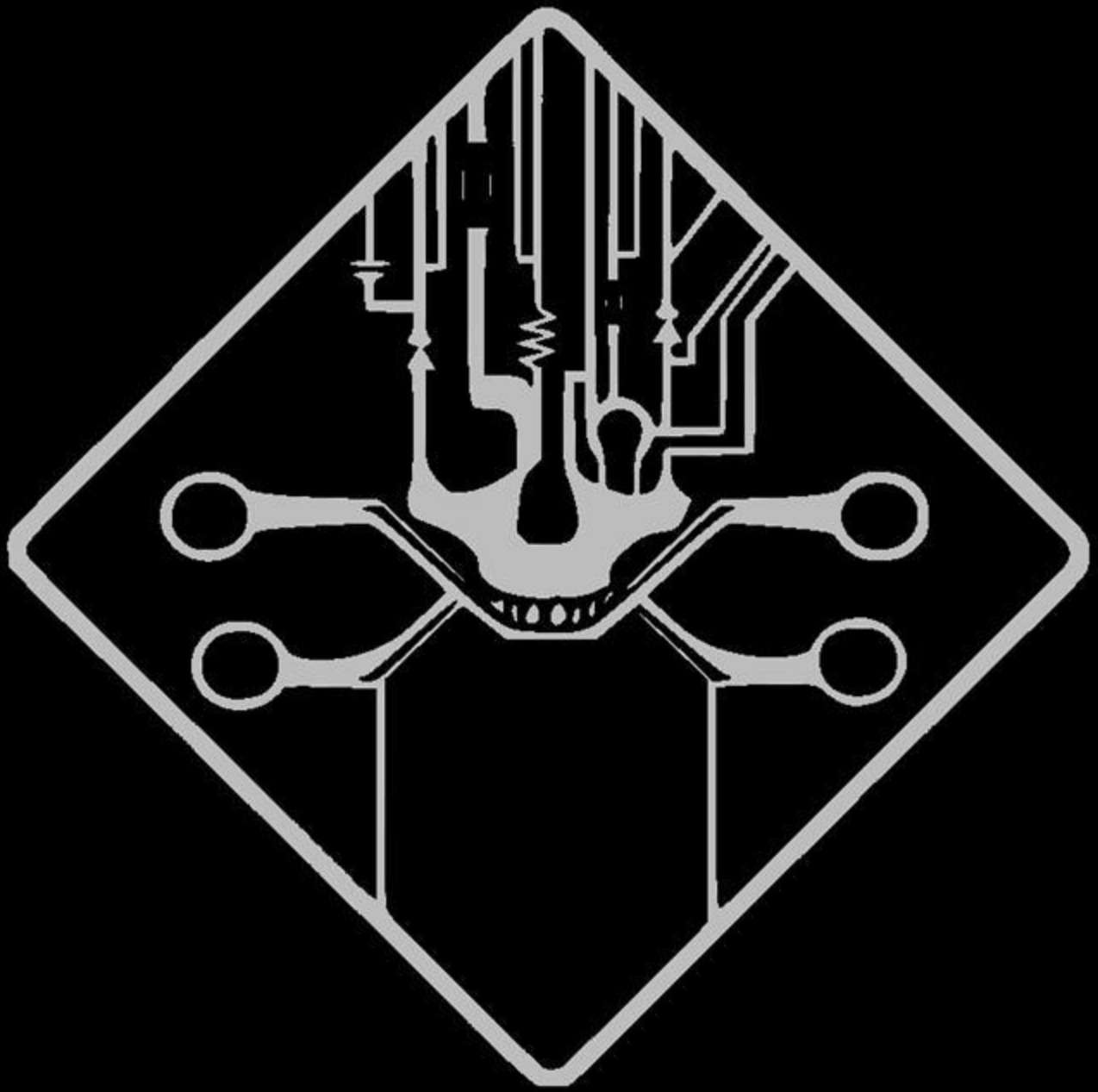

THE DORK
SIDE OF



mes3hacklab


THE DORK
SIDE OF

# THE DORK SIDE OF GOOGLE

**Principali funzioni di ricerca utilizzate:**

| | |
|---|---|
| Site | Specifica il sito da filtrare. |
| Inurl | Specifica cosa deve contenere l'URL. |
| Intext | Specifica le parole chiave nel body della pagina. |
| Intitle | Specifica le parole chiave da cercare nel titolo della pagina. |
| Filetype | Specifica il tipo di file (dal estensione). |

Simboli:

| | | |
|---|---|---|
| - | | Elimina un elemento dalla ricerca. |
| \| | OR | Effettua un'operazione OR sulla ricerca. |
| "" | | Specifica una parola da cercare nel body. |
| . | | Sostituisce un qualsiasi valore tra due parole. |

# THE DORK SIDE OF GOOGLE

## Le shell

# THE DORK SIDE OF GOOGLE

## C99Shell v. 1.0 pre-release build #9

Software: Apache/2.2.15 (CentOS). PHP/5.3.3
uname -a:

Safe-mode: OFF (not secure)
/var/www/clients/ drwxr-xr-x
Free 46.09 GB of 50 GB (92.18%)

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

Listing folder (0 files and 2 folders):

| Name ▲ | Size | Modify | Owner/Group | Perms | Action |
|---|---|---|---|---|---|
| .. | LINK | 05.06.2012 00:07:02 | 0/0 | drwxr-xr-x | |
| . | LINK | 03.06.2012 23:24:01 | 0/0 | drwxr-xr-x | |
| [client1] | DIR | 20.05.2012 08:05:01 | 0/0 | drwxr-xr-x | |
| [client2] | DIR | 03.06.2012 23:24:02 | 0/0 | drwxr-xr-x | |

Select all Unselect all With selected: Confir

:: Command execute ::

Enter: Execute

Select: ---------- Execute

:: Search ::
(.*) - regexp Search

:: Upload ::
Seleccionar archivo No se eli... archivo Upload
[ Read-Only ]

:: Make Dir ::
/var/www/clients/ Create
[ Read-Only ]

:: Make File ::
/var/www/clients/ Create
[ Read-Only ]

# THE DORK SIDE OF GOOGLE

## C99Shell v. 1.0 pre-release build #9

Software: Apache/2.2.15 (CentOS). PHP/5.3.3
uname -a:

Safe-mode: OFF (not secure)
/var/www/clients/ drwxr-xr-x
Free 46.09 GB of 50 GB (92.18%)

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

Listing folder (0 files and 2 folders):

| Name ▲ | Size | Modify | Owner/Group | Perms | Action |
|---|---|---|---|---|---|
| .. | LINK | 05.06.2012 00:07:02 | 0/0 | drwxr-xr-x | |
| . | LINK | 03.06.2012 23:24:01 | 0/0 | drwxr-xr-x | |
| [client1] | DIR | 20.05.2012 08:05:01 | 0/0 | drwxr-xr-x | |
| [client2] | DIR | 03.06.2012 23:24:02 | 0/0 | drwxr-xr-x | |

Select all Unselect all With selected: Confir

:: Command execute ::

Enter: Execute

Select: Execute

:: Search ::
(.*) - regexp Search

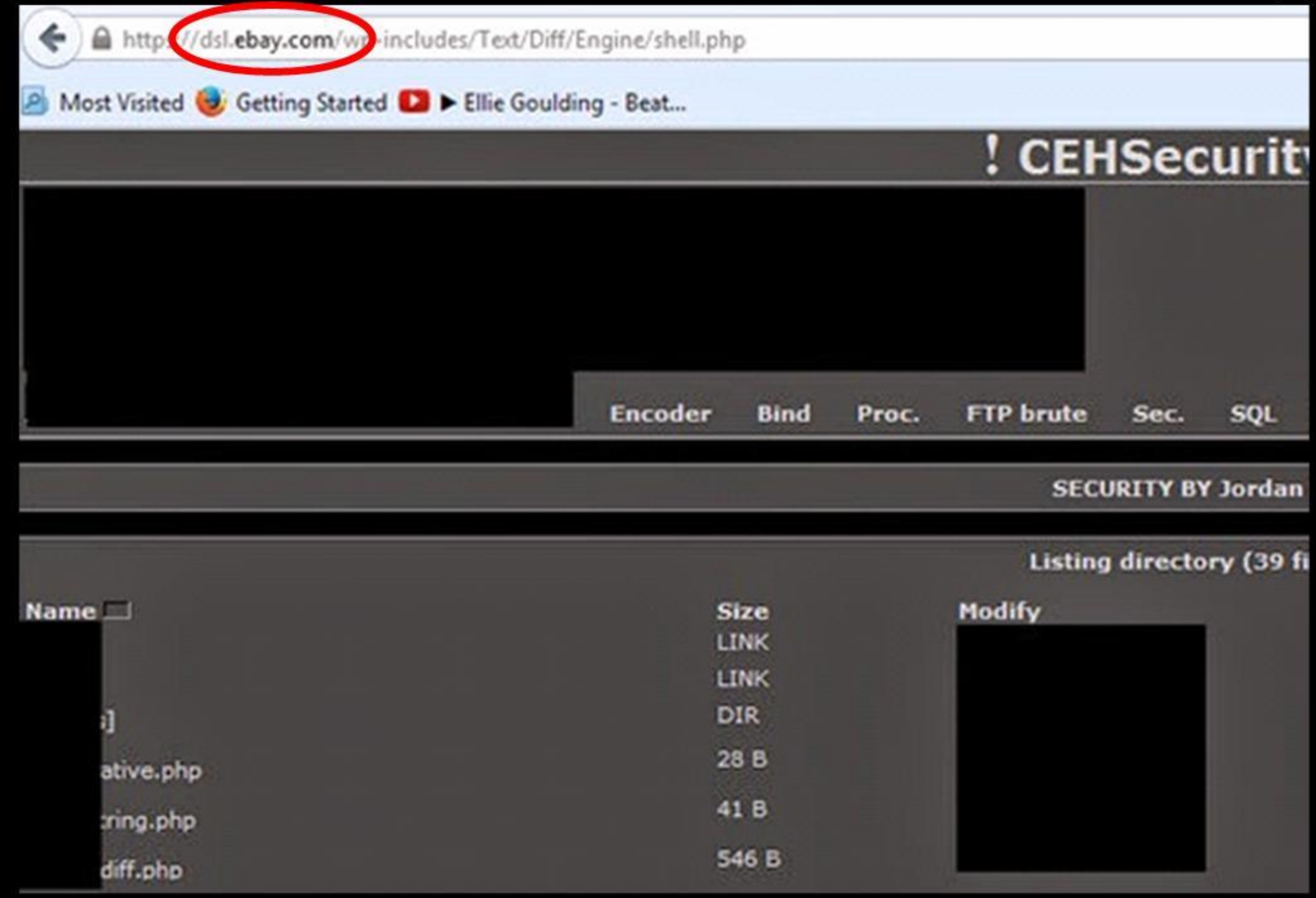
:: Upload ::

:: Make Dir ::
/var/www/clients/ Create
[ Read-Only ]

## Cosa fanno le shell?

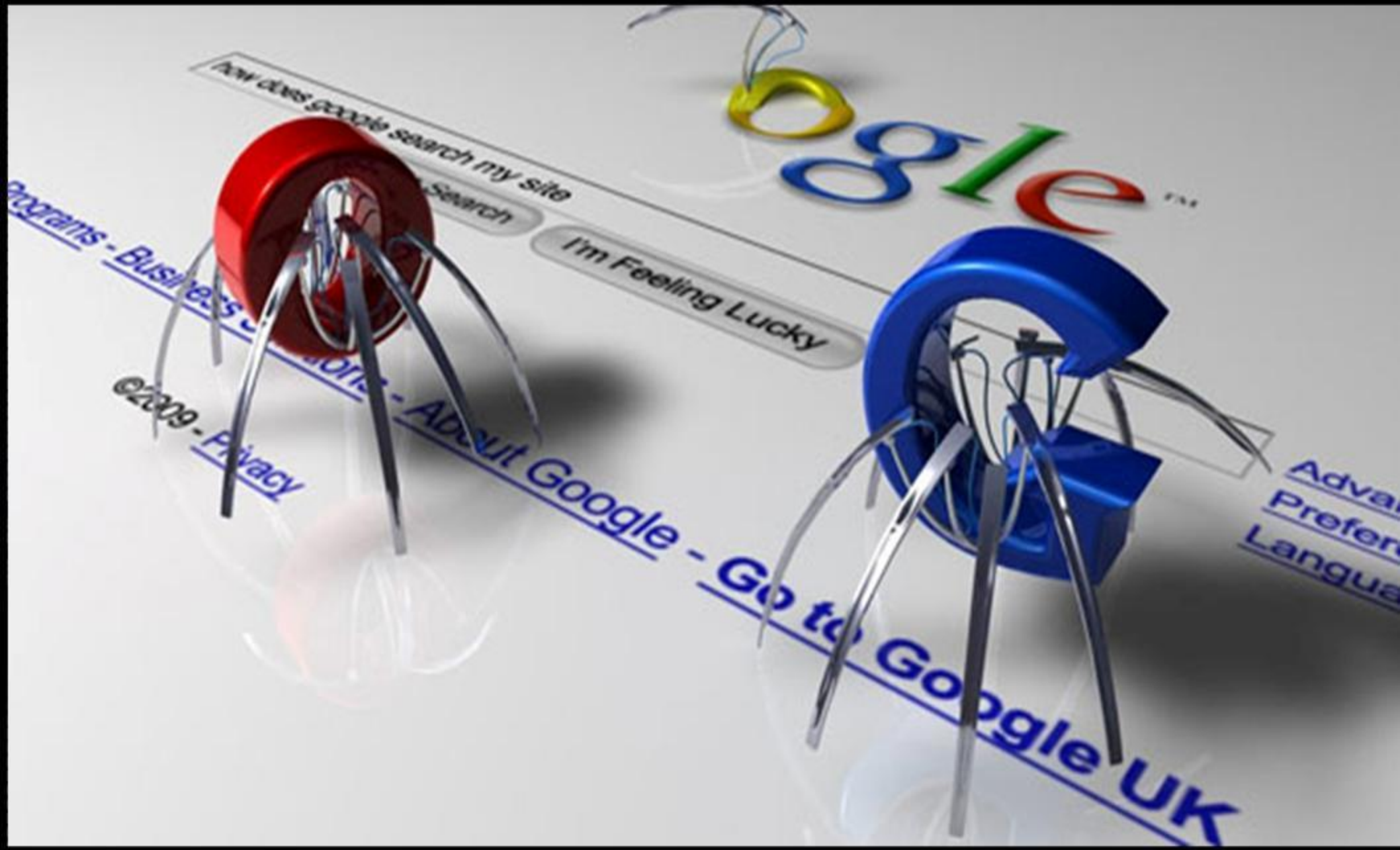
- Accedere ad informazioni riservate.
- Caricare / Scaricare / Modificare file
- Tools DdoS, Mail, Proxy, ...
- Eseguire comandi sul server.

# THE DORK SIDE OF GOOGLE



# THE DORK SIDE OF GOOGLE

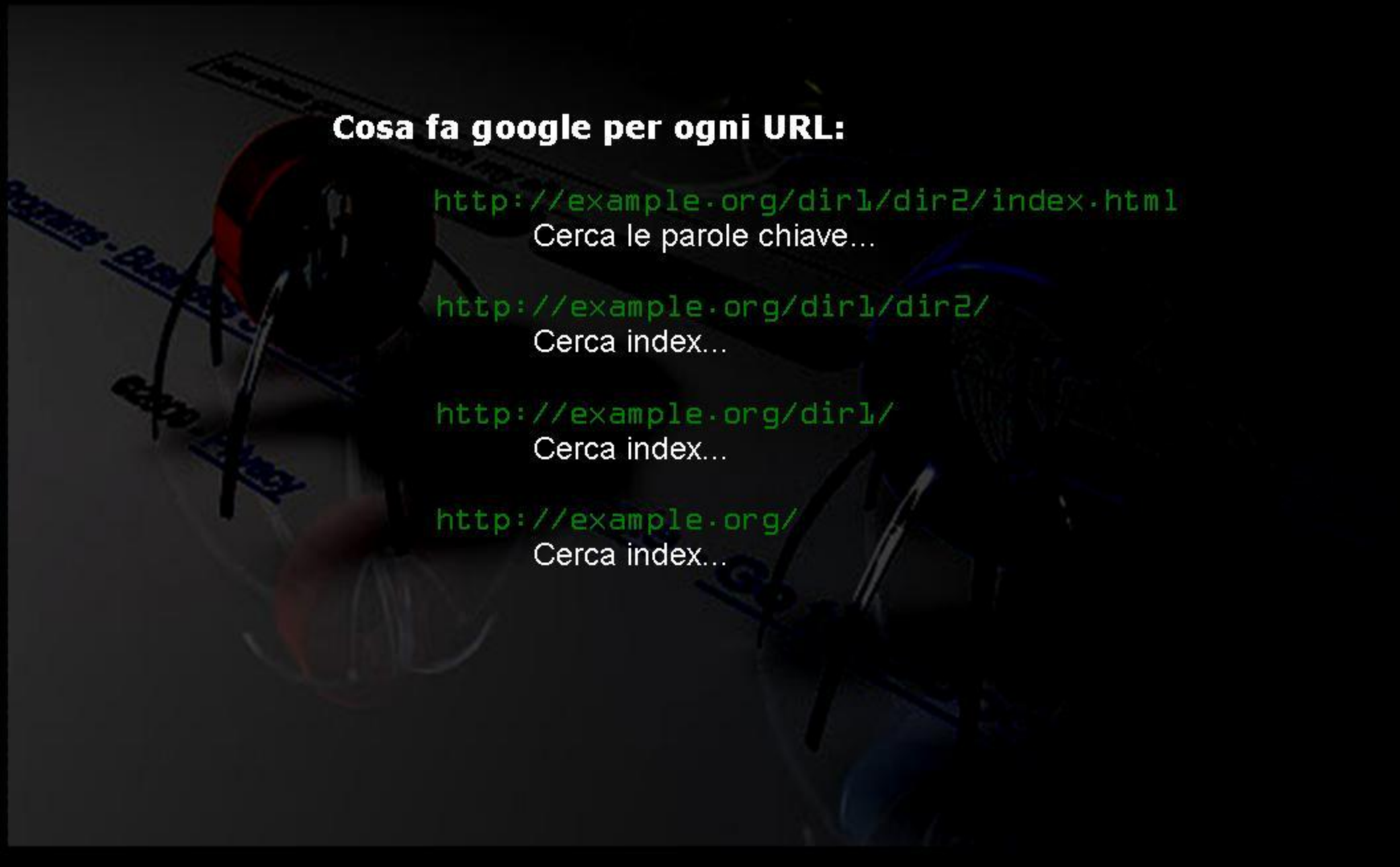
## Come funziona il crawler di Google?



# THE DORK SIDE OF GOOGLE

Seguiamolo ...

# THE DORK SIDE OF GOOGLE



**Cosa fa google per ogni URL:**

`http://example.org/dir1/dir2/index.html`
Cerca le parole chiave...

`http://example.org/dir1/dir2/`
Cerca index...

`http://example.org/dir1/`
Cerca index...

`http://example.org/`
Cerca index...

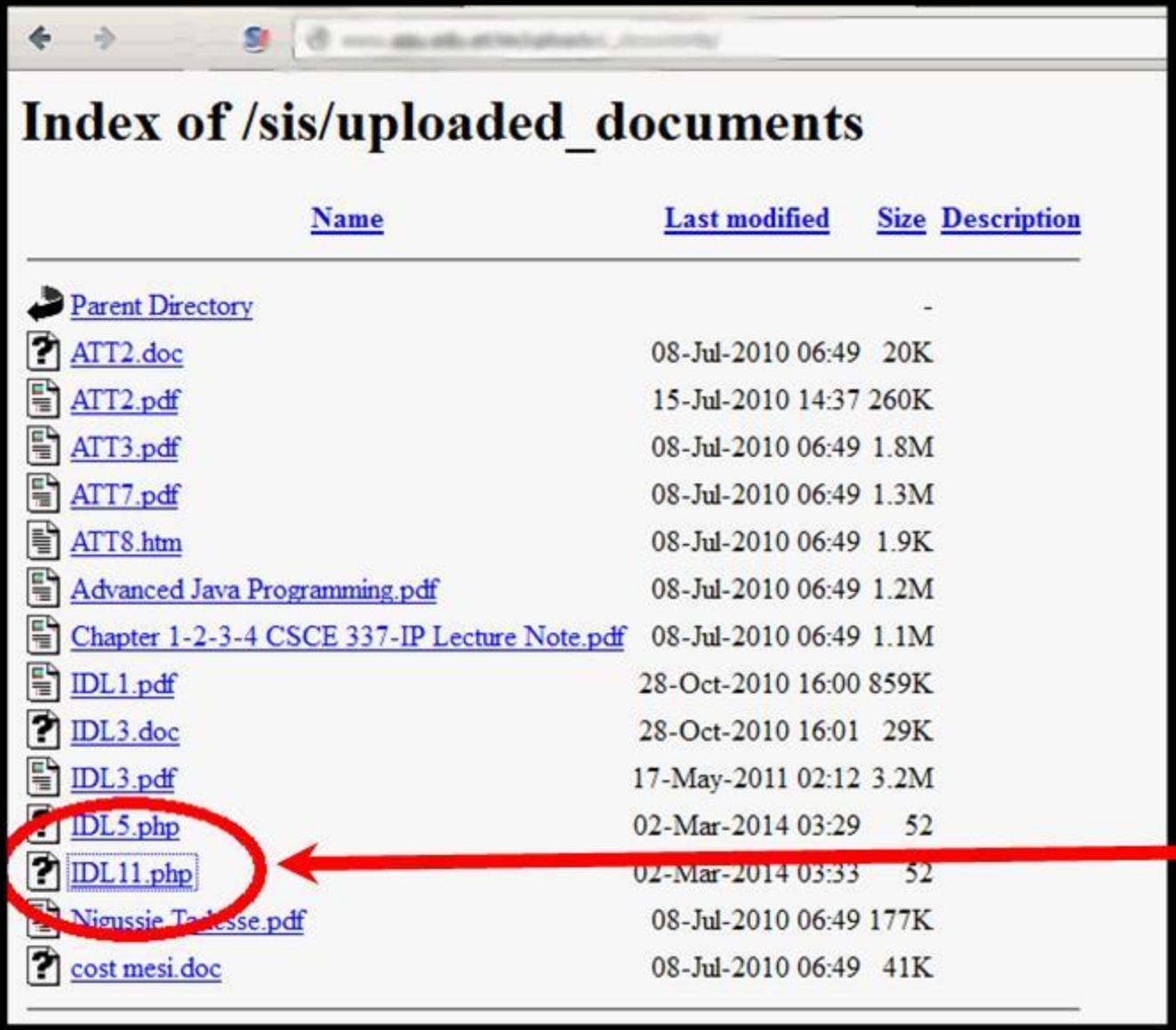
# THE DORK SIDE OF GOOGLE


## Index of /nginx/apk/

| | | |
|---|---|---|
| ../ | | |
| root/ | 28-Mar-2011 04:32 | - |
| ADW_Honeycomb_Theme_(1.0).apk | 07-Mar-2011 08:24 | 1005429 |
| App_Drawer_Icon_Pack_(1.2.3).apk | 07-Mar-2011 08:26 | 547460 |
| Contact2SimPro_v1.6.apk | 09-Mar-2011 02:31 | 23873 |
| Contact2Sim_1.17.apk | 09-Mar-2011 02:32 | 123269 |
| SMS_Unread_Count_(1.5.7).apk | 07-Mar-2011 09:07 | 187762 |
| ZDbox.1.4.77.Android.apk | 06-Apr-2011 05:29 | 1576205 |
| apk | 07-Apr-2011 03:09 | 26 |
| athan.apk | 09-Mar-2011 02:43 | 4695080 |
| com.funfoneapps.speedboostota.apk | 10-Mar-2011 03:03 | 376202 |
| com.stylem.wallpapersota.apk | 10-Mar-2011 03:04 | 122466 |
| iptables | 24-Mar-2011 02:17 | 109020 |
| lv.n3o.swapper_0.2.7.apk | 07-Apr-2011 03:08 | 84365 |
| organizer-widget.apk | 09-Mar-2011 06:14 | 152944 |
| root.rar | 28-Mar-2011 04:32 | 581923 |
| signed-dream_devphone_userdebug-img-14721.zip | 04-Apr-2011 03:54 | 40118457 |
| silverexplorer.apk | 09-Mar-2011 02:39 | 326796 |
| smsbackup.apk | 09-Mar-2011 02:36 | 145363 |
| space_ota.apk | 10-Mar-2011 03:08 | 2915939 |
| speak_text__ota.apk | 10-Mar-2011 03:05 | 135738 |
| streetracing5pp__ota.apk | 10-Mar-2011 03:01 | 3102867 |
| su | 01-Aug-2009 02:08 | 76232 |
| su.zip | 28-Mar-2011 04:22 | 48224 |
| ymst.android.fxcameraota.apk | 10-Mar-2011 03:06 | 1451385 |
| z4root.1.3.0.apk | 18-Mar-2011 02:28 | 978414 |
| zdbox_1.3.71_2020000007_xda-developers.apk | 05-Apr-2011 04:16 | 1989013 |

Autoindex

# THE DORK SIDE OF GOOGLE



## Index of /sis/uploaded_documents

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| ATT2.doc | 08-Jul-2010 06:49 | 20K | |
| ATT2.pdf | 15-Jul-2010 14:37 | 260K | |
| ATT3.pdf | 08-Jul-2010 06:49 | 1.8M | |
| ATT7.pdf | 08-Jul-2010 06:49 | 1.3M | |
| ATT8.htm | 08-Jul-2010 06:49 | 1.9K | |
| Advanced Java Programming.pdf | 08-Jul-2010 06:49 | 1.2M | |
| Chapter 1-2-3-4 CSCE 337-IP Lecture Note.pdf | 08-Jul-2010 06:49 | 1.1M | |
| IDL1.pdf | 28-Oct-2010 16:00 | 859K | |
| IDL3.doc | 28-Oct-2010 16:01 | 29K | |
| IDL3.pdf | 17-May-2011 02:12 | 3.2M | |
| IDL5.php | 02-Mar-2014 03:29 | 52 | |
| IDL11.php | 02-Mar-2014 03:33 | 52 | |
| Nigussie Tadesse.pdf | 08-Jul-2010 06:49 | 177K | |
| cost mesi.doc | 08-Jul-2010 06:49 | 41K | |

SHELL


THE DORK
SIDE OF
COME TROVARE LE SHELL

# THE DORK SIDE OF GOOGLE


Microsoft-IIS/6.0. PHP/4.4.7

Kernel: Windows NT HOSTER8-3 5.2 build 3790 (Microsoft Windows [Version 5.2.3790])

Running As: IUSR_iscgov

Free 100.27 GB of 441.4 GB (22.72%)

Safe-Mode: OFF (not secure)

Disabled PHP Functions: NONE

cURL: ON

Server IP: [redacted] · Your IP: [redacted]

f:\inetpub\vhosts\[redacted]\httpdocs\ drwxrwxrwx

Detected drives: [A:] [C:] [D:] [F:]

[Home] [Back] [Forward] [Up] [Refresh] [Search] [Buffer]

[String/Hash Tools] [Processes] [Users] [System Information] [SQL Manager] [Reverse IP] [Kernel Exploit Search] [Execute PHP Code] [PHP Info]

[PHP Tools] [Bind Shell Backdoor] [Back-Connection] [Mass Code Injection] [Exploits] [cPanel Finder] [RFI/LFI Finder] [Install IP:Port Proxy] [Install PHP Proxy] [Suicide Script]

Listing folder (61 files and 9 folders):

| Name [asc] | Size | Modify | Perms | Action |
|---|---|---|---|---|
| . | LINK | 13.03.2014 09:34:43 | drwxrwxrwx | [info] |
| .. | LINK | 01.01.1970 02:00:00 | ?--------- | [info] [change] [download] |
| [App_Data] | DIR | 05.07.2013 01:01:11 | drwxrwxrwx | [info] |
| [_notes] | DIR | 26.02.2012 14:47:46 | drwxrwxrwx | [info] |
| [aspnet_client] | DIR | 26.02.2012 14:47:38 | drwxrwxrwx | [info] |
| [index2007] | DIR | 26.02.2012 14:47:40 | drwxrwxrwx | [info] |
| [index2008] | DIR | 26.02.2012 14:47:41 | drwxrwxrwx | [info] |
| [index2009] | DIR | 26.02.2012 14:47:42 | drwxrwxrwx | [info] |
| [picture_library] | DIR | 26.02.2012 14:43:10 | drwxrwxrwx | [info] |
| [previouses209] | DIR | 26.02.2012 14:47:46 | drwxrwxrwx | [info] |

# THE DORK SIDE OF GOOGLE


Microsoft-IIS/6.0. PHP/4.4.7

Kernel: Windows NT HOSTER8-3 5.2 build 3790 (Microsoft Windows [Version 5.2.3790])

Safe-Mode: OFF (not secure)

Disabled PHP Functions: NONE

cURL: ON

Running As: IUSR_iscgov

Free 100.27 GB of 441.4 GB (22.72%)

Server IP: [redacted] - Your IP: [redacted]

f:\inetpub\vhosts\[redacted]\httpdocs\ drwxrwxrwx

Detected drives: [A:] [C:] [D:] [F:]

[Home] [Back] [Forward] [Up] [Refresh] [Search] [Buffer]

[String/Hash Tools] [Processes] [Users] [System Information] [SQL Manager] [Reverse IP] [Kernel Exploit Search] [Execute PHP Code] [PHP Info]

[PHP Tools] [Bind Shell Backdoor] [Back-Connection] [Mass Code Injection] [Exploits] [cPanel Finder] [RFI/LFI Finder] [Install IP:Port Proxy] [Install PHP Proxy] [Suicide Script]

Listing folder (61 files and 9 folders):

| Name [asc] | Size | Modify | Perms | Action |
|---|---|---|---|---|
| . | LINK | 13.03.2014 09:34:43 | drwxrwxrwx | [info] |
| .. | LINK | 01.01.1970 02:00:00 | ?--------- | [info] [change] [download] |
| [App_Data] | DIR | 05.07.2013 01:01:11 | drwxrwxrwx | [info] |
| [_notes] | DIR | 26.02.2012 14:47:46 | drwxrwxrwx | [info] |
| [aspnet_client] | DIR | 26.02.2012 14:47:38 | drwxrwxrwx | [info] |
| [index2007] | DIR | 26.02.2012 14:47:40 | drwxrwxrwx | [info] |
| [index2008] | DIR | 26.02.2012 14:47:41 | drwxrwxrwx | [info] |
| [index2009] | DIR | 26.02.2012 14:47:42 | drwxrwxrwx | [info] |
| [picture_library] | DIR | 26.02.2012 14:43:10 | drwxrwxrwx | [info] |
| [previouses209] | DIR | 26.02.2012 14:47:46 | drwxrwxrwx | [info] |

# THE DORK SIDE OF GOOGLE

| | | | | |
|---|---|---|---|---|
| permit for foreign insurance company 2008.doc | 53.5 KB | 26.02.2012 14:47:38 | -rw-rw-rw- | [info] [change] [download] |
| regulation 9812.doc | 324 KB | 26.02.2012 14:47:38 | -rw-rw-rw- | [info] [change] [download] |

Select all | Unselect all | With selected: | Confirm

**Enter:**

Execute

Kernel Info:

Windows NT HOSTER8-3 5.2 build 3790

Google!

Functions

Wipe Logs Using zap2 (*nix)

Execute

Make Dir

f:\inetpub\vhosts\ \httpdocs\

Create

[ ok ]

Go Dir

f:\inetpub\vhosts\ \httpdocs\

Go

Aliases

----------

Execute

Make File

f:\inetpub\vhosts\ \httpdocs\

Create

[ ok ]

Go File

f:\inetpub\vhosts\ \httpdocs\

Go

PHP Safe-Mode Bypass (Read File)

File: Read File

e.g.: /etc/passwd or C:\WINDOWS\system32\.SAM

PHP Safe-Mode Bypass (Directory Listing)

Dir: List Directory

e.g.: /etc/ or C:\

Search

(.*) - regexp Search

Upload

Browse... No file selected. Upload

[ ok ]

.:[ GNY.Shell | Standard Edition | Generated in: 0.0427 ]:.

# THE DORK SIDE OF GOOGLE

| | | | | |
|---|---|---|---|---|
| permit for foreign insurance company 2008.doc | 53.5 KB | 26.02.2012 14:47:38 | -rw-rw-rw- | [info] [change] [download] |
| regulation 9812.doc | 324 KB | 26.02.2012 14:47:38 | -rw-rw-rw- | [info] [change] [download] |

Select all | Unselect all | With selected: | Confirm

**Enter:** Execute

**Kernel Info:**
Windows NT HOSTER8-3 5.2 build 3790
Google!

**Functions**
Wipe Logs Using zap2 (*nix)
Execute

**Make Dir**
f:\inetpub\vhosts\ \httpdocs\
Create
[ ok ]

**Go Dir**
f:\inetpub\vhosts\ \httpdocs\
Go

**Aliases**
----------
Execute

**Make File**
f:\inetpub\vhosts\ \httpdocs\
Create
[ ok ]

**Go File**
f:\inetpub\vhosts\ \httpdocs\
Go

PHP Safe-Mode Bypass (Read File)

File Read File

e.g.: /etc/passwd or C:\WINDOWS\system32\.SAM

PHP Safe-Mode Bypass (Directory Listing)

Dir: List Directory

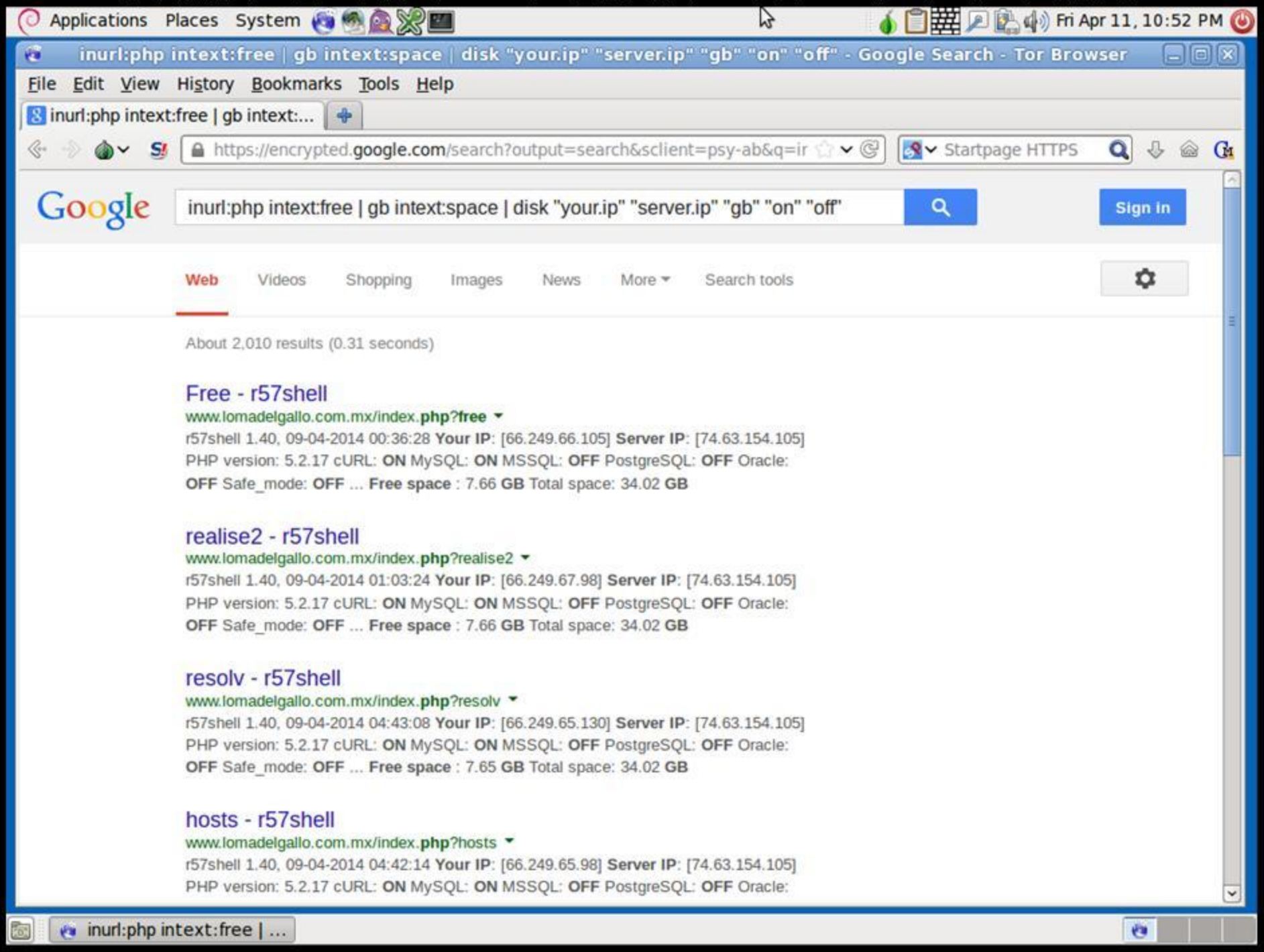
e.g.: /etc/ or C:\

**Search**
(.*) - regexp Search

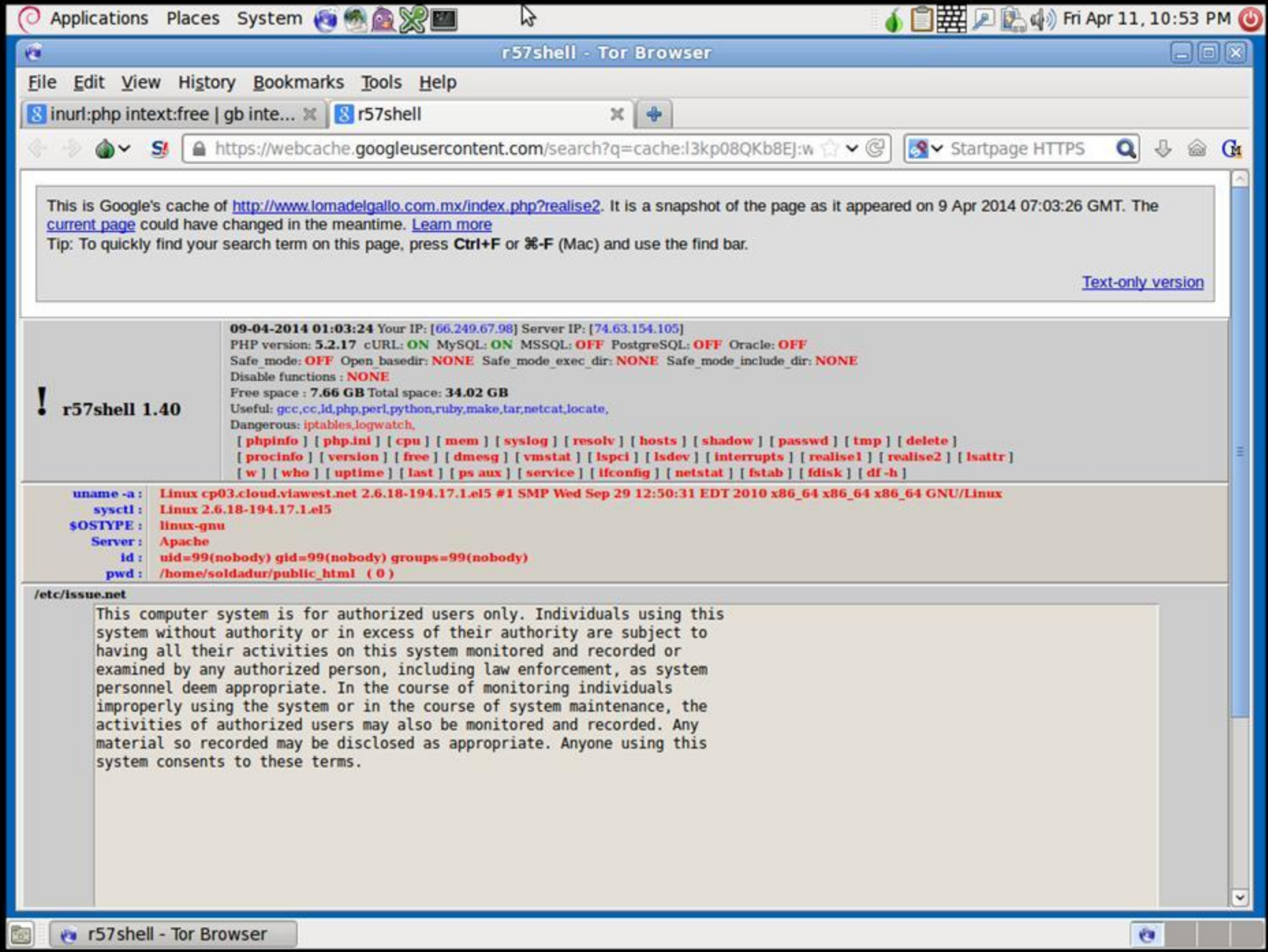
**Upload**
Browse... No file selected. Upload
[ ok ]

.: GNY.Shell Standard Edition | Generated in: 0.0427 ]:.

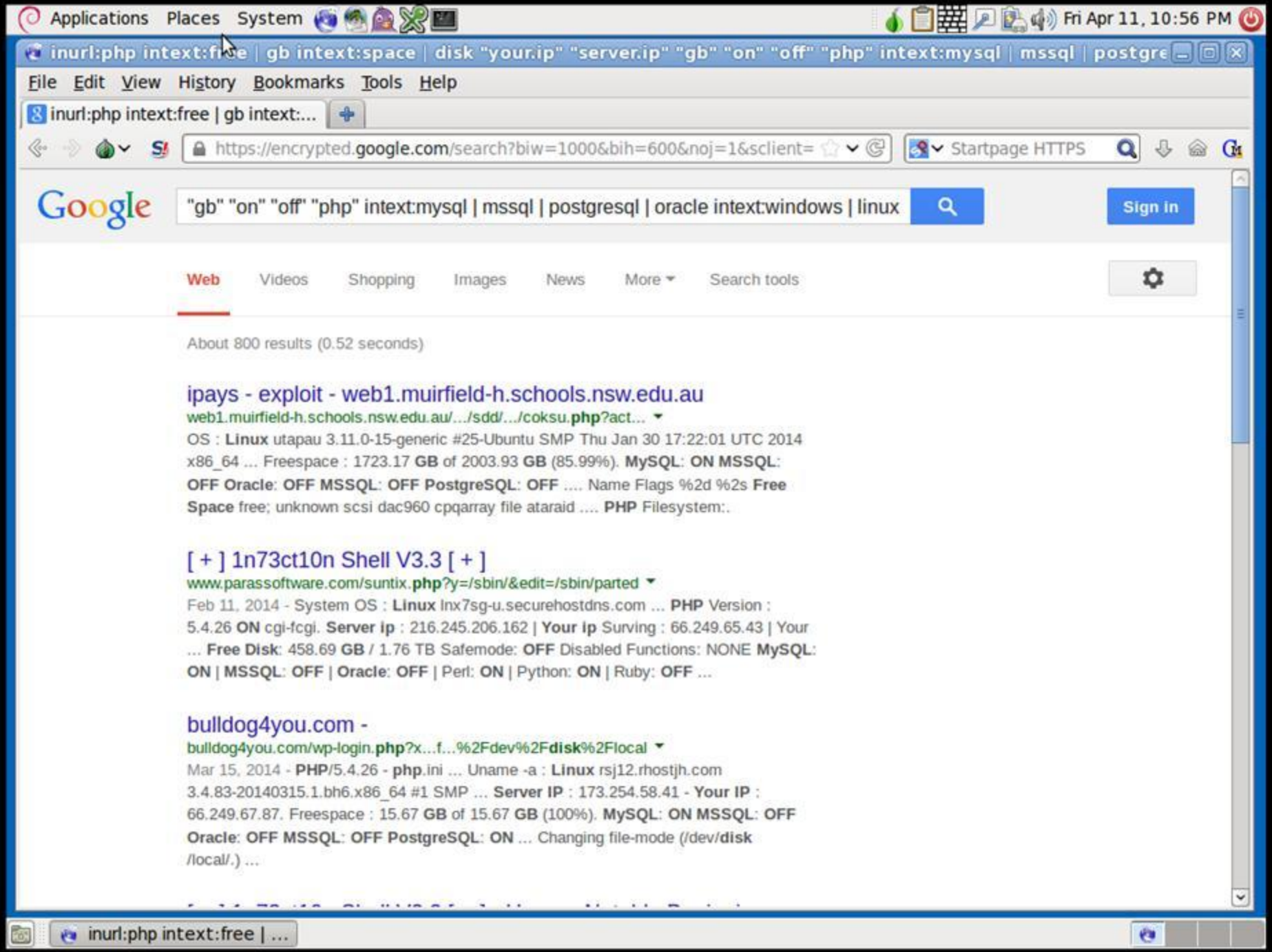
# THE DORK SIDE OF GOOGLE



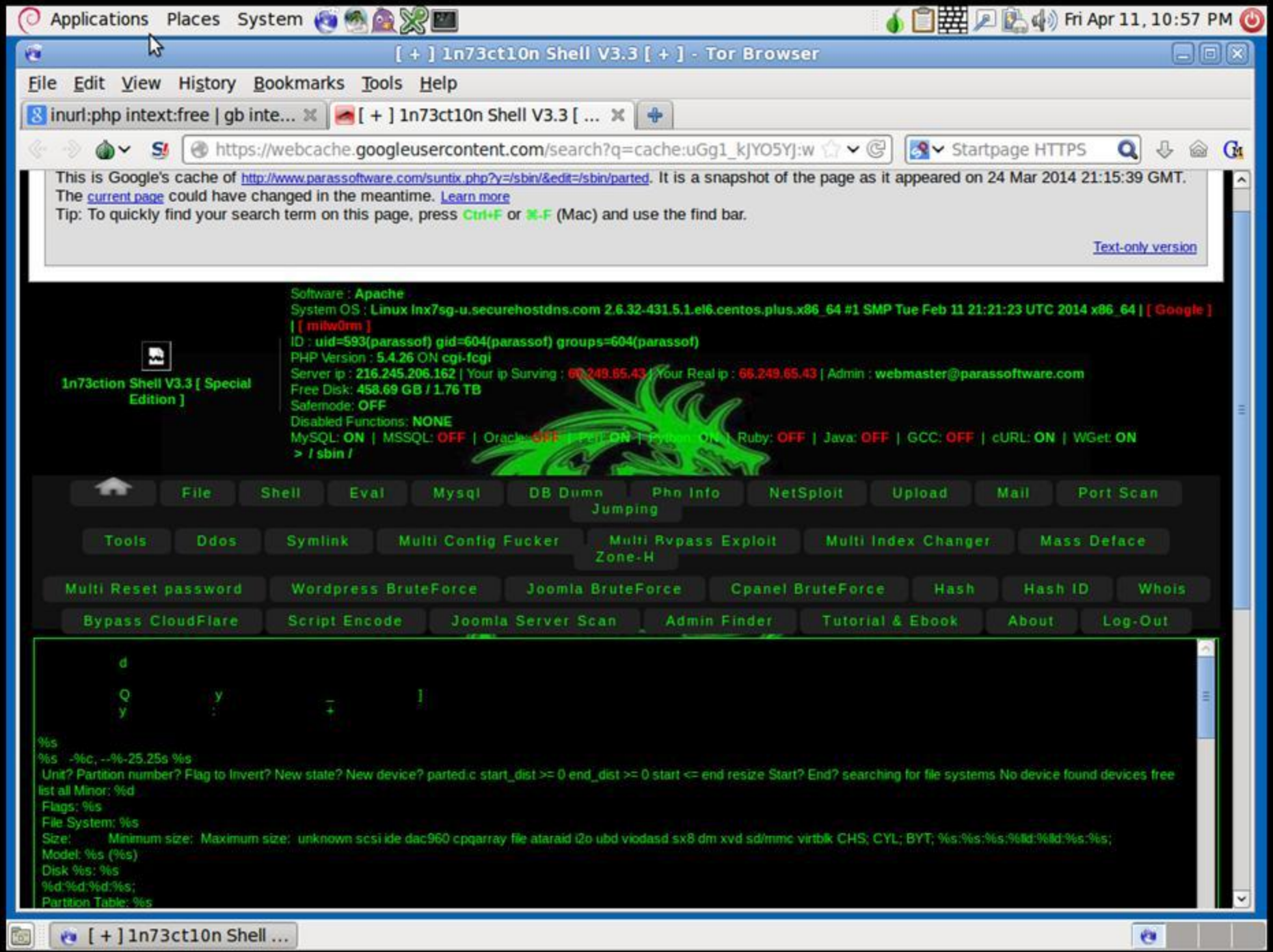
# THE DORK SIDE OF GOOGLE

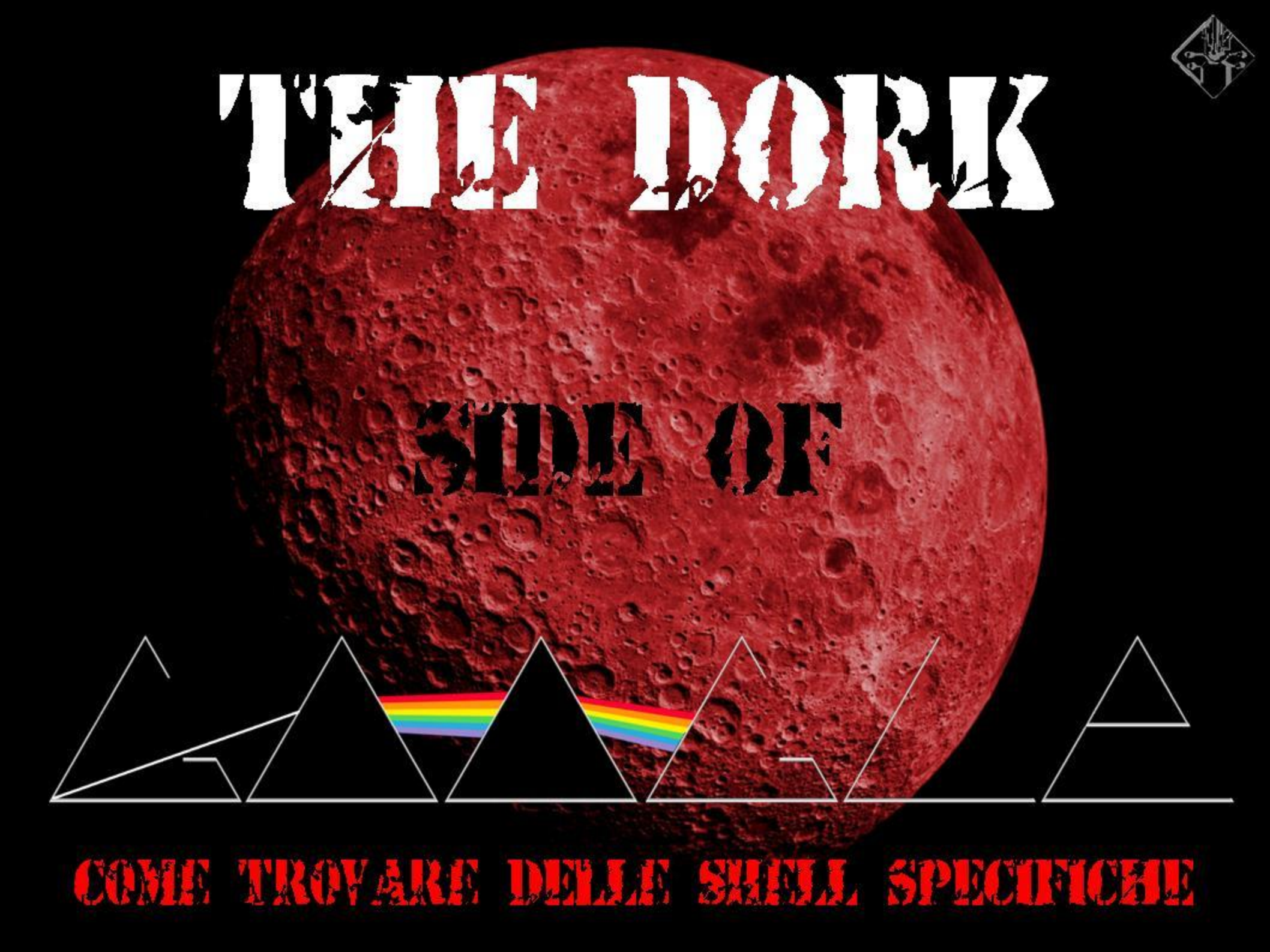


# THE DORK SIDE OF GOOGLE

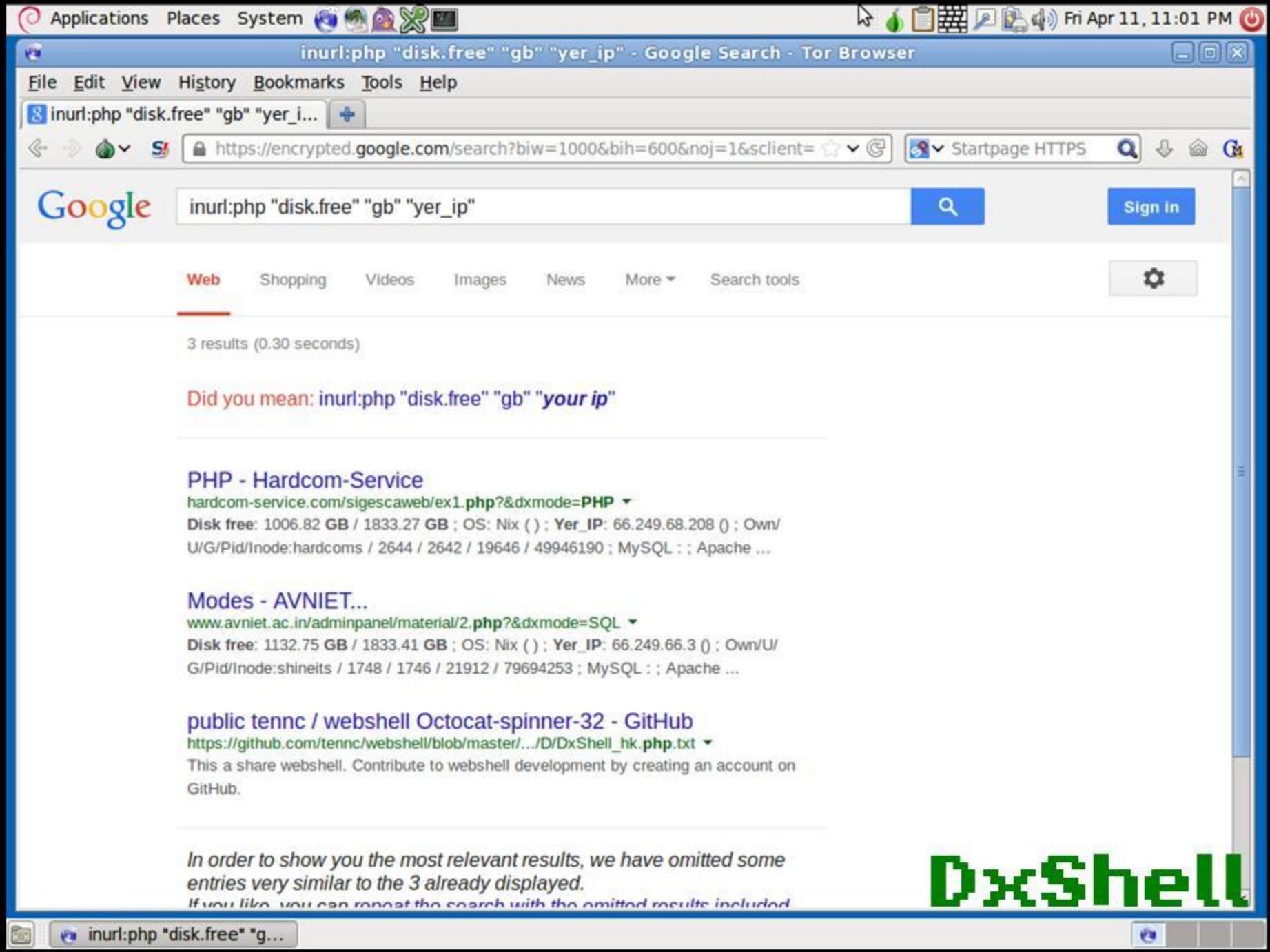


# THE DORK SIDE OF GOOGLE

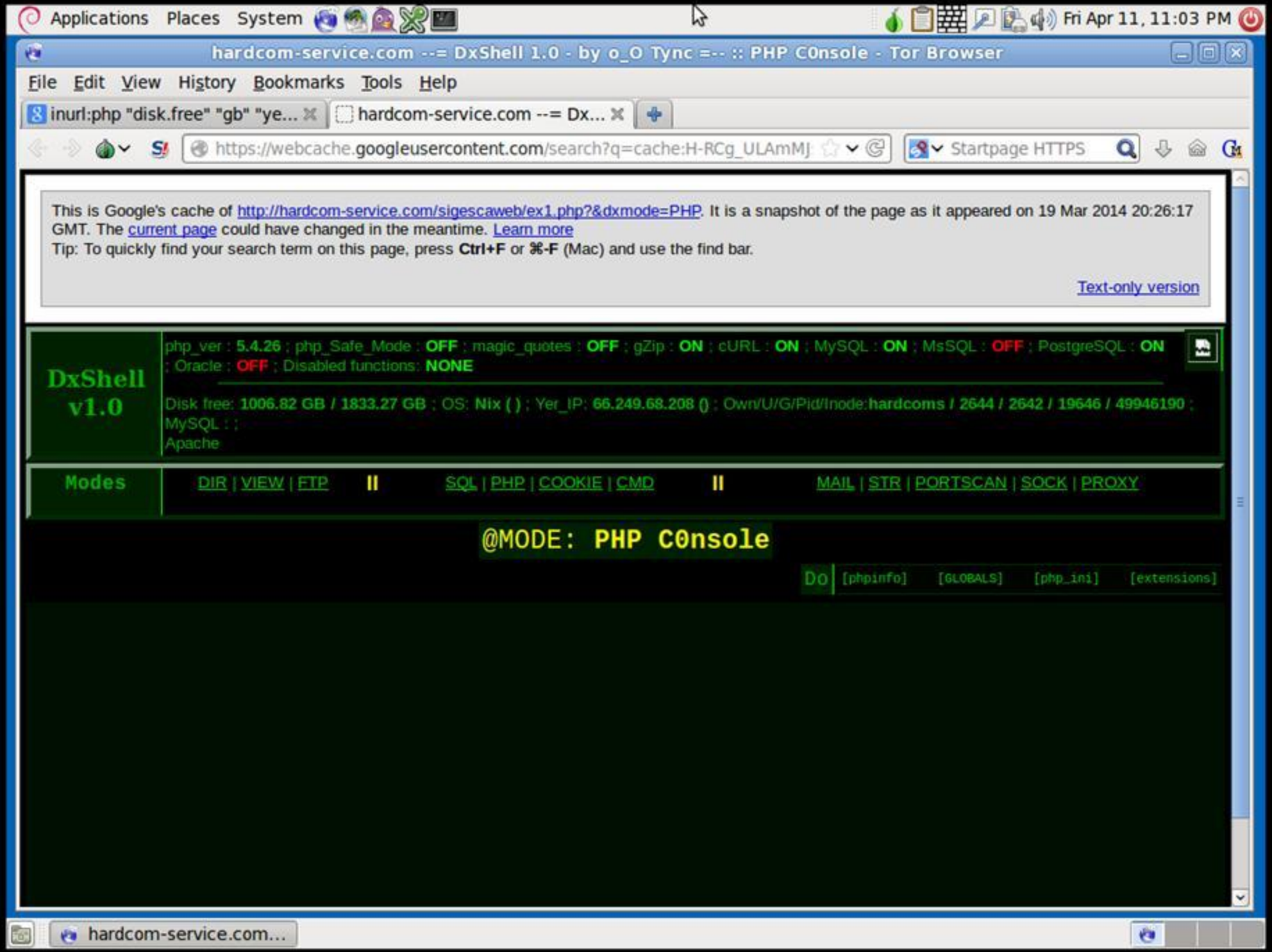



THE DORK
SIDE OF
COME TROVARE DELLE SHELL SPECIFICHE

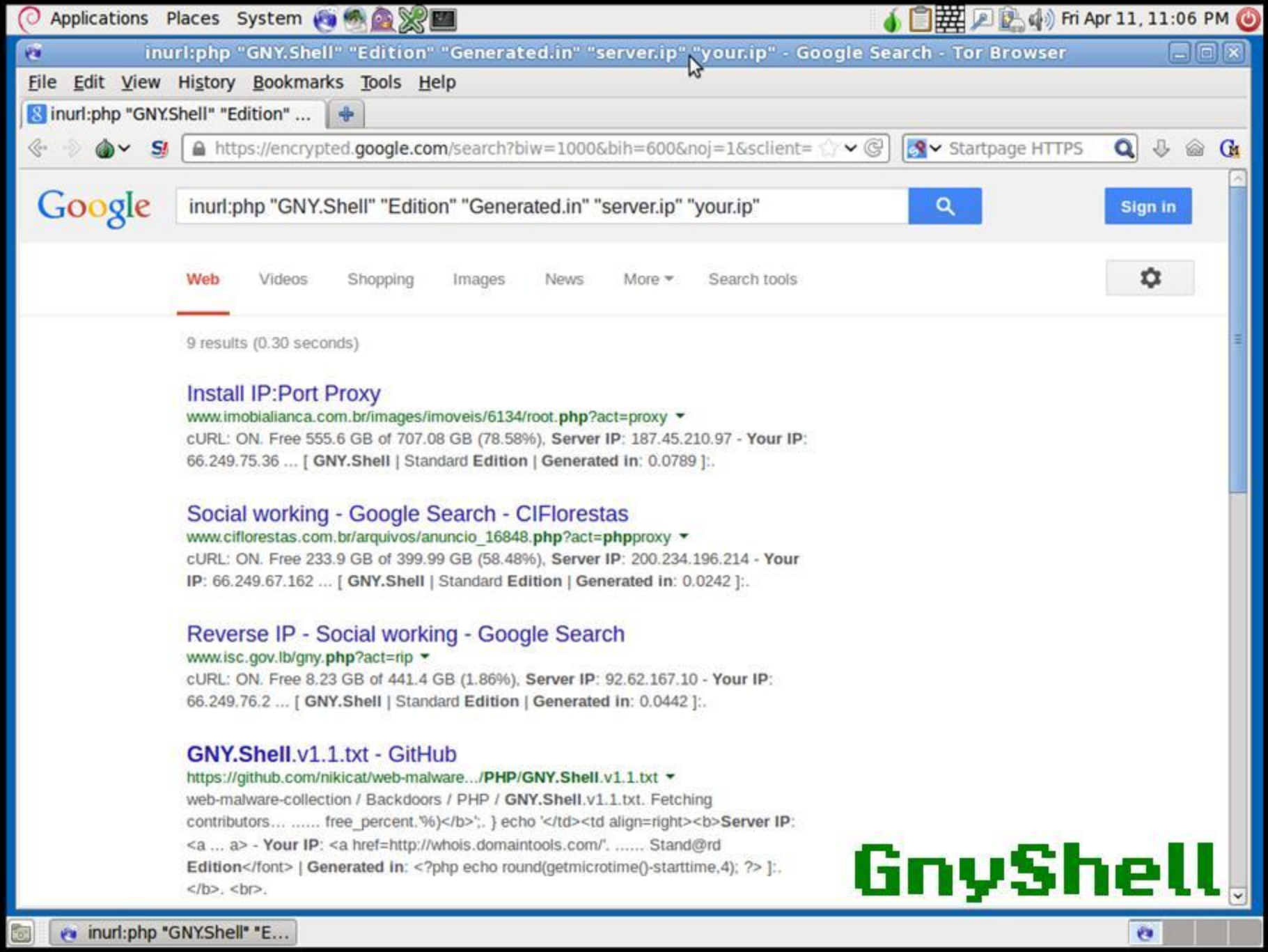
# THE DORK SIDE OF GOOGLE



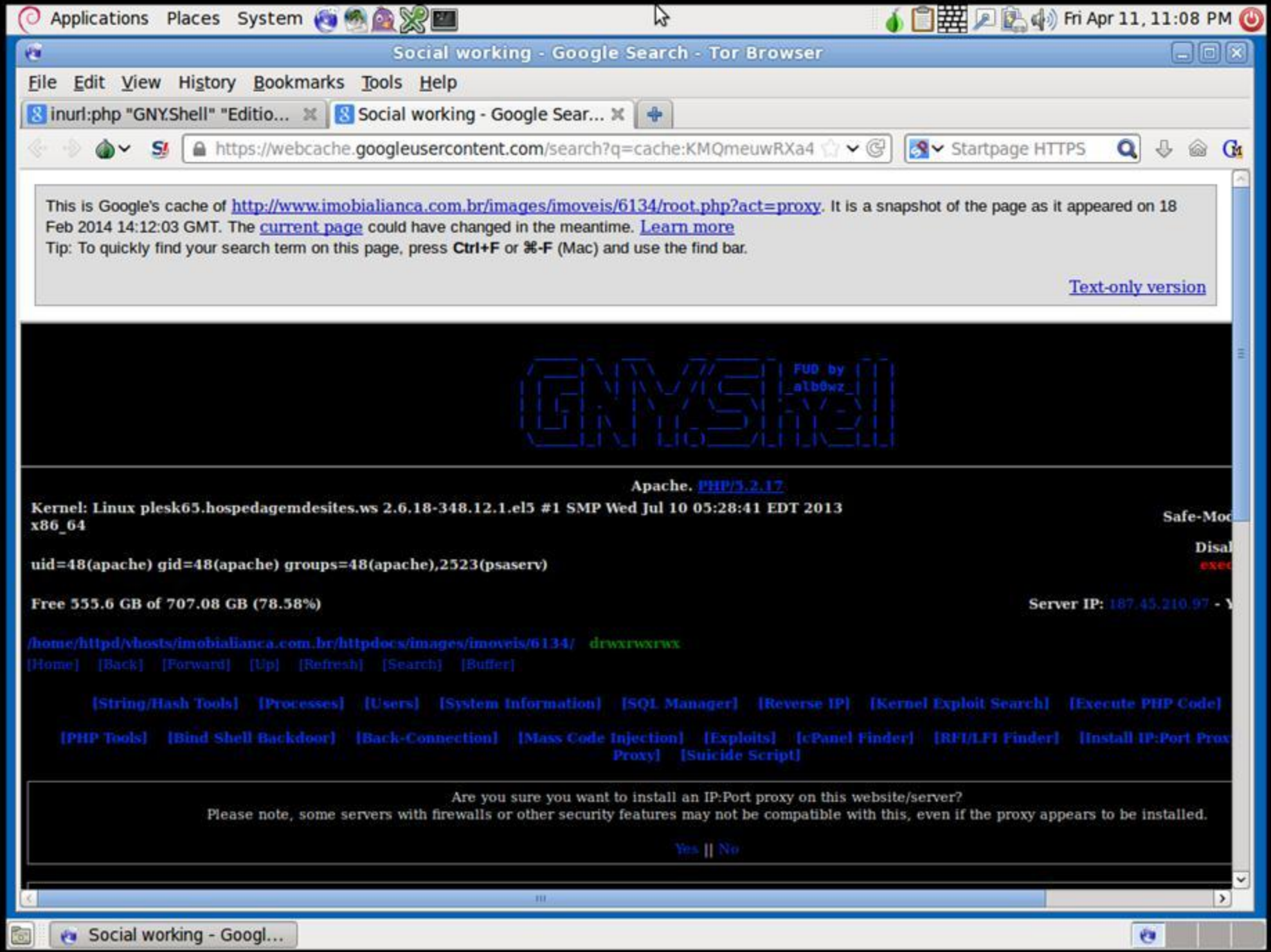
# THE DORK SIDE OF GOOGLE



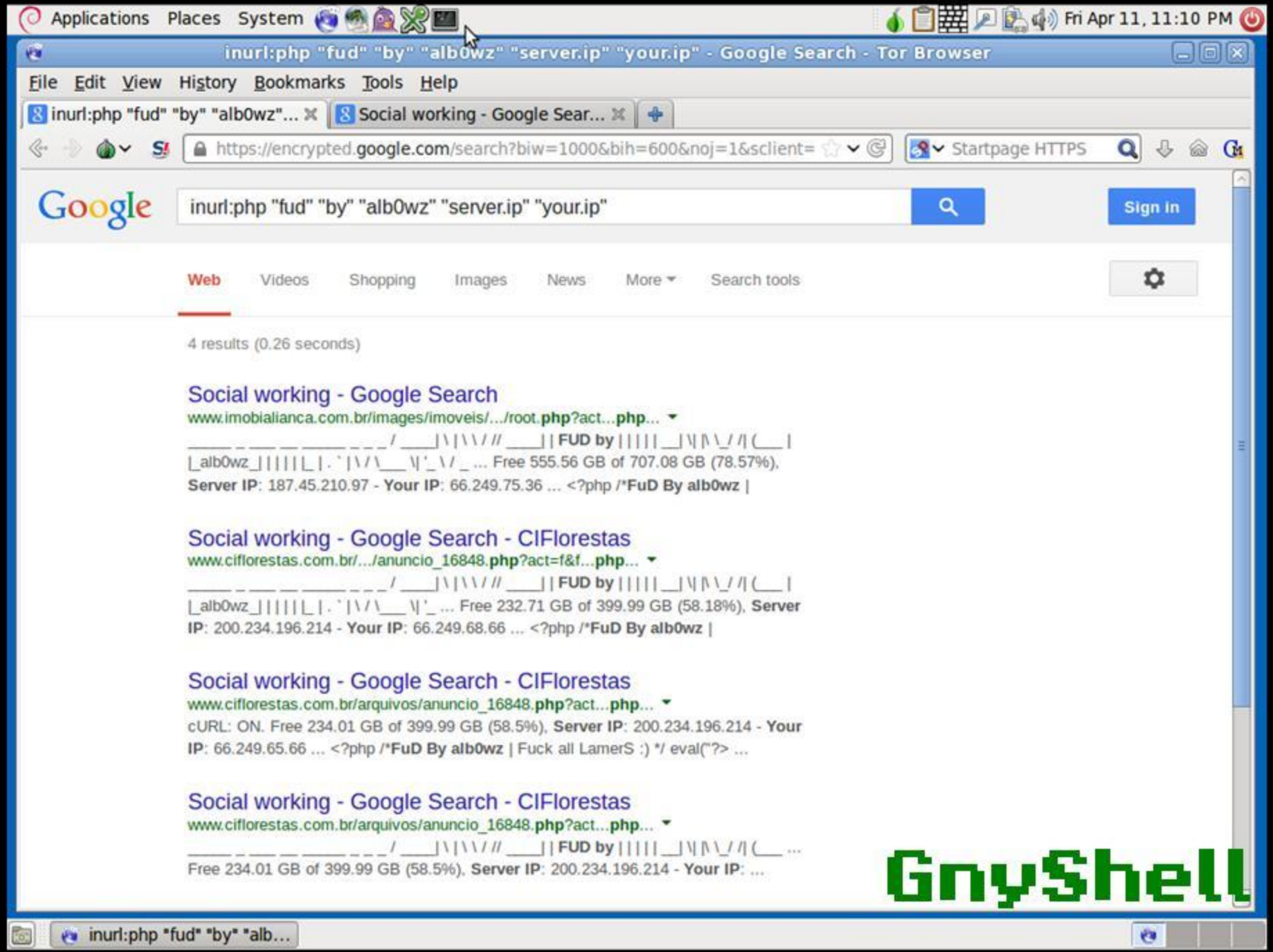
# THE DORK SIDE OF GOOGLE



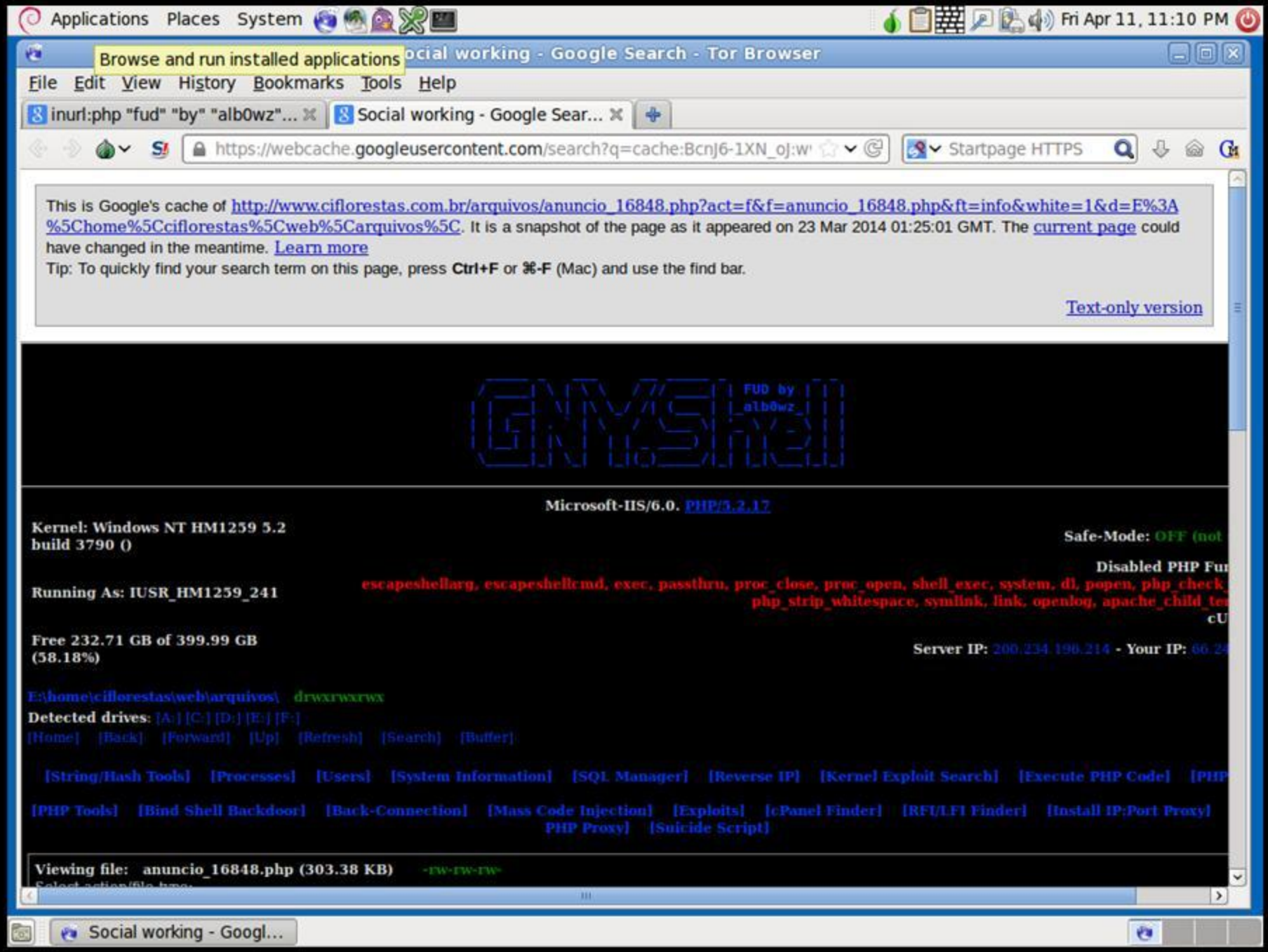
# THE DORK SIDE OF GOOGLE



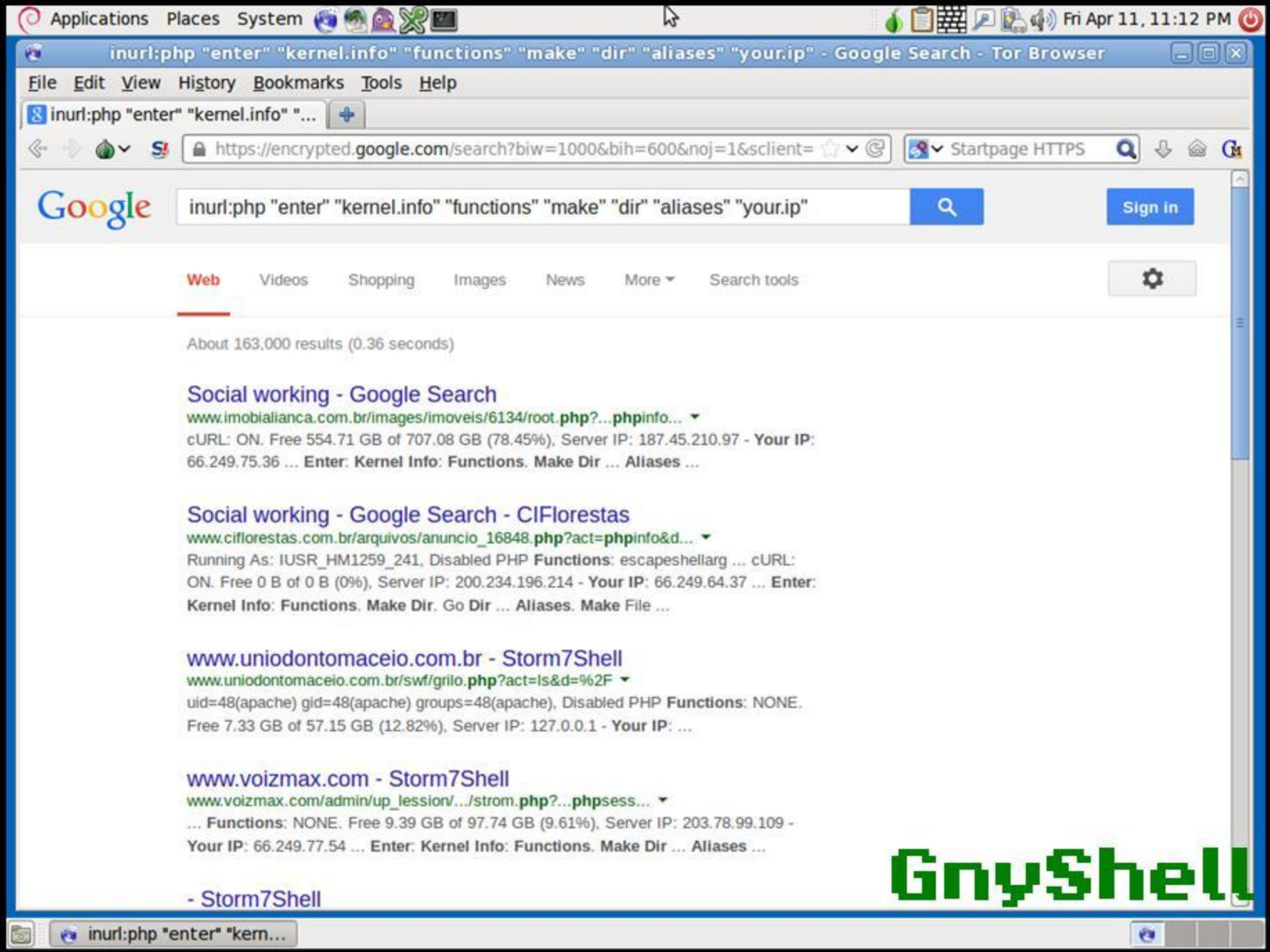
# THE DORK SIDE OF GOOGLE



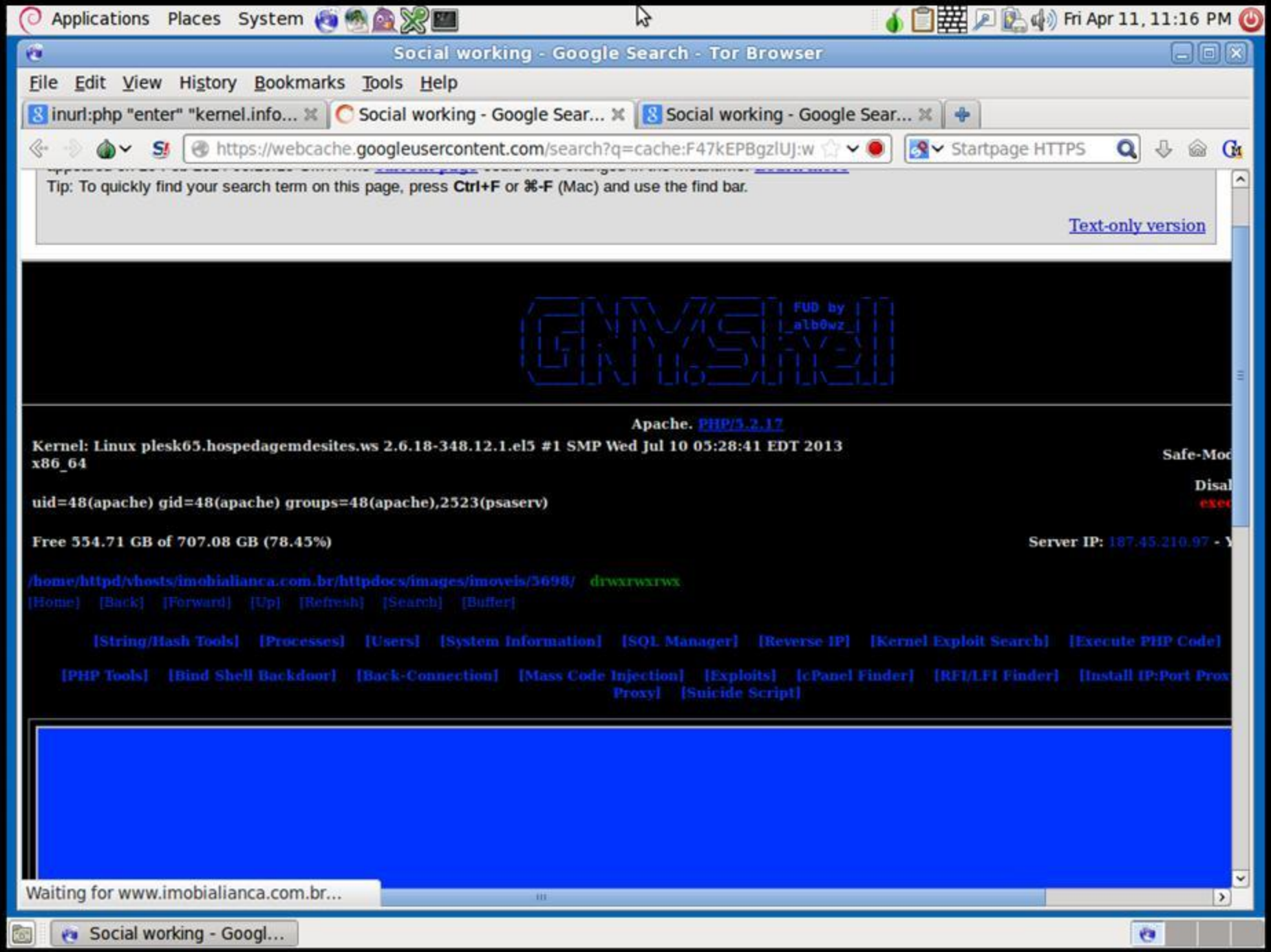
# THE DORK SIDE OF GOOGLE



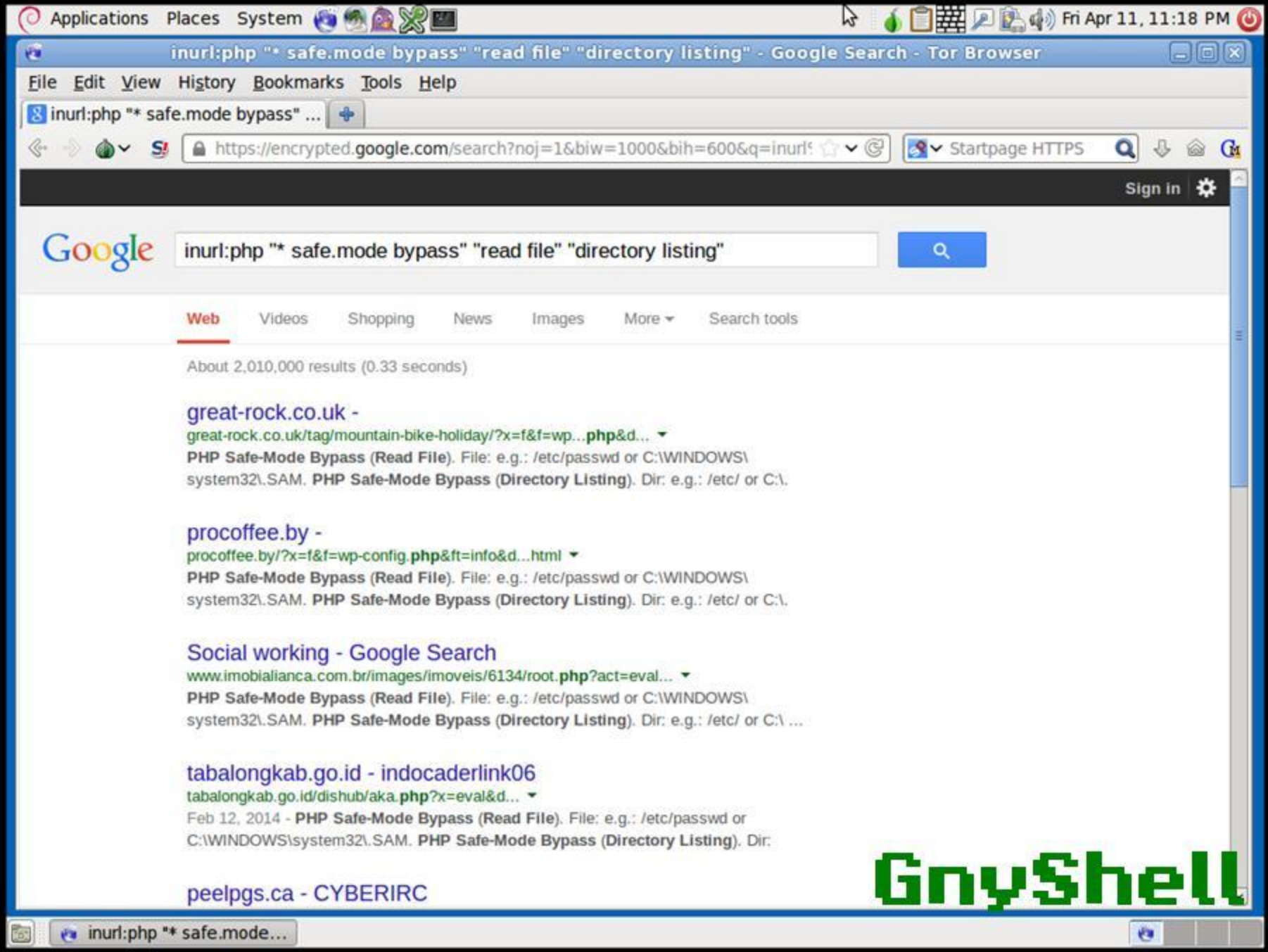
# THE DORK SIDE OF GOOGLE



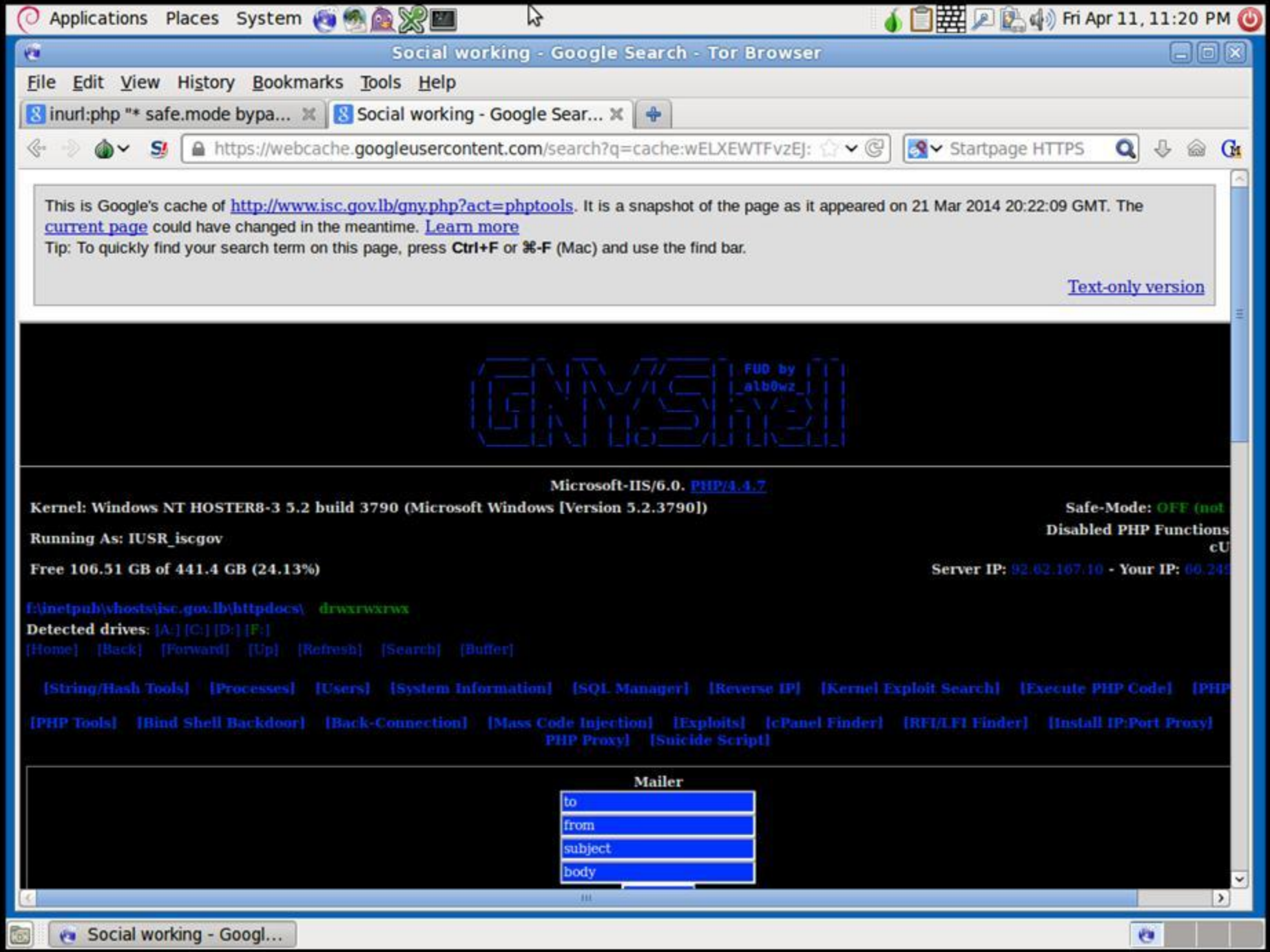
# THE DORK SIDE OF GOOGLE



# THE DORK SIDE OF GOOGLE

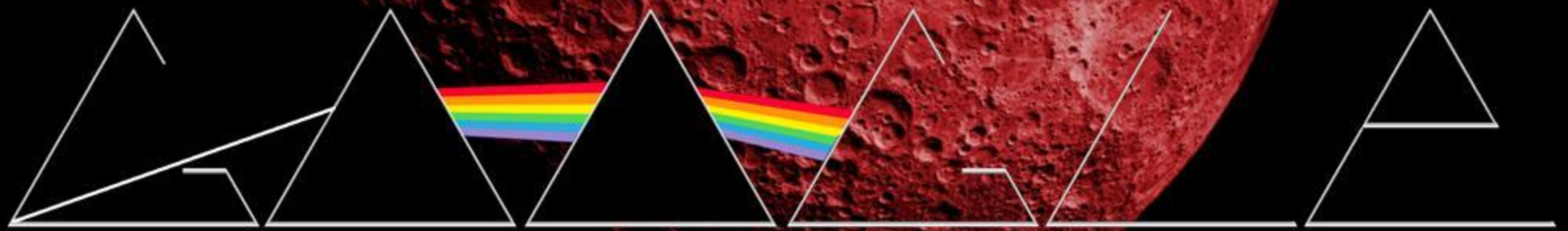


# THE DORK SIDE OF GOOGLE



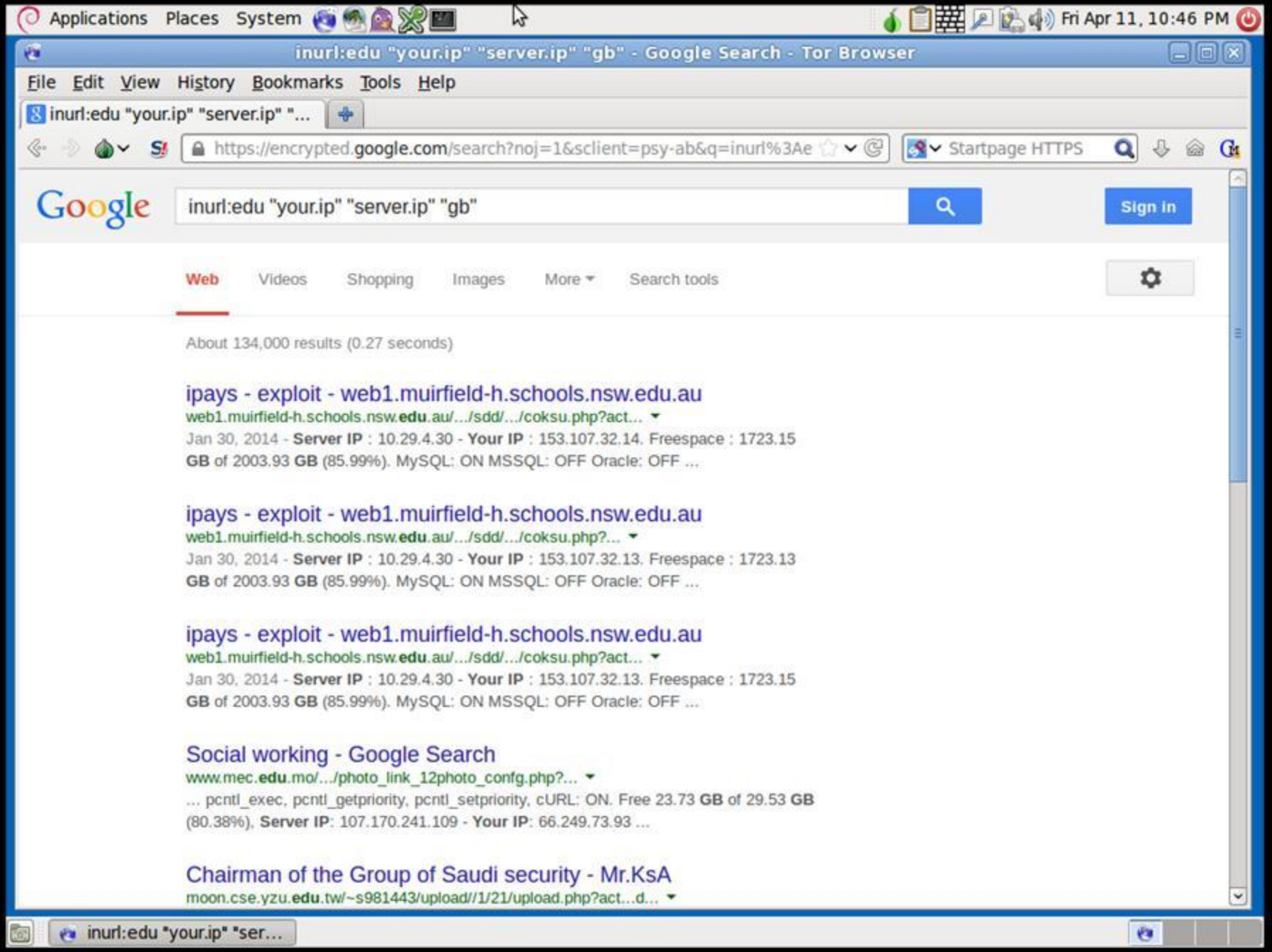
# THE DORK

# SIDE OF

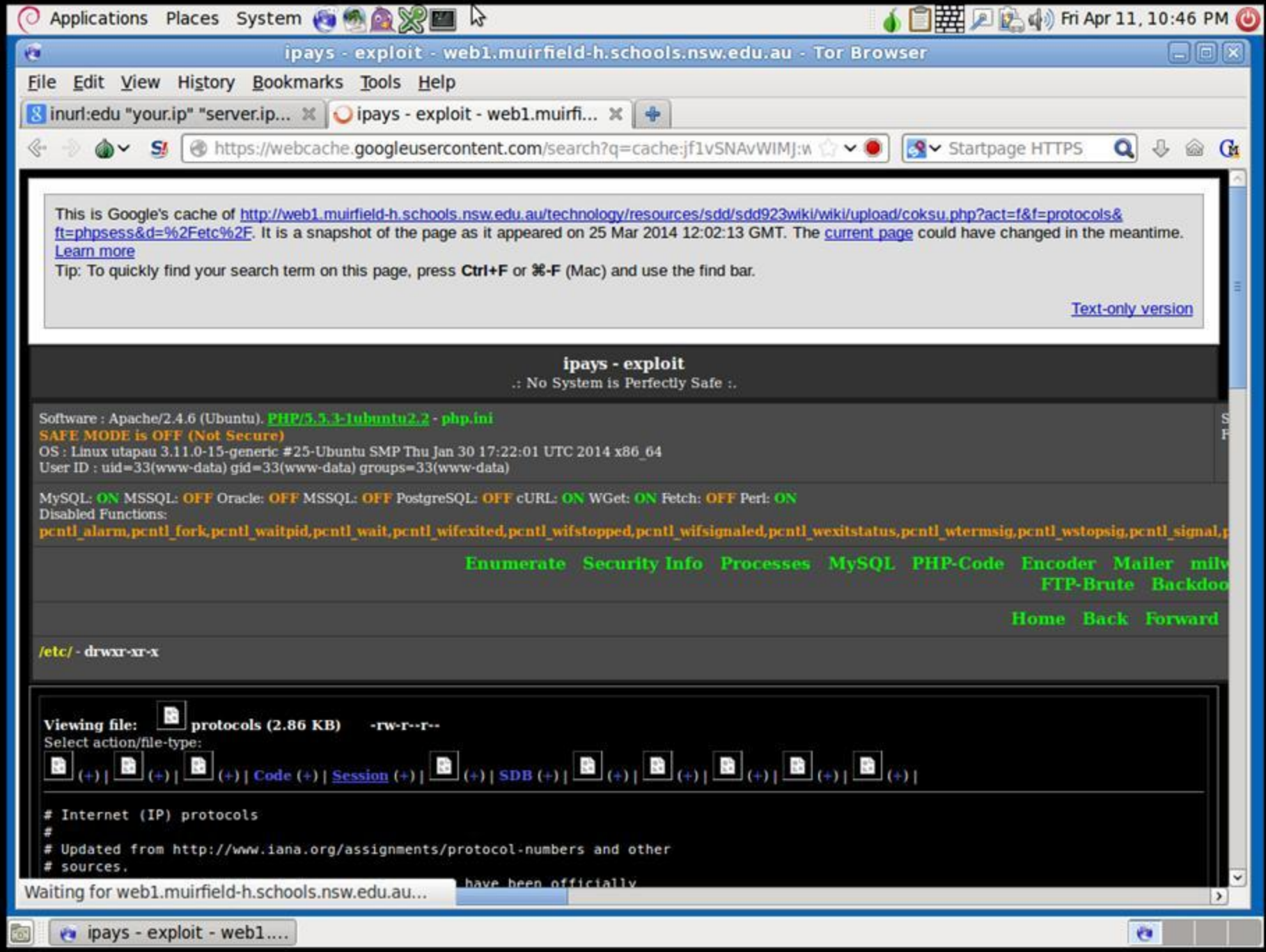


## COME TROVARE DELLE SHELL UNIVERSITARIE

# THE DORK SIDE OF GOOGLE

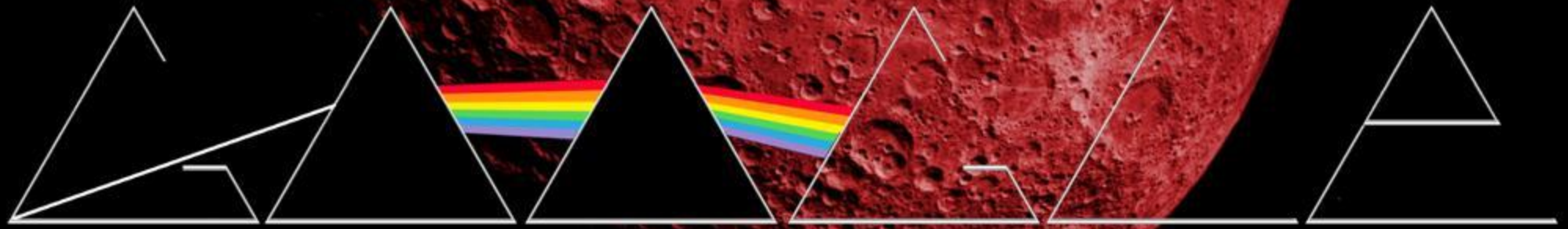


# THE DORK SIDE OF GOOGLE



# THE DORK

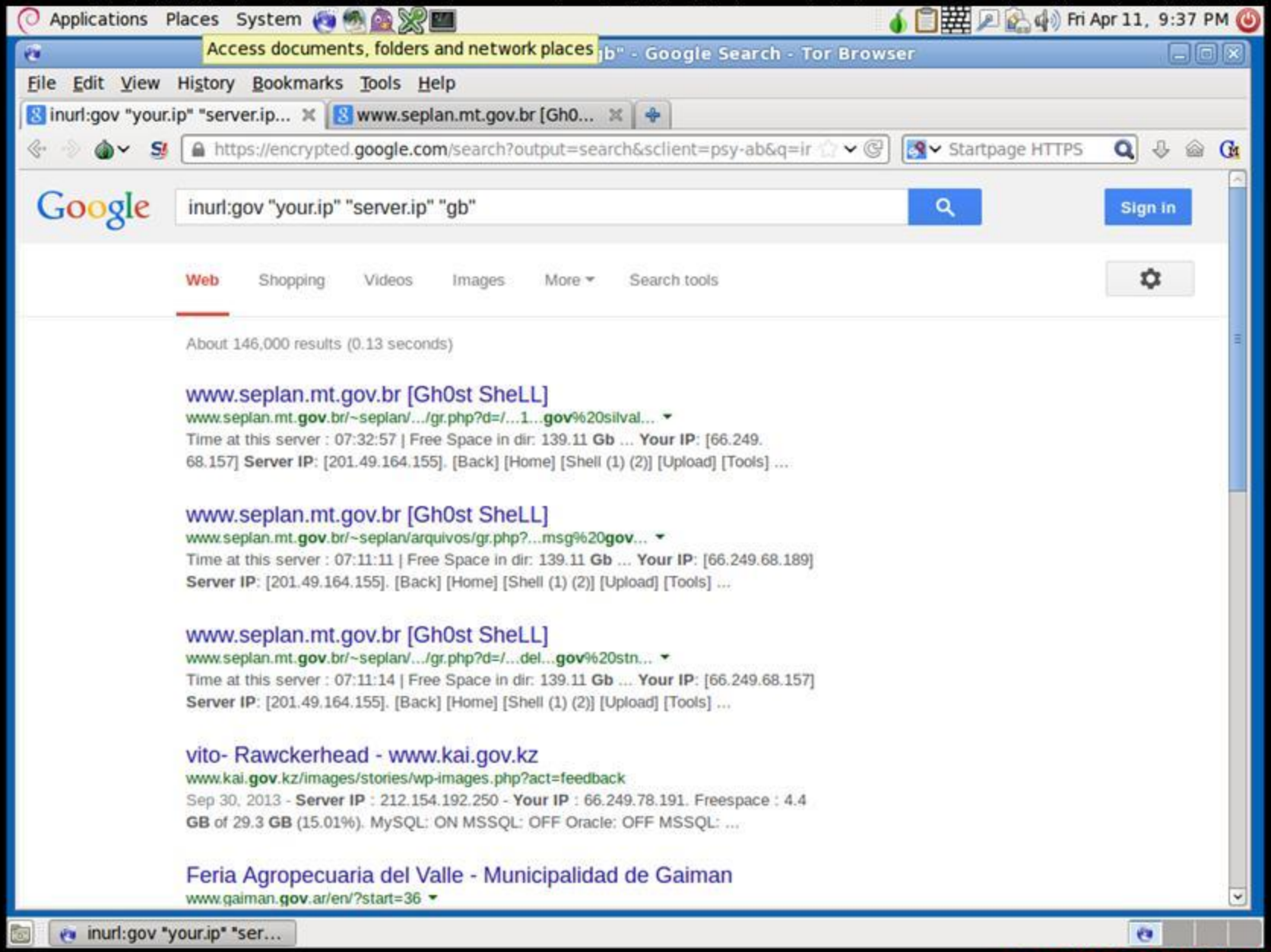
## SIDE OF



## COME OTTENERE LE PAGINE GIALLE DELLE

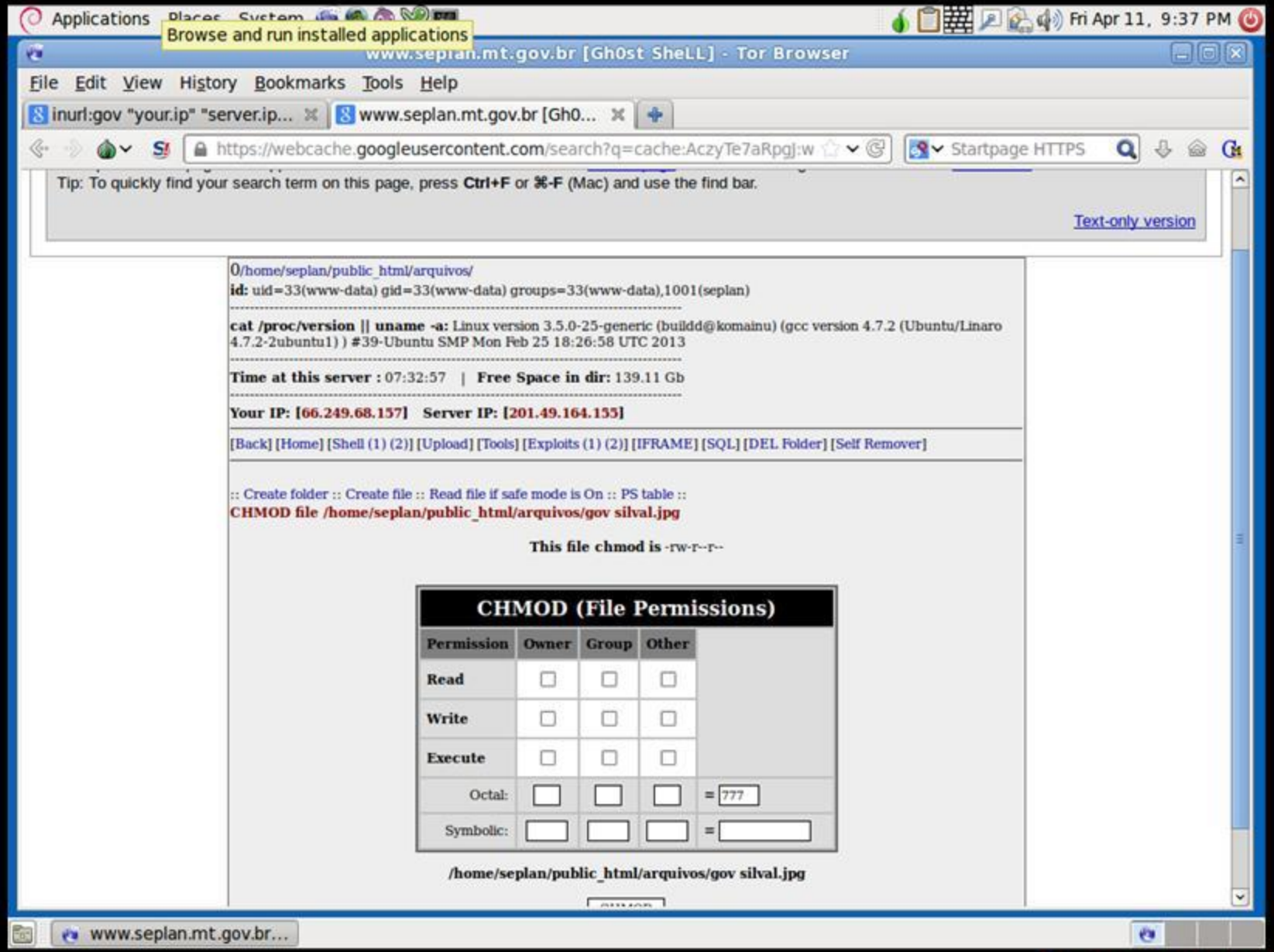
## shell governative

# THE DORK SIDE OF GOOGLE



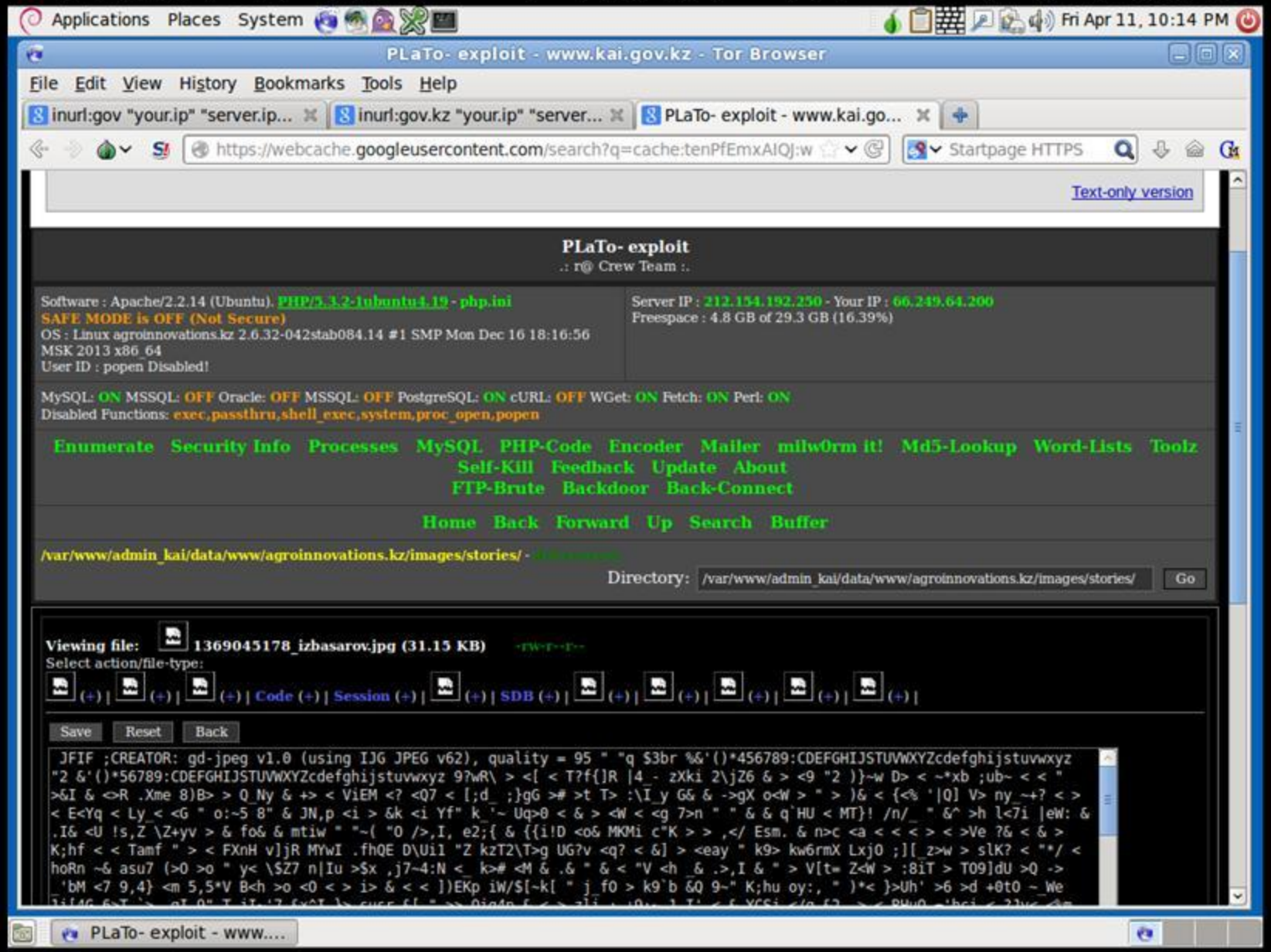

GENERICO

# THE DORK SIDE OF GOOGLE



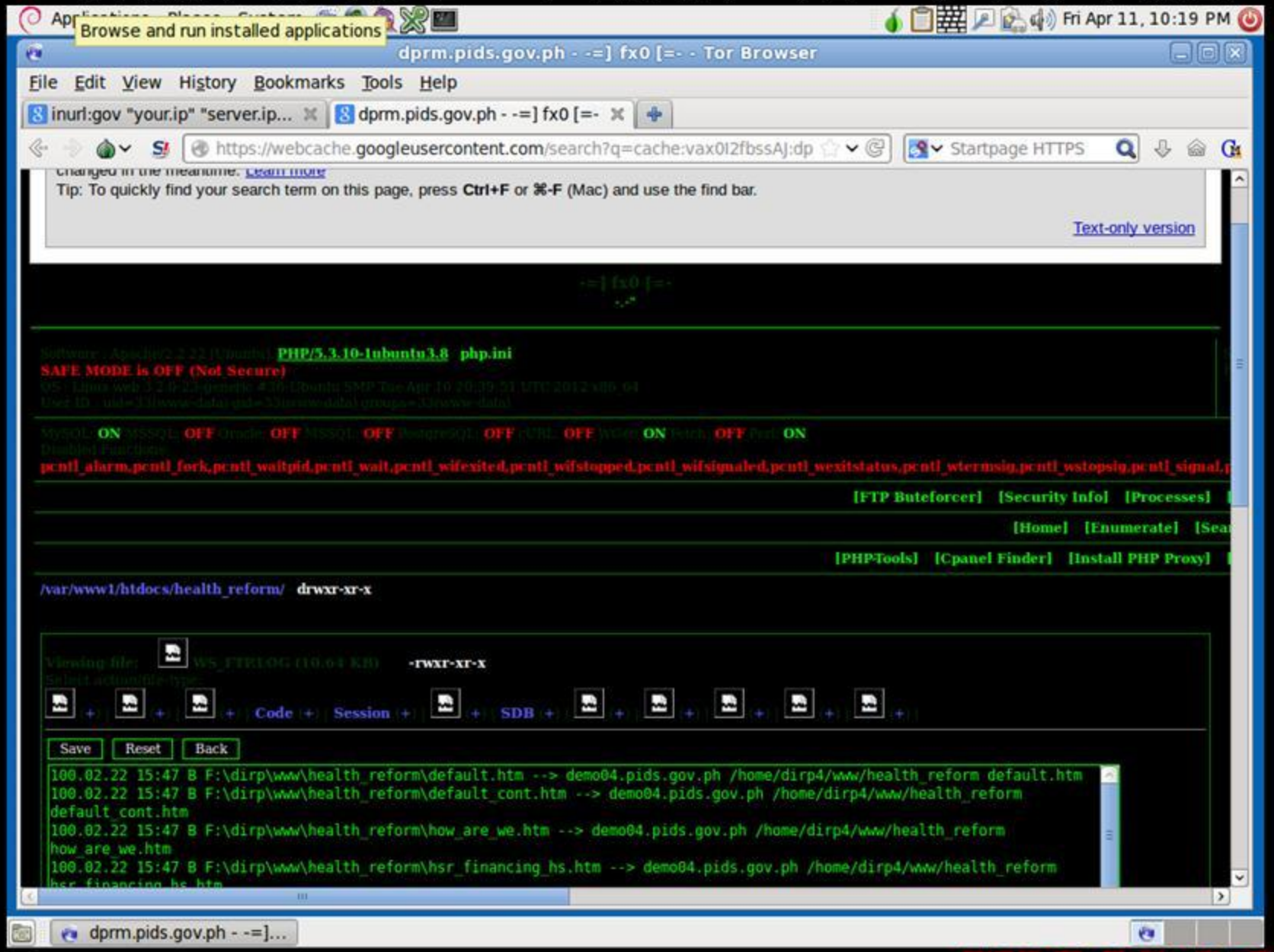

BRASIL

# THE DORK SIDE OF GOOGLE



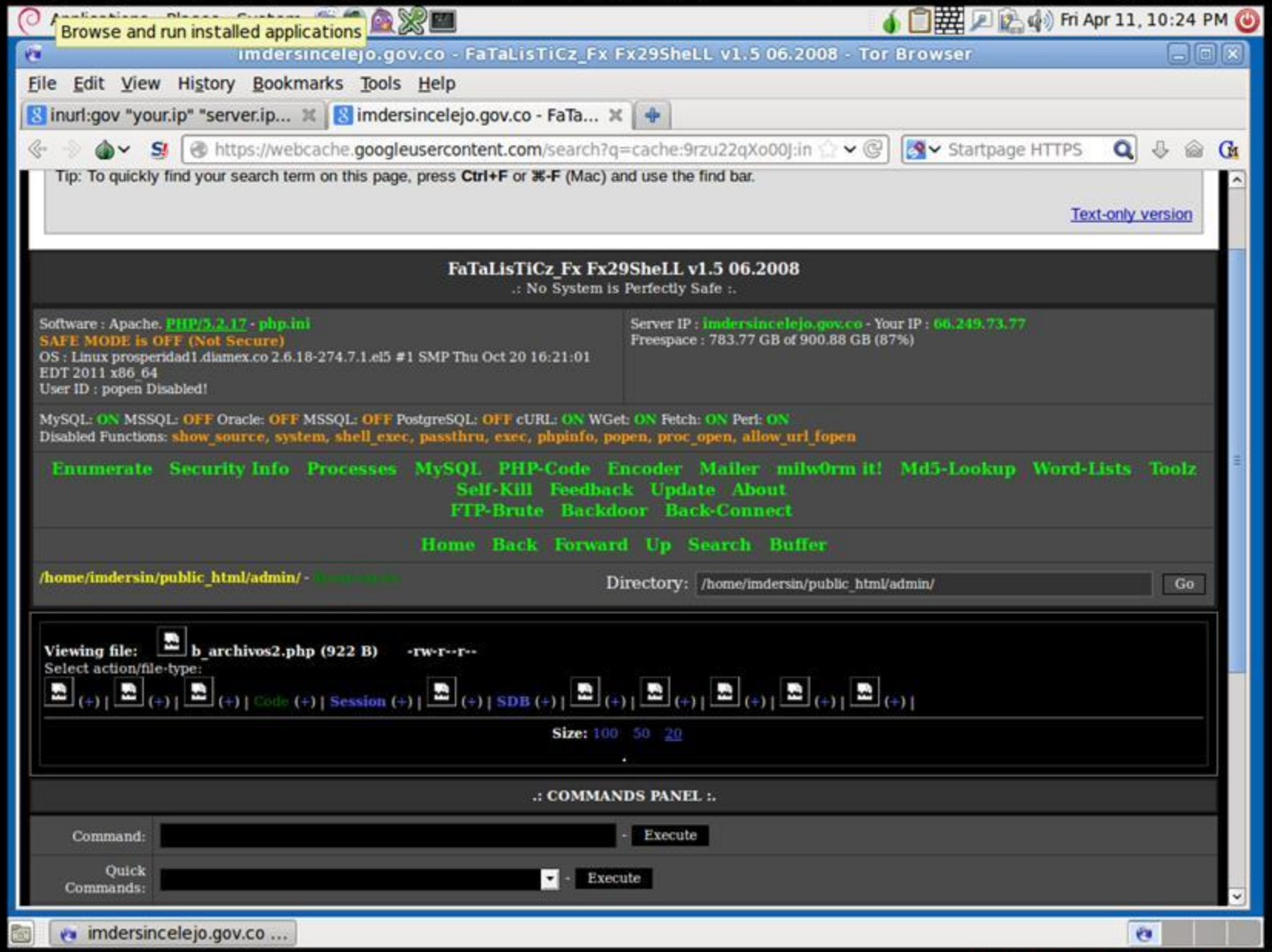

# KAZAKISTAN

# THE DORK SIDE OF GOOGLE



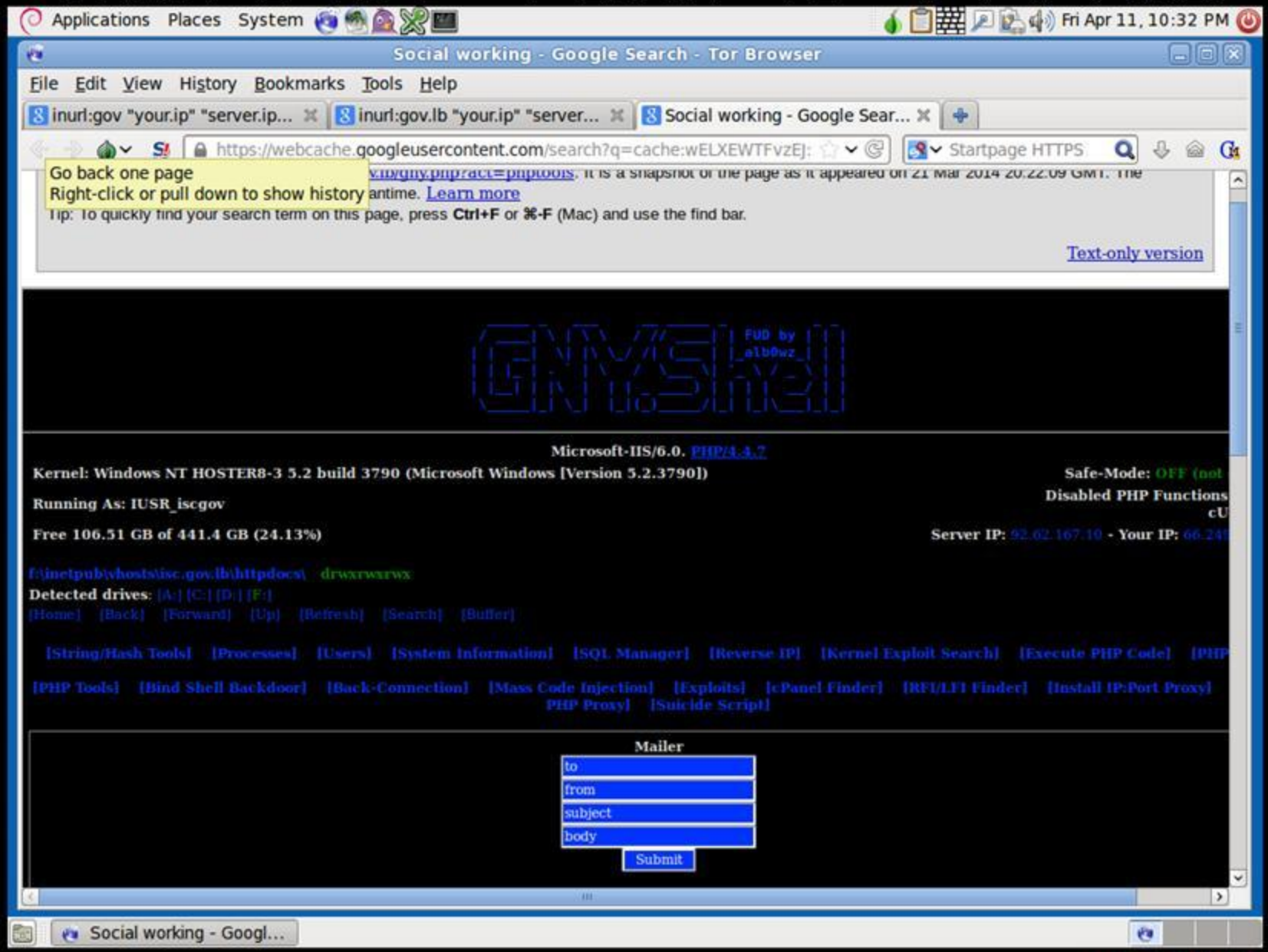

# FILIPINE

# THE DORK SIDE OF GOOGLE



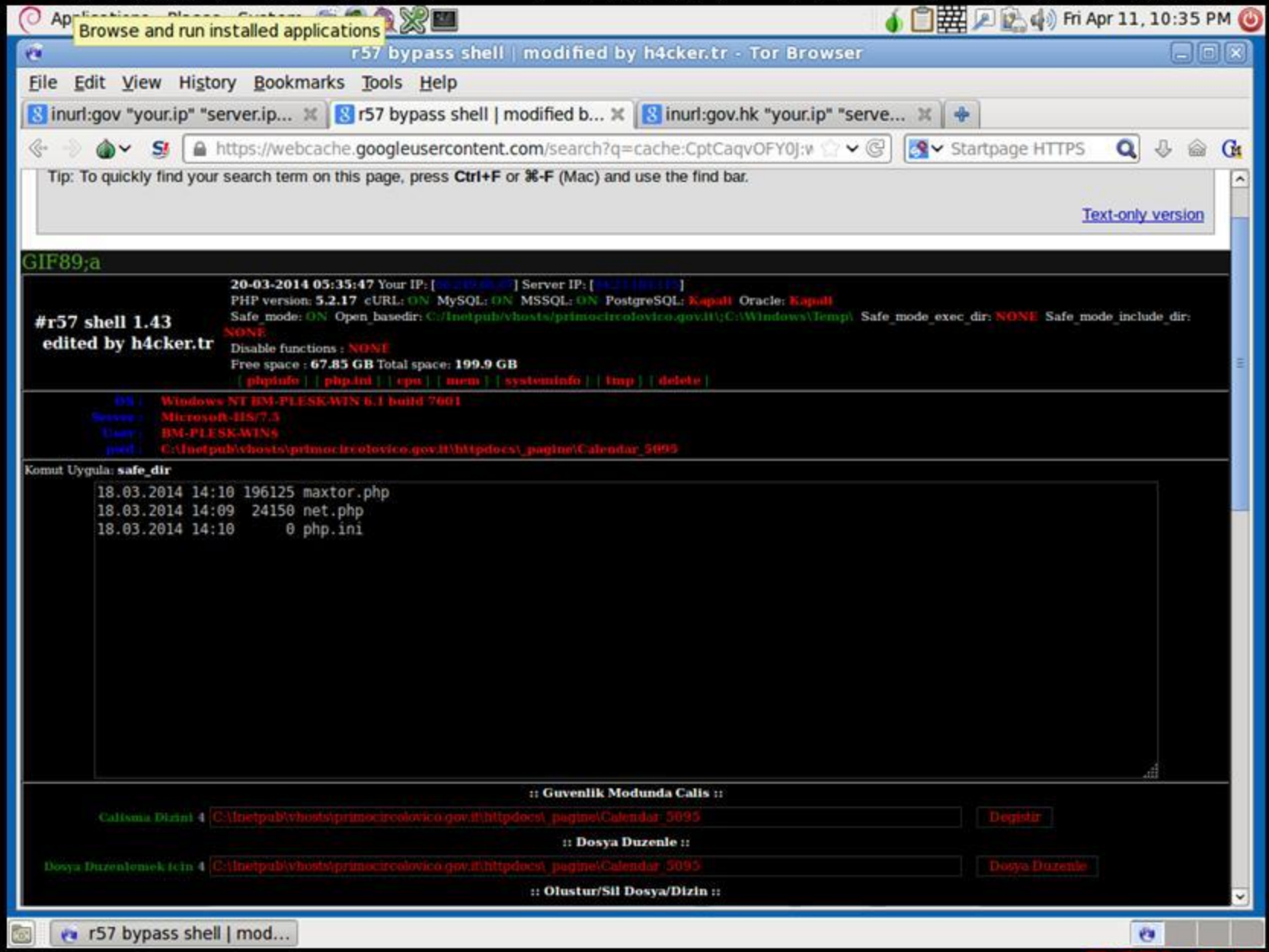

COLOMBIA

# THE DORK SIDE OF GOOGLE




LIBANO

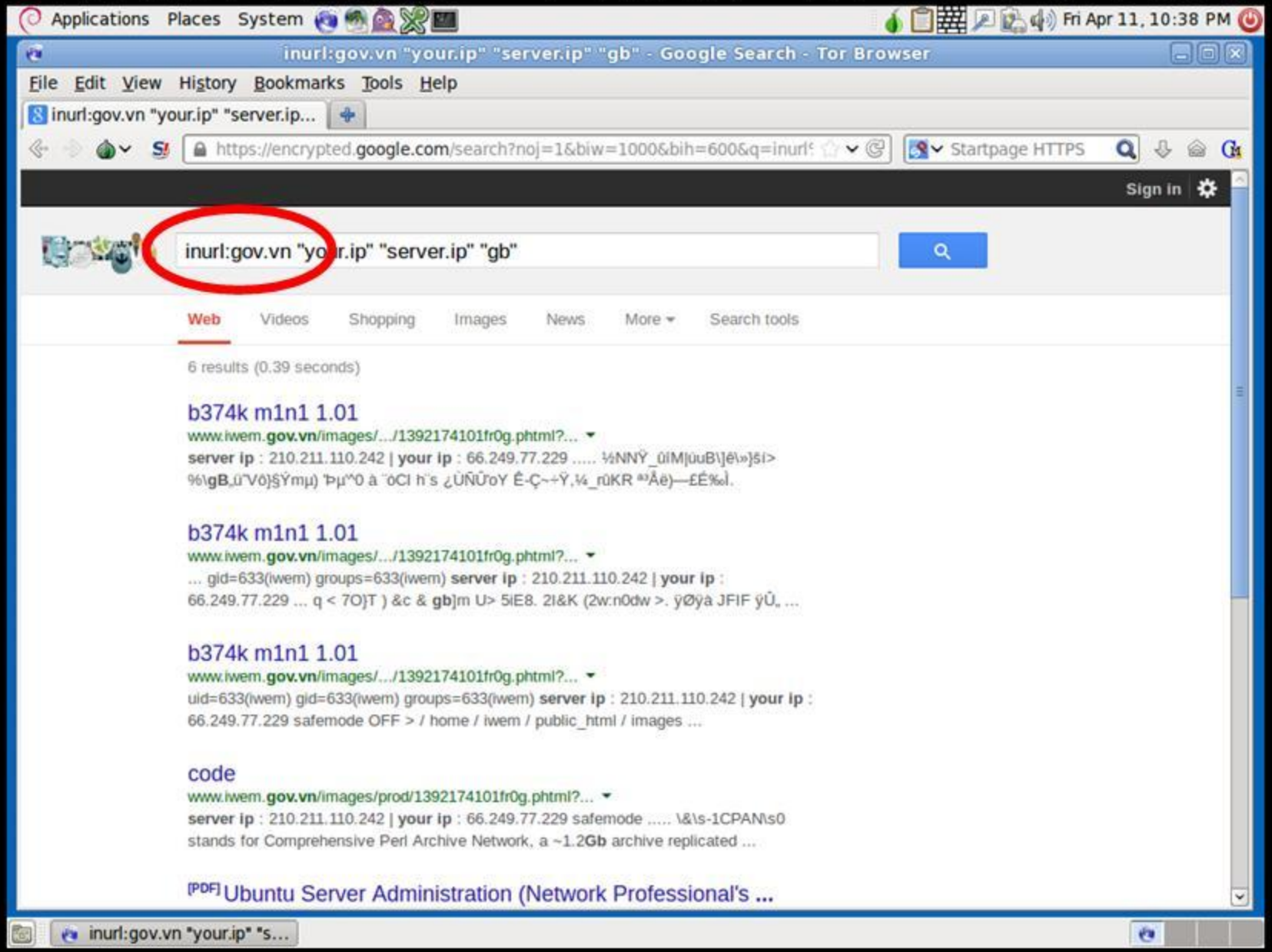
# THE DORK SIDE OF GOOGLE




ITALIA

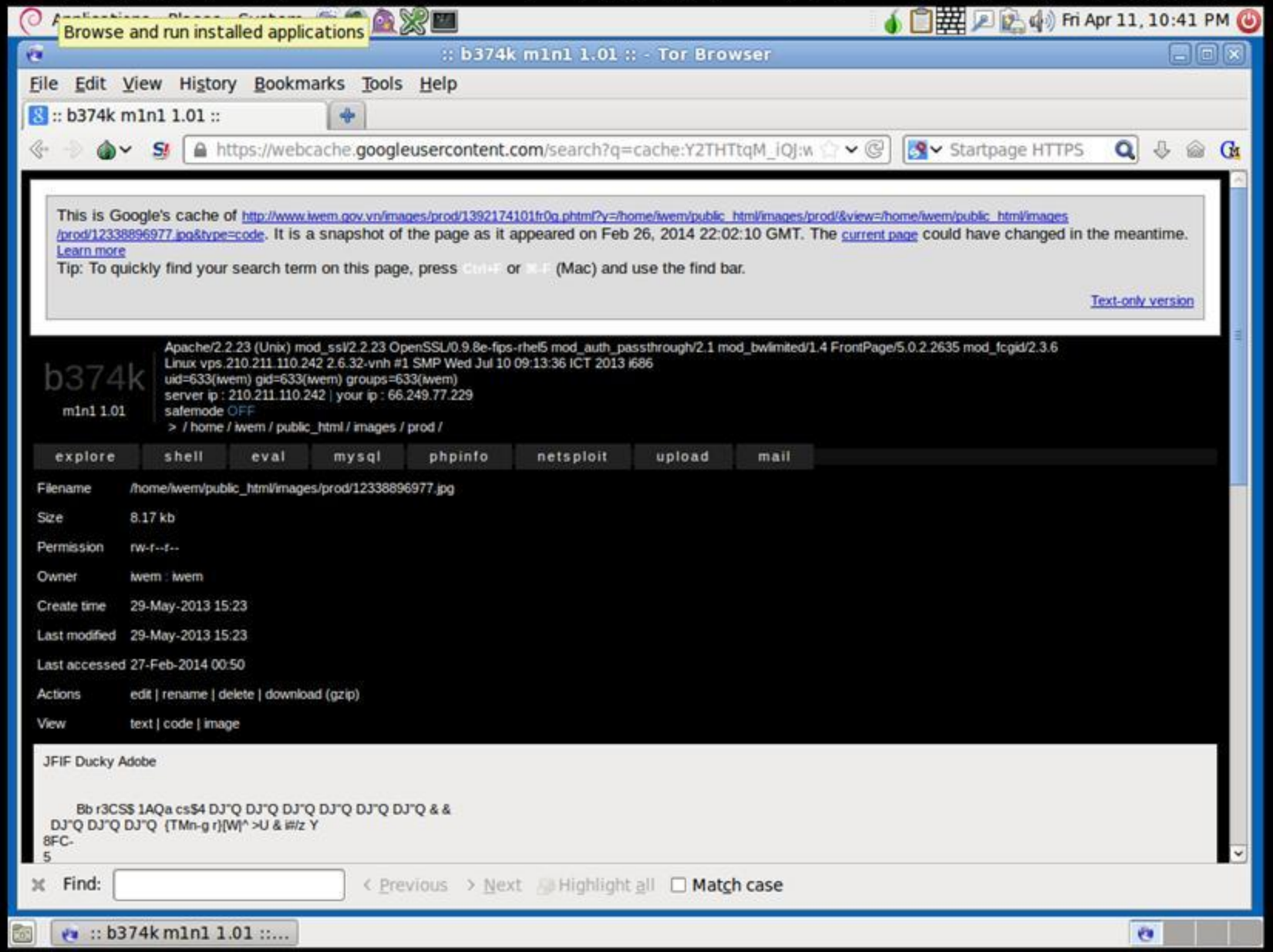

THE DORK
SIDE OF
ALCUNI TRUCCHI DA SAPERE
sulle shell governative

# THE DORK SIDE OF GOOGLE



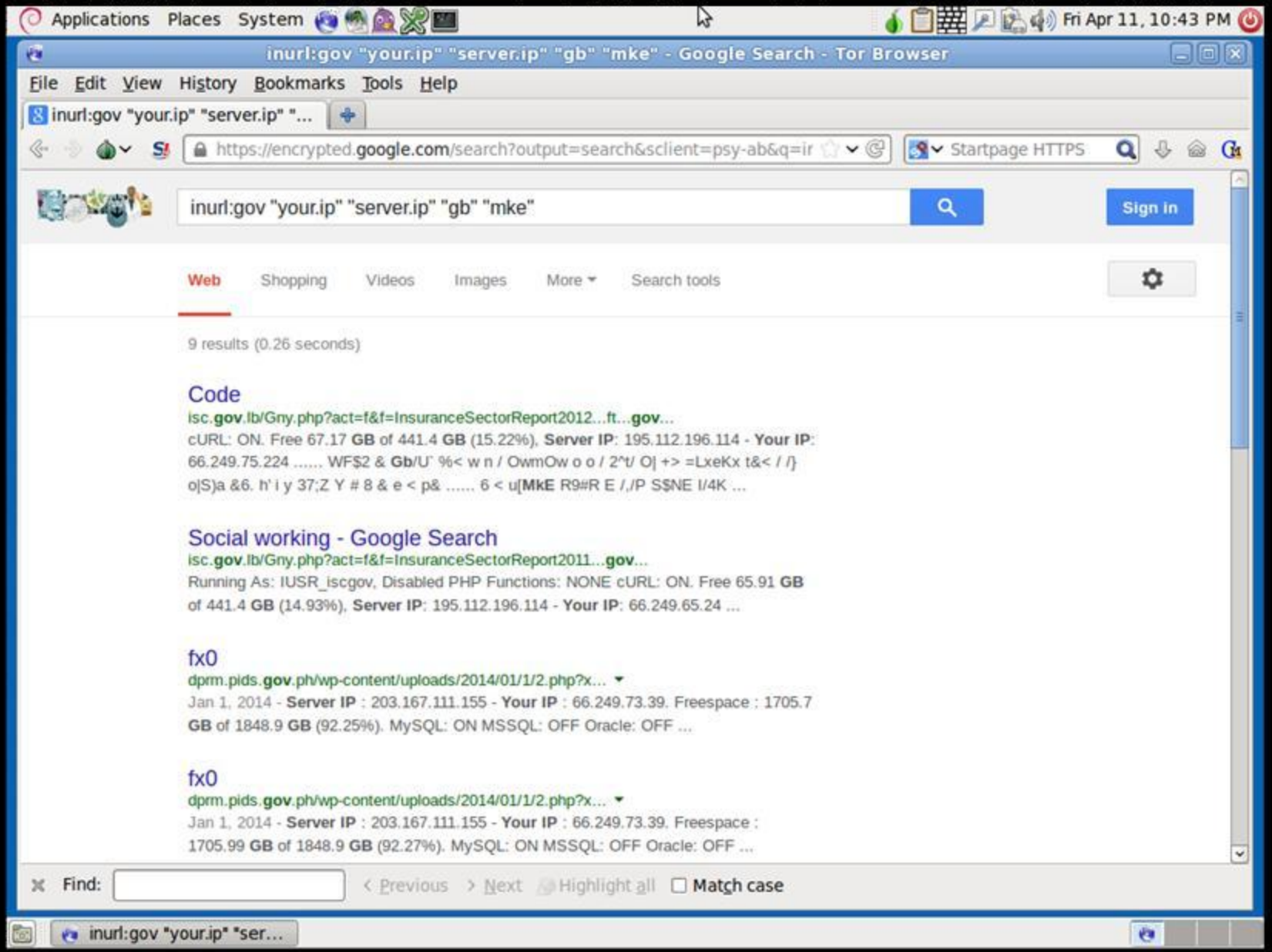

Specificando il paese

# THE DORK SIDE OF GOOGLE



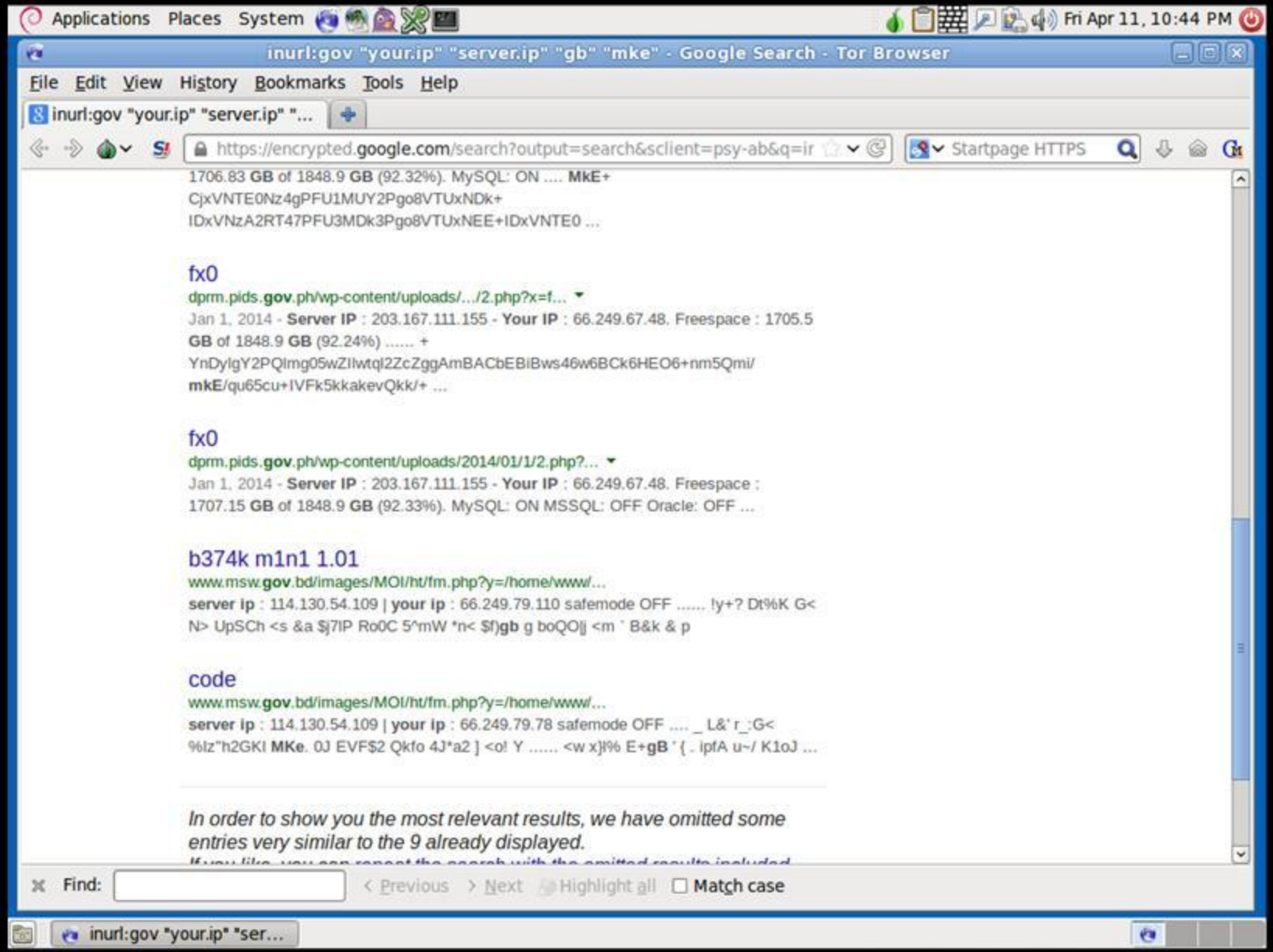

VIETNAM

# THE DORK SIDE OF GOOGLE




Aggiungendo parole chiave

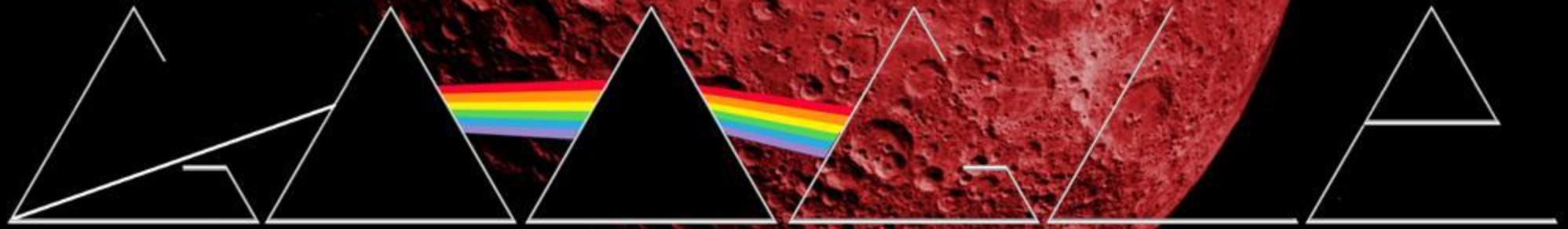
# THE DORK SIDE OF GOOGLE




BANGLADESH

# THE DORK

## SIDE OF

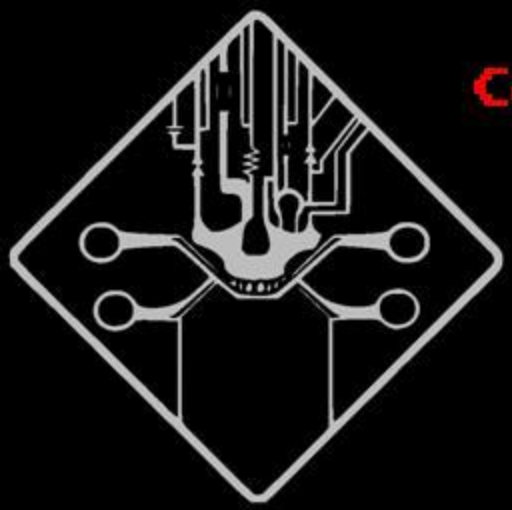


## COME OTTENERE LE PAGINE GIALLE DELLE

## shell governative

# THE DORK SIDE OF GOOGLE

## DOMANDE?



## Contatti:


epto: epto@mes3hacklab.org
b3rito: b3rito@mes3hacklab.org
klez: klez@mes3hacklab.org

Site: http://mes3hacklab.org