JungleFlasher v0.1.66

Complete User Guide

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	USED JUNGLEFLASHER BEFORE
CLICK HERE	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.

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 for many tasks using default settings.

FirmwareTool32 is primarily used for manipulation of firmware to be applied to MTK based drives. (not Hitachi drives! – they should be dumped/flashed/spoofed etc from the Hitachi tab!)

DVDKey32 is primarily used to obtain **Key.bin, Inquiry.bin, Identify.bin and Dummy.bin** from **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.

JungleFlasher v0.165 brought the inclusion of **LO83info** for **LiteOn PLDS DG-16D2S 83850c drives.** This hack being used for obtaining the unique data from the newest drive revision found in consoles. With JungleFlasher v0.1.66b incorporating 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.

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.

MTKFlash32 will also **erase** and **write Samsung** and **BenQ** drives, once the drives have been unlocked.

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

Follow the link CLICK HERE for instructions HOW!

Other Info – for troubleshooting, or the inquisitive mind

FAQ's

Manual Spoofing

Advanced User Functions

VIA Ports Only / Include Non-IDE

Missing Serial Data

Installing PortIO32

Spoofing a different drive

Spoofing a Hitachi

Support for earlier LiteOn dumps

Thanks

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	BenQ	Hitachi	LiteOn
CLICK HERE	CLICK HERE	CLICK HERE	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.

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?

Is The Firmware on drive STOCK?

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 onwards

[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 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.

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.**

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.

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!"**

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.**

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

Now CLICK HERE to proceed

Unlocking iXtreme 1.5 onwards

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.

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

Now CLICK HERE to proceed

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.**

JungleFlasher will prompt you with instructions.

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

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

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

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

Now CLICK HERE to proceed

If it didn't work – read on

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.**

JungleFlasher will prompt you with instructions.

Now power **off** the drive!

Then click **YES,**

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

When **……** Are appearing, <mark>power **ON** the drive!</mark>

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

Now CLICK HERE to proceed

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:

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

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

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

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

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

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.

Then, click **Write.**

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

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

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


```
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,

Now send OUTRO to the drive

Will look like this – unless it's a ms25 (self explanitory)

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 onwards

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+.

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!**".

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 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 diff properties

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.**

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 (inc iXtreme 1.5+).

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 diff properties

JungleFlasher will prompt you with instructions.

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

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

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

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

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.**

JungleFlasher will prompt you with instructions.

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

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

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

<mark>While **…….** are appearing,</mark>

<mark>turn **ON** the power to the drive</mark>

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!".**

Reading the Firmware from the drive.

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

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

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

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

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.

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

Writing Firmware to the drive.

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

Verfify you have good flash chip properties still.

Then, click **Write.**

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).

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.

Which drive properties you have depends on BenQ FW version!

Power off – connect back to console and test!

CLICK HERE TO RETURN TO START OF TUTORIAL

Hitachi GDR-3120L.

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

Overview.

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

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

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

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

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

VIA users with no drivers, must utilise the PortIO option

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

(you must have drivers correctly removed!)

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

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

Drive in Mode-B with stock FW

79

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

Pre – 78

78

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

Setting ModeB

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

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

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

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

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**

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

If not, click **Refresh List**

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

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

BACK TO FLOWCHART!

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**.

.

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

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

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

Click **Have Disk**

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

Select it and click Open. Then click OK

Now click next and the Driver should install.

Click finish and Return to Device manager.

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

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

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

CLICK TO RETURN TO HITACHI FLOWCHART

Dumping the Firmware from the drive (Pre v78)

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

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

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

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

Then, click **Read to Source**

You should see something similar to below

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

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

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

FLASH iX FIRMWARE - CLICK HERE

UNLOCKING v79

FIRST Ensure ModeB is set

V79 ONLY

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

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

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

JungleFlasher should display a log similar to the one below.

```
Found 7 windows drives.
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!
```

The Drive is now unlocked!

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

V78 / V79

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

So, click **Read to Source**

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.

Once saved, it will open it as **Source** in **FirmwareTool32.**

Vendor	Model	Rev	Firmware Type	DVD Key @ 0x4D20 0xAC7F040C
Hitachi	GDR3120L	0079	Stock	26DF74D5AB71E43323D83BCDDB7339B8

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:

So, onto flashing iXtreme

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

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

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

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.

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 unless using flash keys).into iXtreme, and flashed a test sector for stability.

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

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

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

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

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

Then, click **Restore to Stock**

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

Click **Yes** to proceed

Again, JungleFlasher will take control and flash the sectors required

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

Clicking Ok will fix Checksum for you

Check Log for confirmation

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. Flash Key Sector

4. Flash Spoof Data

WARNING – YOU MUST

Flash iXtreme to the drive first before flashing key, Then flashing ID Strings spoof data!!

Flashing Key Sector (90004000)

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 **Flash Key Sector**

Then, click **Flash Keys**

JungleFlasher will then automatically read the drive and prompt you to save it, it is advised that you do!

Upon saving, JungleFlasher will present you with a Spoof section; note that only the key area is accessible, this is to prevent you spoofing before flashing Keys.

Here, you can manually load a Key.bin from a previous dump, (**Key.bin can be saved** by loading donor drives firmware in FirmwareTool32 as Source and Clicking **Save Drive Key.**)

You can also manually type it in, but it is advisable that you allow the software do it as typing errors could result in a bad key.

Simply click **Load key.bin** and navigate to your desired Key.bin and click **Open**

Verify key is the one you required and looks unique, then, click OK

Just like Restore/Flash iXtreme, **JungleFlasher** will flash a test sector and ask if you want to proceed.

Click **Yes** to Proceed

JungleFlasher will then Flash **Key Sector** (Sector 90004000)

Once written it will re-dump Key Sector and verify it has new key set.

```
Repairing Test Sector.
Flashing Sector 9003F000
Done !
Flashing Sector 90004000
Done !
Write verify test..
Dumping Flash:....
Read back & compare, complete, Write Verified!
Flash Keys Complete !
```

Flashing Spoof Data / Drive String ID (OSIG)

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 and correct Key prior to spoofing!

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 **Flash Spoof Data**

Then, click **Flash ID's**

JungleFlasher will then automatically read the drive and prompt you to save it, it's advised that you do!

Upon saving, JungleFlasher will present you with a Spoof section; note that only the **OSIG (Drive String ID)** area is accessible.

Select the Drive Type / OSIG that you want the Hitachi to report as to the console from the drop down box.

If choosing to spoof to any other drive **apart from Lite-On PLDS DG-16D2S,** upon selecting **Spoofed OSIG**, simply click ok to Proceed.

If spoofing as a **Lite-On PLDS DG-16D2S,** upon selecting **Spoofed OSIG** JungleFlasher will enable the **Lite-On Barcode Section**

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

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

You can manually type this in the box and click **Check**

This will enable the Ok Button, Click it to Proceed

Upon clicking **OK** JungleFlasher will Flash a test sector and ask if you wish to Proceed

Click **Yes** to Proceed

JungleFlasher will then Flash **Drive String ID Sector** (Sector 9003D000)

Once written it will re-dump Drive String ID Sector and verify it has been changed.

```
Repairing Test Sector.
Flashing Sector 9003F000
Done !
Flashing Sector 9003D000
Done !
Write verify test..
Dumping Flash:...........
Read back & compare, complete, Write Verified!
Flash ID Strings Complete !
```

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

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

Lite-On PLDS DG-16D2S

Firmware versions 74850C & 83850C

Overview

With the release of the 83850C firmware , LiteOn drives now require two totally different methods for each drive. The older 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) which once extracted are used to create the dummy.bin

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

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

The LiteOns are unique in the way they are handled as they never produce an Original Firmware file from a dump! – SO - once you have flashed a LiteOn, You Cannot put Original Firmware back on it!

LiteOn PLDS DG-16D2S

Which FW Revision?

(read the label on drive lid)

74850C

(requires extra HW if stock)

83850C

(SATA only)

Stock Firmware?

Stock Firmware?

No

Yes

CLICK HERE

Yes

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

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!

<div style="border: 2px solid purple; padding: 10px;">

A FRESH extraction is <u>recommended</u> where possible – but the option remains available

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

For 83850C File (*unique*.bin.key) – <u>Click Here!</u>

</div>

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 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

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 4 files (Key, Inquiry, Identify **and** dummy.bin) as dummy.bin contains all the information of the other 3 files.

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

Save as prompted,

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.

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 4 files (Key, Inquiry, Identify **and** dummy.bin). **USB Xtractor** user should enable **USB Xtractor Switch** check box (shown in blue)

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**.**

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

then prompt you to save **key.bin, inquiry.bin, identify.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.

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.

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.

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 other drives – Click Here!

Spoofing Hitachi – Click Here!

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 and click **Lite-On Erase.**

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.

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

JungleFlasher will present you with another warning.

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.**

Drive is now in Vendor Mode (0x72).

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

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

Different properties when flashing an 83850C

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

Name:

Size:

Type:

Drive Properties
Vendor: PLDS
Name: DG-16D2S
F/W Rev: 7485
Reserved: 0CA0A1D608CG84391400

Flashing Tasks
[Intro / Device ID]   [Outro / ATA Reset]
[Read]   [Erase]   [Write]

```
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!

COMPLETE – CLICK HERE TO RETURN TO START OF TUTORIAL

LiteOn "83850c" Extraction

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

The 83850C Firmware drives <u>DO NOT</u> require the additional Hardware that the 74850C Firmware drives do –

83850C 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 v0.1.66b or above

JungleFlasher 0.1.66 b

For Support join #JungleFlasher on EFnet

Select **DVDKey32 Tab**

Check to see the 83850c Inquires on the port.

Select **LO83info**

You will see this message:

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**

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

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.**.**

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

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

Jungleflasher will now prompt you to save!

Save this file.

Note: I only save dummy.bin as I have dummy.bin only enabled in the DVDKey32 Tab, JungleFlasher *may* prompt you to save Inquiry.bin 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)

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

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

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

CLICK HERE TO CONTINUE TO ERASE/WRITE SECTION

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

Then, click "Device Manager"

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

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

Acknowledge the warning by clicking **Yes**

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

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

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

Depending on your motherboard and OS

For XP normally called **viamraid.sys**
For Vista/Win 7 normally called **vsmraid.sys**

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

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

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

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

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

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

Include non-IDE Ports

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

CLICK HERE TO RETURN

LiteOn 'Serial Fixer'

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

To fix proceed, click Yes.

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

Click yes to rebuild data.

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

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

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. <u>The Drive chassis / Shell</u>

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

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

2. <u>Hardware Revision</u>

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

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

3. The Laser

Self explanitory, located on the base of the laser.

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

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

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

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

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

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

Now go to **firmwaretool 32** tab

Load your dummy.bin as source –

decline any auto load ix messages!

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

Now click **Spoof Source to Target**!

Notice the difference in the target firmware now!

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

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:

- **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!

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

Ensure you have installed Portio32! – CLICK HERE!

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

USE THIS 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!

JF has hung on Outro ..... JF just says sending Outro to port 0x????

As per the User Guide, Once sending an Outro / ATA Reset check under Drive Properties the drive should re-inquire (as opposed to being in vendor mode). If it doesnt inquire, you can try Outro again (Samsungs are particulary tetchy due to the way in which they are flashed). If you have spoofed the drive as another Manufacturer, please be aware it will inquire as the "spoofed drive"

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

Installing Portio32

If you are using XP try running the **Portio32.exe** installer

If you get an error like this (or any error saying it's not installed)

Then return to the manual install folder for instructions in the README file

Follow instructions in that file!

YES, YES, YES! I know, there are **NO** instructions for Vista!
Basically, follow the ones for XP! Works just the same!

Now for Win 7 (x86 only)

Basically – open device manager, right click on the top icon!(i.e. your pc)
Select "**add legacy hardware**"

Then

What do you want the wizard to do?

○ Search for and install the hardware automatically (Recommended)

◉ Install the hardware that I manually select from a list (Advanced)

Common hardware types:

Show All Devices
Display adapters
IDE ATA/ATAPI controllers
IEEE 1284.4 compatible printer
IEEE 1284.4 devices
IEEE 1394 Bus host controllers
Imaging devices
Infrared devices
Media Center Extender

< Back   Next >   Cancel

Then

Add Hardware

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.

(Retrieving a list of all devices)

Have Disk...

< Back   Next >   Cancel

Click browse then give it the **portio32.inf** inside manual install folder!

Click open then install the file!

CLICK HERE TO RETURN

JungleFlasher v0.1.66 beta

Thanks to:

Team Jungle

(long live the Dice!)

CLICK HERE TO RETURN TO STARTING POINT