

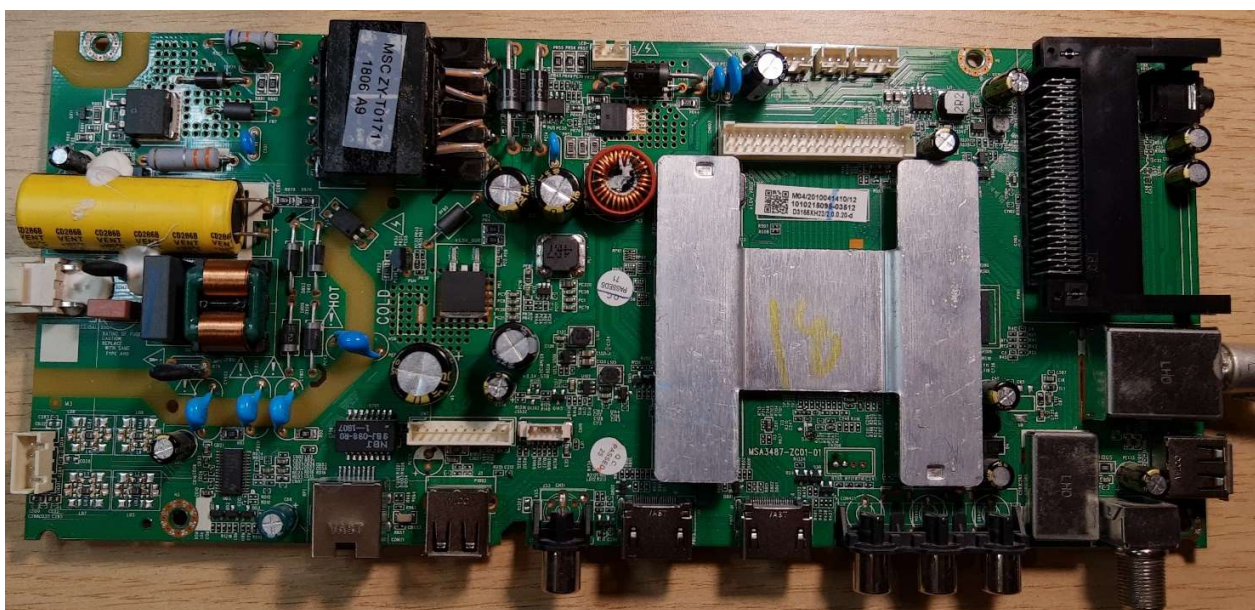
Замена чипа eMMC и восстановление ПО SMART-телевизоров, построенных на ARM-процессорах Mstar, на примере шасси MSA3487-ZC01-001 с помощью программатора RT809H.

1. Общая информация.

Линейка шасси MSA348х... используется в бюджетных SMART телевизорах под управлением ОС Android.

Шасси построено на процессоре MSD6A348AX0 в связке с микросхемой памяти eMMC 5.1 KLM8G1GEME-B041 ёмкостью 8 ГБ и DRAM 4B4G1646E объёмом 512 МБ (ещё 512 МБ находятся в самом процессоре).

Общий вид шасси:



Плата имеет встроенный источник питания от сети 220 В, драйвер led подсветки на микросхеме OV3350CP, слот CI+ (под которым расположен декодер MSB102KA и его SPI флешь MX25L4006E), цифро-аналоговый тюнер, спутниковый тюнер, а также набор различных входов источников сигналов, USB и Ethernet. Присутствуют разъёмы для подключения подсветки, кабеля LVDS, модуля WI-FI, модуля управления и индикации, громкоговорителей.

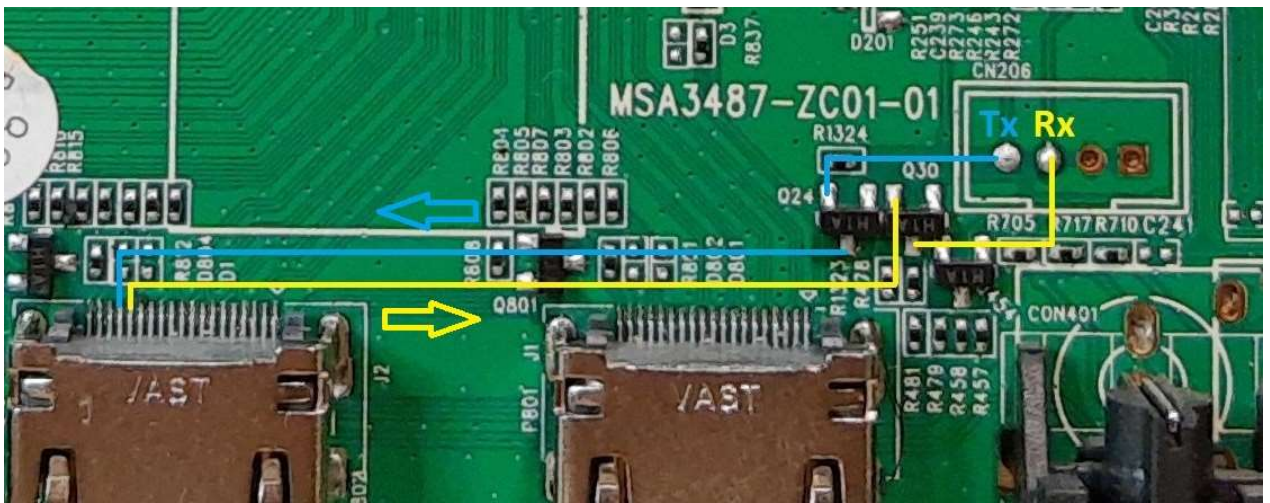
На плате присутствуют следующие напряжения:

- PD15+PD16 (22,5 V для питания подсветки)
- PD3 (12,6 V основное)
- PU2 (SMD marking code 3201) - 5,0V
- U2 (SMD marking code SIK) - 1,17V
- U5 (RT5047A) - 19,6V

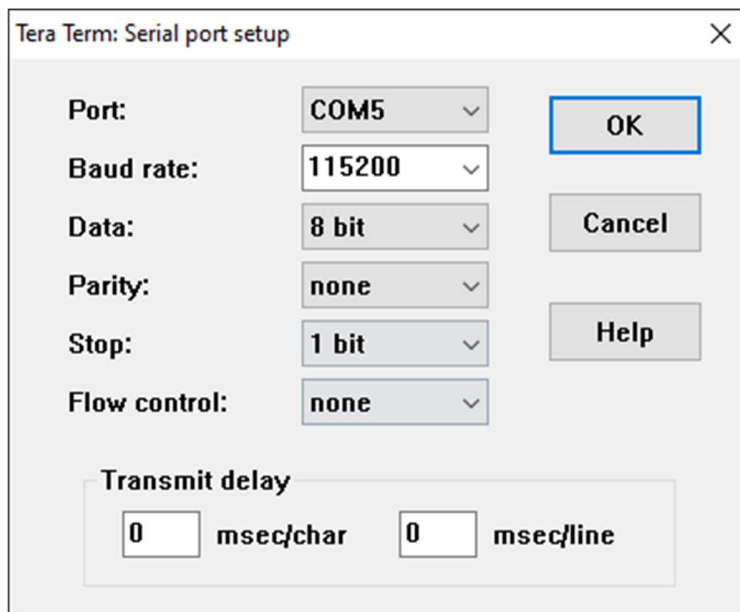
U15 (TPS54528) - 1,05V
U102 (SIK) - 3,35V
U104 (MSH6110A) - 1,0V
U106 (SIK) - 1,5V
U111 (1117-adj) - 1,8 V

2. Порт UART

Порт UART выведен на не распаянный 4-pin разъём CN206, с которого через транзисторы Q30, Q24 выведен на pin 15,16 HDMI-2 (а также на pin 2,14 того же HDMI-2). Программатор RT809H имеет аналогично распаянный (pin 15,16) порт HDMI, что делает возможным подключение его к шасси MSA3487 обычным кабелем HDMI, используя программатор в качестве эмулятора COM порта для диагностики и работы с платой через консоль Mstar.



Для работы через UART необходима установленная на компьютере соответствующая программа, например TeraTerm со следующими настройками:



3. Диагностика eMMC.

Одной из неисправностей данной линейки шасси является сбой программного обеспечения по различным причинам, или выход со строя чипа eMMC KLM8G1GEME-B041, о чём с большой вероятностью можно судить по следующим признакам: на плате присутствуют все необходимые напряжения, светодиод индикации дежурного режима не светится, экран не светится, телевизор на кнопки и пульт не реагирует, нет обмена на шинах данных процессора и нет вывода информации в порт UART, но есть повторяющиеся стартовые импульсы на выводе Reset (R523) и есть генерация на кварце 24.0 МГц.

Для диагностики eMMC прежде всего необходимо подключиться к плате терминалом по UART. При наличии любой информации в логе можно диагностировать работоспособность eMMC, сбой находящегося в ней ПО и попробовать его восстановить, используя инструменты консоли Mstar, либо подпаявшись к eMMC по ISP и перепрошить её проверенным дампом.

При отсутствии информации по UART следует подключиться к eMMC по ISP, для чего достаточно закоротить один из выводов кварца 24.000 МГц на GND и подключить кабель ISP программатора к точкам GND, CLK, CMD и D0, согласно фото.

Для питания eMMC по ISP мощности внутренних источников RT809H по цепям 3,3 и 1,8 вольт недостаточно, поэтому необходимо подать внешнее питание с ЛБП +12,5В на катод диода PD3 (напряжение 3,3 и 1,8 сформируются автоматически). Или подать +3,3 В, согласно фото ниже, либо просто включить кабель питания платы в розетку 220В, соблюдая необходимые меры электробезопасности.

Фото нижней стороны платы:

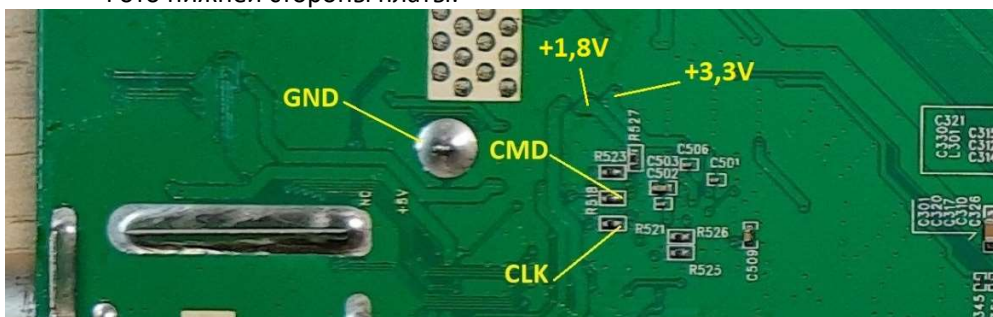
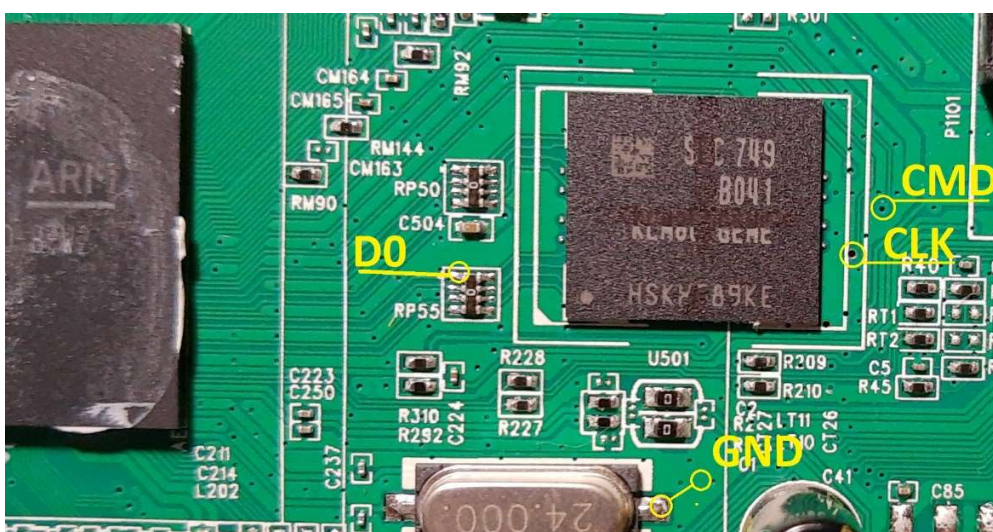
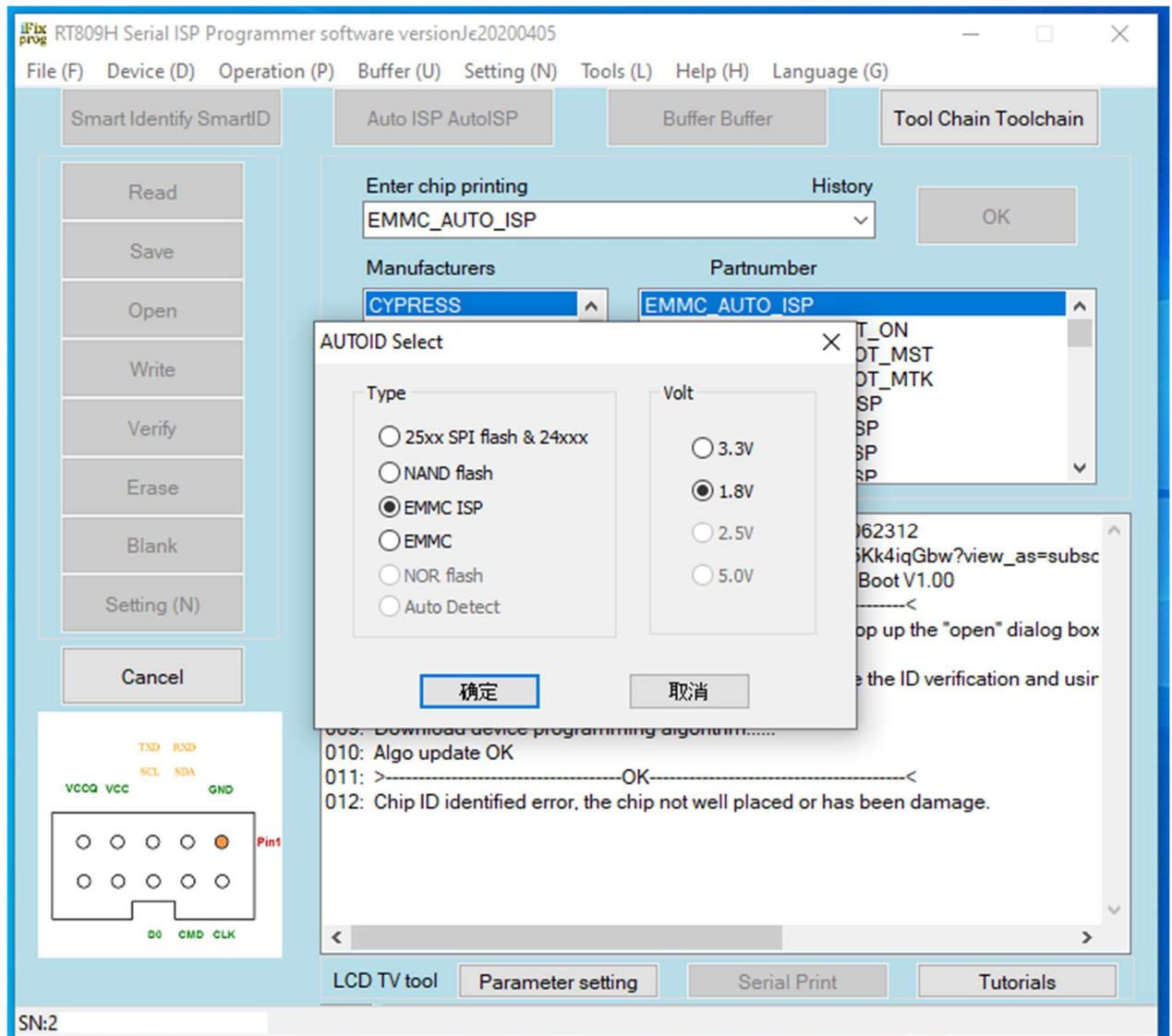


Фото верхней стороны платы, CMD и CLK есть с обеих сторон, D0 только с верхней:



Если подпаиваетесь к резисторам, то рекомендуется произвести замер их сопротивлений, так как при пайке эти резисторы часто обрываются, а после пайки убедиться в исправности резисторов.

Для считывания eMMC в настройках программатора надо выбрать соответствующую микросхему (либо просто нажать **Smart identify SmartID**) и указать напряжение шин данных 1,8 В:



После чего попробовать считать eMMC нажав кнопку «Read».

В случае успешного подключения и рабочей микросхеме eMMC, программатор определит параметры eMMC и откроет окно с предложением сохранить дамп. В этом случае можно просто переписать её рабочим дампом или загрузить стартовое ПО (о нём речь ниже).

Сообщение в логе программатора вида:

033: VCCIO: 1.8V

034: Read timeout.

укажет о неисправности eMMC, при условии правильного подключения к ней.

В этом случае eMMC подлежит замене.

4. Замена eMMC.

Чип KLM8G1GEME-B041 расположен между процессором и слотом CI+ под правым крылом радиатора, в связи с чем доступ к чипу затруднён.

Радиатор припаян в двух точках к плате и приклеен к процессору термоклеем (который при нагреве не очень размягчается) в связи с чем его демонтаж затруднён, но при определённых навыках и опыте мастера эта процедура трудностей не вызывает. Простой отрыв радиатора грозит отрывом пятачков BGA.

Для демонтажа радиатора каждый мастер использует свой метод, кто-то довольно значительно нагревает и отрывает радиатор, надеясь, что повезёт и пайка BGA не нарушится, кто-то просто вырезает часть или полностью крыло радиатора, как на фото:

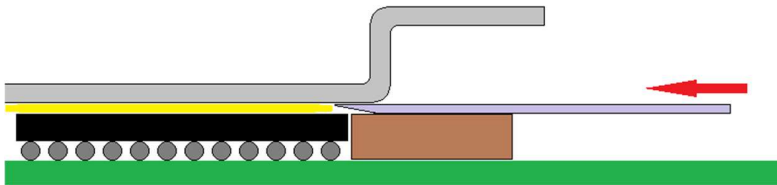


Лично я использую самодельную гибкую стальную стамеску, изготовленную из полотна большого канцелярского ножа), которой скалываю (срезаю) радиатор с процессора:



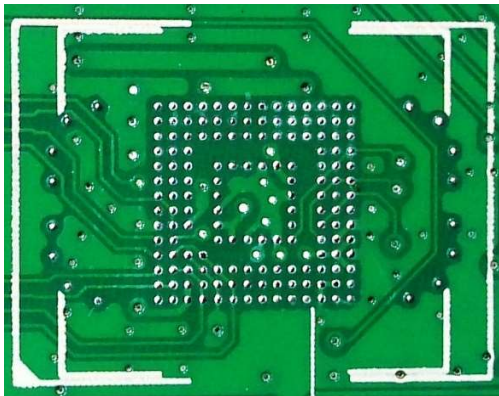
Предварительно следует отпаять точки крепления радиатора к плате, или можно просто нагреть припой, приподнять крылья радиатора на 1-2 мм и оставить в таком положении, как бы дать натяг.

Затем аккуратно вставляю между радиатором и процессором лезвие стамески и немного вдавливаю его. Главное не попасть в торец процессора, либо в шары, для чего можно подложить кусочек пластика подходящего размера, но я приловчился и без подложки. Убедившись, что лезвие вошло правильно, аккуратными, короткими ударами молоточка по стамеске, скалываю радиатор, что не наносит пайке BGA абсолютно никакого ущерба.



Замена eMMC с нижним подогревом на 130 - 140 C° не вызывает затруднений, метки соответствуют габаритам микросхемы.

Фото платы под eMMC:



Радиатор потом не обязательно обратно приклеивать, можно посадить на термопасту или термопрокладку. Без радиатора процессор ощутимо нагревается.

5. Восстановление программного обеспечения.

При наличии проверенного дампа всё значительно упрощается, дамп можно записать в eMMC ещё до запайки её в плату, предварительно произведя конфигурацию eMMC (байтов 162, 177 и 179 раздела ExtCSD):

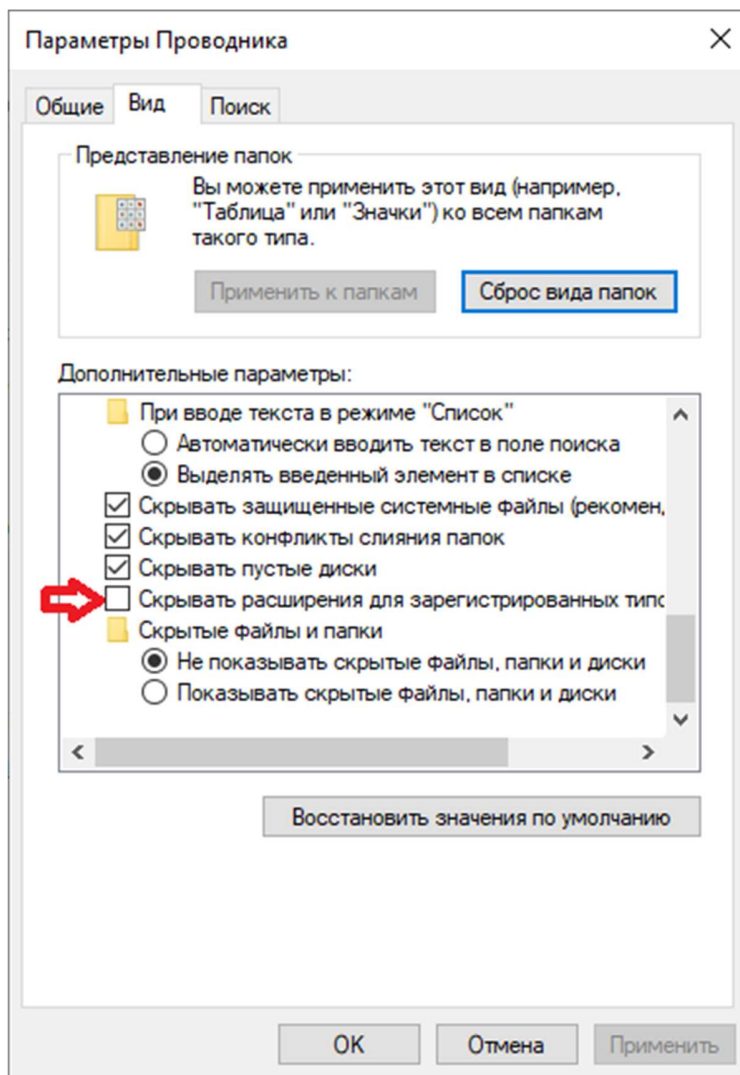
162 – 01 (вывод Reset задействован);

177 – 0A (ширина шины данных во время загрузки, некритично, можно 02);

179 – 08 (загрузка с Boot1).

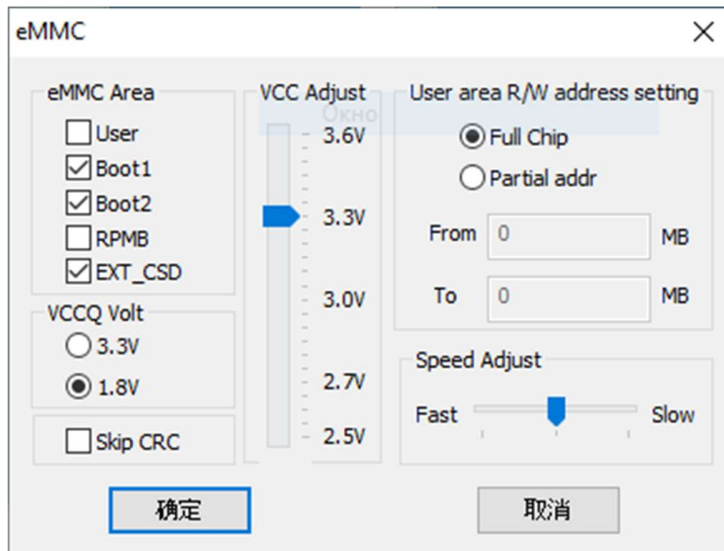
При отсутствии дампа необходимо наличие USB прошивки ремонтируемого аппарата, которую лучше всего получить, отправив соответствующий запрос с указанием серийного номера производителю телевизора. Прошивка должна быть полной, содержать все разделы, а не только обновление некоторых разделов. К счастью подавляющее большинство прошивок содержат всё необходимое нам.

Прежде всего, во избежание недоразумений с отображением наименований файлов, настроим Windows. В «Панели управления», выберем «настройку Проводника» (вида папок) и уберём галку с пункта «Скрывать расширения для зарегистрированных типов файлов»:







Так как RT809H не может выборочно прописывать байты конфигурации eMMC, то для этого считываем с новой микросхемы раздел ExtCSD и обязательно Boot1, Boot2. Это можно сделать хоть на программаторе, через адаптер BGA153, хоть после запайки eMMC, подпаявшись к ней по ISP.

Настройки программатора при этом должны быть следующими:



Считав новую eMMC, получим четыре файла. Файл раздела User тоже будет присутствовать, не смотря на снятую галку, но его размер будет 0 байт.

-  KLM8G1GEME-B041_ISP_5231.BIN
-  KLM8G1GEME-B041_ISP_5231.BIN.BOOT1
-  KLM8G1GEME-B041_ISP_5231.BIN.BOOT2
-  KLM8G1GEME-B041_ISP_5231.BIN.EXT_CSD

После чего открываем файл **KLM8G1GEME-B041_ISP_5231.BIN.EXT_CSD** любым Hex-редактором. В этом примере я буду использовать редактор HxD, но подходит практически любой.

Для удобства отображения адресации байтов в десятичном формате (d) кликаем мышкой на заголовке столбца адресов Offset (h), а далее просто редактируем в окне программы байты 162,177 и 179 под наши значения, кликая по ним мышкой.

Offset (d)	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	Текст декодирован
00000000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000016	39	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	9.....
00000032	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000048	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000064	0F	00	00	C8	C8	00	00	00	00	00	00	00	00	00	00	00	...ИИ.....
00000080	00	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00
00000096	00	00	00	00	00	05	00	00	00	00	00	00	00	00	00	00
00000112	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000128	00	00	01	00	00	00	00	00	00	00	00	00	00	00	00	00
00000144	00	00	00	00	00	00	00	00	00	00	00	00	00	D2	01	00Т..
00000160	07	00	01	00	00	00	14	1F	04	00	00	00	00	00	00	00
00000176	00	0A	00	08	00	00	00	00	01	01	00	00	00	00	00	00
00000192	08	00	02	00	57	1F	0A	02	00	00	00	00	00	00	00	00	...W.....
00000208	00	00	00	01	00	00	E9	00	07	11	00	07	07	10	01	01й.....
00000224	01	07	20	00	07	11	1B	55	02	00	00	00	00	00	00	00U.....
00000240	00	1E	00	00	00	00	00	3C	0A	00	00	01	00	00	06	00<.....
00000256	00	00	00	00	00	00	00	00	01	08	00	01	02	02	00	00
00000272	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000288	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000304	00	00	00	0F	01	00	00	00	00	00	00	00	00	00	00	00
00000320	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Сохраняем отредактированный файл в родную папку с родным именем. Кроме этих четырёх файлов в папке не должно быть ничего постороннего.

Записываем комплект файлов Boot1, Boot2 и ExtCSD обратно в eMMC не изменяя настроек программатора.

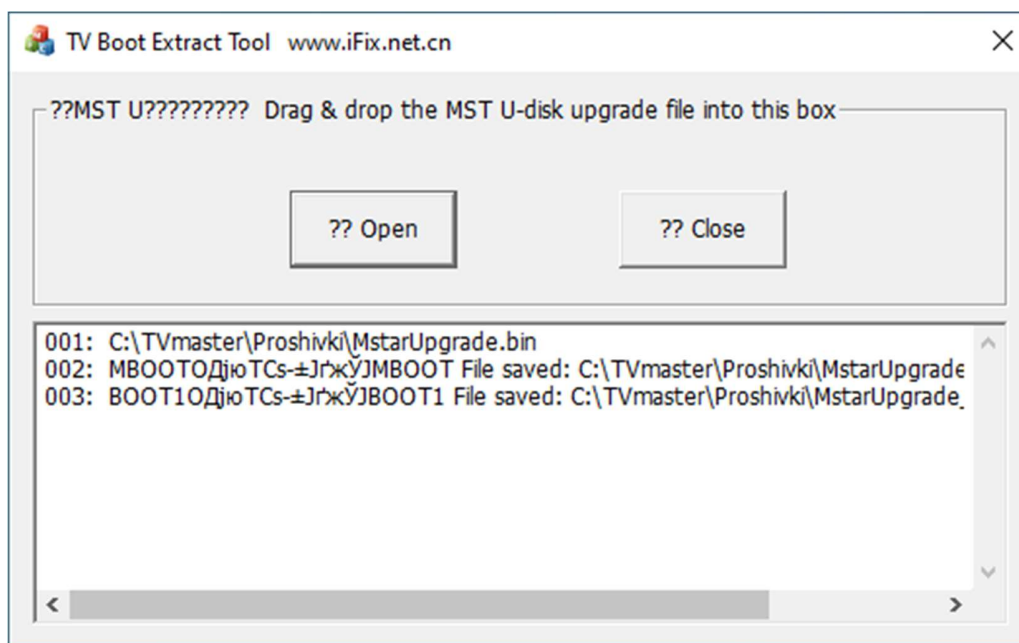
На этом конфигурация новой eMMC завершена.

Для проверки успешной записи байтов конфигурации следует обратно считать eMMC и проверить их значения hex-редактором.




Следующим шагом будет извлечение файлов загрузчиков **sboot.bin** и **Mboot.bin** из USB прошивки и запись их в eMMC с целью формирования стартового ПО для дальнейшей прошивки телевизора уже с флешки через порт USB.

Для этого воспользуемся встроенной утилитой **TV Boot Extract.exe**, расположенной в папке программатора **RT809H\TOOLS\TV Boot Extract.exe** и на которую сильно ругается антивирус, но лично мне утилита неприятностей пока что не принесла. Если вы не можете найти эту программу у себя на компьютере, то скорее всего антивирус удалил, или поместил её в карантин. Эта программа по умолчанию входит в установочный пакет программы RT809H.

Запускаем программу **TV Boot Extract.exe** и открываем ею USB прошивку, нажав кнопку «Open» указав её расположение (можно просто перетянуть прошивку на кнопку «Open»):



После чего в папке с прошивкой, кроме самой прошивки, появятся дополнительно ещё два файла размером 1704 кБ и 78 кБ:

 MstarUpgrade.bin	20.03.2020 19:26	Файл "BIN"	787 253 КБ
 MstarUpgrade_MBOOT.BIN	13.05.2020 11:27	Файл "BIN"	1 704 КБ
 MstarUpgrade_MBOOT.BIN.BOOT1	13.05.2020 11:27	Файл "BOOT1"	78 КБ

Которые и есть необходимые нам **sboot.bin** и **Mboot.bin**, соответственно 78 кБ и 1704 кБ.

Файл **MstarUpgrade_MBOOT.BIN.BOOT1** записывается в раздел boot1 eMMC.

Файл **MstarUpgrade_MBOOT.BIN** записывается в раздел User с адреса 0x200000, но он зашифрован и поэтому нет смысла записывать его напрямую в eMMC.

С одним только **sboot.bin** телевизор не примет USB прошивку.

Для правильной прошивки загрузчиков в eMMC на платформах с процессорами Mstar разработчиками программатора RT809H предусмотрен специальный алгоритм **EMMC_AUTO_ISP_BOOT_MST**, который автоматически дешифрует и записывает файлы по необходимым адресам.

Для использования **EMMC_AUTO_ISP_BOOT_MST** нам необходимо переименовать извлеченные файлы соответственно:

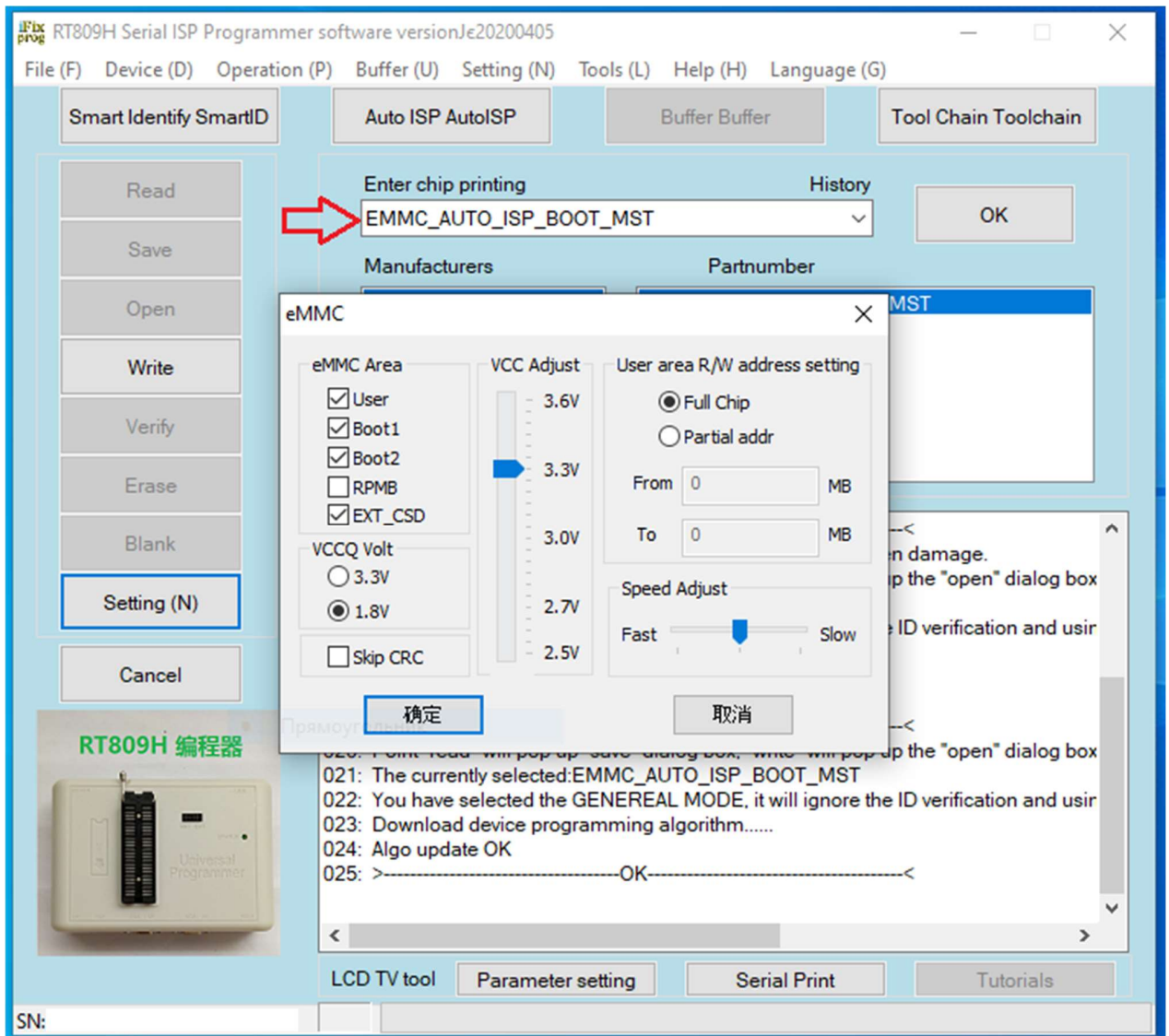
MstarUpgrade_MBOOT.BIN (Mboot) переименовываем в **1.bin**

MstarUpgrade_MBOOT.BIN.BOOT1 (sboot) переименовываем в **1.bin.boot1**

Оба файла должны находиться в одной папке.

Затем коннектимся к eMMC исключительно по ISP.

Далее выбираем в окне программы алгоритм **EMMC_AUTO_ISP_BOOT_MST** с настройками как на фото:



И нажимаем кнопку **Write**. Появится окно, в котором надо будет указать на любой из файлов **1.bin** или **1.bin.boot1**. Пропишутся оба.

Лог программатора будет иметь примерно такой вид:

```
071: Chip Size: User=7456MB,Boot1=Boot2=4096KB,RPMB=512KB.
072: SAMSUNG EMMC Version : V5.1. 0-10% device life time used.
073: Speed set to level 1.
074: C:\TVMMASTER\BOOTLOADERS MSTAR\BOOT MSA3487 SRT32HA3303U OLD FIRMWARE\MSA3487 SBOOT
MBOOT\1.BIN
075: Start writing chip.....
076: BOOT1Write and verify success.
077: . Start to write and check the user area data, large capacity, please be patient.
078: Skip empty file : C:\TVMMASTER\BOOTLOADERS MSTAR\BOOT MSA3487 SRT32HA3303U OLD
FIRMWARE\MSA3487 SBOOT MBOOT\1.BIN.part1
```


079: Elapsed time: 4.74 secondsJ-average speed of -996156049 bytes/sec.

080: >-----OK-----<

Не обращайте внимания на строку 078, так и должно быть.

На этом прошивка стартового ПО в eMMC завершена.

Следующим шагом будет прошивка с флешки через USB.

Отключаем питание платы, отсоединяем подключение ISP, размыкаем кварц от GND, проверяем номиналы резисторов (к которым подпаивались) и устанавливаем плату в телевизор.

При включении телевизора, если всё выполнено правильно, на UART появится лог и консоль Mstar, телевизор будет готов для принятия прошивки с флешки через USB.

На этом этапе не будет изображения на экране телевизора и подсветки, не будет светиться светодиод индикации дежурного режима, на пульт тоже не будет реакции. Будет работать только загрузчик U-boot (Mboot).

Для прошивки берём USB флешку необходимой ёмкости, желательно с индикатором обмена данных (светодиодом), форматируем её в FAT32 и копируем на флешку файл прошивки.

Выключаем телевизор из розетки, вставляем в порт USB флешку с прошивкой **MstarUpgrade.bin**, зажимаем кнопку джойстика строго вертикально и включаем телевизор в розетку. Держим кнопку нажатой примерно 10-15 секунд, после чего отпускаем. Если шить через консоль Mstar, то вставить флешку в USB и ввести команду *custar*, начнётся прошивка.

На экране в этот момент пока ещё ничего не отобразится, так как не прописаны системные файлы, поэтому прошивка первые пару минут будет идти без изображения статуса прогресса на экране. Но видеть процесс прошивки можно по миганию индикатора на USB флешке и по UART.

После пары минут телевизор перезагрузится и появится изображение на экране с прогрессом прошивки. Процесс прошивки довольно длительный, запаситесь терпением.

По окончании прошивки телевизор будет работать с розовым прямоугольником в верхнем левом углу экрана, что означает работу телевизора в инженерном режиме (там так и написано будет). Для выхода из него необходимо войти в сервисное меню с пульта, нажав последовательно **Source 2580**, выбрать пункт Factory menu и в нём выполнить Factory reset.

На этом замена eMMC и восстановление ПО шасси MSA3487-ZC01-001 завершены. Телевизор будет в состоянии «Из коробки».

Аналогичный подход можно применять и к многим распространённым шасси SMART телевизоров на процессорах Mstar в связке с eMMC, при условии, что загрузка производится с Boot1 (ROM1), а U-Boot (Mboot) находится в разделе USER (ROM3) по адресу 0x200000.

С уважением, **ВиталийВМ** (Виталий Васильев)
Україна, м. Першотравенськ

Особая благодарность за содействие
service (Йосип Смоляк)
Україна, м. Тернопіль