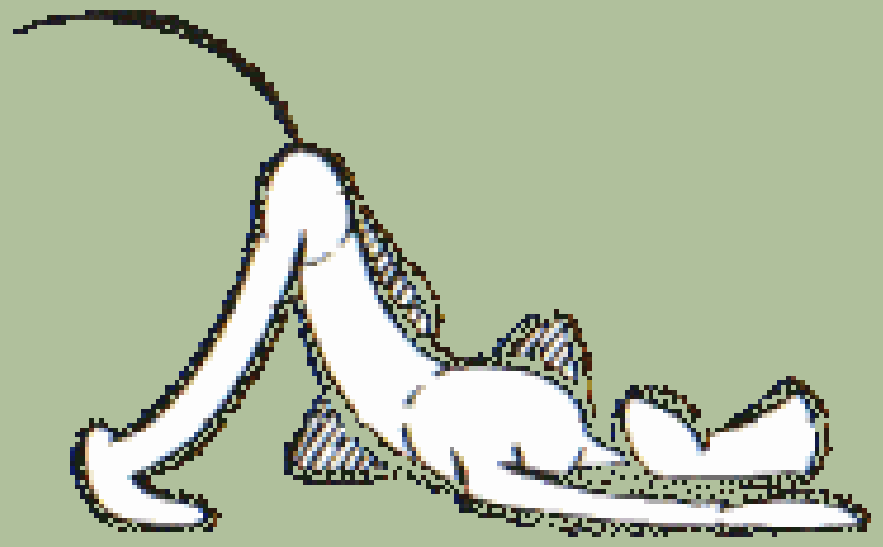
SCAPY

אילת משיח



WIRESHARK

עד עכשיו השתמשנו ב wireshark על מנת להסניף את התעבורה ברשת. אבל ל wirshark יש כמה חסרונות

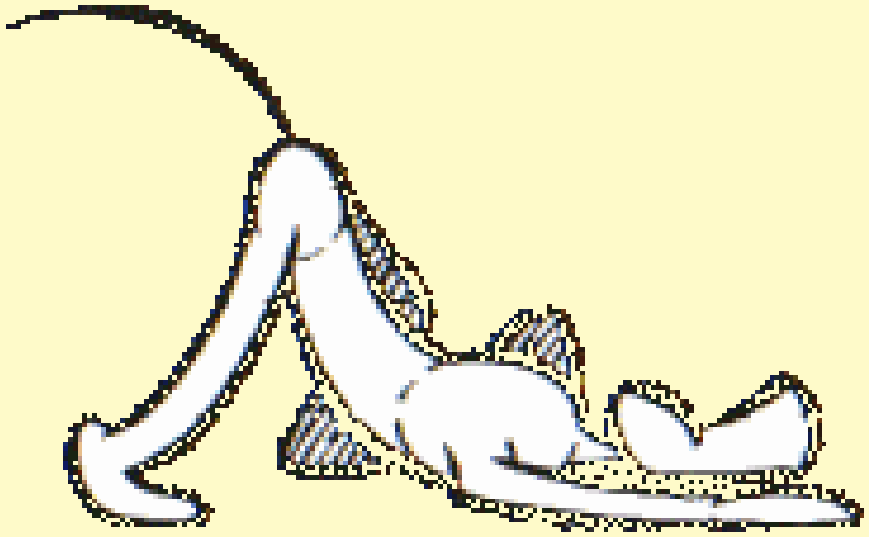
- אוסף הפילטרים שלו מוגבל
- הוא רק קולט ואין אפשרות שליחה

SCAPY

סיפריית פייתון שניתנת להרצה גם באופן אינטראקטיבי.

מאפשרת:

- פילטרים מורכבים
- פעולות תיכנותיות על פקטות
- בניית ושליחת פקטות



SCAPY - תוצאות הסנפה

פקודה	תוצאה
packets	<Sniffed: TCP:1 UDP:1 ICMP:0 Other:0> סטטיסטיקות של ההסנפה – כמה רשומות מכל פרוטוקול (הרמה העליונה של כל פקטה)
packets.show()	0000 Ether / IPv6 / UDP fe80::5032:40f0:5551:c61c:61115 > ff02::c:ssdp / Raw 0001 Ether / IP / TCP 66.102.1.189:https > 10.0.0.2:62796 PA / Raw פירוט השכבות בכל פקטה
Packets[0]	<Ether dst=33:33:00:00:00:0c src=08:60:6e:82:1c:6a type=0x86dd |<IPv6 version=6L tc=0L fl=0L plen=154 nh=UDP hlim=1 src=fe80::5032:40f0:5551:c61c dst=ff02::c |<UDP sport=61115 dport=ssdp len=154 chksum=0xfc12 |<Raw load='M-SEARCH * HTTP/1.1\r\nHost:[FF02::C]:1900\r\nST:urn:Microsoft Windows Peer Name Resolution Protocol: V4:IPV6:LinkLocal\r\nMan:"ssdp:discover"\r\nMX:3\r\n\r\n' |>>>> הדפסה גולמית של תוכן הפקטה הראשונה
Packets[0].show	הדפסה מסודרת של תוכן הפקטה הראשונה

```
>>> packets[0].show()
###[ Ethernet ]###
  dst= 33:33:00:00:00:0c
  src= 08:60:6e:82:1c:6a
  type= 0x86dd
###[ IPv6 ]###
     version= 6L
     tc= 0L
     fl= 0L
     plen= 154
     nh= UDP
     hlim= 1
     src= fe80::5032:40f0:5551:c61c
     dst= ff02::c
###[ UDP ]###
        sport= 61115
        dport= ssdp
        len= 154
        chksum= 0xfc12
###[ Raw ]###
           load= 'M-SEARCH * HTTP/1.1\r\nHost:[FF02::C]:1900\r\nST:urn:Microsoft Windows Peer N
ame Resolution Protocol: V4:IPV6:LinkLocal\r\nMan:"ssdp:discover"\r\nMX:3\r\n\r\n'
```

SCAPY - תוצאות הסנפה

פקודה	תוצאה
packets[TCP]	<TCP from Sniffed: TCP:1 UDP:0 ICMP:0 Other:0> הדפסת סטטיסטיקות על פקטות שמופיע בהן פרוטוקול TCP
packets[TCP].show()	0000 Ether / IP / TCP 66.102.1.189:https > 10.0.0.2:62796 PA / Raw הדפסת כל השכבות בכל פקטה בה מופיע TCP
packets[Ether]	<Ether from Sniffed: TCP:1 UDP:1 ICMP:0 Other:0> הדפסת סטטיסטיקות על פקטות שמופיע בהן פרוטוקול Ether
packets[Ether].show()	0000 Ether / IPv6 / UDP fe80::5032:40f0:5551:c61c:61115 > ff02::c:ssdp / Raw 0001 Ether / IP / TCP 66.102.1.189:https > 10.0.0.2:62796 PA / Raw הדפסת כל השכבות בכל פקטה בה מופיע Ether

SCAPY - תוצאות הסנפה - סיכום

- הדפסת פקטה או קבוצת פקטות בScapy מדפיסה נתונים גולמיים, בניגוד לפקודה **show** שמעבדת את הנתונים ומדפיסה אותם מסודרים
- גישה לנתונים עם סוגריים מרובעים ובתוכם מספר *n* ניגשת לפקטה מספר n לפי סדר ההגעה – **packets[0]**
- גישה לנתונים עם סוגריים מרוbעים ובתוכם שם פרוטוקול ניגשת לקבוצת הפקטות שהשתמשו בפרוטוקול **packets[UDP]**

SCAPY – פתרון תרגיל הסנפה עם פילטר ו

- נמצא את ערכו של packets[0][DNSQR].qtype כשהשאילתה מסוג A.
- עבור פקט שבפקודת show עליה נראה שהשדה qtyp = A נריץ

>>> print packets[0][DNSQR].qtype ➔ 1

- כלומר הפילטר הוא מהצורה

```
def dns_filter(p):
    return DNS in p and p[DNS].opcode == 0 and p[DNSQR].qtype == 1
```

- וההסנפה:

```
>>> sniff(count = 4, lfilter = dns_filter)
INFO: Sniffing on <NetworkInterface Qualcomm A
-7739-4026-9DAD-09E3AECBA6F5}>
<Sniffed: TCP:0 UDP:0 ICMP:0 Other:0>
```

הדפסת RAW DATA

Scapy אינו מנתח עבורנו את שכבת האפליקציה כי אם מעביר את הנתונים בצורה גולמית. עלינו להמיר את הנתונים האלה ל str

בקשות ותשובות בפרוטוקול של שכבתהאפליקציה יושבות ב Raw

```
        options= []
###[ Raw ]###
           load= 'GET /pagead/gen_204?id=wfocus&gqid&qqid=COr5mNaKw9cCFc3iGwod1XYPIw&fg=1 HTTP/1.1\r\nHost: googleads.g.
doubleclick.net\r\nConnection: keep-alive\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
HTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36\r\nAccept: image/webp,image/apng,image/*,*/*;q=0.8\r\nReferer: http
://www.ynet.co.il/home/0,7340,L-2,00.html\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.8\r\nCookie
: DSID=ADyxukuvbS_UNFvs2cWOZW8KUXE6idB4Vc-oYVyFGOcknkZDJujljqJ6zwm1QUBeN26NNSPWvrWKxmo3mmcz0atSus0imR6bSimnLIceOWxHJUOnt
CefyuU; IDE=AHWqTUlN6P8_8eWLr4NrYadJrWH_hvYTCcSfCfd6FjJ6QGuhSB6xZ_z5sn3DLZdH\r\n\r\n'
```