

Philips/BenQ/LiteOn VAD6038 Tutorial



You will need:

- VIA or NForce SATA chipset
- iPrep 101 v006

This method only works with VIA or NForce SATA chipsets, any other chipset requires soldering a switch to the drive and is covered in a 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 decided not to cover opening the Xbox 360 in this tutorial since it is already long enough and there are many other tutorials for opening the Xbox 360. 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. ([See Pic](#))
- In order to push in the back clips, you can do one of two 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. The key would not work for me, it was too flimsy, but it works for some people. You can also purchase an “unlock kit.”
- If all you want to do is just flash the firmware, you only need to remove the six long screws on the bottom. ([See Pic](#))

Read all these guides and watch all the videos, figure out how you want to go about opening the Xbox 360. It is not rocket science.

[Anandtech Guide](#)

[InformIT Guide](#)

[Xbox-Accessories Disassembly](#)

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

[Textbook's Video](#)

[acDC's Video](#)



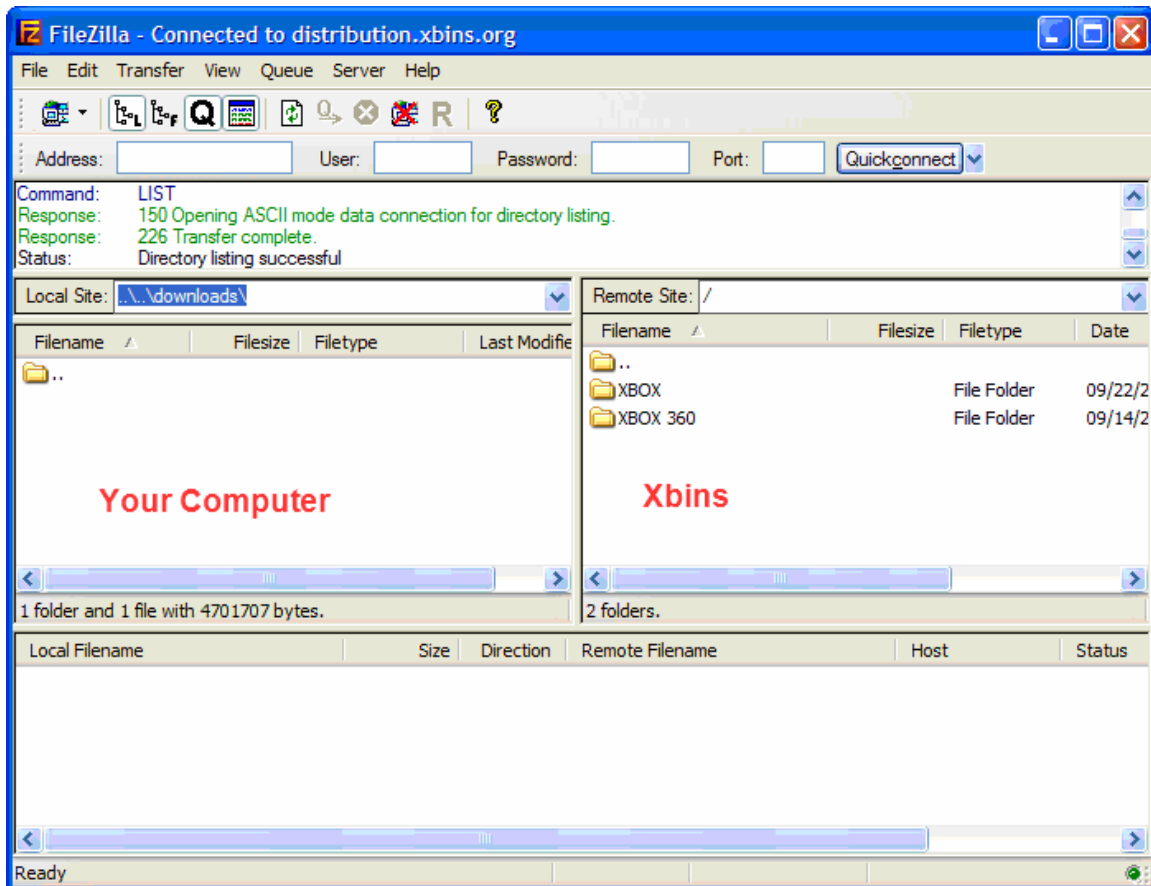
Downloading The Firmware

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 Downloads folder on your left side, and a few folders on your right side (this is the Xbins FTP server).



The hacked firmware can be found in:

/XBOX 360/firmware/hacked firmware/Benq VAD6038/

Simply drag the “BenQ iXtreme v1.1 MultiSpeed_updated_firmtool.rar” file over to the left side of FileZilla and wait for it to finish downloading.



iPrep (USB Flash Drive)

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 iPrep to automatically detect your SATA port, format the USB drive, and copy the required DosFlash and hacked firmware files onto it.

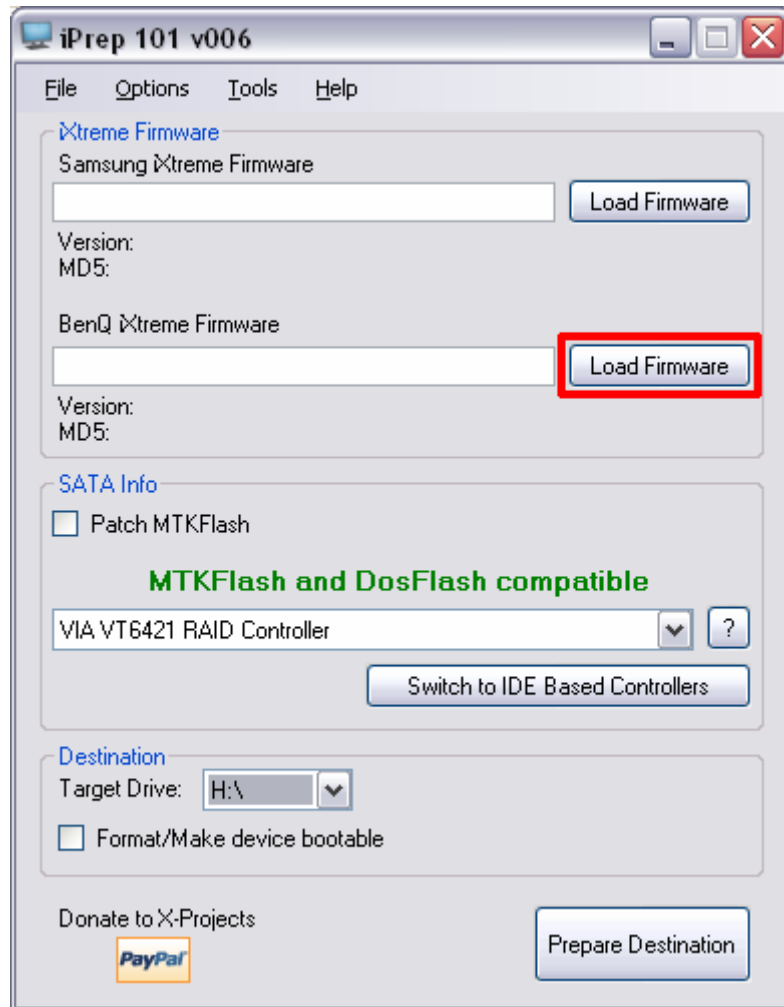
First, you need to make sure [Microsoft .NET Framework v2](#) is installed. It is needed for iPrep to run. If you do not have this installed, you will be prompted to download and install it.

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 latest drivers. The latest drivers for VIA chipsets and Windows XP are [here](#).

Once you have that taken care of, you can download and install iPrep. Klutsh updates iPrep frequently, the latest version is always available on his website at <http://www.x-projects.org> or on xbins in:

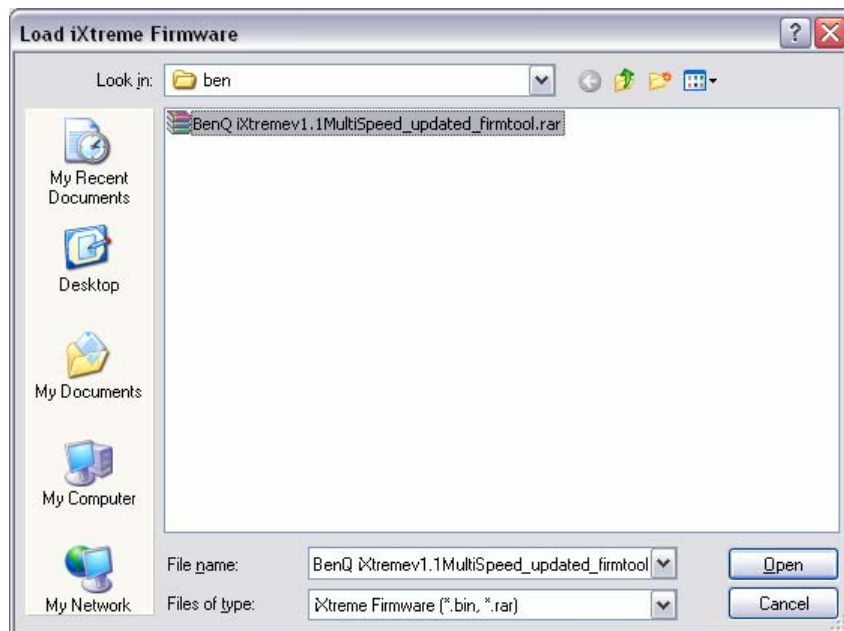
`/XBOX 360/firmware/firmware tools/iPrep 101/`

The download is in the form of a RAR archive. Use WinRAR to extract all the files to a new folder and run the installer to install iPrep.

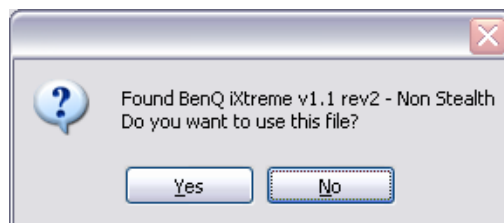


When you hit this button, a “Load iXtreme” window should open for you to browse for the iXtreme firmware. Browse and open the:

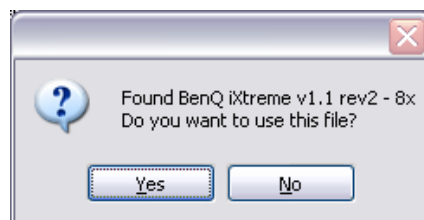
“BenQ iXtremev1.1MultiSpeed_updated_firmtool.rar” file.



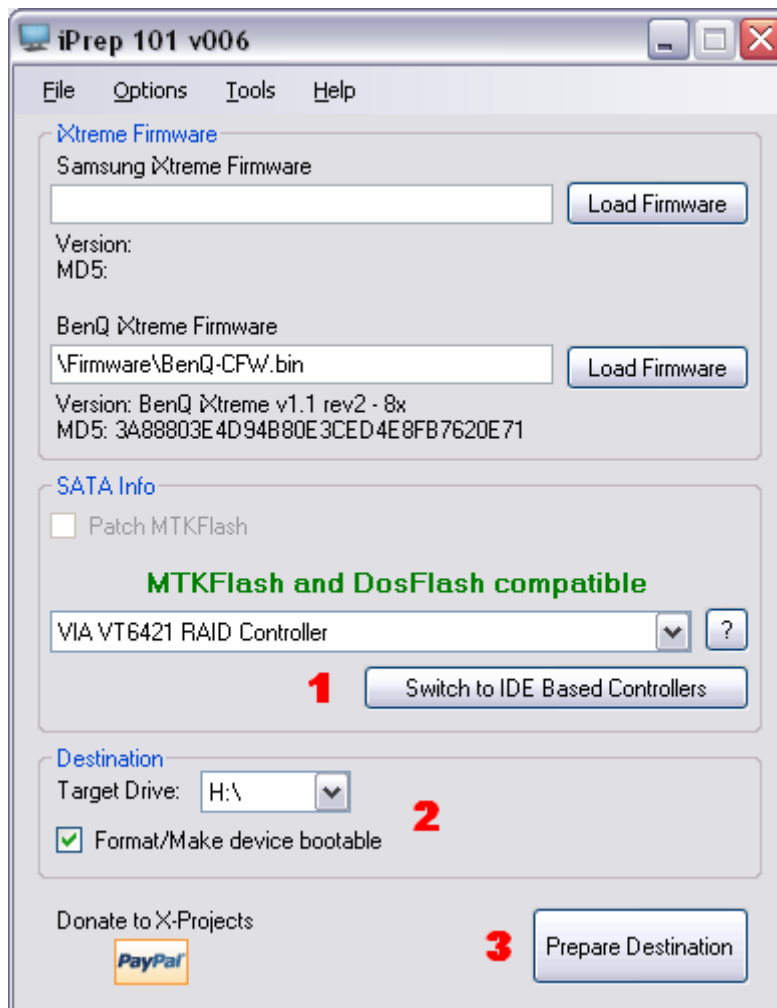
You should then get a series of messages confirming that iPrep has found the iXtreme firmware files inside the rar, the first one will be for the NON-STEALTH version, click No.



iPrep will continue loading the firmware, click Yes to choose the speed that you would like to use. (2x, 5x, 8x, or 12x)



There is no “right” firmware to use here, it is matter of preference. Normal speed is 12x, the slower versions are quieter but the trade-off is longer load times. It’s up to you to choose the one you want or you can simply go with 12x and there will be no change from normal.

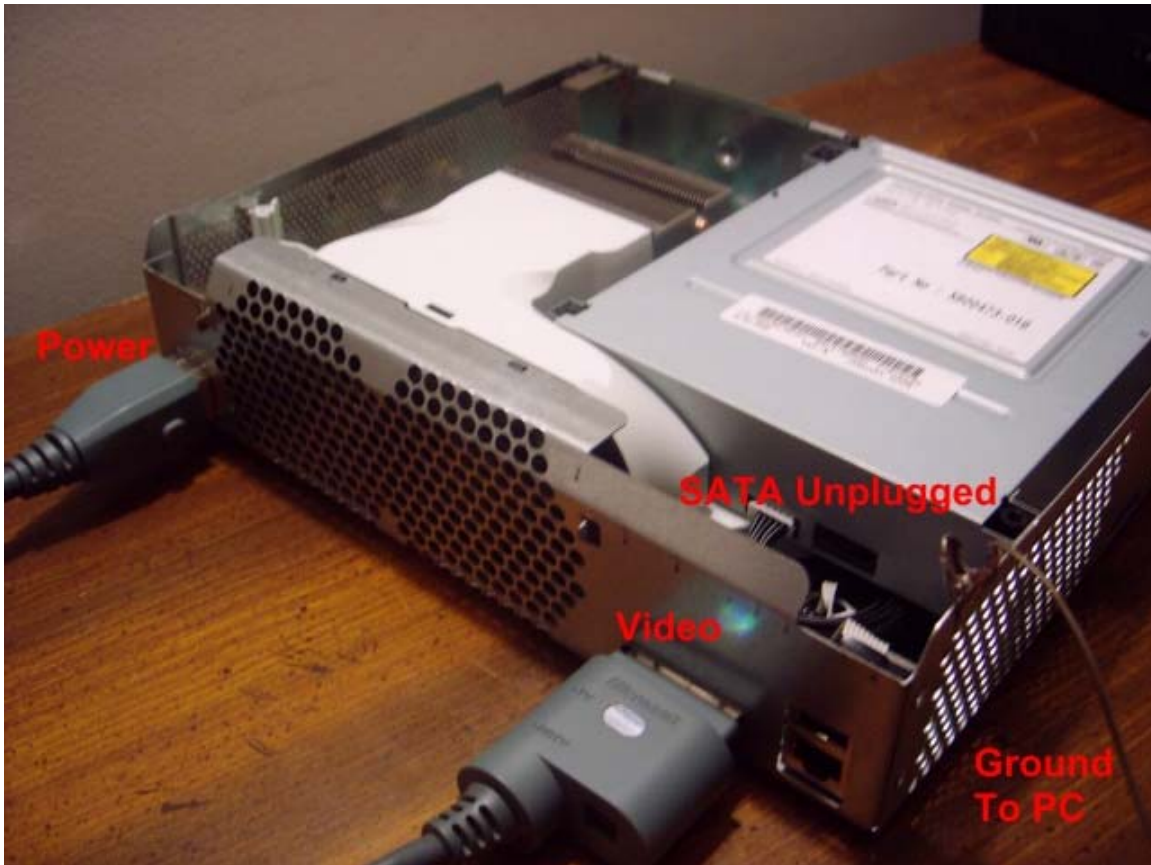


1. Confirm that your SATA chipset is selected in the dropdown menu and that it says “DosFlash compatible”. Click the “Switch to IDE/SCSI Based Controllers” button to redetect chipset(s).
2. Select your USB flash drive from the drop-down list. Check the box to Format the flash drive and make it bootable. *Remember to get any important data off the flash drive first, it will be erased!*
3. Click “Prepare Destination”.

If everything goes smooth you should get a “Preparation Complete” message.

Xbox 360 and PC Connections

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 back of the Xbox 360.





The Xbox 360 uses a floating point ground. Your PC uses a “true earth” ground. This difference can cause excess voltage to travel through your SATA cable and potentially damage your Xbox 360 DVD drive or PC Motherboard / SATA card. You can solve this problem by connecting the Xbox 360’s ground to the PC’s ground. The easiest way to do this is by using a “croc clip wire” and connecting the Xbox 360 metal casing to your PC’s metal case. You can use anything conductive to connect the Xbox 360 case is connected to the PC case. You don’t have to use croc clips, you could just tape some bare/stripped wire to each, or even set the Xbox 360 next to the PC so that they are touching.

Many people have flashed their drives completely ignoring this recommendation. The possibility of damaging something by ignoring this step is rare, but still possible. So, you could say grounding the PC and 360 together isn’t absolutely necessary, but it is recommended. If you have the ability to do so, it is safest to take the time to do it.

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

Reading The Original Firmware

Connect the SATA cable from the 360 to your PC / SATA card, then turn on your PC and boot from the USB flash drive into DOS. The Xbox 360 should still be off at this point.



Enter Y to accept the iPrep Terms of Use.

```
-----  
iPrep Boot Disk v0.0.5                                     [x-projects.org]  
-----  
This iPrep Boot Disk is a collection of MSDOS applications that allow you to  
re-flash an Xbox 360s Samsung and/or BenQ DUD drive.  
The Disk cannot be used for any other type of DUD drive.  
*****  
***      DISCLAIMER: ANY USE OF THIS PROGRAM IS YOUR OWN RISK      ***  
*****  
X-Projects take no responsibility for any damage that may be caused  
to your PC/Xbox 360 through the use these scripts/programs.  
Do you agree? [Y/N]  
y
```



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)

dBen 1234567 12345 [press enter]

```
-----  
iPrep Boot Disk v0.0.5  
-----[x-projects.org]-----  
  
BenQ Usage:  
  To read Firmware and make a hacked Firmware ready for flashing:  
  dBen 7-digit serial 5-digit serial  
  e.g. dBen 1234567 61005  
  
  To flash Firmware:  
  fBen 7-digit serial 5-digit serial  
  e.g. fBen 1234567 61005  
  
Samsung Usage:  
  To read Firmware and make a hacked Firmware ready for flashing:  
  dSam 7-digit serial 5-digit serial  
  e.g. dSam 1234567 61005  
  
  To flash Firmware:  
  fSam 7-digit serial 5-digit serial  
  e.g. fSam 1234567 61005  
  
H:\>dben 1234567 12345
```

Follow the prompts on the screen, make sure your 360 is OFF and press any key to continue. Press Y to resend the MTK Vendor Intro.

```
#####  
Ensure your BenQ DVD drive is turned OFF  
Press any key to continue . . .  
#####  
For the following steps, you need to:  
Press YES to resend the MTK vendor intro command  
Turn ON the drive, wait for status to change to D1  
turn OFF the drive for 2 seconds  
Turn ON the drive, reading should start  
MTK Vendor Intro failed on port 0xCC00. If you choose to resend the command  
you should turn the drive off and on after you pressed "Yes".  
Do you want to resend the command until the drive responds <Y/N)? y
```

360MODS

- Turn on the Xbox 360 and wait 2 or more seconds, status toggles between 0x51 and 0xD1.
- Turn off the Xbox 360 and wait 2 or more seconds, status will stay at 0xD1.
- Turn on the Xbox 360, you should get a good drive status 0x73 and reading should begin automatically.

All 4 banks should read OK and you should get a "Reading finished!" message with a Datasum.

```
MTK Vendor Intro failed on port 0xCC00. If you choose to resend the command
you should turn the drive off and on after you pressed "Yes".
Do you want to resend the command until the drive responds (Y/N)? y
Status 0x73
Reading Bank 0...OK!
Reading Bank 1...OK!
Reading Bank 2...OK!
Reading Bank 3...OK!
Reading finished! Datasum: 8216
```

Firmtool will then run automatically to create the hacked firmware...

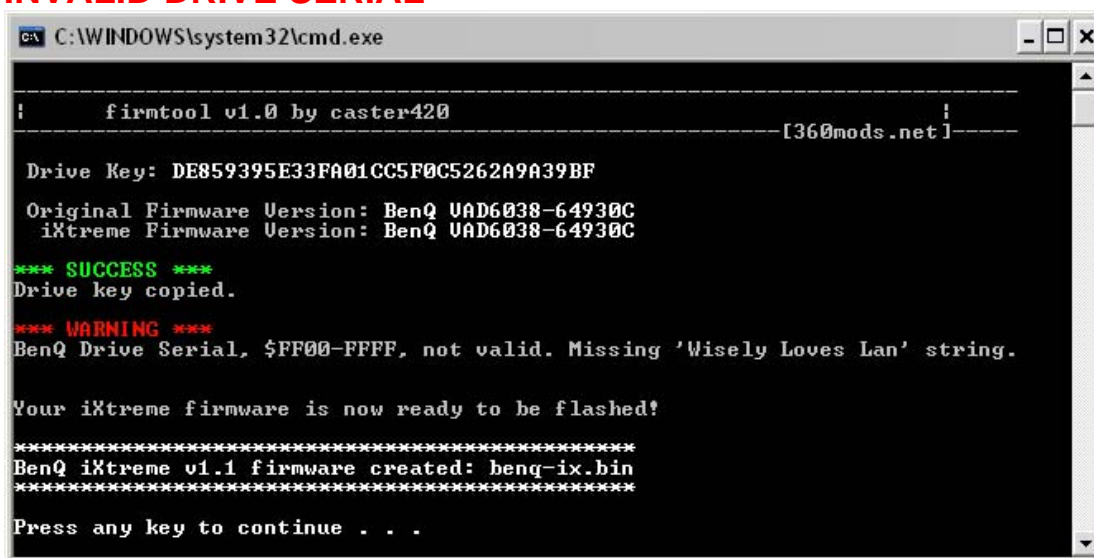
```
-----
|          firmtool v1.1 by caster420          |
|-----[360mods.net]-----|
Drive Key: 1517BF23FC8E64157E12B18C9A622D53
Original Firmware Version: BenQ UAD6038-64930C
iXtreme Firmware Version: BenQ UAD6038-64930C
*** SUCCESS ***
Drive key copied.
Drive serial copied.
Your iXtreme firmware is now ready to be flashed!
Ready to run fBen 1234567 12345
```

If you get a **green success** message from Firmtool power off the 360 and proceed to the flashing page. If you get any **red error** messages **DO NOT** proceed with flashing.

Firmtool Errors

Sometimes there are problems. If your firmware dump is not the correct size, does not contain a valid key, or does not contain a valid drive version, FirmTool will abort. If you get something like any of these pictures, **DO NOT PROCEED WITH FLASHING!** Doing so may brick your Xbox 360 and leave you without a valid drive key. Something is wrong. Make sure you have unplugged all other drives in your PC and try starting this tutorial over again.

INVALID DRIVE SERIAL



```
C:\WINDOWS\system32\cmd.exe

-----
|      firmtool v1.0 by caster420                                     |
-----[360mods.net]-----

Drive Key: DE859395E33FA01CC5F0C5262A9A39BF
Original Firmware Version: BenQ UAD6038-64930C
iXtreme Firmware Version: BenQ UAD6038-64930C

*** SUCCESS ***
Drive key copied.

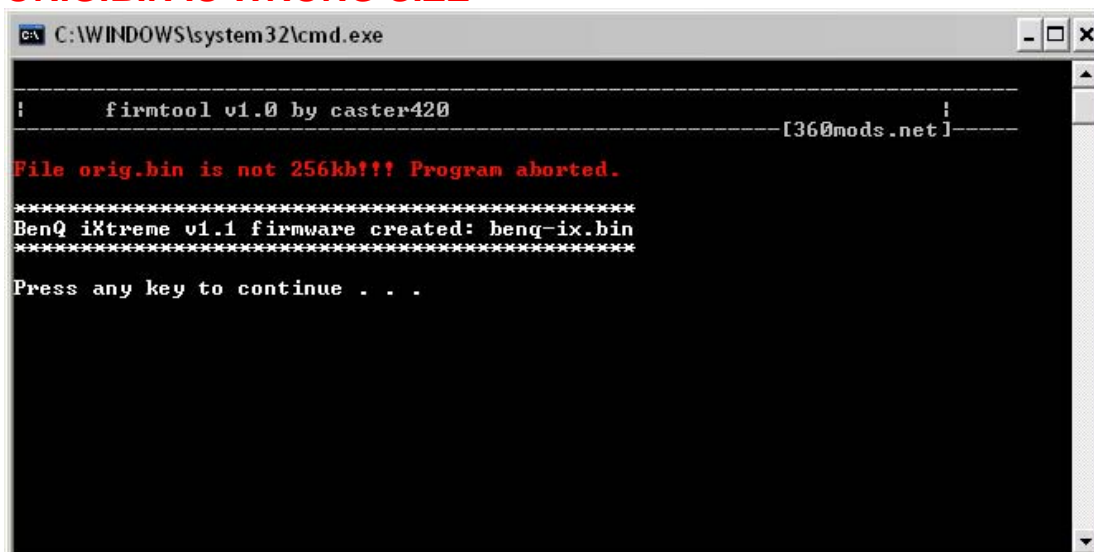
*** WARNING ***
BenQ Drive Serial, $FF00-FFFF, not valid. Missing 'Wisely Loves Lan' string.

Your iXtreme firmware is now ready to be flashed!

*****
BenQ iXtreme v1.1 firmware created: benq-ix.bin
*****

Press any key to continue . . .
```

ORIG.BIN IS WRONG SIZE



```
C:\WINDOWS\system32\cmd.exe

-----
|      firmtool v1.0 by caster420                                     |
-----[360mods.net]-----

File orig.bin is not 256kb!!! Program aborted.

*****
BenQ iXtreme v1.1 firmware created: benq-ix.bin
*****

Press any key to continue . . .
```

NO VALID KEY IN ORIG.BIN



```
C:\WINDOWS\system32\cmd.exe

-----
|          firmtool v1.0 by caster420          |
-----[360mods.net]-----

*** No valid key found in orig.bin! ***

Here is a brief explanation of the valid key not found error...

Key Check locates the key by comparing the all bytes of the key against
the other bytes in the 16 byte key. If there are more than 6 identical
bytes in the 16 byte key, it moves to the next logical key location in
key block. If all of the key locations have more than 6 identical
bytes, then it will respond with a valid key not found.

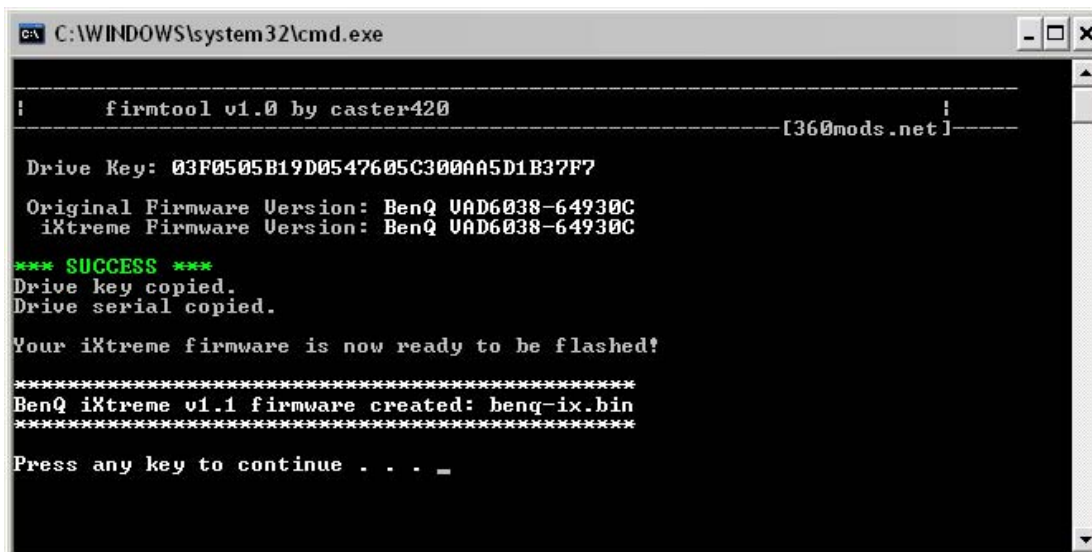
firmtool also checks the key place holders of Samsung firmware. If
there is an incorrect byte in these place holders, it will also result
in this error.

Please check the key range of orig.bin.

Key block not copied - ABORTING!!!
```

Again, your screen should match the screenshot below before proceeding:

FIRMTOOL SUCCESS



```
C:\WINDOWS\system32\cmd.exe

-----
|          firmtool v1.0 by caster420          |
-----[360mods.net]-----

Drive Key: 03F0505B19D0547605C300AA5D1B37F7

Original Firmware Version: BenQ UAD6038-64930C
iXtreme Firmware Version: BenQ UAD6038-64930C

*** SUCCESS ***
Drive key copied.
Drive serial copied.

Your iXtreme firmware is now ready to be flashed!

*****
BenQ iXtreme v1.1 firmware created: benq-ix.bin
*****

Press any key to continue . . . _
```



Flashing The Hacked Firmware

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)

fBen 1234567 12345 [press enter]

```
H:\>fben 1234567 12345
#####
Ensure your BenQ DUD drive is turned OFF
Press any key to continue . . .
#####
For the following steps, you need to:
Press YES to resend the MTK vendor intro command
Turn ON the drive, erasing should start
If status starts to change between D1 and 51, turn OFF drive for 2 seconds,
then turn ON the drive, erasing should start
MTK Vendor Intro failed on port 0xCC00. If you choose to resend the command
you should turn the drive off and on after you pressed "Yes".
Do you want to resend the command until the drive responds (Y/N)? y
```

Follow the prompts on the screen, make sure your 360 is OFF and press any key to continue. Press Y to resend the MTK Vendor Intro.

- Turn on the Xbox 360 and wait 2 or more seconds, status toggles between 0x51 and 0xD1.
- Turn off the Xbox 360 and wait 2 or more seconds, status will stay at 0xD1.
- Turn on the Xbox 360, you should get a good drive status 0x73 and erasing should begin automatically.

```
MTK Vendor Intro failed on port 0xCC00. If you choose to resend the command
you should turn the drive off and on after you pressed "Yes".
Do you want to resend the command until the drive responds (Y/N)? y
Status 0x73
Erasing...OK!
Erasing finished!
```



You will then see this screen which tells you to power OFF the 360:

```
#####  
Ensure your BenQ DUD drive is turned OFF  
Press any key to continue . . .  
#####
```

IMPORTANT! You must power the 360 back ON before pressing any key to continue.

If you press any key to continue with the 360 powered OFF (as instructed to do on screen) it will immediately freeze attempting to write Bank 0. This is a bug in iPrep 006 and will hopefully be resolved in a future release.

So power the 360 OFF, wait a few seconds, power it ON, wait a few seconds, then press any key to continue.

```
#####  
Ensure your BenQ DUD drive is turned OFF  
Press any key to continue . . .  
  
#####  
For the following steps, you need to:  
Press YES to resend the MTK vendor intro command  
Turn ON the drive, flashing should start  
Writing Bank 0...OK!  
Writing Bank 1...OK!  
Writing Bank 2...OK!  
Writing Bank 3...OK!  
Writing finished! DataSum: 8216
```

Writing should begin as soon as you press any key to continue with the 360 already powered ON. All 4 banks should write OK and you should get a "Writing finished!" message with a Datasum.



Additional Notes

- If you are using a PCI card with more than one port, use the internal port closest to the front of the PC tower.
- There have been reports of iPrep detecting and using the wrong port, it seems to be limited to Vista users. If you're sure you're doing everything in this tutorial correctly but reading stays frozen at 0x80 or 0xFF and you're using Vista this may be the problem. If so it is recommended to boot into DOS and try running DosFlash16 in auto mode. To do this boot using the iPrep USB you already made and when you reach DOS type:

cd tools

This changes to the **Tools** directory on the USB, which is where DosFlash is. Then type:

dosflash

- When flashing manually, the erase command is different in DosFlash 1.3 and 1.4. DosFlash 1.3 uses a sector erase while 1.4 uses a chip erase. The commands are as follows:

DosFlash 1.3

```
DosFlash e xxxx 1 a0 1 4 D8 0
```

DosFlash 1.4

```
DosFlash e xxxx 1 a0 1 4 C7 0
```

xxxx is your correct port

This only applies when flashing manually following the DosFlash readme or the manual tutorial [here](#). As Schtrom notes in the readme, try 1 at the end of the command if 0 doesn't work.