Восстановление магнитолы Wanqi AllWinner T3-P1 из состояния "софт-кирпич"

om CobaltDriver Опубликовано <u>15.08.2019</u>

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 <u>os_update_XWQC01D1-O55-1.0.4.3.1_20190715_204335_b1.zip</u>. 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), paздела /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 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: <u>https://4pda.ru/forum/index.php?showtopic=806442</u>. 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 ТЗ-РЗ и ТЗ-Р1 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 принициальна, 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'a бинарниками сгенерировать сначала sys_partition.bin, а затем из него dlinfo.fex и sunxi_mbr.fex.

Имейте в виду: paзмер 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/

/mnt/trash/HomeFolder/T3/a31
/mnt/trash/HomeFolder/T3/a31# ./script svs partition.fex
argc = 2
input name sys partition.fex
Script 1 source file Path=/mnt/trash/HomeFolder/T3/a31/sys partition.fex
Script 1 bin file Path=/mnt/trash/HomeFolder/T3/a31/sys partition.bin
parser 1 file ok
root@192-168-3-2:/mnt/trash/HomeFolder/T3/a31# ./update_mbr sys_partition.bin
partitation file Path=/mnt/trash/HomeFolder/T3/a31/sys_partition.bin
mbr_name file Path=/mnt/trash/HomeFolder/T3/a31/sunxi_mbr.fex
download_name file Path=/mnt/trash/HomeFolder/T3/a31/dlinfo.fex
mbr size = 16384
mbr magic softw411
disk name=bootloader
disk name=system
disk name=vendor
disk name=env
disk name=boot
disk name=misc
disk name=recovery
disk name=cache
disk name=metadata
disk name=private
disk name-irp
disk name-empty
disk name-alog
disk name=media data
disk name=UDISK
this is not a partition key
undate for part info 0
crc 0 = 88d27de6
crc l = ld6f2cbb
crc 2 = 78d9d91d
crc 3 = ed648840
update mbr file ok
root@192-168-3-2:/mnt/trash/HomeFolder/T3/a31#

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:

WINDOW 1 +	
t3-p3:/ \$ su t3-p3:/ # cd /dev/block/by-name/	0
t3-p3:/dev/block/by-name # 1s -1 total 0	
1 root root 20 1969-12-31 16:00 UDISK -> /dev/block/mmcb1k0p1	
ITTERTURE I FOOT FOOT 21 1969-12-31 16:00 alog -> /dev/block/mmcblk0016	
IT/08/108/108 root root 21 1969-12-31 16:00 bhd -> /dev/block/mmcblk0017	
ITTERTURFUR 1 root root 20 1969-12-31 16:00 boot -> /dev/block/mmcblk0p6	
ITVERTURFUR I root root 20 1969-12-31 16:00 bootloader -> /dev/block/mmcb1k0n2	
ITTERFUERFUER I root root 21 1969-12-31 16:00 cache -> /dev/block/mmcblk0p11	
ITUERTWERTWERT 1 root root 21 1969-12-31 16:00 empty -> /dev/block/mmcblk0p15	
ITVERTVERTVER 1 root root 20 1969-12-31 16:00 env -> /dev/block/mmcblk0p5	
Inderwarder 1 root root 21 1969-12-31 16:00 frp -> /dev/block/mmcblk0p14	
ITVIXITVIXITVIX 1 root root 21 1969-12-31 16:00 media_data ab /dev/block/mmcblk0p18	
ITYERVERVER 1 root root 21 1969-12-31 16:00 metadata -> /dev/block/mmcblk0p12	
ITVERTURETURE I root root 20 1969-12-31 16:00 misc -> /dev/block/mmcblk0p9	
Invertering 1 root root 21 1969-12-31 16:00 private -> /dev/block/mmcblk0p13	
ITVXTVXTVX I root root 21 1969-12-31 16:00 recovery -> /dev/block/mmcblk0p10	
Invariante i root root 20 1969-12-31 16:00 system -> /dev/block/mmcblk0p7	
13-D3/ dew/block/mmcblk0p8	
C3-P3-Fider/b10CK/by-name #	

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:

s_update_XWQC01D1-O55-	1.0.4.3.1_2019071	5_204335_b1.zi	p	_	
<u>Ф</u> айл <u>К</u> оманды <u>О</u> перации	Избранное П	араметры <u>С</u>	правка		
Добавить Извлечь Тест	Просмотр	удалить Най	іти Мастер Инфо	рмация Антив	ирус Комме
	1D1-055-1.0.4.3.	1_20190715_204	335_b1.zip - ZIP архив	, размер исходнь	іх файлов 631 V
Имя	Размер	Сжат	Тип	Изменён	CRC32
			Папка с файлами		
META-INF			Папка с файлами		
💿 boot.img	18 391 040	8 054 820	Файл образа диска	01.01.2009 0:00	7C7426FB
boot0_nand.fex	32 768	23 101	Файл "FEX"	01.01.2009 0:00	2E08AC58
boot0_sdcard.fex	32 768	22 745	Файл "FEX"	01.01.2009 0:00	2B79AA19
boot-resource.fex	8 178 688	DD 941 Pla	Файл "РЕХ"	01.01.2009 0:00	C8966363
env.fex	131 072	596	Файл "FEX"	01.01.2009 0:00	C349F4EC
ile_contexts.bin	660 136	25 404	Файл "BIN"	01.01.2009 0:00	F68D5C2D
system.new.dat.br	586 275 852	586 275 852	Файл "BR"	01.01.2009 0:00	3B543471
system.patch.dat	0	0	Файл "DAT"	01.01.2009 0:00	00000000
system.transfer.list	6 987	2 124	Файл "LIST"	01.01.2009 0:00	3C7E7C53
toc0.fex	8	10	Файл "FEX"	01.01.2009 0:00	5564B00E
toc1.fex	8	10	Файл "FEX"	01.01.2009 0:00	680499BE
u-boot.fex	1 294 336	546 696	Файл "FEX"	01.01.2009 0:00	78EF8714
vendor.new.dat.br	15 021 710	15 021 710	Файл "BR"	01.01.2009 0:00	FE26ECB9
🗋 vendor.patch.dat	0	0	Файл "DAT"	01.01.2009 0:00	00000000
vendor.transfer.list	426	186	Файл "LIST"	01.01.2009 0:00	00DD912C
			Всего: 1 папка и 630 ()25 799 байт в 15 (файлах .

Что мы имеем? А имеем мы, не смотря на внешний вид а-ля ОТА 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:

/mnt/trash/HomeFolder/T3/env_repacker	· D	×
	_	
:/mnt/trash/HomeFolder/T3/env_repacker# cat env.txt		^
earlyprint#sunx1-uart,0x01c28000		
initcall_debug=0		
console=ttyS0,115200		
nor_root=/dev/mtdblock2		
nand_root=/dev/nand0p5		
mmc_root=/dev/mmcblk0p5		
init=/init		
loglevel=0		
cma=256M		
vmalloc=384M		
selinux=permissive		
<pre>setargs_nor=setenv bootargs enforcing=\${enforcing} earlyprintk=\${earlyprintk} initcall_debug=\${initcall_debug</pre>	console	=\$ {
<pre>console} loglevel=\${loglevel} root=\${nor_root} init=\${init} partitions=\${partitions} cma=\${cma} androidboot.se</pre>	linux=\${	sel
inux} vmalloc=\${vmalloc}		
<pre>setargs_nand=setenv bootargs enforcing=\${enforcing} earlyprintk=\${earlyprintk} initcall_debug=\${initcall_debug</pre>	<pre>{} consol</pre>	e=\$
<pre>{console} loglevel=\${loglevel} root=\${nand_root} init=\${init} partitions=\${partitions} cma=\${cma} androidboot</pre>	selinux=	\${s
elinux} vmalloc=\${vmalloc}		
<pre>setargs_mmc=setenv bootargs enforcing=\${enforcing} earlyprintk=\${earlyprintk} initcall_debug=\${initcall_debug</pre>	<pre>{} consol</pre>	e=\$
<pre>{console} loglevel=\${loglevel} root=\${mmc_root} init=\${init} partitions=\${partitions} cma=\${cma} androidboot</pre>	selinux=	\${s
elinux} vmalloc=\${vmalloc}		
boot normal=sunxi flash read 40007800 boot;boota 40007800		
boot_recovery=sunxi flash read 40007800 recovery;boota 40007800		
boot fastboot=fastboot		
recovery key value max=0x13		
recovery key value min=0x10		
fastboot key value max=0x8		
fastboot key value min=0x2		
bootdelay=0		
bootcmd=run setargs nand boot normal		
mnt/trash/HomeFolder/T3/env repacker#		
		v

- 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 <u>Brotli.exe</u>, получим system.new.dat, который вместе с двумя остальными файлами кидаем в директорию Input-DAT программы <u>Auto Tool Unpack Repack .DAT & .IMG For</u> <u>Windows</u>. 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:

First File - C:	Users\Inc	car\Dov	nloads\i	mgRePack	ker_206\sun	Biw11p1_	_android_t3-p	1_uart0.img.dump\boot_package.fex
OFFSET	00 01	02 03	04 05	06 07	08 09 OA	0B 0C	OD OE OF	_
00000000 00000010 00000020 00000030 00000060 00000060 00000080 00000080 00000080 00000080 000000	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$egin{array}{cccc} 6E & 78 \\ 11 & 89 \\ 00 & 00 \\ 00 & $	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$\begin{array}{cccccccccccccccccccccccccccccccccccc$		$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	sunxi-package .%byIH @ MIE; u-boot
000001E0 000001E0 000001E0 000001E0 00000200 00000210 00000210 00000240 00000240 00000250 00000250 00000250 00000280 00000280 00000280 00000280 00000280 00000280 00000280 00000280 00000280 00000280 00000280 00000280 00000310 00000310 00000310 00000350 00000380 00000380 00000380 00000380	$\left \begin{array}{ccccc} 6F & 70 \\ 00 & 00 \\ 00 $	$ \begin{array}{ccccccccccccccccccccccccccccccccc$	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	optee

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:

			/						-										
I	00020700	EE.	1 ±	EE.	EE.	EE.	* * EE	EE.	EE.	 EE	EE.								
I	00060700	F F	rr 	rr —	rr —	F F	F F	rr —	F F	<u>F</u> F	rr 	<u>rr</u>	<u>F</u> F	r r	r r	rr —	F F	яяяяяяяяяяяяяя	
I	000E07D0	FF	\mathbf{FF}	FF	FF	FF	FF	\mathbf{FF}	\mathbf{FF}	FF	\mathbf{FF}	\mathbf{FF}	\mathbf{FF}	\mathbf{FF}	FF	FF	\mathbf{FF}	яяяяяяяяяяяя	
I	000E07E0	\mathbf{FF}	FF	\mathbf{FF}	RRRRRRRRRRRRR														
I	000E07F0	FF	FF	FF	FF	FF	FF	FF	FF	FF	****************								
1		ЦA	1111	1111	E.A	ЬP	711	74	b5	hþ	1111	1111		1111	1111			xontee	
I	00020810	ññ	ñň	ñň	00	ññ	'nñ	οÔ.	ñň	ñň	ñň	ñň	ñň	32	2 म	35	ñň	2.5	
I	00020010	00	00	00	00	617	20	24	200	65	00	00	00	00	00	60	40	+ `U	
I	000E0820	00	00	00	00	65	/0	/4	65	. 65	00	00	00	00	00	60	48	optee H	
I	000E0830	00	00	00	00	00	00	ųσ	۶QQ	6 <u>0</u> 9	pp	 00,	100	ալ ներ	00	00	00		
I	000E0840	06	00	00	ΕA	FΕ	\mathbf{FF}	FE.	'EA	UFE	FFI	FF	EAL	FE	\mathbf{FF}	\mathbf{FF}	ΕA	кюяякюяякюяяк	
I	000E0850	FE	\mathbf{FF}	\mathbf{FF}	ΕA	FE	\mathbf{FF}	\mathbf{FF}	ΕA	FE	\mathbf{FF}	\mathbf{FF}	ΕA	FE	\mathbf{FF}	\mathbf{FF}	ΕA	юяякюяякюяяк	
I	000E0860	0E	50	ΑO	E1	00	40	ΑO	E1	02	60	ΑO	E1	01	70	ΑO	E1	.P 5.@ 5.` 5.p 5	
I	000E0870	66	21	00	EΒ	10	0F	11	ΕE	05	00	CO	E3	01	ΟA	C0	E3	f!.лоАгАг	
I	000E0880	01	01	C0	E3	02	00	C0	E3	06	07	80	E3	10	0F	01	ΕE	AzAzЂzo	
I	000E0890	6F	F0	7F	F5	EC	05	9F	E5	10	0F	0C	ΕE	79	0D	00	EΒ	ор∎хм.џеоул	
I	000E08A0	00	00	50	E3	00	00	00	ΟA	5D	01	00	ΕA	D8	05	9F	E5	Pz]ĸŴ.џе	
I	000E08B0	D8	15	9F	E5	00	20	ΑO	E3	00	30	ΑO	E3	0C	00	ΑO	E8	W.ye. z.O z. u	
- 4																			

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 c system.new.dat.br. Только стоит учесть, что программа <u>Auto Tool Unpack Repack</u> .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** <u>выложил</u> 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 КС1С0101:



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. МСU 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:

t3-p3:/# cd /dev/block/by-name/ t3-p3:/dev/block/by-name # ls -1		
total 0		
Investment 1 root root 20 1969-12-31	16:00 UDISK -> /dev/block/mmcblk0p1	
TUCK FUCK FUCK FOOT FOOT 21 1969-12-31	16:00 alog -> /dev/block/mmcblk0p16	
ITVERTVERTVER FOOT FOOT 21 1969-12-31	16:00 bhd -> /dev/block/mmcblk0p17	
1 PUCK FUCK FUCK 1 FOOT FOOT 20 1969-12-31	16:00 boot -> /dev/block/mmcblk0p6	
Investment 1 root root 20 1969-12-31	16:00 bootloader -> /dev/block/mmcblk0p2	
ITVERTURATION I FOOT FOOT 21 1969-12-31	16:00 cache -> /dev/block/mmcblk0p11	
1 PORT PORT 1 FOOT FOOT 21 1969-12-31	16:00 empty -> /dev/block/mmcblk0p15	
1 FOOT FOOT 20 1969-12-31	16:00 env -> /dev/block/mmcblk0p5	
1 MARTHARTHA 1 FOOT FOOT 21 1969-12-31	16:00 frp -> /dev/hlock/mmcblk0p14	
1 THAT HAT WA I FOOT FOOT 21 1969-12-31	16:00 media_data -> /day/block/mmcblk0p18	
1 THE THE TWO I FOOT FOOT 20 1069-12-31	16:00 metadata -> /dev/block/mmcblk0p12	
1 TUXFUERUX 1 FOOT FOOT 21 1969-12-31	16:00 misc -> /dev/block/mmcblk0p9	
1 TWX TWX TWX 1 FOOT FOOT 21 1969-12-31	16:00 private -> /dev/block/mmcblk0p13	
1rwxrwxrwx 1 root root 20 1969-12-31	16:00 Eveter > /dev/block/mmcblk0p10	
1 WK WK 1 Foot root 20 1969-12-31	16:00 verder -> /dev/block/mmcDlk0p7	
t3-p3:/dev/block/by-name #	10:00 VEHIOU -> / UEV/DIOCK/MMCDIKUP8	

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 арк и доустановить рут.

Скачать прошивку и МСИ

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 МСИ 1001КС1 от 12.07.2019:

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

Скачать МСИ 1001КС1 от 18.03.2019:

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