



1 2  
mode select

+12v  
Hi  
Lo  
gnd

## MB FBS3 emulator

for CAN HS  
500kB

Разработан как альтернатива и подмена оригинальному иммо работающему по принципам **FBS3** (авторизация на хэшах). Необходимые исходные данные такие же, как и для ИК ключей - для работы эмулятора необходима начальная хэш, счётчики, номер трэка.

### Конфигурация:

перемычка MODE на эмуляторе должна быть разомкнута. Для конфигурирования необходимо подключить любой CAN логгер, скорость коммуникации - 500кб.

#### Использованные сокращения:

-> передача на эмулятор

<- ответ от эмулятора

**YLED** значит жёлтый светодиод, **RLED** соответственно красный (оба расположены на левом верхнем углу эмулятора).

**Шаг 1:** необходимо передать эмулятору начальную хэш (initial hash)

пример: передаём 14C2DAE130F81AC8

-> 7F0 (8) 14 C2 DA E1 30 F8 1A C8

<- 7FF (8) 14 C2 DA E1 30 F8 1A C8

**YLED** начинает мигать подтверждая приём.

**Шаг 2:** необходимо передать номер трэка (track) и счётчики (distance)

пример: track = **3**, distance = **2F1F7F**. В данном примере передаётся максимальная возможная величина (life=0x2FFFF) соответствующая жизненному циклу нового ключа, однако возможно конфиурировать эмулятор под любую годную величину начиная от 000001 до 2F1F7F)

-> 7F1 (8) 03 2F 1F 7F 00 00 00 00

первая часть ответа от эмулятора, приходит сразу в качестве подтверждения принятия:

<- 700 (4) 03 2F 1F 7F

Если всё в порядке и начальная хэш была принята до этого, эмулятор начинает рассчитывать буферы. **YLED** не горит, **RLED** мигает до окончания расчётов. Пересчёт занимает примерно 20 секунд. По окончании эмулятор в ответ выдаёт рассчитанную хэш для полного диапазона ключа (2F1F7F), независимо от заданного необходимого значения счётчика (это не влияет на рабочий режим, только для контроля).

Вторая часть ответа (буфера рассчитаны, эмулятор готов к работе):

<- 7FF (8) D8 A5 57 F3 F8 FD 87 36

**YLED** включается постоянно, эмулятор готов к работе.

## Рабочий режим:

Переключатель MODE закорочен, эмулятор подключен к ЭБУ через CAN.

после включения **YLED** мигает, эмулятор готов к общению с ЭБУ. После успешной авторизации с ЭБУ **YLED** включается постоянно. Теперь эмулятор проводит некоторые расчёты необходимые для следующего запуска: **RLED** горит, после окончания расчётов гаснет. Это может занять до 1/2 секунды.

Если после авторизации **RLED** и **YLED** оба **мигают синхронно**, авторизация состоялась успешно, однако жизненный цикл подходит к концу - осталось меньше чем 4096 возможных запусков (старший байт актуального счётчика 00) и в скором времени возможно потребуется переконфигурировать под новую начальную хэш или под дугой трэк.

### Состояние ошибки:

В случае если после подачи питания на эмулятор **RLED** и **YLED** оба **мигают переменнно**, эмулятор неготов к коммуникации с ЭБУ. Возможные причины:

- закончился жизненный цикл - счётчики 000000.
- эмулятор неконфигурирован (пустой)

## Дополнительные возможности:

(доступны только в режиме конфигурации — переключатель MODE разомкнут)

### Стереть всё содержимое:

-> 7F1 (8) 55 00 00 00 00 00 00 00

**RLED** горит, в случае успешного завершения процесса гаснет и приходит ответ:

<- 7FF (6) 45 52 41 53 45 44 (ascii: ERASED)

### Запрос текущего состояния и уменьшение счётчиков на 1:

-> 7F1 (8) AA 00 00 00 00 00 00 00

ответ приходит в двух сообщениях:

<- 700 (4) KK DD DD DD, где KK = номер трэка, DDDDDD = текущие счётчики

<- 7FF (8) 8xDATA, где DATA = актуальная хэш

### Запрос блоков данных (EEPROM):

-> 7F1 (8) FF xx 00 00 00 00 00 00, где xx = номер блока данных, от 00 до FF

ответ:

<- 7xx (8) 8xDATA

