JungleFlasher v0.1.70

(x86 and x64 Compatible)

Complete User Guide

(v0.1.3.1b)

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 NOT RECOMMENDED!

USE THE LINKS!

I AM A NEW USER OF JUNGLEFLASHER

CLICK HERE

USED JUNGLEFLASHER BEFORE

CLICK HERE

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. Recent changes allow JungleFlasher to be fully functional in a x64 environment.

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 v0.1.55b also brought the unique feature of dumping "Dummy.bin" from iXtreme flashed LiteOn Drives solely using S-ATA. There is also a facility to create a "dummy.bin" from previously extracted files, although fresh extractions should be completed where possible. Every effort has been made to make key extraction as reliable as possible. Multiple dumps are performed with comparison to account for the slightest chance that serial data may have become corrupt.

The **MTKFlash 32** tab is used to unlock Benq and Samsung 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 3 MTK 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.

Overview of JungleFlasher and its functions

When you start JungleFlasher, you will be presented with **4 tabs**;
FirmwareTool32, DVDKey32, MTKFlash32 and Hitachi GDR-3120L.

FirmwareTool32 is used to view firmware details, manipulate these firmware's, 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 earlier **LiteOn PLDS DG-16D2S** drives. It also has an option to rebuild from previous files (for people who used other, older applications or those who followed poor advice before. Newest LiteOn drives (83850C v2 and 93450C) need to be fully dumped and as such are dealt with using MTK Flash 32 tab.

JungleFlasher v0.165 brought the inclusion of **LO83info** for **LiteOn PLDS DG-16D2S 83850c V1 drives** (83850C V1 occurred up to around Jul/Aug 09 drive manufacture dates)**.** This hack being used for obtaining the unique data from the 83850C V1 drive revision. With JungleFlasher v0.1.66b incorporating Seacrest's OpenKey, used to decrypt the obtained file.

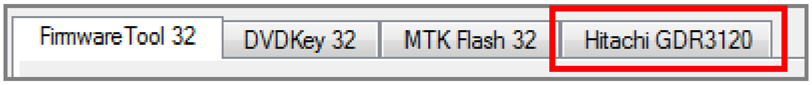
There are also 4 checkboxes found in this tab, **VIA Ports Only** and **Include non-IDE ports,** added for extra safety and compatibility; **USB Xtractor Switch** – for use with the Maximus USB Xtractor Push Button to extract feature this launches the DVDKey32 command from the Hardware Device itself. 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** and **Samsung** 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.

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!)

JungleFlasher Firmware Pack (vital for Hitachi Drives)

Download the latest iXtreme firmwares from xbins – 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 correct operation during Hitachi manipulation/flashing)

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

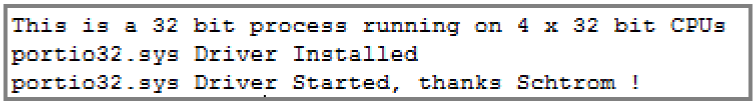
It is advisable as the drivers tend to cause problems on a lot of drives but very noticeable with erased LiteOn, causing the infamous 'Lite-On + VIA Freeze'

CLICK HERE TO FIND OUT HOW TO DO IT PROPERLY

~~You must Install PortIO32~~

NOT ANYMORE!

JungleFlasher now has On-The-Fly PortIO Drivers! (Thanks Schtrom!)



```
This is a 32 bit process running on 4 x 32 bit CPUs
portio32.sys Driver Installed
portio32.sys Driver Started, thanks Schtrom !
```

And Yes, there is a portio64.sys for x64 operating systems too!

The portio32.sys and portio64.sys must be left in same directory as jungleflasher.exe

IF USING ANY Operating System other than WinXP x86 you must right-click on Jungleflasher Icon and select "Run as Administrator"

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

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

Thanks

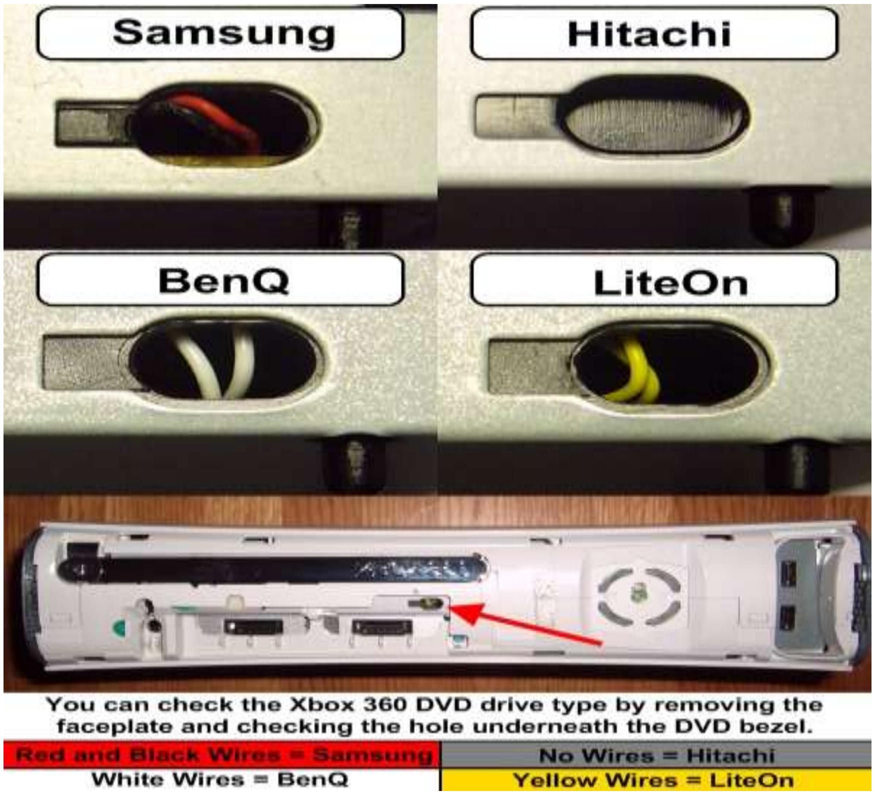
Manual Spoofing

Spoofing a Hitachi

Spoofing a different drive

CONTINUE

Which Drive Do I Have?



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

Samsung
CLICK HERE

BenQ
CLICK HERE

Hitachi
CLICK HERE

LiteOn
CLICK HERE

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!

Samsung (TS-H943) MS25 /MS28.

Overview.

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

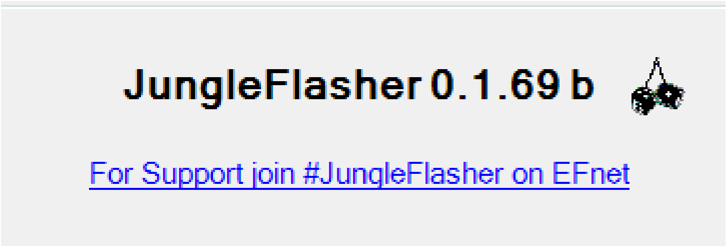
- Unlocking the Drive (MS28 or Xtreme 3.3+ Firmwares)
- Reading the Original firmware
- Patching Key into hacked Firmware
- Writing Drive

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

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.

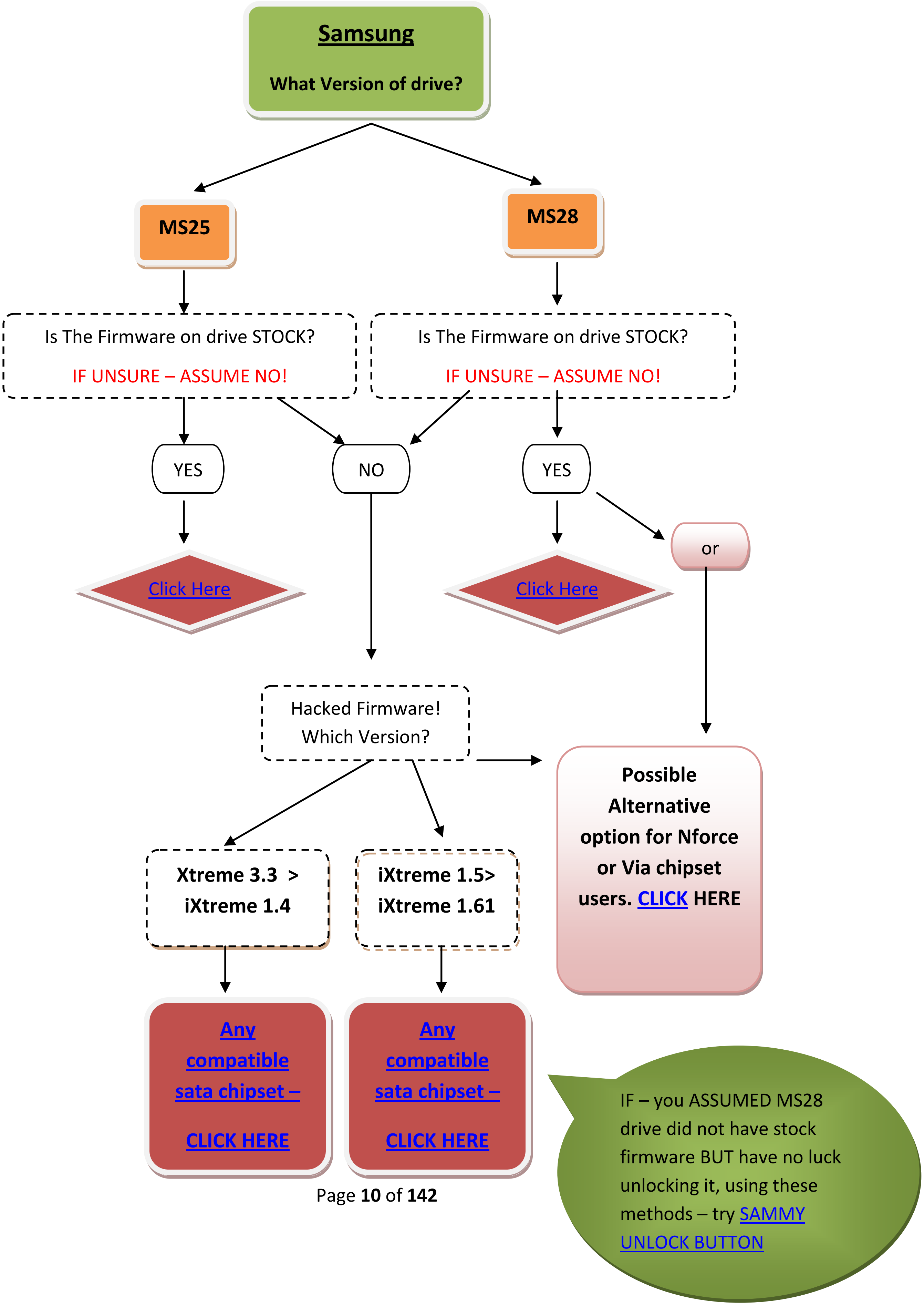


JungleFlasher 0.1.69 b

For Support join #JungleFlasher on EFnet

After a few seconds the main window will load.

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



Samsung

What Version of drive?

MS25

MS28

Is The Firmware on drive STOCK?

IF UNSURE – ASSUME NO!

Is The Firmware on drive STOCK?

IF UNSURE – ASSUME NO!

YES

NO

YES

or

Click Here

Click Here

Hacked Firmware!
Which Version?

Possible Alternative option for Nforce or Via chipset users. CLICK HERE

Xtreme 3.3 > iXtreme 1.4

iXtreme 1.5> iXtreme 1.61

Any compatible sata chipset –

CLICK HERE

Any compatible sata chipset –

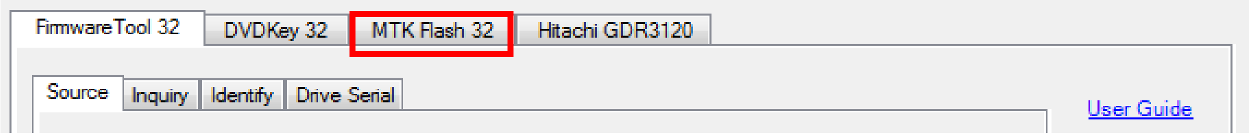
CLICK HERE

IF – you ASSUMED MS28 drive did not have stock firmware BUT have no luck unlocking it, using these methods – try SAMMY UNLOCK BUTTON

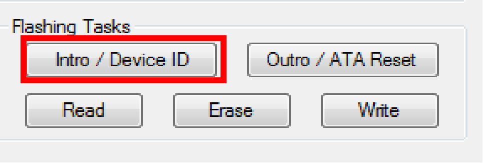
Unlocking the drive.

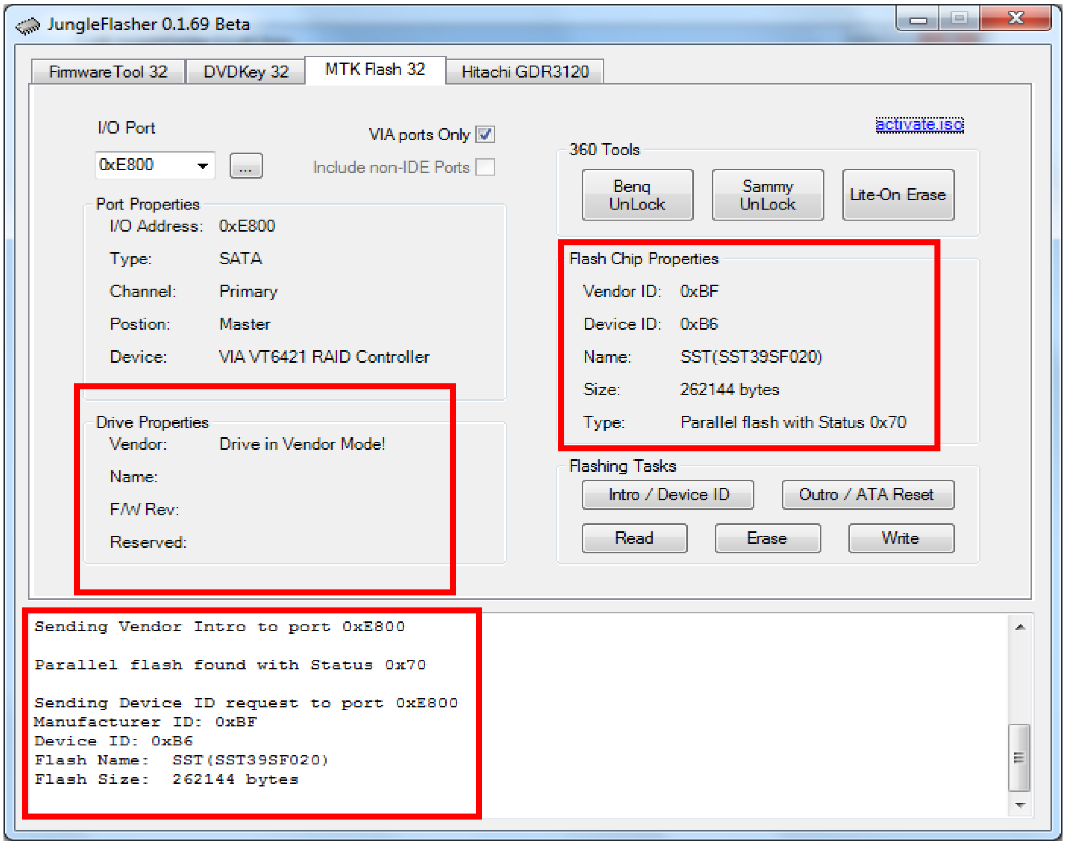
Before we can do anything to the drive, it must be in Vendor Mode (status 0x70).

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



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.





I/O Port: 0xE800

VIA ports Only ☑

Include non-IDE Ports □

Port Properties
I/O Address: 0xE800
Type: SATA
Channel: Primary
Postion: Master
Device: VIA VT6421 RAID Controller

Drive Properties
Vendor: Drive in Vendor Mode!
Name:
F/W Rev:
Reserved:

Flash Chip Properties
Vendor ID: 0xBF
Device ID: 0xB6
Name: SST(SST39SF020)
Size: 262144 bytes
Type: Parallel flash with Status 0x70

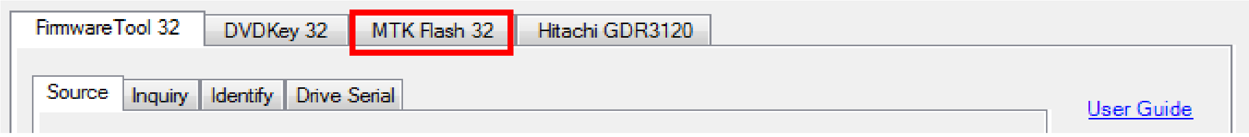
```
Sending Vendor Intro to port 0xE800

Parallel flash found with Status 0x70

Sending Device ID request to port 0xE800
Manufacturer ID: 0xBF
Device ID: 0xB6
Flash Name:  SST(SST39SF020)
Flash Size:  262144 bytes
```

Now CLICK HERE to proceed

Unlocking the drive.

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

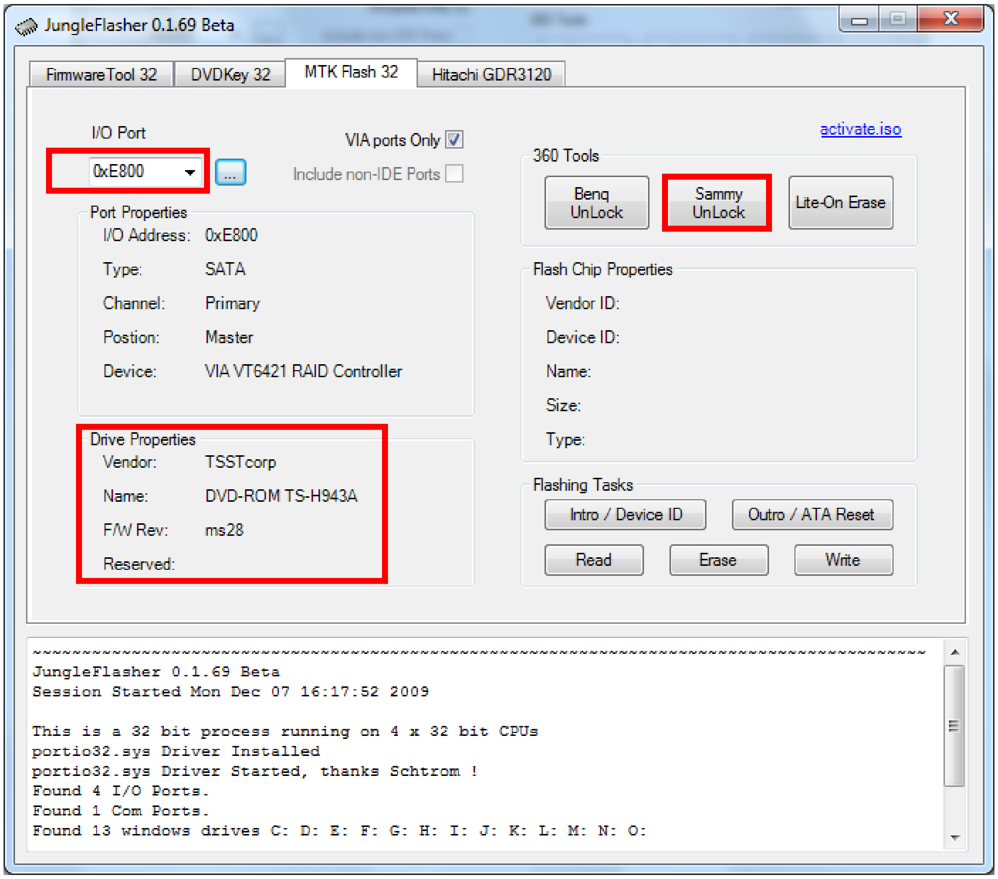
All Unlocking is taken place under the **MTKFlash 32** tab.



Stock MS28's (Unmodified).

Sammy UnLock.

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



I/O Port: 0xE800

VIA ports Only ☑

Include non-IDE Ports □

Port Properties

I/O Address: 0xE800

Type: SATA

Channel: Primary

Postion: Master

Device: VIA VT6421 RAID Controller

Drive Properties

Vendor: TSSTcorp

Name: DVD-ROM TS-H943A

F/W Rev: ms28

Reserved:

Flash Chip Properties

Vendor ID:

Device ID:

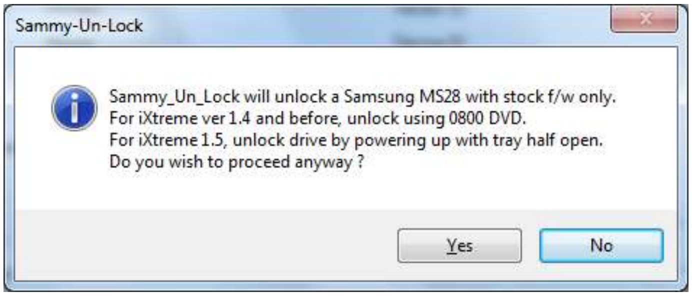
Name:

Size:

Type:

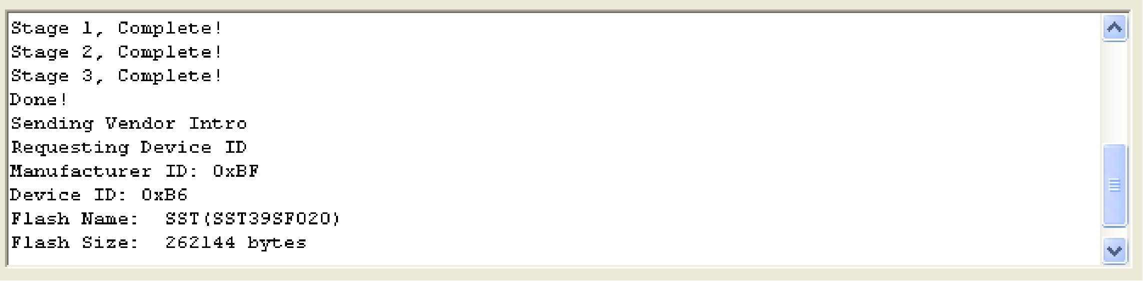
```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
JungleFlasher 0.1.69 Beta
Session Started Mon Dec 07 16:17:52 2009

This is a 32 bit process running on 4 x 32 bit CPUs
portio32.sys Driver Installed
portio32.sys Driver Started, thanks Schtrom !
Found 4 I/O Ports.
Found 1 Com Ports.
Found 13 windows drives C: D: E: F: G: H: I: J: K: L: M: N: O:
```

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



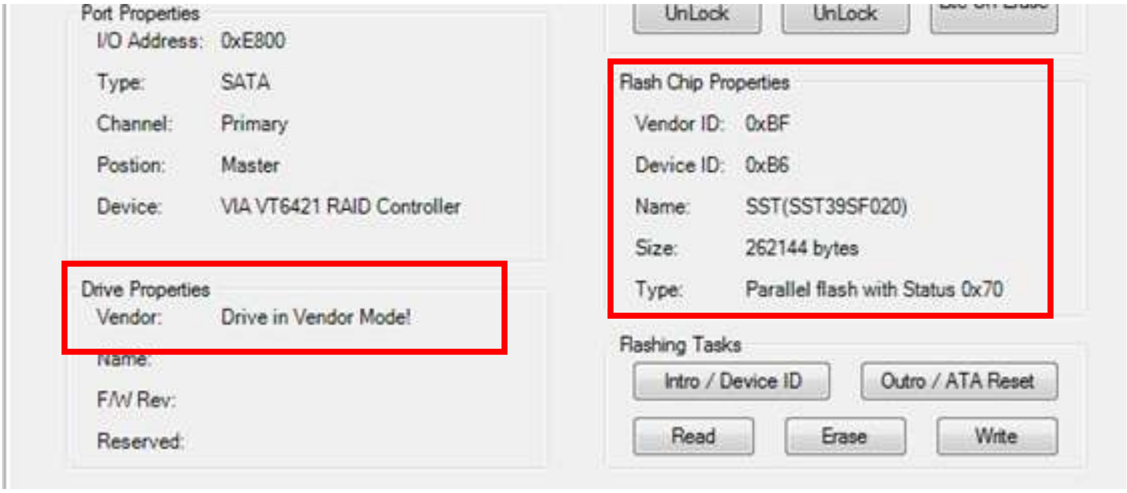
Sammy_Un_Lock will unlock a Samsung MS28 with stock f/w only.
For iXtreme ver 1.4 and before, unlock using 0800 DVD.
For iXtreme 1.5, unlock drive by powering up with tray half open.
Do you wish to proceed anyway ?

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**.



```
Stage 1, Complete!
Stage 2, Complete!
Stage 3, Complete!
Done!
Sending Vendor Intro
Requesting Device ID
Manufacturer ID: 0xBF
Device ID: 0xB6
Flash Name:  SST(SST39SF020)
Flash Size:  262144 bytes
```

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!"**



Port Properties
I/O Address: 0xE800
Type: SATA
Channel: Primary
Postion: Master
Device: VIA VT6421 RAID Controller

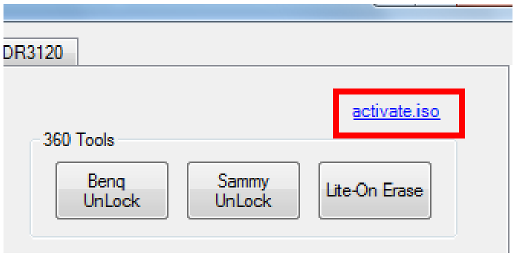
Drive Properties
Vendor: Drive in Vendor Mode!
Name:
F/W Rev:
Reserved:

Flash Chip Properties
Vendor ID: 0xBF
Device ID: 0xB6
Name: SST(SST39SF020)
Size: 262144 bytes
Type: Parallel flash with Status 0x70

Now CLICK HERE to proceed

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,



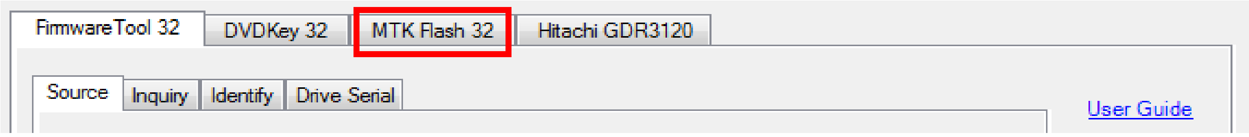
burnt to **Dual Layer + R Media** (this is vital for later firmwares). Simply burn it with no layerbreak settings, with all data present on first Layer, IMGBurn 2.5.0.0 will do this fine just select the ISO and confirm you want to burn to a large capacity disc with all data present on L0 (Layer 0).

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

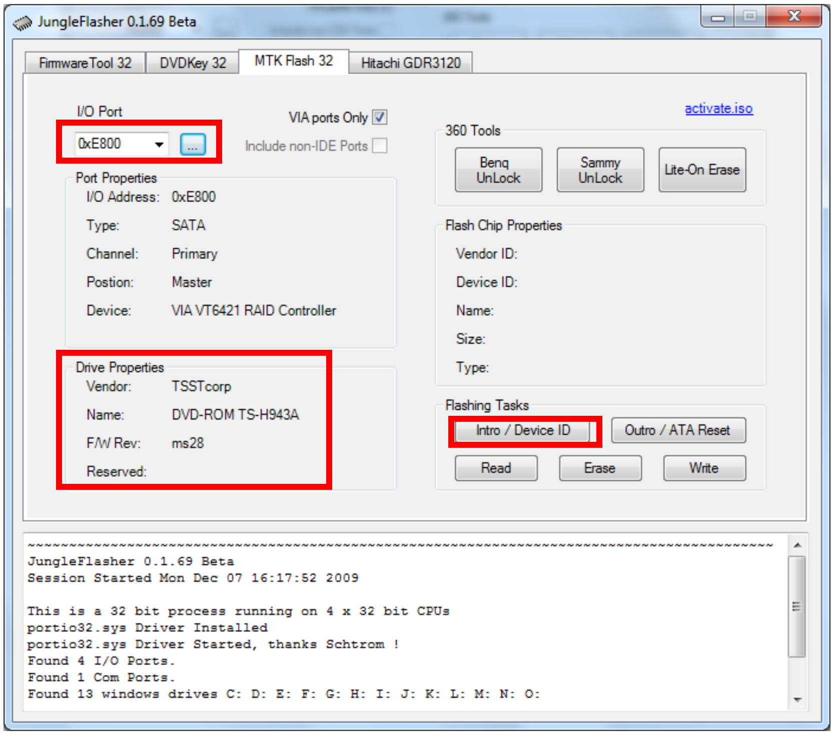
Unlocking the drive.

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



I/O Port: 0xE800

☑ VIA ports Only

□ Include non-IDE Ports

Port Properties

I/O Address: 0xE800

Type: SATA

Channel: Primary

Postion: Master

Device: VIA VT6421 RAID Controller

Drive Properties

Vendor: TSSTcorp

Name: DVD-ROM TS-H943A

F/W Rev: ms28

Reserved:

Flash Chip Properties

Vendor ID:

Device ID:

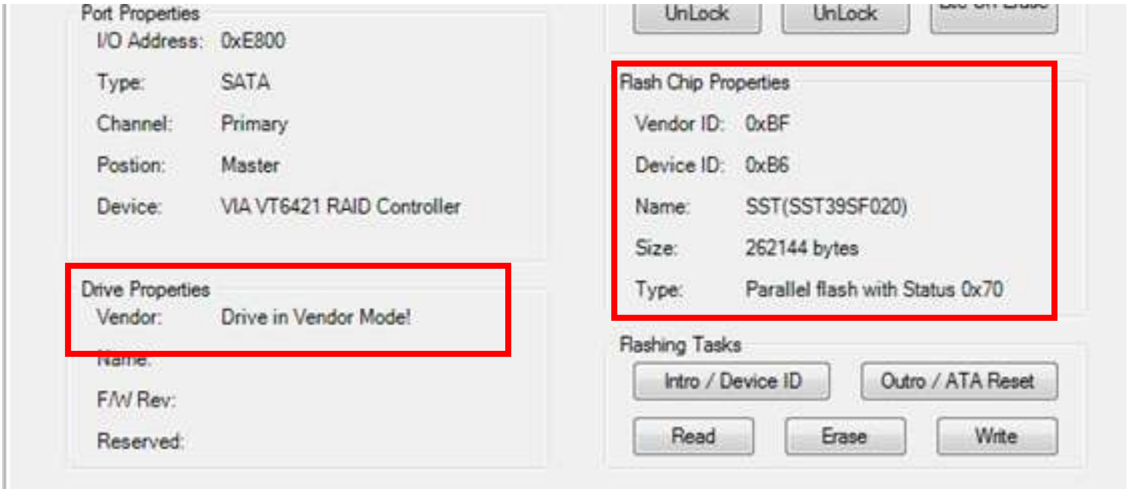
Name:

Size:

Type:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
JungleFlasher 0.1.69 Beta
Session Started Mon Dec 07 16:17:52 2009

This is a 32 bit process running on 4 x 32 bit CPUs
portio32.sys Driver Installed
portio32.sys Driver Started, thanks Schtrom !
Found 4 I/O Ports.
Found 1 Com Ports.
Found 13 windows drives C: D: E: F: G: H: I: J: K: L: M: N: O:
```

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



Port Properties

I/O Address: 0xE800

Type: SATA

Channel: Primary

Postion: Master

Device: VIA VT6421 RAID Controller

Drive Properties

Vendor: Drive in Vendor Mode!

Name:

F/W Rev:

Reserved:

Flash Chip Properties

Vendor ID: 0xBF

Device ID: 0xB6

Name: SST(SST39SF020)

Size: 262144 bytes

Type: Parallel flash with Status 0x70

Now CLICK HERE to proceed

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.**

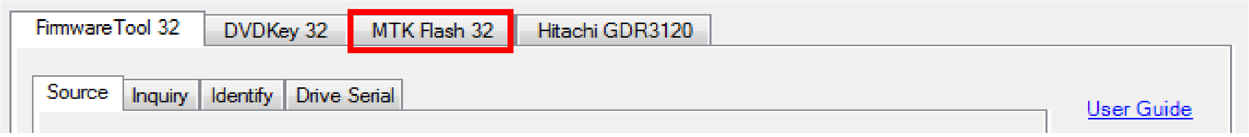
Wait for a few seconds and replace the power plug into the DVD drive taking **extreme caution** to plug the plug the right way around – once done, the drive is now powered, console thinks its closed but it is in fact half open.

If using a connectivity kit to power the drive

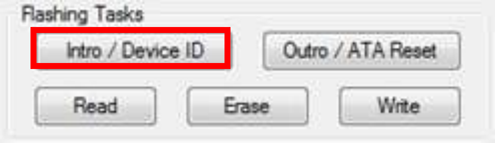
You need to power on the drive with **Eject status closed** but **Tray Half Open** – To do this using a connectivity kit as Power source, eject the DVD drive, then, press eject to ‘close’ the tray. **Now this is the important part – you MUST switch off the power BEFORE it closes fully.**

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.

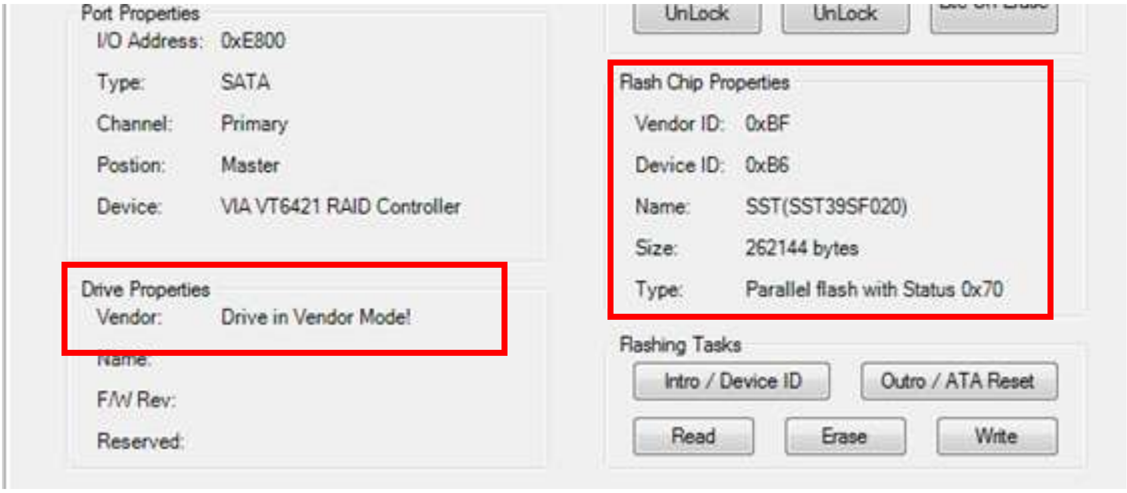
Load JungleFlasher, and select **MTKFlash 32** tab.



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.**



Port Properties
I/O Address: 0xE800
Type: SATA
Channel: Primary
Postion: Master
Device: VIA VT6421 RAID Controller

Drive Properties
Vendor: Drive in Vendor Mode!
Name:
F/W Rev:
Reserved:

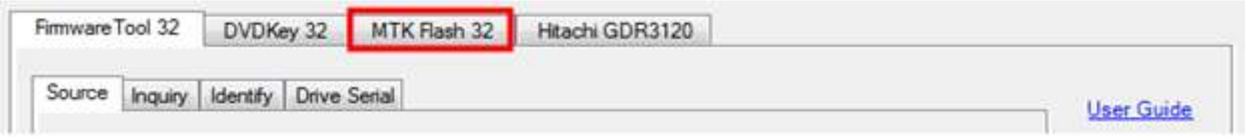
Flash Chip Properties
Vendor ID: 0xBF
Device ID: 0xB6
Name: SST(SST39SF020)
Size: 262144 bytes
Type: Parallel flash with Status 0x70

[Now CLICK HERE to proceed]

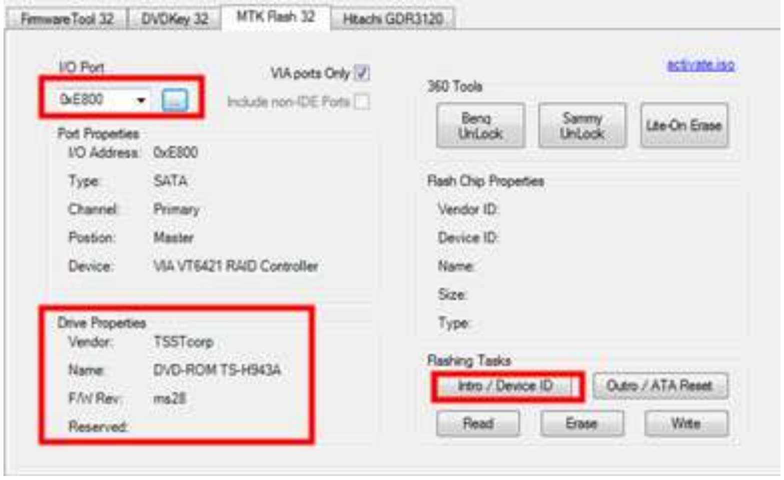
DeviceID Unlock / Vcc Trick (VIA/Nforce only) Stock + Modified Drives.

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.**



I/O Port: 0xE800

VIA ports Only ☑

Include non-IDE Ports □

Port Properties

I/O Address: 0xE800

Type: SATA

Channel: Primary

Postion: Master

Device: VIA VT6421 RAID Controller

Drive Properties

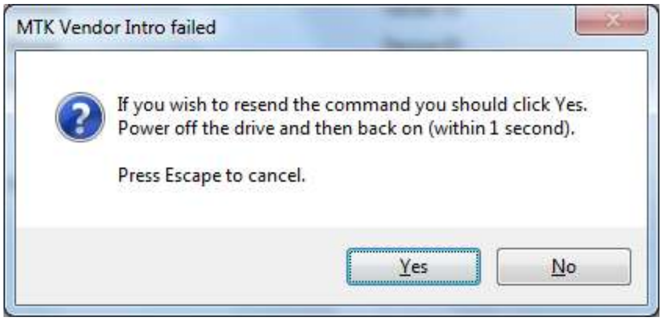
Vendor: TSSTcorp

Name: DVD-ROM TS-H943A

F/W Rev: ms28

Reserved:

JungleFlasher will prompt you with instructions.

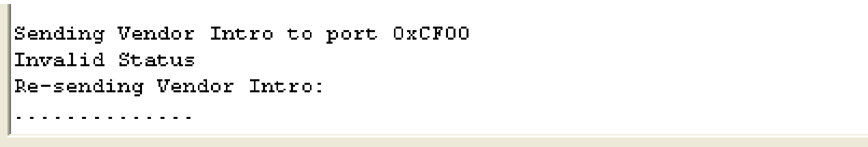


MTK Vendor Intro failed

If you wish to resend the command you should click Yes.
Power off the drive and then back on (within 1 second).

Press Escape to cancel.

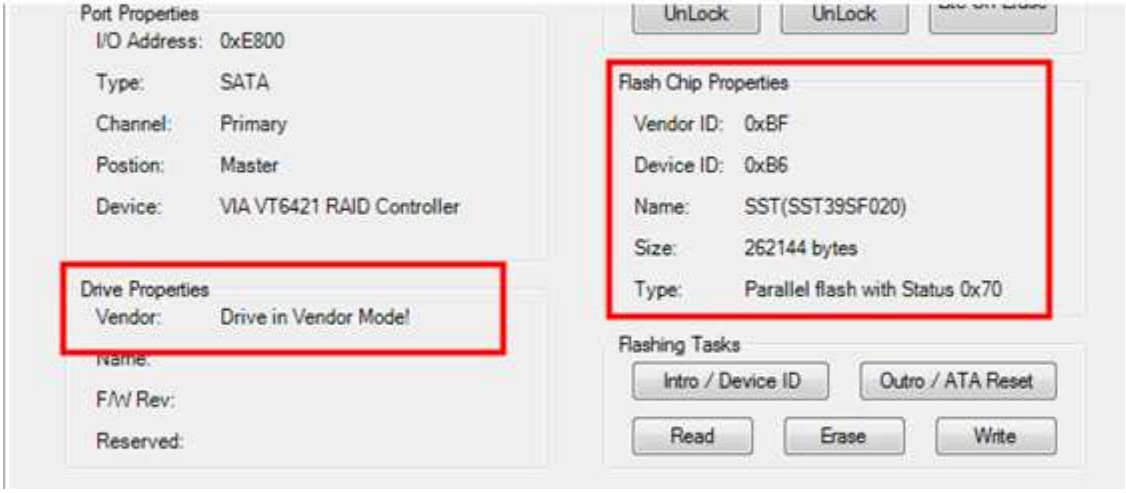
Click **Yes** the **Running Log** will display something similar to this.



```
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.**



Port Properties
I/O Address: 0xE800
Type: SATA
Channel: Primary
Postion: Master
Device: VIA VT6421 RAID Controller

Drive Properties
Vendor: Drive in Vendor Mode!
Name:
F/W Rev:
Reserved:

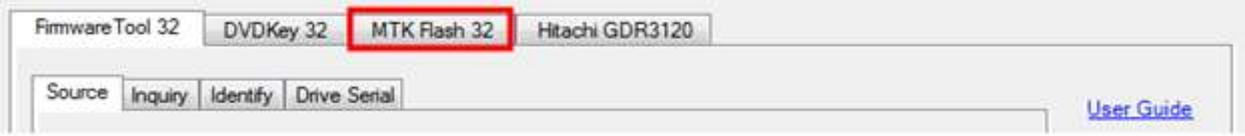
Flash Chip Properties
Vendor ID: 0xBF
Device ID: 0xB6
Name: SST(SST39SF020)
Size: 262144 bytes
Type: Parallel flash with Status 0x70

Now CLICK HERE to proceed

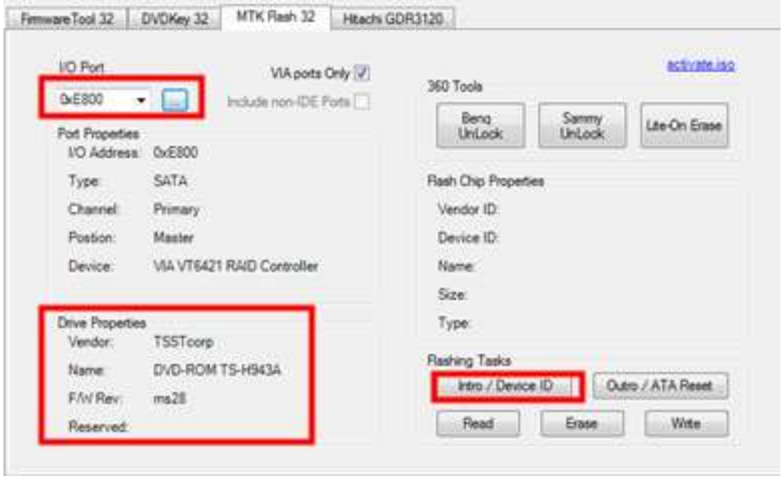
If it didn't work – read on

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.**



I/O Port: 0xE800

VIA ports Only ☑

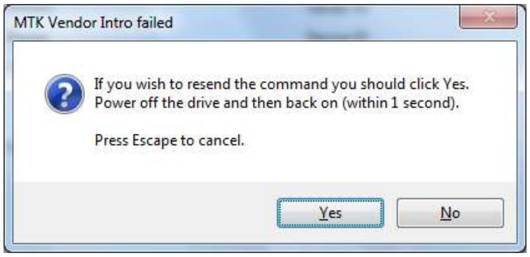
Include non-IDE Ports □

Port Properties
I/O Address: 0xE800
Type: SATA
Channel: Primary
Postion: Master
Device: VIA VT6421 RAID Controller

Drive Properties
Vendor: TSSTcorp
Name: DVD-ROM TS-H943A
F/W Rev: ms28
Reserved:

Flash Chip Properties
Vendor ID:
Device ID:
Name:
Size:
Type:

JungleFlasher will prompt you with instructions.



MTK Vendor Intro failed

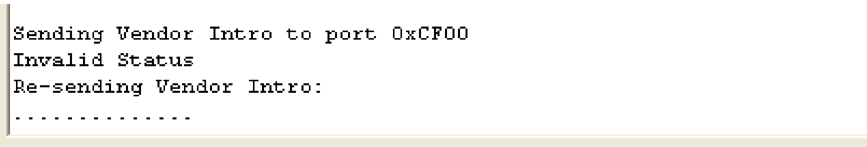
If you wish to resend the command you should click Yes.
Power off the drive and then back on (within 1 second).

Press Escape to cancel.

Now power **off** the drive!

Then click **YES,**

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

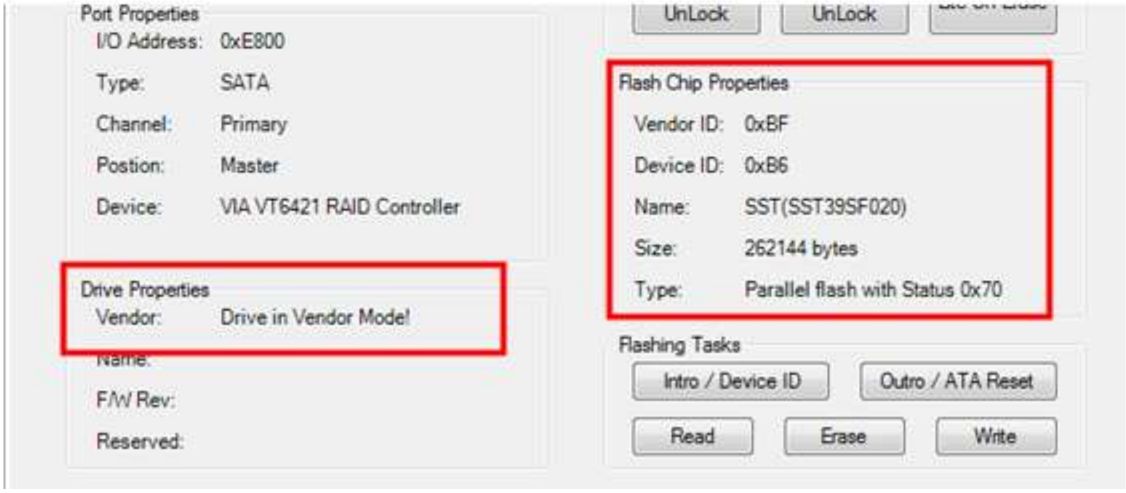


```
Sending Vendor Intro to port 0xCF00
Invalid Status
Re-sending Vendor Intro:
..............
```

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.**



Port Properties

I/O Address: 0xE800

Type: SATA

Channel: Primary

Postion: Master

Device: VIA VT6421 RAID Controller

Drive Properties

Vendor: Drive in Vendor Mode!

Name:

F/W Rev:

Reserved:

Flash Chip Properties

Vendor ID: 0xBF

Device ID: 0xB6

Name: SST(SST39SF020)

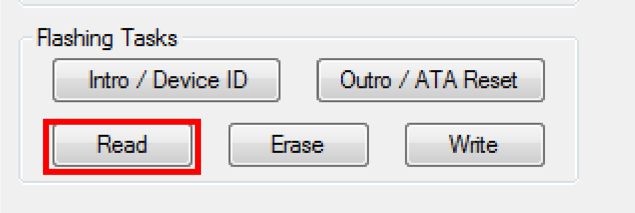
Size: 262144 bytes

Type: Parallel flash with Status 0x70

Now CLICK HERE to proceed

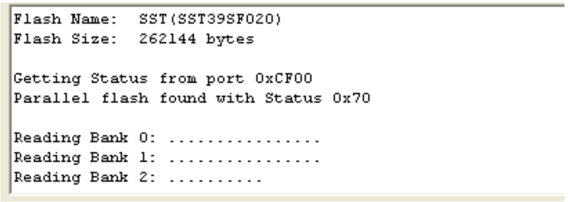
Reading the Firmware from the drive.

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



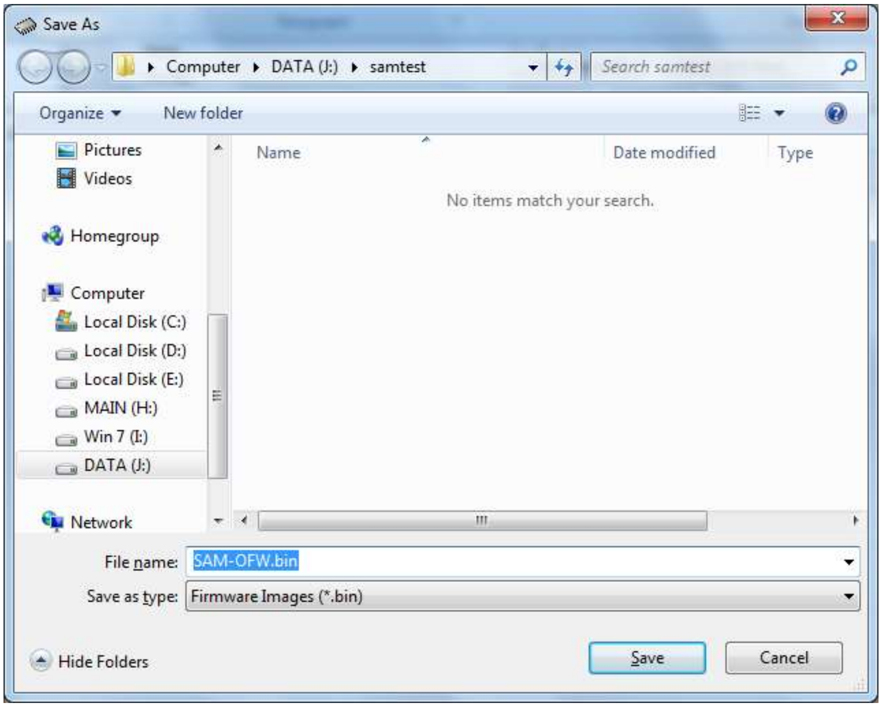
Again, watch the **Running Log** for constant status updates.

Firmware reading:



```
Flash Name:  SST(SST39SF020)
Flash Size:  262144 bytes

Getting Status from port 0xCF00
Parallel flash found with Status 0x70

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

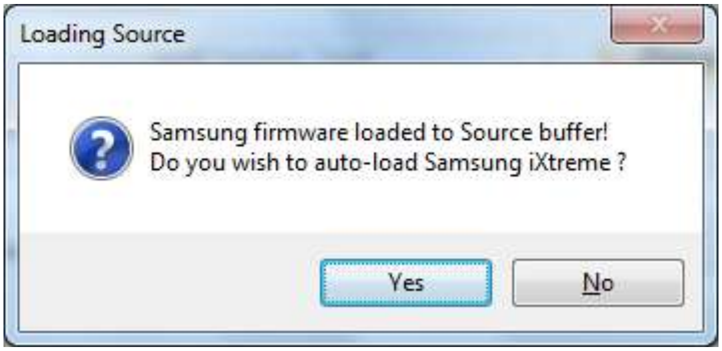
Once the firmware has been successfully read, JungleFlasher will prompt you to save it.



File name: SAM-OFW.bin

Save as type: Firmware Images (*.bin)

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.

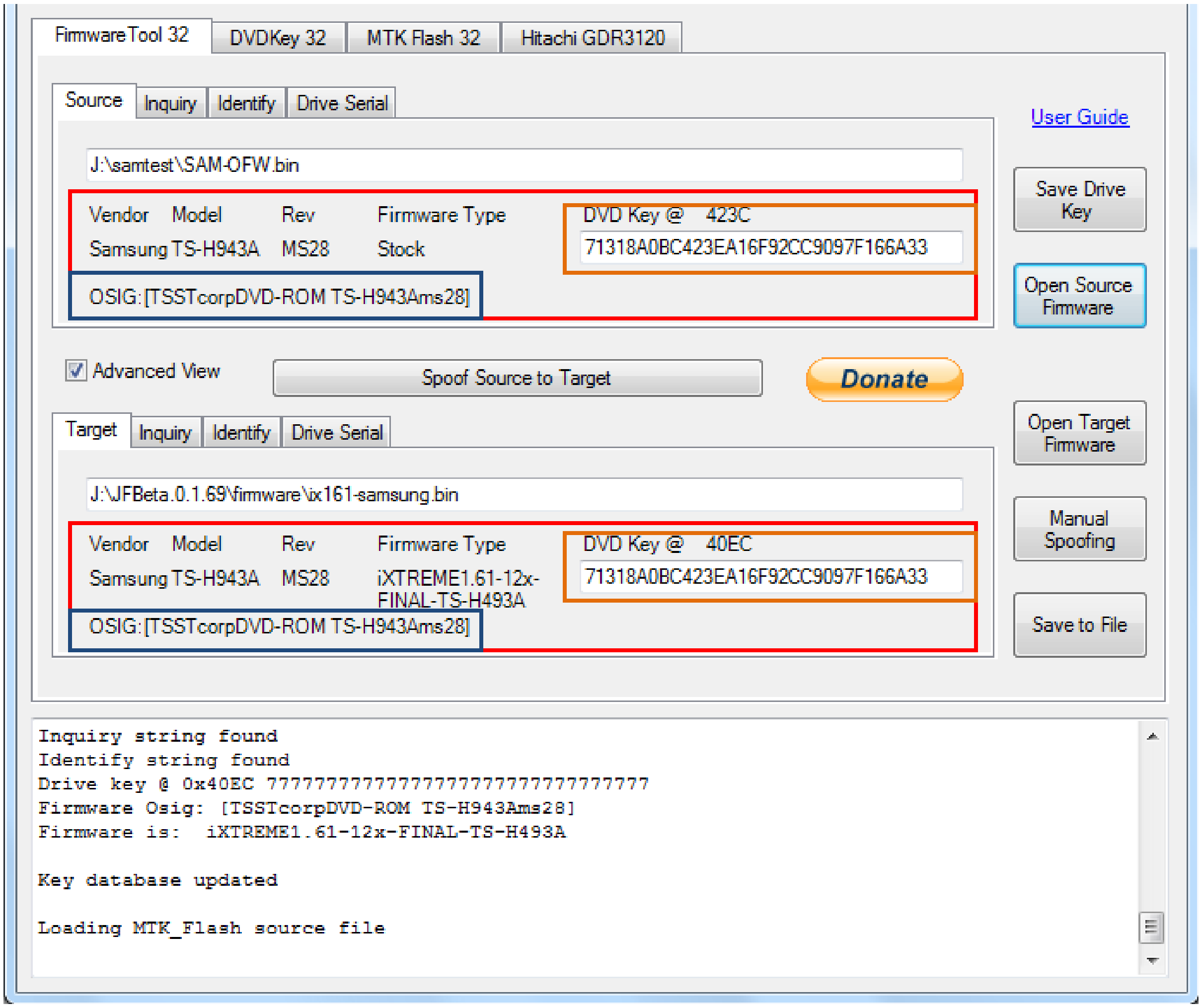


Loading Source

Samsung firmware loaded to Source buffer!
Do you wish to auto-load Samsung iXtreme ?

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**



J:\samtest\SAM-OFW.bin

Vendor Samsung | Model TS-H943A | Rev MS28 | Firmware Type Stock | DVD Key @ 423C 71318A0BC423EA16F92CC9097F166A33

OSIG: [TSSTcorpDVD-ROM TS-H943Ams28]

☑ Advanced View

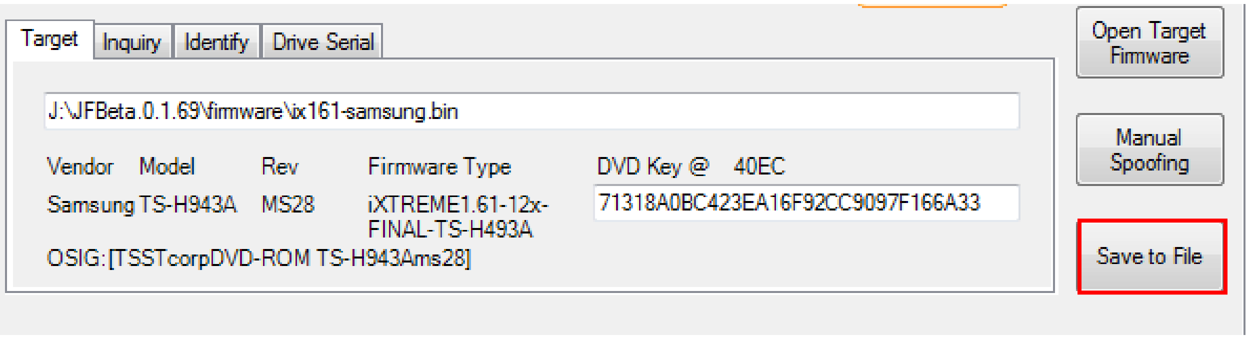
J:\JFBeta.0.1.69\firmware\ix161-samsung.bin

Vendor Samsung | Model TS-H943A | Rev MS28 | Firmware Type iXTREME1.61-12x-FINAL-TS-H493A | DVD Key @ 40EC 71318A0BC423EA16F92CC9097F166A33

OSIG: [TSSTcorpDVD-ROM TS-H943Ams28]

```
Inquiry string found
Identify string found
Drive key @ 0x40EC 77777777777777777777777777777777
Firmware Osig: [TSSTcorpDVD-ROM TS-H943Ams28]
Firmware is:  iXTREME1.61-12x-FINAL-TS-H493A

Key database updated

Loading MTK_Flash source file
```

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



J:\JFBeta.0.1.69\firmware\ix161-samsung.bin

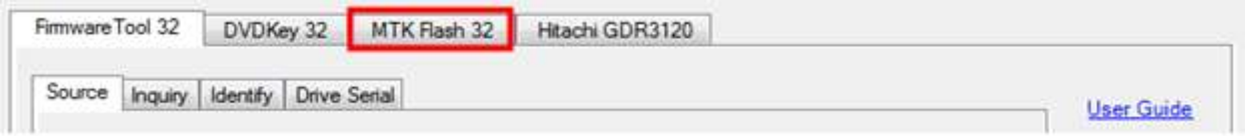
Vendor Samsung | Model TS-H943A | Rev MS28 | Firmware Type iXTREME1.61-12x-FINAL-TS-H493A | DVD Key @ 40EC 71318A0BC423EA16F92CC9097F166A33

OSIG: [TSSTcorpDVD-ROM TS-H943Ams28]

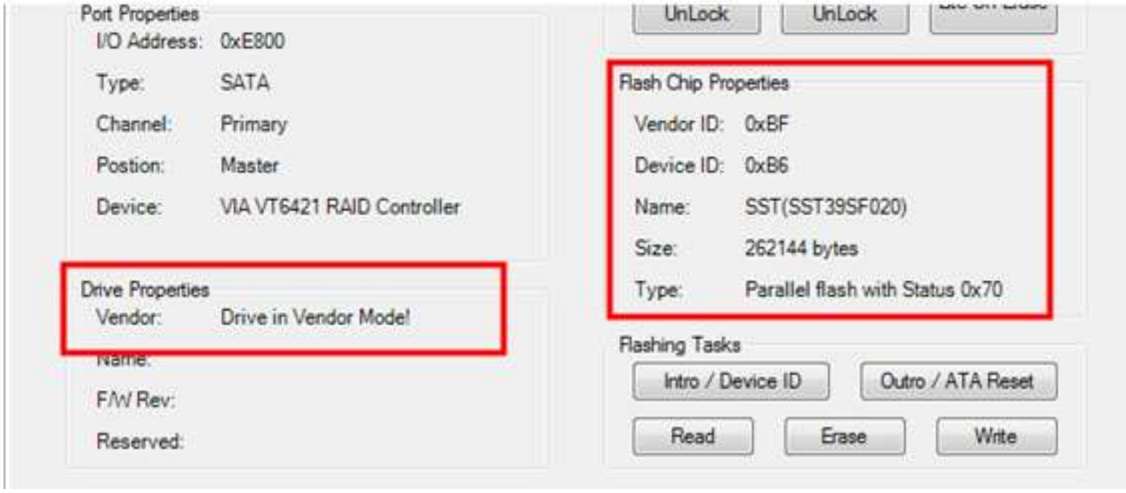
JungleFlasher will ask you where to save the hacked firmware and what you want to name it, and then you can proceed to write the firmware to the drive.

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.



Port Properties

I/O Address: 0xE800

Type: SATA

Channel: Primary

Postion: Master

Device: VIA VT6421 RAID Controller

Drive Properties

Vendor: Drive in Vendor Mode!

Name:

F/W Rev:

Reserved:

Flash Chip Properties

Vendor ID: 0xBF

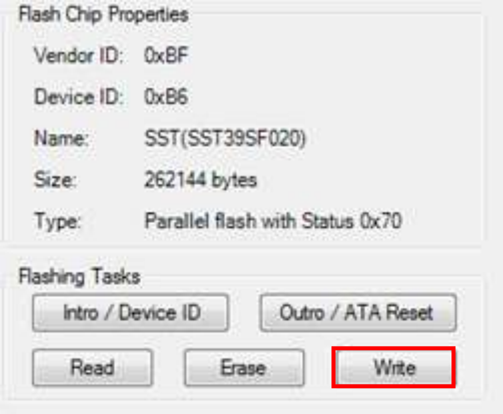
Device ID: 0xB6

Name: SST(SST39SF020)

Size: 262144 bytes

Type: Parallel flash with Status 0x70

Then, click **Write.**



Flash Chip Properties

Vendor ID: 0xBF

Device ID: 0xB6

Name: SST(SST39SF020)

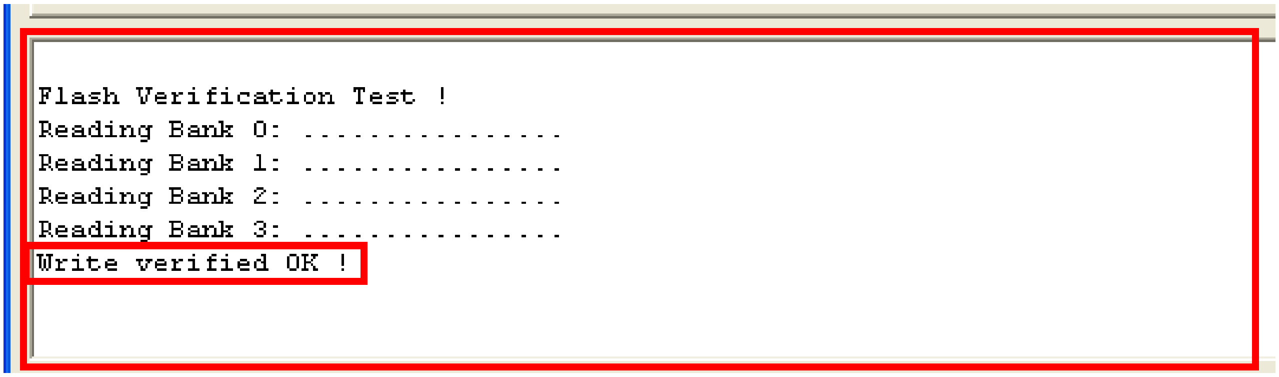
Size: 262144 bytes

Type: Parallel flash with Status 0x70

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!**



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

RETURN TO START OF TUTORIAL

BenQ VAD6038 (62430c and 64930c)

Overview

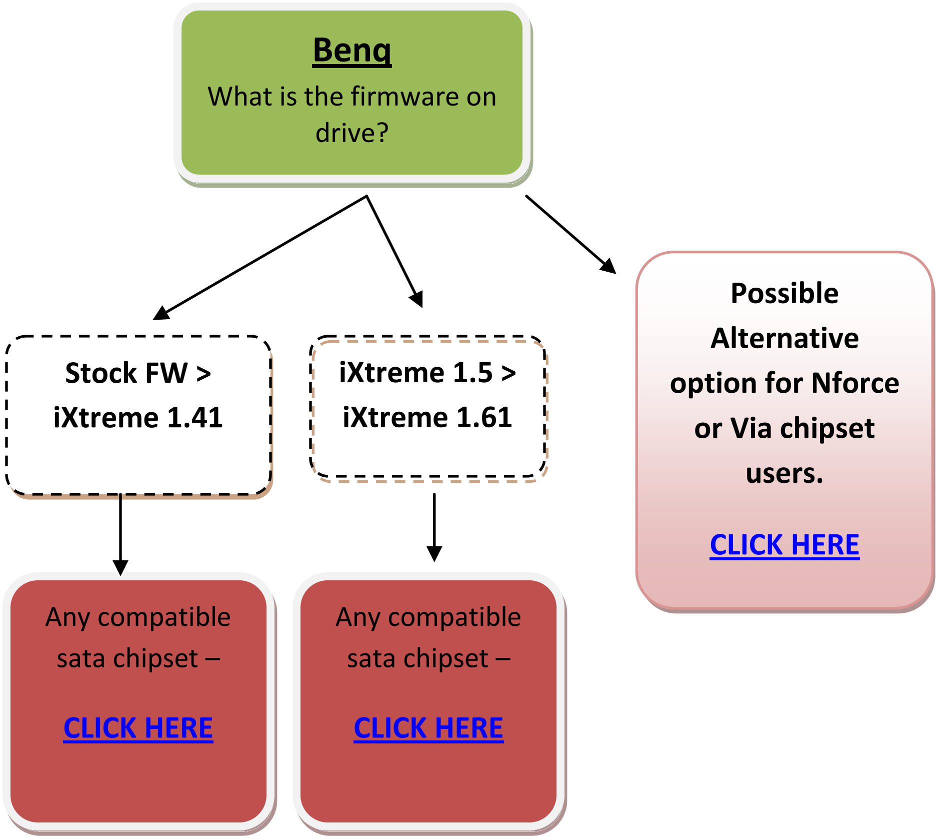
The BenQ Drive revision is tackled in a very similar way to the Samsung Drives.

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!



Benq

What is the firmware on drive?

Stock FW > iXtreme 1.41

iXtreme 1.5 > iXtreme 1.61

Possible Alternative option for Nforce or Via chipset users.

CLICK HERE

Any compatible sata chipset –

CLICK HERE

Any compatible sata chipset –

CLICK HERE

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.

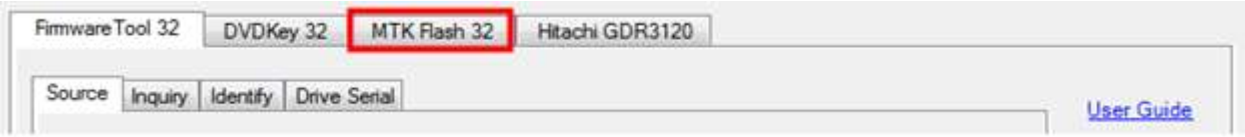
You need to power on the drive with the **Tray Half Open** – To do this using an Xbox 360 as Power source, eject the DVD drive and then **remove the power lead from the Drive.**

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.

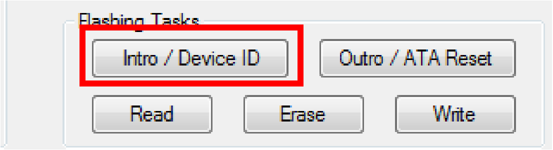
Using a Connectivity Kit / Xtractor to power the drive.

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.

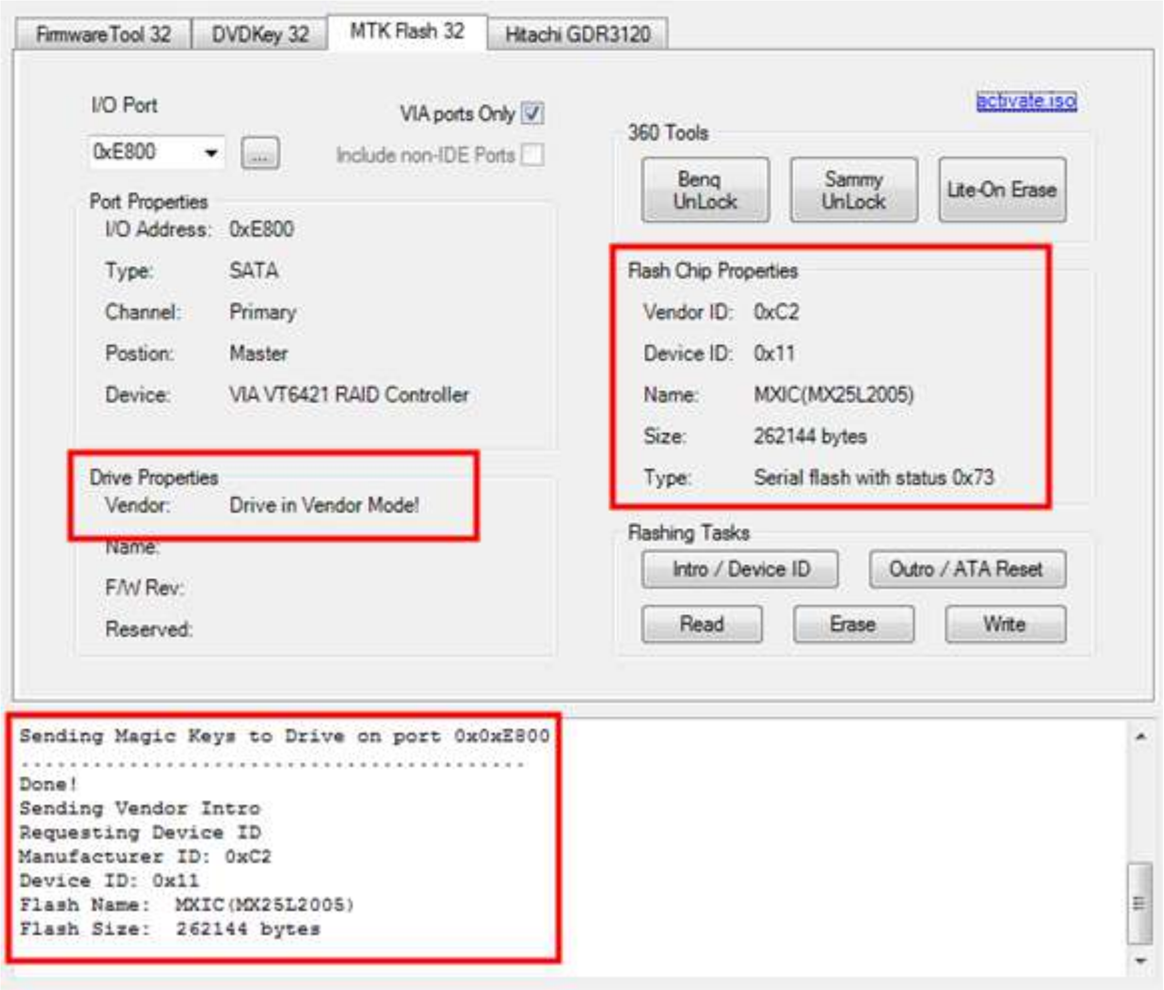
Ok, now we half the half open tray, we navigate to **MTKFlash32** tab if you haven't already.



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!".**



0xE800

Port Properties

I/O Address: 0xE800

Type: SATA

Channel: Primary

Postion: Master

Device: VIA VT6421 RAID Controller

Drive Properties

Vendor: Drive in Vendor Mode!

Name:

F/W Rev:

Reserved:

Flash Chip Properties

Vendor ID: 0xC2

Device ID: 0x11

Name: MXIC(MX25L2005)

Size: 262144 bytes

Type: Serial flash with status 0x73

```
Sending Magic Keys to Drive on port 0x0xE800
..........................................
Done!
Sending Vendor Intro
Requesting Device ID
Manufacturer ID: 0xC2
Device ID: 0x11
Flash Name:  MXIC(MX25L2005)
Flash Size:  262144 bytes
```

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

CLICK HERE TO PROCEED

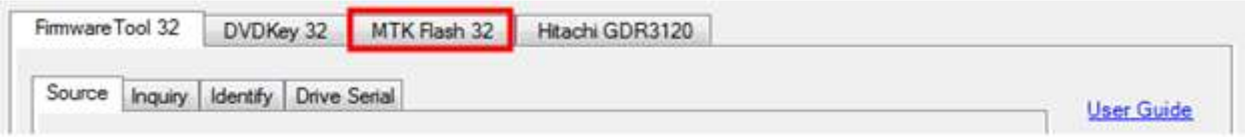
BenQ UnLock Stock/ iXtreme 1.1 -> 1.41 / Xtreme Firmware's Only.

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)

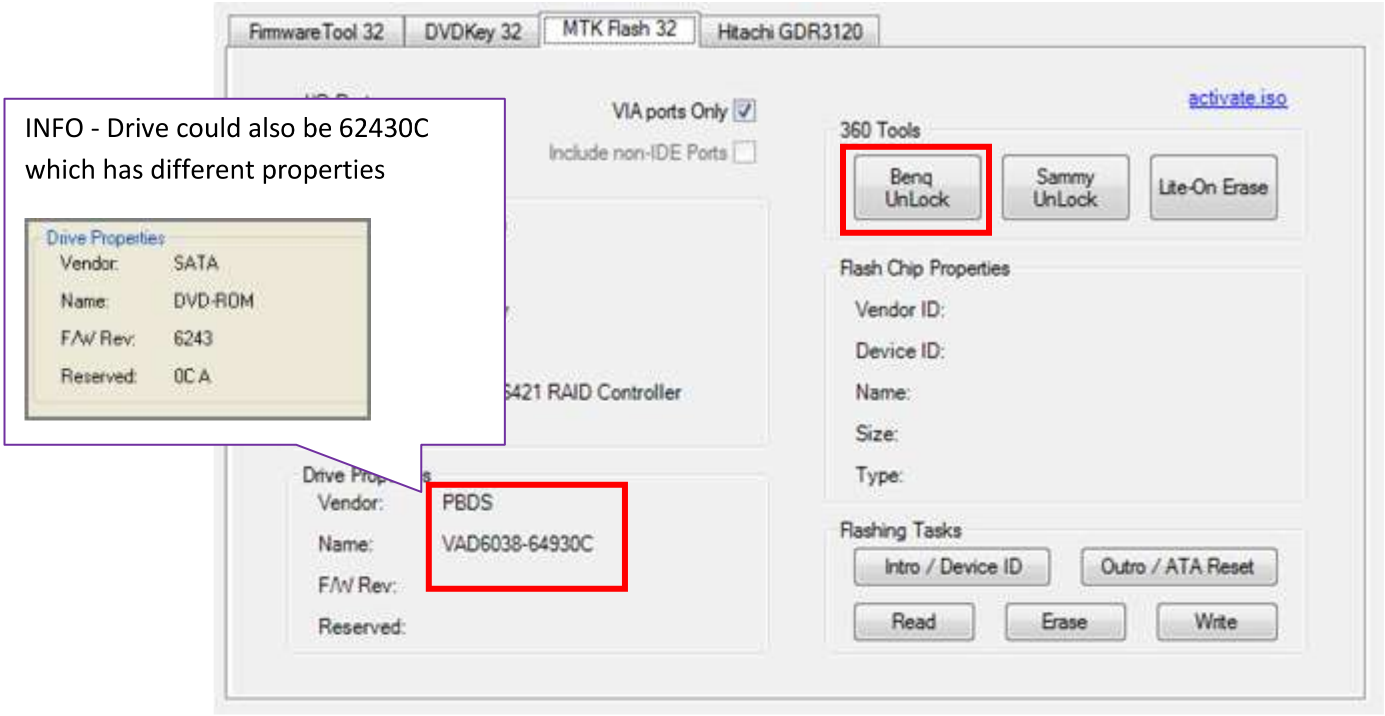
Connect your BenQ drive up via SATA to your PC, power on, and run JungleFlasher.

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** shows in the **Drive Properties** and click **BenQ UnLock.**

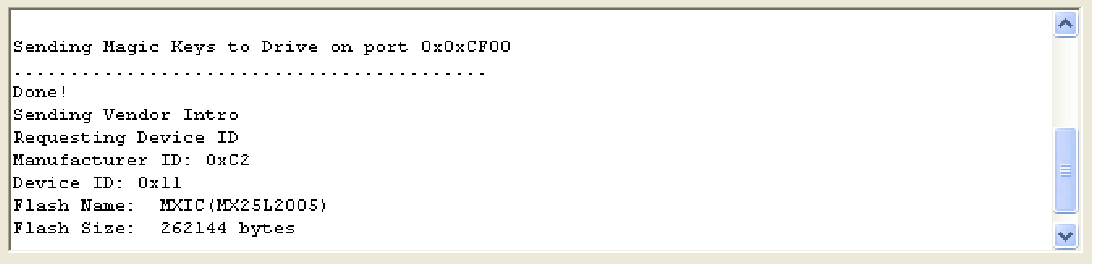


INFO - Drive could also be 62430C which has different properties

Drive Properties
Vendor: SATA
Name: DVD-ROM
F/W Rev: 6243
Reserved: 0C A

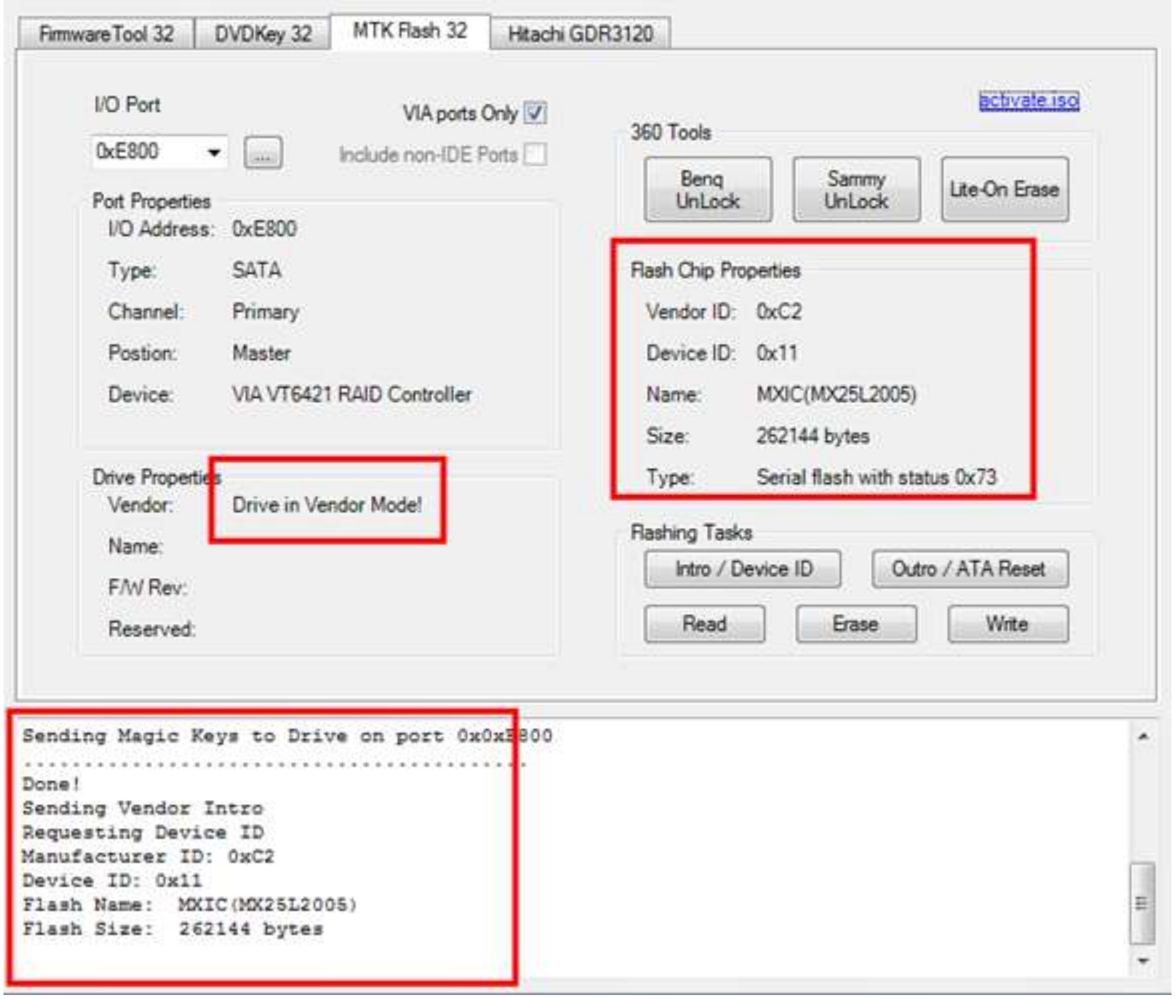
Drive Properties
Vendor: PBDS
Name: VAD6038-64930C
F/W Rev:
Reserved:

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.



```
Sending Magic Keys to Drive on port 0x0xCF00
........................................
Done!
Sending Vendor Intro
Requesting Device ID
Manufacturer ID: 0xC2
Device ID: 0x11
Flash Name:  MXIC(MX25L2005)
Flash Size:  262144 bytes
```

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.**



I/O Port: 0xE800

VIA ports Only ☑

Include non-IDE Ports □

Port Properties

I/O Address: 0xE800

Type: SATA

Channel: Primary

Postion: Master

Device: VIA VT6421 RAID Controller

Drive Properties

Vendor: Drive in Vendor Mode!

Name:

F/W Rev:

Reserved:

Flash Chip Properties

Vendor ID: 0xC2

Device ID: 0x11

Name: MXIC(MX25L2005)

Size: 262144 bytes

Type: Serial flash with status 0x73

```
Sending Magic Keys to Drive on port 0x0xE800
........................................
Done!
Sending Vendor Intro
Requesting Device ID
Manufacturer ID: 0xC2
Device ID: 0x11
Flash Name:  MXIC(MX25L2005)
Flash Size:  262144 bytes
```

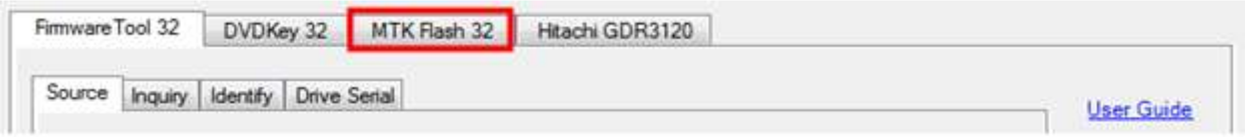
Once the drive is in **Vendor Mode**, you can proceed with **Reading the Drives Firmware.**

CLICK HERE TO PROCEED

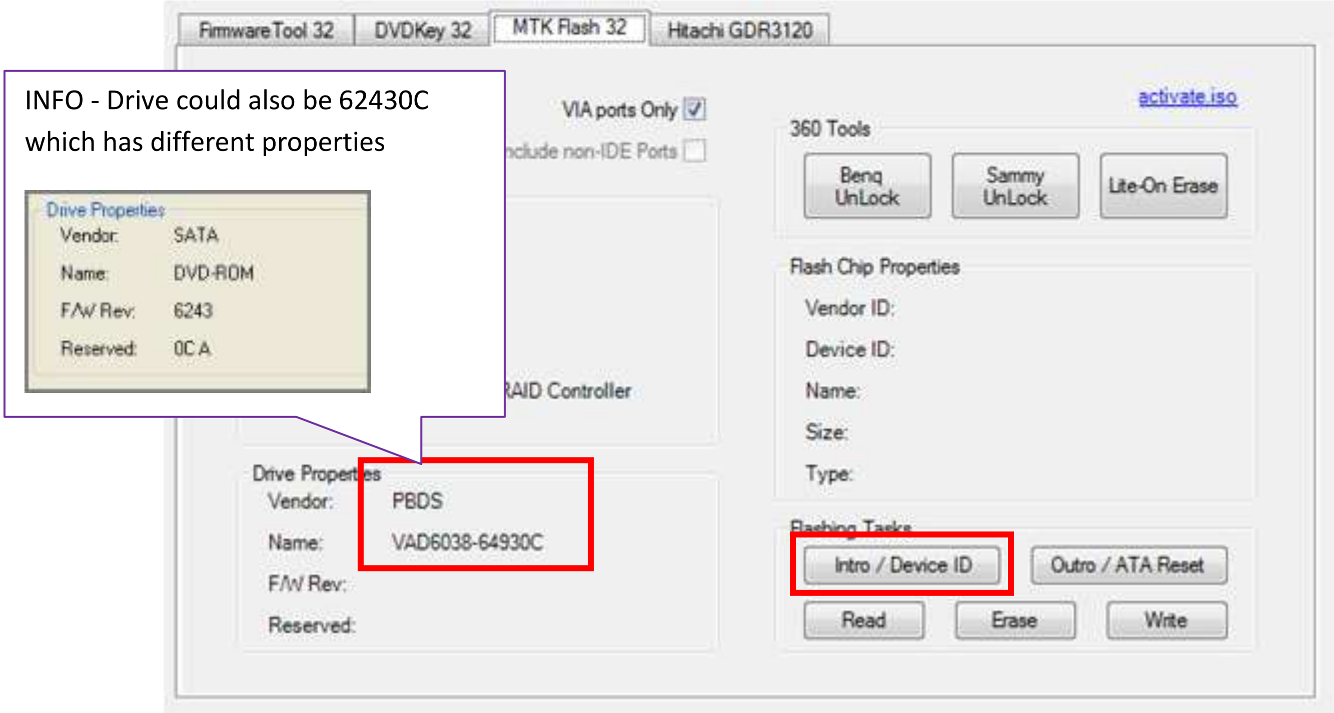
DeviceID Unlock / Vcc Trick (VIA/Nforce only) Stock + Modified Drives

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** shows in the **Drive Properties** and click **Intro / Device ID.**



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

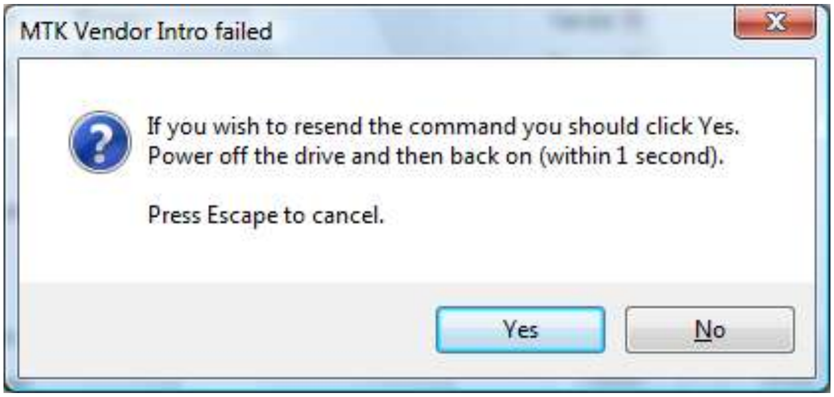
Drive Properties

Vendor:	SATA
Name:	DVD-ROM
F/W Rev:	6243
Reserved:	0C A

Drive Properties

Vendor:	PBDS
Name:	VAD6038-64930C
F/W Rev:	
Reserved:	

JungleFlasher will prompt you with instructions.

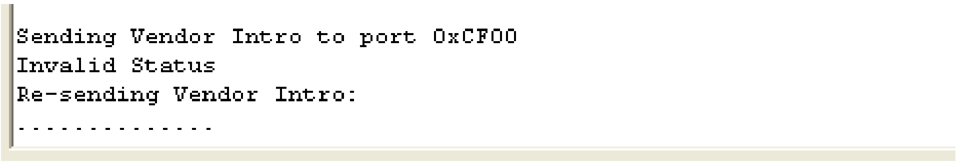


MTK Vendor Intro failed

If you wish to resend the command you should click Yes.
Power off the drive and then back on (within 1 second).

Press Escape to cancel.

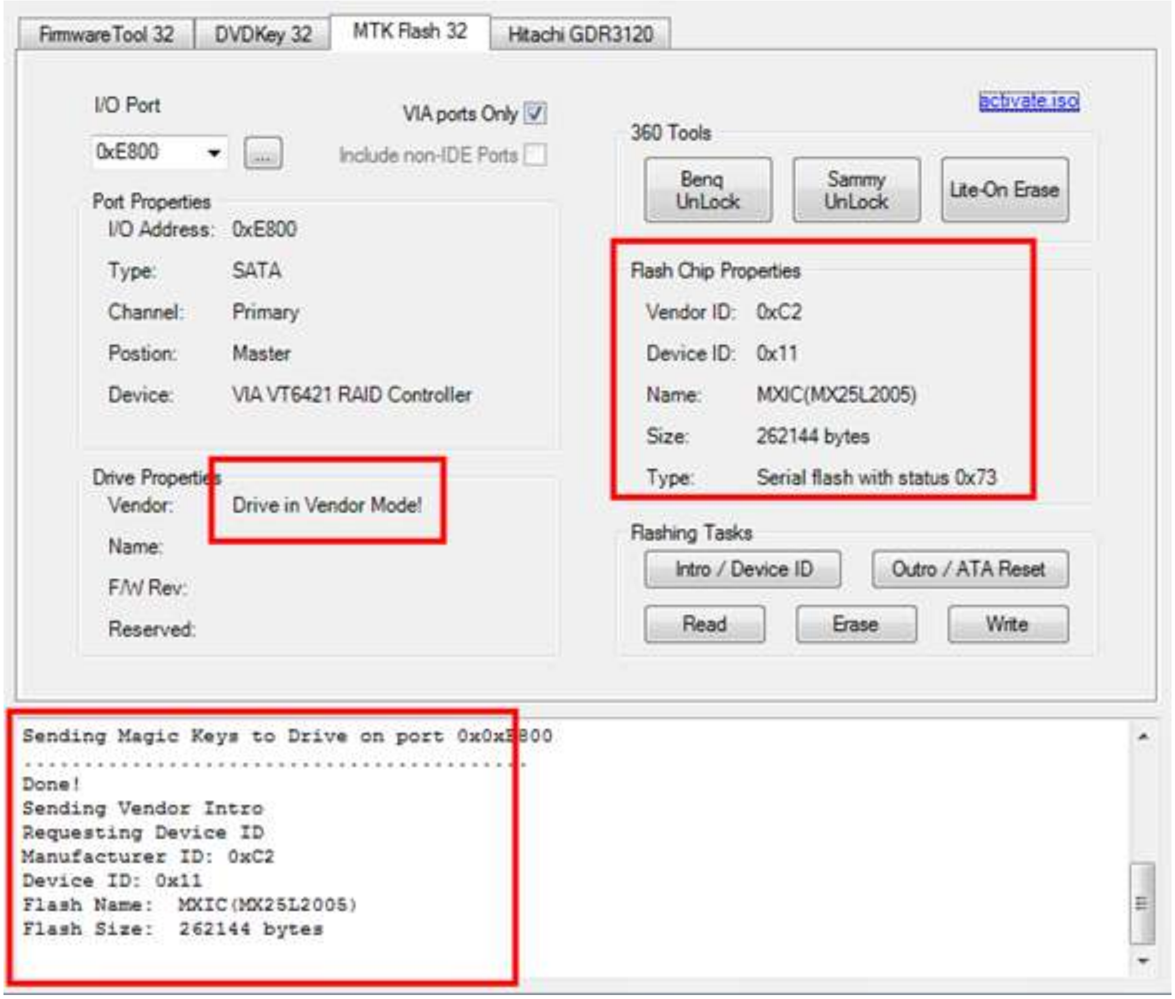
Click **Yes** the **Running Log** will display something similar to this.



```
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!".**



I/O Port: 0xE800

VIA ports Only ☑

Include non-IDE Ports □

Port Properties

I/O Address:	0xE800
Type:	SATA
Channel:	Primary
Postion:	Master
Device:	VIA VT6421 RAID Controller

Drive Properties

Vendor:	Drive in Vendor Mode!
Name:	
F/W Rev:	
Reserved:	

Flash Chip Properties

Vendor ID:	0xC2
Device ID:	0x11
Name:	MXIC(MX25L2005)
Size:	262144 bytes
Type:	Serial flash with status 0x73

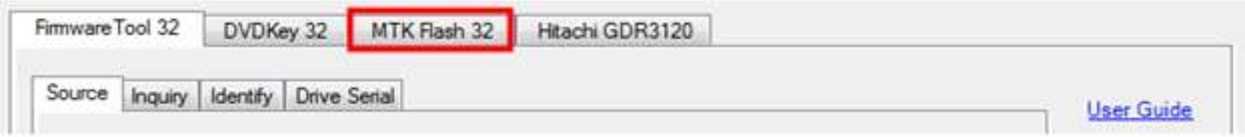
```
Sending Magic Keys to Drive on port 0x0xE800
.........................................
Done!
Sending Vendor Intro
Requesting Device ID
Manufacturer ID: 0xC2
Device ID: 0x11
Flash Name:  MXIC(MX25L2005)
Flash Size:  262144 bytes
```

CLICK HERE TO PROCEED

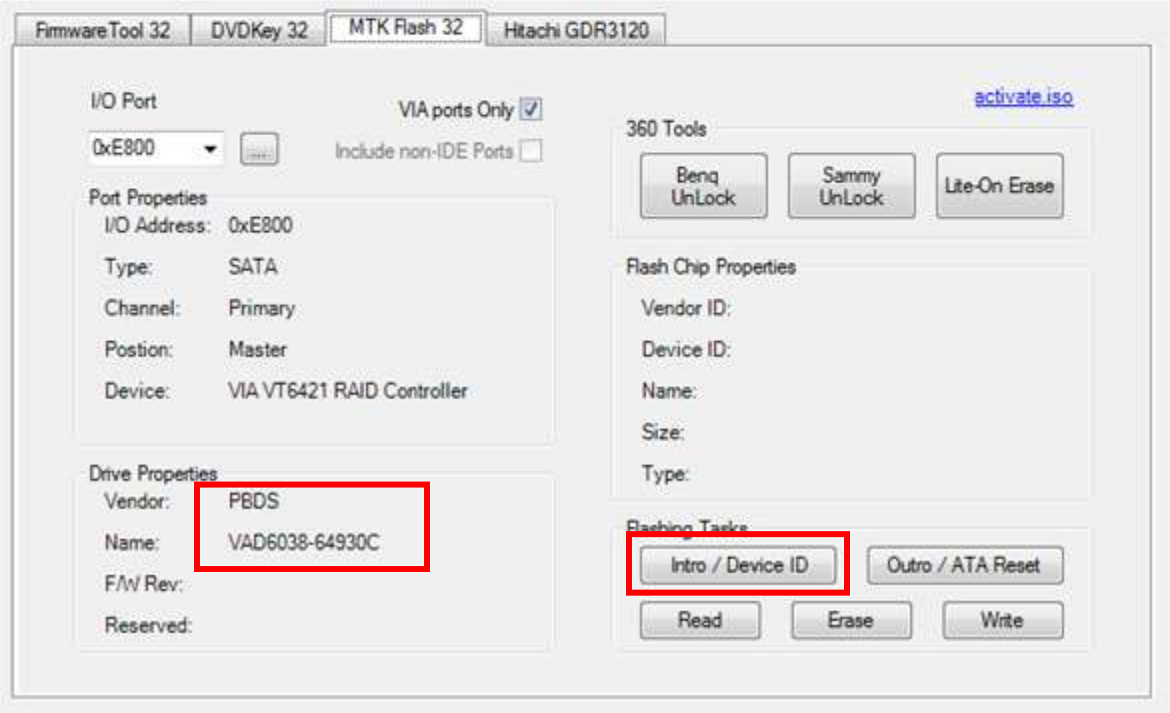
If it didn’t work – read on

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** shows in the **Drive Properties** and click **Intro / Device ID.**



I/O Port: 0xE800

VIA ports Only ☑

Include non-IDE Ports □

Port Properties

I/O Address: 0xE800

Type: SATA

Channel: Primary

Postion: Master

Device: VIA VT6421 RAID Controller

Drive Properties

Vendor: PBDS

Name: VAD6038-64930C

F/W Rev:

Reserved:

Flash Chip Properties

Vendor ID:

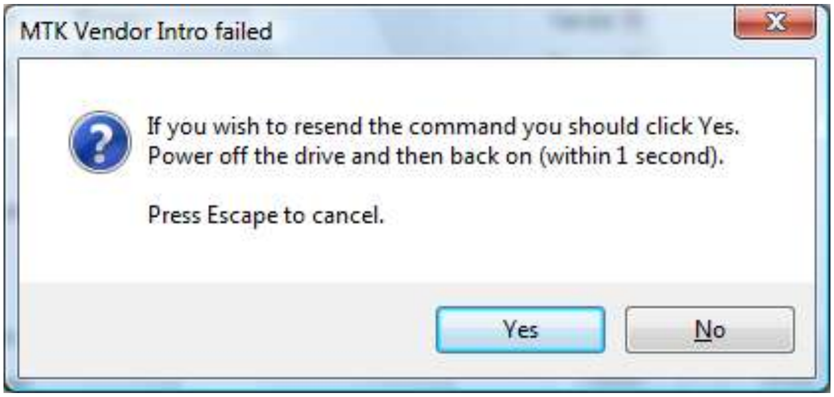
Device ID:

Name:

Size:

Type:

JungleFlasher will prompt you with instructions.



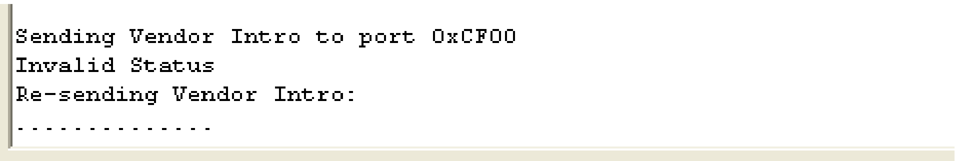
MTK Vendor Intro failed

If you wish to resend the command you should click Yes.
Power off the drive and then back on (within 1 second).

Press Escape to cancel.

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

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

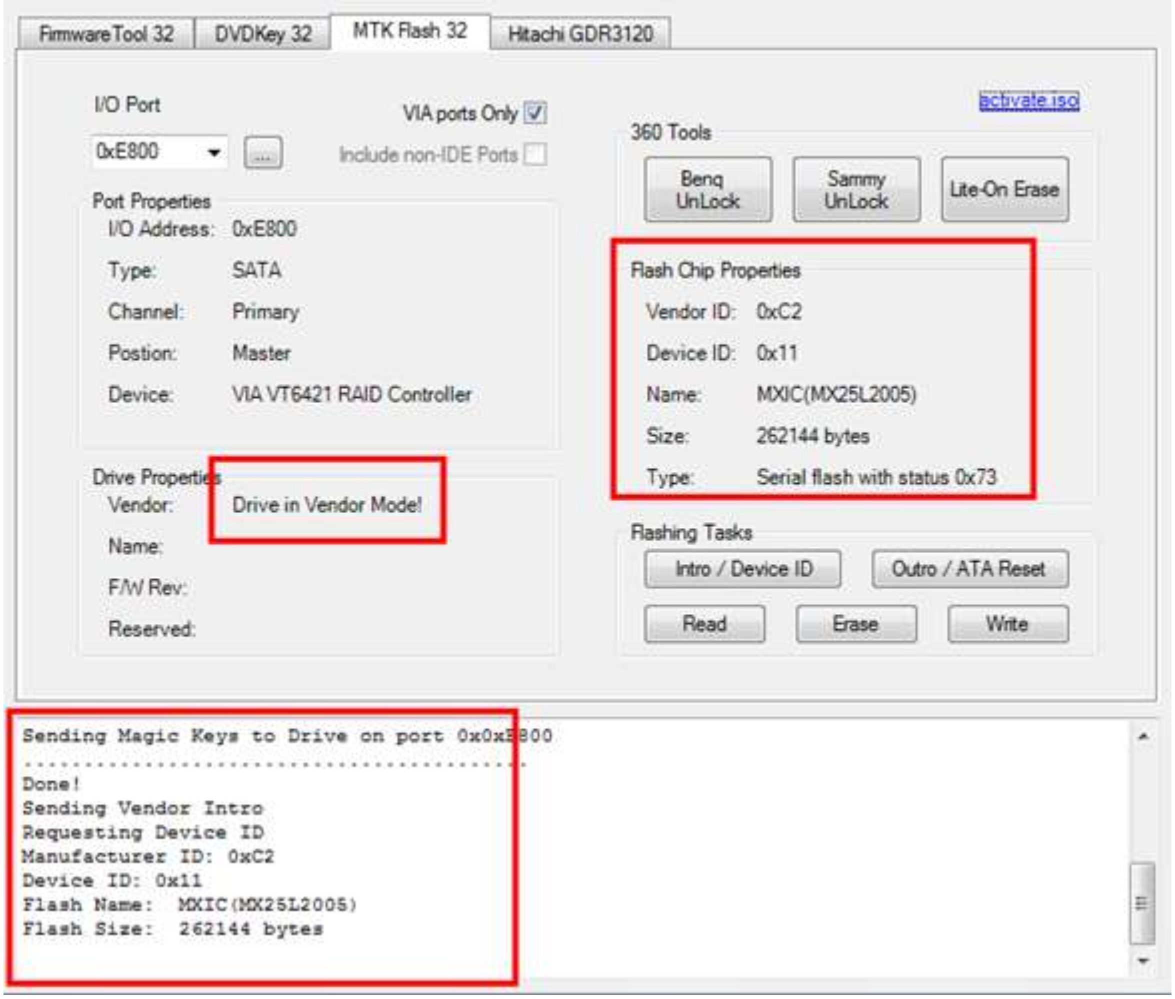


```
Sending Vendor Intro to port 0xCF00
Invalid Status
Re-sending Vendor Intro:
..............
```

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!”.**



I/O Port: 0xE800

VIA ports Only ☑

Include non-IDE Ports □

Port Properties

I/O Address:	0xE800
Type:	SATA
Channel:	Primary
Postion:	Master
Device:	VIA VT6421 RAID Controller

Drive Properties

Vendor:	Drive in Vendor Mode!
Name:	
F/W Rev:	
Reserved:	

Flash Chip Properties

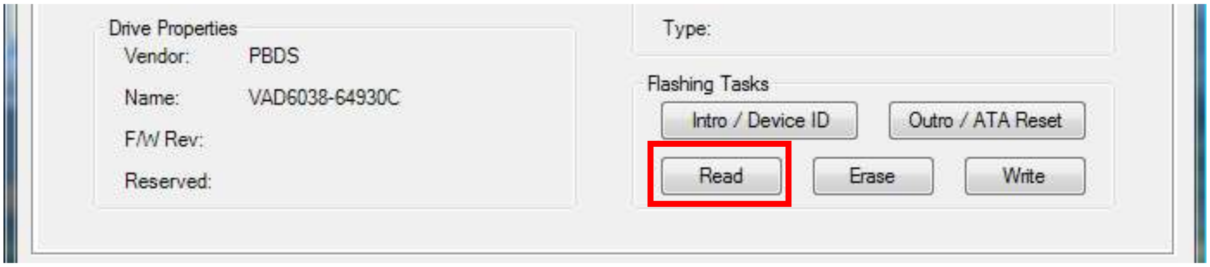
Vendor ID:	0xC2
Device ID:	0x11
Name:	MXIC(MX25L2005)
Size:	262144 bytes
Type:	Serial flash with status 0x73

```
Sending Magic Keys to Drive on port 0x0xE800
.........................................
Done!
Sending Vendor Intro
Requesting Device ID
Manufacturer ID: 0xC2
Device ID: 0x11
Flash Name:  MXIC(MX25L2005)
Flash Size:  262144 bytes
```

CLICK HERE TO PROCEED

Reading the Firmware from the drive.

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



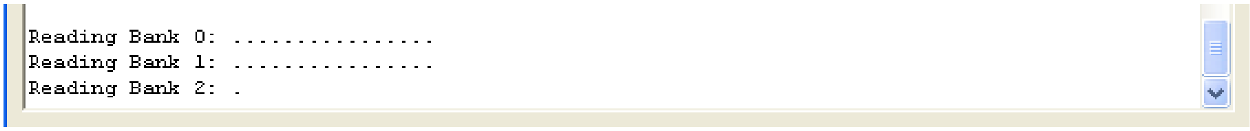
Vendor: PBDS

Name: VAD6038-64930C

F/W Rev:

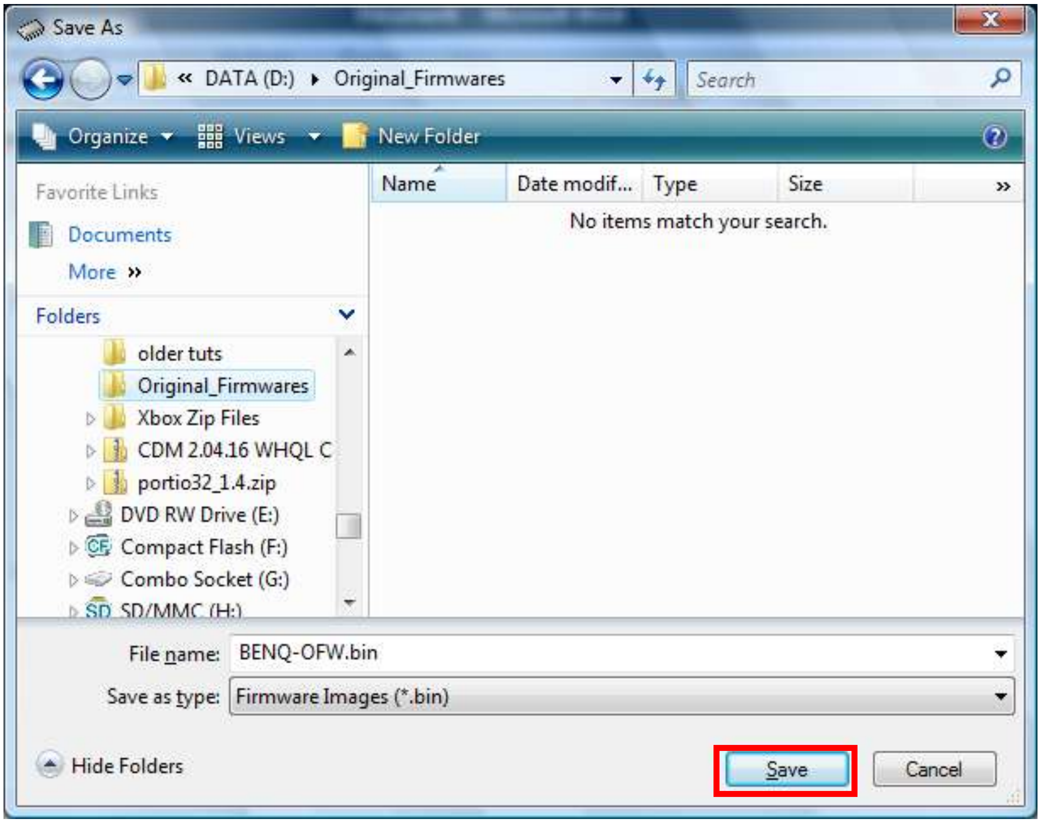
Reserved:

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



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

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.**

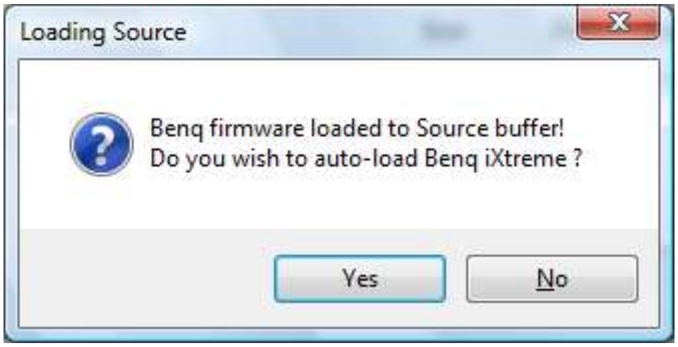


No items match your search.

File name: BENQ-OFW.bin

Save as type: Firmware Images (*.bin)

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.



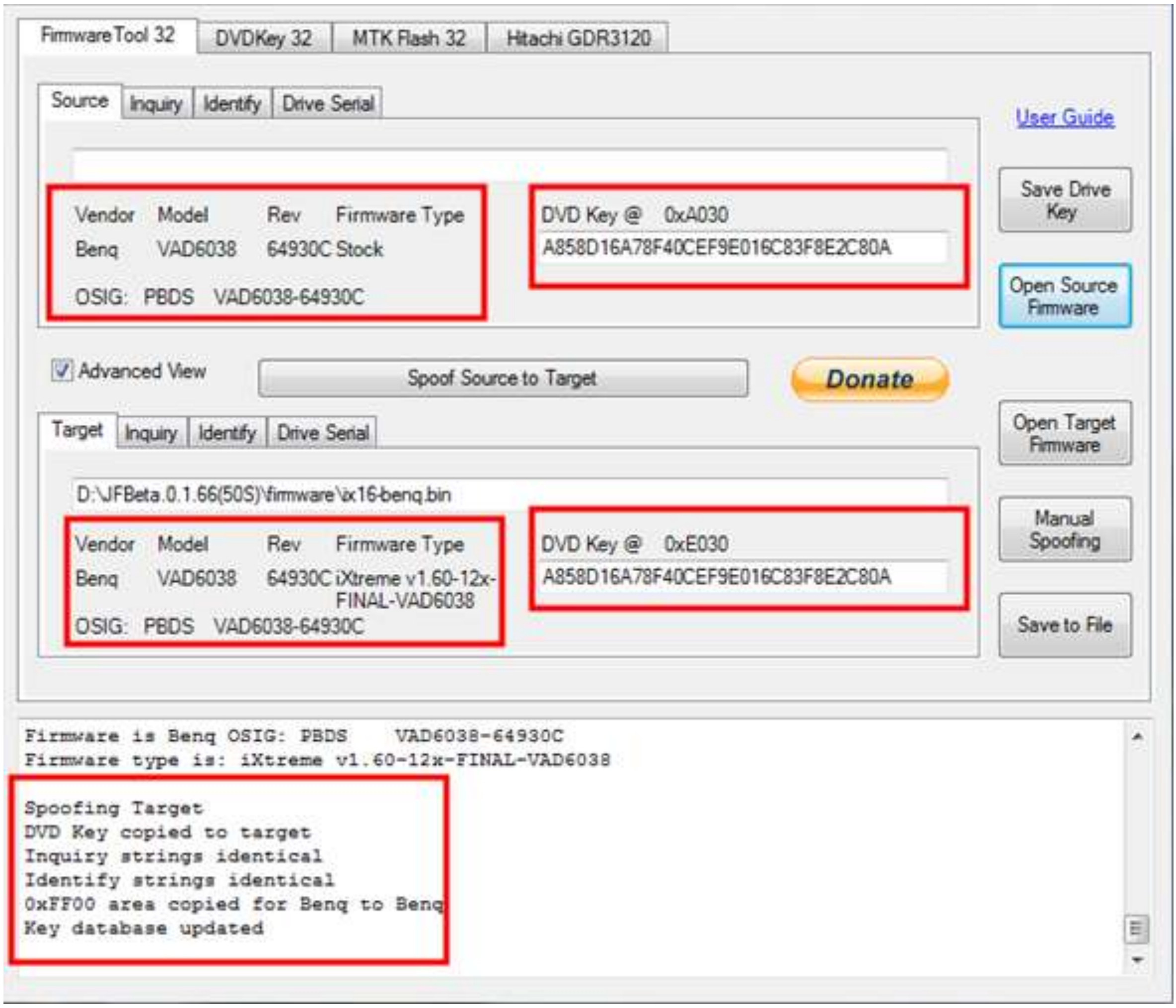
Loading Source

Benq firmware loaded to Source buffer!
Do you wish to auto-load Benq iXtreme ?

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** 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.



Source:

Vendor	Model	Rev	Firmware Type
Benq	VAD6038	64930C	Stock

OSIG: PBDS VAD6038-64930C

DVD Key @ 0xA030
A858D16A78F40CEF9E016C83F8E2C80A

☑ Advanced View

Target:

D:\JFBeta.0.1.66(50S)\firmware\ix16-benq.bin

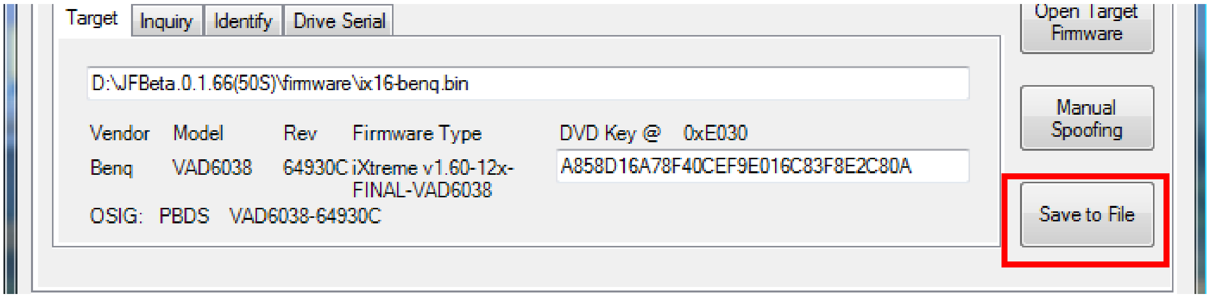
Vendor	Model	Rev	Firmware Type
Benq	VAD6038	64930C	iXtreme v1.60-12x-FINAL-VAD6038

OSIG: PBDS VAD6038-64930C

DVD Key @ 0xE030
A858D16A78F40CEF9E016C83F8E2C80A

```
Firmware is Benq OSIG: PBDS    VAD6038-64930C
Firmware type is: iXtreme v1.60-12x-FINAL-VAD6038

Spoofing Target
DVD Key copied to target
Inquiry strings identical
Identify strings identical
0xFF00 area copied for Benq to Benq
Key database updated
```

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



D:\JFBeta.0.1.66(50S)\firmware\ix16-benq.bin

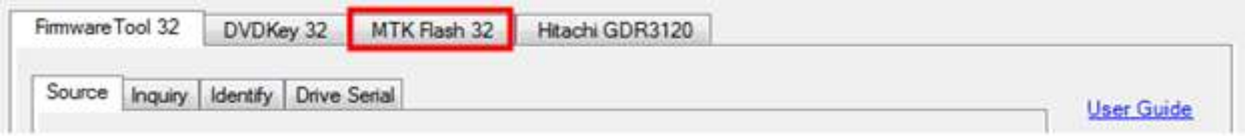
Vendor	Model	Rev	Firmware Type
Benq	VAD6038	64930C	iXtreme v1.60-12x-FINAL-VAD6038

OSIG: PBDS VAD6038-64930C

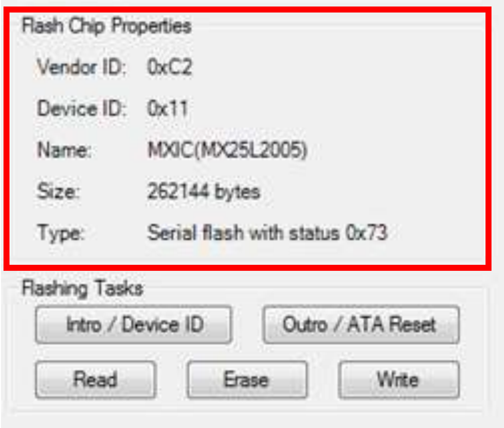
DVD Key @ 0xE030
A858D16A78F40CEF9E016C83F8E2C80A

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.



Flash Chip Properties

Vendor ID: 0xC2

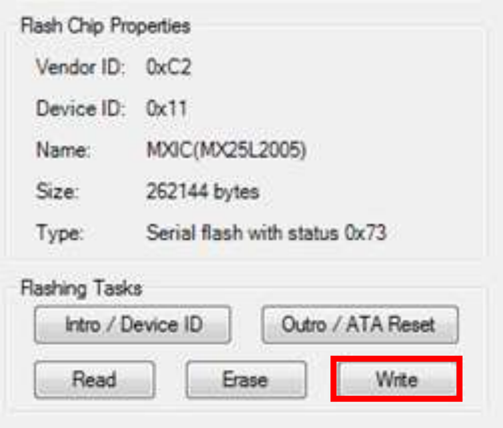
Device ID: 0x11

Name: MXIC(MX25L2005)

Size: 262144 bytes

Type: Serial flash with status 0x73

Then, click **Write.**



Flash Chip Properties

Vendor ID: 0xC2

Device ID: 0x11

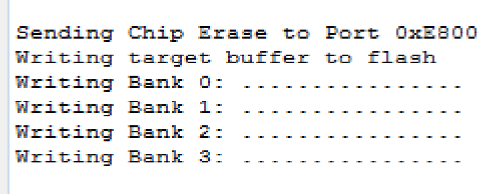
Name: MXIC(MX25L2005)

Size: 262144 bytes

Type: Serial flash with status 0x73

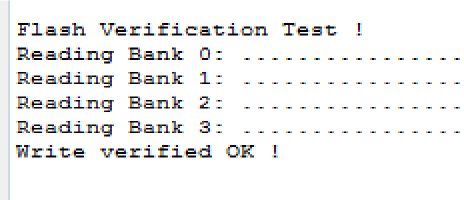
Write Command, will send Chip Erase prior to writing and then proceed to write the 4 banks of the firmware (banks 0/1/2/3).

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



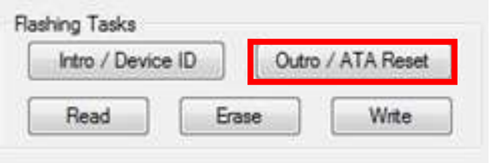
```
Sending Chip Erase to Port 0xE800
Writing target buffer to flash
Writing Bank 0: ................
Writing Bank 1: ................
Writing Bank 2: ................
Writing Bank 3: ................
```

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!**



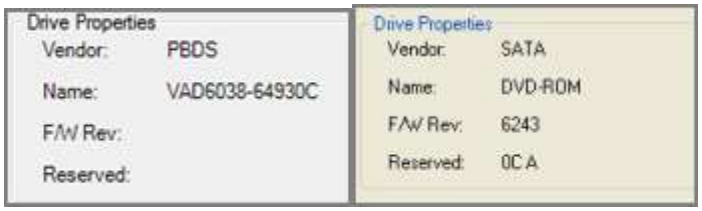
```
Flash Verification Test !
Reading Bank 0: ................
Reading Bank 1: ................
Reading Bank 2: ................
Reading Bank 3: ................
Write verified OK !
```

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.



Drive Properties
Vendor: PBDS
Name: VAD6038-64930C
F/W Rev:
Reserved:

Drive Properties
Vendor: SATA
Name: DVD-ROM
F/W Rev: 6243
Reserved: 0C A

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

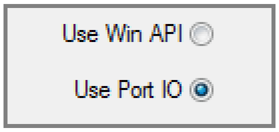
Hitachi GDR-3120L.

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.**



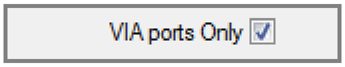
Use Win API ○

Use Port IO ●

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 ports Only ☑

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 drives 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

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.

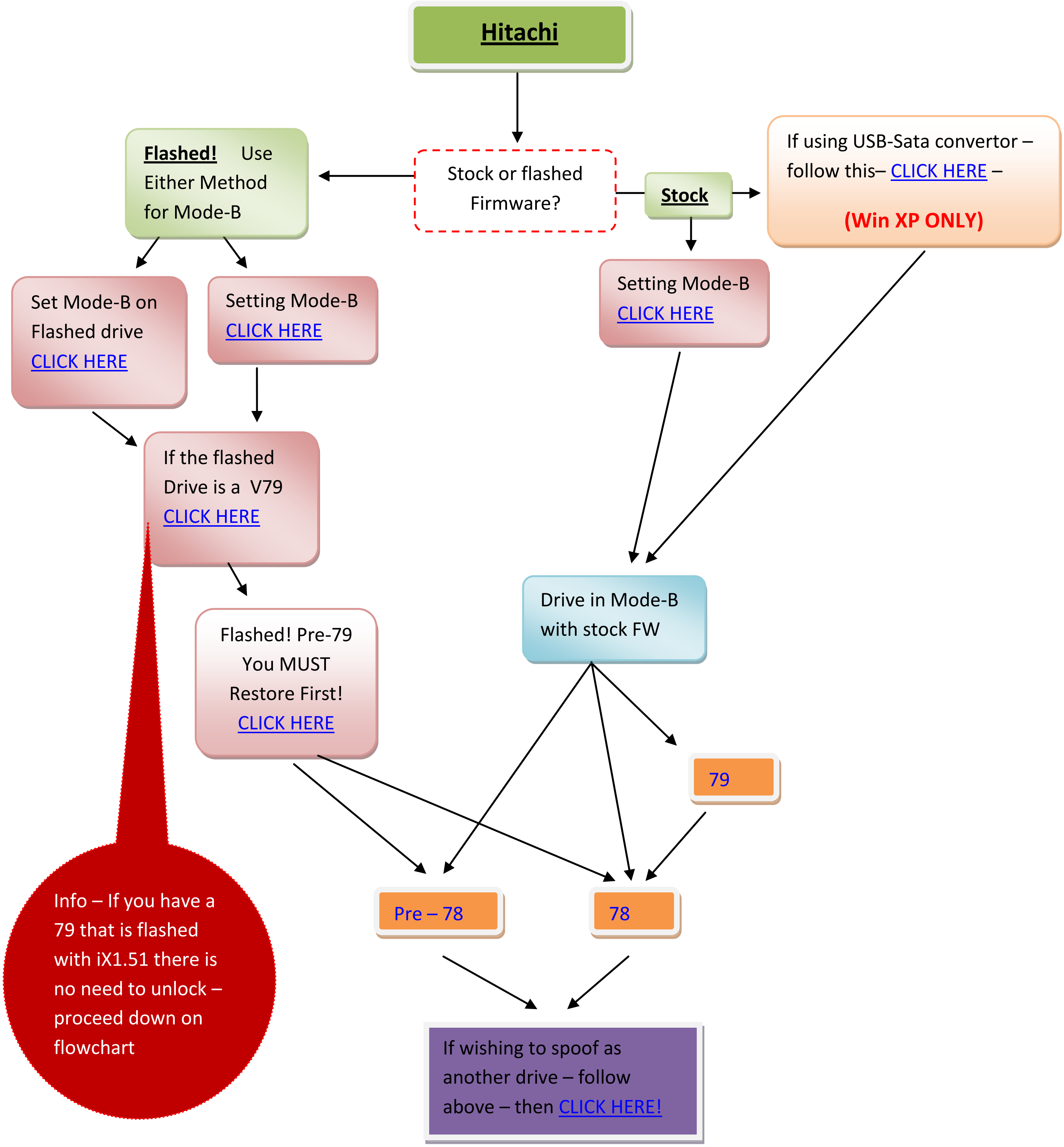
Windows API Users, after setting ModeB, you must wait for hardware changes to be detected (15 secs) If nothing is detected, click "Refresh"

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.

CLICK TO CONTINUE



Hitachi

Stock or flashed Firmware?

Flashed! Use Either Method for Mode-B

Stock

If using USB-Sata convertor – follow this– CLICK HERE –

(Win XP ONLY)

Set Mode-B on Flashed drive CLICK HERE

Setting Mode-B CLICK HERE

Setting Mode-B CLICK HERE

If the flashed Drive is a V79 CLICK HERE

Drive in Mode-B with stock FW

Flashed! Pre-79 You MUST Restore First! CLICK HERE

79

Pre – 78

78

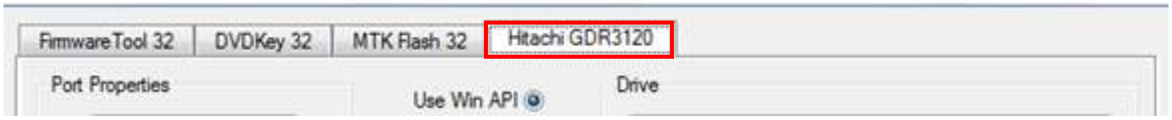
Info – If you have a 79 that is flashed with iX1.51 there is no need to unlock – proceed down on flowchart

If wishing to spoof as another drive – follow above – then CLICK HERE!

Setting ModeB

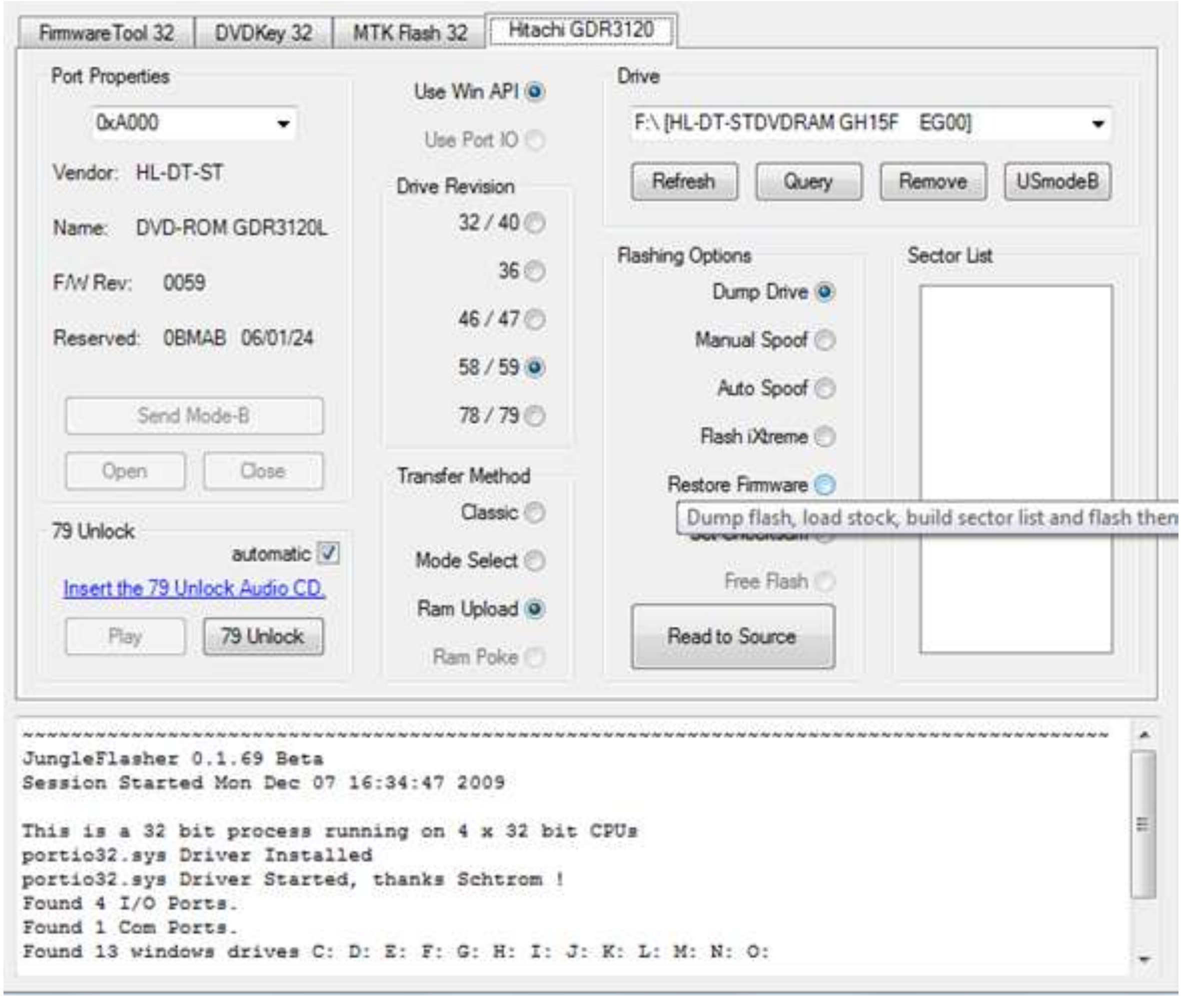
Connect your Hitachi Drive via sata, power it on, then open JungleFlasher and you will be presented with the welcome screen

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



Use Win API ●

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



Port Properties: 0xA000

Vendor: HL-DT-ST

Name: DVD-ROM GDR3120L

F/W Rev: 0059

Reserved: 0BMAB 06/01/24

Use Win API ●

Use Port IO ○

Drive Revision: 32 / 40 ○ 36 ○ 46 / 47 ○ 58 / 59 ● 78 / 79 ○

Transfer Method: Classic ○ Mode Select ○ Ram Upload ● Ram Poke ○

Drive: F:\ [HL-DT-STDVDRAM GH15F EG00]

Flashing Options: Dump Drive ● Manual Spoof ○ Auto Spoof ○ Flash iXtreme ○ Restore Firmware ○ Free Flash ○

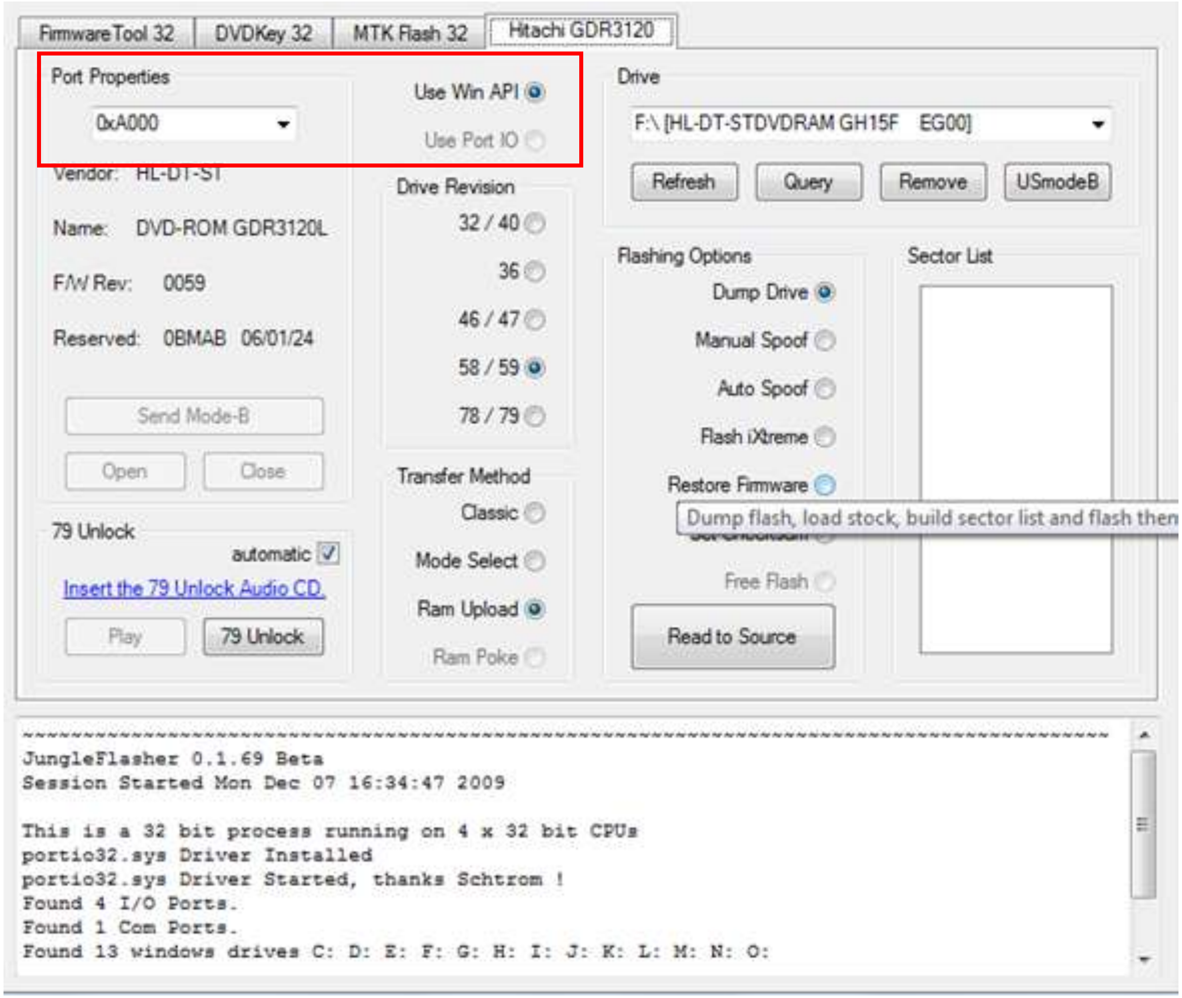
Dump flash, load stock, build sector list and flash then

79 Unlock: automatic ☑

Insert the 79 Unlock Audio CD.

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
JungleFlasher 0.1.69 Beta
Session Started Mon Dec 07 16:34:47 2009

This is a 32 bit process running on 4 x 32 bit CPUs
portio32.sys Driver Installed
portio32.sys Driver Started, thanks Schtrom !
Found 4 I/O Ports.
Found 1 Com Ports.
Found 13 windows drives C: D: E: F: G: H: I: J: K: L: M: N: O:
```

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



Port Properties

0xA000

Use Win API ●

Use Port IO ○

Vendor: HL-DT-ST

Name: DVD-ROM GDR3120L

F/W Rev: 0059

Reserved: 0BMAB 06/01/24

79 Unlock

automatic ☑

Drive Revision

32 / 40 ○

36 ○

46 / 47 ○

58 / 59 ●

78 / 79 ○

Transfer Method

Classic ○

Mode Select ○

Ram Upload ●

Ram Poke ○

Drive

F:\ [HL-DT-STDVDRAM GH15F EG00]

Flashing Options

Dump Drive ●

Manual Spoof ○

Auto Spoof ○

Flash iXtreme ○

Restore Firmware ○

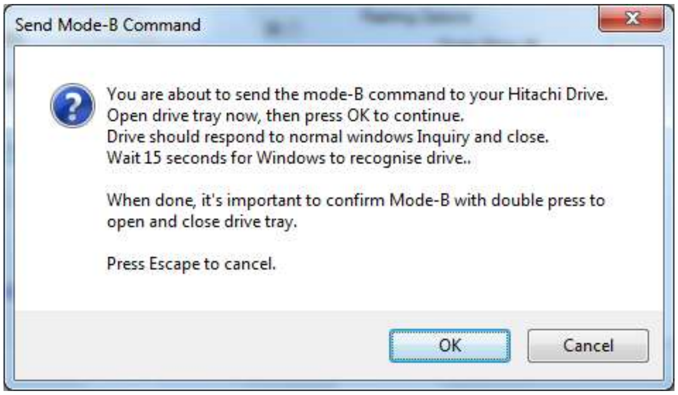
Dump flash, load stock, build sector list and flash then

Free Flash ○

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
JungleFlasher 0.1.69 Beta
Session Started Mon Dec 07 16:34:47 2009

This is a 32 bit process running on 4 x 32 bit CPUs
portio32.sys Driver Installed
portio32.sys Driver Started, thanks Schtrom !
Found 4 I/O Ports.
Found 1 Com Ports.
Found 13 windows drives C: D: E: F: G: H: I: J: K: L: M: N: O:
```

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, its advised you do as it states as the **ModeB button on Connectivity Kit, can cause issues**



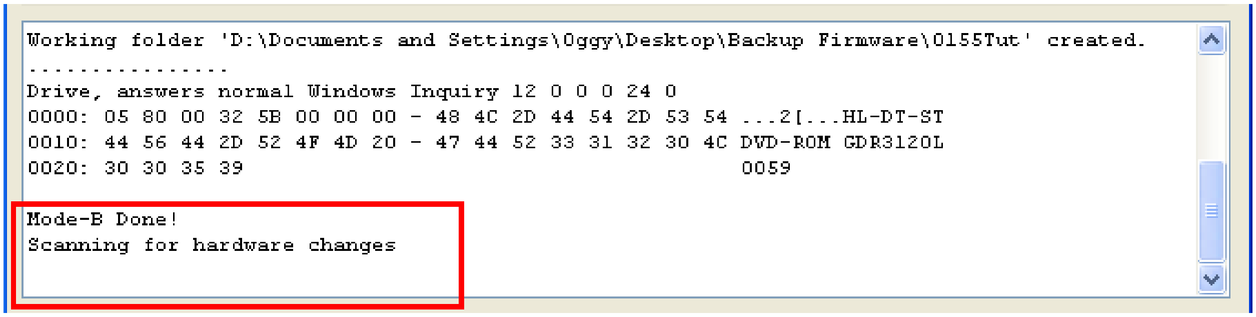
You are about to send the mode-B command to your Hitachi Drive.
Open drive tray now, then press OK to continue.
Drive should respond to normal windows Inquiry and close.
Wait 15 seconds for Windows to recognise drive..

When done, it's important to confirm Mode-B with double press to open and close drive tray.

Press Escape to cancel.

Once done, click **Ok**

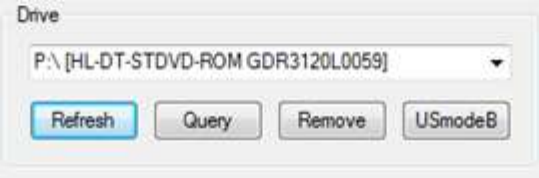
The drive should now report as in **ModeB**



```
Working folder 'D:\Documents and Settings\Oggy\Desktop\Backup Firmware\0155Tut' created.
................
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
```

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 seen similar to this under the ‘Drive’ section



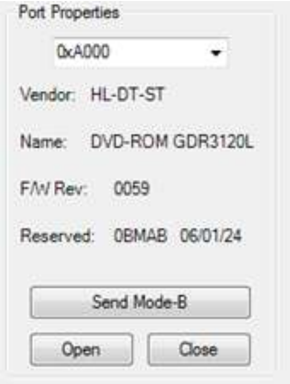
Drive

P:\ [HL-DT-STDVD-ROM GDR3120L0059]

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**



Port Properties

0xA000

Vendor: HL-DT-ST

Name: DVD-ROM GDR3120L

F/W Rev: 0059

Reserved: 0BMAB 06/01/24

BACK TO FLOWCHART!

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.
5. **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!

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).

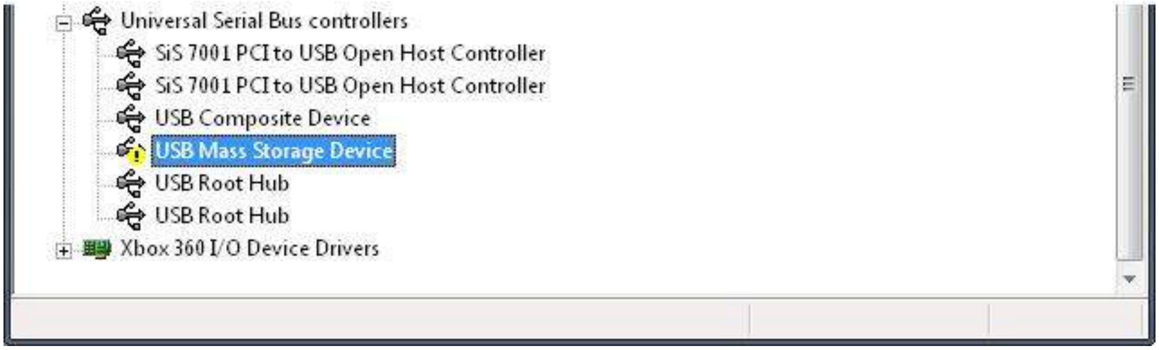
First you need to connect the drive to your PC with a SATA-USB Bridge Adapter

Windows will automatically install the device as

USB Mass Storage Device

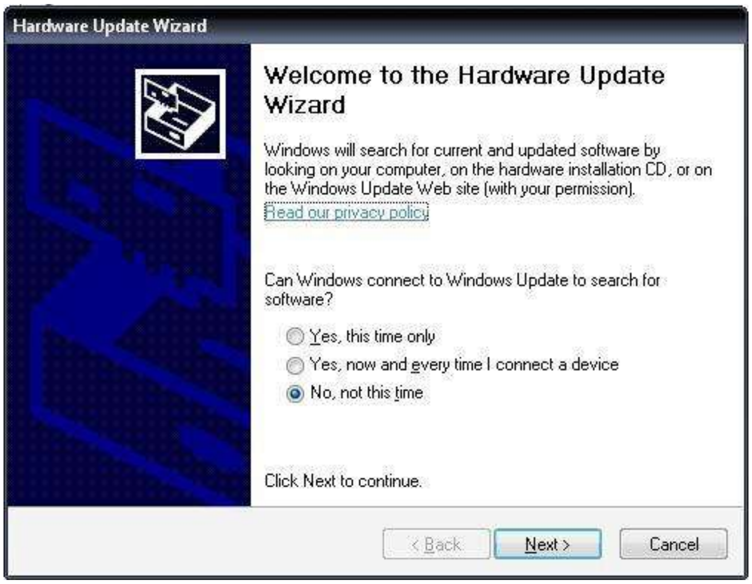
You will need to update driver and install **JungleUSB**

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


Universal Serial Bus controllers
SiS 7001 PCI to USB Open Host Controller
SiS 7001 PCI to USB Open Host Controller
USB Composite Device
USB Mass Storage Device
USB Root Hub
USB Root Hub
Xbox 360 I/O Device Drivers

.

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



Hardware Update Wizard

Welcome to the Hardware Update Wizard

Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission).

Read our privacy policy

Can Windows connect to Windows Update to search for software?

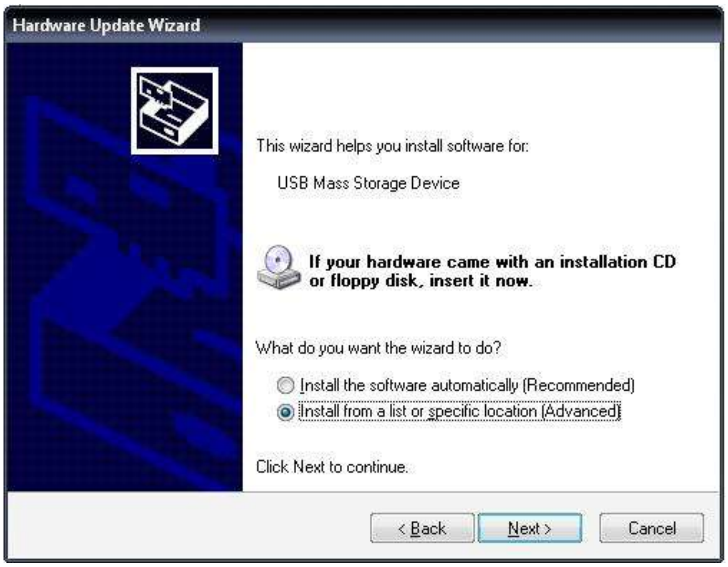
○ Yes, this time only

○ Yes, now and every time I connect a device

● No, not this time

Click Next to continue.

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



Hardware Update Wizard

This wizard helps you install software for:

USB Mass Storage Device

If your hardware came with an installation CD or floppy disk, insert it now.

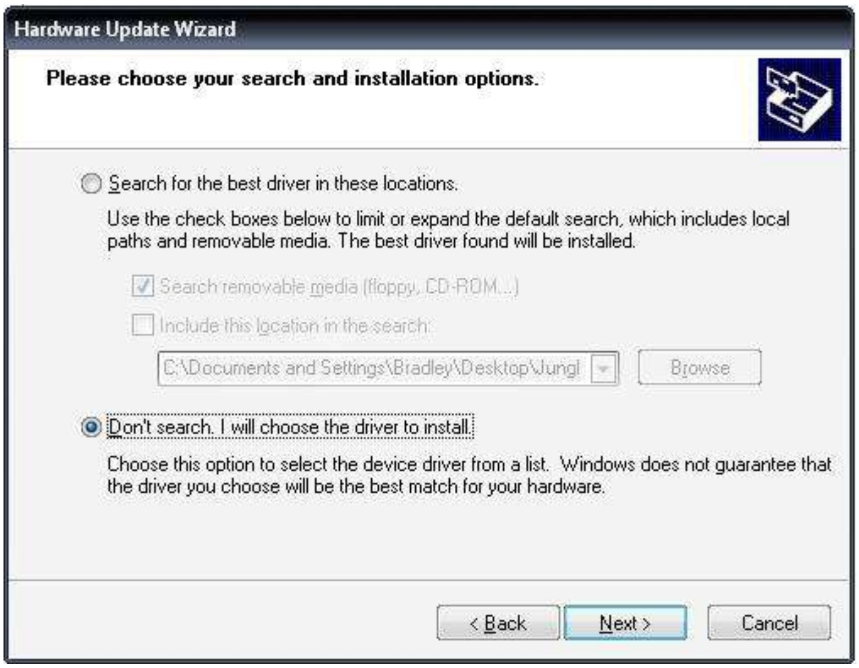
What do you want the wizard to do?

○ Install the software automatically (Recommended)

● Install from a list or specific location (Advanced)

Click Next to continue.

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



Hardware Update Wizard

Please choose your search and installation options.

○ Search for the best driver in these locations.

Use the check boxes below to limit or expand the default search, which includes local paths and removable media. The best driver found will be installed.

☑ Search removable media (floppy, CD-ROM...)

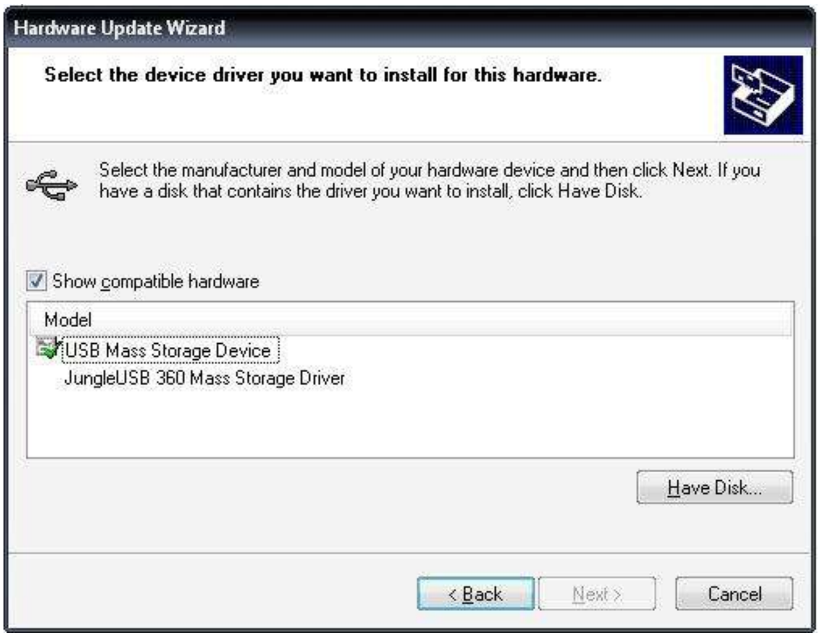
□ Include this location in the search:

C:\Documents and Settings\Bradley\Desktop\Jungl

● Don't search. I will choose the driver to install.

Choose this option to select the device driver from a list. Windows does not guarantee that the driver you choose will be the best match for your hardware.

Click **Have Disk**



Hardware Update Wizard

Select the device driver you want to install for this hardware.

Select the manufacturer and model of your hardware device and then click Next. If you have a disk that contains the driver you want to install, click Have Disk.

☑ Show compatible hardware

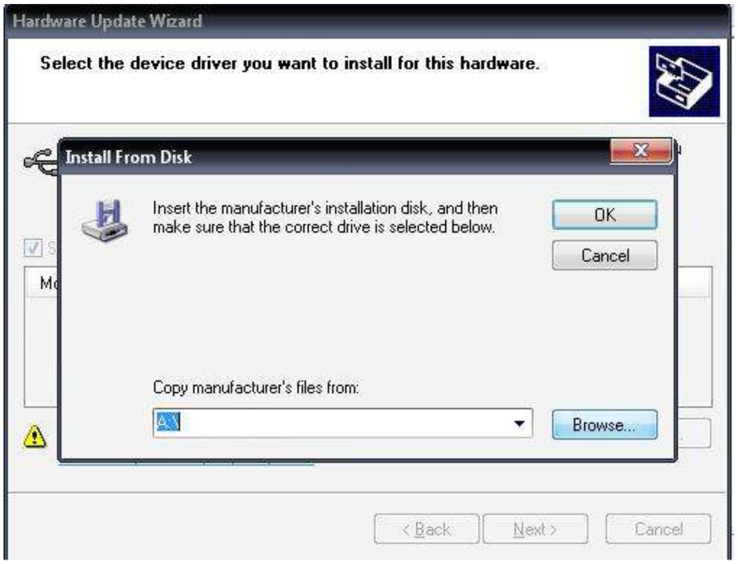
Model

USB Mass Storage Device

JungleUSB 360 Mass Storage Driver

Now click **Browse** and Navigate to **JungleUSB.inf** (can be downloaded from the usual places).

Select it and click Open. Then click OK


Hardware Update Wizard

Select the device driver you want to install for this hardware.

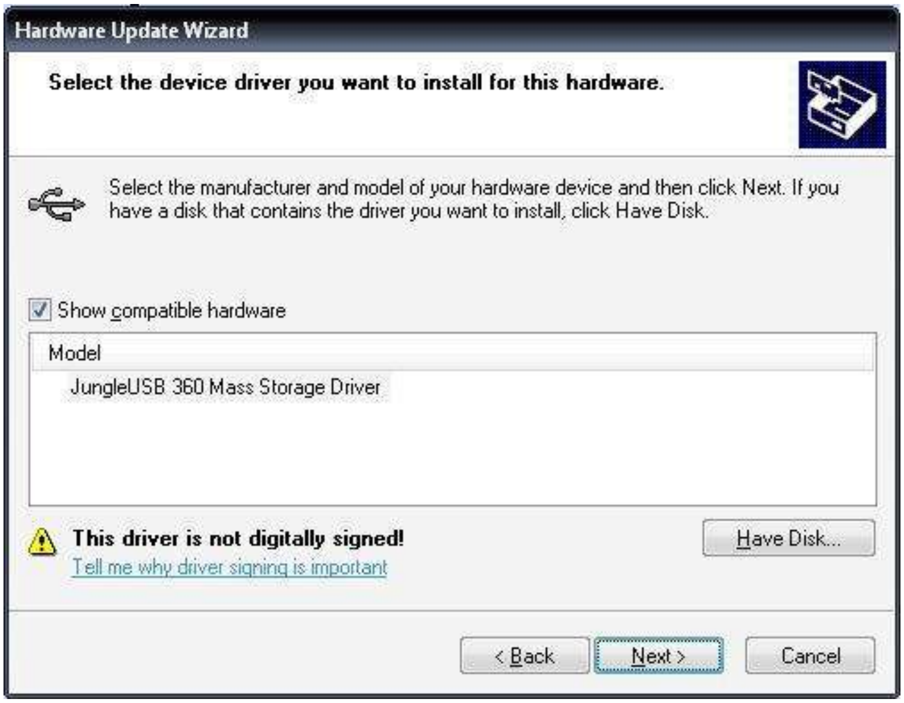
Install From Disk

Insert the manufacturer's installation disk, and then make sure that the correct drive is selected below.

Copy manufacturer's files from:

A:\

Now click next and the Driver should install.


Hardware Update Wizard

Select the device driver you want to install for this hardware.

Select the manufacturer and model of your hardware device and then click Next. If you have a disk that contains the driver you want to install, click Have Disk.

☑ Show compatible hardware

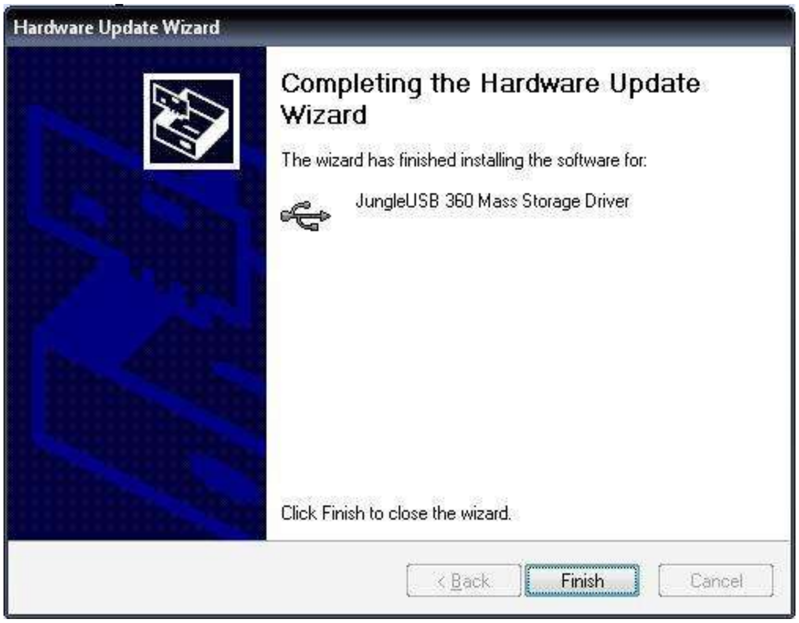
Model

JungleUSB 360 Mass Storage Driver

This driver is not digitally signed!

Tell me why driver signing is important

Click finish and Return to Device manager.



Hardware Update Wizard

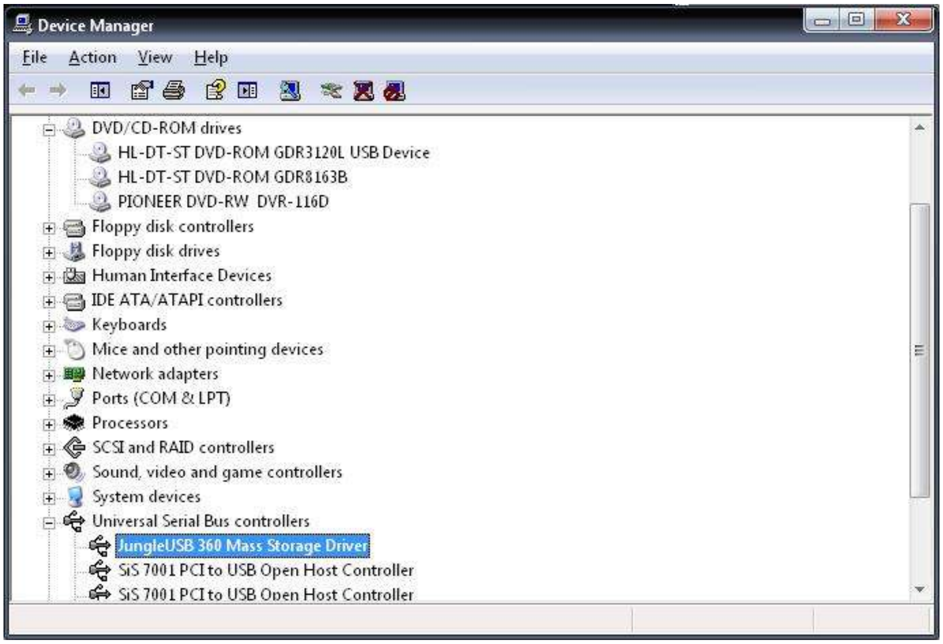
Completing the Hardware Update Wizard

The wizard has finished installing the software for:

JungleUSB 360 Mass Storage Driver

Click Finish to close the wizard.

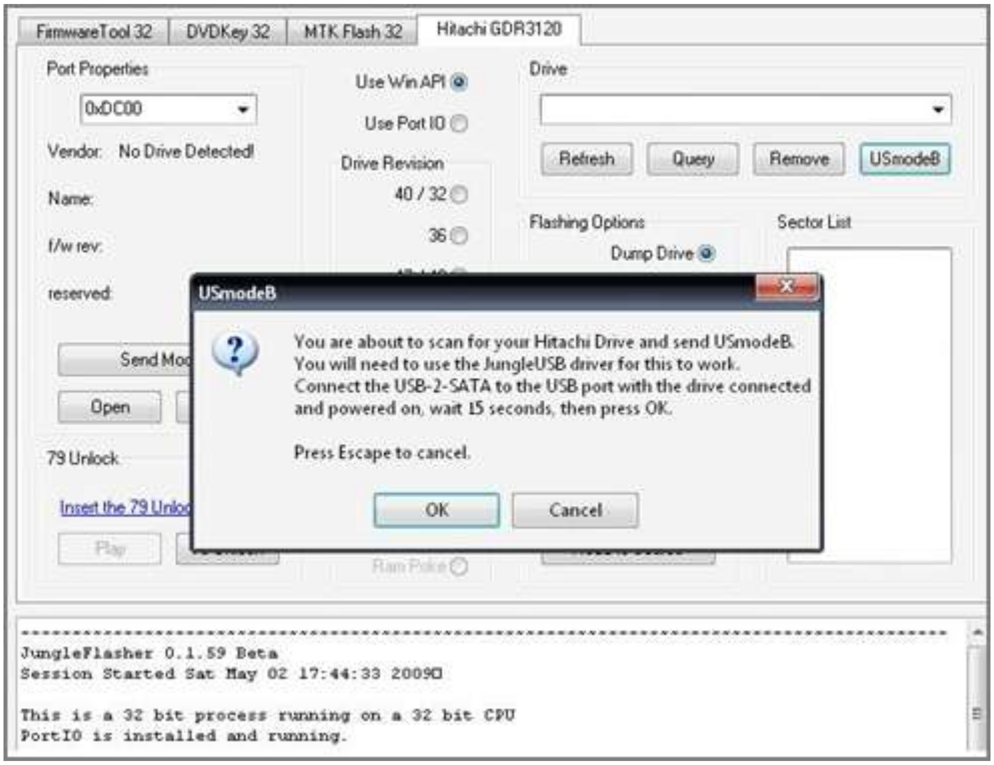
If all went well you should now have **JungleUSB 360 Mass Storage Driver** listed under **Universal Serial Bus Controllers** and **HL-DT-ST DVD-ROM GDR3120 USB Device** listed under **DVD/CD ROM drives.**



Device Manager

- DVD/CD-ROM drives
  - HL-DT-ST DVD-ROM GDR3120L USB Device
  - HL-DT-ST DVD-ROM GDR8163B
  - PIONEER DVD-RW DVR-116D
- Floppy disk controllers
- Floppy disk drives
- Human Interface Devices
- IDE ATA/ATAPI controllers
- Keyboards
- Mice and other pointing devices
- Network adapters
- Ports (COM & LPT)
- Processors
- SCSI and RAID controllers
- Sound, video and game controllers
- System devices
- Universal Serial Bus controllers
  - JungleUSB 360 Mass Storage Driver
  - SiS 7001 PCI to USB Open Host Controller
  - SiS 7001 PCI to USB Open Host Controller

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

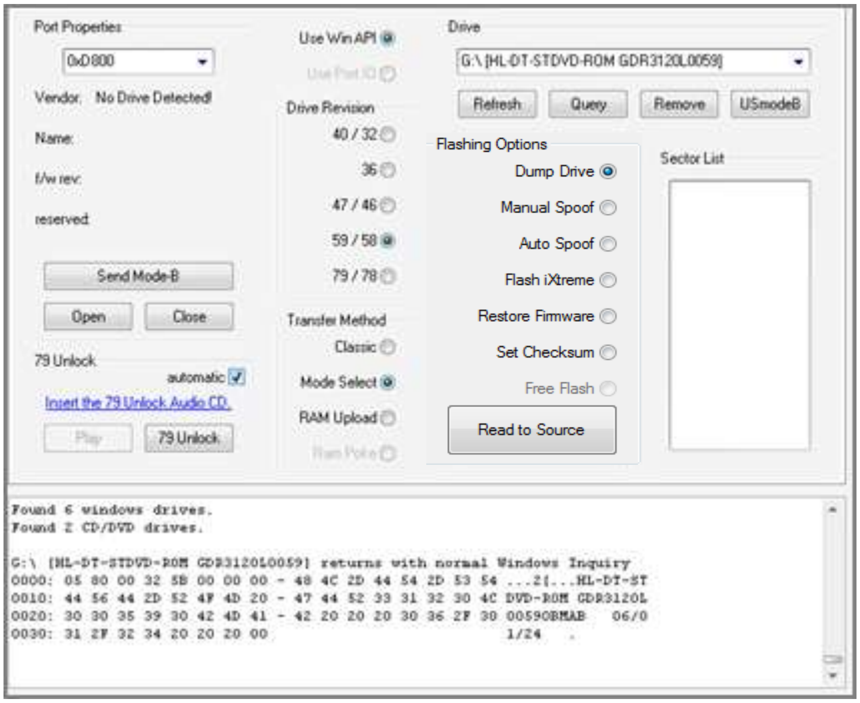


You are about to scan for your Hitachi Drive and send USmodeB.
You will need to use the JungleUSB driver for this to work.
Connect the USB-2-SATA to the USB port with the drive connected and powered on, wait 15 seconds, then press OK.

Press Escape to cancel.

```
================================================================================
JungleFlasher 0.1.59 Beta
Session Started Sat May 02 17:44:33 2009

This is a 32 bit process running on a 32 bit CPU
PortIO is installed and running.
```

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.



```
Found 6 windows drives.
Found 2 CD/DVD drives.

G:\ [HL-DT-STDVD-ROM GDR3120L0059] returns with normal Windows Inquiry
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 30 42 4D 41 - 42 20 20 20 30 36 2F 30 00590BMAB   06/0
0030: 31 2F 32 34 20 20 20 00                           1/24   .
```

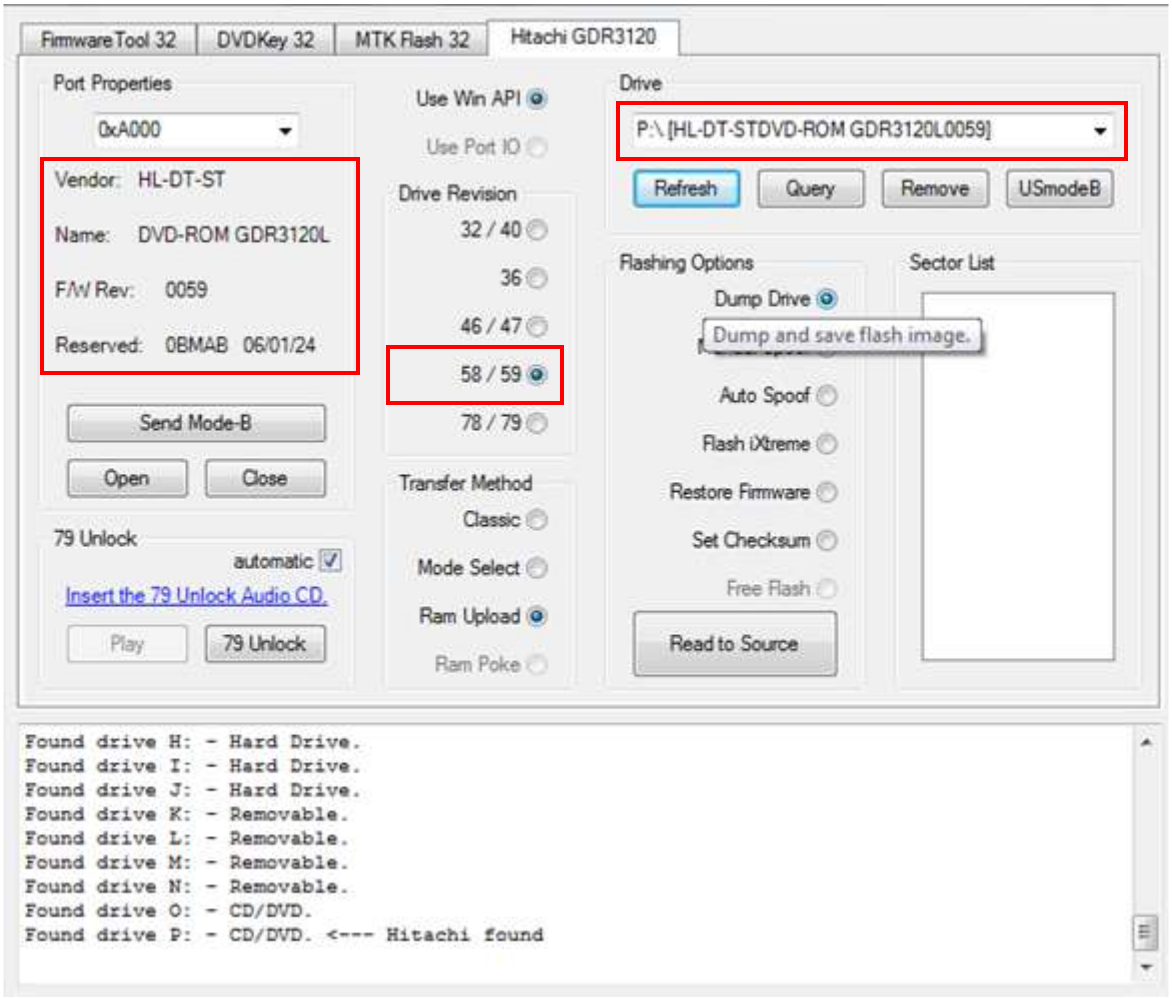
CLICK TO RETURN TO HITACHI FLOWCHART

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



Port Properties: 0xA000

Vendor: HL-DT-ST

Name: DVD-ROM GDR3120L

F/W Rev: 0059

Reserved: 0BMAB 06/01/24

automatic ☑

Use Win API ●

Use Port IO ○

Drive: P:\ [HL-DT-STDVD-ROM GDR3120L0059]

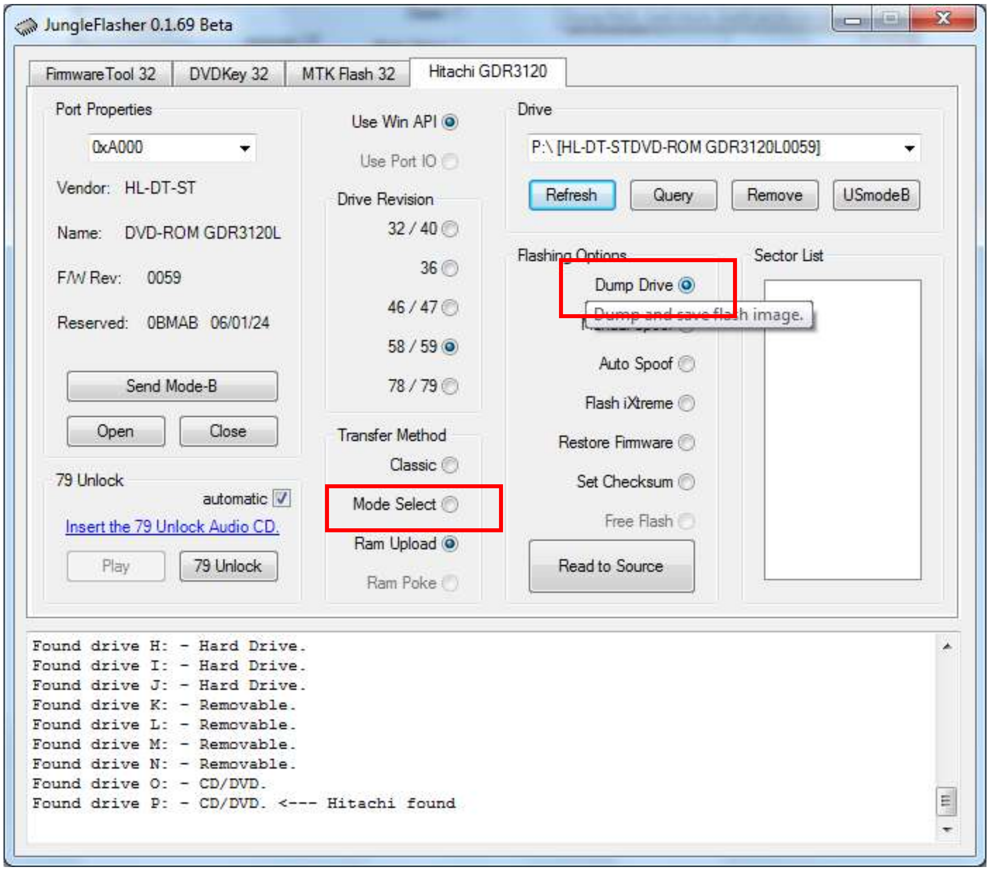
Drive Revision: 32 / 40 ○ 36 ○ 46 / 47 ○ 58 / 59 ● 78 / 79 ○

Transfer Method: Classic ○ Mode Select ○ Ram Upload ● Ram Poke ○

Flashing Options: Dump Drive ● Auto Spoof ○ Flash iXtreme ○ Restore Firmware ○ Set Checksum ○ Free Flash ○

```
Found drive H: - Hard Drive.
Found drive I: - Hard Drive.
Found drive J: - Hard Drive.
Found drive K: - Removable.
Found drive L: - Removable.
Found drive M: - Removable.
Found drive N: - Removable.
Found drive O: - CD/DVD.
Found drive P: - CD/DVD. <--- Hitachi found
```

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



Port Properties

0xA000

Vendor: HL-DT-ST

Name: DVD-ROM GDR3120L

F/W Rev: 0059

Reserved: 0BMAB 06/01/24

79 Unlock

automatic ☑

Use Win API ●

Use Port IO ○

Drive Revision

32 / 40 ○

36 ○

46 / 47 ○

58 / 59 ●

78 / 79 ○

Transfer Method

Classic ○

Mode Select ○

Ram Upload ●

Ram Poke ○

Drive

P:\ [HL-DT-STDVD-ROM GDR3120L0059]

Flashing Options

Dump Drive ●

Dump and save flash image.

Auto Spoof ○

Flash iXtreme ○

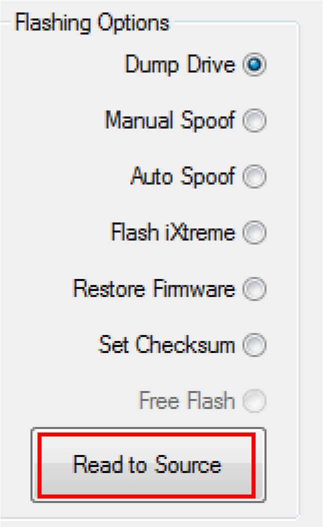
Restore Firmware ○

Set Checksum ○

Free Flash ○

```
Found drive H: - Hard Drive.
Found drive I: - Hard Drive.
Found drive J: - Hard Drive.
Found drive K: - Removable.
Found drive L: - Removable.
Found drive M: - Removable.
Found drive N: - Removable.
Found drive O: - CD/DVD.
Found drive P: - CD/DVD. <--- Hitachi found
```

Then, click **Read to Source**



Flashing Options

Dump Drive ●

Manual Spoof ○

Auto Spoof ○

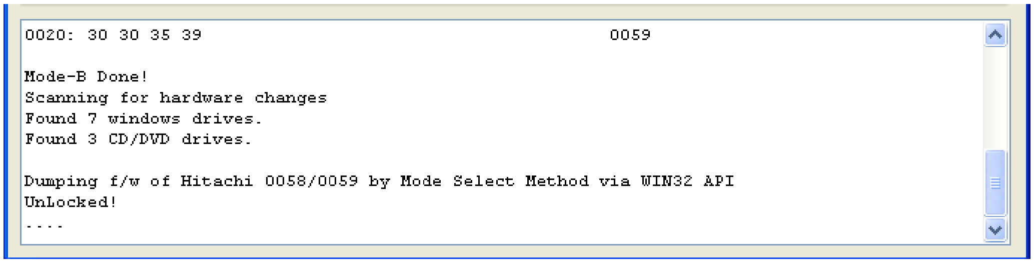
Flash iXtreme ○

Restore Firmware ○

Set Checksum ○

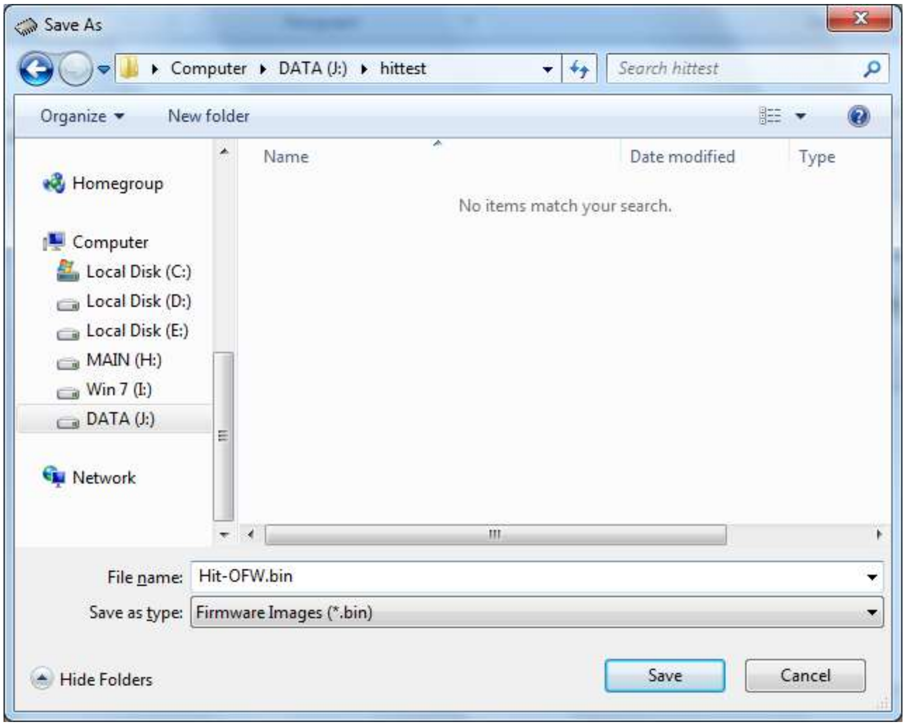
Free Flash ○

You should see something similar to below



```
0020: 30 30 35 39                                          0059

Mode-B Done!
Scanning for hardware changes
Found 7 windows drives.
Found 3 CD/DVD drives.

Dumping f/w of Hitachi 0058/0059 by Mode Select Method via WIN32 API
UnLocked!
....
```

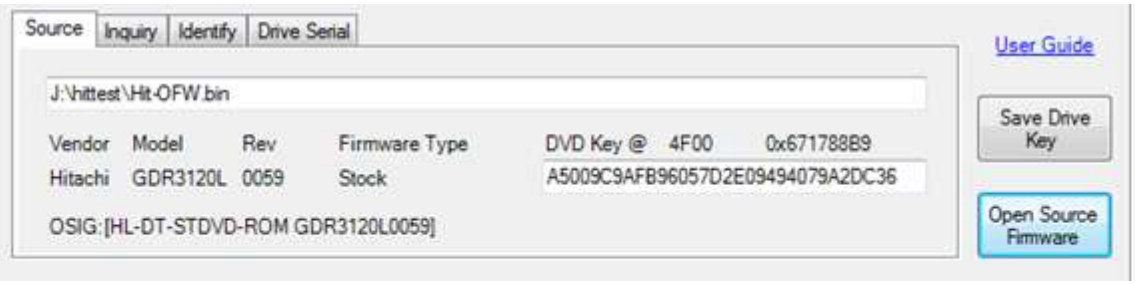
Once firmware is read, JungleFlasher will prompt you to save it.



File name: Hit-OFW.bin

Save as type: Firmware Images (*.bin)

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



J:\hittest\Hit-OFW.bin

Vendor	Model	Rev	Firmware Type	DVD Key @ 4F00	0x671788B9
Hitachi	GDR3120L	0059	Stock	A5009C9AFB96057D2E09494079A2DC36	

OSIG:[HL-DT-STDVD-ROM GDR3120L0059]

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

[**FLASH iX FIRMWARE - CLICK HERE**]

UNLOCKING v79

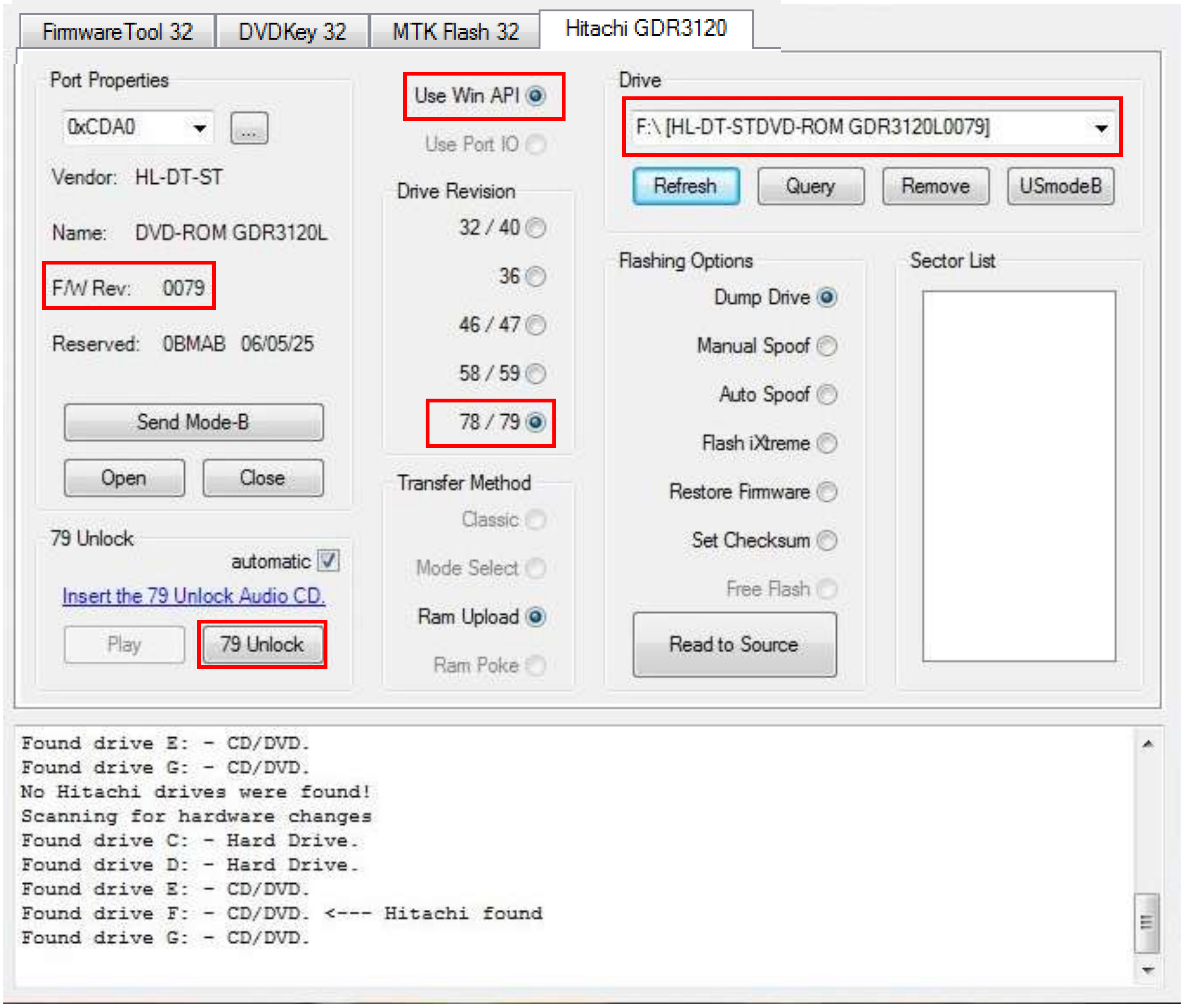
FIRST Ensure ModeB is set

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**



Vendor: HL-DT-ST

Name: DVD-ROM GDR3120L

F/W Rev: 0079

Reserved: 0BMAB 06/05/25

automatic ☑

● Use Win API ○ Use Port IO

● 78 / 79

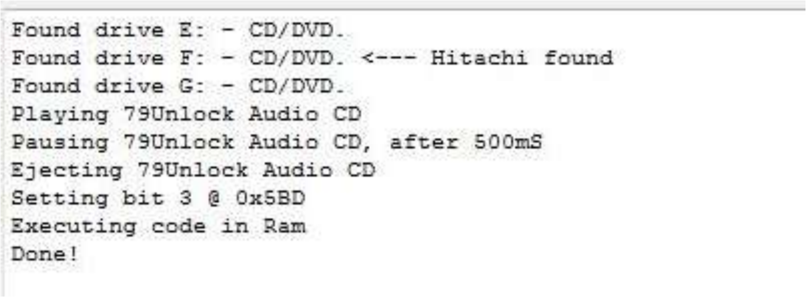
○ Classic ○ Mode Select ● Ram Upload ○ Ram Poke

F:\ [HL-DT-STDVD-ROM GDR3120L0079]

● Dump Drive ○ Manual Spoof ○ Auto Spoof ○ Flash iXtreme ○ Restore Firmware ○ Set Checksum ○ Free Flash

```
Found drive E: - CD/DVD.
Found drive G: - CD/DVD.
No Hitachi drives were found!
Scanning for hardware changes
Found drive C: - Hard Drive.
Found drive D: - Hard Drive.
Found drive E: - CD/DVD.
Found drive F: - CD/DVD. <--- Hitachi found
Found drive G: - CD/DVD.
```

JungleFlasher should display a log similar to the one below.



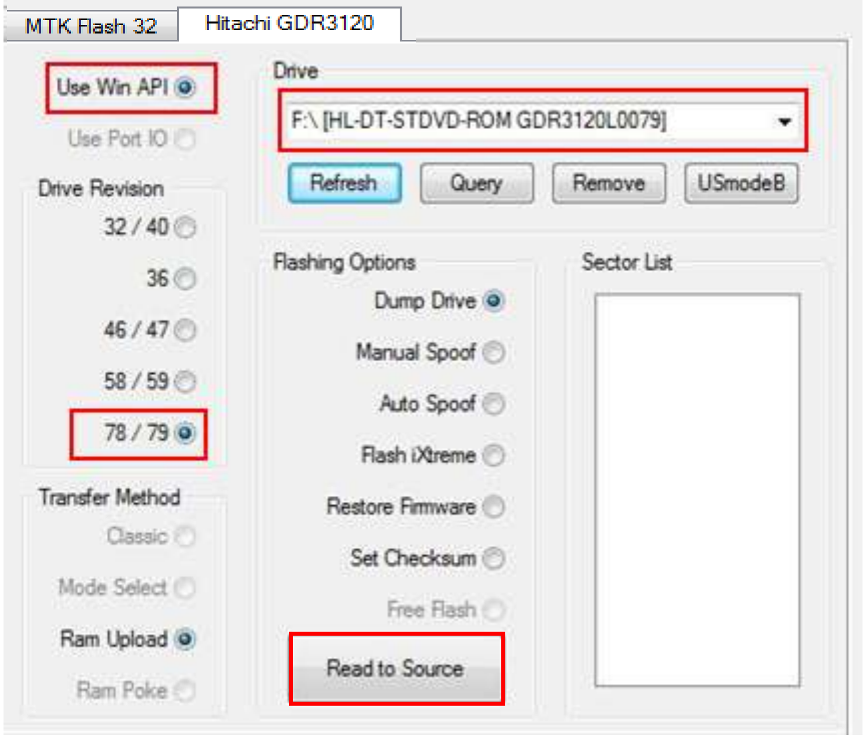
```
Found drive E: - CD/DVD.
Found drive F: - CD/DVD. <--- Hitachi found
Found drive G: - CD/DVD.
Playing 79Unlock Audio CD
Pausing 79Unlock Audio CD, after 500mS
Ejecting 79Unlock Audio CD
Setting bit 3 @ 0x5BD
Executing code in Ram
Done!
```

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



Use Win API ●
Use Port IO ○

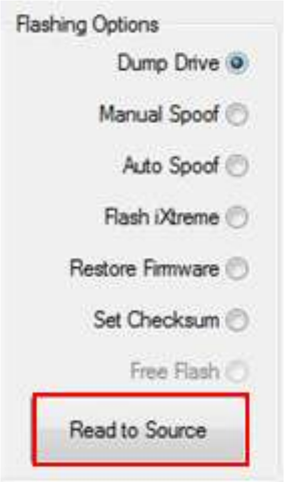
Drive: F:\ [HL-DT-STDVD-ROM GDR3120L0079]

Drive Revision
32 / 40 ○
36 ○
46 / 47 ○
58 / 59 ○
78 / 79 ●

Transfer Method
Classic ○
Mode Select ○
Ram Upload ●
Ram Poke ○

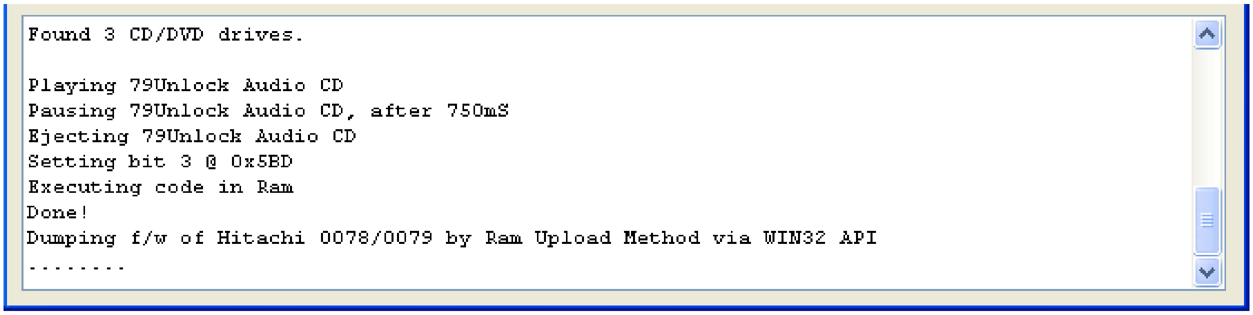
Flashing Options
Dump Drive ●
Manual Spoof ○
Auto Spoof ○
Flash iXtreme ○
Restore Firmware ○
Set Checksum ○
Free Flash ○

So, click **Read to Source**



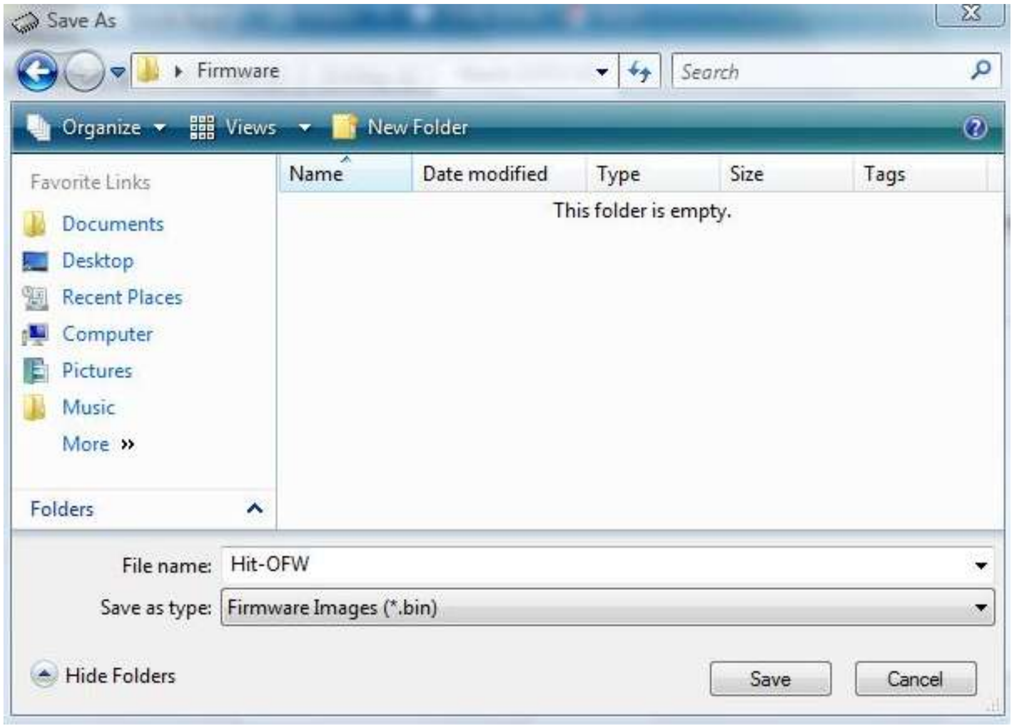
Flashing Options
Dump Drive ●
Manual Spoof ○
Auto Spoof ○
Flash iXtreme ○
Restore Firmware ○
Set Checksum ○
Free Flash ○

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



```
Found 3 CD/DVD drives.

Playing 79Unlock Audio CD
Pausing 79Unlock Audio CD, after 750mS
Ejecting 79Unlock Audio CD
Setting bit 3 @ 0x5BD
Executing code in Ram
Done!
Dumping f/w of Hitachi 0078/0079 by Ram Upload Method via WIN32 API
........
```

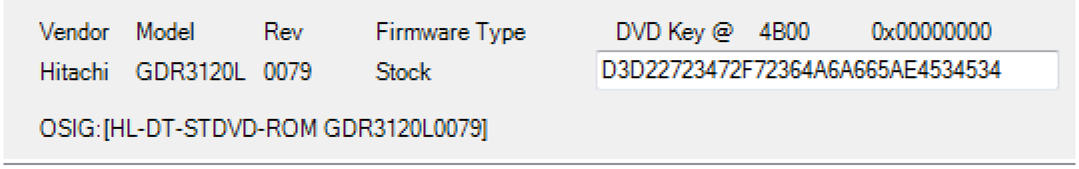
Once it has read the Firmware it will prompt you to save the Firmware.



File name: Hit-OFW

Save as type: Firmware Images (*.bin)

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



Vendor	Model	Rev	Firmware Type	DVD Key @ 4B00	0x00000000
Hitachi	GDR3120L	0079	Stock	D3D22723472F72364A6A665AE4534534	

OSIG:[HL-DT-STDVD-ROM GDR3120L0079]

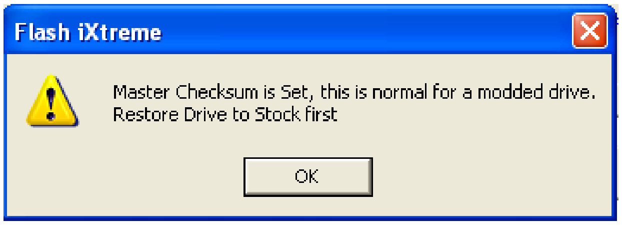
FLASH iX – CLICK HERE TO PROCEED!

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:



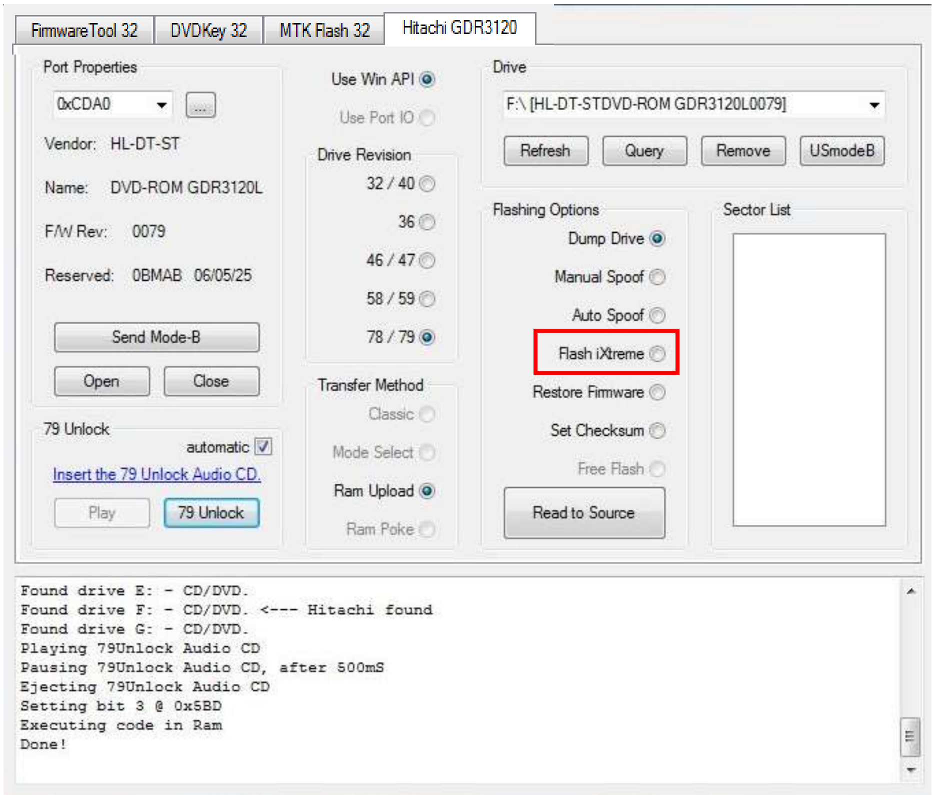
Flash iXtreme

Master Checksum is Set, this is normal for a modded drive.
Restore Drive to Stock first

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



Port Properties: 0xCDA0

Vendor: HL-DT-ST

Name: DVD-ROM GDR3120L

F/W Rev: 0079

Reserved: 0BMAB 06/05/25

automatic ☑

● Use Win API
○ Use Port IO

Drive Revision: ○ 32 / 40 ○ 36 ○ 46 / 47 ○ 58 / 59 ● 78 / 79

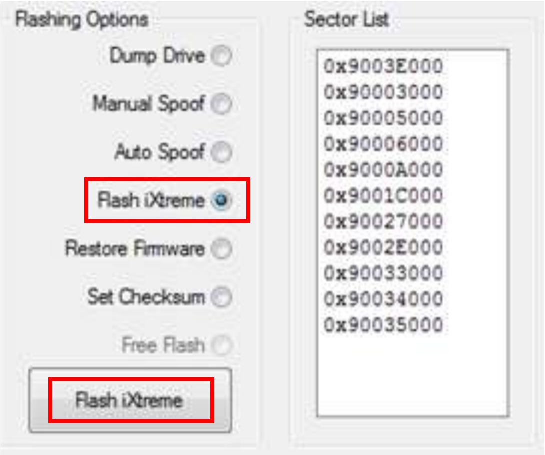
Transfer Method: ○ Classic ○ Mode Select ● Ram Upload ○ Ram Poke

Drive: F:\ [HL-DT-STDVD-ROM GDR3120L0079]

Flashing Options: ● Dump Drive ○ Manual Spoof ○ Auto Spoof ○ Flash iXtreme ○ Restore Firmware ○ Set Checksum ○ Free Flash

```
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!
```

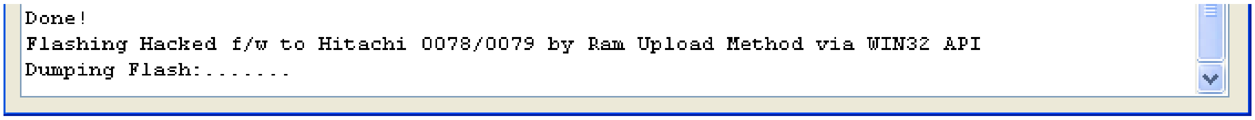
Then, click **Flash Hacked f/w**



Flash iXtreme ●

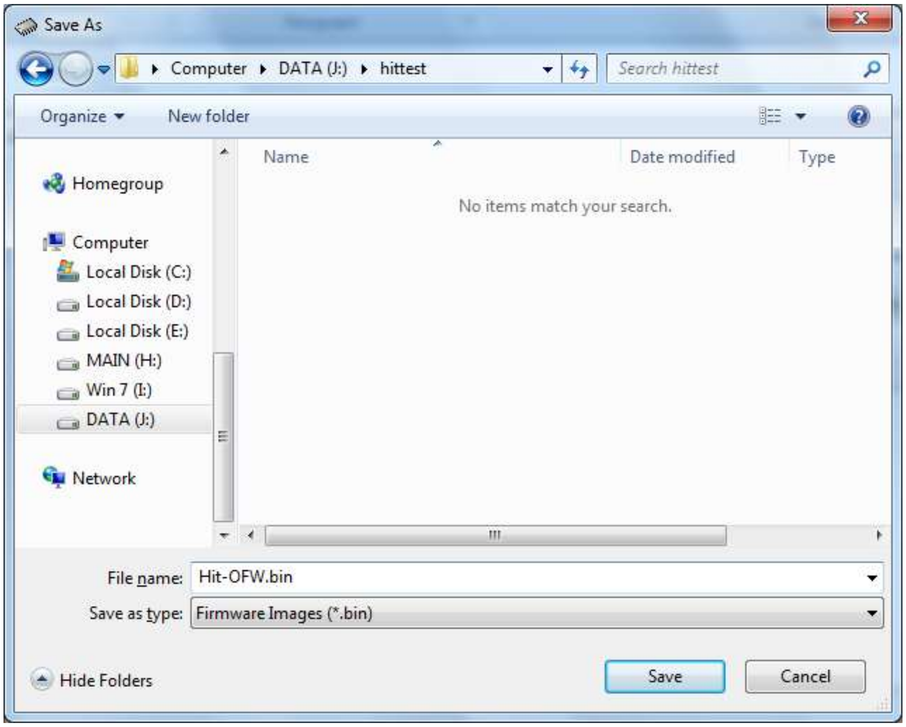
```
0x9003E000
0x90003000
0x90005000
0x90006000
0x9000A000
0x9001C000
0x90027000
0x9002E000
0x90033000
0x90034000
0x90035000
```

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



```
Done!
Flashing Hacked f/w to Hitachi 0078/0079 by Ram Upload Method via WIN32 API
Dumping Flash:.......
```

It will prompt you to save it. It's **heavily advised you do** just in case.



No items match your search.

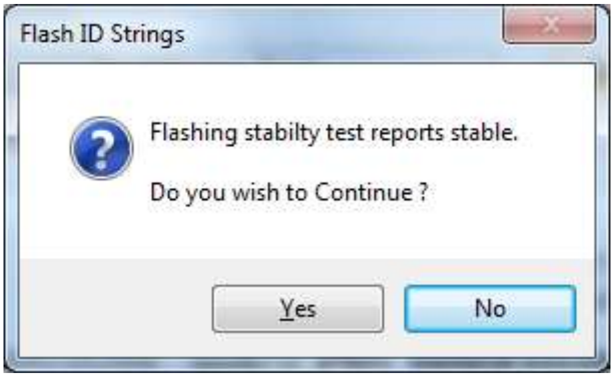
File name: Hit-OFW.bin

Save as type: Firmware Images (*.bin)

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

If you view the log, you see that JungleFlasher has automatically loaded iXtreme 1.51, 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.



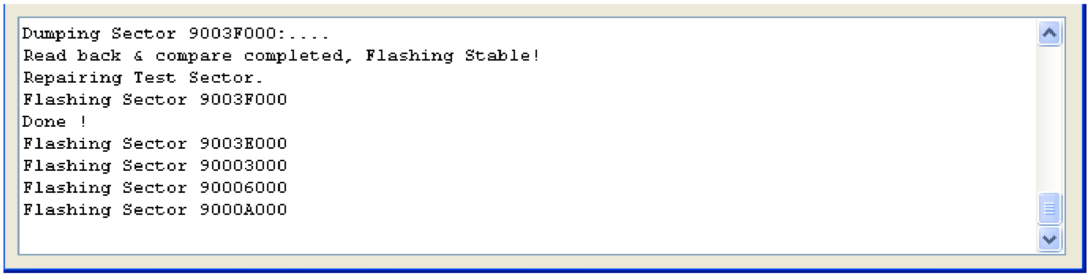
Flash ID Strings

Flashing stabilty test reports stable.

Do you wish to Continue ?

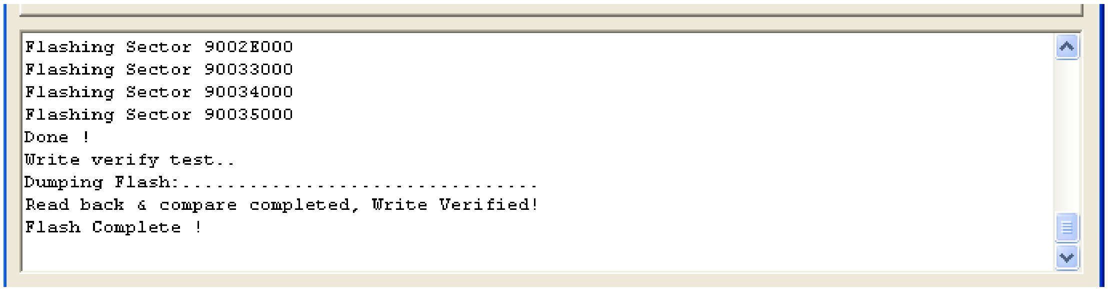
If you wish to proceed, click Y**es**

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



```
Dumping Sector 9003F000:....
Read back & compare completed, Flashing Stable!
Repairing Test Sector.
Flashing Sector 9003F000
Done !
Flashing Sector 9003E000
Flashing Sector 90003000
Flashing Sector 90006000
Flashing Sector 9000A000
```

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



```
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!

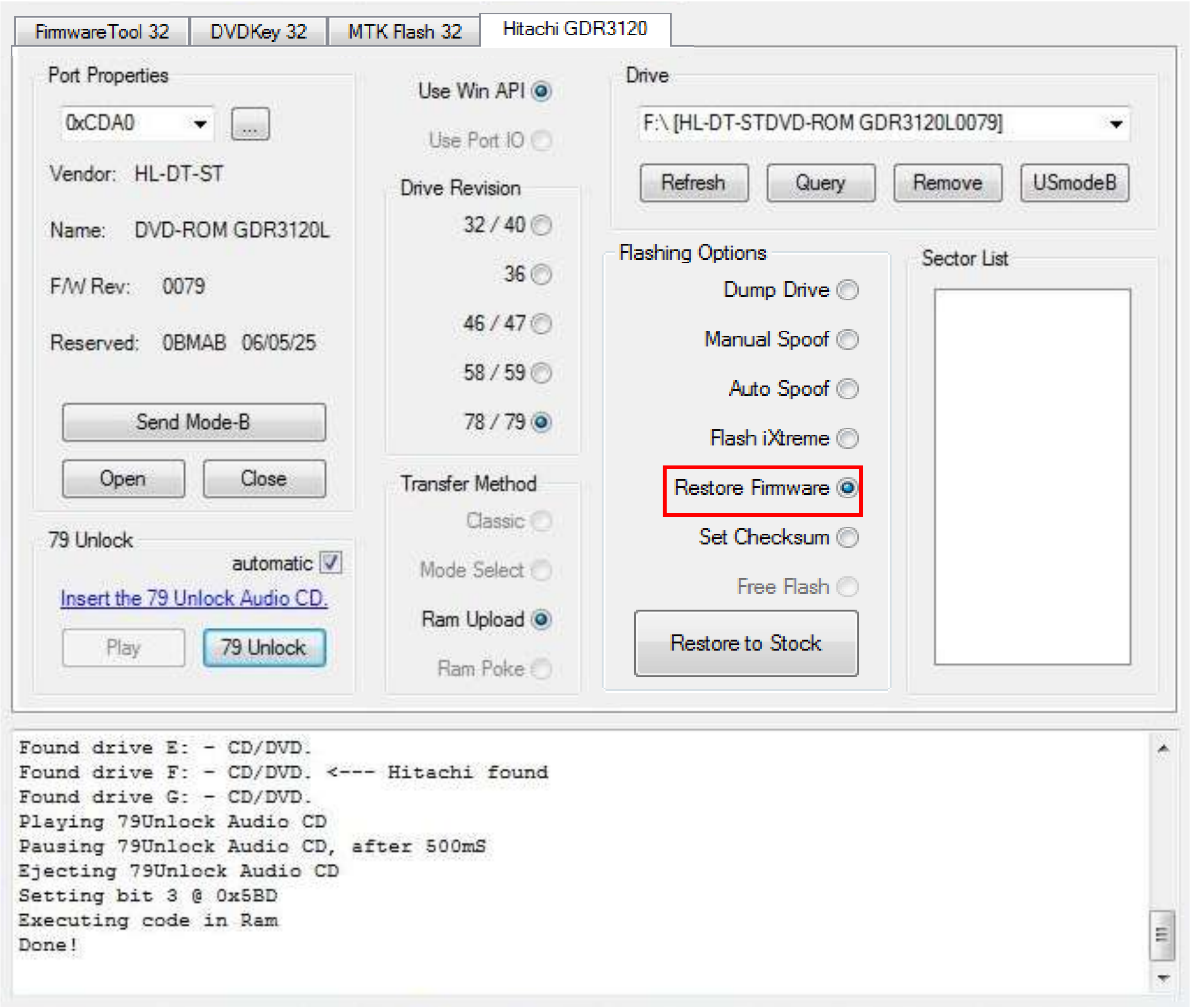
YOU ARE FINISHED – RETURN TO START OF TUTORIAL

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



Port: 0xCDA0

Vendor: HL-DT-ST

Name: DVD-ROM GDR3120L

F/W Rev: 0079

Reserved: 0BMAB 06/05/25

automatic ☑

● Use Win API
○ Use Port IO

Drive Revision: ○ 32 / 40 ○ 36 ○ 46 / 47 ○ 58 / 59 ● 78 / 79

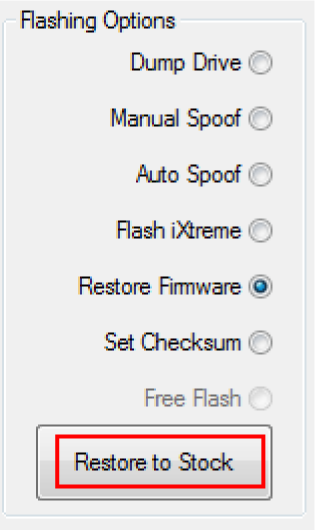
Transfer Method: ○ Classic ○ Mode Select ● Ram Upload ○ Ram Poke

Drive: F:\ [HL-DT-STDVD-ROM GDR3120L0079]

Flashing Options: ○ Dump Drive ○ Manual Spoof ○ Auto Spoof ○ Flash iXtreme ● Restore Firmware ○ Set Checksum ○ Free Flash

```
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!
```

Then, click **Restore to Stock**



Flashing Options

Dump Drive ○

Manual Spoof ○

Auto Spoof ○

Flash iXtreme ○

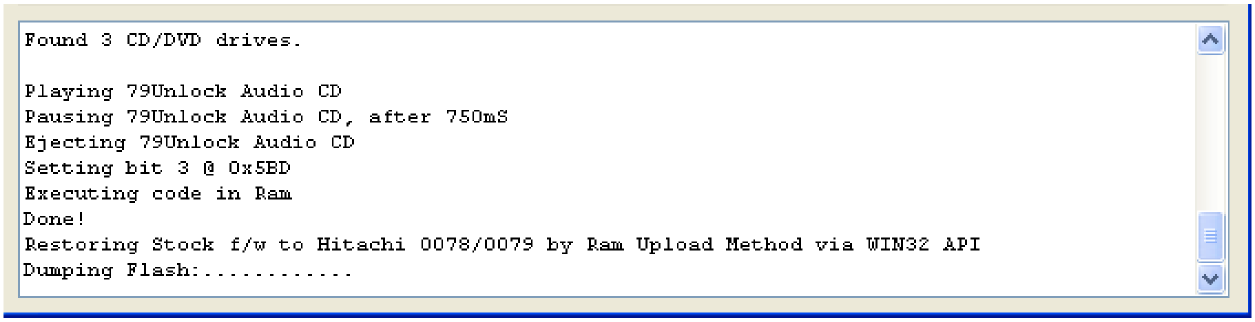
Restore Firmware ●

Set Checksum ○

Free Flash ○

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

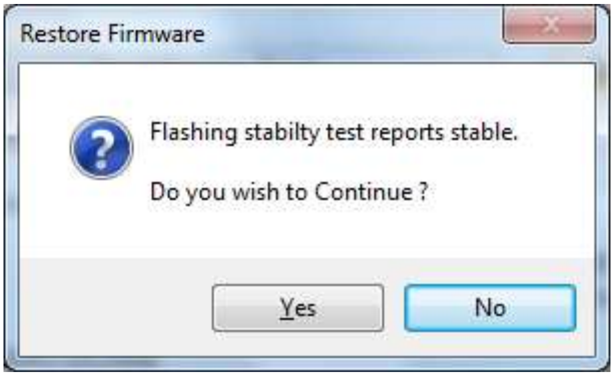
JungleFlasher will take control throughout this.



```
Found 3 CD/DVD drives.

Playing 79Unlock Audio CD
Pausing 79Unlock Audio CD, after 750mS
Ejecting 79Unlock Audio CD
Setting bit 3 @ 0x5BD
Executing code in Ram
Done!
Restoring Stock f/w to Hitachi 0078/0079 by Ram Upload Method via WIN32 API
Dumping Flash:............
```

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


Restore Firmware

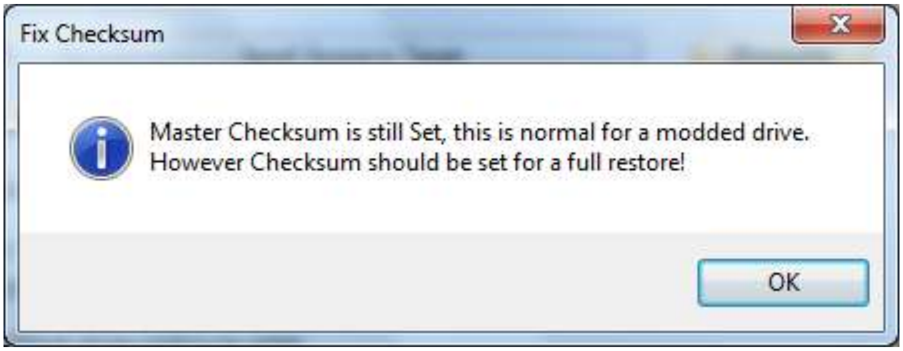
Flashing stabilty test reports stable.

Do you wish to Continue ?

Click **Yes** to proceed

Again, JungleFlasher will take control and flash the sectors required

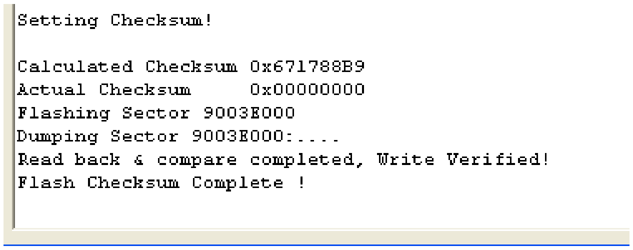
It will then check the checksum and prompt you to fix the Checksum.


Fix Checksum

Master Checksum is still Set, this is normal for a modded drive.
However Checksum should be set for a full restore!

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

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

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

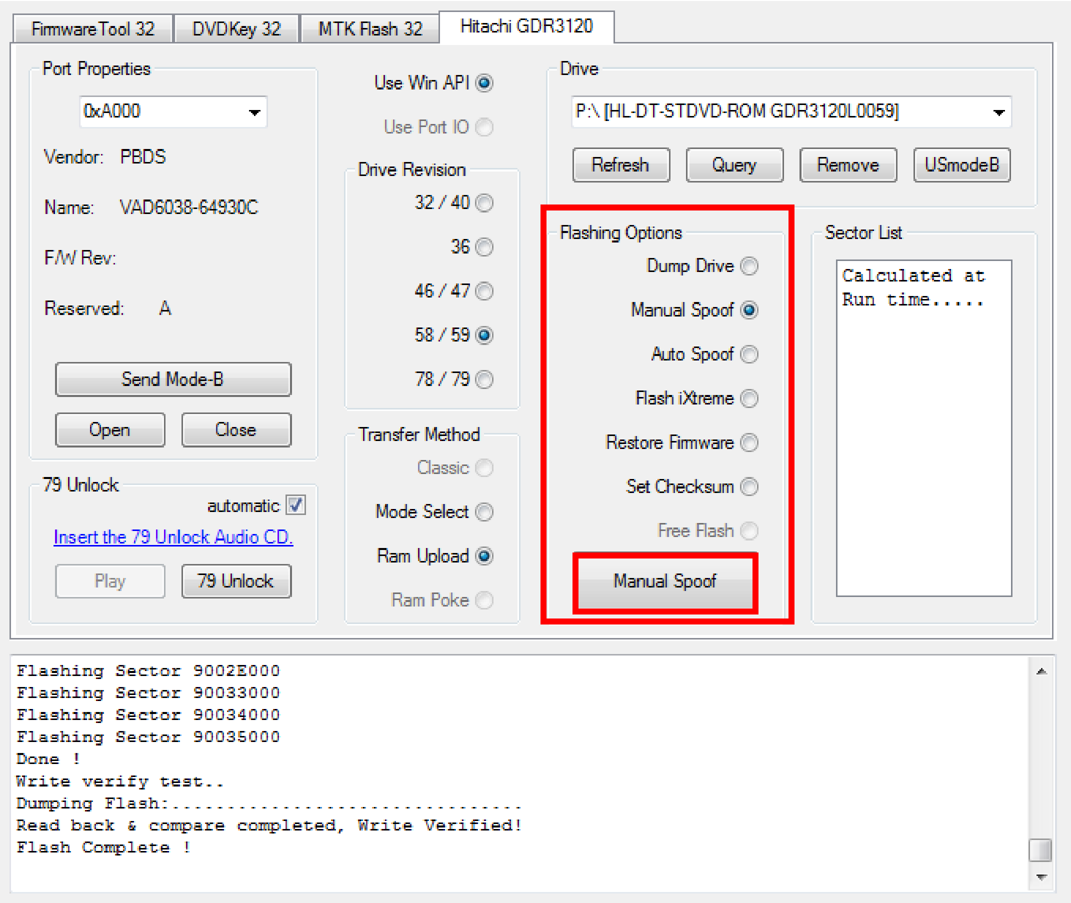
As usual you will need to first get the Drive into **Mode-B** (v79 unlocked) and assigned a drive letter (VIA / No Drivers, utilise PortI0)

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



0xA000

Vendor: PBDS

Name: VAD6038-64930C

F/W Rev:

Reserved: A

automatic ☑

● Use Win API

○ Use Port IO

○ 32 / 40

○ 36

○ 46 / 47

● 58 / 59

○ 78 / 79

○ Classic

○ Mode Select

● Ram Upload

○ Ram Poke

P:\ [HL-DT-STDVD-ROM GDR3120L0059]

○ Dump Drive

● Manual Spoof

○ Auto Spoof

○ Flash iXtreme

○ Restore Firmware

○ Set Checksum

○ Free Flash

```
Calculated at
Run time.....
```

```
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 !
```

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.)**

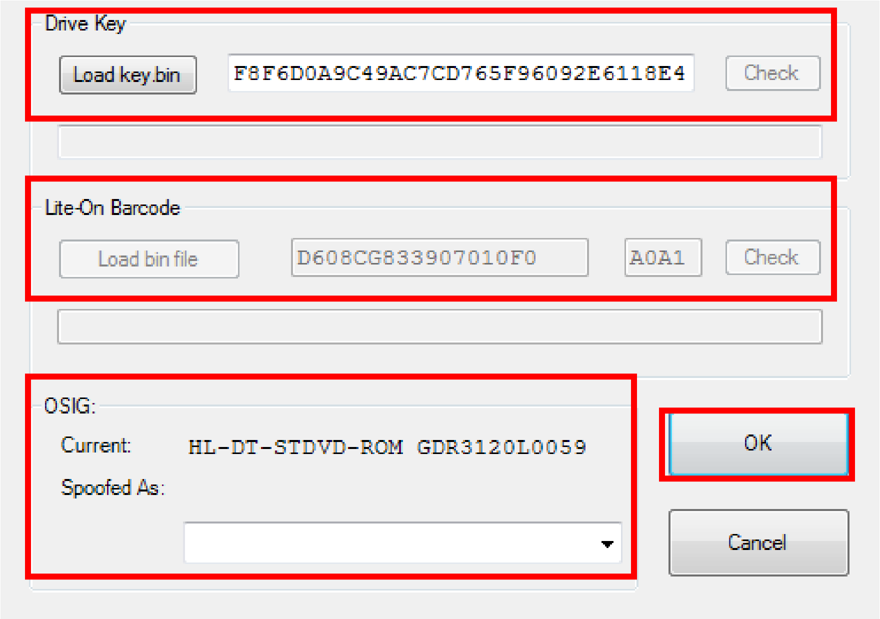
You can Change the **OSIG (ID String)** by selecting the desired drive from the drop down list,

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



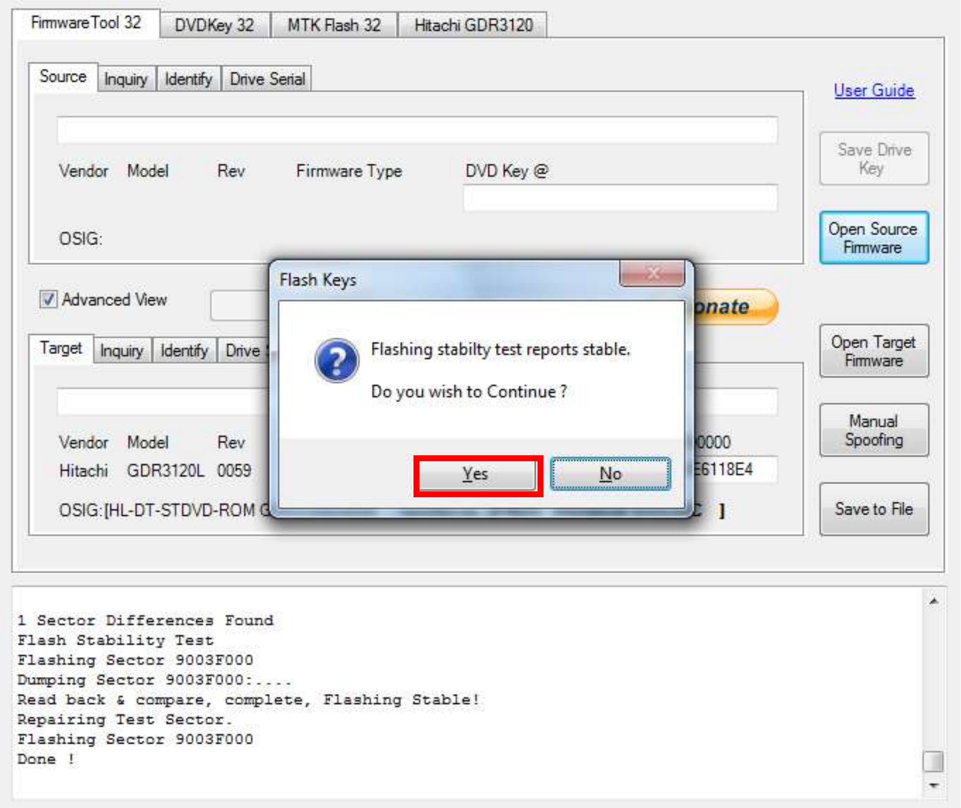
F8F6D0A9C49AC7CD765F96092E6118E4

D608CG833907010F0 A0A1

Current: HL-DT-STDVD-ROM GDR3120L0059

Spoofed As:

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!



Flash Keys

Flashing stabilty test reports stable.

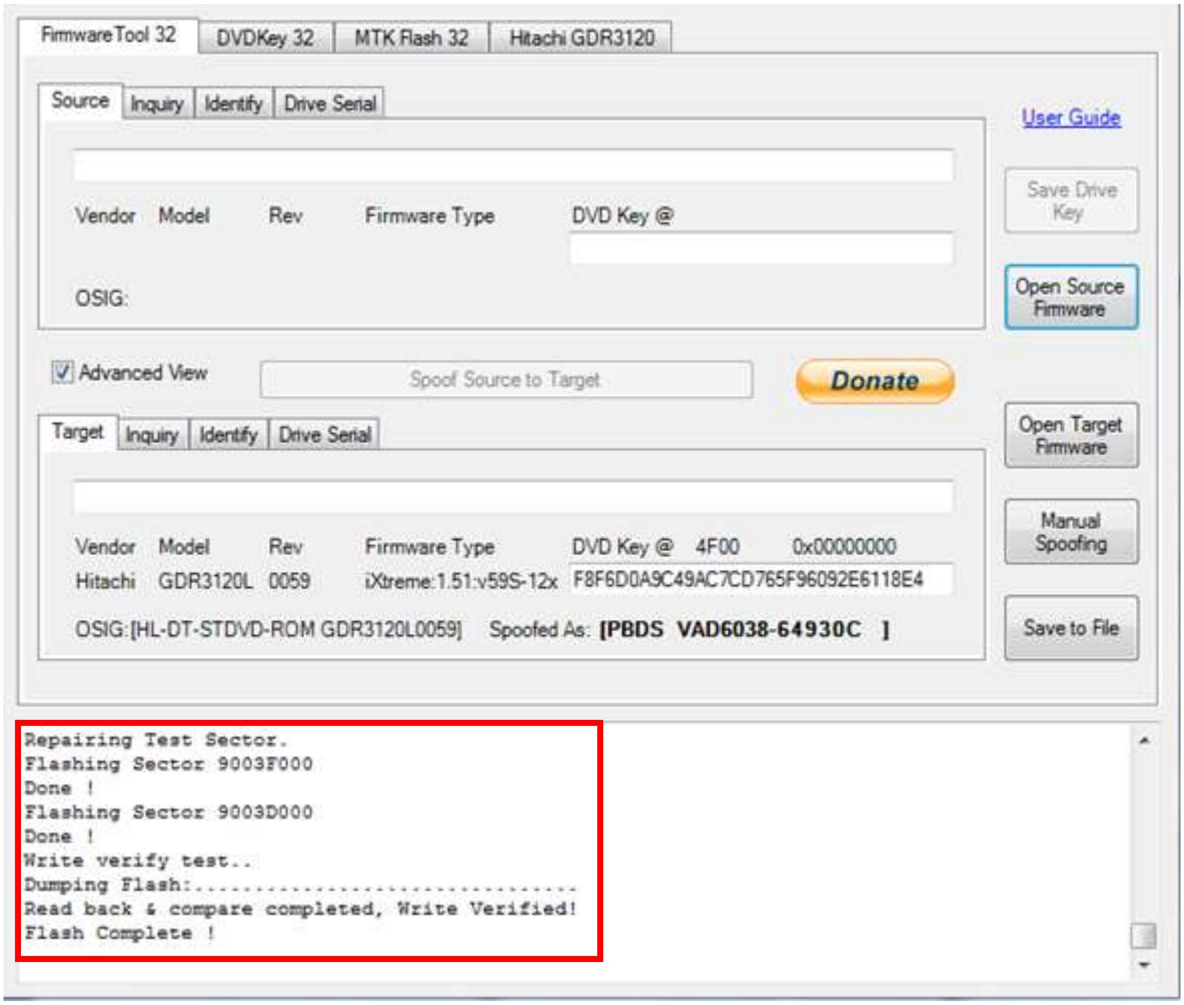
Do you wish to Continue ?

Vendor Model Rev
Hitachi GDR3120L 0059

OSIG:[HL-DT-STDVD-ROM G

```
1 Sector Differences Found
Flash Stability Test
Flashing Sector 9003F000
Dumping Sector 9003F000:....
Read back & compare, complete, Flashing Stable!
Repairing Test Sector.
Flashing Sector 9003F000
Done !
```

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



Source: Vendor Model Rev Firmware Type DVD Key @

OSIG:

Target:

Vendor	Model	Rev	Firmware Type	DVD Key @	4F00	0x00000000
Hitachi	GDR3120L	0059	iXtreme:1.51:v59S-12x	F8F6D0A9C49AC7CD765F96092E6118E4		

OSIG: [HL-DT-STDVD-ROM GDR3120L0059] Spoofed As: **[PBDS VAD6038-64930C]**

```
Repairing Test Sector.
Flashing Sector 9003F000
Done !
Flashing Sector 9003D000
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!

Job Done ☺

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

Auto Spoofing a Hitachi

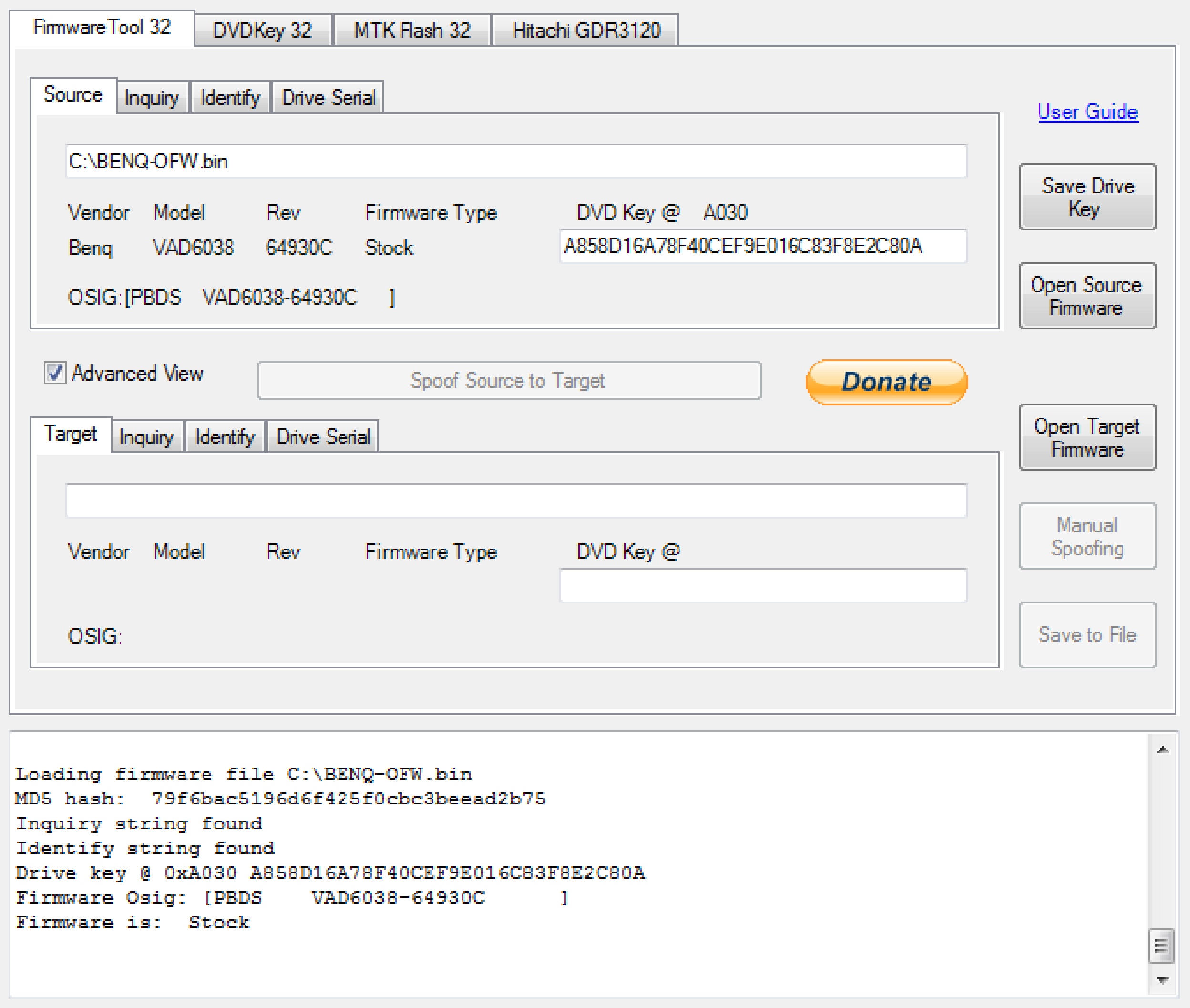
As with all Hitachi Tasks, you must set **Mode-B (and unlocked if v79)** first, have a drive letter assigned if using **Win API**, or, PortIO for VIA / No Drivers.

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!



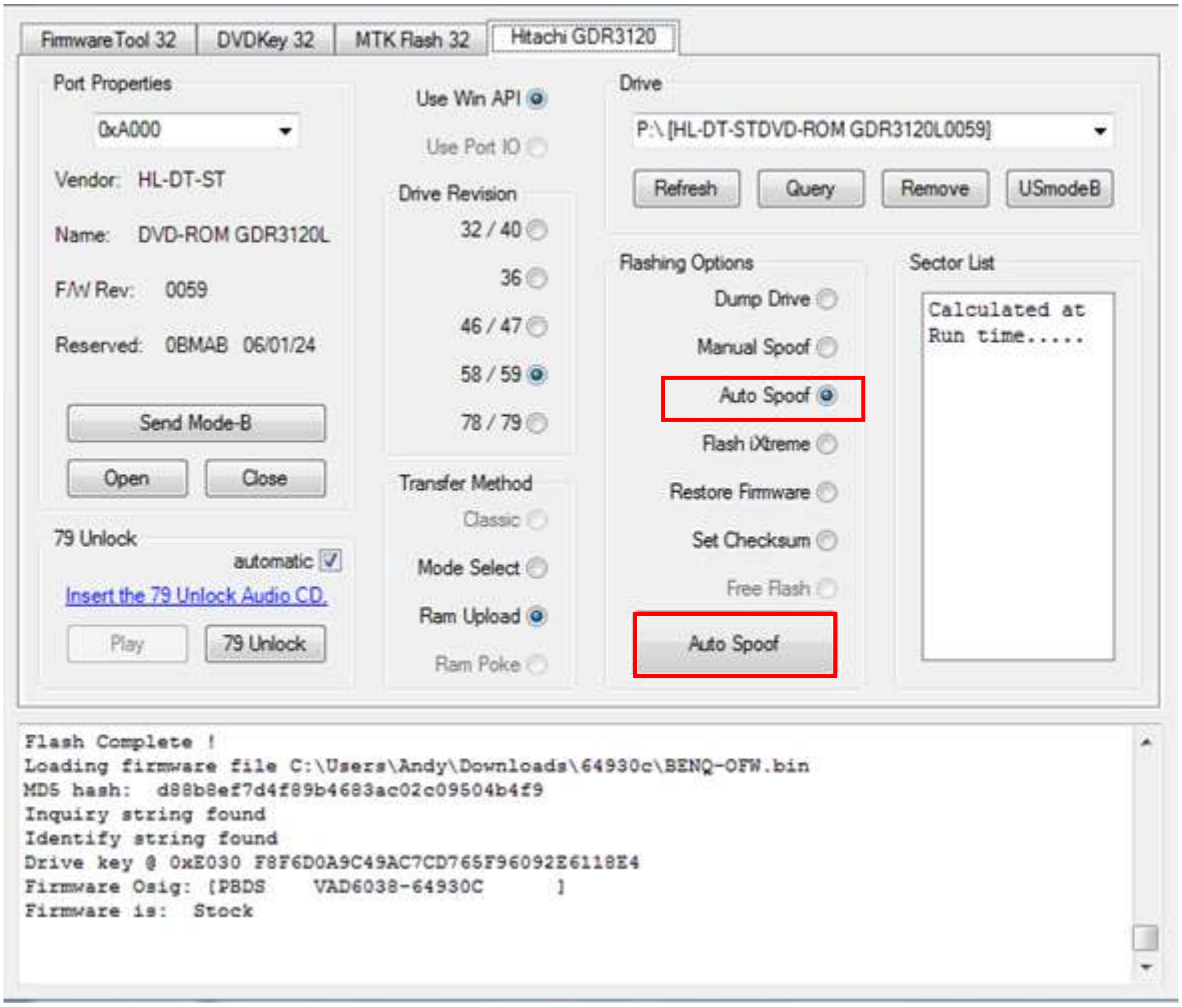
C:\BENQ-OFW.bin

Vendor	Model	Rev	Firmware Type	DVD Key @ A030
Benq	VAD6038	64930C	Stock	A858D16A78F40CEF9E016C83F8E2C80A

OSIG: [PBDS VAD6038-64930C]

```
Loading firmware file C:\BENQ-OFW.bin
MD5 hash:  79f6bac5196d6f425f0cbc3beead2b75
Inquiry string found
Identify string found
Drive key @ 0xA030 A858D16A78F40CEF9E016C83F8E2C80A
Firmware Osig: [PBDS     VAD6038-64930C      ]
Firmware is:  Stock
```

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



Port: 0xA000

Vendor: HL-DT-ST

Name: DVD-ROM GDR3120L

F/W Rev: 0059

Reserved: 0BMAB 06/01/24

automatic ☑

● Use Win API
○ Use Port IO

Drive Revision
○ 32 / 40
○ 36
○ 46 / 47
● 58 / 59
○ 78 / 79

Transfer Method
○ Classic
○ Mode Select
● Ram Upload
○ Ram Poke

Drive: P:\ [HL-DT-STDVD-ROM GDR3120L0059]

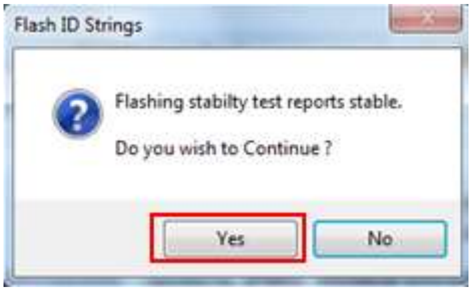
Flashing Options
○ Dump Drive
○ Manual Spoof
● Auto Spoof
○ Flash iXtreme
○ Restore Firmware
○ Set Checksum
○ Free Flash

Sector List:

```
Calculated at
Run time.....
```

```
Flash Complete !
Loading firmware file C:\Users\Andy\Downloads\64930c\BENQ-OFW.bin
MD5 hash:  d88b8ef7d4f89b4683ac02c09504b4f9
Inquiry string found
Identify string found
Drive key @ 0xE030 F8F6D0A9C49AC7CD765F96092E6118E4
Firmware Osig: [PBDS    VAD6038-64930C      ]
Firmware is:  Stock
```

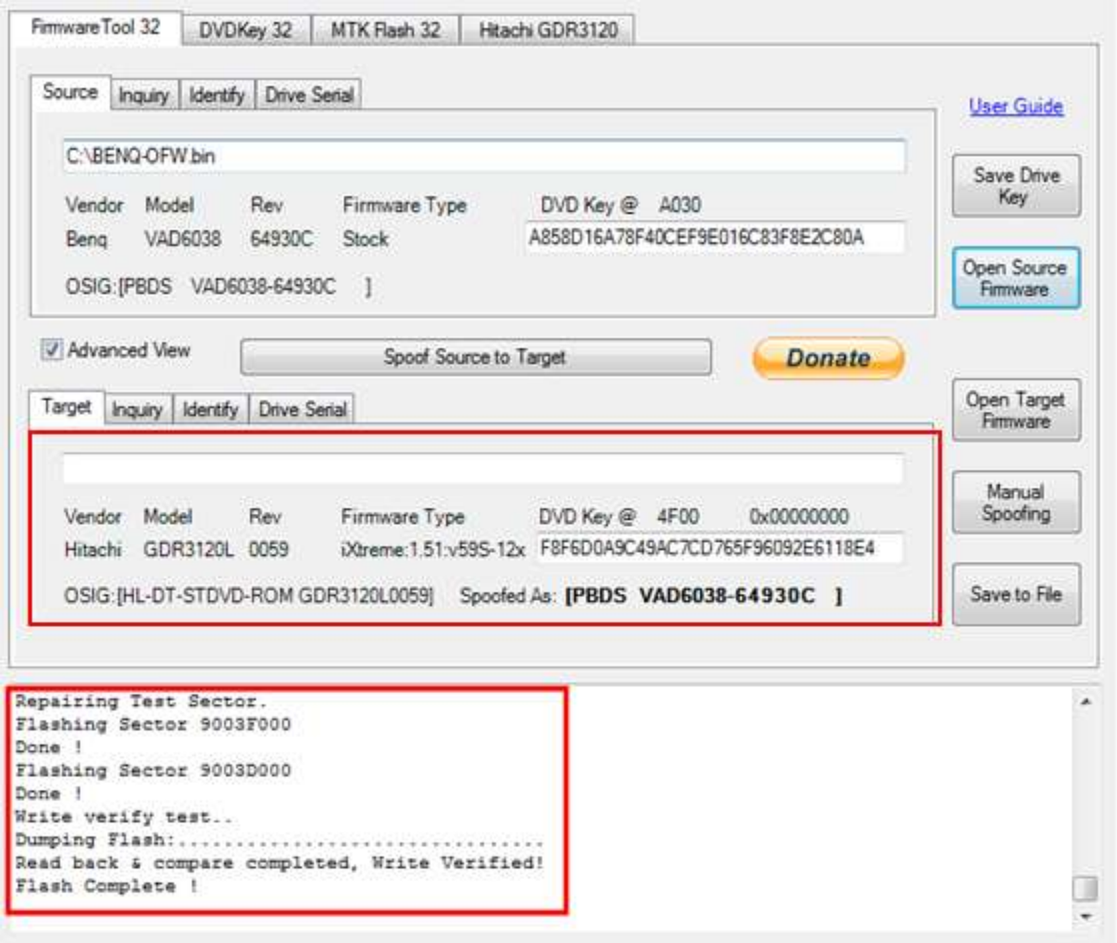
Jungleflasher will then test flash a sector for stability check and ask for confirmation to proceed! Select **YES!**



Flashing stabilty test reports stable.

Do you wish to Continue ?

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)



C:\BENQ-OFW.bin

Vendor Model Rev Firmware Type DVD Key @ A030
Benq VAD6038 64930C Stock A858D16A78F40CEF9E016C83F8E2C80A

OSIG:[PBDS VAD6038-64930C]

Vendor Model Rev Firmware Type DVD Key @ 4F00 0x00000000
Hitachi GDR3120L 0059 iXtreme:1.51:v59S-12x F8F6D0A9C49AC7CD765F96092E6118E4

OSIG:[HL-DT-STDVD-ROM GDR3120L0059] Spoofed As: **[PBDS VAD6038-64930C]**

```
Repairing Test Sector.
Flashing Sector 9003F000
Done !
Flashing Sector 9003D000
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!

Finished! ☺

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

Lite-On PLDS DG-16D2S(-09C)

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 **Maximus USBXtractor & powerunit** or **Connectivity Kit v3 (optional probe)** 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.

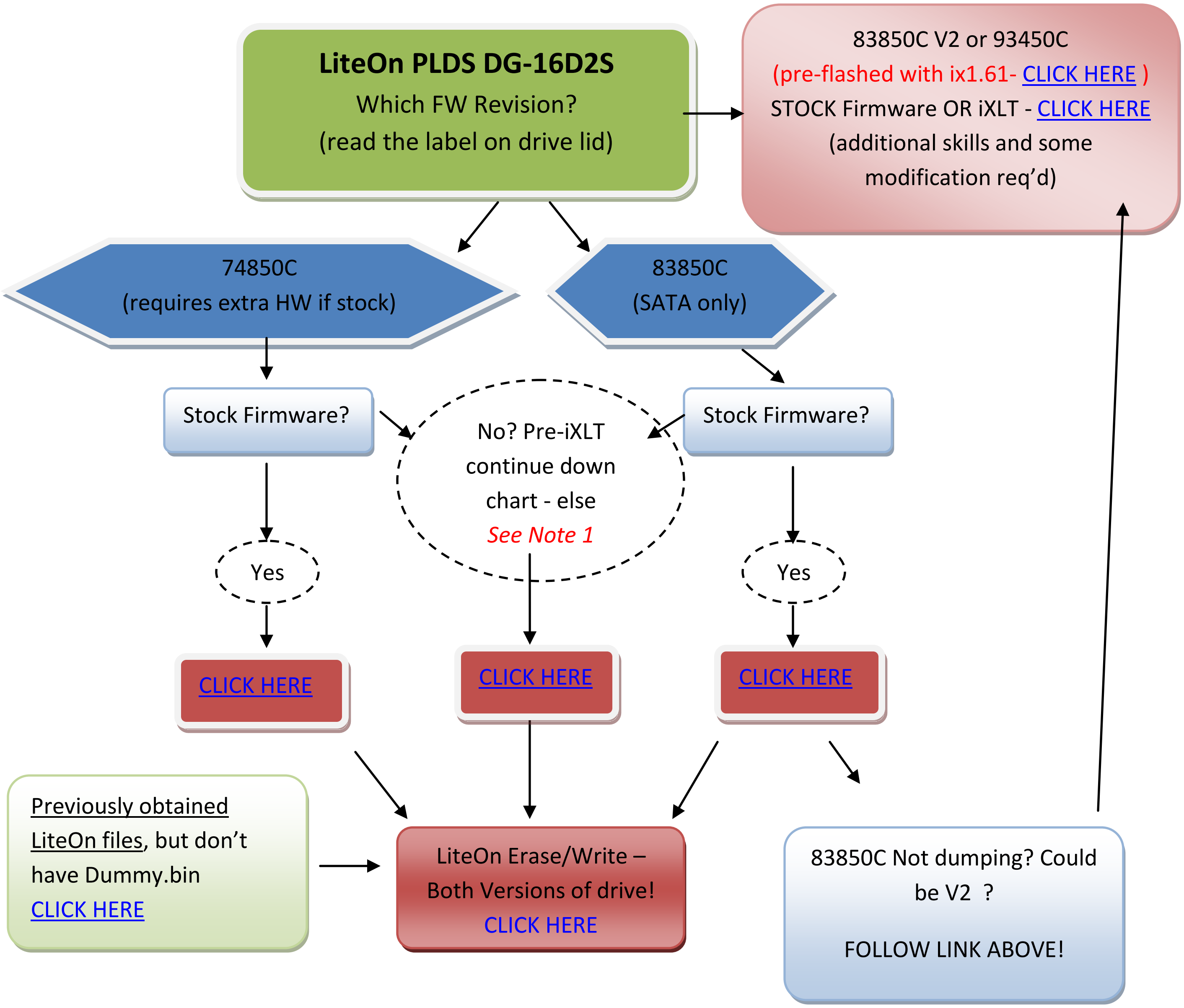
The **93450C** quickly followed – Once again key retrieval was not an option with simple sata commands or probe used for 74850C

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!

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

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.

YOU HAVE BEEN WARNED!



LiteOn PLDS DG-16D2S

Which FW Revision?

(read the label on drive lid)

83850C V2 or 93450C

(pre-flashed with ix1.61- CLICK HERE)

STOCK Firmware OR iXLT - CLICK HERE

(additional skills and some modification req'd)

74850C

(requires extra HW if stock)

83850C

(SATA only)

Stock Firmware?

No? Pre-iXLT continue down chart - else *See Note 1*

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 – Both Versions of drive! CLICK HERE

83850C Not dumping? Could be 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

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".

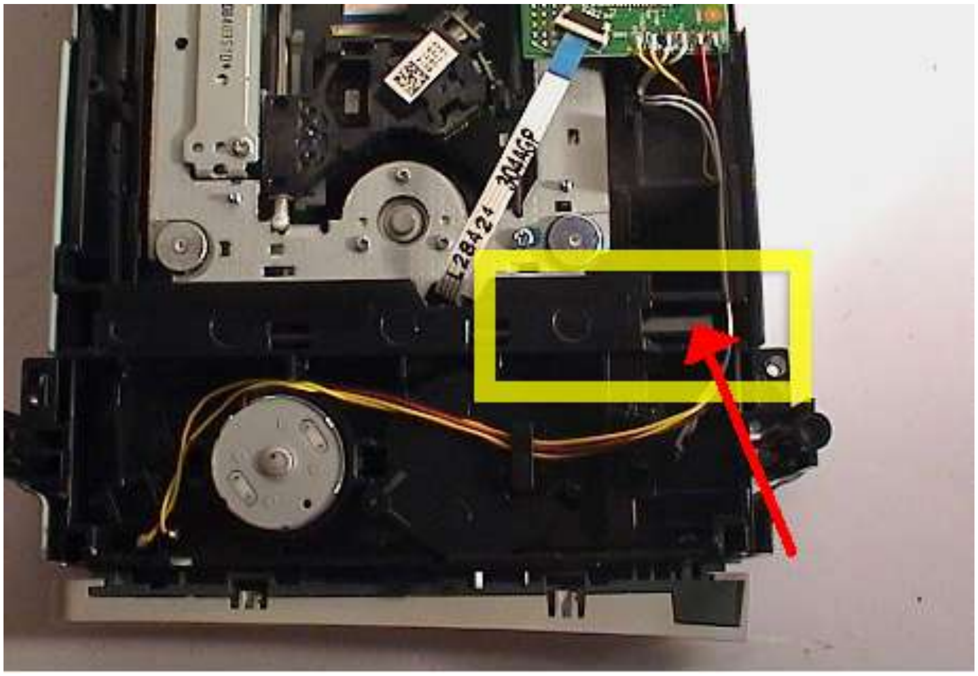
You need to power on the drive with **Eject status closed** but **Tray Half Open** – To do this using a connectivity kit/power unit/Xtractor as Power source, eject the DVD drive, then, press eject to 'close' the tray. **Now this is the important part – you MUST switch off the kit BEFORE it closes fully.**

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

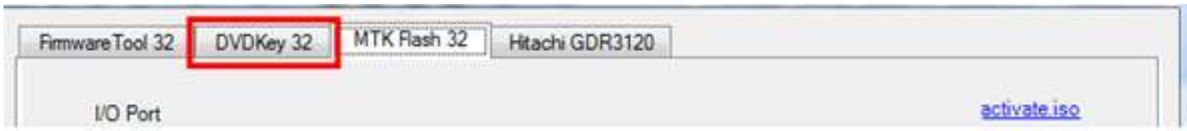
Jungleflasher – maintains backwards compatibility with files that have been extracted from earlier methods!

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

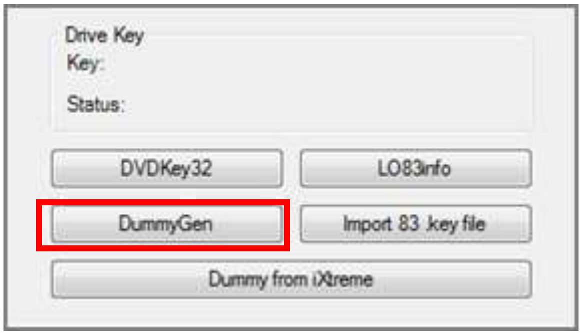
For 74850C Files (Key.bin/Inquiry.bin/Identify.bin) – Read On!

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

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



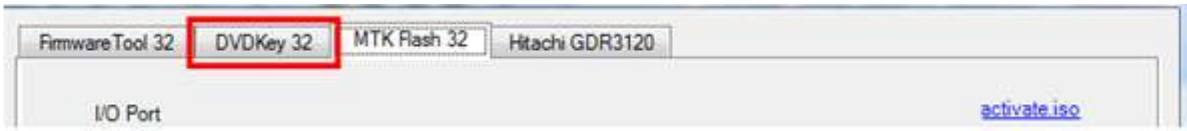
And press the **DummyGen** button – this will allow you to load each file into Jungleflasher which then creates a Dummy.bin and loads it as source. Ready for spoofing to target file and then to proceed onwards to erasing and writing!



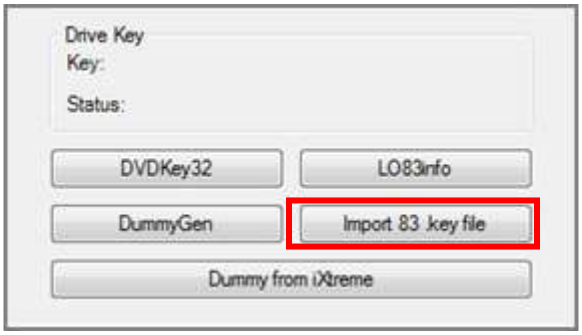
CLICK TO PROCEED TO FIRMWARE MANIPULATION

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

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

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

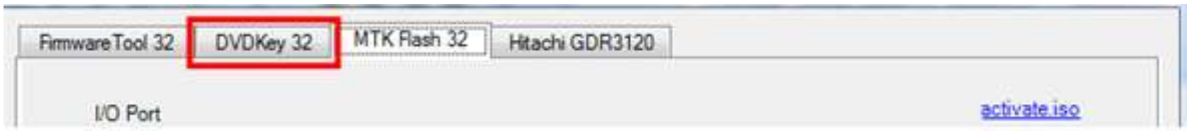
LiteOn drives of either FW version that have already been flashed with iXtreme can be easily dumped using only SATA connection (no requirement for probe or TTL convertor) ***this is a function of the iXtreme firmware NOT a workaround for dumping stock drives!***

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

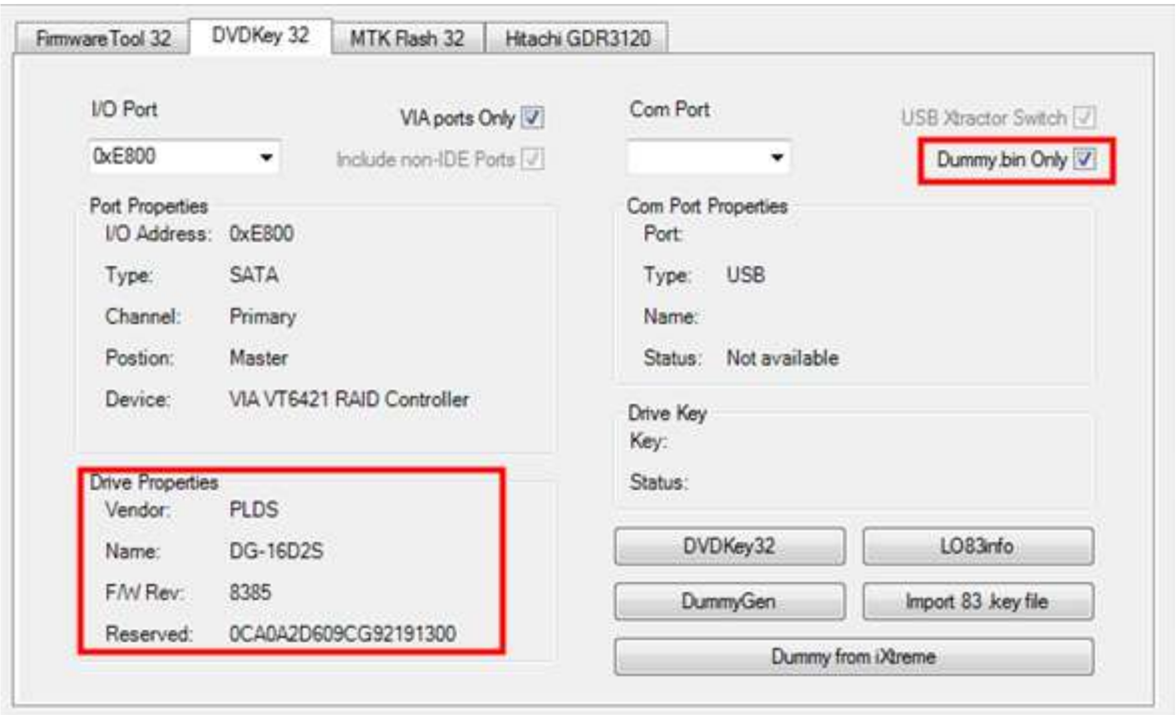
FOR INSTRUCTIONS ON HALF OPEN TRAY – CLICK HERE

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.



I/O Port: 0xE800

VIA ports Only ☑

Include non-IDE Ports ☑

Com Port:

USB Xtractor Switch ☑

Dummy.bin Only ☑

Port Properties

I/O Address:	0xE800
Type:	SATA
Channel:	Primary
Postion:	Master
Device:	VIA VT6421 RAID Controller

Drive Properties

Vendor:	PLDS
Name:	DG-16D2S
F/W Rev:	8385
Reserved:	0CA0A2D609CG92191300

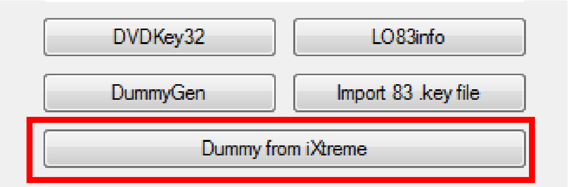
Com Port Properties

Port:	
Type:	USB
Name:	
Status:	Not available

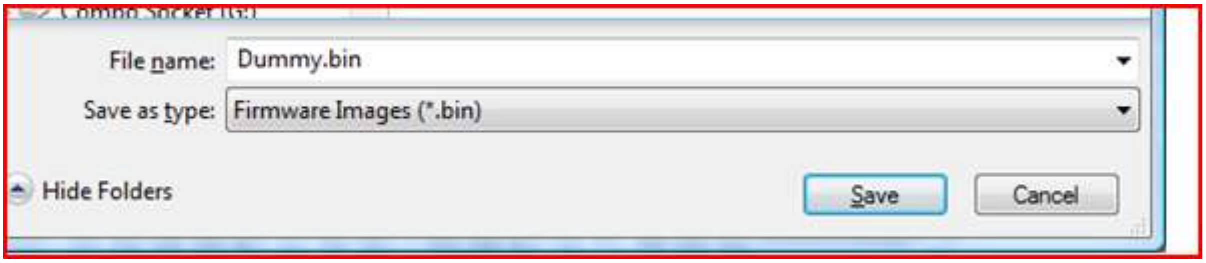
Drive Key

Key:	
Status:	

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



Save as prompted,



File name: Dummy.bin

Save as type: Firmware Images (*.bin)

CONTINUE WITH FIRMWARE SPOOF – CLICK HERE

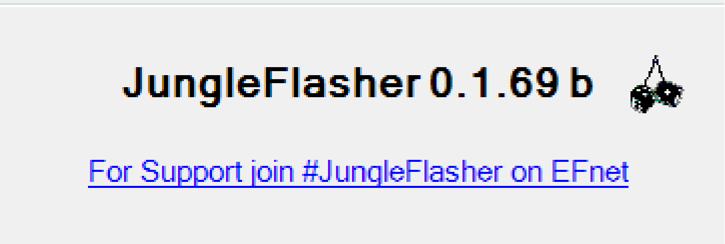
Extracting Key and drive info from 74850C LiteOn

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

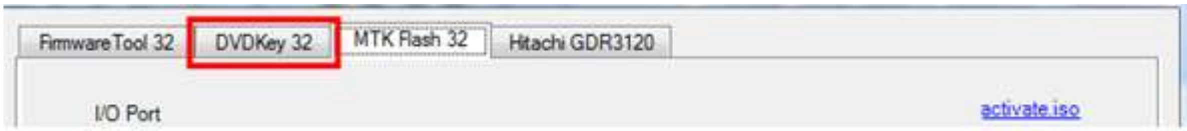
Open JungleFlasher, you will be presented with the Welcome Screen.



JungleFlasher 0.1.69 b

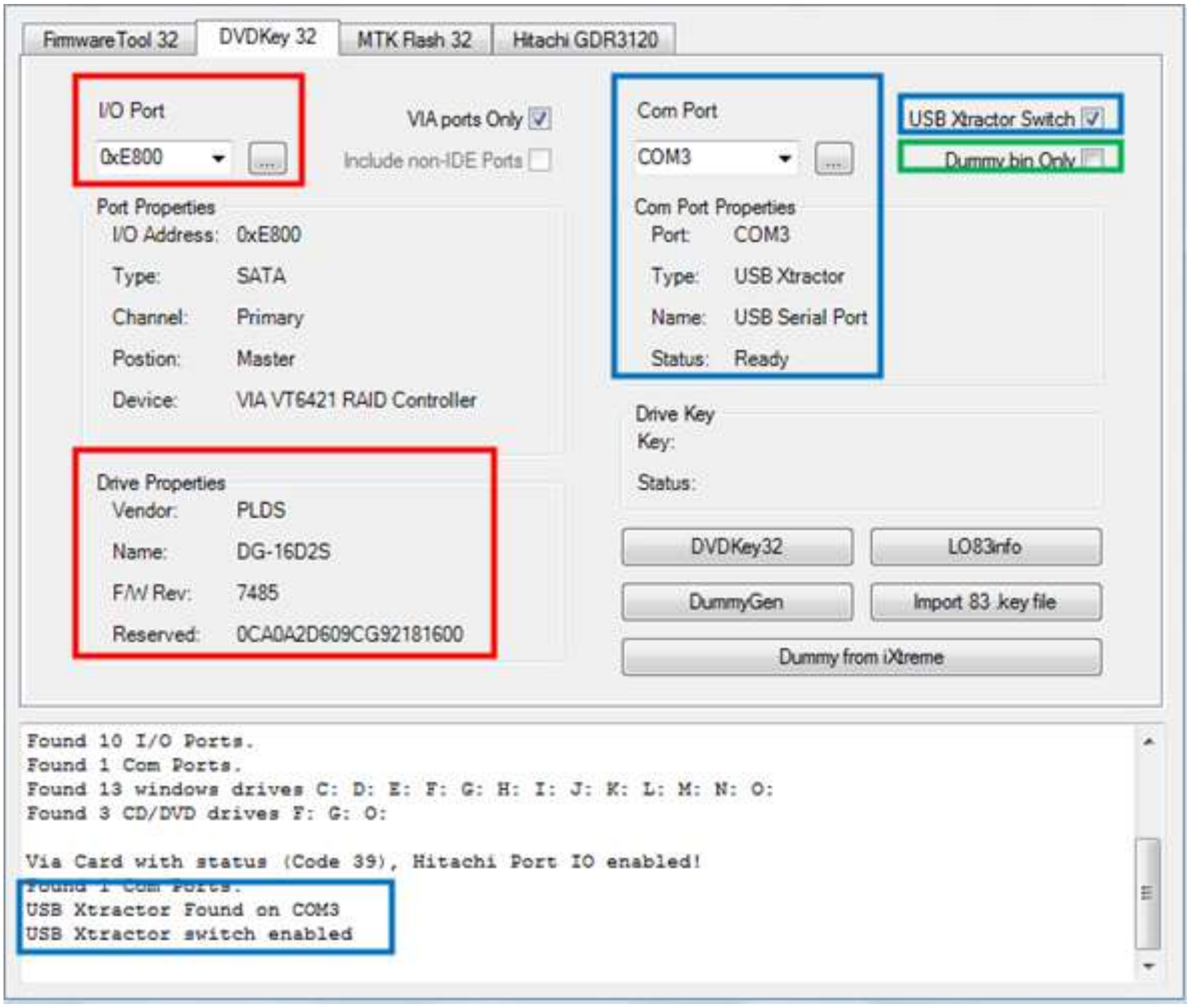
For Support join #JungleFlasher on EFnet

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) and COM port, then **insert probe / spear** into R707 via, optionally, choose to dump dummy.bin only (shown in green)as opposed to all 5 files (Key, Inquiry, Identify, Serial **and** dummy.bin). **USB Xtractor** user should enable **USB Xtractor Switch** check box (shown in blue)



I/O Port: 0xE800

VIA ports Only ☑

Include non-IDE Ports □

Port Properties

I/O Address: 0xE800

Type: SATA

Channel: Primary

Postion: Master

Device: VIA VT6421 RAID Controller

Drive Properties

Vendor: PLDS

Name: DG-16D2S

F/W Rev: 7485

Reserved: 0CA0A2D609CG92181600

Com Port: COM3

USB Xtractor Switch ☑

Dummy bin Only □

Com Port Properties

Port: COM3

Type: USB Xtractor

Name: USB Serial Port

Status: Ready

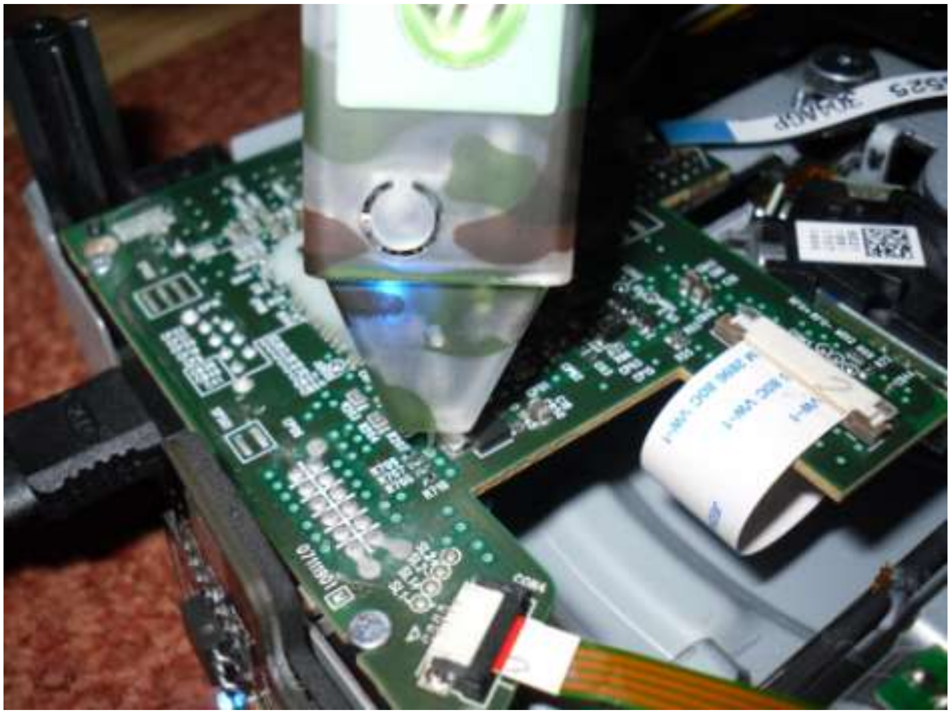
Drive Key

Key:

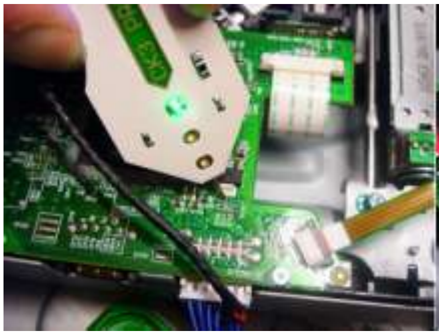
Status:

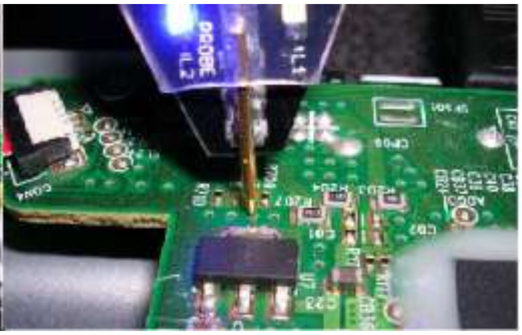
```
Found 10 I/O Ports.
Found 1 Com Ports.
Found 13 windows drives C: D: E: F: G: H: I: J: K: L: M: N: O:
Found 3 CD/DVD drives F: G: O:

Via Card with status (Code 39), Hitachi Port IO enabled!
Found 1 Com Ports.
USB Xtractor Found on COM3
USB Xtractor switch enabled
```

Good status on Probe / Spear / USBXtractor has LED showing.

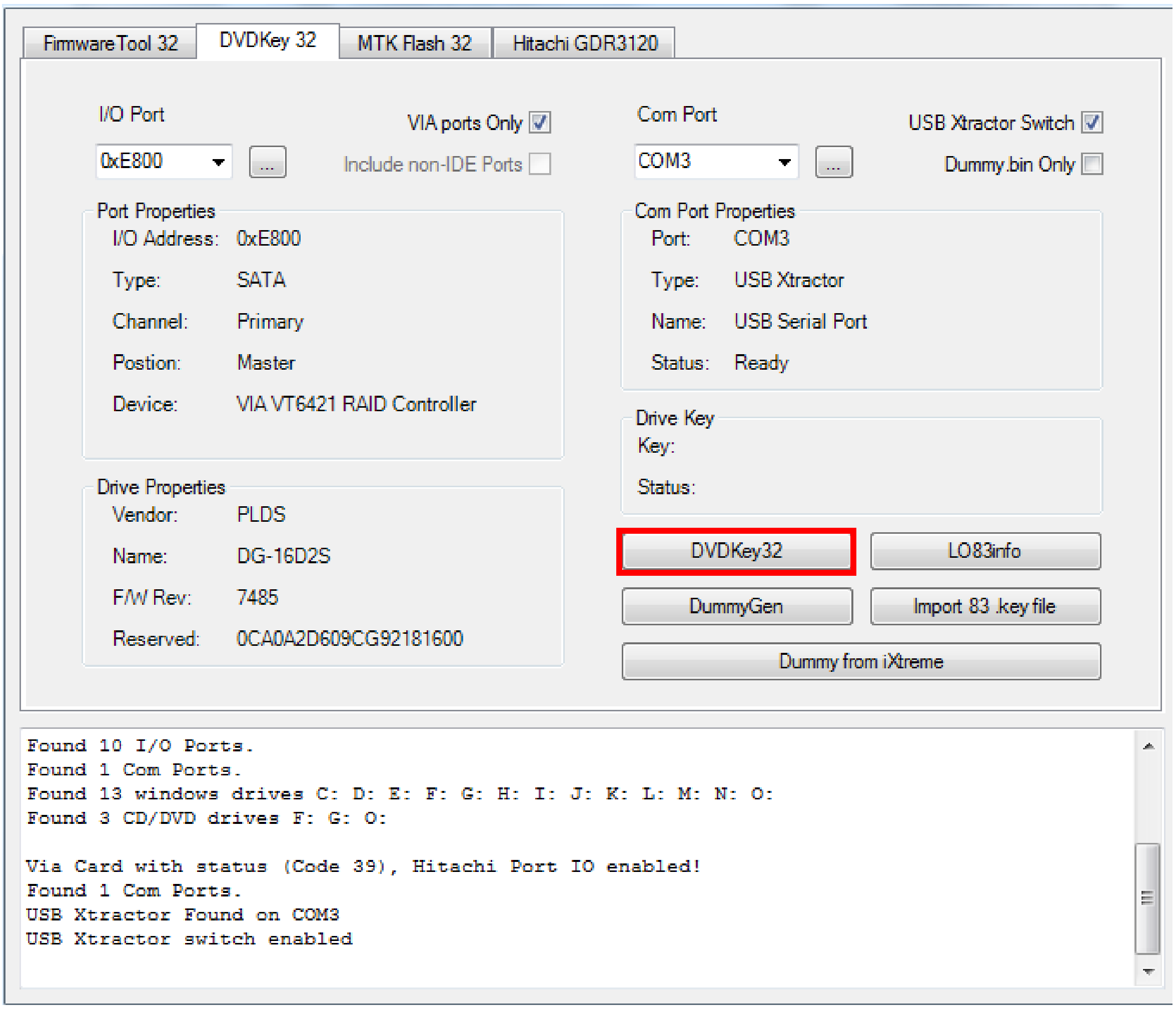


USBXtractor Users can press the button on probe to start DVDKey32 extraction process





Other Users press **DVDKey32** button**.**



I/O Port: 0xE800

VIA ports Only ☑

Include non-IDE Ports □

Com Port: COM3

USB Xtractor Switch ☑

Dummy.bin Only □

Port Properties
I/O Address: 0xE800
Type: SATA
Channel: Primary
Postion: Master
Device: VIA VT6421 RAID Controller

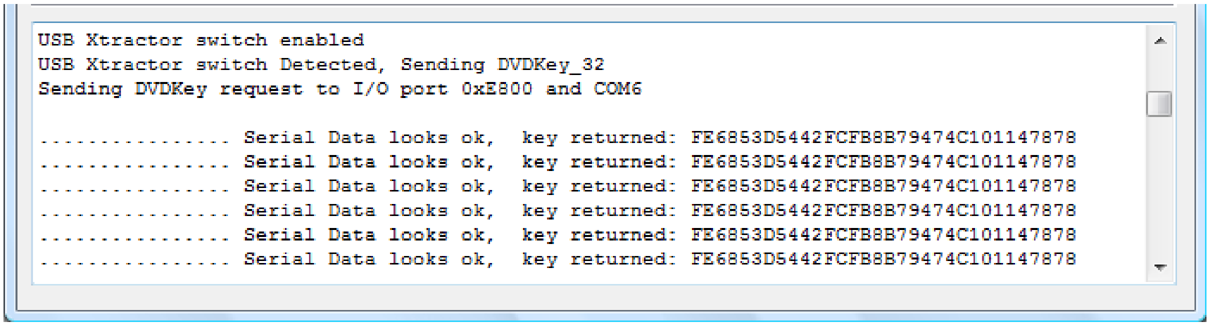
Com Port Properties
Port: COM3
Type: USB Xtractor
Name: USB Serial Port
Status: Ready

Drive Key
Key:
Status:

Drive Properties
Vendor: PLDS
Name: DG-16D2S
F/W Rev: 7485
Reserved: 0CA0A2D609CG92181600

```
Found 10 I/O Ports.
Found 1 Com Ports.
Found 13 windows drives C: D: E: F: G: H: I: J: K: L: M: N: O:
Found 3 CD/DVD drives F: G: O:

Via Card with status (Code 39), Hitachi Port IO enabled!
Found 1 Com Ports.
USB Xtractor Found on COM3
USB Xtractor switch enabled
```

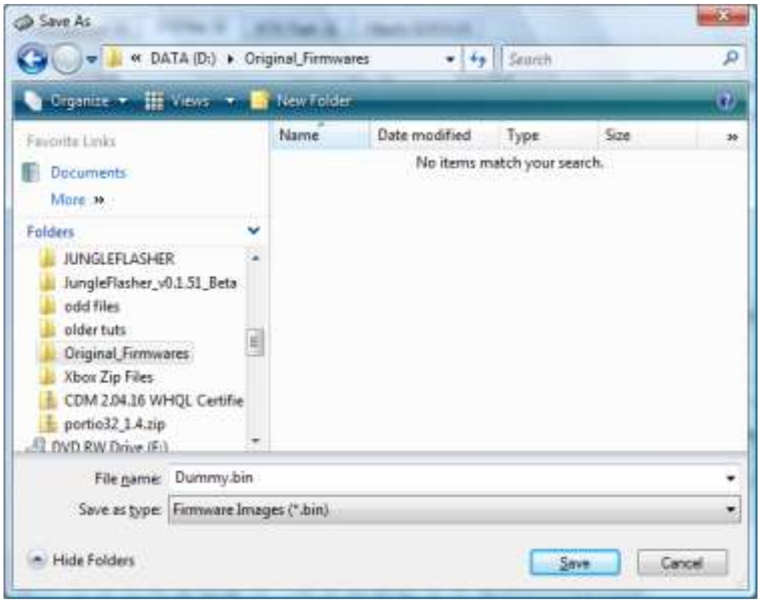
Providing serial connection was good, **DVDKey 32** will dump the key 6 times and compare each dump –



```
USB Xtractor switch enabled
USB Xtractor switch Detected, Sending DVDKey_32
Sending DVDKey request to I/O port 0xE800 and COM6

................ Serial Data looks ok,  key returned: FE6853D5442FCFB8B79474C101147878
................ Serial Data looks ok,  key returned: FE6853D5442FCFB8B79474C101147878
................ Serial Data looks ok,  key returned: FE6853D5442FCFB8B79474C101147878
................ Serial Data looks ok,  key returned: FE6853D5442FCFB8B79474C101147878
................ Serial Data looks ok,  key returned: FE6853D5442FCFB8B79474C101147878
................ Serial Data looks ok,  key returned: FE6853D5442FCFB8B79474C101147878
```

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.



File name: Dummy.bin

Save as type: Firmware Images (*.bin)

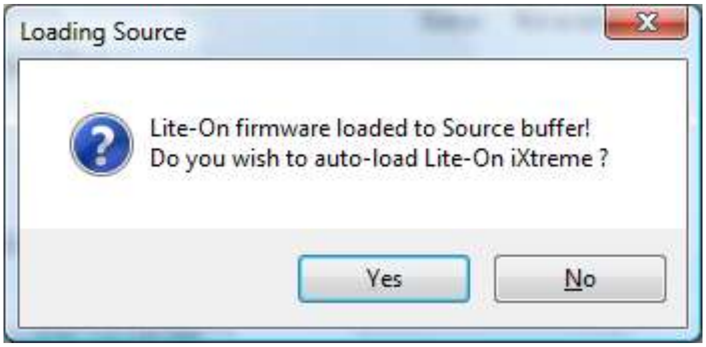
Although extracting the key 6 times increases the chances of correct key being obtained and checks are carried out on validity – There is only one way to know for sure the key is GOOD.

You should, where possible, spoof the data into a different drive and test to see it works BEFORE erasing the Lite-On Drive.

There is no harm in running DVDKey 32 multiple times, increasing the number of key extractions.

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.


Loading Source

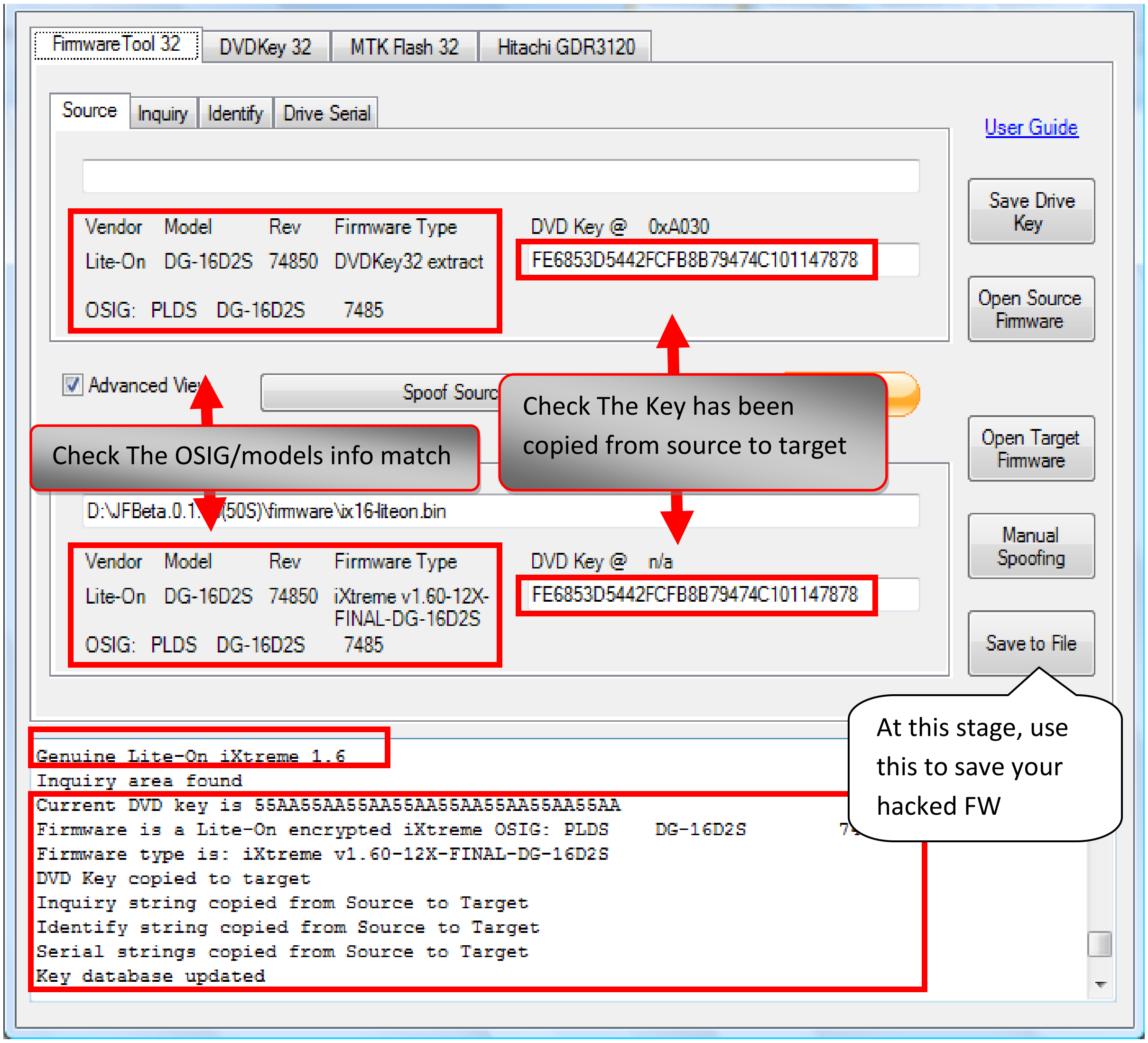
Lite-On firmware loaded to Source buffer!
Do you wish to auto-load Lite-On iXtreme ?

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!



Vendor	Model	Rev	Firmware Type
Lite-On	DG-16D2S	74850	DVDKey32 extract
OSIG: PLDS	DG-16D2S		7485

DVD Key @ 0xA030

FE6853D5442FCFB8B79474C101147878

☑ Advanced View

Check The OSIG/models info match

Check The Key has been copied from source to target

D:\JFBeta.0.1 (50S)\firmware\ix16-liteon.bin

Vendor	Model	Rev	Firmware Type
Lite-On	DG-16D2S	74850	iXtreme v1.60-12X-FINAL-DG-16D2S
OSIG: PLDS	DG-16D2S		7485

DVD Key @ n/a

FE6853D5442FCFB8B79474C101147878

At this stage, use this to save your hacked FW

```
Genuine Lite-On iXtreme 1.6
Inquiry area found
Current DVD key is 55AA55AA55AA55AA55AA55AA55AA55AA
Firmware is a Lite-On encrypted iXtreme OSIG: PLDS     DG-16D2S        7
Firmware type is: iXtreme v1.60-12X-FINAL-DG-16D2S
DVD Key copied to target
Inquiry string copied from Source to Target
Identify string copied from Source to Target
Serial strings copied from Source to Target
Key database updated
```

(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!)

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.**

You should, where possible spoof the data into a different drive and test to see it works BEFORE erasing the Lite-On Drive.

Spoofing Hitachi – Click Here!

Spoofing other drives – Click Here!

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

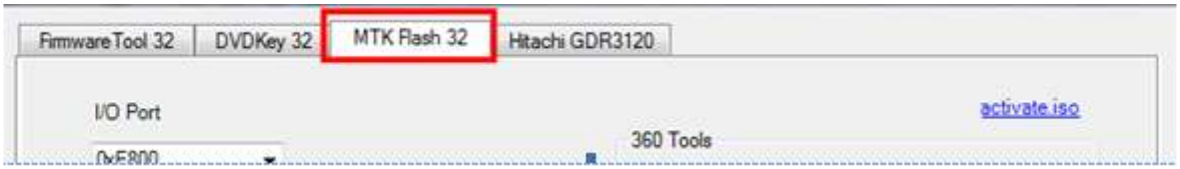
There is no harm in Dumping the key/info multiple times, increasing the number of key extractions.

Erasing a Lite-On PLDS DG-16D2S.

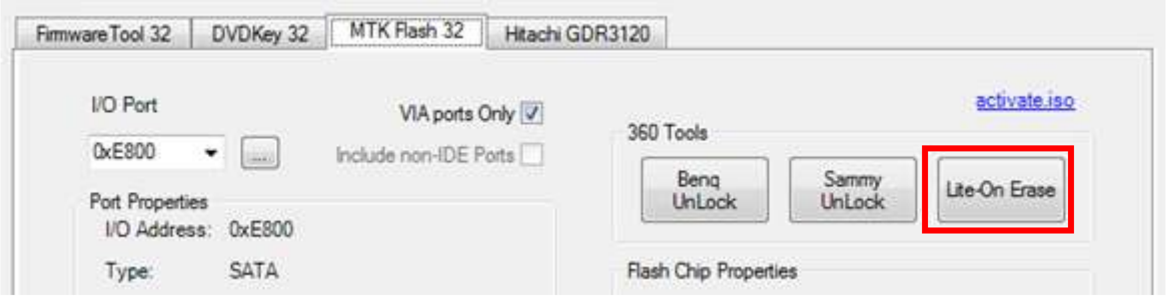
PLEASE READ THE WARNINGS ABOVE.

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.**



I/O Port: 0xE800

VIA ports Only ☑

Include non-IDE Ports □

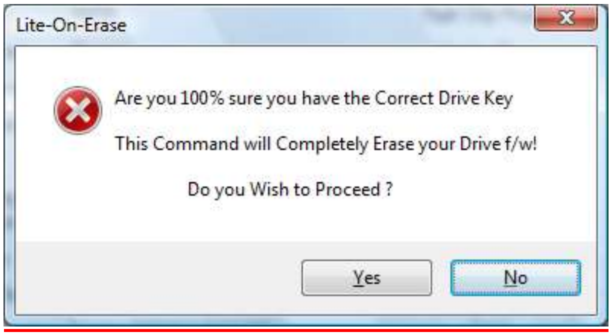
Port Properties

I/O Address: 0xE800

Type: SATA

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

Please Note, the only way to know 100% that a key is good, is to flash a different drive and test BEFORE sending erase command.



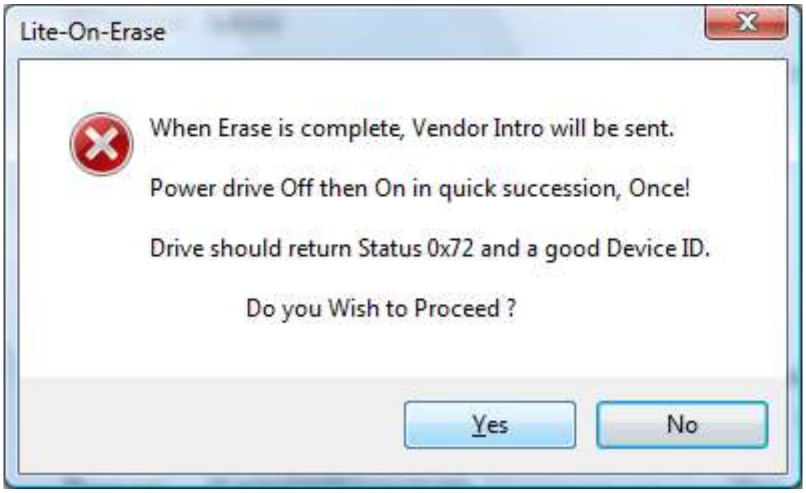
Are you 100% sure you have the Correct Drive Key

This Command will Completely Erase your Drive f/w!

Do you Wish to Proceed ?

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

JungleFlasher will present you with another warning.



When Erase is complete, Vendor Intro will be sent.

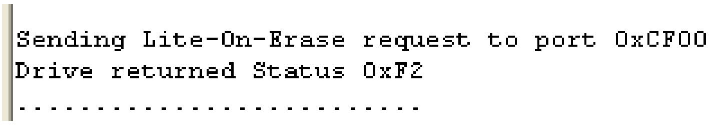
Power drive Off then On in quick succession, Once!

Drive should return Status 0x72 and a good Device ID.

Do you Wish to Proceed ?

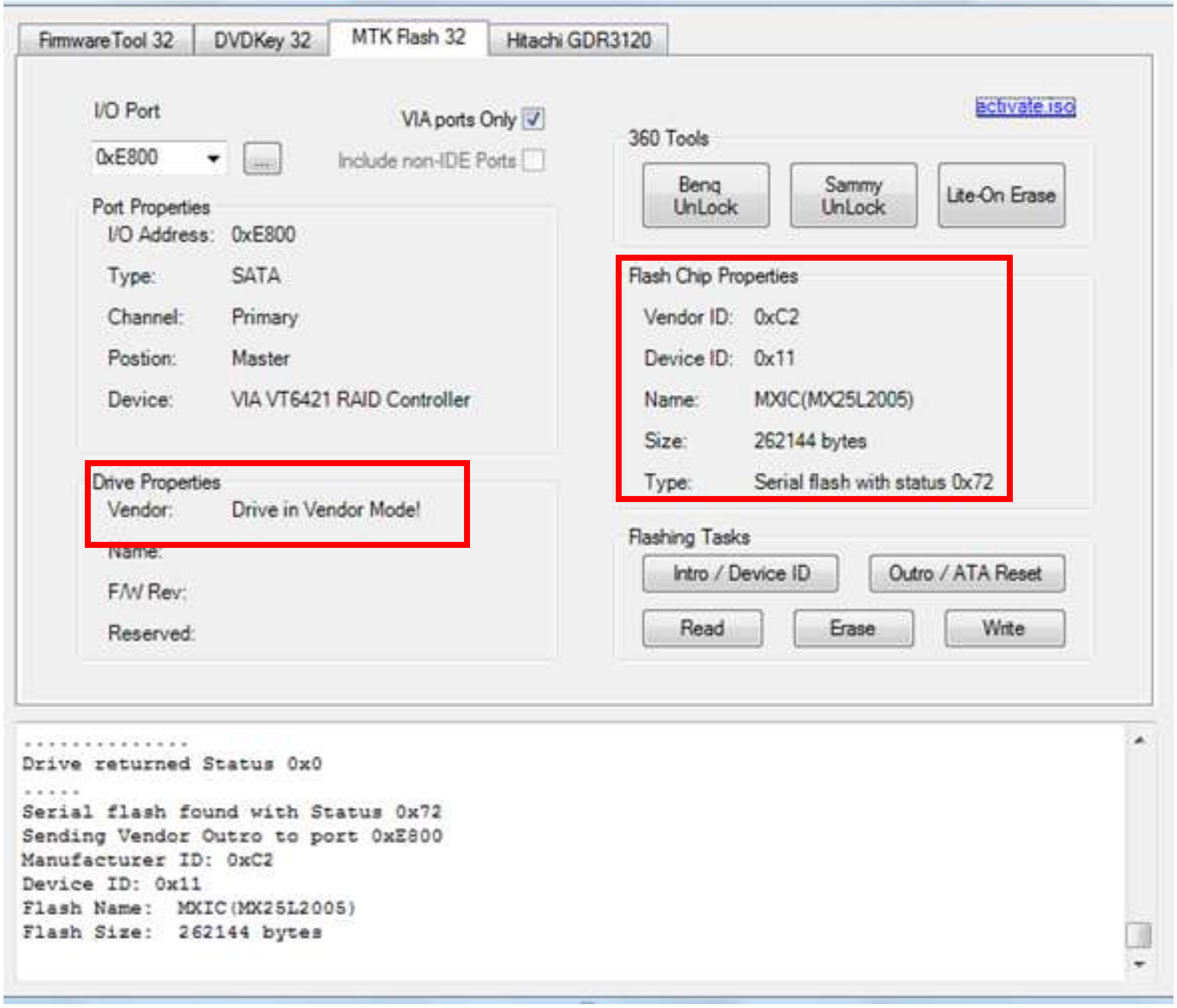
Read this carefully, in most cases JungleFlasher wil return a Running Log similar to this: We have had 0xD0 / 0x80 / 0xF2 / 0xD1 and all worked fine.

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



```
Sending Lite-On-Erase request to port 0xCF00
Drive returned Status 0xF2
. . . . . . . . . . . . . . . . . . . . . . . . . .
```

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.**



I/O Port: 0xE800

VIA ports Only ☑

Include non-IDE Ports □

Port Properties

I/O Address: 0xE800

Type: SATA

Channel: Primary

Postion: Master

Device: VIA VT6421 RAID Controller

Drive Properties

Vendor: Drive in Vendor Mode!

Name:

F/W Rev:

Reserved:

Flash Chip Properties

Vendor ID: 0xC2

Device ID: 0x11

Name: MXIC(MX25L2005)

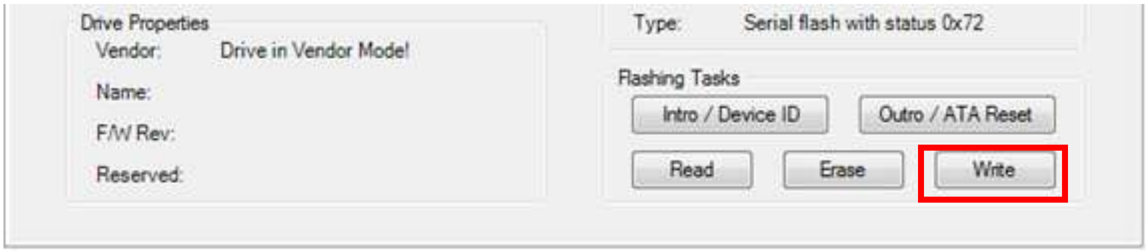
Size: 262144 bytes

Type: Serial flash with status 0x72

```
...............
Drive returned Status 0x0
.....
Serial flash found with Status 0x72
Sending Vendor Outro to port 0xE800
Manufacturer ID: 0xC2
Device ID: 0x11
Flash Name:  MXIC(MX25L2005)
Flash Size:  262144 bytes
```

Drive is now in Vendor Mode (0x72).

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



Drive Properties

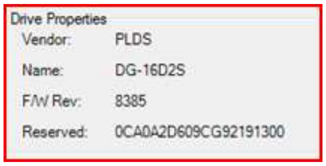
Vendor: Drive in Vendor Mode!

Name:

F/W Rev:

Reserved:

Type: Serial flash with status 0x72



Drive Properties

Vendor: PLDS

Name: DG-16D2S

F/W Rev: 8385

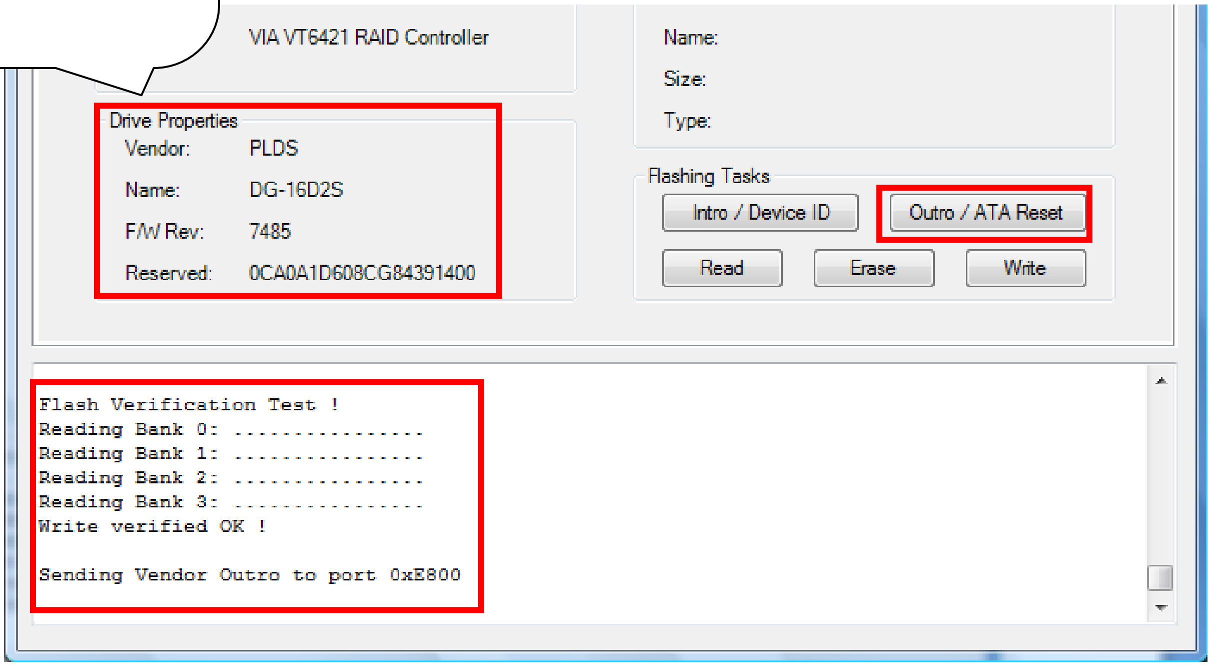
Reserved: 0CA0A2D609CG92191300

Different properties when flashing an 83850C, for example

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

Now send an Outro to the drive.

Done by pressing the **Outro / ATA** Reset Button



VIA VT6421 RAID Controller

Drive Properties

Vendor: PLDS

Name: DG-16D2S

F/W Rev: 7485

Reserved: 0CA0A1D608CG84391400

Name:

Size:

Type:

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

Sending Vendor Outro to port 0xE800
```

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, 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 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 –

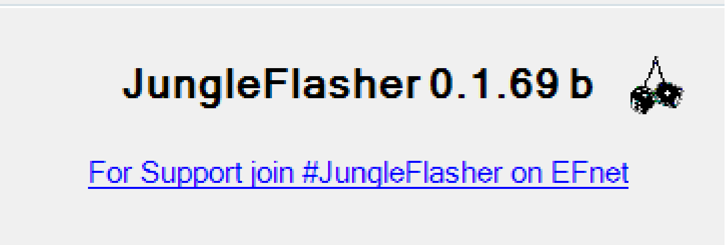
83850C v1 drive's information is extracted through SATA!

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

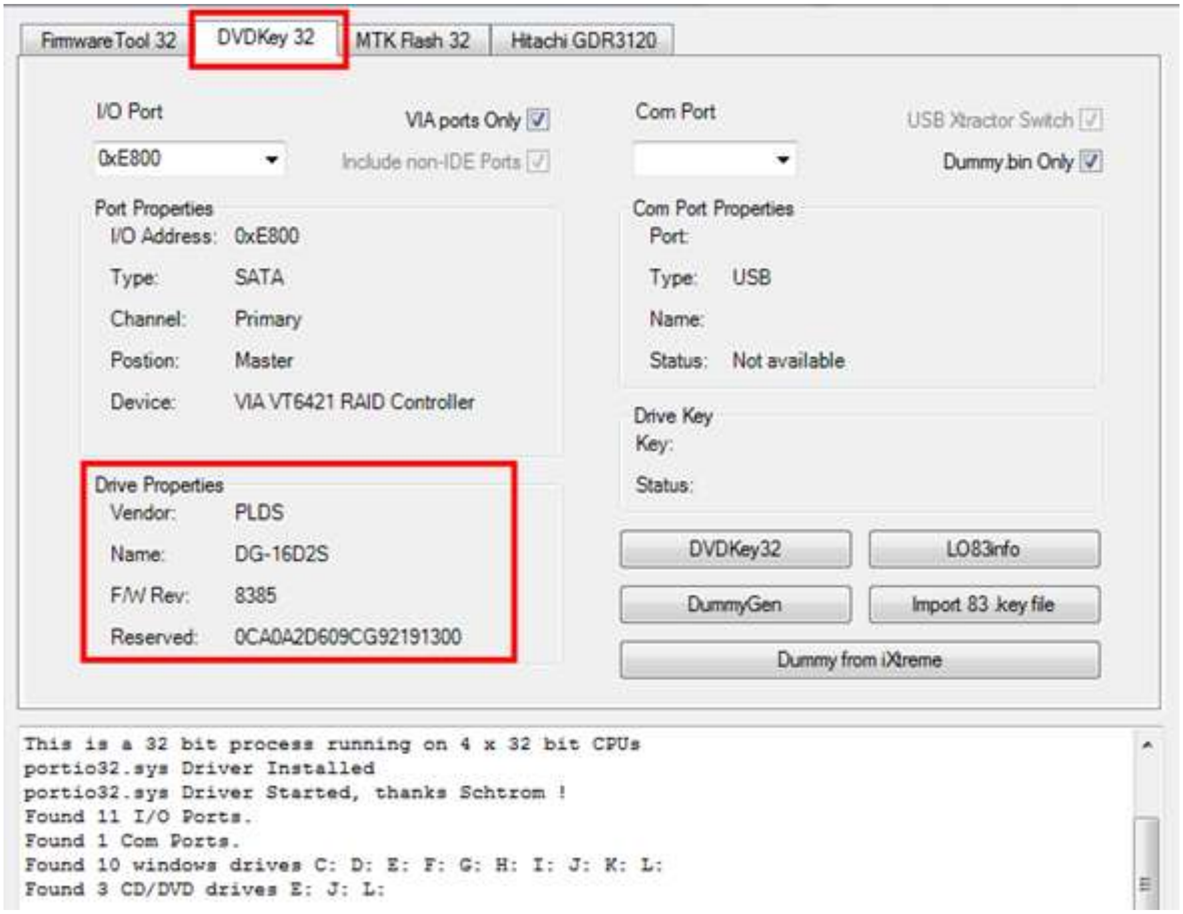
Power on and run JungleFlasher v0.1.69b or above



JungleFlasher 0.1.69 b

For Support join #JungleFlasher on EFnet

Select **DVDKey32 Tab**



I/O Port: 0xE800

VIA ports Only ☑

Include non-IDE Ports ☑

Com Port:

Dummy.bin Only ☑

Port Properties

I/O Address: 0xE800

Type: SATA

Channel: Primary

Postion: Master

Device: VIA VT6421 RAID Controller

Com Port Properties

Port:

Type: USB

Name:

Status: Not available

Drive Properties

Vendor: PLDS

Name: DG-16D2S

F/W Rev: 8385

Reserved: 0CA0A2D609CG92191300

Drive Key

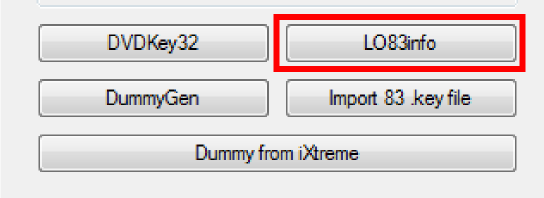
Key:

Status:

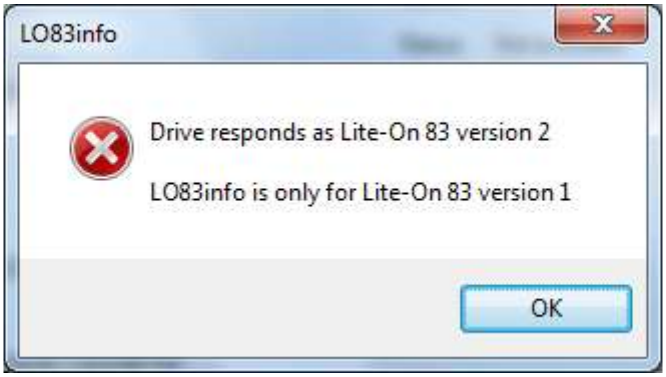
```
This is a 32 bit process running on 4 x 32 bit CPUs
portio32.sys Driver Installed
portio32.sys Driver Started, thanks Schtrom !
Found 11 I/O Ports.
Found 1 Com Ports.
Found 10 windows drives C: D: E: F: G: H: I: J: K: L:
Found 3 CD/DVD drives E: J: L:
```

Check to see the 83850c Inquires on the port.

Select **LO83info**



If you see this message:

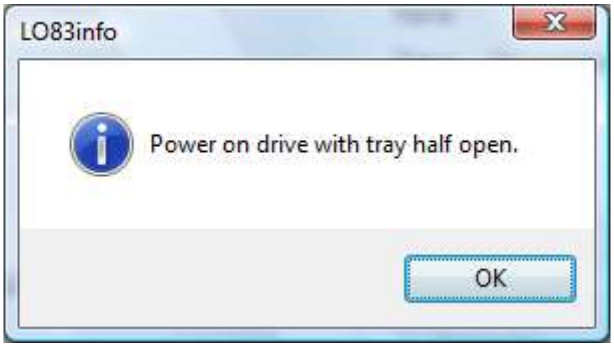

LO83info

Drive responds as Lite-On 83 version 2

LO83info is only for Lite-On 83 version 1

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

IF NOT then you have the **83850C v1** and should see THIS!


LO83info

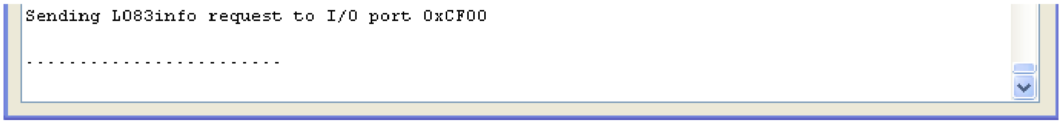
Power on drive with tray half open.

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

FOR INSTRUCTIONS ON HALF OPEN TRAY – CLICK HERE

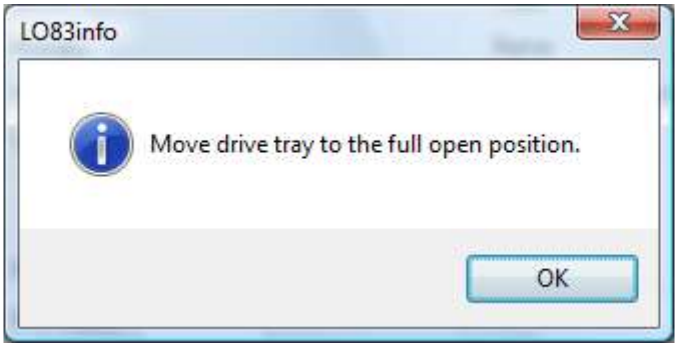
Please ensure you have the drive **fresh / power cycled after setting Half Open Tray, this is essential.** Then, click **OK**

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



```
Sending L083info request to I/O port 0xCF00

------------------------
```

Within a few seconds, you will also be prompted with an instruction from JungleFlasher to set the drive to full Open Tray status



LO83info

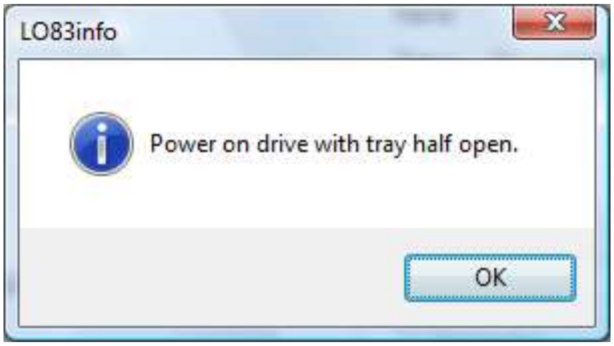
Move drive tray to the full open position.

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 **power on** with half open tray again.

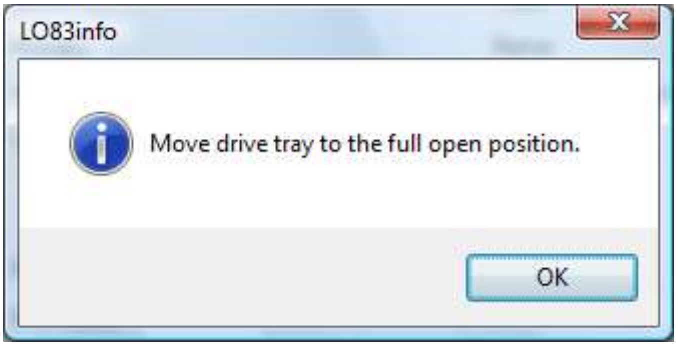

LO83info

Power on drive with tray half open.

As with the original command, please ensure the drive is **fresh / power cycled as part of setting "tray half open" , before continuing**

Once this is set, click **OK**

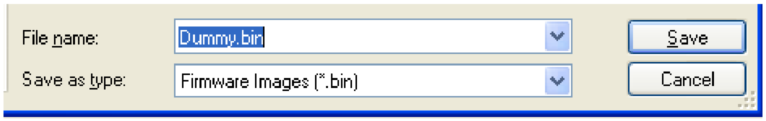
JungleFlasher will then ask you to set full open tray again


LO83info

Move drive tray to the full open position.

Move the tray to the fully ejected position as before and click **OK**

Jungleflasher will now prompt you to save!

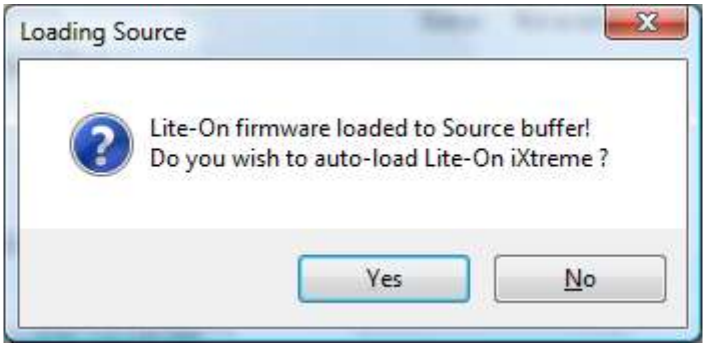

File name: Dummy.bin

Save as type: Firmware Images (*.bin)

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 and Identify.bin 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)

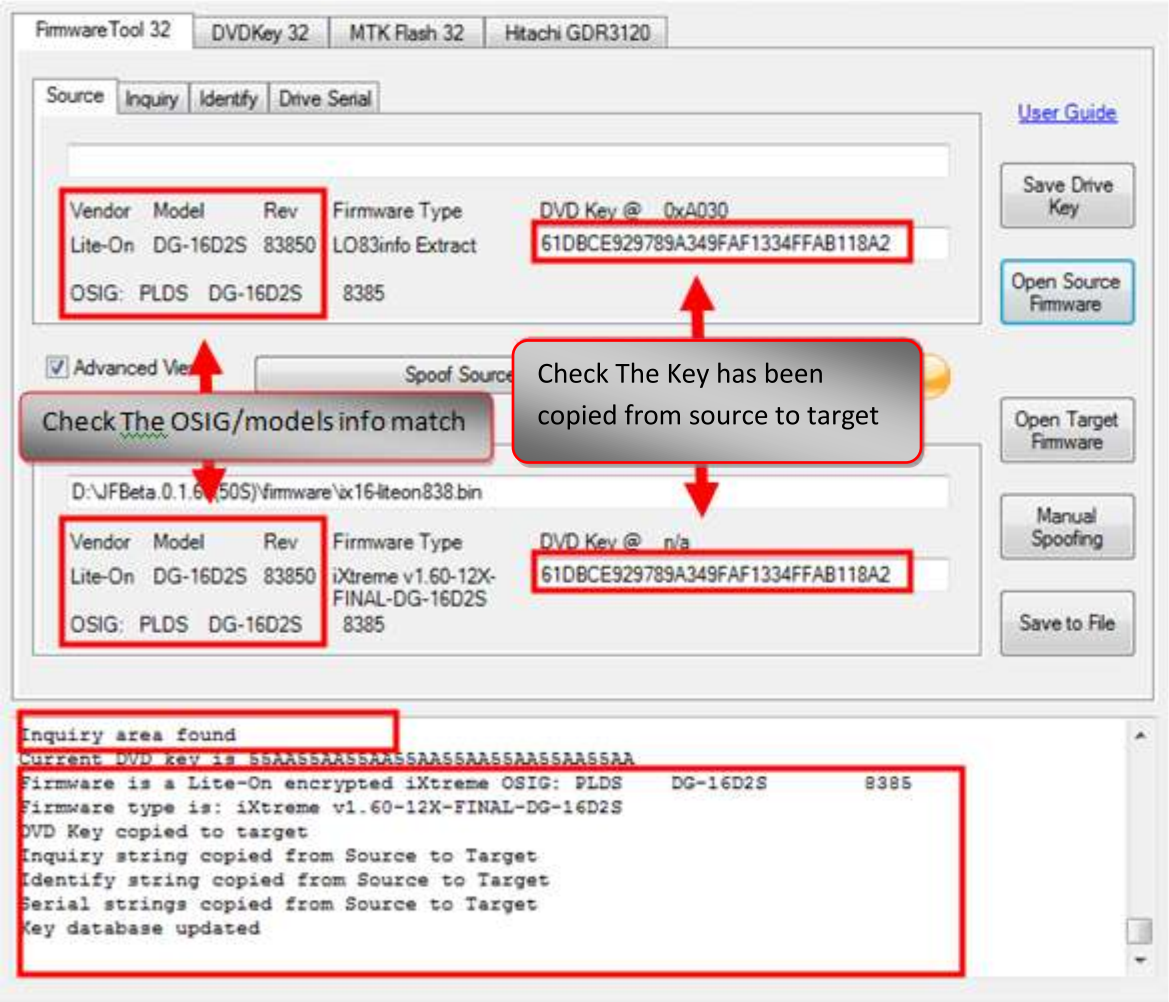


Loading Source

Lite-On firmware loaded to Source buffer!
Do you wish to auto-load Lite-On iXtreme ?

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!



Vendor Model Rev
Lite-On DG-16D2S 83850
OSIG: PLDS DG-16D2S

Firmware Type
LO83info Extract
8385

DVD Key @ 0xA030
61DBCE929789A349FAF1334FFAB118A2

Check The OSIG/models info match

Check The Key has been copied from source to target

D:\JFBeta.0.1.6(50S)\firmware\ix16-liteon838.bin

Vendor Model Rev
Lite-On DG-16D2S 83850
OSIG: PLDS DG-16D2S

Firmware Type
iXtreme v1.60-12X-FINAL-DG-16D2S
8385

DVD Key @ n/a
61DBCE929789A349FAF1334FFAB118A2

```
Inquiry area found
Current DVD key is 55AA55AA55AA55AA55AA55AA55AA55AA
Firmware is a Lite-On encrypted iXtreme OSIG: PLDS    DG-16D2S        8385
Firmware type is: iXtreme v1.60-12X-FINAL-DG-16D2S
DVD Key copied to target
Inquiry string copied from Source to Target
Identify string copied from Source to Target
Serial strings copied from Source to Target
Key database updated
```

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

Dumping OFW from LiteOn (required for 83850C v2 & 93450C or ANY Liteon with iXtreme LT firmware)

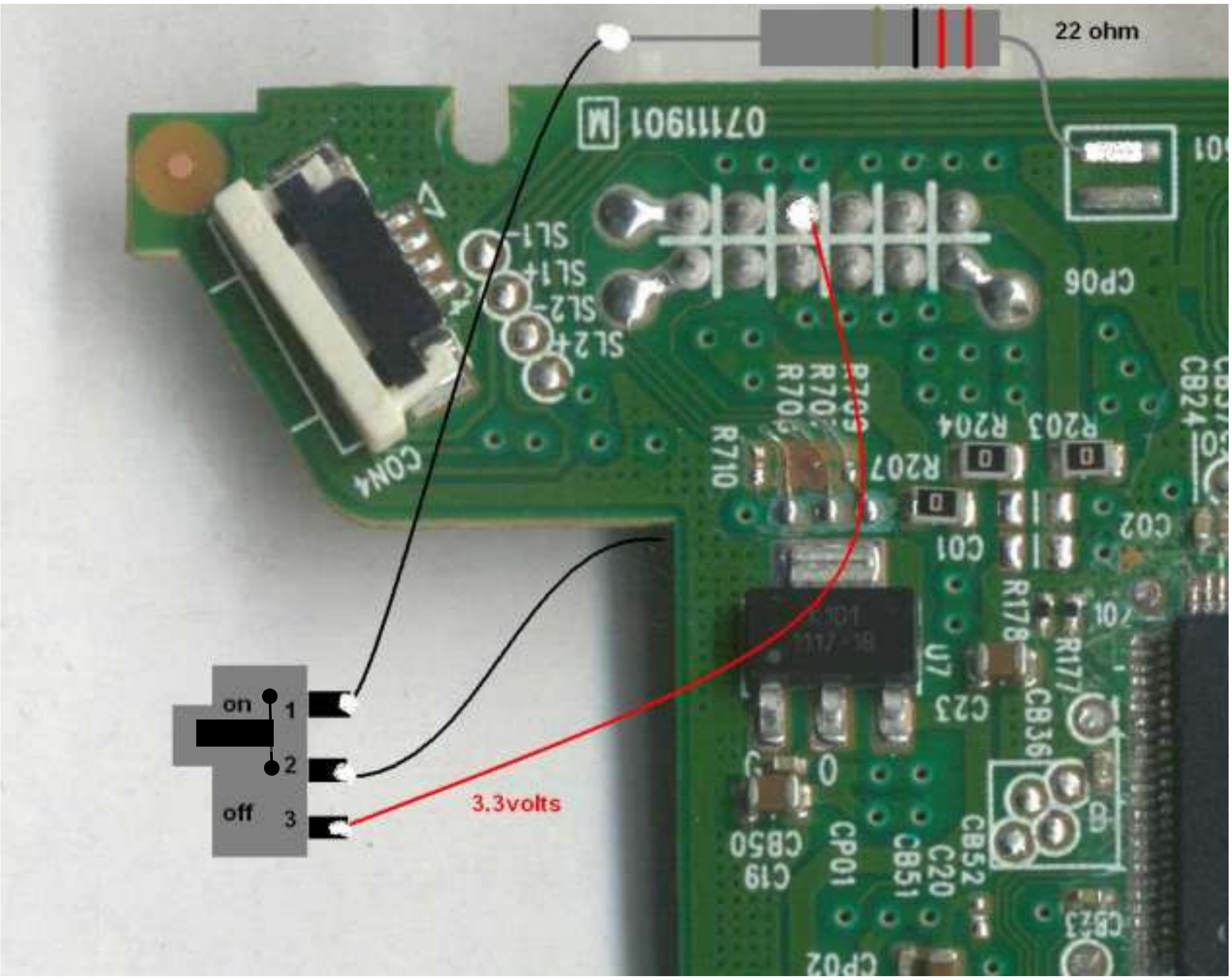
The MRA Hack

Can be used on ALL current LiteOn Drives

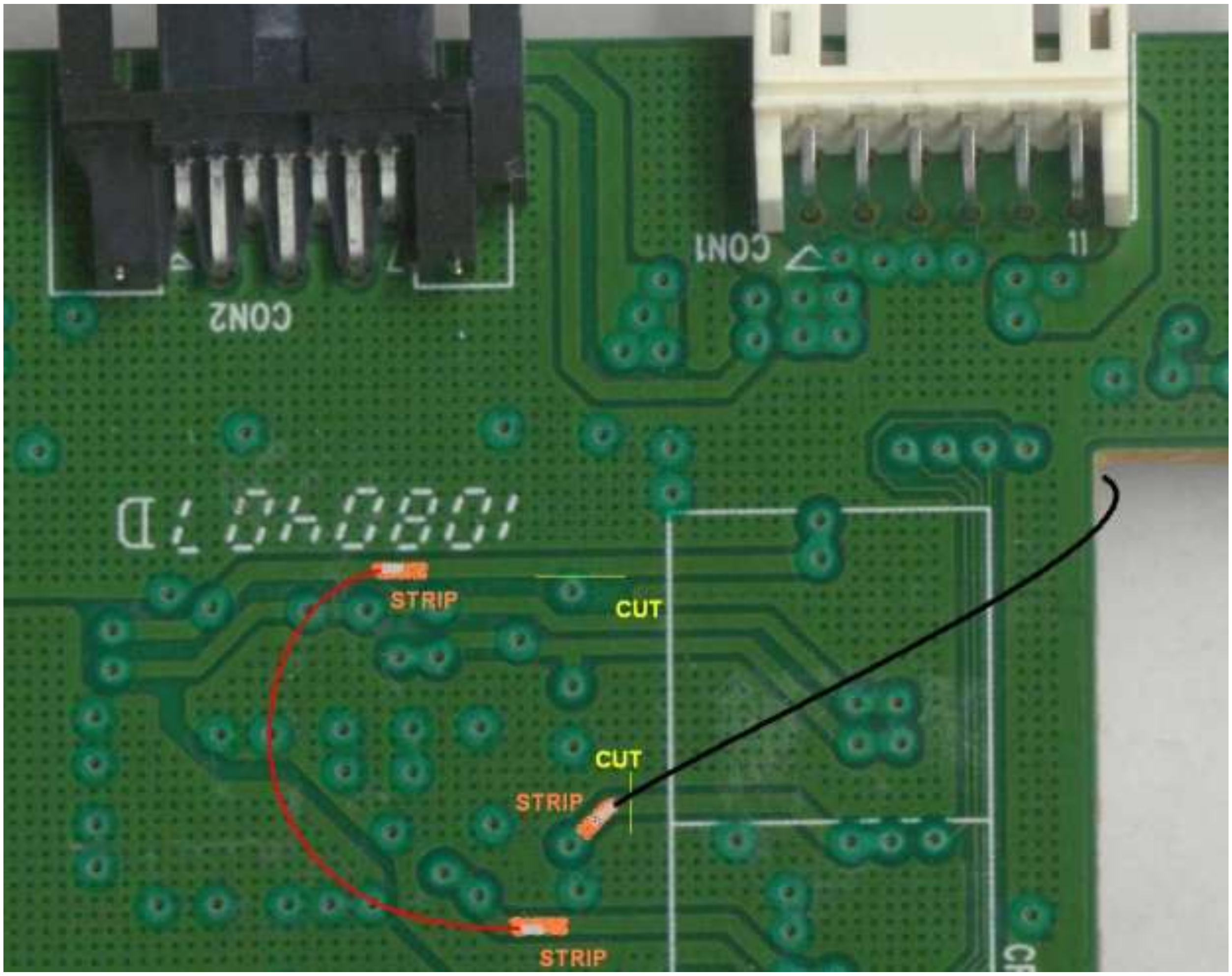
Soldering/Electronics skills are required for this modification – It Should NOT be attempted by people without such skills!

Basic wiring guide for the drives PCB

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



Pic 1



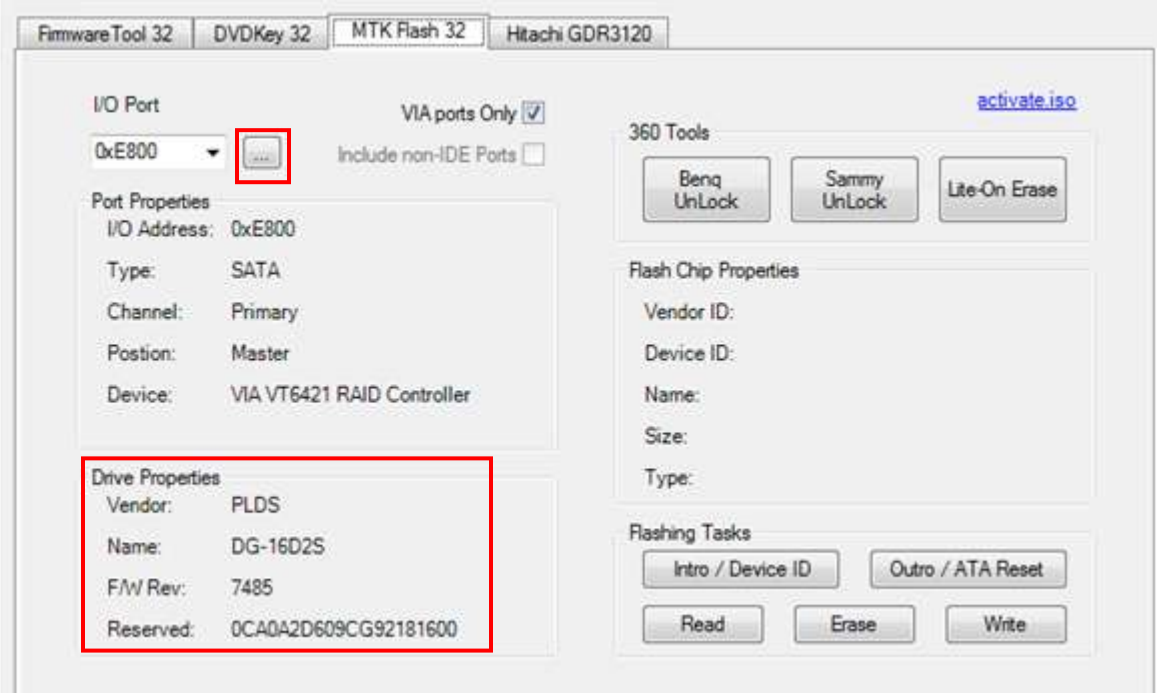
Pic 2

The 2 trace locations in yellow must be cut !

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

Connect drive to sata and power drive, select **MTK** tab

Refresh, drive properties – so drive shows up



I/O Port: 0xE800

VIA ports Only ☑

Include non-IDE Ports □

Port Properties

I/O Address:	0xE800
Type:	SATA
Channel:	Primary
Postion:	Master
Device:	VIA VT6421 RAID Controller

Drive Properties

Vendor:	PLDS
Name:	DG-16D2S
F/W Rev:	7485
Reserved:	0CA0A2D609CG92181600

Flash Chip Properties

Vendor ID:

Device ID:

Name:

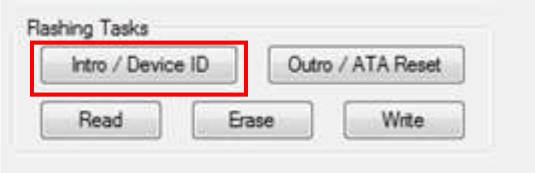
Size:

Type:

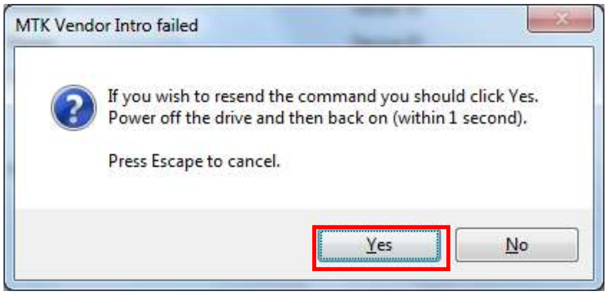
Turn power off to the drive

Operate switch you added! to connect to 22 ohm resistor side (On)

Press **intro/ Device ID button**



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



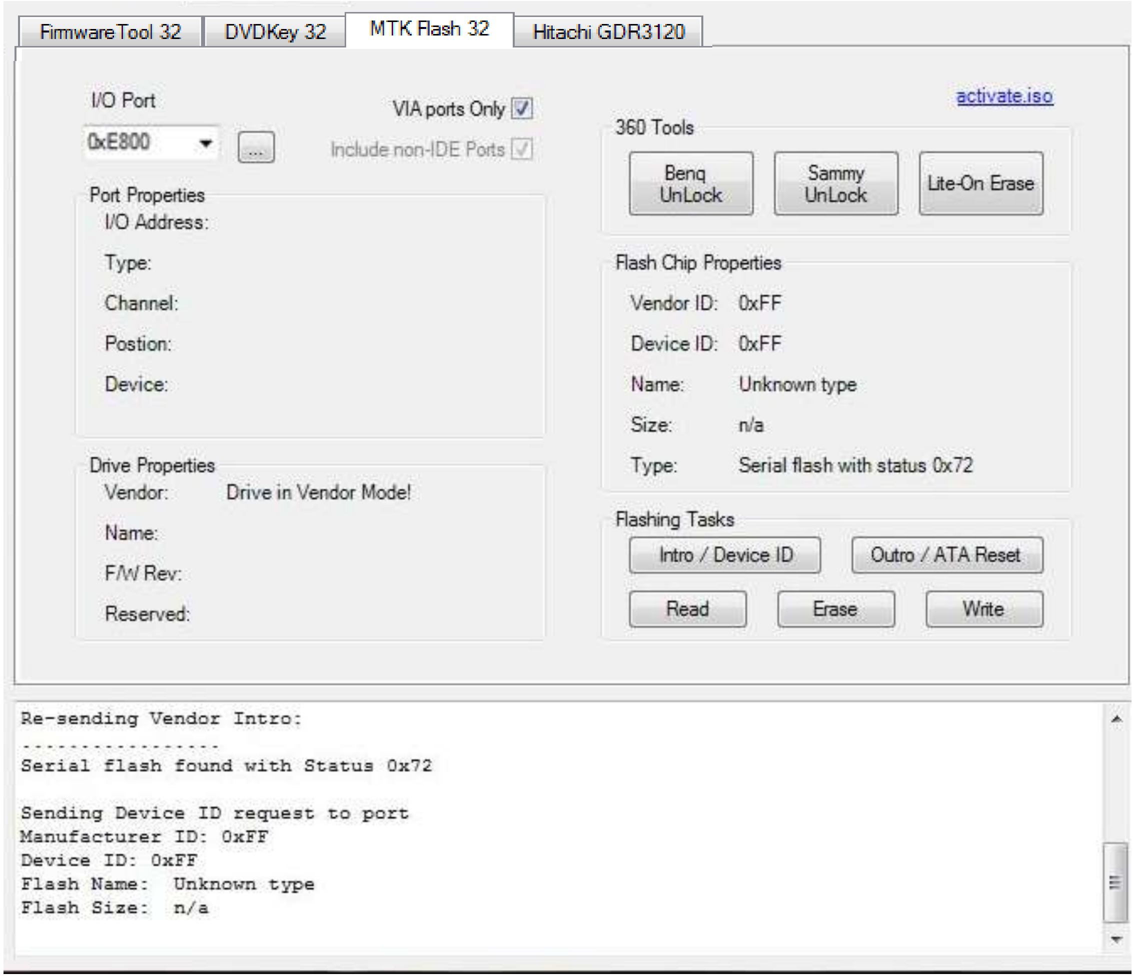
MTK Vendor Intro failed

If you wish to resend the command you should click Yes.
Power off the drive and then back on (within 1 second).

Press Escape to cancel.

Then power on drive! After 2 seconds, operate the added switch again (Off in pic 1) to 3v3 side.

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



I/O Port: 0xE800

VIA ports Only ☑

Include non-IDE Ports ☑

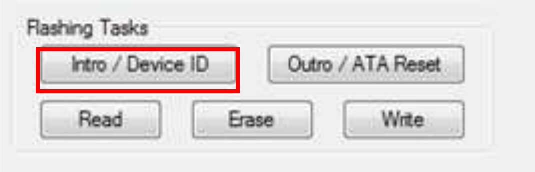
Port Properties
I/O Address:
Type:
Channel:
Postion:
Device:

Drive Properties
Vendor: Drive in Vendor Mode!
Name:
F/W Rev:
Reserved:

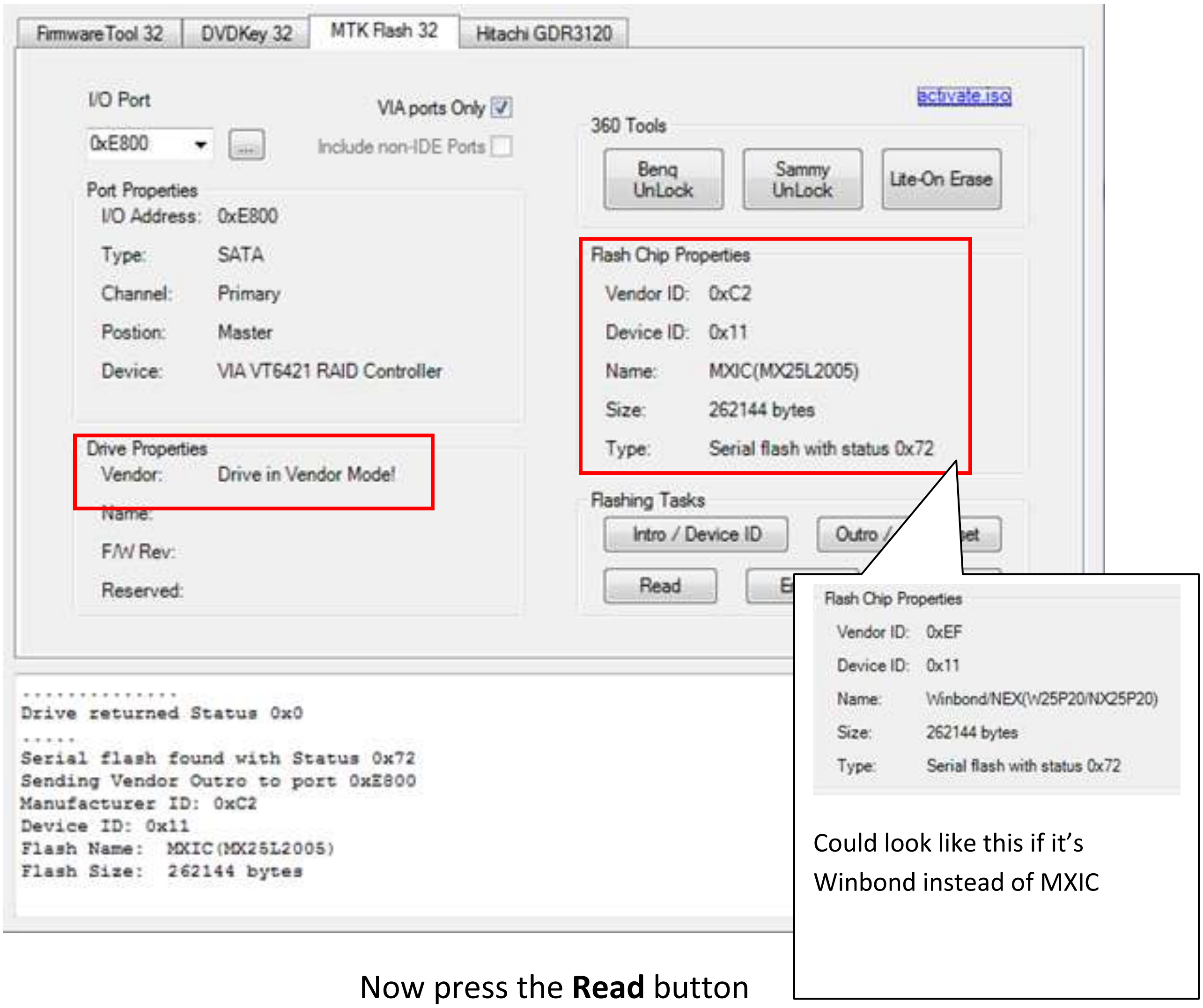
Flash Chip Properties
Vendor ID: 0xFF
Device ID: 0xFF
Name: Unknown type
Size: n/a
Type: Serial flash with status 0x72

```
Re-sending Vendor Intro:
------------------
Serial flash found with Status 0x72

Sending Device ID request to port
Manufacturer ID: 0xFF
Device ID: 0xFF
Flash Name:  Unknown type
Flash Size:  n/a
```

then press **Intro/Device ID** button again – **DO NOT POWER CYCLE!**



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



I/O Port: 0xE800

VIA ports Only ☑

Include non-IDE Ports □

Port Properties

I/O Address:	0xE800
Type:	SATA
Channel:	Primary
Postion:	Master
Device:	VIA VT6421 RAID Controller

Drive Properties

Vendor:	Drive in Vendor Mode!
Name:	
F/W Rev:	
Reserved:	

Flash Chip Properties

Vendor ID:	0xC2
Device ID:	0x11
Name:	MXIC(MX25L2005)
Size:	262144 bytes
Type:	Serial flash with status 0x72

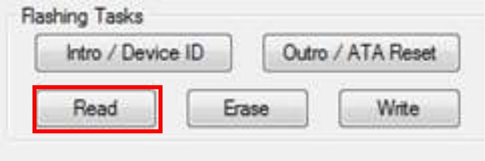
```
...............
Drive returned Status 0x0
.....
Serial flash found with Status 0x72
Sending Vendor Outro to port 0xE800
Manufacturer ID: 0xC2
Device ID: 0x11
Flash Name:  MXIC(MX25L2005)
Flash Size:  262144 bytes
```

Flash Chip Properties

Vendor ID:	0xEF
Device ID:	0x11
Name:	Winbond/NEX(W25P20/NX25P20)
Size:	262144 bytes
Type:	Serial flash with status 0x72

Could look like this if it's Winbond instead of MXIC

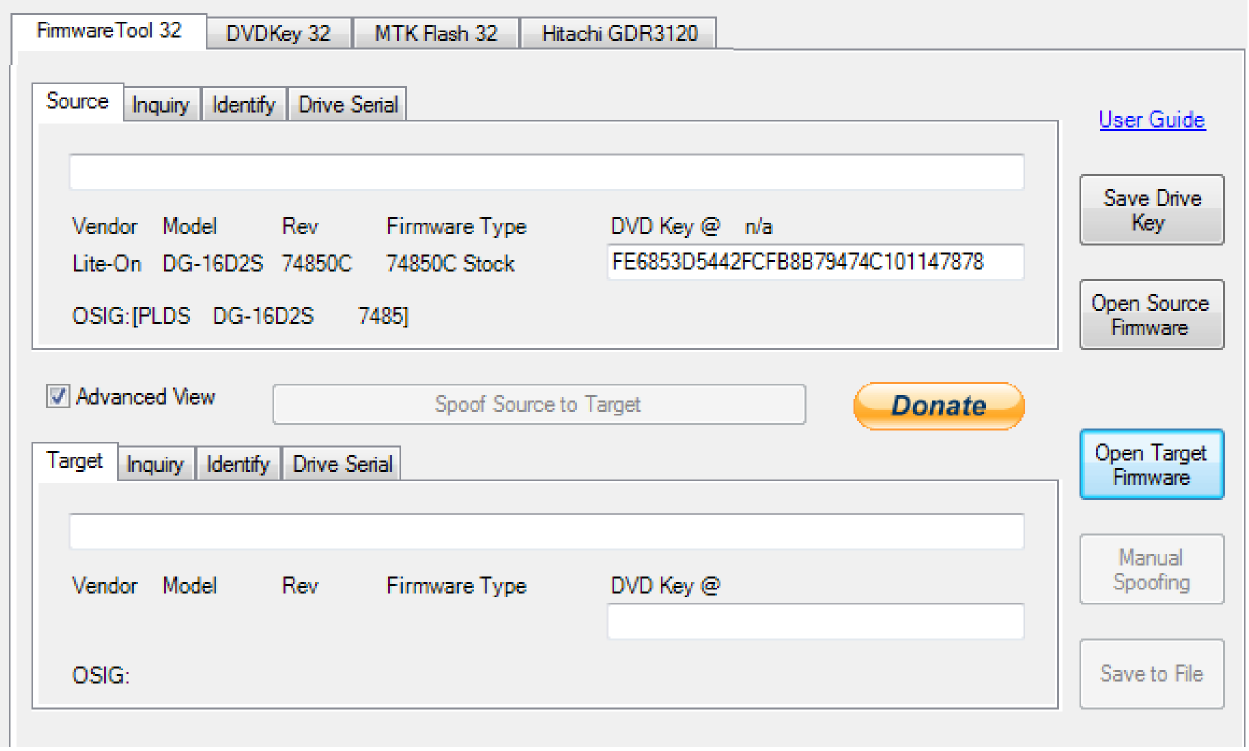
Now press the **Read** button



Jungleflasher will now Dump your Original LiteOn Firmware,

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

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



Vendor	Model	Rev	Firmware Type	DVD Key @ n/a
Lite-On	DG-16D2S	74850C	74850C Stock	FE6853D5442FCFB8B79474C101147878

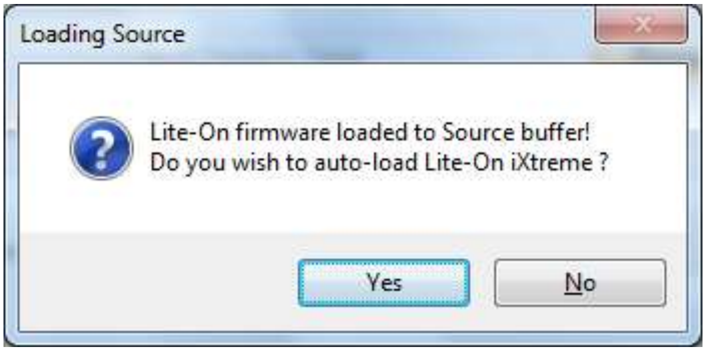
OSIG:[PLDS DG-16D2S 7485]

☑ Advanced View

Vendor	Model	Rev	Firmware Type	DVD Key @

OSIG:

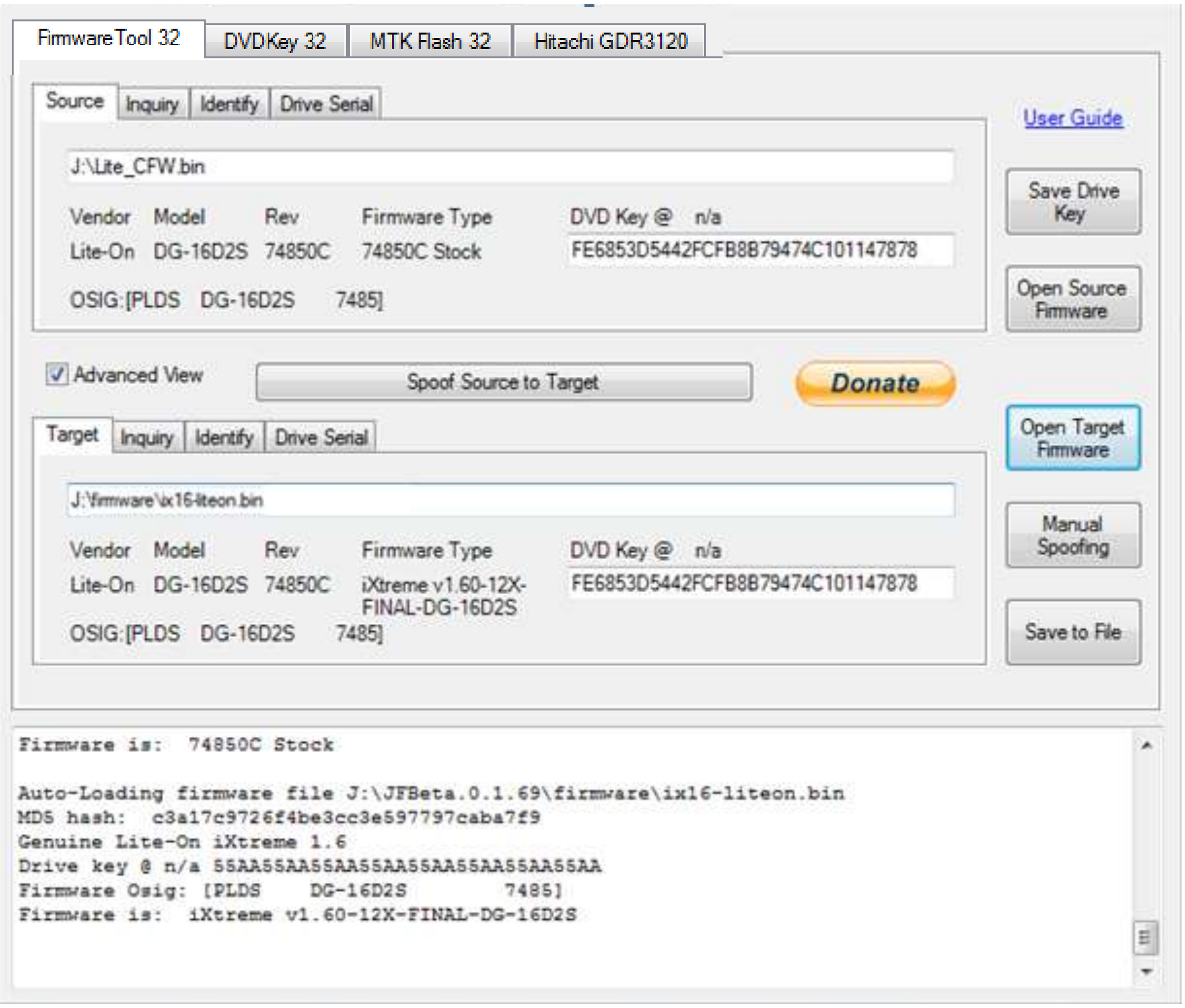
Which will be followed with a request if you wish to auto load iXtreme



Loading Source

Lite-On firmware loaded to Source buffer!
Do you wish to auto-load Lite-On iXtreme ?

Select **Yes**



J:\Lite_CFW.bin

Vendor	Model	Rev	Firmware Type	DVD Key @ n/a
Lite-On	DG-16D2S	74850C	74850C Stock	FE6853D5442FCFB8B79474C101147878

OSIG:[PLDS DG-16D2S 7485]

☑ Advanced View

J:\firmware\ix16-liteon.bin

Vendor	Model	Rev	Firmware Type	DVD Key @ n/a
Lite-On	DG-16D2S	74850C	iXtreme v1.60-12X-FINAL-DG-16D2S	FE6853D5442FCFB8B79474C101147878

OSIG:[PLDS DG-16D2S 7485]

```
Firmware is:  74850C Stock

Auto-Loading firmware file J:\JFBeta.0.1.69\firmware\ix16-liteon.bin
MD5 hash:  c3a17c9726f4be3cc3e597797caba7f9
Genuine Lite-On iXtreme 1.6
Drive key @ n/a 55AA55AA55AA55AA55AA55AA55AA55AA
Firmware Osig: [PLDS     DG-16D2S          7485]
Firmware is:  iXtreme v1.60-12X-FINAL-DG-16D2S
```

Just follow the standard write procedure!

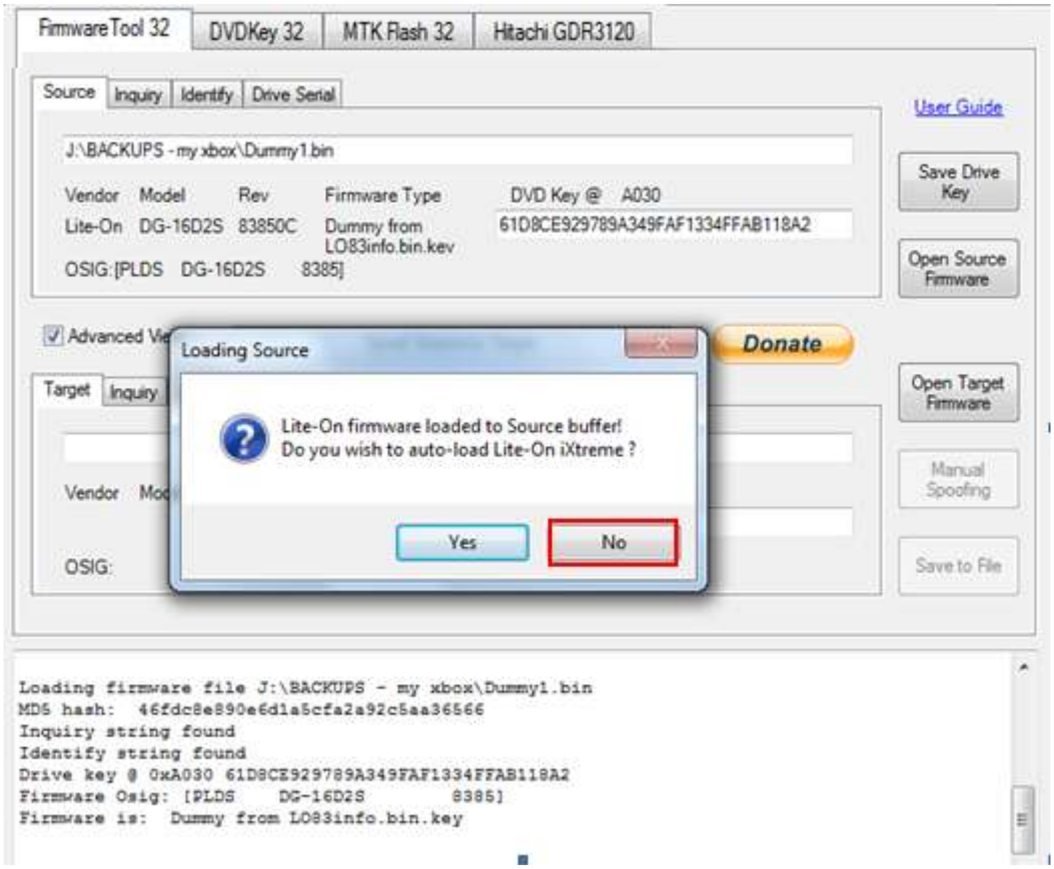
So return to **MTK** tab

NOW CLICK HERE!

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,



J:\BACKUPS - my xbox\Dummy1.bin

Vendor	Model	Rev	Firmware Type	DVD Key @ A030
Lite-On	DG-16D2S	83850C	Dummy from LO83info.bin.kev	61D8CE929789A349FAF1334FFAB118A2

OSIG: [PLDS DG-16D2S 8385]

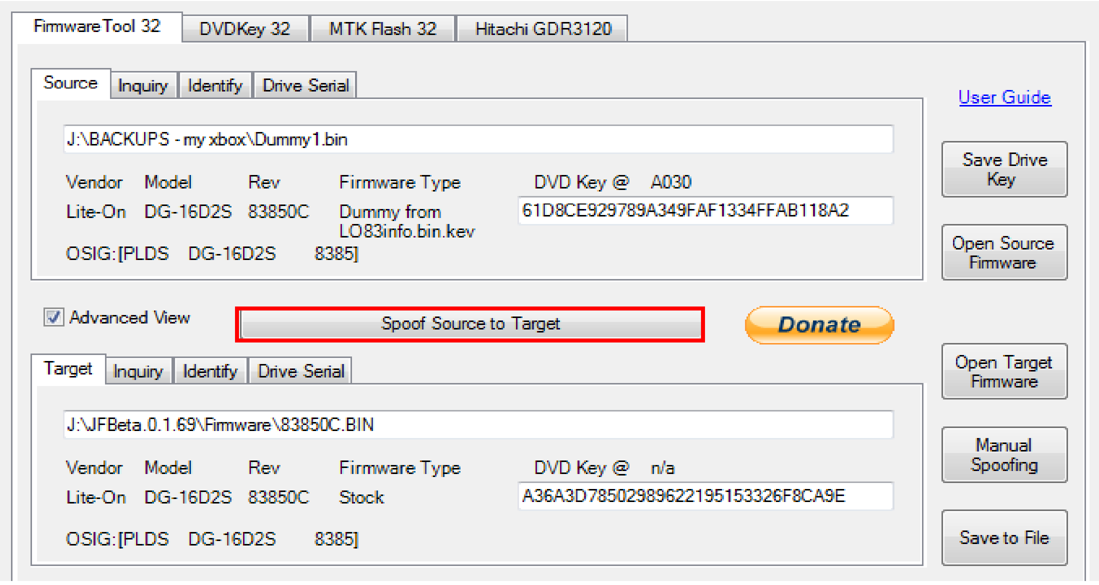
Loading Source

Lite-On firmware loaded to Source buffer!
Do you wish to auto-load Lite-On iXtreme ?

```
Loading firmware file J:\BACKUPS - my xbox\Dummy1.bin
MD5 hash:  46fdc8e890e6d1a5cfa2a92c5aa36566
Inquiry string found
Identify string found
Drive key @ 0xA030 61D8CE929789A349FAF1334FFAB118A2
Firmware Osig: [PLDS    DG-16D2S        8385]
Firmware is:  Dummy from LO83info.bin.key
```

Load the stock firmware as target!

Then press **Spoof Source to Target** button



Source: J:\BACKUPS - my xbox\Dummy1.bin

Vendor	Model	Rev	Firmware Type	DVD Key @ A030
Lite-On	DG-16D2S	83850C	Dummy from LO83info.bin.kev	61D8CE929789A349FAF1334FFAB118A2

OSIG:[PLDS DG-16D2S 8385]

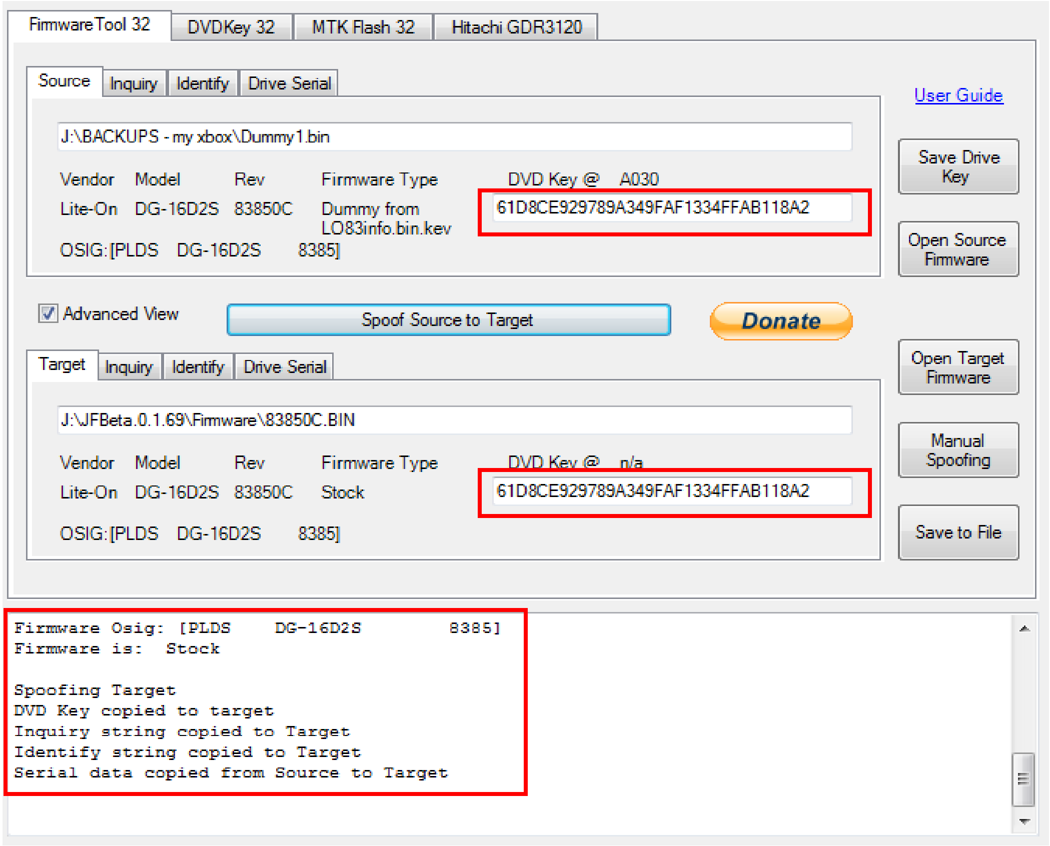
☑ Advanced View

Target: J:\JFBeta.0.1.69\Firmware\83850C.BIN

Vendor	Model	Rev	Firmware Type	DVD Key @ n/a
Lite-On	DG-16D2S	83850C	Stock	A36A3D7850298962219515332 6F8CA9E

OSIG:[PLDS DG-16D2S 8385]

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!



Source: J:\BACKUPS - my xbox\Dummy1.bin

Vendor	Model	Rev	Firmware Type	DVD Key @ A030
Lite-On	DG-16D2S	83850C	Dummy from LO83info.bin.kev	61D8CE929789A349FAF1334FFAB118A2

OSIG:[PLDS DG-16D2S 8385]

☑ Advanced View

Target: J:\JFBeta.0.1.69\Firmware\83850C.BIN

Vendor	Model	Rev	Firmware Type	DVD Key @ n/a
Lite-On	DG-16D2S	83850C	Stock	61D8CE929789A349FAF1334FFAB118A2

OSIG:[PLDS DG-16D2S 8385]

```
Firmware Osig:  [PLDS     DG-16D2S         8385]
Firmware is:  Stock

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

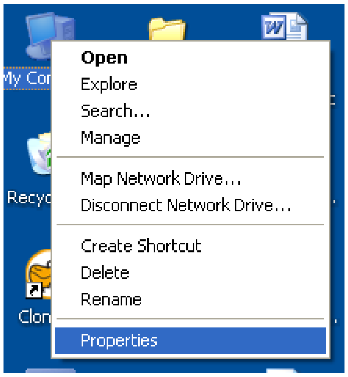
PROCEED TO ERASE & WRITE – CLICK HERE!

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

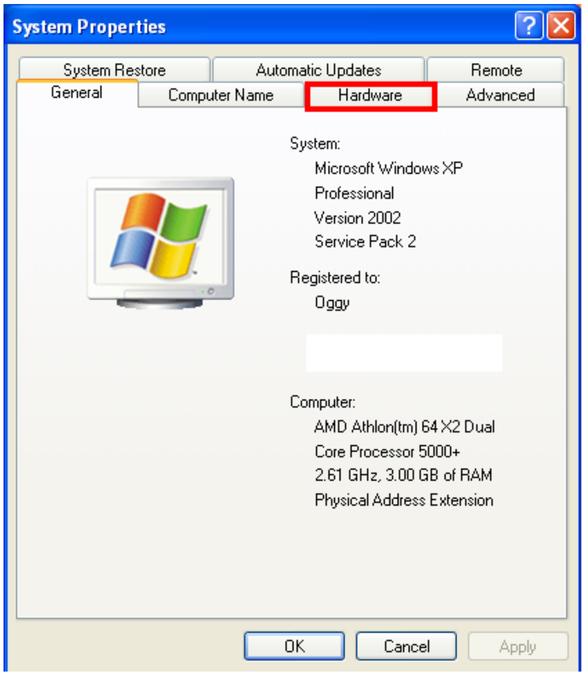
NOT TO BE DONE IF YOUR MAIN HARD DRIVE IS ON VIA SATA CARD or IF YOUR VIA CHIPSET IS ONBOARD(i.e. NOT A PCI CARD)

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

Right Click My Computer, select properties



Click the “Hardware” tab

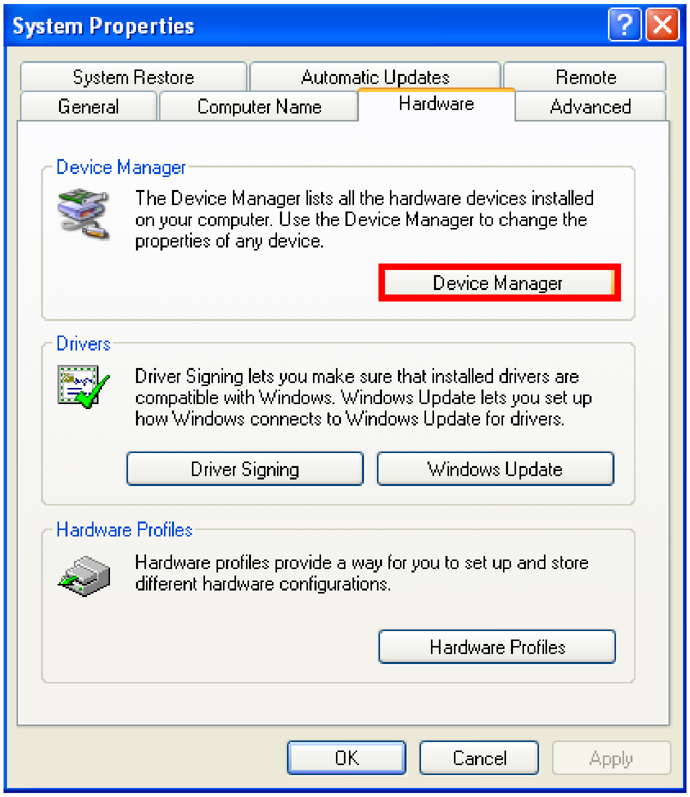


System:
Microsoft Windows XP
Professional
Version 2002
Service Pack 2

Registered to:
Oggy

Computer:
AMD Athlon(tm) 64 X2 Dual
Core Processor 5000+
2.61 GHz, 3.00 GB of RAM
Physical Address Extension

Then, click “Device Manager”

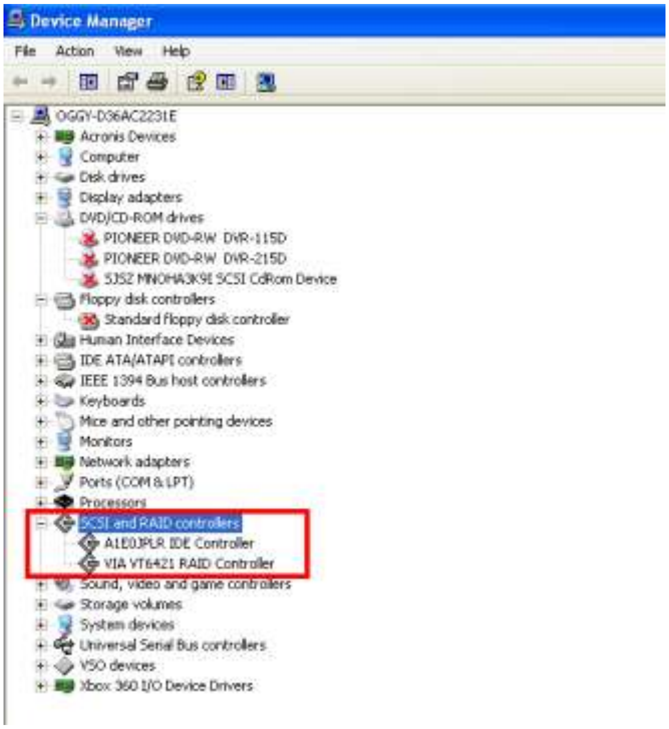


The Device Manager lists all the hardware devices installed on your computer. Use the Device Manager to change the properties of any device.

Driver Signing lets you make sure that installed drivers are compatible with Windows. Windows Update lets you set up how Windows connects to Windows Update for drivers.

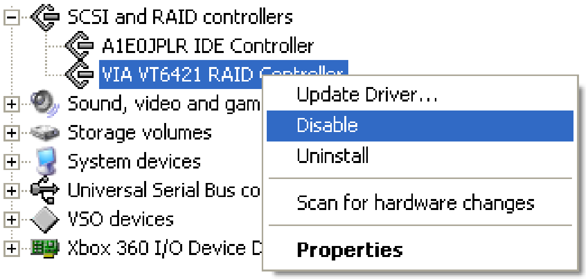
Hardware profiles provide a way for you to set up and store different hardware configurations.

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

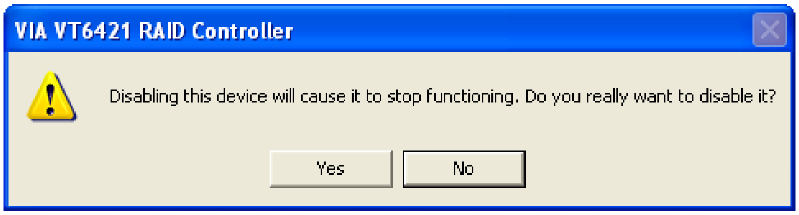


```
OGGY-D36AC2231E
    Acronis Devices
    Computer
    Disk drives
    Display adapters
    DVD/CD-ROM drives
        PIONEER DVD-RW  DVR-115D
        PIONEER DVD-RW  DVR-215D
        5J52 MNOHA3K9E SCSI CdRom Device
    Floppy disk controllers
        Standard floppy disk controller
    Human Interface Devices
    IDE ATA/ATAPI controllers
    IEEE 1394 Bus host controllers
    Keyboards
    Mice and other pointing devices
    Monitors
    Network adapters
    Ports (COM & LPT)
    Processors
    SCSI and RAID controllers
        A1E0JPLR IDE Controller
        VIA VT6421 RAID Controller
    Sound, video and game controllers
    Storage volumes
    System devices
    Universal Serial Bus controllers
    VSO devices
    Xbox 360 I/O Device Drivers
```

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

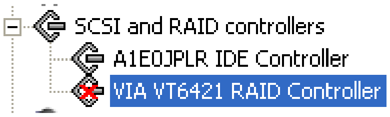


Acknowledge the warning by clicking **Yes**


VIA VT6421 RAID Controller

Disabling this device will cause it to stop functioning. Do you really want to disable it?

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** –

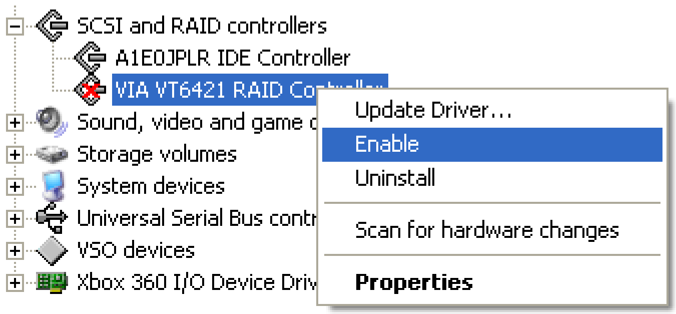
Depending on your motherboard and OS

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

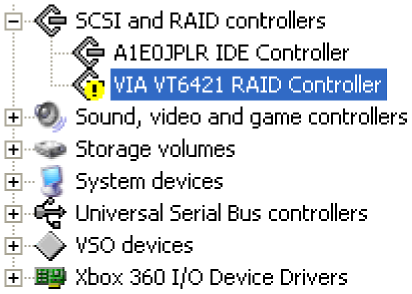
Once found, delete this file.

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

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



It should now show as the image below


SCSI and RAID controllers
A1E0JPLR IDE Controller
VIA VT6421 RAID Controller
Sound, video and game controllers
Storage volumes
System devices
Universal Serial Bus controllers
VSO devices
Xbox 360 I/O Device Drivers

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

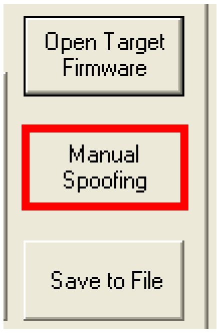
Hopefully the excellent key, OSIG and serial spoofing of FirmwareTool32 should satisfy your needs, but sometimes you need the manual method for whatever reason.

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 Firmware as a DIFFERENT DRIVE

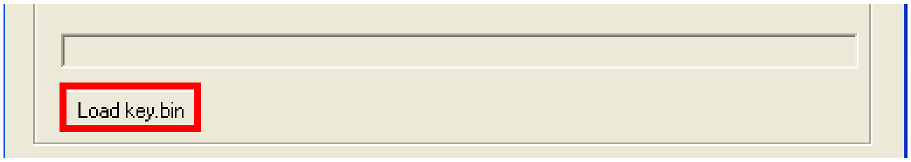
Once loaded, Click **Manual Spoofing**



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.

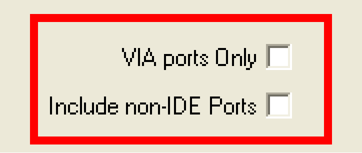
D608CG82690600G2W___

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

CLICK HERE TO RETURN

VIA Ports only & Include Non IDE ports

Found under **DVDKey32** tab,



VIA ports Only □

Include non-IDE Ports □

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**

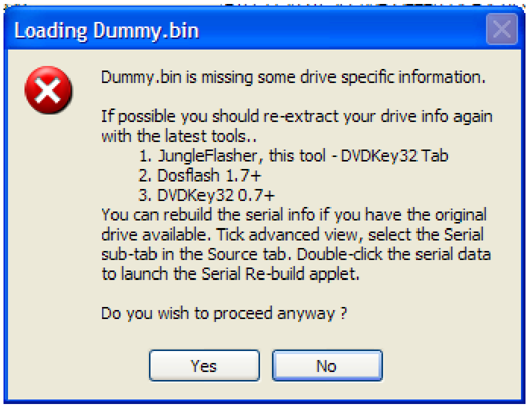
Include non-IDE Ports

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:



Loading Dummy.bin

Dummy.bin is missing some drive specific information.

If possible you should re-extract your drive info again with the latest tools..

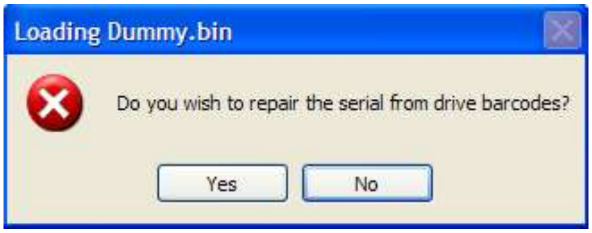
1. JungleFlasher, this tool - DVDKey32 Tab
2. Dosflash 1.7+
3. DVDKey32 0.7+

You can rebuild the serial info if you have the original drive available. Tick advanced view, select the Serial sub-tab in the Source tab. Double-click the serial data to launch the Serial Re-build applet.

Do you wish to proceed anyway ?

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).

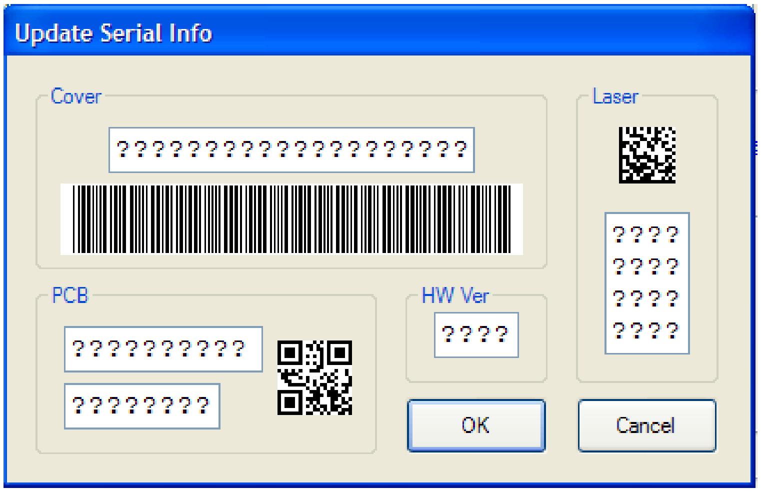


Loading Dummy.bin

Do you wish to repair the serial from drive barcodes?

Click yes to rebuild data.

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



Update Serial Info

Cover: ???????????????????

Laser: ????
????
????
????

PCB: ??????????
????????

HW Ver: ????

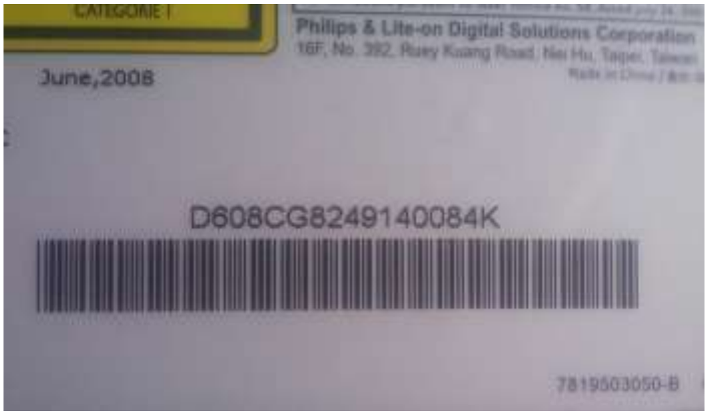
To rebuild the **Serial Data** you must copy the information from the **physical drive itself**, into the boxes in the applet shown.

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

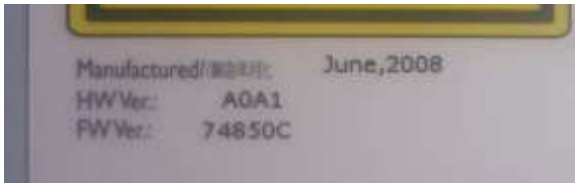
Located on the top of the drive, and 17 Characters long


CATEGORIE I
Philips & Lite-on Digital Solutions Corporation
16F, No. 392, Ruey Kuang Road, Nei Hu, Taipei, Taiwan
June,2008
D608CG8249140084K
7819503050-B

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

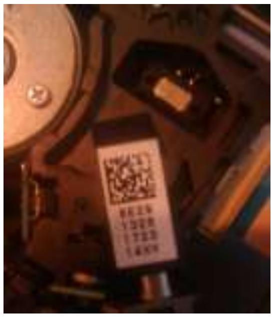


Manufactured/ June,2008
HW Ver.: A0A1
FW Ver.: 74850C

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

3. The Laser

Self explanitory, located on the base of the laser.

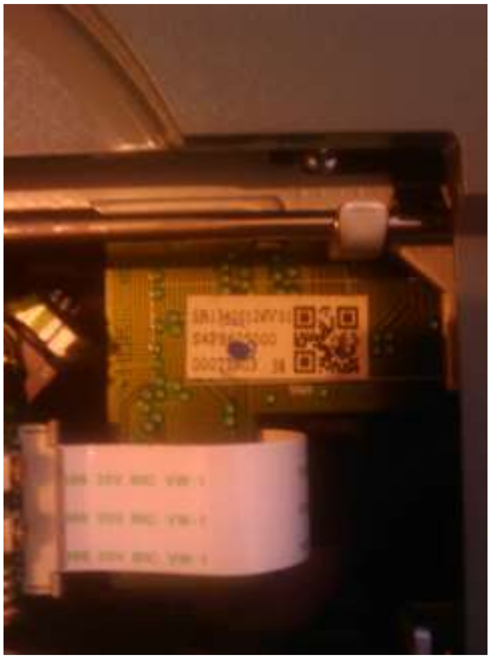


Insert this into the **Laser** area of the **Serial Rebuilder**

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!

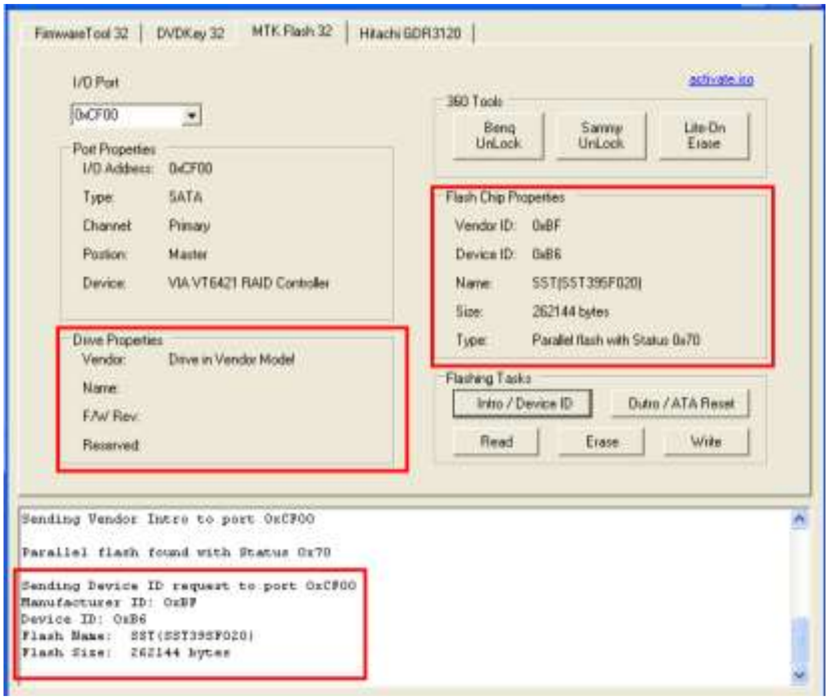
for LiteOn a Dummy.bin
for Samsung a Sam-OFW.bin
for Benq a Ben-OFW.bin
for hitachi a Hit-OFW.bin

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!



I/O Port: 0xCF00

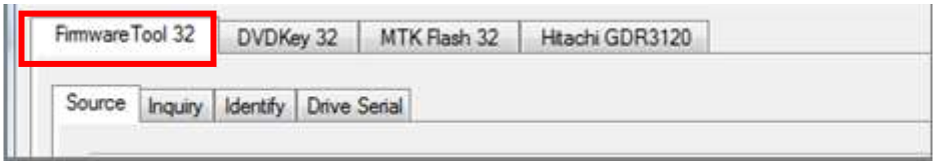
Port Properties
I/O Address: 0xCF00
Type: SATA
Channel: Primary
Position: Master
Device: VIA VT6421 RAID Controller

Drive Properties
Vendor: Drive in Vendor Mode!
Name:
F/W Rev:
Reserved:

Flash Chip Properties
Vendor ID: 0xBF
Device ID: 0xB6
Name: SST(SST39SF020)
Size: 262144 bytes
Type: Parallel flash with Status 0x70

```
Sending Vendor Intro to port 0xCF00

Parallel flash found with Status 0x70

Sending Device ID request to port 0xCF00
Manufacturer ID: 0xBF
Device ID: 0xB6
Flash Name:  SST(SST39SF020)
Flash Size:  262144 bytes
```

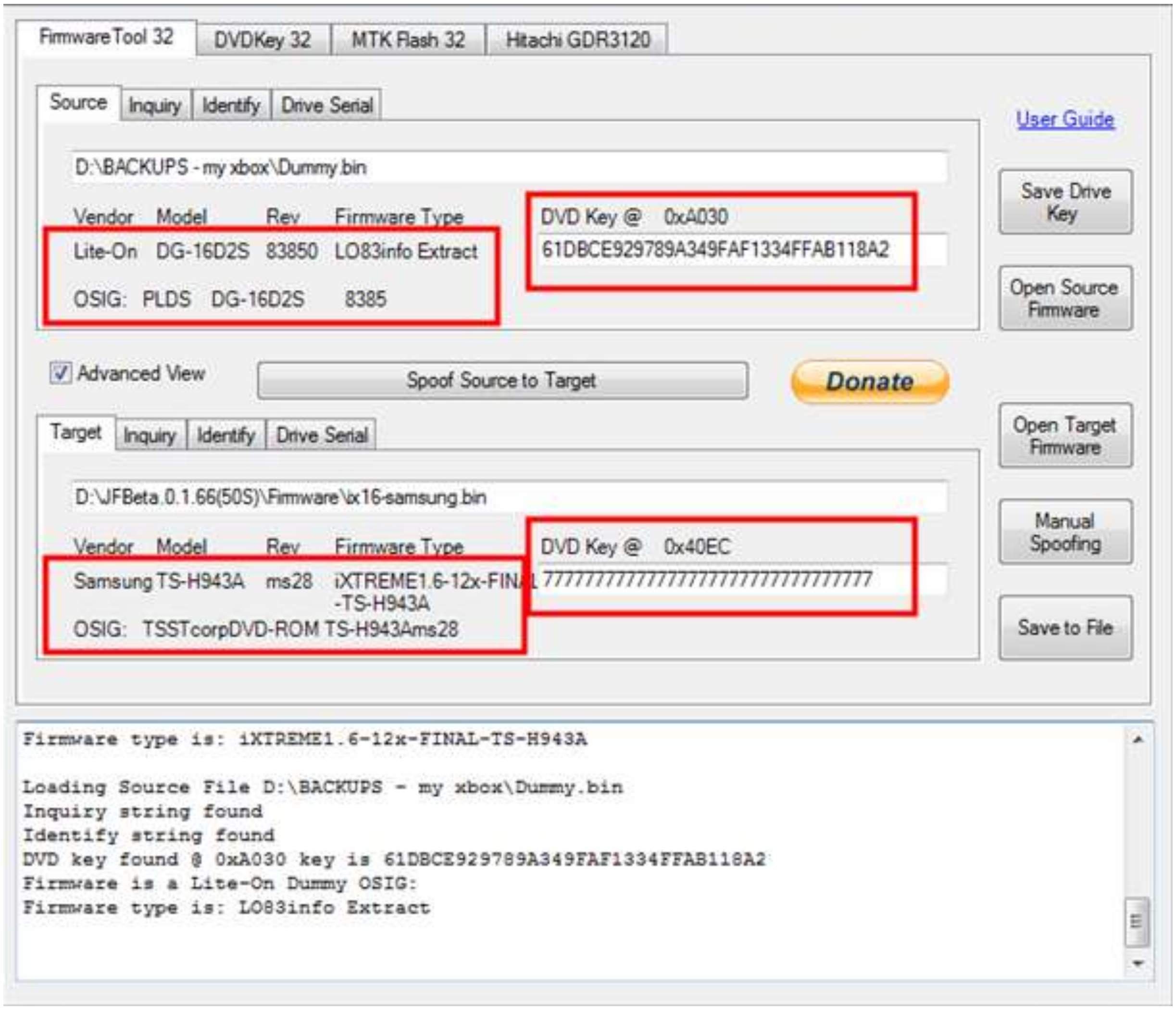
Now go to **firmwaretool 32** tab



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)



Source: D:\BACKUPS - my xbox\Dummy.bin

Vendor	Model	Rev	Firmware Type
Lite-On	DG-16D2S	83850	LO83info Extract

OSIG: PLDS DG-16D2S 8385

DVD Key @ 0xA030
61DBCE929789A349FAF1334FFAB118A2

☑ Advanced View

Target: D:\JFBeta.0.1.66(50S)\Firmware\ix16-samsung.bin

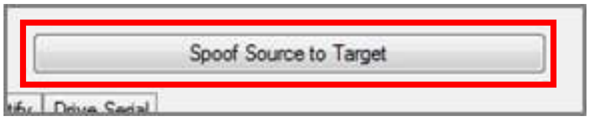
Vendor	Model	Rev	Firmware Type
Samsung	TS-H943A	ms28	iXTREME1.6-12x-FINAL-TS-H943A

OSIG: TSSTcorpDVD-ROM TS-H943Ams28

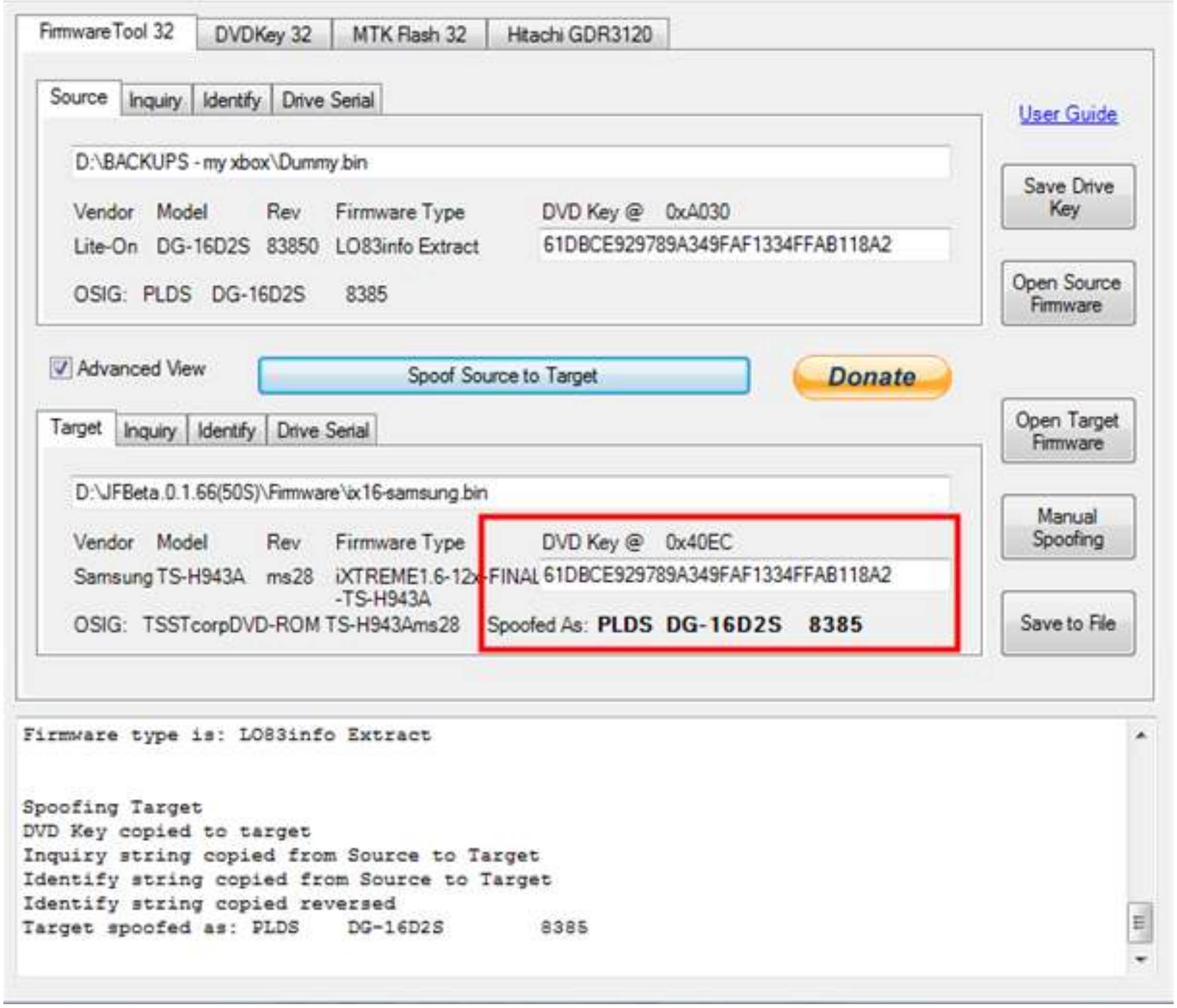
DVD Key @ 0x40EC
77777777777777777777777777777777

```
Firmware type is: iXTREME1.6-12x-FINAL-TS-H943A

Loading Source File D:\BACKUPS - my xbox\Dummy.bin
Inquiry string found
Identify string found
DVD key found @ 0xA030 key is 61DBCE929789A349FAF1334FFAB118A2
Firmware is a Lite-On Dummy OSIG:
Firmware type is: LO83info Extract
```

Now click **Spoof Source to Target**!



Notice the difference in the target firmware now!



D:\BACKUPS - my xbox\Dummy.bin

Vendor	Model	Rev	Firmware Type	DVD Key @ 0xA030
Lite-On	DG-16D2S	83850	LO83info Extract	61DBCE929789A349FAF1334FFAB118A2

OSIG: PLDS DG-16D2S 8385

D:\JFBeta.0.1.66(50S)\Firmware\ix16-samsung.bin

Vendor	Model	Rev	Firmware Type	DVD Key @ 0x40EC
Samsung	TS-H943A	ms28	iXTREME1.6-12x-FINAL-TS-H943A	61DBCE929789A349FAF1334FFAB118A2

OSIG: TSSTcorpDVD-ROM TS-H943Ams28 Spoofed As: **PLDS DG-16D2S 8385**

```
Firmware type is: LO83info Extract


Spoofing Target
DVD Key copied to target
Inquiry string copied from Source to Target
Identify string copied from Source to Target
Identify string copied reversed
Target spoofed as: PLDS    DG-16D2S        8385
```

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

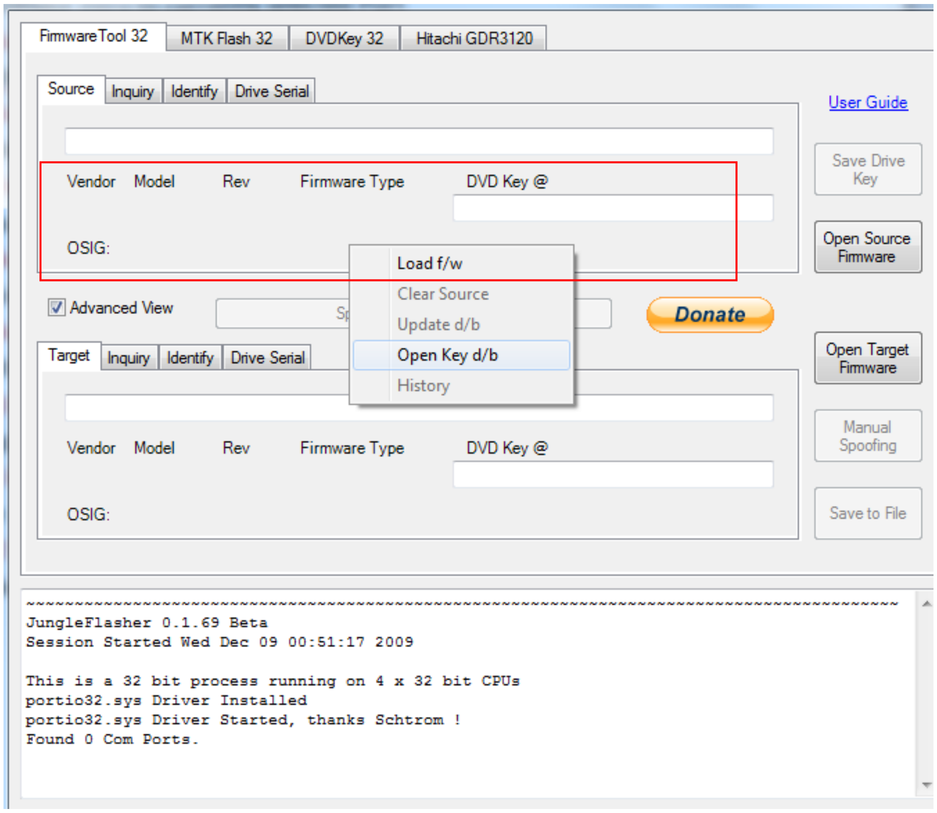
To create .csv from key database

Ctrl + F12 key

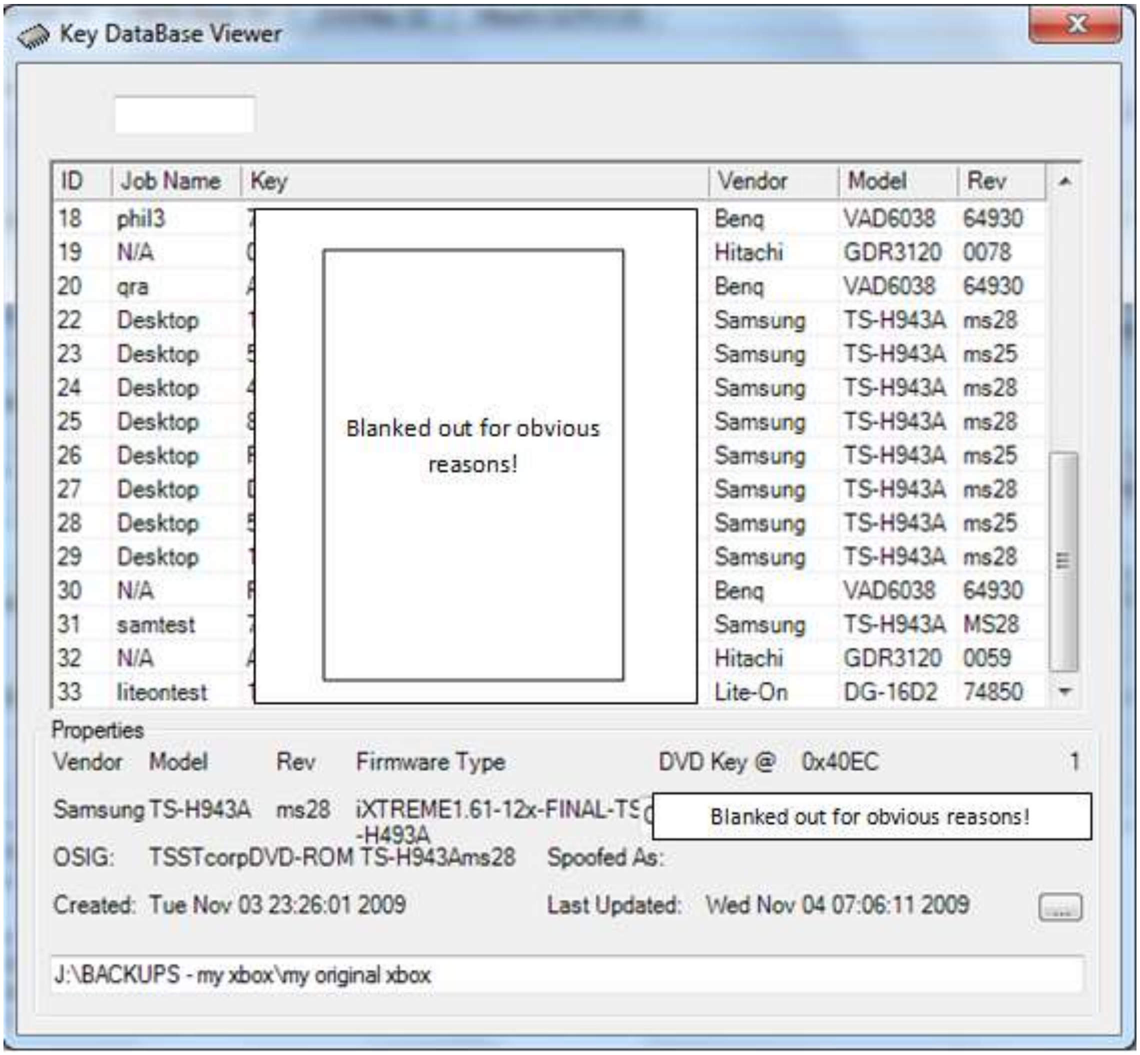
To open key database in Notepad

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.**



```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
JungleFlasher 0.1.69 Beta
Session Started Wed Dec 09 00:51:17 2009

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.
```



Key DataBase Viewer

ID	Job Name	Key	Vendor	Model	Rev
18	phil3		Benq	VAD6038	64930
19	N/A		Hitachi	GDR3120	0078
20	qra		Benq	VAD6038	64930
22	Desktop		Samsung	TS-H943A	ms28
23	Desktop		Samsung	TS-H943A	ms25
24	Desktop		Samsung	TS-H943A	ms28
25	Desktop		Samsung	TS-H943A	ms28
26	Desktop		Samsung	TS-H943A	ms25
27	Desktop		Samsung	TS-H943A	ms28
28	Desktop		Samsung	TS-H943A	ms25
29	Desktop		Samsung	TS-H943A	ms28
30	N/A		Benq	VAD6038	64930
31	samtest		Samsung	TS-H943A	MS28
32	N/A		Hitachi	GDR3120	0059
33	liteontest		Lite-On	DG-16D2	74850

Blanked out for obvious reasons!

Properties

Vendor Model Rev Firmware Type DVD Key @ 0x40EC 1

Samsung TS-H943A ms28 iXTREME1.61-12x-FINAL-TS -H493A

Blanked out for obvious reasons!

OSIG: TSSTcorpDVD-ROM TS-H943Ams28 Spoofed As:

Created: Tue Nov 03 23:26:01 2009 Last Updated: Wed Nov 04 07:06:11 2009

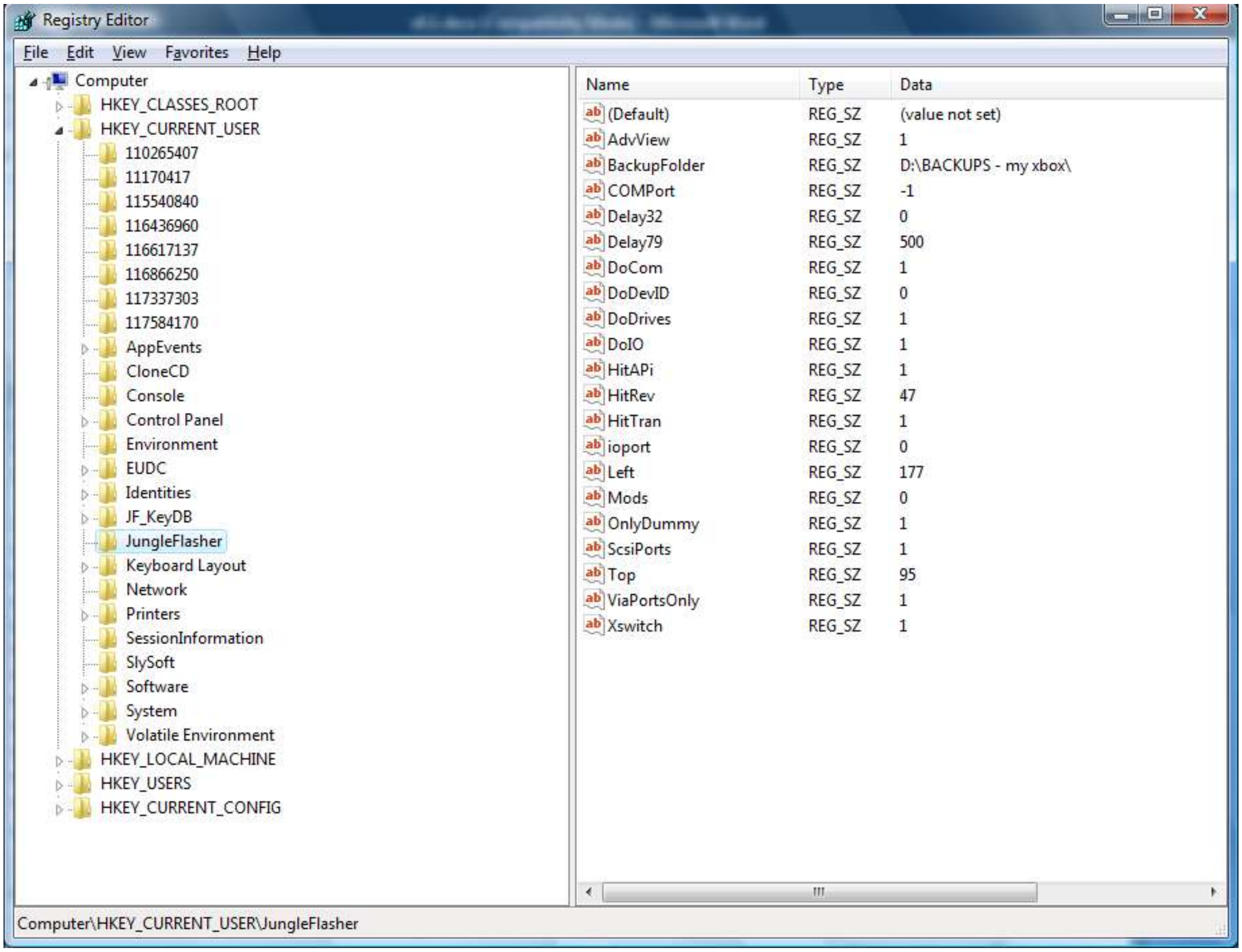
J:\BACKUPS - my xbox\my original xbox

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:



Computer
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
  - 110265407
  - 11170417
  - 115540840
  - 116436960
  - 116617137
  - 116866250
  - 117337303
  - 117584170
  - AppEvents
  - CloneCD
  - Console
  - Control Panel
  - Environment
  - EUDC
  - Identities
  - JF_KeyDB
  - JungleFlasher
  - Keyboard Layout
  - Network
  - Printers
  - SessionInformation
  - SlySoft
  - Software
  - System
  - Volatile Environment
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

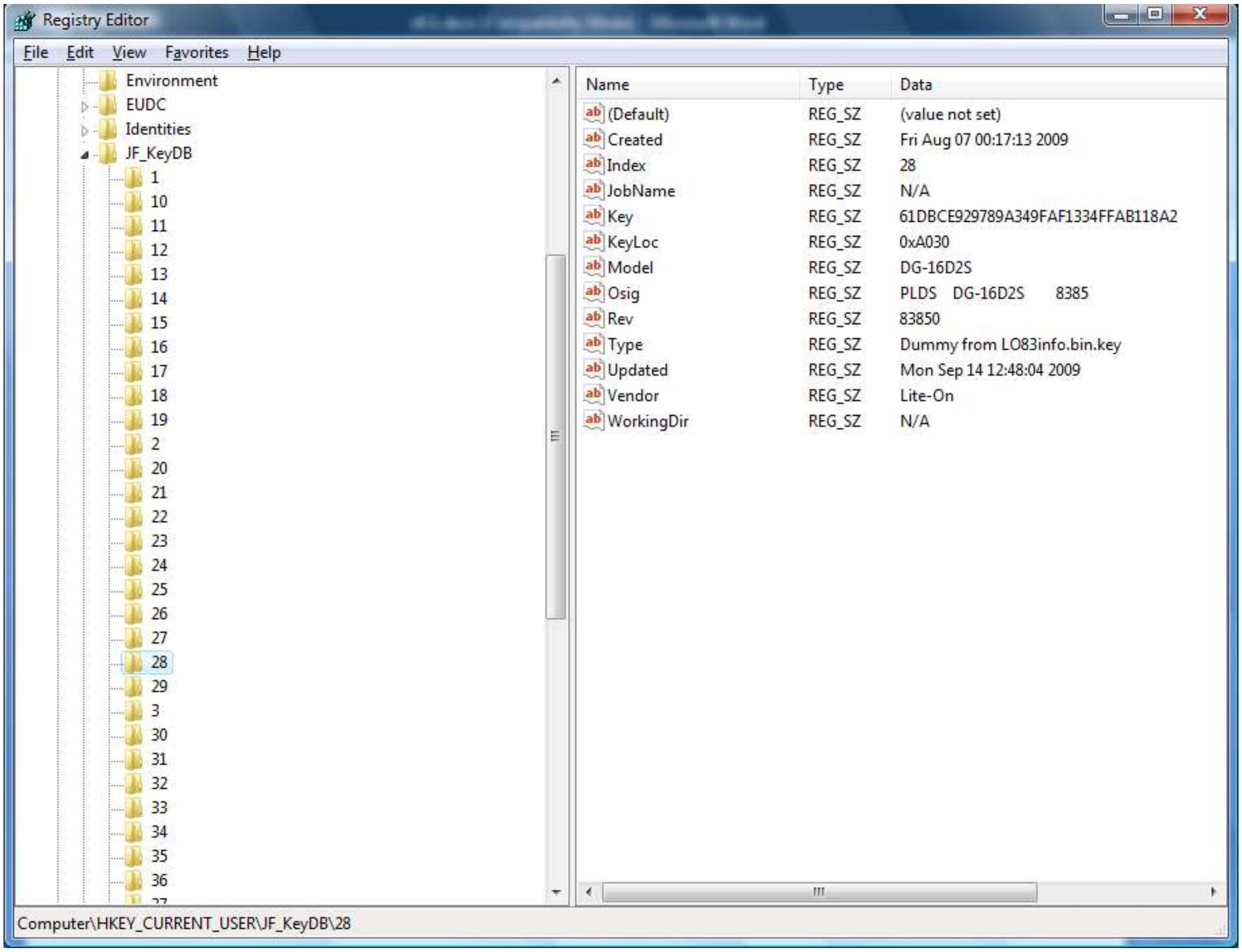
Name	Type	Data
(Default)	REG_SZ	(value not set)
AdvView	REG_SZ	1
BackupFolder	REG_SZ	D:\BACKUPS - my xbox\
COMPort	REG_SZ	-1
Delay32	REG_SZ	0
Delay79	REG_SZ	500
DoCom	REG_SZ	1
DoDevID	REG_SZ	0
DoDrives	REG_SZ	1
DoIO	REG_SZ	1
HitAPi	REG_SZ	1
HitRev	REG_SZ	47
HitTran	REG_SZ	1
ioport	REG_SZ	0
Left	REG_SZ	177
Mods	REG_SZ	0
OnlyDummy	REG_SZ	1
ScsiPorts	REG_SZ	1
Top	REG_SZ	95
ViaPortsOnly	REG_SZ	1
Xswitch	REG_SZ	1

Computer\HKEY_CURRENT_USER\JungleFlasher

- **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)
- **Delay79 –** a set time delay used in the 79unlock command (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
- **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
- **Xswitch –** Remembers if USBxtractor switch is enabled

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

In the same area of registry is a a folder called **JF_KeyDB** which if selected looks something like this!



Name	Type	Data
(Default)	REG_SZ	(value not set)
Created	REG_SZ	Fri Aug 07 00:17:13 2009
Index	REG_SZ	28
JobName	REG_SZ	N/A
Key	REG_SZ	61DBCE929789A349FAF1334FFAB118A2
KeyLoc	REG_SZ	0xA030
Model	REG_SZ	DG-16D2S
Osig	REG_SZ	PLDS DG-16D2S 8385
Rev	REG_SZ	83850
Type	REG_SZ	Dummy from LO83info.bin.key
Updated	REG_SZ	Mon Sep 14 12:48:04 2009
Vendor	REG_SZ	Lite-On
WorkingDir	REG_SZ	N/A

Computer\HKEY_CURRENT_USER\JF_KeyDB\28

If you select a numbered folder it will display all the details of that particular dumped/loaded FW file. The entrys are fairly self explanitery.

CLICK HERE TO RETURN

Common problems and Frequently Asked Questions

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 doing one of these drives, simply ignore it and proceed.

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

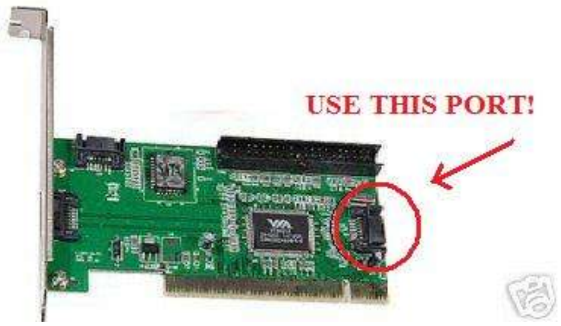
There are multiple causes to this, so first of all ensure **VIA Ports Only** is unchecked and **Non-IDE** is checked under the **DVDKey32 Tab.**

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.

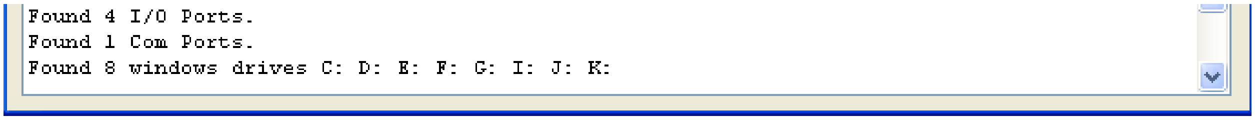
If using a VIA card ensure you use the correct port

If problems persist, please join us in the support channel HERE

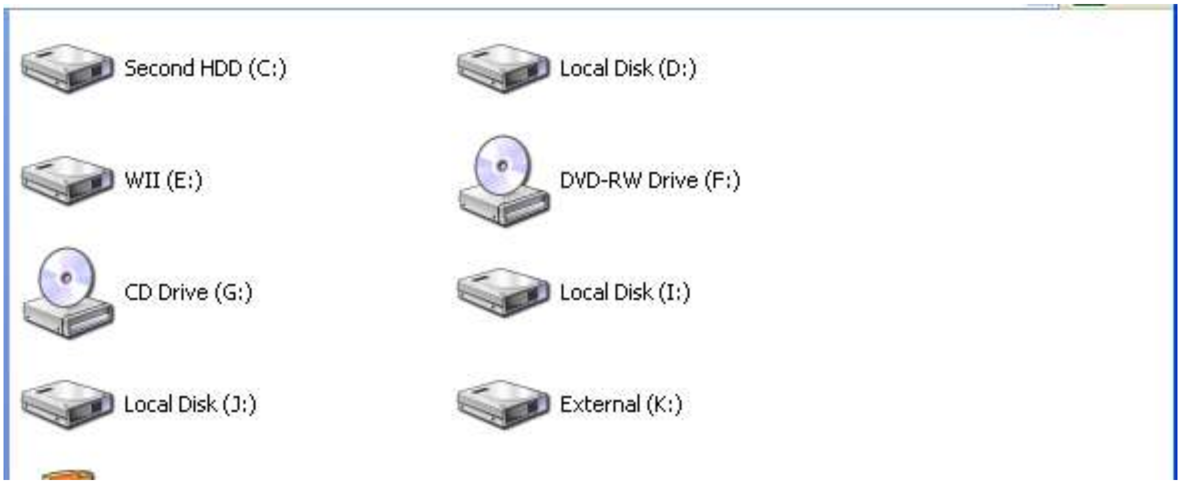


JungleFlasher doesn’t see my DVD Drive (cont)

Quite a few users believe JungleFlasher will report their Xbox 360 DVD Drive being Present in the Running Log:



```
Found 4 I/O Ports.
Found 1 Com Ports.
Found 8 windows drives C: D: E: F: G: I: J: K:
```



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

Is it definitely a **74850c** version? The **83850c** 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 (ie 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.

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 these 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.

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 – causing an error!

I downloaded the Liteon FW for my 74850C– I put it in the firmware folder, BUT Jungleflasher wont auto load it WHY?

If your LiteOn iXtreme firmware is called **ix16-liteon-repack.bin** – rename it **ix16-liteon.bin,** this was a mistake when they released the original ix16-liteon.bin (which was the wrong file!) hence the release of the repacked version! So renaming as above will allow the file to auto load in JungleFlasher.

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 it's key database on every dump carried out, right click on source box in **firmwaretool 32** tab. Select **Open Key d/b**. as shown HERE

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

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 v0.1.70 beta

Thanks to:

c4eva & Team Jungle (Dedication & FW)

Schtrom (Legend in his own right)

Seacrest (Openkey)

Team Modfreakz (for all you have contributed!)

MRA (☺)

&

The Testers (well, obviously for testing)

CLICK HERE TO RETURN TO STARTING POINT