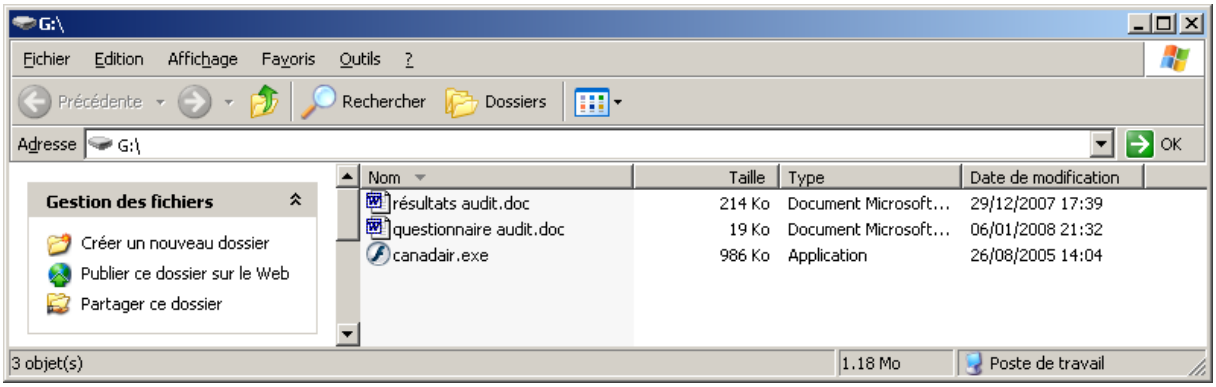
ewatching	**Sécurité Informatique**

Objet :	**Démonstration de USBDumper 2**	Date : Version :	**06/01/2008** **1.0**

Attention, plus que jamais ce qui est présenté ici est pour test et ne doit être reproduit.
L'objectif est ici de montrer aux dirigeants d'entreprises à quel point l'utilisation de clés USB peut être dangereux.

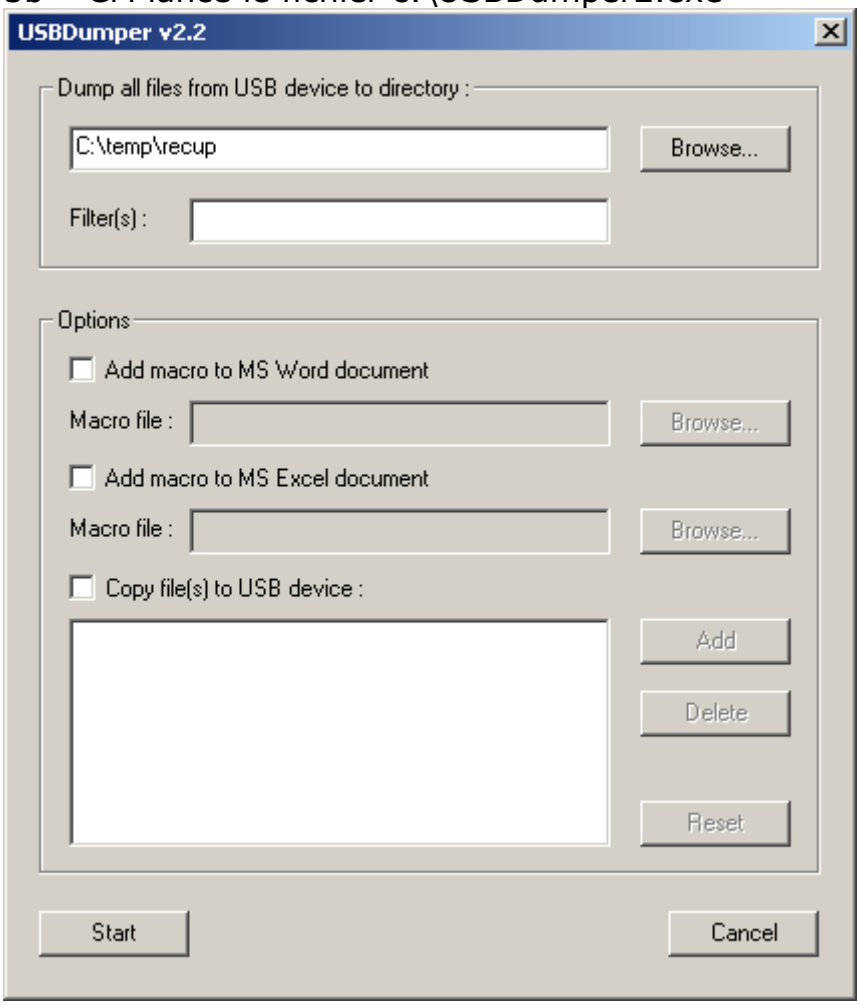
Imaginons la première situation suivante :
Etape 1 - Vous posséder une clé USB avec vos documents privé, confidentiels , de travail ou autre éléments que vous ne souhaitez mettre sur le réseau de votre entreprise, encore moins sur votre portable.
Etape 2 – Vous devez fournir un simple document Word à un collègue ou fournisseur. N'ayant pas confiance, vous ne voulez pas lui prêter la clé USB mais vous souhaitez mettre vous-même le fichier en question sur le PC de destination (qui n'est pas le vôtre).
Etape 3 – Nous sommes le possesseur du PC et sommes aussi interressés par le contenu de la clé USB. Voici ce que nous pourrions faire :

3a – Le parano-naïf (PN) doit posséder une clé USB avec des documents Word, XLS ou même des programmes.



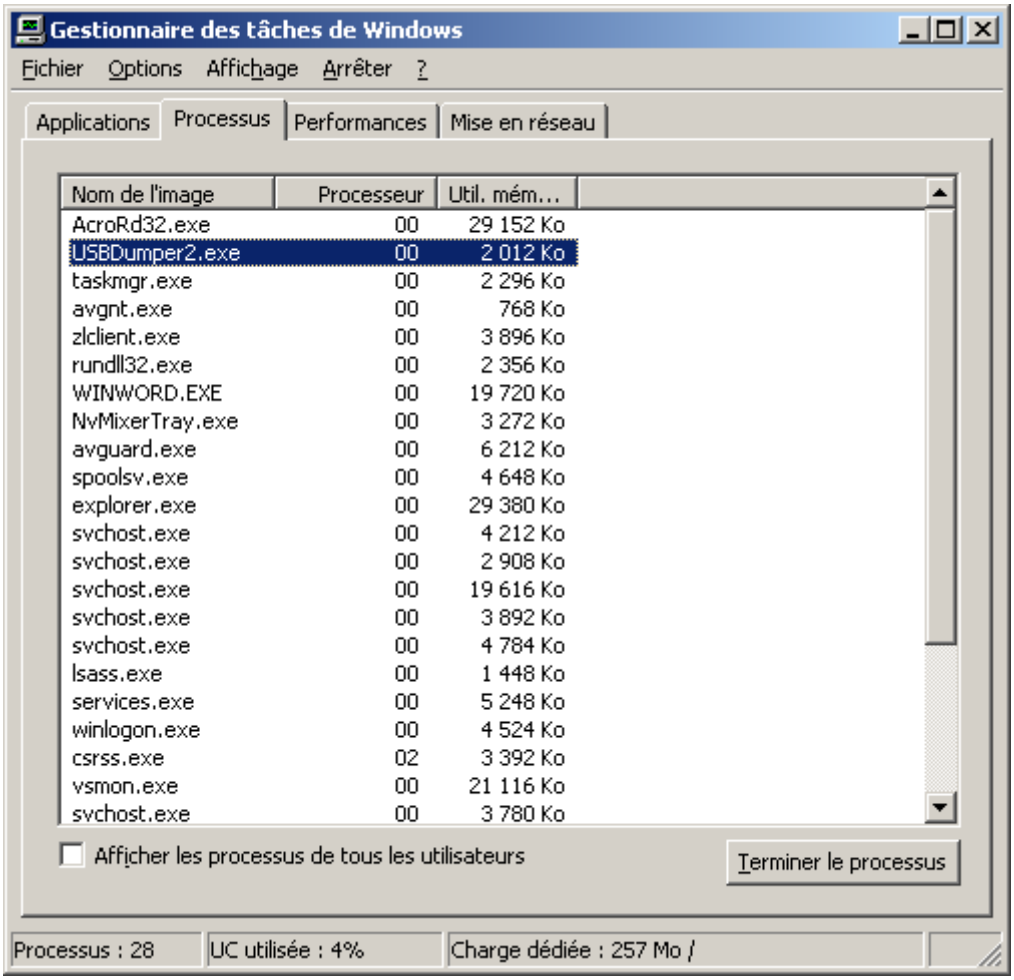
3b – Le curieux-malhonnête (CM) télécharge USBDumper2, et dézippe l'EXE dans le répertoire du PC **c:\temp** . il créé aussi un répertoire nommé **recup** dans **c:\temp**

3b – CM lance le fichier c:\USBDumper2.exe



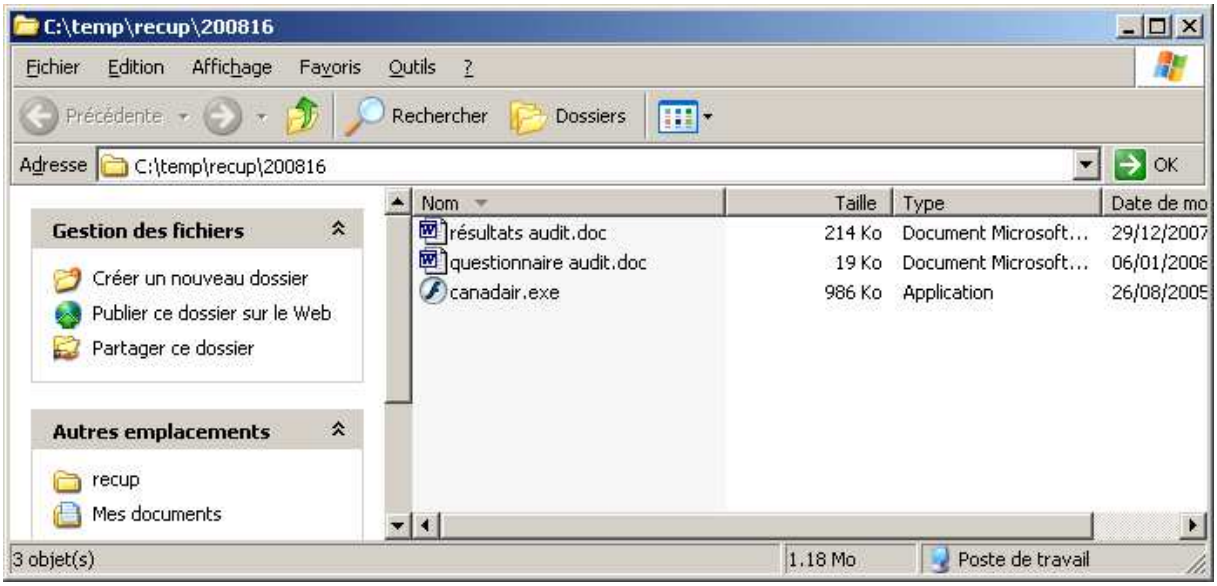
CM indique le chemin de récupération de la clé USB juste dans le champ **« Dump all... »**, ici **c:\temp\recup**

3c – CM clique sur **start** et constatera à l'occasion que USBDumper2 est en mémoire et visible en tant que processus dans le gestionnaire des tâches mais plus d'interface graphique visible.



3d - PN insère sa clé USB protégée en lecture (? on ne sait jamais), copie son fichier sur le bureau du PC et retire sa clé.

3e – CM ouvre le répertoire c:\temp\recup\aaaamj (ou aaaa est l'année, m le numéro du mois sur 1 ou 2 digits, j, le numéro du jour)



3f – CM trouvera une copie complète de la clé USB

3g – CM aurait pu spécifier un filtre sur la recopie des fichiers « souhaités ». Dans le champ **Filter...** de USBDumper, il suffit d'indiquer les extensions attendues séparées par des espaces.

Imaginons la seconde situation où le CM souhaite en plus agir directement sur la clé USB de PN (si celle-ci n'est pas en lecture seule)
Deux façons d'agir sous USBDumper :

- en cochant la case Copy file(s) to USB Device et en sélectionnant un fichier EXE + son autorun.inf = cela aura pour conséquence de recopier dès l'insertion de la clé USB, les fichiers sélectionnés. Si l'hypothèse est que l'autorun fonctionne automatiquement sur la clé USB lorsque celle-ci reviendra dans l'entreprise, les conséquences pourraient être assez néfastes.
- En cochant Add macro to MS Word ou XLS document, il est alors possible de faire pointer une macro du cru de CM par type de document (WRD ou XLS). A l'insertion de la clé de PN sur le PC de CM, tous les fichiers WRD ou XLS seront alors greffés des macros sélectionnées.

Toutes ces explications ou démonstrations sont très limitées mais devraient faire réagir plus d'un responsable sur l'utilisation des clés USB dans son entreprise.

USBDumper a été réalisé par Eric Detoisien et présenté lors du SSTIC 2006 (l'une de ces formidables Rump Sessions).