JungleFlasher v0.1.87

(x86 and x64 Compatible)

Complete User Guide

(v0.1.4.4)

X360USB PRO

USING THIS TUTORIAL!

DO NOT TRY to read this tutorial by scrolling through all the pages!

It is not sequential in any way!

Use the flowchart links and links at bottom of each section to take you directly to the correct instructions for your situation!

Trying to read through each page regardless IS POINTLESS! (And confusing)

USE THE LINKS!

I AM A NEW USER OF JUNGLEFLASHER	USED JUNGLEFLASHER BEFORE
CLICK HERE	CLICK HERE

Things not going as expected? – Read the FAQ's

Introduction

JungleFlasher is developed in conjunction with Team Jungle in an effort to bring all 360 DVD-Drive flashing functions together in one easy to use Win32 Application. JungleFlasher provides several functions that up until now were carried by several different app's in both Dos and Win32. JungleFlasher is also fully supported in x64 environments.
Recent revisions of JungleFlasher have added support for Xecuters X360USB Pro – For USB based flashing on ALL systems, with no freezing/unsigned driver issues.

The **FirmwareTool 32** tab is used to process firmware files. Jungle Flasher will parse the files, identify the firmware type and display relevant information such as the all-important DVD key and OSIG strings etc... On the Target sub-tab, MD5 hash checking of iXtreme firmware files is conducted to confirm authenticity. With both source and target files loaded, the relevant source data can be transferred to the Target (a.k.a. Spoofed), which can then be flashed to the target drive.

The **DVDKey32** tab is used to extract info from LiteOn – the undumpable drive. All unique information is extracted: DVD key, unique inquiry and identify strings and drive serial information. This info is stored in one easy to use file,"Dummy.bin". This is a 256kb file that mimics the approximate structure of a BenQ firmware file and is automatically loaded to the source sub-tab in the FirmwareTool 32 Tab. Jungle Flasher v0.1.79b introduced support for Pógó Mo Thóin (PMT) a new method of extracting the DVDKey from all (Phat) LiteOn DVD Drives, using only a switch on the 3.3v line and a probe to GND at the very least, or using such devices as the **Xecuter Probe 3**.
Legacy methods are still supported under this tab, such as LO83info, DVDKey32, Dummy from iXtreme and rebuilding a Dummy.bin from individual files (key/inquiry/identify/serial) - Users who wish to utilise these methods can find information contained within the LiteOn Flow Chart of the User Guide.

The **MTKFlash 32** tab is used to unlock Benq, Samsung "Slim 9504" LiteOn drives and then dump the current flash for use in the source sub-tab in FirmwareTool 32 tab. You can also erase a LiteOn in preparation for flashing. All MTK (Mediatek) Based drives can be flashed using this tab.

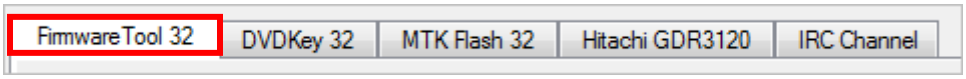
The **Hitachi GDR3120** tab is for Hitachi drives which are flashed differently from the MTK based drives mentioned above, therefore have their own dedicated tab. Hitachi's are flashed as a "Live" drive, on a sector by sector basis and as such needs to be performed in a very controlled way so the process is heavily automated. JungleFlasher will only flash iXtreme to a stock drive and so a restore facility is provided, which allows for a full restore to stock f/w of previously modded drives. Several additional features like setting Mode-B over PortIO, USmodeB and 79Unlock are included for convenience. Dumping and flashing is also possible over PortIO for those who removed VIA drivers to work around Lite-On-Erase lockup issues.

JungleFlasher is intended to be rich in information providing as much relevant and useful information as possible. On the DVDKey 32 and MTKFlash 32 tabs, all I/O and COM port information is detected and displayed, as well as drive and device properties for the currently selected drive.

Things not going as expected? – Read the FAQ's

Overview of JungleFlasher and its functions

When you start JungleFlasher, you will be presented with **5 tabs**;
FirmwareTool32, DVDKey32, MTKFlash32, Hitachi GDR-3120L & IRC Channel.

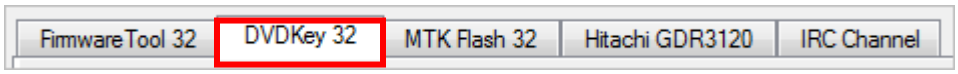


FirmwareTool32 is used to view firmware details, manipulate these firmwares, and to save the firmware and/or details of the firmware.

It is split into 2 sections, Source and Target, with function buttons surrounding it.

Source, this is the originating firmware, this can be previously dumped firmware (containing console specific drive key, Drive string ID and serial data), original firmware, dummy firmware etc. This data should always mimic what the Xbox 360 should expect from the DVD Drive.

The Target area (buffer) should contain the firmware you wish to apply to the drive itself, this firmware will be manufacturer specific, BenQ firmware for BenQ drives / LiteOn firmware for LiteOn Drives etc. Hitachi Drives do not use FirmwareTool32 in the same manner; this is fully explained in Hitachi section.



DVDKey32 is primarily used to obtain **Key.bin, Inquiry.bin, Identify.bin, Serial.bin and Dummy.bin** from **all LiteOn PLDS drives, both Phat and Slim**. It also has an option to rebuild from previous files (for people who used other, older applications or those who followed poor advice before). **Slim 9504** Users can utilize **Slim unlock** in the **MTKFlash32** Tab to read the full FW from the drive.

JungleFlasher v0.1.79b introduced "PhatKey" – A method of obtaining the DVDKey from **Phat LiteOn** drives, using only a probe and a switch on the drives 3.3v line – **Xecuters Probe 3** is a professional / affordable tool targeted at this method and comes highly recommended.

Older legacy methods, such as DVDKey32 and LO83info remain supported for those wishing to use these exploits.

Jungleflasher v0.174 brought a **Key verification routine** which tests the keys, primarily on **Lite-On** drives but is also applied to **pre-78 Hitachi** drives and **Samsung** drives and can be verified on **Benq** too (though not automated like **Lite-on**) Using this ability it's now possible to create a new Dummy.bin from the key database and **Verify** that it is correct.

Things not going as expected? – Read the FAQ's

There are also 5 checkboxes found in this tab, **USB Only, VIA Ports Only** and **Include non-IDE ports,** added for extra safety and compatibility; **Additional Features** – for use with the CK3-CP and Maximus USB Xtractor Push Button to extract feature this launches the DVDKey32 command from the Hardware Device itself. The final one being **Dummy.bin Only** – this being a cleaner method of storing files as Dummy.bin incorporates the other files obtained.

MTKFlash32 contains a variety of functions, from unlocking and reading of **BenQ, Samsung and Slim LiteOn** drives using their dedicated **Unlock** buttons, or **LiteOn** drives after placing them in Vendor Mode (using MRA Hack).

MTKFlash32 is also where you are able to send the Intro of Death (a.k.a LiteOn Erase) to the **LiteOn PLDS DG16-D2S** after obtaining DVDKey, and for writing to the drive after Intro of Death, or once drive placed in Vendor Mode using MRA Hack.

MTKFlash32 will also **erase** and **write Samsung** and **BenQ and LiteOn** drives, once the drives have been unlocked/placed in vendor mode.

MTKFlash32 will show, in the lower left section, the details of the drive inquiring on the respective **I / O Port** listed above. This is where you will identify which S-ATA Port to use for carrying out the process.

Hitachi GDR3120 As mentioned previously, the Hitachi Drives are flashed completely differently to the MTK Based drives; Hitachi's are flashed as a "Live Drive" on a sector by sector basis.

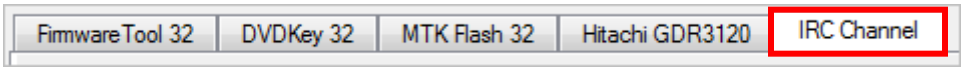
For this reason, JungleFlasher has its own dedicated Hitachi tab, all the flashing options you may need to do can be done under this tab.

As with the other Tabs, JungleFlasher will show the I/O port list for identifying what S-ATA Port your drive is on.

It also incorporates a **Raw Mode-B** command for putting a drive into **Mode-B** and automates the Play/Pause/Eject for **79Unlock** – Audio Disc still required!

Once the drive is actually in **Mode-B** you can use the flashing options located in this section of the application, the options themselves are pretty self explanatory.

With the **Firmware Pack** installed, JungleFlasher will automatically load the correct iXtreme file for your drive, or Original Firmware if restoring.



With the release of JungleFlasher 1.71, there is now a IRC Channel tab within the actual program. If you have **read this tutorial and still cannot figure out your problem**, please feel free to use the chat function and get some live support with your problem. Please DO NOT expect us to help you if you have not even tried to research your problem! There is a huge amount of information in this tutorial and the vast majority of methods are covered for almost all situations.

NOTE: If requesting advice/help in IRC Channel – PLEASE – give a good description of your setup- OS, Drive, FW, SATA chipset, Difficulty you're experiencing etc. DO NOT – give a single line of info and expect people to magically know what your problem is!

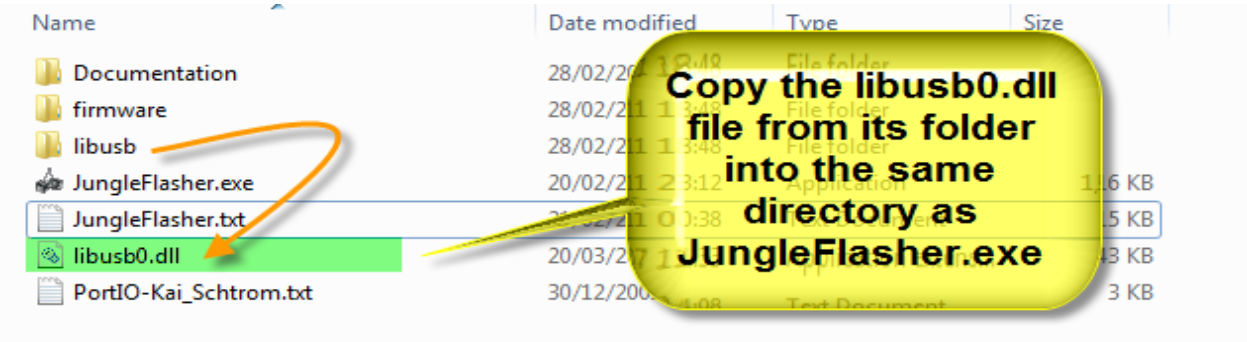
BEFORE USING JUNGLEFLASHER

You Must Have .net framework installed

.net framework 2.0 or later for Windows XP machines
.net framework 3.5 SP1 on Windows Vista Machines
.net framework is built-into Windows 7 (easy life!)

IF you get a libUSB0.dll error

Copy **libUSB0.dll** file from its folder, into the same directory as **JungleFlasher.exe**



You Must

JungleFlasher Firmware Pack (vital for Hitachi Drives)

Place all the individual .bin firmware files inside the firmware folder!

Download the latest iXtreme firmwares from usual sources – place all the .bin files into the firmware folder that is inside the JungleFlasher folder! (This allows for auto-loading of firmware as well as being essential for operation during Hitachi manipulation/flashing)

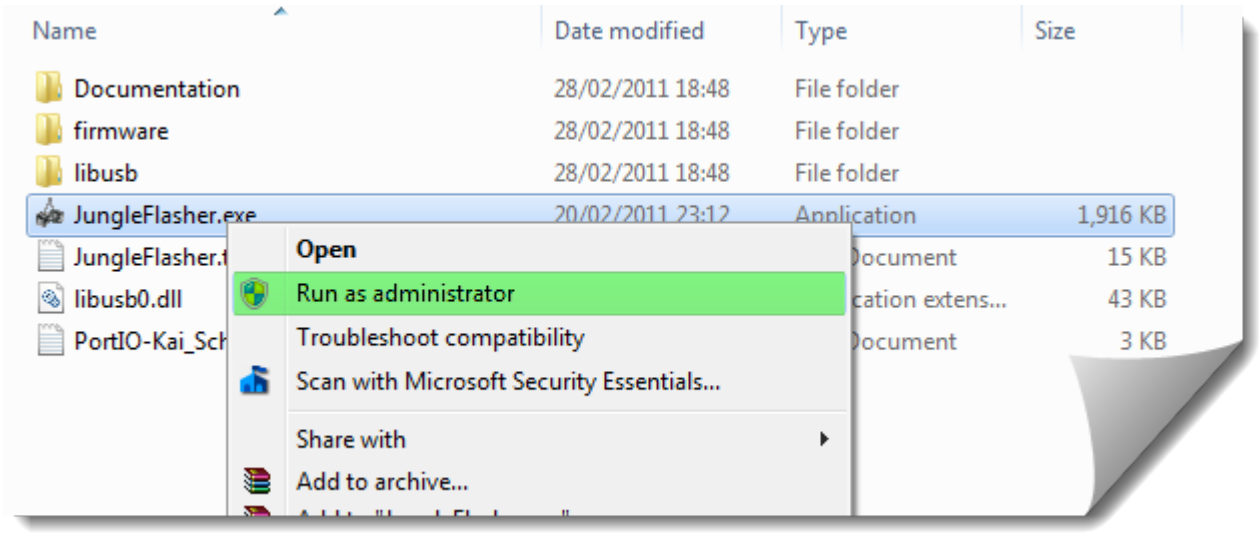
If you are using a VIA card - remove the drivers!

It is advisable as the drivers tend to cause problems on a lot of drives but very noticeable with erased LiteOn, causing the infamous 'Lite-On + VIA Freeze'
CLICK HERE TO FIND OUT HOW TO DO IT PROPERLY

NOTE: 0225/0401/1071 SLIM DRIVES DON'T WORK WELL WITH VIA CHIPSET

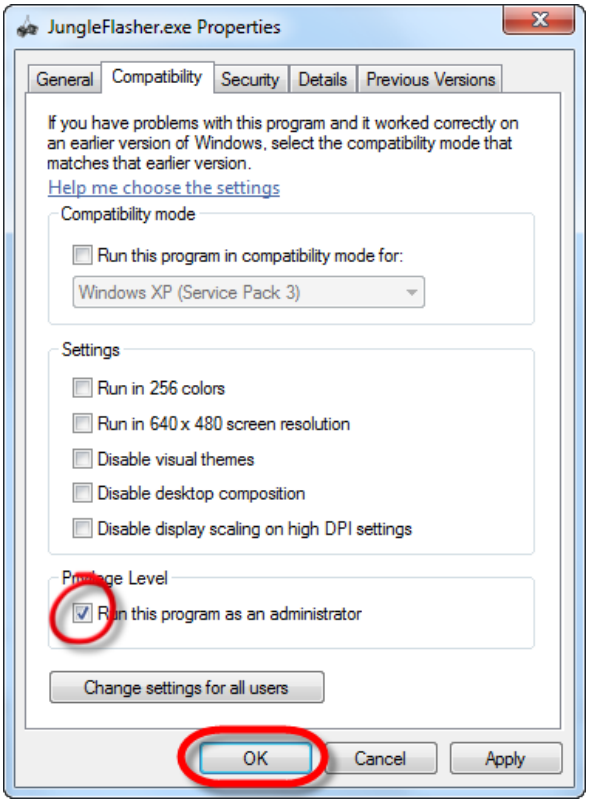
If using ANY Operating System other than Win XP x86 you must right-click on Jungleflasher Icon and select "Run as Administrator"

Things not going as expected? – Read the FAQ's



OR

Right click on icon, select properties > compatibility, tick the box, press ok



CLICK HERE FOR ADDITIONAL INSTRUCTIONS FOR USE WITH x64 VISTA/WIN 7

Things not going as expected? – Read the FAQ's

WHEN you run Jungleflasher you MUST ensure PortIO*XX.sys is RUNNING!**

(Unless using X360USB Pro)

You can do this easily by looking at the log at the bottom of the window (as shown)

*** XX - will be either 32 (for x86 operating systems) or 64 (for x64 operating systems)**

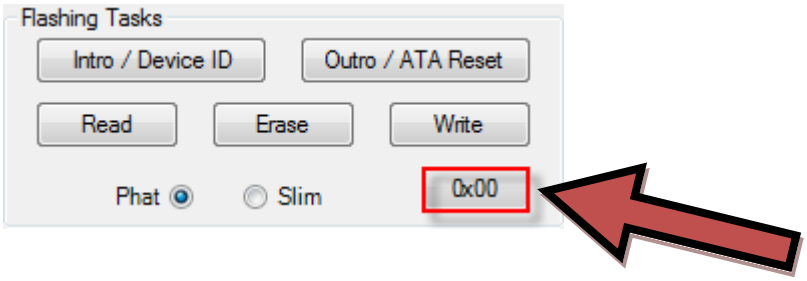
```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
JungleFlasher 0.1.79 Beta (210)
Session Started Sat Mar 05 07:56:28 2011

This is a 32 bit process running on 4 x 32 bit CPUs
portio32.sys Driver Installed
portio32.sys Driver Started, thanks Schtrom !
Found 10 I/O Ports.
Found 0 Com Ports.
Found 9 windows drives C: D: E: F: G: H: I: J: K:
```

IF YOU ARE USING X360USB Pro

PortIO is NOT REQUIRED

Things not going as expected? – Read the FAQ's

WARNING



IF YOU SEE THIS BUTTON WHILST WORKING ON A

Phat LiteOn Drive

It is ONLY for use with Slim PCBs, Replacement 0225 PCB's and Pro-Kit Modified PCB's

DO **NOT** PRESS IT

IT WILL LOCK YOUR DRIVE!

IT IS A PAIN IN THE ASS TO UNLOCK AGAIN

WARNING

PROCEED

Which Drive do you have?

Click on the appropriate link below.

Original Xbox360

Slim Xbox360

Other Info – for troubleshooting, or the inquisitive mind

FAQ's	Advanced User Functions	VIA Ports Only / Include Non-IDE	X64 additional instructions
Support for earlier LiteOn dumps	Missing Serial Data	Return a LiteOn to Stock	Verified Lite-On Key?
Manual Spoofing	Spoofing a Hitachi	Spoofing a different drive	Thanks
Bad Flash Recovery with X360USB	PMT / Probe 3 Samsung Unlock / Recovery	What is Pógó Mo Thóin?	
PMT / Probe 3 Bad Flash Recovery Slim LiteOn	PMT / Probe 3 Bad Flash Recovery BenQ		

Things not going as expected? – Read the FAQ's

Which Phat Drive

Samsung CLICK HERE

Hitachi CLICK HERE

BenQ CLICK HERE

LiteOn CLICK HERE

You can check the Xbox 360 DVD drive type by removing the faceplate and checking the hole underneath the DVD bezel.

Red and Black Wires = Samsung	**No Wires = Hitachi**
White Wires = BenQ	**Yellow Wires = LiteOn**

For **Exact** model information of drive you must read the label on top of the drive case!

You will require this information to enable you to choose the correct methods for your drive!

Things not going as expected? – Read the FAQ's

Which Slim Drive

Currently several different slim drives exist:

LiteOn DG-16D4S (FW Ver. 9504 or if updated 0272)

The Other Drives are

LiteOn DG-16D4S (FW Ver. 0225 ,0401, 1071)

Drive Key can be dumped ONLY (unless unlocked)

Hitachi (FW Ver. 0500)

You can tell the difference between LiteOn and Hitachi by the drive tray

Hitachi Slim (N/A)	LiteOn Slim

Read the label on the drive as which LiteOn drive you have.

Note: There are also some mislabelled as 9504 and are actually 0225, the only 100% method is to connect your drive to your PC and see how it reports in Jungleflasher. If it reports as 0272 is has been updated by dashboard update 13146.

CONTINUE

Samsung (TS-H943) MS25 /MS28.

Overview.

The steps to modifying / restoring a Samsung Drive follow the basic outline of:

- Unlocking the Drive (MS28 or Xtreme 3.3+ Firmwares)
- Reading the Original firmware
- Patching Key into hacked Firmware
- Writing Drive

The tutorial covers multiple unlock methods, which are dependent upon which drive, its current firmware and your SATA chipset!

The following flowchart will help you decide which method you should use to achieve the unlocked state on a Samsung drive (Vendor Mode – status 0x70) in preparation for READING and/or WRITING to, the drive

NOTE: IF YOU HAVE NOT ALREADY DONE SO – UPDATE YOUR XBOX DASHBOARD TO THE LATEST DASHBOARD BEFORE WRITING LT+1.9FW.

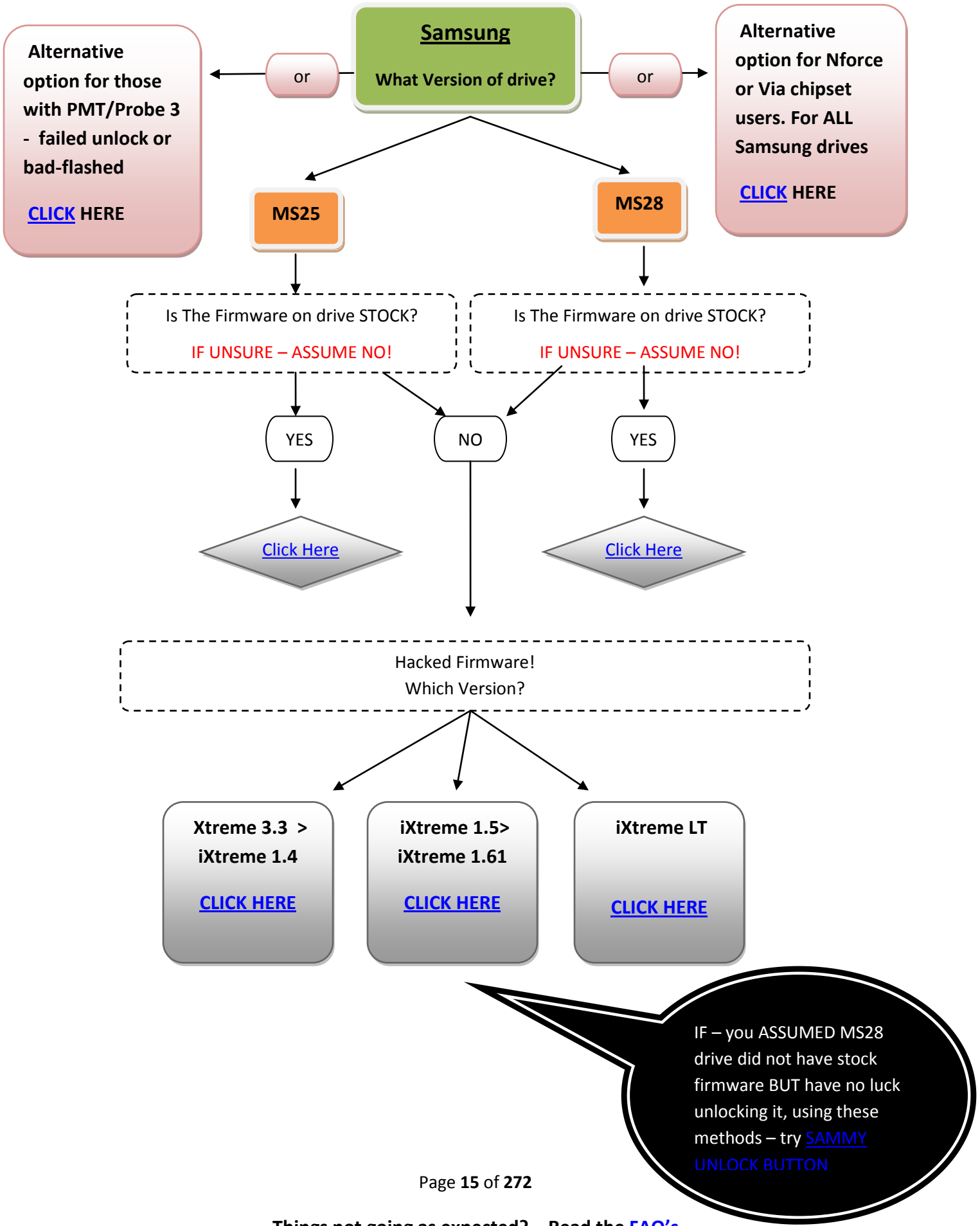
ENSURE YOUR DRIVE IS STOCK BEFORE CARRYING OUT THE DASHBOARD UPDATE

Now, we can proceed to modifying the drive.

Power drive with it connected to PC via SATA then open JungleFlasher.exe. You will be presented with the Welcome Screen.

After a few seconds the main window will load.

Follow the flowchart below to obtain the correct method for your setup and drive!



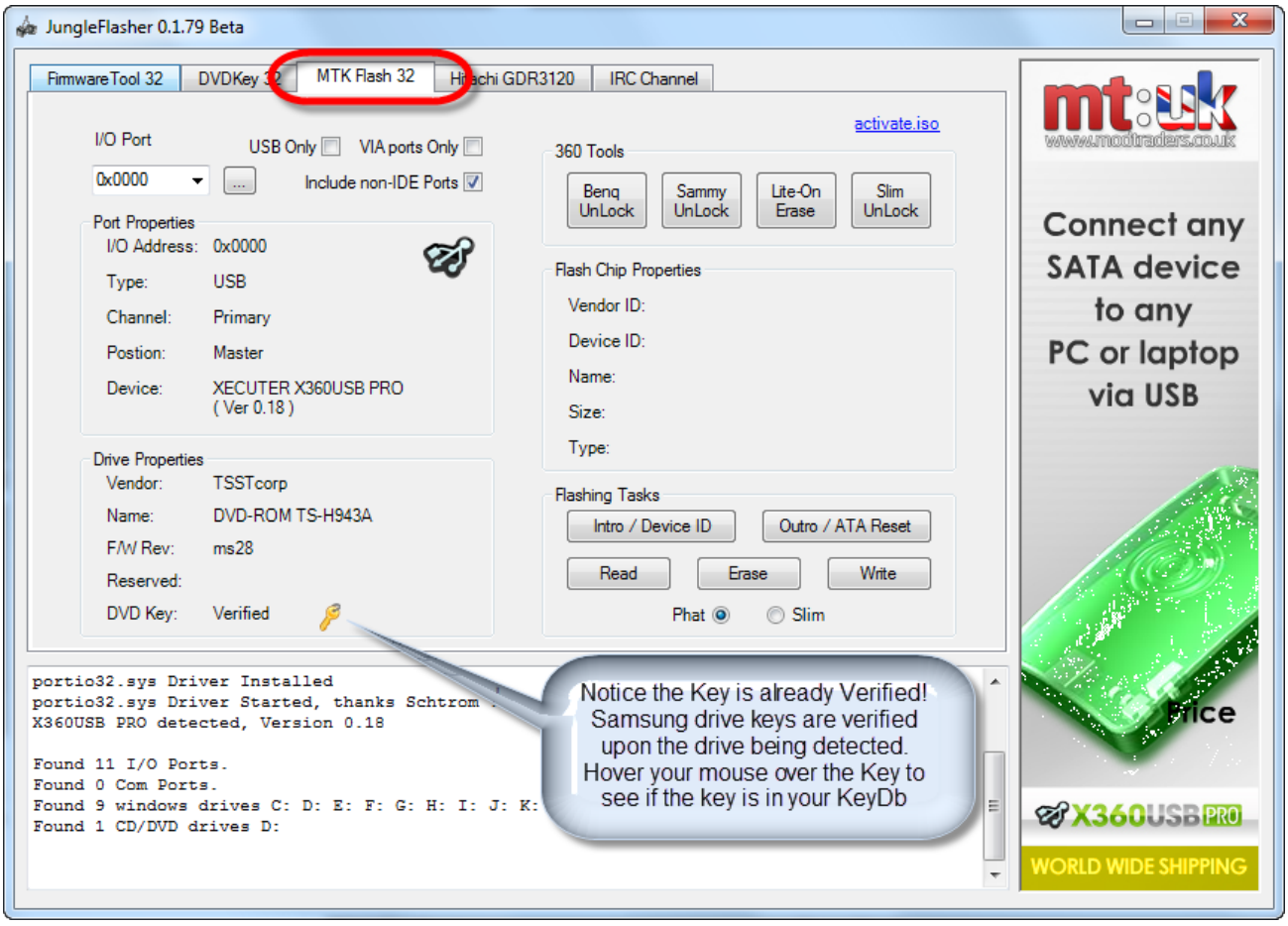
Things not going as expected? – Read the FAQ's

Unlocking the drive.

Before we can do anything to the drive, it must be in Vendor Mode (status 0x70).

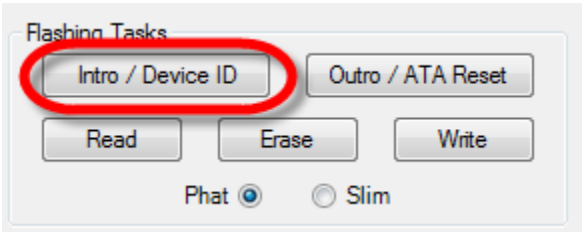
All Unlocking is taken place under the **MTKFlash 32** tab.

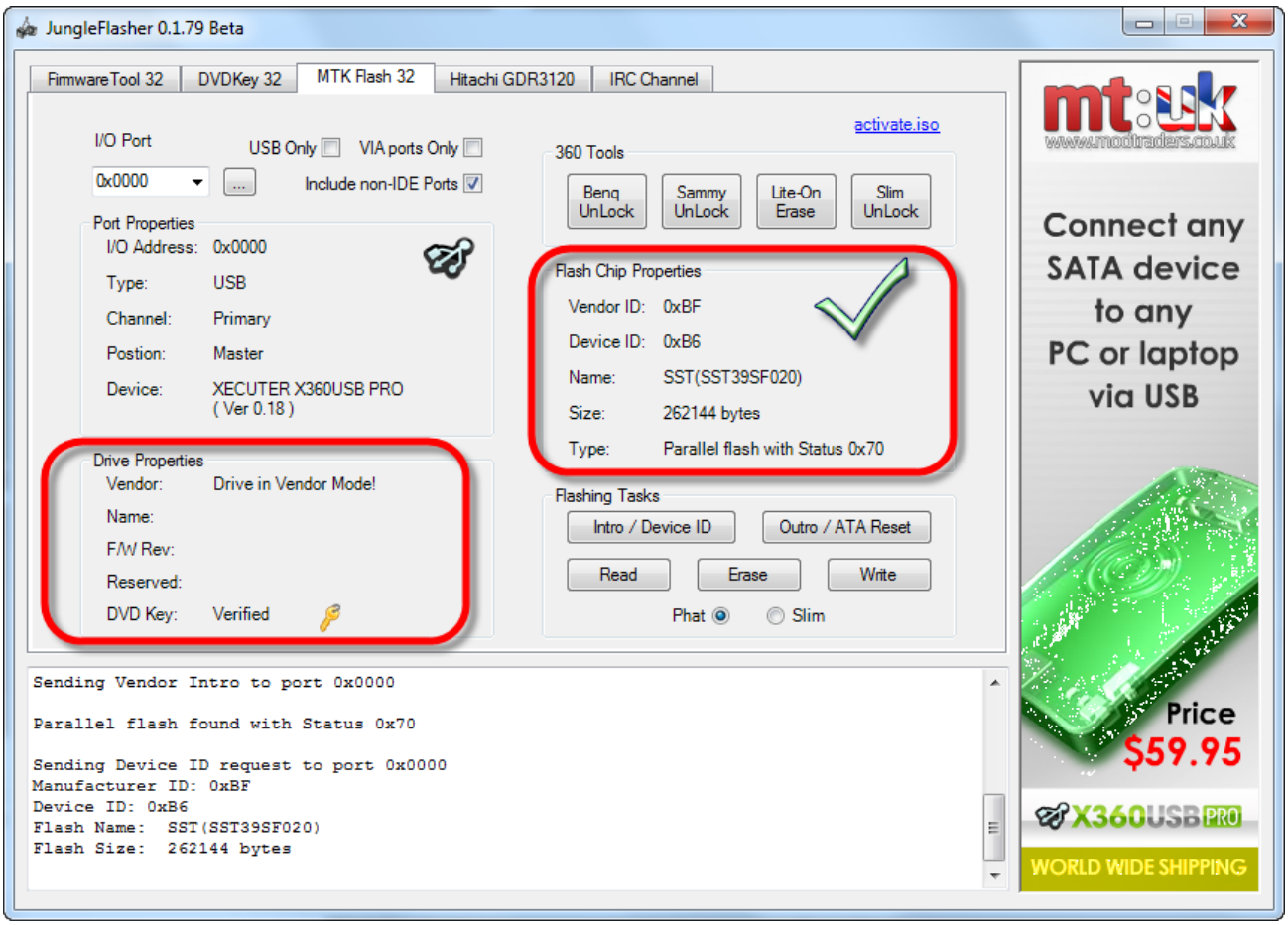
Note: Upon selecting the correct port the drive shows up and key is dumped and verified against the drive! (Before doing anything to the drive) – The firmware has NOT yet been dumped! However if you save the log you now have a known verified key from your drive.



Please note, unmodified **Samsung MS25's** have no **FirmGuard** therefore do not need an unlock method to be applied, simply click **Intro / DeviceID** and check flash chip properties for status 0x70.

Things not going as expected? – Read the FAQ's





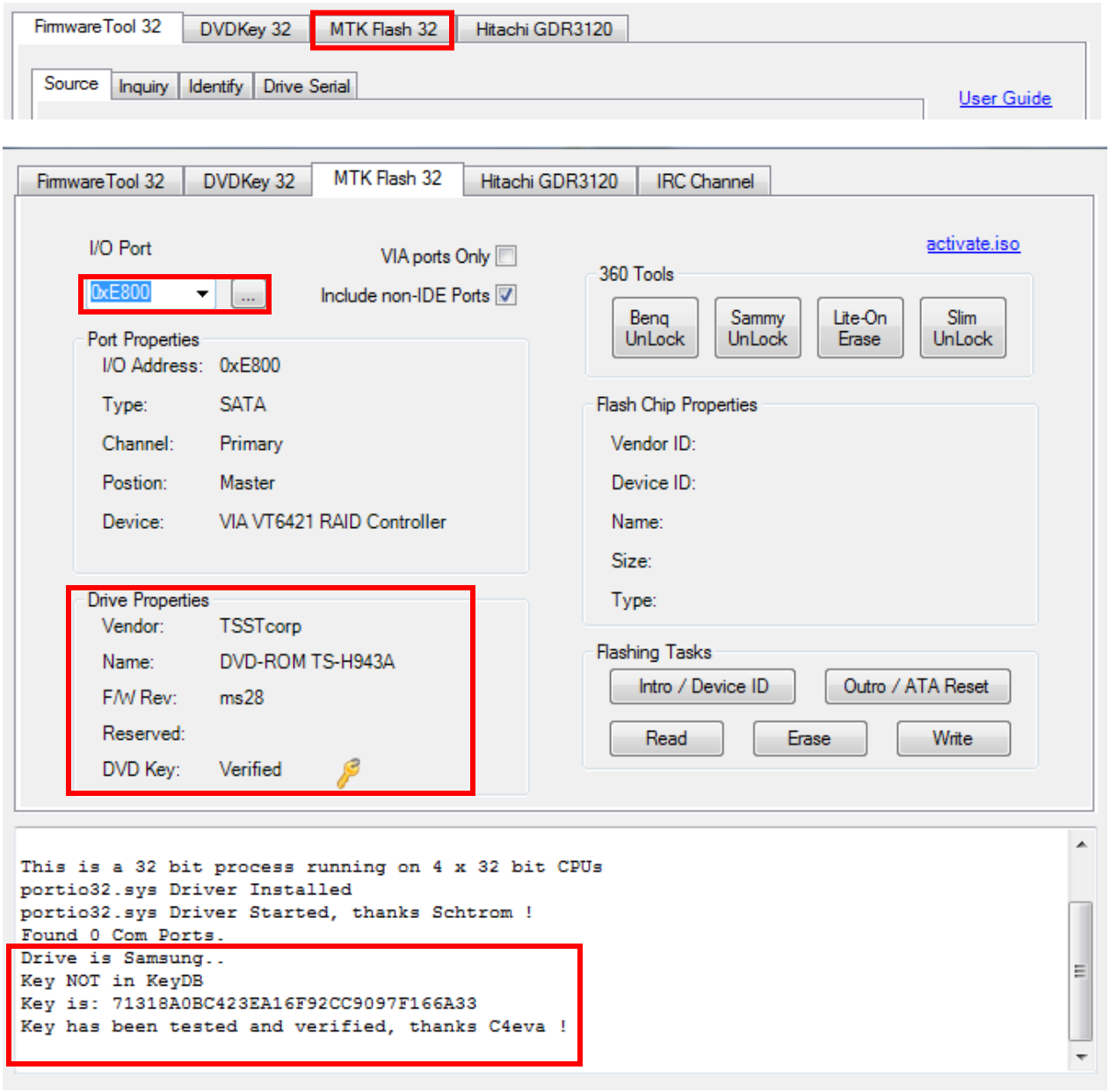
Now CLICK HERE to proceed

Things not going as expected? – Read the FAQ's

Unlocking the drive.

Before we can do anything to the drive, it must be in Vendor Mode (status 0x70).

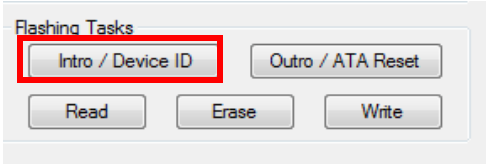
All Unlocking is taken place under the **MTKFlash 32** tab.

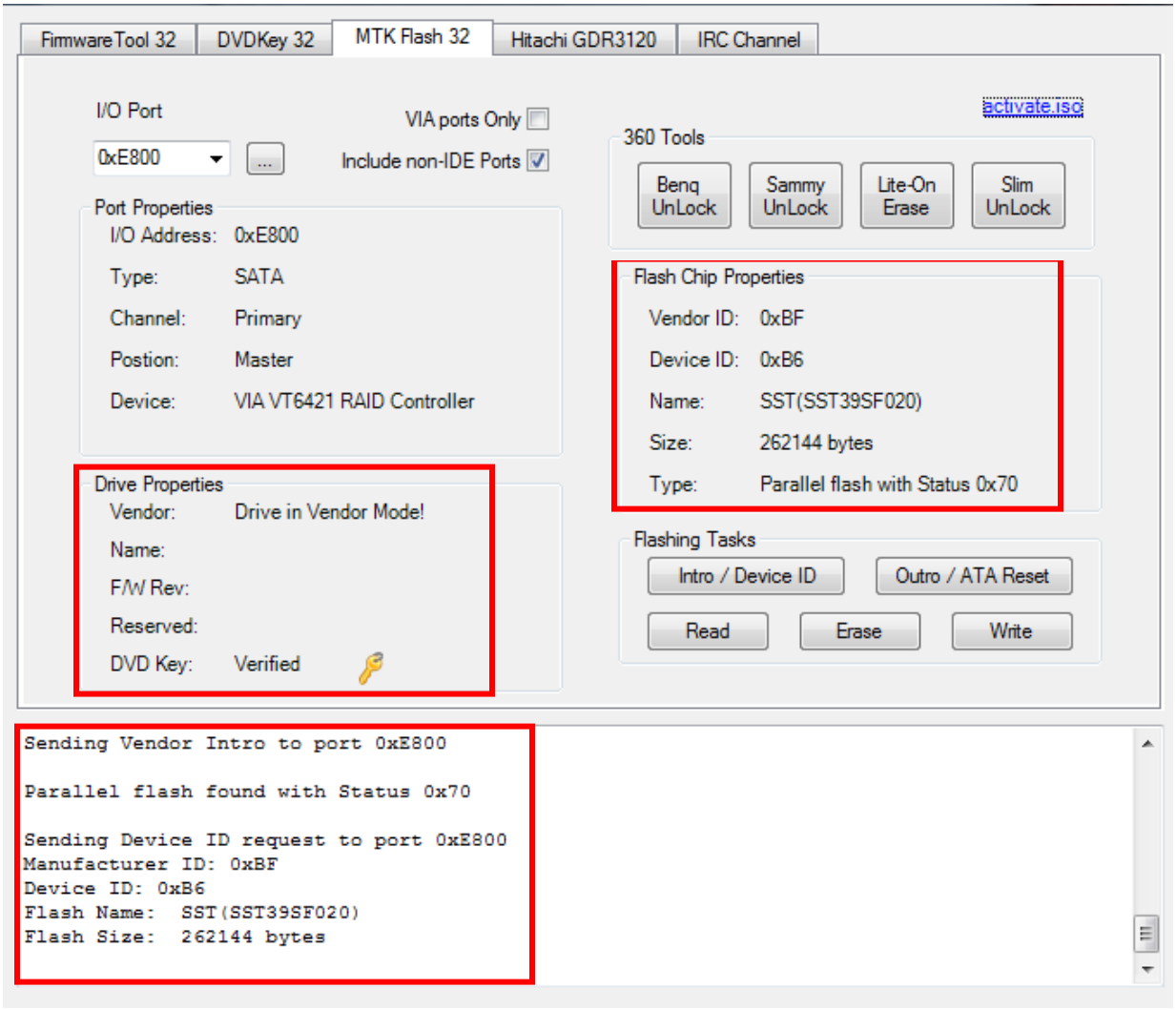


Note: Upon selecting the correct port the drive shows up and key is dumped and verified against the drive! (Before doing anything to the drive) – The firmware has NOT yet been dumped! However if you save the log you now have a known verified key from your drive.

Things not going as expected? – Read the FAQ's

Simply click **Intro / DeviceID** and check flash chip properties for status 0x70.





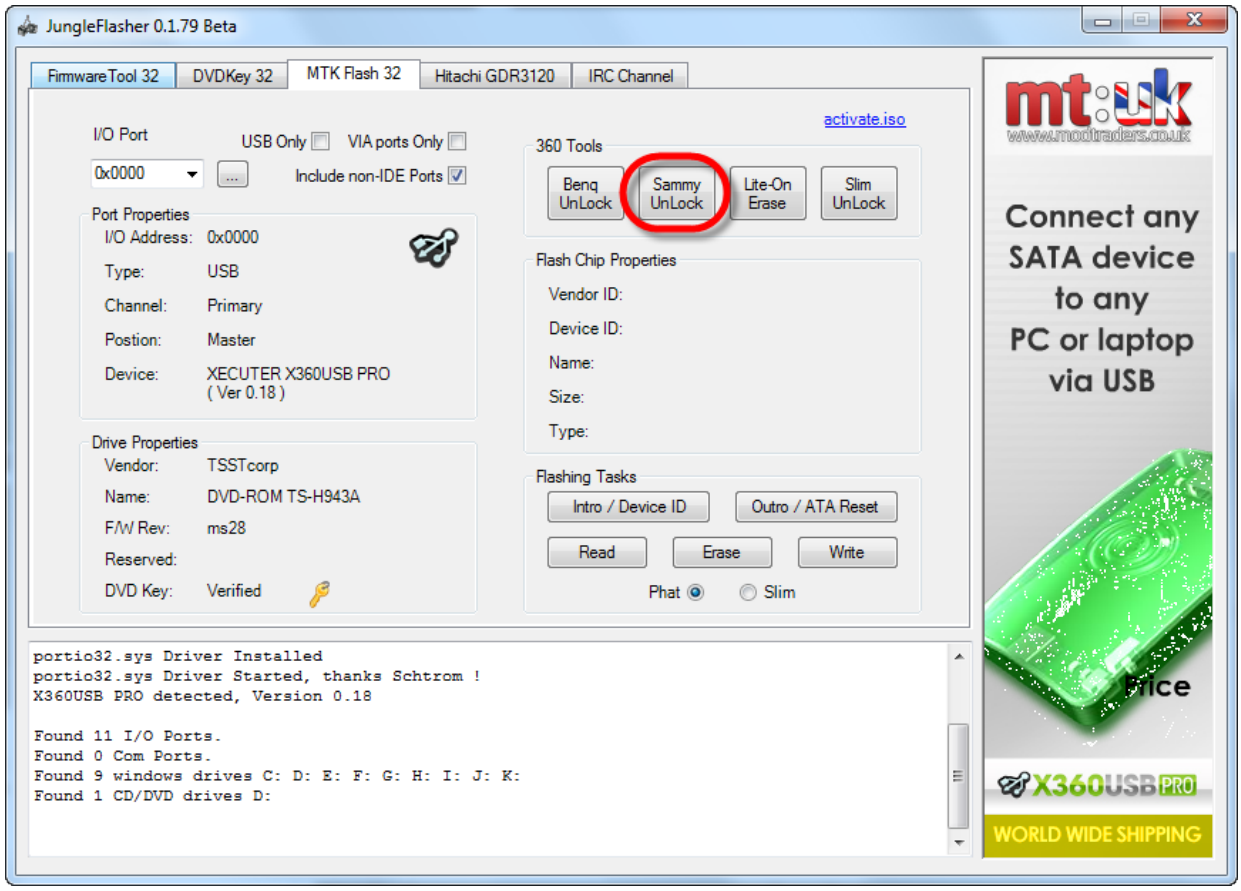
Now CLICK HERE to proceed

Things not going as expected? – Read the FAQ's

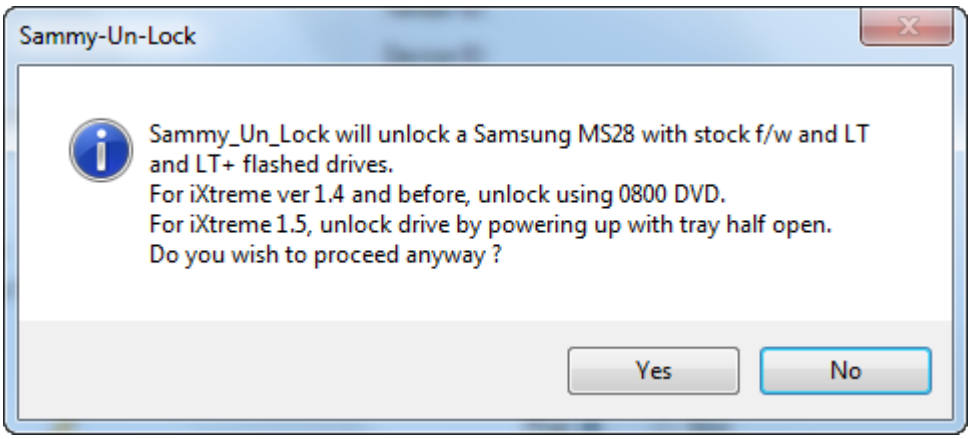
Stock MS28's (Unmodified).

Sammy Unlock.

Select correct **I/O Port (check for TS-H943 in the Drive Properties)** and click **Sammy Unlock.**



You will be presented with the following warning notifying you that Sammy Unlock only works on stock drives & drives with iX LT firmware and how to unlock if using (i)Xtreme.

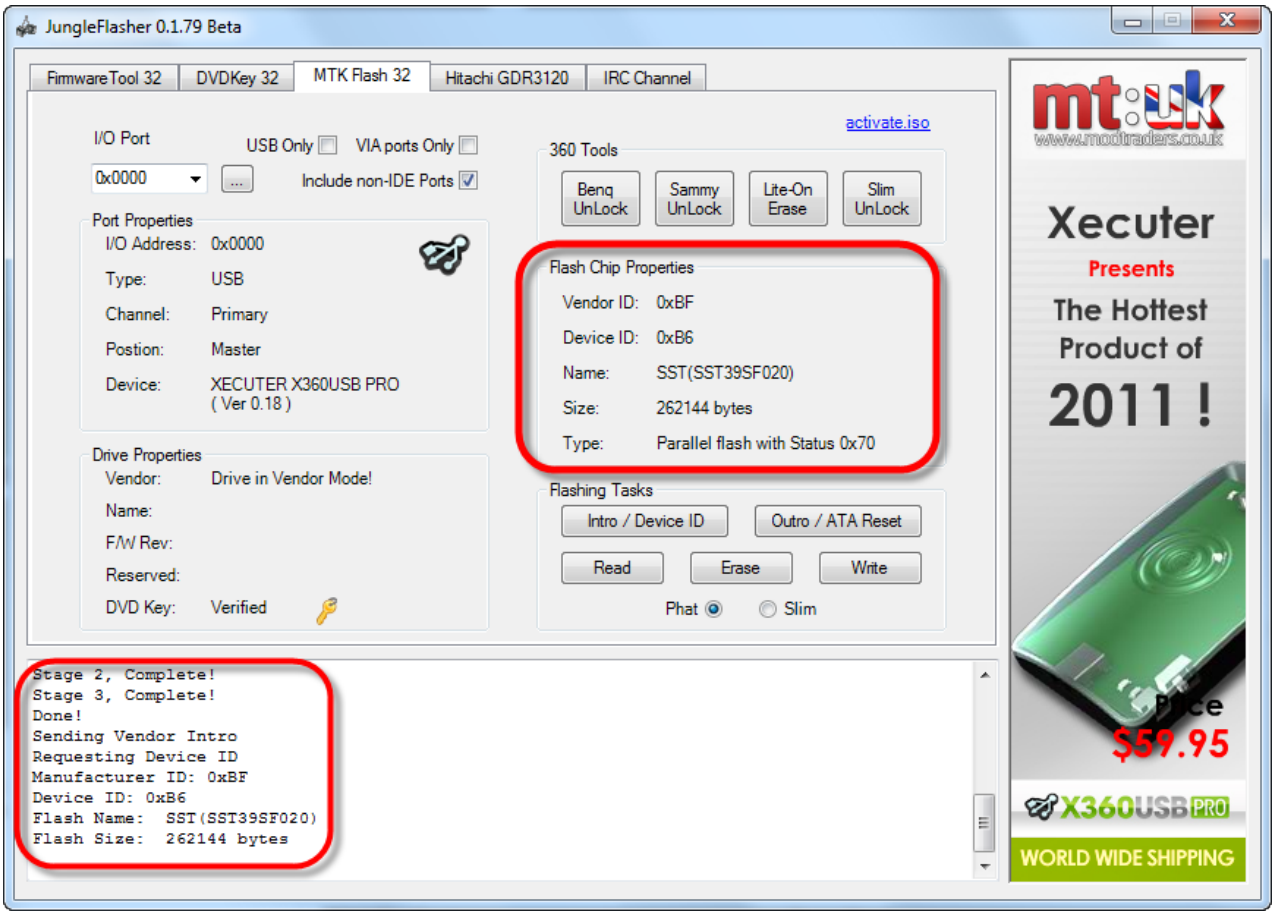


Things not going as expected? – Read the FAQ's

Select yes and watch the **Running Log** in JungleFlasher; this is a 'good' return message, JungleFlasher will also automatically send the intro command and put the drive in **Vendor Mode**.

```
Sending Sammy_Un_Lock to Drive on port 0xE800
Stage 1, Complete!
Stage 2, Complete!
Stage 3, Complete!
Done!
Sending Vendor Intro
```

The drive should be in Vendor Mode (0x70) now and return good flash chip properties; you can check under **Flash Chip Properties, Drive Properties** should show **"Drive in Vendor Mode!"**

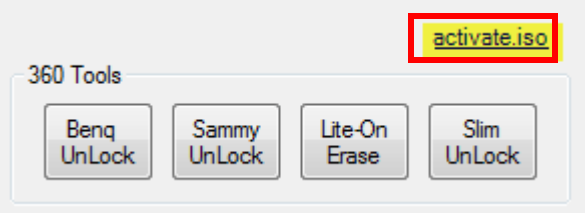


[Now CLICK HERE to proceed]

Things not going as expected? – Read the [FAQ's]

Xtreme 3.3 -> iXtreme 1.4 Unlock using Activate.iso.

For this you need the Activate.iso found in the upper right hand corner of the **MTKFlash 32** tab,



burnt to **Dual Layer + R Media** (this is vital for later firmwares). Simply burn it with no layerbreak settings, with all data present on first Layer, IMGBurn 2.5.0.0 will do this fine just select the ISO and confirm you want to burn to a large capacity disc with all data present on L0 (Layer 0).

Once burned, simply place it in your Samsung drive while connected to the PC, wait 30 seconds and run JungleFlasher.

Unlocking the drive.

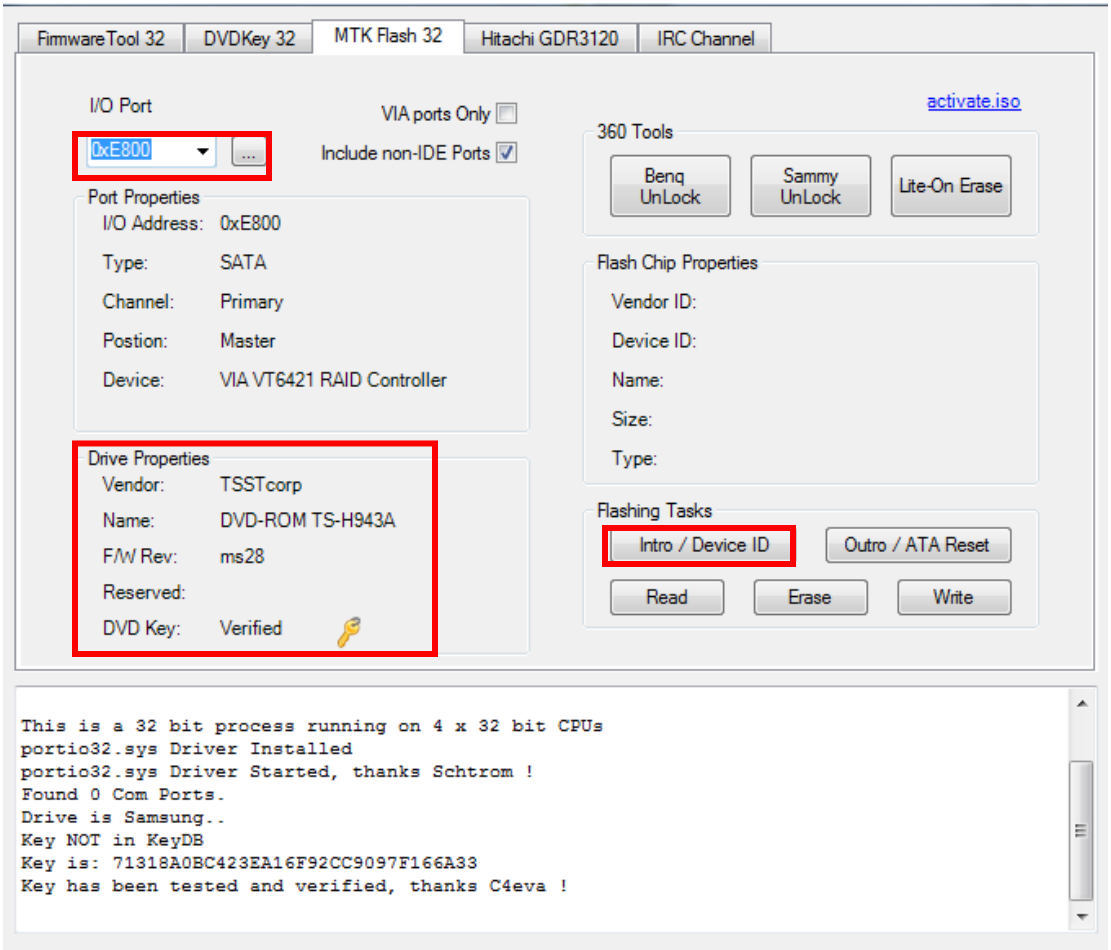
Before we can do anything to the drive, it must be in Vendor Mode (status 0x70).

All Unlocking is taken place under the **MTKFlash 32** tab.

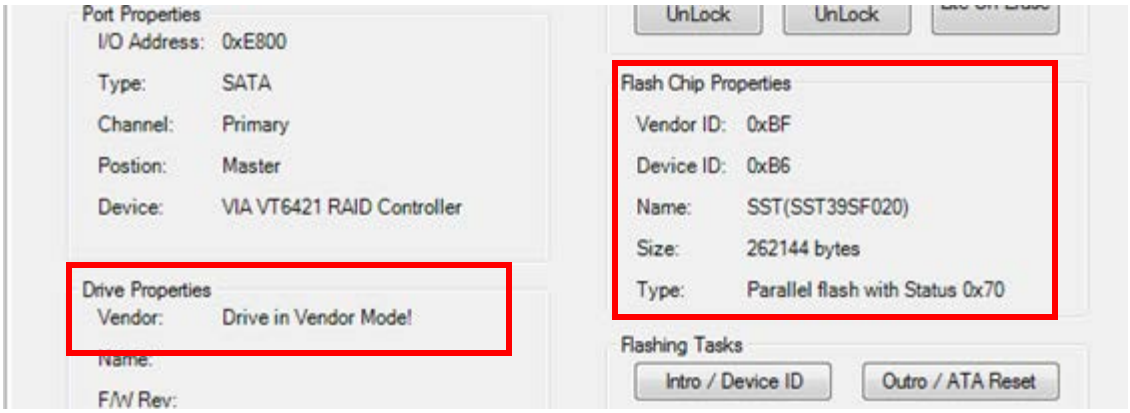
You will presented with a screen resembling this, select correct **I/O Port (check for TS-H943 in the Drive Properties)**

click **Intro / Device ID** and then check the **Running Log.**

Things not going as expected? – Read the FAQ's



If Activate.iso worked correctly, you will get good **flash chip properties (0x70)** and drive will appear in **Vendor Mode** in **Drive Properties.**



Now CLICK HERE to proceed

Things not going as expected? – Read the FAQ's

Unlocking iXtreme 1.5 > 1.61

For this method, we still need to power on the drive with the "half open tray".

If using a 360 to power the drive

This method can be tricky to accomplish.

You need to power on the drive with **Eject status closed** but **Tray Half Open** – To do this using an Xbox 360 as Power source, eject the DVD drive, then, press eject to 'close' the tray. **Now this is the important part – you MUST remove the DVD power plug from the DVD Drive BEFORE it closes fully.**

Wait for a few seconds and replace the power plug into the DVD drive taking **extreme caution** to plug the plug the right way around – once done, the drive is now powered, console thinks its closed but it is in fact half open.

If using a connectivity kit to power the drive

You need to power on the drive with **Eject status closed** but **Tray Half Open** – To do this using a connectivity kit as Power source, eject the DVD drive, then, press eject to 'close' the tray. **Now this is the important part – you MUST switch off the power BEFORE it closes fully.**

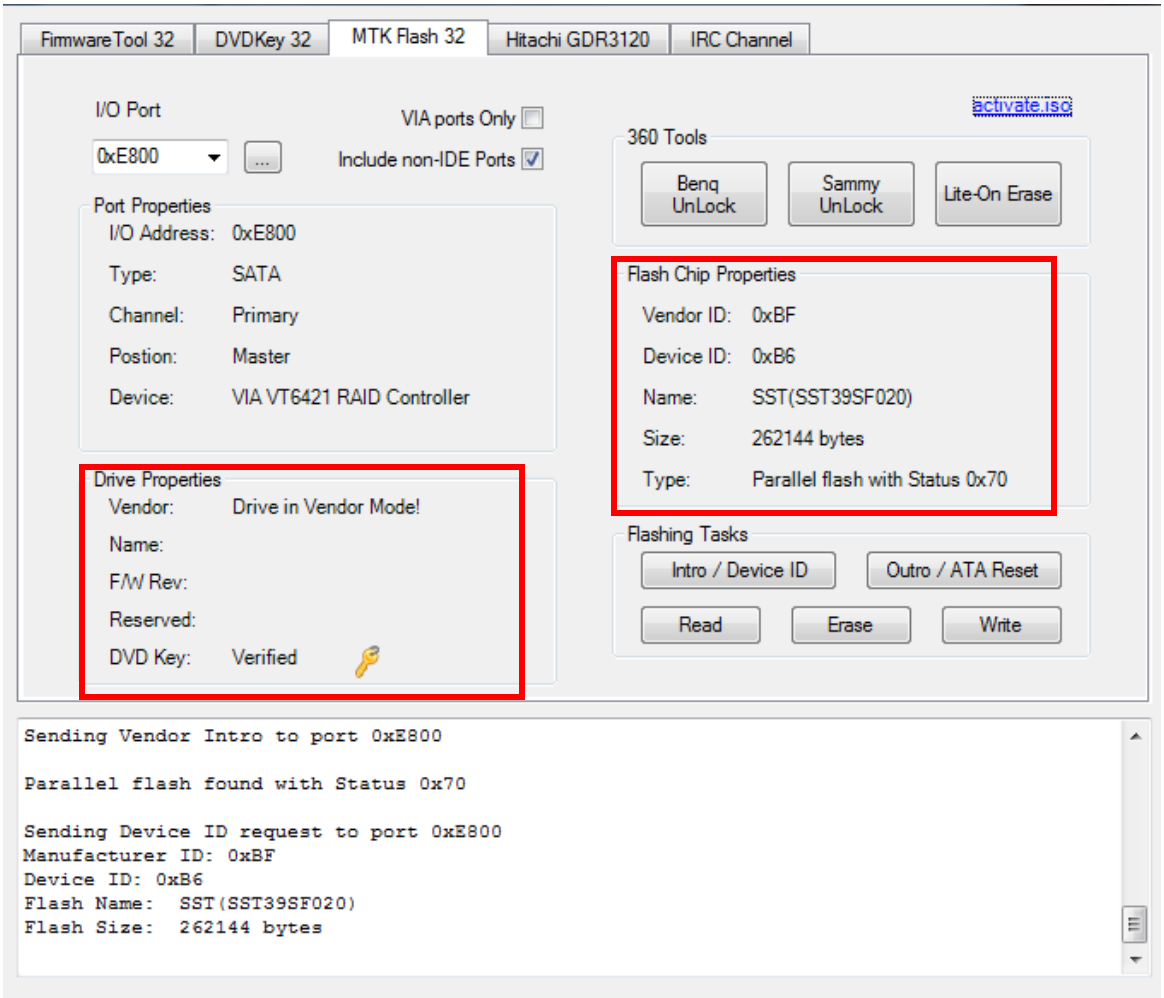
Wait for a few seconds and switch power on connectivity kit back on – once done, the drive is now powered, console thinks its closed but it is in fact half open.

Load JungleFlasher, and select **MTKFlash 32** tab.

Press **Intro / Device ID** button

The drive should be in Vendor Mode (0x70) now and return good flash chip properties, you can check in the **Running Log** or **Flash Chip Properties,** The drive should also show as "**Drive In Vendor Mode!"** in the **Drive Properties.**

Things not going as expected? – Read the FAQ's



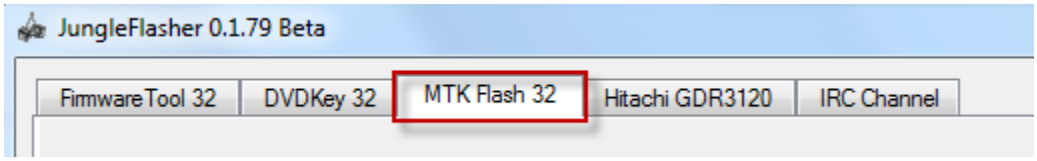
Now CLICK HERE to proceed

Things not going as expected? – Read the FAQ's

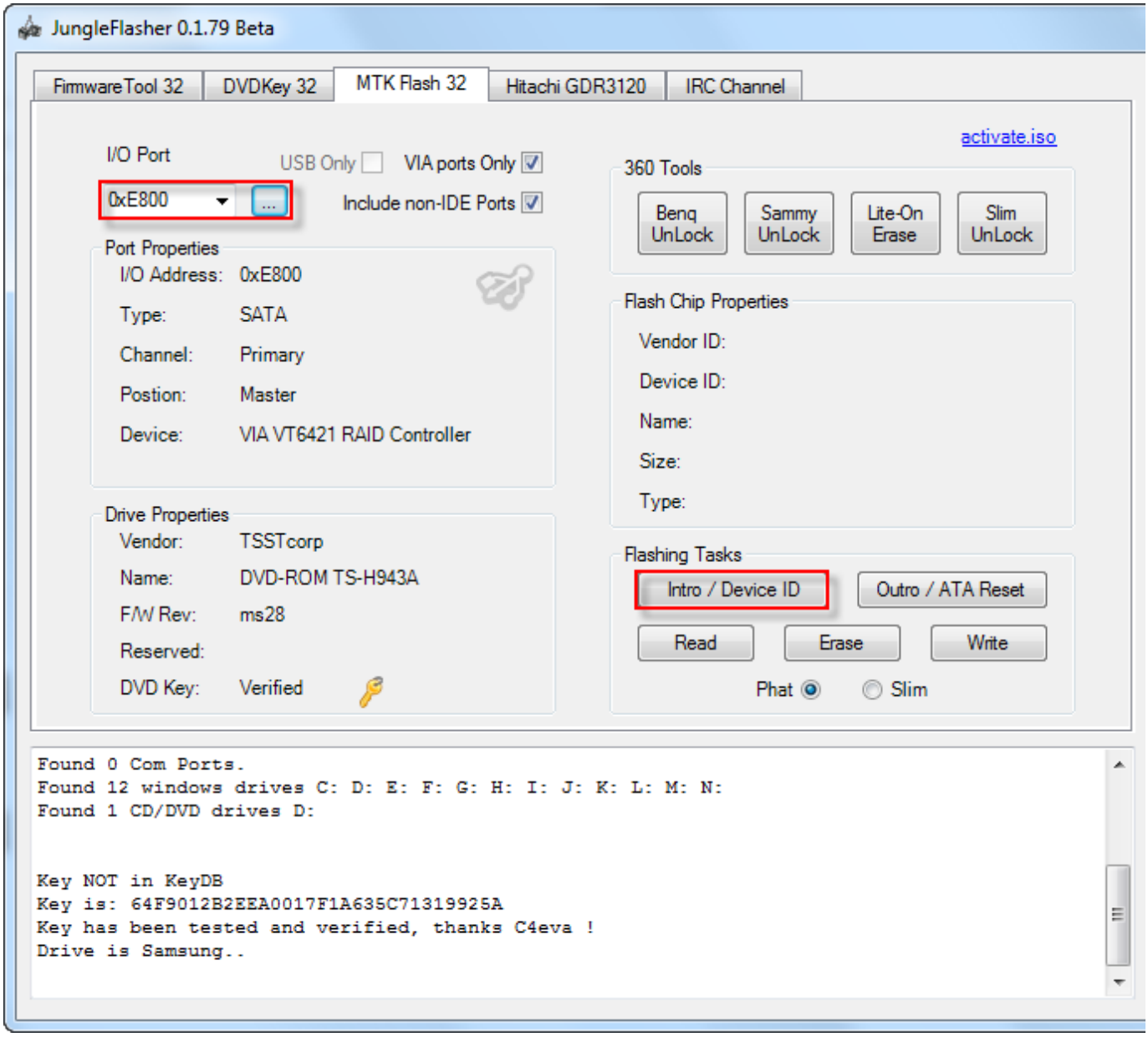
DeviceID Unlock / Vcc Trick (VIA/Nforce only) Stock + Modified Drives.

This method has only really been tested on VIA **(no drivers, or 530c drivers)** and Nforce Chipsets, although there is no harm in trying on others, this method works on Hacked and Stock Drives.

Load JungleFlasher, and select **MTKFlash 32** tab.

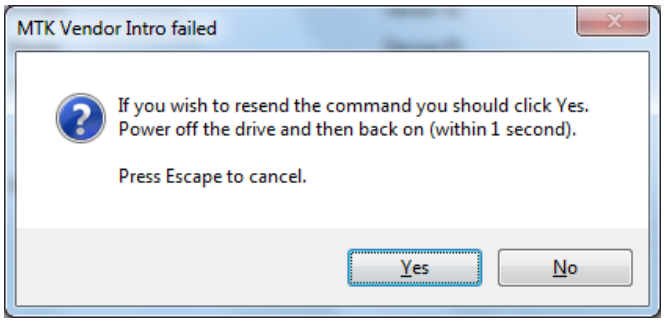


Select correct **I/O Port (check for TS-H943 in Drive Properties)** and click **Intro / Device ID.**



Things not going as expected? – Read the FAQ's

JungleFlasher will prompt you with instructions.

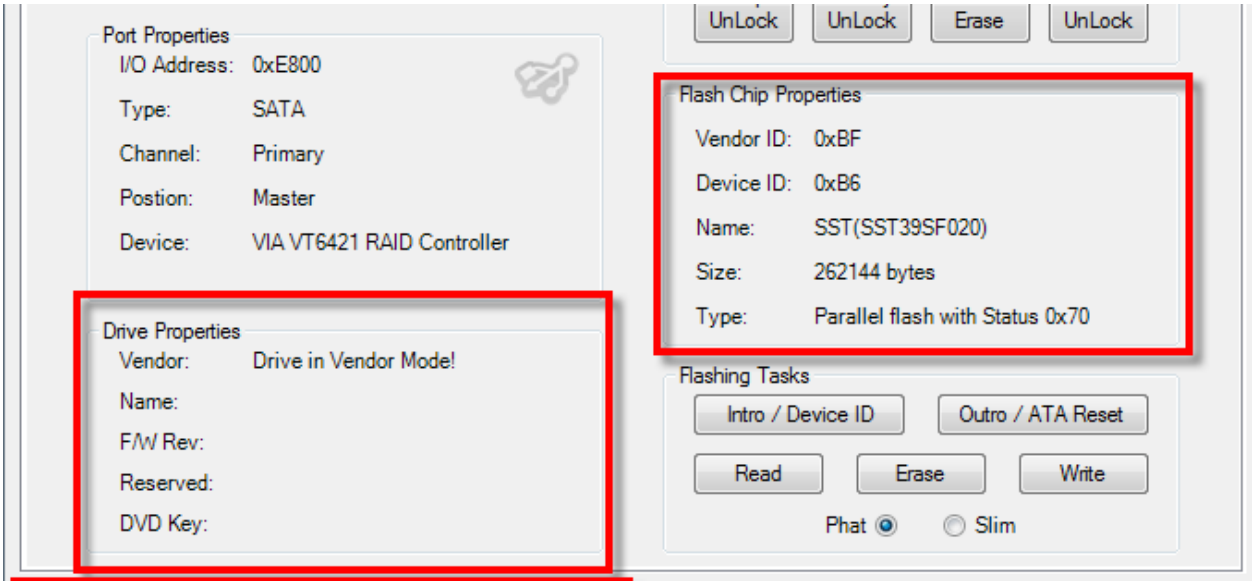


Click **Yes** the **Running Log** will display something similar to this.

```
Sending Vendor Intro to port 0xCF00
Invalid Status
Re-sending Vendor Intro:
.............
```

When **…….** Are appearing, do as previously instructed by JungleFlasher. Power off the drive then, **within 1 second,** power it back on.

The drive should be in Vendor Mode (0x70) now and return good flash chip properties, you can check in the **Running Log** or **Flash Chip Properties,** The drive should also show as "**Drive In Vendor Mode!"** in the **Drive Properties.**



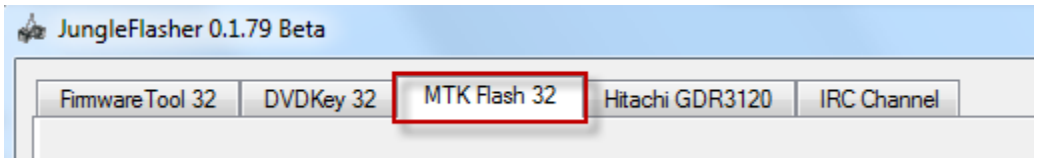
Now CLICK HERE to proceed

If it didn't work – read on

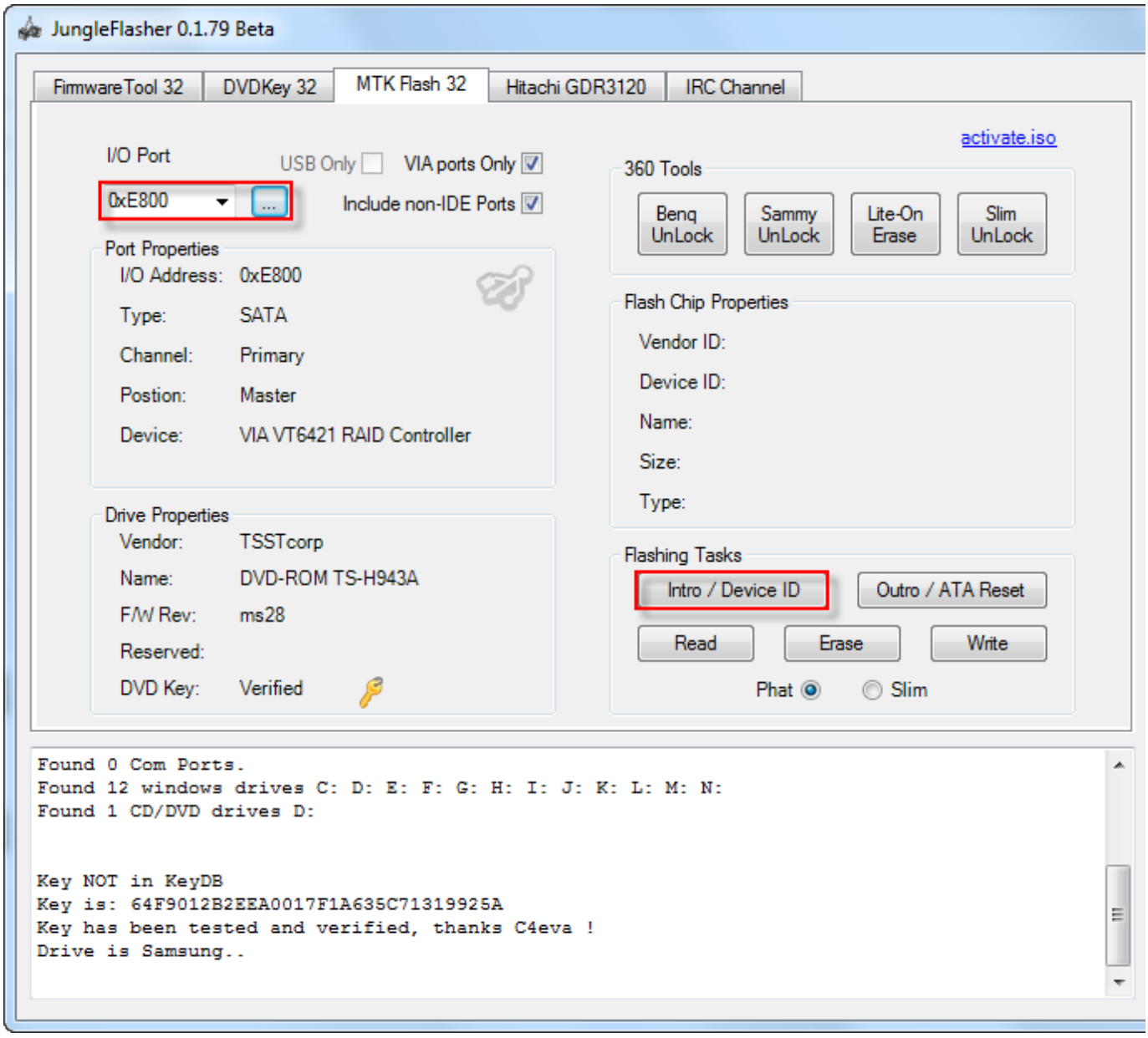
Things not going as expected? – Read the FAQ's

Alternate method if you are struggling with the above

Load JungleFlasher, and select **MTKFlash 32** tab.

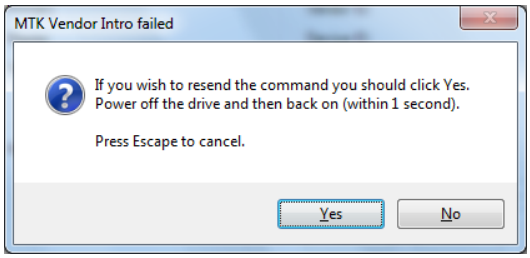


Select correct **I/O Port (check for TS-H943 in Drive Properties)** and click **Intro / Device ID.**



Things not going as expected? – Read the FAQ's

JungleFlasher will prompt you with instructions.



Now power **off** the drive!

Then click **YES,**

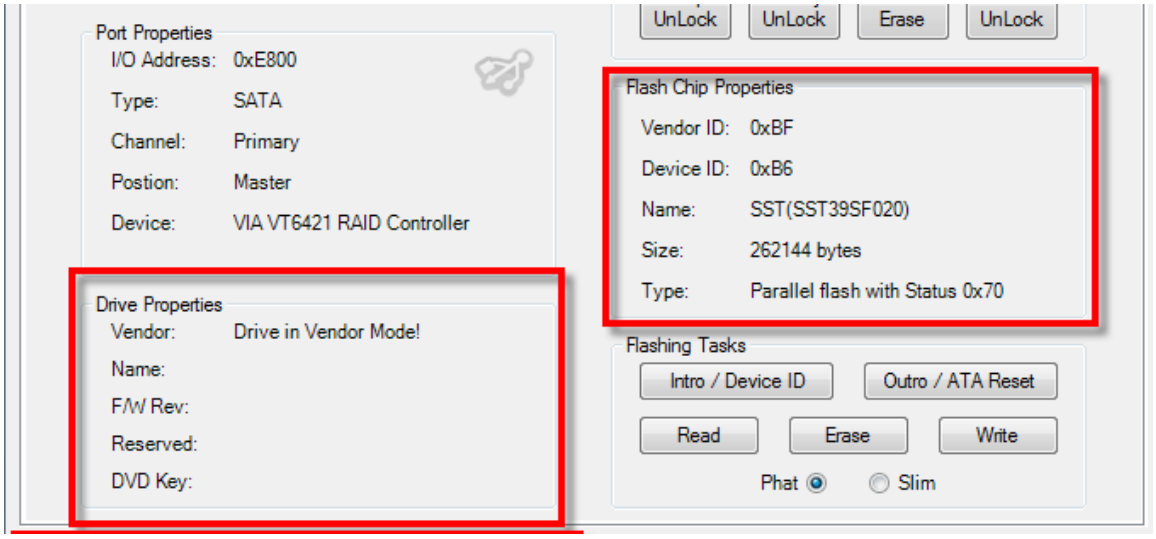
Click **Yes** the **Running Log** will display something similar to this.

```
Sending Vendor Intro to port 0xCF00
Invalid Status
Re-sending Vendor Intro:
..............
```

When **…….** Are appearing,

power **ON** the drive!

The drive should be in Vendor Mode (0x70) now and return good flash chip properties, you can check in the **Running Log** or **Flash Chip Properties,** The drive should also show as "**Drive In Vendor Mode!"** in the **Drive Properties.**

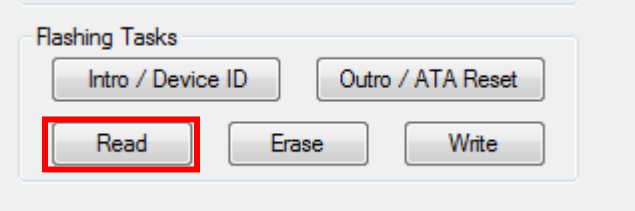


Now CLICK HERE to proceed

Things not going as expected? – Read the FAQ's

Reading the Firmware from the drive.

Now, we would like to read the firmware from the drive first, so select **read.**

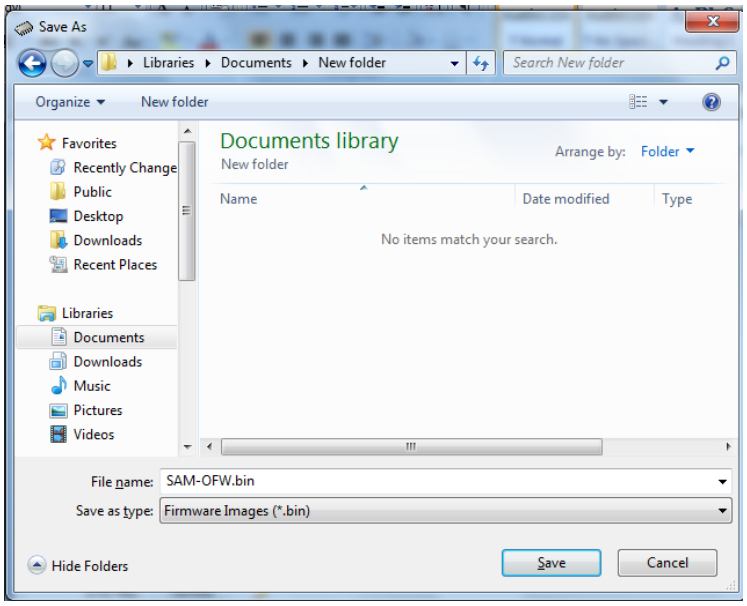


Again, watch the **Running Log** for constant status updates.

Firmware reading:

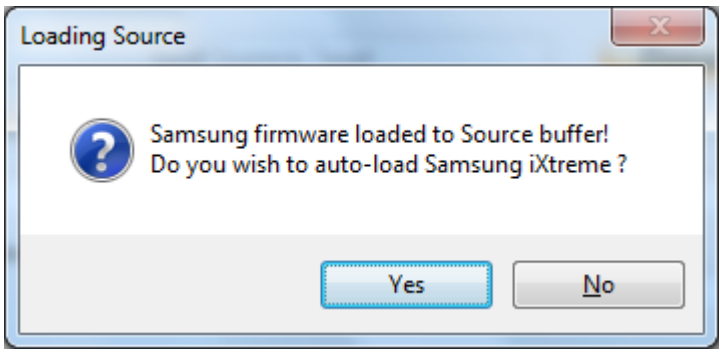
```
Getting Status from port 0xE800
Parallel flash found with Status 0x70

Reading Bank 0: ...............
Reading Bank 1: ...............
Reading Bank 2: ...............
Reading Bank 3: ...............
```

Once the firmware has been successfully read, JungleFlasher will prompt you to save it.



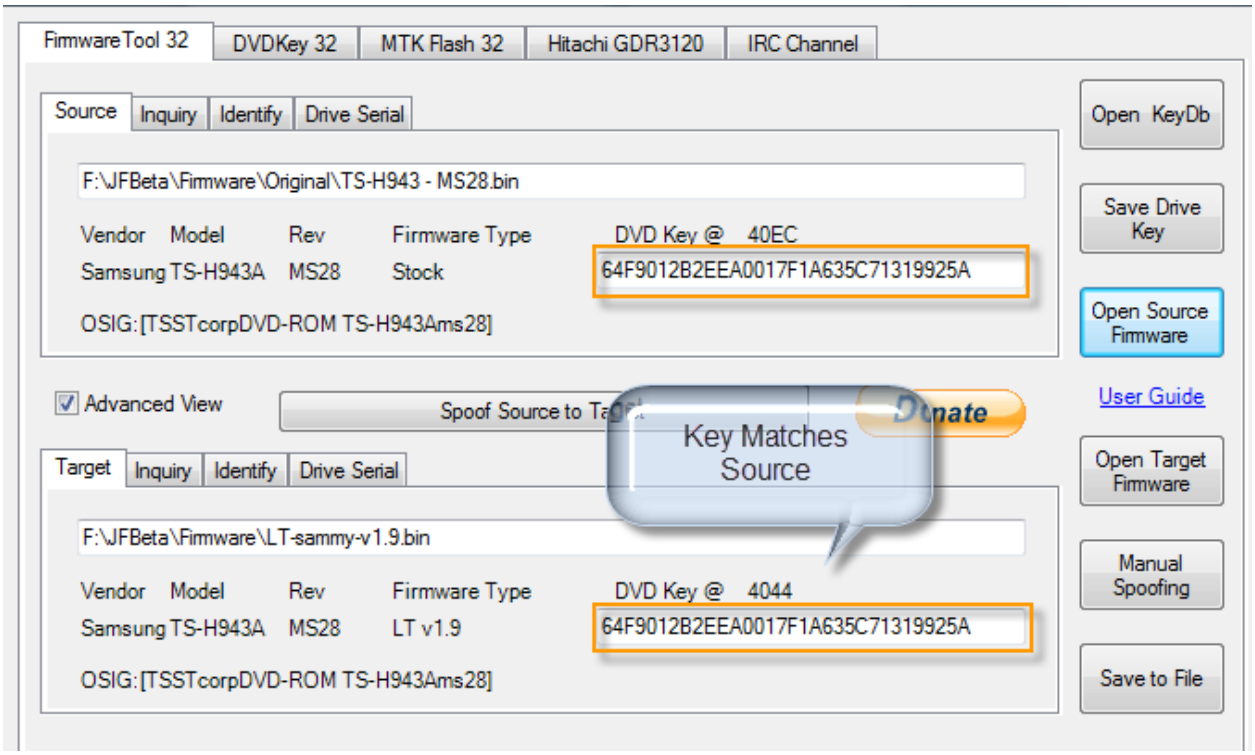
Once saved, JungleFlasher will then prompt you asking if you would like to auto-load iXtreme for Samsung Drives. You must have installed the **JungleFlasher Firmware Pack** into the same directory as JungleFlasher.exe if you wish to benefit from this feature.

IF YOU NEED TO RETURN TO STOCK FOR DASH UPDATE CLICK HERE



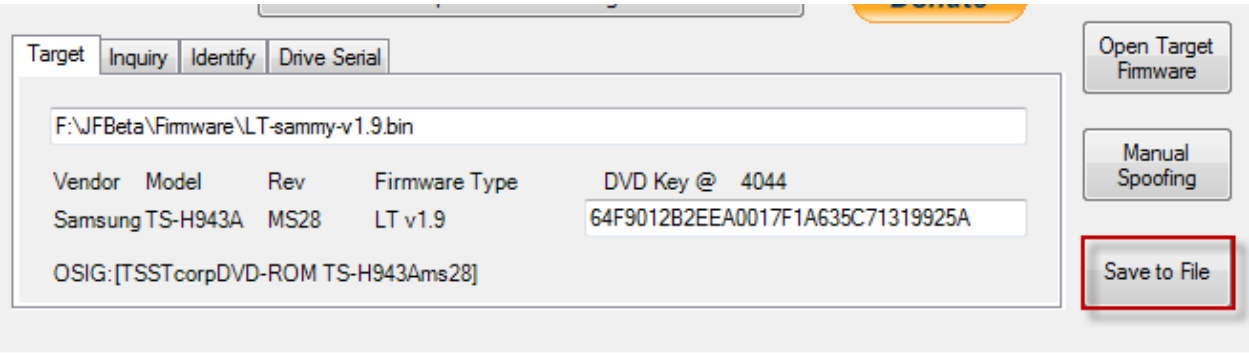
Click **Yes** to auto load iXtreme (from the firmware pack) for Samsung into the **Target Buffer**, JungleFlasher will also load your previously dumped **Sam-OFW.bin** as **Source Firmware.** Then, copy data from **Source to Target automatically.**

Just verify **Source data** reports as it should, OSIG of **TSSTcorpDVD-Rom TS-H943** with a key with no multiple **FF / 00 / 77 bytes**



To save a firmware file based on what's currently in **Target Buffer** click, **Save to File.**

Things not going as expected? – Read the FAQ's



JungleFlasher will ask you where to save the hacked firmware and what you want to name it, and then you can proceed to write the firmware to the drive.

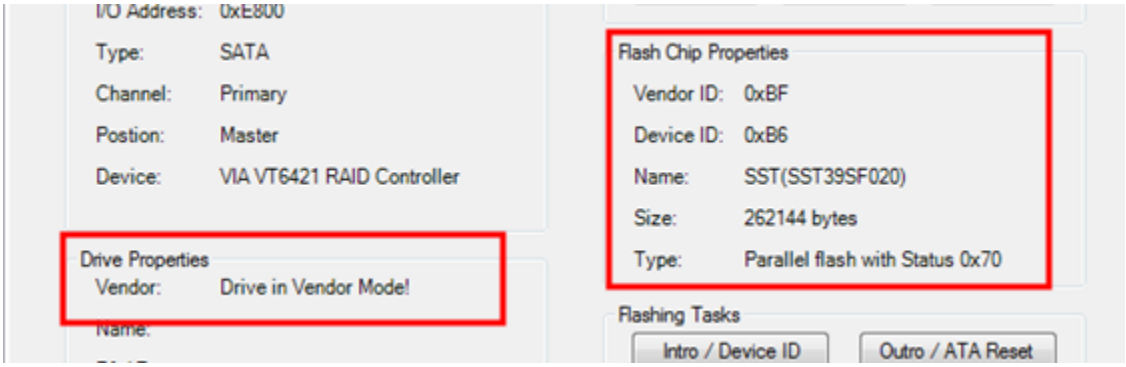
PROCEED

Things not going as expected? – Read the FAQ's

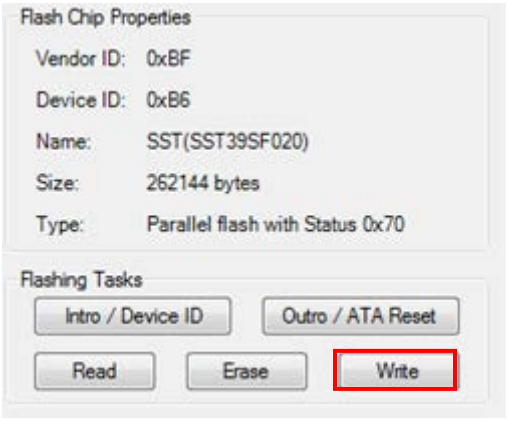
Writing Firmware to the drive

To write the firmware, as long as drive is still unlocked (Vendor Mode) we just click **MTKFlash 32** tab.

Verfify you have good flash chip properties still.



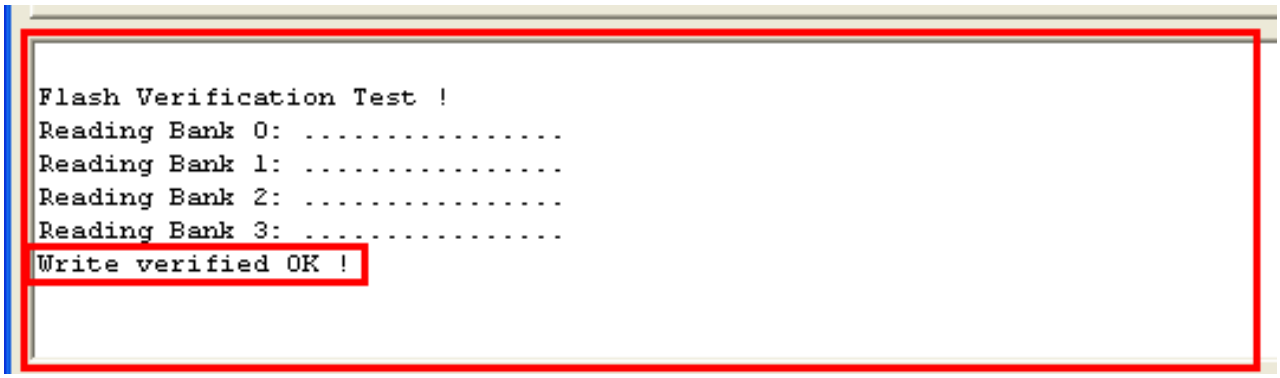
Then, click **Write.**



Write Command, will erase and flash all 4 banks in turn, then read back the flash and verify.

A series of 16 …..'s is JungleFlasher writing the 16 sectors of each bank (4 banks, 0/1/2/3)

After writing all 64 sectors, signaled by 64 dots (16 dots across 4 banks) JungleFlasher will verify what it wrote by reading back and comparing against the **Target Buffer**. So, what we really want to see is **Write Verified OK!**



Ok, now you have flashed your Samsung Drive successfully,

Power off – connect back to console and test!

Should you not get **Write Verified OK!** Please ask for support in the JungleFlasher support channel, found at **irc.efnet.net -** channel **#JungleFlasher, or click HERE**

If you have just Returned your drive to stock Firmware to allow you to update the console – then update your console using Xbox Live, USB or CD (all explained on Xbox Live).

Then return to the start and follow the tutorial for a STOCK drive.

RETURN TO START OF TUTORIAL

BenQ VAD6038 (62430c and 64930c)

Overview

The BenQ Drive revision is tackled in a very similar way to the Samsung Drives.

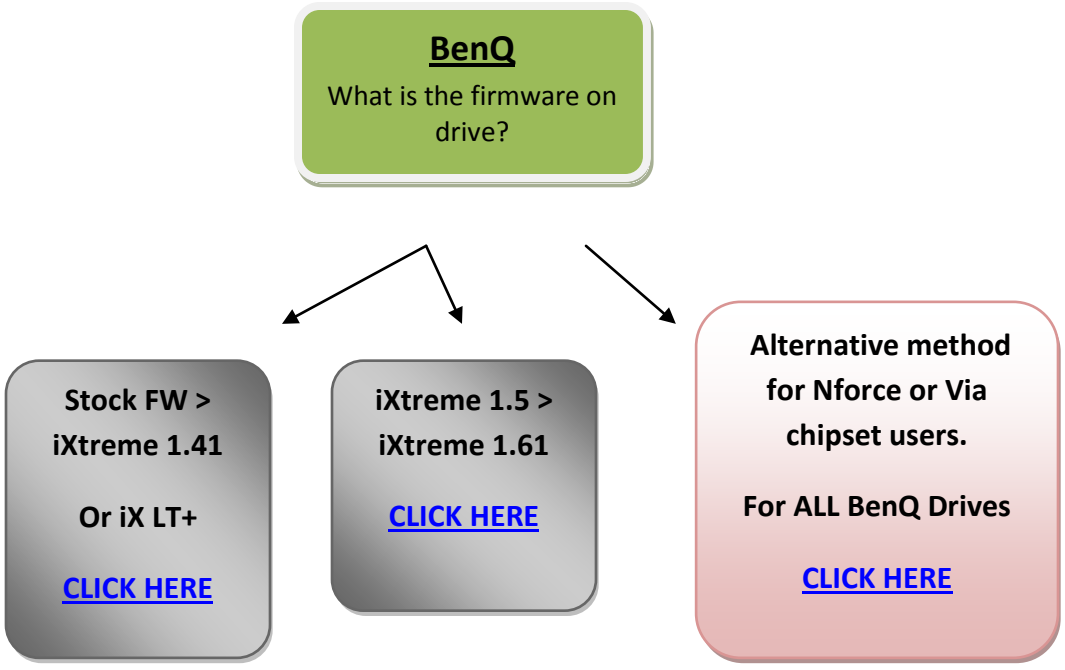
The steps to modifying / restoring a BenQ Drive follow the basic outline of:

- Unlocking the Drive
- Reading the Original firmware
- Patching Key into hacked Firmware
- Erasing Drive
- Writing Drive

The tutorial will state multiple unlock methods, once drive is **Unlocked / In Vendor Mode (0x73)** you should proceed to the next step of **reading the firmware** from the drive.

The following Flowchart Enables you to use the correct method for your drive!

NOTE: IF YOU HAVE NOT ALREADY DONE SO – UPDATE YOUR XBOX DASHBOARD TO THE LATEST DASHBOARD BEFORE WRITING LT+1.91 FW . A POST DASH UPDATE DRIVE WILL BE STOCK (04420 FW)



Things not going as expected? – Read the FAQ's

Unlocking the drive.

Before we can do anything to the drive, it must be in Vendor Mode (status 0x73), the majority of the unlock methods are found under **MTKFlash32** tab,

Half Open Tray Unlock for iXtreme 1.5 > iXtreme 1.61.

If using a 360 to power the drive this method can be tricky to accomplish as the 360 likes to close the DVD Drive after powering it on.

You need to power on the drive with the **Tray Half Open** – To do this using an Xbox 360 as Power source, eject the DVD drive and then **remove the power lead from the Drive.**

Close the tray half way and plug the DVD Drive power cable back into the drive, being VERY cautious to ensure the plug is the right way around.

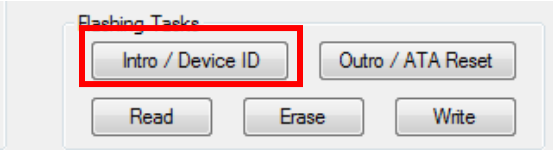
Using a Connectivity Kit / Xtractor to power the drive.

The easiest way to do this is to simply use the eject button on your connectivity kit to eject the drive tray, power off the connectivity kit, push the tray half in and power back on the connectivity kit.

Ok, now we half the half open tray, we navigate to **MTKFlash32** tab if you haven't already.

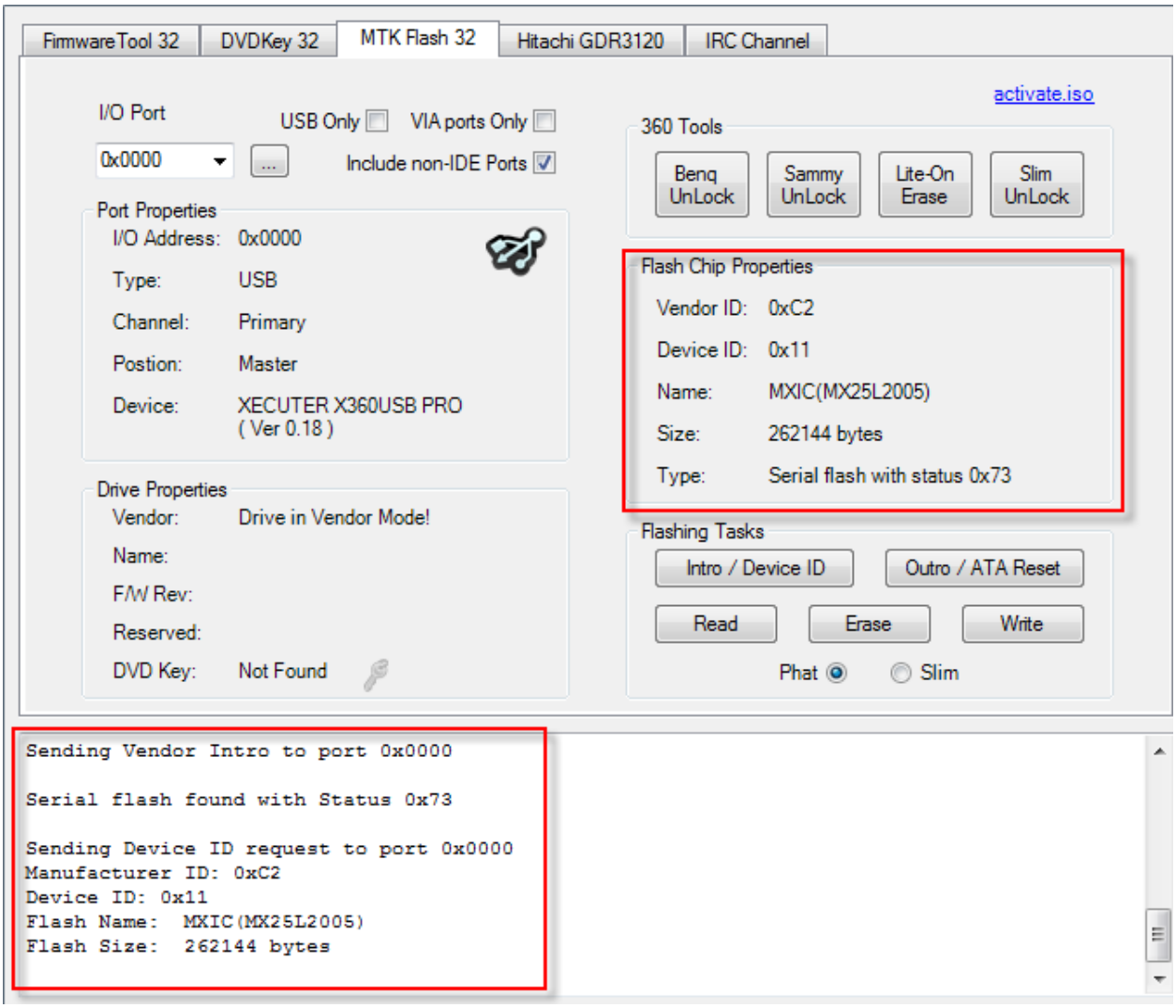
Select correct **I/O Port** then

Click **Intro / DeviceID.**



If tray status is correct, drive should return good **Flash Chip Properties showing status 0x73, Drive Properties** should show "**Drive In Vendor Mode!"**

Things not going as expected? – Read the FAQ's



NOTE: Please ignore the" DVD Key: Not Found" message in drive properties! (BenQ cannot automatically verify key.)

Once drive is in **Vendor Mode**, you can proceed with **Reading the Drives Firmware.**

CLICK HERE TO PROCEED

Things not going as expected? – Read the FAQ's

BenQ UnLock Stock/ iXtreme 1.1 -> 1.41 / Xtreme/iXtreme LT Firmware's Only.

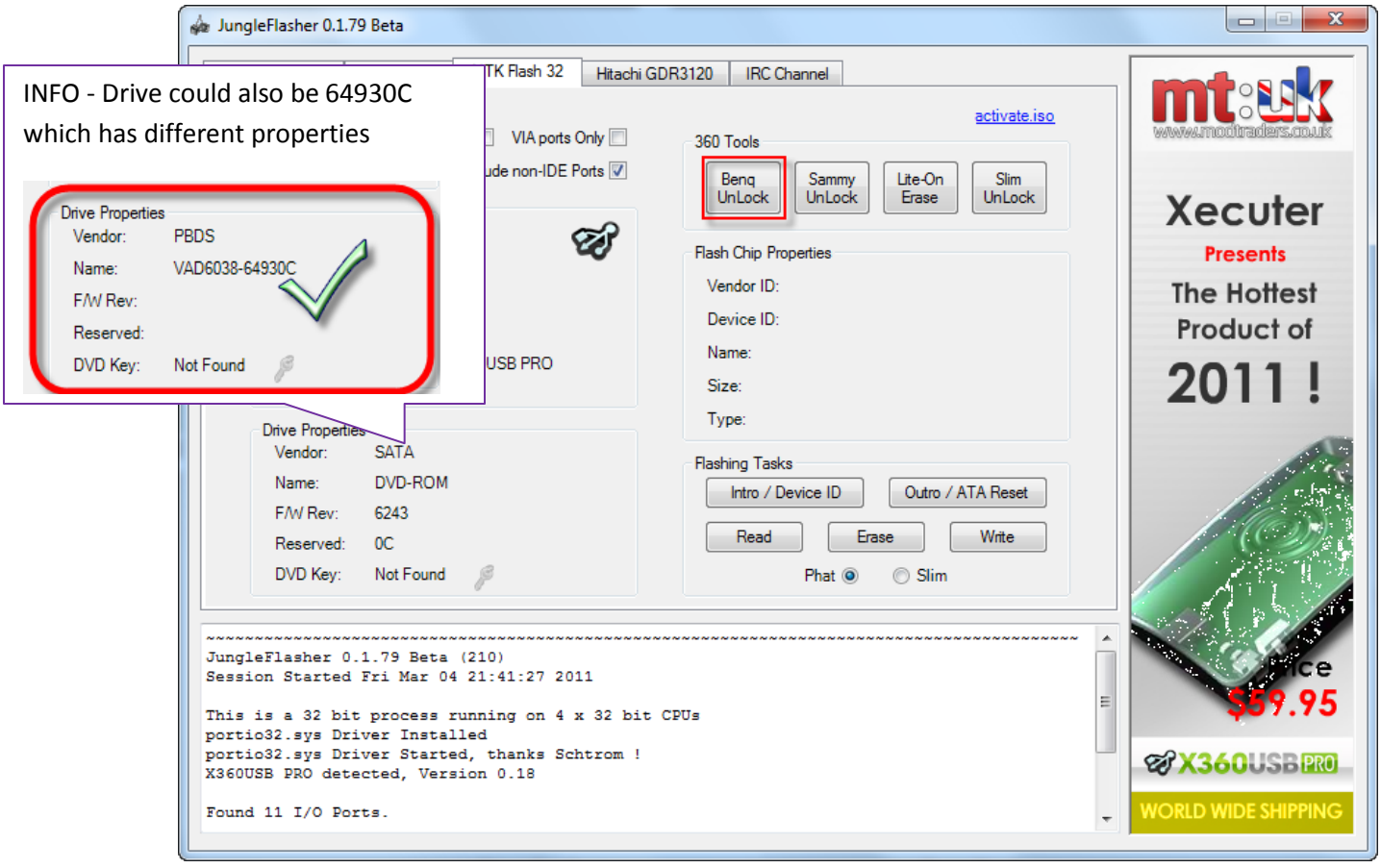
Please note, BenQ-Un-Lock **WILL NOT** work on drives that have iXtreme 1.5>1.61 firmware on them (please use VCC Trick or Half Open Tray)

Connect your BenQ drive up via SATA to your PC, power on, and run JungleFlasher.

After a few seconds you will be taken to the main application.

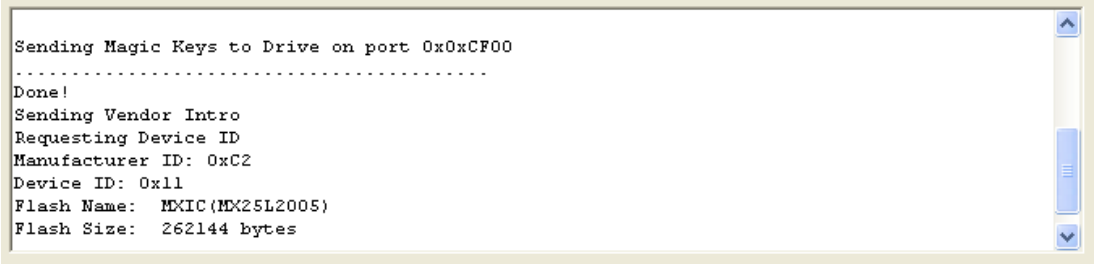
Click the **MTKFlash32** tab.

Then, select correct **I/O Port** by verifying **PBDS VAD6038** or **SATA DVD-ROM** shows in the **Drive Properties** and click **BenQ UnLock.**

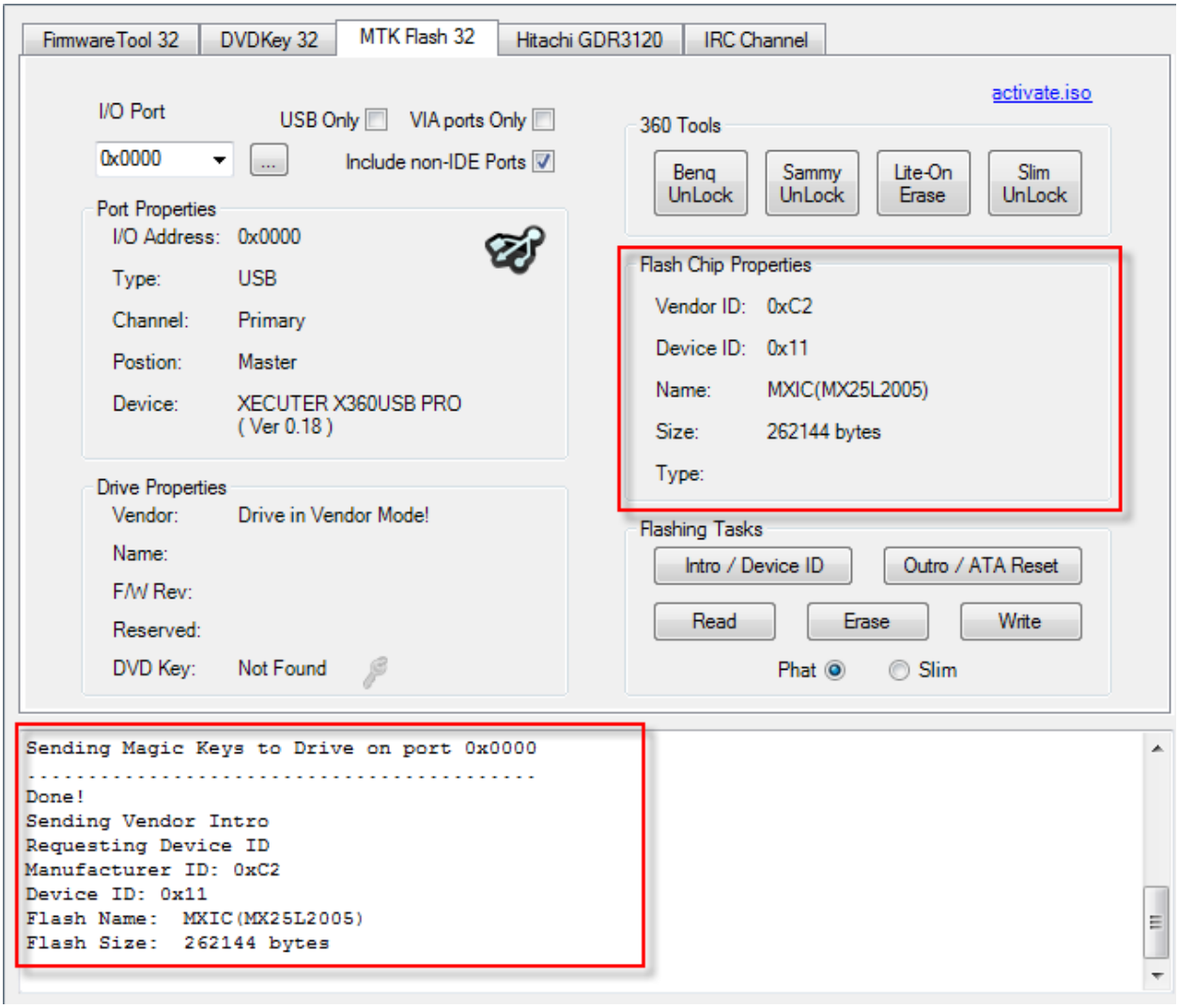


JungleFlasher will send the Magic Keys to unlock the drive and should return this message in the **Running Log.** JungleFlasher has also sent the Intro command to the drive.

Things not going as expected? – Read the FAQ's



The drive should be in **Vendor Mode (0x73)** now and return good flash chip properties, you can check in the **Running Log, Drive Properties** or **Flash Chip Properties.**



NOTE: IF USING X360USB Pro the Status DOES NOT INITIALLY SHOW as 0x73 BUT THE DRIVE IS STILL IN VENDOR MODE! (press Intro/Device ID again if you wish status to show up)

Once the drive is in **Vendor Mode**, you can proceed with **Reading the Drives Firmware.**

CLICK HERE TO PROCEED

Things not going as expected? – Read the FAQ's

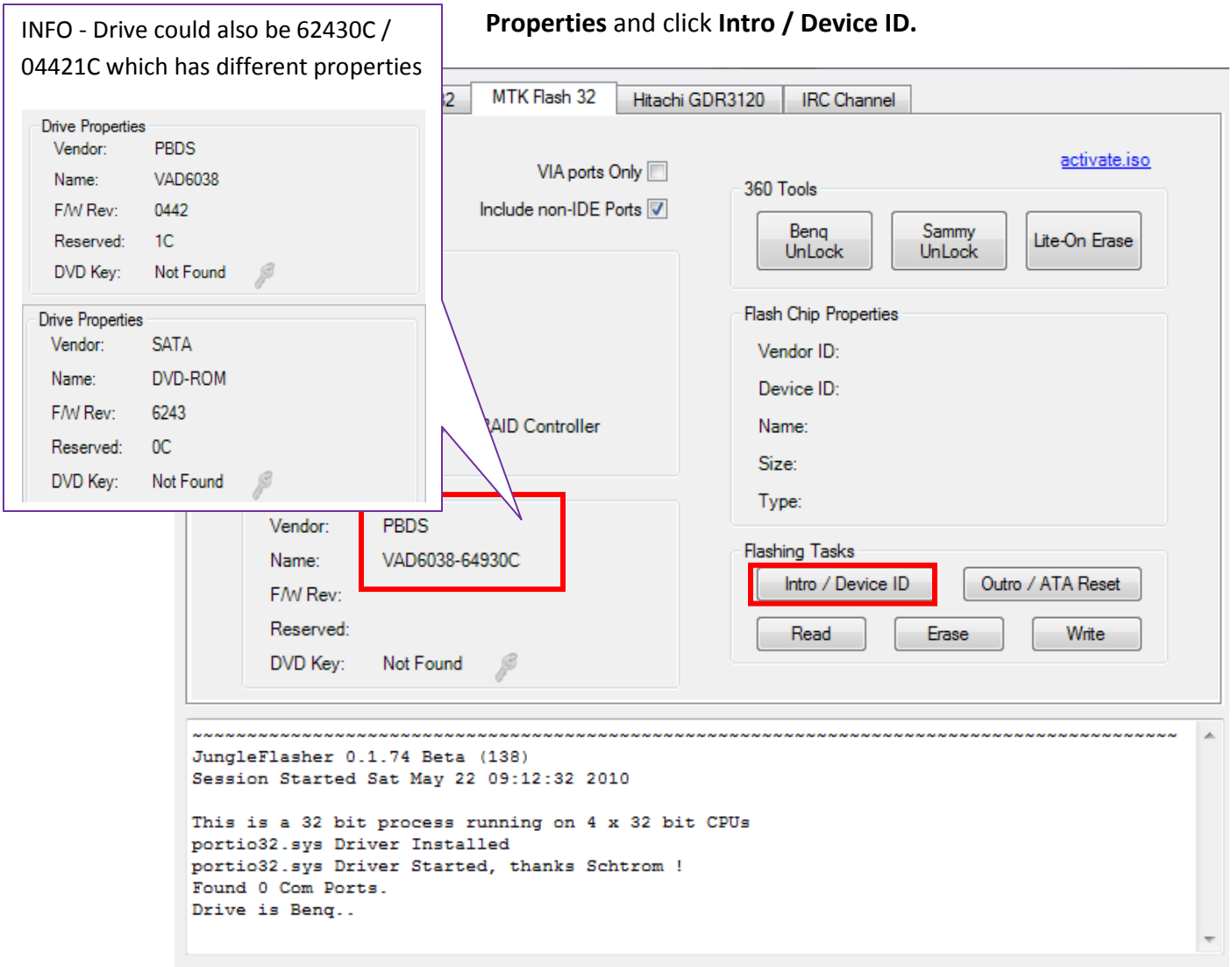
DeviceID Unlock / Vcc Trick (VIA/Nforce only) Stock + Modified Drives

This method has only really been tested on VIA **(no drivers, or 530c drivers)** and Nforce Chipsets, although there is no harm in trying on others, this method works on Hacked and Stock Drives.

Load JungleFlasher, and select **MTKFlash32** tab.

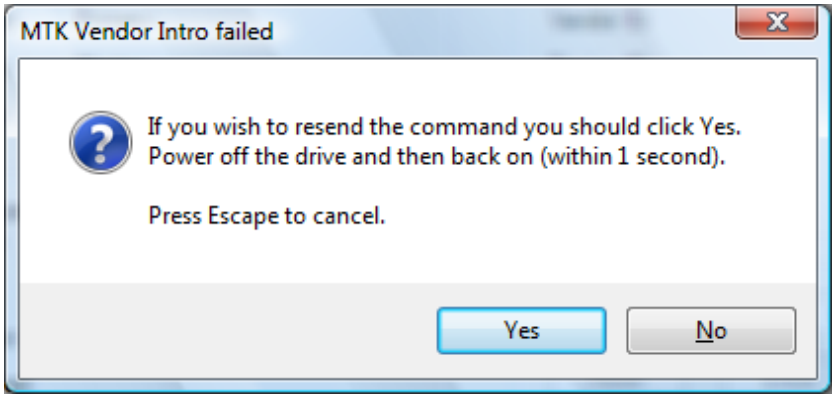
Then, select correct **I/O Port** by verifying **PBDS VAD6038**, **SATA DVD-ROM** shows in the **Drive Properties** and click **Intro / Device ID.**

INFO - Drive could also be 62430C / 04421C which has different properties



Things not going as expected? – Read the FAQ's

JungleFlasher will prompt you with instructions.



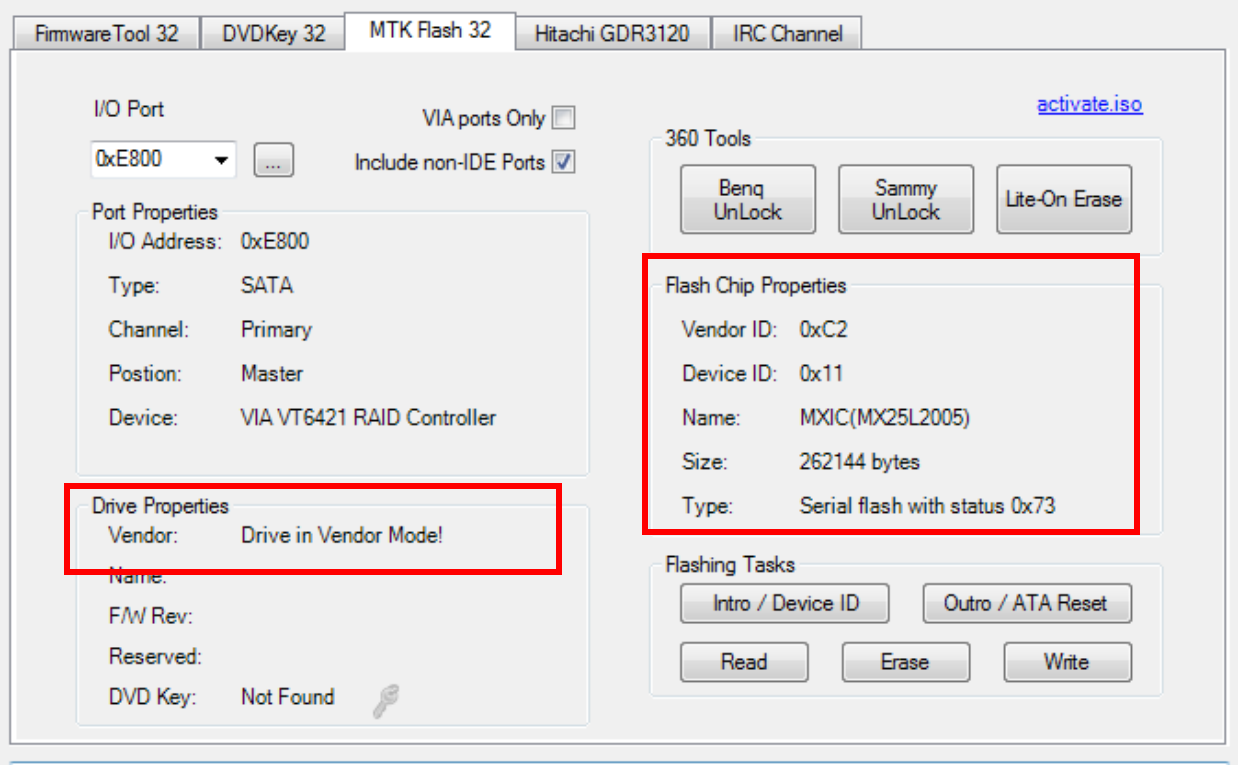
Click **Yes** the **Running Log** will display something similar to this.

```
Sending Vendor Intro to port 0xCF00
Invalid Status
Re-sending Vendor Intro:
.............
```

When **…….** are appearing, do as previously instructed by JungleFlasher. Power off the drive, then, **within 1 second,** power it back on.

The drive should be in Vendor Mode (0x73) now and return good flash chip properties, you can check in the **Running Log** or **Flash Chip Properties,** Drive properties should display "**Drive in Vendor Mode!".**

Things not going as expected? – Read the FAQ's



CLICK HERE TO PROCEED

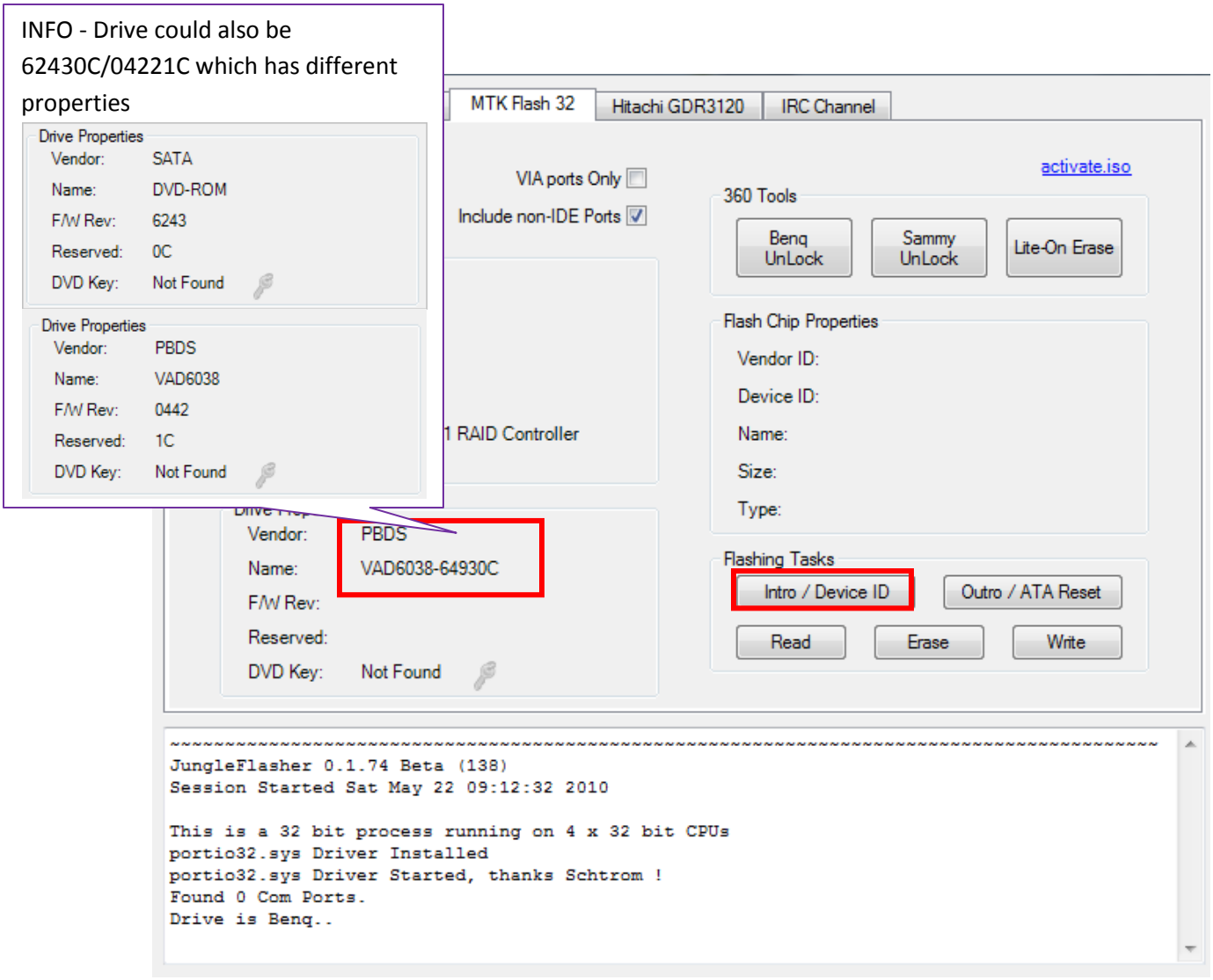
If it didn't work – read on

Alternate method if you are struggling with the above!

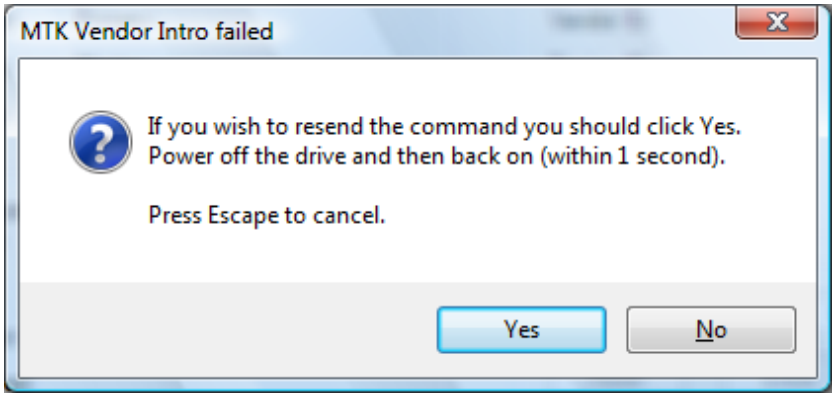
Load JungleFlasher, and select **MTKFlash32** tab.

Then, select correct **I/O Port** by verifying **PBDS VAD6038** or **SATA DVD-ROM** shows in the **Drive Properties** and click **Intro / Device ID.**

Things not going as expected? – Read the FAQ's



JungleFlasher will prompt you with instructions.



Now turn **OFF** the power to the drive!

Click **Yes,** the **Running Log** will display something similar to this.

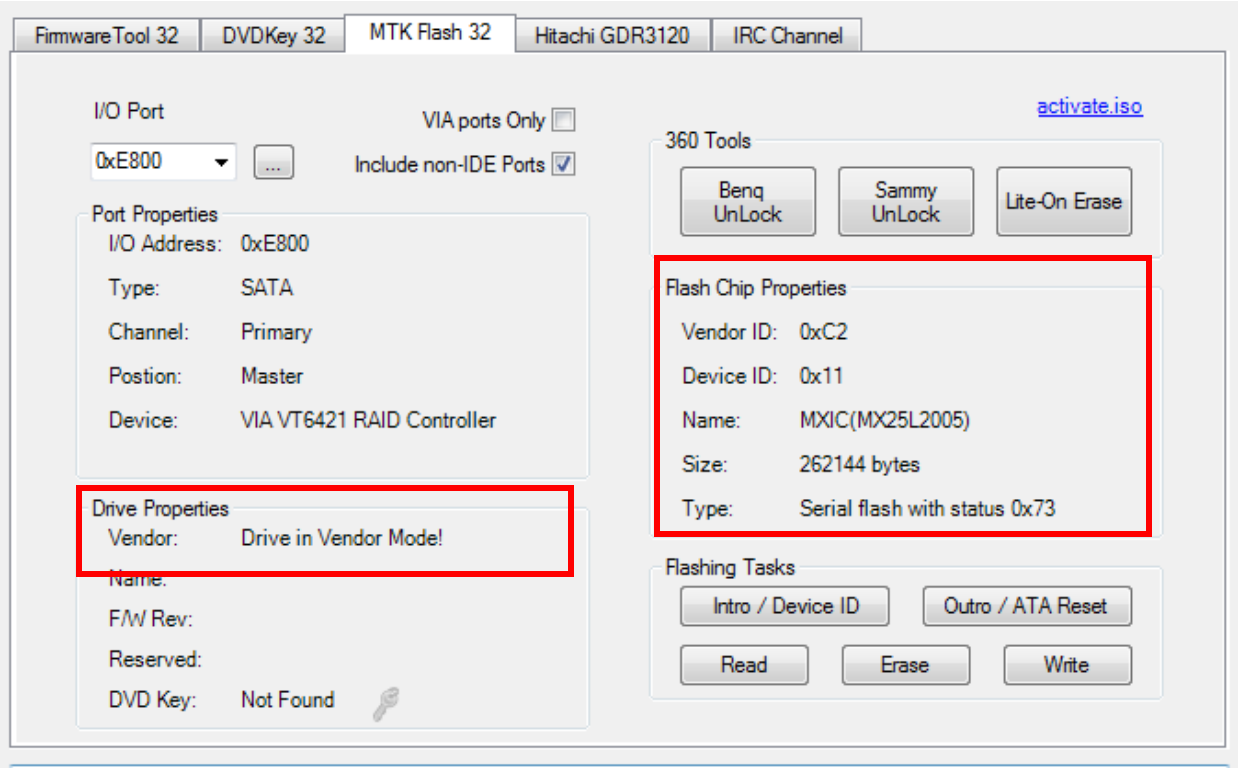
Things not going as expected? – Read the FAQ's

```
Sending Vendor Intro to port 0xCF00
Invalid Status
Re-sending Vendor Intro:
..............
```

While ……. are appearing,

Turn **ON** the power to the drive

The drive should be in Vendor Mode (0x73) now and return good flash chip properties, you can check in the **Running Log** or **Flash Chip Properties,** Drive properties should display "**Drive in Vendor Mode!".**

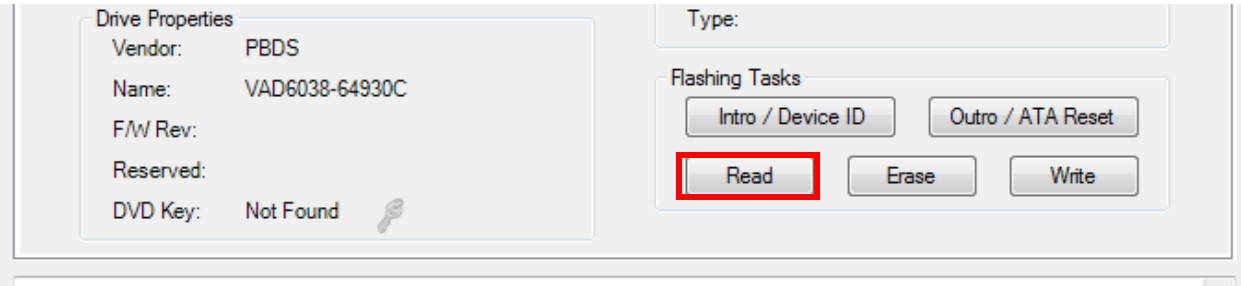


CLICK HERE TO PROCEED

Things not going as expected? – Read the FAQ's

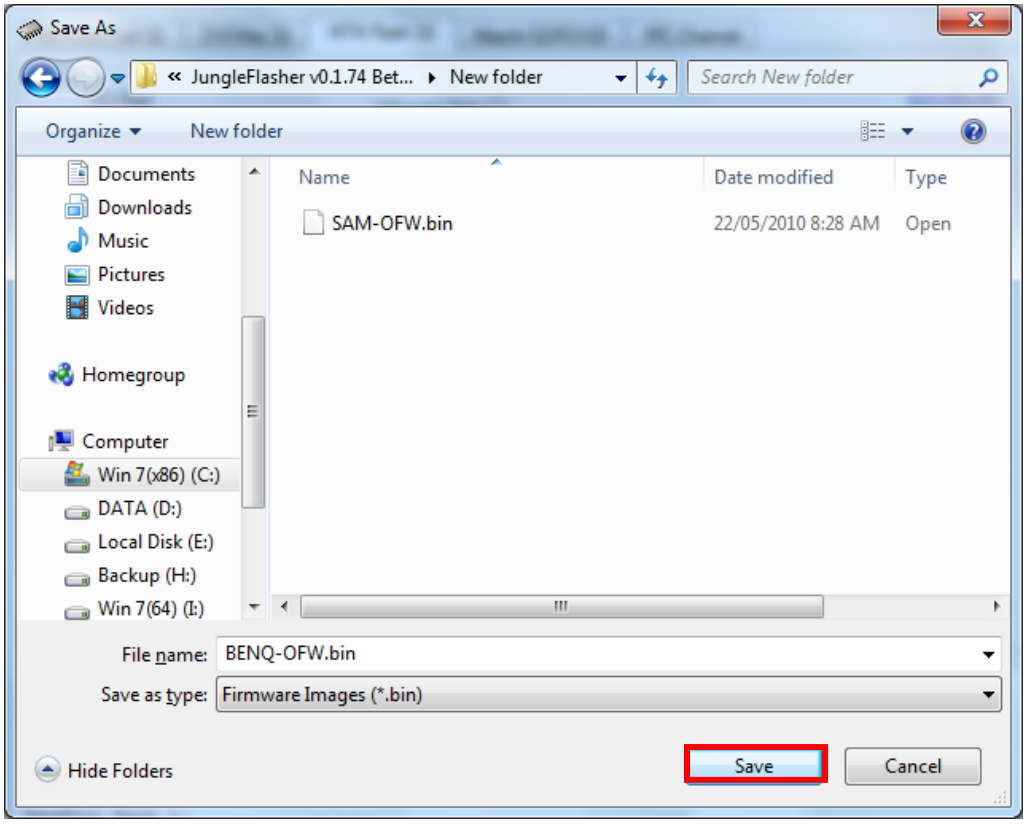
Reading the Firmware from the drive.

Now, we would like to read the firmware from the drive first, so select **read.**



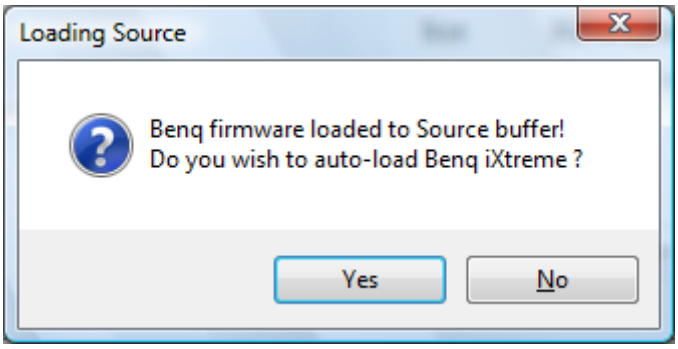
Check the **Running Log** and you will see it reading the firmware from the drive.

Once the firmware has been read JungleFlasher will prompt you to save the firmware. Name it what you wish and select directory path of your choice and click **Save.**



Once saved, JungleFlasher will then prompt you asking if you would like to auto-load iXtreme for BenQ Drives. You must have installed the **JungleFlasher Firmware Pack** into the same directory as JungleFlasher.exe if you wish to benefit from this feature.

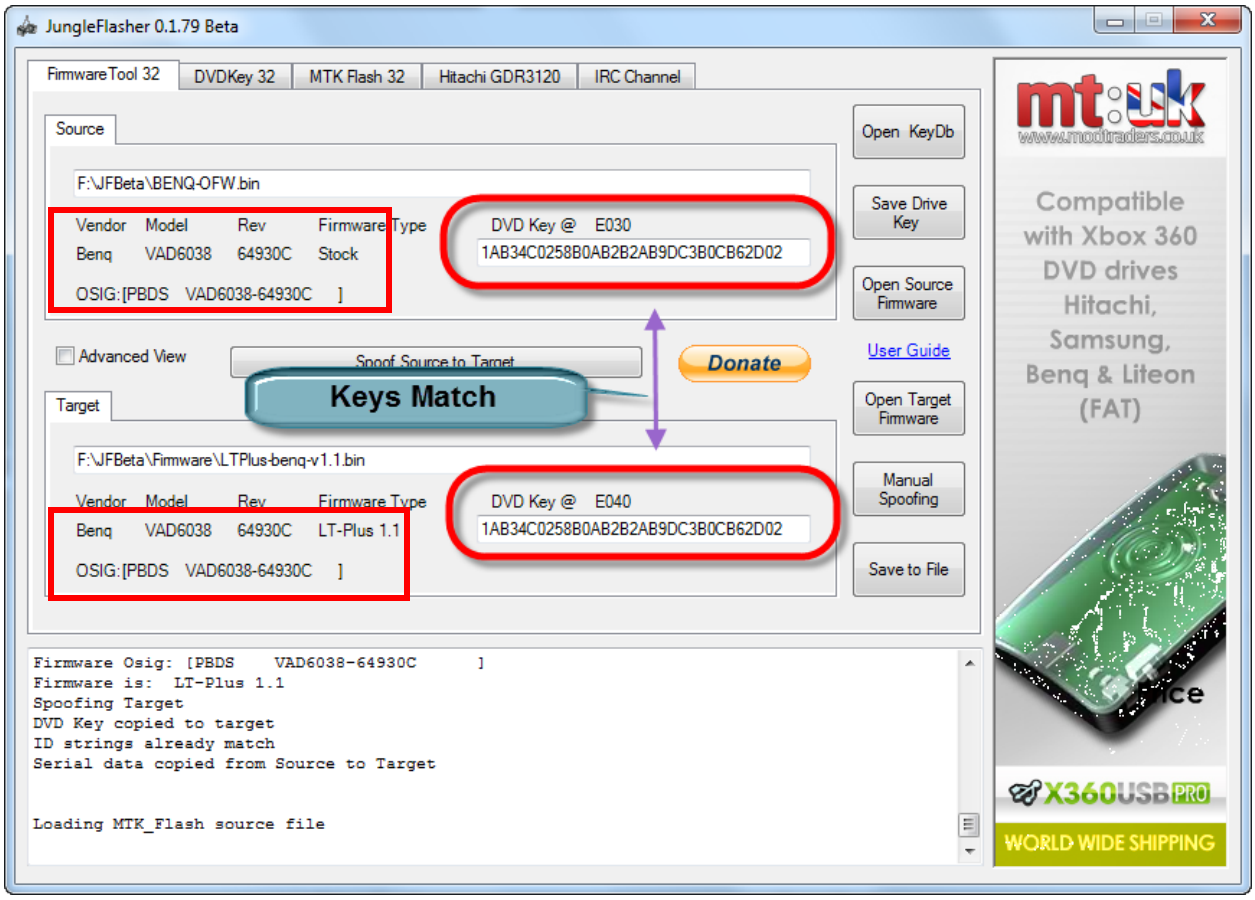
Things not going as expected? – Read the FAQ's



Click **Yes** to auto load iXtreme (from the firmware pack) for BenQ into the **Target Buffer**, JungleFlasher will also load your previously dumped **BenQ-OFW.bin** as **Source Firmware.** Then, copy data from **Source to Target automatically.**

Just verify **Source data** reports as it should, OSIG of **VAD 6038 or SATA DVDROM** with a key with no multiple **FF/00/77 bytes.**

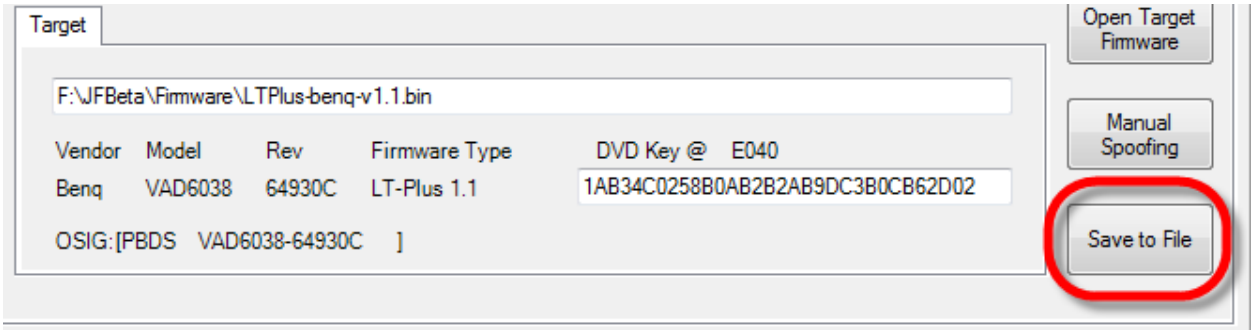
Now, verify **unique Source Data** matches that in **Target Buffer** and click save to file if you wish to backup your Hacked firmware.



(This Example is for PRE-DASH 13146, FOR POST-DASH UPDATE Rev will be 04421, Target will be LT+1.91 FW Type).

Things not going as expected? – Read the FAQ's

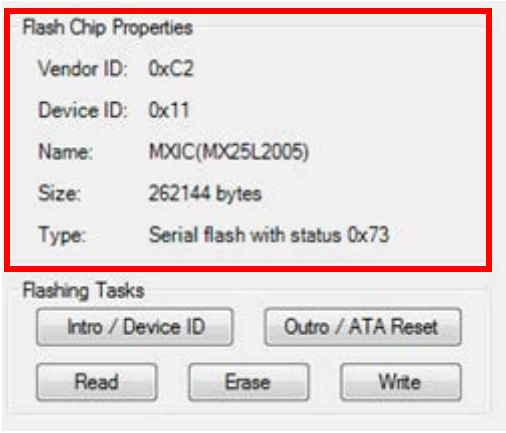
You can now save the **Target Buffer** to file by clicking **Save to File.**



Writing Firmware to the drive.

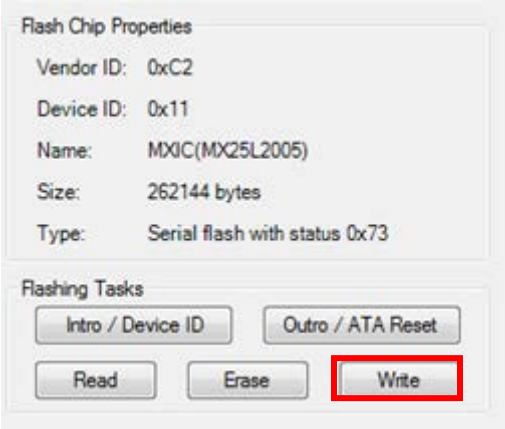
To write the firmware, as long as drive is still unlocked (Vendor Mode) we just **click MTKFlash 32** tab.

Verfify you have good flash chip properties still.



Then, click **Write.**

Things not going as expected? – Read the FAQ's



Write Command, will send Chip Erase prior to writing and then proceed to write the 4 banks of the firmware (banks 0/1/2/3).

A series of 16 …..'s is JungleFlasher writing the 16 sectors of each bank (4 banks, 0/1/2/3).

```
Sending Chip Erase to Port 0xE800
Writing target buffer to flash
Writing Bank 0: ................
Writing Bank 1: ................
Writing Bank 2: ................
Writing Bank 3: ................
```

After writing all 64 sectors, signaled by 64 dots (16 dots across 4 banks) JungleFlasher will verify what it wrote by reading back and comparing against the Target Buffer, what we really want to see is **Write Verified OK!**

```
Flash Verification Test !
Reading Bank 0: ................
Reading Bank 1: ................
Reading Bank 2: ................
Reading Bank 3: ................
Write verified OK !
```

Now send an Outro to the drive.

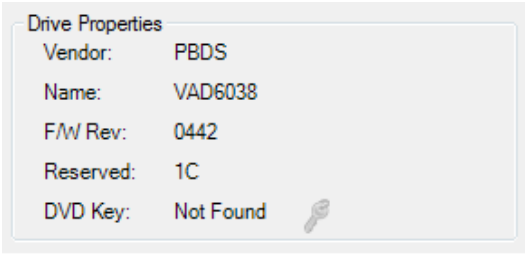
This will release a drive from **Vendor Mode** and send **ATA Reset** to the Drive. It then sends an inquiry command to the drive.

This will save you power cycling the drive and then changing port away and change it back again, with the click of a button, drive will 'reset' itself and JungleFlasher will send an inquiry command to the drive. If successfully flashed the drive should Inquire correctly and display drive properties.

Things not going as expected? – Read the FAQ's

PRE- DASH UPDATE

POST DASH UPDATE



Which drive properties you have depends on BenQ FW version!

Power off – connect back to console and test!

CLICK HERE TO RETURN TO START OF TUTORIAL

Hitachi GDR-3120L.

Rom Versions 32/36/40/46/47/58/59/78/79.

Overview.

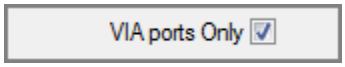
Hitachi drives are completely unique in the way and which they are modded. We modify Hitachis on a sector by sector basis. For this to happen the drive must be in Mode-B (mode-b allows windows to recognise the drive!) there are several transfer methods available (some only to certain revisions) But **RAM Upload** can be used for all drives!

JungleFlasher can be used over **Windows API or PortIO.**

WinAPI should used where possible, although ***WinAPI*** *requires the drive to be assigned a drive letter*, this **isnt** possible with a **VIA 6421** with **Drivers Removed.**

PortIO functionality was added for VIA 6421 Sata users who removed drivers to hack the Lite-On drives without freezing issues.

To enable PortIO usage, check VIA Ports Only under DVDKey 32 tab.



VIA users with no drivers, must utilise the PortIO option

you will not be assigned a drive letter in windows with no drivers!!! – You can still dump/flash the drive – it just will NOT SHOW UP IN THE DRIVE LIST!
To enable PortIO usage, check VIA Ports Only under DVDKey32 tab

(you must have drivers correctly removed!)

Not installing VIA drivers IS NOT the same as removing them, JF will not enable portIO on status 28

39 = drivers couldnt be loaded

28 = drivers are not installed

Things not going as expected? – Read the FAQ's

Regardless of option chosen, the Hitachi Drive must still be in **ModeB**, this is essential to be assigned a drive letter in Windows, for using **WinAPI**, but, also vital for **PortIO** users as most dump and flash commands require it.

Windows API Users, after setting ModeB, you must wait for hardware changes to be detected (15 secs) If nothing is detected, click "Refresh"

Sometimes the drive will not automatically show up – if this is the case (WinAPI users only) open device manager and "scan for changes"

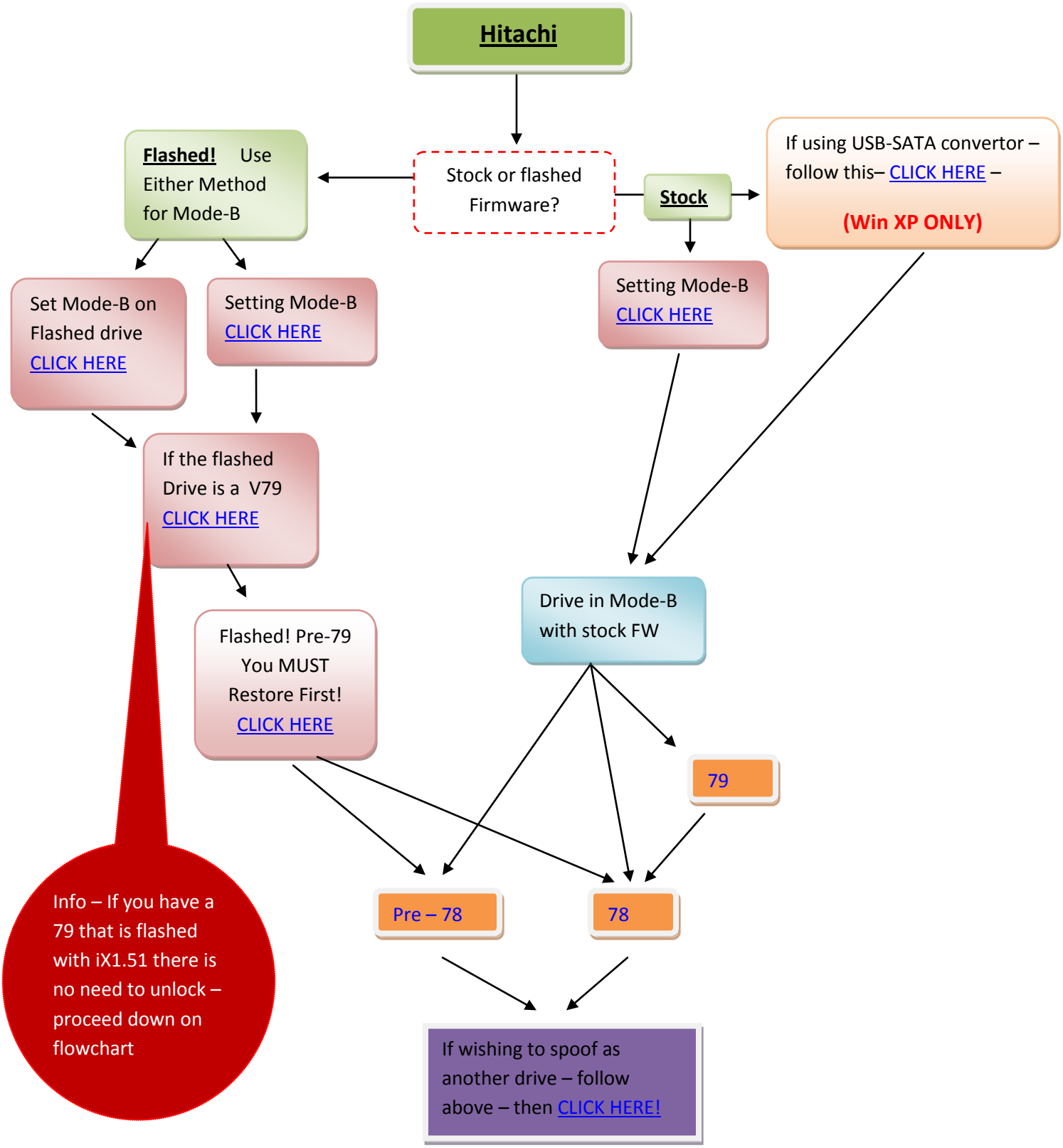
JungleFlasher uses a unique way of calculating the checksum of the firmware and JungleFlasher will also take over from the user as soon as possible to prevent user error, its not necessary to dump the drive to patch the firmware, JungleFlasher will dump before you try to do anything to the drive.

JungleFlasher also incorporates a "Stability Test" prior to modifying the drive, as safety is paramount.

X360USB PRO

The x360USB Pro is a unique piece of hardware, It incorporates WinAPI and Portio usage when flashing a Hitachi (winAPI is a lot faster) so select WinAPI before you start, Jungleflasher will automatically switch between the two without user interference. PortIO drivers are not required at all when using the X360USB Pro and if you tick USB Only box(DVDKey 32 tab) – you will see the PortIO drivers are even unloaded.

CLICK TO CONTINUE



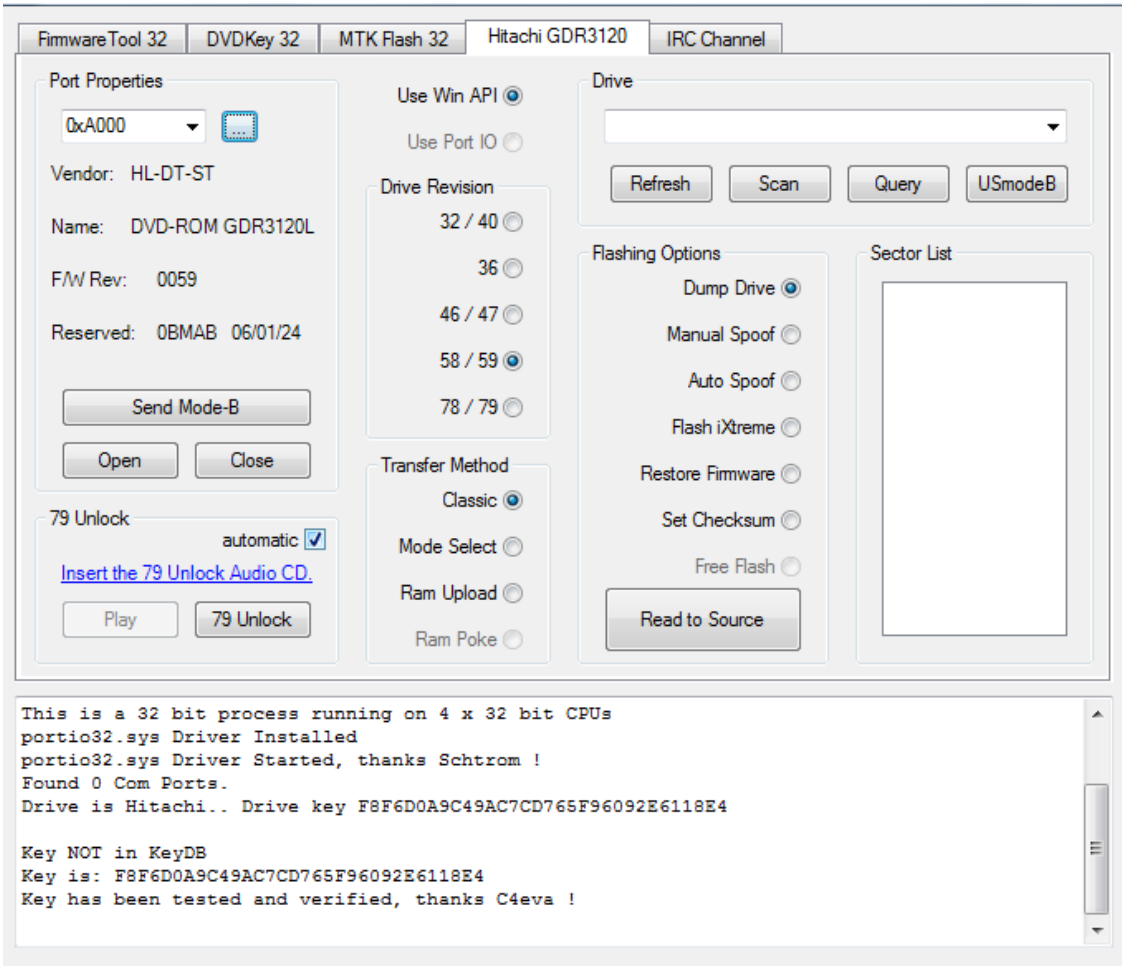
Things not going as expected? – Read the FAQ's

Setting ModeB

Connect your Hitachi Drive via sata, power it on, then open JungleFlasher and you will be presented with the welcome screen

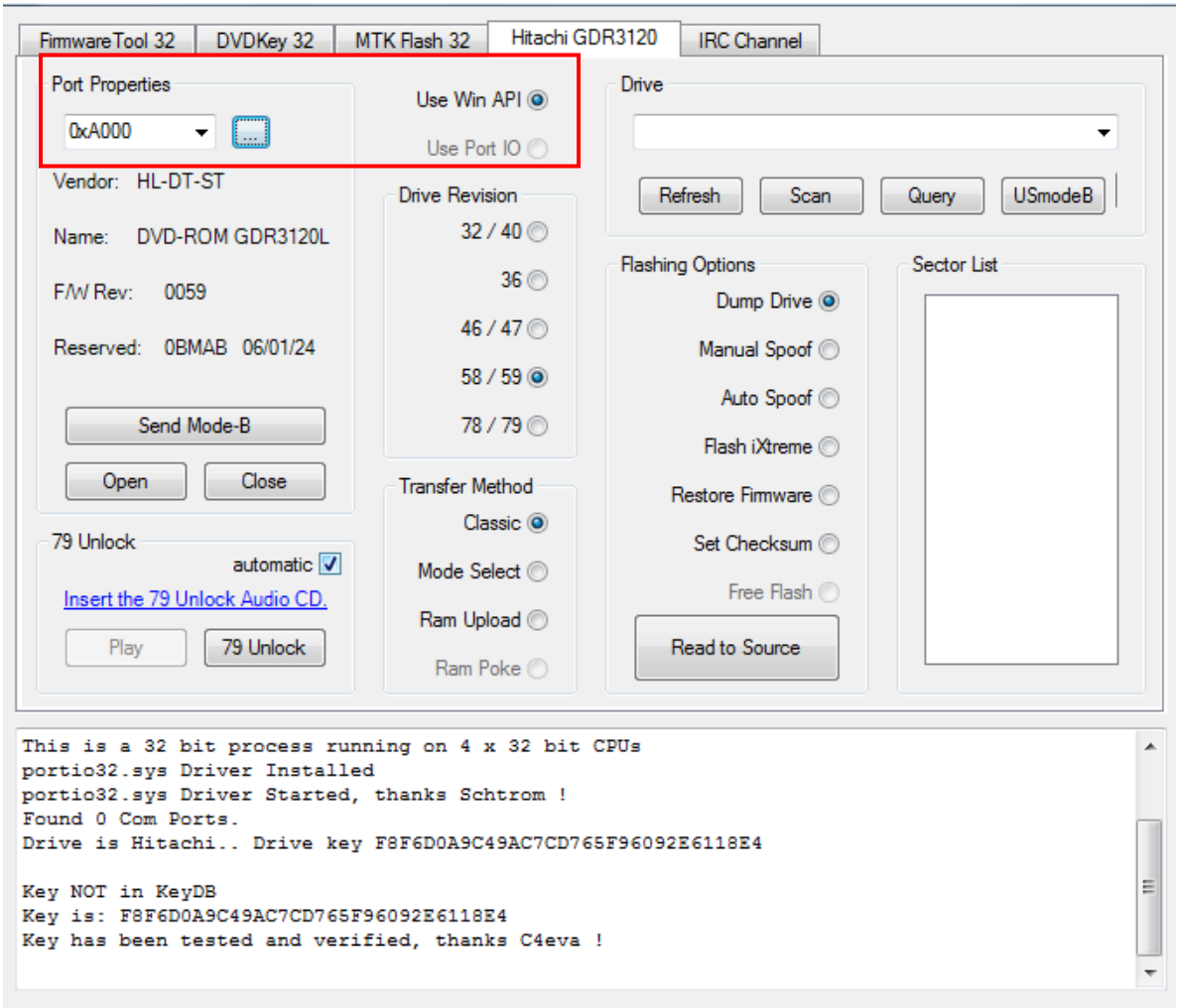
Then, click the **Hitachi GDR-3120 tab**

You will be presented with the dedicated **Hitachi tab** shown below (or similar to)



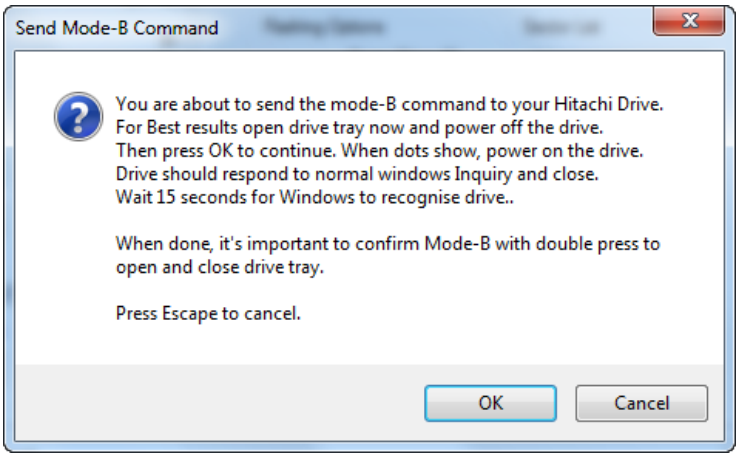
Note the **Hitachi Drive** inquires on my **I/O Port** and that **PortIO** is disabled (using **non-VIA** chipset)

Things not going as expected? – Read the FAQ's



The drive needs to inquire on **I/O** port for **Raw ModeB Commands to work** (this applies to spoofed drives also)

Once it inquires, Click **send ModeB**, you will be presented with the following message, **do as it states**, as the **ModeB built in on some Connectivity Kits, can cause issues.**



Things not going as expected? – Read the FAQ's

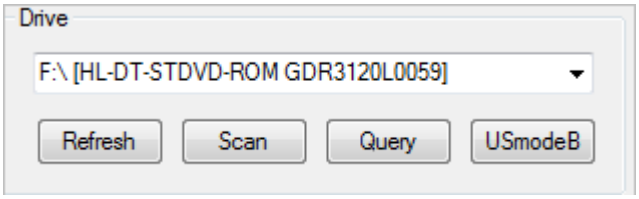
The drive should now report as in **ModeB**

```
Drive, answers normal Windows Inquiry 12 0 0 0 24 0
0000: 05 80 00 32 5B 00 00 00 - 48 4C 2D 44 54 2D 53 54 ...2[...HL-DT-ST
0010: 44 56 44 2D 52 4F 4D 20 - 47 44 52 33 31 32 30 4C DVD-ROM GDR3120L
0020: 30 30 35 39                                       0059

Mode-B Done!
Scanning for hardware changes
```

```
Found drive C: - Hard Drive.
Found drive D: - Hard Drive.
Found drive E: - Hard Drive.
Found drive F: - CD/DVD. <--- Hitachi found
Found drive G: - CD/DVD.
```

Once **ModeB** is set, if using **WinAPI**, JungleFlasher will scan for hardware changes automatically after 15 seconds (if using vista/win 7 ensure you run jungleflasher as administrator) if drive does not show up then scan for changes in device manager!

WinAPI users should see similar to this under the 'Drive' section



If not, click **Refresh List**

JungleFlasher WILL NOT scan for Hardware Changes after setting ModeB for PortIO users. The Drive will NOT appear in drive list on right hand side!

Instead, the tasks are carried out, as long as the drive Inquires on the **I / O Port**

BACK TO FLOWCHART!

Things not going as expected? – Read the FAQ's

Mode B on an already flashed drive

Mode B can be easily achieved on a pre-flashed Hitachi

Ensure SATA cable connected to pc!

This is done by powering **on** the drive with the tray fully open

To do this using a Xbox 360 console for powering the drive;

1. Eject the drive
2. Pull the power cable from the rear of the DVD-Rom
3. Plug cable back in (ensuring correct orientation of plug)
4. The drive tray will close (if pre-flashed)
5. Check that it takes 2 presses to eject and 2 or 3 to close.

Your drive is now in Mode B

Using a connectivity kit / power dongle

1. Eject drive using button on kit
2. Switch power off, then on again
3. The drive tray will close (if pre-flashed)
4. Check that it takes 2 presses to eject and 2 or 3 to close.

Your drive is now in Mode B

Start Jungleflasher – click on Hitachi Tab, ensure correct I/O port

If using WinAPI – drive should show in drive list on right hand side!

If using PortIO option – drive should be visible in port on left hand side ONLY!

CONTINUE ON FLOWCHART

JungleUSB Drivers and USmodeB (XP ONLY)

JungleUSB is a hacked USB Storage driver that enables windows to see a Mode A drive over USB, this enables USmodeB command to be sent and the drive.

Installing JungleUSB Driver

(can be downloaded from the usual places).

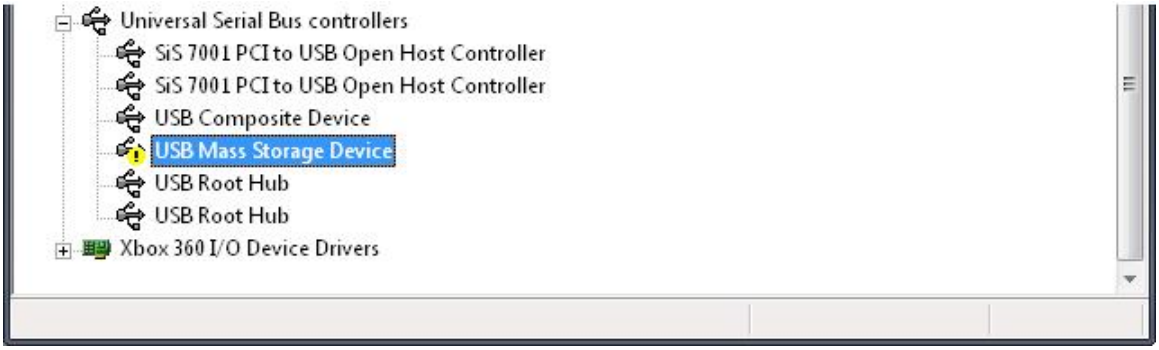
First you need to connect the drive to your PC with a SATA-USB Bridge Adapter

Windows will automatically install the device as

USB Mass Storage Device

You will need to update driver and install **JungleUSB**

Open Device manager and Find **USB Mass Storage Device** under **Universal Serial Bus Controllers.** Right click on it and **Update Driver**.



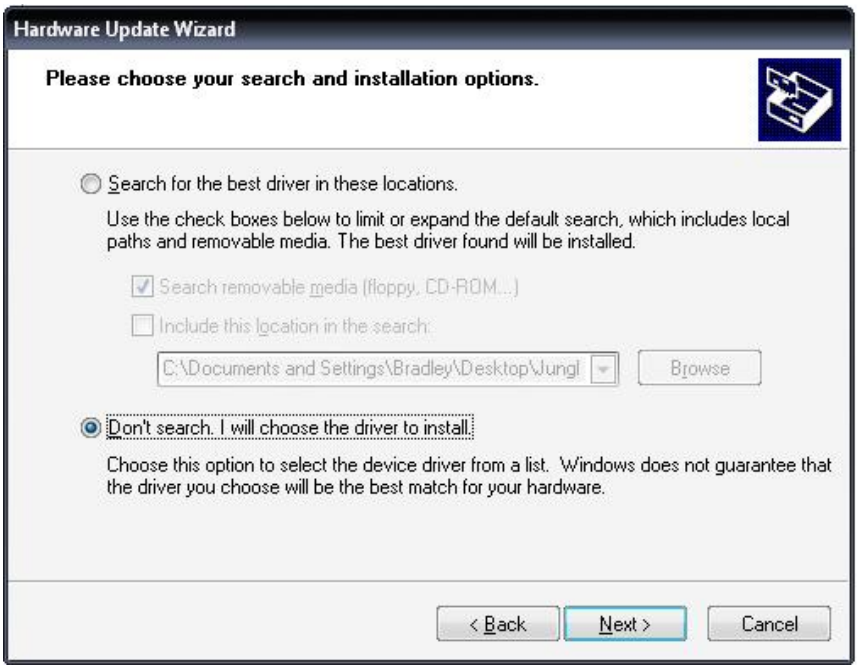
.

Select **No, not this time**. Then click Next

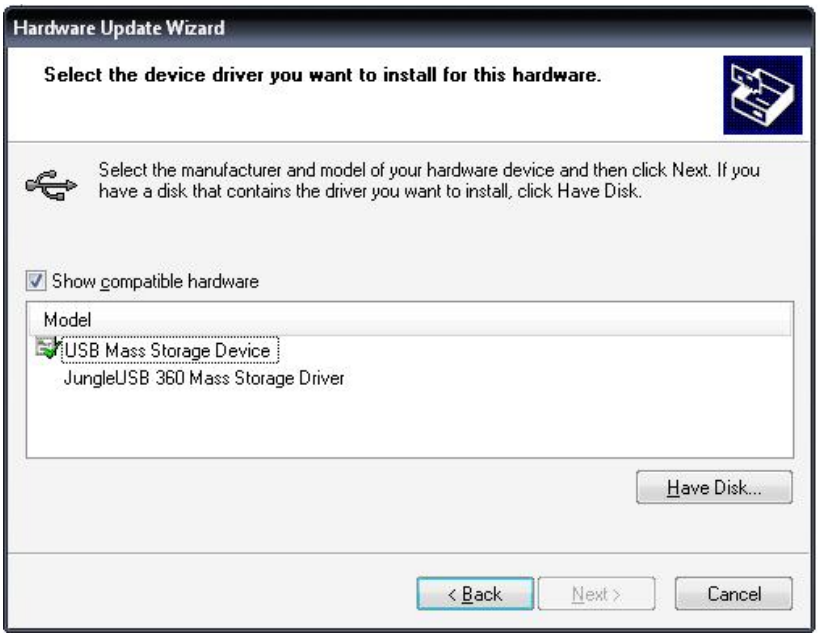
Things not going as expected? – Read the FAQ's

Select **Install from specific location** and click Next

Select **Don`t search I will choose the driver to install** and click Next.

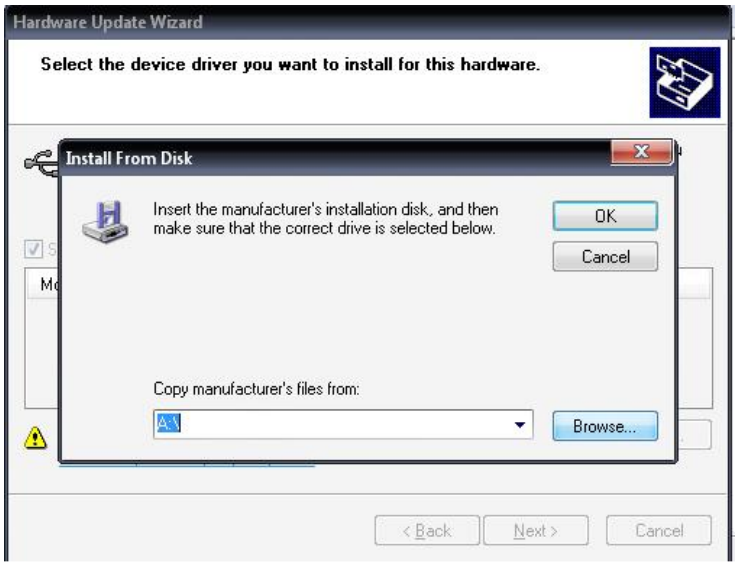


Click **Have Disk**



Now click **Browse** and Navigate to **JungleUSB.inf** (can be downloaded from the usual places).
Select it and click Open. Then click OK

Things not going as expected? – Read the FAQ's

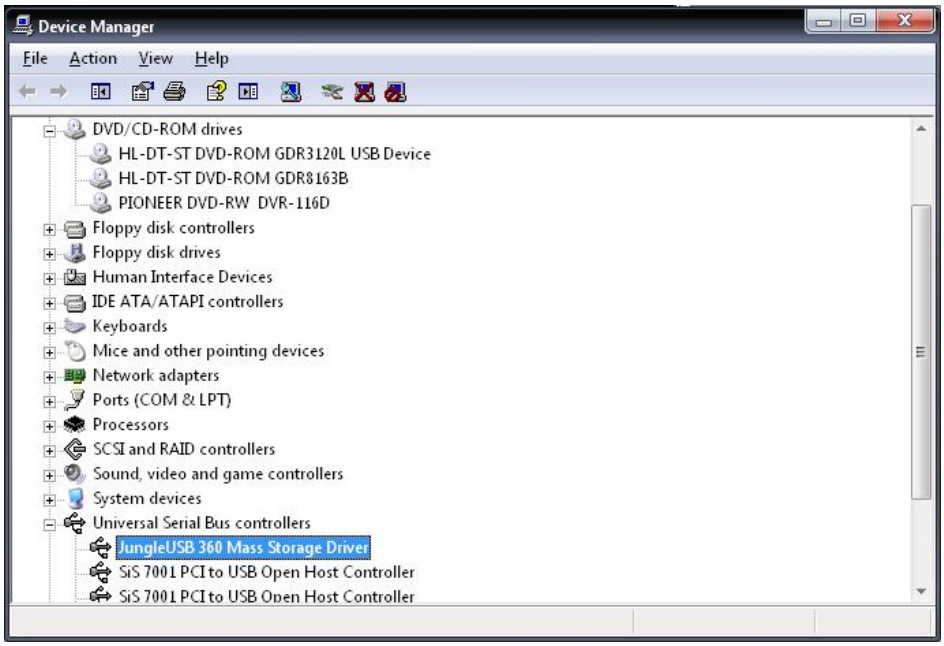


Now click next and the Driver should install.

Click finish and Return to Device manager.

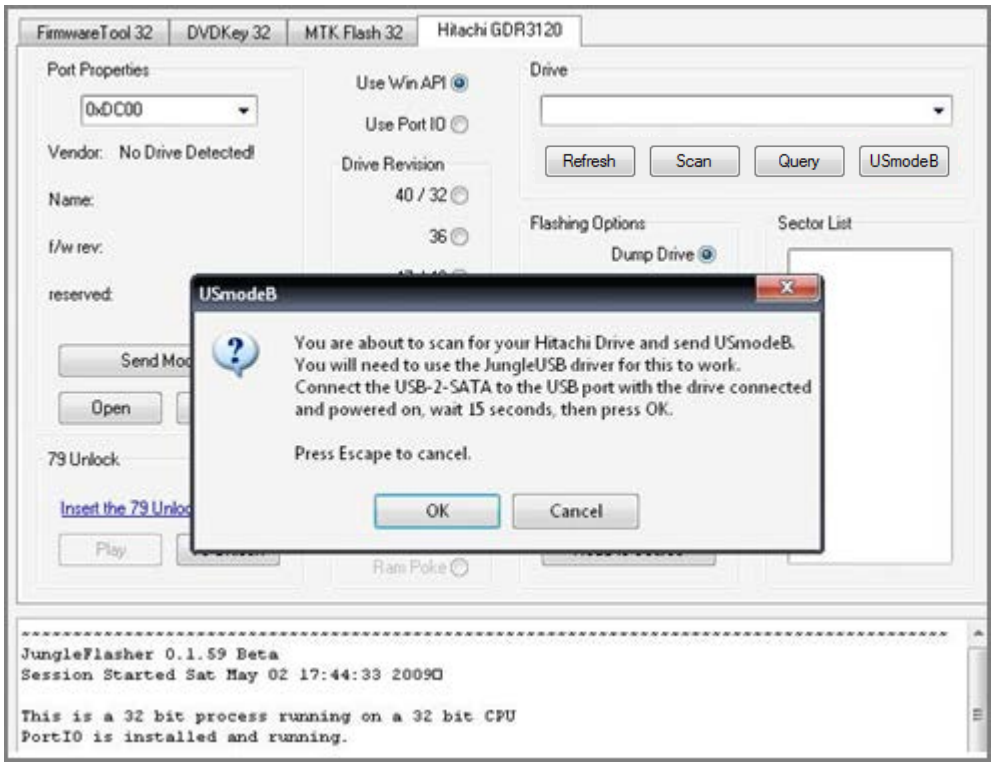
Things not going as expected? – Read the FAQ's

If all went well you should now have **JungleUSB 360 Mass Storage Driver** listed under **Universal Serial Bus Controllers** and **HL-DT-ST DVD-ROM GDR3120 USB Device** listed under **DVD/CD ROM drives.**

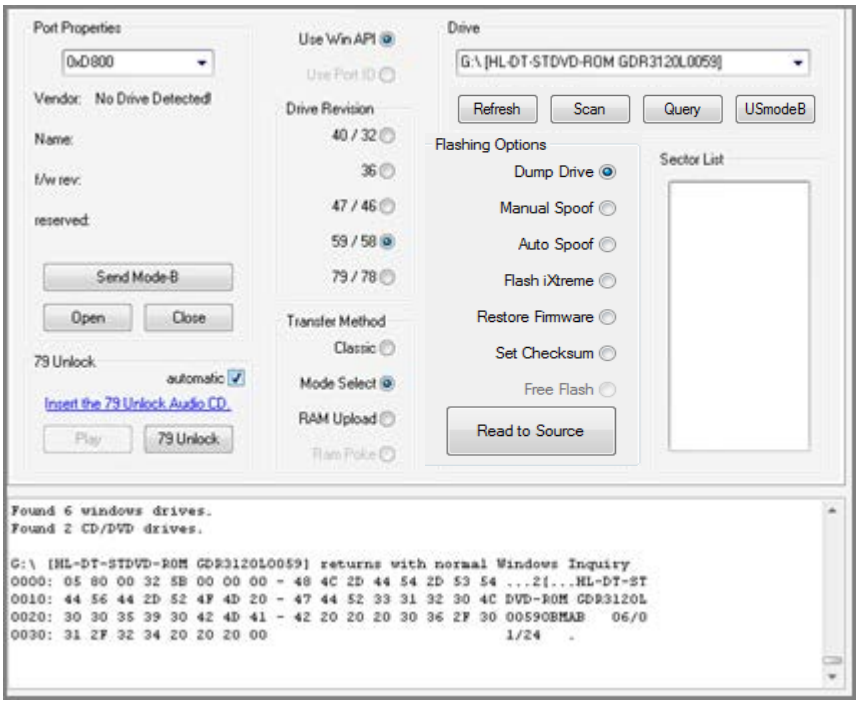


Now Start JungleFlasher and select the **Hitachi GDR3120** tab, Click the **USmodeB** button

Things not going as expected? – Read the FAQ's



JungleFlasher will scan for any 360 Hitachi Drives connected via USB and send Mode-b Command to that drive. The Drive should now be selectable in the drop down box.



[CLICK TO RETURN TO HITACHI FLOWCHART]

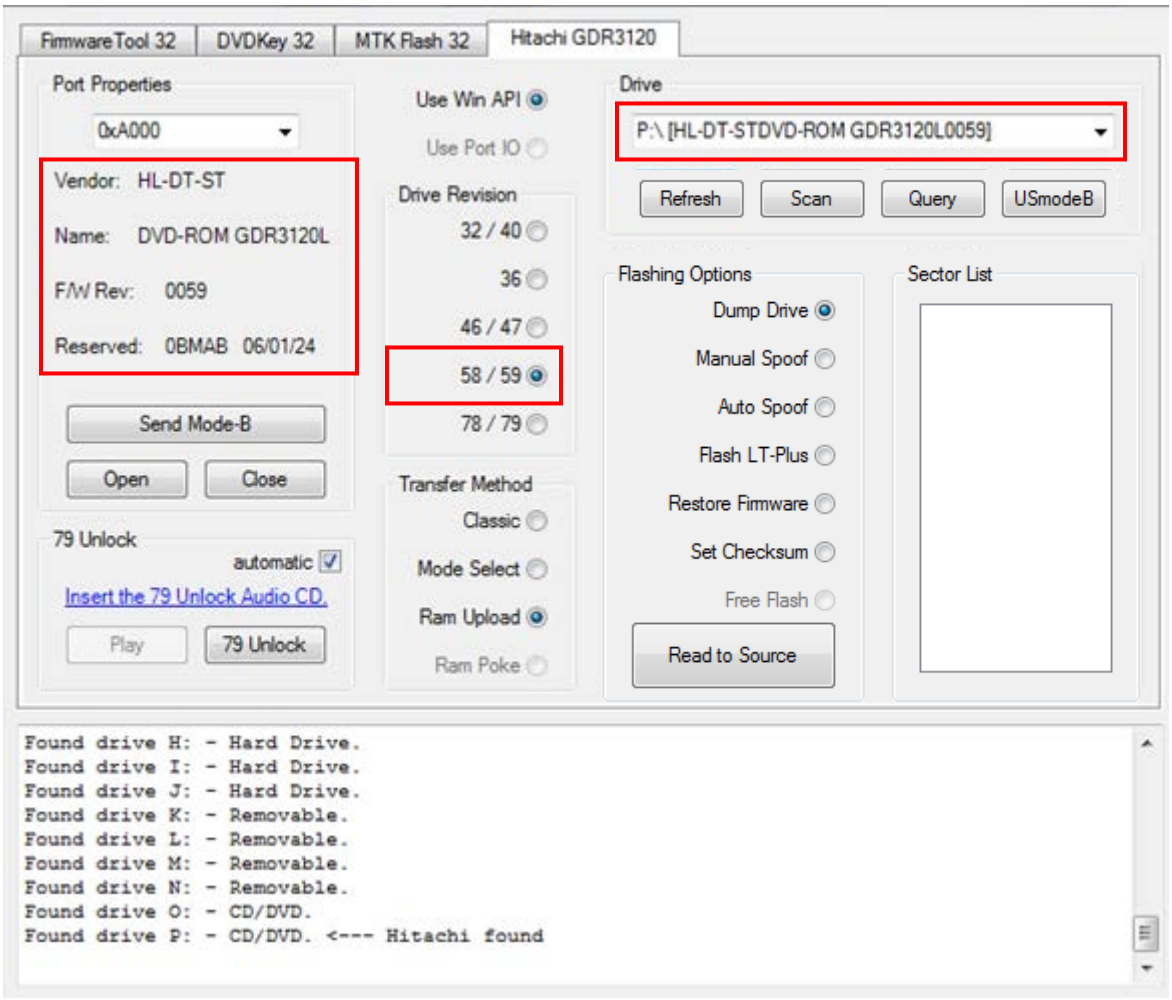
Things not going as expected? – Read the [FAQ's]

Dumping the Firmware from the drive (Pre v78)

Older ROM Versions of the drive, v32, v36, v40, v46, v47, v58 and v59 are dumped using **Classic Mode**, **Mode Select, or RAM upload.** For the purpose of the tutorial, I'll use **Mode Select**

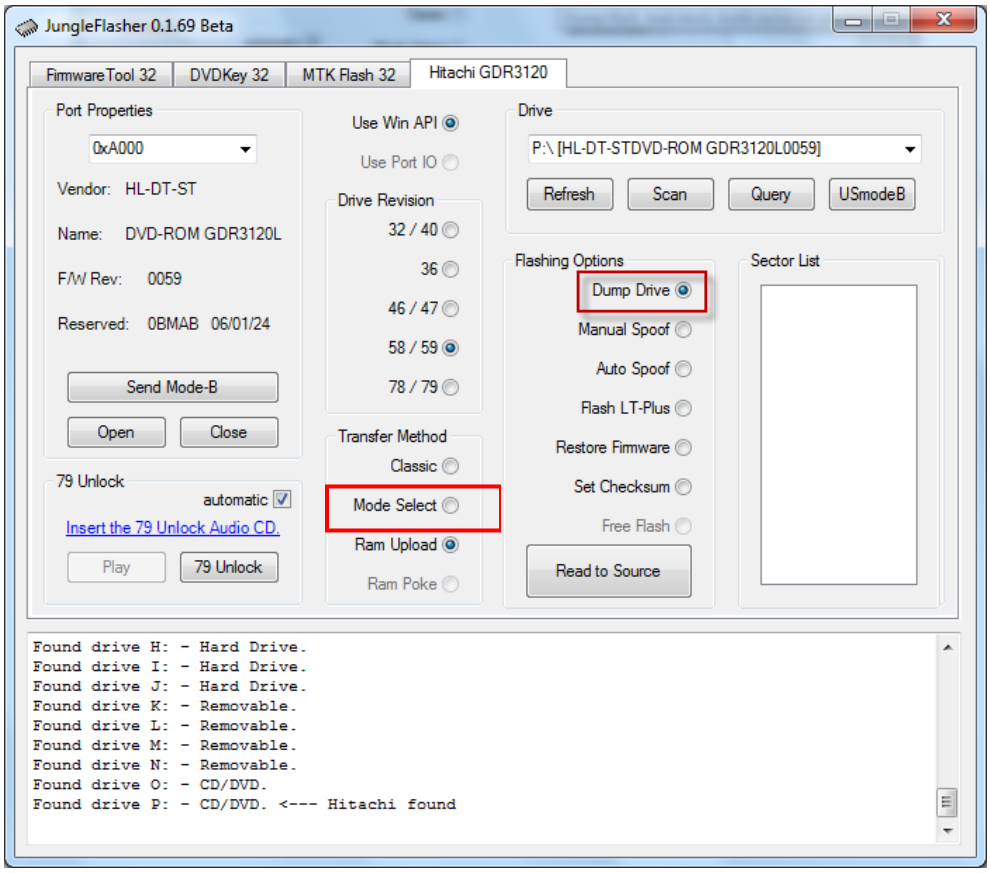
**** Dumping the firmware from a Drive Using 'Classic Mode' will be fooled by firmware stealth, this means, it WILL report as stock even though it isnt. ****

As the drive is in **ModeB** already, we simply ensure drive revision matches that of the drive

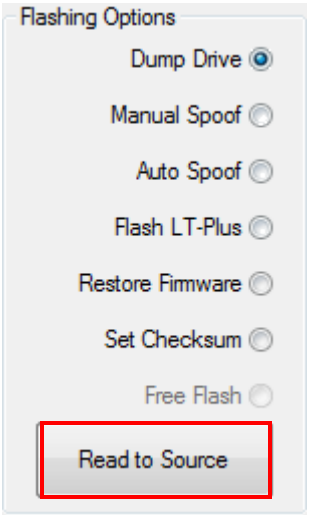


Select **Dump Drive** and **Mode Select**

Things not going as expected? – Read the FAQ's

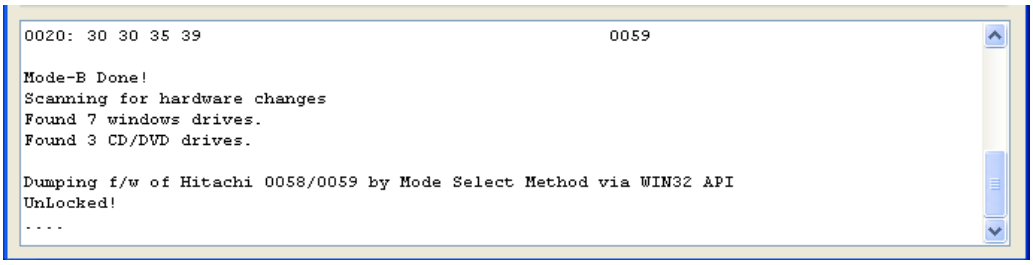


Then, click **Read to Source**

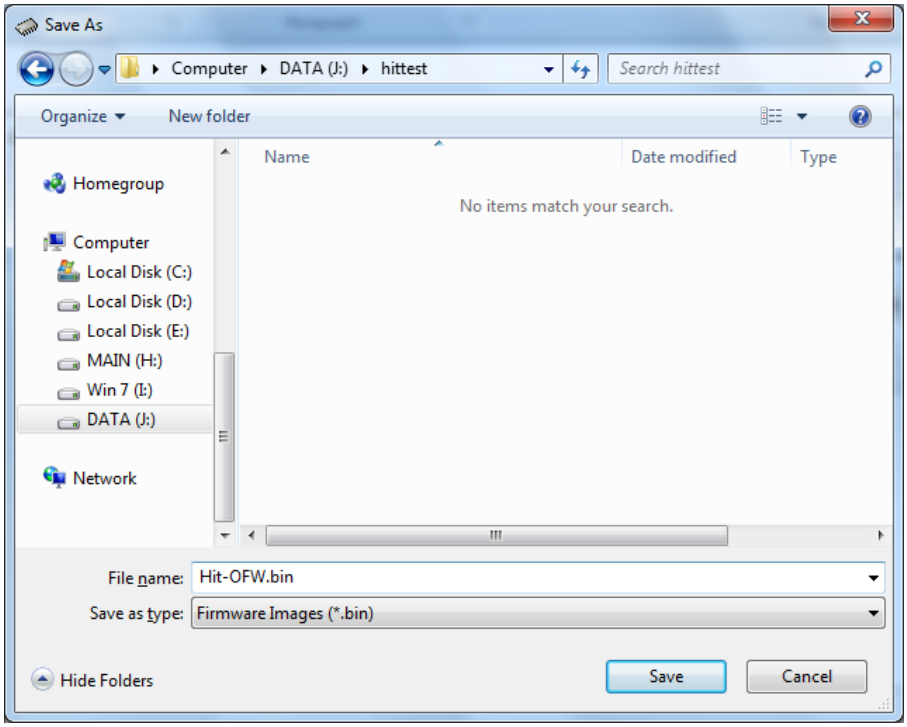


You should see something similar to below

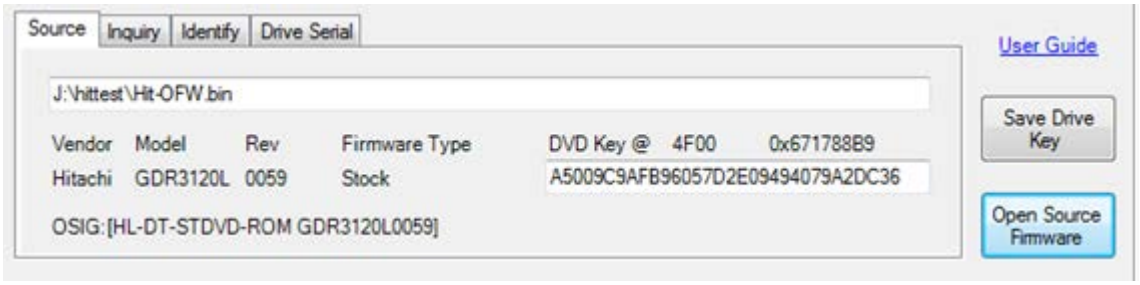
Things not going as expected? – Read the FAQ's



Once firmware is read, JungleFlasher will prompt you to save it.



Upon saving the Firmware from the Drive, you can verify the key appears good and it reports as **GDR 3120 (ROM Ver)**



The **Running Log** should also show this data.

[FLASH iX FIRMWARE - CLICK HERE]

Things not going as expected? – Read the [FAQ's]

UNLOCKING v79

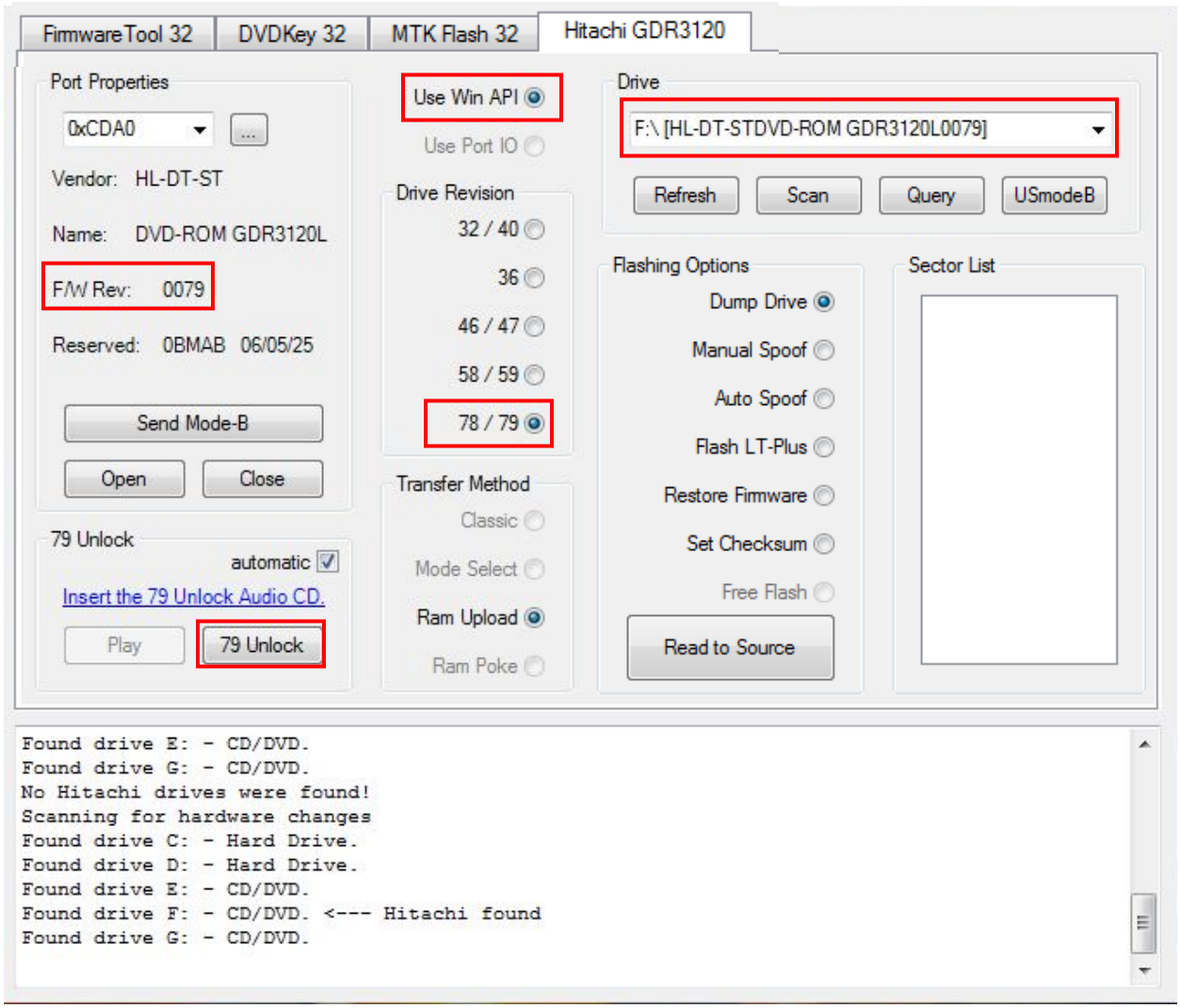
FIRST Ensure ModeB is set

V79 ONLY

The Hitachi v79 requires 'unlocking' via Audio CD which can be downloaded **here**

Burn the .bin, using the cue sheet in **IMGBurn** (done by right clicking .cue file and selecting "burn with imgburn") and write to CD-R

Insert the disc into the Hitachi v79, wait for it to spin up (windows media player may try to open! - just close it) then click **79 unlock**



JungleFlasher should display a log similar to the one below.

Things not going as expected? – Read the FAQ's

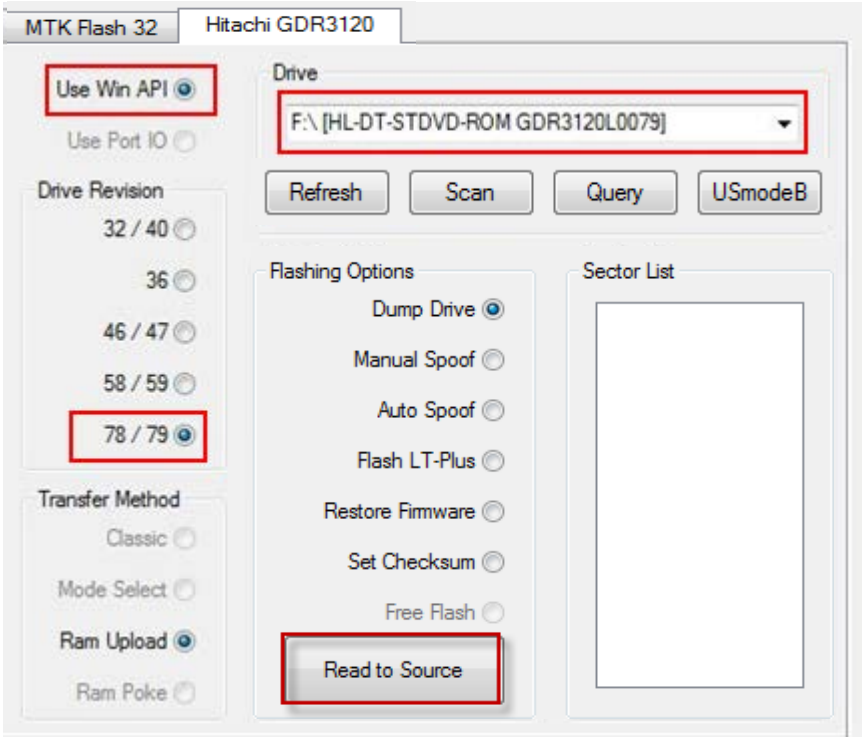
```
Found drive E: - CD/DVD.
Found drive F: - CD/DVD. <--- Hitachi found
Found drive G: - CD/DVD.
Playing 79Unlock Audio CD
Pausing 79Unlock Audio CD, after 500mS
Ejecting 79Unlock Audio CD
Setting bit 3 @ 0x5BD
Executing code in Ram
Done!
```

The Drive is now unlocked!

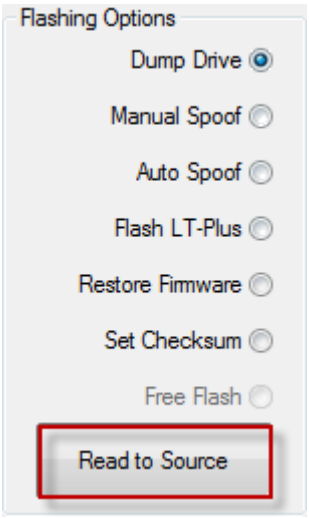
UNLOCKED - PROCEED! NOW TREAT IT AS PER A 78 – CONTINUE FROM POINT IN FLOWCHART YOU WERE AT -CLICK HERE

V78 / V79

Now, onto dumping the drive. With the V79 **unlocked**, or the v78 in **ModeB** We can now dump the drive using **RAM Upload** method

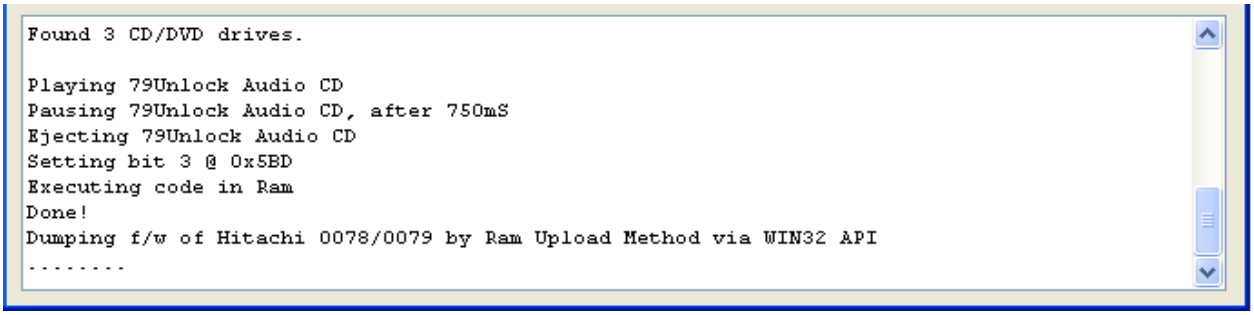


So, click **Read to Source**

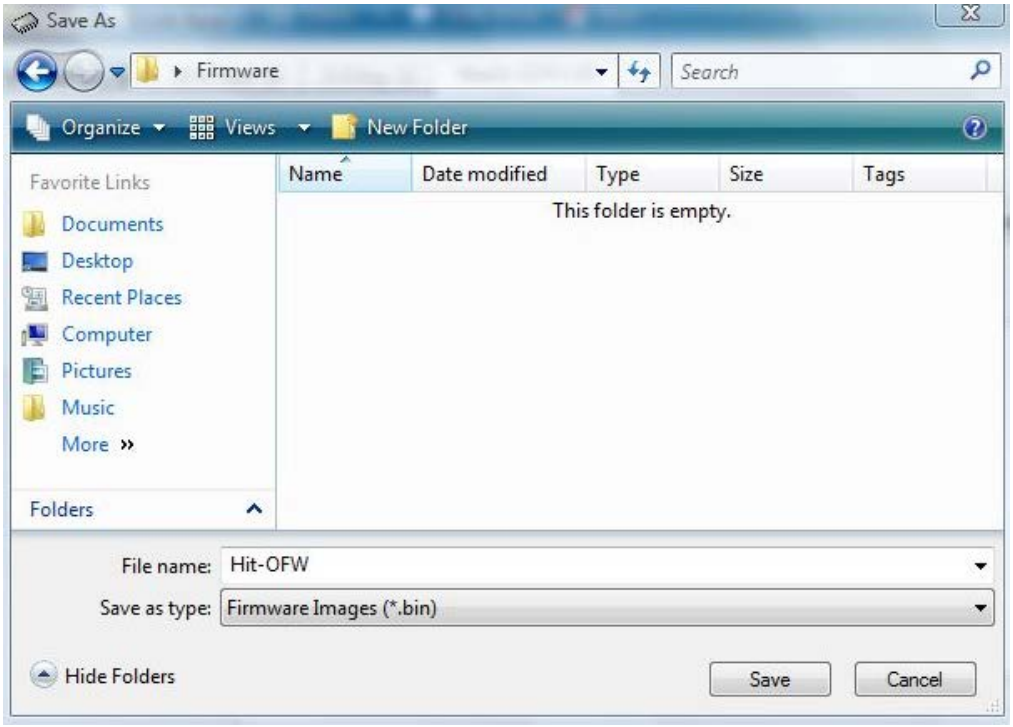


Things not going as expected? – Read the FAQ's

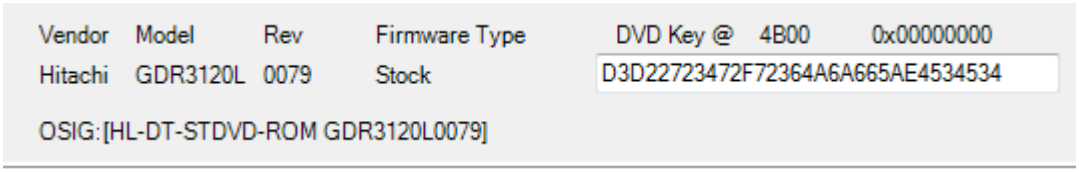
JungleFlasher will now dump the drive using **RAM Upload Method**



Once it has read the Firmware it will prompt you to save the Firmware.



Once saved, it will open it as S**ource** in F**irmwareTool32.**



FLASH iX – CLICK HERE TO PROCEED!

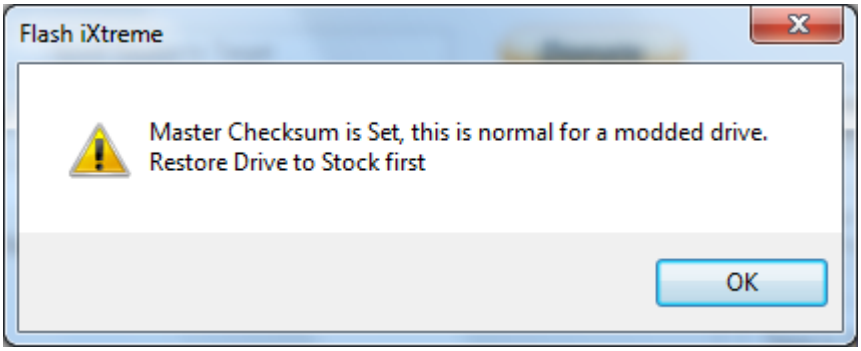
Things not going as expected? – Read the FAQ's

Flashing iXtreme to a stock Hitachi Drive

Flashing iXtreme to a Hitachi has taken a huge step in development with JungleFlasher's methods.

JungleFlasher **WILL NOT** allow you to flash iXtreme over iXtreme, it will detect the checksum and detect its hacked by checksum and force restore first.

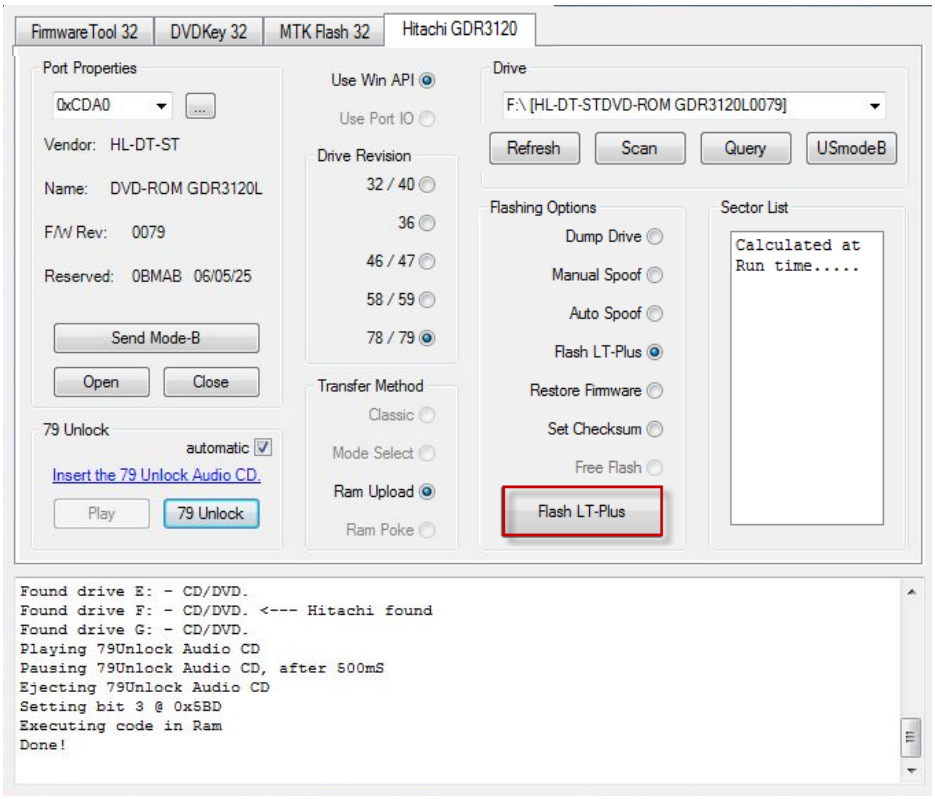
Typical error if user tries:



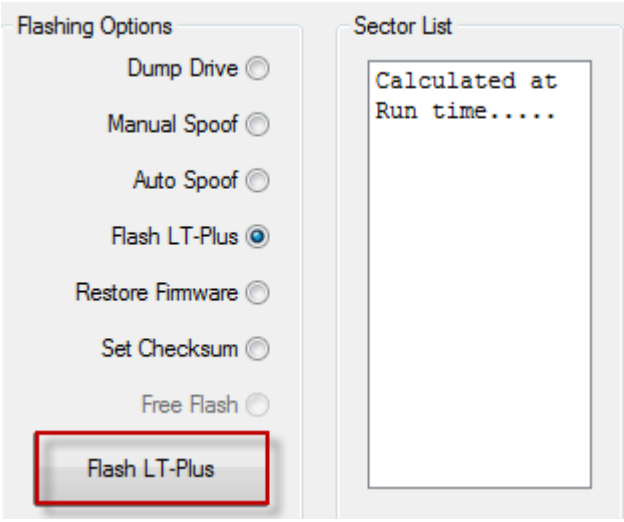
So, onto flashing iXtreme

You will need the **JungleFlasher Firmware Pack** for this to work.

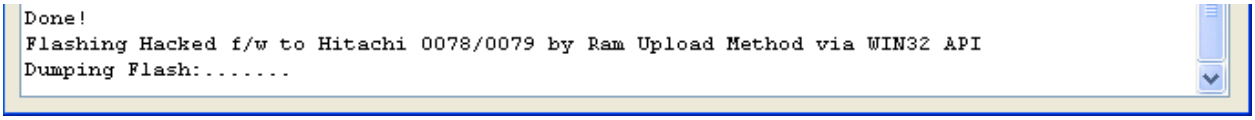
With the drive in **Mode-B** (and Unlocked if a v79) simply select **Flash iXtreme** from the **Flashing Options** list



Then, click **Flash LT Plus**



JungleFlasher will then dump the drive so it can compare sectors that will need to be written.

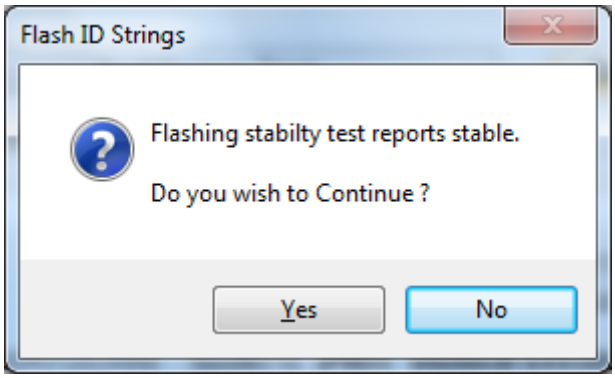


Things not going as expected? – Read the FAQ's

JungleFlasher will seemingly take control, don't worry, this is normal.

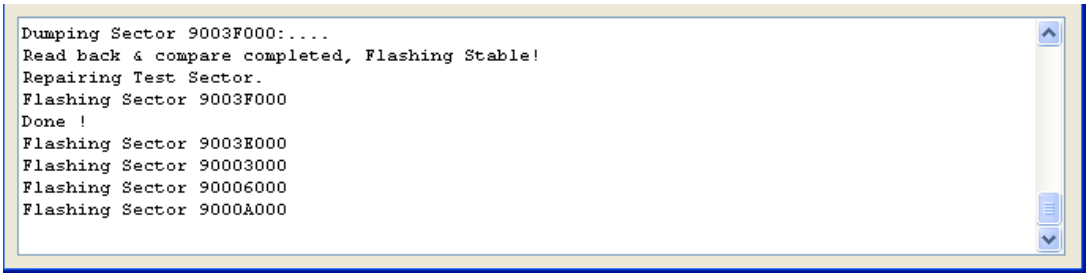
If you view the log, you see that JungleFlasher has automatically loaded iXtreme LT-Plus 1.1, copied all your data (key sector 90004000 isn't touched) into iXtreme, and flashed a test sector for stability.

The stability test should return as stable, if so, you will see this message.



If you wish to proceed, click Y**es**

Again, JungleFlasher will take over and you will see it flashing the sectors like below:



Once finished, JungleFlasher will verify the firmware written to the drive and report back

Things not going as expected? – Read the FAQ's

```
Flashing Hacked f/w to Hitachi 0058/0059 by Ram Upload Method via WIN32 API
UnLocked!
Dumping Flash:................................
Drive is rev 0059
Loading firmware from buffer
Inquiry string found
Identify string found
Drive key @ 0x4F00 1AB34C0258B0AB2B2AB9DC3B0CB62D02
Firmware Osig: [HL-DT-STDVD-ROM GDR3120L0059]
Firmware is:  Stock
Key database updated


Drive is Stock, rev 0059
Auto-Loading firmware file F:\JFBeta\Firmware\LTPlus-59-1.1.bin
MD5 hash:  e7c86ba77cd6f78295d4d037cc32df5f
Inquiry string found
Identify string found
Drive key @ 0x4F00 00000000000000000000000000000000
Firmware Osig: [HL-DT-STDVD-ROM GDR3120L0059]
Firmware is:  LT-Plus 1.1
11 Sector Differences Found
Flash Stability Test
Flashing Sector 9003F000
Dumping Sector 9003F000:....
Read back & compare completed, Flashing Stable!
Repairing Test Sector.
Flashing Sector 9003F000
Done !
Flashing Sector 9003E000
Flashing Sector 90003000
Flashing Sector 90005000
Flashing Sector 90006000
Flashing Sector 9000A000
Flashing Sector 9001C000
Flashing Sector 90027000
Flashing Sector 9002E000
Flashing Sector 90033000
Flashing Sector 90034000
Flashing Sector 90035000
Done !
Write verify test..
Dumping Flash:................................
Read back & compare completed, Write Verified!
Flash Complete !
```

Power Off – Disconnect drive, connect SATA back to console and test!

YOU ARE FINISHED – RETURN TO START OF TUTORIAL

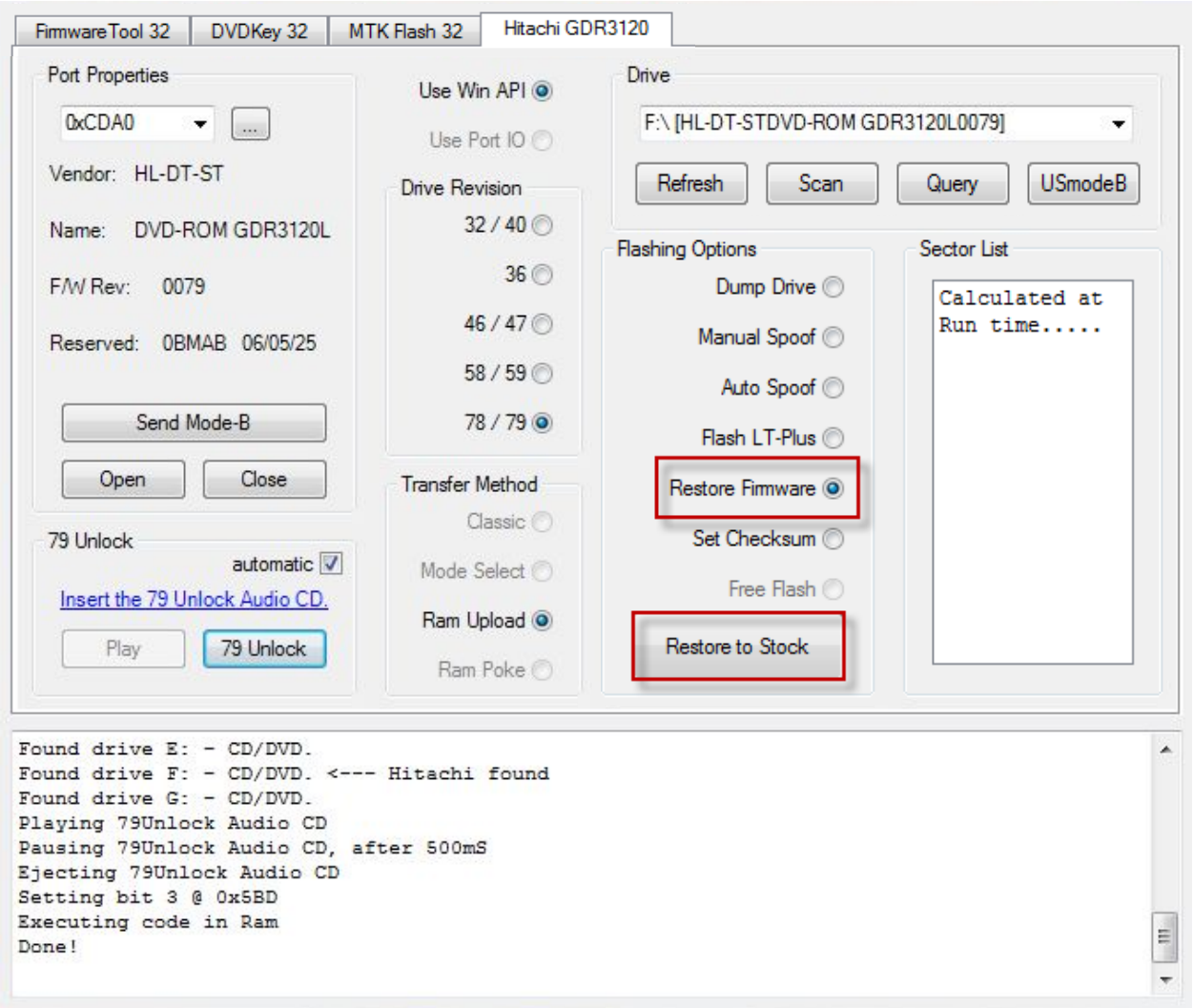
Things not going as expected? – Read the FAQ's

Restoring from Hacked Firmware

As the title suggests, it is simply a reversal of flashing the Drive with Hacked Firmware. This also applies to Hitachi Drives Spoofed as other Drive types / Revisions.

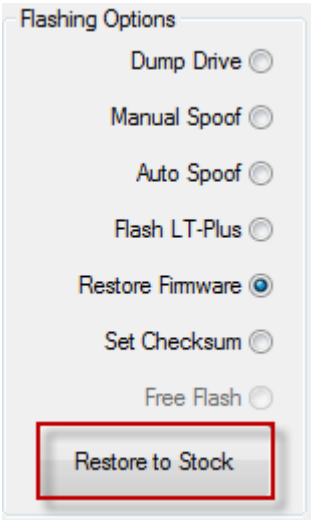
Again, JungleFlasher will depend on the **JungleFlasher Firmware Pack** being in the same directory as **JungleFlasher.exe**

With the Drive in **Mode-B** (and **unlocked** if it's a v79) simply select **Restore Firmware** from the **Flashing Options** list



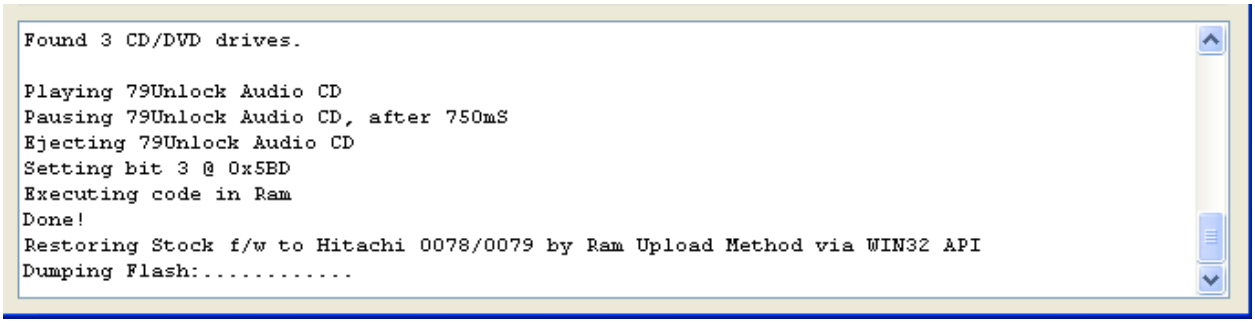
Then, click **Restore to Stock**

Things not going as expected? – Read the FAQ's



JungleFlasher will dump the Hacked Firmware from the drive, check key location and compare to the corresponding Original Firmware in the **Firmware Pack**

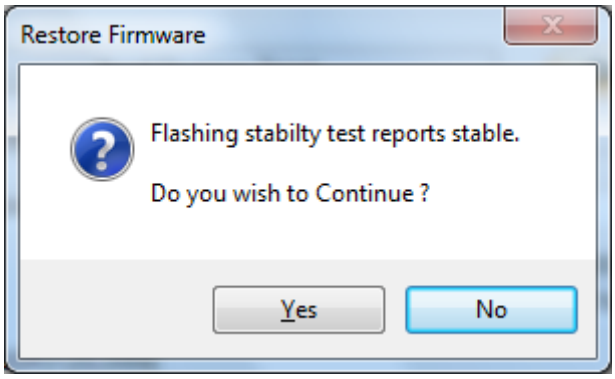
JungleFlasher will take control throughout this.



After it has dumped and compared the firmware, it will flash a test sector. If this flashes ok, it will report it has passed the **Stability Test**

It should show as below

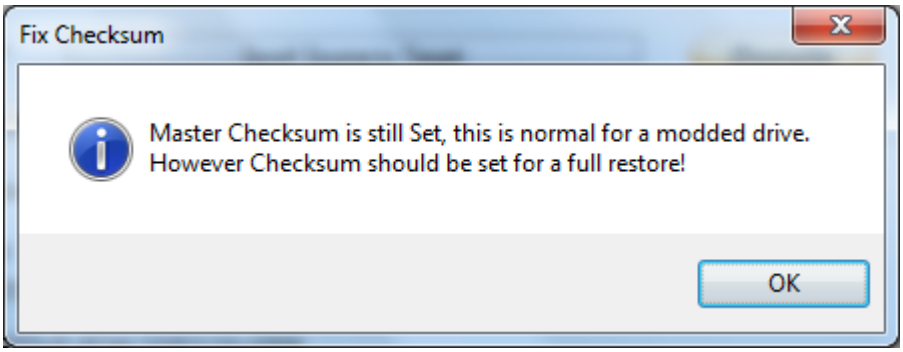
Things not going as expected? – Read the FAQ's



Click **Yes** to proceed

Again, JungleFlasher will take control and flash the sectors required

It will then check the checksum and prompt you to fix the Checksum.



Clicking Ok will fix Checksum for you

Check Log for confirmation

```
Setting Checksum!

Calculated Checksum 0x671788B9
Actual Checksum     0x00000000
Flashing Sector 9003E000
Dumping Sector 9003E000:....
Read back & compare completed, Write Verified!
Flash Checksum Complete !
```

PROCEED TO FLASH iX FW

Things not going as expected? – Read the FAQ's

Spoofing a Hitachi Drive to report as a Different Drive Revision / Version

NOTE _ SPOOFING DRIVES IS NOT ADVISED FOR XBOX LIVE USE

If you wish to flash a Hitachi Drive using JungleFlasher and change the **Drive String ID,** you should follow the procedure of:

1. Restore to Stock if necessary
2. Flash iXtreme to the Drive

IF YOU HAVE FOLLOWED THE FLOWCHART YOU SHOULD BE STARTING HERE!

3. Auto Spoofing **OR** Manual Spoofing

WARNING – YOU MUST

Flash iXtreme to the drive first before Auto/manual Spoofing

Manual Spoofing

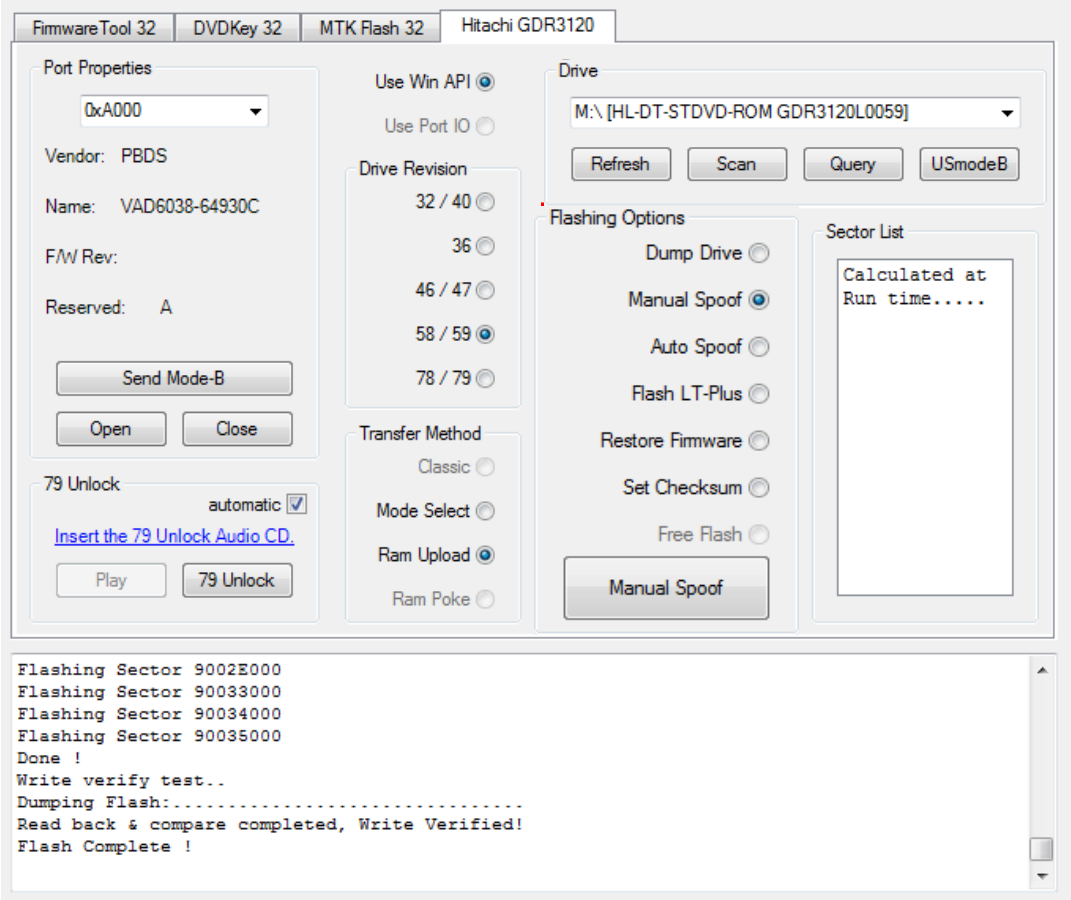
As usual you will need to first get the Drive into **Mode-B** (v79 unlocked) and assigned a drive letter (VIA / No Drivers, utilize PortI0)

The drive should, as above, be flashed with iXtreme to start

Open JungleFlasher and proceed to the **Hitachi GDR3120L tab**

Ensure correct **Drive Revision** is selected; choose chosen transfer method (Pre78 use **Mode Select** or **RAM Upload**, v78/79 users **can only use RAM Upload**)

Then, select **Manual Spoof** radio button, Then press **Manual Spoof** Button



You will then be presented with the screen below,

You can alter the **drive key** by manually typing it/pasting it/loading a saved key.bin
(**Key.bin can be saved** by loading donor drives firmware in FirmwareTool32 as Source and Clicking **Save Drive Key.)**

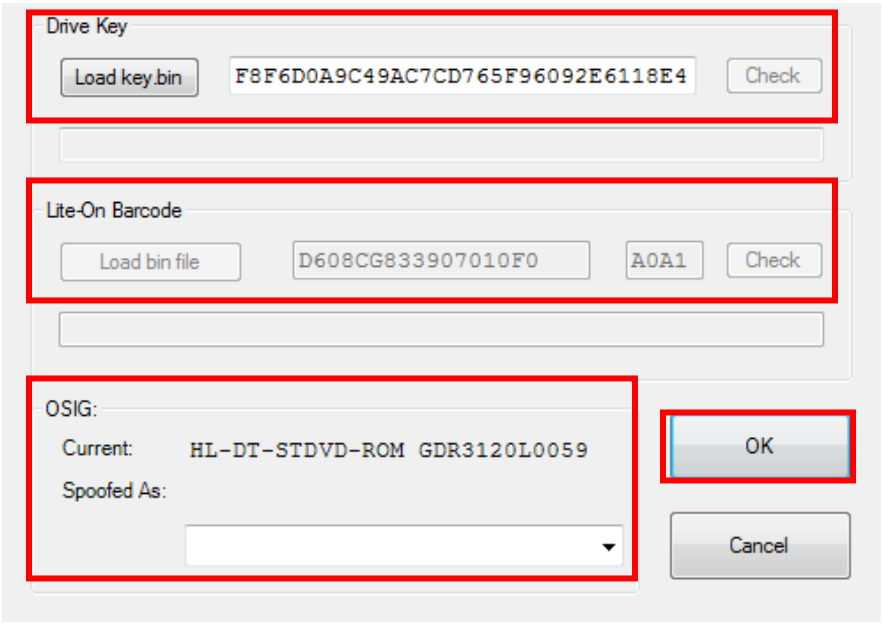
You can Change the **OSIG (ID String)** by selecting the desired drive from the drop down list,

And IF you have selected a **LiteOn drive** from **OSIG list** then you are able to enter the **liteon Barcode** details by either:

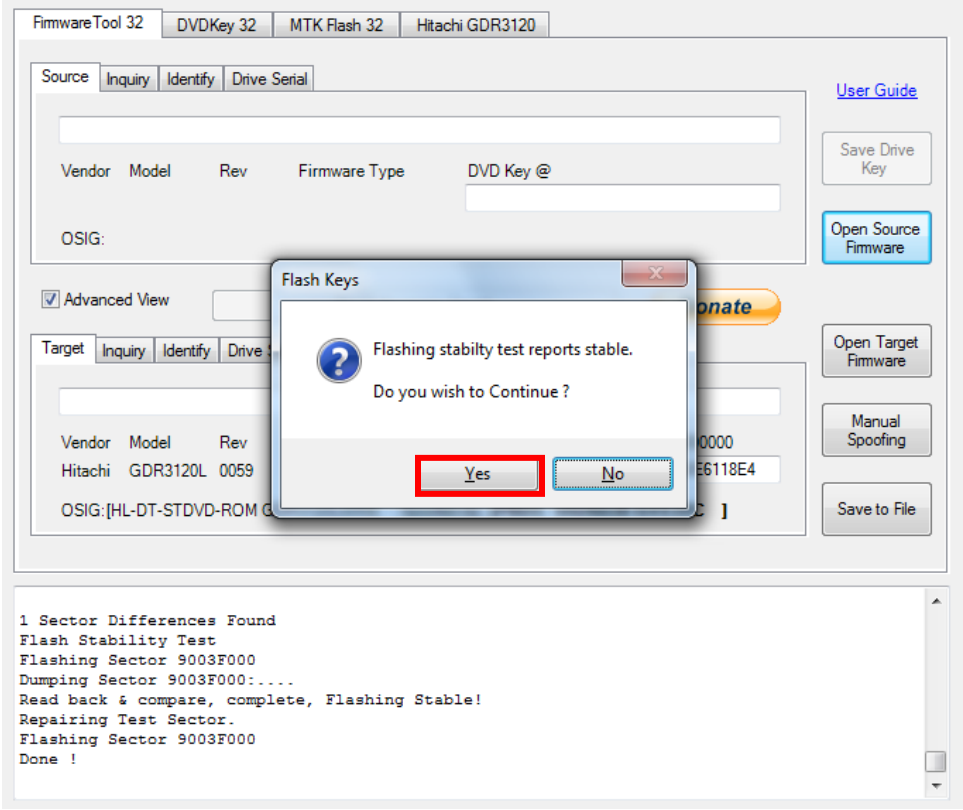
1. If you have the **Inquiry.bin** from the Donor Lite-On, you can load it through **Load bin file** button and navigating to the file and opening it.

2. If you have the **Donor Lite-On Drive** to hand, you can manually type the Alphanumeric code on the top of the Drive like shown below

When you have selected **ALL** the sections you require to be changed, press the **OK** Button

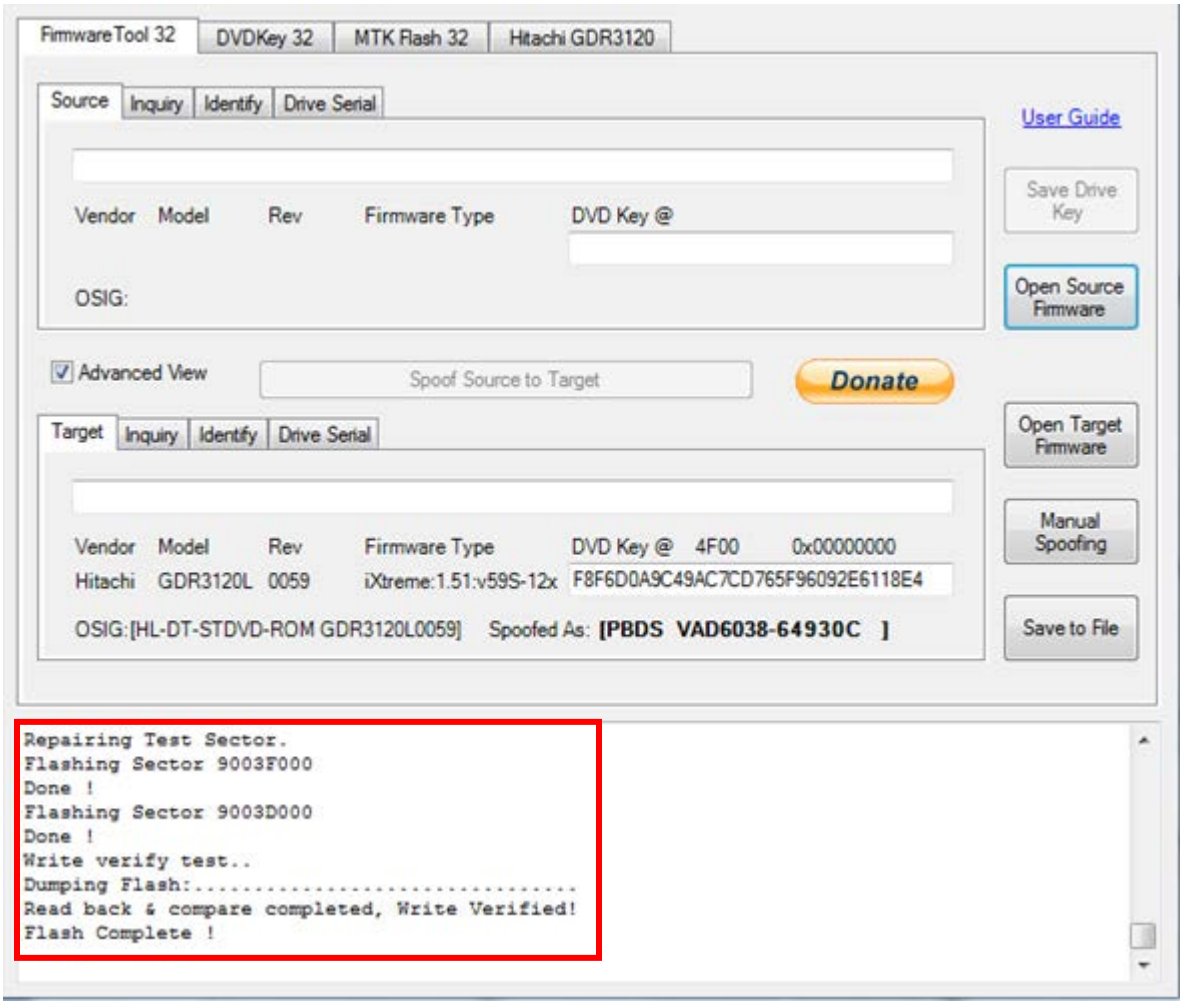


JungleFlasher will then read, compare and carry out a test flash and ask if you wish to continue! Select **YES**, Manual spoofing will be carried out!



The example below is a Hitachi – manually spoofed to show as a BenQ!

Things not going as expected? – Read the FAQ's



Power Off – Disconnect drive, connect SATA back to console and test!

Job Done ☺

YOU ARE FINISHED – CLICK HERE TO RETURN TO START OF TUTORIAL

Things not going as expected? – Read the FAQ's

Auto Spoofing a Hitachi

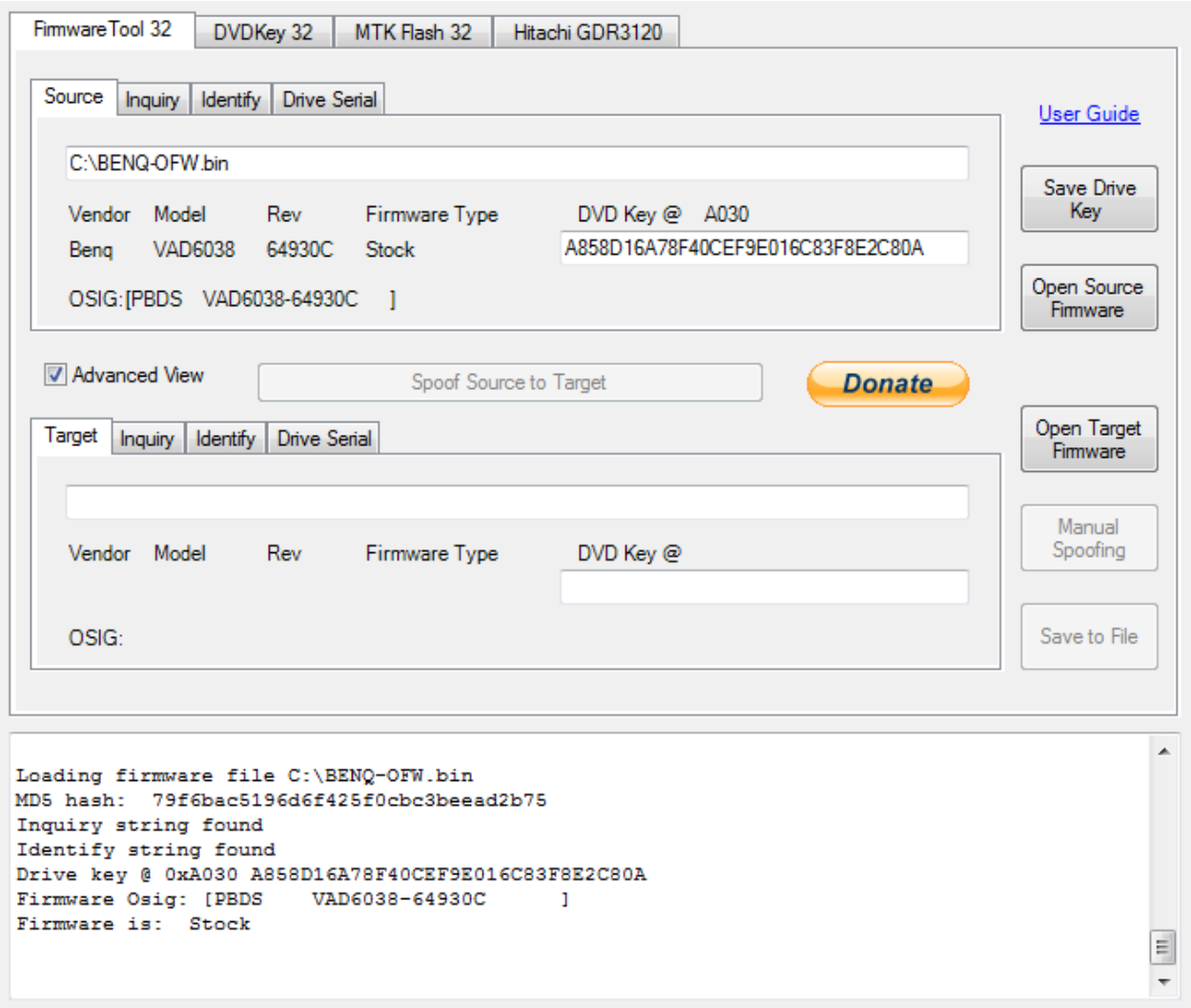
As with all Hitachi Tasks, you must set **Mode-B** **(and unlocked if v79)** first, have a drive letter assigned if using **Win API**, or, PortIO for VIA / No Drivers.

Ensure Drive is flashed with iXtreme prior to spoofing!

Proceed to the **Firmwaretool 32** tab

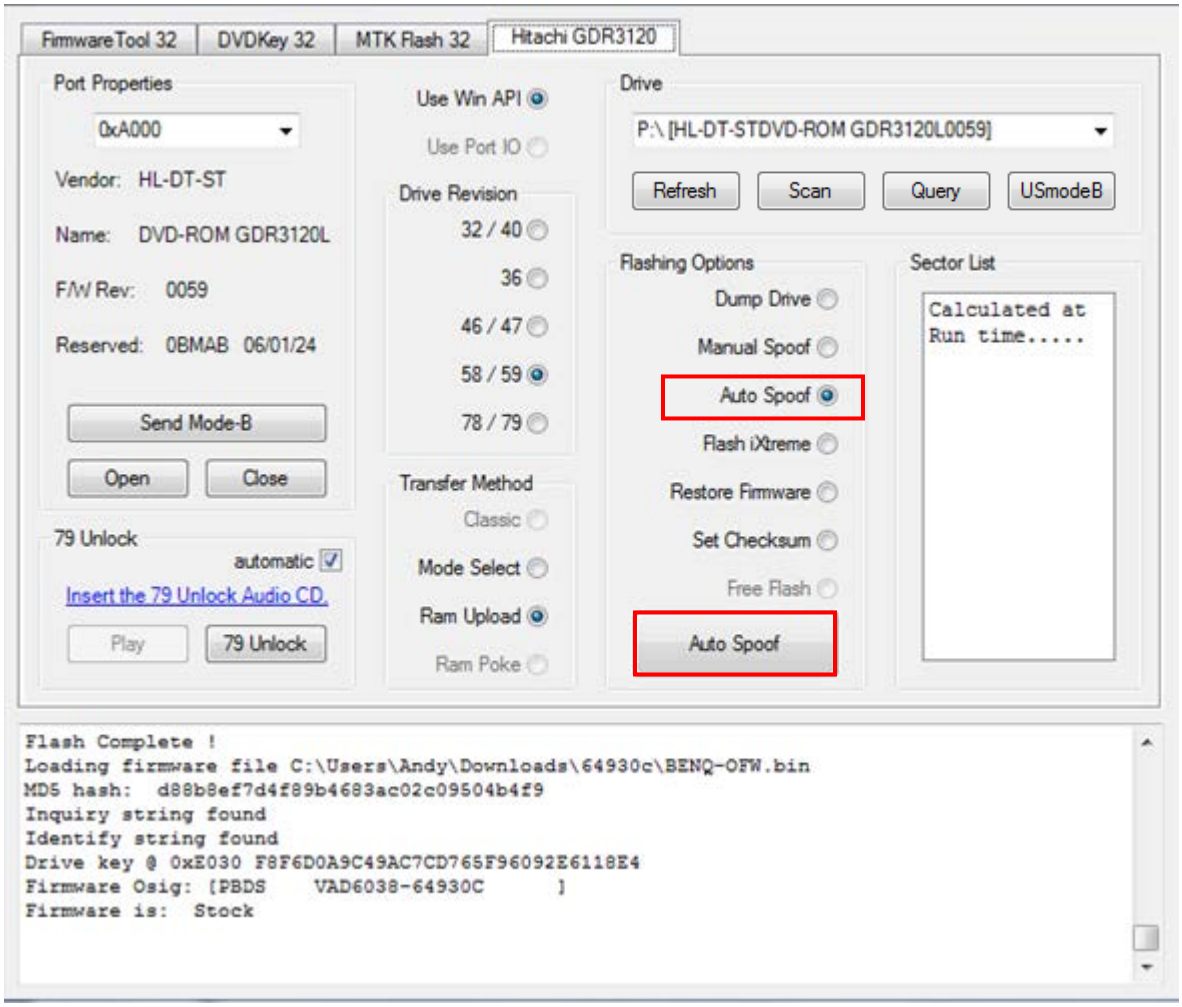
Click **Open Source Firmware** button, load the Dumped firmware file from the donor drive.

In this example from a BenQ drive!

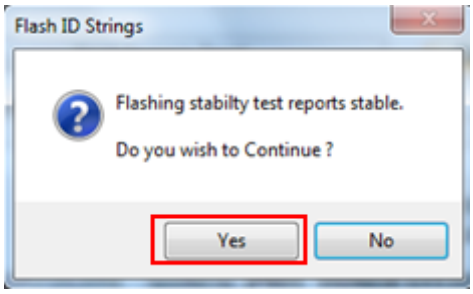


Things not going as expected? – Read the FAQ's

Now select the **Hitachi GDR3120** tab, select the **Auto Spoof** radio button. Then press **Auto Spoof** button

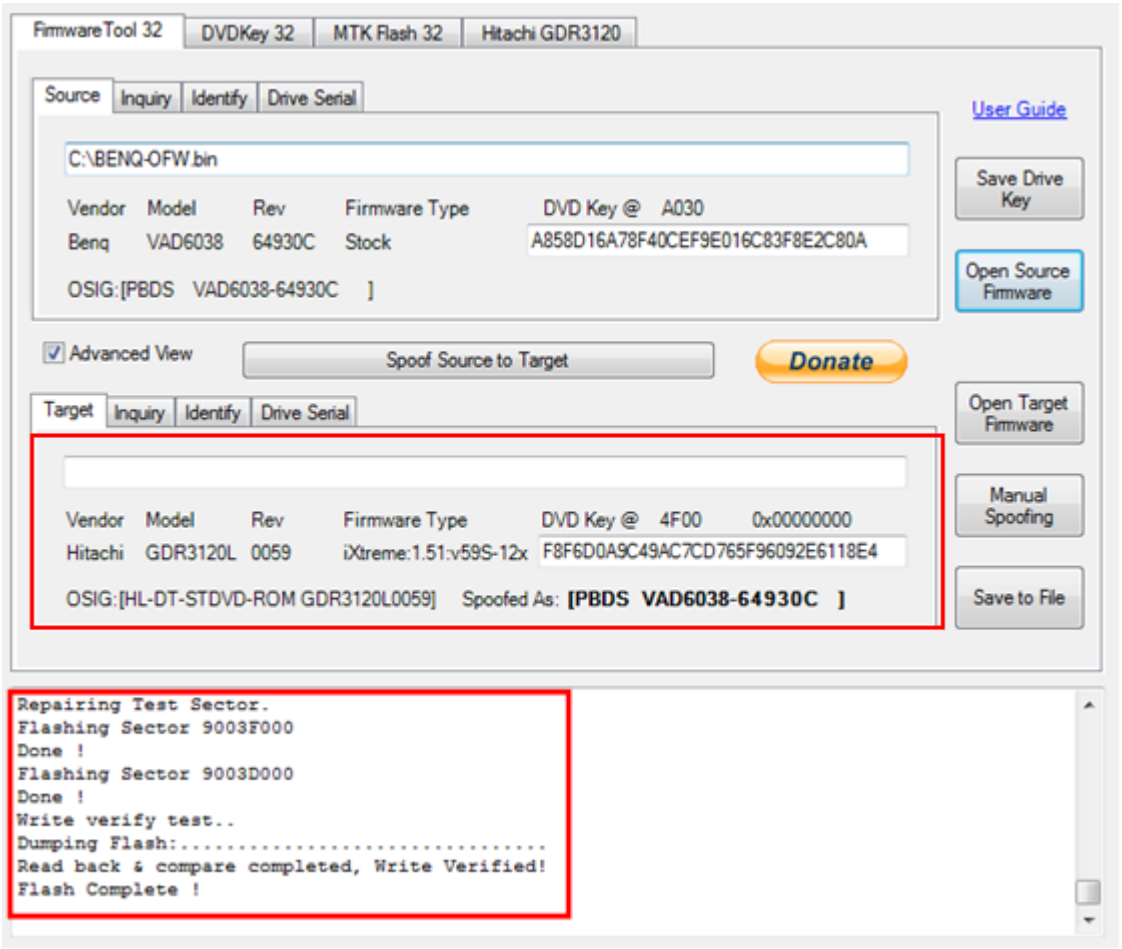


Jungleflasher will then test flash a sector for stability check and ask for confirmation to proceed! Select **YES!**



Jungleflasher will then proceed to read, compare and write to drive – **Firmwaretool 32** tab will automatically open to show you the **source** (the drives previous firmware) and the **target** (the Firmware that is now on your drive – including the spoof information)

Things not going as expected? – Read the FAQ's



Power Off – Disconnect drive, connect SATA back to console and test!

Finished! ☺

YOU ARE FINISHED – CLICK HERE TO RETURN TO START OF TUTORIAL

Things not going as expected? – Read the FAQ's

LiteOn (Phats and Slims)

Currently in circulation there are several distinct versions of LiteOn drive. These can be split into 2 Categories:

Phats: **Firmware versions 74850C , 83850C , 83850C v2, 93450C, 02510C**

These all had differing methods of obtaining the drive keys (which have been kept in the tutorial for completeness) however a new method “Pogo Mo Thoin”(PMT) has been released and can be used to obtain all the required info from ALL these drives.

The only drive that you *shouldn’t* need to use the PMT method for is the **83850C v1 with stock Firmware**(as this can be done without opening the drive case! – the easier the better! Right?)

NOTE: AFTER DASHBOARD UPDATE (13146) ALL PHAT LITEONS ARE NOW STOCK 02510 FW

NOTE: ALL PHAT LITEON POST DASH UPDATE WILL REQUIRE PMT/PROBE 3 or MRA

IF YOU HAVE A STOCK 83850 v1 YOU CAN DUMP DUMMY.BIN BEFORE UPDATE, THEN UPDATE. MANUAL LOAD LT+1.91 AND SPOOF. THIS WILL AVOID OPENING YOUR DRIVE.

The other remaining drives are the

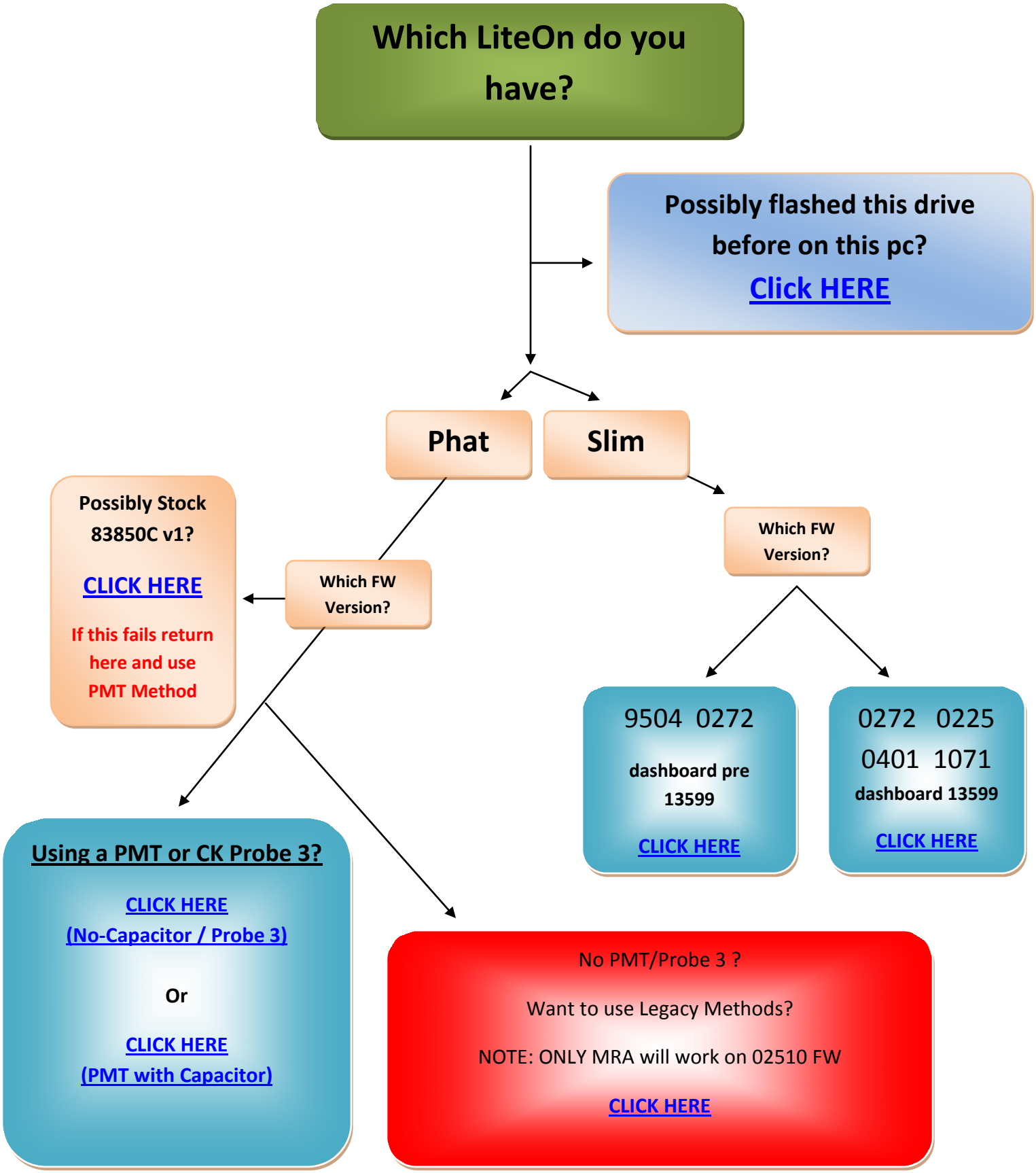
Slims: **Firmware Versions 9504, 0272 , 0225 , 0401 , 1071**

Currently Only the LiteOn Slim Drive with 9504/0272 (pre 13599 dashboard) can be written to (unless you have a unlocked 0225/0401 – Rare!) The Drives with Firmware Version 0272 (if you have dashboard 13599) 0225, 0401 and 1071 can ONLY have their Keys Read unless they have been modified or unlocked

NOTE: AFTER DASHBOARD UPDATE (13146) ALL SLIM 9504 LITEONS ARE NOW STOCK 0272 FW – AFTER DASHBOARD UPDATE (13599) 0272 ARE NOW LOCKED!

NOTE: IF YOU HAVE NOT ALREADY DONE SO – UPDATE YOUR XBOX DASHBOARD TO THE LATEST DASHBOARD BEFORE WRITING LT+ FW.

PROCEED



Things not going as expected? – Read the FAQ's

Lite-On PLDS DG-16D2S(-09C) – Legacy Methods

Firmware versions 74850C , 83850C , 83850C v2, 93450C

Overview

With the release of the 83850C firmware , LiteOn drives required two totally different methods. With the release of the 83850C v2 and the 93450C there ***was*** no known way to extract the key. However there is now a method to dump the whole FW from any of these LiteOn drives! *(which is the ONLY method to get the key from the 83850C v2 & the 93450C)* Although MRA method works on all (current) LiteOn's - DVDKey32 / LO83Info will always remain the simpler method to obtain info from earlier drives.

The **74850C** requires additional hardware (it **requires** the utilization of a RS232 to TTL serial hardware, or a popular variant such as **Xecuter CK3 Pro or Xecuter CK3 Lite with the Xecuter Probe (v1 or v2)** or **Maximus USBXtractor & powerunit** or **Maximus Xtractor (with optional spear)** to obtain the drive specific data (key/inquiry/identify/Serial) which once extracted are used to create the dummy.bin

Whereas the **83850C v1** does **NOT** require additional hardware and can be dumped/flashed using only a SATA connection

The key/inquiry/identify/serial files are merged into a dummy.bin (this allows for easy manipulation of the drive info for placing into the iXtreme firmware). They contain information that is required for proper identification and security related issues.

The **83850C v2** was quickly released to combat key retrieval by the earlier methods so key retrieval using 83850C v1 or original method was no longer an option! This change occurred around July/Aug 09 drive manufacture dates. There is no outward difference between the 83850C v1 and the 83850C v2 – the only way to discover which you have is to try the 83850C v1 method! If successful you have the version 1 – IF NOT Jungleflasher will tell you, you have an 83850C v2 and Lo83 function is ONLY for v1.

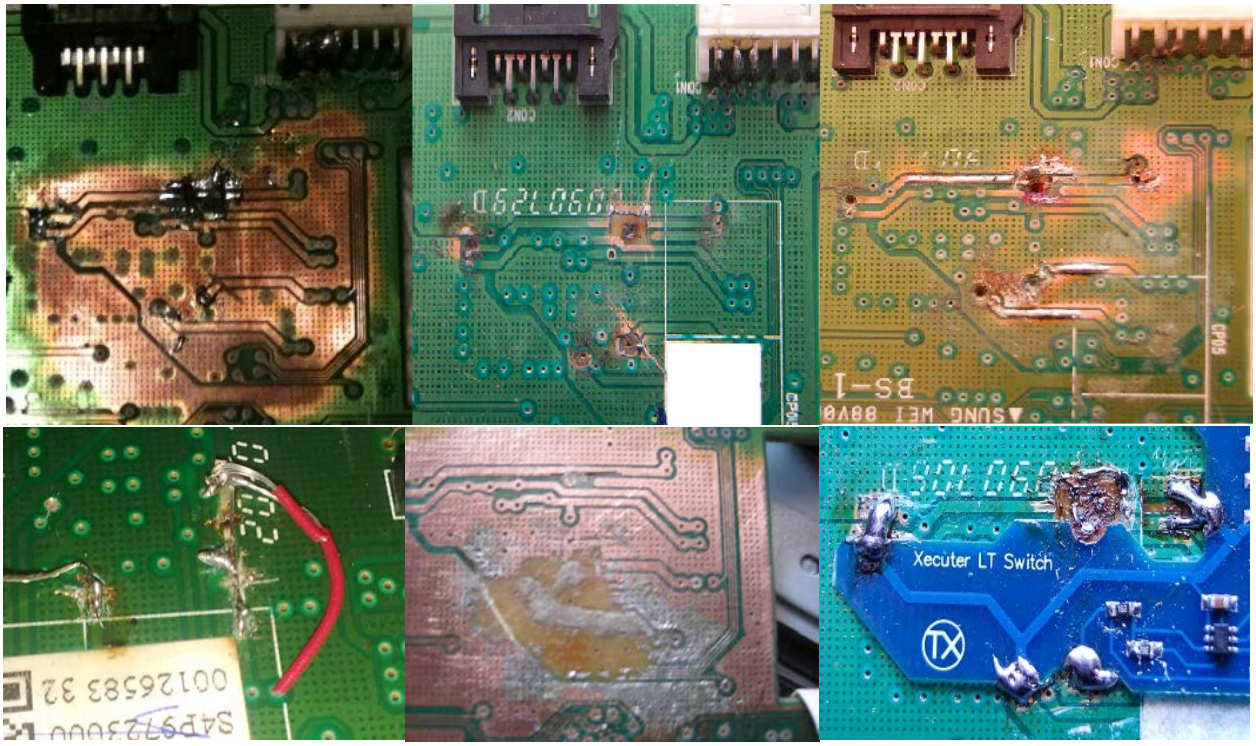
The **93450C** quickly followed – Once again key retrieval was not an option with simple SATA commands or probe used for 74850C

Now available, is a method to dump the whole firmware from ALL current LiteOn Drives – The MRA Hack method is a little more complex than previous methods and requires some soldering skills and cutting and reconnection of traces on the PCB! However there are now some other options available – the best of these are described in this tutorial.

WITH THIS IN MIND – IT SHOULD ONLY BE ATTEMPTED BY SOMEONE WITH SOME PREVIOUS SKILL OF WORKING WITH ELECTRONICS / SOLDERING

It is recommended to use the original (Simpler) methods for the 74850C and the 83850C v1. The FULL firmware dump can be performed on these drives – BUT it is a lot easier and less likely to go wrong if using the earlier methods described in this tutorial.

Here are some examples of those people without skill enough for the job!



If you are going to produce results like these – Don't expect any sympathy!

And - expect to pay to have a professional fix it for you!

YOU HAVE BEEN WARNED!

Things not going as expected? – Read the FAQ's

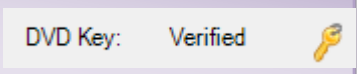
LiteOn PLDS DG-16D2S

Which FW Revision?

(read the label on drive lid)

IF you have previously flashed this drive and think you have its details in the Key Database – Consider this option! No need to re-dump or MRA the drive?

– CLICK HERE –



Otherwise continue through the flowchart

74850C
(Requires extra HW if stock)
See Note 2

83850C
(SATA only)
See Note 2

83850C V2 or 93450C
(Pre-flashed with ix1.61- CLICK HERE)
STOCK Firmware OR iX LT - CLICK HERE
(Additional skills and some modification req'd)

Stock Firmware?

No?
Pre-iX LT, continue down chart! –
If LT *See Notes 1&2*

Stock Firmware?

Yes

Yes

CLICK HERE

CLICK HERE

CLICK HERE

Previously obtained LiteOn files, but don't have Dummy.bin
CLICK HERE

LiteOn Erase/Write –
CLICK HERE

83850C, tried it but JF says it's a V2?
FOLLOW LINK ABOVE!

1. *If your Drive has been previously flashed with iXtreme LT – then you will no longer be able to use 74850C or 83850C v1 or 'Dummy-from-iXtreme' methods to retrieve Dummy.bin! A full dump can still be performed using MRA method* CLICK HERE

2. During Flashing process – IF your drive has been flashed before (i.e. NOT a VIRGIN DRIVE) OR you have **not** used MRA hack to get a FULL OFW, then you are going to get a statement like this: `No Calibration data in source` This is normal for a PRE-FLASHED drives or you have used a Dummy.bin – Ignore it!

   If you wish to include this info from a 74850C or 83850C v1 VIRGIN drive – you must do a full dump using MRA style method - CLICK HERE

Things not going as expected? – Read the FAQ's

LiteOn "HALF TRAY OPEN" method!

To obtain the key and other drive specific info from LiteOn drives the user must be familiar with the correct method to set "Half Tray Open" – this is especially important when doing 83850C fw'd drives as the drive must be set into this position twice during the extract!

Using xbox360 to power the drive

If using a 360 to power the drive this method can be tricky to accomplish.

You need to power on the drive with **Eject status closed** but **Tray Half Open** – To do this using an Xbox 360 as Power source, eject the DVD drive, then, press eject to 'close' the tray. **Now this is the important part – you MUST remove the DVD power plug (the black cable with white plug on back of DVD-ROM) from the DVD Drive BEFORE it closes fully.**

Wait for a few seconds and replace the power plug into the DVD drive taking **extreme caution** to plug the plug the right way around – once done, the drive is now powered, console thinks its closed but it is in fact half open.

Using a Connectivity Kit / Xtractor / power dongle to power the drive

For this method, we still need to power on the drive with the "half open tray".

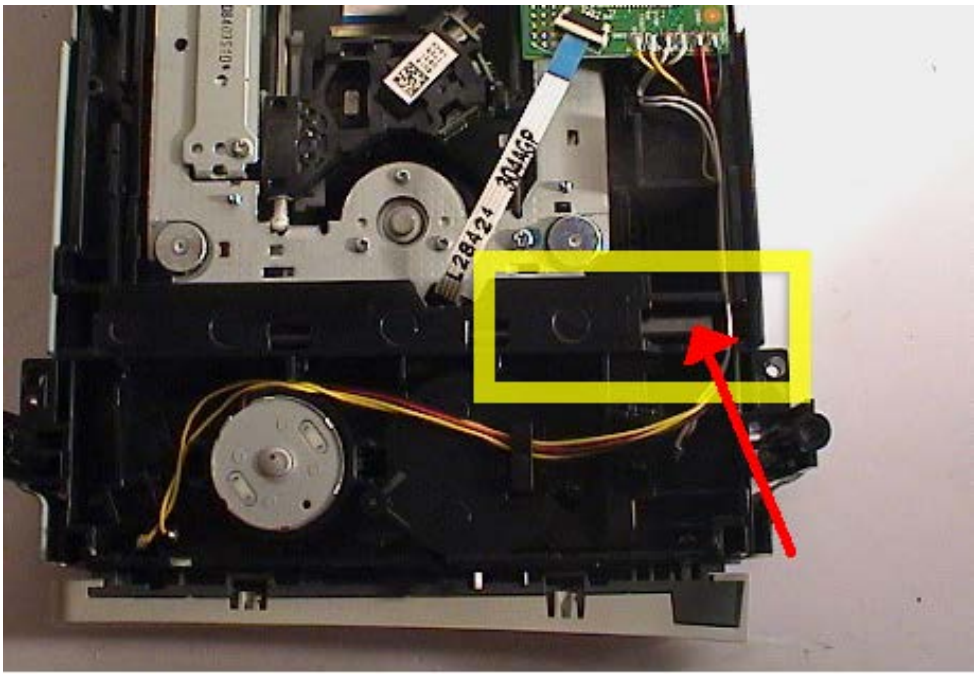
You need to power on the drive with **Eject status closed** but **Tray Half Open** – To do this using a connectivity kit/power unit/Xtractor as Power source, eject the DVD drive, then, press eject to 'close' the tray. **Now this is the important part – you MUST switch off the kit BEFORE it closes fully.**

Wait for a few seconds and switch the connect kit on again – drive is now at "half open tray"

(NOTE- if using Maximus power unit – you must **hold in** the eject switch till fully open then release to close – as it closes switch off, then switch back on!)

Manually

The easiest way to do this is to use manual eject before powering the drive, to manual eject simply push this slider along until the tray is released.



Then, pull the tray out fully and push half way back in. Now, hook it up to the PC using Connectivity Kit and SATA then power on. (If powering with Xbox – then DVD power plug must be removed before this process, with Xbox powered on – then power plug connected after tray position is set!)

Now, with the eject status set, Open JungleFlasher

RETURN TO FLOWCHART AND CONTINUE – CLICK HERE

If you have LiteOn files from previous extractions/methods

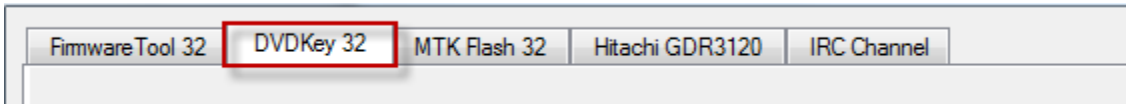
Jungleflasher – maintains backwards compatibility with files that have been extracted from earlier methods!

A FRESH extraction is recommended where possible – but the option remains available

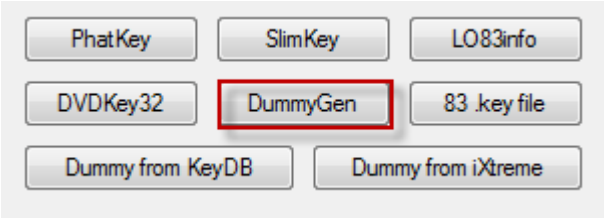
For 74850C Files (Key.bin/Inquiry.bin/Identify.bin) – Read On!

For 83850C File (*unique*.bin.key) – Click Here!

For 74850C firmware files **(Key.bin/Inquiry.bin/Identify.bin)** simply go to **DVDKey32** tab,



And press the **DummyGen** button – this will allow you to load each file into Jungleflasher which then creates a Dummy.bin and loads it as source. Ready for spoofing to target file and then to proceed onwards to erasing and writing!



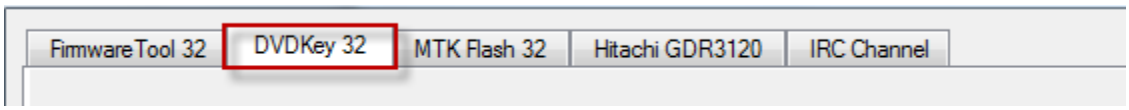
CLICK TO PROCEED TO FIRMWARE MANIPULATION

For 83850C v1 firmware files **(*unique*.bin.key)**

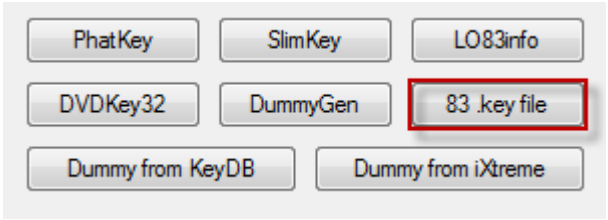
Things not going as expected? – Read the FAQ's

Note: If you wish to include calibration data from the 83850C v1 (VIRGIN drives ONLY) – you must do a full dump using MRA style method - CLICK HERE – if you are not bothered, continue!

Go to **DVDKey32** tab



Then press the **Import83.key** button



this will allow you to load the file into Jungleflasher which then creates a Dummy.bin and loads it as source. Ready for spoofing to target file and then to proceed onwards to erasing and writing!

CLICK TO PROCEED TO FIRMWARE MANIPULATION

Things not going as expected? – Read the FAQ's

Obtaining Key/Inquiry/Identify and Dummy.bin from iXtreme flashed Lite-On Drives (DOES NOT WORK ON iXtreme LT)

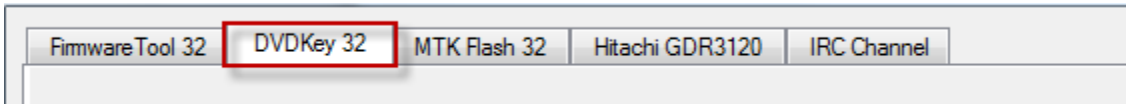
LiteOn drives of either FW version that have already been flashed with iXtreme can be easily dumped using only SATA connection (no requirement for probe or TTL convertor) ***this is a function of the iXtreme firmware NOT a workaround for dumping stock drives!***

For this method, we still need to power on the drive with the "half open tray".

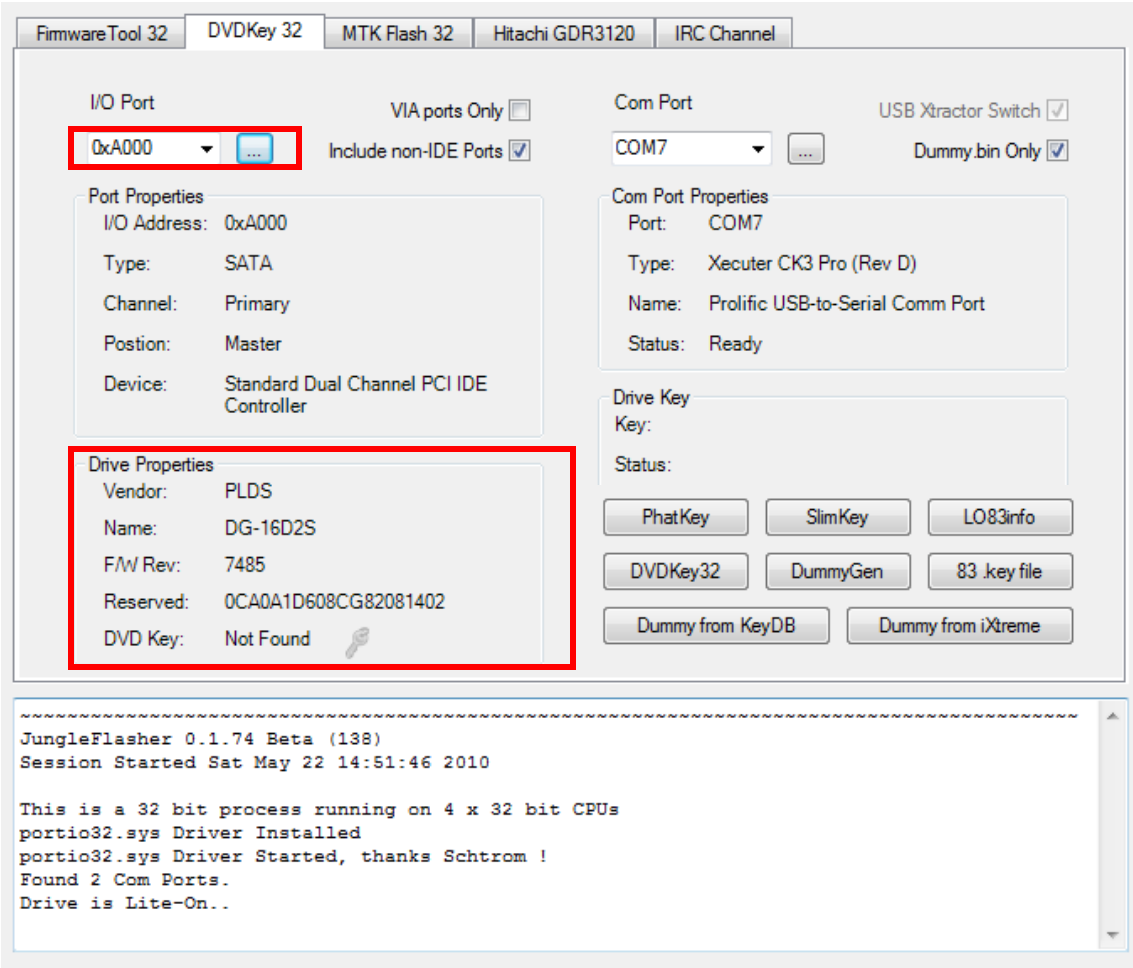
FOR INSTRUCTIONS ON HALF OPEN TRAY – CLICK HERE

Now, with the eject status set, Open JungleFlasher, you will be presented with the Welcome Screen. After a few seconds the main window will load.

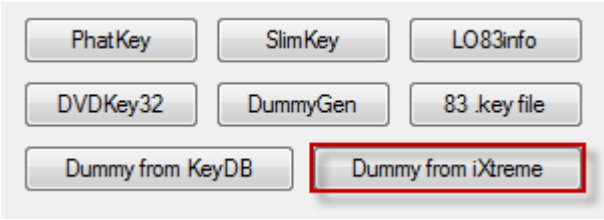
Now, click the **DVDKey32 Tab**



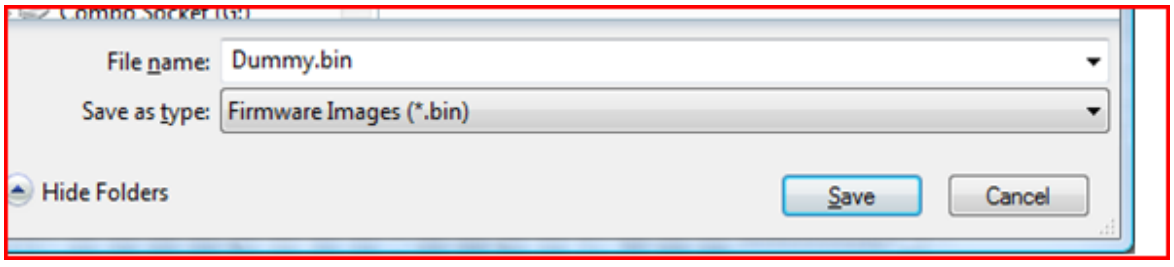
Select **Correct I/O port** (check for drive properties in the **Drive Properties** section) it should report as **PLDS DG-16D2S** (unless spoofed), you can choose to dump dummy.bin only as opposed to all 5 files (Key, Inquiry, Identify, Serial **and** dummy.bin) as dummy.bin contains all the information of the other 4 files.



Then, simply click **Dummy from iXtreme.**



Save as prompted,



[CONTINUE WITH FIRMWARE SPOOF – CLICK HERE]

Things not going as expected? – Read the [FAQ's]

Extracting Key and drive info from 74850C LiteOn

Note: If you wish to include calibration data from the 74850C (VIRGIN drives ONLY) – you must do a full dump using MRA style method - CLICK HERE – if you are not bothered, continue!

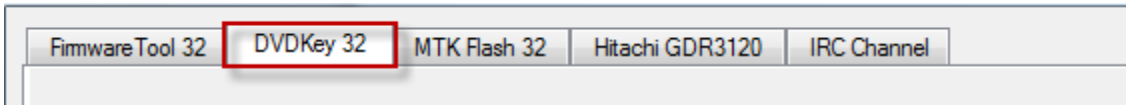
You need to power on the drive with **Eject status closed** but "**Tray Half Open**" –

FOR INSTRUCTIONS ON HALF OPEN TRAY – CLICK HERE

With the correct tray status

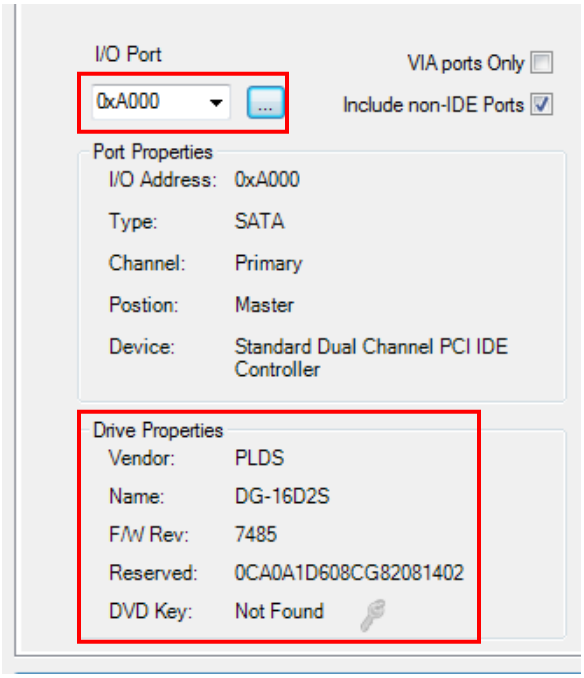
Open JungleFlasher,

As you are using **DVDKey 32** to obtain data, select **DVDKey32 Tab**



Check **Drive Properties** for **PLDS DG-16D2S.**

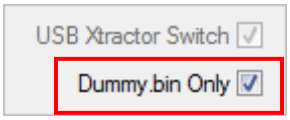
Select **Correct I/O port** (check for drive properties in the **Drive Properties** section)



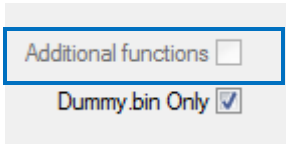
Select **COM port (relavant to your setup – shown in table below)**,

Things not going as expected? – Read the FAQ's

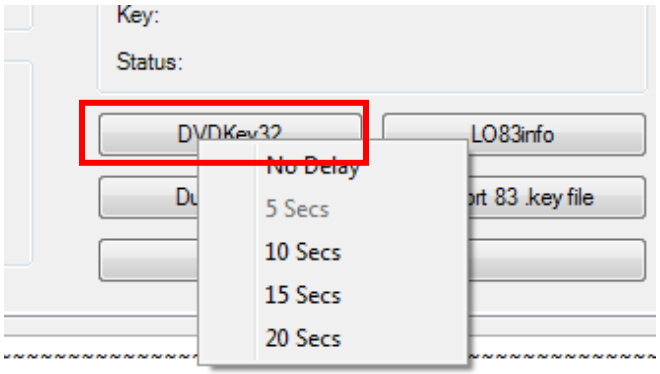
optionally, choose to dump dummy.bin only (shown in red)as opposed to all 5 files (Key, Inquiry, Identify, Serial **and** dummy.bin).



USB Xtractor user should enable **Additional Functions** check box (shown in blue)



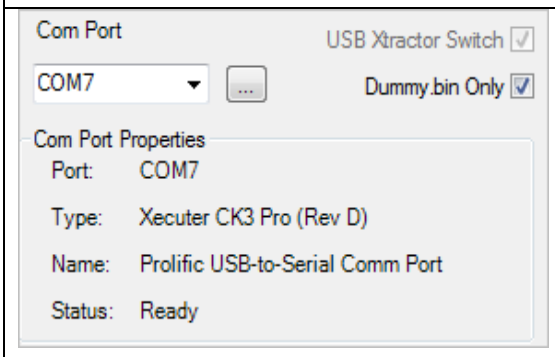
Right-click on **DVDKey32 button** for time delay settings if you require a little settling time to ensure probe is correct position before Jungleflasher attempts to read the key (time after button press before key read starts)

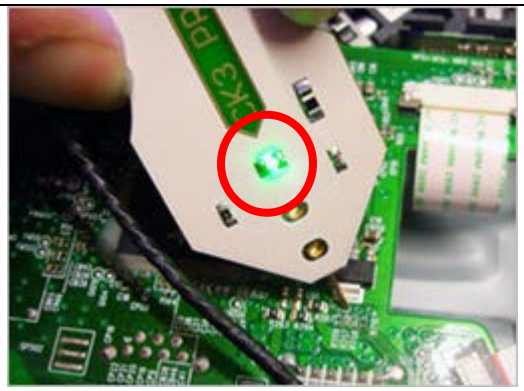


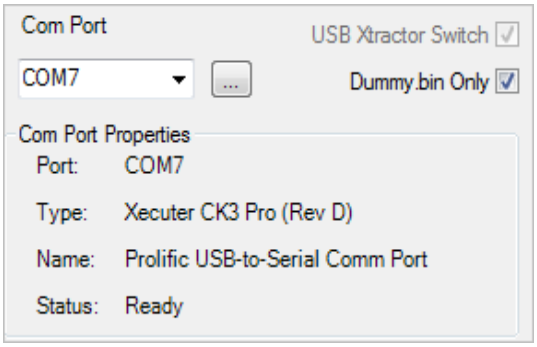
then **insert probe / spear** into R707 via **(as per table below)**,

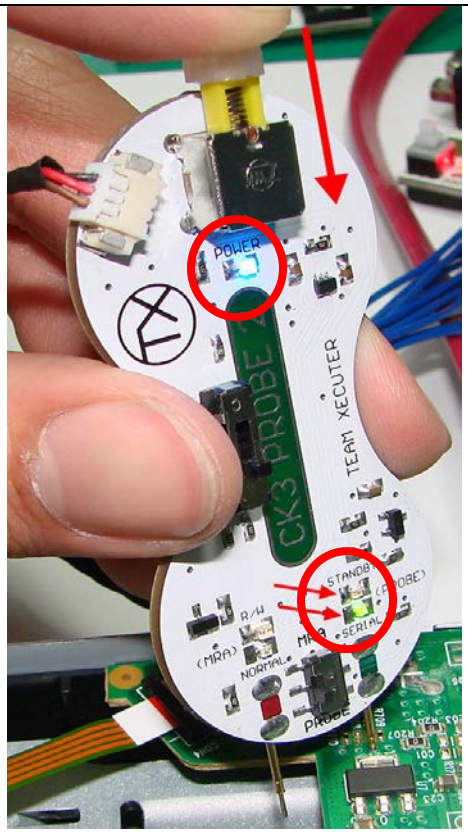
Things not going as expected? – Read the FAQ's

PROBE VARIATIONS AND LED INDICATION AS FOLLOWS

<table>
<tr><th>CHECKED / SELECTED THIS</th><th colspan="2">WHAT YOU SHOULD SEE</th><th>DO THIS</th></tr>
<tr>
<td> 

Using USB cable to connect (can also use serial)</td>
<td> 
</td>
<td>BLUE POWER LED LIT

GREEN LED LIT (once probe touches R707 to indicate a good circuit/connection)</td>
<td>PRESS DVDKey32 button to commence the read sequence</td>
</tr>
<tr>
<td> 

Using USB cable to connect (can also use serial)</td>
<td> 

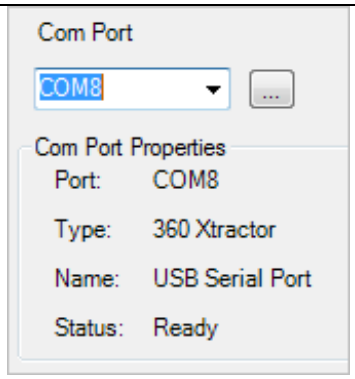
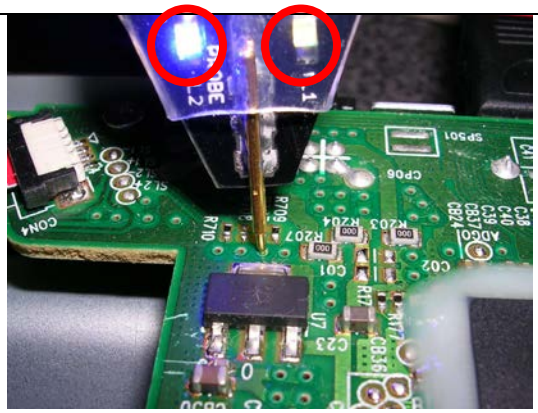
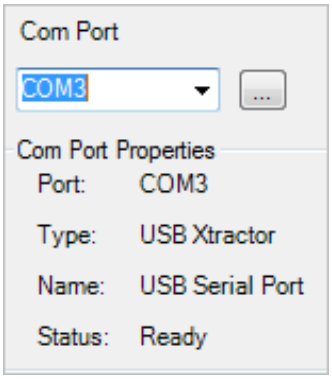
XECUTER PROBE 2 (in PROBE v1 MODE)</td>
<td>Mode switch to PROBE,

BLUE POWER LED LIT (power supplied to probe)

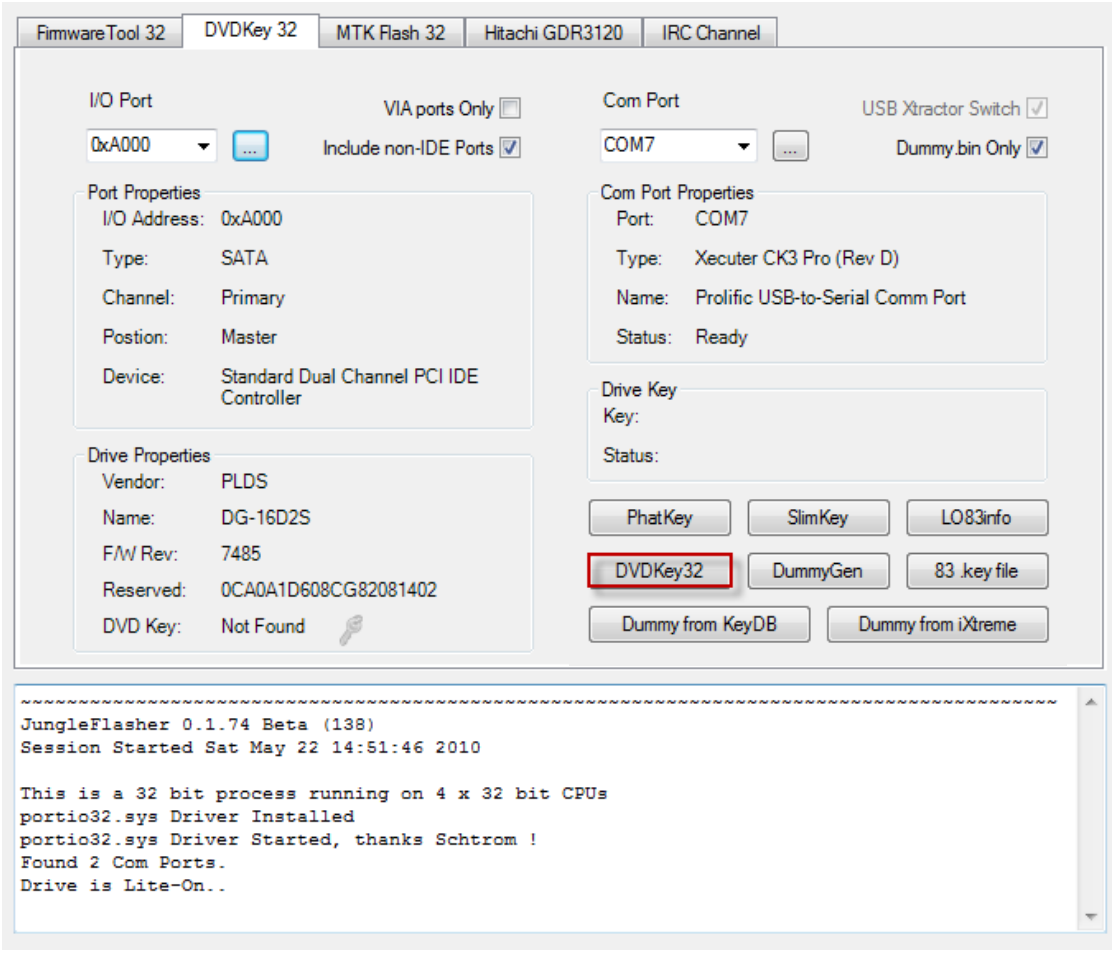
GREEN CONENCTION LED LIT - (indicates good connection to R707 circuit)

ORANGE STANDBY LED <u>EXTINGUISHED</u> (safety circuit disengaged)</td>
<td>PRESS DVDKey32 button to commence the read sequence</td>
</tr>
</table>

Things not going as expected? – Read the FAQ's

 Using USB Cable to connect (can also use serial)	 **MAXIMUS SPEAR**	**GREEN POWER LED LIT** **BLUE CONNECTION LED LIT** (when probing R707 to indicate good connection /circuit)	PRESS **DVDKey32** button to commence the read sequence
 USB ONLY	 **USBXtractor**	**BLUE LED SHOWING** when in contact with R707 and ready to read	USBXtractor Users can press the button on probe to start DVDKey32 extraction process (if ticked on DVDtab screen)

Things not going as expected? – Read the FAQ's



Providing serial connection was good, **DVDKey 32** will dump the key, then will test the key against the drive for 100% Verification that it is the correct key!

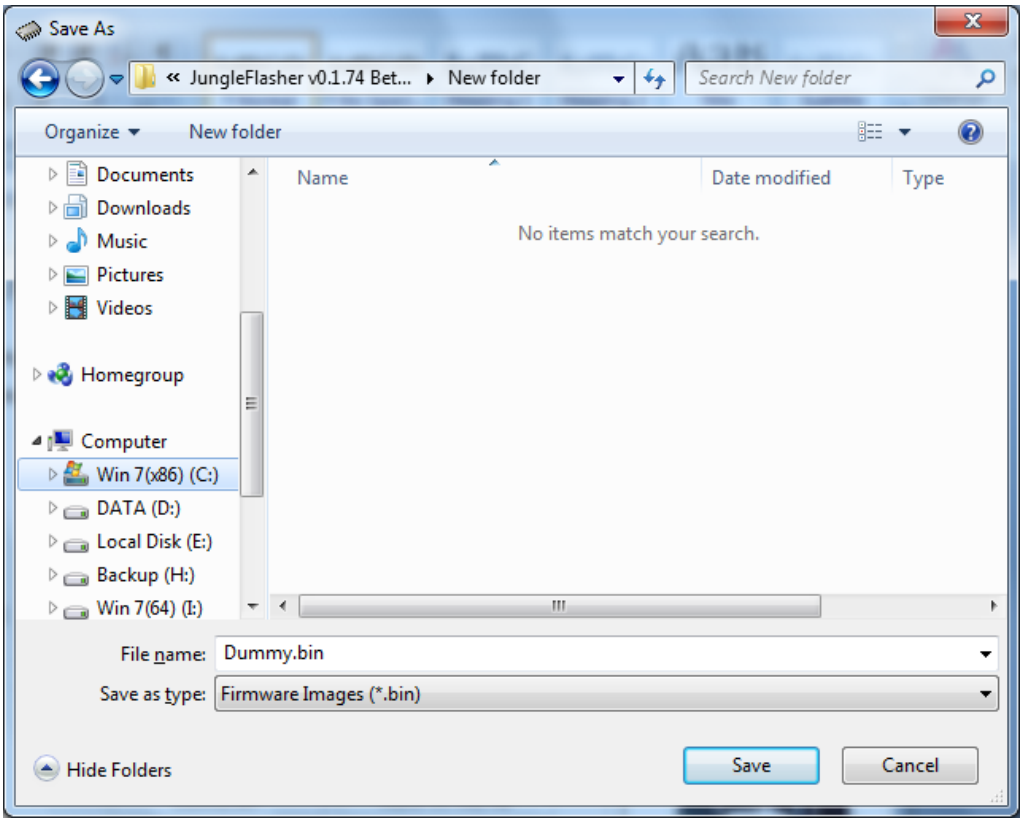
```
DVDkey delayed by 5 seconds
--------------------
Sending DVDKey request to I/O port 0xA000 and COM7

.................. Serial Data looks ok,  key returned: 9B749DEBF3935822C0950FB44B2D148B

Extracted drive key passed Verification !
```

Quickly followed by a lot of actual dumped information from drive,

then prompt you to save **key.bin, inquiry.bin, identify.bin, serial.bin (unless you have selected dummy.bin only box)** and **dummy.bin.**

Of course, should you have enabled the 'Dummy.bin Only' option you will only be prompted to save Dummy.bin.

Things not going as expected? – Read the FAQ's



There is now *No Requirement* to dump the key multiple times!

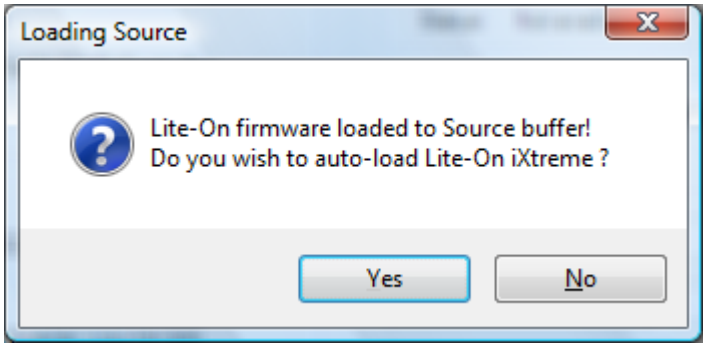
Nor is there a requirement to test it in a spare drive!

The key is dumped then Verified against the drive itself! Using c4eva's extremely clever verification routine, Jungleflasher tests the key against the drive (much like the xbox itself does!)

There is a 1 in 3.4025 x 10^38 chance of guessing the right key – so the fact it verifies means it's correct! ☺

Firmware Manipulation

JungleFlasher will then prompt you asking if you would like to auto-load iXtreme for Lite-On Drives. You must have installed the **JungleFlasher Firmware Pack** into the same directory as JungleFlasher.exe if you wish to benefit from this feature.

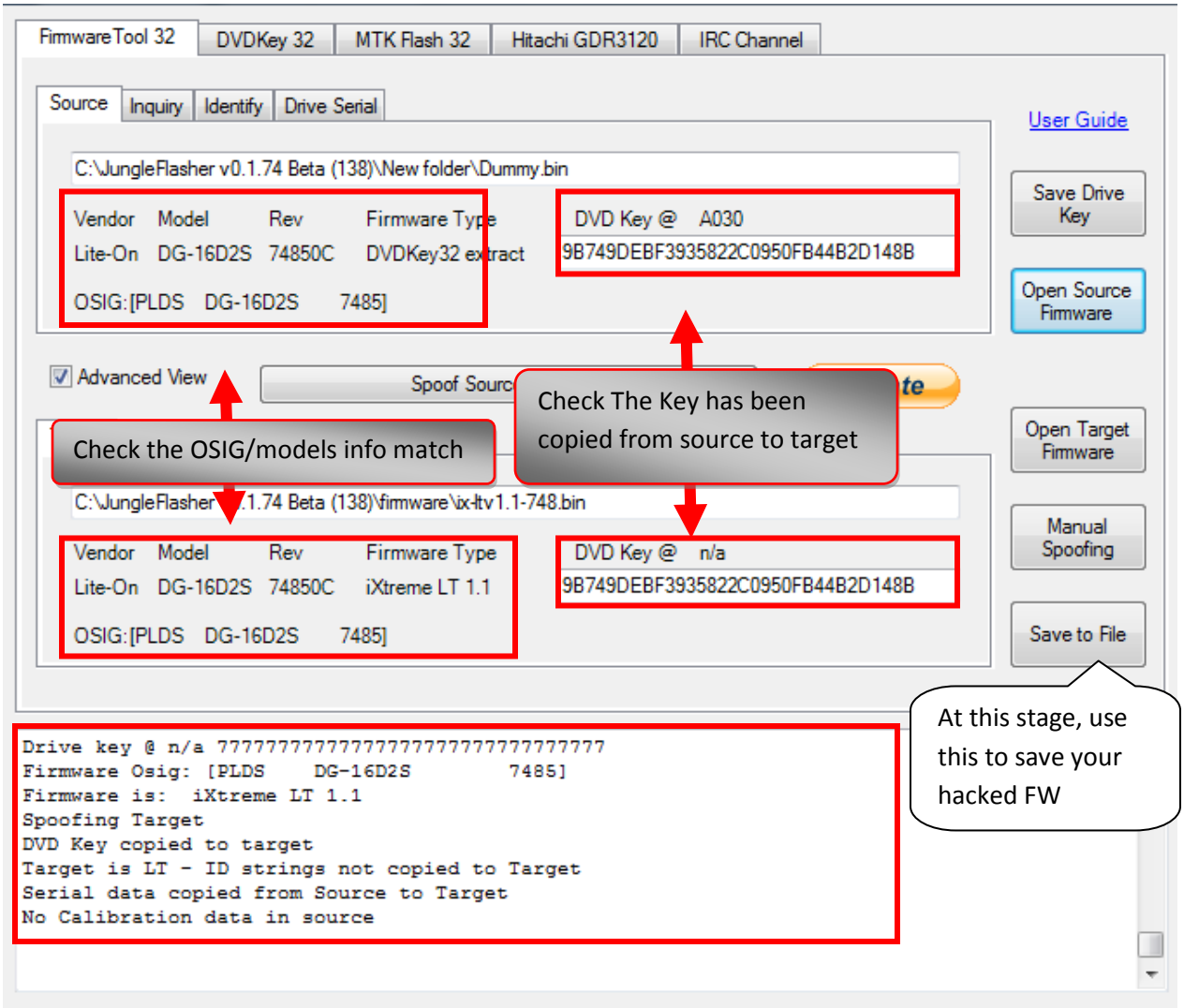


Click **Yes** to auto load iXtreme (from the firmware pack) for Lite-On into the **Target Buffer**, JungleFlasher will also load your previously dumped **Dummy.bin** as **Source Firmware.** Then, copy data from **source to target automatically.**

Just verify **Source data** reports as it should, **DVDKey 32 Extract with** OSIG **of PLDS DG-16D2S with the same key you dumped (check log for reference).**

Now, verify **unique Source Data** matches that in **Target Buffer** and click save to file if you wish to backup your Hacked firmware.

NOTE – IF (by some bizarre reason!) you load an ***83850C V2 dummy*** into source then Jungleflasher will assume it to be 83850C V1 (as dummy is only "Usually" acquired from 83850C V1 – as opposed to a full OFW dump from a 83850C V2) – IF this happens – select "NO" to the autoload question and manually load and spoof the correct 83850C V2 firmware!



(Please note the picture above is an example only! If you have a different firmware versioned drive then obviously you will have different numbers appearing – The important part is that Key and OSIG matches!)

Things not going as expected? – Read the FAQ's

The Next step is to ERASE the drive, its vitally important you only do this once you KNOW you are ready and have read the tutorial, in full, to understand the risks.

IMPORTANT!!!!!

Sending the erase command to the Lite-On using VIA Card with drivers installed poses the potential risk of the system locking up due to the VIA chipset polling the erased Lite-On and not liking the response!!!!!!!

Please CLICK HERE and follow instructions to remove Card Drivers if you have not done so already.

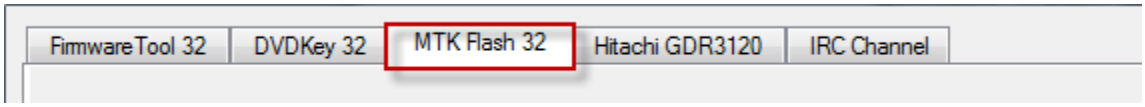
NOTE- You CANNOT SPOOF a LiteOn Drive with LT Firmware as a DIFFERENT DRIVE

Erasing a Lite-On PLDS DG-16D2S.

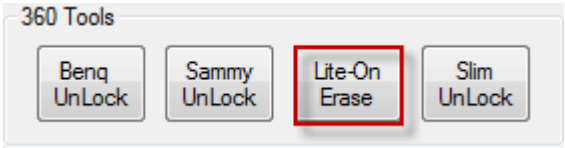
PLEASE READ THE WARNINGS ABOVE.

Once you erase the drive, there is NO GOING BACK.

Click the **MTKFlash 32** Tab.

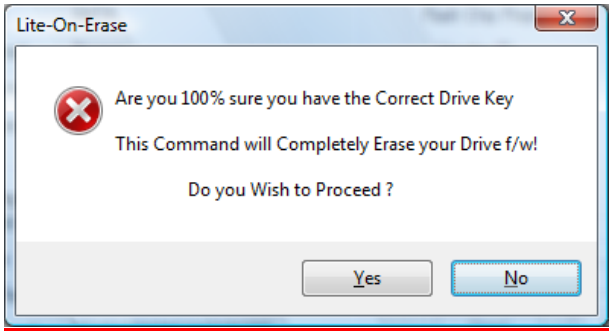


Verify I/O Port is correct(for your setup!) and click **Lite-On Erase.**



JungleFlasher will warn of the importance of having a verified **Good Drive Key.**

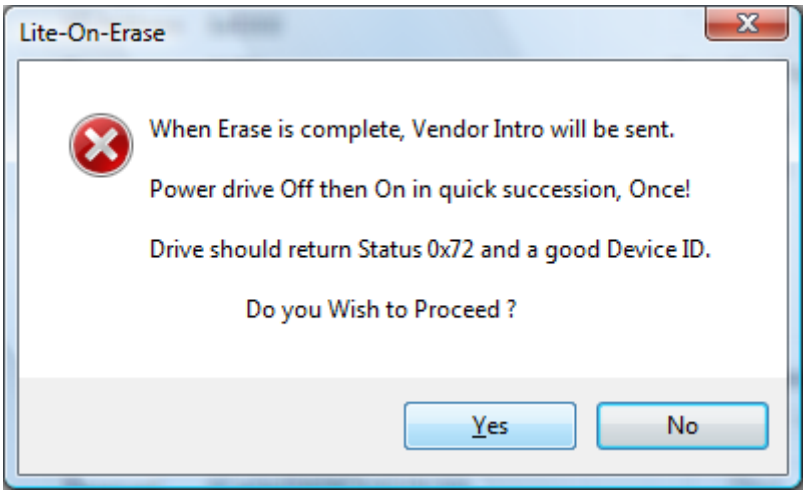
Please Note, the only ways to know 100% that a key is good, is to ensure your drive key was Verified by JungleFlasher or flash your firmware to a identical drive first and test it in the xbox itself



Click **Yes** if you wish to Proceed.

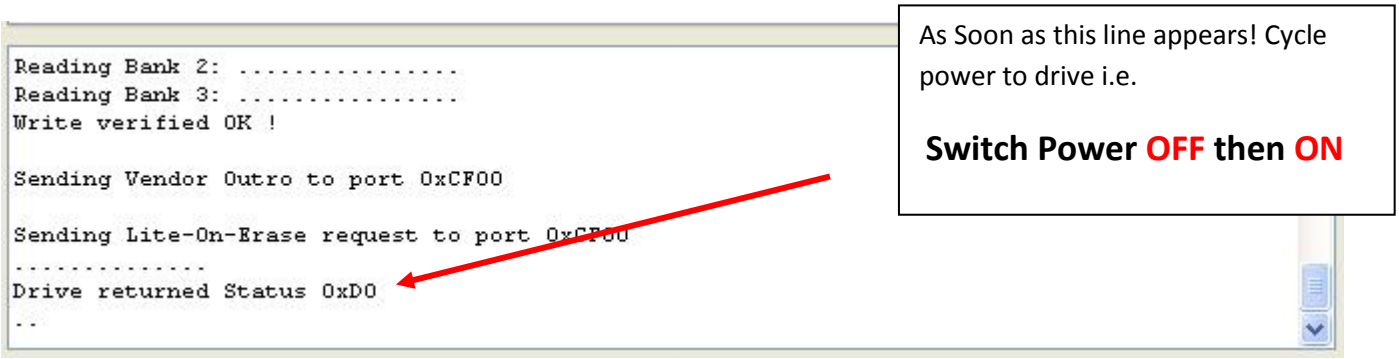
JungleFlasher will present you with another warning.

Things not going as expected? – Read the FAQ's



Read this carefully, in most cases JungleFlasher wil return a Running Log similar to this: We have had 0xD0 / 0x80 / 0xF2 / 0xD1 and all worked fine.

After pressing yes and during the sequence of dots shown below, switch drive Power Off then On - ONCE.

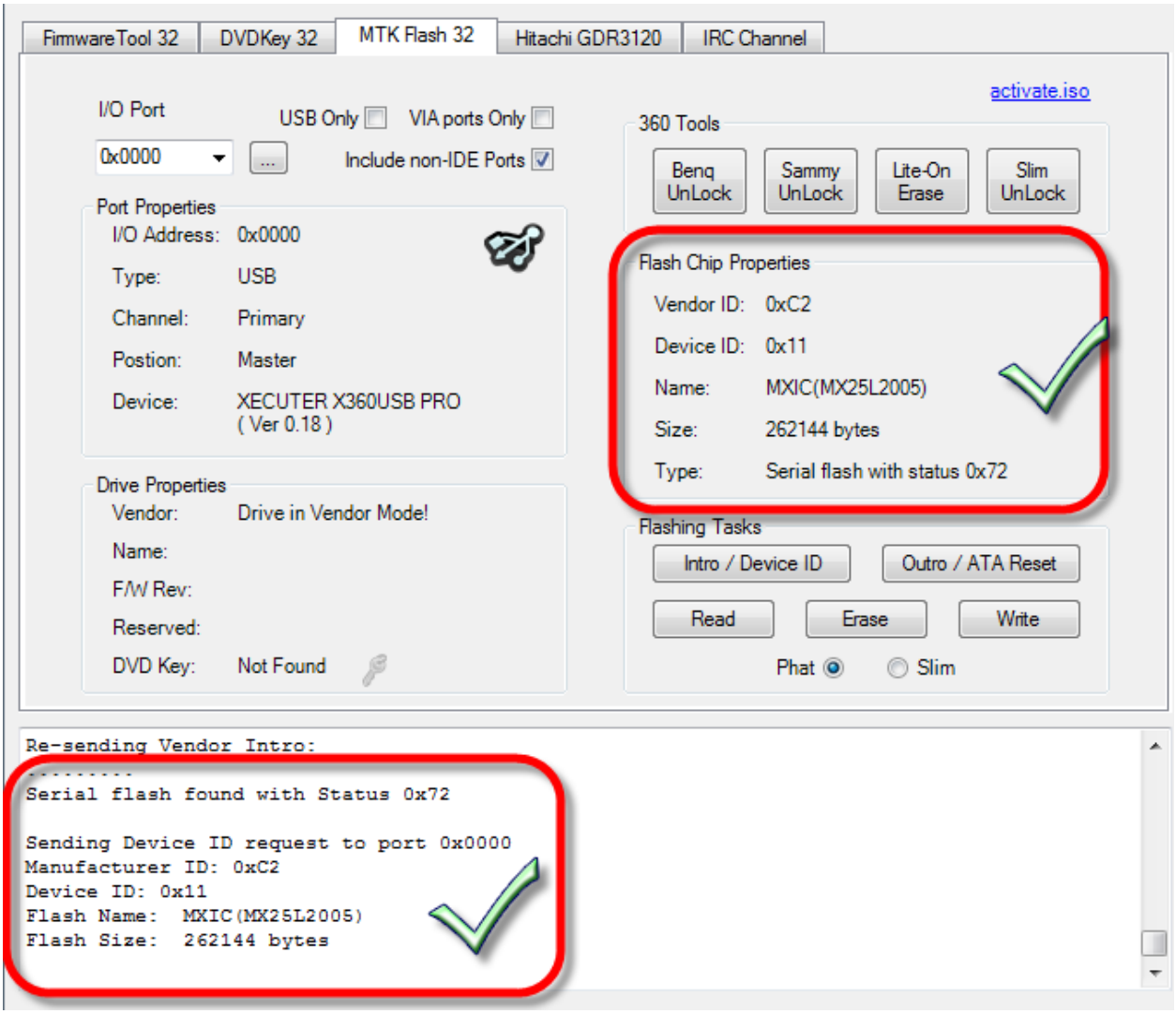


Hopefully you will see good **Flash Chip Properties** and **Status 0x72** (2 known SPi Chips for Lite-On's, Winbond **and** MXIC) MXIC Shown, drive will appear in **Vendor Mode** under **Drive Properties.**

DON'T PANIC IF IT DOESN'T ENTER VENDOR MODE FIRST TIME OR IF YOUR DRIVE IS NOW NOT SHOWING UP AND WILL NO LONGER EJECT

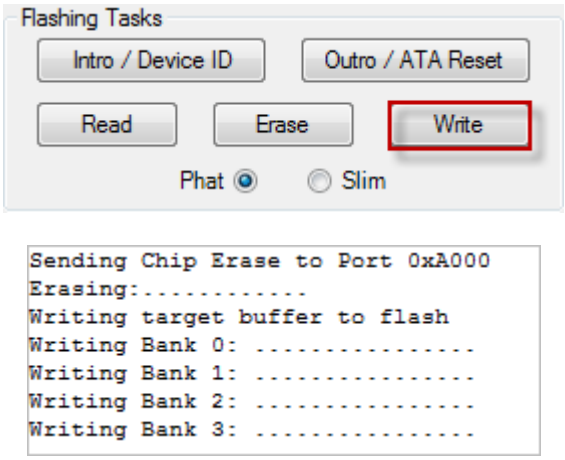
– SIMPLY PRESS INTRO AND CYCLE DRIVE POWER – IF STILL NOT IN VENDOR MODE, TRY ERASING AGAIN!

Things not going as expected? – Read the FAQ's



Drive is now in Vendor Mode (0x72).

Click the **Write** button to write **Target Buffer** to the drive.



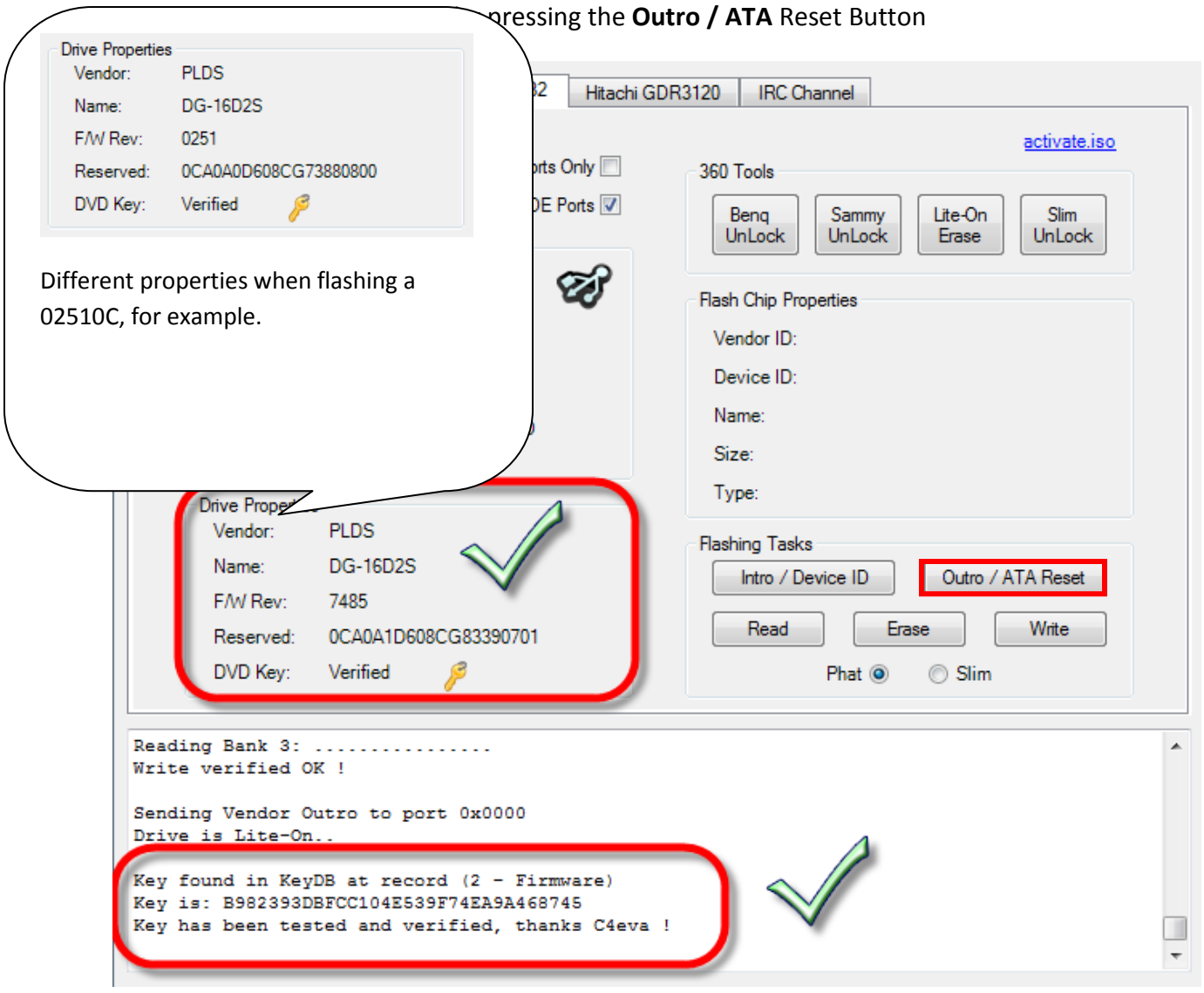
Things not going as expected? – Read the [FAQ's]

```
Flash Verification Test !
Reading Bank 0: ..................
Reading Bank 1: ..................
Reading Bank 2: ..................
Reading Bank 3: ..................
Write verified OK !
```

Write Verified OK! in **Running Log** signals good write.

Now send an Outro to the drive.

pressing the **Outro / ATA** Reset Button



This will release a drive from **Vendor Mode** and send **ATA Reset** to the Drive. It then sends an inquiry command to the drive.

Things not going as expected? – Read the FAQ's

This will save you power cycling the drive and then changing port away and change it back again, with the click of a button, the drive will 'reset' itself and JungleFlasher will send an inquiry command to the drive. If successfully flashed the drive should Inquire correctly and display drive properties.

Power Off – Disconnect SATA from PC, connect SATA back to console and test!

ADDITIONAL INFO – IF YOU HAVE BEEN FOLLOWING MRA HACK PROCEDURE TO DUMP ORIGINAL LITEON FIRMWARE - REMEMBER YOU MUST REMOVE YOUR ADDED WIRING AND RECONNECT ANY CUT TRACES! BEFORE TESTING

COMPLETE – CLICK HERE TO RETURN TO START OF TUTORIAL

LiteOn "83850c v1" Extraction

How to obtain the unique data from your PLDS DG-16D2S **83850c v1** drive and create a Dummy.bin.

The 83850C v1 Firmware drives DO NOT require the additional Hardware that the 74850C Firmware drives do –

83850C v1 drive's information is extracted through SATA!

Obtaining Dummy.bin

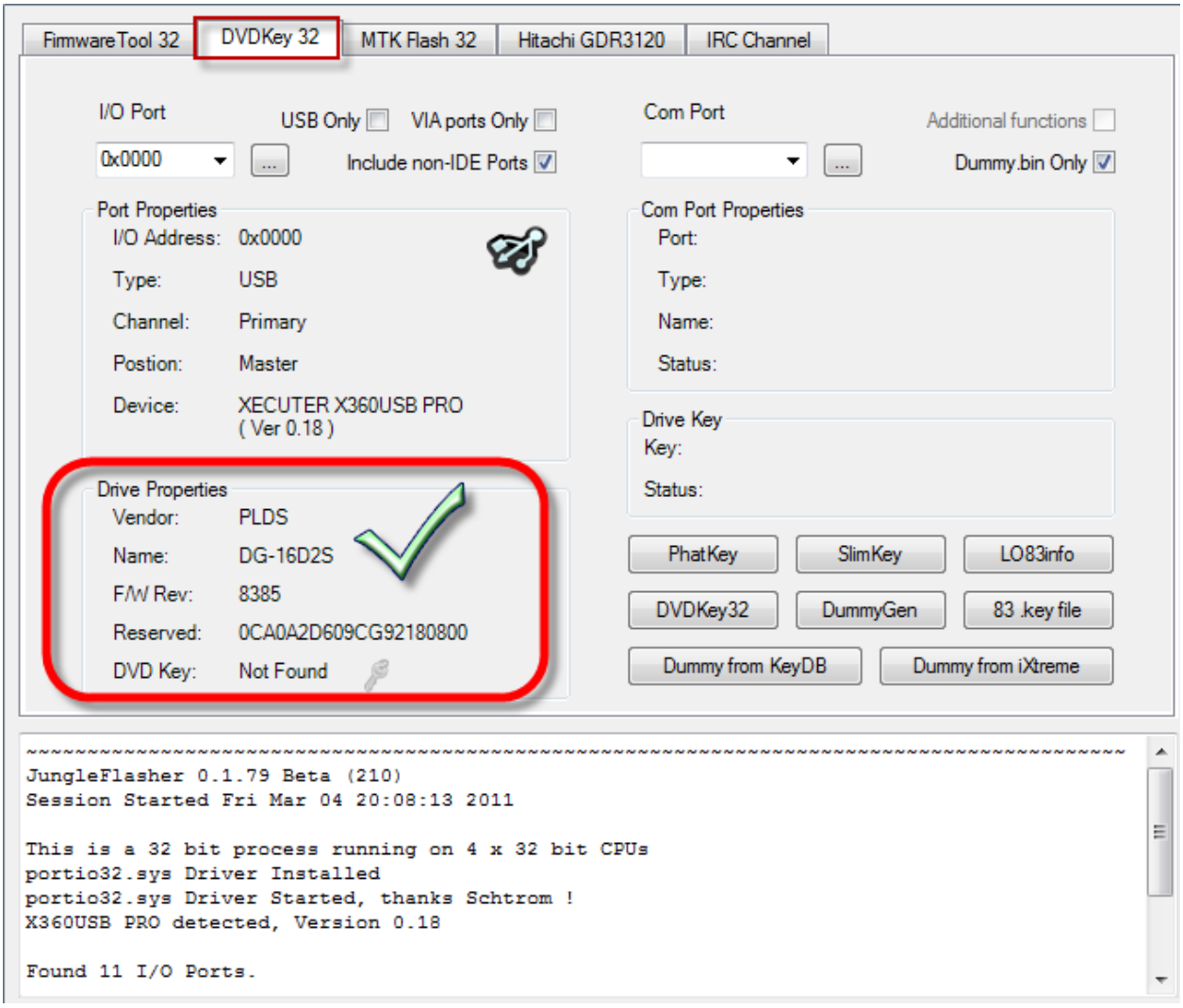
Please Note: Dummy.bin is **not** Original firmware, it is [FAKE] firmware based on the structure of an Original firmware file, and this makes everything easier to work with.

Connect your 83850c to your PC via S-ATA

Power on and run JungleFlasher v0.1.69b or above

(example only)

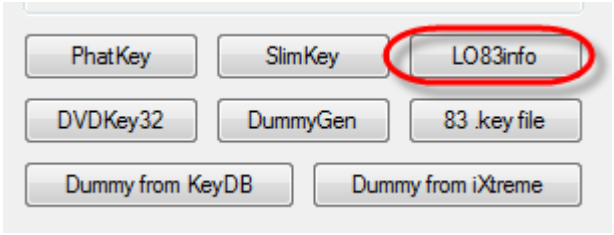
Select **DVDKey32 Tab**



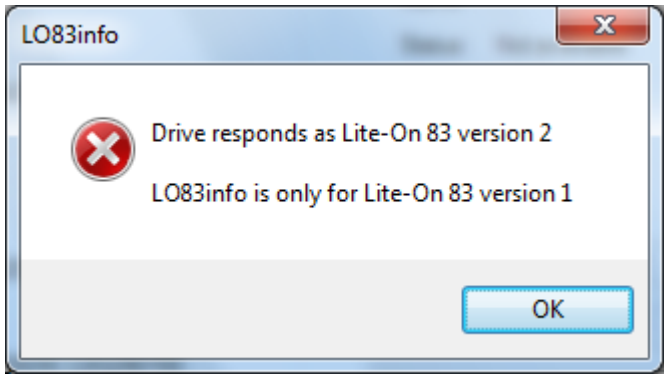
Check to see the 83850c Inquires on the port.

Things not going as expected? – Read the FAQ's

Select **LO83info**



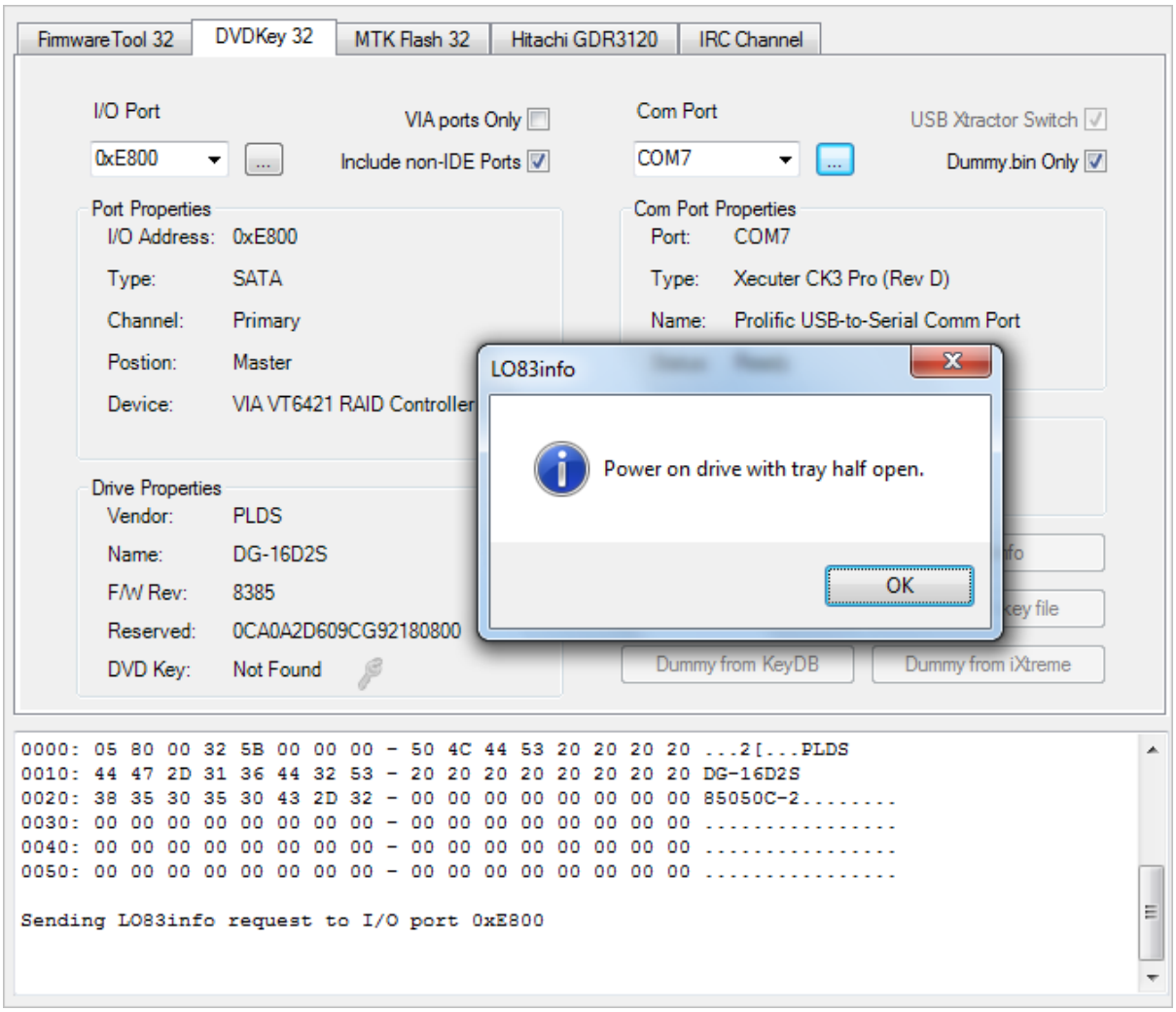
If you see this message:



You have a **83850C v2** so **CLICK HERE TO PROCEED**

IF NOT then you have the **83850C v1** and should the image shown below!

Things not going as expected? – Read the FAQ's

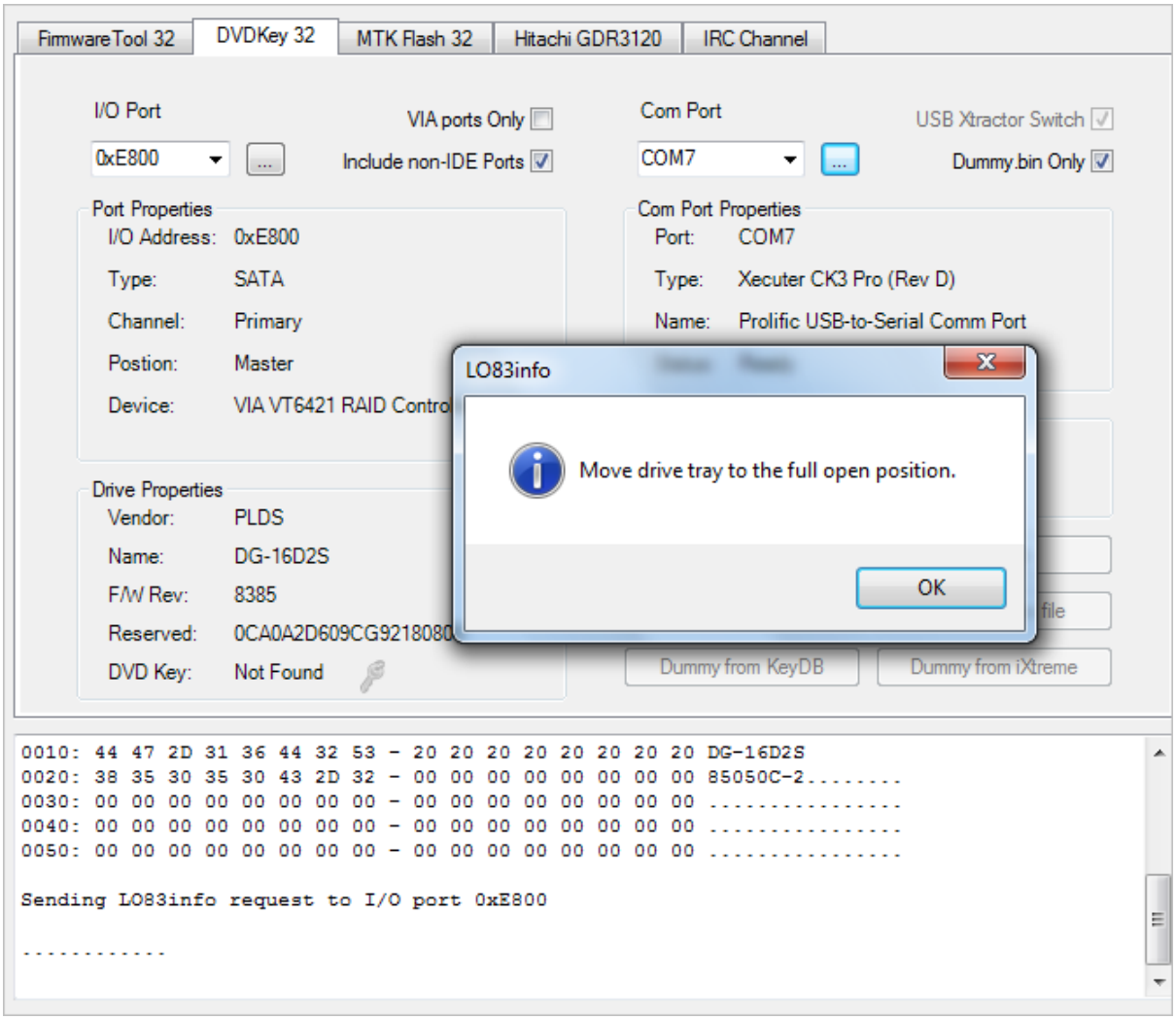


Here you must set the tray to '**Half Open (but half closed status)**',

FOR INSTRUCTIONS ON HALF OPEN TRAY – CLICK HERE

Please ensure you have the drive **fresh / power cycled after setting Half Open Tray, this is essential.** Then, click **OK**

JungleFlasher will then send the LO83info command to the drive; you will see the following in the **Running Log**



DO NOT POWER CYCLE THE DRIVE AT THIS STAGE; DOING SO WILL RESULT IN A BAD/FAILED DUMP!!!!

Eject the drive (so it is fully open) OR manually move the tray fully open by hand!

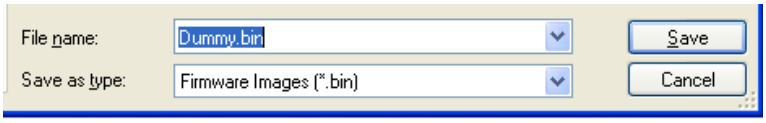
Once tray is fully ejected, click **OK**

If the dump appears to JungleFlasher that it was valid, JungleFlasher will prompt you to save, but look for this in the log: (with Your key!)

```
Extracted drive key 9B749DEBF3935822C0950FB44B2D148B
Extracted drive key Passed Verification !
```


Things not going as expected? – Read the FAQ's

Jungleflasher will now prompt you to save!

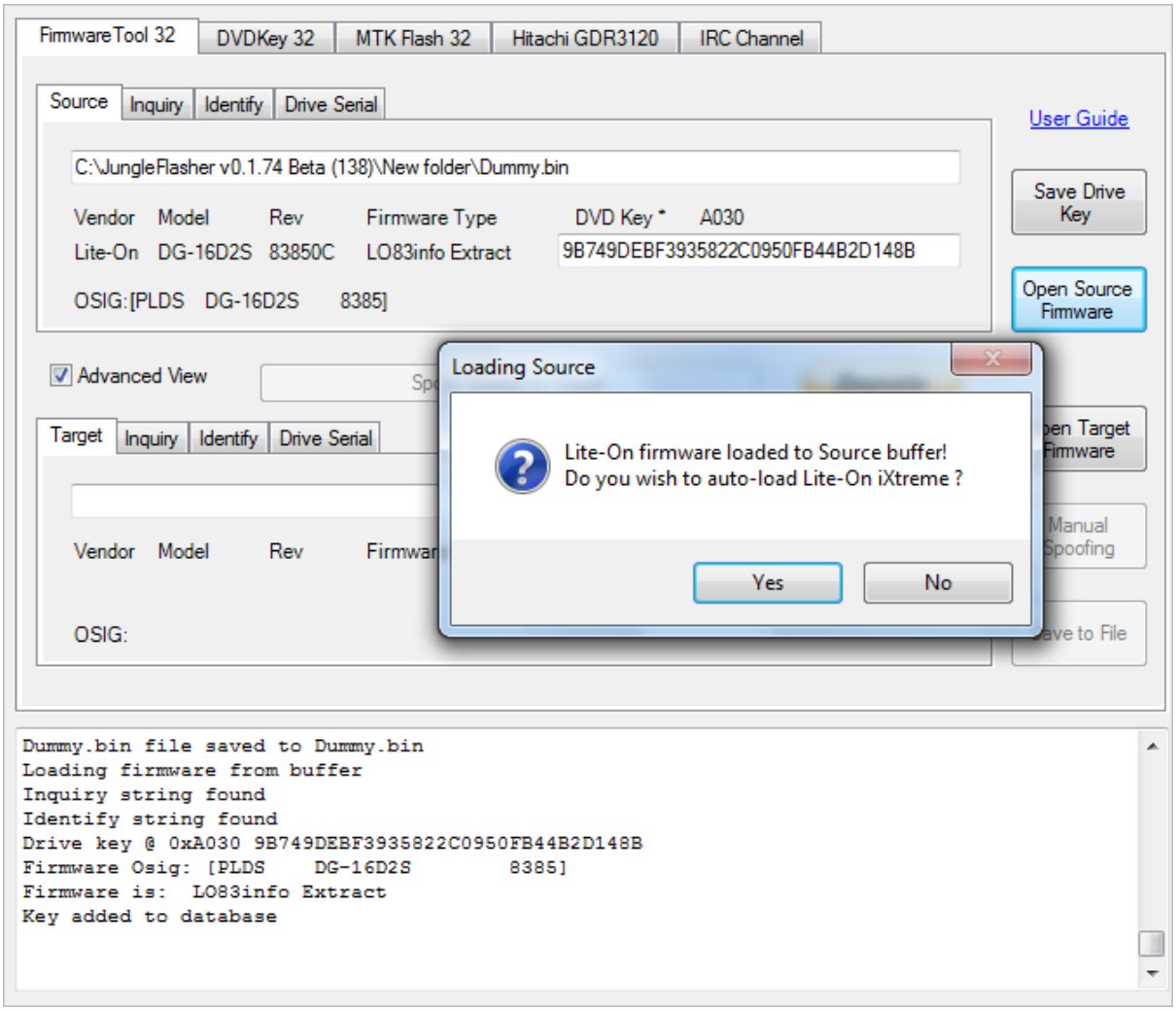


Save this file.

Note: I only save dummy.bin as I have dummy.bin only enabled in the DVDKey32 Tab, JungleFlasher *may* prompt you to save Inquiry.bin, Identify.bin, Serial.bin and Key.bin also, if this isnt enabled.

Once saved, JungleFlasher will load Dummy.bin as Source Firmware in FirmwareTool32 and prompt you to auto load iXtreme (from the firmware pack)

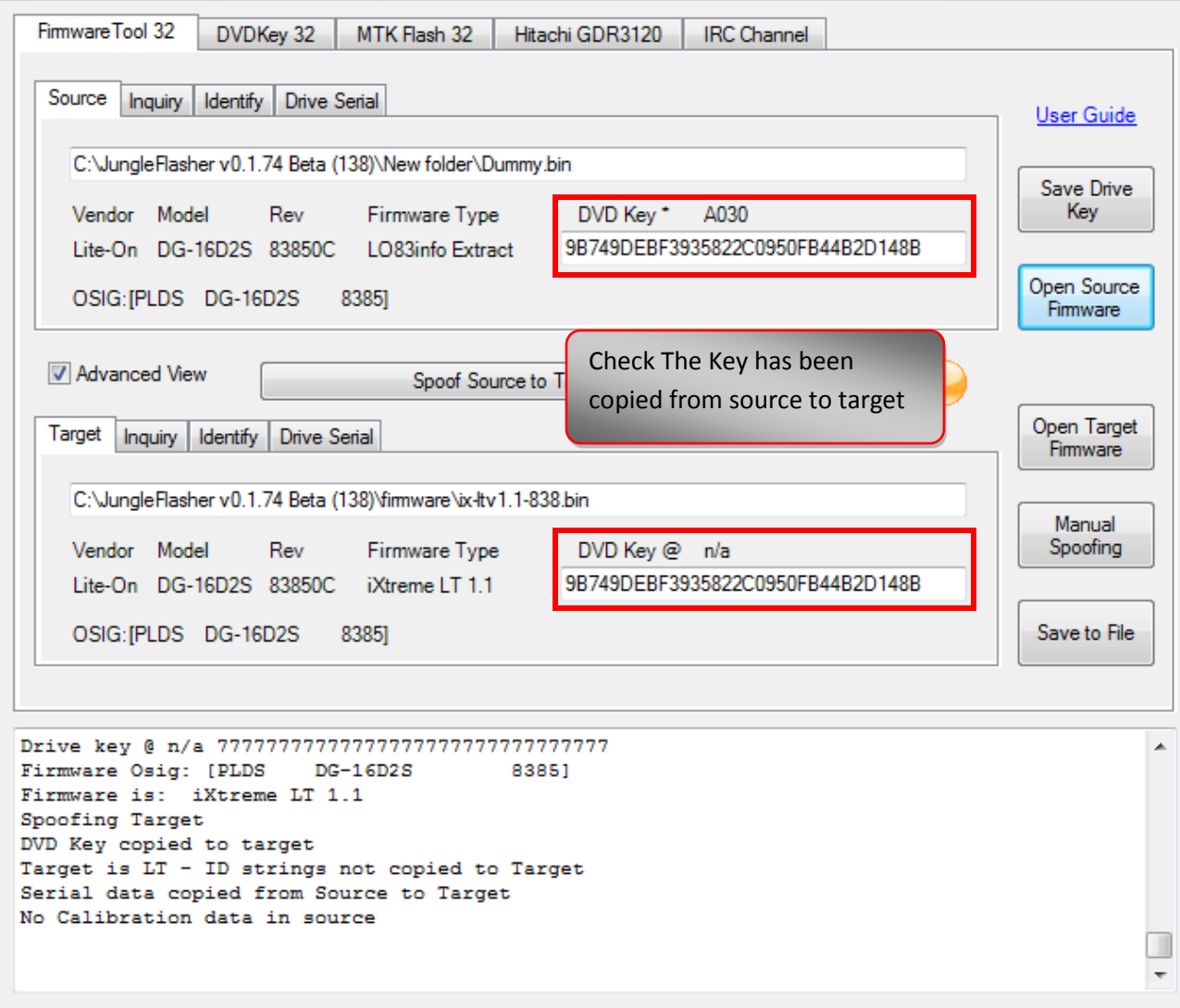
[(IF YOU INTEND TO UPDATE YOUR DASHBOARD TO 13146 STOP HERE AND UPDATE YOUR DASH THEN RETURN TO START OF TUTORIAL)]



Things not going as expected? – Read the [FAQ's]

If you have selected **YES,** target firmware will be loaded and automatically spoofed

Check the keys match and the OSIG/model info is the same!



Then if you wish you can click **Save to File** button to save a copy of your hacked Firmware.

CLICK HERE TO CONTINUE TO ERASE/WRITE SECTION

Things not going as expected? – Read the FAQ's

Dumping OFW from LiteOn for 83850C v2 & 93450C

(& All LiteOn flashed with iXtreme LT firmware unless you previously dumped this drive and have the details in the Key database)

When this hack was first released there was several differing methods appeared varying mainly in where to connect certain wires and which traces to cut. After testing several of them we have listed the popular methods, the **original MRA Hack**, **The Xecuter Probe II,** The **Xecuter LT Switch, Vampire & Rebuild Board, and Vampire w/o Rebuild Board**

NOTE: With the release of Jungleflasher 1.70 a section of data is now copied over starting from hex address 3C000 this data has been talked about as "calibration data" At the time of writing this, it's thought to contain data from manufacture tests but is not used! However for completeness is now copied over to your iXtreme firmware. This is shown in the running log at time of spoofing the firmware like:

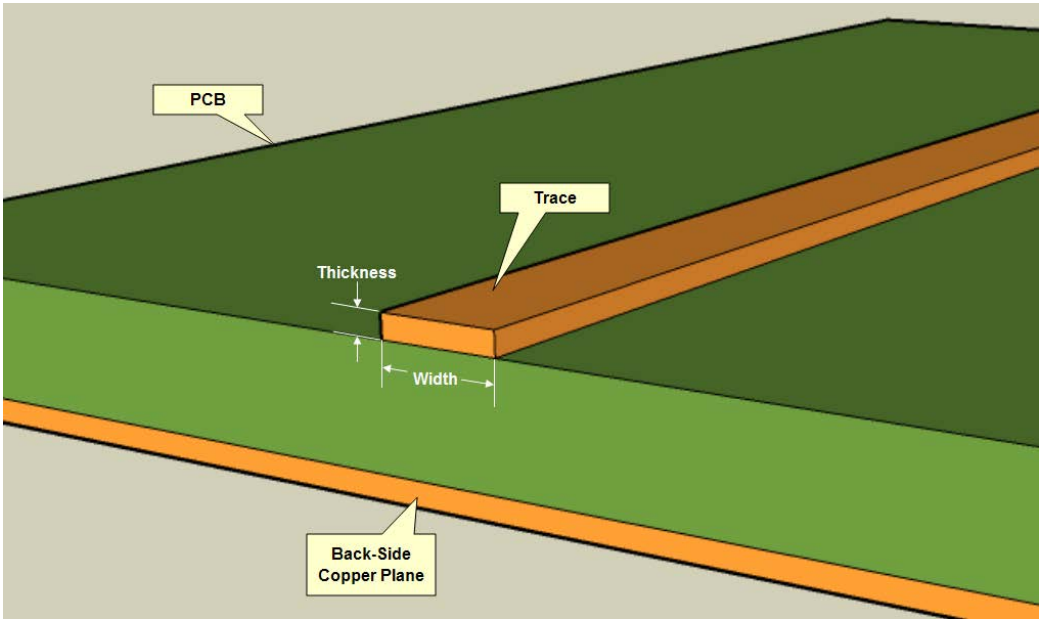
```
Spoofing Target
DVD Key copied to target
Inquiry string copied to Target
Identify string copied to Target
Serial data copied from Source to Target
Calibration data copied from Source to Target
```

A full dump of your **VIRGIN drive** (not one that has been returned with other stock firmware) is the **ONLY WAY** to get the **ORIGINAL DATA** from your drive into the iXtreme LT firmware. So IF your drive has been flashed before please IGNORE the statement that appears `No Calibration data in source` as it is NOT important and there is NOTHING you can do – it has been lost forever!

All the methods involve cutting traces on the PCB! Please read on for some handy information regarding this topic!

For your information:

Trace cuts!



Cutting traces on the PCB: The traces that requires cutting on the PCB are only a thin strip of copper laid on top of the PCB! They do NOT need carving up with a chainsaw! A reasonable pressure with a sharp craft knife is sufficient to cut through them. Easily less than .5mm thick!

Moral of the story: You don't have to cut right through half the PCB to cut the trace!

Click on the link for the method of your choice!

The MRA Hack

Xecuter Probe II , Xecuter LT Switch

Vampire With Board , Vampire w/o Board

Please Note: The following methods have been superseded by PMT Probe, As such the Jungleflasher Version shown in the pictures are OLDER and the layout differs slightly to current version – The methods still work – just the buttons may have moved slightly from shown.

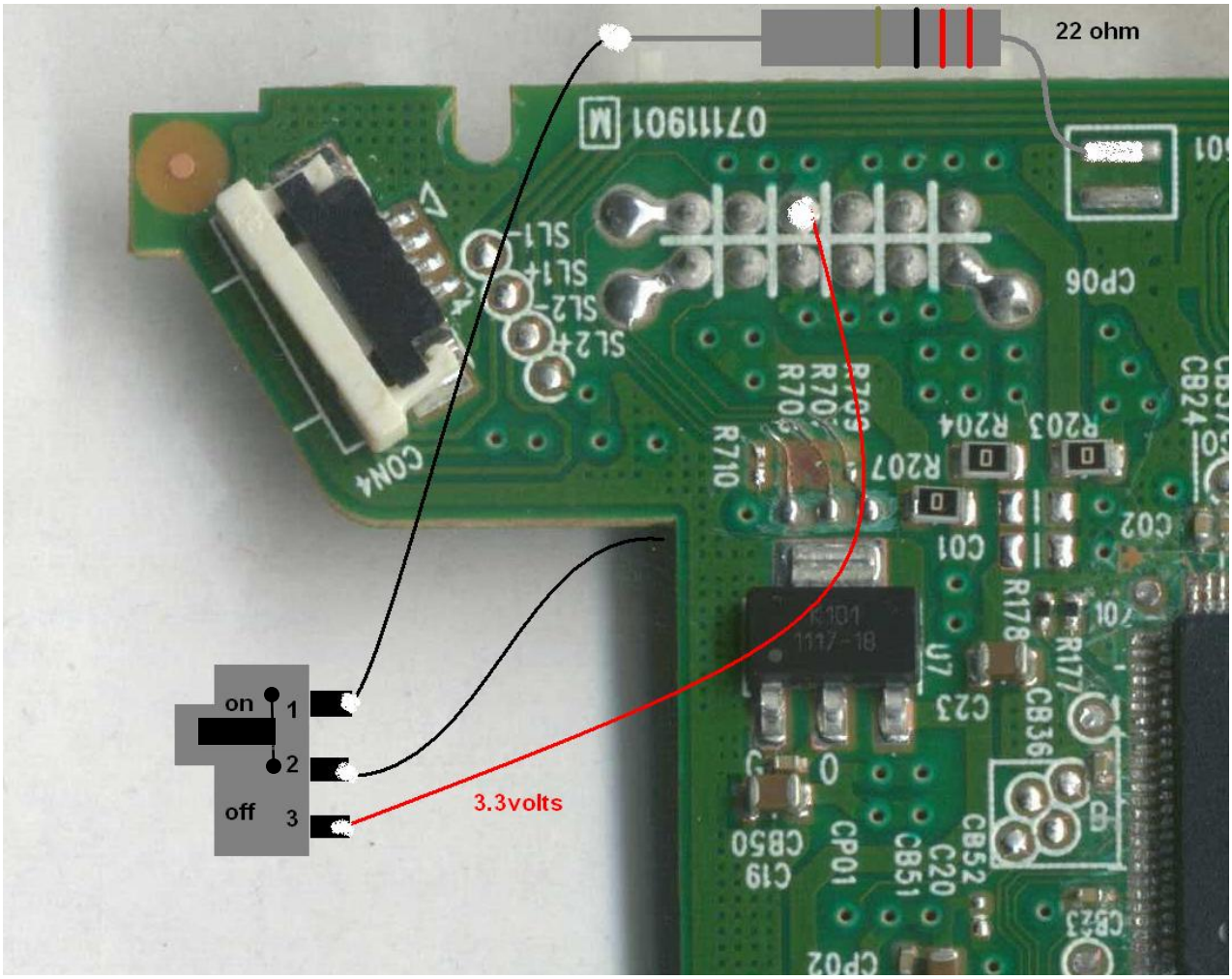
The MRA Hack

Can be used on ALL current LiteOn Drives

Soldering/Electronics skills are required for these modifications – It Should NOT be attempted by people without such skills!

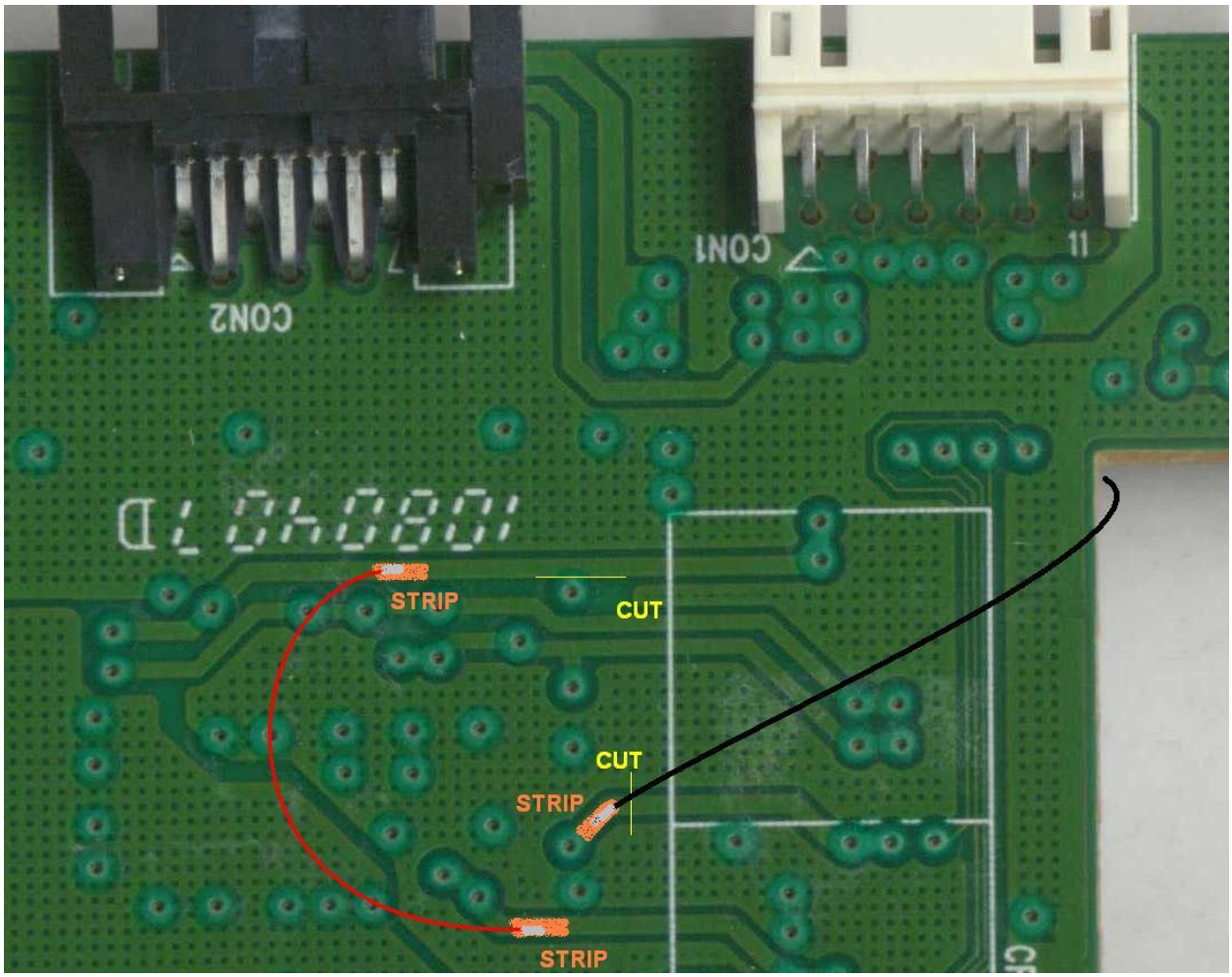
Basic wiring guide for the drives PCB

A 18 - 22 Ω resistor is required and a switch such as dpdt (double pole, double throw) -using one side only



Pic 1

Things not going as expected? – Read the FAQ's



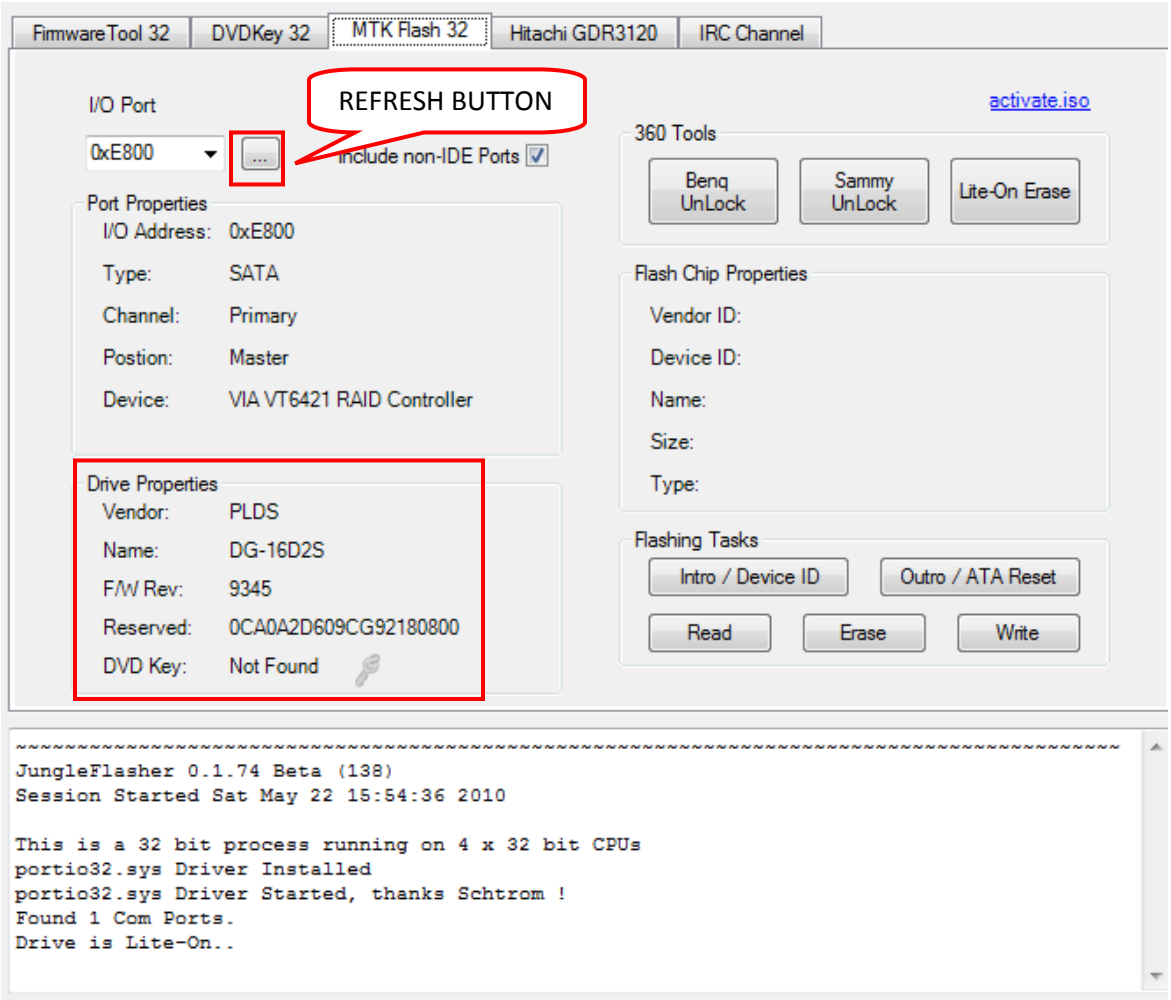
Pic 2

The 2 trace locations in yellow must be cut!

With Jungleflasher running, have the switch so it connects 3.3v line to the middle cable showing in picture 1 (switch selected OFF).

Connect drive to PC's SATA and power drive, select **MTK Flash 32** tab

Refresh, drive properties – so drive shows up



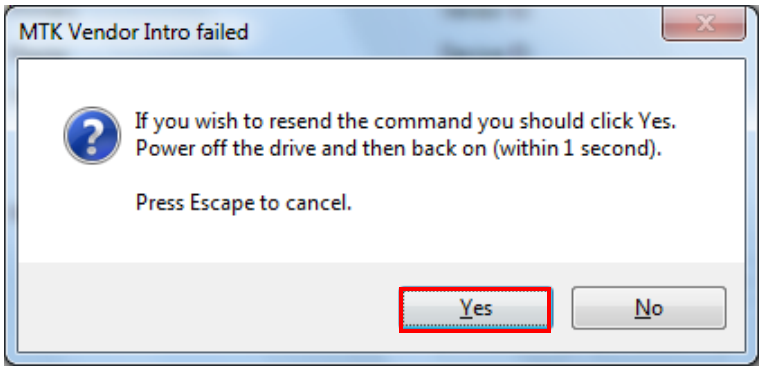
Turn power off to the drive

Operate switch you added! To connect to the 22 Ω resistor side (On)

Press **intro/ Device ID button**

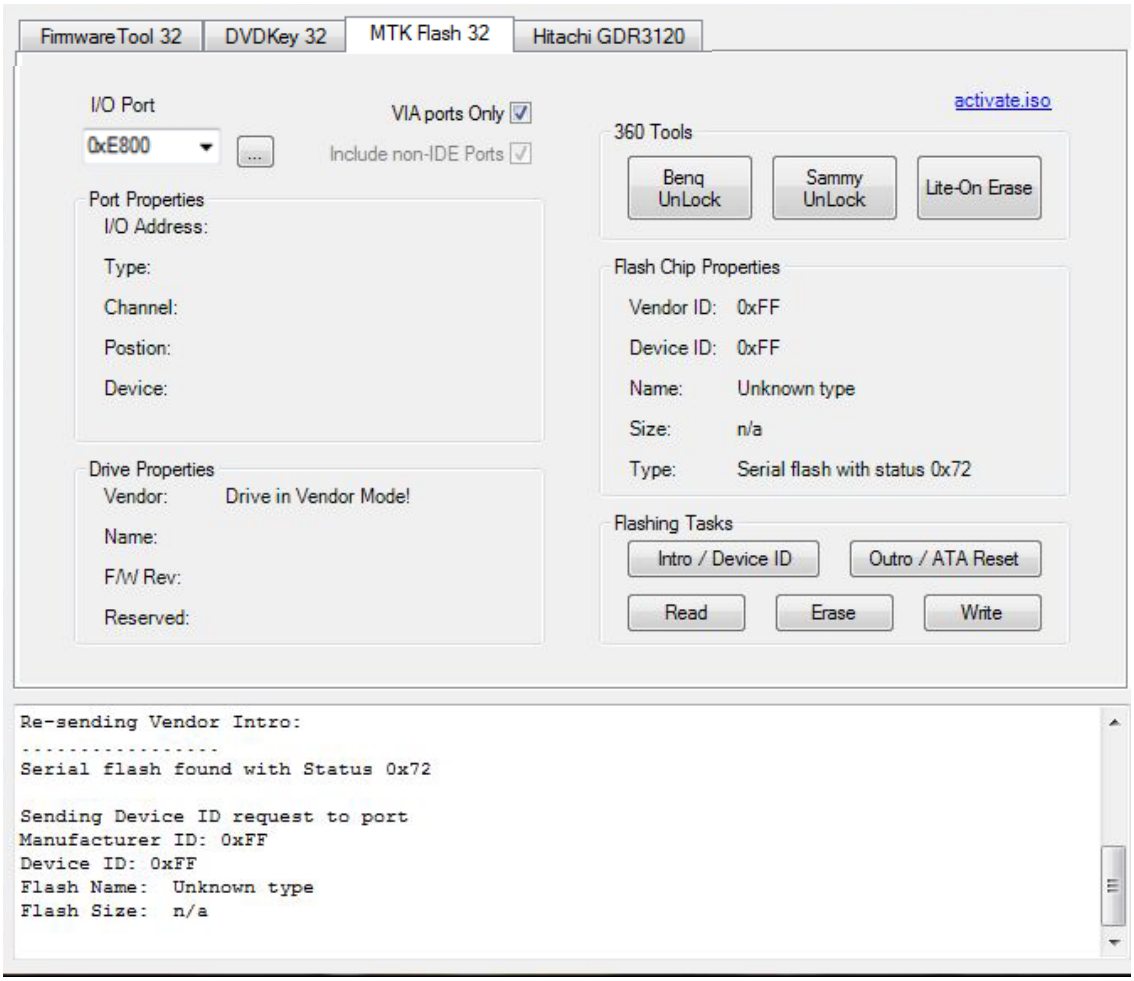
The following will appear! Press **Yes** button

Things not going as expected? – Read the FAQ's



Then power on the drive!

IF this produces a screen showing **BAD FLASH PROPERTIES** (shown below)

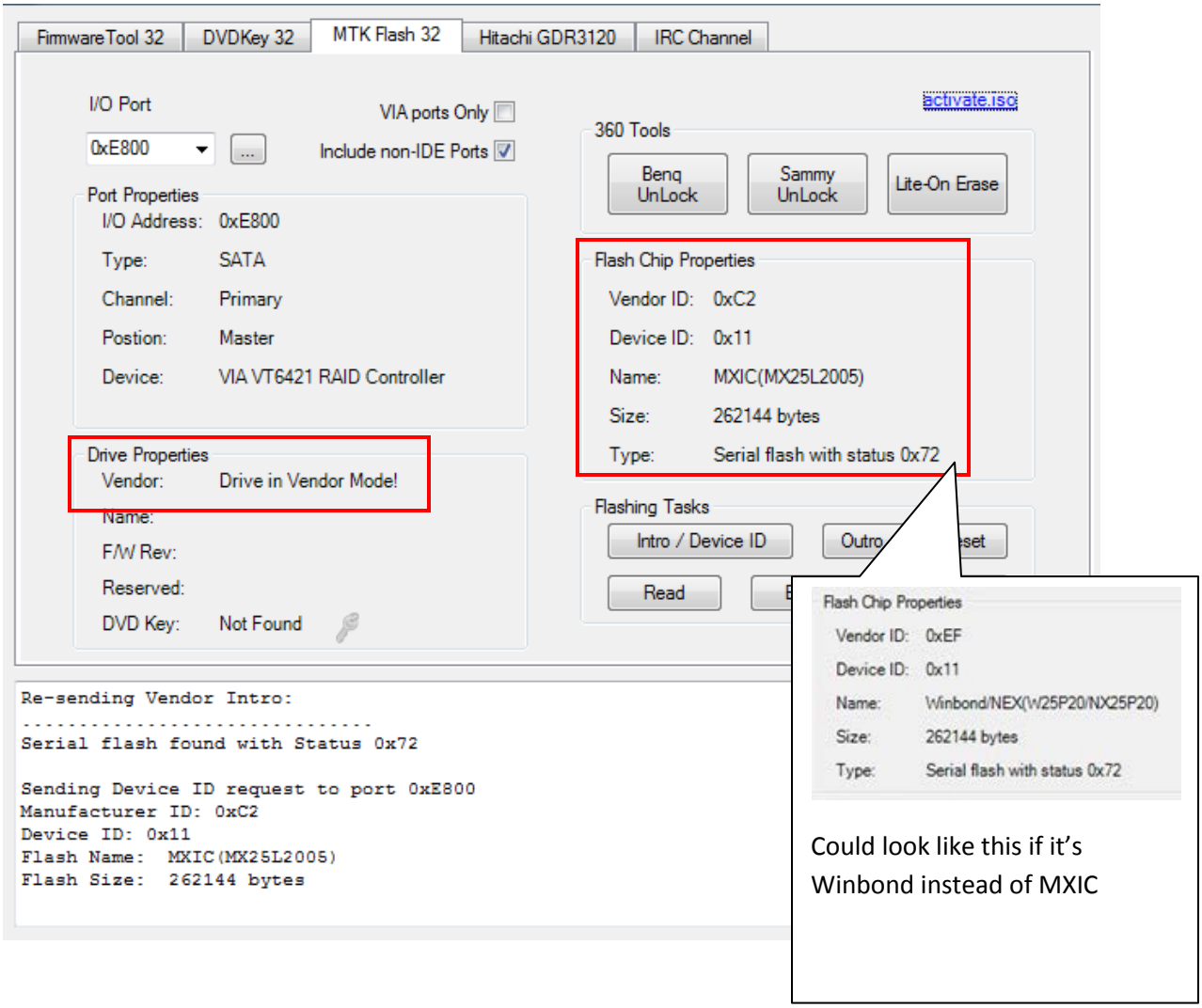


then press **Intro/Device ID** button again –

Things not going as expected? – Read the FAQ's

DO NOT POWER CYCLE!

If everything has been done correctly – you should be faced with this!



After you get these good flash properties, quickly operate the added switch again to 3v3 side (Off in pic 1)

Now press the **Read** button

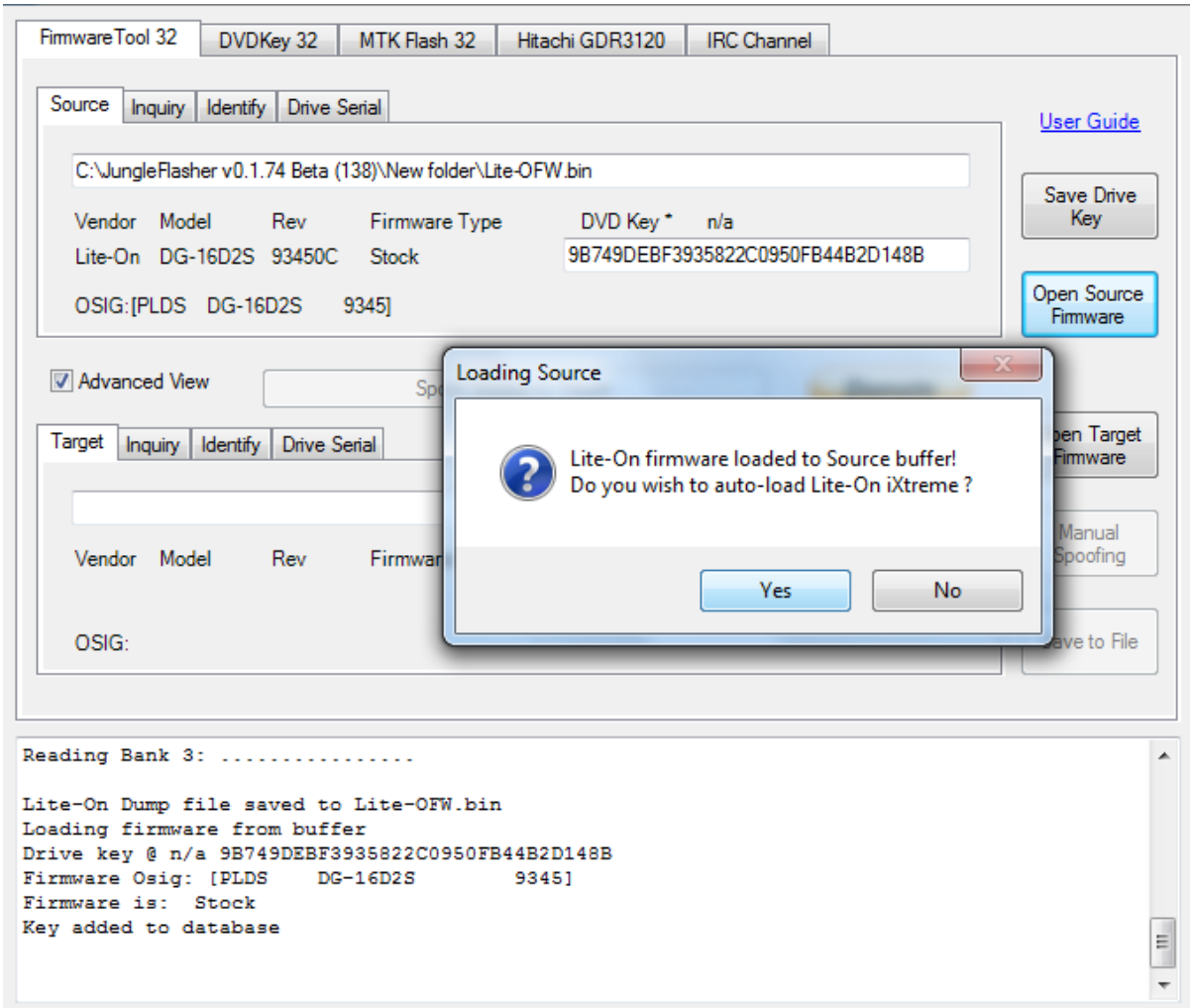
Things not going as expected? – Read the FAQ's

Jungleflasher will now dump your Original LiteOn Firmware,

When prompted to SAVE **– it is advised you do so!**

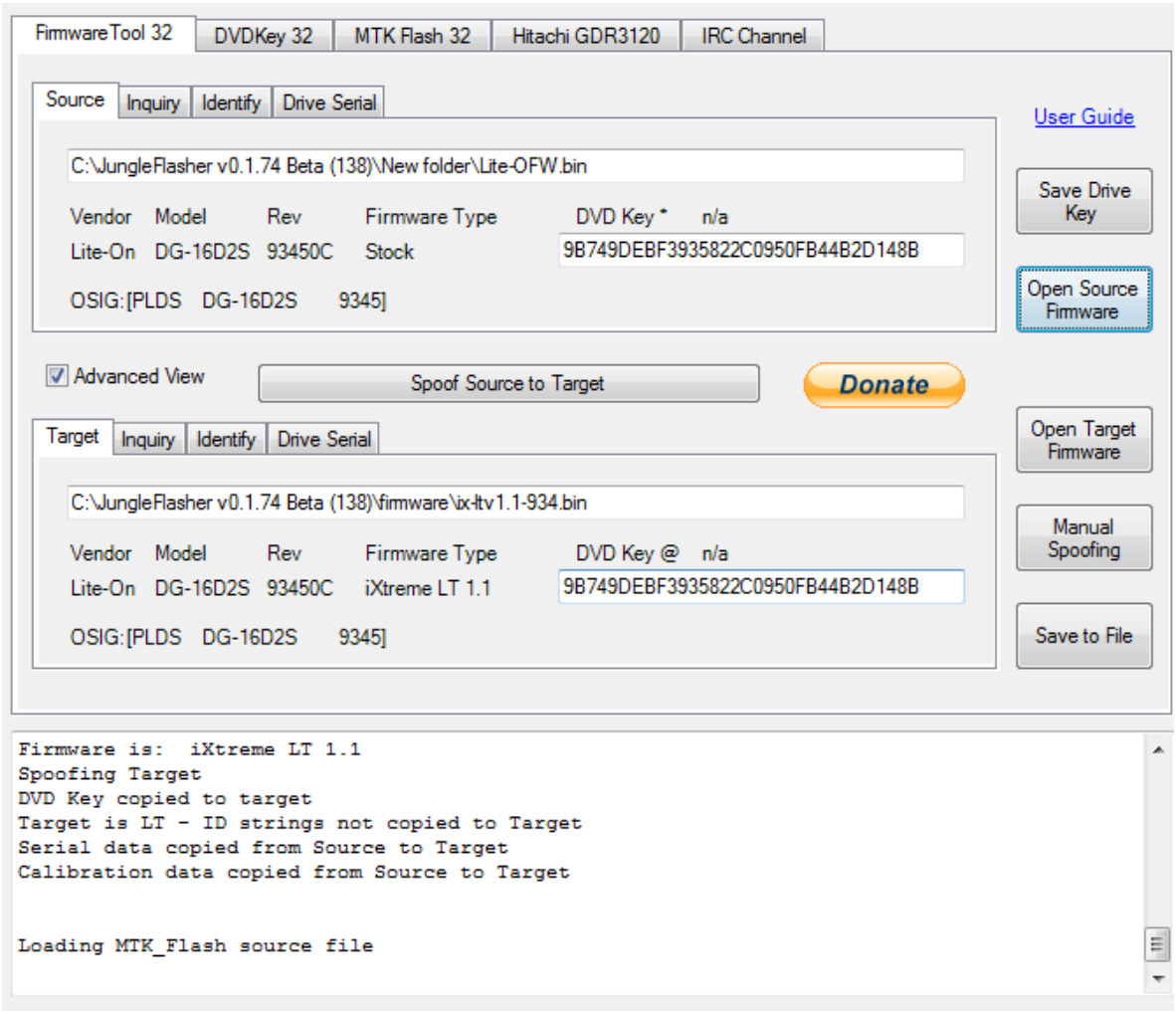
IF you get "parse failed" read THIS

The dumped firmware will now automatically be loaded into source in **firmwaretool 32** tab.



Things not going as expected? – Read the FAQ's

Select **Yes**



Now, Just follow the standard write procedure!

So return to **MTK** tab

NOW CLICK HERE!

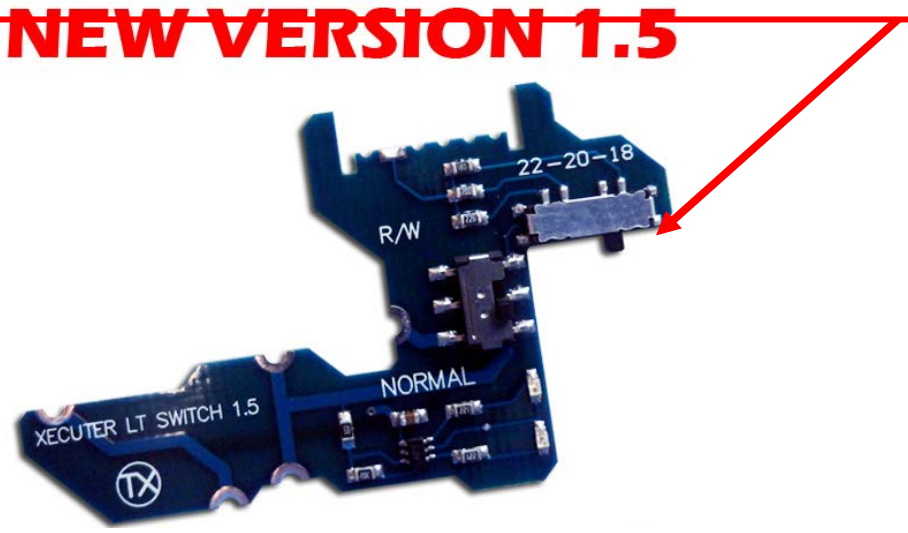
Things not going as expected? – Read the FAQ's

Dumping Firmware from a drive with a Xecuter LT Switch Fitted

For full fitting instructions go here

Essentially the board preparation is the similar to the MRA hack but once fitted need not be removed and has a switch on it to select between 'normal' operation and R/W (presumably meaning read/write) though technically all reading and writing is done with switch in 'normal' position, the R/W position is ONLY used to place the drive into vendor mode!, then switched back to normal for reading and writing operations.

NOTE: v1.5 has now been released! Added MULTI-R feature! Select 20Ωs normally – if drive status fails to leave 0x51, try selecting 18Ωs or 22Ωs and try again.

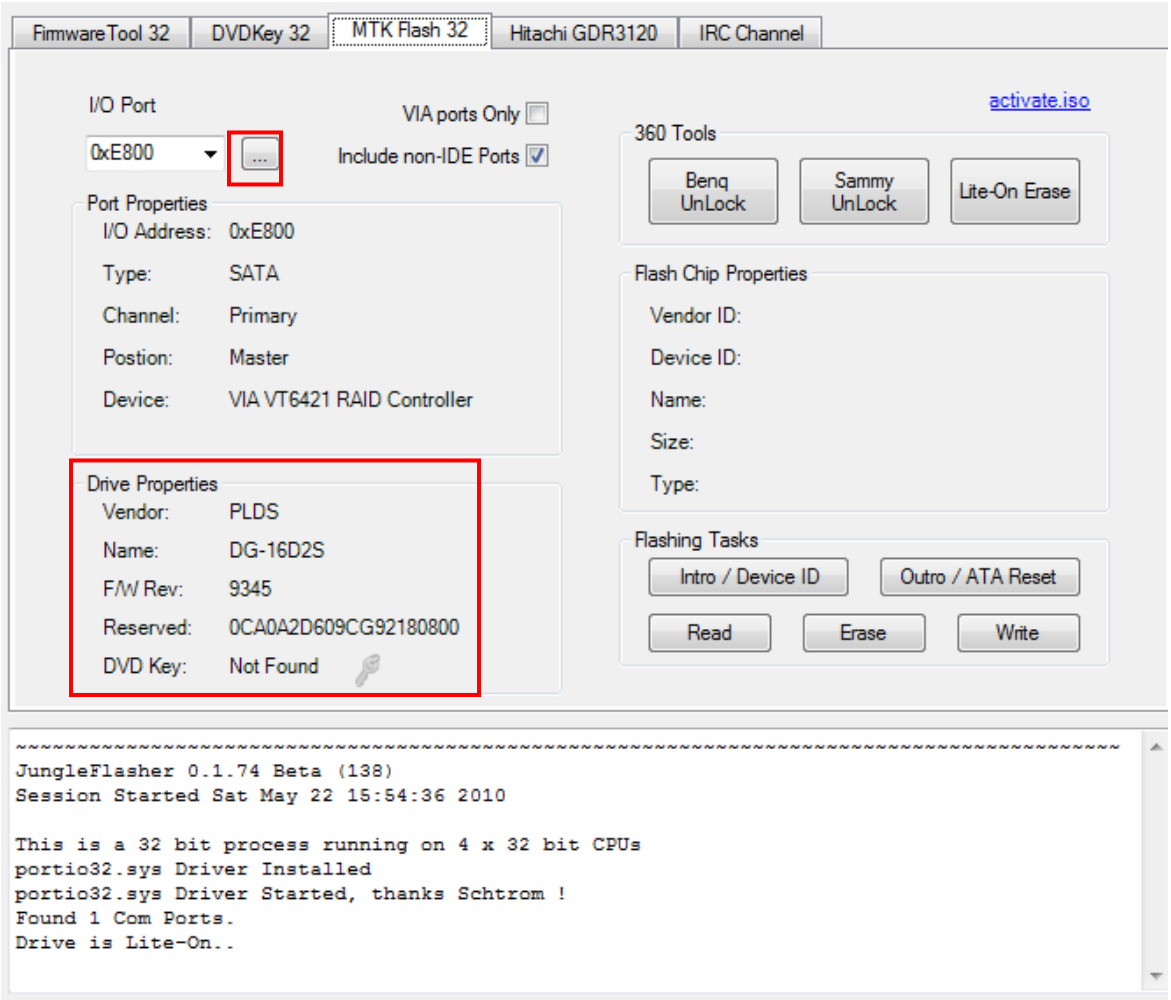


Once installed as per fitting instructions,

With switch in "Normal" position and MULTI-R set to 20 Ωs

Connect drive to PC's SATA and power drive (GREEN LED will be LIT), select **MTK Flash32** tab

Refresh, drive properties – so drive shows up



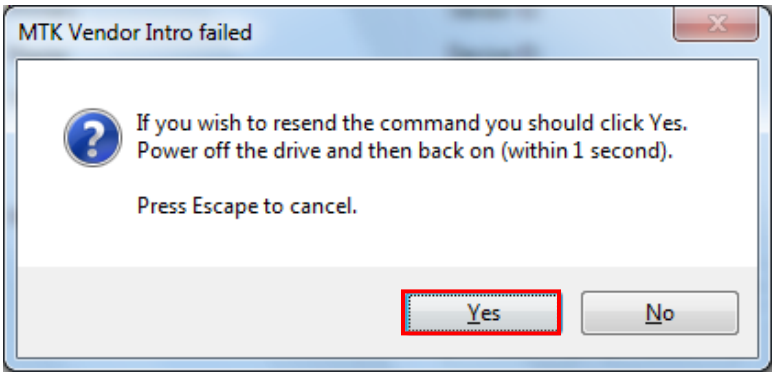
Turn power to the drive **off**.

Operate switch to the **R/W** position

Press **Intro/ Device ID** button

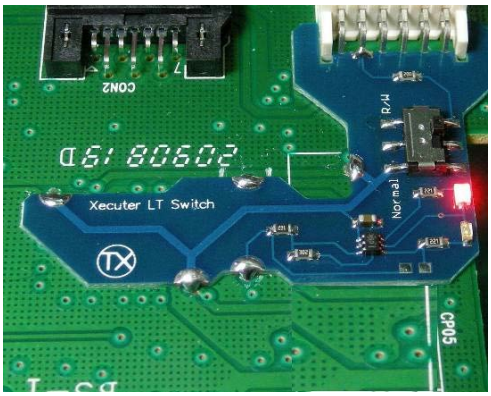
The following will appear! Press **Yes** button

Things not going as expected? – Read the FAQ's

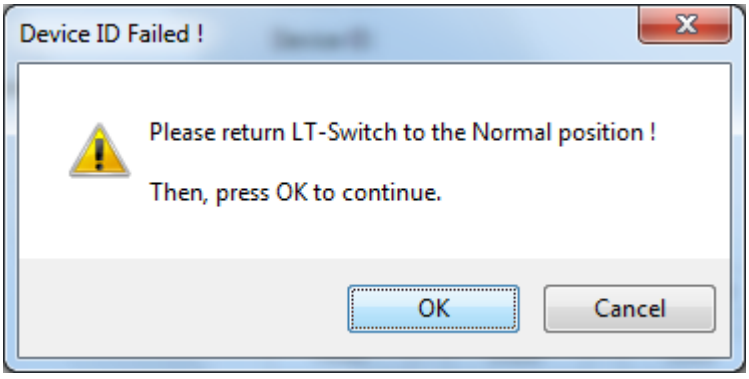


Then turn power to the drive ON again,

(Note the LED will now be RED instead of GREEN)



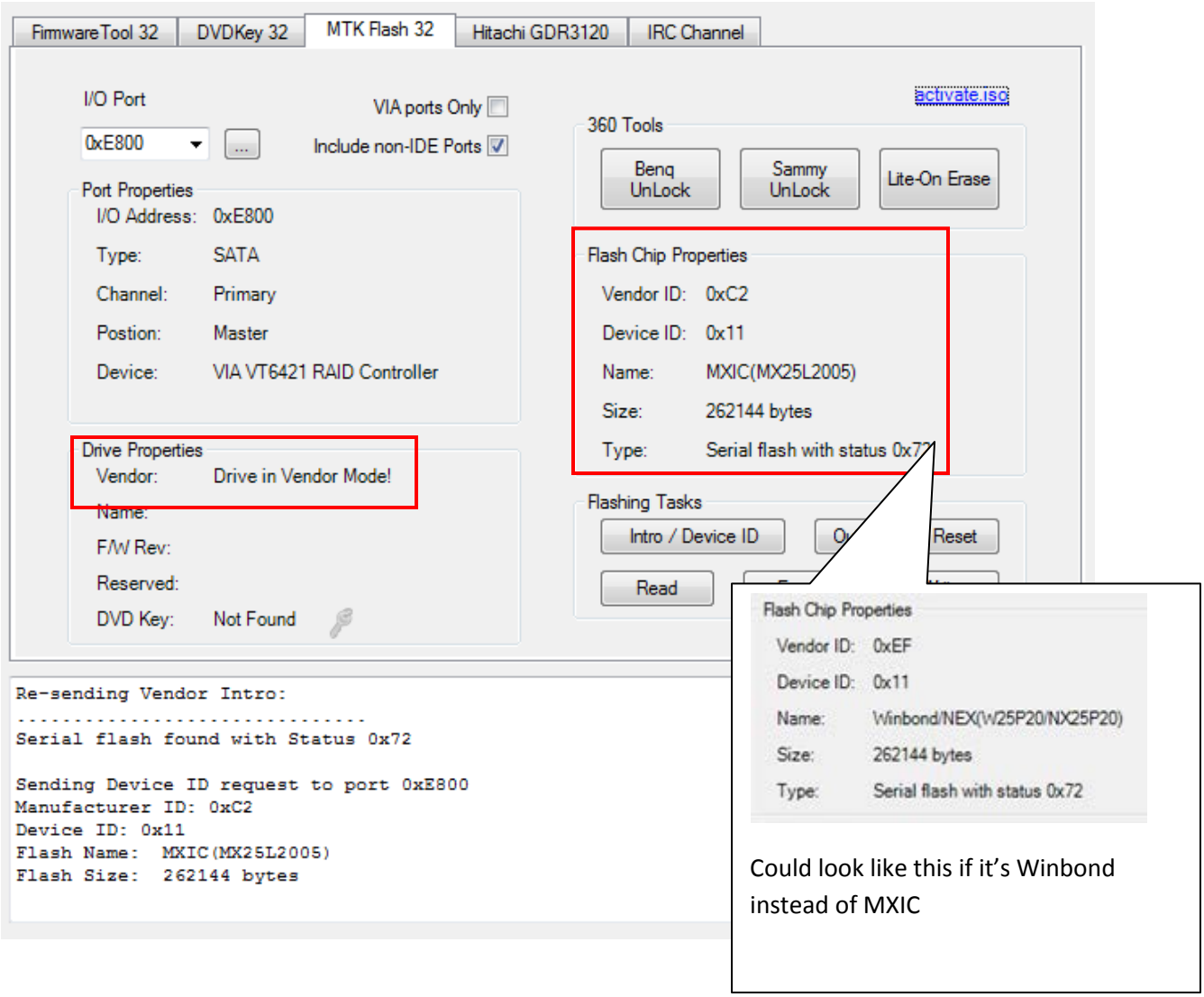
IF your drive has a WINBOND chipset then this will produce a screen showing **further instructions** (shown below)



then put LT Switch back to **Normal** and press **OK**

If everything has been done correctly – you should be faced with this!

Things not going as expected? – Read the FAQ's



Once you have the Correct status (shown above),

If you have a MXIC chipset & haven't already done so – now quickly return the switch to the '**normal**' position (GREEN LED iluminated)

Now press the **Read** button

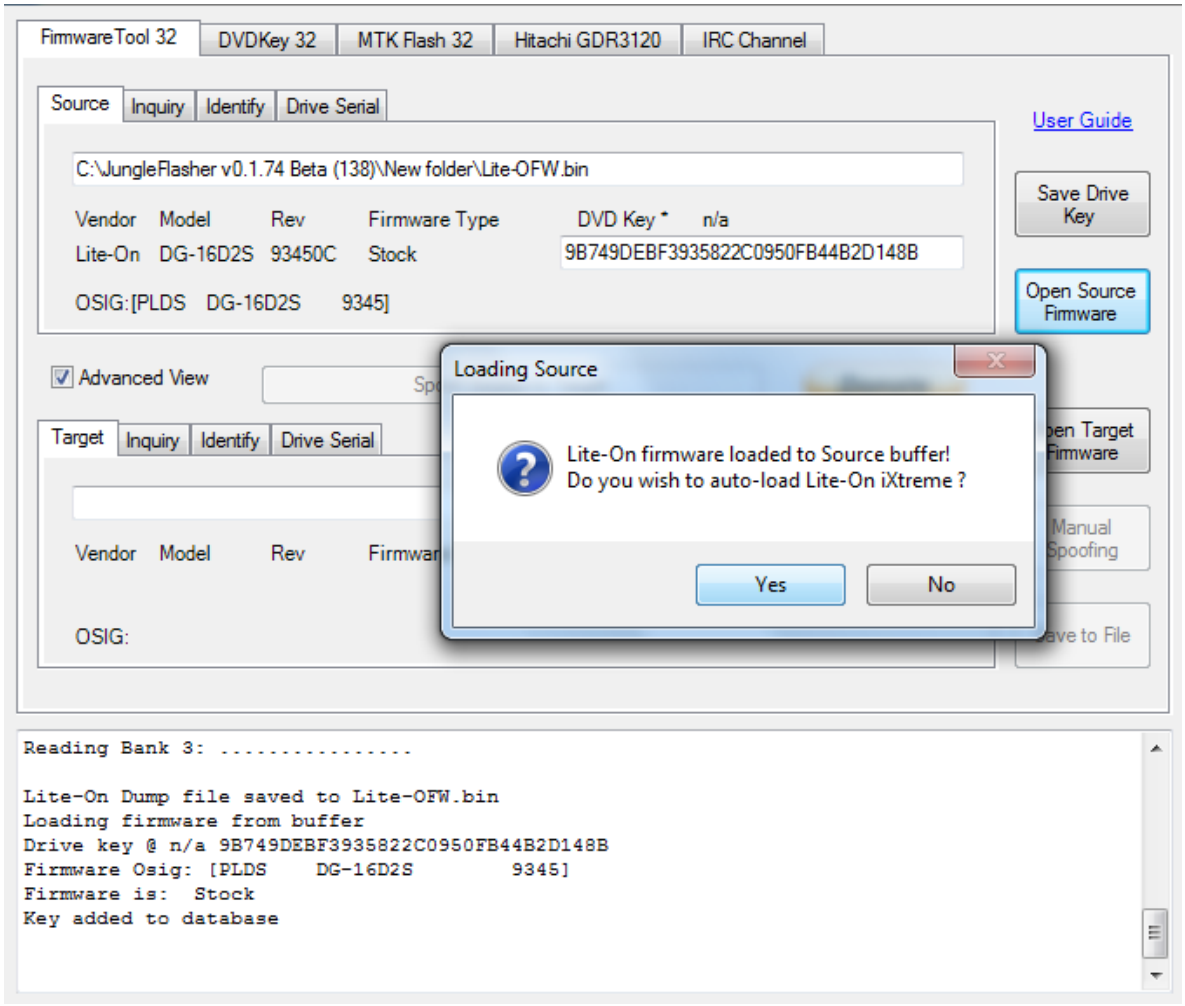
Jungleflasher will now Dump your Original LiteOn Firmware,

<u>When prompted to SAVE it is advised you do so!</u>

Things not going as expected? – Read the FAQ's

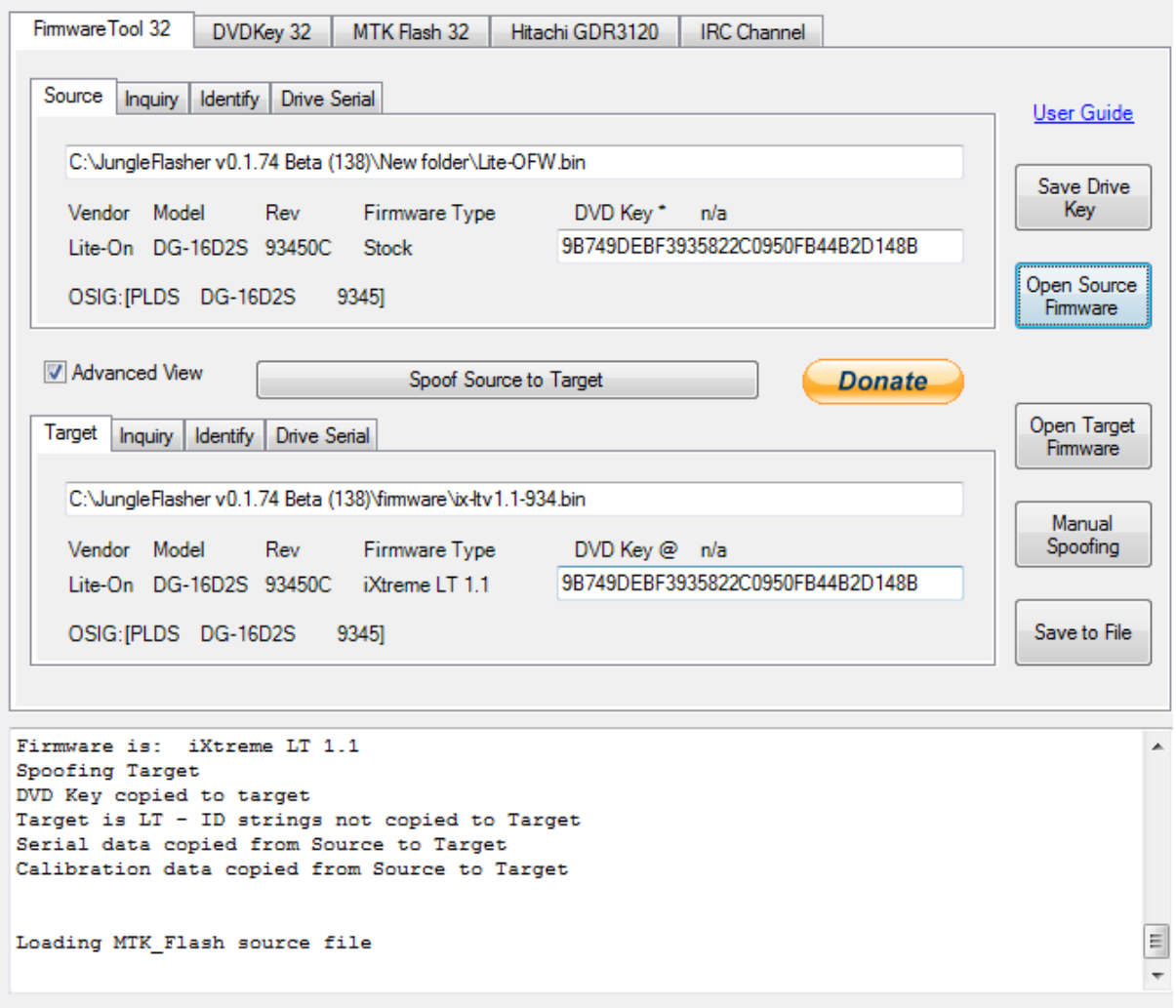
IF you get "parse failed" read THIS

The dumped firmware will now automatically be loaded into source in **firmwaretool 32** tab.



Select **Yes**

Things not going as expected? – Read the FAQ's



Just follow the standard write procedure!

So return to **MTK Flash 32** tab

NOW CLICK HERE!

Things not going as expected? – Read the FAQ's

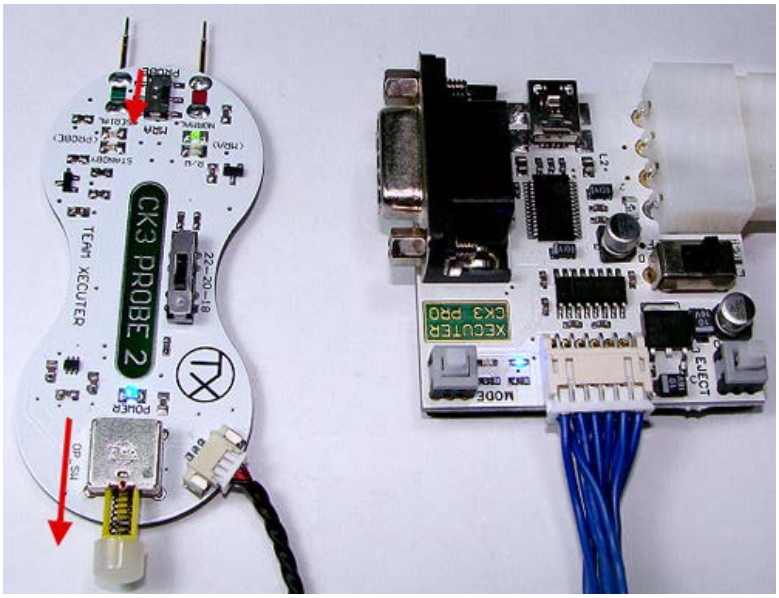
Xecuter Probe II Method

Connect the Xecuter probe II to the CK3 Pro.

Make sure the OP Switch is in the UP (ON) position and switch the mode to MRA.

Power on the CK3 pro you will see that the Xecuter probe II BLUE POWER LED is on and the MRA GREEN NORMAL LED is on (IF RED is LIT – op-switch is in WRONG position). This shows that everything is functioning.

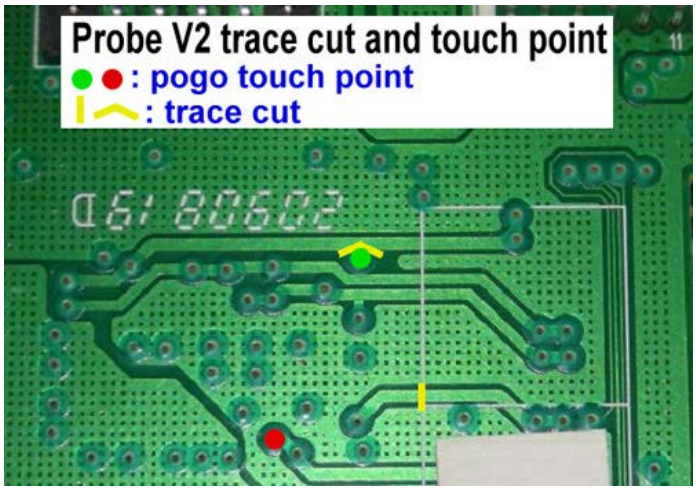
Now turn the CK3 Pro power OFF.



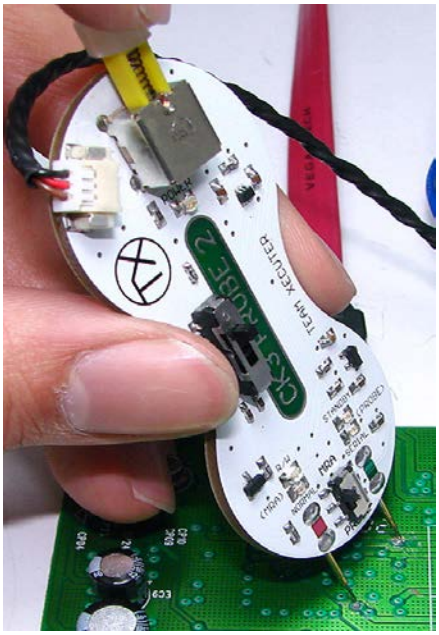
Use a *fiberglass scratch pen* and clean up the 2 holes to make the Probes contact better – Do this before cutting traces, as you are less likely to stress the pad 101 while it's still connected to trace

Cut traces on the PCB. The cuts are small and not difficult to do. Most people use a *Xacto knife* or a small dremel tool. Make 2 small cuts where the yellow lines are. . ***(Be very careful not to damage pad 101, once cut from the trace it becomes quite fragile)***

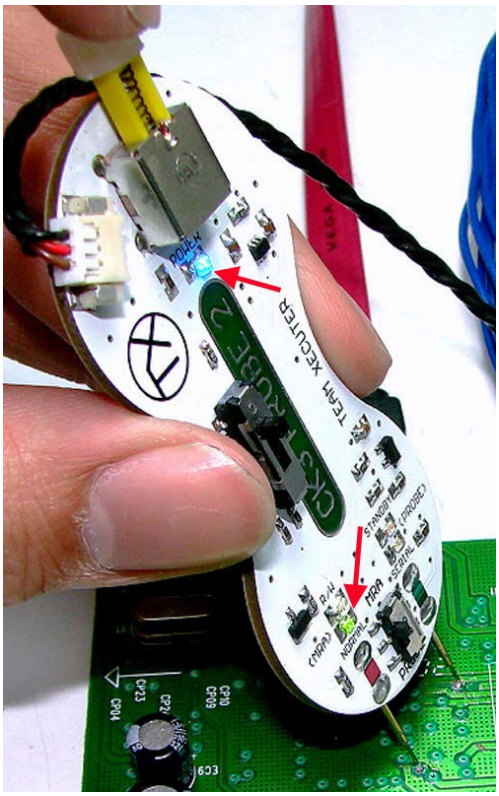
Things not going as expected? – Read the FAQ's



Now take the Xecuter Probe II and place the points onto the marked red and green positions. The Probe's pins are clearly marked. Remember at this stage the CK3 Pro power should be OFF.



Now turn the CK3 Pro power switch to on. You will now see the Xecuter Probe II BLUE POWER LED come on and also the MRA GREEN NORMAL LED come on.

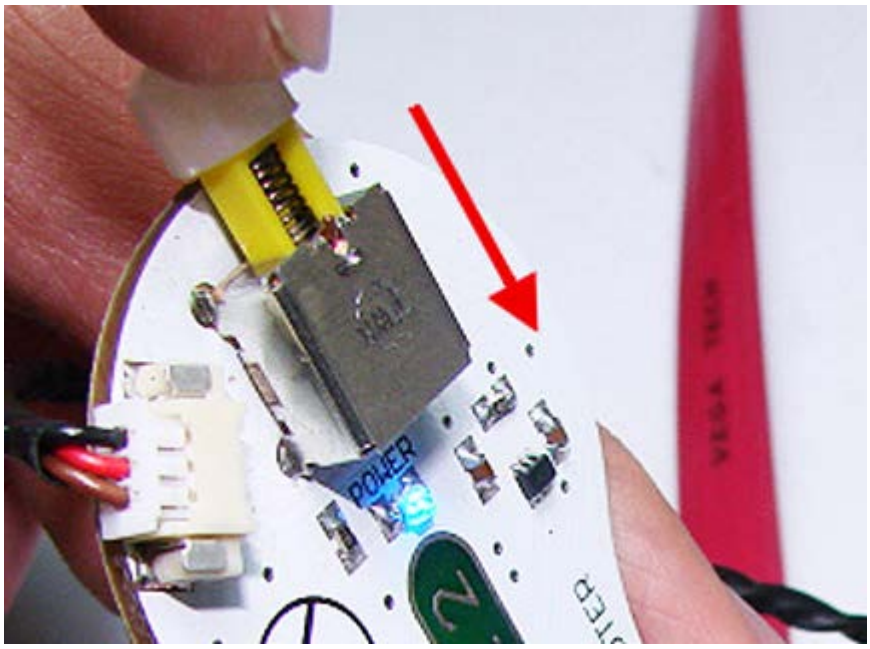


Refresh the I/O port in Jungleflasher on MTK tab. You should see the DVD drive properties if everything is connected and setup correctly. This is also an indication that your SATA is setup correctly. You may need to select another I/O port then return to the correct I/O port for it to show properly.

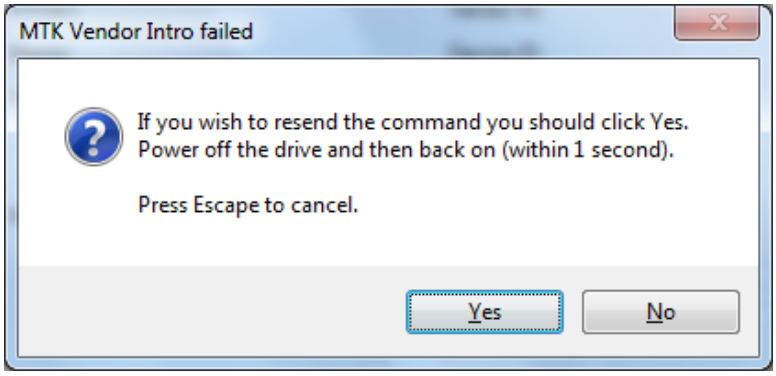
(ONLY EXAMPLE – You will see FW revision of YOUR drive)

Press the **Intro/Device ID** Button

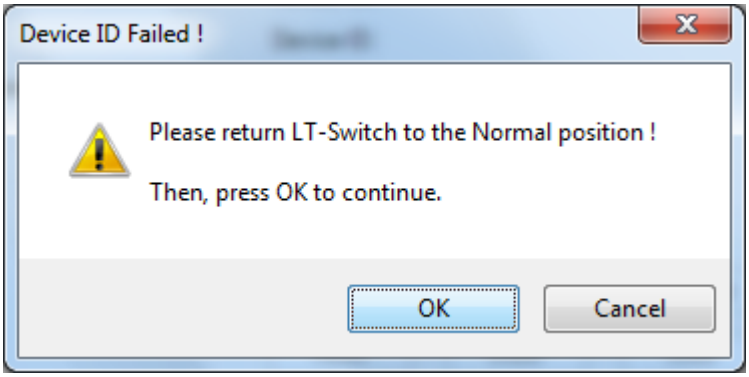
Turn the power OFF on the CK3. Push the OP Switch on the Xecuter Probe II down



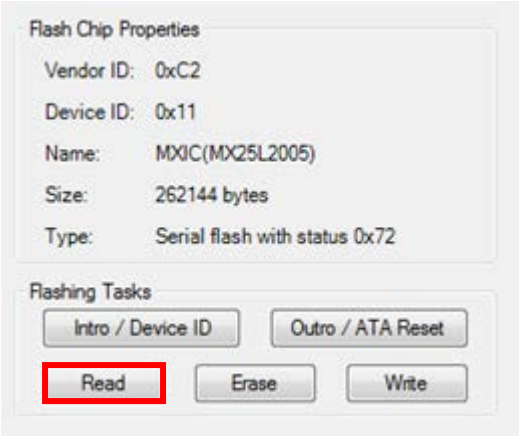
Press Yes! – Then power ON CK3,(RED LED – if it doesn't go on – don't worry – continue)



(NOTE: If you have a Winbond IC you may see a warning to switch LT switch back to normal then press ok! Simply operate OP Switch to up position then click ok)



You should now get Status 0x72 and you are in vendor mode. As soon as you see the flash chip properties switch the OP SWITCH up to Normal mode right away (Green LED). Hold probes in place and dump firmware by pressing READ button,



Now you have a choice, you can either

1. ONCE "save" button appears you can remove probe, power off CK3 and SAVE that OFW Once you have dumped the drive simply repair the traces with the conductive glue that is included with the Xecuter Probe II (or use your own if you bought the early batch that wasn't included - simply solder) and you can then proceed to erase and flash your liteOn as normal!

   Simply load your Lite-OFW as source (if you have closed Jungleflasher whilst you repaired your PCB traces) AUTO load the target firmware, then Proceed to **ERASE & WRITE**

   OR

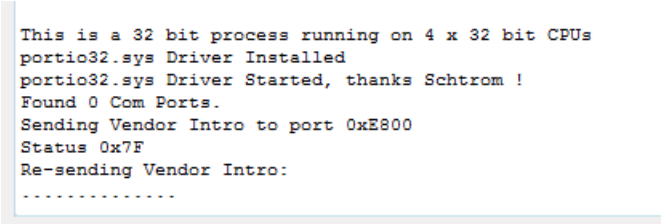
2. Continue to hold probe in place, allow JF to Autololad the fw, select **Mtk tab** then press **WRITE** **(***remember to repair your trace cuts when finished!- before testing in console*).

Vampire Using Rebuild Board

Install the Rebuild board as shown on [360Xtractor website](#).

On MtkFlash32 Tab of Jungleflasher – Press **intro/Device ID** Button then press the Yes on the pop-up window that appears.

Which will lead to show the following

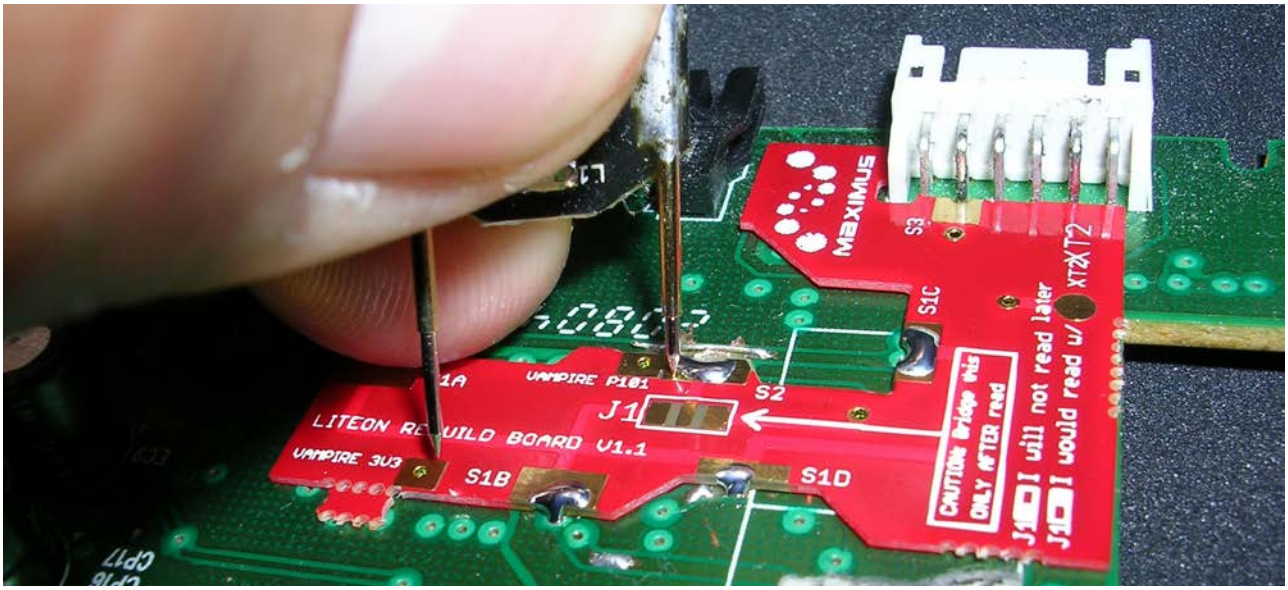


DONT POWER XTRACTOR YET.

PRESS THE BUTTON ON THE VAMPIRE AND HOLD IT, then make the PIN101 Probe touch the "VAMPIRE P101" Pad on the rebuild board,

IMPORTANT, IT'S RECOMMENDED - TOUCH ON THE PAD SURFACE AND NOT ON THE HOLE.

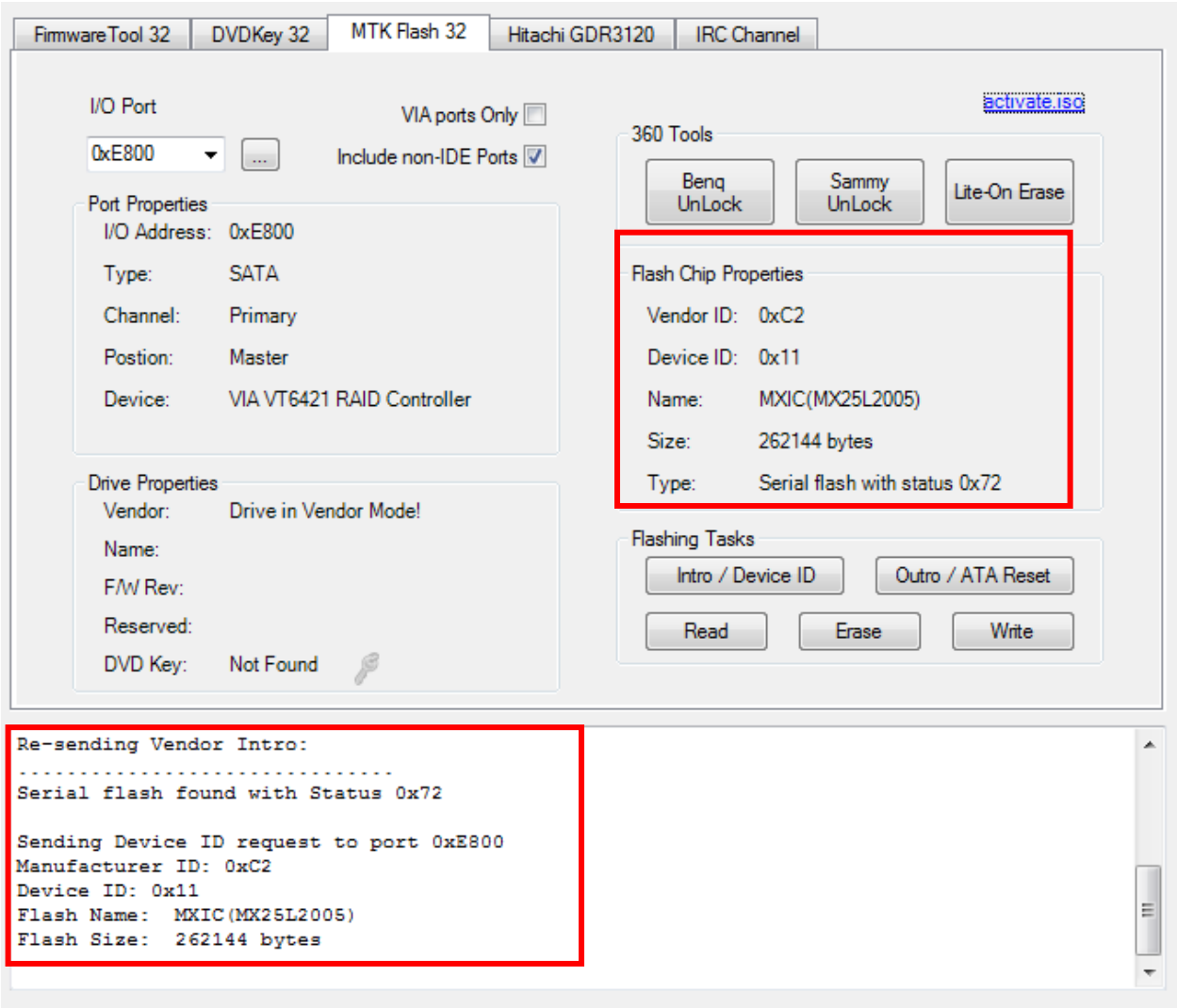
3.3v probe it's **NOT Required** to touch the pad since the rebuild board already supplies the required voltage, you can just have it not touching the pad at all, in case you choose to touch with the probe make sure **don't put into the hole.**



While you are holding the button in and the probes are in contact with board

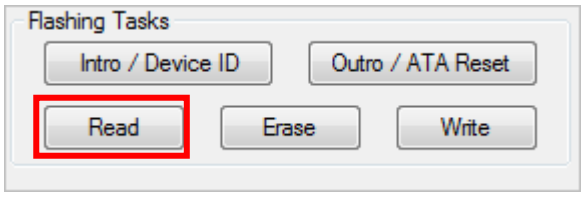
TURN ON XTRACTOR

after 1 or 2 seconds you should see the drive gets detected with a Status 0x72



In case you get STATUS 0x72 but the VENDOR ID/DEVICE is 0xFF press **INTRO/DEVICE ID** If status keeps 0xFF try removing the Vampire first then press **INTRO/DEVICE ID** Button

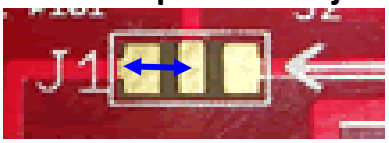
Now if you have not done, remove the Vampire from touching the board and press **READ** button



Things not going as expected? – Read the FAQ's

SAVE the Firmware you have just Dumped!

Power off the 360xtractor and proceed to join jumper as required!

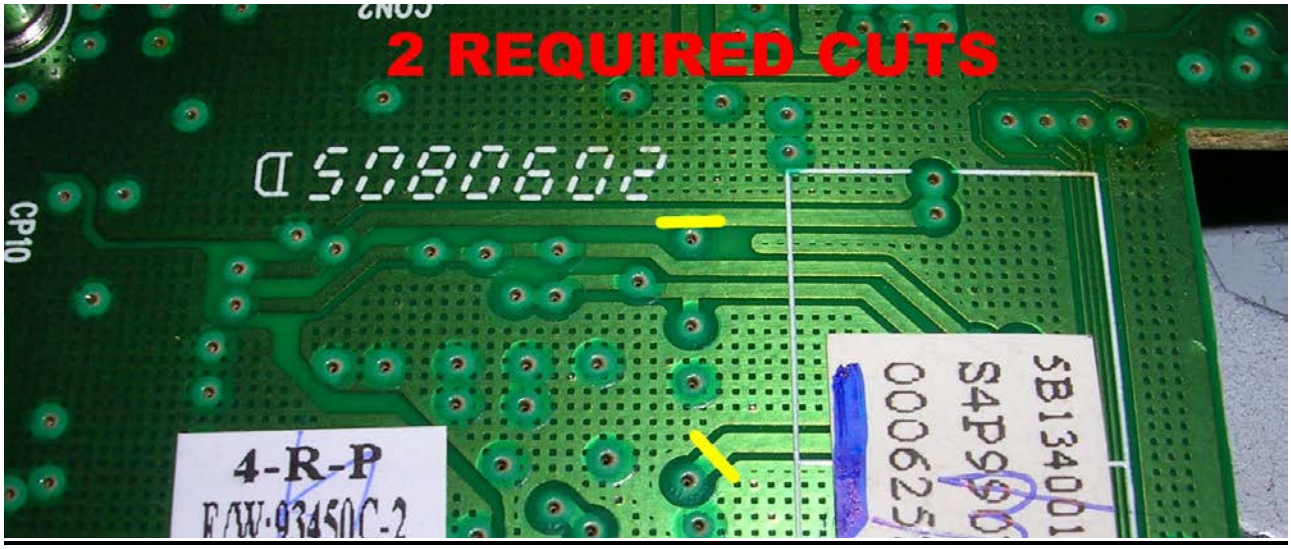


Once you have soldered the jumper of your choice! Power on the 360xtractor again – Proceed to

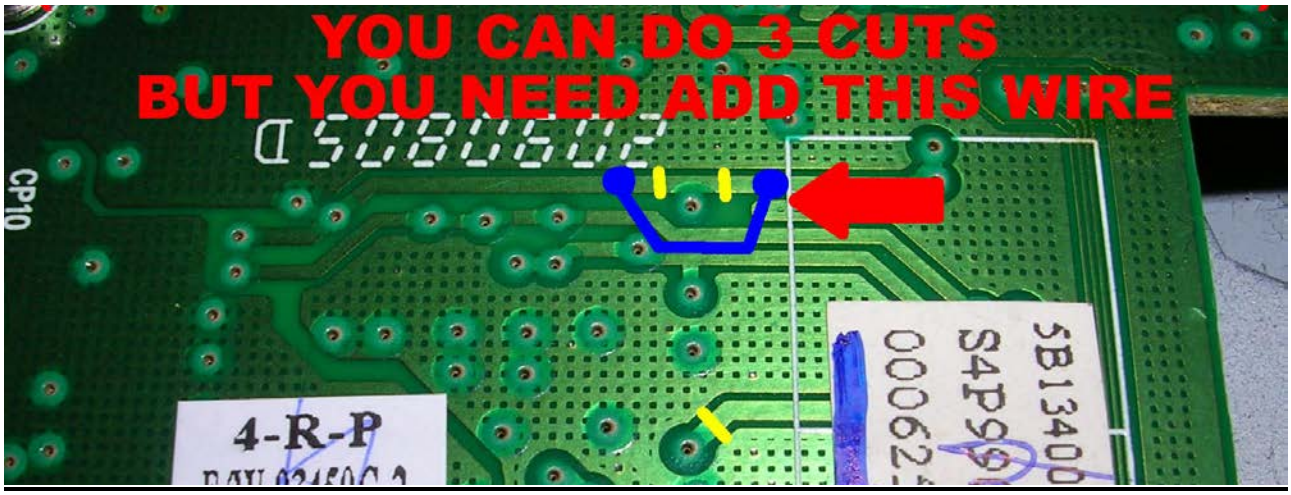
ERASE & WRITE

Using Vampire if you are NOT USING REBUILD BOARD!

Visit website. For their own Tutorial – they suggest cutting PCB as follows

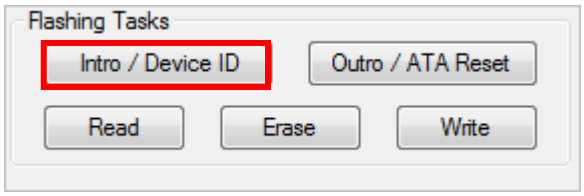


OR



On MtkFlash32 Tab of Jungleflasher – Press **intro/Device ID** Button then press the **Yes** on the pop-up window that appears.

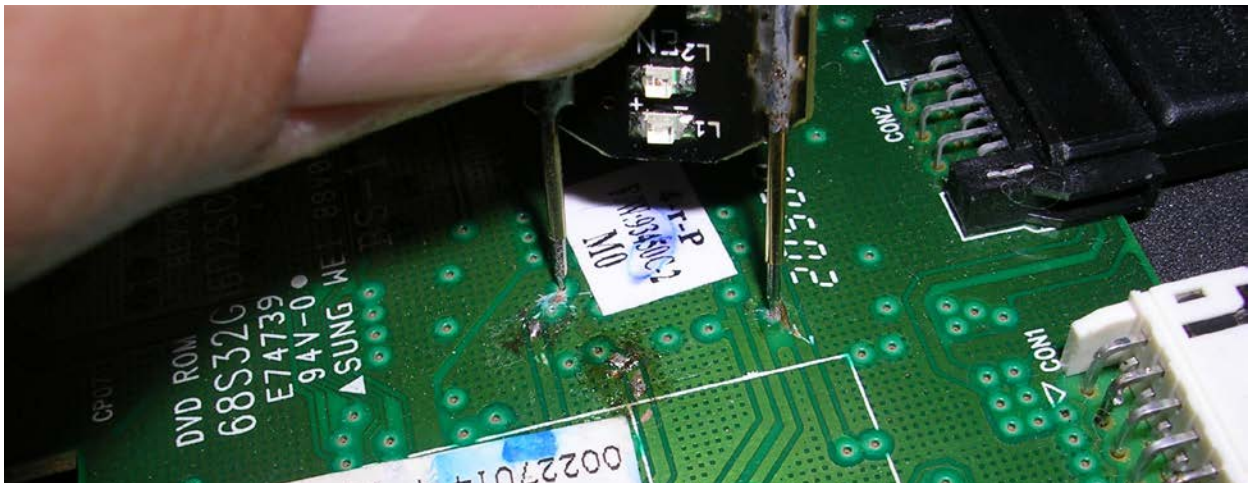
Things not going as expected? – Read the FAQ's



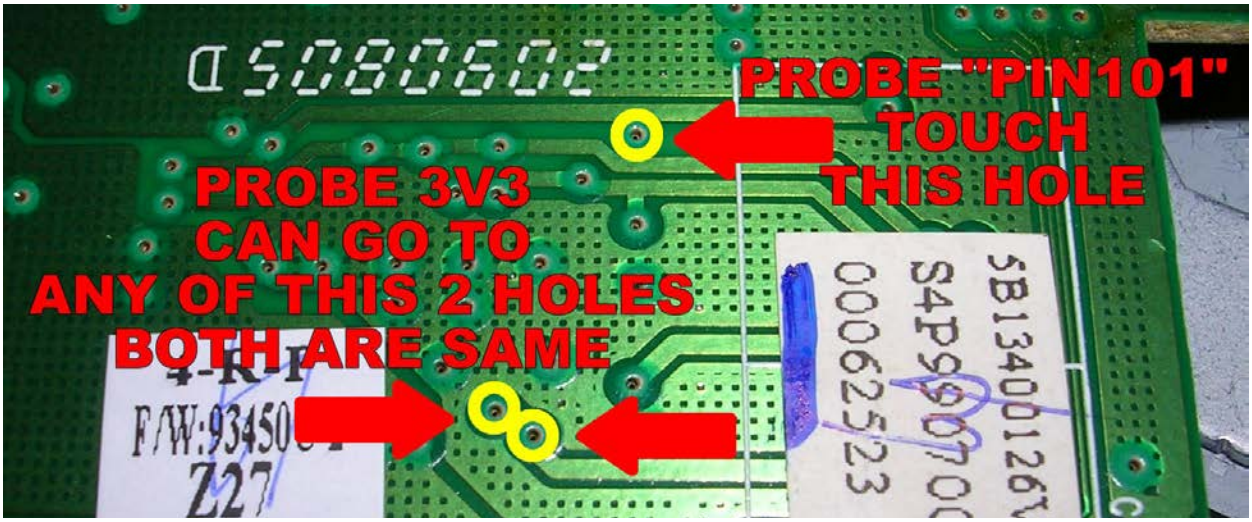
Which will lead to show the following

```
This is a 32 bit process running on 4 x 32 bit CPUs
portio32.sys Driver Installed
portio32.sys Driver Started, thanks Schtrom !
Found 0 Com Ports.
Sending Vendor Intro to port 0xE800
Status 0x7F
Re-sending Vendor Intro:
.............
```

Probe the 101 pad and 3.3v points on PCB whilst holding the button on vampire pressed in!



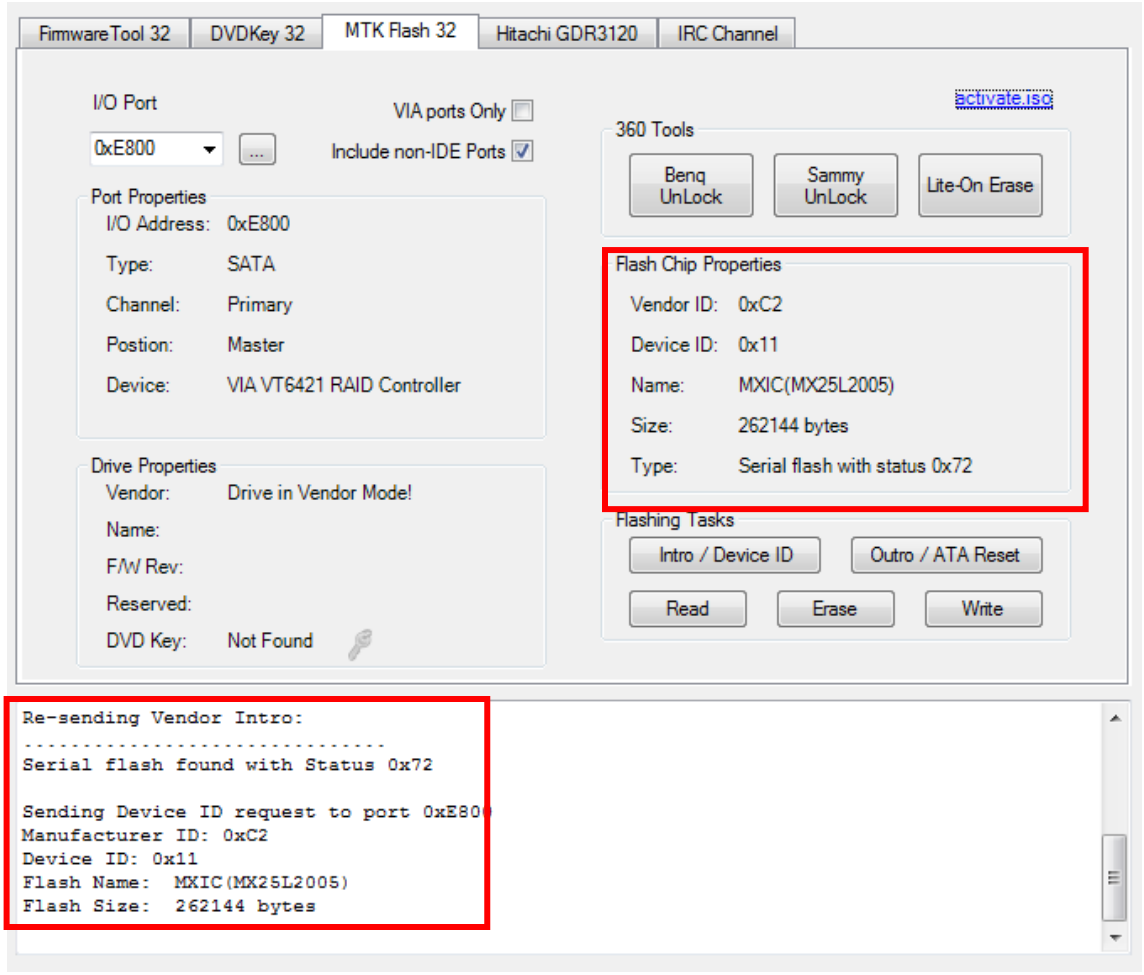
Things not going as expected? – Read the [FAQ's]



While you have the button on Vampire pressed in and probing the correct holes

TURN ON XTRACTOR,

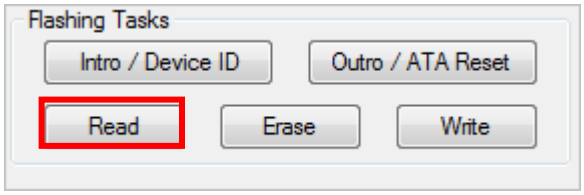
after 1 or 2 seconds you should see the drive gets detected with Status 0x72



Now release the button on vamp

whilst still Holding the probes in contact with PCB

Then press **READ!**



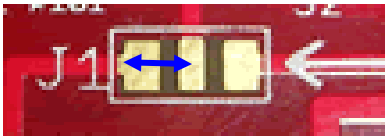
when the "Save" option appears it's safe to remove probe from PCB

SAVE the Firmware you have just Dumped!

Power off the 360xtractor

Proceed to join jumper with solder as required!

Things not going as expected? – Read the FAQ's



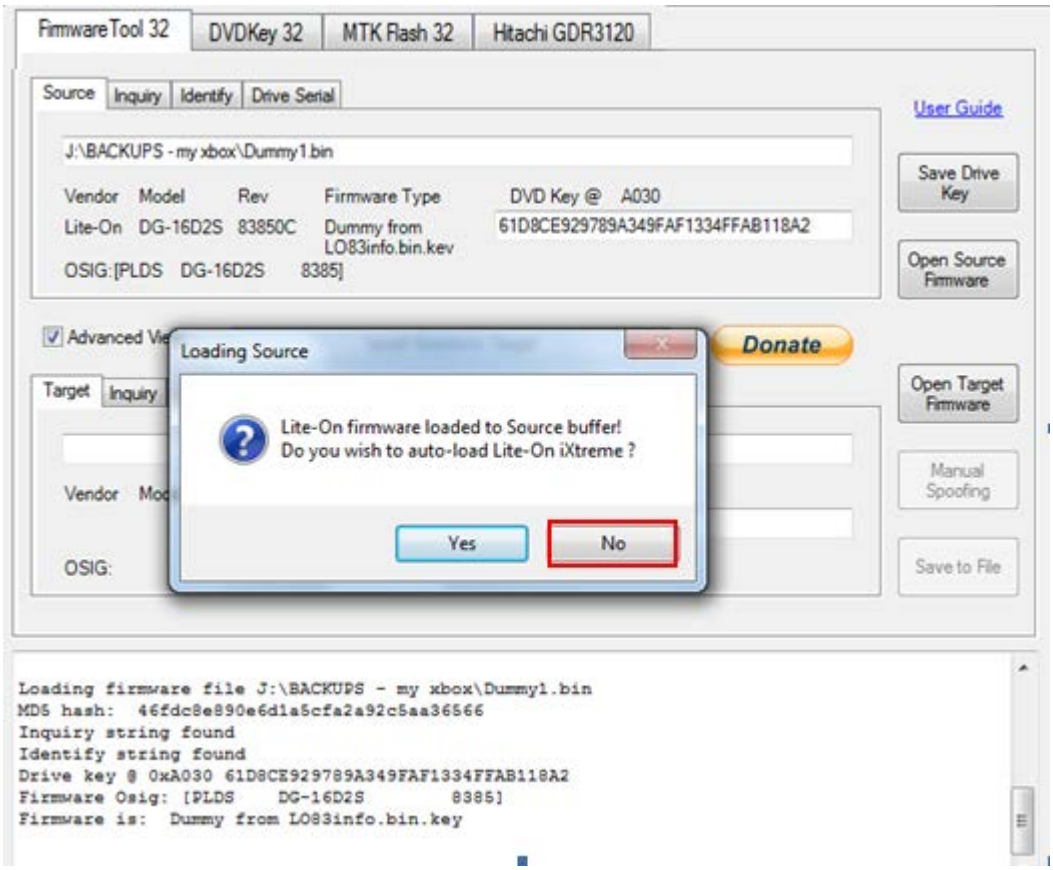
Once you have soldered the jumper of your choice! Power on the 360xtractor again – Proceed to

ERASE & WRITE

Return a LiteOn to Stock Firmware

To return a LiteOn drive to stock you need your Dummy.bin and a Stock FW for your relevant drive.

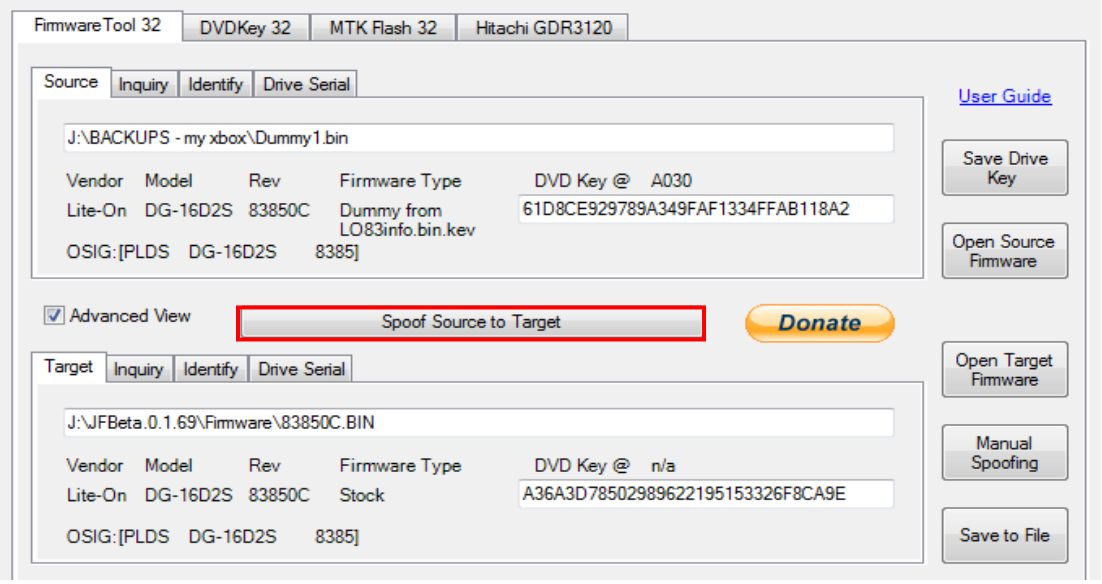
Simply load your Dummy as Source, **Decline** the Auto load of iXtreme firmware,



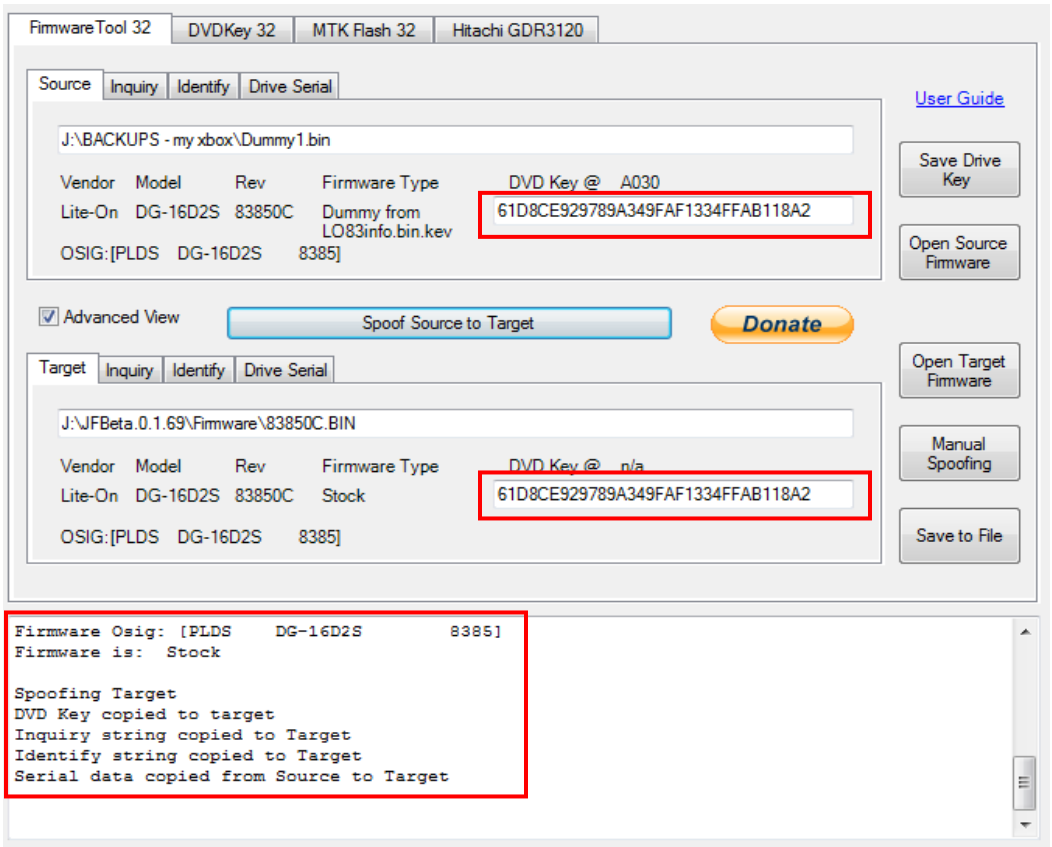
Load the stock firmware as target!

Then press **Spoof Source to Target** button

Things not going as expected? – Read the FAQ's



Check the running log to see all the info has been copied over, double check the key matches. Then if required, press **Save to File** button!

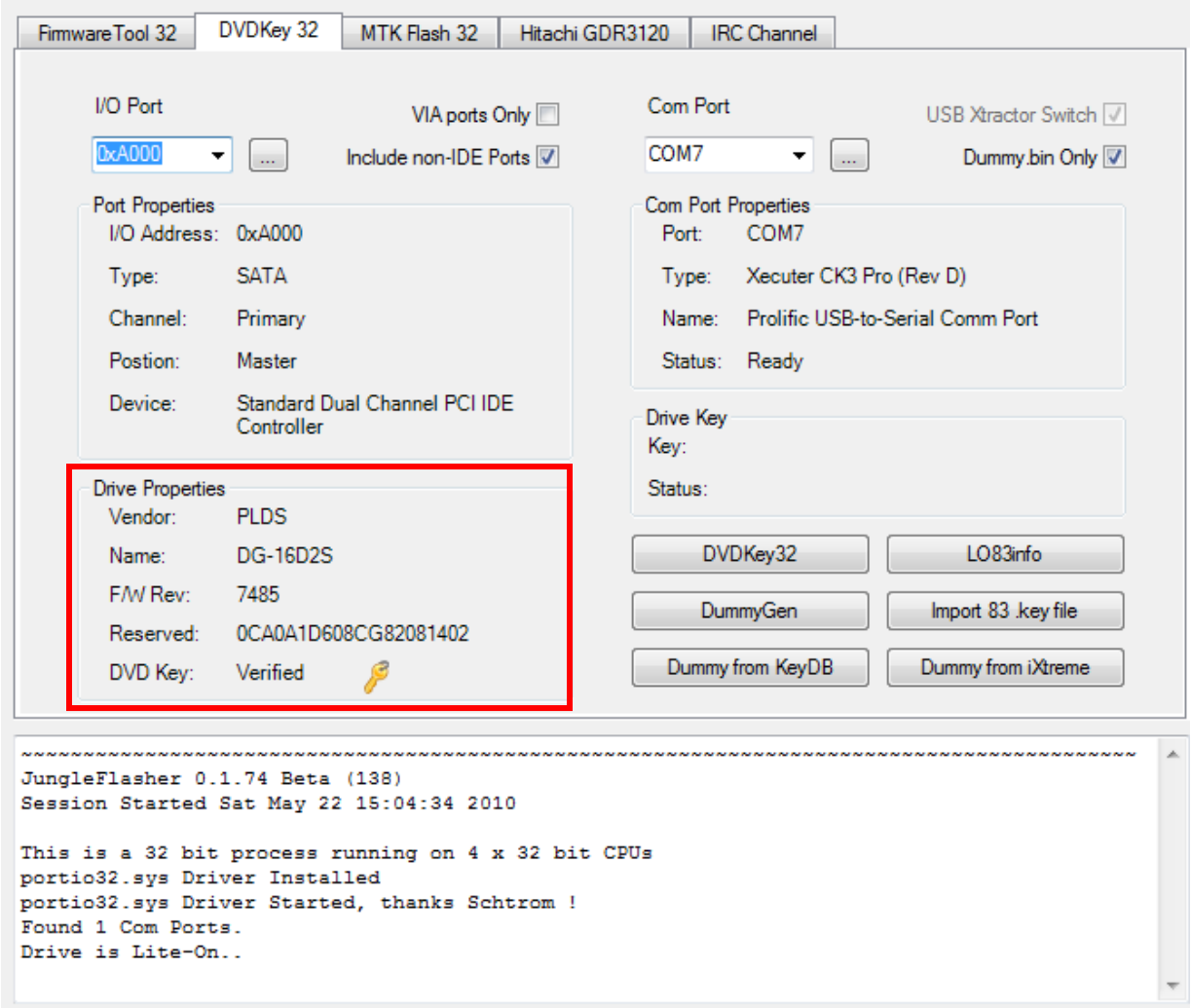


PROCEED TO ERASE & WRITE – CLICK HERE!

Things not going as expected? – Read the FAQ's

Using the KeyDatabase to Retrieve/Create your Firmware

So – you have connected your drive that you flashed already! You know it's in your Key Database as you flashed it previously. Connect it and refresh the port!



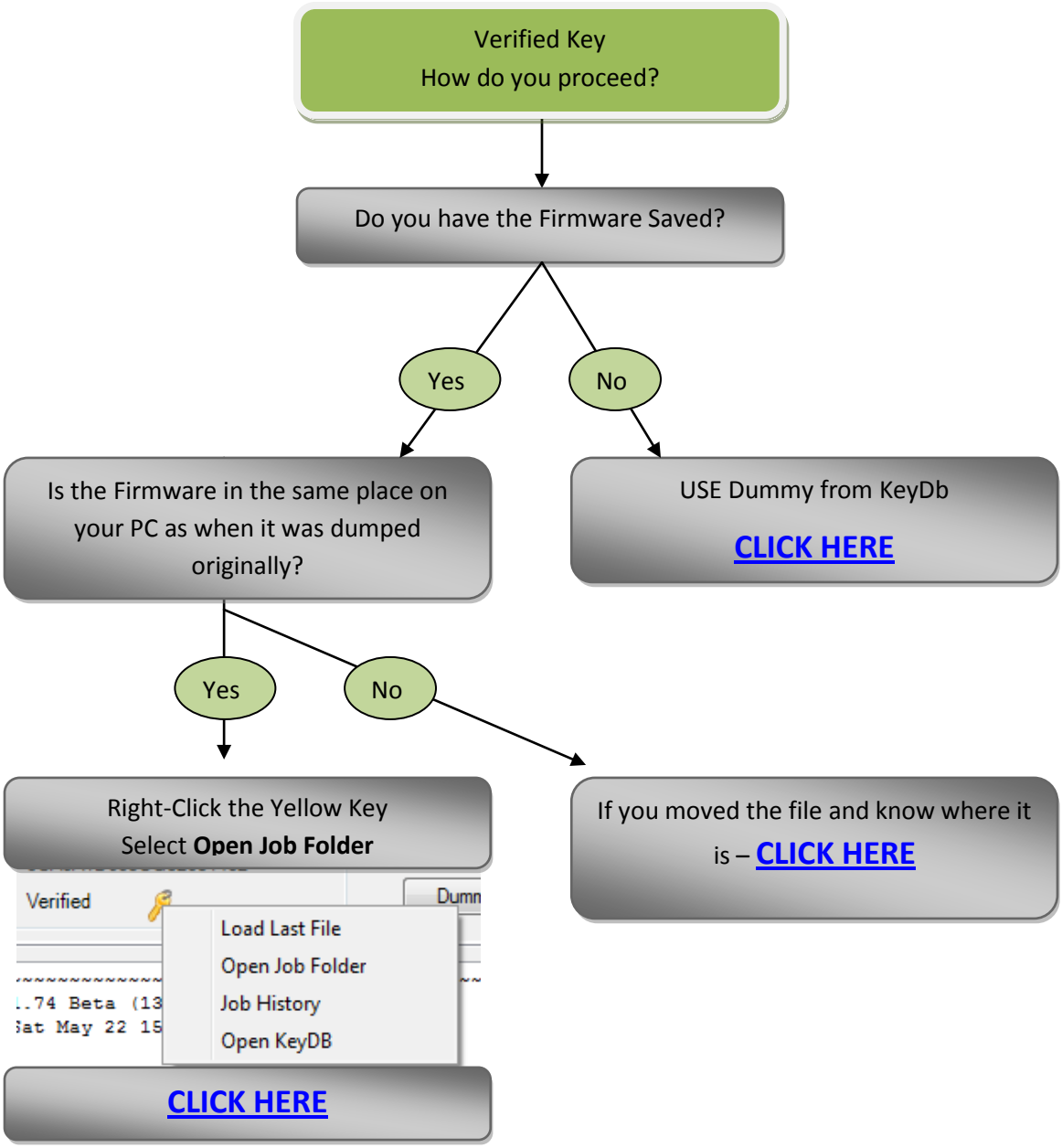
Just from refreshing the port Jungleflasher has identified that you have previously dumped this drive, it looks up the key from the database and tests it on the drive! – It's verified! ☺

So WITHOUT Opening the drive - you know what the key is for this drive!

As it's in the Key Database.

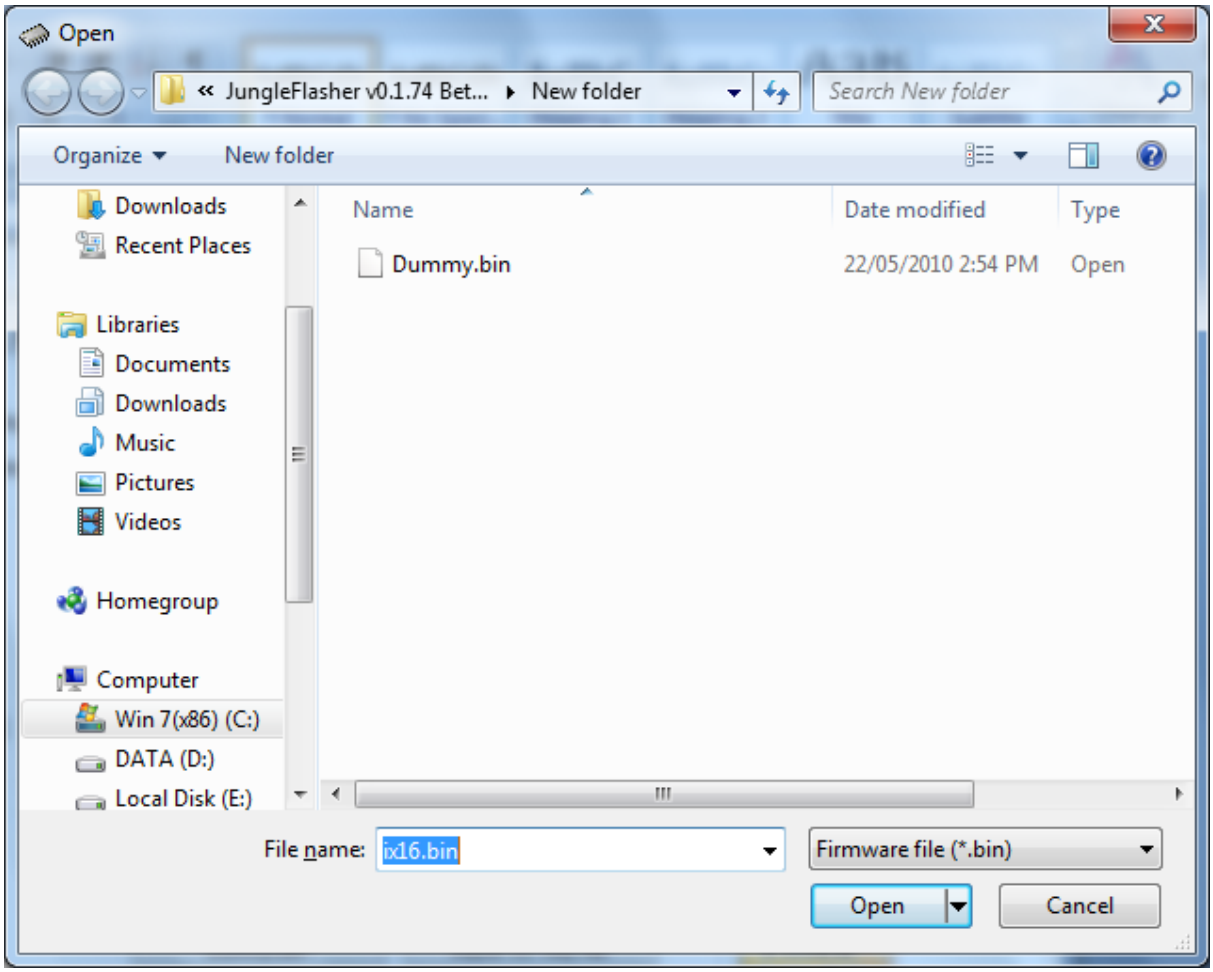
To use this information to re-flash your drive with an update or back to stock firmware, you have several choices! Follow the route below

Things not going as expected? – Read the FAQ's



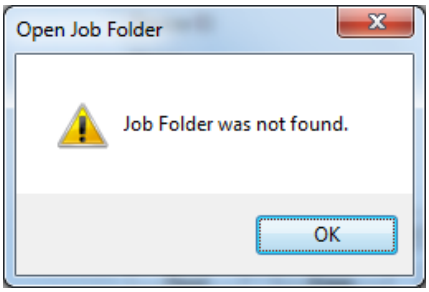
The other options in that menu are self-explanatory! If you need to ask what they do then maybe you shouldn't be modding drives!

IF you want to open the folder containing the firmware you dumped from the drive originally select **Open Job Folder**



Select the Dummy.bin or Lite-OFW.bin (dependant on how you dumped firmware in first place)

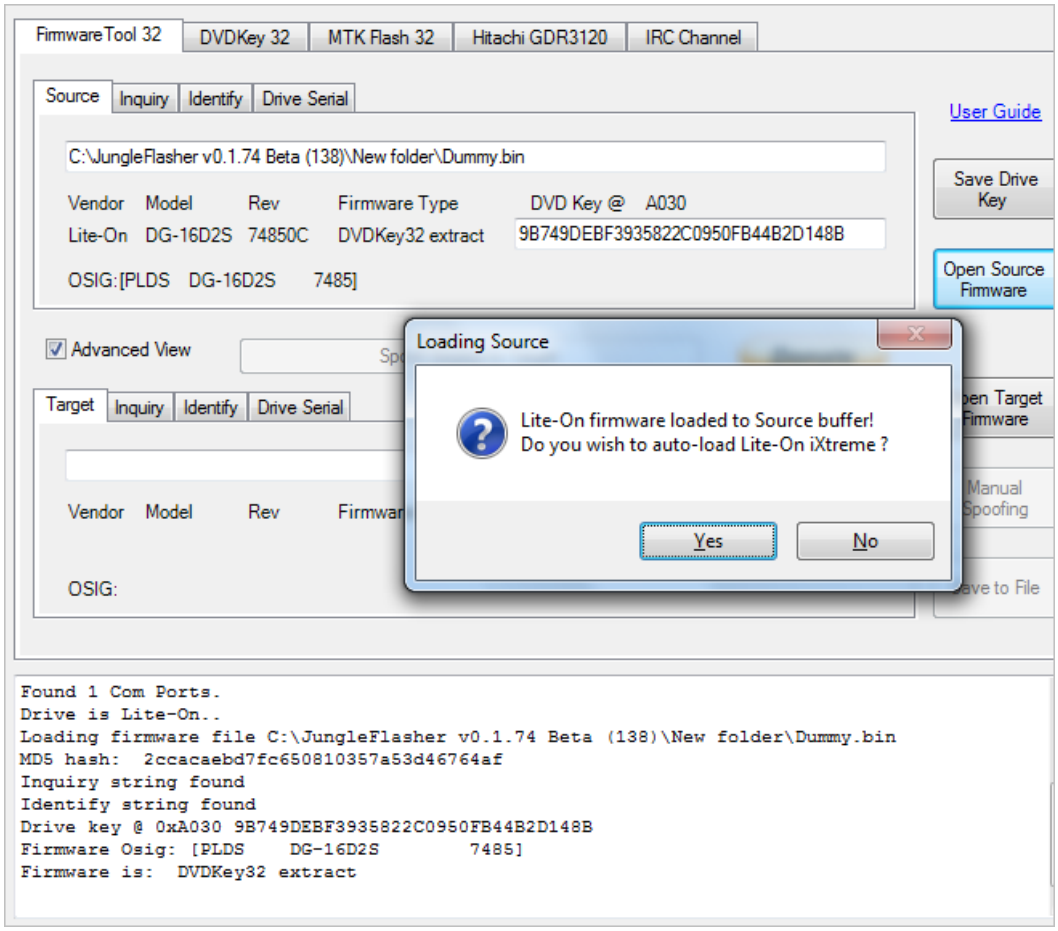
NOTE : If you have moved the folder you will see this!



If you know where it is **CLICK HERE**

NOTE: IF YOU DONT HAVE THE FIRMWARE SAVED? **CLICK HERE**

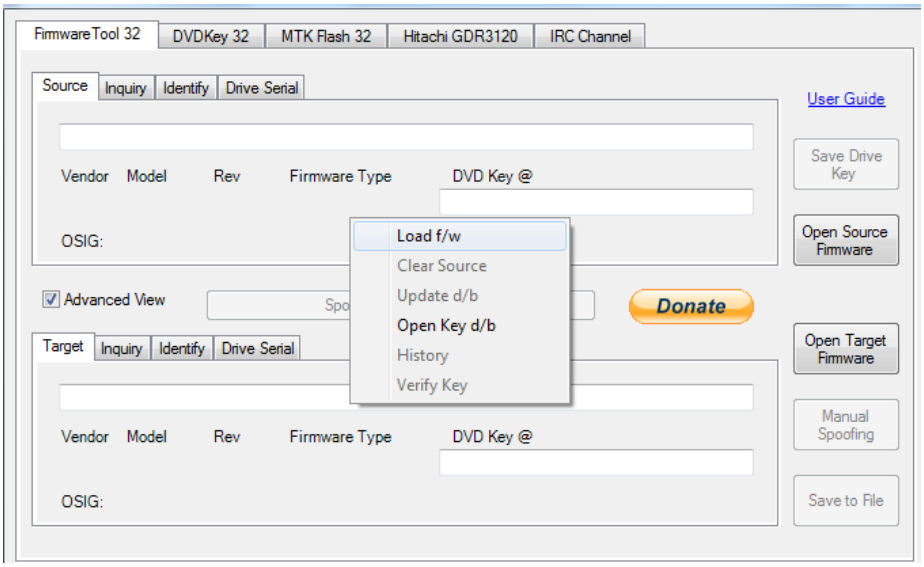
It will open as source and auto load the latest iXtreme firmware.



Then follow the normal **ERASE/WRITE procedure**

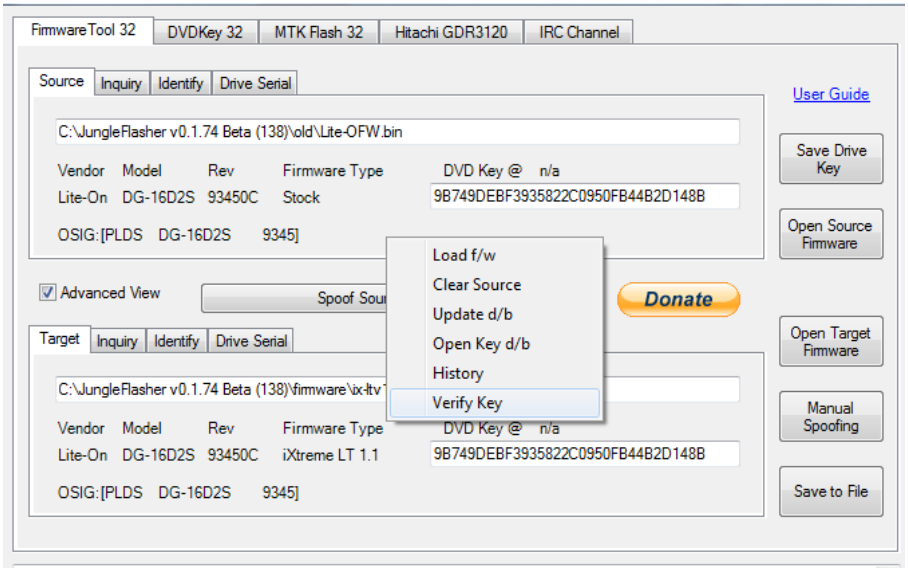
Things not going as expected? – Read the FAQ's

Have the firmware saved in another location? Go to **Firmwaretool 32** tab, **right-click** over the source section and select **load fw** or click **Open Source Firmware** button



Open the firmware file you think is the correct Dummy.bin or Lite-OFW.bin

Allow it to autoload the latest iXtreme Firmware. Then **right-click** over the source firmware section again. Select **Verify Key**.



Now check the Running log for this!

```
Attempting to verify Source Key to drive on port 0xE800

Source Key 9B749DEBF3935822C0950FB44B2D148B verified.
```

It's Verified against drive ☺ click **MTKFlash 32tab** and proceed to **ERASE/WRITE**

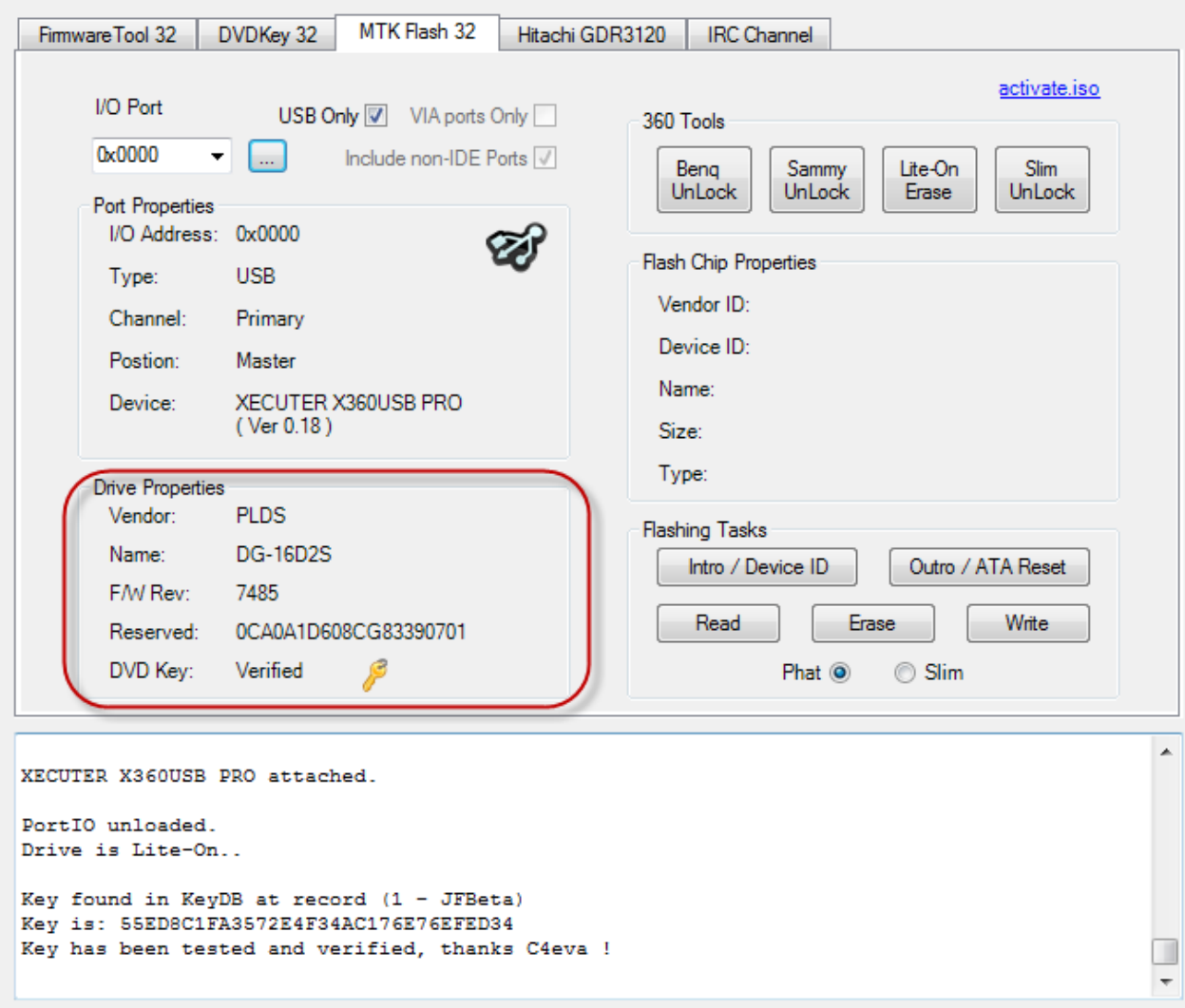
Things not going as expected? – Read the FAQ's

Using the KeyDatabase to Create your Firmware

If you are convinced that you have flashed this drive before (regardless of type) but it doesn't show as verified initially - you can test all the keys in your Key Database by using "Dummy from KeyDB" it will only create new firmware for Lite-ons but it will find the correct key of other types of drive, if you have it in the database! (if you have a lot of keys in DB it may take some time)

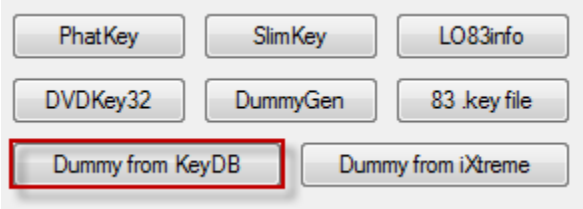
You no longer have the Dummy.bin or OFW.bin but the drive is showing as verified in KeyDB?

Connect the drive and refresh the port, ensure it shows up as having a verified key.

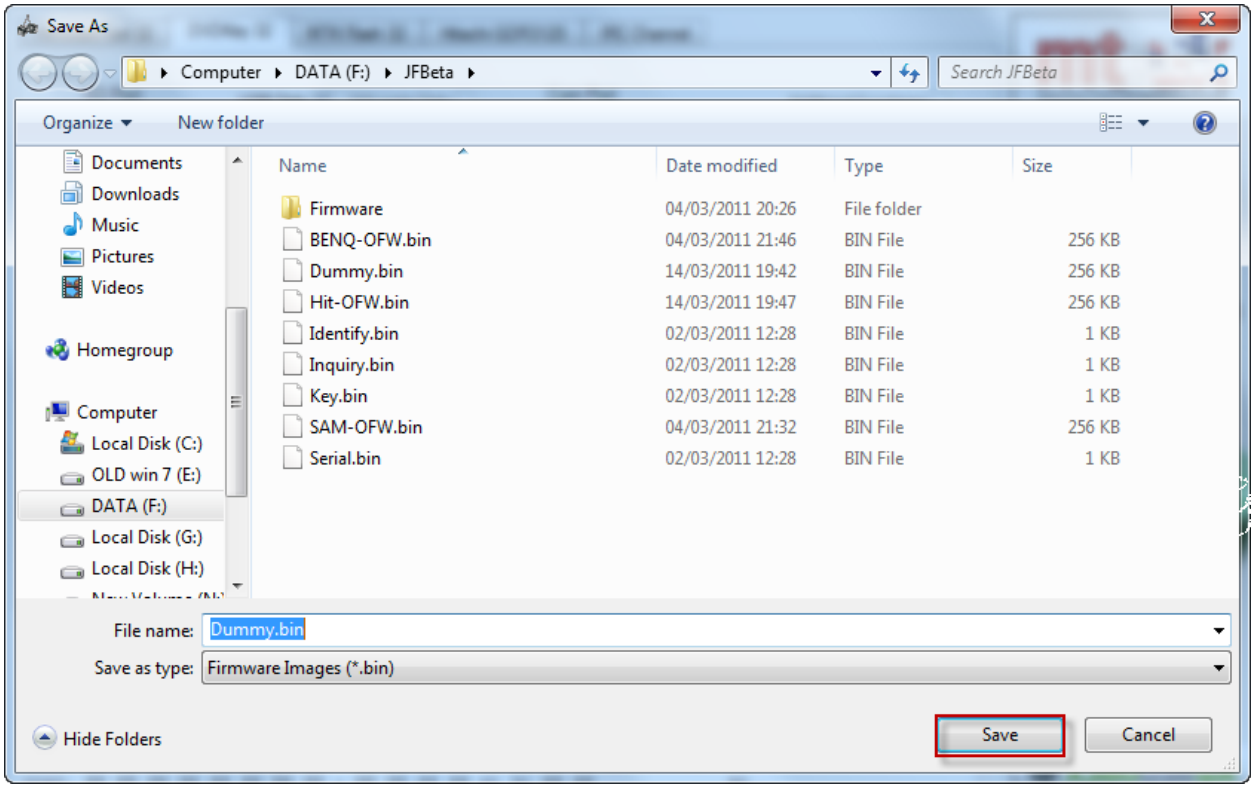


Click **Dummy from KeyDB** button

Things not going as expected? – Read the FAQ's

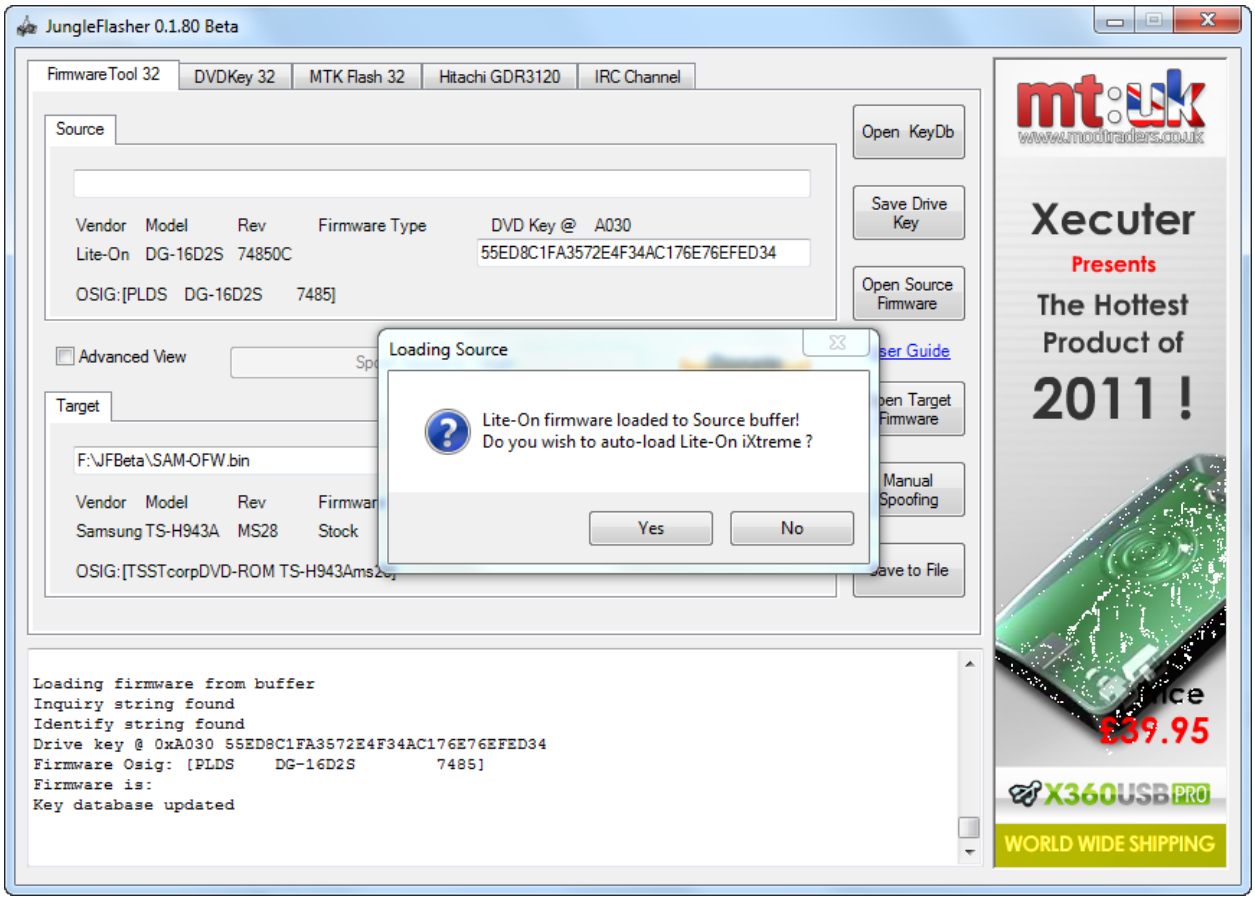


Then it will ask you to save the new Firmware it has created from the Key DB and querying the drive itself.



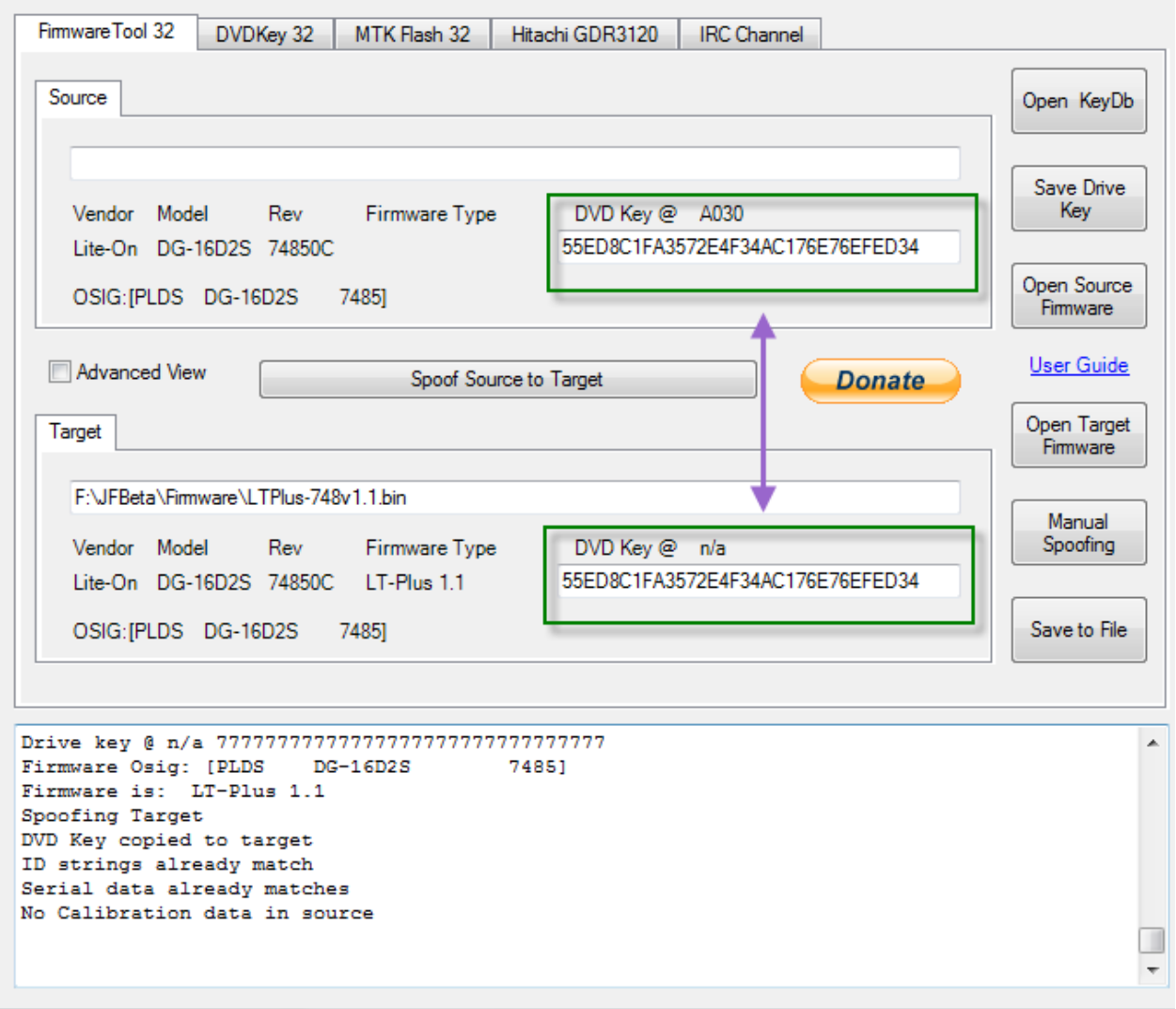
Then will automatically load the new firmware as source

Things not going as expected? – Read the FAQ's



Click **Yes**,

Things not going as expected? – Read the [FAQ's]



then follow the normal procedures for erasing and writing to the drive!

For **Slim LiteOn 9504** **CLICK HERE**

For **Phat LiteOn** **CLICK HERE**

Things not going as expected? – Read the FAQ's

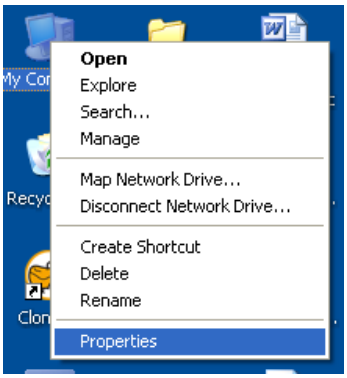
Removing VIA drivers (Windows XP/Vista/Win 7)

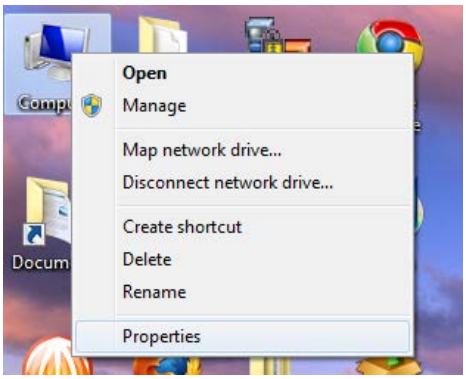
NOT TO BE DONE IF YOUR MAIN HARD DRIVE IS ON VIA SATA CARD or IF YOUR VIA CHIPSET IS ONBOARD(i.e. NOT A PCI CARD)

This is how I done it, it worked fine, may not be 100%

In Win XP	Win 7

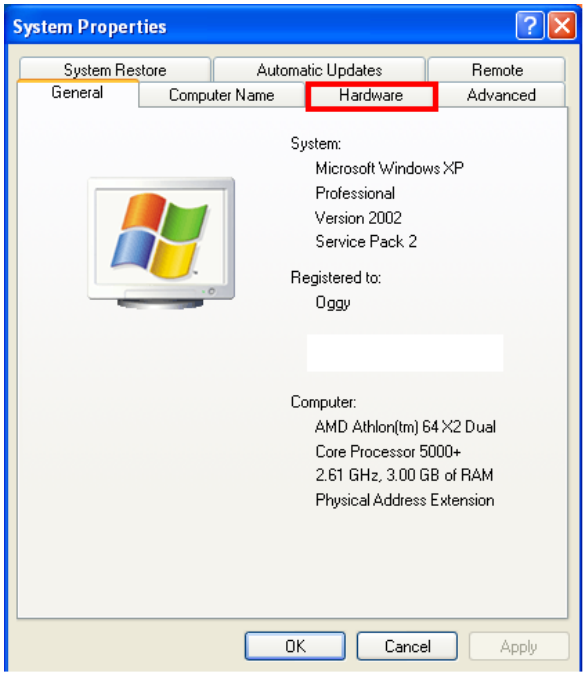
Right Click My Computer, select properties



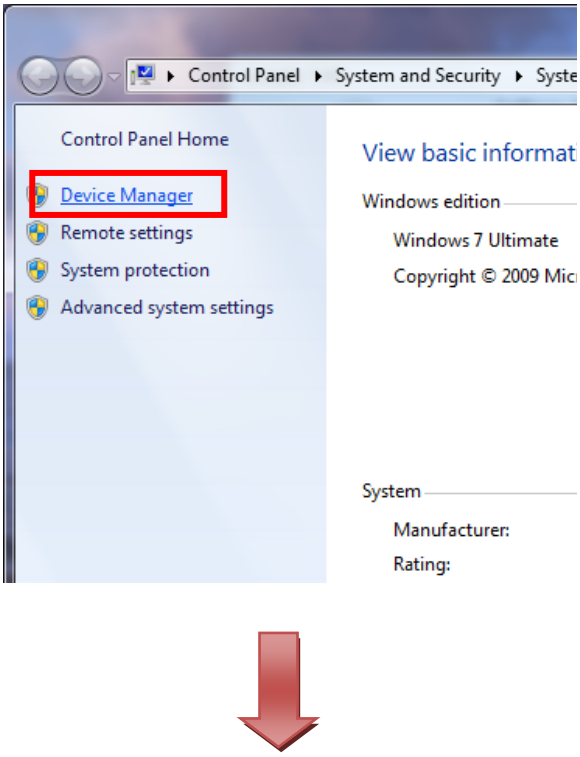


Click the “Hardware” tab

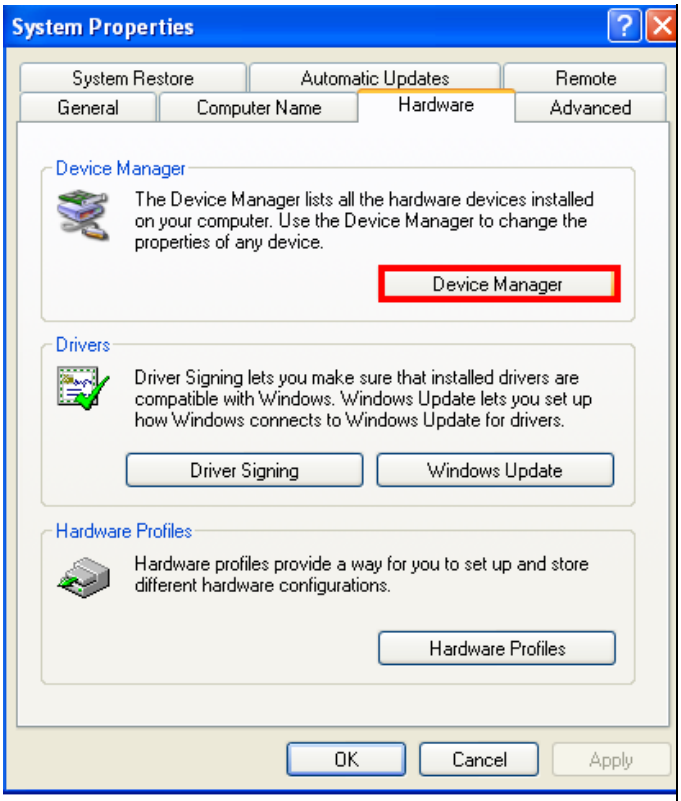
Click “Device Manager”



Then, click “Device Manager”

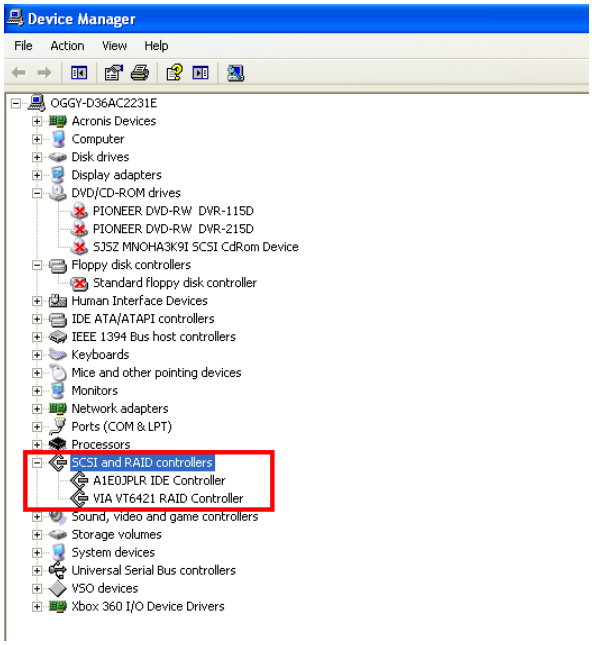


Things not going as expected? – Read the FAQ’s



BOTH OS INSTRUCTION'S NOW BECOME IDENTICAL

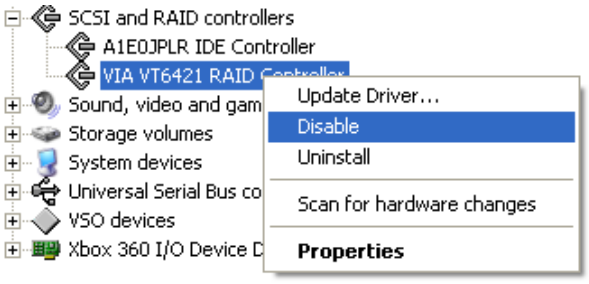
Navigate to "SCSI and RAID Controllers" and click the **+** sign to expand the list



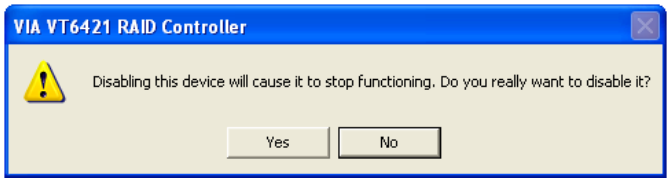
Right Click the VIA 6421 RAID Controller (may report as 3249 if using 550b drivers or above) and

Things not going as expected? – Read the FAQ's

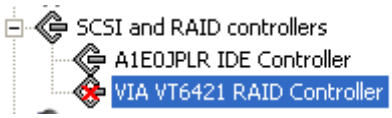
select **Disable**



Acknowledge the warning by clicking **Yes**



It should now show as disabled in Device Manager like so:



Now, to remove drivers we must navigate to where relevant file is

mine were located, and most will be: C :\WINDOWS\system32\drivers\ XXXXXXX**.sys file** –

Depending on your motherboard and OS

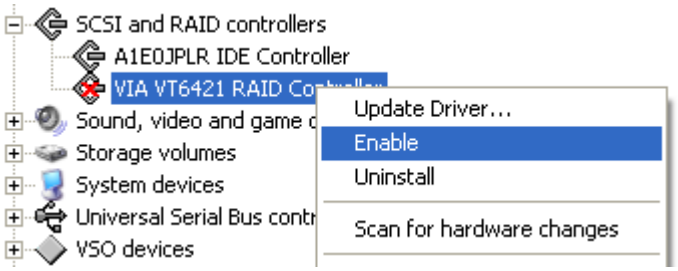
For XP normally called **viamraid.sys**
For Vista/Win 7 normally called **vsmraid.sys**
For some x64 setups it may be called **viamrx64.sys**

Once found, delete this file.

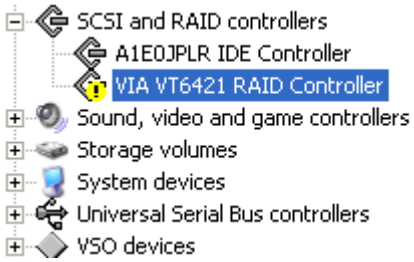
Once deleted, go back to device manager using the same steps outlined above.

Find your disabled VIA 6421 Card, right click and select enable

Things not going as expected? – Read the FAQ's



It should now show as the image below



If so, reboot your PC

Upon reboot, verify VIA 6421 still has a Yellow Exclamation Mark in Device Manager

You have successfully removed VIA drivers from your machine

CLICK HERE TO RETURN TO STARTING POINT

Manual Spoofing

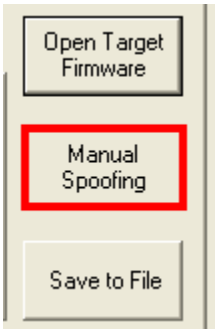
Hopefully the excellent key, OSIG and serial spoofing of FirmwareTool32 should satisfy your needs, but sometimes you need the manual method for whatever reason.

Located in FirmwareTool32

You need the firmware you wish to Spoof loaded into the target buffer

NOTE- You CANNOT SPOOF a LiteOn Drive with LT/LT+ Firmware as a DIFFERENT DRIVE.

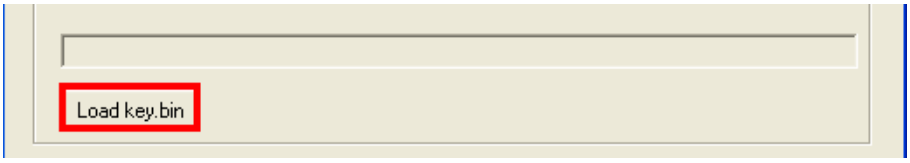
Once loaded, Click **Manual Spoofing**



Changing Drive Keys

Here you can manually type a Drive Key – It must be in Hex-Decimal format. It should **ONLY EVER** really be used if you have your Drive Key in a text file or email.

If you have a key.bin or 'Original Firmware' you can save to key.bin as shown above in the **Save key to file** section and use the **Load key.bin** option



Just click load key.bin and navigate to your key.bin file, select it then it will automatically load it into the **Manual Spoof Window.**

Changing Drives OSIG (String ID)

Simply select the drive you want your new drive to report to the console as, from the drop down list and click **OK.**

If Changing OSIG to a Lite-On PLDS DG-16D2S this will activate the Lite-On Barcode section of Manual Spoofing, please see below for instructions.

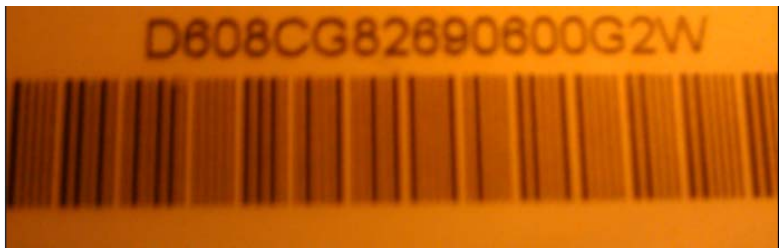
Spoofing Lite-On Barcode into Inquiry String

This is for Spoofing a drive in place of a Lite-On manually, once Drive Key is inserted, you will want to spoof as PLDS DG-16D2S, next you want to load your identify.bin by clicking **Load Inquiry.bin** and navigating to **Inquiry.bin**, upon selecting it, JungleFlasher will load it into the window, now you can click **OK** to finish spoofing the firmware.

If you don't have the **Inquiry.bin** file, JungleFlasher will let you manually type the barcode (located on the top of the Lite-On) into the cox, in the format of **17 Alpha-Numberic Characters followed by 3 spaces. You MUST include the spaces manually.**

e.g.

D608CG82690600G2W___

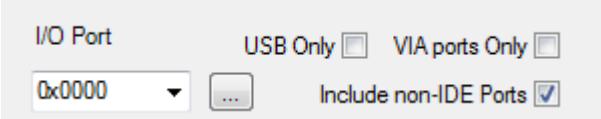


Then, click **Ok** to finish Spoofing the Firmware

CLICK HERE TO RETURN

USB Only, VIA Ports only & Include Non IDE ports

Found under **DVDKey32** tab,



USB Only

This feature allows automatic selection of the use of the new X360USB Pro from Xecuter

Checking the box unloads the PortIO Drivers too (less unnessasary stuff running!)

VIA Ports Only

This feature suits those who have quirky onboard Sata Cntrollers (SIL, JMicron) and a VIA6421 PCI Sata Card.

Checking the box removes all **non-via** sata ports, this will stop you trying to Inquire / DVDKey a drive on your non-via SATA/IDE ports. Some chipsets don't like the Inquiry and will hang the system.

****NOTE** If you do not actually have any VIA ports, JungleFlasher will itself uncheck the box and re-enable the non VIA ports**

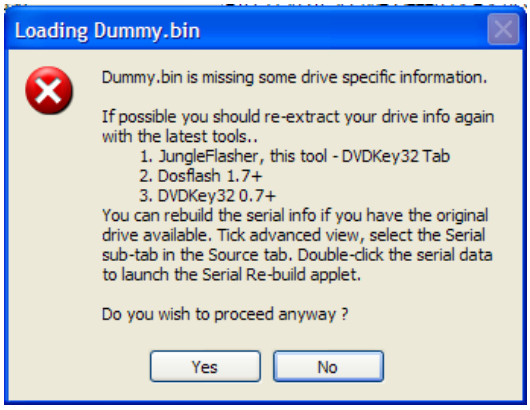
Include non-IDE Ports

This option allows you to scan port for contollers Classed as SCSIAdapter. Some newer chipset use the Class rather than hdc (aka IDE). However this will also show actual SCSI contoller which are obviously of no use for flashing. Please avoid this function unless you know what you are doing.

CLICK HERE TO RETURN

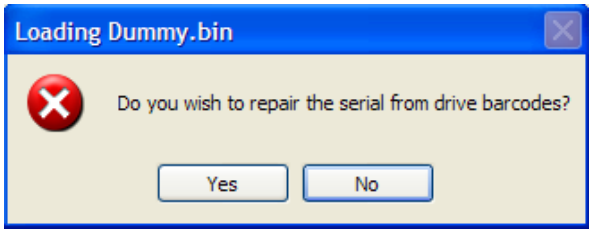
LiteOn 'Serial Fixer'

If you are prompted that serial data is missing in an error similar to this:



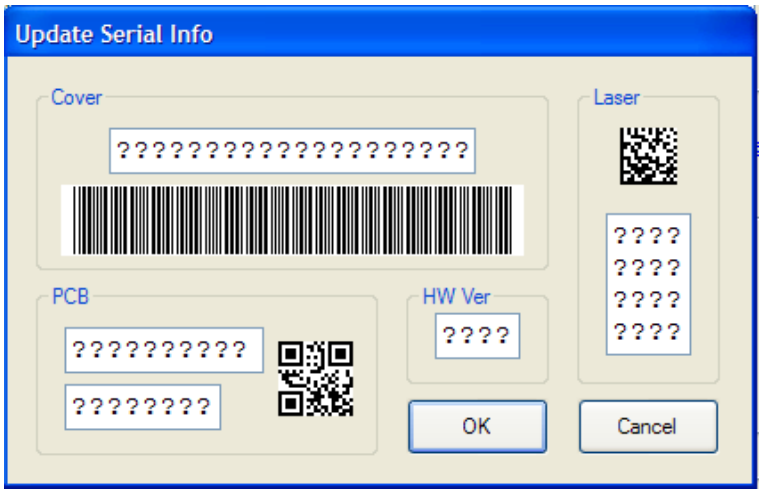
To fix proceed, click Yes.

JungleFlasher will then, ask if you wish to repair this data (only possible if you have original source liteon available).



Click yes to rebuild data.

JungleFlasher will then pop up the **Serial Rebuilder Applet**



To rebuild the **Serial Data** you must copy the information from the **physical drive itself**, into the boxes in the applet shown.

Things not going as expected? – Read the FAQ's

The data required is located in 4 places:

1. The **Drive Chassis / Shell**
2. The **Hardware Revision** of the drive
3. The **Laser**
4. The **PCB** of the drive itself

1. The Drive chassis / Shell

Located on the top of the drive, and 17 Characters long

Insert into the **cover** area on the **Serial Rebuilder**

2. Hardware Revision

Possibly the easiest of the four, located on the top sticker of the drive and usually A0A1 or A0A2

Insert this data into the **HW Ver** section of the **Serial Rebuilder**

3. The Laser

Self explanitory, located on the base of the laser.

Things not going as expected? – Read the FAQ's

Insert this into the **Laser** area of the **Serial Rebuilder**

4. The PCB of the Drive

You will need to remove the top of the Drive Case to see this data and it is sometimes obscured by pen.

The Data will start **S4P……** It's the 2nd and 3rd Line you require

Insert this data to the **PCB** section of the **Serial Rebuilder**

Once done, click Ok, and save Dummy_fixed.bin when prompted

CLICK HERE TO RETURN

Spoofing as a different type of drive

Apart from spoofing a hitachi drive(as another type), the technique is very simple!
To begin with you should have a original dump from the drive you wish to “clone”

NOTE- You CANNOT SPOOF a LiteOn Drive with LT Firmware as a DIFFERENT DRIVE

– so, you should have a pre dumped bin file from the donor drive!

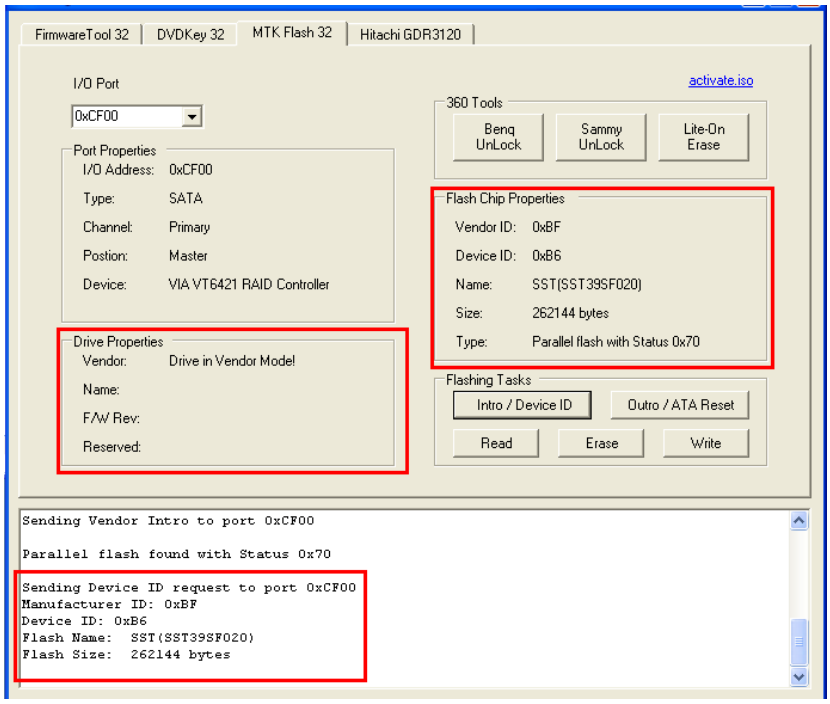
for LiteOn a Dummy.bin
for Samsung a Sam-OFW.bin
for Benq a Ben-OFW.bin
for hitachi a Hit-OFW.bin

Now follow the tutorial to unlock (follow the tut for that specific drive up to the point you would write to the drive) for whichever drive you are going to spoof as the donor drive.

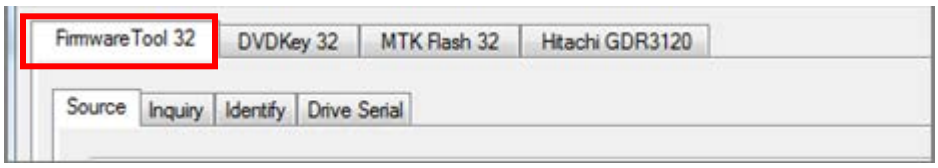
For instance you have a spare samsung drive you want to test a liteOn key with before you erase your LiteOn! (you have already dumped the drive and saved the Dummy.bin)

So you take your samsung, unlock it in accordance with the tutorial!

Which would then be in vendor mode ready to write firmware to!



Now go to **firmwaretool 32** tab

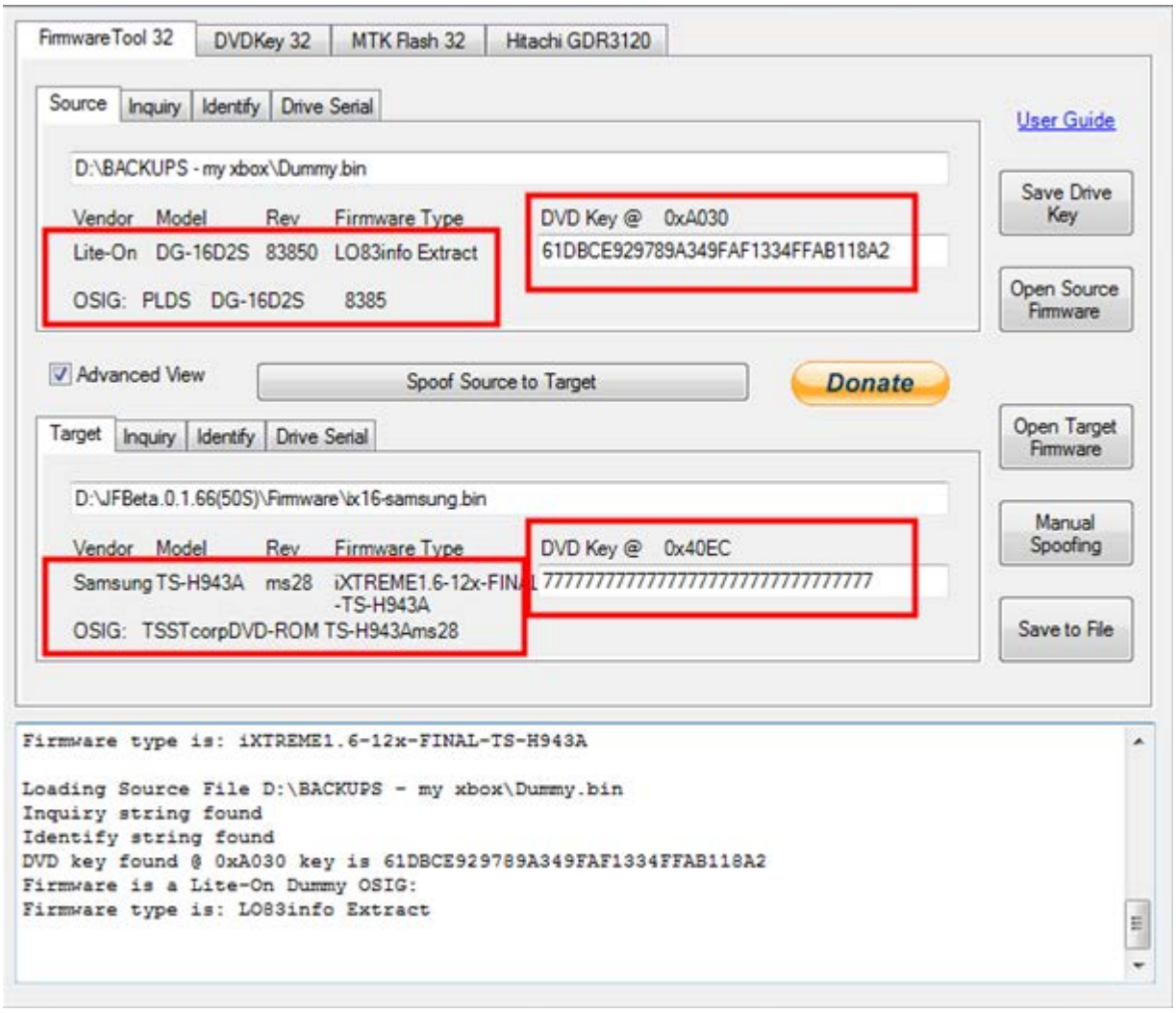


Load your dummy.bin as source –

decline any auto load ix messages!

Load target firmware – (you are about to flash a samsung so choose ix firmware for a samsung drive)

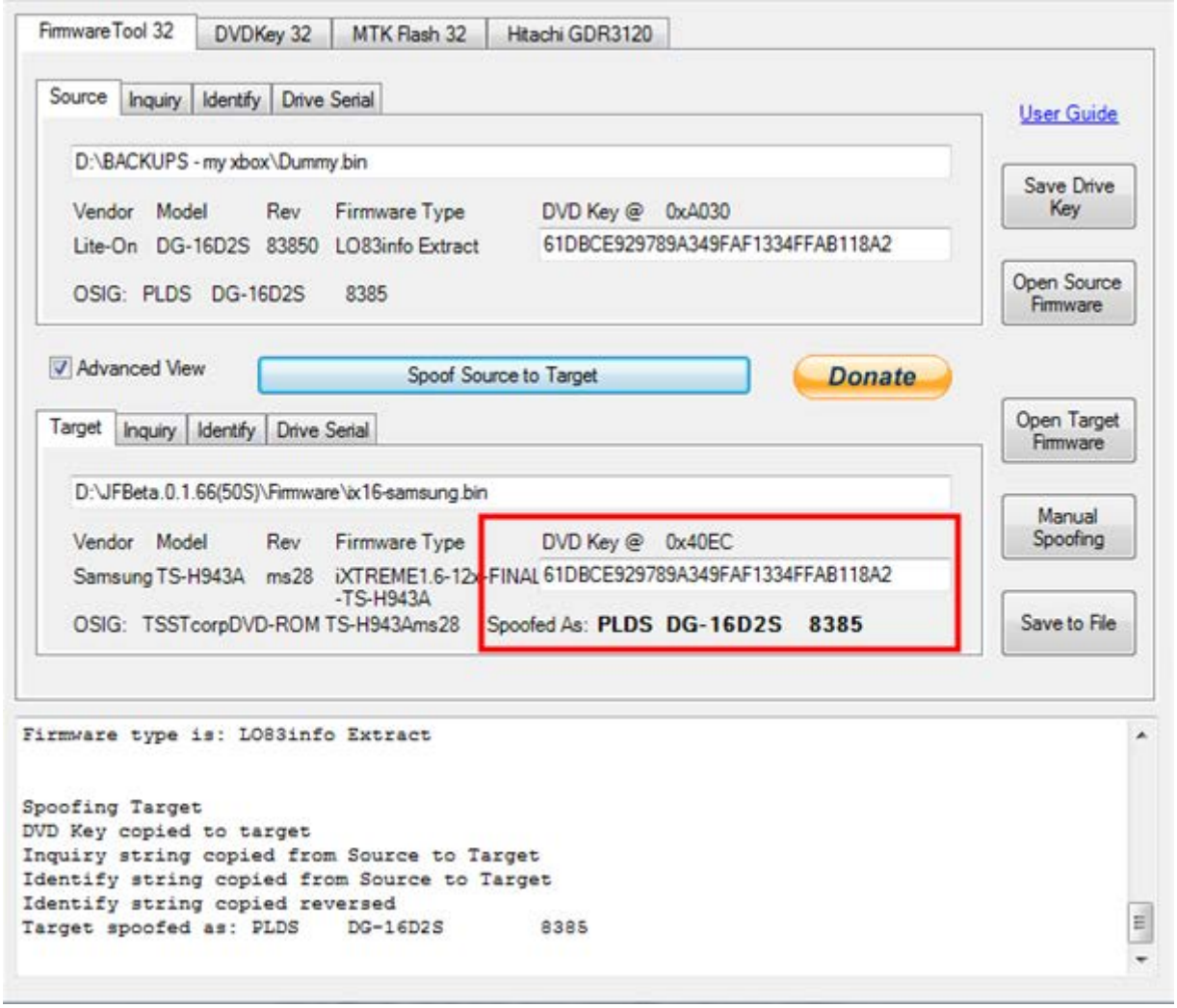
Things not going as expected? – Read the FAQ's



Now click **Spoof Source to Target**!

Notice the difference in the target firmware now!

Things not going as expected? – Read the FAQ's



Then all you have to do is Write to the drive the same way as you would for that type of drive! In a samsungs case – click **Write** when on the **MTK** tab!

The same method applies to all drives apart from Hitachi which is covered **HERE**

CLICK HERE TO RETURN

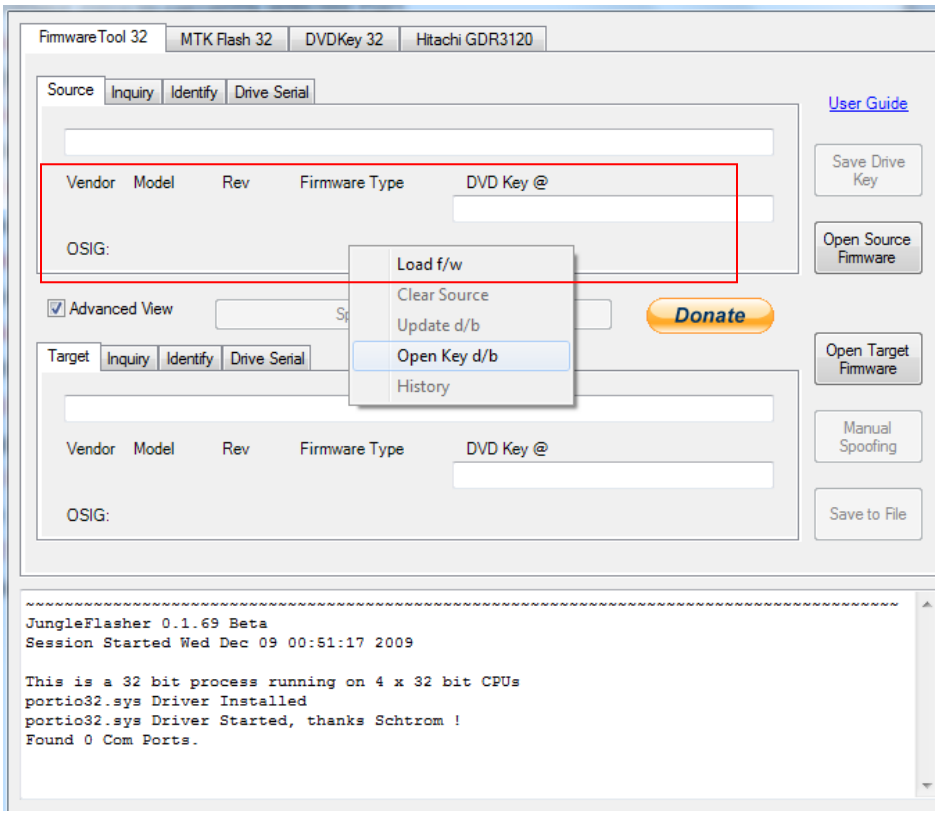
Advanced User Info

Advanced Ctrl+Fkey Functions

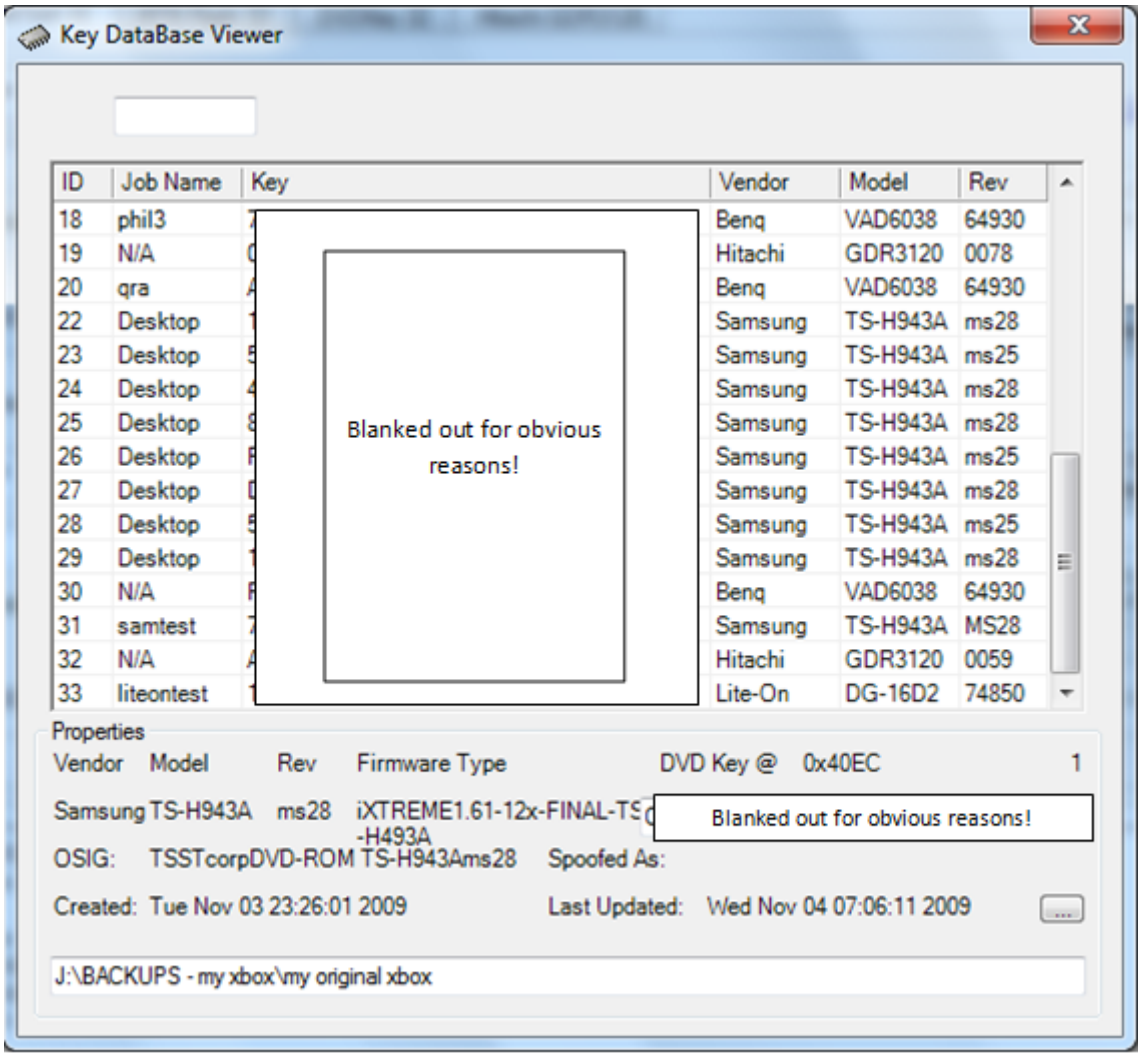
Ctrl + F1 key,
Enable context menus
Ctrl + F2 key,
Disable context menus
Ctrl+ F3 key
To Send Vendor Intro to currently selected Port
Ctrl + F4 key
To open iXtreme from firmware folder to Target
Ctrl + F5 key,
Set Modder mode backup directory, clear folder to disable it
Ctrl + F6 key,
Hitachi read block size 100 --> 2000 (78 and 79 FK models will fail on this)
Ctrl + F7 key,
Set working folder in Modder mode... clear all tabs and save log
Ctrl + F8 key,
Enable Hitachi Expert Mode!
Ctrl + F10 key
To add/update key database from Source tab info
Ctrl+ F11 key
To create .csv from key database
Ctrl + F12 key
To open key database in Notepad

Key Database

For those who have NOT saved their dumped file and need their key details back.
Try right clicking on source box and select **Open Key d/b.**



Things not going as expected? – Read the FAQ's



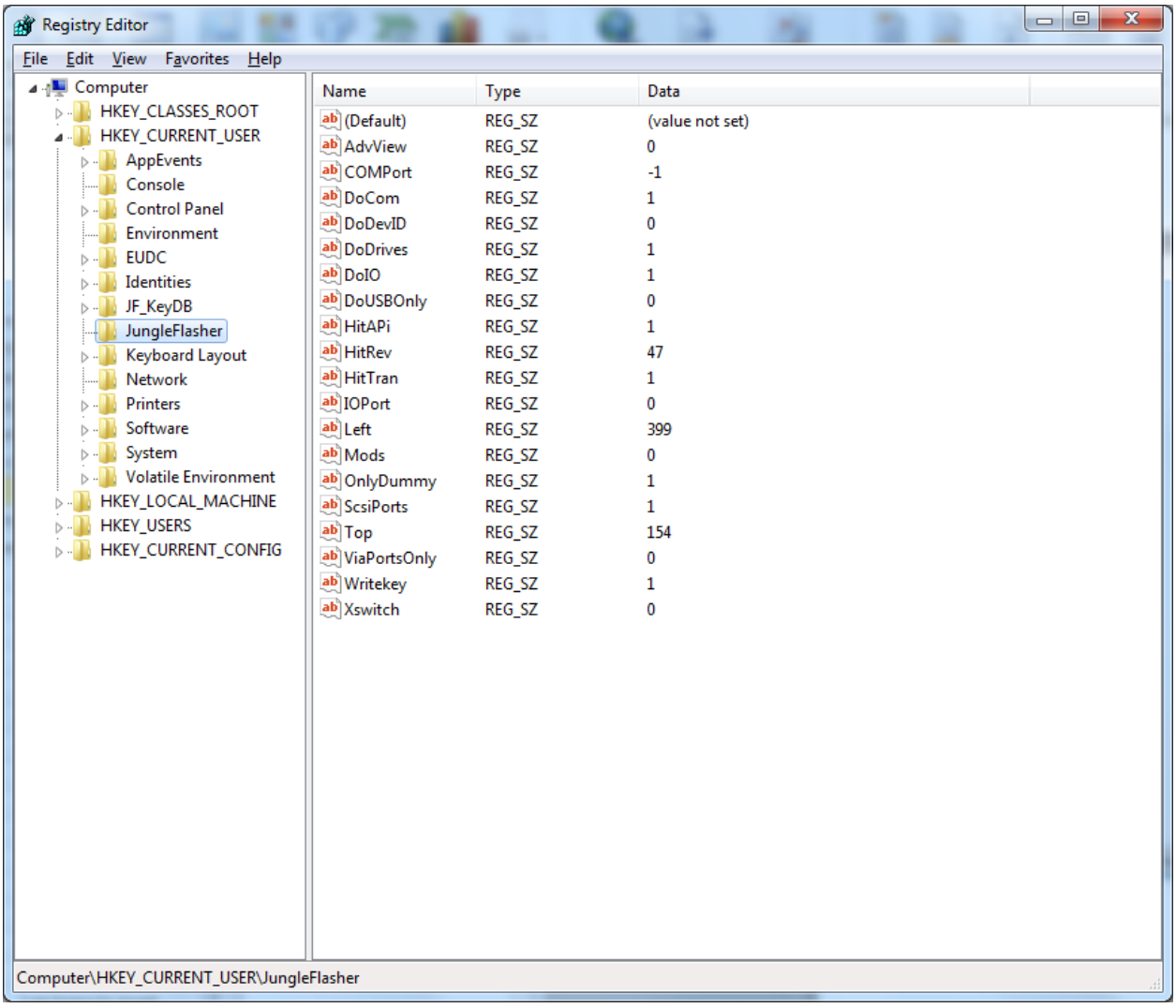
Things not going as expected? – Read the FAQ's

Registry Settings

Only really for troubleshooting and debugging and should only be attempted by those confident enough to play about in the systems registry settings

Click **Start**, click **run,** type **regedit** and press **enter**
Navigate to **HKEY_CURRENT_USER**
Click on **JungleFlasher**

You will see something similar to this:



Things not going as expected? – Read the FAQ's

- **Adview -** Remembers whether **Advanced View** was selected or not
- **BackupFolder –** Contains the location set for backup folder for modder mode (blanked if modder mode not set
- **COMPort -** Remembers last COM Port selected, number represents position in drop down menu
- **Delay32 –** timed delay between clicking dvdkey32 and running the command, to allow time to probe r707 (milli-seconds)
- **DoCom -** Enumerates comports, for debug use only
- **DoDevID –** Will send Intro if drive reports as in **Vendor Mode**
- **DoDrives -** Enumerates drive letters, for debug use only
- **DoIO -** Enumerates I / O ports, for debug use only
- **DoUSBOnly –** Selects USB only option
- **HitAPi –** Remembers if WinAPi is selected (1 yes, 0 no)
- **HitRev –** Remembers last drive revision selection
- **HitTran -** Remembers last Tranfer Method selection
- **IOPort -** Remembers last IO Port selected, number represents position in drop down menu
- **Left -** Remembers postion of JungleFlasher window (left hand side)
- **Mods –** Counter for CTRL + F7 operations
- **OnlyDummy –** Remembers if Dummy.bin only is enabled
- **ScsiPorts -** enumerate SCSIAdapter IO ports also (NON-IDE)
- **Top -** Remembers postion of JungleFlasher window (Top
- **ViaPortsOnly -** enumerate only Via IO ports, for safety (Value 1) Lists all if removed or Value 0
- **WriteKey –** Allows the ability to write the key Only from context menu
- **Xswitch –** Remembers if USBxtractor switch is enabled

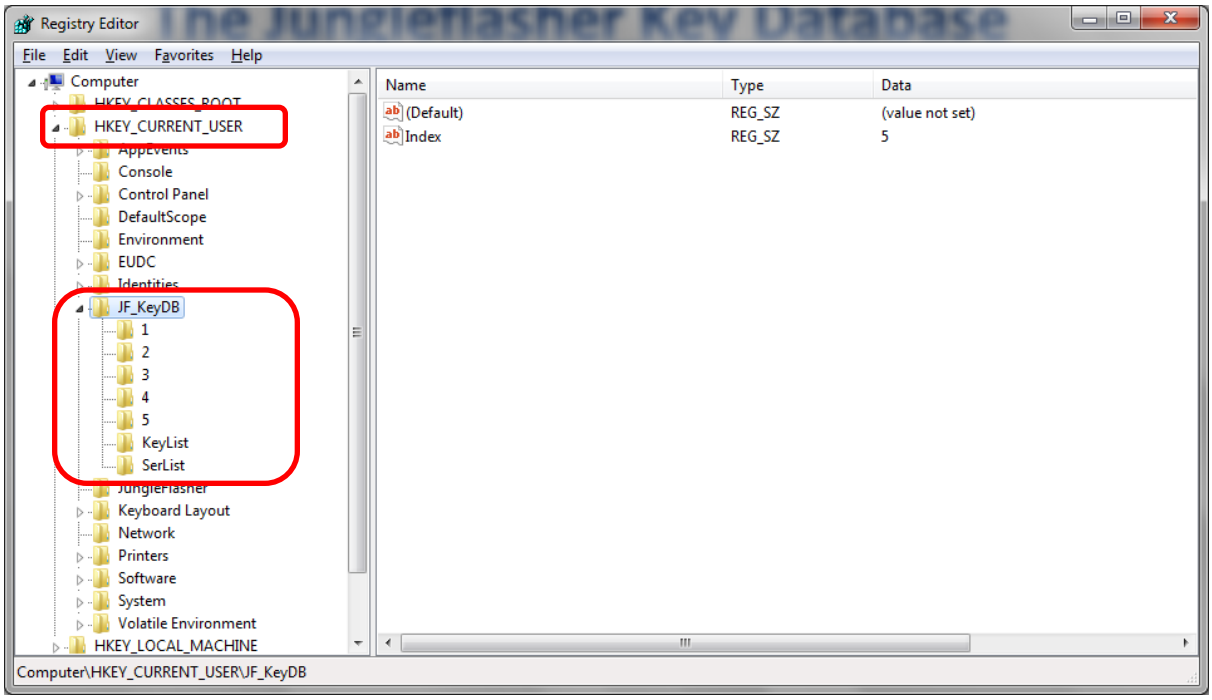
In addition to the above registry settings – The key database is also stored in registry!

The Jungleflasher Key Database

So you know about the all-important KEY? The one that every tutorial about xbox360 drive flashing tells you to SAVE, WRITE DOWN, EMAIL IT TO YOURSELF!

Well the exceedingly clever guys from Jungleflasher have been helping you out with this since version 0.1.74. Yet somehow very few people know about this fantastic addition.

The JF (JungleFlasher) key database (dB) is a store of all (locally) dumped keys whilst using JF on that particular PC. This dB is only kept on the PC the keys are dumped on. The dB itself is held within your pc's registry (shown below)



To see the information shown above you simply run "Regedit" from the "Run line" in start menu, and then select HKEY_CURRENT_USER

"What does the JF KeydB do for me?"

1. Automatically saves every key dumped using JF
2. Allows you to search the KeydB for a working key for any drive you attach

3. Will create a dummy.bin from the info in the KeydB if it verifies a key against a drive.
4. Gives you piece of mind – you lost the original dump, it'll be in the dB!

In Short! – If you used JF to dump a drive on the same PC, re-flashing the drive becomes incredibly easy! (No need to MRA LiteOn drives more than once!) You no longer need to have a complex way to track all the drives you flashed to be able to locate original firmwares.

How do I take advantage of this phenomenal feature?

CLICK HERE TO RETURN

PMT Probe (Non-Cap) or CK Probe 3

The PMT Probe is designed to be able to allow you to dump the Key from ALL Phat LiteOn without resorting to MRA .

This method works regardless of current FW on the drive.

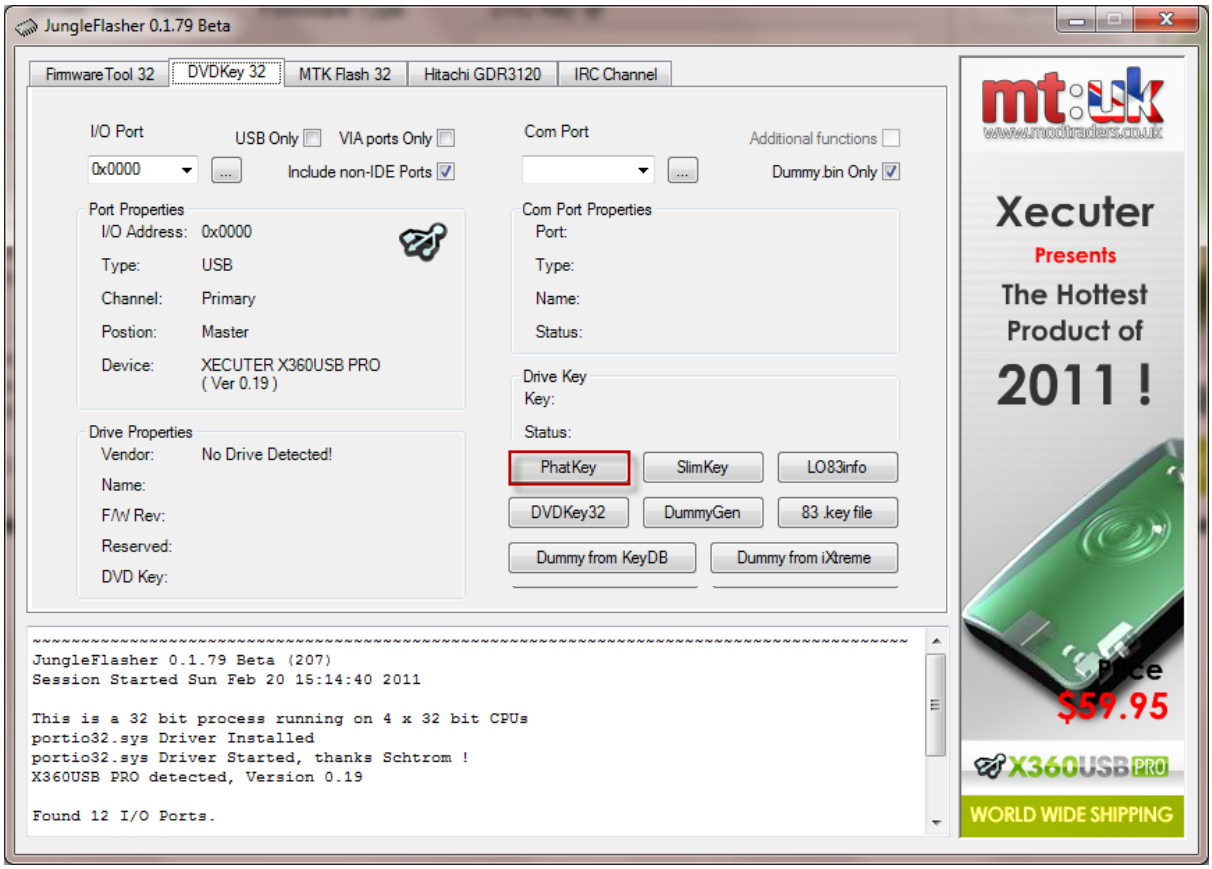
In the following example – I use the X360USB Pro for my SATA connection

– This is NOT a pre-requisite –

If you have a currently working SATA setup – it will work just as well

So select your I/O port as Normal

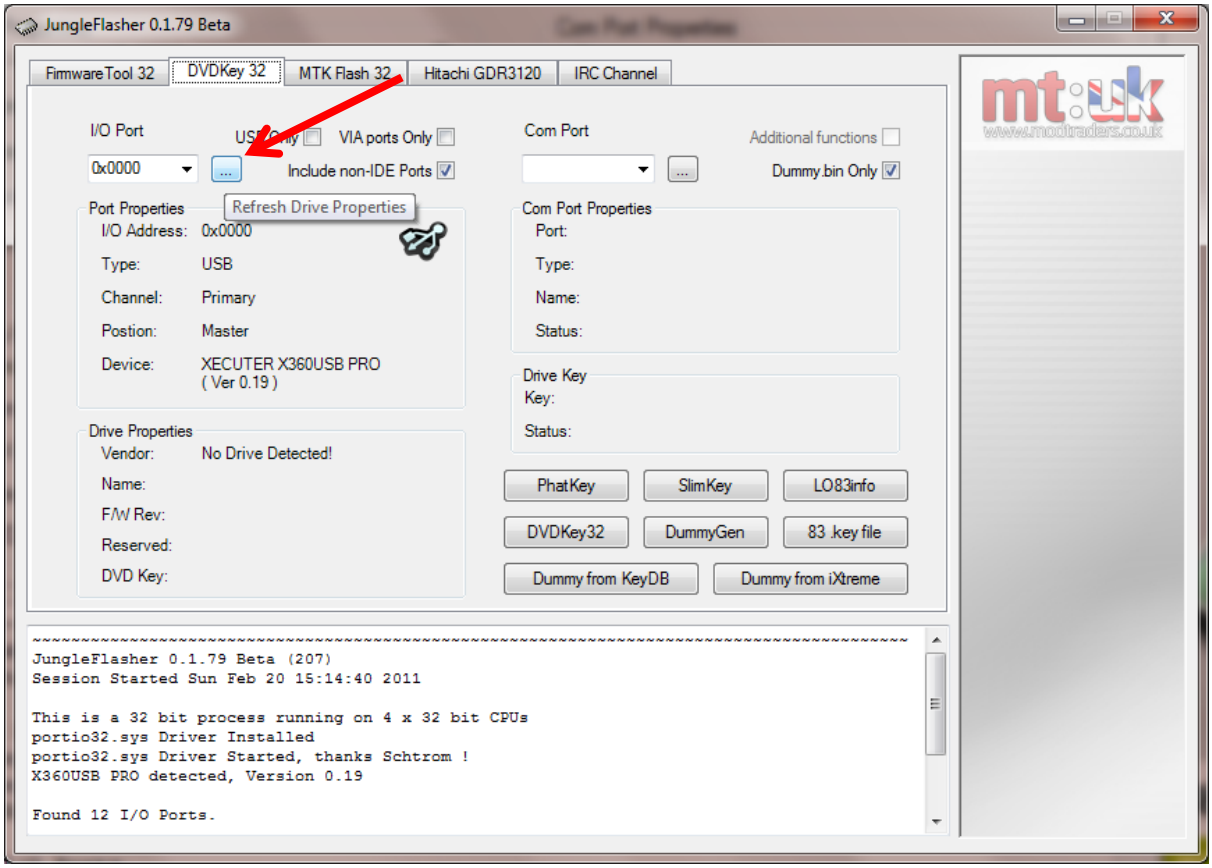
You will notice a new Button “PhatKey”



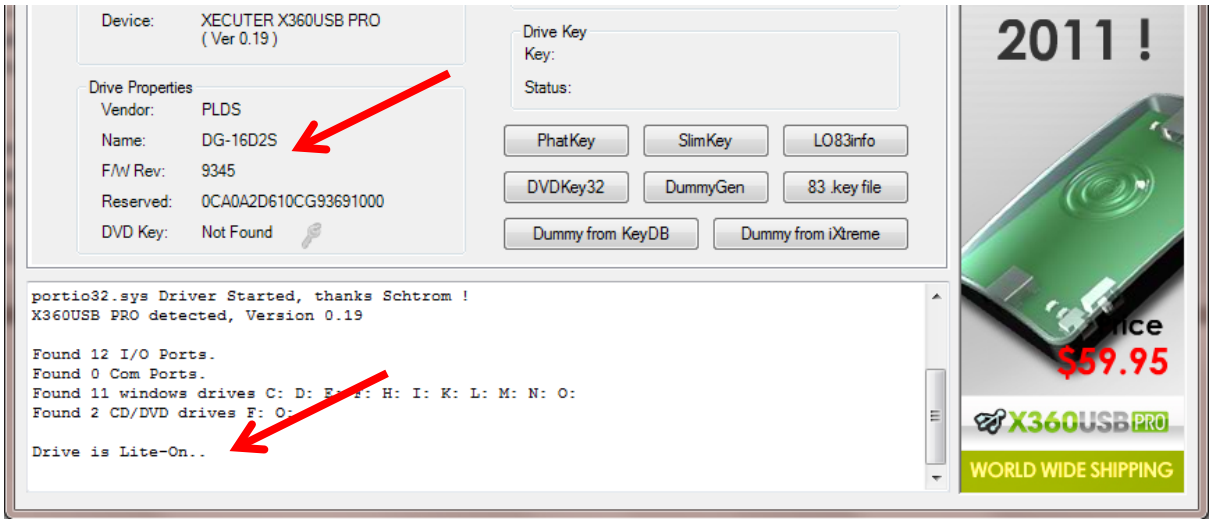
Things not going as expected? – Read the FAQ’s

Using the PMT

With drive powered on and showing in drive properties, click refresh ([…])

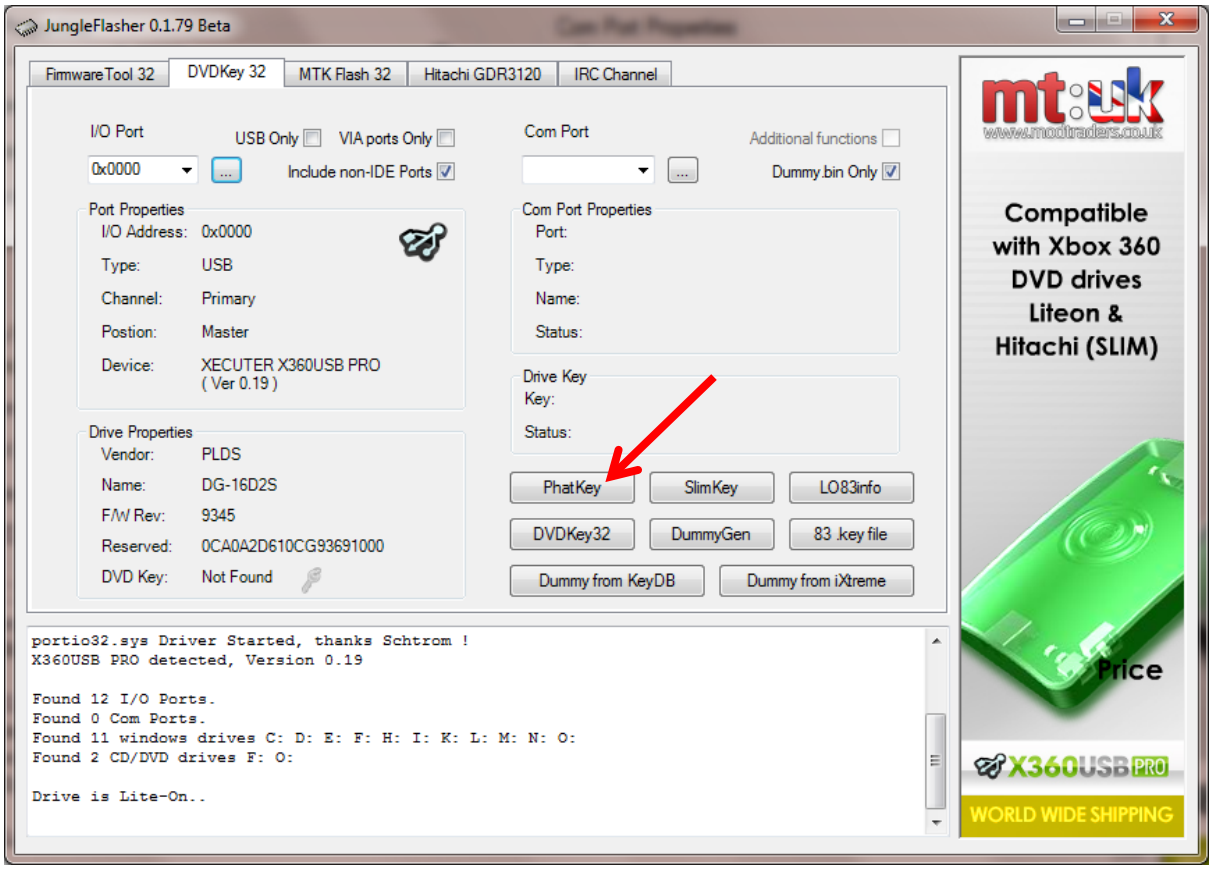


Notice the drive being identified!

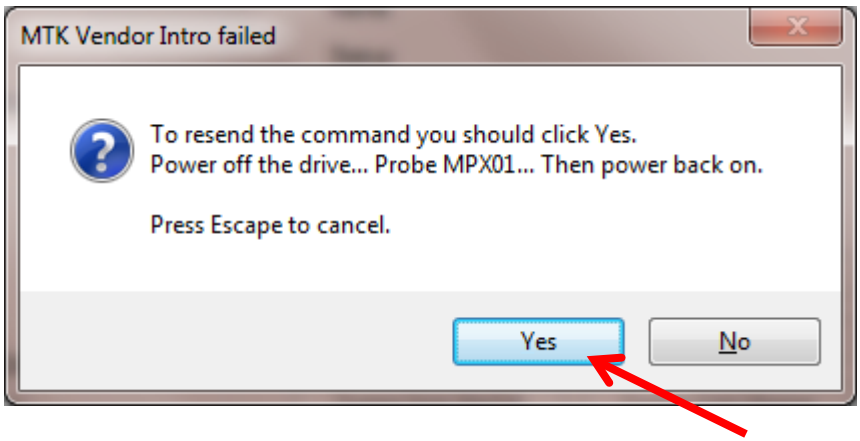


Things not going as expected? – Read the [FAQ's]

Now press the “PhatKey” Button



The following message will appear

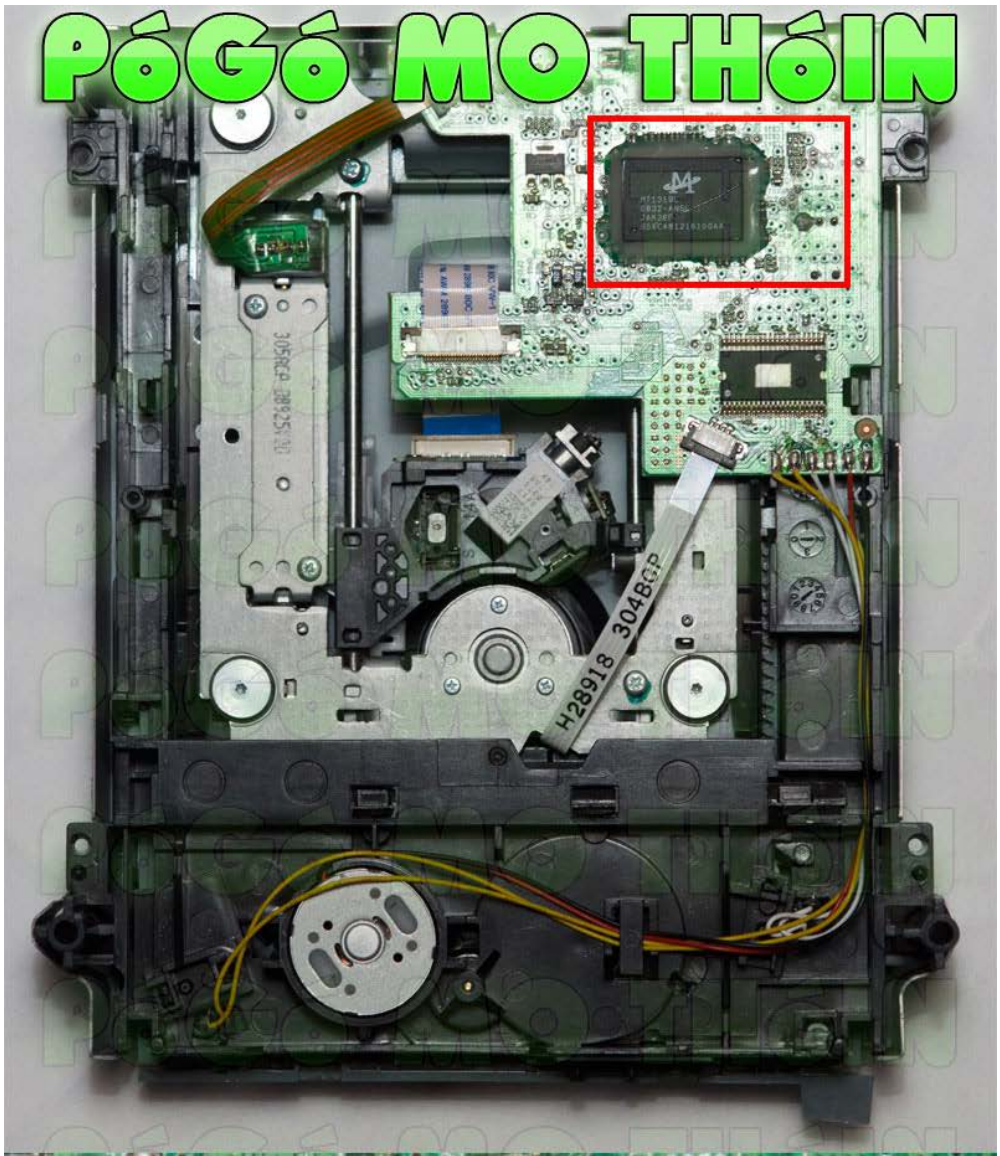


Please read this carefully. Then click **YES**

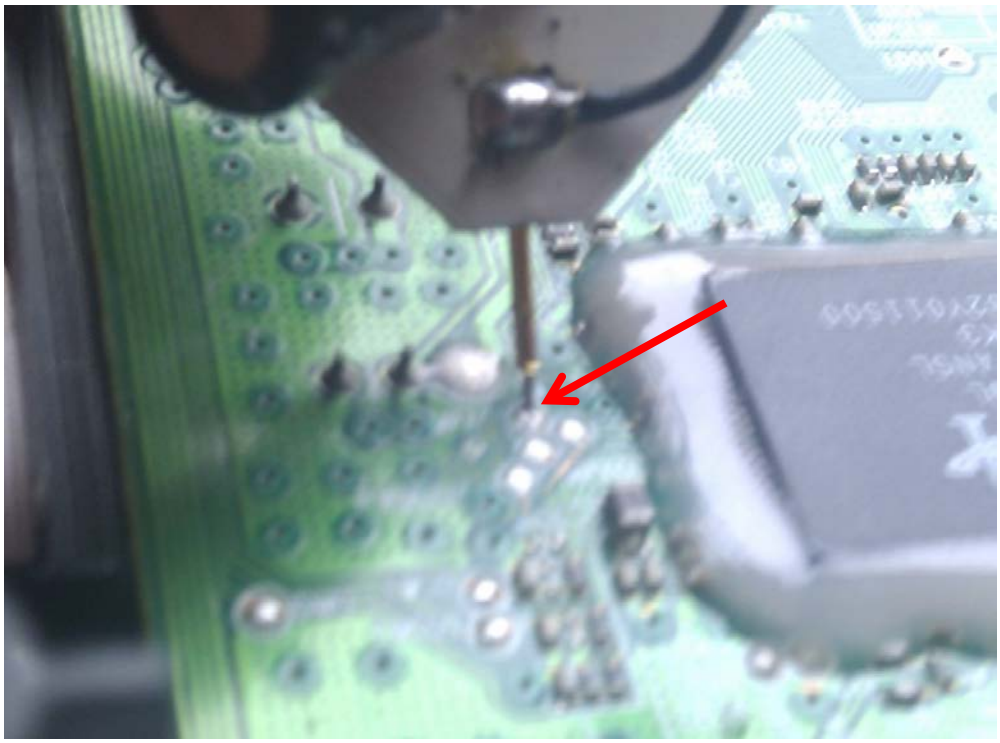
Switch 3.3v inline switch **OFF**

Probe the point **MPX01 (shown below)**

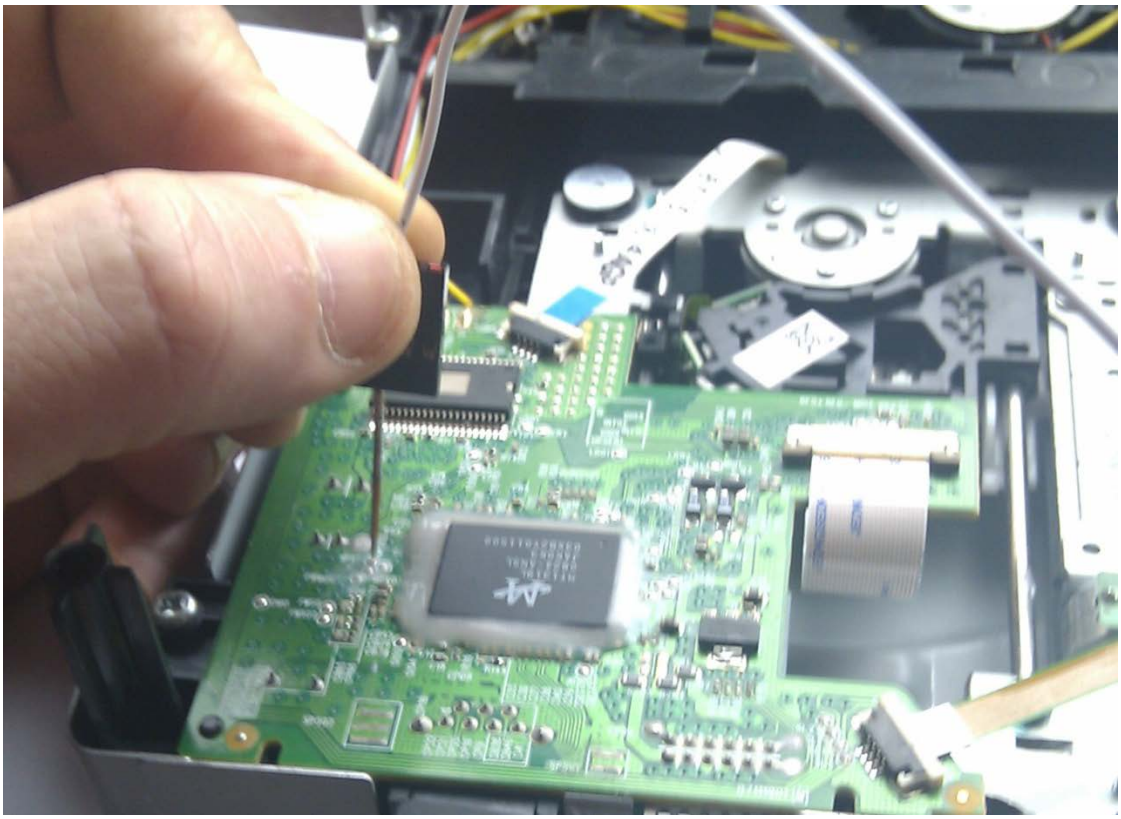
Things not going as expected? – Read the FAQ’s



Things not going as expected? – Read the [FAQ's]



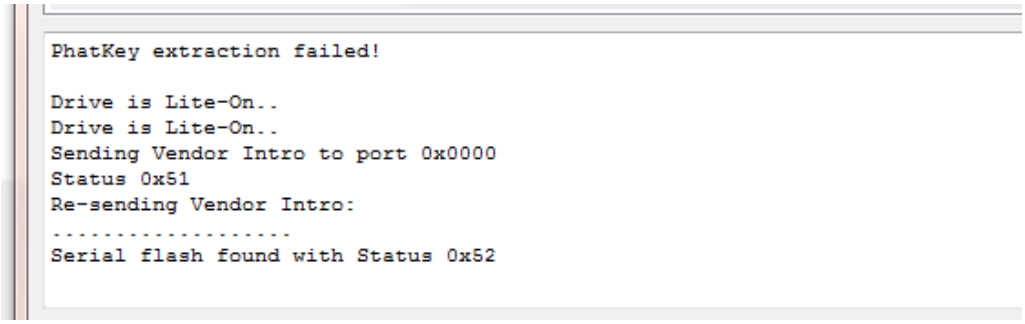
or



Things not going as expected? – Read the FAQ's

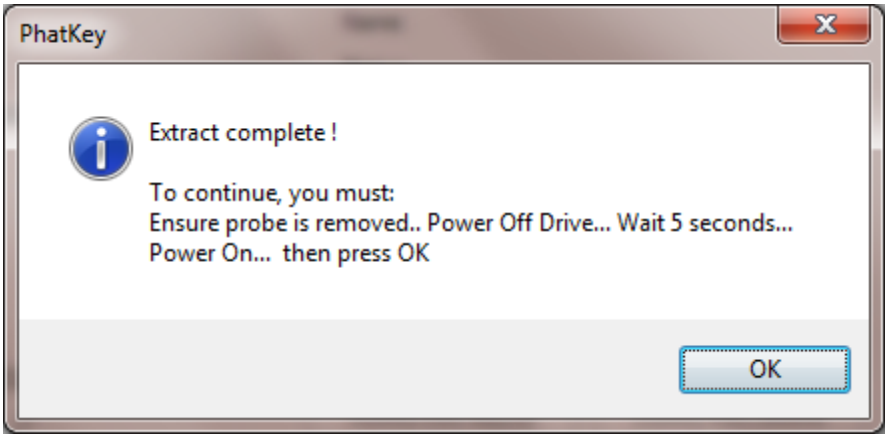
Switch 3.3v inline switch **ON** again

This message should appear in log window



As soon as you see status 0x52 appear – lift the probe off from the point

Within a few seconds this should appear



Again read it carefully, (note: the 5 sec timing not required)

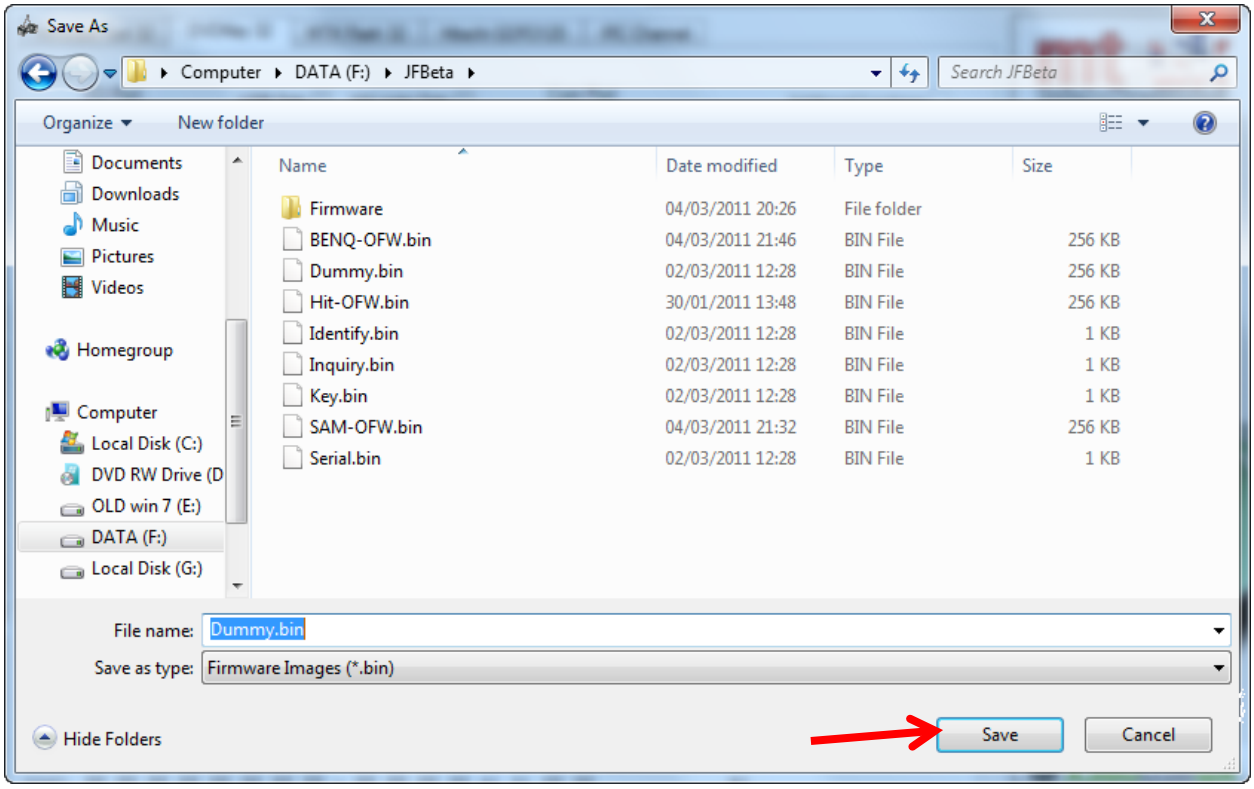
Switch 3.3v switch **OFF** then **ON** again.

Then Press "**OK**"

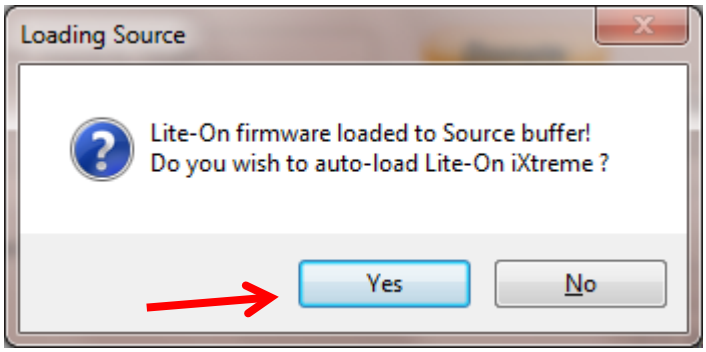
IF all has gone well

You will see the save box appear to save your Dummy.bin

Click “SAVE”



Then you will be presented with the question to auto-load the iXtreme FW

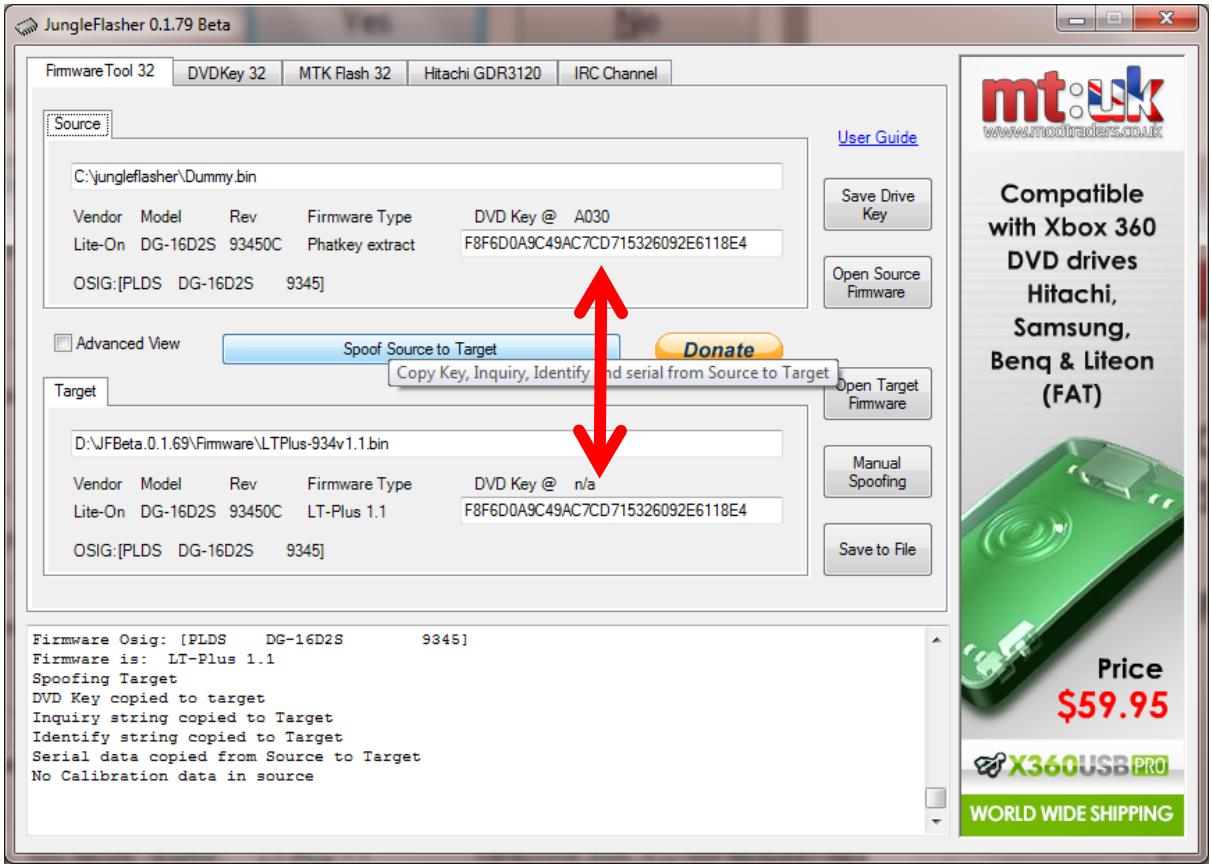


If this is what you wish to do click “YES”

This will as normal take you to the Firmware Tool 32 tab, with your Dummy.bin loaded as source and the target Firmware loaded and spoofed with your drives details.

From here the Jungleflasher procedure is identical to the previous versions

Ensure the 2 keys match each other – then proceed to erase and write your drive.



[CLICK TO CONTINUE TO ERASE & WRITE SECTION]

PMT Probe (with capacitor)

The PMT Probe is designed to be able to allow you to dump the Key from ALL Phat LiteOn without resorting to MRA .

This method works regardless of current FW on the drive.

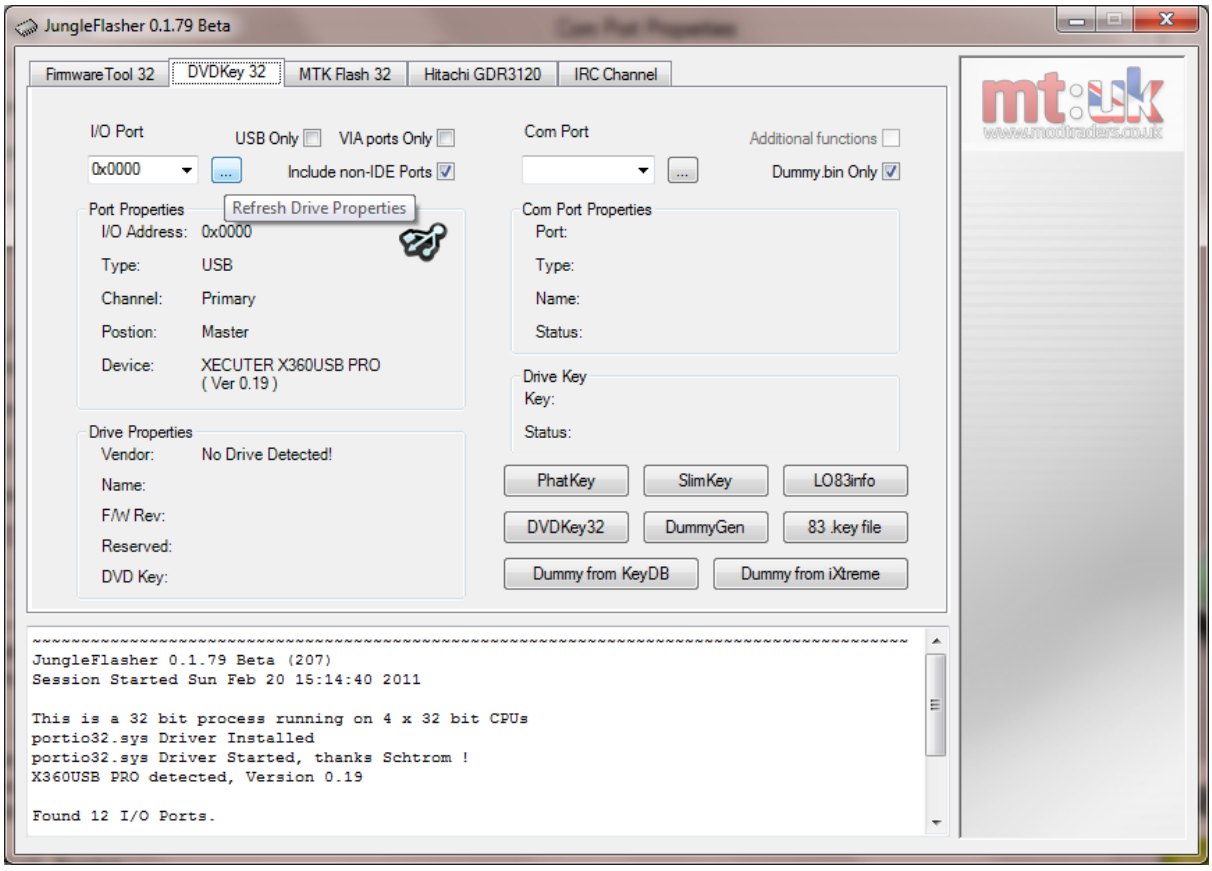
In the following example – I use the X360USB Pro for my SATA connection

– This is NOT a pre-requisite –

If you have a currently working SATA setup – it will work just as well

So select your I/O port as Normal

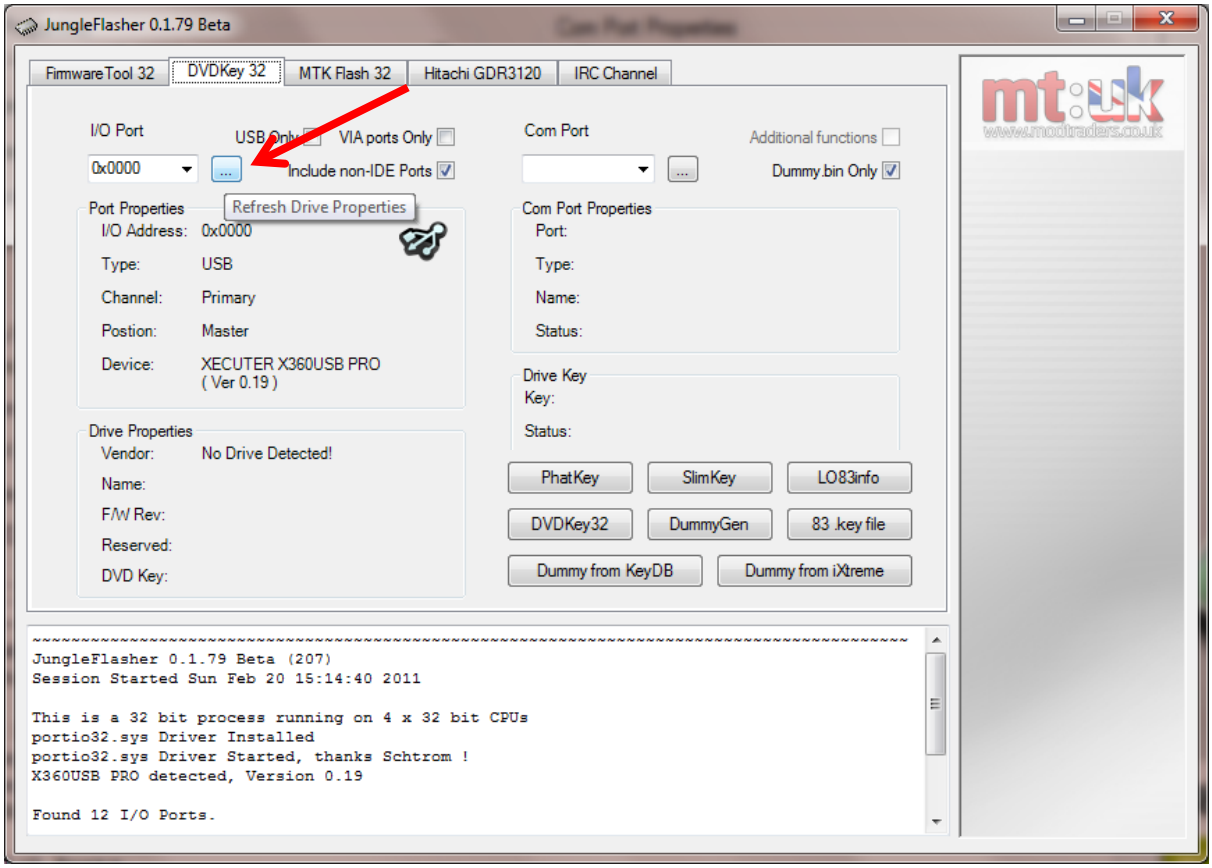
You will notice a new Button “PhatKey”



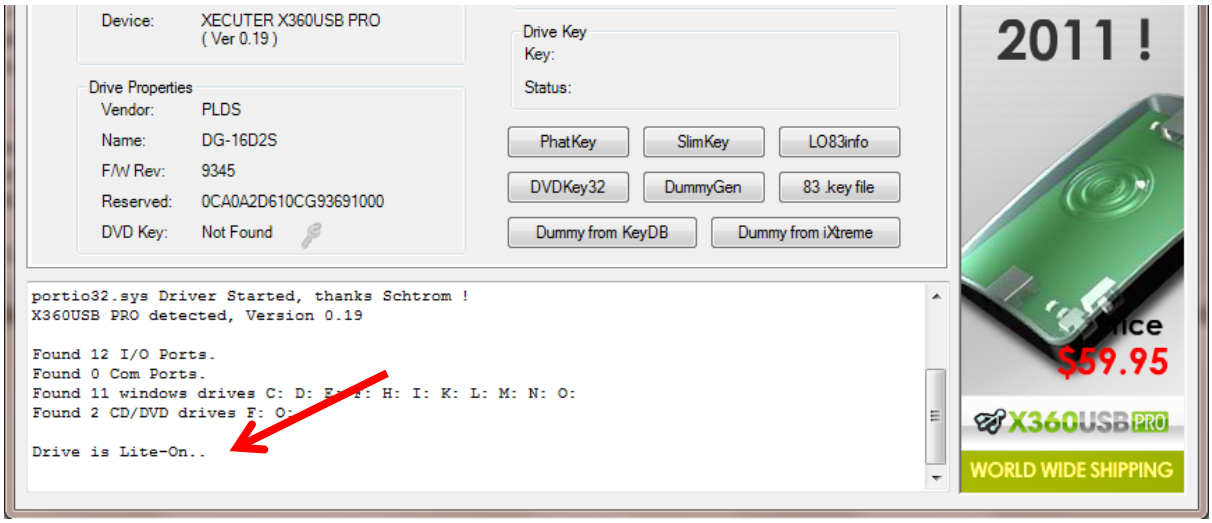
Things not going as expected? – Read the FAQ’s

Using the PMT

With drive powered on and showing in drive properties, click refresh ([…])

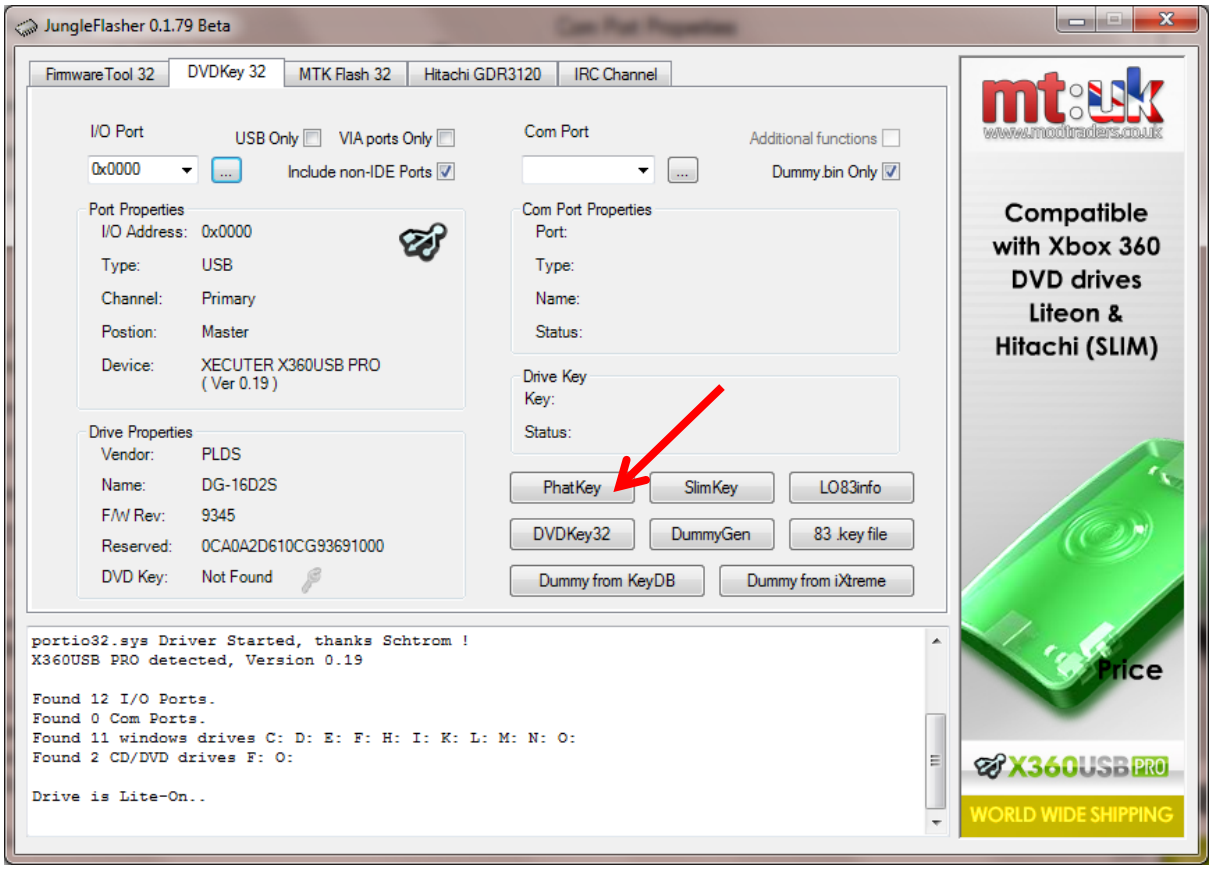


Notice the drive being identified!

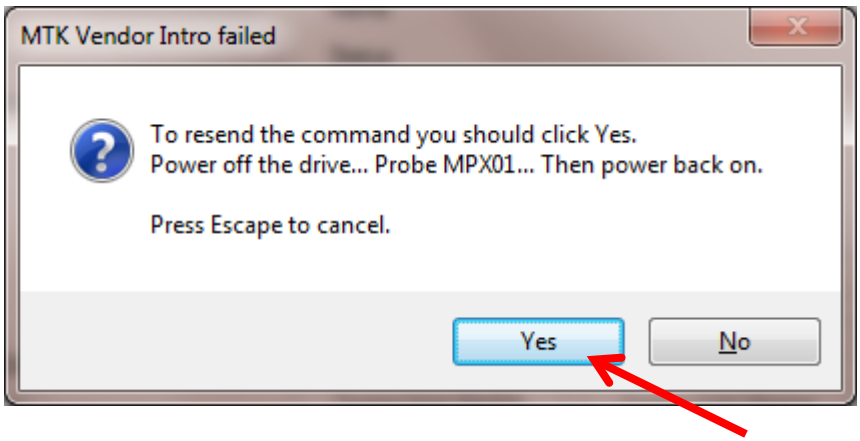


Things not going as expected? – Read the [FAQ's]

Now press the "**PhatKey**" Button



The following message will appear

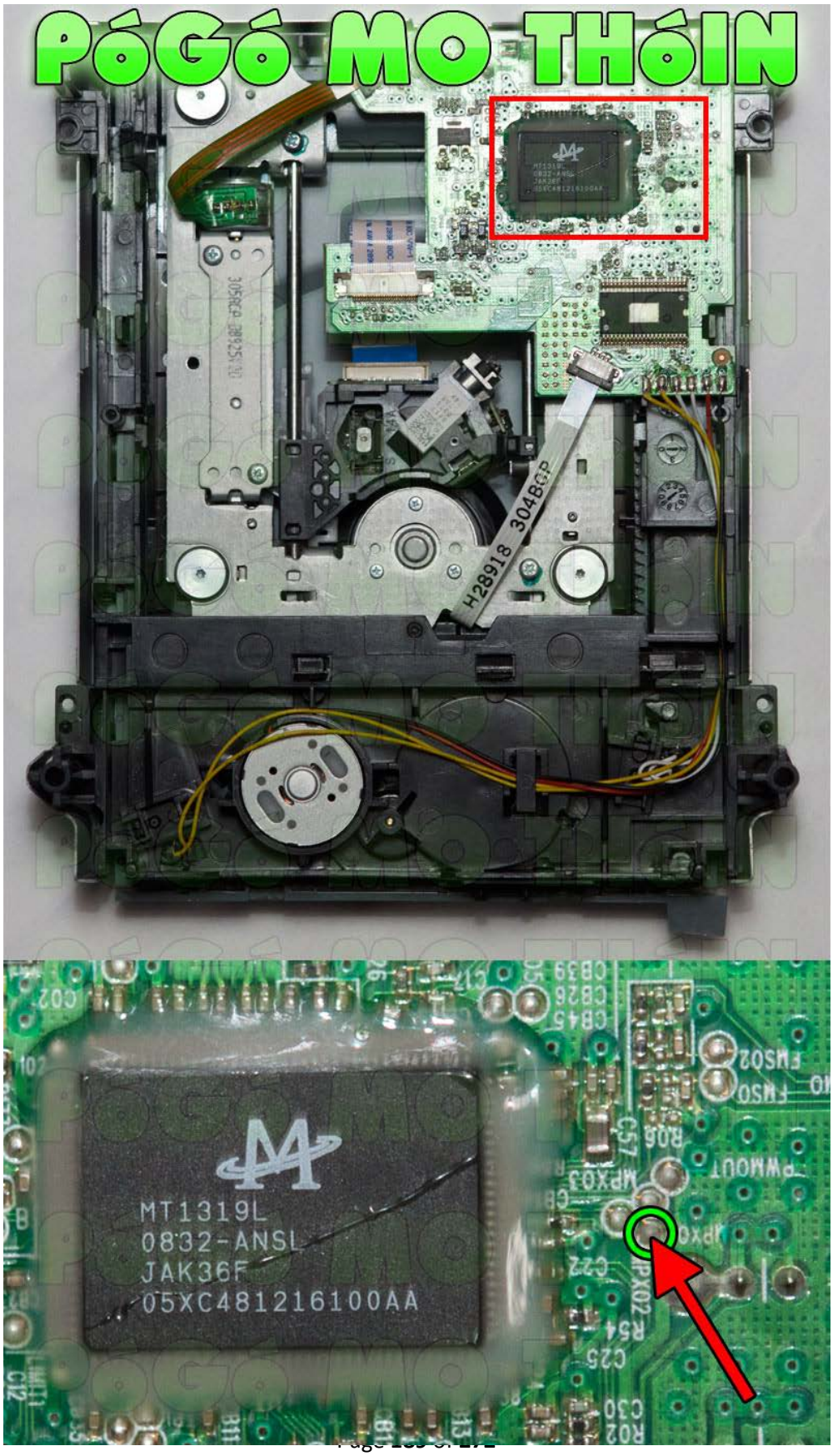


Please read this carefully. Then click **YES**

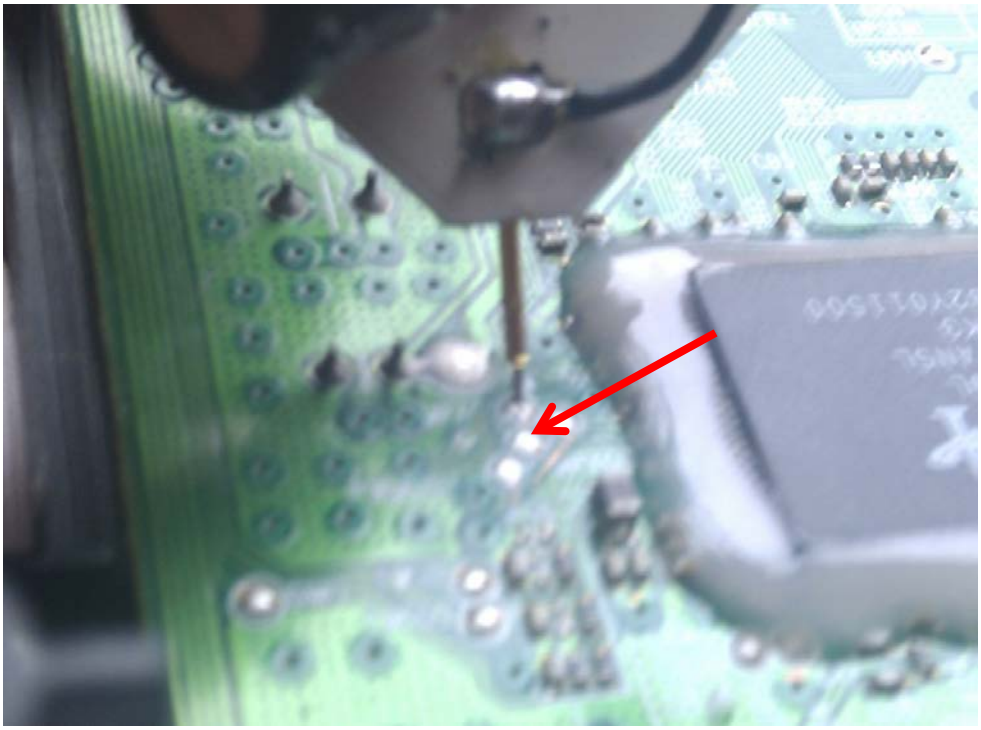
Switch drive power **OFF**

Probe the point **MPX01** (shown below)

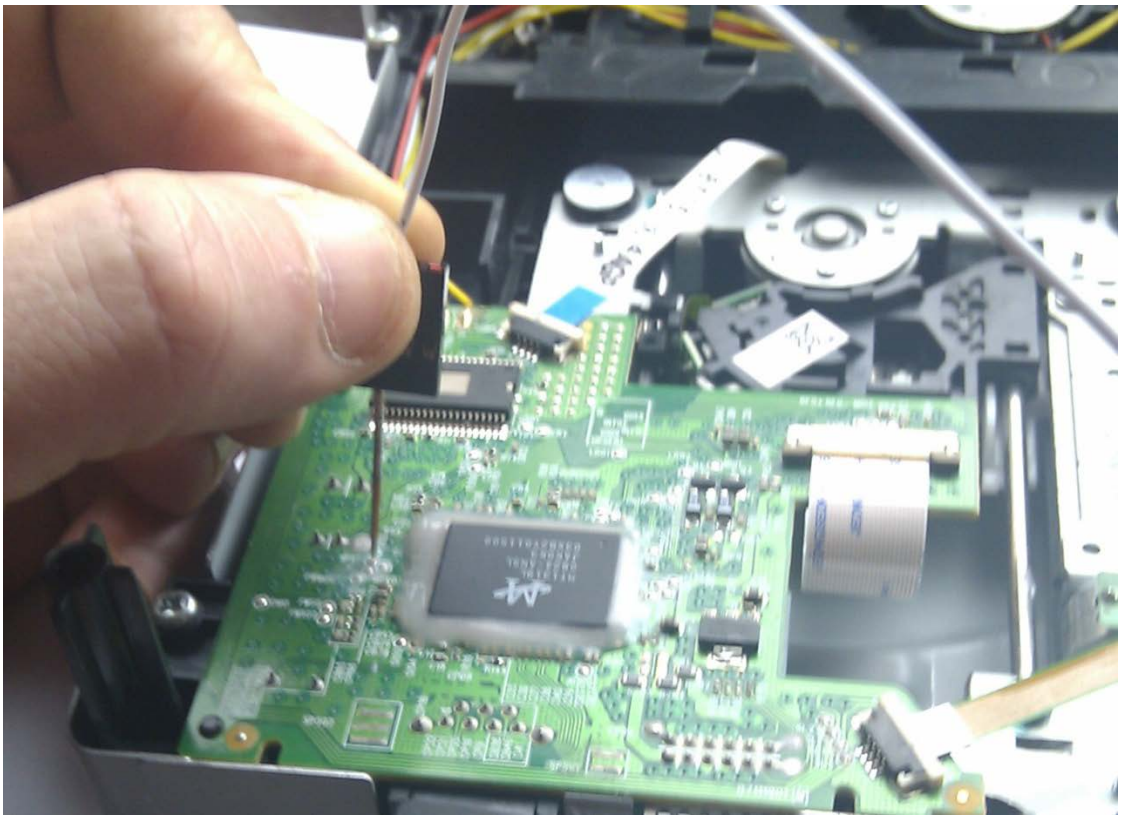
Things not going as expected? – Read the FAQ's



Things not going as expected? – Read the [FAQ's]



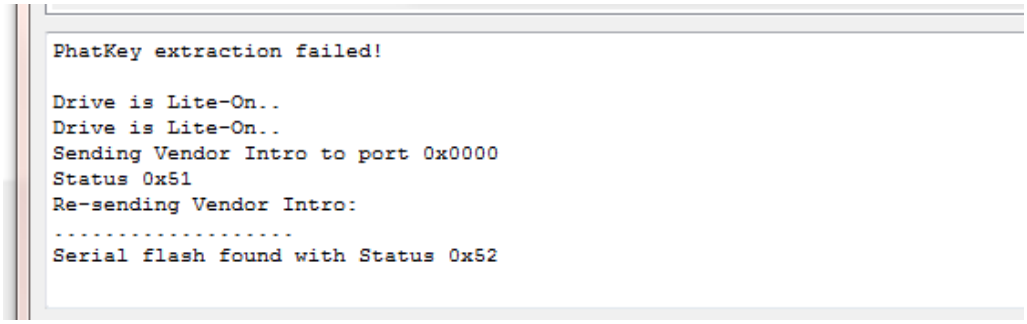
Or



Things not going as expected? – Read the FAQ's

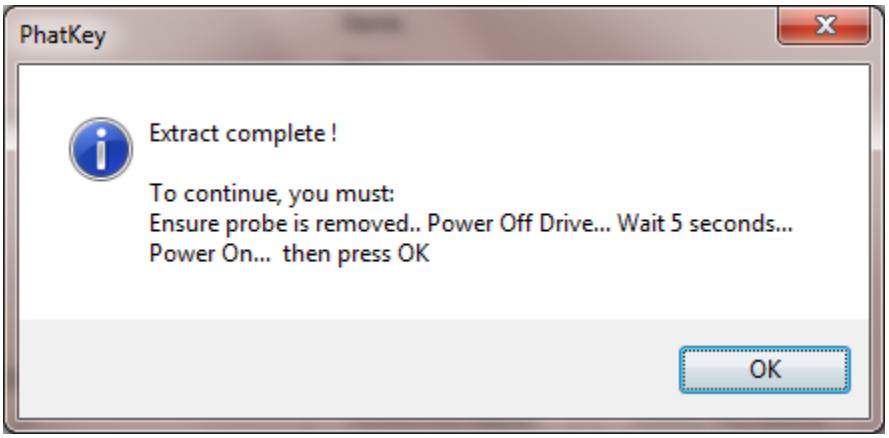
Switch Drive Power **ON** again

This message should appear in log window



As soon as you see status 0x52 appear **– lift the probe off from the point**

Within a few seconds this should appear



Again read it carefully,

Switch drive power **OFF**

Wait 5 seconds

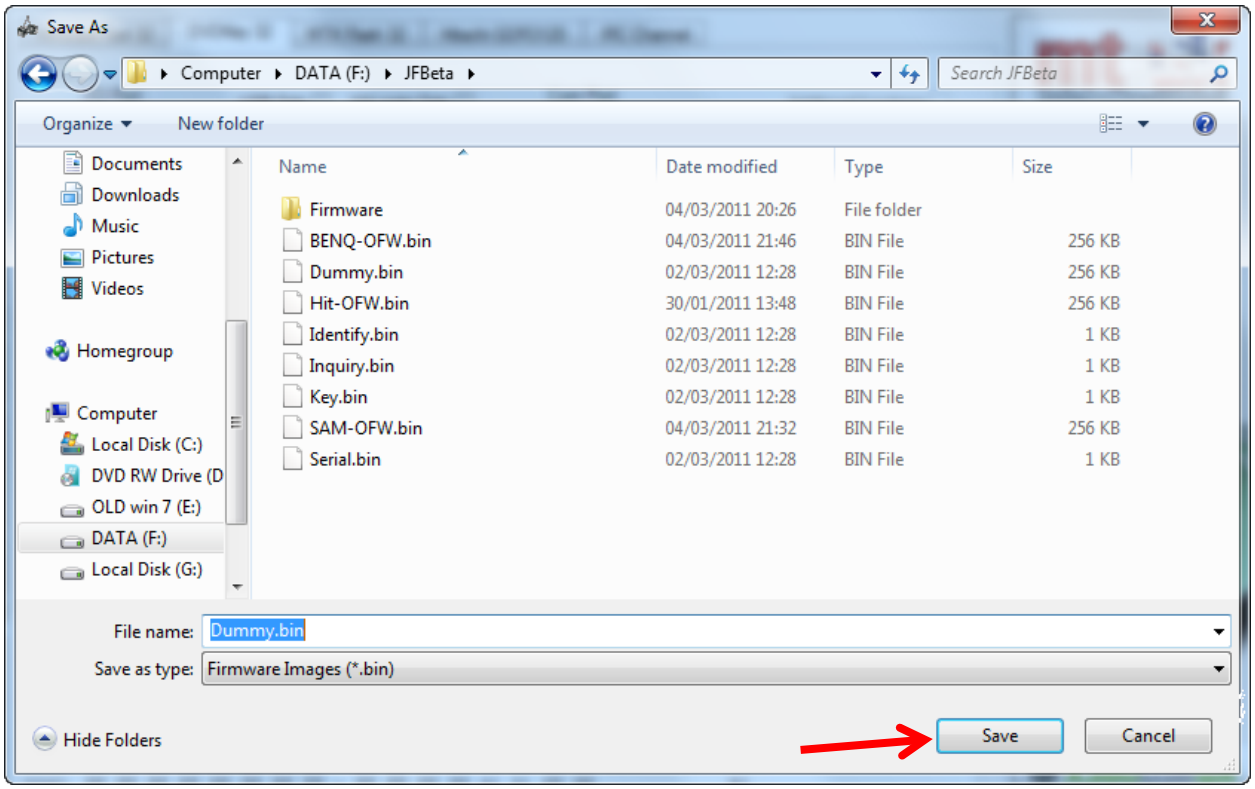
Switch drive power back **ON**

Then Press "**OK**"

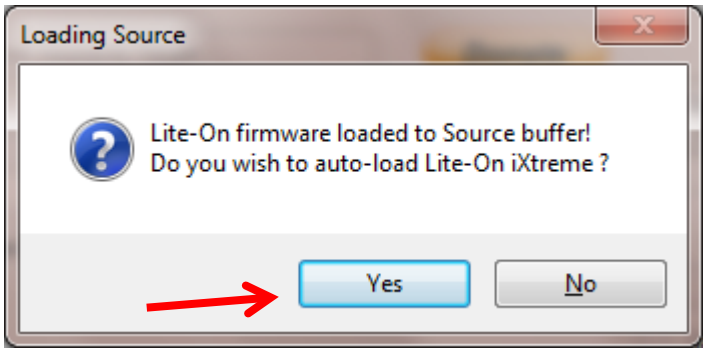
IF all has gone well

You will see the save box appear to save your Dummy.bin

Click “SAVE”



Then you will be presented with the question to auto-load the iXtreme FW



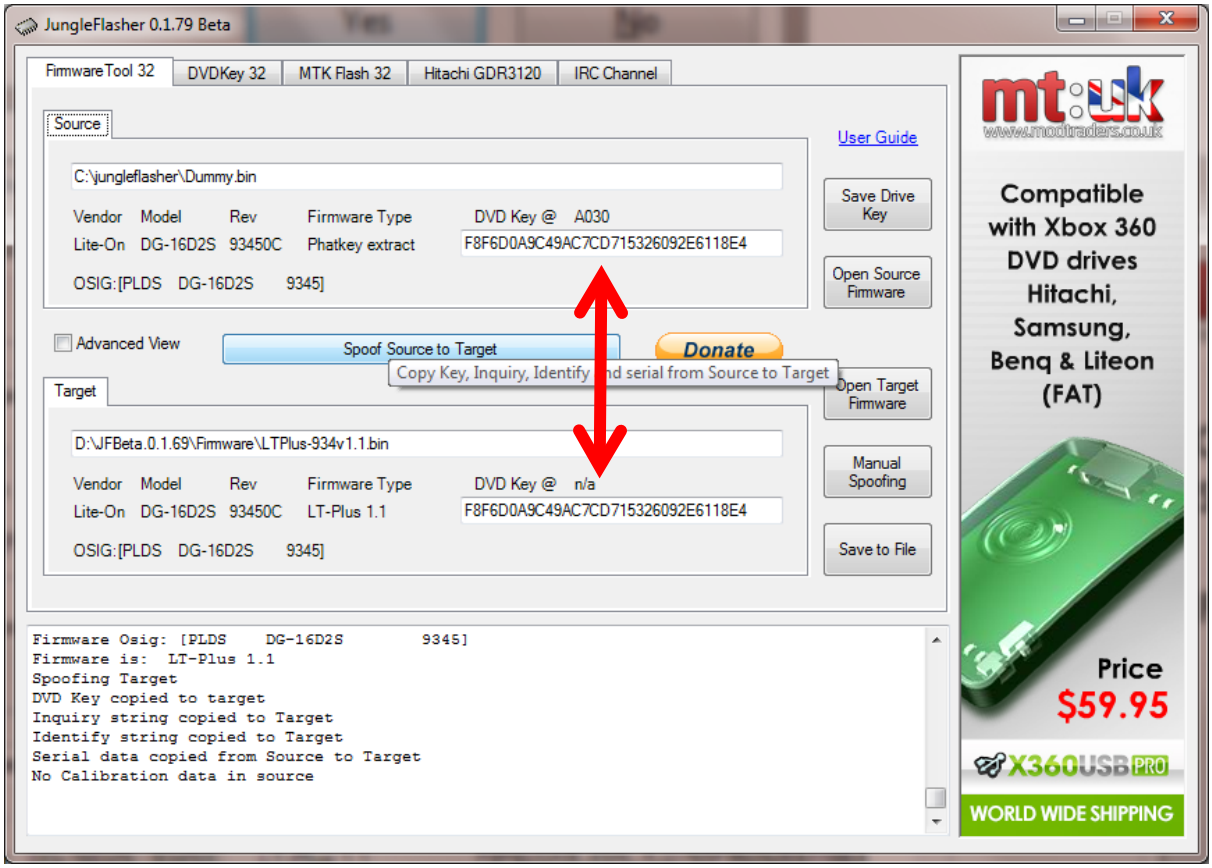
If this is what you wish to do click “YES”

Things not going as expected? – Read the FAQ’s

This will as normal take you to the Firmware Tool 32 tab, with your Dummy.bin loaded as source and the target Firmware loaded and spoofed with your drives details.

From here the Jungleflasher procedure is identical to the previous versions

Ensure the 2 keys match each other – then proceed to erase and write your drive.



[CLICK TO CONTINUE TO ERASE & WRITE SECTION]

Things not going as expected? – Read the [FAQ's]

Badflash Recovery Using X360USB Pro of Samsung, BenQ & LiteOn Drives.

This method is to recover from those horrible moments (when something has gone wrong during flashing/erasing procedure. You know the ones – You forgotten to plug in AV cable and your Xbox powered off (even though we told you not to use Xbox for power) or your child has stood on a power cable and yanked it out the wall, you forgot to pay the electricity and have been cut off!

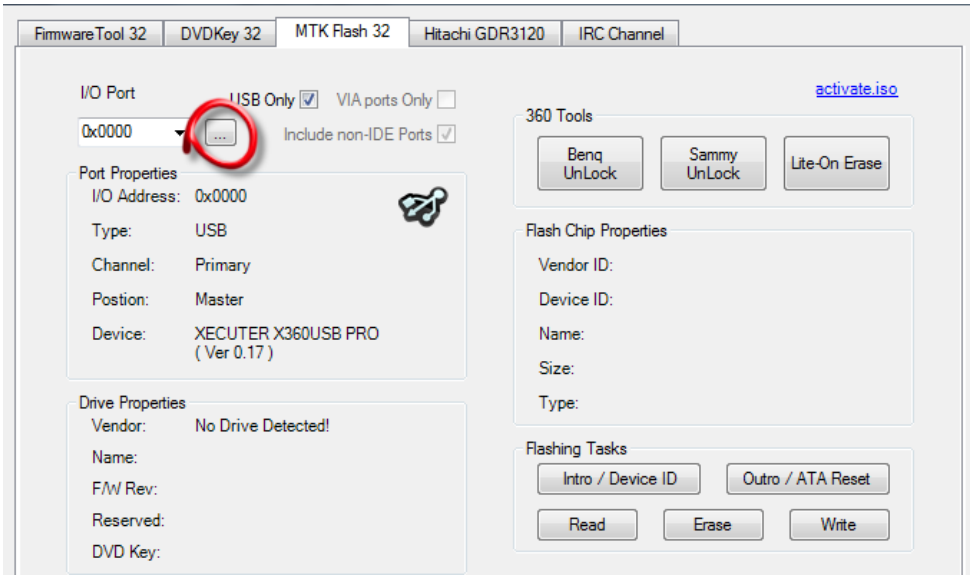
So get it all up and running and now the drive doesn't show up on the port where it was previously, eject does nothing (don't even bother plugging it into console) **it's Bad Flashed!**

With the X360USB Pro recovery works very simply 99% of the time (sometimes Samsung can be a pain – but usually it works in the end!)

Unplug your X360USB Pro and power off the drive. Close JungleFlasher.

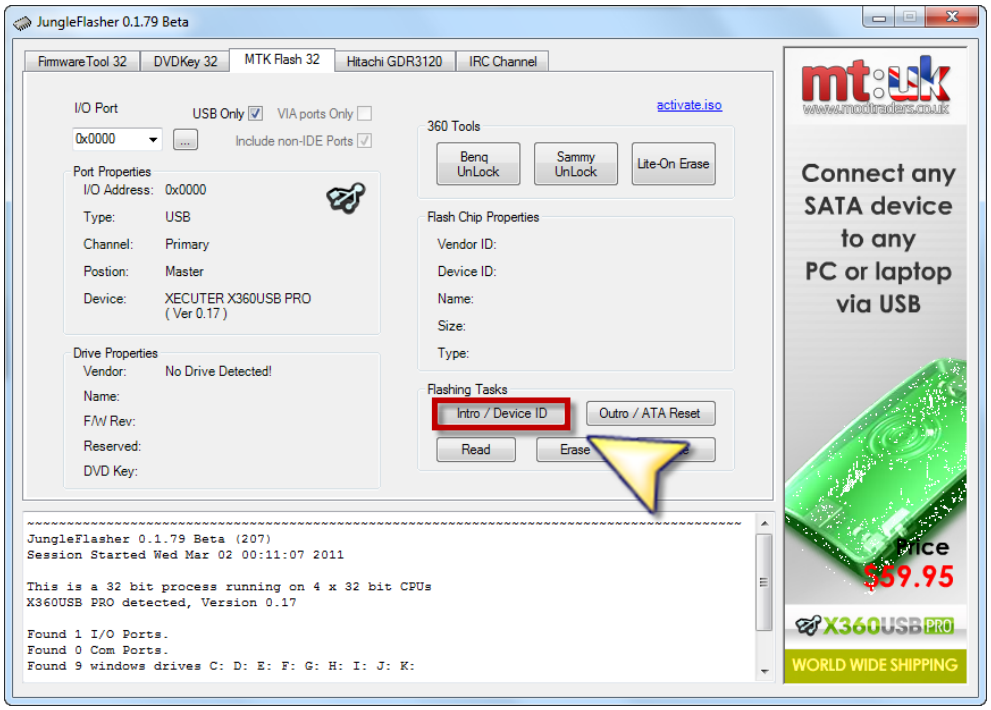
Reopen JungleFlasher, plug the X360USB Pro back in – select it from the IO Port list (if it hasn't automatically done it for you). Power on the drive!

So you clicked refresh, the drive is powered on and nothing shows up

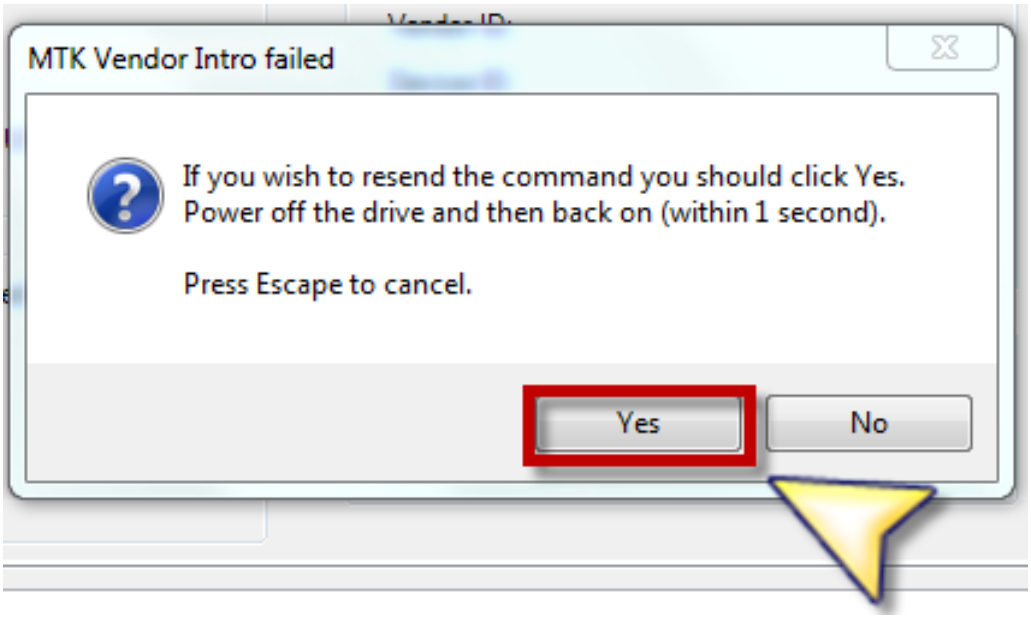


Things not going as expected? – Read the FAQ's

Then select Intro / Device ID button



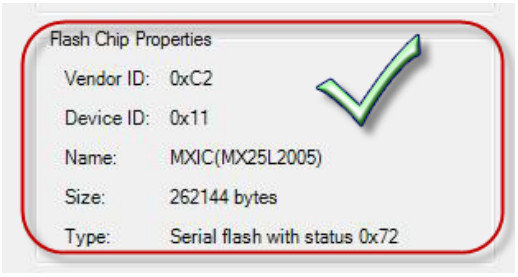
Then power off your drive – you will be asked for confirmation



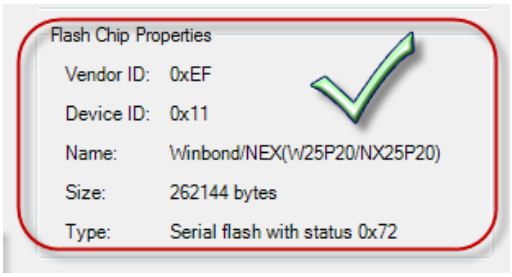
Click **YES** then Power on the drive again.

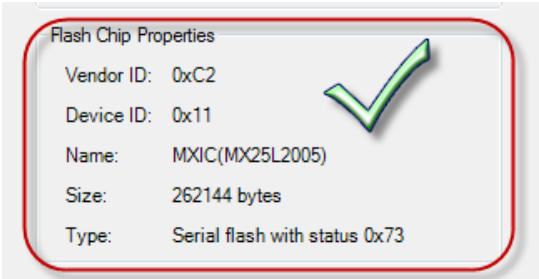
Things not going as expected? – Read the [FAQ's]

At this point (dependant on which drive) you should be faced with the drive in vendor mode (with appropriate status for drive type).

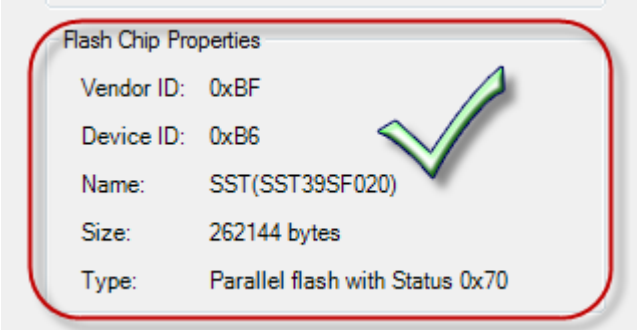


LiteOn





BenQ



Samsung

Now simply proceed at the part of the flashing process you were at when the writing of your drive went wrong!

(Remember you must load your previously dumped Dummy.bin / OFW.bin as source and auto-load your iXtreme firmware as target.)

CLICK HERE TO PROCEED

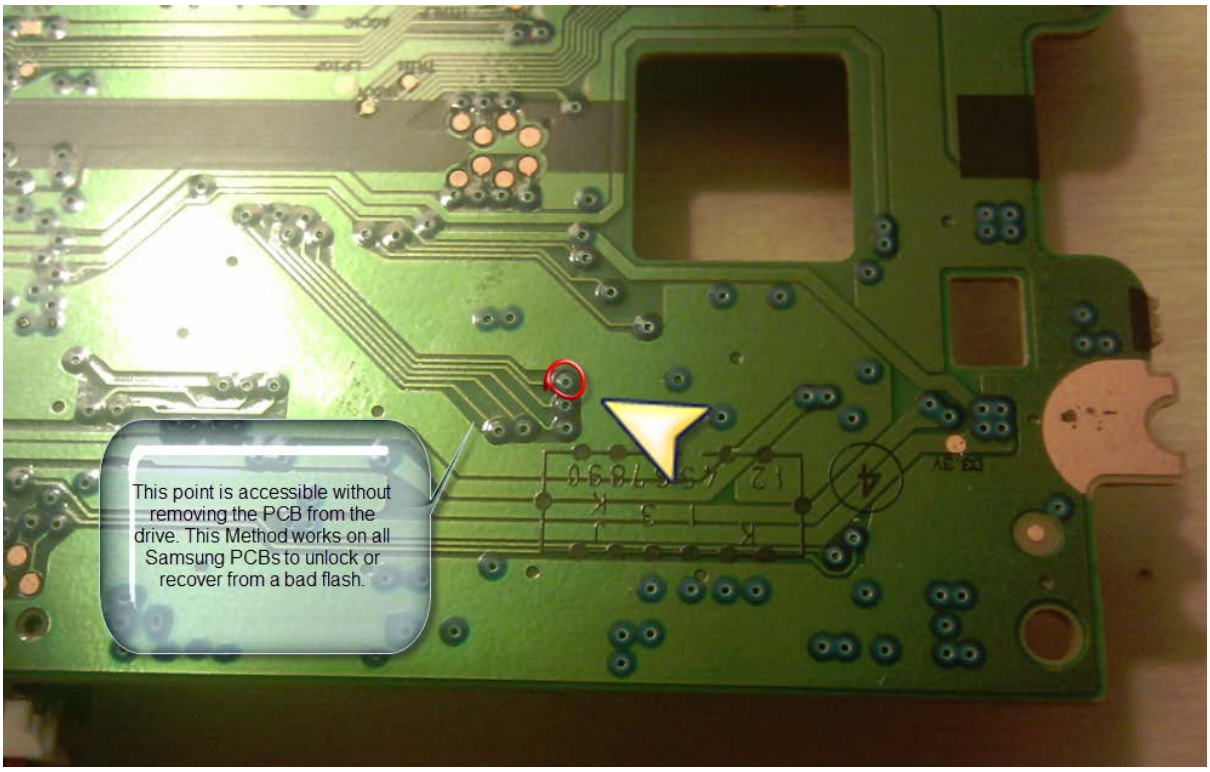
Samsung Drives Using PMT or CK Probe 3 When normal bad-flash won't work

For those awkward moments when things just haven't gone as planned! – There is a longer but simple method.

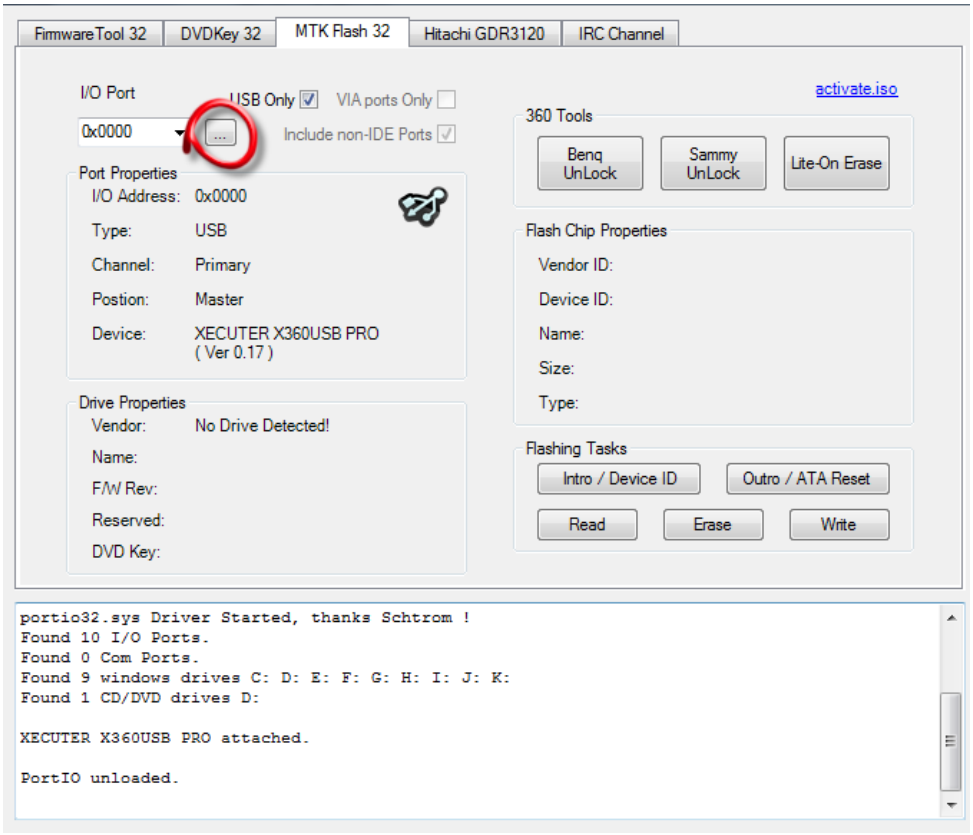
Utilize the Xecuter Probe 3 or PMT (probe goes to GND)

Open the drive case and expose the bottom of the PCB

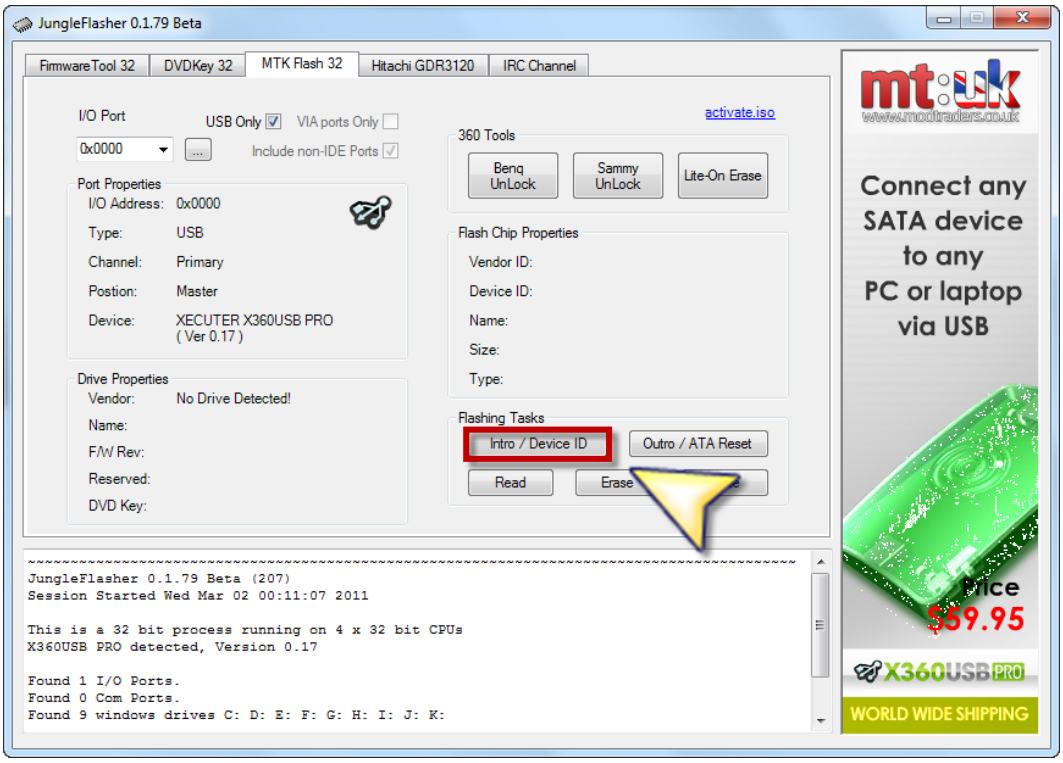
Then locate the point you need to probe with your PMT/CK Probe 3



Then load Jungleflasher, ensure you have correct IO port selected! If the drive is Bad-flashed it won't show up even after a port refresh like the example below

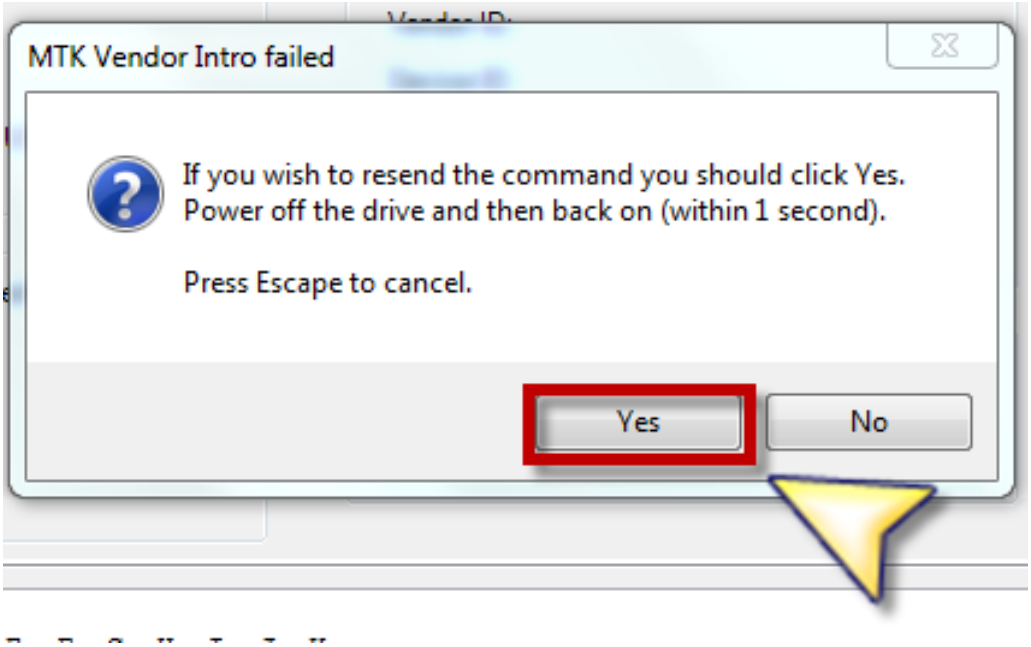


Then select Intro / Device ID button

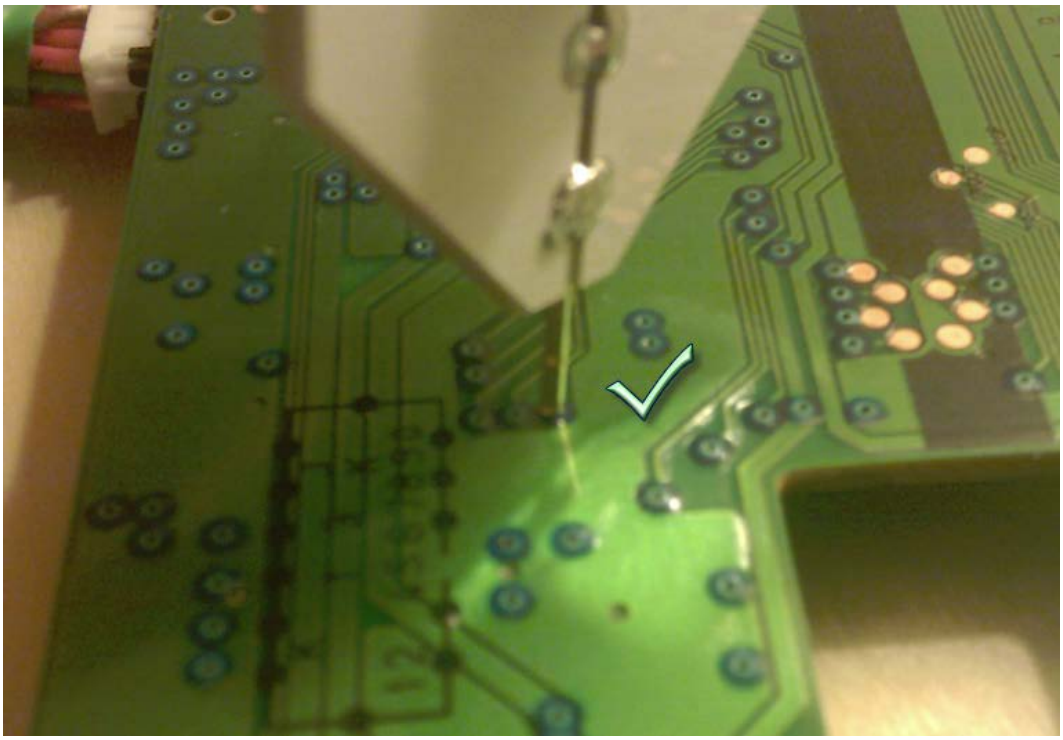


Things not going as expected? – Read the [FAQ's]

Then power off your drive – you will be asked for confirmation

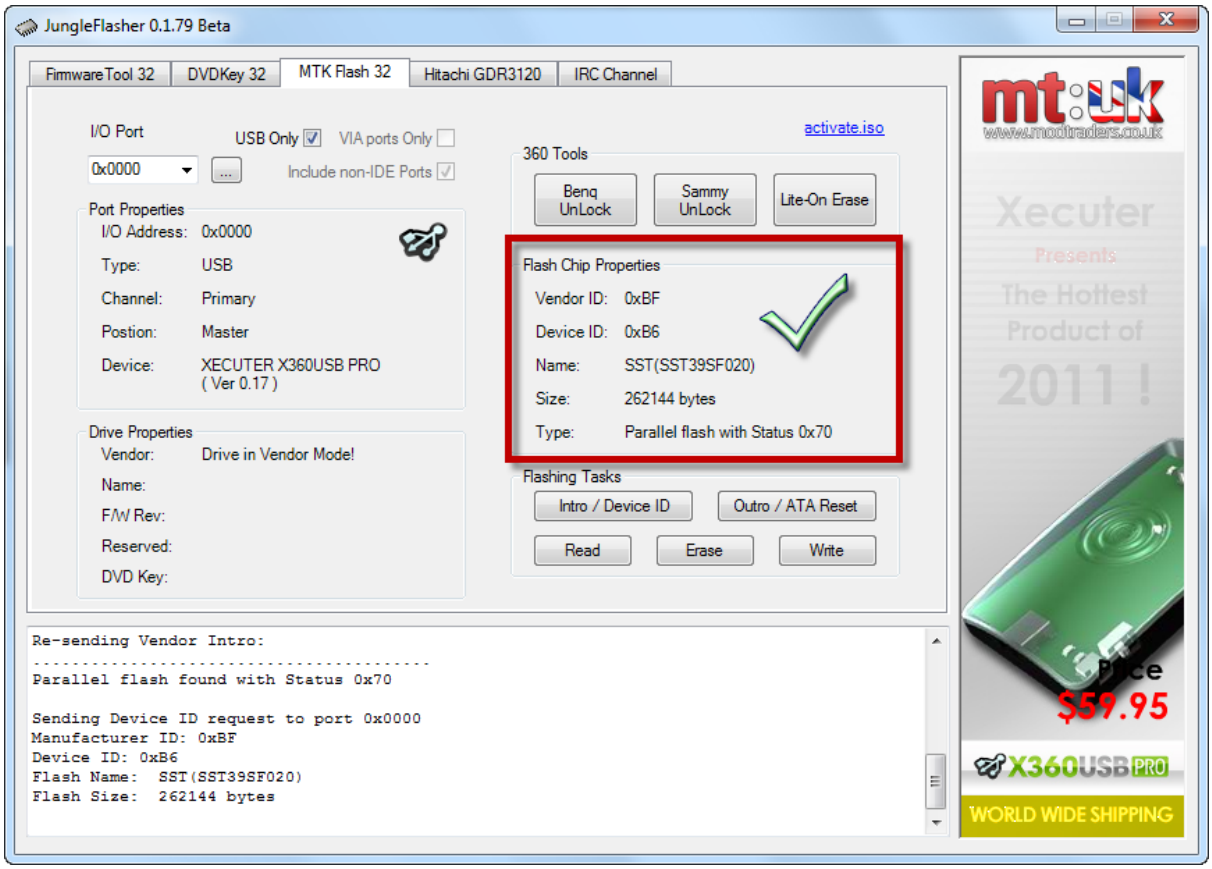


Click YES and probe the point on the board



Power on the drive and watch Jungleflasher window for status 0x70

Things not going as expected? – Read the FAQ's



Immediately lift the probe – then Continue with the correct procedure for what you were doing!

If you had bad-flashed it – then

Write your target firmware.

If you were unlocking – proceed to the

Reading of your firmware.

Things not going as expected? – Read the FAQ's

Benq Badflash Recovery

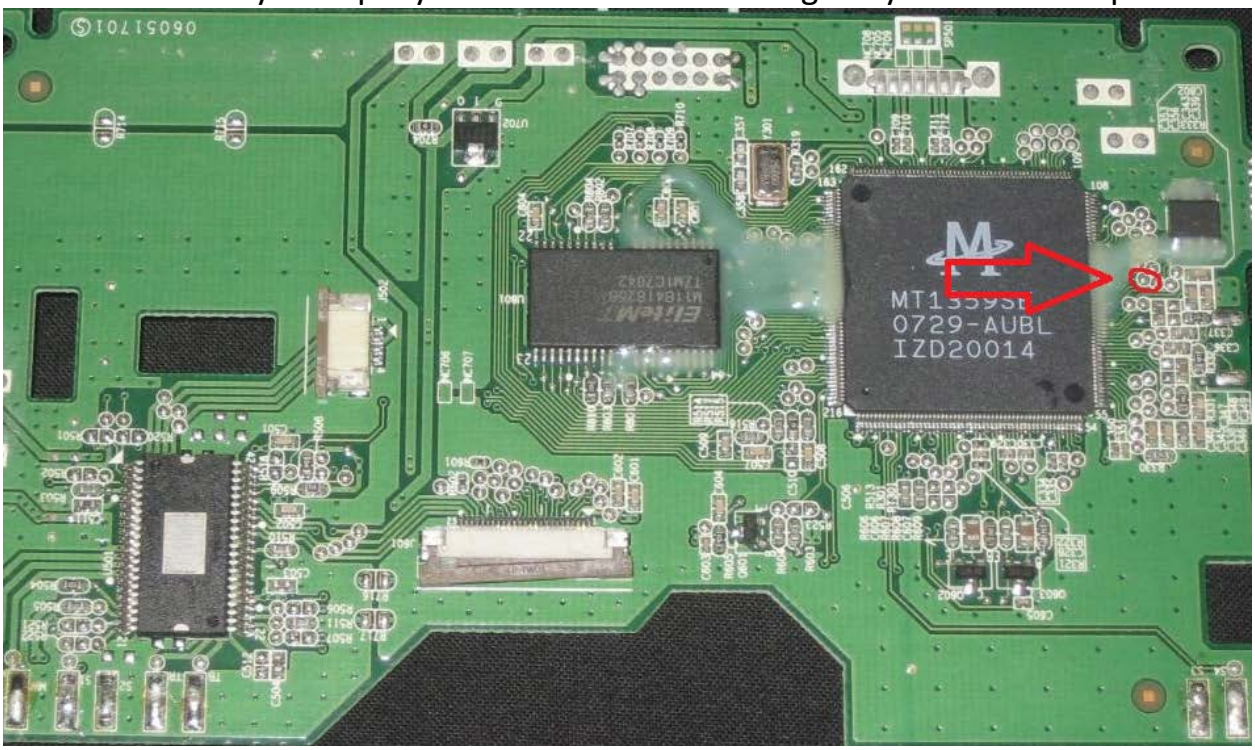
Badflash can happen if your PC freezes midway through flashing, your xbox powers off during flashing (you should have had the A/V cable inserted), if you took the 13146 update with custom firmware or a spoofed drive, or for other reasons.
If things haven't gone as planned with your Benq flash, then you might need badflash recovery methods outside of a simple "intro/device id, yes, power cycle."

This version of badflash recovery should NOT be needed for VIA 6421 cards, but may be necessary for many onboard setups and use of the x360usb pro.

You will need a Xecuter Probe 3, PMT, or a GND probe of your own building (as the switch of the Probe 3/PMT isn't required).

Open the drive case and expose the bottom of the PCB.

Locate MPX01 as shown below, as it is unlabeled on the PCB.
If your MPX01 point is covered in epoxy, you can use a soldering iron on low heat to "burn" away the epoxy. Make sure to not damage any of the solder points.



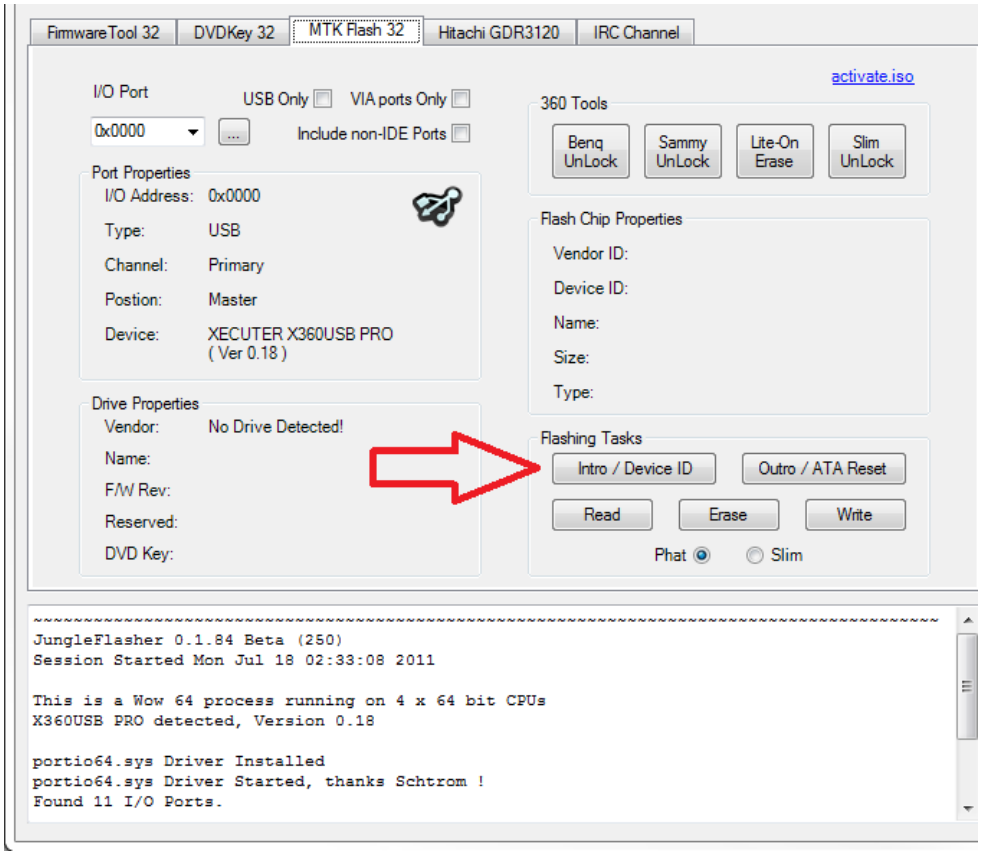
Things not going as expected? – Read the FAQ's

Load up Jungleflasher, and ensure you are using the correct IO port. The drive will NOT show up in JF if the drive is badflashed, even if you refresh the port.

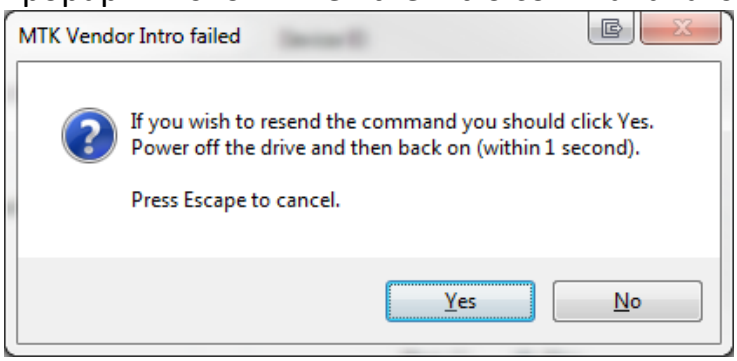
Power off your drive.

NOTE: This power off is done with the switch on the ck3 or by unplugging the drive from the xbox. (The Probe 3/PMT switch will NOT suffice.)

Press **Intro/Device ID**.



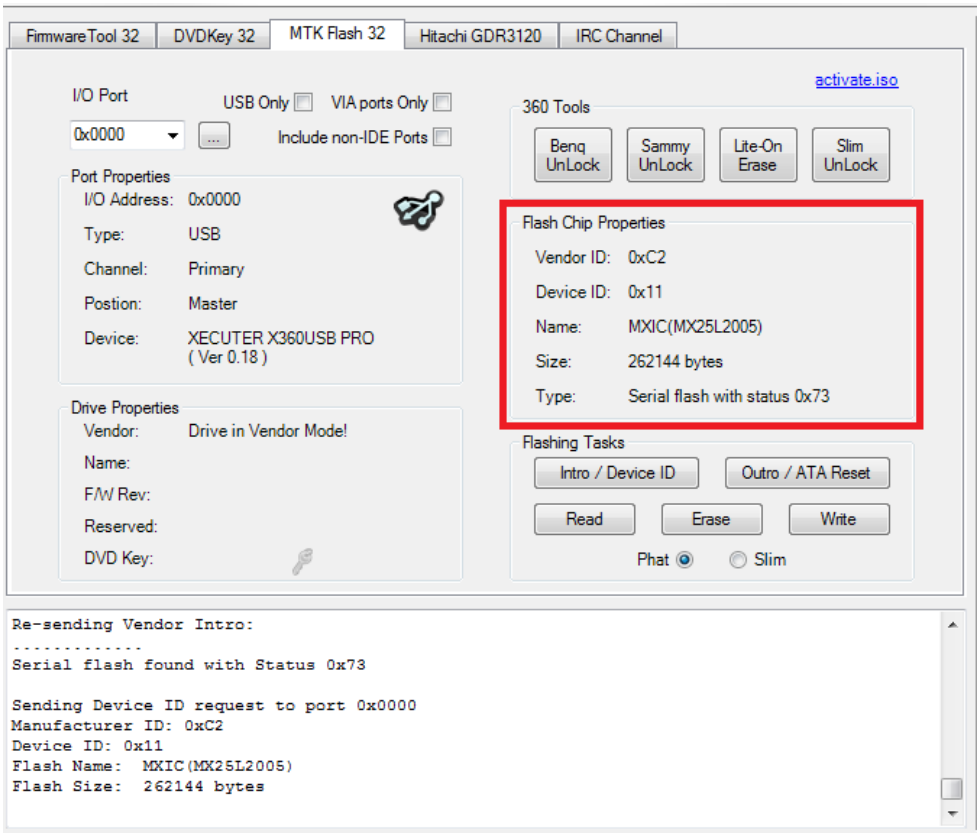
A popup will show when the Intro command fails.



Click YES and probe MPX01 on the PCB with the Probe 3 or PMT.

Things not going as expected? – Read the FAQ's

Power on the drive and watch in Jungleflasher for status 0x73.



When you see 0x73, *immediately lift the probe*. If your flash chip properties are shown similar to above, you can continue to the normal section of the tutorial and proceed to your next step.

However, if your flash chip properties are not shown and you get “n/a” for size, you will not be able to read or write firmware to the drive. Often, simply pressing “Intro/Device ID” will fix the problem and Jungleflasher will return good flash chip properties.

CONTINUE

Slim Lite-on Badflash Recovery

If things haven't gone as planned with your Slim Lite-on flash, then you might need badflash recovery methods outside of a simple "intro/device id, yes, power cycle."

NOTE: most often only needed for semi-compatible chipsets (like VIA 6421 and some onboards). The X360USB Pro should almost always be able to get Slim Lite-ons into Vendor Mode without probing.

Badflash can happen if your PC freezes midway through flashing, your xbox powers off during flashing (you should have had the A/V cable inserted), or for other reasons.

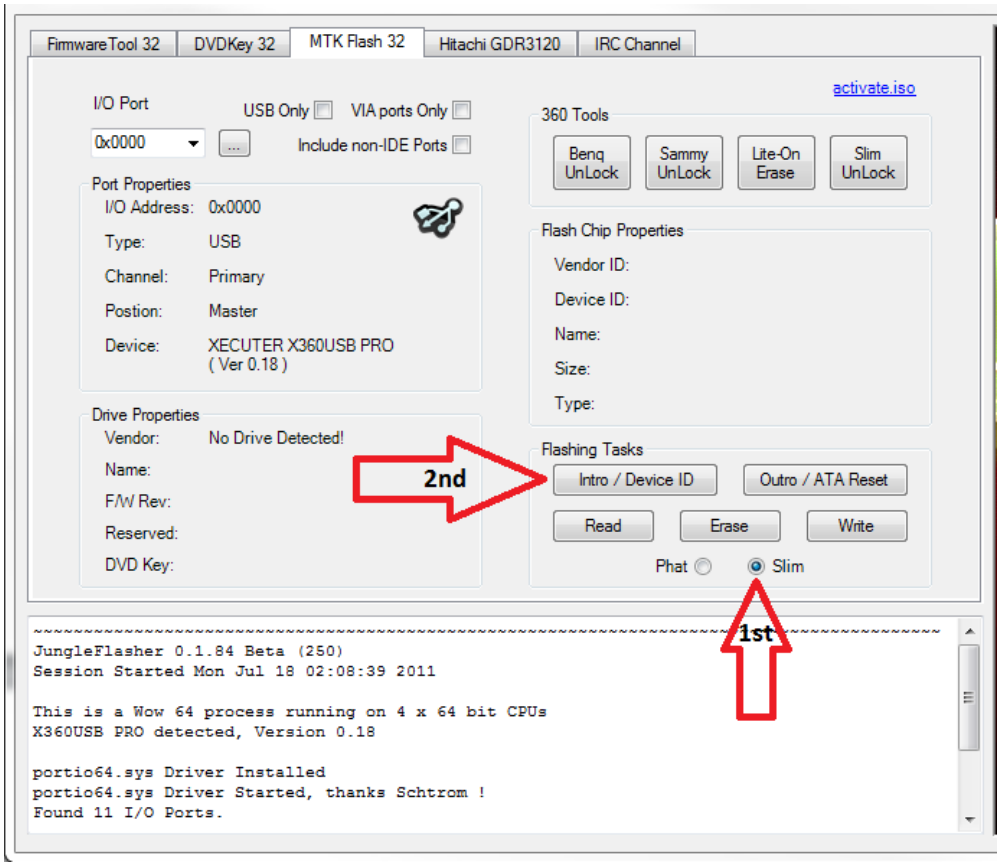
You will need a Xecuter Probe 3, PMT, or a GND probe of your own building (the switch of the Probe 3/PMT isn't required).

Open the drive case and expose the bottom of the PCB.
Locate MPX01, it is labeled on the PCB.

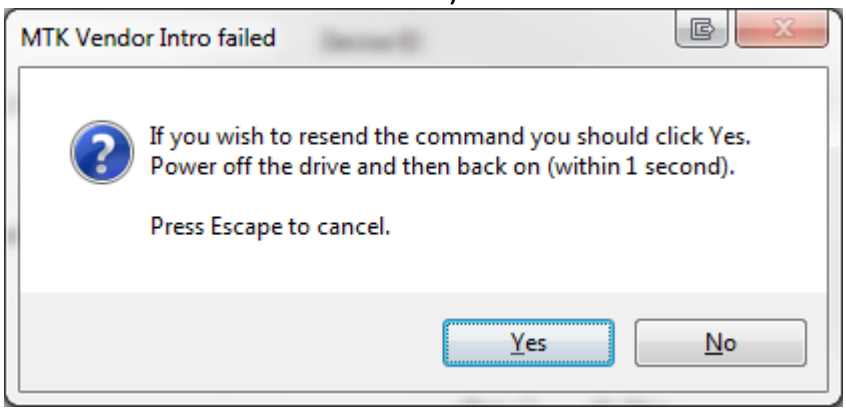
Things not going as expected? – Read the FAQ's

Load up Jungleflasher and make sure you have the correct IO port selected. If your drive is badflashed it will NOT show in Jungleflasher, even after a port refresh.

Make sure the "**Slim**" button is ticked. Then press **Intro/Device ID**.



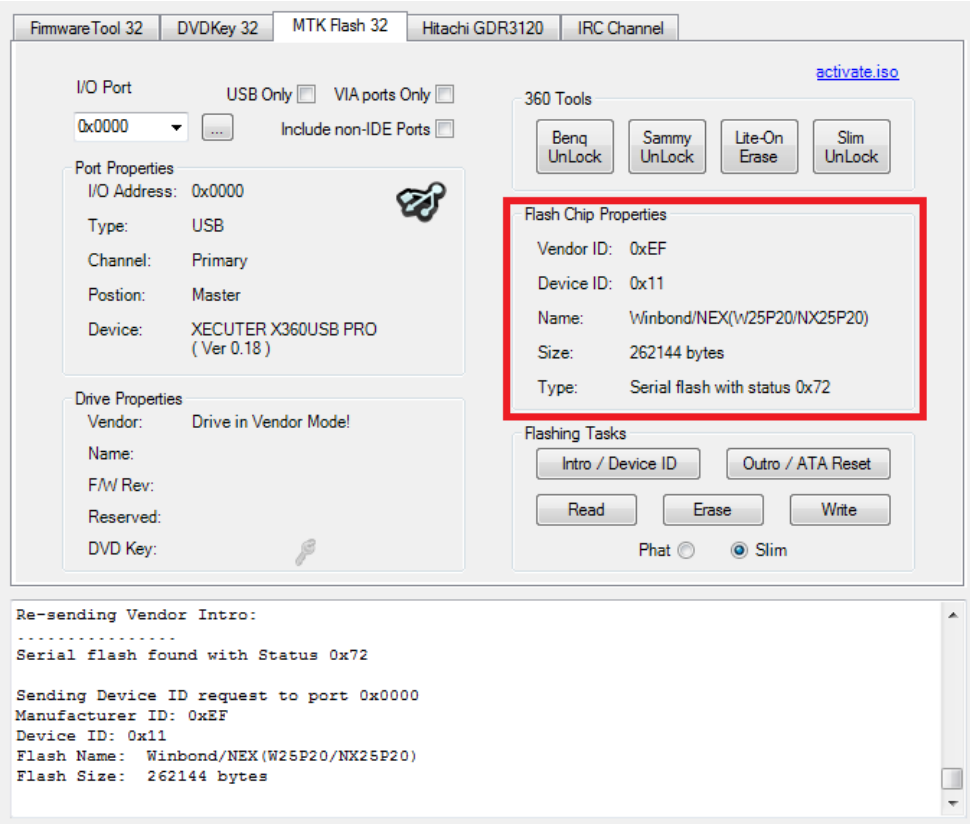
A popup will appear when the Intro command fails.
Power off your drive (using the ck3 switch or by unplugging the drive from your xbox).



Things not going as expected? – Read the FAQ's

Probe MPX01 on the PCB (shown above)
Press **YES**

Power on the drive and watch Jungleflasher for status 0x72.



When 0x72 appears, *immediately lift the probe*. If good flash chip properties appear then continue to the correct procedure to whatever you were doing.

If you do not get flash chip properties, and get “n/a” for size, check to make sure that the “Slim” button is ticked.

NOTE: If “Slim” is ticked, and you still get bad flash chip properties, make sure that you are using an original Slim Lite-on PCB. If the PCB has been modified with an Xecuter Pro Unlock Kit or is an Xecuter Unlock PCB, then Jungleflasher must have “Phat” ticked.

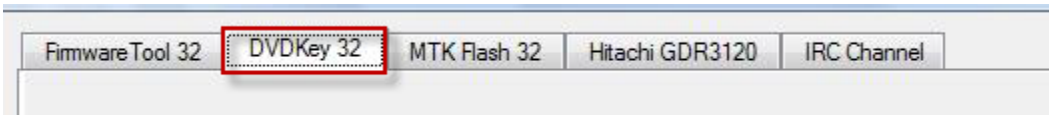
CONTINUE

Things not going as expected? – Read the FAQ’s

LiteOn Slim FW Ver. 0225, Locked 0272, 0401, 1071

Dumping the required drive info is very straight forward.

First select the **DVDKey 32** tab.

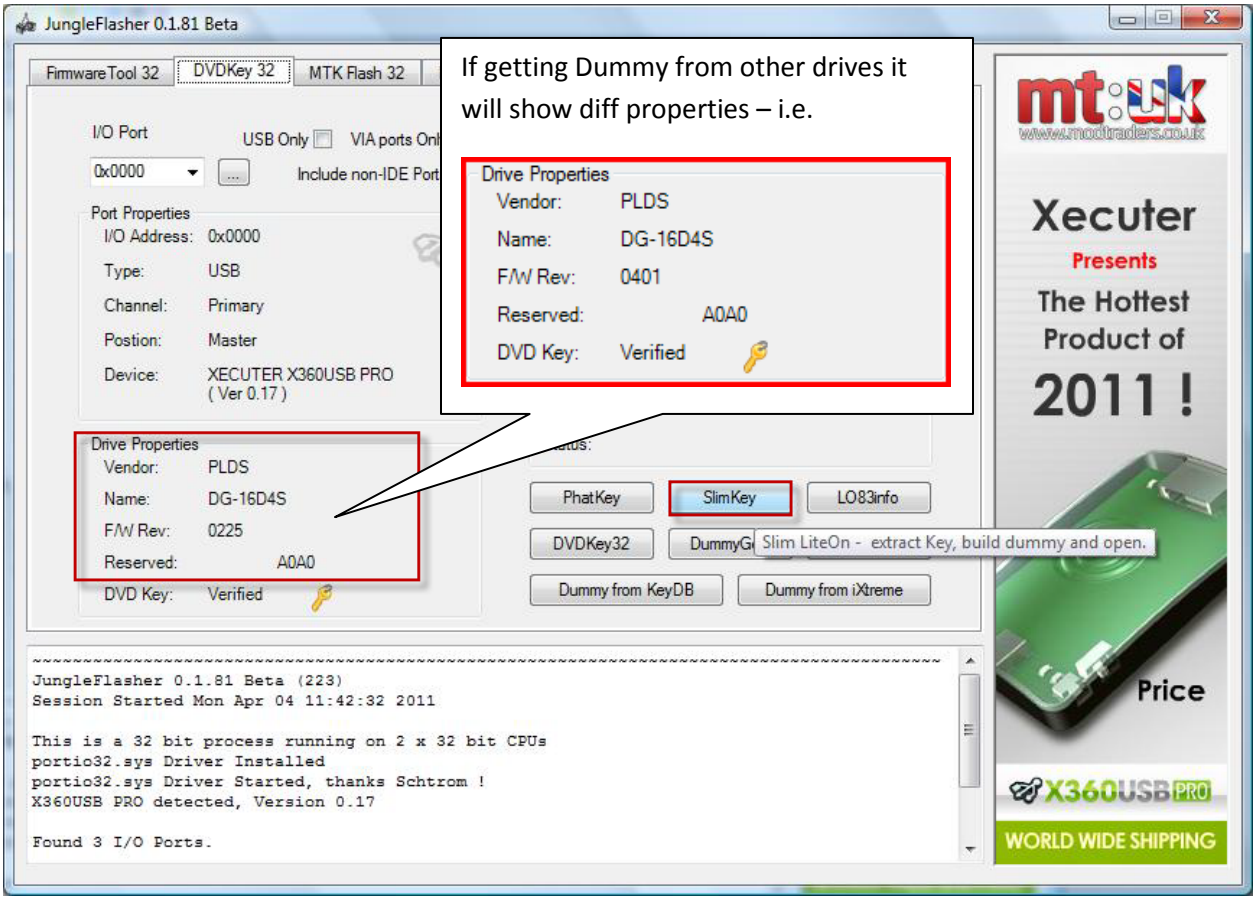


NOTE: Very few chipsets are known to work reliably for 0225 (and subsequent) drives

(Hence why we are using X360USB Pro)

Ensure it inquires on the I/O port.

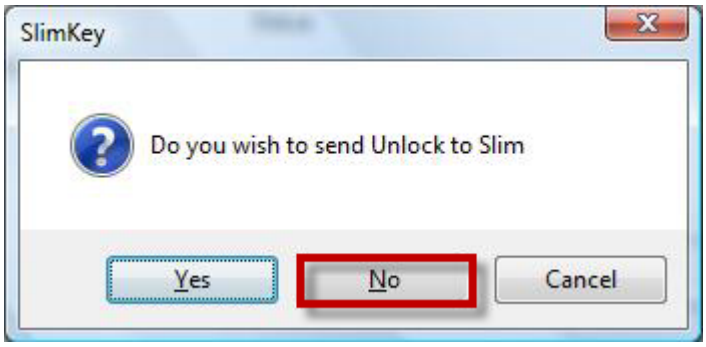
Click the **SlimKey** Button



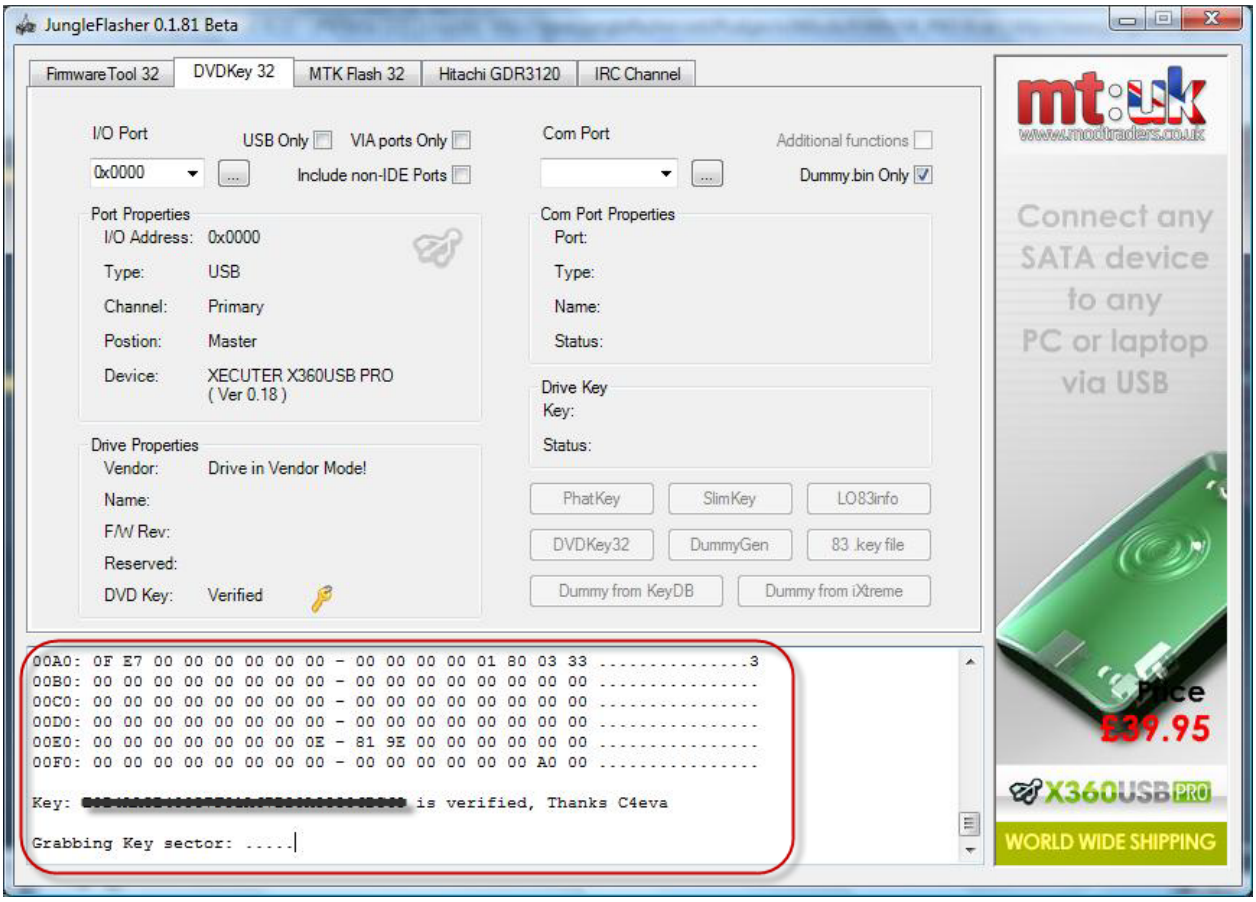
Things not going as expected? – Read the FAQ's

You will be presented with an option box asking if you wish to send *Slim Unlock*

Select **NO**

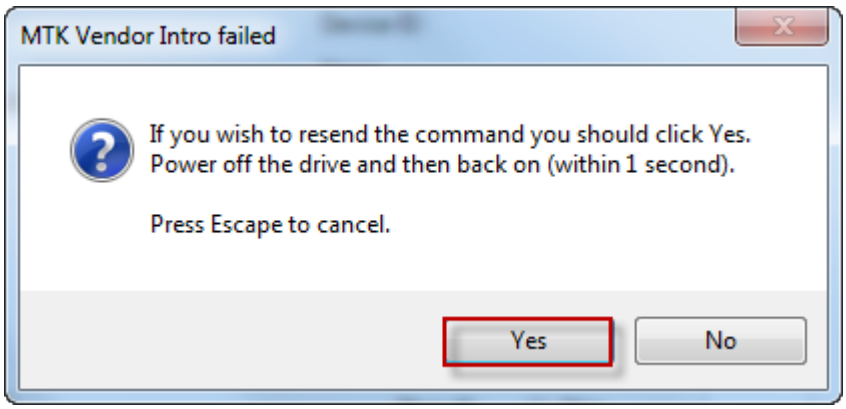


JungleFlasher will start to grab the key sector and serial data



You will be faced with this

Things not going as expected? – Read the FAQ's



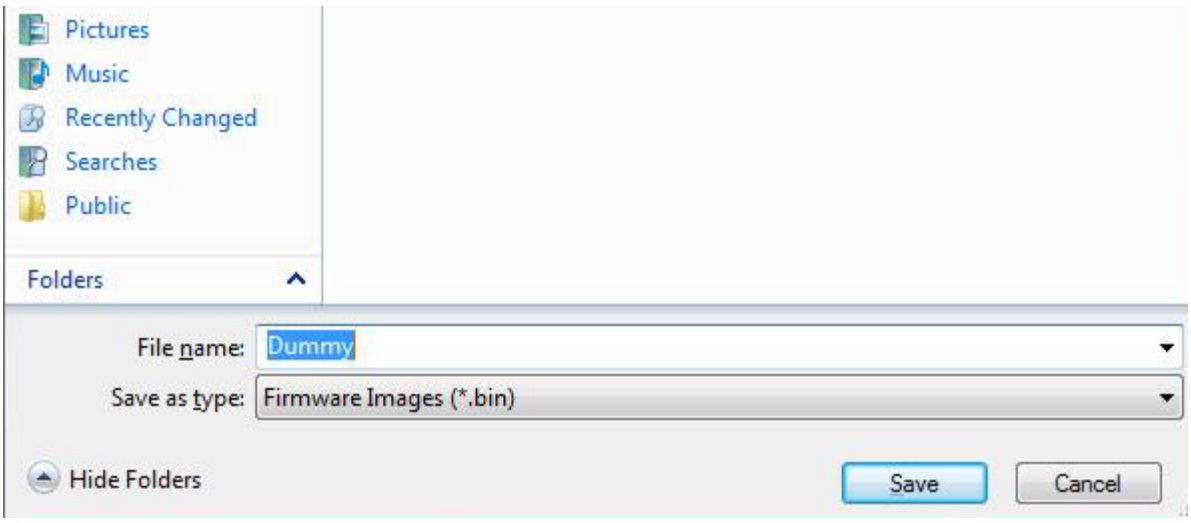
Click **Yes** the power off then on again

Once dump has completed it will also verify the Key

(as shown below)

Jungleflasher will then populate this information and create a Dummy.bin,

You will be asked to Save the file (as always – Please do so!)



Firmware Tool 32 tab will be automatically opened and your Dummy.bin loaded as source.

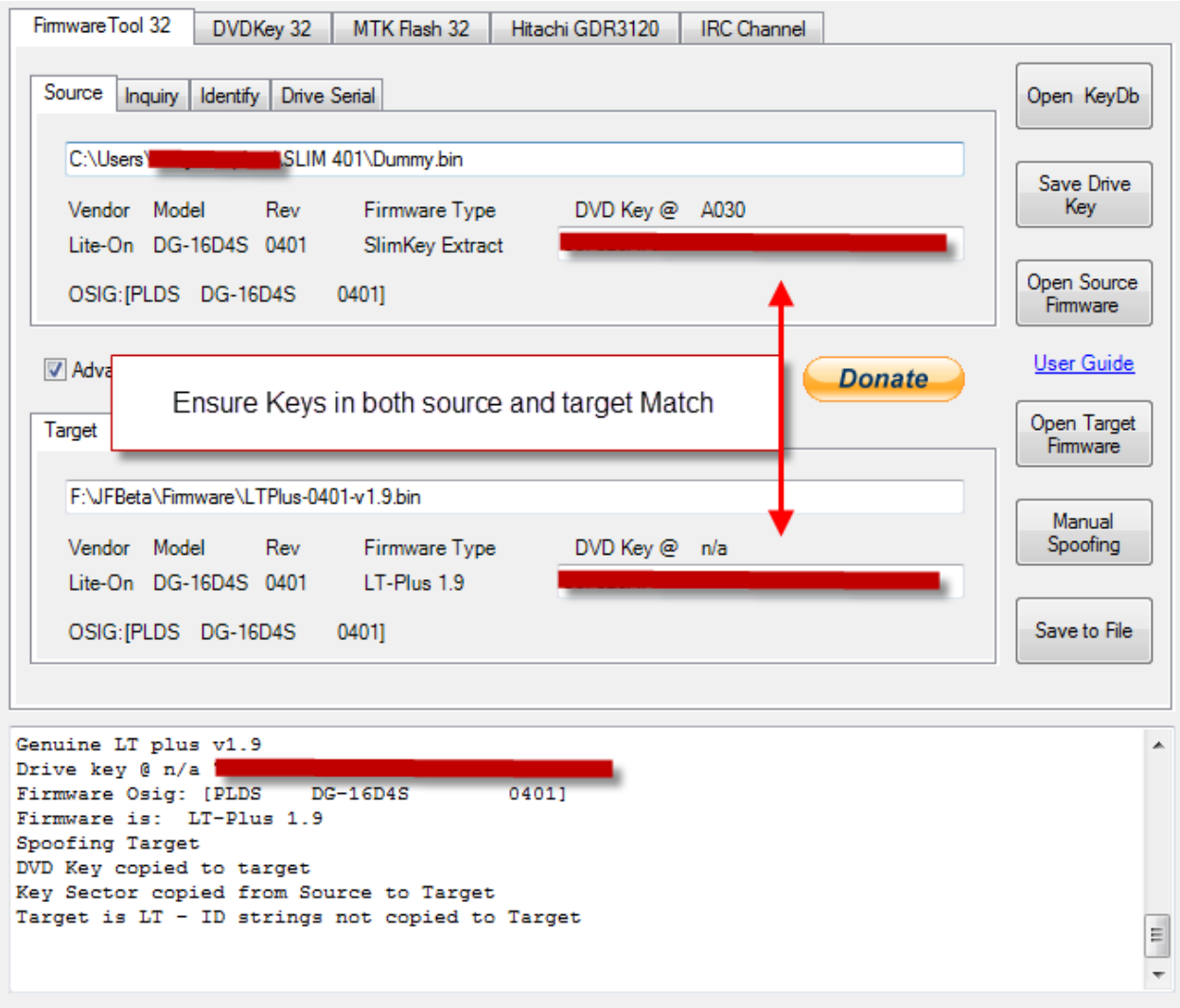
Option 1 : Use a replacement PCB / Pro-kit modified Orig PCB

Option 2 : Use a ***spare*** 9504 PCB (During 13599 Dash update 0272 stock firmware is flashed to your PCB and locked)

Option 3: Unlocking your PCB (more difficult)

Flashing your Replacement PCB (T-X) or Pro-Kit modified PCB

You should already have Slimkey'd your drive and obtained a dummy.bin. This should be loaded as source and allowed to auto-load iXtreme Firmware as target



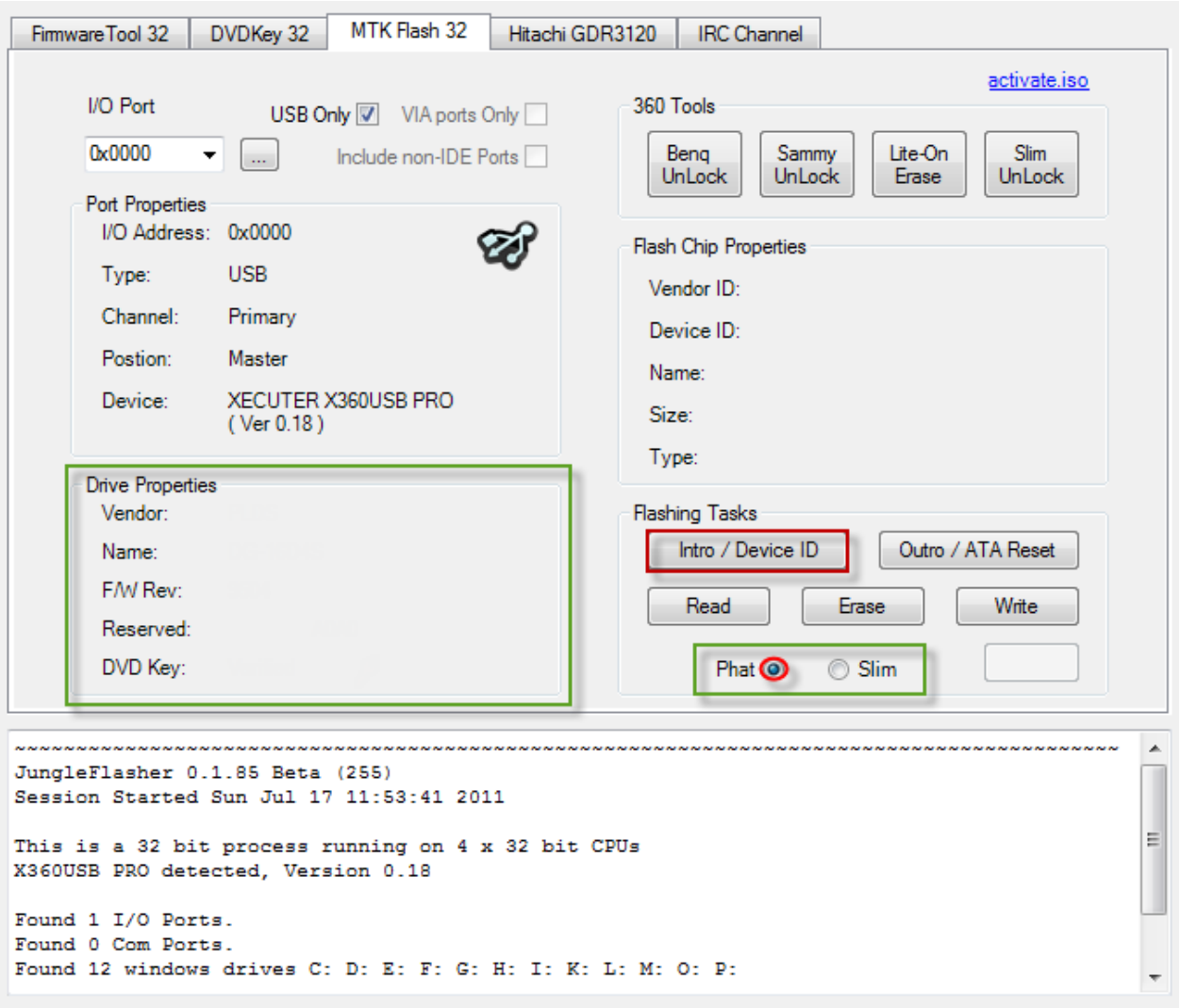
Connect your Replacement PCB

And select **MTK Flash 32** Tab

Note PCB's are blank when shipped as are the Pro-kit installed chips

So Drive properties will NOT show up

Ensure you are on the correct **I/O Port**

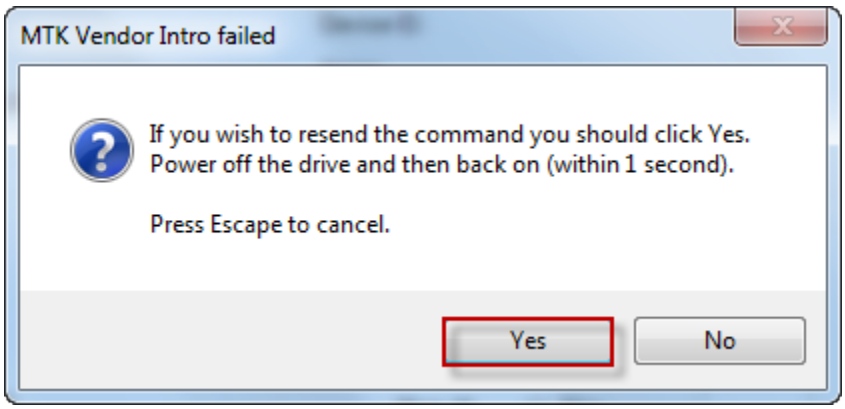


Ensure **Phat** is selected

Then press **Intro / Device ID**

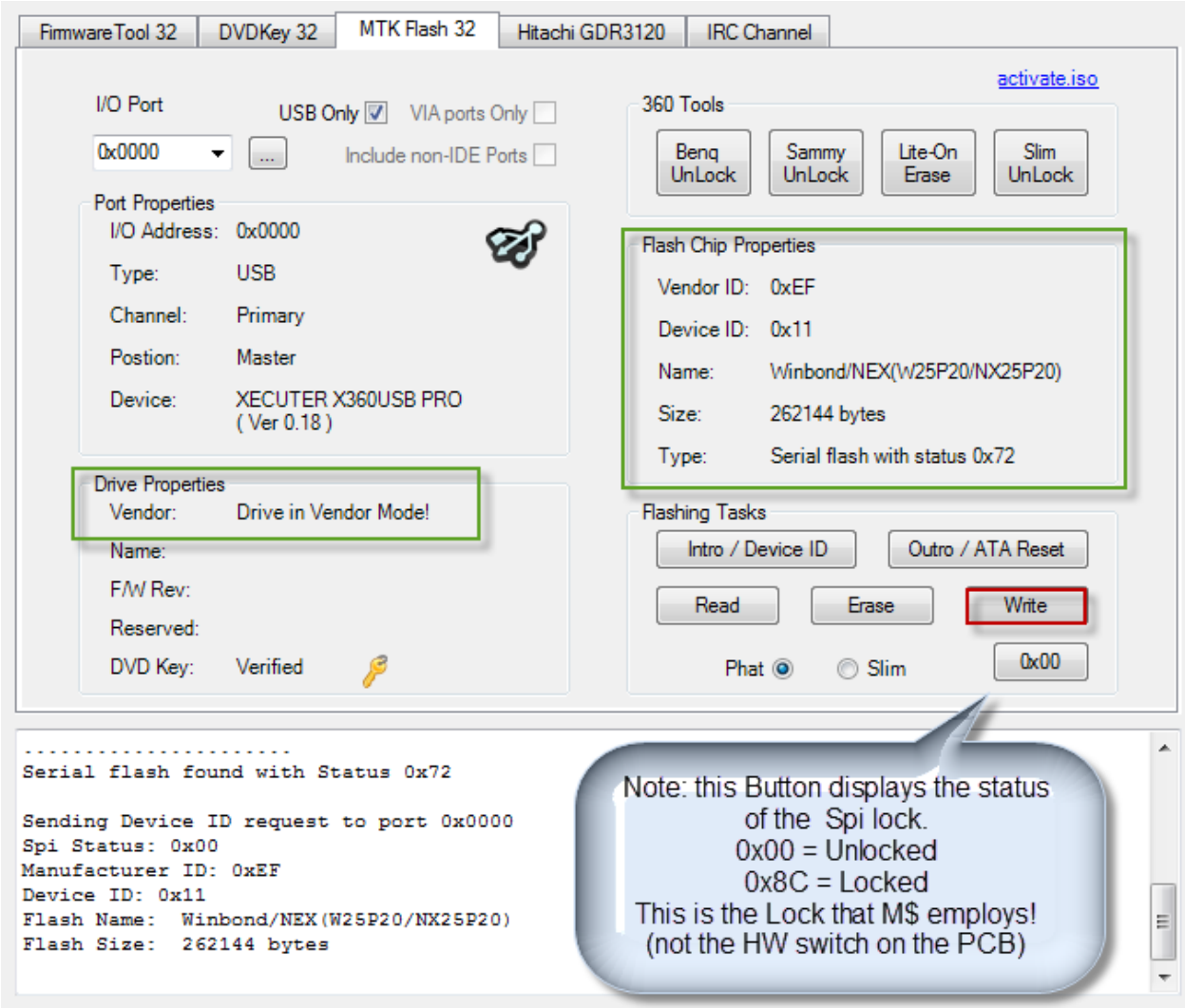
You may get this box appear

Things not going as expected? – Read the FAQ's



If so, then press **Yes** and turn drive power **OFF** then **ON** again quickly.

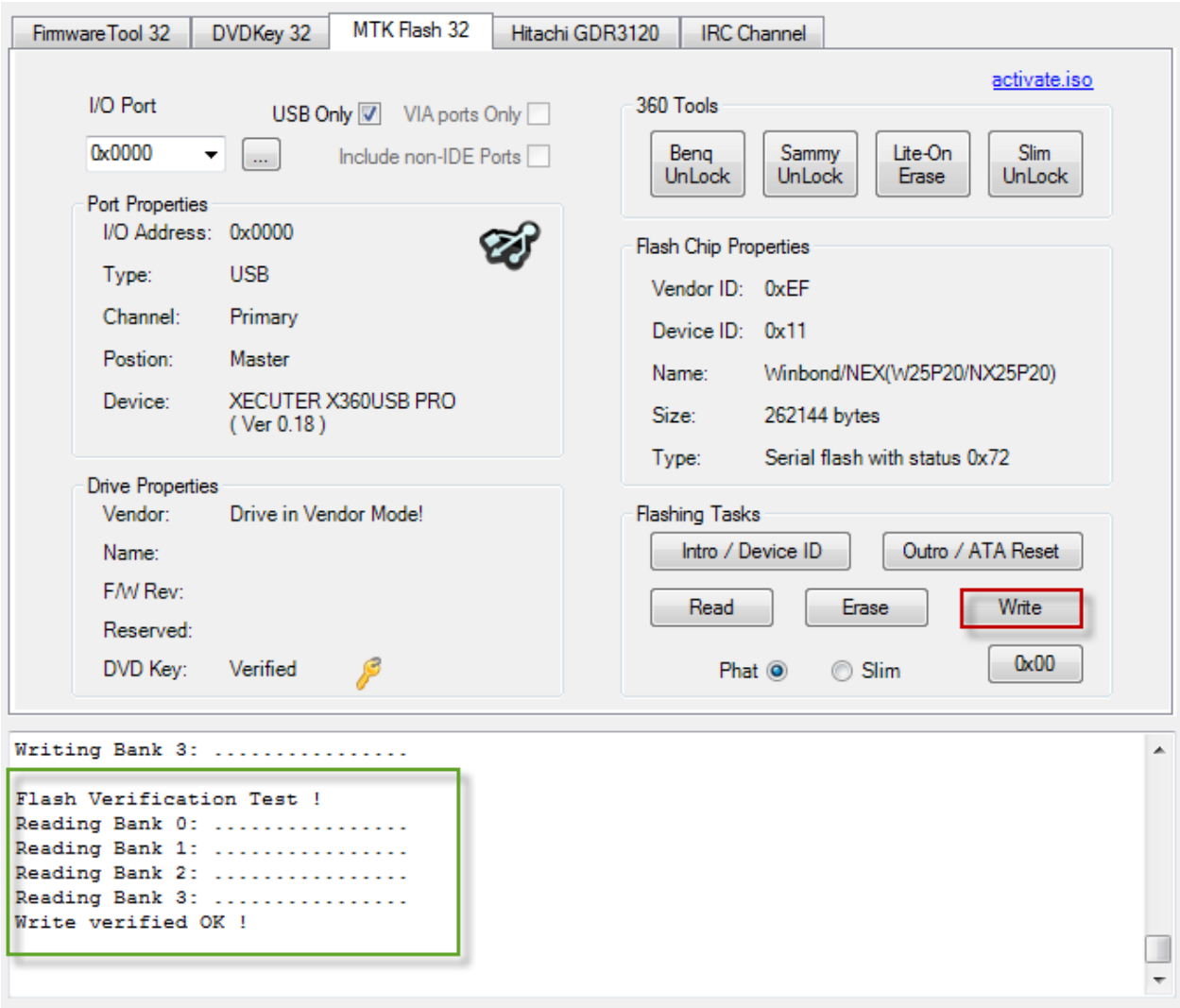
You should now see this. Including a button (0x00) that was previously blank.



Things not going as expected? – Read the FAQ's

NOTE: If the button is 0x8C – ensure switch on board is set to wp#1 then press the button to unlock the board

Now press the **Write** button



Jungleflasher will proceed to write the firmware that was loaded in target buffer on the FirmwareTool 32 Tab.

Once complete check the log for the **Write Verified OK!** Message

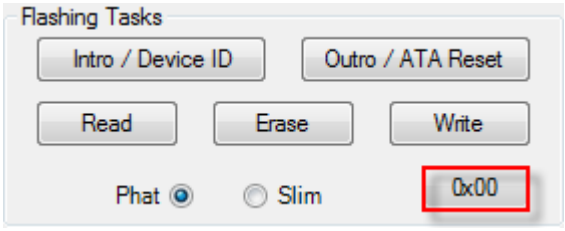
Now – Very importantly!

The original drives should all be locked so you need to ensure your replacement is the same!

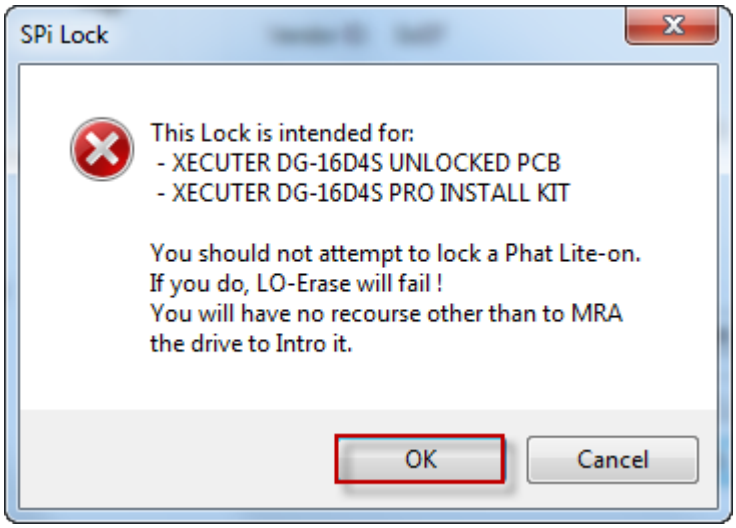
Things not going as expected? – Read the FAQ's

Press the **Spi-Lock Status** Button

Currently displaying **0x00**

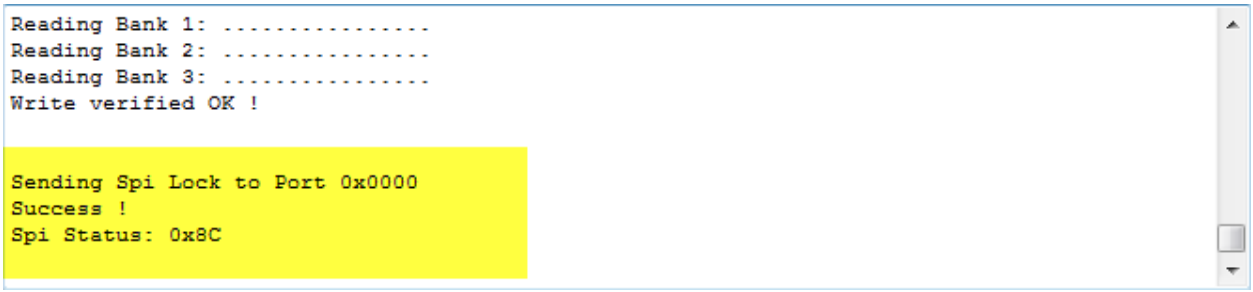


You will see this warning



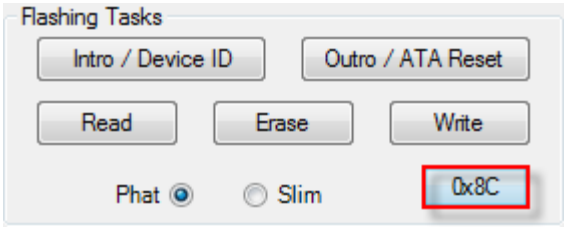
Click **OK** to lock the drive

This sends the command to lock the Spi (just as M$ did with 0272 drives on the 13599 dashboard update) you should see this in the log!

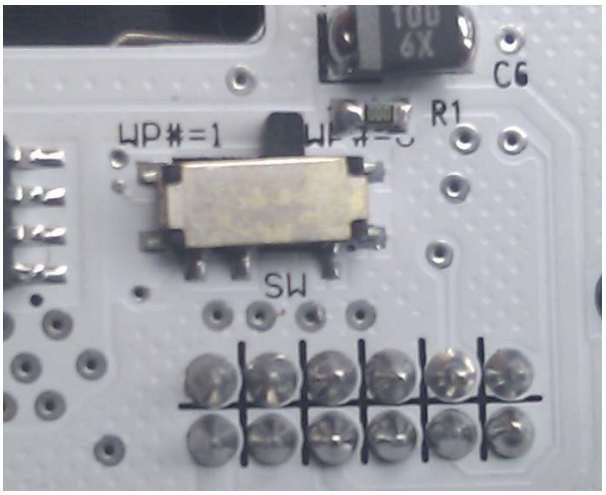


Now note the button text has changed to **0x8C**

Things not going as expected? – Read the FAQ's



Now set your Hardware switch on the PCB to WP*=0



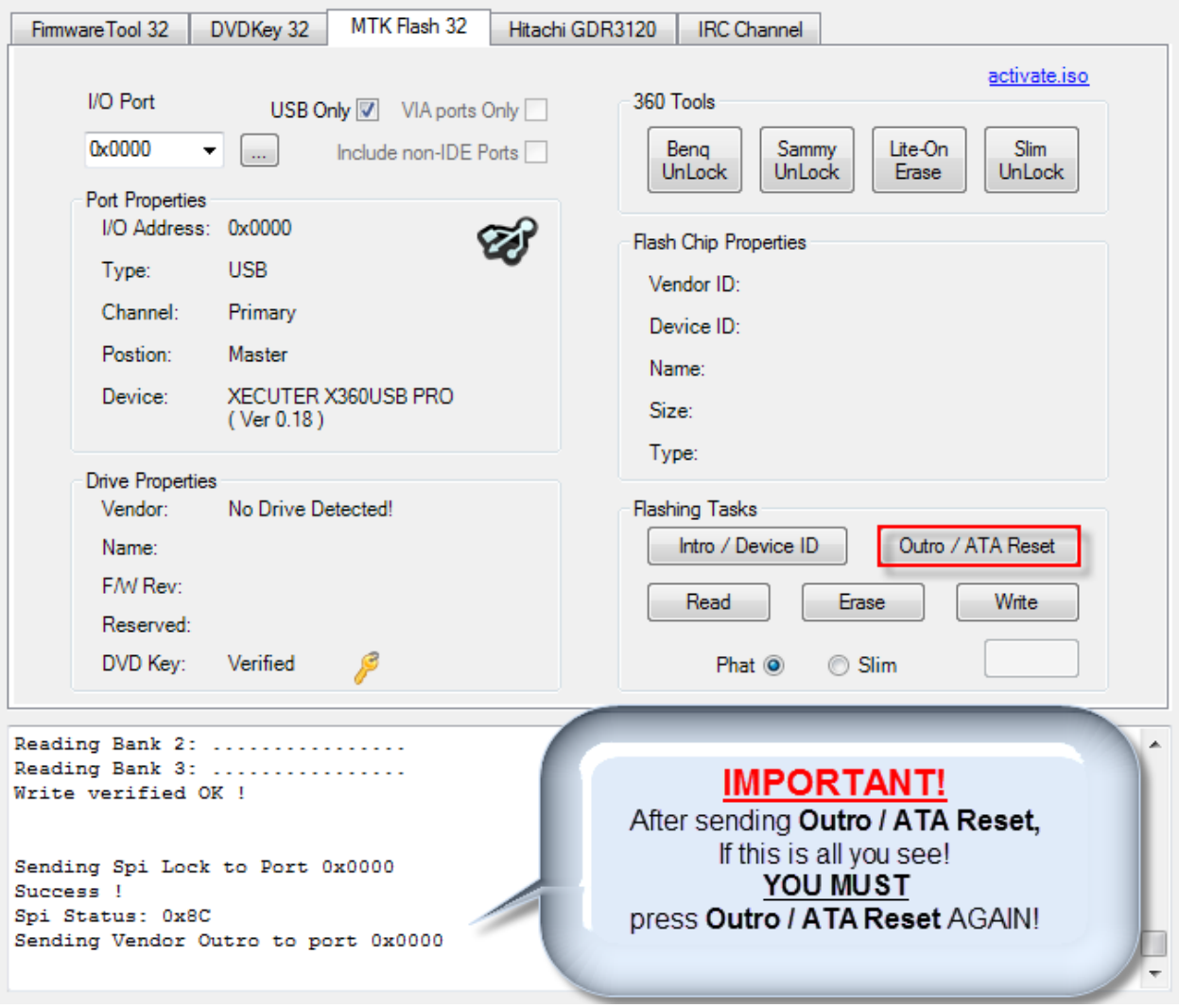
Now pressing the Spi-Lock button again will fail to unlock it! (that is exactly the way M$ expect an original drive to behave!)

So Ensure you set the switch to WP#=0

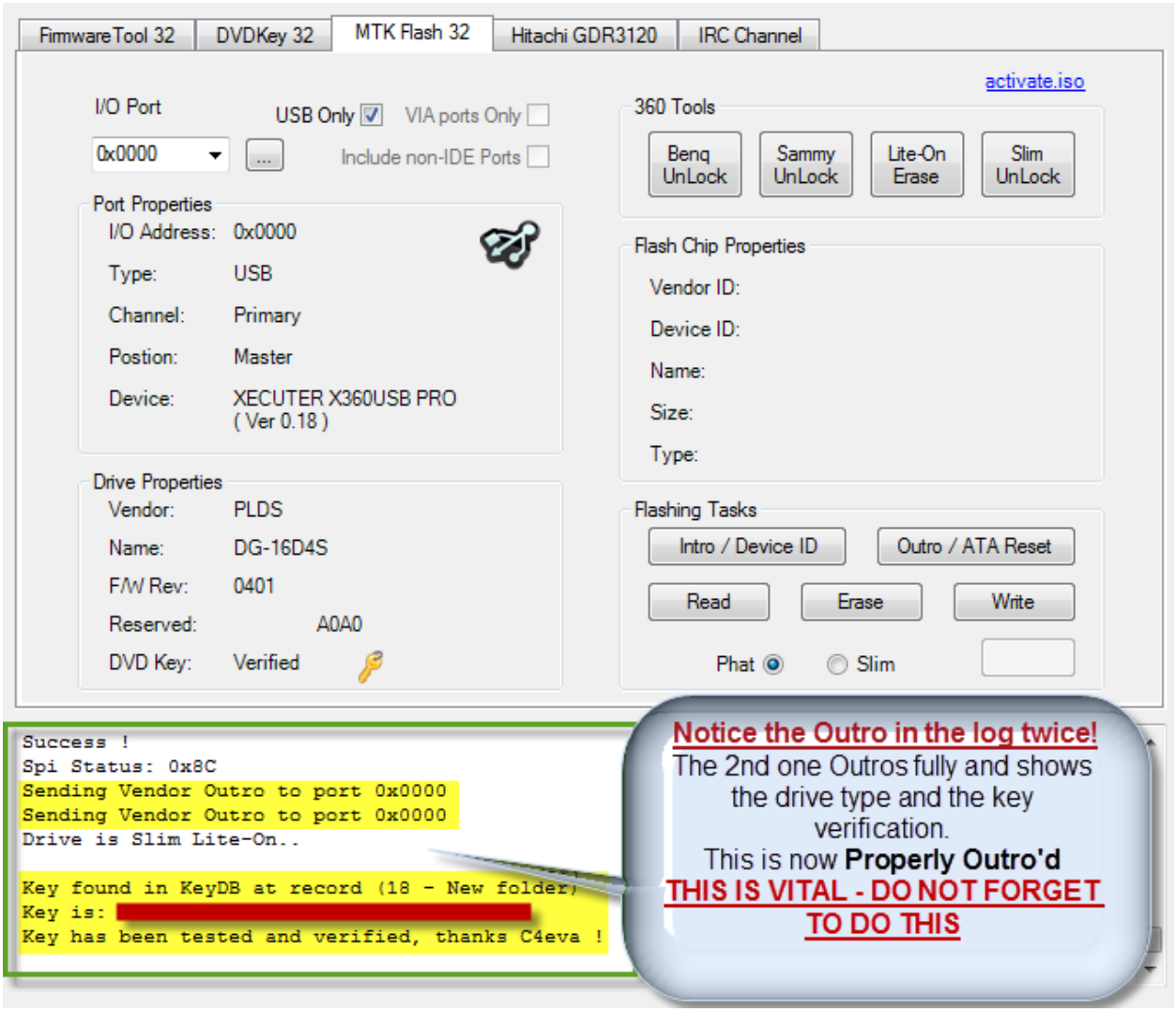
NOTE: If you wish to reflash later, set switch to WP#=1 and pressing the 0x8C button will allow unlocking of the Spi.

Very Important Final Step!

Press the **Outro /ATA Reset** Button



If you do **NOT** get a Key tested and Verified message in log – Press **Outro /ATA Reset** Button **AGAIN**



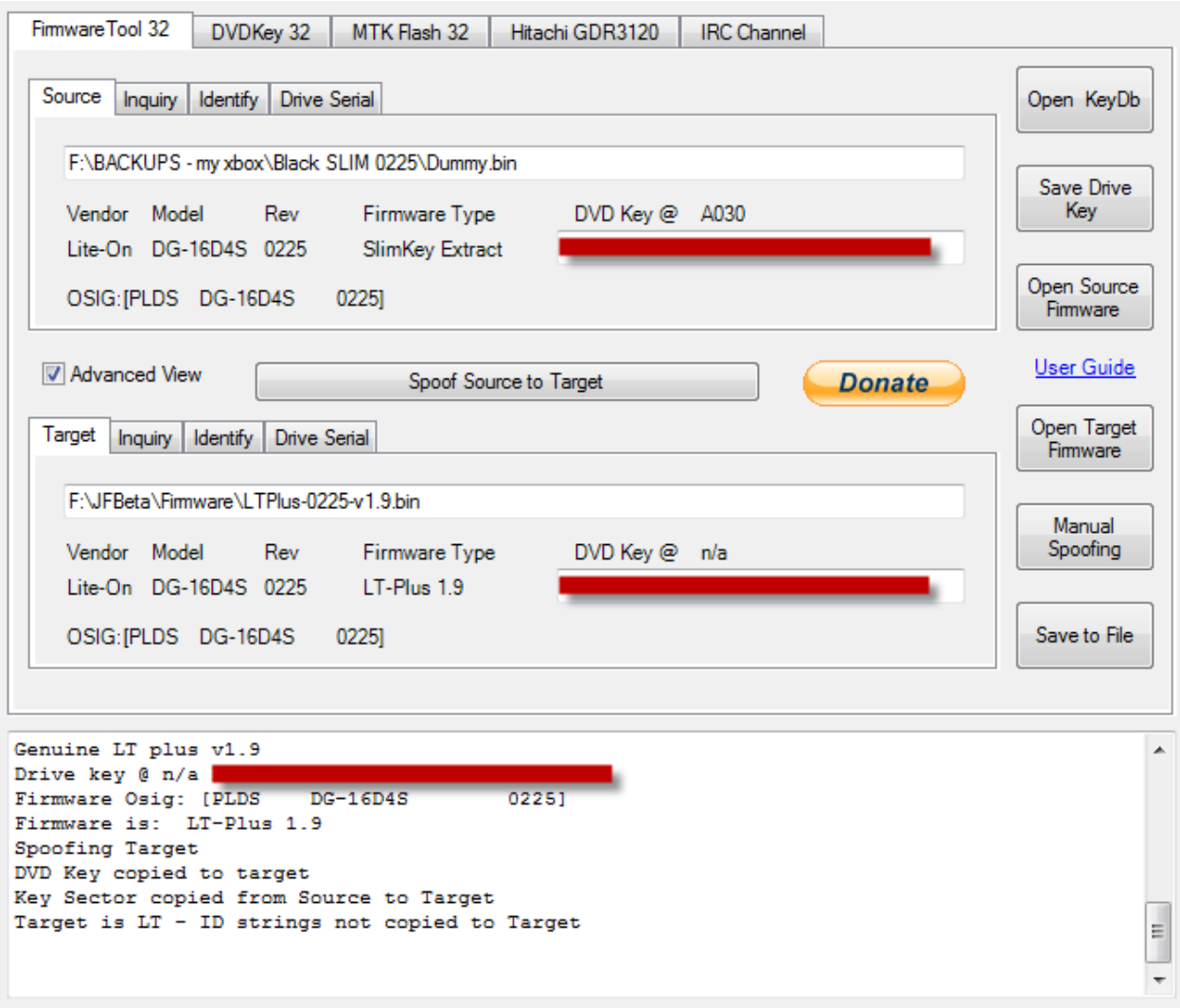
Switch off power to drive, Disconnect and test in your xbox!

YOU ARE FINISHED – CLICK HERE TO RETURN TO START

Using a Spare Unlocked 9504 PCB

You should already have Slimkey'd your drive and obtained a dummy.bin. This should be loaded as source and allowed to auto-load iXtreme Firmware as target

.

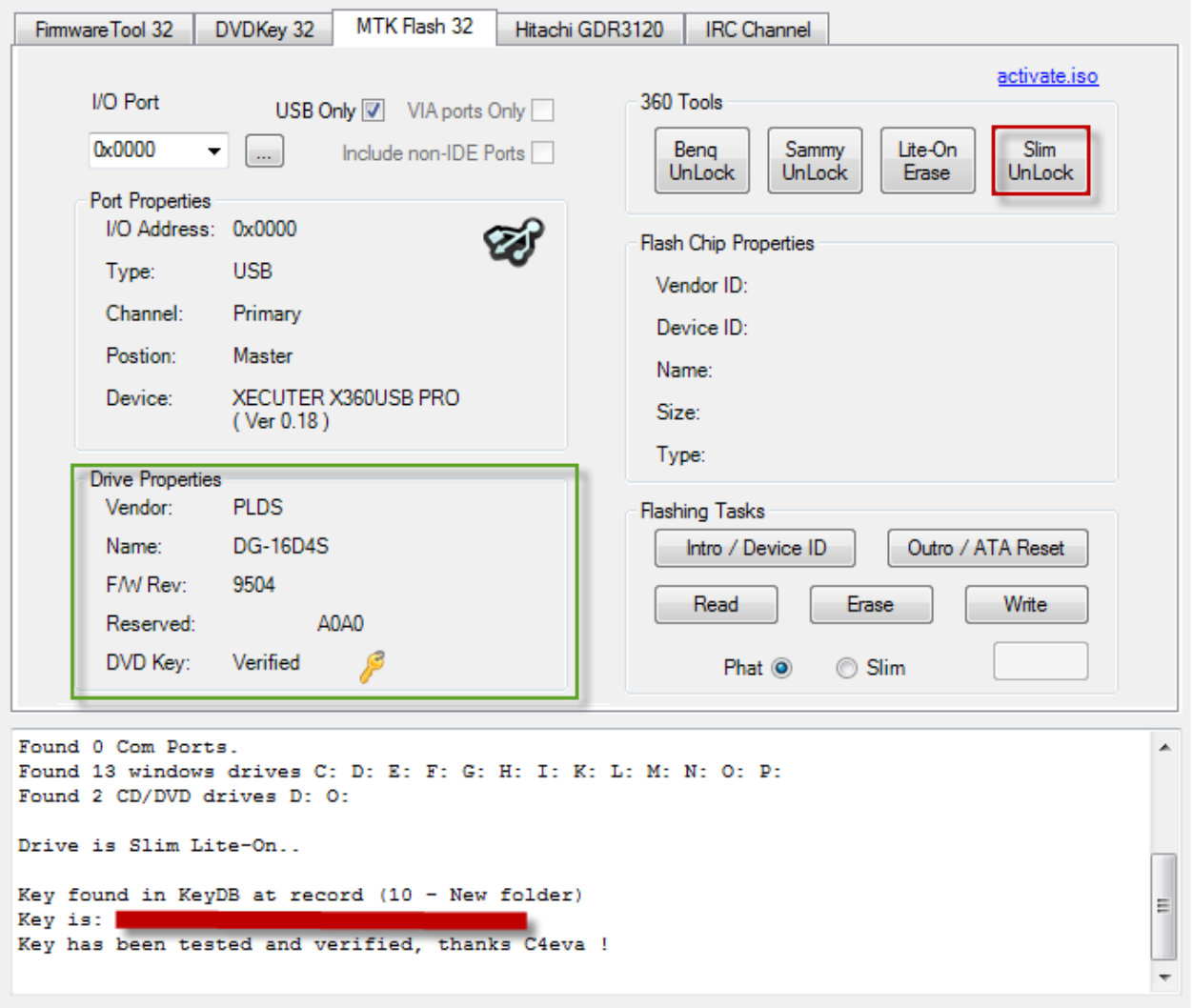


Connect your **spare** 9504 PCB

Select **MTK Flash 32** Tab

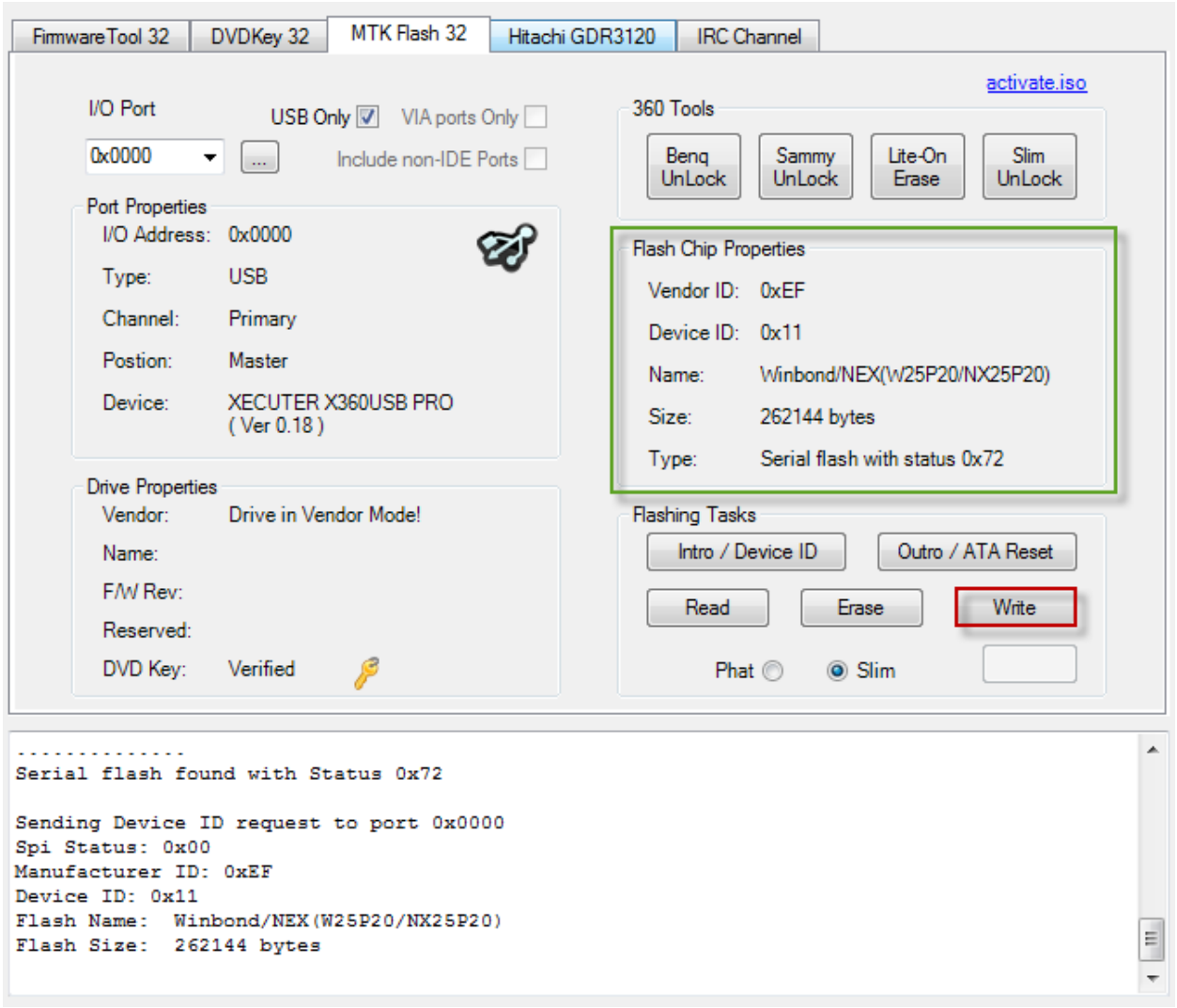
Press **Slim UnLock** Button

Things not going as expected? – Read the FAQ's



The screen should now show the drive in vendor mode (Unlocked)

Things not going as expected? – Read the FAQ's



Press the **Write** Button

The log window will scroll through the operation as it erases, writes and then authorizes the process!

Showing similar to below

Things not going as expected? – Read the FAQ's

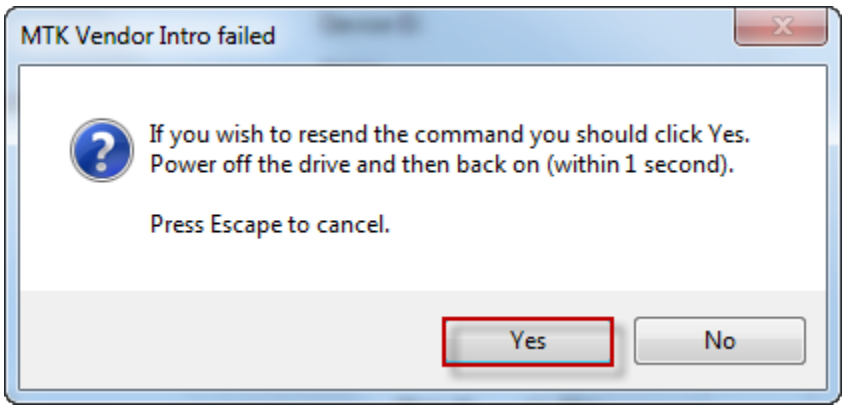
```
Getting Status from port 0x0000
Invalid Status 0x50
Sending Vendor Intro to port 0x0000
Status 0x51
Re-sending Vendor Intro:
..................
Serial flash found with Status 0x72

Sending Device ID request to port 0x0000
Spi Status: 0x00
Manufacturer ID: 0xEF
Device ID: 0x11
Flash Name:  Winbond/NEX(W25P20/NX25P20)
Flash Size:  262144 bytes

Getting Status from port 0x0000
SPi flash found with Status 0x72

Sending Chip Erase to Port 0x0000
Erasing:
Writing target buffer to flash
Writing Bank 0: ................
Writing Bank 1: ................
Writing Bank 2: ................
Writing Bank 3: ................
............
Flash Verification Test !
Reading Bank 0: ................
Reading Bank 1: ................
Reading Bank 2: ................
Reading Bank 3: ................
Dumped in 4792mS

Write verified OK !

Restoring sector 0x3E000.

Sending Sector Erase to Port 0x0000
Erasing: 0x3E000
Writing: 0x3E000
............
Authorised !
..............
Restore verified OK !
Drive is Slim Lite-On..

Key found in KeyDB at record (10 - New folder)
Key is: [redacted]
Key has been tested and verified, thanks C4eva !
```

This is what you should see appearing in the log as you write to the drive

Now you must Lock the Spi if you intend to use this on Xbox live

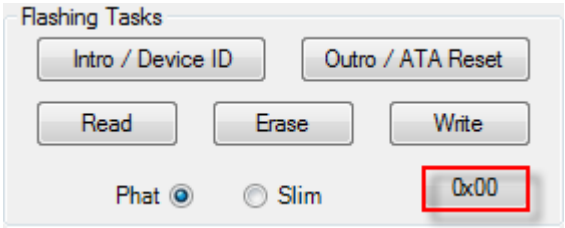
Then press **Intro / Device ID**

This box will appear

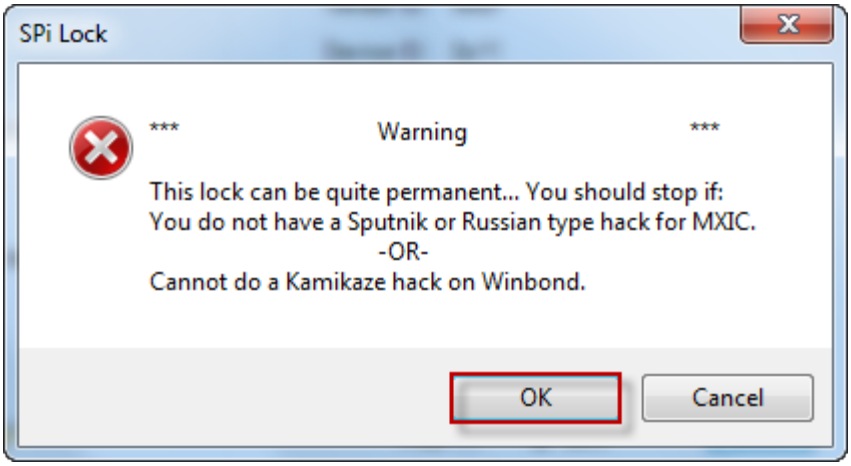


Press the **Spi-Lock Status** Button

Currently displaying **0x00**



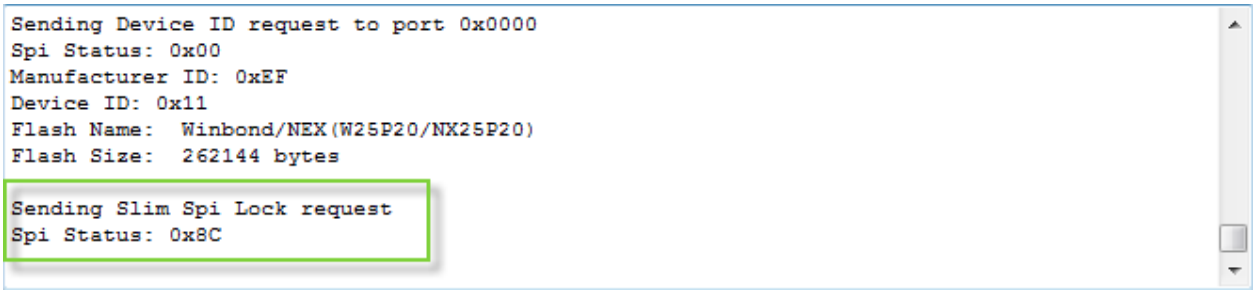
You will see this warning



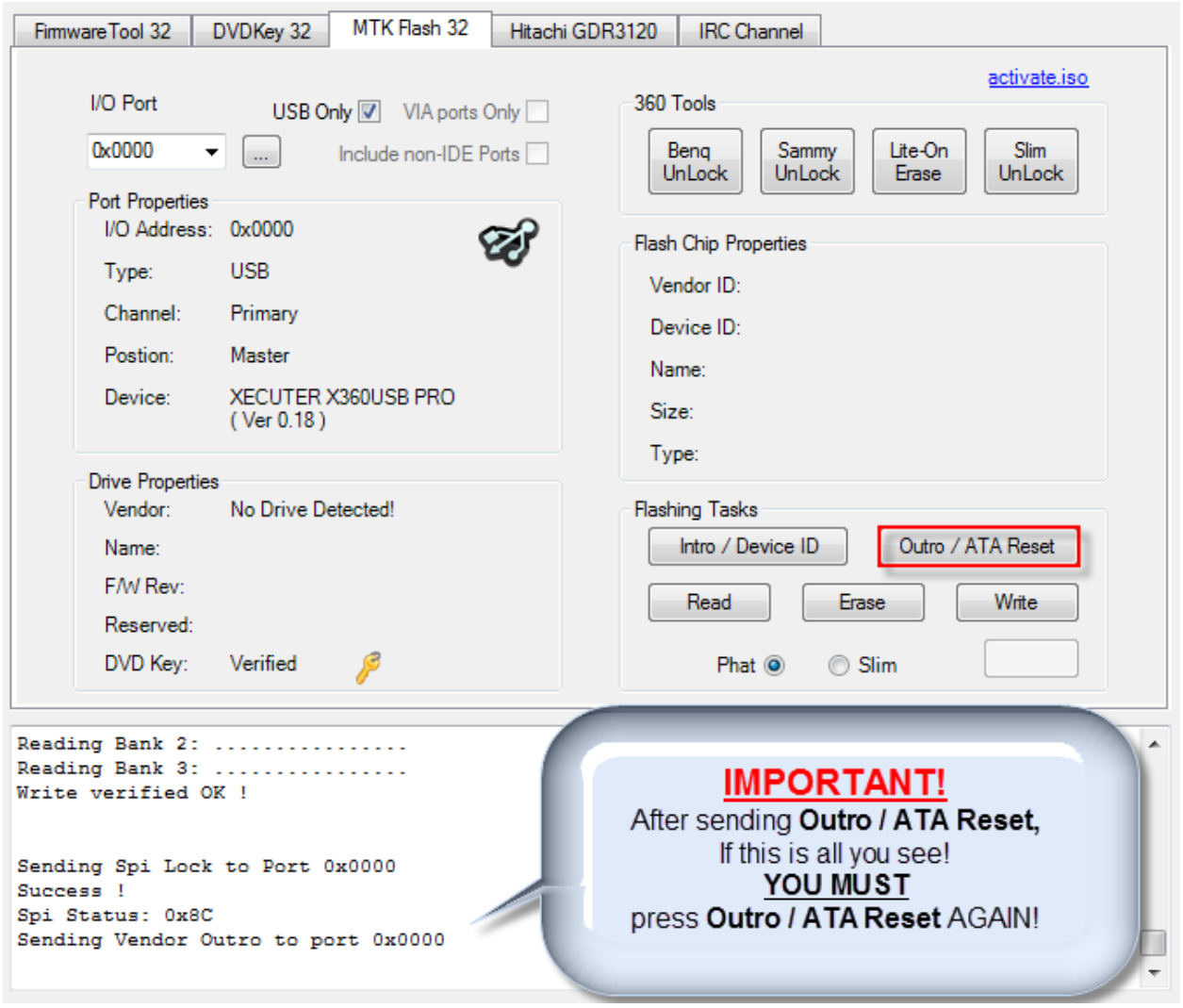
Heed this warning – once locked you will require hardware modification to unlock the PCB in the future!

Click **OK**

You should see the Spi lock message in the log and the button will show **0x8C like** this:



Now press **Outro/ATA Reset** button



Now Power off the drive, disconnect and refit to your xbox and test!

Things not going as expected? – Read the FAQ's

YOU ARE FINISHED – CLICK HERE TO RETURN TO START

Unlocking a Slim Liteon PCB

There are 2 differing vendor producers of LiteOn PCB Chips:

Open your Drive and look at the Main IC on the PCB (click on the chip you have)

Things not going as expected? – Read the FAQ's

MXIC UNLOCKING

There are several methods to unlock these PCB's, we will only mention the 3 main ones here. They all work on exactly the same principle any way. And their use is almost identical.

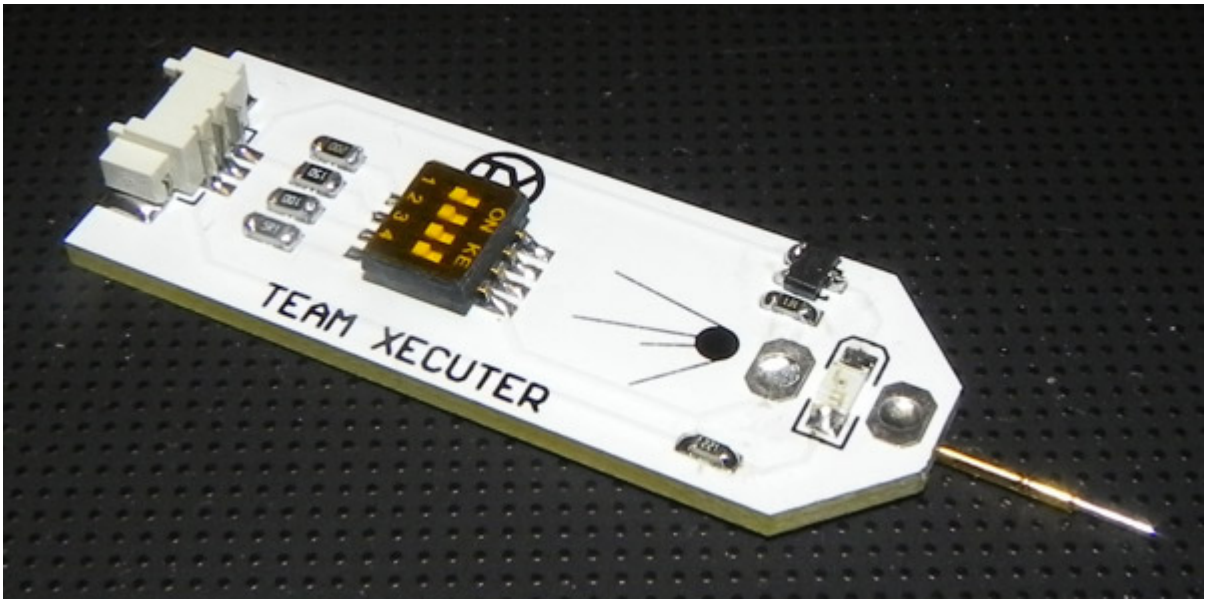
1. The Sputnik360 MX Edition PCB from Team-Xecuter

A simple to fit PCB with switch and selectable resistors. Makes this a very easy to use unlock solution.

1 simple trace cut and 3 solder points will permanantly attach to the PCB in your drive. This will make future updating of firmware simple as can be.

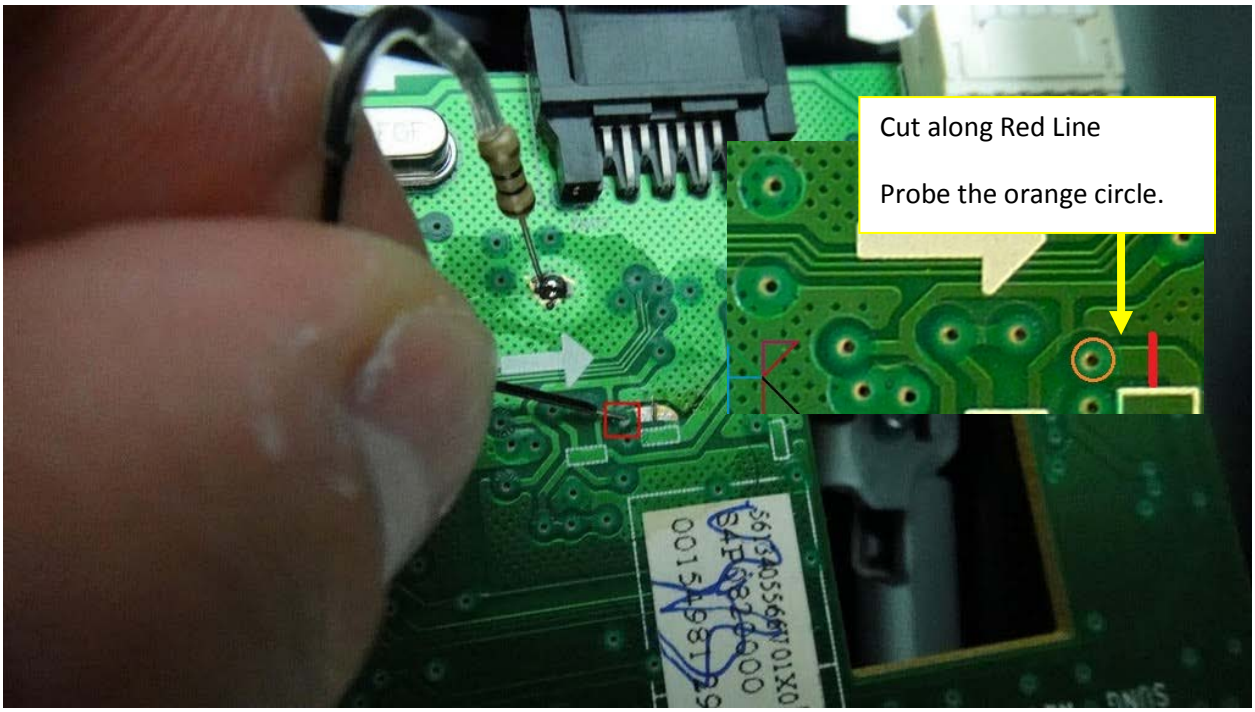
Or

2. The Sputnik MX Probe



Make the same trace cut shown below and use it to probe same via point

3. The Basic Russian Hack



(Thanks to whoever posted this picture on the net! -)

Things not going as expected? – Read the FAQ's

This involves 1 trace cut and soldering a 10 Ω(approx) Resistor to GND – then momentarily touching the VIA that you cut from the trace(at the appropriate time)

Either method – proceed as follows

CLICK HERE TO CONTINUE

WINBOND UNLOCKING

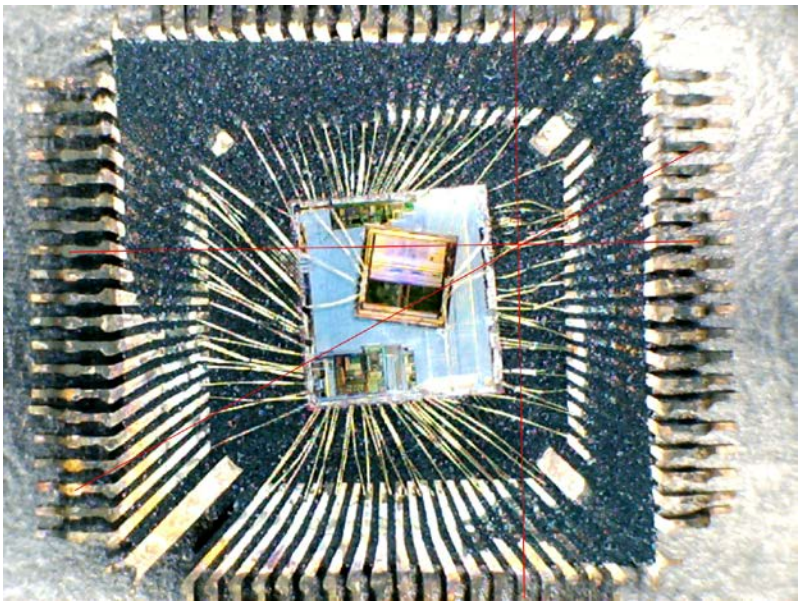
Kamikaze Unlock

WARNING: THIS LOOKS EASY – BUT IT CAN BE MESSED UP VERY VERY EASILY.

Using this method, it is very easy to cut wrong wire, or more than 1 wire- destroying the chip and rendering it useless! –

DO NOT START COMPLAINING IF YOU MESS THIS UP – YOU HAVE BEEN WARNED

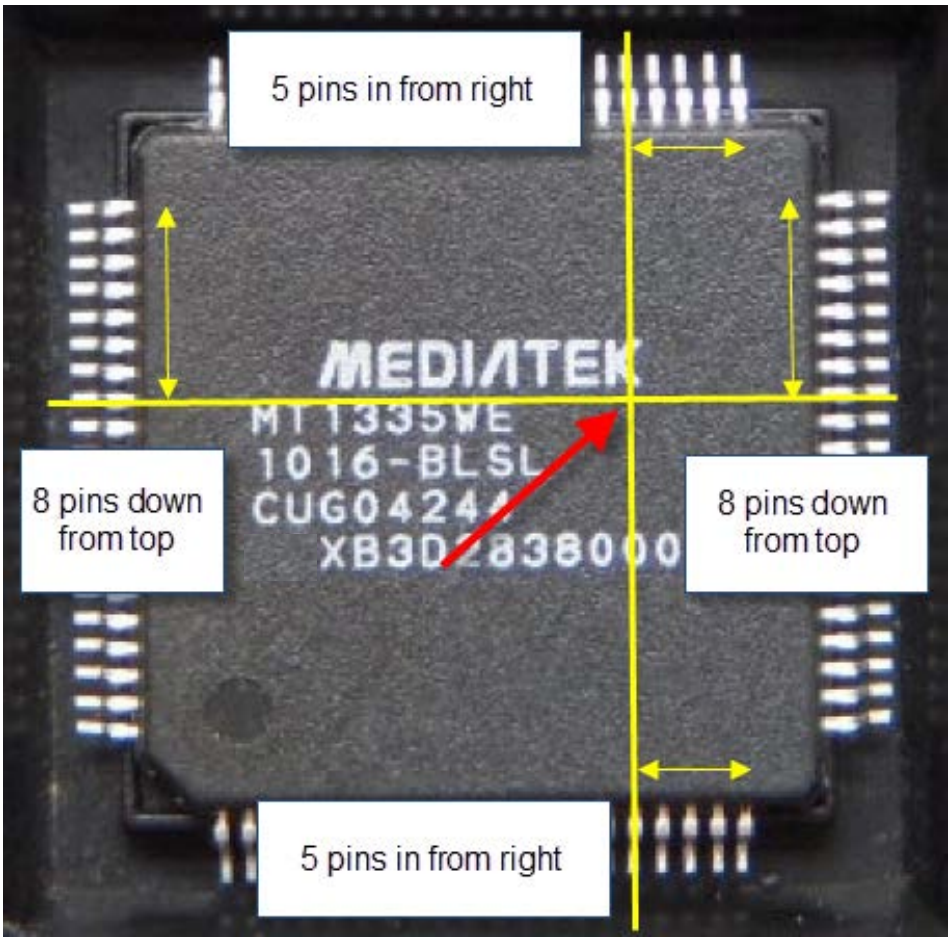
This involves cutting into the IC with a Dremel whilst providing 3.3v with a 100 Ω capacitor in series at the Dremel tip and sending SPI unlock command at the same time! The picture below show the complexity and point you are aiming to cut!



Please research as much on this method as possible before even considering using it! (It wasn't named **Kamikaze Unlock Method** for nothing)

You must first be as accurate as possible and mark the top of the chip with the correct point at which you are aiming to find the correct internal wire. The picture below shows the location of the point!

DO NOT RELY ON THE WHITE TEXT ON THE CHIP - IT VARIES IN POSITION FROM CHIP TO CHIP!



(Uninstalled chip shown for clarity)

Measure 5 pins in from the right (on the top and bottom row of pins) mark the line with a very thin bladed scalpel and steel rule.

Then measure 8 pins down from the top (on the left and right side pins) mark the line.

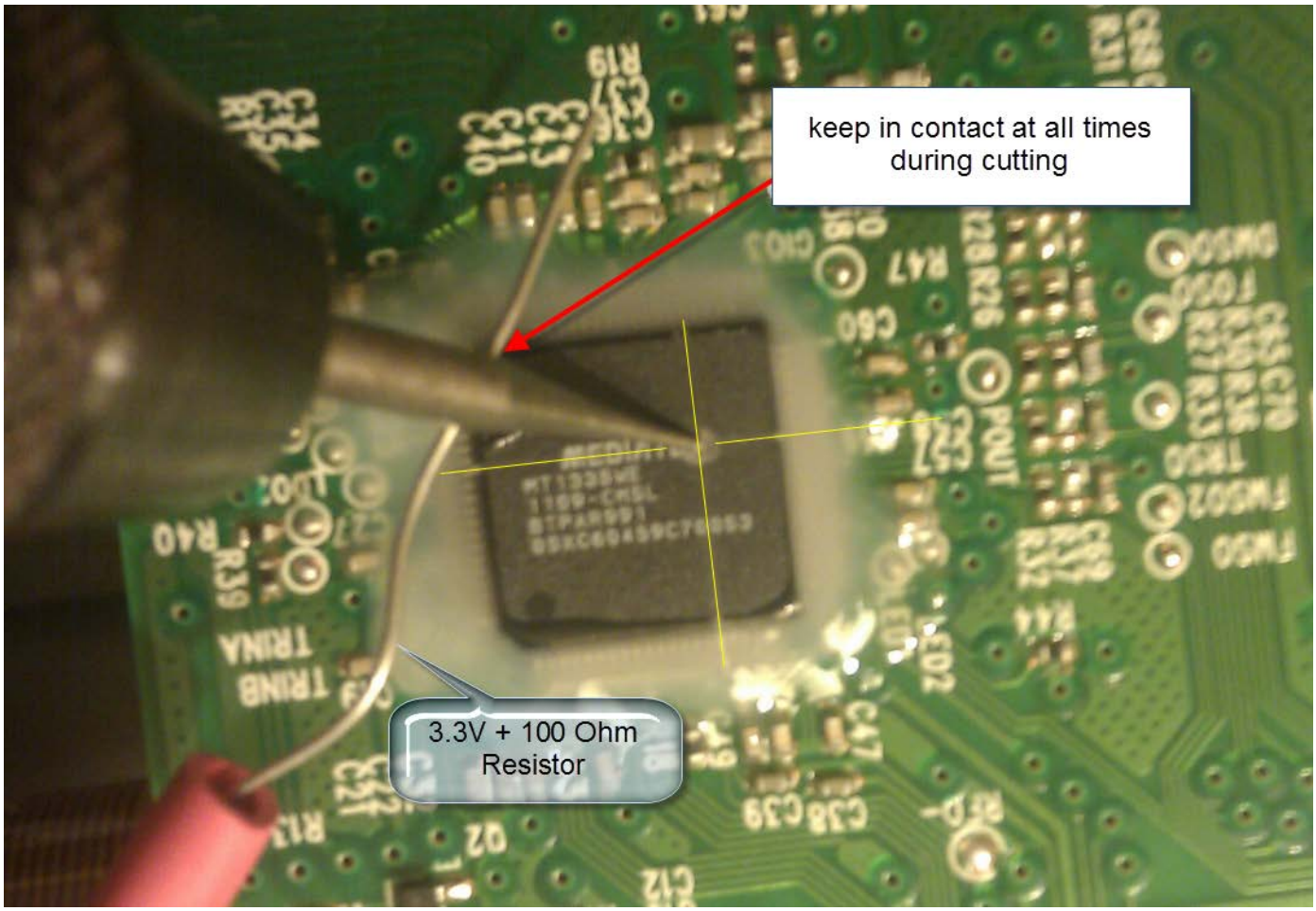
Where these lines cross, is the point you are aiming to cut.

There are several methods to achieve the cut (Dremel, soldering iron, knife)

The Dremel appears to be the most accurate – providing you have a steady hand and good eye. (again, DO NOT ATTEMPT UNLESS YOU ARE SURE YOU UNDERSTAND THE RISKS!)

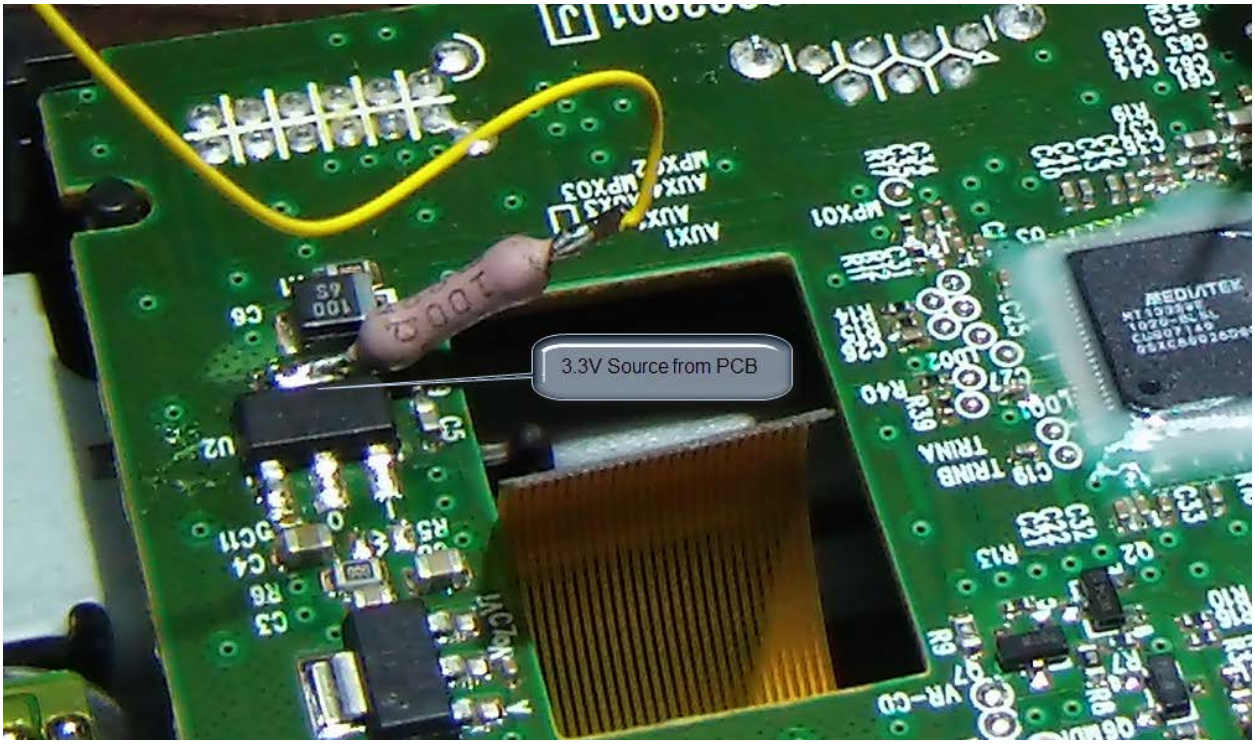
Dremel Method

The method is to slowly perform the grinding whilst contacting the cutting tip with a 3.3v supply with a 100 Ω resistor in the line.



Things not going as expected? – Read the FAQ's

3.3v can be obtained from the PCB itself or from your 3.3V cable in drive power cable (the cable the switch is on, on the probe 3 cable)



3.3V source on PCB

The important thing is accuracy and very light pressure! Cutting slowly to ensure you don't overcut and destroy other wires in the chip. Listen for the BEEP and keep a check on the screen status! (Dremel tip used here is 0.8mm cutting head).

TEAM JUNGLE and Jungleflasher author take no responsibility if you screw your drive using this method! – It is awkward and fiddly. If you don't feel confident then pay someone to do the job for you!

CLICK HERE TO CONTINUE

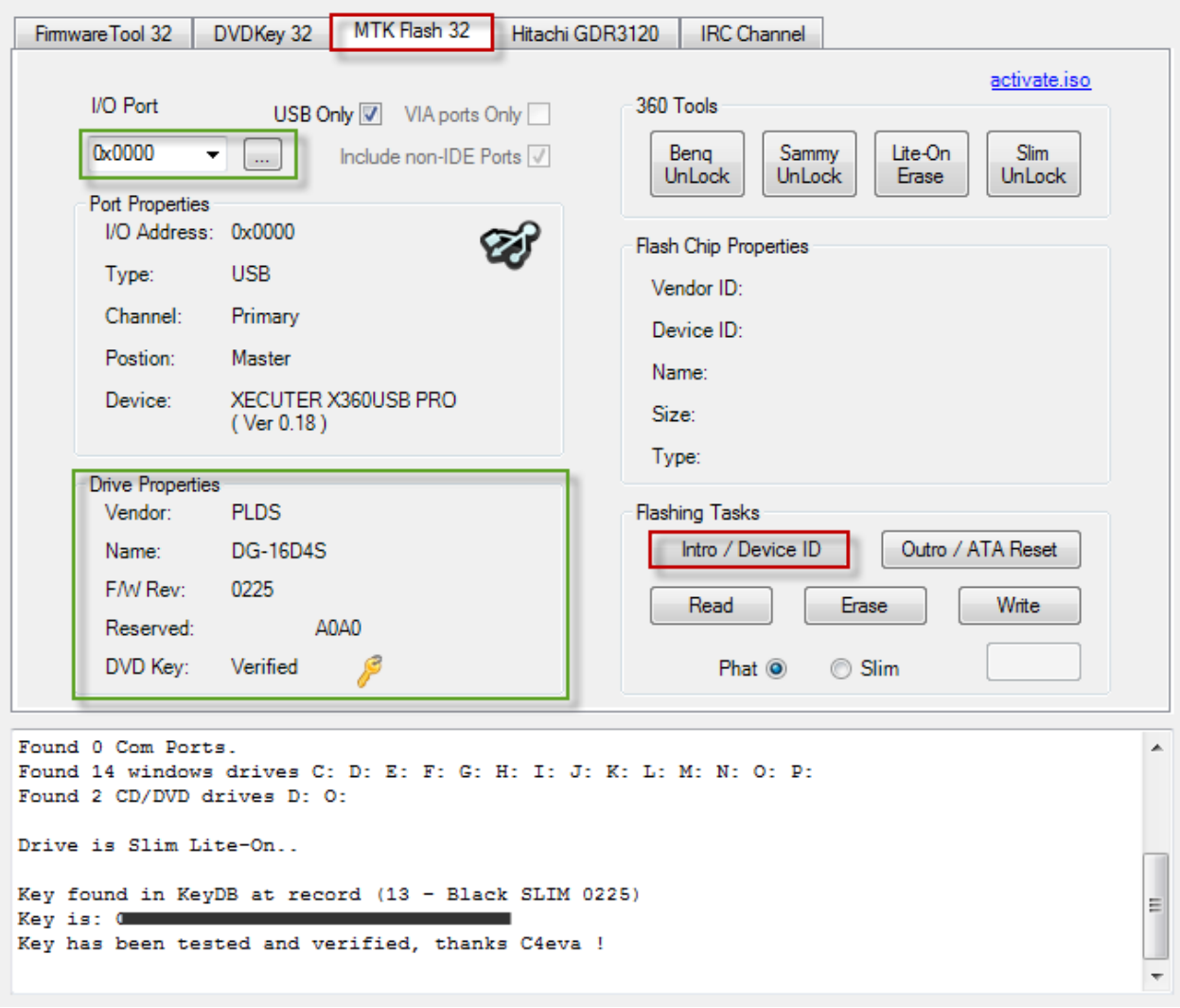
Locked Slim LiteOn Drives

First – You should have prepared your Winbond or MXIC unlock method in advance.

Then open Jungleflasher, select **MTK Flash 32 Tab**

Select the correct **I/O port**

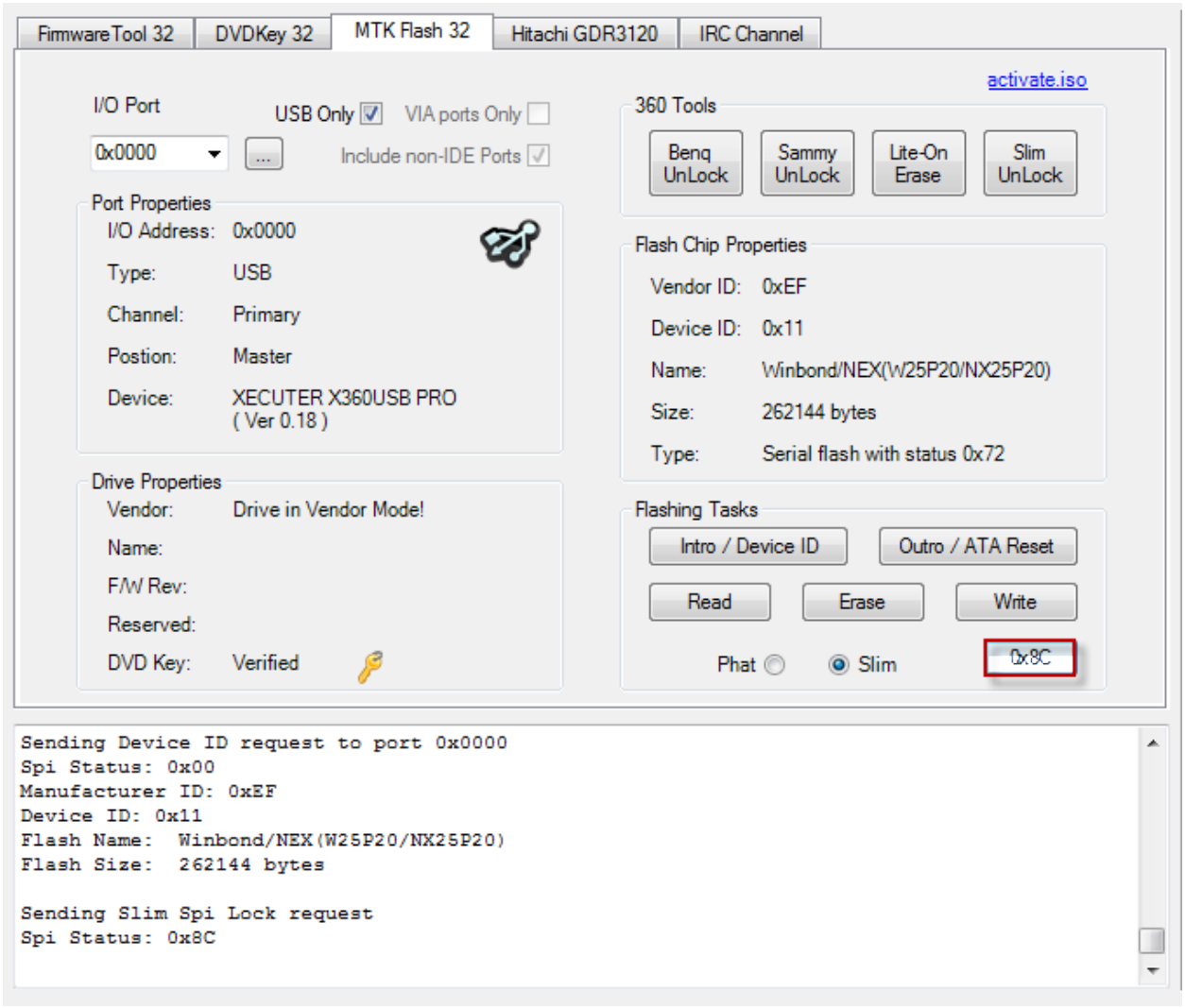
Power on your drive, click **I/O Port refresh button** and ensure drive properties show up



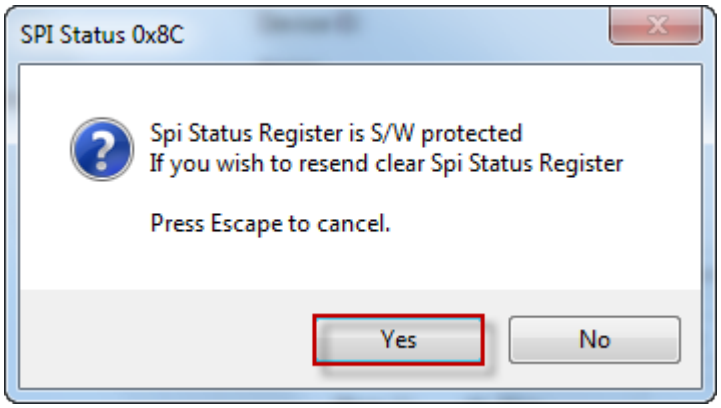
Now Press **Intro / Device ID** button

Things not going as expected? – Read the FAQ's

Once in vendor mode, Press the Spi Status Button (currently showing **0x8C**)



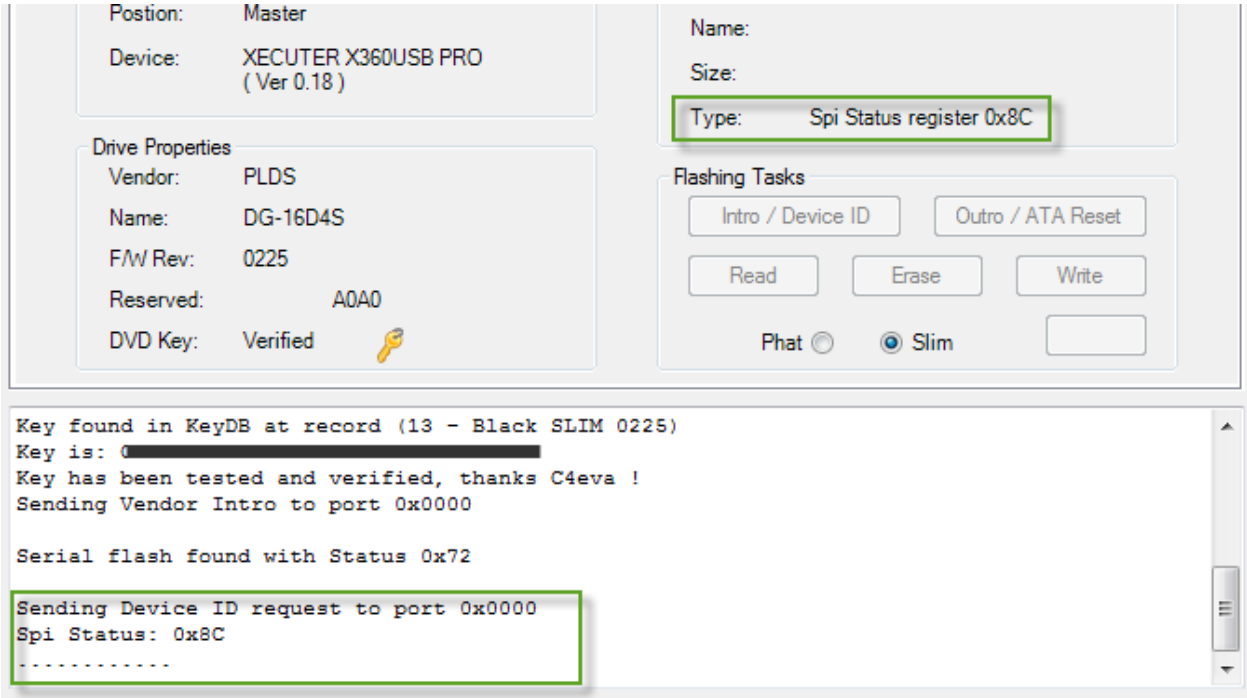
Because your drive has a locked Spi – this message will show up



Things not going as expected? – Read the FAQ's

Press **Yes**

Jungleflasher will now start to continuously send the unlock command to the drive. This will be shown in the log, represented by appearing dots …….



At this point you commence with which ever unlock procedure you are following

NOTE: FOR EASE ENSURE YOUR SPEAKERS ARE ON AND VOLUME IS UP AS AN AUDIBLE BEEP WILL OCCUR WHEN YOU ACHIEVE AN UNLOCKED STATUS OF 0x00

Dependent on your drive Vendor Manufacturer and the method you are attempting to unlock the drive – choose the appropriate item from the table below.

UNLOCK PROCEDURE OF CHOICE

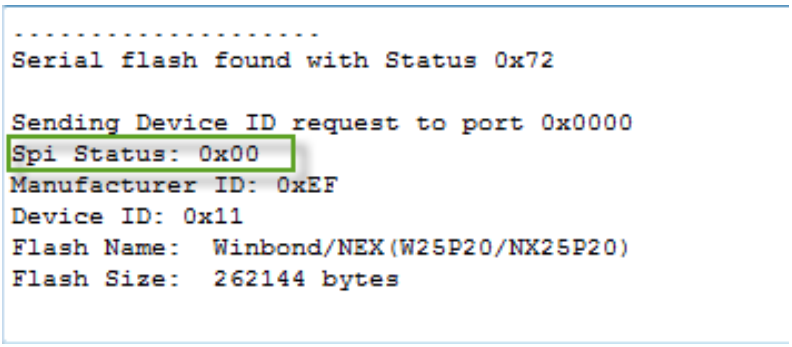
Things not going as expected? – Read the FAQ's

<table>
<tr><th>MXIC</th><th>WINBOND</th></tr>
<tr><td>a. Put switch to unlock on SPUTNIK360 MX Switch</td><td rowspan="3">Start up your Dremel, and begin grinding (ensuring you have the 3.3v power supply with resistor in contact with the Dremel tip)

“SLOWLY DOES IT!”

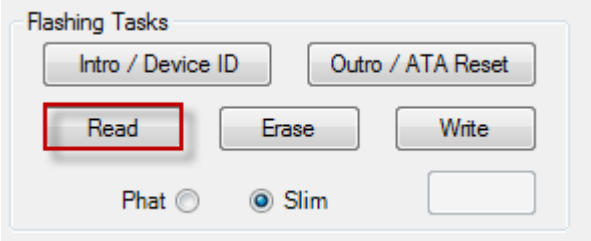
Good Luck!</td></tr>
<tr><td>b. Probe the VIA (Sputnik360 MX Probe)</td></tr>
<tr><td>c. Probe The VIA (Russian hack wire)</td></tr>
<tr><td colspan="2">PREVIOUSLY UNLOCKED DRIVES</td></tr>
<tr><td>Carry out as above</td><td>Simply touch same 3.3v +100 Ω wire in hole – Or drop a little rubbing alcohol(or similar) into hole</td></tr>
</table>

At the point that Jungleflasher is able to successfully unlock the drive – a “**DUAL-TONE BEEP**” will be heard through your speakers and you should see this

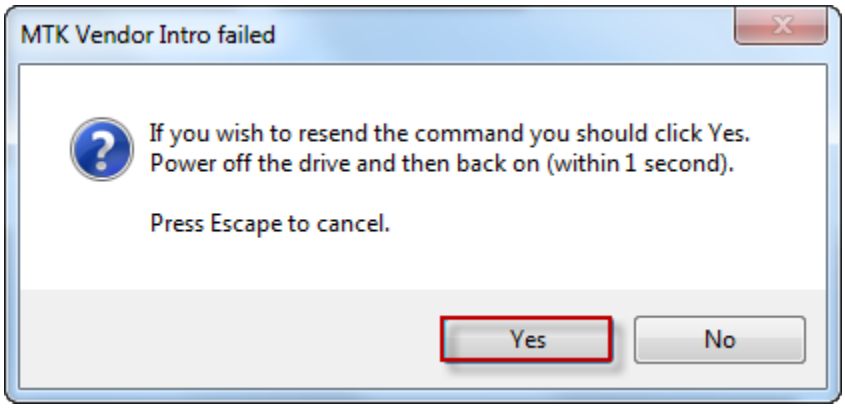


(once 0x00 has been achieved – stop probing / switch sputnik back to normal /stop dremeling)

Now as always, read the Original Firmware from the drive for safe keeping, by pressing the **Read** button



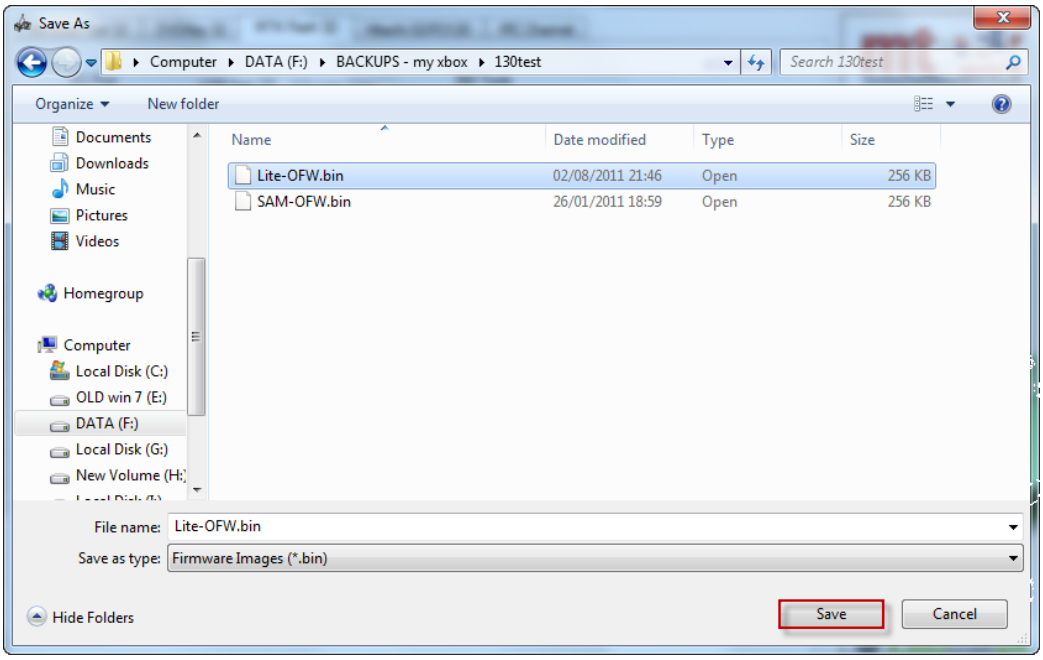
as part of the read you will be faced with this



Click **YES** then Cycle the power to the drive **OFF then ON**

You will then be asked to save your Firmware – DO SO!

This is your Original Firmware (stock) keep it safe

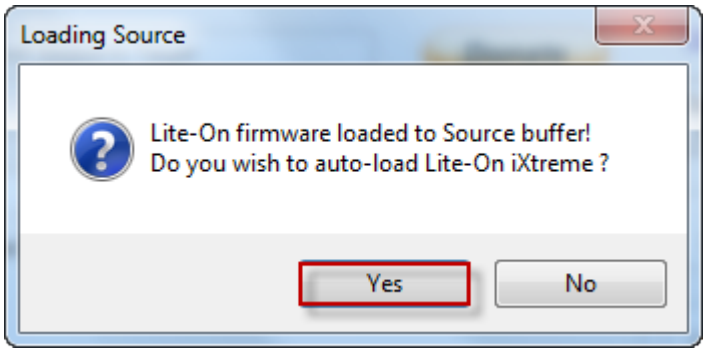


Click **Save**

Your firmware will automatically be loaded into source in the **Firmware** Tab

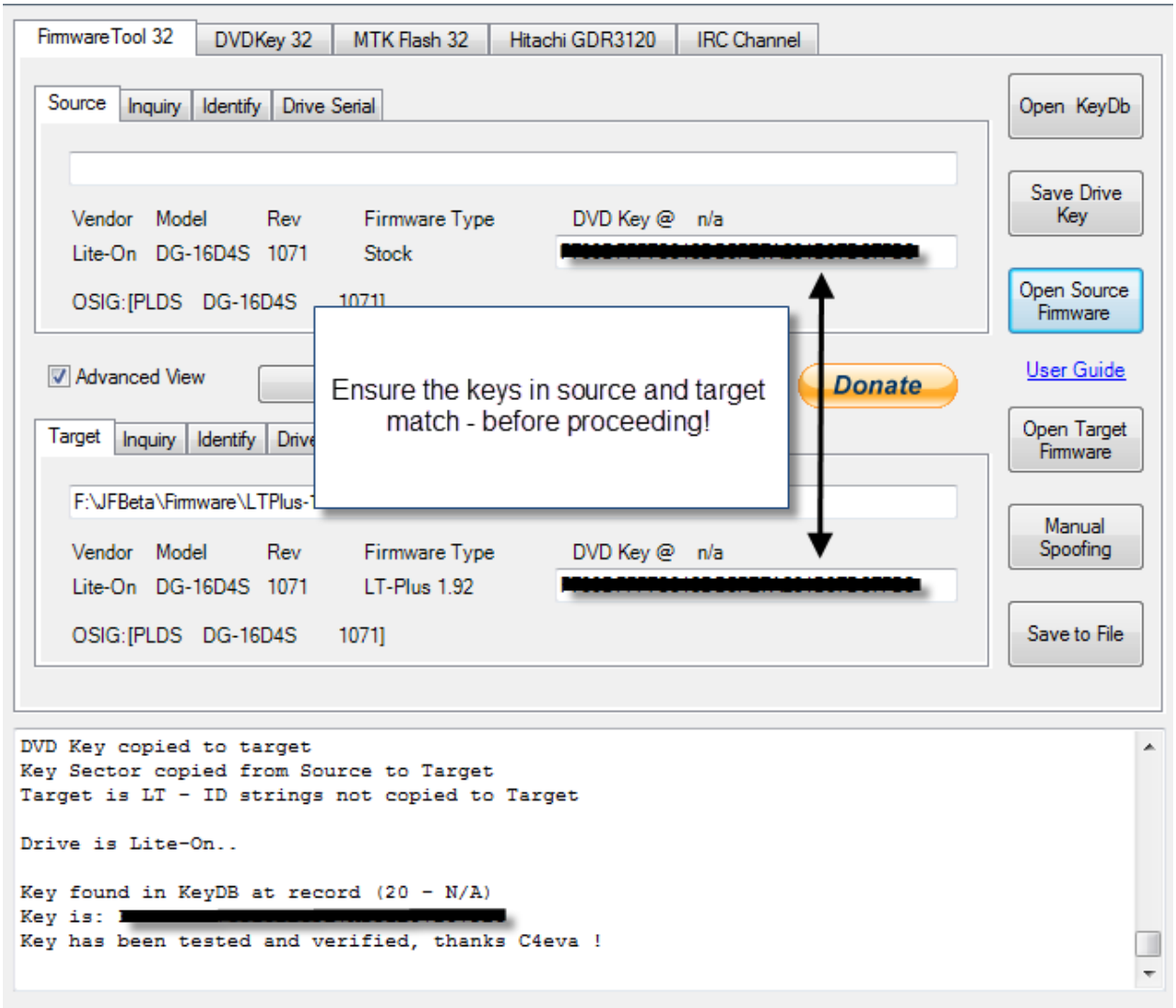
You will then be asked if you wish to autoload iXtreme.

Click **YES**



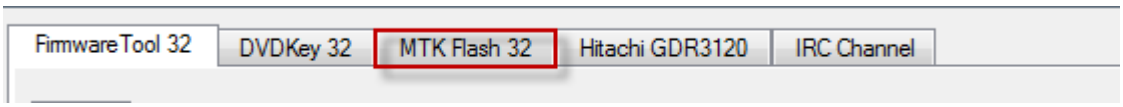
The latest firmware will be autoloaded from the firmware folder (where you should have placed it earlier)

And your drive details will be spoofed into the firmware in target buffer, ready to be written to the drive.



To write the prepared firmware to the drive you must place the drive into vendor mode once again.

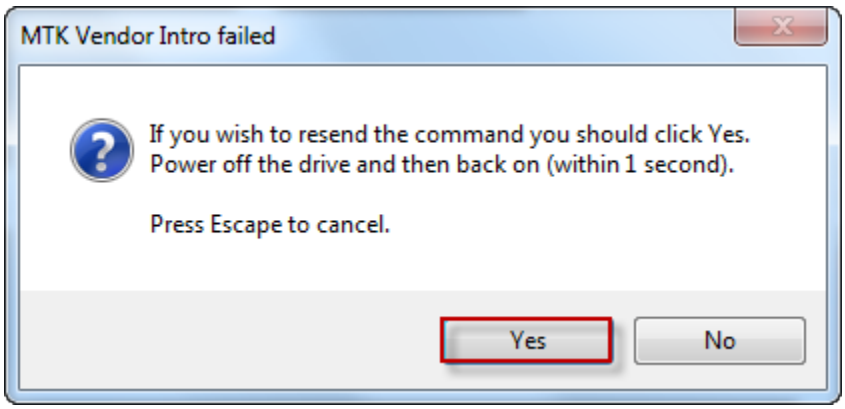
Simply select **MTK Flash 32** tab



Now press **Intro / Device ID** button

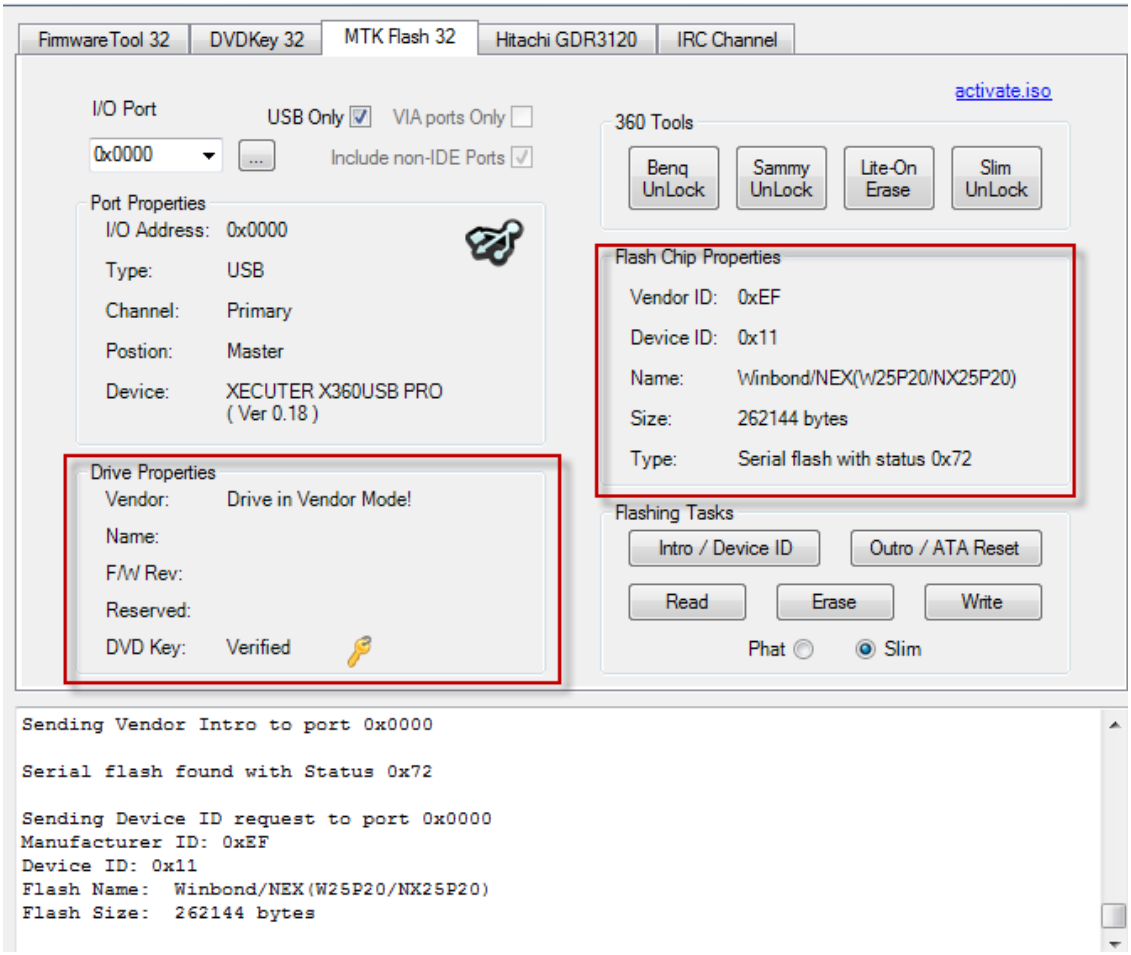
You may or may not be asked to resend and power cycle

Things not going as expected? – Read the FAQ's



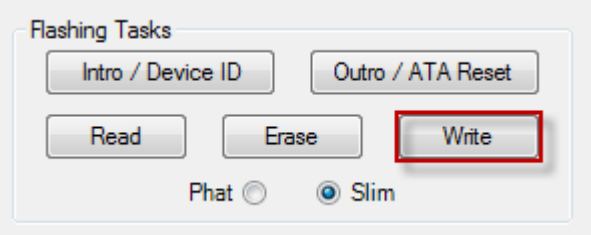
If so – click **YES** then Cycle the power to drive!

The drive should appear in vendor mode once again



Now the drive is in Vendor Mode, select the **Write** Button

Things not going as expected? – Read the [FAQ's]



Writing will commence and its progress shown in the log

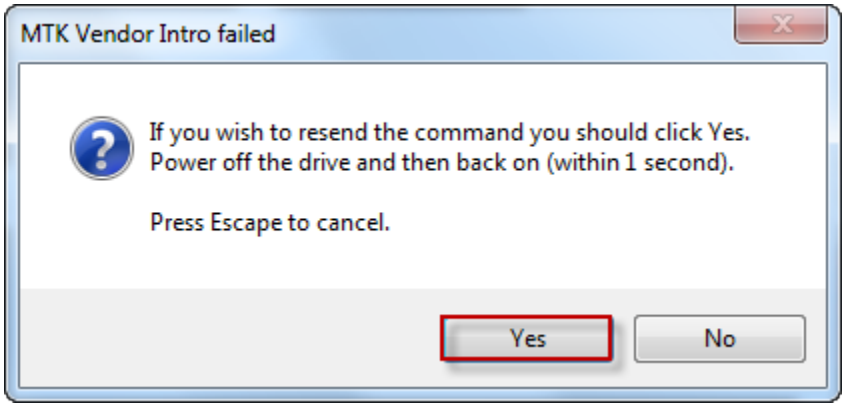
```
Getting Status from port 0x0000
SPi flash found with Status 0x72

Sending Chip Erase to Port 0x0000
Erasing:
Writing target buffer to flash
Writing Bank 0: ................
Writing Bank 1: ................
Writing Bank 2: ................
Writing Bank 3: ................
............
Flash Verification Test !
Reading Bank 0: ................
Reading Bank 1: ................
Reading Bank 2: ................
Reading Bank 3: ................
Dumped in 4912mS

Write verified OK !

Restoring sector 0x3E000.

Sending Sector Erase to Port 0x0000
Erasing: 0x3E000
Writing: 0x3E000
............
Authorised !
................
Restore verified OK !
Drive is Lite-On..

Key found in KeyDB at record (20 - N/A)
Key is: [redacted]
Key has been tested and verified, thanks C4eva !
```

Now to RE-LOCK the drive!

To re-lock the drive it must be in vendor mode

So once again – Press **Intro /Device ID**

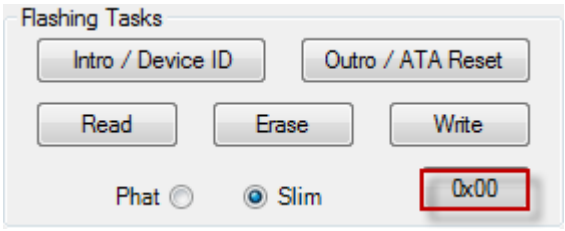
You will be asked to resend and power cycle



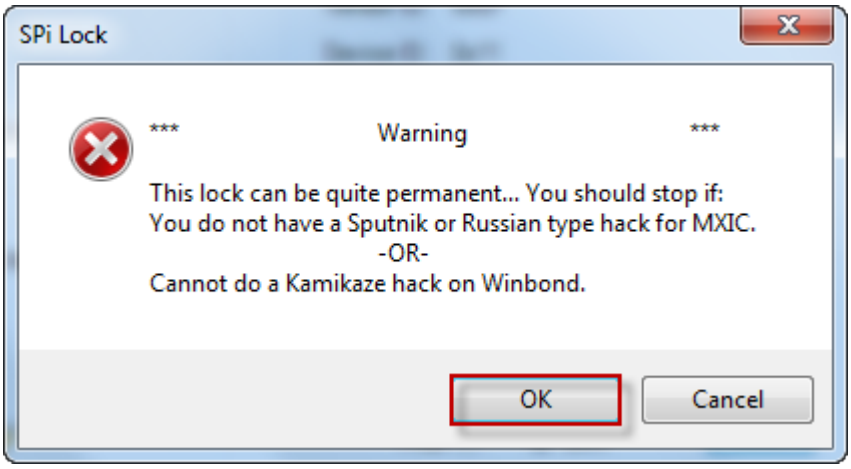
click **YES** then Cycle the power to drive!

The drive should appear in vendor mode once again

Simply press the Spi Status Button (currently 0x00)



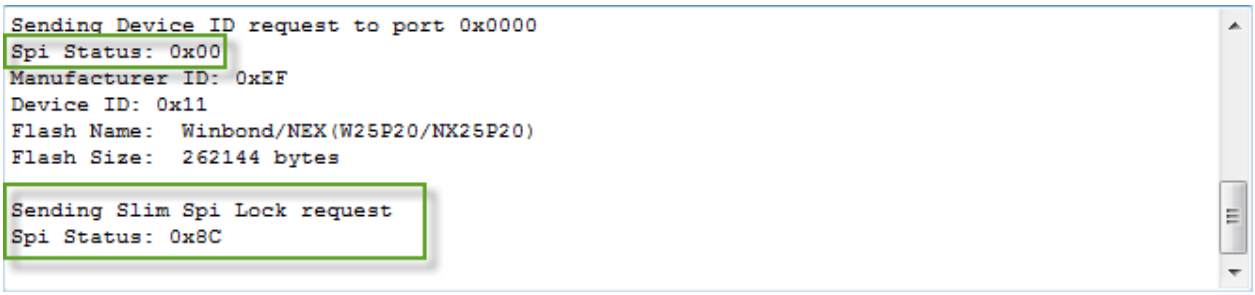
The following warning will appear



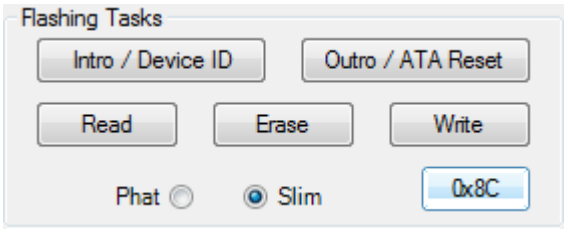
Click **OK**

You should see the following in the log

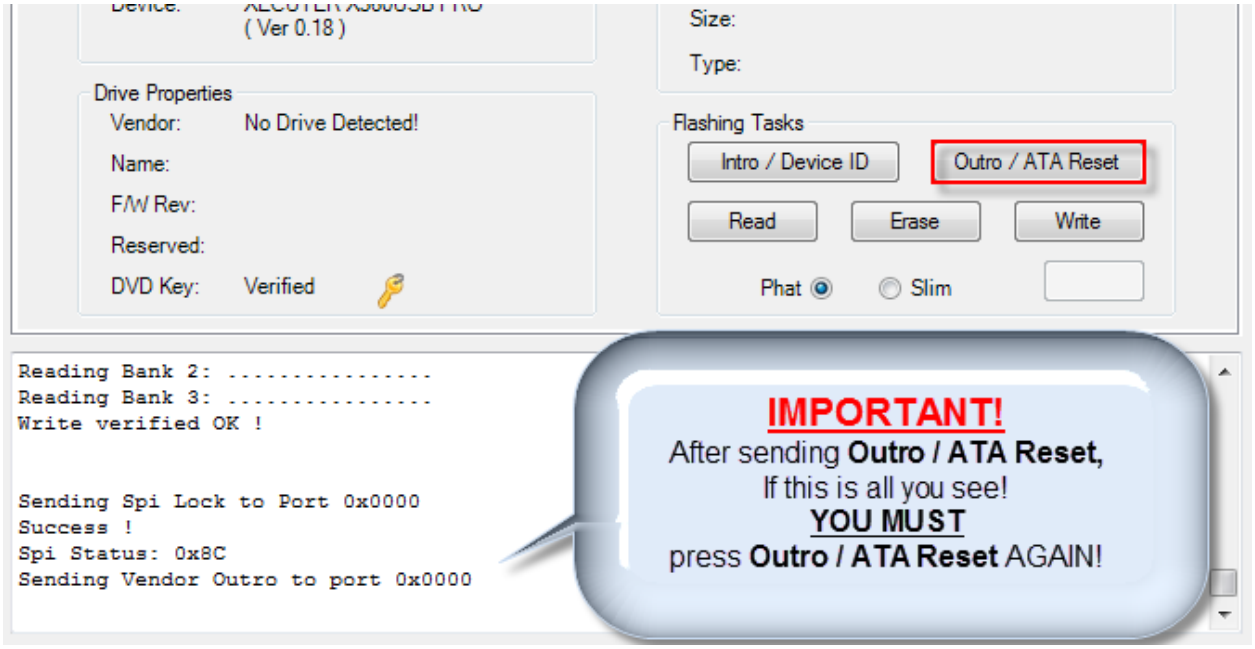
Things not going as expected? – Read the FAQ's



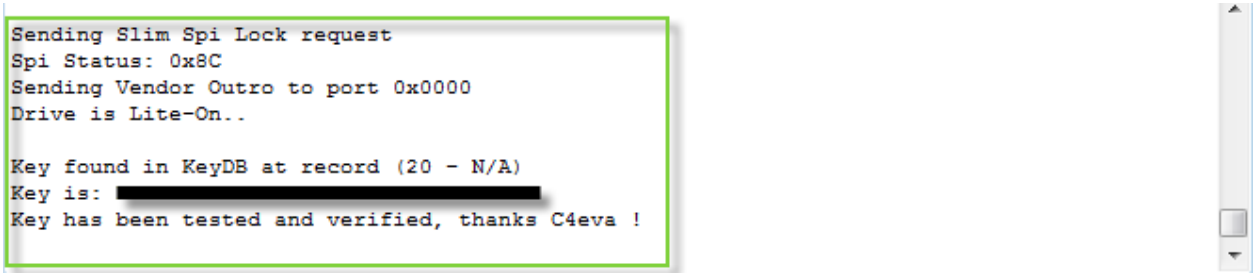
And the Spi Status Button should now show **0x8C**



Now press **Outro/ATA Reset** button



If you see this Key Verification message then – Outro has been successful



Now Power off the drive, disconnect and refit to your xbox and test!

YOU ARE FINISHED – CLICK HERE TO RETURN TO START

Things not going as expected? – Read the FAQ's

LiteOn Slim FW Ver. 09504 / 0272 (dash 13146)

There are 2 methods available to obtain the drive details you require from this drive. You can either

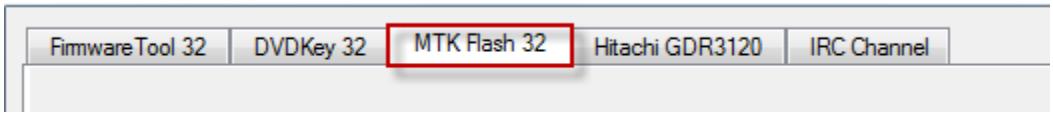
A. **Dump the original Firmware from the drive (always recommended)**

B. **Use SlimKey**

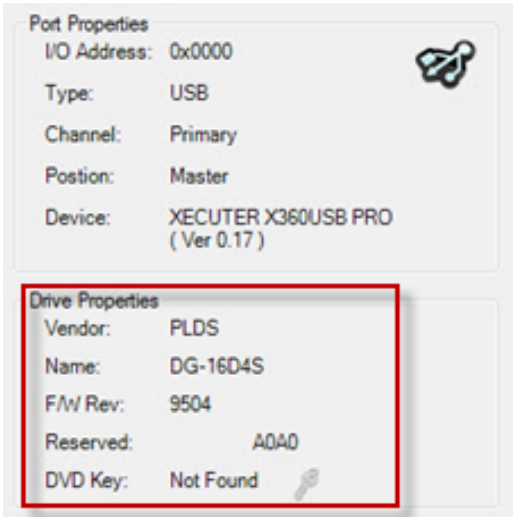
Method A – Dump the original Firmware

Dumping the Original Firmware is very straight forward.

Select **MTK Flash 32** tab

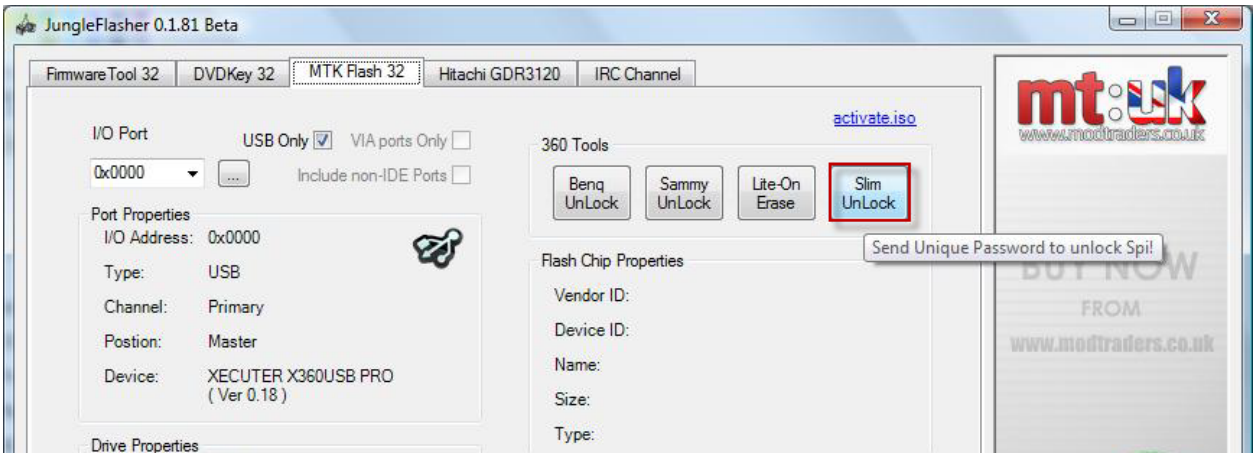


First ensure it inquires on the I/O port.

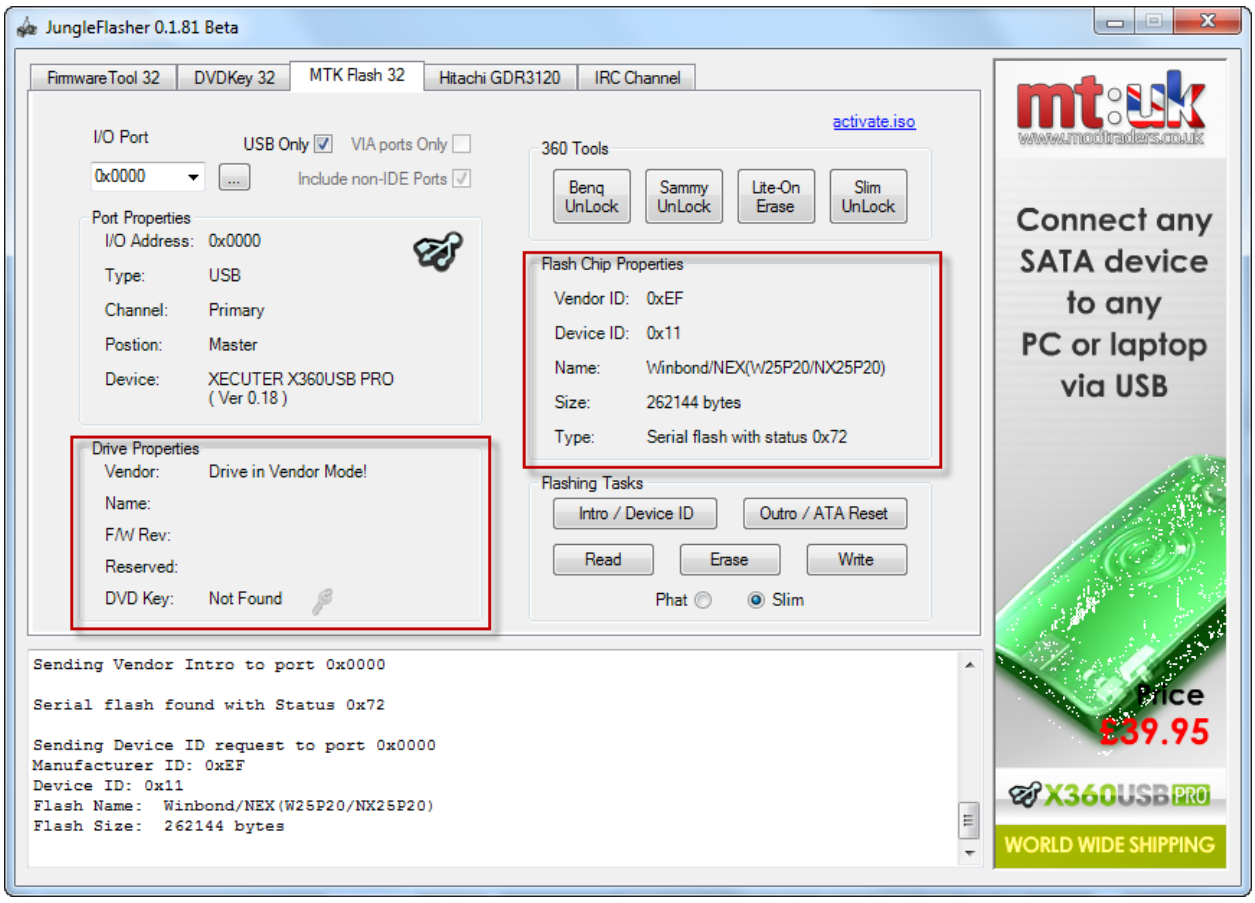


Things not going as expected? – Read the FAQ's

Now select **Slim Unlock**

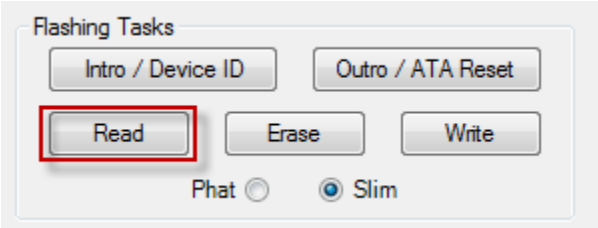


Jungleflasher will unlock the drive and place it into **Vendor Mode**



Things not going as expected? – Read the FAQ's

Now the drive is in Vendor Mode, simply click on the **Read** Button

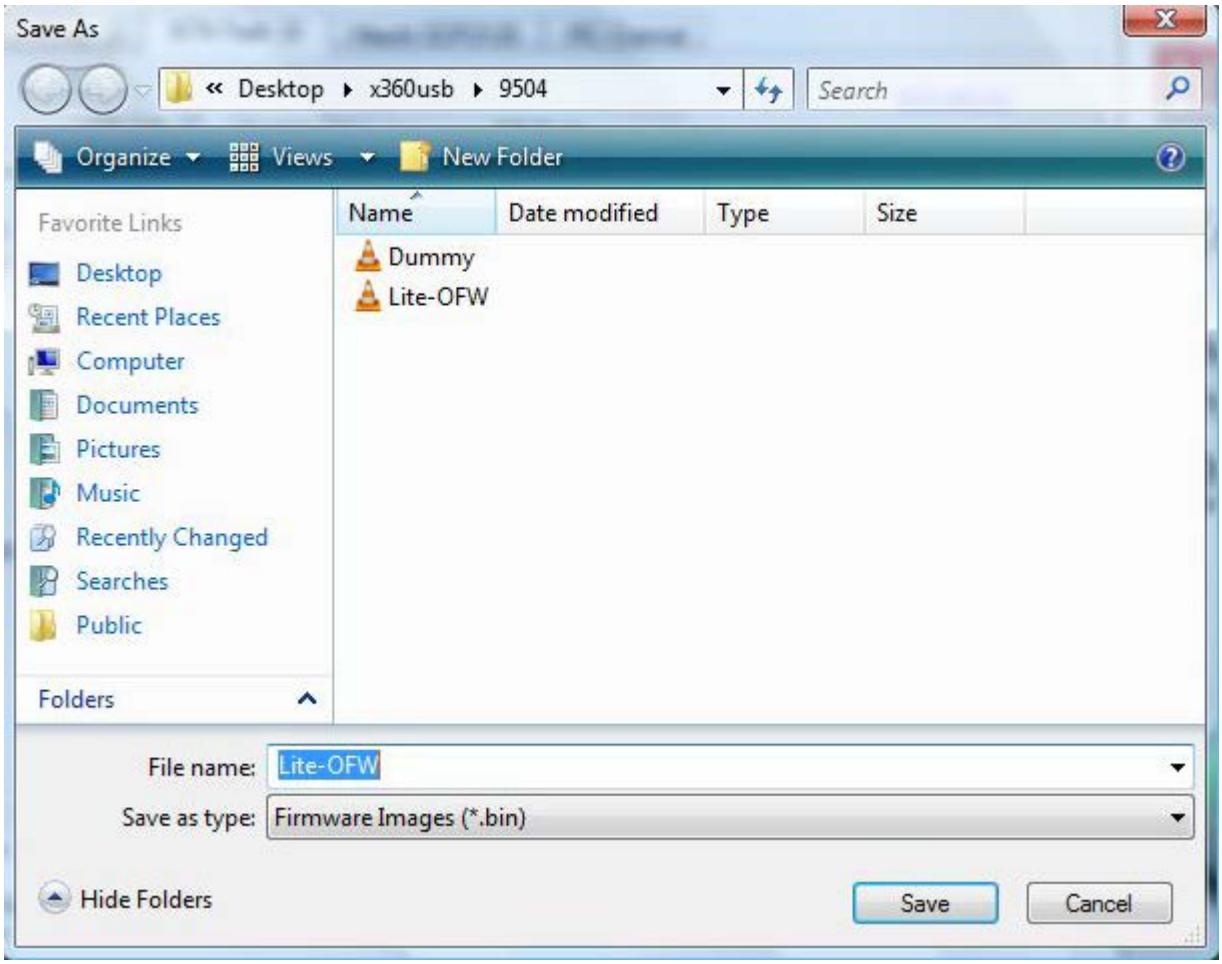


This will produce some text in the log as it reads the original Firmware from the drive

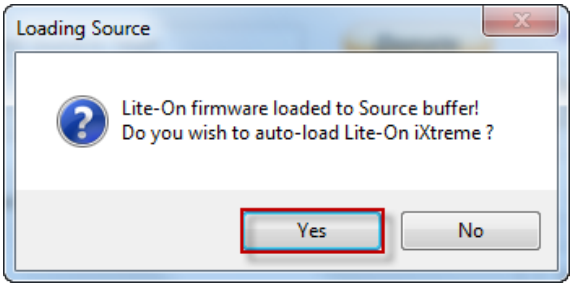
```
Sending Device ID request to port 0x0000
Manufacturer ID: 0xEF
Device ID: 0x11
Flash Name:  Winbond/NEX(W25P20/NX25P20)
Flash Size:  262144 bytes

Updating flash for on-line dump.

Sending Sector Erase to Port 0x0000
Erasing: 0x3E000
Writing: 0x3E000

Reading Bank 0: ................
Reading Bank 1: ................
Reading Bank 2: ................
Reading Bank 3: ................
Dumped in 4828mS

Restoring sector 0x3E000.

Sending Sector Erase to Port 0x0000
Erasing: 0x3E000
Writing: 0x3E000

Authorised !
.
Restore 0x3E000 verified !

Lite-On Dump file saved to Lite-OFW.bin
Loading firmware from buffer
Drive key @ n/a #########REMOVED################
Firmware Osig: [PLDS    DG-16D4S        9504]
Firmware is:  Stock
Key added to database
```

You will also be prompted to save the file you have just dumped. It is recommended you do so!

Note: This is your original firmware – please keep it safe

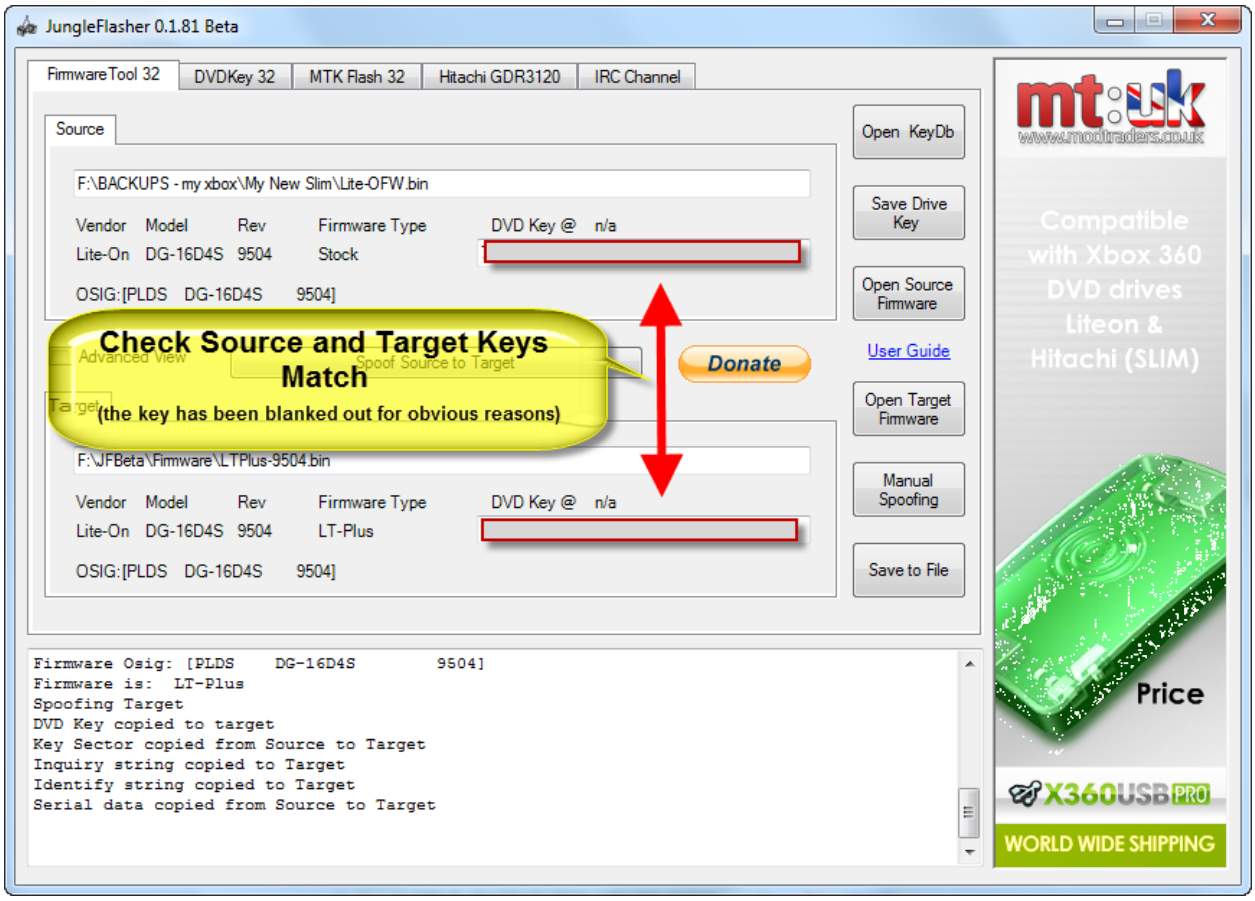


Now Jungleflasher will change to the Firmware Tool 32 Tab and automatically load your OFW as the source. Then ask if you wish to Auto-Load Latest Firmware

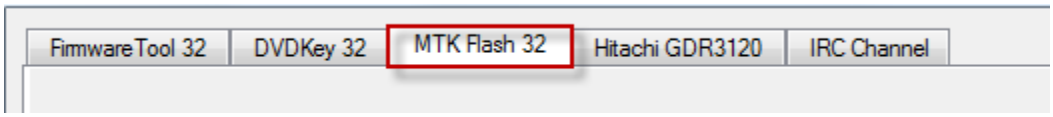


Click yes to Auto-Load the Firmware and Auto-Spoof your data from your drive into the ixtreme.

Things not going as expected? – Read the FAQ's



Now re-select **MT Flash 32** Tab



You will notice in the log that the key has now been Verified against the drive

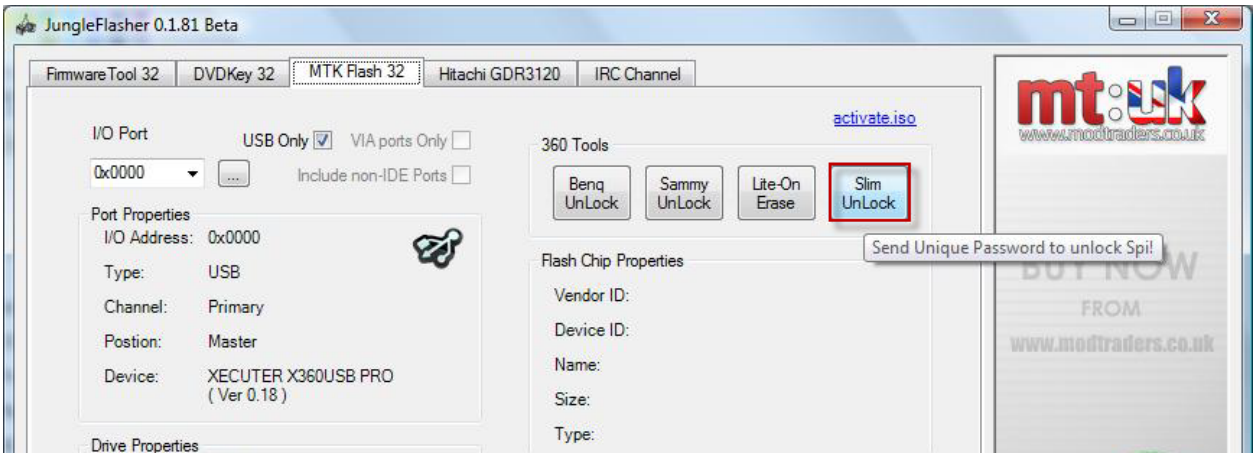
```
Drive is Slim Lite-On..

Key found in KeyDB at record (10 - My New Slim)
Key is: ##########REMOVED################
Key has been tested and verified, thanks C4eva !
```

To be able to write the target firmware to the drive you must unlock the drive once more (it was taken out of Vendor mode to Verify the Key)

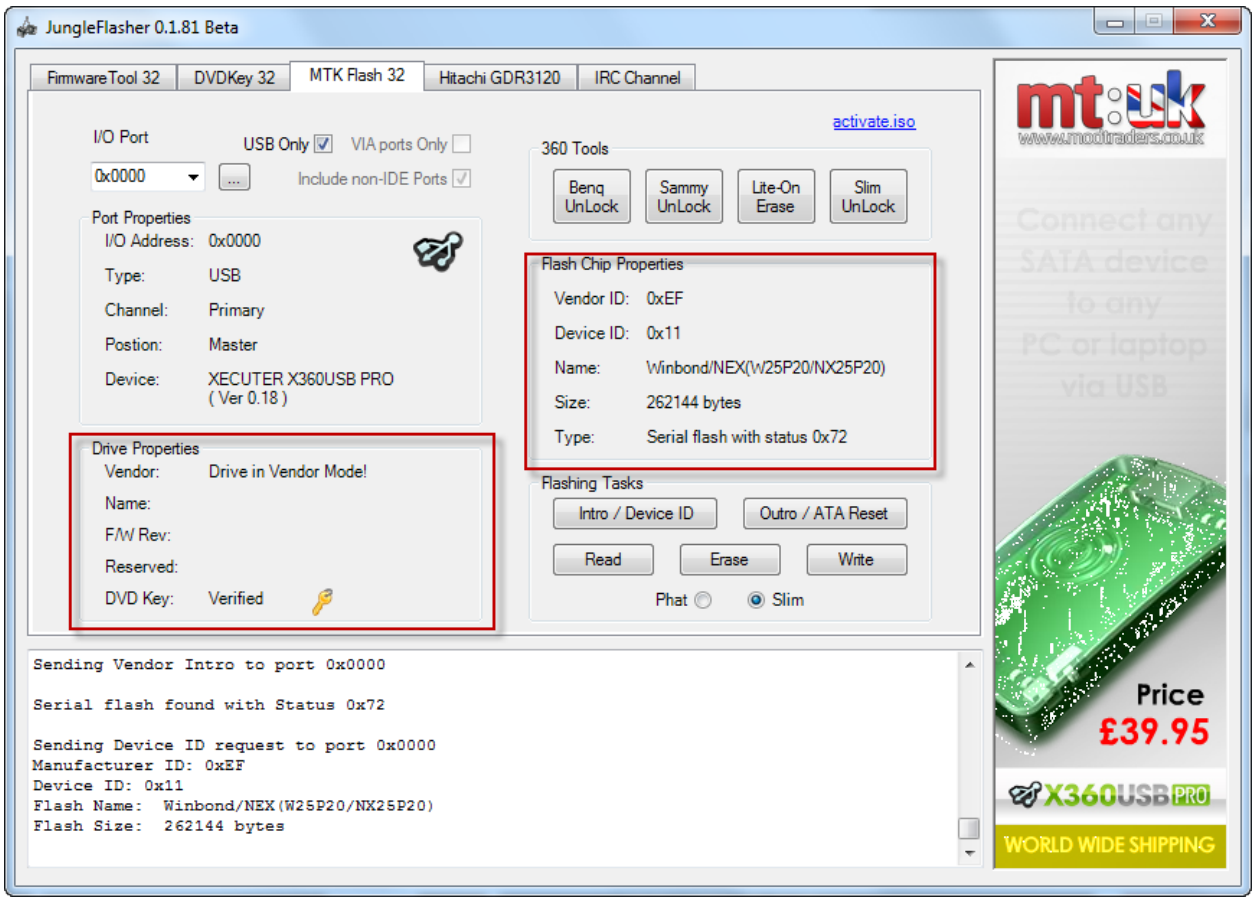
Things not going as expected? – Read the FAQ's

Write Firmware to the Slim 9504/0272

Select Slim **Unlock**



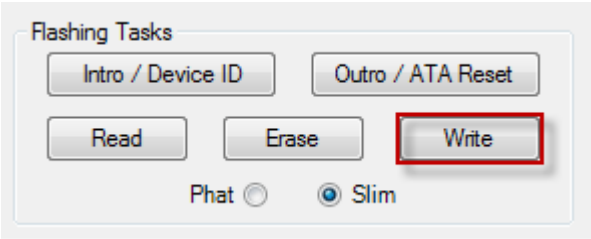
Jungleflasher will unlock the drive and place it into **Vendor Mode**



(Notice that the drive shows **Verified** this time)

Things not going as expected? – Read the FAQ's

Now the drive is in Vendor Mode, select the **Write** Button



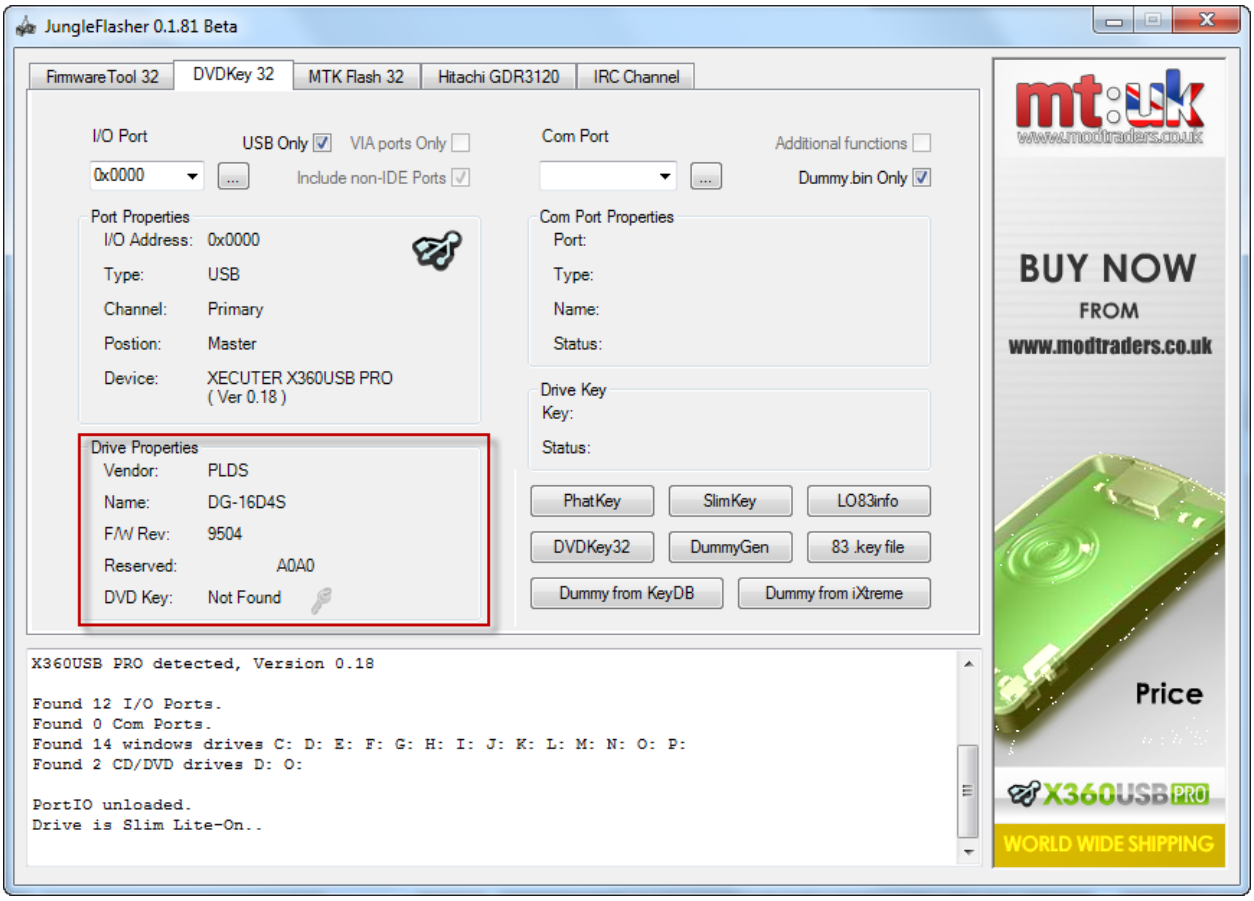

```
Serial flash found with Status 0x72

Sending Device ID request to port 0x0000
Manufacturer ID: 0xEF
Device ID: 0x11
Flash Name:  Winbond/NEX(W25P20/NX25P20)
Flash Size:  262144 bytes

Getting Status from port 0x0000
SPi flash found with Status 0x72

Sending Chip Erase to Port 0x0000
Erasing:
Writing target buffer to flash
Writing Bank 0: ................
Writing Bank 1: ................
Writing Bank 2: ................
Writing Bank 3: ................

Flash Verification Test !
Reading Bank 0: ................
Reading Bank 1: ................
Reading Bank 2: ................
Reading Bank 3: ................
Dumped in 4885mS

Write verified OK !

Restoring sector 0x3E000.

Sending Sector Erase to Port 0x0000
Erasing: 0x3E000
Writing: 0x3E000

Authorised !
................
Restore verified OK !
Drive is Slim Lite-On..

Key found in KeyDB at record (10 - My New Slim)
Key is: ##########REMOVED################
Key has been tested and verified, thanks C4eva !
```

Writing will commence and its progress shown in the log

[YOU ARE FINISHED – CLICK HERE TO RETURN TO START]

Method B – Using SlimKey

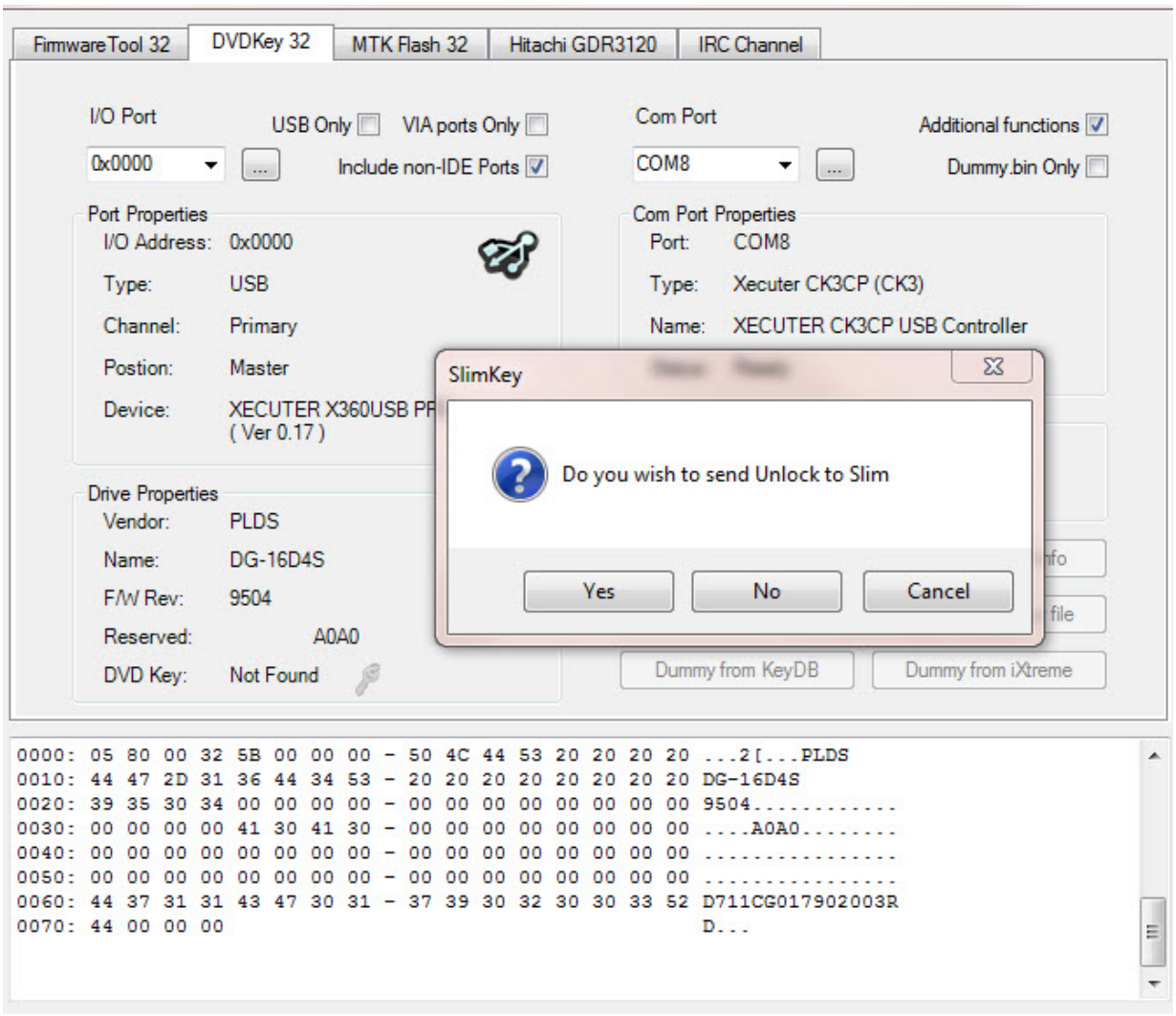
First select the correct **I/O port** and ensure drive shows up in drive properties



Then select **SlimKey** Button

You will be faced with Jungleflasher asking if you want to send Unlock to slim – click **YES**

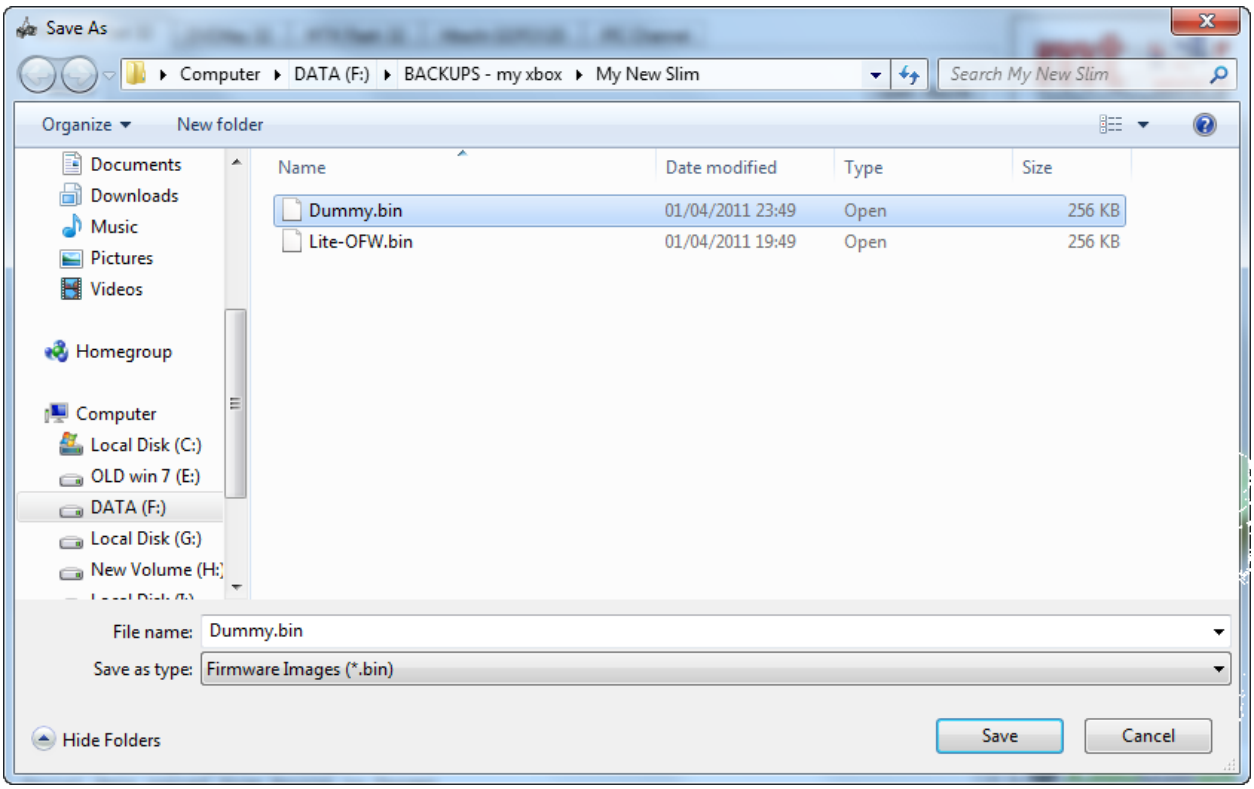
Things not going as expected? – Read the FAQ's



Once Jungleflasher has carried out its Unlock Procedure – it will Automatically Grab the Key and all other required information from the drive and generate a Dummy.bin.

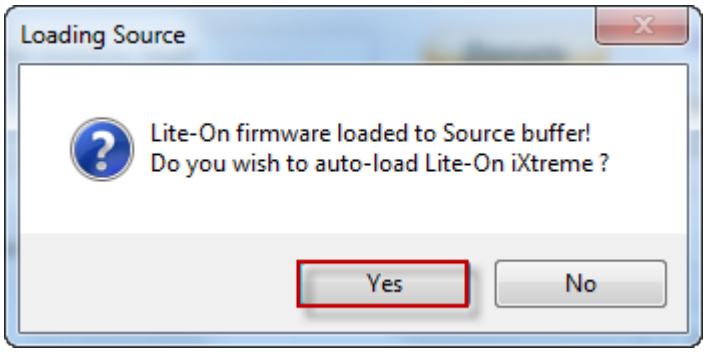
You will be prompted to save the generated Dummy.bin

Things not going as expected? – Read the FAQ's



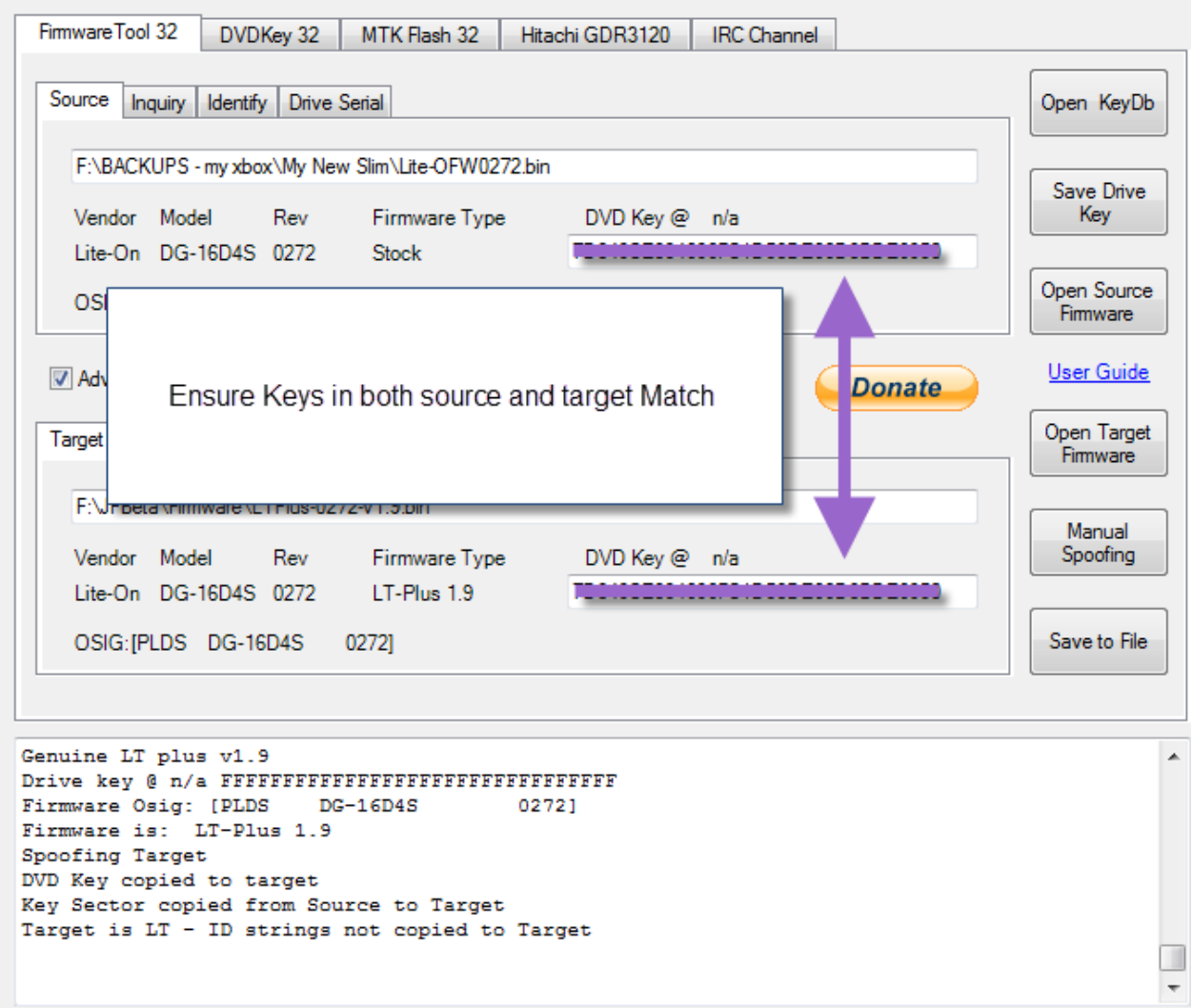
Please do so – having a saved copy of your Dummy.bin will enable very easy updating at any point in the future.

Jungleflasher will then proceed to Load your newly generated Dummy.bin as the Source File in **FirmwareTool 32** Tab and ask if you wish to Auto-Load the latest iXtreme Firmware.

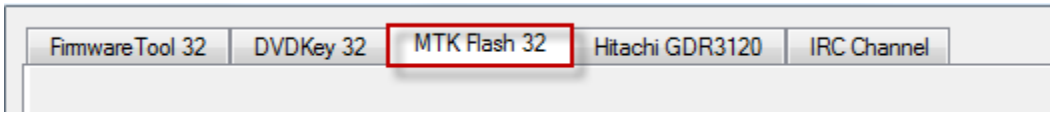


Select **Yes**

You will be faced with this



Now return to the **MTK** Flash 32 Tab



You will notice in the log that the key has now been Verified against the drive

```
Drive is Slim Lite-On..

Key found in KeyDB at record (10 - My New Slim)
Key is: #########REMOVED################
Key has been tested and verified, thanks C4eva !
```

To be able to write the target firmware to the drive you must unlock the drive once more (it was taken out of Vendor mode to Verify the Key)

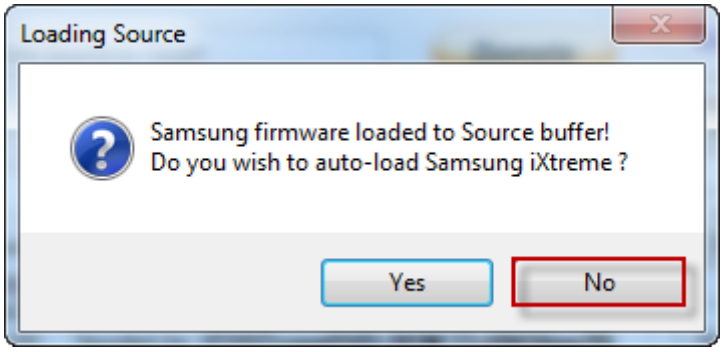
Things not going as expected? – Read the FAQ's

CLICK HERE TO CONTINUE

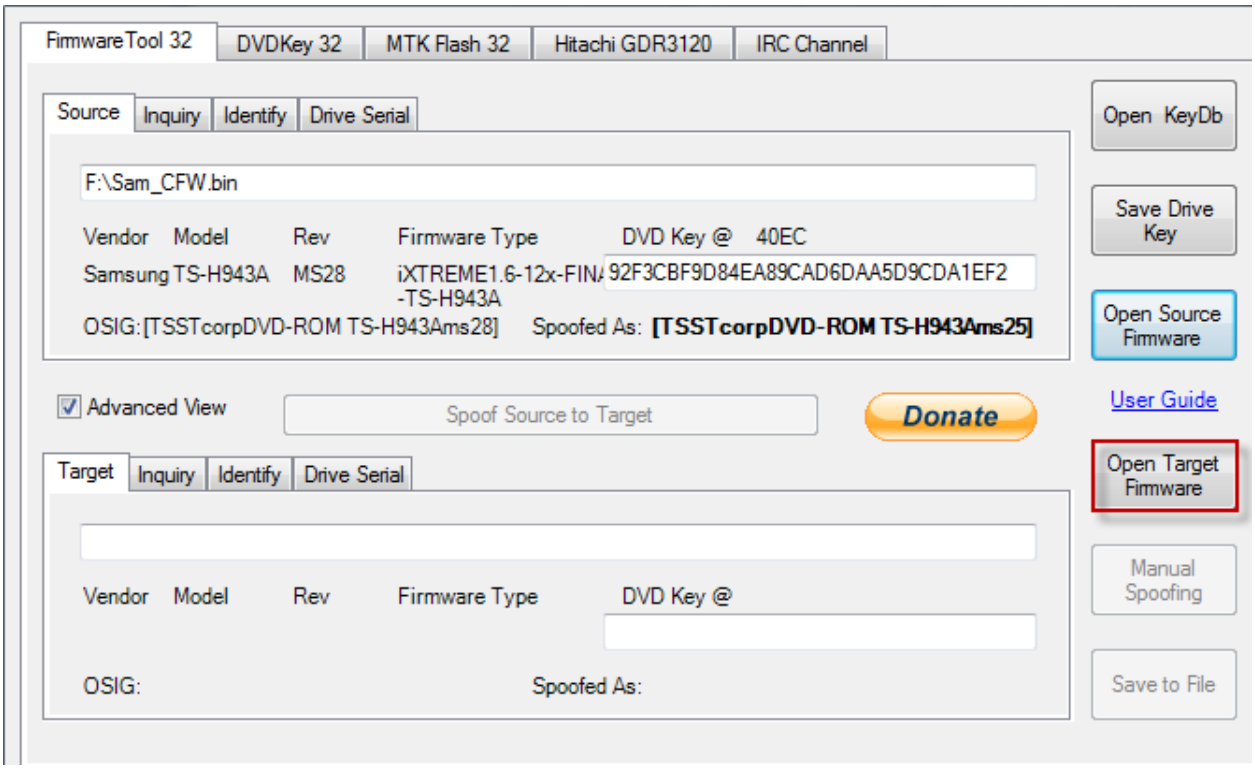
Things not going as expected? – Read the FAQ's

Sammy Return to Stock

When asked to auto load firmware select NO



Select Open Target Firmware

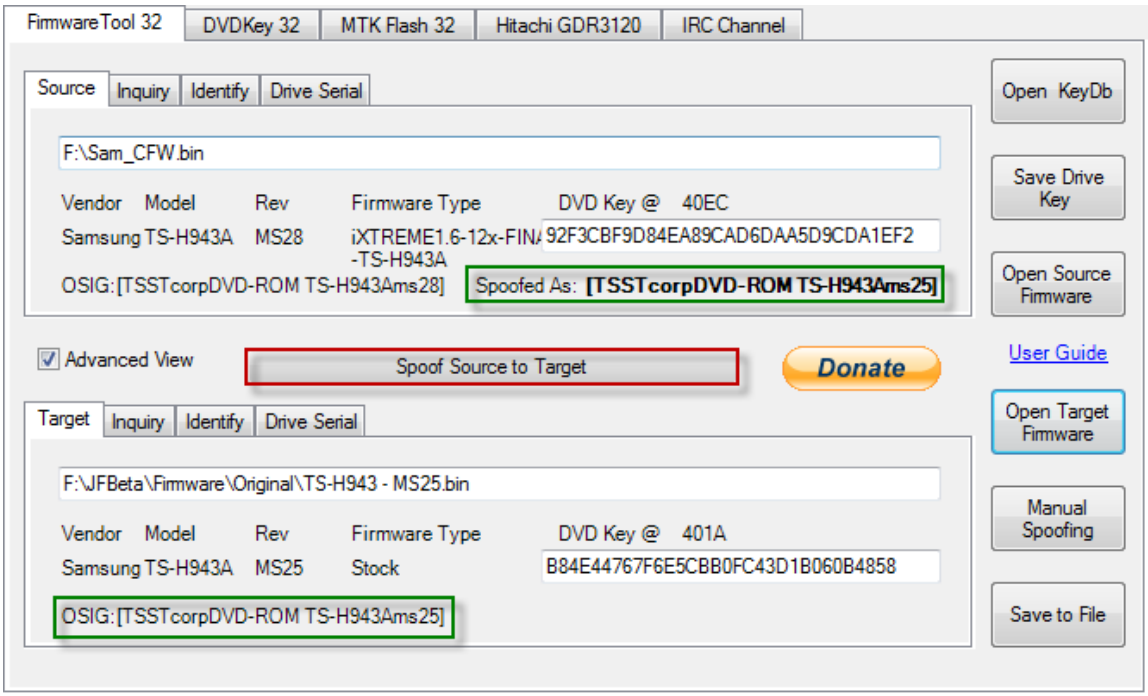


Select the stock firmware for your drive

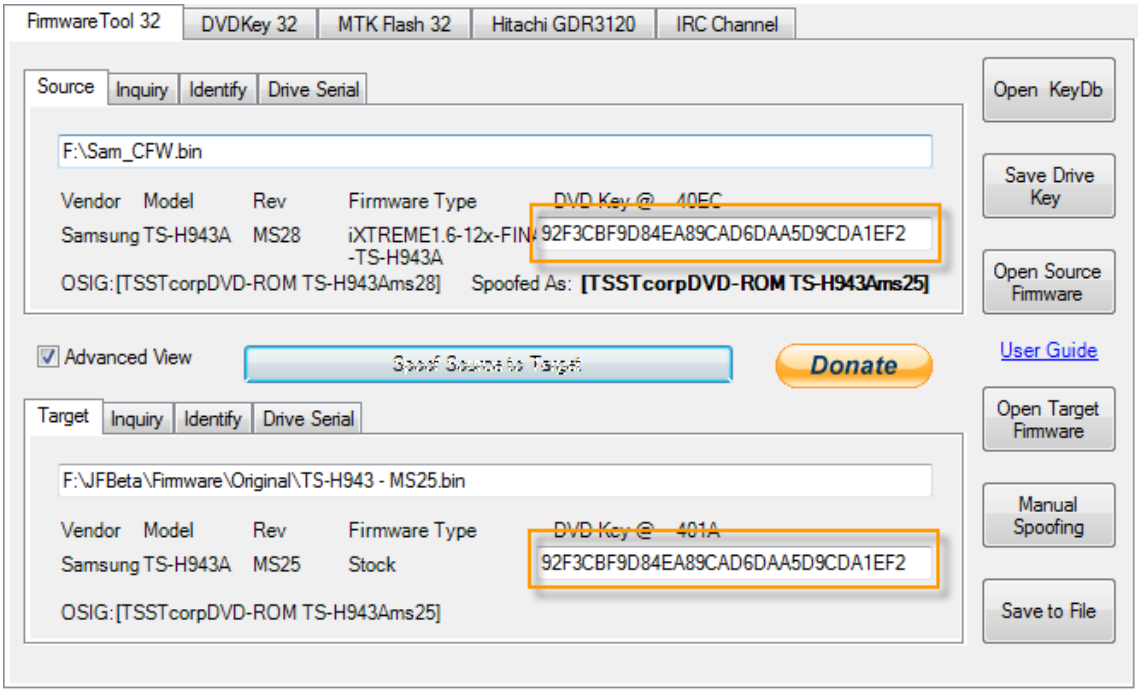
MS25 or MS28

A MS25 is shown in the example

Things not going as expected? – Read the FAQ's



Press the Spoof Source to Target **button**



Note the keys Now Match

CLICK HERE TO CONTINUE

Things not going as expected? – Read the FAQ's

Common problems and Frequently Asked Questions

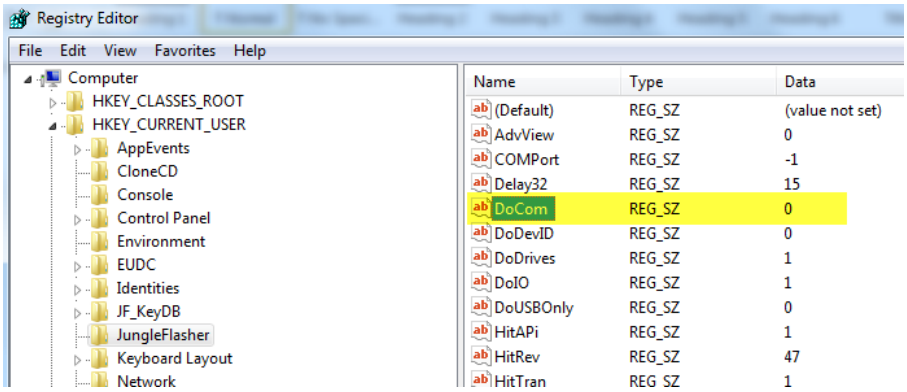
JungleFlasher tells me "Cant install portio32/64.sys driver"

If you are running any OS other than XP x86, then you must run the program as Administrator, see here for explanation how!

JungleFlasher tells me "No Com ports found during enumeration"

The LiteOn DG-16D2S 74850c Drive requires the utilization of an RS232 Serial Adapter to obtain the DVD Drives key (Unless you are using a Probe 3/PMT). Unless you are doing one of these drives, simply ignore it and proceed.

If you no longer use COM ports (With PMT there is no need) then you can stop Jungleflasher from Enumerating COM ports by setting DoCom (in registry – see advanced user functions) to the value 0



When using X360USB Pro – the drive reboots when trying to dump the drive or JungleFlasher seems to Lag OR I get erroneous issues

Try changing the USB cable you are connecting the device with / failing that try another USB Port.

JungleFlasher warns me of "No VIA Ports Found"

Due to quirky issues with some VIA Motherboards with VIA PCI SATA Cards, causing JungleFlasher to fail to load, we've forced via ports only as default.

This, for those without a VIA PCI SATA card, or VIA motherboard will get this warning.

If you do not have a VIA PCI card or a VIA Motherboard, proceed to the **DVDKey32 Tab**, and ensure **Non-IDE Ports is checked**. You will no longer get the warning when running JungleFlasher.

JungleFlasher cannot see my drive

There are multiple causes to this, so first of all ensure **VIA Ports Only** is unchecked and **Non-IDE** is checked under the **DVDKey32 Tab.**

If using RAID, it will cause issues. Set it to Native IDE / Disable AHCI (Intel) / Raid in your computers BIOS.

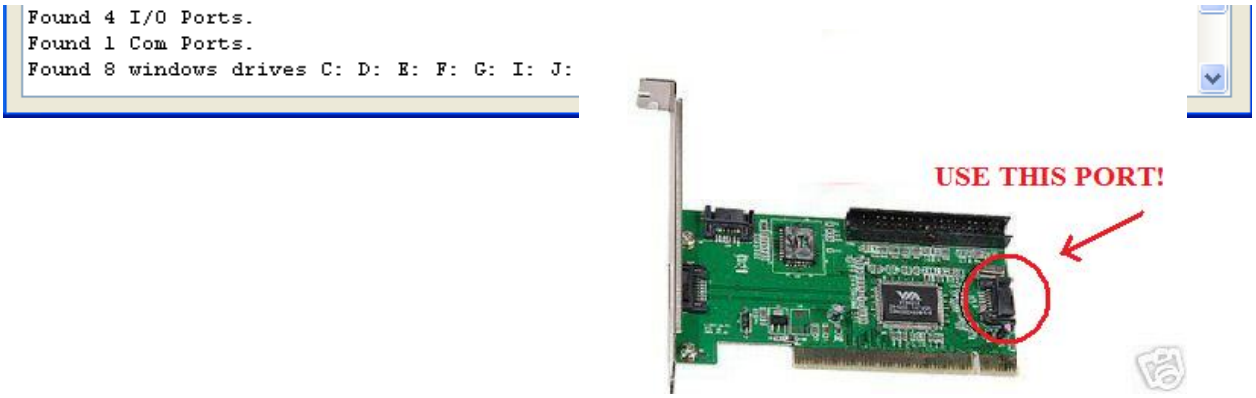
Use a Primary SATA port where possible.

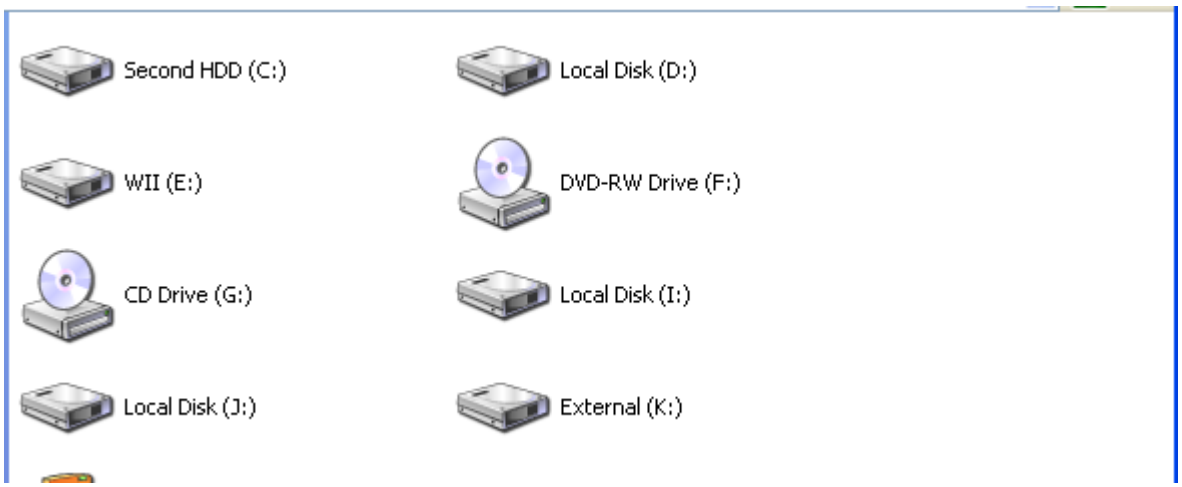
If using a VIA card ensure you use the correct port

If problems persist, please join us in the support channel HERE

JungleFlasher doesn't see my DVD Drive (cont)

Quite a few users believe JungleFlasher will report their Xbox 360 DVD Drive being Present in the Running Log:





JungleFlasher will only show drives that have been assigned a drive letter in windows.

The only 360 DVD Drive that has this during the process is the Hitachi Drives (Once in mode-b) and using WinAPI. Please, don't be surprised if JungleFlasher doesn't enumerate your DVD Drive.

I keep getting **Warning Serial Data is Bad Errors when trying to DVDKey my LiteOn**

Are you sure it doesn't have LT Firmware on it? LT Firmware does NOT allow DVDKey key extraction!

Using Probe 2? – ensure "Standby" is disabled.

Is it definitely a **74850c** version? The **83850c V1** uses **LO83Info** instead.

If this is the case, there are several things you will need to check.

Are you probing the R707 hole?

Using the USB connection from your CK3/Xtractor? If so check their websites for installation instructions (i.e. installing USB etc)

Using the Serial cable, double check this is connected properly.

Is the tray half in? You can check the User Guide on how to do this. Without the tray half in, you will get this error.

When Jungleflasher tells you to power drive with half open tray cycle power then – (**even if you set it before you started**!)

Is the Probe/Spear connected properly, have the correct lights? Double check these connections.

Using a home-made? Well unfortunately we can't troubleshoot this for you, if you choose the home-made method it's your responsibility.

Never rule out the possibility of one of the cables being faulty. If you have tried all of the other checks, then try using alternative cables.

My Maximus power adapter doesn't eject

This is a common one and deceives every user of the kit. You must keep eject pushed in for the drive to eject. Letting go will close the tray back over.

I don't know what SATA Chipset I have

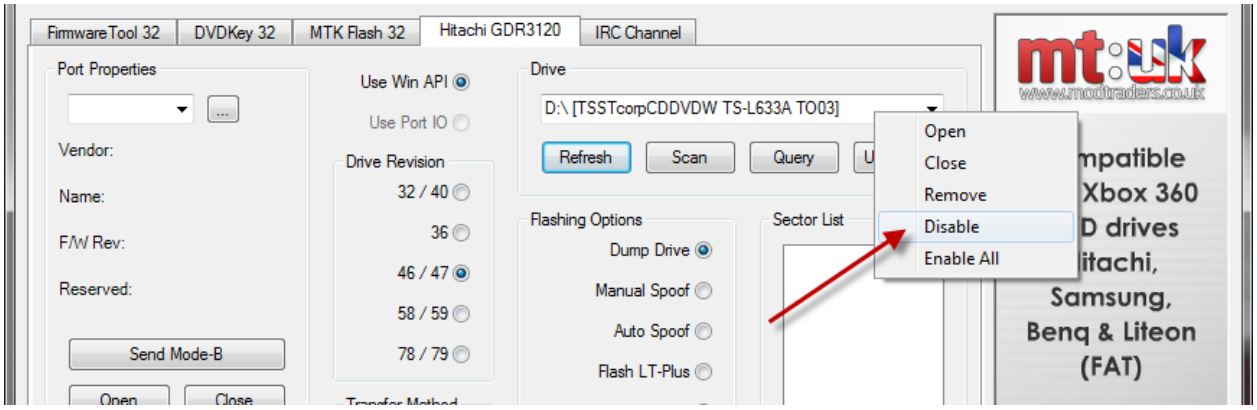
Download this program **CPU-Z** HERE and install it. Once installed, run the application, click on the **Mainboard Tab.** Your SATA Chipset is listed under **Chipset**.

I got an x/y when reading/writing/verifying my drive.

One, or a couple of instances is fine, JungleFlasher retries and as long as you have the **16 dots** and **Write Verified OK!** It's fine.

It fails during read / write.

It has been discovered that some CD/DVD-ROMS in your PC can cause issues with Jungleflasher when using onboard SATA. Disable it in in Hitachi Tab by **right-clicking** on it in drive list and selecting **disable**



or disconnect it! OR don't be a tight wad and buy a X360USB Pro!

I have an xxxxxxxx Drive but JungleFlasher sees it as yyyyyyyy

This is more than likely a Spoofed Drive. This is where a manufacturer of one drive, is used in place of a different manufacturer's drive.

The Xbox 360 checks what DVD Drive is in there using the drives OSIG. If this doesn't match, the console will report E66.

To overcome this, we can change one string in the drives Firmware, making one drive, report as the other, this fools the Xbox 360, but has an adverse affect with JungleFlasher as it will also report as the "other" drive.

Just treat it as the drive it really is, so if it is physically a Samsung, unlock it like a Samsung, write Samsung Firmware too it (with spoofed OSIG)

I LiteOn Erased my LiteOn and it failed / Device Intro Failed, now JungleFlasher won't detect my drive!

Calm down, your drive isn't bricked! JungleFlasher tries to automate as much of the process as possible, making it seamless. This time, sadly, it didn't work.

All you need to do is manually do the process again, power cycle the Drive, then send a MTK Intro to the drive.

JungleFlasher Will **not** see the Drive (No Drive Detected) as it is actually, now erased.

I get "Drive Rev Undetermined… Aborting!" When trying to dump my Hitachi

There are two main causes for this, the main one being a user trying to dump the drive using **WinAPI** but not having the correct drive selected in the **Top Right** drop down box. Try closing JungleFlasher, scanning in Device Manager and reopening JungleFlasher.

The second is caused by trying to dump a **v79** that **hasn't been 79unlocked**

I've set Mode-B but my drive won't show in the drop down box.

If using Windows Vista, or Windows 7, please close JungleFlasher, scan in Device Manager and re-open JungleFlasher, if this doesn't help, please leave your drive tray Ejected, and reboot your PC with **drive still powered and in Mode-B.** If the problem persists, please feel free to join the support channel and seek further assistance. HERE

If you are using PortIO option in Hitachi tab – It's not meant to!

My Xbox keeps turning itself off while I'm trying to flash my drive

If you are using the Xbox to power your drive during flashing, you **MUST** have the AV cable plugged into the Xbox (other end does **NOT** need to be connected to TV), otherwise it will power down after a few minutes (disaster if you are flashing a Hitachi). The HDMI cable can be used instead but it **MUST BE** connected to the TV!

It keeps saying serial data missing? OMG what do I do?

There is the option to rebuild the serial data from the serial numbers on the LiteOn case, laser and PCB. You can proceed and fill this data in IF YOU WISH! Go HERE for instructions on how. But – remember if the data is missing from the drive, do you really want to add it now? If it's a brand new drive that's not been touched before then it may be advisable to leave it!

I am trying to insert the unlock79 CD but I press twice to close and it opens again!

This is fairly common, in mode B some drives take 3 presses of eject button instead of 2 to get the drive to stay closed!

Every time I connect my drive to my VIA card my PC slows down or freezes

Try **reading** the tutorial……! Remove your drivers for the card!

Instructions for how to do it properly are HERE. OR in the less likely event that you have already correctly removed the drivers from the card and it still freezes – try moving your card into another PCI slot! (You may be required to reinstall drivers then remove using same method as before)

I just flashed my LiteOn – placed in a game and it doesn't work – OMG!

Before you panic – try ejecting then closing, and then reboot the console! It's possible the tray wasn't fully closed when the console booted and 0800 mode was activated (ix 1.6-1.61 only) – causing an error!

In what sequence should I switch things on/connect things?

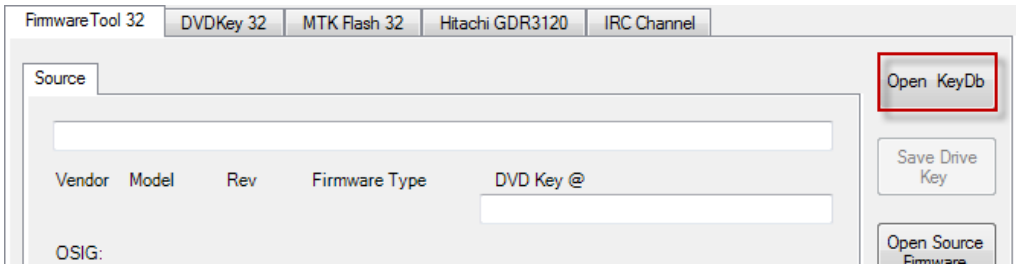
Generally (apart from the occasional stubborn Hitachi drive) you should boot the pc, then connect the SATA, then power on the drive (by which ever method you're using, Xbox or kit!) then open JungleFlasher.

My VIA 6421 Raid Controller is showing up as a VIA 3249 controller?

You installed the wrong drivers for the card! Go to HERE download the correct drivers install those – the drive will now show as VIA 6421 (now reboot) – Now return to HERE and remove them as previously instructed!

I didn't save my OFW, I lost my key – what can I do?

Do not fear – Jungleflasher updates its key database on every dump carried out, box in **firmwaretool 32** tab. Select **Open Key d/b**.



During spoofing the firmware – I got "No Calibration data in source"?

With the release of Jungleflasher 1.70, a section of data is now copied over starting from hex address 3C000 this data has been talked about as "calibration data" At the time of writing the data is considered to be manufacturing test data and is unused by the drive, but for completeness is now copied over to your iXtreme firmware. This is shown in the running log at time of spoofing the firmware like:

```
Spoofing Target
DVD Key copied to target
Inquiry string copied to Target
Identify string copied to Target
Serial data copied from Source to Target
Calibration data copied from Source to Target
```

A full dump of your **VIRGIN drive** (not one that has been returned with other stock firmware) is the **ONLY WAY** to get the **ORIGINAL DATA** from your drive into the iXtreme LT firmware.

So IF your drive has been flashed before *please IGNORE the statement* that appears: `No Calibration data in source`

As there is NOTHING you can do about it – it has been lost forever!

I've dumped the OFW using MRA Hack and get "Parse Failed" on loading firmware

There is a good chance you clicked "read" whilst the resistor is selected to GND (or in case of LT Switch – switch is in R/W position). After you have vendor mode put switch back to 3.3v (or "normal" – LT Switch) BEFORE pressing READ!

I've been banned from the JungleFlasher support channel wtf?

You have obviously been bashing noobs, talking piracy or generally being obnoxious – the support channel doesn't tolerate that sort of thing! Start groveling and change your ways.

CLICK HERE TO RETURN

Additional Info for running JungleFlasher in VISTA/WIN 7 x64

In VISTA and Win 7 it is a requirement that every driver must be signed. Because PortIO driver is NOT signed – it becomes necessary to work-around the Driver Signature Enforcement

There are 2 ways to do this.

One is simple but is required to be done every time you boot the pc and wish to use the driver!

The other, is a way of setting test mode to be selected upon every boot of the system

Easy Way of Disabling Driver Signature Enforcement

1) On boot up press F8 to get to the extended boot options screen
2) Choose "Disable Driver Signature Enforcement"
3) To start JungleFlasher right click on it in Windows Explorer and choose “properties”/compatibility – tick "Run as administrator" > click “ok”.
(This will enable JungleFlasher to run as Administrator every time you run it)
4) If a "Program Compatibility Assistant" warning message is displayed whilst you run JungleFlasher, you can simply ignore this by pressing the "Close" button

Recommended Way of Disabling Driver Signature Enforcement

PortIO64.sys file is no longer included in Jungleflasher download – if you wish to sign it – download it here

1) ***Disable User Account Control (UAC) In WIN 7***
- go to "Start Menu" > "Control Panel" > "User Accounts and Family Safety" >"User Accounts"
- click on "Change User Account Control settings"
- set the slider bar to the lowest value (Never notify) > click "OK"

Disable User Account Control (UAC) In Vista

- go to "Start Menu" > "Control Panel" > "User Accounts and Family Safety" >"User Accounts"
Click “Turn User Account Control on or off” > click continue, untick the box, click OK

2) **Sign the portio.sys driver**
- download the "Driver Signature Enforcement Overrider" (DSEO) from http://www.ngohq.com/home.php?page=dseo
- start DSEO > click "Next" > "Yes" > choose "Sign a System File" > "Next" > enter the path to the used driver (portio32.sys or portio64.sys) > "OK" > "OK"
3) **Disable Driver Signature Enforcement**
- start DSEO > click "Next" > "Yes" > choose "Enable Test Mode" > "Next" > "OK"
4) **Restart the computer**

CLICK HERE TO RETURN

JungleFlasher v0.1.87 beta

Thanks to:

c4eva & Team Jungle

Team - Xecuter

Schtrom (Legend in his own right)

Seacrest (Openkey)

Team Modfreakz (for all you have contributed!)

MRA (☺)

Geremia (Kamikaze Unlock)

Maximus (for Scorpion2 - to reverse and improve)

Giampy (LiteOn Barcode Rebuilder)

&

The Testers (well, obviously for testing)

CLICK HERE TO RETURN TO STARTING POINT

Things not going as expected? – Read the FAQ's