Option "List Key".

This option allows you to retrieve data for calculating key password on the server.

To do this you must do the following.

I will show this by the example EZS 221 old with keys keyless 08 ROM version.

Insert a valid key into the ignition lock (EZS) four consecutive times with intervals of 5-10 seconds.

Remove the key and reads EZS via CAN or IR. Save the dump.

Select a car.



Read EZS data

mp ECU Open Dump Key	Export Import Help			
Test				
CAN connection	Work Block	Work		
C via OBD	• EZS MCU	Get Info	Read Eeprom	
arrect 525		Read Coding	Write Coding	
please wait		Renew	Read Data	
))12350 Waltons 1y. 108 06/37	Unlock Key	EZS Write		
06/37	Check/Read PSW			
YES	-			
YES	5			
s				
keys.		Save Dump	Calc Dealer PSW	
			-	
	+	Save Log	Clear Log	
	mp ECU Open Dump Key Test CAN connection Via OBD C direct EZS ,please wait 19. 108 06/37 06/37 YES action unlock : YE: YES s keys.	mp ECU Open Dump Key Export Import Help Test CAN connection • via OBD • direct EZS work Block • EZS MCU • EZS MCU	mp ECU Open Dump Key Export Import Help Test CAN connection O via OBD O direct EZS Mork Get Info Read Coding Renew Unlock Key Ob/37 D6/37 VES action unlock : YES YES s keys. Save Dump	

Save EZS data

camp c	are							-	202			05017	21 22		20						
Porta	1				CA	NC	con	nec	tio	on	I PN	lor	k B	100	:k			Work			
C H-L C IR	ane				0	via	1 01	BD	75			•	EZ:	S M	CU			Get Info	Read Eeprom		
• CAN	I					un			20									Read Coding	Write Coding		
Log Start	read	lee	pro	om.	Ple	ease	e w	ait								_		Renew	Read Data		
Read d	ump	EZS	5 MC	U																	
0000:	A 8	95	49	B7	00	OF	3F	10	00	00	00	00	00	00	00	00	-	Unlock Kev	EZS Write		
0010:	81	79	31	6B	FA	35	4A	E6	00	00	00	00	00	00	00	00	-	-			
0020:	66	79	AC	29	65	35	SA	89	00	00	00	00	00	00	00	00					
0030:	22	AE	07	A2	20	U1	18	08	00	00	00	00	00	00	00	00		Check/Read PS	4		
0040.	C0	19	59	58	12	70	43	95	00	00	00	00	00	00	00	00		-			
0060-	CS	CE	13	07	411	08	D4	חח	00	00	00	00	00	00	00	00					
0070:	AC	CE	1E	29	DB	9B	80	FB	00	00	00	00	00	00	00	00					
0080:	53	OC	71	OF	64	BE	C3	99	00	00	00	00	00	00	00	00					
0090:	73	AA	EO	19	13	BE	CC	72	00	00	00	00	00	00	00	00		2			
00A0:	F7	D9	D4	OA	F1	00	A4	87	00	00	00	00	00	00	00	00			1		
00B0:	F6	BS	D4	6E	06	AB	4D	BC	00	00	00	00	00	00	00	00		Save Dump	Calc Dealer		
0000:	82	C8	07	01	AO	ED	90	51	00	00	00	00	00	00	00	00		Sars Dump	PSW		
0000:	CO	D9	59	5B	12	7C	43	95	00	00	00	00	00	00	00	00			1		
00E0:	C8	CE	13	07	4D	08	D4	DD	00	00	00	00	00	00	00	00		Save Log	Clear Log		
DOFO:	AC	CE	1E	29	DB	9B	80	FB	00	00	00	00	00	00	00	00	120	-			

The program will show the last used key and its hash.

pen Dump EZS Open Dump ECU Open Dump Key E	cport Import Help					
ump Calc Portal Test						
ZZS Data SSID Odo Ke SSW C0 00 00 00 00 00 00 Construction Constret <t< th=""><th>eyû Block Used eyî Block Used eyî Block No Used</th><th>89 8A 35 6. ED 9C 71 90 51 9C ED A 95 43 7C 12 DD D4 08 41 FB 8C 9B D1 99 C3 BE 6.</th><th>5 C9 AC 79 66 C 87 6F 54 2D D 01 07 C8 82 2 5B 59 D9 C0 D 07 13 CE C8 B 29 1E CE AC 4 0F 71 0C 53</th></t<>	eyû Block Used eyî Block Used eyî Block No Used	89 8A 35 6. ED 9C 71 90 51 9C ED A 95 43 7C 12 DD D4 08 41 FB 8C 9B D1 99 C3 BE 6.	5 C9 AC 79 66 C 87 6F 54 2D D 01 07 C8 82 2 5B 59 D9 C0 D 07 13 CE C8 B 29 1E CE AC 4 0F 71 0C 53			
WDD2211861A219871	y7 Block No Used Dealer key	72 CC BE 13 E6 4A 35 FA	3 19 EO AA 73 A 6B 31 79 81			
Calc	Work					
Key 0 Key 4 On-Line Key 1 Key 5 Key 2 All	Renew ECU	Sinhro ECU	Save EZS			
Key 2 Key 6	ISM/7G Module	Key Calc	Generate			

Close the window with EZS and go to Key Module. IR-tester must be attached to the Base module. Test the key that was inserted last in the EZS.

овая папка							
A		-					
Імя	Дата изменения	Тип Размер					
🖟 datal	13.11.2014 10:11	Папка с файлами					
Data recovery of the flash MCU HC908 EZS.pdf	12.04.2013 14:03	Foxit Reader PDF 43 KB					
Description.pdf	07.09.2013 9:28	Foxit Reader PDF 926 K5					
Key Module	40.44.0044.46.00						
)ata	Test					
IR tester. Get data. SSID: A8 95 49 B7 Number Key: 0 Resourse: 185115 Version ROM: 08 Type key NEC with keyless go Status key:14 EC Used.	08 Version ROM Number Key 14 EC Status SSID A8 95 49 B7 Counter Hash 2D Block 1 06 Block 2 18 Block 3 185115 Resource	D0 00 00 00 00 00 00 00 pSW RW Bytes Read RW Get Hash Write RW Get PSW List Work 2 IR Tester Activate Save Log Open Dump Renew 1					
ester	185115 Resource	Write Get Data					

Be careful, not to confuse the key. This will determine the success of the process !!!

If the key is properly tested, press the «List» button. The program prompts you to select from two variants. Fast list saves time and resource key, but does not guarantee the success of the password finding.

Slow list is preferred, but it is not always possible to get a result from the first time. It may be necessary to repeat the data collection. After selecting the program will make connection to the server on-line and do key calculating. Click to the "Close" button when it prompts.



Next, the program will start preparation process for data collection. This process takes about 1-2 minutes.



After preparation stage program automatically proceed to the data collection process of the key. Current status can be observed in status bar at the bottom of the window. It displays the completion percentage or message about key waiting. There are can be long waiting period when the key is in a state of hash math calculation, and does not respond on IR. Be patient and wait for the completion of the process. Depending on the chosen option and key ROM version this time may vary from 15 minutes to several hours.

овая папка						
1мя	Дата изменения	Тип	Размер			
🔓 datal	13.11.2014 10:11	Папка с файлами				
A89549B7.lst	15,08.2015 0:43	List file	3 КБ			
Data recovery of the flash MCU HC908 EZS.pdf	12.04.2013 14:03	Foxit Reader PDF	43 KB			
	an ao sata a an					
	Data	Waat				
IR tester.			0 00 00			
Get data.	Version ROM					
SSID: A8 95 49 B7	0 Number Key		RW Bytes			
Number Key: U Resourse: 185115	14 EC Status	Read RV Get Ha	sh Led ON			
Version ROM: 08	SSID					
Type key NEC with keyless go	A8 95 49 B7	Write RW Get P	SW Stop			
Preparation.	Counter Hash	Work				
Start creating of the list.		TR Tester				
Please wait	2D Block 1					
	06 Block 2	Activate	Save Log			
	10					
	Block 3	Open Dump	Renew			
	185115 Resource	Write	Get Data			
	, nobour ou		000 0404			

In operation, the program will create a list file in own directory (default is "C:\Program Files\Key Less Prog). This file necessary to send via e-mail to calculate the key password.

Either program will connect to the server to automatically calculate using a password token (this feature in development).



If there was a failure while operation or program hangs don't worry.

It is necessary to insert the key in the EZS again and wait about 10 seconds before remove.

Repeat it four times for the reliable synchronization of the key with $\ensuremath{\mathsf{EZS}}$.

Repeat all steps from "Read EZS data" stage. The program will continue to fill the list file with the same place and name. Wait until the process is complete.

and the state	Terrar data	-	- 0 X				
ata	Test						
08 Version ROM	00 00 00 0	0 00 00 0	0 00 PSW				
0 Number For	-		DW Buton				
Number Key	1	and sources	RW Dytes				
14 EC Status	Read RW	Get Hash	Led ON				
A8 95 49 B7	Write RW	Get PSW	List				
10 33 43 57		ace con					
ounter Hash	Work						
C Block 1	IR Tester		<u> </u>				
Block 2	Activat	e S	Save Log				
Block 3	Open Du	up	Renew				
181100	Musika		at Data				
Resource	write		et Data				
				21			
Ara use Data 08 Versio 0 Number 14 EC Stat SSID A8 95 49 E Counter Has 100r, 48 Minute, 06 Block 181100 Re	18 Version ROM Number Key 14 EC SID 18 95 19 10 10 11 16 11 16 11 16 11 16 11 16 11 16 11 16 11 10 11 11 12 12 13 14 14 15 16 16 17 18 19 10 10 11 12 14 15 16 16 17 18 19 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10	28 Version ROM 00 00 00 00 2 Number Key 14 EC Status SID Write RW 48 95 49 48 95 49 48 95 49 48 95 49 48 95 49 48 95 49 48 95 49 48 95 49 48 95 49 48 95 49 48 95 49 48 95 49 48 95 49 48 95 49 48 95 49 48 95 49 48 95 49 44 40 40 45 81 40 46 81 40 47 40 40 48 40 40 48 40 40 48 40 40 48 40 40 49 40 40 40 81 40 40 81 40 40	28 Version ROM 00 00 00 00 00 00 00 2 Number Key 14 EC 15 Block 1 16 Block 2 16 Block 3 100 Resource 1100 Resource	18 Version ROM 00 00 00 00 00 00 00 00 PSW 1 Number Key RW Bytes 14 EC Status Read RW Cet Hash Led ON 14 EC Status Write RW Get PSW 15 Work IR Tester 16 Block 2 Open Dump 100 Resource Write	18 Version ROM 00 00 00 00 00 00 00 00 PSW 14 EC Status RW Bytes 14 EC Status Read RW Get Hash Led ON 14 EC Status Write RW Get PSW 15 Write RW Get PSW List 16 Block 1 Activate 16 Block 2 Open Dump 1100 Resource Write	18 Version ROM 00 00 00 00 00 00 00 00 00 00 PSW 14 EC Status Read RW Get Hash 14 EC Status Read RW Get PSW 14 EC Status Write RW Get PSW 15 IR Tester IR 16 Block 2 Open Dump Renew 181100 Resource Write Get Data	18 Version ROM 00 00 00 00 00 00 00 00 00 PSW 14 EC Status Read RW Get Hash Led ON 14 EC Status Write RW Get PSW 14 EC Status Write RW Get PSW 15 Block 1 Activate 16 Block 2 Open Dump 1100 Resource Write

If there are two keys, it is desirable to select a key with more resources.

We are constantly working to improve the program and calculating service, and soon the effectiveness of finding passwords will be much higher.

Will be sufficient it to 1-2 fast lists for a guaranteed result.

ATTENTION !!!

The process to receive a password may be used only on vehicles with EZS on NEC. If EZS CPU is Motorola possible "the key out of sync with EZS" situation, and as a consequence the loss of key functionality.

Getting a password is possible only from fully operational and not blocked key, which operating with EZS (synchronized).

Mehaco

15.08.2015