Présentation des Alternate Data Stream (ADS)

par Manumation (Mes articles)

Date de publication : 26.02.2008

Dernière mise à jour : 26.02.2008

Cet article présente les Alternate Data Stream, autrement dit les flux alternatifs de données. Bienvenue dans le côté sombre de l'informatique...

I - Introduction
II - Que sont les ADS ?
III - L'explication par l'exemple
IV - Les contre-mesures
V - Conclusion

I - Introduction

Dans cet article, je vais vous présenter les Alternate Data Stream...

Quoi ? Vous n'en avez jamais entendu parler ? Pas de souci, c'est normal ! Il s'agit d'une fonctionnalité bien méconnue du public, qui est surtout utilisée par les créateurs de virus et autres hackers...Ne vous en faites pas, il n'y a rien d'illégal dans ces manipulations ! Aussi, je tiens à souligner que cet article est à titre informatif et que tout ce que vous pourrez faire avec les informations suivantes ne me concerne en rien, ni ne concerne Développez.com

II - Que sont les ADS ?

ADS est un acronyme qui signifie : **Alternate Data Stream**. En français cela se traduirait par flux de données additionnels. Cette technique ne concerne que les **systèmes de gestion de fichiers** NTFS.

Cela consiste en fait à ajouter à un fichier ou un dossier, un nouveau flux de données. Vous, vous n'avez accès en temps normal qu'à un seul flux de données, comme par exemple lorsque vous lisez un fichier texte, c'est le "flux normal". Mais NTFS offre la possibilité d'en ajouter un ou plusieurs à un même fichier. Ces flux additionnels sont en quelque sorte des meta-données, qui sont invisibles en temps normal. Non pas seulement invisible comme des fichiers cachés, ils sont complètement invisibles ! C'est-à-dire qu'avec l'explorateur de Windows vous n'avez aucune chance de les détecter. D'ailleurs, vous ne pourrez même pas connaître leur taille.

Vous commencez à comprendre l'intérêt que peut susciter une telle technique chez les créateurs de virus.

Les ADS ont été créés dans le but d'offrir une compatibilité avec HFS, le système de gestion de fichiers sous **Mac**. Sans entrer dans les détails, le but était de pouvoir créer un serveur de fichier Windows avec comme clients des Mac. De nos jours, ils sont aussi utilisés dans certaines techniques de traçabilité de fichiers, et pour par exemple, des résumés (voir fin du chapitre).

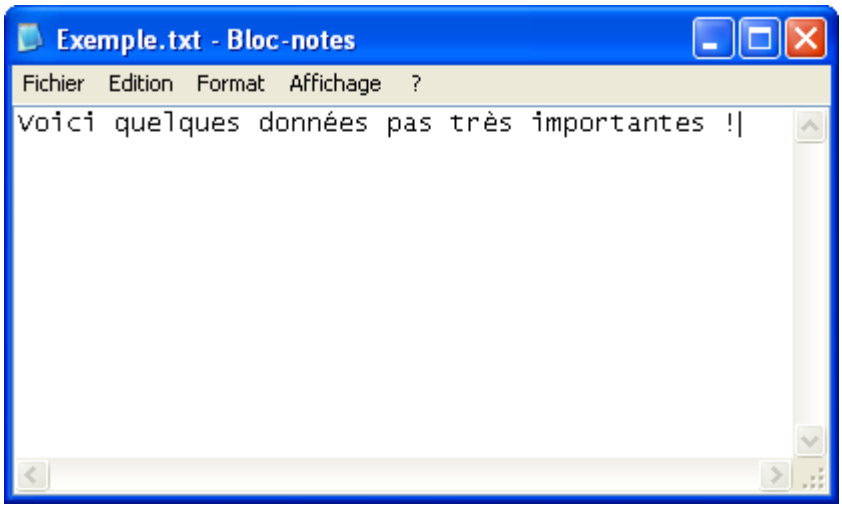
Il faut aussi noter que ces flux peuvent être de tout type, pas seulement du simple texte, mais également des images et même des exécutables ! Néanmoins, tout passage des données dans un autre système de gestion de fichiers (*FAT16, FAT32...*), détruira ces meta-données. Par exemple le transfert des fichiers sur une disquette.

Bon, finis les grands discours, passons à la pratique !

III - L'explication par l'exemple

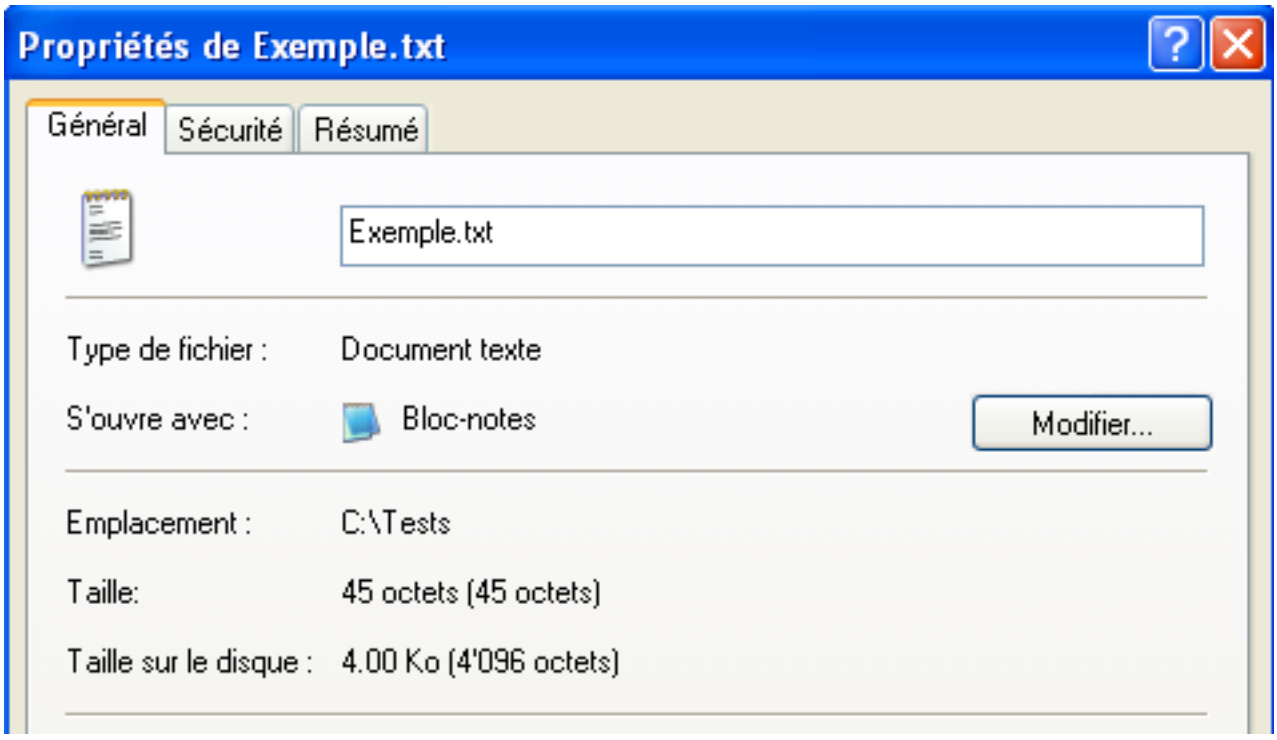
Vous allez me dire que c'est bien beau tout ça...Mais comment fait-on ? Et bien en avant...

Tout d'abord je vais créer un simple fichier texte (.txt), que je vais appeler "Exemple.txt" et enregistrer dans "C:\Tests\". Dans ce fichier, je vais écrire quelques données :



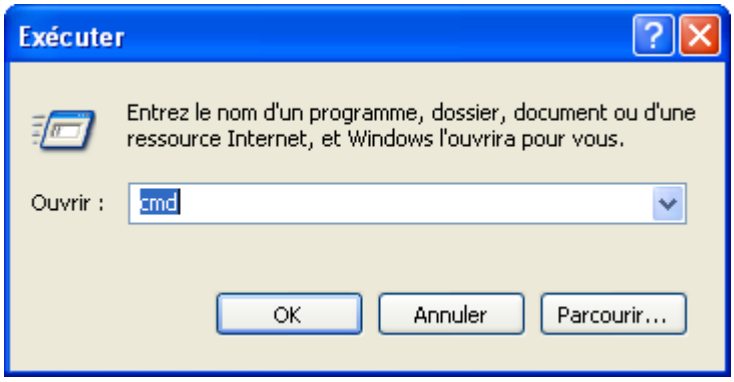
Un simple fichier texte

Notez bien sa taille qui est ici de 45 octets :



Propriétés avant l'ajout d'un ADS

Ensuite, je vais ouvrir une fenêtre DOS (*Démarrer --> Exécuter*) :



Ouvrir une fenêtre DOS

Pour simplifier les opérations, je vais me mettre dans le répertoire contenant mon fichier (*C:\Tests*) avec la commande

```
C:
```

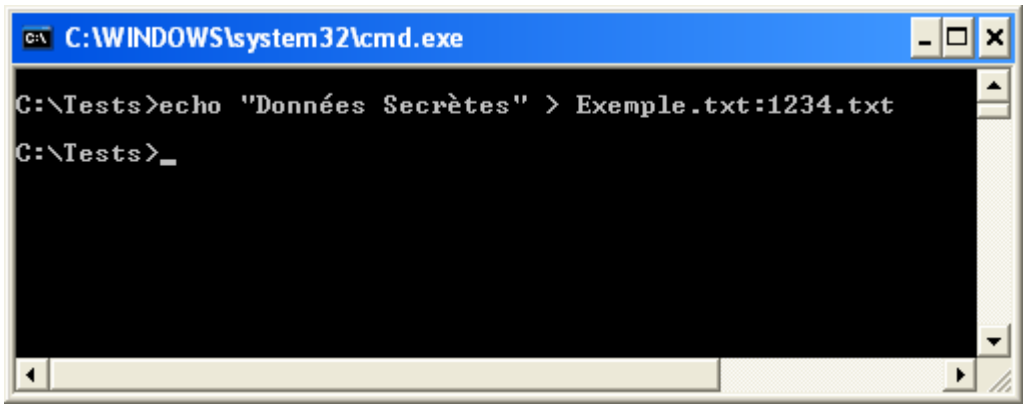
Puis avec la commande :

```
cd Tests
```

Puis, pour ajouter un ADS, tapez la commande suivante :

```
echo "Données Secrètes" > Exemple.txt:1234.txt
```

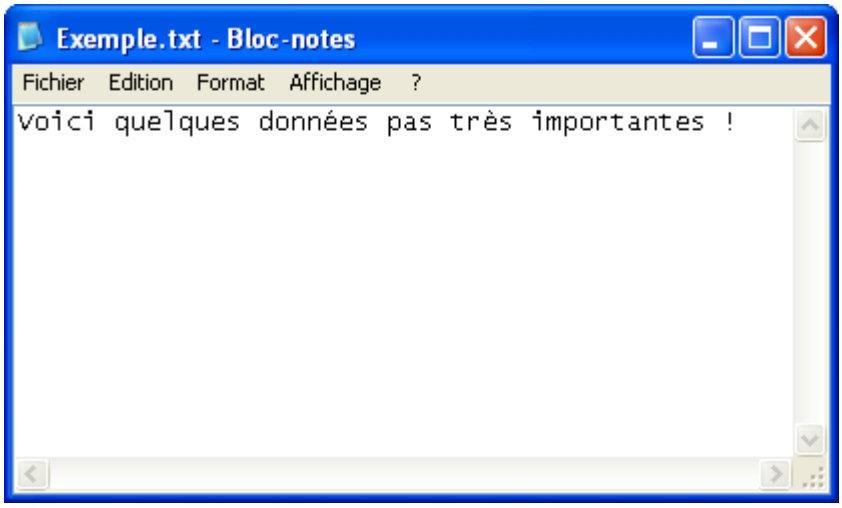
L'ADS a été ajouté. Voici à quoi ressemble la fenêtre DOS :



Ajouter un ADS

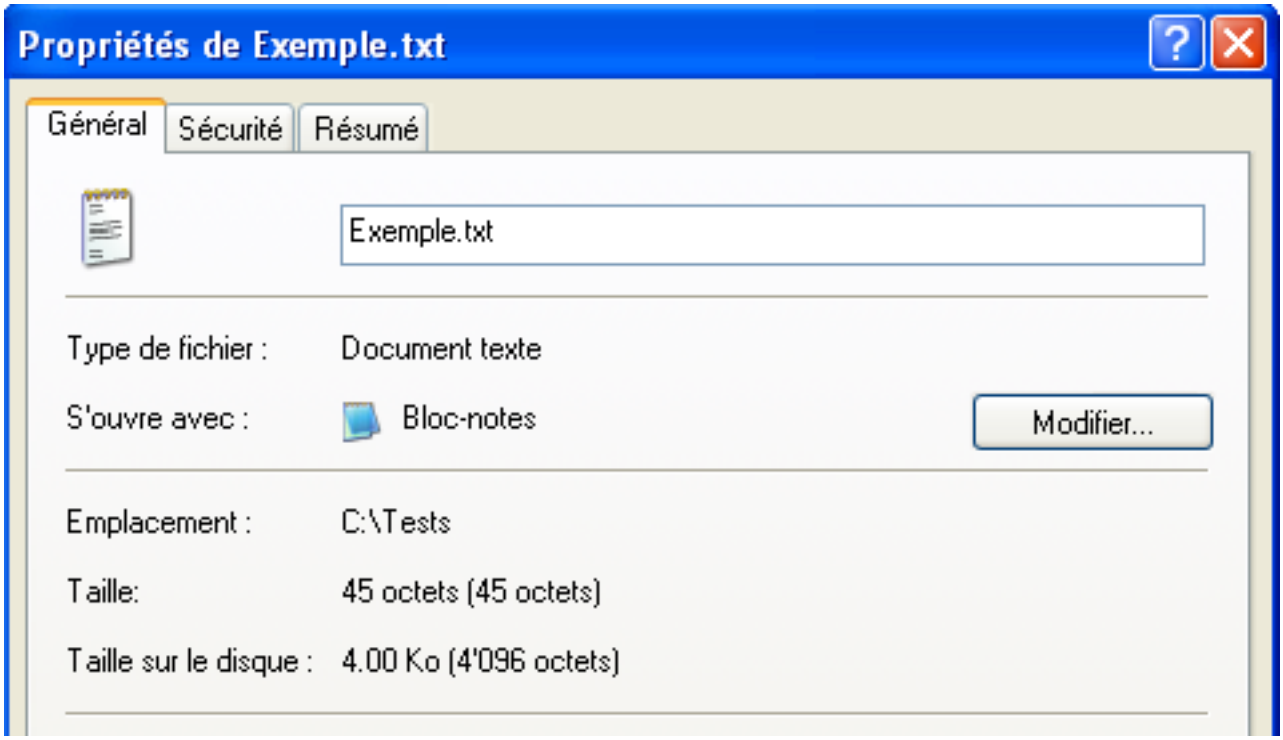
La commande décrite ci-dessus a en fait ajouté un nouveau flux qui est *1234.txt* avec comme données "*Données Secrètes*". Le nom du flux (*1234.txt*) est en quelque sort la clé qui permet de retrouver les données, sans cette dernière, impossible de retrouver les données !

Si vous ouvrez le fichier, rien n'aura changé :



Rien n'a changé, ni vu ni connu

Dans la taille non plus, rien n'a bougé :



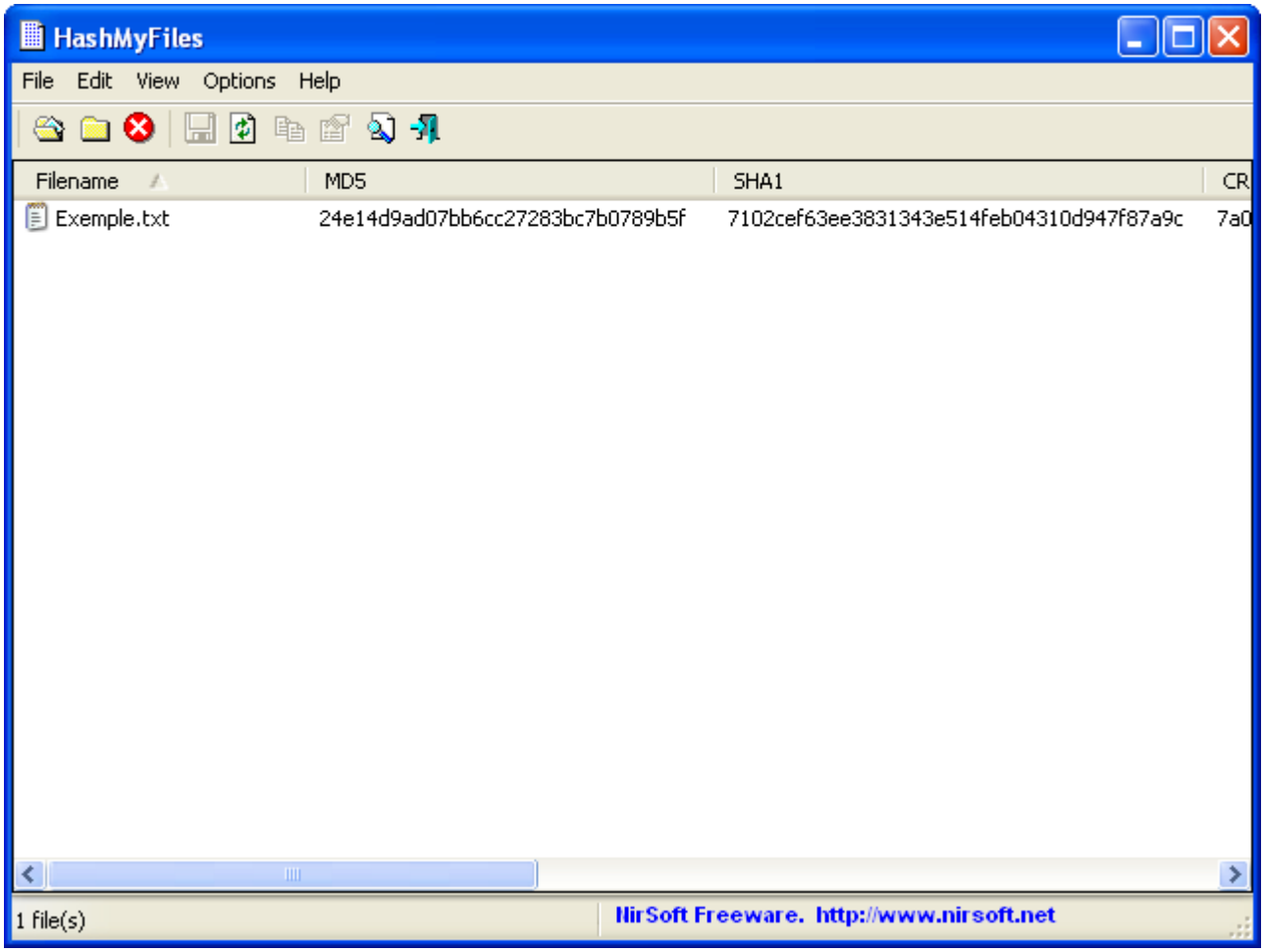
Là non plus, pas de changement

Note : ça n'est pas visible sur cette image, mais la date d'accès a été modifiée, il s'agit de la seule conséquence de notre intervention.

Pour pousser encore un peu plus loin la vérification, j'ai essayé de tester la somme **MD5** avant et après l'ajout de l'ADS. Pour cela, je me suis servi du logiciel **HashMyFiles**, disponible gratuitement à l'adresse **http://www.nirsoft.net/utils/hash_my_files.html**

Pas besoin d'installation, il suffit de le dézipper et de l'ouvrir. Ce logiciel ne fait pas que donner la somme MD5, il donne aussi la valeur SHA1 et CRC32.

J'ouvre donc mon fichier *Exemple.txt* avant l'ajout de l'ADS, ce qui me donne ceci :



La somme MD5 avant

MD5 = "24e14d9ad07bb6cc27283bc7b0789b5f" (avant)

Ensuite je fais la manipulation d'ajout, c'est-à-dire :

```
echo "Données Secrètes" > Exemple.txt:1234.txt
```

Et que me donne la somme MD5 ? Ceci :

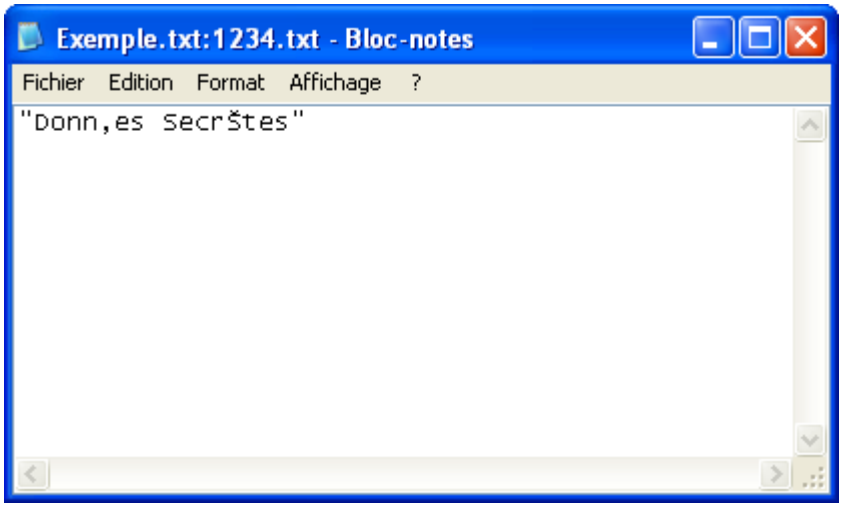
MD5 = "24e14d9ad07bb6cc27283bc7b0789b5f" (après)

Donc la même chose...Même avec cette technique, pas moyen de savoir s'il y a eu manipulation ou pas...

Revenons à nos moutons. Pour avoir la possibilité de voir les données que vous avez ajoutées en ADS, il faut taper la commande suivante :

```
notepad Exemple.txt:1234.txt
```

Avec pour résultat, vos données secrètes :

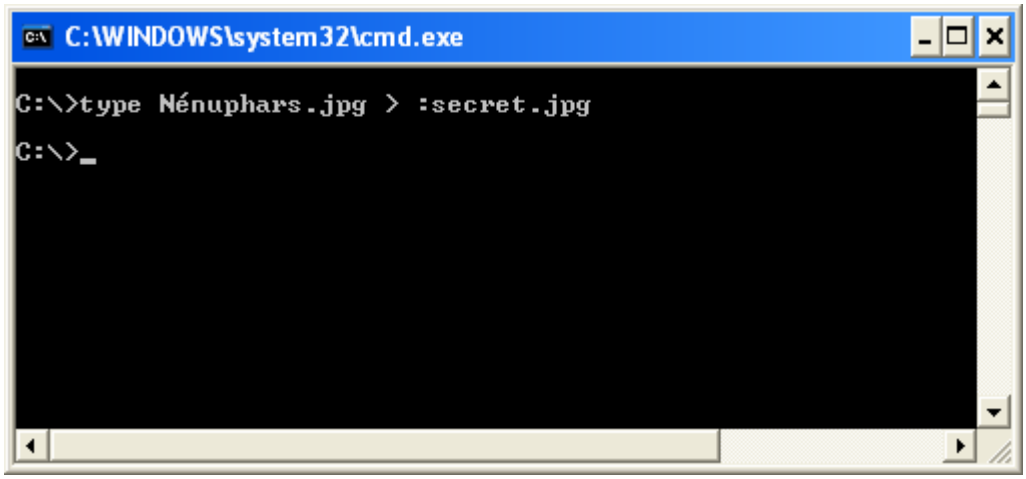


Voici vos données

Pas mal, hein ? Mais ce n'est pas tout, vous pouvez aussi ajouter des ADS sans avoir besoin d'un fichier visible. Ici avec cette commande, je vais ajouter un fichier (une image en l'occurrence *Nénuphars.jpg* que j'ai précédemment copiée dans le dossier racine *C:*) dans un ADS de la partition sous le nom de *secret.jpg* :

```
type Nénuphars.jpg > :secret.jpg
```

Voici l'équivalent dans la commande DOS :

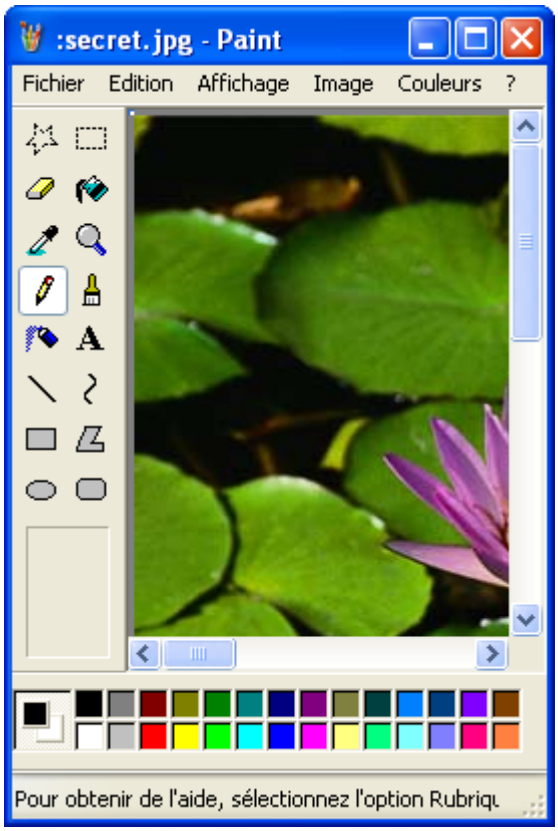


Cacher une image

Notez que l'image doit être présente dans le dossier racine (ici C:) pour l'ajouter au flux. Maintenant, supprimez-là ! Votre image sera ainsi cachée aux yeux de tous, et vous seul saurez comment la visionner. Ici, ce sera avec la commande :

```
mspaint :secret.jpg
```

Miracle ! Votre image apparaît dans Paint, et pourtant elle n'est pas visible dans C: C'est là même tout le principe des ADS !



L'image secrète est révélée

Note : Ici, le flux ADS créé ne pourra être supprimé que si la partition est formatée.

Bien, maintenant que vous êtes chaud, nous allons passer à du plus sérieux...

Je vais démontrer ici comment il est possible de cacher un exécutable à l'intérieur d'un autre exécutable. Pour ce faire, je vais utiliser deux exécutable déjà présents dans Windows ; calc.exe et notepad.exe

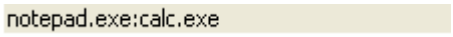
Toujours dans la fenêtre DOS, tapez :

```
type C:\WINDOWS\system32\calc.exe > C:\WINDOWS\system32\notepad.exe:calc.exe
```

Je vous laisse deviner ce qui va se passer...Vous ne savez pas ? Et bien lorsqu'on tapera la commande suivante :

```
start C:\WINDOWS\system32\notepad.exe:calc.exe
```

Ce sera la calculatrice qui s'exécutera...Remarquez la forme que prend le processus dans le gestionnaire des tâches :



Gestionnaire des tâches

Ici la calculatrice est "cachée" dans le bloc-notes, sans en affecter les fonctionnalités ! Vous me direz que la calculatrice ne représente pas grand danger, mais imaginez que ce soit un trojan qui dorme paisiblement en attendant son heure !

Heureusement, Il n'y a pas que des mauvais côtés aux ADS (belle transition hein ?). Par exemple, Windows utilise lui-même des ADS pour enregistrer les résumés des fichiers. Ils sont enregistrés dans le flux ^EDocumentSummaryInformation. "^E" signifie ici la combinaison **Ctrl + E.** Si j'ajoute un résumé à mon fichier *Exemple.txt* en allant dans *Propriétés --> Onglet Résumé* Et que je tape ensuite la commande (toujours depuis ma fenêtre DOS) :

```
more < C:\Tests\Exemple.txt:^EDocumentSummaryInformation
```

Alors je verrai s'afficher le résumé (la plupart du temps dans un langage incompréhensible il est vrai) dans ma fenêtre DOS. Ce ne sont pas les seuls ADS que Windows utilise, mais je ne vais pas faire l'inventaire du reste.

Voilà pour les ADS inoffensifs, pour les autres, vous pouvez vous reportez à la section suivante.

IV - Les contre-mesures

Avec tous les risques que les ADS représentent pour votre PC (seulement, je le rappelle, si vous êtes sous NTFS), vous devez être impatient de connaître les contre-mesures...

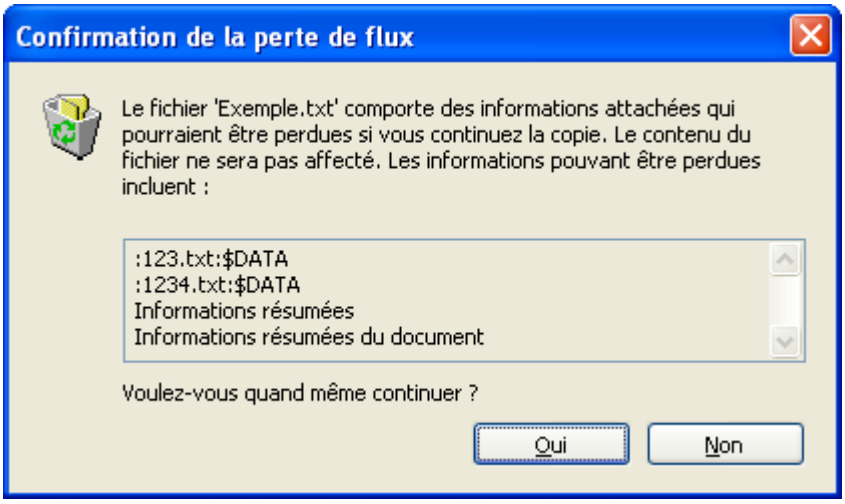
Je vous rassure tout de suite, certains antivirus de nos jours contrôlent la présence d'ADS. Mais je vais quand même vous montrer les quelques techniques qui permettent de se rassurer.

Premièrement, il faut savoir qu'on ne peut pas supprimer un flux aussi simplement qu'on l'a créé. En effet la commande :

```
del Exemple.txt:1234.txt
```

ne fonctionne pas.

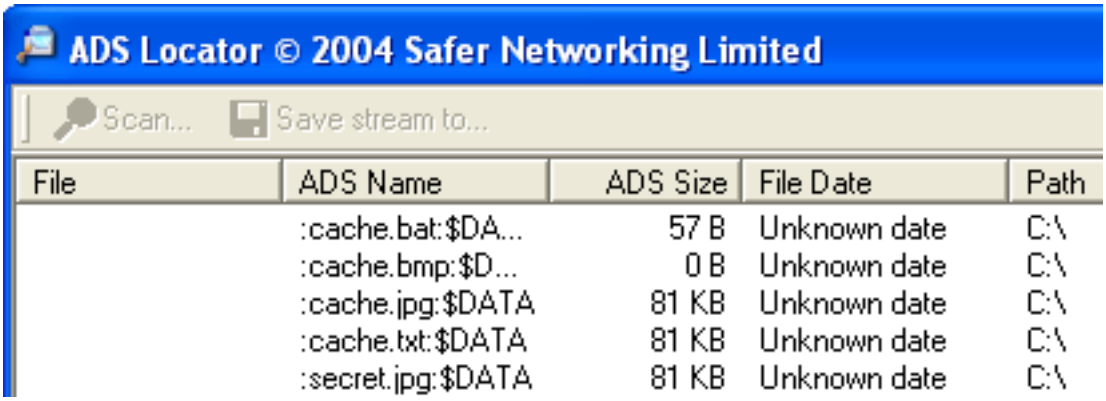
Néanmoins, vous pouvez toujours transporter les fichiers suspects sur un système de gestion de fichier autre que NTFS. Par exemple une disquette. Vous supprimez le fichier source, puis vous recopiez le fichier depuis la disquette. Cela fonctionne, mais c'est assez laborieux.



Passage en FAT

Comme vous pouvez le voir, le passage du fichier *Exemple.txt* sur une disquette (FAT) fait apparaitre une boîte de dialogue qui nous informe que les ADS seront supprimés. Cela révèle donc les flux du fichier.

Autre solution, vous pouvez utiliser un logiciel spécialisé, tel que ADS locator (**http://www.safer-networking.org/fr/tools/index.html**). Ici non plus, pas d'installation, on l'ouvre et on clique sur Scan. Le résultat ne se fait pas attendre :



ADS locator en action

Il me liste tous les flux que j'ai réalisés en essai, et le scan n'est pas fini. Bravo à **Patrick Kolla** pour cet excellent logiciel.

Autre logiciel, tout aussi intéressant, Hijackthis. Il possède en effet une option anti-ADS. Elle se trouve dans les options du programme sous *Open the Misc tools section*, puis *Open ADS spy*. Là, surprise, je clique sur Scan, le scan se termine, mais rien ne se passe, aucun flux trouvé...Je reste sur ma faim...

Il existe aussi une multitude d'autres outils sur le net, plus ou moins confortables pour découvrir les différents flux. Je vous laisse rechercher par vous-même !

V - Conclusion

Vous voilà arrivés à la fin de cet article. J'espère qu'il aura été instructif et que vous avez eu du plaisir à le suivre. Je tiens à remercier le site **http://assiste.com.free.fr/** qui a été une source d'informations intéressantes.

Un grand merci également à **caro95470** qui a pris le temps de corriger mon article et l'a fait avec une grande attention. Ainsi qu'à **Louis-Guillaume Morand**, qui m'a aidé tout au long de la rédaction et a procédé à la relecture technique. Merci à vous !