

Philips/BenQ/LiteOn VAD6038 Tutorial



You will need:

- VIA or NForce SATA chipset
- DosFlash 1.3
- Bootable DOS disk

**** IMPORTANT! **** 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](#).

This tutorial will cover using DosFlash16 in manual mode from a USB DOS boot disk.



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](#)



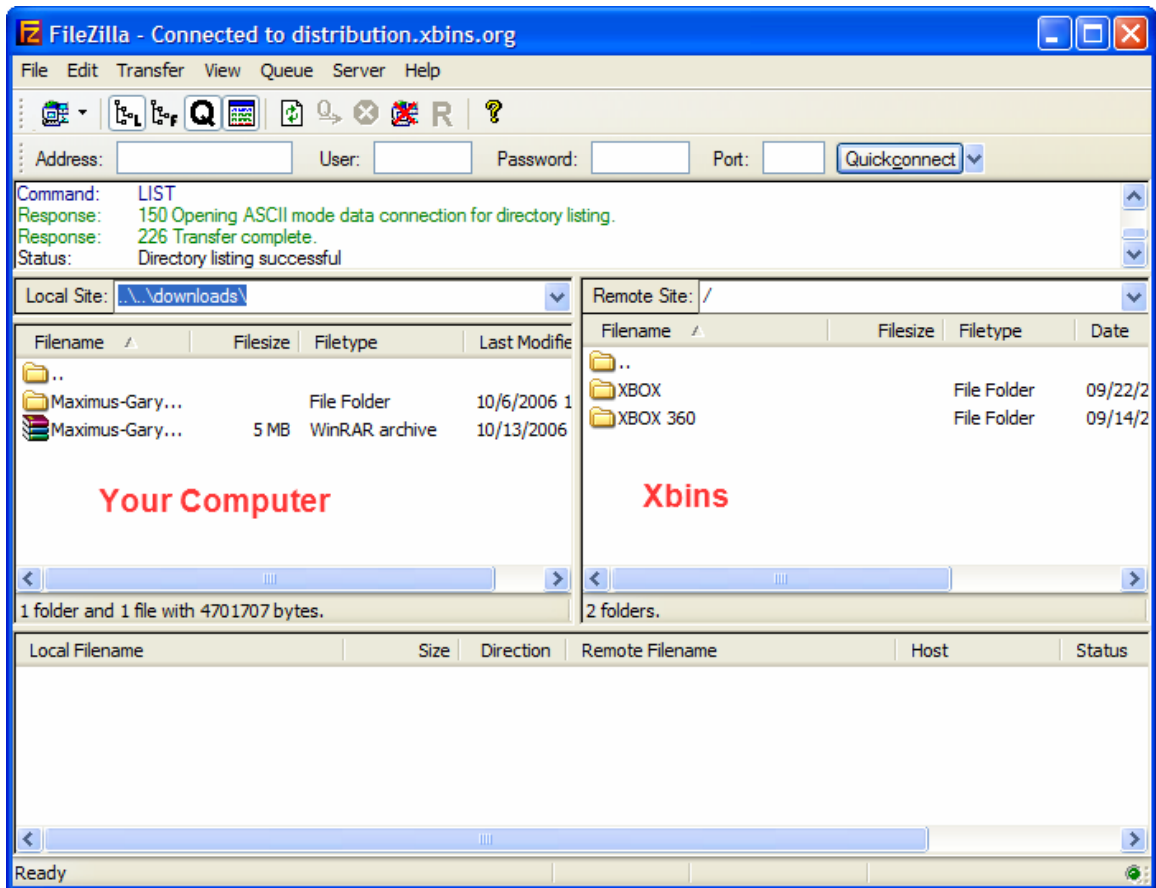
Downloading The Firmware

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.rar” file over to the left side of FileZilla and wait for it to finish downloading. Use WinRAR to extract the BenQ iXtreme v1.1.rar files to a new folder.



iPrep

We will use iPrep for 2 things:

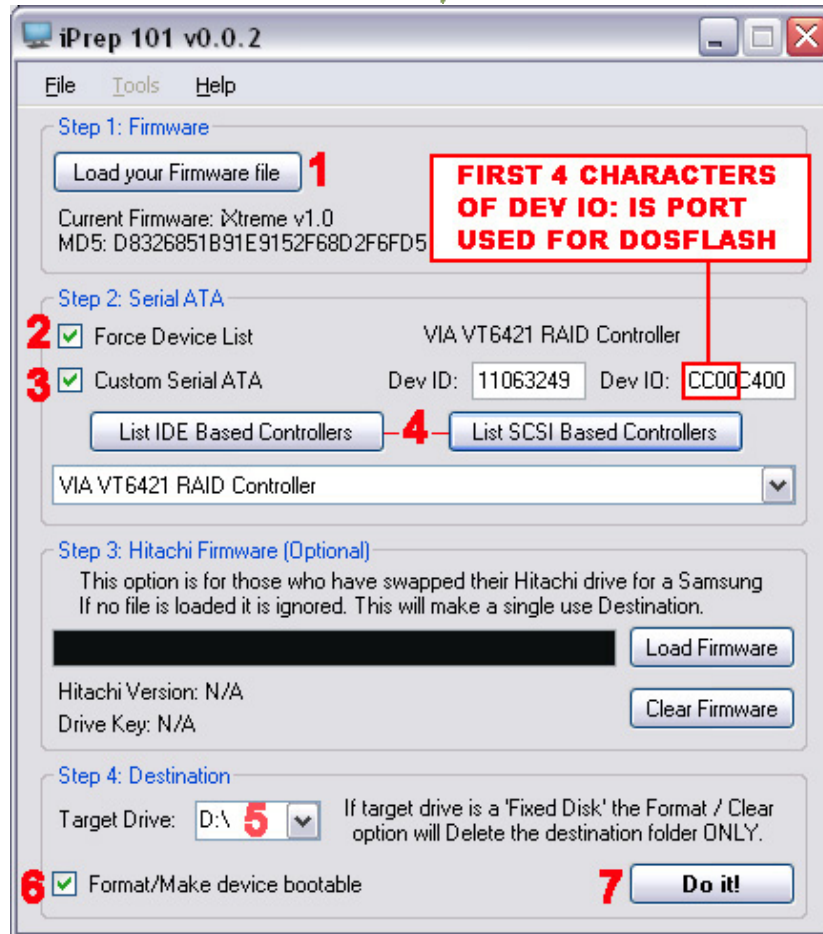
1. Detect SATA and note required port for DosFlash16.
2. Create bootable USB DOS disk.

Floppies will work but are not recommended due to their unreliability. You can also use the NTFS4DOS method instead of a bootable USB drive, that process is covered [here](#). Simply add DosFlash16 to the folder that iPrep creates on your harddrive before booting with the NTFS4DOS CD.

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 XP and VIA chipsets are [here](#).

Once you have that taken care of, you can download and install iPrep. Klutsh updates iPrep frequently, so please visit the website at <http://www.x-projects.org> to download the latest version. The download is in the form of a RAR archive. Use WinRAR to extract all the files to a new folder, then launch iPrep from that folder.



1. Load any Samsung iXtreme firmware. This is not the firmware we will be flashing, iPrep simply requires that a valid firmware file is loaded before it will format a drive and make it bootable.
2. Force Device List should already be checked, just make sure it is.
3. Check the box for Custom Serial ATA.
4. Hit either of the list buttons and select your SATA controller from the drop-down list. It should input the ID and IO values in the textboxes above. **** Note the first 4 characters of your Dev IO: field, this will be the port you need to use in DosFlash! ****
5. Select your USB flash drive from the drop-down list.
6. 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!
7. Click Do it!

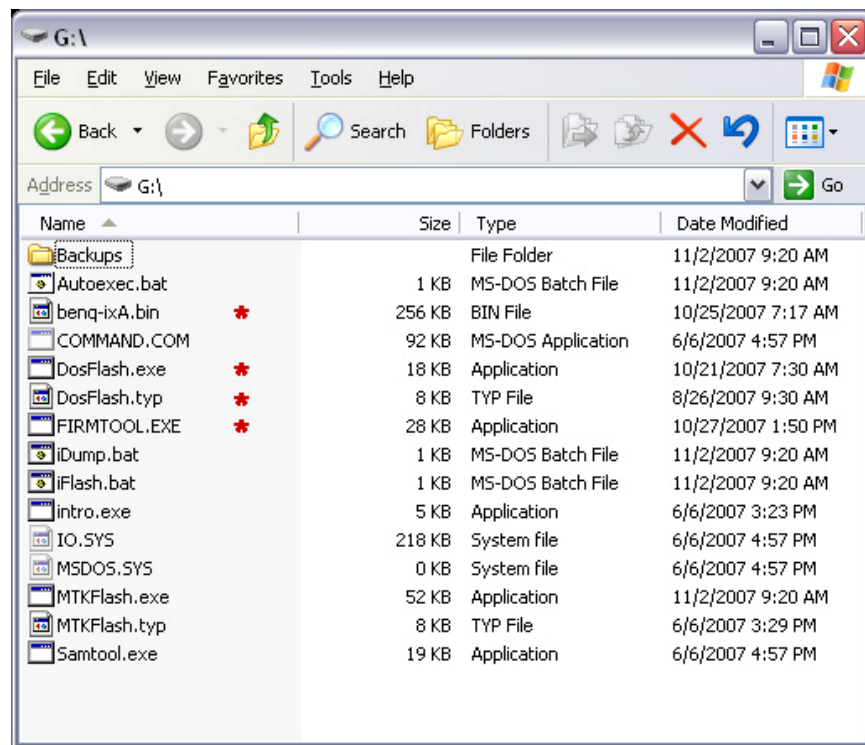


Once the format is complete, copy the DosFlash.exe and DosFlash.typ files from the DosFlash16 folder to the root of the USB drive you just formatted.

You have 2 options for creating hacked firmware, both use the same program and will yield the same results so it's a matter of preference.

1) Use Firmtool directly in DOS (optional)

This allows you to run Firmtool from DOS immediately after dumping your orig.bin. To do so, you must copy Firmtool.exe and the BenQ iXtreme file of your choice (Fast or Quiet) to the root of the bootable USB drive you created. If you choose to do it this way your USB drive should match the screenshot below, files that need to be added manually are marked with a red asterisk.



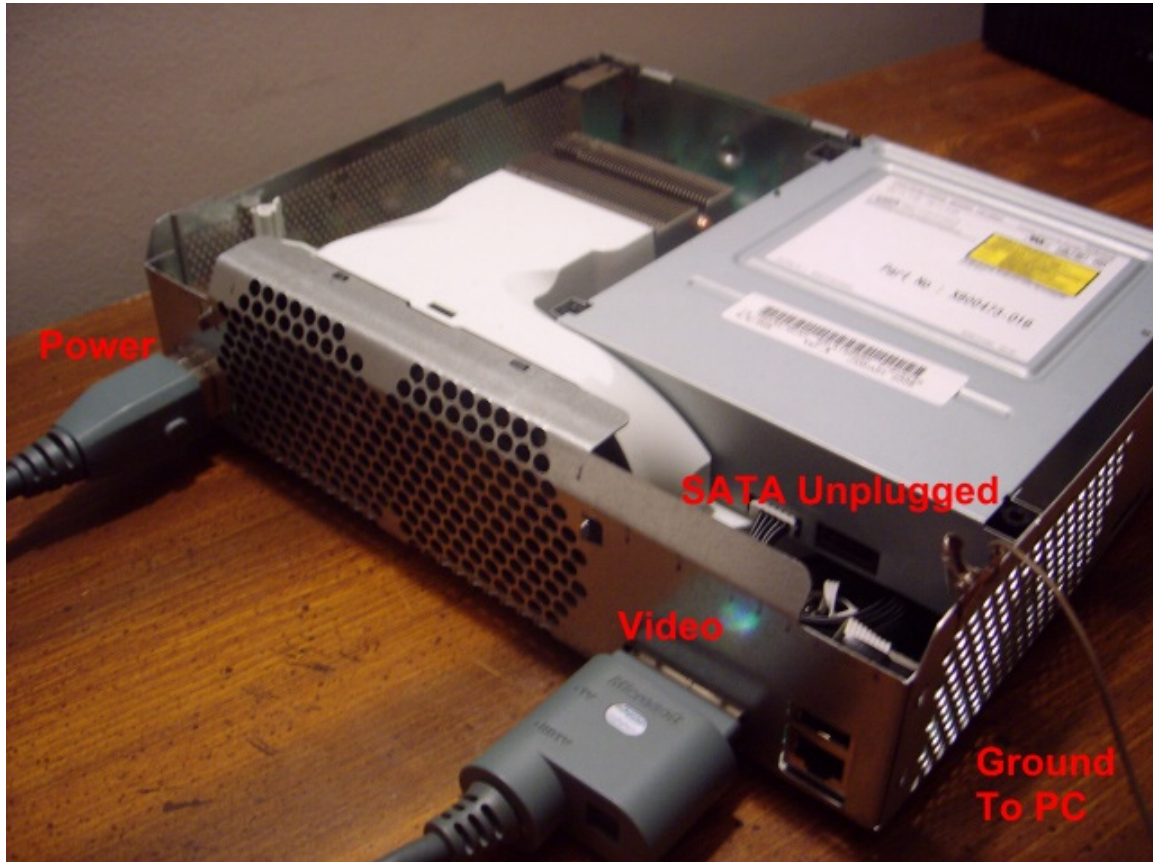
2) Use "Make iXtreme firmware" batch file in Windows

This requires no additional files on the USB as you will boot into Windows to create your hacked firmware after dumping.



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



Type in the following command, using your 4 digit port that you got from iPrep in place of xxxx.

```
DosFlash r xxxx 1 a0 1 4 orig.bin 0
```

Note the spaces, they are very important. Put a space wherever you see an underscore below. DO NOT type the underscores in DOS, they are just for your reference here and to make the spaces easier to see.

```
DosFlash_r_xxxx_1_a0_1_4_orig.bin_0
```



[press enter]

DosFlash16 will ask you if you want to resend the MTK Vendor Intro command, enter Y for Yes. When you hit enter the drive status is shown on the screen, it's something like 0x7F, this will change during the next few steps.

```
C:\>dosflash r CC00 1 a0 1 4 orig.bin 0
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: 0x7F
```

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.

```
C:\>dosflash r CC00 1 a0 1 4 orig.bin 0
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
```

If your screen looks like the screenshot above and all 4 banks read OK and you get a "Reading finished!" message with a Datasum you can proceed. If not, something likely went wrong with the dump and you **SHOULD NOT** proceed until you get that resolved.



Creating Hacked Firmware in DOS

This section is only for those who chose to copy the required files to run Firmtool from DOS after creating the boot disk in iPrep. If you did not copy these additional files, simply skip to the next page and follow the instructions for creating hacked firmware in Windows.

After DosFlash completes the dump, run the following command to create your hacked firmware:

```
firmtool <original filename> <hacked filename>
```

For example if you are using v1.1 Fast firmware the command is:

```
firmtool orig.bin benq-ixA.bin
```

Firmtool should run and your screen should match the screenshot below. If you do not get a **green** success message or if you get any **red** error messages stop and go [here](#) to the Firmtool error section.

A screenshot of a DOS command prompt window titled "C:\WINDOWS\system32\cmd.exe". The window shows the output of the "firmtool v1.0 by caster420" command. The output includes a drive key, original and iXtreme firmware versions, a green "SUCCESS" message, and a confirmation that the BenQ iXtreme v1.1 firmware was created as "benq-ix.bin". The prompt asks to "Press any key to continue".

```
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.

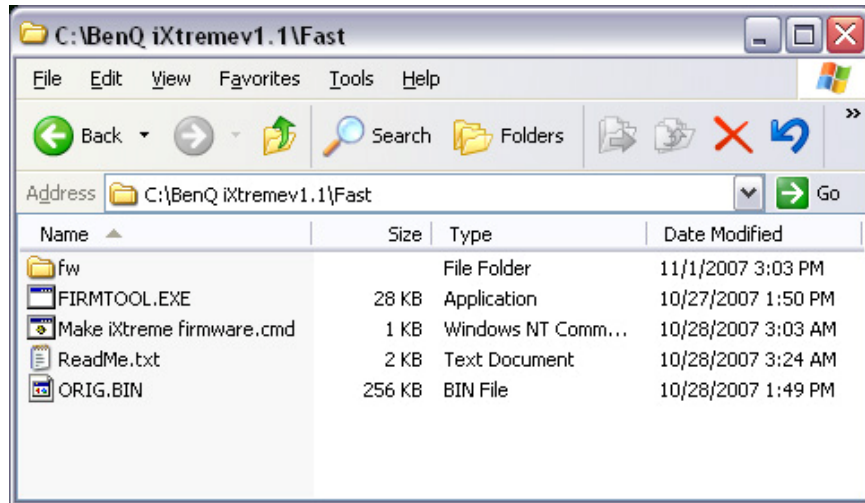
Your iXtreme firmware is now ready to be flashed!

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

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

Creating Hacked Firmware in Windows

After DosFlash completes the dump, boot back into Windows (or use Windows on another computer) and copy your orig.bin file to the BenQ iXtreme 1.1 folder of your choice (Fast or Quiet). That folder should now look like the screenshot below:



Double click the “Make iXtreme firmware.cmd” file. Firmttool should run and your screen should match the screenshot below. If you do not get a **green success** message or if you get any **red error** messages stop and go [here](#) to the Firmttool error section.

```

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 . . . _
  
```



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 . . . _
```

Erasing The Original Firmware

When using a VIA chipset to flash a BenQ drive, it is necessary to first erase the original firmware before flashing the hacked. If you do not erase first you will likely get a message saying that there were write errors during the flash.

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



Type in the following command, using your 4 digit port that you got from iPrep in place of xxxx.

DosFlash 1.3 use:

DosFlash e xxxx 1 a0 1 4 D8 0

DosFlash 1.4 use:

DosFlash e xxxx 1 a0 1 4 C7 0



Note the spaces, they are very important. Put a space wherever you see an underscore below. DO NOT type the underscores in DOS, they are just for your reference here and to make the spaces easier to see.

DosFlash_e_xxxx_1_a0_1_4_D8_0

or

DosFlash_e_xxxx_1_a0_1_4_C7_0

[press enter]

DosFlash16 will ask you if you want to resend the MTK Vendor Intro command, enter Y for Yes. When you hit enter the drive status is shown on the screen, it's something like 0x7F, this will change during the next few steps.

```
C:\>dosflash e CC00 1 a0 1 4 D8 0
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: 0x7F
```

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.

```
C:\>dosflash e CC00 1 a0 1 4 D8 0
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!
```

Flashing The Hacked Firmware

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



Type in the following command, using your 4 digit port that you got from iPrep in place of xxxx.

DosFlash w xxxx 1 a0 1 4 benq-ix.bin 0

Note the spaces, they are very important. Put a space wherever you see an underscore below. DO NOT type the underscores in DOS, they are just for your reference here and to make the spaces easier to see.

DosFlash_w_xxxx_1_a0_1_4_benq-ix.bin_0



[press enter]

DosFlash16 will ask you if you want to resend the MTK Vendor Intro command, enter Y for Yes. When you hit enter the drive status is shown on the screen, it's something like 0x7F, this will change during the next few steps.

```
C:\>dosflash w CC00 1 a0 1 4 beng-ix.bin 0
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: 0x7F
```

Turn on the Xbox 360, you should get a good drive status 0x73 and writing should begin automatically.

```
C:\>dosflash w CC00 1 a0 1 4 beng-ix.bin 0
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
Writing Bank 0...OK!
Writing Bank 1...OK!
Writing Bank 2...OK!
Writing Bank 3...OK!
Writing finished! Datasum: 8248
```

If your screen looks like the screenshot above and all 4 banks were written OK and you get a "Writing finished!" message with a Datasum then your flash is successful!

Your original firmware with your drive key is on the root of the USB drive, it is called orig.bin. Make sure to save that file somewhere safe!