

# Cacher des fichiers dans une image

Vous avez un texte ou un fichier secret à faire parvenir à un ami ? Vos emails sont surveillés ? Vous pouvez bien sûr le crypter afin de le protéger contre les regards indiscrets.

Le problème est que ce fichier existe et laisse des traces, même s'il est crypté. Pour plus de sécurité, **vous pouvez le cacher au sein d'une image**. C'est ce qu'on appelle la **stéganographie**. Les pixels du texte à cacher sont codés, cryptés et dilués dans les pixels de l'image. Ainsi, vos données sensibles n'attirent pas l'attention.

Malgré cette transformation, l'apparence de l'image demeure inchangée aux yeux de l'observateur. Tout repose sur l'incapacité de l'oeil humain à visualiser dans une image la modification des bits de poids faibles ayant servis à la nouvelle codification des octets d'un pixel donné. De plus l'image avec le texte caché ne change pas de taille.

Qui pourrait alors se douter qu'un texte est caché dans une image ?



Notez que cette méthode peut également vous permettre **d'apposer**

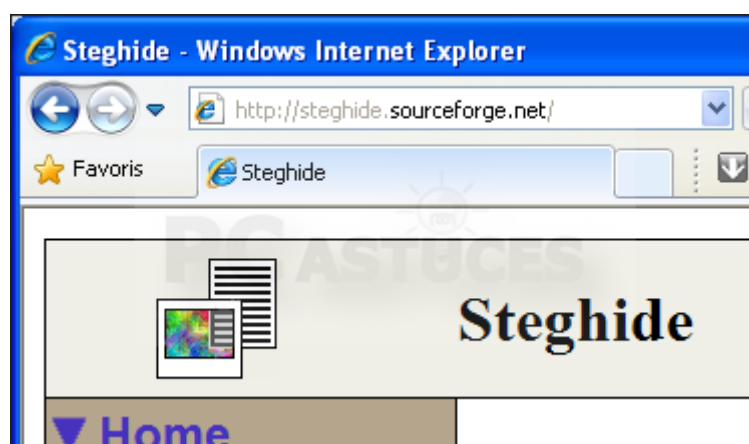
**une signature cachée dans vos images et photos** (watermark) afin de faire valoir vos droits d'auteur, de cacher des informations sensibles sur votre ordinateur ou même si un site Web (un mot de passe par exemple).

Le logiciel libre Steghide va vous permettre cacher un fichier ou un message texte dans une image (BMP ou JPG) ou un fichier son (WAV) et de le crypter. Le guide pour Windows et Linux.

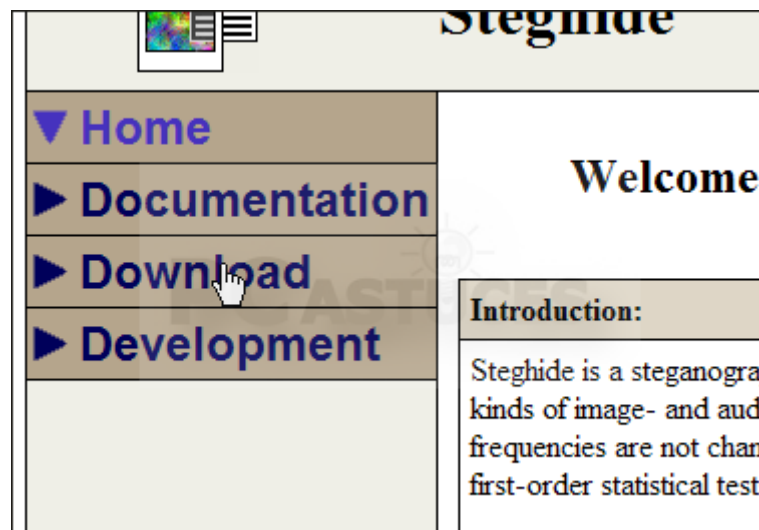
### **Télécharger et décompresser Steghide avec Windows**

Steghide est un logiciel OpenSource disponible pour Windows et Linux. Vous pouvez le télécharger sur la bibliothèque OpenSource SourceForce.

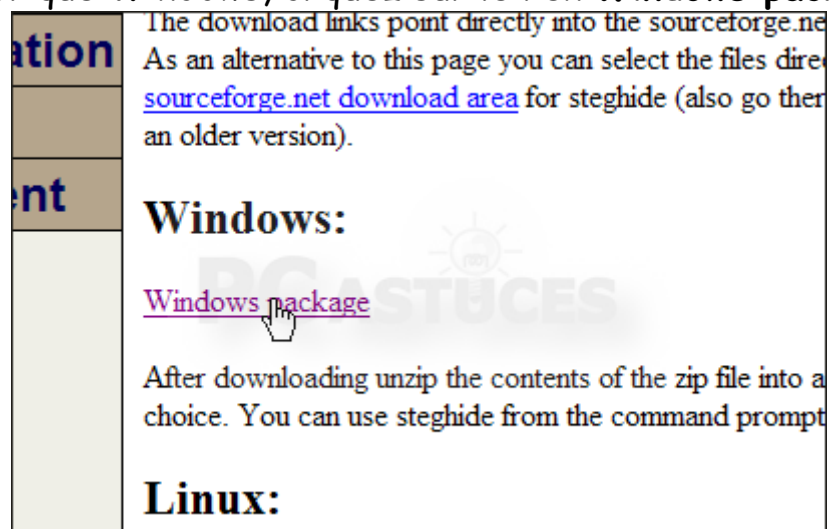
Rendez-vous à l'adresse <http://steghide.sourceforge.net/>



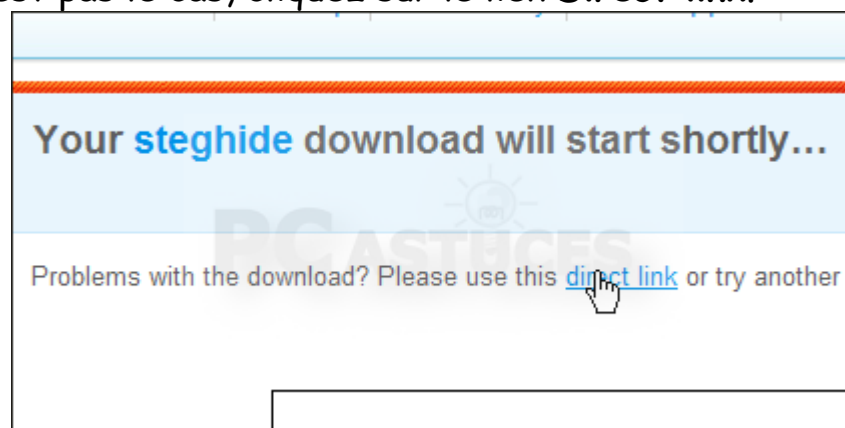
Cliquez sur le menu **Download**.



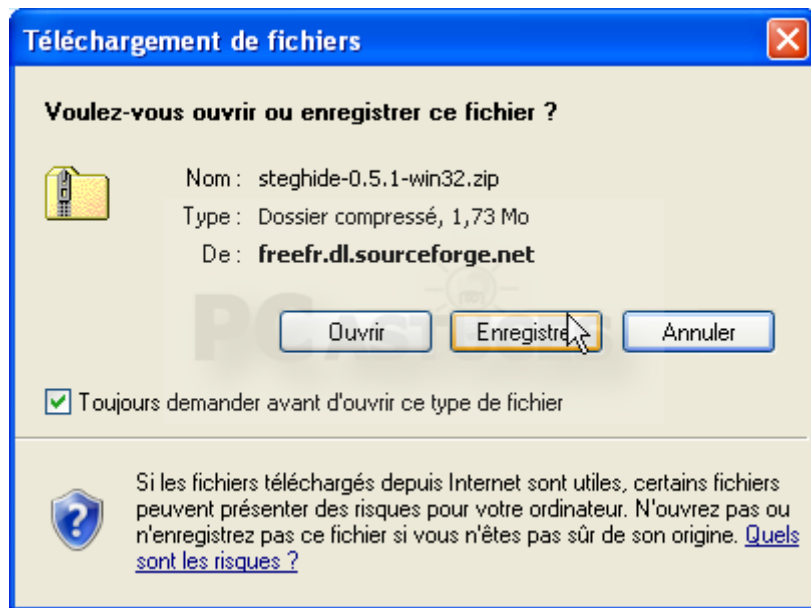
Dans la rubrique Windows, cliquez sur le lien **Windows package**.



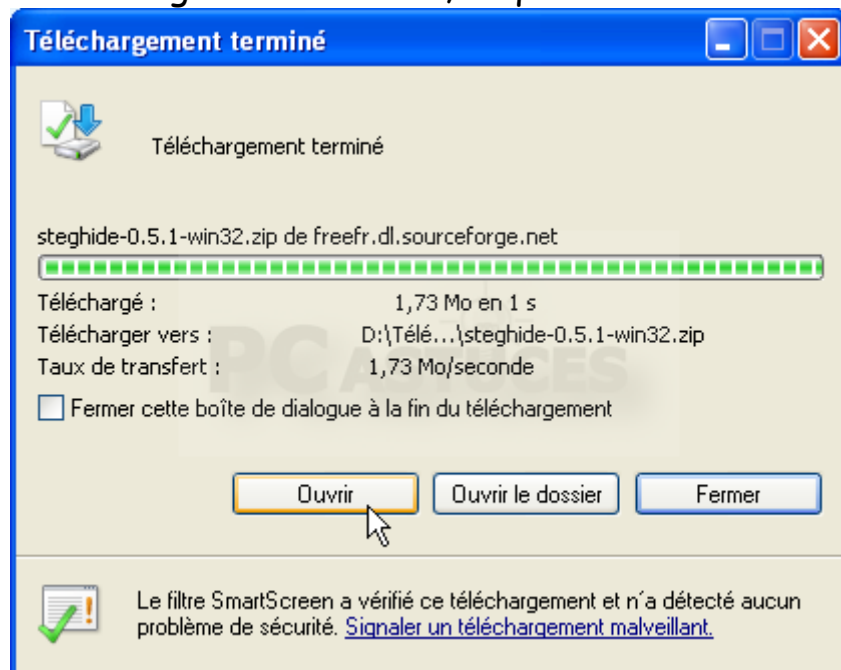
Après quelques secondes, le téléchargement de Steghide commence. Si cela n'est pas le cas, cliquez sur le lien **Direct link**.



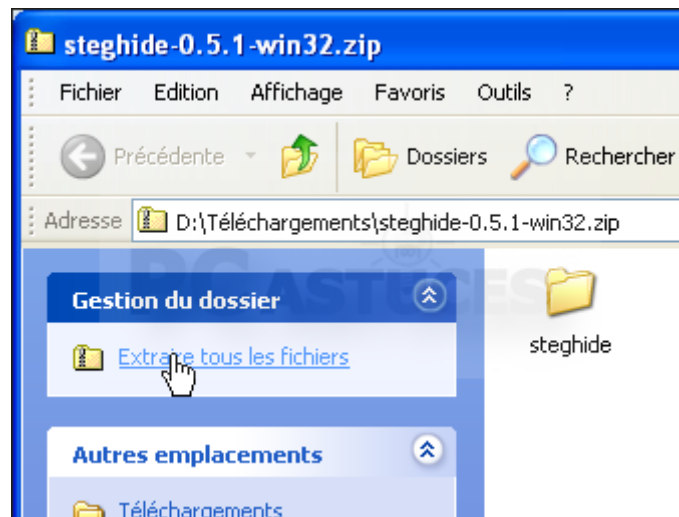
Cliquez sur le bouton **Enregistrer**.



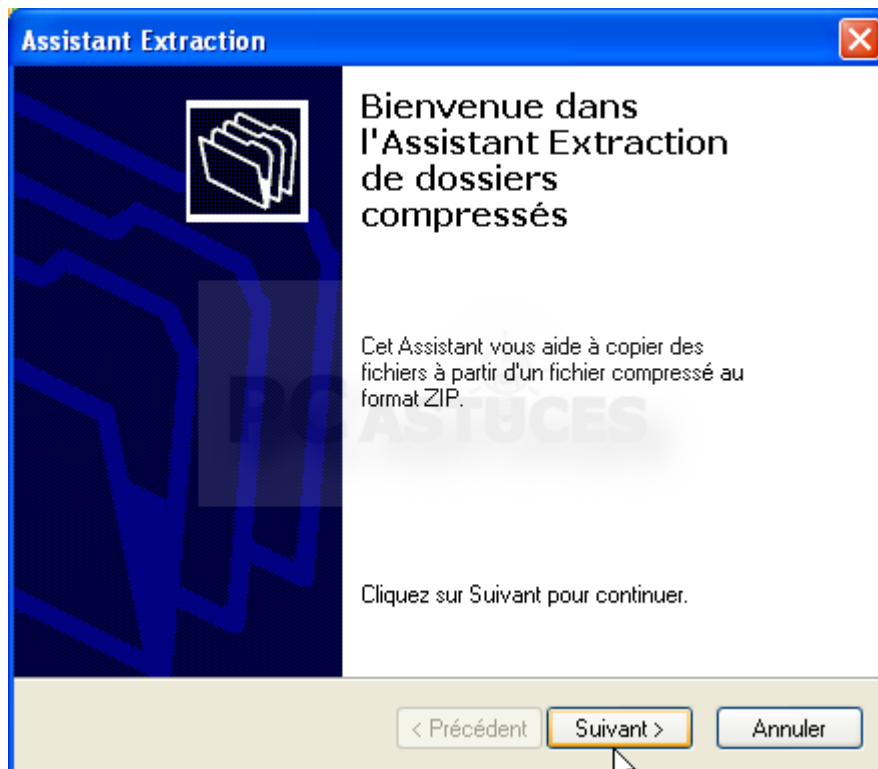
Une fois le téléchargement terminé, cliquez sur le bouton **Ouvrir**.



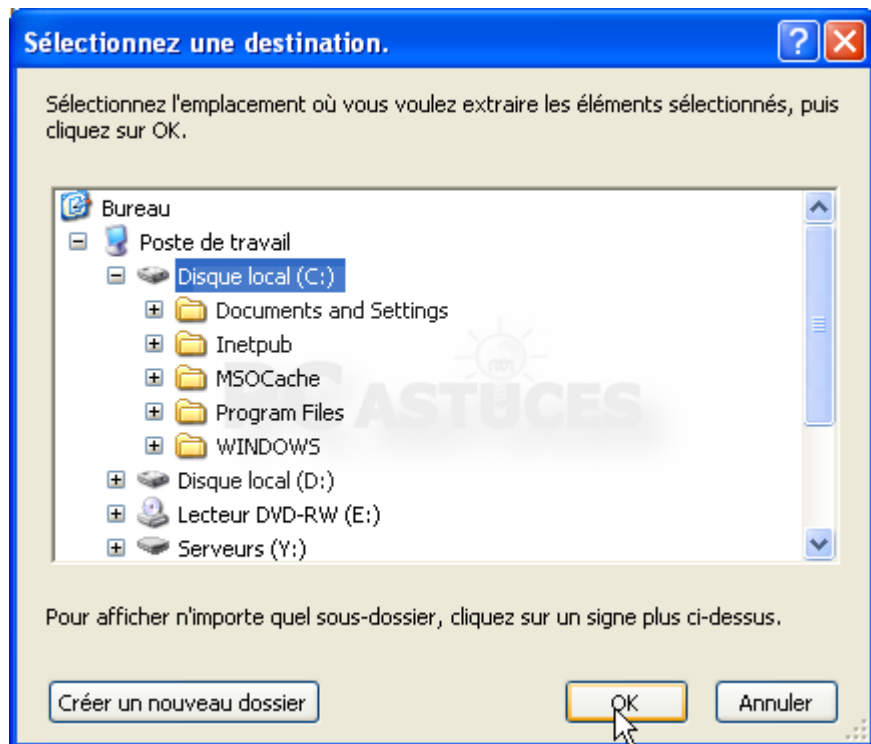
Cliquez sur le lien **Extraire tous les fichiers**.



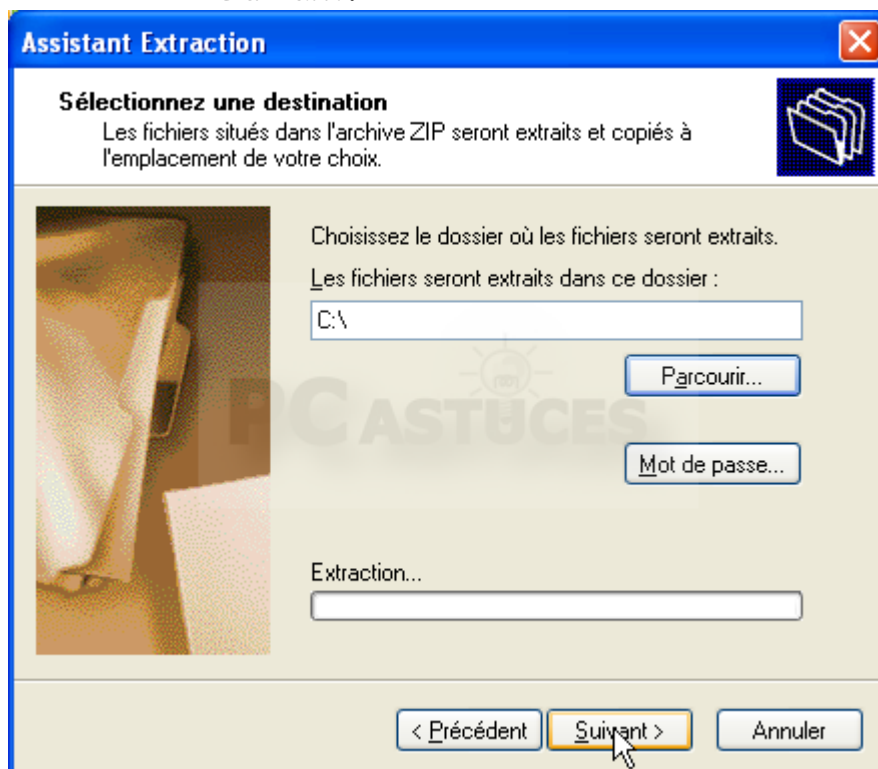
Cliquez sur le bouton **Suivant**.



Cliquez sur le bouton **Parcourir** et sélectionnez la racine de votre disque dur (C:\ par exemple). Cliquez sur le bouton **Ouvrir**.



Cliquez sur le bouton **Suivant**.



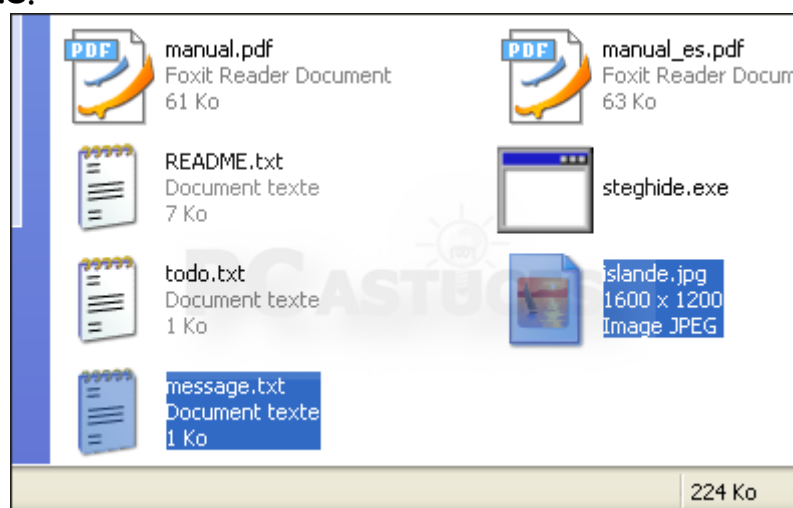
Une fois les fichiers décompressés, cliquez enfin sur le bouton **Terminer**.



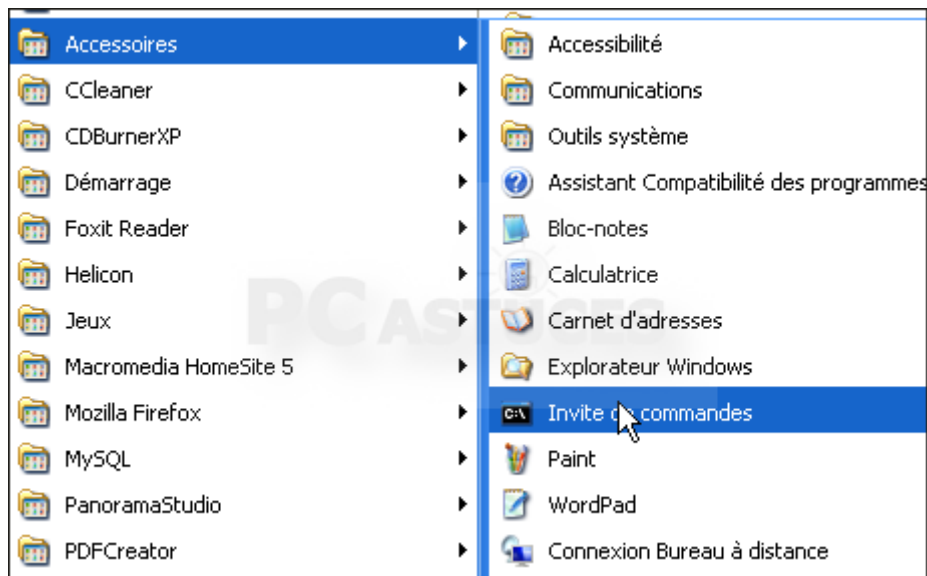
## Cacher un élément dans une image avec Windows

StegHide fonctionne en ligne de commandes et est assez simple à utiliser.

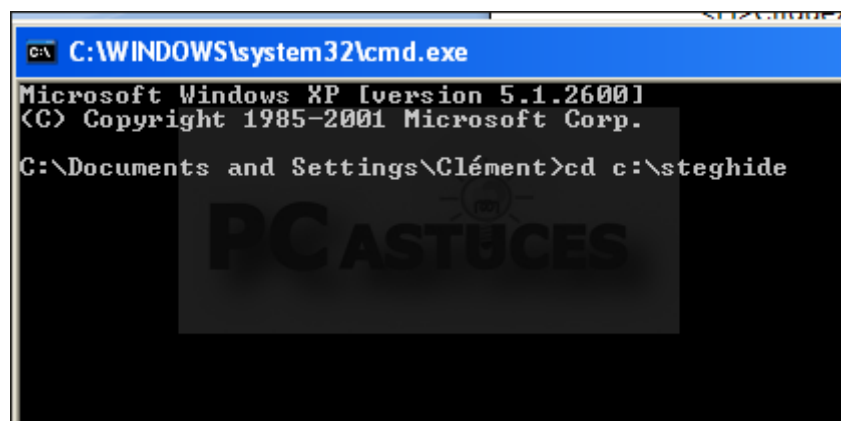
Si vous ne maîtrisez pas la navigation dans les dossiers en ligne de commandes, copiez dans un premier temps le fichier que vous souhaitez cacher et l'image dans laquelle le cacher dans le dossier **C:\StegHide**.



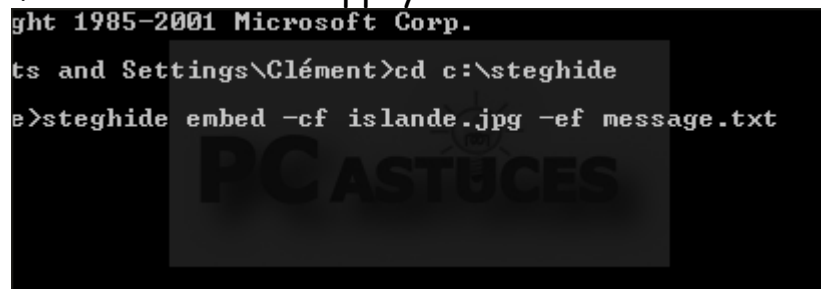
Cliquez sur le bouton **Démarrer**, sur **Tous les programmes**, sur **Accessoires** puis sur **Invite de commandes**.



Saisissez la commande **cd C:\steghide** et appuyez sur la touche **Entrée**.



Saisissez alors la commande **steghide embed -cf islande.jpg -ef message.txt** en remplaçant **islande.jpg** par le chemin complet fichier image à utiliser comme cachette et **message.txt** par le chemin complet du fichier à cacher. Appuyez sur la touche **Entrée**.





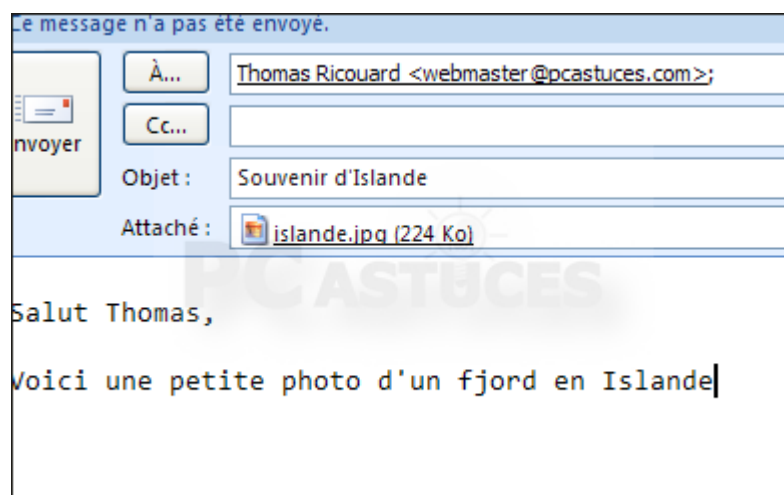
Le fichier caché étant crypté, saisissez un mot ou une phrase secrète. Elle vous sera nécessaire pour récupérer le fichier. Appuyez sur la touche **Entrée** et saisissez de nouveau votre phrase secrète.

```
C:\steghide>steghide embed -cf islande.jpg
Entrez la passphrase:
Entrez à nouveau la passphrase:
```

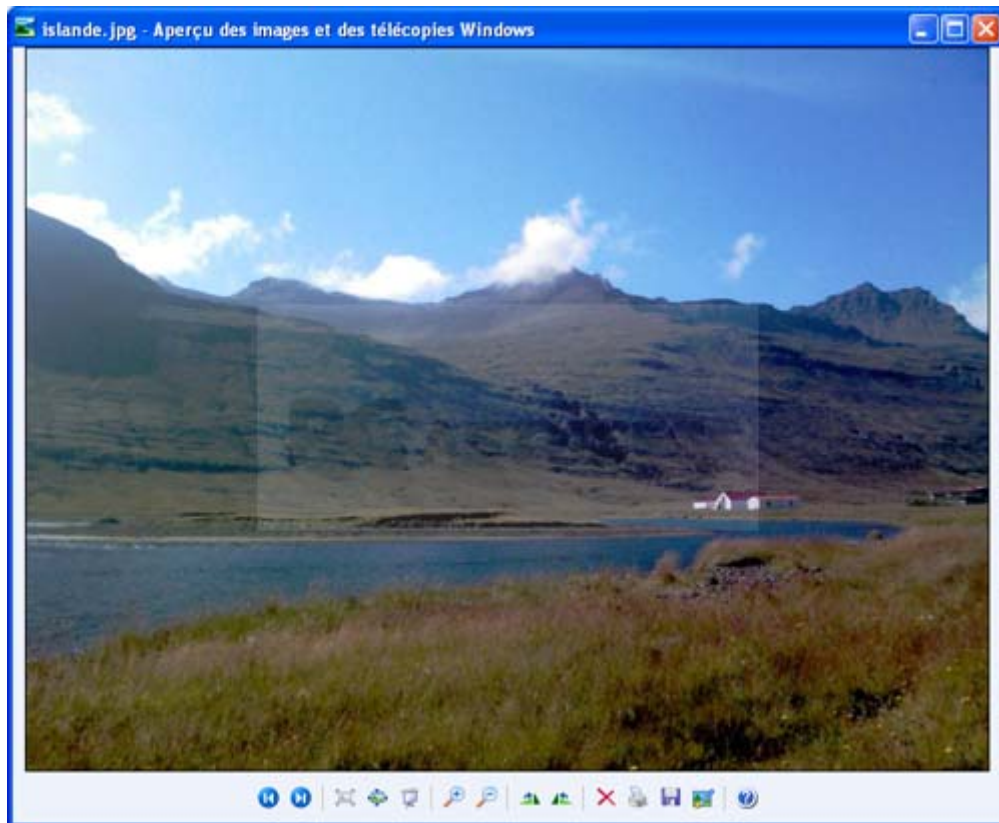
Le fichier est alors camouflé dans l'image.

```
C:\steghide>steghide embed -cf islande.jpg -er message.txt
Entrez la passphrase:
Entrez à nouveau la passphrase:
camouflage des données de "message.txt" dans "islande.jpg". terminé.
C:\steghide>
```

Vous pouvez alors envoyer l'image à votre ami ou bien la mettre à sa disposition sur Internet par exemple.



Aux yeux de tous, l'image est affichée normalement.



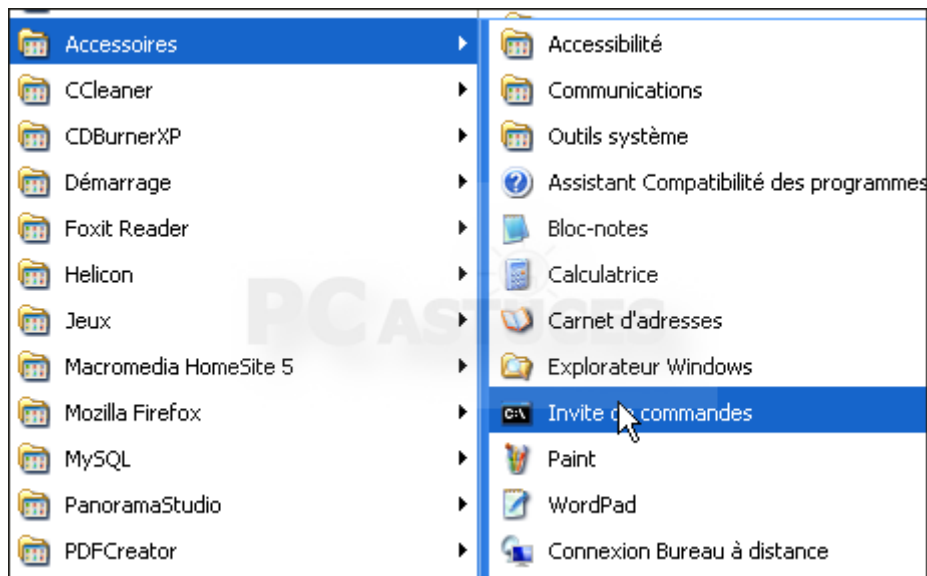
## Améliorer le cryptage

Par défaut, un cryptage 128 bits est utilisé pour protéger votre fichier caché. Pour plus de sécurité vous pouvez utiliser un cryptage plus fort de 256 bits : blowfish, cast-256. Pour connaître la liste des algorithmes de cryptage supportés, saisissez la commande **steghide encinfo**. Rajoutez ensuite le paramètre **-e blowfish** à la commande de camouflage pour utiliser un autre algorithme de cryptage (ici blowfish).

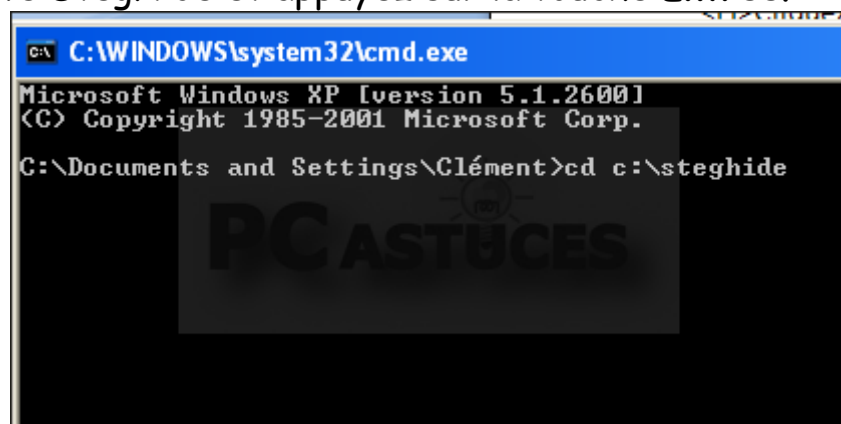
## Récupérer l'élément caché avec Windows

Pour récupérer un élément caché dans une image, vous avez bien sûr besoin de StegHide et de la phrase secrète utilisée lors du camouflage.

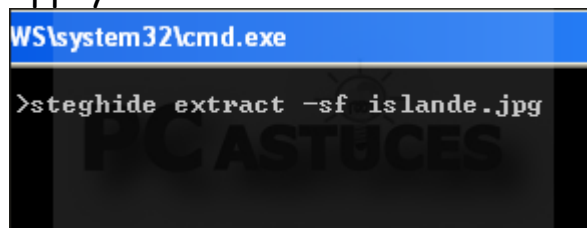
Ouvrez une fenêtre d'invite de commandes : cliquez sur le bouton **Démarrer**, sur **Tous les programmes**, sur **Accessoires** puis sur **Invite de commandes**.



Saisissez la commande **cd C:\steghide** pour basculer dans le dossier où se trouve StegHide et appuyez sur la touche **Entrée**.



Saisissez alors la commande **steghide extract -sf islande.jpg** en remplaçant islande.jpg par le chemin complet du fichier image utilisé comme cachette. Appuyez sur la touche **Entrée**.



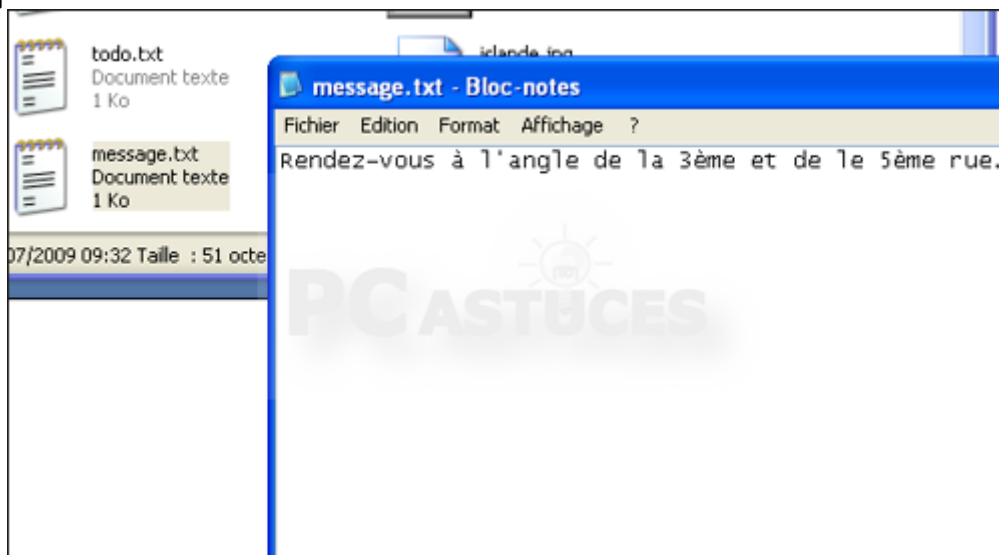
Saisissez le mot où la phrase secrète utilisé pour crypter le fichier caché et appuyez sur **Entrée**.

```
C:\WINDOWS\system32\cmd.exe - steghide extract -s
C:\steghide>steghide extract -sf islande.jpg
Entrez la passphrase: _
```

Le fichier caché est alors extrait.

```
C:\steghide>steghide extract -sf islande.jpg
Entrez la passphrase:
écriture des données extraites dans "message.txt".
C:\steghide>_
```

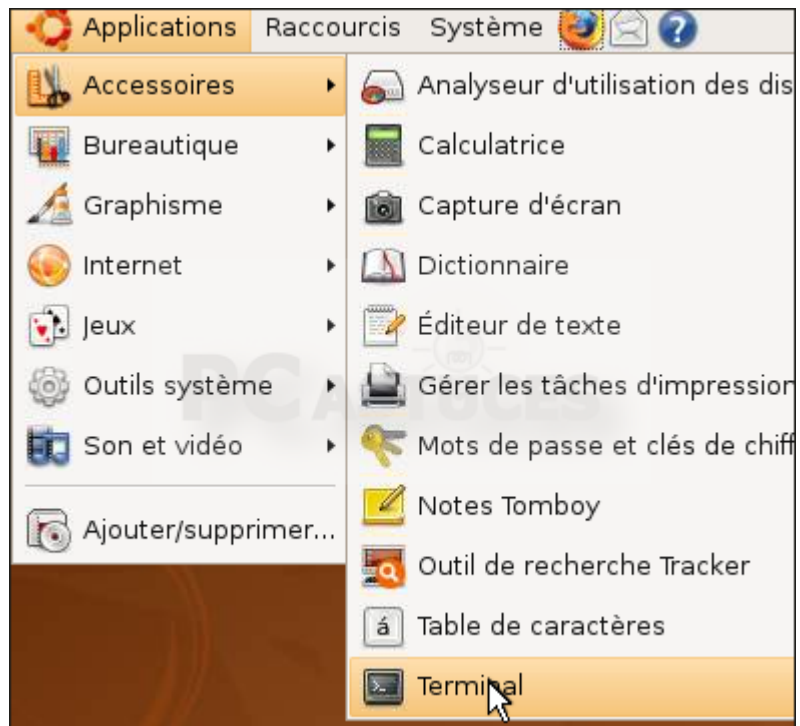
Vous pouvez l'ouvrir normalement.



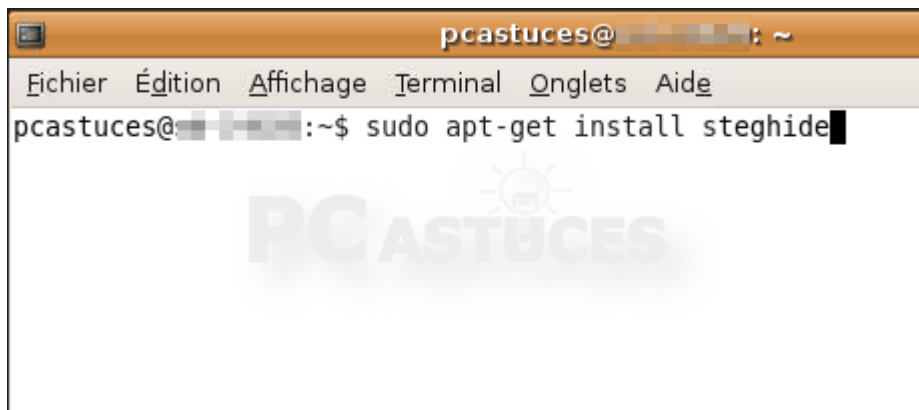
## Télécharger et installer StegHide avec Linux

Vous pouvez facilement télécharger et installer StegHide avec le gestionnaire de paquets APT.

Ouvrez un terminal en cliquant sur le menu **Applications**, sur **Accessoires** puis sur **Terminal**.



Saisissez la commande **sudo apt-get install steghide** et pressez la touche **Entrée**.



Saisissez votre mot de passe.  
Appuyez sur la lettre **O** et pressez la touche **Entrée**.

```

Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libmccrypt4 libmhash2
Paquets suggérés :
  libmccrypt-dev mccrypt
Les NOUVEAUX paquets suivants seront installés :
  libmccrypt4 libmhash2 steghide
0 mis à jour, 3 nouvellement installés, 0 à enlever et 92 non mis à jour.
Il est nécessaire de prendre 392ko dans les archives.
Après cette opération, 1200ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer [O/n] ?

```

StegHide est alors téléchargé et installé.

```

Souhaitez-vous continuer [O/n] ? O
Réception de : 1 http://fr.archive.ubuntu.com hardy/universe libmccrypt4
[79,2kB]
Réception de : 2 http://fr.archive.ubuntu.com hardy/main libmhash2
B]
Réception de : 3 http://fr.archive.ubuntu.com hardy/universe steghide
80kB]
392ko réceptionnés en 0s (1653ko/s)
Sélection du paquet libmccrypt4 précédemment désélectionné.
(Lecture de la base de données... 89140 fichiers et répertoires déjà
Dépaquetage de libmccrypt4 (à partir de ../libmccrypt4_2.5.7-5_i386
Sélection du paquet libmhash2 précédemment désélectionné.
Dépaquetage de libmhash2 (à partir de ../libmhash2_0.9.9-1_i386.de
Sélection du paquet steghide précédemment désélectionné.
Dépaquetage de steghide (à partir de ../steghide_0.5.1-8_i386.deb)
Paramétrage de libmccrypt4 (2.5.7-5) ...

Paramétrage de libmhash2 (0.9.9-1) ...

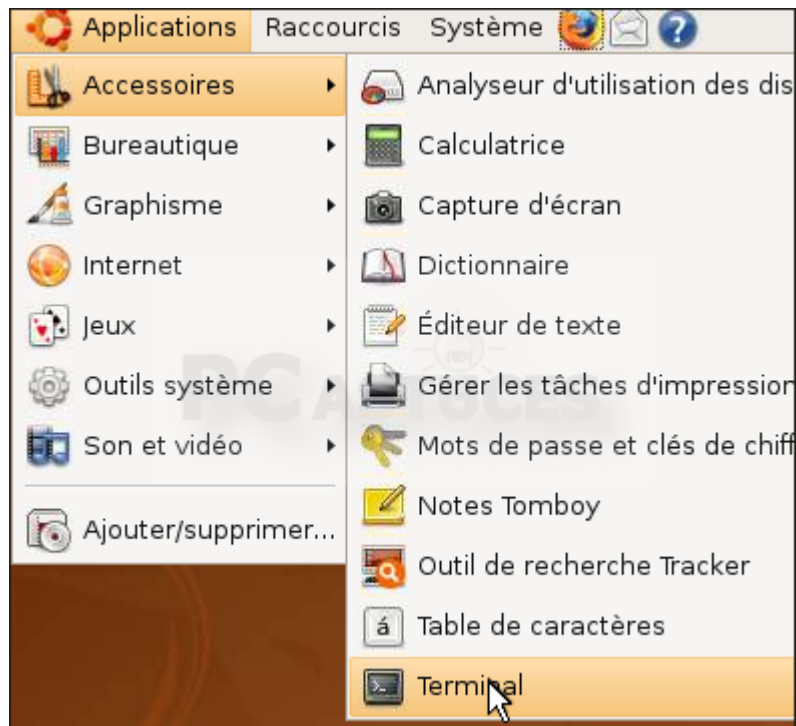
Paramétrage de steghide (0.5.1-8) ...
Processing triggers for libc6 ...
ldconfig deferred processing now taking place
pcastuces@~$

```

## Cacher un élément dans une image avec Linux

StegHide fonctionne en ligne de commandes et est assez simple à utiliser.

Ouvrez un terminal en cliquant sur le menu **Applications**, sur **Accessoires** puis sur **Terminal**.



Saisissez alors la commande **steghide embed -cf**  
**/home/pcastuces/Images/maya\_bay.jpg -ef**  
**/home/pcastuces/message.odt** en remplaçant  
 /home/pcastuces/Images/maya\_bay.jpg par le chemin complet  
 fichier image à utiliser comme cachette et  
 /home/pcastuces/message.odt par le chemin complet du fichier à  
 cacher. Appuyez sur la touche **Entrée**.

```
Terminal Onglets Aide
steghide embed -cf /home/pcastuces/Images/maya_bay.jpg -ef
message.odt
passphrase:
de "/home/pcastuces/message.odt" dans "/home/pcastuces/Im
```

Le fichier caché étant crypté, saisissez un mot ou une phrase  
 secrète. Elle vous sera nécessaire pour récupérer le fichier. Appuyez  
 sur la touche **Entrée** et saisissez de nouveau votre phrase secrète.

```
/home/pcastuces/message.odt
Entrez la passphrase:
Entrez à nouveau la passphrase:
camouflage des données de "/home/
```

Le fichier est alors camouflé dans l'image.



```
camouflage des données de "/home/pcastuces/message.odt" dans  
camouflage des données de "/home/pcastuces/message.odt" dans  
ages/maya_bay.jpg". terminé.  
pcastuces@~:~$
```

Vous pouvez alors envoyer l'image à votre ami ou bien la mettre à sa disposition sur Internet par exemple.

Aux yeux de tous, l'image est affichée normalement.



### Améliorer le cryptage

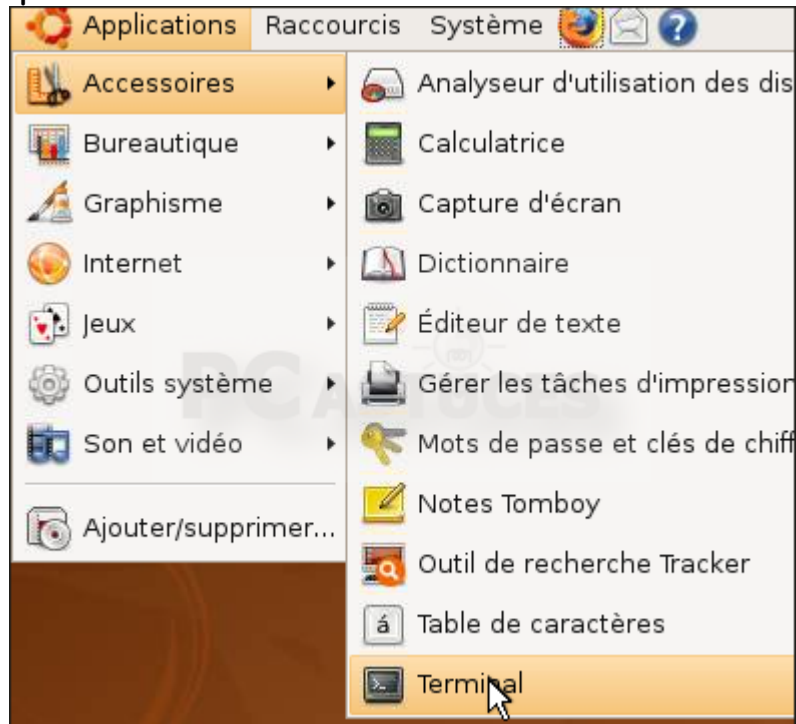
Par défaut, un cryptage 128 bits est utilisé pour protéger votre fichier caché. Pour plus de sécurité vous pouvez utiliser un cryptage plus fort de 256 bits : blowfish, cast-256. Pour connaître la liste des algorithmes de cryptage supportés, saisissez la commande **steghide encinfo**. Rajoutez ensuite le paramètre **-e blowfish** à la commande de camouflage pour utiliser un autre algorithme de cryptage (ici blowfish).



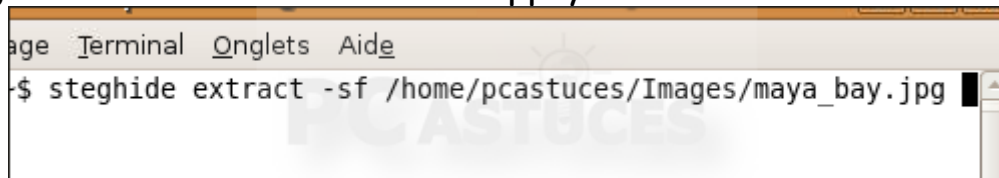
## Récupérer l'élément caché avec Linux

Pour récupérer un élément caché dans une image, vous avez bien sûr besoin de StegHide et de la phrase secrète utilisée lors du camouflage.

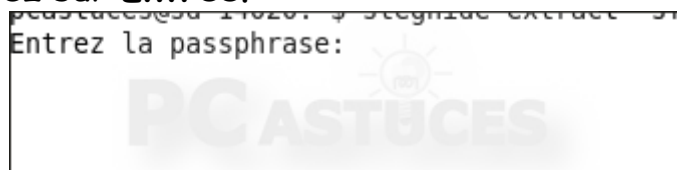
Ouvrez un terminal en cliquant sur le menu **Applications**, sur **Accessoires** puis sur **Terminal**.



Saisissez alors la commande **steghide extract -sf /home/pcastuces/Images/maya\_bay.jpg** en remplaçant **/home/pcastuces/Images/maya\_bay.jpg** par le chemin complet de l'image utilisée comme cachette. Appuyez sur la touche **Entrée**.



Saisissez le mot où la phrase secrète utilisé pour crypter le fichier caché et appuyez sur **Entrée**.



Le fichier caché est alors extrait.

```
écriture des données extraites dans "message.odt".  
pcastuces@~$
```

Vous pouvez l'ouvrir normalement.

