

How to Insert a Disc Encryption Key Into a Hitachi-LG GDR- Drive in an Xbox 360

Tutorial by [GaZ]

Introduction

After an unsuccessful attempt to mod my first Xbox 360, I was left with an Xbox 360 with a bricked Hitachi drive. Unfortunately I was not able to return the console, as I had misplaced the RF shielding from the top section of the case (Doh!). Luckily I was able to source a new Hitachi (for free cheers Griff!!), and I set about trying to replace the dead drive with the new one.

After a long process of researching and learning and much head scratching, I was able to complete the switch, **without** the help of an easy tutorial, so I decided to help my fellow modders and explain the process in a simple tutorial.

The process of replacing these drives is a bit more complicated than doing the same with a Samsung. This is because with a Samsung, you are able to flash the entire FW image onto the drive in one go, so once you have obtained your 360's disc encryption key, you simply insert it into a stock image of the FW and flash it to the drive.

The Hitachi FW image contains read routines that are used in the read/write process, so if you attempt to flash an entire FW image to the drive, you flash over the routines that are used, and this causes the flash to stop, and the FW chip becomes useless, i.e. a bricked drive.

In order to replace the drive it is **essential** that you have the 360's disc encryption key, without it no drive can be made to work in your console. If you have killed the drive without obtaining this key the only solution is to de-solder the FW chip on the drives motherboard and read it in an external programmer. There are some skillful people over on xboxhacker.net that can do this for a fee.

This tut covers the insertion of the key into a Hitachi drive. This key can come from any other drive, Samsung or Hitachi, for the purposes of this tutorial, my orig.bin came from a Hitachi.

Tools Required

Memdump_win.exe by Seventhson (for dumping images of FW)

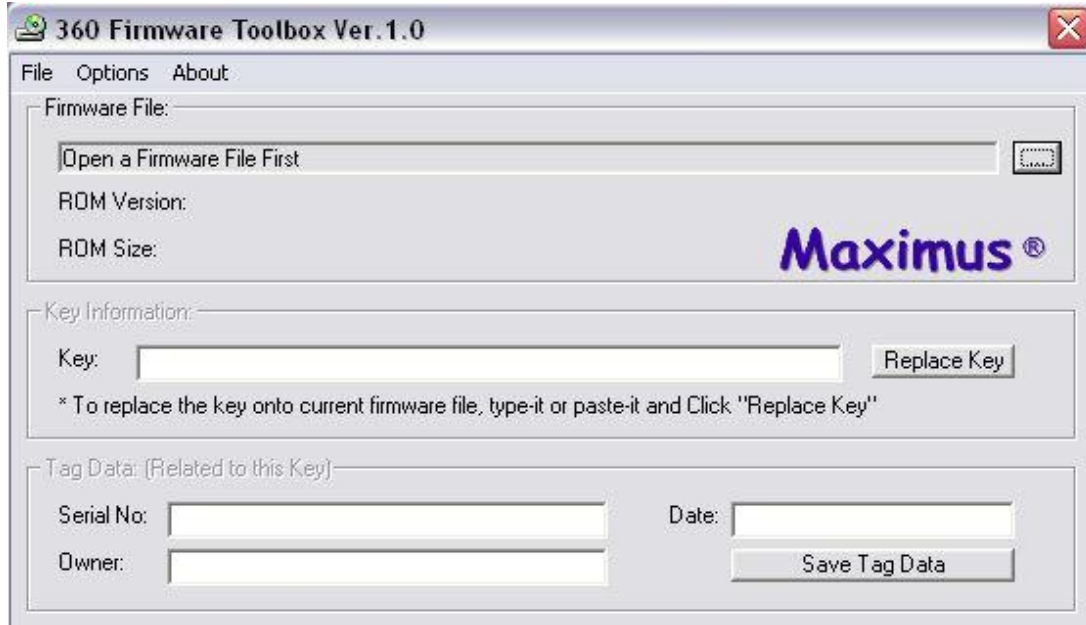
XXFlash (where XX is the revision number of your drive) (for flashing FW to drive)

360FirmwareToolbox by Maximus (to get keys from FW)

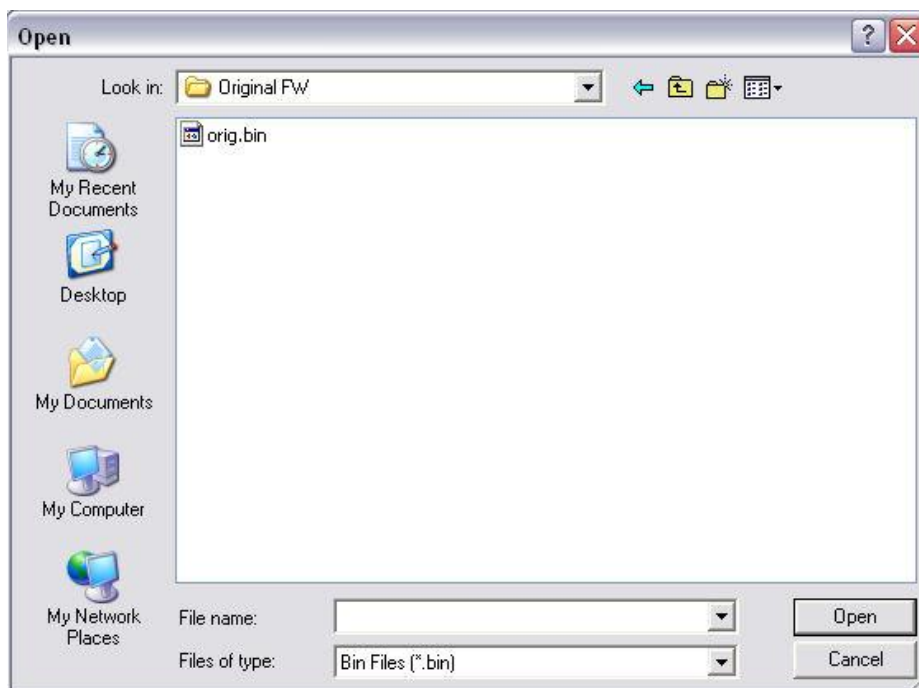
Orig.bin (dump of original FW)

Step1 – Obtaining the Disc Encryption Key from FW of drive to be replaced

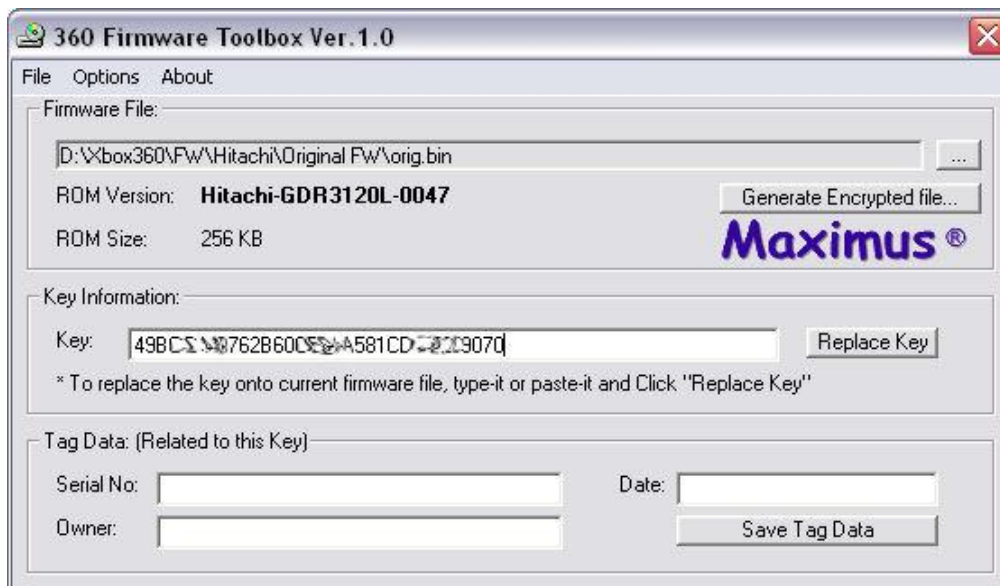
Open 360FirmwareToolbox, and you will see the following screen:



Next hit the button on the right and navigate to where you have the orig.bin saved and load it



You will see this:



Here the disc encryption key will be shown in the box. Copy and paste this into a text file, and copy it several times. **KEEP IT SAFE!!!**

Step 2 – Obtaining a Dump of the Hitachi drive's FW

The idea here is to dump the FW of the new drive, so that the key can be patched into it. It is always better to flash a drive with its original FW, rather than another drive's FW, **especially** if the two drives are different model revisions (46, 47, 59 etc), and even in my opinion better than using a downloaded stock image of the drives FW. No other FW will match the drives FW better than its own.

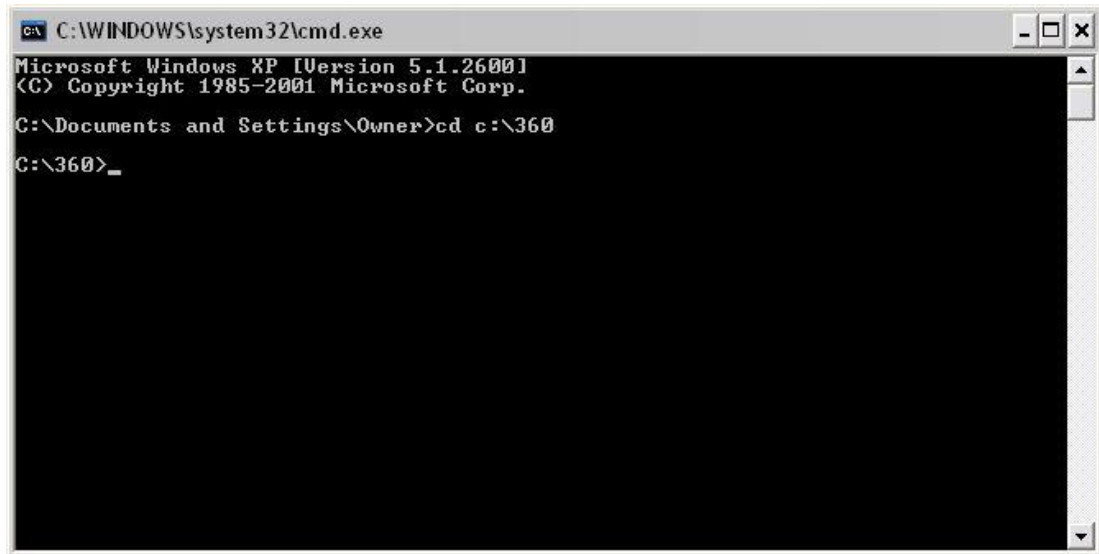
Once the drive has been put into modeb, connect it to the PC via SATA. The PC will assign it a letter. For the tutorial I will assume the letter is E:\

PLEASE ENSURE YOU USE THE CORRECT LETTER!!

Personally, I keep a directory in my C drive for flashing Hitachi drives, C:\360\ as I find it is easier to use in command prompts.

Put the files flashsec47_win.exe (or variant for drive model revision), and memdump_win.exe into this directory, run a command prompt and use the command

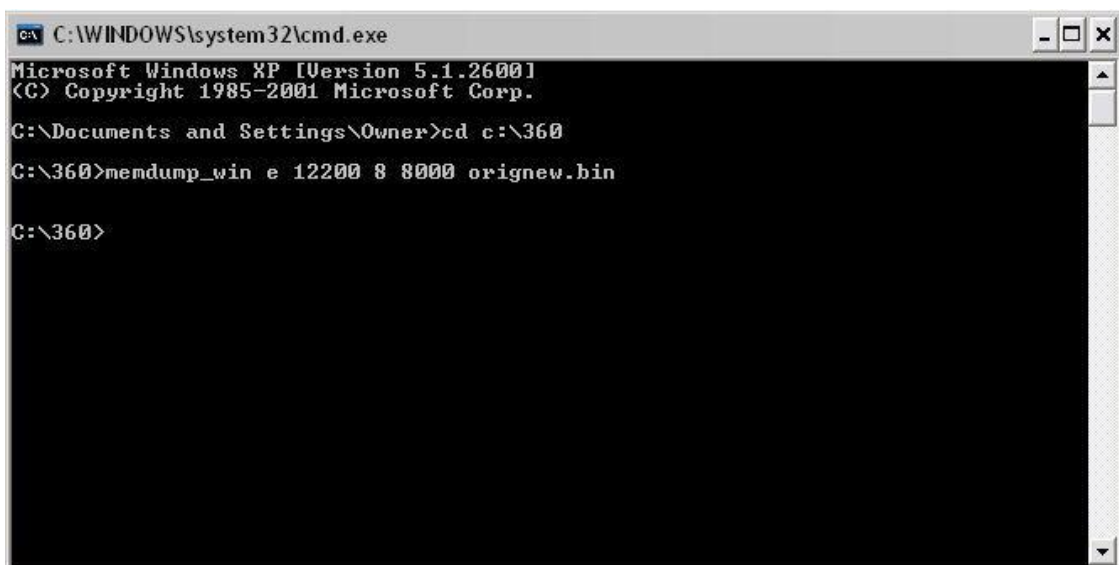
```
cd c:\360          to change to that directory.
```



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Owner>cd c:\360
C:\360>_
```

Next type the following command:

```
memdump_win e 12200 8 8000 orignew.bin
```

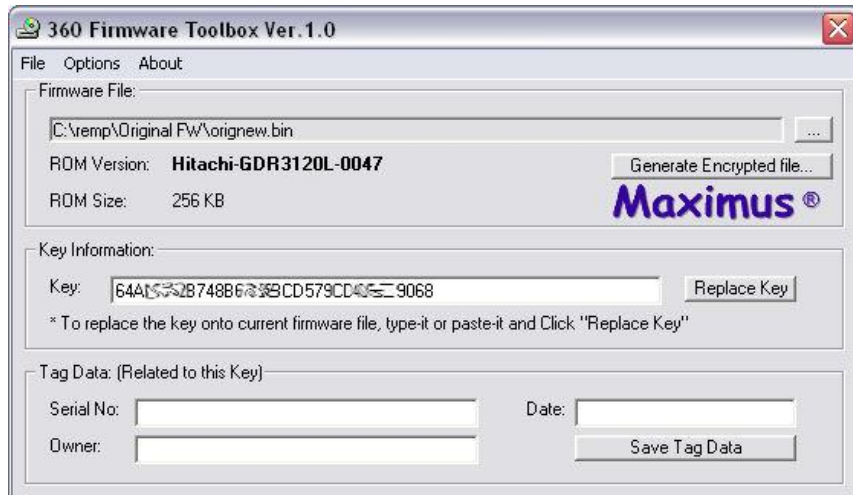


```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Owner>cd c:\360
C:\360>memdump_win e 12200 8 8000 orignew.bin
C:\360>
```

This will save a file in the directory C:\360 named orignew.bin. This is the dump of the new drive's FW.

Step 3 – Inserting the disc encryption key into the new FW

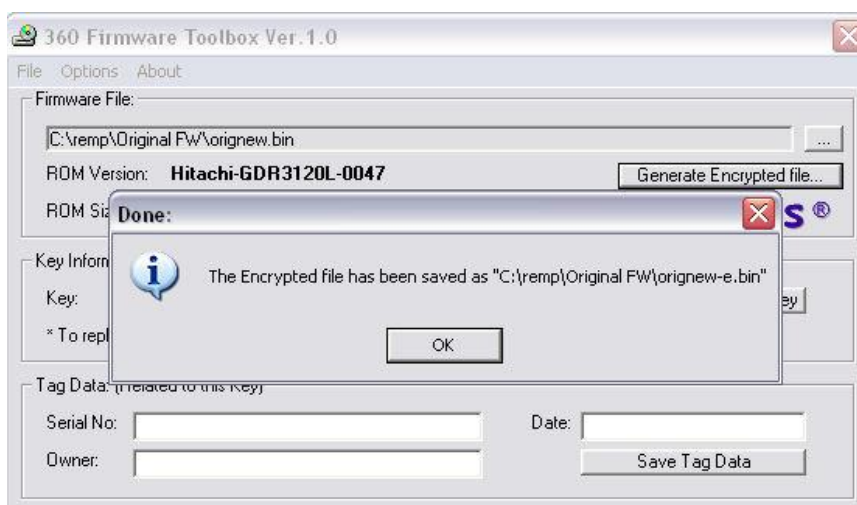
Once we have the new FW image, open 360FirmwareToolbox again and navigate to orignew.bin and open it. You will see the following screen:



Here you can now insert the original drive's disc encryption key by copy and pasting it into the box, and pressing replace key. Then press the generate encrypted file button above to generate an encrypted copy of the firmware (oddly enough!!)

The FW on the drive is encrypted, so therefore you need to encrypt any image before you flash, or you will inject an incorrect key into the drive and it will not work correctly.

Once completed, you will receive a message that a file named orignew-e.bin has been created. This is the encrypted FW image that we need for the final flash:



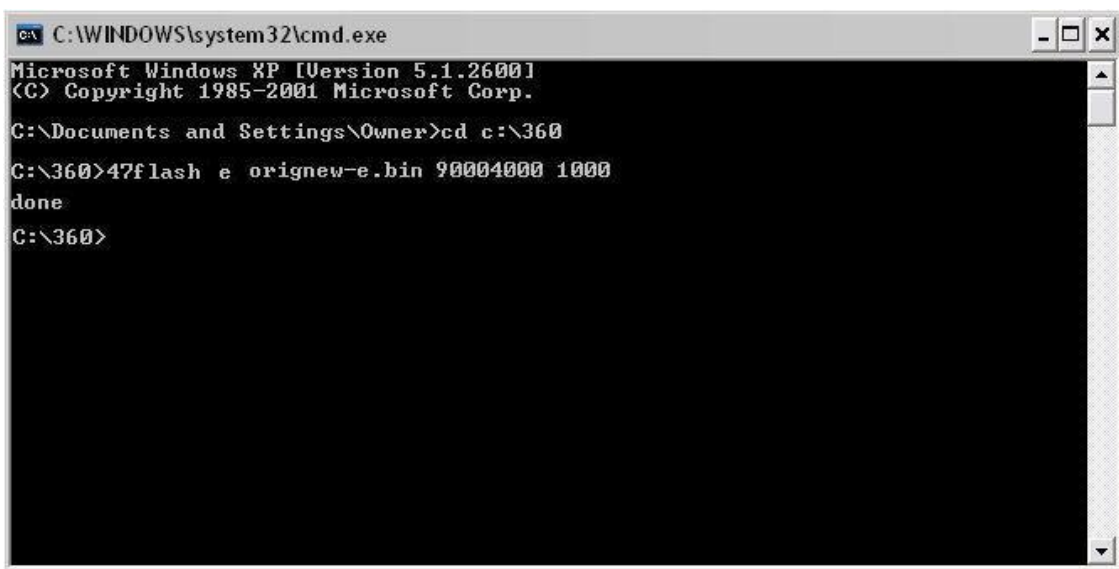
Step 4 – Flashing the new drive with the correct FW

Once we have obtained the encrypted FW image with the correct key inserted, we will then use it to inject the key into the ROM chip in the drive.

Open a command prompt and change to the dir as in step 2.

Then type the following command

```
47flash e orignew-e.bin 90004000 1000
```



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Owner>cd c:\360
C:\360>47flash e orignew-e.bin 90004000 1000
done
C:\360>
```

This injects the key only into the part of the Rom chip where the key is located.

Once completed, you will get a message saying 'done' at which point you are indeed done. Remove the DVD drive and place it into your Xbox 360, power it up and enjoy the fact that you have just resurrected a dead console.

With thanks to [Ton3] and gillife on #fw for the info, as well as Seventhson, Loser, C4eva and all the other haxors involved in the 360 modding scene.