SIEMENS VDO SIMK31/41/43

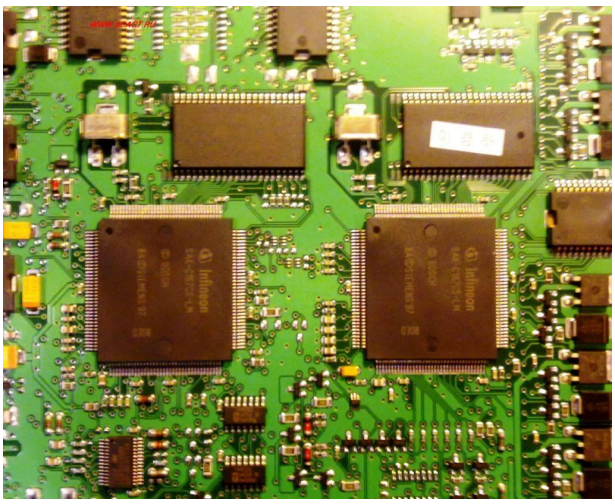
ADACT ACADEMY 2010

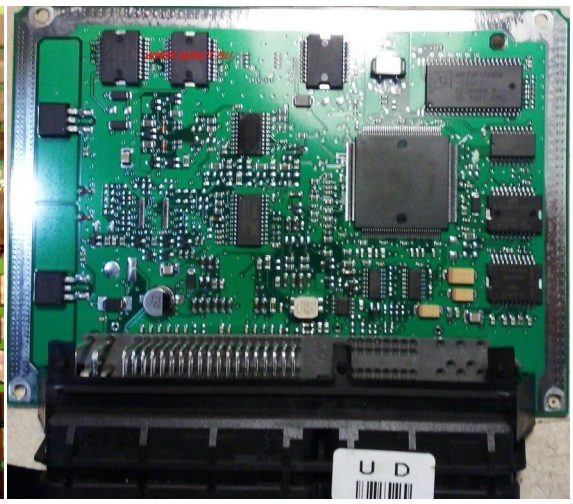
1.1 SIMK_31/41/43 ПОДРОБНО:

Начиная с 2001 модельного года по 2010 модельный год на ряд легковых автомобили концерна KIA-HYUNDAI с 16 клапанными бензиновыми двигателями объемом 1.8L, 2.0L, 2.4L, 2.7L с МКПП и АКПП устанавливались ЭБУ SIEMENS VDO SIMK_31/41/43

Как правило ЭБУ расположены в салоне автомобиля над левым коленом водителя и крепятся через пластину-переходник двумя гайками и одним болтом.

Принципиально ЭБУ построены на базе 16-ти разрядного процессора C167, работающего в паре с FLASH памятью AM29F400BB.
В блоках автомобилей оборудованных МКПП используется один процессор, в ЭБУ автомобилей с АКПП используются соответственно два процессора и две микросхемы внешней памяти. Второй работает совместно с первым и управляет АКПП.





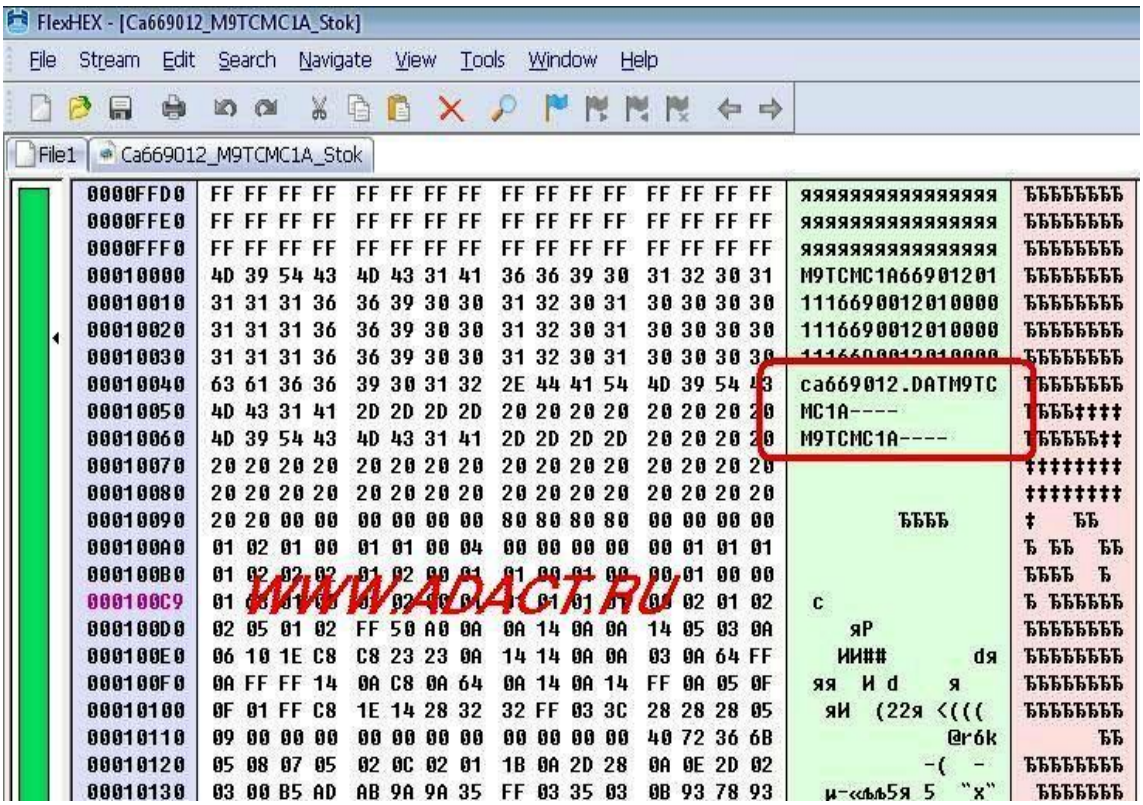
1.2 МАРКИРОВКА ПО:

Буквенно-цифровой код маркировки прописывается в калибровках и выглядит примерно так:

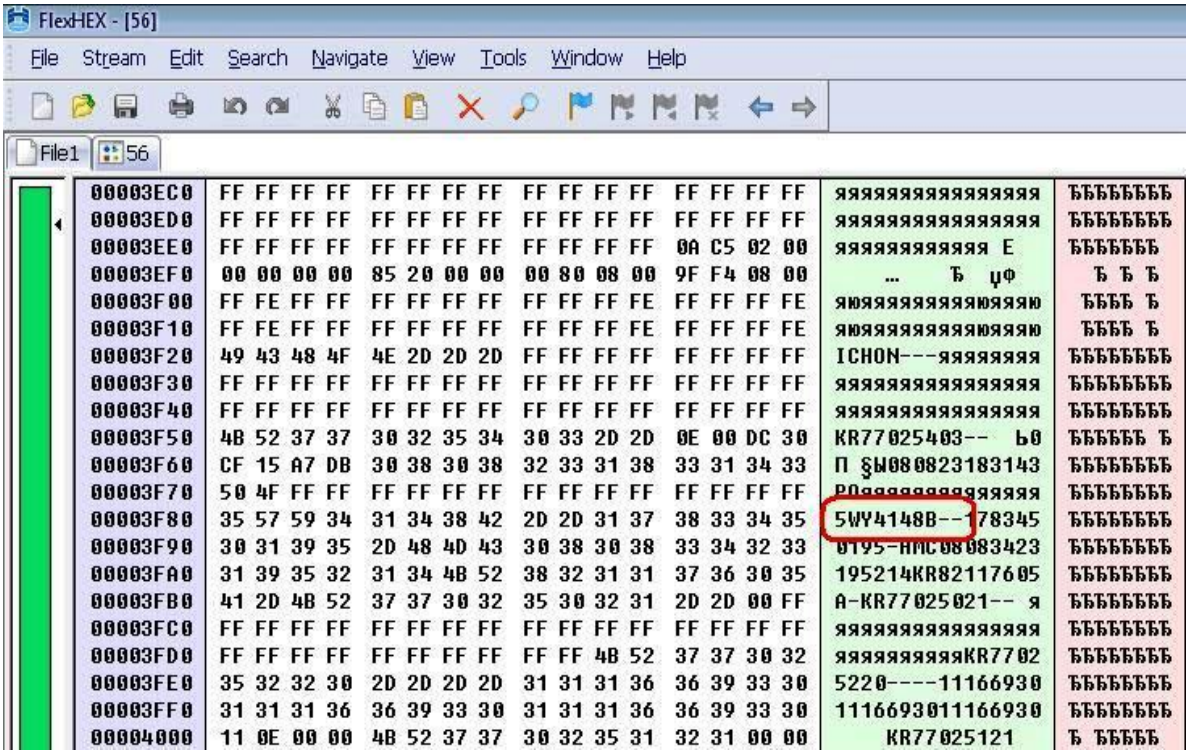
ca669012.DAT
M9TCMC1A---- , где

ca669012 - Software ID (Идентификаторы базового софта)
M9TCMC1A - Hardware ID (Идентификаторы калибровок)

Данный код маркировки можно увидеть открыв ПО в любом HEX-Редакторе.



Кроме того в eeprom прописывается заводской код маркировки данной комплектации ЭБУ, он же указываются и на шильдике приклеенном к самому блоку управления.



ВНИМАНИЕ!

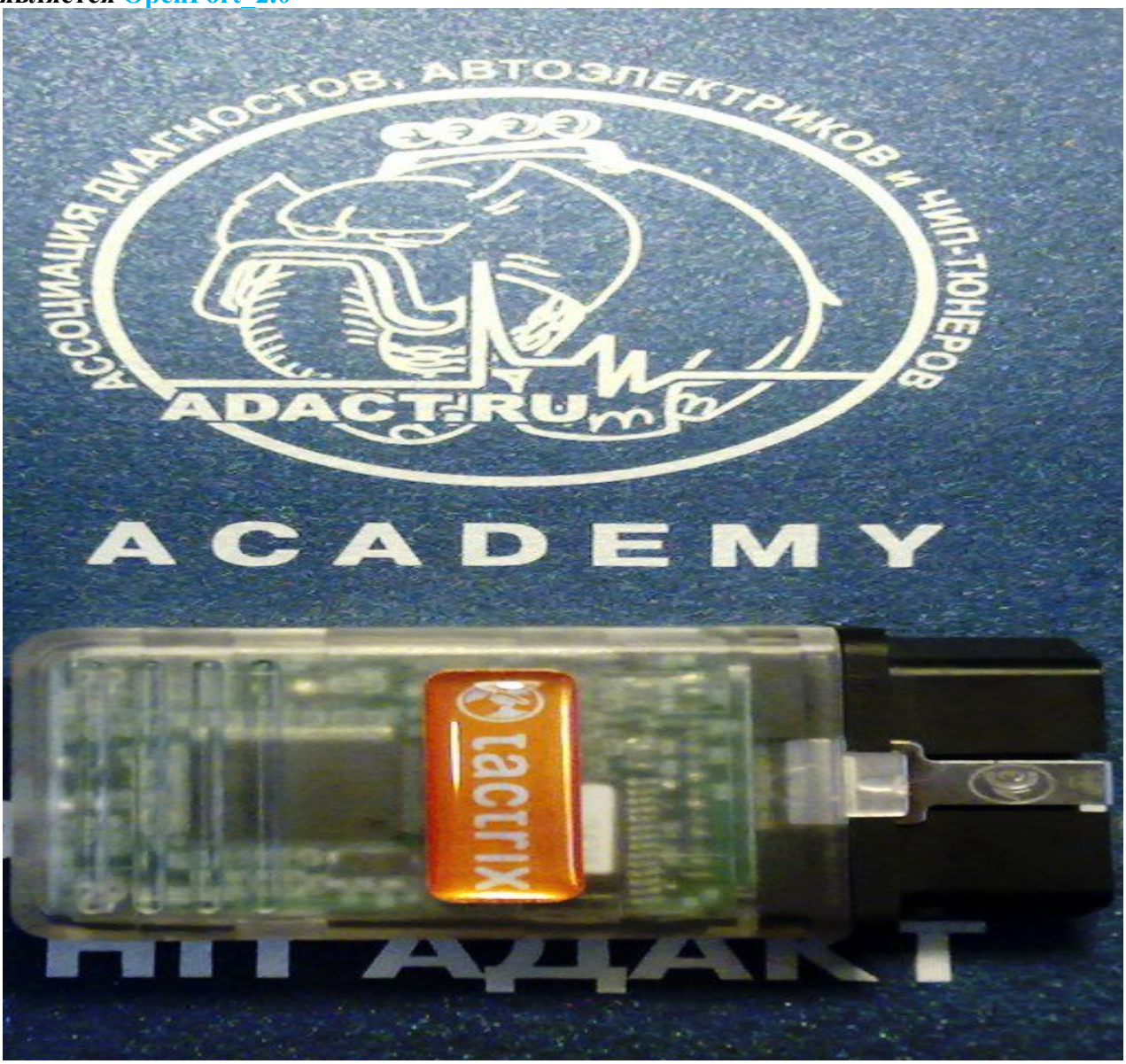
В пределах одного софта ВСЕ прошивки СОВМЕСТИМЫ!

Reprogramming:

На сегодня имеются различные варианты перепрограммирования этих ЭБУ.

1. **Флешеры.**

Устройства позволяющие работать с ЭБУ через диагностическую колодку. Из наиболее доступных на сегодня широкому кругу тюнеров это CombiLoader **и** ChipLoader 2.3**. С большинством ЭБУ этого семейства данные флешеры способны работать без дополнительного адаптера, но на ряде автомобилей начиная с 2008 года, а с 2010 года на всех автомобилях с установленным данным типом ЭБУ отсутствует K-Line в диагностическом разъеме, что делает невозможным перепрограммирование данных ЭБУ через обычный K-Line адаптер. Здесь нам поможет интерфейс работающий по одному из вариантов базового протокола J2534 с соответствующим модулем для вышеназванных загрузчиков. Самым доступным по цене-качество на сегодня является OpenPort 2.0**



2. Внутрисхемные программаторы.

Устройства позволяющие работать с семейством процессоров C167xxx через BSL-режим «на столе». Например -ChipLoader
-CombiLoader

Достоинства:
- Позволяют «поднимать уснувший» ЭБУ
- Малобюджетны по сравнению с флешерами (зачастую работают с обычным K-Line адаптером)

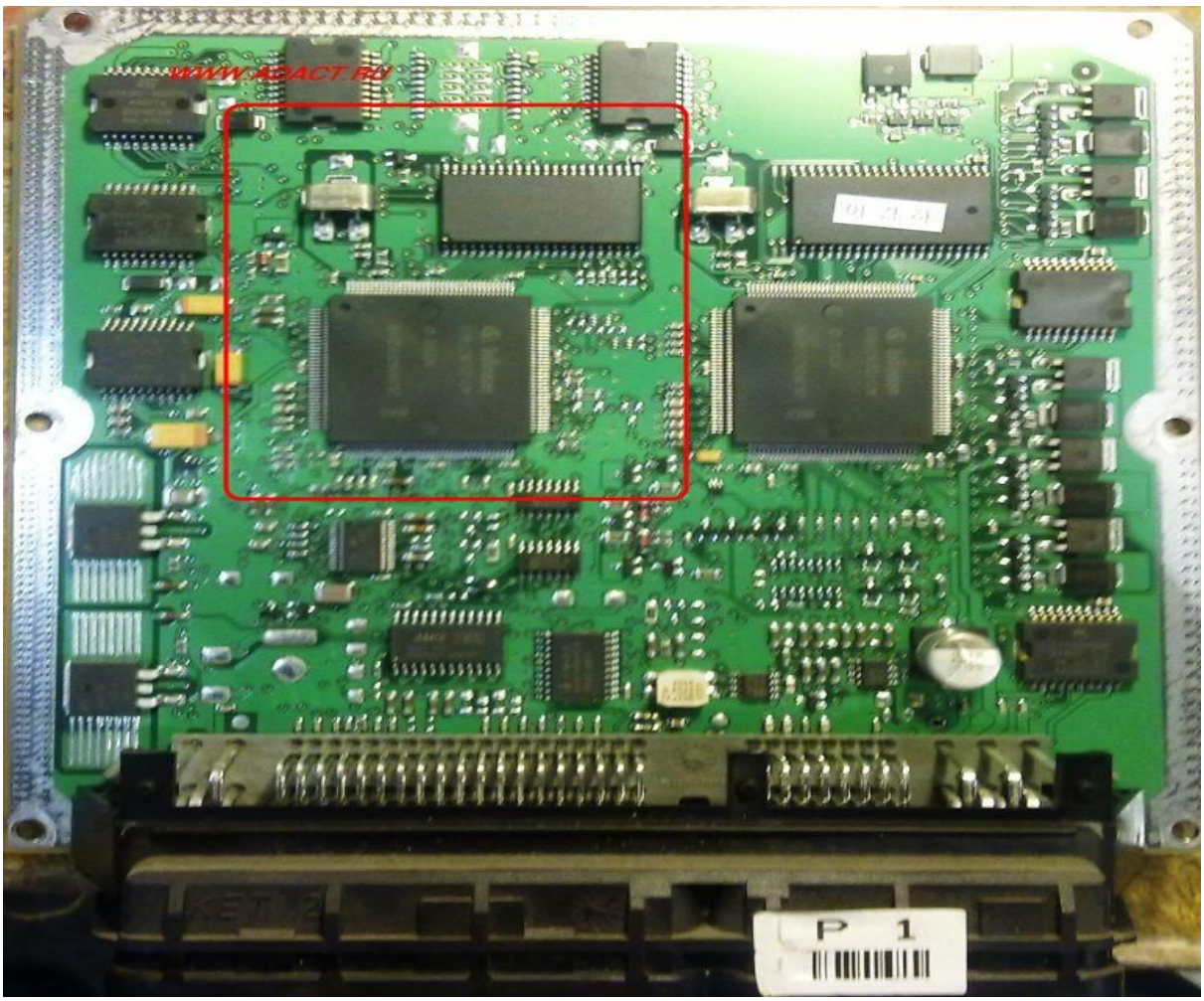
Недостатки:
- Необходимо знать точки коммутации для перевода процессора в BSL-режим, подключения питания «на столе» и подключения линии диагностики.
- Определенная трудоемкость по снятию и разборке ЭБУ

Подключение к ЭБУ Siemens 5WY SIMK 41, SIMK 43 с двумя разъемами

81-пиновый разъем

2 - масса ЭБУ (-12В)
3 – Постоянное питание (+12В)
83 - Зажигание (+12В)
47 - K-Line

В ЭБУ автомобилей с АКПП операции по переводу процессора в BSL-режим проводятся с процессором находящимся со стороны 81-пинового разъема.



Подключение к ЭБУ Siemens 5WY 5 разъемов

Левый 9-пиновый разъем

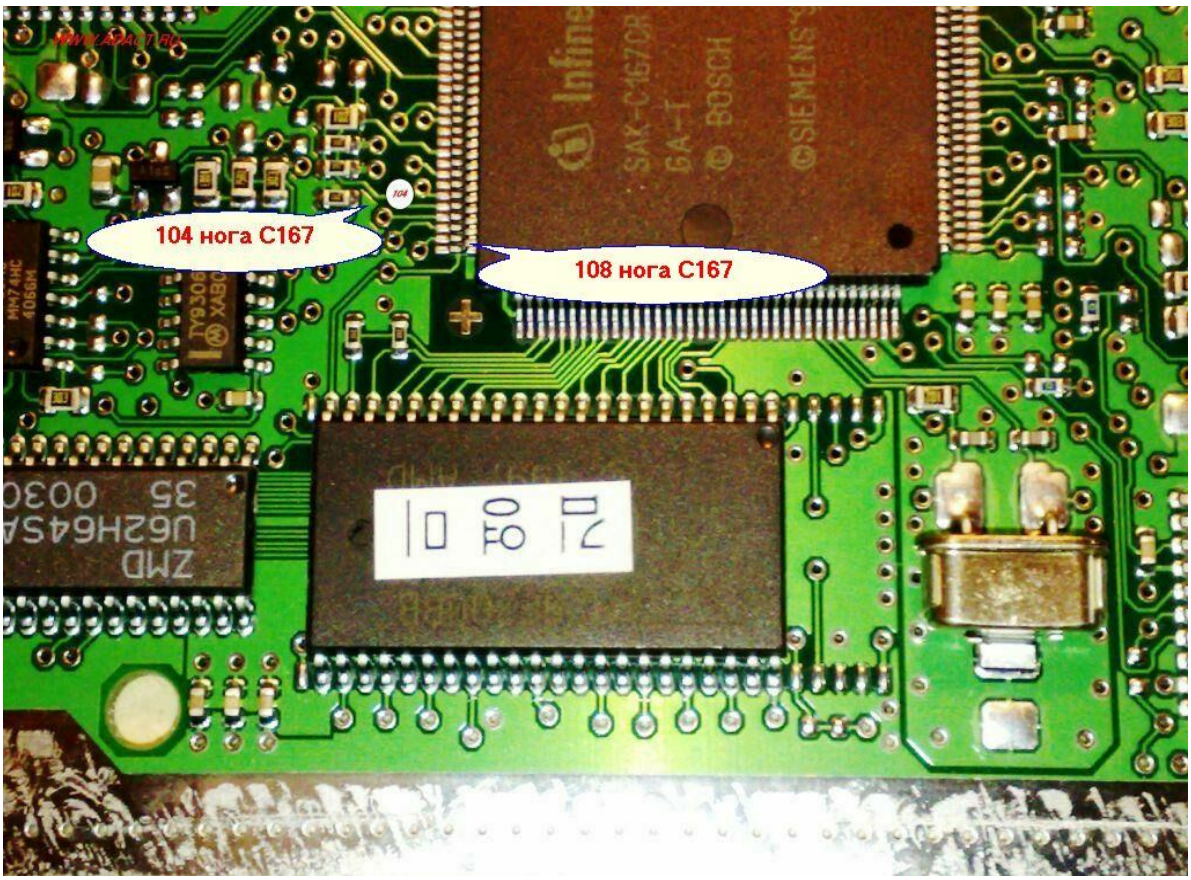
4,5,6 – масса ЭБУ («-12В») (используется любой из перечисленных контактов)
1,7,8,9 – «+12В»
3 – K-Line

Подключение к ЭБУ Siemens 5WY SIMK 31 с двумя разъемами

81-пиновый разъем

1,2 – Масса ЭБУ («-12В»)
21,22,44,63 – «+12В»
77 – K-Line

Для чтения-записи необходимо до подачи питания на ЭБУ замкнуть 104 ногу процессора C167 или 28 ногу FLASH-памяти на массу через резистор 6.8-10кОм.



3. Внешние программаторы микросхем

Для работы с микросхемой FLASH AM29F400BB в корпусе PSOP44 понадобится паяльная станция, программатор, работающий с данным типом микросхем ,и «КРОВАТКА-Переходник» для нее.

При считывании содержимого FLASH-памяти во внешнем программаторе мы имеем считанные данные в так называемом «криптованном» виде. Как и во многих современных ЭБУ, программисты Siemens, дабы усложнить доступ к содержимому своих блоков для посторонних людей, используют криптоалгоритмы. В данных используются алгоритмы Siemens 2001.

Другими словами в считанном криптованном виде в некоторых редакторах просмотреть ПО будет не реально.

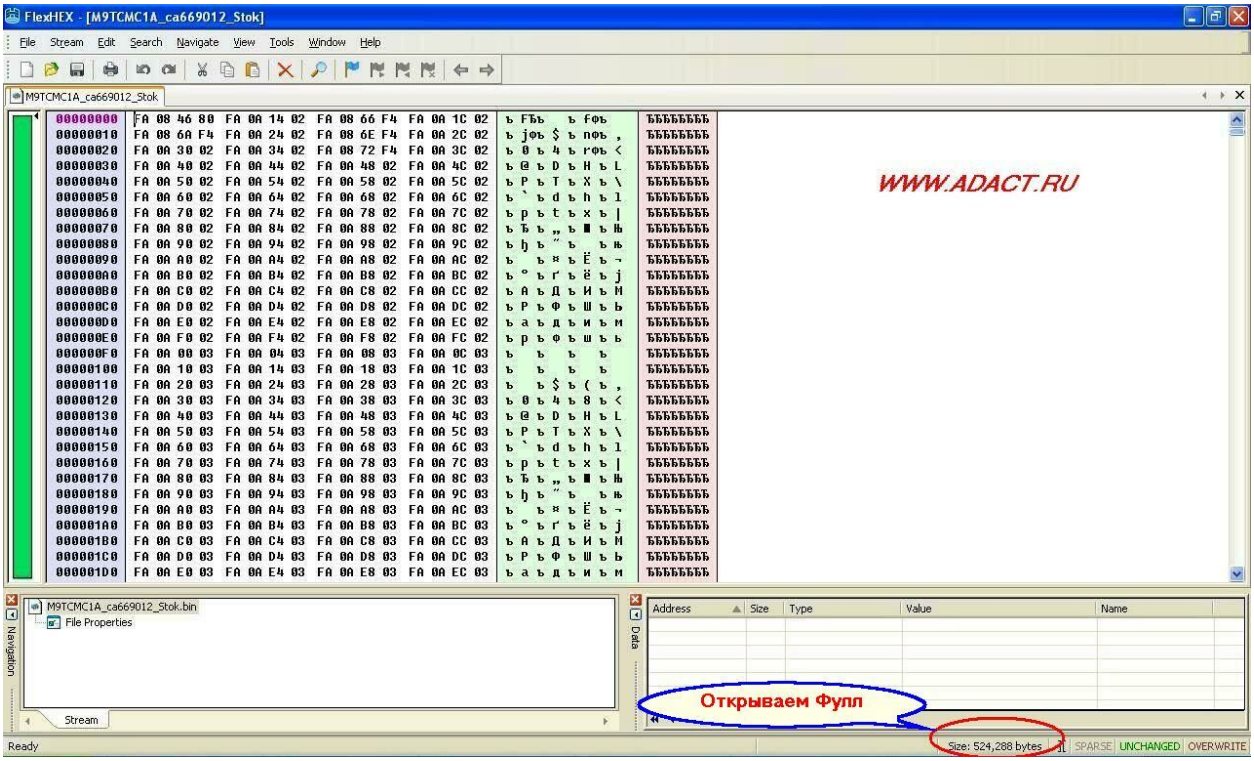
Далее рассмотрим более подробно репрог с использованием внешнего программатора, ибо с репрогом посредством специализированных флешеров достаточно все понятно.

Итак, с помощью любой доступной паяльной станции «сдуваем» микросхему FLASH. Зачищаем надфилем контакты микросхемы, вставляем ее в панель-переходник, и считываем ее содержимое во внутренний буфер программатора.

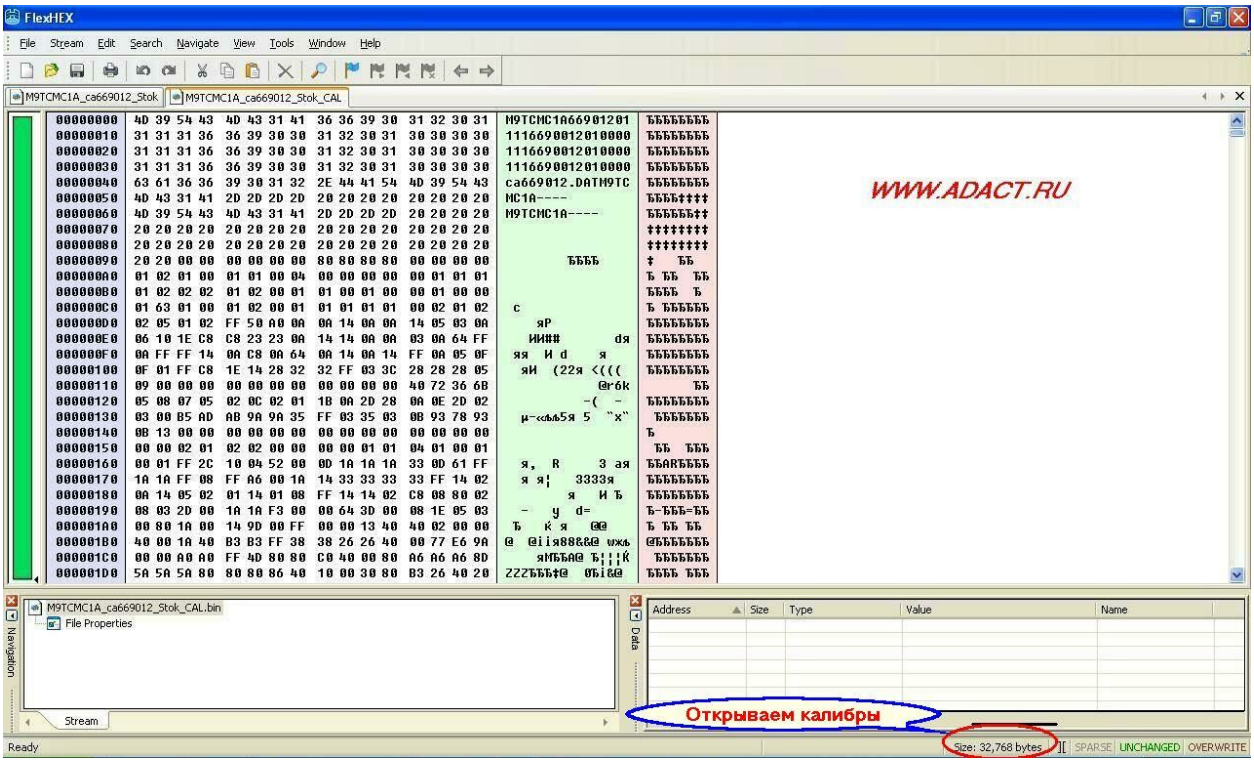
В последующем с помощью программы, ну например ECM 2001, АДАКТ-Флешер, WinOls,CTP_7x декриптуем считанную прошивку в обычный «BIN» формат и сохраняем ее.

Далее рассмотрим порядок работы с прошивкой на примере Hyundai_Tucson 2.0L:

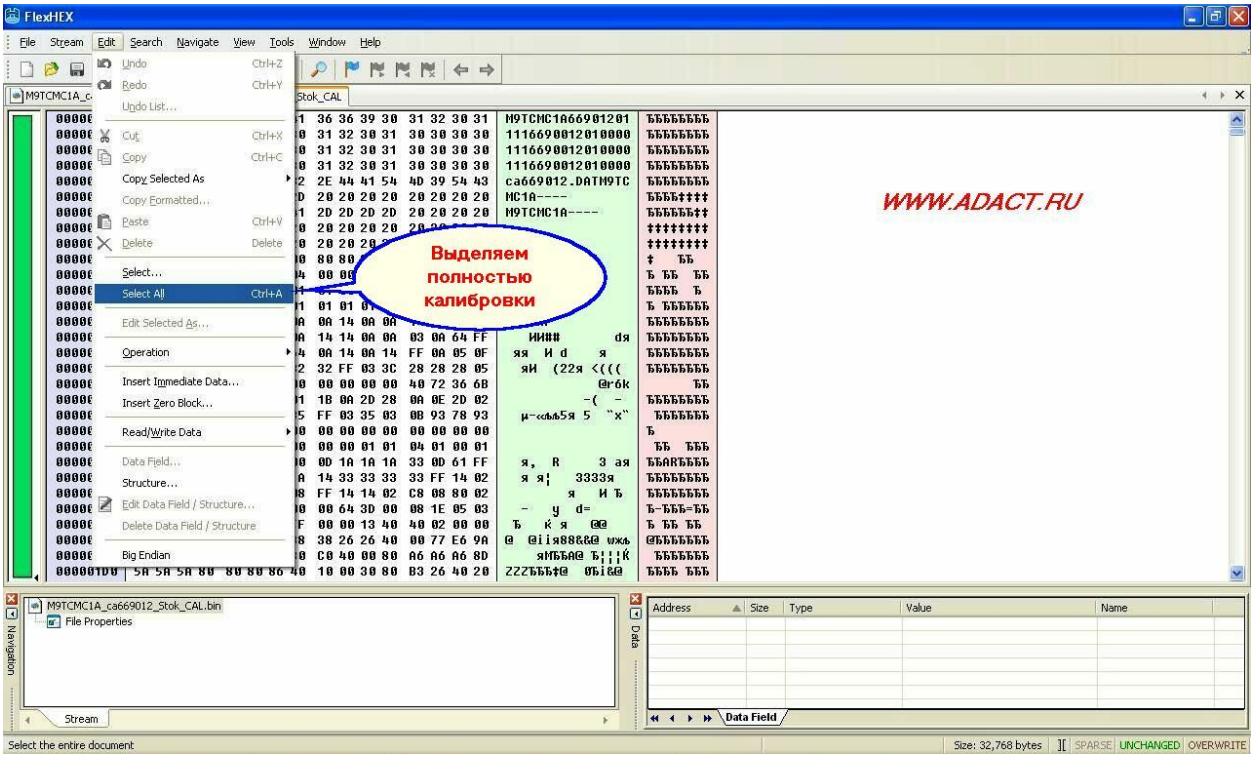
1. Открываем прошивку в HEX-Редакторе

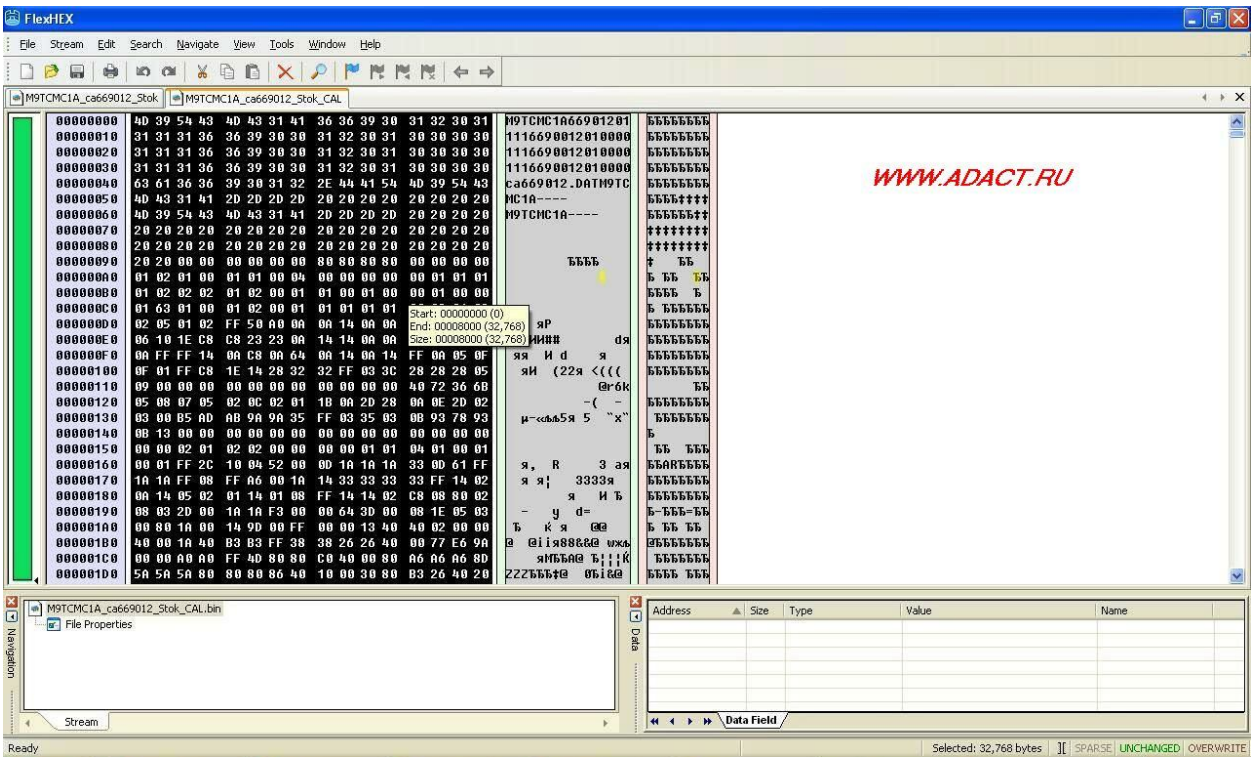


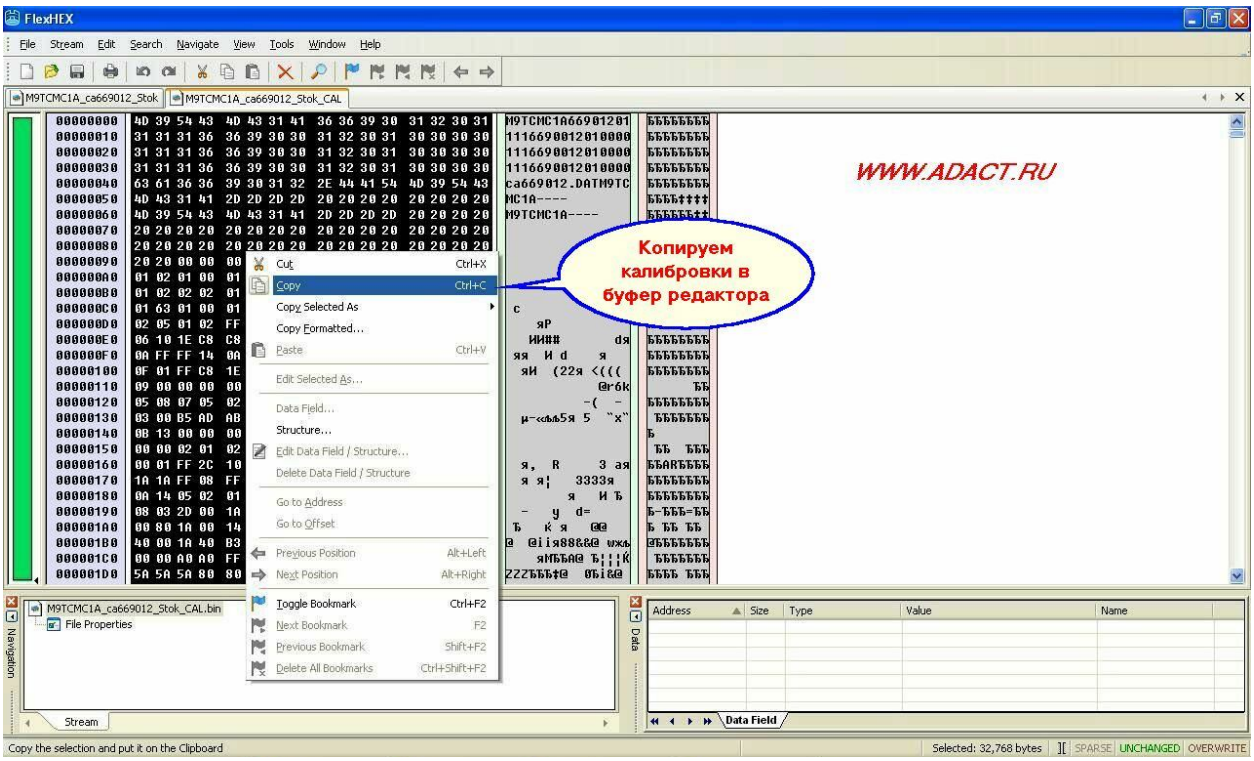
2. Открываем модифицированные калибровки.



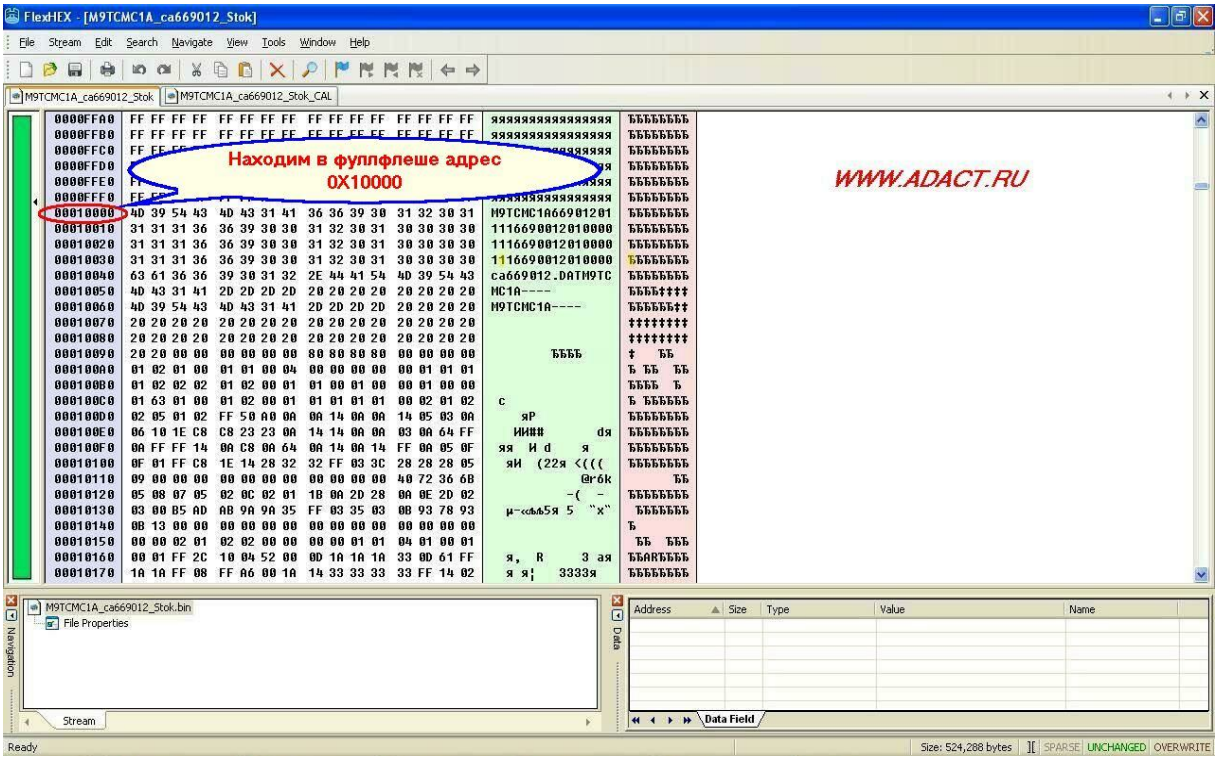
3.Выделяем калибровки и копируем их в буфер программы.



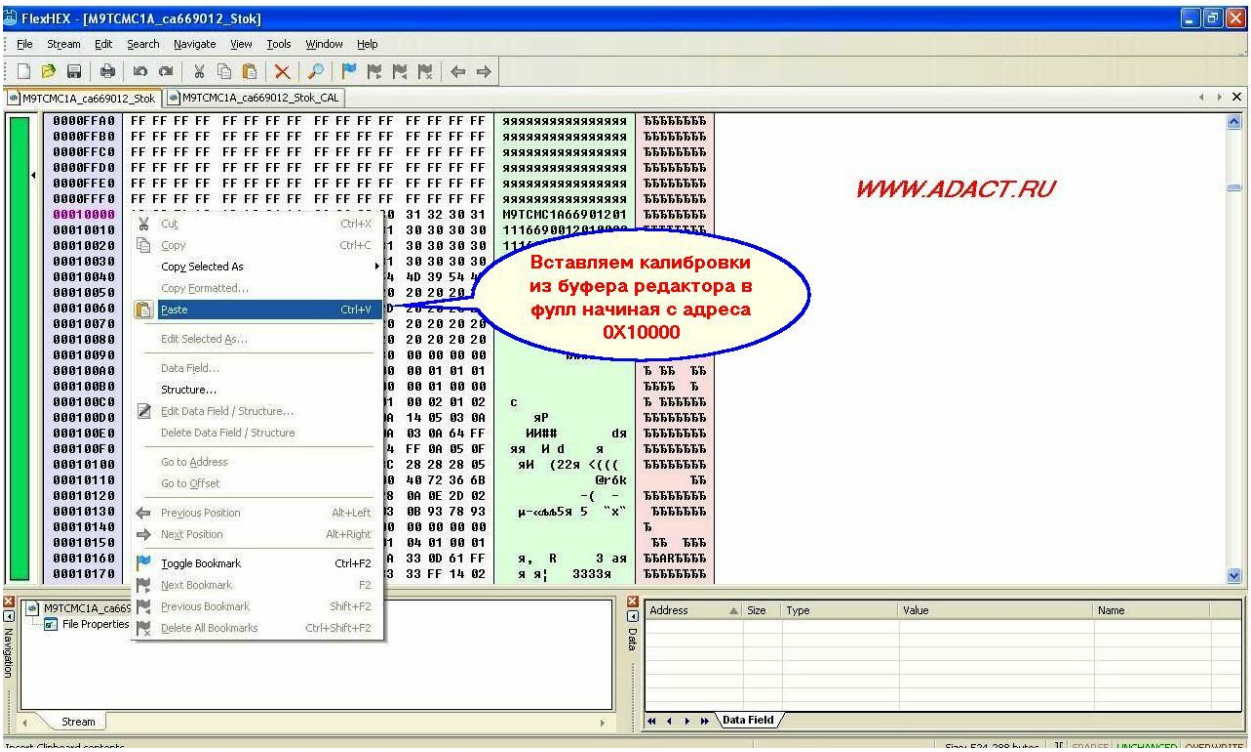




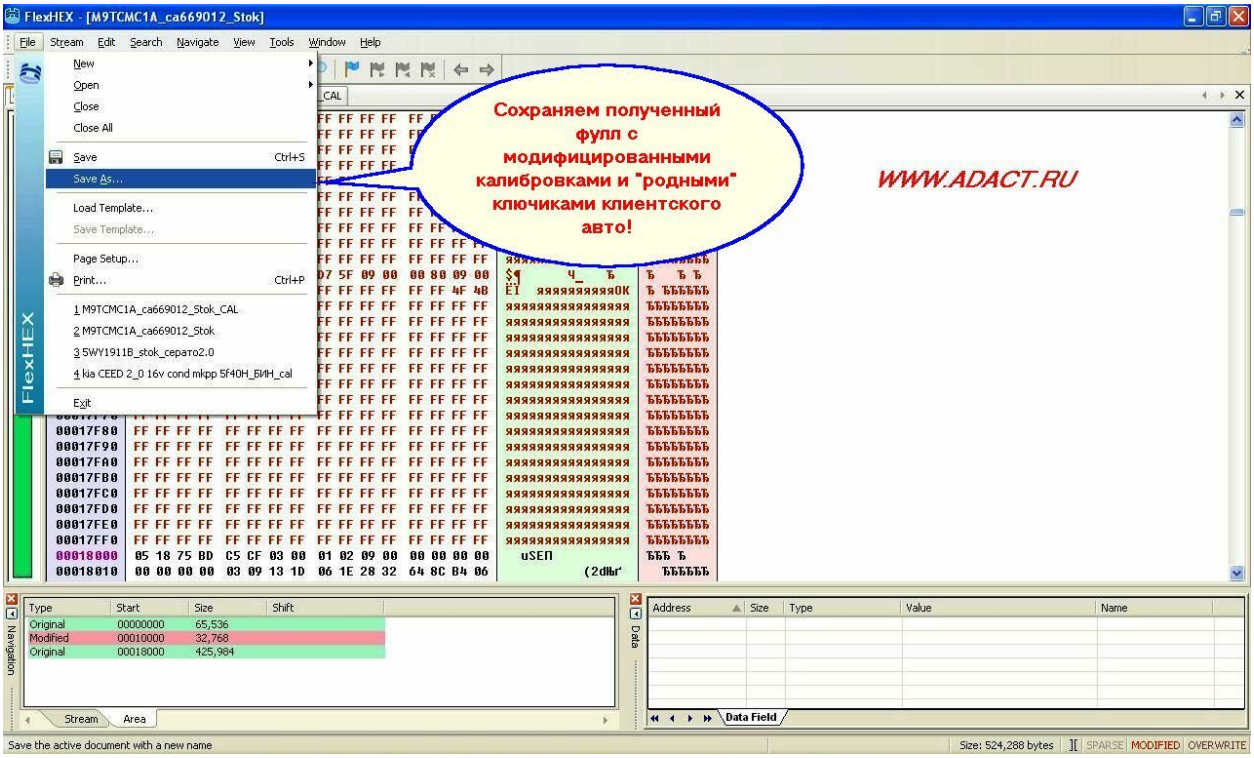
4.Выбираем вкладку со считанной прошивкой и в редакторе ищем адрес 0X10000



5.Вставляем модифицированные калибровки в считанный фулл начиная с адреса 0X10000



6.Сохраняем полученную прошивку



криптуем получившийся «BIN» файл по обратной процедуре, записываем файл во флешь и запаиваем ее в ЭБУ.

МОДИФИЦИРОВАННОЕ ПО:

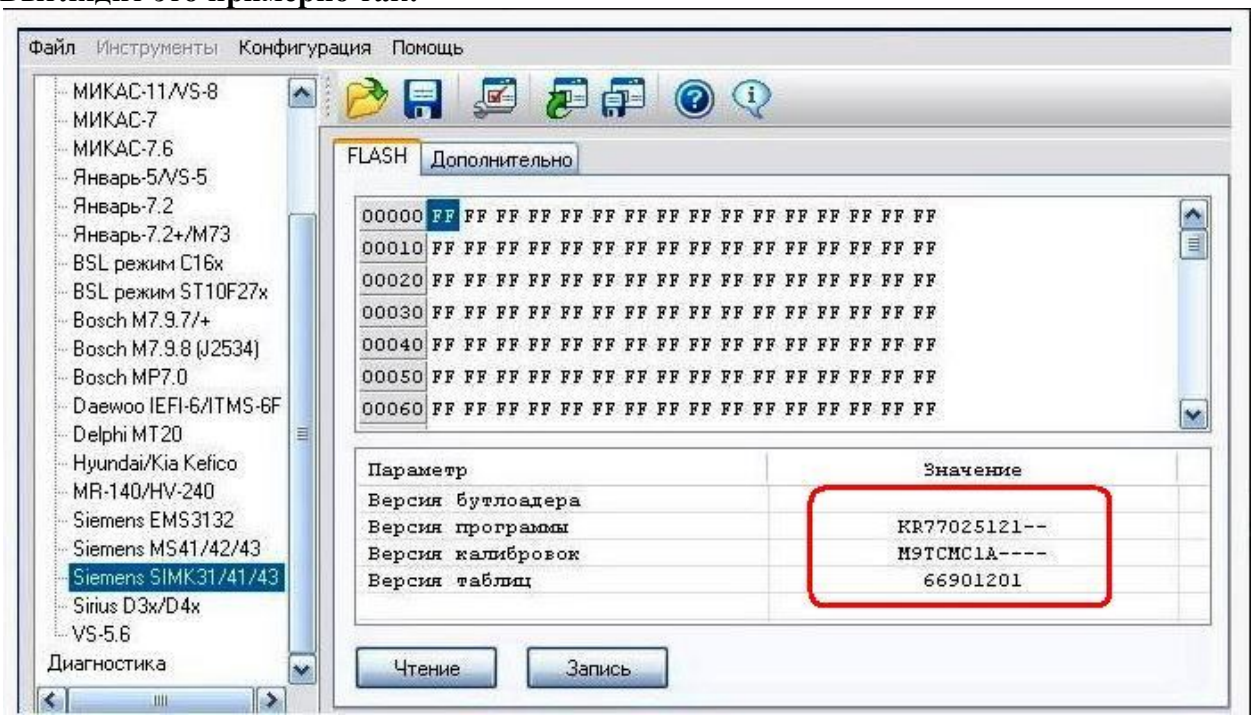
Во всех модифицированных прошивках улучшена динамика за счет оптимизации УОЗ и Топливоподачи, изменен алгоритм работы системы в режиме кондиционирования, алгоритм динамической коррекции УОЗ и Anti-Jerk. Оптимизирована работа системы в режиме XX. Снижен расход топлива.

ВНИМАНИЕ!

Во избежание проблем с «засыпанием» ЭБУ, необходимо заливать в блок модифицированные прошивки откалиброванные на базе «родного» софта, т.е. Software ID вида например: Ca663045 в родных и модифицированных прошивках должны совпадать.

Все флешеры позволяют определить ID Базового софта конкретного ЭБУ.

Выглядит это примерно так:



Ну и конечно желательно чтобы Hardware ID (Идентификаторы калибровок) были родственными. При наличии модифицированной прошивки сделанной на базе «родного» софта переливать полностью FULL нет необходимости, при работе флешерами обновляйте только калибровки. Это связано с особенностями «организации» FLASH-памяти ЭБУ.
В данных типах ЭБУ физическая память EEPROM отсутствует. Данные, которые хранятся в euro, эмулируются внутри самой FLASH-памяти. В первую очередь это данные по синхронизации ЭБУ с модулем иммобилайзера. При заливке чужого FULL-FLASH в ЭБУ, машина не заведется. Избежать данной неприятности возможно несколькими способами:
1.Заливать модифицированное ПО сделанное на базе считанного из ЭБУ «родного» софта.
2.Заливать только модифицированные калибровки.
3.Считывать «родной» eeprom и при необходимости заливать его после репрога.

4. Воспользоваться утилитой загрузчика Дениса Супруненко ChipLoader которая копирует все необходимые данные из «родной» прошивки в модифицированную.
5. В «ручную» в любом HEX-Редакторе подготавливать модифицированную прошивку перенося в нее данные из области eeprom оригинальной прошивки.

Но, если вдруг произошло то, что произошло. И Вы по какой-то причине залили флешером «враждебный» софт, сильно страшного ничего нет, т.к. как и описывалось эти блоки можно «поднять» на столе через BSL-режим.

Ознакомиться с перечнем модифицированных прошивок и ценами на них можно по адресу: http://forum.adact.ru/index.php/topic/7131/ и http://forum.adact.ru/index.php/topic/5980/