Help

You can make electronic keys for Mercedes vehicles via this device and software, check authenticity of the information that keeps in memory dumps from electronic units, edit it and make the reading off of the dumps from the electronic units via K-line, IR-portal (EZS) or CAN.

Attention!
This manual does not pretend to be the most up-to-date. The program is constantly being improved and the latest updates may not be included in this manual. We recommend you to use the button "Help" in the corresponding windows of the program.
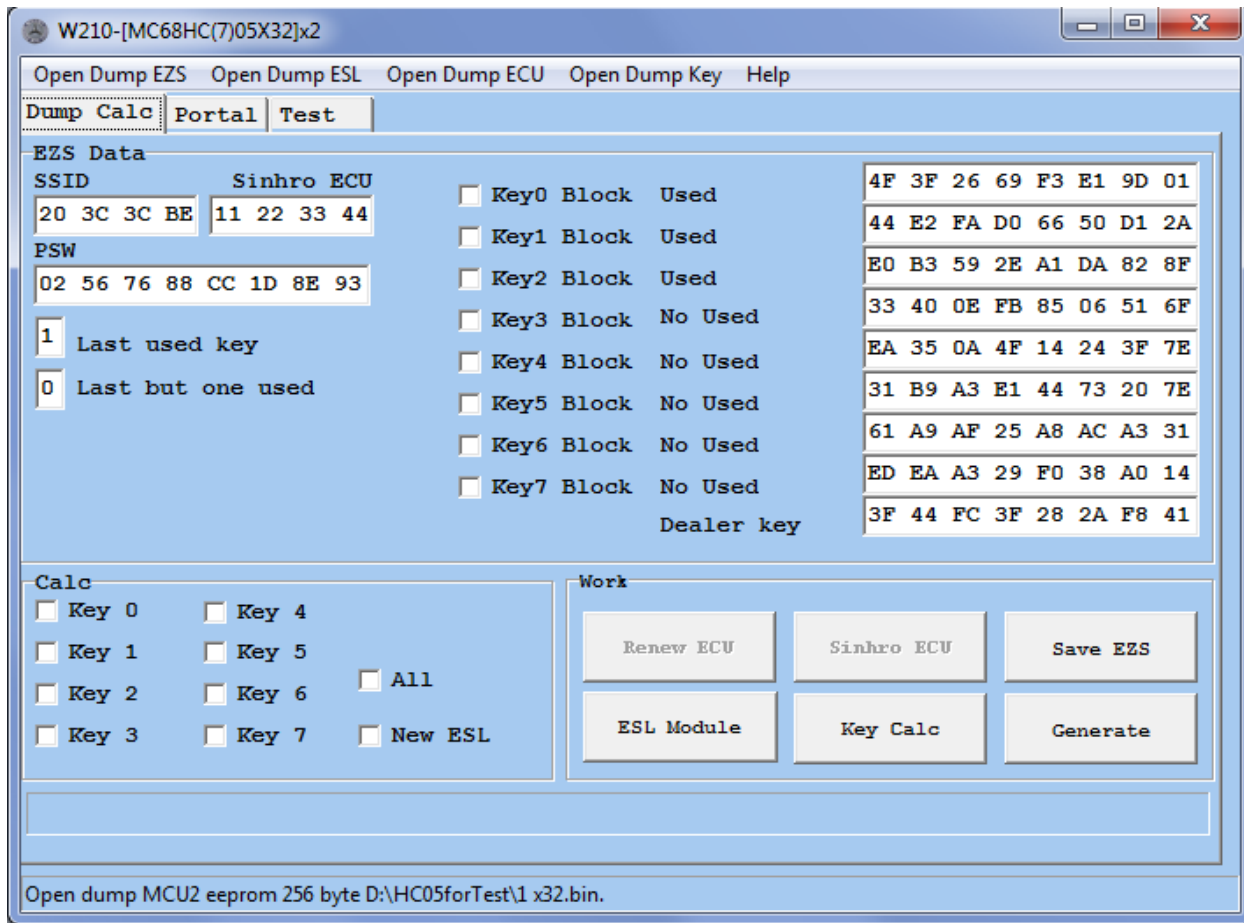
Having connected the basic unit with USB, you are required to set drivers. The process of setting drivers is not considered in this manual.

The main window of the program. There is a choice between a calculator and a module.

There is type of the vehicle and a microprocessor, used for EZS of this calculator version, calculator to choose from.

The window of a dump calculator.


```
W210-[MC68HC(7)05X32]x2

Open Dump EZS   Open Dump ESL   Open Dump ECU   Open Dump Key   Help

Dump Calc  Portal  Test
┌─EZS Data──────────────────────────────────────────────────────────────────┐
│ SSID              Sinhro ECU                              4F 3F 26 69 F3 E1 9D 01 │
│ 20 3C 3C BE    11 22 33 44       ☐ Key0 Block  Used       44 E2 FA D0 66 50 D1 2A │
│ PSW                              ☐ Key1 Block  Used       E0 B3 59 2E A1 DA 82 8F │
│ 02 56 76 88 CC 1D 8E 93         ☐ Key2 Block  Used       33 40 0E FB 85 06 51 6F │
│                                 ☐ Key3 Block  No Used     EA 35 0A 4F 14 24 3F 7E │
│ 1  Last used key                ☐ Key4 Block  No Used     31 B9 A3 E1 44 73 20 7E │
│ 0  Last but one used            ☐ Key5 Block  No Used     61 A9 AF 25 A8 AC A3 31 │
│                                 ☐ Key6 Block  No Used     ED EA A3 29 F0 38 A0 14 │
│                                 ☐ Key7 Block  No Used     3F 44 FC 3F 28 2A F8 41 │
│                                           Dealer key                              │
└──────────────────────────────────────────────────────────────────────────────┘
┌─Calc──────────────────────────────┐ ┌─Work──────────────────────────────────┐
│ ☐ Key 0    ☐ Key 4                │ │                                        │
│ ☐ Key 1    ☐ Key 5                │ │  Renew ECU    Sinhro ECU    Save EZS   │
│ ☐ Key 2    ☐ Key 6    ☐ All       │ │                                        │
│ ☐ Key 3    ☐ Key 7    ☐ New ESL   │ │  ESL Module   Key Calc     Generate    │
└───────────────────────────────────┘ └────────────────────────────────────────┘

Open dump MCU2 eeprom 256 byte D:\HC05forTest\1 x32.bin.
```

The objects of program control.

Open Dump EZS – loading of dumps of the EZS. The following BIN files are supported:
- eeprom (eeprom field of the microprocessor)
- ETL (a dump version for HC908, being read by ETL Programmer)
- Full (the whole memory field of the microprocessor)

You can make the choice in the dialog window of loading a file.

Open Dump EZS / Open Dump ESM – loading of dumps of steering lock of the ESM , it depends on the vehicle type.

Open Dump ECU – loading of dumps of the ECU to renew it, to synchronize it with the EZS and to test it. The actions assign by the corresponding button.

Open Dump Key – loading of key dumps that are mentioned in "eeprom" of the key to test authenticity with all the loaded dumps.

Help – the help in connection with a diagnostic slot or a unit to check it on the table.

Renew ECU – to make a new dump of the loaded unit, ECU, with the up link via STAR Diagnostic.

Synchro ECU – synchronization with EZS dump and the ECU assigns via the ID static bytes or HASH of keys, it depends on a type of the unit.

Save EZS – saving of the EZS dump after the changes made from the fields of the form.

ESL Module / ESM Module – a call of the operating window with ESL or the ESM selector, it depends on a type of the vehicle.

Key Calc – a call of the calculator window with key dumps is required to make a test of the key dump in order to check the damage of the information in the HASH units, the calculation of the key dump with the necessary data, the mentioned resource of response, the recovery of the damaged key dump, adjustment to the EZS dump according to the HASH mathematics (if it is an original key and there is a run beyond the maximum limits of HASH steps).

Generate – generation of new key dumps to calculate them. The key dumps, the changed EZS dumps, the dump of ESL or ESM and the dump of ECU save if they have been loaded and it is necessary to edit them. If the flag New ESL/New ESM has been set, the dump ESL or ESM will be fully calculated according to the EZS dump.

SSID* – the serial number of the set, identical number.

Syncro /Odo* – the bytes of synchronization with the lock and the motor control unit, or the doublet of odometer.

PSW* – the transport password of the key. The transport crypto-mask.

Key Block* – the sign of disabling the key.

Key Used – the sign of used keys.

The fields of key HASH contain the actual HASH for every key.

*The data of the field are interactive. The data changing in them leads to the changing in dumps.

Generation flags serve for the allowance of generation of the chosen key number and for setting a type of the dump to save it.

New ESL – the sign of necessity in generation the dump of locking the steering wheel or the selector AKPP according to the data of the lock.

The tabbed page for operation via the informational portal.
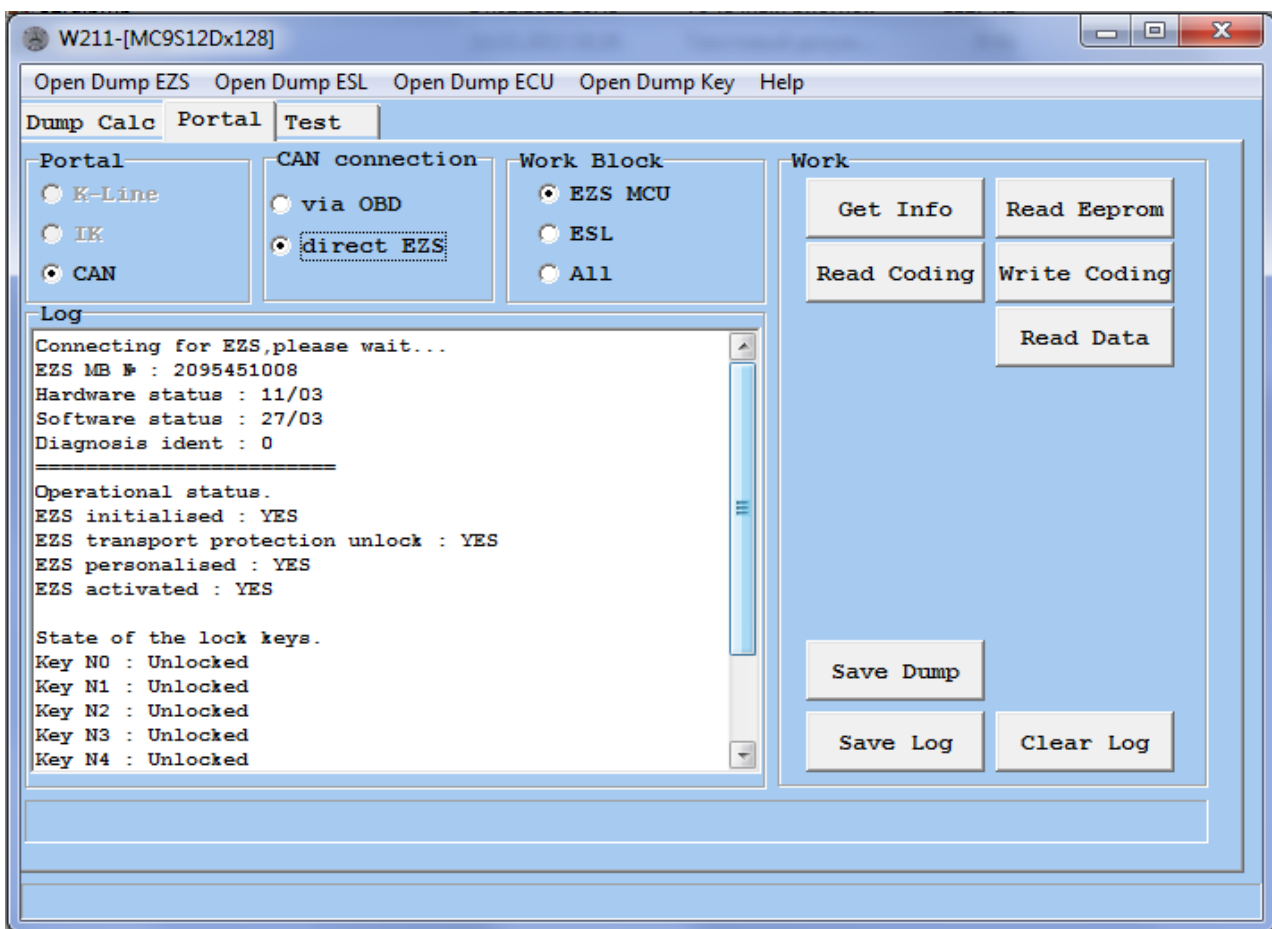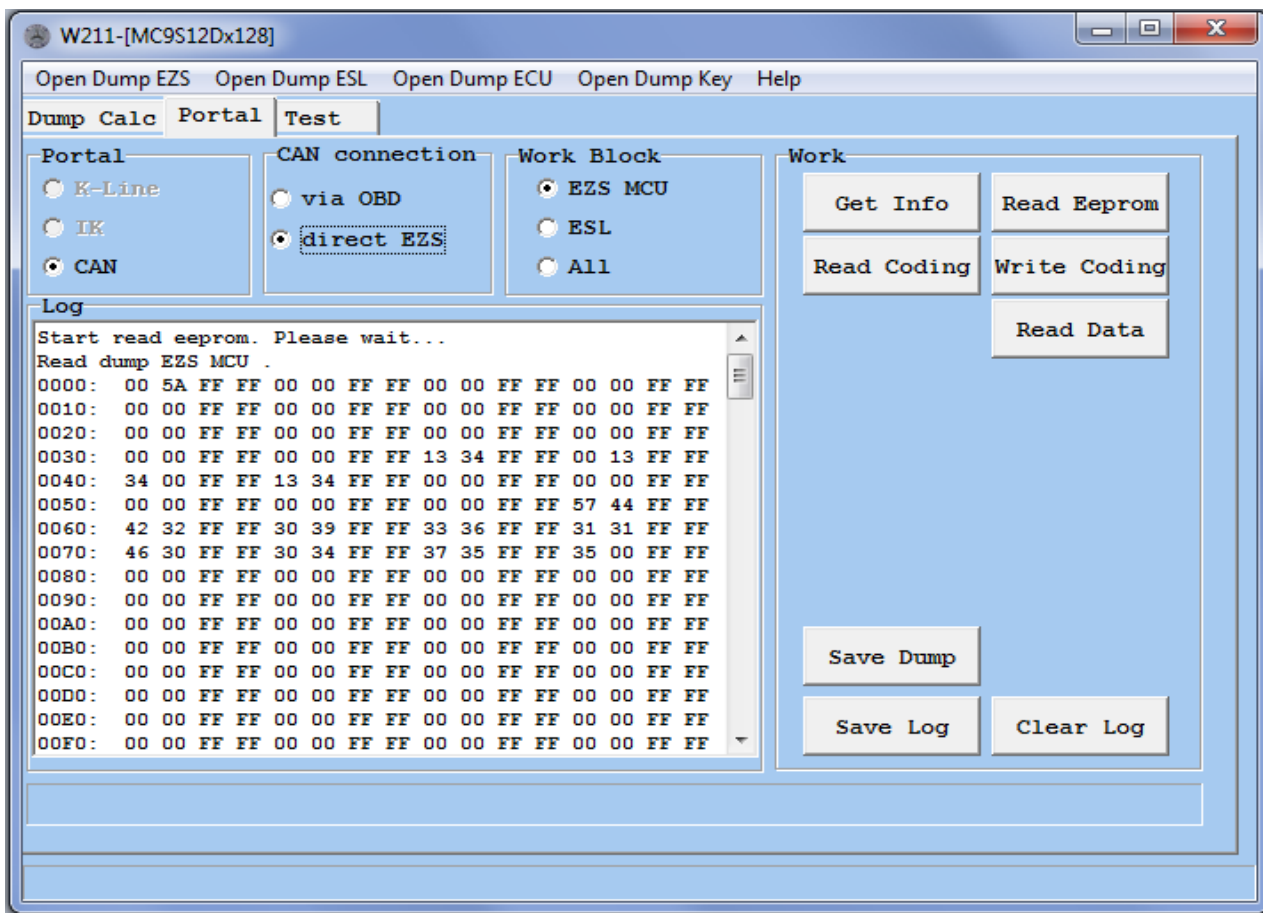
Portal – the choice of the informational portal via K-line, IR-report or CAN.

The choice of dump or unit for operating. If the reading of of the dump or the operation with the unit is unsupported by the chosen report, the flags of choice will be inaccessible.

Get Info – getting of the information from the unit (number, version hardware and software, the most important states and the other information).
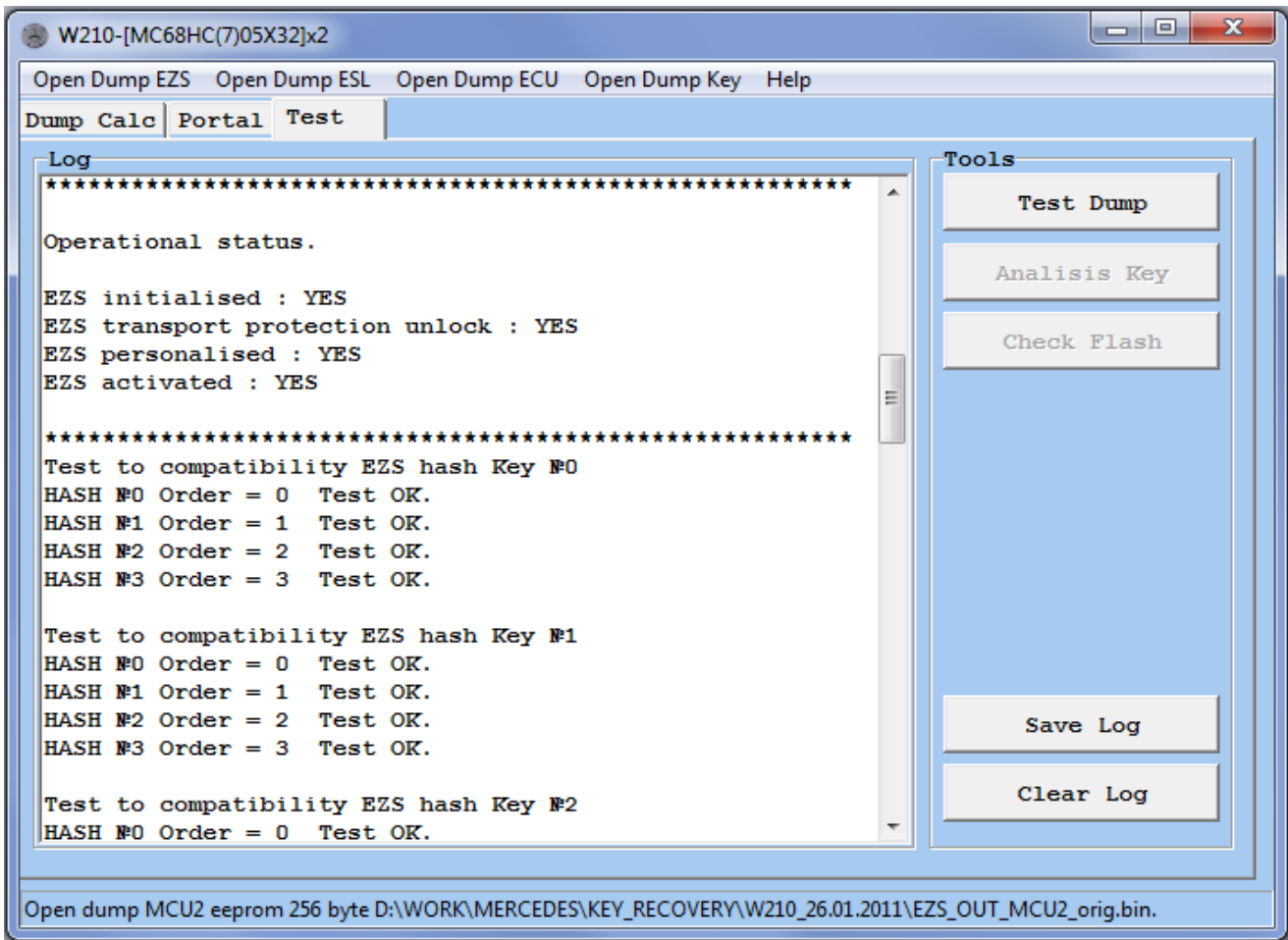
 Read Eeprom – the reading of of the chosen dump "eeprom" or the unit will be assigned via the chosen informational portal.

Save Eeprom – saving of the dump "eeprom" that was read off at that moment.

Save Log – saving the field of the log in the Word-document.

Clear Log – clearing the field of the log from a text.

The tabbed page of testing the loaded dumps.

Test Dump –launching of the process of testing the loaded dumps. There assign a test of the operational state of the EZS , the check sums of the key HASH, coherence of the key HASH. There defines compatibility with the loaded dumps of every key according to the HASH mathematics within the limits of the calculation steps.
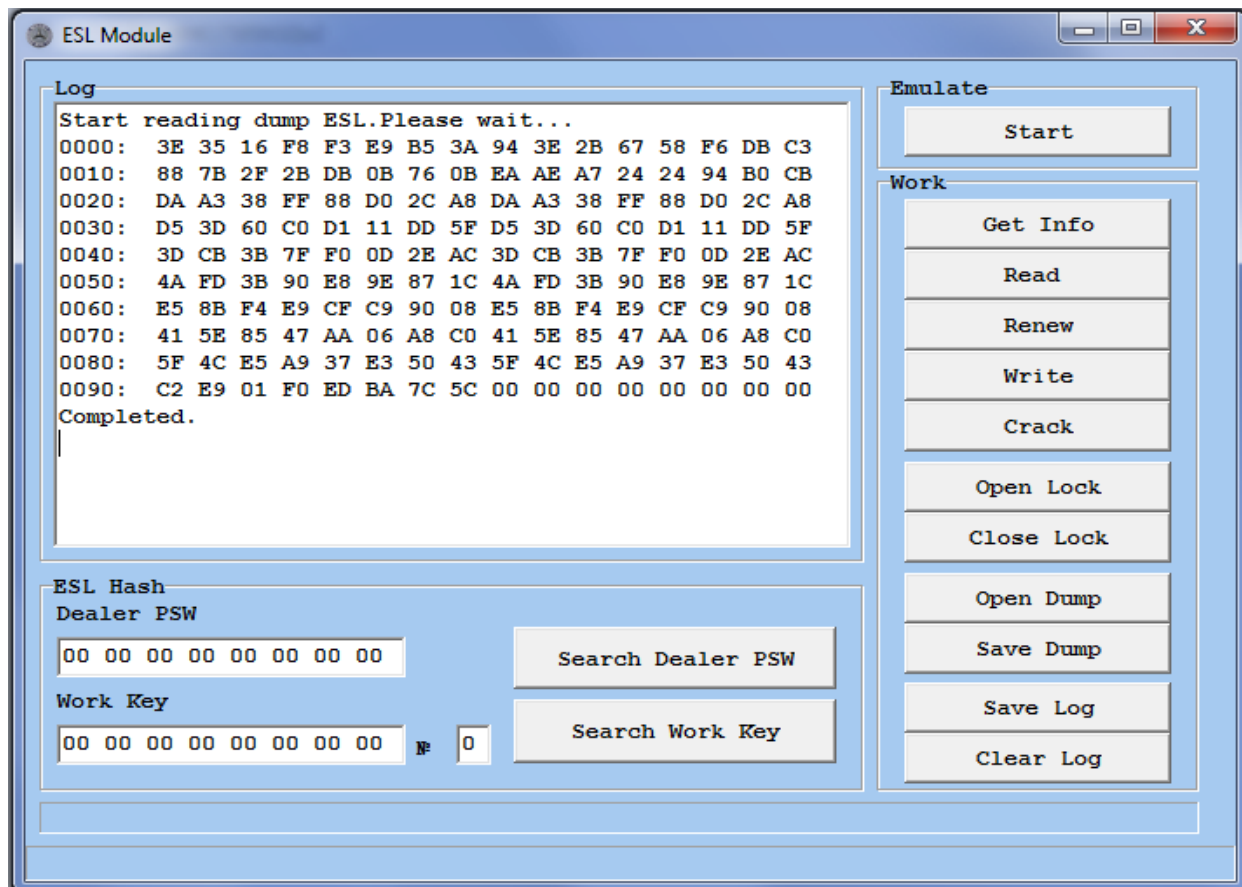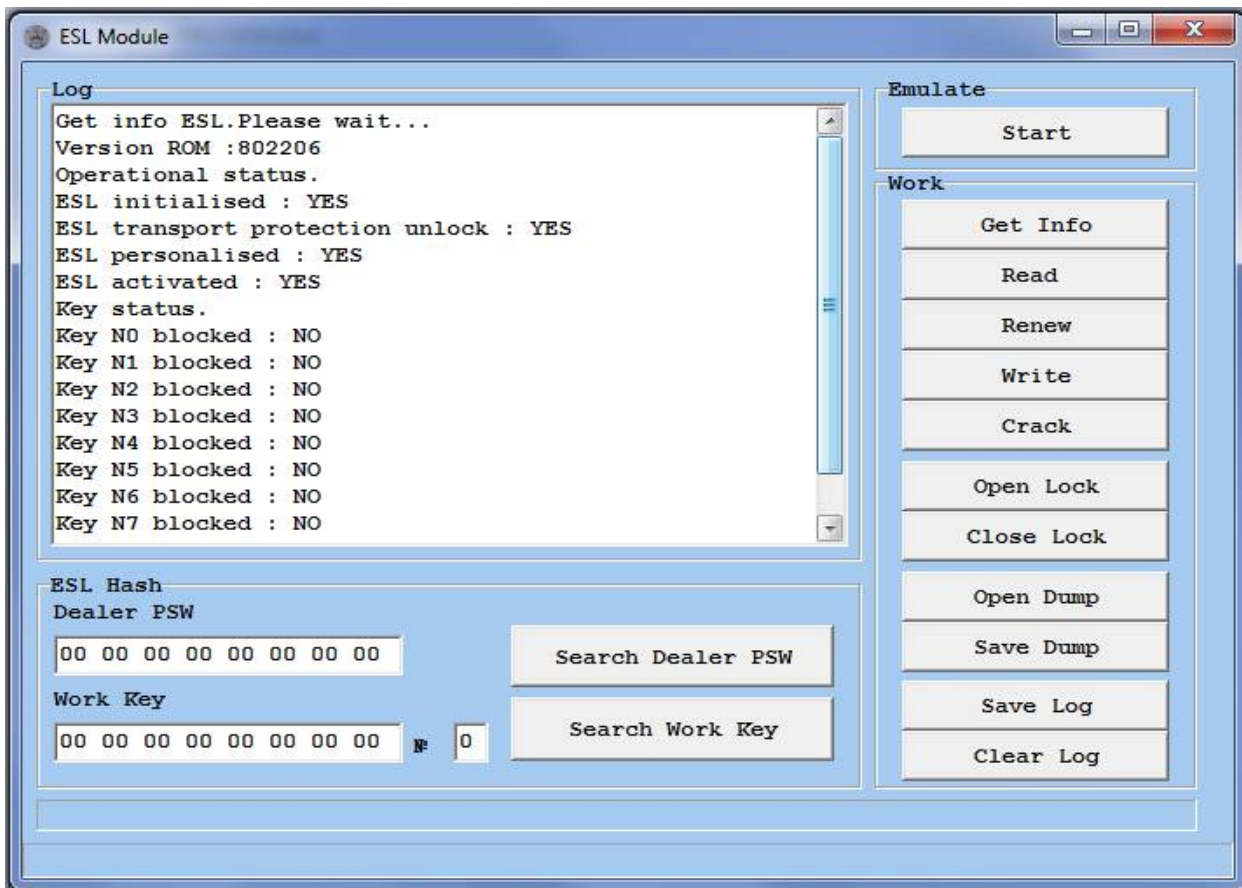
Analisis Key – the analysis of the loaded key dump and the display output of the short information about it.

*The red lines in the log of the test mean that it is an error or it is a lack of compatibility according to this step of checking.

Save Log – saving of the field of the log in the Word-document.

Clear Log – clearing of the field of the log from the text.

The module of operating with locking of the steering lock.

ESL Module

Log

```
Get info ESL.Please wait...
Version ROM :802206
Operational status.
ESL initialised : YES
ESL transport protection unlock : YES
ESL personalised : YES
ESL activated : YES
Key status.
Key N0 blocked : NO
Key N1 blocked : NO
Key N2 blocked : NO
Key N3 blocked : NO
Key N4 blocked : NO
Key N5 blocked : NO
Key N6 blocked : NO
Key N7 blocked : NO
```

ESL Hash

Dealer PSW

`00 00 00 00 00 00 00 00`   Search Dealer PSW

Work Key

`00 00 00 00 00 00 00 00` № `0`   Search Work Key

Emulate

Start

Work

Get Info
Read
Renew
Write
Crack
Open Lock
Close Lock
Open Dump
Save Dump
Save Log
Clear Log

ESL Module

Log

```
Start reading dump ESL.Please wait...
0000:   3E 35 16 F8 F3 E9 B5 3A 94 3E 2B 67 58 F6 DB C3
0010:   88 7B 2F 2B DB 0B 76 0B EA AE A7 24 24 94 B0 CB
0020:   DA A3 38 FF 88 D0 2C A8 DA A3 38 FF 88 D0 2C A8
0030:   D5 3D 60 C0 D1 11 DD 5F D5 3D 60 C0 D1 11 DD 5F
0040:   3D CB 3B 7F F0 0D 2E AC 3D CB 3B 7F F0 0D 2E AC
0050:   4A FD 3B 90 E8 9E 87 1C 4A FD 3B 90 E8 9E 87 1C
0060:   E5 8B F4 E9 CF C9 90 08 E5 8B F4 E9 CF C9 90 08
0070:   41 5E 85 47 AA 06 A8 C0 41 5E 85 47 AA 06 A8 C0
0080:   5F 4C E5 A9 37 E3 50 43 5F 4C E5 A9 37 E3 50 43
0090:   C2 E9 01 F0 ED BA 7C 5C 00 00 00 00 00 00 00 00
Completed.
```

ESL Hash

Dealer PSW

`00 00 00 00 00 00 00 00`   Search Dealer PSW

Work Key

`00 00 00 00 00 00 00 00` № `0`   Search Work Key

Emulate

Start

Work

Get Info
Read
Renew
Write
Crack
Open Lock
Close Lock
Open Dump
Save Dump
Save Log
Clear Log

Emulate – launching/stop of the emulation mode of the operating with ESL in order to check EZS.

Get Info – receiving of the information about the version and the state of ESL.

Read – reading ESL .

Renew – refreshment to make ESL new. **Dealer PSW** from the input field is used.
*If the password has not been found (there was 0 in the input field while launching of renew) or the password from the other ESL has been entered, the response on such a command may take a lot of time (till 4-5 minutes). Wait for the response.

Write – the recording of ESL via the loaded dump. The recording is possible if the only ESL is renewed.

Crack – cracking of EZL old type of the steering wheel (within two microprocessors HC05E6). The opening and the renewing of locking of the steering wheel happen while the procedure is launching (there is a lack in seeking the Dealer password).

Open Lock – opening of the locking via HASH of the operating key from the input field **Work Key** and a number from the input field **№.**

*If HASH has not been found (there was 0 in the input field while launching of this procedure) or the password from the other or earlier used ESL has been entered. The response on such a command may take a lot of time (till 4-5 minutes). Wait for the response.

Close Lock – closing of the locking via HASH of the operating key from the input field **Work Key** and a number from the input field **№.**

Search Dealer PSW – launching of the procedure of seeking the dealer password to the dump of the locking. It may take about a minute or even an hour. It depends on the power of your computer. The higher it is the clock rate of the processor,

the faster the password will be found. Being found once, the password to the proper dump can be used several times if it is necessary.

*Recommendation! If it takes more than 15-20 minutes to find the password, you should stop the search and launch it again in a few seconds (it is necessary for generation of the new original HASH for the search).
Save the log!

Search Work Key – launching of the search procedure of HASH of one operating key to open the locking (to remove it from the vehicle). It may take about a minute or even an hour. It depends on the power of your computer. The higher it is the clock rate of the processor, the faster HASH will be found.

*You can use the found operating HASH only once. All the HASH of the key will be changed in "eeprom" of the locking of the steering wheel.
*Recommendation! If it takes more than 15-20 minutes to find the password, you should stop the search and launch it again in a few seconds (it is necessary for generation of the new original HASH for the search).

Open Dump – opening of the dump "eeprom" for recording or searching of the password.

Save Dump – saving of the dump "eeprom" that has been read off.

Save Log – saving of the field of the log.

Clear Log – clearing of the field of the log from the text.

The module of operating with the key dump.
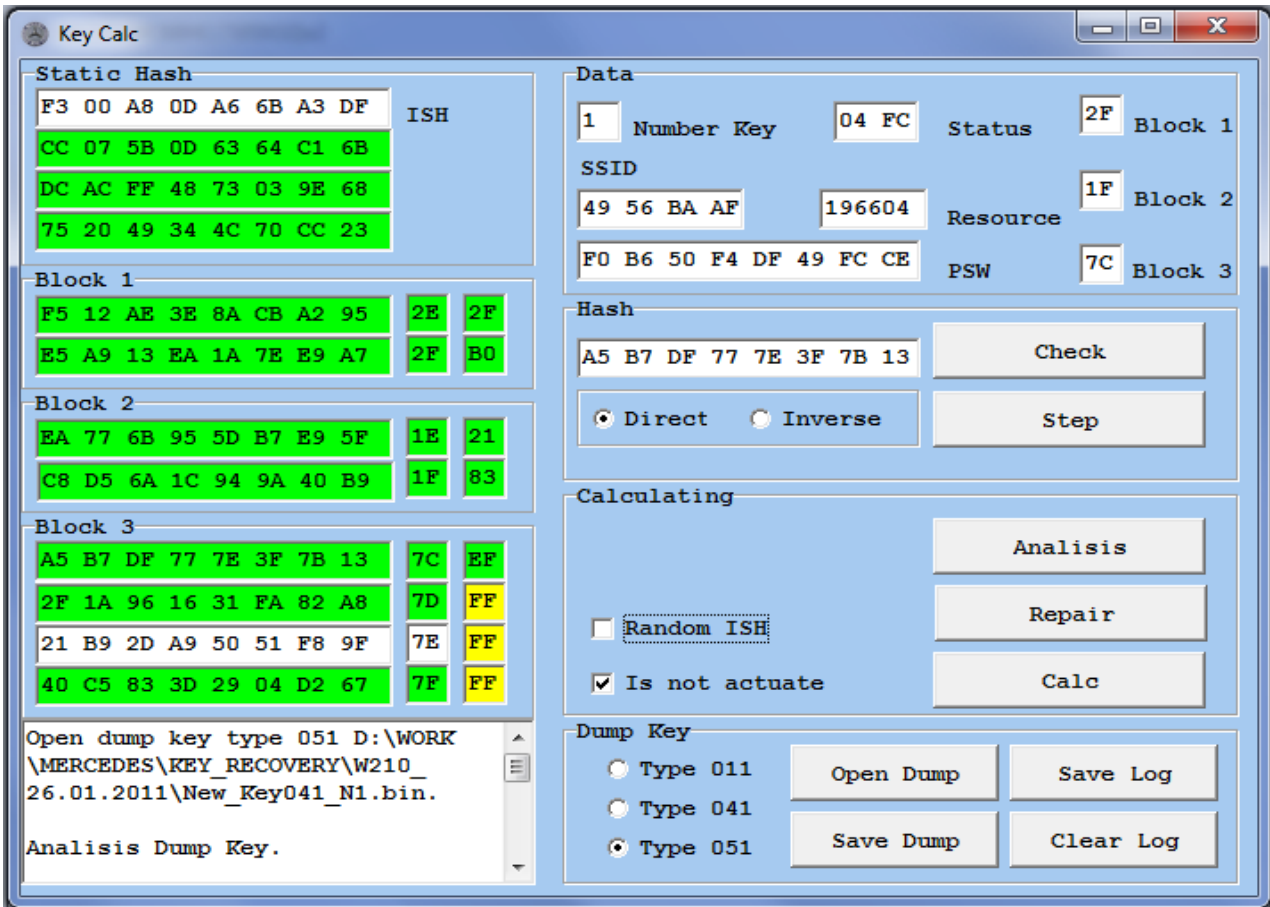
ISH* - the initial of the key dump. It is the main HASH, which provides the calculation of the remaining dumps.

The static HASH - the unit includes 3 HASH, which do not change during the operating process.

Block 1 – the first block of the key HASH.

Block 2 – the second block of the key HASH.

Block 3 – the third block of the key HASH.

Check – checking of compatibility with HASH from the input field and an initial. If they are compatible, there will be a current coherence of HASH in the log.

Step – a step of HASH (+1). Make this step according to the HASH mathematics.

Dump type – you can choose a type of the dump with a tick. You should load the file of one type and save it in the other type.
*Pay attention to the fact that types 041 and 051 cannot have the resource more than 196607 if you convert type 011.

Save Log – saving of the field of the log in the Word-document.

Clear Log – clearing of the field of the log from the text.

Number Key* – the number of the key (from 0 to 7).

SSID* – the serial number of the set. ID number.

PSW* – the transport password of the key. The transport crypto-mask.

Status – the state of the "eeprom" dump". If the field of the status is red, the mode is inactive or it is an error.
The custom operating modes: 14EC, 15 EB.
The new unused key: 04 FC, 05 FB.
The new key. The crypto-mode: 21 DF.
Inactive modes. The state of the "eeprom" error: 94 6C, 95 6B.

Resource* – resource of the key response.

*The interactive data is considered as the basis for calculation the key dump.

The counters of the HASH units – the current counters of all the three HASH units.

HASH – the field of HASH is used to check compatibility with the input HASH in the initial field or to count directly according to the HASH mathematics.

The type of counting –
- **Direct** – the direct counting of HASH;
- **Inverse –** the indirect type of counting HASH

Random ISH – the calculation of the key dump with a randomly generated initial. If there is no tick, the calculation assigns from the initial in the field **ISH**.

Is not actuate – the state of the dump is not authorized. There is a new key.

Analysis – the analysis of the key dump. The ways of coloring the HASH fields:
Green is normal. The analysis has been counted from the initial or the control point is right.
Red is an error. The analysis has not been counted from the initial or the control point is damaged.
Yellow is to check HASH. HASH has already been used.

Repair – recovering of the damaged key dump.
*You should make the following actions to recover the original key:
 - Read the EZS via K-line or Programmer and load the EZS dump and the not working key in the tabbed page "Dump Calc".
- Make a test in the tabbed page "Test" in order to assure that there is no compatibility with the lock and the key via HASH.
- Go to the module "Key Calc". The key dump will have already been opened in the calculator.
- Make an analysis ("Analysis") to check the state of the dump.
- Press the button "Repair". If there is HASH in the EZS(it is calculated according to the key number), a new dump will be calculated according to the HASH resource in the lock. This resource will be shown in the log or there will be a message that recovery is impossible.

Calc – the calculation of the key dump according to the data of the calculation fields.

Open Dump – loading of the key dump according to the chosen type.

Save Dump – saving of the key dump according to the chosen type.

The operating module with selector ESM.
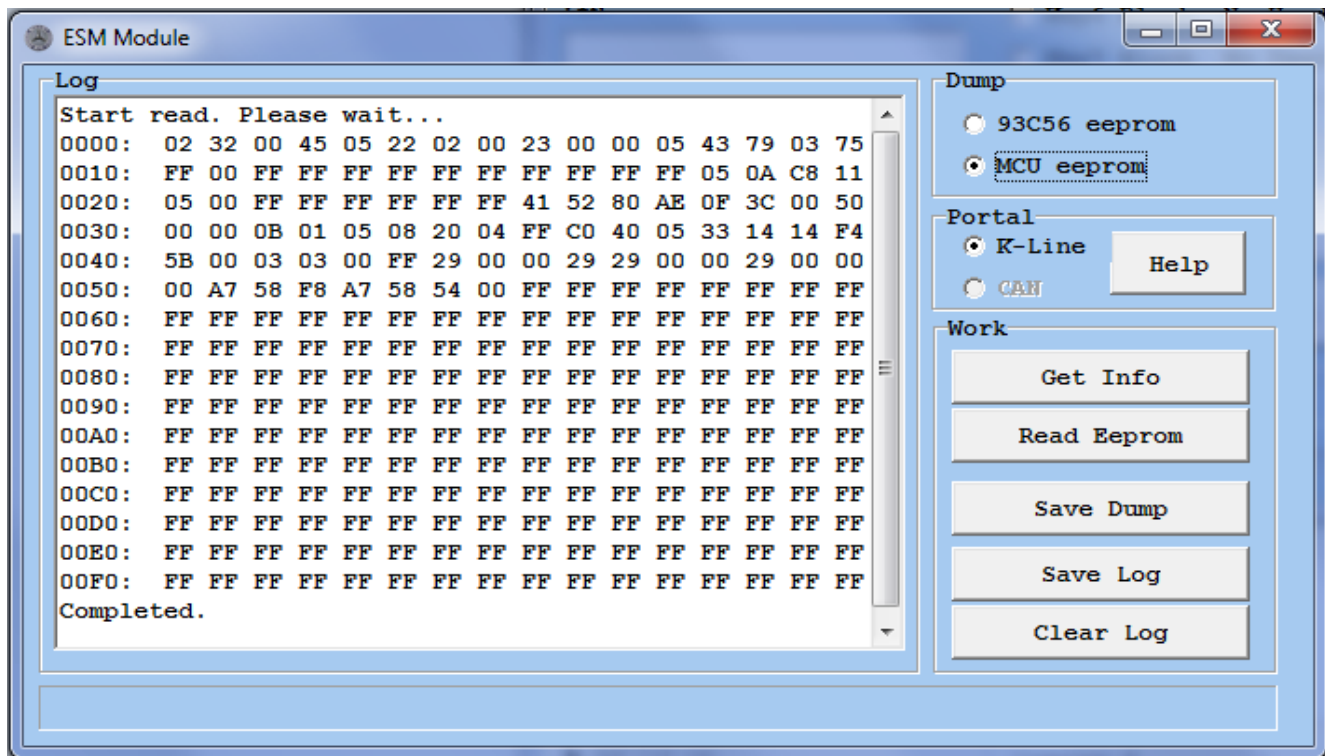
Dump – the choice of the micro type for reading. The "eeprom" of the microprocessor and the outward "eeprom" 93C56 with the key HASH are available.
Attention! Use this option to check correctness of reading 93C56 by Programmer. Some types of Programmers save the dumps in SWAP that have been read from the micro schemes (pairs of bytes are changed in their places).

Portal – the choice of the information portal to operate with the unit.

Get Info – getting information from the unit.

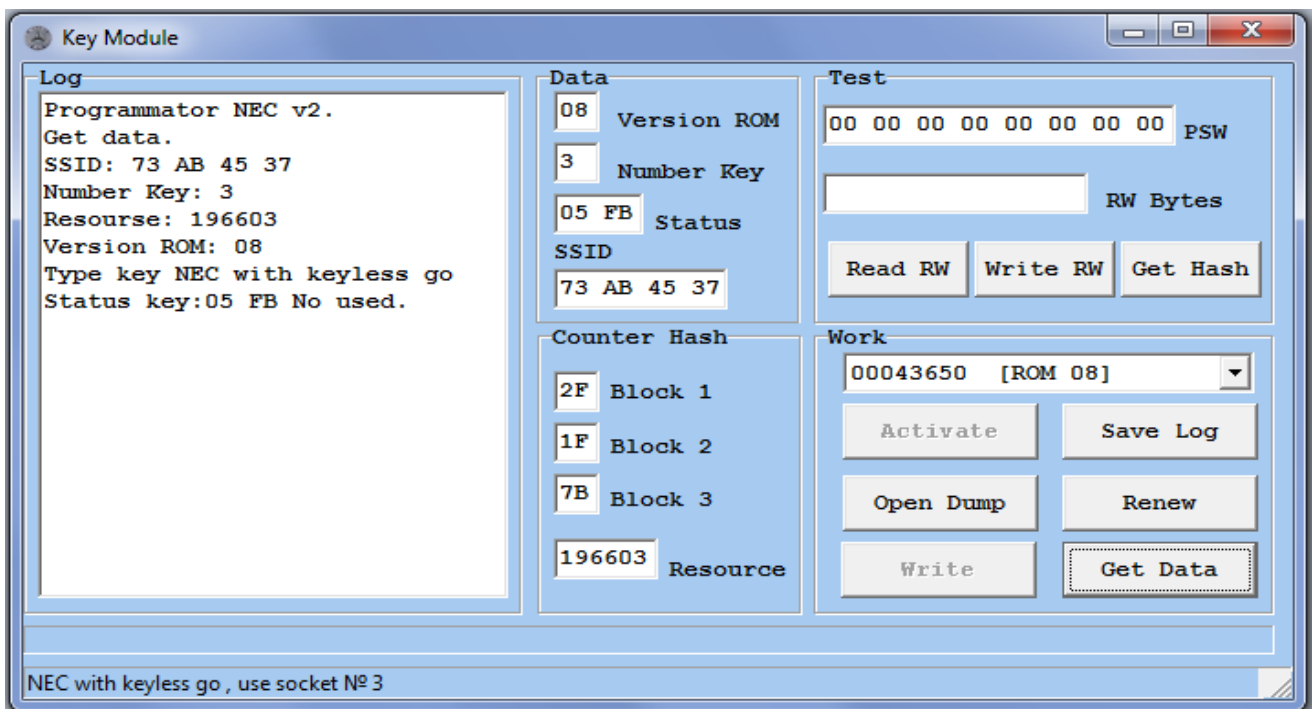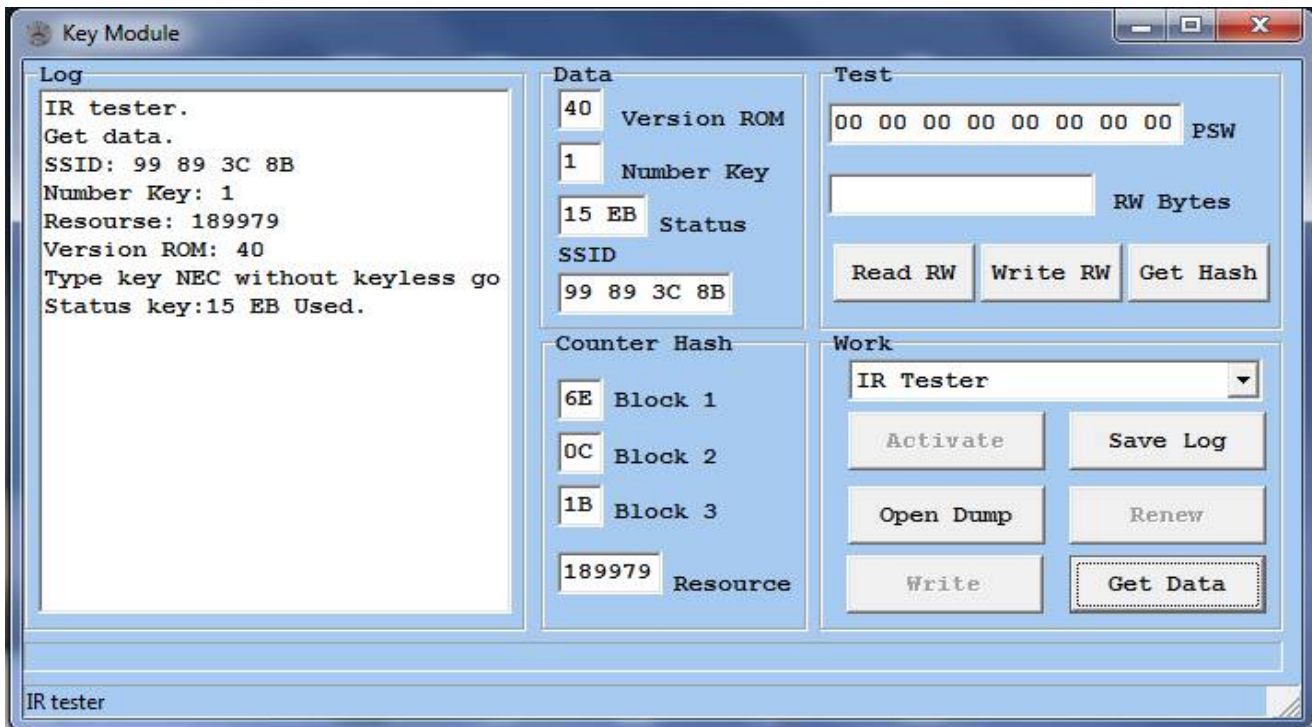**Read Eeprom** – reading off of the chosen dump "eeprom".

Save Dump – saving of the dump "eeprom" that has been read off.

Save Log – saving of the log in the Word-document.

Clear Log – clearing the log from the text.

Help – calling for the help information.

The operating module with a key or NEC programmer


```
Key Module

Log
IR tester.
Get data.
SSID: 99 89 3C 8B
Number Key: 1
Resourse: 189979
Version ROM: 40
Type key NEC without keyless go
Status key:15 EB Used.

Data
40     Version ROM
1      Number Key
15 EB  Status
SSID
99 89 3C 8B

Counter Hash
6E  Block 1
0C  Block 2
1B  Block 3
189979  Resource

Test
00 00 00 00 00 00 00 00  PSW
_____  RW Bytes
Read RW   Write RW   Get Hash

Work
IR Tester
Activate      Save Log
Open Dump     Renew
Write         Get Data

IR tester
```



```
Key Module

Log
Programmator NEC v2.
Get data.
SSID: 73 AB 45 37
Number Key: 3
Resourse: 196603
Version ROM: 08
Type key NEC with keyless go
Status key:05 FB No used.

Data
08     Version ROM
3      Number Key
05 FB  Status
SSID
73 AB 45 37

Counter Hash
2F  Block 1
1F  Block 2
7B  Block 3
196603  Resource

Test
00 00 00 00 00 00 00 00  PSW
_____  RW Bytes
Read RW   Write RW   Get Hash

Work
00043650   [ROM 08]
Activate      Save Log
Open Dump     Renew
Write         Get Data

NEC with keyless go , use socket № 3
```

The choice of the operating module:

   IR Tester -operating with the key via IR-channel. The module of expansion is IR Tester.
   xxxxxx [ROM xx] - operating with the NEC microprocessor from the key on the card of NEC Programmer.

Get Data – the beginning of work, getting data of the key, the first test of the state and the correctness of work. Possible responses:
- **Get data.** The primary set with the serial number and the counters of the HASH units are received.
- **Key busy calculation.** The microprocessor of the key is busy with the calculation of HASH. Repeat the attempt of getting data. If the situation does not change during several attempts, "eeprom" of the key is possibly damaged, the removing and the new recording is required.
- **No response to a service command.** It means that the key did not respond to the calling of the state and the version of the program. The key must be damaged or the key could not receive the IR command from the device.
- **Service status. Perhaps reading data and activation.** It means the service state of the key, when the reading of the data is available. Read the additional document about the operating with the keys in the state 0C F4.

Renew – refreshing of the key is available only on the board of NEC Programmer.

Attention! Programmer controls the state of the expansion bytes of the radio-transmitting in the microprocessor NEC during the process of renewing. If the bytes were damaged earlier of during the process of renewing, Programmer will continue the process until the time when the state of bytes becomes normal. It may take some time, be patient. The renewed micro-controller will definitely transmit radio-command after recording.

Open Dump – loading the key dump "eeprom" for recording. The key files of the 041 and 051 types are available.

Write – recording "eeprom" of the removed key via the loaded dump.

Save Log – saving of the log in the Word-document.

Read RW – reading of 6 bytes of the available data from the key "eeprom".

Write RW – recording of 6 bytes of the available data in the key "eeprom".

Attention! The first two bytes RW for NEC have the particular number, being made in the factory, and it is

Get HASH – getting of the current key HASH. Decoding of the response of the key can be assigned by the key password from the field PSW. The decoded HASH will be right if only the transport password corresponds with the key. This function is quite comfortable as it allows recovering the work of the key without rewriting with the HASH run with the lock. You can take the password from the EZS dump, HASH (that has been got and decoded) should be written in the dump and the remaining units. The resource of the key reduces by 2.

Version ROM – the version of the key program. You can learn about the supported versions in the additional document.

Number Key – the number of the key (from 0 to 7).

Status – the state of the dump "eeprom".
   Normal operating modes: 14 EC, 15 EB.
   A new unused key: 04 FC, 05 FB.
   A new key. The crypto-mode: 21 DF.
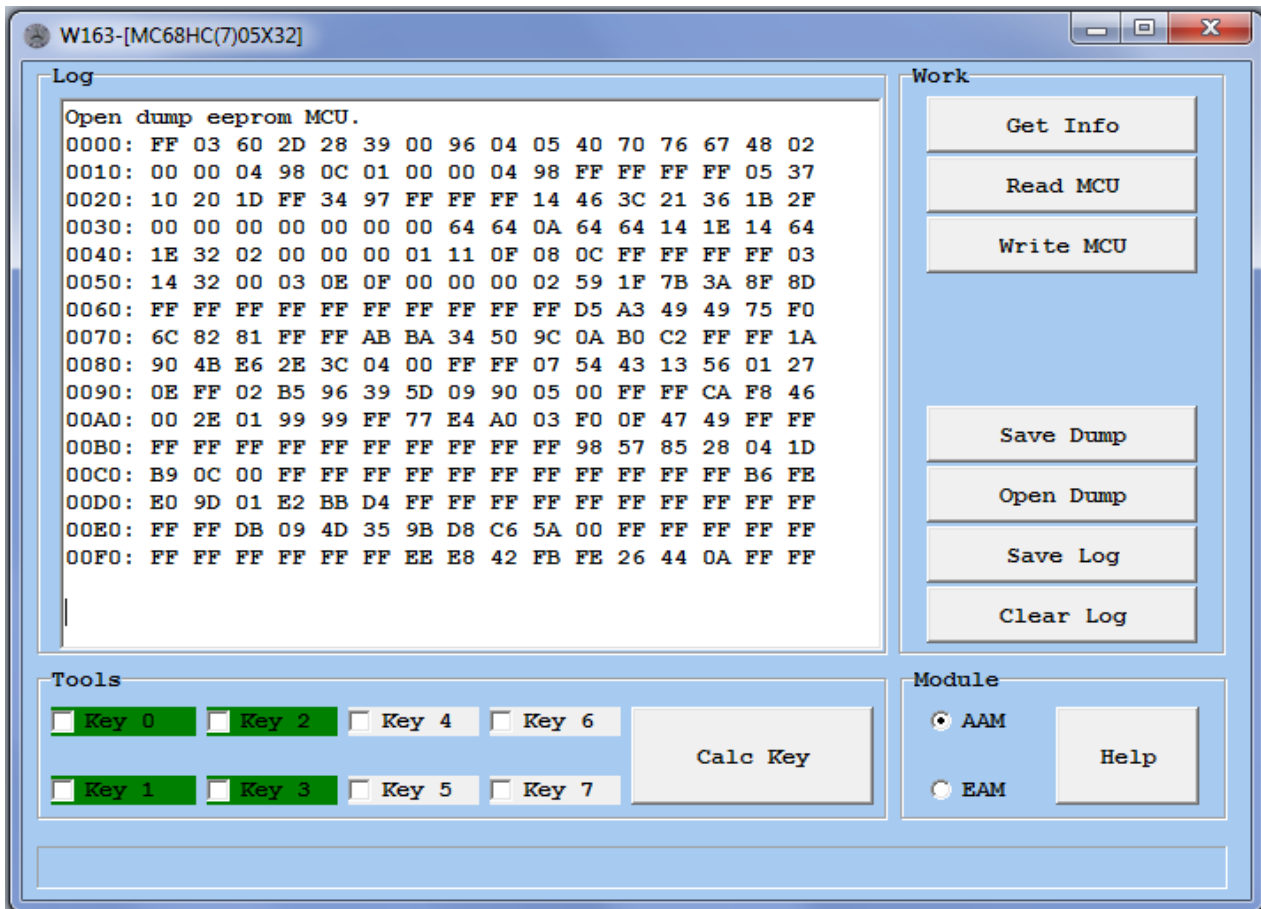   A new key. The service state: 0C F4.
   Bad modes. The state of the error "eeprom": 94 6C, 95 6B.

SSID – the serial number of the set. ID-number.

PSW – the transport password of the key. The transport crypto-mask.

Resource – the resource of responding the key.

Get Info – getting info about the unit.

Read MCU – reading off of the "eeprom" microprocessor of the chosen unit.

Write MCU – recording of the "eeprom" microprocessor of the chosen unit.

Read 93C56 – reading off of the outward "eeprom" of the unit DAS/EAM.

Write 93C56 – recording of the outward "eeprom" of the unit DAS/EAM.

Save Dump – saving of the dump that was read at that moment.

Open Dump – opening of the dump for calculation and recording.

Save Log – saving of the log in the Word-document.

Clear Log – clearing of the log field.

Keys for calculation – the key number that have been used are highlighted green.

Calc Key – the calculation of the chosen key numbers according to the dump.

*Attention! The calculation of keys for the EAM unit is possible if only it is done according to the dump of the microprocessor. The 93C56 calculation will not be valid during the loading of the dump of the outward "eeprom".

Module – the choice of the unit for operating. AAM/EAM (DAS).

Help – the help information by connection.