**LAPORAN TUGAS**

Wireless WEP WPA2 Hacking

Disusun untuk Memenuhi Tugas Mata Kuliah Network Security  
Dosen Pengampu Amang Sudarsono, ST., Ph.D.

Oleh :

**Muhammad Taufiq Sumadi**

**2020191020**

****

**PROGRAM STUDI TEKNIK INFORMATIKA DAN KOMPUTER**

**PROGRAM PASCASARJANA**

**POLITEKNIK ELEKTRONIKA NEGERI SURABAYA**

**2019**

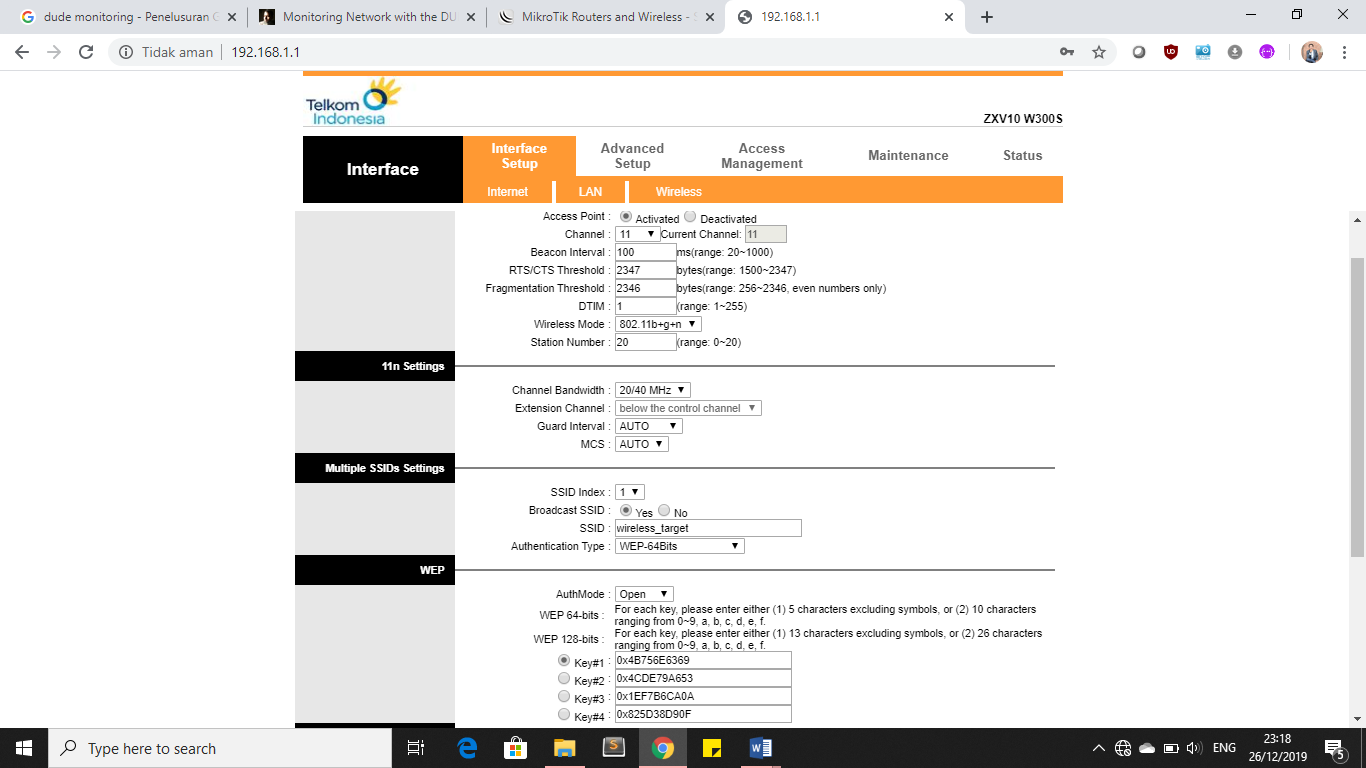
Aircrack For Wifi Penetration Testing

Aircrack adalah tools sederhana yang sering digunakan untuk melakukan penetration testing wifi. Secara sederhana konsep aircrack adalah melakukan capture data/sniffing packet dengan wireless card pada perangkat kita yang diatur dengan mode monitoring.

* Crack Wifi yang menggunakan WEP

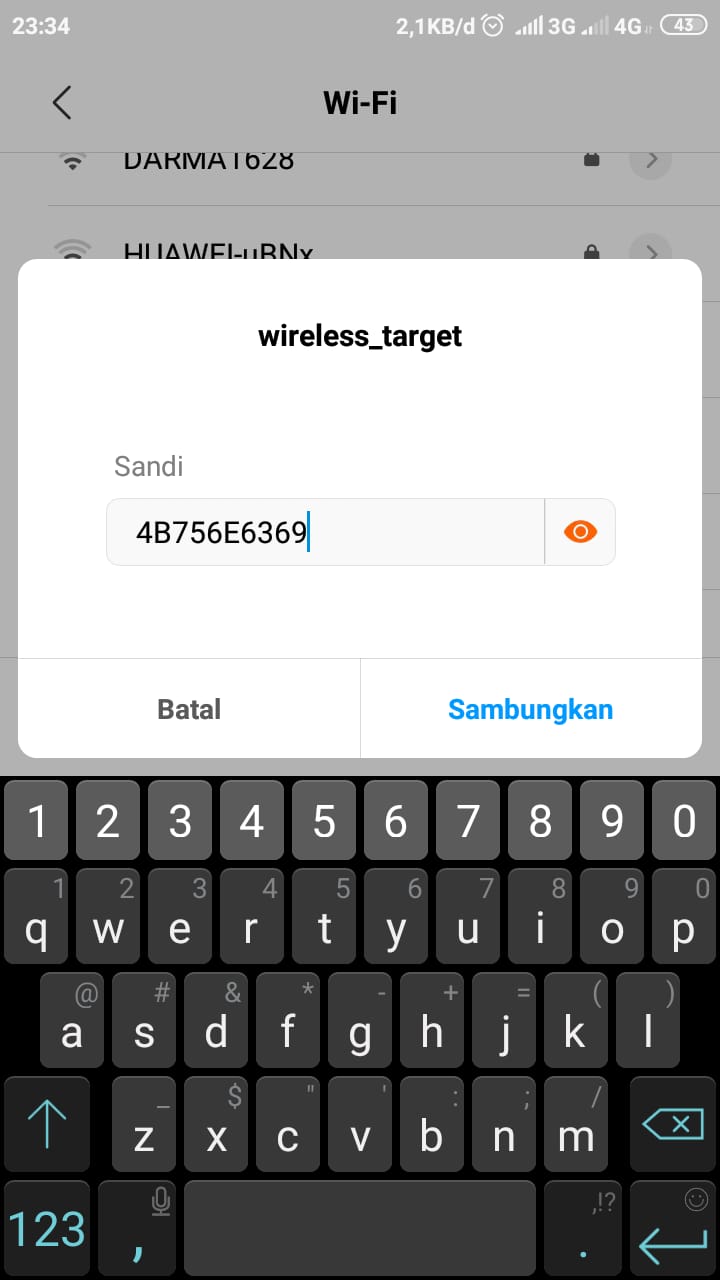
1. Setting wifi dengan keamanan WEP

Disini saya menggunakan ZTE ZXV10 W300S, access point (AP) bekas indihome. Reset terlebih dahulu AP dengan menekan lubang kecil yang terdapat pada bagian belakang AP dengan menggunakan jarum atau benda lain. Kemudian hubungkan AP dengan komputer anda menggunakan kabel UTP. Langkah selanjutnya buka browser dengan mengetikan alamat IP AP. Disini AP yang saya gunakan beralamatkan 192.168.1.1.



Masukan username dan password default AP, pada AP ZTE ZXV10 W300S username:**admin** password:**admin**. Kemudian konfigurasi seperti gambar diatas, pilih channel yang akan digunakan, beri nama SSID, pilih authentication type WEP dan setting key ***0x4B756E6369*** (hex).

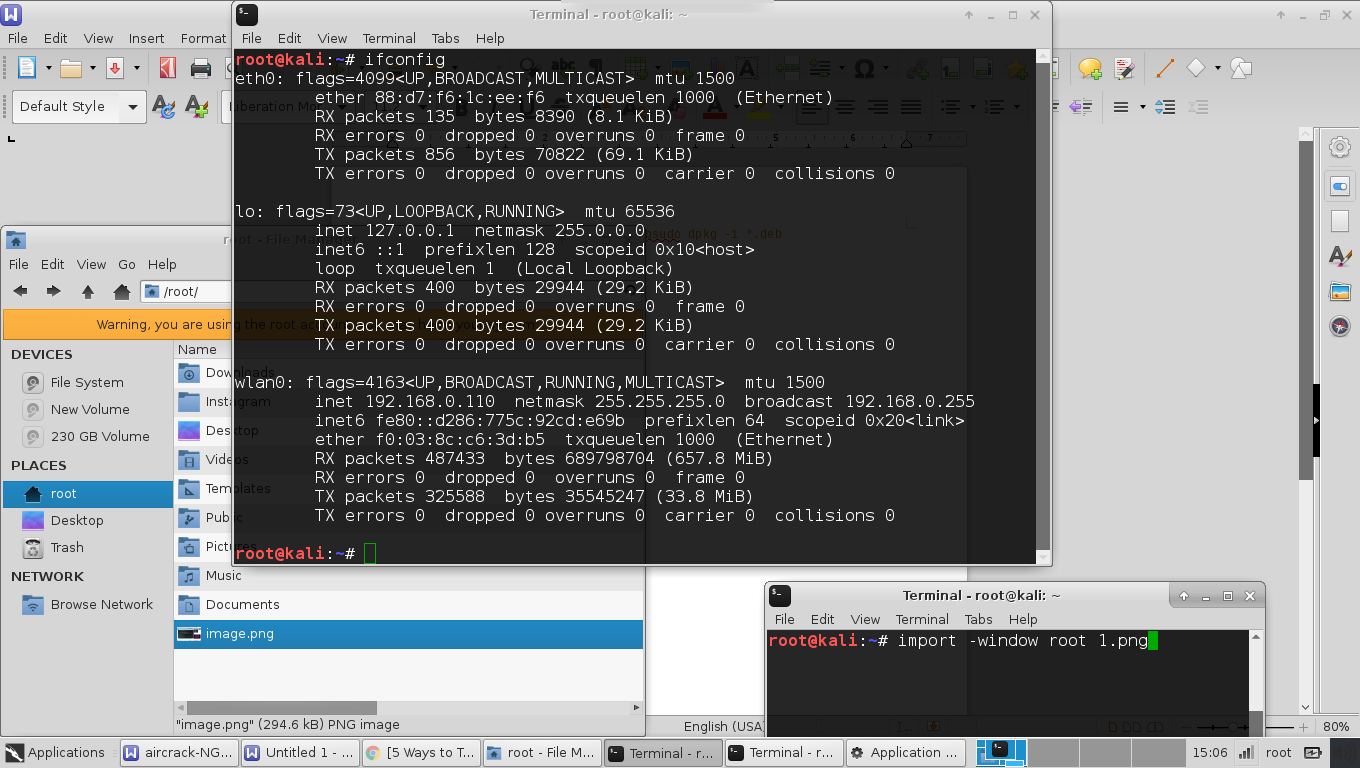




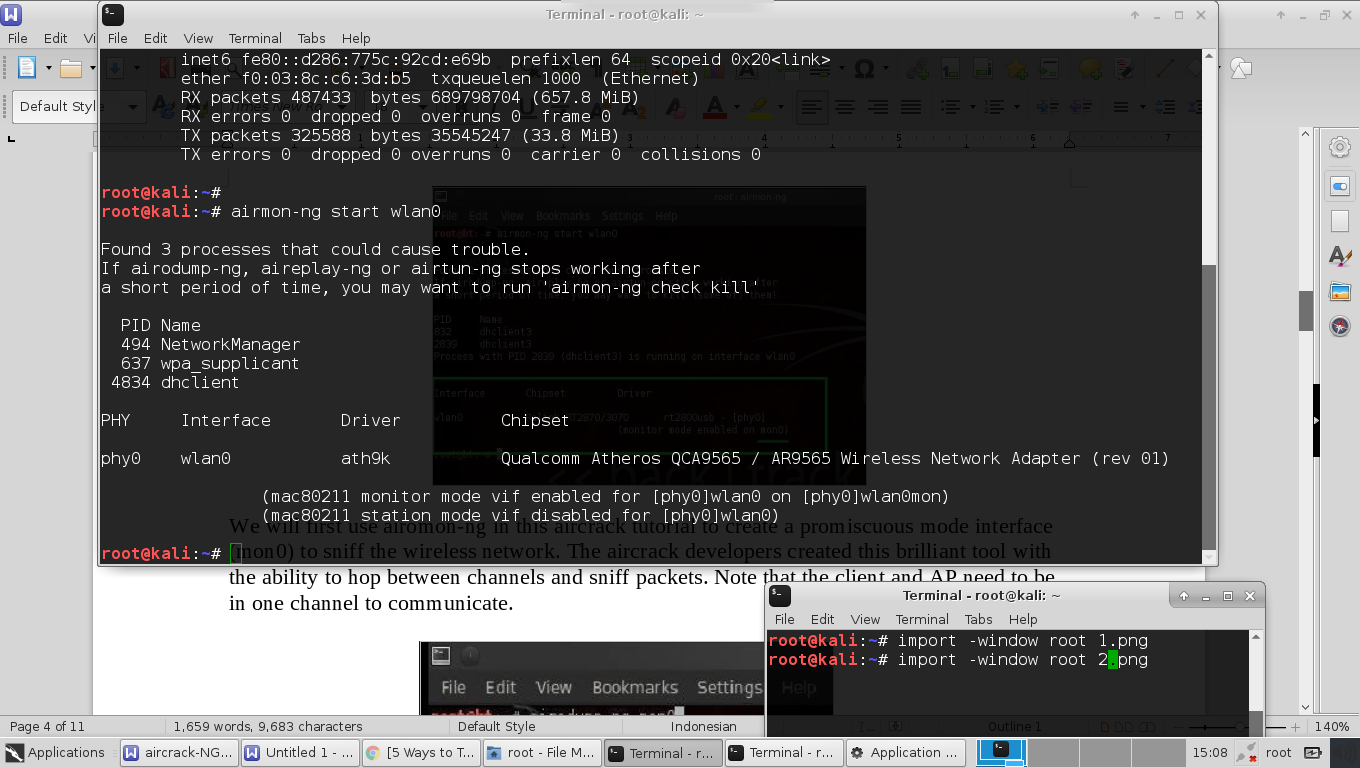
Saya menggunakan smartphone android sebagai target. Koneksikan smartphone ke AP dapat dengan mengisikan sandi dalam bentuk hexadecimal atau karakter (string).

1. Konfigurasi pada Attacker

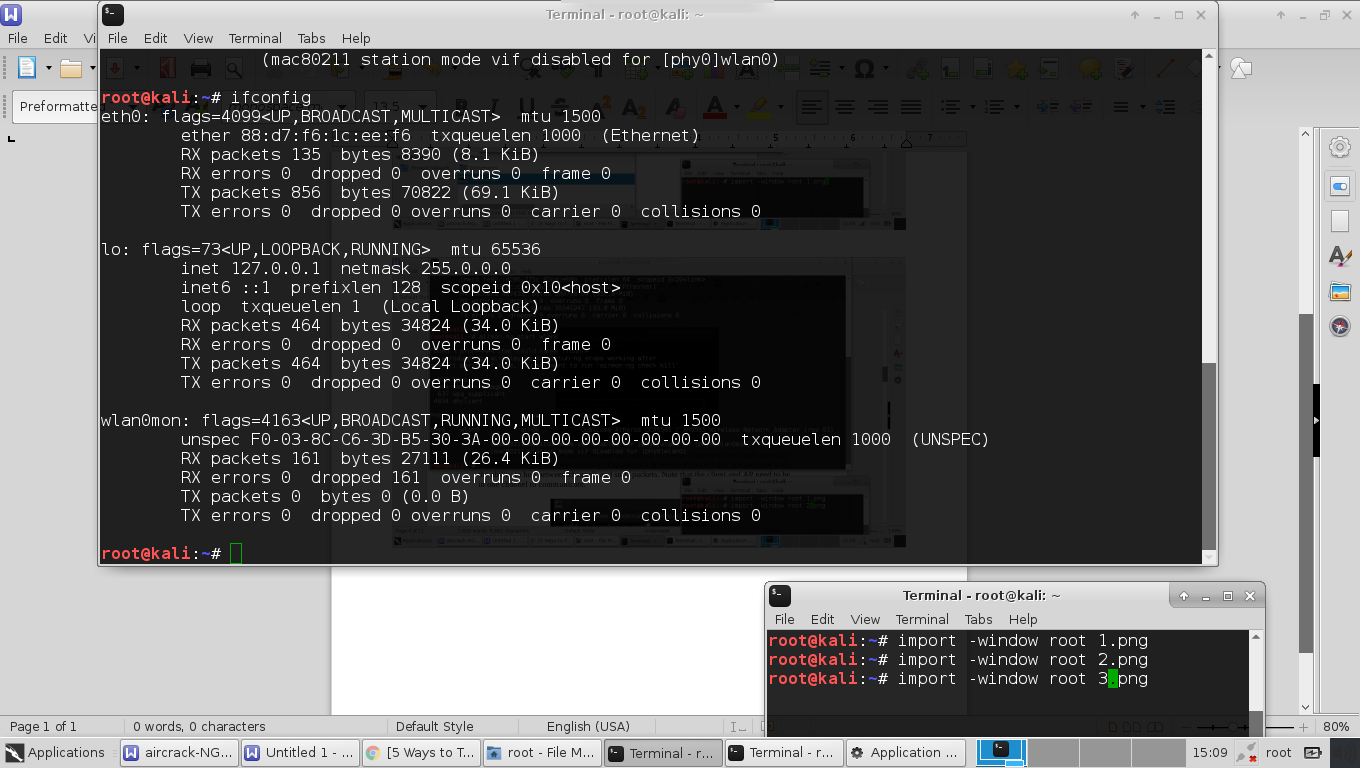
Cek kartu jaringan pada perangkat kita, disini saya menjalankan sistem operasi kali linux sebagai host, jika anda menjalankan kali linux pada vmware/virtual box anda membutuhkan kartu jaringan tambahan untuk dapat melakukan monitoring paket. Cek kartu jaringan pada komputer kita dengan perintah “**ifconfig**”.



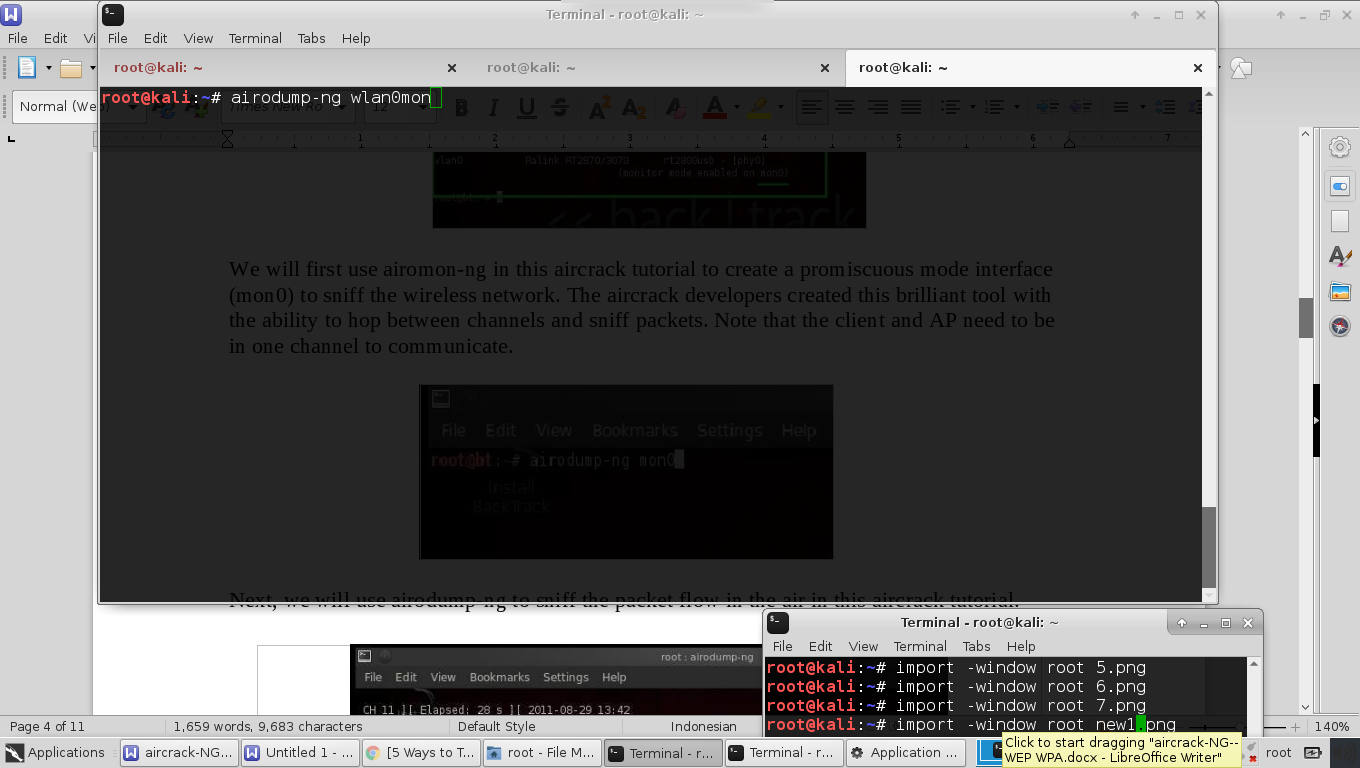
Maka akan muncul wlan0 (penamaan ini dapat berbeda di tiap komputer terutama jika operating system yang digunakan berbeda). Langkah selanjutnya adalah merubah fungsi wireless pada perangkat kita menjadi mode monitor, “**airmon-ng wlan0**”.

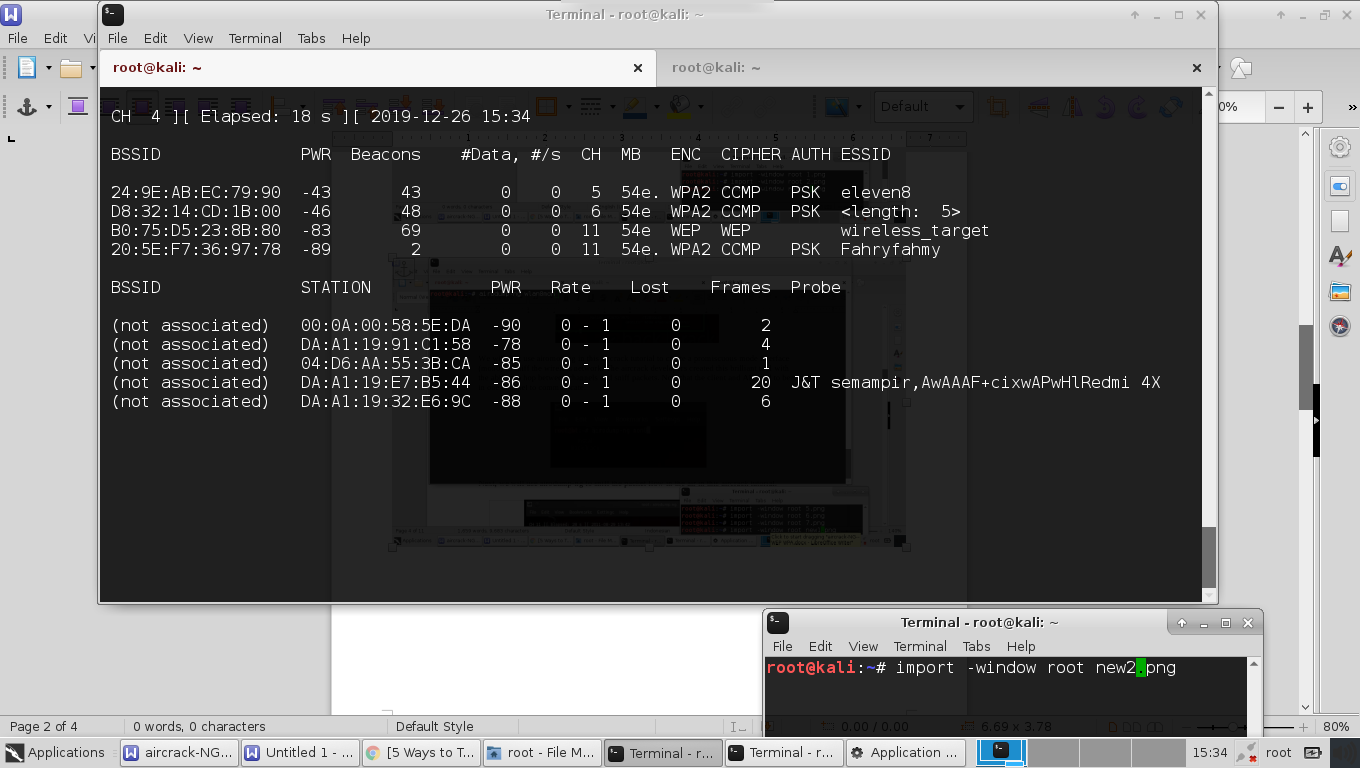


Setelah menjalankan script bash diatas, maka wireless card yang kita gunakan menjadi mode monitor, cek dengan menggunakan perintah “**ifconfig**”.

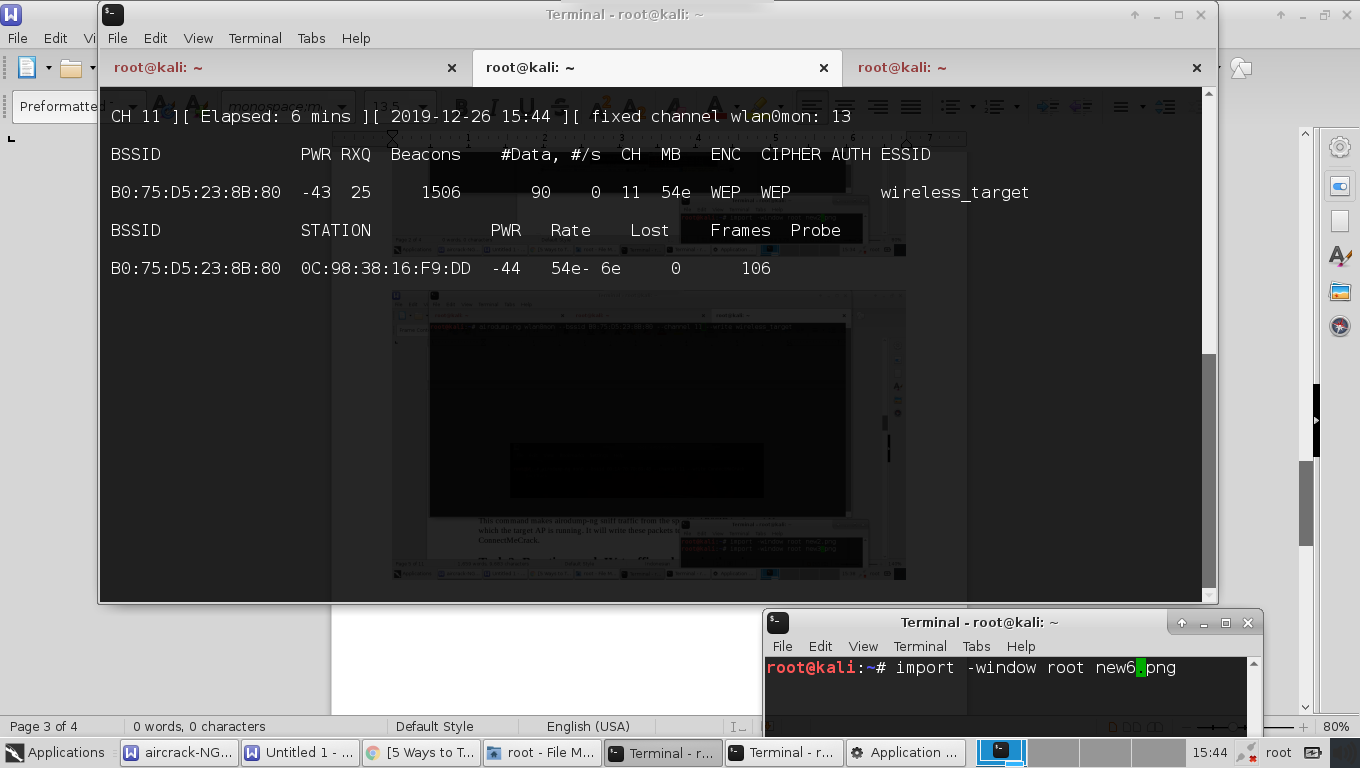
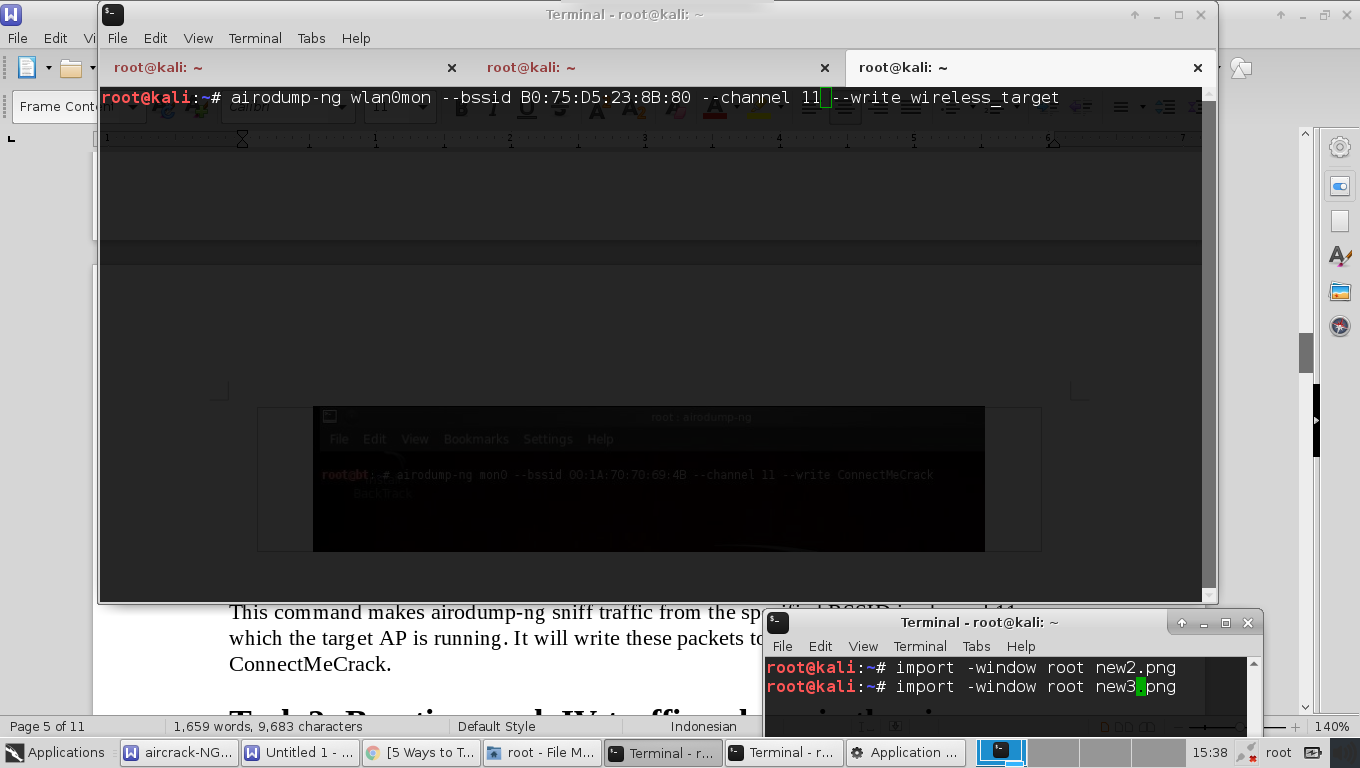


“*wlan0mon*” menunjukan bahwa wireless card yang digunakan sudah menjadi mode monitor. Jalankan bash shell dengan perintah “**airodump-ng wlan0mon**”.

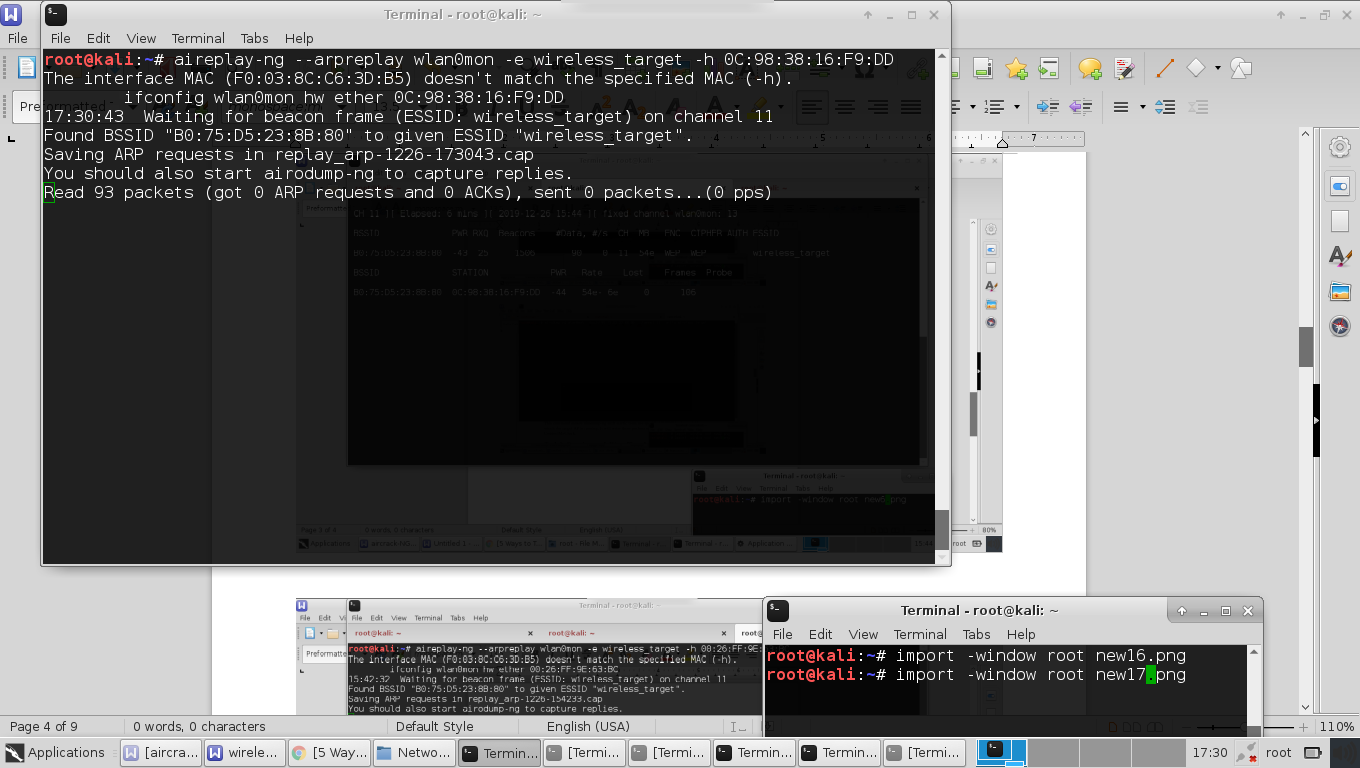




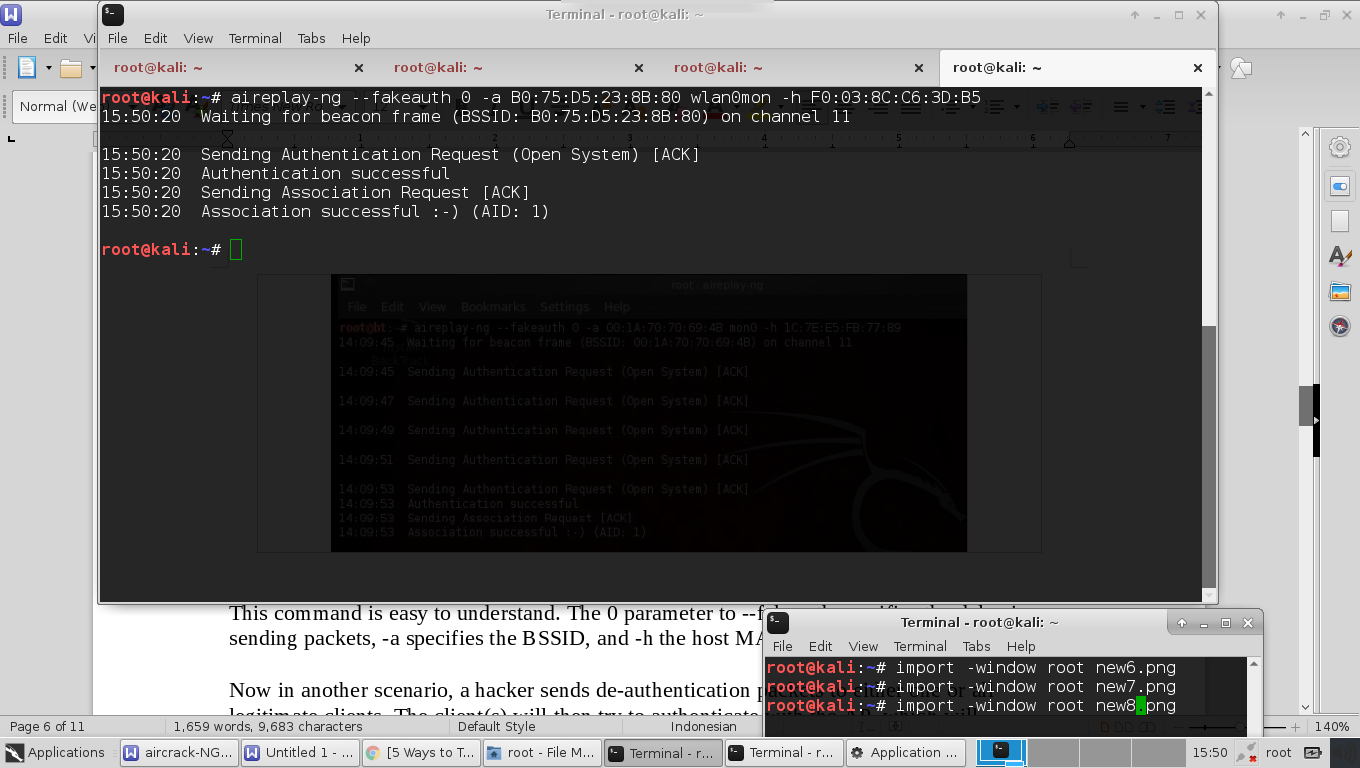
Perintah ini akan menampilkan list AP yang berada dalam jangkauan wireless card kita. Kemudian jalankan perintah “**airodump-ng [name\_wireless\_card] –bssid [bssid\_target] –channel [channel] --write [nama\_file\_hasil\_capture]**”.



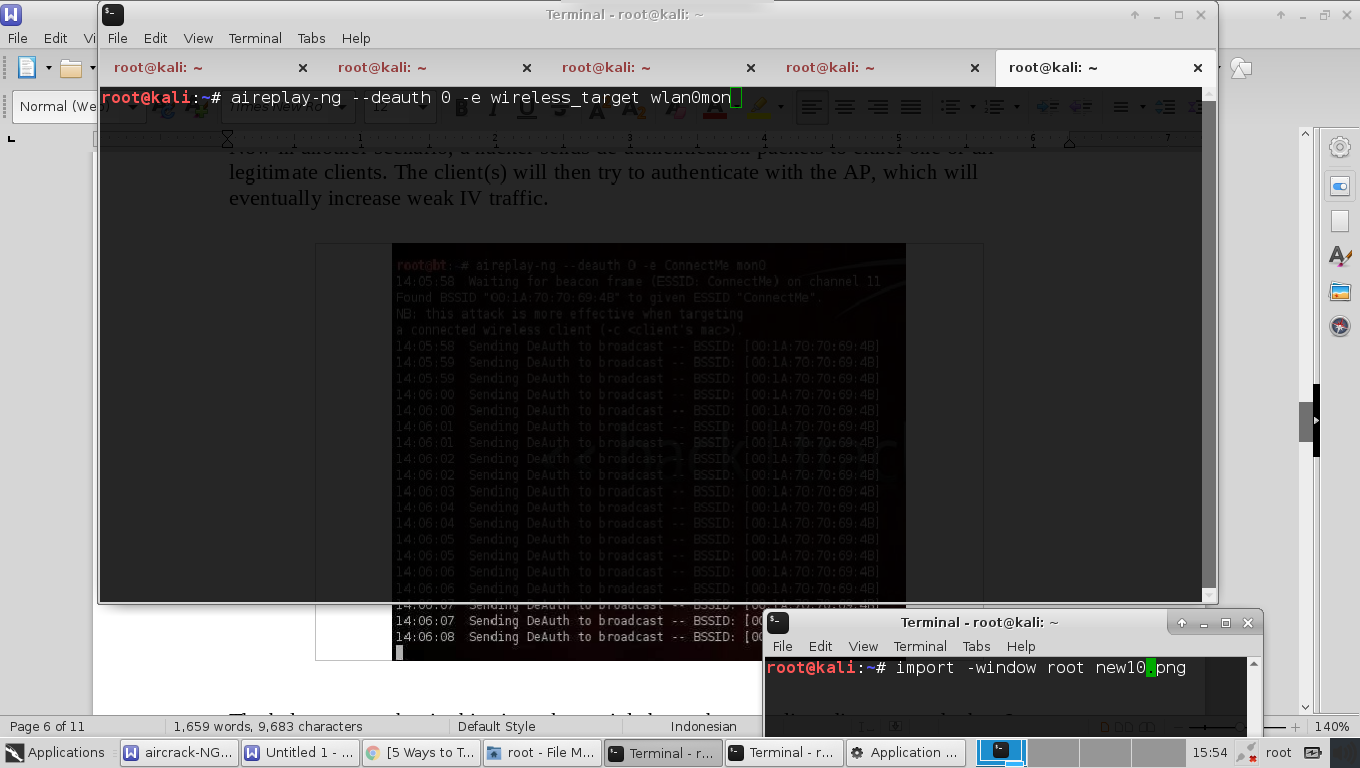
Proses diatas akan melakukan proses capture paket pada ESSID “**wireless\_target**” dan STATION menunjukan mac address yang terkoneksi ke AP (mac address smarphone korban). Kemudian jalankan perintah shell “**aireplay-ng –arpreplay [name\_wireless\_card] –e [ESSID] –h [mac\_address\_client\_yang\_terkoneksi\_AP]**”. Mac address client yang terkoneksi dengan AP dapat dilihat dari proses sebelumnya menggunkan **airodump-ng** dibagian STATION.



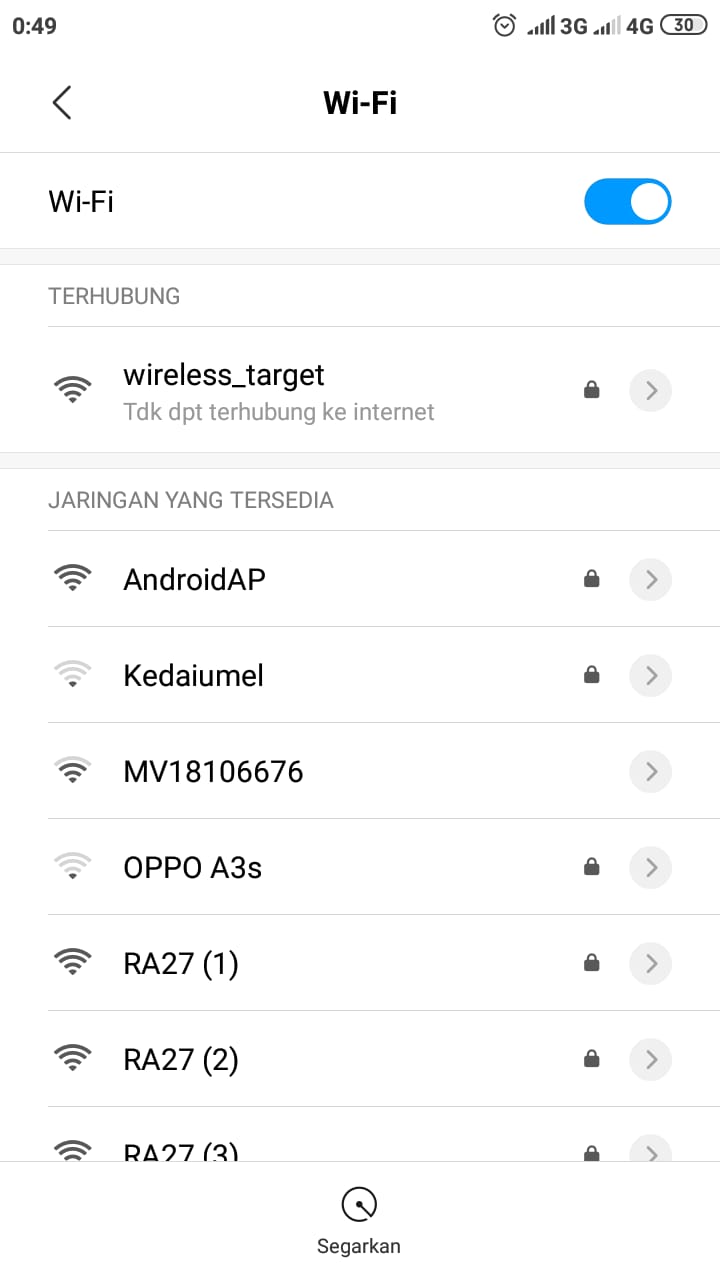
Kemudian jalankan “**aireplay-ng –fakeauth 0 –a [mac\_address\_AP] [name\_wireless\_card] –h [mac\_address\_attacker]**”



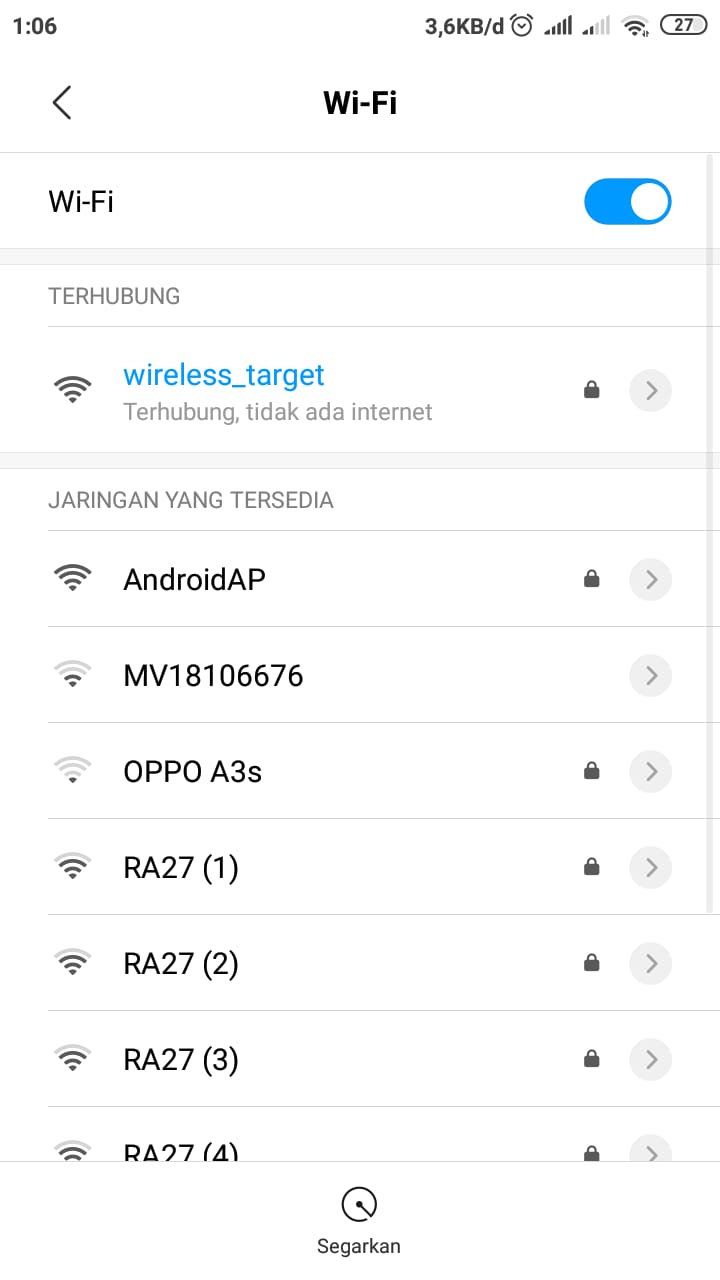
Langkah selanjutnya jalankan “**aireplay-ng –deauth 0 –e [ESSID] [name\_wireless\_card]**”



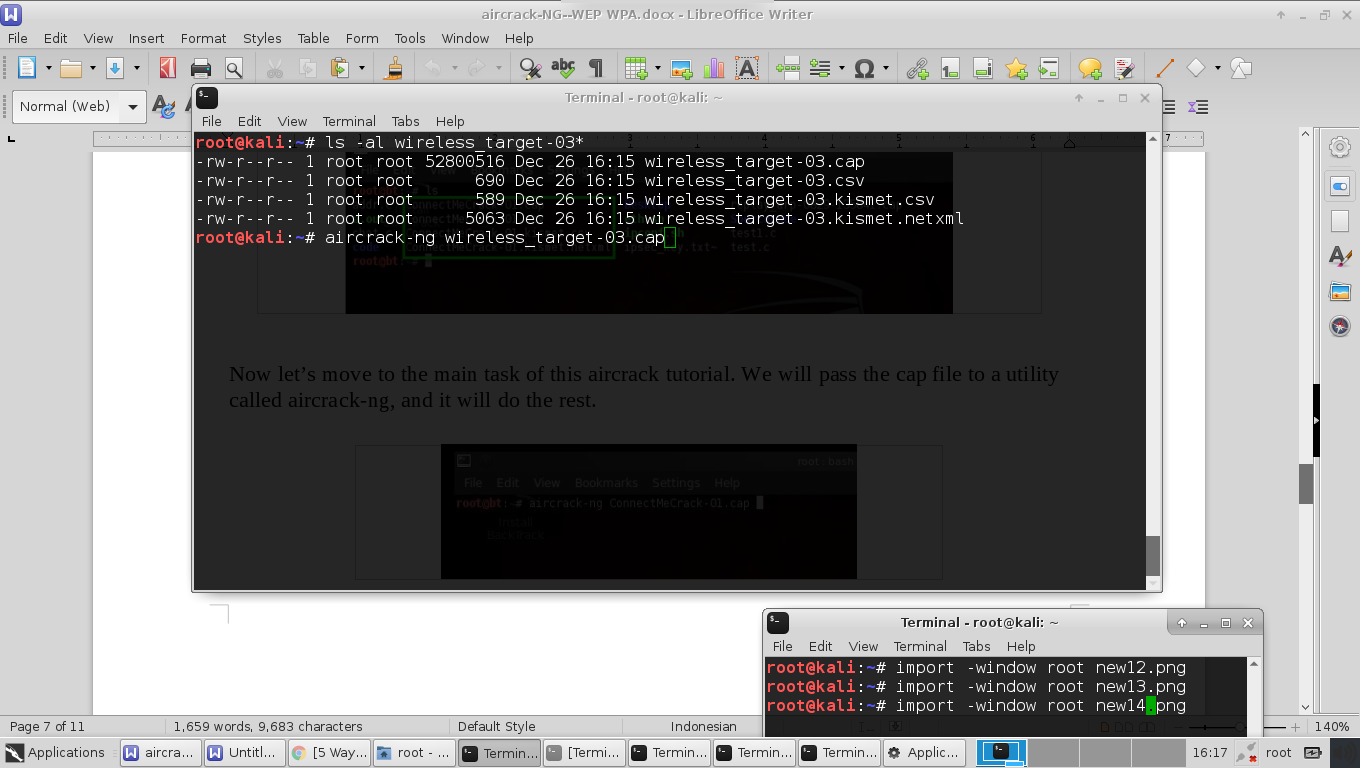
Proses ini akan mengakibatkan seluruh client yang terkoneksi ke AP, terputus. Tunggu sampai beberapa saat dalam jangka waktu tertentu hingga seluruh client terputus kemudian “**Ctrl+c**” untuk menghentikan proses ini.

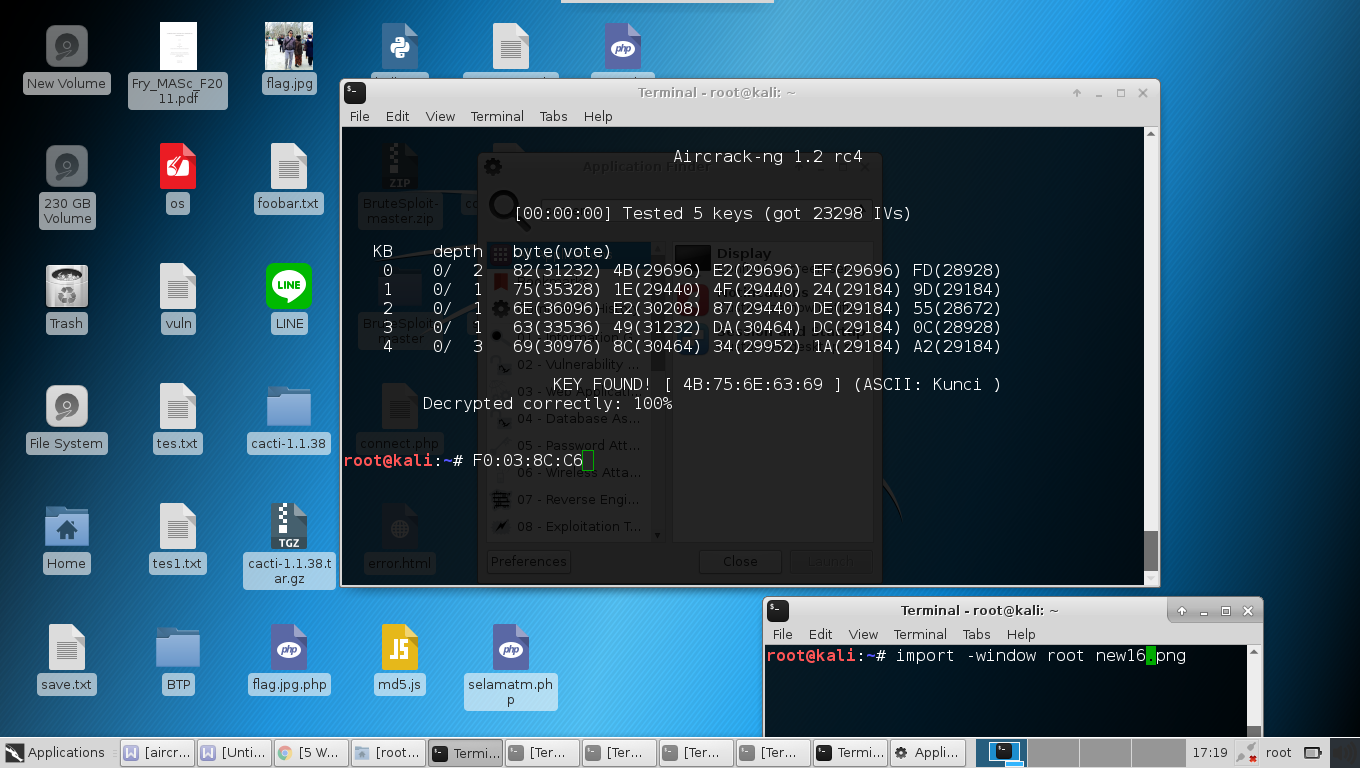


Pada smartphone korban akan terputus seperti ditunjukan pada gambar diatas. Setelah proses deauth flooding diberhentikan, client akan terkoneksi kembali.



Setelah client terkoneksi kembali, kemudian jalankan “**aircrack-ng** **[file\_name\_capture.cap]**”.

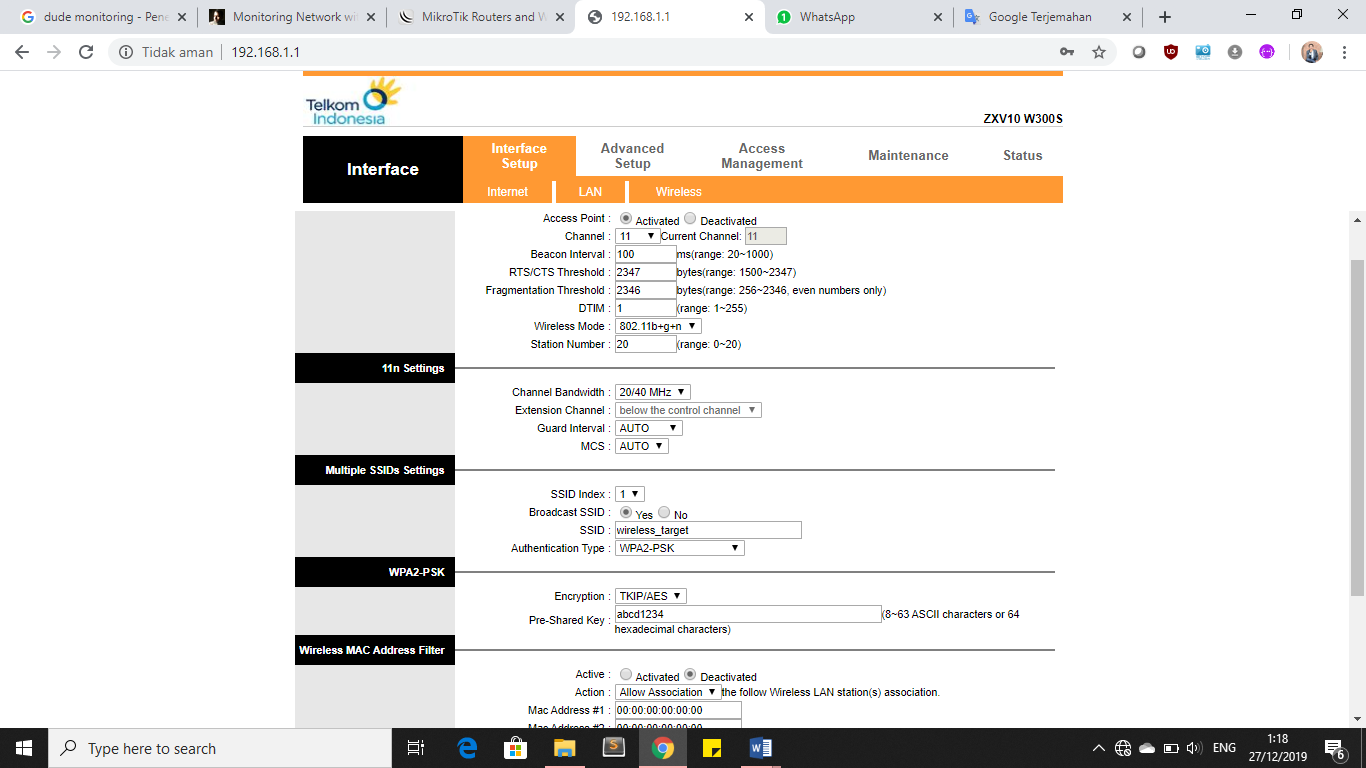




Pada gambar diatas menunjukan password AP berhasil dihack **4B756E6369 (hex) atau Kunci (Ascii).**

* Crack Wifi yang menggunakan WPA2

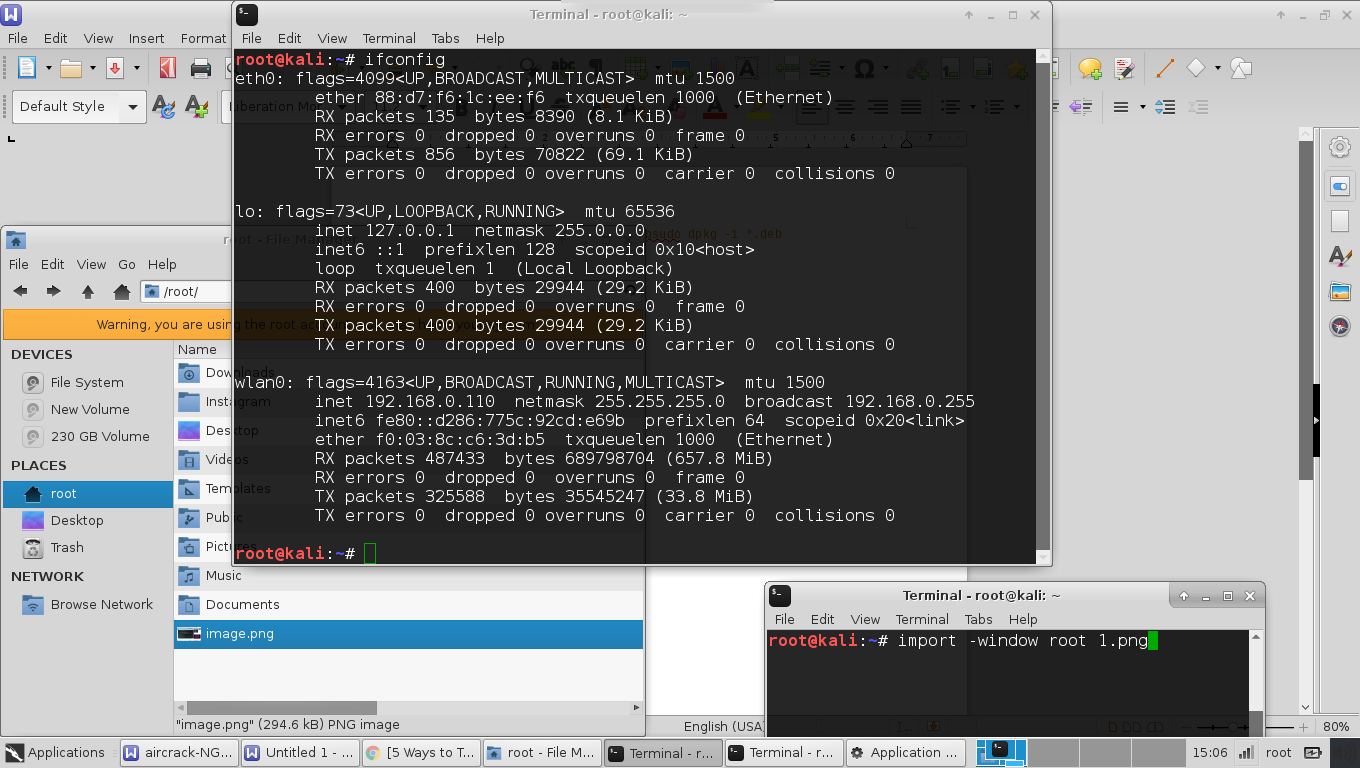
1. Setting wifi dengan keamanan WPA2



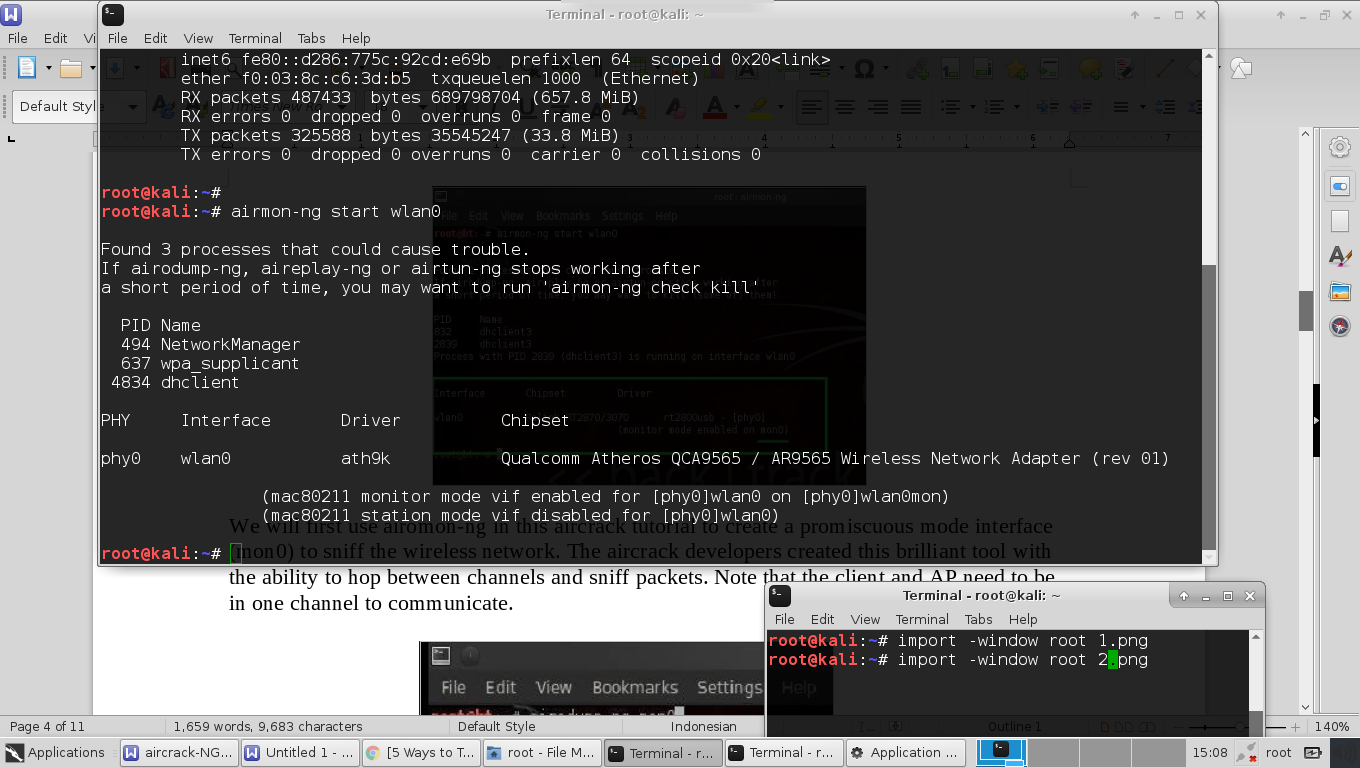
Konfigurasi AP, pilih channel yang digunakan, beri nama SSID, pilih Authentication Type **WPA2-PSK**, Encryption **TKIP/AES** danisikan password AP.

1. Konfigurasi pada Attacker

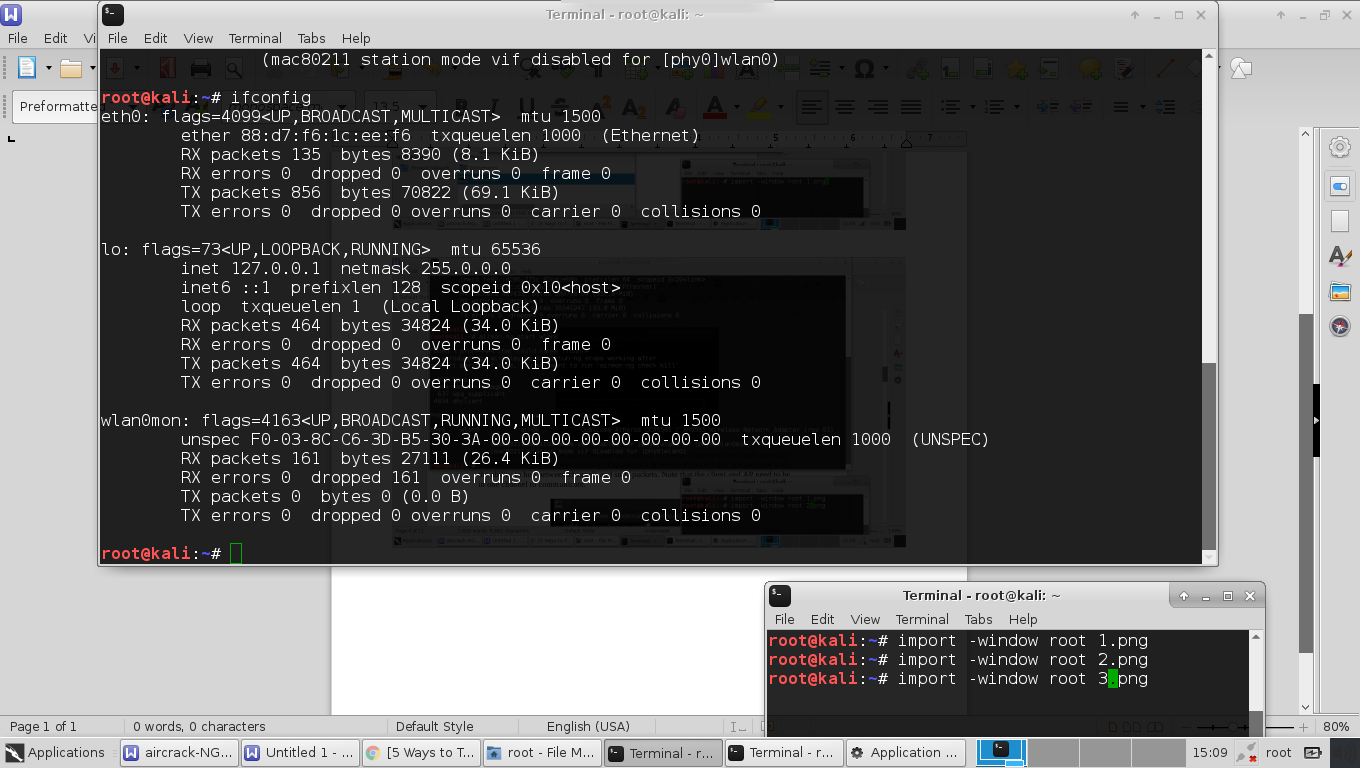
Cek kartu jaringan pada perangkat kita, disini saya menjalankan sistem operasi kali linux sebagai host, jika anda menjalankan kali linux pada vmware/virtual box anda membutuhkan kartu jaringan tambahan untuk dapat melakukan monitoring paket. Cek kartu jaringan pada komputer kita dengan perintah “**ifconfig**”.



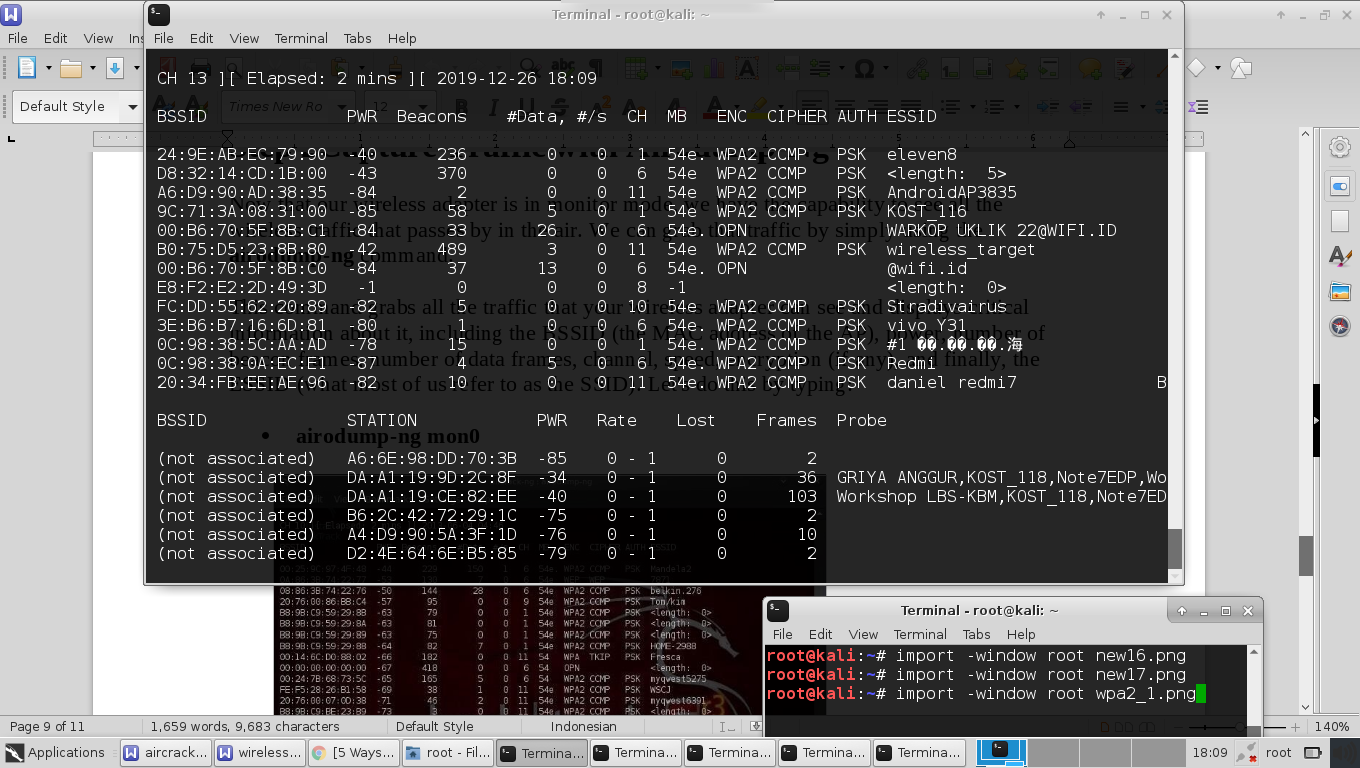
Maka akan muncul wlan0 (penamaan ini dapat berbeda di tiap komputer terutama jika operating system yang digunakan berbeda). Langkah selanjutnya adalah merubah fungsi wireless pada perangkat kita menjadi mode monitor, “**airmon-ng wlan0**”.



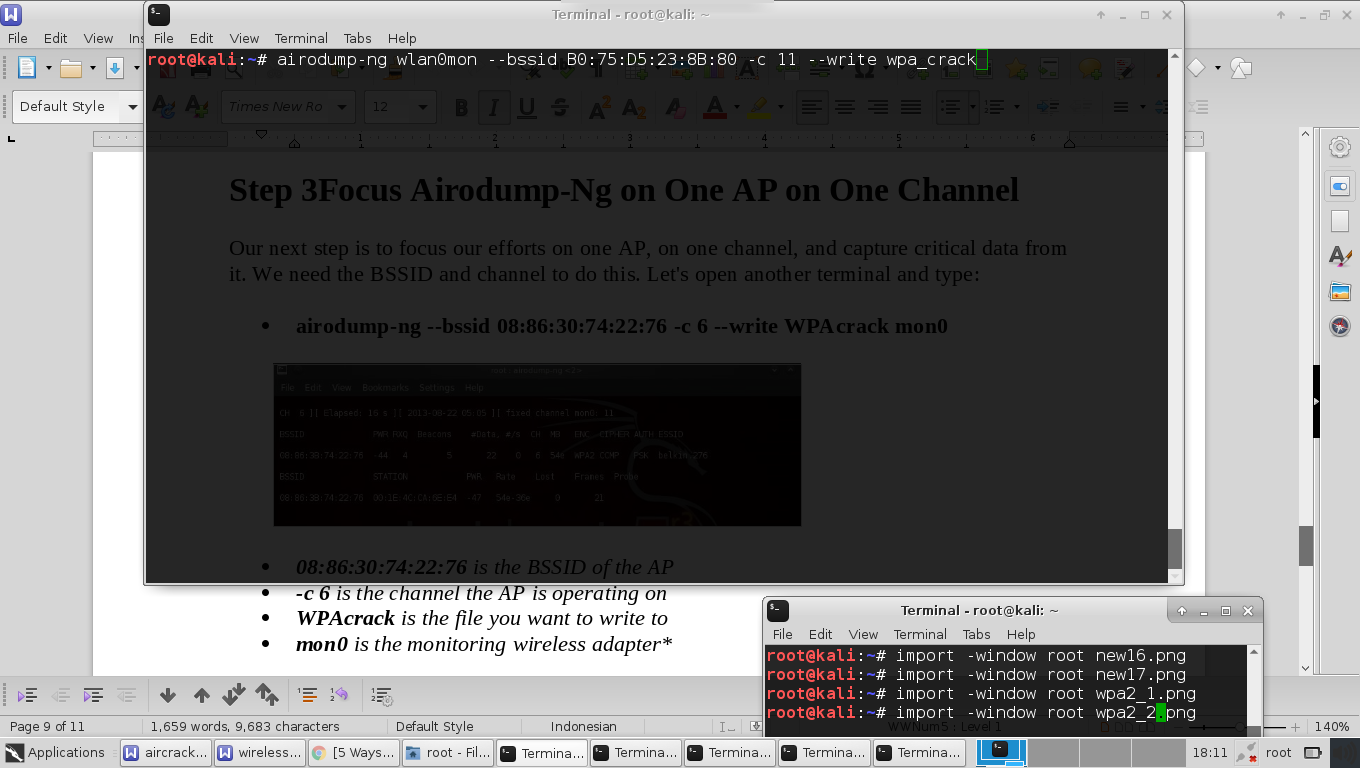
Setelah menjalankan script bash diatas, maka wireless card yang kita gunakan menjadi mode monitor, cek dengan menggunakan perintah “**ifconfig**”.

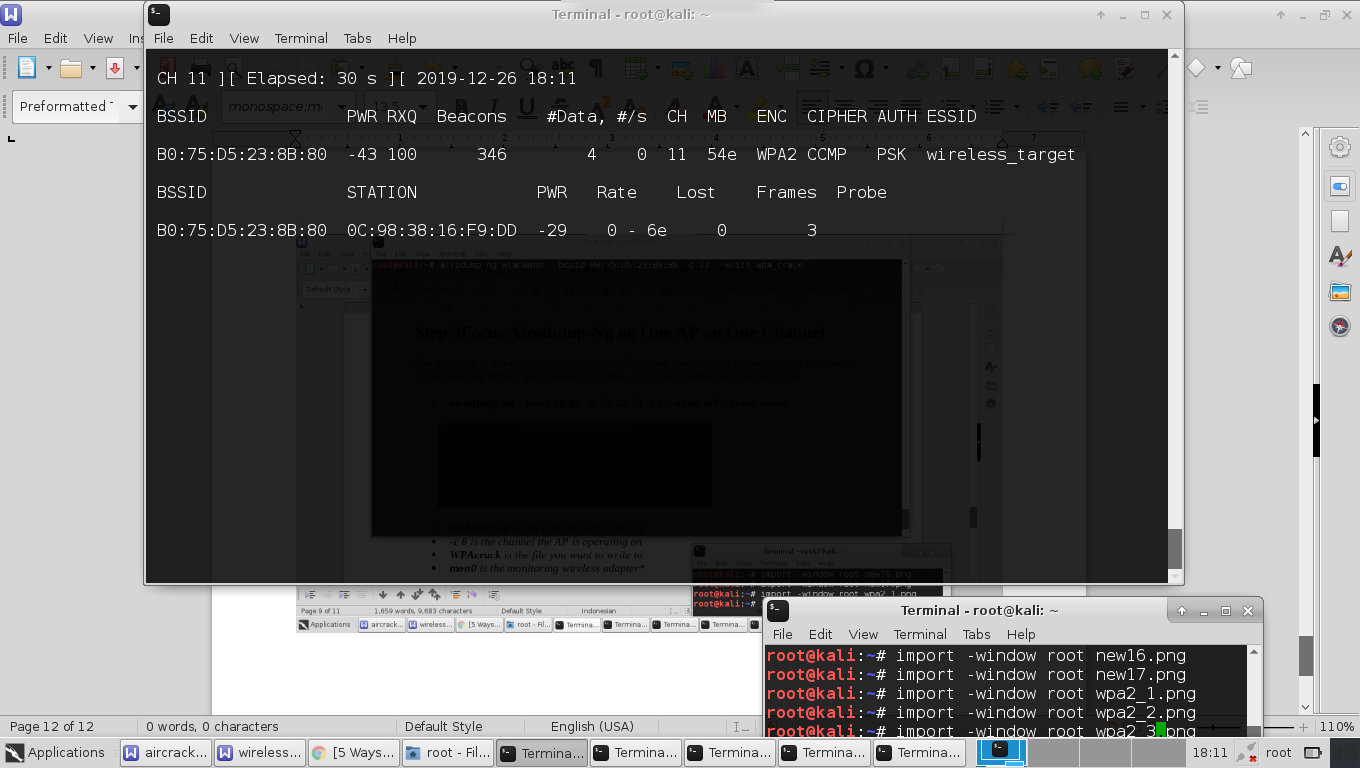


“*wlan0mon*” menunjukan bahwa wireless card yang digunakan sudah menjadi mode monitor. Jalankan bash shell dengan perintah “**airodump-ng wlan0mon**”.

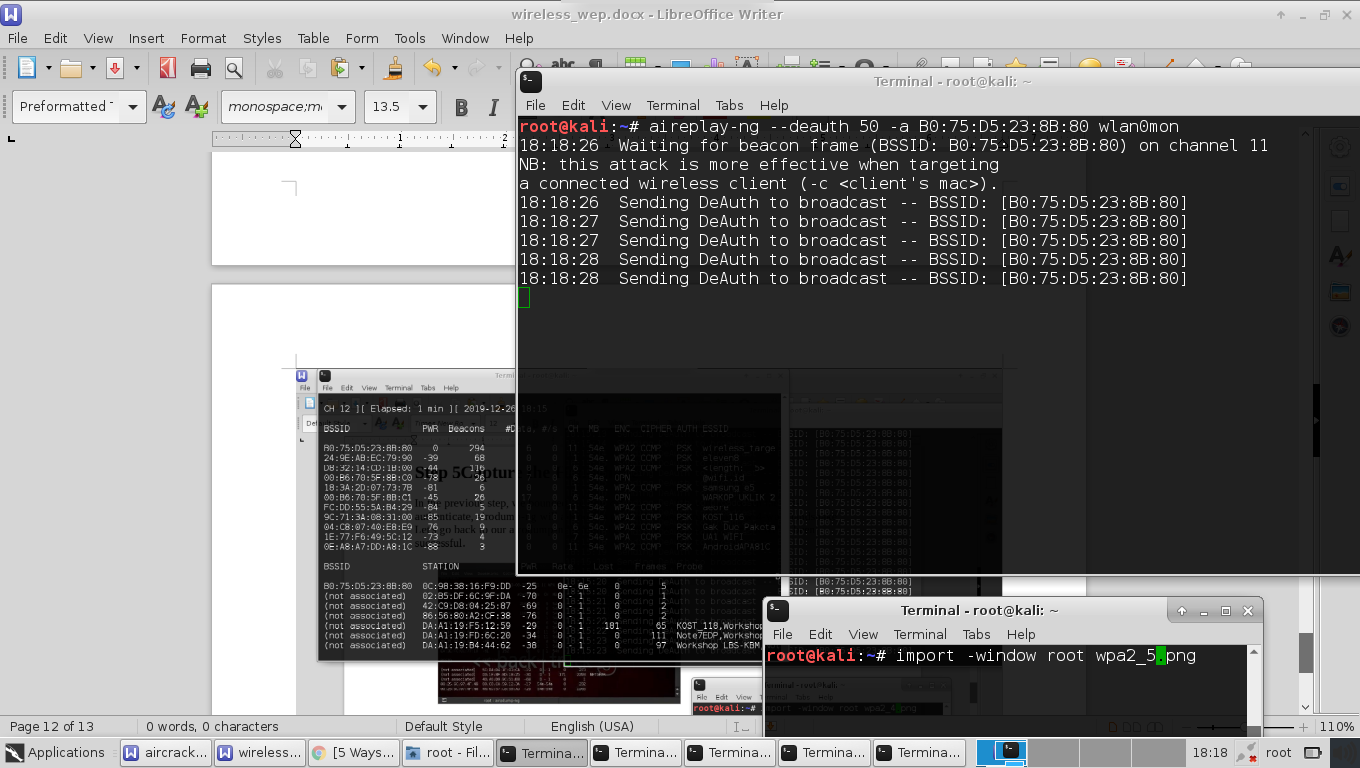


Perintah ini akan menampilkan list AP yang berada dalam jangkauan wireless card kita. Kemudian jalankan perintah “**airodump-ng [name\_wireless\_card] –bssid [bssid\_target] –c [channel] --write [nama\_file\_hasil\_capture]**”.

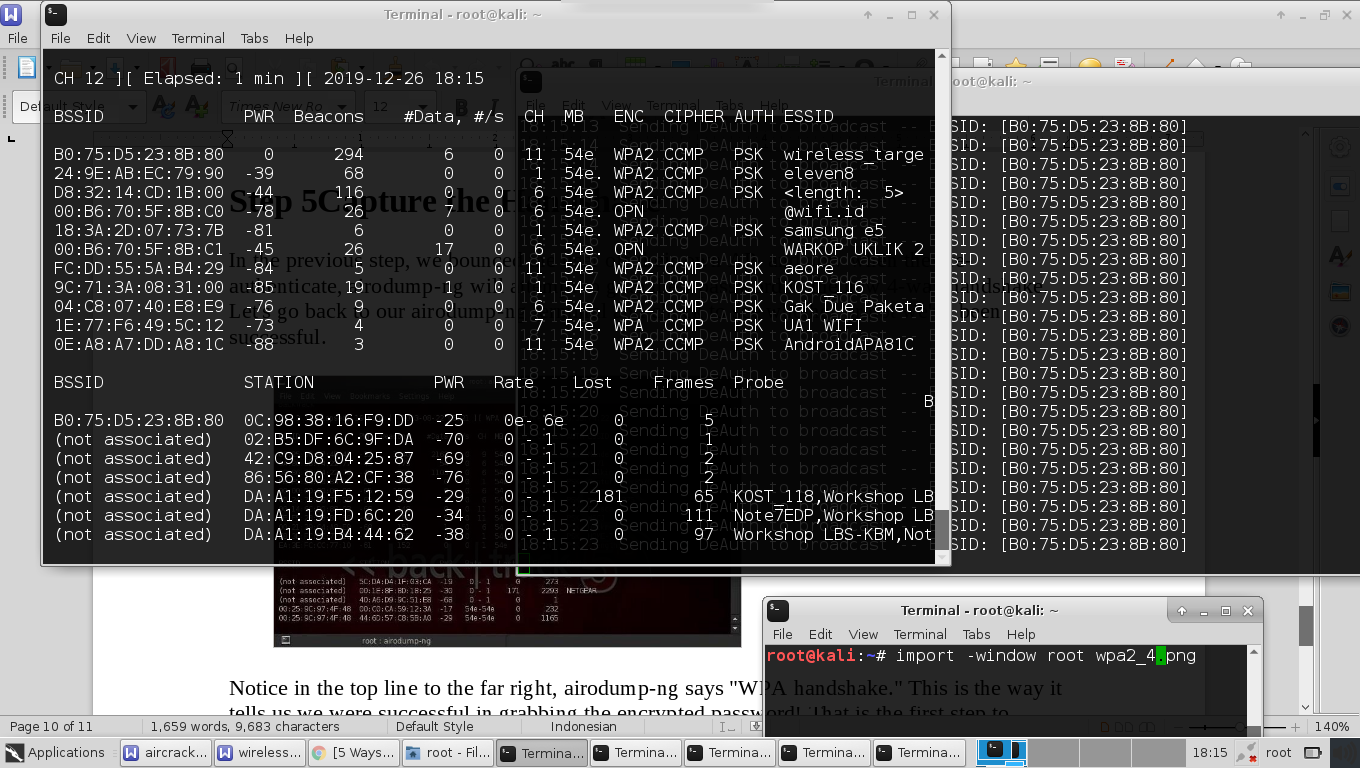




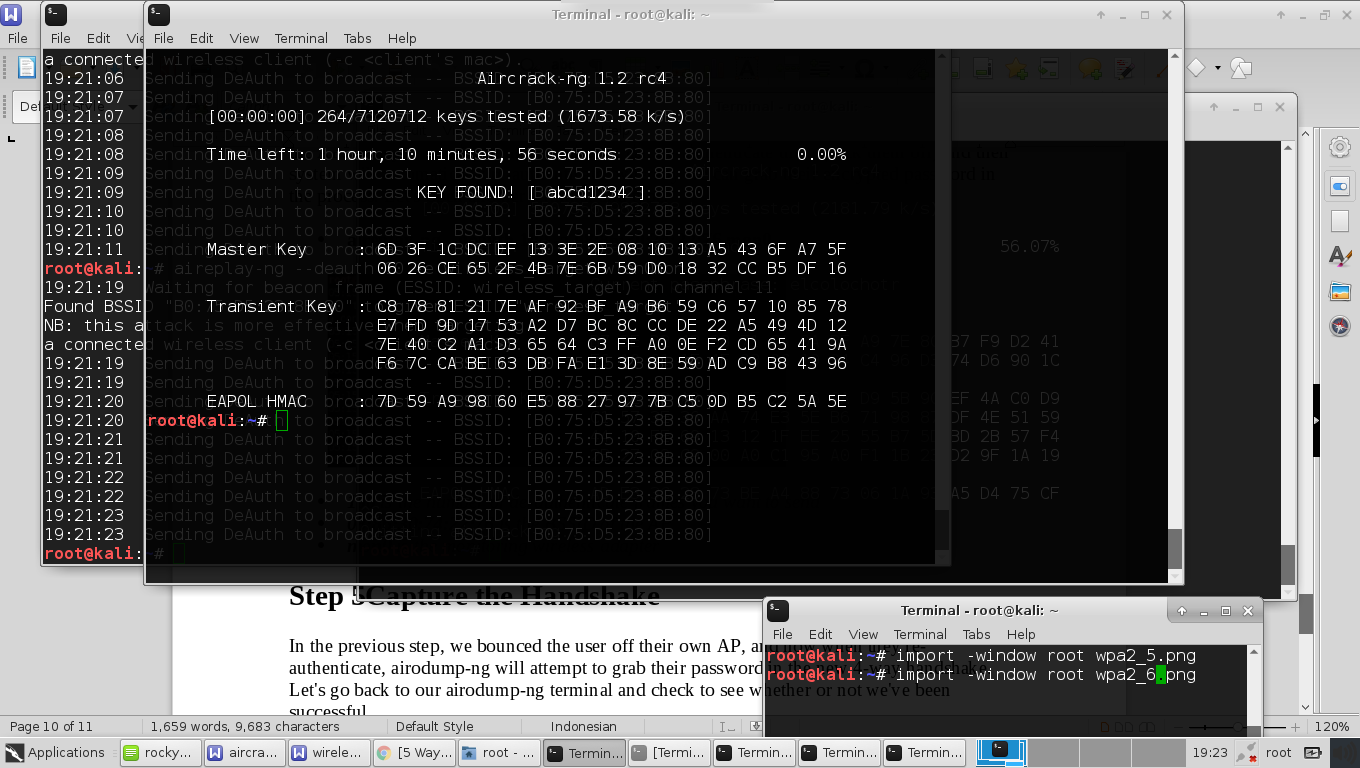
Proses diatas akan melakukan proses capture paket pada ESSID “**wireless\_target**” dan STATION menunjukan mac address yang terkoneksi ke AP (mac address smarphone korban). Kemudian jalankan perintah shell “**aireplay-ng –deauth [banyaknya\_paket\_deauth] –a [mac\_address\_AP] [name\_wireless\_card]**”. Mac address ap dapat dilihat dari proses sebelumnya menggunakan **airodump-ng** dibagian BSSID.



Setelah 50 paket deauth selesai dikirim, client akan terkoneksi kembali dan pada airodump-ng akan menangkap password pada 4-way handshake yang baru.



Pada gambar diatas perhatikan BSSID dan STATION (mac address client) jika sudah muncul maka WPA handshake telah dilakukan dan password terenkripsi berhasil ditangkap. Jalankan “**aircrack-ng [nama\_file\_hasil\_capture] –w [password\_list]**”, jika anda menginstall kali linux wordlist bisa ditemukan di directory /usr/share/wordlist/rockyou.txt.



Jika password pada AP ditemukan pada wordlist aircrack akan menampilkan hasil seperti diatas. Disini kemampuan mengumpulkan informasi (social engineering) dari korban sangat diperluhkan untuk keberhasilan menemukan password AP.