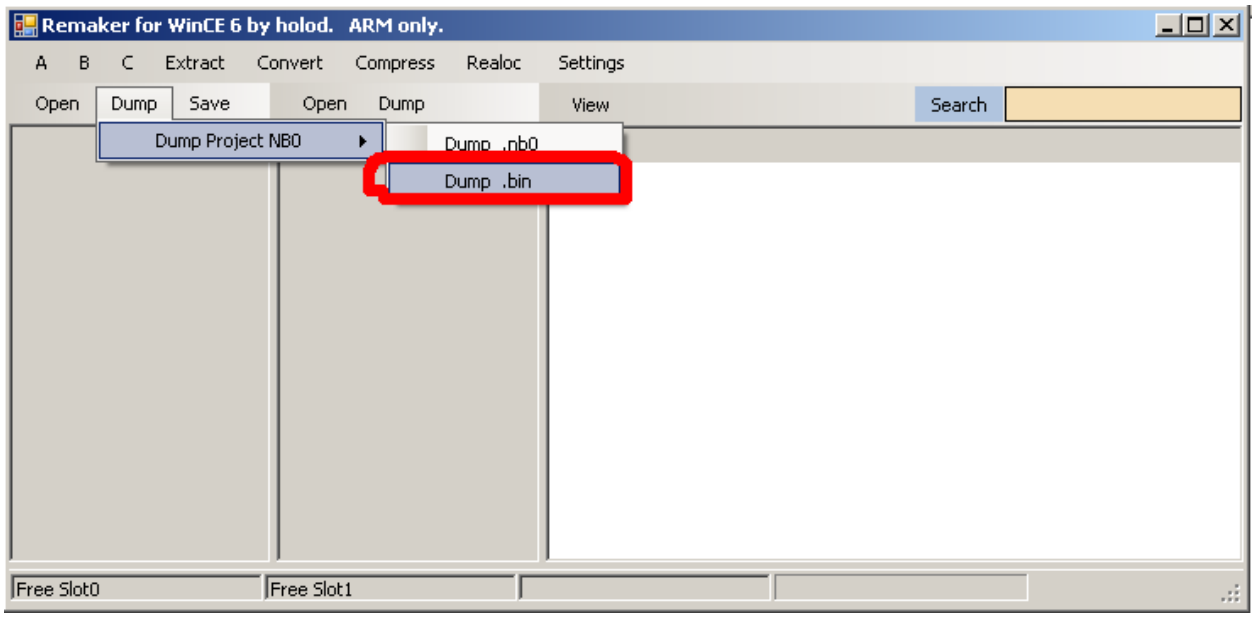
Задача - интегрировать драйвер USB ELM327 в прошивку магнитолы, дабы избавиться от надоедливого окна с просьбой указать драйвер устройства после каждого запуска. С учетом того, что у меня китайская винда в магнитоле, скрипт для MortScript, отслеживающий окно по заголовку и вбивающий ему автоматом путь, заставить работать так и не удалось.
Итак, нам нужны файлы nk.bin и tinynk.bin из нашей прошивки.
Если у вас есть архив с прошивкой для вашей магнитолы, навроде тех, что RepPower поставляет для своих магнитол - вам повезло, можно препарировать их (убедившись предварительно, что будучи зашитыми в магнитолу в исходном виде они работают, и работают так, как вам того хотелось - без глюков и прочих не-радостей).
Мне не повезло, архив с прошивкой добыть не удалось, поэтому были проделаны следующие шаги:

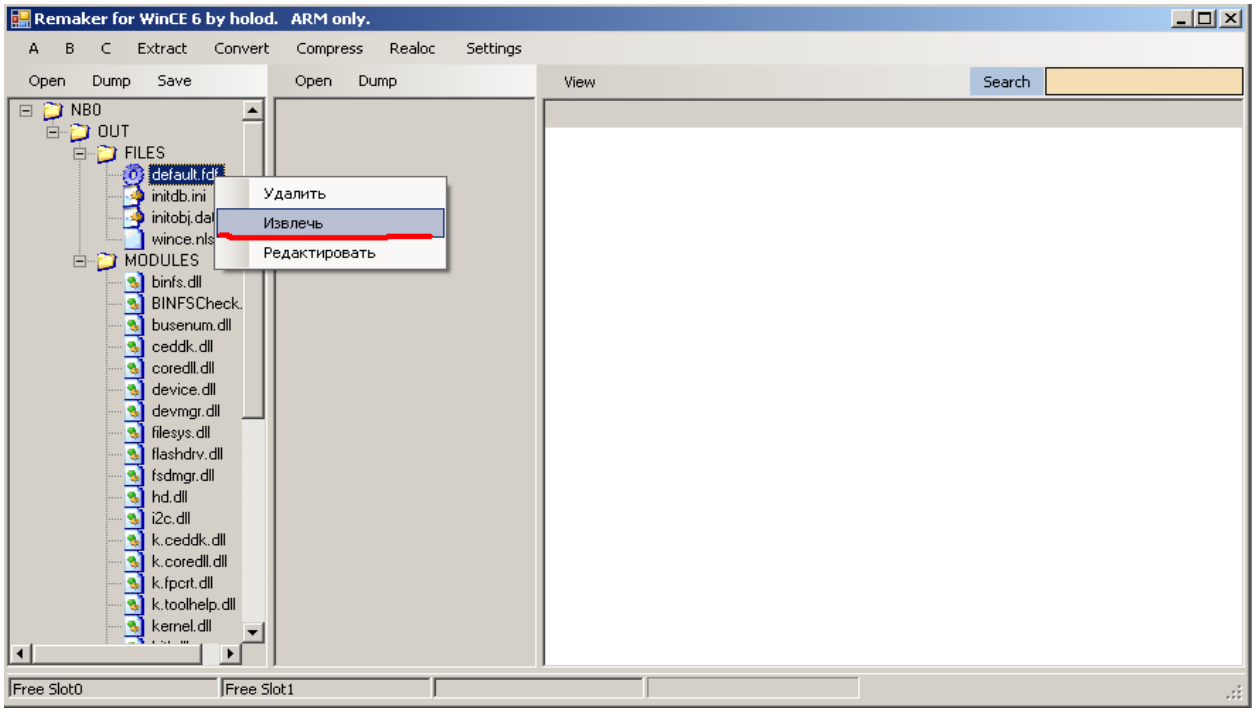
1. Снят дамп с магнитолы утилитой *NDumpCE6.exe,* был получен файл Dump.bin размером около 100 мбайт.
2. Данный файл “скормлен” утилите Sourcery от Kir7, брал здесь http://4pda.ru/forum/index.php?showtopic=119060&st=480#entry3241570 , на выходе получены файлы:
    a. Chain.bin
    b. Chain.lst
    c. NK.BIN
    d. TINYNK.BIN
    e. Decompile.txt, но он нам не особо интересен.
3. Далее будем препарировать TINYNK.BIN и NK.BIN. Для этого нам понадобится утилита Remaker CE 6.0 (она не единственная пригодна для наших целей, но дальнейший процесс буду описывать на ее примере). Саму программу можно взять здесь http://4pda.ru/forum/index.php?showtopic=119060&st=4660#entry19511219
   Нам необходимо сделать две вещи:
    a. прописать в реестре путь к файлу драйвера для USB ELM327 (а т.к. реестр у нас по умолчанию не сохраняемый, нам и придется препарировать прошивку)
    b. Положить файл драйвера в образ прошивки.

4. Итак, приступаем: запускаем remaker_ce6, видим окошко как на картинке ниже. Нажимаем над левым полем Dump -> DumpProject NB0 -> Dump .bin



5. Начнем с реестра, для этого в появившемся окне откроем наш TINYNK.BIN из шага 3. Видим перед собой дерево файлов, нам нужен default.fdf - собственно сам файл реестра. Кликаем на

нем правой кнопкой и выбираем “Извлечь” (к сожалению, Remaker_CE6 все еще в статусе “бета” и функция “Редактировать” в нем не работает).



6. Полученный файл преобразуем в REG формат при помощи perl-скрипта fdf2reg отсюда http://4pda.ru/forum/index.php?s=&showtopic=119060&view=findpost&p=2660765 Там же можно подробнее почитать про изменение реестра, у нас - ROM BASED реестр.
7. полученный REG-файл необходимо отредактировать обычным блокнотом, добавив в него содержимое REG-файла из комплекта FTDI драйверов для WinCE6. Сами драйверы берем здесь http://www.ftdichip.com/Drivers/VCP/WinCE/CE60/ARMv4VCPDriver60_1.1.0.20.zip

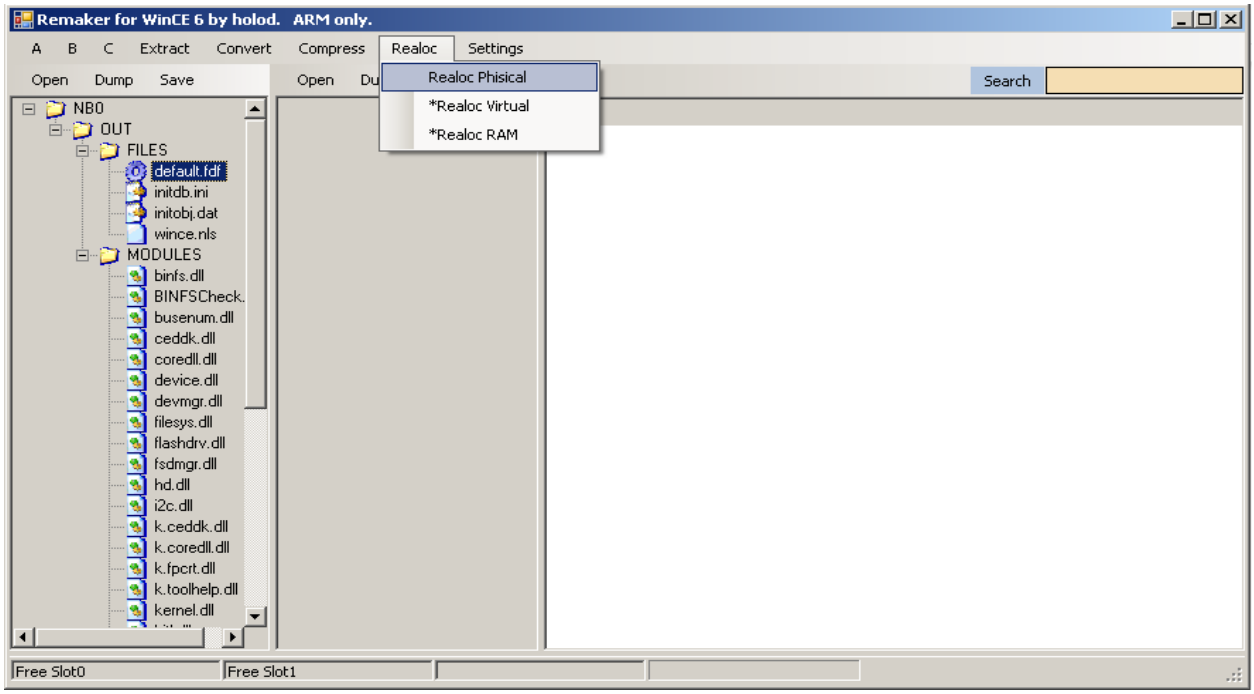
   В архиве есть файл FTDI.REG, его содержимое необходимо скопипастить в наш файл реестра из шага 6.

   Обратите внимание, в квадратных скобках в файле указаны имена разделов, далее обычно следуют параметры внутри этого раздела. Содержимое файла FTDI.REG необходимо вставить после последнего параметра, перед именем очередного раздела. Я делал так: искал поиском строку “[HKEY_LOCAL_MACHINE\Drivers\USB\ClientDrivers\”, и между разделами вставлял необходимые данные.

```
[HKEY_LOCAL_MACHINE\Drivers\USB\ClientDrivers\Printer_Class]
"IClass"="{4FE1CEF1-E765-4a1e-B503-5B8C674D7C68}"
"Prefix"="LPT"
"DLL"="USBPRN.DLL"

[HKEY_LOCAL_MACHINE\Drivers\USB\ClientDrivers\Hid\Hid_Class]
"QueuedTransferCount"=dword:00000002
"Prefix"="HID"
"DLL"="USBHID.DLL"

ВСТАВЛЯТЬ СЮДА



[HKEY_LOCAL_MACHINE\Drivers\USB\ClientDrivers\Hid\Instance]
"DLL"="USBHID.DLL"
```

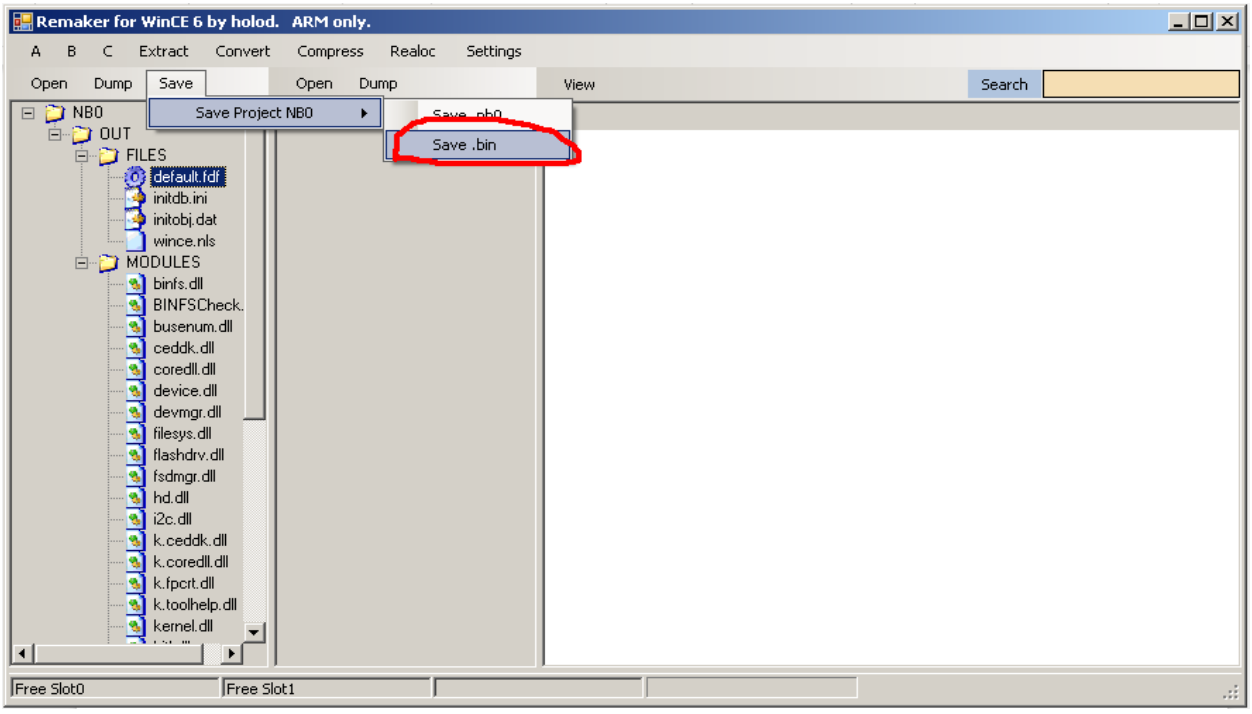
После чего сохраняем наш реестр в REG-формате и преобразуем обратно в default.fdf

8. Далее нам необходимо удалить старый default.fdf из образа TINYNK.BIN и заменить его свежесгенерированным, содержащим необходимые записи для драйвера FT232. Для этого все в том же окне remaker_ce6 кликаем на файле правой кнопкой, выбираем “удалить”. После чего последовательно нажимаем пункты в меню
Realloc.



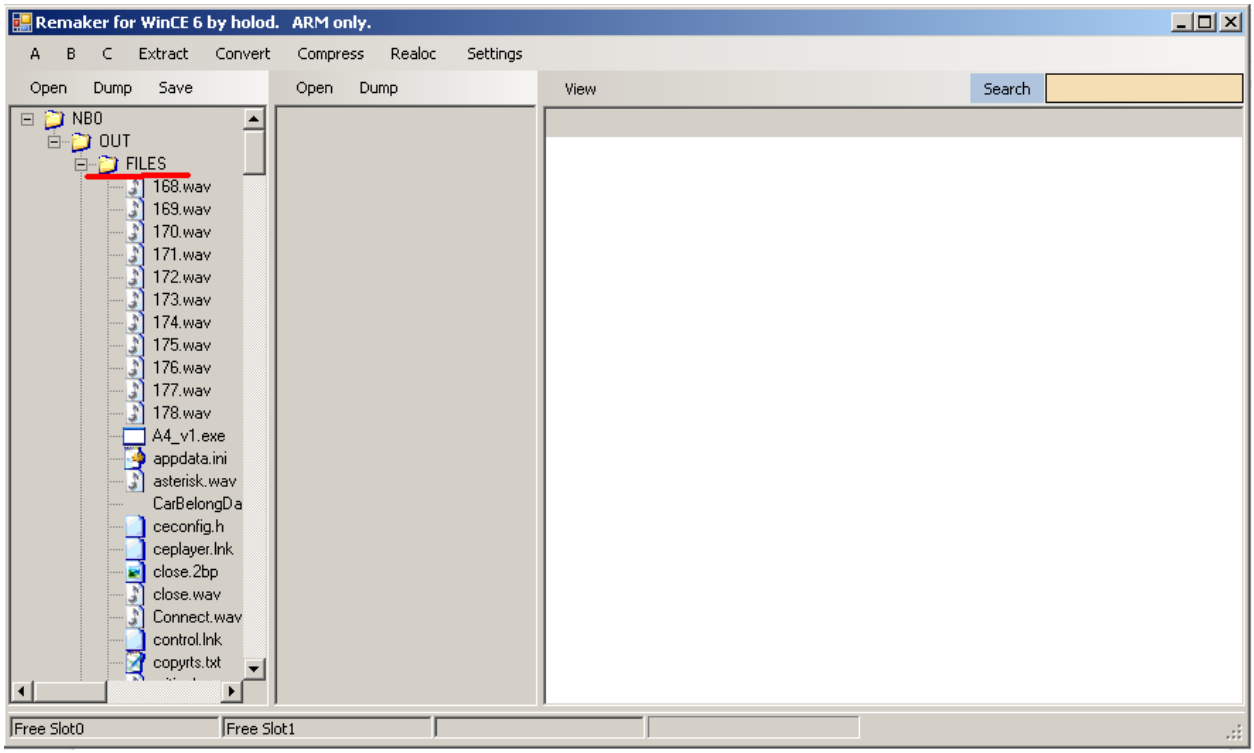
Эти действия для себя я обозначил на уровне “шаманства”, т.к. разбираться досконально что именно делает каждая из кнопок мне было лень, а без них у меня в некоторых случаях пропадала папка ResidentFlash из операционки.

9. Отредактирванный default.fdf методом drag’n’drop перетаскиваем на старое место, после чего опять Realloc по всем пунктам и “ Save -> Save Project NB0 -> Save .bin”



10. Готово, сохраняем файл под именем TINYNK.BIN и кладем в набор для прошивки на SD карту.

11. Далее, аналогичным образом открываем файл NK.BIN и видим следующее дерево:



Берем файл ftdi_ser.dll и перетаскиваем его в секцию FILES. Не могу сказать насколько необходимо этому файлу быть в секции MODULES или FILES, в обоих случаях у меня драйвер работал. Но, иногда добавление в секцию MODULES не происходило по причине нехватки свободных слотов. Не знаю, то ли баг бета-версии remaker'a, то ли так и должно быть. В любом случае, в секции FILES работает отлично, поэтому помещаем файл туда.

12. Далее меню Realloc последовательно по всем пунктам, потом "Save -> Save Project NB0 -> Save .bin". Сохраняем файл под именем NK.BIN и так же помещаем его на SD карту в набор для прошивки.
13. В итоге мы имеем на SD карте все файлы, которые предоставлялись производителем в виде обновления прошивки, при этом TINYNK.BIN и NK.BIN содержат необходимые нам изменения в реестре и соответствующий файл драйвера. Можно прошивать в магнитолу.
14. Если исходные файлы для модификации были взяты не из комплекта от производителя, а из дампа магнитолы, необходимо обратить внимание на следующие моменты:
    a. необходимо убедиться, что комплект файлов для прошивки на SD карте содержит следующие файлы:

       chain.bin
       chain.lst
       EBOOT.nb0
       hgs4.fmt
       hgs4.upd
       NK.bin
       store.bin
       TINYNK.bin

       Самый тонкий момент это файл EBOOT.nb0, это загрузчик. Если у вас нет 100% подходящего к вашей магнитоле загрузчика (и нет опыта восстановления магнитолы через JTAG) лучше прошивкой не заниматься.

Насколько я понимаю, при обновлении прошивки на данной платформе стирается полностью весь NAND и прошивать загрузчик необходимо в любом случае. Могу ошибаться, но пробовать шить без загрузчика я не решился.
Файлы hgs4.fmt и hgs4.upd это просто пустые файлы, по их наличию загрузчик понимает что SD карта не простая и надо попытаться обновить прошивку с нее.

b. файл chain.bin, созданный программой Sourcery на шаге 2 из вашего дампа не содержит всей необходимой инфы. Необходимо вручную поправить адреса регионов, как описано здесь http://4pda.ru/forum/index.php?showtopic=119060&st=2760#entry5253583 читать после фразы “Почему почти готовый? Потому что **Sorcery** не прописывает адрес загрузки для **Chain.bin**.”
c. Файл chain.lst имеет следующее содержимое:
+TINYNK.bin
NK.bin
chain.bin