



Hacking the Xbox 360

The Tutorial



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

Written by: Mksoftware and geebee

BEFORE YOU START, READ

[Start Your Reading Here](http://forums.xbox-scene.com/index.php?s=cdbaa5713c3134aa66aa2493c814c259&showtopic=513412)

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

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 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:

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
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



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:

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.







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!

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 11 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.

CDB Structure			
CDB 0	FF	CDB 6	00
CDB 1	08	CDB 7	00
CDB 2	01	CDB 8	00
CDB 3	01	CDB 9	00
CDB 4	00	CDB 10	00
CDB 5	00	CDB 11	00

All CDB values are expected to be in HEXADECIMAL

Buttons: Close, Send, Example, Help, Clear CDB, Set Defaults, Clear Buffer, Pre-load Buffer

☒ Prompt before Send

Command Parameters:

CDB Size (decimal): 10

Buffer Size (decimal): 80

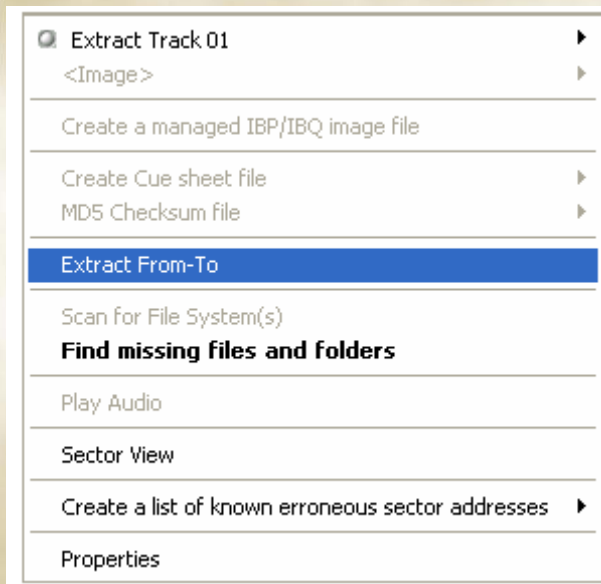
☒ READ ☐ WRITE

Media

Making the Image (Isobuster Method):

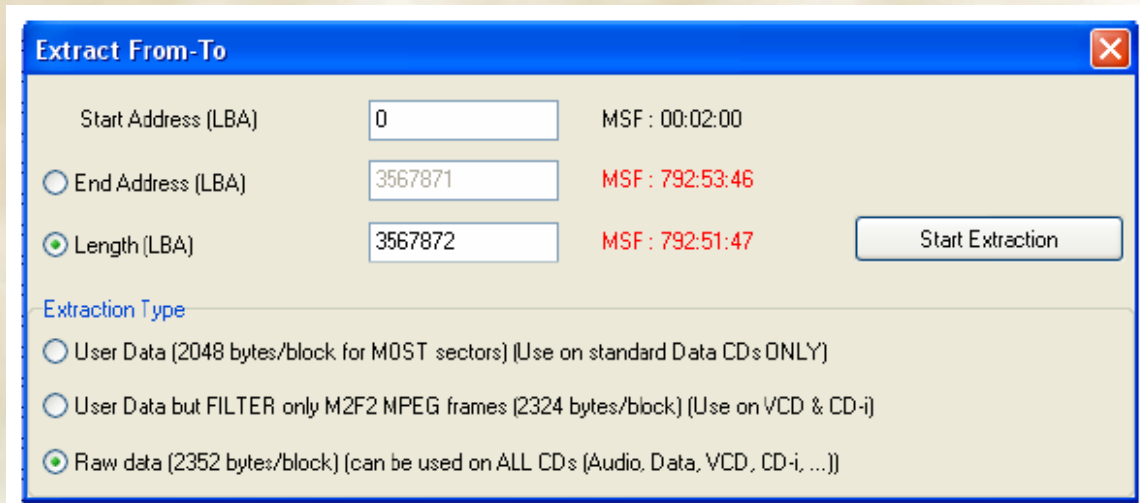
The next tool we will need is Isobuster, included in the Xtreme bundle.

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



☒ Extract Track 01 ▶
 <Image> ▶
 Create a managed IBP/IBQ image file
 Create Cue sheet file ▶
 MD5 Checksum file ▶
Extract From-To
 Scan for File System(s)
Find missing files and folders
 Play Audio
 Sector View
 Create a list of known erroneous sector addresses ▶
 Properties

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



Extract From-To [X]
 Start Address (LBA) MSF : 00:02:00
 End Address (LBA) MSF : 792:53:46
 Length (LBA) ☒ MSF : 792:51:47
 Extraction Type
☐ User Data (2048 bytes/block for MOST sectors) (Use on standard Data CDs ONLY)
☐ User Data but FILTER only M2F2 MPEG frames (2324 bytes/block) (Use on VCD & CD-i)
☒ Raw data (2352 bytes/block) (can be used on ALL CDs (Audio, Data, VCD, CD-i, ...))

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_1.3 (thanks to HellDoc) and wxRipper (thanks for the great too Gael360).

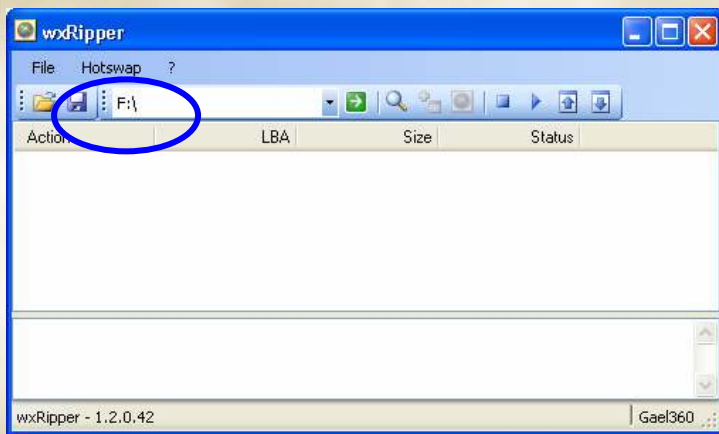
http://dwl.xbox-scene.com/xbox360pc/isotools/XBOX360_SS_Merger_1.3.rar
<http://gael360.free.fr/files/wxRipper-1.2.rar>

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).

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. 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:



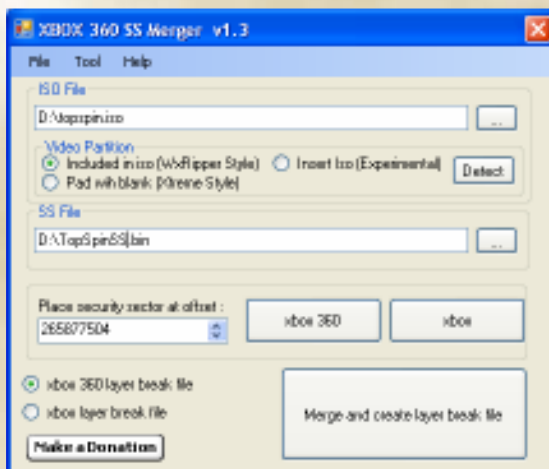
Stick in your large DVD. Let it get recognised then press The “Stop” button on wxRipper. If you use a USB DVD drive you may need to wait 2 minutes for it to spin down by itself as the “Stop” button does not work on USB. Remove the disk without using eject and replace it with your Xbox360 game disk.

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.

Combining the Image & SS Files (wxRipper Method):

Now you can start up HellDocs excellent XBOX360 SS Merger 1.3.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:

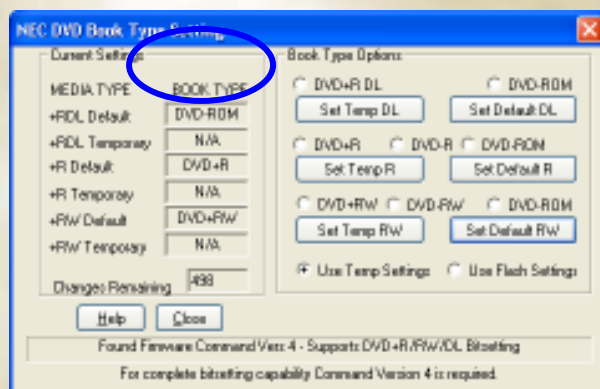
Run build360.bat (**Xbox 360 game**) or build.bat (xbox 1 game)
Ensure your burner will set the booktype of DVD+R DL to DVD-Rom
Burn with CloneCd and choose the image.dvd file

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:

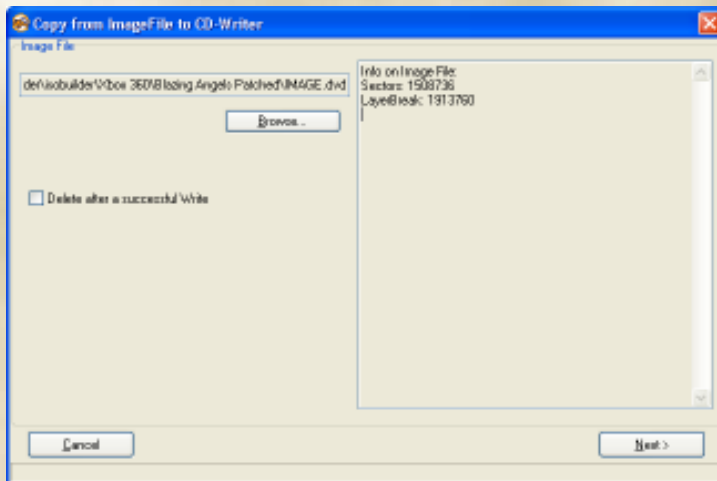
Start DVDInfoPro
Click on the "+RW" icon on the top row
Select DVD-ROM
Press button marked "Change +RDL Mode"
Press Close



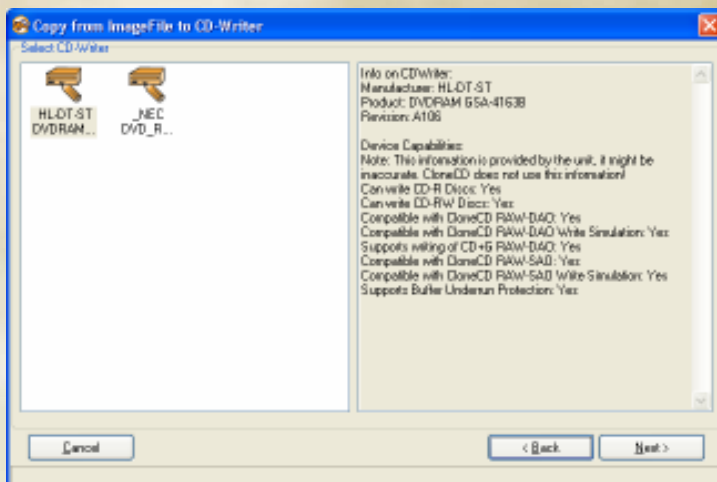
Now whenever a DVD+R DL is burned it will be bitset to read like a DVD-ROM.
BE AWARE: If you start Nero or similar that can also change the bitsetting, make sure Nero is set to "unmodified" or "current recorder setting", found in Recorder-> Choose Recorder then select the drive and click on "Options"

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!

Thanks to:

Scener, Commodore4Eva, 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.

