Basic Guide to LiteOn DG-16D2S hacking.

This guide will cover Windows based flashing, if I have time Ill support 16bit (DOS) in a further guide. I won't cover tray status too much – needs to be 'closed' but half open, nor will I cover Hardware, CK3 / Xtractor are there for the people that need it, want to make your own? Tray status or Schematics? Excellent guide to it here: http://beta.ivancover.com/wiki/index.php/Xbox_360_Lite-On_DG16D2S_Extract_Key

YOU MUST INSTALL PORTIO32.EXE BEFORE RUNNING THESE PROGRAMS

Programs required / used:

DVDKey32 v0.7
Firmtool v1.3
Lite-On-Erase
Dosflash32 v1.6

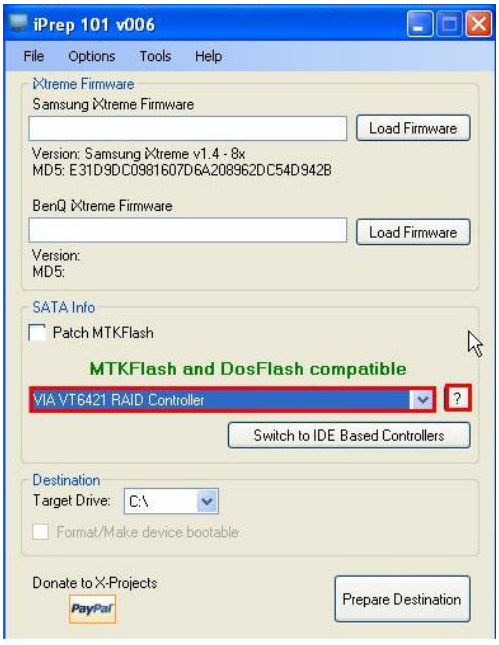
One of the most vital parts of LiteOn modding is the use of your 'Command Base Register' Or, sata port.

Identifying your Sata Port Info

There are a few ways to do this, Ill cover the simple ones feel free to use your own methods.

Method One: iPrep

Run iPrep 101 v006 and select your Sata Controller in the drop down box. Then, click the ?



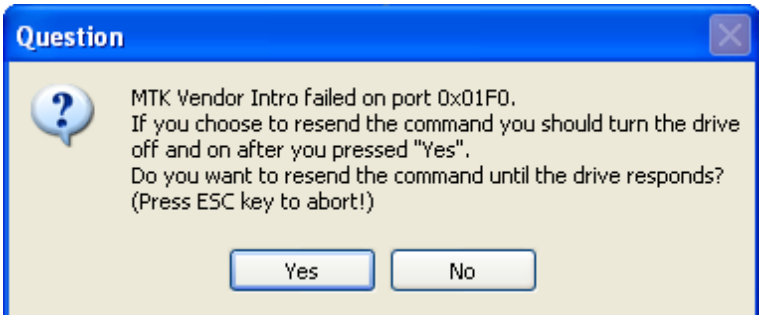
You will be presented with something resembling the image below.

Your command base register is the first 4 characters of DeviceIO – In this case CF00

Method Two: Dosflash32

Hook up your LiteOn to your PC power(ed) On

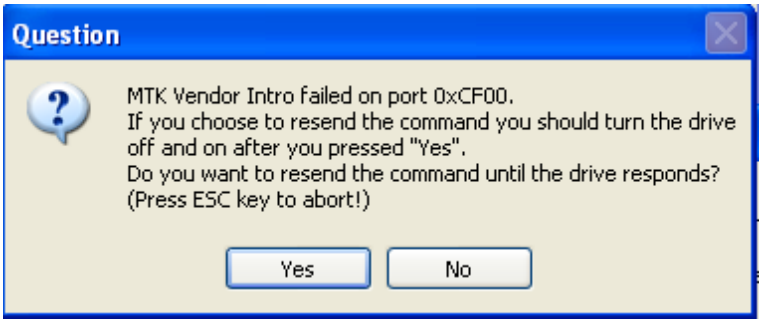
Run Dosflash32.exe



You may or may not see this, this is it failing on my Pioneer DVDRW – 0x1F0 and 0x170 are generally NOT your magic port.

Select No if it returns 0x170/0x1F0 ports.

If all is good, you will receive something similar to the image below, note my port. 0xCF00 – The same magic port iPrep returned ☺

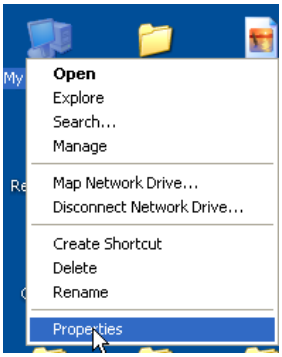


You might as well say No once this is returned as the LiteOn drive is locked, so it won't respond to the mtk intro query.

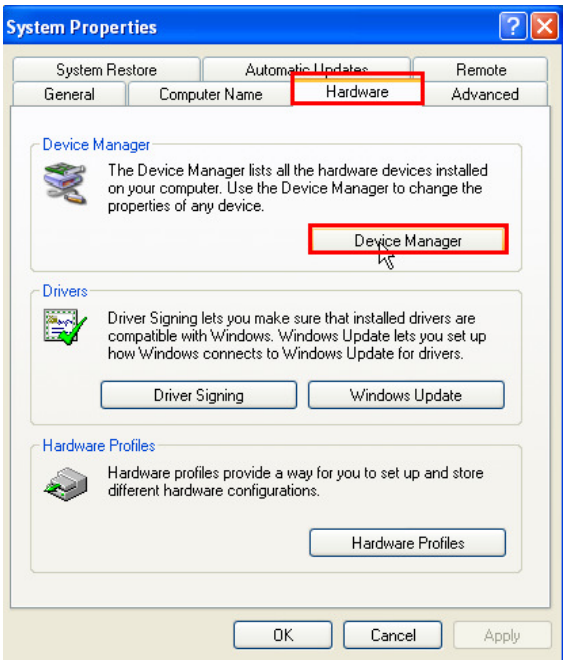
OK, now you have your command base register, we need the com port you will be using (usually 1 for Serial Cables, needs to be 1-9 for USB or USB To Serial Adapters)

Right Click "My Computer"

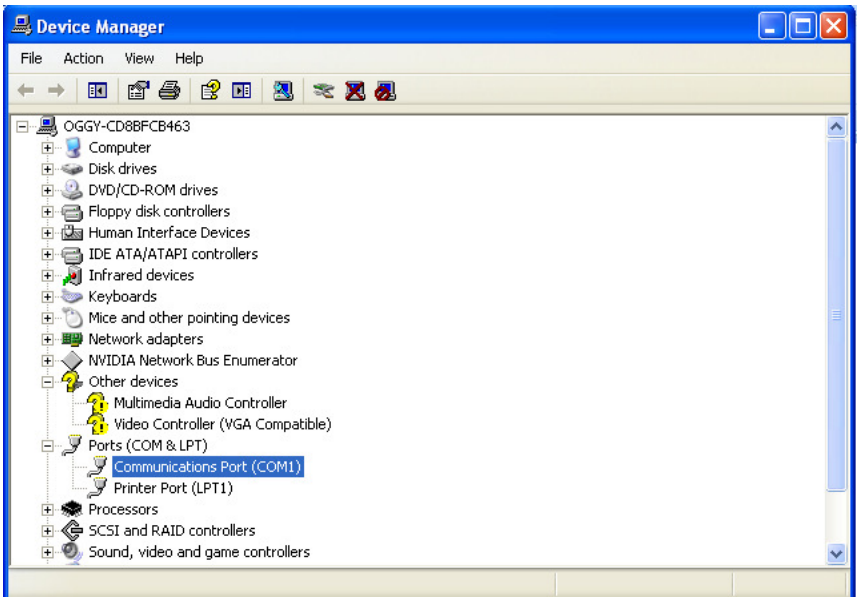
Select properties



Select 'Hardware' tab, then, 'Device Manager'



Scroll Down to 'Ports COM & LPT'



You will see that I have been assigned Com Port 1

Now you can prepare to dump the data from the LiteOn

At this point, you should have all the system info you need to complete the process.

Next Step:

Obtaining dummy.bin using DVDKEY32 v0.7

DVDKEY32 is run from the command line and requires the command of:

Dvdkey32 SATA PORT COM PORT

In my instance, this is Dvdkey32 CF00 1

If you are not familiar with using Command Prompt, grab this neat powertoy.

http://download.microsoft.com/download/whistler/Install/2/WXP/EN-US/CmdHerePowertoySetup.exe

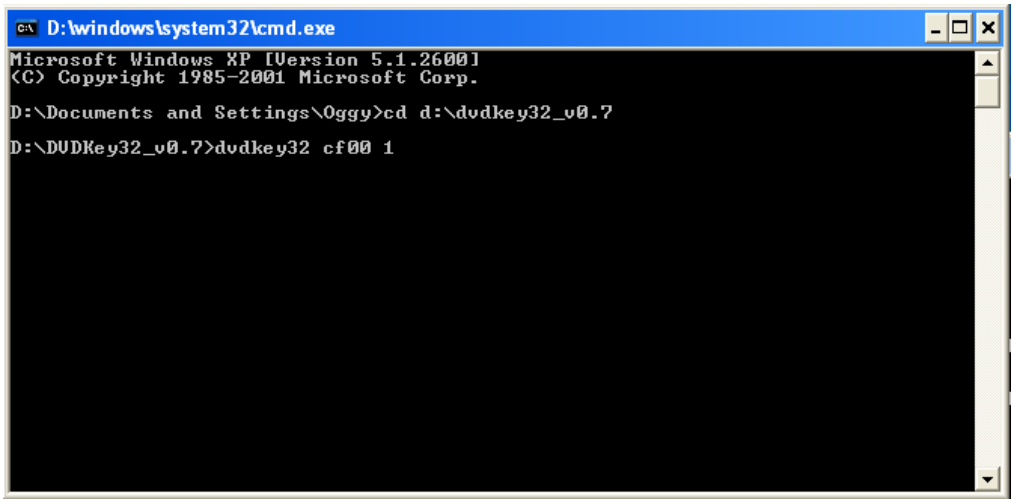
Navigate to the folder containing DVDKey32 v0.7 and right click→Open Command Window Here

Or, navigate manually in command prompt.

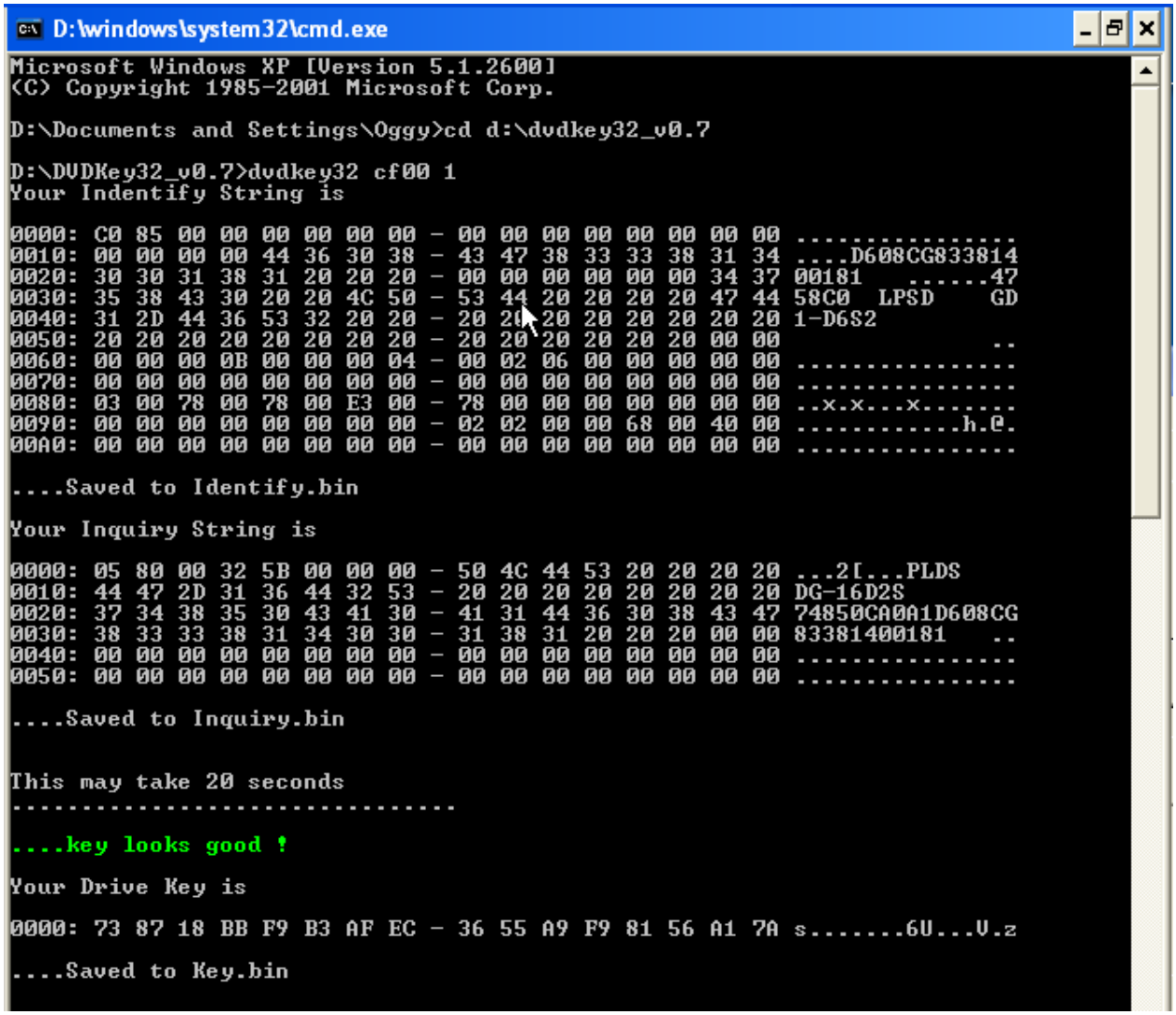
Important notes:

- Tray Status needs to be closed, but drive half open
- Serial port on LiteOn **MUST** be in tact (or using a probe/spear)
- You only need R707 joined
- Sata and Serial/USB connected to PC
- Drive powered **ON**

Type you DVDKEY32 command in the command prompt as shown below.



Insert probe / spear / homemade version if using one into via above R707 and press Enter



You will be presented with something similar to this, if key is returned as CC CC CC CC CC CC CC CC - CC CC CC CC CC CC CC CC – Then check your serial port / eject status.

Only proceed if you get green success message shown above.

DVDKey32 has just also created dummy.bin for firmtool support

THIS IS NOT AN ORIGINAL FIRMWARE FILE BUT IS TO BE TREATED AS SUCH IT WILL NOT WORK IF FLASHED TO A DRIVE

Inserting unique data into Hacked Firmware

This process is also run from the command line, using FirmTool v1.3.

You need Firmtool.exe, dummy.bin and LiteOn iXtreme all in the same directory.

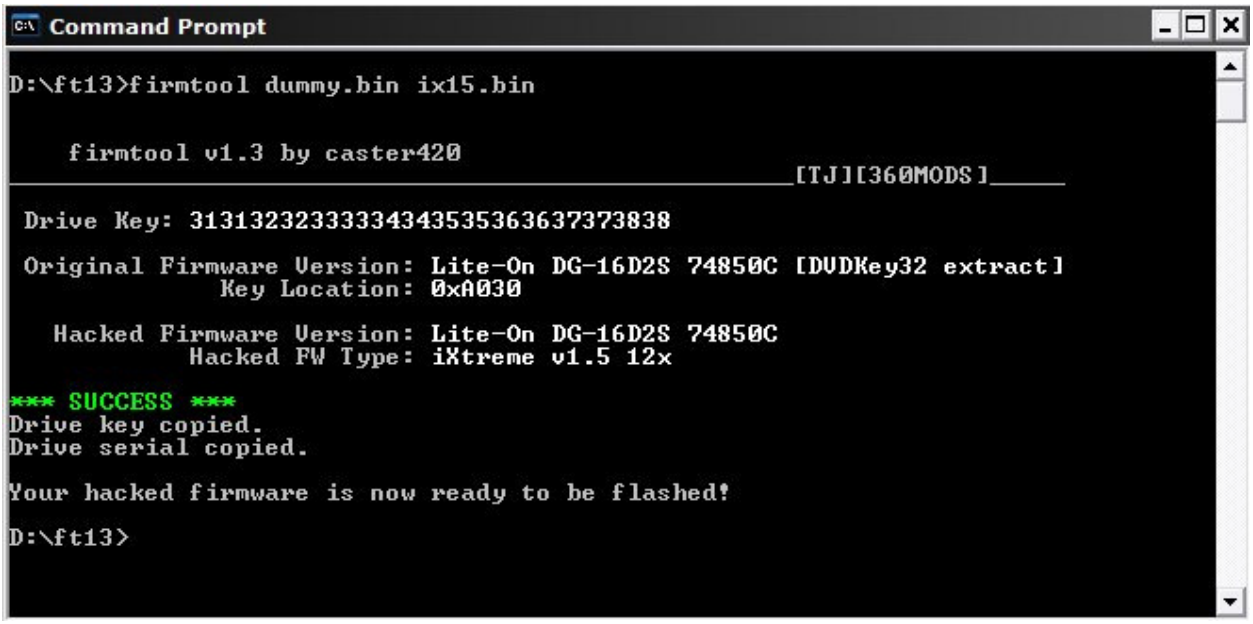
Use the command powertoy or navigate in DOS to the containing folder of FirmTool.

Usage:

Firmtool *source.bin* *hacked.bin*

e.g. **Firmtool dummy.bin iX15.bin**

It should look like this:



Again, look for a green success message, abort if this isn't produced.

Upon getting green success message, you are ready to erase the LiteOn drive.

Its ESSENTIAL you have the correct Drive Key backed up, once this erase cdb is sent there is no going back.

Erasing LiteOn Drive

Again, used from command line. Open containing folder of lite-on-erase.exe or navigate manually.

Command for erase is:

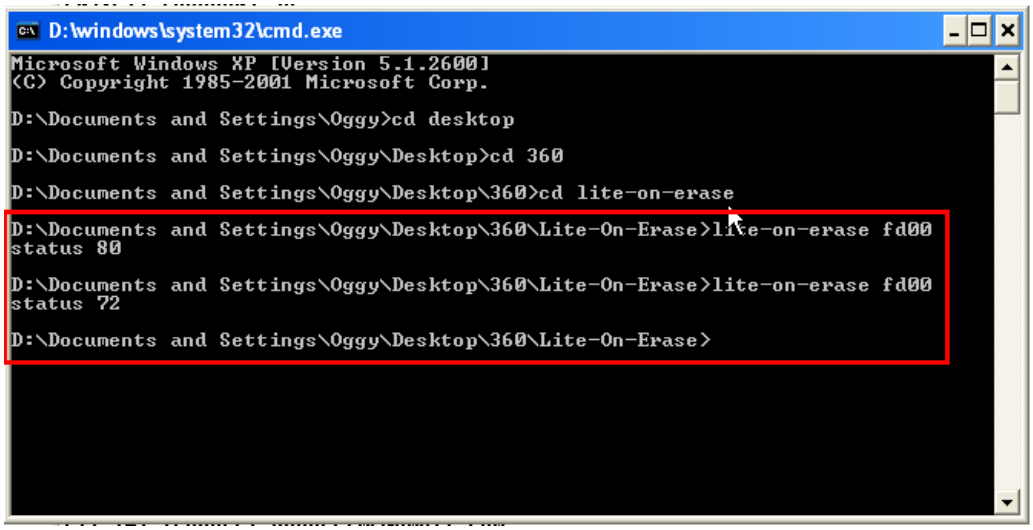
Lite-on-erase SATA PORT

e.g. Lite-on-erase CF00

You may get status 0x80 a few times, keep retrying until status 0x72

Image below shows me getting 0x80 before 0x72 – 0x72 is erased.

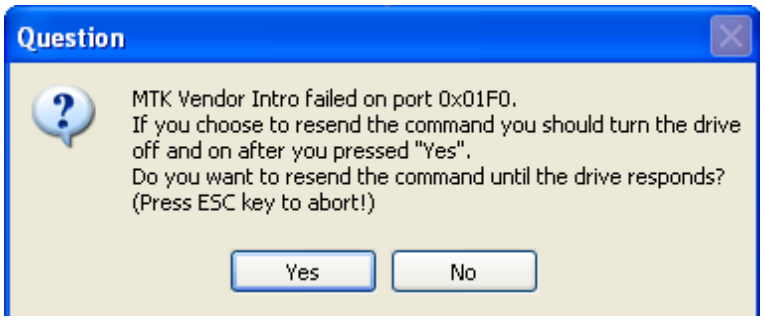
N.B I erase LiteOns on my onboard Sata, so my sata port has changed in the image.



Writing the hacked firmware

Now, status is 0x72 we need to power cycle the DVD Drive.

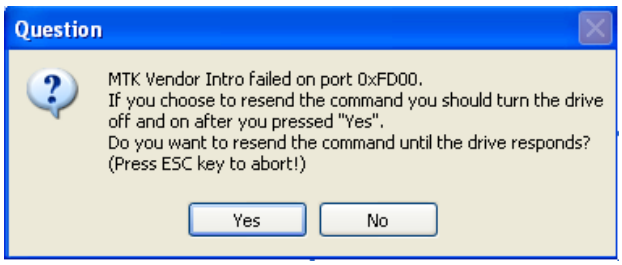
Do so, then, run dosflash32.exe



You may or may not see this, this is it failing on my Pioneer DVDRW – 0x1F0 and 0x170 are generally NOT your magic port.

Select No if it returns 0x170/0x1F0 ports, you want the port you have used for DVDKey32 and Lite-On-Erase.

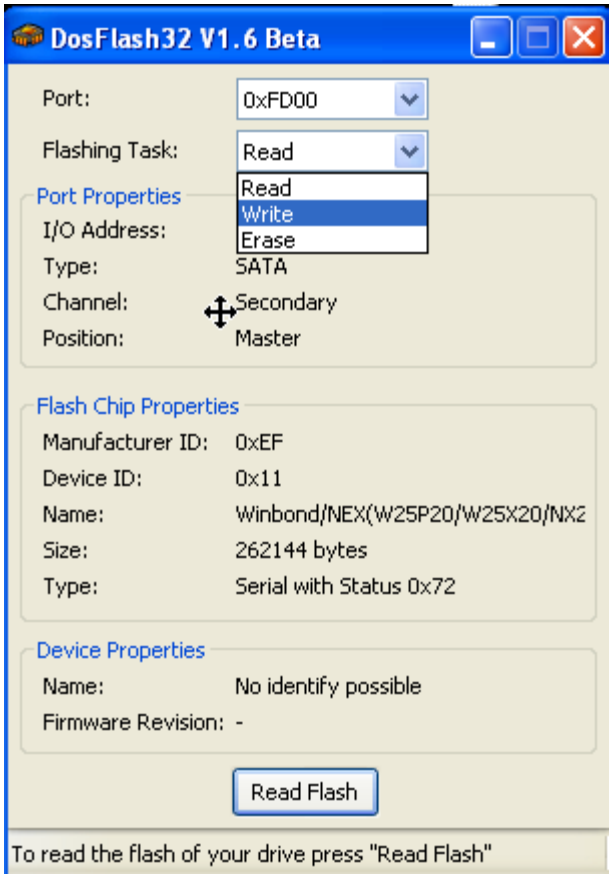
Failing on correct port shown below:



Select Yes.

If prompted for any other ports before/after just say No.

You will end up here:

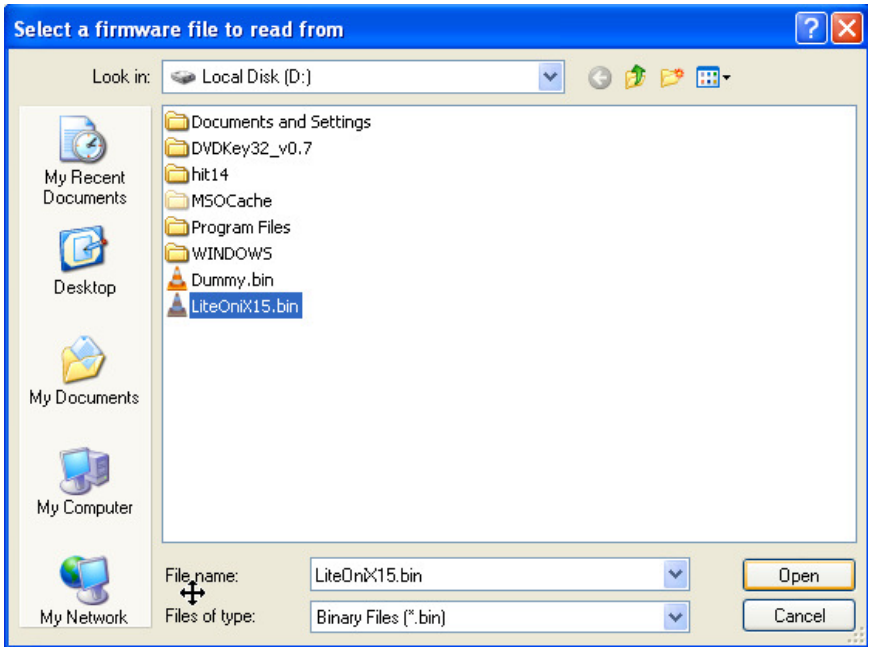


Ensure correct port is selected at the top.

If flash chip properties are not filled in, you probably didn't power cycle the LiteOn after erase – Close Dosflash32, power cycle drive then restart Dosflash.

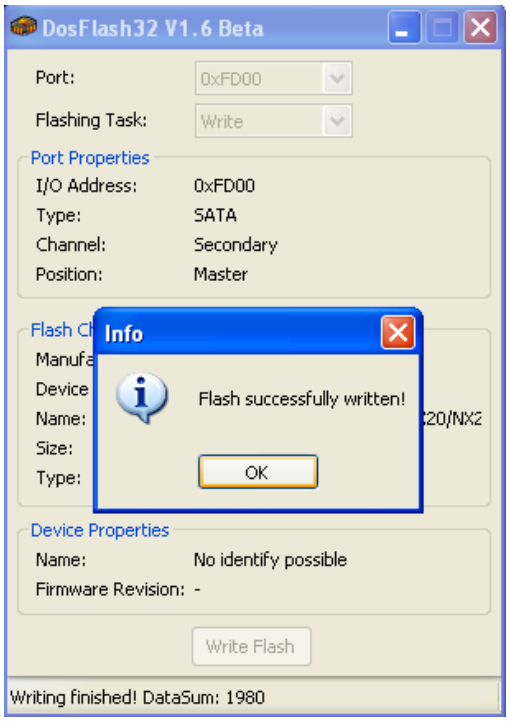
Select write in the drop down box and Click **Write Flash**

Navigate to your hacked firmware (iX15.bin) you created in FirmTool Directory.



Select it, click Open.

It will flash all 4 banks and hopefully give the message you want to see ☺



If write errors occur, you will need to erase / flash again.

Major thanks to Team Jungle on this.