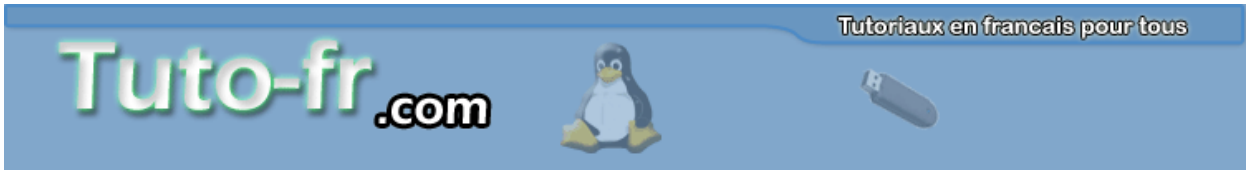


Acceuil
Tuto
A venir
Vidéos
Forum
A propos

Tutorial: Test de votre réseau wifi par crack de clef wep.

Aujourd'hui la plupart des fai qui fournissent un modem offre un modem wifi (livebox, freebox, neufbox, aol-box..)
La plupart (pour ne pas dire toutes) de ces box wifi appliquent le cryptage wep par défaut si on active le sans fil.
Or maintenant il est reconnu que cette protection est dépassée, faible et facilement craquable.
Une petite heure suffit à craqué une clé wep 128 (capture de paquets + crack clé wep).
Je vous propose donc un petit didacticiel pour tester votre réseau wifi, voir en démontrer sa faiblesse sécuritaire.

Attention vous ne pouvez faire ce test que si vous êtes le propriétaire du réseau ou si vous avez un accord de son propriétaire !!!

**Le piratage est un fait grave et ce tutorial n'est en aucun cas destiné à cet utilisation.
Il est simplement la pour vous sensibilisé à la sécurité de votre réseau.
Je le rappelle pour les boulets qui veulent à tout pris hacker leurs voisins. Vous devez avoir une autorisation du proprio pour pénétrer, utiliser son reseau.
Sinon vous encourez de fortes peine de prison et amendes.**

Rappelez vous de quels noms vous traiter le créateur du dernier virus qui se pointe sur votre ordi et appliquez les vous si vous n'avez pas assez de moralité pour suivre des règles simples de civilité.

Sommaire:

Annexes

Fichiers utiles

Tuto: test par crack de la clée wep

Pour tester la sécurité de votre réseau wifi, nous avons besoin de la suite **aircrack** de Christophe

Devine. Cette suite fonctionne sous windows et linux mais certaines fonctionnalités sont impossible sous Windows (injection de paquets par exemple) c'est pourquoi nous utiliserons une suite linux live (bootable) : **Whax**, une distribution spécialisée dans les tests d'intrusion.
Dans cette distribution, tout est déjà pré installé : les drivers des cartes wifi et tous les logiciels nécessaire (aireplay, airodump, aircrack, ethereal, kismet ..).
Par contre, toutes les cartes wifi ne sont pas supportées, en gros cela dépend du chipset, voici une liste non exhaustive des cartes et de leurs possibilités dans l'aide d'aircrack et aussi une Liste des cartes testées sur le forum de iwhax.

Personnellement le tutorial a été réalisée avec une D-link DWL G650 (et pas G650 + !!!), achetée sur ldlc comme d'hab ;) et grâce à un ami voisin possédant une livebox qui m'a autorisé à tester son réseau.
Il m'a autorisé à tester la sécurité de son installation wifi pensant pertinemment que je n'y arriverais pas en fait.
Il s'est avéré qu'il a eu tord :D. Il m'a fallu a peu près 2 heure pour pénétrer son réseaux :D.
Ca ma fais un bon apprentissage.
Pour des raisons d'annonymat tous les noms des réseaux (ESSID) ont été masqué mis à part celui du test qui n'a été masqué que partiellement.
Les adresses mac (BSSID) ont-elles aussi été censurées partiellement, j'ai laissé affiché que la première partie des adresses mac qui correspond aux constructeurs du matériel.

Je le répète, vous ne pouvez tenter de pénétrez un réseau que si celui-ci est le votre ou si vous avez l'accord de son propriétaire !!!

1:// Whax :

Bon on rentre un peu dans le vif du sujet maintenant :
Procurez vous la distribution WHAX ici:

Télécharger Whax:
http://ftp.rz.tu-bs.de/pub/mirror/ftp.whoppix.net/
ou
http://search.belnet.be/mirror/www.whoppix.net/

Gravez la sur une belle galette mettez la de coté 2 secondes. En parallèle, je vous conseil de créer une partition FAT32 de 2 ou 3 giga.
L'avantage du FAT32 c'est qu'il est lisible par windows et linux.
Cette partition va en fait servir à stocker les paquets capturés et les différents fichiers nécessaires pour le crack de la clé wep.
Cette partition n'est pas indispensable mais recommandée surtout si vous ne disposez que de peu de RAM (128 ou moins) car la distrib Whax est un live cd donc les fichiers de capture sont stockés dans la ram.
Le fait d'avoir une partition fat32 vous permet aussi d'arrêter le pc et de redémarrer sans perdre tous les paquets déjà capturés !!!

Par contre votre partition ne portera pas le même nom sous linux que sous Windows, mettez donc un fichier particulier dedans pour pouvoir la reconnaître.

Apres avoir booté sur whax vous tombez sur un écran de login.
Le **login est root**, le **mot de passe est toor** et pour lancer le **mode graphique tapez startx** (il faut taper **stqrtx** car le clavier est anglais :s)

> Vous tombez ensuite sur cet écran :
> Ecran d'acceuil de whax

La première chose à faire est de passer en **clavier français** c'est plus agréable :).
Pour ce faire : clic droit sur l'icône du drapeau américain en bas à droite puis sélectionnez français.
Ensuite ouvrez une console (**l'interface est KDE donc pour ouvrir c'est simple clic partout**) :

Puis tapez **"airmon.sh"** pour détecter les interfaces wifi puis sélectionnez celle que vous voulez démarrer par la commande **"airmon.sh start « l'interface wifi » "**

Ici on voit que la carte est correctement reconnue et que le **mode monitor** est directement activé. Le mode monitor permet de capter tous les paquets qui transitent même ceux qui ne vous sont pas adressés.

Et si vous utilisez deja une distribution linux et souhaitez simplement installer la suite **aircrack**:

Télécharger aircrack airodump, aireplay ici

2:// Airodump :

Maintenant nous allons commencer à scanner les réseaux wifi avec **airodump** :

On tape dans la console : "**airodump « notre interface » « le nom du fichier de sortie » « le canal a scanner »** "

Pour choisir de scanner tous les canaux mettez **0**

Vous pouvez rajouter le **paramètre 1** après pour enregistrer dans le fichier de sortie (ici out) que ce qui va nous servir à cracker la clef wep :
« airodump ath0 out 0 1 »
Le fait de rajouter ce parametre crée un fichier de sortie dont l'extention est differente: .ivs à la place de .cap mais le principal avantage est que ce fichier ne contient pas toutes les information de paquets mais uniquement les IVs, sa taille est donc bcp plus petite.

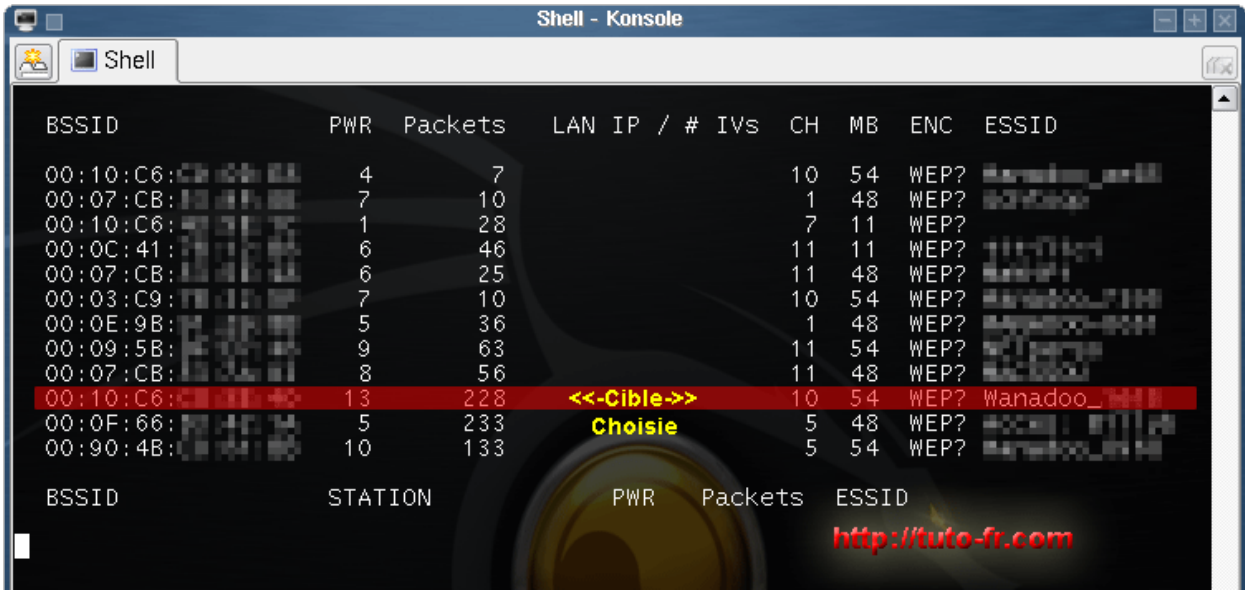
.Vous devez choisir cette méthode si vous n'avez pas crée de partition Fat32 sinon vous risquez un plantage !!!
Preferez cependant enregistrer en .cap si vous avez une patition Fat32

Si vous avez choisis de faire une partition FAT32, vous devez vous placez dans cette partition avec la console :

Fait **« cd .. »** pour remonter à la racine. Puis **"cd mnt"** pour aller dans le dossier qui correspond au poste de travail sous windows. Puis faites "**cd « la partition fat32 »** "

Pour ma part je tape donc **« cd .. » puis « cd mnt/hda6 »**

On obtient ceci ensuite une fois airodump lancé:



Je suis en résidence étudiante donc y a pas mal de monde :D.

La colonne BSSID correspond à l'adresse mac des points d'accès (AP)
La colonne ESSID correspond au nom du réseau (monRezoWifi, Wanadoo-XXXX, WiFI-freebox.)

La première partie correspond aux points d'accès et la seconde partie aux stations (en gros les ordinateurs qui se connectent aux AP).
Ici il n'y a pas encor de stations.

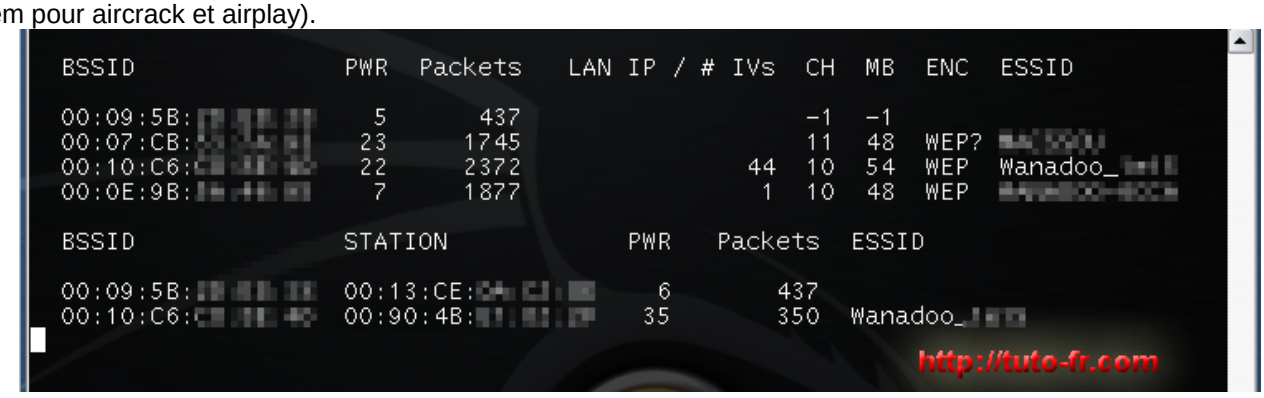
La colonne qui nous intéresse est la colonne des **IVs**, c'est ces fichiers qui vont nous permettre de **cracker les clefs wep**.

Ici l'AP de mon voisin est le seul dont le Essid n'est pas totalement masqué. Pour plus de performance dans la capture des paquets, on relance airodump en choisissant seulement le canal ou il se trouve : le 10

« airodump ath0 out 10 »

Pour arrêter la capture et pouvoir entrer des commandes faites Ctrl+C.
Vous êtes également obligés de stopper la capture si vous souhaiter copier une adresse mac car l'ecran se rafraichi.
Pour copier quelque-chose selectionnez simplement avec la souris et fait clic droit copy. Idem pour coller ou utilisez shift+inser.

Pour plus de détails sur airodump tapez uniquement « airodump » dans la console et l'aide apparaîtra (idem pour aircrack et airplay).



Là, on a des stations dont une qui est connecté à l'AP qui nous intéresse.
Bingo car les acces-point ont parfois (et c'est le cas des livebox) un **filtrage des adresses mac**, appelé **mode association**. Et pour aireplay on a besoin de cette adresse mac, en fait on se fais passer pour l'ordinateur qui à le droit d'accès à l'AP.

Dès que l'on commence à choper des **IVs airodump** nous dit quel est le **cryptage : WEP WPA ou OPN.**

Maintenant que l'on sait que le cryptage est WEP, qu'une station est présente et qu'il y a du trafic (350

paquets pour la station en peu de temps), on va lancer **aireplay**, un injecteur de paquets pour accélérer le trafic et surtout stimuler l'envoi le **IVs**

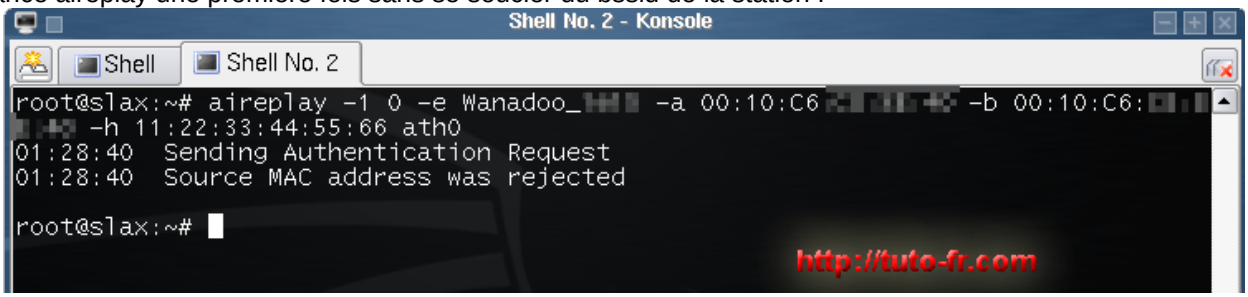
Il faut savoir que pour **cracker la clef wep d'un réseau wifi**, il est préférable qu'il y ai un minimum de trafic. Par expérience la capture de IVs est beaucoup plus rapide, et de plus ils doivent être plus diversifié car le crackage de la clef wep nécessite moins de IVs. Par exemple ici il y a du trafic mais malheureusement après il n'y en avait plus donc j'ai du capturer bcp de IVs avant de pouvoir trouver la clef.

3:// Aireplay :

3.1:// Fake authentication

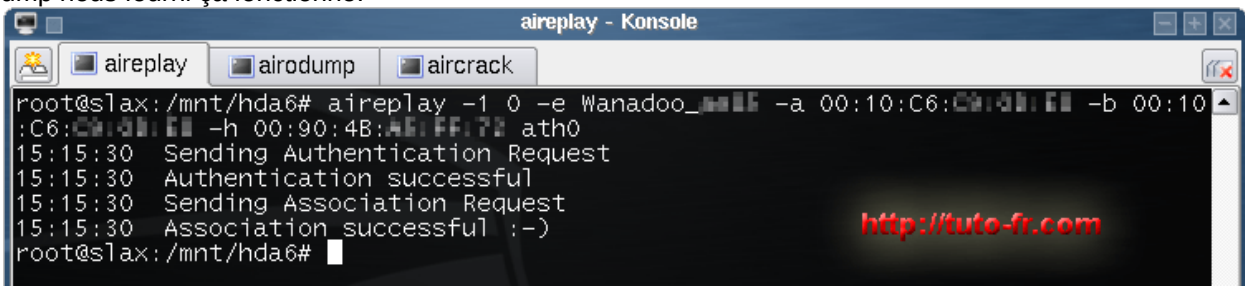
Pour lancer aireplay ouvrez une autre console dans la même fenêtre à l'aide du petit icône en haut à gauche. Vous pouvez également la renommer grâce à un clic droit.

On lance aireplay une première fois sans se soucier du bssid de la station :



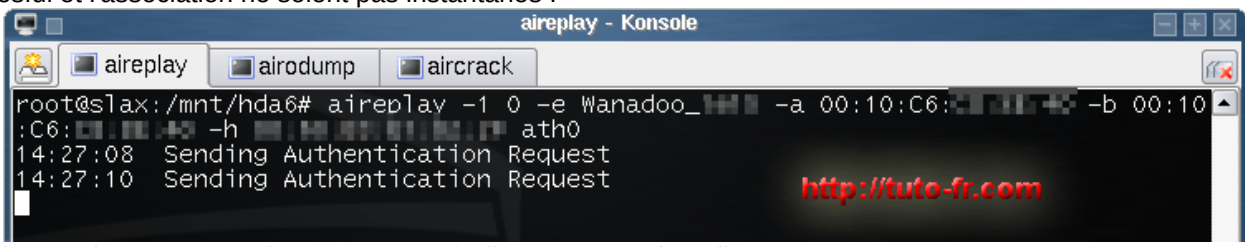
Les paramètres sont :
"**aireplay -1 0 -e « Essid » -a « Bssid de l'AP » -b « Bssid de l'AP » -h « Bssid de la station » « interface »** "

« -1 0 » correspond à une attaque par "**fake authentification**" le zéro indiquant le délais de réponse accepté.
Ici on voit que si l'on met une adresse mac au pif, l'AP nous refoule alors que si on met le bssid que airodump nous fourni ça fonctionne:



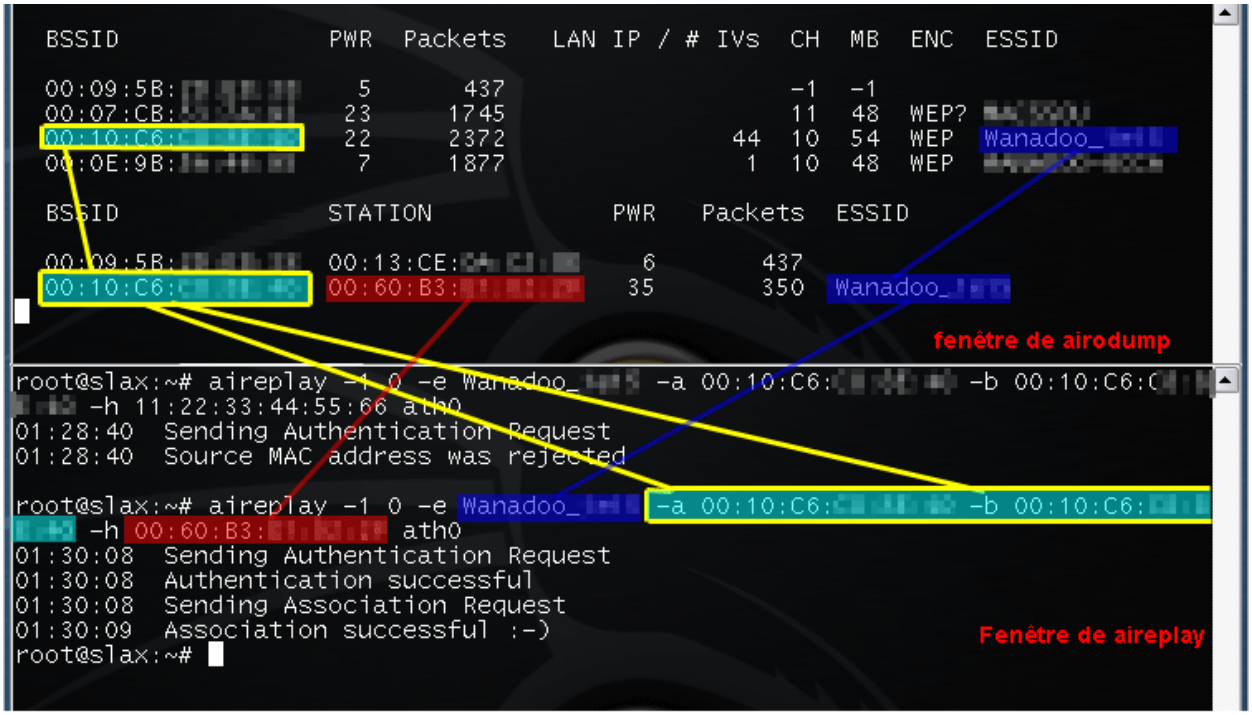
Certain AP n'ont pas de filtrage d'adresse mac et vous pouvez en mettre une au hasard.
Une fois que l'on a « **association succesfu**l », c'est déjà une première victoire. En gros on est accepté par le point d'accès wifi.

Il se peut que si vous ne captez pas très bien le signal (si le power est bas) que l'authentification succesful et l'association ne soient pas instantanés :



Et la l'exemple est court mais vous pouvez facilement en avoir 40 lignes :-S

Voici un petit schéma qui vous montre les relations entre les paramètres de aireplay et la capture de airodump :



Lien entre les parametres de aireplay et la reception de airodump

3.2:// Injection de paquets :

Une fois que l'association est bonne, on **relance aireplay** en changeant et rajoutant quelques paramètres.

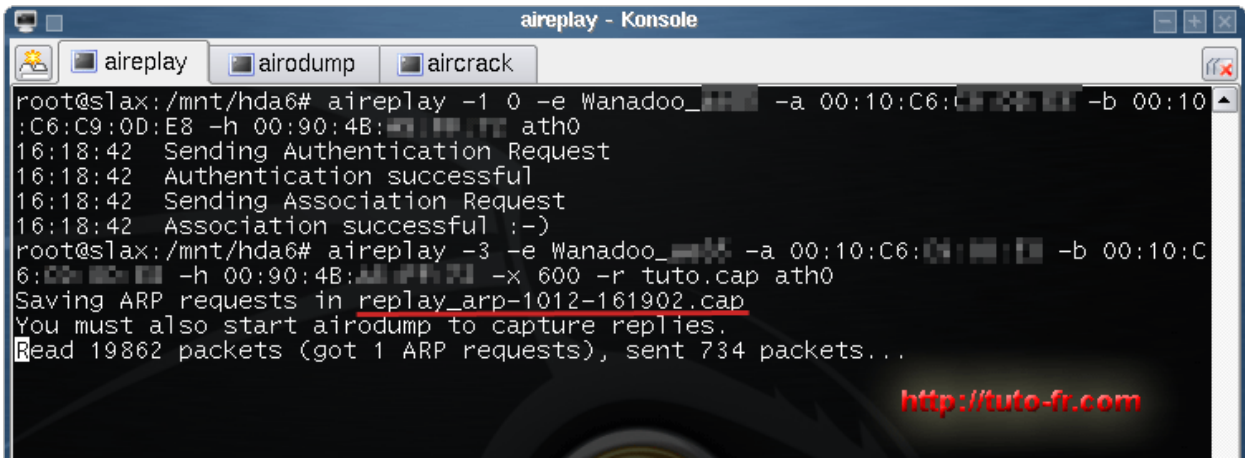
Il faut changer le premier paramètre et le remplacer par **"-3"** qui correspond à une **attaque par injection de paquets**.

Il faut rajouter le paramètre **"-x"** suivis d'une valeur qui correspond au nombre de paquets par second que aireplay va injecter. Ici **600**. Mettez plus ou moins suivant si la puissance du signal de l'AP est forte ou faible.

Ajoutez également le paramètre **-r** suivi du nom de fichier de capture (celui de airodump). Ce paramètre indique dans quel fichier lire pour voir si il y a des ARP a l'intérieur. Ce sont ces arp justement qui vont nous permettre d'influencer le trafic.

N'oubliez pas de vous placez dans le même répertoire.

Pour vous évitez de tout taper, vu que la syntaxe est quasiment identique qu'avec le paramètre -1 appuyé sur la flèche haute pour retrouvez ce que vous aviez entré précédemment.



Pour airodump, les IVs sont importants mais notez que pour aireplay, les ARP le sont tout autant, c'est eux qui vont vous permettre d'augmenter la production de IVs.

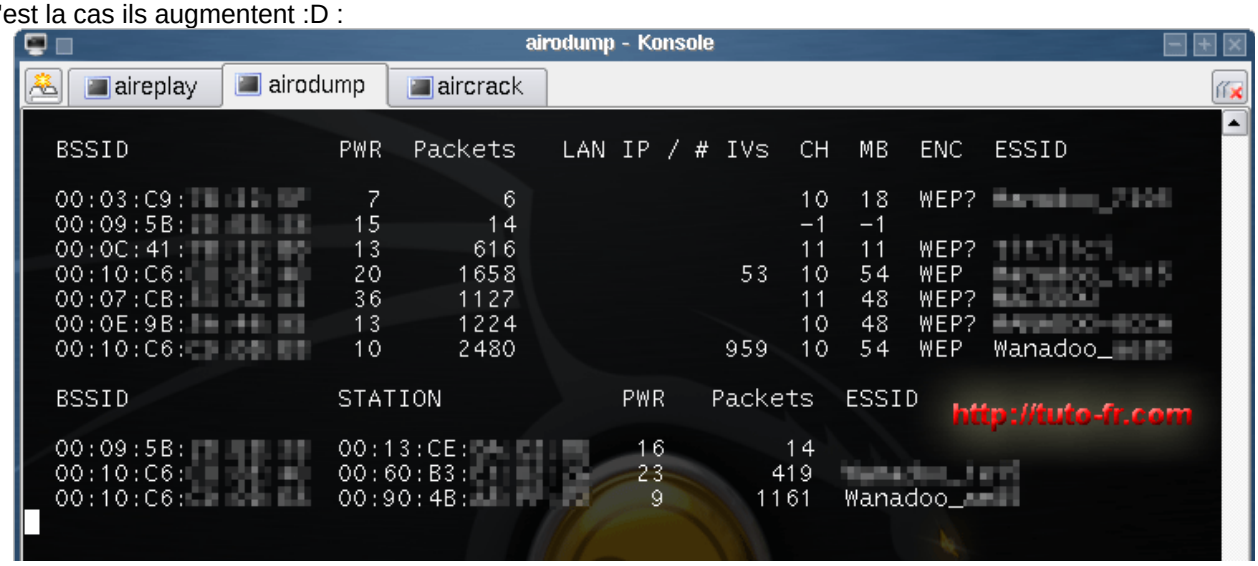
Aireplay vous sauvegarde donc les arp dans un fichier qu'il créé à chaque fois qu'il est lancé.
Il est souligné sur la photo.

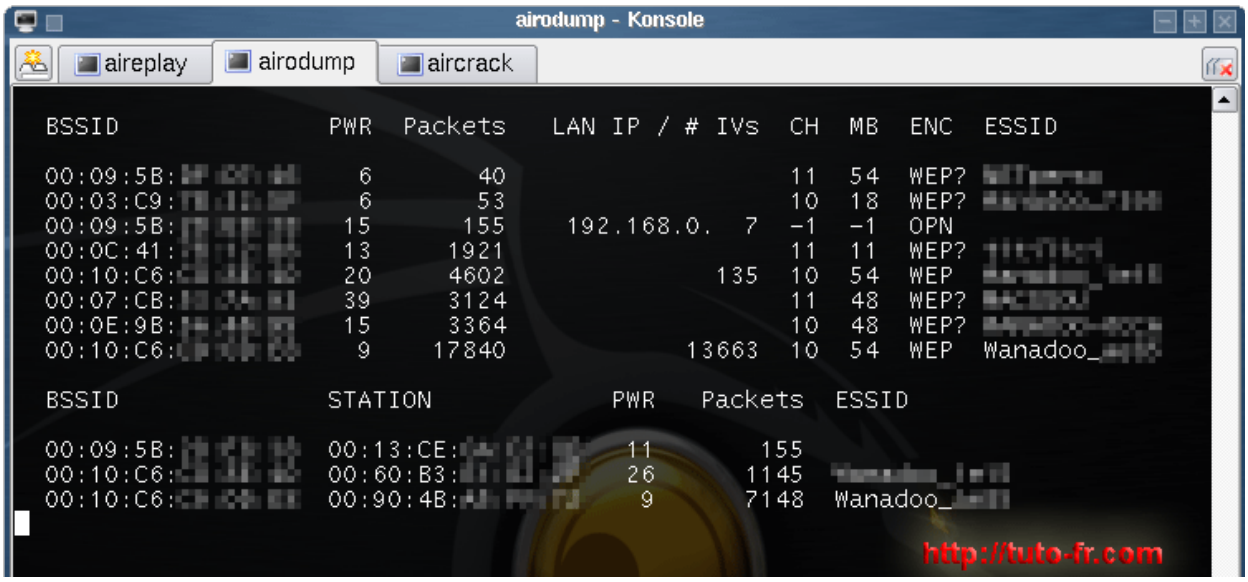
Ce fichier se trouve dans le répertoire duquel vous avez lancé airplay.
C'est ce fichier que vous mettrez ensuite après le paramètre -r si vous avez chopé des ARP.

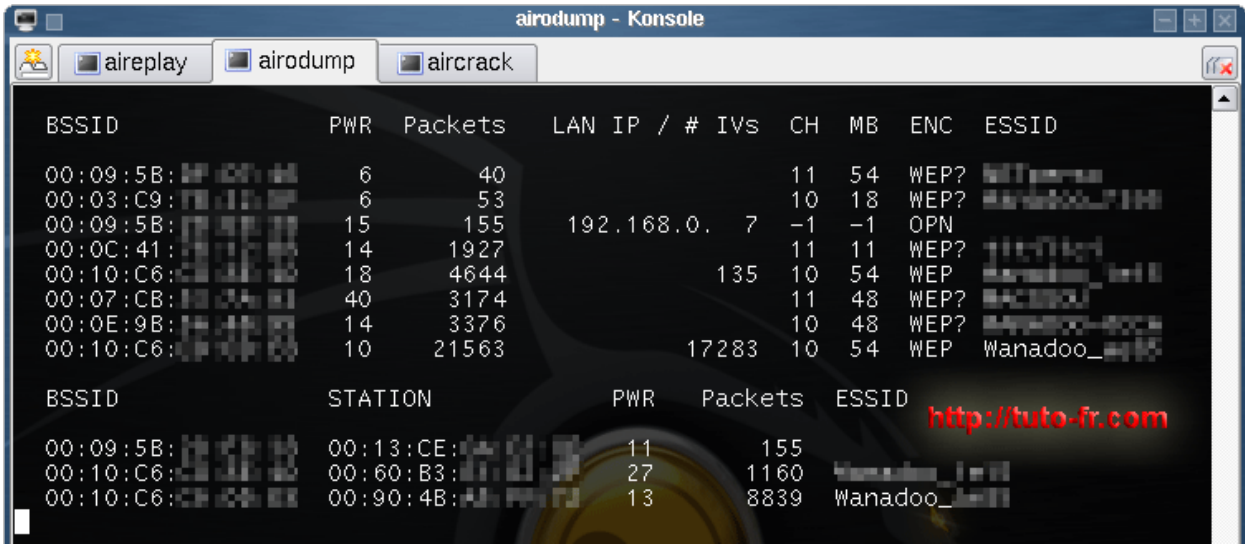
Les arp sont obtenu en lisant le fichier indiqué mais aussi en sniffant le réseaux comme le fait airodump.

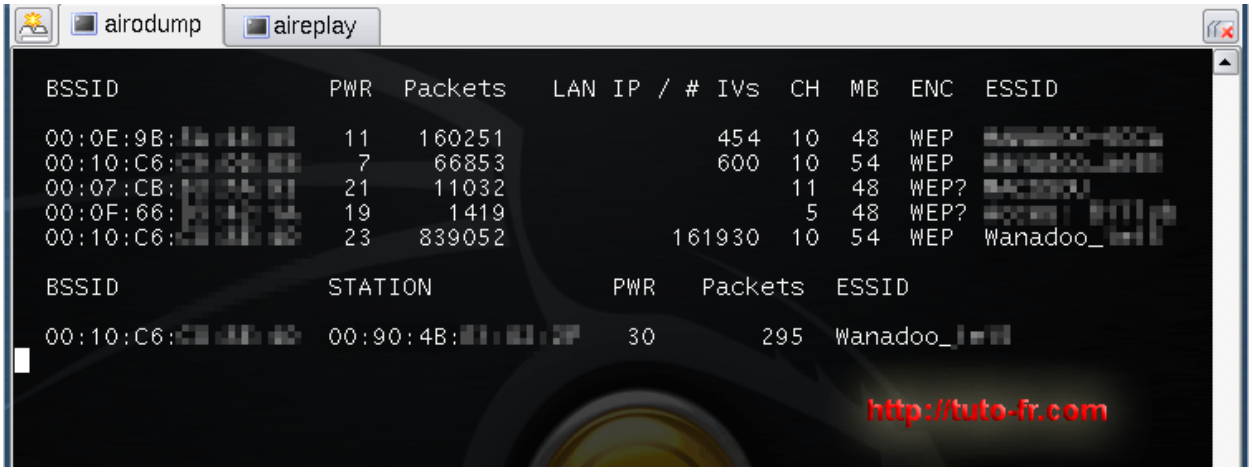
Ici, on voit que l'on a un arp. Des que l'on a un arp aireplay commence à envoyer des paquets.
Et normalement si tous se passe bien, les IVs augmentent.

Et c'est la cas ils augmentent :D :

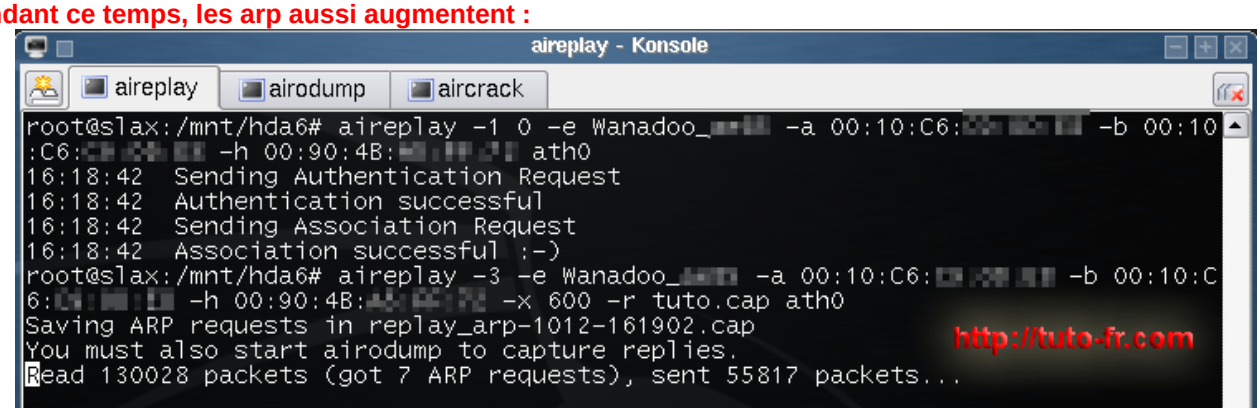


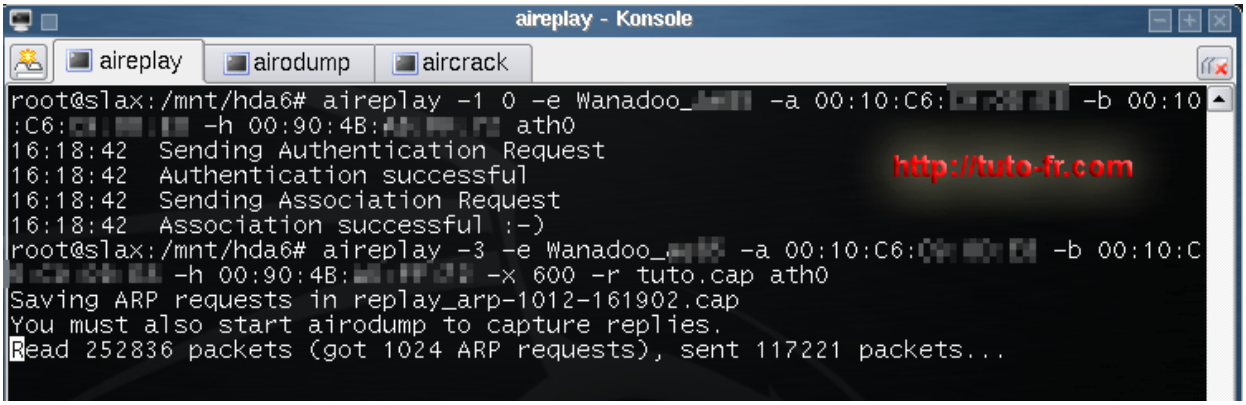






Pendant ce temps, les arp aussi augmentent :





Au maximum aireplay garde 1024 ARP.

Pour vous donner une idée de la vitesse de croissance des IVs j'ai fais quelques print full screen, mattez l'horloge :

A 16h25 190 000 IVs
A 16h30 290 000 IVs
A 16h43 650 000 IVs

4:// Aircrack :

Sachant qu'il faut environ **300 000 IVs pour cracker une clef wep 64bits**
Et environ **1 000 000 pour une clef wep 128** ça va assez vite :D.

Il est donc conseillé de lancer une première fois aircrack des que l'on a 300k paquets si on suppose que la clef peut être de 64 bits.

Pour cela dans les paramètre de aircrack, il suffit de rajouter **-n 64**, et aircrack va tenter de cracker la clef wep comme si c'était une clef 64 même si il s'avère que c'est une 128.

Personnellement pour le tuto, la cible étant une livebox, je sais que le cryptage est 128 donc je ne lance donc pas cette étape préliminaire. Par contre vu que j'ai environ 700 000 IVS je peut commencer à lancer

aircrack en parallèle à la capture de paquets avec airodump.

Ouvrez un nouveau shell et lancer **aircrack.**
N'oubliez pas de vous placez dans le dossier contenant les fichiers de airodump si vous avez créé une partition FAT32.
Pour lancer aircrack, on tape :

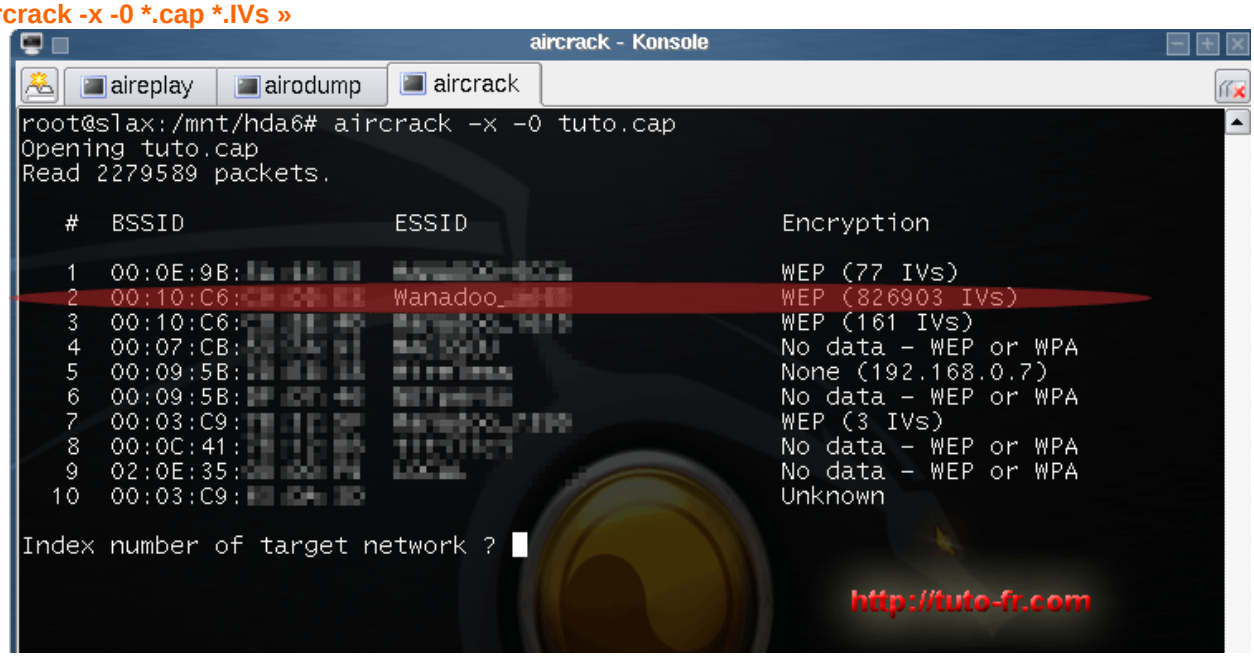
« aircrack -x -0 nomduFichierDeCapture »

Le paramètre **-x** permet de ne pas brute forcer les 2 derniers bits. (ça accélère le crack en principe)
Le paramètre **-0** met aircrack en couleur et c'est la sa seul vocation :D

Ensuite le dernier paramètre est le nom du fichier de capture de airodump.
Vous pouvez également utiliser la syntaxe **« *.cap » et « *.ivs »** pour ouvrir tout les fichiers .cap et .ivs.

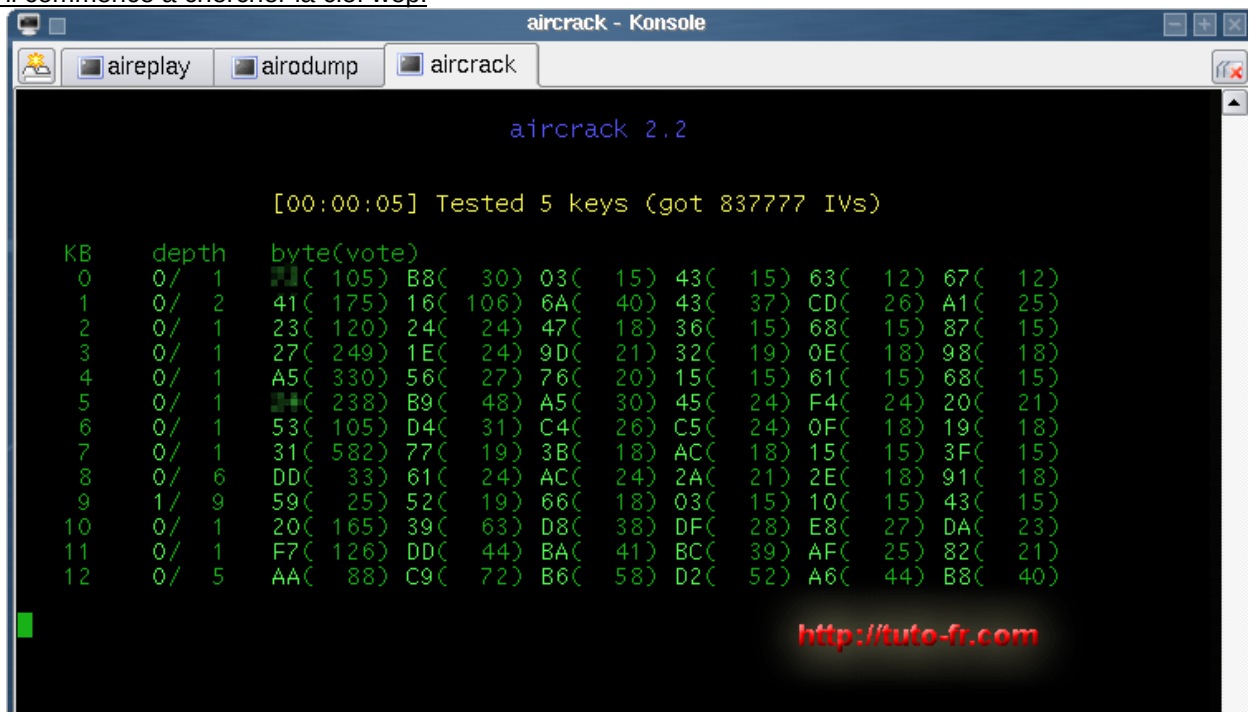
Ce qui donnerai :

« aircrack -x -0 *.cap *.IVs »



Une fois lancé aircrack nous affiche **tous les réseaux** qu'il a rencontré, **leur cryptage** et le **nombre de IVs correspondant**. Il vous suffit d'entrer le numéro du réseau : ici **2** et de lancer aircrack.

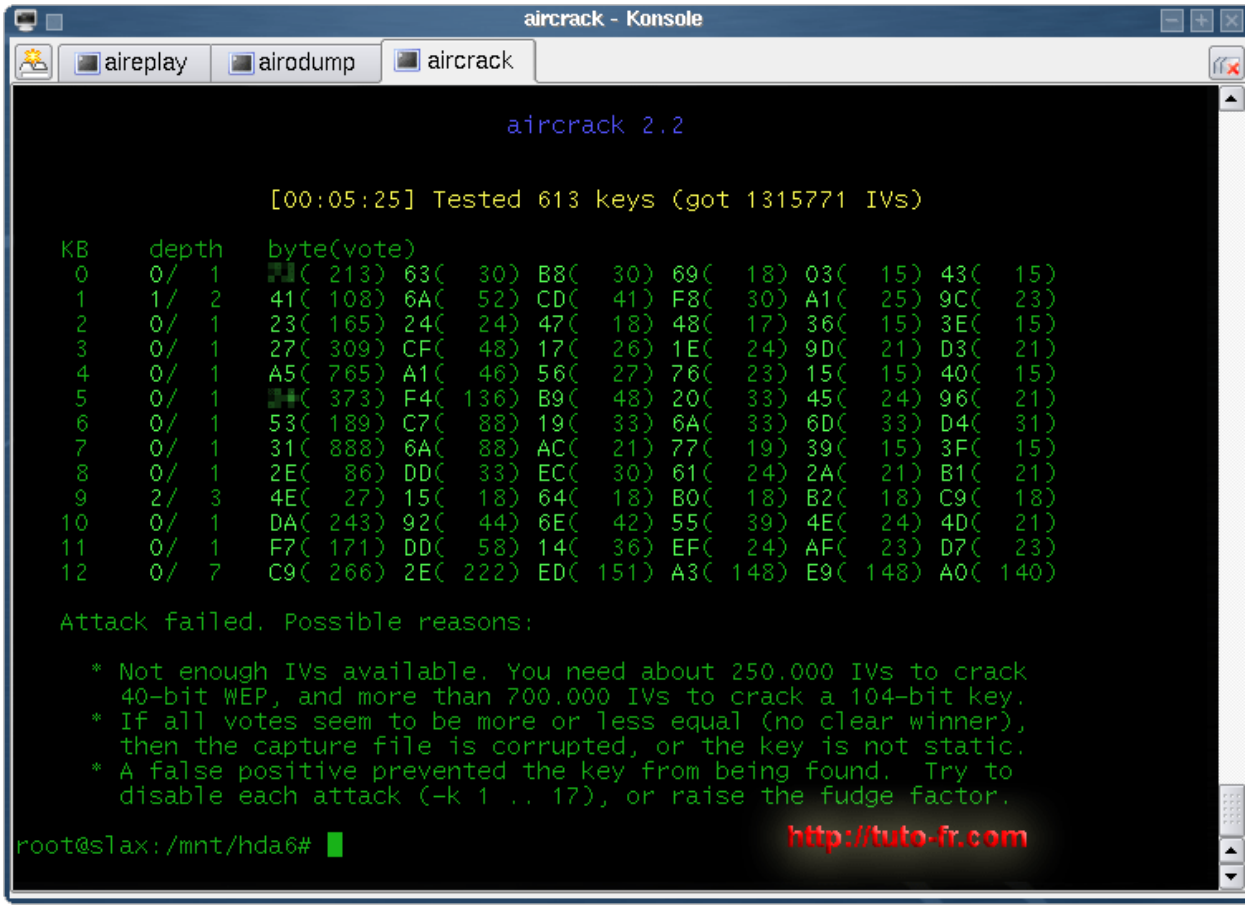
Et là il commence à chercher la clef wep:



Pendant ce temps la capture avec airodump se poursuit et aircrack incrémente automatiquement les IVs et s'en sert pour cracker la clef wep.

La, il vous suffit de laisser tourner et la clef wep devrait apparaître en rouge d'elle même si le crack fonctionne.
En gros ça fonctionne statistiquement par rapport aux IVs et par un systeme de vote, plus un bit a de vote par rapport au autres bit du meme rang, plus il a de chances d'etre le bon.

Malheureusement pour moi, le crack a échoué pourtant, le nombre de IVs était monté à 1 300 000 !!!
Alors que d'habitude 1 000k suffisent.
J'explique cela par le fait que le trafic était très faible voir inexistant.
(Sans doute uniquement msn et même pas un programme de p2p ou du surf) :



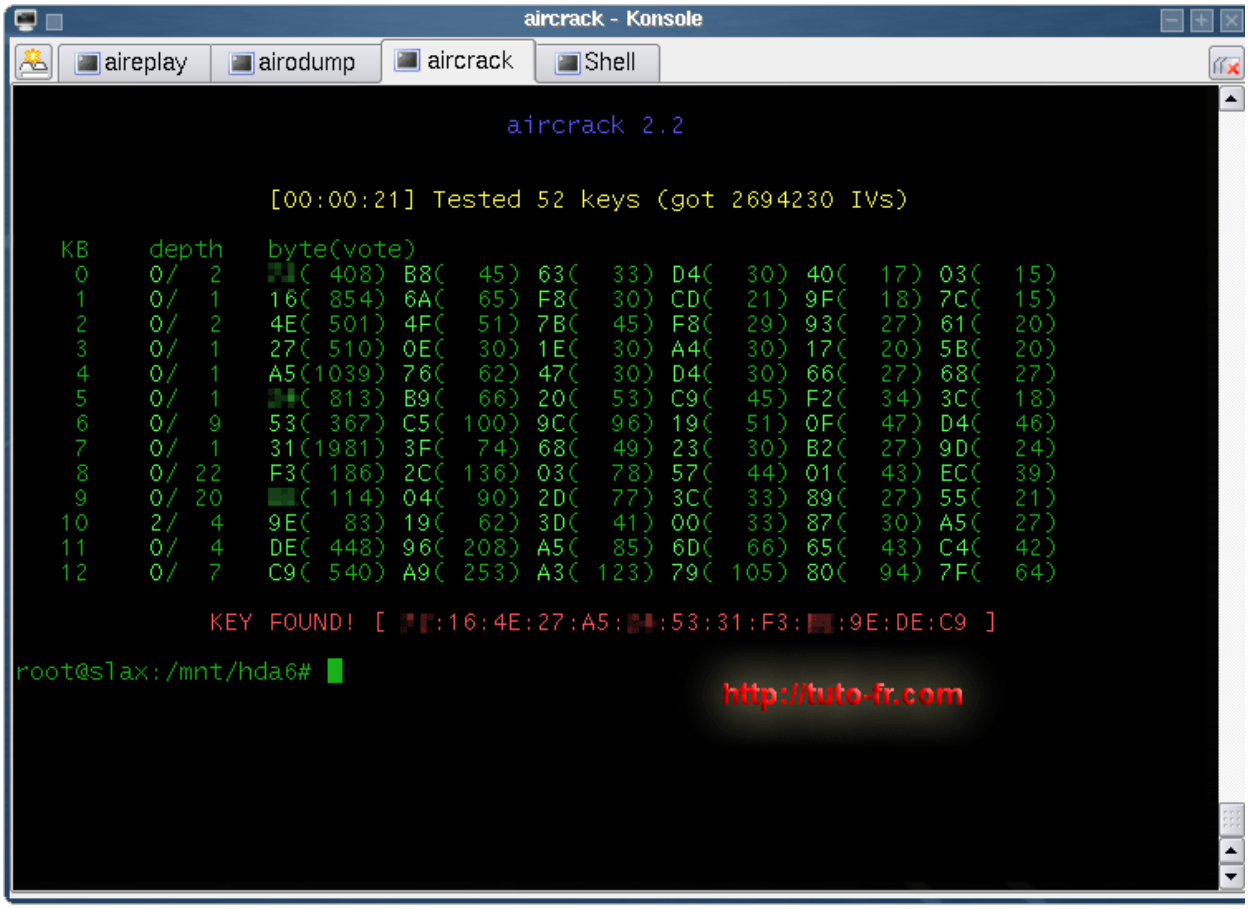
Qu'a cela ne tienne, il suffit simplement de choper plus de IVs.

Pour se faire il est préférable d'attendre la station, de choper de nouveaux ARP avec aireplay (je préfère plutôt que d'utiliser les anciens) et de lancer airodump tourner :D

Personnellement j'ai laisser tourné airodump et j'ai relancer un aireplay en ôtant le paramètre -r afin de choper de nouveaux arp. Comme ça des que la station se pointe, de nouveaux arp circulent, lancent mon airplay et airodump chope les paquets. C'est la meilleur méthode.

Si jamais vous n'arrivez pas à choper d'arp, laisser tourner le plus longtemps possible et si une station est présente lancez une attaque par dés-authentification qui devrait stimuler l'envoi d'arp:
« aireplay -2 + les paramètres habituels Essid et bssid »
Je suis donc parti en cours et à mon retour j'avais à peu près 2.6M de IVs plus qu'il n'en faut :D

Et en relançant aircrack :



Bingo !!!!

On s'aperçoit en comparant les 2 image celle ou l'attaque a échoué et celle réussie que l'on retrouve sensiblement les même chiffres, il suffisait donc simplement de choper plus de IVs.
Si jamais cela ne fonctionnait toujours pas, augmentez le fudge factor de aircrack en rajoutant un paramètre **« -f chiffre en 2 et 10 »**

Exemple :
« aircrack -x -0 *.cap *.IVs -f 4 »

Par défaut le fudge factor est à 2.

Aircrack utilise 17 type de statistiques crées par Korek.
Vous pouvez choisis de desactiver l'une d'entre elles les une apres les autres si jamais vous avez bcp de IVs mais que le crackage foire :/

Exemple :
« aircrack -x -0 *.cap *.IVs -k 4 »
« aircrack -x -0 *.cap *.IVs -k 12 » ...

On peut bien entendu combiner avec le fudge factor

Si jamais vous avez + de 3M de IVs que vous avez capturé alors qu'il y avait du trafic (bcp) et que l'attaque foire il peut y avoir plusieurs raisons :

-Le réseau a changé de clef mais bon ça vous devriez le savoir puisque vous en êtes le proprio
-Le fichier de capture est corrompu
-Vous z'avez trop pas de chance :s
...

5://Configuration de la connection :

Bon maintenant c'est bien beau vous avez la clé wep **copiez la vite fait dans un fichier écrivez la 12 fois sur un papier**. Ne confondez pas les 0 avec des o majuscules car le codage est hexadécimal, les seules possibilités sont 0 à 9 et A à F.

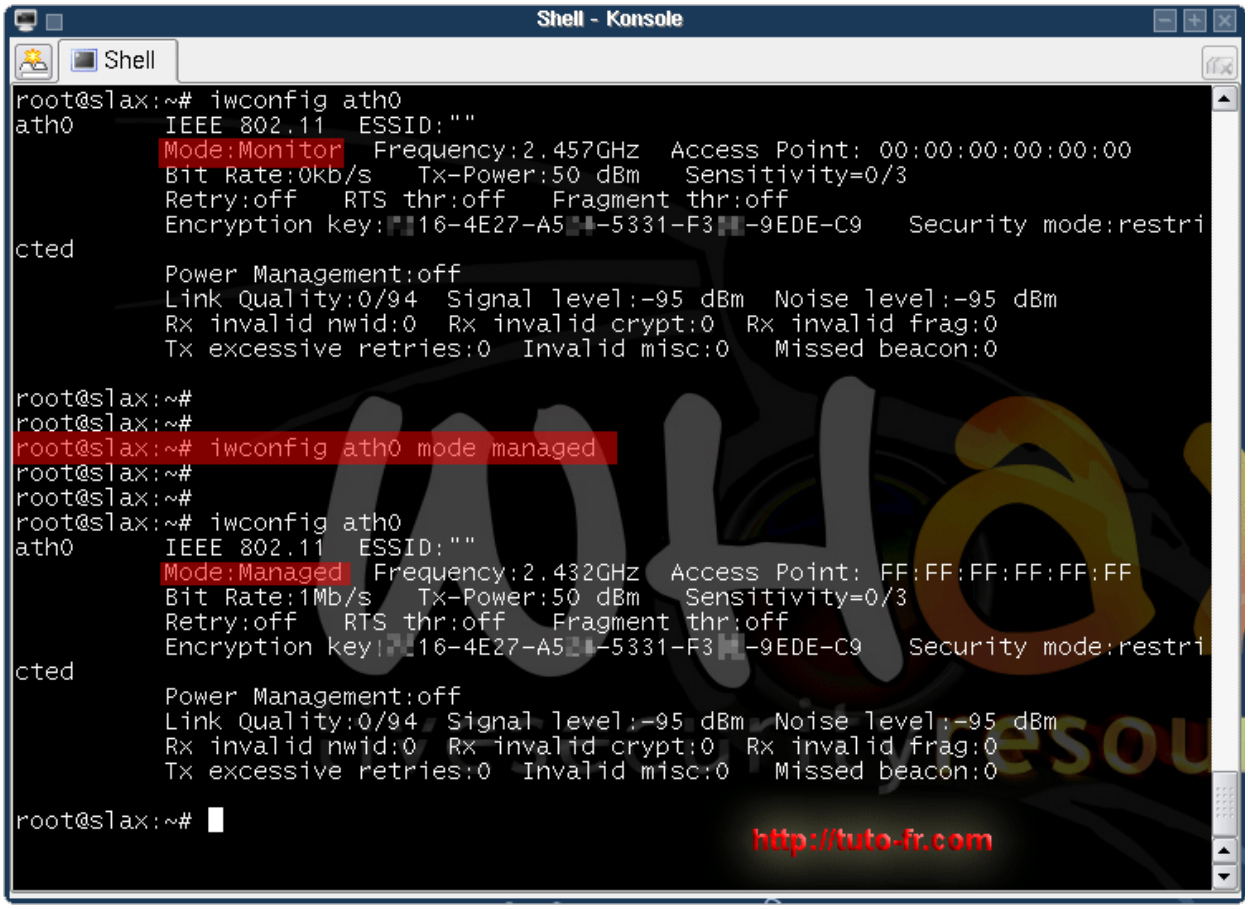
Bon maintenant on a la clef wep, il ne nous manque plus que le **plan d'adressage du réseau**. Cependant, il est bien souvent inutile car la quasi-totalité des réseaux utilisent **dhcp**, c'est-à-dire ip automatique : vous vous connectez à l'accès point et il vous attribut une ip.

Vous pouvez donc tenter de vous connecter avec windows (attention sous windows, il faut enlever les **« : »** entre les parties de la clef et si il y a un filtrage d'adresse mac : Changer son adresse mac sous windows) ou alors avec whax qui intègre un module de connection wifi.

5.1://Avec le module de whax :

Pour l'utiliser vous devez d'abord passer votre carte en **« mode managed »** pour cela tapez :
« iwconfig ath0 mode managed »

Et si vous souhaiter repasser en mode monitor pour la capture de paquets il vous suffit de mettre :
« iwconfig ath0 mode monitor »



Si l'AP applique un filtrage d'adresse mac changez votre adresse mac et remplacez la par celle d'une station qui s'est connectée a l'AP :

Changer son adresse mac sous linux
Changer son adresse mac sous windows

Ensuite pour ouvrir l'assistant, aller dans le menu démarrer puis choisissez **« Whax tool/Wireless/wireless assistant »** et configurez pépère votre réseau. (si dhcp ne fonctionne pas essayer sous windows ou voir plus bas pour trouver l'adressage du réseau)
Le module vous dira si la connection est réussie ou non.

Et vous pouvez toujours tester par une commande de type :

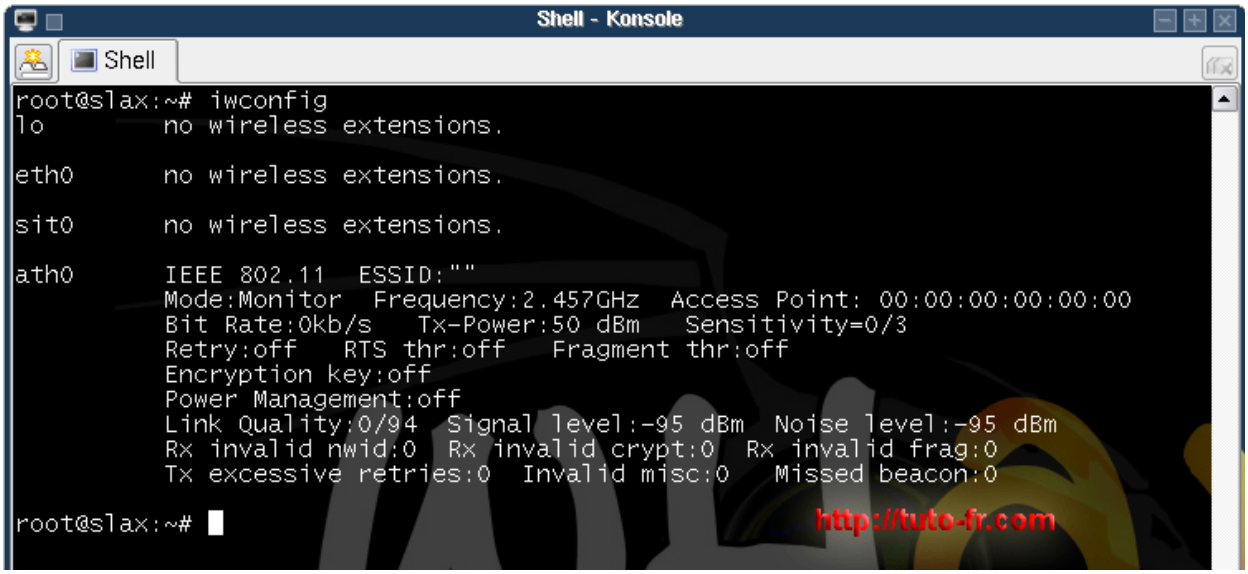
« ping www.google.fr »

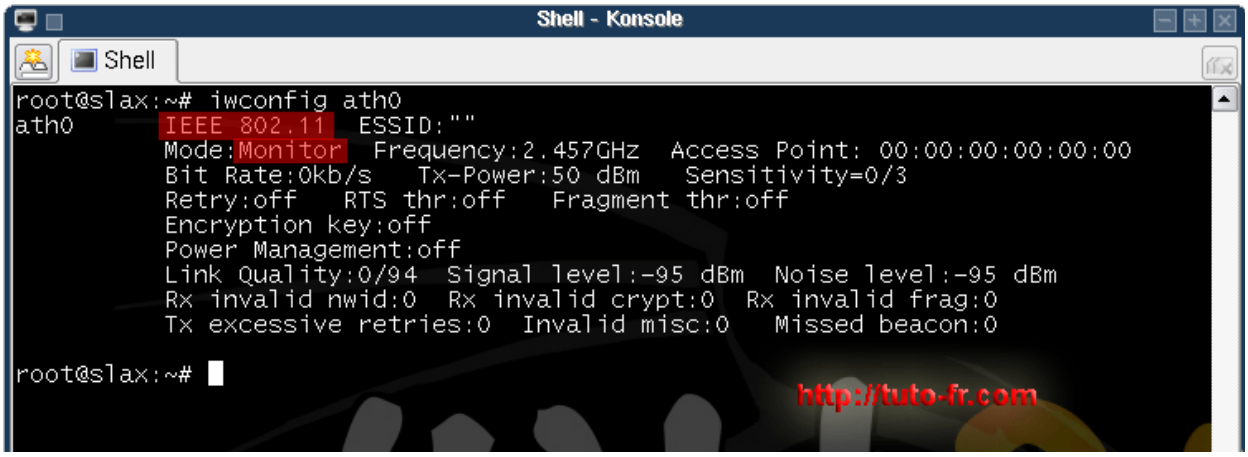
5.2://En mode console :

Si vous passez par whax vous pouvez aussi le faire en mode console :D.

Le commande du mode console sont :

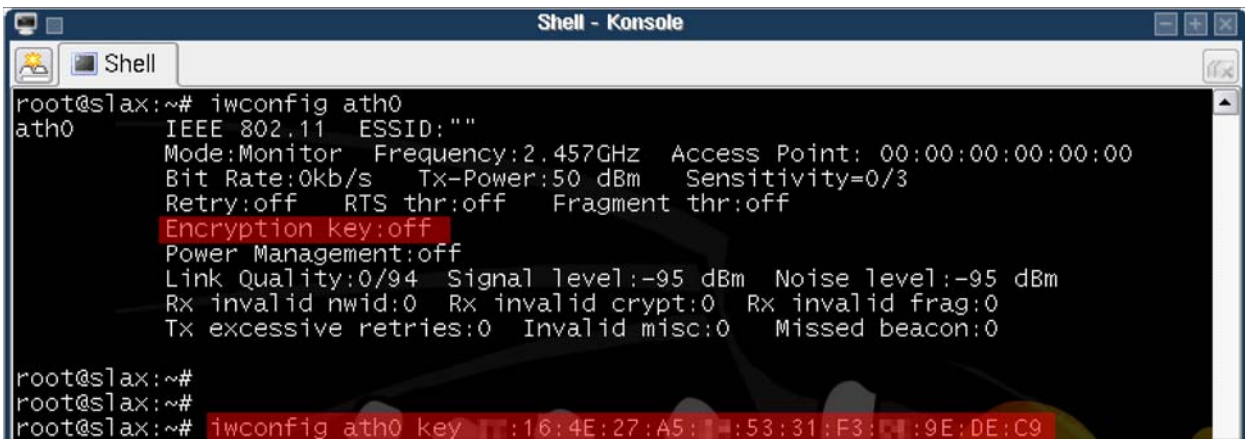
Tout les paramètre de votre configu wireless s'affichent en tapant :
« iwconfig ath0 »





Passage en mode managed :
« iwconfig ath0 mode managed »

Configuration de la clef wep :
« iwconfig ath0 key xx :xx :xx :xx :xx :xx »



Vous pouvez parfaitement combiner les paramètres :
« iwconfig ath0 mode managed key xx :xx :xx :xx :xx :xx »

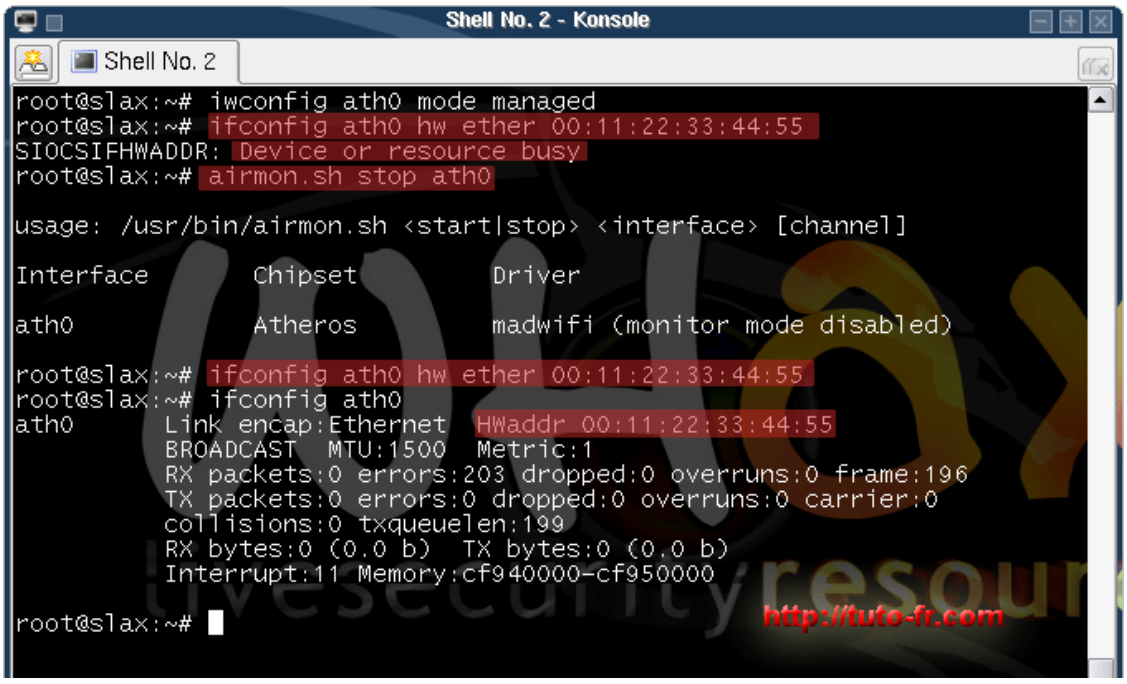
5.3:// Changer son adresse mac :

5.3.1:// Sous linux :

Si l'AP applique un filtrage d'adresse mac changez votre adresse mac et remplacez la par celle d'une station qui s'est connectée a l'AP :

Pour se faire vous devez en premier éteindre le périphérique wifi :
« airmon.sh stop ath0 »

Puis pour changer l'adresse mac :
« ifconfig ath0 hw ether xx :xx :xx :xx :xx :xx » (remplacer xx :xx. par l'adresse mac de la station : son bssid)



Dernière étape : activation de dhcp :
« dhcp ath0 »

Si vous avez le retour de console c'est que c'est réussi pour dhcp (si dhcp ne fonctionne pas essayer sous windows ou voir plus bas pour trouver l'adressage du réseau)
Ensuite faite un **« ping www.google.fr »** pour vérifier que tout fonctionne.

5.3.2:// Sous widows :

Si jamais vous devez **changer votre adresse mac sous windows**, aller dans :
« démarrer/ panneau de configuration/performance et maintenance/système » Onglet matériel puis gestionnaire de périphériques.

Choisissez la catégorie **carte réseau**, choisissez **votre carte** et faites **clic droit/ propriétés**. Choisissez l'onglet avancé et vous devez avoir une catégorie **adresse mac** ou équivalente. Choisissez **administrer**

localement et mettez la valeur d'adresse mac que vous voulez (en particulier le bssid de la station)

Vous pouvez également utiliser **etherchange** un programme pour windows qui **change** votre **adresse mac.**
Télécharger etherchange.

Lancez le choisissez l'interface reseau dont vous voulez changer l'adresse physique puis entrez l'adresse mac de remplacement :D Et voila ;)

6:// Trouver l'addressage du reseau :

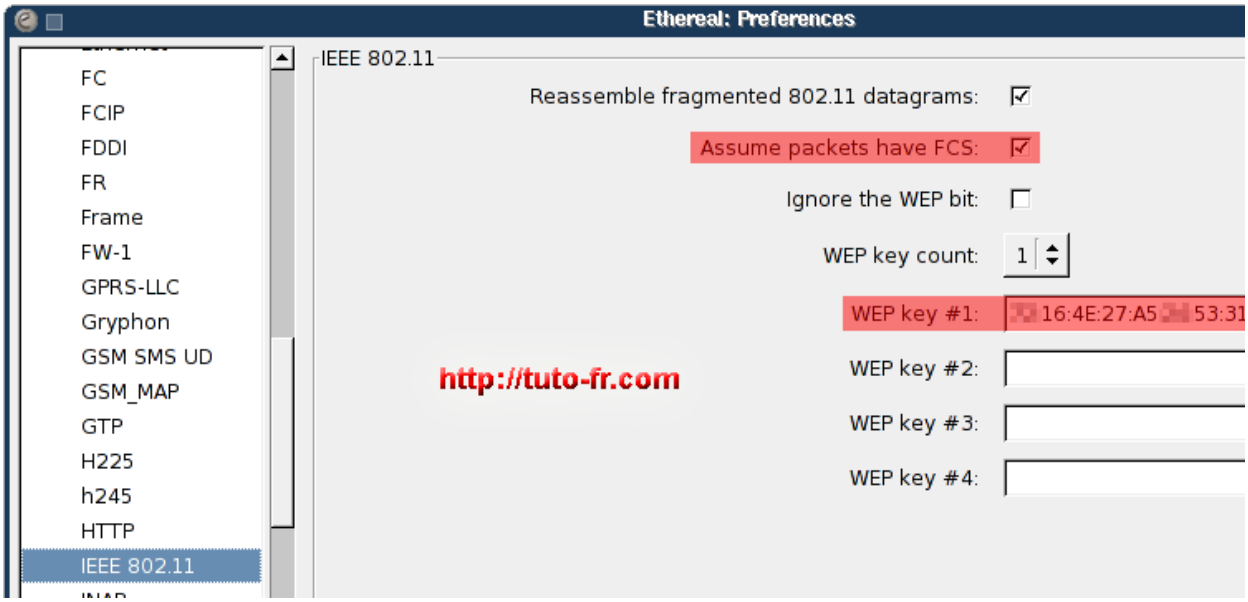
Si le réseau ne possède pas de dhcp ou si le dhcp est désactivé vous devez trouvez le plan d'adressage du réseau.
Dans la plupart des cas il s'agit de

192.168.1.xxx avec le point d'accès 192.168.1.1 et le masque de sous réseau 255.255.255.0

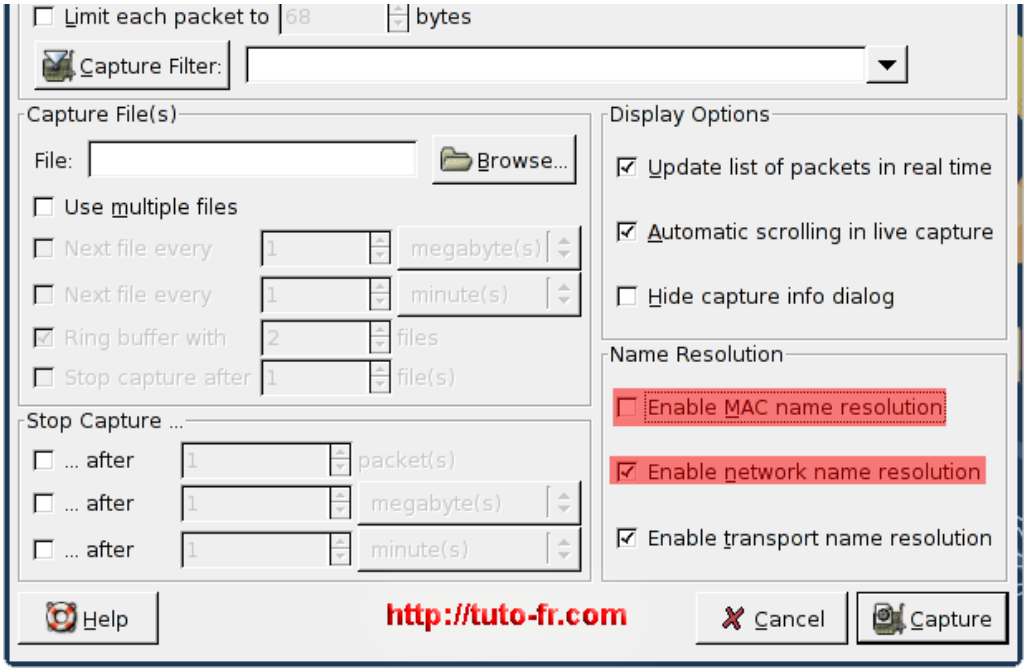
Cependant il existe un moyen simple rapide et sur de connaître l'ip du point d'accès grâce à **ethereal** un **sniffeur de réseau** (**vous devez posséder la clef wep pour trouver l'ip**).

Pour lancer ethereal faite
« menu démarrer/WHAX Tools/Sniffers/ethereal »

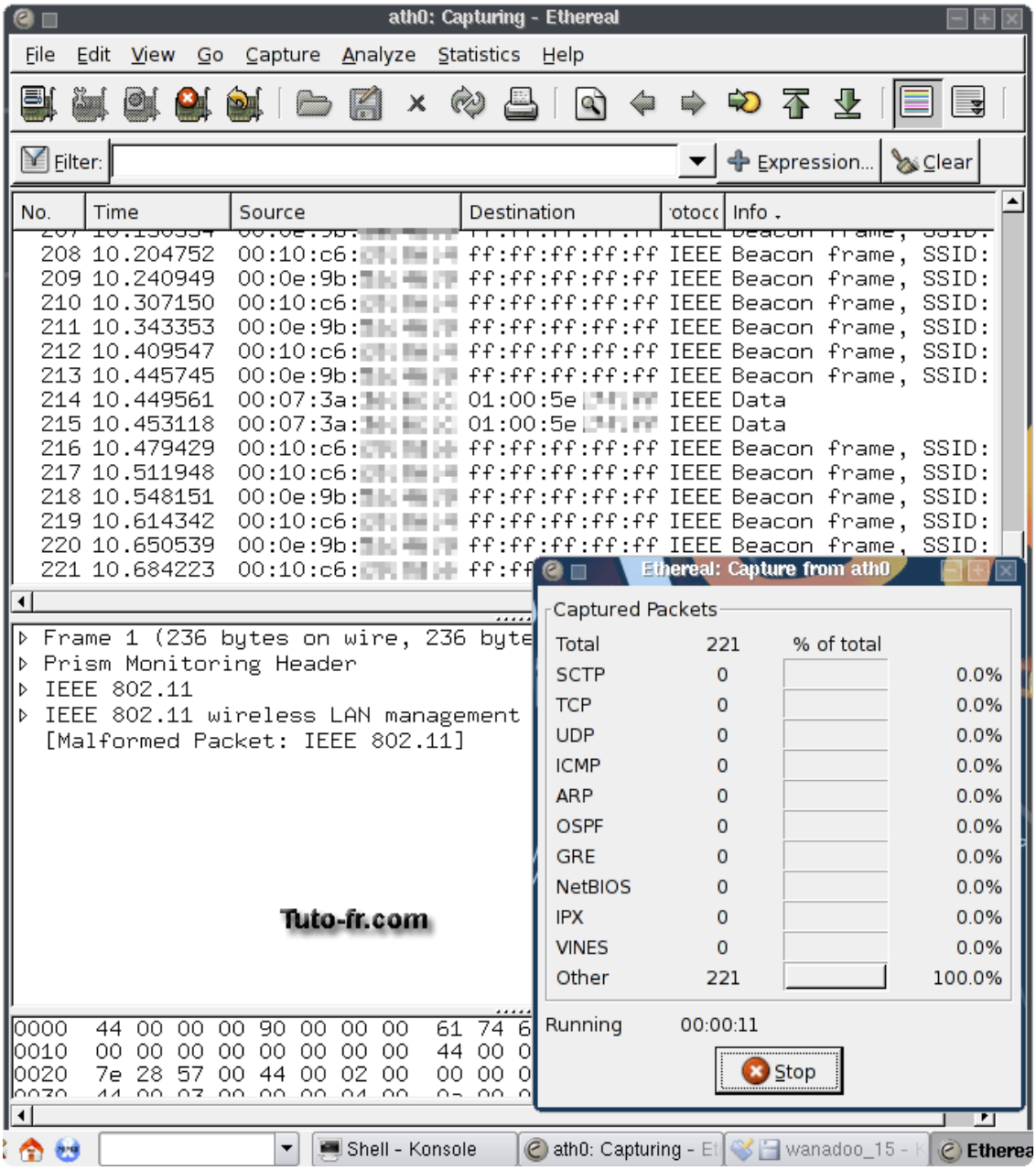
Configurer ethereal pour qu'il décrypte les paquet avec la clef wep que vous venez juste de trouver (sinon vous n'aurez pas les ip) :
Faites : « Edit/préférences/protocols/IEEE 802.11 » (pour ouvrir protocols cliquez sur le petit triangle ensuite appuyez sur la touche i pour tomber directement sur IEEE 802.11)
Et configurez la clef wep :
Cochez bien « Assume packets have FCS »



Confirmez avec ok puis commencez la capture :
Faites **« capture/options »**
Choisissez l'interface (ath0)
Cochez la case (capture paquets in promiscuous mode)
Cochez la case enable network name résolution



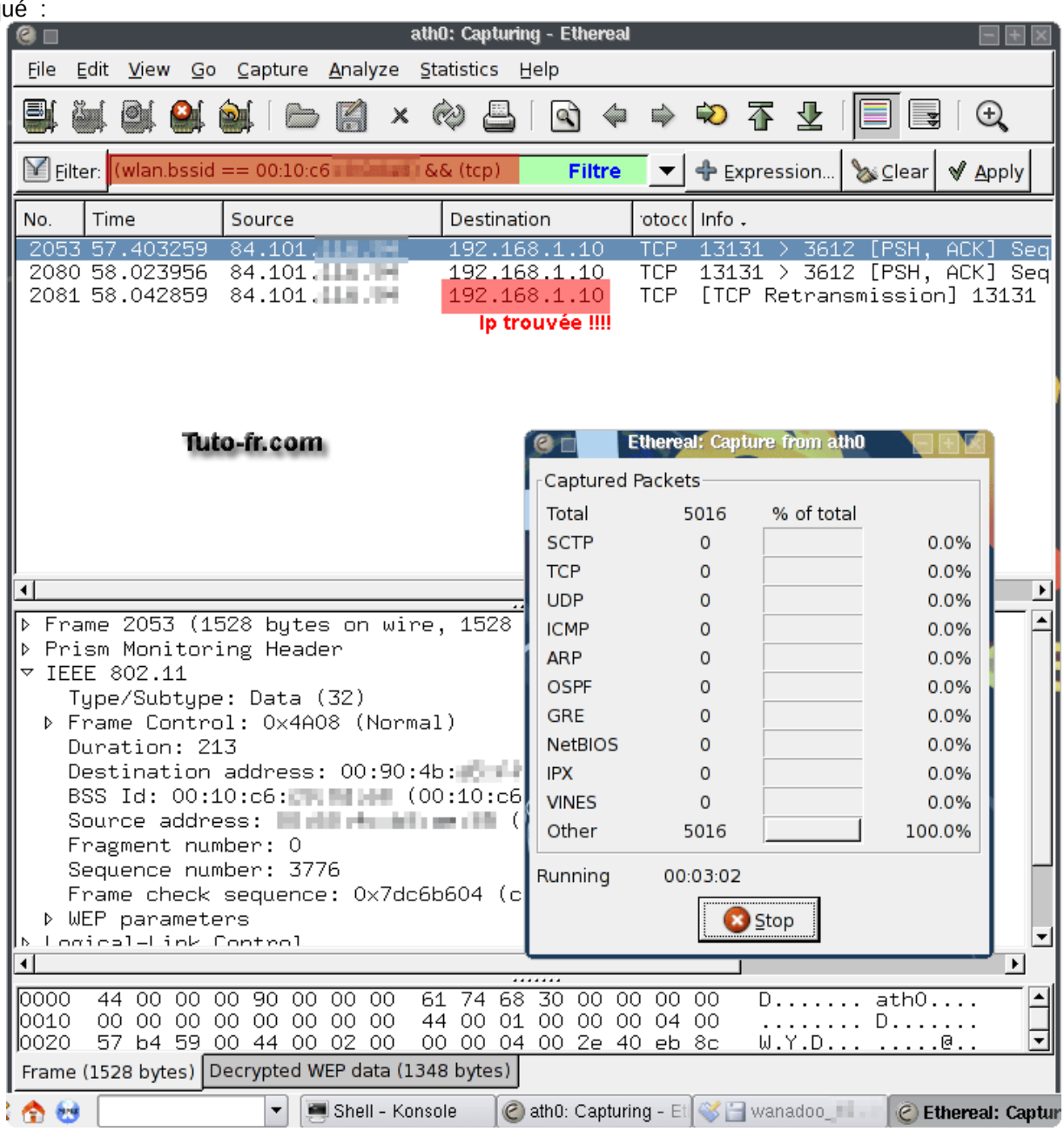
Cliquez sur capture et la capture commence :D.
Vous allez vous retrouvez avec un sacré paquets de paquets :P :



Pour n'afficher que ceux qui vous intéressent **appliquez un filtre dans la case filter.**

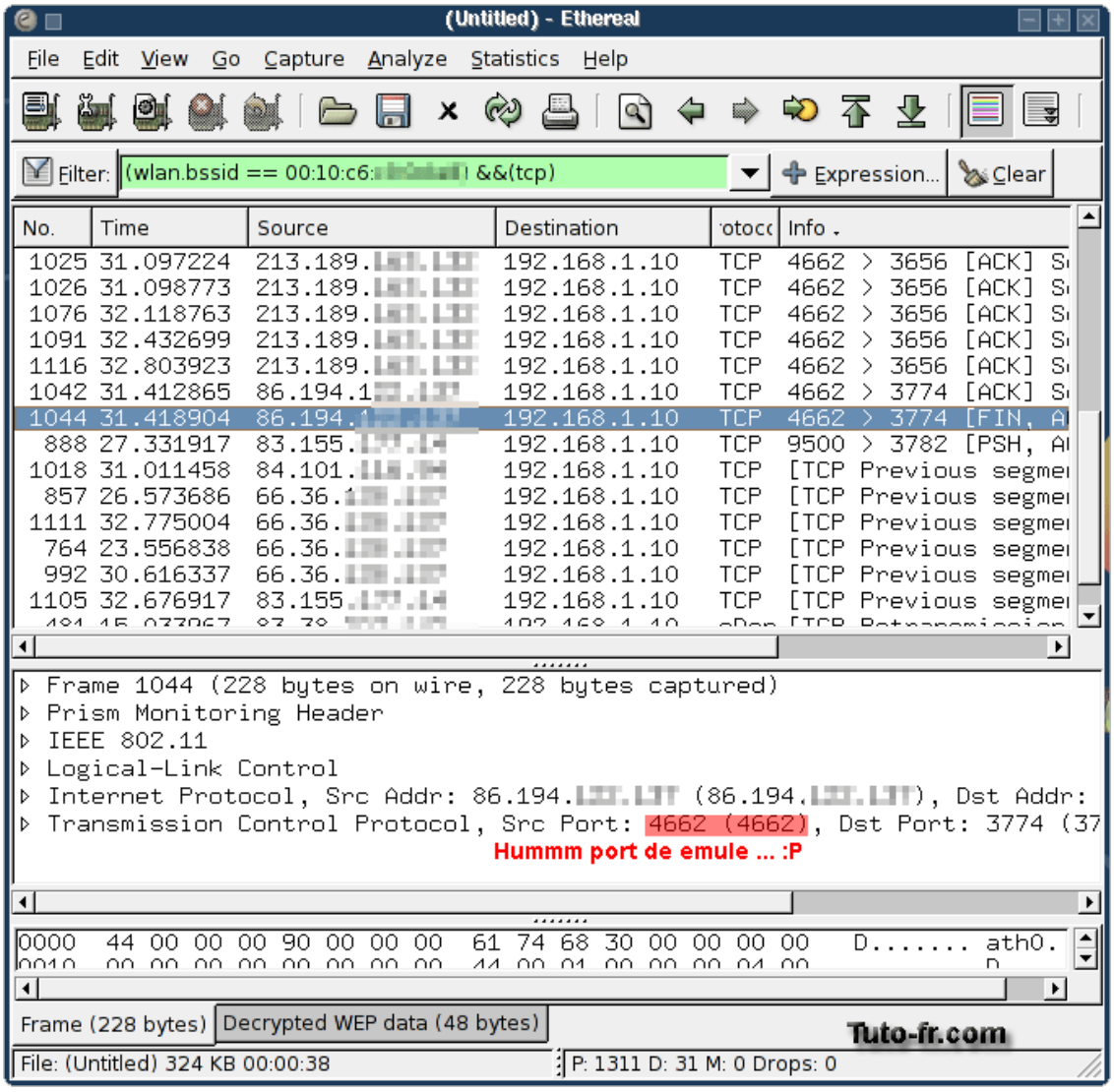
Un filtre de type « (wlan.bssid == bssid de l'ap) && (TCP) marche du tonnerre :

En fait vous choisissez de voir que les paquets transportés par protocole TCP et dont le bssid est celui indiqué :



Et la : Bingo, on trouve l'ip.

Si vous laissez tourner un peu on peu même avoir d'autres information et confirmer l'ip :



Par exemple ici on voit que mon cher voisin doit sûrement utiliser émule :D.

Et voila le boulot est terminé, vous avez l'adressage du réseau, l'adresse mac de la station, et la clef wep il vous reste plus qu'a vous connecter.

En cas de soucis, le forum de support est également là pour vous aider

Ce didacticiel a été réalisé en particulier grâce à la vidéo de Christophe Devine et surtout l'aide de aircrack. Ces sites m'ont également aidé (en anglais) :

L'aide de aircrack:
http://www.cr0.net:8040/code/network/

Un forum interressant:
http://new.remote-exploit.org/index.php/Main_Page

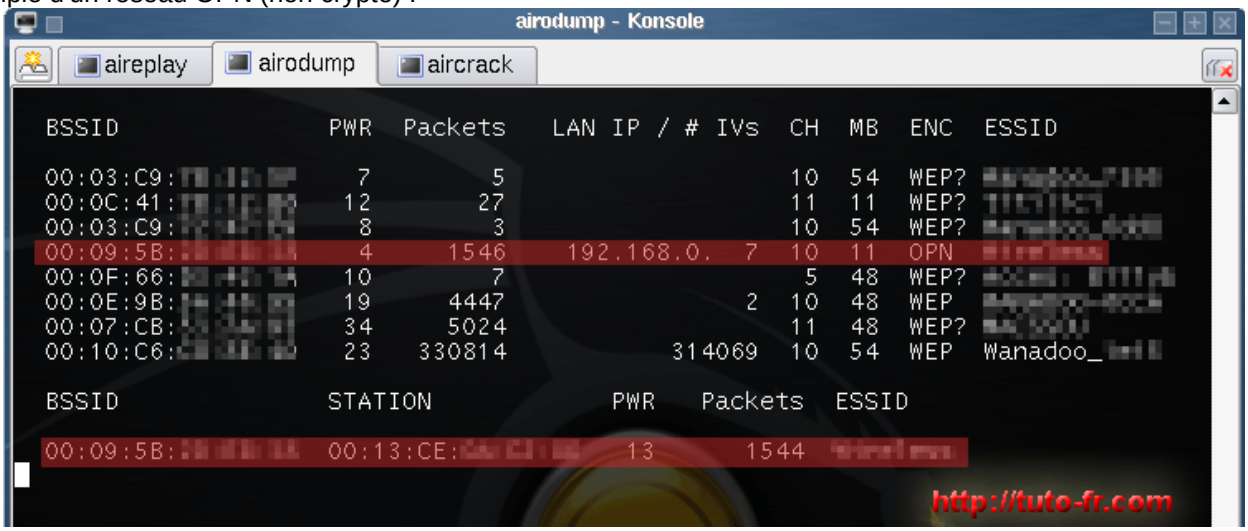
Un site de tuto en vidéo:
http://www.crimemachine.com/

Le site officiel de Whax

http://www.iwhax.net/modules/news/

Annexes :

exemple d'un reseau OPN (non crypté) :



Injection de paquet sous Windows :

Il existe different logiciel pour faire de l'**injection de paquets wifi** sous **plateforme win32.**

Notamment pour les cartes à chipset Atheros:

CommView for WiFi ou sur le site de l'editeur: http://www.tamos.com/products/commwifi/
Voici une liste des cartes supportées par commView

Pour les cartes à chipset Prism:

AirGobbler Packet Generator ou sur le site de l'éditeur: http://www.tuca-software.com/transmit.php

Décryptage de paquets avec airdecap :

Télécharger airdecap

Utilisation:

```
airdecap [options] <pcap file>
```

Options:

```
-l       : Ne pas enlever la frame header 802.11
-b bssid : Filtre adresse mac de l'acces point
-p pass  : Clef WPA
-e essid : Identifiant ascci du reseau cible
-w key   : Clef wep en haxa du reseau cible
-k pmk   : WPA Pairwise Master Key in hex
```

Exemples:

```
airdecap -b 00:09:5B:10:BC:5A open-network.cap
airdecap -w 11A3E229084349BC25D97E2939 wep.cap
airdecap -e "the ssid" -p passphrase  tkip.cap
```

Source: http://www.cr0.net:8040/code/network/aircrack/#q150

Fichiers :

Télécharger la suite aircrack avec les dll peek.dll **peek.dll**, **peek5.sys et cygwin1.dll**

Winaircrack une interface graphique pour aircrack sous windows codé par *hexanium* : **Winaircrack**

Utilitaire pour tout connaitre sur votre adaptateur wifi ou adaptateur reseau Wlandrv par Hexanium également ;) **Wlandrv**

Drivers windows Xp supportant le WPA pour les chipset Prism 2 avec support du WPA source: http://www.cr0.net:8040/code/network/aircrack/

Pour les **drivers tout chipset** regardez le guide aircrak: http://www.cr0.net:8040/code/network/aircrack/#q080

La liste des adresses mac de tous les constucteurs
Grace à cette liste, il vous suffit de regarder simplement les 3 premiers bit des adress mac pour trouver le constructeur