DOWNGRADE OF DASHBOARD USING THE CHIP INFECTUS

IMPORTANT:

Follow precisly the instructions below, a minimum error or the premature cancellation of NAND will result in a console UNUSABLE.

The following procedure will VOID COMPLETLY your WARRANTY

First we need:

- Backup of the NAND just made
- 1888.FS.rar package is available on Xbins' FTP
- Programs iDGTool, Degraded and 360 Flash Tool downloadable on infectus site: CLICK
- Alternatively if you intend to downgrade the new Dash 6683 you will need a modified Degraded (thank Ciariello): CLICK
- An hexadecimal editor like Hex Workshop

Open Degraded program and select setting, we set the value 1BLKey on DD88AD0C9ED669E7B56794FB68563EFA and we sign the item "VALID", in the "File System Start" box we put 39 and then we selectpoi the Filesystem of the 1888 Dash downloaded from Xbins' FTP e proceed clicking OK:

We can now open the dump of our NAND done previously; at this point are two possibilities:

- Program recognizes the Bad Block Dump on the NAND (then continue to read)
- Program does not recognize bad blocks (skip directly the part below about bad blocks)

If the program detects "Bad Block" try to check soldering and to shorten the wires, then try again the dump, if the situation does not change, it's bad news, unfortunately the flash issuing bad blocks, although Robinsod (he made all this possible with Team MODFREAKz) said that there are no problems whatsoever. To confirm this point of view you can check what is been said on XboxHacker forum

"Handling of bad blocks in Cx area Now you will see the bad blocks (and the replacements) listed as "notes". if you are very unlucky the block at 0x8400 (where the CB header is located) will be bad. In this case the tools will fail and the image is unusable today.

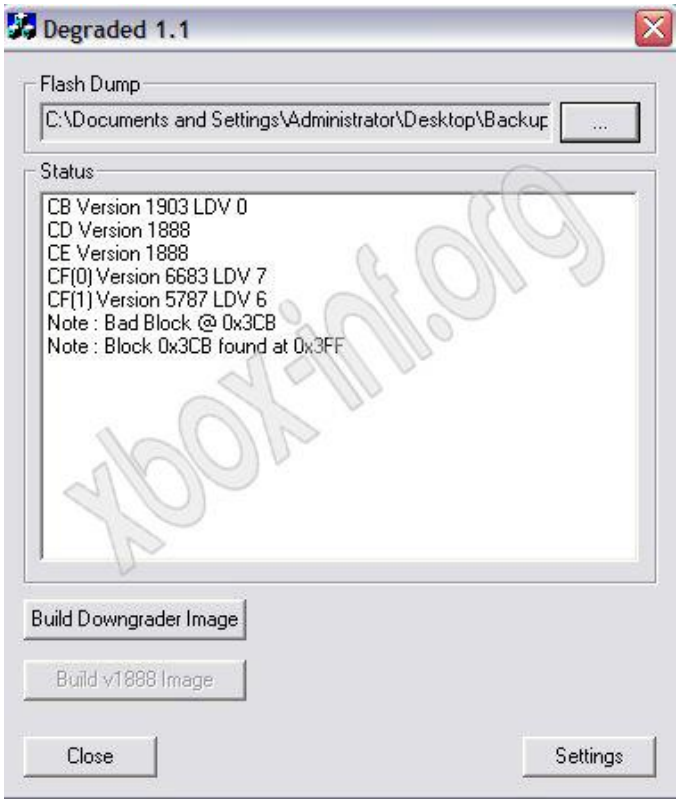
Handling of bad blocks in FS area (not 100% yet). Currently I test for bad blocks as I insert files into the flash image. If a bad block is detected it is simply skipped over. I had a look at a dump that contains bad blocks in the File System area and it appears the file system is unaware that some of the blocks it is using are marked as bad. I guess the flash driver silently does the remapping of bad blocks for the file system. I will fix this soon since it crashes the flash tool Wink

Handling of replacement blocks at end of flash image

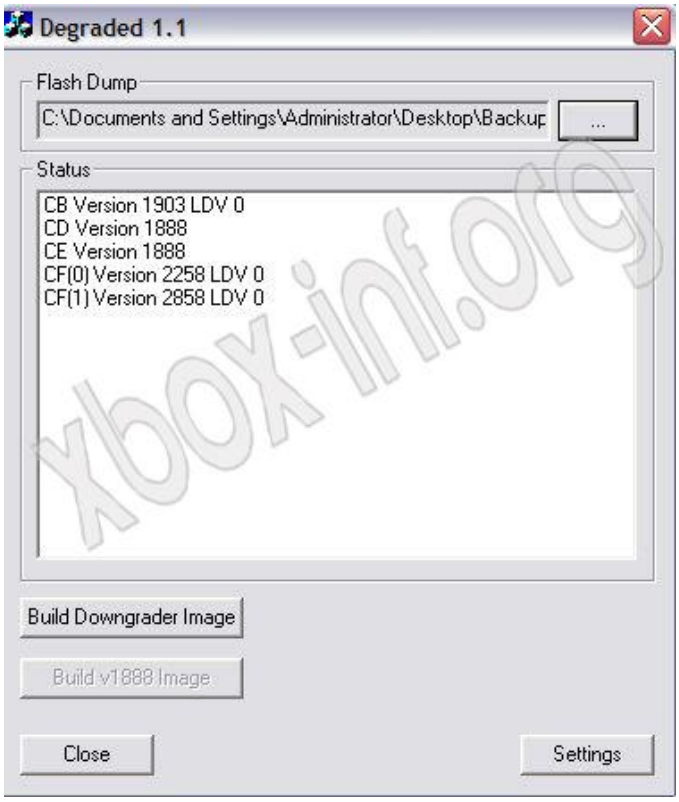
Now you will see the bad blocks (and the replacements) listed as "notes". if you are very unlucky the block at 0x8400 (where the CB header is located) will be bad. In this case the tools will fail and the image is unusable today - sorry."

Summarized, if there are errors in the block 0x8400 at the time, DO NOT PROCEED FURTHER, you risk damaging the console. The rest of BAD SECTOR should be safe. I contacted directly Robinsod on this matter, remember that this is a delicate operation, and even a little unexpected variable (also in case it's not your fault) is likely to make the console irreparable.

In this example the NAND releases corrupt blocks.

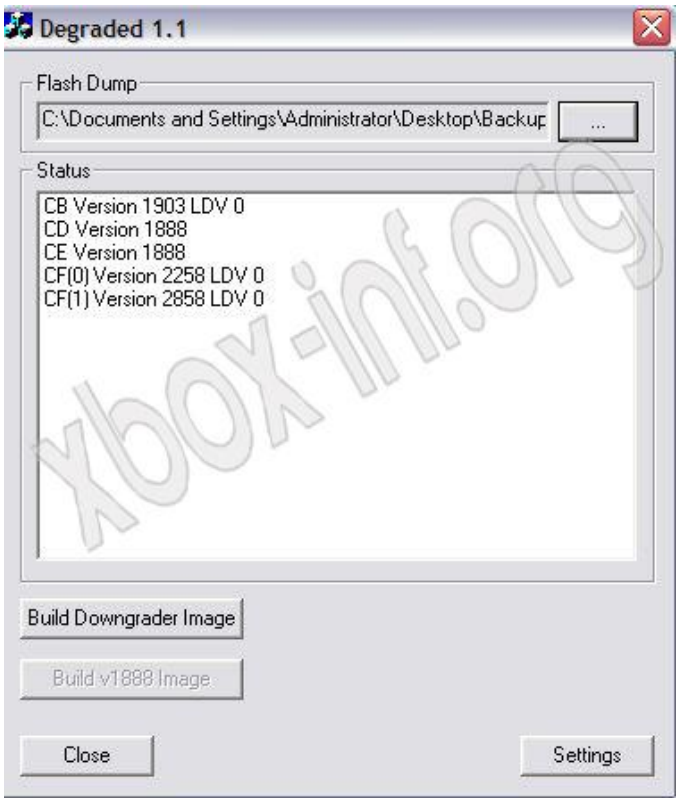


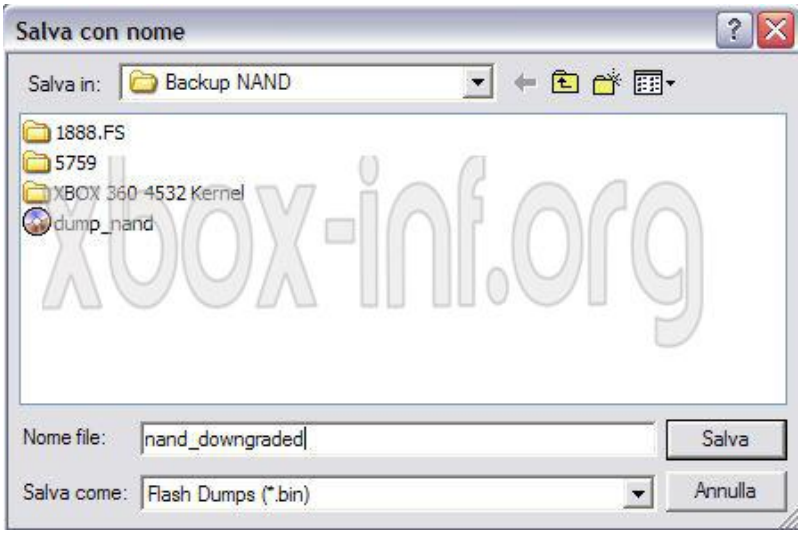
If everything is fine, the program will display a screen like this:



In this case there aren' t errors then we can proceed relatively quiet (this type of operations are risky anyway).

Click on "Build Image Downgrader", decide where to save the new modified dump and wait for the end of the process:





Proceed now with the last part of the downgrade ... Searching of 2BL Key Hash .

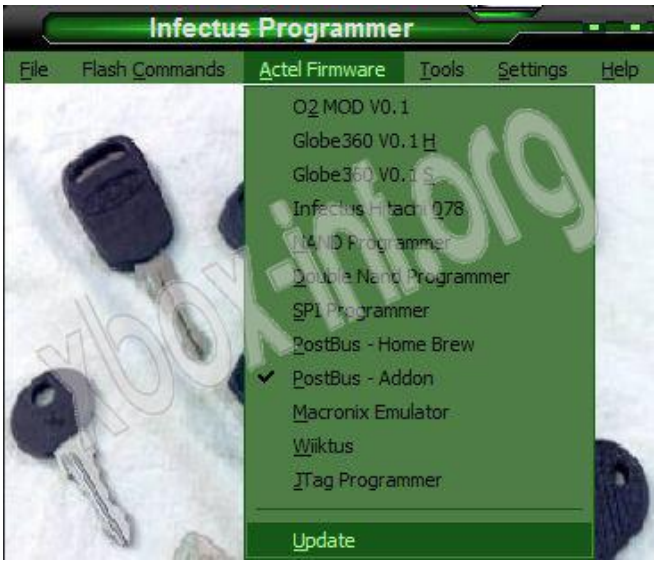
To do this we need:

- Degraded image previously created and inserted into the NAND of our console

- Files iDGTool.exe, Infectus.dll and SiUSBXp.dll foundable in 1888.FS.rar included together in the same directory

Let's execute the Infectus programmer and select "Actel Firmware \ PostBus Addon":

Run the command "UPDATE", once finished we can close the Programmer:



We must now flash the newly created NAND Dump (with Degraded) within our console, to do this we need:

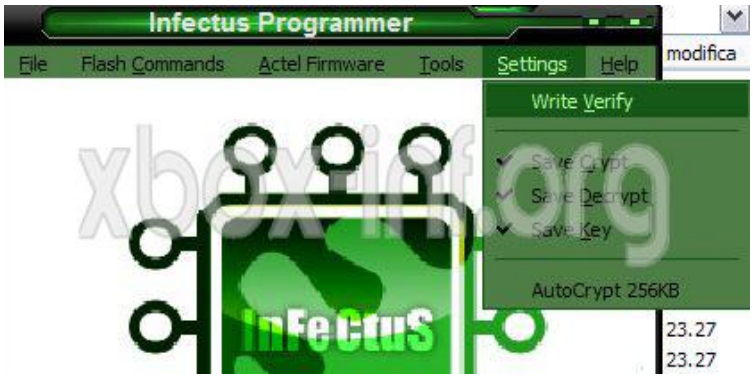
- Mini USB cable connected to Chip Infectus but NOT PC

- Video cable connected to the console (there is no need to connected it to the TV)

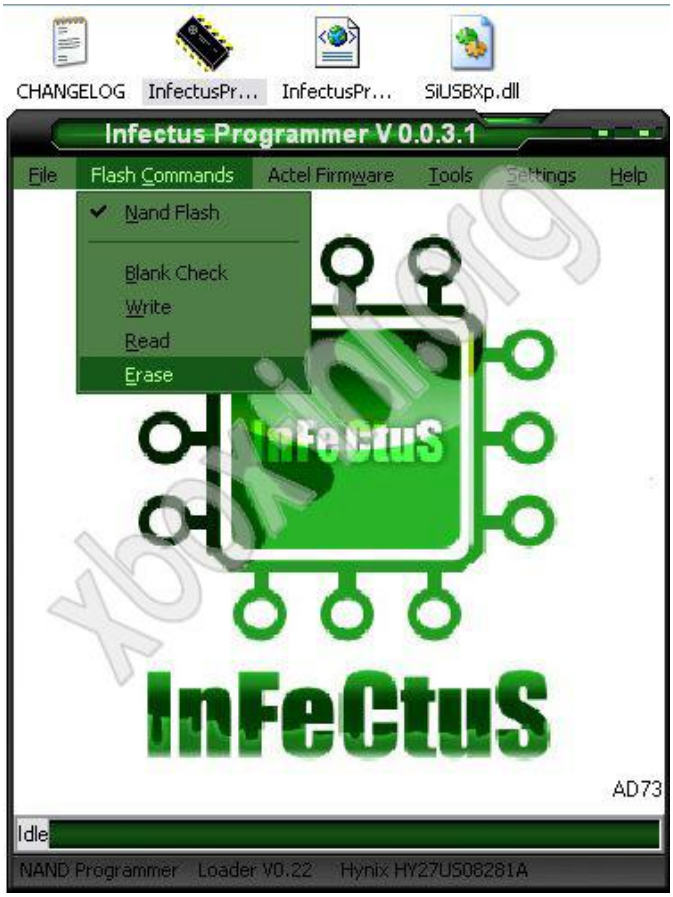
- Console and PC possibly connected to an uninterruptible power supply

- Power supply connected to the console but not on the wall (because the NAND recives 3,3 volts also in standby)

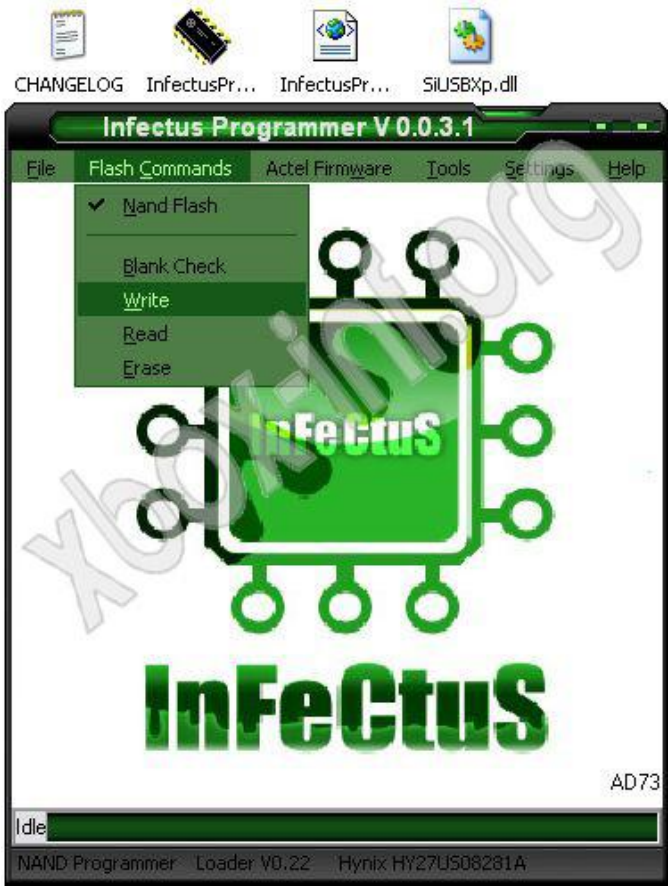
Now we can plug the power supply to the wall than we turn on the 360 and we connect the USB cable to PC, run the Infectus programmer and then we select "Setting" and we verify that "Write Verify " is disabled:



Select "Flash Commands" and then click "ERASE":

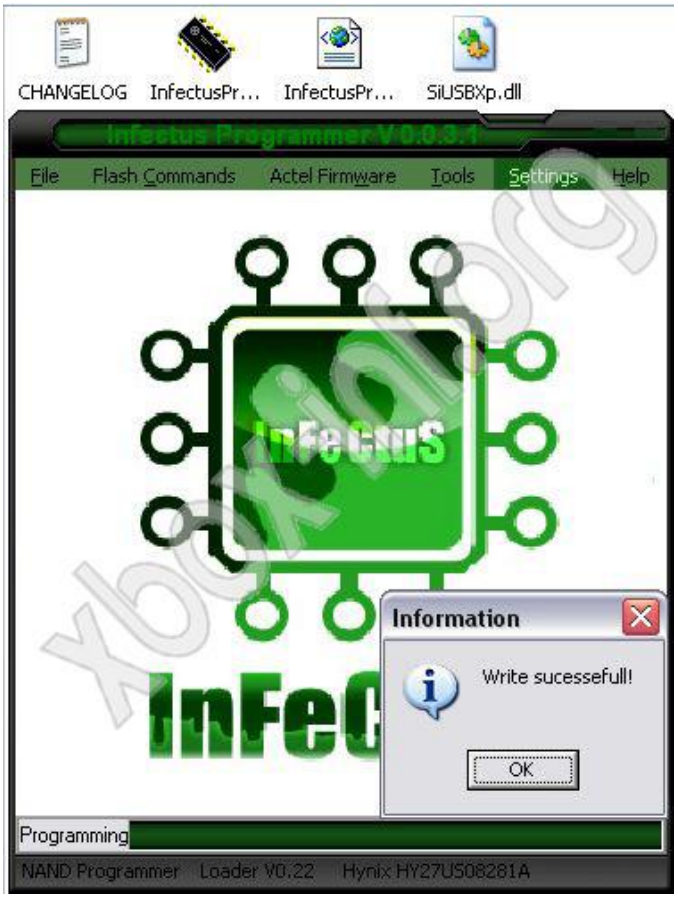


Swithout touching anything we select now "Flash Commands" option and click "Write":



We will select our NAND Backup file :

Than the NAND will be flashed:



Perfect, turn on the console, if it starts everything is gone right, if it isn't, try to reflash the NAND. If during this second flash the NAND is not recognized it means that we went on a bad flash ... Do not worry, there is a way to rewrite it and is shown on this tutorial: CLICK

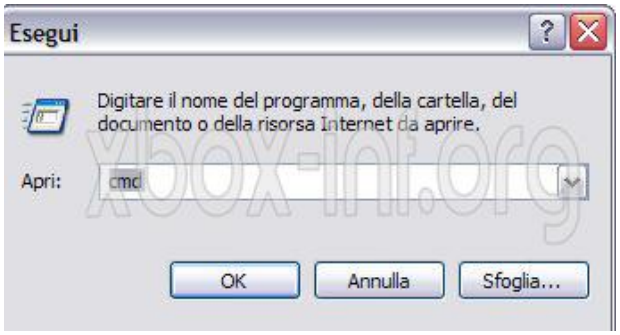
Create a directory and put inside it:

- IDGTool,

- Infectus.dll

- SiUSBXp.dll

Run MS dos prompt than reach the directory just created containing iDGTool, Infectus.dll and SiUSBXp.dll:



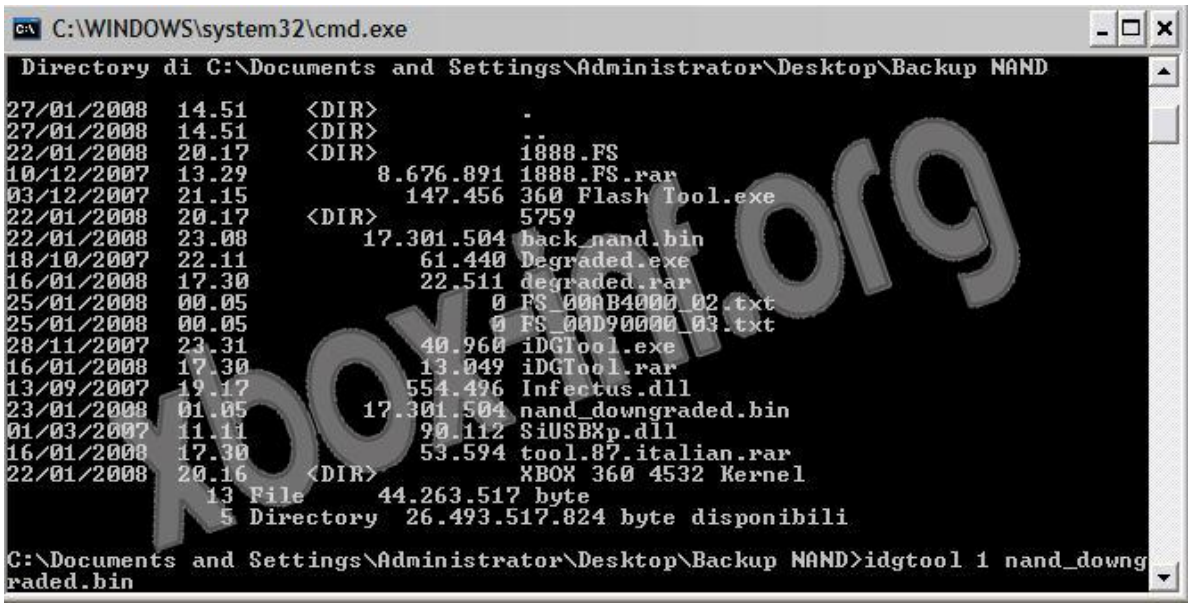
Write the command to execute IDGTOOL followed by the number of attempts which it must try to make the detection of 2BL key Hash (1 recommended attempt) and the name of the previously created image by the Degraded program. Example:

- IDGTool 1 <image downgrader name>

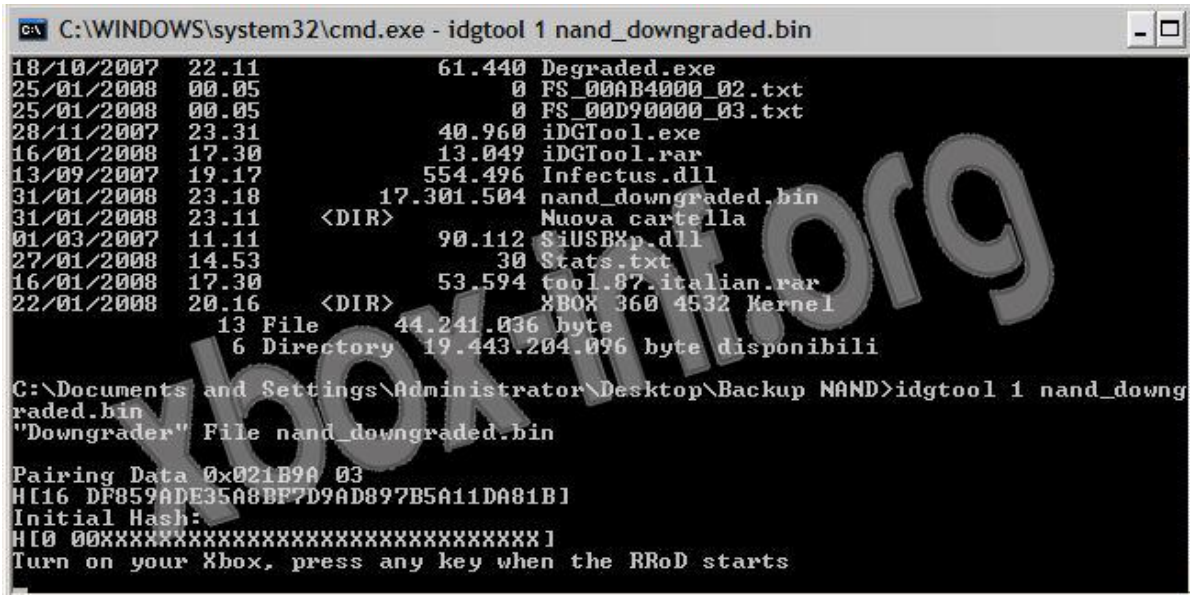
That in my case becomes:

- IDGTool 1 nand_downgraded

And we press RETURN:



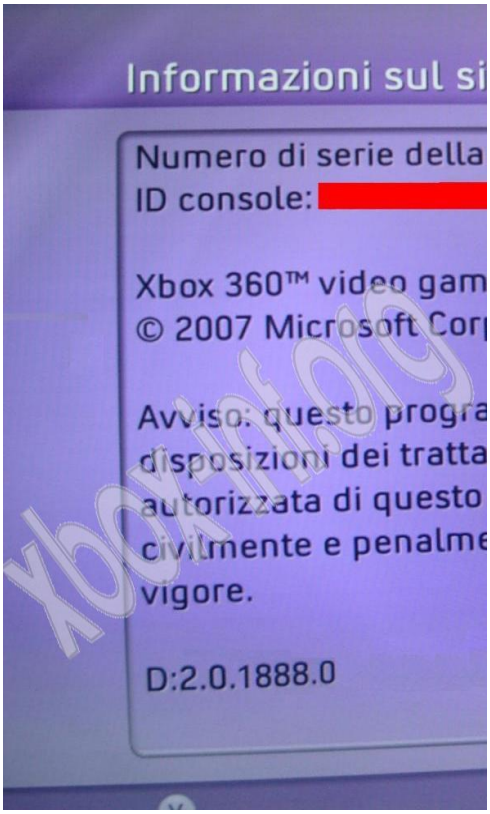
Turn on the console and when it will hit 3 red leds press any button to begin the process. Be advised that the process could take up to 1 hour:



Searching the key:

The program will end the extraction of 2BL HASH when at the bottom of all processes will appear "BOOT":

Done, once finished we test the console, removing USB cable from infectus and turning the 360 on. If everything worked the version of the Dash will be "D" & "K" 2.0.1888:



Congratulations, you just made it, you now have several options:

- Load dash 4532 to exploit the bug and start Gentoo Linux (if you are a developer)

- Run another backup NAND and keep it for future use

Remember that if you launch a recent game the dash will be upgraded again, then unless you want to redo the whole process I recommend strongly make a backup of your downgraded NAND and keep it jealously.

Put everything back to verify if the 360 works normally, after that, we can proceed with our last NAND backup

Back to Home

For technical support click here: Forum Xbox-Inf

THANKS: Hardstore, Oscar Dalvit, Splinter, the Hardstore Team and the Origa Team

Tutorial Written by Titty, Maw80 and Ciariello, translated by Raiden for the Xbox-Inf Forum