Forum: Propositions de logiciels

Topic: Re: HashOnClick

Subject: Re: HashOnClick

Publié par: Constance

Contribution le : 19/02/2007 14:01:08

L'explication de lucjoqc est pas mal, sauf ce point :
Citation :
C'est une série de lettres et chiffres unique à chaque fichier. qui est faux.
Plusieurs fichiers distincts peuvent avoir le même hash, même si c'est peu probable du fait du nombre de possibilités.
Si chaque fichier avait un md5 qui lui était unique, alors on aurait plus besoin de programmes de compression mais seulement du dit md5 pour recalculer entièrement le fichier d'origine ;)
D'ailleurs comme il est dit dans l'article wikipedia, (http://fr.wikipedia.org/wiki/Md5) , il est possible de créer un fichier ayant un md5 défini à l'avance, et donc de corrompre un fichier sans que ce soit détectable par le hashage md5. (D'où l'intérêt de vérifier non seulement le hash md5 mais aussi le SHA-1 et pourquoi pas même le CRC32 ... plusieurs vérifications valent mieux qu'une, sachant qu'a priori, deux fichiers distincts ayant toutefois le même md5 ne devraient pas pour autant avoir le même CRC etc...).