

360MODS

The best hacking tutorial out there!

Hacking The Xbox 360

FOR
DUMMIES

Shutup and
Read This,
Noobs

*A Reference
for the
Rest of Us!*

By Textbook





Textbook's Xbox 360 Firmware Tutorial

www.360mods.net

Table of Contents

[Introduction](#)

[Warnings](#)

[Samsung or Hitachi](#)

Samsung

[Opening The Xbox 360](#)

[MS25 or MS28](#)

[MS25](#)

[Sata/MTKFlash Compatibility](#)

[Downloading The Firmware](#)

[Xtreme Boot Maker \(USB\)](#)

[Updating x360sam, Adding Keycheck](#)

[Flashing Your Drive \(USB\)](#)

[Xtreme Boot Maker \(NTFS4DOS CD\)](#)

[Updating x360sam, Adding Keycheck](#)

[Flashing Your Drive \(NTFS4DOS CD\)](#)

[Xtreme Boot Maker \(Floppy\)](#)

[Updating x360sam, Adding Keycheck](#)

[Flashing Your Drive \(Floppy\)](#)

[MS28](#)

[VCC Switch Method \(requires soldering\)](#)

[Setting Up The Switch](#)

[Flashing](#)

[Bad Flash Method \(solderless\)](#)

[Setup](#)

[Flashing](#)

[Upgrading From 4.x / 5.x \(disabling FirmGuard\)](#)

Hitachi

[Opening The Xbox 360](#)

[ModeB](#)

[Slax CD](#)

[2-Wire Trick](#)

[Connectivity Kits](#)



[Hotswap](#)

[ModeB Indicators](#)

[Detecting The Drive in Windows](#)

[Installing "CMD Here" Powertoy](#)

[Downloading The Firmware](#)

[Restoring The Drive \(if previously flashed\)](#)

[Flashing The Drive](#)

[v0078FK Instructions](#)

Making Backups of Your Xbox 360 Games

[Using the Samsung drive](#)

[Using a Kreon drive](#)

[WxRipper Method](#)

[Bitsetting](#)

[Burning Using IMGBurn](#)

[Burning Using CloneCD](#)



Introduction

The Xbox 360 DVD-ROM drive firmware hack is currently the only modification or hack available for the Xbox 360. The firmware hack allows you to play properly created backups of Xbox 360 games. The firmware hack does **NOT** allow homebrew programs to run and does **NOT** bypass region protection. If a video game is locked to a particular region, then it will only play on an Xbox 360 of that same region. Before jumping into this modification, it is a good idea to learn how this hack works.

In the most basic form, an Xbox 360's game protection comes from two security measures. First of which is encryption. Nearly all files on an Xbox 360 game disc as well as the Xbox 360 hard drive are signed with Microsoft's private key. If anything, even just a single bit, is changed, the signature is broken and the Xbox 360 refuses to run the file. The second security measure is media locking. The game is restricted to run only from a certain type of media. For example, all Xbox 360 games are restricted to run only from "Xbox 360" media. Game demos downloaded from Xbox Live are restricted to run only from "Xbox 360 Hard Drive." Xbox Live Arcade games aren't restricted at all; they can run from any media. Before the firmware hacks, if you were to copy an Xbox 360 game and try running it from "DVD+R DL", the Xbox 360 would obviously see that it wasn't "Xbox 360" media and refuse to run it because of the media restriction.

This media restriction is what the firmware hack bypasses. The firmware fakes out the Xbox 360 into thinking that any media is "Xbox 360" media. You copy your game to DVD+R DL, insert it into a firmware-hacked drive, and instead of returning "DVD+R DL" to the Xbox 360, the drive says it is an "Xbox 360" disc and it then plays the game. As you can see, the firmware hack does not bypass any signature protection whatsoever. Some Xbox 360 games use region protection to restrict the playing of a game in a certain region. The firmware hack will not allow you to play games out of a region if they are region-locked. If the original will play in your Xbox 360, the same backup will. If the original won't, neither will the backup of it.



Warnings

The Xbox 360 firmware hack may be illegal under the Digital Millennium Copyright Act (United States), the European Union Copyright Directive (Europe), or other copyright laws in your country. Downloading, installing, and using this firmware could potentially be illegal. You are doing so at your own risk.

Copying or downloading games that you have not legally purchased or own is illegal in all countries. This violates not only laws in your own country, but international copyright laws as well. The purpose of the firmware hack is for making backup copies of games that you legally own. Software piracy is illegal, carries a huge penalty if convicted, is ethically wrong, and hurts the game companies. Support the game developers by purchasing the games you play. You wouldn't work for free, would you?

Using this firmware hack and running your backups on Xbox Live violates the Xbox Live Terms of Service agreement that you agreed to when you signed up. Microsoft withholds the right to terminate the Xbox Live service from you for any reason, at any point, with no warning, and no refunds. With hacks on the original Xbox, the Xbox was banned permanently from Xbox Live. The same risk applies to the Xbox 360. Simply put, if you are worried about Xbox Live, do not install this firmware modification - or purchase two Xbox 360 systems. With that said, at this time nobody has been banned for using the firmware hack, but you use it at your own risk and should expect to be banned one day.

Upgrading your Xbox 360 firmware requires you to open your Xbox 360, open your PC, and connect the Xbox 360 DVD-ROM drive to your computer via a SATA cable. This will void your Xbox 360 warranty. There is no way to flash the drive firmware without opening the Xbox 360. Also, this firmware upgrade is not recommended for novices. A technical level of computer knowledge is required, with an understanding of how to configure your PC BIOS, use MS-DOS, or the MS-DOS command prompt, and the use of CD/DVD software. If, after reading through this tutorial, you still do not understand it completely, get an experienced installer to do the job for you.

Samsung or Hitachi

Use the following image to see what brand DVD drive you have, then follow this tutorial accordingly. Note that there are different versions of these drives. You can only tell the brand of the drive by looking at the tray. To determine the version of that drive, you have to open the Xbox 360 and check the sticker on the drive.



Click your drive below:

[Samsung](#) or [Hitachi](#)



Toshiba-Samsung TS-H943A Tutorial

[Video Tutorial Here](#)

Opening The Xbox 360

The outer Xbox 360 “shell” is entirely screwless. Plastic friction tabs hold the case together. There are many different tutorials for opening the Xbox 360, with different methods. Here are some links to “opening the Xbox 360” tutorials. I felt it unnecessary to cover opening the Xbox 360 in this tutorial when there are already so many other guides out there. Nevertheless, here are some quick notes:

- The Anandtech guide says you need to use a Torx 12 screwdriver. There is no such thing. You need a Torx 10 screwdriver.
- Removing the grey side grill on the hard drive side is a little tricky. The first friction tab is actually inaccessible from the top holes in the case, so you need to stick your screwdriver in the hole by where the hard drive button is and unclip it.
- In order to push in the back clips, you can do a few things. You can use a thin metal object such as a precision flathead screwdriver / bobby pin / paperclip OR you can make an opening “key” out of a CD spindle case or old credit card. Anotehr alternative is purchasing an “unlock kit.”
- If all you want to do is just flash the firmware, you only need to remove the six long Torx screws on the bottom of the inside metal casing.

[Anandtech Guide](#)

[InformIT Guide](#)

[Xbox-Accessories Disassembly](#)

[Hydra's Guide to Making an Unlock Key](#)

[Textbook's Video](#)

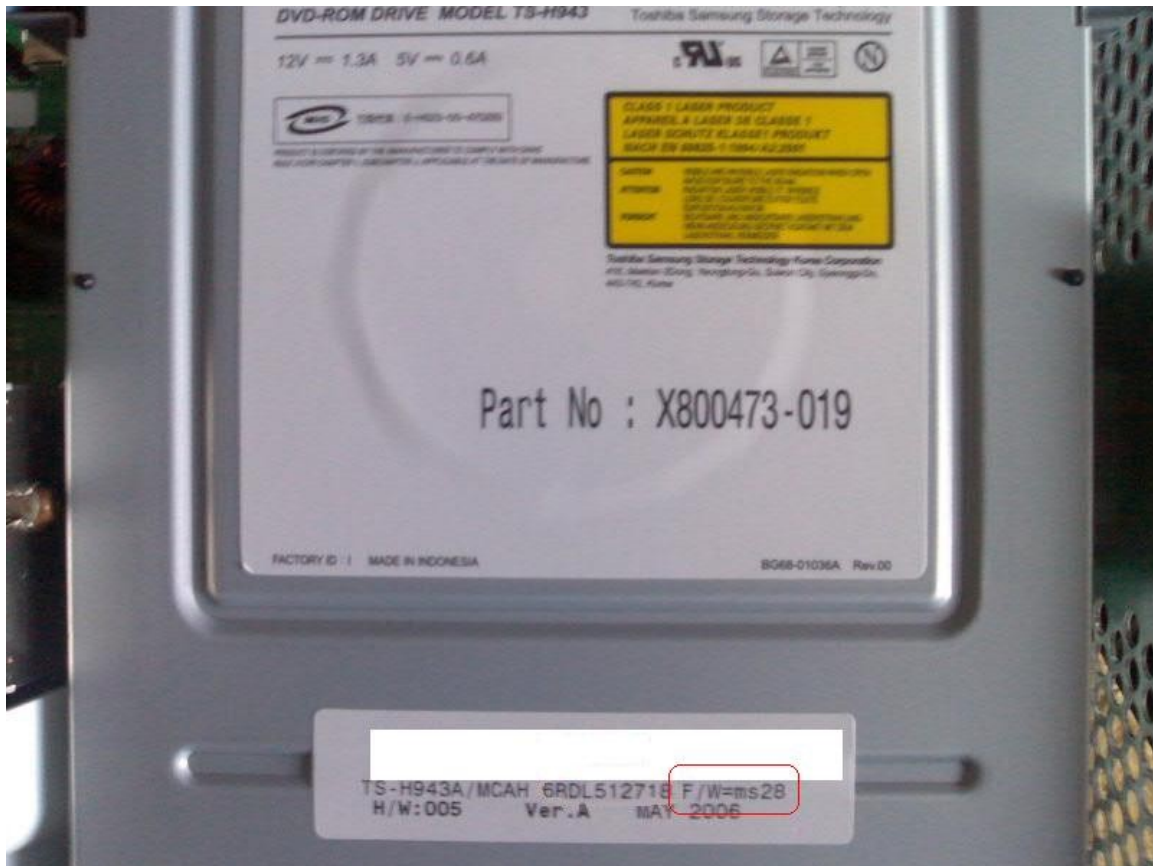
[Syrax2Beta's Video](#)

[Google Video](#)

[shishnit's Video](#)

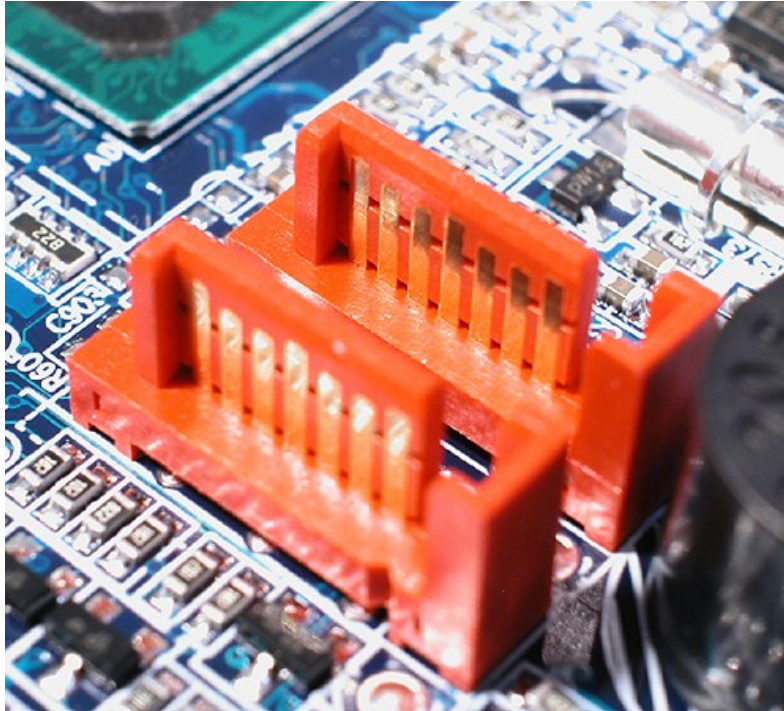
MS25 or MS28

There are currently two versions of the Samsung drive. The hardware is identical, but there are different firmware revisions. The MS25 is the easier drive to flash. The MS28 can be flashed, but different “tricks” need to be used in order for MTKFlash to read or write to the drive. Once you have your Xbox 360 opened, check the sticker to see if your drive is MS25 or MS28, and follow the instructions below. If you have an MS25 drive, just continue reading. If you have an MS28 drive, click [here](#).



SATA/MTKFlash Compatibility

MTKFlash is the program used to flash the Samsung drives. It is an older program, and because of this, it does not work with all SATA chipsets. You must first figure out if you even have SATA ports on your motherboard. SATA connections are L-shaped and have 7 contacts.



If you do not have SATA, you must purchase a PCI SATA card. For Samsung drives, the most compatible card is one with the [VIA 6421](#) chipset.

If you do have onboard SATA already on your PC motherboard, you will have to figure out what chipset it is and compare it to this compatibility chart. You can determine your SATA chipset by reading the manual that came with your motherboard, or looking up your motherboard specs on the manufacturer's website or doing research of your own ([Google](#)).

You can also determine your SATA chipset by doing the following:

Start > Run > msinfo32 > Components > Storage > SCSI.



You will want to see if there is a SATA controller listed, usually containing Serial ATA or RAID in the name. If you see just SCSI/RAID Host Controller, this is not the chipset, it is the default Windows driver. If you see VAXSCSI in the list, this is most likely an image drive program on your PC like Daemon Tools or Alcohol 120%.

If you do not see your SATA chipset listed in SCSI, go to Storage > IDE and see if it is in there, some are. Remember, you're looking for Serial ATA, RAID, or in some cases, Ultra ATA. **NOT** IDE.

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 if you flash the chip to non-RAID BIOS?
ALL*	VIA VT 8251	Yes	Yes	Tested by Matt Tracy
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	82801GB / GR / GH ICH7 MTKFlash 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. MTKFlash1 MTKFlash2
ALL*	VIA VT 6410	Yes	Yes	Try manual hex-edit first, or try one of these. MTKFlash1 MTKFlash2
VIA Epia SP Mini-iTX	VIA EPIA SP	Yes	Yes	MTKFlash

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	Maybe	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.
VIA VT 6421L	Yes	Yes	This is the card to get. Cheap, widely available, with a pre-hex-edited MTKFlash for download. MTKFlash1 MTKFlash2
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.
Newlink NL-PCISATAIEXT	No ?	Yes	Thanks to Thraxed, best card to buy in UK.

Note: Even if your chipset is listed as not requiring that MTKFlash be hexedited, it is still probably a good idea to do so. Use Xtreme Boot Maker to make a custom hexedited MTKFlash specifically for your SATA chipset.



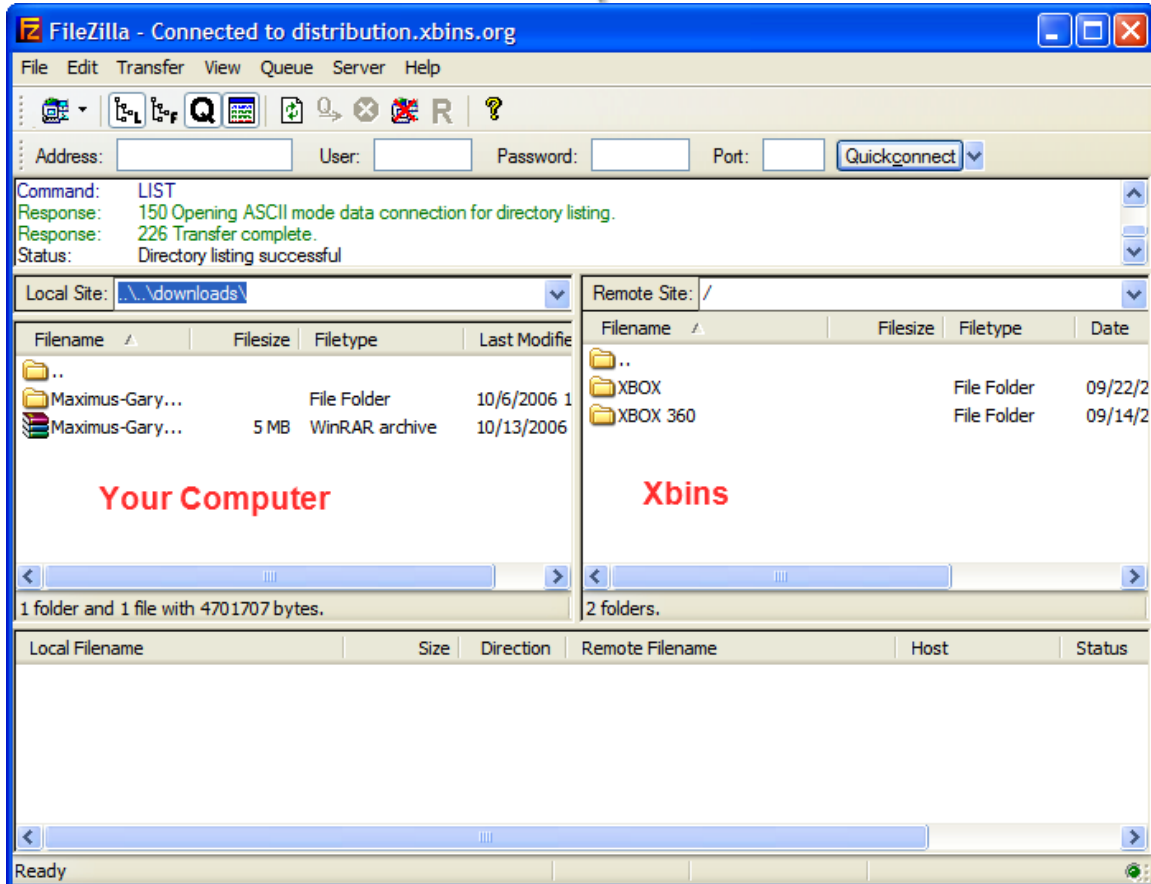
Downloading The Firmware

The hacked firmware may be illegal under the DMCA, EUCD, or other local, national, and international copyright laws. The hacked firmware contains portions of Microsoft's copyrighted firmware and therefore cannot be linked to or downloaded publicly. Do not request the firmware on any forums because it is against most forum rules and you will most likely be banned. The best method to obtain the firmware is by using Xbins. Xbins is an IRC channel and FTP server that hosts Xbox and Xbox 360 mod files, homebrew programs, and development software.

If you have never used Xbins before, the easiest method is to use Ground Zero's automated Xbins downloader.

[Download](#)

Download the self-extracting archive and run the xbins.exe file. It will ask you where you want to save the files, choose your desktop. Now, go into the "Xbins" folder on your desktop and run the .bat file. The program will automatically connect to the IRC channel, message the bot, and connect to the FTP server. When filezilla opens up you should see the local Xbins folder on your left side, and a few folders on your right side (this is the FTP server).



The hacked firmware can be found in:

/XBOX 360/firmware/hacked firmware/Toshiba-Samsung TS-H943/

Simply drag the "Xtreme52.rar" file over to the left side of FileZilla and wait for it to finish downloading. You can use [WinRAR](#) or [7-zip](#) to extract the RAR archive.

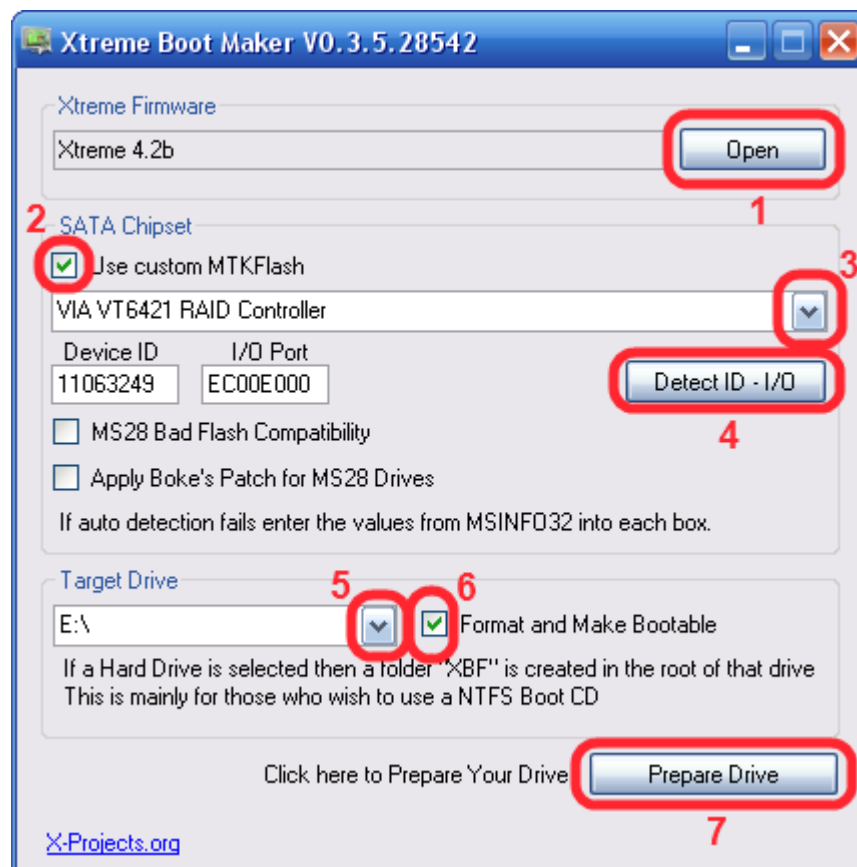
Xtreme Boot Maker (USB)

The following process will set up a bootable USB flash drive with everything necessary to read your original firmware and write the hacked firmware onto the drive. We will use Xtreme Boot Maker to hex-edit MTKFlash, format the USB drive, and copy the files onto it.

First, you need to make sure [Microsoft .NET Framework v2](#) is installed. It is needed for Xtreme Boot Maker to run. If you do not have this installed, you will be prompted to download and install it.

Second, you need to make sure the drivers for your SATA chipset are installed. Use either the CD that came with your computer/SATA card, or use the manufacturer's web site to install the drivers.

Once you have that taken care of, you can download and install [Xtreme Boot Maker](#).





1. Hit the Open button to browse your computer and select your firmware. You should select xtrem52a.bin, xtrem52b.bin, xtrem52c.bin, or xtrem52d.bin from the archive you downloaded off Xbins.

With Xtreme 5.2A, backups are always read at 12x speed, the same speed as originals. The read speeds of original discs are unaffected. With the faster reading speed, the drive is significantly louder, and may have problems reading cheaper media, but you have the benefit of slightly faster loading times.

With Xtreme 5.2B, backups are always read at 4x speed. The read speeds of original discs are unaffected. With the slower reading speed, the drive is quieter, may read cheaper media better, but has slightly longer loading times.

With Xtreme 5.2C, the default backup read speed is 12x. When an original disc is placed in the drive, all subsequent backups will be read at 4x. Read speed of original game discs will remain unaffected. Restart the system if you wish to read backups at 12x.

With Xtreme 5.2D, the default backup read speed is 4x. When an original disc is placed in the drive, all subsequent backups will be read at 12x. Read speed of original game discs will remain unaffected. Restart the system if you wish to read backups at 4x.

2. Select the checkbox "Use custom MTKFlash."
3. Select your SATA chipset from the drop-down list.
4. Click "Detect ID – I/O." It should input some characters in the Device ID and I/O Port boxes when it finishes.
5. Select your Target Drive as the USB Flash Drive
6. Check the box labeled "Format and Make Bootable"
7. Select "Prepare Drive." Wait until the program finishes.



Updating X360SAM and Keycheck

The current version of Xtreme Boot Maker includes version 0.4 of X360SAM. The latest version is v0.6, and includes a feature that copies the drive version string. This is necessary for avoiding the error code 66. The newest version of X360SAM will make the hacked firmware report as whatever drive version your original firmware was.

In addition to this update, Caster420 wrote a dos-based program named Keycheck that will check your drive key of the original firmware, as well as the hacked firmware that x360sam creates, and verify that they match. This is important because some people were having “partial” reads of the firmware and ended up bricking their drives.

You can download both the updated x360sam and keycheck in one zip archive [here](#).

Simply copy the three files from the zip archive to your USB flash drive. If it asks you if you want to overwrite x360sam.exe and samread.bat, select Yes.

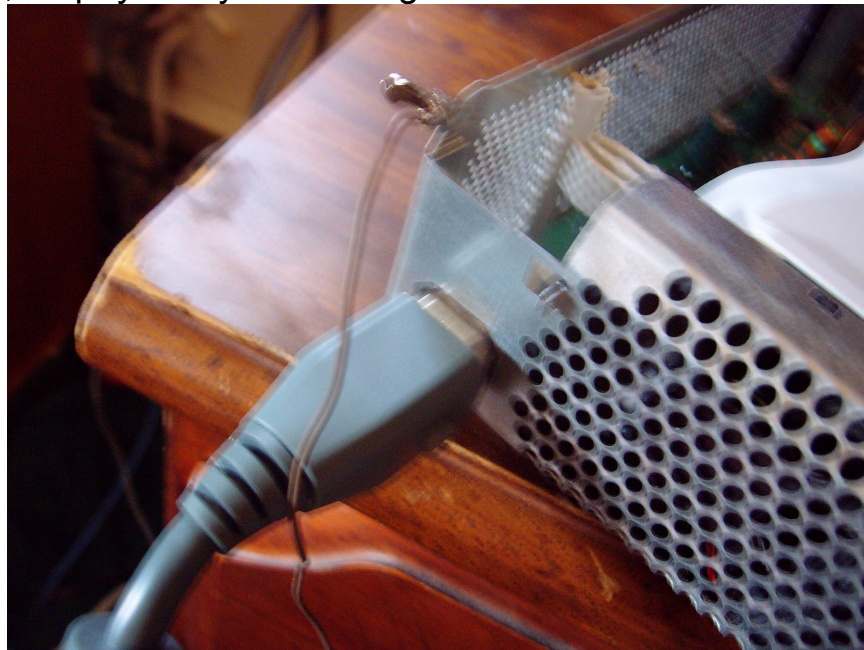
Flashing Your Drive (USB)

Reading The Original Firmware

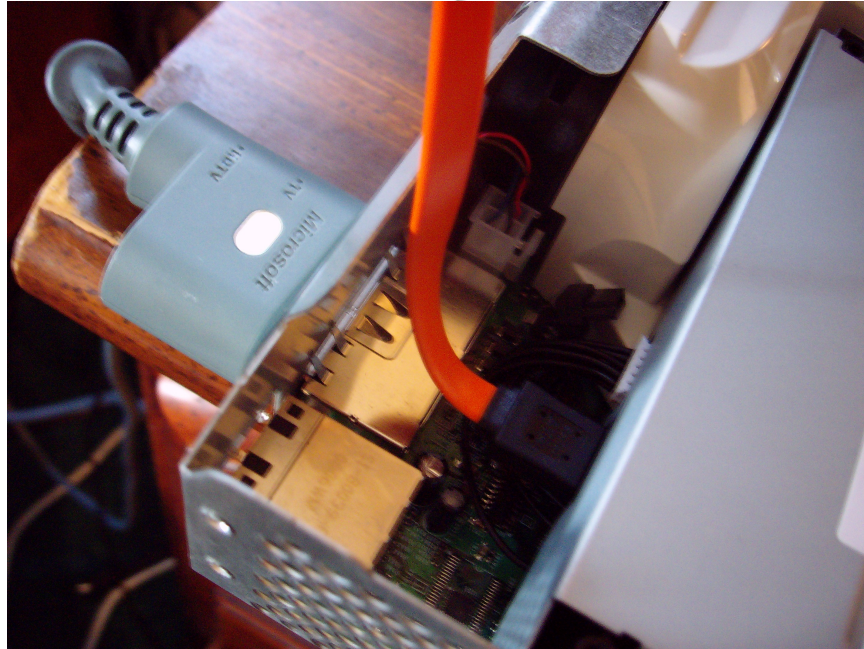
Power off both your PC and Xbox 360. Make sure the Xbox 360 power cable and video cable are both plugged in. You do not need to hook up the video to a TV, but the cable does have to be plugged into the Xbox 360. Unhook the small black SATA cable connecting the Xbox 360 DVD drive to the motherboard. Have a long SATA cable connected to your PC, but leave it unplugged from the Xbox 360 drive.

(The picture shows the SATA cable connected, leave it unplugged from the drive)

Disconnect all other drives in your PC. You should disconnect both hard drives and DVD drives so they do not accidentally get flashed with the hacked firmware. Disabling these devices in your BIOS may not work, so physically unhooking them is the best solution.



360 MODS



Turn on your PC and Xbox 360 at the same time, and boot your PC from the USB flash drive, into DOS. When you reach the DOS command prompt, plug the SATA cable into the Xbox 360 DVD drive.

Type in the following command, using your Xbox 360 serial number found on the back of the Xbox 360 case.

(We'll use the serial number 1234567 12345 as an example)



SAMREAD 1234567 12345 [press enter]

If you get an error like “Directory already exists” or “MKDIR failed...” don’t worry. X360SAM is trying to create a new folder but you already have one, so there’s no need to.

MTKFlash should run and your SATA controller should be listed. If you see an item in the list named “XTREME”, choose that. This is not your USB flash drive, as some people were guessing. It is actually your SATA controller. Xtreme Boot Maker will name it this when it creates the MTKFlash. Select your SATA controller and it should make a backup of your original firmware. Then you will see X360 pop up really fast. After it is done creating the hacked firmware, it will give you the next instructions:

“Now unplug the SATA cable and power-cycle the PC and DVD drive before running SAMHACK 1234567 12345”

So do just that. Unplug the SATA cable from the 360 DVD drive and power off the Xbox 360, then the PC.



Flashing The Hacked Firmware

Turn on your PC and Xbox 360 at the same time, and boot your PC from the USB flash drive, into DOS. When you reach the DOS command prompt, plug the SATA cable into the Xbox 360 DVD drive.

Type in the following command, using your Xbox 360 serial number that you used with the SAMREAD command.

```
SAMHACK 1234567 12345 [press enter]
```

MTKFlash should run and your SATA controller should be listed. Select your SATA controller and it will flash the drive with your hacked firmware. It should flash 4 banks. The 4th bank may say something like Datasum, this is normal. When it is done flashing, unplug the SATA cable from the 360 DVD drive, power off the Xbox 360, and power off your PC. Reconnect the 360 DVD drive to the 360 motherboard and test it.

Backup Your Original Firmware!

Boot into Windows. Plug in your USB drive and find your orig.bin in the BACKUPS folder. This is your Xbox 360 drive 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.

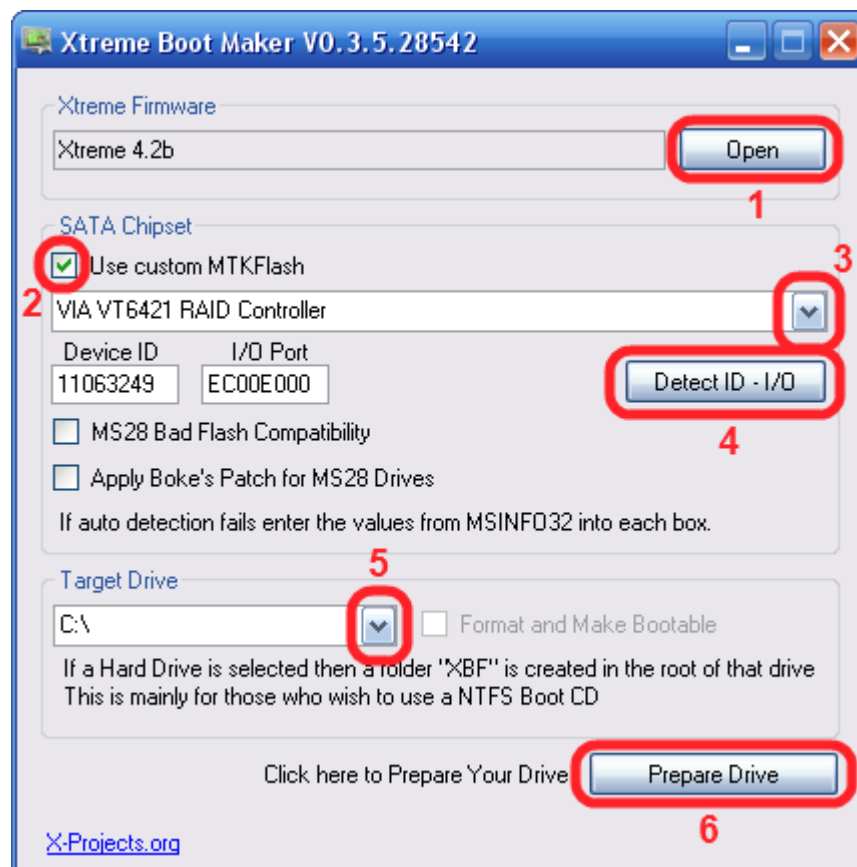
Xtreme Boot Maker (NTFS4DOS CD)

The following process will set up an NTFS-mountable boot CD so that you can use your computer's hard drive to flash your Xbox 360 firmware. We will use Xtreme Boot Maker to hex-edit MTKFlash and copy the files to your hard drive.

First, you need to make sure Microsoft .NET Framework v2 is installed. It is needed for Xtreme Boot Maker to run. If you do not have this installed, you will be prompted to download and install it.

Second, you need to make sure the drivers for your SATA chipset are installed. Use either the CD that came with your computer/SATA card, or use the manufacturer's web site to install the drivers.

Once you have that taken care of, you can download and install [Xtreme Boot Maker](#).





1. Hit the Open button to browse your computer and select your firmware. You should select xtrem52a.bin, xtrem52b.bin, xtrem52c.bin, or xtrem52d.bin from the archive you downloaded off Xbins.

With Xtreme 5.2A, backups are always read at 12x speed, the same speed as originals. The read speeds of original discs are unaffected. With the faster reading speed, the drive is significantly louder, and may have problems reading cheaper media, but you have the benefit of slightly faster loading times.

With Xtreme 5.2B, backups are always read at 4x speed. The read speeds of original discs are unaffected. With the slower reading speed, the drive is quieter, may read cheaper media better, but has slightly longer loading times.

With Xtreme 5.2C, the default backup read speed is 12x. When an original disc is placed in the drive, all subsequent backups will be read at 4x. Read speed of original game discs will remain unaffected. Restart the system if you wish to read backups at 12x.

With Xtreme 5.2D, the default backup read speed is 4x. When an original disc is placed in the drive, all subsequent backups will be read at 12x. Read speed of original game discs will remain unaffected. Restart the system if you wish to read backups at 4x.

2. Select the checkbox "Use custom MTKFlash."
3. Select your SATA chipset from the drop-down list.
4. Click "Detect ID – I/O." It should input some characters in the Device ID and I/O Port boxes when it finishes.
5. Select your Target Drive as the hard drive
6. Select "Prepare Drive." Wait until the program finishes.

[Download the NTFS4DOS ISO](#) and burn it to a blank CD-R using any recording software capable of burning ISO files. ([IMGBurn](#) is a nice, free program)



Updating X360SAM and Keycheck

The current version of Xtreme Boot Maker includes version 0.4 of X360SAM. The latest version is v0.6, and includes a feature that copies the drive version string. This is necessary for avoiding the error code 66. The newest version of X360SAM will make the hacked firmware report as whatever drive version your original firmware was.

In addition to this update, Caster420 wrote a dos-based program named Keycheck that will check your drive key of the original firmware, as well as the hacked firmware that x360sam creates, and verify that they match. This is important because some people were having “partial” reads of the firmware and ended up bricking their drives.

You can download both the updated x360sam and keycheck in one zip archive [here](#).

Simply copy the three files from the zip archive to the XBF directory. If it asks you if you want to overwrite x360sam.exe and samread.bat , select Yes.

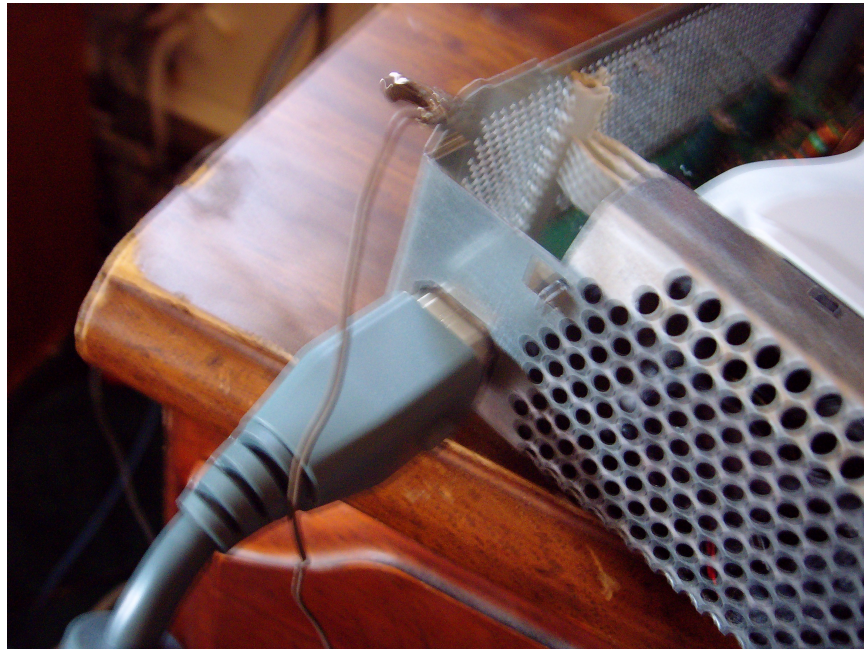
Flashing Your Drive (NTFS4DOS)

Reading The Original Firmware

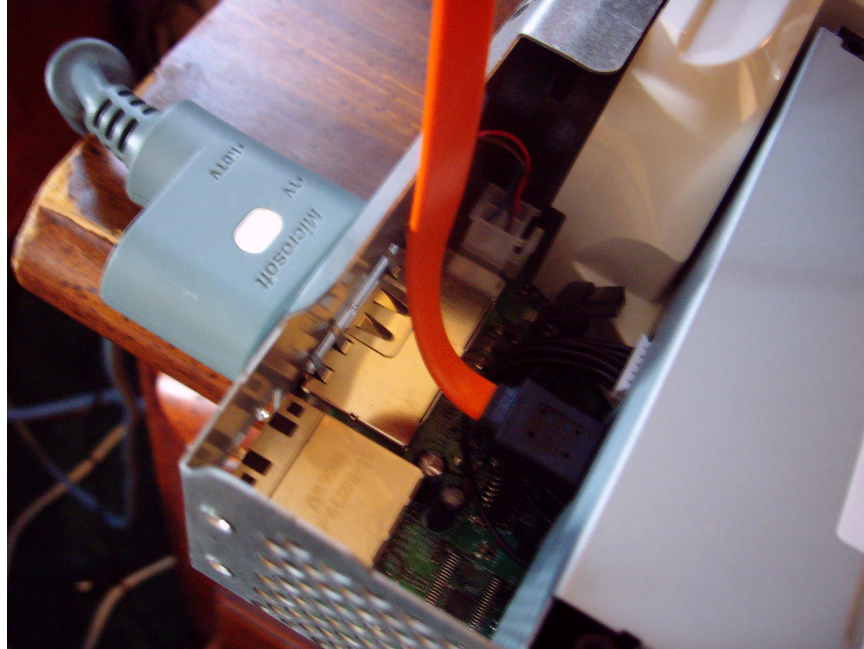
Power off both your PC and Xbox 360. Make sure the Xbox 360 power cable and video cable are both plugged in. You do not need to hook up the video to a TV, but the cable does have to be plugged into the Xbox 360. Unhook the small black SATA cable connecting the Xbox 360 DVD drive to the motherboard. Have a long SATA cable connected to your PC, but leave it unplugged from the Xbox 360 drive.

(The picture shows the SATA cable connected, leave it unplugged from the drive)

Disconnect all other drives in your PC. You should disconnect both hard drives and DVD drives so they do not accidentally get flashed with the hacked firmware. Disabling these devices in your BIOS may not work, so physically unhooking them is the best solution. Of course, since you will have to use one of the PC DVD drives to boot from the NTFS4DOS CD, you should leave this drive connected, but disconnect all others.



360MODS



Turn on your PC and Xbox 360 at the same time, with the SATA cable still disconnected. Boot your PC from the NTFS4DOS CD. After a while it should say:

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

360MODS

Hit the Enter key and you should see an NTFS for DOS logo screen with a disclaimer. On this screen, please notice your drive letter that has been mounted at the top. You will need to know this when typing in commands. It is normally not assigned the same drive letter as Windows does; it is usually a letter after. My Windows C: partition is D: in NTFS4DOS for example.

```
Initializing HardDisks5      Size: 78150744 KB (LBA)
Disk5 Volume1 ( Windows NT NTFS ) - Initialized.

C:  disk1 volume1  35299 MB  Windows NT NTFS
D:  disk2 volume1  38162 MB  Windows NT NTFS
E:  disk3 volume1  141329 MB  Windows NT NTFS
F:  disk3 volume2  14998 MB  Windows NT NTFS
G:  disk4 volume1  38170 MB  Windows NT NTFS
H:  disk5 volume1  76316 MB  Windows NT NTFS
```

NTFS FOR DOS

This version of NTFS4DOS is free for private usage und evaluation. The private version is delivered "as is" without any support. Republishing of NTFS4DOS requires a written permission of Datapol GmbH.
For commercial usage licensed versions of NTFS4DOS Professional must be used.

The disclaimer asks you if you are going to use this for private usage only, please type in "Yes" without the quotes, and hit the Enter key.

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

At this point, plug the SATA cable into the Xbox 360 DVD drive.

Type in the following command, using your Xbox 360 serial number found on the back of the Xbox 360 case.

(We'll use the serial number 1234567 12345 as an example)

SAMREAD 1234567 12345 [press enter]



If you get an error like “Directory already exists” or “MKDIR failed...” don’t worry. X360SAM is trying to create a new folder but you already have one, so there’s no need to.

MTKFlash should run and your SATA controller should be listed. If you see an item in the list named “XTREME”, choose that. This is not your USB flash drive, as some people were guessing. It is actually your SATA controller. Xtreme Boot Maker will name it this when it creates the MTKFlash. Select your SATA controller and it should make a backup and then you will see X360 pop up really fast. After it is done creating the hacked firmware, it will give you the next instructions:

“Now unplug the SATA cable and power-cycle the PC and DVD drive before running SAMHACK 1234567 12345”

So do just that. Unplug the SATA cable from the 360 DVD drive and power off the Xbox 360 and then your PC.

Note: Some people may have trouble reading the firmware, where it gets to 01% then stops, and says Invalid Opcode. Try making a new, smaller partition on your hard drive, around 1gb in size. For some reason, NTFS4DOS does not support all drives with 32gb or larger partitions. You will have to run Xtreme Boot Maker again and mount the new small partition, then run the SAMREAD command again.



Flashing The Hacked Firmware

Power on your Xbox 360 and your PC at the same time, leaving the SATA cable disconnected. Boot your PC from the NTFS4DOS CD. Do the same things as before, hit Enter at the singlestepping prompt, type Yes and hit enter at the private usage disclaimer, then mount your drive and use the command `cd XBF` to change to the XBF directory. When you're back into DOS, plug the SATA cable back into the Xbox 360 DVD drive.

Type in the following command, using your Xbox 360 serial number that you used with the SAMREAD command.

```
SAMHACK 1234567 12345 [press enter]
```

MTKFlash should run and your SATA controller should be listed. Select your SATA controller and it will flash the drive with your hacked firmware. It should flash 4 banks. The 4th bank may say something like Datasum, it is normal. When it is done flashing, unplug the SATA cable from the 360 DVD drive, power off the Xbox 360, and power off your PC. Reconnect the 360 DVD drive to the 360 motherboard and test it.

Backup Your Original Firmware!

Boot into Windows. Go to the C: drive and find your orig.bin in the BACKUPS folder. This is your Xbox 360 drive 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.



Xtreme Boot Maker (Floppy)

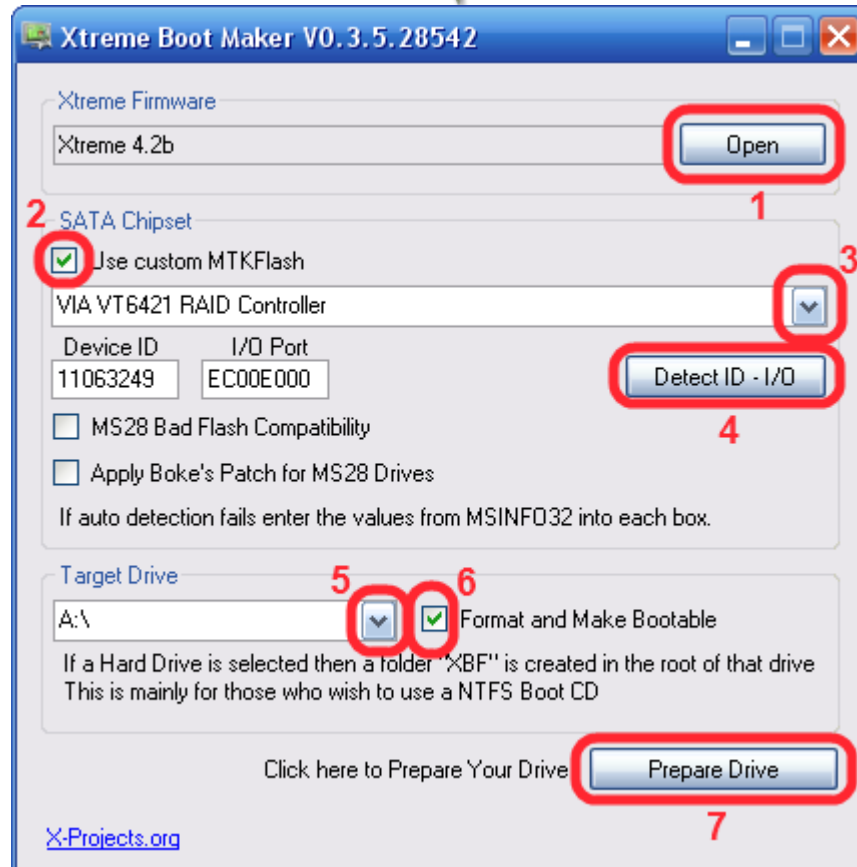
Quick warning about floppies. More and more people lately have been bricking their Samsung drives. The floppy disk is deciding to die out right in the middle of a flash. Sometimes the person is lucky and the bad flash recovery method can be used to reflash the drive. Many people have not been so lucky. The only way to fix the drive when the bad flash recovery method will not work is by opening the DVD drive, removing the epoxy on the firmware chip, desoldering the chip, and reflashing it externally via a programmer. Floppies are old technology for a reason. They are very unreliable. Please try to refrain from using a floppy. If you can use a bootable USB stick or burn an NTFS4DOS CD, do that instead. If you absolutely must use a floppy, use a new one!

The following process will set up a floppy disk with everything necessary to read your original firmware and write the hacked firmware onto the drive. We will use Xtreme Boot Maker to hex-edit MTKFlash, format the floppy disk, and copy the files onto it.

First, you need to make sure Microsoft .NET Framework v2 is installed. It is needed for Xtreme Boot Maker to run. If you do not have this installed, you will be prompted to download and install it.

Second, you need to make sure the drivers for your SATA chipset are installed. Use either the CD that came with your computer/SATA card, or use the manufacturer's web site to install the drivers.

Once you have that taken care of, you can download and install [Xtreme Boot Maker](#).



1. Hit the Open button to browse your computer and select your firmware. You should select xtrem51a.bin, xtrem51b.bin, xtrem51c.bin, or xtrem51d.bin from the archive you downloaded off Xbins.

With Xtreme 5.2A, backups are always read at 12x speed, the same speed as originals. The read speeds of original discs are unaffected. With the faster reading speed, the drive is significantly louder, and may have problems reading cheaper media, but you have the benefit of slightly faster loading times.

With Xtreme 5.2B, backups are always read at 4x speed. The read speeds of original discs are unaffected. With the slower reading speed, the drive is quieter, may read cheaper media better, but has slightly longer loading times.

With Xtreme 5.2C, the default backup read speed is 12x. When an original disc is placed in the drive, all subsequent backups will be



read at 4x. Read speed of original game discs will remain unaffected. Restart the system if you wish to read backups at 12x.

With Xtreme 5.2D, the default backup read speed is 4x. When an original disc is placed in the drive, all subsequent backups will be read at 12x. Read speed of original game discs will remain unaffected. Restart the system if you wish to read backups at 4x.

2. Select the checkbox "Use custom MTKFlash."
3. Select your SATA chipset from the drop-down list.
4. Click "Detect ID – I/O." It should input some characters in the Device ID and I/O Port boxes when it finishes.
5. Select your Target Drive as A:\
6. Check the box labeled "Format and Make Bootable"
7. Select "Prepare Drive." Wait until the program finishes.



Updating X360SAM and Keycheck

The current version of Xtreme Boot Maker includes version 0.4 of X360SAM. The latest version is v0.6, and includes a feature that copies the drive version string. This is necessary for avoiding the error code 66. The newest version of X360SAM will make the hacked firmware report as whatever drive version your original firmware was.

In addition to this update, Caster420 wrote a dos-based program named Keycheck that will check your drive key of the original firmware, as well as the hacked firmware that x360sam creates, and verify that they match. This is important because some people were having “partial” reads of the firmware and ended up bricking their drives.

You can download both the updated x360sam and keycheck in one zip archive [here](#).

Simply copy the three files from the zip archive to your floppy disk. If it asks you if you want to overwrite x360sam.exe and samread.bat , select Yes.

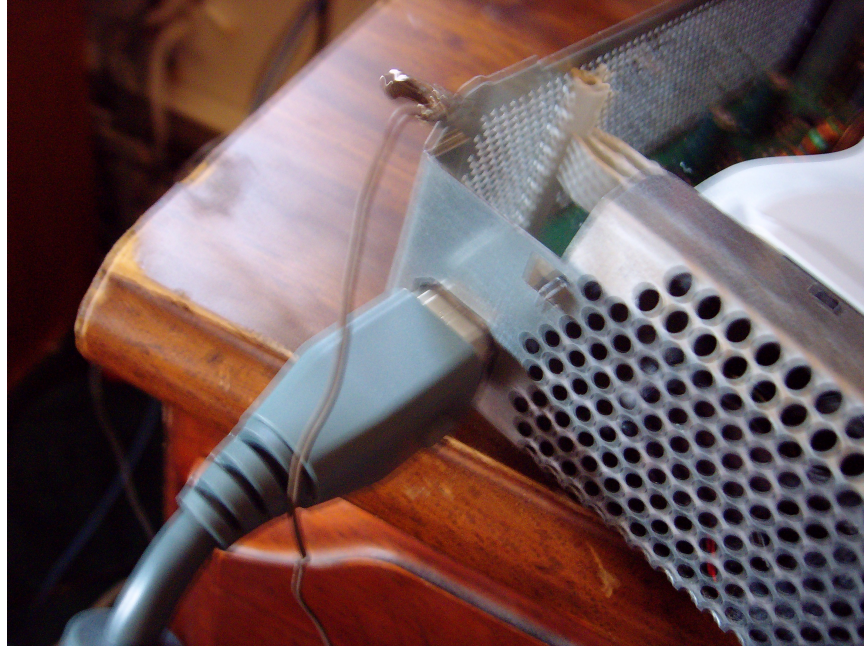
Flashing Your Drive (Floppy)

Reading The Original Firmware

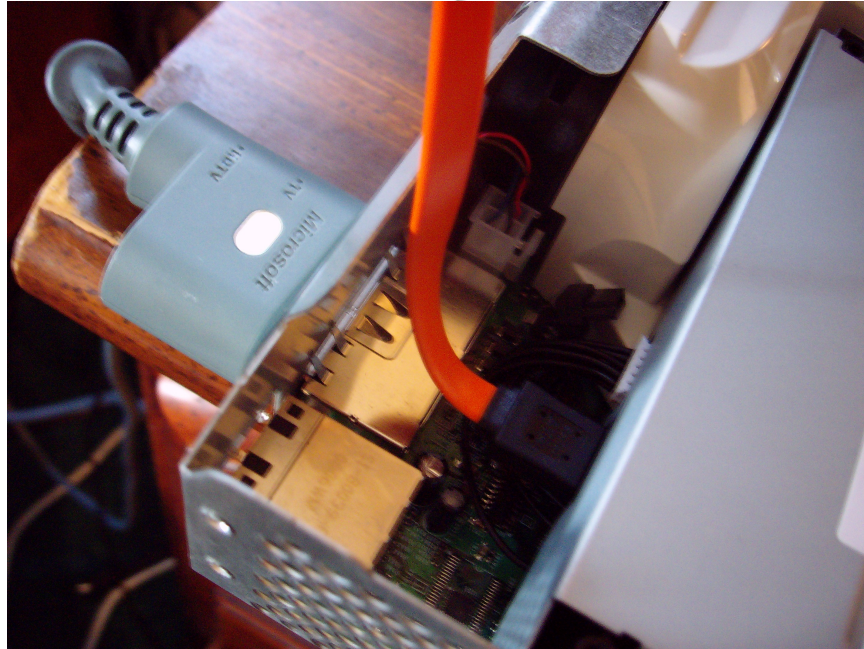
Power off both your PC and Xbox 360. Make sure the Xbox 360 power cable and video cable are both plugged in. You do not need to hook up the video to a TV, but the cable does have to be plugged into the Xbox 360. Unhook the small black SATA cable connecting the Xbox 360 DVD drive to the motherboard. Have a long SATA cable connected to your PC, but leave it unplugged from the Xbox 360 drive.

(the picture shows the SATA cable connected, leave it unplugged from the drive)

Disconnect all other drives in your PC. You should disconnect both hard drives and DVD drives so they do not accidentally get flashed with the hacked firmware. Disabling these devices in your BIOS may not work, so physically unhooking them is the best solution.



360MODS



Turn on your PC and Xbox 360 at the same time, and boot your PC from the floppy disk, into DOS. When you reach the DOS command prompt, plug the SATA cable into the Xbox 360 DVD drive.

Type in the following command, using your Xbox 360 serial number found on the back of the Xbox 360 case.

(We'll use the serial number 1234567 12345 as an example)



SAMREAD 1234567 12345 [press enter]

If you get an error like “Directory already exists” or “MKDIR failed...” don’t worry. X360SAM is trying to create a new folder but you already have one, so there’s no need to.

MTKFlash should run and your SATA controller should be listed. If you see an item in the list named “XTREME”, choose that. This is not your USB flash drive, as some people were guessing. It is actually your SATA controller. Xtreme Boot Maker will name it this when it creates the MTKFlash. Select your SATA controller and it should make a backup and then you will see X360 pop up really fast. After it is done creating the hacked firmware, it will give you the next instructions:

“Now unplug the SATA cable and power-cycle the PC and DVD drive before running SAMHACK 1234567 12345”

So do just that. Unplug the SATA cable from the 360 DVD drive and power off the Xbox 360.



Flashing The Hacked Firmware

Reboot your PC back into DOS, power on your Xbox 360, and plug the SATA cable back in when you get to DOS.

Type in the following command, using your Xbox 360 serial number that you used with the SAMREAD command.

```
SAMHACK 1234567 12345 [press enter]
```

MTKFlash should run and your SATA controller should be listed. Select your SATA controller and it will flash the drive with your hacked firmware. It should flash 4 banks. The 4th bank may say something like Datasum, it is normal. When it is done flashing, unplug the SATA cable from the 360 DVD drive, power off the Xbox 360, and power off your PC. Reconnect the 360 DVD drive to the 360 motherboard and test it.

Backup Your Original Firmware!

Boot into Windows and insert your floppy disk. Find your orig.bin in the BACKUPS folder. This is your Xbox 360 drive 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.



MS28 Instructions

Newer Xbox 360 systems have been shipping with Samsung drives with a newer firmware. This firmware, MS28, has certain lockout routines and can not be normally flashed via MTKFlash like an MS25 can. There are a couple workarounds to get the drive flashed. The VCC switch method requires you to open up the drive, desolder a resistor, and use a switch or wires to read/write to the drive. The Bad Flash Recovery method does not require desoldering/soldering, but will only work with VIA chipsets. The preparation for flashing an MS28 drive is the same as if you were flashing an MS25. The only difference is the actual flashing.

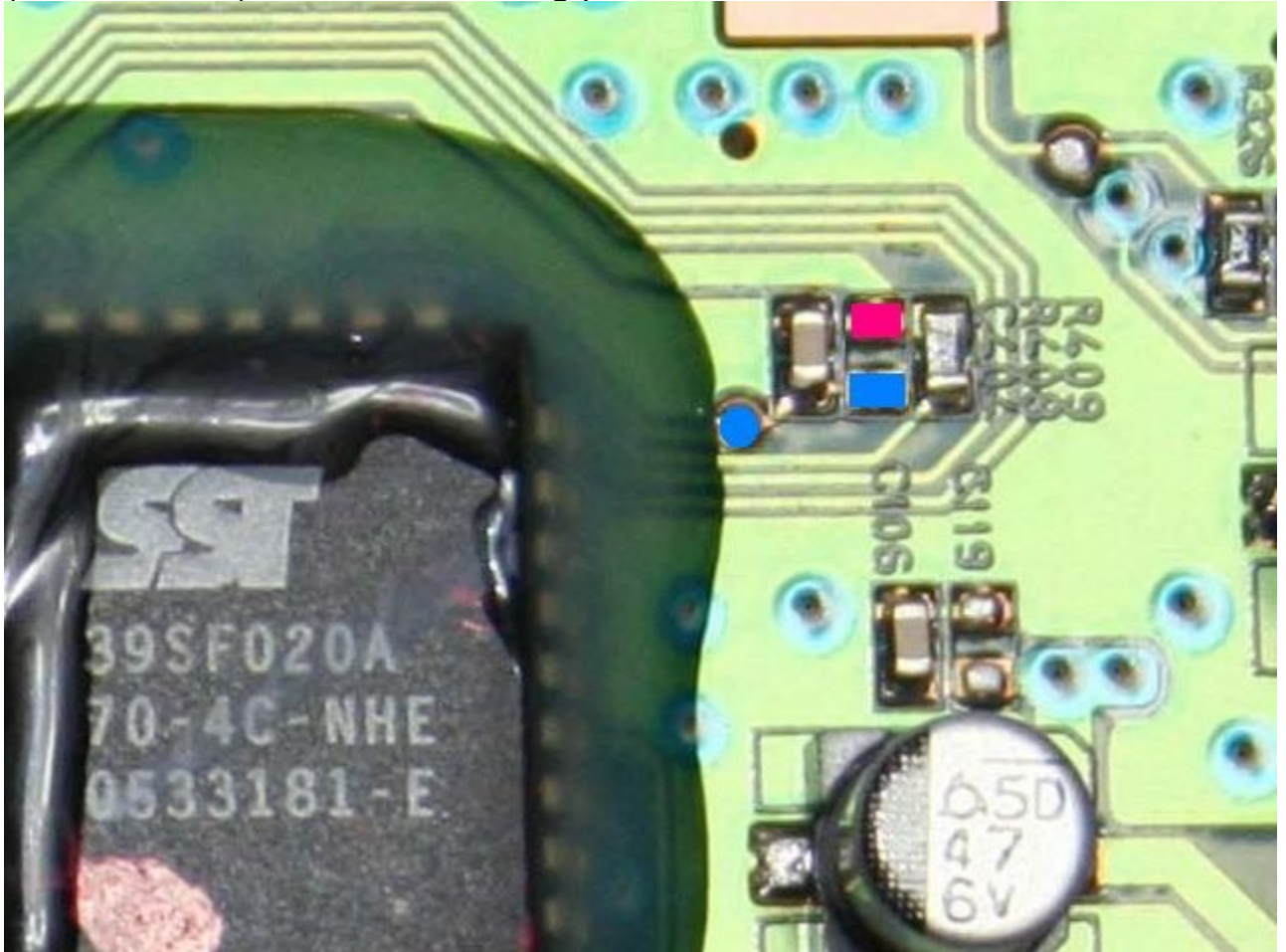
Preliminary Setup (same as MS25)

1. Check the SATA/MTKFlash Compatibility List
2. Download The Hacked Firmware
3. Use Xtreme Boot Maker to prepare a floppy/USB/NTFSCD (instructions for these are in the MS25 tutorial)

360MODS

Flashing an MS28 Using The VCC Switch Method (not for noobs, requires desoldering of a small smt resistor)

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 (or use wires) to one of the blue locations, and the other to the only red location. 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 xbocto 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.

360MODS





Reading The Original Firmware

Power off both your PC and Xbox 360. Make sure the Xbox 360 power cable and video cable are both plugged in. You do not need to hook up the video to a TV, but the cable does have to be plugged into the Xbox 360. Unhook the small black SATA cable connecting the Xbox 360 DVD drive to the motherboard. Have a long SATA cable connected to your PC, but leave it unplugged from the Xbox 360 drive.

Disconnect all other drives in your PC. You should disconnect both hard drives and dvd drives so they do not accidentally get flashed with the hacked firmware. Disabling these devices in your BIOS may not work, so physically unhooking them is the best solution.

Turn on your PC and Xbox 360 at the same time, and boot your PC from the USB/floppy/NTFS4DOS, into DOS. When you reach the DOS command prompt, plug the SATA cable into the Xbox 360 DVD drive.

Type in the following command, using your Xbox 360 serial number found on the back of the Xbox 360 case.

SAMREAD XXXXXXXX YYYYYY , using your Xbox 360 serial number
! Do not hit enter yet ! (leave the SAMREAD command up there)

Flick your VCC switch to “on” (or cross your wires) 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.

After the firmware is dumped, X360SAM creates the hacked firmware and give you the next instructions:

“Now unplug the SATA cable and power-cycle the PC and DVD drive before running SAMHACK 1234567 12345”

360 MODS

So do just that. Unplug the SATA cable from the 360 DVD drive and power off the Xbox 360. Set your VCC switch back to the “Off” position.



Flashing The Hacked Firmware

Reboot your PC back into DOS, power on your Xbox 360, and plug the SATA cable back in when you get to DOS.

Type in the following command, using your Xbox 360 serial number that you used with the SAMREAD command.

```
SAMHACK 1234567 12345
```

! Do not hit enter yet ! (leave the SAMHACK command up there)

Flick your VCC switch to “on” (or cross your wires and hold them) and then you can hit enter for the SAMHACK command.

MTKFlash should run and your SATA controller should be listed. Select your SATA controller and it will flash the drive with your hacked firmware. It should flash 4 banks. The 4th bank may say something like Datasum, it is normal. When it is done flashing, unplug the SATA cable from the 360 DVD drive, power off the Xbox 360, and power off your PC. Reconnect the 360 DVD drive to the 360 motherboard and test it.

Backup Your Original Firmware!

Boot into Windows and insert your floppy/USB or go to the C: drive. Find your orig.bin in the BACKUPS folder. This is your Xbox 360 drive 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.



Flashing an MS28 Using the Bad Flash Recovery Method (this method is easier and safer than the VCC method)

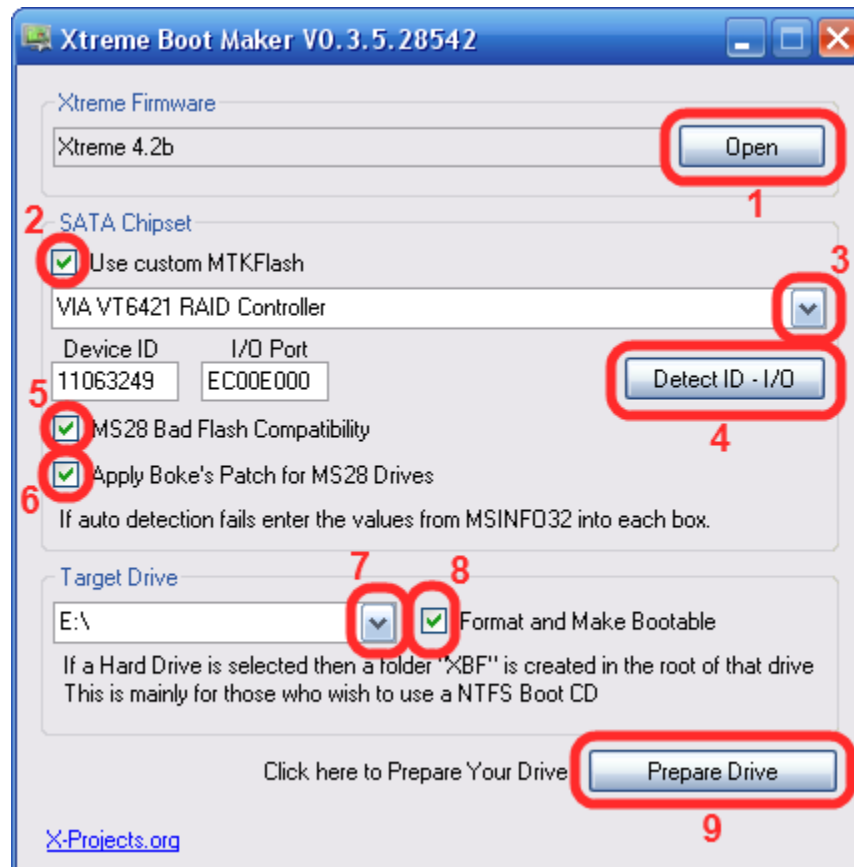
[Video Tutorial Here](#)

Requirements:

- [VIA chipset](#), simply will not work for other chipsets
- Need to be able to power off the drive and power it back on.
Recommend using the console to power the drive or the Xecuter Connectivity Kit v2 (which has a power switch).
- Need to use the /sata switch in the MTKFlash command or the drive will not show up

Setup

Use Xtreme Boot Maker to prepare your USB/floppy/C: with the correct files. In order to use the bad-flash recovery method, select the two checkboxes in the middle for MS28 Bad Flash Compatibility and for enabling Boke's Hexedit for detection of a single drive.



1. Hit the Open button to browse your computer and select your firmware. You should select xtrem52a.bin, xtrem52b.bin, xtrem52c.bin, or xtrem52d.bin from the archive you downloaded off Xbins.
2. Select the checkbox "Use custom MTKFlash."
3. Select your SATA chipset from the drop-down list.
4. Click "Detect ID – I/O." It should input some characters in the Device ID and I/O Port boxes when it finishes.
5. Select the checkbox for MS28 Bad Flash Compatibility.
6. Apply Boke's Patch for MS28 Drives
7. Select your Target Drive as the USB, floppy, or C: drive.

360MODS

8. Check the box labeled "Format and Make Bootable"
9. Select "Prepare Drive." Wait until the program finishes.



Updating X360SAM and Keycheck

The current version of Xtreme Boot Maker includes version 0.4 of X360SAM. The latest version is v0.6, and includes a feature that copies the drive version string. This is necessary for avoiding the error code 66. The newest version of X360SAM will make the hacked firmware report as whatever drive version your original firmware was.

In addition to this update, Caster420 wrote a dos-based program named Keycheck that will check your drive key of the original firmware, as well as the hacked firmware that x360sam creates, and verify that they match. This is important because some people were having “partial” reads of the firmware and ended up bricking their drives.

You can download both the updated x360sam and keycheck in one zip archive [here](#).

Simply copy the three files from the zip archive to the USB/floppy/XBF directory. If it asks you if you want to overwrite x360sam.exe and samread.bat , select Yes.



Reading The Original Firmware

Power off both your PC and Xbox 360. Make sure the Xbox 360 power cable and video cable are both plugged in. You do not need to hook up the video to a TV, but the cable does have to be plugged into the Xbox 360. Unhook the small black SATA cable connecting the Xbox 360 DVD drive to the motherboard. Have a long SATA cable connected to your PC, but leave it unplugged from the Xbox 360 drive.

(The picture shows the SATA cable connected, leave it unplugged from the drive)

Disconnect all other drives in your PC. You should disconnect both hard drives and DVD drives so they do not accidentally get flashed with the hacked firmware. Disabling these devices in your BIOS may not work, so physically unhooking them is the best solution.

Turn on your PC and Xbox 360 at the same time, and boot your PC from the floppy disk, into DOS. When you reach the DOS command prompt, plug the SATA cable into the Xbox 360 DVD drive.

Type in the following command, using your Xbox 360 serial number found on the back of the Xbox 360 case.

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.”

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, giving you a port error. Count to about ten, then turn on the Xbox 360. It should start reading and dumping automatically. It should 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.



After the firmware is dumped, X360SAM creates the hacked firmware and give you the next instructions:

“Now unplug the SATA cable and power-cycle the PC and DVD drive before running SAMHACK 1234567 12345”

So do just that. Unplug the SATA cable from the 360 DVD drive and power off the Xbox 360.

Flashing The Hacked Firmware

Reboot your PC back into DOS, and power on your Xbox 360. 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 plug the SATA cable back into the drive. Type the following command, using the serial number you entered when using SAMREAD.

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.”

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.

Backup Your Original Firmware!

Boot into Windows. Plug in your floppy/USB (or go to the C: drive) drive and find your orig.bin in the BACKUPS folder. This is your Xbox 360 drive 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.



Upgrading From a 4.x or Later Firmware

Firmware versions v4.x or higher included FirmGuard, which makes reading and writing to the drive much more difficult. This FirmGuard uses the MS28 core firmware lockout routines. In order to be able to read or write from a drive that is flashed with 4.x/5.x firmware, you would follow all the previous directions for setting up Xtreme Boot Maker and follow the directions for reading/flashing with this one extra step:

You need to disable FirmGuard. Burn the enable0800.iso found [here](#) to a DVD+R DL using IMGBurn or CloneCD. Even though the .iso image is only about 250mb, it needs to be burned onto DVD+R DL for it to work correctly.

Now, when following the above instructions, remember to do this instead:

1. Boot your PC to DOS, with SATA disconnected from the 360 drive, but with both power and video cables connected. Power on your 360 as well.
2. When you reach the DOS command prompt, connect the SATA cable into the drive, hit the eject button, and insert your 0800 disc. Let it spin up and read the disc. It usually takes a good 10 to 20 seconds. If you listen carefully, you can hear the drive laser shift and when you hear no more sounds except for the constant spinning disc, the disc has done the job.
3. Eject the drive back open and take out the 0800 disc.
4. FirmGuard should now be disabled and you should be able to read and write to the drive just like it was a normal MS25 drive.
5. Users with a VIA chipset can avoid using the 0800 disc altogether if they can correctly follow the instructions for “Bad-Flashing an MS28 Drive” in this tutorial. The FirmGuard is basically just the MS28 firmware, and this method for flashing the MS28 drives also works with 4.x firmware revisions.
6. Restarting the Xbox 360 disables the 0800 mode.



Hitachi-LG GDR3120L Tutorial

[Video Tutorial Here \(non-78 drives\)](#)

Opening The Xbox 360

The outer Xbox 360 “shell” is entirely screwless. Plastic friction tabs hold the case together. There are many different tutorials for opening the Xbox 360, with different methods. Here are some links to “opening the Xbox 360” tutorials. I felt it unnecessary to cover opening the Xbox 360 in this tutorial when there are already so many other guides out there. Nevertheless, here are some quick notes:

- The Anandtech guide says you need to use a Torx 12 screwdriver. There is no such thing. You need a Torx 10 screwdriver.
- Removing the grey side grill on the hard drive side is a little tricky. The first friction tab is actually inaccessible from the top holes in the case, so you need to stick your screwdriver in the hole by where the hard drive button is and unclip it.
- In order to push in the back clips, you can do a few things. You can use a thin metal object such as a precision flathead screwdriver / bobby pin / paperclip OR you can make an opening “key” out of a CD spindle case or old credit card. Anotehr alternative is purchasing an “unlock kit.”
- If all you want to do is just flash the firmware, you only need to remove the six long Torx screws on the bottom of the inside metal casing.

[Anandtech Guide](#)

[InformIT Guide](#)

[Xbox-Accessories Disassembly](#)

[Hydra's Guide to Making an Unlock Key](#)

[Textbook's Video](#)

[Syrax2Beta's Video](#)

[Google Video](#)

[shishnit's Videoshishnit's Video](#)

What Version

You can determine what version Hitachi drive you have simply by looking at the sticker. Your ROM version **will** matter in this tutorial. ROM version 46/47/59 drives will all have the same instructions. ROM 0078FK drives can only use the Slax disc to be put into ModeB, and must use a different method when flashing the drive.



ROM v0078FK

If you have a drive with ROM v0078FK, you will need to follow different instructions for flashing. The drive must still be put into ModeB, but can only be done using [Method 1, the Slax CD](#).

Currently, SATA-to-USB adapters like the X360USB and generic adapters will not work. SIL SATA chipsets are also not supported at this time due to read corruption. Your best bet would be to use onboard Intel ICH* chipsets, or Nforce chipsets. VIA chipsets work with most v78 drives, but not all of them.



ModeB

ModeB is the Hitachi drive's built-in debug mode that we need to get into before anything else can be done. When in ModeB, the drive can be recognized in Windows and flashed with the hacked firmware. There are a few different ways to get into ModeB. You only need to use whatever method works and you feel comfortable with.

ModeB Method 1 – SLAX

The first method you can use to get your Hitachi drive into ModeB is by using a bootable SLAX Live CD. It is a specially edited Linux LiveCD that will send custom commands to the Hitachi drive through on bootup.

1. [Download the latest SLAX image from Xbox-Scene](#)
2. Open the .rar archive using WinRar and extract the .iso image file.
3. Burn the .iso image to a blank CD-R using IMGBurn, CloneCD, Nero, or any other recording software capable of burning .iso image files.
4. Make sure your computer's BIOS is set to boot from CD first. Most are set to this by default.
5. Power off both the Xbox 360 and PC.
6. Make sure both power and video cables are plugged into the Xbox 360. Also provide a true path to ground between the Xbox 360 case and PC case by using croc clips, small wire, or setting them against each other so they are touching.
7. Unplug the small, black SATA cable from the back of the Hitachi DVD drive and connect your Hitachi drive to your PC via a SATA cable.
8. Power on the Xbox 360 and PC at the same time. Boot the PC from the Slax CD and wait until you reach the login prompt.
9. If you get a line of text that says "Spinning Up Disc..." eject the Hitachi drive and Slax should continue loading.
10. Check for ModeB! ([see below](#))


If you have the Hitachi v0078FK drive, click [here](#) for the instructions.



ModeB Method 2 – Two-Wire/Resistor Trick

Note: This ModeB method will not work on Hitachi v0078FK drives. You must use Slax if you have a v0078FK drive.

Experimentation and research by SeventhSon and others early on found a way to put the drive into ModeB by grounding one of the pins on the DVD power plug. This method works every time when done correctly, but take caution. This method is much more dangerous than other ModeB methods. You must read this entirely and understand what you are doing. If you screw up on this, you may brick your drive and what is worse, is without an original firmware backed up, you won't be able to purchase a new drive for your Xbox 360. Screw up on this and it's a good chance you'll make a permanent drive-less Xbox 360.

For safety reasons (less chance of bricking) please use a 1K-ohm resistor when doing the "two-wire trick." You can purchase resistors at a local RadioShack or other hobby electronics shop. This resistor has brown-brown-red-gold bands on it.  RadioShack model number 271-1118.

Now, take a look at the back of your DVD drive and you should see a black SATA cable to the right and the power cable to the left. The power cable consists of ten smaller black wires and has a white connector.



Xbox 360 DVD drive power connector pinout

What you will want to observe is pins 0 and 9. Since the left side holes of the connector are empty, the wires you want end up being the top right and bottom left wires.

Stick a sewing pin in next to these wires as shown in the image below.



What you need to do is use the resistor to touch these two pins together when booting the Xbox 360, then release the resistor immediately afterwards. So, with the Xbox 360 off, hold the resistor so that each end touches the sewing pin. With your other hand, hit the power button on your Xbox 360 and as soon as you see the power light come on, remove the resistor and break the connection. This is the tricky part and where people were bricking their drives. You can screw this up in two ways. First, some people were accidentally using the wrong points on the power cable. Second, people were holding the two wires together for too long. The pins should be connected at most for only a half second on bootup.

Again, just for clarity:

1. Make the cable as shown above by sticking sewing pins in the 0 and 9 locations on the power plug.
2. Plug this newly made power plug back into the back of the DVD drive with the Xbox 360 off.
3. With the Xbox 360 powered off, use a 1Kohm resistor and hold it to connect the two pins together.

360 MODS

4. Power on the Xbox 360 and immediately remove the resistor as soon as you see the green power led on the Xbox 360 light up.
5. Check for ModeB! ([see below](#))



ModeB Method 3 – Connectivity Kit

Note: This ModeB method will not work on Hitachi v0078FK drives. You must use Slax if you have a v0078FK drive. The kit can still be used to power the drive, but the debug/ModeB button will not work.

If the Slax disc did not work for you and you are too afraid to use the two-wire/resistor trick method, you can purchase a Xeno or Xecuter Connectivity Kit to put the drive into ModeB.

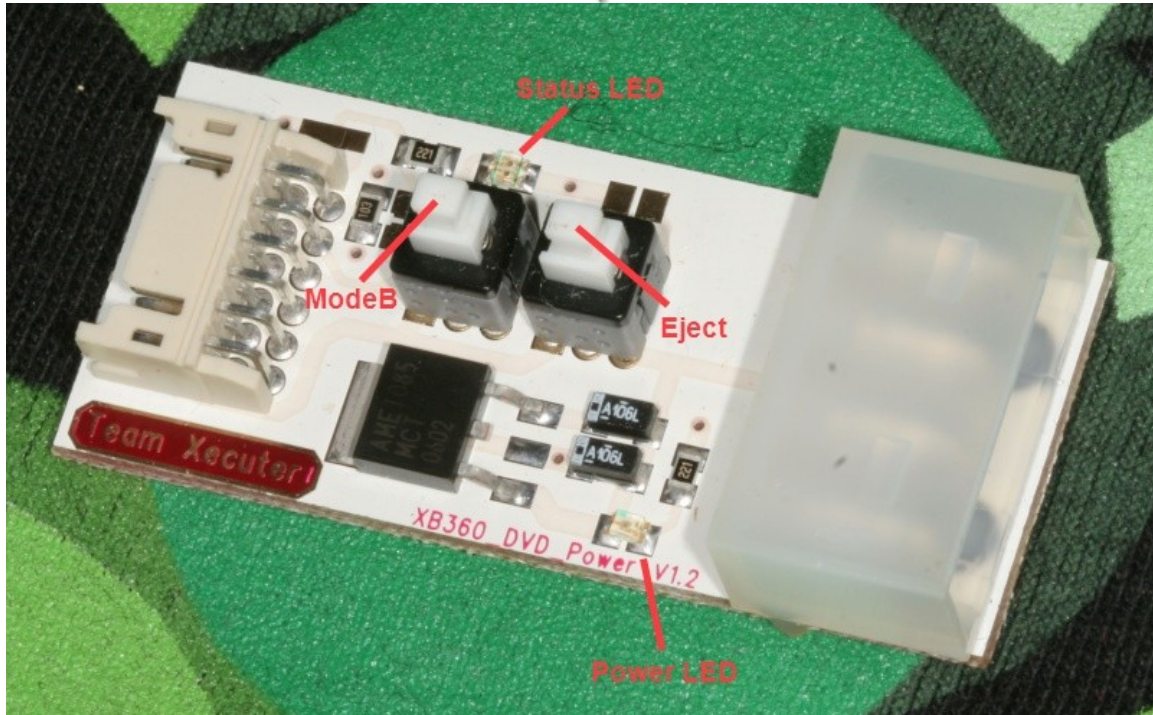
Some important warnings about the kits –

You can fry the kit and/or drive if you plug in the DVD power cables upside down. Look on the connector. There are small tabs to make sure you are connecting the cables correctly.

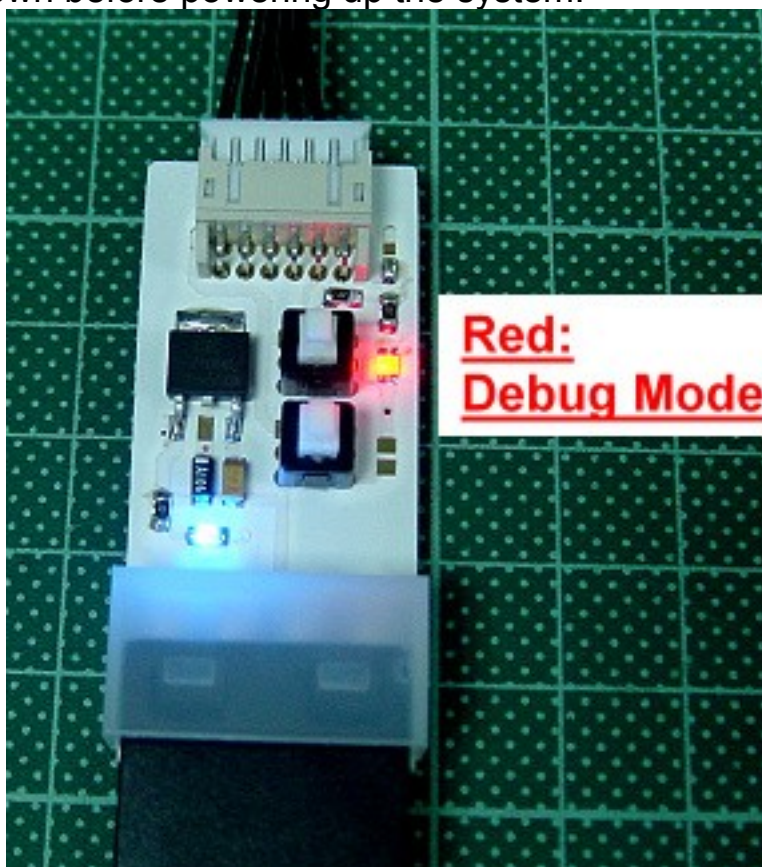
You can also fry the kit and/or drive if you short it out on something. The back of the kit is not protected, and you can see bare solder points on the circuit. If you aren't careful, you can short the kit onto your PC case, Xbox drive, or another metal object.

For a clear explanation of the danger, take a look at [this pdf](#).

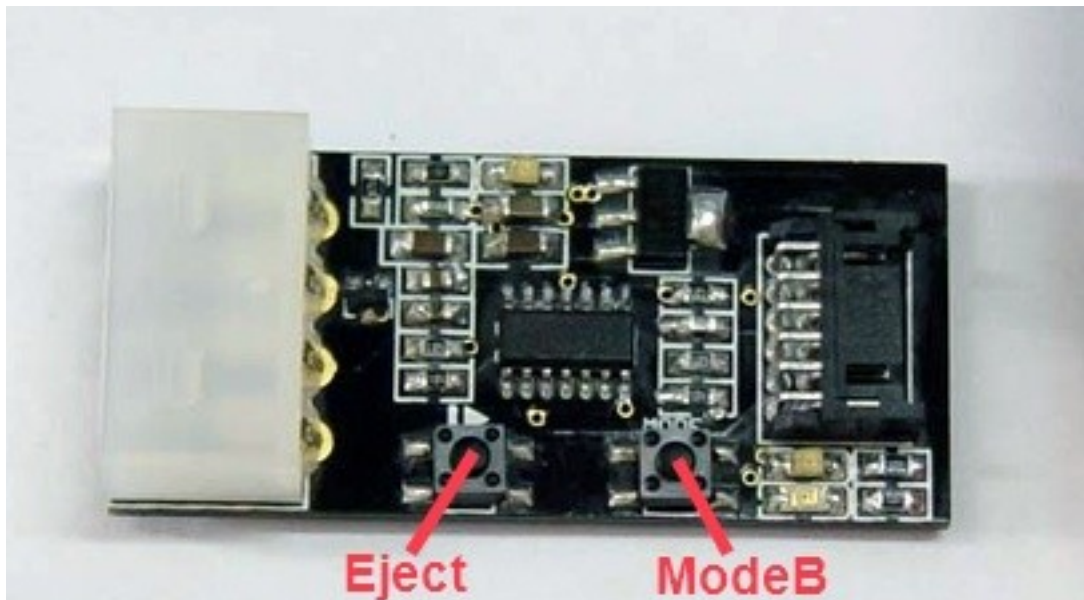
Disconnect both power and SATA cables from the DVD drive and take it out of the Xbox 360. Power off your PC and hook up the connectivity kit. Hook up the SATA cable to the DVD drive as well. Push the ModeB button down and power on your PC and boot into Windows.



For the Xecuter kit, make sure the Eject button is up and the ModeB button is down before powering up the system.



360MODS



The same status LED configuration is used for the Xeno kit. If you power up the drive and the LED is green, hit the ModeB button so that the LED turns red for ModeB.



ModeB Method 4 – Hotswap

The fourth method of ModeB in fact is not a method to get into ModeB at all. The drive never goes into ModeB, but using this method, you will be able to flash your drive and since that's what we are trying to do here, it is still included as a "ModeB method." This method is not very applicable to many people so I won't spend too much time going over it.

You need a SATA DVD-ROM drive hooked up to your PC and detected in Windows. This can be a normal PC SATA DVD-ROM drive like the SH-D163A or it can also be an Xbox 360 Samsung drive in 0800 mode. Whatever it is, it has to be a SATA DVD-ROM drive detected and working in Windows. Note your drive letter, then unplug the SATA cable from your "normal" drive and plug it into the Hitachi drive. You can then flash your Hitachi with that drive letter.



ModeB Indicators

It is obvious that we must first get the Hitachi drive into ModeB before doing anything else. Before worrying about your PC, before worrying about flashing, or anything else, focus on ModeB. ModeB is a property of the DVD drive alone. It does not rely on SATA and has nothing to do with your computer. In fact, you can do the following checks with no SATA cable hooked up to the Hitachi drive at all. The following are signs of ModeB. Your Hitachi drive must be doing one of the following. Your drive does not have to display all these signs to be in ModeB. If your drive is showing just one of these, it is in ModeB.

Signs of ModeB:

1. If using the Xbox 360 to power the drive and using the wire/resistor trick, your Xbox 360's power LED should flash rapidly
2. With all methods, it should take two presses of the eject button to either open or close the DVD tray.
3. With all methods, when you eject the drive back in using the eject button, it should auto-eject back open a second later.
4. Obviously, if the drive shows up in Windows, then it is in ModeB.



Drive Detection in Windows

When you have made sure your drive is in ModeB, connect it to your PC and power up your PC. If you used Slax, remember to take out the Slax disc because you need to boot from the hard drive into Windows. At the Windows loading bar, you should eject the Hitachi drive in and out a few times. Some people believe that they only need to eject the drive if the loading gets stuck, but this is NOT true! Testing has shown that Device I/O Errors while flashing were a result from the failure to eject the Hitachi drive at the Windows loading bar.

When Windows boots up, check to see if the drive is detected. First, open device manager. Right-click "My Computer" and select "Manage." A Computer Management window should open up with a list to the left. In that list to the left, under System Tools, is Device Manager.

Check your CD/DVD drives to see if the Hitachi GDR-3120L is listed. If it is not listed, try updating your SATA drivers.

Open up "My Computer" and see if you have a new CD-ROM drive. Right-click on your drive and eject it. You just want to make sure you know which drive is the Hitachi drive. Remember the drive letter.



Note: The following instructions are for Hitachi drive versions 46/47/59. If you have a Hitachi v78, follow [these instructions](#).

A Neat Powertoy

To save time and make it easier, you should download and install a Windows XP powertoy titled “Open Command Window Here.” By using this, you will not have to navigate to your directory using the command prompt. This is an absolute must if you do not have much experience using a command prompt.

[Download](#)

Run the “CmdHere.exe” and go through the installation.

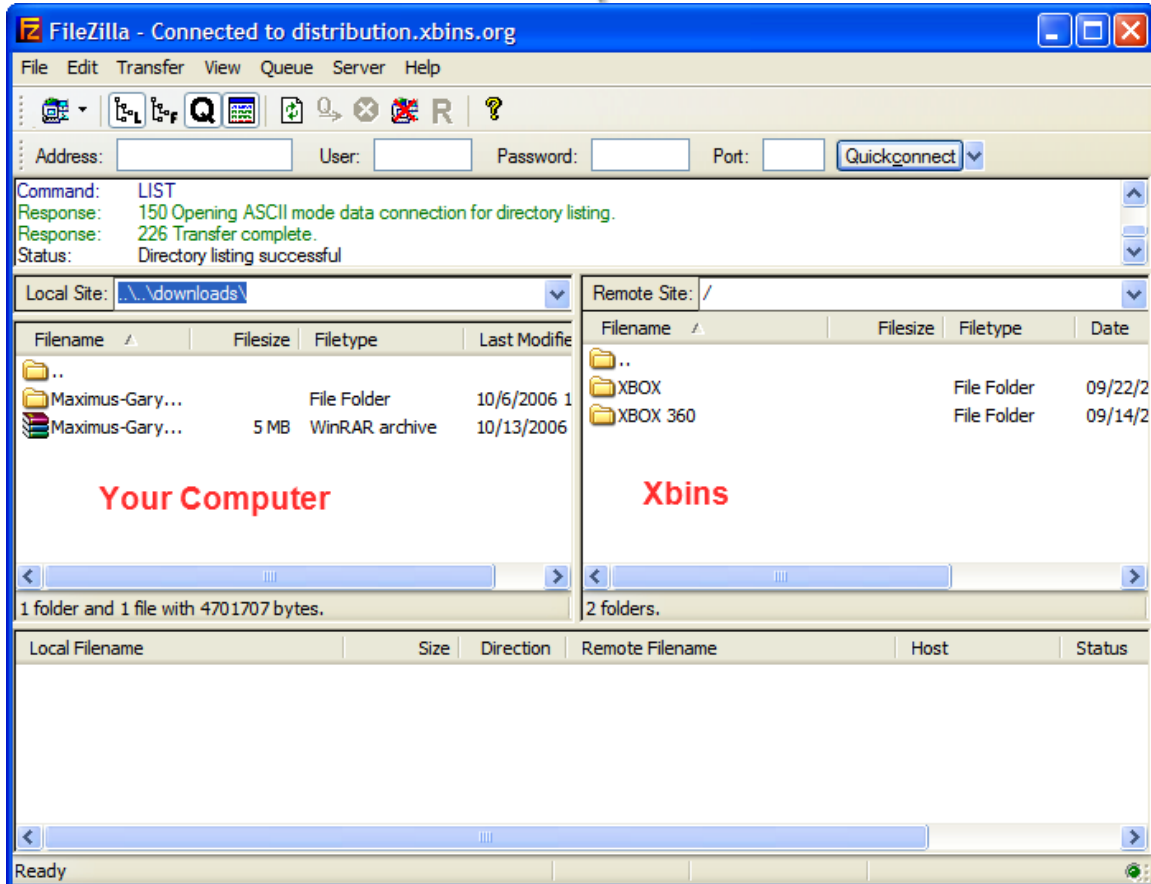
Downloading The Firmware

The hacked firmware may be illegal under the DMCA, EU CD, or other local, national, and international copyright laws. The hacked firmware contains portions of Microsoft’s copyrighted firmware and therefore cannot be linked to or downloaded publicly. Do not request the firmware on any forums because it is against most forum rules and you will most likely be banned. The best method to obtain the firmware is by using Xbins. Xbins is an IRC channel and FTP server that hosts Xbox and Xbox 360 mod files, homebrew programs, and development software.

If you have never used Xbins before, the easiest method is to use Ground Zero’s automated Xbins downloader.

[Download](#)

Download the self-extracting archive and run the xbins.exe file. It will ask you where you want to save the files, choose your desktop. Now, go into the “Xbins” folder on your desktop and run the .bat file. The program will automatically connect to the IRC channel, message the bot, and connect to the FTP server. When filezilla opens up you should see the local Xbins folder on your left side, and a few folders on your right side (this is the FTP server).



The hacked firmware can be found in:

/XBOX 360/firmware/hacked firmware/ Hitachi-LG GDR-3120L/

Simply drag the “Maximus-Garyopa_XTRM-HITACHI_v2_3_Stealth.rar” file over to the left side of FileZilla, into the Xbins folder and wait for it to finish downloading. You can use WinRAR or 7-zip to extract the RAR archive.



Upgrading From Older Firmware?

If you are upgrading from an older hacked firmware, like a previous GaryOPA firmware, a Birdy firmware, or the original Commodore4Eva package, you must restore your drive to the original firmware before continuing. If you are flashing the firmware to a stock drive, ignore this section and skip to "[Flashing The Drive.](#)"

Right-click on the X-LG folder and select "Open Command Window Here." A command window should open up.

Type in the following command and hit Enter:

```
RESTORE.BAT
```

It will search for any Hitachi drives connected and restore the firmware back to the original. This is necessary before flashing to the latest firmware. After restoring the firmware, it is probably a good idea to disconnect the SATA cable, power off the Xbox 360 and PC, then continue the process of getting the drive into ModeB before flashing with the updated firmware.



Flashing The Drive

Right-click on the X-LG folder and select “Open Command Window Here.” A command window should open up.

Type in the following command and hit Enter, where X is your Hitachi drive letter and ##### is any four numbers you want

```
FLASH23S X #####
```

For example, if my Hitachi drive is showing up in “My Computer” as E, I may flash the drive using the command

```
FLASH23S E 1337
```

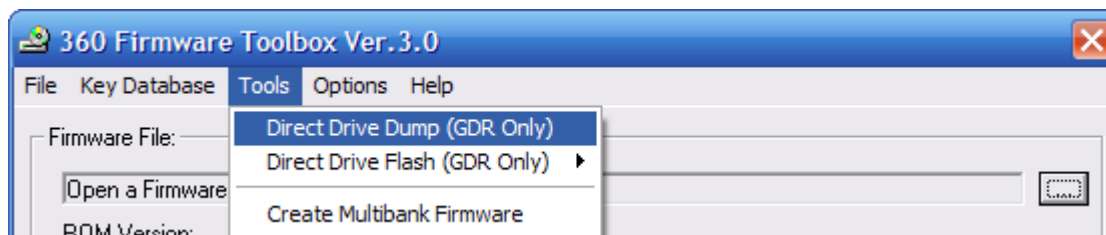
Wait until the process to finish. You will find a backup of your original firmware in the X-LG folder. There will be a folder in there named X23S-##### for whatever four numbers you chose when you flashed the firmware. Zip or Rar this folder up and email it to yourself for backup purposes.

Flashing the v0078FK Drive

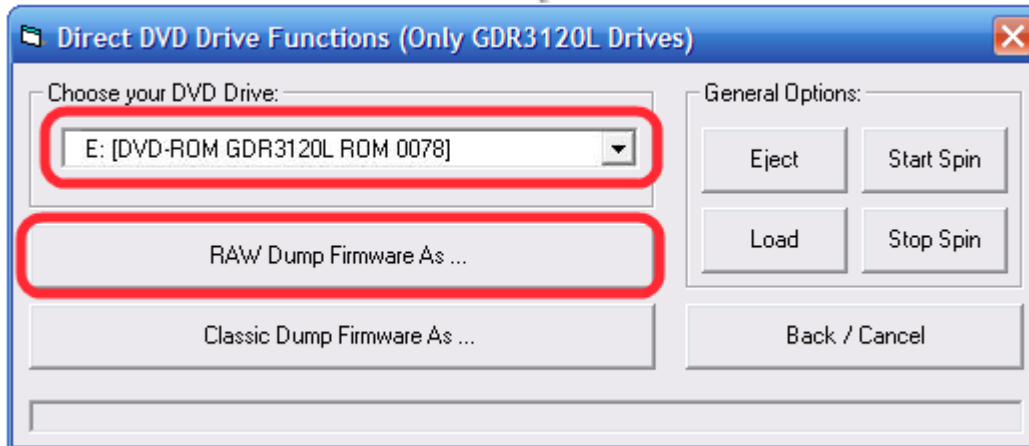
[Video Tutorial Here](#)

Once you have the v78 drive in ModeB using the Slax disc and detected in Windows, follow these instructions for flashing the v0078FK drive.

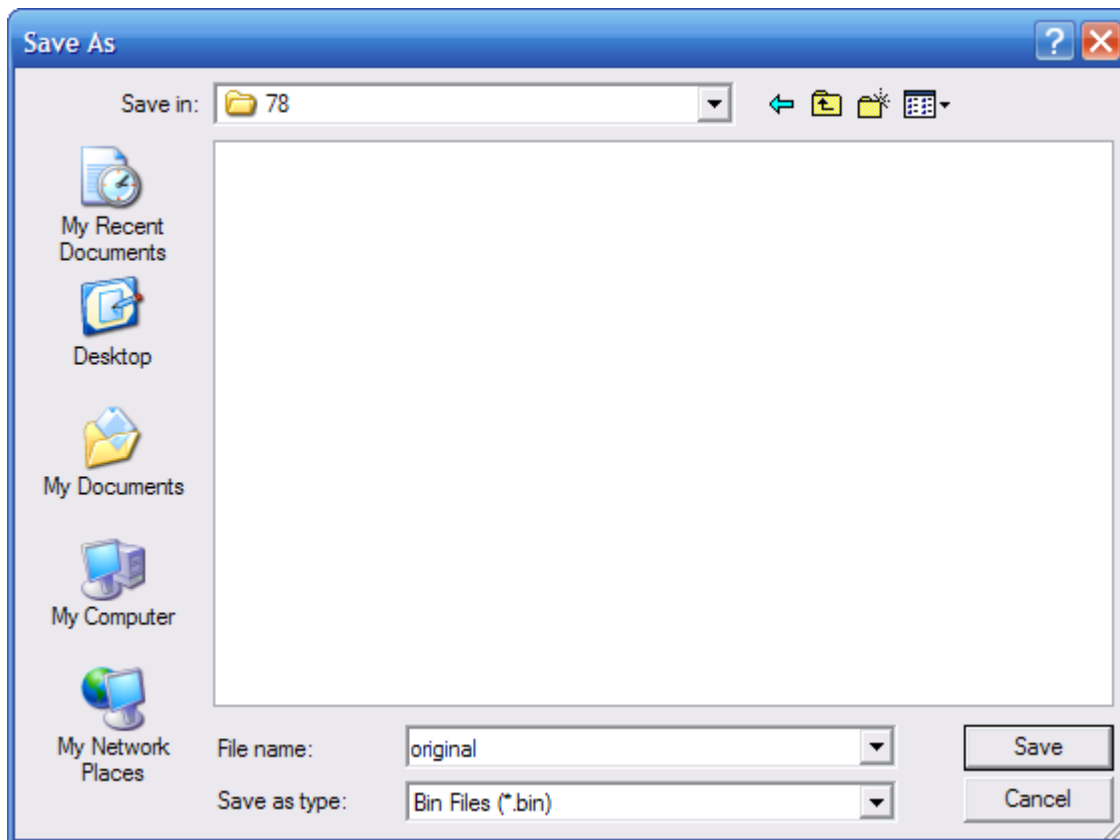
1. Download Maximus 360 Firmware Toolbox v3.0 from [here](#). It is a .NET application that requires Microsoft [.NET framework v2](#) to run properly.
2. Insert an original retail game or movie DVD into the Hitachi drive. Remember that the Hitachi drive in ModeB likes to automatically eject after a few seconds. Follow one of these methods to keep the drive closed.
 - With the Hitachi drive tray open, press the eject button once, then push the tray in manually or..
 - Press eject a third time, while the tray is closing
3. Wait for Windows to recognize the disc inserted, then close out of any autoruns caused by the disc.
4. Open 360 Firmware Toolbox.
5. Select Tools > Direct Drive Dump (GDR Only)



6. Make sure your Hitachi drive is selected in the drop-down list
7. Select "Raw Dump Firmware As..."

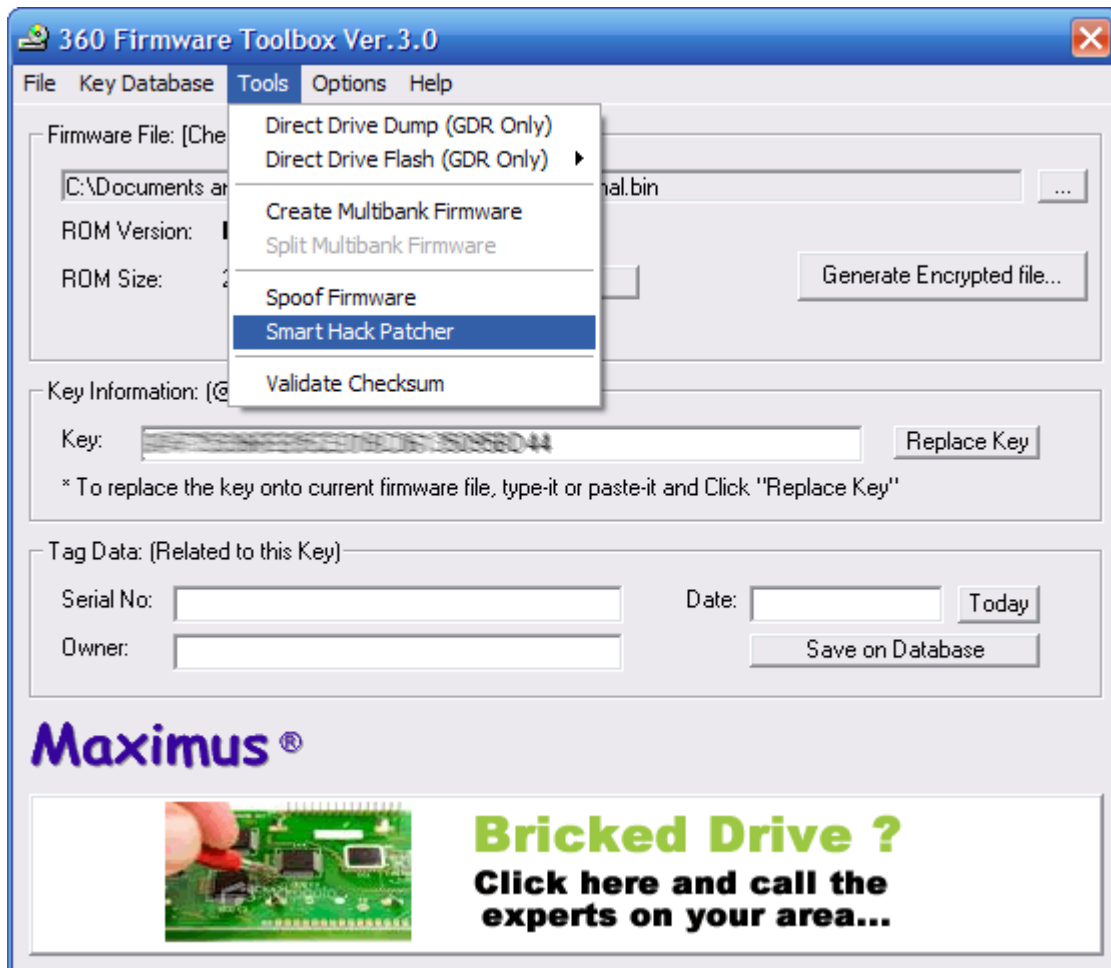


8. Save the original firmware as original.bin somewhere safe



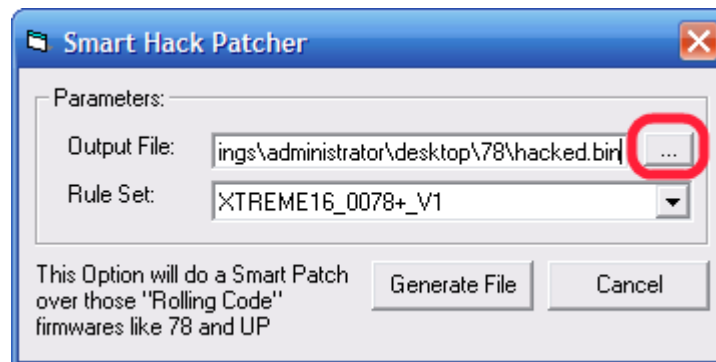
9. The program will tell you that your firmware has been dumped and asks if you want to open it, select "Yes"
10. Make sure the key displayed looks fairly unique, with no multiple FF or 00 bytes. You may also want to dump the firmware a couple times and make sure the key is the same for each dump.

11. Select Tools > Smart Hack Patcher



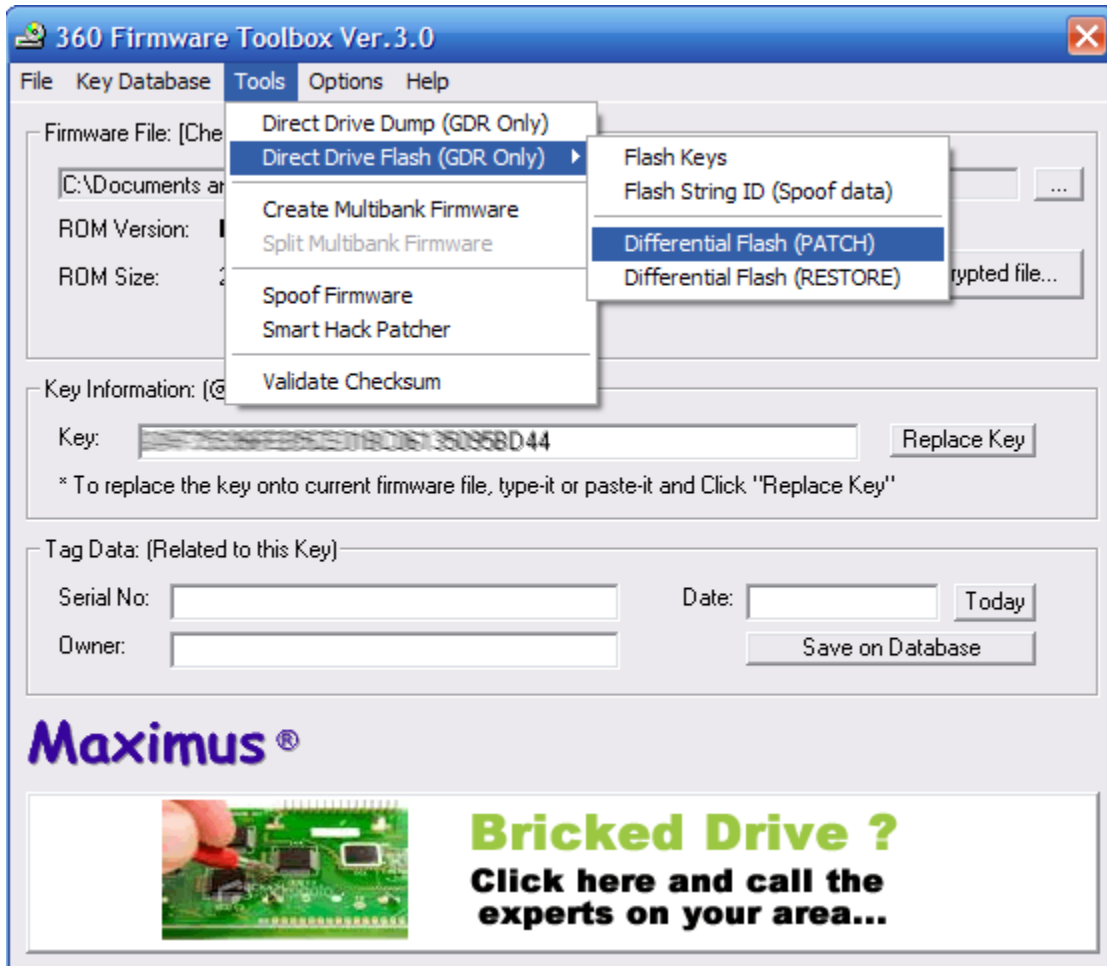
12. Read the warning and accept it

13. On the line labeled output file, click the box to the right with the ellipsis (three dots) and save the file as hacked.bin where you saved the original firmware.

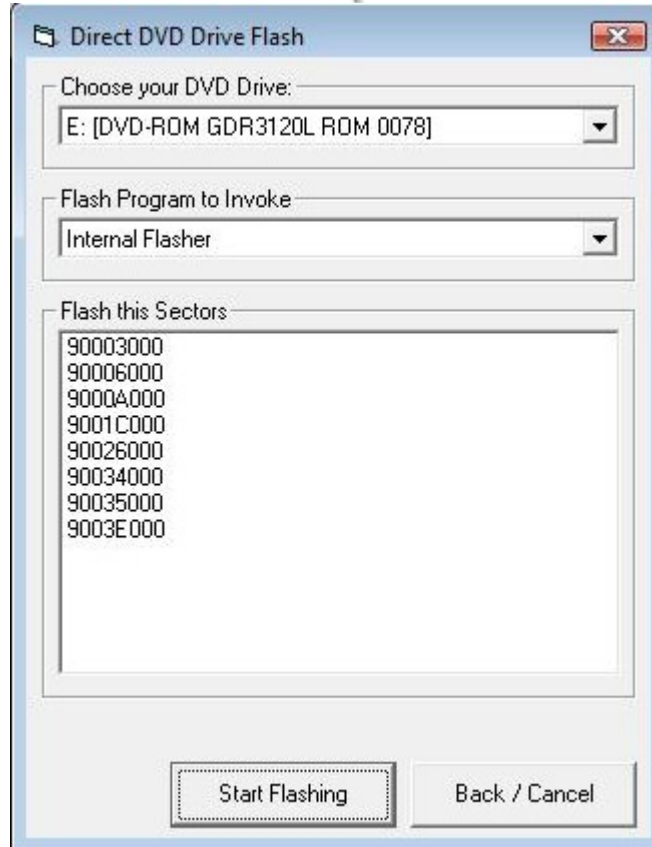


360MODS

14. Check that the rule set is for Hitachi v78
15. Select "Generate File"
16. It should say that the hacked firmware was created, and asks if you want to open it, again select "Yes"
17. Verify that the key is still the same as before
18. Select Tools > Direct Drive Flash (GDR Only)
19. Select Differential Flash (PATCH)



20. Check that your Hitachi drive is selected in the drop-down list
21. Hit "Read and Detect Differences"
22. Select "Start Flashing" and let it finish



23. Close out of the program, hook the drive back up to the 360, and test it out.



Backing Up Xbox 360 Games

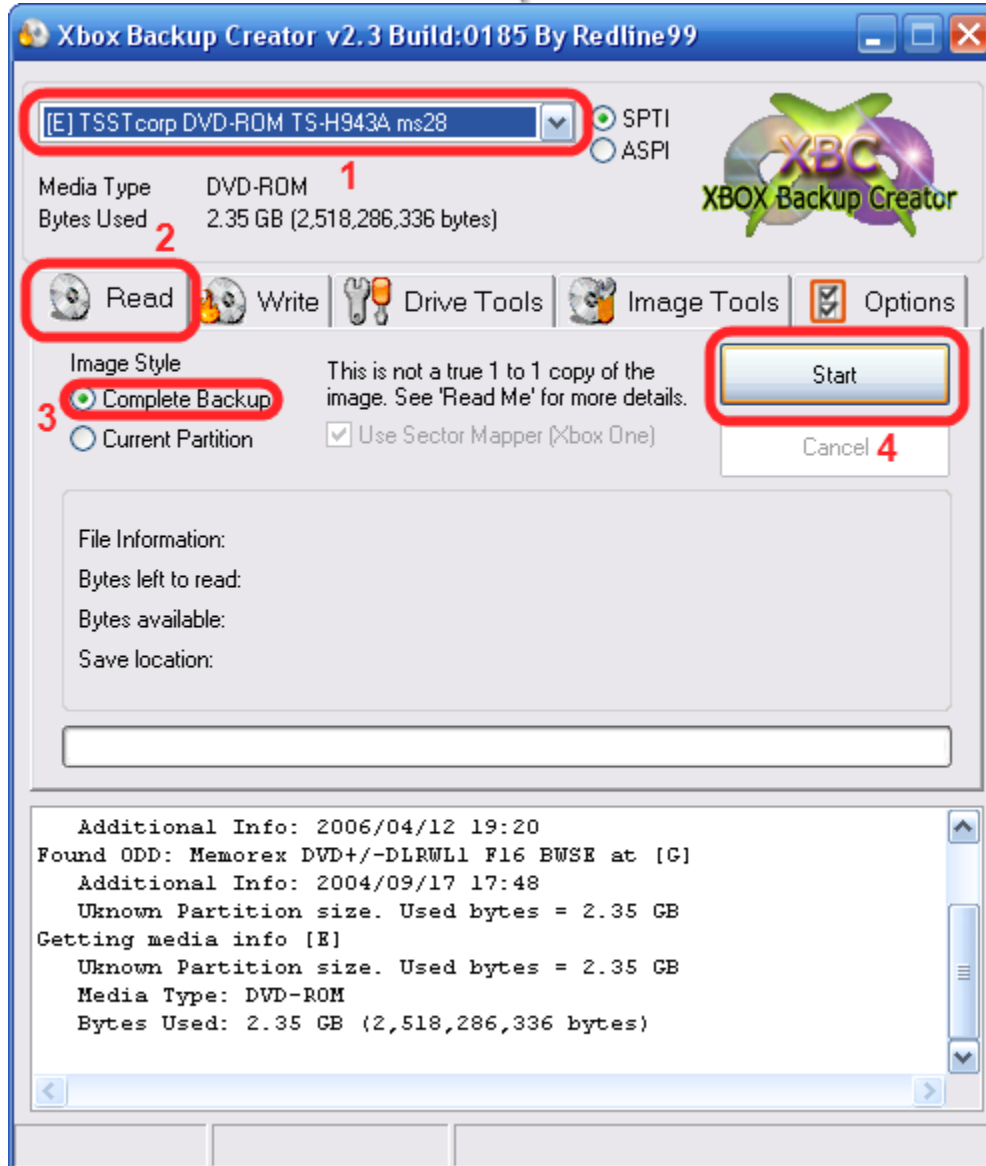
There are a few different ways to back up your Xbox 360 games. There are two free/cheap methods, but are pretty complex. There is a much easier method as well, but it requires that you purchase a specific DVD-ROM drive and install it in your PC.

Method 1 – Using Your Xbox 360 Drive (Samsung only)

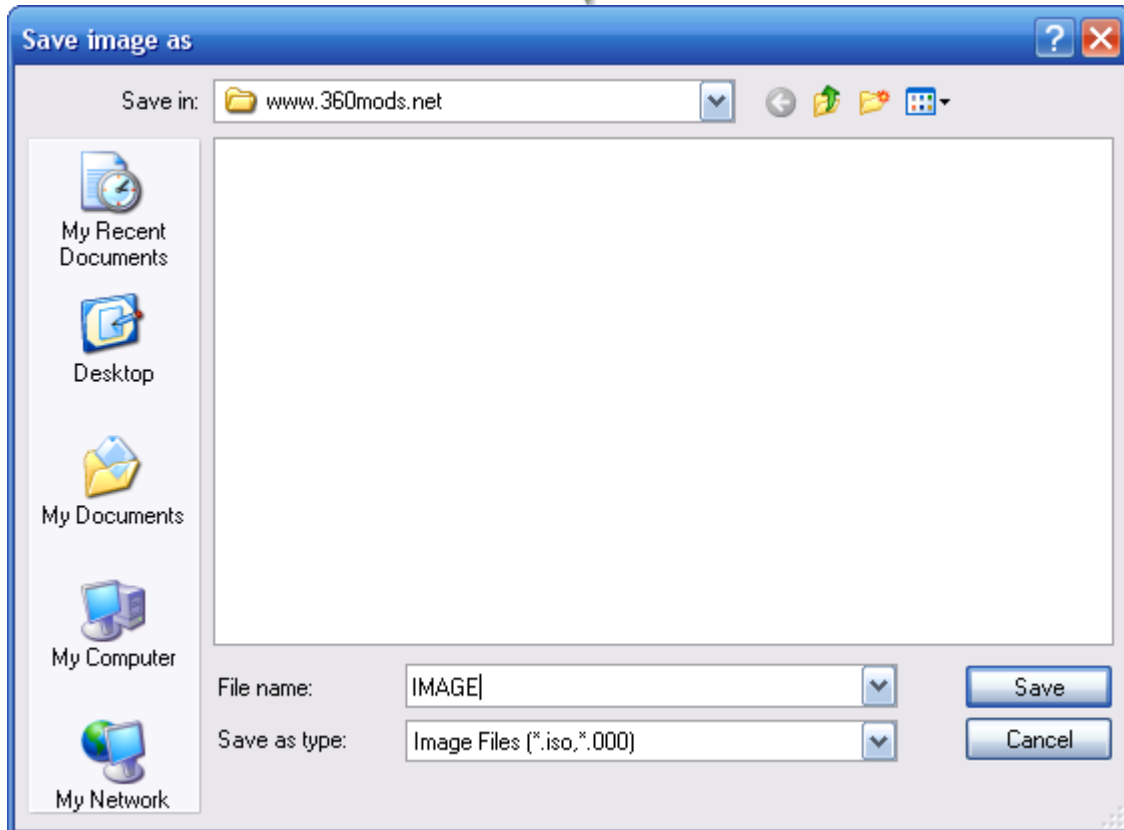
This method involves connecting the Samsung drive to your PC. This method currently does not work with the Hitachi drive because the game partition fails to unlock correctly. In order to get the Samsung drive recognized in Windows, the drive needs to already have the flashed firmware on it. You will need to enable the built-in 0800 mode of the firmware. First, you need to burn the enable0800.iso found in the firmware package to a DVD+R DL using IMGBurn or CloneCD. Even though the .iso image is only about 250mb, it needs to be burned onto DVD+R DL for it to work correctly.

Have the Xbox 360 and PC both powered off. Both power and video cables should be hooked up to the Xbox 360. Connect the Samsung drive to your PC via a SATA cable. Power on the 360 (leave your PC off) and insert the 0800 disc you burned. Listen to the drive, let it spin up and read the disc. After 10-20 seconds, you can take eject the drive and take out the 0800 disc. Now, you can power on your PC and boot into Windows. Your drive should show up in “My Computer”

The easiest method to backup your games is by using [Xbox Backup Creator](#). All you need to do is insert your game and run Xbox Backup Creator.



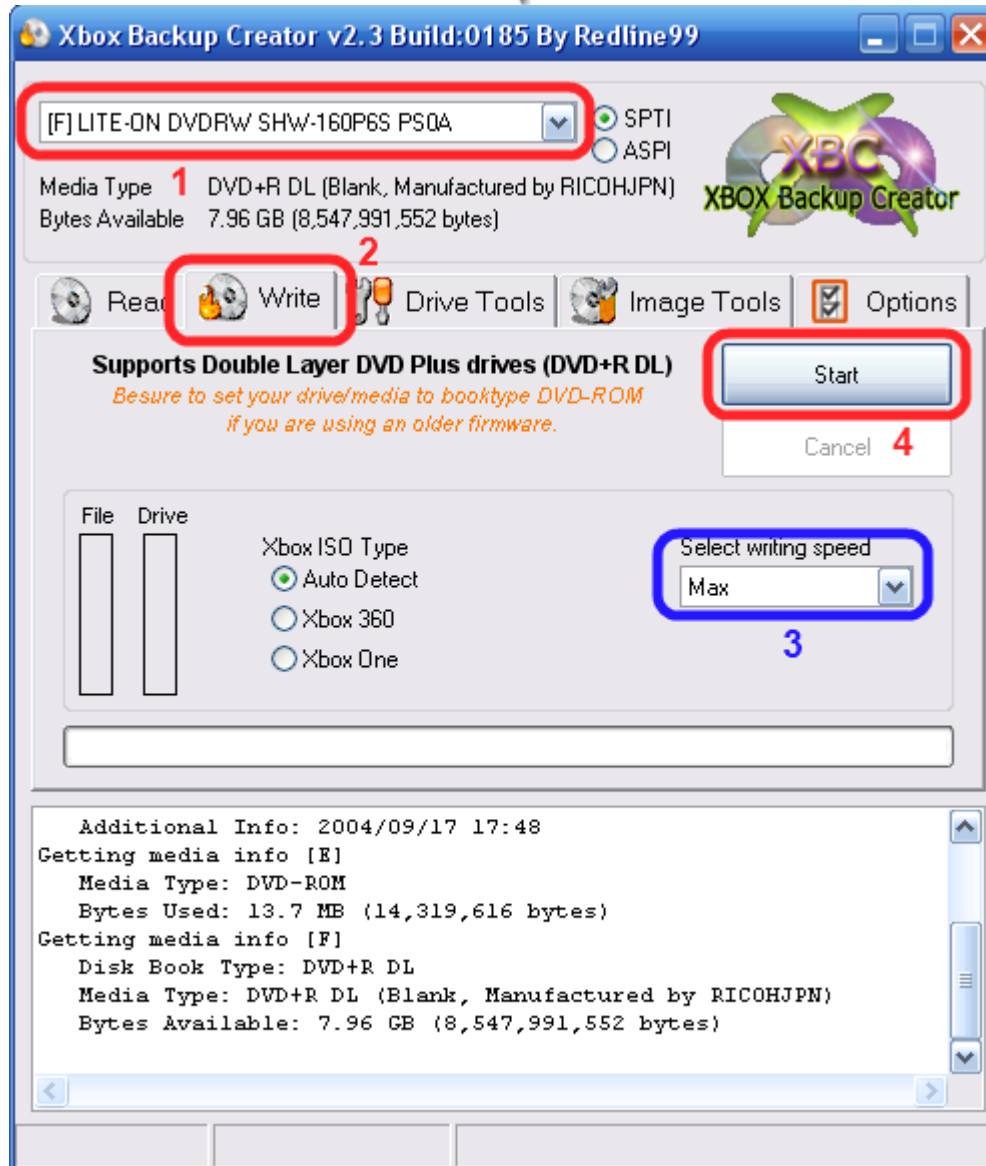
1. Make sure your Xbox 360 drive is selected.
2. Select the Read tab.
3. Select Complete Backup
4. Hit Start



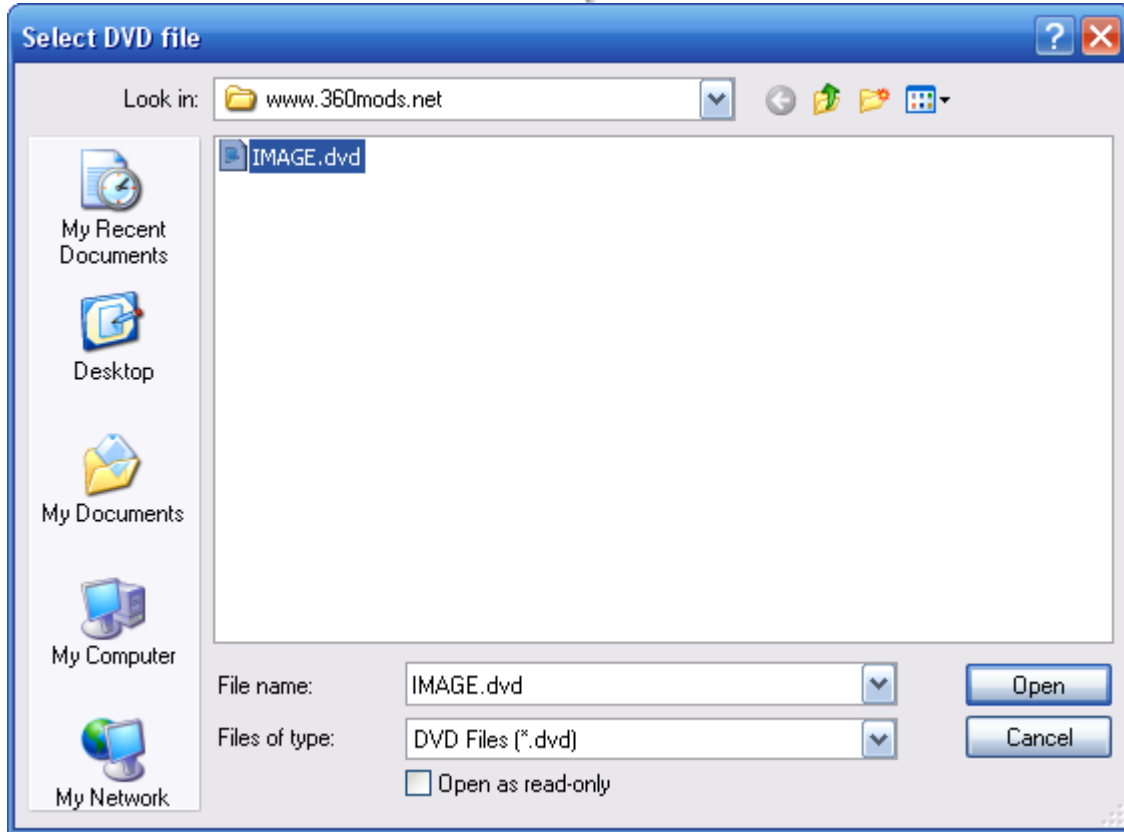
Name the file anything you want and hit Save.

Wait for the game to backup to your computer.

To burn the game, you can also use Xbox Backup Creator.



1. Make sure your DVD recorder is selected.
2. Select the Write tab
3. Select your writing speed , 2.4x recommended
4. Hit Start and select your .dvd file





Method 2 – Purchasing a “Kreon” Drive

The following drives can be purchased, installed in your PC, then flashed with one of Kreon’s alternate firmwares for reading Xbox 360 games.

SH-D162C (IDE)
TS-H352C (IDE)
SH-D163A (SATA)
TS-H353A (SATA)

After purchasing the drive, install it in your PC and then get on Xbins and download the firmware.

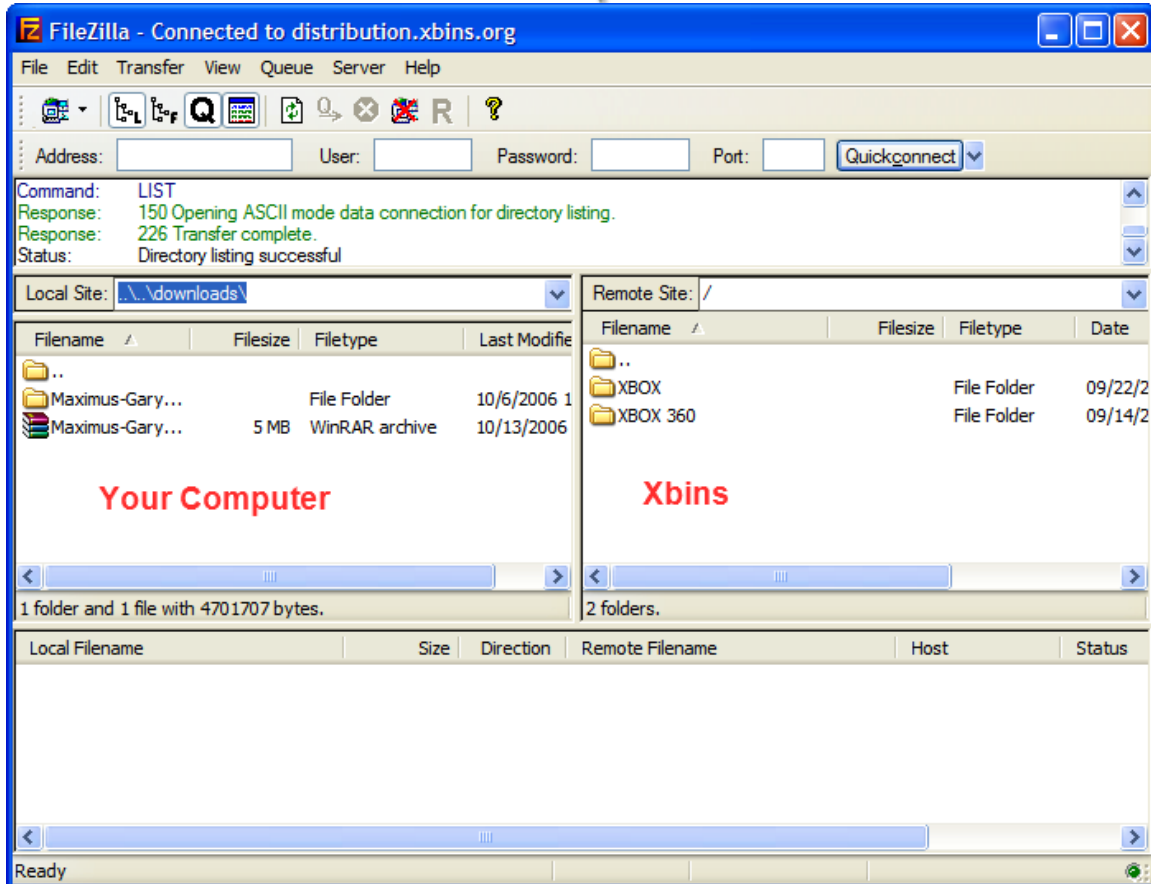
Downloading the Kreon Firmware

The best method to obtain the firmware is by using Xbins. Xbins is an IRC channel and FTP server that hosts Xbox and Xbox 360 mod files, homebrew programs, and development software.

If you have never used Xbins before, the easiest method is to use Ground Zero’s automated Xbins downloader.

[Download](#)

Download the self-extracting archive and run the xbins.exe file. It will ask you where you want to save the files, choose your desktop. Now, go into the “Xbins” folder on your desktop and run the .bat file. The program will automatically connect to the IRC channel, message the bot, and connect to the FTP server. When filezilla opens up you should see the local Xbins folder on your left side, and a few folders on your right side (this is the FTP server).



The hacked firmware can be found in:

/XBOX 360/firmware/hacked firmware/**Samsung SH-D162C/**

Or

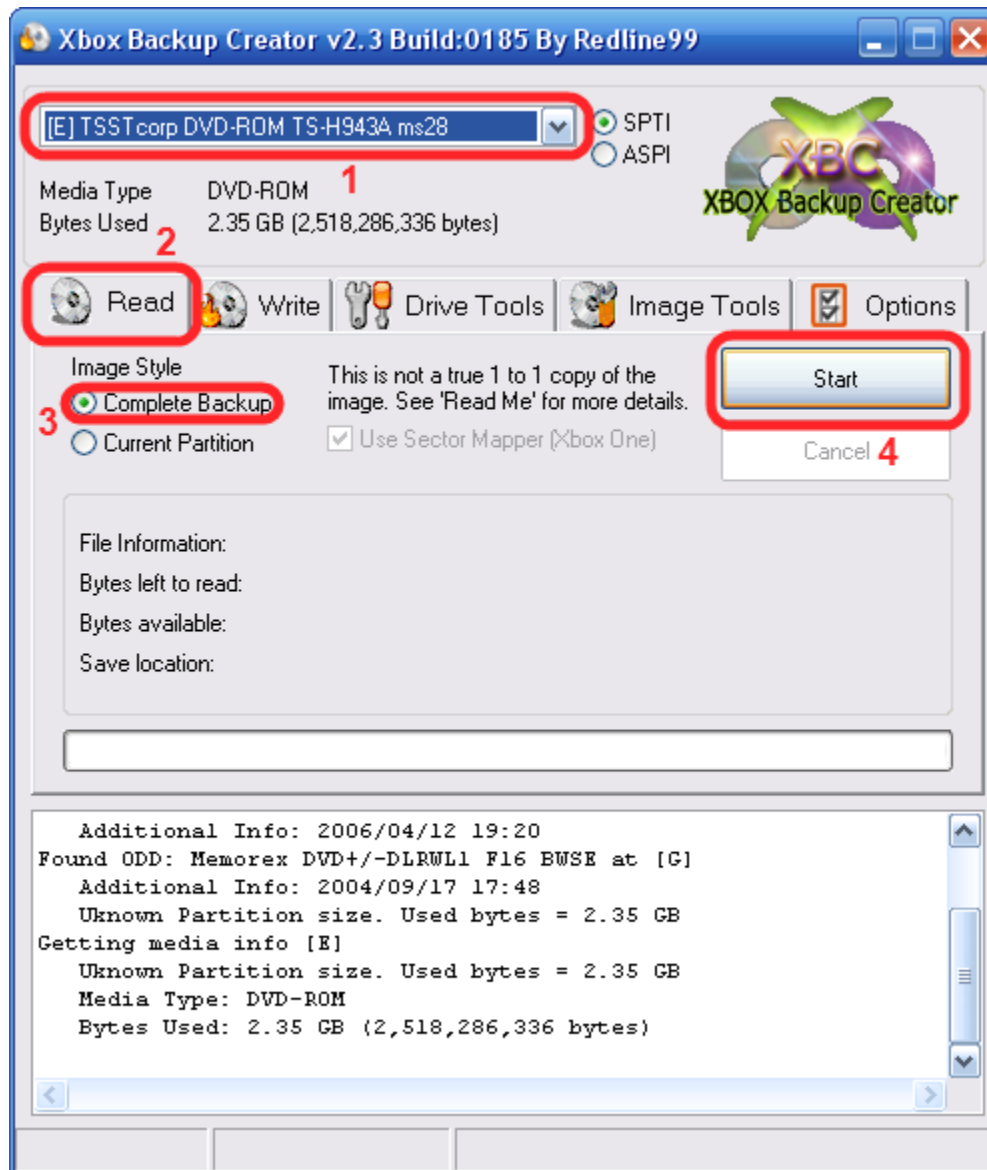
/XBOX 360/firmware/hacked firmware/**Samsung SH-D163A/**

Simply drag the “SH-D162C_KREON_V081.RAR” or “SH-D163A_KREON_V080.RAR” file over to the left side of FileZilla and wait for it to finish downloading. You can use WinRAR or 7-zip to extract the RAR archive.

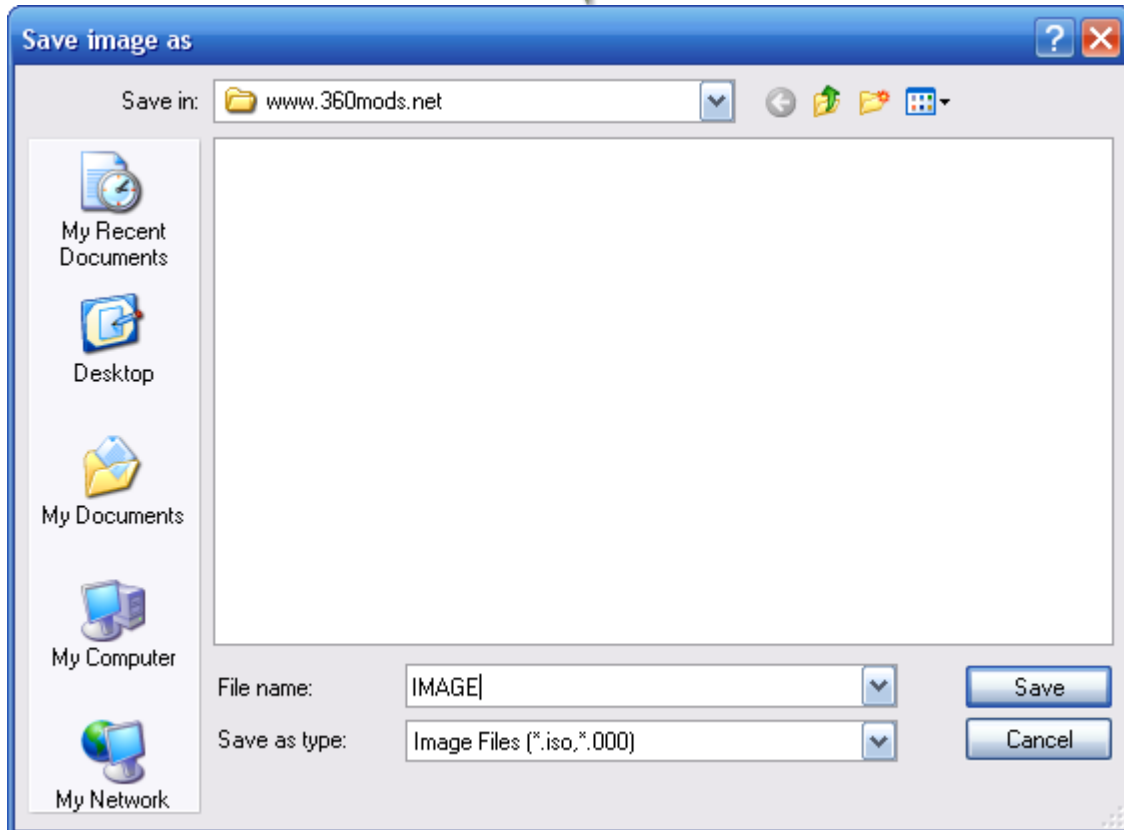
Read the “How to upgrade firmware.txt” included in the RAR archive for instructions on flashing your drive with the Kreon firmware.

When the drive is flashed with the Kreon firmware, you can start making backups of your Xbox 360 games.

The easiest method to backup your games is by using [Xbox Backup Creator](#). All you need to do is insert your game and run Xbox Backup Creator.



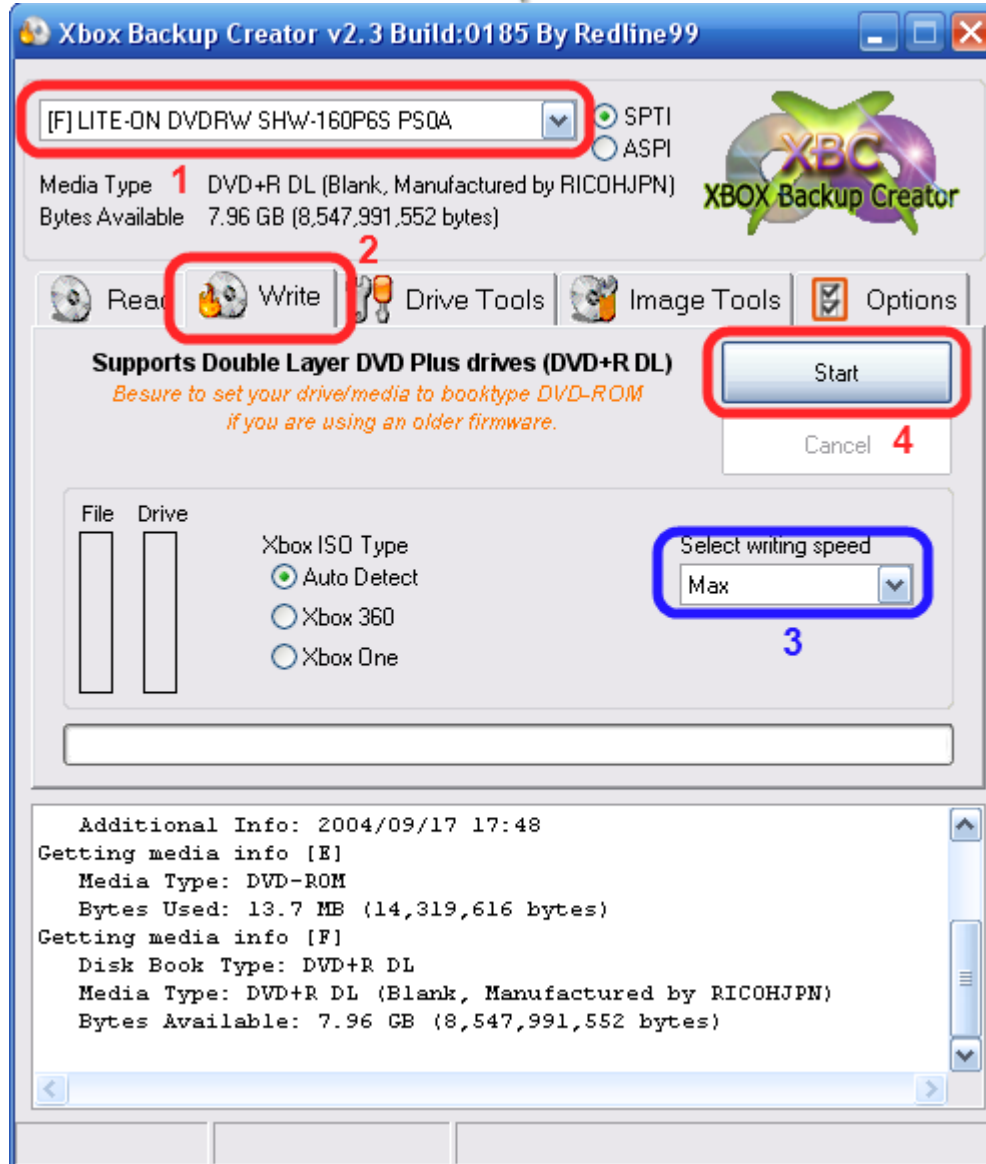
1. Make sure your Kreon drive is selected. (pic shows a 360 drive)
2. Select the Read tab.
3. Select Complete Backup
4. Hit Start



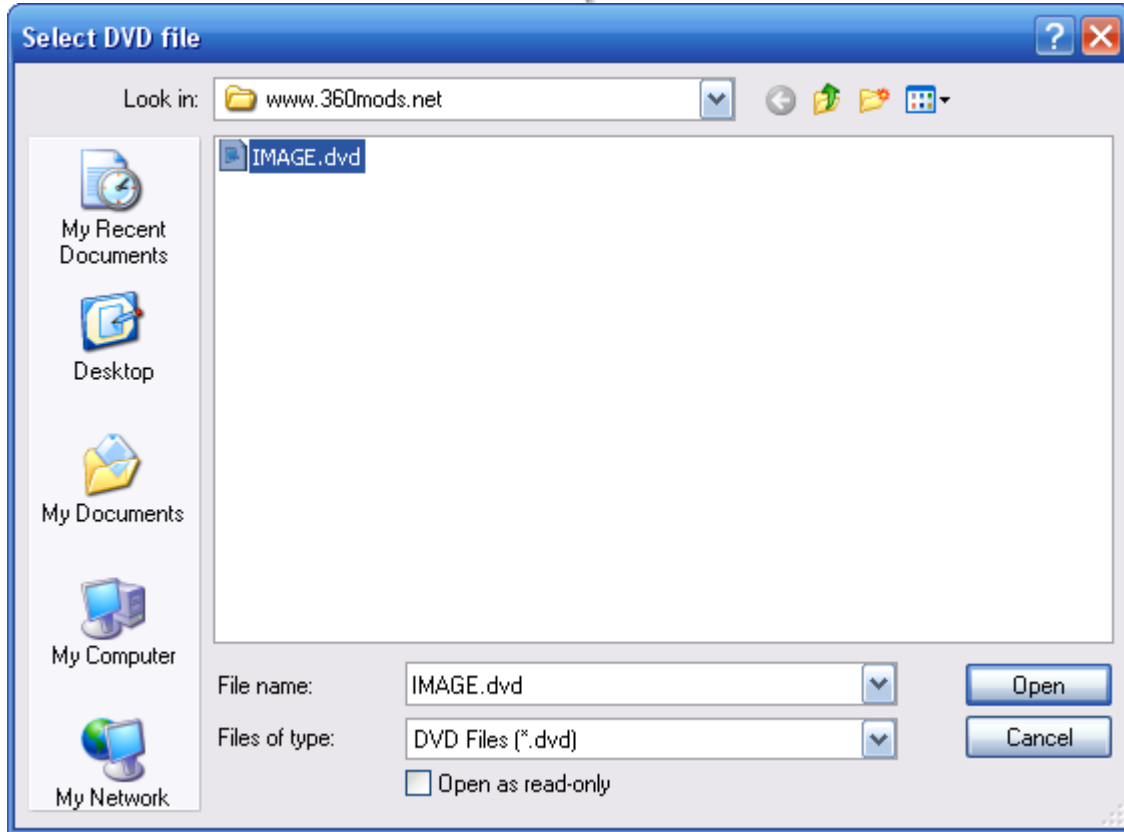
Name the file anything you want and hit Save.

Wait for the game to backup to your computer.

To burn the game, you can also use Xbox Backup Creator.



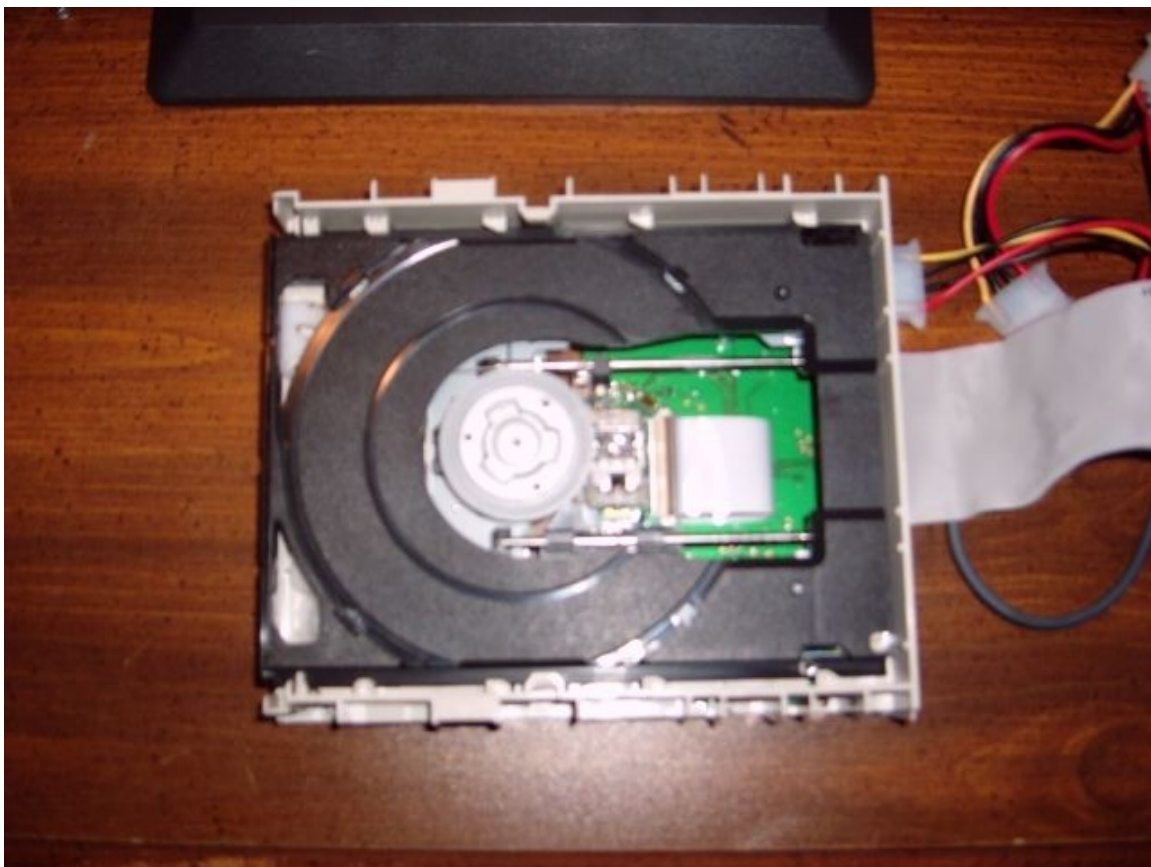
5. Make sure your DVD recorder is selected.
6. Select the Write tab
7. Select your writing speed , 2.4x recommended
8. Hit Start and select your .dvd file



Method 3 – WxRipper

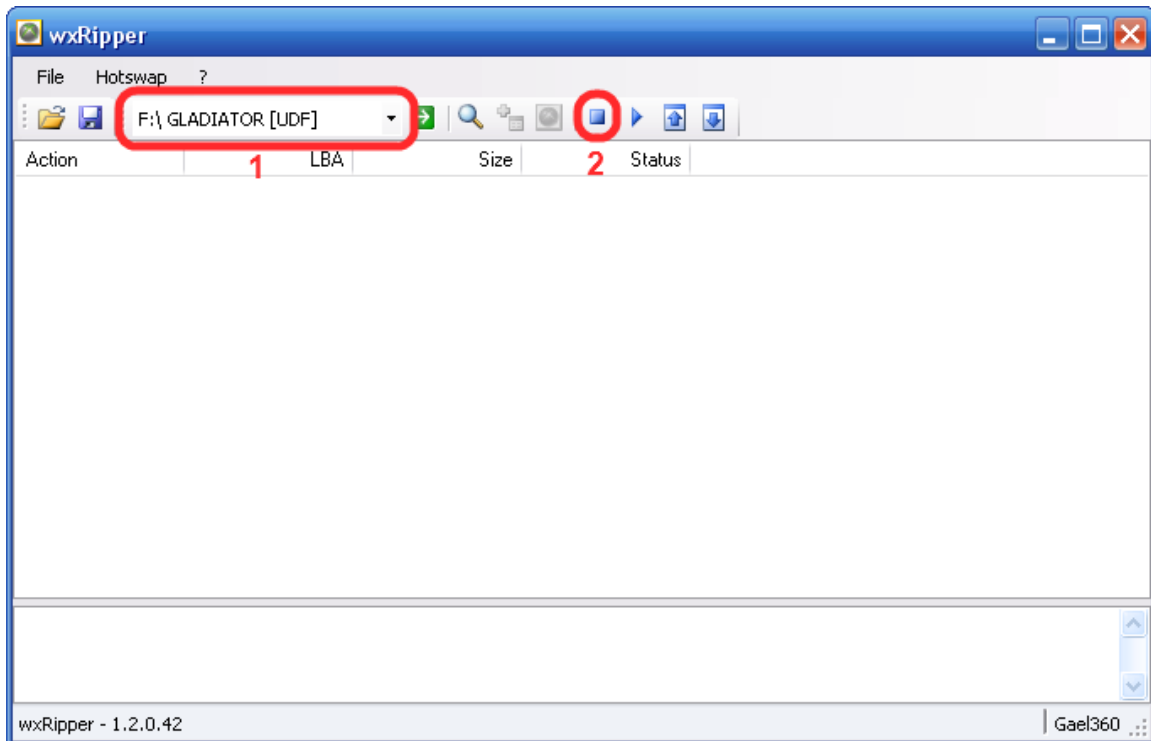
There is another method used to backup Xbox 360 games by hotswapping discs with a normal PC DVD-ROM drive. This method involves hotswapping a large (8gb+) movie DVD with your Xbox 360 game. The reason this is done is because the Xbox 360 discs have a fake table of contents. So, hotswapping and finding the “magic number” offset is the only way to read the real contents of discs. Hotswapping the discs means switching them without actually hitting the eject button on your drive. So, you will have to either use the emergency eject hole on your drive or open the drive up and make it external with the screws off so you can take off the lid.

Here is an example of my setup using a magnet from a drive lid to keep the discs in place.



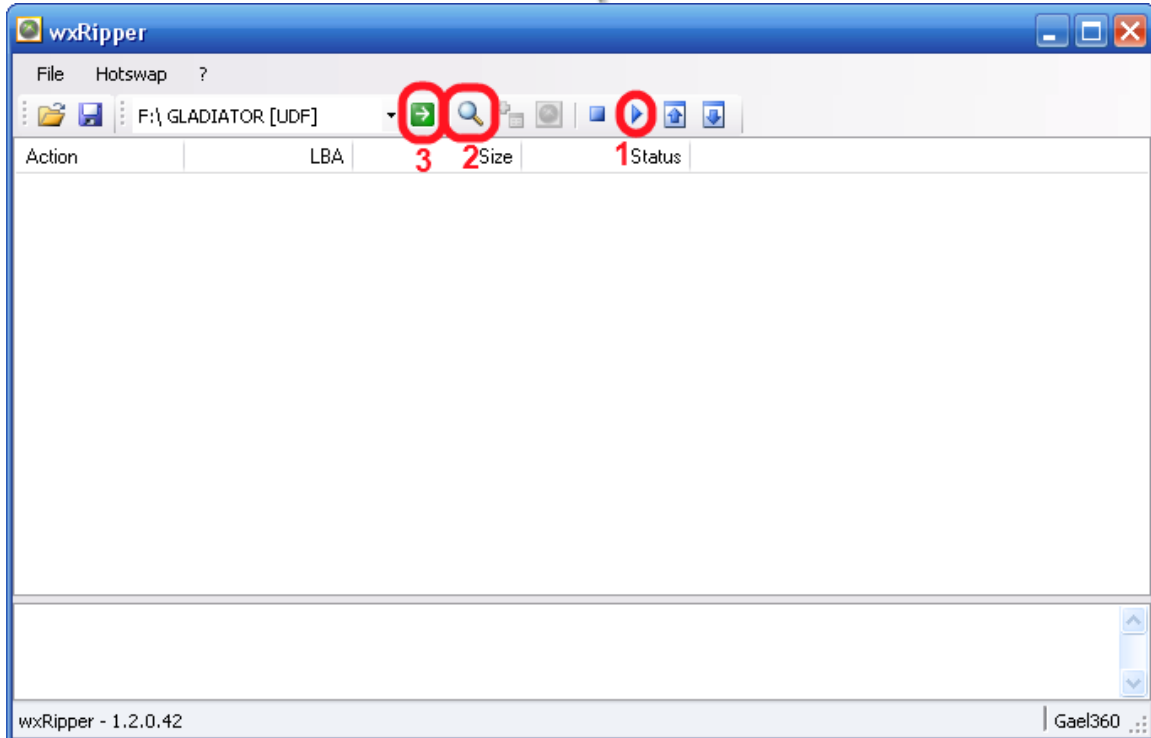
[Download WxRipper 1.2](#)

Insert your large DVD, let it get recognized by Windows, and then close out of any autoruns or installers. Then, open up WxRipper.



1. Make sure your DVD drive is selected
2. Hit the Stop button to stop the disc from spinning

This is when you swap the DVD with your Xbox 360 game. Either use the emergency eject hole or take off the lid and stick in your Xbox 360 game. Make sure you replace the lid completely so the disc will spin correctly.



1. Select the Play button to spin the Xbox 360 disc.
2. Select the magnifying glass to find the magic number.
3. Select the green arrow to start dumping the game.

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



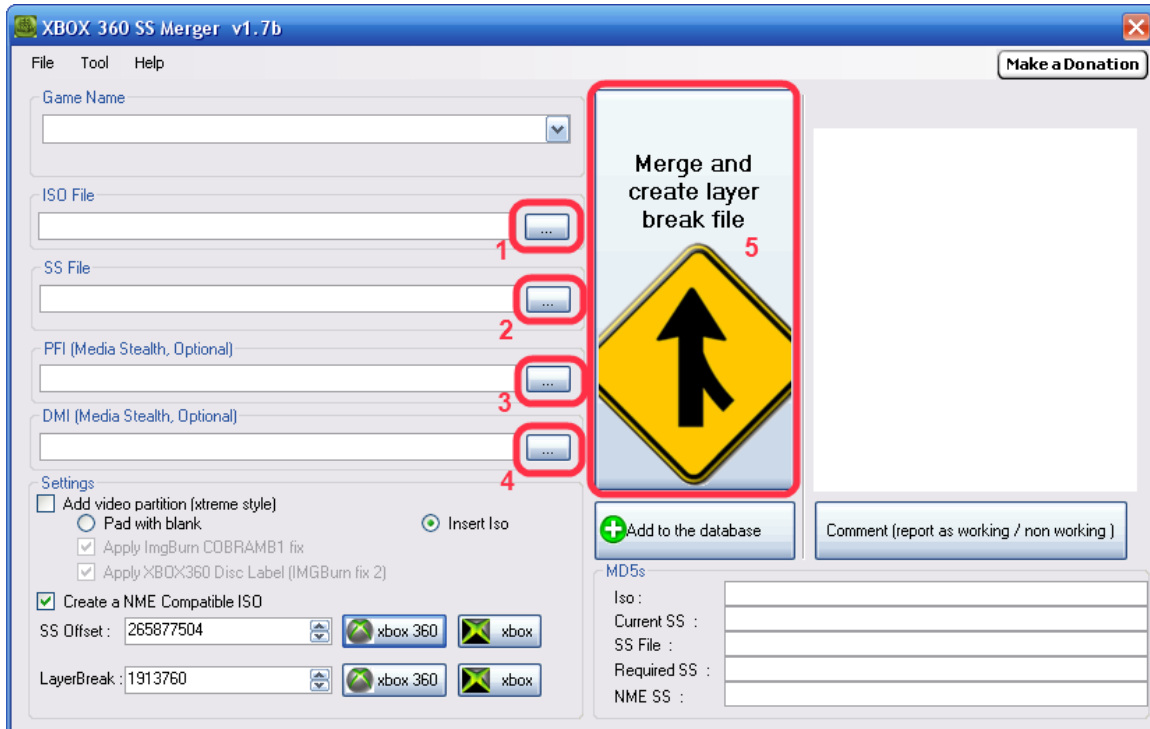
CRC error at 91136, especially on games like Tomb Raider and Hitman, I use this layout (replace first 3 lines with these 4):

- 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)

Patching Your Image

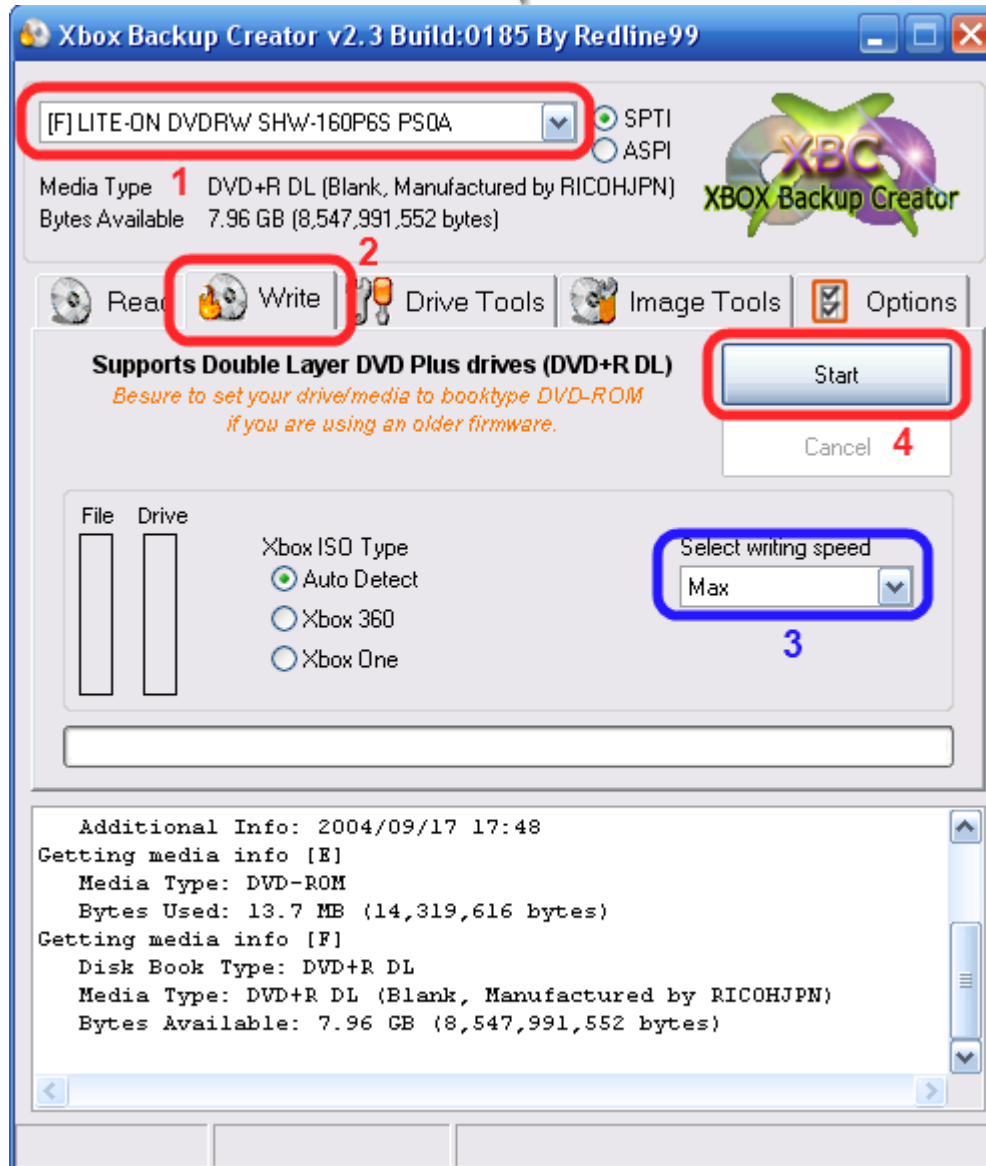
After making the dump with WxRipper, you must inject the security sector, pfi, and dmi files into the image before burning it. To do this, download HellDoc's SS Merger 1.7B.

[Download](#)

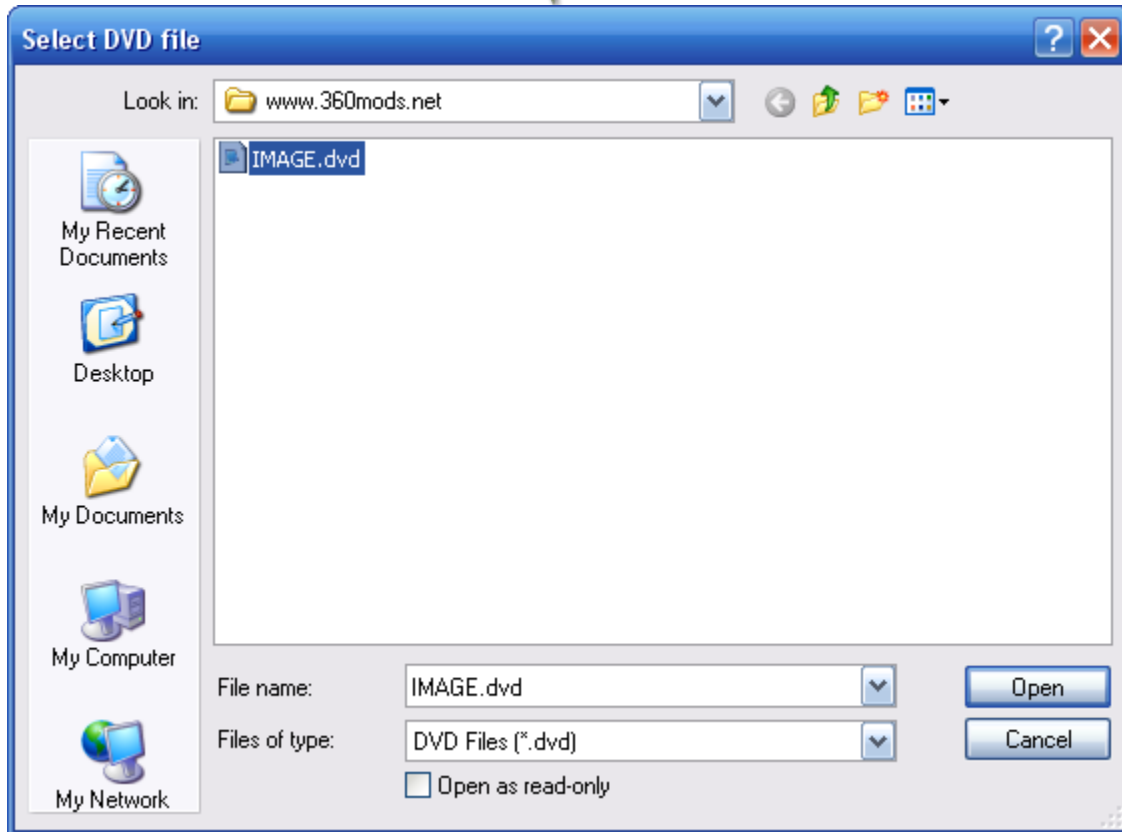


1. Open the ISO you dumped using WxRipper
2. Select the SS file
3. Select the PFI file
4. Select the DMI file
5. Hit the huge merge button to patch the ISO and make a .dvd file.

To burn the game, you can use Xbox Backup Creator.



9. Make sure your DVD recorder is selected.
10. Select the Write tab
11. Select your writing speed , 2.4x recommended
12. Hit Start and select your .dvd file





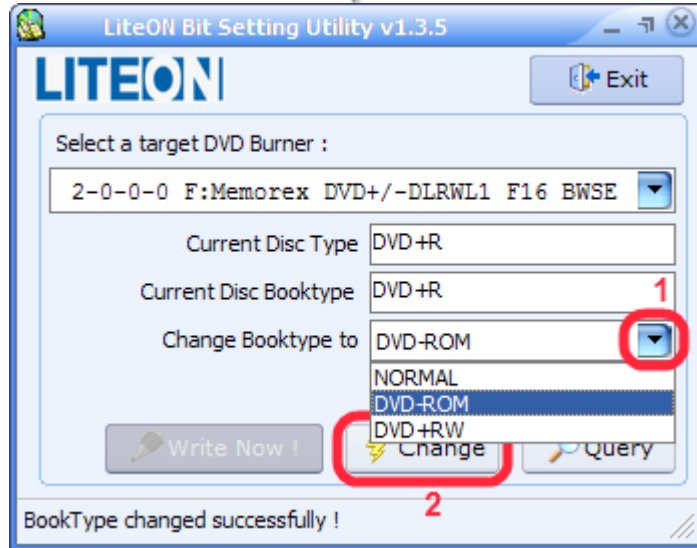
Bitsetting

The latest firmware for both the Xbox 360 Hitachi and Samsung drives does not require bitsetting. For the most part, this is true. But in some cases, bitsetting is still required and it is still recommended, even when using the latest firmware. It only takes a second and if it doesn't cause any problems and may actually help, why not do it?

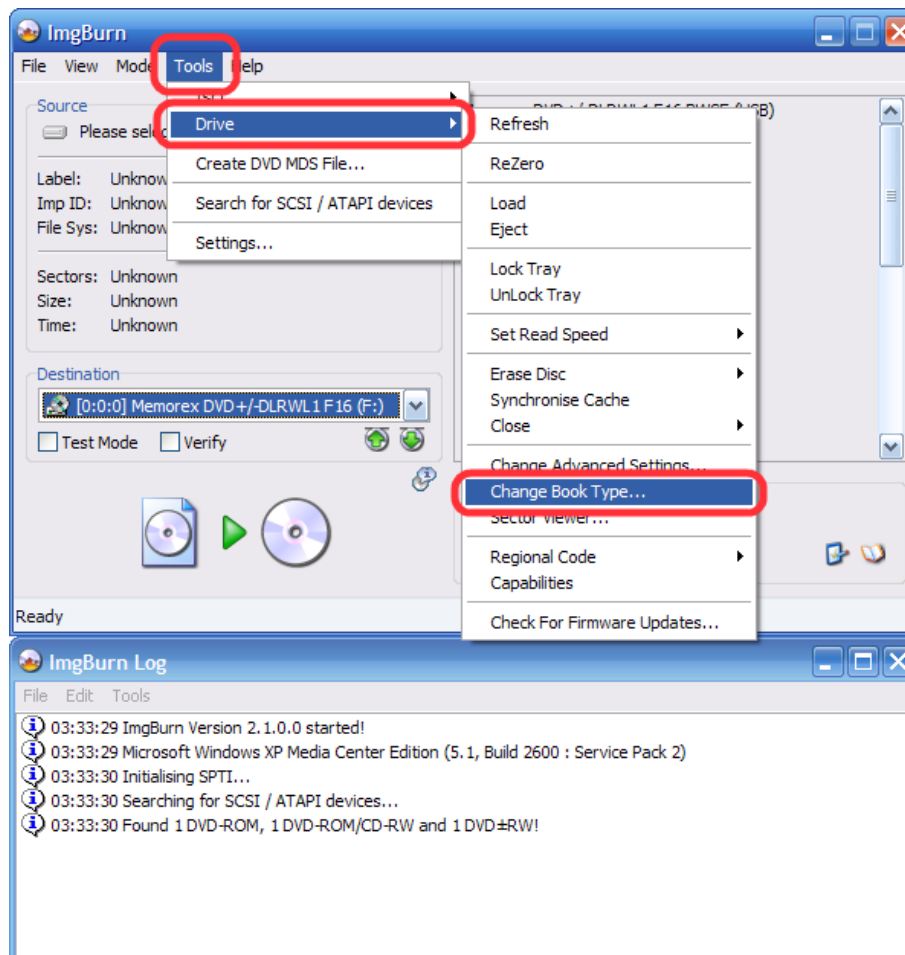
Bitsetting is a standard of the +R DVD format. It allows you set the booktype of your +R and +R DL discs to DVD-ROM for greater compatibility. Since bitsetting/booktyping is dependent on what burner you are using, I can't give you universal instructions that everybody will be able to follow, but I can help.

I would recommend using your favorite search engine such as [Google](#) and search for your dvd burner model number with the terms bitsetting and/or booktype. Just do a little research on your drive. Some drives auto-bitset, some may need a firmware update, some may need to use a specific program, and some may work with IMGBurn alone.

1. Pioneer burners, including the popular Pioneer 111D, are already set to auto-bitset all +R and +R DL media to DVD-ROM. No firmware update is needed, no program, no settings at all. Just burn the discs without messing with anything. They will already be set for you.
2. LiteOn burners enable bitsetting different from other drives. You can use the [LiteOn Bitsetting Utility](#) or IMGBurn to bitset to DVD-ROM. In order to bitset, you must have a blank +R disc already inserted into the drive. Also, if the booktype does not look like it changed, don't worry. Mine doesn't appear to change when I use this, but every burn does end up being DVD-ROM booktype.

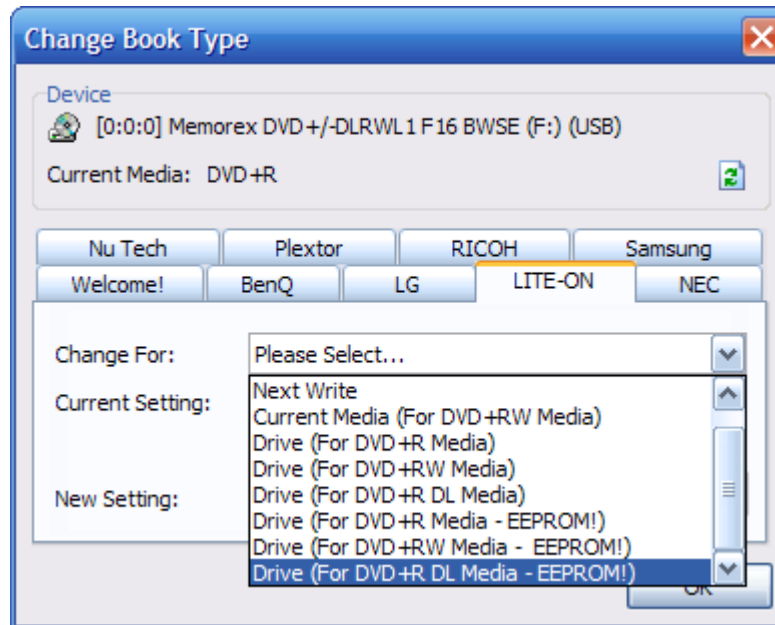


3. For other drives, you can try using [IMGBurn](#). With a +R disc in the drive, open IMGBurn and go to Tools > Drive > Change Booktype.



360MODS

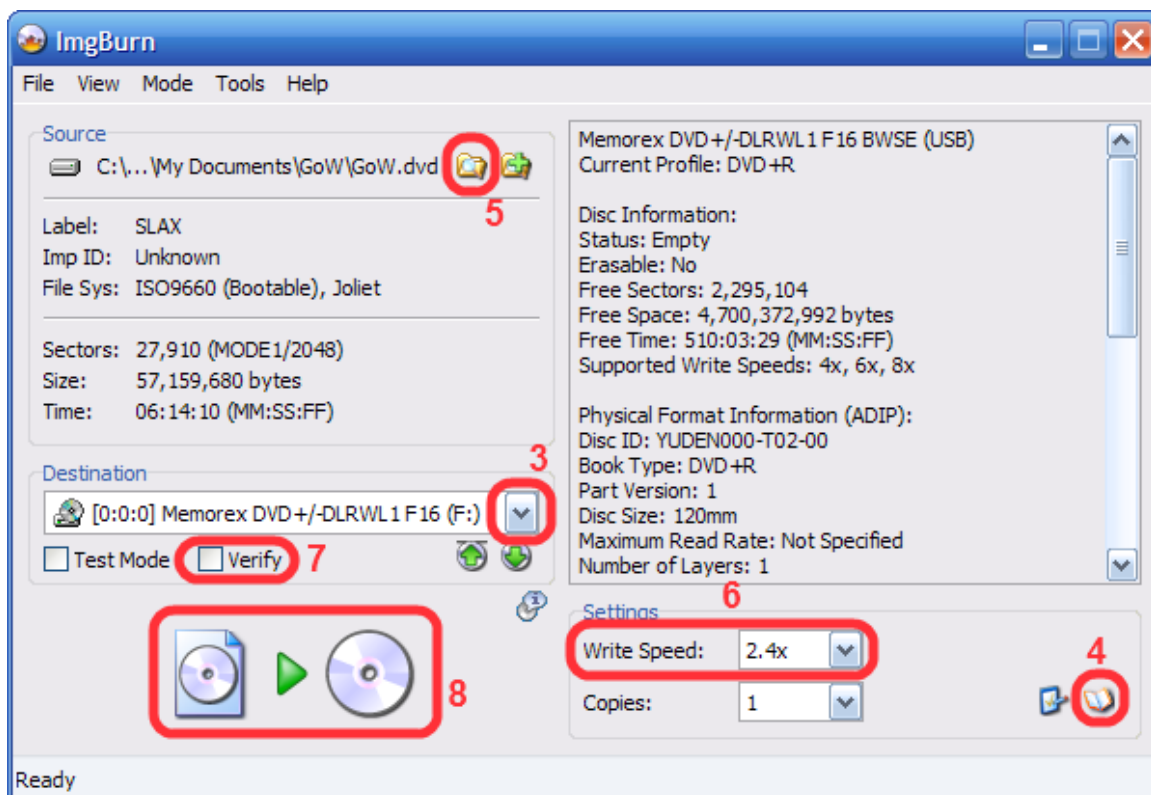
There will be tabs for different types of drives. If you select your drive and it says “Unknown” then you do not have that drive type or your drive does not support bitsetting. As I said earlier, some drives have an updated firmware for bitsetting support. You may notice some settings for “EEPROM.” This will permanently change the bitsetting of the drive, so that it will always set to DVD-ROM, similar to how the Pioneer drives bitset automatically. You will only have to bitset one time if you choose the eeprom option.



Burning Using IMGBurn

You can also burn any backups using IMGBurn. The latest version of IMGBurn supports setting the layerbreak via .dvd files.

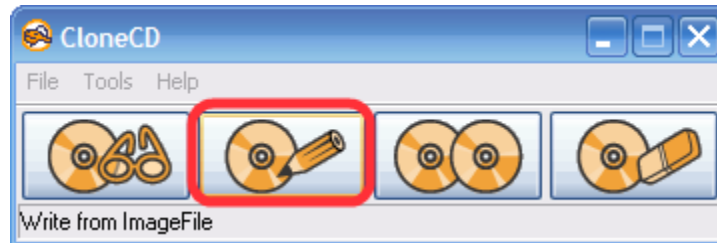
1. Insert your blank DVD+R DL into your burner
2. Open IMGBurn
3. Make sure the destination drive is your burner
4. Change the booktype if necessary
5. Load your .dvd file
6. Set your write speed (2.4x recommended, approximately 45 minutes to burn)
7. Uncheck verify as it is unnecessary and will just add time to the process
8. Burn the image to the disc



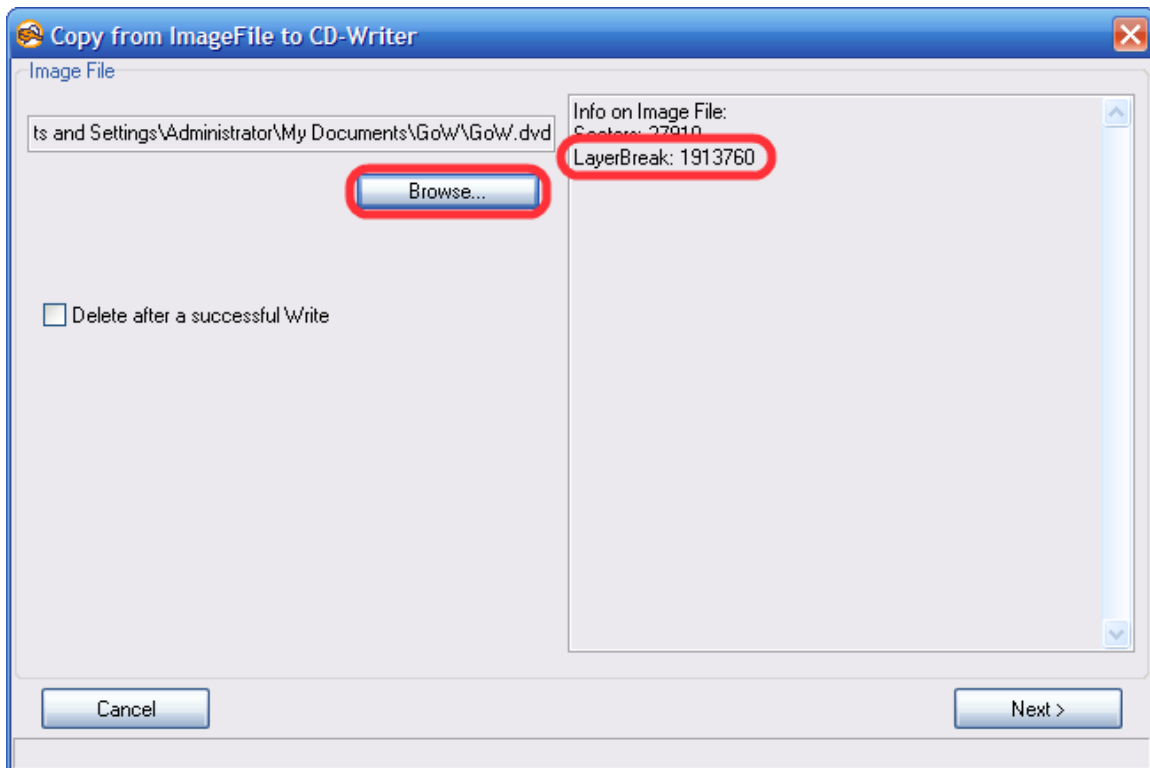
Burning Using CloneCD

CloneCD also supports the custom layerbreak via the .dvd file. To burn using CloneCD:

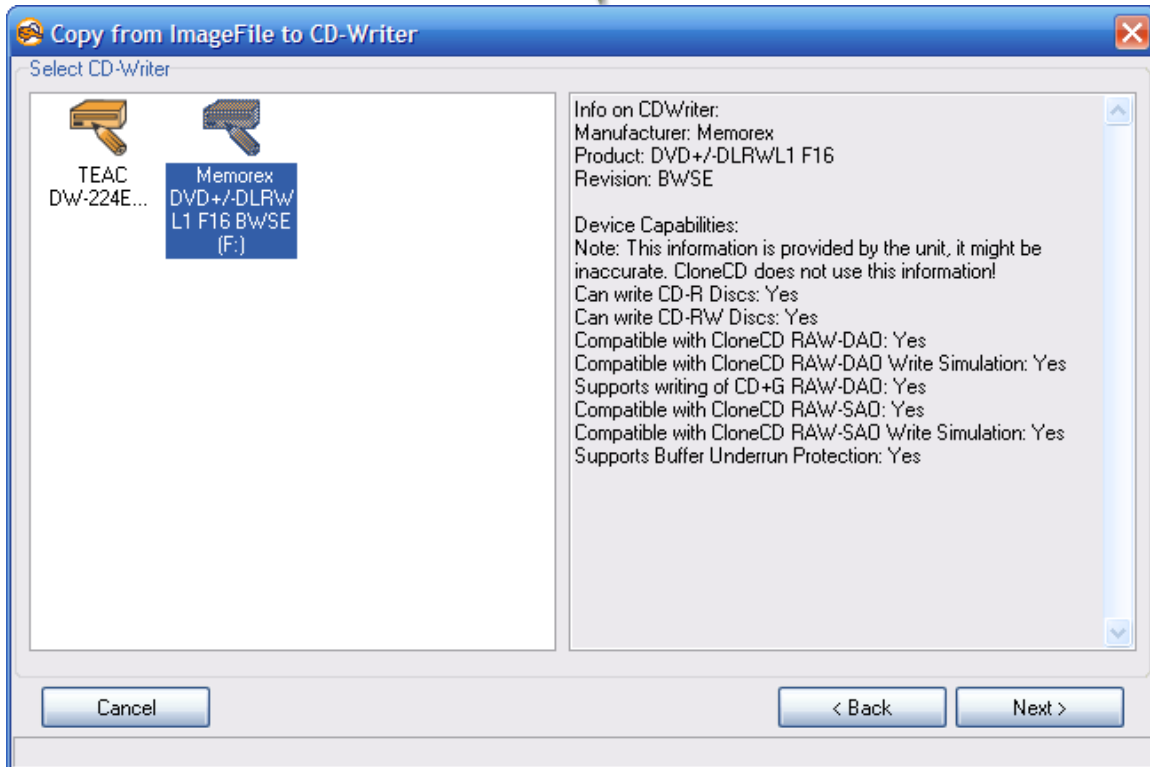
1. Insert your blank DVD+R DL into your burner
2. Open CloneCD
3. Select "Write from image file"



4. Hit the browse button and open your .dvd file. Check to make sure the layerbreak is set to 1913760.



5. Hit next, and select your burner from the list of drives to the left.



6. Hit next again, select your write speed, and then hit Ok to start burning.

