

שאלה 1:

שליחת הודעת ICMP (PING) ל-www.google.com

```
mohamadassi@mohamadassi-VirtualBox: ~/Desktop/209027820
File Edit View Search Terminal Help
mohamadassi@mohamadassi-VirtualBox:~/Desktop/209027820$ sudo ./myping
[sudo] password for mohamadassi:

////////////////////////////////////
      in milliseconds: 73.793999
      in microseconds: 73794.000000
////////////////////////////////////
mohamadassi@mohamadassi-VirtualBox:~/Desktop/209027820$
```

ping request:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	216.58.212.196	ICMP	98	Echo (ping) request id=0xf307, seq=256/1, ttl=255 (reply in 2)
2	0.071922474	216.58.212.196	10.0.2.15	ICMP	98	Echo (ping) reply id=0xf307, seq=256/1, ttl=116 (request in 1)

▶	Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▶	Ethernet II, Src: PcsCompu_dc:2f:70 (08:00:27:dc:2f:70), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▶	Internet Protocol Version 4, Src: 10.0.2.15, Dst: 216.58.212.196
▶	Internet Control Message Protocol
	Type: 8 (Echo (ping) request)
	Code: 0
	Checksum: 0xc006 [correct]
	[Checksum Status: Good]
	Identifier (BE): 62215 (0xf307)
	Identifier (LE): 2035 (0x07f3)
	Sequence number (BE): 256 (0x0100)
	Sequence number (LE): 1 (0x0001)
	[Response frame: 2]
▶	Data (56 bytes)

0000	52 54 00 12 35 02 08 00 27 dc 2f 70 08 00 45 00	RT	5 ... /p--E
0010	00 54 4c 0c 40 00 ff 01 76 8e 0a 00 02 0f d8 3a	TL	@ ... v ... :
0020	d4 c4 08 00 c8 06 f3 07 01 00 30 31 32 33 34 35	012345
0030	36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45	6789;	<= >@ABCDE
0040	46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55	FGHIJKLM	NOPQRSTU
0050	56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65	VWXYZ[\]	^_`abcde
0060	66 00	f	

ping reply:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	216.58.212.196	ICMP	98	Echo (ping) request id=0xf307, seq=256/1, ttl=255 (reply in 2)
2	0.071922474	216.58.212.196	10.0.2.15	ICMP	98	Echo (ping) reply id=0xf307, seq=256/1, ttl=116 (request in 1)

▶	Frame 2: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▶	Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_dc:2f:70 (08:00:27:dc:2f:70)
▶	Internet Protocol Version 4, Src: 216.58.212.196, Dst: 10.0.2.15
▶	Internet Control Message Protocol
	Type: 0 (Echo (ping) reply)
	Code: 0
	Checksum: 0xd006 [correct]
	[Checksum Status: Good]
	Identifier (BE): 62215 (0xf307)
	Identifier (LE): 2035 (0x07f3)
	Sequence number (BE): 256 (0x0100)
	Sequence number (LE): 1 (0x0001)
	[Request frame: 1]
	[Response time: 71.922 ms]
▶	Data (56 bytes)

0000	08 00 27 dc 2f 70 52 54 00 12 35 02 08 00 45 00	--'--/pRT	--5--E
0010	00 54 4a 33 00 00 74 01 43 68 d8 3a d4 c4 0a 00	TJ3--t-	Ch:--
0020	02 0f 00 00 d0 06 f3 07 01 00 30 31 32 33 34 35	012345
0030	36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45	6789;	<= >@ABCDE
0040	46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55	FGHIJKLM	NOPQRSTU
0050	56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65	VWXYZ[\]	^_`abcde
0060	66 00	f	

חלק ב:

ניתן לראות כי ההודעה נתפסה ע"י תוכנת ה-sniffing, אחרי שליחת הודעת ICMP

```
File Edit View Search Terminal Help
mohamadassi@mohamadassi-VirtualBox:~/Desktop/209027820$ sudo ./myping

////////////////////////////////////
in milliseconds: 73.195984
in microseconds: 73195.984375
////////////////////////////////////
mohamadassi@mohamadassi-VirtualBox:~/Desktop/209027820$

mohamadassi@mohamadassi-VirtualBox: ~/Desktop/209027820
File Edit View Search Terminal Help
mohamadassi@mohamadassi-VirtualBox:~/Desktop/209027820$ gcc Sniffer.c -o Sniffer -lpcap
mohamadassi@mohamadassi-VirtualBox:~/Desktop/209027820$ sudo ./Sniffer

WAITING...
Ip source: 173.184.64.0
Ip dest: 255.1.27.66
Type: 0
Code: 8
-----
Ip source: 121.125.0.0
Ip dest: 116.1.26.126
Type: 0
Code: 0
-----
█
```