YouTube Hacking

Conserver en « dur » ce qu'on visionne en « live »

Introduction

Tout le monde connait YouTube, la plus grande plateforme d'hébergement de vidéos du Web, en plus de Daylimotion ou Google Video.

YouTube permet à des milliers d'utilisateurs du monde entier depuis 2005, de visionner des vidéos (protégées ou non) directement en ligne grâce à un lecteur flash embarqué.

Ce principe est celui du *streaming*, on se connecte, on choisit une vidéo (par le biais d'un moteur de recherche intégré), on clique et on visionne. En plus de tout ceci, chacun peut commenter la vidéo qu'il visionne.

Mais avec tout ce qu'il se passe en ce moment, on peut être à même de se demander si tout ceci est légal ?! Et bien en fait, YouTube (qui est une firme de Google) possèdent plusieurs accords avec certains grands studios (Sony, Warner, Universal ...) et un partenariat avec la Sacem. YouTube diffuse donc les œuvres, en se protégeant d'un possible conflit juridique par le biais d'un contrat.

Mais pour l'utilisateur lambda, le désir est grand de vouloir quelque fois conserver une vidéo pour le simple fait de pouvoir l'avoir sous le coude, non pas pour la revendre (idée complètement stupide), mais tout simplement pour ne pas être dépendant d'Internet (Train, Avion, Voiture, Bus ...).

Handle Unlock

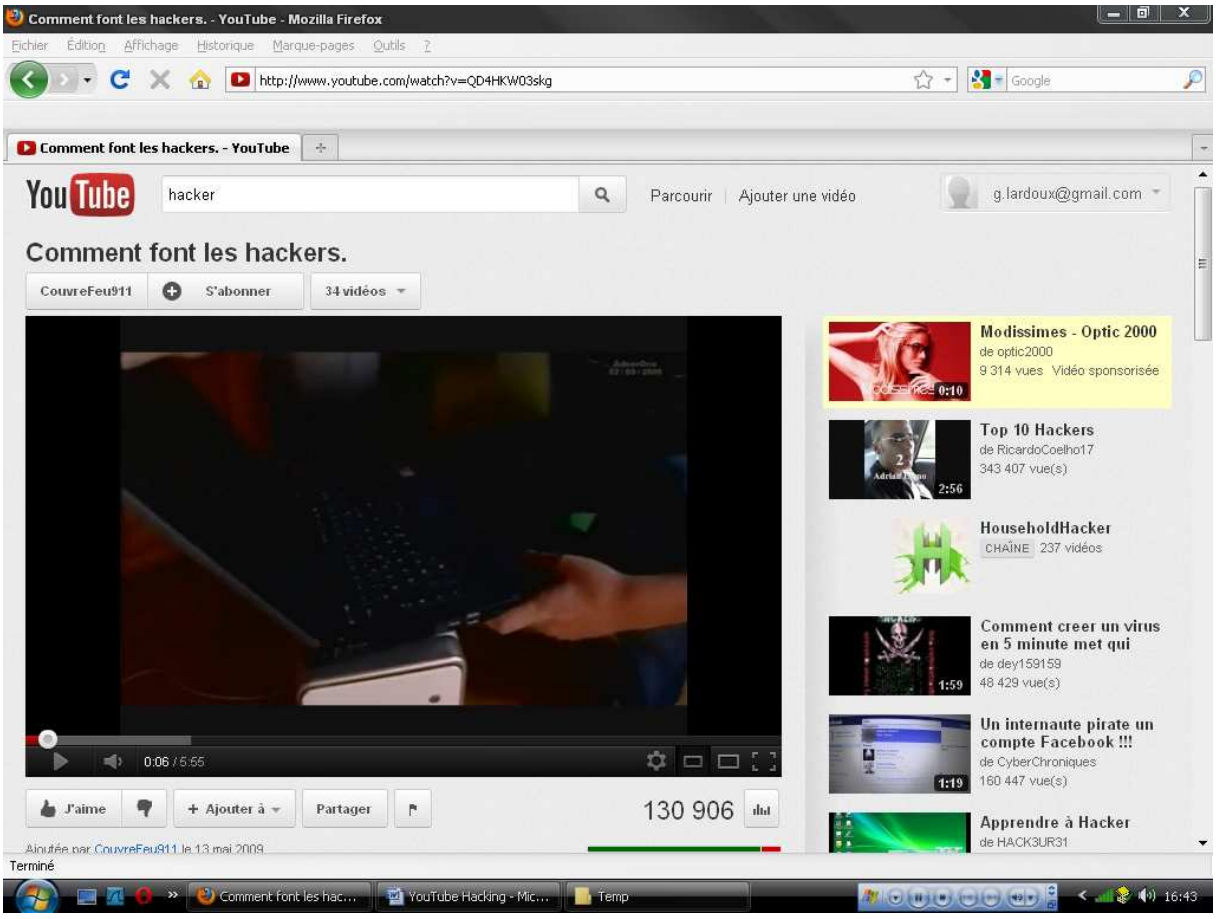
Rare sont les utilisateurs qui le savent, mais lorsque l'on regarde une vidéo sur YouTube, ce dernier copie le fichier Flash Video (FLV) sur notre disque dur.

Par conséquent, dès qu'on visionne une vidéo sur ce site, nous possédons dès lors une copie du fichier sans même l'avoir demandé. Alors pourquoi ne pas en profiter pour en faire une petite copie ? C'est là la première faiblesse.

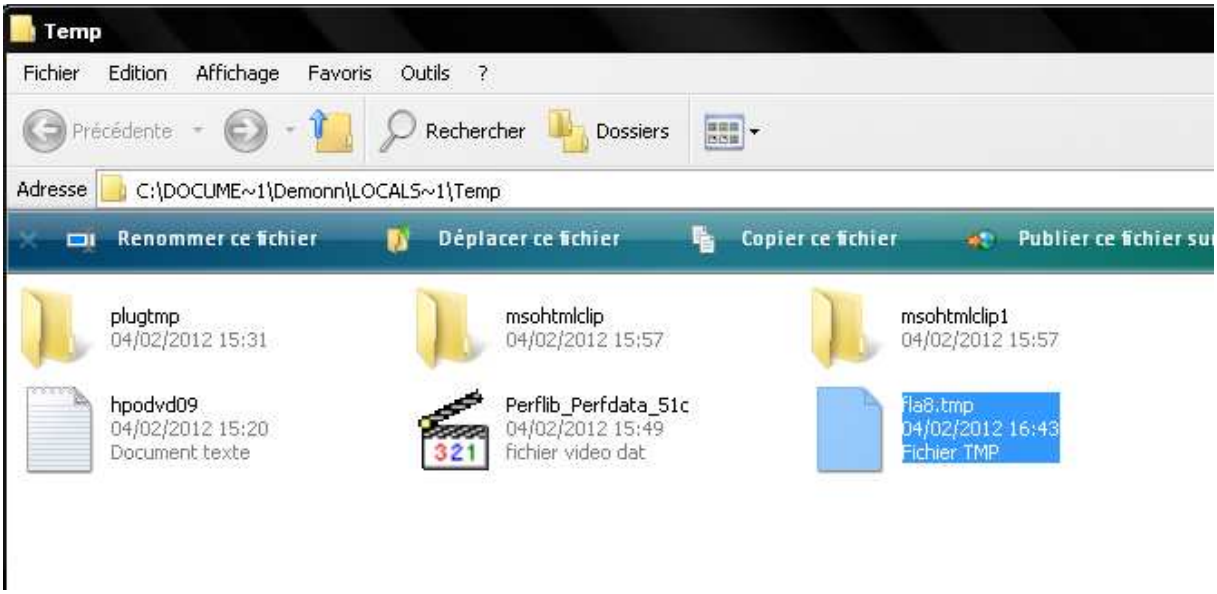
Un outil super sur Internet, ou doux nom de « Unlocker » permet de copier/renommer/effacer un fichier tandis qu'un processus possède un handle dessus. Le principe de fonctionnement de cet outil est qu'il va dupliquer le handle du processus d'origine pour se retrouver avec le même accès que celui-ci.

Pour plus de détails sur le fonctionnement interne de Unlocker (ce n'est pas le but de cet article), allez voir sur www.ivanlef0u.tuxfamily.org/?p=112

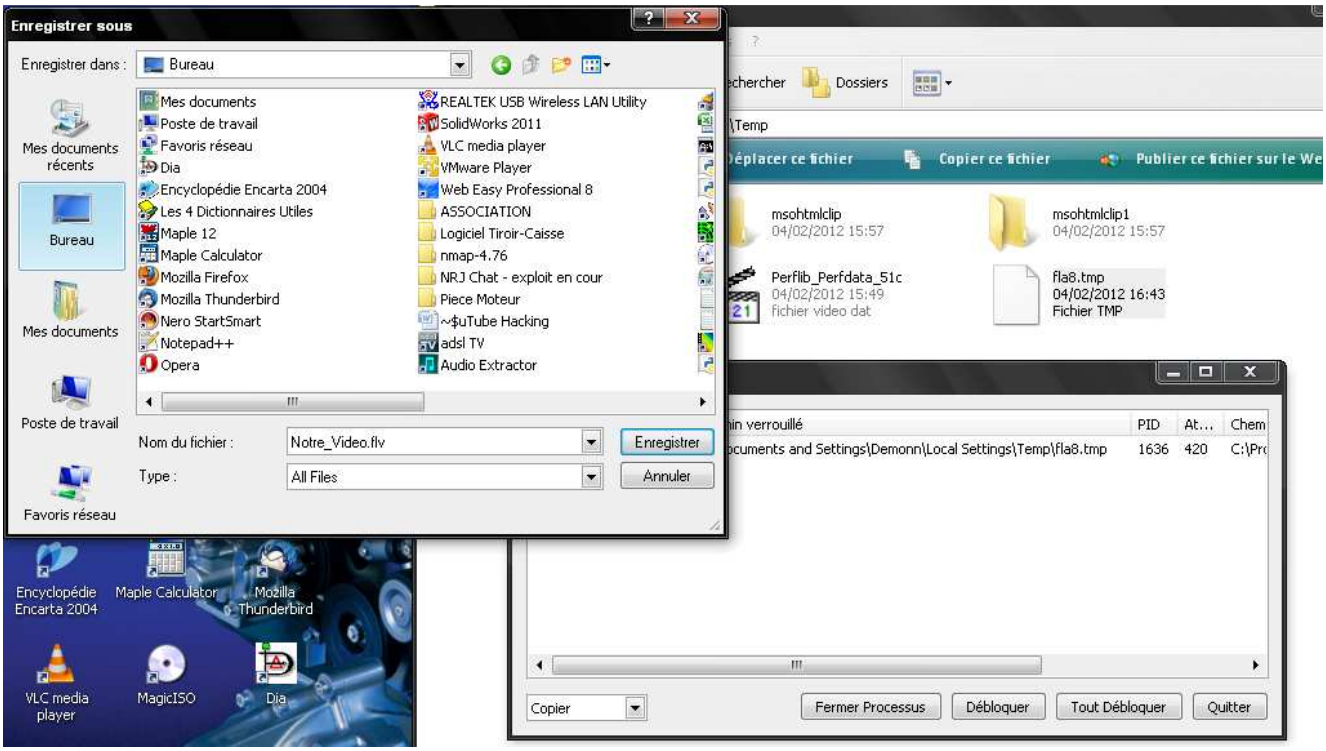
Commençons par visionner une vidéo …



On ouvre ensuite %TMP%, et qu'est-ce qu'on y voit ? Un nouveau fichier a été créé, commençant par «fla ».



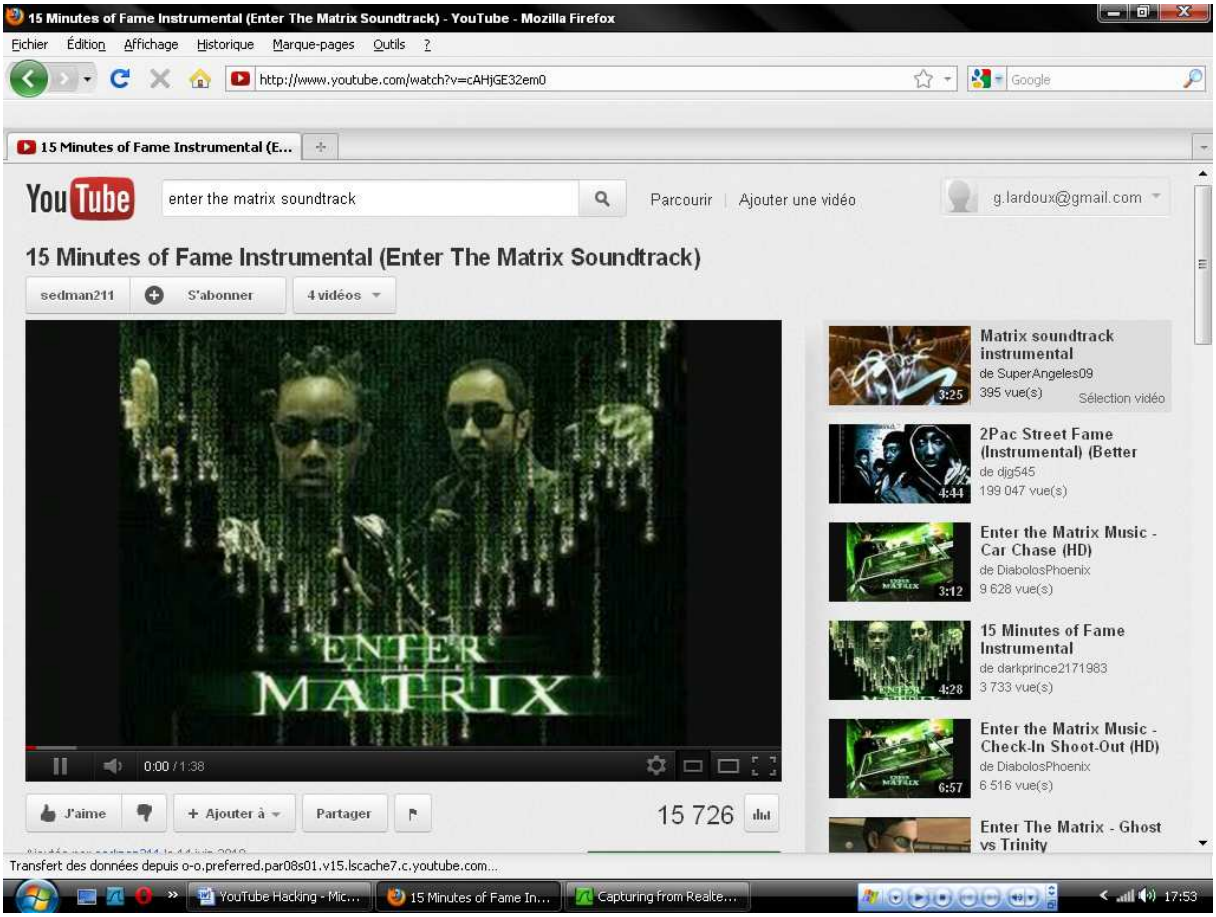
Si vous ouvrez avec un Editeur Hexadécimale type WinHex, vous verrez que c'est un fichier FLV : c'est notre vidéo. Il n'y a plus qu'à sortir Unlocker, pour copier ça sur notre Bureau.



Une fois enregistré, le fichier est à notre disposition sur le Bureau avec l'extension FLV, qui se lit avec VLC ou FLV Player.

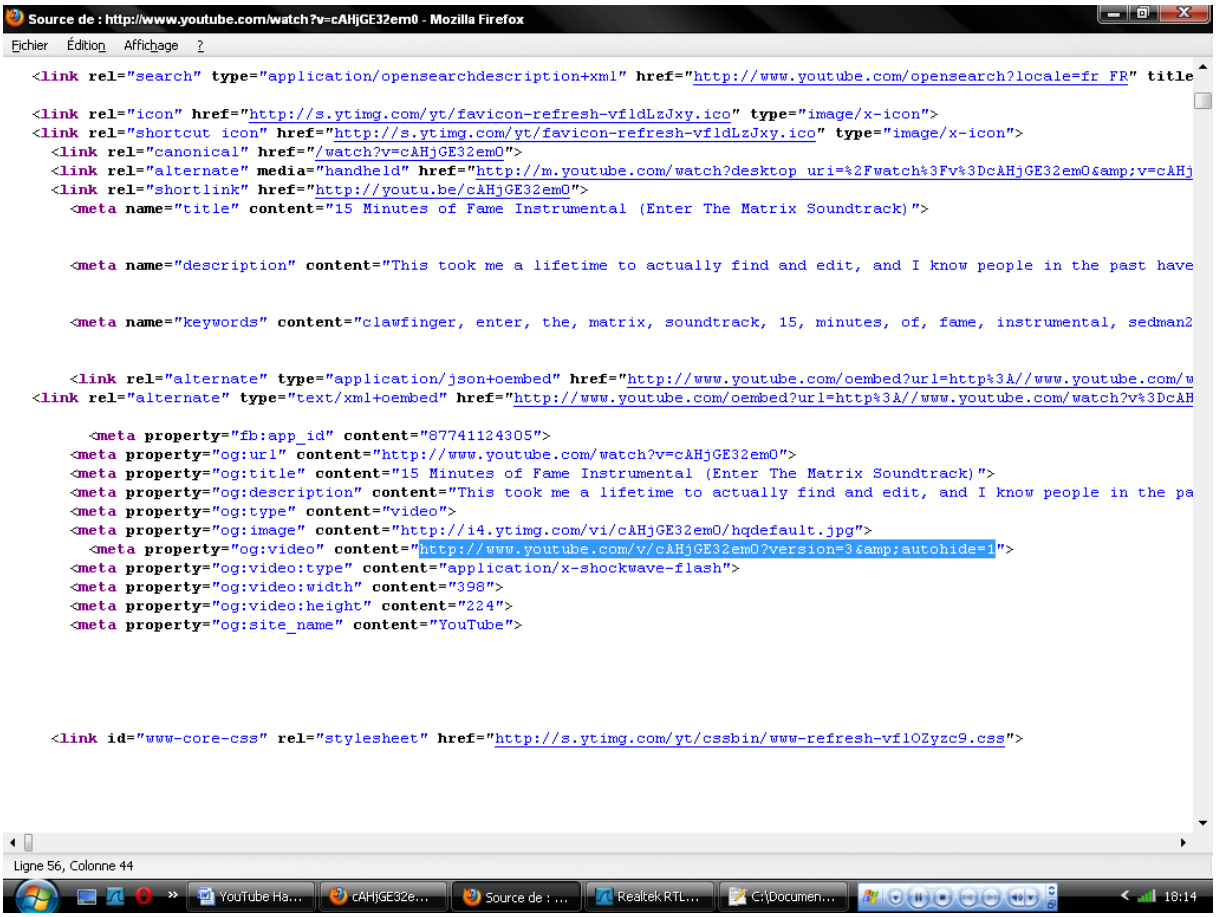
Retour aux Sources

Une méthode plus technique à présent, consiste à retrouver la source du fichier sur les serveurs de YouTube (enfin en réalité ils appartiennent à Google, car YouTube = Google). C'est parti, et on va sur YouTube pour lire une petite vidéo.

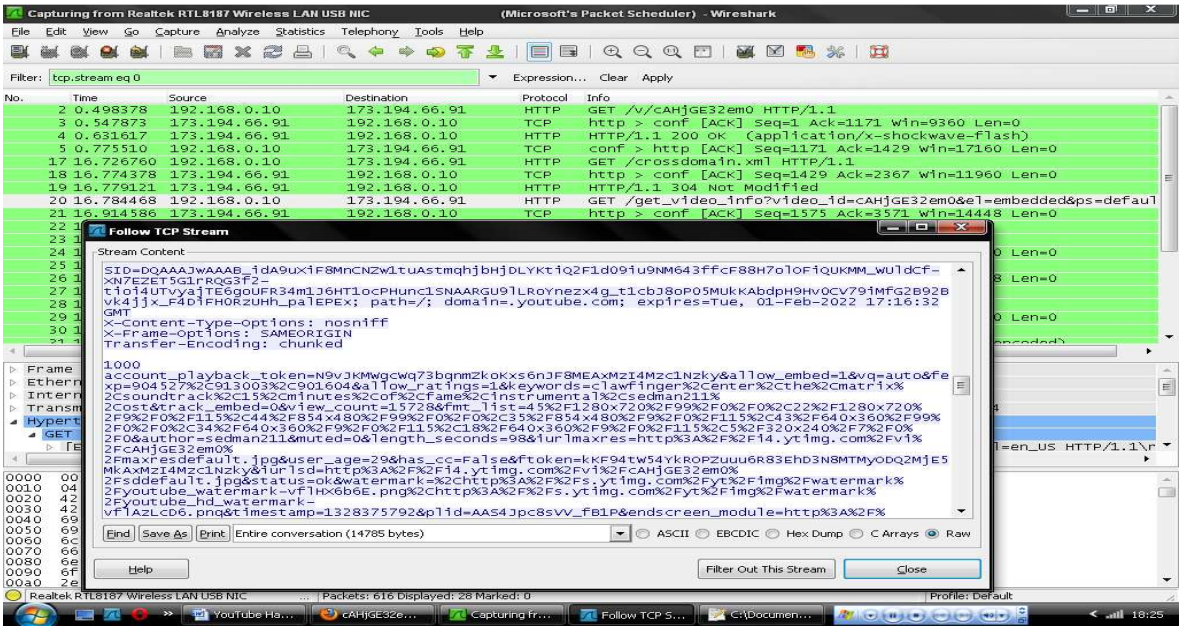


On affiche le code source [CTRL+U] et on cherche, un peu au feeling c'est vrai, une origine possible… Finalement cela porte ses fruits.

Quelques lignes plus bas, on tombe sur la partie de code qui gère l'affichage de la vidéo dans la page, grâce au lecteur Flash Video embarqué, et comme souvent, les paramètres en disent un peu trop sur les sources des médias…



On copie tout ça dans notre Navigateur, et on affiche, on pensera au passage à « nettoyer » cette URL, soit www.youtube.com/v/cAHjGE32em0 . On sort ensuite son petit Wireshark, et on lance la lecture sur le navigateur. On va pouvoir tracer l'origine des trames réseaux, et donc la vidéo, car il n'y a aucun cryptage.



Intéressant, nous avons là un GET /get_video_info?video_id=cAHjGE32em0 avec une réponse très bavarde. Voici le contenu de la réponse…

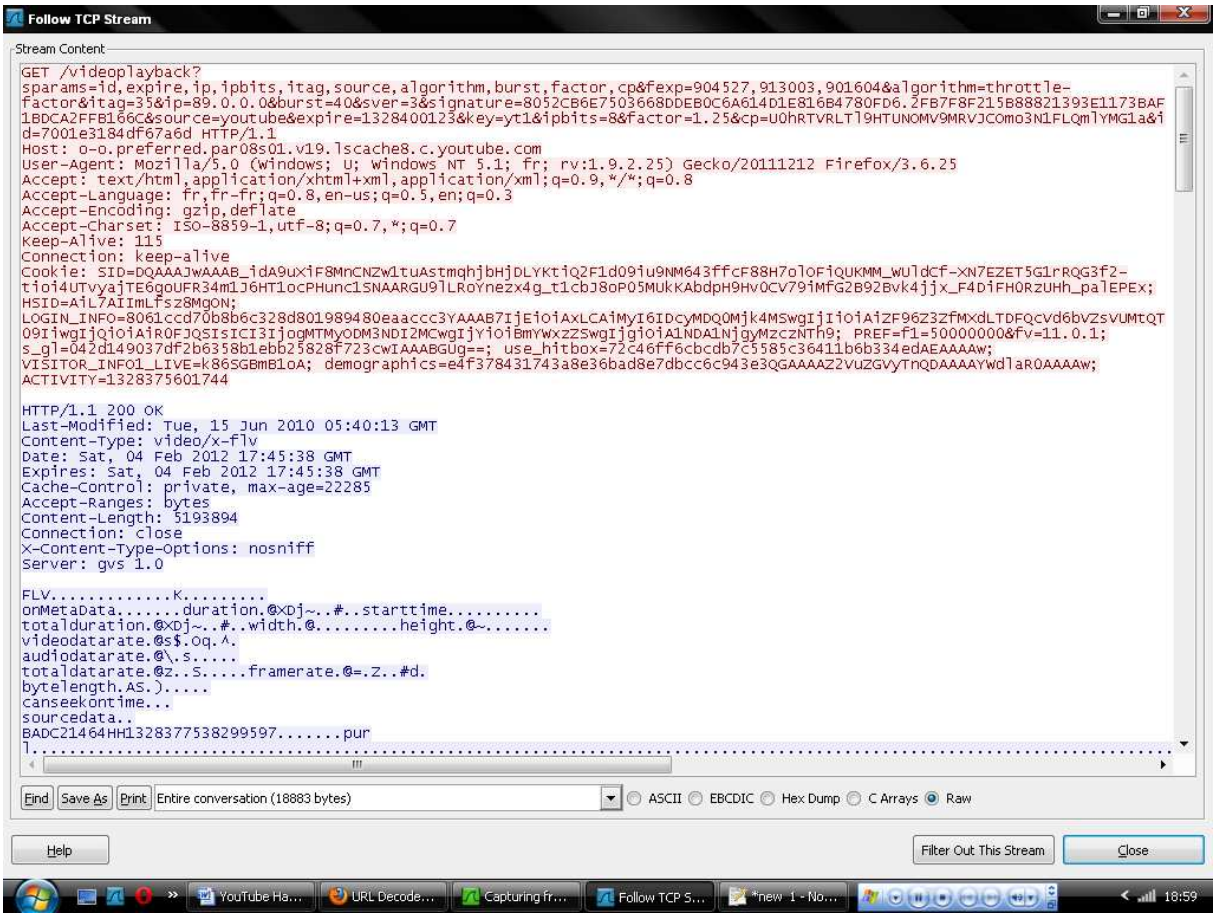

```
account_playback_token=N9vJKMWgcWq73bqnmZkoKxs6nJF8MEAxMzI4Mzc1Nzky&
allow_embed=1&vq=auto&fexp=904527%2C913003%2C901604&allow_ratings=1&
keywords=clawfinger%2Center%2Cthe%2Cmatrix%2Csoundtrack%2C15%2Cminut
es%2Cof%2Cfame%2Cinstrumental%2Csedman211%2Cost&track_embed=0&view_c
ount=15728&fmt_list=45%2F1280x720%2F99%2F0%2F0%2C22%2F1280x720%2F9%2
F0%2F115%2C44%2F854x480%2F99%2F0%2F0%2C35%2F854x480%2F9%2F0%2F115%2C
43%2F640x360%2F99%2F0%2F0%2C34%2F640x360%2F9%2F0%2F115%2C18%2F640x36
0%2F9%2F0%2F115%2C5%2F320x240%2F7%2F0%2F0&author=sedman211&muted=0&l
ength_seconds=98&iurlmaxres=http%3A%2F%2Fi4.ytimg.com%2Fvi%2FcAHjGE3
2em0%2Fmaxresdefault.jpg&user_age=29&has_cc=False&ftoken=kKF94tW54Yk
ROPZuuu6R83EhD3N8MTMyODQ2MjE5MkAxMzI4Mzc1Nzky&iurlsd=http%3A%2F%2Fi4
.ytimg.com%2Fvi%2FcAHjGE32em0%2Fsddefault.jpg&status=ok&watermark=%2
Chttp%3A%2F%2Fs.ytimg.com%2Fyt%2Fimg%2Fwatermark%2Fyoutube_watermark
vflHX6b6E.png%2Chttp%3A%2F%2Fs.ytimg.com%2Fyt%2Fimg%2Fwatermark%2Fyo
utube_hd_watermarkvflAzLcD6.png&timestamp=1328375792&plid=AAS4Jpc8sV
V_fB1P&endscreen_module=http%3A%2F%2Fs.ytimg.com%2Fyt%2Fswfbin%2Fend
screen-vfl-
YxJV9.swf&watch_ajax_token=ckteZotKnq_Ts9K3irQOwWemsrB8MTMyODQ2MjE5M
kAxMzI4Mzc1Nzky&url_encoded_fmt_stream_map=url%3Dhttp%253A%252F%252F
oo.preferred.par08s01.v1.lscache1.c.youtube.com%252Fvideoplayback%25
3Fsparams%253Did%25252Cexpire%25252Cip%25252Cipbits%25252Citag%25252
Csource%25252Cratebypass%25252Ccp%2526fexp%253D904527%25252C913003%2
5252C901604%2526itag%253D45%2526ip%253D89.0.0.0%2526signature%253D68
703E653B70ECF87AFBB309EE1B35FB4A9D8457.772B0CB3BDDEF7DB4783C25F326A2
F286EA948F9%2526sver%253D3%2526ratebypass%253Dyes%2526source%253Dyou
tube%2526expire%253D1328400123%2526key%253Dyt1%2526ipbits%253D8%2526
cp%253DU0hRTVRLTl9HTUNOMV9MRVJCOmo3N1FLQmlYMG1a%2526id%253D7001e3184
df67a6d%26quality%3Dhd720%26fallback_host%3Dtc.v1.cache1.c.youtube.c
om%26type%3Dvideo%252Fwebm%253B%2Bcodecs%253D%2522vp8.0%252C%2Bvorbi
s%2522%26itag%3D45%2Curl%3Dhttp%253A%252F%252Fo-
o.preferred.par08s01.v18.lscache3.c.youtube.com%252Fvideoplayback%25
3Fsparams%253Did%25252Cexpire%25252Cip%25252Cipbits%25252Citag%25252
Csource%25252Cratebypass%25252Ccp%2526fexp%253D904527%25252C913003%2
5252C901604%2526itag%253D22%2526ip%253D89.0.0.0%2526signature

[...]
```

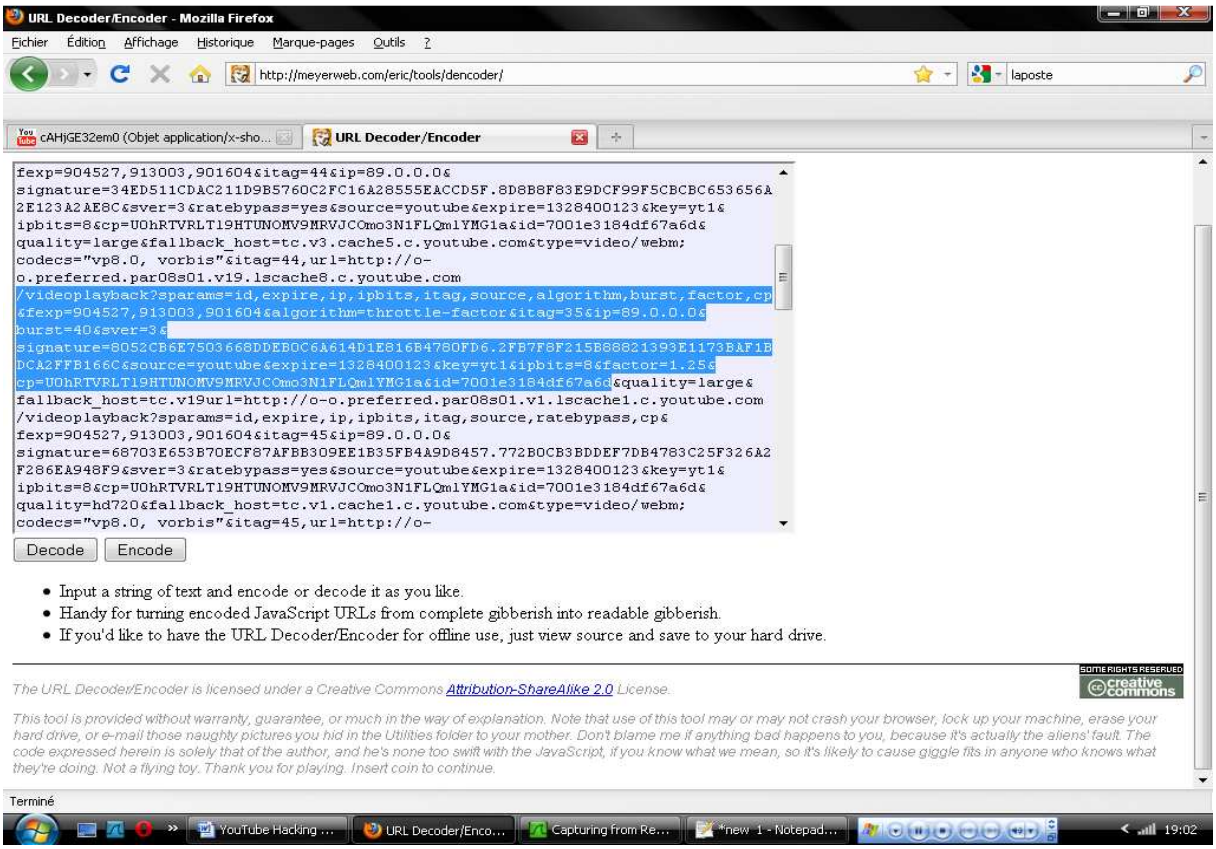

La réponse étant très longue, j'ai coupé un peu (beaucoup…). Avec notepad++ on remet tout ça en forme (remplacer « & » par « &\n » via le mode étendu).

On « URL Decode » la variable url_encoded_fmt_stream_map, et en regardant de plus près via une petite recherche dans le résultat « décodé », on s'aperçoit que la requête est en fait incluse dans cette opacité de donnée.

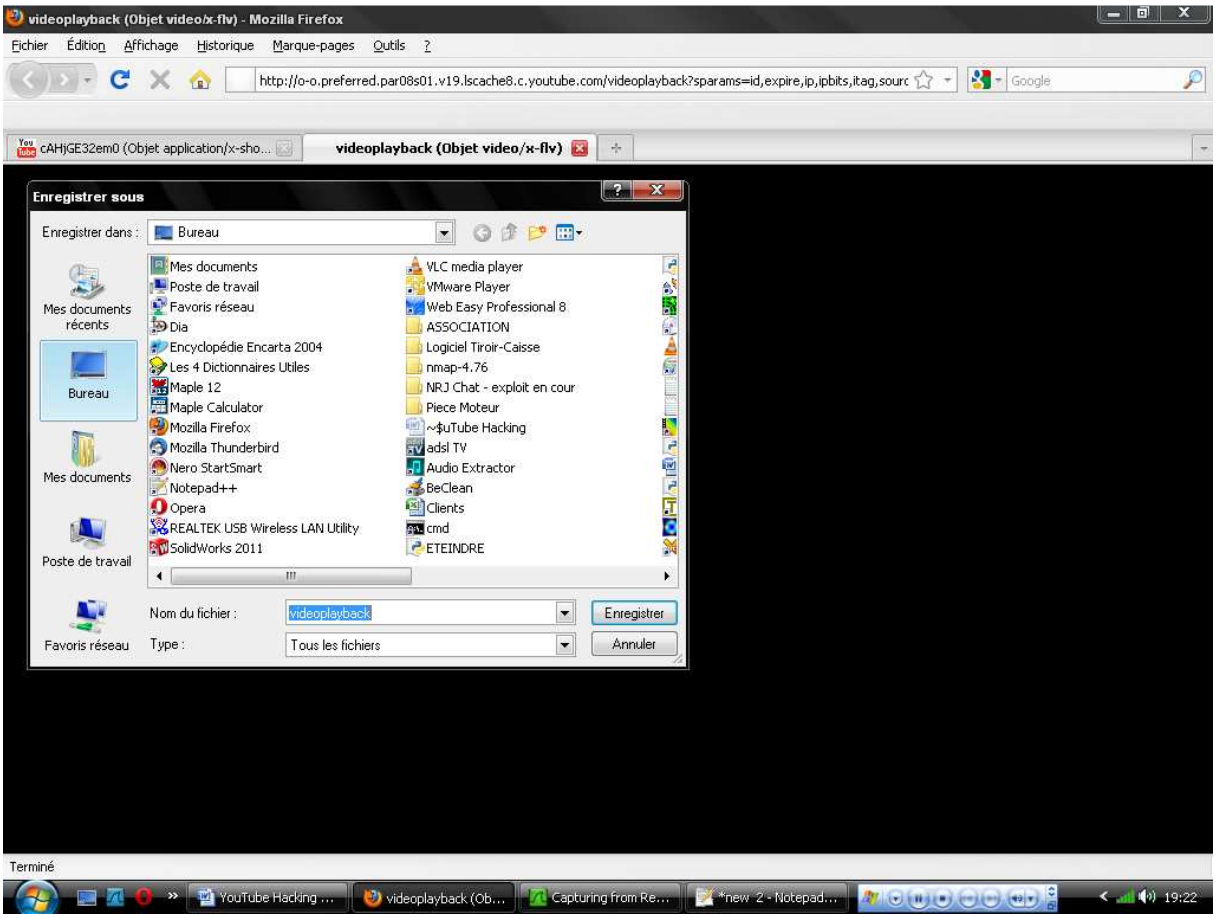
Voici ce que cela donne sous Wireshark, et si vous faites une recherche de la variable « signature », vous trouverez l'URL exacte…



Voici ce que nous cherchions…



Le travail étant fait, il n'y a plus qu'à coller ça dans le navigateur et enregistrer notre vidéo FLV.



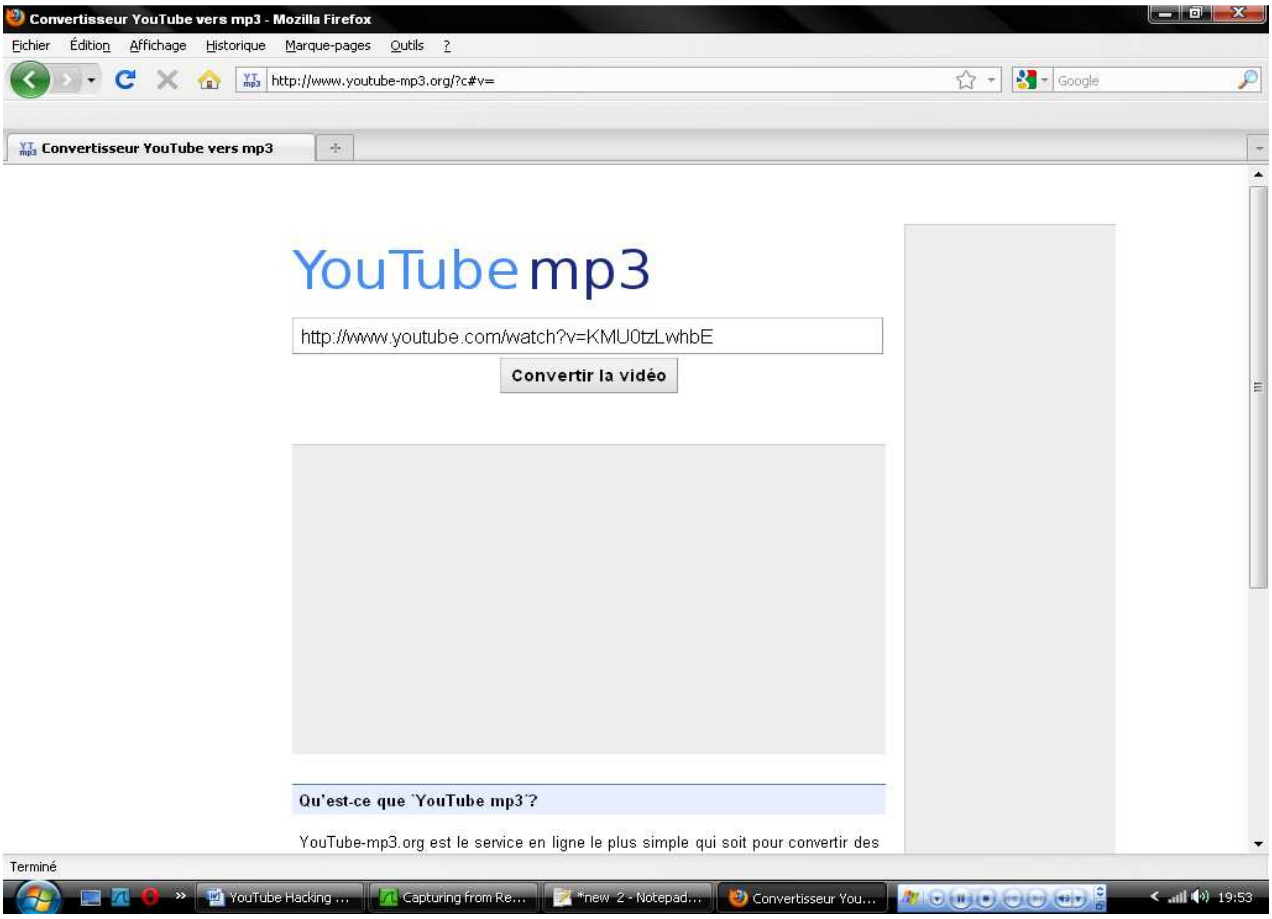
Pour résumer, il nous suffit globalement d'effectuer une simple requête /get_video_info?video_id=cAHjGE32em0 pour pouvoir ressortir le fichier d'information, d'analyser ce dernier pour ressortir l'URL source, et télécharger notre fichier FLV.

GET Télécharges_moi_ça HTTP/1.0

Depuis la création de YouTube de nombreux sites ont vu le jour afin de permettre aux utilisateurs lambda de télécharger les vidéos diffusées. Beaucoup permettent des choses intéressantes et rapides, en plus des logiciels spécialisés comme FLV Downloader, ou YouTube Downloader.

Le problème avec ces logiciels, c'est qu'ils ne fonctionnent pas toujours comme on le voudrait.

- **YouTube MP3 : http://www.youtube-mp3.org**



Ce site permet comme son nom l'indique de télécharger sous le format MP3 le « son » des vidéos en fournissant simplement l'URL de celle-ci.

Avec une simple recherche sur Google, on peut trouver une multitude de sites/logiciels capables d'effectuer ce genre d'actions.

Outils

- **Wireshark : http://www.wireshark.org/download.html**
- **WinPCAP : http://www.winpcap.org/install/default.htm**
- **Unlocker : http://www.emptyloop.com/unlocker/**
- **URL Encoder/Decoder : http://meyerweb.com/eric/tools/dencoder/**