Xbox360 Hacking Guide

by ITXtutor

Version 1.0
12.07.13

Intro

- No Piracy Talk
- No Illegal Links
- If you have questions please comment this video
- Do not use this for piracy – Support developers and buy the games.
- Modding is not illegal but Piracy is !
- Im not responsible for breaking your console

Hacking methods

- Flashing the Drive
  - Easy – Putting hacked firmware on Drive
- X360Key or Wasabi (ODDE)
  - No soldering modchip (Like flash)
  - Very easy
- JTAG
  - Old Phat < =7371
- RGH
  - New Slim´s supported
    - RGH1 and RGH2 (Do not do RGH2 on phat -> RJTAG)
    - Dual Nand
- R-jTAG
  - Phat consoles only + Dual Nand

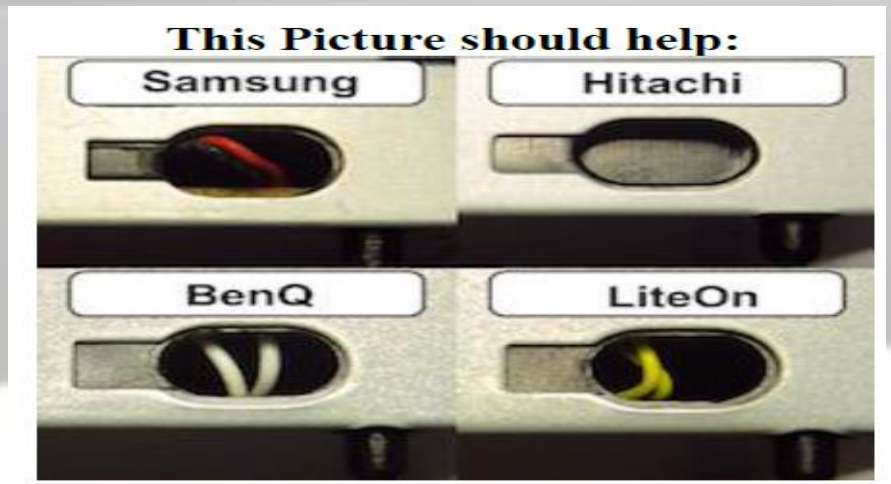
- (King Kong Exploit) <= Kernel 4548

Flashing the Drive

- **What can you do with this:**
  - **You can play backups**
  - **Play online and use xbox live (Ban risk)**
- **What you can´t do with it:**
  - **Run unsigned code**
    - **Software modding – Freestyle Dash - emulators**
  - **Free DLC and Arcade games**
  - **Play games from Harddrive**
  - **Install Bigger internal harddrive or use USB harddrive**
  - **….. All Jtag / RGH features.**

What drives are compatible ?

- 1. Determine your Drive brand and revision
- All Slim and Phat can be flashed!



Slim only:

Xbox 360 Drives

- **Phat:**

- **Hitachi FW*:** 32, 36, 40, 46, 47, 58, 59. 78 and 79
  Samsung FW: MS24, MS25
  BenQ FW: 62430C, 64930C
  Liteon FW: 74850C, 83850Cv1, 83850Cv2, 93450C

- **Slim:**

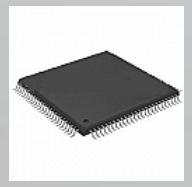
- **Liteon DG-16D4S** FW: 9504/0272, 0225, 0401, 1071,
- **Liteon DG-16D5S** FW: 1175, 1214 and 1532 (1532 are always in the redesigned Slim – Xbox 360 E)

- **Hitachi FW:** 0500, 0502

- **9504/0272** PCB got locked after Dash13599 -> need replacement PCB or hack

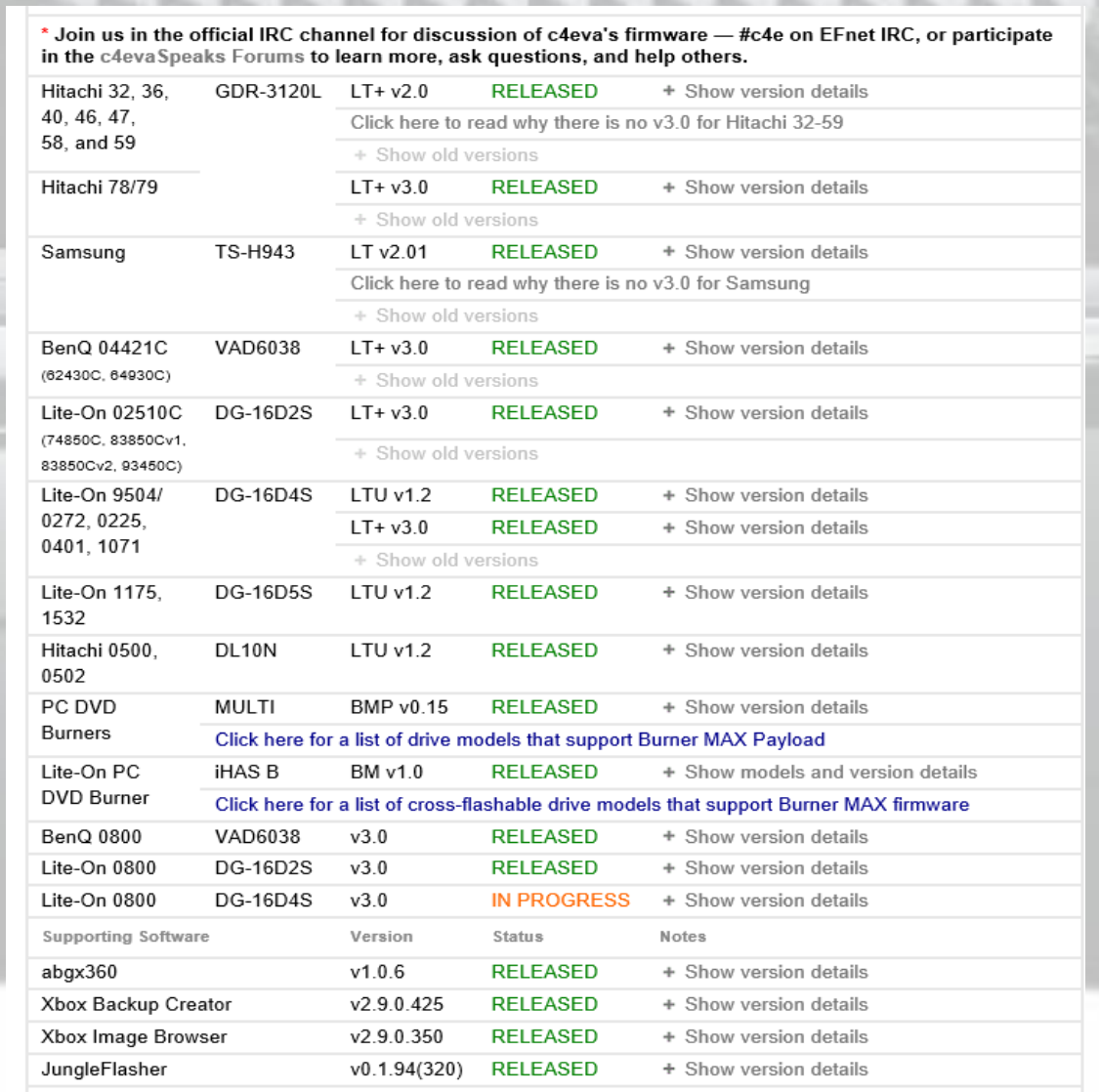
How does it work ?

- 1. Reading the **key of your Drive**
  - **Phat**
    - **All Drives easy to read (Only liteon needs Probe)**
  - **Slim**
    - **Drives** 9504/0272, 0225, 0401, 1071 are easy to read
    - **Drives** 1175, 1214 and 1532 and all Hitachi need RGH to get the key !
- 2. Flashing a **Custom Firmware** by C4eva
  - Unlocked PCB (replacement) or chip for pro installers
  - Unlocking the PCB on your own (Only 9504/0272, 0225, 0401, 1071)



Firmware

- Firmware pack c4eva
- LT+ 3.0
- LTU 1.2
- Need Xecuter Unlocked PCB
- Or hacked PCB



* Join us in the official IRC channel for discussion of c4eva's firmware — #c4e on EFnet IRC, or participate in the c4evaSpeaks Forums to learn more, ask questions, and help others.

Hitachi 32, 36, 40, 46, 47, 58, and 59	GDR-3120L	LT+ v2.0	RELEASED	+ Show version details
		Click here to read why there is no v3.0 for Hitachi 32-59		
		+ Show old versions		
Hitachi 78/79		LT+ v3.0	RELEASED	+ Show version details
		+ Show old versions		
Samsung	TS-H943	LT v2.01	RELEASED	+ Show version details
		Click here to read why there is no v3.0 for Samsung		
		+ Show old versions		
BenQ 04421C (62430C, 64930C)	VAD6038	LT+ v3.0	RELEASED	+ Show version details
		+ Show old versions		
Lite-On 02510C (74850C, 83850Cv1, 83850Cv2, 93450C)	DG-16D2S	LT+ v3.0	RELEASED	+ Show version details
		+ Show old versions		
Lite-On 9504/ 0272, 0225, 0401, 1071	DG-16D4S	LTU v1.2	RELEASED	+ Show version details
		LT+ v3.0	RELEASED	+ Show version details
		+ Show old versions		
Lite-On 1175, 1532	DG-16D5S	LTU v1.2	RELEASED	+ Show version details
Hitachi 0500, 0502	DL10N	LTU v1.2	RELEASED	+ Show version details
PC DVD Burners	MULTI	BMP v0.15	RELEASED	+ Show version details
	Click here for a list of drive models that support Burner MAX Payload			
Lite-On PC DVD Burner	iHAS B	BM v1.0	RELEASED	+ Show models and version details
	Click here for a list of cross-flashable drive models that support Burner MAX firmware			
BenQ 0800	VAD6038	v3.0	RELEASED	+ Show version details
Lite-On 0800	DG-16D2S	v3.0	RELEASED	+ Show version details
Lite-On 0800	DG-16D4S	v3.0	IN PROGRESS	+ Show version details

Supporting Software	Version	Status	Notes
abgx360	v1.0.6	RELEASED	+ Show version details
Xbox Backup Creator	v2.9.0.425	RELEASED	+ Show version details
Xbox Image Browser	v2.9.0.350	RELEASED	+ Show version details
JungleFlasher	v0.1.94(320)	RELEASED	+ Show version details

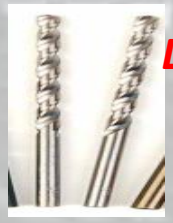
What you need for flashing

- **Phat Xbox:**
  - Your Drive (Open Xbox – Check link)
  - A Power source for the drive
    - Xbox (FLAG ?) or CK3 , Ck3i , ck3 mini , X360USBPRO, maximus lizard..
  - **Option1 :** A Computer
    - SATA ports on mainboard or PCI cardand Sata cable
  - **Option 2:** Laptop or Computer with X360USBPRO V2
  - **Optional:** Probe for reading Liteons (check out my video)and philips screw driver

+Flash package including Firmwares

What you need for flashing DG-16D4S

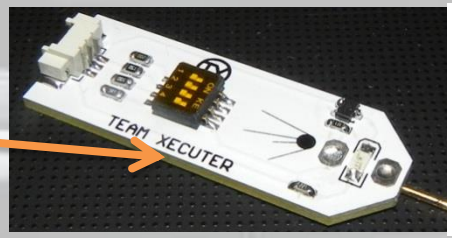
Only for DG-16D4S 9504/0272, 0225,0401 and 1071

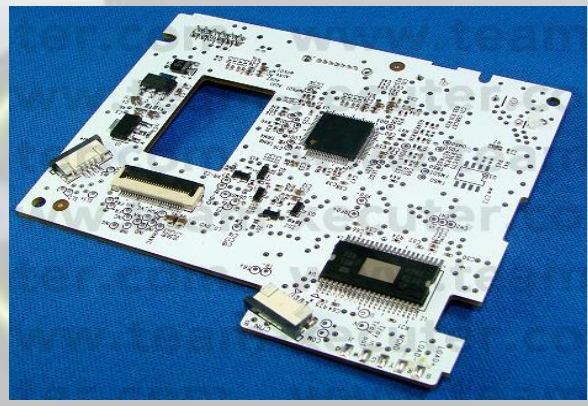


Drills or Soldering Iron

Sputnik probe or selfmade

- **Slim Xbox:**
  - **Windbond/kamikaze Hack**
  - **MXIC**
  - **Replacing PCB**

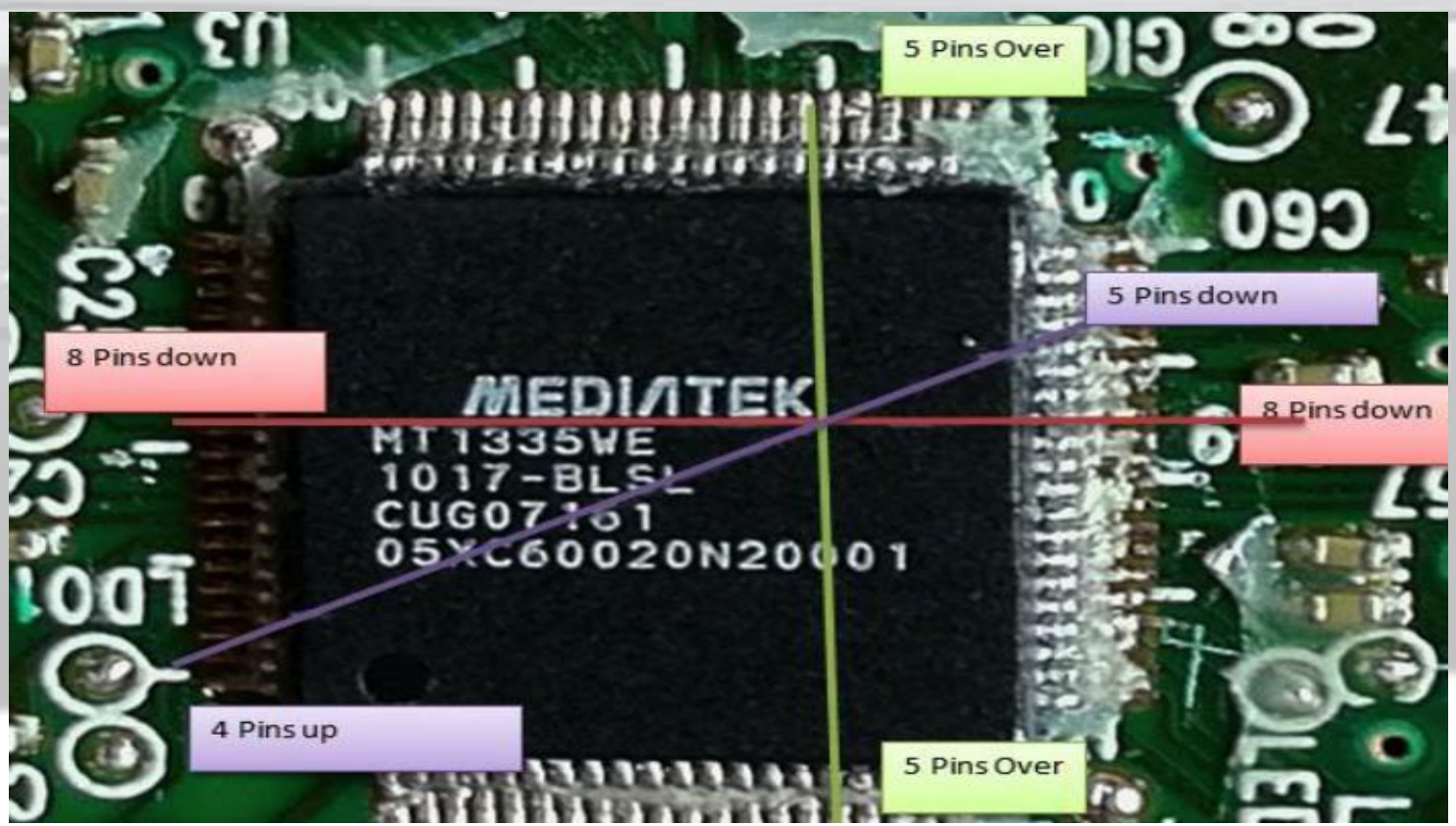




- **And A X360USBPRO V2 or Maximus Lizard + A PC or Notebook !**

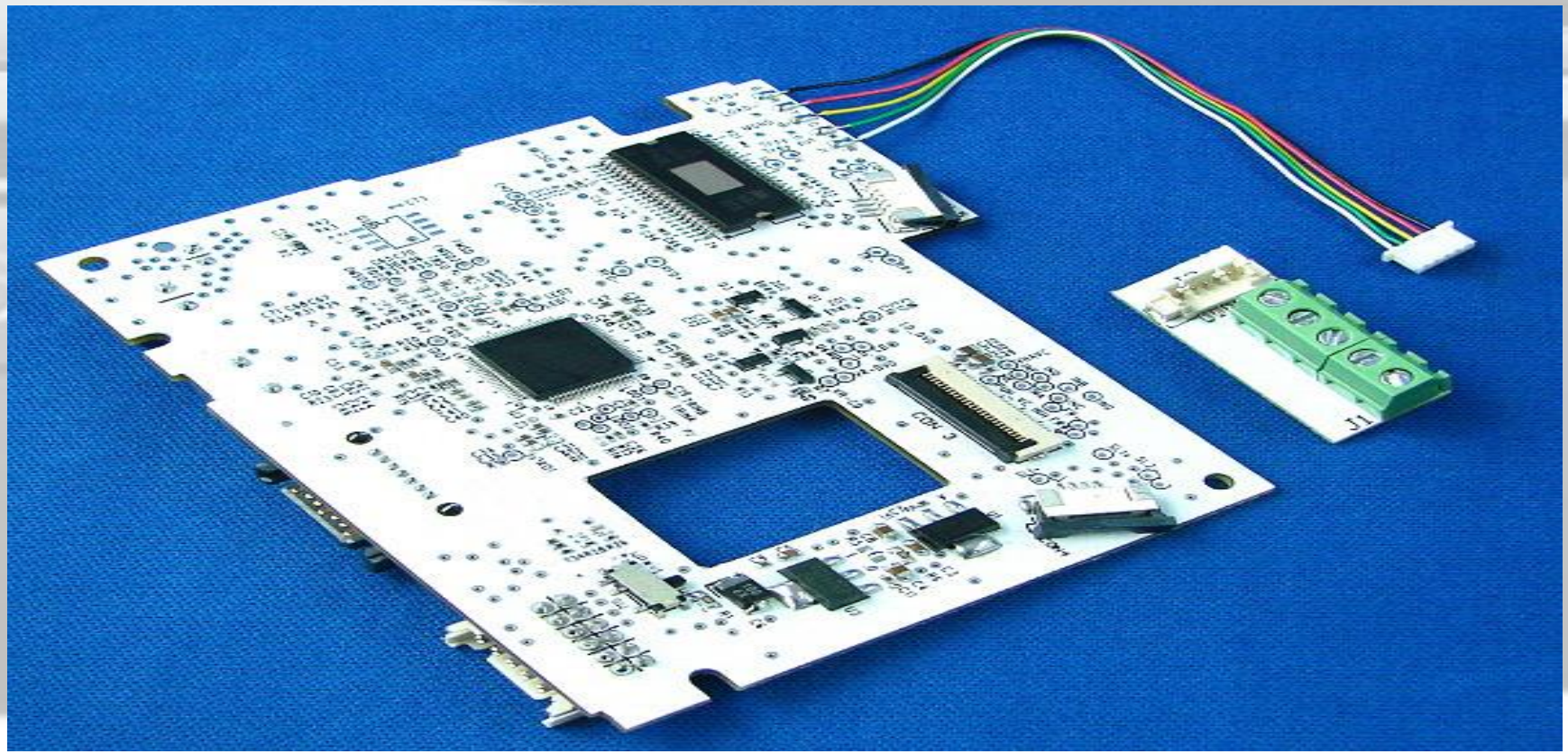
Winbond Kamikaze Hack

- Drilling the hole is risky
- May consider buying a replacement PCB



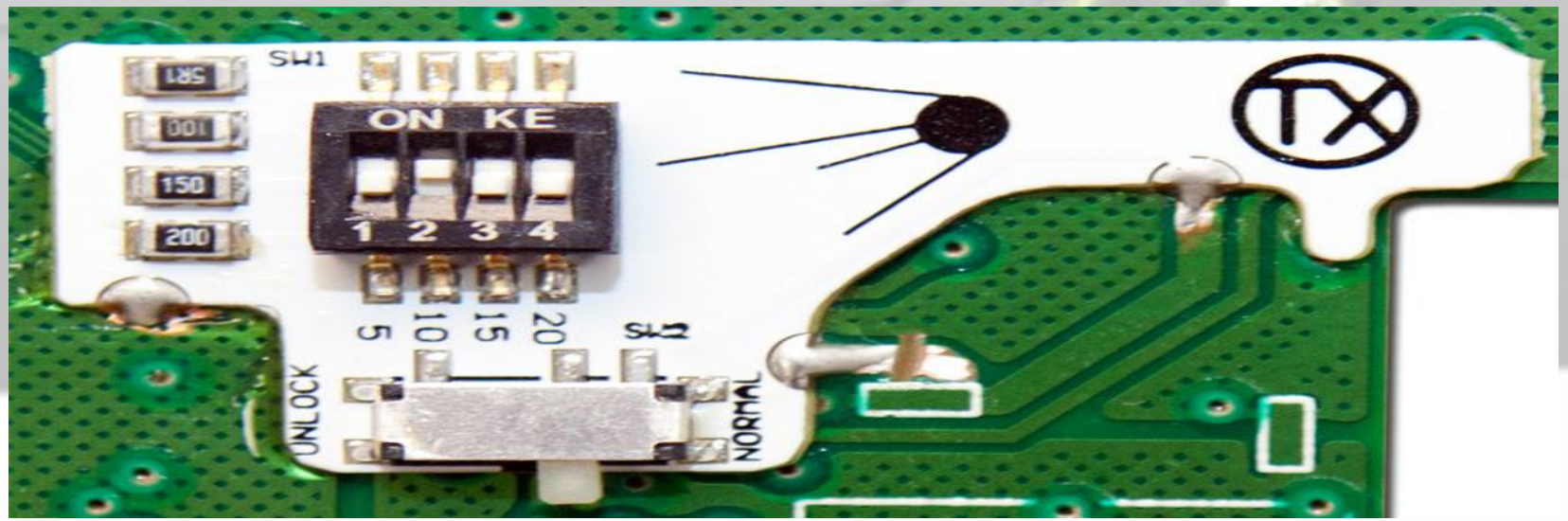
Winbond Replacement

- **Xecuter DG-16D4S Unlocked PCB:**



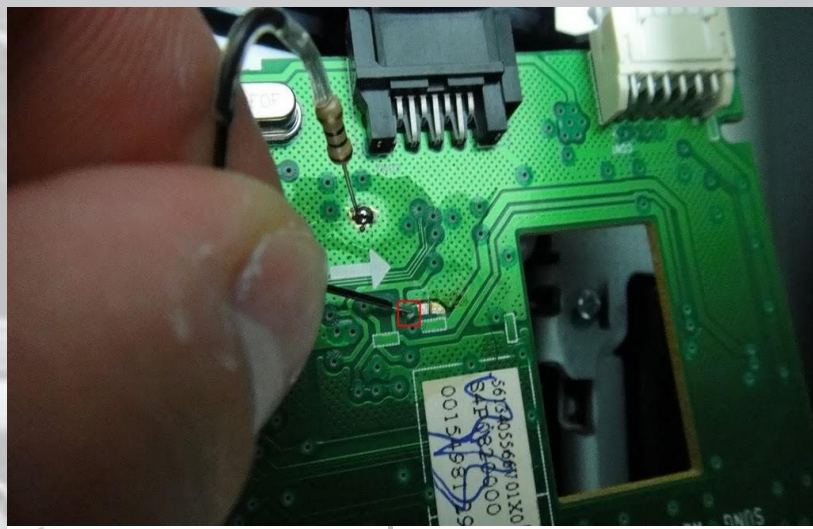
MXIC Hack

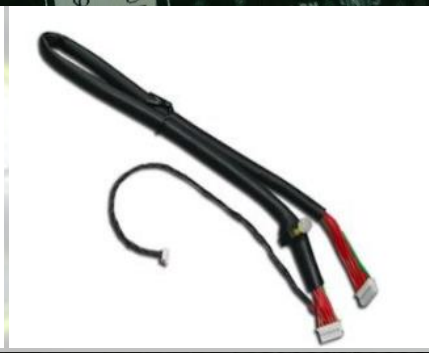
- **MXIC can be unlocked with the SPUTNIK360 Unlock Switch:**
- **Activates firmware flash**
- **Only 3 solder points**



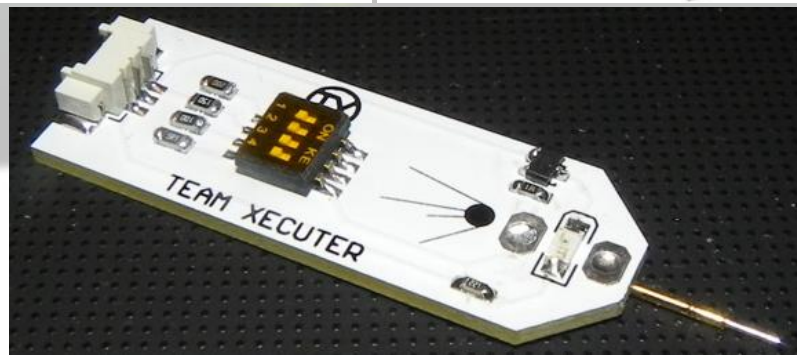
MXIC Hack

- But need to cut copper lines
- And solder /desolder wires
- Stuff you will also need →





- + X360USBPRO V2 or Lizard



- **Or buy Replacement PCB**

What you need for flashing DG-16D5S and Hitachi

- **TX LITEON DG-16D5S - REPLACEMENT PCB 1175+**
- Any **Glitch Chip** (CoolRunner, CR3 Lite, CR3 PRO, DGX) (Any one, all of them work fine)
- **A way to read/write nand**
  - For All 16Mb console
    - **Nand-X** or **JR-Programmer**
  - **OR**
    - **4GB R/W Kit for 4Gb Coronas**
    - A compatible **SD card reader**
    - **CORONA POSTFIX ADAPTER** (if needed, check link above)

Do i need post out fix ?

1: NAND IDENTIFICATION

The following information is correct to the best of our knowledge. There may be variations or inconsistencies, but from the hundreds of boards we have tested, this info is pretty solid.
Note: Corona V5 & V6 are from the XBOX 360E and basically the same as the v3 & v4

CORONA V1 (WITH 250GB HDD)

16MB NAND - (HYNIX or ST TSOP)
Standard NAND R/W (NAND-X, JR Programmer etc)
Standard POST_OUT

CORONA V2 (WITHOUT HDD)

4GB EMMC NAND (PHISON CONTROLLER - NAND IS UNDER MOBO)
4GB NAND R/W SD KIT Required
Standard POST_OUT
There are reports of POST_OUT being removed on some of these v2 models, therefore simply follow the POSTFIX ADAPTER info from v3 and v4.

CORONA V3/V5 (WITH 250GB HDD)

16MB NAND (HYNIX or ST TSOP)
Standard NAND R/W (NAND-X, JR Programmer etc)
NO POST_OUT - POSTFIX ADAPTER REQUIRED

CORONA V4/V6 (WITHOUT HDD)

4GB EMMC NAND (HYNIX/SKhynix or SAMSUNG BGA)
4GB NAND R/W SD KIT Required (New V4 QSB is also available)
NO POST_OUT - POSTFIX ADAPTER REQUIRED

What you need for flashing DG-16D5S and Hitachi

- **X360USB PRO** (v2 recommended, or ck3i)
- If the drive is DL10N a **slim Lite-On chassis**
  - **PCB wont fit in Hitachi case!**
- A molex/sata power adapter to power x360usb/ck3i/whatever
- + **Softwarepack (JF , J-runner ….)**

How does it work ?

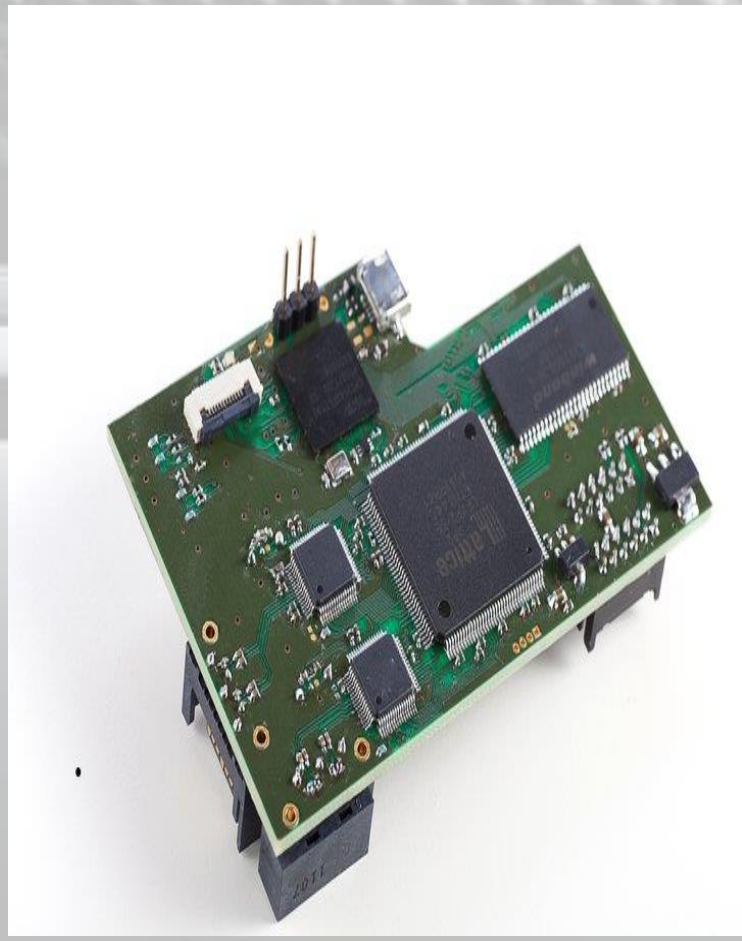
- Get a valid dump of your nand
- Get the cpukey
- Build the fw and write it to the replacement pcb

- On hitachi – you need the liteon case and PCB will be spoofed to hitachi

ODDE

- **Optical Disc Drive Emulator**

- Mainly:
  use an external HDD to store your game ISO's
- Play backups
- every Slim 360 is emulated for it but some drives require extra steps.,
- Liteon 1175 and Hitachi 0500/0502 both need you to RGH to obtain your CPU key + FCRT.bin



X360Key

- **Do not play online (High risk of ban !)**
  - Work in progress
- Play games from USB harddrive
- No Soldering
- No drive flashing or JTAG hack required
- Backup original Xbox 360 games to USB hard drive
- Compatible with both Fat and Slim models
- Easy to install

Wasabi 360

- Solderless installation
- Automatic Key extraction
- ESATA interface is used in place of USB providing superior performance
- Cool design

- **No xbox live Compatibility (coming soon)**

- Compatible with both Fat and Slim models

JTAG , RGH and R-JTAG

- Hacking the NAND of the xbox 360
- Requires Additional Hardware
- Good Soldering Skills
- Additional tools
- Higher Danger of Breaking your console (BRICK)
- Allows running unsigned code

Features

- Play almost any Xbox 360 game and DLC for free
- Use custom dashboards
- Use any sized hard drive in the hard drive port OR any sized external hard drive through USB
- Mod many games
- Use custom apps and games
- Take screenshots or video of your console without a capture card
- Make your console run the same software as development kits
- Rip games to your hard drive and never need the discs
- Play ANY original Xbox game
- Run linux on your xbox
- Play a variety of emulators such as: Recover your DVD key
- **RGH ONLY:** Use a DemoN to do a dual NAND setup and have two consoles in one. **DOESNT WORK ON CORONA V2's/V4's**

Materials and Tools

- A Soldering iron + Solder
- Desoldering Tool
- Torx 10 and 8 and Flathead
- A case opening tool
- Flux
- Multi-meter
- Hot glue gun
- A lighter/Heat-gun
- A Windows XP/Vista/7 computer
- Some form of wire
- Heat-shrink/Electrical Tape
- Isopropyl alcohol
- Thermal Paste

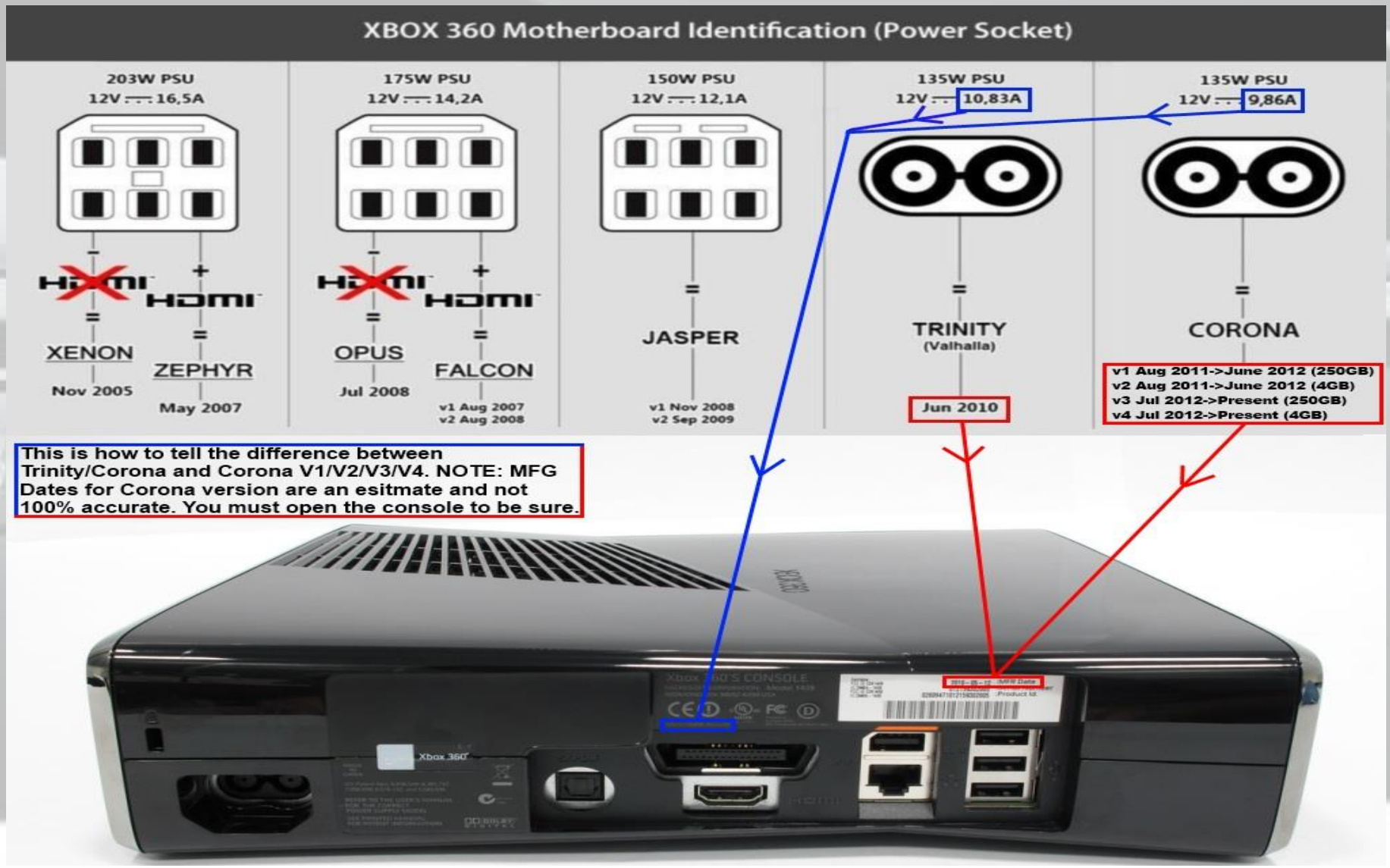
- RGH Chipboards and Nand Extractor

Steps

- **Dumping the NAND**
  - Basically OS/BIOS Copy
- **Hack itself**
  - Bypass the security System of the XBOX

- To do this steps we need **to Identify our Xbox** 360

Identifying your Mainboard



Identifying your Mainboard

- **If you have a redesigned slim (Xbox 360 E)**
  - It´s a corona
    - 250GB = V5
    - 4GB = V6

Is my console JTAG/RGH able ?

Dashboard exploit checker
Martin C
Correct as of 06/05/2013

Dashboard Version	Likely CB Version (not Gospel so dump the NAND and check in J-Runner!)	Xenon	Zephyr	Falcon / Opus	Jasper	Trinity	Corona	Notes
2.0.4532 - 2.0.7371	1888, 1902, 1903, 1920, 1921, 8192 4558, 4540, 4570, 4580 5760, 5761, 5766, 5770 6712, 6723							Follow JTAG guides
2.0.8498 - 2.0.14699	1922, 1923, 1940, 7373, 7375 4571, 4572, 4578, 4579 5771 6750, 6751 9188 13121	1						
2.0.14717 - 2.0.14719	1941 4576, 4577 5772, 5773 6752, 6753 9230 13180							
2.0.15572 - 2.0.16203	1942 4569, 4574 5774 6754 9231 13181		2	2	2			

Key:

JTAG	
RGH	
RGH2	
R-JTAG	

Notes:

1 - RGH usable for DVD key recovery only
2 - Whilst RGH2 will work on phat consoles,
we recommend R-JTAG for a far better boot experience.

V5 and V6 Xbox 360 E is RGHable too !

	16203≥Dash>14719	Dash=14719	Dash=14699	14669>Dash>7371	Dash=7371	Dash<7371
Xenon	Not Exploitable	Dvd Key Only	Dvd Key Only	Dvd Key Only	May be JTAG'able	JTAG
Zephyr	R-JTAG	R-JTAG	May be RGH1	RGH1	May be JTAG'able	JTAG
Falcon	R-JTAG	R-JTAG	May be RGH1	RGH1	May be JTAG'able	JTAG
Opus	R-JTAG	R-JTAG	May be RGH1	RGH1	May be JTAG'able	JTAG
Jasper	R-JTAG	R-JTAG	May be RGH1	RGH1	May be JTAG'able	JTAG
Jasper BB 256MB	R-JTAG	R-JTAG	May be RGH1	RGH1	May be JTAG'able	JTAG
Jasper BB 512MB	R-JTAG	R-JTAG	May be RGH1	RGH1	May be JTAG'able	JTAG
Trinity	RGH2	RGH2	RGH2	RGH2	N/A	N/A
Corona V1	RGH2	RGH2	RGH2	RGH2	N/A	N/A
Corona V2	RGH2	RGH2	RGH2	RGH2	N/A	N/A
Corona V3	RGH2	RGH2	RGH2	RGH2	N/A	N/A
Corona V4	RGH2	RGH2	RGH2	RGH2	N/A	N/A

JTAG

- Nand Dumping
- Easy, only requires 3 wires and a diode
- Cheap: Only cost is a diode, and wires.
- Normal boot times
- Can only be done on phats (RROD) with the dashboard 7371 or below
- Cannot run Xecuter Fusion

Dashboard

- Dashboard **1888** -> First dash (very unlikely that you have it ;))
- Dashboard **2241** Launchday dash (If you have it till launch and never updated)
- Dashboard **4532** and **4548** -> King kong exploit
- Dashboard **7371** and lower -> JTAG ABLE ! Do not update if you want to JTAG
- Dashboard **14699** and lower -> RGH 1
- Dashboard **14717 14719** -> RGH 2 (slim style hack)
- Dashboard **15572**, **15574**, **16197, 16202, 16203** are hackable with the newly released ECC files.
  They use the same method as the RGH2.

I STILL ADVISE YOU TO NOT UPDATE TO ANY DASH AFTER 14717 IF YOU WANT TO GLITCH YOUR 360, it's cheaper and RGH1 (for dashes below 14717) has far better boot times. On fat use R-JTAG !

Dashboard

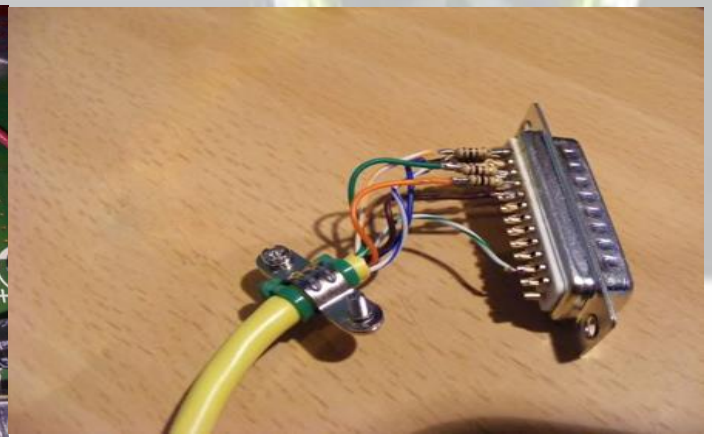
- **If you are exactly on 7371:**
  - Need to determine if jtagable
  - Nand Dump and check with J-Runner
  - Nand Info section -> Check CB

  - **Look at what your CB is and see if it is in this list:**
    -Xenon: 1922, 1923, 1940, 7373
    -Zephyr: 4571, 4572, 4578, 4579, 4580
    -Falcon/Opus: 5771
    -Jasper: 6750

If your CB is on the list -> Its patched and NOT JTAGABLE!

Nand Dumping

- **LPT Method:**
  - **Cheap**
  - **Involves soldering 7 wires to the Xbox and an LPT**
  - **Slow and Needs PC with LPT**
  - **Takes some more time because you have to make it** (you can buy one though if you want)
  - All Phat and Slim excl. Crona V2/V4

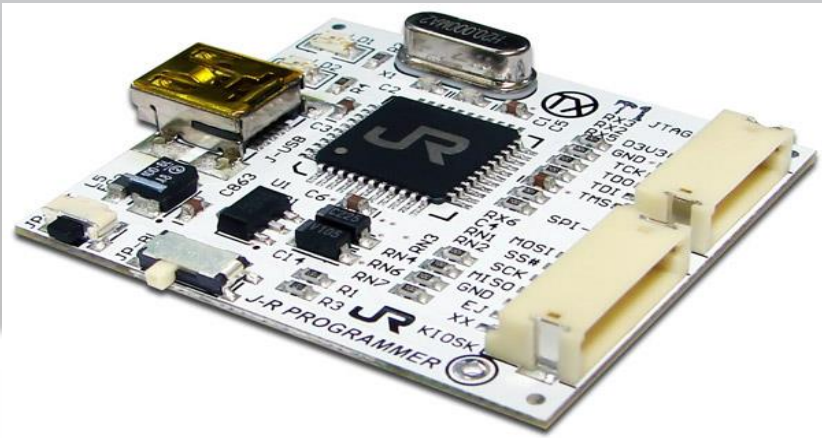


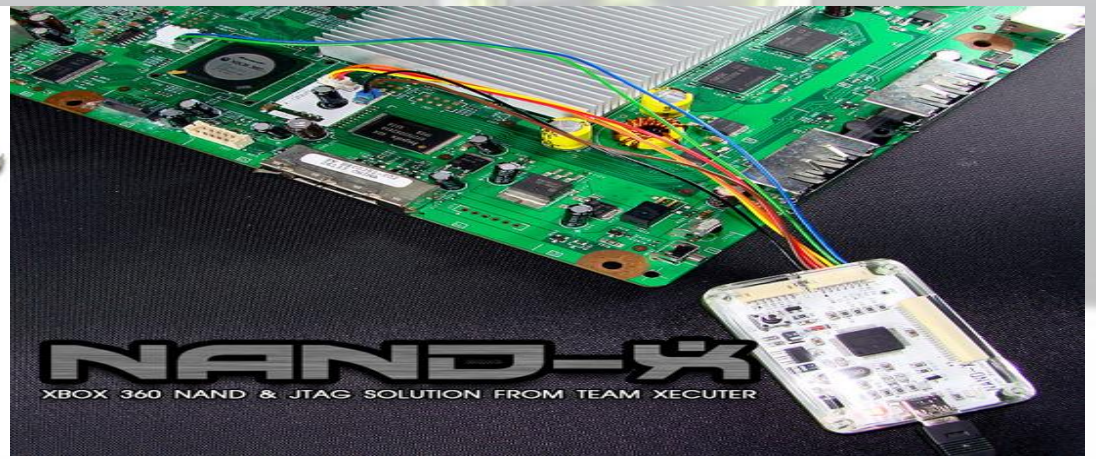
Nand Dumping

- **USB SPI flasher**
  - **Selfmade**
  - **Faster and safer than LPT**
  - **You need a PIC flasher (chip)**
    - **Computer with LPT**
  - **Buy it**
  - **All Phat and Slim excl. Corona 4GB**

Nand Dumping

- **NAND-X / J-R Programmer**
  - **Expensive:** Costs around 40 dollars
  - Involves **soldering** a few wires/pins (7) into just the Xbox. The other end plugs into the device
  - **Fast:** Takes at least 5 minutes to read NAND
  - **Worth the investement ?**



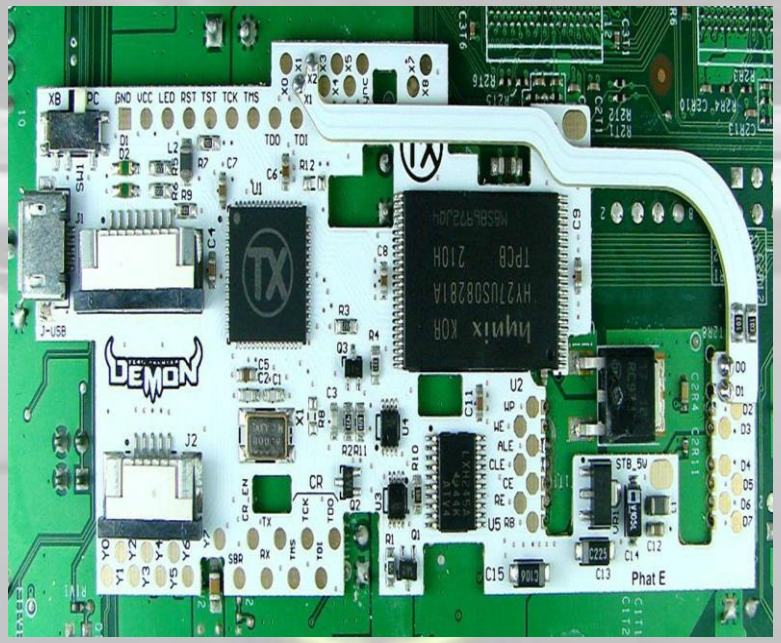


R/W Kit (Corona V2/V4/V5)

- Needs SD card reader
- Computer and J-Runner tool
- Only on corona 4gb v2 v4 v5
  - YOU NEED Corona R/W KIT if you have 4GB
  - You can dump it partially (48 MB) or the full 3.8 GB.
    The full 3.8 GB is slow but if you do first time then dump the full 4GB.

Nand Dumping with Demon

- Dual Nand
- Built in USB Nand Read /Write Hardware
- you can have a stock image that can go on LIVE
- Stays in permanently
- Supports Corona V1 & V3, V5 and Trinity
- Corona 4GB Not Supported

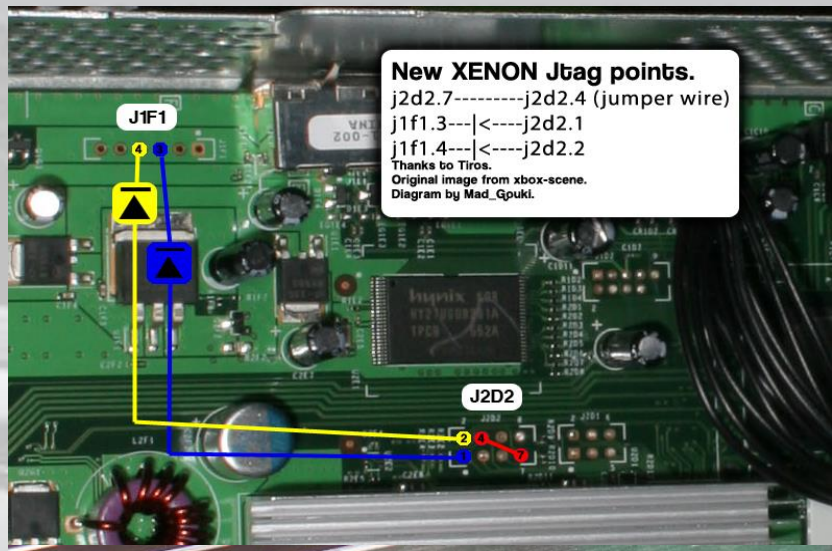


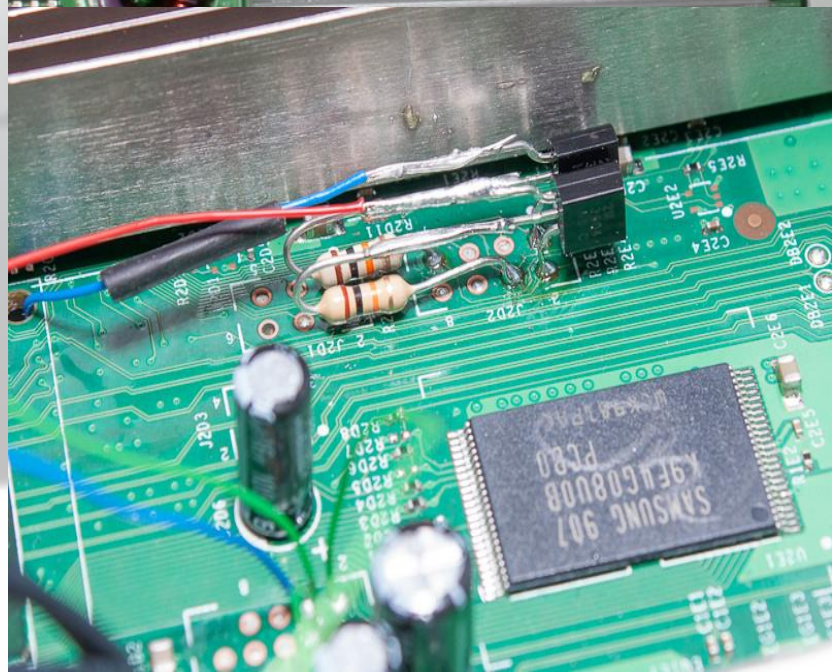
So what dumping method do i need ?

- **Phat**
  - LPT – USB SPI
  - Nand X/JR-Programmer
  - Demon
- **Slim**
  - LPT –USB SPI
  - Nand X/JR Programmer
  - Demon (NOT ON V2/V4)
  - R/W Kit Corona V2/V4 **(You have to do this On v2/v4)!**
  - **Corona v6 = XBOX 360E 4GB (XECUTER 4GB R/W ADAPTER REQUIRED)**

3 JTAG Methods

- **1. The Xenon Method** (Xenon only)
- **2. The Boxxdr Method** (Zephyrs, Opus, Falcon, and Jasper)
- **3. The Boxxdr Method plus DVD Tray** (Zephyrs, Opus, Falcon, and Jasper)
- Boxxdr Method is most **stable**
- Boxxdr + Tray only wenn frequent e79´s





RGH = Reset Glitch Hack

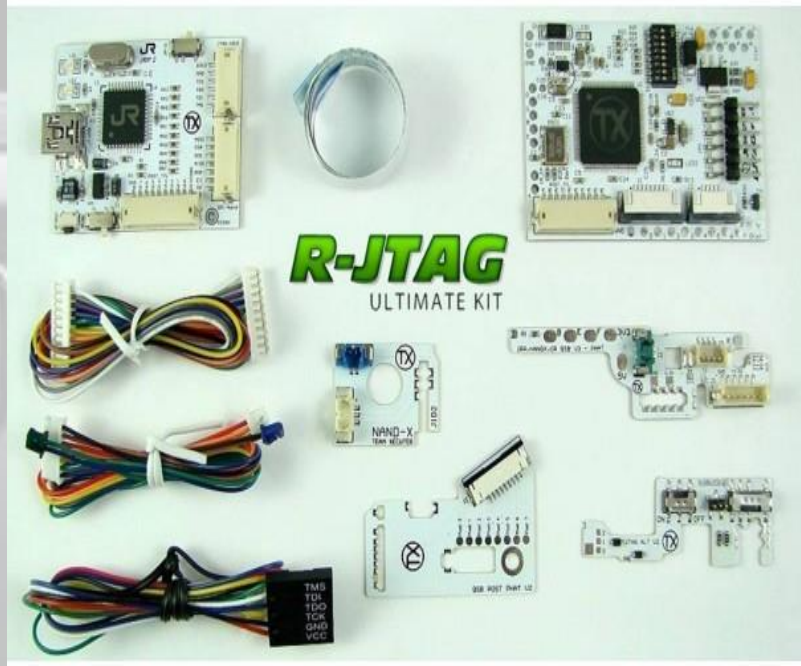
- Harder to install (Chip)
- Expensive
- Longer boot times: 5 sek – 2min !
- Can be done on phats (but better to use R-JTAG) or slims (any dash)
- Can run Xecuter Fusion
- Can use DemoN to do a dual NAND setup (about an extra 50-60 dollars) DOESNT WORK ON CORONA V2's/V4's
- Works on all Slims with any Dashboard

RGH1 VS RGH2 VS R-JTAG

- **Two versions of RGH**
  - **RGH1**
    - Better boot times
    - Stopped working after dash 14699
    - Only works on PHAT
  - **If you are exactly on 14699:**
    - Check if CB was patched
  - **RGH2**
    - Also on >14699
    - Slims
    - Dashes 15xxx and above use a new set of timing files but they still use the wiring of RGH2.
  - **Zephyrs are shit on RGH1 and RGH2 better consider to R-JTAG them**

Additional Hardware

- QSBs
  - Little circuit boards that makes wiring and reading nand easier.
  - Cost 10 USD
  - If you have Corona V2/V4 You need a QSB !!!!
  - On R-JTAG you also NEED THE QSB !
    - Buying Full starter KIT
  - No QSB for xenon

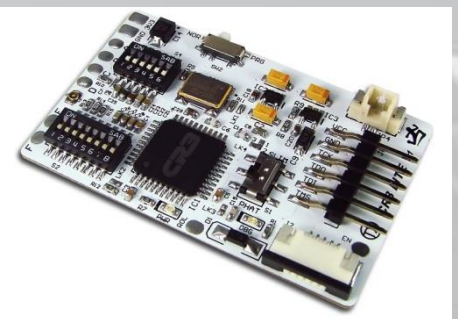


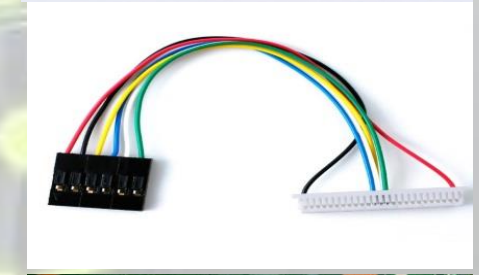
RGH2 - Hardware

- **If your Console if Slim or Xenon**
- **Dash higher thahn 7371**

- **You need:**
- Cr3 Lite/Pro or Coolrunner Rev C
- LPT cable if you dont have a NAND-X/J-R Programmer or Demon
- Nand –X to coolrunner JTAG cable
- On Corona V3/V4 you need a POST OUT FIX ADAPTER (10USD)
- **On V5/V6 Postfix adapter V2**

Since release of R-JTAG do not RGH2 on PHAT !





R-JTAG

- **Dash 15574 or above and PHAT consoles only**
  Harder to install
- **Expensive:** Chip with wires costs around 50
  Decent Boot Times 10sek
- Can **only be used on phats** of any dash version
- Can run **Xecuter Fusion**
- **Can use DemoN to do a dual NAND setup (about an extra 50-60 dollars) (DOESN'T WORK ON CORONA V2's/V4's)**

R-JTAG Hardware

- **if you have a phat**
- **Dash 15574 Or above**
- **R-Jtag Ultimate KIT :**

R-JTAG Methods

- **The are two ways to setup the R-JTAG hack:**
  - The regular way
  - The AUD_CLAMP way

- **AUD_CLAMP more reliable !**

Aud_CLAMP

So what method should i use ?

- **If you got a Slim**
  - Flash
  - Or RGH
  - Wasabi or X360key If you play offline
- **If you got a Phat:**
  - Dash <= 7371
    - JTAG or RGH / JTAG
  - Dash > 7371
    - RGH / R-JTAG
  - But if you are <= 7371 makes more sense to JTAG (Cheap)
  - Or Flash
  - Wasabi or X360key If you play offline

Additional Mods

- Protecting yourself from **accidental updates** (prevents e-fuses from blowing)
- **12V fan mod**: Change LEDs on the ROL
- **Internalizing** your HDD
- Using a **PC power supply**
- Getting **quieter Talismoon fans**

Good tutorials and Sources

- http://team-xecuter.com/forums/showthread.php/78885-RGH-roadmap-for-n00bies
- http://www.se7ensins.com/forums/threads/jtag-rgh-xbox-360-ultimate-exploit-guide.804054/
- http://www.nextgenupdate.com/forums/xbox-360-achievements-jtag/667126-ultimate-jtag-rgh-guide.html
- http://team-xecuter.com/forums/showthread.php/99437-DG-16D5S-Replacement-PCB-LTU-Tutorial
- http://gbatemp.net/threads/guide-how-to-hack-your-360.334203/

Questions ?

- ***Contact me on:***
- Youtube:
  - www.youtube.com/itxtutor
- Facebook:
  - https://www.facebook.com/pages/ITXtutor/454184481403350
- Twitter:
  - https://twitter.com/itxtutor