

Тема: USB-RFID эмулятор-копировщик

Автор копировщика: iplogger (ru)

## Инструкция

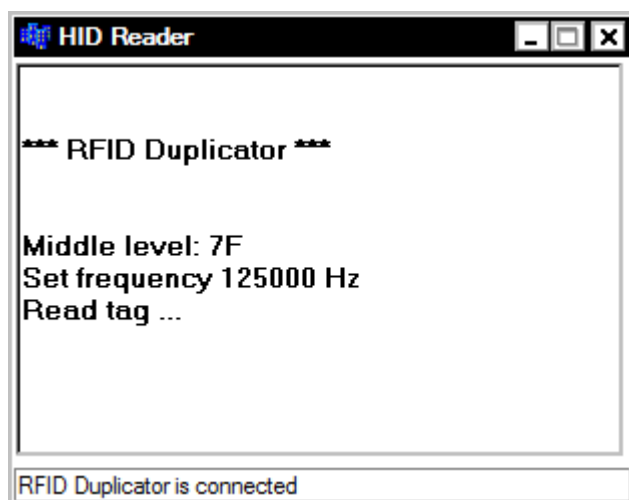
Авторы инструкции: koulja (ua), federic (ru)

2014 год

Итак, запускаем программу SimpleHIDWrite.exe

Обесточенный копировщик подключаем к USB комп'ютера

Загорится светодиод. Ждем 15 секунд, копировщик издаст звук. Устройство готово читать и копировать.



Теперь поднесем карту к катушке

Read tag ... Ok  
Code: 0300485987  
Wait tag remove ... Ok

В EPPROM atmega 16 он запишется в таком виде (на примере PonyProg)

```
003FE0) FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
003FF0) FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
004000) 2F EE FF FF FF FF FF FF - 00 06 00 00 09 11 0A 12
004010) 11 0F 18 FF FF FF FF FF - FF FF FF FF FF FF FF FF
004020) FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
```

Далее устройство входит в режим записи на заготовку

Устройство всегда записывает код последней прочитанной карты, не зависимо от наличия подключения по USB.

## Правила перевода RFID ключа

Имеем код карты

0  
3  
0  
0  
4  
8  
5  
9  
8  
7

Переведем его в вид для хранения в EPROM atmega 16 (HEX)

### Памятка

0 00000 00  
1 00010 02  
2 00101 05  
3 00110 06  
4 01001 09  
5 01010 0A  
6 01100 0C  
7 01111 0F  
8 10001 11  
9 10010 12  
A 10100 14  
B 10111 17  
C 11000 18  
D 11011 1B  
E 11101 1D  
F 11110 1E

Переведем наш ключ **0300485987** в вид 00 06 00 00 09 11 0A 12 11 0F 18 для хранения в EPROM (HEX)

Столбики

1234



|   |       |           |
|---|-------|-----------|
| 0 | 00000 | <u>00</u> |
| 3 | 00110 | <u>06</u> |
| 0 | 00000 | <u>00</u> |
| 0 | 00000 | <u>00</u> |
| 4 | 01001 | <u>09</u> |
| 8 | 10001 | <u>11</u> |
| 5 | 01010 | <u>0A</u> |
| 9 | 10010 | <u>12</u> |
| 8 | 10001 | <u>11</u> |
| 7 | 01111 | <u>0F</u> |
|   |       | <hr/>     |
|   | 11000 | <u>18</u> |

Считаем первый столбик  $0+0+0+0+0+1+0+1+1+0=3$ . Не четная, пишем 1

Считаем второй столбик  $0+0+0+0+1+0+1+0+0+1=3$ . Не четная, пишем 1

Считаем третий столбик  $0+1+0+0+0+0+0+0+0+1=2$ . Четная, пишем 0

Считаем четвертый столбик  $0+1+0+0+0+0+1+1+0+1=4$ . Четная, пишем 0

Пятый столбик **всегда** пишем **0**

Получили двоичное значение 11000. Переведем его в шестнадцатеричное и получим 18

Еще пример

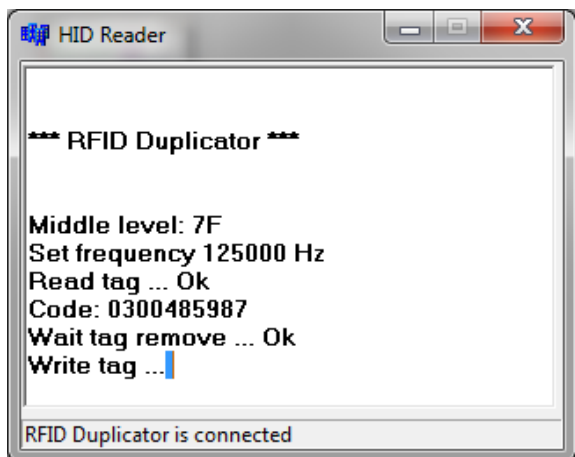
```
2 00101 05
5 01010 0A
0 00000 00
0 00000 00
E 11101 1D
0 00000 00
9 10010 12
6 01100 0C
0 00000 00
9 10010 12
11110 1E
```

## Эмуляция

Включите устройство (подождите 15 сек. для выхода в рабочий режим)  
нажмите кнопку S1 для включения режима эмуляции (пикнет один раз) **Emulator ON** |  
поднесите устройство к домофону. Устройство автоматически выдаст код из EPPROM.  
Нажмите S1 повторно, устройство вернется в первоначальный режим считывания **Emulator OFF**  
Кнопка S2 выводит в режим записи на заготовку.

## Запись на заготовку типа EM-marine, T5557

Включите устройство (подождите 15 сек. для выхода в рабочий режим)  
нажмите кнопку S2 для включения режима записи на заготовку



Поднесите заготовку, устройство запишет в нее код из EPPROM

**Write tag ... Ok**  
**Code: 0300485987**  
**Wait tag remove ... Ok**

+ пикнет 2 раза

Устройство может работать автономно

Эмуляция, считывание и запись на заготовки работает не зависимо от наличия подключения по USB.

Дата составления документа 05.05.2014