Scapy – תרגילים ראשונים

1) צור פקטת TCP והרץ עליה את המתודה show(). מה ערך ברירת המחדל ש-Scapy נותן עבור שדה גודל החלון (window)?

```
>>> TCP().show()
###[ TCP ]###
  sport= ftp_data
  dport= http
  seq= 0
  ack= 0
  dataofs= None
  reserved= 0
  flags= S
  window= 8192
  chksum= None
  urgptr= 0
  options= []
```

2) שנה את ערך השדה גודל החלון (window) בפקטת ה-TCP הנ"ל ל-5700. בצע show בשנית. האם הערך השתנה?

```
>>> a=TCP()
>>> a.show()
###[ TCP ]###
  sport= ftp_data
  dport= http
  seq= 0
  ack= 0
  dataofs= None
  reserved= 0
  flags= S
  window= 8192
  chksum= None
  urgptr= 0
  options= []

>>> a.window
8192
>>> a.window=5700
>>> a.show()
###[ TCP ]###
  sport= ftp_data
  dport= http
  seq= 0
  ack= 0
  dataofs= None
  reserved= 0
  flags= S
  window= 5700
  chksum= None
  urgptr= 0
  options= []
```

3) צור פקטת UDP שפורט היעד שלה הוא 666. דאג לכך שהיא תהיה מעל שכבת IP. הצג את הפקטה. כיצד Scapy מתאר את הפורט הנ"ל?

```
>>> a=IP()/UDP(dport=666)
>>> a.show()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= udp
  chksum= None
  src= 127.0.0.1
  dst= 127.0.0.1
  \options\
###[ UDP ]###
     sport= domain
     dport= 666
     len= None
     chksum= None
```

4) צור פקטת UDP נוספת, הפעם גם פורט היעד שלה וגם פורט המקור שלה יהיה 666. דאג לכך שהיא תהיה מעל שכבת IP שה-TTL שלה הוא 128. הצג את הפקטה בצורת Hexdump.

```
>>> c=IP(ttl=128)/UDP(dport=666,sport=666)
>>> c.show()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 128
  proto= udp
  chksum= None
  src= 127.0.0.1
  dst= 127.0.0.1
  \options\
###[ UDP ]###
     sport= 666
     dport= 666
     len= None
     chksum= None
>>> hexdump(c)
0000  45 00 00 1C 00 01 00 00 80 11 3C CE 7F 00 00 01  E.........<.....
0010  7F 00 00 01 02 9A 02 9A 00 08 FC A7              ............
```

5) כתוב סקריפט שמקבל מהמשתמש כתובת (IP או דומיין) ושולח 4 פקטות פינג (echo request) לכתובת זו.

script:	`from scapy.all import *`
	
	`a=input("enter IP or url: ")`
	`sendp(IP(dst=a)/ICMP())`

run test:	anna@HP-Printer:~/Desktop/scapy-2019B-II/Day 02 - 26.03.2019$ sudo python3 app.py [sudo] password for anna: enter IP or url: 8.8.8.8 . Sent 1 packets. anna@HP-Printer:~

6) צור סקריפט שמבקש מהמשתמש מספר, ומסניף את מספר הפקטות המבוקש (לדוגמא – המשתמש ביקש 10, ולכן הסקריפט יסניף 10 פקטות). לאחר מכן הסקריפט צריך להציג למשתמש איזה פקטות הוא קיבל (TCP, UDP, ICMP או אחר).

script:	`from scapy.all import *`
	
	`a=(int)(input("enter number of packets: "))`
	`b=sniff(a)`
	
	`print(b)`
	`b.summary()`

run test:	anna@HP-Printer:~/Desktop/scapy-2019B-II/Day 02 - 26.03.2019$ sudo python3 app.py enter number of packets: 2 <Sniffed: TCP:0 UDP:0 ICMP:0 Other:2> Ether / ARP who has 10.6.1.162 says 10.6.15.254 / Padding Ether / ARP who has 10.6.1.55 says 10.6.15.254 / Padding

7) גרום לסקריפט שכתבת בסעיף הקודם להציג בפירוט את תוכן הפקטה הראשונה שהוא קיבל (באמצעות המתודה show).

script:

```
from scapy.all import *

a=(int)(input("enter number of packets: "))
b=sniff(a)

b[0].show()
```

run test:

```
anna@HP-Printer:~/Desktop/scapy-2019B-II/Day 02 - 26.03.2019$ sudo python3 app.py
enter number of packets: 3
###[ Ethernet ]###
  dst       = 01:00:5e:00:00:fb
  src       = 8c:8e:f2:df:1f:7a
  type      = 0x800
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 118
     id        = 23352
     flags     =
     frag      = 0
     ttl       = 255
     proto     = udp
     chksum    = 0x7279
     src       = 10.4.2.198
     dst       = 224.0.0.251
     \options   \
###[ UDP ]###
        sport     = mdns
        dport     = mdns
        len       = 98
        chksum    = 0xb022
###[ DNS ]###
          id       = 0
          qr       = 0
          opcode   = QUERY
          aa       = 0
          tc       = 0
          rd       = 0
          ra       = 0
          z        = 0
          ad       = 0
          cd       = 0
          rcode    = ok
          qdcount  = 2
          ancount  = 0
          nscount  = 0
          arcount  = 1
          \qd       \
           |###[ DNS Question Record ]###
           |  qname     = '_homekit._tcp.local.'
           |  qtype     = PTR
           |  qclass    = 32769
           |###[ DNS Question Record ]###
           |  qname     = '_sleep-proxy._udp.local.'
           |  qtype     = PTR
           |  qclass    = 32769
          an        = None
          ns        = None
          \ar       \
           |###[ DNS OPT Resource Record ]###
           |  rrname    = '.'
           |  type      = OPT
           |  rclass    = 1440
           |  extrcode  = 0
           |  version   = 0
           |  z         = 4500
           |  rdlen     = 18
           |  \rdata     \
           |   |###[ DNS EDNS0 TLV ]###
           |   |  optcode   = Reserved
           |   |  optlen    = 14
           |   |  optdata   = '\x00&\xae\x8e\xf2\xdf\x1fz\x8c\x8e\xf2\xdf\x1fz'
```

8) שדרג את הסקריפט שכתבת בסעיף 5, וגרום לו לקבל גם את התשובות. הדפס למשתמש הודעה בה רשום כמה הודעות פינג נענו בהצלחה וכמה לא.

script:	`from scapy.all import *`
	
	`a=input("enter IP or url: ")`
	`b=sr1(IP(dst=a)/ICMP())`
	`print(b)`

run test:	anna@HP-Printer:~/Desktop/scapy-2019B-II/Day 02 - 26.03.2019$ sudo python3 app.py enter IP or url: 8.8.8.8 Begin emission: .Finished sending 1 packets. .* Received 3 packets, got 1 answers, remaining 0 packets b'E\xb8\x00\x1cU\x06\x00\x00y\x01\xd0\x0e\x08\x08\x08\x08\n\x06\x01\xff\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'

בהצלחה!