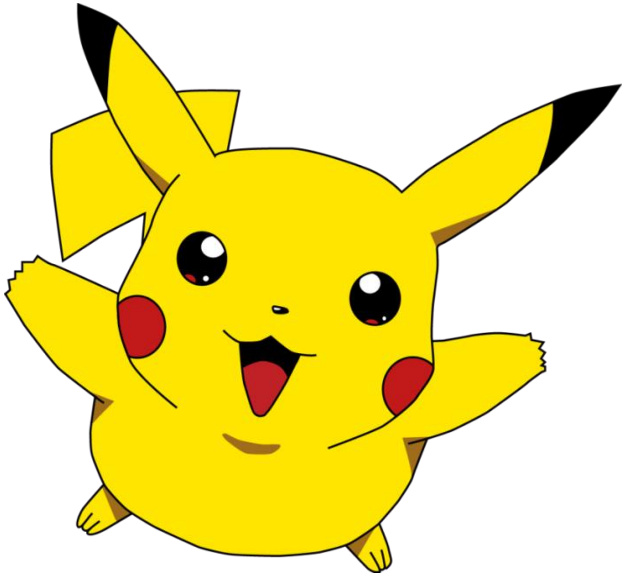
WIFI ATTACK AND DEFENSE

Besim ALTINOK
Security Engineer

Kablosuz Ağlara Yönelik Keşif Çalışmaları



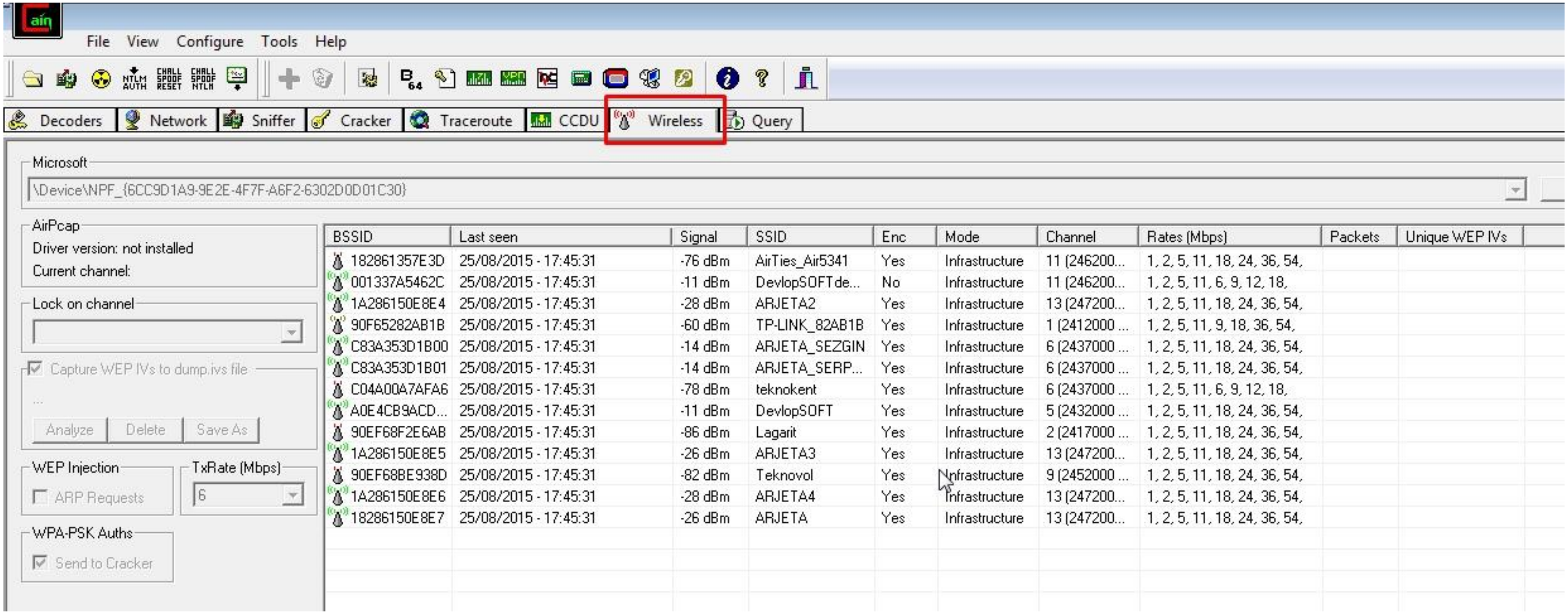
# Cain & Abel

# Cain & Abel

* Platform : Windows
* İndirme Linki : http://www.oxid.it/cain.html
* Analiz sırasında elde edilebilecek bilgiler

$ Son göründüğü tarih (GG:AY:YIL-SA:DK:SN formatında)
$ Sinyal seviyesi
$ SSID bilgisi
$ BSSID bilgisi(Cihazın MAC Adresi)
$ Channel (Frekans)
$ Encryption

Cain & Abel



Microsoft

\Device\NPF_{6CC9D1A9-9E2E-4F7F-A6F2-6302D0D01C30}

AirPcap

Driver version: not installed

Current channel:

Lock on channel

☑ Capture WEP IVs to dump.ivs file

...

WEP Injection

□ ARP Requests

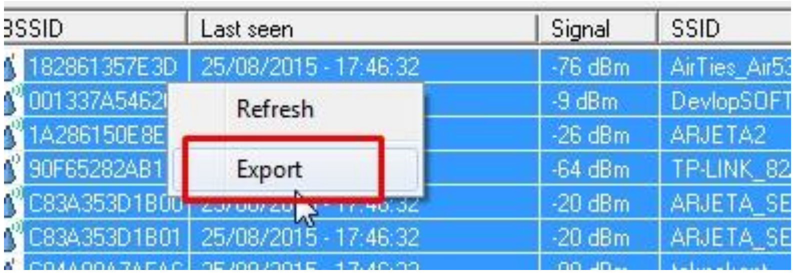
TxRate (Mbps) 6

WPA-PSK Auths

☑ Send to Cracker

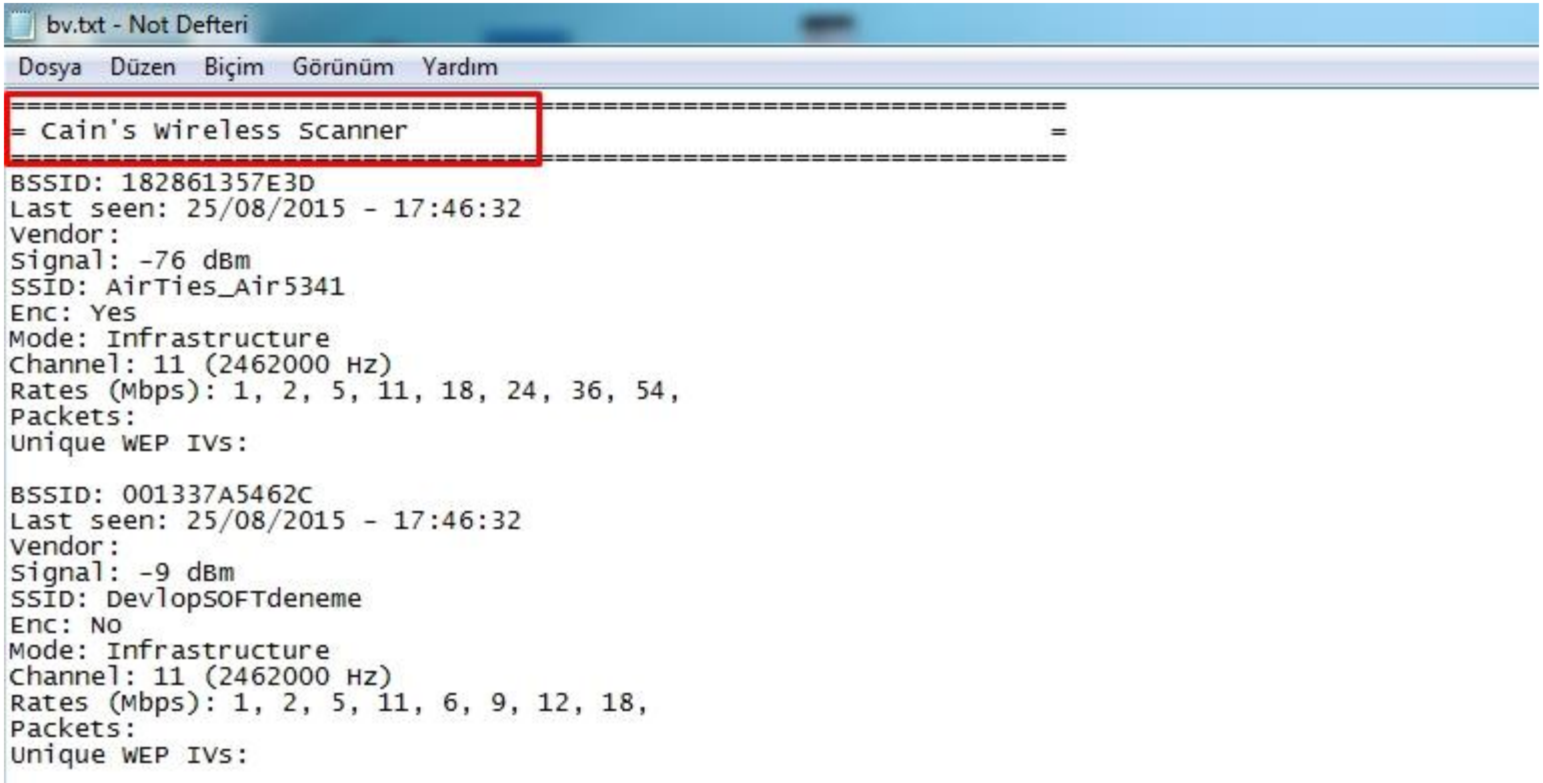
BSSID	Last seen	Signal	SSID	Enc	Mode	Channel	Rates (Mbps)	Packets	Unique WEP IVs
182861357E3D	25/08/2015 - 17:45:31	-76 dBm	AirTies_Air5341	Yes	Infrastructure	11 (246200...	1, 2, 5, 11, 18, 24, 36, 54,		
001337A5462C	25/08/2015 - 17:45:31	-11 dBm	DevlopSOFTde...	No	Infrastructure	11 (246200...	1, 2, 5, 11, 6, 9, 12, 18,		
1A286150E8E4	25/08/2015 - 17:45:31	-28 dBm	ARJETA2	Yes	Infrastructure	13 (247200...	1, 2, 5, 11, 18, 24, 36, 54,		
90F65282AB1B	25/08/2015 - 17:45:31	-60 dBm	TP-LINK_82AB1B	Yes	Infrastructure	1 (2412000 ...	1, 2, 5, 11, 9, 18, 36, 54,		
C83A353D1B00	25/08/2015 - 17:45:31	-14 dBm	ARJETA_SEZGIN	Yes	Infrastructure	6 (2437000 ...	1, 2, 5, 11, 18, 24, 36, 54,		
C83A353D1B01	25/08/2015 - 17:45:31	-14 dBm	ARJETA_SERP...	Yes	Infrastructure	6 (2437000 ...	1, 2, 5, 11, 18, 24, 36, 54,		
C04A00A7AFA6	25/08/2015 - 17:45:31	-78 dBm	teknokent	Yes	Infrastructure	6 (2437000 ...	1, 2, 5, 11, 6, 9, 12, 18,		
A0E4CB9ACD...	25/08/2015 - 17:45:31	-11 dBm	DevlopSOFT	Yes	Infrastructure	5 (2432000 ...	1, 2, 5, 11, 18, 24, 36, 54,		
90EF68F2E6AB	25/08/2015 - 17:45:31	-86 dBm	Lagarit	Yes	Infrastructure	2 (2417000 ...	1, 2, 5, 11, 18, 24, 36, 54,		
1A286150E8E5	25/08/2015 - 17:45:31	-26 dBm	ARJETA3	Yes	Infrastructure	13 (247200...	1, 2, 5, 11, 18, 24, 36, 54,		
90EF68BE938D	25/08/2015 - 17:45:31	-82 dBm	Teknovol	Yes	Infrastructure	9 (2452000 ...	1, 2, 5, 11, 18, 24, 36, 54,		
1A286150E8E6	25/08/2015 - 17:45:31	-28 dBm	ARJETA4	Yes	Infrastructure	13 (247200...	1, 2, 5, 11, 18, 24, 36, 54,		
18286150E8E7	25/08/2015 - 17:45:31	-26 dBm	ARJETA	Yes	Infrastructure	13 (247200...	1, 2, 5, 11, 18, 24, 36, 54,		

Cain & Abel



BSSID	Last seen	Signal	SSID
182861357E3D	25/08/2015 - 17:46:32	-76 dBm	AirTies_Air53
001337A5462(		-9 dBm	DevlopSOFT
1A286150E8E		-26 dBm	ARJETA2
90F65282AB1		-64 dBm	TP-LINK_82
C83A353D1B00	- 17:46:32	-20 dBm	ARJETA_SE
C83A353D1B01	25/08/2015 - 17:46:32	-20 dBm	ARJETA_SE

Analiz sonuçlarını export etmek için



```
==================================================================
= Cain's Wireless Scanner                                        =
==================================================================
BSSID: 182861357E3D
Last seen: 25/08/2015 - 17:46:32
Vendor:
Signal: -76 dBm
SSID: AirTies_Air5341
Enc: Yes
Mode: Infrastructure
Channel: 11 (2462000 Hz)
Rates (Mbps): 1, 2, 5, 11, 18, 24, 36, 54,
Packets:
Unique WEP IVs:

BSSID: 001337A5462C
Last seen: 25/08/2015 - 17:46:32
Vendor:
Signal: -9 dBm
SSID: DevlopSOFTdeneme
Enc: No
Mode: Infrastructure
Channel: 11 (2462000 Hz)
Rates (Mbps): 1, 2, 5, 11, 6, 9, 12, 18,
Packets:
Unique WEP IVs:
```

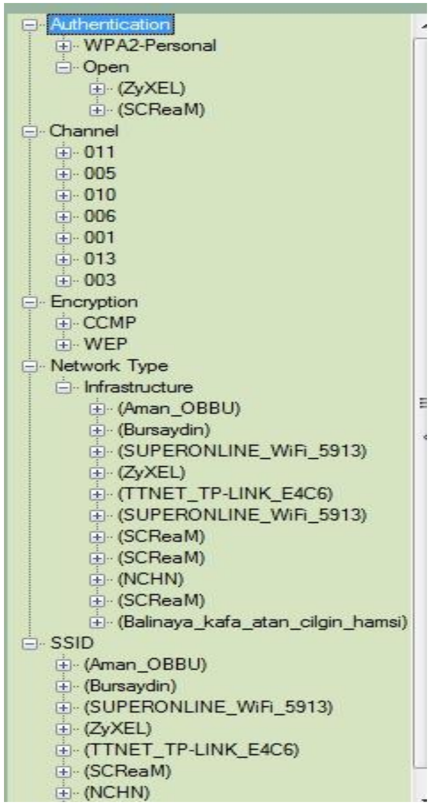
# Vistumbler

# Vistumbler

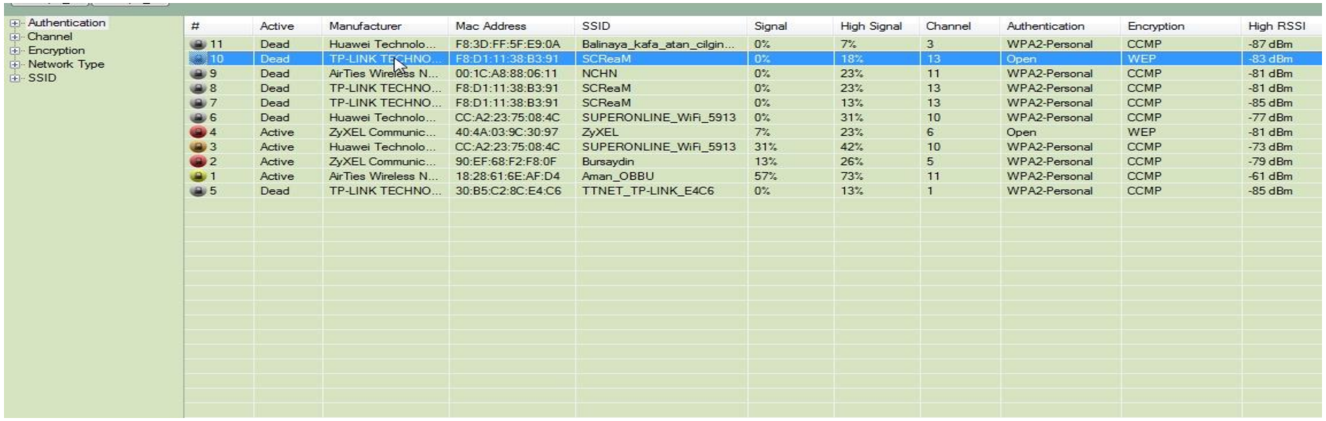
* Platform : Windows
* İndirme Linki : http://www.vistumbler.net/
* Elde edilebilecek bilgiler

$ Cihazın aktif olup olmadığı
$ Son göründüğü tarih
$ Sinyal seviyesi
$ SSID bilgisi
$ BSSID bilgisi (Cihazın MAC Adresi)
$ Channel
$ Authentication
$ Encryption
$ Cihazın üretici firması (MAC adresinin ilk 24 bitinden bulur)

Vistumbler



- Authentication
  - WPA2-Personal
  - Open
    - (ZyXEL)
    - (SCReaM)
- Channel
  - 011
  - 005
  - 010
  - 006
  - 001
  - 013
  - 003
- Encryption
  - CCMP
  - WEP
- Network Type
  - Infrastructure
    - (Aman_OBBU)
    - (Bursaydin)
    - (SUPERONLINE_WiFi_5913)
    - (ZyXEL)
    - (TTNET_TP-LINK_E4C6)
    - (SUPERONLINE_WiFi_5913)
    - (SCReaM)
    - (SCReaM)
    - (NCHN)
    - (SCReaM)
    - (Balinaya_kafa_atan_cilgin_hamsi)
- SSID
  - (Aman_OBBU)
  - (Bursaydin)
  - (SUPERONLINE_WiFi_5913)
  - (ZyXEL)
  - (TTNET_TP-LINK_E4C6)
  - (SCReaM)
  - (NCHN)



- Authentication
- Channel
- Encryption
- Network Type
- SSID

#	Active	Manufacturer	Mac Address	SSID	Signal	High Signal	Channel	Authentication	Encryption	High RSSI
11	Dead	Huawei Technolo...	F8:3D:FF:5F:E9:0A	Balinaya_kafa_atan_cilgin...	0%	7%	3	WPA2-Personal	CCMP	-87 dBm
10	Dead	TP-LINK TECHNO...	F8:D1:11:38:B3:91	SCReaM	0%	18%	13	Open	WEP	-83 dBm
9	Dead	AirTies Wireless N...	00:1C:A8:88:06:11	NCHN	0%	23%	11	WPA2-Personal	CCMP	-81 dBm
8	Dead	TP-LINK TECHNO...	F8:D1:11:38:B3:91	SCReaM	0%	23%	13	WPA2-Personal	CCMP	-81 dBm
7	Dead	TP-LINK TECHNO...	F8:D1:11:38:B3:91	SCReaM	0%	13%	13	WPA2-Personal	CCMP	-85 dBm
6	Dead	Huawei Technolo...	CC:A2:23:75:08:4C	SUPERONLINE_WiFi_5913	0%	31%	10	WPA2-Personal	CCMP	-77 dBm
4	Active	ZyXEL Communic...	40:4A:03:9C:30:97	ZyXEL	7%	23%	6	Open	WEP	-81 dBm
3	Active	Huawei Technolo...	CC:A2:23:75:08:4C	SUPERONLINE_WiFi_5913	31%	42%	10	WPA2-Personal	CCMP	-73 dBm
2	Active	ZyXEL Communic...	90:EF:68:F2:F8:0F	Bursaydin	13%	26%	5	WPA2-Personal	CCMP	-79 dBm
1	Active	AirTies Wireless N...	18:28:61:6E:AF:D4	Aman_OBBU	57%	73%	11	WPA2-Personal	CCMP	-61 dBm
5	Dead	TP-LINK TECHNO...	30:B5:C2:8C:E4:C6	TTNET_TP-LINK_E4C6	0%	13%	1	WPA2-Personal	CCMP	-85 dBm

Sol taraftaki açılır menüden filtreleme seçeneklerini kullanabiliriz

# Windows "netsh" komutu

# Windows "netsh" komutu

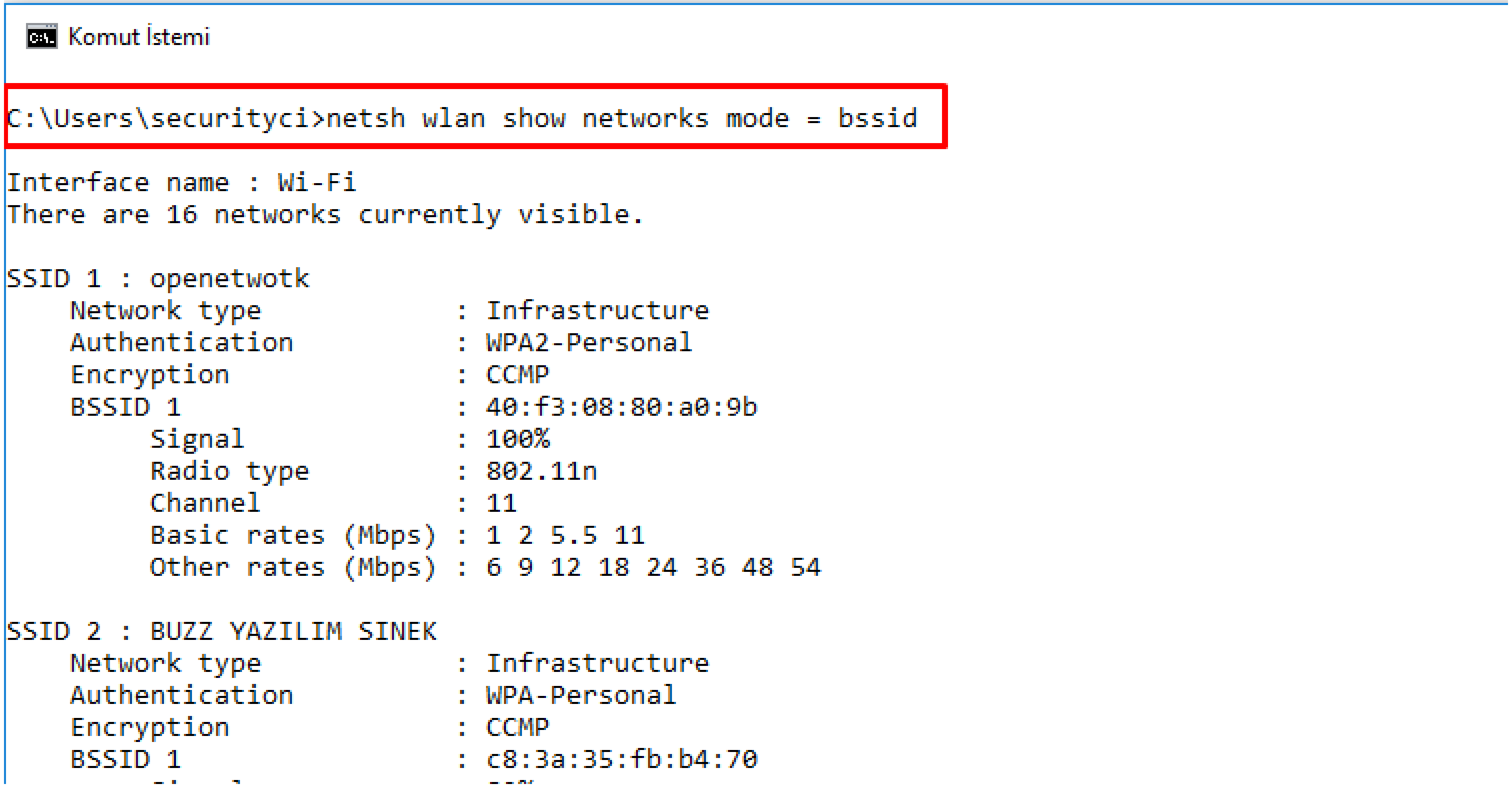
* **netsh wlan show networks mode = bssid**
* Etraftaki ağlar için aşağıdaki bilgileri getirir.

$ SSID
$ BSSID
$ Şifreleme Türü (WPA/WPA2-WEP-OPN)
$ Sinyal Gücü
$ Radyo Türü (802.11a)

* **netsh wlan show networks**
* Etraftaki ağlar için aşağıdaki bilgileri getirir.

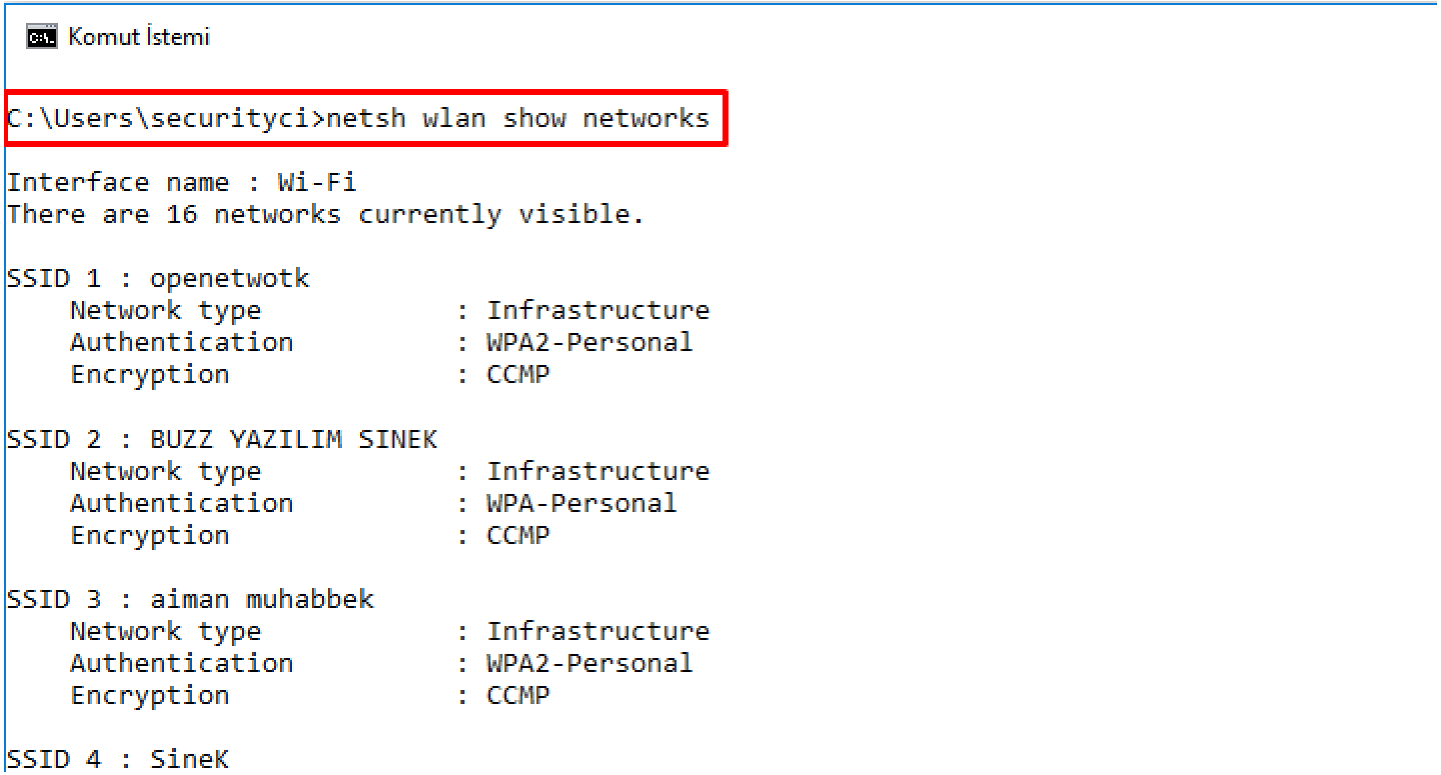
$ SSID
$ Şifreleme Türü (WPA/WPA2-WEP-OPN)

Windows "netsh" komutu



```
C:\Users\securityci>netsh wlan show networks mode = bssid

Interface name : Wi-Fi
There are 16 networks currently visible.

SSID 1 : openetwotk
    Network type            : Infrastructure
    Authentication          : WPA2-Personal
    Encryption              : CCMP
    BSSID 1                 : 40:f3:08:80:a0:9b
         Signal             : 100%
         Radio type         : 802.11n
         Channel            : 11
         Basic rates (Mbps) : 1 2 5.5 11
         Other rates (Mbps) : 6 9 12 18 24 36 48 54

SSID 2 : BUZZ YAZILIM SINEK
    Network type            : Infrastructure
    Authentication          : WPA-Personal
    Encryption              : CCMP
    BSSID 1                 : c8:3a:35:fb:b4:70
```

Windows "netsh" komutu



```
C:\Users\securityci>netsh wlan show networks

Interface name : Wi-Fi
There are 16 networks currently visible.

SSID 1 : openetwotk
    Network type            : Infrastructure
    Authentication          : WPA2-Personal
    Encryption              : CCMP

SSID 2 : BUZZ YAZILIM SINEK
    Network type            : Infrastructure
    Authentication          : WPA-Personal
    Encryption              : CCMP

SSID 3 : aiman muhabbek
    Network type            : Infrastructure
    Authentication          : WPA2-Personal
    Encryption              : CCMP

SSID 4 : SineK
```

# Linux "**iwlist**" komutu

# Linux "**iwlist**" komutu

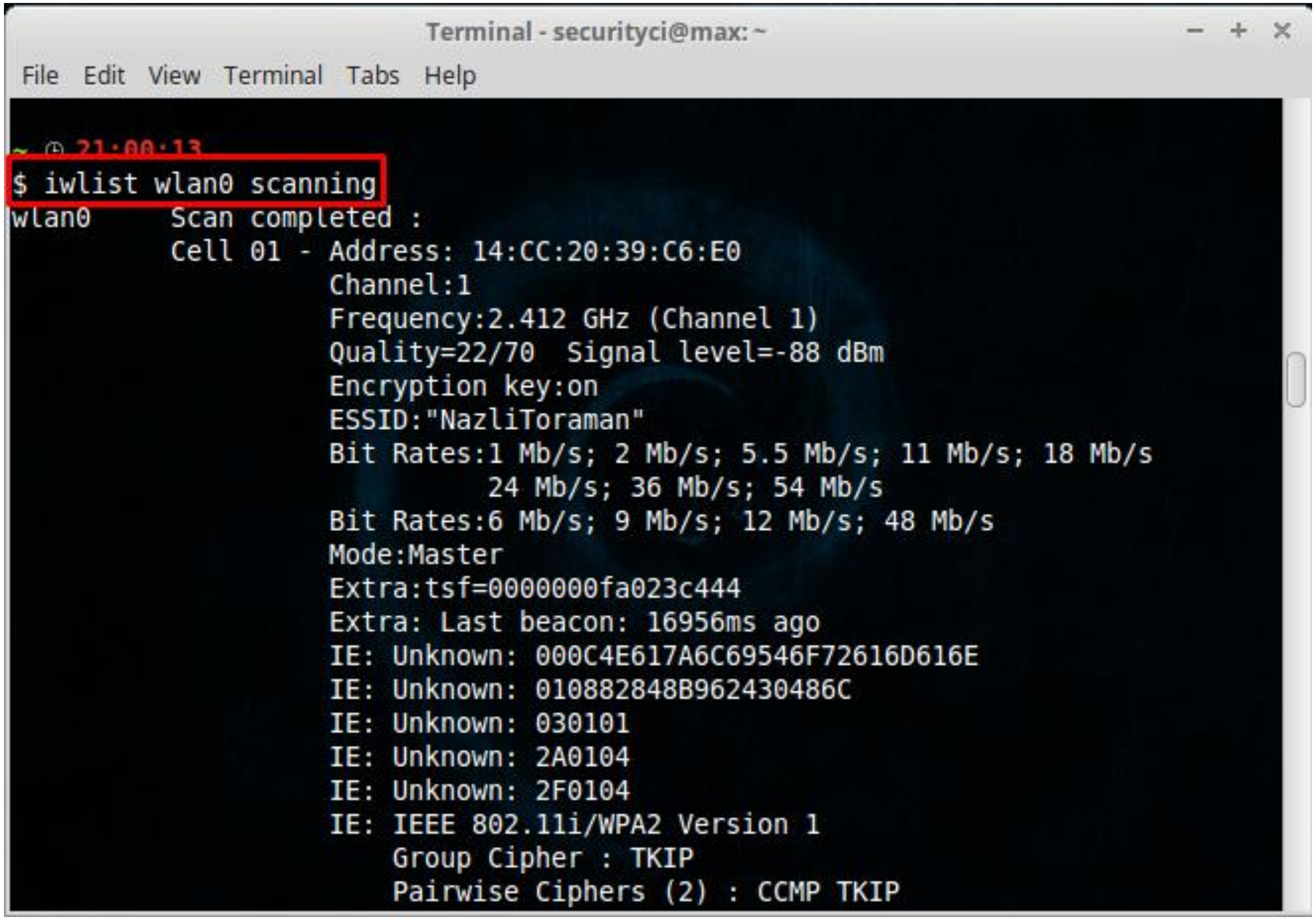
* **iwlist wlan6 scanning**
* Etraftaki AP cihazları için aşağıdaki bilglerini getirir.

$ SSID
$ BSSID
$ Şifreleme Türü (WPA/WPA2-WEP-OPN)
$ Sinyal Gücü
$ Radyo Türü (802.11a)
$ Channel

* **iwlist wlan6 scanning | grep -i "Cell" | awk '{print $5}‘**
* Etraftaki AP cihazları için MAC adreslerini verir.

* **iwlist wlan6 scanning | grep -i "ssid"**
* Etraftaki ssid listesini verir.

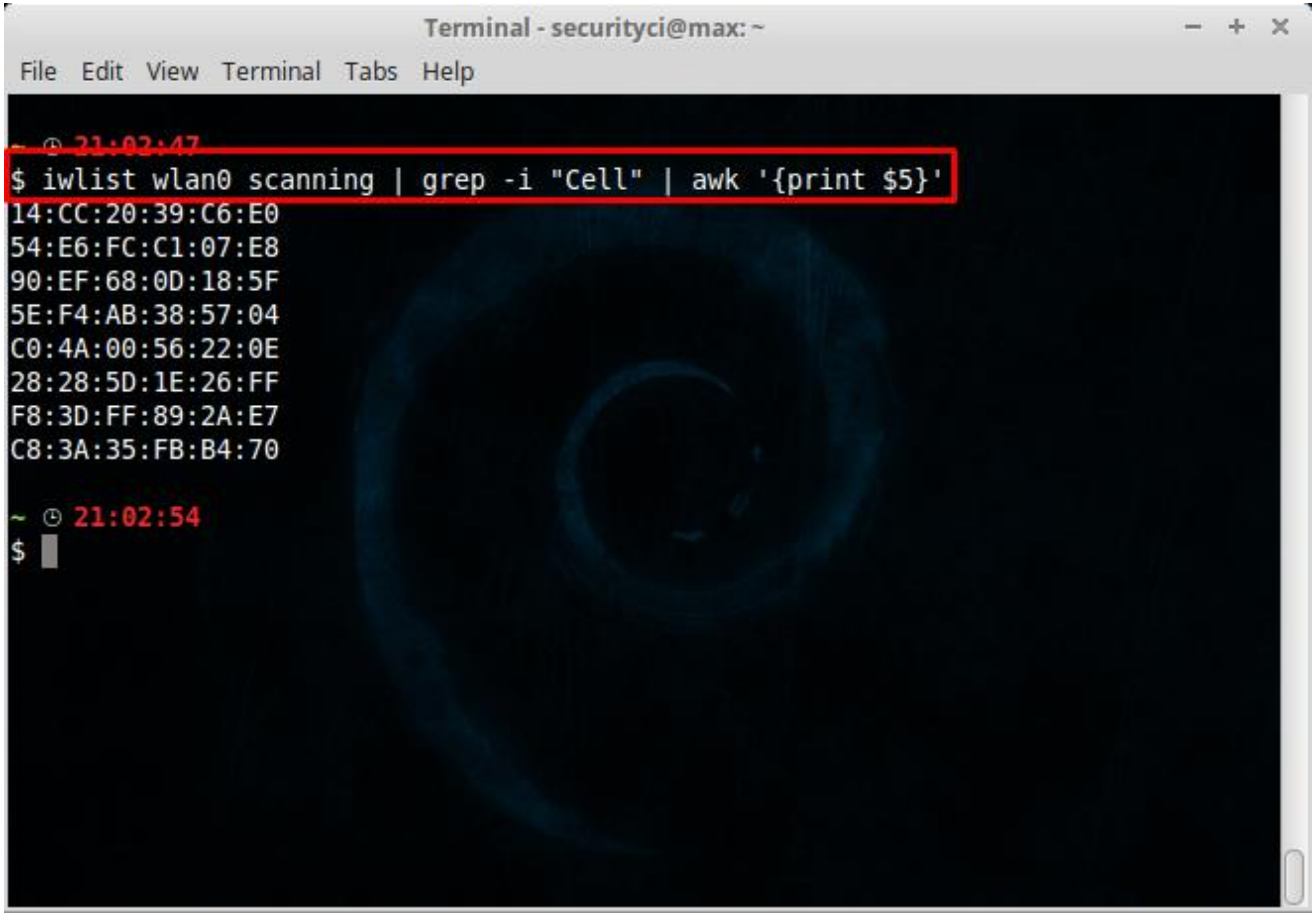
Linux "**iwlist**" komutu



Terminal - securityci@max: ~
File Edit View Terminal Tabs Help

```
~ ◷ 21:00:13
$ iwlist wlan0 scanning
wlan0     Scan completed :
          Cell 01 - Address: 14:CC:20:39:C6:E0
                    Channel:1
                    Frequency:2.412 GHz (Channel 1)
                    Quality=22/70  Signal level=-88 dBm
                    Encryption key:on
                    ESSID:"NazliToraman"
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 18 Mb/s
                              24 Mb/s; 36 Mb/s; 54 Mb/s
                    Bit Rates:6 Mb/s; 9 Mb/s; 12 Mb/s; 48 Mb/s
                    Mode:Master
                    Extra:tsf=0000000fa023c444
                    Extra: Last beacon: 16956ms ago
                    IE: Unknown: 000C4E617A6C69546F72616D616E
                    IE: Unknown: 010882848B962430486C
                    IE: Unknown: 030101
                    IE: Unknown: 2A0104
                    IE: Unknown: 2F0104
                    IE: IEEE 802.11i/WPA2 Version 1
                        Group Cipher : TKIP
                        Pairwise Ciphers (2) : CCMP TKIP
```

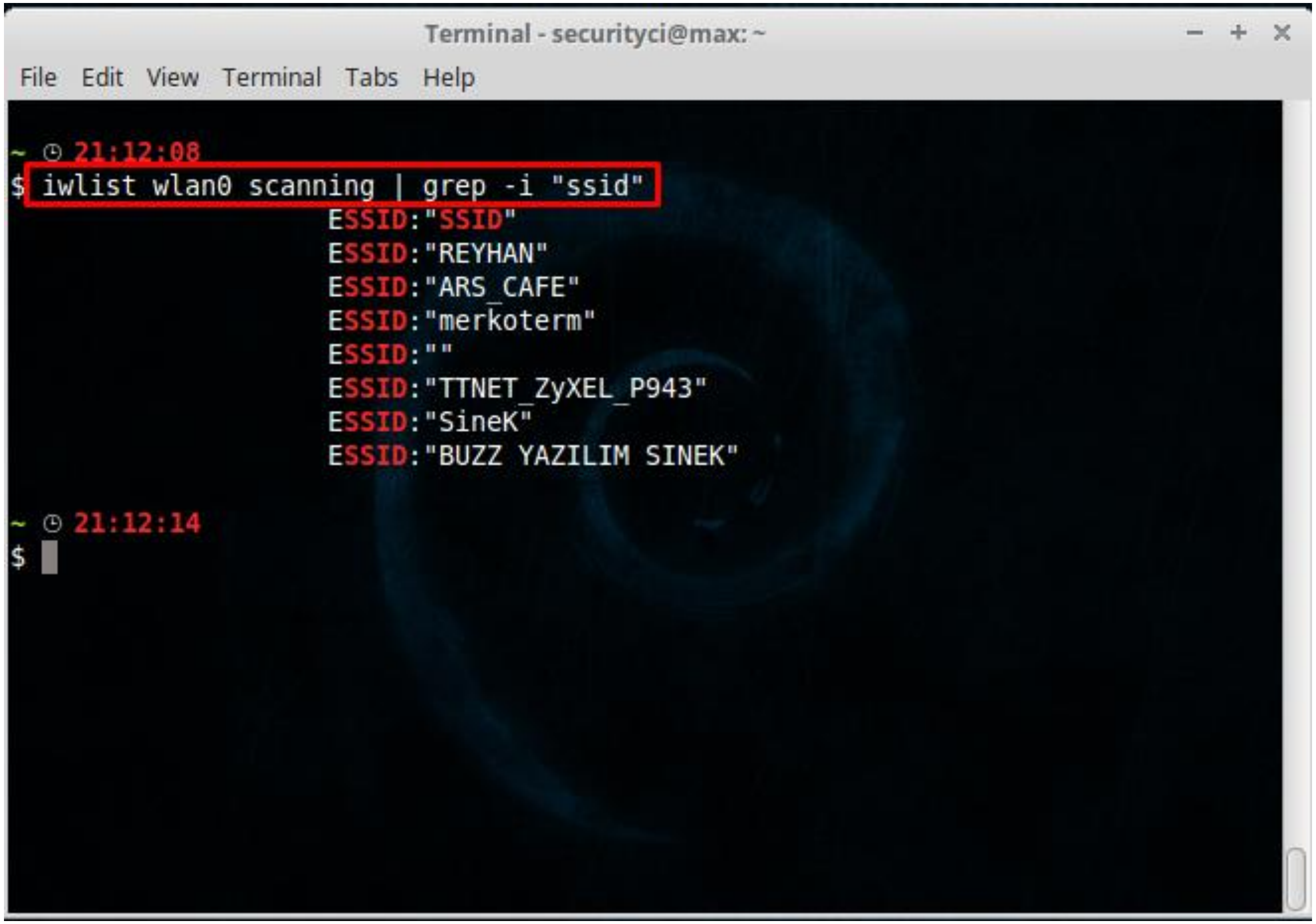
Linux "**iwlist**" komutu



Terminal - securityci@max: ~
File Edit View Terminal Tabs Help

```
~ ◷ 21:02:47
$ iwlist wlan0 scanning | grep -i "Cell" | awk '{print $5}'
14:CC:20:39:C6:E0
54:E6:FC:C1:07:E8
90:EF:68:0D:18:5F
5E:F4:AB:38:57:04
C0:4A:00:56:22:0E
28:28:5D:1E:26:FF
F8:3D:FF:89:2A:E7
C8:3A:35:FB:B4:70

~ ◷ 21:02:54
$ 
```

Linux "**iwlist**" komutu



Terminal - securityci@max: ~
File Edit View Terminal Tabs Help

```
~ ◷ 21:12:08
$ iwlist wlan0 scanning | grep -i "ssid"
                    ESSID:"SSID"
                    ESSID:"REYHAN"
                    ESSID:"ARS_CAFE"
                    ESSID:"merkoterm"
                    ESSID:""
                    ESSID:"TTNET_ZyXEL_P943"
                    ESSID:"SineK"
                    ESSID:"BUZZ YAZILIM SINEK"

~ ◷ 21:12:14
$
```

# Airodump-ng

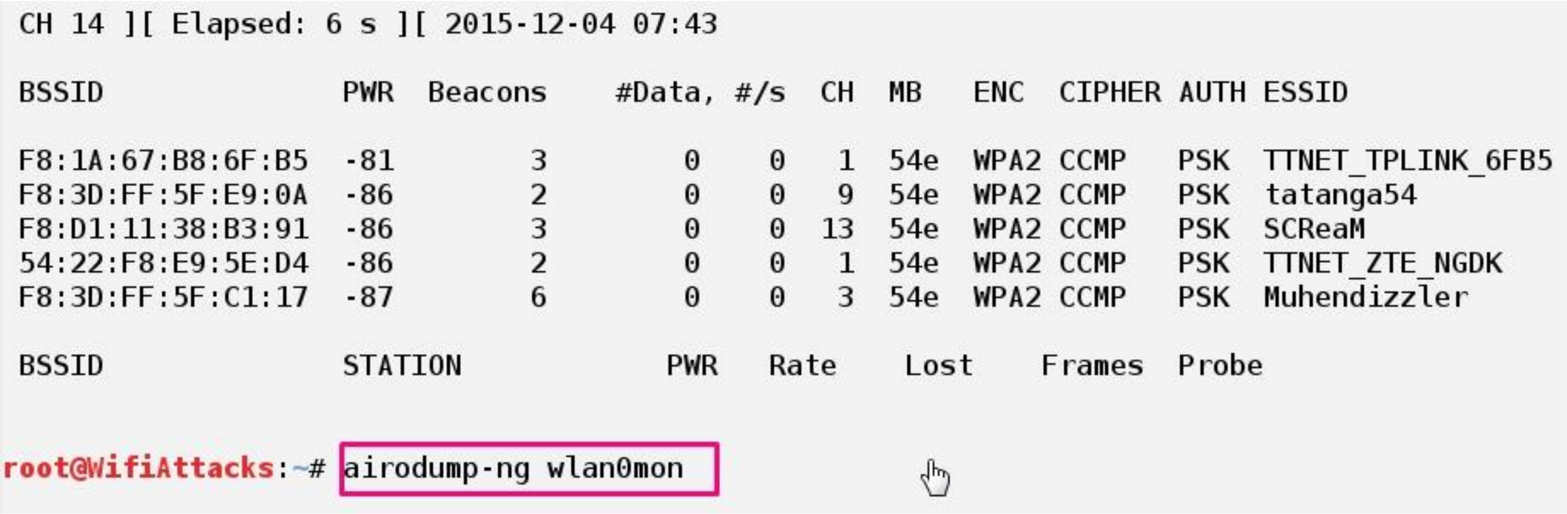
# Airodump-ng

* Platform : Linux
* İndirme Linki : Kurulum için aircrack-ng paketini kurmak yeterlidir.

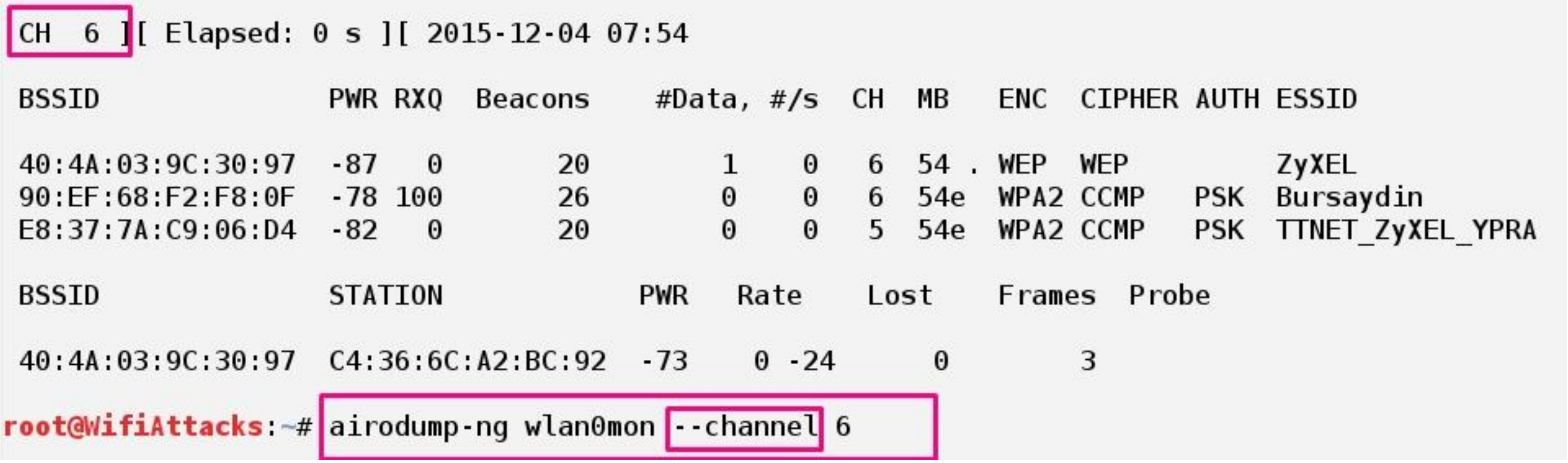
* Kullanılabilecek önemli filtreler

$ --bssid : Belirttiğiniz MAc adresine göre monitoring işlemi yapar
$ --essid : Belirttiğiniz kablosuz ağ adına göre monitoring işlemi yapar.
$ --wps : WPS destekli cihazları görüntülemenize yardımcı olur
$ --uptime : AP in açık olma süresini sizlere gösterir.
$ --ivs : Sadece IVs paketlerini yakalar
$ --w : Monitore ettiğiniz trafiği bir dosyaya kayıt edebilirsiniz.
$ --essid-regex : İstediğiniz regex ifade ile kablosuz ağ adını monitore edebilirsiniz.
$ --channel : Monitore etmek istediğiniz kanal numarasını veya numaralarını belirtebilirsiniz.

Airodump-ng

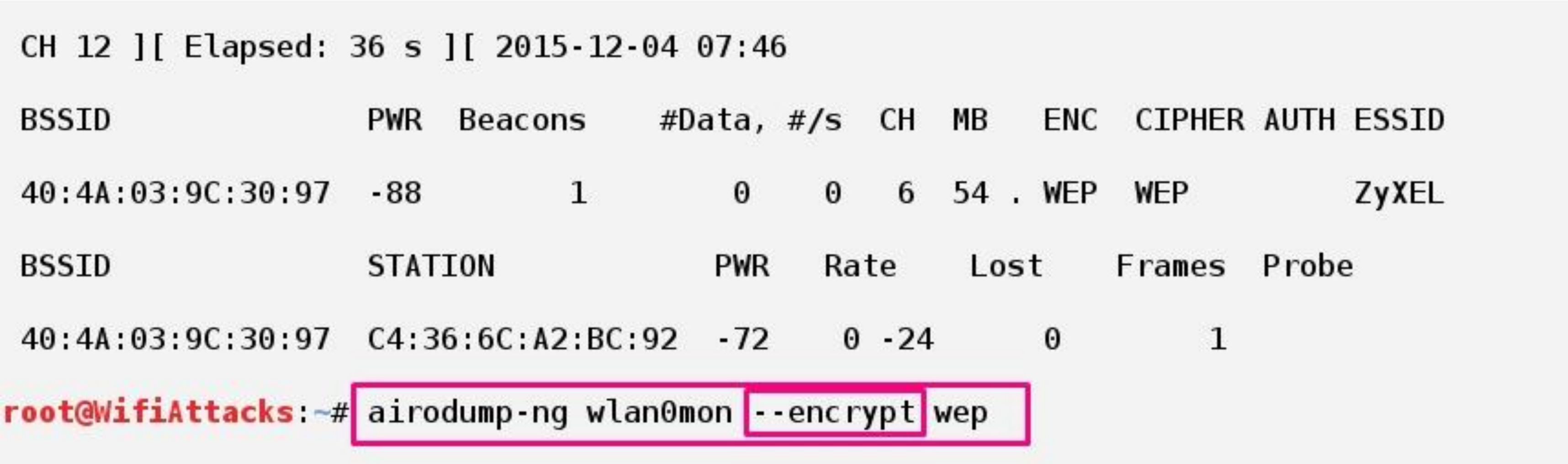


```
 CH 14 ][ Elapsed: 6 s ][ 2015-12-04 07:43

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 F8:1A:67:B8:6F:B5  -81        3        0    0   1  54e  WPA2 CCMP   PSK  TTNET_TPLINK_6FB5
 F8:3D:FF:5F:E9:0A  -86        2        0    0   9  54e  WPA2 CCMP   PSK  tatanga54
 F8:D1:11:38:B3:91  -86        3        0    0  13  54e  WPA2 CCMP   PSK  SCReaM
 54:22:F8:E9:5E:D4  -86        2        0    0   1  54e  WPA2 CCMP   PSK  TTNET_ZTE_NGDK
 F8:3D:FF:5F:C1:17  -87        6        0    0   3  54e  WPA2 CCMP   PSK  Muhendizzler

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe


root@WifiAttacks:~# airodump-ng wlan0mon
```

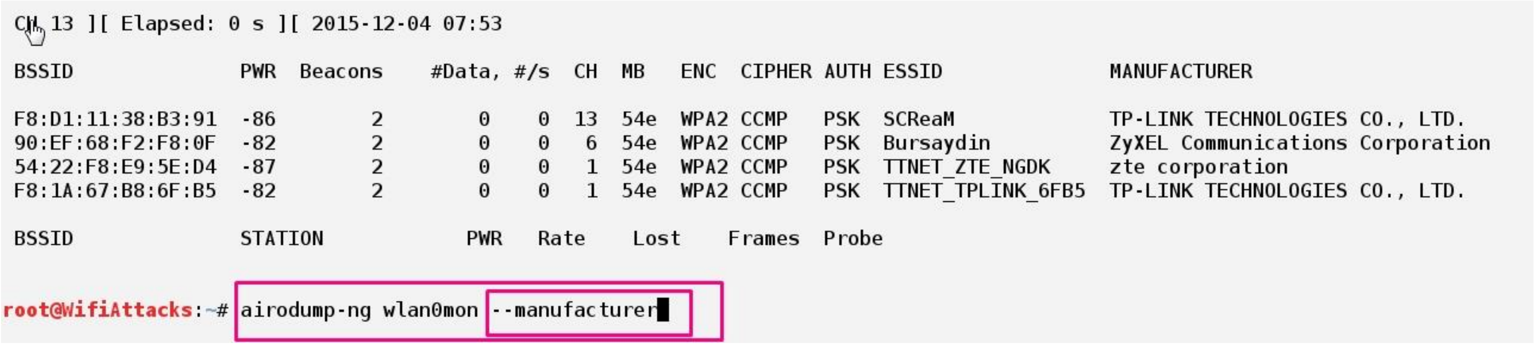


```
CH  6 ][ Elapsed: 0 s ][ 2015-12-04 07:54

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

40:4A:03:9C:30:97  -87   0       20        1    0   6  54 . WEP  WEP         ZyXEL
90:EF:68:F2:F8:0F  -78 100       26        0    0   6  54e  WPA2 CCMP   PSK  Bursaydin
E8:37:7A:C9:06:D4  -82   0       20        0    0   5  54e  WPA2 CCMP   PSK  TTNET_ZyXEL_YPRA

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

40:4A:03:9C:30:97  C4:36:6C:A2:BC:92  -73    0 -24      0        3

root@WifiAttacks:~# airodump-ng wlan0mon --channel 6
```

Airodump-ng

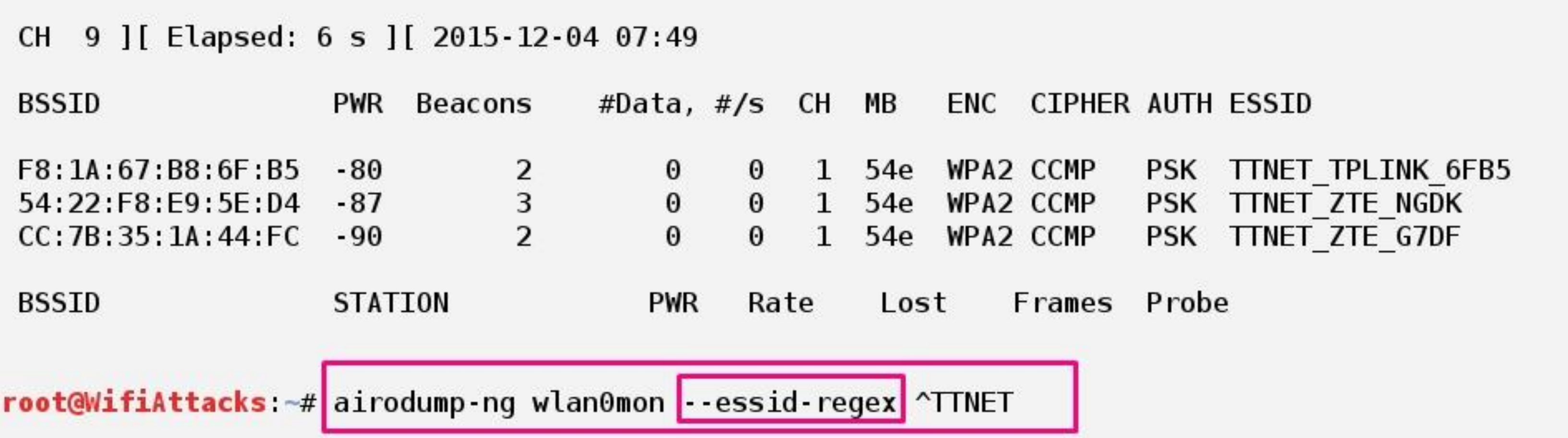


```
CH 12 ][ Elapsed: 36 s ][ 2015-12-04 07:46

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

40:4A:03:9C:30:97  -88        1        0    0   6  54 . WEP  WEP         ZyXEL

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

40:4A:03:9C:30:97  C4:36:6C:A2:BC:92  -72    0 -24      0        1

root@WifiAttacks:~# airodump-ng wlan0mon --encrypt wep
```

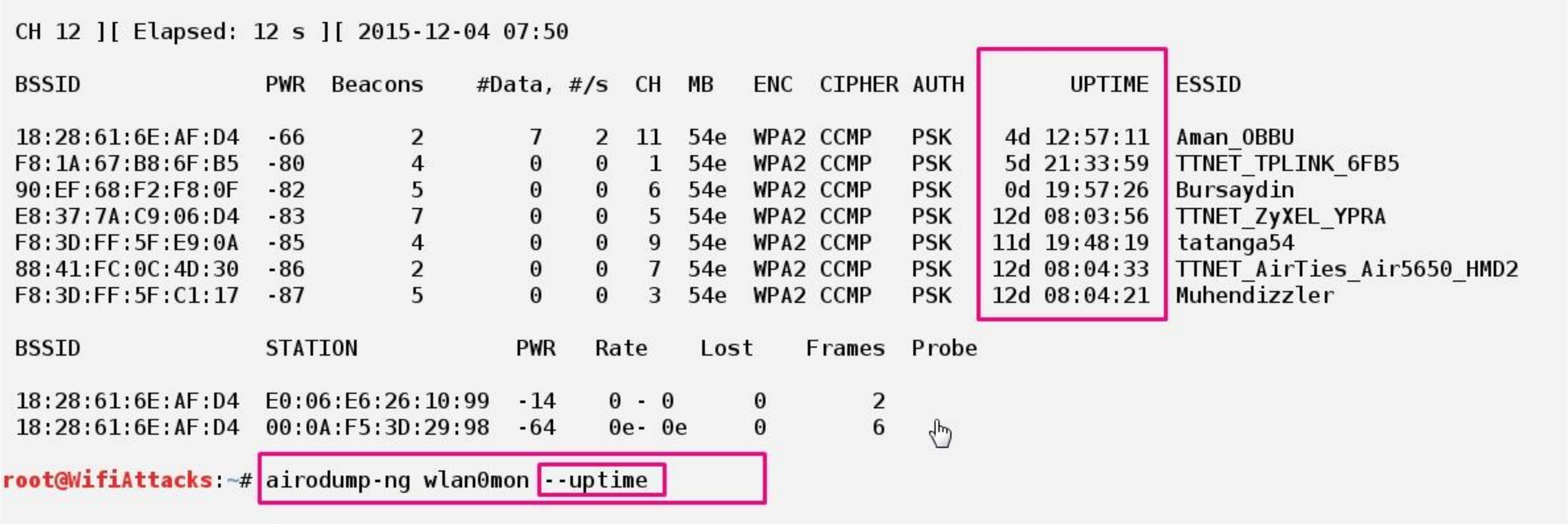


```
CH 13 ][ Elapsed: 0 s ][ 2015-12-04 07:53

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID                MANUFACTURER

F8:D1:11:38:B3:91  -86        2        0    0  13  54e  WPA2 CCMP   PSK  SCReaM               TP-LINK TECHNOLOGIES CO., LTD.
90:EF:68:F2:F8:0F  -82        2        0    0   6  54e  WPA2 CCMP   PSK  Bursaydin            ZyXEL Communications Corporation
54:22:F8:E9:5E:D4  -87        2        0    0   1  54e  WPA2 CCMP   PSK  TTNET_ZTE_NGDK       zte corporation
F8:1A:67:B8:6F:B5  -82        2        0    0   1  54e  WPA2 CCMP   PSK  TTNET_TPLINK_6FB5    TP-LINK TECHNOLOGIES CO., LTD.

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

root@WifiAttacks:~# airodump-ng wlan0mon --manufacturer
```

Airodump-ng

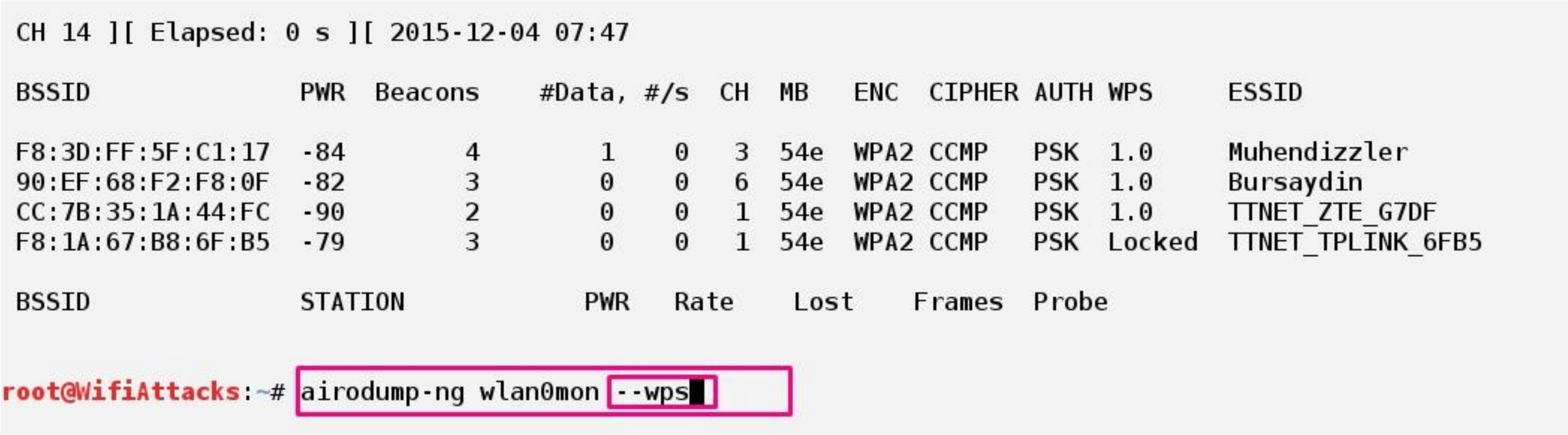


```
CH  9 ][ Elapsed: 6 s ][ 2015-12-04 07:49

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

F8:1A:67:B8:6F:B5  -80        2        0    0   1  54e  WPA2 CCMP   PSK  TTNET_TPLINK_6FB5
54:22:F8:E9:5E:D4  -87        3        0    0   1  54e  WPA2 CCMP   PSK  TTNET_ZTE_NGDK
CC:7B:35:1A:44:FC  -90        2        0    0   1  54e  WPA2 CCMP   PSK  TTNET_ZTE_G7DF

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

root@WifiAttacks:~# airodump-ng wlan0mon --essid-regex ^TTNET
```

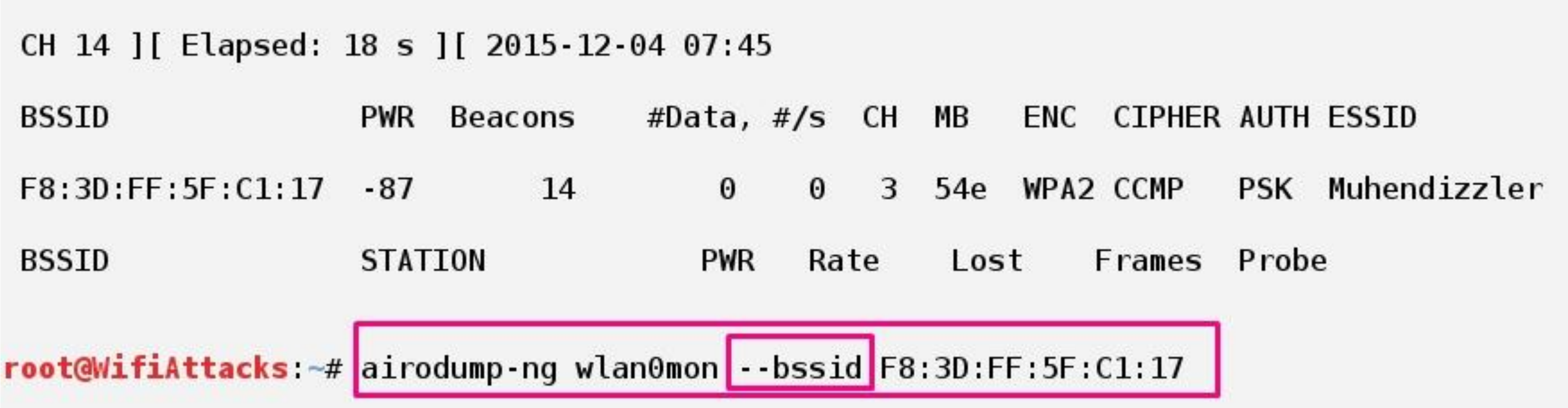


```
CH 12 ][ Elapsed: 12 s ][ 2015-12-04 07:50

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH       UPTIME  ESSID

18:28:61:6E:AF:D4  -66        2        7    2  11  54e  WPA2 CCMP   PSK   4d 12:57:11  Aman_0BBU
F8:1A:67:B8:6F:B5  -80        4        0    0   1  54e  WPA2 CCMP   PSK   5d 21:33:59  TTNET_TPLINK_6FB5
90:EF:68:F2:F8:0F  -82        5        0    0   6  54e  WPA2 CCMP   PSK   0d 19:57:26  Bursaydin
E8:37:7A:C9:06:D4  -83        7        0    0   5  54e  WPA2 CCMP   PSK  12d 08:03:56  TTNET_ZyXEL_YPRA
F8:3D:FF:5F:E9:0A  -85        4        0    0   9  54e  WPA2 CCMP   PSK  11d 19:48:19  tatanga54
88:41:FC:0C:4D:30  -86        2        0    0   7  54e  WPA2 CCMP   PSK  12d 08:04:33  TTNET_AirTies_Air5650_HMD2
F8:3D:FF:5F:C1:17  -87        5        0    0   3  54e  WPA2 CCMP   PSK  12d 08:04:21  Muhendizzler

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

18:28:61:6E:AF:D4  E0:06:E6:26:10:99  -14    0 - 0      0        2
18:28:61:6E:AF:D4  00:0A:F5:3D:29:98  -64   0e- 0e      0        6

root@WifiAttacks:~# airodump-ng wlan0mon --uptime
```

Airodump-ng



```
CH 14 ][ Elapsed: 0 s ][ 2015-12-04 07:47

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH WPS     ESSID

F8:3D:FF:5F:C1:17  -84        4        1    0   3  54e  WPA2 CCMP   PSK  1.0     Muhendizzler
90:EF:68:F2:F8:0F  -82        3        0    0   6  54e  WPA2 CCMP   PSK  1.0     Bursaydin
CC:7B:35:1A:44:FC  -90        2        0    0   1  54e  WPA2 CCMP   PSK  1.0     TTNET_ZTE_G7DF
F8:1A:67:B8:6F:B5  -79        3        0    0   1  54e  WPA2 CCMP   PSK  Locked  TTNET_TPLINK_6FB5

BSSID              STATION            PWR   Rate    Lost    Frames  Probe


root@WifiAttacks:~# airodump-ng wlan0mon --wps
```



```
CH 14 ][ Elapsed: 18 s ][ 2015-12-04 07:45

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

F8:3D:FF:5F:C1:17  -87       14        0    0   3  54e  WPA2 CCMP   PSK  Muhendizzler

BSSID              STATION            PWR   Rate    Lost    Frames  Probe


root@WifiAttacks:~# airodump-ng wlan0mon --bssid F8:3D:FF:5F:C1:17
```