



Effacer les données cachées de différents types de fichiers

Pour plus de sécurité, adoptez les réflexes CASES !

Effacer les données cachées de différents types de fichiers

Certains types de fichiers contiennent des données masquées, qui ne sont pas nécessairement visibles à première vue. Ces données sont de nature très diverse et renseignent sur les auteurs, correcteurs, dates de création ou autres propriétés du fichier.

Malheureusement ces données peuvent contenir des informations sensibles qui ne doivent pas sortir de l'organisme.

La fuite d'informations peut se révéler désastreuse pour une PME, une administration mais également pour les citoyens. Pour les PME par exemple, cette fuite d'information peut permettre au destinataire d'un mailing de connaître le nom de tous les clients et fournisseurs de l'entreprise.

Imaginez que vous êtes à la recherche d'un emploi et que le document que vous envoyez par e-mail permette à l'entreprise dans laquelle vous postulez de connaître vos autres candidatures ! La réaction du destinataire pourrait se révéler néfaste pour votre avenir.

Les téléphones modernes peuvent, par exemple, inscrire des données de géo-localisation d'une prise de vue dans les fichiers de photos ; mais souhaitez-vous vraiment que l'on retrouve la position exacte de votre maison suite à la mise en ligne d'une photo la représentant ?

Voulez-vous que votre nom soit visible dans les métadonnées d'un document que vous auriez souhaité garder anonyme ?

Voici donc quelques moyens d'effacer ces métadonnées sur certains types de fichiers :

Photos

Certains formats d'images, comme le très courant jpeg, peuvent contenir des métadonnées comme :

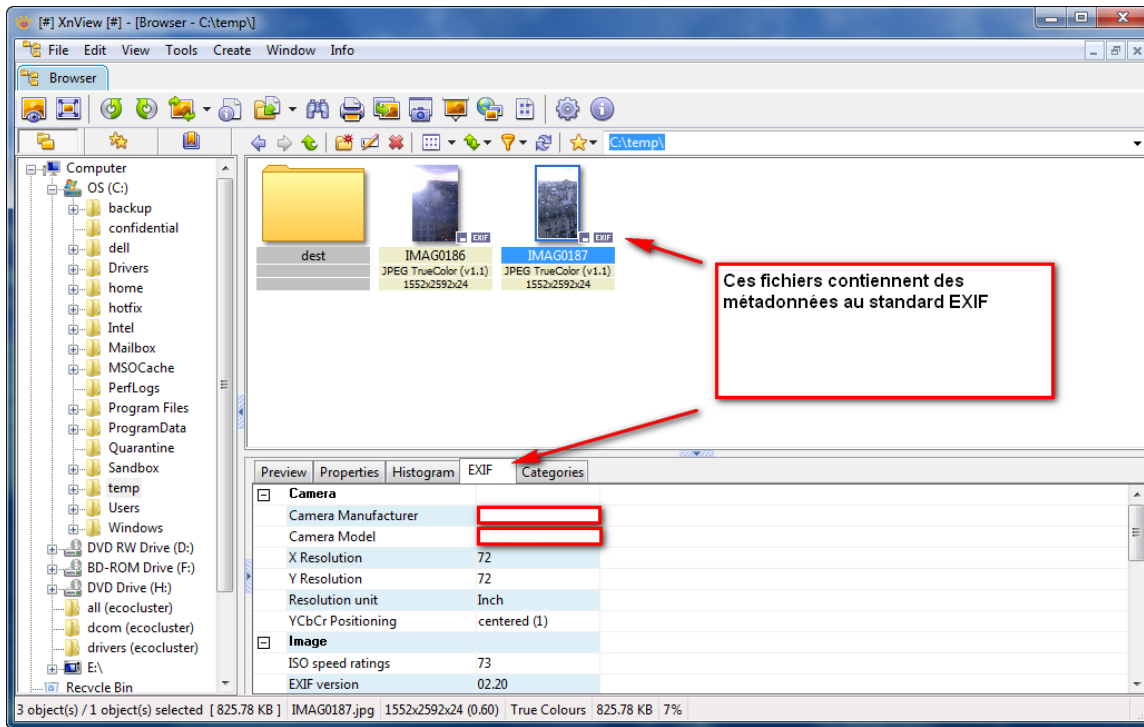
- l'appareil photo utilisé,
- les données de prises de vue
- les données de géo-localisation si l'appareil contient un module GPS (téléphones modernes),
- le moment exact de la prise de vue,
- le nom du propriétaire de l'appareil.

Il est difficile de savoir exactement quels sites web assainiront ces données et quels sites garderont la photo telle quelle. Il est donc intéressant de savoir effacer soi-même les métadonnées préalablement à une mise en ligne.

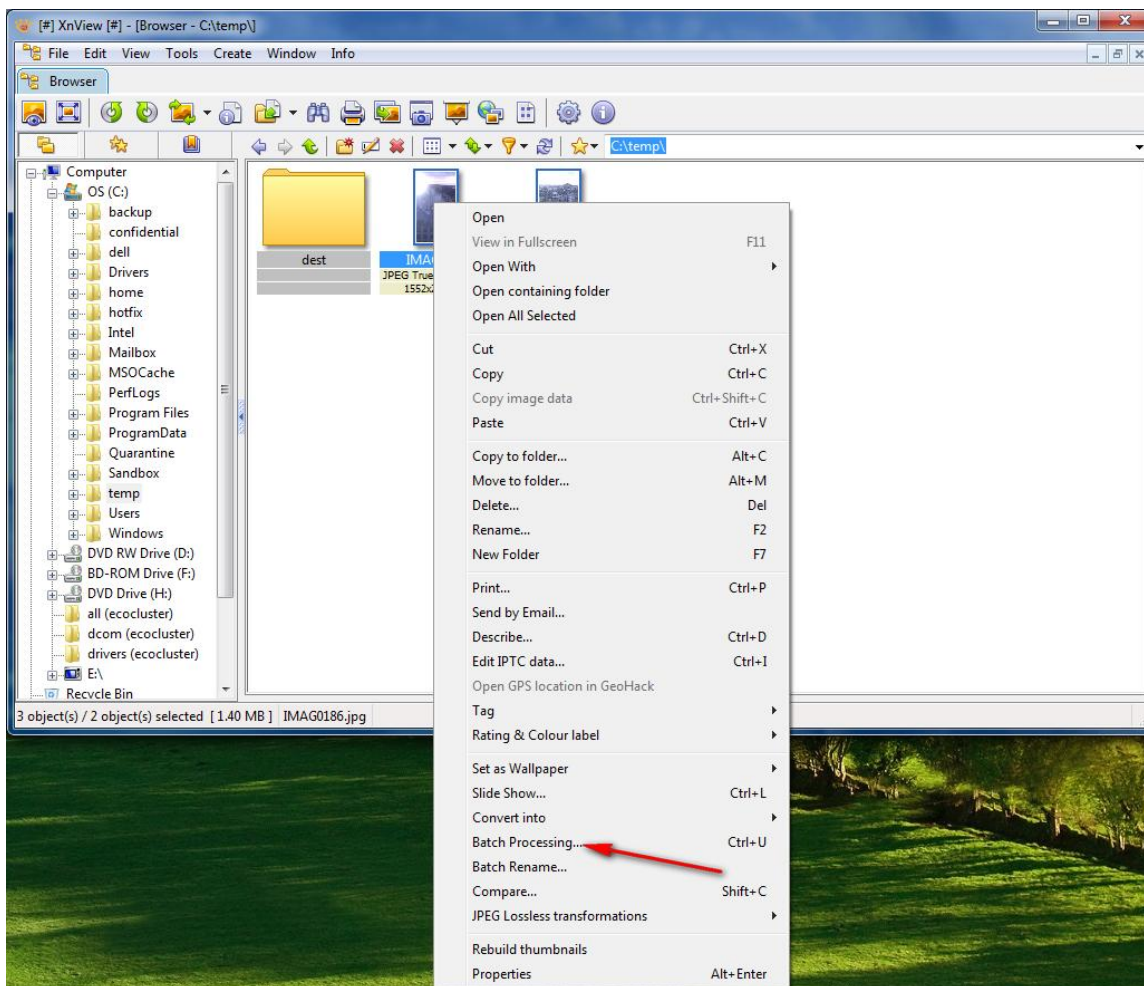
Nous avons trouvé plusieurs logiciels gratuits capables d'effacer ces données. L'un d'eux fonctionne sur Microsoft Windows et Apple Mac : xnview (<http://www.xnview.com/>)

xnview

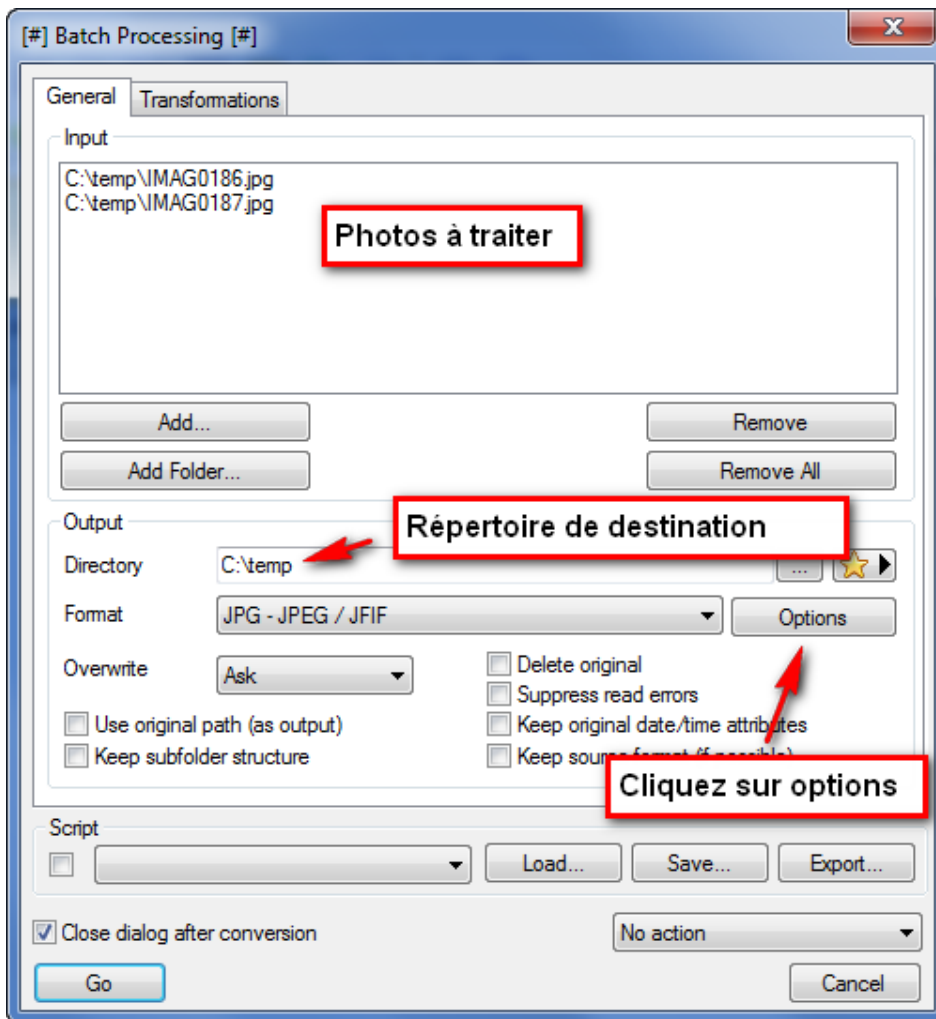
Après installation du logiciel, il suffit de choisir dans la navigation le répertoire contenant les photos incriminées :



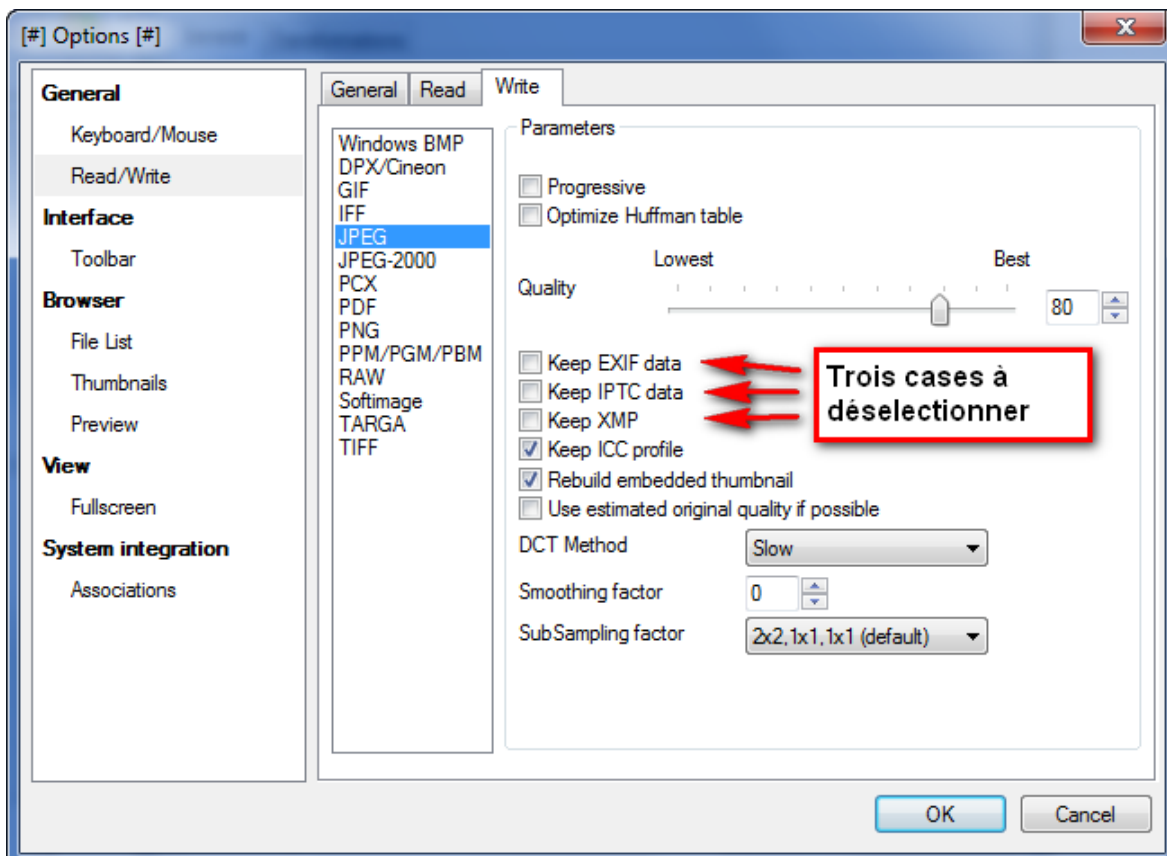
Sélectionnez les photos que vous voulez assainir et faites un click droit pour ouvrir le menu contextuel.



Sélectionnez « batch processing ».

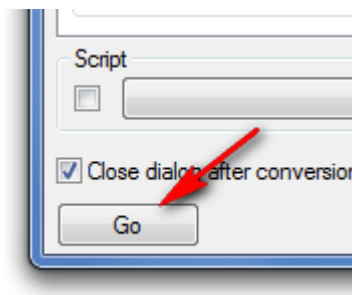


Cliquez sur « options ».

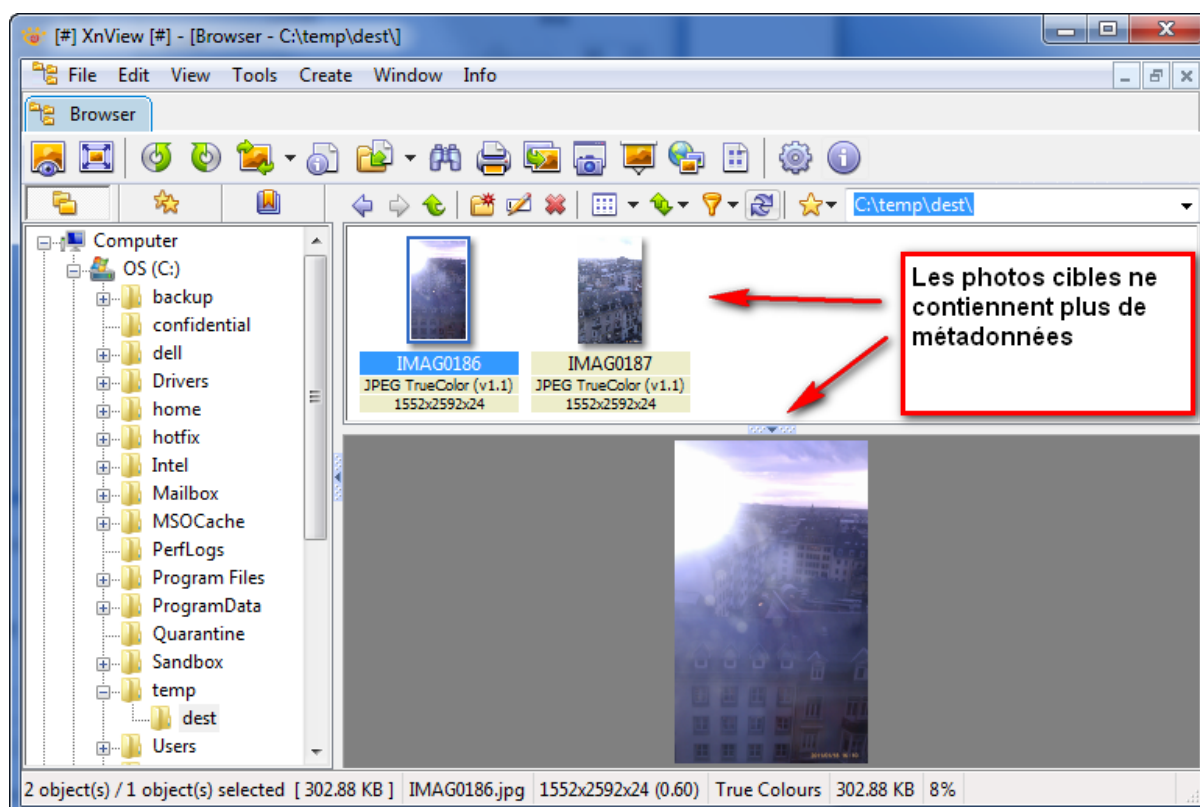


Désélectionnez les trois cases EXIF, IPTC et XMP qui sont les trois différents types de métadonnées dans les photos JPEG.

Cliquez « Ok » puis « GO » :



Le logiciel copiera les photos dans le répertoire de destination sans les métadonnées.



Documents Microsoft Office

Les documents Microsoft Office peuvent contenir des données cachées comme :

- les auteurs d'un document,
- des commentaires,
- des parties effacées du document,
- des parties d'autres documents.

Nous n'entrerons pas dans le détail de l'effacement de ces données car l'aide en ligne de Microsoft Office est excellente. Nous vous invitons donc à visiter le lien suivant qui contient toutes les informations nécessaires pour effacer les métadonnées des documents Microsoft Office :

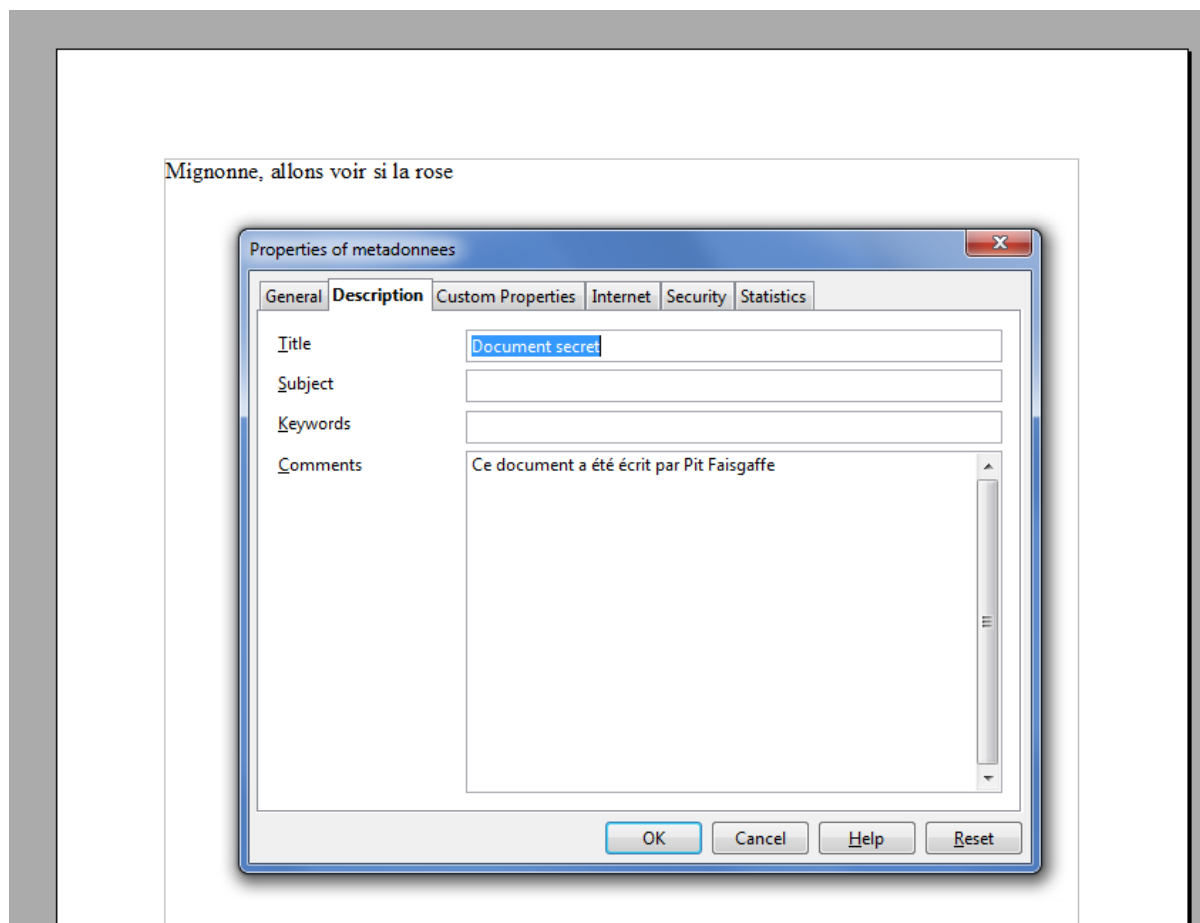
<https://office.microsoft.com/fr-fr/word-help/inspecter-des-documents-a-la-recherche-de-donnees-masquees-et-d-informations-personnelles-HA010074435.aspx>

Documents de type OpenDocument (OpenOffice, LibreOffice, etc.)

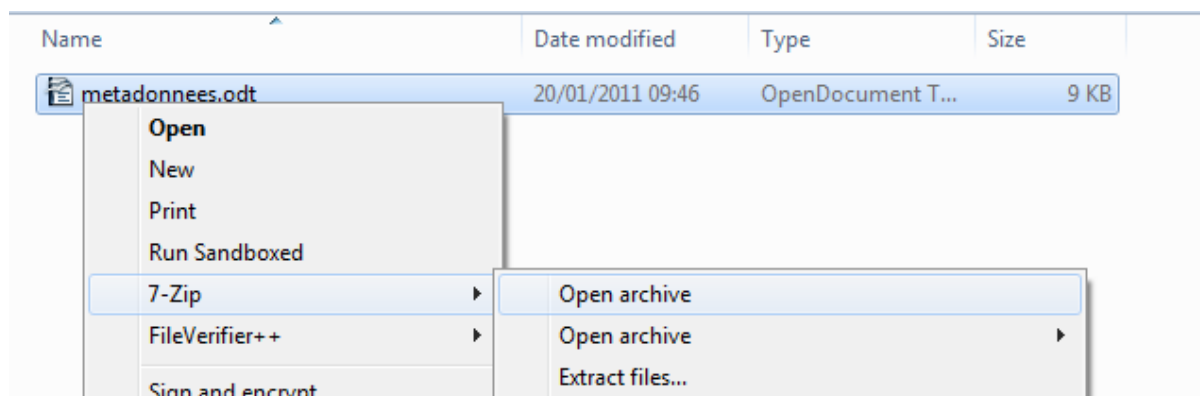
Dans les documents OpenDocument il existe deux types de données cachées : les métadonnées et les informations de suivi des modifications. Pour les effacer il faut d'abord comprendre que les documents OpenDocument sont des archives « zip ».

Effacer les métadonnées

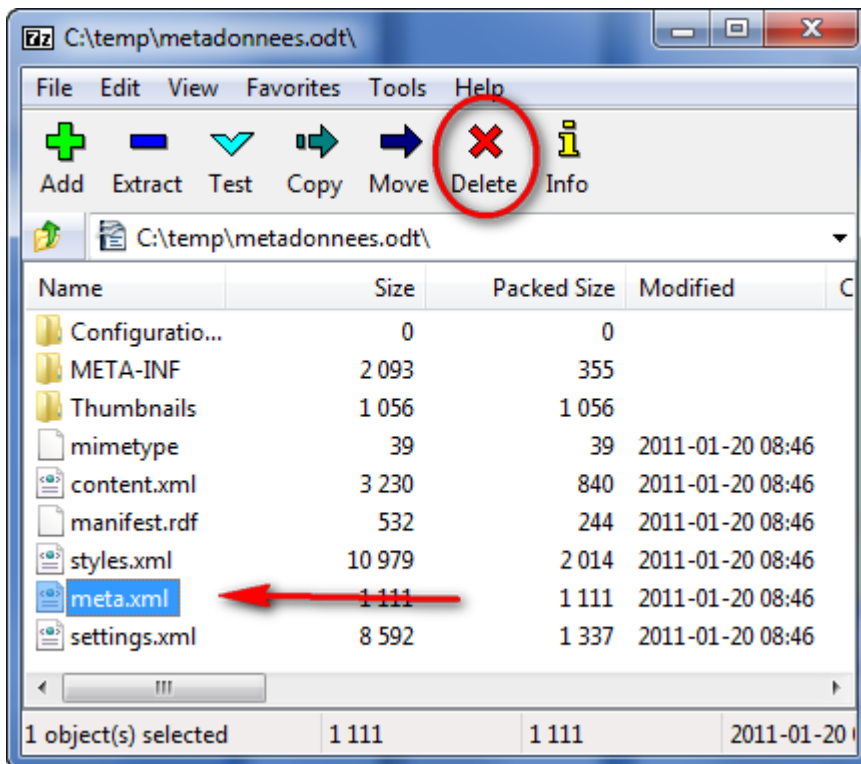
Effacer les métadonnées est assez simple, il suffit d'utiliser un logiciel de compression adéquat. Pour les besoins de cet exemple nous allons utiliser « 7-zip » qui est un logiciel libre disponible sur <http://www.7-zip.org/> . Nous avons testé d'autres logiciels d'archivage qui ont corrompu les documents manipulés, nous attirons votre attention sur le fait que l'explication ci-dessous ne fonctionne pas avec tous les logiciels de ce type.



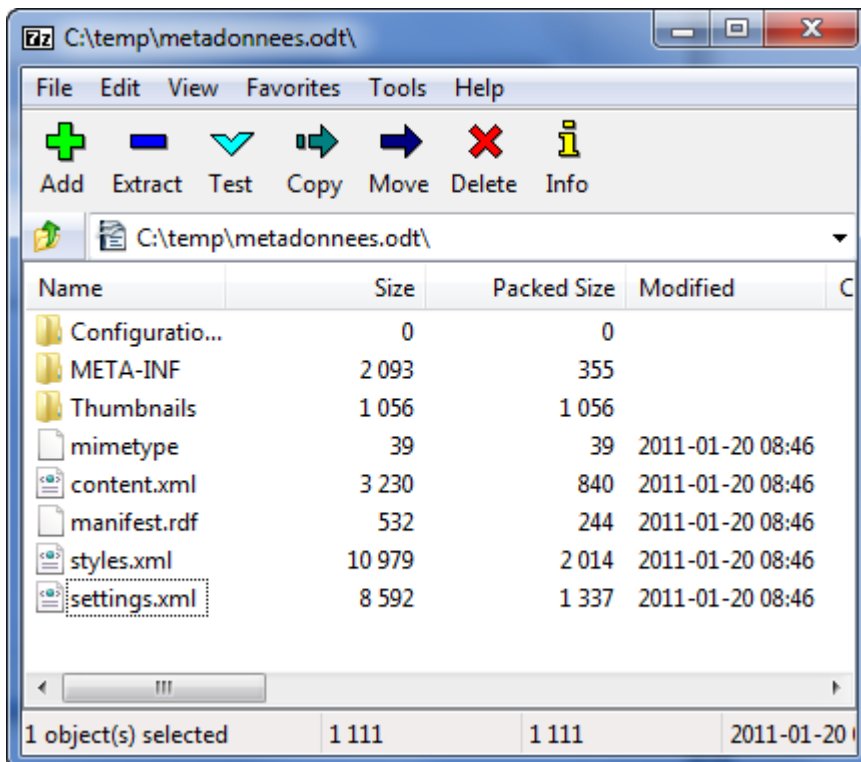
Faites d'abord un click droit sur le fichier pour ouvrir le menu contextuel.



Puis sélectionnez « 7-Zip->Open Archive » cela va ouvrir une nouvelle fenêtre avec le contenu de l'archive.

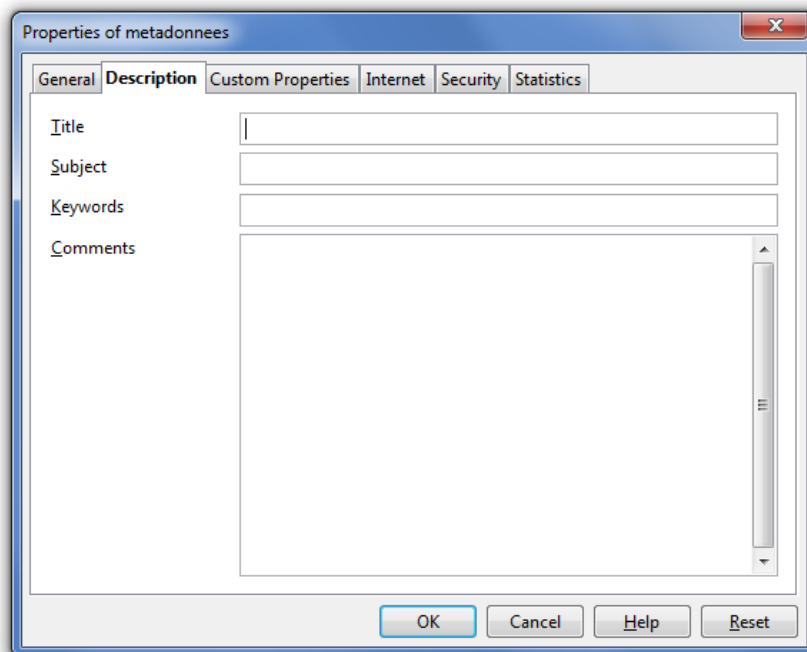


Sélectionnez le fichier « meta.xml » et effacez le à l'intérieur de l'archive.



Vous pouvez maintenant fermer la fenêtre et charger le document dans office.

Mignonne, allons voir si la rose



Comme vous pouvez le constater les métadonnées ont disparu.

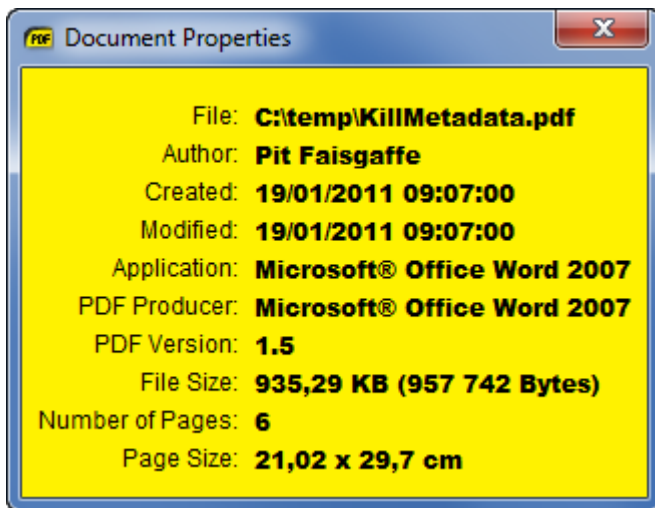
Effacer les données de suivi de modifications

Malheureusement, les données de suivi de modifications ne sont pas enregistrées dans un fichier central comme les métadonnées et nous n'avons pas trouvé de moyen technique permettant d'effacer simplement ces données. Nous vous proposons soit de ne pas utiliser cette option, soit d'enlever ces données en enregistrant le fichier dans un format alternatif comme « rtf » (textes) ou « csv » (tableur) puis de les reconverter en OpenDocument. Attention cette dernière méthode risque de vous faire perdre certaines propriétés du document comme la mise en page par exemple.

Documents PDF

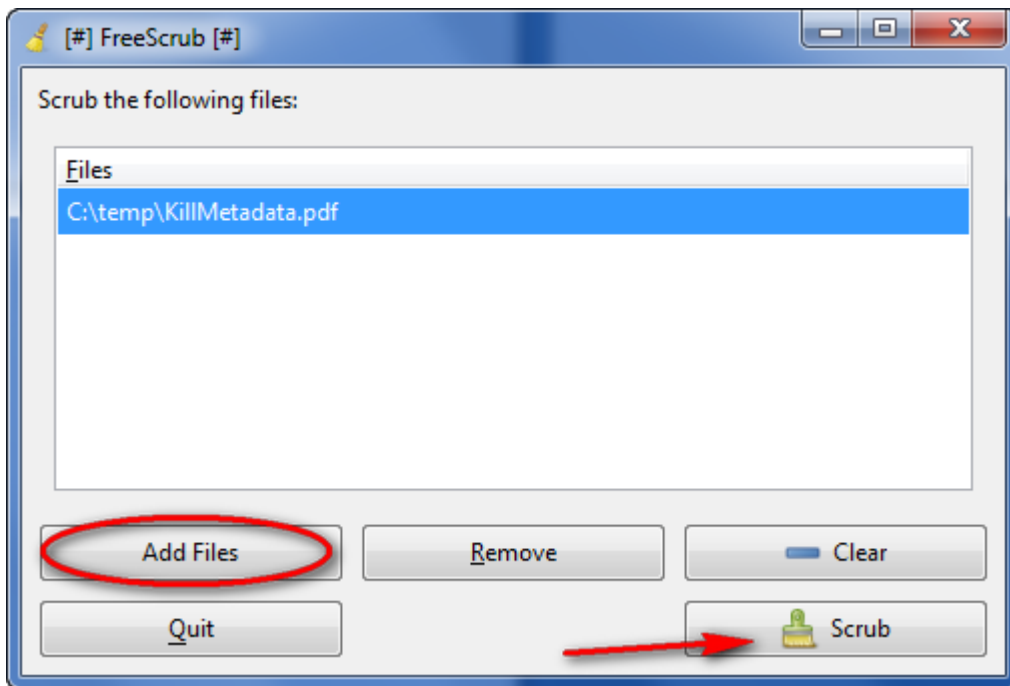
Les documents PDF contiennent souvent au moins le nom du créateur du fichier. Même si vous utilisez une un pilote d'imprimante PDF, celui-ci introduit souvent votre identifiant dans le document.

Dans le cas présent, nous avons un PDF créé à partir de Microsoft Word. Comme vous pouvez le constater, les métadonnées du document originel ont été copiées dans le PDF créé.



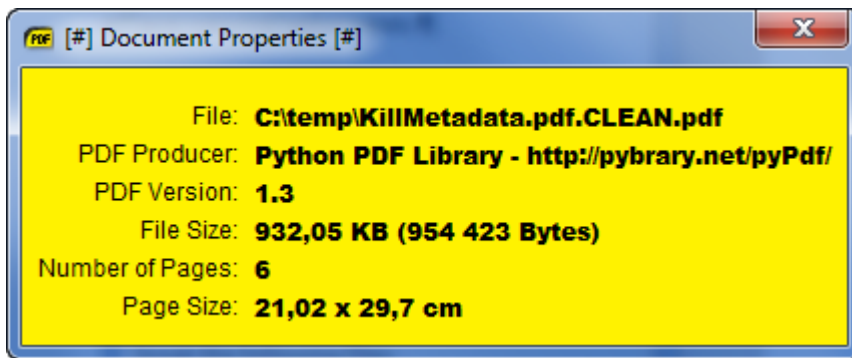
Attention, si vous n'avez pas d'éditeur PDF comme Adobe Acrobat vous ne pourrez pas effacer ces métadonnées.

Nous avons heureusement trouvé une petite application qui s'en charge. L'application s'appelle « FreeScrub » et est disponible à l'adresse <https://github.com/mikm/FreeScrub>.



Ce petit programme est assez simple, il suffit d'ajouter les fichiers que vous voulez nettoyer à l'aide du bouton « Add Files », puis de les nettoyer avec « Scrub ». Les auteurs affirment que leur application fonctionne pour les formats image JPEG, TIFF et PNG ainsi que PDF et veulent étendre leur application à d'autres formats dans le futur.

Toutefois, « FreeScrub » n'est pas très stable et une erreur est apparue lors de nos tests, un fichier à l'extension « .CLEAN » a néanmoins été créé dans le répertoire d'origine. Après avoir renommé ce fichier en lui donnant l'extension « .pdf » nous avons pu constater que les métadonnées avaient bien été enlevées.



Le mot de la fin

Nous avons essayé de présenter ici certaines méthodes possibles pour l'effacement des données cachées dans différents types de fichiers. Il est possible que certains logiciels payants soient plus efficaces ; nous nous sommes contentés ici de présenter des outils gratuits, si ce n'est libres.

D'autres types de fichiers, comme les vidéos par exemple, peuvent aussi contenir des métadonnées. Si vous avez peur de la fuite d'informations non contrôlée, il est toujours intéressant de s'informer au préalable sur le contenu éventuel des données cachées.

Si vous trouvez d'autres solutions, nous sommes ouverts à tout commentaire ou critique, n'hésitez pas à nous contacter.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu