Ripping Media Off of the Wire
A Step-by-Step Guide

By Honey

honey.rtmp@gmail.com

whoami: Honey is

- a Network Administrator for 4+ years
- a Research Assistant for a Ballistic research grant by the NIST
- an Adjunct Professor at John Jay College of Criminal Justice, located in NYC
- gaining her Master's degree in Forensic Computing
- has worked in the IT industry for the past 9+ years.
- holds a Computer of Information Systems B.S.
- dual A.A.S. degrees in Industrial Electronic Engineering and Computer Networking

Scope: Download MP3s from

myspace.com

YouTube

- Discussion of lack of security of "protected streaming" implementations

Tools:

- wget version 1.11.4i
- Mozilla Firefox version 3.6.3ii
- an add-on for Mozilla Firefox called: “HttpFox” version 0.8.4iii
- rtmpdump version 2.1b for windowsiv
- “Convert FLV to MP3 version 1.0”
- ** All tools used are available for use under the GNU license. Specific versions are cited although may not be required*

Disclosure:

- This presentation describes methods to download protected materials in an effort raise awareness of the various weaknesses that exist within each implementation.
- All music/media used in this demonstration has the appropriate permissions for use by the musical artists themselves.
- Any illegal use of the following methods by third parties is the sole responsibility of the third party.
- The author of this presentation bares no legal responsibility for misuse of said techniques.

Legal Statement:

- The following demonstration does violate YouTube‘s terms of service, MySpace’s terms of service, and the Digital Millennium Copyright Act, and intellectual property rights, should you download copyrighted materials.
- YOUR USE OF THE INCLUDED TECHNIQUES SHALL BE AT YOUR OWN RISK.
- IN NO EVENT SHALL THE PRESENTER, DEFCON, OR ANY DEFCON EMPLOYEES, BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES WHATSOEVER RESULTING FROM ANY (I) ERRORS, MISTAKES, OR INACCURACIES OF CONTENT, (II) PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM YOUR USE OF THE FOLLOWING TECHNIQUES.

Before We Begin: some thoughts

- Not everything is on USENET
- Third party plug-ins are not always reliable or kept current with changes
- You got an MD5 sum on that MP3? I didn't think so!
- Third parties could be injecting into your media if you are trusting them to convert things for you online
- **This presentation is not intended to encourage piracy, but is about the dissemination or data/media and the failing security methods for "protected streaming"**

RTMP:

- is “Real Time Messaging Protocol” and is a proprietary protocol developed by Adobe Systems for streaming audio, video and data over the Internet, between a Flash player and a server.
- The RTMP protocol has three variations:
  - RTMP itself works on top of TCP and uses port number 1935
  - RTMPT is encapsulated within HTTP requests to traverse firewalls
  - RTMPS which is RTMP, but over a secure HTTPS connection.

RTMPE:

- is “Encrypted Real Time Messaging Protocol” and is a proprietary protocol created by Macromedia used for streaming video and DRM. It *supposedly* allows secure transfer of data without SSL. It is implemented in flash player 9.0.115 and some versions of Flash Media Server 3.

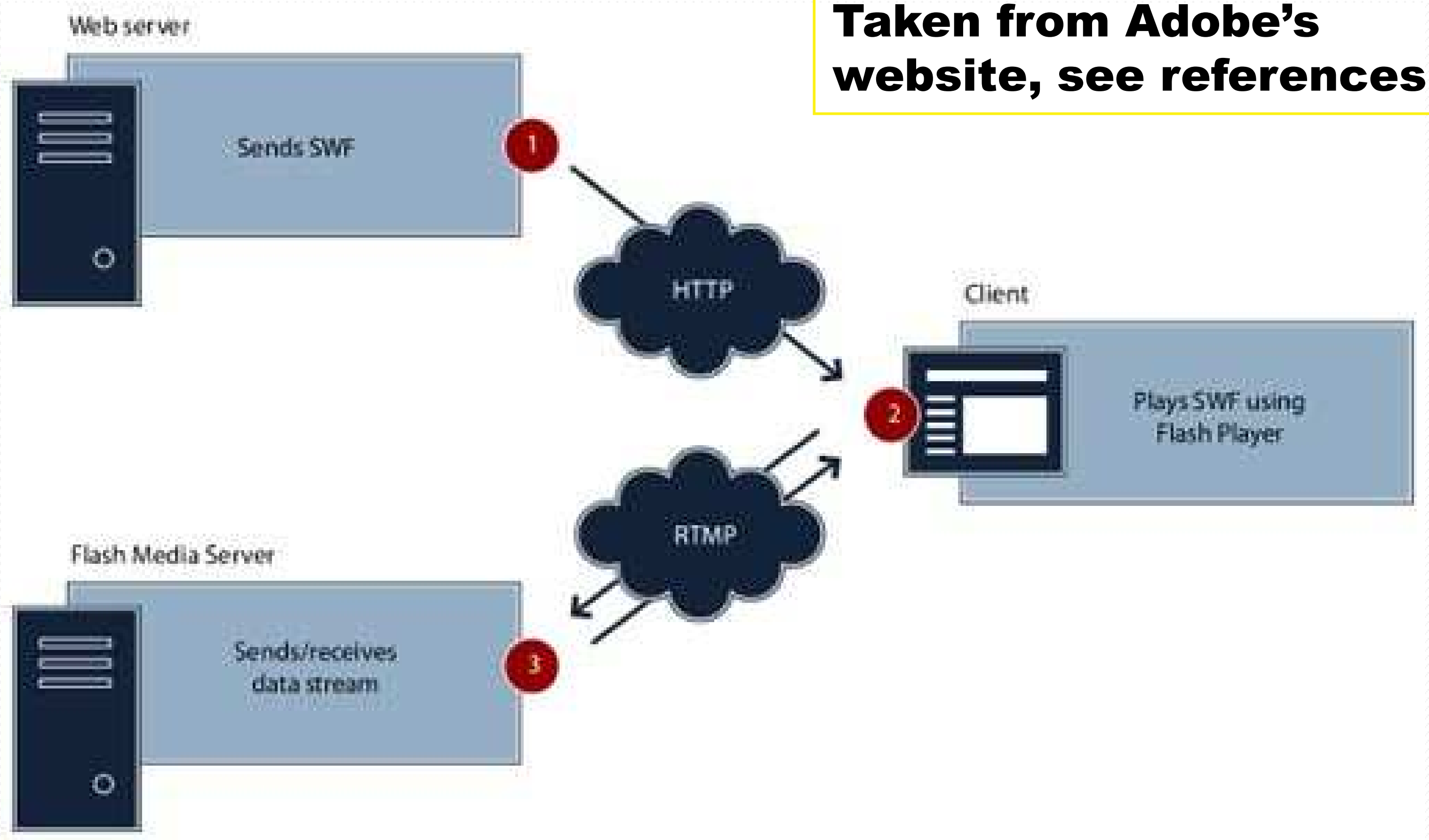
Taken From Adobe's Website

"Defend against replay technologies

Replay technologies, or "stream ripping," has been a difficult security issue to solve because it allows the viewer to directly access and record the data of a stream.

Stream encryption prevents stream ripping. In the past, SSL was the only choice and was too slow for most applications. ***With FMS 3, we now have the RTMPE protocol which is much more efficient and easier to implement."***

- "Flash Media Server communicates with its clients using the Adobe patented, Real-Time Messaging Protocol (RTMP) over TCP that manages a two-way connection, allowing the server to send and receive video, audio, and data between client and server (see Figure 1). In FMS 3, you also have the option to utilize stronger stream security with encrypted RTMP (RTMPE). RTMPE is easy to deploy and faster than utilizing SSL for stream encryption. RTMPE is just one of the robust new security features in FMS 3. (This will be discussed more in the following sections.)"



Taken from Adobe's website, see references.

Adobe Describing DRM:

- *“Digital rights management (DRM) has two key elements, encryption and access control. There are two ways to deliver video to a consumer: stream it or download it. When you stream video from Flash Media Server, you immediately increase your protection.*

- *Encryption with Flash Media Server is done in real time with RTMPS (SSL) or RTMPE in Flash Media Server 3.”*

Rtmpdump and what it does:

The following text is from the rtmpdump readme:

- HTTP gateway: this is an HTTP server that accepts requests that consist of rtmpdump parameters. It then connects to the specified RTMP server and returns the retrieved data in the HTTP response.

- all subsequent audio/video data received from the server will be written to a file, as well as being delivered back to the client.

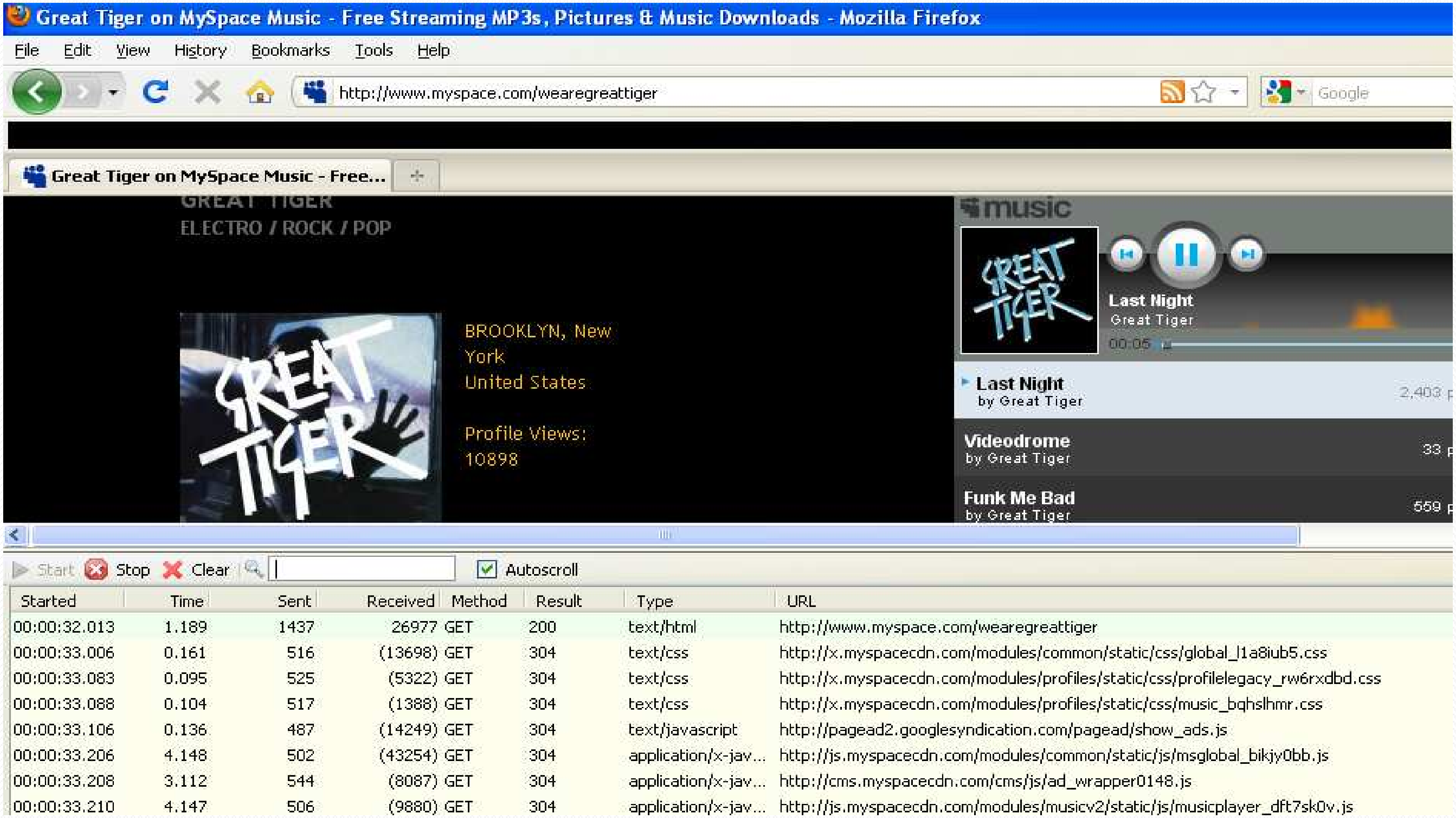
Let’s Get This Party Started:

- HowTO: Get mp3 files from MySpace

- Step One: Install your HttpFox Firefox Plugin.

- Step Two: **Start** HttpFox and go to the target MySpace page.

For my example, I will be downloading an MP3 from my favorite Brooklyn-based band called: "Great Tiger". When I first discovered these guys, their music was available ONLY on MySpace. Clearly, I wanted to be able to listen to their great music if my Internet connection went down or something ☺.



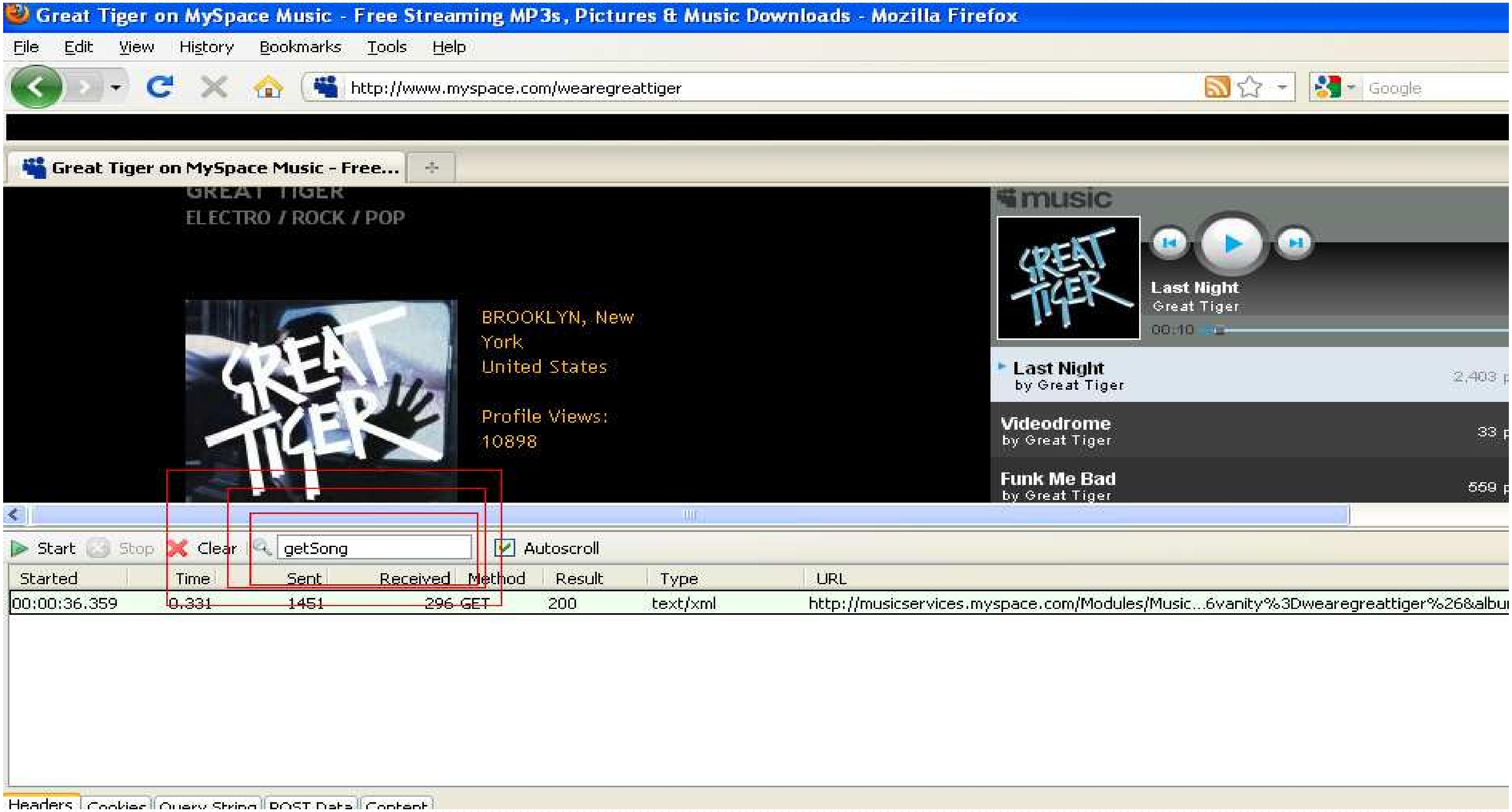
Great Tiger on MySpace Music - Free Streaming MP3s, Pictures & Music Downloads - Mozilla Firefox

http://www.myspace.com/wearegreattiger

Started	Time	Sent	Received	Method	Result	Type	URL
00:00:32.013	1.189	1437	26977	GET	200	text/html	http://www.myspace.com/wearegreattiger
00:00:33.006	0.161	516	(13698)	GET	304	text/css	http://x.myspacecdn.com/modules/common/static/css/global_l1a8iub5.css
00:00:33.083	0.095	525	(5322)	GET	304	text/css	http://x.myspacecdn.com/modules/profiles/static/css/profilelegacy_rw6rxdbd.css
00:00:33.088	0.104	517	(1388)	GET	304	text/css	http://x.myspacecdn.com/modules/profiles/static/css/music_bqhslhmr.css
00:00:33.106	0.136	487	(14249)	GET	304	text/javascript	http://pagead2.googlesyndication.com/pagead/show_ads.js
00:00:33.206	4.148	502	(43254)	GET	304	application/x-jav...	http://js.myspacecdn.com/modules/common/static/js/msglobal_bikjy0bb.js
00:00:33.208	3.112	544	(8087)	GET	304	application/x-jav...	http://cms.myspacecdn.com/cms/js/ad_wrapper0148.js
00:00:33.210	4.147	506	(9880)	GET	304	application/x-jav...	http://js.myspacecdn.com/modules/musicv2/static/js/musicplayer_dft7sk0v.js

Step Three: Sift through the captured traffic.

Do a search for “getSong"



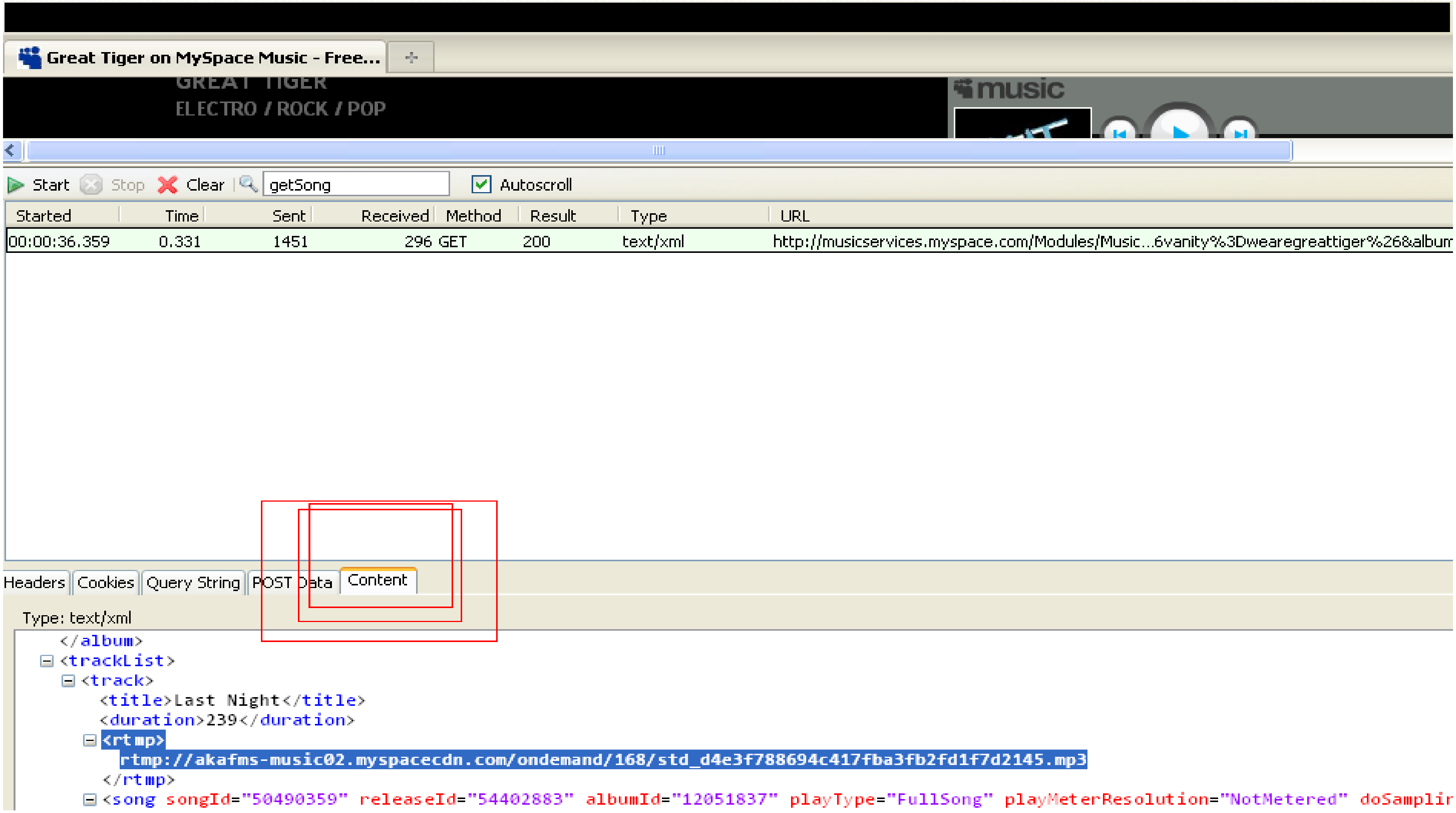
http://www.myspace.com/wearegreattiger

Search: getSong

☑ Autoscroll

Started	Time	Sent	Received	Method	Result	Type	URL
00:00:36.359	0.331	1451	296	GET	200	text/xml	http://musicservices.myspace.com/Modules/Music...6vanity%3Dwearegreattiger%26&albu

Step Four: Click on the "Content" tab at the bottom of HttpFox. Search through the XML file until you find a URL ending in “mp3”. Copy the URL. This URL is the actual location of the file hosted on their servers.



Started	Time	Sent	Received	Method	Result	Type	URL
00:00:36.359	0.331	1451	296	GET	200	text/xml	http://musicservices.myspace.com/Modules/Music...6vanity%3Dwearegreattiger%26&albur

Type: text/xml

```
    </album>
  <trackList>
    <track>
      <title>Last Night</title>
      <duration>239</duration>
     <rtmp>
       rtmp://akafms-music02.myspacecdn.com/ondemand/168/std_d4e3f788694c417fba3fb2fd1f7d2145.mp3
      </rtmp>
     <song songId="50490359" releaseId="54402883" albumId="12051837" playType="FullSong" playMeterResolution="NotMetered" doSamplir
```

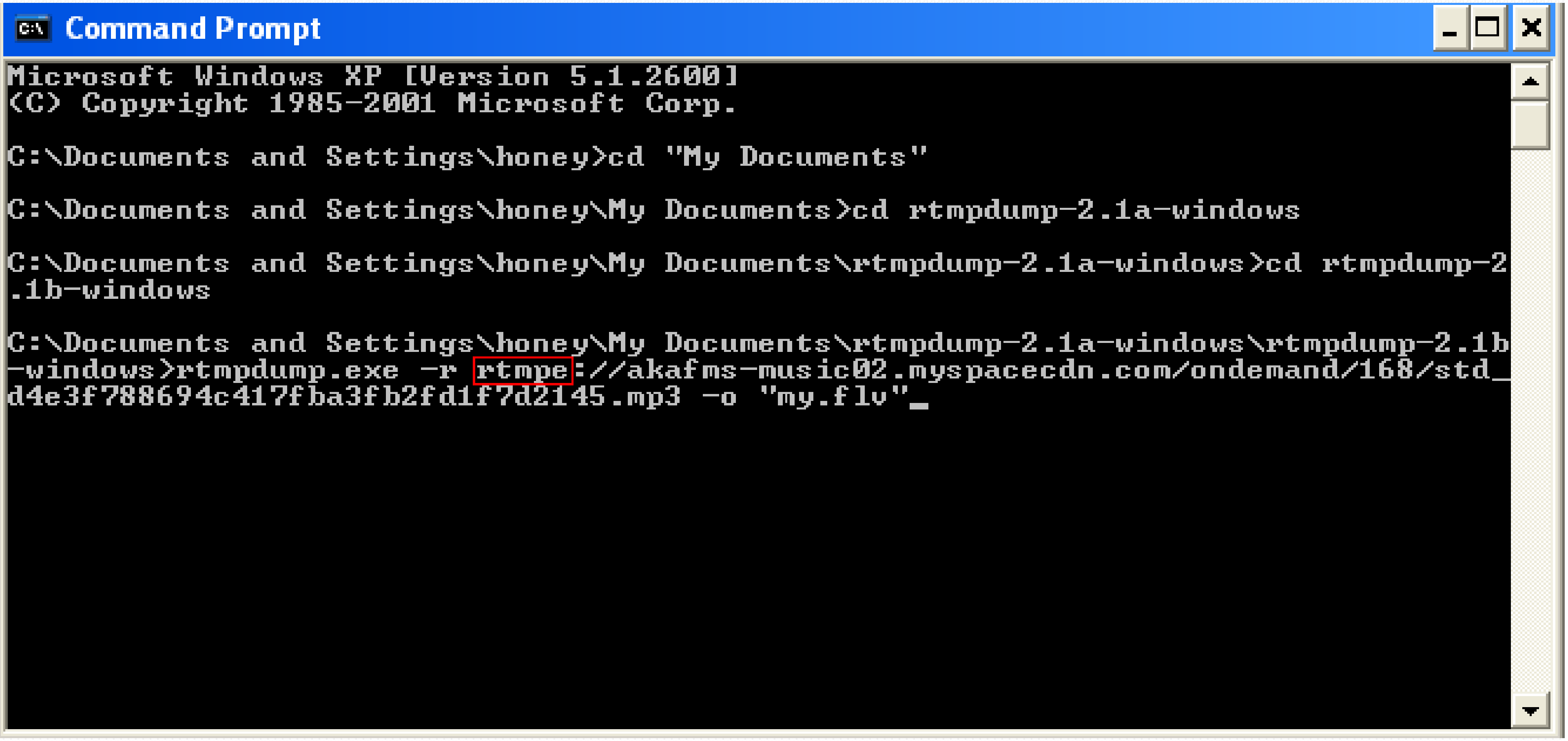
Step Five: Download rtmpdump. Here is the fun part: The xml url contains: "rtmp://" But they are really using rtmpe!

- Modify the captured URL.

** You have to replace the leading “rtmp://” to “rtmpe://” and then run the command:

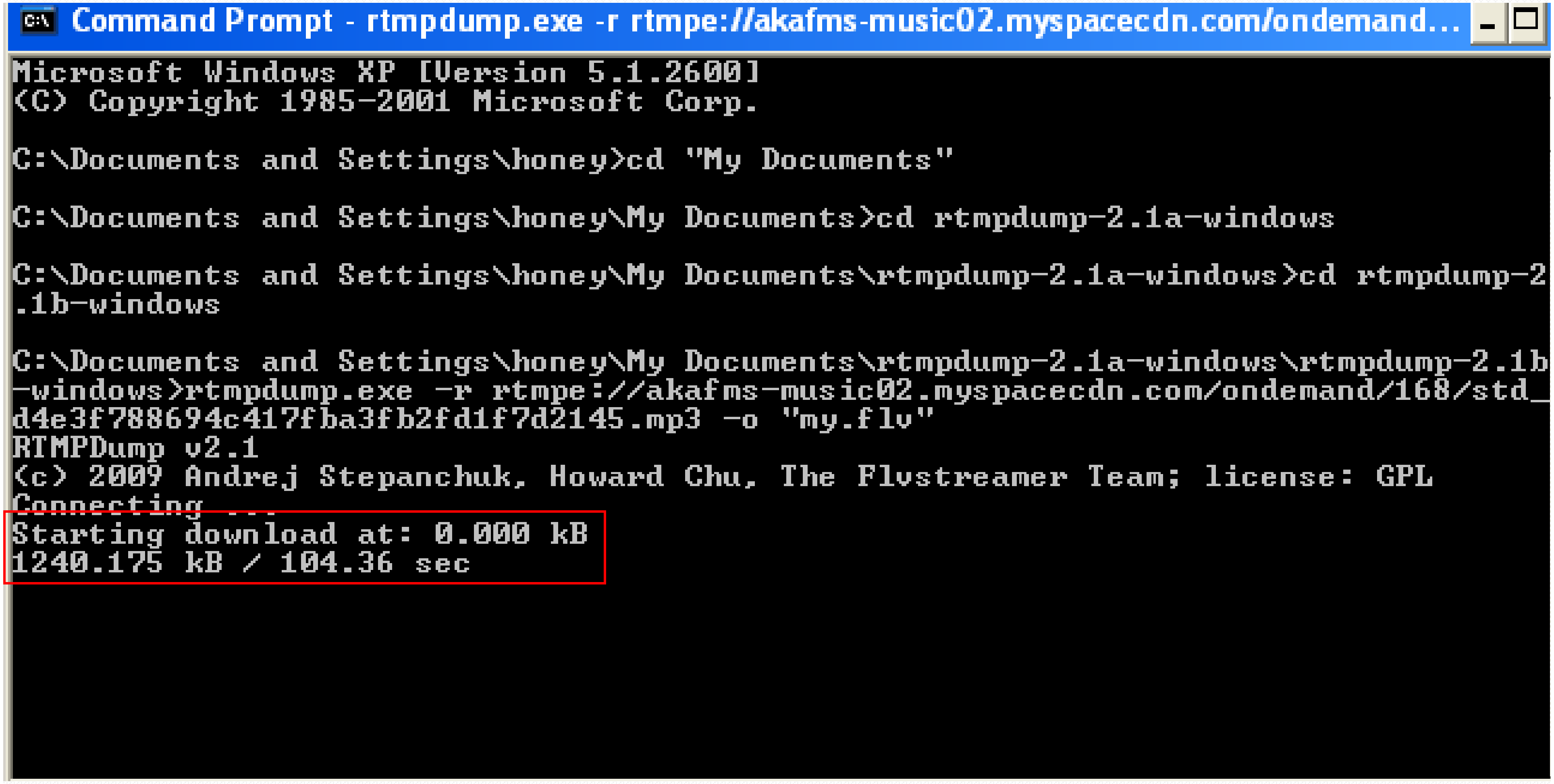
```
rtmpdump.exe –r [modified captured URL] –o “my.flv”
```

- Notice how I changed the leading rtmp to rtmpe when I issued the command within in the command prompt:



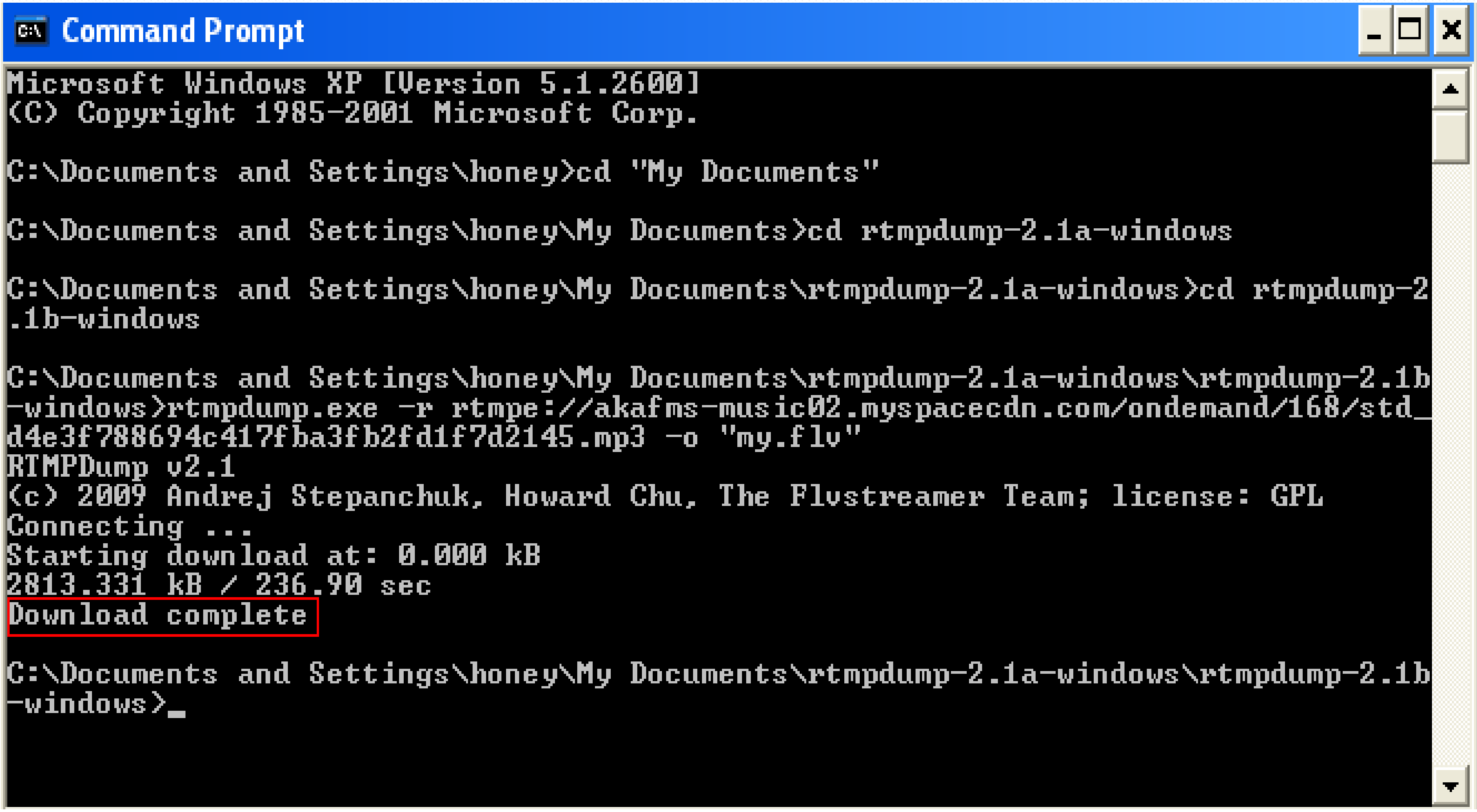
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\honey>cd "My Documents"

C:\Documents and Settings\honey\My Documents>cd rtmpdump-2.1a-windows

C:\Documents and Settings\honey\My Documents\rtmpdump-2.1a-windows>cd rtmpdump-2
.1b-windows

C:\Documents and Settings\honey\My Documents\rtmpdump-2.1a-windows\rtmpdump-2.1b
-windows>rtmpdump.exe -r rtmpe://akafms-music02.myspacecdn.com/ondemand/168/std_
d4e3f788694c417fba3fb2fd1f7d2145.mp3 -o "my.flv"_
```

Now execute the command and watch the download start!


Command Prompt - rtmpdump.exe -r rtmpe://akafms-music02.myspacecdn.com/ondemand...

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\honey>cd "My Documents"

C:\Documents and Settings\honey\My Documents>cd rtmpdump-2.1a-windows

C:\Documents and Settings\honey\My Documents\rtmpdump-2.1a-windows>cd rtmpdump-2
.1b-windows

C:\Documents and Settings\honey\My Documents\rtmpdump-2.1a-windows\rtmpdump-2.1b
-windows>rtmpdump.exe -r rtmpe://akafms-music02.myspacecdn.com/ondemand/168/std_
d4e3f788694c417fba3fb2fd1f7d2145.mp3 -o "my.flv"
RTMPDump v2.1
(c) 2009 Andrej Stepanchuk, Howard Chu, The Flvstreamer Team; license: GPL
Connecting ...
Starting download at: 0.000 kB
1240.175 kB / 104.36 sec
```

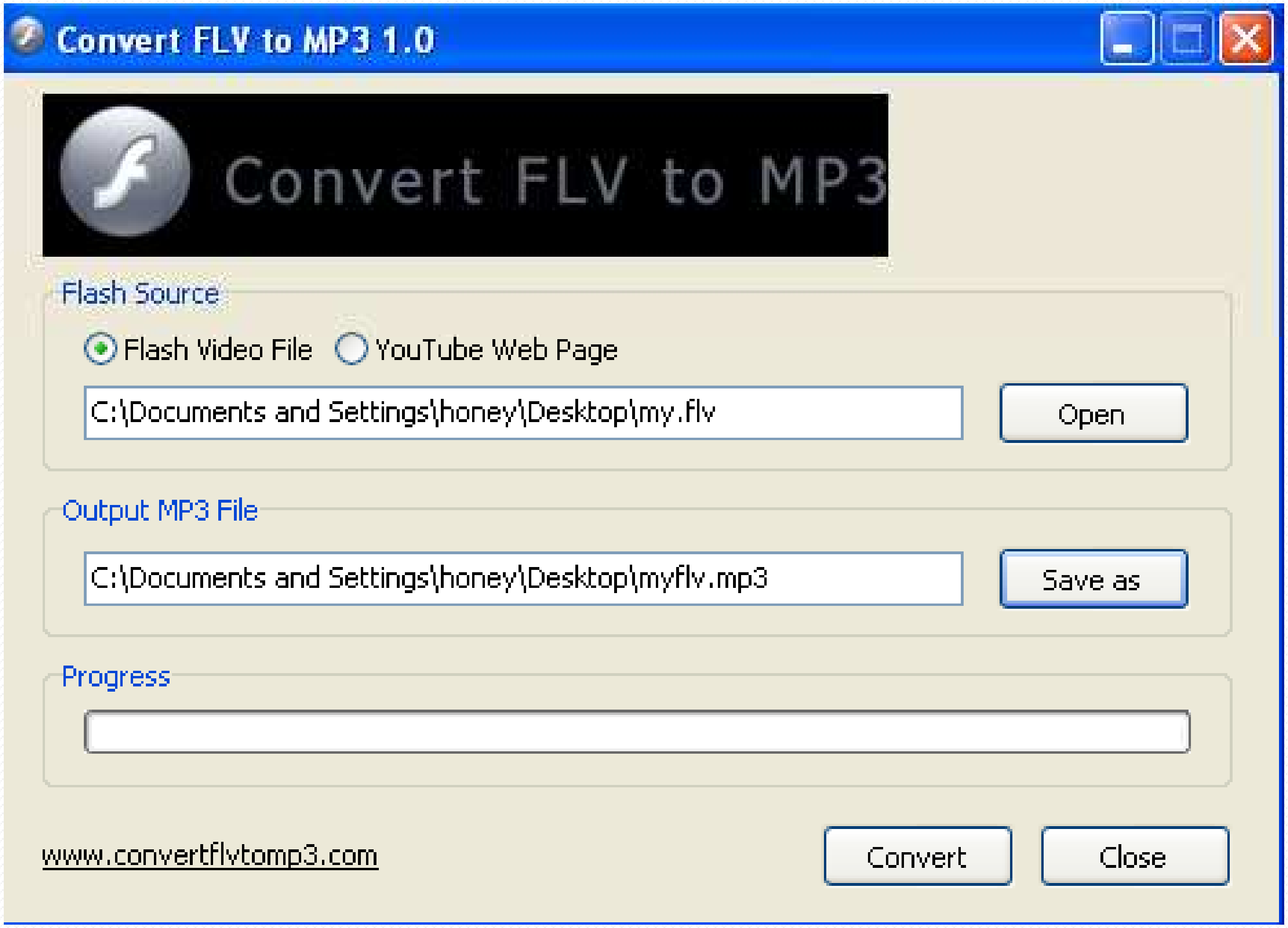
Next, watch your download complete! YaY!



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\honey>cd "My Documents"

C:\Documents and Settings\honey\My Documents>cd rtmpdump-2.1a-windows

C:\Documents and Settings\honey\My Documents\rtmpdump-2.1a-windows>cd rtmpdump-2
.1b-windows

C:\Documents and Settings\honey\My Documents\rtmpdump-2.1a-windows\rtmpdump-2.1b
-windows>rtmpdump.exe -r rtmpe://akafms-music02.myspacecdn.com/ondemand/168/std_
d4e3f788694c417fba3fb2fd1f7d2145.mp3 -o "my.flv"
RTMPDump v2.1
(c) 2009 Andrej Stepanchuk, Howard Chu, The Flvstreamer Team; license: GPL
Connecting ...
Starting download at: 0.000 kB
2813.331 kB / 236.90 sec
Download complete

C:\Documents and Settings\honey\My Documents\rtmpdump-2.1a-windows\rtmpdump-2.1b
-windows>_
```

- Step Six: Convert the “flv” file into an “mp3”.

if you download the file as an mp3 and not as a flv file and do not convert it – it has very poor quality. Convert FLV to MP3 resolves this.



Convert FLV to MP3 1.0

Flash Source

● Flash Video File ○ YouTube Web Page

C:\Documents and Settings\honey\Desktop\my.flv

Output MP3 File

C:\Documents and Settings\honey\Desktop\myflv.mp3

Step Seven:

- Listen and enjoy your mp3!

- Can we see those steps again? How about a quick video? YES.

INTERMISSION

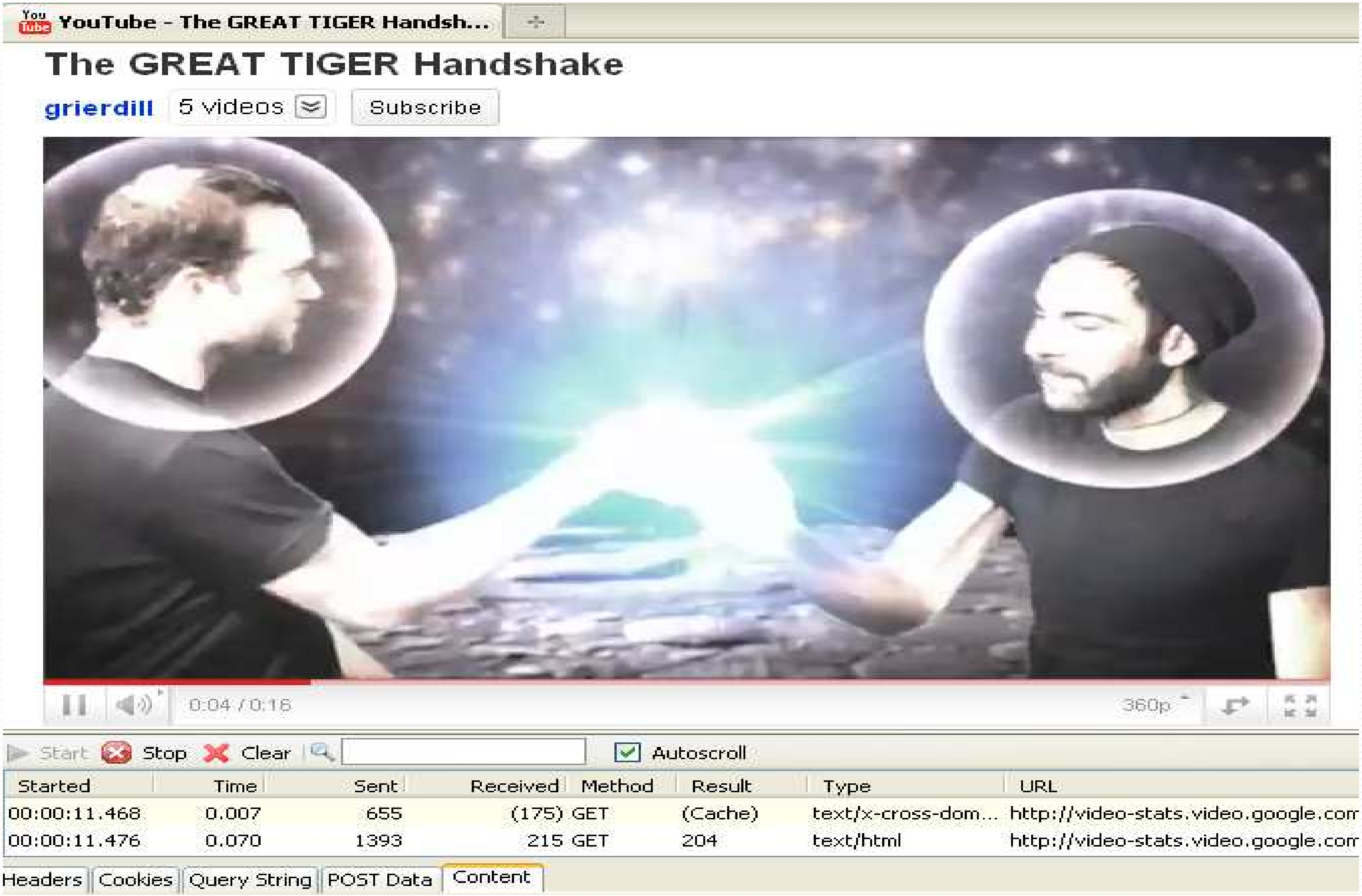
Let’s Party Hop Onto the Next One:

- HowTO: Get mp3 files from YouTube

- Step One: Install your HttpFox Firefox Plugin.

- Step Two: **Start** HttpFox and go to the target YouTube video.

For my example, I will be downloading an MP3 from my favorite Brooklyn-based band called: “Great Tiger”, because I got their permission.



YouTube - The GREAT TIGER Handsh...

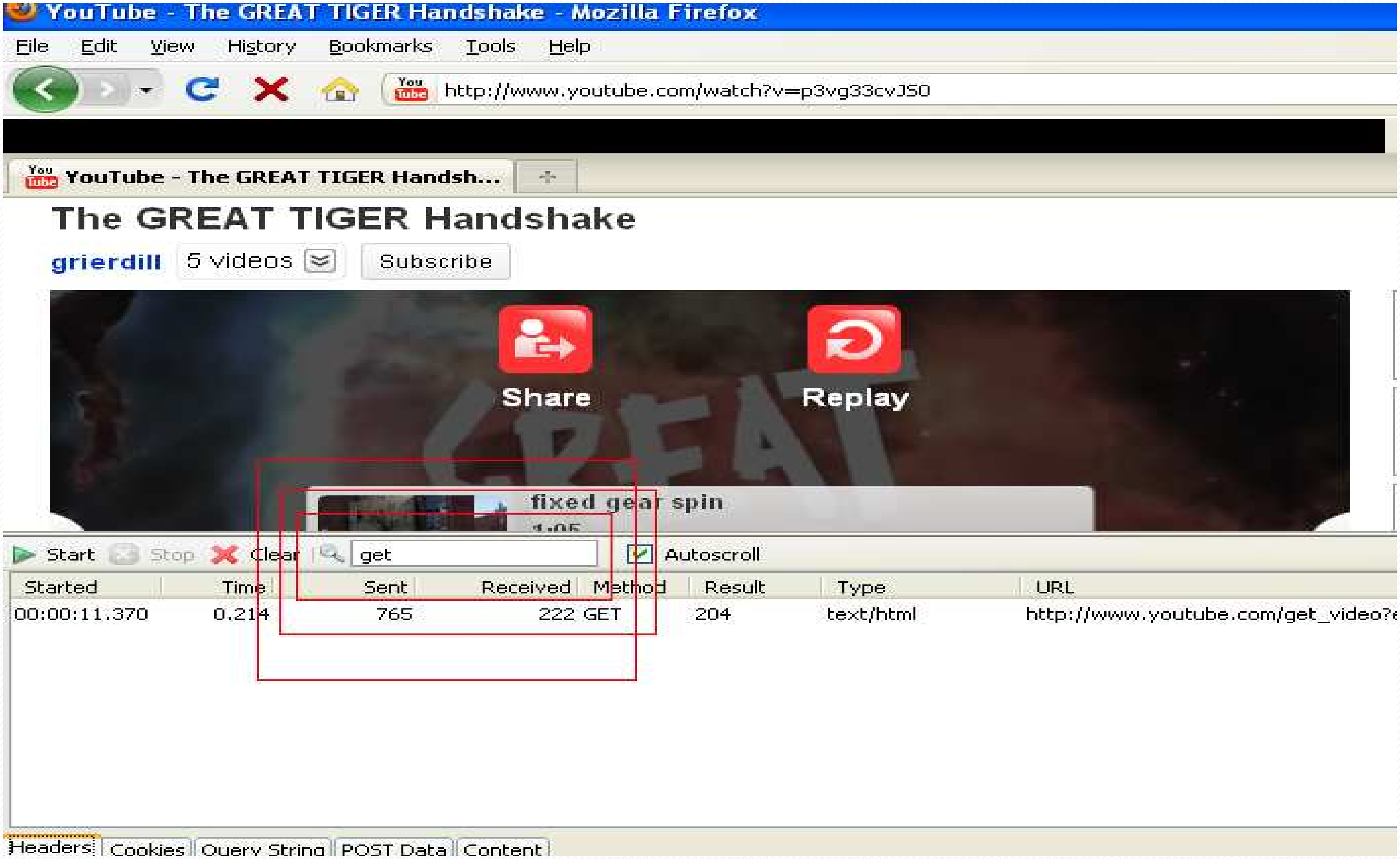
The GREAT TIGER Handshake

grierdill

Started	Time	Sent	Received	Method	Result	Type	URL
00:00:11.468	0.007	655	(175)	GET	(Cache)	text/x-cross-dom...	http://video-stats.video.google.com
00:00:11.476	0.070	1393	215	GET	204	text/html	http://video-stats.video.google.com

Step Three: Sift through the captured traffic.

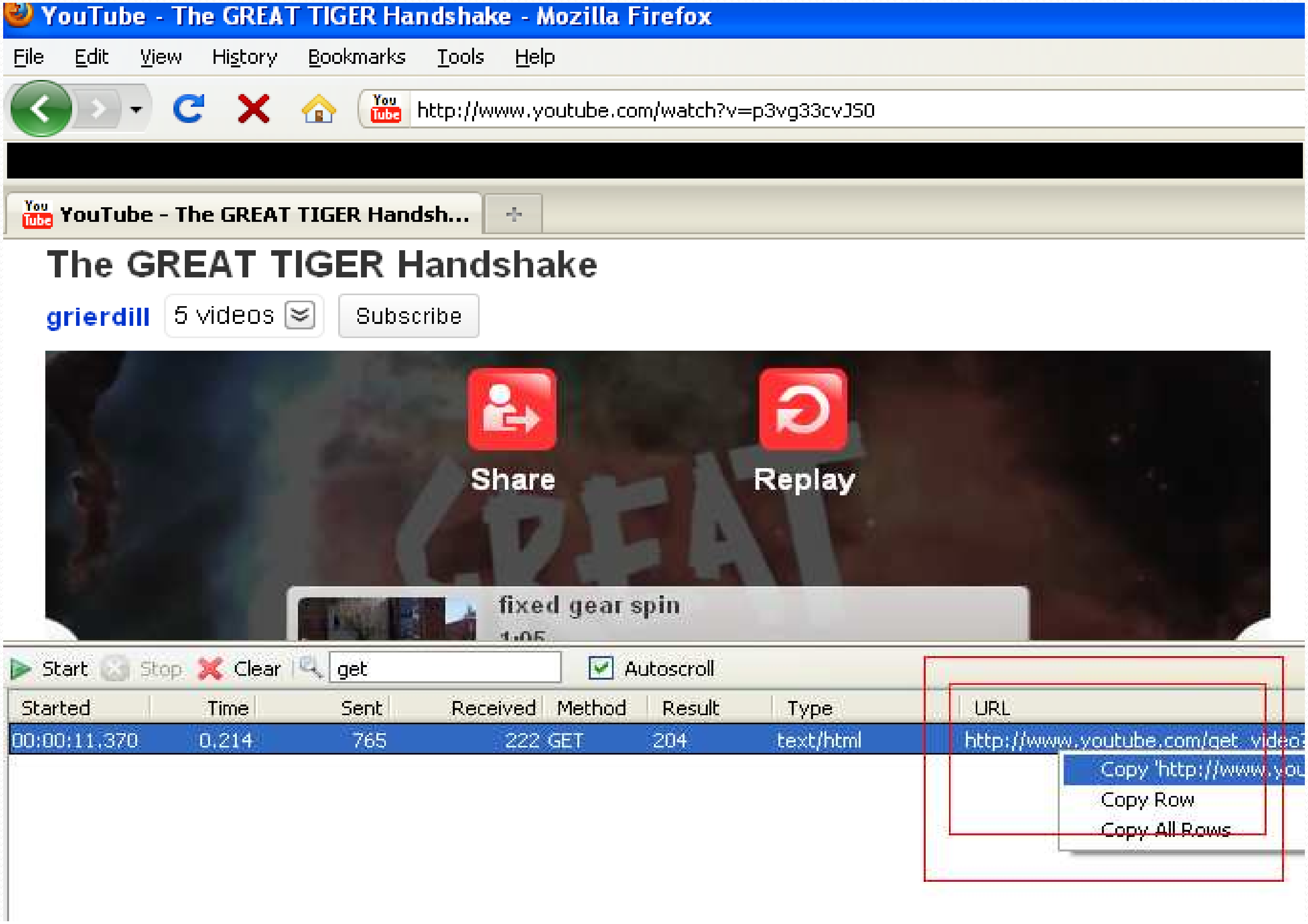
Do a search for "get".


YouTube - The GREAT TIGER Handshake - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
http://www.youtube.com/watch?v=p3vg33cvJS0
YouTube - The GREAT TIGER Handsh...
The GREAT TIGER Handshake
grierdill
5 videos
Subscribe
Share
Replay
fixed gear spin
Start
Stop
Clear
Autoscroll
Headers
Cookies
Query String
POST Data
Content

get

Started	Time	Sent	Received	Method	Result	Type	URL
00:00:11.370	0.214	765	222	GET	204	text/html	http://www.youtube.com/get_video?e

Step Four: Copy the URL.



YouTube - The GREAT TIGER Handshake - Mozilla Firefox

http://www.youtube.com/watch?v=p3vg33cvJS0

Started	Time	Sent	Received	Method	Result	Type	URL
00:00:11.370	0.214	765	222	GET	204	text/html	http://www.youtube.com/get_video?

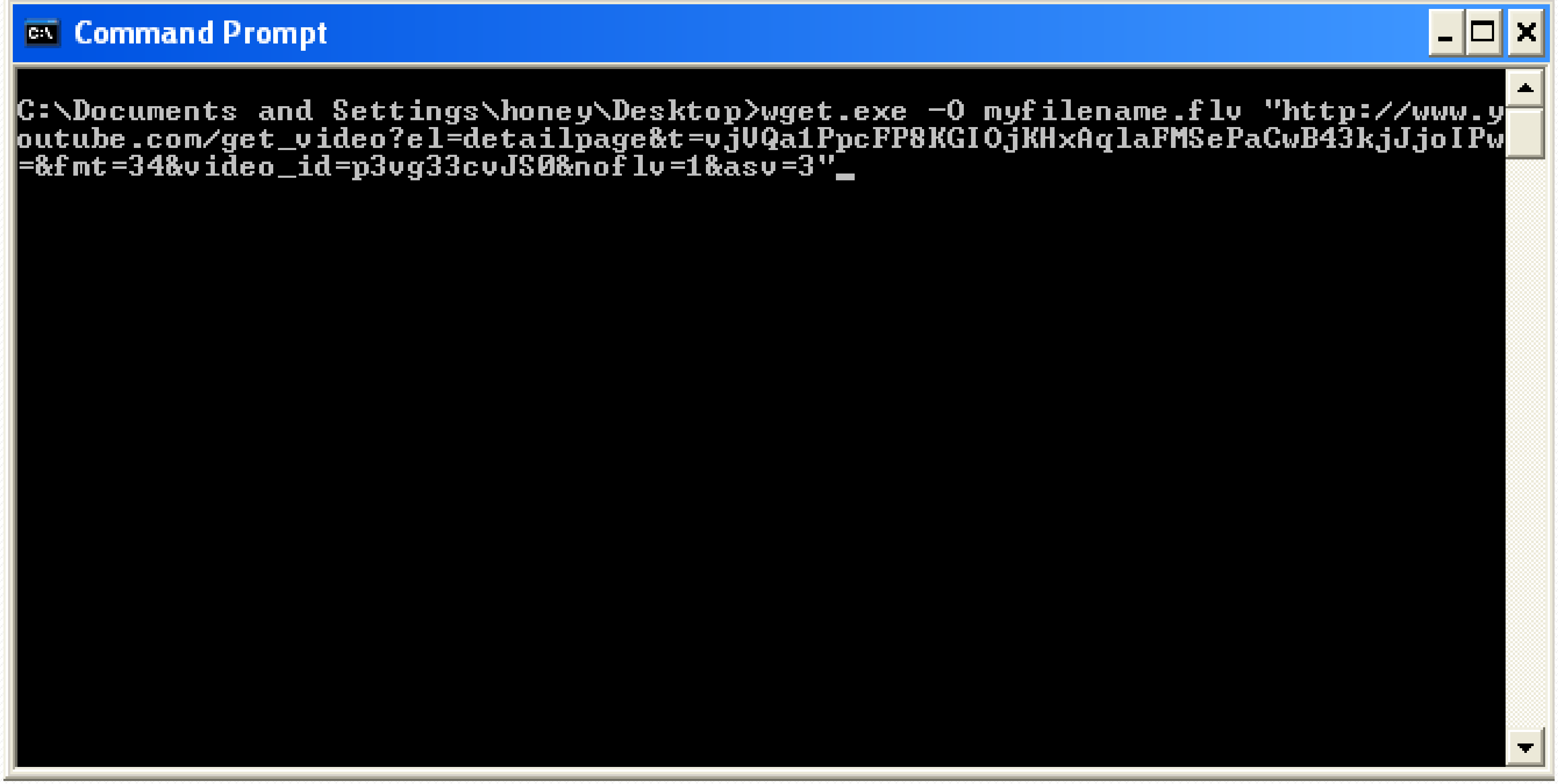
Step Five: Download wget. Modify the URL.
You do not need all of these parameters in the URL.
In fact, if you do not remove the unneeded parameters, the conversion may fail.

- So we want to execute the following command in wget:

```
wget.exe –O [myfilename.flv] “[captured URL]”
```

But we need to modify the URL to remove the extra parameters so our mp3 can be converted properly.

Here is the unedited URL we copied from HttpFox. We can notice several parameters within the URL.



```
C:\Documents and Settings\honey\Desktop>wget.exe -O myfilename.flv "http://www.y
outube.com/get_video?el=detailpage&t=vjVQa1PpcFP8KGIOjKHxAqlaFMSePaCwB43kjJjoIPw
=&fmt=34&video_id=p3vg33cvJS0&noflv=1&asv=3"_
```

Here is my example URL:

- http://www.youtube.com/get_video?el=detailpage&t=vjVQa1PpcFP8KGIOjKHxAqlaFMSePaCwB43kjJjoIPw=&fmt=34&video_id=p3vg33cvJSo&noflv=1&asv=3

- The parameters are:
- 1) get_video?
- 2) el=detailpage
- 3) t=some string of characters
- 4) fmt=34
- 5) video_id=somestring of characters
- 6) noflv=1
- 7) asv=3

******* These parameters are embedded in the URL out of order!!!!! (with exception to the get_video? parameter) *******

All of the parameters are separated by & symbols, except the very first parameter which comes directly after the get_video? parameter.

- The URL should be quotes when it is input into wget
- The URL does not need a trailing &

Ok, so the only parameters we need from the list of 7 are:

1) get_video?

2) t=some string of characters

3) video_id=somestring of characters

4) asv=3

It does not matter if parameters 2,3,4 are out of order. But they must:

- be separated by an &
- come before the “get_video?” parameter

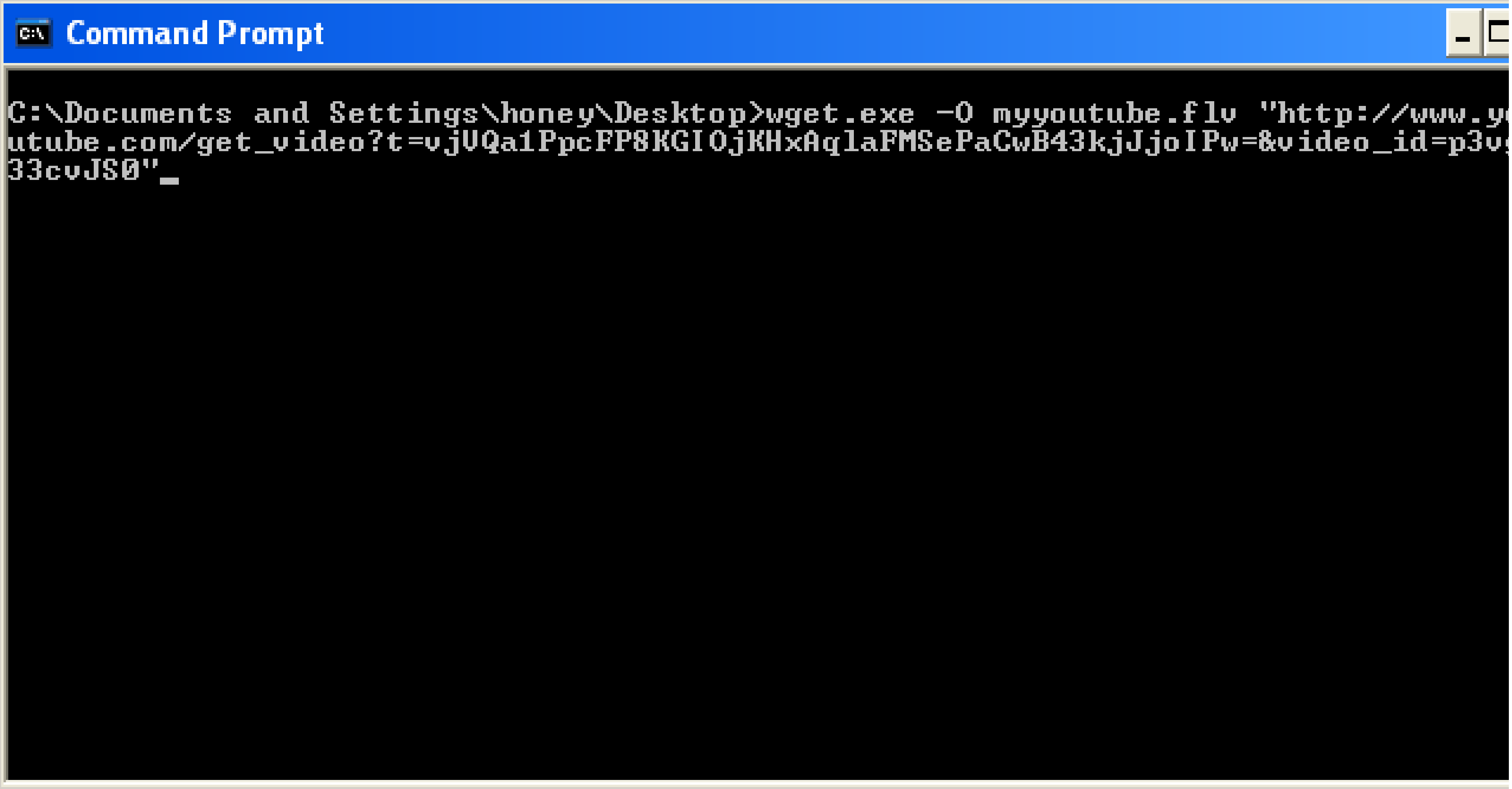
- Original URL:

  http://www.youtube.com/get_video?el=detailpage&t=vjVQa1PpcFP8KGIOjKHxAqlaFMSePaCwB43kjJjoIPw=&fmt=34&video_id=p3vg33cvJSo&noflv=1&asv=3

- Modified URL:

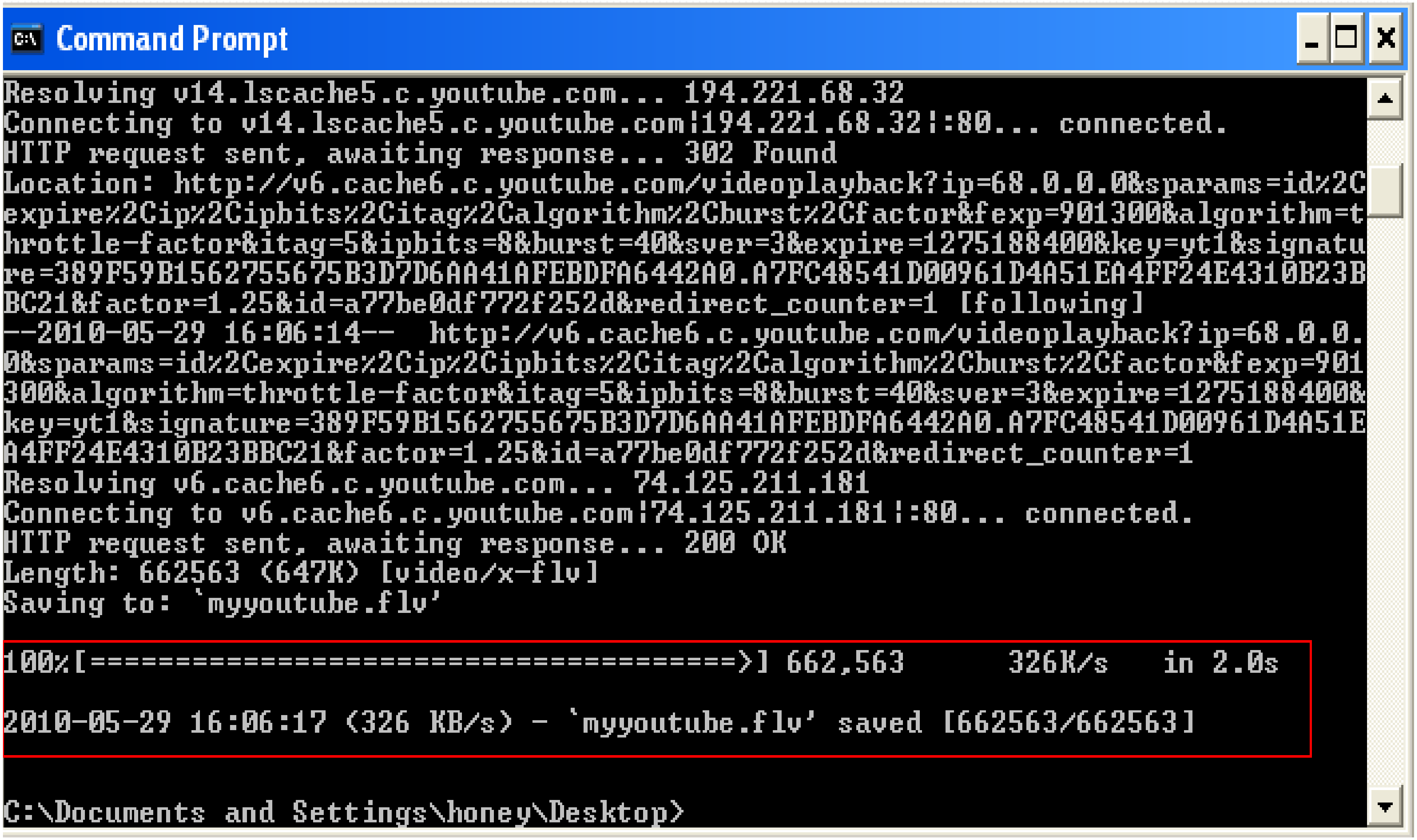
  http://www.youtube.com/get_video?t=vjVQa1PpcFP8KGIOjKHxAqlaFMSePaCwB43kjJjoIPw=&video_id=p3vg33cvJSo&asv=3

Enter in wget.exe –O [filename.flv] "[modified URL]"



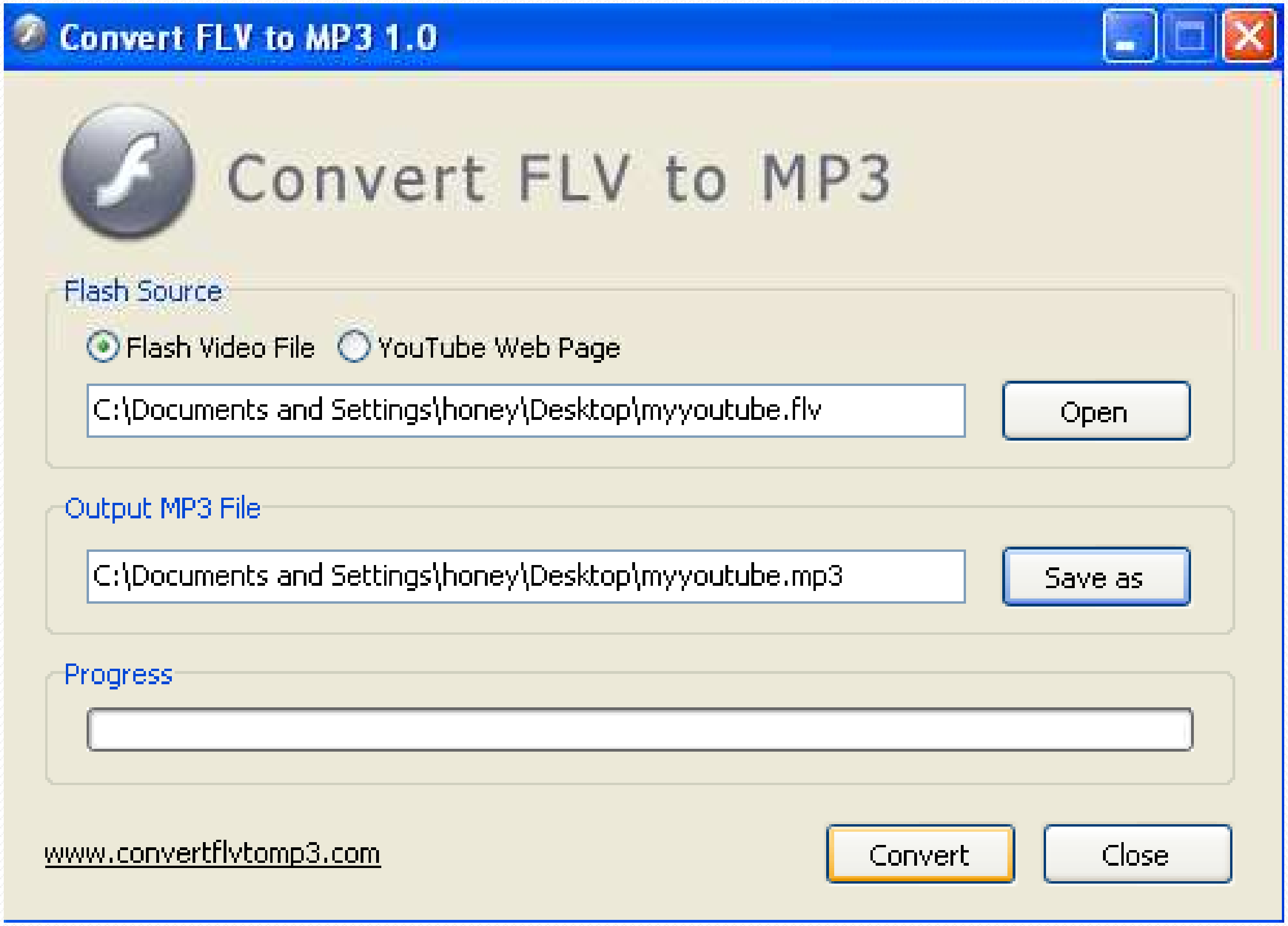
```
C:\Documents and Settings\honey\Desktop>wget.exe -O myyoutube.flv "http://www.y
utube.com/get_video?t=vjVQa1PpcFP8KGIOjKHxAqlaFMSePaCwB43kjJjoIPw=&video_id=p3v
33cvJS0"_
```

Next, watch your download complete! YaY!



```
Resolving v14.lscache5.c.youtube.com... 194.221.68.32
Connecting to v14.lscache5.c.youtube.com|194.221.68.32|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: http://v6.cache6.c.youtube.com/videoplayback?ip=68.0.0.0&sparams=id%2C
expire%2Cip%2Cipbits%2Citag%2Calgorithm%2Cburst%2Cfactor&fexp=901300&algorithm=t
hrottle-factor&itag=5&ipbits=8&burst=40&sver=3&expire=1275188400&key=yt1&signatu
re=389F59B1562755675B3D7D6AA41AFEBDFA6442A0.A7FC48541D00961D4A51EA4FF24E4310B23B
BC21&factor=1.25&id=a77be0df772f252d&redirect_counter=1 [following]
--2010-05-29 16:06:14--  http://v6.cache6.c.youtube.com/videoplayback?ip=68.0.0.
0&sparams=id%2Cexpire%2Cip%2Cipbits%2Citag%2Calgorithm%2Cburst%2Cfactor&fexp=901
300&algorithm=throttle-factor&itag=5&ipbits=8&burst=40&sver=3&expire=1275188400&
key=yt1&signature=389F59B1562755675B3D7D6AA41AFEBDFA6442A0.A7FC48541D00961D4A51E
A4FF24E4310B23BBC21&factor=1.25&id=a77be0df772f252d&redirect_counter=1
Resolving v6.cache6.c.youtube.com... 74.125.211.181
Connecting to v6.cache6.c.youtube.com|74.125.211.181|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 662563 (647K) [video/x-flv]
Saving to: `myyoutube.flv'

100%[======================================>] 662,563      326K/s   in 2.0s

2010-05-29 16:06:17 (326 KB/s) - `myyoutube.flv' saved [662563/662563]


C:\Documents and Settings\honey\Desktop>
```

Step Six: Convert your “.flv” file into an “mp3” file.



Convert FLV to MP3 1.0

Convert FLV to MP3

Flash Source

● Flash Video File ○ YouTube Web Page

C:\Documents and Settings\honey\Desktop\myyoutube.flv

Output MP3 File

C:\Documents and Settings\honey\Desktop\myyoutube.mp3

Progress

www.convertflvtomp3.com

Step Seven:

- Listen and enjoy your mp3!

- Can we see those steps again? How about in a quick video? YES.

INTERMISSION

Conclusion:

- DRM implementations will almost always fail without some type of special hardware on the client computer.

- Protected Streaming is supposed to protect digital content from unauthorized use, this is a DRM technology by Adobe.

- Encrypted content by the Flash Media Server "on the fly“ means there is no encryption of the source file. When data is ready for transmission, either RTMPE or RTMPS is used…

- RTMPE was designed to be simpler than RTMPS which requires an SSL certificate. But usability is being traded for security because…

- Although the CPU-load is less with RTMPE than RTMPS on the Flash Media Server, ***there isn't actually any security***.
- In January 2009, Adobe attempted to fix the security, but there are still security holes in the design of the RTMPE algorithm itself.!!!
- The RTMPE algorithm relies on security through obscurity!!!
- RTMPE is vulnerable to Man in the Middle attacks.
- Rtmpdump can extract RTMPE streams and Adobe has issued DMCA takedowns of the tool.

Maybe Adobe should fix its protocol instead of issuing DMCA takedowns of tools…

References and Downloads:

- [i] Download wget here: http://www.gnu.org/software/wget/
- [ii] Download Mozilla Firefox here: http://www.mozilla.com/en-US/
- [iii] Download the addon HttpFox here: https://addons.mozilla.org/en-US/firefox/addon/6647/
- [iv] Download rtmpdump here: http://rtmpdump.mplayerhq.hu/
- [v] ConvertFLVtoMP3 http://www.convertflvtomp3.com
- [vi] RTMP http://www.adobe.com/devnet/rtmp/
- [vii] RTMPE http://lkcl.net/rtmp/RTMPE.txt
- [viii] MySpace copyrighted logo is a trademark of MySpace, Inc.
- [ix] Great Tiger the band: http://wearegreattiger.com/ and http://www.myspace.com/wearegreattiger
- [x] YouTube copyrighted logo is a trademark of Google Inc.
- [xi] Adobe's website content: http://www.adobe.com/devnet/flashmediaserver/articles/overview_streaming_fms3_02.html