

# XeLL-HACK (XBR)

XENON-ZEPHYR-FALCON-OPUS-JASPER

In diesem Tutorial beschreibe ich wie Ihr den XeLL-Homebrew-Hack auf eurer Konsole aufspielt.

## 1. Welche Xbox Revision habe ich?

Anhand des Netzteil-Anschlusses könnt Ihr die Revision eurer Xbox bestimmen.

Unterscheidung zwischen Xenon/Zephyr: Zephyr hat HDMI, Xenon nicht.

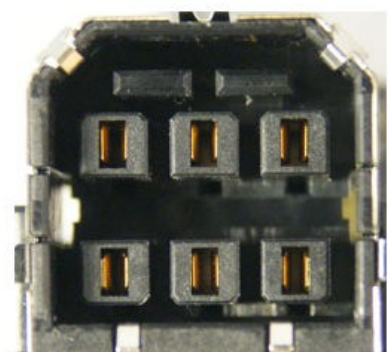
Unterscheidung zwischen Falcon/Opus: Falcon hat HDMI, Opus nicht.



Xenon/Zephyr  
1st Generation Xbox 360 (2005)



Opus/Falcon  
2nd Generation Xbox 360 (2007)



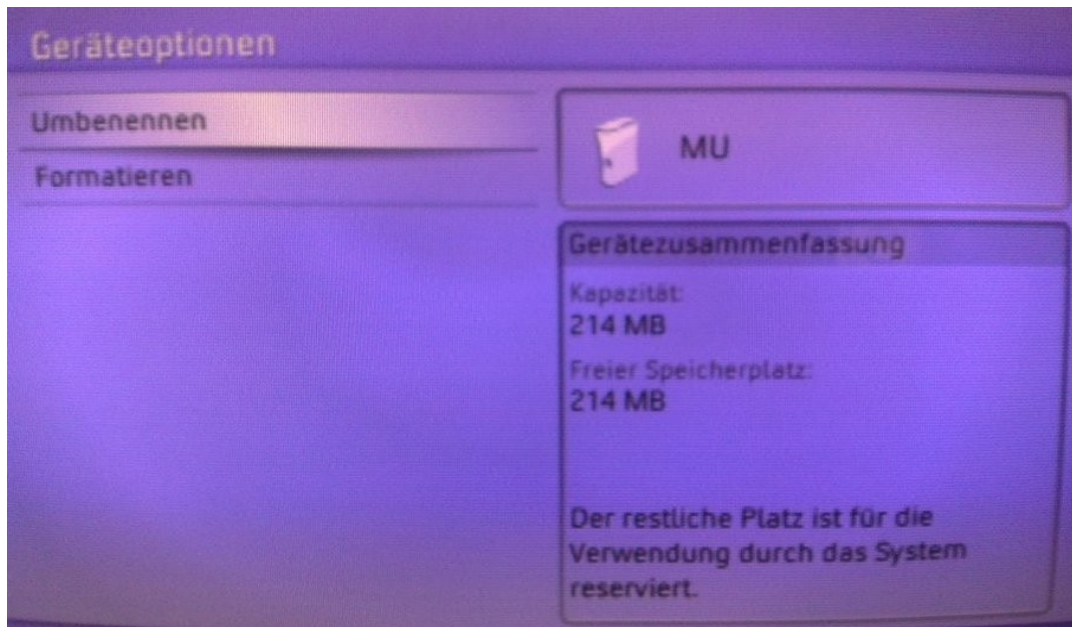
Jasper  
3rd Generation Xbox 360 (2008)

Hat man eine Jasper-Box so sollte man noch überprüfen welche NAND-Größe sie besitzt (NAND = Interner Flash-Chip der Xbox, auf dem das Dashboard gespeichert ist, bei Jaspers wird ein Teil des NANDs auch als interne Memory Unit gehandhabt).

Zieht eventuell vorhandene Speichermedien von der Xbox ab (HDD, Memory Unit etc.) und navigiert zu „Systemeinstellungen“, „Speicher“.

Wenn Ihr dort keine Speichereinheit seht besitzt Ihr eine Jasper Konsole ohne integrierte Memory Unit, also mit 16MB NAND.

Wird euch eine Memory Unit angezeigt (mit einem Symbol einer Xbox Konsole davor) drückt ihr die Y-Taste und eine Zusammenfassung des Speichermediums sollte erscheinen.



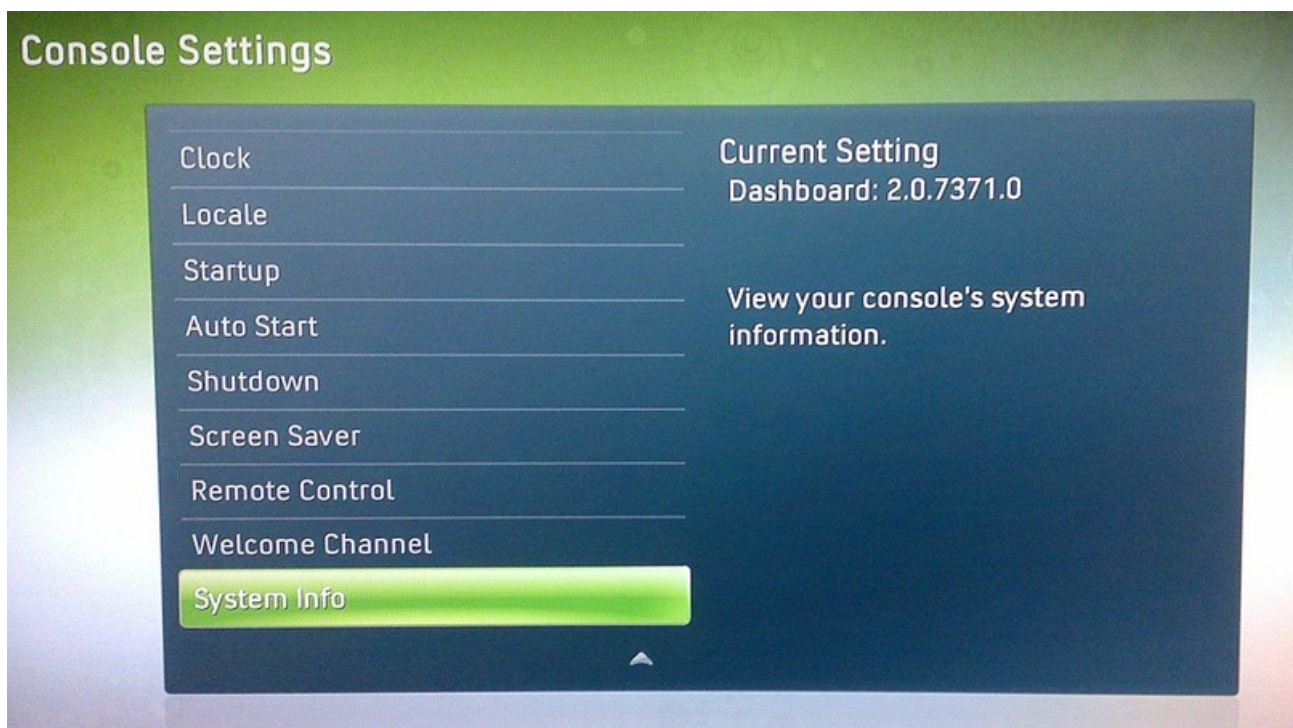
Identifizierung wie folgt:

Kapazität: 214MB = 256MB NAND

Kapazität: 451MB = 512MB NAND

## 2. Welche Dashboard-Version hat meine Konsole?

Als erstes müsst Ihr herausfinden welche Dashboard-Version eure Xbox360-Konsole hat. Dazu geht ihr auf „Systemeinstellungen“, „Konsoleneinstellungen“ und wählt dort „Systeminformationen“ aus. Unter Steuerung sollte euch so etwas wie „2.0.7371.0“ angezeigt werden.



**Bis hin zu Version 7371 ist es möglich den Hack durchzuführen, bei Dashboard-Version ab 8xxx leider nicht mehr.**

Bei Jasper, ab ca. Herstellungsdatum Juli, muss man erst noch den NAND auslesen um Gewissheit zu haben das der Hack klappt (den NAND sollte man aber sowieso, egal bei welcher Mainboard-Revision, vorher auslesen).

Also auf geht's :)

### **3.LPT Programmer basteln**

Für den LPT-Programmer benötigt ihr folgende Sachen:

Computer mit LPT-Anschluß (Druckerport)

Lötkolben (Feinlötkolben 15W o.ä.)

Lötzinn

Litze (Kabel) (reichelt-Artikelname: LITZE SW)

1x LPT-Stecker (reichelt-Artikelname: D-SUB ST 25)

5x 100 Ohm Widerstände (reichelt Artikelname: 1/4W 100)

1x 1N4148 Diode (reichelt Artikelname: 1N 4148)

optional:

Schrumpfschlauch oder Isoband

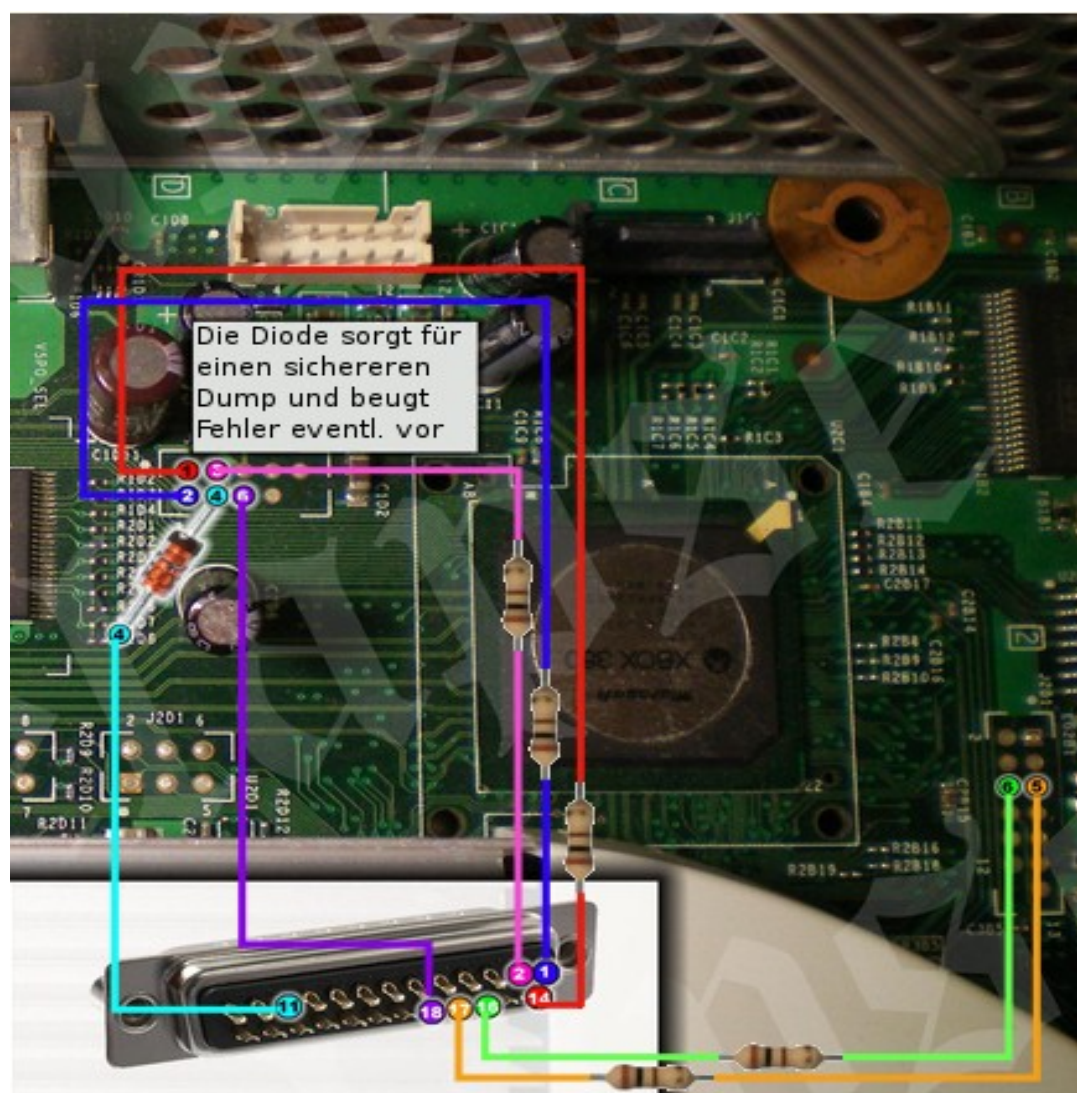
Später benötigt Ihr für die JTAG-SMC Verbindungen noch:

2x 1N4148 Dioden (reichelt Artikelname: 1N 4148)

Welche Ihr euch logischerweise direkt mitbesorgen solltet ;)

Lötet nun die Verbindungen anhand des folgenden Diagramms an den LPT Stecker und das Xbox-Mainboard. Nach dem kontrollieren auf Kurzschlüsse am LPT-Stecker und Mainboard (Sich berührende Lötkontakte o.ä.) isoliert Ihr am besten die einzelnen Pins am LPT-Stecker mit Isoband oder Schrumpfschlauch.





## 4.NAND auslesen

Nun, wenn Ihr alles richtig gelötet habt, kann es auch schon mit dem Auslesen des NAND-Speichers weitergehen.

Folgende Software ist nötig:

NANDPro (aktuell Version 2.0 b)

Infectus NAND Checker (aktuell Version 1.1)

MD5 Summer

360 Flash Tool (aktuell Version 0.91)

CD Info (aktuell Version 1b)

Geht als erstes in das NANDPro Verzeichnis und führt die Datei „port95nt.exe“ aus, startet dann den PC neu.

Klickt nun auf „Start“ → Ausführen und gebt in die Eingabezeile „command“ oder „cmd“ ein. Navigiert nun per „cd“-Kommando in euren NANDPro-Ordner (wenn ihr NANDPro z.B auf dem Desktop entpackt habt gebt ihr „cd Desktop/NANDPro ein).

Wenn Ihr euch nun im NANDPro-Ordner befindet könnt Ihr eure Xbox mit Strom versorgen (nur StandBy-Strom, also NICHT anschalten) und den angelöteten LPT-Stecker in den PC einstecken.

Führt nun NANDPro folgendermaßen aus:

## **Für Xenon/Zephyr/Opus/Falcon und Jasper(16MB NAND)**

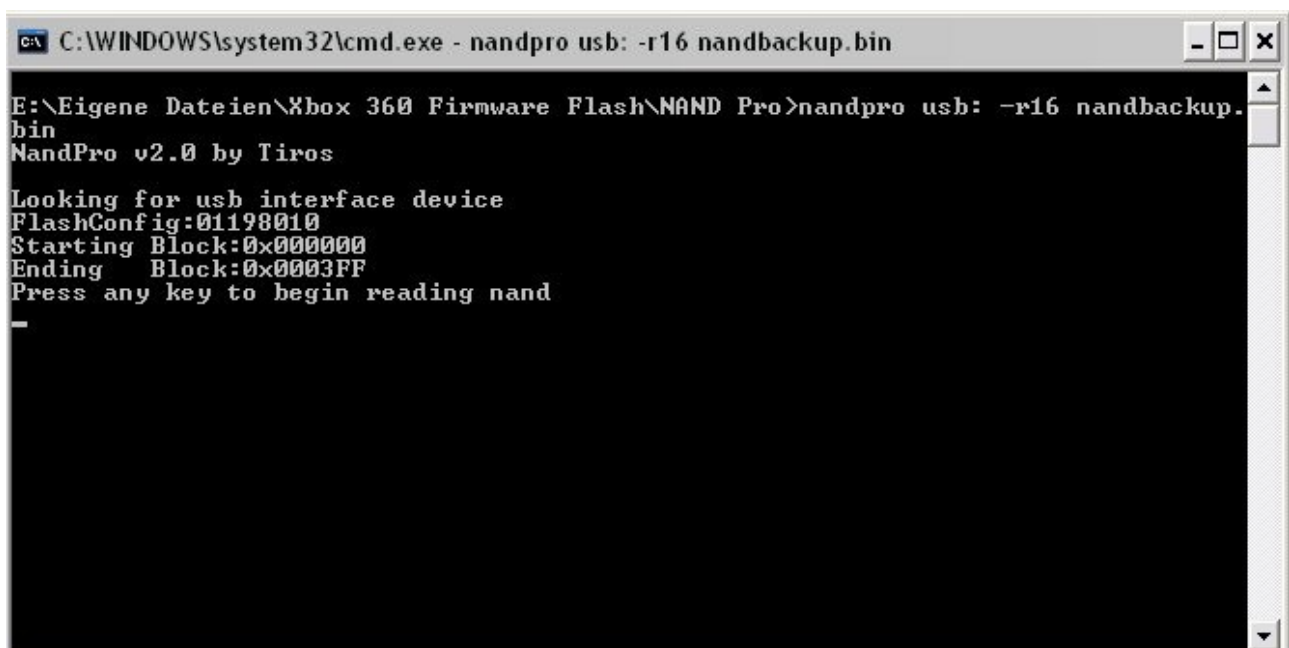
Nandpro lpt: -r16 nandbackup.bin

## **Für Jasper (256MB NAND)**

Nandpro lpt: -r256 nandbackup.bin

## **Und für Jasper (512MB NAND)**

Nandpro lpt: -r512 nandbackup.bin

A screenshot of a Windows command prompt window. The title bar reads "C:\WINDOWS\system32\cmd.exe - nandpro usb: -r16 nandbackup.bin". The command prompt shows the user typing "nandpro usb: -r16 nandbackup.bin" at the prompt "E:\Eigene Dateien\Xbox 360 Firmware Flash\NAND Pro>". The output of the command is displayed as follows:  
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  
A horizontal line is shown below the prompt.

```
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 sollte euch nun ein ähnliches Bild anzeigen.

Überprüft vor dem Auslesen nun die Flashcodes damit ihr nicht einen 40minütigen Auslesevorgang komplett umsonst macht.



## **Für Xenon/Zephyr/Opus/Falcon**

FlashConfig: 01198010

## **Für Jasper (16MB)**

FlashConfig: 00023010

## **Für Jasper (256MB)**

FlashConfig: 008A3020

256MB NAND Detected

## **Für Jasper (512MB)**

FlashConfig: 00AA3020

512MB NAND Detected

Ist euer Flashcode korrekt startet Ihr den Auslesevorgang mit dem Drücken einer beliebigen Taste.

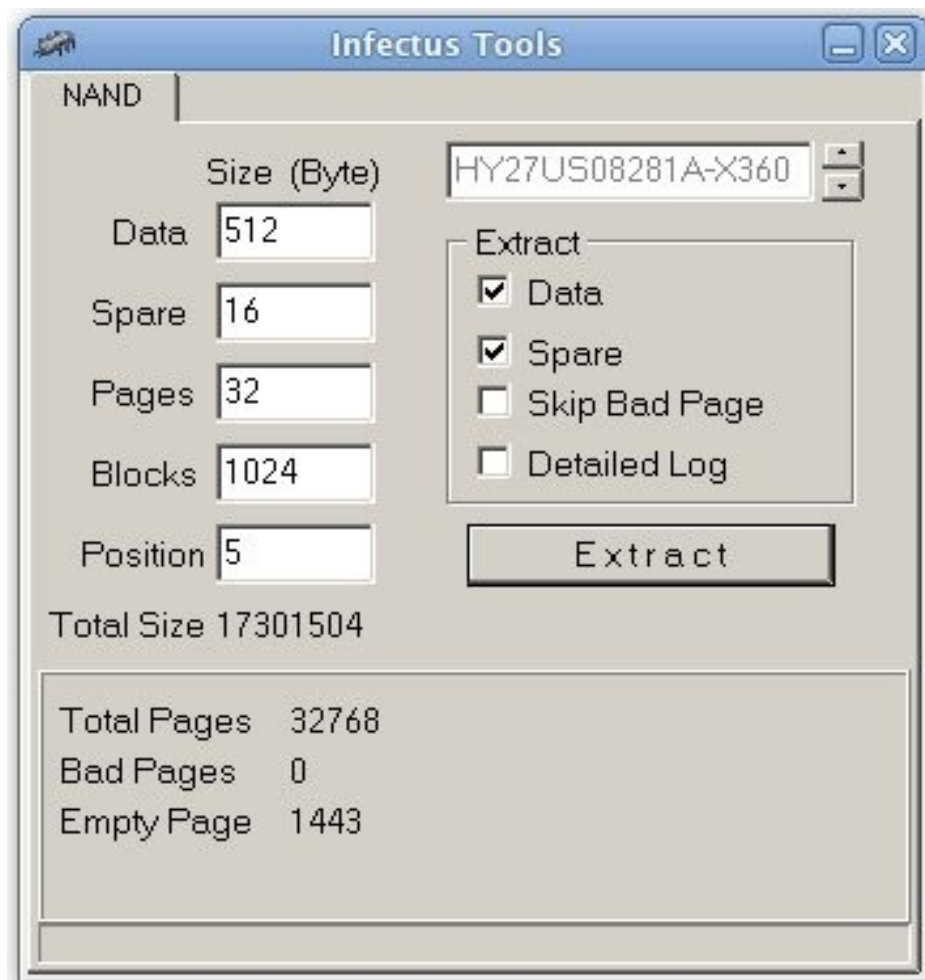
Am sichersten ist es ein paar Dumps zu machen und diese dann mit einem Checksum-Programm zu vergleichen.

Habt ihr identische Checksummen bei Euren Dumps erhalten überprüft diese, um ganz sicher zu gehen, noch mit dem NAND Checker.

Dieser unterstützt momentan leider nur 16MB Dumps, für größere Jasper Dumps gibt es also noch keine gute Möglichkeit diese zu überprüfen.

Startet also den Infectus NAND Checker, klickt auf „Extract“ wo ihr euren vorhin erstellten Dump auswählt und wartet bis dieser überprüft wurde.

Ein fehlerfrei ausgelesener NAND sieht so aus:



Es kann allerdings vorkommen das Ihr „Bad Pages“ bzw. „Bad Blocks“ beim Auslesen bekommt. Meldet euch dann einfach mit Eurem NANDPro-Log und der NAND Checker-Ausgabe im Forum, damit man feststellen kann ob die Anzahl und Position der fehlerhaften Daten kritisch ist.

Wenn nun alles im grünen Bereich ist muss man bei den Jasper Boards noch checken ob diese überhaupt „XeLL-fähig“ sind. Dazu öffnet man das kleine Tool „CD Info“, drückt auf „Open nand-backup“ und wählt folglich den NAND-Dump aus. Die Zeile „CD“ ist nun für euch von Bedeutung.



Hier eine Liste der kompatiblen CD-Versionen:

**Xenon: 1888, 1902, 1903, 1920, 1921**

**Zephyr: 4558**

**Falcon: 5761, 5766, 5770**

**Jasper: 6712, 6723**

Alle inkompatiblen Revisionen haben (zur Zeit) CD Version 8453.

Eure restlichen NAND-Infos erfahrt ihr mit dem „360 Flash Dump Tool“. Das Tool ist (zur Zeit) NICHT kompatibel mit Jasper 256MB/512MB Dumps, deswegen wurde eben CD Info benutzt.

Flash Tool wird beim ersten Start eine Dialog-Box mit Namen „Keys“ anzeigen, dort tragt ihr bei 1BL folgenden Key ein, hakt diesen an und startet danach das Tool neu.

**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

Wenn Ihr zu den glücklichen Usern mit einer kompatiblen Version gehört und euer NAND-Dump fehlerfrei war geht es nun mit dem Flashen des XeLL-Images weiter.

## **5.Flashen des XeLL-Images**

Besorgt euch das Image entsprechend eurer Xbox-Revision aus den üblichen Quellen, entpackt dieses und kopiert die bin-Datei (xenon/zephyr/falcon(opus)/jasper\_hack.bin) in das NANDPro Verzeichnis.

Wechselt nun wie gehabt per „Command-Prompt“ in das NANDPro-Verzeichnis und gebt folgenden Befehl zum Flashen des Images ein.

### **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

Wobei „xboxrev“ für eure Xbox-Revision steht, also xboxrev\_hack.bin Euer entsprechendes XeLL-Image angibt.

Ist das Flashen erfolgreich abgeschlossen (sollte ca. 5 Minuten dauern) trennt zuerst das LPT Kabel vom PC, dann das Netzteil von der Xbox.

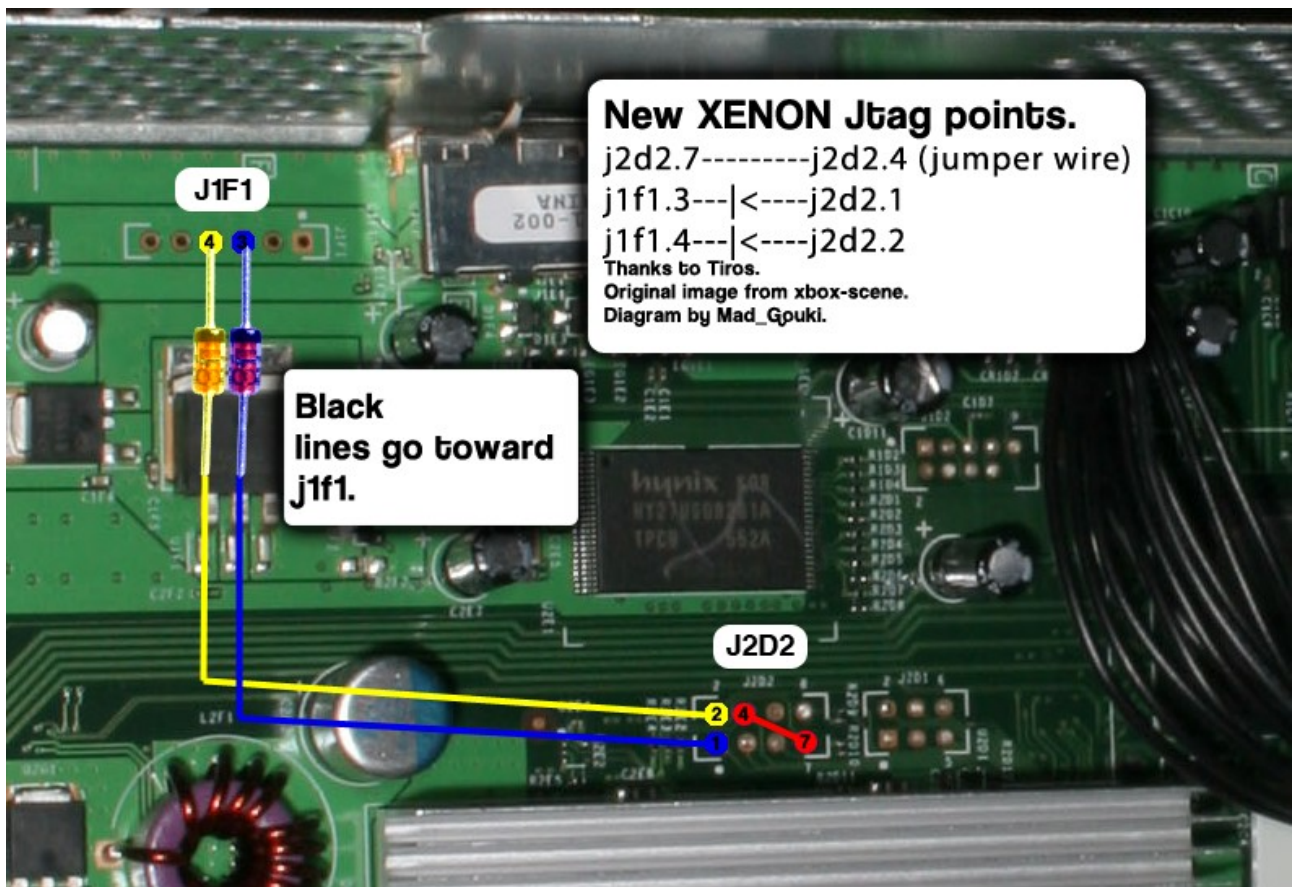
Nun ist es Zeit die SMC-JTAG Verbindungen einzulöten.

## 6. Lötén der SMC-JTAG Verbindungen

Baut nun, falls noch nicht geschehen, das Xbox Mainboard aus dem Gehäuse bzw. Gehäusekäfig aus. Legt euch 2 Dioden bereit.

Lötet nun nach folgendem Plan die Dioden ein:

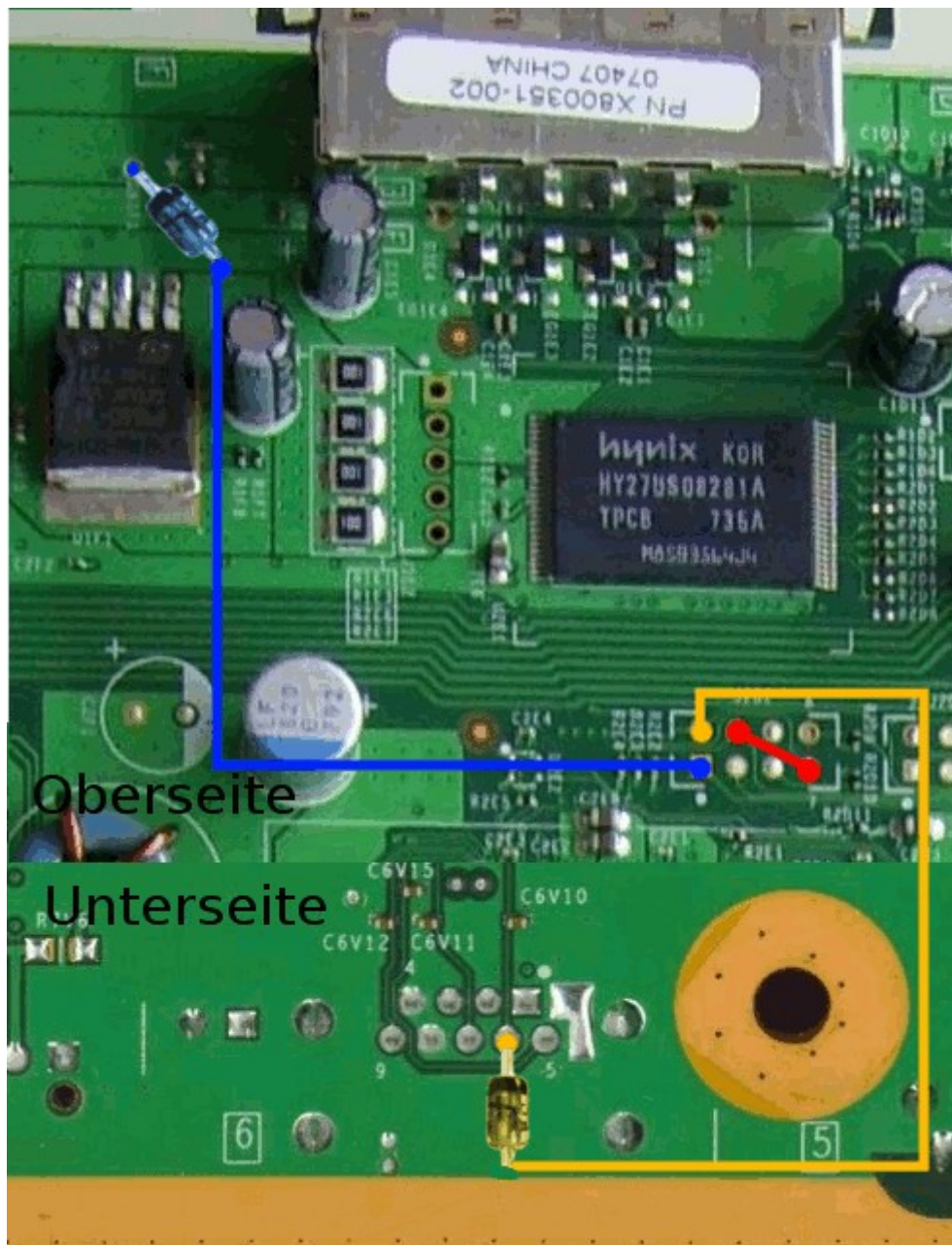
**Xenon:**



Anmerkung: Es existiert auch eine ältere Version der JTAG-SMC Verbindungen für Xenon Boards welche 3x330Ohm Widerstände nutzt. Die hier beschriebene Dioden Lösung ist jedoch um einiges sicherer.



## Zephyr/Opus/Falcon/Jasper:



Habt ihr nun die Verbindungen sauber eingelötet ist es Zeit zum Testen :)

Baut das Mainboard wieder in den Metallkäfig ein und schließt dann AV-Kabel (VGA, Composite oder YUV/Komponenten) und Netzteil an.

Beim Starten der Box solltet Ihr nun mit einem blauen Screen mit weißer Schrift begrüßt werden der etwa so aussieht

```
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
```

Ist dies der Fall habt Ihr es geschafft :)

Nun könnt ihr auch den LPT Programmer wieder auslöten.

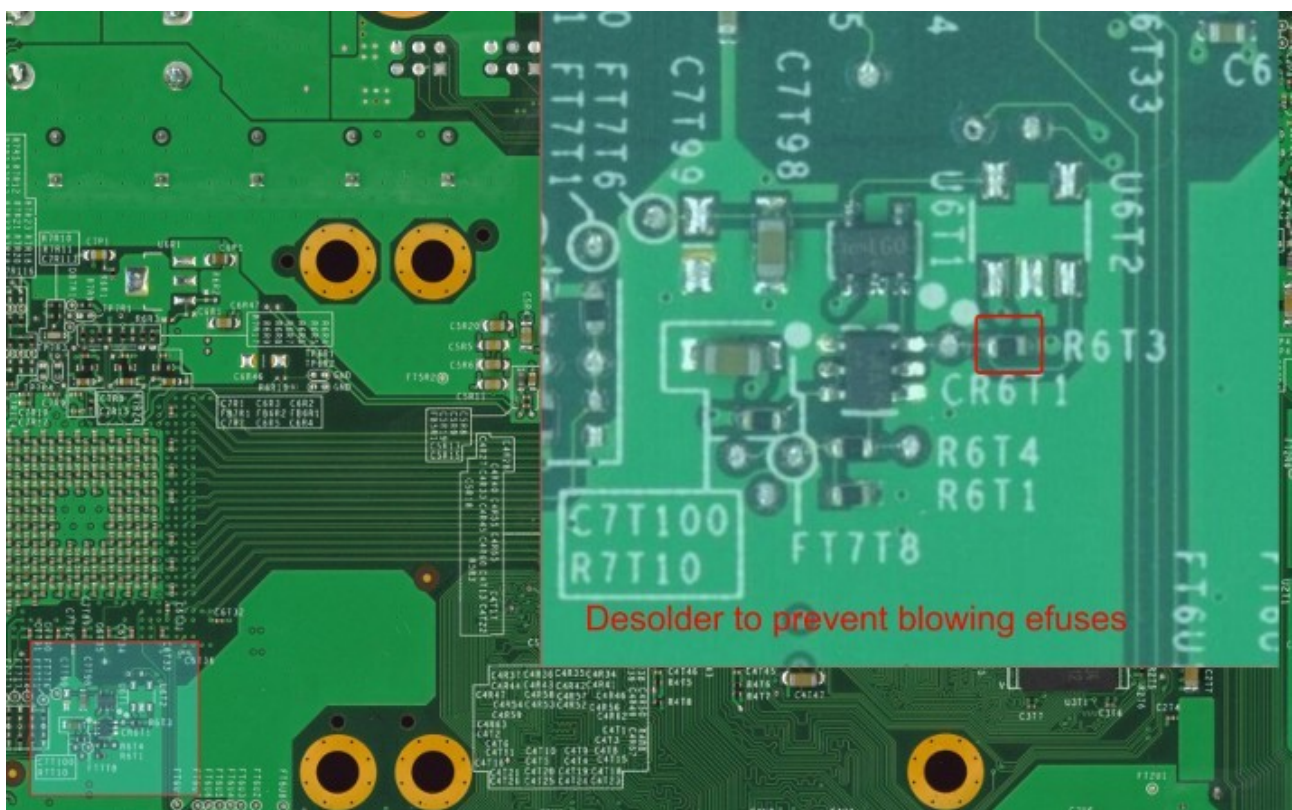
Ihr könnt nun diverse Emulatoren testen und Linux auf Eurer Konsole nutzen. Viel Spaß!



## 7.Optional: Auslöten des R6T3 Widerstands

Optional könnt Ihr nun noch den R6T3 Widerstand auslöten. Das Auslöten verhindert, dass man nach dem eventuellen Zurückflashen des Original Images nicht durch ein Dashboard-Update die Möglichkeit verhindert den XeLL-Hack auszuführen.

Das folgende Bild zeigt die Position des R6T3 auf der Unterseite des Mainboards



## 8. Xbox-Rebooter Image vorbereiten

Folgende Software ist dafür nötig:

Xbox-Rebooter-Image, passend für die Konsolen-Revision  
NANDPro v2.0b (! mindestens v2.0b !)

Eventuell, falls man unbehebbarer „Bad Blocks“ hat:  
Redline99's BadBlockMover (funktioniert momentan nur für nicht-Jasper Images)

Als erstes braucht Ihr euren Original Dump (orig.bin) und das XBR-Image im NANDPro-Ordner. Jetzt navigiert Ihr per Kommandozeile in diesen Ordner.

Um die rawkv.bin auszulesen tippt man folgendes:

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

Um diese in das XBR-Image zu schreiben:

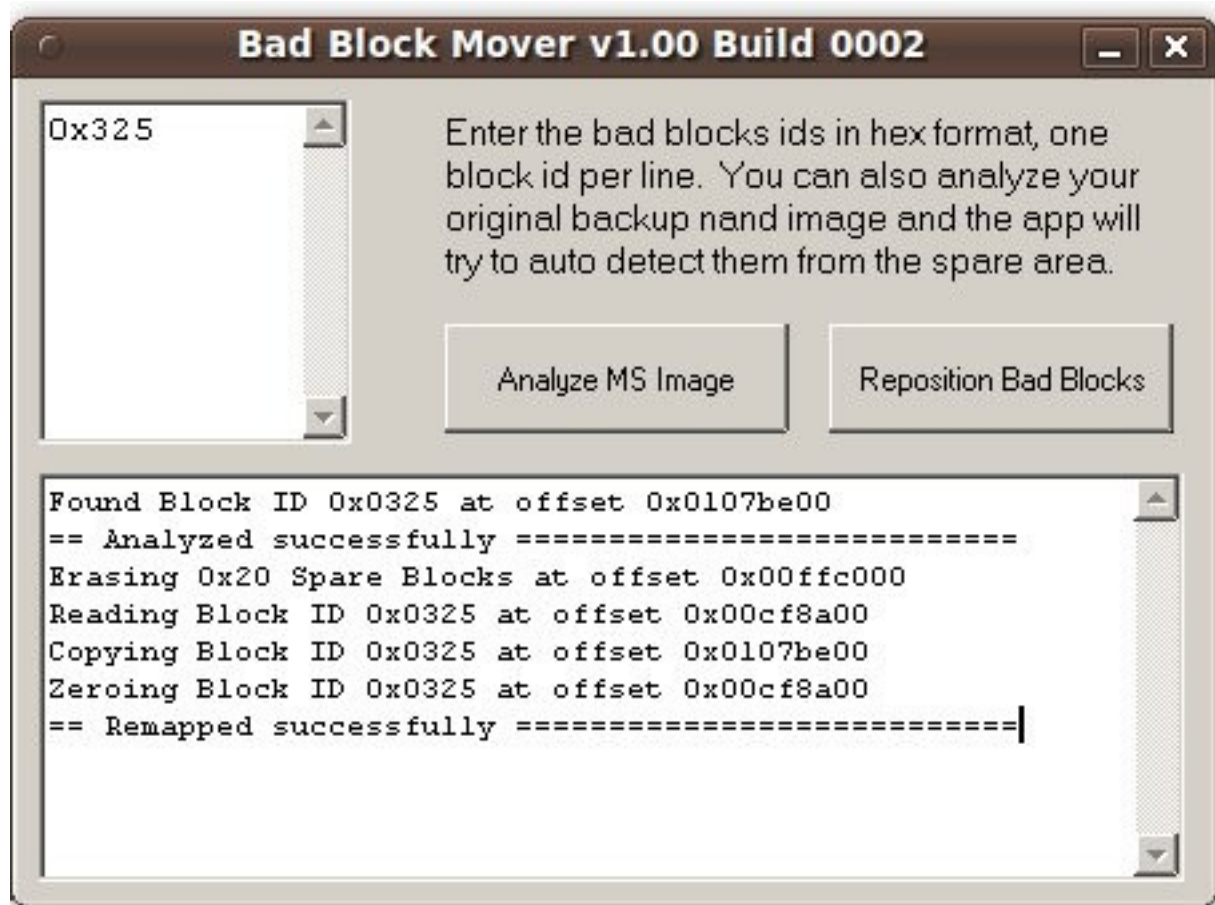
```
nandpro XBR.bin: -wXX rawkv.bin 1 1
```

(-rXX/-wXX ist spezifisch für die NAND-Größe, z.B. Xenon/ Zephyr/ Opus/ Falcon und Jasper(16MB) wäre -r16 und -w16)

Um sicher zu gehen das man nach dem Flashen keinen Fehler bekommt ist es ratsam „BadBlockMover“ zu nutzen, was die Bad Blocks im XBR-Image „remapped“.

Startet „BadBlockMover“ und klickt auf „Analyze MS Image“, wählt dann eure orig.bin aus. Nun werden die Bad Blocks analysiert und in der linken Box angezeigt.

Klickt nun auf „Reposition Bad Blocks“ und wählt eure XBR.bin aus. Eure Bad Blocks werden remapped und es sollte in etwa sowas angezeigt werden:



## 9. Flashen des Xbox-Rebooter Images

Ihr könnt nun das remapped XBR-Image flashen. Um dies zu tun schließt wieder das Netzteil und den LPT-Flasher an, navigiert in den NandPro-Ordner und tippt folgendes:

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

(-wXX ist wieder spezifisch für die NAND-Größe)

Macht nun was sinnvolles in diesen 40Minuten anstatt auf die hochzählenden Block-Nummern auf dem Bildschirm zu starren :P

Wenn es abgeschlossen ist schaltet die Konsole an und Ihr solltet das MS Dashboard starten sehen. Glückwunsch, Eure Xbox spielt nun unsignierten Code ab :)

Tutorial by tuxuser

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 ;)