Forum: Propositions de logiciels

Topic: TrIDNet - File Identifier

Subject: TrIDNet - File Identifier

Publié par: danee

Contribution le : 08/07/2007 18:22:19

TrID - File Identifier TrIDNet v1.80 (free)
TrID is a utility designed to identify file types from their binary signatures.
TrID has many uses: identify what kind of file was sent to you via e-mail, aid in forensic analysis, support in file recovery, etc.

site ... http://mark0.net/soft-tridnet-e.html
télécharger les fichier ....
http://mark0.net/download/trid_net.zip TRIDNet is the GUI version of TrID.
http://mark0.net/download/triddefs_xml.rar (package with 2625 defininitions)
et les déZIPer dans un repertoire, pas besoin d'install
TrID, identifie les fichier même si l'extension est fausse.
definition pour 2625 types de fichiers. ouvrez le TrIDNet et analysez ....
N.B. The .NET Framework is required.
trid.exe --> c'est une verssion "ligne de command" voir ... http://mark0.net/soft-trid-e.html
ex: D:TrID>trid f:testdoctutorial.doc

si vous ne voulez pas l'installer, vous pouvez utiliser la version
OnLine http://mark0.net/onlinetrid.aspx

MiniDumper
Simple tool to display an hex dump of the header (first 256 bytes) of a file.
http://mark0.net/download/minidumper.exe

POUR utilisateurs avancés
si vous avez bien décompresé .... dans le rerertoire se trouve le fichier tridscan.exe ce fichier vous permet de créer vos propres définitions ....
TrIDScan - Patterns scanner
TrIDScan creates new definitions to be used with TrID. You can use it to help collect new unique definitions.
voir ici pour plus de details...
http://mark0.net/soft-tridscan-e.html
(c'est un program qui travail de la ligne de command)
ex: vous voulez créer une définition pour les fichier .class
D:Trid>tridscan f:test*.class
pour avoir une définition valable, il faut que le dossier (f:test) contien au moins 5-10 ou plus fichiers du même type