3e:55:46:24)
Internet Protocol Version 4, Src: 192.168.1.47, Dst: 213.57.22.5
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 28
Identification: 0x0001 (1)
Flags: 0x0000
Fragment offset: 0
Time to live: 10
Protocol: ICMP (1)
Header checksum: 0x03cb [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.47
Destination: 213.57.22.5
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf7ff [correct]
[Checksum Status: Good]
Identifier (BE): 0 (0x0000)
Identifier (LE): 0 (0x0000)
Sequence number (BE): 0 (0x0000)
Sequence number (LE): 0 (0x0000)
[Response frame: 31]

0000 5c b1 3e 55 46 24 08 00 27 16 80 9e 08 00 45 00 \->UF\$.. '.....E.
0010 00 1c 00 01 00 00 0a 01 03 cb c0 a8 01 2f d5 39#...../.9
0020 16 05 08 00 f7 ff 00 00 00 00

Help Close

-1.4

ping 1.2.3.4:

הVM השנייה שולחת פינג ל-1.2.3.4 אבל בגלל שהכתובת לא קיימת ברשף האינטרנט הודעת ARP יוצאת מהרשף המקומיית והVM הראשונה עושה sniff וזו spoof.

```

Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Dec 28 20:34
hezz123@hezz123-VirtualBox: ~/Desktop/communication_e$ sudo python3 spoofing.py
Original:
Source IP----- 192.168.1.26
Destination IP--- 1.2.3.4
Spoofing IP:
New Source IP----- 1.2.3.4
New Destination IP--- 192.168.1.26
-----
Original:
Source IP----- 192.168.1.26
Destination IP--- 1.2.3.4
Spoofing IP:
New Source IP----- 1.2.3.4
New Destination IP--- 192.168.1.26
-----
Original:
Source IP----- 192.168.1.26
Destination IP--- 1.2.3.4
Spoofing IP:
New Source IP----- 1.2.3.4
New Destination IP--- 192.168.1.26
-----
Original:
Source IP----- 192.168.1.26
Destination IP--- 1.2.3.4
Spoofing IP:
New Source IP----- 1.2.3.4
New Destination IP--- 192.168.1.26
-----

seed@seed-VirtualBox: ~
seed@seed-VirtualBox: ~$ ping 1.2.3.4
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
64 bytes from 1.2.3.4: icmp_seq=1 ttl=15 time=84.9 ms
64 bytes from 1.2.3.4: icmp_seq=2 ttl=15 time=30.9 ms
64 bytes from 1.2.3.4: icmp_seq=3 ttl=15 time=21.7 ms
^C
--- 1.2.3.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 21.717/45.850/84.942/27.894 ms
seed@seed-VirtualBox: ~$ 

```

No.	Time	Source	Destination	Protocol	Length	Info
677	8.096137232	192.168.1.26	1.2.3.4	ICMP	98	Echo (ping) request id=0x0004, seq=1/256, ttl=64 (reply in 6...
681	8.145325431	PcsCompu_16:80:9e	Broadcast	ARP	42	Who has 192.168.1.26? Tell 192.168.1.47
682	8.145795691	PcsCompu_d9:1c:d7	PcsCompu_16:80:9e	ARP	60	192.168.1.26 is at 08:00:27:d9:1c:d7
686	8.180142967	1.2.3.4	192.168.1.26	ICMP	98	Echo (ping) reply id=0x0004, seq=1/256, ttl=15 (request in...
720	8.559701426	PcsCompu_16:80:9e	Sagemcom_55:46:24	ARP	42	Who has 192.168.1.1? Tell 192.168.1.147
721	8.566292707	Sagemcom_55:46:24	PcsCompu_16:80:9e	ARP	60	192.168.1.1 is at 5c:b1:3e:55:46:24
773	9.097034315	192.168.1.26	1.2.3.4	ICMP	98	Echo (ping) request id=0x0004, seq=2/512, ttl=64 (reply in 7...
774	9.127496820	1.2.3.4	192.168.1.26	ICMP	98	Echo (ping) reply id=0x0004, seq=2/512, ttl=15 (request in...
882	10.098094100	192.168.1.26	1.2.3.4	ICMP	98	Echo (ping) request id=0x0004, seq=3/768, ttl=64 (reply in 8...
885	10.119327176	1.2.3.4	192.168.1.26	ICMP	98	Echo (ping) reply id=0x0004, seq=3/768, ttl=15 (request in...
832	10.880253091	Sagemcom_25:73:0e	Giga-Byt_3a:44:f0	ARP	60	Who has 192.168.1.13? Tell 192.168.1.31
833	10.880253809	Giga-Byt_3a:44:f0	Sagemcom_25:73:0e	ARP	60	192.168.1.13 is at 50:e5:49:3a:44:f0
834	10.881071025	Sagemcom_e9:c7:07	Giga-Byt_3a:44:f0	ARP	60	Who has 192.168.1.13? Tell 192.168.1.17
835	10.881071181	Sagemcom_e9:c7:08	Giga-Byt_3a:44:f0	ARP	60	Who has 192.168.1.13? Tell 192.168.1.11
836	10.881071269	Sagemcom_e9:c7:0c	Giga-Byt_3a:44:f0	ARP	60	Who has 192.168.1.13? Tell 192.168.1.16
837	10.881071350	Giga-Byt_3a:44:f0	Sagemcom_e9:c7:07	ARP	60	192.168.1.13 is at 50:e5:49:3a:44:f0
838	10.881071431	Giga-Byt_3a:44:f0	Sagemcom_e9:c7:0a	ARP	60	192.168.1.13 is at 50:e5:49:3a:44:f0
839	10.881071512	Giga-Byt_3a:44:f0	Sagemcom_e9:c7:0c	ARP	60	192.168.1.13 is at 50:e5:49:3a:44:f0
840	10.889485969	Sagemcom_47:40:82	Giga-Byt_3a:44:f0	ARP	60	Who has 192.168.1.13? Tell 192.168.1.30
841	10.889486270	Giga-Byt_3a:44:f0	Sagemcom_47:40:82	ARP	60	192.168.1.13 is at 50:e5:49:3a:44:f0
879	11.354796460	AmazonTe_f3:3b:ba	Giga-Byt_3a:44:f0	ARP	60	Who has 192.168.1.13? Tell 192.168.1.15
880	11.354796789	Giga-Byt_3a:44:f0	AmazonTe_f3:3b:ba	ARP	60	192.168.1.13 is at 50:e5:49:3a:44:f0
1050	13.332863140	PcsCompu_d9:1c:d7	Sagemcom_55:46:24	ARP	60	Who has 192.168.1.1? Tell 192.168.1.26
1051	13.333018213	PcsCompu_d9:1c:d7	Sagemcom_55:46:24	ARP	60	192.168.1.1 is at 5c:b1:3e:55:46:24

ping 10.9.0.99:

הVM השנייה שולחת פינג לאבל בגל שהכתובת לא קיימת בראש המוקומית הודעתו יצאת מהרשת המקומיית והVM השנייה עושה sniff ואז spoof(בדומה לסעיף הקודם שבו שלחנו לכתובת שלא קיימת באינטרנט).

```

Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Dec 28 20:42
hezz123@hezz123-VirtualBox: ~/Desktop/communication_6$ sudo python3 spoofing.py
Original:
Source IP----- 192.168.1.26
Destination IP--- 10.9.0.99
Spoofing IP:
New Source IP----- 10.9.0.99
New Destination IP--- 192.168.1.26
-----
Original:
Source IP----- 192.168.1.26
Destination IP--- 10.9.0.99
Spoofing IP:
New Source IP----- 10.9.0.99
New Destination IP--- 192.168.1.26
-----
Original:
Source IP----- 192.168.1.26
Destination IP--- 10.9.0.99
Spoofing IP:
New Source IP----- 10.9.0.99
New Destination IP--- 192.168.1.26
-----

seed@seed-VirtualBox: ~
seed@seed-VirtualBox: ~$ ping 10.9.0.99
PING 10.9.0.99 (10.9.0.99) 56(84) bytes of data.
64 bytes from 10.9.0.99: icmp_seq=1 ttl=15 time=83.9 ms
64 bytes from 10.9.0.99: icmp_seq=2 ttl=15 time=33.5 ms
64 bytes from 10.9.0.99: icmp_seq=3 ttl=15 time=22.8 ms
^C
--- 10.9.0.99 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2088ms
rtt min/avg/max/mdev = 22.849/46.748/83.905/26.630 ms
seed@seed-VirtualBox: ~$ 

```

No.	Time	Source	Destination	Protocol	Length	Info
581	3.878150325	192.168.1.26	10.9.0.99	ICMP	98	Echo (ping) request id=0x0006, seq=1/256, ttl=64 (reply in 5..)
588	3.931129624	PcsCompu_16:80:9e	Broadcast	ARP	42	Who has 192.168.1.26? Tell 192.168.1.47
589	3.931540531	PcsCompu_d9:1c:d7	PcsCompu_16:80:9e	ARP	60	192.168.1.26 is at 08:00:27:d9:1c:d7
598	3.961324865	10.9.0.99	192.168.1.26	ICMP	98	Echo (ping) reply id=0x0006, seq=1/256, ttl=15 (request in..)
645	4.206451124	Sagemcom_55:46:24	Giga-Byt_3a:44:f0	ARP	60	Who has 192.168.1.13? Tell 192.168.1.1
646	4.206451410	Giga-Byt_3a:44:f0	Sagemcom_55:46:24	ARP	60	192.168.1.13 is at 50:e5:49:3a:44:f0
721	4.895952978	192.168.1.26	10.9.0.99	ICMP	98	Echo (ping) request id=0x0006, seq=2/512, ttl=64 (reply in 7..)
728	4.928687266	10.9.0.99	192.168.1.26	ICMP	98	Echo (ping) reply id=0x0006, seq=2/512, ttl=15 (request in..)
838	5.966117633	192.168.1.26	10.9.0.99	ICMP	98	Echo (ping) request id=0x0006, seq=3/768, ttl=64 (reply in 8..)
842	5.988485426	10.9.0.99	192.168.1.26	ICMP	98	Echo (ping) reply id=0x0006, seq=3/768, ttl=15 (request in..)

ping 8.8.8.8:

הVM השנייה שולחת פינג ל-8.8.8.8 ובגלל שהכתובות ה зат קיימת אז בኒגוד לכתובות שלא קיימות, פה אנחנו מקבלים כמה תשובות (אחד מה כתובות 8.8.8.8 ואחת מה VM השנייה). זה בעצם DUP! שניתן לראות בתמונה שצירפנו למטה.

No.	Time	Source	Destination	Protocol	Length	Info
172	2.055637496	Sagemcom_55:46:24	Broadcast	ARP	60	Who has 192.168.1.23? Tell 192.168.1.1
203	2.475277589	192.168.1.26	8.8.8.8	ICMP	98	Echo (ping) request id=0x0008, seq=1/256, ttl=64 (reply in 2..)
207	2.525892563	PcsCompu_16:80:9e	Broadcast	ARP	42	Who has 192.168.1.26? Tell 192.168.1.47
208	2.526323278	PcsCompu_d9:1c:d7	PcsCompu_16:80:9e	ARP	60	192.168.1.26 is at 08:00:27:d9:1c:d7
210	2.541219602	8.8.8.8	192.168.1.26	ICMP	98	Echo (ping) reply id=0x0008, seq=1/256, ttl=15 (request in..)
211	2.549855754	8.8.8.8	192.168.1.26	ICMP	98	Echo (ping) reply id=0x0008, seq=1/256, ttl=10
286	3.607994579	192.168.1.26	8.8.8.8	ICMP	98	Echo (ping) request id=0x0008, seq=2/512, ttl=64 (reply in 2..)
290	3.641086287	8.8.8.8	192.168.1.26	ICMP	98	Echo (ping) reply id=0x0008, seq=2/512, ttl=15 (request in..)
295	3.682165509	8.8.8.8	192.168.1.26	ICMP	98	Echo (ping) reply id=0x0008, seq=2/512, ttl=10
391	4.716521767	192.168.1.26	8.8.8.8	ICMP	98	Echo (ping) request id=0x0008, seq=3/768, ttl=64 (reply in 3..)
393	4.753363668	8.8.8.8	192.168.1.26	ICMP	98	Echo (ping) reply id=0x0008, seq=3/768, ttl=15 (request in..)
397	4.789916666	8.8.8.8	192.168.1.26	ICMP	98	Echo (ping) reply id=0x0008, seq=3/768, ttl=110
501	6.077940279	Sagemcom_55:46:24	Giga-Byt_3a:44:f0	ARP	60	Who has 192.168.1.13? Tell 192.168.1.1
502	6.077940422	Giga-Byt_3a:44:f0	Sagemcom_55:46:24	ARP	60	192.168.1.13 is at 50:e5:49:3a:44:f0
654	7.546894004	Sagemcom_55:46:24	PcsCompu_d9:1c:d7	ARP	60	Who has 192.168.1.26? Tell 192.168.1.1
655	7.547084914	PcsCompu_d9:1c:d7	Sagemcom_55:46:24	ARP	60	192.168.1.26 is at 08:00:27:d9:1c:d7

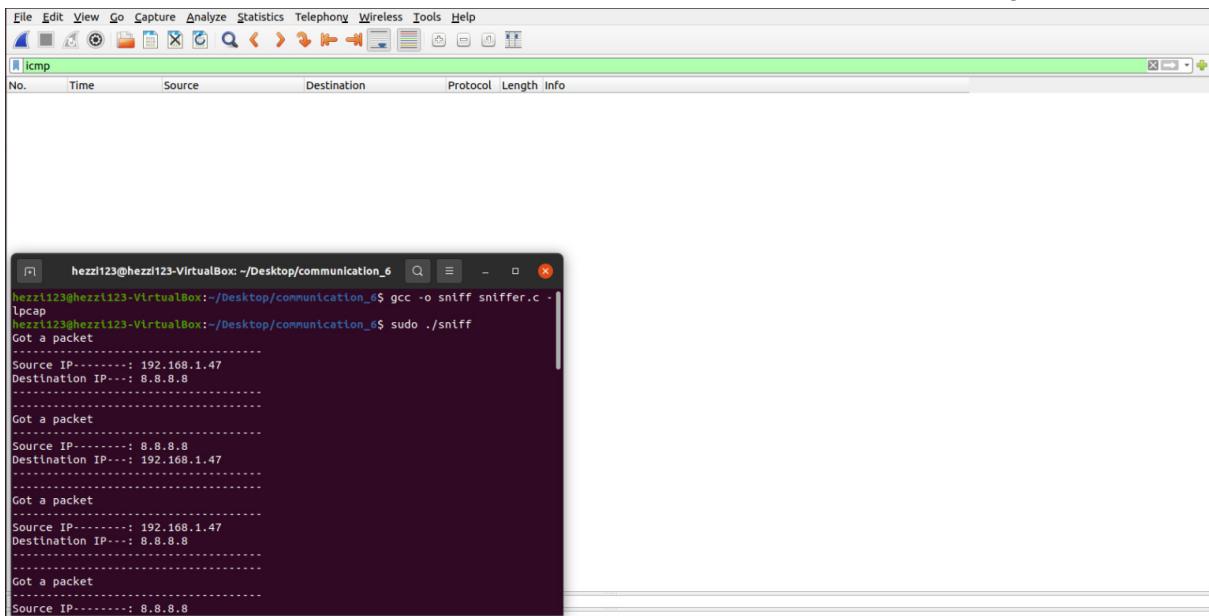
2.1A - 2.2

שאלה 1: פותחים סשן של pcap שיפתח לנו raw-socket דרכו נסניף. נגדיר את הממשק שנרצה, כמוות הדאטא שנקלב, וכל כמה זמן נקבל DATA ומבנה נתונים שייקבל שגיאות. בנוסף נגדיר שאנו נוכנסים למצב מופקר כדי שנעשה sniffiff לכל התעבורה ולא רק מה שברשת שלנו. נגדיר את הפילטר הרצוי.

שאלה 2: נctrar הרשאה בשבייל לעשות sniffiff, אחרת נקלט שגיאה כמו בחלק אחד של המטלה.

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

כأن אנחנו עושים ping.



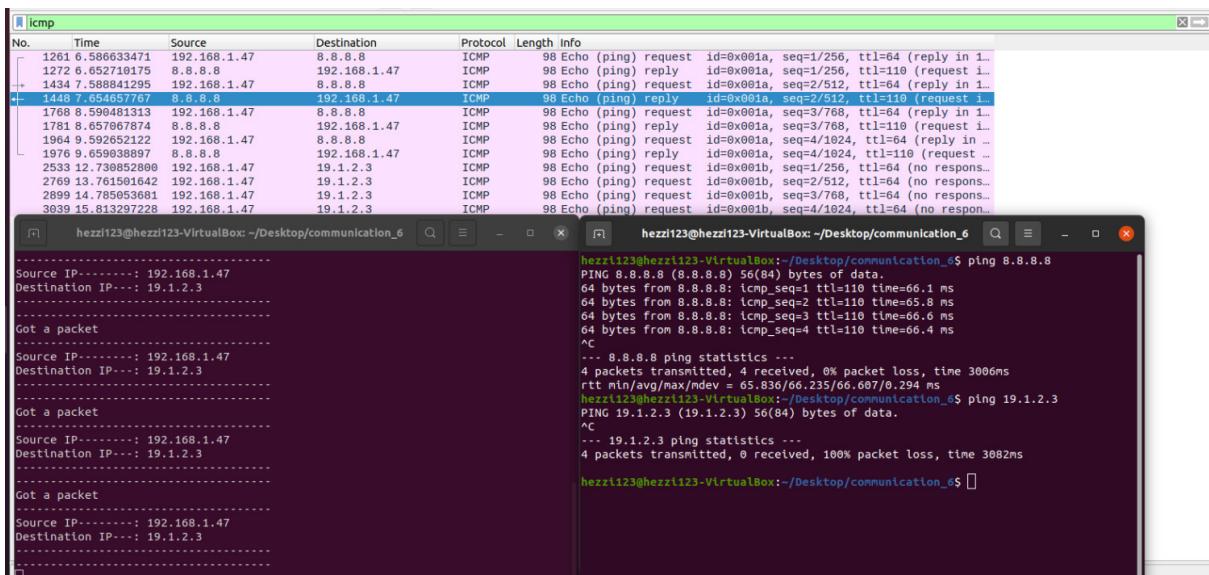
Wireshark interface showing captured ICMP traffic. The packet list shows several ICMP Echo requests and replies between two hosts with IP addresses 192.168.1.47 and 8.8.8.8. The details and bytes panes show the structure of the ICMP messages.

```

hezzli23@hezzli23-VirtualBox:~/Desktop/communication_6$ gcc -o sniff sniff.c -lpcap
hezzli23@hezzli23-VirtualBox:~/Desktop/communication_6$ sudo ./sniff
Got a packet
Source IP-----: 192.168.1.47
Destination IP---: 8.8.8.8
.
.
.
Got a packet
Source IP-----: 8.8.8.8
Destination IP---: 192.168.1.47
.
.
.
Got a packet
Source IP-----: 192.168.1.47
Destination IP---: 8.8.8.8
.
.
.
Got a packet
Source IP-----: 8.8.8.8

```

כأن ניתן לראות את התעבורה.



Wireshark interface showing captured ICMP traffic and a terminal window running a ping test. The terminal shows the ping command being run and the resulting ICMP echo requests and replies.

```

hezzli23@hezzli23-VirtualBox:~/Desktop/communication_6$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=110 time=66.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=110 time=65.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=110 time=66.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=110 time=66.4 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 65.836/66.235/66.607/0.294 ms
hezzli23@hezzli23-VirtualBox:~/Desktop/communication_6$ ping 19.1.2.3
PING 19.1.2.3 (19.1.2.3) 56(84) bytes of data.
^C
--- 19.1.2.3 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3082ms
hezzli23@hezzli23-VirtualBox:~/Desktop/communication_6$ 

```

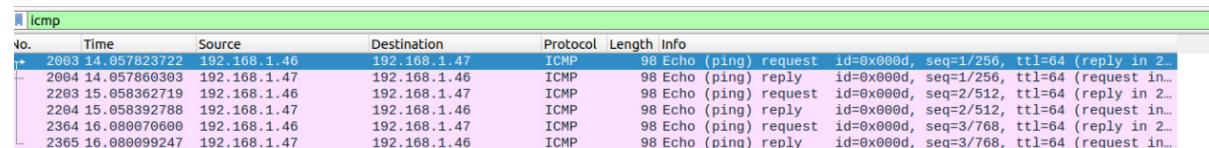
-2.1B

char filter exp[] =

הבדל בקוד הוא שורה אחת בחסן: main
ובעזרת מכונה חדשה שכתובות הIP שלה הינה 192.168.1.46

כל פעם רוצים לפ' מה שאנחנו רוצים להסニア.

Between two specific hosts:

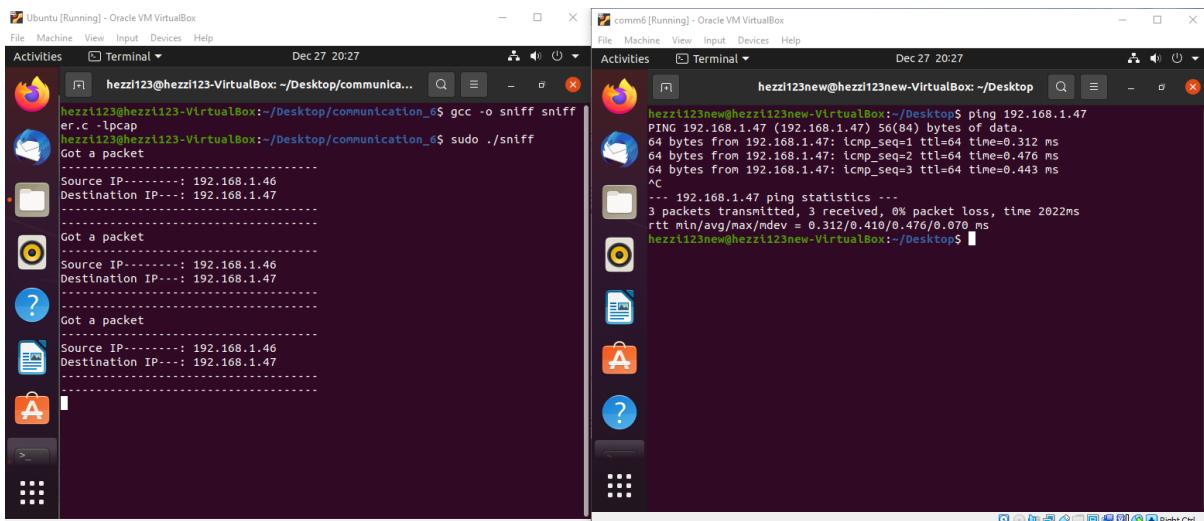


Wireshark interface showing captured ICMP traffic between two specific hosts (192.168.1.46 and 192.168.1.47). The packet list shows ICMP Echo requests and replies between these two hosts.

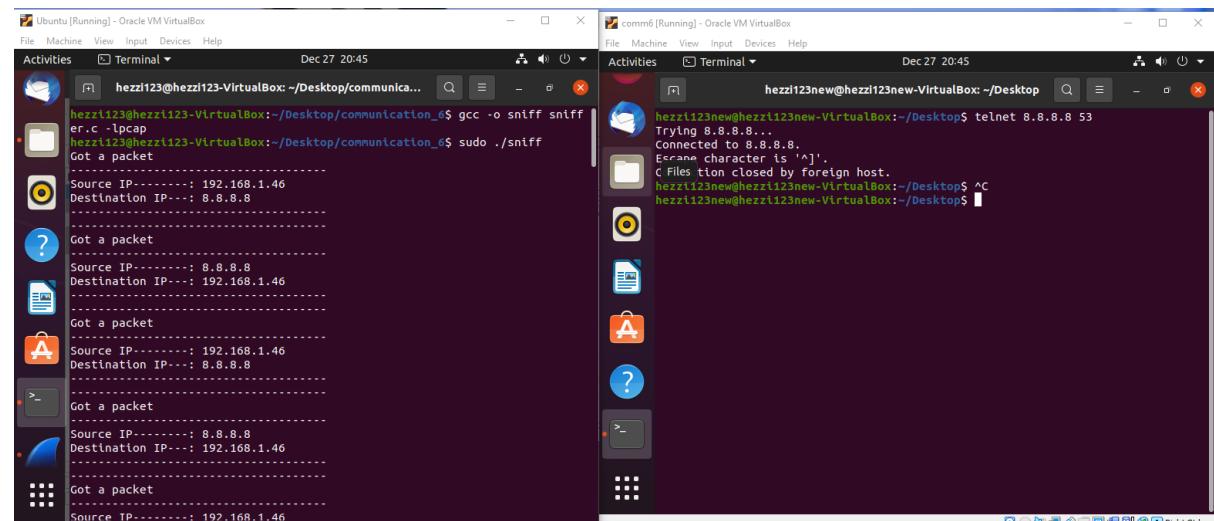
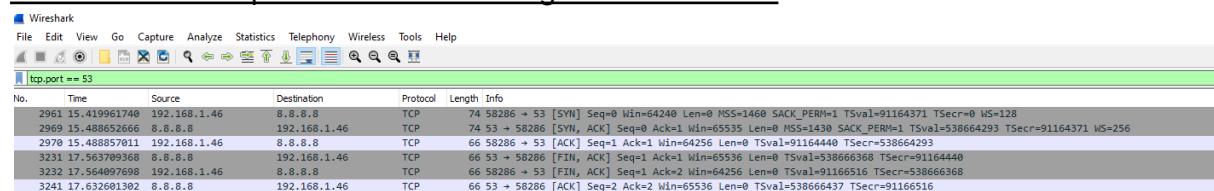
```

hezzli23@hezzli23-VirtualBox:~/Desktop/communication_6$ gcc -o sniff sniff.c -lpcap
hezzli23@hezzli23-VirtualBox:~/Desktop/communication_6$ sudo ./sniff
Got a packet
Source IP-----: 192.168.1.46
Destination IP---: 192.168.1.47
.
.
.
Got a packet
Source IP-----: 192.168.1.47
Destination IP---: 192.168.1.46
.
.
.
Got a packet
Source IP-----: 192.168.1.46
Destination IP---: 192.168.1.47
.
.
.
Got a packet
Source IP-----: 192.168.1.47
Destination IP---: 192.168.1.46
.
.
.

```

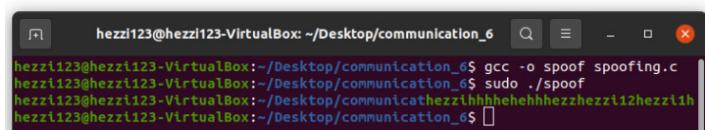


With a destination port number in the range from 10 to 100:



2.2A&2.2B - שלחנו פקודות ICMP מכתובת 192.168.1.47 לכתובת 192.168.1.26 אבל השתמשנו בכתובת מזיהפת 1.2.3.4.

NO.	TIME	SOURCE	Destination	Protocol	Length	INFO
→	1273 7.178524382	1.2.3.4	192.168.1.26	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=99 (reply in 127.178524382)
↑	1274 7.178524890	192.168.1.26	1.2.3.4	TCP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 127.178524382)



שאלה 4 – כו, ניתן להגדיר את השדה במספר שירוטי, בגלל של אחר מכך הגודל משתנה לגודל אמיתי, למרות מה שהגדכנו בשדה.

שאלה 5 לא, מערכת הפעלה תעשה את זה בשביילנו אם $\text{ip_check} = 0$ ב-`ip_header` (זה הערך הדיפולטיבי).

שאלה 6 - נדרש root privilege לצורך הרשות להריץ raw socket ולשנות מידע בתוך החבילות. אך נרייז ללא root privilege התוכנית תסתימ בשגיאה. הودעת שהגיהה תהיה שאין לנו permission. השגיהה תהיה כאשר ננסה ליצור את ה-socket.

2.3 - הריצנו את התוכנית ממוכנה אחת ועשינו sniff ממוכנה שנייה ואז spoofing (שינינו את כתובת ה-IP לכתובת לא-קיימת 1.2.3.4).

