

## Last updated 21-8-06

Samsung Changes from v40: better SATA/MTKFlash compatibility list , moved hex editing MTKFlash up , uses free hex editors, X360SAM instructions, boot from USB or CD , removed KDX from guide, instructions for MS28

Hitachi Changes from v40: added SLAX/SATA list, instructions for stealth firmware

**OPA-XTREME-HITACHI-7IN1-V2\_1.RAR** is the current Hitachi fw to use.

**Xtreme firmware 3.0 (xtreme30.rar)** is the current Samsung fw to use.

Written & Compiled by: geebee & contributors  
([geebee@gmail.com](mailto:geebee@gmail.com) or [Textbook](#) for any changes)

# Hack the 360: The Tutorial

Backing Up, Modifying & Flashing the  
Samsung Drive  
&  
How to Create Game Backups  
&  
Bad Flash Recovery

**Samsung**  
**BEFORE YOU START, READ**

## [Start Your Reading Here](#)

<http://forums.xbox-scene.com/index.php?s=cdbaa5713c3134aa66aa2493c814c259&showtopic=513412>

## [Then if you want more background read here](#)

[www.kev.nu](http://www.kev.nu)

Now read this tutorial, twice. If you don't understand any terms, think twice about doing this.

This tutorial will explain every step in backing up your original firmware, creating a working hacked firmware for your Toshiba-Samsung DVD-Drive and flashing it back to the DVD-Drive. It will also explain how to create successful game backups.

It is really important to keep in mind that the complete process can be risky if you don't know what you are doing.

## **WARNINGS**

**IF YOU WANT TO KEEP YOUR WARRANTY DO NOT TRY THIS.  
OPENING THE CASE INVALIDATES THE WARRANTY.**

**Don't ask for illegal files. ANYWHERE. Especially not on public forums.  
Read all the forum rules. Do not talk about .ISO images you have  
downloaded.**

**We are not responsible for any misreading or damage done to your  
Microsoft Xbox 360 in any way.**

**Please do not attempt to try this if you don't understand any of the steps  
below. Normal to Average PC experience is required in order to  
successfully complete the installation.**

**Do not stick your fingers into live electrical parts. Do not stick any other  
parts of your anatomy in either.**

**Lasers BLIND! Do not look into them if you need to hotswap disks when  
using WxRipper (to follow)**

## Overview:

### Firmware Tasks:

- Disassemble Xbox360
- Connect Xbox360 Drive to PC
- Make floppy/usb/cd boot disk with mktflash on it
- Boot PC with bootable disk
- Backup Xbox360 Drive firmware
- Restart PC and flash hacked firmware
- Rebuild Xbox360 (unless you want to make some backups now)
- Test Xbox360

### Game Backup Tasks:

- Disassemble Xbox360
- Connect Xbox360 Drive to PC
- Burn activate.iso and use the integrated 0800 mode in Windows
- Extract Security Sectors
- Extract PFI and DMI
- Make Image with wxRipper or Isobuster
- Combine SS and game image with SS Merger 1.6
- Burn image
- Rebuild Xbox360
- Test backups

**WARNING:** If you are going to connect your 360 and PC together in *\*any\** way, then you *\*must\** provide the 360 with a path to true earth ground. This is because the 360 has a floating ground and horrible things happen if all connected systems do not agree on the reference voltage. I used a couple of croc clips from the chassis of the 360 to the chassis of my PC to achieve this.

## Tools:

- 1) Xbox 360 with Samsung Drive ROM v. MS25 (MS28 instructions below)



- 2) Commodore4Eva's Xtreme Firmware (Xtreme v3 is the latest).
- 3) A floppy disk and floppy drive, USB flash drive and USB-bootable motherboard, or a blank CD-R.
- 4) A PC with a suitable SATA chipset:

## MTKFlash SATA Compatibility

Onboard SATA				
Motherboard	Chipset	Requires Hex Editing MTKFlash?	Works?	Comments
Abit NF7-S2GN	nForce2	No	Yes	Must be mapped as IDE ports 3 and 4
Asus A8N5X	SIL 3114	Yes	Yes	Reported working only with most updated motherboard BIOS and hex-edited MTKFlash. <a href="#">Windows Drivers</a>
ALL*	VIA VT 8251	Doesn't Work	No	Only incompatible onboard VIA, tested on Asus AV8 MX Motherboard
ALL*	Promise Fastrack 376	Doesn't Work	No	Tested on ASUS A7V8X Motherboard
Asus P4C800e-deluxe	Promise (unknown info)	No	Yes	
ALL*	Intel ICH6	No	Yes	Tested with ASUS P5 AD2 Premium
ECS AMD 939 RS480-M	ATI Xpress 200	Doesn't Work	No	
ALL*	Intel ICH5	No	Yes	
ALL*	Intel ICH5R	No	Yes	
?	Intel ICH7	Yes	Yes	<a href="#">82801GB / GR / GH ICH7 MTKFlash</a> Marvell ICH7 needs a different MTKFlash
Gigabyte GA-81945P-L	Intel 945PL Express	No	Yes	
Gigabyte GA-K8NSC-939	nForce3	No	Yes	
ALL*	NF4SAT1 nForce 4	Yes	Yes	
ECS KV2 Extreme	SIS964	No	Yes	Must connect to Sata port 3 or 4, ports 1 and 2 will not work
ALL*	SIL 3112	Doesn't Work	No	
ALL*	SIL 3132	Doesn't Work	No	
MSI K7N2 Delta2	Promise	Doesn't Work	No	
MSI K7N2 Delta2	nForce2	Yes	Yes	
ALL*	VIA VT 8237	No	Yes	Some people reported success only when hex-edited, try one of these. <a href="#">MTKFlash1</a> <a href="#">MTKFlash2</a>
ALL*	VIA VT 6410	Yes	Yes	Try manual hex-edit first, or try one of these. <a href="#">MTKFlash1</a> <a href="#">MTKFlash2</a>
VIA Epia SP Mini-iTX	VIA EPIA SP	Yes	Yes	<a href="#">MTKFlash</a>

PCI SATA CARDS			
Chipset	Requires Hex-Editing MTKFlash?	Works?	Comments
SIL 3112	Doesn't Work	No	
SIL 3122	Doesn't Work	No	
SIL 3115A	Doesn't Work	No	
SIL 3512	Doesn't Work	No	
SIL 3114	Doesn't Work	No	
Adaptec ASH-1205SA (SIL 3112)	Doesn't Work	No	
ALI M5283	Yes	Yes	Not recommended, Geremia says it hangs during writing
ALI M5289	Yes	Yes	
Maxtor SATA (Promise)	Doesn't Work	No	
RocketRAID 1520	Yes	Yes	Rather expensive
RocketRAID 1640	Yes	Yes	Rather expensive
VIA VT 8237	No	Yes	Difficult to find a PCI Sata card with this chipset.
<a href="#">VIA VT 6421L</a>	Yes	Yes	This is the card to get. Cheap, widely available, with a pre-hex-edited MTKFlash for download. <a href="#">MTKFlash1</a> <a href="#">MTKFlash2</a>
VIA VT 6237R	Yes	Yes	You can hex edit manually or try the links above for the 6421L.
VIA VT 6421A	Yes	Yes	You can hex edit manually or try the links above for the 6421L.
<a href="#">Newlink NL-PCISATAIEXT</a>	No ?	Yes	Thanks to Thraxed, best card to buy in UK.

\* Note: When using a hex-edited MTKFlash, you must also download a [normal MTKFlash](#) and use the MTKFlash.typ file from it. Also, your MTKFlash .exe and .typ files must be named exactly the same. Ex: if you download MTKFlashvia.exe , rename it to MTKFlash.exe

### SATA NOTES:

Mtkflash.exe must have the Xbox360 Drive on a SATA channel, not an ide channel (ie not with SATA-to-IDE converter).

Mtkflash cannot flash via a USB or Firewire connection (DOS doesn't have drivers!)

Mtkflash has the following support documented inside the compiled executable:  
 ICH5, ICH6P, ICH6, ICH6M, VIA8237, Si3114, SiS964, SiS180, SiS965, NV nForce3

Make sure your SATA ports are set to NATIVE/IDE mode NOT RAID. You set this in your computer's BIOS. When booting your computer, look for text that says "Press key for Setup." Press this key until you get into your BIOS menu.

Configure your SATA ports to use NATIVE , IDE, or SATA mode (not RAID).

You can hexedit Mtkflash to modify support for which channel, etc. the application scans. This differs by machine/card/controller, so this is obviously only something more advanced users can do.

**WARNING:** If you are going to connect your 360 and PC together in *\*any\** way, then you *\*must\** provide the 360 with a path to true earth ground. This is because the 360 has a floating ground and horrible things happen if all connected systems do not agree on the reference voltage. I used a couple of croc clips from the chassis of the 360 to the chassis of my PC to achieve this.

## **Editing MTKFlash to Work With Your SATA Chipset:** [\(Thanks to Grim187\)](#)

You will need:

HEX Editor (The [free HHD Hex Editor](#) works perfect)

SATA Controller Card or an Onboard SATA Controller

If you do not have a SATA Controller You can most likely find one at your local Computer store or online.

See safe list at the top of this document.

### **1. Finding out What SATA Chipset You Have**

If you have a SATA Controller Card it should say on the Box, In the Manual or on The Chip itself, If you have a Onboard Check your mobo/Computer Manufacturers Website

Example:

Onboard: VIA KM400 / **8237** = [VIA 8237 SATA Chipset](#)

SATA Controller Card: [VIA 6421](#)

### **2. Install SATA Drivers**

Motherboards will come with a driver CD and PCI CARDS should also come with a driver CD. Please install the correct SATA drivers for your operating system. If you don't see your drive in MSInfo, it is because your SATA drivers are not installed.

### **3. Finding The Correct Values**

You will need to Open up MSInfo32.exe (Start>Run, Type "MSinfo32.exe" w/o Quotes, Press OK), with MSInfo open (Should Look Something Like [This](#)) Click the + next to "Components", Click the + next to "Storage" Now Click on SCSI You Should See

## Something That looks Like This

Name Serial ATA Controller

Manufacturer

Status OK

PNP Device ID

PCI\VEN\_2211&DEV\_4433&SUBSYS\_31491106&REV\_80\3&61AAA01&0&78

I/O Port 0x00006655-0x00006662

I/O Port 0x00000000-0x00000003

I/O Port 0x00008877-0x00008884

I/O Port 0x00000000-0x00000003

I/O Port 0x00000000-0x0000000F

I/O Port 0x00000000-0x000000FF

IRQ Channel IRQ 20

Driver c:\windows\system32\drivers\driver.sys (5.1.2600.201, 74.63 KB (76,416 bytes), 5/15/2006 7:00 AM)

All of that Should Look Different in Your Info, Next to Name it Should Say Something About "Serial ATA" if it Doesn't Try Scrolling Down and/or Make Sure Your in the Right Place,

What You Are looking For in This is 8bytes (16 Numbers/Letters) That MTKFlash Can Identify Your Chipset with, The First 4bytes are Found in The "PNP Device ID" (2 Numbers/Letters = one byte)

PNP Device ID

PCI\VEN\_2211&DEV\_4433&SUBSYS\_31491106&REV\_80\3&61AAA01&0&78

You need to swap around the bytes to get it in the correct order. The correct order is digits 34127856. Example: From above, we have **22114433**. The correct order after swap is **11223344**

**PNP Device ID**

**PCI\VEN\_2211&DEV\_4433&SUBSYS\_3149**

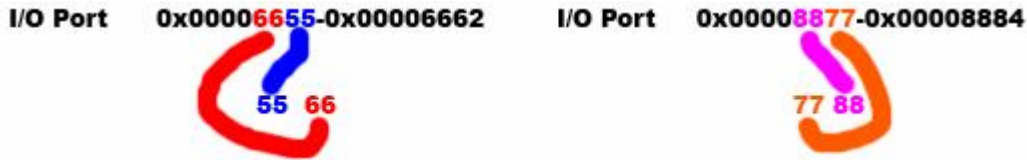


The Next 4Bytes are Found in 2 Different Lines of "I/O Port" Hex Values, You Want to Identify The 2 Lines That Have a 7Byte Difference, Extract the Last 4 Digits of the First Section of Numbers/Letters from Them and Swap the 2 Bytes (As You did with The "PNP Device ID" Line)

I/O Port 0x0000**6655**-0x00006662

I/O Port 0x0000**8877**-0x00008884

This is Only Known to Work if You Use The 2 "I/O Port" lines With a Difference of 7 in Order (as Shown Above), As They are Values for The Primary Master and Slave SATA Device. You must do the same byte swap as before. The correct order is digits 34127856. Example: from above, we have **66558877**. The correct order after swap is **55667788**.



Put Together The 4bytes of Hex (8 Numbers/Letters) That You Have From The "PNP Device ID" Line and the 4 You have from The "I/O Port" Lines and You Have The Values You Need to Insert in to Your MTKFlash.exe File.

### 3. Injecting Chipset's Hex Values

The Xtreme v3 release does not include MTKFlash for some reason. It is included in Xtreme versions 1 and 2, so you can get it from there or download it [HERE](#).

Right-click MTKFlash.exe and select Edit with Hex Editor (if using HHD Free Hex Editor). Select Edit > Goto... and type in B307 and hit enter. In the text display to the right, you should see names of chipsets such as ICH5, VIA8237, NV NForce3, etc. In the text area, click on the second dot before your chipset name. A "01" should now be boxed in the hex area to the left. In the hex area, highlight this, going back 8 bytes (16 numbers/letters).

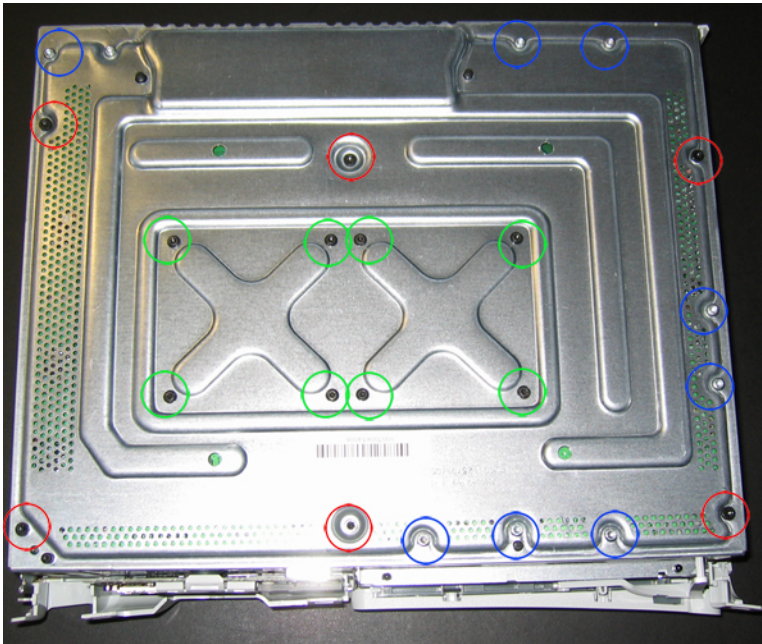
	Hex	Text
0000b370:	00 70 00 00 00 00 00 ff 00 ff 00 f0 01 70 01 01	.p.....ÿ.ÿ.ð.p..
0000b380:	49 44 45 00 00 00 00 00 00 00 86 80 d1 24 f0 01	IDE.....+€Ñ\$ð.
0000b390:	70 01 00 49 43 48 35 00 00 00 00 00 86 80 6f	p..ICH5.....+€o
0000b3a0:	26 f0 01 70 01 00 49 43 48 36 50 00 00 00 00	ðð.p..ICH6P.....
0000b3b0:	86 80 52 26 f0 01 70 01 00 49 43 48 36 00 00 00	+€R&ð.p..ICH6...
0000b3c0:	00 00 00 86 80 53 26 f0 01 70 01 00 49 43 48 36	...+€S&ð.p..ICH6
0000b3d0:	4d 00 00 00 00 00 06 11 49 31 f0 01 70 01 00 56	M......I1ð.p].V
0000b3e0:	49 41 38 32 33 37 00 00 00 95 10 12 31 f0 01 70	IA8237...*.1ð.p
0000b3f0:	01 00 53 69 33 31 31 32 00 00 00 95 10 14 31	..Si3112....*.1
0000b400:	f0 01 70 01 00 53 69 33 31 31 34 00 00 00 00 39	ð.p..Si3114....9
0000b410:	10 80 01 f0 01 70 01 00 53 69 53 39 36 34 00 00	.€.ð.p..SiS964..
0000b420:	00 00 39 10 81 01 f0 01 70 01 00 53 69 53 31 38	..9.ð.p..SiS18
0000b430:	30 00 00 00 00 39 10 82 01 f0 01 70 01 00 53 69	0....9.,.ð.p..Si
0000b440:	53 39 36 35 00 00 00 00 de 10 e3 00 f0 01 70 01	S965....P.ä.ð.p.
0000b450:	00 4e 56 20 6e 46 6f 72 63 65 33 ff 00 ff 00 f0	.NV nForce3ÿ.ÿ.ð
0000b460:	01 70 01 00 55 6e 6b 6e 6f 77 6e 00 00 00 00 50	.p..Unknown....P
0000b470:	72 69 20 4d 61 73 74 65 72 00 00 00 00 00 00 00	ri Master.....

Simply edit in your 8-byte value we got earlier, and save the MTKFlash.exe file.

[To Conclude the Example's in Step 3 \(Don't Edit The Red 00's\)](#)

## Xbox 360 Disassembly:

To disassemble your Xbox 360 to get the DVD Drive out, follow these instructions but you do **NOT** need to remove the black heatsink screws. All you need to remove is the six silver long screws circled in RED:



[Anandtech Xbox 360 Stripping Guide](#)

Keep the power connector plugged in your Xbox 360.

## Opening the 360 (the perfect way)

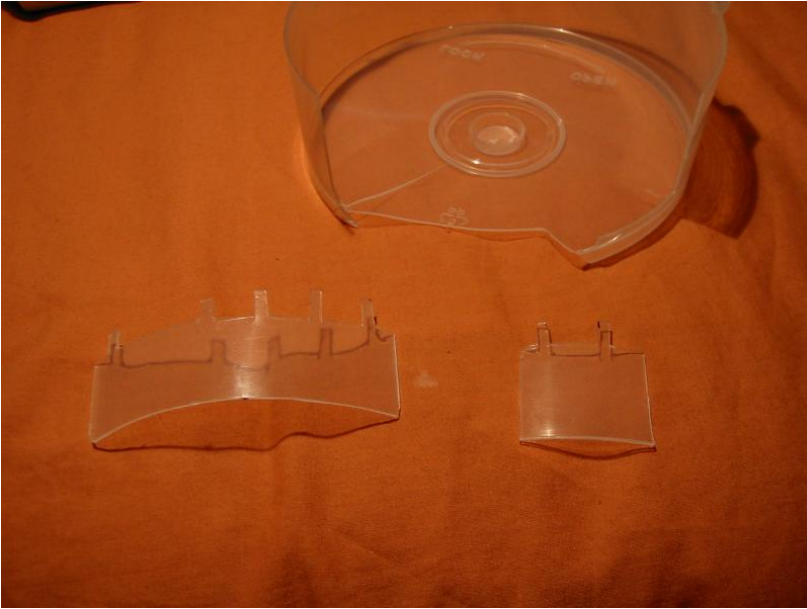
Take the tub your spindle of discs came and cut a bit from the side of it and put it over the console as shown. Mark out where the holes are...



... then make it into a key like this. the tabs need to be about 1cm long.



Do the same for the other side and you'll get two xbox 360 case opening keys that look like these...



## Step 2

Open the front of the console as normal and put a bit of newspaper or something inside the case to hold the front open a bit, then insert the key, push with a bit of force and you should hear it click and the case will open....



... repeat for the other side and you're done!

V41



Thanks to Hydra!

## **Xbox 360 Connection:**

Unplug the SATA cable from the back of the Xbox360 Drive. Connect a SATA cable from your PC SATA connection to the back of the Xbox360 Drive. Connect the video cable to the back of the Xbox360. If you do not do this, the Xbox360 will power off at an inappropriate moment (like when flashing). Do not power on the Xbox360, leave it off.

## **USING X360SAM TO HACK THE SAMSUNG**

X360SAM is like a “semi-autopatcher” that is much better than the autoflasher previously recommended. The reason being is that the autoflasher does not work with version 25b and 28 drives, X360SAM does. I call it a “semi-autopatcher” because it requires one reboot. Using X360SAM is basically the same thing as a manual method because it hex edits the original drive key into the Xtreme v3 firmware, just what you would do if you were doing it the manual method. It has also been updated to include the correct 4000-43FF range suggested by Sniperkil. This means it will work with all DVD drives, no bricks. Everything is done from DOS, making it faster and easier.

1. Download [X360SAM 0.2](#)
2. Download the Xtreme v3 firmware from the usual place
3. Copy Xtreme30.bin to /X360SAM 0.2/Xbox360/SAMSUNG/
4. If your SATA chipset requires a hex-edited MTKFlash, use that instead of the included one in /X360SAM 0.2/Xbox360/
5. Remember that MTKFlash's .exe and .typ files must be named the same
6. Write down your Xbox 360's serial number on a piece of paper, you will need it when reading and flashing

## **X360SAM on a Bootable Floppy Disk:**

Make a bootable floppy disk. To do this insert a floppy in your A: drive while in Windows.. Right Click on the A: drive in My Computer. Select “Format” then tick “Create an MS-DOS startup disk”. When it is finished, copy the folders and files from /X360SAM 0.2/Xbox360/ to the floppy disk.

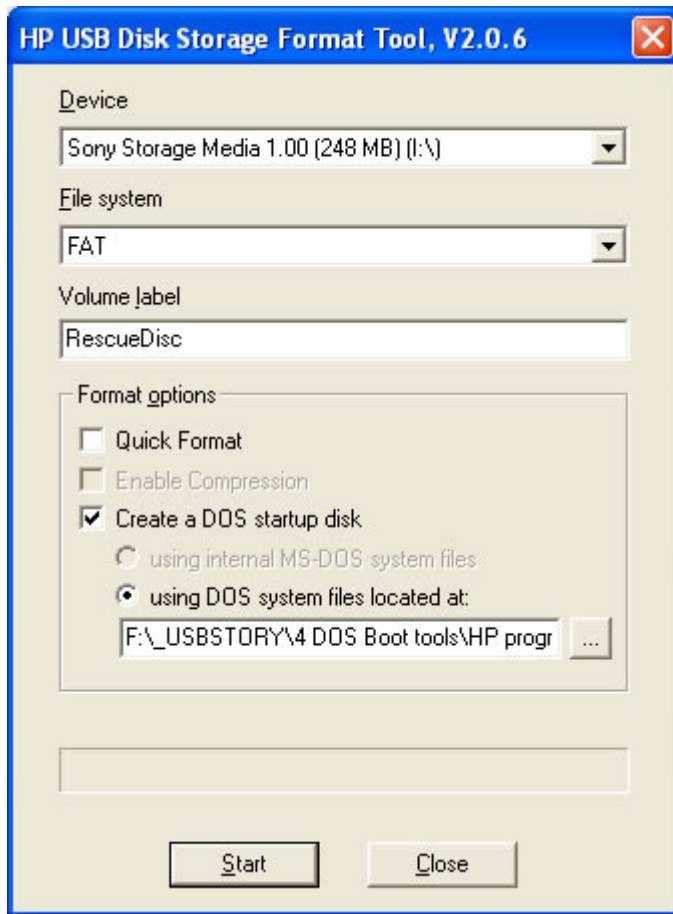
1. At this point, you should have the Xbox 360 disassembled, with a SATA cable connecting your Samsung drive to your PC. Turn off both the Xbox 360 and PC.

2. Insert the bootable floppy you made, power on the PC, but leave your Xbox 360 off. Your PC should boot to a command prompt. When it does, power on your Xbox 360.
3. In the next step, you need to use your Xbox 360's serial number. The X's are the 7-digit first part, the Y's are the 5-digit second part.
4. Type SAMREAD XXXXXXXX YYYYYY , using your serial number. For example, if my S/N is 5242924 61305, I would type SAMREAD 5242924 61305.
5. Your original firmware will be read and dumped. When you return to the command prompt, power off the Xbox 360, then restart your PC.
6. Your PC will boot from the floppy again, when it gets to the command prompt, power on your 360.
7. Type SAMHACK XXXXXXXX YYYYYY, using the serial number of your Xbox 360 again.
8. Your drive will be flashed, and when you get back to the command prompt, power off the Xbox 360, and then power off your PC.
9. Put your Xbox 360 back together and test.

## **X360SAM on a Bootable USB Flash Drive:**

In order to create a bootable USB Flash Drive, your motherboard must support booting from USB. You may have to enable it in the BIOS menu. You will also have to format the drive, erasing all data on it. So get the data off the USB drive before continuing.

1. Download [HP DOS Files](#).
2. Download [HP USB Disk Storage Format Tool](#).
3. Extract the HP DOS files and install the HP USB Formatting tool.
4. Plug in your USB drive and run the HP USB Formatting tool. Select your device, choose to format as FAT, and select Create a DOS Startup disk, using DOS files located at: (browse to the folder you extracted).



5. When it is done formatting, copy all folders and files from /X360SAM 0.2/Xbox360/ to the USB Flash Drive.

Now that your USB flash drive is prepared, let's get to the fun stuff.

1. At this point, you should have the Xbox 360 disassembled, with a SATA cable connecting your Samsung drive to your PC. Turn off both the Xbox 360 and PC.
2. Insert the bootable USB you made, power on the PC, but leave your Xbox 360 off. Your PC should boot to a command prompt. When it does, power on your Xbox 360.
3. In the next step, you need to use your Xbox 360's serial number. The X's are the 7-digit first part, the Y's are the 5-digit second part.
4. Type SAMREAD XXXXXXXX YYYYYY, using your serial number. For example, if my S/N is 5242924 61305, I would type SAMREAD 5242924 61305.
5. Your original firmware will be read and dumped. When you return to the command prompt, power off the Xbox 360, then restart your PC.
6. Your PC will boot from the USB again, when it gets to the command prompt, power on your 360.

7. Type SAMHACK XXXXXXXX YYYYYY, using the serial number of your Xbox 360 again.
8. Your drive will be flashed, and when you get back to the command prompt, power off the Xbox 360, and then power off your PC.
9. Put your Xbox 360 back together and test.

## X360SAM using NTFSDOS CD

If you don't have a floppy drive and your motherboard can't boot from USB or you don't have a USB flash drive, you can use your normal computer hard drive and an NTFSDOS bootable CD. [Download this ISO](#) and burn using a burning program capable of burning ISO images. (Nero, IMGBurn, CloneCD, etc.). Copy all folders and files in /X360SAM/Xbox360/ to the root of your C: drive.

Boot your PC with the bootable NTFSDOS CD and let it do its thing. After a while it will say:

“Select from Menu [0123], or press [ENTER – Singlestepping (F8) is: OFF”

Hit enter and you should see this disclaimer.



Type Yes and hit enter. Also notice at the top of this screen the label your NTFS hard drive is given. Mine showed up as D. When you get to the flashing A:\ command prompt, type the following:

D:\ [press enter] ← use the drive letter your hard drive was given

1. In the next step, you need to use your Xbox 360's serial number. The X's are the 7-digit first part; the Y's are the 5-digit second part.
2. Type SAMREAD XXXXXXXX YYYYYY, using your serial number. For example, if my S/N is 5242924 61305, I would type SAMREAD 5242924 61305.
3. Your original firmware will be read and dumped. When you return to the command prompt, power off the Xbox 360, then restart your PC.
4. Your PC will boot from the CD again, hit enter again, type yes again, and type your drive letter to get back to where we started. When it gets to the correct drive letter's command prompt, power on your 360.

5. Type SAMHACK XXXXXXXX YYYYYY, using the serial number of your Xbox 360 again.
6. Your drive will be flashed, and when you get back to the command prompt, power off the Xbox 360, and then power off your PC.
7. Put your Xbox 360 back together and test.

## THE MANUAL WAY TO HACK THE SAMSUNG:

### Bootable Floppy Disk:

Make a bootable floppy disk. To do this, insert a floppy in your A: drive while in Windows. Right Click on the A: drive in My Computer. Select "Format" then check "Create an MS-DOS start-up disk". When it is finished, copy MTKFlash.exe (the one you hex-edited) and MTKFLASH.TYP to your floppy disk. Your exe and typ must be named exactly the same. If you have MTKFlashvia.exe then you can either rename it to just MTKFlash.exe or you can rename your .typ to MTKFlashvia.typ. Just make sure they are named the same. That's your disk prepared.

Power off your Xbox 360 and PC. Connect the Samsung drive to the PC using a SATA cable, but leave the 360 powered off. Insert your floppy disk or bootable USB drive and turn on the computer, booting to a command prompt. If you boot to Windows, restart your computer and set your BIOS to boot from floppy first.

You should get to a command prompt with just A: on it. At this point, you can finally turn on your Xbox 360. Type the following command a few seconds after turning on your Xbox 360.

```
mtkflash r /m orig.bin
```

Press Enter

It should display your SATA chipset. Type in the corresponding number and it should read and dump the original firmware. If you're not seeing the SATA chipset, try the following command:

```
mtkflash r /m /sata orig.bin
```

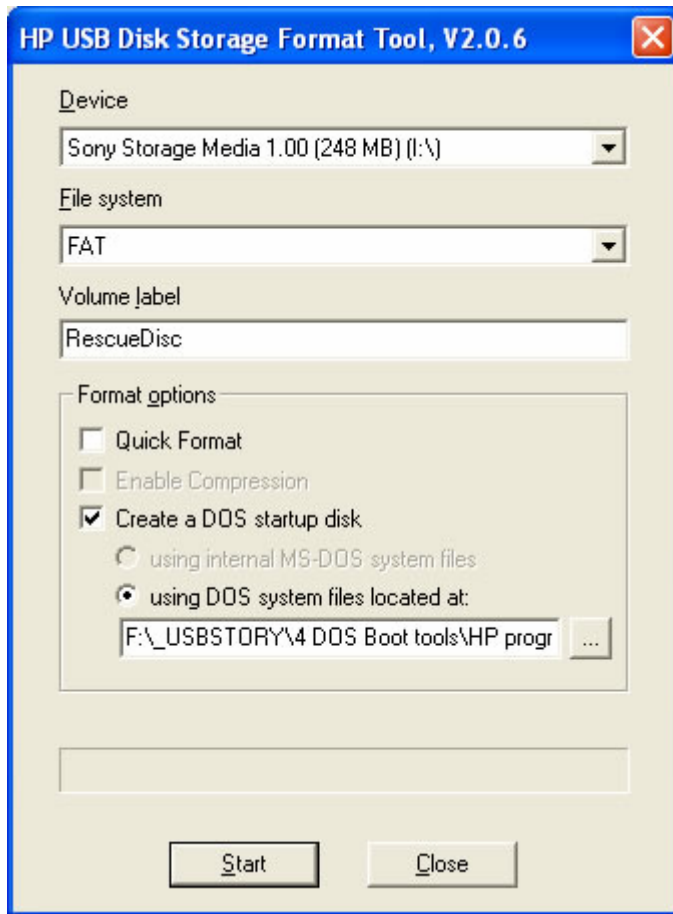
If it still isn't showing up, you didn't hexedit mtkflash correctly or you have an incompatible chipset.

When the dump is done, it will tell you to restart your pc. Disconnect the SATA cable and power off the Xbox 360. Eject your floppy and restart your computer. Boot into Windows. Open the floppy from My Computer and select the file ORIG.BIN. This is your Xbox360 Drives firmware and needs to be kept safe! Make a copy of the file. Then make another one on another drive or CD or USB Stick. Email it to yourself. Then make another somewhere else. You get the drift.

## **Bootable USB Flash Drive:**

In order to create a bootable USB Flash Drive, your motherboard must support booting from USB. You may have to enable it in the BIOS menu. You will also have to format the drive, erasing all data on it. So get the data off the USB drive before continuing.

6. Download [HP DOS Files](#).
7. Download [HP USB Disk Storage Format Tool](#).
8. Extract the HP DOS files and install the HP USB Formatting tool.
9. Plugin your USB drive and run the HP USB Formatting tool. Select your device, choose to format as FAT, and select Create a DOS Startup disk, using DOS files located at: (browse to the folder you extracted).



10. When it is done formatting, copy your hexedited MTKFlash.exe and MTKFlash.typ onto the USB drive as well.

Power off your Xbox 360 and PC. Connect the Samsung drive to the PC using a SATA cable, but leave the 360 powered off. Insert your bootable USB drive and turn on the computer, booting to a command prompt. If you boot to Windows, restart your computer and set your BIOS to boot from USB first.

You should get to a command prompt with just A: on it. At this point, you can finally turn on your Xbox 360. Type the following command a few seconds after turning on your Xbox 360.

```
mtkflash r /m orig.bin
```

Press Enter

It should display your SATA chipset. Type in the corresponding number and it should read and dump the original firmware. If you're not seeing the SATA chipset, try the following command:

```
mtkflash r /m /sata orig.bin
```

If it still isn't showing up, you didn't hexedit mtkflash correctly or you have an incompatible chipset.

When the dump is done, it will tell you to restart your pc. Disconnect the SATA cable and power off the Xbox 360. Unplug your USB drive and restart your computer. Boot into Windows. Plug in your USB drive and find orig.bin. This is your Xbox360 Drives firmware and needs to be kept safe! Make a copy of the file. Then make another one on another drive. Then make another somewhere else. Email it to yourself. You get the drift.

## Bootable NTFS4DOS CD

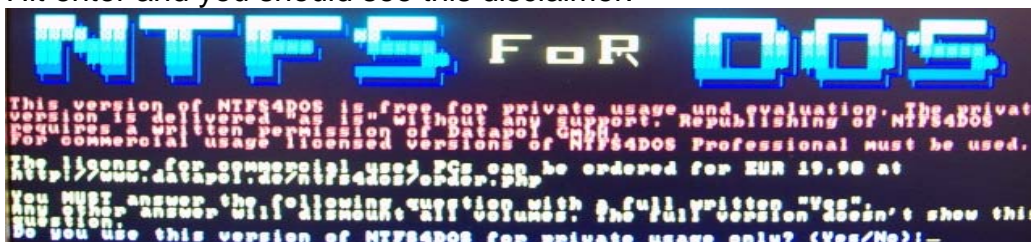
If you don't have a floppy drive and your motherboard can't boot from USB or you don't have a USB flash drive, you can use your normal computer hard drive and an NTFS4DOS bootable CD. [Download this ISO](#) and burn using a burning program capable of burning ISO images. (Nero, IMGBurn, CloneCD, etc.). Copy MTKFlash (.exe and .typ) to the root of your C: drive on your computer.

Power off both your Xbox 360 and PC. Connect the Samsung drive to the PC using a SATA cable, but leave the 360 powered off.

Boot your PC with the bootable NTFS4DOS CD and let it do its thing. After a while it will say:

"Select from Menu [0123], or press [ENTER – Singlestepping (F8) is: OFF"

Hit enter and you should see this disclaimer.



Type Yes and hit enter. Also notice at the top of this screen the label your NTFS hard drive is given. Mine showed up as D. When you get to the flashing A:\ command prompt, power on the Xbox 360. Type the following:

```
D:\ [press enter] ← use the drive letter your hard drive was given
Mtkflash r /m orig.bin [press enter]
```

It should display your SATA chipset. Type in the corresponding number and it should read and dump the original firmware. If you're not seeing the SATA chipset, try the following command:

```
mtkflash r /m /sata orig.bin
```

If it still isn't showing up, you didn't hexedit mtkflash correctly or you have an incompatible chipset.

When the dump is done, it will tell you to restart your pc. Disconnect the SATA cable and power off the Xbox 360. Eject your CD and restart your computer. Boot into Windows. Open the C: drive from My Computer and select the file ORIG.BIN. This is your Xbox360 Drives firmware and needs to be kept safe! Make a copy of the file. Then make another one on another drive or CD or USB Stick. Email it to yourself. Then make another somewhere else. You get the drift.

## Getting Your Key:

Now that we have the original firmware, we need to extract the Key out of it so we can inject it into the hacked firmware. This process will be done using the [freeware XVI32 Hex Editor](#). Extract XVI32 from the zip archive, and run the exe. Open the ORIG.BIN. When it opens up, press Ctrl+G (or Address > Goto...). Make sure Hexadecimal is selected and type in \$4000. Now, select Edit > Block <n> chars... Select Hexadecimal and type in \$400. You should see the text go red. Press Ctrl+H (or Edit > Clipboard > Copy as hex string) to copy as hex string.

Now, open up another instance of XVI32 and this time open up the Xtreme30.bin hacked firmware. Press Ctrl+G (or Address > Goto...). Make sure hexadecimal is selected and type in \$4000. Now, select Edit > Block <n> chars... Select Hexadecimal and type in \$400. You should see the text go red. Then select Edit > Overwrite String. Choose Hex String and paste (Ctrl+V) into the bar. Now save as Modified.bin.

If you need help understanding this process, there is a video tutorial [HERE](#).

## Reflashing Your Drive:

The last step is writing the firmware to your DVD-Drive. This will be done with MTKFLASH.EXE again. All you have to do is copy your modified.bin onto the floppy, USB drive, or C: drive (if using NTFSDOS CD) and you are all set to go.

Power off both your Xbox 360 and PC. Connect the Samsung drive to the PC using a SATA cable, but leave the 360 powered off. Insert your floppy disk, bootable USB drive, or NTFSDOS CD and turn on the computer, but leave the 360 powered off.

With floppy or USB, you will boot to a regular A:\ command prompt. With the NTFSDOS CD, follow the same instructions above to get to the command prompt where your files are stored. When you get to the command prompt, power on your Xbox 360 and type the following command:

```
mtkflash w /m modified.bin
```

It should display your SATA chipset. Type in the corresponding number and it should read and dump the original firmware. If you're not seeing the SATA chipset, try the following command:

```
mtkflash w /m /sata modified.bin
```

If it still isn't showing up, you didn't hexedit mtkflash correctly or you have an incompatible chipset.

When the flash is done, it will tell you to restart your pc. Disconnect the SATA cable and power off the Xbox 360. Put the Xbox 360 back together and test.

## THE ALTERNATE FLASHING METHOD

### Samsung AutoFlasher v3

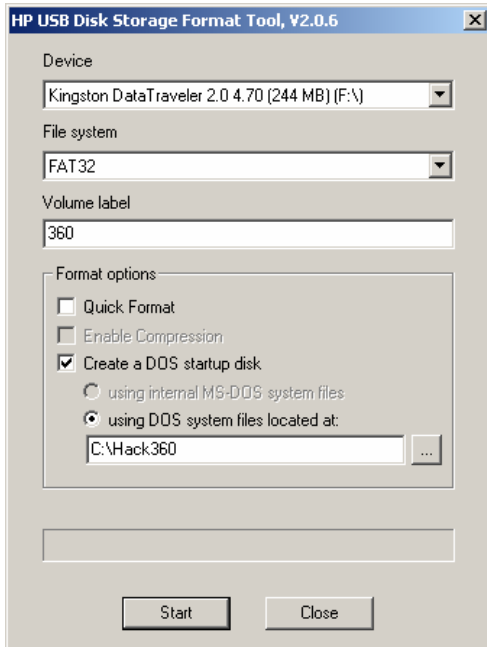
**DOES NOT WORK WITH v25b (April 2006) OR v28 DRIVES!**

The autoflasher is an easier, but less stable way to flash the Samsung as it does not require you to copy the key across using KDX or hex editor. It patches the firmware around the key.

The autoflasher works off a floppy or preferably a USB stick. Extract the files and use the USB formatter (HPUSBFW.EXE) to make a bootable stick. Use the DOS system files provided in the release.

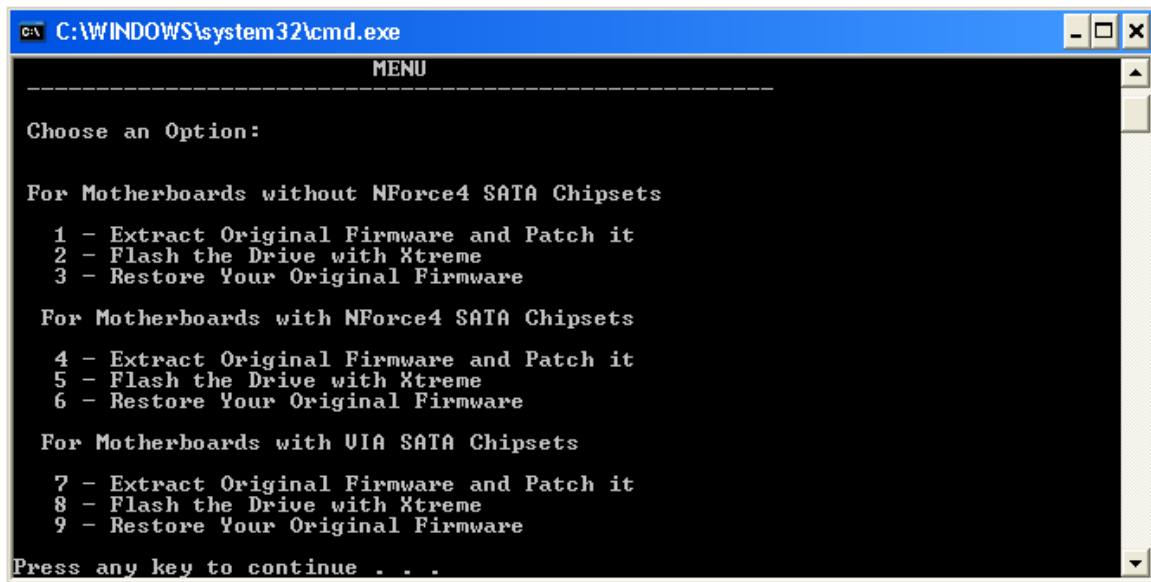
Quite a few people have claimed that the autoflasher is a less stable method of flashing the Samsung drives. Although the manual flashing method is more

difficult, it has been proven time and time again if you do it correctly and follow directions.



Set your PC to boot from the USB stick and start it up.

Depending on your chipset, press the appropriate key:



The first option for each chipset backs up your original firmware and patches the xtreme firmware with your DVD drive key.

The second option flashes your Samsung with the **xtreme hacked firmware**.

The third option flashes your Samsung with **your original firmware**.

Reboot the PC and 360 and you are done!

## MS28 Instructions

Newer Xbox 360s are using a Samsung drive with an updated MS28 firmware version. Reading and flashing this drive is a little tricky, but it can be done using one of two methods. The first method is the bad flash recovery method, which does not require opening up your drive and soldering. It is best to try this method first. If you can't get this to work, then you can try the VCC switch method.

### Flashing an MS28 Using Bad Flash Recovery Method

**Testing by Redline, XTNS06, rodpad, and IIsTixII showed why some people were able to use this method while others were not. Apparently, using the bad flash recovery method to flash an MS28 drive will only work with VIA chipsets. Even if your chipset works with MS25 and even if you use a hex-edited MTKFlash, it will not work if you do not have a VIA chipset. Please use the VCC switch method instead.**

Follow the previous steps to “prepare” your reading setup (floppy, usb, or NTFSDOS cd). Both X360SAM and manual method will work with MS28, but you need to use an [updated X360SAM](#) with the /sata command in the batch files. This also applies to the manual method, you must use the /sata switch in the MTKFlash command.

#### Reading Original MS28 Firmware with X360SAM and Bad Flash Method

First things first, make sure your SATA chipset is compatible or you are using the hex-edited MTKFlash. ||sTix|| found that he could only get this working if he had a PC cd/dvd drive hooked up to IDE. I would suggest trying to hook up a MTK-based cd or dvd drive to IDE. If you do not hook up the pc drive, you will not get the MTKFlash menu after typing the command.

Power off your Xbox 360 and PC. Connect the Samsung drive to the PC using a SATA cable, but leave the 360 powered off. Insert your bootable floppy/USB /NTFSDOS CD and turn on the computer, booting to a command prompt. If you boot to Windows, restart your computer and set your BIOS boot priority. If using

the NTFSDOS boot CD, hit Enter at the "Select from Menu..." , hit Yes at the NTFSDOS picture, and then move to your NTFS drive.

You should get to a command prompt. At this point, you can finally turn on your Xbox 360. Type the following command a few seconds after turning on your Xbox 360.

SAMREAD XXXXXXXX YYYYYY , using your Xbox 360 serial number

Press Enter

It should display your SATA chipset. **DO NOT** select the port yet. Leave it at the "menu."

If your SATA port isn't showing up, you didn't hexedit mtkflash correctly or you have an incompatible chipset.

While at MTKFlash's port selection menu, power off the Xbox 360. Select the port that the 360 is connected to, even though the 360 is now off. It will "pause" when you select that port. Count to about ten, then turn on the Xbox 360. It should start reading and dumping automatically. It will go from 0-100% 3-4 times, all on the same line. It looks like it is doing the same thing over and over again, because it doesn't start a new line, but let it go, it will finish in a little while.

When the dump is done, it will tell you to restart your pc. Disconnect the SATA cable and power off the Xbox 360. Unplug your floppy/USB/CD and restart your computer. Boot into Windows. Plug in your floppy/USB (or go to the C: drive) drive and find orig.bin. This is your Xbox360 Drives firmware and needs to be kept safe! Make a copy of the file. Then make another one on another drive. Then make another somewhere else. Email it to yourself. You get the drift.

### **Writing the Hacked MS28 Firmware Using X360SAM and Bad Flash Method**

First things first, make sure your SATA chipset is compatible or you are using the hex-edited MTKFlash. ||sTix|| found that he could only get this working if he had a PC cd/dvd drive hooked up to IDE. I would suggest trying to hook up a MTK-based cd or dvd drive to IDE. If you do not hook up the pc drive, you will not get the MTKFlash menu after typing the command.

Power off your Xbox 360 and PC. Connect the Samsung drive to the PC using a SATA cable, but leave the 360 powered off. Insert your bootable floppy/USB /NTFSDOS CD and turn on the computer, booting to a command prompt. If you boot to Windows, restart your computer and set your BIOS boot priority. If using the NTFSDOS boot CD, hit Enter at the "Select from Menu..." , hit Yes at the NTFSDOS picture, and then move to your NTFS drive.

You should get to a command prompt. At this point, you can finally turn on your Xbox 360. Type the following command a few seconds after turning on your Xbox 360.

SAMHACK XXXXXXXX YYYYYY , using your Xbox 360 serial number

Press Enter

It should display your SATA chipset. **DO NOT** select the port yet. Leave it at the "menu."

If your SATA port isn't showing up, you didn't hexedit mtkflash correctly or you have an incompatible chipset.

While at MTKFlash's port selection menu, power off the Xbox 360. Select the port that the 360 is connected to, even though the 360 is now off. It will "pause" when you select that port. Count to about ten, then turn on the Xbox 360. It should start flashing automatically. It will go from 0-100% 3-4 times, all on the same line. It looks like it is doing the same thing over and over again, because it doesn't start a new line, but let it go, it will finish in a little while.

When the flash is done, it will tell you to restart your pc. Disconnect the SATA cable and power off the Xbox 360. Put your Xbox 360 back together and test.

### **Reading the Original MS28 Firmware Using Manual Method and Bad Flash Method**

First things first, make sure your SATA chipset is compatible or you are using the hex-edited MTKFlash. ||sTix|| found that he could only get this working if he had a PC cd/dvd drive hooked up to IDE. I would suggest trying to hook up a MTK-based cd or dvd drive to IDE. If you do not hook up the pc drive, you will not get the MTKFlash menu after typing the command.

Power off your Xbox 360 and PC. Connect the Samsung drive to the PC using a SATA cable, but leave the 360 powered off. Insert your bootable floppy/USB /NTFSDOS CD and turn on the computer, booting to a command prompt. If you boot to Windows, restart your computer and set your BIOS boot priority. If using the NTFSDOS boot CD, hit Enter at the "Select from Menu..." , hit Yes at the NTFSDOS picture, and then move to your NTFS drive.

You should get to a command prompt. At this point, you can finally turn on your Xbox 360. Type the following command a few seconds after turning on your Xbox 360.

```
mtkflash r /m /sata orig.bin
```

Press Enter

It should display your SATA chipset. **DO NOT** select the port yet. Leave it at the "menu."

If your SATA port isn't showing up, you didn't hexedit mtkflash correctly or you have an incompatible chipset.

While at MTKFlash's port selection menu, power off the Xbox 360. Select the port that the 360 is connected to, even though the 360 is now off. It will "pause" when you select that port. Count to about ten, then turn on the Xbox 360. It should start reading and dumping automatically. It will go from 0-100% 3-4 times, all on the same line. It looks like it is doing the same thing over and over again, because it doesn't start a new line, but let it go, it will finish in a little while.

When the dump is done, it will tell you to restart your pc. Disconnect the SATA cable and power off the Xbox 360. Unplug your floppy/USB/CD and restart your computer. Boot into Windows. Plug in your floppy/USB (or go to C: drive) and find orig.bin. This is your Xbox360 Drives firmware and needs to be kept safe! Make a copy of the file. Then make another one on another drive. Then make another somewhere else. Email it to yourself. You get the drift.

### **Injecting DVD Drive Key into Xtreme Firmware**

Follow the hex editing instructions above; they are exactly the same with MS28 firmware. Put the modified.bin firmware on your floppy / USB / C: drive.

### **Writing the Hacked MS28 Firmware Using Manual Method and Bad Flash Method**

First things first, make sure your SATA chipset is compatible or you are using the hex-edited MTKFlash. ||sTix|| found that he could only get this working if he had a PC cd/dvd drive hooked up to IDE. I would suggest trying to hook up a MTK-based cd or dvd drive to IDE. If you do not hook up the pc drive, you will not get the MTKFlash menu after typing the command.

Power off your Xbox 360 and PC. Connect the Samsung drive to the PC using a SATA cable, but leave the 360 powered off. Insert your bootable floppy/USB /NTFSDOS CD and turn on the computer, booting to a command prompt. If you boot to Windows, restart your computer and set your BIOS boot priority. If using the NTFSDOS boot CD, hit Enter at the "Select from Menu...", hit Yes at the NTFSDOS picture, and then move to your NTFS drive.

V41

You should get to a command prompt. At this point, you can finally turn on your Xbox 360. Type the following command a few seconds after turning on your Xbox 360.

```
mtkflash w /m /sata /modified.bin
```

Press Enter

It should display your SATA chipset. **DO NOT** select the port yet. Leave it at the "menu."

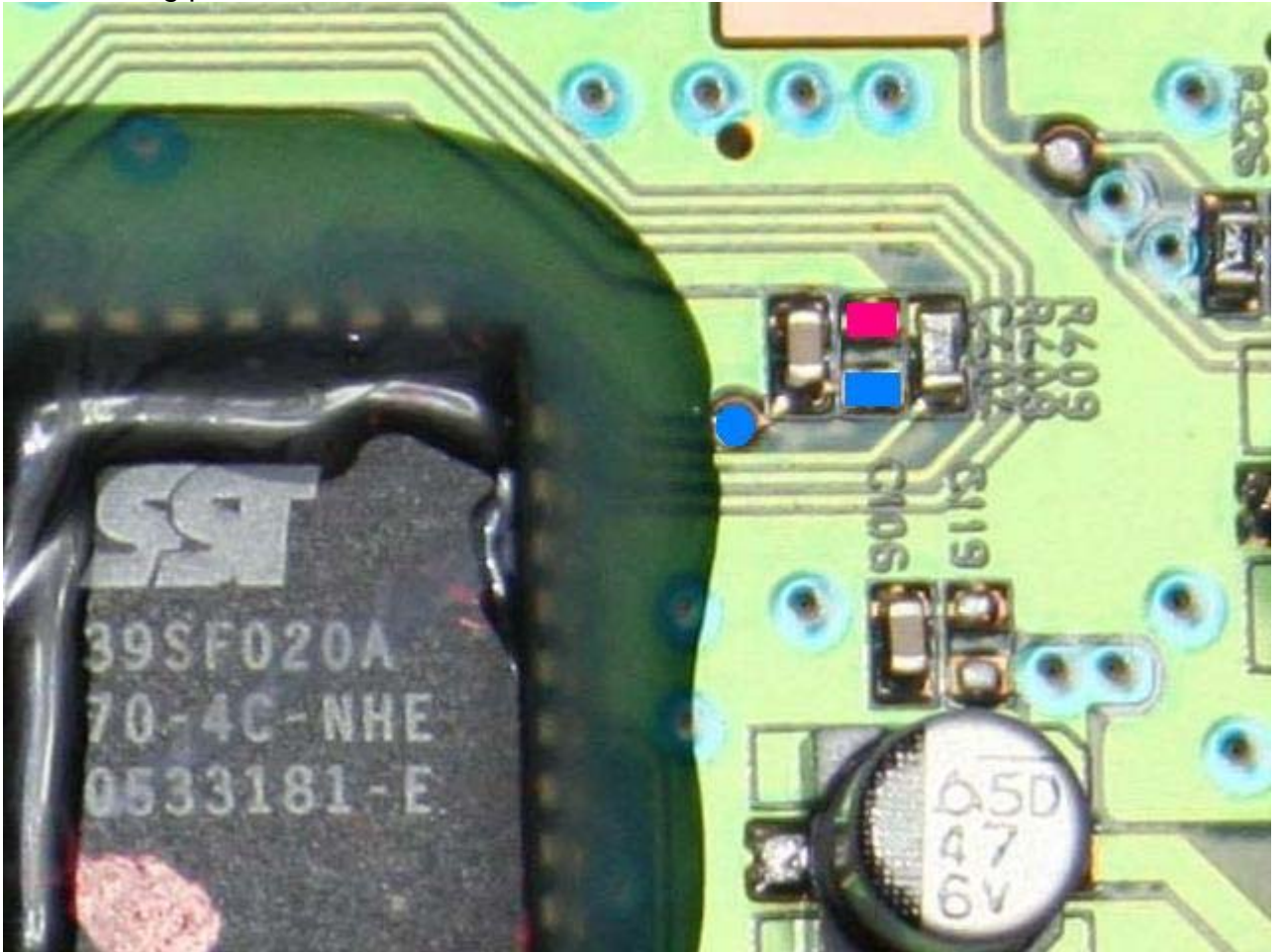
If your SATA port isn't showing up, you didn't hexedit mtkflash correctly or you have an incompatible chipset.

When the flash is done, it will tell you to restart your pc. Disconnect the SATA cable and power off the Xbox 360. Put your Xbox 360 back together and test.

## **Flashing an MS28 Drive Using VCC Switch Method**

Use this method if you can not get the bad flash recovery method to work for you. This method involves opening your drive, de-soldering a resistor, and wiring up a switch.

Open up your drive and desolder the middle VCC resistor (resistor R408) like in the following picture:



Wire up a simple SPST toggle/slide switch to the blue and red locations. Set the switch to “Off.”

Since you already have the drive apart and now have a switch installed on it, it’s probably easier to flash the PCB out of the DVD drive. This is what xboxto did in the following picture. Just make sure you supply power to the board through the Xbox 360 and make sure you still have the video cables hooked up to the Xbox 360.



You can use X360SAM or Manual method to read and flash if using the VCC switch method.

### Reading the Original Firmware Using X360SAM and VCC Switch

First things first, make sure your SATA chipset is compatible or you are using the hex-edited MTKFlash. ||sTix|| found that he could only get this working if he had a PC cd/dvd drive hooked up to IDE. I would suggest trying to hook up a MTK-based cd or dvd drive to IDE. If you do not hook up the pc drive, you will not get the MTKFlash menu after typing the command.

Power off your Xbox 360 and PC. Connect the Samsung drive to the PC using a SATA cable, but leave the 360 powered off. Insert your bootable floppy/USB /NTFSDOS CD and turn on the computer, booting to a command prompt. If you boot to Windows, restart your computer and set your BIOS boot priority. If using the NTFSDOS boot CD, hit Enter at the "Select from Menu..." , hit Yes at the NTFSDOS picture, and then move to your NTFS drive.

You should get to a command prompt. At this point, you can finally turn on your Xbox 360 but leave the switch off. Type the following command a few seconds after turning on your Xbox 360. **Just type the command, don't hit enter!**

SAMREAD XXXXXXXX YYYYYY, using your Xbox 360 serial number

Flick your VCC switch to "on" and then you can hit enter for the SAMREAD command.

It should display your SATA chipset. Select your chipset and it should read and dump your firmware.

If your SATA port isn't showing up, you didn't hexedit mtkflash correctly or you have an incompatible chipset.

When the dump is done, it will tell you to restart your pc. Disconnect the SATA cable and power off the Xbox 360. Unplug your floppy/USB/CD and restart your computer. Boot into Windows. Plug in your floppy/USB (or go to the C: drive) drive and find orig.bin. This is your Xbox360 Drives firmware and needs to be kept safe! Make a copy of the file. Then make another one on another drive. Then make another somewhere else. Email it to yourself. You get the drift.

### **Writing the Hacked Firmware Using X360SAM and VCC Switch**

First things first, make sure your SATA chipset is compatible or you are using the hex-edited MTKFlash. ||sTix|| found that he could only get this working if he had a PC cd/dvd drive hooked up to IDE. I would suggest trying to hook up a MTK-based cd or dvd drive to IDE. If you do not hook up the pc drive, you will not get the MTKFlash menu after typing the command.

Power off your Xbox 360 and PC. Connect the Samsung drive to the PC using a SATA cable, but leave the 360 powered off. Insert your bootable floppy/USB /NTFSDOS CD and turn on the computer, booting to a command prompt. If you boot to Windows, restart your computer and set your BIOS boot priority. If using the NTFSDOS boot CD, hit Enter at the "Select from Menu..." , hit Yes at the NTFSDOS picture, and then move to your NTFS drive.

You should get to a command prompt. At this point, you can finally turn on your Xbox 360 but leave the switch off. Type the following command a few seconds after turning on your Xbox 360. **Just type the command, don't hit enter!**

SAMHACK XXXXXXXX YYYYYY, using your Xbox 360 serial number

Flick your VCC switch to "on" and then you can hit enter for the SAMHACK command.

It should display your SATA chipset. Select your chipset and it should read and dump your firmware.

If your SATA port isn't showing up, you didn't hexedit mtkflash correctly or you have an incompatible chipset.

When the flash is done, it will tell you to restart your pc. Disconnect the SATA cable and power off the Xbox 360. Put your Xbox 360 back together and test.

## Reading the Original Firmware Using Manual Method and VCC Switch

First things first, make sure your SATA chipset is compatible or you are using the hex-edited MTKFlash. ||sTix|| found that he could only get this working if he had a PC cd/dvd drive hooked up to IDE. I would suggest trying to hook up a MTK-based cd or dvd drive to IDE. If you do not hook up the pc drive, you will not get the MTKFlash menu after typing the command.

Power off your Xbox 360 and PC. Connect the Samsung drive to the PC using a SATA cable, but leave the 360 powered off. Insert your bootable floppy/USB /NTFSDOS CD and turn on the computer, booting to a command prompt. If you boot to Windows, restart your computer and set your BIOS boot priority. If using the NTFSDOS boot CD, hit Enter at the "Select from Menu..." , hit Yes at the NTFSDOS picture, and then move to your NTFS drive.

You should get to a command prompt. At this point, you can finally turn on your Xbox 360 but leave the switch off. Type the following command a few seconds after turning on your Xbox 360. **Just type the command, don't hit enter!**

```
mtkflash r /m orig.bin
```

Flick your VCC switch to "on" and then you can hit enter for the MTKFlash command.

It should display your SATA chipset. Select your chipset and it should read and dump your firmware.

If your SATA port isn't showing up, you didn't hexedit mtkflash correctly or you have an incompatible chipset.

When the dump is done, it will tell you to restart your pc. Disconnect the SATA cable and power off the Xbox 360. Unplug your floppy/USB/CD and restart your computer. Boot into Windows. Plug in your floppy/USB (or go to the C: drive) drive and find orig.bin. This is your Xbox360 Drives firmware and needs to be kept safe! Make a copy of the file. Then make another one on another drive. Then make another somewhere else. Email it to yourself. You get the drift.

## Injecting DVD Drive Key into Xtreme Firmware

Follow the hex editing instructions above; they are exactly the same with MS28 firmware. Put the modified.bin firmware on your floppy / USB / C: drive.

## Writing the Modified Firmware Using Manual Method and VCC Switch

First things first, make sure your SATA chipset is compatible or you are using the hex-edited MTKFlash. ||sTix|| found that he could only get this working if he had a PC cd/dvd drive hooked up to IDE. I would suggest trying to hook up a MTK-based cd or dvd drive to IDE. If you do not hook up the pc drive, you will not get the MTKFlash menu after typing the command.

Power off your Xbox 360 and PC. Connect the Samsung drive to the PC using a SATA cable, but leave the 360 powered off. Insert your bootable floppy/USB /NTFSDOS CD and turn on the computer, booting to a command prompt. If you boot to Windows, restart your computer and set your BIOS boot priority. If using the NTFSDOS boot CD, hit Enter at the "Select from Menu...", hit Yes at the NTFSDOS picture, and then move to your NTFS drive.

You should get to a command prompt. At this point, you can finally turn on your Xbox 360 but leave the switch off. Type the following command a few seconds after turning on your Xbox 360. **Just type the command, don't hit enter!**

```
mtkflash w /m modified.bin
```

Flick your VCC switch to "on" and then you can hit enter for the MTKFlash command.

It should display your SATA chipset. Select your chipset and it should read and dump your firmware.

If your SATA port isn't showing up, you didn't hexedit mtkflash correctly or you have an incompatible chipset.

When the flash is done, it will tell you to restart your pc. Disconnect the SATA cable and power off the Xbox 360. Put your Xbox 360 back together and test.

## **Backing Up Games (xtreme3.0 method):**

**Use this if you have flashed with xtreme v3.0 only!!!**

Connect the Samsung drive to the PC.  
Power on the Xbox 360.  
Burn activate.iso to a Dual Layer DVD+R disc.  
Insert activate DVD into the Samsung drive.  
Wait 5 or so seconds then remove the activate DVD.  
Drive now in 0800 mode.

Turn on PC and wait for Windows to boot  
Insert original game disk into Samsung drive and wait for windows to detect disk change.

V41

Run DVDInfoPro

Enter the following four custom cdb commands:

```
AD 00 FF 02 FD FF FE 00 08 00 01 C0  
AD 00 FF 02 FD FF FE 00 08 00 03 C0  
AD 00 FF 02 FD FF FE 00 08 00 05 C0  
AD 00 FF 02 FD FF FE 00 08 00 07 C0
```

Then save hexadecimal display as bin file as SS.bin

## **Extracting PFI (Physical Format Information) Sector**

Run DVDInfoPro.

From Advanced Commands pull down menu, choose Send Custom Command  
From Preset Commands pull down menu choose "00h Physical Format Information" from under the Read DVD Struct Commands heading  
Click "Send"

Then save hexadecimal display as bin file as PFI.bin

## **Extracting DMI (Disk Manufacturing Information) Sector**

Run DVDInfoPro

From Advanced Commands pull down menu choose "04h Disc Manufacturing Info"

Click OK on Read DVD Structure Option window

Then save hexadecimal display as bin file as DMI.bin

## **Creating a game backup**

Make sure the Samsung is still in 0800 mode with the activate DVD

Extract Isobuilder.rar

Insert original game disk into drive and wait for windows to detect disk change

Run DVDInfoPro

Enter the following custom cdb command to unlock drive: (game data visible)

V41

FF 08 01 01

If you receive a sense error, just ignore it. It means the drive is already unlocked. Sometimes the drive will unlock after extracting the ss. Open ISO Buster as normal.

Run Isobuster

Right click on DVD and select Extract From-To

Click Length and enter number of LBAs as follows:

Xbox 1 Original Number of LBA to read 3431264 decimal

or

Xbox 360 Original Number of LBA to read 3567872 decimal

Select User Data (2048 bytes/block)

Click Start Extraction

Enter filename as game.iso and click Save

Upon read error dialogue box choose fill with blank zeros for sector and select use this selection for all errors

Copy game.iso, ss.bin, PFI.bin and DMI.bin to the relevant isobuilder directory (Depending on Xbox 360 or Xbox 1 game)

Run build360.bat (Xbox 360 game) or build.bat (xbox 1 game).

These batch files now expect PFI and DMI bin files

Ensure your burner will set the booktype of DVD+R DL to DVDRom

Burn with CloneCd and choose the image.dvd file

## Turning off 0800 mode of firmware

Either insert game backup (Xbox 360 or Xbox 1) or DVD movie. This de-activates 0800 part of firmware or turn off console.

## Backing Up Games (non-xtreme3.0 method):

**DO not use this if you have flashed with xtreme v3.0!!!**

To backup Xbox360 games we need to get the Xbox360 Drive visible in Windows. This requires a slightly different firmware. We then need to extract the

V41

Security Sectors (SS) from the disc. After that we create the .iso image and inject the SS's into it.

You will need [DVDInfoPro](#) CloneCD and WxRipper.

## Flashing the Firmware (non-xtreme3.0 method):

First you need to flash the XTRM0800.BIN on your Xbox360 Drive using your MTKFLASH.EXE floppy disk. Make sure you have your modified firmware with your Key in it backed up safe somewhere.

Copy XTRM0800.BIN onto the floppy if you haven't already.

Boot to the floppy as before. At the prompt type:

```
A:> mtkflash w /m xtrm0800.bin
```

(If you are not using a floppy change directory to wherever you put the files)

Press Enter & proceed as before.

Reboot into Windows and insert the game you want to backup into your Xbox360 Drive.

## Extracting the Security Sectors:

Open DVDInfoPro.

Down in the bottom left, you can select your xbox360 drive. On the left bottom of the screen select "Send Custom Command", there will be a warning displayed on screen, click "OK". This will extend the right side of the program with a new window. Leave all of the default boxes checked, you don't need to mess with any of the settings.

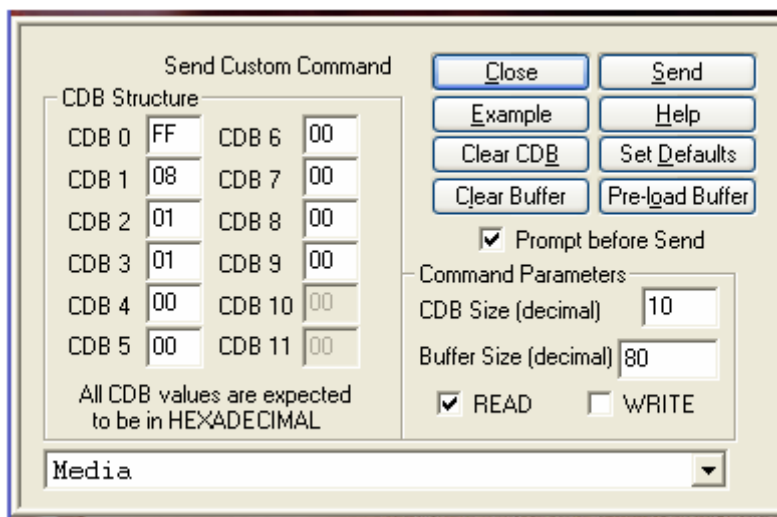
You have 12 boxes here, all filled with 00s. Going from top to bottom (they are numbered in order) you can put in a command.

Each two digits is a byte:

```
AD 00 FF 02 FD FF FE 00 08 00 01 C0
AD 00 FF 02 FD FF FE 00 08 00 03 C0
AD 00 FF 02 FD FF FE 00 08 00 05 C0
AD 00 FF 02 FD FF FE 00 08 00 07 C0
```

Put those commands in, in order. After each string, click the "Send" button. Once you have sent all four commands, look for a button in the top right. It will say "Save As Hexadecimal BIN File". Save your file as SS.BIN.

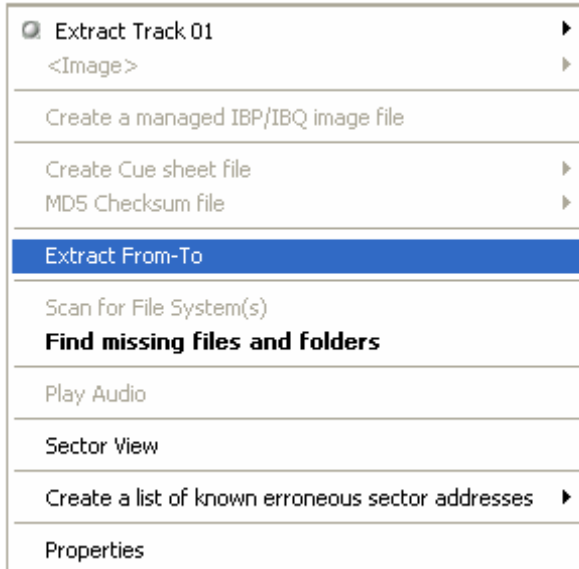
4. Now put in the command displayed on the image below and press send.



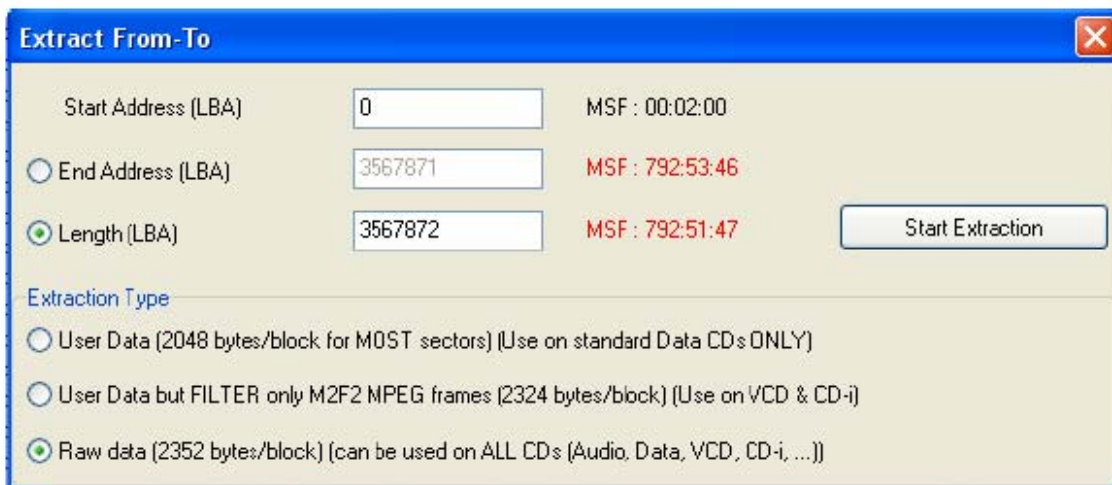
## Making the Image (Isobuster Method):

The next tool we will need is Isobuster, included in the Xtreme bundle.

Open Isobuster, right click on the Toshiba-Samsung DVD-Drive and press "Extract From-To" (see image).



Unlike the image below, select User Data (2048 bytes/block for MOST sectors)



At the Length (LBA) for Xbox 360 games enter 3567872, for Xbox 1 games enter 3431264, when finished press "Start Extraction".

Save your file as GAME.ISO

When you receive a read error dialogue box, choose "fill with blank Zeros" for sector and select "use this selection" for all errors.

## Combining the Image & SS Files (Isobuster Method):

Copy the GAME.ISO and SS.BIN to the Xbox1 or Xbox360 isobuilder Directory.

Run build360.bat (Xbox360 game) or build.bat (xbox1 game)  
You will have 2 files when this is finished; IMAGE.000 and IMAGE.DVD.

## Making the Image (wxRipper Method):

You need XBOX360\_SS\_Merger\_1.6 (thanks to HellDoc) and wxRipper (thanks for the great too Gael360).

<http://dwl.xbox-scene.com/xbox360pc/isotools/XBOX360-SS-Merger-1.6.rar>  
<http://gael360.free.fr/files/wxRipper-1.2.rar>

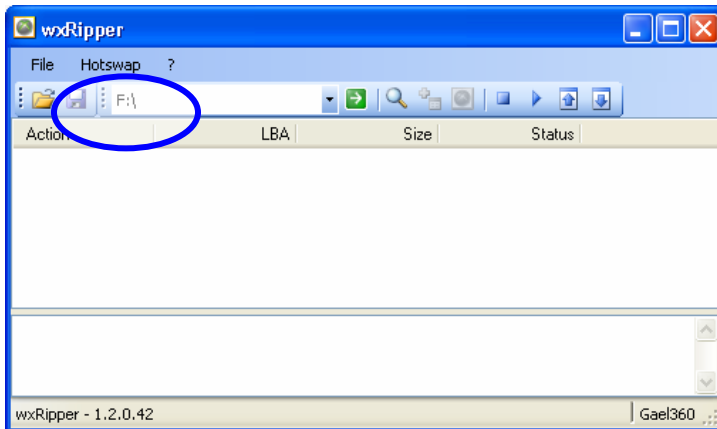
You also need a DVD drive you can use externally that you are not that attached to (it is going to get dismantled a bit). **Or you can use the eject hole on the front of your drive and a paperclip! Try this method first before taking your drive apart.**

You also need a large DVD...8gb or more preferably. I use Hitch (the movie). It is 7.95GB and I still think it might be too small for Tomb Raider Legend. I will not go into why we need it, lets just say we need the TOC.

Open up your DVD drive case so you can swap disks without pressing eject.  
**OR use a paper clip in the little eject hole to avoid damaging the drive – thanks Sniperkilla - edit: sometimes this doesn't work...depends on your drive make and model.**

Remember the laser is dangerous and remember the little magnetic bit in the top that holds the disc in place.

Start wxRipper and select the right drive:



**Stick in your large DVD. Let it get recognised then press The “Stop” button on wxRipper. If you use a USB DVD drive you may need to wait 2 minutes for it to spin down by itself as the “Stop” button does not work on USB. Remove the disk without using eject and replace it with your Xbox360 game disk.**

**Press the “Play” button then the “Find Magic Number” button. You can now press the “Start Dump” green button.**

**Save the image with whatever name you like.**

**If you get errors in wxRipper, your DVD drive doesn't like the bad sectors between LBA19408 & LBA20479. LBA20480 isn't a bad sector, but your drive has a problem aligning the lens on LBA20480...**

To fix :

- 1 - Click on 'Find magic number', the action list is generated
- 2 - Save the action list to a layout file (File->Save layout file...)
- 3 - Edit the layout file with notepad, you should have these 3 first lines :

```
C19408
D1072
C109344
```

if you want to make an ISO with the XDVDFS session starting at LBA129824, like a raw dump, replace these 3 lines with these ones :

```
D19408
D1072
D109344
```

Then File-> Load Layout File and dump as normal.

**OR METHOD 2:**

*Regarding the layout file:*

- Usually the first 3 lines are like this:

- C19408
- D1072
- C109344

- People say to change them to this (bold represents the changes):

- **D**19408 <- D = Dummy instead of C (Copy)
- D1072 <- Same as original
- **D**109344 <- D= Dummy instead of C (Copy)

In this case, all you're doing is 'faking' the first three lines. I figured out that 9 out of 10 problems occur at the 3rd line, so that's really the only one you need to Dummy. Therefore:

- Most of the time this will work (bold represents the only change):

- C19408 <- Same as original
- D1072 <- Same as original
- **D**109344 <- D = Dummy instead of C (Copy)

This way you get more of the original information. I'm not sure if this matters, but I say more is better when it comes to duplicating a game.

*If you want to go even further:*

- Since I noticed most people (myself included) occasionally get a CRC error at 91136, especially on games like Tomb Raider and Hitman, I use this layout (replace first 3 lines with these 4):

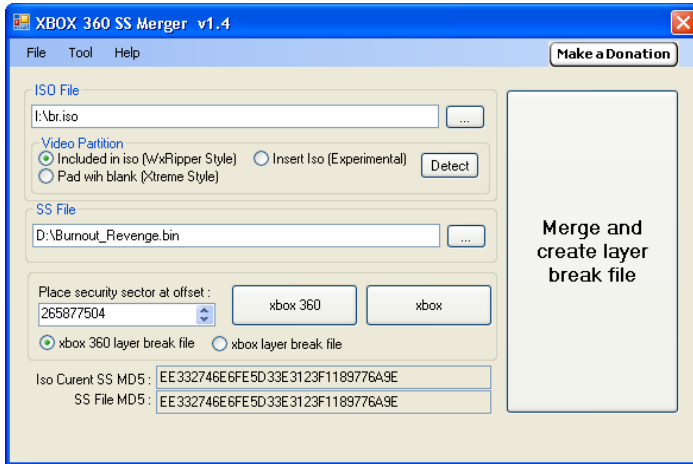
- C19408 <- Same as original
- D1072 <- Same as original
- C91135 <- Original used to be C109344, which I split into 2 parts, stopping at 1 byte before my CRC error @ 91136
- D18209 <- Dummy the remainder of the part that gives the error. 18209 (this line) + 91135 (previous line) = 109344 (original number)

V41

Thanks to PSoft!

## Combining the Image & SS Files (wxRipper Method):

Now you can start up HellDocs excellent XBOX360 SS Merger 1.4.exe.



Select the .iso file you just made in the top box.

Choose which method you ripped your backup; isobuster (also known as xtreme style) or wxRipper. If you downloaded an iso and you don't know how it was made, tough. You are a bad, bad person.

Now press "Xbox360" if you are backing up an Xbox360 game (duh).

Select "Xbox360 layer break file".

Press "Merge and create layer break file"

Press "donation" if you think HellDoc deserves it!

That's it. You can now burn your game! But before you do, read about bitsetting...

## Booktype / Bitsetting:

**From Xtreme's readme:**

Run build360.bat (Xbox 360 game) or build.bat (xbox 1 game)

**Ensure your burner will set the booktype of DVD+R DL to DVDRom**

**Burn with CloneCd and choose the image.dvd file**

When the booktype field (bitsetting) is changed to DVD-ROM then DVD players are fooled and will think the user has put in a DVD-ROM disc instead of a DVD+R disc and will read it accordingly. This results in an increased chance that the player is able to read the disc and that's why the ability to change the booktype field (bitsetting) is essential to a lot of users. Certainly owners of a DVD player that requires this field to be set to DVD-ROM, in order to work properly, will prefer a DVD recorder that supports setting the booktype field. - Quote from CDFreaks.com

**REMEMBER** you must have a bitsetting capable DVD+R DL drive. If you do not you may be able to upgrade its firmware (wow a legit firmware flash!) See here for a LOT of drive firmwares: <http://tdb.rpc1.org/>

To set the booktype in DVDInfoPro:

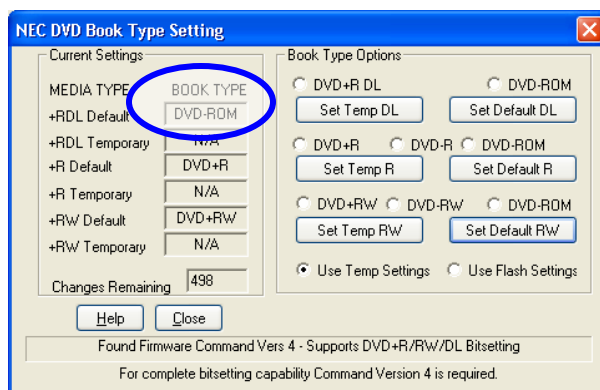
Start DVDInfoPro

Click on the "+RW" icon on the top row

Select DVD-ROM

Press button marked "Change +RDL Mode"

Press Close

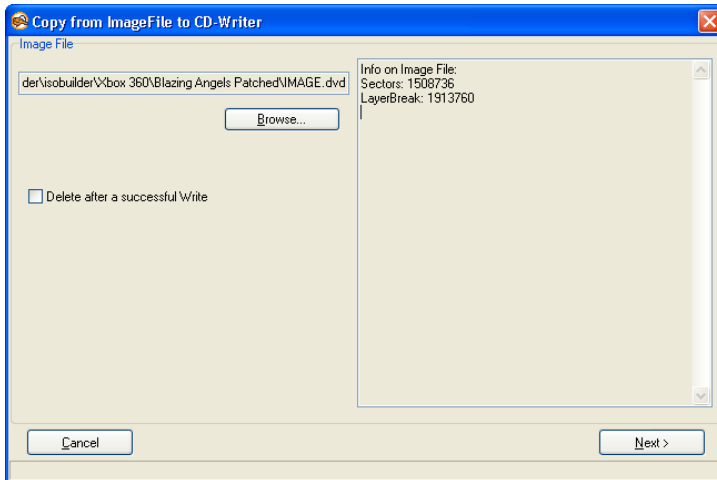


Now whenever a DVD+R DL is burned it will be bitset to read like a DVD-ROM.

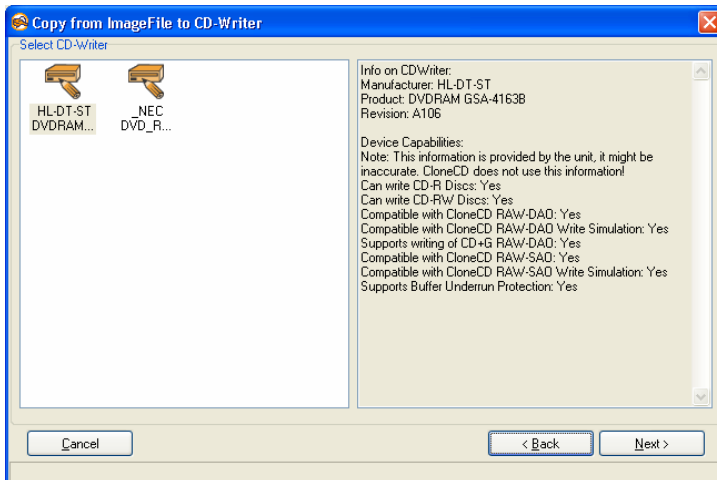
**BE AWARE:** If you start Nero or similar that can also change the bitsetting, make sure Nero is set to "unmodified" or "current recorder setting", found in Recorder-> Choose Recorder then select the drive and click on "Options"

## Burning Your Backup:

You need the latest version of CloneCD for this. Once you have checked your booktype/bitsetting open CloneCD and select “Write from Image File” (second icon from left). Press “Browse” and select your IMAGE.DVD file.



Select the correct drive you wish to burn with and press “Next”



Set the write speed to 2.4x and press “OK”

Wait until it completes. If writing the lead-out takes a while, be patient and go make a drink. Don’t smoke though, its bad for you.

## 2<sup>nd</sup> Reflash To Play (if currently flashed to 0800):

Now you need to go back to “Reflashing Your Drive” in this tutorial and put your hacked firmware back on.

Then test your backup and give yourself and all the people below a big cheer!

## Flashing the Samsung MS28

### Overview

Disassemble Xbox 360  
Connect Xbox 360 DVD drive to PC  
Make Floppy/USB boot disk  
Boot PC with bootable disk  
Backup Xbox 360 Drive firmware using Bad Flash Recovery method (or VCC method)  
Boot to Windows  
Patch original firmware to Xtreme firmware  
Flash

### Bad Flash Recovery: (thanks to Andy H.)

OK, I've seen lots of posts in various topics about people with apparently dead drives. I had exactly the same problem after my floppy decided to give up the ghost mid-flash and the drive Borked.

Various solutions were offered by the group, none of which worked, so I was left with the task of finding another drive to hotswap with (Yeah, right!) or find my own solution.

This is what I found worked for me. (Twice, as I tested again by borking it a 2nd time)

You'll need a Bootable Floppy with MTKFLASH and your firmware. (we'll call this your original.bin)

Your Borked [DVD drive](#) attached to SATA 1 on your [motherboard](#).

Boot from Floppy and get to a Dos prompt.

Type in "MTKFLASH W /SATA /M original.bin

You should get a response from the system with a list of possible sata ports to flash to. (For arguments sake this is SATA 1 and SATA2 in this tutorial)

Turn off the power to the [DVD](#) drive wait a second and turn it back on again.

Now hit 1 on the [keyboard](#) to start the flash. (in response to the Sata 1 port on the screen)

OK, now it will start flashing or sits waiting at "Port: d800, Master/Slave: a0"

V41

If it is waiting for more than a few seconds hit escape twice to stop the attempt and power off the drive again and keep trying the last part again. It will work after a few attempts.

This is what I have figured out so far and why this works.

MTKFLASH is looking for a response code 70 from the drive to start flashing. Whilst the hitachi drives have a distinct recovery mode the samsungs show a code 70 JUST after power on. I'm assuming this is a small recovery window that we can use.

The MTKFLASH [software](#) doesn't really care what device is on the SATA bus at the beginning, as long as it can detect something. Hence is people put a hot swap drive or [hard drive](#) on the sata bus, the software says "Ahh, SATA 1 has a device on there" and gives to the option to flash that port.

Only when you press 1 on the keyboard to start flashing does it try to detect what KIND of device it is and waits for the required 70 code to start flashing.

So in summary ..

Get MTKFLASH working so it detects a device on your Sata bus (Either the DVD drive or a hard drive)

Then start the flashing procedure JUST AFTER the dvd is given power, after a couple of attempts it should catch the Code 70 and start flashing.

Hope this helps.

## Thanks to:

[Kev/SeventhSon](#), Commodore4Eva, xbox-scene.com, xboxhacker.net, Probutus, Bluecop, MacDennis, TheSpecialist, Gael360 & JSR, Helldoc and everyone else who did the hard work. The boys did good. Thanks to kev for the \$50 for putting his name in a flash font.

## Last updated 21-8-06

Changes from v40: added SLAX/SATA list, instructions for stealth firmware

**OPA-XTREME-HITACHI-7IN1-V2\_1.RAR** is the current Hitachi fw to use.

Written & Compiled by: geebee & contributors  
([geebee@gmail.com](mailto:geebee@gmail.com) or [Textbook](#) for any changes)

# Hack the 360: The Tutorial

Backing Up, Modifying & Flashing the Hitachi/LG Drive (32, 36, 40, 46, 47 & 59 FW's)

v40 now hacked! Thanks to Team Avalaunch...

Written/Made/Everything by: geebee  
([geebee@gmail.com](mailto:geebee@gmail.com) for any changes)  
Compiled by: Sergio965

**BEFORE YOU START, READ**

[Start Your Reading Here](#)

<http://forums.xbox-scene.com/index.php?s=cdbaa5713c3134aa66aa2493c814c259&showtopic=513412>

[Then if you want more background read here](#)

[www.kev.nu](http://www.kev.nu)

Now read this tutorial, twice. If you don't understand any terms, think twice about doing this.

This tutorial will explain every step in backing up your original firmware, creating a working hacked firmware for your Hitachi v47 DVD-Drive and flashing it back to the DVD-Drive. It will also explain how to burn successful game back-ups.

It is really important to keep in mind that the complete process can be risky if you don't know what you are doing.

## **WARNINGS**

**IF YOU WANT TO KEEP YOUR WARRANTY DO NOT TRY THIS.  
OPENING THE CASE INVALIDATES THE WARRANTY.**

**Don't ask for illegal files. ANYWHERE. Especially not on public forums.  
Read all the forum rules. Do not talk about .ISO images you have  
downloaded.**

**We are not responsible for any misreading or damage done to your  
Microsoft Xbox 360 in any way.**

**Please do not attempt to try this if you don't understand any of the steps  
below. Normal to Average PC experience is required in order to  
successfully complete the installation.**

**Do not stick your fingers into live electrical parts. Do not stick any other  
parts of your anatomy in either.**

**Lasers BLIND! Do not look into them if you need to hotswap disks when  
using WxRipper (to follow)**

## Overview:

### Firmware Tasks:

- Disassemble Xbox360
- Connect Xbox360 Drive to PC
- Boot to Windows
- Backup Xbox360 Drive firmware
- Backup Xbox360 Drive firmware to 2 other places for safety
- Flash Xbox360 Drive with hacked firmware
- Rebuild Xbox360 (unless you want to make some backups now)
- Test Xbox360

### Game Backup Tasks:

- Disassemble Xbox360
- Connect Xbox360 Drive to PC
- Boot to Windows
- Patch your orig,bin with f900 fw
- Firmcrypt the patched fw
- Flash the appropriate sectors with flashsec\_47
- Extract Security Sectors
- Make Image with wxRipper
- Combine SS and game image with SS Merger 1.x
- Burn image
- Flash Xbox360 Drive with v47 hacked firmware to play games
- Rebuild Xbox360
- Test backups

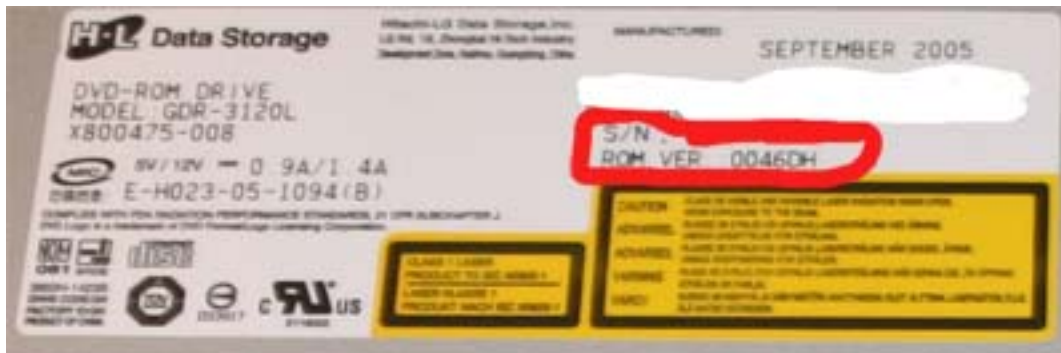
**WARNING:** If you are going to connect your 360 and PC together in *\*any\** way, then you *\*must\** provide the 360 with a path to true earth ground. This is because the 360 has a floating ground and horrible things happen if all connected systems do not agree on the reference voltage. I used a couple of croc clips from the chassis of the 360 to the chassis of my PC to achieve this.

## Tools:

- 1) Xbox 360 with Hitachi Drive



How to find your ROM version:



(pictures from X-S)

- 2) **OPA-XTREME-HITACHI-7IN1-V2\_1** contains the fw
- 3) Torx t10 screwdriver head
- 4) A PC with a suitable SATA chipset. (Pretty much anything will work, once you get into ModeB and have the right drivers, as long as your drive is recognized by Windows)

ModeB Slax List		
Motherboard	Chipset	ModeB?
SOME ?	VIA VT 8237 (onboard)	Yes – but reported not working by some people ?
ALL*	SIL 3112 (onboard and pci)	Yes
ASUS K8N	nForce3	Yes
HP 5100MT	Intel 915	Yes
	SIIG SC-SAT212 (pci card)	Yes

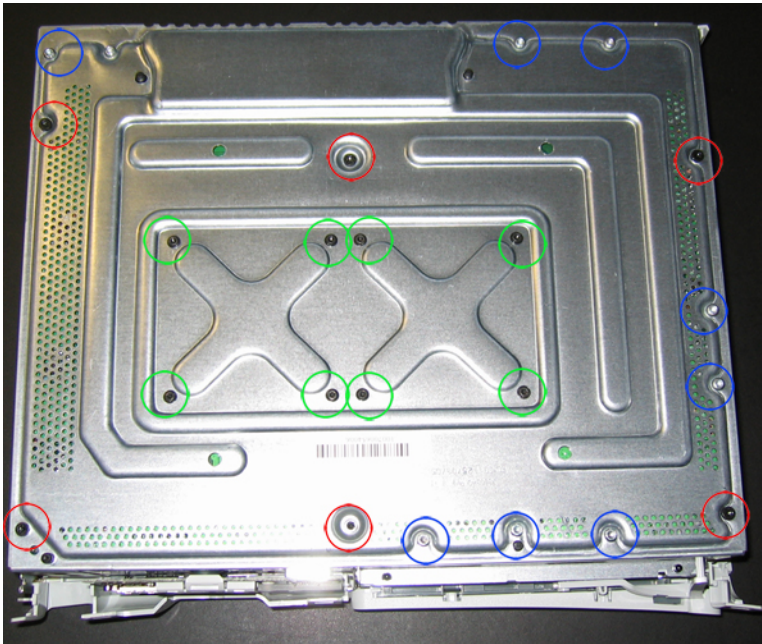
### SATA NOTES:

Make sure your SATA ports are set to NATIVE/IDE mode NOT RAID

**WARNING:** If you are going to connect your 360 and PC together in *\*any\** way, then you *\*must\** provide the 360 with a path to true earth ground. This is because the 360 has a floating ground and horrible things happen if all connected systems do not agree on the reference voltage. I used a couple of croc clips from the chassis of the 360 to the chassis of my PC to achieve this.

## Xbox 360 Disassembly:

To disassemble your Xbox 360 to get the DVD Drive out, follow these instructions but you do **NOT** need to remove the black heatsink screws. All you need to remove is the six silver long screws circled in RED:



[Anandtech Xbox 360 Stripping Guide](#)

Keep the power connector plugged in your Xbox 360.

## Opening the 360 (the perfect way)

Take the tub your spindle of discs came and cut a bit from the side of it and put it over the console as shown. Mark out where the holes are...

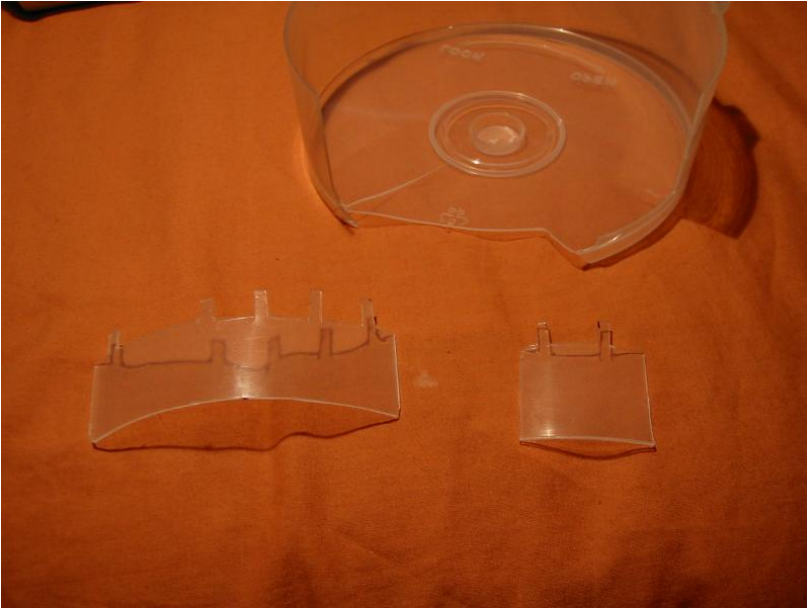
V41



... then make it into a key like this. the tabs need to be about 1cm long.



Do the same for the other side and you'll get two xbox 360 case opening keys that look like these...



## Step 2

Open the front of the console as normal and put a bit of newspaper or something inside the case to hold the front open a bit, then insert the key, push with a bit of force and you should hear it click and the case will open....



... repeat for the other side and you're done!

V41



Thanks to Hydra!

## Xbox 360 Connection:

Unplug the SATA cable from the back of the Xbox360 Drive. Connect a SATA cable from your PC SATA connection to the back of the Xbox360 Drive. Connect the video cable to the back of the Xbox360. If you do not do this, the Xbox360 will power off at an inappropriate moment (like when flashing). You need to disable RAID for that SATA connection in your PC bios. Set it to IDE instead.

## Connecting the Hitachi/LG Drive to your PC:

To get it recognised in Windows we need to get the drive into modeb (pronounced “mode bee”).

To do this we will use Probutus’s excellent Slax Live CD **or** the crossed wires / 1k Resistor method **or** the HotSwap method (thanks stonersmurf) **or** xecuters Connectivity Kit: **NOW INCLUDES OPA-XTREME-HITACHI-7IN1-V2\_1 METHOD!!!**

### Geebees Method Rating:

#### **OPA-XTREME-HITACHI-7IN1-V2\_1 method:**

100% ALWAYS WORKS. Don’t use anything else **once** your drive is flashed with this fw.

#### **Slax CD :**

100% (if your SATA chipset is compatible) 0% (If chipset isn’t compatible)

#### **Crossed Wires or 1k Resistor Method:**

100% ALWAYS WORKS. If it doesn’t for you, you are doing it wrong. Some risk.

#### **HotSwap:**

100% but you need a 360 Samsung drive or SATA DVD-ROM

#### **Xecuter Connectivity Kit:**

100% but expensive ;-)

<http://rapidshare.de/files/18684918/live-cd.iso.html>

Note: you cannot use ANY other Slax iso. This one is specially adapted.

and Memdump:

<http://www.kev.nu/360/dvdshort.html#2> and click on memdump\_win.zip or find it in c4e’s firmware release.

## New **OPA-XTREME-HITACHI-7IN1-V2\_1**Method:


Once you have flashed your Hitachi with this firmware you can get into modeb by turning on the 360 with the drive tray OPEN. To flash the first time, you still need to use one of the methods below...

### **Slax Method:**

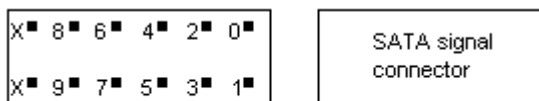
Connect the Xbox360 Drive up to your PC as above to a suitable SATA port. Set your bios to boot from CD first and boot the Slax CD. When it boots you will see a lot of text. If you look close you will see it say the drive is in modeb (with thanks to Kev). When you get to the "login:" prompt reset your PC (with the reset button) but leave the Xbox360 on!

Remove the CD and boot into Windows. If it sticks at booting into windows...press eject on the Hitachi drive tray!

### **Crossed Wires/ 1k Resistor Method to get to modeB:**

**FOR SAFETY:** Use a 1k Resistor  (brown black red gold bands) instead of or connected to the piece of wire. They are easy to find and will prevent you bricking your 360. (thanks Seventhson)

Stick 2 pieces of thin wire in the back of the white connector without cutting or opening anything, in the pin 9 and GND (0) position. These wires jam in next to the black ones that are in the same hole. It is easier to lift the small white tab and pull out the existing wire, then hold the new wire against that one and slide the connector back in.



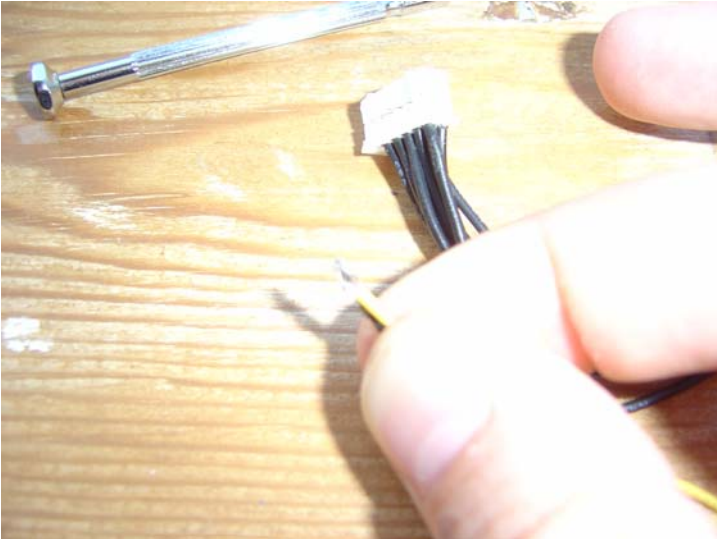
Xbox 360 DVD drive power connector pinout

Lift tab and pull out existing wire:

V41



Hold new wire against the existing one:



Now push both back into the slot:

V41



A bit of tape to hold them in place:



Connect a SATA cable from the 360 drive to your PC

With the 360 turned OFF, hold the 2 wires connected together with your fingers.

Push the 360 power button and as soon as the green light comes on disconnect the wires as quickly as possible. **KEEP THOSE WIRES TOGETHER TOO LONG AND YOU COULD GET AN XBOX-SHAPED BRICK!**

The little green light in the centre (not the ring of light) will flash fast and you will hear the drive start to spin. **THOSE ARE THE INDICATORS YOU ARE IN MODEB.**

Turn on your pc and windows will recognize it. If XP freezes at boot, eject the 360 drive and it should carry on booting. To get out of Modeb, just restart the 360.

What you can do simply is lift the tab of white plastic and slide the connectors for 0 and 9 out of the block. Then put your two wires alongside them and slide them back in. This takes less than a minute. Solder a £1 switch from Halfords on and off you go...

### **HotSwap Method:**

This is possible if you have a SATA dvd-drive/IDE dvd-drive with a SATA adaptor or a 360 with a Samsung drive and one with a Hitachi drive. Boot into Windows and after your SATA drive (dvd-rom or Samsung dvd-rom drive) is detected (ie has a drive letter) just swap the SATA cable to your Hitachi DVD-ROM. When you use memdump, remember that the drive letter will still show as the old drive, in My Computer it would still show as whatever drive you used to HotSwap. Don't let it confuse you!

### **Connectivity Kit Method:**

If you're using the Xecuter kit, nothing should be plugged into your Xbox360, only the DVD drive from it. No clips/grounding necessary. Remove the DVD drive from the console and put the console somewhere safe.

1. Turn your PC off
2. Plug the Hitachi drive in (power via xecuter kit and SATA into your SATA card or onboard port)
3. Make sure the debug button is **down** and eject button is **up**
4. Turn the PC on (should see red light on power adaptor)
5. Boot into Windows
6. Check Explorer to see if the drive has been assigned a letter. If not, right click My Computer, click Manage, goto Disk Management under Storage, right click the drive and assign it a letter e.g E:

You should leave the debug switch down (red LED on power adaptor). It does no harm to the drive. You do not need to press it quickly or anything.

Whichever method you use, carry on from here:

If you get it into mode b and windows cannot see it...go to Device Manager and see if it is in there under "DVD/CD ROM Drives". If it is, right click on it and select "Properties". Then select the "Volumes" tab and click "Populate". Now go to My Computer and it should be visible.

## Hitachi Flashing with Hitachi-LG Firmware v2.1:

The autoflasher is the **best** way to flash the Hitachi as it **does not** require you to copy the key across using KDX or hex editor. It patches the firmware around the key.

Also everything is in one auto-detecting batch control, no more bricked drives, due to flashing the wrong FW to the wrong version of drive, and updating does not start unless a BACKUP has been correctly stored and checked and it will reflash automatically until it is correct!

Even better, you can get to modeb easily by turning the 360 on with the drive tray open.

Also, if when booting a backup game and the dashboard displays OPEN TRAY, you just need to press the EJECT button, the tray will stay CLOSED, but the dashboard will "auto-trick" into reading the game!

### To Use:

Extract the files and from a cmd prompt in the right folder run FLASH21.BAT  
<Hitachi drive letter> <unique 4 digit number> batch file from a dos prompt specifying drive letter:

V41

E.g.

```
C:>flash21.bat g 1571
```

This will create a BACKUP directory "X21-1571.OPA" and the program will store FIVE firmware files:

```
---- key.bin   ---- DRIVE KEY /// DRIVE KEY
---- was.bin   ---- Your drive before FLASH
---- gdrXX.bin ---- The untouch original fw
---- XX_21.bin ---- The patched Xtreme21 fw
---- now.bin   ---- Your drive after FLASH!
```

XX in the above names will be the version of your Hitachi

Program will not flash anything unless a BACKUP is correctly made and stored!

## **To restore the Hitachi Drive with Original firmware:**

In the right folder run RESTORE.BAT <Hitachi drive letter> batch file from a dos prompt specifying drive letter:

E.g.

```
C:>restore.bat
```

## **Patching Your Firmware For Stealth**

For now, Stealth firmware can only be used if the drive is already flashed with GaryOPA's Xtreme v2.1 firmware.

Download Maximus/Carranzafp's v1.2 Hitachi Stealth Maker from the usual place. Connect your pre-hacked Hitachi drive to your PC and get it into ModeB using one of the previously mentioned methods. Open a command prompt, and move to the Tools directory where you extracted the stealth maker. Use the following command:

```
read.bat <your_drive_letter> hacked.bin
```

Ex: If my Hitachi drive is drive letter G: , I would use read.bat g hacked.bin

Now open the Hitachi Stealth Maker program (hitachi\_stealth.exe). At the top labelled input firmware, browse and select the hacked.bin that you just dumped in the Tools directory. In the Options section, choose Non Stealth on MODE B and Tray Open. Click "Generate Stealth FW" and save as stealth.bin in the Tools directory.

## Flashing the Stealth Firmware for v47 Hitachi Drives

Open a command prompt and move to the Tools directory. Notice you will be flashing the “suffix -e” firmware. Type the following command:

```
47flash <your_drive_letter> stealth-e.bin 90005000 1000
```

Ex: 47flash H stealth-e.bin 90005000 1000

**Do not advance further until the above command executes without error. If it errors, keep retrying until it does not!**

Next, type the command:

```
47flash <your_drive_letter> stealth-e.bin 90033000 1000
```

Ex: 47flash H stealth-e.bin 90033000 1000

**Once again, don’t exit until that command executes without error. If it errors, keep retrying until it does not!**

Your drive should now be flashed with the stealth firmware.

## Flashing the Stealth Firmware for v46, v32, v36, and v40 Hitachi Drives

Open a command prompt and move to the Tools directory. Notice you will be flashing the “suffix -e” firmware. Type the following command:

```
46flash <your_drive_letter> stealth-e.bin 90005000 1000
```

Ex: 46flash H stealth-e.bin 90005000 1000

**Do not advance further until the above command executes without error. If it errors, keep retrying until it does not!**

Next, type the command:

```
46flash <your_drive_letter> stealth-e.bin 90033000 1000
```

Ex: 46flash H stealth-e.bin 90033000 1000

**Once again, don’t exit until that command executes without error. If it errors, keep retrying until it does not!**

Your drive should now be flashed with the stealth firmware.

## **Flashing the Stealth Firmware for v59 Hitachi Drives**

Open a command prompt and move to the Tools directory. Notice you will be flashing the “suffix -e” firmware. Type the following command:

```
59flash <your_drive_letter> stealth-e.bin 90005000 1000
```

Ex: 59flash H stealth-e.bin 90005000 1000

**Do not advance further until the above command executes without error. If it errors, keep retrying until it does not!**

Next, type the command:

```
59flash <your_drive_letter> stealth-e.bin 90033000 1000
```

Ex: 59flash H stealth-e.bin 90033000 1000

**Once again, don't exit until that command executes without error. If it errors, keep retrying until it does not!**

Your drive should now be flashed with the stealth firmware.

## **Extract a Security Sector:**

Once flashed with v2.1...

Connect the Hitachi to PC.

Ensure XBOX video cable is plugged into back of console.

Power on the Xbox 360 console.

Open the drive Tray, by pressing the EJECT button.

Pull the power connector out of the 360 (back of console).

This will force the console to leave the tray in the OPEN position.

Plug the power connector back into the Xbox 360.

Power on the 360 using the "power" button.

V41

Drive is now in Mode B.

Turn on your PC and wait for Windows to boot.

Insert original game disk into Hitachi drive and wait for windows to detect disk change.

In the right folder run "getss.exe <Hitachi drive letter> ss.bin" from a dos prompt specifying drive letter:

E.g.

C:>getss.exe g ss.bin

## Creating a game backup

Make the SS.BIN file first.

Extract the included "ISOBUILD.RAR" package.

Insert original game disk into Hitachi drive and wait for windows to detect disk change.

Run Isobuster

Right click on DVD and select Extract From-To

Click Length and enter number of LBAs as follows:

Xbox **1** Original Number of LBA to read 3431264 decimal

Xbox **360** Original Number of LBA to read 3567872 decimal

Select User Data (2048 bytes/block)

Click Start Extraction

Enter filename as game.iso and click Save

Upon read error dialogue box choose fill with blank zeros for sector and select use this selection for all errors

\* Copy game.iso and ss.bin to the relevent isobuilder directory  
(Depending on Xbox 360 or Xbox 1 game)

V41

- \* Run build360.bat (Xbox 360 game) or build.bat (xbox 1 game)
- \* Ensure your burner will set the booktype of DVD+R DL to DVDRom
- \* Burn with CloneCd and choose the image.dvd file

## **What to Try if Backups Don't Boot:**

Thanks to Penfolduk

Use Garyopas method first...press the eject button when you get the Open Tray message.

or

- 1.Insert a backup that you know was burned correctly in your 360 and power off.
- 2.Power on,wait for fanfare/ring of light to finish.
- 3.Flick the HDTV switch on the video cable and the soft reset this causes will allow the backup to boot. You can in fact do anything that will soft reset the 360.

If you don't have an HD video cable with the switch, but have a hard drive:

- 1.Remove hard drive.
- 2.Insert a backup that you know was burned correctly in your 360 and power off.
- 3.Power on,wait for fanfare/ring of light to finish.
- 4.Slap the hard drive back on-game now boots

## **Booktype / Bitsetting:**

**From Xtreme's readme:**

**Run build360.bat (Xbox 360 game) or build.bat (xbox 1 game)**

**Ensure your burner will set the booktype of DVD+R DL to DVDRom**

**Burn with CloneCd and choose the image.dvd file**

When the booktype field (bitsetting) is changed to DVD-ROM then DVD players are fooled and will think the user has put in a DVD-ROM disc instead of a DVD+R disc and will read it accordingly. This results in an increased chance that the player is able to read the disc and that's why the ability to change the booktype field (bitsetting) is essential to a lot of users. Certainly owners of a DVD player that requires this field to be set to DVD-ROM, in order to work properly, will prefer a DVD recorder that supports setting the booktype field. - Quote from CDFreaks.com

**REMEMBER** you must have a bitsetting capable DVD+R DL drive. If you do not you may be able to upgrade its firmware (wow a legit firmware flash!) See here for a LOT of drive firmwares: <http://tdb.rpc1.org/>

To set the booktype in DVDInfoPro:

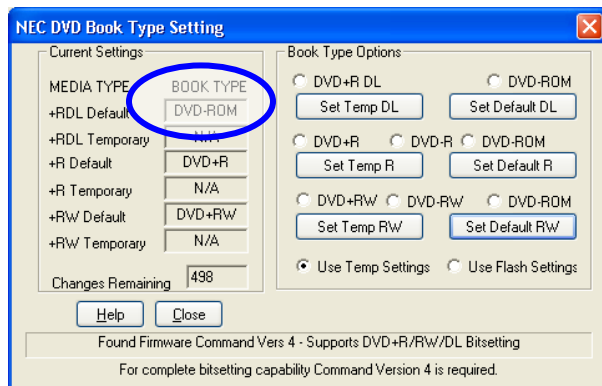
Start DVDInfoPro

Click on the “+RW” icon on the top row

Select DVD-ROM

Press button marked "Change +RDL Mode"

Press Close

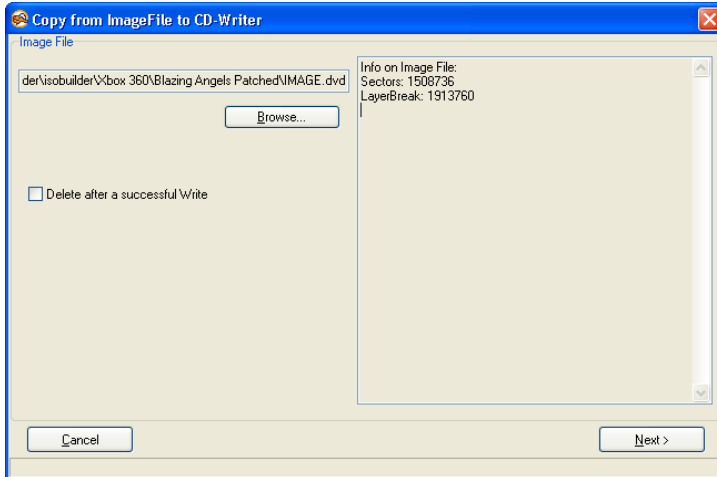


Now whenever a DVD+R DL is burned it will be bitset to read like a DVD-ROM.

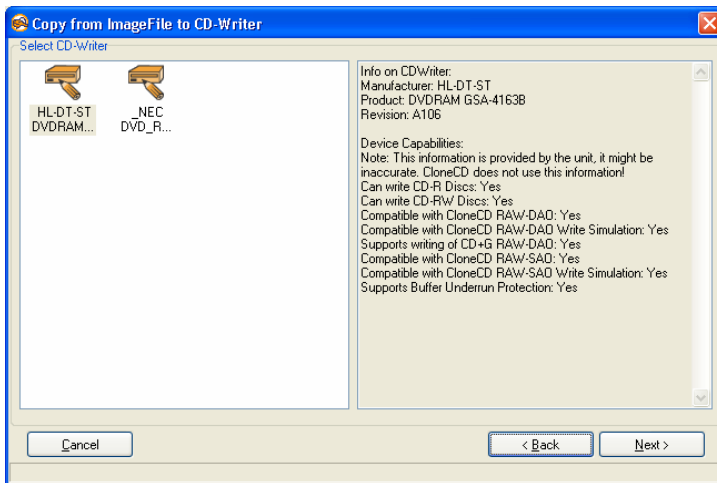
BE AWARE: If you start Nero or similar that can also change the bitsetting, make sure Nero is set to "unmodified" or "current recorder setting", found in Recorder-> Choose Recorder then select the drive and click on "Options"

## Burning Your Backup:

You need the latest version of CloneCD for this. Once you have checked your booktype/bitsetting open CloneCD and select “Write from Image File” (second icon from left). Press “Browse” and select your IMAGE.DVD file.



Select the correct drive you wish to burn with and press “Next”



Set the write speed to 2.4x and press “OK”

Wait until it completes. If writing the lead-out takes a while, be patient and go make a drink. Don't smoke though, its bad for you.

**Thanks to:**

[Kev/SeventhSon](#), Commodore4Eva, xbox-scene.com, xboxhacker.net, Probutus, Geremia, Bluecop, MacDennis, TheSpecialist, Gael360 & JSR, Helldoc, garyOPA and everyone else who did the hard work. The boys did good.