DECRYPTAGE

D'UNE

CLEF WEP

SOUS

WINDOWS

(XP OU 2000)

Par **Maisse Sébastien**

Document en date du 10 novembre 2005

Table des matières

Préambule :

Bienvenue dans ce document qui a pour but de vous faire découvrir la manipulation pour cracker une clef WEP sous un environnement Windows (XP ou 2000 voir 98).

Dans ce présent document, je vais utiliser le programme **WinAircrack** qui est en fait une interface graphique pour les programmes **airodump**, **aircrack**.

ATTENTION, CE DOCUMENT EST FOURNI A TITRE PEDAGOGIQUE. EN AUCUN CAS, IL VOUS EST PERMIS DE METTRE CETTE TECHNIQUE EN PRATIQUE SUR UN RESEAU DONT VOUS N'AURIEZ PAS OBTENU AU-PREALABLE L'ACCORD DU PROPRIETAIRE.

Dans mon cas, j'ai effectué le test sur mon réseau sans fil personnel, il est constituer d'un point d'accès de marque Linksys. Concernant le matériel utilisé pour l'écoute du réseau wifi, j'ai utilisé une clef de marque **Sagem** modèle **WL5061S** (une clé livrée avec la livebox de chez wanadoo).

Avant de commencer notre test, si vous souhaitez réaliser cette action, il vous est possible d'utiliser la live CD (linux) du nom de **WHAX**. Par ailleurs, un tutoriel sur la manip' est disponible à l'url suivante :

http://www.tuto-fr.com/tutoriaux/tutorial-crack-wep-aircrack.php

Téléchargement de WinAircrack :

Pour ce qui est de WinAircrack, qui je vous le rappel est une interface graphique pour les programmes aircrack et airodump, dont l'auteur est **Hexanium** est disponible à l'url suivante :

http://www.subagora.com/subagora/navigate.php?cmd=soft_detail&ret=1&soft_id=132

Dans le cas présent, nous allons télécharger la version complète de WinAircrack (le pack complet), il ne sera donc pas nécessaire de télécharger Aircrack en supplément.

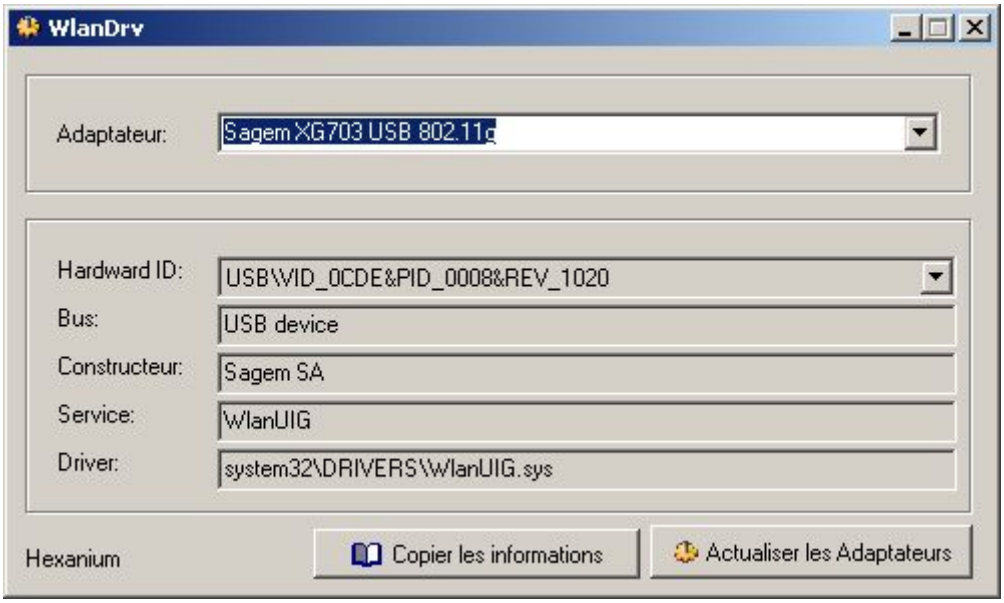
http://www.subagora.com/WinAircrack/download/WinAircrackPack.zip

Par ailleurs, on pourra aussi télécharger le programme WlanDrv du même auteur :

http://www.subagora.com/WinAircrack/download/WlanDrv.zip

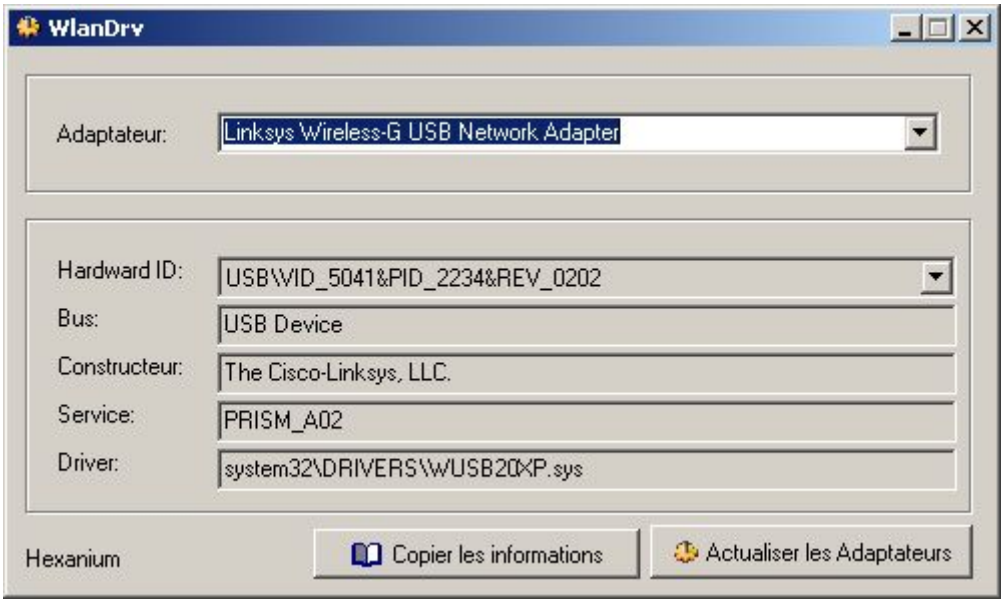
Lancement de WinAircrack :

Avant de lancé WinAircrack, on décompresse le fichier « WlanDrv.zip » qui fournira des informations concernant l'adaptateur usb ou la carte réseau wifi que nous allons utiliser.



Les informations concernant la clé usb wifi Sagem modèle WL5061S.

Si vous avez un adaptateur/carte réseau wifi utilisant un chipset **Prism**, il y a de forte de chance pour que vous deviez passer votre chemin.

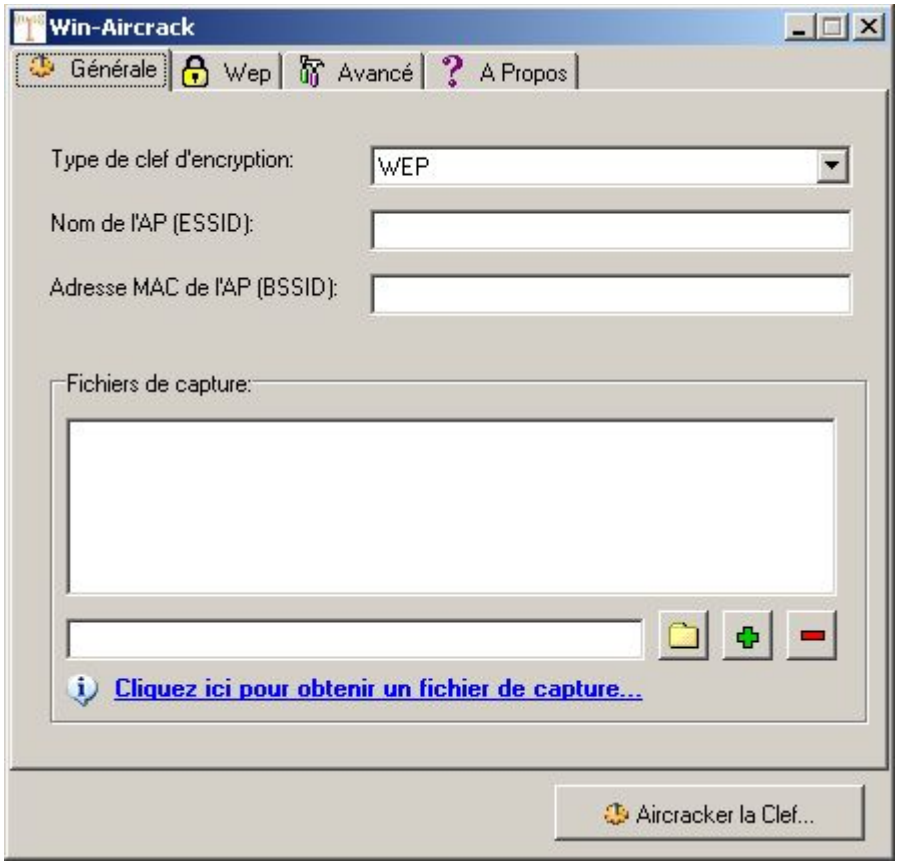


Les informations concernant un adaptateur usb de marque **Linksys** modèle **WUSB54G**.

Note : L'adaptateur a été testé sans succès, lors d'un second test...

Une fois, les informations de votre carte réseau ou de votre adaptateur récupérées, vous pouvez à présent décompressé le contenu du fichier « WinAircrackPack.zip », puis vous lancez le programme principale « WinAircrack.exe ».

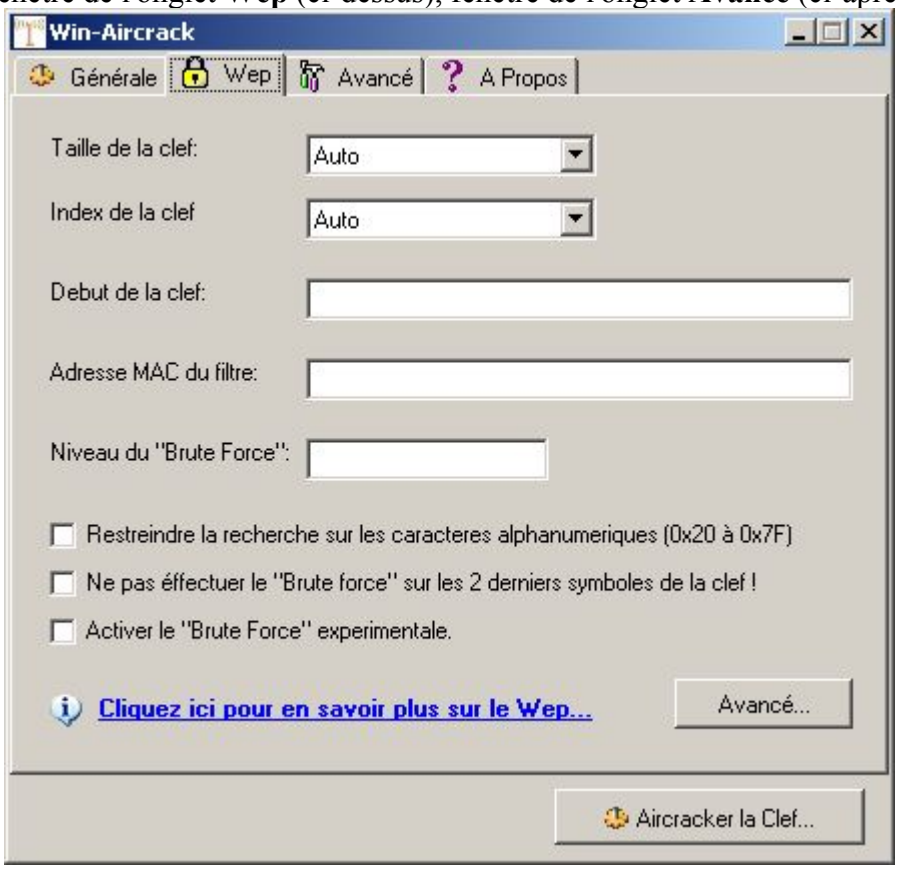
Vous arriverez sur une fenêtre similaire à celle ci-dessous :

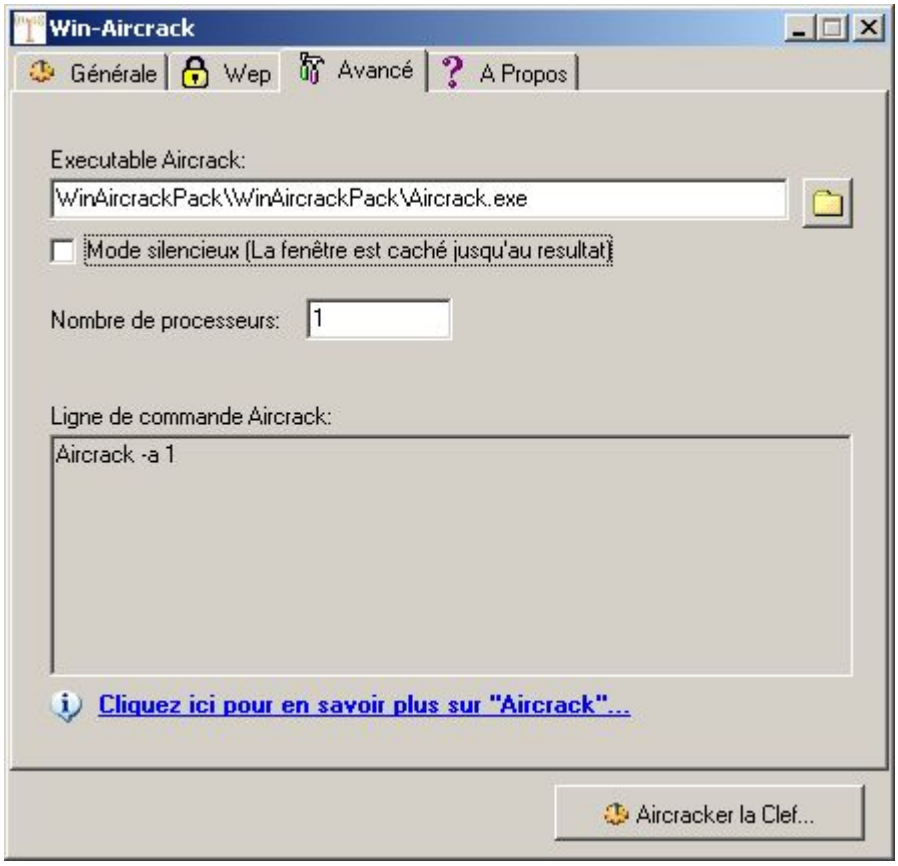


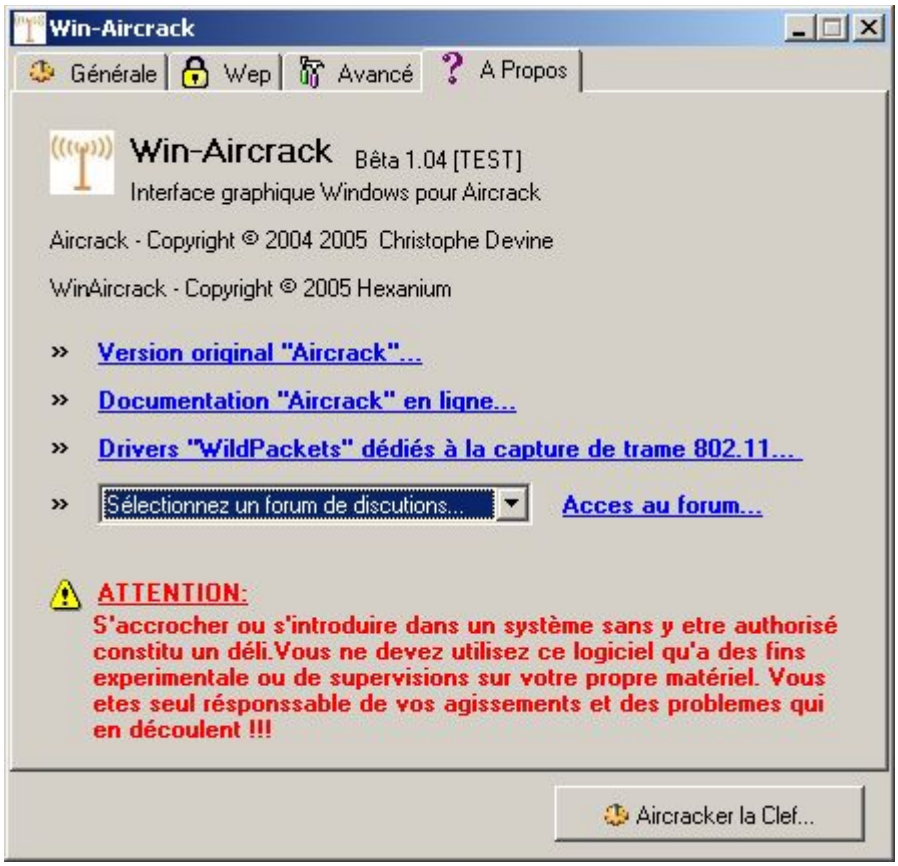
Fenêtre de l'onglet **Générale**.

Voici les différentes fenêtres des onglets **Wep**, **Avancé** et **A Propos**...

Fenêtre de l'onglet **Wep** (ci-dessus), fenêtre de l'onglet **Avancé** (ci-après).

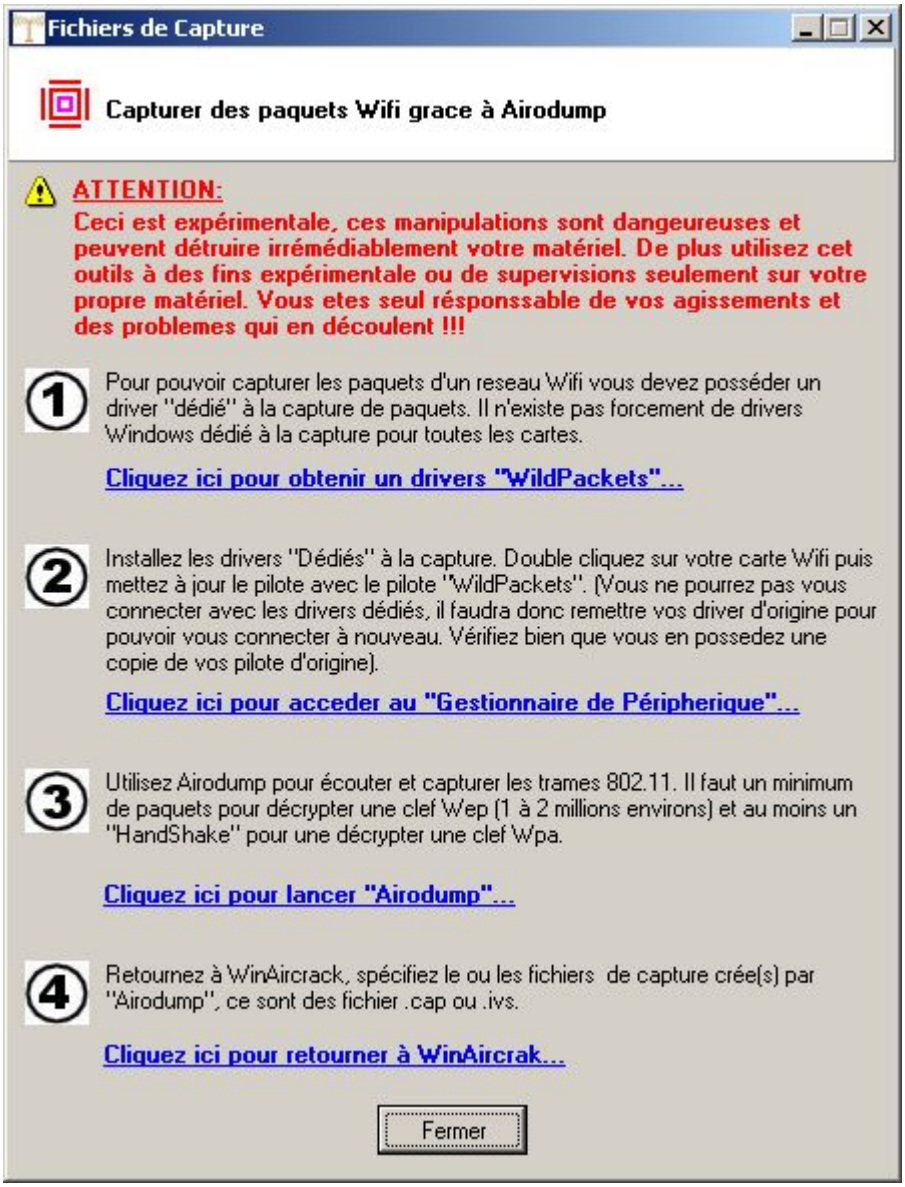






Fenêtre de l'onglet **A Propos**.

Le visite des onglets effectuée, nous allons commencer par écouter notre réseau wifi. Pour ce faire rendez-vous dans l'onglet **Générale**. Puis cliquer sur le lien « cliquez ici pour obtenir un fichier de capture ». Ce qui aura pour effet d'afficher la fenêtre suivante :



Comme vous pouvez le voir, il y a différents liens de disponible selon le cas qui se présente à vous.

En théorie, il faut suivre les étapes dans l'ordre suivants :

1. Obtenir un drivers « WildPackets » qui sont disponible à l'url suivante :

   http://www.wildpackets.com/support/downloads/drivers

2. Installer le driver « WildPackets » sur son windows.

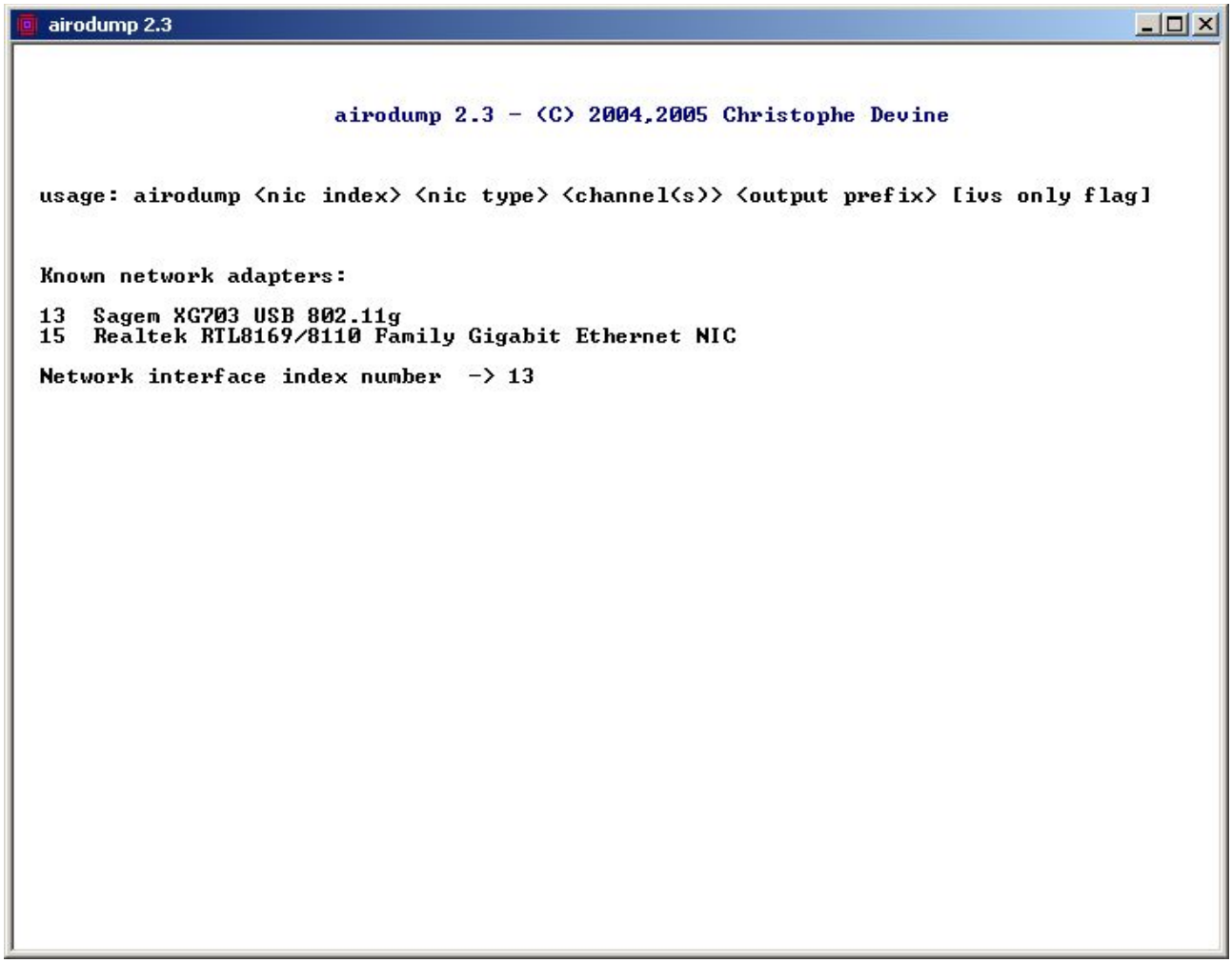
3. Lancer l'utilitaire Airodump

4. Revenir à WinAircrack pour traité le fichier de capture.

Dans le cas présent, j'ai pu sans soucis ne pas me préoccupé des étapes **1** et **2**. Je suis donc passé directement à l'étape **3** qui consiste à « capturé » des paquets de données grâce au programme **Airodump**.

Ici, je prend donc en considération que vous avez rempli si nécessaire les étapes 1 et 2... avant de poursuivre plus en avant dans ce document. Si tel est le cas, nous pouvons continuer.

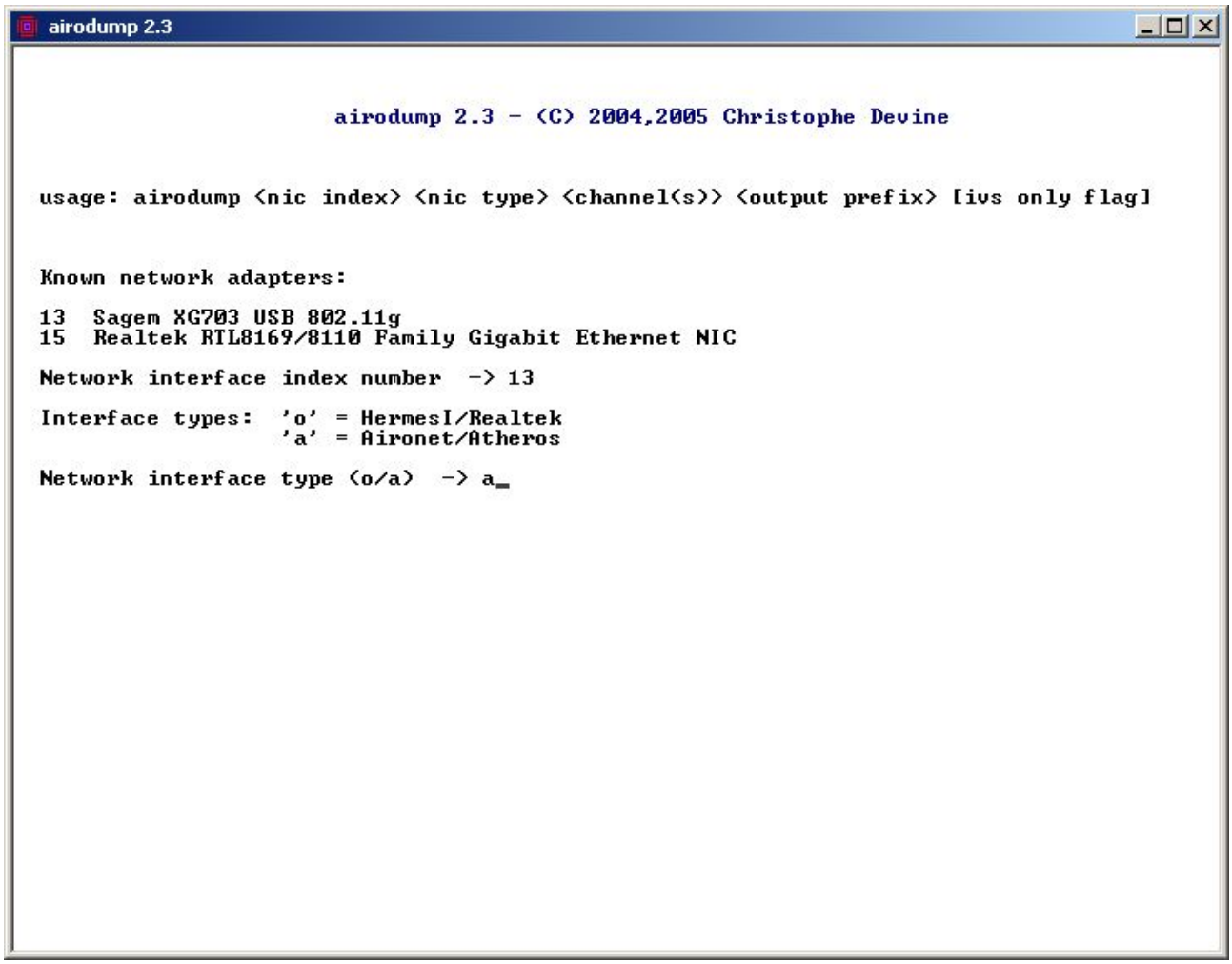
Tout d'abord, je choisi l'interface réseau que je vais utiliser pour réalisé l'écoute du réseau.



Choix de l'interface réseau, ici la clé usb Sagem (choix numéro 13).

J'appuie sur sur la touche **Entrée** pour confirmé mon choix.

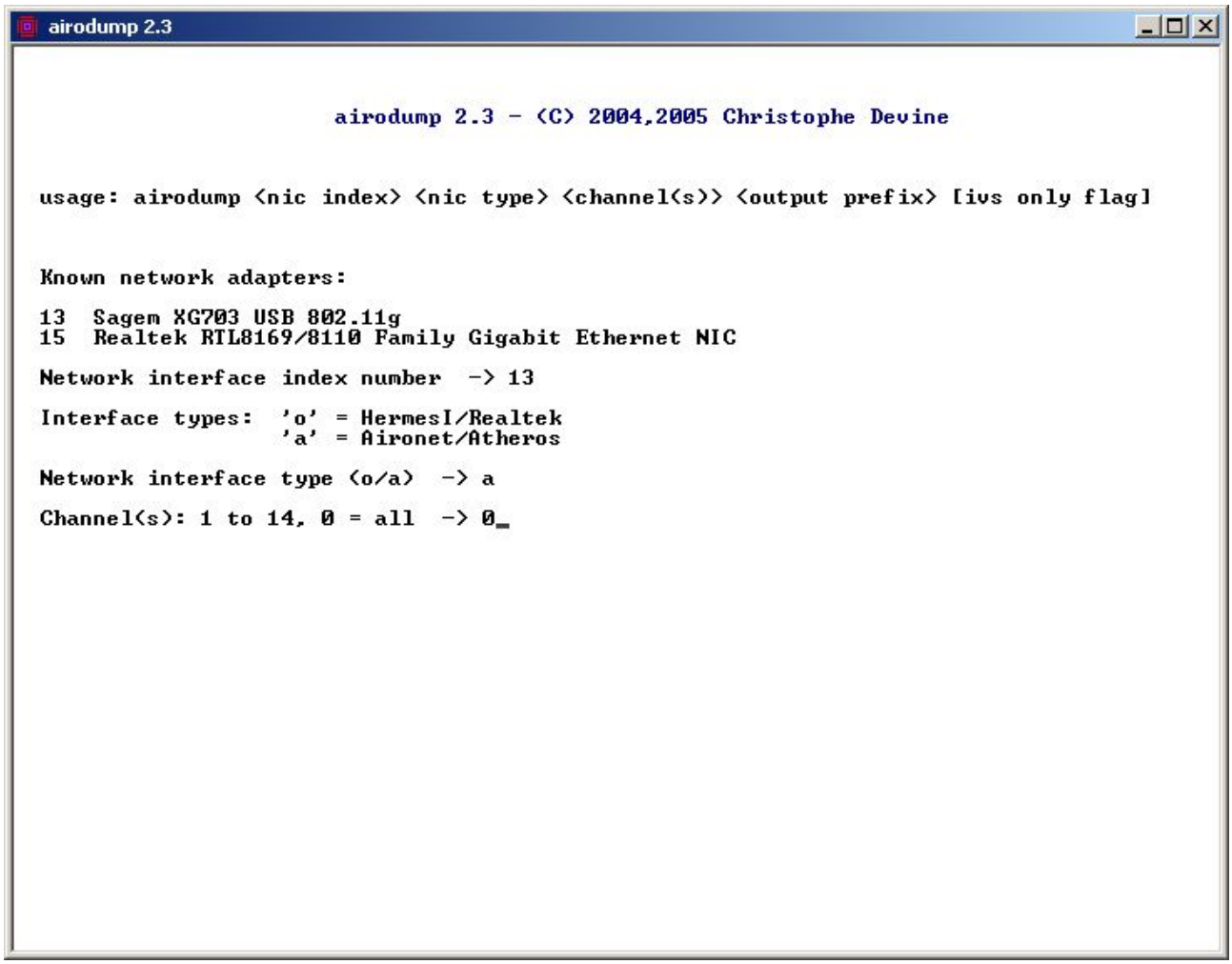
Je choisi ici le type d'interface, à savoir les pilotes « générique » de capture qui seront utiliser.



Mon choix est **a** pour la clé que je vais utiliser.

Ceci n'est valide que si votre matériel fonctionne avec ses drivers « générique », dans le cas contraire vous aurez pris soin d'installer le driver « WildPackets » adéquate pour votre carte/adaptateur.

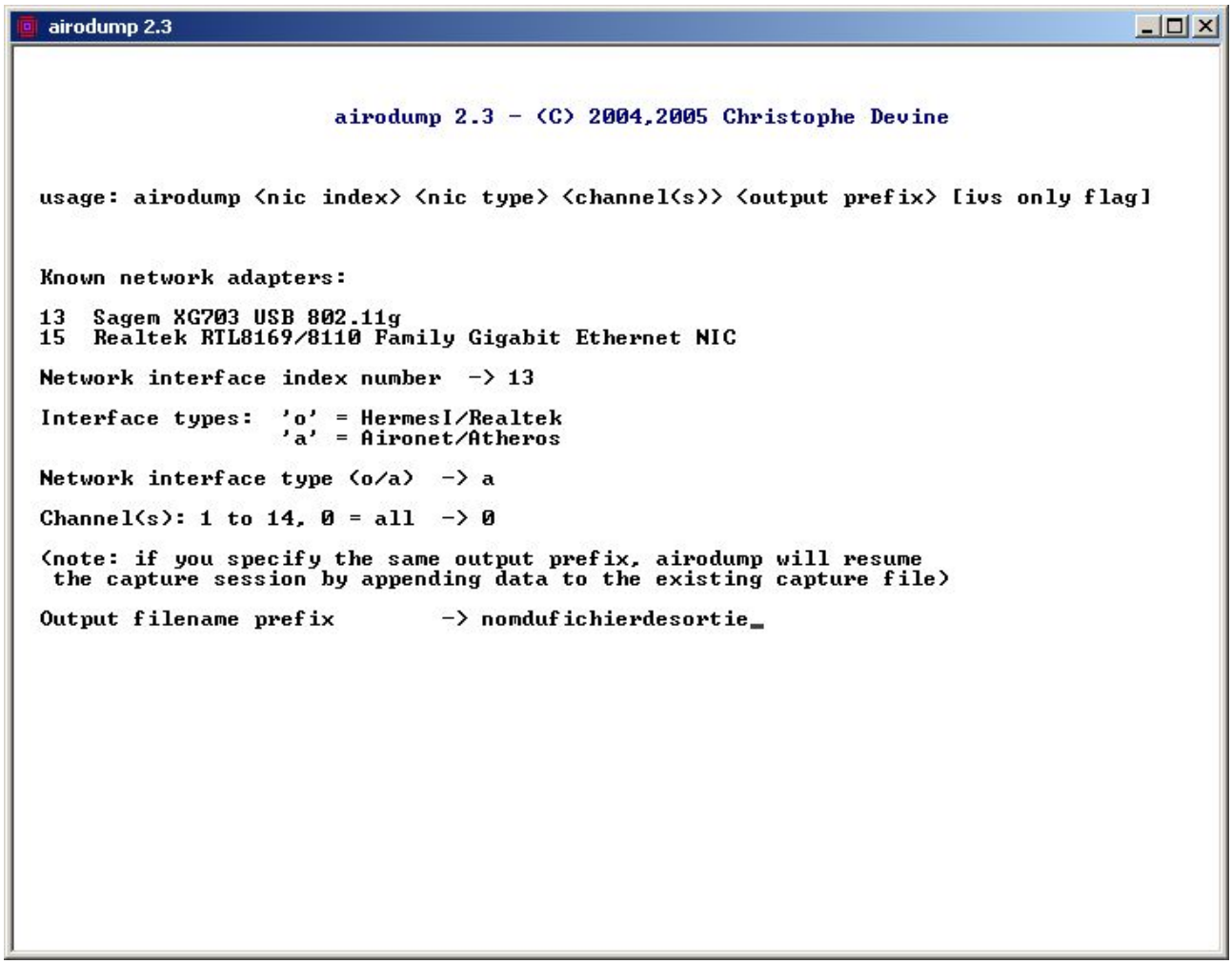
Ici, nous choisissons le canal qui sera écouter.. cela va de **1** à **14**. **0** permettant d'écouter automatiquement tout les canaux disponibles.



0 pour écouter tout les canaux.

Si vous connaissez le canal qui est utilisé par le réseau... Dans ce cas, vous pouvez le spécifier directement en lieu et place de **0**.

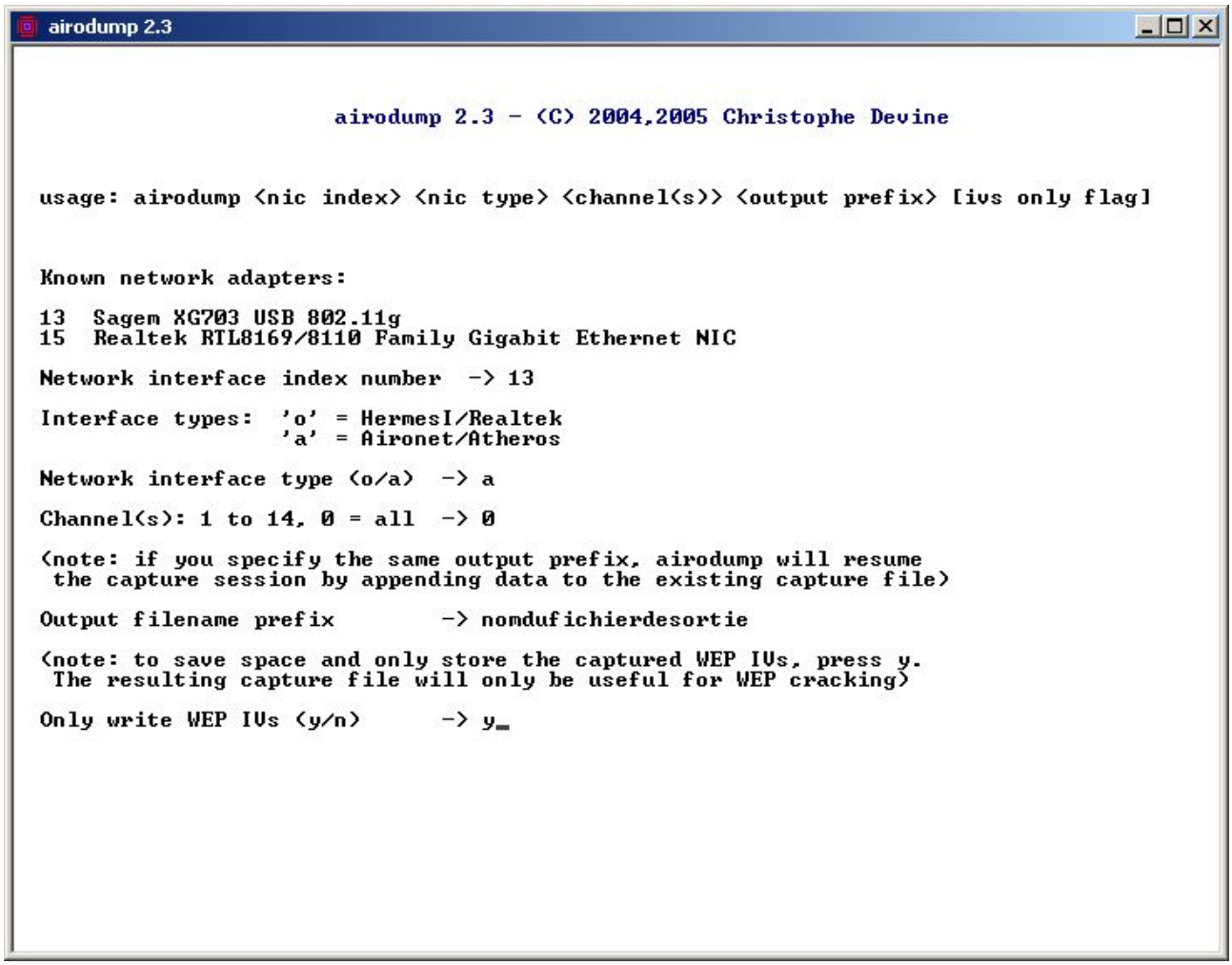
Nous déterminons le nom du fichier de sortie qui sera utiliser pour enregistré les données de la capture.



Ici, j'ai mis en nom de fichier de sortie « nomdufichierdesortie ».

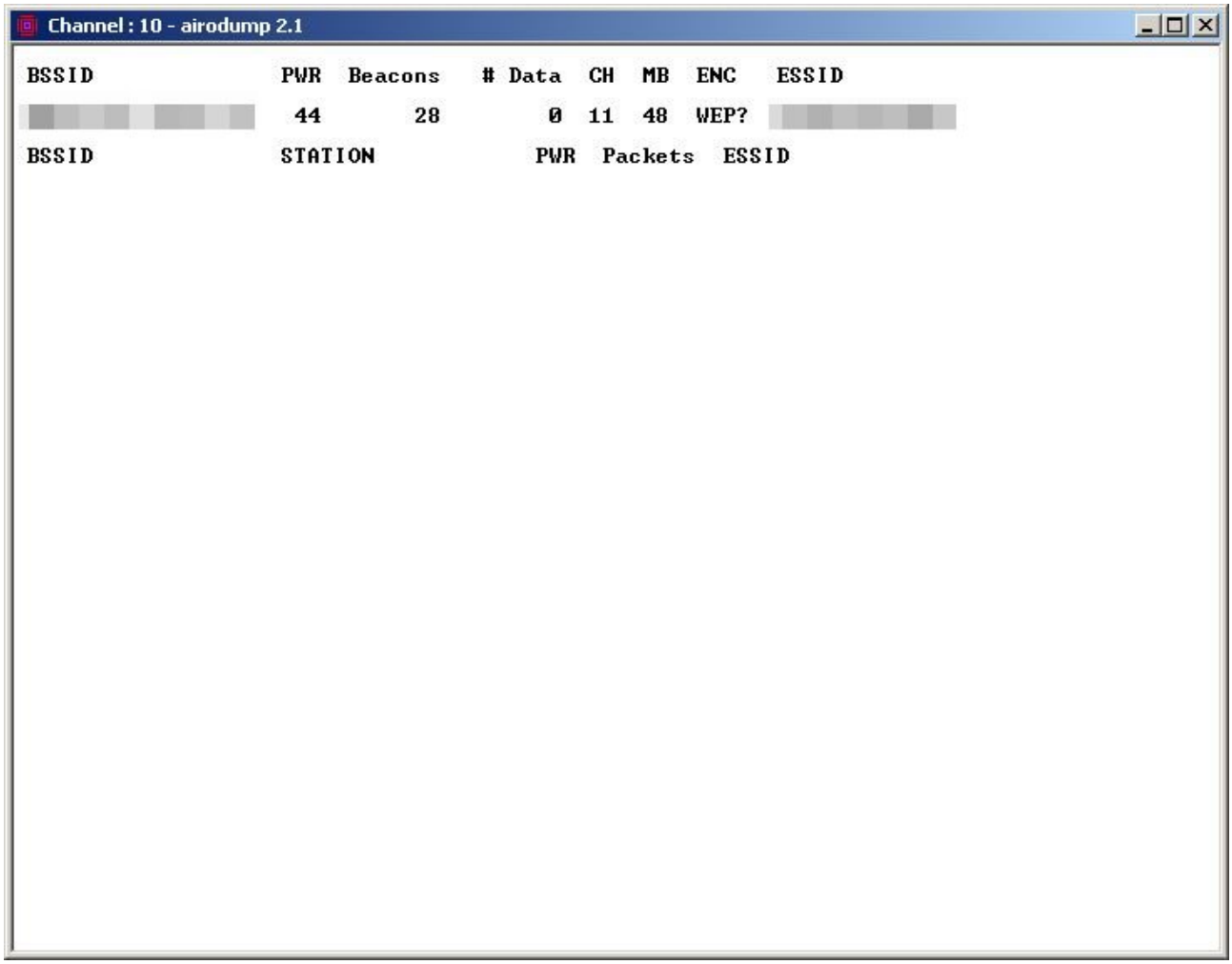
Je décide si mon fichier est destiné seulement dans l'optique d'un crackage de clé WEP.

Dans le cas présent, c'est le cas donc je répond **Y** (yes = oui)



Je répond **y** et j'appuie sur la touche **Entrée**.

Si tout c'est bien passé vous devriez Airodump qui lance l'écoute des ondes...



BSSID : Adresse MAC du point d'accès (connu sous la forme **XX:XX:XX:XX:XX:XX**).

CH : Canal utilisé (exemple : **11**).

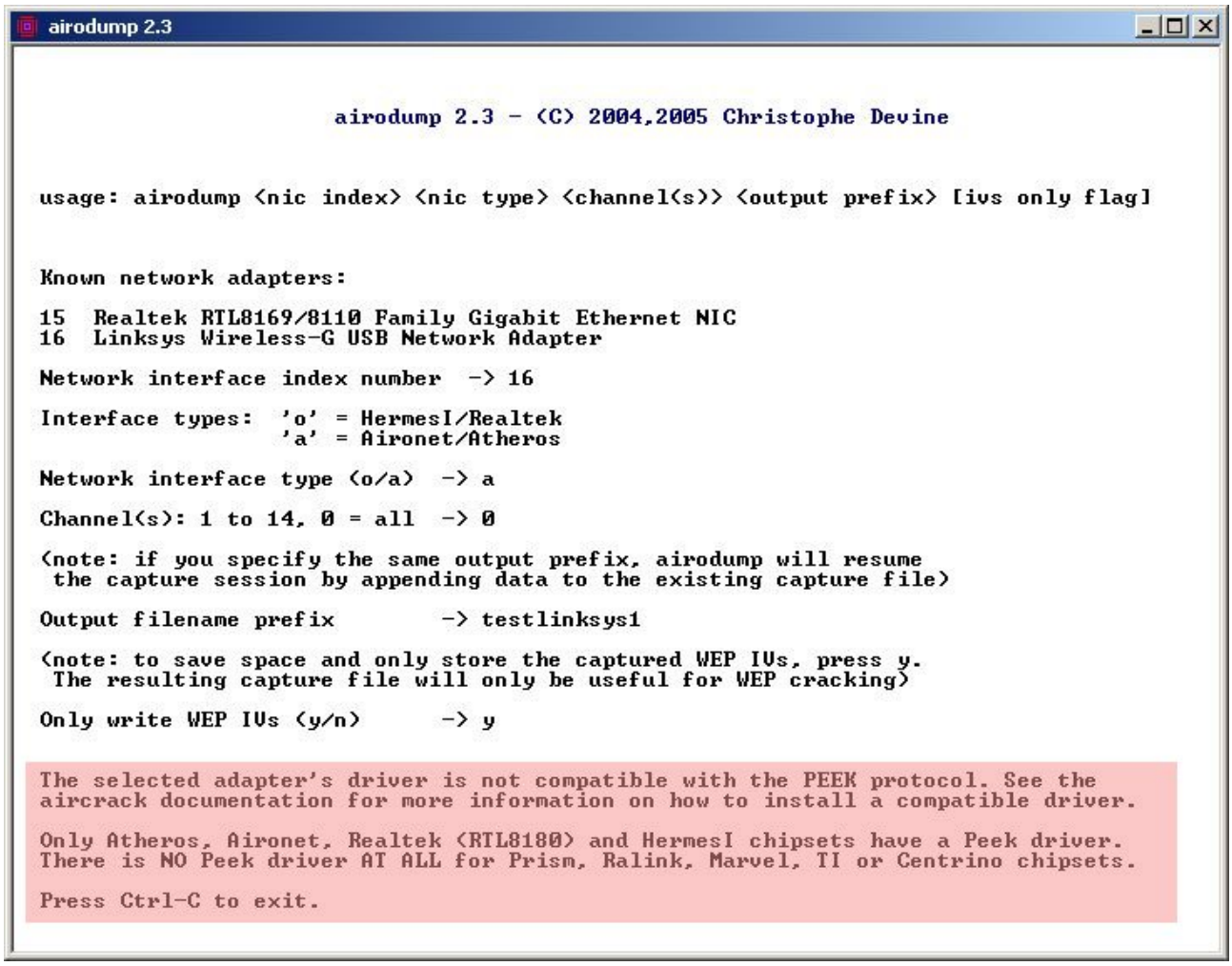
DATA : Nombre de paquet qui ont circulé sur le réseau.

ENC : Type de cryptage utilisé (dans le cas présent **WEP**).

ESSID : Nom du réseau sans fil (exemple : **WIFIDEMO**).

A retenir : les 3 informations nécessaires sont **BSSID, CH, ESSID**.

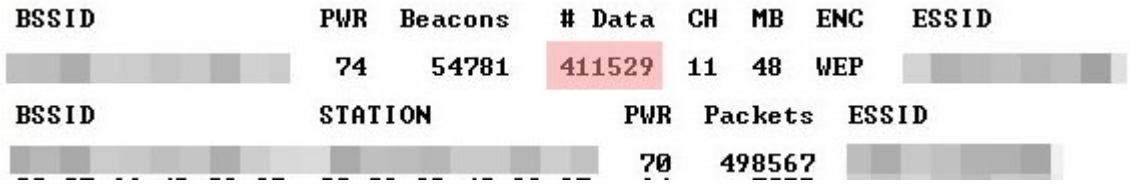
Si au contraire Airodump a affiché un écran similaire à celui ci-dessous :



Erreur que j'ai obtenu avec l'adaptateur usb Linksys.

Ceci signifie que l'adaptateur ou la carte wifi utilisée n'est pas compatible avec le protocole PEEK. Donc, il vous est conseillé d'installer un pilote adéquate pour cela.

Poursuivons, nous avons donc notre capture qui est en cours comme le montre notre capture ci-dessous :



Comme on peut le voir ici, j'ai déjà un peu plus de **400.000** paquets de récupérés.

Ceci étant, je suis encore loin du compte pour ce qui est de cracker une clé ayant une taille de **128bits**.

Pour décrypter une clé de **64bits**, j'ai besoin d'environ **300.000** paquets (ou IVs).
Pour décrypter une clé de **128bits**, j'ai besoin d'environ **1.000.000** paquets (ou IVs).

Ceci étant, si vous avez un réseau sans fil qui ne génére que peu de trafic cela peut prendre un bon moment avant d'atteindre la quantité de paquet adéquate.

A cela une solution, soit vous êtes patient... et vous laissez faire.

Soit vous utilisez un logiciel qui permet l'injection de paquet sur le réseau.

Sous windows, il y a 2 logiciels disponibles selon si vous utilisez une carte/adaptateur à base de chipset **Atheros** ou d'un chipset **Prism**.

Pour les cartes avec chipset **Atheros** :

CommView for WiFi de la société **Tamos**.

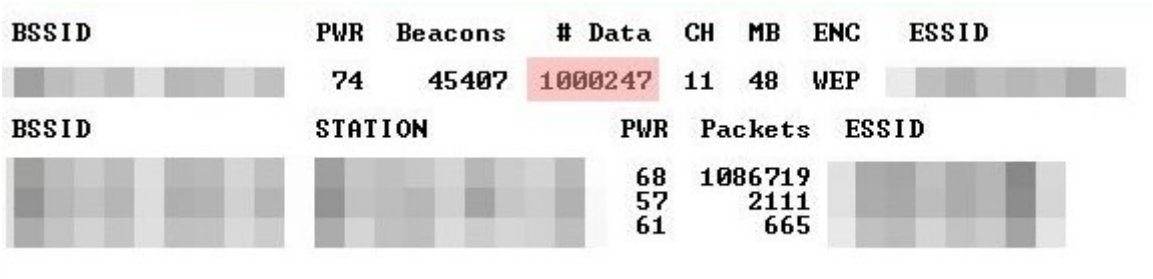
Site officiel : http://www.tamos.com/products/commwifi/

Pour les cartes avec un chipset **Prism** :

AirGobbler Packet Generator de la société **Tucasoftware**.

Site officiel : http://www.tuca-software.com/transmit.php

Pour ma part, au vu du fait que j'étais sur mon réseau personnel, j'ai procédé à quelques transferts de fichiers afin de me permettre d'atteindre le minimum d'un million de IVs capturés.

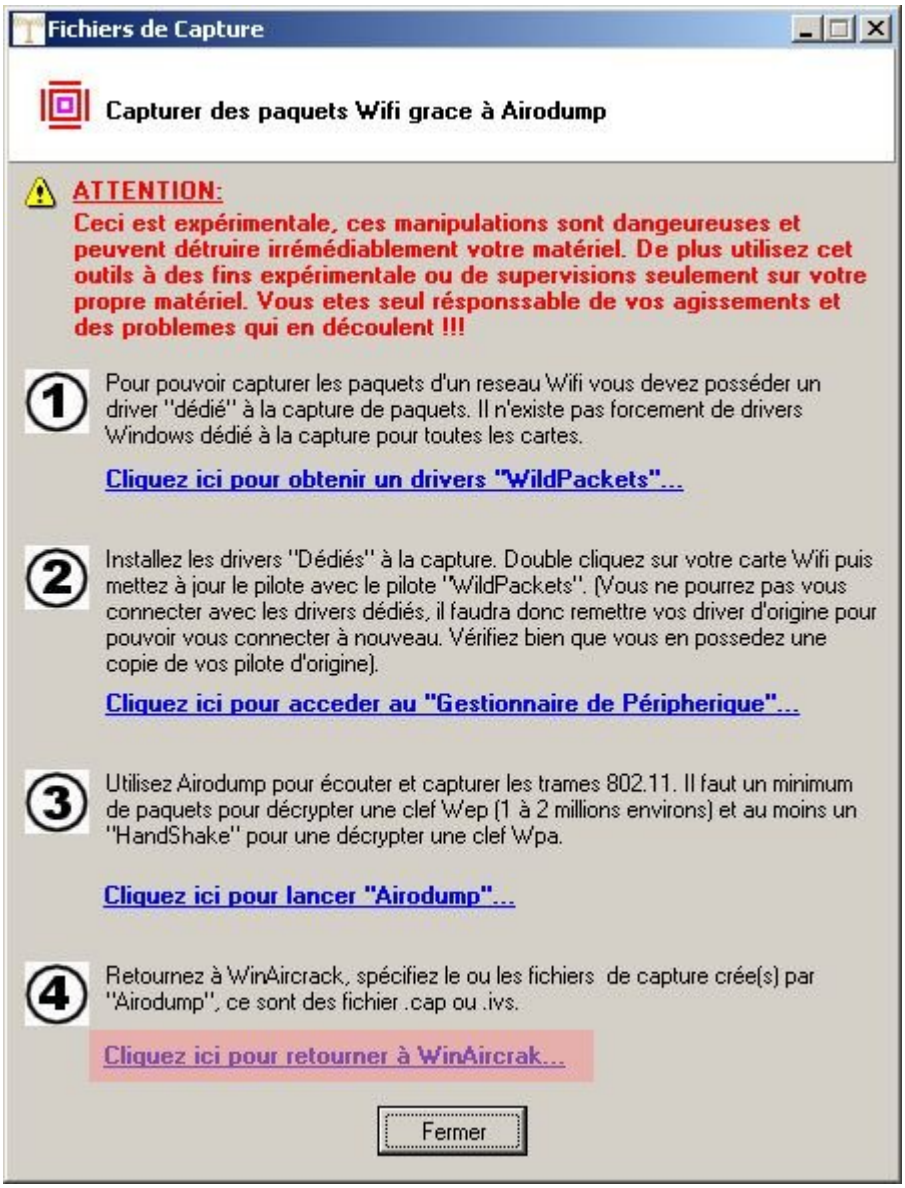


1 millions de paquets capturés.

Ceci étant, j'ai pu commencer à lancé le calcul de la clé tout en continuant à capturer de nouveau paquet.

Donc, tout en concernant ma fenêtre **Airodump** ouverte, je suis retourné dans WinAircrack.

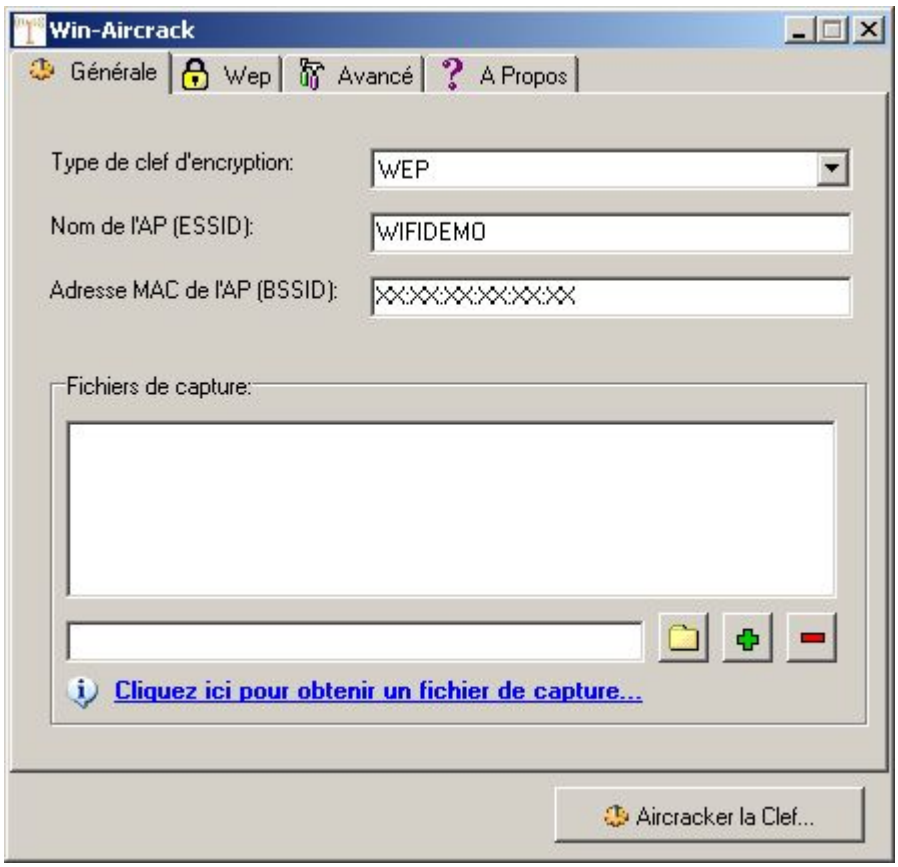
Pour ce faire, on clique sur le lien « Cliquez ici pour retourner à WinAircrack » dans la fenêtre « Fichiers de Capture ».



Ceci ayant l'avantage de permettre le retour dans le programme tout en laissant la fenêtre de Airodump ouverte.

Une fois de retour dans Winaircrack, et souhaitant commencer le décryptage de la clé WEP.

Je dois fourni les informations suivantes dans la fenêtre de l'onglet **Générale** :



Type de clef d'encryption : WEP (par défaut).

Nom de l'AP (ESSID) : ici, j'ai mis **WIFIDEMO**.

Adresse MAC de l'AP (BSSID) : **XX:XX:XX:XX:XX:XX**

Par ailleurs, je dois fourni le fichier ou les fichiers de capture qui font être utiliser pour le crackage de la clé.

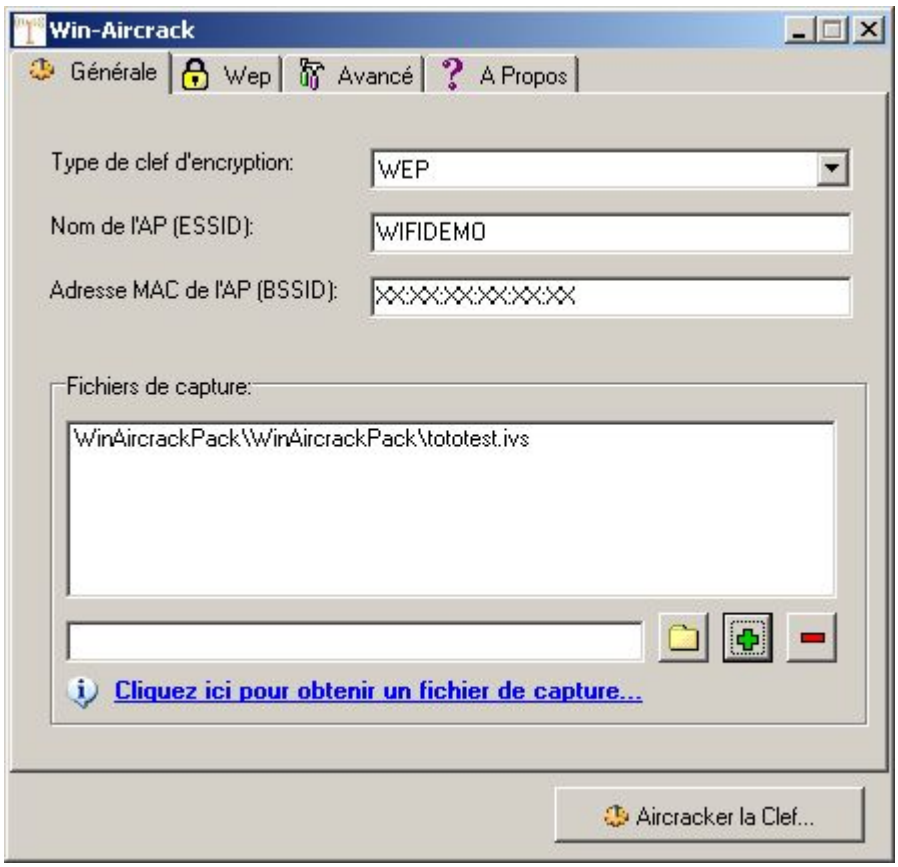
Pour ce faire, je clique sur le bouton 

Puis on choisi le fichier portant l'extension **.ivs** qu'on va utiliser, attention, par défaut, c'est l'extension **.cap** qui est sélectionnée. Et l'on clique sur **Ouvrir**.

Et pour finir on clique sur le bouton 

Pour ajouter notre fichier à la liste des fichiers de capture.

Vous devriez avoir un résultat similaire à celui-ci :



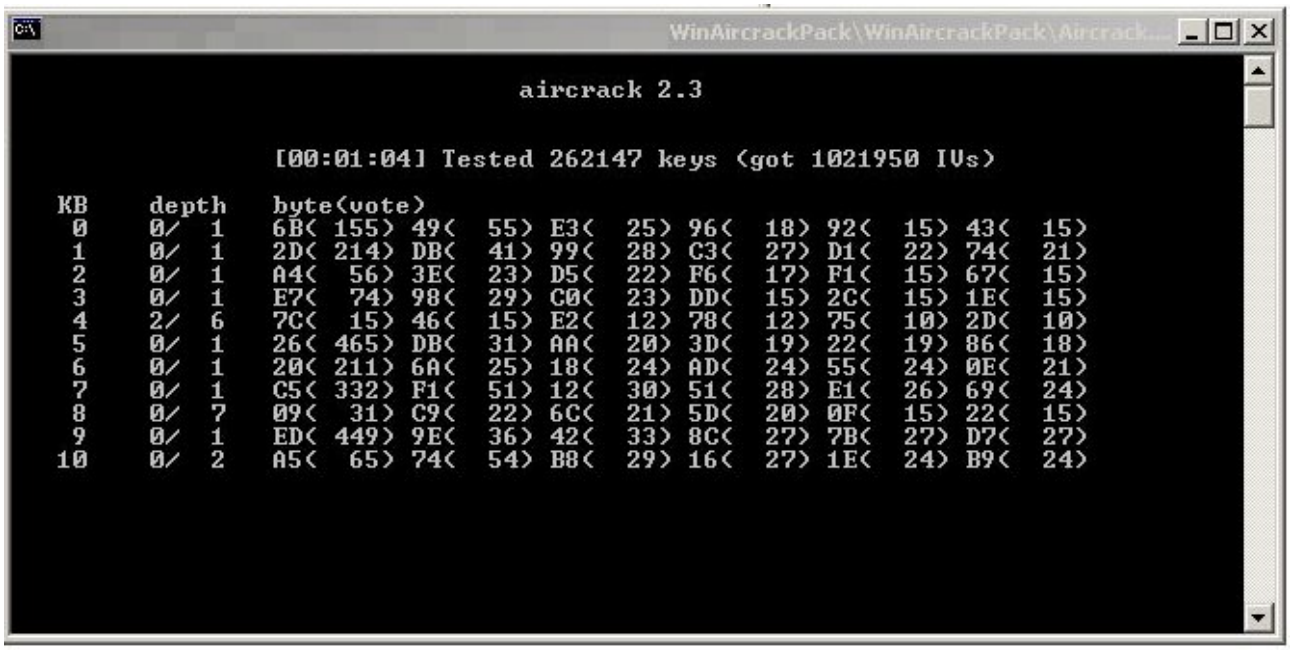
Si vous souhaitez supprimer de la liste des **Fichiers de capture** un fichier,

Vous appuyez sur le bouton 

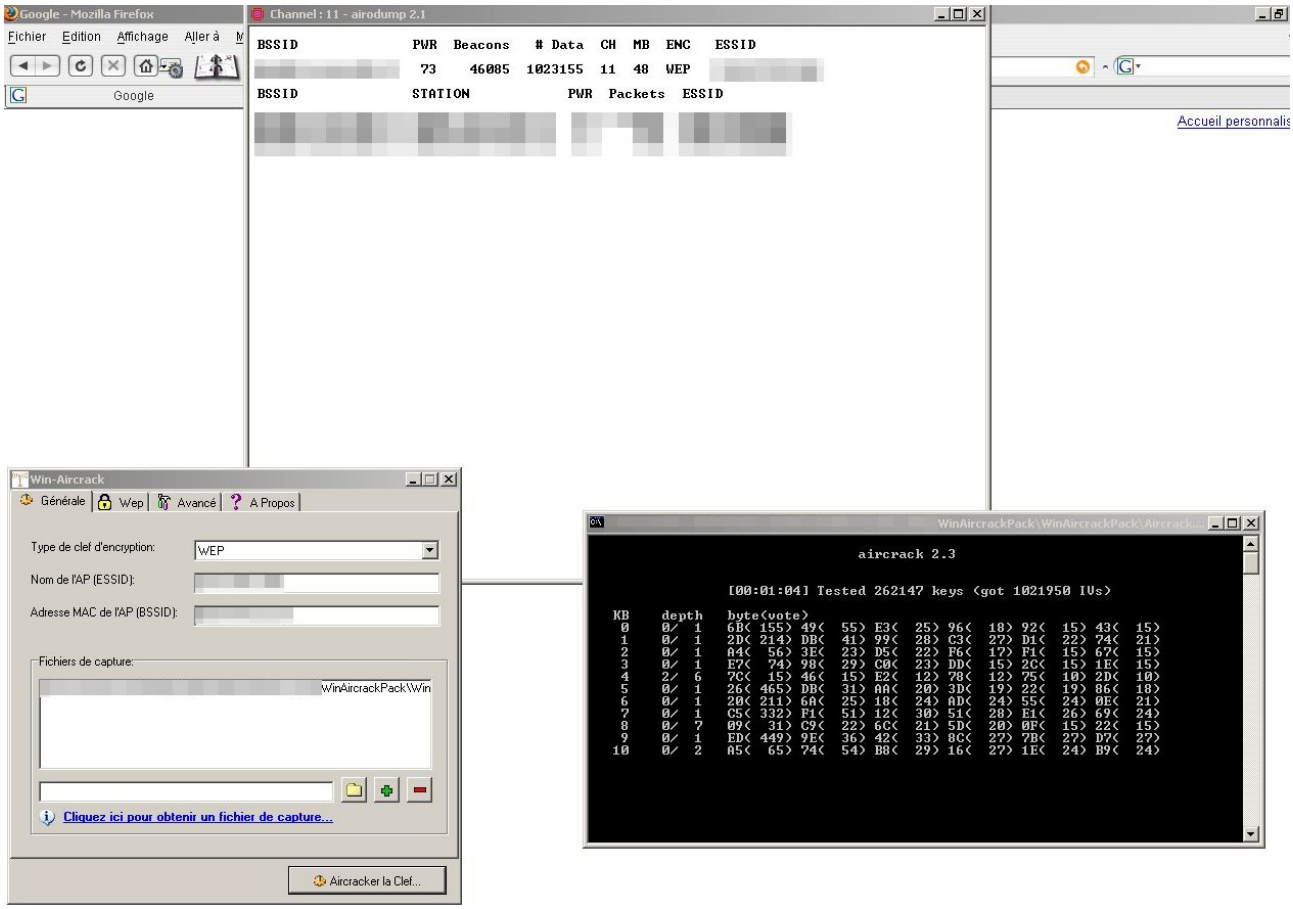
Ceci étant, nous pouvons à présent lancé le programme Aircrack qui va nous permettre la découverte de la clé WEP.

Pour ce faire on clique sur le bouton 

Ce qui aura pour effet de lancé une fenêtre comme celle-ci :



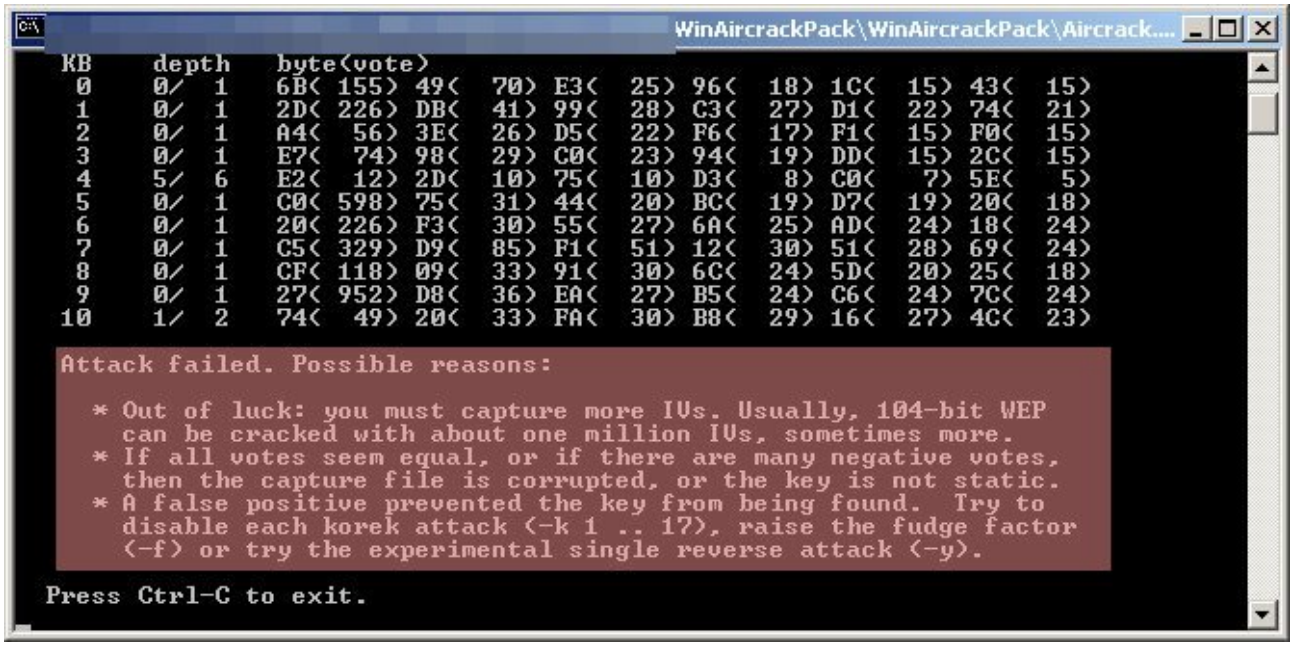
Comme nous pouvons le voir, le fichier de capture contient **1.021.950 IVs**.



Airodump en haut entrain de capturé, aircrack à droite entrain de décrypté.

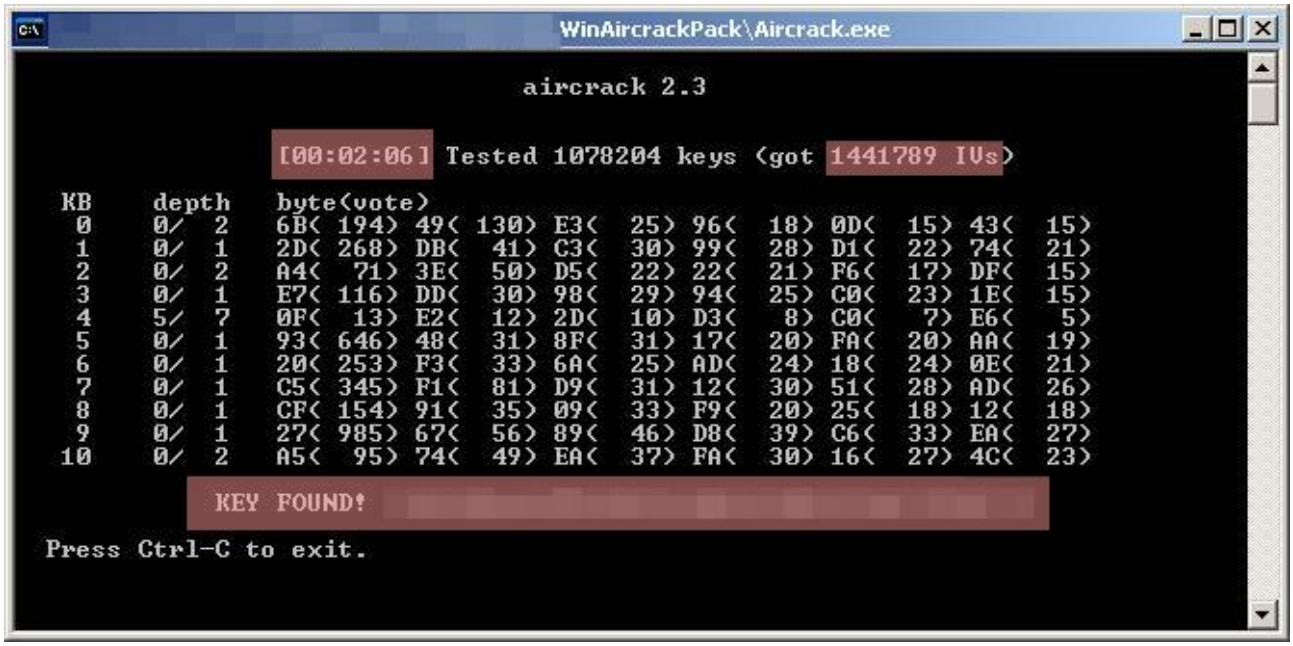
Après un moment plus ou moins long que vous aurez occuper à d'autres choses, nous pouvons avoir **2** réponses pour le décryptage de la clef WEP.

Soit tout d'abord **une mauvaise nouvelle**...



Dans ce cas, il n'y a pas un nombre conséquent de **IV**s... donc, il faut continuer à écouter le réseau.

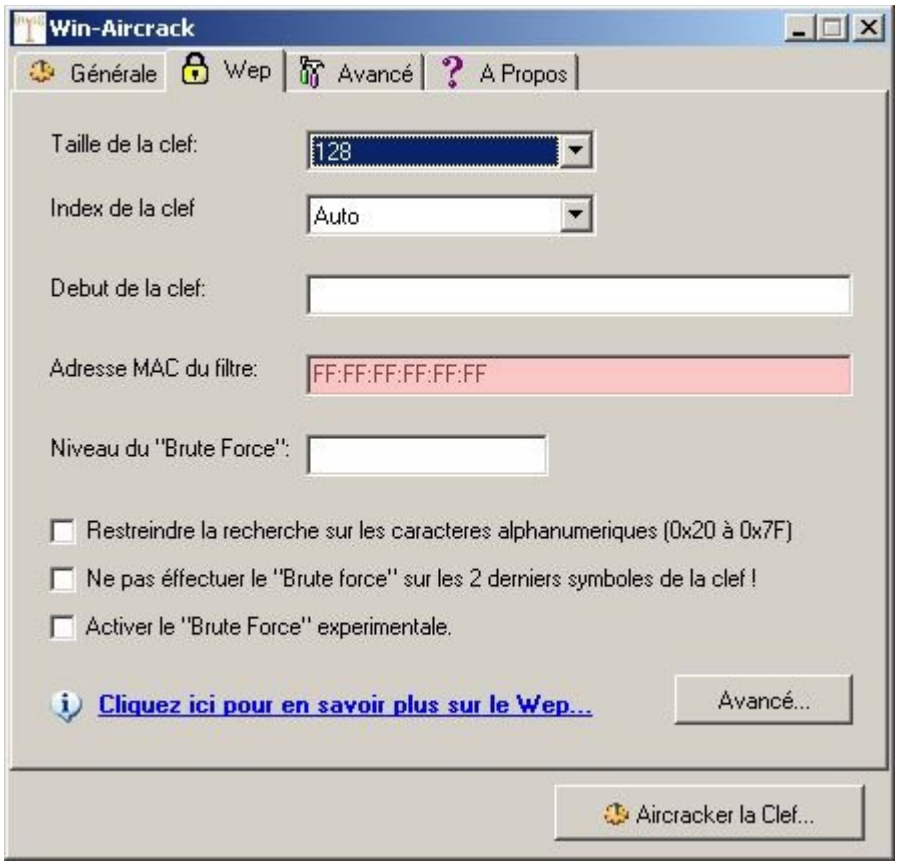
Soit **la réponse est positif**, c'est le bonheur...



KEY FOUND ! Pas de doute...

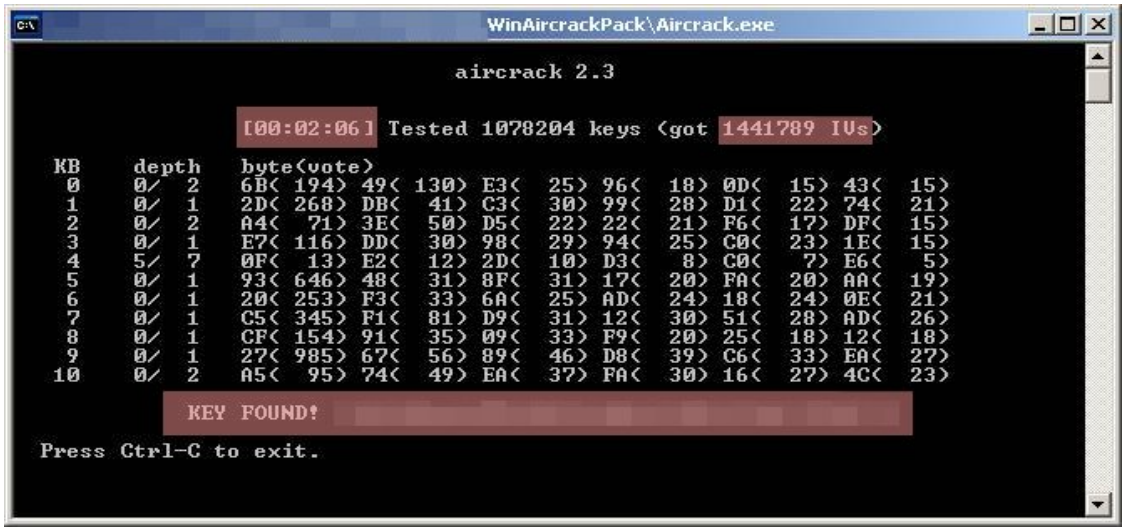
A noter que dans mon cas, la première réponse fût négatif, nombre de paquet insuffisant.

Par ailleurs, j'ai activé une option dans l'onglet **Wep**...



J'ai mis l'adresse **MAC du filtre**.

Ce qui à permis la découverte de la clef WEP en **2 minutes 06 secondes** sur un portable doté d'un **Pentium IV à 2 Ghz** avec un total d'un peu plus de **1.400.000 IVs**.



On note la clef WEP dans un coin du bureau.

Voilà, si tout c'est bien passé pour vous aussi vous devriez avoir découvert votre clef WEP.

On peut quitter à présent Airodump et Aircrack en pressant les touches **CTRL et C** simultanément.

Ceci étant maintenant qu'on a la clef WEP du réseau sans fil, on va souhaiter établir une connexion sur ce dernier.

1 : le réseau auquel on veut se connecter est en DHCP, dans ce cas l'IP me sera fourni et par ailleurs, il n'y pas de reconnaissance d'adresse MAC.

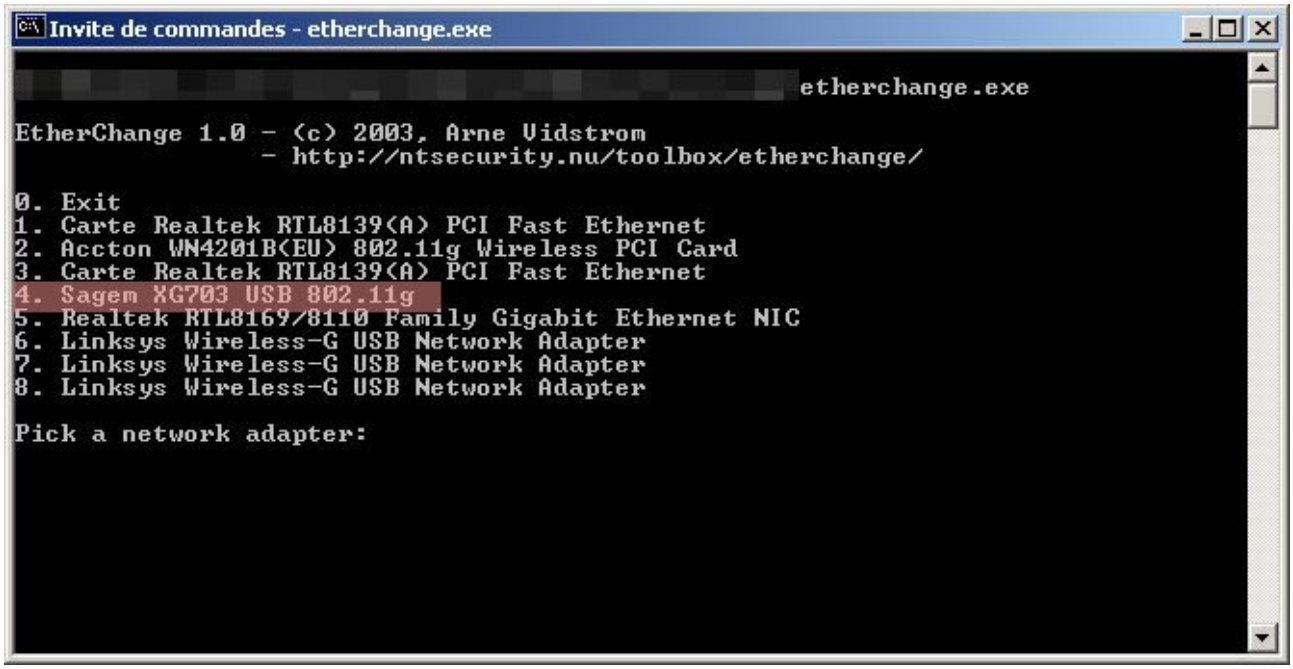
2 : le réseau auquel on veut se connecter est en DHCP, mais une reconnaissance de l'adresse MAC du client est activé.

3 : le réseau auquel on veut se connecter est en IP fixe, dans ce cas, il faut déterminé la plage IP utilisée par le réseau. Par ailleurs, il n'y pas de reconnaissance d'adresse MAC.

4 : le réseau auquel on veut se connecter est en IP fixe, dans ce cas, il faut déterminé la plage IP utilisée par le réseau. Par ailleurs, il y a une reconnaissance d'adresse MAC.

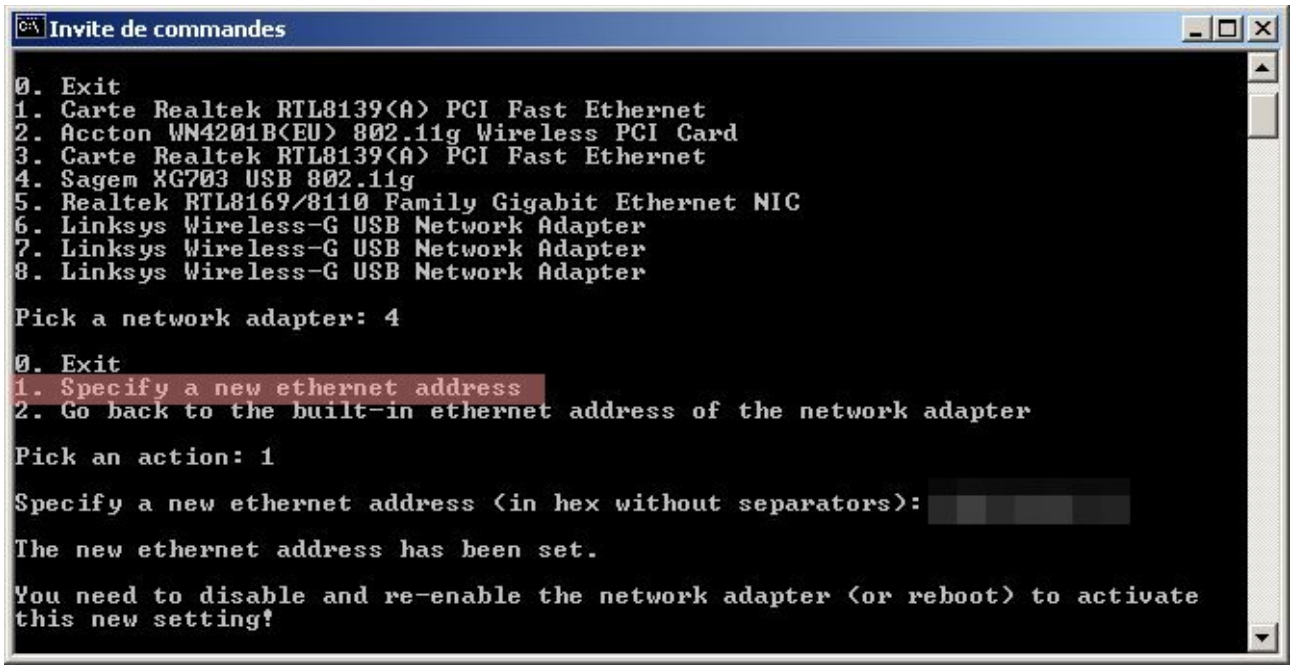
Pour changer votre adresse MAC vous pouvez utilisé le programme EtherChange qui est disponible à l'url suivante :

http://ntsecurity.nu/downloads/etherchange.exe



EtherChange en action...

L'adresse MAC que j'ai ainsi créé sera actif mais avant il me faudra désactivé la carte ou l'adaptateur pour prendre en compte la nouvelle adresse MAC.

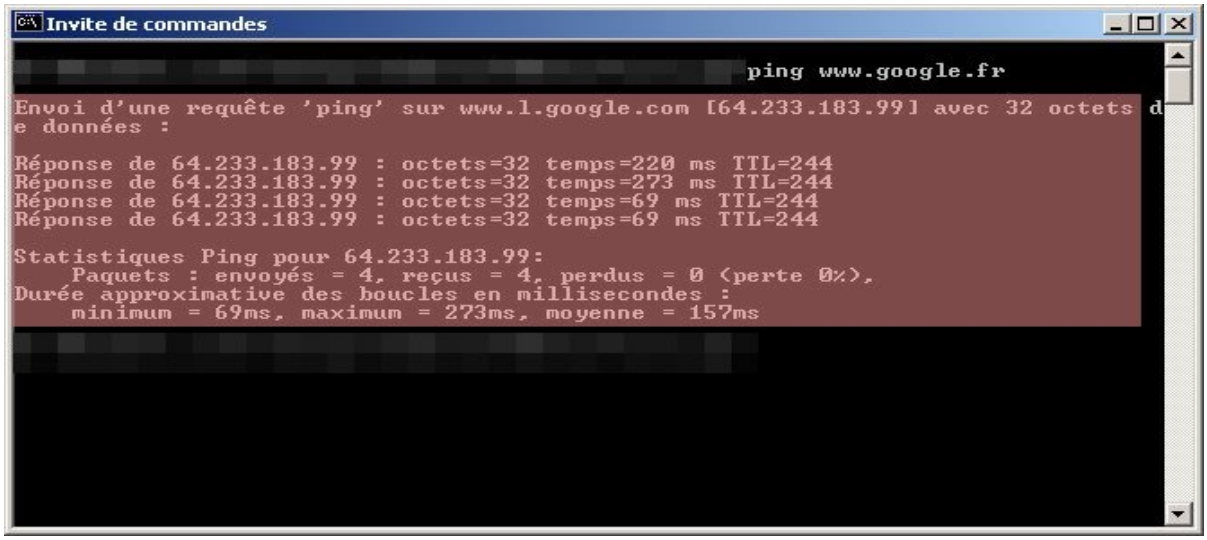


Vous devez rentrer l'adresse MAC sans les séparations « **:** » c'est-à-dire comme ceci :

XXXXXXXXXXXX

Si vous souhaitez restaurer l'adresse MAC d'origine de la carte, rien de plus simple, choisissez le menu **2** « Go back to the built-in ethernet address of ther network adapter », n'oublier pas de désactivé cette dernière pour activé à nouveau l'ancienne adresse MAC.

Pour ma part j'ai juste eu à **remplacer l'adresse MAC** de mon adaptateur usb pour obtenir une connexion au réseau sans fil au vu du fait que le **DHCP était activé**.



L'adresse MAC que j'ai utilisé avait été noté dans le fichier de capture lors de l'écoute du réseau. Pour ce faire jeter un oeil au fichier portant le même nom que votre fichier **.ivs**.

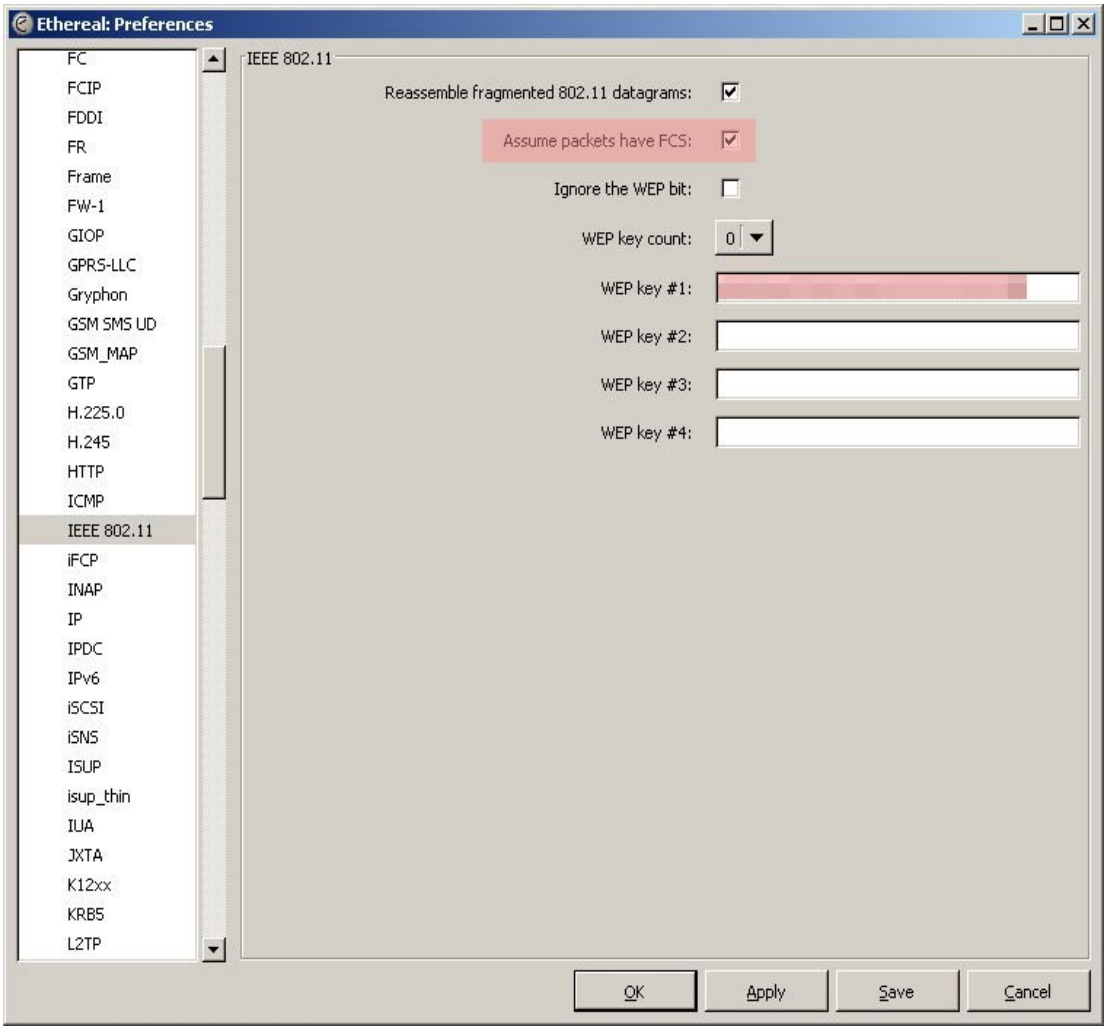
Si vous êtes dans la situation où **le DHCP n'est pas activé ou il y en a pas**, et donc où il va falloir déterminé **l'adressage du réseau**.

Pour ce faire, nous allons avoir besoin d'un sniffer de réseau... **Ethereal** est bon dans ce domaine.

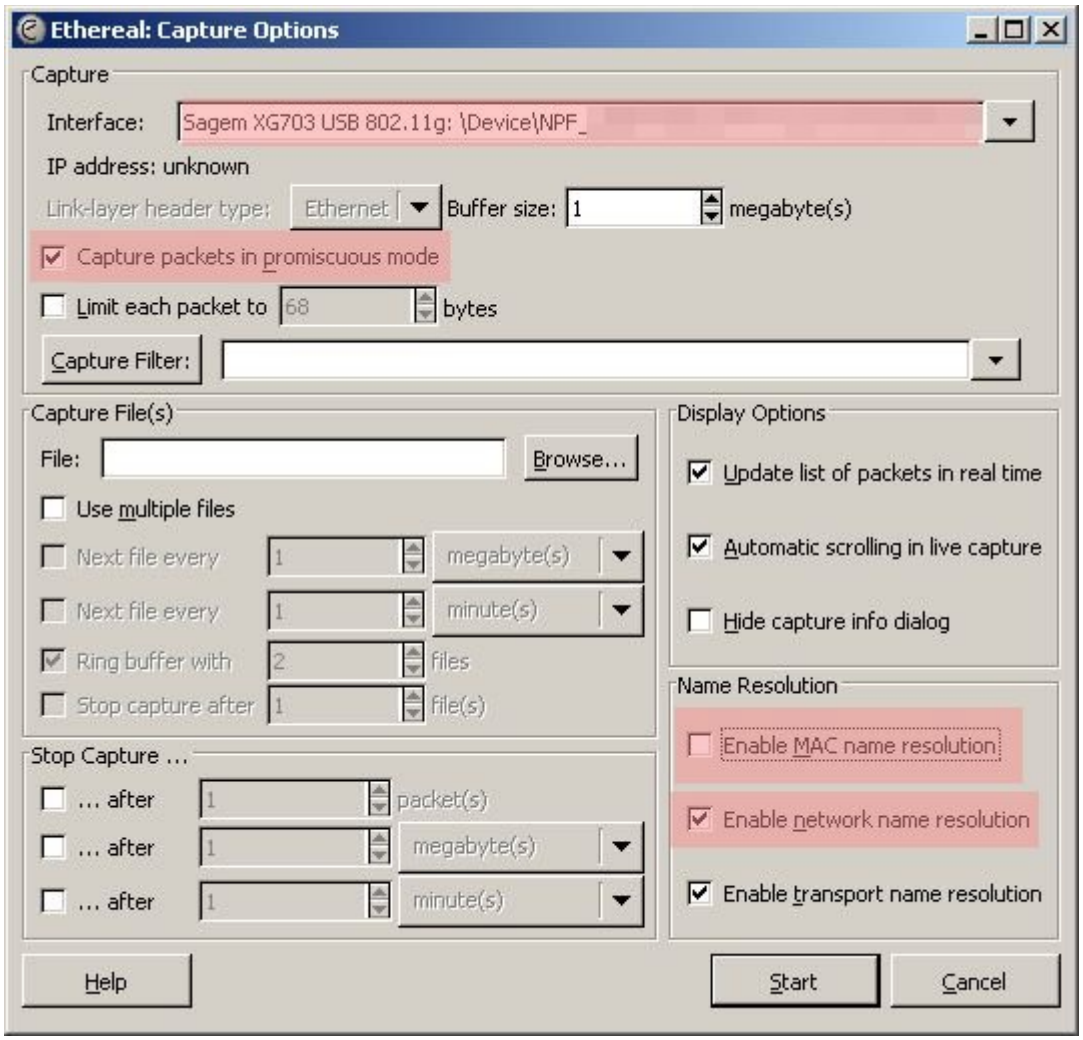
Site officiel : http://www.ethereal.com

Une fois Ethereal installé si ce n'est déjà fait. Lancer Ethereal est aller dans le menu **Edit / Preferences,** dans la section **Protocol** puis **IEEE 802.11**, là vous allez rentré la clef WEP qu'on a découvert.

Cochez tout d'abord « Assume packets have FCS »... puis au niveau WEP key #1 rentrer la clef.



Cliquer sur le bouton **OK**.



Là, aller dans le menu **Capture** / **Options** et configuré comme ceci :

Choisissez l'interface réseau qui va être utilisée, ici la clef Sagem.

Cochez « **Capture packets in promiscuous mode** » si ce n'est pas déjà fait.

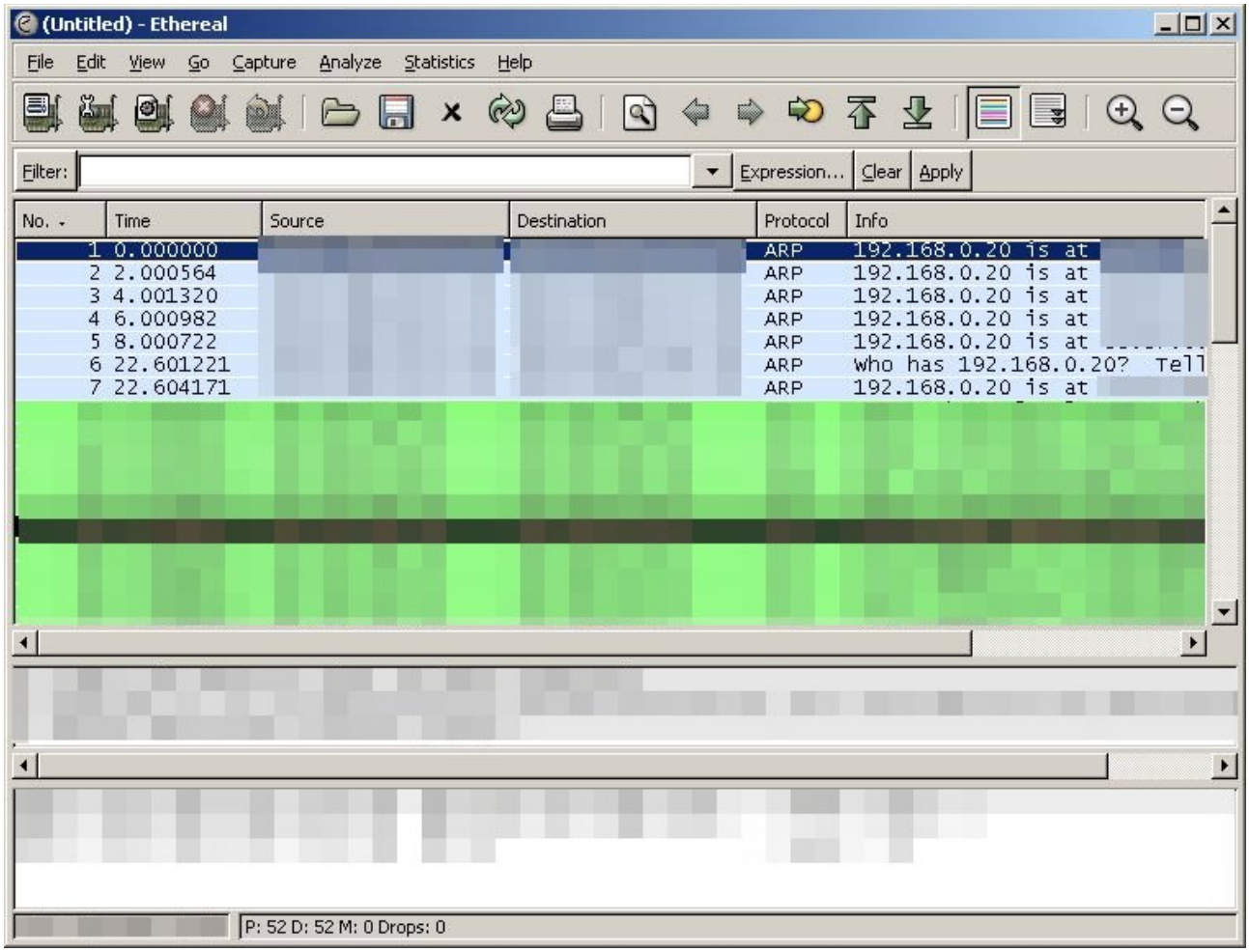
Décochez « **Enable MAC name resolution** ».

Cochez « **Enable network name resolution** ».

Vérifier qui « **Update list of packets in real time** » et « **Automatic scrolling in live capture** » soit bien cochés.

Puis lancer la capture en cliquant sur le bouton **Start**.

Vous devriez avoir tout un tas de requête, vous permettant d'identifier l'adressage du réseau.



Un filtre qui vous permettra de trouver les requêtes intéressantes dans le cas présent est :

(wlan.bssid == bssid de l'ap) && (TCP)

Requête que vous rentrez dans le champs **Filter**.

Dans le cas présent, l'IP du point d'accès est **192.168.0.20**

De là, il le ne reste plus qu'à faire la connexion au réseau muni d'une part le **la clef WEP** et d'autre part d'une **IP valide pour le réseau**.

Note : Dans bien des cas l'adressage est soit 192.168.0.x ou 192.168.1.x C'est le type d'adressage utilisé le plus fréquemment sur le matériel de réseau sans fil.

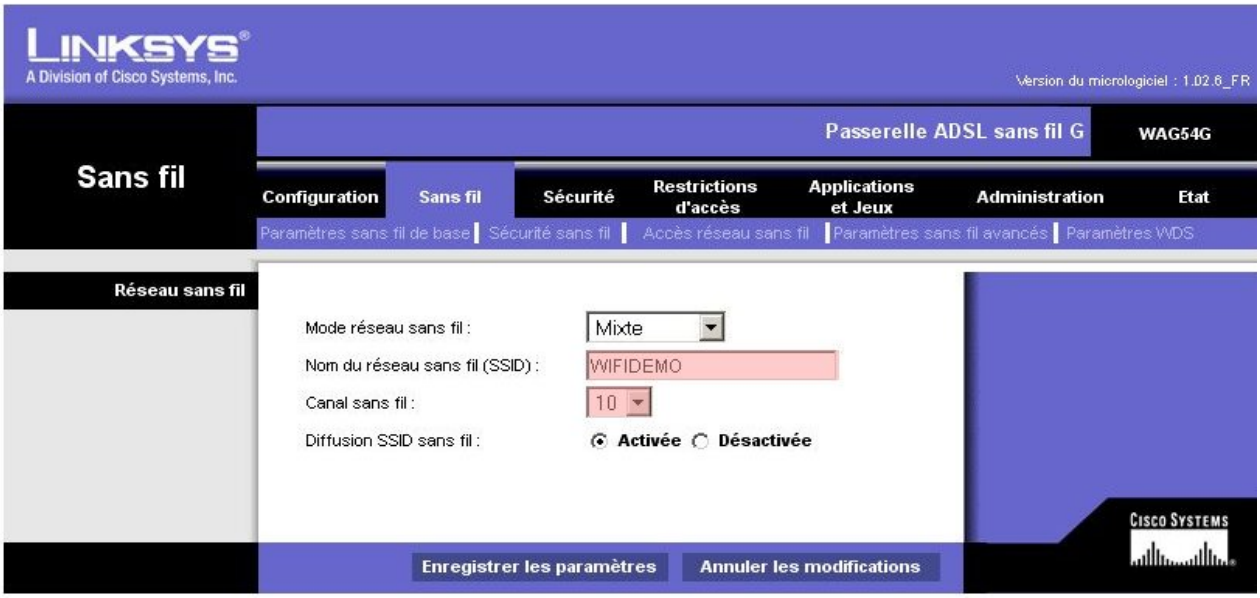
Décryptage d'une clef WPA-PSK :

Pour faire suite au décryptage de la clef WEP, j'ai voulu faire le test du décryptage d'une clef WPA-PSK. Vous trouverez la description de ce qu'est une clef WPA sur le lien suivant: http://fr.wikipedia.org/wiki/WPA

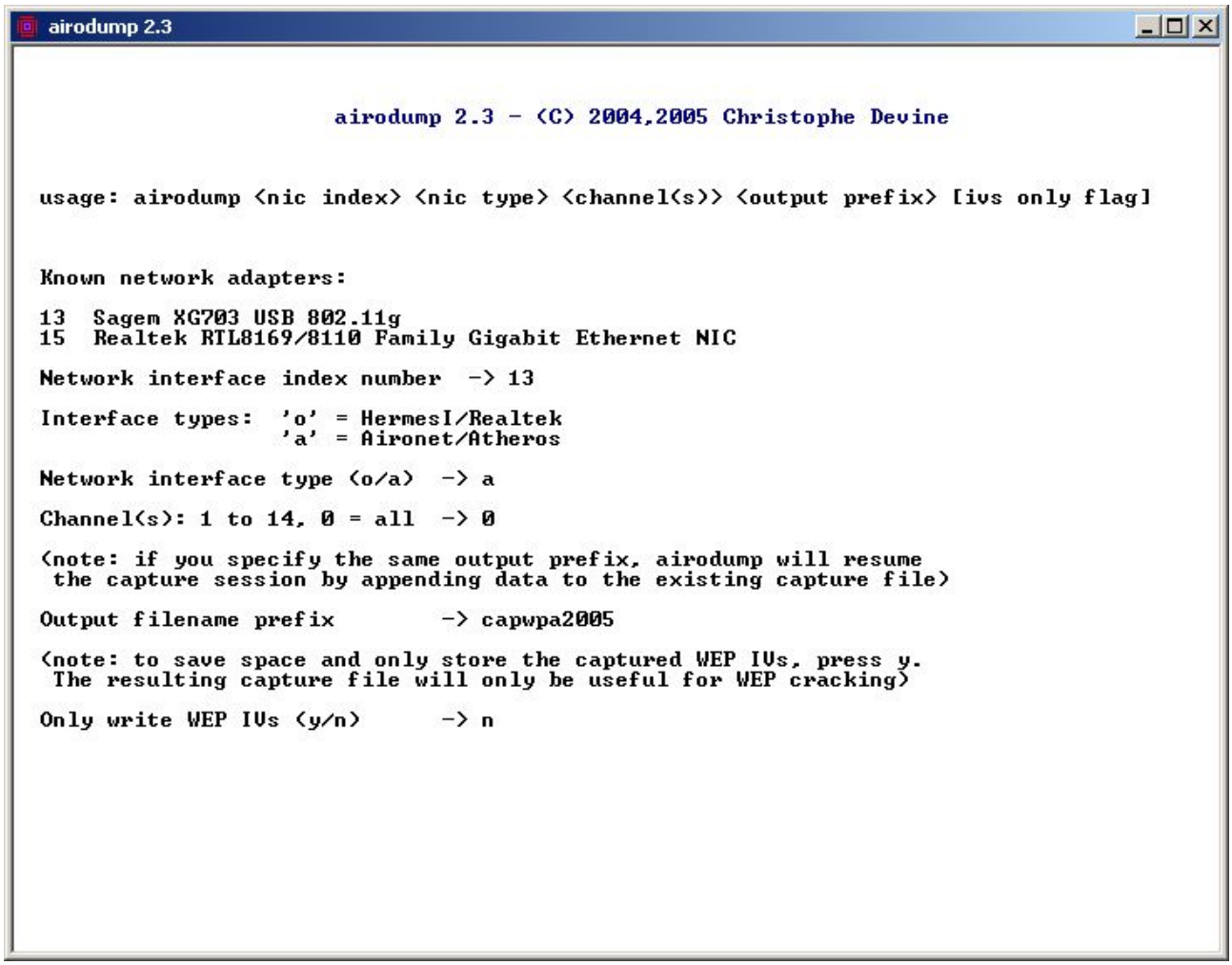
Ceci étant, j'ai configuré un **Linksys WAG54G** via la page d'administration web qui est disponible à l'IP 192.168.1.1.

SSID : **WIFIDEMO -** Canal sans fil : **10 –** Mode sécurité : **Clé WPA pré-partagée**

Algorithme WPA : **TKIP –** Clé pré-partagé WPA : **W0I1F2I3D4E5M6O**



Ceci fait, j'enregistre les changements puis je me tourne vers WinAircrack pour commencer le travail. Tout d'abord je fais la configuration de airodump.

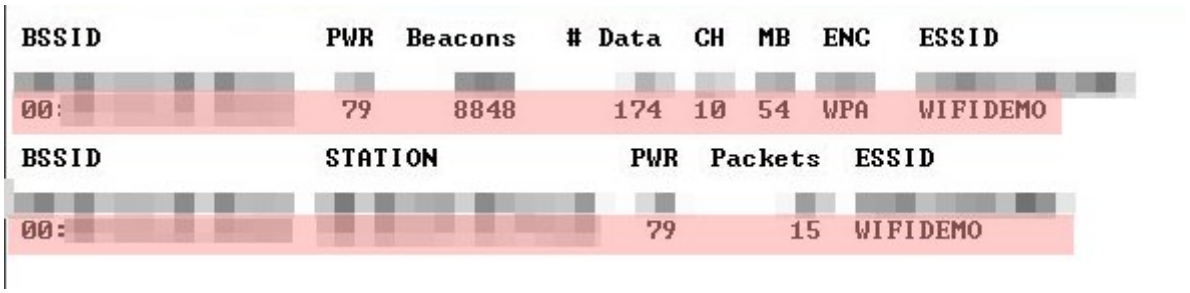


Une information change par rapport à la configuration que j'avais fait pour une capture pour le WEP. Ici à la question « **Only write WEP IVs (y/n)** », j'ai répondu **n** (no=non).

Ce qui aura pour effet d'enregistrer toute les données... en conséquence mon fichier de capture sera **d'une taille plus volumineuse**. Dans mon cas, à la fin de la capture, le fichier présenté une taille de **1.4 Go** pour **2.7 millions paquets**. Par ailleurs, l'extension sera **.cap** et non **.ivs** comme précédemment avec le WEP.

La configuration faite, j'ai mis en route la capture...

Ici, j'ai le point d'accès que j'ai configuré tout-à-l'heure (**WIFIDEMO**). On voit qu'il utilise le cryptage **WPA** et qu'il communique sur la canal **10.**



Etant dans un réseau wifi fonctionnant pour l'occasion et donc susceptible de ne pas générer beaucoup de trafic, j'ai utilisé tout d'abord le logiciel AirGobbler Packet Generator de la société Tucasoftware dont j'avais parlé au cours de la partie concernant le WEP.

Ce logiciel m'a permis de générer du trafic, mais quelques minutes plus tard, j'ai eu l'idée d'utiliser le logiciel iperf qui d'ordinaire permet de tester la bande passante exploitable sur un réseau.

IPERF est disponible à l'url suivante : http://www.noc.ucf.edu/Tools/Iperf/

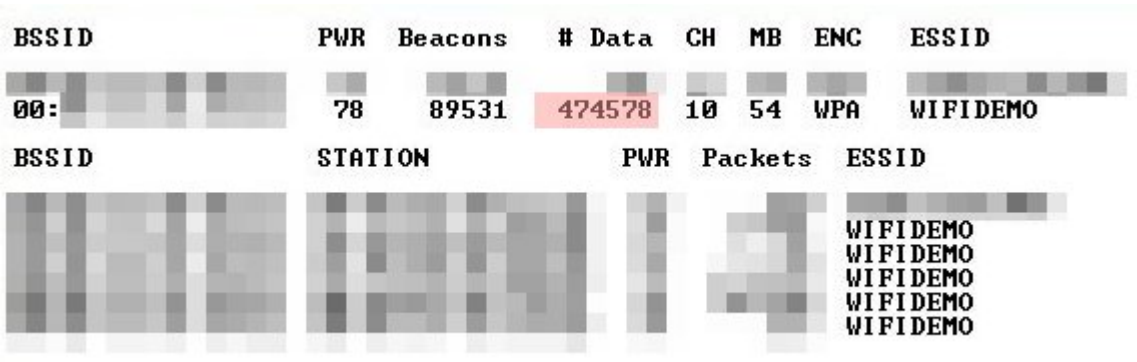
Donc, j'ai utilisé d'une part **en tant que serveur** sur un poste et **en tant que client** sur l'autre poste.

iperf côté serveur : **iperf -s**

iperf côté client : **iperf -t 1000 -c 192.168.1.100**

-t = 1000 Mo soit 1 Go de données en transfert

Ceci permet mis donc de générer rapidement un nombre de paquets conséquents après quelques minutes de transfert.



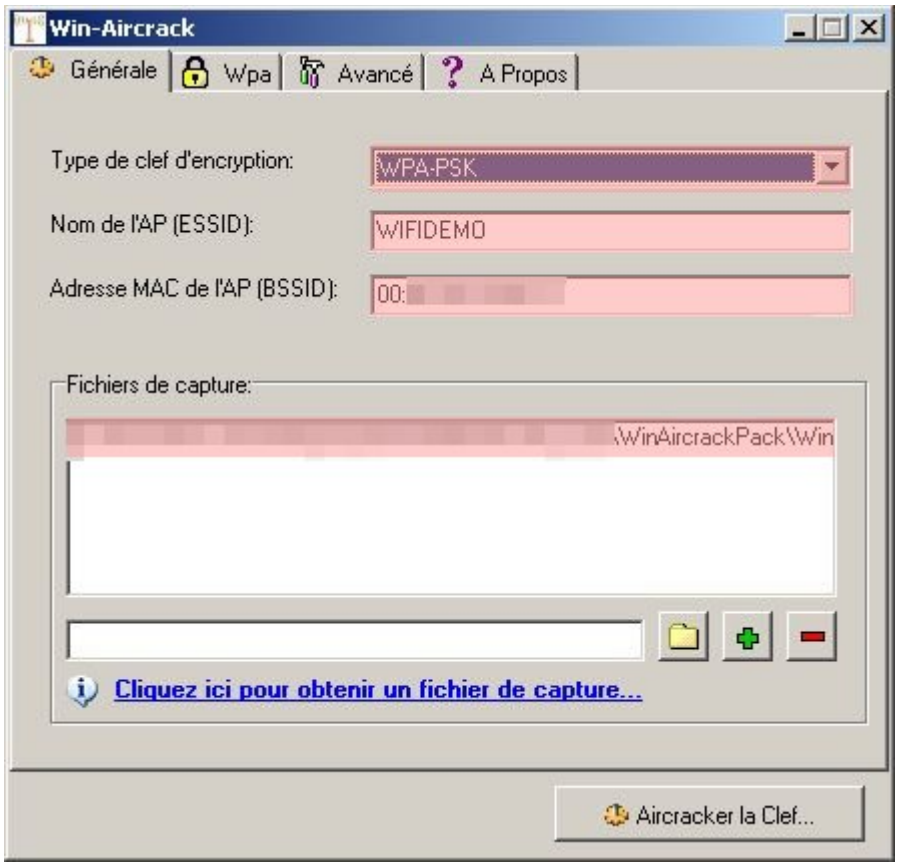
Un peu plus de 400.000 paquets..

Après 20-30 minutes, j'arrive au nombre paquet minimum requis pour une clé de ce type.

Un peu plus de 1 Millions de paquets.

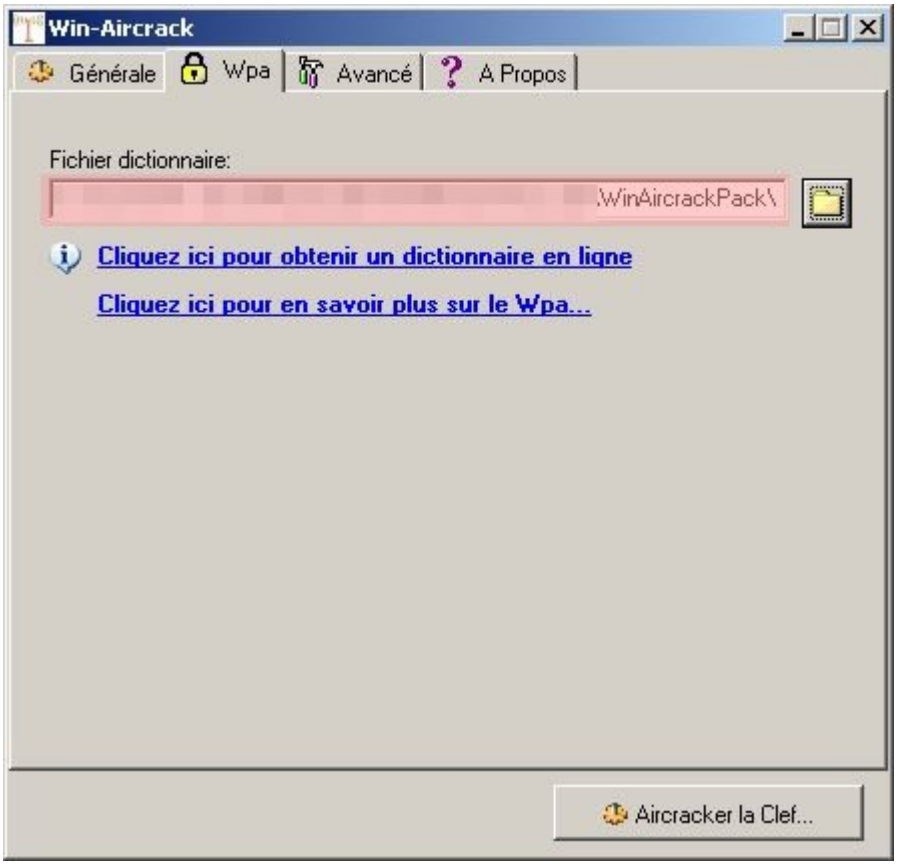
Ce qui dans l'absolu était un bon début pour commencer en parallèle le décryptage de la clef WPA-PSK. Donc, je suis retourné à WinAircrack.

Là, j'ai choisi le type de clef d'encryption, dans le cas présent **WPA-PSK**, j'ai rentré le ESSID (**WIFIDEMO**) ainsi que le BSSID (**XX:XX:XX:XX:XX:XX**). Par ailleurs, j'ai choisi le fichier de capture que j'allais utilisé.



Pour ajouter le fichier de capture : on clique sur le bouton  puis sur le bouton  .

De là je me suis rendu dans la fenêtre de l'onglet **WPA** pour ajouter un dictionnaire qui va servir pour cracker la **Passphrase** que j'ai mis lors de la configuration de mon Linksys.



Les dictionnaires ne sont pas livrés avec WinAircrack mais part contre le lien « **Cliquez ici pour obtenir un dictionnaire en ligne** » est disponible.

Une des url's où l'on trouve des dictionnaires est là suivante :

http://ftp.se.kde.org/pub/security/tools/net/Openwall/wordlists/

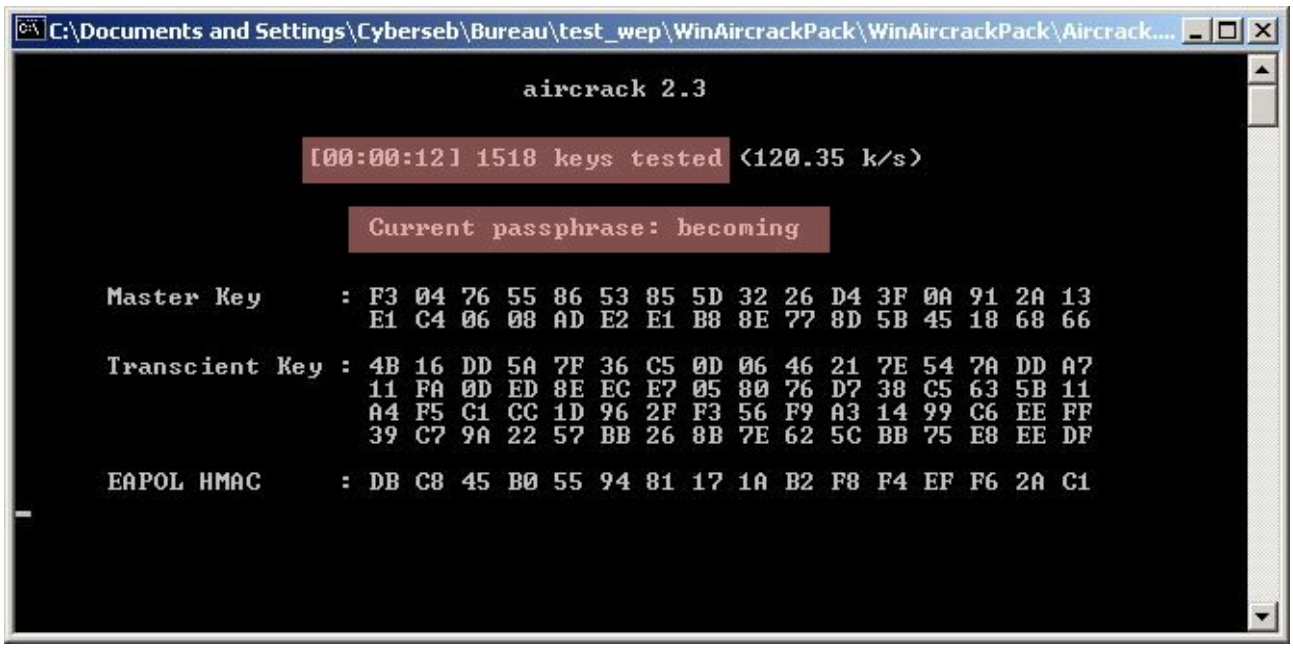
Pour ma part, j'ai téléchargé le dictionnaire complet (11 Mo) portant le nom de « all.tgz », donc le contenu est un fichier **all.lst** (42 Mo), ceci étant vous trouverez un dictionnaire pour de multiples langues ainsi que des dictionnaires spécifiques.

Une fois mon dictionnaire choisi, j'ai pu lancé Aircrack...

En cliquant sur le bouton 

Pour information, la Passphrase peut avoir une taille comprise entre **8** à **63** caractères. Le dictionnaire **all.lst** contient plus de **4 millions de mots**.

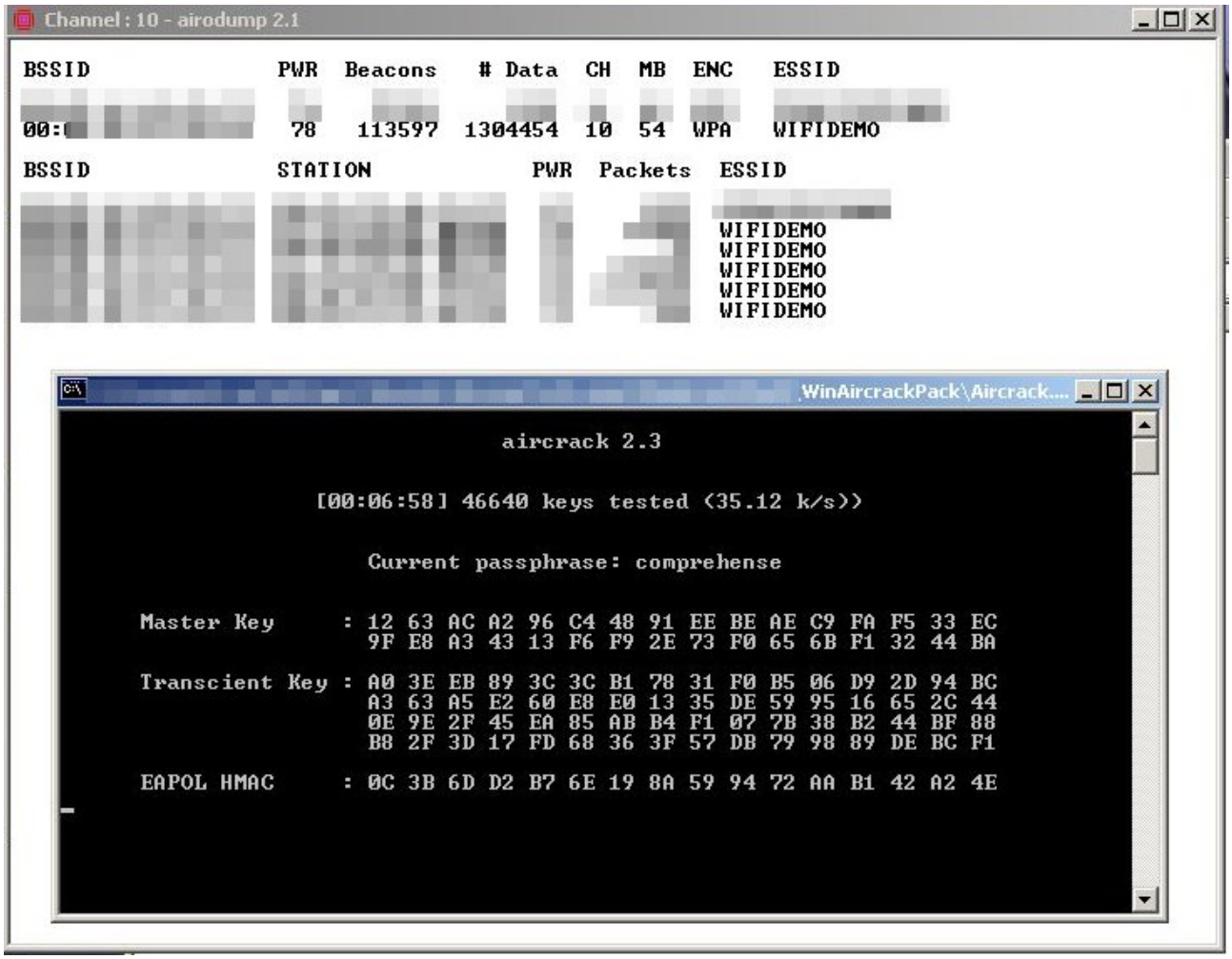
Aircrack en cours...



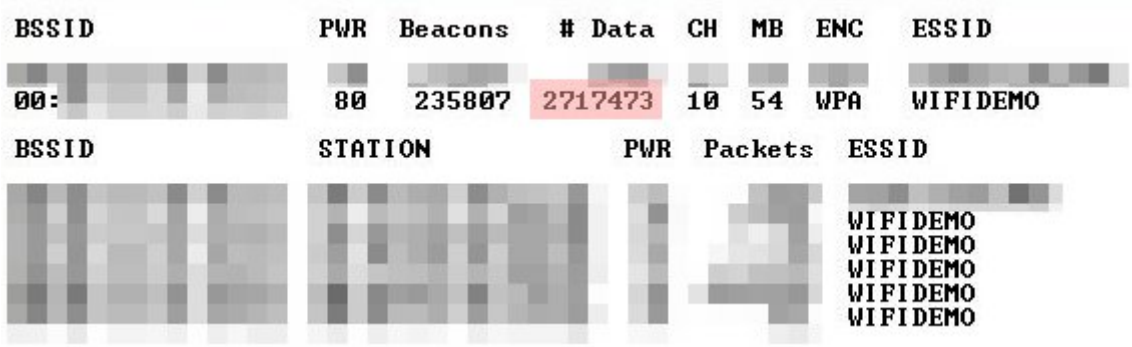
Nous voyons le temps passé ainsi que le nombre de clef testé. Par ailleurs, nous avons la Passphrase (**current passphrase**) qui est actuellement testé.

Il faut savoir que dans le décryptage du Passphrase d'un encryptage de type WPA-PSK... cela est très aléatoire, soit, la passaphrase n'est pas un mot de la vie de tout les jours, ni un prénom d'une personne, il y aura très peu de chance que cette dernière se trouve dans un dictionnaire. Ce qui pourrait entraîner plusieurs heures de calcul pour rien. A contrario, si la passphrase est de type prénom ou mot utilisé fréquemment, vous aurez de grande chance de découvrir cette dernière. Pour ma part et même avec le dictionnaire de 4 millions de mots, après 2h30, j'ai laissé tombé l'exercice, puisque la passphrase n'était nullement de type générique (mot ou prénom, etc...). Je vous rappel que dans le cas présent j'avais mis pour passphrase **W0I1F2I3D4E5M6O**, ce qui n'était nullement, je présume dans le dictionnaire que j'avais téléchargé.

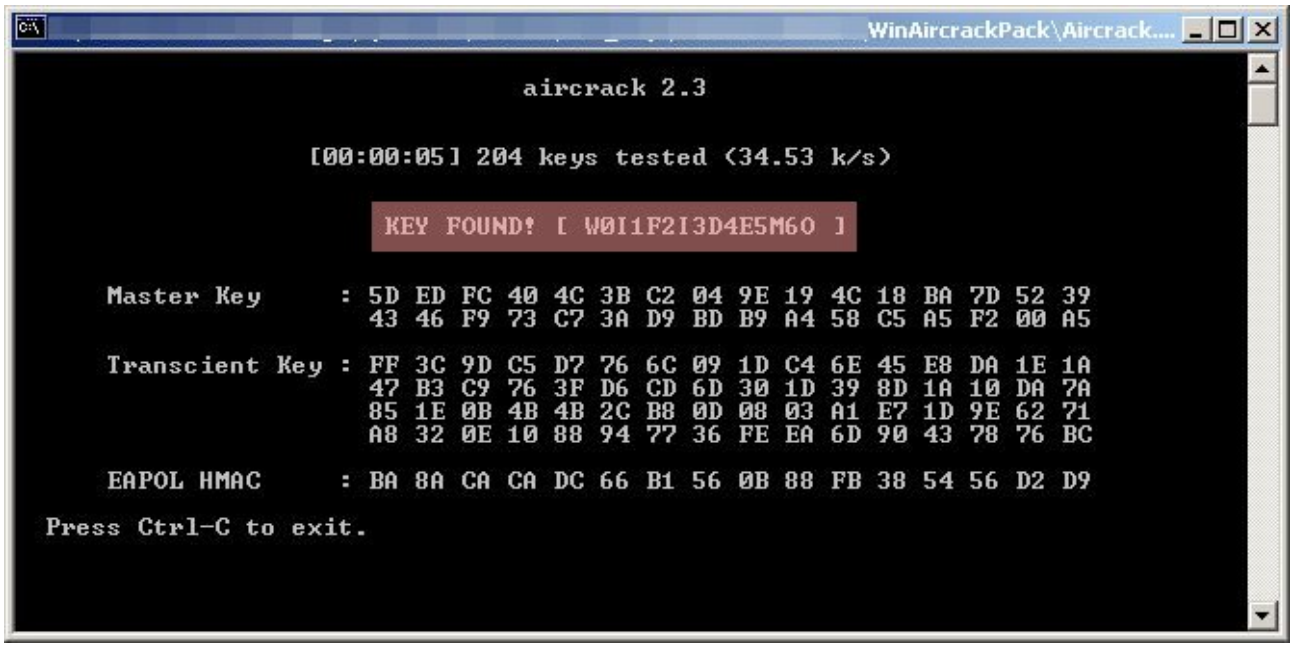
Comme d'habitude, je faisais travailler de concert Airodump et Aircrack en simultané.



Pour information, lorsque que j'ai arrêté le calcul de la passphrase, j'avais obtenu **2.7 millions de paquets**.



Si j'avais mis une passphrase qui aurait pu être dans un des dictionnaires qui sont disponibles, nous aurions obtenu un écran similaire à celui ci-dessous :



KEY FOUND! Que du bonheur...

De là, il ne reste plus qu'à faire comme pour la clef WEP, une fois obtenu cette dernière, on s'intègre au réseau.

Pour la petite histoire, j'ai obtenu le **KEY FOUND** en faisant un fichier dico avec quelques mots « bidon » ainsi que la passphrase que j'avais configuré dans le Linksys.

A noter, que sous linux un programme (WPA cracker) permettant le décryptage d'une passphrase **WPA-PSK** est disponible à l'url suivante :

http://www.tinypeap.com/html/wpa_cracker.html

Conclusion :

Voilà, j'espère que ce document vous aura permis de mettre en pratique **le décryptage de la clé wep voir de la clef WPA-PSK de votre réseau sans fil**.

Comme vous l'aurez certainement remarqué, le cryptage **WEP** est très aisément décrypté, au-contraire de la passphrase **WPA-PSK** qui si elle est bien configurée (du style **a65g8hD9j2d**) peut mettre plus de temps avant d'être découverte.

Si vous avez des questions / suggestions concernant ce document, je vous encourage à me contacter soit par e-mail à thecyberseb@hotmail.com, soit en laissant un message sur le forum qui se trouve à l'url suivante :

http://forum.monserveurperso.com

Pour de plus amples documents sur divers sujets, faite un tour à l'url ci-dessous...

http://tutorial.monserveurperso.com

Merci d'avoir pris le temps de lire ce document :-)

Merci à l'auteur de ce tutoriel (lien ci-dessous) qui a inspiré mon tutoriel.

http://www.tuto-fr.com/tutoriaux/tutorial-crack-wep-aircrack.php