ANNEXE 1

##COPIE##

SCP Eric ALBOU & Carolle YANA
Huissiers de Justice Associés

160 rue du Temple 75003 PARIS

Tel : 01.42.72.14.08 Fax : 01.42.72.20.14
Email : info@albouyana.com

PROCES VERBAL DE CONSTAT

L'AN DEUX MIL HUIT
ET LE VINGT SIX MAI

A LA REQUETE DE :

ASSOCIATION UFC-QUE CHOISIR, ayant son siège social au 233 Boulevard voltaire 75011 PARIS agissant poursuites et diligences de son Président y domicilié en cette qualité.

LAQUELLE ME FAIT EXPOSER PAR M. MACHANOVITCH Jean Philippe, Chargé de mission en Communication Web Politique.

- Que dans le cadre de la future Loi dite HADOPI, il est prévu une coupure de connexion au réseau Internet pour les abonnés dont l'adresse IP aurait été relevé par des sociétés privées traquant le téléchargement illégal.

- Que ce moyen de preuve rapporté par les sociétés ne peut pas être une preuve irréfutable de l'implication de l'abonné en cas de détection de téléchargement illégal.

- En effet, la plupart des constructeurs de matériel permettant la connexion au réseau Internet et les Fournisseurs d'Accès à Internet fournissent des systèmes de connexions sans fil sécurisés ou non.

- Que les systèmes de connexion sans fil sécurisés n'apportent pas toujours une protection efficace contre le détournement d'adresse IP et qu'il existe de nombreux tutoriels sur Internet qui permettent à un débutant en informatique de se connecter chez un tiers par ondes Wi-Fi et ce sans que l'abonné n'ait connaissance de ces faits.

- Qu'elle me requiert en conséquence de procéder à plusieurs opérations depuis mon étude et le voisinage afin de relever toutes informations nécessaires, et ce, pour la sauvegarde de ses droits, moyens et actions.

C'est pourquoi,

DEFERANT A CETTE REQUISITION,

Je, Eric ALBOU, Huissier de Justice associé de la SCP Eric ALBOU & Carolle YANA prés le Tribunal de Grande Instance de Paris y demeurant 160 rue du Temple sis à Paris 3eme, soussigné

J'AI CONSTATE CE QUI SUIT :

De mon étude ce jour à 11 Heures, à l'aide de mon ordinateur de marque ASUS de la marque ASUS TEK COMPUTER modèle W6J composé d'un processeur INTEL CORE DUO T5600 fréquence 1,67 GHz avec un 2 GO de mémoire ram sous environnement WINDOWS XP PRO SP2 le navigateur est INTERNET EXPLORER 7.00.

Ma connexion est reliée au réseau Internet de la société FREE dont les serveurs DNS sont les suivants :

Primaires 212.27.32.176 et 212.27.32.177

J'utilise un routeur et je ne suis pas connecté à un proxy-serveur.
L'adresse IP de mon domicile est 82.225.88.91. J'ouvre mon navigateur Internet.

Je m'assure que la page affichée est réellement celle qui est en ligne à la date et à l'heure du constat. Afin d'effacer toutes traces de navigations antérieures et dans un souci de ne charger que des pages actualisées en vue de mes constatations, je procède donc au vidage du cache d'Internet Explorer et à la suppression des cookies. Pour ce faire, je clique sur « Outils », puis « Options Internet ». Une fenêtre apparaît, je clique sur « supprimer les fichiers ». En suite je coche la case « supprimer tout le contenu hors connexion » et je clique sur « OK ».

Je clique ensuite sur « Supprimer les cookies ». Une nouvelle fenêtre apparaît me demandant de confirmer la suppression, je confirme en cliquant sur « OK ».

Pour les besoins de cette opération, je me connecte sur http://www.free.fr et accède à mon interface abonné après avoir entré mon login et mot de passe ; j'active le routeur DHCP de ma Freebox ainsi que son interface Wi-Fi. Je paramètre le cryptage du Wi-Fi sur WEP, il m'est communiqué une clé WEP que je conserve.

Puis, je redémarre ma Freebox depuis mon bureau, après quelques minutes celle-ci recharge son firmware avec les nouveaux paramètres saisis dans l'interface client de Free. Je retire mon câble réseau RJ45 qui me reliait à mon routeur.

Le tutoriel que j'utilise, disponible à l'adresse http://www.tuto-fr.com/tutoriaux/tutorial-crack-wep-aircrack.php, préconise l'utilisation de Live CD Linux de type backTrack 2 et d'une clé Wi-Fi compatible Linux et permettant les injections de données.

Une fois terminé, je place un CD-Rom que me remets M. MACHANOVITCH Jean Philippe, il s'agit d'un Live CD Linux BackTrack 3 Bêta Build du 14 DECEMBRE 2007. Il me déclare que ce CD permet d'utiliser Linux sans atteindre ou incrémenter mon disque dur, il me précise que ce système Live CD est un outil conçu pour tester la résistance aux intrusions des réseaux informatiques de particuliers et de professionnels.

Je redémarre mon PC et choisi de démarrer sur le Cd-Rom. Au bout de quelques minutes, le système d'exploitation (distribution Linux) du Live CD s'exécute et me propose un écran de type muti fenêtres.

Je connecte une clé USB contenant un résumé des commandes présentées dans le tutoriel disponible à l'adresse http://www.tuto-fr.com/tutoriaux/tutorial-crack-wep-aircrack.php.
Je constate la présence de lignes de commandes à exécuter, je connecte une clé USB Wifi DLINK DWL-G122 pour me permettre la connexion à un point d'accès Wifi.

Il est ici rappelé que cette méthode permet de repérer un Point d'Accès Wifi, même si ce dernier ne diffuse pas le nom de son réseau (SSID), ainsi que ses Clients réseau (utilisateurs connectés qui passent par ce Point d'Accès Wifi pour accéder à Internet) et permet également de trouver la clé de cryptage et d'authentification du Point d'Accès en mode WEP.

J'ouvre une première fenêtre de commandes (SHELL 1) et je saisi les commandes suivantes :

- Je saisis « **airmon-ng stop rausb0** ». *Il m'est précisé qu'il s'agit d'arrêter le Monitoring des points d'accès à partir de la clé Wi-Fi.*
- Je saisis « **ifconfig rausb0 down** ». *Il m'est précisé que cette commande désactive la clé Wi-Fi.*
- Je saisis « **macchanger -mac 00:11:22:33:44:55 rausb0** ». *Il m'est précisé que cette commande permet de changer l'adresse MAC attribuée par le constructeur à ma clé Wi-Fi pour une de mon choix ici « 00:11:22:33:44:55 ».*
- Je saisis « **airmon-ng start rausb0** ». *Il m'est précisé qu'il s'agit de relancer le Monitoring des points d'accès à partir de la clé Wi-Fi.*
- Je saisis « **airodump-ng rausb0** ». *Il m'est précisé qu'il s'agit d'une commande qui va détecter les adresses MAC des points d'accès captés dans le périmètre de ma clé Wi-Fi et me permettre, notamment, de connaitre le Canal de diffusion, le type de Cryptage défini (OPN-ouvert-, WEP, WPA, WPA2) et le nom du réseau utilisé (SSID) même si celui-ci est « caché ». Cette commande permet aussi de détecter tout les clients réseau (et leurs adresses MAC) qui sont connectés aux différents points d'accès et qui échangent des données avec eux.*

  Après avoir repéré mon Point d'Accès Freebox à pirater qui se dénomme « Freehd », dont l'adresse MAC est « BE:A4:6F:4D:C6:D0 » et qui communique sur la Canal 10, j'effectue un raccourci clavier CTRL+C pour figer l'écran et saisir une commande qui, pour des raisons de déontologie, ne prendra pour cible que mon propre réseau Wi-Fi Freebox. Je sais donc la même commande que précédemment en ajoutant des paramètres de filtrage : « **airodump-ng -c 10 -w wepivs -bssid BE:A4:6F:4D:C6:D0 rausb0 ».** *Cette commande va récupérer les vecteurs d'initialisations dans un fichier, wepivs, sauvegardé dans la mémoire vive de mon PC ».*

Je laisse la commande s'exécuter dans SHELL 1, puis j'ouvre une deuxième fenêtre de commandes (SHELL 2).

Je saisis la commande suivante « **aireplay-ng -1 0 –a BE:A4:6F:4D:C6:D0 –h 00:11:22:33:44:55 rausb0 ».** *Il m'est précisé qu'il s'agit d'une attaque de fausse authentification auprès du Point d'Accès.* La clé Wi-Fi est maintenant associée au Point d'Accès « Freehd ».

Je saisis la commande « **aireplay-ng -3 –b BE:A4:6F:4D:C6:D0 –h 00:11:22:33:44:55 rausb0 ».** *Il m'est précisé qu'il s'agit d'une attaque d'injection de données visant à stimuler le trafic sur le Point d'Accès et ainsi de générer plus rapidement le nombre requis de vecteurs d'initialisation qui serviront à décrypter la clé WEP.*

Parallèlement, je constate dans SHELL 1 que le trafic s'accélère. Après quelques minutes SHELL 1 indique que les vecteurs d'initialisation sont aux nombres de 23000.

J'ouvre alors une troisième fenêtre de commandes (SHELL 3) et je saisis la commande **« aircrack-ng –n 64 –b BE:A4:6F:4D:C6:D0 wepivs-01.cap ».** *Il m'est précisé qu'il s'agit d'une commande de décryptage de la clé WEP à partir des vecteurs d'initialisation collectés dans le fichier* ***wepivs-01.cap*** .

En quelques secondes la clé WEP est révélée, je compare celle-ci avec l'originale fournie par Free, il s'agit de la même clé.

Puis, j'enregistre sur la clé USB la copie écran que j'imprime par la suite.
Puis, j'éteins mon PC.

Puis, nous sortons de l'étude à 12H40 et je cherche dans la rue avec mon PC de marque ASUS de la marque ASUS TEK COMPUTER modèle W6J composé d'un processeur INTEL CORE DUO T5600 fréquence 1,67 GHz avec un 2 GO de mémoire ram sous environnement WINDOWS XP PRO SP2 le navigateur est INTERNET EXPLORER 7.00, allumé en recherche de réseau Wi-Fi, s'il existe des points d'accès ouverts dans le quartier de mon bureau.

Nous nous rendons au « l'adresse est occultée pour des raisons de confidentialité et pourra être communiquée le cas échéant » 75003 PARIS, mon PC détecte plusieurs points d'accès Wi-Fi, qui diffusent leurs SSID, en précisant si ces points d'accès sont accessibles ou non accessibles.

Je relève la présence d'un Point d'Accès Wi-Fi accessible « NUMERICABLE-E1A0 », je clique sur ce Point d'Accès et après quelques secondes, je suis connecté avec les paramètres suivants :

- Nom du réseau : NUMERICABLE-E1A0 ;
- Vitesse : 54.0 Mbit/s ;
- Qualité du signal : Excellente ;
- Adresse IP : 192.168.0.19.

Afin de vérifier que la connexion fonctionne, premièrement je m'assure que la page affichée est réellement celle qui est en ligne à la date et à l'heure du constat. Afin d'effacer toutes traces de navigations antérieures et dans un souci de ne charger que des pages actualisées en vue de mes constatations, je procède donc au vidage du cache d'Internet Explorer et à la suppression des cookies. Pour ce faire, je clique sur « Outils », puis « Options Internet ». Une

fenêtre apparaît, je clique sur « supprimer les fichiers ». En suite je coche la case « supprimer tout le contenu hors connexion » et je clique sur « OK ».

Je clique ensuite sur « Supprimer les cookies ». Une nouvelle fenêtre apparaît me demandant de confirmer la suppression, je confirme en cliquant sur « OK ».

Puis je lance mon navigateur qui démarre sur la page d'accueil http://www.google.fr/. *Il est ici précisé que je vais télécharger le logiciel eMule qui permet de télécharger en Peer to Peer différents fichiers dont des fichiers aux formats audio (Mp3, etc.), vidéos (Mp4, DivX, etc.), des jeux et des logiciels.*

Je tape dans la zone de rechercher de http://www.google.fr/ le mot « emule » et je valide. Il apparait alors une liste de résultats, je clique sur le premier lien non commercial www.emule-project.net/home/perl/general.cgi?l=13

S'ouvre alors la page d'accueil du site français « officiel » (dixit les auteurs) d'eMule. Je clique sur le lien téléchargement, puis je lance mon logiciel NeoTrace 3.25 qui indique que l'adresse IP de ce site est 216.239.59.104.

Le logiciel est téléchargé, il s'agit de la version v0.49a d'eMule. J'installe eMule puis le lance sur mon PC. Je choisis un serveur disponible : « Razorback 3.0 ». La connexion avec le serveur s'effectue. Puis, dans le moteur de recherche d'eMule, je recherche un logiciel Peer to Peer gratuit µTorrent en saisissant « utorrent ». Apparait alors une liste comprenant un nombre important de fichiers, je télécharge le premier de la liste sur mon PC. Le téléchargement aboutit au bout de quelques minutes.

Puis, je tape l'URL suivante dans mon explorateur Internet : http://www.deezer.com, là étant je lance NeoTrace 3.25 qui fait apparaitre l'adresse IP « 78.40.120.132 ». Dans le moteur de recherche je saisis « Madonna », je valide et apparait un nombre de résultats important, je choisis la première chanson proposée « Hung up ». Au bout de quelques secondes la chanson se lance, puis je choisi une autre chanson dans la liste « Like a virgin » qui se lance aussitôt.

Je retourne sur EMULE et dans le moteur de recherche je saisis « Madonna », apparait alors un grand nombre de résultats et je constate une grande disponibilité d'albums entier de l'artiste Madonna au format ZIP et RAR.

Puis, je me déconnecte. Afin d'effacer toutes traces de navigations antérieures et dans un souci de ne charger que des pages actualisées en vue de mes constatations, je procède donc au vidage du cache d'Internet Explorer et à la suppression des cookies. Pour ce faire, je clique sur « Outils », puis « Options Internet ». Une fenêtre apparaît, je clique sur « supprimer les fichiers ». En suite je coche la case « supprimer tout le contenu hors connexion » et je clique sur « OK ». Je clique ensuite sur « Supprimer les cookies ». Une nouvelle fenêtre apparaît me demandant de confirmer la suppression, je confirme en cliquant sur « OK ».

Après avoir remis le Live CD Linux BackTrack 3 Bêta Build du 14 DECEMBRE 2007, je redémarre mon PC et choisi de démarrer sur le CD-Rom. Au bout de quelques minutes, le système d'exploitation (distribution Linux) du Live CD s'exécute et me propose un écran de

type muti fenêtres. Le Live CD utilise dorénavant la puce Wi-Fi intégrée à mon PC pour les commandes suivantes.

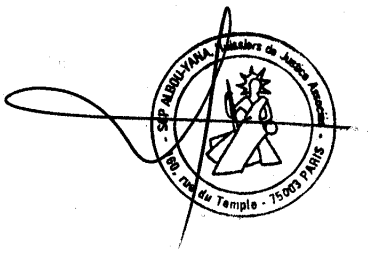
J'ouvre une fenêtre de commandes (SHELL KONSOLE), je saisis la commande « **airodump-ng wlan0** » *Il est ici précisé que cette commande permet de détecter tous les points d'accès diffusant ou ne diffusant pas leurs SSID ainsi que les clients réseau y étant connectés et, parallèlement, les adresses MAC de ces mêmes points d'accès et clients réseau.*

Au bout de quelques secondes, apparait sur « SHELL KONSOLE » 40 points d'accès dont 6 ouverts (OPN), 12 WEP, 8 WPA et 14 WPA2. *Il m'est ici précisé que la procédure établie en mon étude aurait pu être répétée sur les réseaux cryptés WEP. En ce qui concerne les 6 points d'accès ouverts (OPN) ceux-ci semblaient sans aucune protection apparente.*

Mes opérations se terminent à 14H20.

TELLES SONT MES CONSTATATIONS J'ANNEXE L ENSEMBLE DES PAGES CONSULTEES QUI SONT LE REFLET EXACT DE MES CONSTATATIONS.

POUR LESQUELLES J AI DRESSE LE PRESENT PROCES VERBAL DE CONSTAT POUR SERVIR ET VALOIR CE QUE DE DROIT



Me Eric ALBOU