JungleFlasher

(0.0.43 beta)

Basic User Guide v1.2f

Introduction

Jungle Flasher is developed by Team Jungle in an effort to bring all 360 DVD-Drive flashing functions together in one easy to use Win32 Application.

Jungle Flasher provides several functions that up until now where carried by several different apps in both Dos and Win32.

The first tab you will see is the FirmwareTool32 tab. In this window you can load f/w files, Jungle Flasher will parse the files and identify the f/w type and display relevant information, like the all important DVD key and OSIG strings etc. On the Target sub-tab, it will also conduct MD5 hash checking of iXtreme files to confirm authenticity etc. With both source and target files loaded the relevant source data and be transferred to the Target (a.k.a. Spoofed), which can then be flashed to the target drive.

The next tab is DVDKey32, this tab is used to extract info from Lite-On the un-dump-able drive. All, unique information is extracted: Drive Key, Unique Inquiry and Identify strings and Drive serial information. This info is all stored in 1 easy to use file, "Dummy.bin", this is a 256kb file that mimics the approximate structure of a Benq f/w file and is automatically loaded to the source sub-tab in the FirmwareTool32 Tab. There is also a facility to create a "dummy.bin" from previously extract files, although, fresh extractions should be completed where possible. Every effort has been made to make the key extraction as reliable as possible, with multiple dumps with comparison to account for the slightest chance that the serial data could become corrupt.

The Third tab is MTKFlash32. You can use this tab to Unlock Benq and Samsung drives and then dump the current flash for use in the source sub-tab in Firmwaretool32 tab. You can also erase a Lite-on in preperation for flashing. All 3 drives can be flashed in this tab.

The last tab is Hitachi. This is on it's own as it is flashed in the different way to the MTK based drives above. Hitachi Is flashed as a "Live" drive, on a sector by sector basis. At present only dumping is supported. Flashing, is in the final stages and is expected to be available with the release of iXtreme 1.5 for Hitachi.

Jungle Flasher is intended to be rich in information giving as much relevant and useful info as is possible. On the DVDKey32 and MTKFlash32 tabs, all IO and COM port information is detected and displayed as well as drive and device properties for the currently selected drive.

LiteOn PLDS DG-16D2S 74850c

There is no soft method for the LiteOn PLDS DSG-16D2S

Overview

Things become a little different with the LiteOn drives as there is no software only way of unlocking the drive and reading the firmware, it **requires** the utilization of a RS232 to TTL serial hardware, or a popular variant such as **Connectivity Kit v3 (optional probe)** or **Maximus Xtractor (with optional spear)**. This is necessary to extract the key/inquiry/identify/dummy .bin files. These files are necessary for spoofing & gathering your key, even if you are just flashing the 1.5 IXtreme to a LiteOn drive. They contain serial information that is required for proper identification and security related issues.

You only really need the probe / spear if you fear soldering as these eliminate the need to do this although if doing a few drives they can be more convenient.

If you choose to solder the R707 serial point back together, please ignore reference to probe / spear instructions – Serial should be intact before proceeding in your case (R707 bridged)

Using DVDKey32 to obtain key/inquiry/identify/dummy.bin

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.

Page **3** of **59**

Using a Connectivity Kit / Xtractor to power the drive

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

With the correct eject/tray status we can run DVDKey32 either from Command Line, or as depicted below in JungleFlasher.



Open JungleFlasher, you will be presented with the Welcome Screen

After a few sconds the main window will load.

Page **4** of **59**

Source Inquiry Identify Drive Serial		i
Vendor Model Rev Firmware Type	DVD Key @	Save Drive Key
OSIG:		Load Source Firmware
Advanced View Spoof So Target Inquiry Identify Drive Serial	urce to Target	Open Target Firmware
Vendor Model Rev Firmware ver:	DVD Key @	Manual Spoofing
OSIG:		Save to File

As you are using DVDKey32 to obtain data, select DVDKey32 Tab



Select Correct I/O port (check for drive propeties in **Drive Properties** section) and COM port and **insert probe / spear** into R707 via

nwareTool 32 [OVDKey 32 MTK Flash 32 Hitachi G	DR3120
I/O Port 0xCF00	VIA ports Only	Com Port
Port Properties		Com Port Properties
I/O Address:	0xCF00	Port: COM1
Туре:	SATA	Type: Standard
Channel:	Primary	Name: Communications Port
Postion:	Master	Status: Ready
Device:	VIA RAID Controller - 3249	Drive Key Key:
Drive Properties	·	Status:
Vendor:	PLDS	
Name:	DG-16D2S	Get Kev, Create Dummv, bin, Open as Source
F/W Rev:	7485	
Pergrand	000010609009201400	1

Good status on Probe / Spear has LED showing.

Page **5** of **59**



Now, click Get Key, Create Dummy.bin, Open as Source

achi GDR3120
- Com Port
Com Port Properties Port: COM1 Type: Standard Name: Communications Port Status: Ready Drive Key Key: Status: Get Key, Create Dummy, bin, Open as Source
Load from Previous dump files

Providing serial connection was good, DVDKey32 will dump the key 6 times and compare each dump – then prompt you to save **key.bin**, **inquiry.bin**, **identify.bin** and **dummy.bin**

Page **6** of **59**

	Save As						? 🛛	
Signut 🦏	Save in:	🗀 LiteOn			•	- 🗈 💣 🎟	 +	
Firmwar								1
l.	My Recent							
ſ								
F	Desktop							
	>							
	My Documents							
	My Computer							
-L	(
	My Network	File name:	Key.bin			•	Save	
	Places	Save as type:	Firmware Ir	mages (*.bin)		-	Cancel	
				1	200		aomp moo	
	Seri	al Data looks	ok, key	returned:	738718BB	F9B3AFEC365	5A9F98156A17A	~
	Seri Seri	al Data looks al Data looks	ok, key	returned: returned:	738718BB	F9B3AFEC365 F9B3AFEC365	5A9F98156A17A 5A9F98156A17A	
	Seri	al Data looks	ok, key	returned:	738718BB	F9B3AFEC365	5A9F98156A17A	
	Seri Seri	al Data looks	ok, key	returned:	738718BB	F9B3AFEC365 F9B3AFEC365	5A9F98156A17A	
				reconned.			ond is crooke the	
Extract	ed drive key m	atched 6 time:	5.					
1								~

Save As					? 🔀
Save in:	🗀 LiteOn		•	+ 🗈 💣 🎟+	
My Recent Documents	A Identify.bin Inquiry.bin Key.bin				
Desktop My Documents					
My Computer					
My Network	File name:	dummy.bin		• •	Save
Places	Save as type:	Firmware Images (*.bin)		•	Cancel

Although extracting the key 6 times increases chances of correct key being obtained and checks are carried out on validility – 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 LiteOn Drive

There is no harm in running DVDKey32 multiple times, increasing the number of key extractions.

FirmwareTool 32 DVDKey 32 MTK Flash 32 Source Inquiry Identify Drive Serial D:\JF TUT\LiteOn\dummy.bin Vendor Model Rev Firmware Type	P Hitachi GDR3120 Hitachi GDR3120 DVD Key @ 0xA030	Save Drive Key
Lite-On DG-16D2S 74850 DVDKey32 extra OSIG: PLDS DG-16D2S 7485	act 73871888F983AFEC3655A9F98156A17A	Load Source Firmware
✓ Advanced View	oof Source to Target	Open Target Firmware
 Vendor Model Rev Firmware ver:	DVD Key @	Manual Spoofing
OSIG:		Save to File
mmy bin file saved to D:\JF TUT\Lit ading DVDkey source file	eOn\dummy.bin	

JungleFlasher will then open dummy.bin in FirmwareTool32

Page 8 of 59

Just verify data reports as it should, DVDKey32 Extract with OSIG of PLDS DG-16D2S with same key you dumped (check log for reference).

Source Inquiry Identify Drive Serial	
Vendor Model Rev Firmware Type DVD Key @ 0xA030	Save Drive Key
OSIG: PLDS DG-16D2S 7485	Load Source Firmware
	.56A17A .56A17A .56A17A
	.56A17A .56A17A .56A17A

Now, you need to load hacked firmware into the Target Buffer

Select Open Target Firmware

Advanced View	Spoof Source	ce to Target	
Target Inquiry Identify Drive Ser	rial		Open Target Firmware
Vendor Model Rev Fir	rmware ver:	DVD Key @	Manual Spoofing
OSIG:			Save to File

When the box pops up, navigate to your hacked firmware (as iXtreme v1.5 is the only firmware out at time of composing, we will be using that)

Once you have navigated to your desired Target Firmware click Open



Upon clicking **Open** JungleFlasher will take you back to **FirmwareTool32** and will have loaded your target firmware into the target buffer – You will see below the Key isn't good, it's all 55aa55aa's

JungleFlasher 0.0.43 Beta	
FirmwareTool 32 DVDKey 32 MTK Flash 32 Hitachi GDR3120	
Source Inquiry Identify Drive Serial	
D:\JF TUT\LiteOn\dummy.bin Vendor Model Rev Firmware Type DVD Key @ 0x4030 Vendor Pool 100000000000000000000000000000000000	Save Drive Key
Lite-Un DG-16D2S 74850 DVDKey32 extract [73871888F983AFEL3655A9F98156A17A OSIG: PLDS DG-16D2S 7485	Load Source Firmware
Advanced View Spoof Source to Target	
Target Inquiry Identify Drive Serial	Open Target Firmware
D:\Documents and Settings\Oggy\Desktop\360\LiteOn_Ktreme_v1.5\ix15-liteon.bin Vendor Model Rev Firmware ver: DVD Key @ n/a	Manual Spoofing
DSIG: PLDS DG-16D2S 7485	Save to File
Firmware type is: DVDKey32 extract Loading target file D:\Documents and Settings\Oggy\Desktop\360\LiteOn_iXtreme_v1.5\ix15-liteon.bin Target File MD5 hash is: d8aaa30797c7680109b395bc3a380d5f Genuine Lite-On iXtreme 1.5 Final Inquiry area found Current DVD key is 55AA55AA55AA55AA55AA55AA55AA55AA Firmware is a Lite-On encrypted iXtreme OSIG: PLDS DG-16D2S 7485 Firmware type is: iXtreme v1.5 12X	

Page **10** of **59**

JungleFlasher will do an MD5 Hash check on the firmware to see if it verifies ok, you should always check this in the **Running Log** to ensure you have good, valid target firmware.



Now, we need to insert your unique Drive Key into the hacked firmware, also copy any necessary serials into it.

🥔 JungleFlasher 0.0.43 Beta	
FirmwareTool 32 DVDKey 32 MTK Flash 32 Hitachi GDR 3120	
Source Inquiru I Identifu Drive Serial	
	1
D:\JF TUT\LiteOn\dummy.bin	Save Drive
Vendor Model Rev Firmware Type DVD Key @ 0xA030	Key
OSIG: PLDS DG-16D2S 74850 DVDRey32 extract 173671666F3634FEC363043F36130417A	Load Source Firmware
Advanced View Spoof Source to Target	·
Target Inquiry Identify Drive Serial	Open Target Firmware
D:\Documents and Settings\Oggy\Desktop\360\LiteOn_Xtreme_v1.5\ix15-liteon.bin	Manual
Vendor Model Rev Firmware ver: DVD Key @ n/a	Spoofing
Lite-On DG-16D2S 74850 Xtreme v1.5 12X 55AA55AA55AA55AA55AA55AA55AA55AA55AA	1
OSIG: PLDS DG-16D2S 7485	Save to File
Firmware type is: DVDKey32 extract	~
Loading target file D:\Documents and Settings\Oggy\Desktop\360\LiteOn_iXtreme_v1.5\ix15-liteon.bin	
Target File MD5 hash is: d8aaa30797c7680109b395bc3a380d5f Genuine Lite-On iXtreme 1.5 Final	
Inquiry area found Current DVD key is 55AA55AA55AA55AA55AA55AA55AA55AA	
Firmware is a Lite-On encrypted iXtreme OSIG: PLDS DG-16D2S 7485 Firmware type is: iXtreme v1.5 12X	
	<u>×</u>

To do this, simply click Spoof source to Target

Page **11** of **59**

Again, check the **Running Log** to see it all went smoothly, you will visually see that your data has been inserted into **Target Buffer**

🤝 JungleFlasher 0.0.43 Beta	
FirmwareTool 32 DVDKey 32 MTK Flash 32 Hitachi GDR 3120	
Source Inquiry Identify Drive Serial	
D:\JF TUT\LiteOn\dummy.bin	· · · · · · · · · · · · · · · · · · ·
Vendor Model Rev Firmware Type DVD Key @ 0xA030	Save Drive Key
OSIG: PLDS DG-16D2S 7485	Load Source Firmware
Advanced View Spoof Source to Target	
Target Inquiry Identify Drive Serial	Open Target Firmware
D:\Documents and Settings\Oggy\Desktop\360\LiteOn_Xtreme_v1.5\ix15-liteon.bin	
Vendor Model Rev Firmware ver: DVD Key@n/a	Spoofing
Lite-On DG-16D2S 74850 Xtreme v1.5 12X 738718BBF9B3AFEC3655A9F98156A17A	
OSIG: PLDS DG-16D2S 7485	Save to File
2	·
Genuine Lite-On iXtreme 1.5 Final Inquiry area found Current DVD key is 55AA55AA55AA55AA55AA55AA55AA55AA Firmware is a Lite-On encrypted iXtreme OSIG: PLDS DG-16D2S 7485 Firmware two is iXtreme v1.5 12X	
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	~

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

Advanced View Spoof Source to Target	
Target Inquiry Identify Drive Serial	Open Target Firmware
D:\Documents and Settings\Oggy\Desktop\360\LiteOn_Xtreme_v1.5\ix15-liteon.bin Vendor Model Rev Firmware ver: DVD Key @ n/a Lite-On DG-16D2S 74850 Xtreme v1 5 12X 738718BBF983AFEC3655A9F98156A17A	Manual Spoofing
OSIG: PLDS DG-16D2S 7485	Save to File

🧼 Jungl	eFlasher 0.0.43	l Beta		2 1 7			
	Save As					? 🔀	Î Î
Sour	Save in:	🗀 LiteOn		• •	- 💣 🛅 -		
D Vi Li O I₹ A Targ D Vi	My Recent Documents Desktop My Documents My Computer	Aummy.bin Ldentify.bin Key.bin					e Drive Key Source nware
Genuir Inquir Current Firnwa Firnwa DVD Key Inquiry Identi	My Network Places y area found t DVD key is 5 re is a Lite-0; re type is: iX y copied to ta y string copie fy string copi	File name: Save as type: 5AA55AA55AA55 n encrypted i treme v1.5 12 rget d from Source ed from Source	Lite_CFW.bin Firmware Images (*.bin) AA55AA55AA55AA55AA Xtreme OSIG: PLDS X to Target e to Target	DG-16D2S	7485	Save Cancel	e to File
Serial	strings copie	d from Source	to Target				*

Jungleflasher will ask you where to save the generated firmware and what you want to name it

Once saved to an output file JungleFlasher will return back to FirmwareTool32, click on MTKFlash32 Tab

IMPORTANT!!!!!

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

Please see pre-requisites (Page 48) and follow instructions to remove Drivers.

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

There is no harm in running DVDKey32 multiple times, increasing the number of key extractions.

Erasing a LiteOn PLDS DG-16D2S

PLEASE READ THE WARNINGS ABOVE

Once you erase the drive, there is NO GOING BACK

JungleFlasher 0.0.43 Beta		
FirmwareTool 32 DVDKey 32 MTK Flash 32	Hitachi GDR3120	
Source Inquiry Identify Drive Serial		
D:\JFTUT\LiteOn\dummy.bin Vendor Model Rev FirmwareType	DVD Key @ 0xA030	Save Drive Key
Lite-On DG-16D2S 74850 DVDKey32 extract	738718BBF9B3AFEC3655A9F98156A17A	
OSIG: PLDS DG-16D2S 7485		Load Source Firmware

Click the MTKFlash32 Tab

Page 14 of 59

Verify I/O Port is correct and click Lite-On Erase

FirmwareTool 32 DVDKey 32	MTK Flash 32 Hitachi GDR3120	
I/O Port OxCF00 Port Properties I/O Address: 0xCF00	360 Tools Benq Sammy UnLock UnLock 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, Power Off / On drive ONCE

Sending Lite-On-Erase	request	to	port	OxCFOO
Drive returned Status	0xF2			

Hopefully you will see Good Flash Chip Properties and Status 0x72 (2 known SPi Chips for LiteOn's, Winbond and MXIC) MXIC Shown, drive will appear in Vendor Mode under Drive Properties

JungleFlasher 0.0.43 Beta FirmwareTool 32 DVDKey 32 MTK Flash 32 Hitachi GD	(R3120)
I/O Port 0xCF00 Port Properties I/O Address: 0xCF00 Type: SATA Channel: Primary Postion: Master Device: VIA RAID Controller - 3249 Drive Properties Vendor: Vendor: Drive in Vendor Mode! Name: F/W Rev: Reserved: Vendor Mode!	360 Tools Benq Sammy Lite-On UnLock UnLock Erase Flash Chip Properties Vendor ID: 0xC2 Device ID: 0x11 Name: MXIC(MX25L2005) Size: 262144 bytes Type: Serial flash with status 0x72 Flashing Tasks Intro / Device ID Outro / ATA Reset Read Erase Write
Sending Lite-On-Erase request to port OxCFOO Drive returned Status OxDO Serial flash found with Status Ox72 Sending Vendor Outro to port OxCFOO Manufacturer ID: OxC2 Device ID: Ox11 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

^

```
Device ID: 0x11
Flash Name: MXIC(MX25L2005)
Flash Size: 262144 bytes
Getting Status from port 0xCF00
SPi flash found with Status 0x72
Sending Chip Erase to Port 0xCF00
Writing target buffer to flash
Writing Bank 0: .....
```

Write Verified OK ! in Running Log signals good write.

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

Samsung (TS-H943) MS25 /MS28

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 it will proceed to the Application itself

🥔 JungleFlasher 0.0.43 Beta	
FirmwareTool 32 DVDKey 32 MTK Flash 32 Hitachi GDR 3120	
Source Lumin Libratio Daine Cariel	
	1
	Save Drive
Vendor Model Rev Firmware Type DVD Key @	Key
OSIG:	Load Source Firmware
Advanced View Spool Source to Target	· · · · · · · ·
Target Inquiry Identify Drive Serial	Open Target Firmware
	Manual
OSIG:	Save to File
JungleFlasher 0.0.43 Beta	
Session Started Sat Jan 24 14:32:27 20090	
Found 11 I/O Ports.	
Found 1 Com Ports.	
Found 1 CD/DVD drives.	
	~

Unlocking the drive

Before we can do anything to the drive, it must be in vendor mode (status 0x70)

Stock Drives (Unmodified)

There are 2 methods of unlock for Stock Drives, the first, is Sammy-Un-Lock – To do this, click the MTKFlash32 Tab

🥔 JungleFlasher	0.0.43 Beta			
FirmwareTool 32	DVDKey 32	MTK Flash 32	Hitachi GDR3120	

Select correct I/O Port (check for TS-H943 in Drive Properties) and click Sammy-Un-Lock

I/0 Port ØxCF00	360 Tools
Port Properties I/O Address: 0xCF00 Type: SATA Channet: Primary Postion: Master Device: VIA RAID Controller - 3249 Drive Properties	Beng Sammy UnLock Erase Flash Chip Properties Vendor ID: Device ID: Name: Size: Type: Flashing Tasks Intro / Device ID Outro / ATA Reset Read
ngleFlasher 0.0.43 Beta ssion Started Thu Jan 22 14:53:47 20090 und 10 I/O Ports. und 1 Com Ports. und 6 windows drives. und 1 CD/DVD drives.	

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

Page **19** of **59**



Select yes and watch the running log in Jungleflasher; this is a 'good' return message

Found 0 CD/DVD drives.	^
Cardina Care In Lock to Daine an east 000700	
Stard Compared	
Stage 2, Complete!	
Stage 3, Complete!	
Done!	
	¥

Now, Click Intro / Device ID

R3120 360 Tools Benq Sammy Lite-On UnLock UnLock Erase Flash Chip Properties Vendor ID: Device ID: Name: Size: Type: Flashing Tasks Intro / Device ID Outro / ATA Reset Read Erase Write

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, Drive Properties** should show **"Drive in Vendor Mode"**

🥪 JungleFlasher 0.0.43 Beta	
JungleFlasher 0.0.43 Beta FirmwareTool 32 DVDKey 32 MTK Flash 32 Hitachi GD I/O Port I/O Port 0xCF00 I/O Port Properties I/O Address: 0xCF00 Type: SATA Channel: Primary Postion: Master Device: VIA RAID Controller - 3249 Drive Properties Vendor: Drive in Vendor Mode!	360 Tools Beng Sammy UnLock UnLock Flash Chip Properties Vendor ID: 0xBF Device ID: 0xBF Device ID: 0xB6 Name: SST(SST39SF020) Size: 262144 bytes Type: Parallel flash with Status 0x70
F/W Rev: Reserved: 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	Read Erase Write

Xtreme 3.0 -> iXtreme 1.4 Unlock using Enable0800.iso

For this you need the enable0800.iso found in the Xtreme 4.0 Distributable Package, 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, <u>IMGBurn</u> 2.4.2.0 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.

FirmwareTool 32 DVDKey 32 MTK Flash 32 Hitachi GDR3120 Source Inquiry Identify Drive Serial Vendor Model Rev Firmware Type DVD Key @ DSIG: ✓ Advanced View <u>Spoor Source to Target</u> Target Inquiry Identify Drive Serial	Save Drive Key Load Source
Source Inquiry Identify Drive Serial Vendor Model Rev Firmware Type DVD Key @ DSIG:	Save Drive Key Load Source
Vendor Model Rev Firmware Type DVD Key @ DSIG: Vadvanced View Spool Source to Target Target Inquiry Identify Drive Serial	Save Drive Key Load Source
Vendor Model Rev Firmware Type DVD Key @ DSIG: Vendor Model Rev Firmware Type DVD Key @ DSIG: Target Advanced View Spool Source to Target Target Inquiry Identify Drive Serial	Save Drive Key Load Source
Vendor Model Rev Firmware Type DVD Key @ DSIG: Advanced View Spool Source to Target Target Inquiry Identify Drive Serial	Load Source
DSIG: Advanced View Spoof Source to Target Target Inquiry Identify Drive Serial	Load Source
DSIG: Advanced View Spoof Source to Target Target Inquiry Identify Drive Serial	Load Source
Advanced View Spoof Source to Target Target Inquiry Identify Drive Serial	Elfmware I
Advanced View Spool Source to Target Target Inquiry Identify Drive Serial	
Target Inquiry Identify Drive Serial	
Target Inquiry Identify Drive Serial	Open Target
	Firmware
	- []
	Manual
Vendor Model Rev Firmware ver: DVD Key @	Spooting
	- I
OSIG:	Save to File

ngleFlasher 0.0.43 Beta	
ssion Started Sat Jan 24 14:32:27 20090	
und 11 I/O Ports. und 1 Com Ports.	
und 6 windows drives.	
und 1 CD/DVD drives.	

Click MTKFlash32 tab

🥔 JungleFlasher	0.0.43 Beta			
FirmwareTool 32	DVDKey 32	MTK Flash 32	Hitachi GDR3120	N.

Page 22 of 59

You will presented with a screen resembling this, select correct I/O Port (check for TS-H943 in Drive Properties) and click Intro / Device ID and then check the Running Log

I/O Port DxCF00 Port Properties I/O Address: 0xCF00 Type: SATA Channel: Primary Postion: Master Device: VIA RAID Controller - 3249	360 Tools Beng Sammy Lite-On UnLock UnLock Erase Flash Chip Properties Vendor ID: Device ID: Name:
Drive Properties Vendor: TSSTcorp Name: DVD-RDM TS-H943A F/W Rev: ms28 Reserved:	Size: Type: Flashing Tasks Intro / Device ID Outro / ATA Reset Read Erase Write
ungleFlasher 0.0.43 Beta ession Started Thu Jan 22 15:10:07 20090 ound 10 I/O Ports. ound 1 com Ports. ound 6 windows drives.	

If enable0800.iso worked correctly, you will get good **flash chip properties (0x70)** and drive will appear in **Vendor Mode** in **Drive Properties**

I/O Port OxCF00 ▼ Port Properties I/O Address: 0xCF00 Type: SATA Channet Primary Postion: Master Device: VIA RAID Controller - 3249 Drive Properties Vendor: Drive in Vendor Mode! Name: F/W Rev: Reserved:	360 Tools Beng Sammy Lite-On UnLock UnLock Erase Flash Chip Properties Vendor ID: 0x8F Device ID: 0x86 Name: SST(SST 39SF020) Size: 262144 bytes Type: Parallel flash with Status 0x70 Flashing Tasks Intro / Device ID Outro / ATA Reset Read Erase Write
Sending Vendor Intro to port 0xCF00 Parallel flash found with Status 0x70 Sending Device ID request to port 0xCF00 famufacturer ID: 0xBF Perice ID: 0xBF Plash Name: SST(SST39SF020) Plash Size: 262144 bytes	

Page 23 of 59

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

🧼 JungleFlasher	0.0.43 Beta			
FirmwareTool 32	DVDKey 32	MTK Flash 32	Hitachi GDR3120	
				[]

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

I/O Port 0xCF00 Port Properties I/O Address: 0xCF00 Type: SATA Channel: Primary Postion: Master Device: VIA RAID Controller - 3249	360 Tools Beng Sammy Lite-On UnLock UnLock Erase Flash Chip Properties Vendor ID: Device ID: Name:
Drive Properties Vendor: TSST.corp Name: DVD-ROM TS-H943A F/W Rev: ms28 Reserved:	Flashing Tasks Flashing Tasks Read Erase Write
ungleFlasher 0.0.43 Beta Session Started Thu Jan 22 15:17:51 20090 Sound 10 I/O Ports. Sound 1 Com Ports. Sound 6 windows drives. Sound 1 CD/DVD drives.	

JungleFlasher will prompt you with instructions



Page 24 of 59

Click Yes the Running Log will display something similar to this

```
Sending Vendor Intro to port OxCFOO
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 **In Vendor Mode** in **Drive Properties**

🧇 JungleFlasher 0.0.43 Beta	
FirmwareTool 32 DVDKey 32 MTK Flash 32 Hitachi GD	R3120
I/0 Port 0xCF00 Port Properties I/0 Address: 0xCF00 Type: SATA Channel: Primary	360 Tools Benq Sammy Lite-On UnLock UnLock Erase Flash Chip Properties Vendor ID: 0xBF
Postion: Master	Device ID: 0xB6
Device: VIA RAID Controller - 3249	Name: SST(SST39SF020) Size: 262144 bytes
Drive Properties Vendor: Drive in Vendor Mode! Name: F/W Rev: Reserved:	Type: Parallel flash with Status 0x70 Flashing Tasks Intro / Device ID Outro / ATA Reset Read Erase Write
Re-sending Vendor Intro: 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	

Once we have the drive in Vendor mode (status 0x70 with good flash chip properties) we can read / write / erase the firmware.

Page **25** of **59**

Reading the Firmware from the drive

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

Type: Parallel flash with Status 0x70
Flashing Tasks
Head Lrase Wille

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

🧼 JungleFlash	er 0.0.43 Beta						×
Save As					? 🔀		
Save jn:	Camsung		- (+ 🗈	di 📰 🕶			
My Recent Documents						Lite-On Erase	
Desktop							
Documents							
Solution My Computer						×70	
Singura Angeleria						TA Reset	
My Network	File <u>n</u> ame:	SAM-OFW.bin		<u> </u>	<u>S</u> ave	Write	
1 10000	Save as <u>t</u> ype:	Firmware Images (*.bin)		• _	Cancel		
Flash Size:	262144 bytes						^
Getting Stat	us from port	0xCF00					
Parallel fla	sh found with	. Status 0x70					
Reading Bank	0:						
Reading Bank	1:						
Reading Bank	2:	* * * * * * *					
	· · · · · · · · · · · · · · · · · · ·						~

Page **26** of **59**

So, save it, once saved it will automatically load the firmware into **FirmwareTool32** here you can verify key looks good (no multiple 77 / FF / 00 etc bytes)

Source Inquiry Identify Drive Serial	
D:\JF TUT\SAM-0FW.bin	
Vendor Model Rev Firmware Type DVD Key @ 0x40C2	Save Key to Key.bin
Samsung TS-H943A ms28 Stock 738718BBF9B3AFEC3655A9F98156A17A	
OSIG: TSSTcorpDVD-ROM TS-H943Ams28	Load f/w Image

Just verify data reports as it should, Samsung, original/hacked firmware, key looks good etc.

Now, you need to load hacked firmware into the Target Buffer

Select Open Target Firmware

Advanced View	Spoof Sourc	e to Target	
Target Inquiry Identify Drive Seri	ial		Open Target Firmware
Vendor Model Rev Fir	rmware ver:	DVD Key @	Manual Spoofing
OSIG:			Save to File

When the box pops up, navigate to your hacked firmware (or stock if restoring a drive, for this example, I will be using iXtreme v1.5 for Samsungs)

Once you have navigated to your desired **Target Firmware** click **Open**

Open			
Look in:	CiteOn_	\$treme_v1.5 ► ● ● ● ●	
My Recent Documents Desktop My Documents My Computer	DOS DVDKey32 FirmTool 1 A Benq_CFU ix15-liteon Ix15-liteon	Demo .3 FINAL // bin bin .bin sim 0x40C2 AFEC3655A9F9815	Save Key to Key bin Load f/w Image
My Network Places	File name: Files of type:	ix15-sam.bin	Manual Spoofing
		OSIG:	Save to File
		Samsung Dump file saved to D:\JF TUT\SAH-OFW.bin Loading MTK_Flash source file Inquiry string found Identify string found DVD key found @ 0x40C2 key is 738718BEF9E3AF#C3655A9F98156A17A Firmware is Samsung OSIC: TSSTcorpDVD-ROM TS-H943Ams28 Firmware type is: Stock	

Upon clicking **Open** JungleFlasher will take you back to **FirmwareTool32** and will have loaded your target firmware into the target buffer – You will see below the Key isn't good, it's all 77's

JungleFlasher 0.0.43 Beta	
FirmwareTool 32 DVDKey 32 MTK Flash 32 Hitachi GDR3120	
Source Inquiry Identify Drive Serial	
D:\JFTUT\Samsung\SAM-OFW.bin	Save Drive
Vendor Model Rev Firmware Type DVD Key @	Key
Samsung TS-H943A ms28 Stock 7387188BF9B3AFEC3655A9F98156A17A	
OSIG: TSSTcorpDVD-ROM TS-H943Ams28	Load Source Firmware
D:\Documents and Settings\Oggy\Desktop\360\LiteOn_Ktreme_v1.5\ix15-sam.bin Vendor Model Rev Firmware ver: DVD Key @ 0x40E8	Manual Spoofing
Samsung TS-H943A ms28 KTREME1.5-12x-FINAL 777777777777777777777777777777777777	
OSIG: TSSTcorpDVD-ROM TS-H943Ams28	Save to File
Dading target file D:\Documents and ettings\Oggy\Desktop\360\LiteOn_iXtreme_v1.5\ix15-sam.bin arget File MD5 hash is: 4bc77f39c4cc65d6lb7cdc2574119912 enuine Sammy iXtreme 1.5 Final nquiry string found dentify string found db key found @ 0x4088 key is 77777777777777777777777777777777777	
irmware type is: iXTREME1.5-12x-FINAL	

Page **28** of **59**

JungleFlasher will do an MD5 Hash check on the firmware to see if it verifies ok, you should always check this in the **Running Log** to ensure you have good, valid target firmware.



Now, we need to insert your unique Drive Key into the hacked firmware, also copy any necessary serials into it.

rimware100132 DVDKey 32 MTK Hash 32 Hitachi GDR3120	
Source Inquiry Identify Drive Serial	
D:\JF TUT\Samsung\SAM-0FW.bin	
Vendor Model Rev Firmware Type DVD Key @ Samsung TS-H9434 ms28 Stock 738718BRE9B34FEC365549F981564174	Save Drive Key
OSIG: TSSTcorpDVD-ROM TS-H943Ams28	Load Source Firmware
Advanced View Spoof Source to Target	
Target Inquiry Identify Drive Serial	Open Target Firmware
D:\Documents and Settings\Oggy\Desktop\360\LiteOn_Xtreme_v1.5\ix15-sam.bin Vendor Model Rev Firmware ver: DVD Key @ 0x40E8 Sampung TS-H9430 mo28 XTREMET 5-12x-FINAL 777777777777777777777777777777777777	Manual Spoofing
OSIG: TSSTcorpDVD-ROM TS-H943Ams28	Save to File
ading target file D:\Documents and ttings\Oggy\Desktop\360\LiteOn_iXtreme_v1.5\ix15-sam.bin rget File MD5 hash is: 4bc77f39c4cc65d6lb7cdc2574l19912 nuine Sammy iXtreme 1.5 Final quiry string found lentify string found D key found @ 0x40B8 key is 77777777777777777777777777777777777	

To do this, simply click **Spoof source to Target**

Again, check the **Running Log** to see it all went smoothly, you will visually see that your data has been inserted into **Target Buffer**

🥔 JungleFlasher 0.0.43 Beta	
FirmwareTool 32 DVDKey 32 MTK Flash 32 Hitachi GDR3120	
Source Inquiry Identify Drive Serial	
D:\JF TUT\Samsung\SAM-0FW.bin Vendor Model Rev Firmware Type DVD Key @ Samsung TS-H943A ms28 Stock 73871888F983AFEC3655A9F98156A17A	Save Drive Key
DSIG: TSSTcorpDVD-RDM TS-H943Ams28	Load Source Firmware
Advanced View Spoof Source to Target Target Inquiry Identify Drive Serial	Open Target Firmware
D:\Documents and Settings\Oggy\Desktop\360\LiteOn_Xtreme_v1.5\ix15-sam.bin Vendor Model Rev Firmware ver: DVD Key @ 0x40E8 Sameuro 15.H9434 ms28 AVTREME15.12x=EIN41 Z38718BBE9836FEC3655549E981564174	Manual Spoofing
OSIG: TSSTcorpDVD-ROM TS-H943Ams28	Save to File
Identify string found DVD key found @ 0x40E8 key is 77777777777777777777777777777777777	

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

Advanced View Spoof Source to Target	
Target Inquiry Identify Drive Serial	Open Target Firmware
D:\Documents and Settings\Oggy\Desktop\LiteOn_Xtreme_v1.5\ix15-sam.bin Vendor Model Rev Firmware ver: DVD Key @ 0x40E8 Z2027.00DE00024.EE_2025E4.0E001EC41.74	Manual Spoofing
Samsung TS-H943A ms28 KTREME1.5-12x-FINAL 73871888F983AFEC3655A9F98156A17A OSIG: TSSTcorpDVD-ROM TS-H943Ams28	Save to File

? X Save As Save in: 🛅 JF TUT 🔶 🗈 💣 📰 -for the ? 📥 BENQ-OFW.bin 📥 dummy.bin My Recent 📥 Identify.bin Documents 📥 Inquiry.bin 📥 Key.bin 📥 SAM-OFW.bin Desktop Save Key to Key.bin My Documents Load f/w Image My Computer Open Target My Network Sam_CFW.bin Save Firmware • File name: Places Cancel • Save as type: Firmware Images (*.bin) Manual Spoofing Vendor Model Rev Firmware ver: DVD Key @ 0x40E8 Samsung TS-H943A ms28 KTREME1.5-12x-FINAL 738718BBF9B3AFEC3655A9F98156A17A Save to File OSIG: TSSTcorpDVD-ROM TS-H943Ams28 Identify string found ~ DVD key found @ 0x40C2 key is 738718BBF9B3AFEC3655A9F98156A17A Firmware is Samsung OSIG: TSSTcorpDVD-ROM TS-H943Ams28 Firmware type is: Stock Spoofing Target DVD Key copied to target Inquiry strings identical Identify strings identical

Jungleflasher will ask you where to save the generated firmware and what you want to name it

Once saved to an output file, we can proceed with writing the firmware to the drive.

Writing Firmware to the drive

To write the firmware, as long as drive is still unlocked we just click MTKFlash32 tab

🧼 JungleFlasher	0.0.43 Beta			
FirmwareTool 32	DVDKey 32	MTK Flash 32	Hitachi GDR3120	*

Verfify you have good flash chip properties still

Flash Chip Properties		
Vendor ID:	0xBF	
Device ID:	0xB6	
Name:	SST(SST39SF020)	
Size:	262144 bytes	
Туре:	Parallel flash with Status 0x70	
Flashing Tasks		
Intro / Device ID Outro / ATA Reset		
Read Erase Write		

Then, click Write

Flash Chip Properties				
Vendor ID:	0xBF			
Device ID:	0xB6			
Name: SST(SST39SF020)				
Size:	262144 bytes			
Туре:	Parallel flash with Status 0x70			
Intro / Device ID Outro / ATA Reset				
Read	Erase Write			

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

A series of 16's are it 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 Target Buffer. So, what we really want to see is **Write Verified OK!**



Ok, now you have flashed your Samsung Drive successfully, should you not get Write Verified OK! Please ask for support in the JungleFlasher support channel, found at irc.efnet.net channel #JungleFlasher

BenQ VAD6038 (62430c and 64930c)

Unlocking the drive

Before we can do anything to the drive, it must be in vendor mode (status 0x73)

BenQ-Un-Lock Stock/ iXtreme 1.1 -> 1.41 / Xtreme Firmwares Only

Please note, BenQ-Un-Lock **WILL NOT** work on drives that have iXtreme 1.5 firmware on them

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

You will be presented with the Welcome Screen shown below.

JungleFlasher 0.0.4	13 b
For Support join #JungleFlasher	on EFnet
Remove Context Menus	<u>User Guide</u>

Click Go to proceed into the program itself

Click the MTKFlash32 Tab

🥔 JungleFlasher	0.0.43 Beta			
FirmwareTool 32	DVDKey 32	MTK Flash 32	Hitachi GDR3120	

Then, select correct I/O Port by verifying PLBS VAD6038 shows in Drive Properties and click BenQ-Un-Lock

nwareTool 32 DVDKey 32 MTK Flash 32 Hita	chi GDR3120
I/D Port ØxCF00 Port Properties I/O Address: 0xCF00 Type: SATA Channet: Primary Postion: Master Device: VIA RAID Controller - 3249	360 Tools Benq Sammy Lite-On UnLock UnLock Erase Flash Chip Properties Vendor ID: Device ID: Name: Size-
Drive Properties Vendor: PBDS Name: VAD6038-64930C F/W Rev: Reserved:	Type: Flashing Tasks Intro / Device ID Outro / ATA Reset Read Erase Write

JungleFlasher will send the Magic Keys to unlock the drive and should return this message in the **Running Log**

Found 1 Com Ports.
Found 5 windows drives.
Found 1 CD/DVD drives.
Sending Magic Keys to Drive on port 0x0xCF00 Done!

The drive is now unlocked, click Intro / DeviceID

I/D Port DxCP00 ▼ Port Properties I/D Address: 0xCF00 Type: SATA Channet: Primary Postion: Master Device: VIA RAID Controller - 3249 Drive Properties Vendor: PBDS Name: VAD6038-64930C FAW Rev: Reserved:	360 Tools Benq Sammy Lite-On UnLock UnLock Erase Flash Chip Properties Vendor ID: Device ID: Name: Size: Type: Flashing Tasks Intro / Device ID Outro / ATA Reset Read Erase Write
Yound 10 I/O Ports. Yound 1 Com Ports. Yound 5 Windows drives. Yound 1 CD/DVD drives. Sending Magic Keys to Drive on port OxOxCFOO Youne!	

Page **35** of **59**

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.**

✓ JungleFlasher 0.0.43 Beta FirmwareTool 32 DVDKey 32 MTK Flash 32 Hitachi (I/0 Port	GDR3120 360 Tools Benq Sammy Lite-On UnLock UnLock Erase Flash Chip Properties Vendor ID: 0xC2 Device ID: 0x11 Name: M×IC(M×25L2005) Size: 262144 bytes Type: Serial flash with status 0x73 Flashing Tasks Intro / Device ID Outro / ATA Reset Read Erase Write
Sending Vendor Intro to port 0xCF00 Serial flash found with Status 0x73 Sending Device ID request to port 0xCF00 Manufacturer ID: 0xC2 Device ID: 0x11 Flash Name: MXIC(MX25L2005) Flash Size: 262144 bytes	

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 Jungle flasher, and select MTKFlash32 Tab

🧼 JungleFlasher	0.0.43 Beta			
FirmwareTool 32	DVDKey 32	MTK Flash 32	Hitachi GDR3120	

Then, select correct I/O Port by verifying PLBS VAD6038 shows in Drive Properties and click Intro / Device ID

🧇 JungleFlasher 0.0.43 Beta	
JungleFlasher 0.0.43 Beta FirmwareTool 32 DVDKey 32 MTK Flash 32 Hitachi I/0 Port OxCF00 Port Properties I/0 Address: 0xCF00 Type: SATA	GDR3120] 360 Tools Benq Sammy Lite-On UnLock UnLock Erase
Channel: Primary Postion: Master Device: VIA RAID Controller - 3249	Vendor ID: Device ID: Name: Size:
Drive Properties Vendor: PBDS Name: VAD6038-64930C F/W Rev: Reserved:	Type: Flashing Tasks Intro / Device ID Outro / ATA Reset Read Erase Write
JungleFlasher 0.0.43 Beta Session Started Sun Jan 25 01:09:43 2009D Found 10 I/O Ports. Found 1 Com Ports. Found 5 windows drives. Found 1 CD/DVD drives.	

JungleFlasher will prompt you with instructions

Page **37** of **59**



Click Yes the Running Log will display something similar to this

Sending Vendor Intro to port 0:	xCFOO
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**

JungleFlasher 0.0.43 Beta FirmwareTool 32 DVDKey 32 MTK Flash 32 Hitachi I/D Port I/D Port I/D Port ØxCF00 I/D Address: 0xCF00 Type: SATA Channet: Primary Postion: Master Device: VIA RAID Controller - 3249 Drive Properties Vendor: Drive in Vendor Model Name: F/W Rev: I/D	GDR3120 GDR320 GDR3
Reserved: Sending Vendor Intro to port 0xCF00 Serial flash found with Status 0x73 Sending Device ID request to port 0xCF00 Manufacturer ID: 0xC2 Device ID: 0x11 Flash Name: MNIC(MX25L2005) Flash Size: 262144 bytes	Read Erase Write

Page 38 of 59

Reading the Firmware from the drive

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

Drive Properties Vendor: Drive in Vendor Model	Type: Serial flash with status 0x73
Name:	Flashing Tasks
F/W Hev: Reserved:	Read Erase Write

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**

🧼 Junglef	lasher 0.0.43 l	Beta				
Firmware	Save As				? 🛛	
	Save in:	🗀 BenQ		🔹 🗢 🖻 🖻	« 📰 -	
1/						
los Ios	My Recent					
-Po	Documents					
	Desktop					
	My Documents					
1	My Computer					
	~					
	My Network Places	File name:	BENQ-OFW.bin		Save	
		Save as type:	Firmware Images (*.bin)		Cancel	
Flash Si	ze: 262144 bj	rtes				^
Getting	Status from po	ort OxCFOO				
Serial f	lash lound wit	n scatus Ux.	(3			
Reading	Bank U: Bank 1:					
Reading	Bank 2: Bank 3:					
						~

Page **39** of **59**

Once saved it will automatically load the firmware into **FirmwareTool32** here you can verify key looks good (no multiple 77 / FF / 00 etc bytes)

Just verify data reports as it should, BenQ, original/hacked firmware, key looks good etc.

🥔 JungleFlasher 0.0.43 Beta	
FirmwareTool 32 DVDKey 32 MTK Flash 32 Hitachi GDR 3120	
Source Inquiry Identify Drive Serial	1
D:\JF TUT\BenQ\BENQ-OFW.bin	
Vendor Model Rev Firmware Type DVD Key @ 0x4030	Key
OSIG: PBDS VAD6038-64930C	Load Source Firmware
Advanced View Spoof Source to Target	
Target Inquiry Identify Drive Serial	Open Target Firmware
Vendor Model Rev Firmware ver: DVD Key@	Manual Spoofing
OSIG:	Save to File
	<u>ا</u> ا
Benq Dump file saved to D:\JF TUT\BenQ\BENQ-OFW.bin	~
Loading MTK_Flash source file	
Induity string found Identify string found DVD key found @ 0x4030 key is FAFID0725C0FFAC226FFASB23C52D8F6	
Firmware is Benq OSIG: PBDS VAD6038-64930C Firmware type is: Stock	
	~

Now, you need to load hacked firmware into the Target Buffer

Select Open Target Firmware

Advanced View Spoof	Source to Target
Target Inquiry Identify Drive Serial	Open Ta Firmwa
Vendor Model Rev Firmware ver:	DVD Key @ Spoofin
OSIG:	Save to

When the box pops up, navigate to your hacked firmware (or stock if restoring a drive, for this example, I will be using iXtreme v1.5 for BenQ Drives)

-	Junglef	lasher 0.0.43 B	leta					
T	Firmware	Open					? 🛛	
	Source	Look in:	C LiteOn_Xtrem	ne_v1.5	• +	• 🗈 💣 🎫		
	D:V	Mv Recent	DOS DVDKey32 Dem	no. Mai				prive
	Vend	Documents	New Folder					
	Bend		Beng_CFW.bin	in .				
	OSIC	Desktop	k 15Beng.bin]				are
	🗹 Adv	>	ix15-liteon.bin					
	Target	My Documents						arget are
		Mu Computer						Ial
	Vend							ing
	OSIC	My Network Places	File name:	ix15Benq.bin		•	Open	o File
		110005	Files of type:	Firmware file (*.bin)			Cancel	
Be	enq Dum pading	p file saved t MTK_Flash sour string found	o D:\JF TUT\B ce file	enQ\BENQ-OFW.bin				
Ic	lentify	string found						
DI	D key	found @ 0xA030	key is FAF1D(0725C0FEAC226EFA8B23C	52D8 E 6			
Fi	.rmware .rmware	is Beng USIG: type is: Stoc	PBDS VAD60 k	U38-6493UC				
1								<u>×</u>

Once you have navigated to your desired Target Firmware click Open

Upon clicking **Open** JungleFlasher will take you back to **FirmwareTool32** and will have loaded your target firmware into the target buffer – You will see below the Key isn't good, it's all 77's

🔎 JungleFlasher 0.0.43 Beta		
FirmwareTool 32 DVDKey 32 MTK Flash 32 H	Hitachi GDR3120	
Source Inquiru Identifu Drive Serial		
been set of the set of		1
D:\JF TUT\BenQ\BENQ-OFW.bin Vendor Model Rev Firmware Type	DVD Key @ 0x4030	Save Drive Key
Beng VAD6038 64930C Stock	FAF1D0725C0FEAC226EFA8B23C52D8E6	
OSIG: PBDS VAD6038-64930C		Load Source Firmware
I Advanced View Spoof So	purce to Target	
Target Inquiry Identify Drive Serial		Open Target Firmware
D:\Documents and Settings\Oggy\Desktop\360\Lite	On_Xtreme_v1.5\ix15Benq.bin	
Vendor Model Rev Firmware ver:	DVD Key @ 0xE030	Manual Spoofing
Beng VAD6038 64930C Xtreme v1.50-12x-	777777777777777777777777777777777777777	
FINAL OSIG: PBDS VAD6038-64930C		Save to File
-		
Loading target file D:\Documents and		~
Settings\0ggy\Desktop\360\Lite0n_iXtreme_	vl.5\ix15Benq.bin	
Genuine Beng iXtreme 1.5 Final		
Inquiry string found Identify string found		
DVD key found @ 0xE030 key is 7777777777	****	
Firmware is Beng OSIG: PBDS VAD6038-64	930C	
Filmware cype is. increme vi.30-12x-filmab		

JungleFlasher will do an MD5 Hash check on the firmware to see if it verifies ok, you should always check this in the **Running Log** to ensure you have good, valid target firmware

Loading target file D:\Documents and Settings\Oggy\Desktop\360\LiteOn iXtreme v1.5\ix15Beng.bin	^
Target File MD5 hash is: a6d4c666c0014cadd0ca51c98cd3c80b Genuine Beng iXtreme 1.5 Final	
Inquiry string found Identify string found DVD key found @ 0xE030 key is 77777777777777777777777777777777777	

Page **42** of **59**

Now, we need to insert your unique Drive Key into the hacked firmware, also copy any necessary serials into it.

🔎 JungleFlasher 0.0.43 Beta	
FirmwareTool 32 DVDKey 32 MTK Flash 32 Hitachi GDR 3120	1
Source Inquiry Identify Drive Serial	· ·
D:\VF TUT\BenQ\BENQ-OFW.bin	Save Drive
Vendor Model Rev Firmware Type DVD Key @ 0xA030	Key
Beng VAD6038 64930C Stock FAF1D0725C0FEAC226EFA8B23C52D8E6	
OSIG: PBDS VAD6038-64930C	Load Source
Target Inquiry Identify Drive Serial D:\Documents and Settings\Oggy\Desktop\360\LiteOn_Xtreme_v1.5\ix15Benq.bin Variate Madel Drive Serial	Open Target Firmware Manual Spoofing
Beng VAD6038 64930C Xtreme v1.50-12x- FINAL 777777777777777777777777777777777777	Save to File
Loading target file D:\Documents and Settings\Oggy\Desktop\360\LiteOn_iXtreme_vl.5\ix15Benq.bin Target File MD5 hash is: a6d4c666c0014cadd0ca51c98cd3c80b Genuine Benq iXtreme 1.5 Final Inquiry string found Identify string found	<u> </u>
DVD key found @ 0xE030 key is 77777777777777777777777777777777777	

To do this, simply click Spoof source to Target

Again, check the **Running Log** to see it all went smoothly, you will visually see that your data has been inserted into **Target Buffer**

Tungle Flasher 0.0.43 Beta	
Source Inquiry Identify Drive Serial	1
D:\JF TUT\BenQ\BENQ-OFW.bin Vendor Model Rev Firmware Type DVD Key @ 0xA030	Save Drive Key
Beng VAD6038 64930C Stock JFAFTD0725C0FEAC226EFA8823C52D8E6 OSIG: PBDS VAD6038-64930C	Load Source Firmware
Target Inquiry Identify Drive Serial D:\Documents and Settings\Dgay\Desktop\360\LiteOn Ktreme v1.5\ix15Beng.bin	Open Target Firmware
Vendor Model Rev Firmware ver: DVD Key @ 0xE030 Beng VAD6038 64930C Xtreme v1.50-12x- FINAL	Manual Spoofing
OSIG: PBDS VAD6038-64930C	Save to File
D key found @ 0xE030 key is 77777777777777777777777777777777777	
quiry strings identical entify strings identical FFOO area copied for Benq to Benq	

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

Target Inquiry Identify Drive Serial	Open Target Firmware
D:\Documents and Settings\Oggy\Desktop\360\LiteOn_Xtreme_v1.5\ix15Benq.bin	
Vendor Model Rev Firmware ver: DVD Key @ 0xE030	Spoofing
Beng VAD6038 64930C Ktreme v1.50-12x- [FAF1D0725C0FEAC226EFA8B23C52D8E6 FINAL OSIG: PBDS VAD6038-64930C	Save to File

Jungleflasher will ask you where to save the generated firmware and what you want to name it

🥔 Junglei	lasher 0.0.43 E	leta					
Firmware	Save As					? 🛛	
Source	Save in:	🗁 BenQ		•	🗈 📸 🎫		
D:W	My Recent						vrive
Vend Bend	Documents						
OSIC	Desktop						are
🔽 Adv	6						
Target	My Documents						arget are
D:\C	My Computer						ual
Bend	6						
	My Network Places	File name:	Benq_CFW.bin		J	Save	o File
		Save as type:	Firmware Images (*.bin)		•	Cancel	
DVD key Firmware Firmware	found @ OxEO30 is Benq OSIG: type is: iXtr	key is 77777 PBDS VAD60 eme v1.50-12x-	77777777777777777777777777777777777777	777777			~
Spoofing DVD Key	Target copied to targ	et					
Inquiry Identify 0xFF00 a	strings identi strings ident rea copied for	cal ical Benq to Benq					
1							*

Once saved to an output file, we can proceed with writing the firmware to the drive.

Writing Firmware to the drive

To write the firmware, as long as drive is still unlocked we just click MTKFlash32 tab

🧼 JungleFlasher	0.0.43 Beta			
FirmwareTool 32	DVDKey 32	MTK Flash 32	Hitachi GDR3120	

Verfify you have good flash chip properties still

—Flash Chip Pro	operties
Vendor ID:	0xC2
Device ID:	0x11
Name:	MXIC(MX25L2005)
Size:	262144 bytes
Туре:	Serial flash with status 0x73

Then, click Write

Flash Chip Pro	operties
Vendor ID:	0xC2
Device ID:	0x11
Name:	MXIC(MX25L2005)
Size:	262144 bytes
Туре:	Serial flash with status 0x73
- Flashing Task	8
Intro / D	evice ID Outro / ATA Reset
Read	Erase 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 are it 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 Target Buffer what we really want to see is **Write Verified OK!**

Page **46** of **59**

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.

-Flashing Tasks				
Intro / Device	ID	Outro	/ ATA Reset	
Read	Eras	e	Write	

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:	Type: 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 OxCFOO	

Appendix

This section is for more advanced users, and the lesser used funtions of JungleFlasher

Pre requisites

- If using a VIA 6421x PCI Sata card, it is advisable to remove the drivers from the \Windows\System 32\Drivers\ directory as they do not handle erased LiteOns very well at all, causing the infamous 'LiteOn + VIA Freeze'
 - You must install PortIO32
- .net framework 2.0 Or later for Windows XP machines I believe you need .net framework 3.5 SP1 on Windows Vista Machines

Removing VIA drivers (Windows XP)

NOT TO BE DONE IF YOUR MAIN HARD DRIVE IS ON VIA SATA CARD

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

Right Click My Computer, select properties



Click the "Hardware" tab

Page 48 of 59

System Restore	Automa	itic Updates	Remote
General Cor	mputer Name	Hardware	Advanced
	Si	etem:	
		Microsoft Window	s XP
		Professional	
	1	Version 2002	
		Service Pack 2	
	Be	egistered to:	
-	.0	Oggy	
	Co	omputer:	
		AMD Athlon(tm) 6	4 X2 Dual
		Core Processor 50)00+ D (D (D () (
		2.61 GHz, 3.00 G	B of HAM
		Physical Address	Extension

Then, click "Device Manager"



Page 49 of 59

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

File Action View Help	
- → 🖪 🖆 👙 😫 🖪 🧕	
Acronis Devices	
🕂 🗳 Disk drives	
🕂 🧐 Display adapters	
E DVD/CD-ROM drives	
PIONEER DVD-RW_DVR-115D	
PIONEER DVD-RW DVR-215D	
SJSZ MNOHA3K9I SCSI CdRom Device	
Eloppy disk controllers	
Standard floppy disk controller	
T C IDE ATA/ATAPI controllers	
F S IEEE 1394 Bus host controllers	
🕂 🦢 Keyboards	
+ Mice and other pointing devices	
🕂 🧃 Monitors	
Ball Network adapters	
🕂 👮 Ports (COM & LPT)	
+ 🐱 Processors	
E CSI 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



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



Now, to remove drivers we must navigate to where viamraid.sys is

Mine were located, and most will be: C :\WINDOWS\system32\drivers\viamraid.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 Page **51** of **59** You have successfully removed VIA drivers from your machine

Installing PortIO32

PortIO32 is a driver and library which allows you to do low-level port IO from any programming language which can use a DLL in Windows

Simply double click PortIO32.exe found in the JungleFlasher package and wait





PortIO32.exe

Look for the confirmation message (image taken from Windows Vista)



If you require .net framework, follow link / instructions here:

http://www.microsoft.com/downloads/details.aspx?familyid=0856eacb-4362-4b0d-8eddaab15c5e04f5&displaylang=en

With the pre requisites met, we are now able to move onto using JungleFlasher itself.

Save key to file

With the element of risk involved with manually input keys JungleFlasher supports outputting to key.bin for all drives.

DVDKey32 will create it for BenQ / LiteOn but Jungleflasher also supports dumping key.bin from source firmware.

To do this, **Open Source Firmware** in **FirmwareTool32** and click **Save Drive Key** select where you want to store it and click **Save**

Load from previous dump files

Found under DVDKey32,



The only real reason you should be using this feature is if you **DO NOT** have your **Original** LiteOn PLDS DG-16D2S but have Key/Inquiry.Identify .bin files

Simply click this, read the warning, if you want to proceed, click **Yes**, then proceed to load each file in turn and click **OK**

Page **53** of **59**

This will create **Dummy.bin** and load it into **FirmwareTool32** IF YOU CAN OBTAIN YOUR DATA FROM THE DRIVE ITSELF ITS HIGHLY RECOMMENDED THAT YOU DO – THIS SHOULD BE USED AS A LAST RESORT ONLY.

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 LiteOn PLDS DG-16D2S this will activate the LiteOn Barcode section of Manual Spoofing, please see below for instructions.

Spoofing LiteOn Barcode into Inquiry String

This is for Spoofing a drive in place of a LiteOn 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 LiteOn) 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

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 newr 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 fuction unless you know what you are doing.

Registry Settings

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

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

my computer	Name	Type	Data	
🗄 🧰 HKEY_CLASSES_ROOT	ab)(Default)	REG SZ	(value not set)	
	AdvView	REG_SZ	1	
AppEvents	COMPort	REG_SZ	0	
	DoCom	REG_SZ	1	
	DoDevID	REG_SZ	1	
	DoDrives	REG_SZ	1	
	DoIO	REG_SZ	1	
JungleFlasher	abjioport	REG_SZ	10	
🕀 🦲 Keyboard Layout	بالله Left	REG_SZ	296	
🕀 🧰 Printers	all position	REG_SZ	Master	
🗌 📄 RememberMe	ScsiPorts	REG_SZ	1	
SessionInformation	ab) Top	REG_SZ	208	
SlySoft		REG_SZ	0	
Software				
Volatile Environment				
Windows 3.1 Migration Status				
	,			
E CURRENT CONFIG				
Adview - Remembers	• Do	Drives - Enume	rates drive	Position –No lon
Adview - Remembers	• Do	Drives - Enume	rates drive	Position – No lor was used in 026
Adview - Remembers ther Advanced View was	• Do	DTives - Enume etters, for debug	rates drive g use only	Position – No lor was used in .026
Adview - Remembers ther Advanced View was selected or not	• Do	DTives - Enume etters, for debug	rates drive g use only	 Position –No lor was used in .026 JungleFla
Adview - Remembers ther Advanced View was selected or not	• Do lo	D Drives - Enume etters, for debug DolO - Enumera	rates drive g use only ites I / O	 Position –No lor was used in .026 JungleFla
Adview - Remembers ther Advanced View was selected or not MPort - Remembers last	• Do lo	D Drives - Enume etters, for debug DolO - Enumera ports, for debug	rates drive g use only ites I / O use only	 Position – No lor was used in .026 JungleFla ScsiPorts - en
Adview - Remembers ther Advanced View was selected or not MPort - Remembers last VI Port selected, number	• Do la	D Drives - Enume etters, for debug DoIO - Enumera ports, for debug	rates drive g use only ntes I / O use only	 Position – No lor was used in .026 JungleFla ScsiPorts - en SCSIAdapter IO
Adview - Remembers ther Advanced View was selected or not MPort - Remembers last M Port selected, number resents position in drop	• Do a 	DDrives - Enume etters, for debug DolO - Enumera ports, for debug DPort - Rememb	rates drive g use only ites I / O use only ers last IO	 Position – No lor was used in .026 JungleFla ScsiPorts - en SCSIAdapter IO (NON-II
Adview - Remembers ther Advanced View was selected or not MPort - Remembers last M Port selected, number presents position in drop	• De le • le	DDrives - Enume etters, for debug DolO - Enumera ports, for debug DPort - Rememb	rates drive g use only ites I / O use only ers last IO	 Position – No lor was used in .026 JungleFla ScsiPorts - en SCSIAdapter IO (NON-IE
Adview - Remembers ther Advanced View was selected or not MPort - Remembers last M Port selected, number presents position in drop down menu	• Do lo • •	DDrives - Enume etters, for debug DolO - Enumera ports, for debug DPort - Rememb Port selected, r	rates drive g use only ates I / O use only ers last IO number	 Position –No lor was used in .026 JungleFla ScsiPorts - en SCSIAdapter IO (NON-IE
Adview - Remembers ether Advanced View was selected or not MPort - Remembers last M Port selected, number presents position in drop down menu	• Do lo • • IC	DDrives - Enume etters, for debug DolO - Enumera ports, for debug DPort - Rememb Port selected, r epresents positio	rates drive g use only ites I / O use only ers last IO number on in drop	 Position –No lor was used in .026 JungleFla ScsiPorts - en SCSIAdapter IO (NON-IE Top - Remember
Adview - Remembers ether Advanced View was selected or not MPort - Remembers last M Port selected, number presents position in drop down menu DoCom - Enumerates	• Do lo • • • • • • •	DDrives - Enume etters, for debug DolO - Enumera ports, for debug DPort - Rememb Port selected, r epresents positio down men	rates drive g use only ates I / O use only ers last IO number on in drop nu	 Position –No lor was used in .026 JungleFla ScsiPorts - en SCSIAdapter IO (NON-IE Top - Remember JungleFlasher w
Adview - Remembers ether Advanced View was selected or not MPort - Remembers last M Port selected, number presents position in drop down menu DoCom - Enumerates ports, for debug use only	• Do lo • lo • IC	DDrives - Enume etters, for debug DolO - Enumera ports, for debug DPort - Rememb Port selected, r epresents positic down mer	rates drive g use only ates I / O use only ers last IO number on in drop nu	 Position –No lor was used in .026 JungleFla ScsiPorts - en SCSIAdapter IO (NON-IE Top - Remember JungleFlasher wi
Adview - Remembers ether Advanced View was selected or not MPort - Remembers last M Port selected, number presents position in drop down menu DoCom - Enumerates ports, for debug use only	• D(- - (- (C - (C) - (C)	DDrives - Enume etters, for debug DolO - Enumera ports, for debug DPort - Rememb Port selected, r epresents positic down mer	rates drive g use only ites I / O use only ers last IO number on in drop nu postion of	 Position –No lor was used in .026 JungleFla: ScsiPorts - en SCSIAdapter IO (NON-IE Top - Remember JungleFlasher wi ViaPortsOnly - e
Adview - Remembers ether Advanced View was selected or not MPort - Remembers last M Port selected, number presents position in drop down menu DoCom - Enumerates ports, for debug use only DevID – Will send Intro if	• Do - - - IC - - - - - - - - - - - - - - - - - - -	DDrives - Enume etters, for debug DolO - Enumera ports, for debug Port - Rememb Port selected, r epresents positic down mer ft - Remembers ungleFlasher wir	rates drive g use only ites I / O use only ers last IO number on in drop nu postion of ndow (left	 Position –No lor was used in .026 JungleFla: ScsiPorts - en SCSIAdapter IO (NON-IE Top - Remember JungleFlasher wi ViaPortsOnly - e only Via IO ports

You will see something similar to this:

Page 58 of 59

•

Mode

- er in use, elease of er
- nerate orts also
- ostion of low (Top
- umerate or safety (Value 1) Lists all if removed or Value 0

JungleFlasher v0.0.043 beta

Thanks to:

Team Jungle

&

The testers for all the hard work!