Magic

Éric BERTHOMIER
eric.berthomier@free.fr

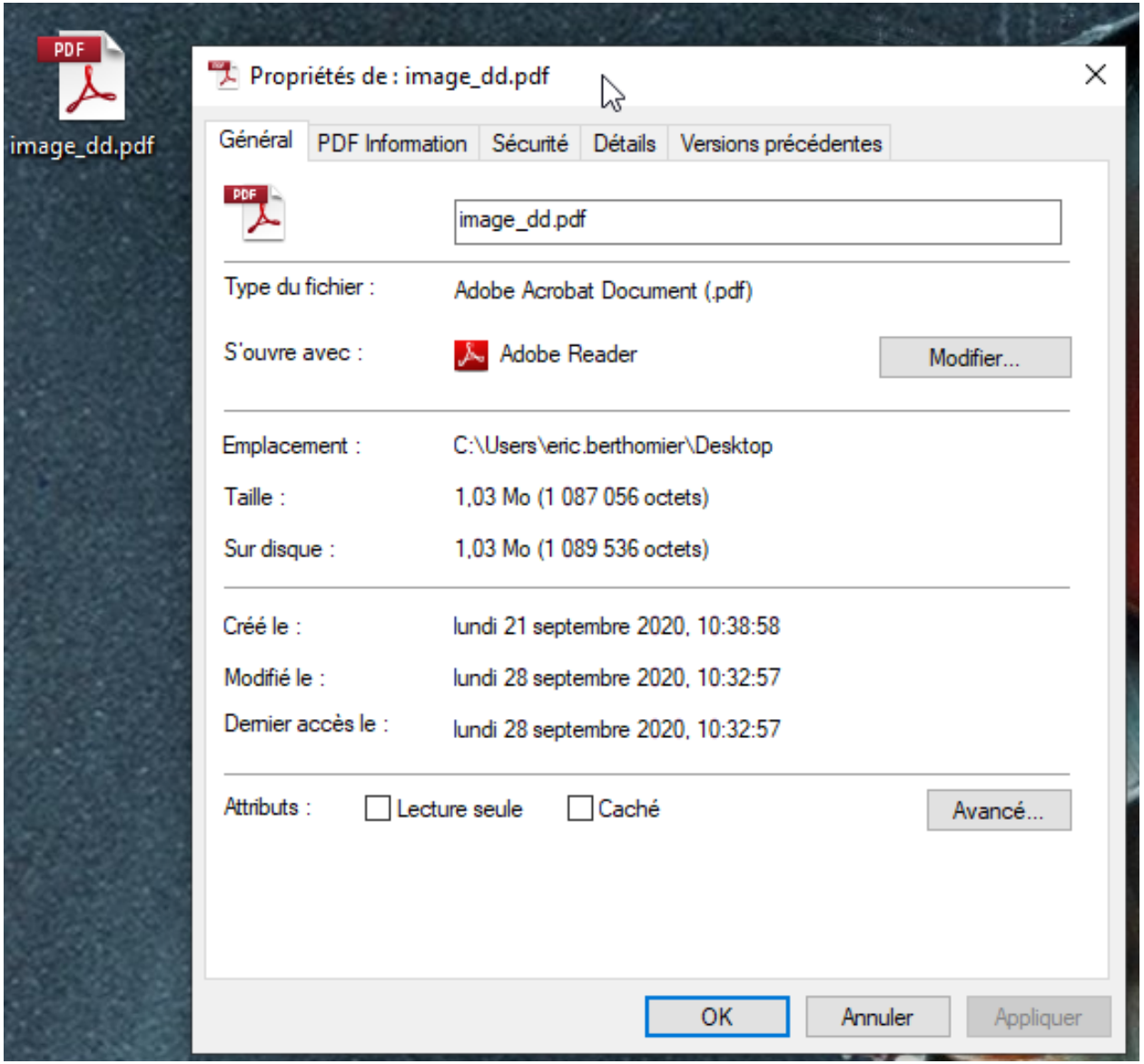
20 juin 2022

Version 1.3 - Version Stagiaire

Quelle icône dois-je associer avec les fichiers ?

Lors de l'utilisation de votre système d'exploitation, la question que ce denier se pose est de connaître l'icône qui doit être associée avec le fichier.

Une question de propriété . . .



Comment ça marche ?

- Lors de l'installation d'une application, cette dernière déclare au système d'exploitation qu'elle peut ouvrir un certain type de fichiers.

Comment ça marche ?

- Lors de l'installation d'une application, cette dernière déclare au système d'exploitation qu'elle peut ouvrir un certain type de fichiers.
- Cette information est enregistrée dans le système et le fichier sera donc ouvert avec l'application déclarée par défaut.

Comment ça marche ?

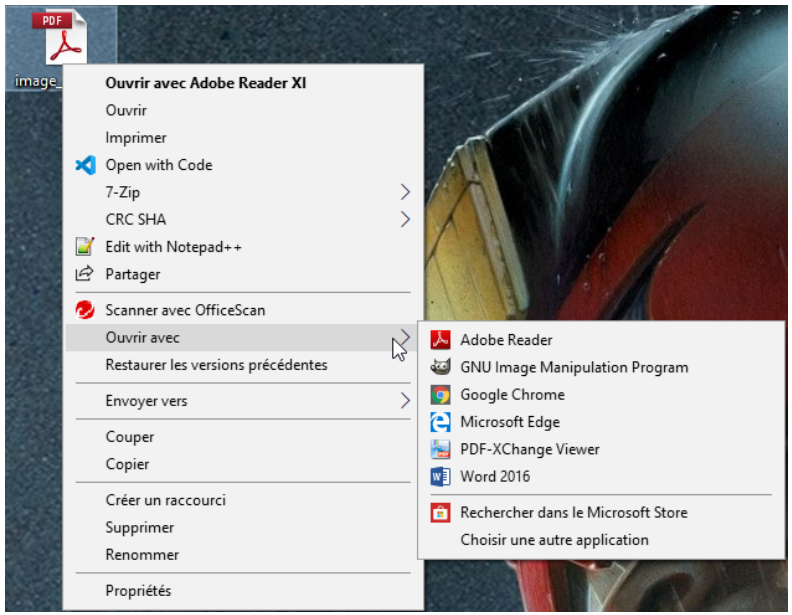
- Lors de l'installation d'une application, cette dernière déclare au système d'exploitation qu'elle peut ouvrir un certain type de fichiers.
- Cette information est enregistrée dans le système et le fichier sera donc ouvert avec l'application déclarée par défaut.
- Les autres applications sont accessibles à l'aide de l'option "Ouvrir avec" (Shift clic-droit)

Comment ça marche ?

- Lors de l'installation d'une application, cette dernière déclare au système d'exploitation qu'elle peut ouvrir un certain type de fichiers.
- Cette information est enregistrée dans le système et le fichier sera donc ouvert avec l'application déclarée par défaut.
- Les autres applications sont accessibles à l'aide de l'option "Ouvrir avec" (Shift clic-droit)

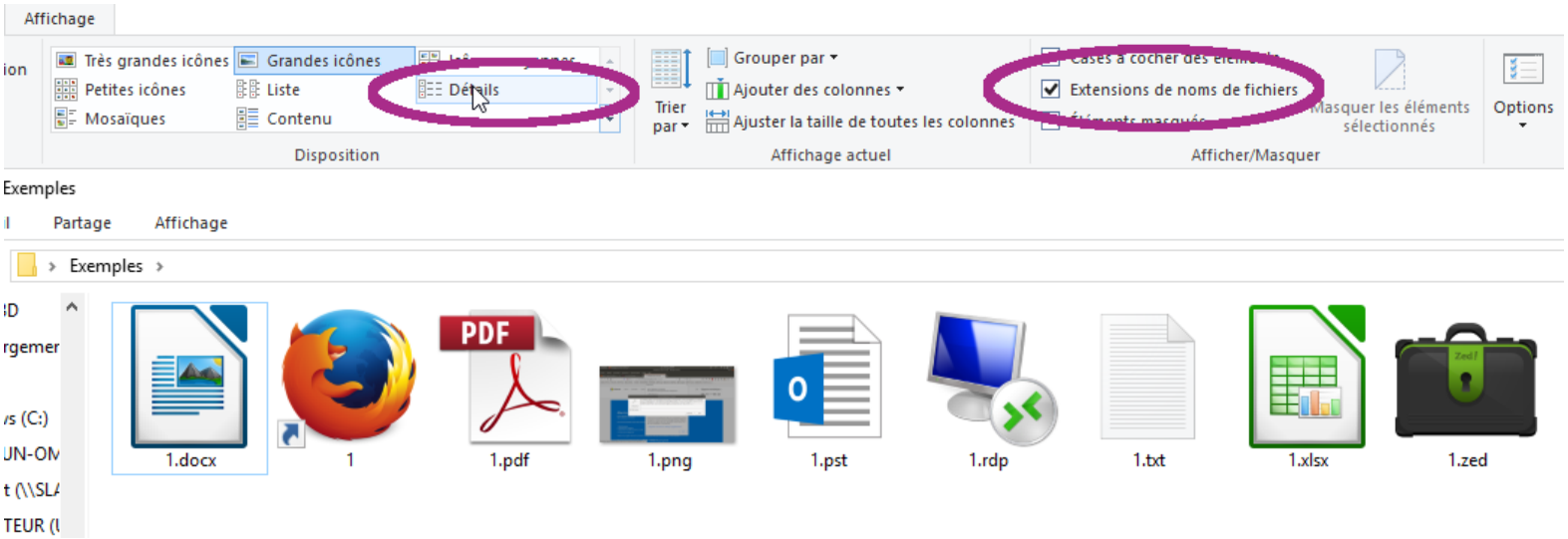
Comment ça marche ?

- Lors de l'installation d'une application, cette dernière déclare au système d'exploitation qu'elle peut ouvrir un certain type de fichiers.
- Cette information est enregistrée dans le système et le fichier sera donc ouvert avec l'application déclarée par défaut.
- Les autres applications sont accessibles à l'aide de l'option "Ouvrir avec" (Shift clic-droit)



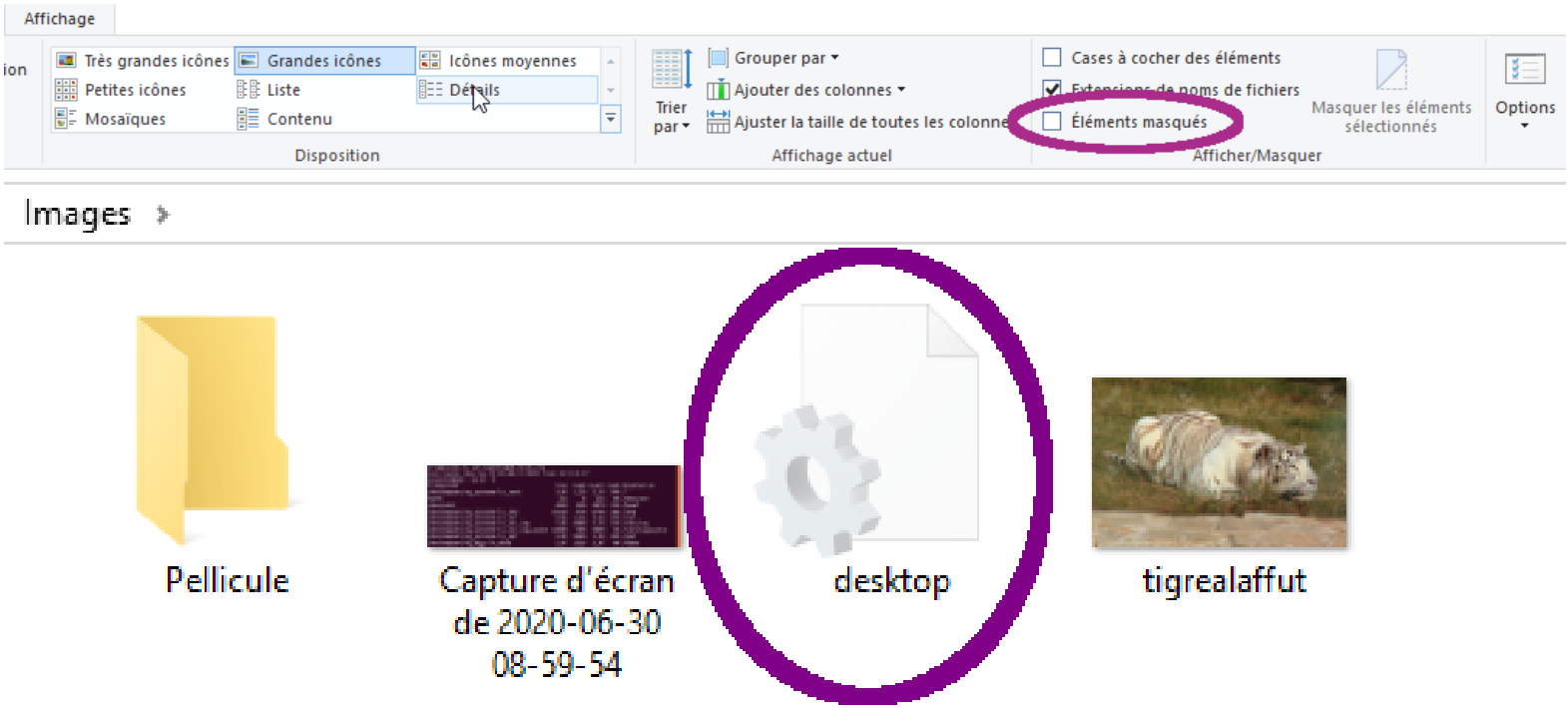
Une question d'affichage . . .

Tout est en fait réalisé pour que vous ne sachiez, voyiez rien ... il est donc nécessaire d'aller dans les options d'affichage pour y voir un peu plus clair.



Et si on jouait à cache-cache ?

Tout est en fait réalisé pour que vous ne sachiez, voyiez rien ... il est donc nécessaire d'aller dans les options d'affichage pour y voir un peu plus clair.



Quel rapport avec la SSI ?

En sécurité on aime cacher les informations ...

- Pour qu'elles ne soient pas vues.

Quel rapport avec la SSI ?

En sécurité on aime cacher les informations ...

- Pour qu'elles ne soient pas vues.
- Pour qu'elles ne soient pas accessibles.

Quel rapport avec la SSI ?

En sécurité on aime cacher les informations ...

- Pour qu'elles ne soient pas vues.
- Pour qu'elles ne soient pas accessibles.
- Pour vous faire croire des choses (marketing).

Quel rapport avec la SSI ?

En sécurité on aime cacher les informations ...

- Pour qu'elles ne soient pas vues.
- Pour qu'elles ne soient pas accessibles.
- Pour vous faire croire des choses (marketing).
- Pour qu'un fichier confidentiel apparraisse comme une image anodine !

Rendre invisible un fichier

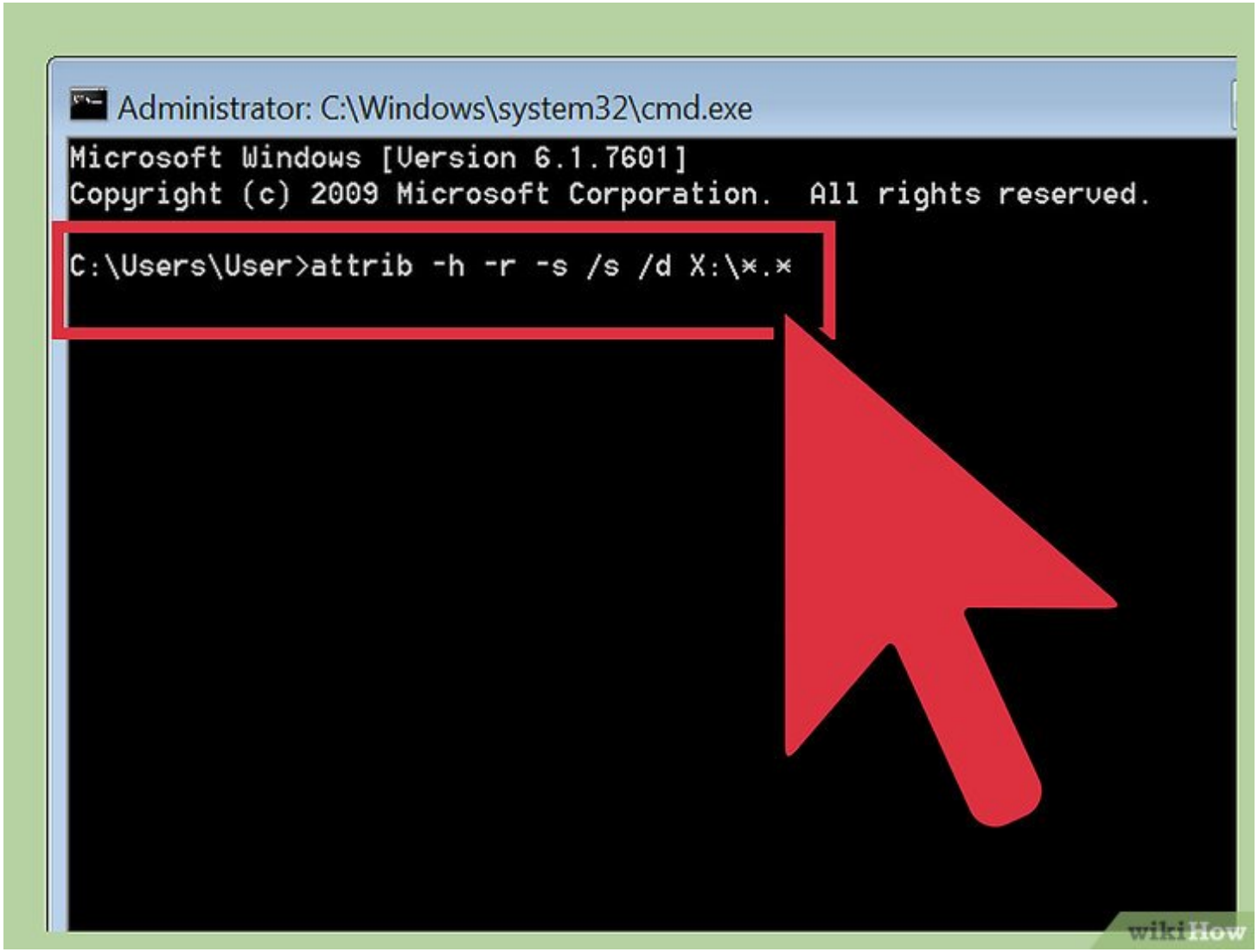
La commande "attrib" accessible au travers de l'invite de commande de Windows permet de rendre invisible / visible des fichiers mais pas que . . .

```
Exemples>attrib +h 1.png

Exemples>attrib -h 1.png
```

+	Sets an attribute.
-	Clears an attribute.
R	Read-only file attribute.
A	Archive file attribute.
S	System file attribute.
H	Hidden file attribute.
I	Not content indexed file attribute.
X	No scrub file attribute
V	Integrity attribute.
/S	Processes matching files in the current folder and all subfolders.
/D	Process folders as well.
/L	Work on the attributes of the symbolic link versus the target of the symbolic link.

Exemple d'utilisation



Les hackers connaissent Mac & Linux

Nombre de fichiers contenant des virus sont préfixés par un .

.monfichier

Les hackers connaissent Mac & Linux

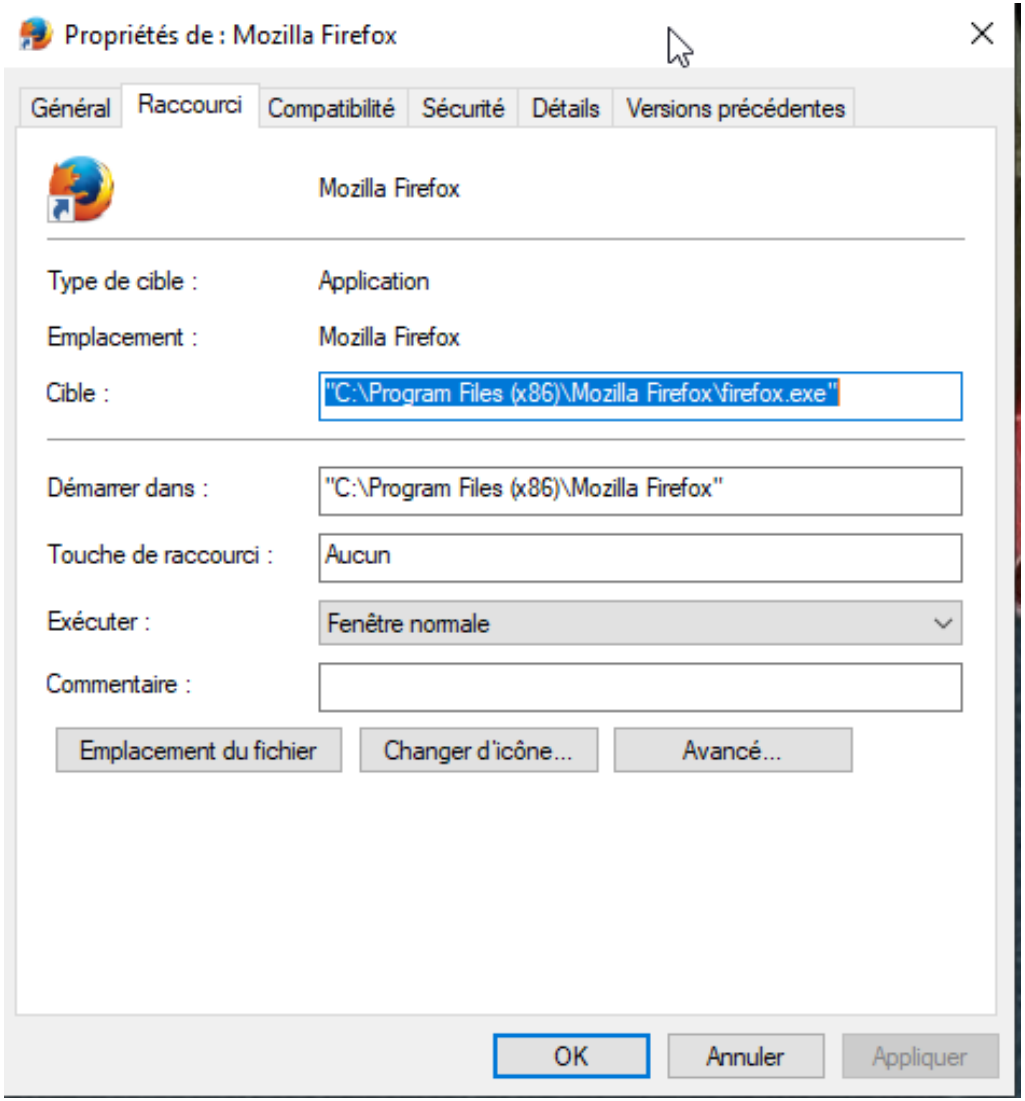
Nombre de fichiers contenant des virus sont préfixés par un .

.monfichier

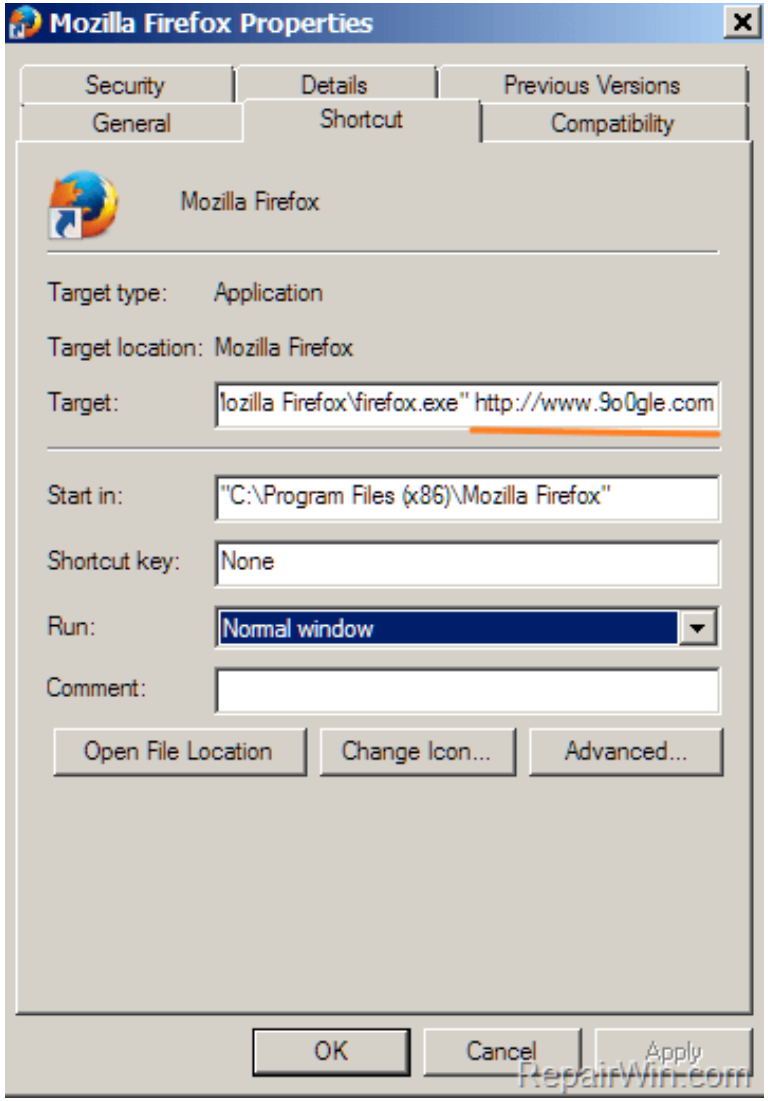
Le . rend les fichiers invisibles sur les systèmes Mac ou Linux.

Le périphérique de stockage contenant ce genre de fichier n'affichera donc pas, par défaut, ces fichiers cachés.

Raccourci : faire ce qu'il ne faut ...



Raccourci : faire plus qu'il ne faut . . .



Leurrer le contenu d'un fichier

Comme indiqué précédemment Windows se fixe sur l'extension du nom de fichier pour afficher l'icône associée, voir la miniature associée notamment pour les images.

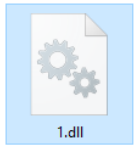
Leurrer le contenu d'un fichier

Comme indiqué précédemment Windows se fixe sur l'extension du nom de fichier pour afficher l'icône associée, voir la miniature associée notamment pour les images.
Observons maintenant un fichier texte dont l'extension a été mise en bitmap (.bmp)

Leurrer le contenu d'un fichier

Comme indiqué précédemment Windows se fixe sur l'extension du nom de fichier pour afficher l'icône associée, voir la miniature associée notamment pour les images.
Observons maintenant un fichier texte dont l'extension a été mise en bitmap (.bmp)

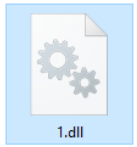
Un pdf transformé en librairie (.dll)



Leurrer le contenu d'un fichier

Comme indiqué précédemment Windows se fixe sur l'extension du nom de fichier pour afficher l'icône associée, voir la miniature associée notamment pour les images.
Observons maintenant un fichier texte dont l'extension a été mise en bitmap (.bmp)

Un pdf transformé en librairie (.dll)



Des icônes qui ne donnent pas vraiment envie de regarder le contenu du fichier !

Comment connaître le type du fichier ?

Pour connaître le type du fichier, il est nécessaire d'avoir 3 éléments hyper puissants :

- Un éditeur de texte (Notepad++ conseillé)

Comment connaître le type du fichier ?

Pour connaître le type du fichier, il est nécessaire d'avoir 3 éléments hyper puissants :

- Un éditeur de texte (Notepad++ conseillé)
- Un lien vers la table des magic numbers : `https://fr.wikipedia.org/wiki/Nombre_magique_(programmation)#Magics_GUIDs`

Comment connaître le type du fichier ?

Pour connaître le type du fichier, il est nécessaire d'avoir 3 éléments hyper puissants :

- Un éditeur de texte (Notepad++ conseillé)
- Un lien vers la table des magic numbers : `https://fr.wikipedia.org/wiki/Nombre_magique_(programmation)#Magics_GUIDs`
- Savoir faire shift clic-droit $->$ Ouvrir avec ...

Comment connaître le type du fichier ?

Pour connaître le type du fichier, il est nécessaire d'avoir 3 éléments hyper puissants :

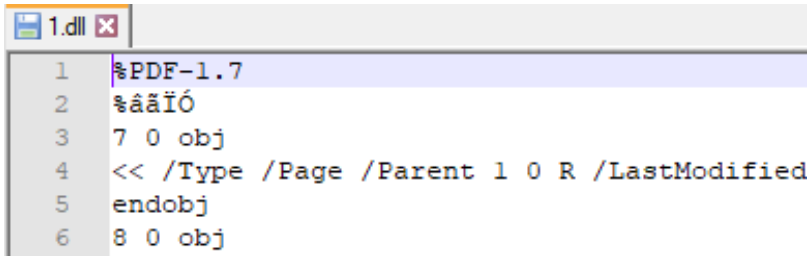
- Un éditeur de texte (Notepad++ conseillé)
- Un lien vers la table des magic numbers : `https://fr.wikipedia.org/wiki/Nombre_magique_(programmation)#Magics_GUIDs`
- Savoir faire shift clic-droit $->$ Ouvrir avec ...

Comment connaître le type du fichier ?

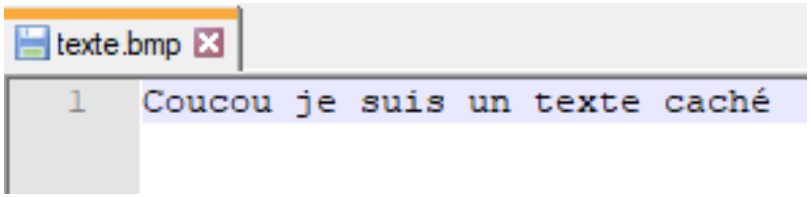
Pour connaître le type du fichier, il est nécessaire d'avoir 3 éléments hyper puissants :

- Un éditeur de texte (Notepad++ conseillé)
- Un lien vers la table des magic numbers : `https://fr.wikipedia.org/wiki/Nombre_magique_(programmation)#Magics_GUIDs`
- Savoir faire shift clic-droit $->$ Ouvrir avec ...

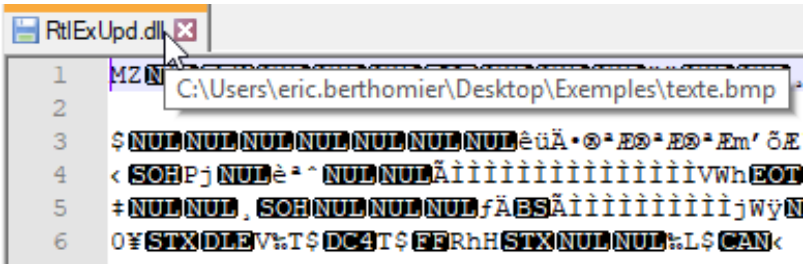
Mise en application



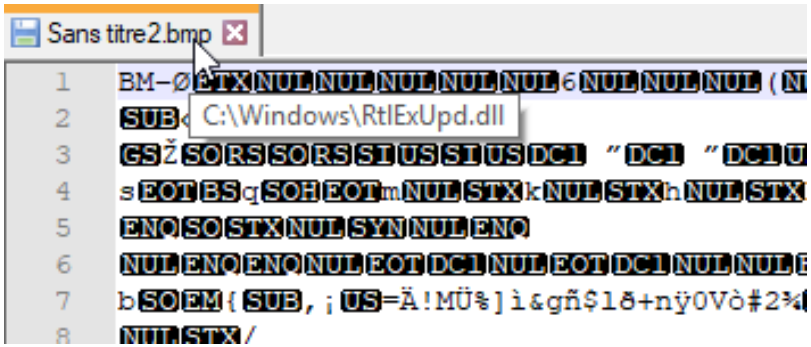
Faux fichier de type DLL



Faux fichier de type Bitmap

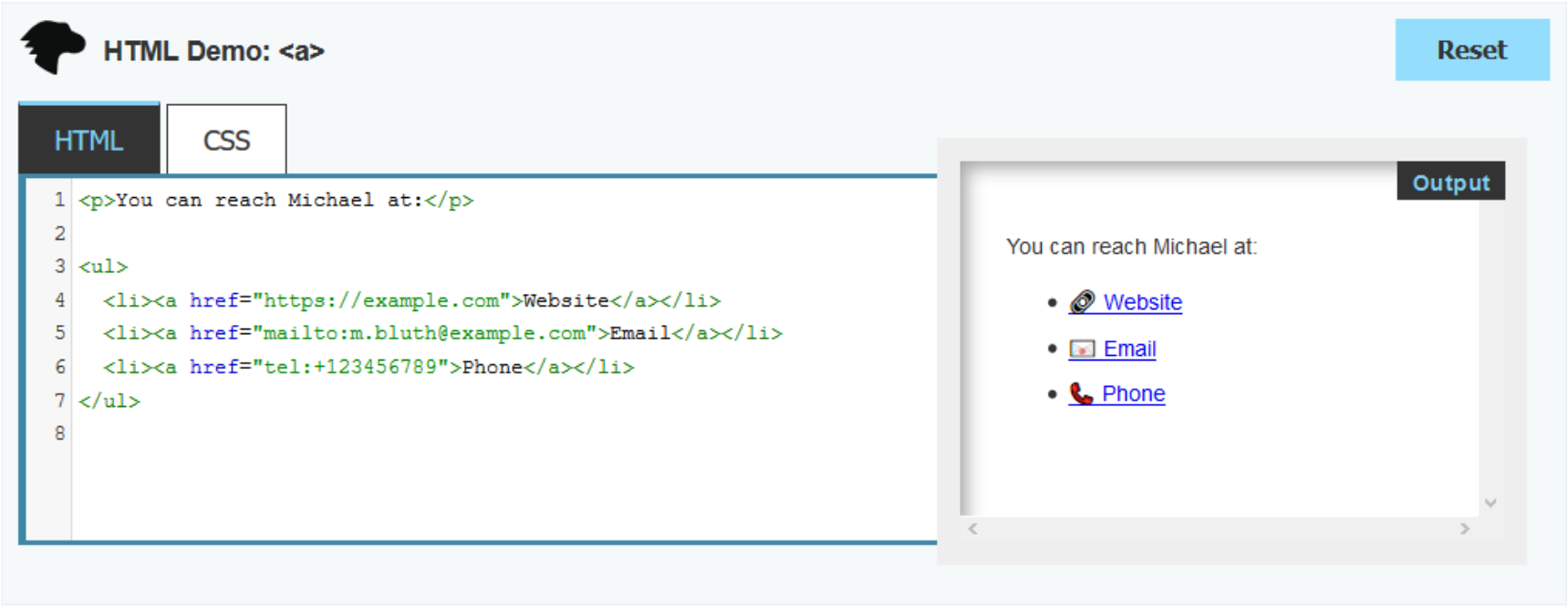


Fichier de type dll



Fichier de type Bitmap

Des liens, des liens, des liens . . .



Lien Web : https ://viensmonmignon.fr

Courriel : eric.berthomier@free.fr

Des petits liens : tiny url

Une tiny url permet de transformer une url longue :

`http://ericberthomier.fr/spip.php?page=recherche&recherche=ssi`

Des petits liens : tiny url

Une tiny url permet de transformer une url longue :

`http://ericberthomier.fr/spip.php?page=recherche&recherche=ssi`

en une petite url :

`https://tinyurl.com/y5pn72nj`

Des petits liens : tiny url

Une tiny url permet de transformer une url longue :

`http://ericberthomier.fr/spip.php?page=recherche&recherche=ssi`

en une petite url :

`https://tinyurl.com/y5pn72nj`

Vous devenez alors aveugle sur la destination de l'url ....

Expansion des tiny URLs . . .

TinyURL Ajouter "preview" avant la partie tinyurl.com du lien.
Exemple : https ://tinyurl.com/y5pn72nj devient
https ://preview.tinyurl.com/y5pn72nj

Expansion des tiny URLs . . .

TinyURL Ajouter "preview" avant la partie tinyurl.com du lien. Exemple : https ://tinyurl.com/y5pn72nj devient https ://preview.tinyurl.com/y5pn72nj

URL Expander vous permettra de voir l'URL de manière décompressée.

Expansion des tiny URLs . . .

TinyURL Ajouter "preview" avant la partie tinyurl.com du lien. Exemple : https ://tinyurl.com/y5pn72nj devient https ://preview.tinyurl.com/y5pn72nj

URL Expander vous permettra de voir l'URL de manière décompressée.

Expansion des tiny URLs . . .

TinyURL Ajouter "preview" avant la partie tinyurl.com du lien.
Exemple : https ://tinyurl.com/y5pn72nj devient
https ://preview.tinyurl.com/y5pn72nj

URL Expander vous permettra de voir l'URL de manière décompressée.

https://tinyurl.com/y5pn72nj http://ericberthomier.fr/spip.php?page...

↓ Download results as .CSV list

« Expand another URL

Previsualisation et analyse des URLs . . .

Get Link Info vous permettra d'avoir des renseignements sur l'url en question.

Previsualisation et analyse des URLs . . .

Get Link Info vous permettra d'avoir des renseignements sur l'url en question.

Zulu URL Risk Analyzer vous permettra d'analyser une url.

Previsualisation et analyse des URLs . . .

Get Link Info vous permettra d'avoir des renseignements sur l'url en question.

Zulu URL Risk Analyzer vous permettra d'analyser une url.

Should I Click vous permettra d'avoir d'avoir un visuel sur l'url en question.

Previsualisation et analyse des URLs . . .

Get Link Info vous permettra d'avoir des renseignements sur l'url en question.

Zulu URL Risk Analyzer vous permettra d'analyser une url.

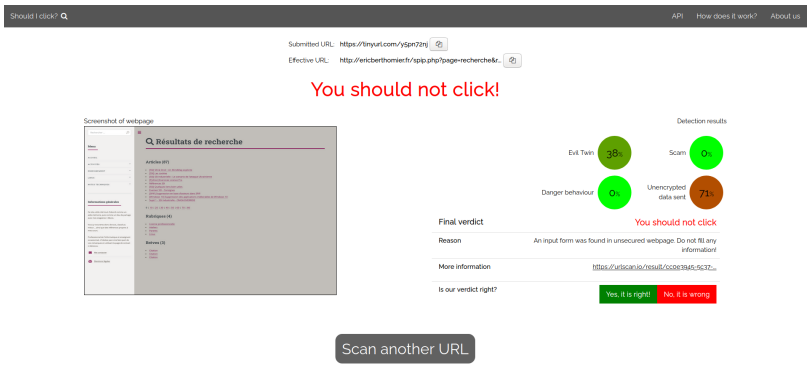
Should I Click vous permettra d'avoir d'avoir un visuel sur l'url en question.

Previsualisation et analyse des URLs . . .

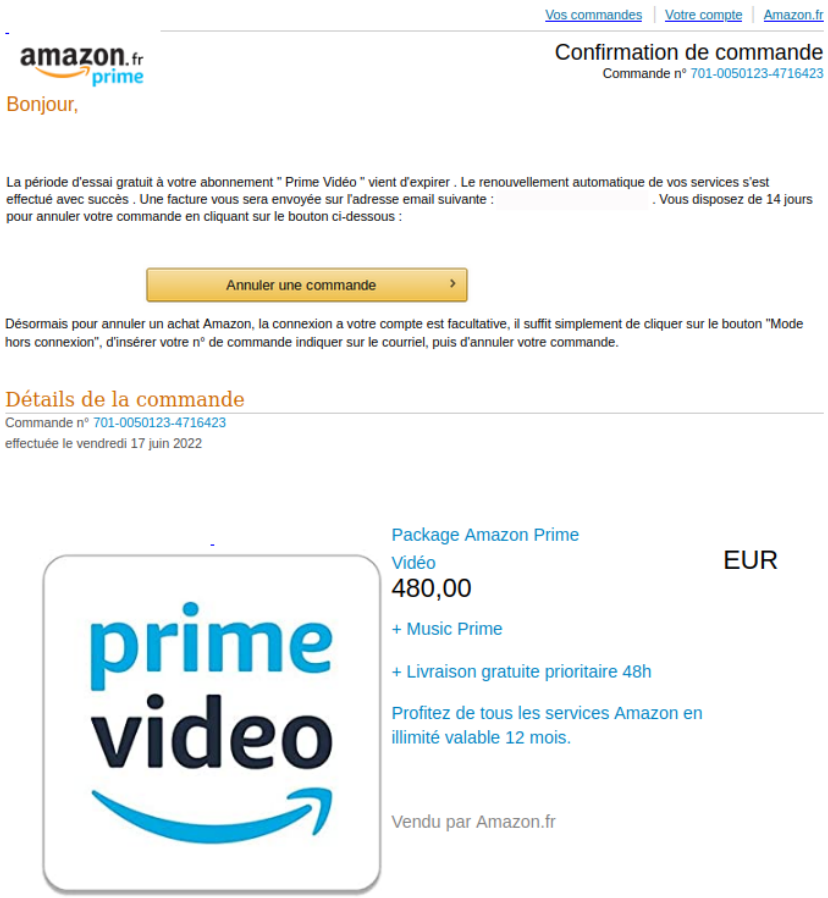
Get Link Info vous permettra d'avoir des renseignements sur l'url en question.

Zulu URL Risk Analyzer vous permettra d'analyser une url.

Should I Click vous permettra d'avoir d'avoir un visuel sur l'url en question.



Question piège. . .



Vos commandes | Votre compte | Amazon.fr

amazon.fr prime

Confirmation de commande

Commande n° 701-0050123-4716423

Bonjour,

La période d'essai gratuit à votre abonnement " Prime Vidéo " vient d'expirer . Le renouvellement automatique de vos services s'est effectué avec succès . Une facture vous sera envoyée sur l'adresse email suivante : . Vous disposez de 14 jours pour annuler votre commande en cliquant sur le bouton ci-dessous :

Annuler une commande ›

Désormais pour annuler un achat Amazon, la connexion a votre compte est facultative, il suffit simplement de cliquer sur le bouton "Mode hors connexion", d'insérer votre n° de commande indiquer sur le courriel, puis d'annuler votre commande.

Détails de la commande

Commande n° 701-0050123-4716423

effectuée le vendredi 17 juin 2022

prime video

Package Amazon Prime Vidéo

480,00 EUR

+ Music Prime

+ Livraison gratuite prioritaire 48h

Profitez de tous les services Amazon en illimité valable 12 mois.

Vendu par Amazon.fr

Comment savoir si ce courriel est un phishing ou non (sans utiliser les méthodes vues précédemment) ?

Plusieurs réponses

Magique . . .