JTAG Manager

How to use RIFF Box eMMC EFI/PIT/MBR/EBR Partitioning plugin

This plugin works with eMMC image files and phones which have following formatting:

1. Image Files or Phones with Standard Master Boot Record (MBR) and Extended Boot Record (EBR) formatting. Most of eMMC-bootable mobile phones have their eMMC memory formatted in such style. In this case partitions are accessed in standard way, by Partition ID: for example boot loader partitions or OS image partition (compare with qualcomm MIBIB partitioning: while ‘MIBIB’-type partitions have standalone partition descriptor block which contains info on all partitions and is posistioned in a definite NAND address, the eMMC partitioning is one MBR sector at fixed position + a chain of EBR sectors which are scattered throughout the eMMC address space in a literally random way);
2. Image Files or Phones which do not have standard Master Boot Record (MBR) and Extended Boot Record (EBR) formatting, but instead, partition information for such phones is taken from the PIT Table (some Samsung phones);
3. Image Files or Phones which do not have standard Master Boot Record (MBR) and Extended Boot Record (EBR) formatting, but instead, partition information for such phones is taken from the EFI Table (some Samsung, LG, Pantech and other phones).

Most of eMMC-bootable mobile phones have their eMMC memory formatted in such style. In this case partitions are accessed in standard way, by Partition ID:

For example boot loader partitions or OS image partition (compare with qualcomm MIBIB partitioning: while ‘MIBIB’-type partitions have standalone partition descriptor block which contains info on all partitions and is posistioned in a definite NAND address, the eMMC partitioning is one MBR sector at fixed position + a chain of EBR sectors which are scattered throughout the eMMC address space in a literally random way).

This plugin is a powerfull tool which enormously simplifies resurrection process (providing you have the required boot files from an official firmware or you have a ‘donor’ device) for those devices which are not yet supported by a dedicated resurrector DLL.

In this manual, we will explain basic functions of plugin, and how to use it to repair, unlock or do forensic investigation on supported phones.

This plugin supports following CPU/eMMC combinations:

- MSM7230, with eMMC as boot memory
- MSM8255, with eMMC as boot memory

- MSM8255T, with eMMC as boot memory
- MSM8655, with eMMC as boot memory
- MSM8655T, with eMMC as boot memory
- MSM8260, with eMMC as boot memory
- MSM8260A, with eMMC as boot memory
- MSM8660, with eMMC as boot memory
- MSM8660A, with eMMC as boot memory

- APQ8060, with eMMC as boot memory
- MSM7225A with eMMC as boot memory

- MSM7227A with eMMC as boot memory

- MSM7667A with eMMC as boot memory

- MSM8960 with eMMC as boot memory

- APQ8064 with eMMC as boot memory
- MSM8225 with eMMC as boot memory
- Samsung Exynos 4212 with eMMC as boot memory

- Samsung Exynos 4412 with eMMC as boot memory

- Samsung Exynos 3110 with eMMC as boot memory

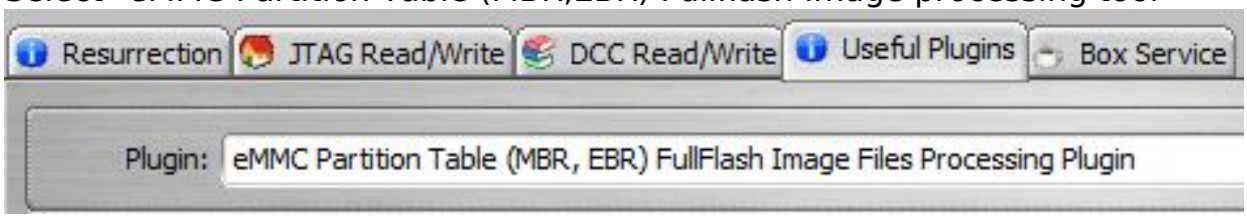
- Samsung Exynos 4210 with eMMC as boot memory

You can check list of models based on specific CPU if You click "Browse Devices Based On . . .".

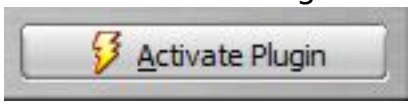
Links and CPU information provided by PDADB.net

To start the plugin, follow this procedure:

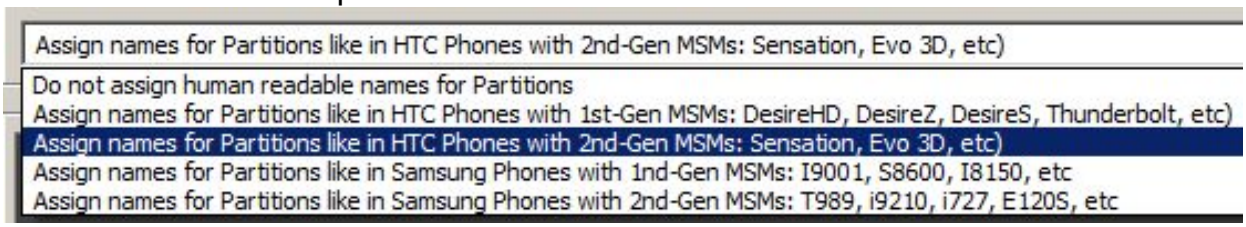
- Launch RIFF Box JTAG Manager
- Select desired Brand/Model DLL (Or corresponding one)
- Go to "Useful Plugins" TAB
- Select "eMMC Partition Table (MBR,EBR) Fullflash Image processing tool



- Click "Activate Plugin"



- Now You have plugin interface started. Select which type of Human Readable names for partitions You want to use:



There are two ways You can use this plugin now:

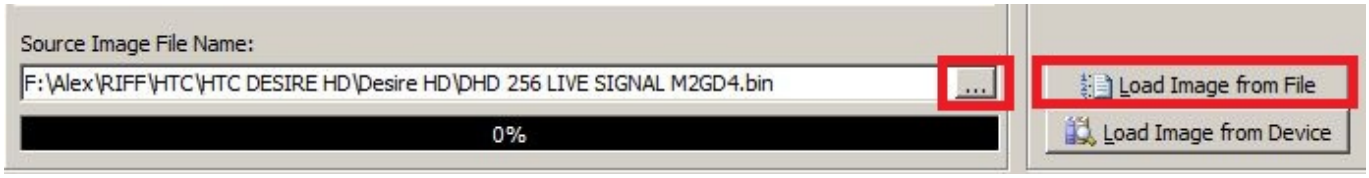
- Work with Flash Image from file
- Work with Flash Image from connected device

With Flash Image file You have many useful functions:

- Load partitions structure
- Save partitioning structure to single file, to be used with blank chips
- Check for blank partitions
- Save all or single partitions into separate files
- Replace single partitions inside full or partial image and save as new file
- Examine partitions content with integrated Hex Viewer
- Play smart with friends who don't own a RIFF Box
- Re-Partition new or erased eMMC on any device based on supported CPU-s platform
- Repair bricked or partially damaged any device based on supported CPU-s platform
- Write any partition(s) to any device based on supported CPU-s platform

How to Load partitions structure:

- Open source file
- Click "Load Image from file"



In this example, partial flash image is used. (256MB from HTC Desire HD)

We can see partitions structure now:

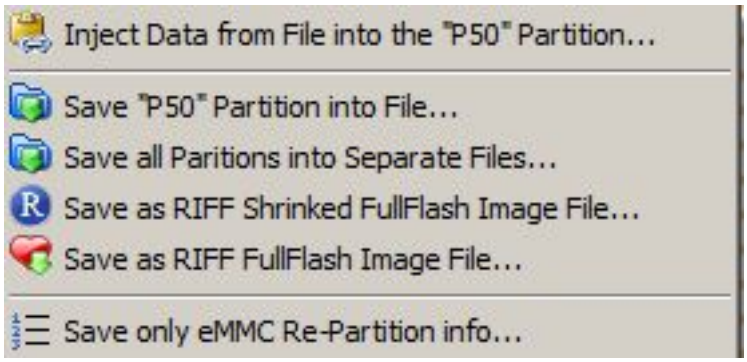
#.	S.		Partition Id	Starting Offset	Size in Bytes
1		YES	P4D_DBL	0x0000 0000 0200	0x0000 0007 D000
2		NO	P45	0x0000 0007 D200	0x0000 0001 0000
3		NO	P46_OSBL	0x0000 0008 D200	0x0000 0046 5000
4		NO	P49_AMSS	0x0000 004F 2400	0x0000 01D4 C000
5		NO	P50	0x0000 0223 E600	0x0000 00C3 5000
6		NO	P51_HTC	0x0000 02E7 3800	0x0000 0020 0000
7		NO	P52	0x0000 0307 3A00	0x0000 0030 0000
8		NO	P53	0x0000 0337 3C00	0x0000 0020 0000
9		NO	P54	0x0000 0357 3E00	0x0000 0010 0000
10		NO	P56	0x0000 0367 4000	0x0000 0010 0000
11		NO	P55	0x0000 0377 4200	0x0000 0088 BE00
12		NO	P4A	0x0000 0400 0200	0x0000 0030 0000
13		NO	P4B	0x0000 0430 0400	0x0000 0030 0000
14		NO	P74	0x0000 0460 0600	0x0000 0010 0000
15		NO	P75	0x0000 0470 0800	0x0000 008B F600
16		NO	P76_MISC	0x0000 04FC 0000	0x0000 0004 0000
17		NO	P47_SPL	0x0000 0500 0200	0x0000 0010 0000

We have list of present partitions now, and we can see many information - partition names (if assigned) starting address, size, and if partition is active or no. Active partition is first boot partition in phone, and it's responsible for boot sequence. In this particular model, these are boot partitions:

- DBL (Initial Boot)
- OSBL (Radio Boot)
- SPL (HBOOT)

How to Save partitioning structure to single file, to be used with blank chips

Right click to any of listed partitions will bring context menu:

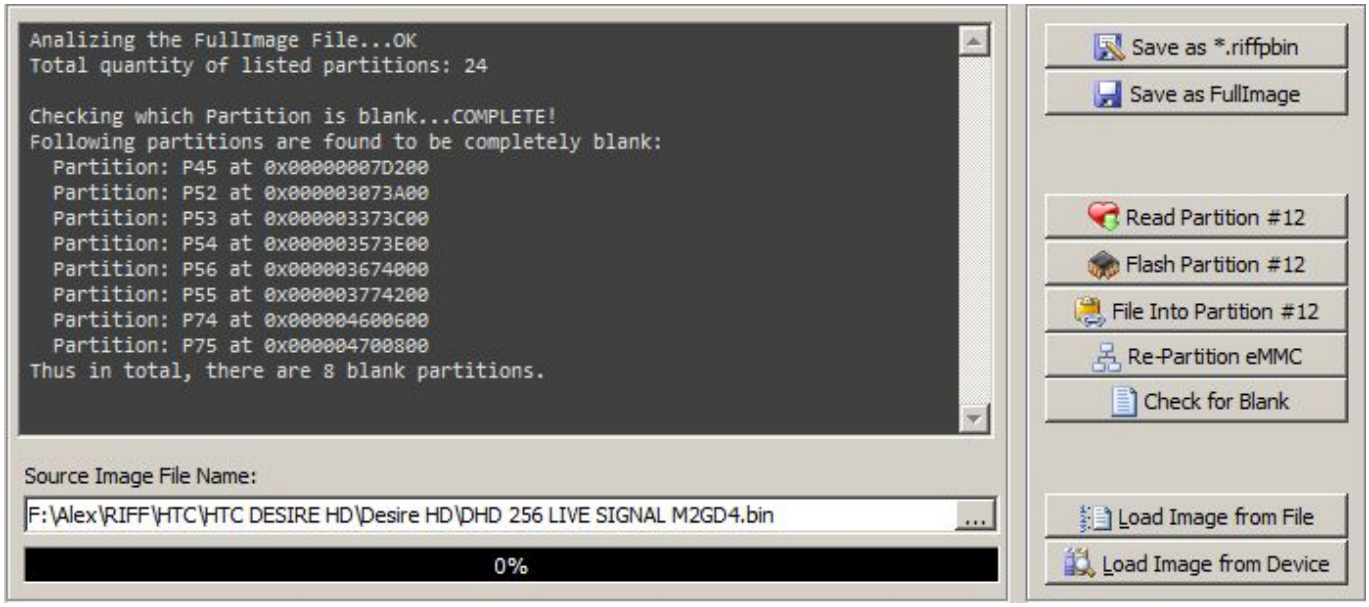


Select "Save only eMMC Re-partition info" . This will save "partition table", which can be used late for blank (erased or new) eMMC chips. **Take note, only file saved from working fullflash image is valid.**

How to Check for blank partitions:

To decrease required time when flashing flash image to phone, You can check if there are some blank partitions, thus skipping them will shorten the required time. Or - in case that You're analyzing full flash image from not working phone, You can see if there is any partition empty.

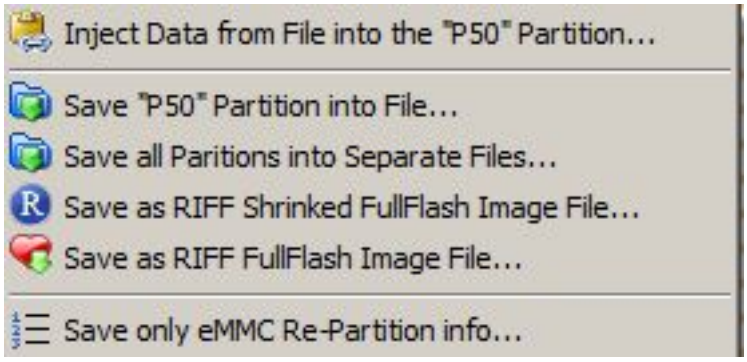
After You load flash image, click "Check for Blank" button. Flash image file will be analyzed and result shown in logging window:



How to Save all or single partitions into separate files:

Right click to any listed partition will bring the context menu. Select option You

want to use.



If You select to save single all partitions, You'll need to enter prefix for file name(s). It will help You later, so You wont mix it with files from another model:

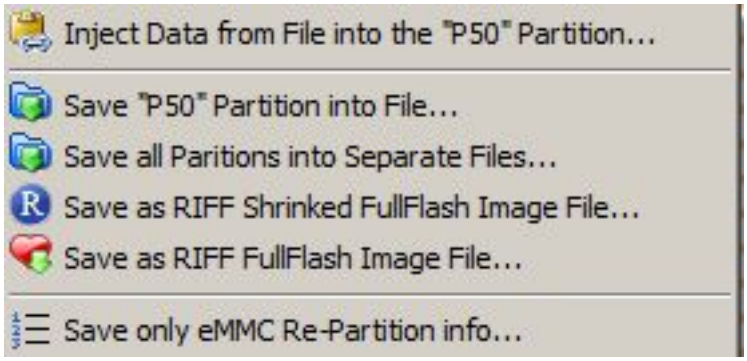
Files will be saved in following name structure:

Prefix_startaddress_partition_name. Example:

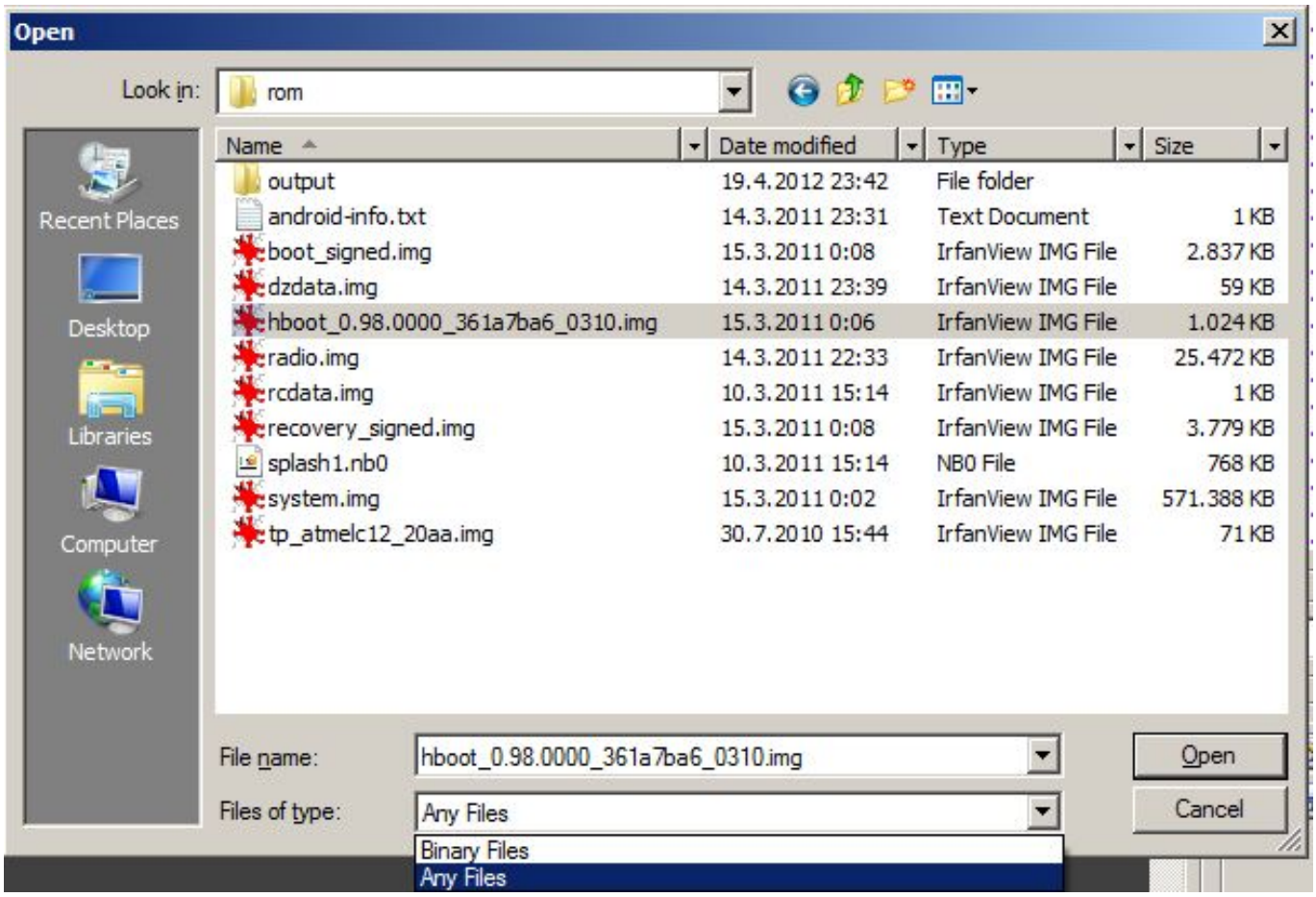
HTC_Desire_HD_000005FC0000_P73_WLAN.bin

How to Replace single partitions inside full or partial image and save as new file:

Right click to selected partition will bring the context menu. Select "Inject Data from file into the "selected" partition"



A file open dialog will popup where You can select source file. In this example, we will use HBOOT for HTC Desire S, from ROM.zip package:



As You can see, You can use two file open filters.

- Binary files (*.bin)

- Any Files (*.*)

With this method, we can build flash image from RUU *.zip package. For example You have model which is not officially supported, but You can connect it either via JTAG or via USB cable. Presuming that phone has only HBOOT damaged/erased, You can make fully working flash image now.

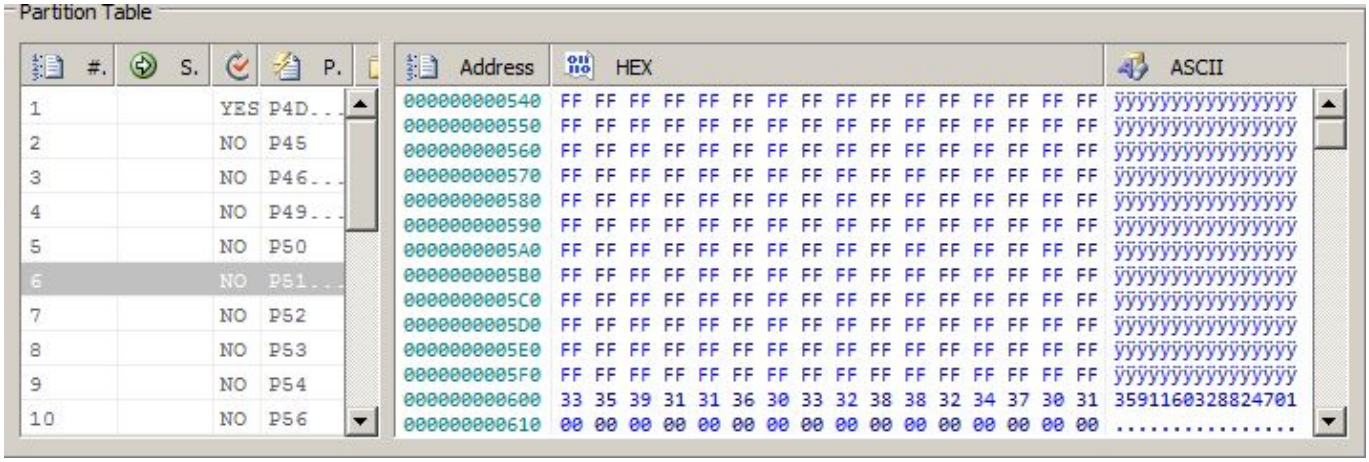
You can save newly built image using two methods:

- Save as *riffpbin (compressed image format)

- Save as FullImage

How to Examine partitions content with integrated Hex Viewer:

That's prety simple - once You select partition, it's content is show in hex viewer window. In bellow screenshot, You can see content of HTC Desire Z HTC partition with IMEI number:



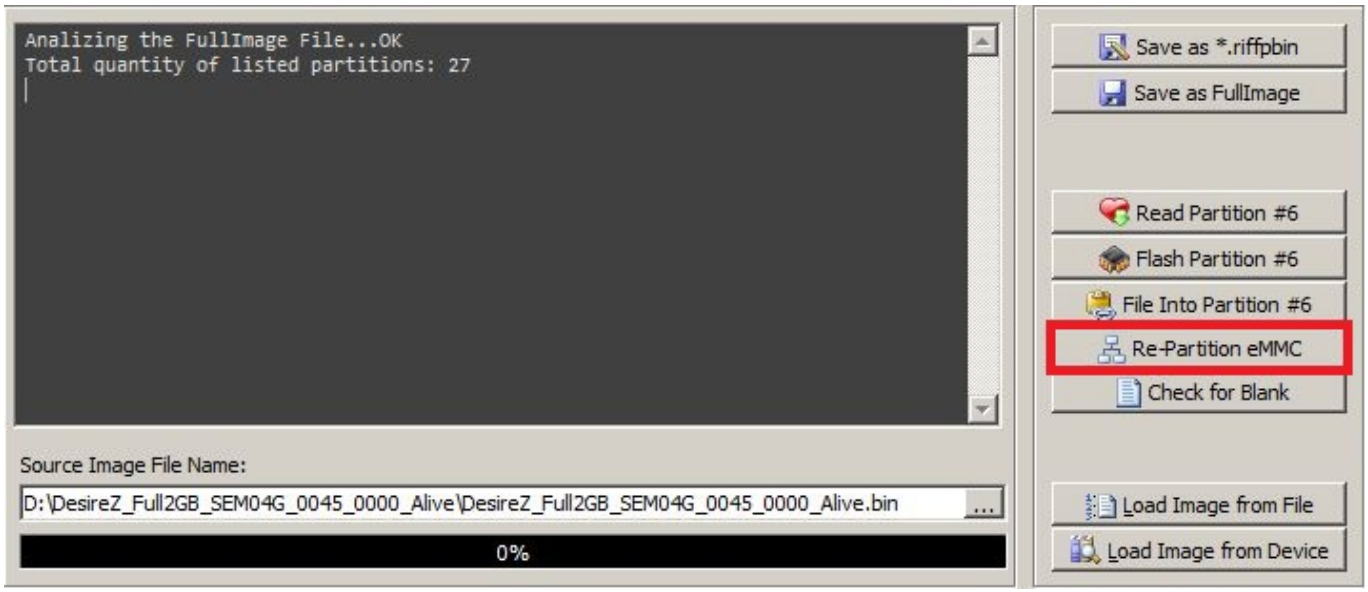
How to Repartition new or erased eMMC on any device based on supported CPU-s platform:

Since eMMC chips can sustain damages - in many cases they need to be replaced. Most notorius eMMC chip is M4G2DE **-** as You can see, Google search returns many results, mostly with problems. This chip was widely used in early eMMC based HTC mobile phones - HTC Desire S, HTC Desire Z, etc. Once You replace this damaged chip, You need to perform two operations:

- Re-Partitioning

- Repair boot areas and security

To Re-partition eMMC chip, load image from full flash, or fom previously saved partitioning file, and simply click "Re-Partition eMMC":



How to Repair bricked or partially damaged any device based on supported CPU-s platform:

Depending on phone brand and platform, there are different list of partitions to be restored. Basically, it can be devided in few groups. In this manual, HTC Android models are covered:

HTC Models, based on MSM7230, MSM8255, MSM8255T, MSM8655, MSM8655T: (SnapDragon S2)
Boot partitions: (Required)

- DBL
- OSBL
- SPL (HBOOT)

Android partitions: (Optional)

- Recovery
- Boot

Security, calibration and hw_config info: (**To be flashed only in case that nothing else helps, or in case where eMMC is blank**)

- HTC
- MISC
- WLAN
- SPLASH1

HTC Models, based on MSM8260, MSM8660, APQ8060 and derivates (SnapDragon S3)

Boot partitions: (Required)

- DBL (SBL1)
- SBL2
- SBL3
- RPM
- TZ
- HBOOT

Android partitions: (Optional)

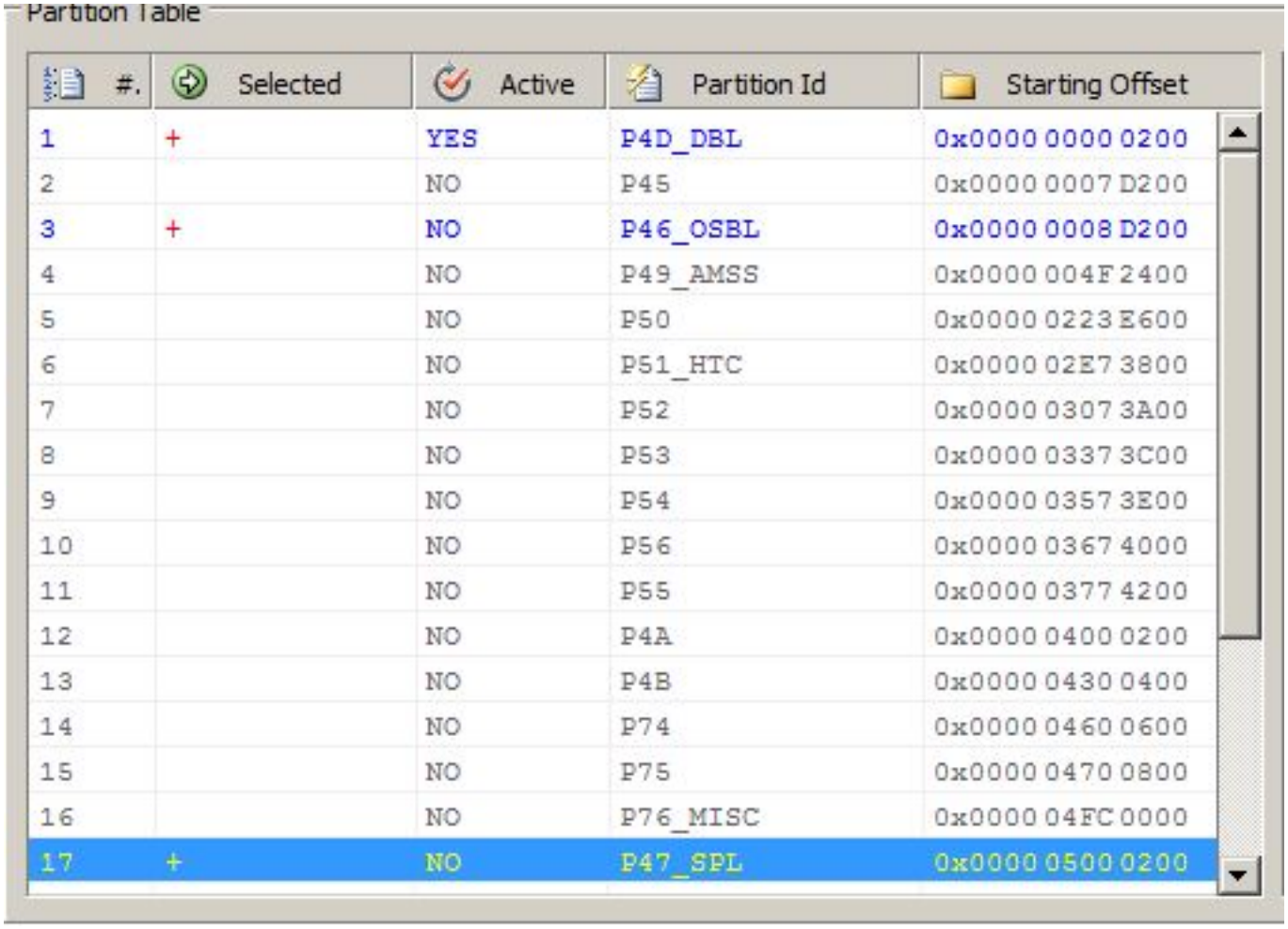
- Recovery
- Boot

Security, calibration and hw_config info: (**To be flashed only in case that nothing else helps, or in case where eMMC is blank**)

- P5D (PGFS)
- ID
- WLAN
- P76_MISC
- HTC
- SPLASH1

Load working flash image, or image You built from partitioning file and files from RUU package.

Select desired partitions by double click on partition list:


Partition Table

#.	Selected	Active	Partition Id	Starting Offset
1	+	YES	P4D_DBL	0x0000 0000 0200
2		NO	P45	0x0000 0007 D200
3	+	NO	P46_OSBL	0x0000 0008 D200
4		NO	P49_AMSS	0x0000 004F 2400
5		NO	P50	0x0000 0223 E600
6		NO	P51_HTC	0x0000 02E7 3800
7		NO	P52	0x0000 0307 3A00
8		NO	P53	0x0000 0337 3C00
9		NO	P54	0x0000 0357 3E00
10		NO	P56	0x0000 0367 4000
11		NO	P55	0x0000 0377 4200
12		NO	P4A	0x0000 0400 0200
13		NO	P4B	0x0000 0430 0400
14		NO	P74	0x0000 0460 0600
15		NO	P75	0x0000 0470 0800
16		NO	P76_MISC	0x0000 04FC 0000
17	+	NO	P47_SPL	0x0000 0500 0200

As You can see, selected partitions will be marked with "+" sign. Now simply click "Flash Selected" button and wait for process to be finished. Presuming that only boot partitions were damaged, You should be able to enter hboot mode and update phone ROM with RUU executable.

How to Write any partition(s) to any device based on supported CPU-s platform

If You, for any reason, need to write specific partition from one phone to another, follow this procedure:

- Load previously readed flash image
- Select partition(s)
- Click "Flash Selected"

Work with Flash Image from connected device

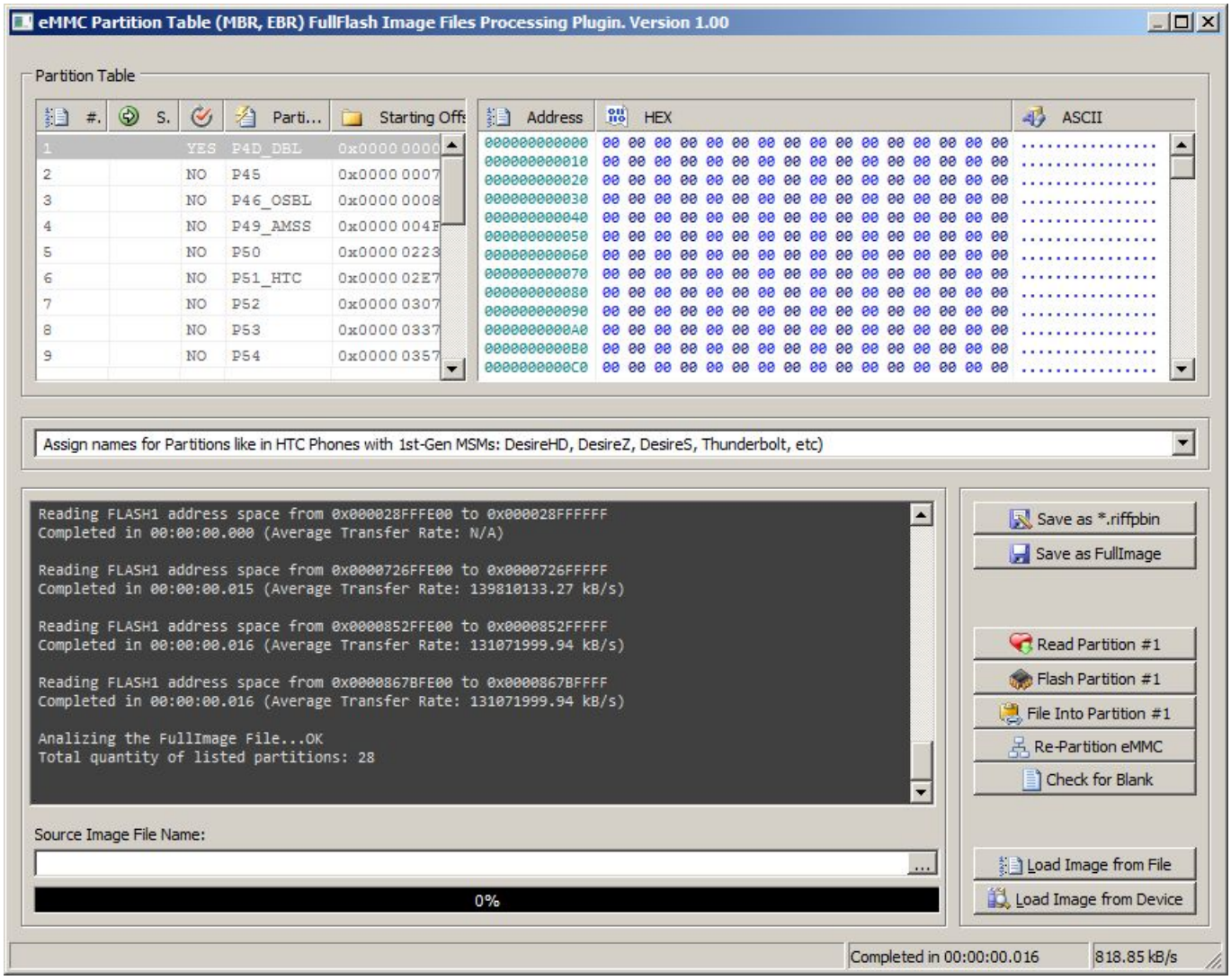
JTAG Manager

There is a number of useful functions You can use with connected device:

- Read and save Partitioning info and structure (To be used later with blank eMMC)
- Read and examine single partitions from device in Hex Viewer
- Read and save single or all partitions from device to separate files
- Read all partitions and save it in compressed *.riffpbin format
- Read all partitions and save as full image
- Replace partition content with external file and write it to device
- Null erase single or all partitions in connected device

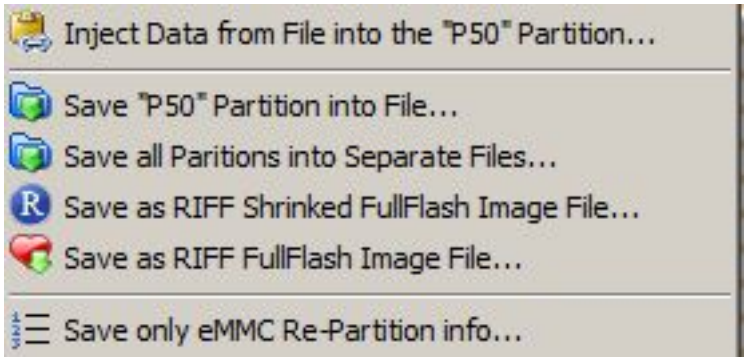
How to Read and save Partitioning info and structure:

Click "Load Image from Device" button. Device partitioning will be readed and shown in plugin interface:



At this point an empty flash image will be created, filled with 00 00. Remember, this is just "placeholder" for actual flash content, and not a valid flash image.

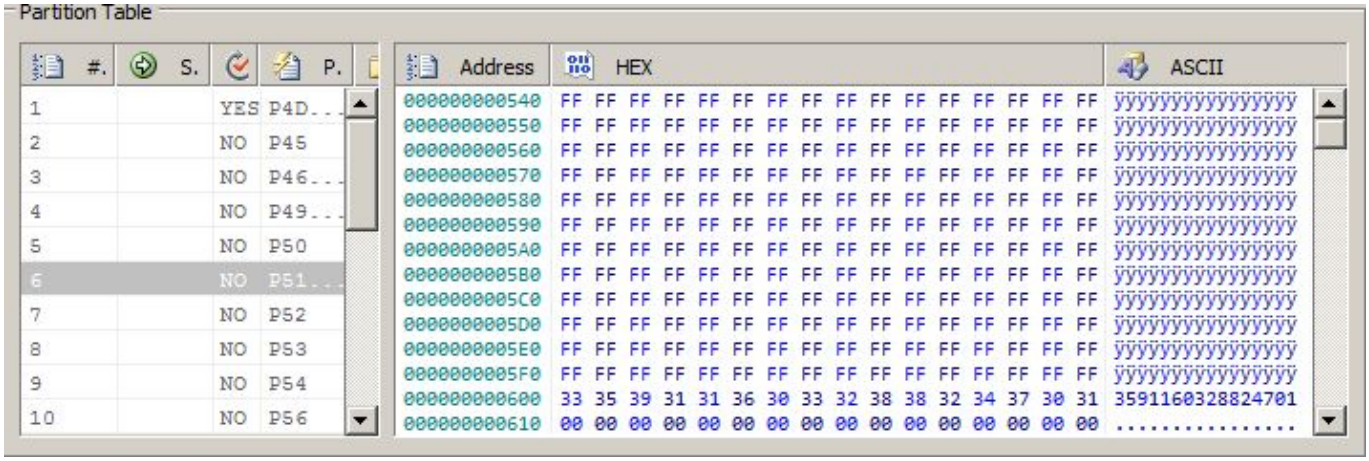
To save partitioning info, right click to any partition and select "**Save only eMMC Re-partition info**"



This will save "partition table", which can be used later for blank (erased or new) eMMC chips. **Take note, only file saved from working device is valid.**

How to Read and examine single partitions from device in Hex Viewer

Select desired partition, and click "Read Partition #". Partition content will be readed from device, and shown in Hex View window: On screenshot bellow, You can see content of HTC Desire Z HTC partition with IMEI number:



How to Read and save single or all partitions from device to separate files

Unique solution ID: #1052
Author: Legija

JTAG Manager

Last update: 2013-05-17 17:15