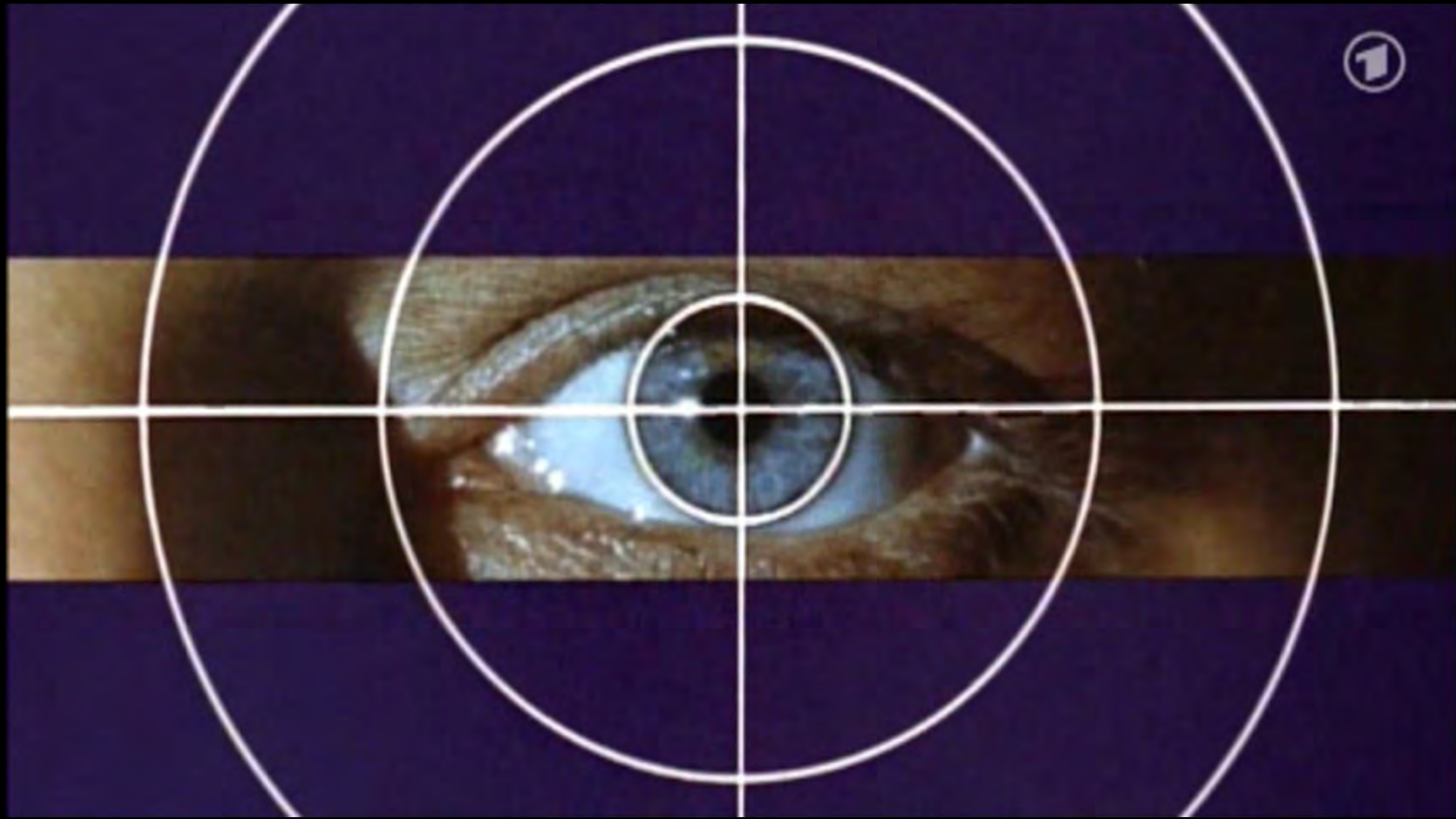
The background of the slide features a stylized, grayscale circuit board pattern. It consists of various geometric shapes, lines, and circular nodes, resembling a printed circuit board (PCB) layout. The pattern is symmetrical and repeats across the width of the slide.

NinjaTV - Increasing Your Smart TV's IQ Without Bricking It

Felix Leder

D



About Myself

- Passion:
 - Reverse Engineering (+ tool development)
 - Being out in the snow, being out on a bike, being out in the water
- Fun Projects:
 - Bug hunting in malware
 - Botnet takeovers and countermeasure
 - The Honeynet Project
- \$\$\$ Job:
 - Mobile Threat Research @ Blue Coat Norway



Credits

nSense

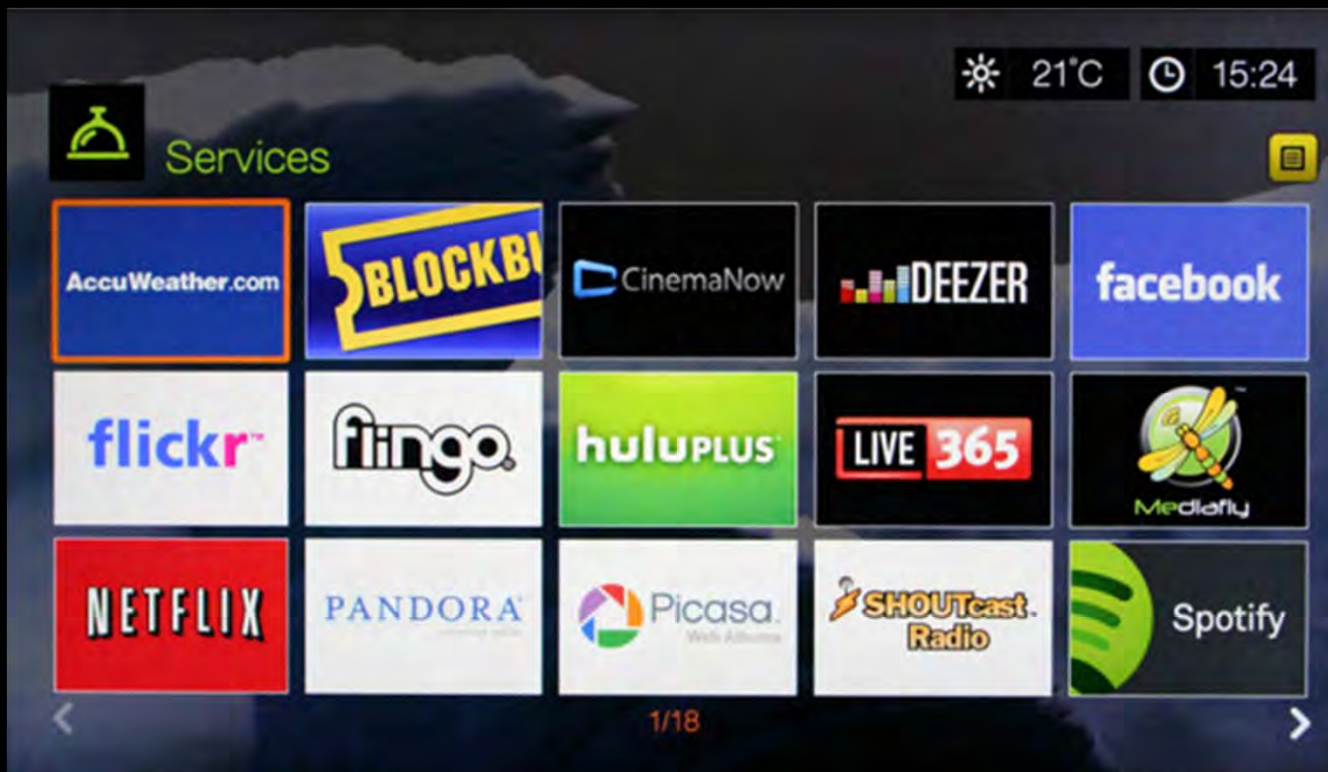
Western Digital TV (Live Hub)



Inside



Motivation to get other TV stations




Offline Analysis 1

Drive Investigation

- WDTVPriv partition
 - Hauppauge TV app storage
 - Spotify offline storage
 - Last update pkg
- WDTVLiveHub
 - Main media
- Swap



Offline Analysis 2 Updates



WD TV Live Hub Media Center

Product Update

We're pleased to offer the following updates for your WD TV Live Hub Media Center. Updating your media center is simple. Just follow the instructions below, grab your remote and enjoy the show!

What's in this update? Release 3.12.13 (7/23/2013)

- Supports Creepster Channel
- Supports euronews
- Supports MLB.TV closed captioning
- Resolved AccuWeather weekend forecast not displaying the full weekend

[Download Now](#)

[Release Notes](#)

[User Manual](#)

[Product Info](#)

[WD Community](#)

Update contents

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
wdtvlivehub.bi2	48 066 624	47 916 096	BI2 File	16.07.2013 10:31	D1F6200A
wdtvlivehub.bin	94 881 840	94 428 174	VLC media file (.bin)	16.07.2013 10:31	CD50B969
wdtvlivehub.fff	11 599 872	4 521 100	FFF File	16.07.2013 10:30	5FEB976C
wdtvlivehub.info	2 816	940	INFO File	23.07.2013 11:43	B8CA25AA
wdtvlivehub.ver	102	79	VER File	16.07.2013 10:30	1D41F2AB

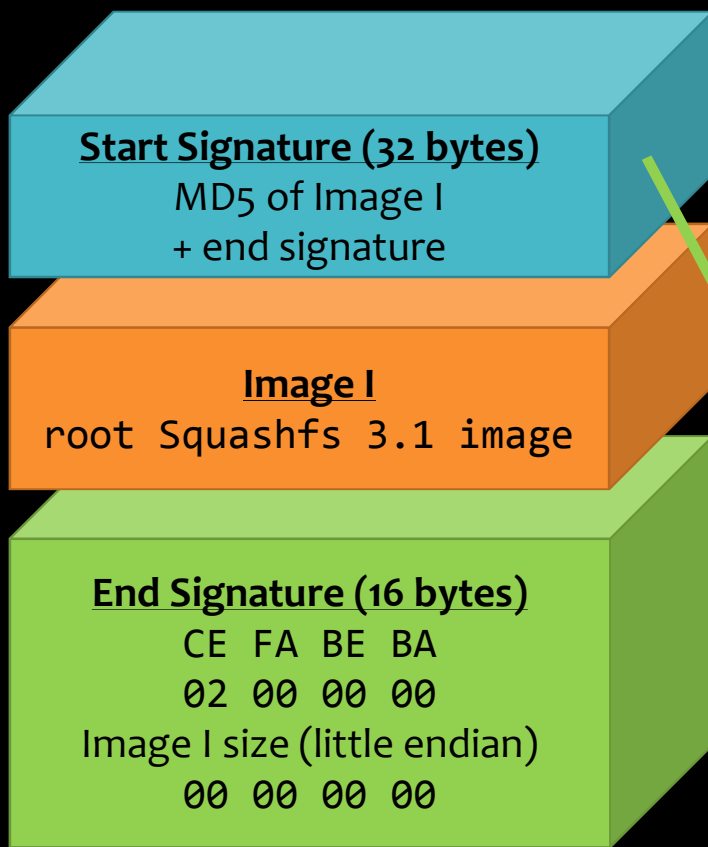
```
felix@xxx:~$ binwalk wdtvlivehub.bin
```

```
-----  
DECIMAL          HEX          DESCRIPTION  
-----  
32              0x20        Squashfs filesystem, little endian, version 3.1,  
size: 94877984 bytes, 6913 inodes, blocksize: 131072 bytes, created: Tue Jul 16  
05:17:54 2013
```

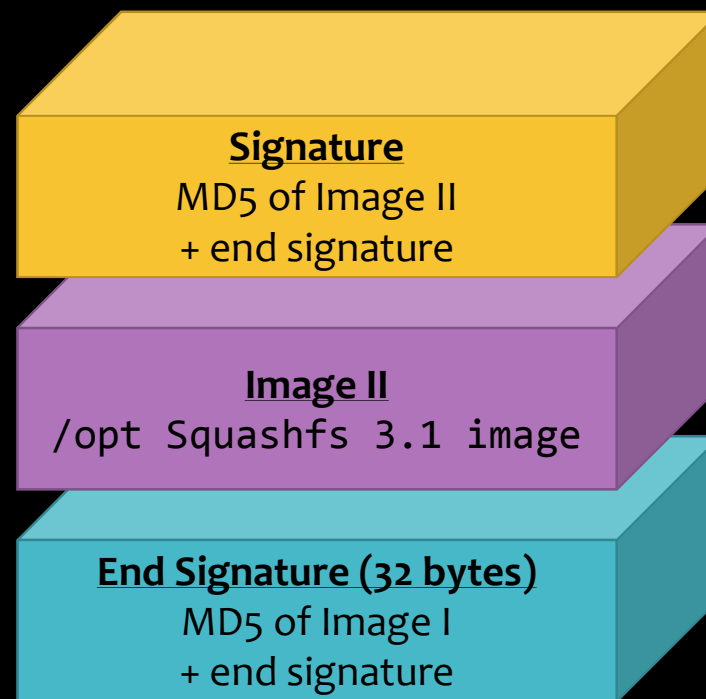
```
00000000  63 34 32 63 35 34 61 63 32 66 38 33 34 32 66 66 | c42c54ac2f8342ff |  
00000010  38 31 36 65 36 36 65 64 36 64 39 38 38 33 31 30 | 816e66ed6d988310 |  
00000020  68 73 71 73 01 1b 00 00 00 00 00 00 00 00 00 00 | hsqs..... |  
00000030  00 00 00 00 00 00 00 00 00 00 00 00 03 00 01 00 | ..... |  
00000040  00 00 11 00 e0 01 00 62 bb e4 51 b4 1b 06 08 01 | .....b..Q..... |
```

Firmware signatures

wdtvlivehub.bin



wdtvlivehub.bi2



Update contents 2

Wdtvlivehub.bin

bin	01.03.2014 11:55	File folder	
conf_src	01.03.2014 11:58	File folder	
dev	01.03.2014 12:00	File folder	
etc	01.03.2014 11:55	File folder	
home	01.03.2014 11:56	File folder	
lib	01.03.2014 11:56	File folder	
mnt	01.03.2014 11:55	File folder	
opt	01.03.2014 11:55	File folder	
osd	01.03.2014 11:58	File folder	
proc	01.03.2014 11:55	File folder	
sbin	01.03.2014 12:00	File folder	
sys	01.03.2014 11:55	File folder	
tmp	01.03.2014 11:55	File folder	
usr	01.03.2014 11:56	File folder	
var	01.03.2014 11:56	File folder	
#sysconfig#	01.03.2014 11:56	File	1 KB
init	01.03.2014 12:00	File	9 KB
md5sum.txt	01.03.2014 12:00	Text Document	176 KB
sysconfig	01.03.2014 11:55	File	1 KB

Wdtvlivehub.biz

- /opt mounted

bin	01.03.2014 12:13
game	01.03.2014 12:14
include	01.03.2014 12:14
lib	01.03.2014 12:14
qt	01.03.2014 12:14
share	01.03.2014 12:13
swf	01.03.2014 12:13
twky	01.03.2014 12:13
webserver	01.03.2014 12:13
sysconfig	01.03.2014 12:13

Which way in?



Vulnerability Finding

Login

Password

Language

English

I accept [END USER LICENS](#)

Keep me signed in

- System
- Remote
- Media
- Online
- RSS

- System
- Remote
- Media
- Online
- RSS
- Support

Let us help you

Control Your WD TV
Control your WD TV from your web browser or smart phone

Open in a separate window

Admin Password | Date & Time | Storage Status | Network Infomation | Device Name

Old Password:

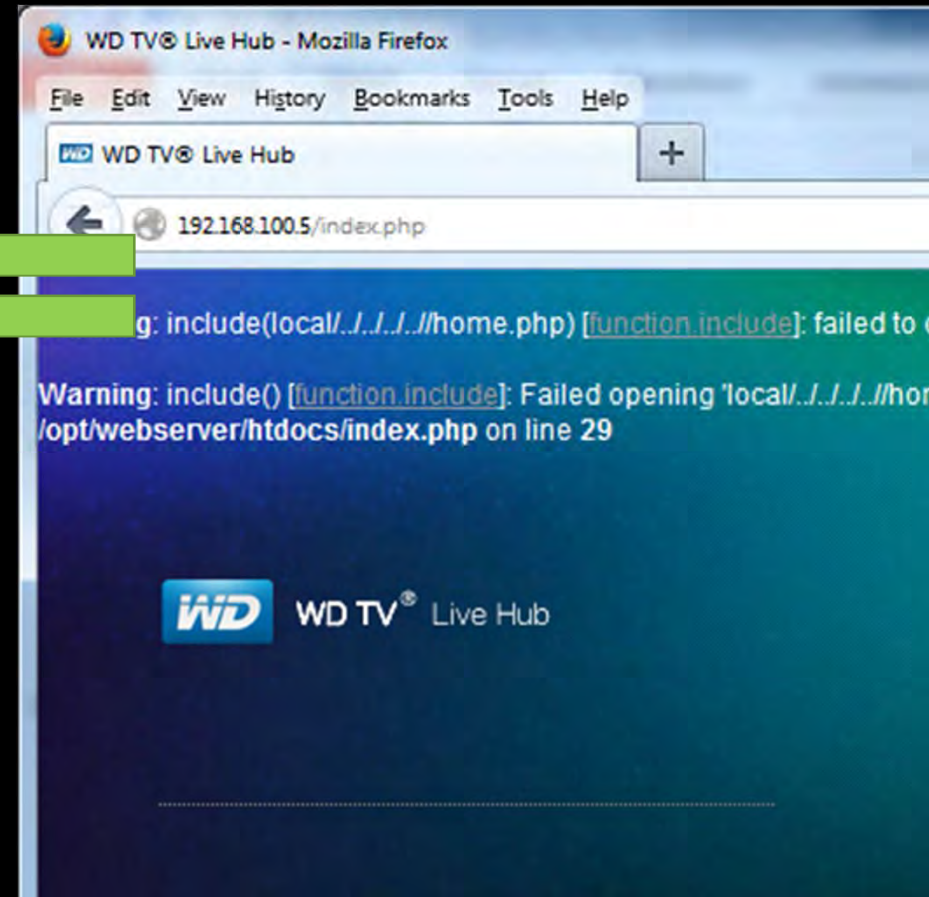
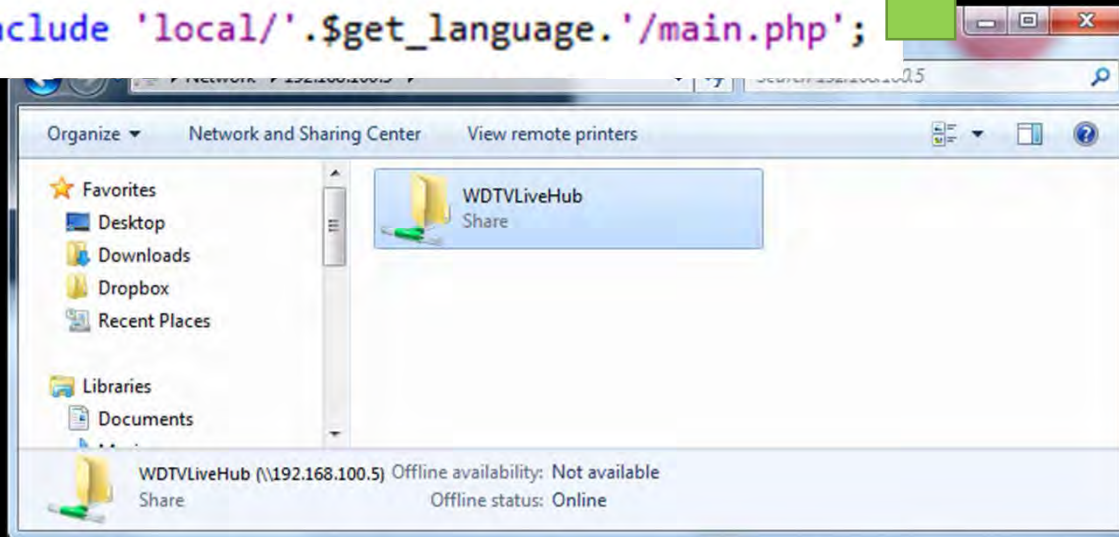
New Password:

Confirm Password:

Vulnerability finding

RFI - remote file inclusion

```
$get_language=$_SESSION['lang_id'];  
  
if($get_language==''){  
    $get_language=0;  
}  
include 'local/.'.$get_language.'/main.php';
```



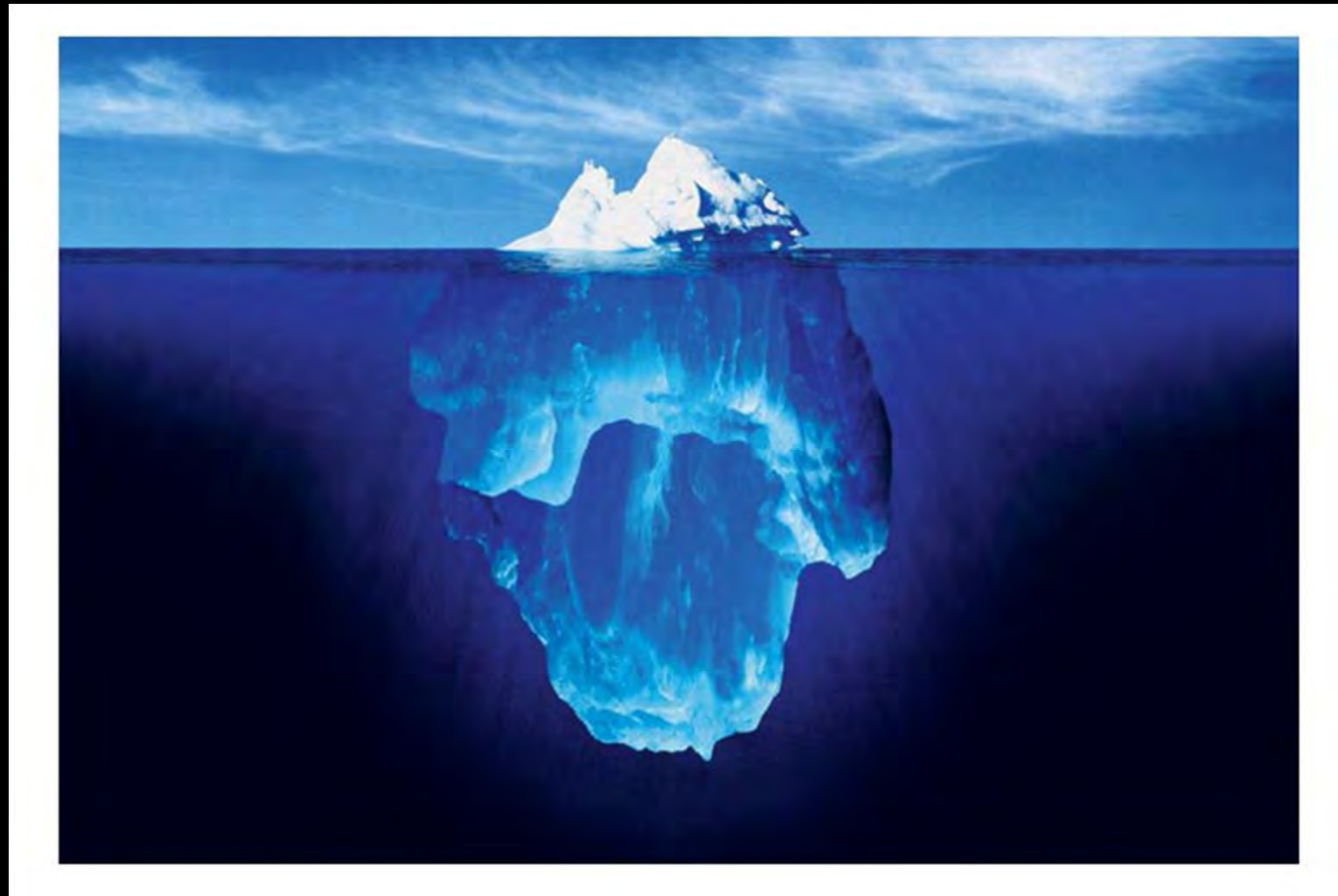
Where to place my PHP shell?

Investigating more files:

- `/tmp/media/usb/Local/WDTV LiveHub/` is root of SMB share
- So my videos are in `/tmp/media/usb/Local/WDTV LiveHub/Videos/`

Name	Size	Modify	Owner/Group	Permissions	Actions
[..]	dir	2013-07-16 03:14:48	1007/1007	drwxrwxr-x	RT
[api]	dir	2013-07-16 03:14:48	1007/1007	drwxrwxr-x	RT
[DB]	dir	2013-07-16 03:14:48	1007/1007	drwxrwxr-x	RT
[image]	link	2013-07-16 03:14:49	1007/1007	drwxrwxr-x	RT
[js]	dir	2013-07-16 03:14:48	1007/1007	drwxrwxr-x	RT
[local]	dir	2013-07-16 03:14:48	1007/1007	drwxrwxr-x	RT
[tmp]	dir	2013-07-16 03:14:48	1007/1007	drwxrwxr-x	RT
[user]	link	2013-12-12 20:34:46	root/root	drwxrwxrwx	RT
[wd_nas]	dir	2013-07-16 03:14:48	1007/1007	drwxrwxr-x	RT
[wdtvlivehub]	dir	2013-07-16 03:14:48	1007/1007	drwxrwxr-x	RT
[whatson]	dir	2013-07-16 03:14:48	1007/1007	drwxrwxr-x	RT
device_name.php	1.36 KB	2013-06-24 02:44:47	1007/1007	-rw-rw-r--	RTED
favicon.ico	1.37 KB	2013-06-24 02:44:47	1007/1007	-rw-rw-r--	RTED
file_exists.php	95 B	2013-06-24 02:44:47	1007/1007	-rw-rw-r--	RTED
index.html	44 B	2004-11-20 20:16:24	1007/1007	-rw-r--r--	RTED
index.php	8.18 KB	2013-06-24 02:44:47	1007/1007	-rw-rw-r--	RTED
madia_itune.php	2.25 KB	2013-06-24 02:44:47	1007/1007	-rw-rw-r--	RTED
madia_twonky.php	2.68 KB	2013-06-24 02:44:47	1007/1007	-rw-rw-r--	RTED
Main.php	27.16 KB	2013-06-24 02:44:47	1007/1007	-rw-rw-r--	RTED

That was only the beginning...



Uname: Linux WDTVLiveHub 2.6.22.19-29-4 #5 PREEMPT Tue Jul 16 11:16:34 CST
User: 0 (root) **Group:** 0 (root)
Php: 5.2.17 **Safe mode:** OFF [phpinfo] **Datetime:** 2014-03-01 13:22:04
Hdd: 45.88 MB **Free:** 0 B (0%)
Cwd: /opt/webserver/htdocs/ drwxrwxr-x [home]

[Sec. Info] [Files] [Console] [Sql] [Php]

Console

List dir [>>] [se]

```
$
```

Change dir:

/opt/webserver/htdocs/ [>>]

Make dir: (Not writable)

[>>]

Execute:

telnetd -l /bin/sh [>>]

Telnet 192.168.100.5

```
BusyBox v1.10.0 (2013-06-21 20:40:53 CST) built-in  
Enter 'help' for a list of built-in commands.  
  
/tmp/media/usb/Local/WDTULiveHub # id  
uid=0(root) gid=0(root)  
/tmp/media/usb/Local/WDTULiveHub #
```

➔ Webservice running as **root = woot**

Must remember low hanging fruits...

```
/opt/webserver/htdocs # ls -l
```

```
...
```

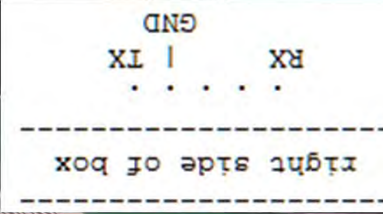
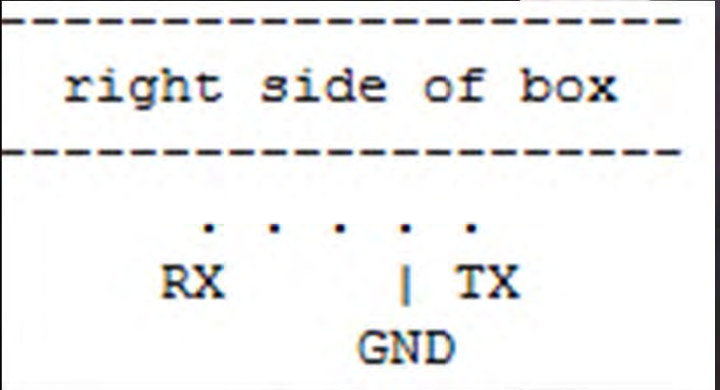
```
-rw-rw-r-- 1 1007 1007 1685 Jun 24 2013 system_password.php
-rw-rw-r-- 1 1007 1007 142 Jun 24 2013 test.php
drwxrwxr-x 3 1007 1007 21 Jul 16 2013 tmp
lrwxrwxrwx 1 1007 1007 32 Dec 12 08:15 user -> /tmp/media/usb/Local/WDTVLiveHub
drwxrwxr-x 8 1007 1007 298 Jul 16 2013 wd_nas
drwxrwxr-x 3 1007 1007 23 Jul 16 2013 wdtvlivehub
drwxrwxr-x 2 1007 1007 102 Jul 16 2013 whatson
```



Approach for HW hackers

D

Looking for interesting pins



Warning: 3.3 Volts

Booting up

```
*****
* SMP86xx zboot start ...
* Version: 3.1.0
* Started at 0xd00ee720.
* Configurations (chip revision: 1):
*   Enabled checkpoints.
*****
```

```
SYSCONF_FIRMWARE_MTD_PARTITION = /dev/sigmblockh
FW_SIGN = okok
=====
===== Boot from /dev/sigmblockh =====
=====
Mounting application firmware...
Application firmware mounted..
Check the authentication of whole file..
random_number = 7
256+0 records in
256+0 records out
File /dev/sigmblockh authenticated
All files have been checked for their integrity...
Launch application firmware...
=====ROOTFS=====
export SYSCONF_BUILD_DATE=2013.07.16-1106
export SYSCONF_BUILD_VERSION=3.12.13
export SYSCONF_NAND_DRIVER=LEGACY
export SYSCONF_FIRMWARE_BIN=wdtvlivehub.bin
export SYSCONF_FIRMWARE_VER=wdtvlivehub.ver
export SYSCONF_BOOTLOADER_MTD_PARTITION=/dev/sigmblockh
export SYSCONF_KERNEL_MTD_PARTITION=/dev/sigmblockd
export SYSCONF_FIRMWARE_MTD_PARTITION=/dev/sigmblockh
export SYSCONF_FIRMWARE_MTD_SIZE=96468992
export SYSCONF_LAST_PARTITION_NODE_NAME=/dev/sigmblockl
export SYSCONF_STATIC_CONFIG_MOUNT_POINT=/tmp/static_config
export SYSCONF_PRODUCT_EXT_WDTV_RV=y
export SYSCONF_MOUNT_LOCAL_SATA_DRIVE=y
export IS_DTS=y
export IS_DTCP=n
export SYSCONF_ROOTFS2=y
export SYSCONF_ROOTFS2_DEVICE=/dev/sigmblocki
export SYSCONF_ROOTFS2_PATH=/opt
=====
```

```
=====PRIMARY SYSTEM=====
export SYSCONF_BUILD_DATE=2013.07.16-1106
export SYSCONF_BUILD_VERSION=3.12.13
export SYSCONF_NAND_DRIVER=LEGACY
export SYSCONF_FIRMWARE_BIN=wdtvlivehub.bin
export SYSCONF_FIRMWARE_VER=wdtvlivehub.ver
export SYSCONF_BOOTLOADER_MTD_PARTITION=/dev/sigmblockh
CS 0 vendor id 0xec.....
ION=/dev/sigmblockh CS 0 device id 0xda.....
cka
export SYSCONF_KERNEL_MTD_PARTITION=/dev/sigmblockd
export SYSCONF_FIRMWARE_MTD_PARTITION=/dev/sigmblockh
export SYSCONF_FIRMWARE_MTD_SIZE=96468992
export SYSCONF_BOOTLOADER_AUTH=y
export SYSCONF_FIRMWARE_FS=squashfs
=====
Primary built date: 2013.07.16-1106.
```


End of boot

41fa4f6ac0b8ebdefb89d443cb6c5ece login:

- What is the password?

```
/etc # cat /tmp/shadow.conf
root:Be1Ua5fK12N76:10933:0:99999:7:::
bin:*:10933:0:99999:7:::
daemon:*:10933:0:99999:7:::
adm:*:10933:0:99999:7:::
lp:*:10933:0:99999:7:::
sync:*:10933:0:99999:7:::
shutdown:*:10933:0:99999:7:::
halt:*:10933:0:99999:7:::
uucp:*:10933:0:99999:7:::
operator:*:10933:0:99999:7:::
nobody:*:10933:0:99999:7:::
default::10933:0:99999:7:::
/etc # ls -l /etc/shadow
lrwxrwxrwx    1 1007    1007    16 Jul 16 2013 /etc/shadow -> /tmp/shadow.conf
```

```
firmware reload successful
Loaded xenpv2 file, xenpv2size = 268
Password for 'root' changed
insmod: cannot insert '/lib/modules/irkernel.ko': Device
insmod: cannot insert '/lib/modules/irkernel.ko': Device
insmod: cannot insert '/lib/modules/thermal_g751.ko': Ope
insmod: cannot insert '/lib/modules/wdtv_rv_microp.ko': D
insmod: cannot insert '/lib/modules/wdtv_rv_microp.ko': D
insmod: cannot insert '/lib/modules/wdtv rv microp.ko': D
```

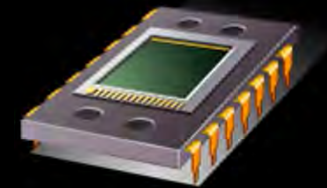
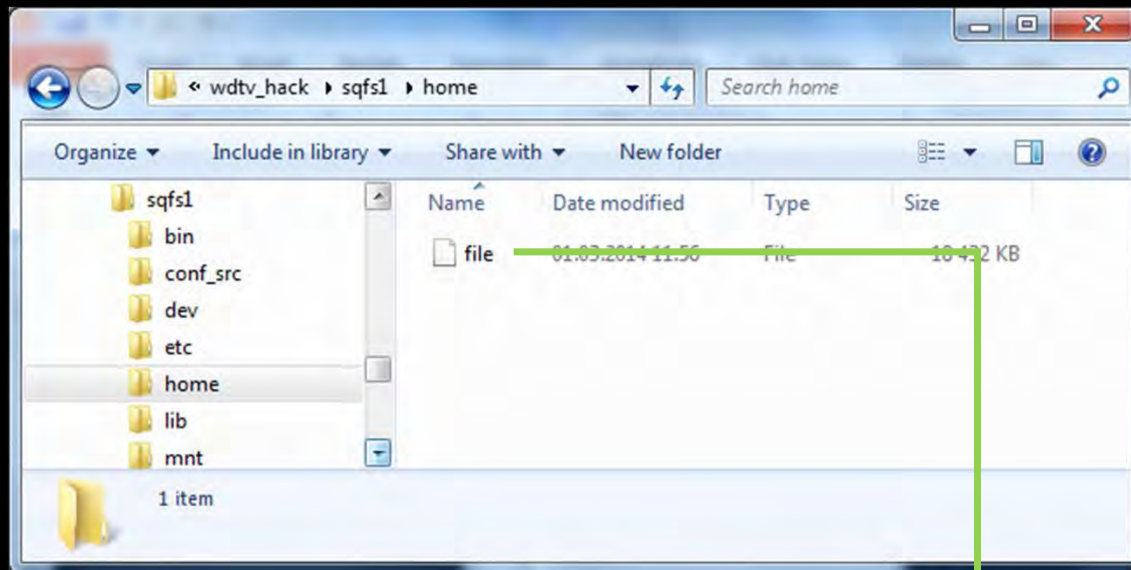
Reverse Engineering the boot process (parts of it)

- Password is set by a tool called `gbus_read_serial_num`
- Located in `/usr/local/sbin` (encrypted file system image)
- Original: `/home/file` AES encrypted
- AES key to mount this image retrieved from ROM during boot
- Not visible in raw update bins

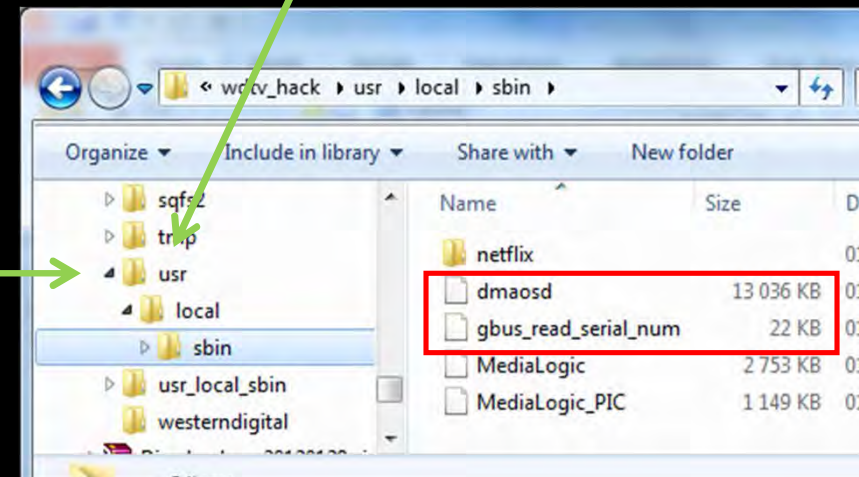
```
if [ -f /bin/init_3 ]; then
    /bin/init_3
fi
gbus_read_serial_num
ln -s /dev/ir /dev/irda
echo "/sbin/modprobe -q" > /proc/sys/kernel/modprobe
```

```
gbus_read_bin_to_file 0x61d00 0x280 /tmp/xosinfo && genxenv2 g /tmp/xosinfo bc01 \
| sed 's/.*.bc01\(.*\)/\1/g' | sed 's/\ //g' > /tmp/log1 2>&1
echo `cat /tmp/log1` | mymount /home/file /usr/local/sbin -oencryption=aes -p 0
```

Visual



AES Key



What's the root password?

- RE `gbus_read_serial_num`

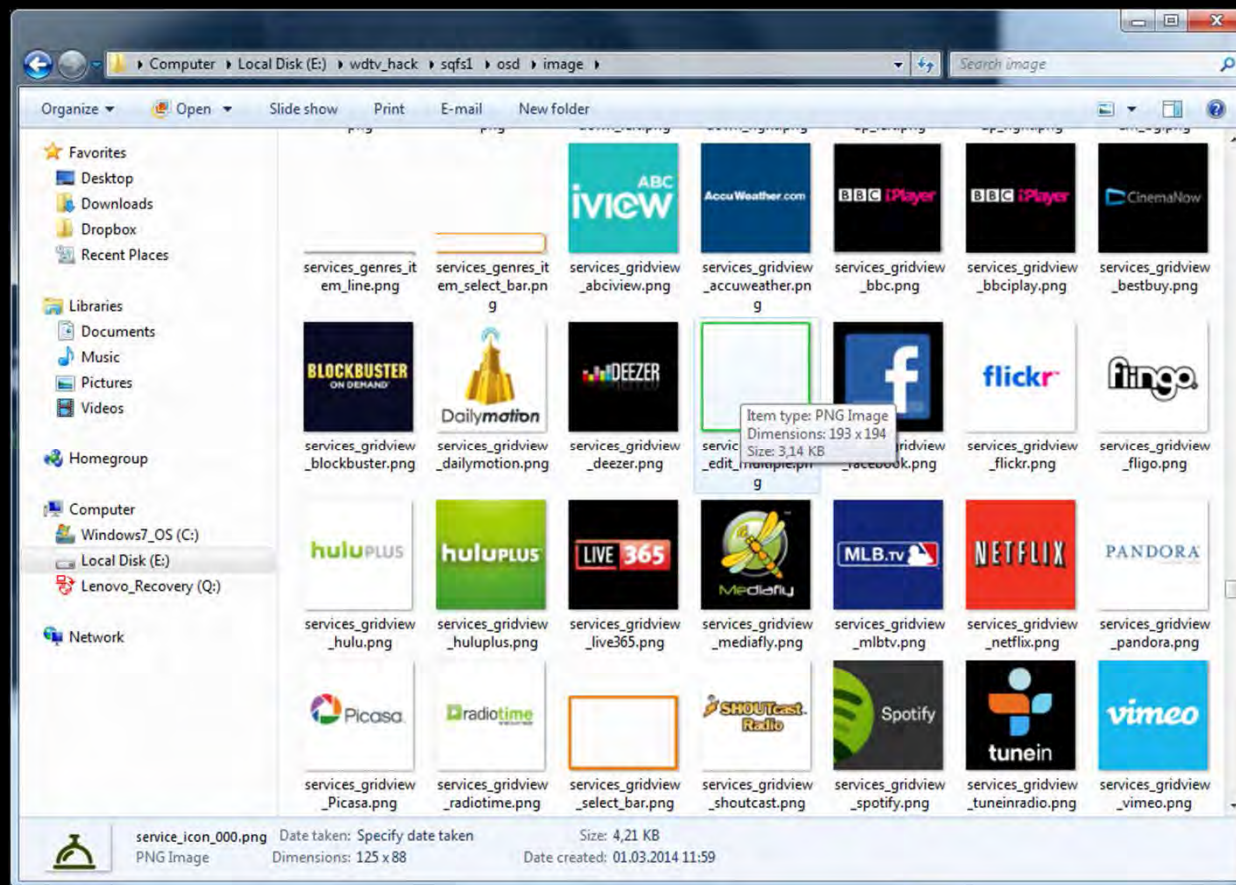
```
['s'] .rodata:004046... 00000026 C   %s: Error: %s must be multiple of %d\n
['s'] .rodata:004046... 0000003C C   Error: %s: %s must be decimal, octal or hexadecimal
['s'] .rodata:004046... 00000065 C   Error: %s: the environment variable %s not set co
['s'] .
['s'] echo $SERIALNUMBER | md5sum
['s'] .rodata:004045... 0000002F C   echo -n \root:%s\ | cut -d ' ' -f 1 | chpasswd
['s'] .rodata:004045. 41fa4f6ac0b8ebdefb89d443cb6c5ece login: root
['s'] .rodata:004045. Password: <MD5SUM_OF_^^>
['s'] .rodata:004045.
['s'] .rodata:004045.
['s'] .rodata:004045. BusyBox v1.10.0 (2013-06-21 20:40:53 CST) built-in shell
['s'] .rodata:004045. (ash)
Enter 'help' for a list of built-in commands.

#
```

Where are the Apps?

Many traces on disk

- Logos for all services
- Libraries and DRM files for some
 - Spotify
 - Netflix
 - ...
- NO Apps for e.g. redbull.tv, AOL, Bild.de



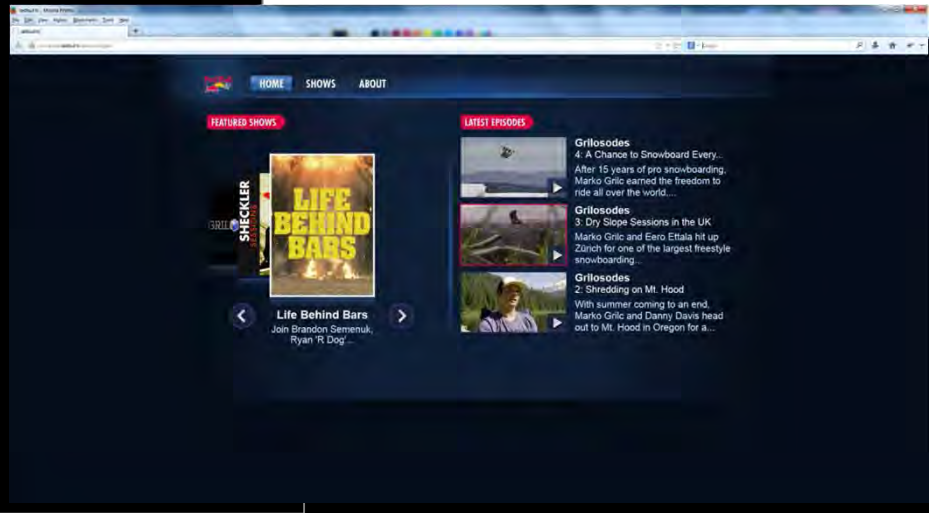
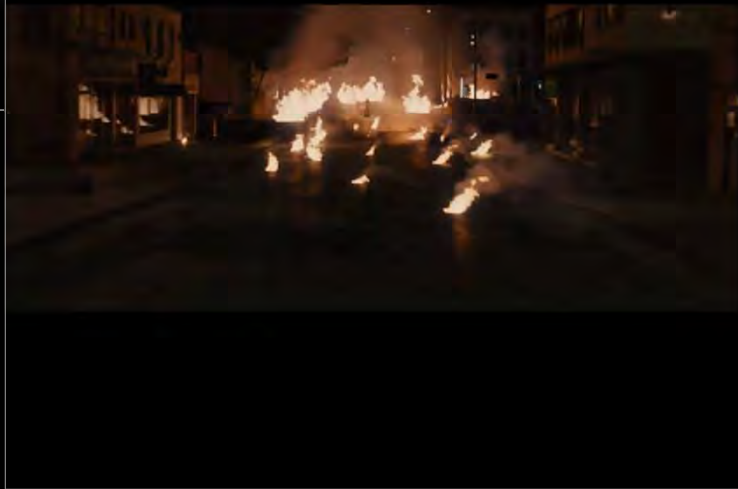
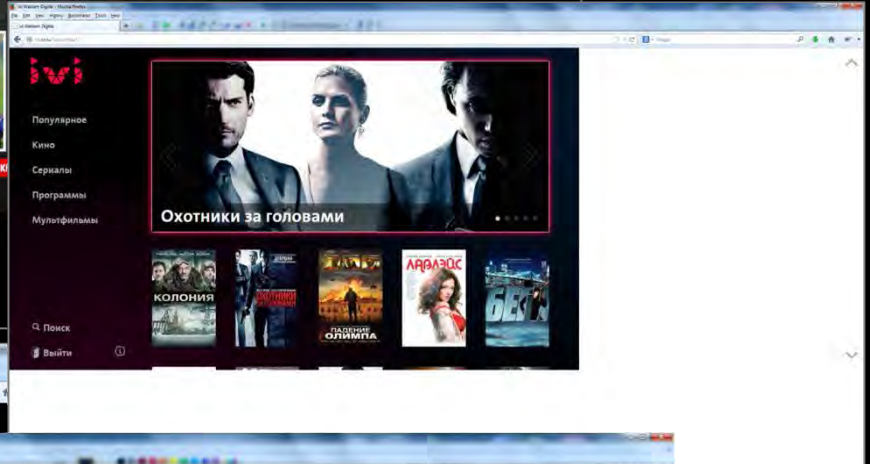
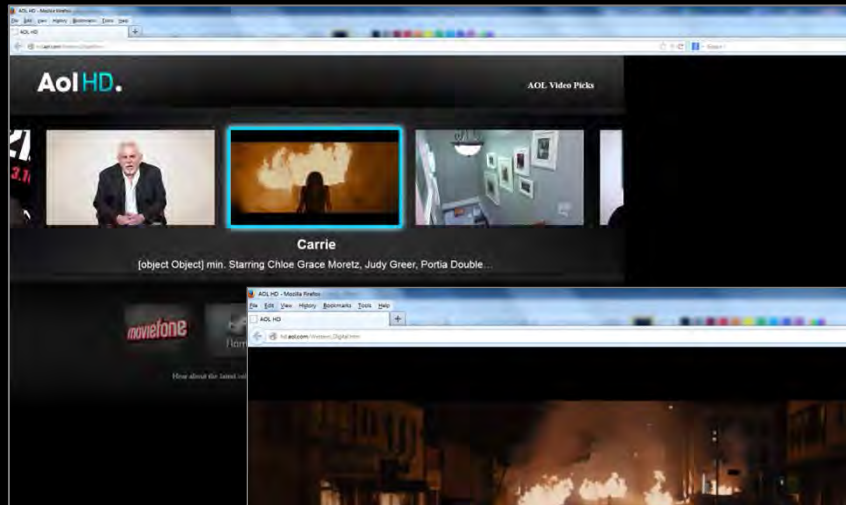
DMAOSD – the heart of WD TV

- Last process started
- System automatically reboots after process dies (e.g. is killed)
- Located in the encrypted partition
- Uses 75% of available RAM

```
.rodata:00DCF284 aHttpHd_aol_com:.ascii "http://hd.aol.com/Western_Digital.htm"<0>
.rodata:00DCF284                                     # DATA XREF: start_video_app_guess+7C0↑o
.rodata:00DCF2AA                                     .align 2
.rodata:00DCF2AC aHttpConnected_:.ascii "http://connected.redbull.tv/westerndigital/"<0>
.rodata:00DCF2AC                                     # DATA XREF: start_video_app_guess+800↑o
.rodata:00DCF2D8 aHttpJson_bild_:.ascii "http://json.bild.de/tv/index_1280.html"<0>
.rodata:00DCF2D8                                     # DATA XREF: start_video_app_guess+840↑o
```

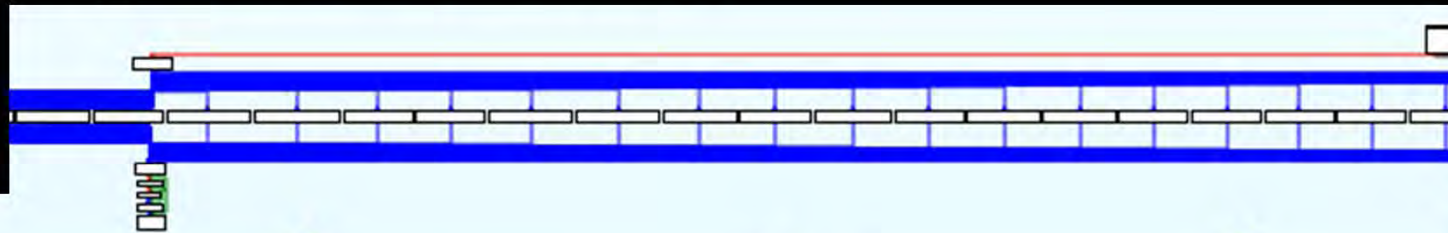
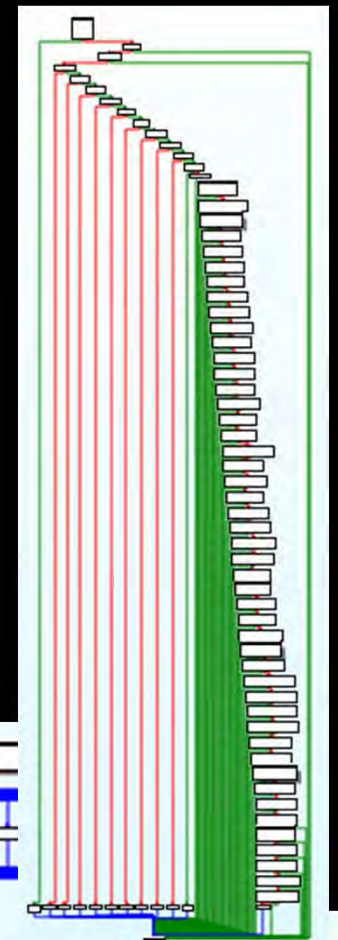
M

Services



Service details

- On first connection WD TV uses GeoIP to determine country
- Some services are country specific (e.g. bild.de, ivi.ru)
- Pure web-pages
- Others use pipes to connect to local binaries/libraries (e.g. spotify)
- Crazy jump tables and if- statements



```
loc_712FA0:          # jumtable 00712D94 case 58
lui     $v0, 0xDD
j      loc_7130E8
addiu  $a0, $v0, (aAol_hd_server_ - 0xDD0000) # "AOL_HD_SERVER_HANDLE"
```

```
loc_712FAC:          # jumtable 00712D94 case 59
lui     $v0, 0xDD
j      loc_7130E8
addiu  $a0, $v0, (aRed_bull_tv_se - 0xDD0000) # "RED_BULL_TV_SERVER_HANDLE"
```

```
loc_712FAD:          # jumtable 00712D94 case 60
lui     $v0, 0xDD
j      loc_7130E8
addiu  $a0, $v0, (aRed_bull_tv_se - 0xDD0000) # "RED_BULL_TV_SERVER_HANDLE"
```

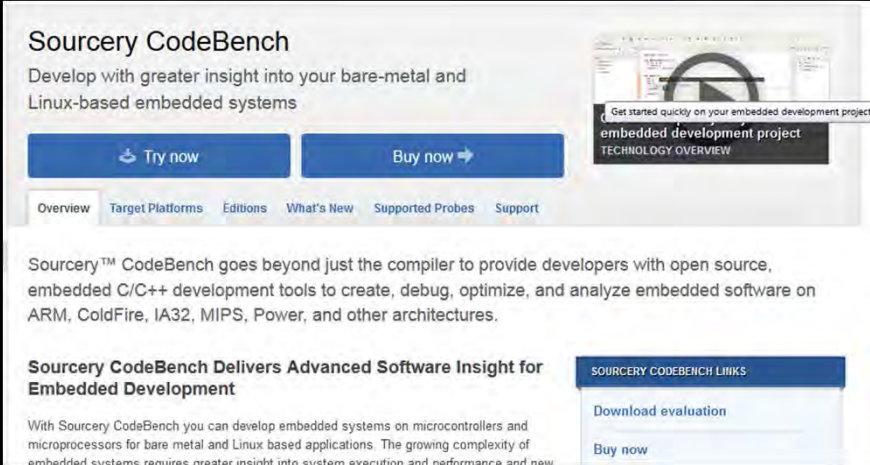
Dmaosd – all in one

- 13 MB (huuge executable for MIPS – even for x86)
- Everything statically linked in
 - QT webbrowser to access the web “services”
 - Libraries for HDMI and codec chips
 - Auto-mounts attached USB sticks, built-in harddrive
 - Controls network shares
 - Update daemon
- Renderer for XML based menus
- Loads all resources (templates, pictures, ...) into it's process space

Debugging Dmaosd live – get GDB up

Step 1: GDBServer on device

- Compile chain for MIPS → create GDBServer
 - <http://www.mentor.com/embedded-software/sourcery-tools/sourcery-codebench/overview/>
 - LSB, software floating point, shared libraries (COMPILEKIND=glibc,softfloat mipsel-linux-gcc -o test.mips test.c)
- Copy GDBServer executable on device



The screenshot shows the Sourcery CodeBench website. The main heading is "Sourcery CodeBench" with the tagline "Develop with greater insight into your bare-metal and Linux-based embedded systems". There are two prominent buttons: "Try now" and "Buy now". Below this is a navigation menu with links for "Overview", "Target Platforms", "Editions", "What's New", "Supported Probes", and "Support". The main content area features a paragraph describing the tool's capabilities for various architectures. A sidebar on the right contains a "TECHNOLOGY OVERVIEW" section with a "Download evaluation" button and a "Buy now" button.

Sourcery CodeBench
Develop with greater insight into your bare-metal and Linux-based embedded systems

[Try now](#) [Buy now](#)

[Overview](#) [Target Platforms](#) [Editions](#) [What's New](#) [Supported Probes](#) [Support](#)

Sourcery™ CodeBench goes beyond just the compiler to provide developers with open source, embedded C/C++ development tools to create, debug, optimize, and analyze embedded software on ARM, ColdFire, IA32, MIPS, Power, and other architectures.

Sourcery CodeBench Delivers Advanced Software Insight for Embedded Development

With Sourcery CodeBench you can develop embedded systems on microcontrollers and microprocessors for bare metal and Linux based applications. The growing complexity of embedded systems requires greater insight into system execution and performance and new

SOURCERY CODEBENCH LINKS

[Download evaluation](#)

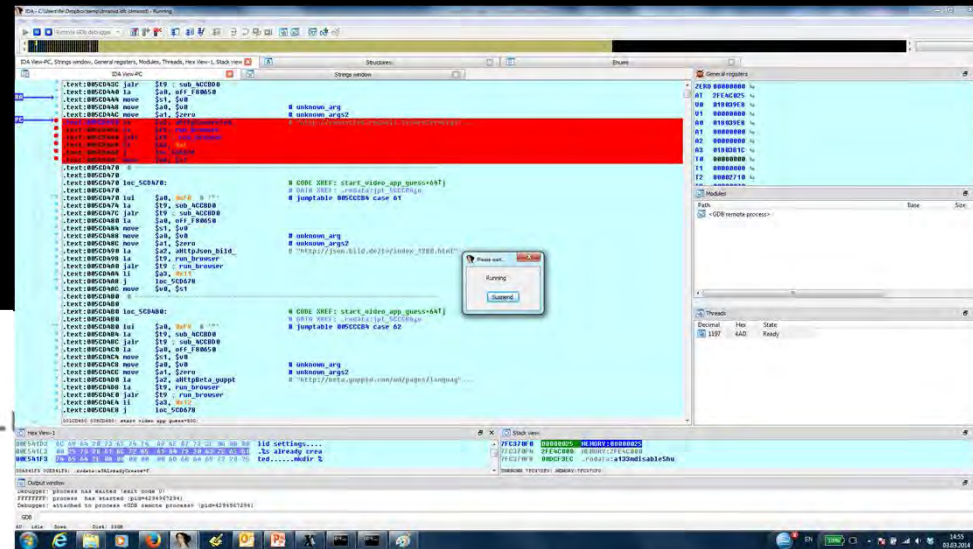
[Buy now](#)

Debugging Dmaosd- attach IDA Pro

- IDA Pro for remote debugging (alternatively MIPS gdb)
- Very sensitive / unreliable
- Don't be fooled by pipelining in assembly
- You cannot break much 😊 (more on that later)

```
move $s1, $v0
move $a0, $v0          # unknown_arg
move $a1, $zero       # unknown_args2
la $a2, aHttpJson_bild_ # "http://json.bild.de/tv/index_1280.
la $t9, run_browser
jalr $t9 ; run_browser
li $a3, 0x11
j loc_5CD678
move $v0, $s1
```

This is executed



Tatort

How to get my own services on the box?

Broadcaster “Das Erste” live stream

The screenshot shows a live stream of a ski race on the Das Erste website. The main video player displays a skier, Elena FANCHINI, on a snowy slope. The video player includes a progress bar at the bottom with a pause icon, a volume icon, and a full-screen icon. The video title is "CRANS MONTANA ABFAHRT LIVE".

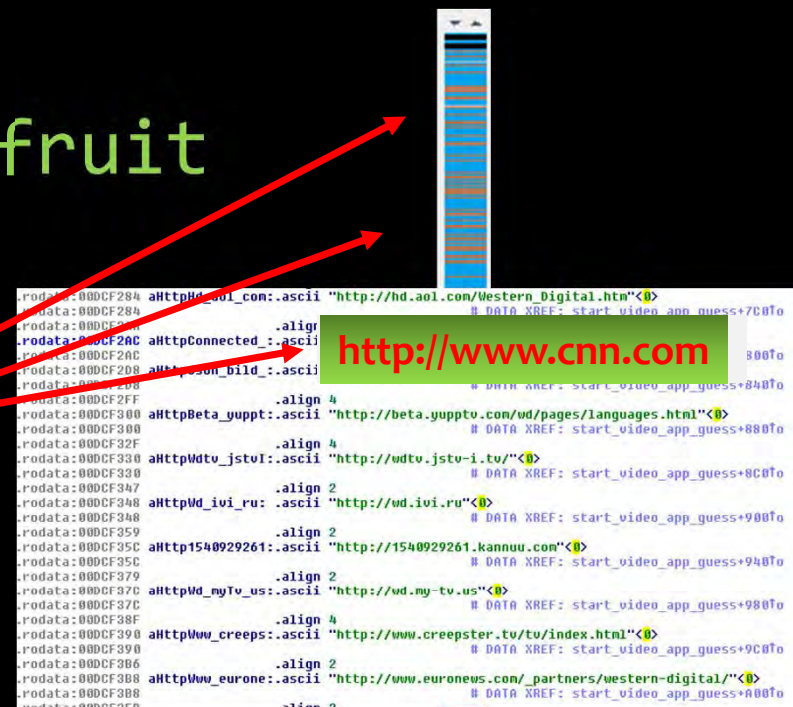
Below the video player, there is a program schedule section with the following items:

- 09:35 Sportschau live**
Weltcup Ski-Mountaineering
Reporter: Johannes Krauthaimer
Zusammenfassung aus Diablerets
[MEHR INFOS](#)
- 14:55 Tagesschau**
- 17:00 W wie Wissen**
Fledermäuse - faszinierend und bedroht
Moderation: Dennis Wilms
- 17:30 Gott und die Welt**

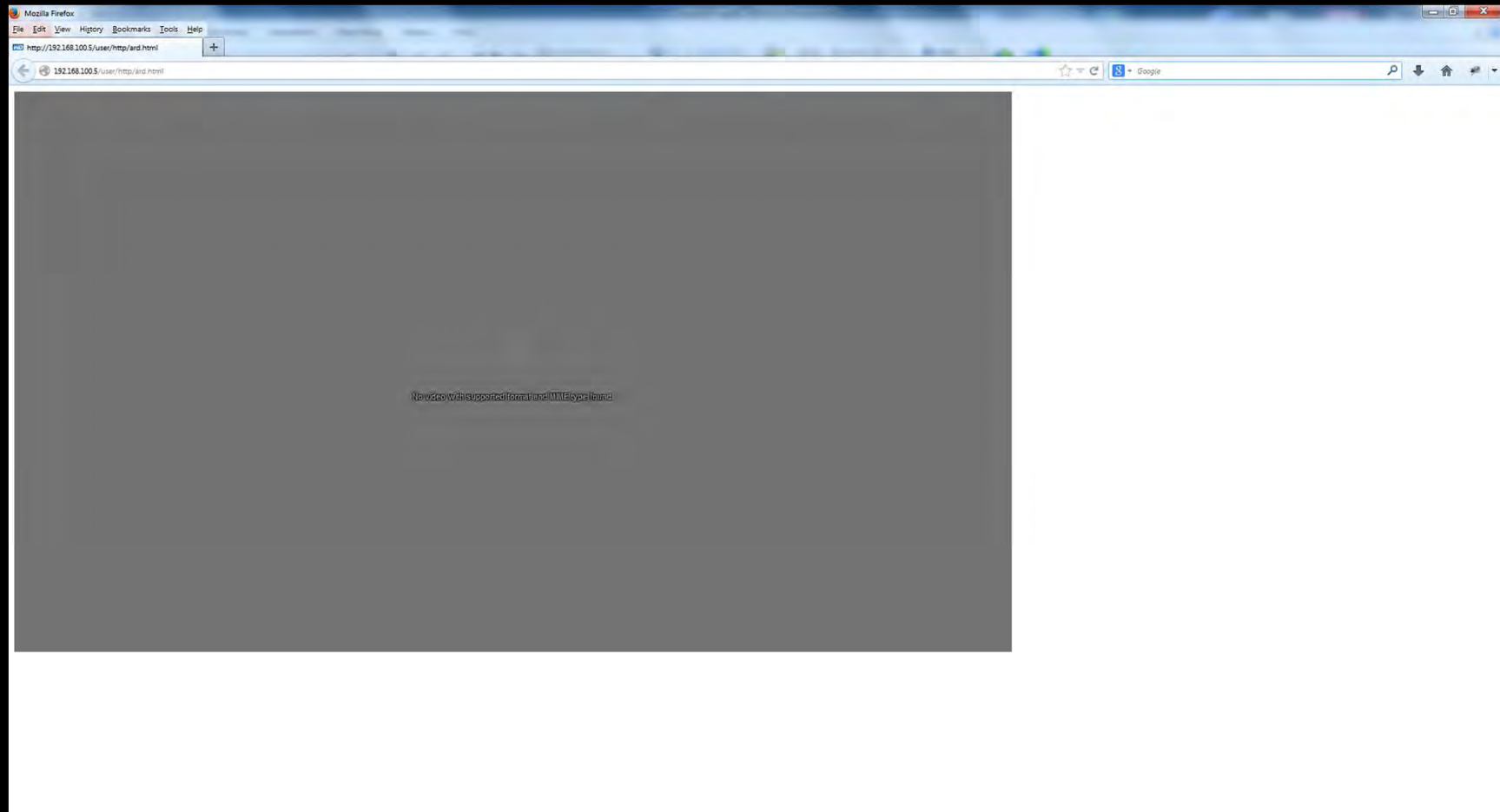
The website header includes "Das Erste® LIVE", "Das Erste® Mediathek", and "DasErste.de®". The browser address bar shows "http://www.daserste.de/ins/streams/MyProgram".

Browser – lowest hanging fruit

- QT embedded browser started
- Run – time patch the urls
- Windows: OpenProcess, WriteProcessMemory
- Linux: ptrace
 - PTRACE_ATTACH to process
 - PTRACE_PEEKDATA to search
 - PTRACE_POKEKDATA to overwrite (in place – size limit)



Supported (HW) codecs?



TV station codec has to fit

NPPVpluginDescriptionString The Totem 0.10.2 plugin handles video and audio streams

NP_GetMIMEDescription = application/acetrax:mp4, wmv, mp3:video/x-ms-wmv;video/wmv:wmv:video/wmv;video/x-ms-asf:wmv:video/x-ms-asf;application/maxdome:mp4, wmv, mp3:video/x-ms-wmv;video/wmv:wmv:video/wmv;video/x-ms-asf:wmv:video/x-ms-asf;application/sigma:mp4, wmv, mp3:video/x-ms-wmv;audio/mp3:mp3:audio/mp3;video/mp4:mp4:video/mp4;audio/mpeg:mpg:audio/mpeg;video/wmv:wmv:video/wmv;video/mpeg4:mp4:video/mpeg4;video/x-flv:flv,f4v:video/x-flv;application/x-mpegurl:m3u8:vnd.apple.mpegurl;audio/x-wav:wav:audio/wav;video/mp2t:ts:video/mp2t;application/x-netcast-av::;application/yotavideo:mp4, wmv, mp3:video/x-ms-wmv;video/wmv:wmv:video/wmv;video/x-ms-asf:wmv:video/x-ms-asf;video/vnd.ms-playready.media.pyv:pyv:video/vnd.ms-playready.media.pyv;application/nowtilus:mp4, wmv:video/x-ms-wmv;video/mpeg4:mp4:video/mpeg4

Finally 😊



Root but not 0wnd

ROM filesystem

root but not owned by me

- All persistent file systems are read-only (from ROM)
- All dynamic parts are copied over to `/tmp` (including shadow, hosts, ...)
- Fresh reset after reboot

```
# mount
```

```
...
```

```
/dev/sigmblockh on / type squashfs (ro) ← root
```

```
...
```

```
none on /tmp type tmpfs (rw)
```

```
/dev/sigmblocki on /opt type squashfs (ro)
```

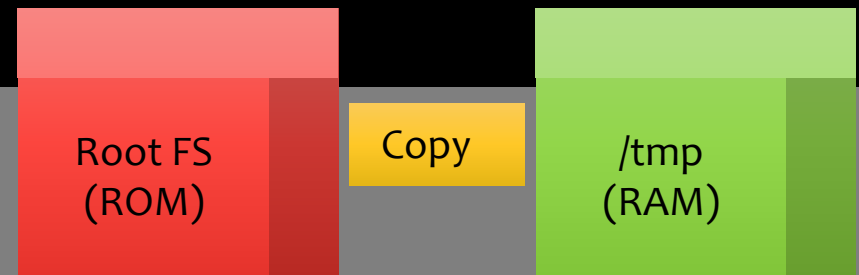
```
/dev/loop0 on /tmp/static_config type minix (rw)
```

```
/dev/loop1 on /usr/local/sbin type romfs (ro)
```

```
tmpfs on /opt/webserver/logs type tmpfs (rw)
```

```
none on /lib/sigma type ramfs (rw)
```

```
/dev/sda3 on /tmp/media/usb/Local/WDTVLiveHub type ufsd (rw,nls=utf8,uid=0,gid=0,fmask=0,...)
```



Persistence

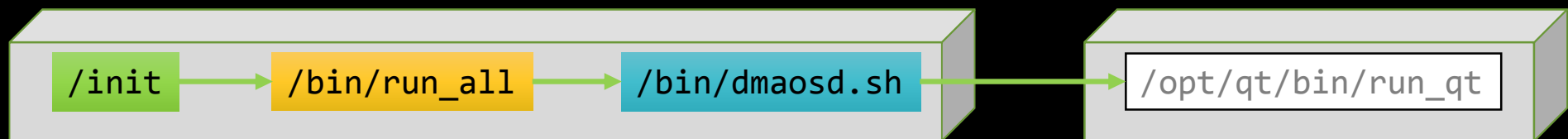
... without the risk of bricking it



Patch firmware conservatively

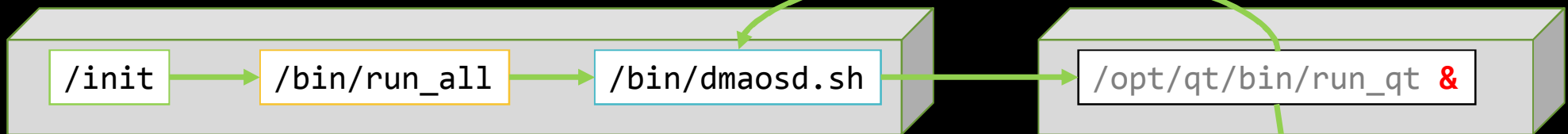
Want to avoid bricking

- Use clean reset scheme
- Place other tools where they can be removed externally - harddrive (just in case)
- Don't patch the main image → has several integrity checks (good conditions to run into problems)
- ... patch as little as possible



Challenge: Mount order

- Dmaosd is last process started
 - Mounts the hard drive
 - Race condition: No dmaosd if run_qt blocks → no hard drive → block



- Solution:
 1. Return control and continue as **background process**
 2. **Wait for hard drive** to be mounted
 3. **Continue booting** there



Where are the lawyers?

GPL? Linux? ...

GPL Firmware

- Available but ...
 - will lose all DRM keys
 - Potentially WD keys
- ... I haven't tried what is lost

Downloads Support by Country Feedback Print SHARE

WD TV Live Hub Media Center

[Home Entertainment](#) [Installation](#) [Downloads](#) [Knowledge Base](#) [Discussions](#)

Available software for this product

For Windows

- WD Discovery Software
- My Net View Network Evaluation Tool

For Windows & Mac

- **WD TV Live Hub GPL Code**
- Current Firmware - 3.12.13 (7/2013) | Release Notes

For Windows & Mac

- **WD TV Live Hub GPL Code**
- Current Firmware - 3.12.13 (7/2013) | Release Notes

3/28/2012(3.03.16), 2/28/2012(3.03.13), 12/20/2011(3.01.19), 11/17/2011(3.00.28), 10/6/2011(2.08.13), 8/1/2011(2.07.17),

Contact Support

Warning! This is the GPL source code. This is NOT the firmware for the device. If you use this source code to update the device, it will be treated as a third party user-modified firmware. We recommend using firmware released by Western Digital only. Using third party or user-modified firmware will cause malfunction and will void your product warranty. Once you install third party or user-modified firmware, even if the product is rolled back to the original firmware from WD, access to certain features will be disabled.

Files available for download

Where is the security?

Conspiracy Theory

- Why is WD basically leaving the device open?

Outlook

My situation




Your options

Livestation Channels

World News Regional Business Politics Special Interest New Channels Radio

ALJAZEERA ALJAZEERA BBC WORLD NEWS BBC WORLD SERVICE CCTV NEWS

Free trial time remaining: 00:01:46



GRIGOR DIMITROV
Mexican Open Champion

BBC WORLD NEWS TER: @bbcworld AND @bbcbreaking

Share with Facebook Tweet 665 +1 688

INDIA TV Billige Kontorfellesskap
regus.no/Oslo
Mon, March 3, 2014, Updated: 12:55 AM IST
Optil 2 måneder Gratis leie! Fleksible kontorer, klare til bruk

HOME VIDEO INDIA WORLD POLITICS BUSINESS SPORTS ENTERTAINMENT CRIME LIVE TV PHOTOS LIFESTYLE

Hot Topics: Narendra Modi | Rahul Gandhi | Arvind Keirival | Telangana

Se Sport på Sumo
sumo.tv2.no/Sport
Med TV 2 Sumo er du som bestemmer. Det beste utvalget, abonnér i dag.

µTorrent WebUI v0.310 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Most Visited Digix Homepage Digix AdminCP Digix cPanel Digix Mail Digix Upload µTorrent Nimrod uTorrent Matts uTorrent

Name	Status	Size	Done	Downloaded	Uploaded	Ratio	DL	UL
Battlestar.Galactica.S04E08.HDTV.XviD-BIA	Seeding [F]	360.85 MB	100%	361.1 MB	3.9 GB	11.084	0.2 KB/s	118.1 KB/s
Dexter.S01.HDTV.XviD-TorrentLeech	Seeding [F]	4.14 GB	100%	4.1 GB	1.0 GB	0.263	0.0 KB/s	1.5 KB/s
Doctor Who Special - Time Crash (16 November 2007) [DVD]	Seeding [F]	79.85 MB	100%	79.8 MB	2.0 GB	26.191	0.0 KB/s	0.0 KB/s
GTA IV Complete Strategy Guide Maps Cheats Codes-Torrer	Seeding [F]	16.48 MB	100%	16.4 MB	85.4 MB	5.180	0.0 KB/s	0.0 KB/s
Hells.Kitchen.US.S04E06.PROPER.HDTV.XviD-2HD	Seeding [F]	361.90 MB	100%	361.9 MB	12.2 GB	34.755	0.0 KB/s	0.0 KB/s
Hells.Kitchen.US.S04E07.HDTV.XviD-XOR	Seeding [F]	359.19 MB	100%	359.1 MB	2.2 GB	6.462	0.0 KB/s	0.0 KB/s
Hells.Kitchen.US.S04E08.INTERNAL.WS.PDTV.XviD-RentBoy	Seeding [F]	350.90 MB	100%	350.9 MB	4.6 GB	13.479	0.0 KB/s	0.0 KB/s
Hells.Kitchen.US.S04E09.HDTV.XVID.PROPER-BAJSKORV	Seeding [F]	348.84 MB	100%	349.0 MB	3.9 GB	11.598	0.0 KB/s	0.0 KB/s
Lost.4x12.Theres_No_Place_Like_Home.HDTV_XviD-FoV	Seeding [F]	352.38 MB	100%	352.3 MB	8.7 GB	25.429	0.0 KB/s	2.8 KB/s
Skins.S02E09.HDTV.XviD-BIA	Seeding [F]	364.40 MB	100%	364.4 MB	20.9 GB	58.784	0.0 KB/s	0.0 KB/s
Skins.S02E10.WS.PDTV.XviD-RIVER	Seeding [F]	352.37 MB	100%	352.3 MB	17.3 GB	50.378	0.0 KB/s	0.0 KB/s
The.Apprentice.UK.S04E09.WS.PDTV.XviD-SPAREL	Seeding [F]	706.68 MB	100%	706.6 MB	33.2 GB	48.182	0.0 KB/s	31.9 KB/s
The.Apprentice.UK.S04E10.WS.PDTV.XviD-SPAREL	Seeding [F]	704.81 MB	100%	704.8 MB	11.1 GB	16.224	0.1 KB/s	0.1 KB/s
The.F.Word.S04E01.PROPER.WS.PDTV.XviD-NOsegment	Seeding [F]	358.13 MB	100%	358.1 MB	3.6 GB	10.367	0.0 KB/s	0.0 KB/s

General Files Logger

Transfer

Time Elapsed: Remaining: Share Ratio:
Downloaded: Download Speed: Down Limit:
Included: Includ Speed: In Limit:

Done

Questions?

WHY DO WHALES JUMP
WHY ARE WITCHES GREEN
WHY ARE THERE MIRRORS ABOVE BEDS
WHY DO I SAY UH
WHY IS SEA SALT BETTER
WHY ARE THERE TREES IN THE MIDDLE OF FIELDS
WHY IS THERE NOT A POKEMON MMO
WHY IS THERE LAUGHING IN TV SHOWS
WHY ARE THERE DOORS ON THE FREEWAY
WHY ARE THERE SO MANY SUCHOSTEIKE RUNNING
WHY AREN'T THERE ANY COUNTRIES IN ANTARCTICA
WHY ARE THERE SCARY SOUNDS IN MINECRAFT
WHY IS THERE KICKING IN MY STOMACH
WHY ARE THERE TWO SLASHES AFTER HTTP
WHY ARE THERE CELEBRITIES
WHY DO SNAKES EXIST
WHY DO OYSTERS HAVE PEARLS
WHY ARE DUCKS CALLED DUCKS
WHY DO THEY CALL IT THE CLAP
WHY ARE KYLE AND CARTMAN FRIENDS
WHY IS THERE AN ARROW ON A PING'S HEAD
WHY ARE TEXT MESSAGES BLUE
WHY ARE THERE MUSTACHES ON CLOTHES
WHY ARE THERE MUSTACHES ON CARS
WHY ARE THERE SO MANY BIRDS IN OHIO
WHY IS THERE SO MUCH RAIN IN OHIO
WHY IS OHIO WEATHER SO WEIRD
WHY ARE THERE MALE AND FEMALE BIKES
WHY ARE THERE BRADSHIRTS
WHY DO DIVING PEOPLE RESURF UP
WHY AREN'T THERE UNKIDGEE FRIENDS
WHY ARE OLD HUNGONS DIFFERENT

WHY DO TESTICLES MOVE
WHY ARE THERE PSYCHICS
WHY ARE HATS SO EXPENSIVE
WHY IS THERE OFFENSE IN MY SHIRTPOO
WHY DO YOUR BOOBS HURT


WHY ARE THERE SLAVES IN THE BIBLE
WHY DO TWINS HAVE DIFFERENT FINGERPRINTS
WHY ARE AMERICANS AFRAID OF DRAGONS
WHY IS HTTPS CROSSED OUT IN RED
WHY IS THERE A LINE THROUGH HTTPS
WHY IS THERE A RED LINE THROUGH HTTPS ON FACEBOOK
WHY IS HTTPS IMPORTANT

QUESTIONS
FOUND IN GOOGLE AUTOCOMPLETE

WHY AREN'T ECONOMISTS RICH
WHY DO AMERICANS CALL IT SOCCER
WHY ARE MY EARS RINGING
WHY ARE THERE SO MANY AVENGERS
WHY ARE THE AVENGERS FIGHTING THE X MEN
WHY IS WOLVERINE NOT IN THE AVENGERS


WHY ARE THERE ANTS IN MY LAPTOP
WHY IS EARTH TILTED
WHY IS SPACE BLACK
WHY IS OUTER SPACE SO COLD
WHY ARE THERE PYRAMIDS ON THE MOON
WHY IS NASA SHUTTING DOWN

WHY ARE THERE GHOSTS
WHY IS THERE AN OWL IN MY BACKYARD
WHY IS THERE AN OWL OUTSIDE MY WINDOW
WHY IS THERE AN OWL ON THE DOLLAR BILL
WHY DO OWLS ATTACK PEOPLE
WHY ARE AK 47S SO EXPENSIVE
WHY ARE THERE HELICOPTERS CIRCLING MY HOUSE
WHY ARE THERE GODS
WHY ARE THERE TWO SPOOKS
WHY IS MT VESUVIUS THERE
WHY DO THEY SAY T MINUS
WHY ARE THERE OBELISKS
WHY ARE WRESTLERS ALWAYS WET
WHY ARE OCEANS BECOMING MORE ACIDIC
WHY IS ARWEN DYING
WHY AREN'T MY QUAIL LAYING EGGS
WHY AREN'T MY QUAIL EGGS HATCHING
WHY AREN'T THERE ANY FOREIGN MILITARY BASES IN AMERICA

WHY AREN'T MY ARMS GROWING


WHY ARE THERE DOGS AFRAID OF FIREWORKS
WHY ARE THERE NO KING IN ENGLAND

WHY ARE THERE SQUIRRELS


WHY ARE THERE FEMALE MR MINES
WHY IS SEX SO IMPORTANT


WHY AREN'T THERE GUNS IN HARRY POTTER


WHY ARE ULTRASOUNDS IMPORTANT
WHY ARE ULTRASOUND PROBED DOPPEL
WHY IS STEALING WRONG

WHY ARE THERE MEN'S
WHY DO I FEEL DIZZY

WHY ARE THERE SO MANY CROWS IN ROCHESTER,
WHY IS PSYCHIC WEAK TO BUG
WHY DO CHILDREN GET CANCER
WHY IS POSEIDON ANGRY WITH ODYSSEUS
WHY IS THERE ICE IN SPACE

WHY ARE THERE PHLEIGHT
WHY IS THERE LANA

WHY IS THERE A LINE THROUGH HTTPS
WHY IS THERE A RED LINE THROUGH HTTPS ON FACEBOOK

WHY ARE THERE BRADSHIRTS
WHY DO DIVING PEOPLE RESURF UP
WHY AREN'T THERE UNKIDGEE FRIENDS
WHY ARE OLD HUNGONS DIFFERENT

WHY ARE THERE TINY SPIDERS IN MY HOUSE
WHY ARE THERE HUGE SPIDERS IN MY HOUSE
WHY ARE THERE LOTS OF SPIDERS IN MY HOUSE
WHY ARE THERE SPIDERS IN MY ROOM
WHY ARE THERE SO MANY SPIDERS IN MY ROOM
WHY DO SPIDER BITES ITCH
WHY IS DYING SO SCARY

WHY IS THERE NO GPS IN LAPTOPS
WHY DO KNEES CLICK
WHY AREN'T THERE E GRADES
WHY IS ISOLATION BAD
WHY DO BOYS LIKE ME
WHY DON'T BOYS LIKE ME
WHY IS THERE ALWAYS A TRAP UPDATE
WHY ARE THERE RED DOTS ON MY THIGHS
WHY IS LYING GOOD

WHY IS PROGRAMMING SO HARD
WHY IS THERE A 0 ON RESISTOR
WHY DO AMERICANS HATE SOCCER
WHY DO RHYMES SOUND GOOD
WHY DO TREES DIE
WHY IS THERE NO SOUND ON OWN
WHY AREN'T POKEMON REAL
WHY AREN'T BULLETS SHARP
WHY DO DREAMS SEEM SO REAL

WHY ARE THERE ZIPPER
WHY DO ISLANDS DIE

WHY ARE THERE PHLEIGHT
WHY IS THERE LANA

WHY ARE THERE MEN'S
WHY DO I FEEL DIZZY

WHY ARE THERE SO MANY CROWS IN ROCHESTER,
WHY IS PSYCHIC WEAK TO BUG
WHY DO CHILDREN GET CANCER
WHY IS POSEIDON ANGRY WITH ODYSSEUS
WHY IS THERE ICE IN SPACE

WHY ARE THERE PHLEIGHT
WHY IS THERE LANA

WHY IS THERE A LINE THROUGH HTTPS
WHY IS THERE A RED LINE THROUGH HTTPS ON FACEBOOK

WHY ARE THERE BRADSHIRTS
WHY DO DIVING PEOPLE RESURF UP
WHY AREN'T THERE UNKIDGEE FRIENDS
WHY ARE OLD HUNGONS DIFFERENT

WHY ARE THERE TINY SPIDERS IN MY HOUSE
WHY ARE THERE HUGE SPIDERS IN MY HOUSE
WHY ARE THERE LOTS OF SPIDERS IN MY HOUSE
WHY ARE THERE SPIDERS IN MY ROOM
WHY ARE THERE SO MANY SPIDERS IN MY ROOM
WHY DO SPIDER BITES ITCH
WHY IS DYING SO SCARY

WHY IS THERE NO GPS IN LAPTOPS
WHY DO KNEES CLICK
WHY AREN'T THERE E GRADES
WHY IS ISOLATION BAD
WHY DO BOYS LIKE ME
WHY DON'T BOYS LIKE ME
WHY IS THERE ALWAYS A TRAP UPDATE
WHY ARE THERE RED DOTS ON MY THIGHS
WHY IS LYING GOOD

WHY IS PROGRAMMING SO HARD
WHY IS THERE A 0 ON RESISTOR
WHY DO AMERICANS HATE SOCCER
WHY DO RHYMES SOUND GOOD
WHY DO TREES DIE
WHY IS THERE NO SOUND ON OWN
WHY AREN'T POKEMON REAL
WHY AREN'T BULLETS SHARP
WHY DO DREAMS SEEM SO REAL