Embedding hidden files in jpeg images
Tested target : FaceBook
(*other known working target :* flickr)

(Antoine Santo 30-01-2011)

--[0. - **Introduction**

This document describes the technique to embed any kind of file in a jpg image, then upload it as a trivial image to facebook photo album.
This research was made to understand how facebook process images in-order to prevent abuses of it and suggest solutions.
Disclaimer: When using parts from this paper, you should still credit the author. I won't be held responsible for the damages done to yourself or others nor for illegal uses. It's at your own risk.
This paper uses no specific knowledge execept basics about jpg format, gd library and base 64 encoding.

--[1. - The FaceBook process

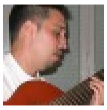
Facebook allows its subscribers to create photo albums and to upload photos. Facebook allows the sending of large, high resolution pictures, since resizing will be done by the site automatically. It seems that facebook keeps the EXIF data of the original image for the resized photo.

--[2. - The embedding process

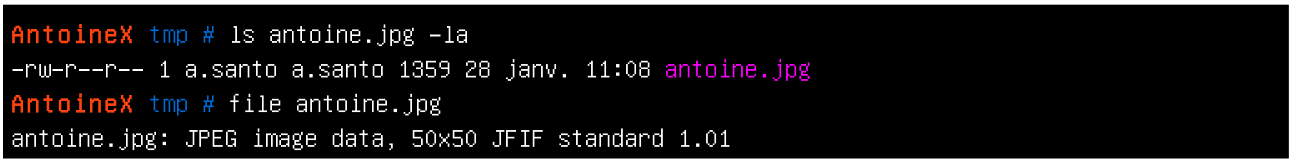
During the different steps of the process, notice the size of each file.

----[2.0. - We need some files

You need a container image :

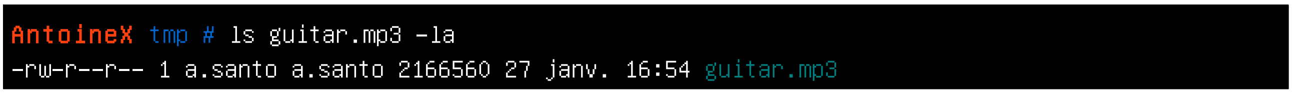


antoine.jpg



```
AntoineX tmp # ls antoine.jpg -la
-rw-r--r-- 1 a.santo a.santo 1359 28 janv. 11:08 antoine.jpg
AntoineX tmp # file antoine.jpg
antoine.jpg: JPEG image data, 50x50 JFIF standard 1.01
```

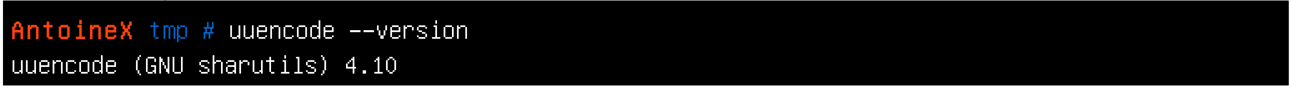
And you need the file you want to embed to it. I will use a music file called « *guitar.mp3* »



```
AntoineX tmp # ls guitar.mp3 -la
-rw-r--r-- 1 a.santo a.santo 2166560 27 janv. 16:54 guitar.mp3
```

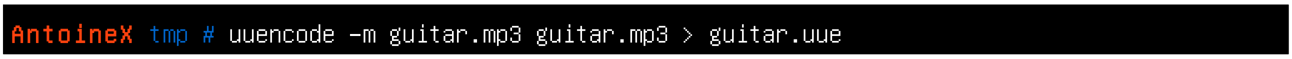
----[2.1. - Encoding the file you want to embed

For this step i use uuencode

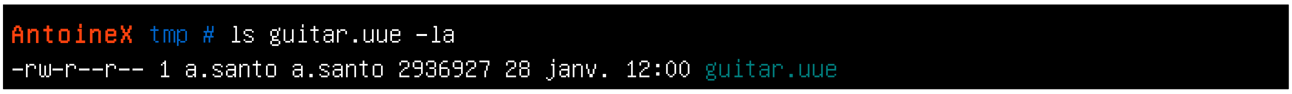


```
AntoineX tmp # uuencode --version
uuencode (GNU sharutils) 4.10
```

I use the « -m » parameter to encode it using base64.



```
AntoineX tmp # uuencode -m guitar.mp3 guitar.mp3 > guitar.uue
```

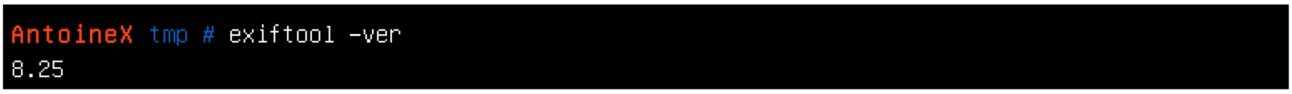


```
AntoineX tmp # ls guitar.uue -la
-rw-r--r-- 1 a.santo a.santo 2936927 28 janv. 12:00 guitar.uue
```

----[2.2. - **Injecting the encoded file in the container jpg image**

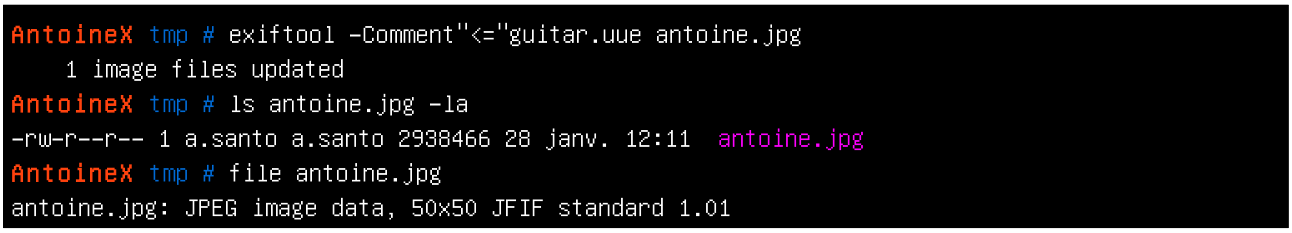
Here is the « *magic », i* inject the encoded file in the jpg image using the EXIF « Comment » field.

For this i use the exiftool.



```
AntoineX tmp # exiftool -ver
8.25
```

I use the « <= » parameter of exiftool, that allows to use a file content to fill an EXIF field.

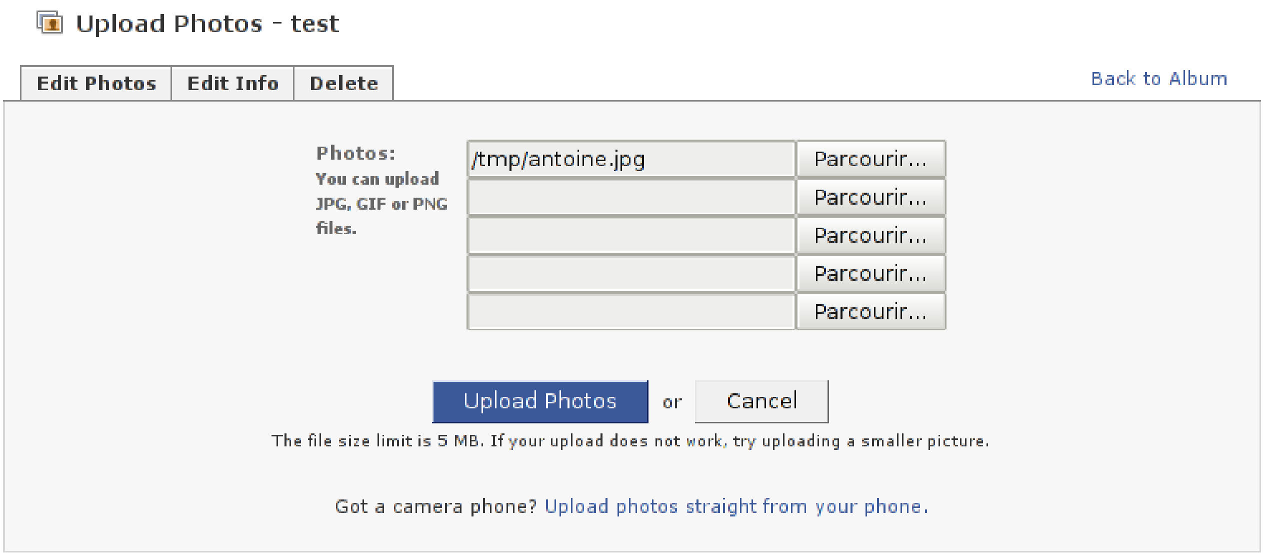


```
AntoineX tmp # exiftool -Comment"<="guitar.uue antoine.jpg
    1 image files updated
AntoineX tmp # ls antoine.jpg -la
-rw-r--r-- 1 a.santo a.santo 2938466 28 janv. 12:11  antoine.jpg
AntoineX tmp # file antoine.jpg
antoine.jpg: JPEG image data, 50x50 JFIF standard 1.01
```

I now have a nice and tiny 50x50 jpg image embedding a 2+ MB mp3 file.

--[3. - **Let's try it on FaceBook**

I logon to my FaceBook account, then upload this new image to my album called « *test* »



Upload Photos - test

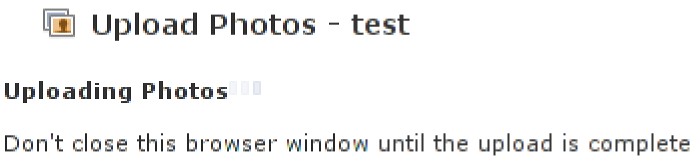
Photos: You can upload JPG, GIF or PNG files.

/tmp/antoine.jpg

The file size limit is 5 MB. If your upload does not work, try uploading a smaller picture.

Got a camera phone? Upload photos straight from your phone.

Let's wait some minutes :

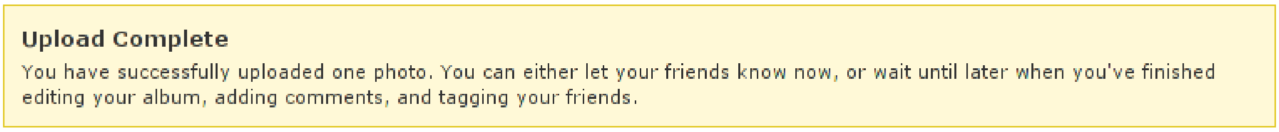


Upload Photos - test

Uploading Photos

Don't close this browser window until the upload is complete

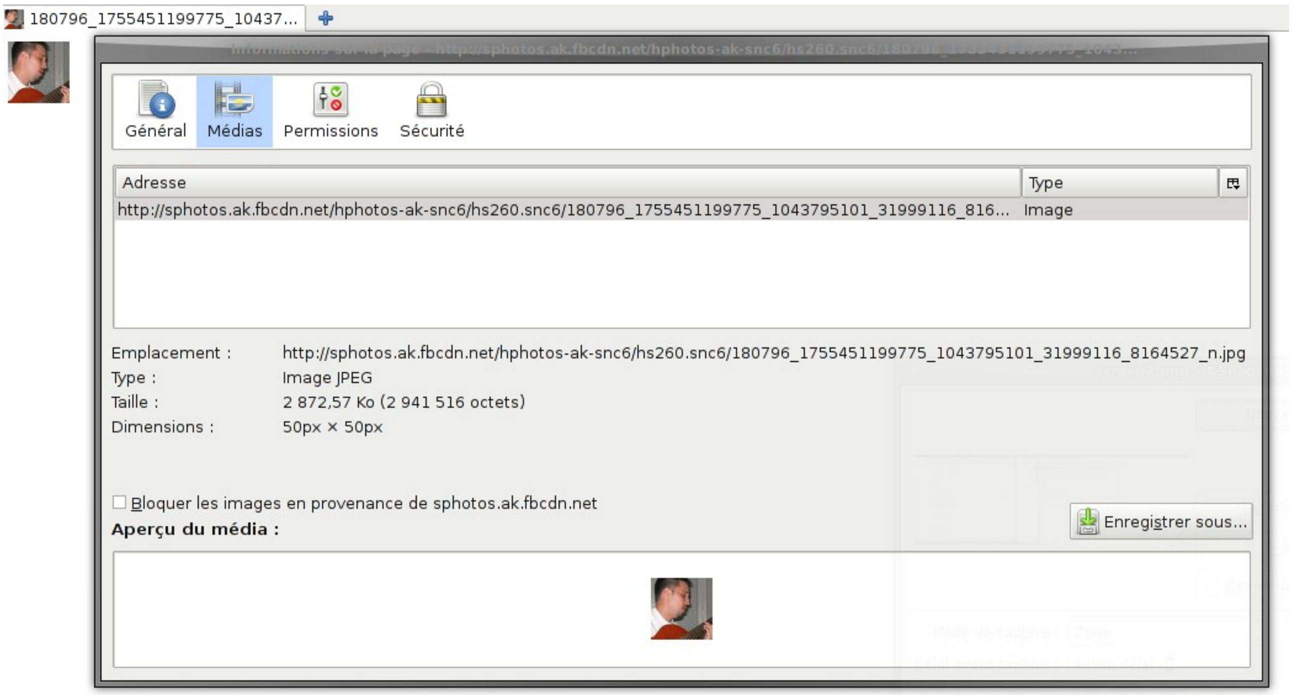
Then :



Upload Complete

You have successfully uploaded one photo. You can either let your friends know now, or wait until later when you've finished editing your album, adding comments, and tagging your friends.

So, it's seems there was no problem about my image for the facebook process. Let's have a look at the image on the facebook CDN servers.



180796_1755451199775_10437...

Informations sur la page - http://sphotos.ak.fbcdn.net/hphotos-ak-snc6/hs260.snc6/180796_1755451199775_1043...

Adresse	Type
http://sphotos.ak.fbcdn.net/hphotos-ak-snc6/hs260.snc6/180796_1755451199775_1043795101_31999116_816...	Image

Emplacement : http://sphotos.ak.fbcdn.net/hphotos-ak-snc6/hs260.snc6/180796_1755451199775_1043795101_31999116_8164527_n.jpg
Type : Image JPEG
Taille : 2 872,57 Ko (2 941 516 octets)
Dimensions : 50px × 50px

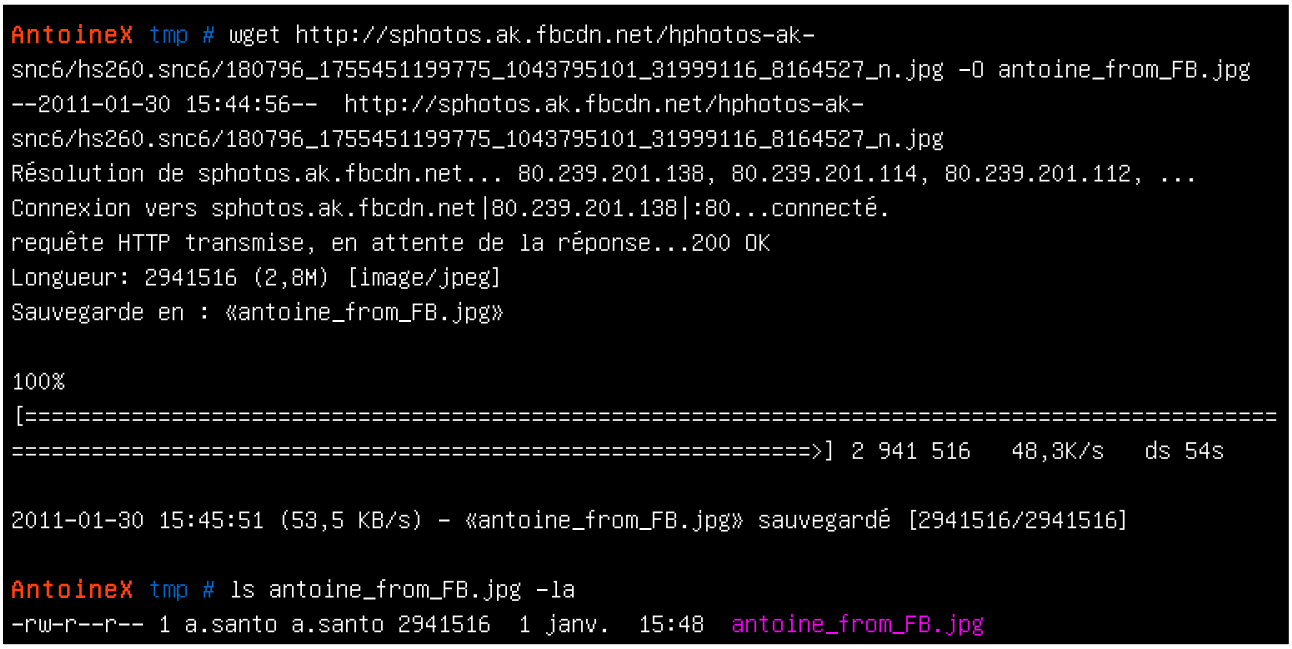
□ Bloquer les images en provenance de sphotos.ak.fbcdn.net

Aperçu du média :

As you can see my tiny 50x50 image is 2,8MB... And it's displayed well on my FaceBook profile.

--[4. - Exctract the hidden document from the image

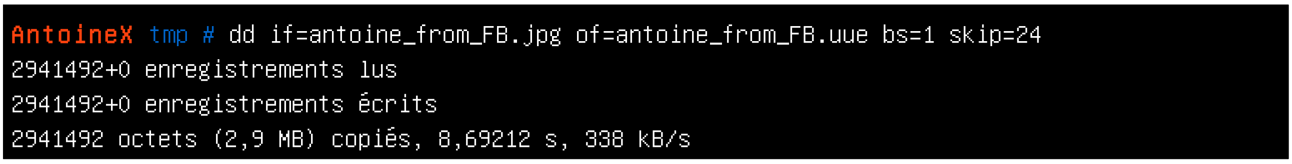
First i will download the image :



```
AntoineX tmp # wget http://sphotos.ak.fbcdn.net/hphotos-ak-
snc6/hs260.snc6/180796_1755451199775_1043795101_31999116_8164527_n.jpg -O antoine_from_FB.jpg
--2011-01-30 15:44:56--  http://sphotos.ak.fbcdn.net/hphotos-ak-
snc6/hs260.snc6/180796_1755451199775_1043795101_31999116_8164527_n.jpg
Résolution de sphotos.ak.fbcdn.net... 80.239.201.138, 80.239.201.114, 80.239.201.112, ...
Connexion vers sphotos.ak.fbcdn.net|80.239.201.138|:80...connecté.
requête HTTP transmise, en attente de la réponse...200 OK
Longueur: 2941516 (2,8M) [image/jpeg]
Sauvegarde en : «antoine_from_FB.jpg»

100%
[=============================================================================================
==========================================================>] 2 941 516   48,3K/s   ds 54s

2011-01-30 15:45:51 (53,5 KB/s) - «antoine_from_FB.jpg» sauvegardé [2941516/2941516]

AntoineX tmp # ls antoine_from_FB.jpg -la
-rw-r--r-- 1 a.santo a.santo 2941516  1 janv.  15:48  antoine_from_FB.jpg
```

As you can see the image size is a little bit different from the image i uploaded. I think the image has been reworked by GD, but it keeps our EXIF field unchanged.

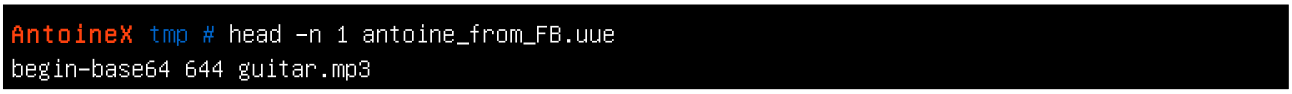
Then for the second step i need to remove the jpg header (24 Bytes) :



```
AntoineX tmp # dd if=antoine_from_FB.jpg of=antoine_from_FB.uue bs=1 skip=24
2941492+0 enregistrements lus
2941492+0 enregistrements écrits
2941492 octets (2,9 MB) copiés, 8,69212 s, 338 kB/s
```

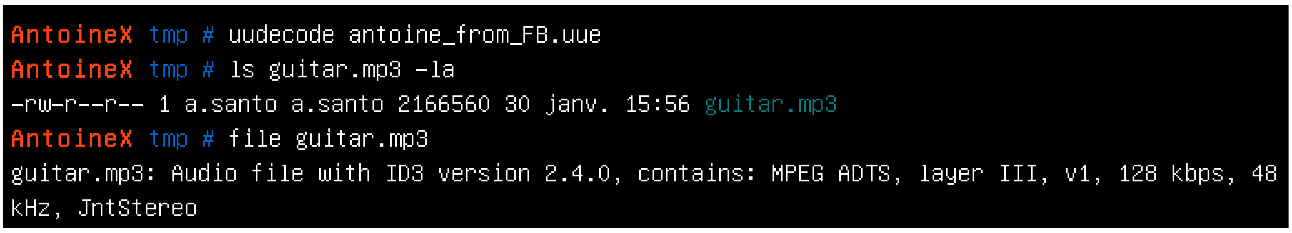
We now have a file called *antoine_from_FB.uue*.

Lets see the first line of this uue file :



```
AntoineX tmp # head -n 1 antoine_from_FB.uue
begin-base64 644 guitar.mp3
```

So we can read that, the uudecoding process will generate a file called *guitare.mp3*



```
AntoineX tmp # uudecode antoine_from_FB.uue
AntoineX tmp # ls guitar.mp3 -la
-rw-r--r-- 1 a.santo a.santo 2166560 30 janv. 15:56 guitar.mp3
AntoineX tmp # file guitar.mp3
guitar.mp3: Audio file with ID3 version 2.4.0, contains: MPEG ADTS, layer III, v1, 128 kbps, 48
kHz, JntStereo
```

--[5. - **Conclusion and potential uses**

This white paper show the abiltiy to hide any documents in a simple jpg file, and the permission to upload it on a web site like FaceBook.
It means, abusing space storage, bandwith of a website.

The second dangerous aspect of this, is that the abused websites can't control the hidden embedded documents. Is this legal ?

Here is two simple potential uses on FaceBook :

Someone creates a FaceBook group called « clouds lovers ». Some FaceBook users join the group. They are all sharing clouds pictures via the group's picture facility. All this seems perfectly legal and it's nice to see people loving clouds so much !!! **BUT** it can be a PEDO group sharing hidden stuff in thoses clouds pictures.....

Someone creates a FaceBook group called « Rolling Stones Fans ». Some FaceBook users join the group. They are all sharing Rolling stones album cover via the group's picture facility. All this seems perfectly legal **BUT** it can be a warez group, sharing mp3 in images.....

and for these two exemples, all the illegal content would be hosted by FaceBook CDN...

Since the images from the CDN are accessible without any FaceBook account, the whole internet can acces the illegal stuff....

--[5. - **Author**

Antoine Santo (during independant research)
For questions : antoinesanto [a t] yahoo [d 0 t] com
No blog / No twitter / No WebSite ;)