

V17

Hack the 360: The Tutorial

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

Written by: geebee
(geebee@gmail.com for any changes)

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

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
(Samsung Only) Make floppy/usb/cd boot disk with mkthflash on it
(Samsung Only) Boot PC with bootable disk
(Samsung Only) Backup Xbox360 Drive firmware
Boot to Windows
(Hitachi Only) Backup Xbox360 Drive firmware
Backup Xbox360 Drive firmware to 2 other places for safety
Extract unique key from backed-up firmware
Inject key into xtreme's hacked firmware
Flash Xbox360 Drive with xtreme's hacked firmware
Rebuild Xbox360 (unless you want to make some backups now)
Test Xbox360

Game Backup Tasks:

Disassemble Xbox360
Connect Xbox360 Drive to PC
Add Xtrm0800.bin firmware to bootable disk
Boot PC with bootable disk
Flash Xbox360 Drive with Xtrm0800.bin
Boot to Windows
Extract Security Sectors
Make Image with wxRipper or Isobuster
Combine SS and game image with SS Merger 1.4
Burn image
Flash Xbox360 Drive with xtreme's hacked firmware with your key in again
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



- 2) Xtreme/Commodore4Eva/KDX Xbox 360 firmware on a bootable floppy/USB stick/CD: This must be the KDX F360TEAM patched version if you want to use KDX v1.5.
Xtreme_Firmware_PROPER_PATCH_XBOX360-iND is the release name for the patch.
- 3) [KDX1.5-by-F360TEAM.rar](#) to patch the firmware with your key
- 4) A PC with a suitable SATA chipset:

PCI SATA:

VIA VT 8237 **WORKS**

VIA VT 6421L **WORKS** (with edited mtkflash)

Nforce 410 chipset (mcp51) **WORKS** (with edited mtkflash)

[Download Nforce 410 Edited MTKFLASH](#) (Thanks Grim187, elitedev & will5)

Sil3112 Chipset **Does not work**

Sil3114 **Does not work**

Sil3512 (CompUsa) **Does not work**

Maxtor SATA card w Promise chipset (free with hard drives) **Does not work**

Onboard SATA:

MSI k7n2 delta (Promise SATA) - **Does not work**

ASUS with sil3114 Controller (ICH6) - **Compatible for some?**

VIA Chipset - **Compatible**

Intel Chipset (ICH5 / ICH6) **Compatible**

ASUS p5ad2 premium (with ich6) - **Compatible**

Intel Chipset ICH7) - **Compatible** with hex-edited mtkflash?

Promise Sata controller on the ASUS P4C800E-Deluxe - **Compatible**, not HDD

NF4SAT1 nForce 4 SATA Controller - **Compatible** with proper Mtkflash

Abit NF7-S2GNnforce2 SATA (mapped as IDE ports 3+4) - **Compatible**

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 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.

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:

[Anandtech Xbox 360 Stripping Guide](#)

Keep the power connector plugged in your Xbox 360.

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). Power on the Xbox360.

Bootable Floppy Disk:

Make a bootable floppy disk. To do this insert a floppy in your A: drive. Right Click on the A: drive in My Computer. Select "Format" then tick "Create an MS-DOS startup disk". Then copy onto this disk MTKFLASH.EXE, MTKFLASH.TYP, XTREME.BIN and XTRM0800.BIN. That's your disk prepared. If you prefer to use a USB stick or CD just put those same files on it. If you have an Nforce4 chipset motherboard, use the version of MTKFLASH found in MTK-NF4.rar. See the forums for info on editing mtkflash for other chipsets.

Backing Up Your Firmware:

Turn on your Xbox360 and boot your PC with your bootable floppy. At the prompt type:

```
A:> mtkflash r /m orig.bin
```

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

Press Enter

Now you have the choice to select SEC Master or SEC Slave: select Master. The application should start reading the flash. After it's finished it will tell you to reboot the system.

Remove the floppy and 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. Then make another somewhere else. You get the drift.

Getting Your Key:

Now that we have the firmware, we need to extract the Key out of it so we can inject it into the hacked firmware. This process will be done with KDX v1.5 (KDX1.5-by-F360TEAM). Run KDX1.5.exe and press "Open Firmware". Select a copy of your ORIG.BIN file you created earlier. The DVD key will be displayed in the DVD Key box. Highlight and copy it. Now press "Open Firmware" again and select the hacked firmware (XTREME.BIN or possibly XTREME_PROPER.BIN). It must be a patched version of the original hacked firmware. Now press "Save Firmware" and save your modified hacked firmware to wherever you like and call it MODIFIED.BIN. Not a bad idea to back that up to a few places too!

Alternative Method – thanks Sniperkilla – with Hexworkshop (<http://www.shareup.com/downloading-18151.html>)

Open hexworkshop, open original firmware, press ctrl + g, set offset to 4000 and "hex", select edit, select block, enter 200 and select "hex", select edit, then right-click and select copy. Then open the xtreme.bin, and repeat but paste instead of copy... works perfect every time.. no need for a "fixed or proper" xtreme firmware.

Reflashing Your Drive:

The last step is writing the firmware to your DVD-Drive. This will be done with MTKFLASH.EXE again. If you use a floppy disk just put the hacked firmware you just made on the same Floppy. Make sure you put on the one you just modified with your Key!

Reboot the PC following the same procedure you did to backup your original firmware. At the prompt type:

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

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

Press Enter and proceed as before.

If you did everything all right your Xbox360 will now read all correctly made backups.

When you need to make your own backups you will need to flash your Xbox360 Drive again with a different firmware (Xtrm0800.bin). This will be covered in a separate tutorial.

Backing Up Games (Isobuster Method):

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 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:

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.

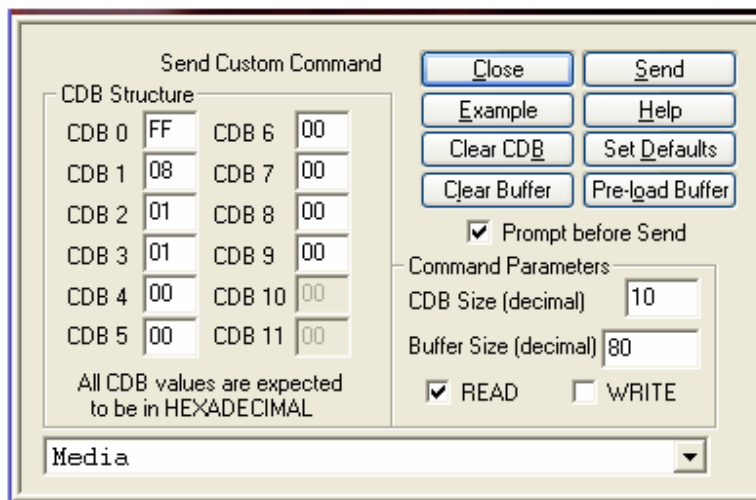
You have 12 boxes here, all filled with 00s. Going from top to bottom (they are numbered in order) you can put in a command.

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.

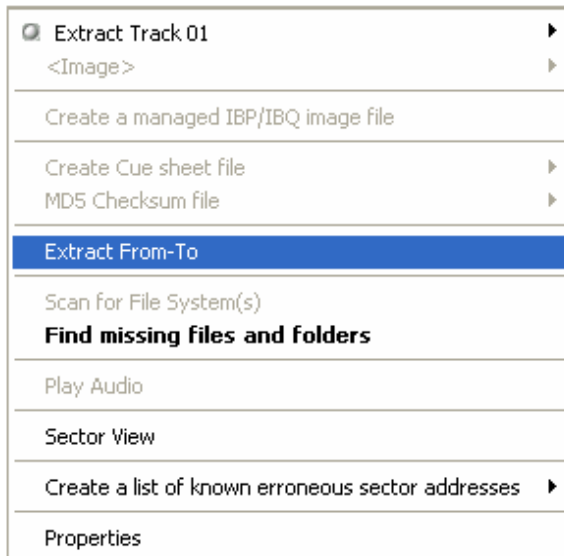
4. Now put in the command displayed on the image below and press send.



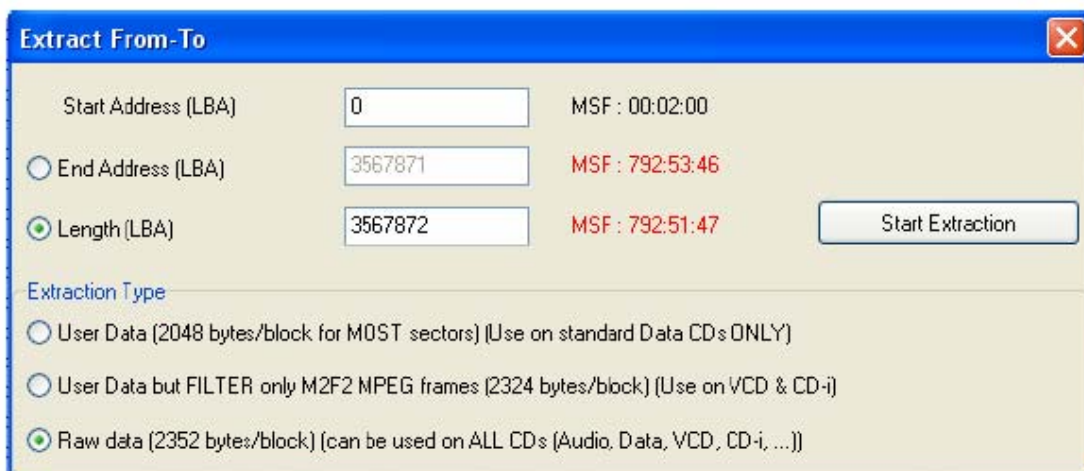
Making the Image (Isobuster Method):

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>

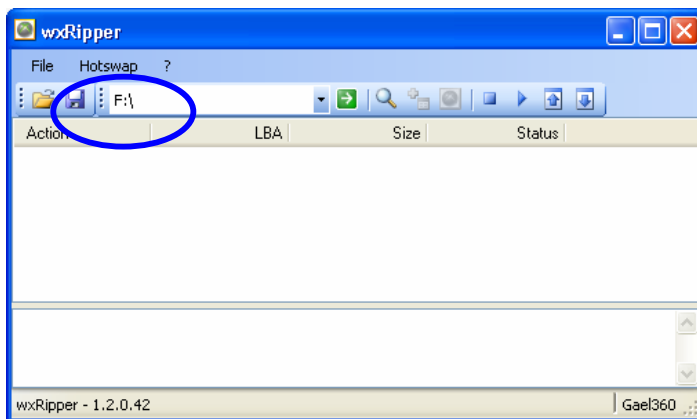
You also need a DVD drive you can use externally that you are not that attached to (it is going to get dismantled a bit). **Or you can use the eject hole on the front of your drive and a paperclip! Try this method first before taking your drive apart.**

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 Sniperkill - 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:

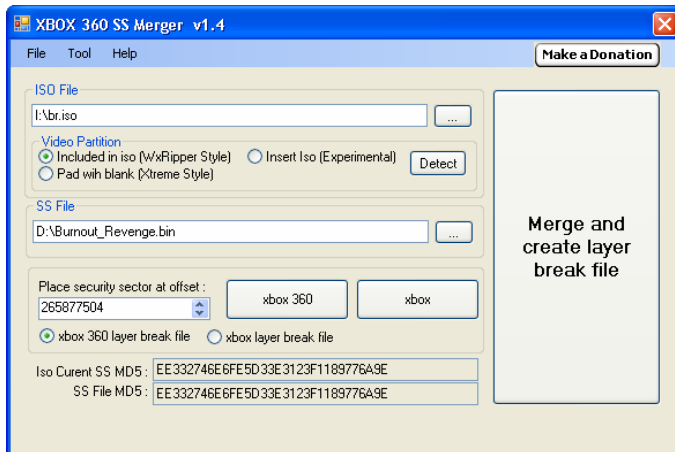
- Since I noticed most people (myself included) occasionally get a CRC error at 91136, especially on games like Tomb Raider and Hitman, I use this layout (replace first 3 lines with these 4):

- 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)

Thanks to PSoff!

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:

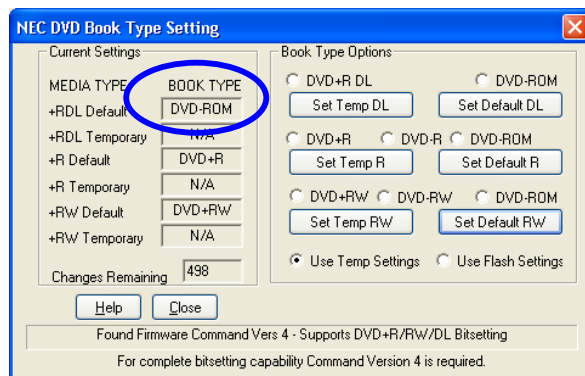
Start DVDInfoPro

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

Select DVD-ROM

Press button marked "Change +RDL Mode"

Press Close

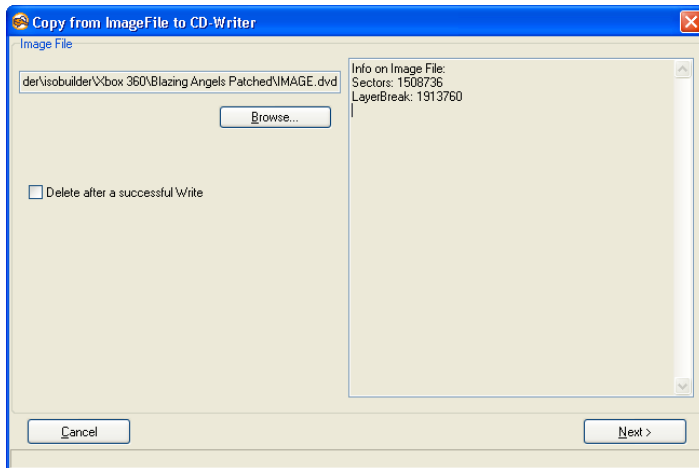


Now whenever a DVD+R DL is burned it will be bitset to read like a DVD-ROM.

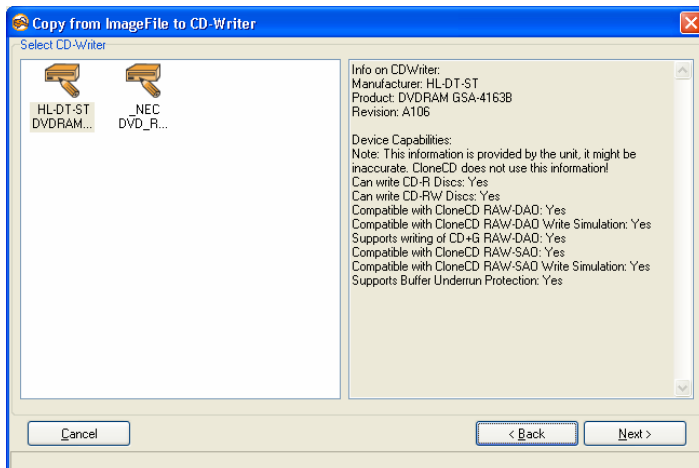
BE AWARE: If you start Nero or similar that can also change the bitsetting, make sure Nero is set to "unmodified" or "current recorder setting", found in Recorder-> Choose Recorder then select the drive and click on "Options"

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.

2nd Reflash To Play:

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!

Backing up the Hitachi/LG Drive:

Well we don't have a hacked firmware yet (except for TheSpecialist) but we can backup the firmware. 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 method or the HotSwap method (thanks stonersmurf):

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

and Memdump:

<http://www.kev.nu/360/dvdshort.html#2> and click on memdump_win.zip!

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.

Crossed Wires Method to get to modeB:

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.



Xbox 360 DVD drive power connector pinout

Hold the 2 wires connected together with your fingers before powering on the 360,

pushed the power button and disconnecting the wires just a fraction of second after the power light came on. Connect your SATA cable then turn on your pc and windows will recognize it.

KEEP THOSE WIRES TOGETHER TOO LONG AND YOU GET AN XBOX-SHAPED BRICK!

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, hd or Samsung 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!

Whichever method you use, carry on from here:

Check what drive letter the Xbox360s Drive is on.

Open a cmd window (start → run. type "CMD" then hit "ok") and change to the directory you created.

Enter the following command:

Replace the "e" with the drive letter of your Xbox360 drive.

```
C:\Memdump> memdump_win e 12200 8 8000 firmware.bin
```

The firmware should then be dumped to the file c:\memdump\firmware.bin

And there you have your Hitachi firmware! Back it up 2 or 3 times! If you load KDX v1.5 as above you can get your Key for later use.

Editing MTKFlash to Work With Your SATA Chipset:

(Thanks to Grim187)

You will need:

HEX Editor (Hex Workshop is Recommended)

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. 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

So From This Example Your Line So Far Should be 11223344 (Need it Explained Better? Click [Here](#))

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 0x00006655-0x00006662

I/O Port 0x00008877-0x00008884

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,

So in this Example Your line Should be 55667788 (Need it Explained Better? Click [Here](#)),

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

Now Open up MTKFlash.exe in Your Hex Editor (Hex Workshop: Right Click on the file and Click "Hex Edit using Hex Workshop"), Your Hex Editor Should have a Goto Function (Hex Workshop: Ctrl+g (If your Hex Editing Program doesn't have this Function Scroll to the Bottom and look for Chipset Names) Open it and put in B370 in Hex, Make Sure You have it "Start at the Beginning" of the file, Once here you should see in the Text part, The Names of ChipSets ICH5,VIA8237,NV NForce3,ect. (Should Look Something Like [This](#)),

If Your Chipset is in Here that's Good You can compare the Actual Hex Value's to the ones "On File" and if There not the Same Change What you Need to, The Info for a Chipset is 1byte (2 00's(In Hex) Before the Name of That Chipset (in TXT),If Your Chipset is Not Here You Can Just Edit one That is (I do Not Recommend Creating a New one), For Example Say i Have a VIA8237 Chipset These are The Values That i Would Edit (Don't Edit the 00 in RED)

```

0000 00FF 00FF 00F0 0170 0101 4944 4500 0000 0000 | .....p..IDE.....
0000 8680 D124 F001 7001 0049 4348 3500 0000 0000 | .....$.p..ICH5.....
0086 806F 26F0 0170 0100 4943 4836 5000 0000 0000 | ...o&..p..ICH6P.....
8680 5226 F001 7001 0049 4348 3600 0000 0000 0086 | ..R&..p..ICH6.....
8053 26F0 0170 0100 4943 4836 4D00 0000 0000 0611 | .S&..p..ICH6M.....
4931 F001 7001 0056 4941 3832 3337 0000 0095 1012 | I1..p..VIA8237.....
31F0 0170 0100 5369 3331 3132 0000 0000 9510 1431 | 1..p..Si3112.....1
F001 7001 0053 6933 3131 3400 0000 0039 1080 01F0 | ..p..Si3114....9....
0170 0100 5369 5339 3634 0000 0000 3910 8101 F001 | .p..SiS964....9.....
7001 0053 6953 3138 3000 0000 0039 1082 01F0 0170 | p..SiS180....9.....p
0100 5369 5339 3635 0000 0000 DE10 E300 F001 7001 | ..SiS965.....p.
004E 5620 6E46 6F72 6365 33FF 00FF 00F0 0170 0100 | .NV nForce3.....p..
556E 6B6E 6F77 6E00 0000 0050 7269 204D 6173 7465 | Unknown....Pri Maste

```

[To Conclude the Example's in Step 2 \(Don't Edit The Selected 00's\)](#)

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"

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, Scener, Commodore4Eva, uberfry, Foros360.com, Xbox-scene.com, xboxhacker.net, Probutus, Bluecop, MacDennis, TheSpecialist, Gael360, Helldoc and everyone else who did the hard work. The boys did good.