**La position de CoPeerRight Agency :**
**Le recours aux signatures numériques de fichier (le hachage)**

1) Une solution applicable à l'ensemble des œuvres présentes sur les réseaux

- La détection des œuvres protégées de toute nature :

Alors que les empreintes numériques (Fingerprint) ne sont pas toujours réalisables (elles ne fonctionnent pas sur le binaire), les signatures numériques (Md4, Md5, SHA1, Tiger Free…) permettent de détecter l'ensemble des œuvres contrefaites mises à disposition sur les réseaux, de quelque nature qu'elles soient : les fichiers musicaux, vidéos, mais aussi les logiciels exécutables, y compris les logiciels de loisirs, les fichiers archivés (.zip, .rar) etc.

- La détection des œuvres sur les réseaux « underground » :

30% seulement des œuvres protégées sont disponibles sur les sites UGC légaux (Youtube, Dailymotion, Wat.tv…), le reste étant mis à disposition sur les réseaux underground qui ne sont pas surveillés. Pour l'internaute, peu importe le serveur sur lequel est hébergé le fichier contrefait, il peut le lire et en profiter de la même manière. Les signatures numériques permettent la détection des fichiers contrefaits présentés sur ces sites.

2) Une solution fiable sur le long terme et rentable

- La fiabilité des techniques utilisées :

Les signatures numériques sont générées par des algorithmes de hachage qui permettent de ressortir d'un fichier une valeur unique. Les fonctions de hachage cryptographique les plus fréquemment utilisées sont MD5 et SHA-1. Si l'on modifie la valeur d'un ou plusieurs octets dans le fichier, la signature de ce dernier sera très différente. Les signatures numériques permettent ainsi d'identifier les fichiers avec une grande précision.
Aucune collision n'est possible (autrement dit, deux fichiers différents ne peuvent pas avoir une signature numérique identique).

- La rentabilité de la solution :

Les algorithmes de hachage sont sous licence open source. Par conséquent, le retour sur investissement est nul : ces techniques peuvent être utilisées gratuitement. La constitution de la base de données est également beaucoup moins coûteuse qu'une base d'empreintes puisqu'elle nécessite moins de serveurs.
Enfin, l'utilisation des signatures numériques de fichiers est rentable sur le long terme, puisque ces dernières obéissent à un principe de rétrocompatibilité.

- L'harmonisation internationale du suivi des fichiers contrefaits :

De nombreux organismes professionnels (MPAA, IFPI, FAP, FAPV, BAF…) utilisent déjà dans le monde entier les signatures numériques (Md4, Md5, SHA1, Tiger Free…). Pourquoi la France utiliserait-elle plusieurs méthodes différentes ? Ces signatures sont même déjà utilisées par des organismes français : lors de l'établissement de PV par des agents assermentés, les signatures numériques sont précisées.