Ce qui suit peut être un long processus, qui n'a besoin que de patience.

TUTORIEL CRACKAGE WIFI BY Ra Fifa (Facebook)

J'ai décidé d'écrire ce petit tutoriel en vue de vous montrer qu'il est facilement possible de CRACKER un réseau WIFI.

Je ne serai en aucun cas responsable de la mauvaise utilisation de ce tutoriel vis-à-vis de vos voisins.

Voici ci-dessus les techniques permettant de cracker un réseau wifi.

Tout d'abord, voici une mise en situation avec la représentation d'un réseau wifi :

Chaque ordinateur échange des données avec le point d'accès wifi, et ces données sont cryptées via une clé (wep, wpa, wpa2-psk, wpa2-tkip, wpa2-aes,wps, sns…)

Ce qui suit peut être un long processus, qui n'a besoin que de patience.

PRESENTATION

C'est un outil facile à utiliser pour les débutants et les experts de piratage en Wifi. Il dispose d'une interface graphique lisse et nécessitent pas de taper des commandes Linux.
La rapidité du crackage dépend de votre carte wifi (ny tena tsara dia capteur wifi manana chipset Realtek RTL8187L,RT73, Atheros,)

Card name	Chipset	Antenna	Windows support	Linux support	Notes
Asus WL-167g v2	Ralink RT73	Internal	No	Yes	
Airlink AWLL3026	Zydas zd1211	Internal	No	Yes	USB info: 0ace:1211 See Notes 1 and 4.
Alfa AWUS036E	RTL8187L	RP-SMA	No	Yes	80mW
Alfa AWUS036H	RTL8187L	RP-SMA	No	Yes	Click here for a test of this adapter
Alfa AWUS036S	Ralink rt73	RP-SMA	No	Yes	Click here for a test of this adapter
Alfa AWUS050NH	Ralink RT2770F	RP-SMA	No	Yes	
Digitus DN-7003GS	RTL8187L	Internal	No	Yes	USB info: 0bda:8187 Realtek Semiconductor Corp. Manufacturer page
D-Link DWL-G122 B1	Ralink RT2570	Internal	No	Yes	
D-Link DWL-G122 C1	Ralink RT73	Internal	No	Yes	
D-Link WUA-1340	Ralink RT73	Internal	No	Yes	
Edimax EW-7318USg	Ralink rt73	RP-SMA	No	Yes	See Note 2
Hawking HWUG1	Ralink rt73	RP-SMA	No	Yes	
Linksys WUSB54G v4	Ralink rt2570	Internal or RP-SMA	No	Yes	
Linksys WUSB54GC v1	Ralink RT73	Internal	No	Yes	See Note 5
Linksys WUSB54GC v2	RTL8187B	Internal	No	Yes	See Note 5
Netgear WG111 v1	PrismGT SoftMAC	Internal	airodump-ng	Untested	See note 3. Needs a recent GIT kernel from the wireless-testing branch.
Netgear WG111 v2	RTL8187L	Internal	No	Yes	See note 3
Netgear WG111 v3	RTL8187B	Internal	No	Yes	See note 3
Netgear WNDA3100 v1	Atheros 9170	Internal	No	Yes	See Note 6
TP-Link TL-WN321G	Ralink RT73	Internal	No	Yes	Manufacturer page
TP-Link TL-WN321G v4	Ralink RT2070	Internal	No	Yes	Supported by rt2800usb
Trendnet TEW-429UB C1	Zydas zd1211b	Internal	No	Yes	USB info: 157e:300d
ZyXEL AG-225H	Zydas zd1211	Internal	No	Limited	See Note 4
ZyXEL G-202	Zydas zd1211b	Internal	No	Limited	See Note 4

Le système contient également un certain nombre d'outils pour pirater des réseaux cryptés :

- ***WiFi Protected Setup (WPS),***
- ***WiFi Protected Access (WPA)***
- ***Wireless Equivalent Privacy (WEP)***

Ce qui suit peut être un long processus, qui n'a besoin que de patience.

Ireto ny karazana logiciel misy @ ilay CD :

Reaver: nouvelle application développée avec la possibilité de WPS de cracker par force brute (WPA / WPA2).

Feeding Bootle: il s'agit de la version GUI de ligne de commande Reaver sous
<< Back | track 5.

Aircrack-ng: la principale épine dorsale de nombreux autres outils de Wifislax y compris FeedingBottle (FB) et minidwep-gtk avec la capacité d'attaquer des réseaux WPA grâce à une attaque par dictionnaire et les réseaux WEP grâce à la collecte et l'injection de paquets ARP.

Minidwep-gtk: est une meilleure interface graphique similaire et qui est encore plus facile à utiliser que Feeding Bottle.

L'avantage supplémentaire de minidwep est que vous pouvez également exécuter Reaver et effectuer des attaques multiples.

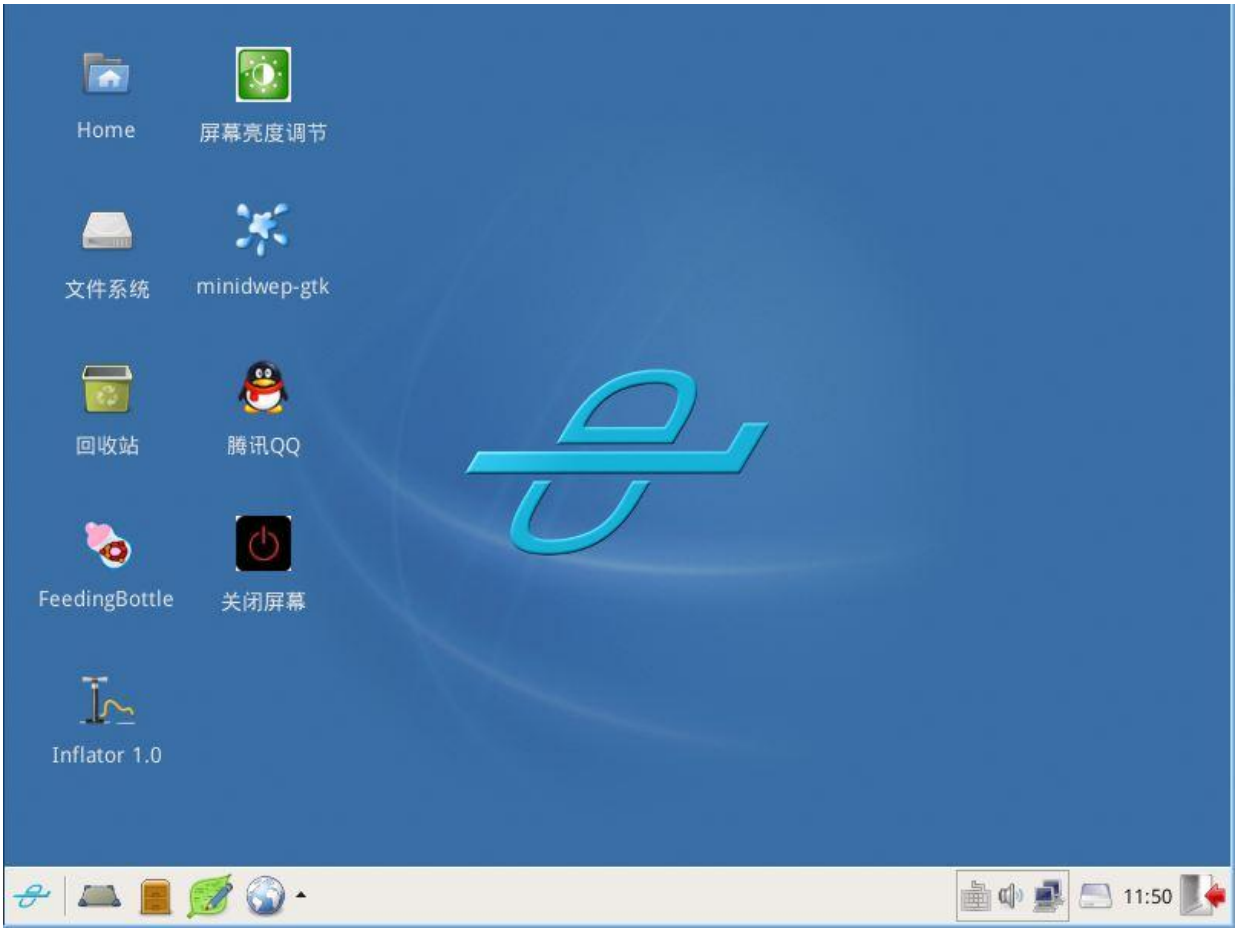
Remarques :

Ny atao hoe « **DICTIONNAIRE** » dia boky feno mot de passe be dia be izay namboarina , raha WIFI no resahana eto.
Ny ilàna azy dia hicomparena ilay mot de passin lé olona alainao ny codiny.
Tadidio anefa fa ao anaty dictionnaire ntéléchargena t@ internet dia tsy hisy «***TENY MALAGASY MIHITSY*** »,**DONC**, c'est inutile d'utiliser le dictionnaire raha ohatra ka teny Gasy no mot de passin le olona.

ETAPES A SUIVRE

1. **Placer le CD dans votre lecteur, puis redémarrer.**
2. **Au démarrage de votre ordinateur, celui doit Booter sur le CD.**
3. **Un choix vous est alors proposé.**
4. **Sélectionner l'interface en appuyant toujours sur la touche « Enter »**
5. **Après chargement vous arrivez sur une interface graphique, et suivre le chemin ci-après pour trouver les outils de craquage wifi :**

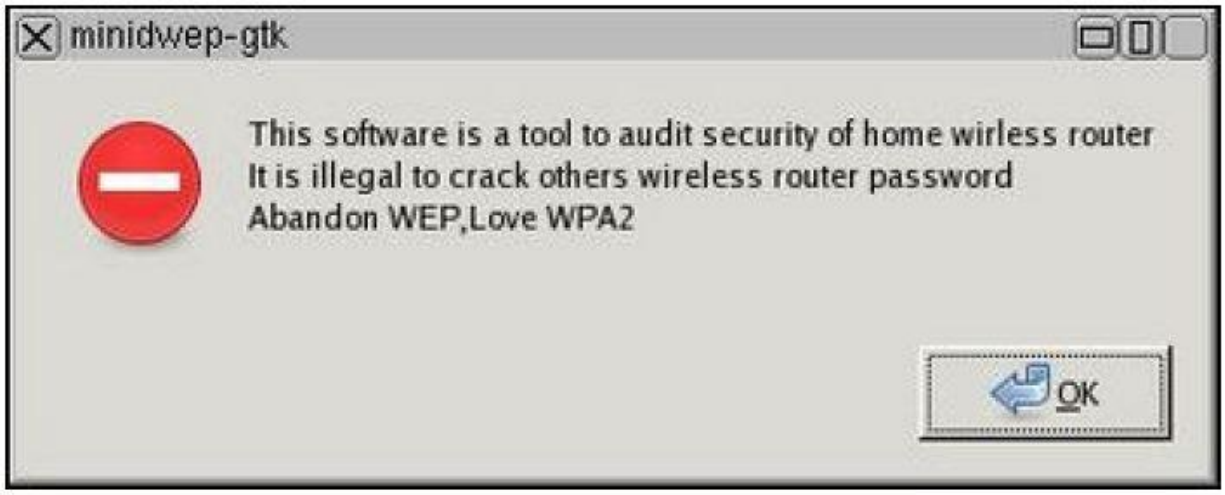
Ce qui suit peut être un long processus, qui n'a besoin que de patience.



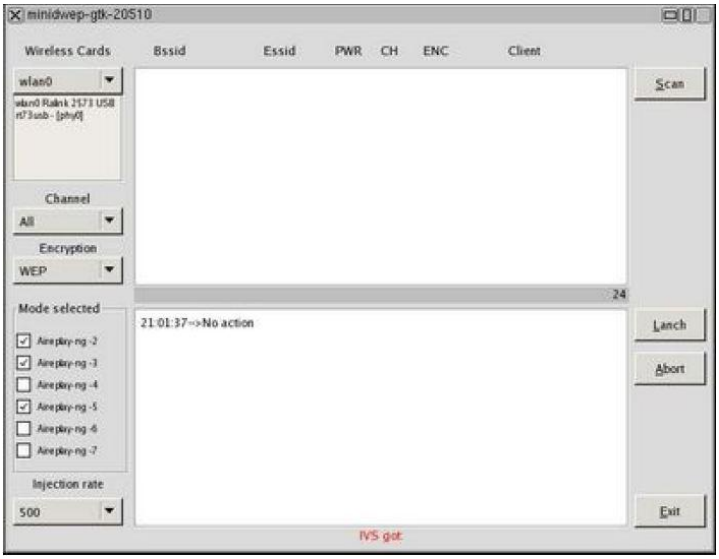
METHODE avec MINIDWEP-GTK (90% de CHANCE)

Cet outil montre les mots de passe sans **Dictionnaires** ne parviennent pas une erreur dans la passerelle, c'est à dire le routeur.
Il est le plus dangereux de cette distribution. Comme vous pouvez le voir, un avertissement mettant en garde l'utilisateur apparait.

Ce qui suit peut être un long processus, qui n'a besoin que de patience.



Après l'apparition de cette fenêtre, clique sur OK



C'est une belle interface graphique, très simple et configuré par défaut de façon EFFICACE.

Voici les actions à faire pour cracker le réseau WIFI

Secret de CRACKAGE WEP

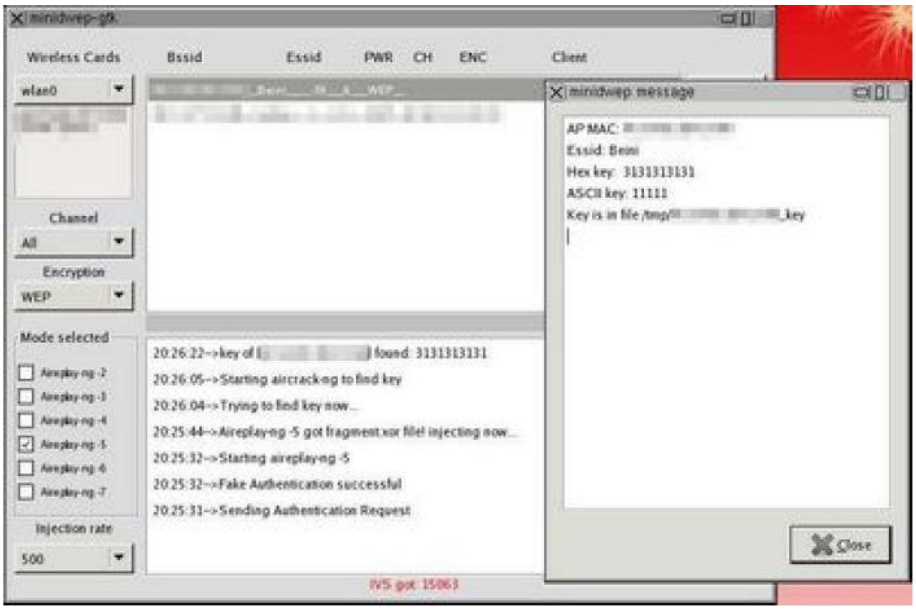
Avec ***minidwep-gtk***, exécutez le logiciel

1. **Choisissez le cryptage WEP**
2. **Cliquez sur le bouton «Scan»**
3. **Sélectionnez un réseau qui apparait dans les routeurs sans fil scannées**
4. **Cliquez sur ' « Lanch »,**

Ensuite tout est automatisé, il lance les injections et si c'est un succès (dans 90% des cas) alors l'opération démarre.

Ce qui suit peut être un long processus, qui n'a besoin que de patience.

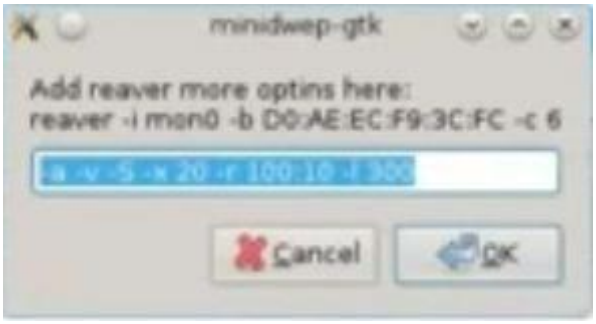
Il récupère les IVS et dès qu'il en a environ 8000 (je crois), il lance en arrière-plan un crack. (On peut voir les différents modules travailler si l'on le souhaite, ils sont cachés en arrière-plan). Si le crack est un échec, il retentera plus tard.
Puis si c'est un succès il le dit et affiche la clé directement.



Secret de CRACKAGE WPA/WPA2

Avec ***minidwep-gtk,*** exécutez

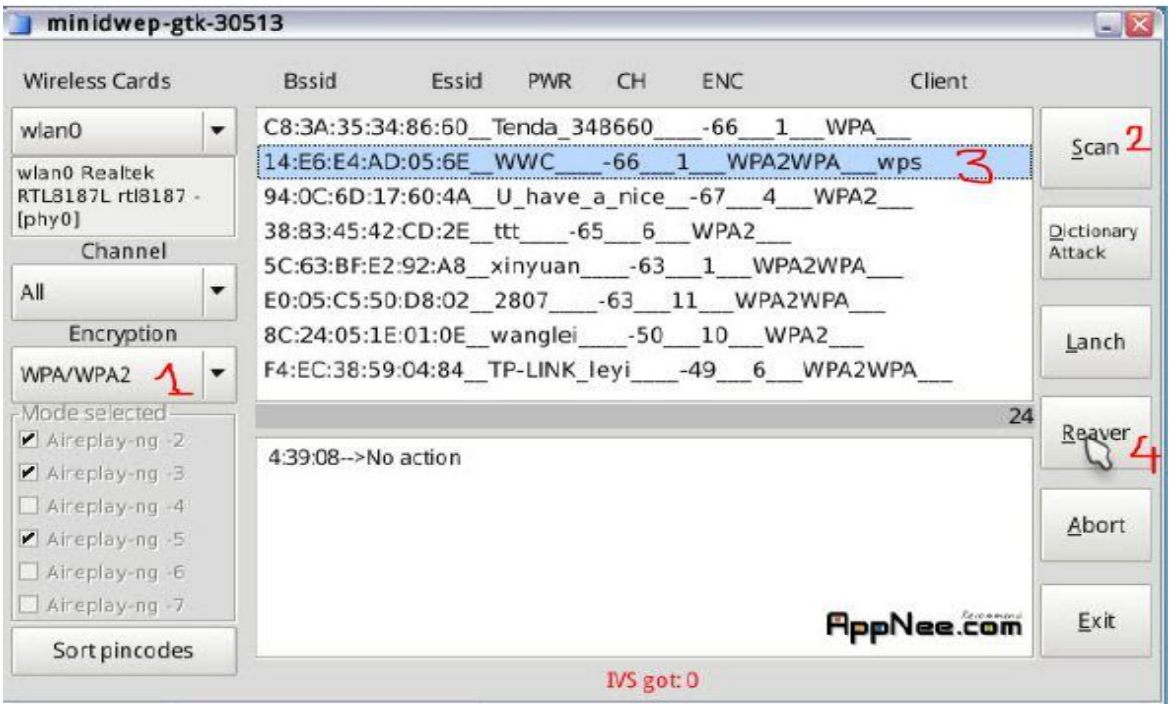
1 choisissez le cryptage **WPA/WPA2** '
2 cliquez sur le bouton «**Scan**»
3 choisissez un client dans les routeurs sans fil scannées
4 cliquez sur '' **Reaver** " (quand une boîte de dialogue, apparaît,



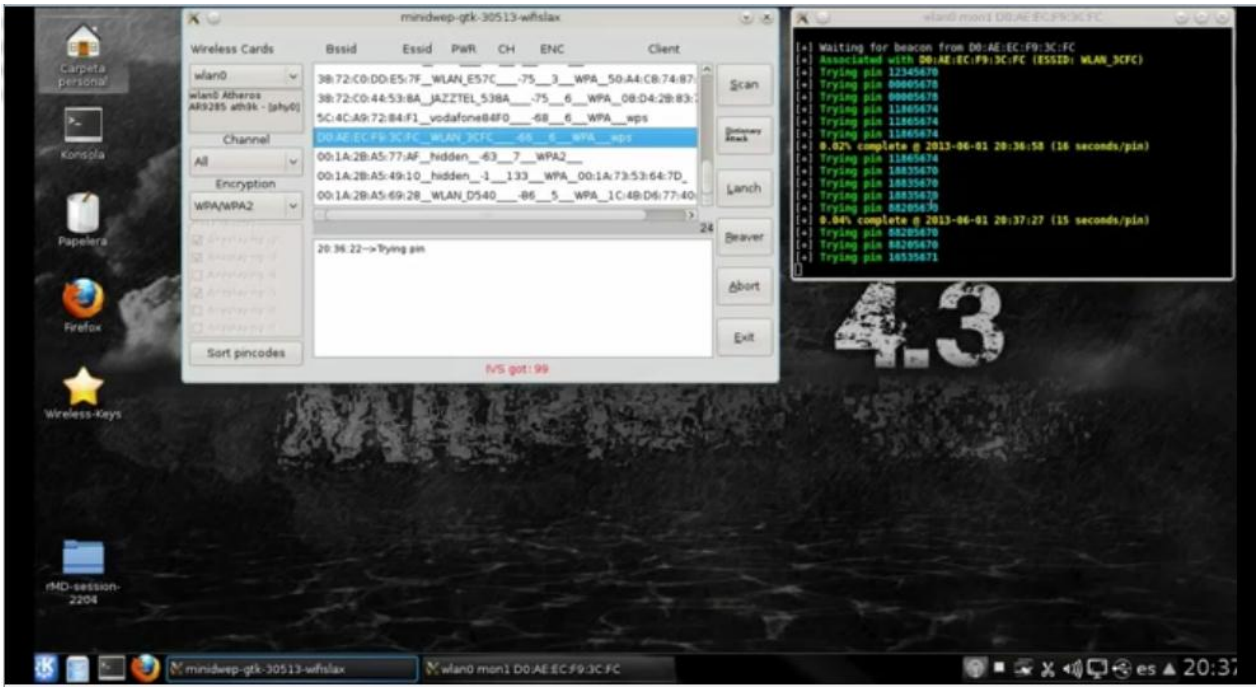
Cliquez sur" **OK** "). Ce qui suit peut être un long processus, qui n'a besoin que de patience.

Ce qui suit peut être un long processus, qui n'a besoin que de patience.

Arao ny filaharan'ny chiffre eo @ sary eto ambany

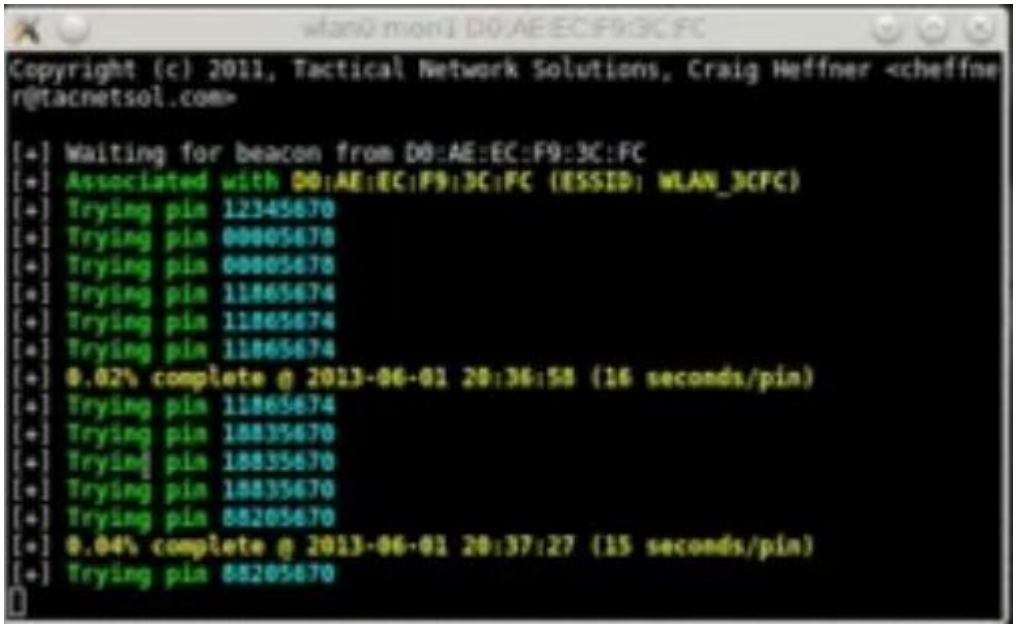


Ce qui suit peut être un long processus, qui n'a besoin que de patience.



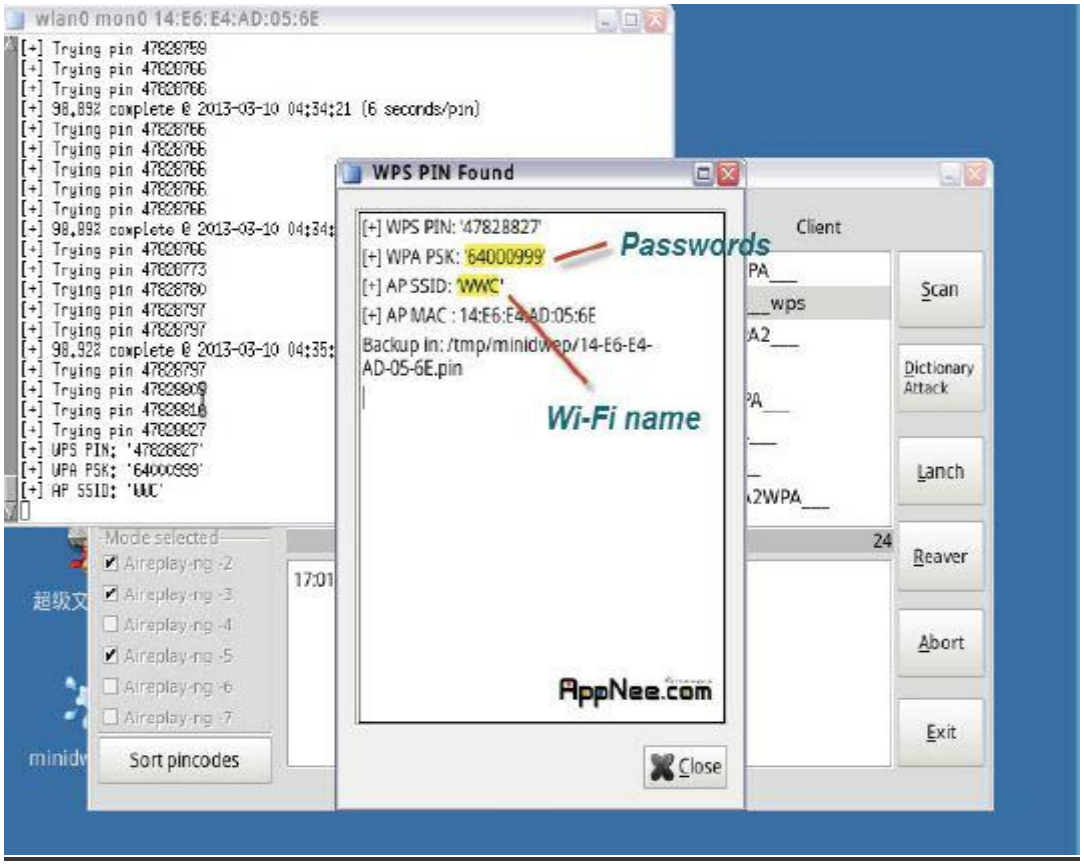
Après avoir cliqué sur le bouton REAVER, une autre fenêtre s'ouvre
(Comme celle de la droite au schéma ci -dessus)

Misy soratra hoe « Trying pin » sy pourcentage an'ilay crackage atao.



Après quelques longue attente, une fenêtre s'ouvrira et à vous de faire le reste.

Ce qui suit peut être un long processus, qui n'a besoin que de patience.



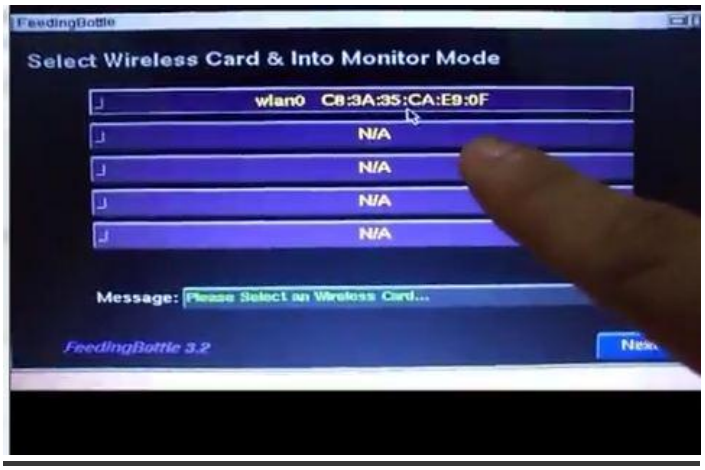
METHODE avec FEEDING BOOTTLE

Crackage clé WEP

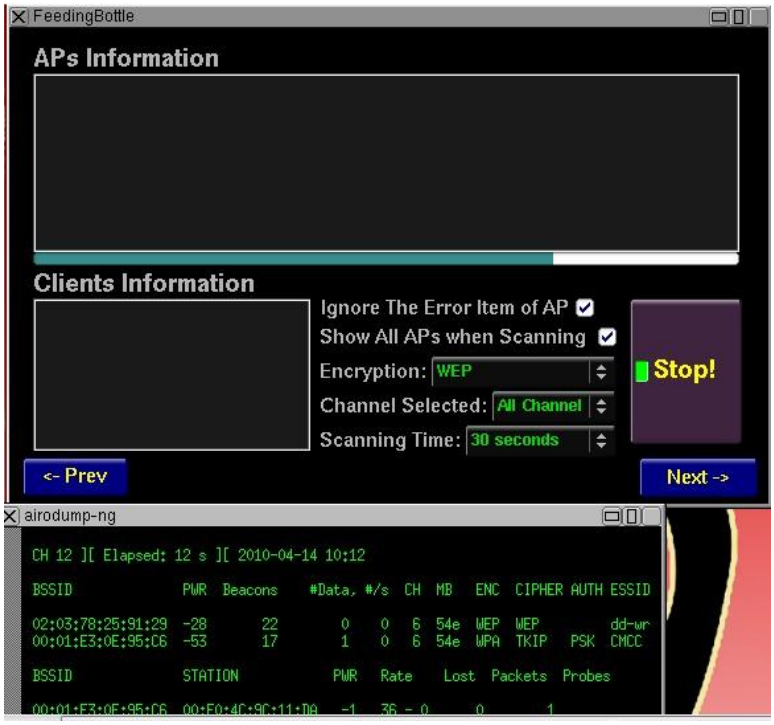
- Cliquez sur feeding bottle (**Bibéron Rose**),

Puis « **YES** », puis cliquez sur votre carte WIFI comme suit :

Ce qui suit peut être un long processus, qui n'a besoin que de patience.

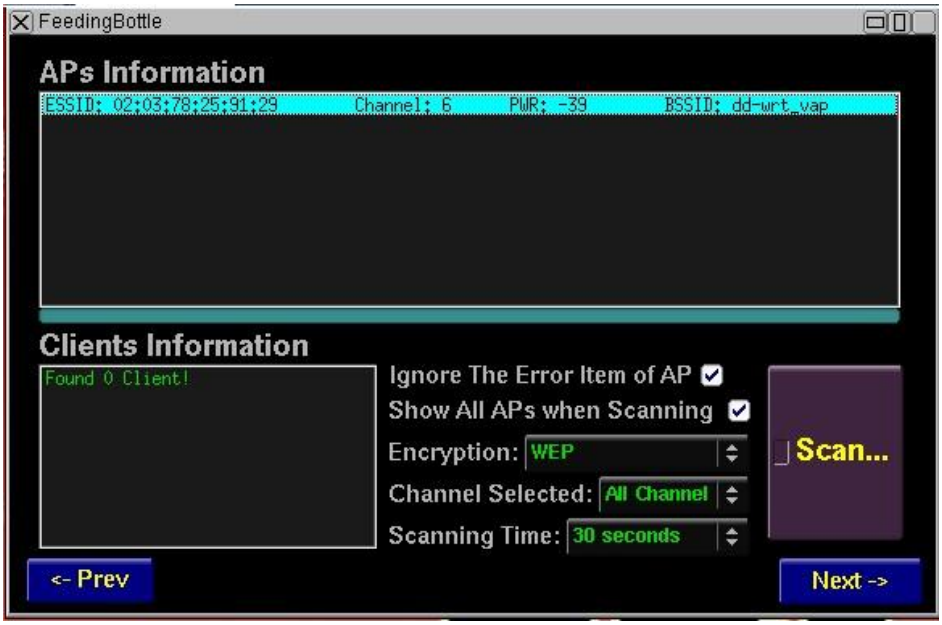


- Puis cliquez sur « **SCAN** ».



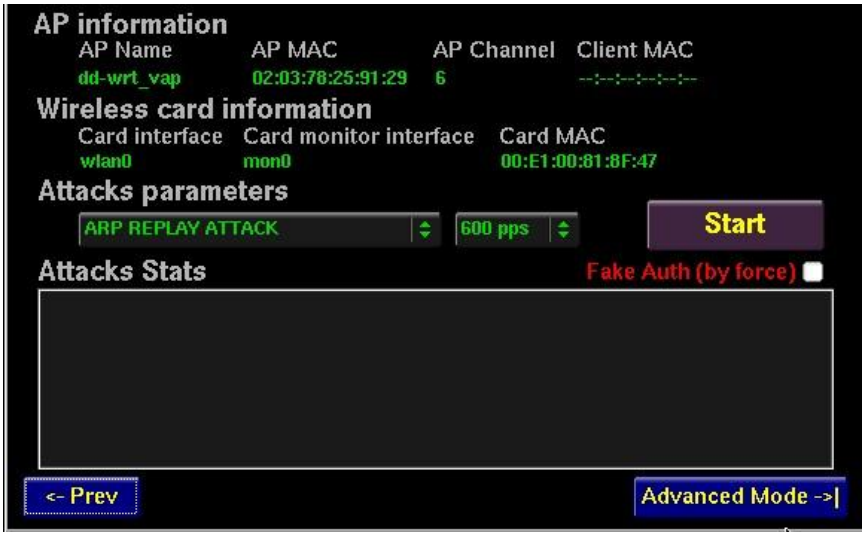
Puis choisissez sur le réseau wifi à cracker, ensuite « **NEXT** »

Ce qui suit peut être un long processus, qui n'a besoin que de patience.



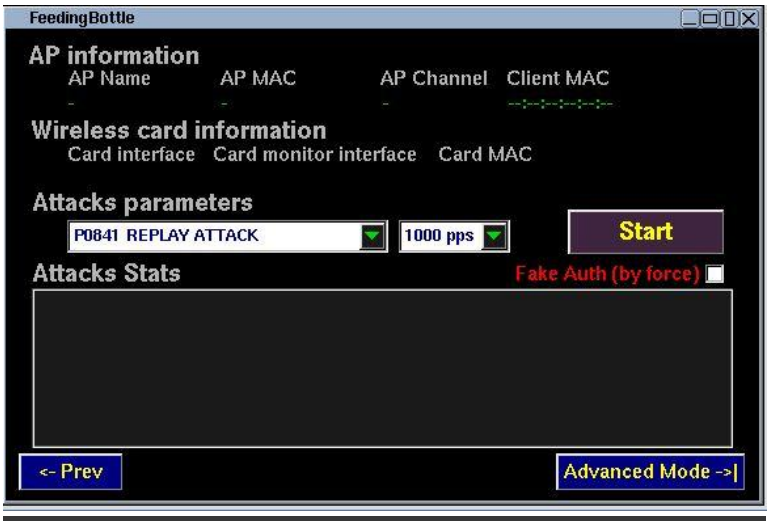
- Choisissez **P0841 REPLAY ATTACK** au lieu **ARP REPLAY ATTACK**

Par Défaut :



Ovaina an'ity fa tsy io no ampiasaina:
P0841 REPLAY ATTACK au lieu **ARP REPLAY ATTACK et 1000 PPS**

Ce qui suit peut être un long processus, qui n'a besoin que de patience.



- Choisissez ensuite « **1000 pps** »
- Cochez sur **Fake Auth (by force)**
- Puis sur le bouton **START**

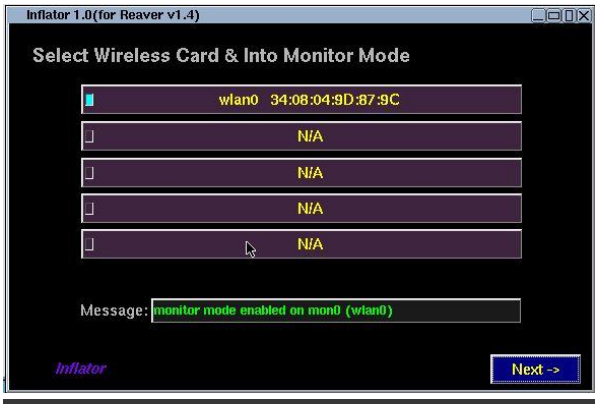
Le nombre d'IVS va augmenter et le **key found** fait apparaît le mot de passe.

(eo @ farany ambany @ sary etsy ambany)

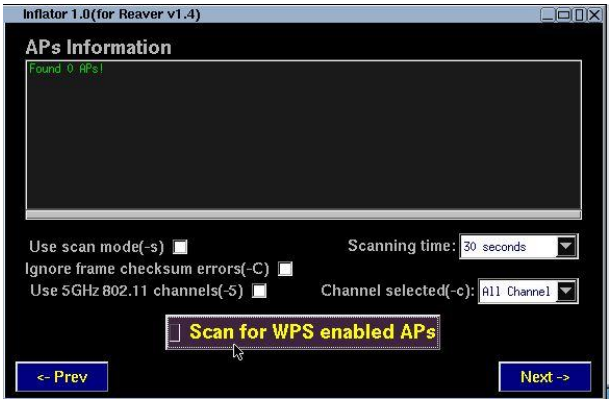
Ce qui suit peut être un long processus, qui n'a besoin que de patience.

METHODE avec INFLATOR (Gonfleur)

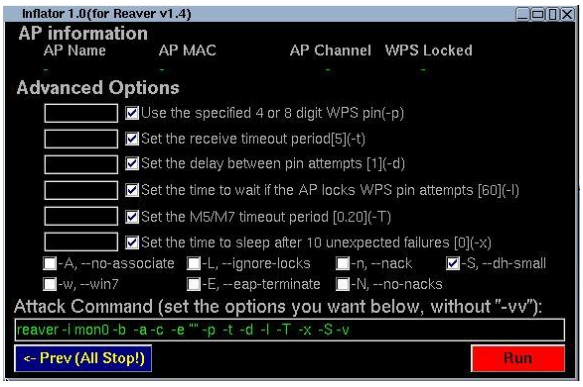
Cliquez sur “**INFLATOR**”, puis sur “**YES**”, ensuite sélectionner votre carte Wifi.



Cliques sur « Scan for WPS enabled APs »



Sélectionner ensuite sur votre VICTIME puis « **NEXT** », et cochez comme indiquez le schéma ci-dessous :



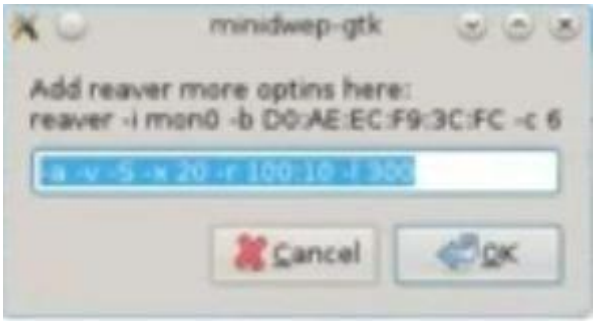
Cliquez sur « **RUN** **»** et veuillez attendre une fenêtre qui s’ouvrira, puis attendre que le mot de passe apparaisse comme suit :

Ce qui suit peut être un long processus, qui n'a besoin que de patience.

NB : Si la victime change le mot de passe après quelques moments, veuillez suivre les étapes ci-après :

Avec ***minidwep-gtk,*** exécutez

1 choisissez le cryptage **WPA/WPA2** '
2 cliquez sur le bouton «**Scan**»
3 choisissez un client dans les routeurs sans fil scannées
4 cliquez sur '' **Reaver** " (quand une boîte de dialogue, apparaît, **AJOUTER LE CODE WPS PIN,** puis Cliquez sur" **OK** ").



Pas besoin d'être patient, la nouvelle code « **WPS PSK** » apparait immédiatement.

Donc, ici se termine le tutoriel sur la façon de se fissurer réseau sans fil facilement en utilisant les outils de crackage.

Bonne chance ...!