

XeLL-HACK (XBR)

XENON-ZEPHYR-FALCON-OPUS-JASPER

In this tutorial I will describe how to flash your console with the XeLL-Homebrew-Hack / XBox-Rebooter-Kernel.

1. Which Xbox Revision do I have?

By looking at the power supply connector, you can see which console revision you have.

Differences between Xenon/Zephyr: Zephyr has HDMI, Xenon does not.

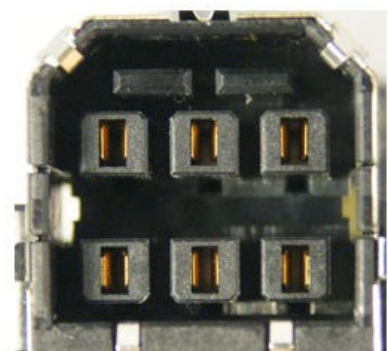
Difference between Falcon/Opus: Falcon has HDMI, Opus doesn't.



Xenon/Zephyr
1st Generation Xbox 360 (2005)



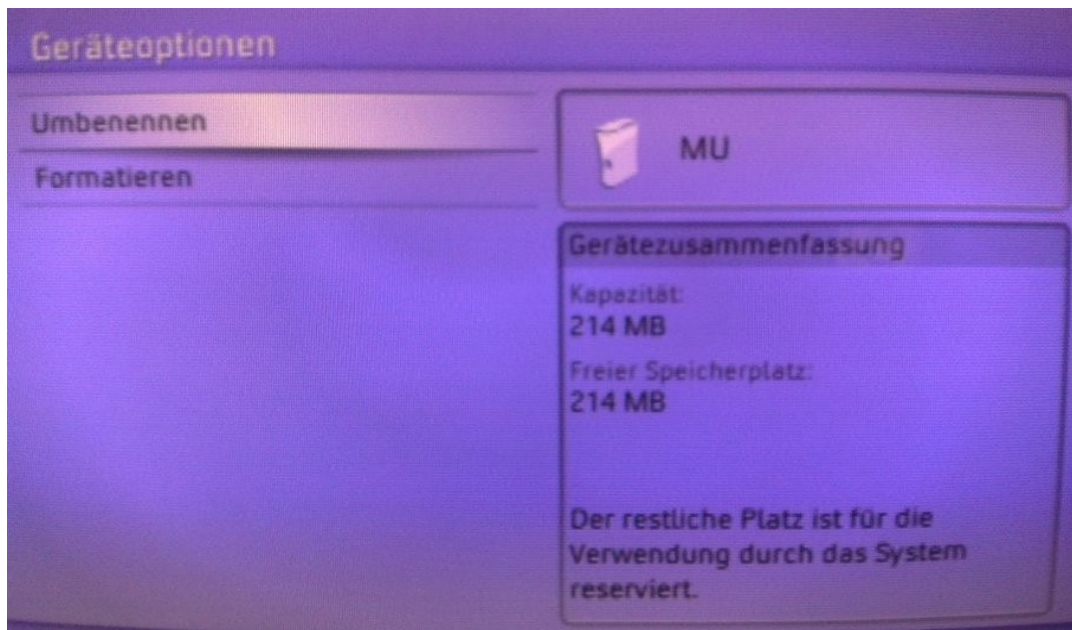
Opus/Falcon
2nd Generation Xbox 360 (2007)



Jasper
3rd Generation Xbox 360 (2008)

If you have a Jasper box, you should also check which NAND size it has (NAND = Internal Flash-Chip, stores the Dashboard/Config. On Jasper a part is also functioning as an internal Memory Unit). Unplug all storage devices (HDD, Memory Unit etc.) and navigate to “System Settings”, “Memory”.

If you don't see a storage device listed there you have a Jasper without an integrated Memory Unit, so you have a 16MB NAND. If a storage device is listed (with a symbol of an Xbox console in front) press the Y-Button and a summary from the storage device will appear.



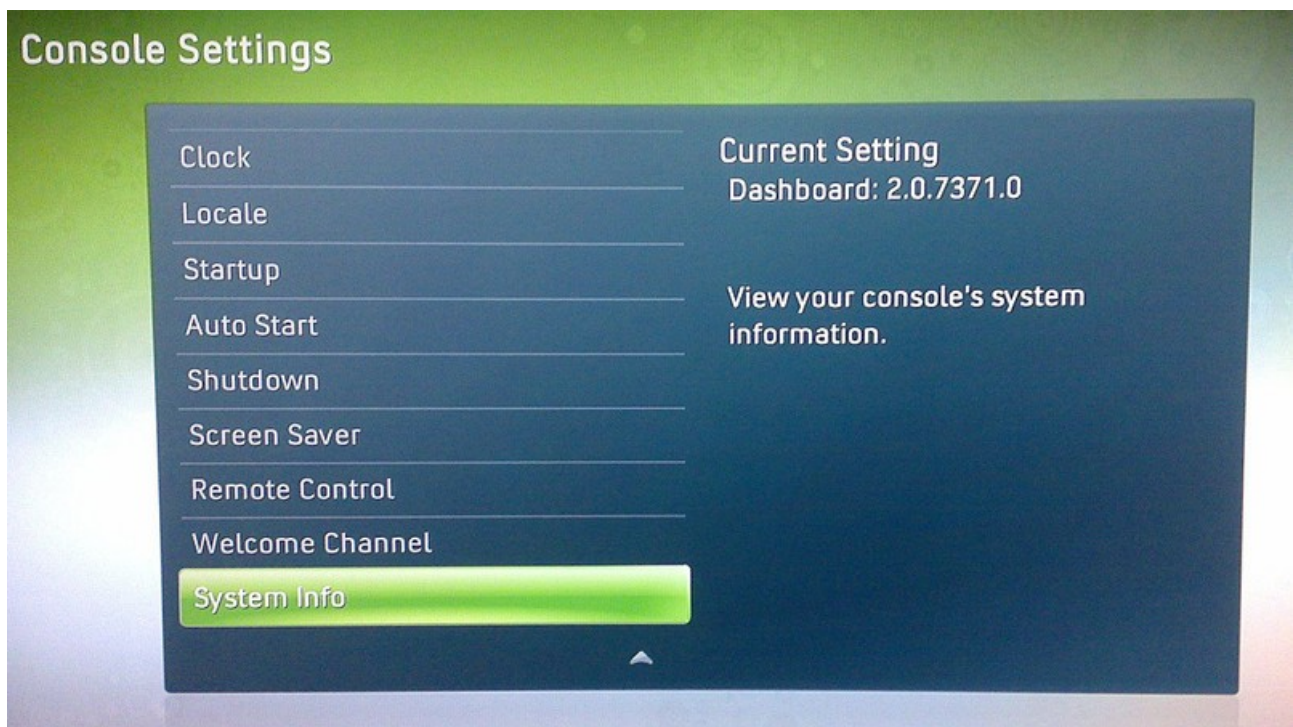
Identification:

Capacity: 214MB = 256MB NAND

Capacity: 451MB = 512MB NAND

2. Which Dashboard-Version does my console have?

At first you have to find out which dashboard version your Xbox console has. Go to “System Settings”, “Console Settings” and choose “System Info”. The dashboard should show something like “2.0.7371.0”.



It is possible to use the hack up to Version 7371, but starting with Dashboard-Version **8xxx** it **isn't** possible anymore.

With Jasper, beginning MFR July, you have to read out the NAND first anyway to know for sure that the Hack will work. (The NAND should be read out anyway, doesn't matter which Mainboard-Revision you have).

So let's go!

3. Building the LPT-Programmer

For soldering the LPT-Programmer you will need the following:

A computer with an LPT-Port (Printer port)

Soldering Iron (15W recommended)

Soldering tin

Wire (reichelt.de-Article: LITZE SW)

1x LPT-Plug (DB25) (reichelt.de-Article: D-SUB ST 25)

5x 100 Ohm Resistors (reichelt.de-Article: 1/4W 100)

1x 1N4148 Switching Diode (reichelt.de-Article: 1N 4148)

(1N914 Switching Diodes will also work where 1N4148 Diodes are mentioned)

Optional:

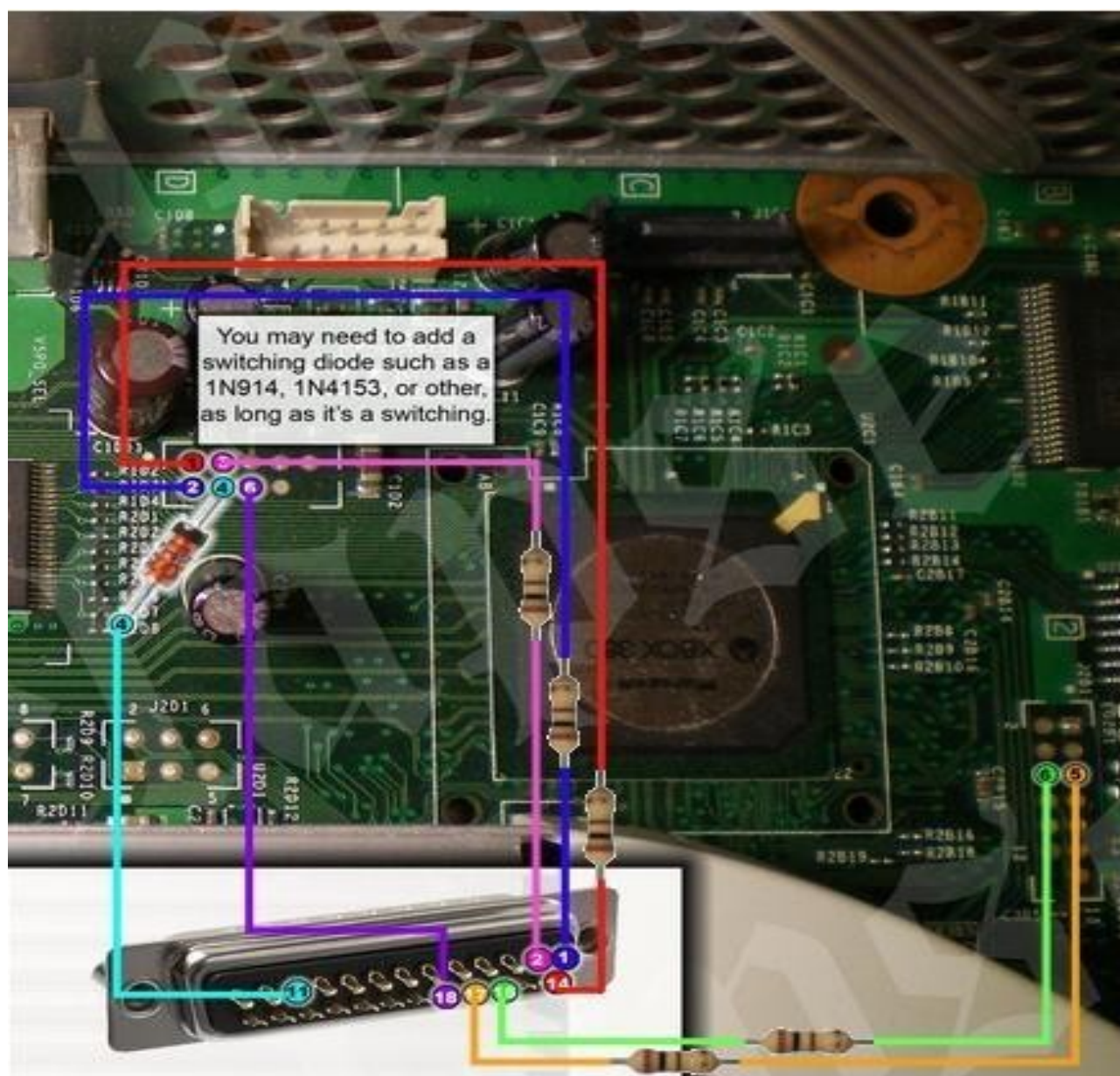
shrink tubing or iso tape

For the JTAG-SMC Connections you will need:

2x 1N4148 Diodes (reichelt.de-Article: 1N 4148)

Which you should buy also ;)

Now solder the connections shown on the following diagram to the LPT-Plug and the Xbox-Mainboard. After checking for shorts isolate the single pins on the LPT-Plug with some shrink tubing or electrical tape. Hot glue might also work.



4. Reading out the NAND

If you soldered everything correctly you can continue with reading out the NAND-Flash.

The following software is required:

NANDPro (currently Version 2.0 b)

Infectus NAND Checker (currently Version 1.1)

MD5 Comparison Tool (hex editors can do this)

360 Flash Tool (currently Version 0.91)

CD Info (currently Version 1b)

First go into your NANDPro directory, execute the file “port95nt.exe” and reboot the PC.

Now click on “Start” → “Run”(on xp) and enter “command” or “cmd”. Navigate now via the “cd” command to your NANDPro folder (for example: if you unpacked NANDPro to the Desktop enter “cd Desktop/NANDPro”).

When you are in the NANDPro-folder, you can connect the power to your Xbox (just stand-by power, DON'T TURN IT ON) and connect the LPT plug to your computer.

Start NANDPro according to the following:

For Xenon/Zephyr/Opus/Falcon and Jasper(16MB NAND)

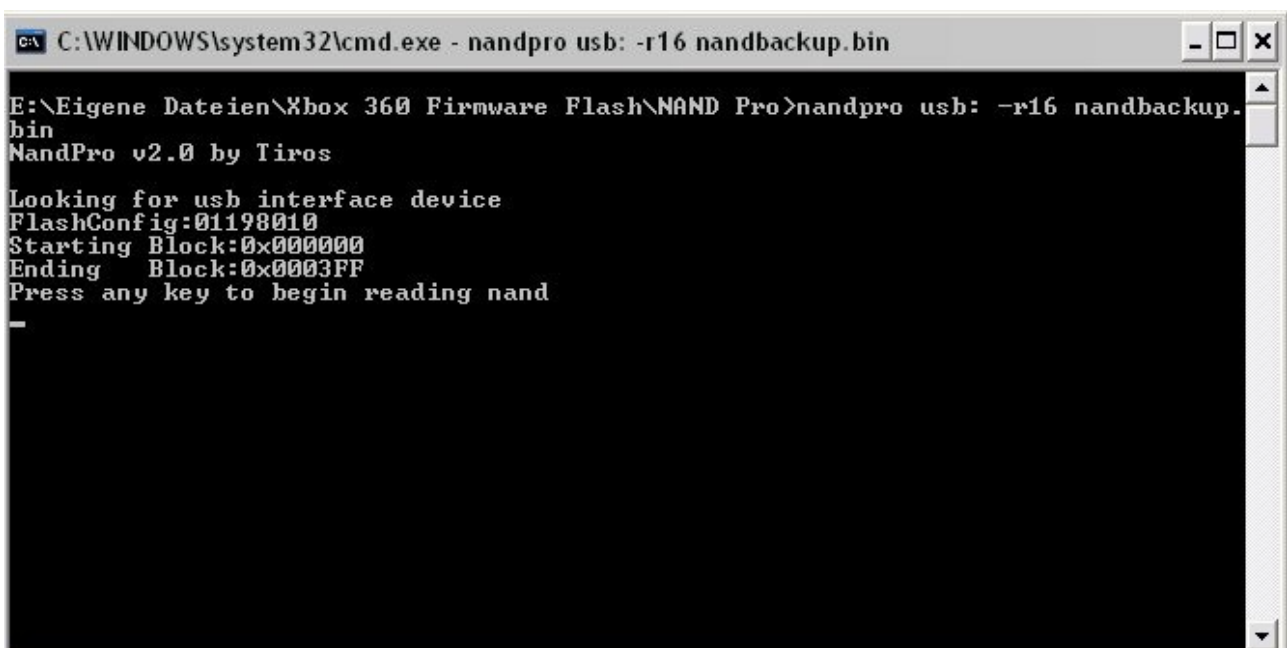
Nandpro lpt: -r16 nandbackup.bin

For Jasper (256MB NAND)

Nandpro lpt: -r256 nandbackup.bin

And for Jasper (512MB NAND)

Nandpro lpt: -r512 nandbackup.bin



```
C:\WINDOWS\system32\cmd.exe - nandpro usb: -r16 nandbackup.bin

E:\Eigene Dateien\Xbox 360 Firmware Flash\NAND Pro>nandpro usb: -r16 nandbackup.
bin
NandPro v2.0 by Tiros

Looking for usb interface device
FlashConfig:01198010
Starting Block:0x000000
Ending Block:0x0003FF
Press any key to begin reading nand
-
```

NANDPro should show you something similar to this.

Check before reading out that the Flash codes are correct, otherwise you will waste 40 minutes dumping nothing.

For Xenon/Zephyr/Opus/Falcon

FlashConfig: 01198010

For Jasper (16MB)

FlashConfig: 00023010

For Jasper (256MB)

FlashConfig: 008A3020

256MB NAND Detected

For Jasper (512MB)

FlashConfig: 00AA3020

512MB NAND Detected

If your Flash code is correct, you can start the dump by pressing a random key. (NANDPro v2.0a needs the key, 2.0b does not)

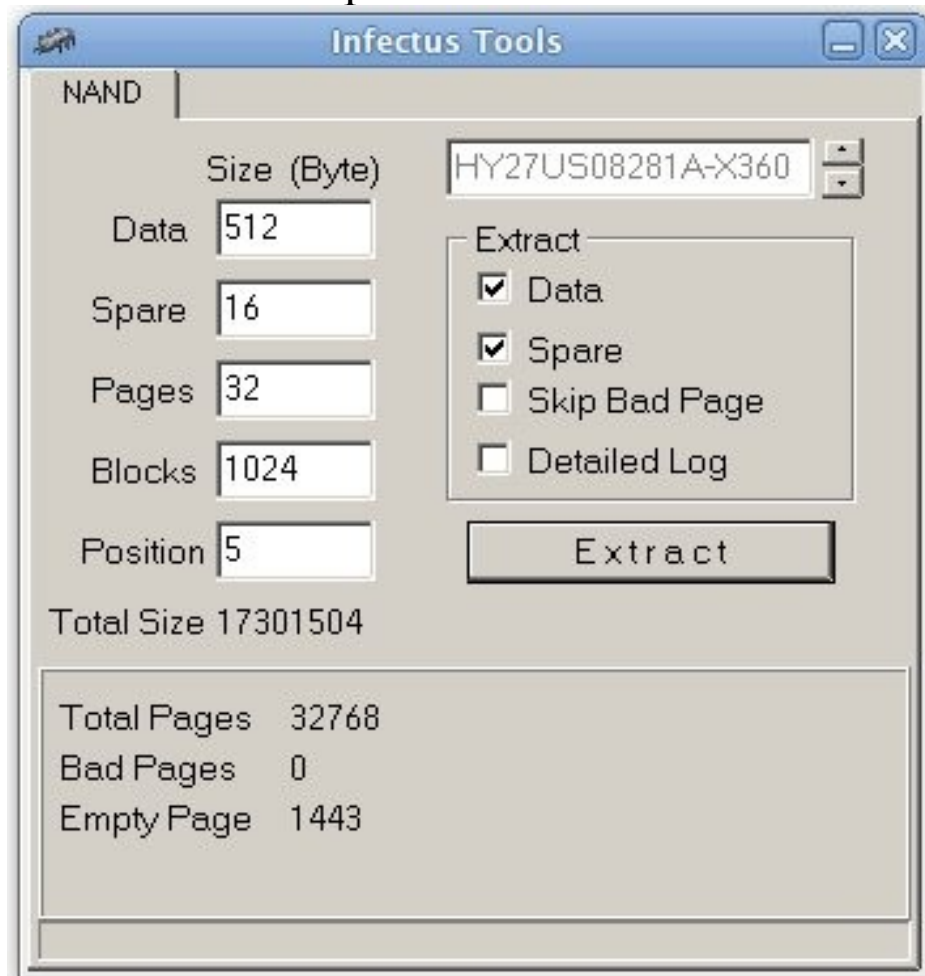
The safest way to check the dumps is to make a few and compare them with a checksum program.

If you have identical checksums, check the dumps again with the Infectus NAND Checker, just to be 100% sure.

It only supports 16MB Dumps at the moment, so for NANDs bigger than that there is no good method (known to me) to verify them.

Start the Infectus NAND Checker, click on “Extract” where you choose your dump and wait for the check to complete.

An error free NAND-Dump looks like this:



It can happen that you get “Bad Pages” or “Bad Blocks”. If you get these messages, post your NANDPro log and your NAND checker output to the forums so that someone can figure out if the number or locations of these bad blocks are due to a bad dump or NAND damage.

If everything is alright, you still have to check Jasper Boards to see if they are “XeLL-compatible”. To do this you open the “CD Info” tool, press “Open nand backup” and choose your NAND-Dump. The line “CD” is important.



Here's a list of compatible CD-Versions:

Xenon: 1888, 1902, 1903, 1920, 1921

Zephyr: 4558

Falcon: 5761, 5766, 5770

Jasper: 6712, 6723

All incompatible Revisions have (currently) CD Version 8453.

The remaining NAND info you will get with “360 Flash Dump Tool”. The Tool is (currently) NOT compatible with Jasper 256MB/512MB Dumps, so the CD info will be used in this case.

Flash Tool will show a dialog-box named “Keys” on the first start, you have to enter the 1BL Key. Check the box in front of it and restart the tool.

1BL-Key: DD88AD0C9ED669E7B56794FB68563EFA

360 Flash Tool V0.88b - Retail Only

Open Dump File
 C:\Dokumente und Einstellungen\Administr

Cx Sections

CB	5770	Pairing	0x998749	LDV	0
CD	5770	Patch 0	7363	LDV	3
CE	1888	Patch 1	6690	LDV	2

Key Vault

Type Serial Region

DVD Key

OSIG

Patch Extract Keys Close

FFS

Name	Start Block	Length
aac.xexp1	0x03A5	0x00004000
bootanim.xex	0x0029	0x00061000
createprofile.xexp1	0x03A6	0x0000D000
createprofile.xex	0x0044	0x0000A000
dash.xex	0x03A4	0x004B3000
deviceselector.xexp1	0x0140	0x00002800
deviceselector.xex	0x0154	0x00005000
gamerprofile.xexp1	0x0141	0x0000F800
hud.xexp1	0x0145	0x00025800
huduiskin.xex	0x014F	0x00055000
mfgbootlauncher.xexp1	0x0167	0x00004800
minimediaplayer.xexp1	0x0169	0x00007800
gamerprofile.xex	0x016E	0x00013000
signin.xexp1	0x0168	0x00007800
hud.xex	0x0177	0x0001F000
updater.xexp1	0x016D	0x00003000
vk.xexp1	0x0173	0x0000B000
ximecore.xex	0x0176	0x00012000
ximedic.xexp1	0x0183	0x00002000
mfgbootlauncher.xex	0x019D	0x00009000
minimediaplayer.xex	0x01A1	0x00009000

If you have a compatible Version and your NAND dumped properly you can continue with flashing the XeLL-Image.

5.Flashing the XeLL-Image

Get the correct XeLL-Image for your Xbox-Revision from *the usual places*, extract it and copy the bin-file (xenon/zephyr/falcon(opus)/jasper_hack.bin) into the NANDPro directory.

Go into the NANDPro-folder from within the Command Prompt and enter the following command to flash the Image.

Xenon/Zephyr/Opus/Falcon/Jasper(16MB NAND)

NANDPro lpt: -w16 xboxrev_hack.bin

Jasper (256MB NAND)

NANDPro lpt: -w256 xboxrev_hack.bin

Jasper (512MB NAND)

NANDPro lpt: -w512 xboxrev_hack.bin

Where “xboxrev” stands for your Xbox-Revision, so xboxrev_hack.bin is pointing to your XeLL-Image.

After successful Flashing (should take approx. 5 Minutes) unplug the LPT-Cable from PC, and then the power supply from the Xbox.

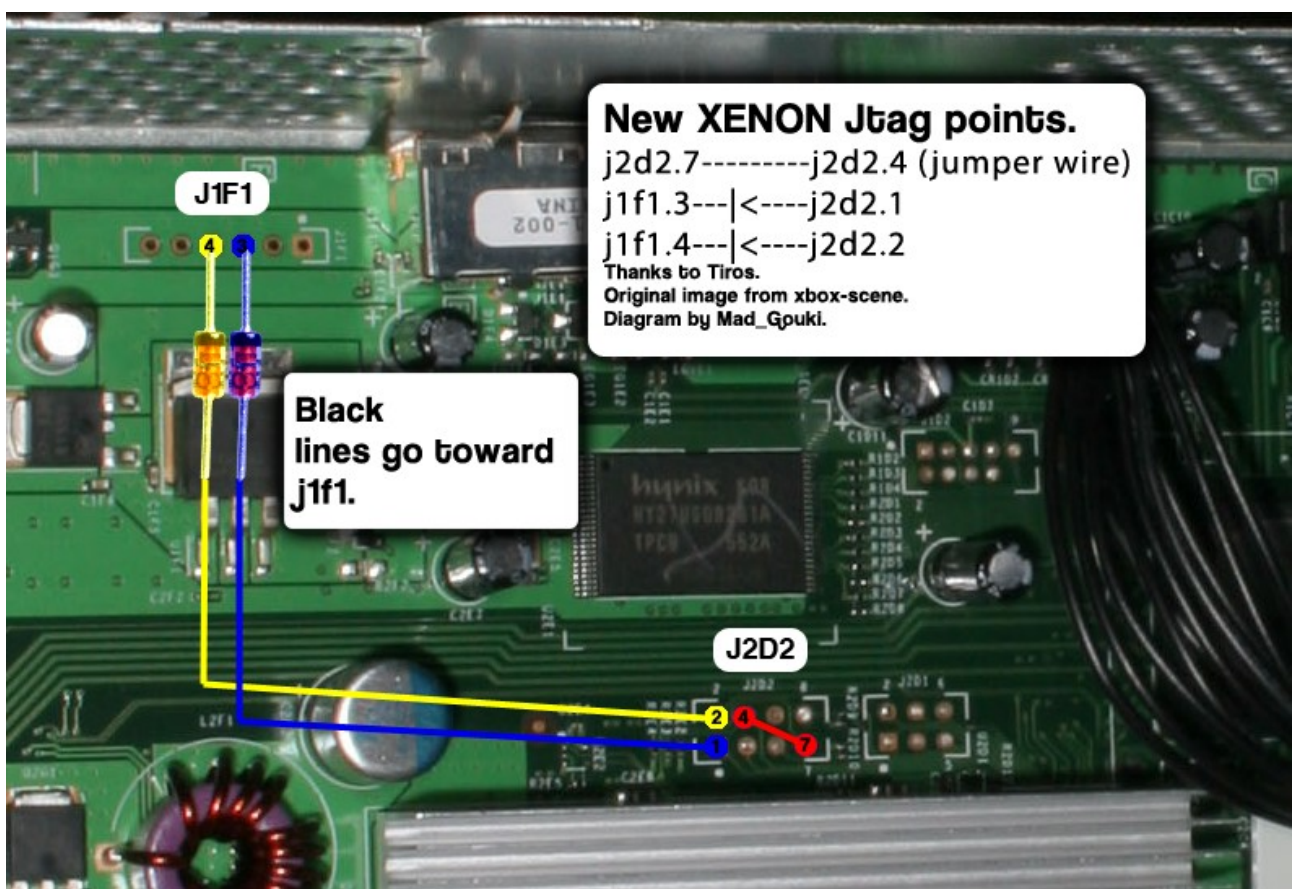
Now it's time to solder the SMC-JTAG Connections.

6.Soldering the SMC-JTAG Connections

Open the Xbox360 so that you are looking at the motherboard.
You don't have to remove the board from the metal case.

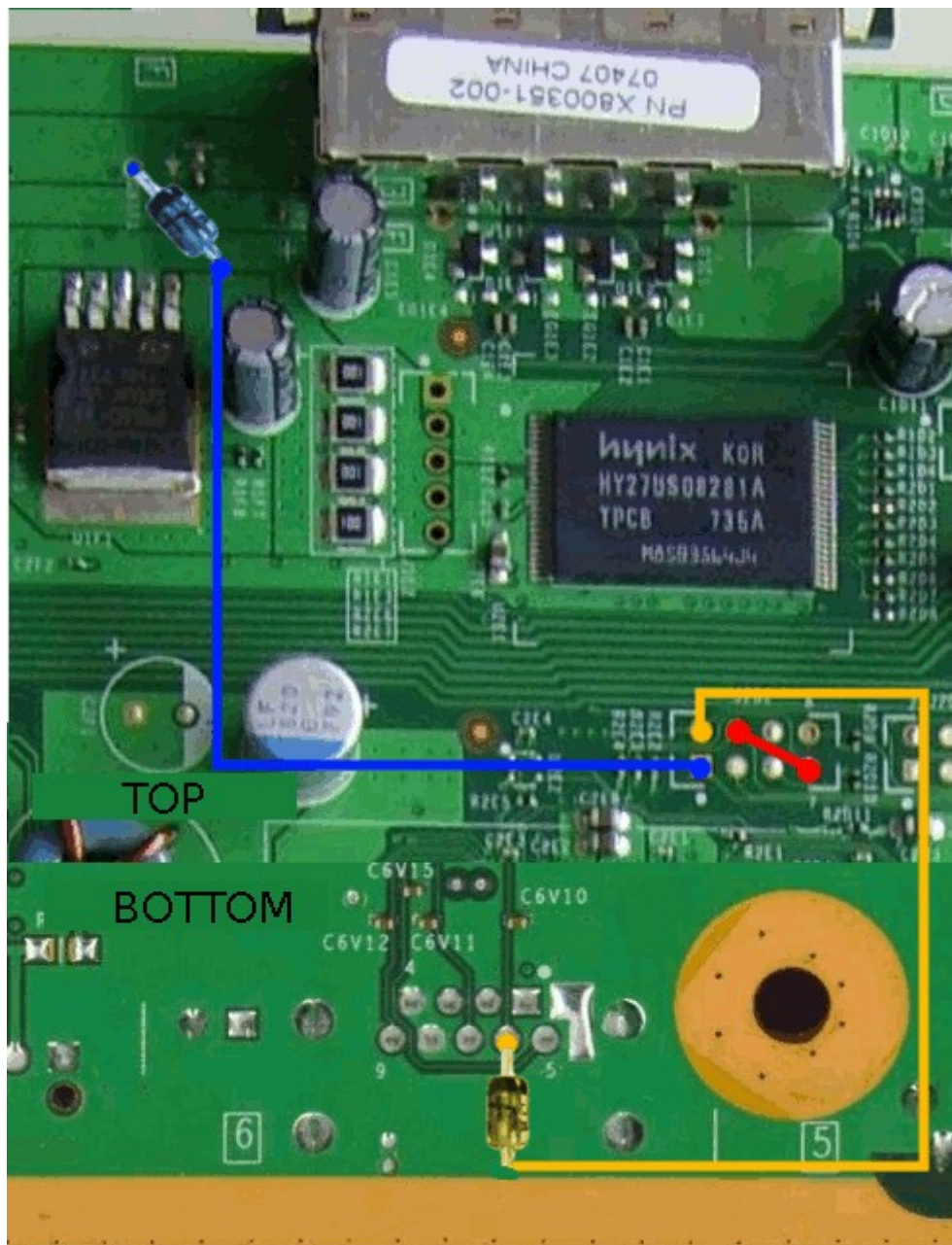
Solder two switching diodes and the jumper according to the following plan:

Xenon:



Note: There is also an older version of the JTAG SMC connections for the xenon board which uses 3x330Ohm Resistors. The diode solution described here is safer.

Zephyr/Opus/Falcon/Jasper:



When you have the connections cleanly soldered is it time for testing :)

Assemble the Motherboard into the case and plug in the AV-Cable (VGA, Composite or YUV) and the power supply.

When starting the box you should see a blue screen with white text.

```
useset 09: 0000000000000000
useset 10: 0000000000000000
useset 11: 0000000000000000
SB bus 0 device 1: vendor 0000 product 0000 class 09: USB Hub
SB bus 1 device 1: vendor 0000 product 0000 class 09: USB Hub
* Waiting for USB...
SB: New device connected to bus 0 hub 1 port 1
SB bus 0 device 2: vendor 067B product 2515 class 09: USB Hub
SB: New device connected to bus 0 hub 2 port 1
SB bus 0 device 3: vendor 067B product 2517 class 08: Mass-Storage Device
SBMASS: Do not understand devices with SubClass 0x05, Protocol 0x50
SB: New device connected to bus 1 hub 1 port 1
SB bus 1 device 2: vendor 045E product 0291 class FF: Not found.
* try booting tftp
o tftp
FTP boot from 10.0.120.78:/tftpbboot/xenon, to 8000000004000000
FTP: no answer from server, retrying
FTP: no answer from server, retrying
FTP: no answer from server, retrying
FTP: no answer from server, retrying
FTP: no answer from server, retrying
FTP: no answer from server, retrying
FTP: no answer from server, retrying
FTP: no answer from server, retrying
FTP: no answer from server, retrying
FTP: no answer from server, retrying
0 tries exceeded, aborting.
ftp result: -2
* try booting from CDROM
```

If that's the case you succeeded :)

Now you can desolder your LPT-Programmer (or just shove it in the case if you want).

Don't desolder it if you want to flash XBR now :)

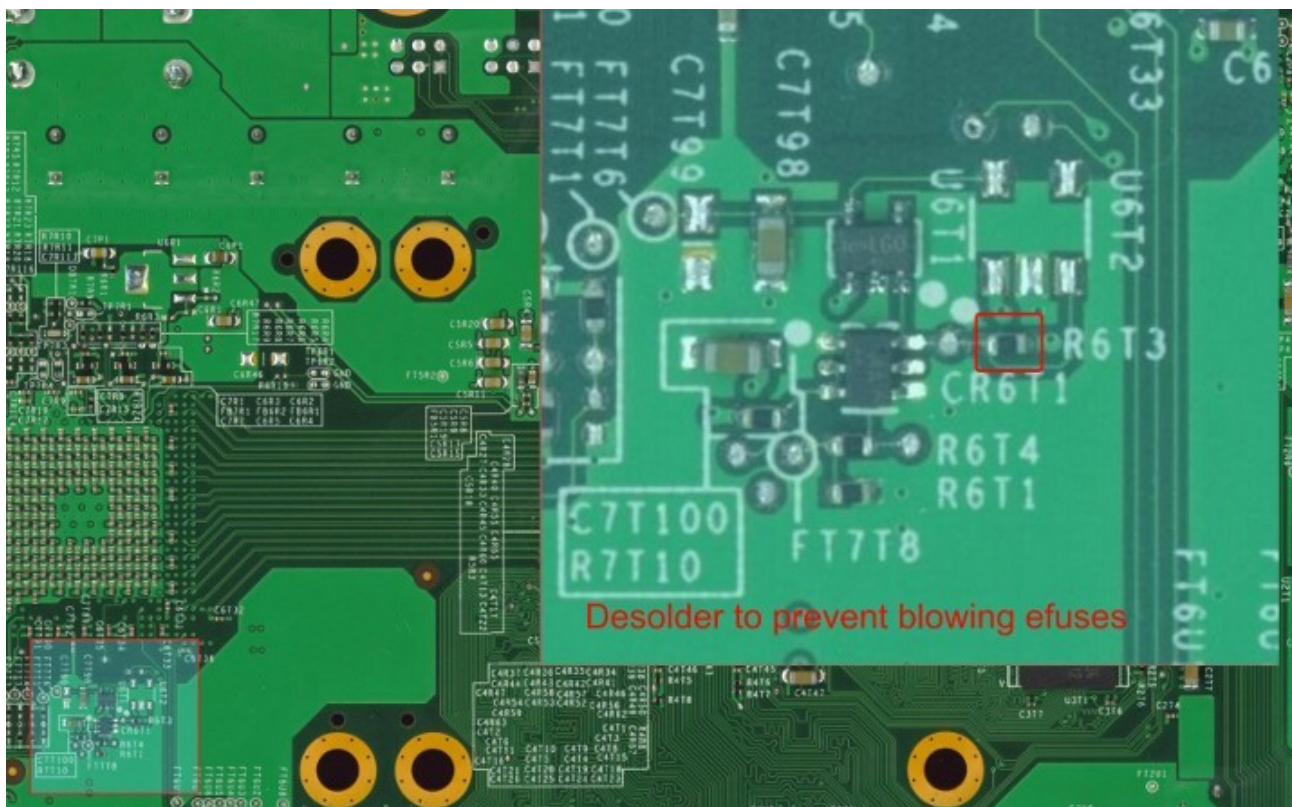
You can test various emulators and Linux on your console now.

Have fun!

7.Optional: Desolder the R6T3 Resistor

Optionally, you can desolder the R6T3 Resistor. The desoldering prevents a dashboard update (or malicious program) from locking you out of using XeLL. Instead of upgrading the Dashboard it will show an E80 Error.

The following picture shows the position of the R6T3 on the back-side of the mainboard



8. Preparing the Xbox-Rebooter Image

The following software is required:

Xbox-Rebooter-Image for your Console Revision
NANDPro v2.0b (! at least v2.0b !)

Eventually if you got unfixable Bad Blocks:
Redline99's BadBlockMover (currently only working for non-Jasper Images)

At first you need to have your Original Dump (orig.bin) and the XBR-Image (XBR.bin) in the NandPro-Directory. Now you navigate through Commandline into this directory.

To read out the rawkv.bin type the following:

```
nandpro orig.bin: -rXX rawkv.bin 1 1
```

To write it into your XBR-Image you type:

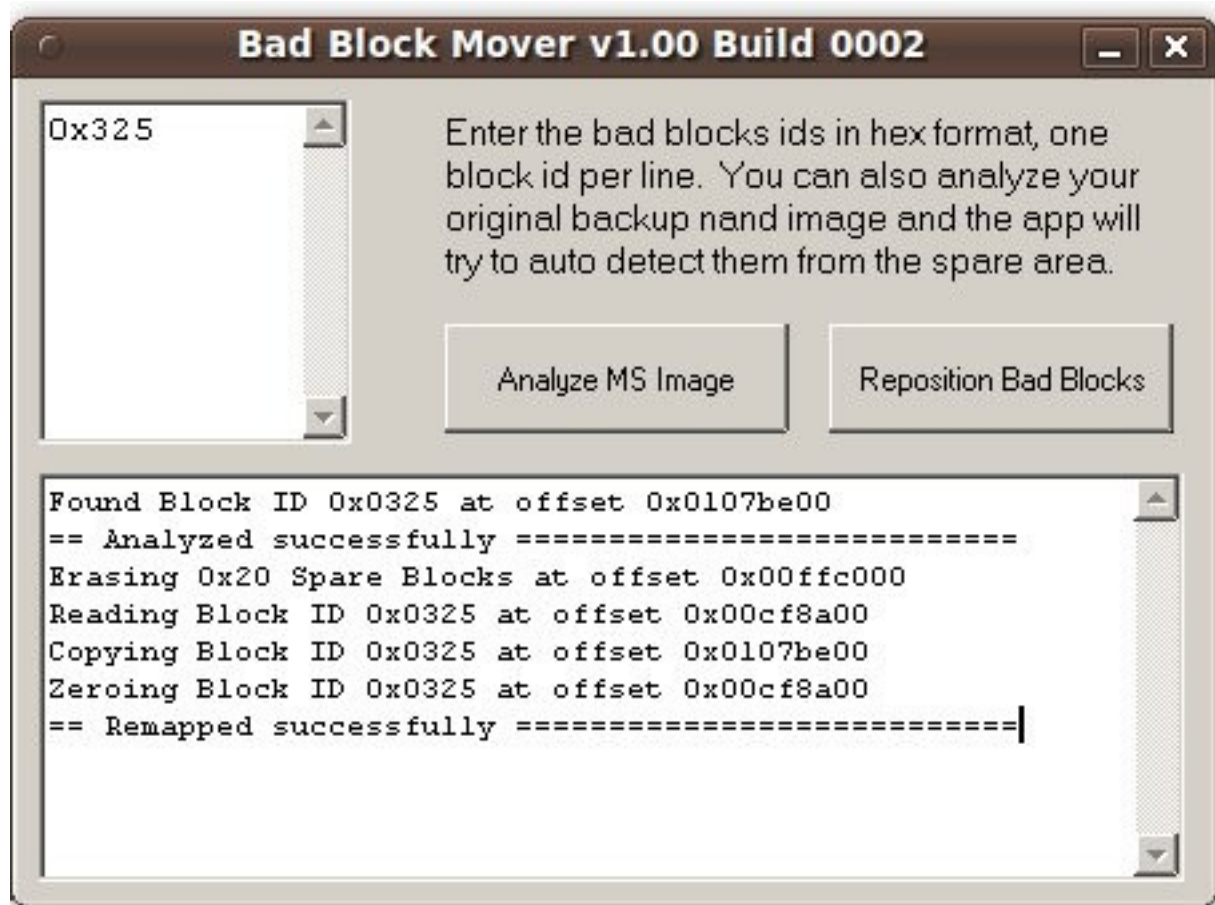
```
nandpro XBR.bin: -wXX rawkv.bin 1 1
```

(-rXX/-wXX is specific for your NAND-Size, for example Xenon/ Zephyr/ Opus/ Falcon and Jasper(16MB) would be -r16 and -w16)

To be safe its now recommended to run BadBlockMover which will remap bad blocks to the XBR Image so you won't get an error after flashing it.

Open BadBlockMover and click on "Analyze MS Image", then point the application to your orig.bin. It will analyze the Bad Blocks from your Original Image and will show them at the left box.

Now click on "Reposition Bad Blocks" and choose your XBR.bin. It will remap the Bad Blocks and show you something like this:



9. Flashing the Xbox-Rebooter Image

You can now flash the remapped XBR-Image.

To do this connect the power supply and the LPT flasher again, navigate with CMD to the NandPro-Directory and type the following:

```
nandpro lpt: -wXX XBR.bin
```

(-wXX is again specific for your NAND-Size)

Do something useful in this 40 minutes flashing procedure instead of watching at the screen which is counting blocks up :P

When it finished turn on the console and you should see the MS Dashboard coming up. Congrats, your Xbox runs unsigned code now :)

Tutorial by tuxuser

English editing by: Mad_Gouki

Credits go out to:

tmbinc, Tiros, Redline99, robinsod, stonersmurf, SeventhSon, Ge0rg, Oggy, Cr4zi3, EMAXX, Ced2911, [CoZ], sonic-iso, Fallen93, Jefff, jester`, ZeZu, Rad0x, B1gfoot, cpasjuste, Mad_Gouki, relapse, sandugas, GhaleonX, IceKiller, w3b, Millhouse, Moon666, Hoax, humba_, LAN-S, Warhammer and to all I maybe forgot ;)