Tracer un Flux Vidéo

Ou comment remonter à la source d'une vidéo…

Sophocle

10/10/2011

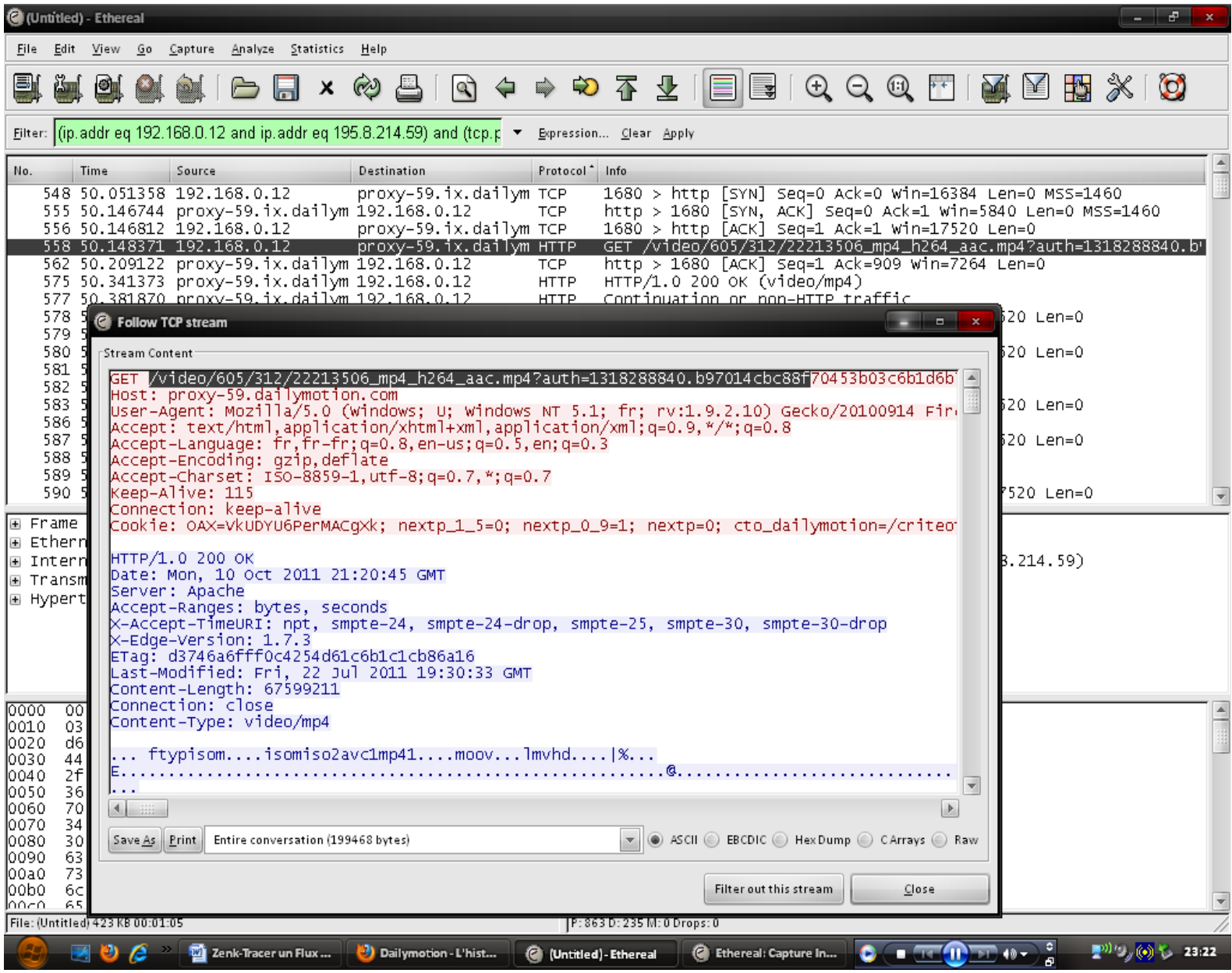
- ## Tracer une Vidéo Daylimotion

Daylimotion est un site web permettant de lire des vidéos en streaming directement depuis ce dernier. Mais quelques fois, par soucis de facilité, certaines personnes préfèrent – lorsqu'une telle option est disponible – télécharger la vidéo plutôt que d'être obligé de se connecter à chaque fois sur un serveur uniquement pour la visualiser.

Ce document a été écrit dans ce but, et pour cette démonstration, je vais vous montrer comment avec un simple analyseur réseau (Wireshark, Ethereal…) et un navigateur (Firefox, IE, Opera…) il est possible de remonter la source d'un signal vidéo reçu sur des sites comme Daylimotion, Youtube, ARTE...

Pour cette étude, je vais choisir comme vidéo « L'histoire interdite du piratage informatique 1.3 ».

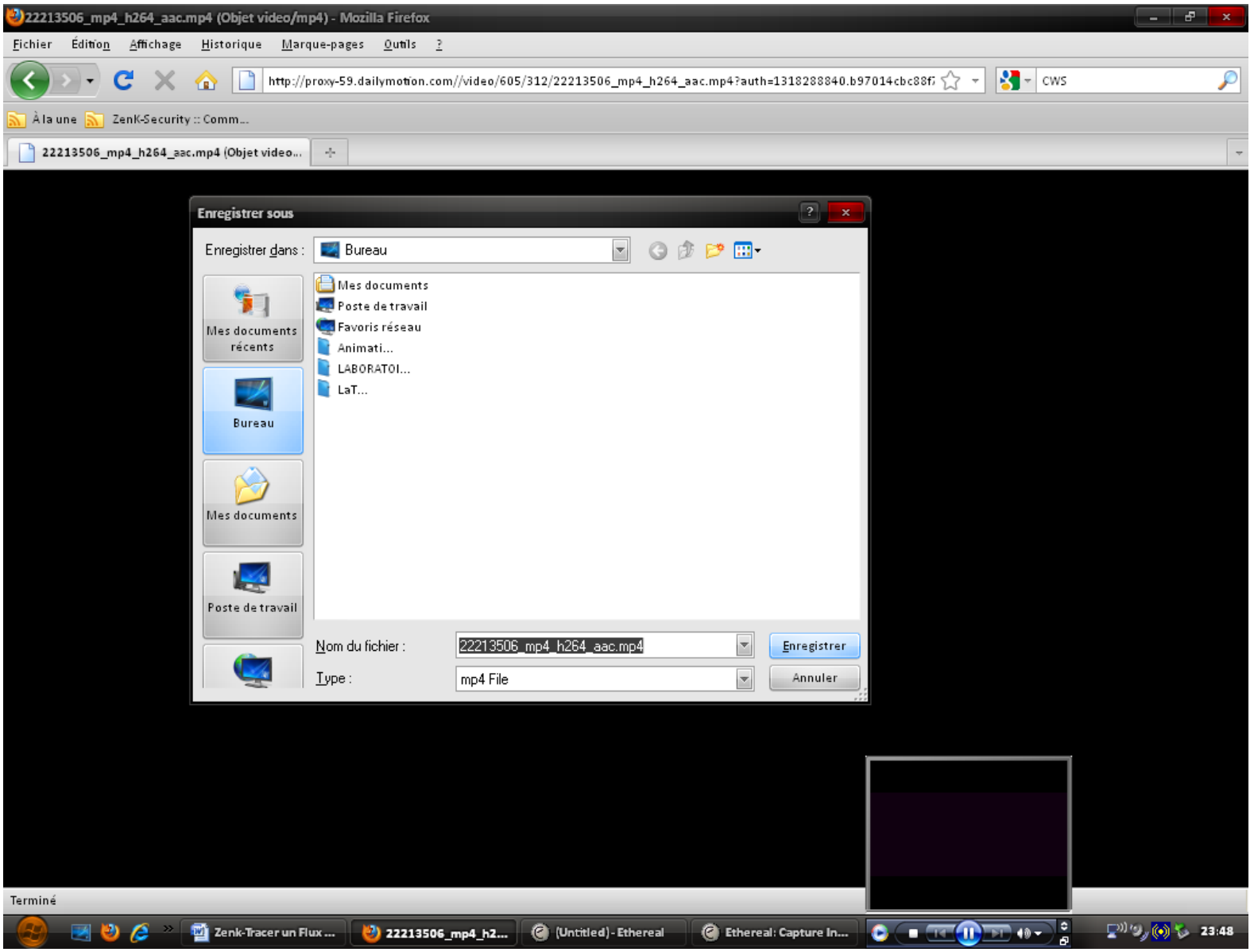
À partir de là, on lance une analyse réseau et on cherche tout simplement à obtenir la source du flux vidéo, qui au passage est au format MP4 sur ce site.



Je disais donc, on lance son sniffeur préféré (Ethereal pour la démo), on lance une capture réseau, on recharge sa page Daylimotion (afin de relancer une requête HTTP sur la source d'origine), on place un filtre sur la transaction via un petit « Follow TCP Stream » [Clic Droit], et on obtient l'écran ci-dessus.

On retrouve bel et bien l'hôte cible (un Reverse Proxy de prime abord…), et le fichier source en MP4. Une fois remis en forme, on obtient l'URL d'origine du fichier qu'il suffit juste de copier dans la barre d'adresse (F6) , soit « proxy-59.dailymotion.com/video/605/312/22213506_mp4_h264_aac.mp4?auth=1318288840.b97014cbc88f70453b03c6b1d6b7ecb5 ».

Ce qui nous donne finalement avec Firefox …



Cet exemple était très simpliste et se base sur HTTP, mais d'autres sites comme ARTE, utilise le protocole RTMP et quelques crytages, il vaut donc mieux utiliser RTMP Dump par facilité.

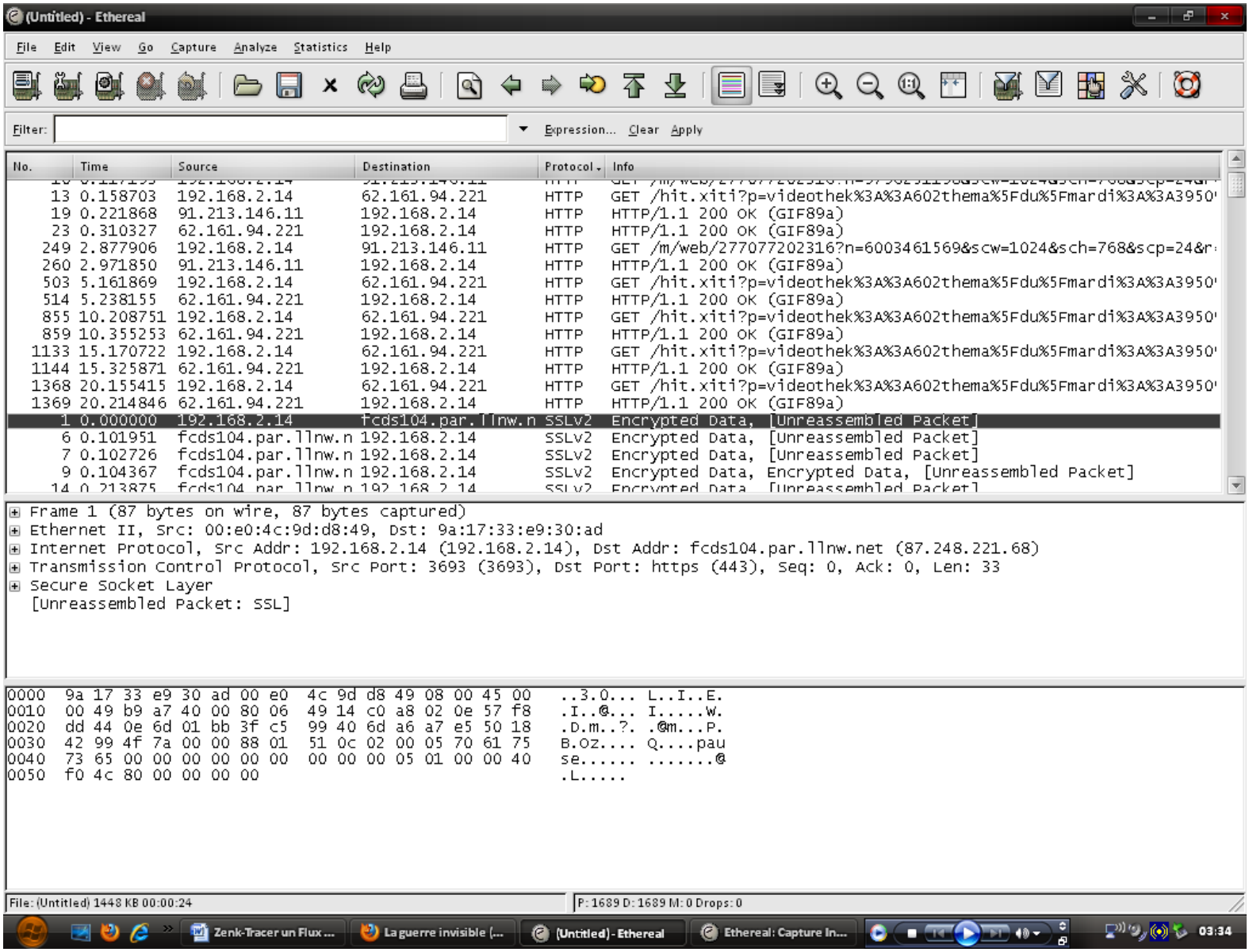
- ## Tracer une Vidéo ARTE

À présent que les bases sont posées, nous allons découvrir que certains sites internet se défendent plutôt pas mal contre ce genre de menace (qui au passage, peut être assimilé à un viol de Copyright !!).

Bien, on commence par ce que nous connaissons : le sniffing. Mécaniquement vous allez vous dire « On a qu'à exécuter un GET sur la page affichant la vidéo, capturer le traffic via Ethereal/Wireshark, remonter l'origine du flux dans le logiciel, et sauvegarder avec le navigateur… ». OK essayons !!

Je choisi comme source vidéo « La Guerre Invisible ½ » disponible sur http://videos.arte.tv/fr/videos/la_guerre_invisible_extrait_1_2_-3952072.html

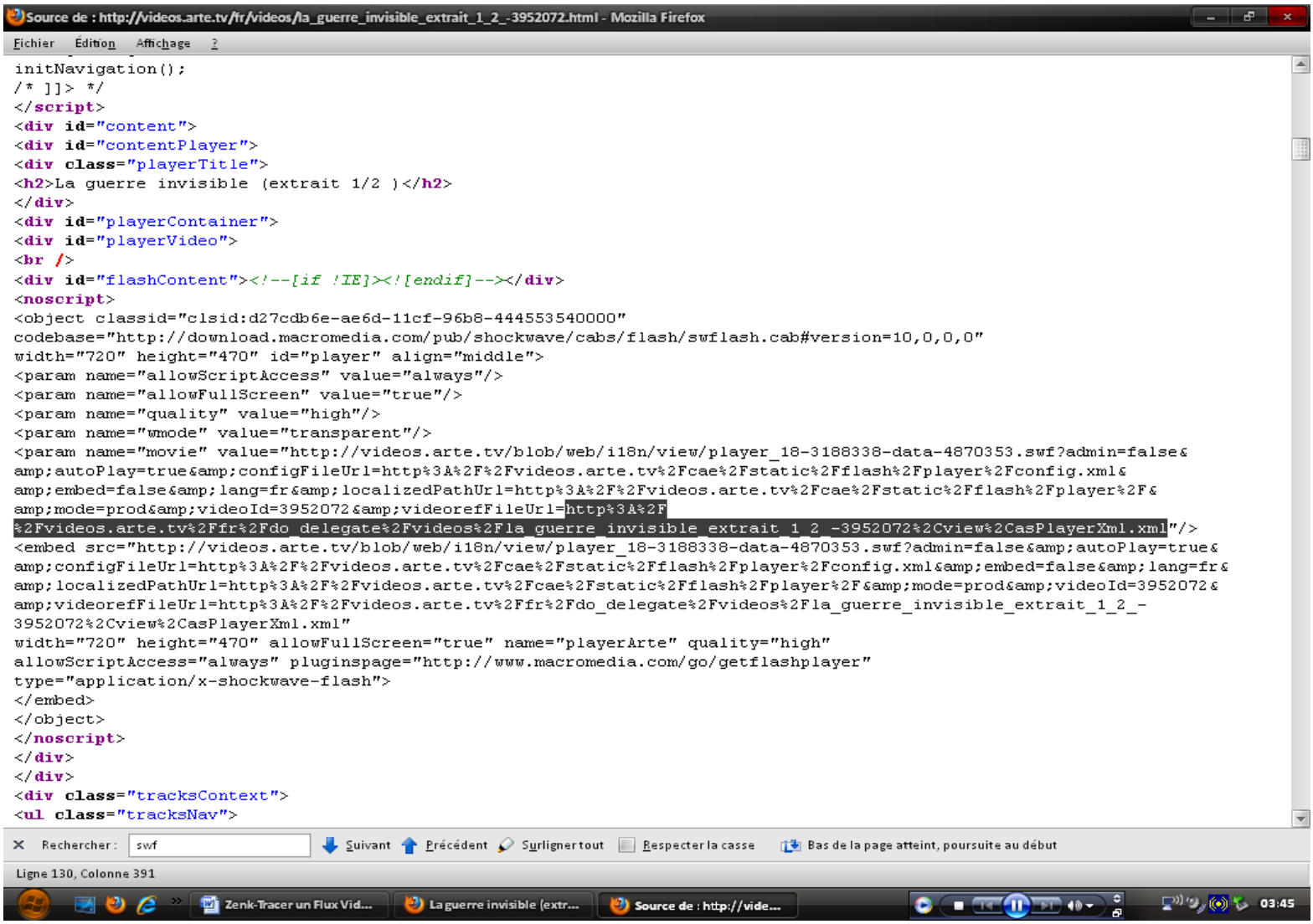
On lance la requête, on sniff les trames réseaux, et on observe tranquillement le résultat…



Oh mince… Que vois-je ?! Un Cryptage SSLv2 !! Et oui, comme dit plus haut, certains sites utilisent quelques techniques simples mais très efficaces pour se protéger. Le fonctionnement pourrait être le suivant :

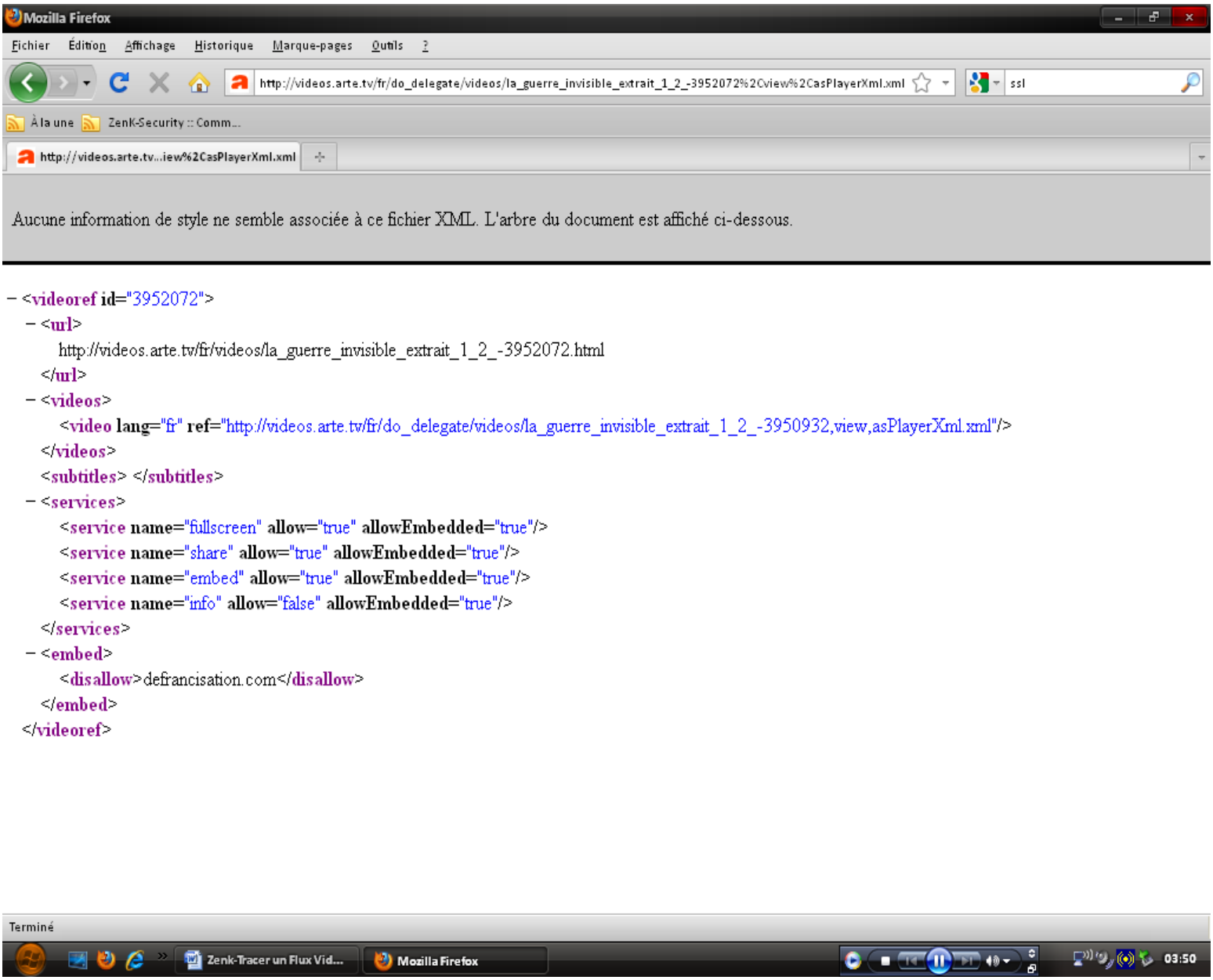
- **Le navigateur télécharge le lecteur vidéo propriétaire du site**
- **Le player télécharge petit à petit la vidéo en cryptant la liaison avec le serveur (via SSL)**
- **Le player décrypte à la volé, et affiche à l'écran**

Mais réfléchissons, SSL permet de protéger les données qui transitent sur un réseau, par sur un système. Donc de l'autre côté, comme du notre au travers du Player, le fichier est en clair !! Regardons un peu la source.



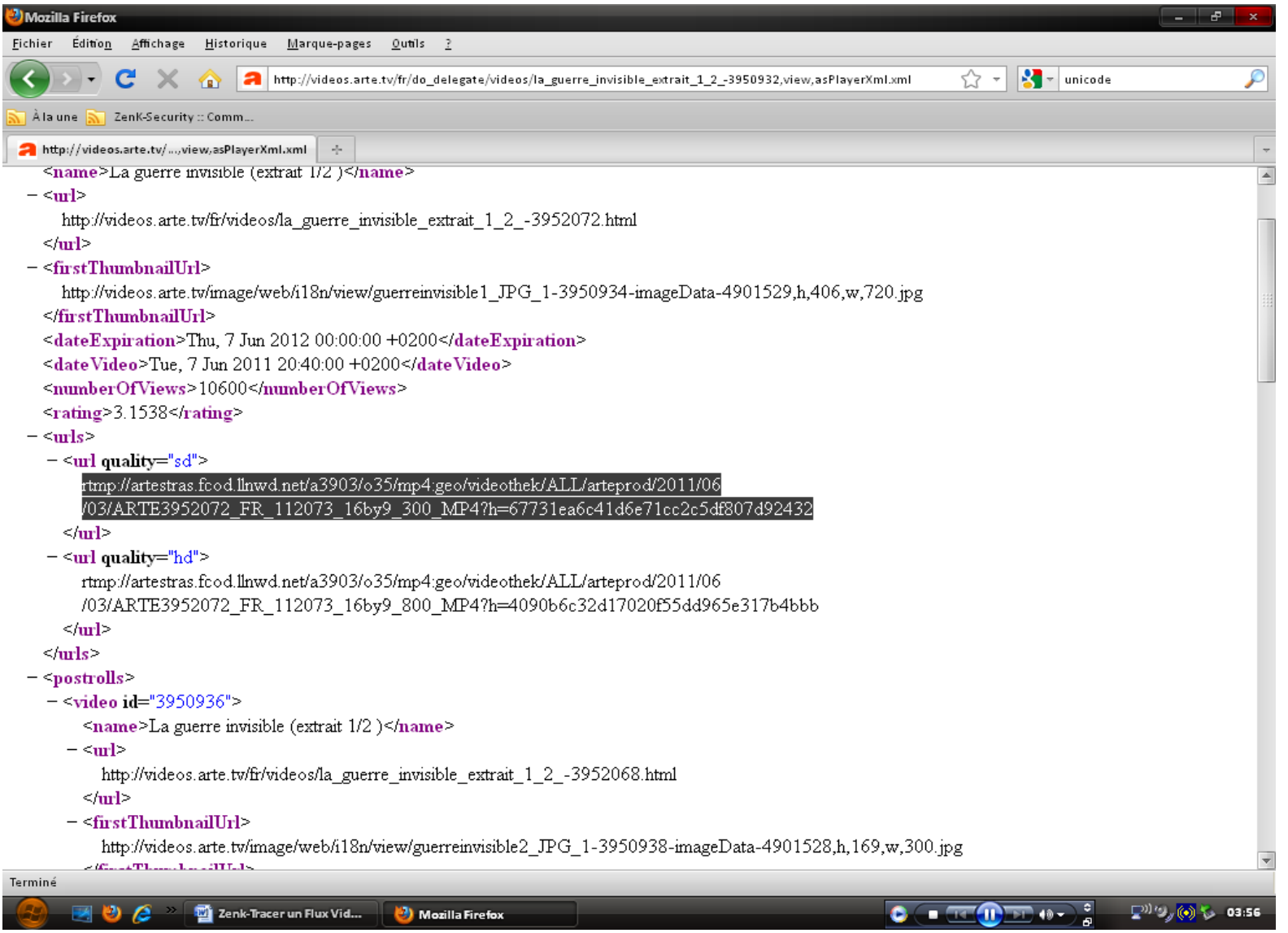
Un petit [CTRL+U], suivit d'une recherche sur le mot clé « SWF », et on tombe sur la plage de code gérant l'affichage de la vidéo sur la page. En y regardant de plus près, on trouve une variable intéressante : « videorefFileUrl ».

On Copie-Colle cet URL dans Firefox (après l'avoir remis en forme), et on observe quelque chose d'intéressant : Un fichier XML plein d'informations !!



Ce fichier source XML contient un lien vers un autre fichier XML « ligne 6 ». Et en affichant ce dernier fichier avec son navigateur, on obtient l'origine du flux vidéo, et en clair qui plus est !!

Bien entendu, le Hack ne s'arrête pas ici, essayez d'ouvrir un protocole RTMP avec Firefox, vous verrez…

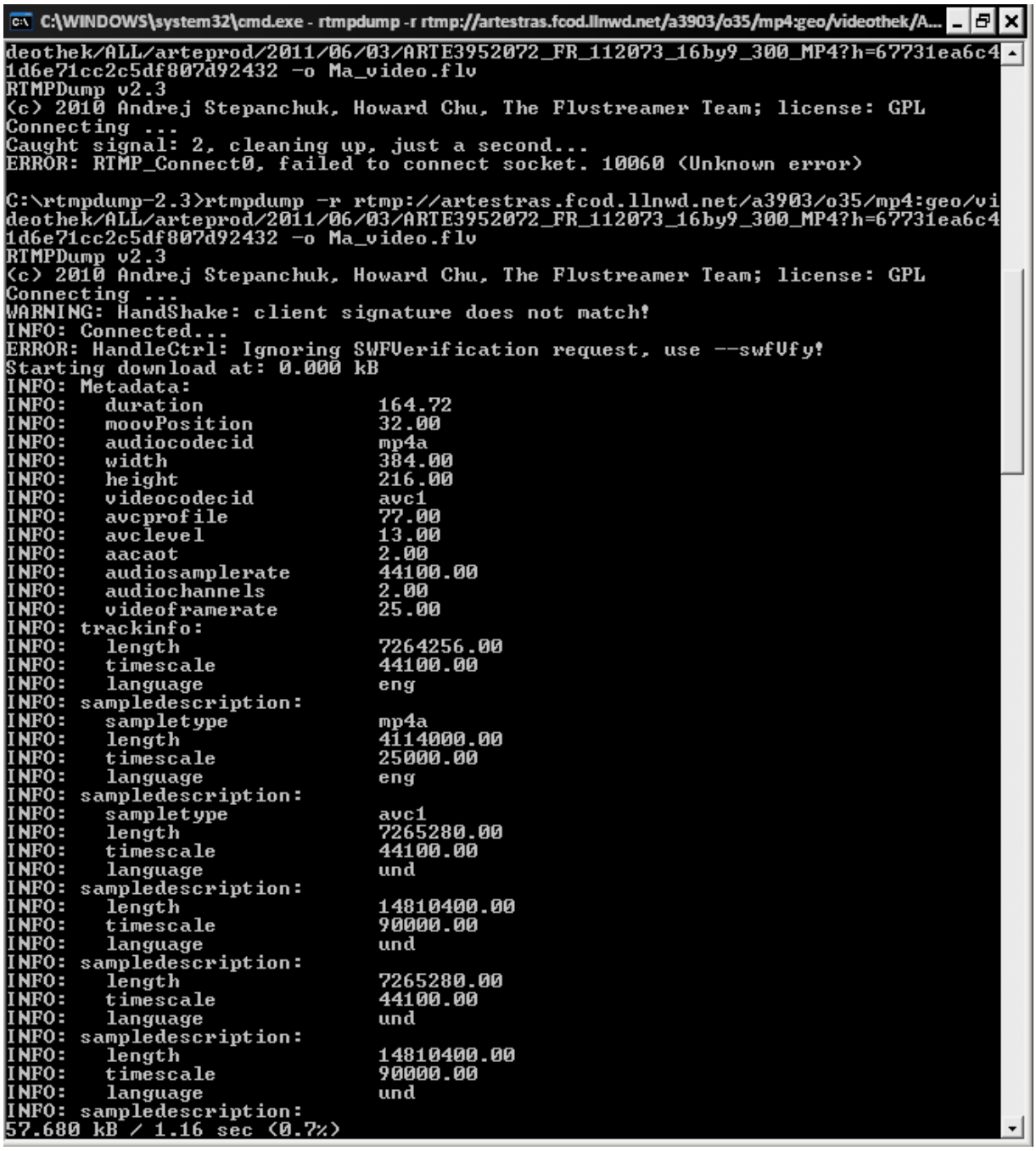


Maintenant que nous connaissons l'origine exacte du flux, il nous suffit d'en faire une copie sur Disque. Mais il faut en premier lieu le récupérer. Et pour ce faire, il existe un outil : RTMP Dump. C'est un programme portable et open-source disponible à l'adresse fournit en bas de document.

On ouvre son Invite de Commande favorite, on se place dans le répertoire de RTMP Dump, et on a plus qu'à télécharger gentiment .

Commande : rtmpdump -r rtmp://artestras.fcod.llnwd.net/a3903/o35/mp4:geo/videothek/ALL/arteprod/2011/06/03/ARTE3952072_FR_112073_16by9_300_MP4?h=67731ea6c41d6e71cc2c5df807d92432 -o Ma_Video.flv

L'extension FLV est qui plus est une erreur car c'est du MP4… Pas grave.



- ## Outils

Wireshark : http://www.wireshark.org/download.html

RTMP Dump : http://rtmpdump.mplayerhq.hu/download

WinPCAP : http://www.winpcap.org/install/default.htm

Amusez-vous bien ;)