Восстановление магнитолы Wanqi AllWinner T3-P1 из состояния “софт-кирпич”

от CobaltDriver
Опубликовано 15.08.2019

Окирпичил свою магнитолу на третий день владения в попытках получить рут-права. Абсолютно никакой информации на просторах интернета о магнитолах на T3-P1 с Android 8.1 с завода. Китаец, естественно, опрокинул с поддержкой и я бросился во все тяжкие. Целая неделя нервотрепки, сломанный тачскрин ввиду многократных разборок/сборок магнитолы для пробы прошивок. И теперь я готов предоставить свой вариант загрузочного образа для PhoenixCard, который вновь оживил мою магнитолу. Но обо всем по порядку.

Содержание страницы

Как всё начиналось

Попытался получить рут путем прошивки SuperSU через рекавери переименовав его в os_update_*.zip. Он успешно прошился, но магнитола словила бутлуп. Действовал на тот момент я так смело потому, что имел свою оригинальную прошивку **os_update_XWQC01D1-O55-1.0.4.3.1_20190715_204335_b1.zip**. Ведь что может пойти не так? Ну сломал ведро, зайди в рекавери да накати по новой раздел /system и /vendor. А вот здесь начались сложности.

Сначала я шел от банального: пробовал всевозможные комбинации с кнопкой Reset (единственная физическая кнопка на данной магнитоле), но не похоже, что она имеет какую-то программную обработку. Скорее всего она задействована на банальный разрыв питания магнитолы.

Затем на ютубе нашел ролик, в котором на первый взгляд аналогичная внешне магнитола, с таким же точно лаунчером. В нем автор демонстрирует способ перезагрузки в рекавери через зажатие кнопки Reset, пока не начнет мигать подсветка сенсорных кнопок, и после нажать 3 раза Reset одновременно с тиками подсветки. И что странно, мне этот способ не помог — магнитола по прежнему мгновенно перезагружается при касании Reset’а. Из этого делаем вывод, что абсолютно одинаковые внешне магнитолы (даже программно) могут иметь абсолютно другое железо внутри.

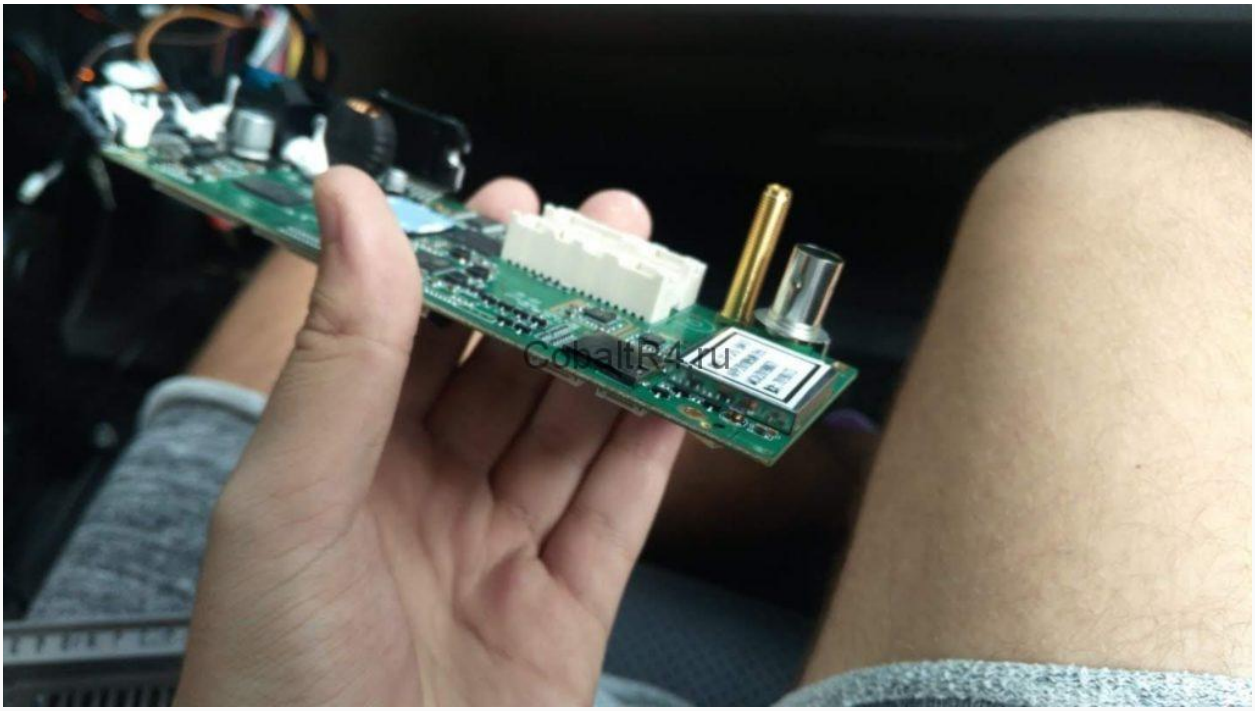
На 4pda вдоль и поперек изучил три имеющиеся темы по магнитолам на T3 (он же **sun8iw11p1**). Там популярен способ с зажатием трех клавиш на внешней USB-клавиатуре, а именно: **ALT** + **PrintScreen** и спамить клавишу **I**. Бесполезно, на момент бутлоадера, ю-бута, ядра и затем даже той части загрузки андроида до бутлупа клавиатура просто напросто не работает. В последствии, когда я перебирал всевозможные прошивки для феникса от совсем разных магнитол, на одной из них я все таки смог воспользоваться этим способом, так что он тоже слишком ситуативный.

Я уже начинал отчаиваться, умолял китайца выслать прошивку для феникса или хотя бы поделиться комбинацией для загрузки в рекавери. **Китаец**, естественно, **отморозился** и на связь выходить перестал.

Поняв, что терять нечего, я полез разбирать магнитолу в поисках хоть какой-нибудь зацепки: модель платы, каких-нибудь модулей или еще что-нибудь, что можно вбить в поисковик и найти магнитолы со схожим железом и готовые решения для них.

Снимаем декоративную рамку, ради которой приходится покупать эти богомерзкие магнитолы без поддержки

Видим, что исполнение аналогичное: Android-составляющая, MCU, питание и усилитель размещены вместе, без модулей как привычно для многих других магнитол. А это уже тревожный звоночек. Но как было сказано ранее, терять нечего, и разбираем дальше.



К моему огромному **ВЕЗЕНИЮ** обнаруживается распаянный слот MicroSD на обратной стороне платы, закрытый радиатором.

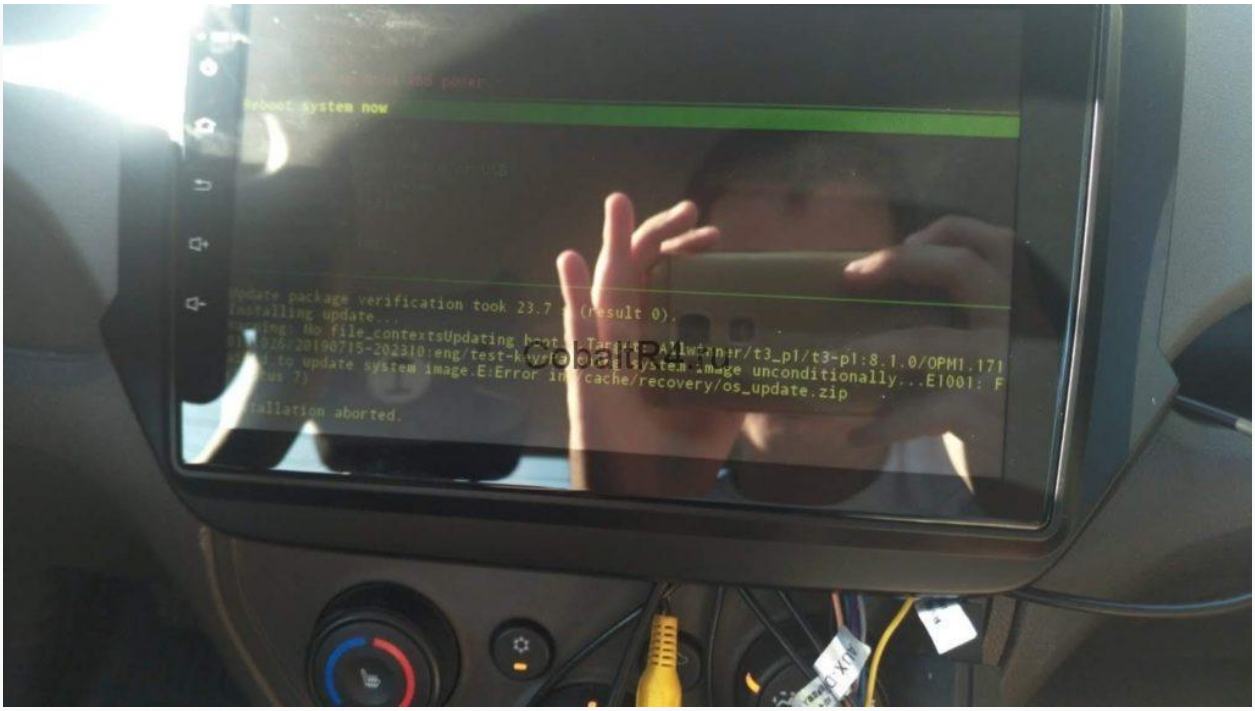
Как известно, аварийный способ восстановить прошивку на всех AllWinner — это создать загрузочную флешку с помощью программы PhoenixCard и образа .img, который состоит из разметки разделов (sys_partition.fex, dlinfo.fex, sunxi_mbr.fex), boot0 загрузчика (boot0_nand.fex, boot0_sdcard.fex), boot1 загрузчика (он же — u-boot.fex, который в свою очередь запакован в boot_package.fex), параметров запуска ядра (env.fex), раздела /bootloader (boot-resource.fex, содержит в себе MAGIC.BIN и изображения загрузчика), ну и привычные для андроида boot.fex, recovery.fex, system.fex и в случае восьмой версии ведра vendor.fex. По сути, имея такой слот на магнитоле и прошивку для своей модели, можно не бояться программных экспериментов, ибо прошивка фениксом это самая что ни на есть полная переразметка всей NAND с последующей перезаписью данных.

Но прежде чем начинать радоваться, нужно было убедиться, что этот слот действительно загрузочный. Обычно в магнитолах на AllWinner два MicroSD слота, и только один из них используется как загрузочный. Неизменный загрузчик, с которого начинается запуск всегда в приоритете пытается выполнить загрузку с MicroSD карты, и затем, не обнаружив её, уже переключается на NAND.

Бегу на 4pda в ближайшую тему к нашей магнитоле: https://4pda.ru/forum/index.php?showtopic=806442. Беру оттуда первую попавшуюся прошивку седьмого андроида для феникса, накатываю на флешку, вставляю в магнитолу и о чудо:

Слот загрузочный, процесс пошел. Не смотря на вопли в топике по ссылке выше о том, что T3-P3 и T3-P1 не взаимнопрошиваемы, система всё таки загрузилась:

Но сразу же бросается в глаза, что абсолютно ничего больше не работает. Слава Богу, что хотя бы сам андроид стартанул. Не было ни блютуза, ни вай-фая, ни радио и естественно отсутствовал звук. Версия андроида не приниципальна, как и внешний вид лаунчера, после нескольких дней езды с кирпичом вместо новенькой магнитолы хотелось любой работоспособности. Но её не было, и потому сразу была предпринята попытка прошить имеющийся zip для рекавери от китайца с оригинальным восьмым андроидом. На тот момент я еще не знал, что в восьмом андроиде иная таблица разделов, и самое основное изменение — это раздел /vendor, вместо которого раньше был симлинк /vendor -> /system/vendor. Естественно, не было никаких шансов накатить восьмой андроид на седьмой, даже если бы рекавери прошил ядро, оба загрузчика и раздел /system, без /vendor система бы не загрузилась:



И в голову сразу же пришла другая идея: отталкиваться от того, что работает на данный момент. С помощью **ImgRePacker** и параметра **/noiso** извлек работающую семерку и получил папку **YMHC0101-N39-1.5.4.2.5_20171212_152614.img.dump**. Не имея ранее опыта сборки прошивок, и тем более никогда не юзав устройства на AllWinner, было потрачено достаточно времени в понимании устройства образа прошивки для феникса. Первоначально я хотел просто добавить недостающие разделы, которые появились в восьмом ведре: vendor, dto вместо alog и media_data.

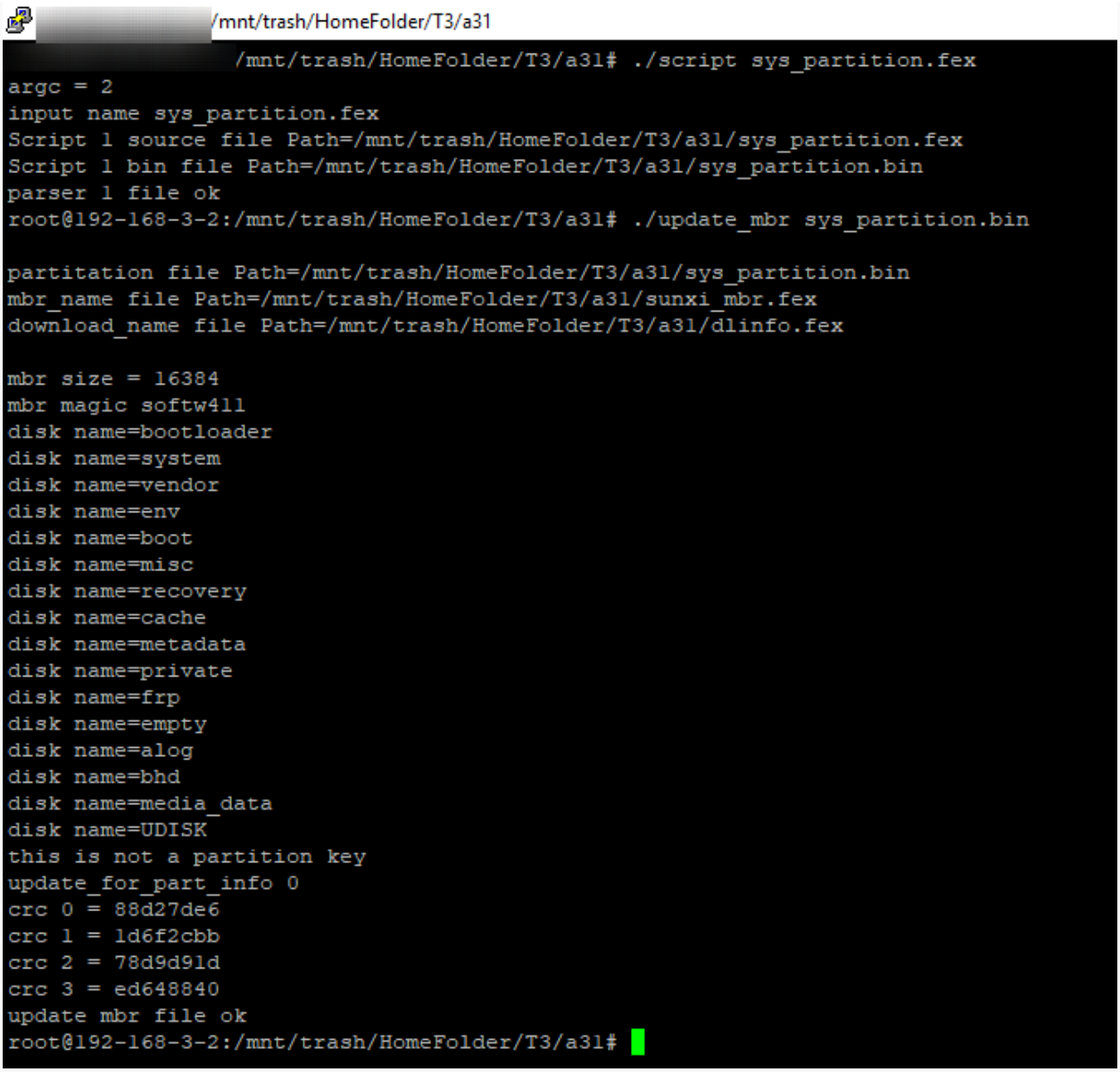
Для этого достаточно текстовым редактором открыть **sys_partition.fex** , исправить секции в соответствии с нашими требованиями и воспользовавшись найденными на просторах github’а бинарниками сгенерировать сначала sys_partition.bin, а затем из него dlinfo.fex и sunxi_mbr.fex.

Имейте в виду: размер в sys_partition.fex указывается в так называемых секторах, где 1 байт равняется 2 секторам. Указывая конкретный размер раздела, не забудьте его умножить на 2.

Если раздел будет меньше, чем заливаемый в него образ, то процесс прошивки с флешки магнитолы зависнет примерно на середине зеленого прогресс бара. Не забываем увеличивать размеры имеющихся разделов в соответствии с размерами образов.

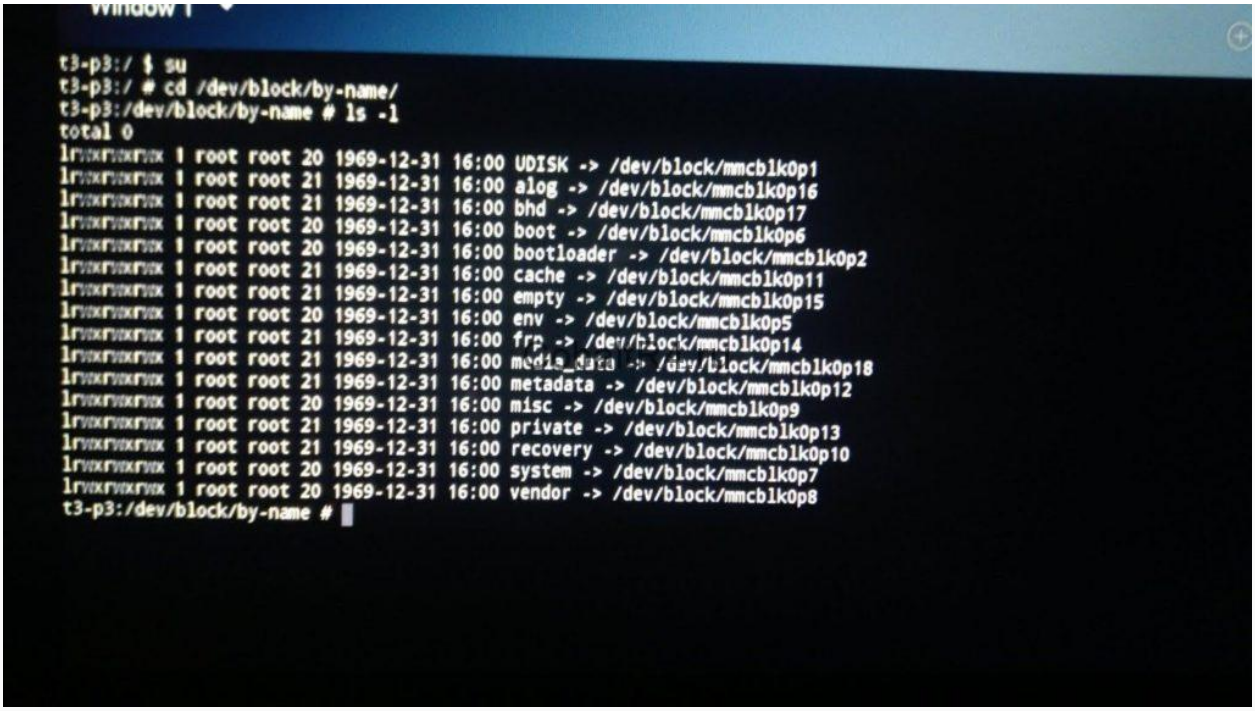
А так же порядок партиций в данном файле напрямую определяет, какими они будут в mmcblk0p*:
Первая запись в файле будет разделом mmcblk0p2
Вторая запись в файле будет разделом mmcblk0p5
Третья, четвертая, пятая, … — mmcblk0p6, mmcblk0p7, mmcblk0p8
И дальше в обычном порядке, но при этом UDISK всегда получает mmcblk0p1.

Sys partition.fex
https://cobaltr4.ru/download/484/

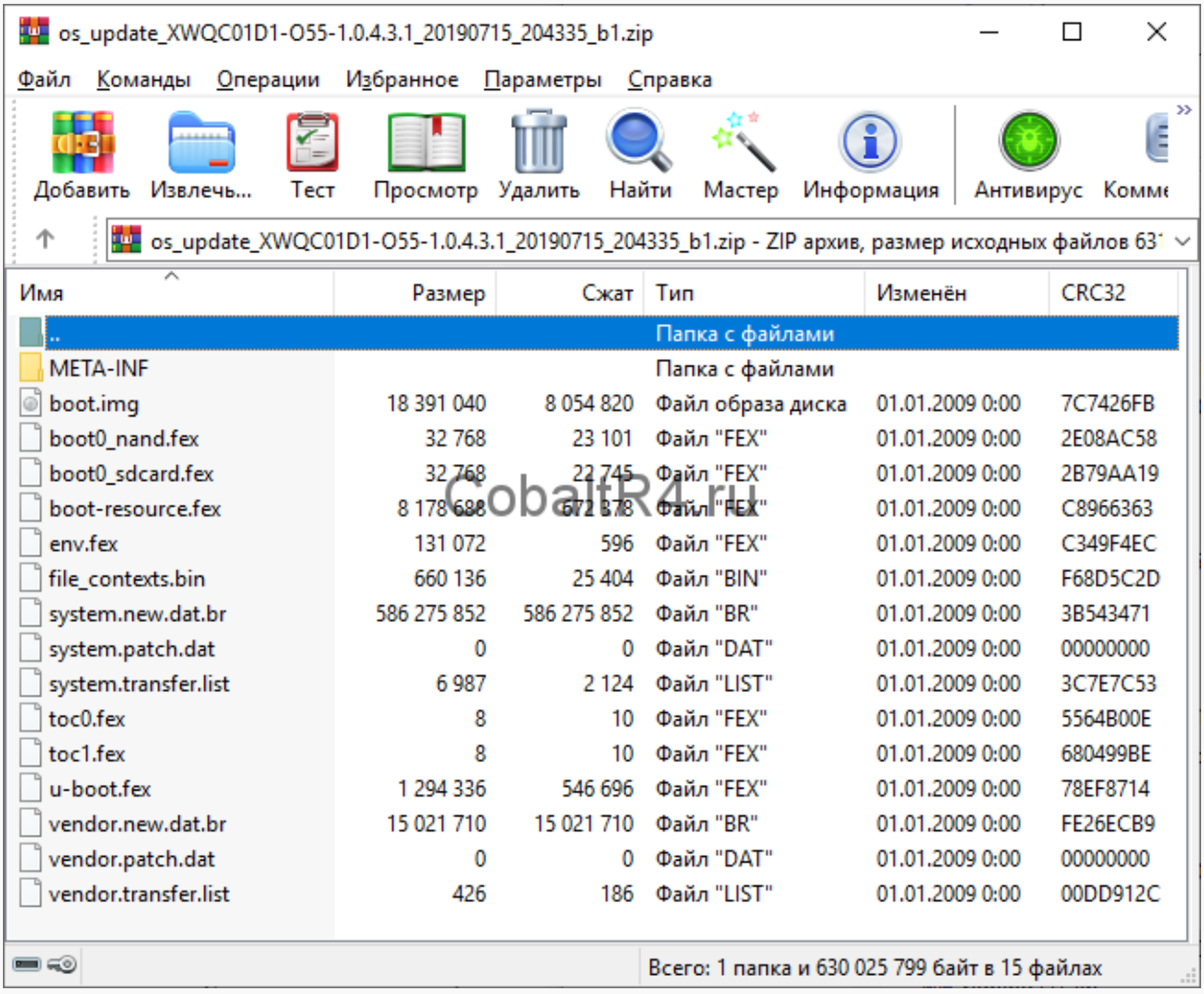


Бинарник sys_partition.bin нам не нужен, а вот оставшиеся два файла скидываем обратно в дамп распакованной img прошивки. dlinfo.fex содержит в себе информацию о заливаемых образах разделов в NAND. sunxi_mbr.fex, как можно догадаться из раздела, MBR для нашей mmcblk0.

Не изменяя ничего более, я собираю дамп обратно в .img всё той же программой и заливаю образ через феникс на флешку. Прошиваем, система успешно грузится. Отлично, значит таблицу разделов мы можем менять как нам захочется. Делаем рут и проверяем что получилось:



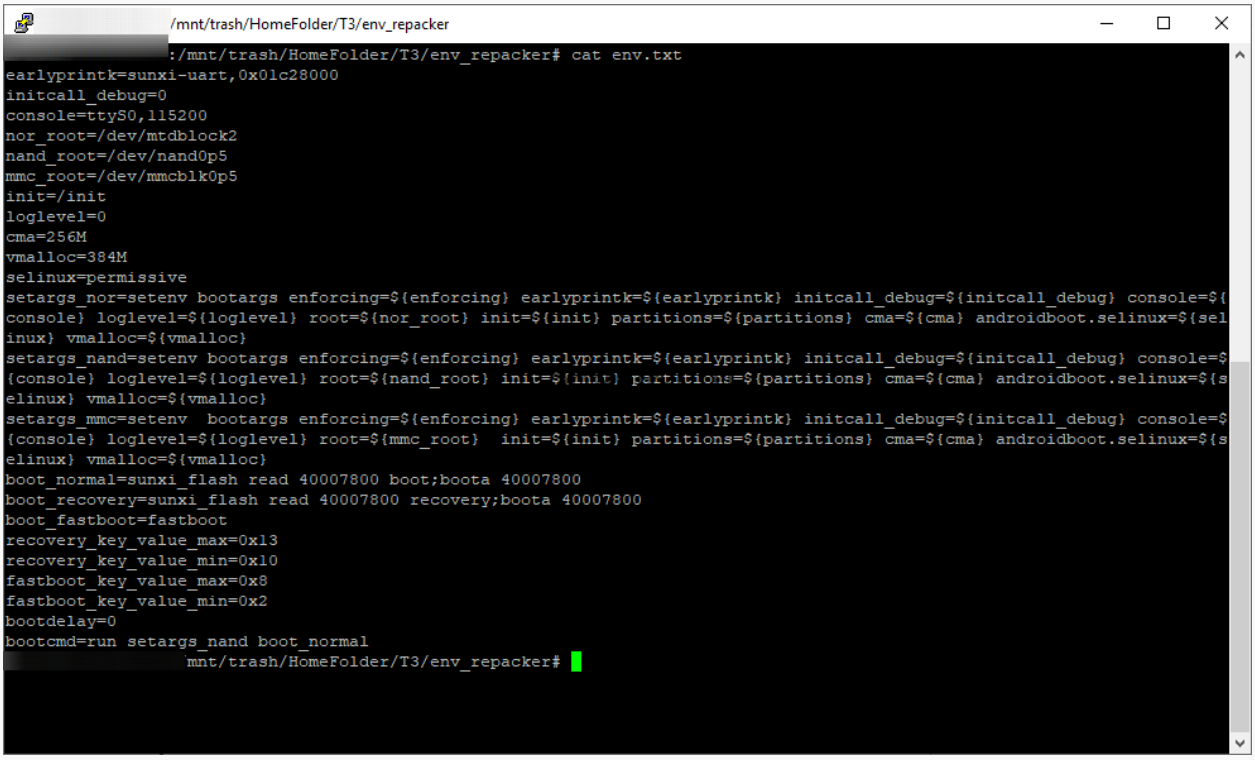
Бинго, вот и vendor в седьмом андроиде. Сразу же стало очевидно попытаться dd’шкой загнать образы разделов прям с работающей системы. Для этого вернемся к нашему zip архиву с восьмеркой и вытащим из него все возможное:



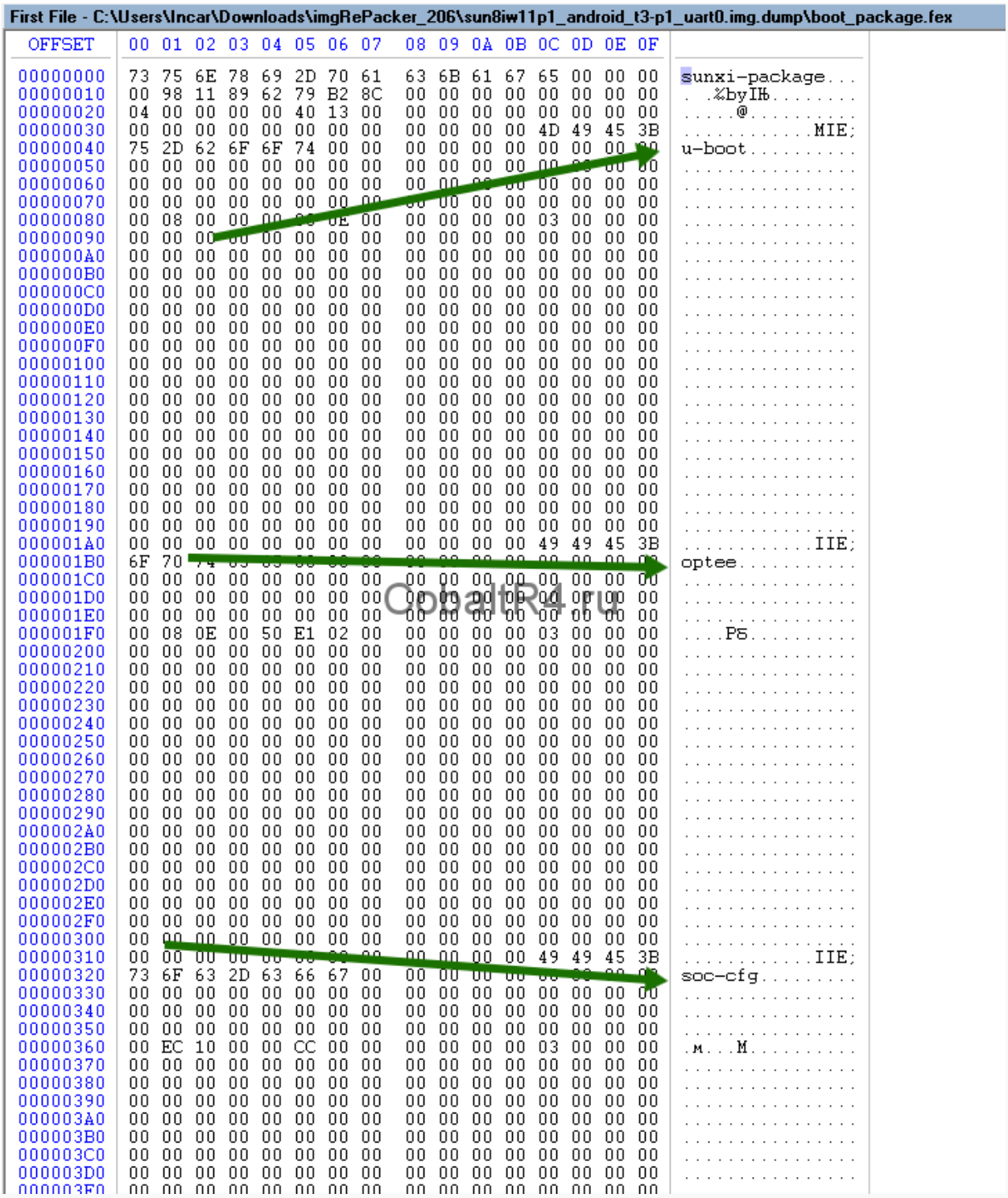
Что мы имеем? А имеем мы, не смотря на внешний вид а-ля OTA обновление из-за патчей system и vendor, полноценную систему. Разбираем содержимое архива:

- **boot.img** - ядро андроида, при встраивании в образ для феникса просто переименовываем в **boot.fex**

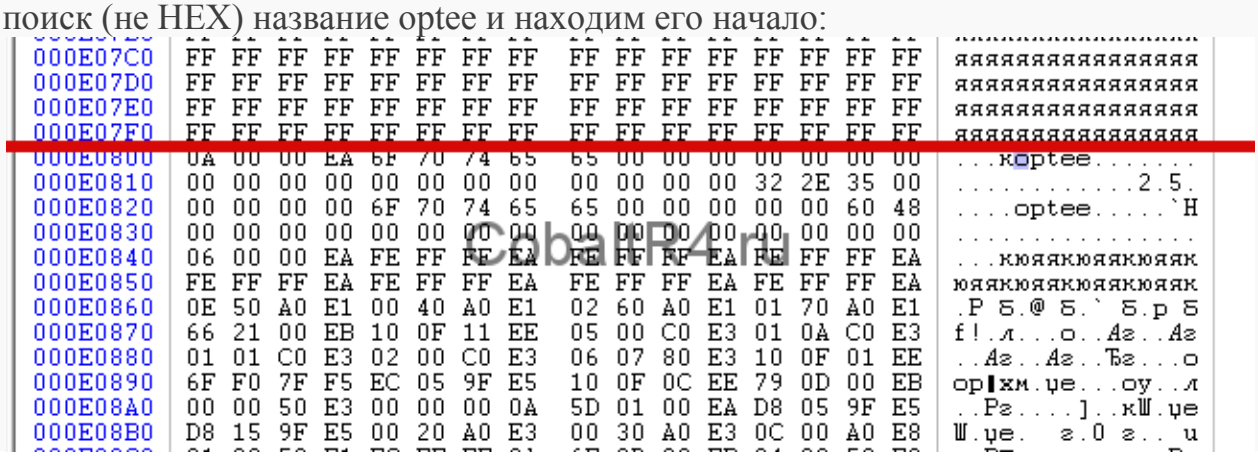
- **boot0_nand.fex** и **boot0_sdcard.fex** - boot0 загрузчик для типов памяти сооветственно, копируем без изменений
- **boot-resource.fex** — образ раздела /bootloader в файловой системе FAT16, копируем как есть
- **env.fex** - параметры запуска ядра, если распаковать, то получим следующее содержимое:



- **file_contexts.bin** — список пермишинов selinux для файлов, не используется в нашем случае
- **system.new.dat.br**, **system.patch.dat**, **system.transfer.list** — раздел /system. Сначала необходимо пройтись по файлу .dat.br утилитой Brotli.exe, получим system.new.dat, который вместе с двумя остальными файлами кидаем в директорию Input-DAT программы Auto Tool Unpack Repack .DAT & .IMG For Windows. Выбираем первый пункт, ожидаем завершение процесса и в корне программы обнаруживаем наш полноценный образ **system.dat.img**. С помощью **img2simg.exe** можно сжать файл за счет удаление свободного пространства, которое в изначальном файле представлено нулями. Я этого делать не стал, потому что опасаюсь, что без нулей образ не покроет полностью соответствующий раздел в NAND. Полученный файл переименовываем в **system.fex** и бросаем в наш дамп
- **toc0.fex** и **toc1.fex** — копируем без изменений
- **u-boot.fex** - не смотря на аналогичное название файла файлу в дампе, они отличаются. А вот с файлом **boot_package.fex** у них полное совпадение, потому переименовываем u-boot из архива zip в boot_package.fex и заменяем. Это первое. Второе: данный пакет содержит в себе в том числе и **u-boot.fex** для img образа феникса. Любым удобным HEX-редактором открываем файл и видим следующее:



Это своего рода пакет-склейка нескольких файлов: u-boot, optee, soc-cfg и еще не влез dtb конфиг. Видим, что нужный нам u-boot идет первым, а за ним следует optee. Значит, в начале файла обрезаем всё вплоть до **8E 01 00 EA 75 62 6F 6F 74**, что соответствует строке kuboot. Теперь наша задача определить конец юбута, для этого вернемся к структуре пакета на скриншоте выше и видим, что за юбутом следует **optee**. Вбиваем в поиск (не HEX) название optee и находим его начало:



Наблюдаем ярко выраженную границу двух файлов, потому сразу после множества FF FF FF … FF обрезаем наш boot_package до самого конца. Получившийся файл сохраняем как **u-boot.fex** в дамп для феникса. Еще раз: из одного файла u-boot.fex из зип архива мы получаем два файла boot_package.fex и u-boot.fex для img дампа феникса.

- **vendor.new.dat.br**, **vendor.patch.dat**, **vendor.transfer.list** — по аналогии с **system.new.dat.br**. Только стоит учесть, что программа Auto Tool Unpack Repack .DAT & .IMG For Windows на вход принимает файл строго с названием system.new.dat.br, поэтому все три файла переименовываем из vendor в system, а затем полученный образ обратно в **vendor.fex** и бросаем в дамп феникса.

Возвращаемся к **ImgRePack**, теперь уже запаковываем дамп обратно в img, введя название папки **YMHC0101-N39-1.5.4.2.5_20171212_152614.img.dump** и параметр **/noiso**. Получаем образ, который с помощью PhoenixCard записываем на флешку и идем прошивать магнитолу.

Но ничего не получалось, как я не комбинировал работающий седьмой андроид и имеющийся архив для рекавери с восьмеркой — получал либо черный экран, либо артефакты вместо изображения. Пробовал всякое, курил кучу тематических форумов, но ничего не помогало.

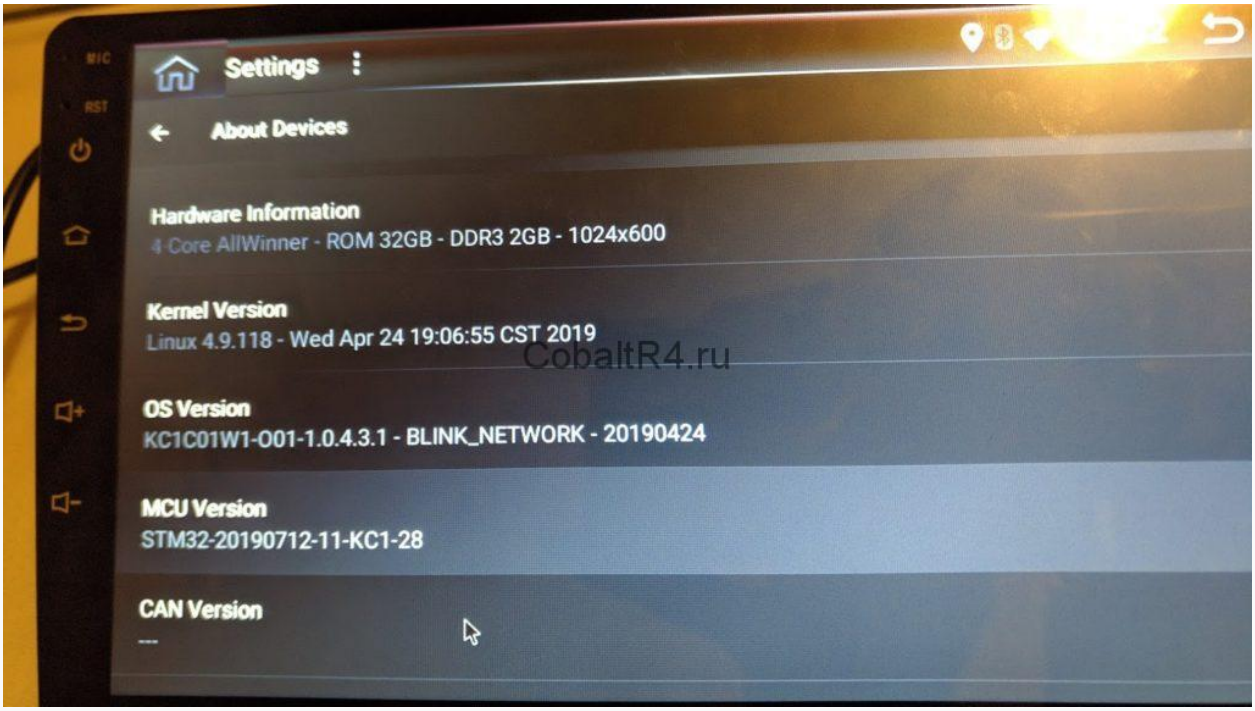
И вот вчера в теме на 4pda ув. **ahmed68** выложил полный образ восьмерки для феникса. Естественно, я сразу побежал его прошивать, но прошивка даже не стартовала. Просто черный экран при включении магнитолы с подключенной флешкой MicroSD. Я начал заменять в ней файлы по одному своими из zip архива, естественно начиная связанных с загрузкой, ибо ни ядро, ни разделы самого андроида очевидно не влияют на процесс прошивки. И когда список замененных файлов был следующим: boot_package.fex, boot0_nand.fex, boot0_sdcard.fex, boot-resource.fex и u-boot.fex прошивка таки пошла. И даже больше: появилась загрузочная картинка из /bootloader. Это был прогресс на фоне всех моих ранних мучений.

Естественно, я сразу же заменил и оставшиеся разделы андроида, но загрузка так и не пошла. Даже больше: при замене boot.fex ядром от моего восьмого андроида, загрузка начала прерываться ежесекундной перезагрузкой. Причину, по которой содержимое моего архива не хотело грузиться я не знаю. От безысходности я решил попробовать повторить аналогичное, но с другим архивом: **os_update_KC1C01W1-O01-1.0.4.3.1_20190424_192823_b1.zip**. Внутри такой же андроид 8.1, настоящий, не переименованный в build.prop. Но с лаунчером не как у нас, а как и в ранних прошивках KC1C0101, только с андроидом 7.

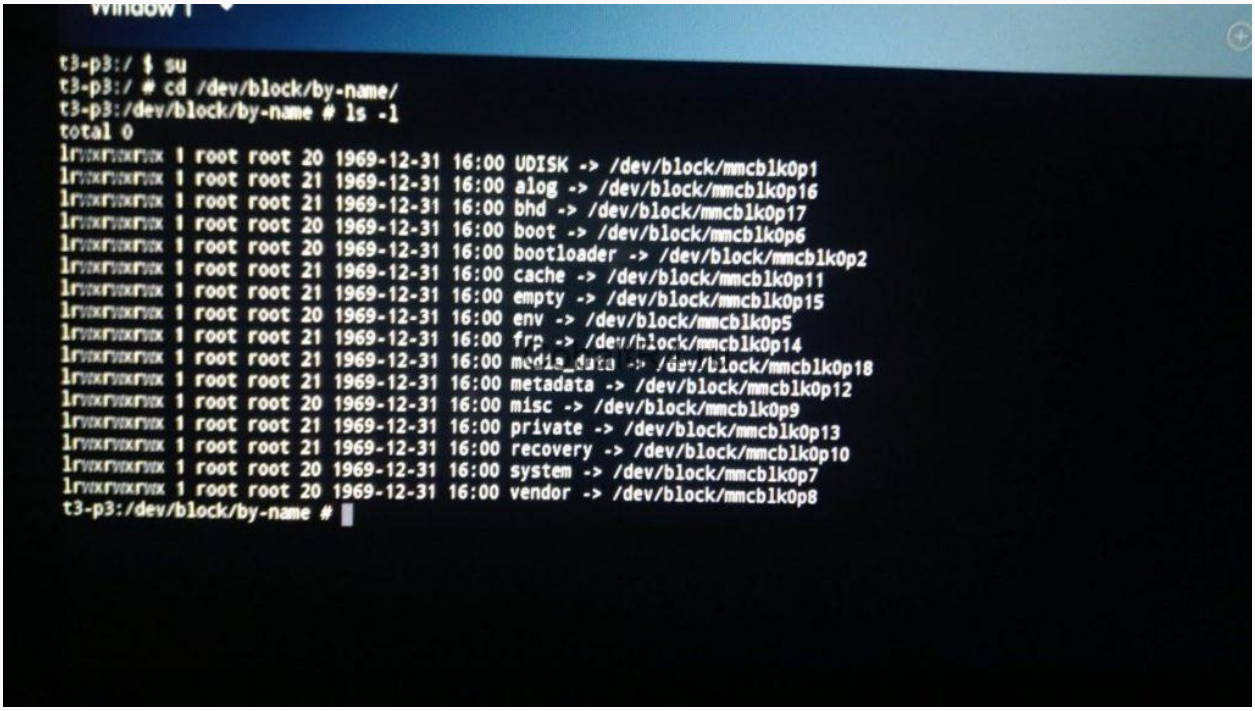
И всё, появилась бутанимация восьмого ведра:

А затем и лаунчер от KC1C0101:

Сразу в глаза бросилась иконка Wi-Fi, и не зря: он заработал. Так же, как и всё остальное. Появилось радио, начали сохраняться настройки эквалайзера. Блютуз снова находит другие устройства. MCU не менял, прекрасно работает и с моим июльским, хотя прошивка апрельская:



Прикладываю разметку разделов, на которой 100% восьмой андроид грузится. Да, тут есть лишние разделы, но они не мешают и я их оставил прозапас:



Не знаю, связано ли это с последней прошивкой от ув. **ahmed68** или же мне сразу стоило пытаться накатить **KC1C01W1-O01**, а не мучиться с моей оригинальной. Но в любом случае магнитола снова работает, чему я безумно рад. Естественно, сразу же сделал рут, с чего это приключение и начиналось. Пропатчил ядро boot.fex с помощью Magisk Manager и собрал архив .zip для прошивки через рекавери. Переименовал его в os_update_kernel.zip и прошил обычным путем через юсб-флешку на работающей системе. После этого остается поставить Magisk Manager из apk и доустановить рут.

Скачать прошивку и MCU

Образ для феникса:

https://cobaltr4.ru/download/503/

Единственный PhoenixCard, который у меня смог без ошибок записывать образы на MicroSD-карты:

https://cobaltr4.ru/download/507/

Пропатченное ядро для рута, кинуть на юсб-флешку и выбрать для прошивки в интерфейсе системы:

https://cobaltr4.ru/download/505/

Скачать MCU 1001KC1 от 12.07.2019:

https://cobaltr4.ru/download/404/

Скачать MCU 1001KC1 от 18.03.2019:

https://cobaltr4.ru/download/597/