VOLVO Immobilizer Manual

(Created Date: 20220415, the content is subject to change with software updates)

1. Introduction to VOLVO Immobilizer

You can add semi-intelligent or intelligent keys and lose all of them. You can replace CEM and KVM modules for some models

At present, Volvo mainly has three kinds of systems: knob with or without gear, semi-intelligent and intelligent key. The anti-theft difference between semi-intelligent and intelligent key is that the intelligent key system has a KVM module system to participate in anti-theft matching. At present, most Volvo models need to open and read the CEM/KVM module to read anti-theft data to obtain the password

2. Toothless knob anti-theft system

2.1Model Coverage：

Brand	Model	Year	Key type
VOLVO	C30	2007-2013	Toothless Knob Key
VOLVO	C70	2007-2013	Toothless Knob Key
VOLVO	S40	2004-2012	Toothless Knob Key
VOLVO	V50	2006-2012	Toothless Knob Key

2.2 Requirements

1.Launch IMMO PRO/IMMO PAD (professional version).

2. The toothless knob key used for anti-theft matching is divided into 16-digit and 24-digit remote control data. Before purchasing the key, please confirm whether the key used by the current vehicle is a 16-digit remote control data key or a 24-digit one. Please refer to Step 4 of anti-theft operation.

2.3 Procedure

The operation process demonstration takes Volvo S40 2008 toothless knob key as an example

Vehicle series entry

Select [Volvo] -> [Anti-theft Key Matching] -> [S40] -> [2004-2012] -> [Toothless Knob Key] (See Figure 1, Figure 2, Figure 3, Figure 4, Figure 5, Figure 6 for the process steps)

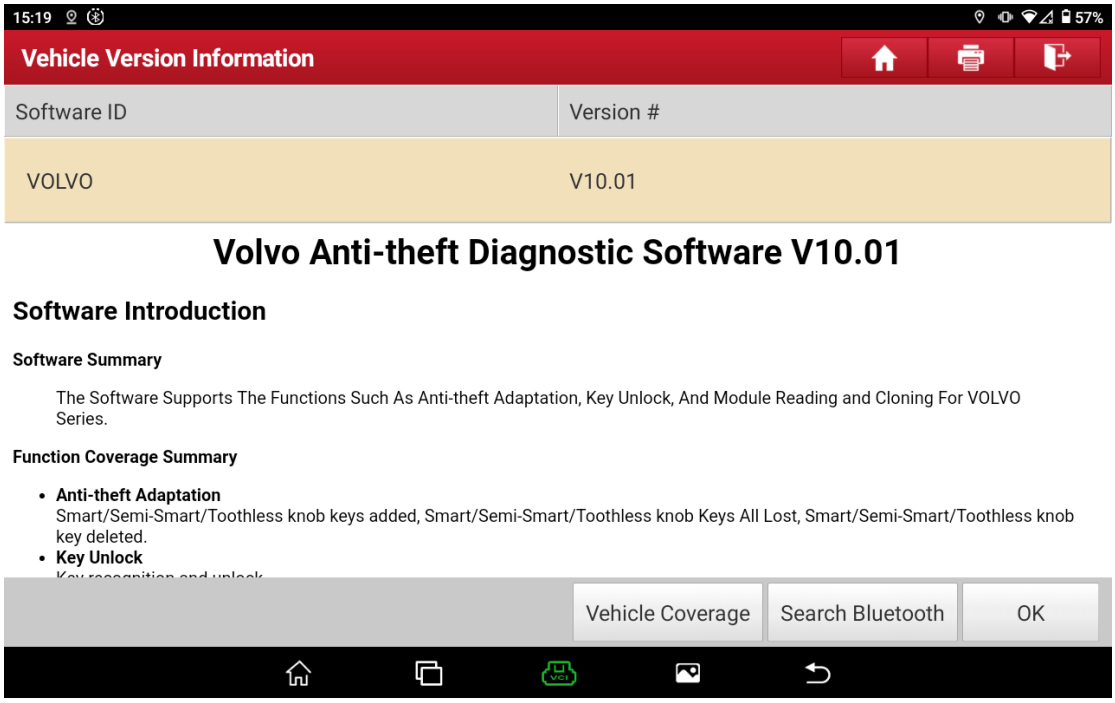


Figure 1

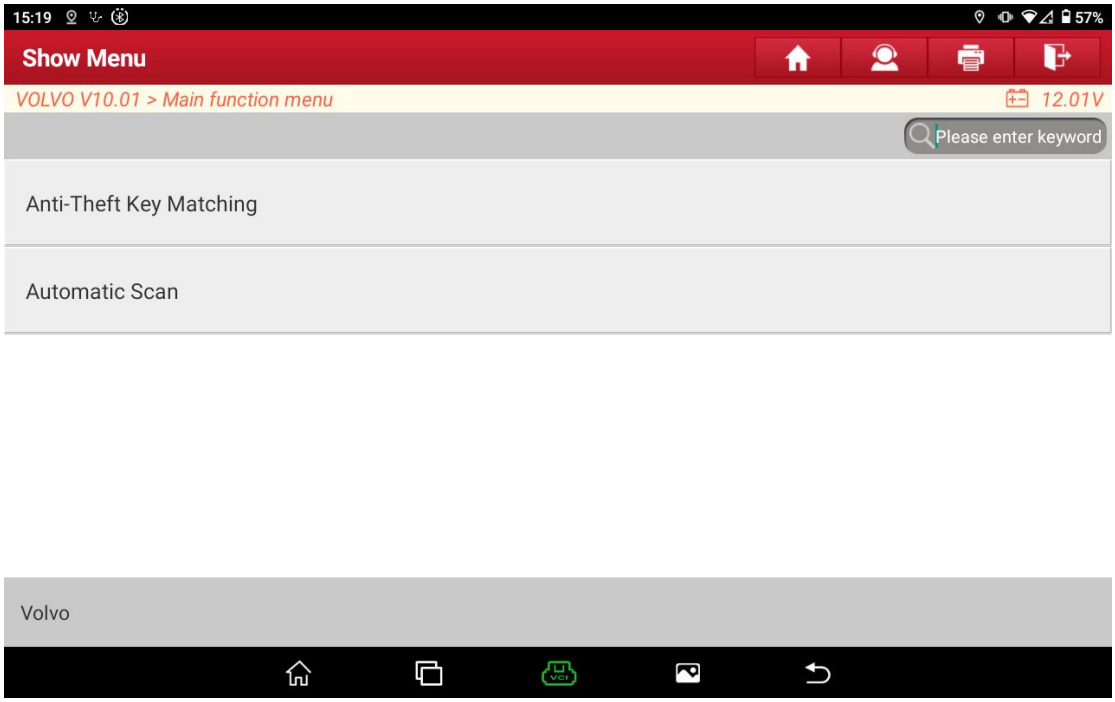


Figure 2

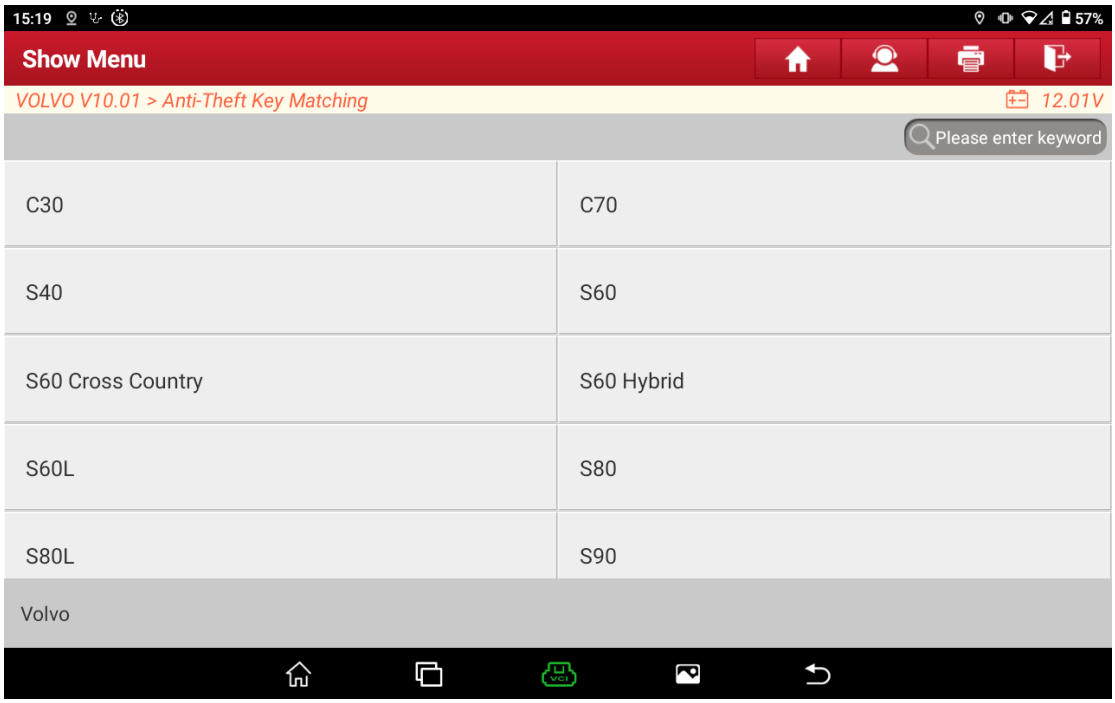


Figure 3

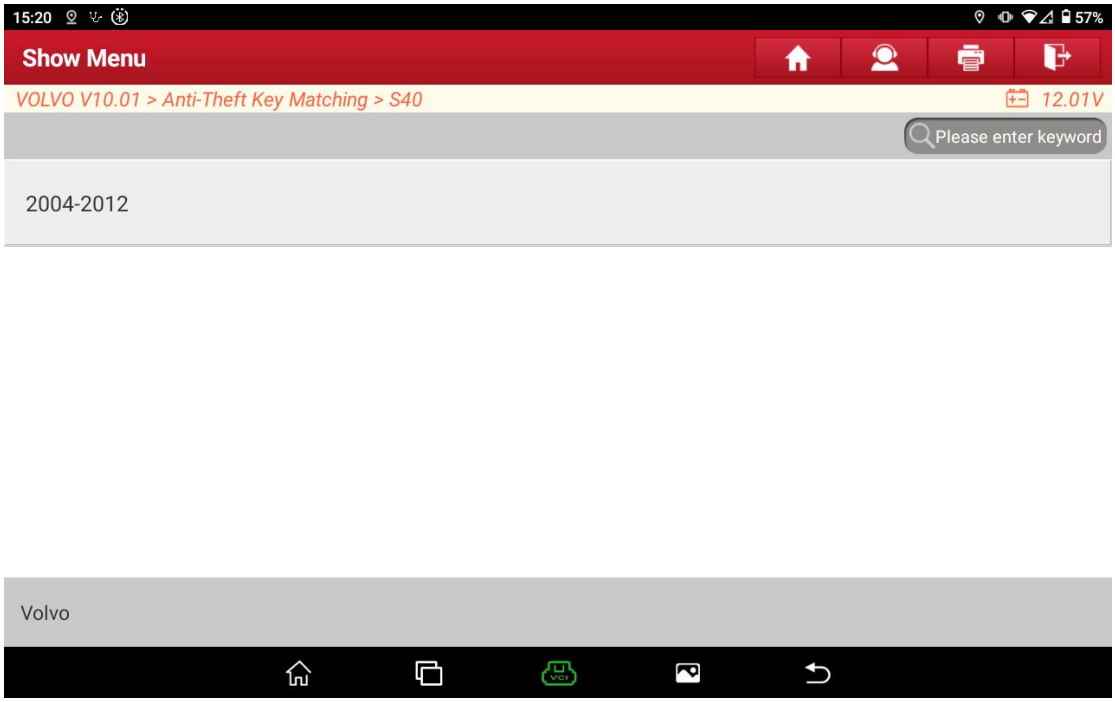


Figure 4

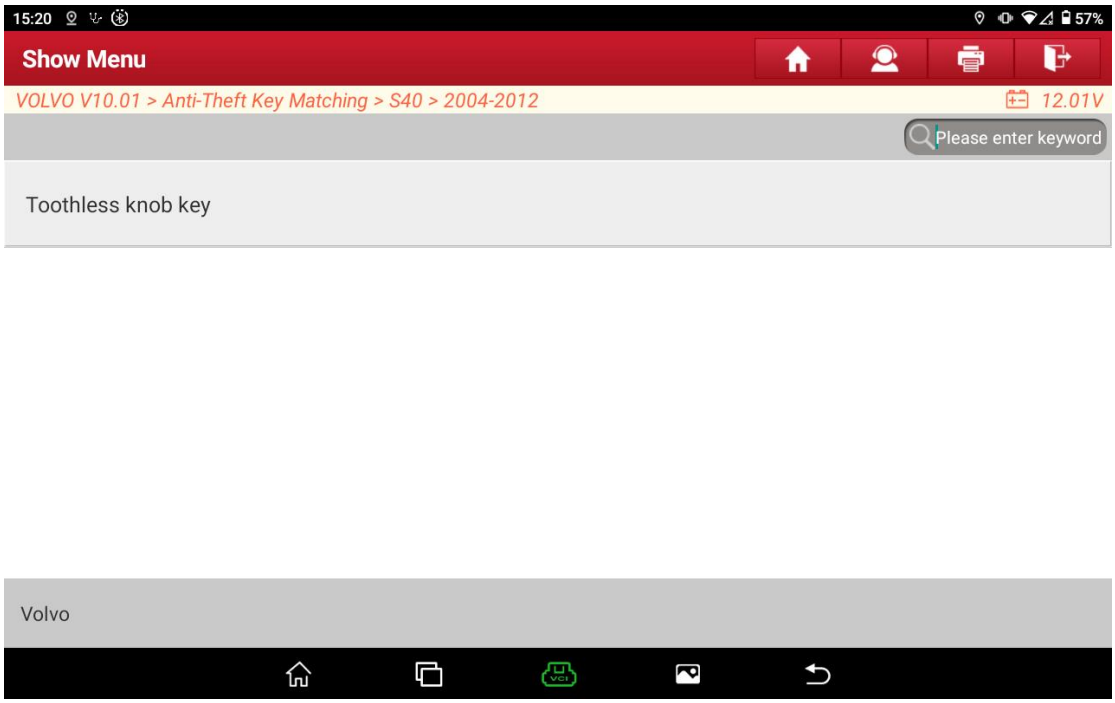


Figure 5

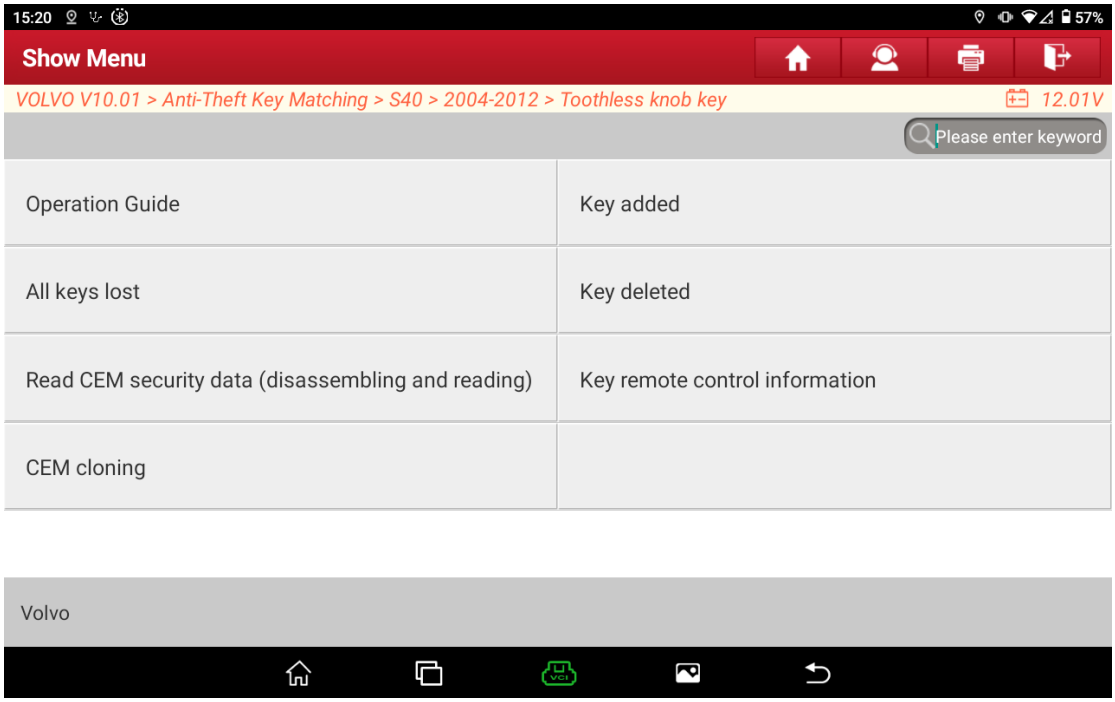


Figure 6

2. [Operation Guide]

Check the basic steps and precautions of the anti-theft matching process.

1) Select [Operation Guide] function to check the operation guide documents.

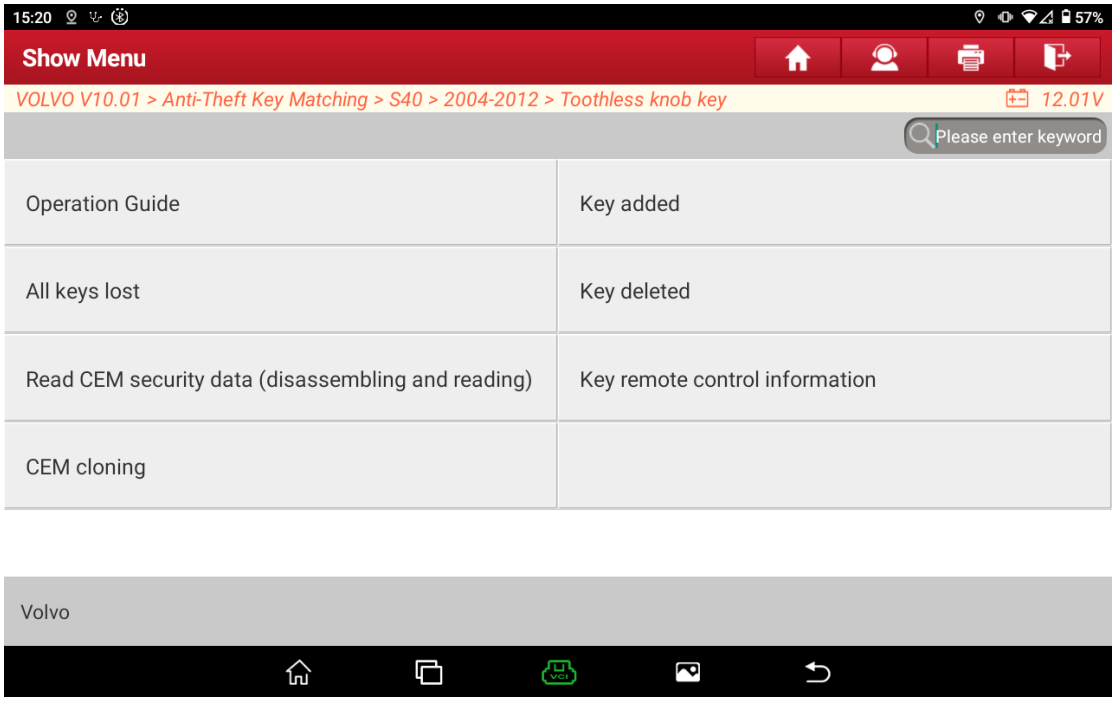


Figure 8

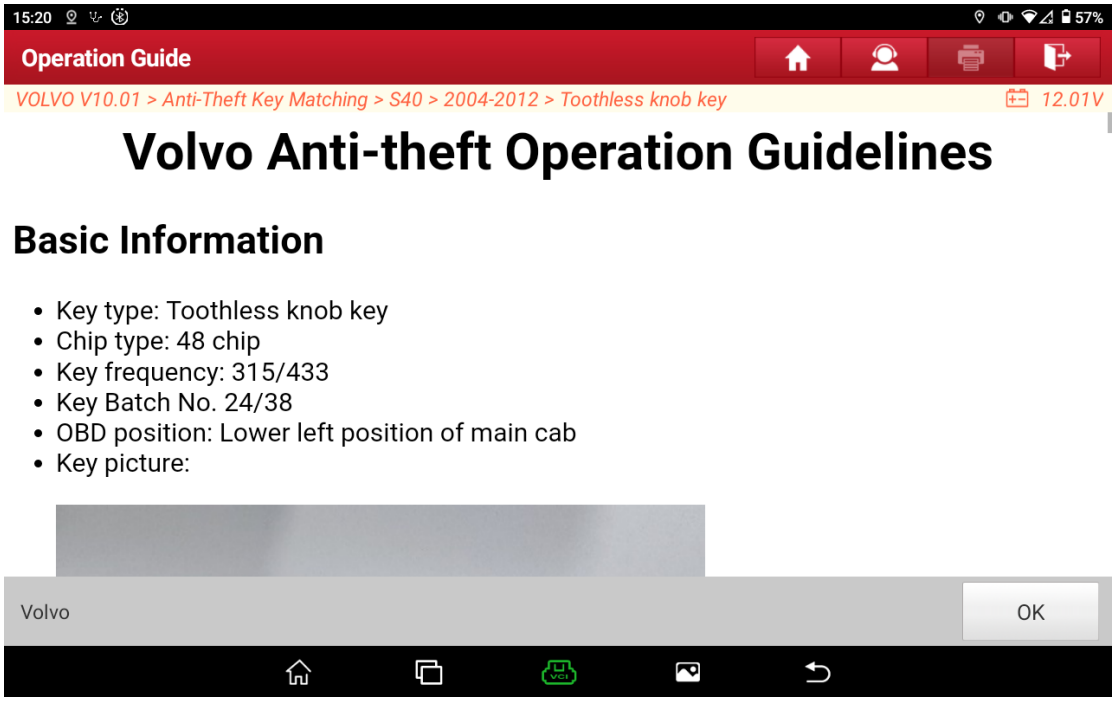


Figure 9

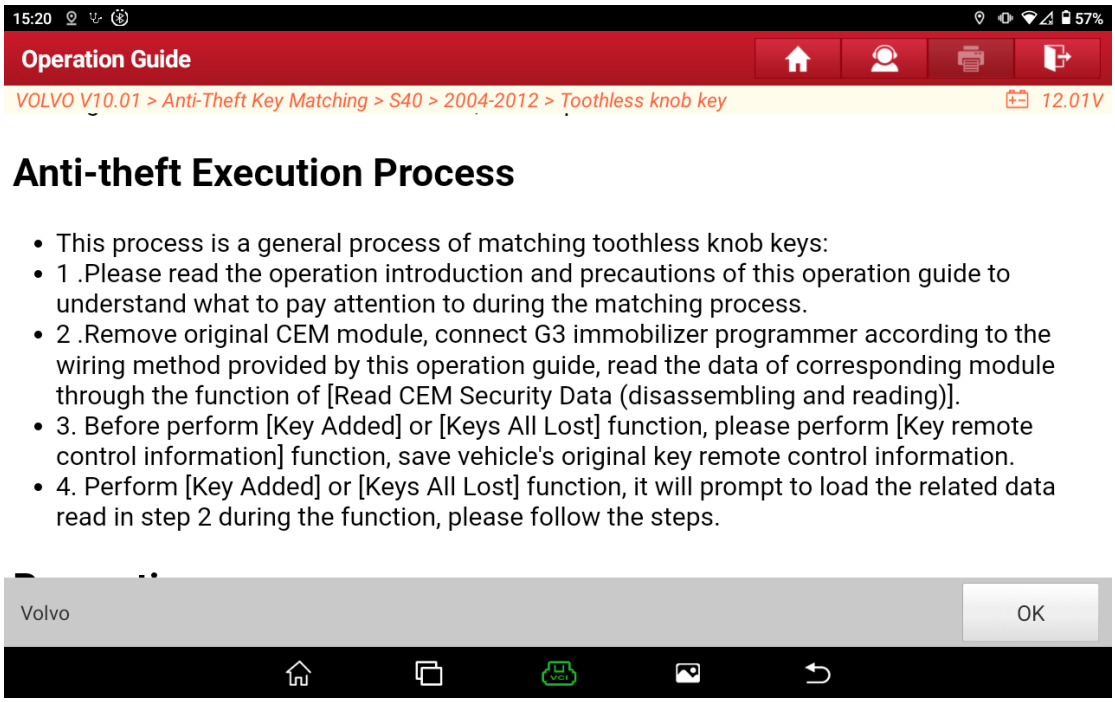


Figure 10

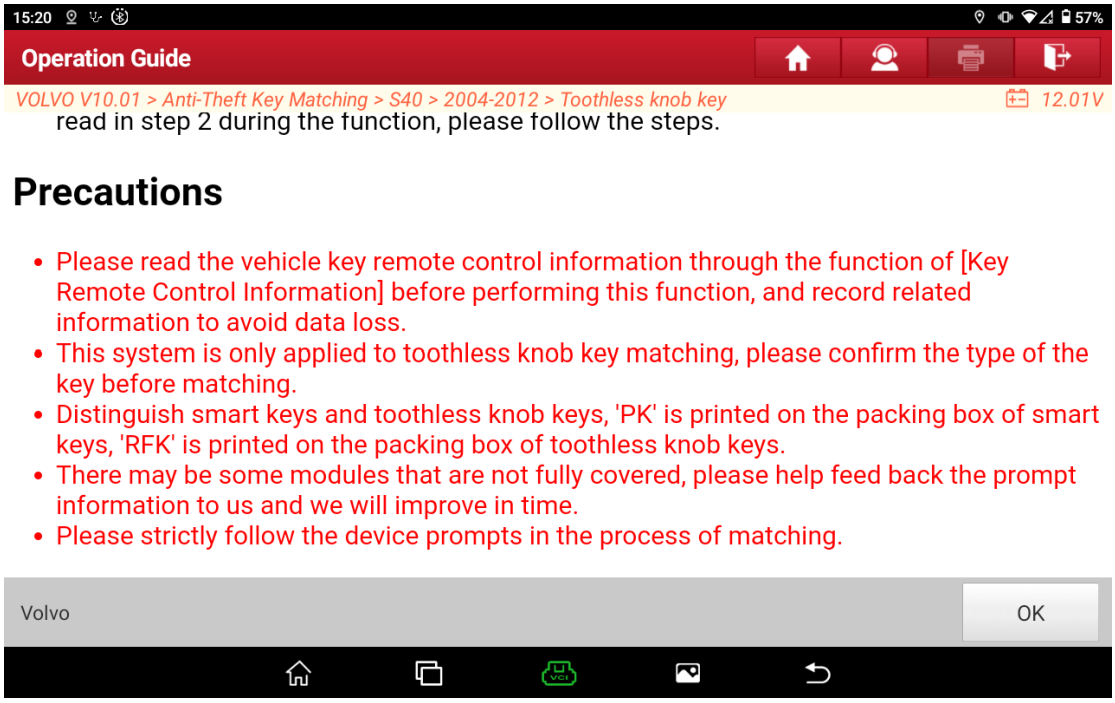


Figure 11

3. [Read CEM security data (disassembling and reading)]

By reading the operation document through the function of [Operation Guide], the MCU Cable V1 harness of G3 programmer should be used to connect the disassembled vehicle module, and then the MCU V2 adapter should be used to connect the G3 programmer to the vehicle module. Finally, the function [Read CEM security data (disassembling and reading)] should be selected to read the anti-theft data of the vehicle module. (The module location and cable connection are detailed in the [Operation Guide]. This document will not describe this part in detail. The procedure is as follows)

1) The connection diagram is as follows:

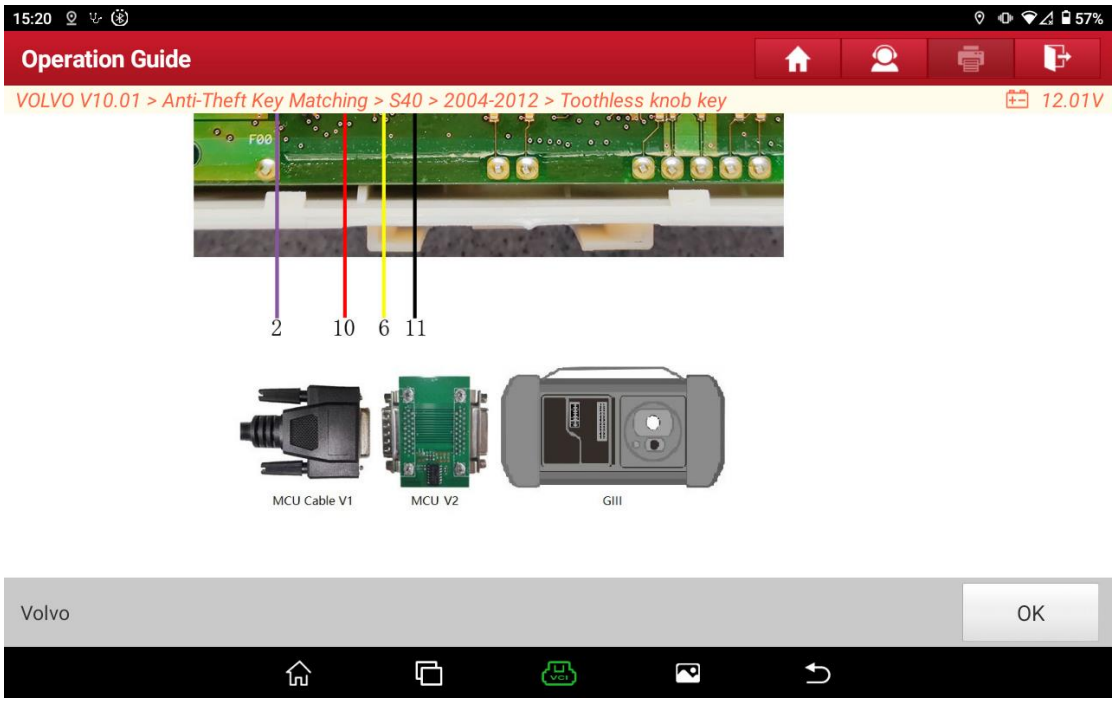


Figure 12

2) Select [Read CEM security data (disassembling and reading)] function

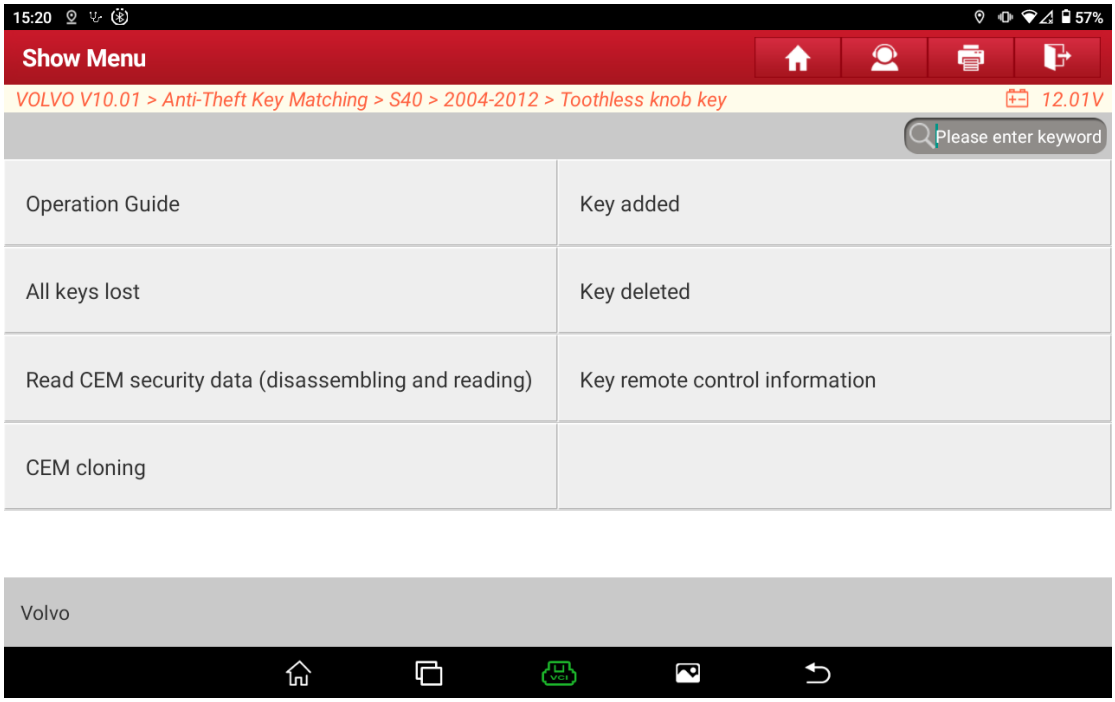


Figure 13

3) Prompt to view the [Operation Guide] function and click [YES] to proceed to the next step.

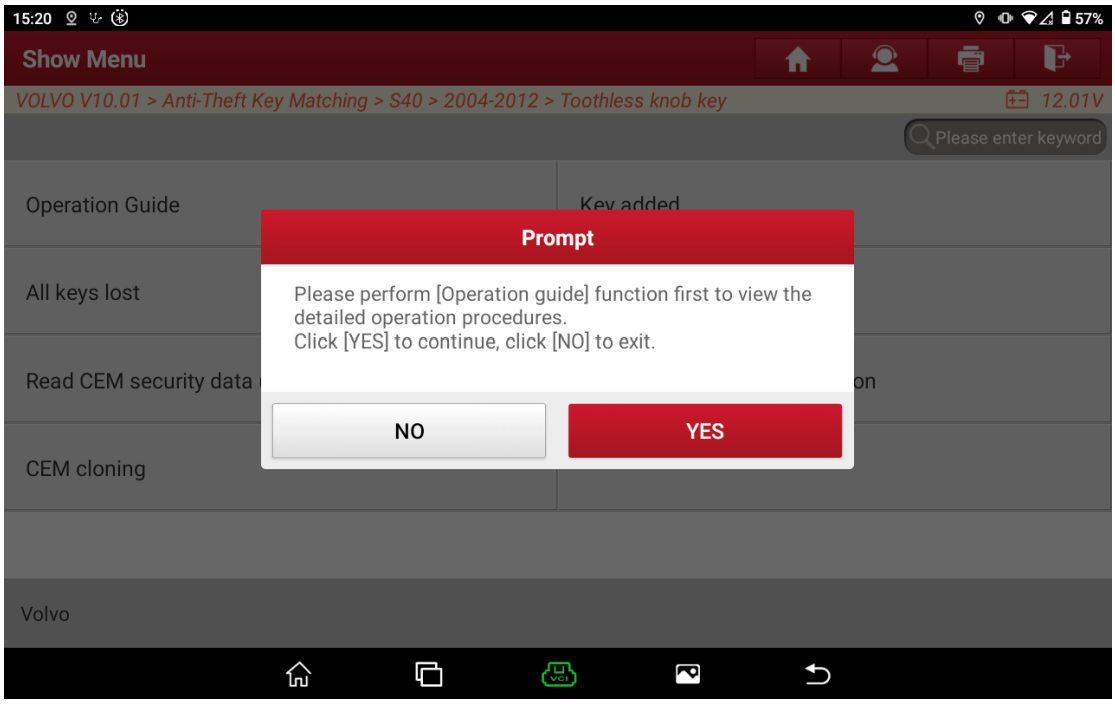


Figure 14

4) Connect G3 programmer. Connect anti-theft device, programmer and vehicle module according to [Operation guide]. Click [Yes] to proceed to the next step.

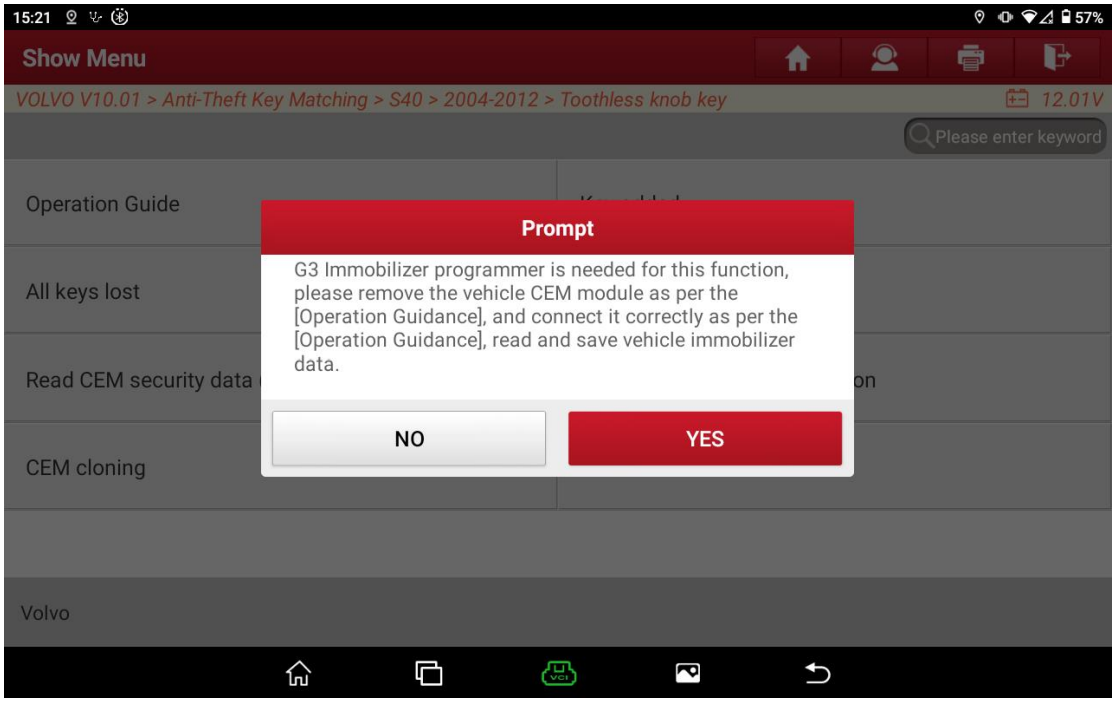
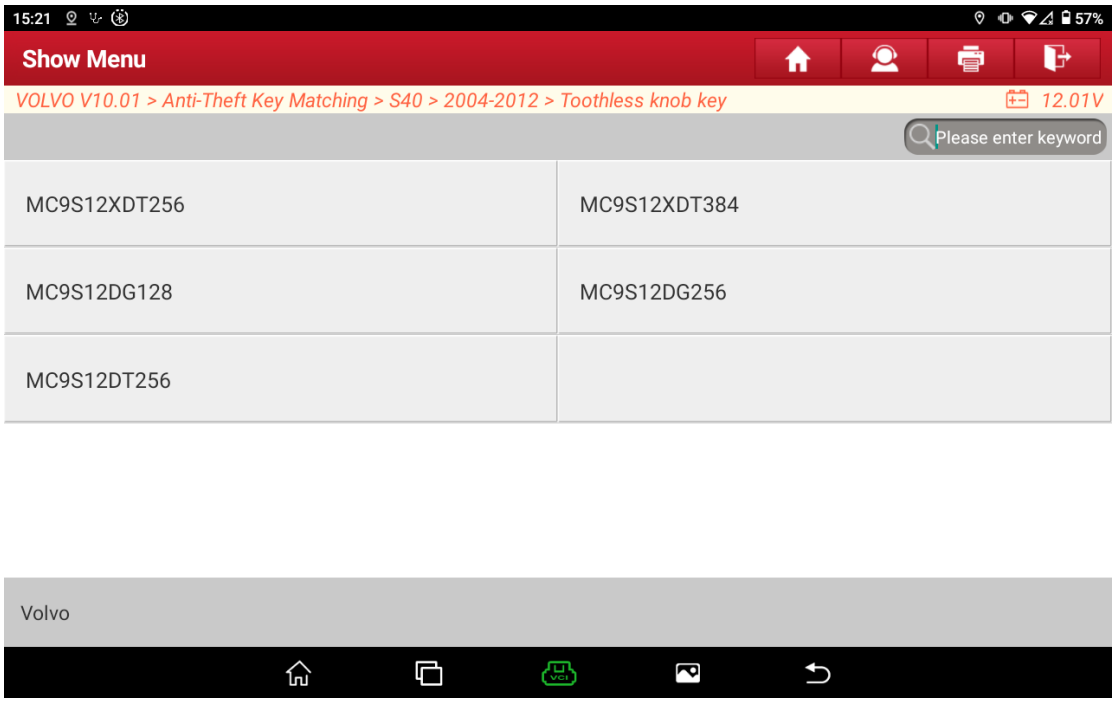


Figure 15

5) The module needs to read the relevant data of two chips. Select the corresponding module chip menu to read the data. For example, select MC9S12DT256 and MC9S12DG128 to read the data. For details about the connection mode, please refer to [Operation Guide] function.



6) A message is displayed indicating that data is being read. The read time is about 30 seconds. Do not move the device during this period to avoid data read failure.

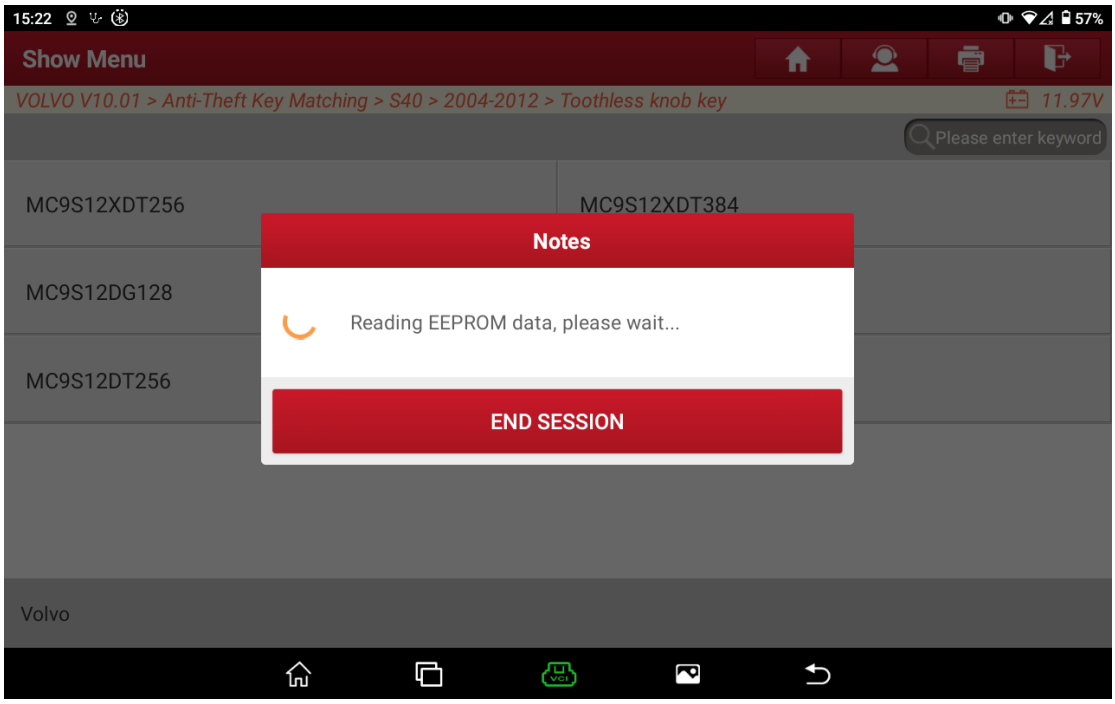


Figure 16

7) After the data is read successfully, a message is displayed indicating that the EEPROM data is read successfully and saved. After the data is saved, the function is executed successfully.

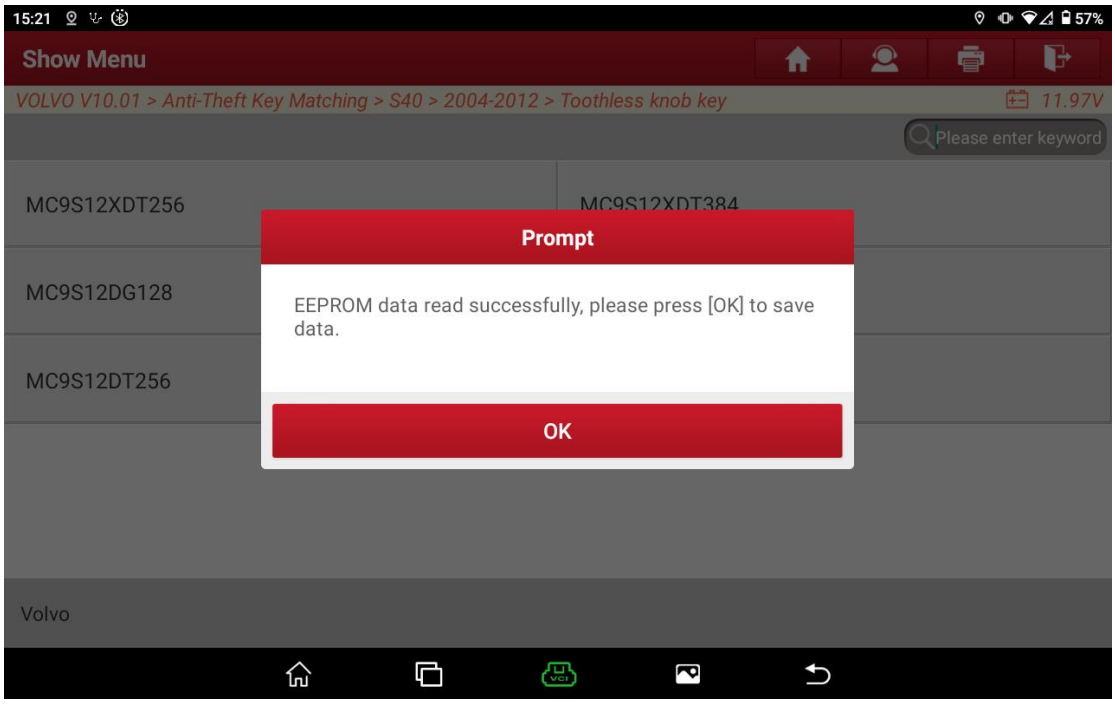


Figure 17

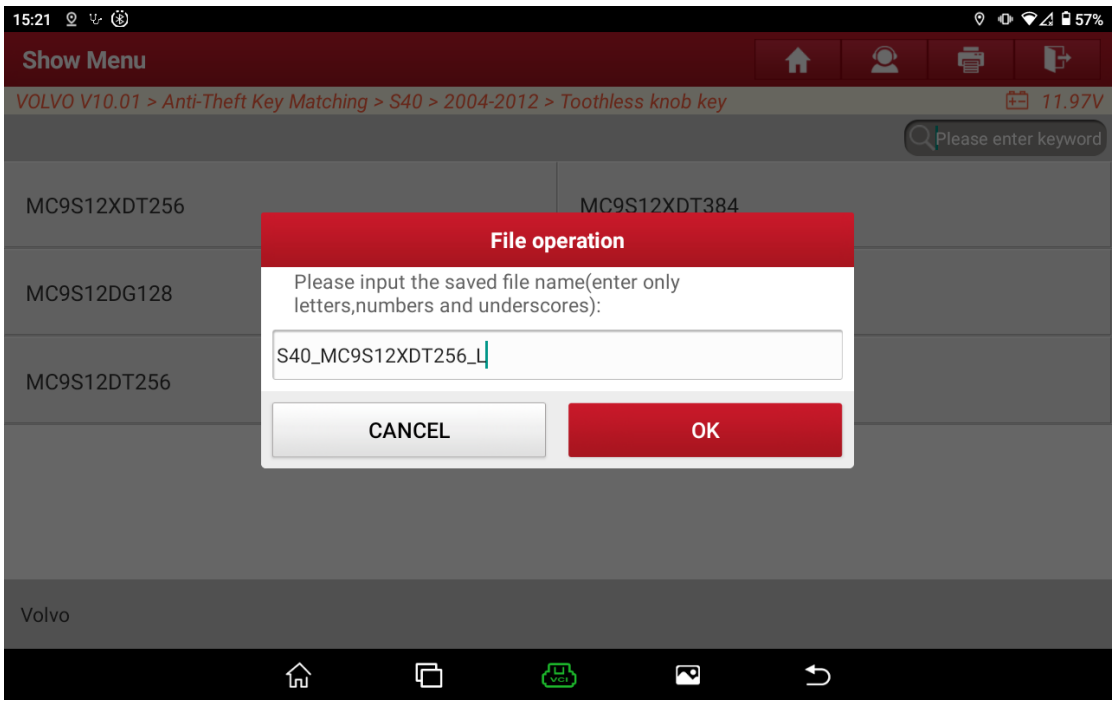


Figure 18

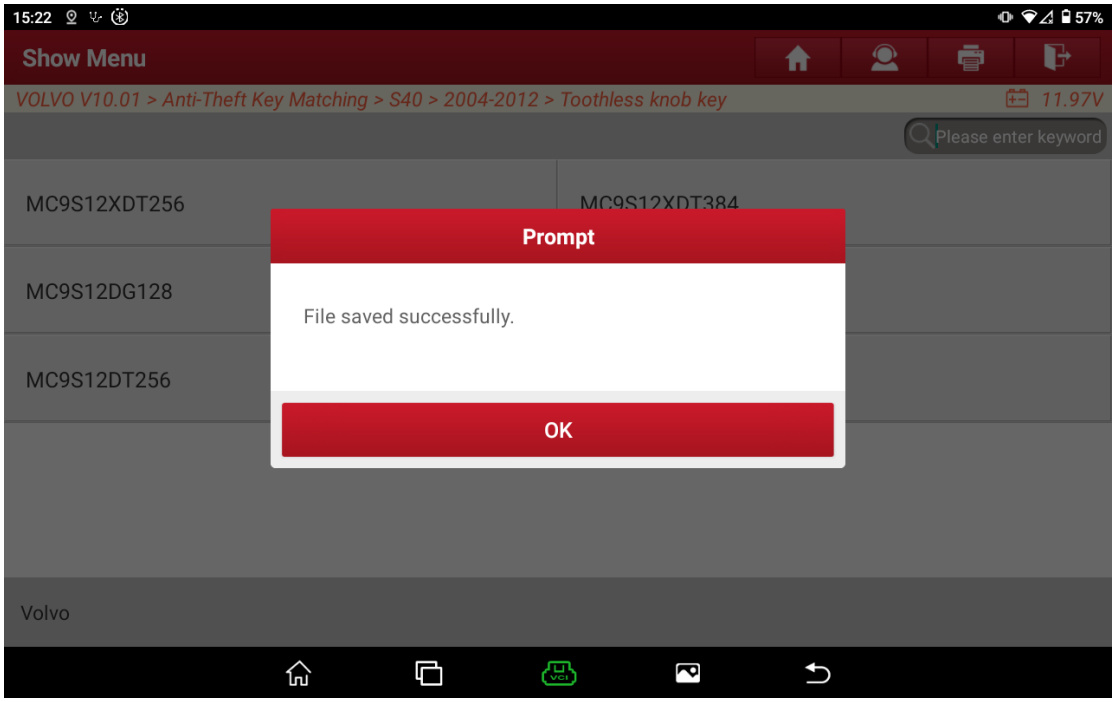


Figure 19

8) For details about how to read other chip data, see Step 5 to Step 7

4. [Key Remote Control Information]

Before implementing the key matching anti-theft function, it is necessary to perform the function of [Key remote control information] to read the key and remote control data information of the current vehicle, and save the screenshots in case the key and remote control data cannot be recovered if they are lost.

The read key remote control information can be used to confirm whether the current model uses 16-digit remote control data or 24-digit remote control data, and purchase the corresponding key according to the actual situation.

5. [Key added]

The function of [Key added] is used to add keys to the vehicle without deleting the original car keys. The function of [All keys lost] is used to add keys to the vehicle after deleting all the original car keys. After deleting the original car keys, the original car keys need to be re-matched before they can be used again. The function of [Key deleted] is used to delete the original car keys. Please select a function based on actual requirements. This document takes [Key added] as an example:

1) **Select [Key added] function, and the prompt is displayed to view the [Operation guide] function, click [YES] to proceed to the next step.**

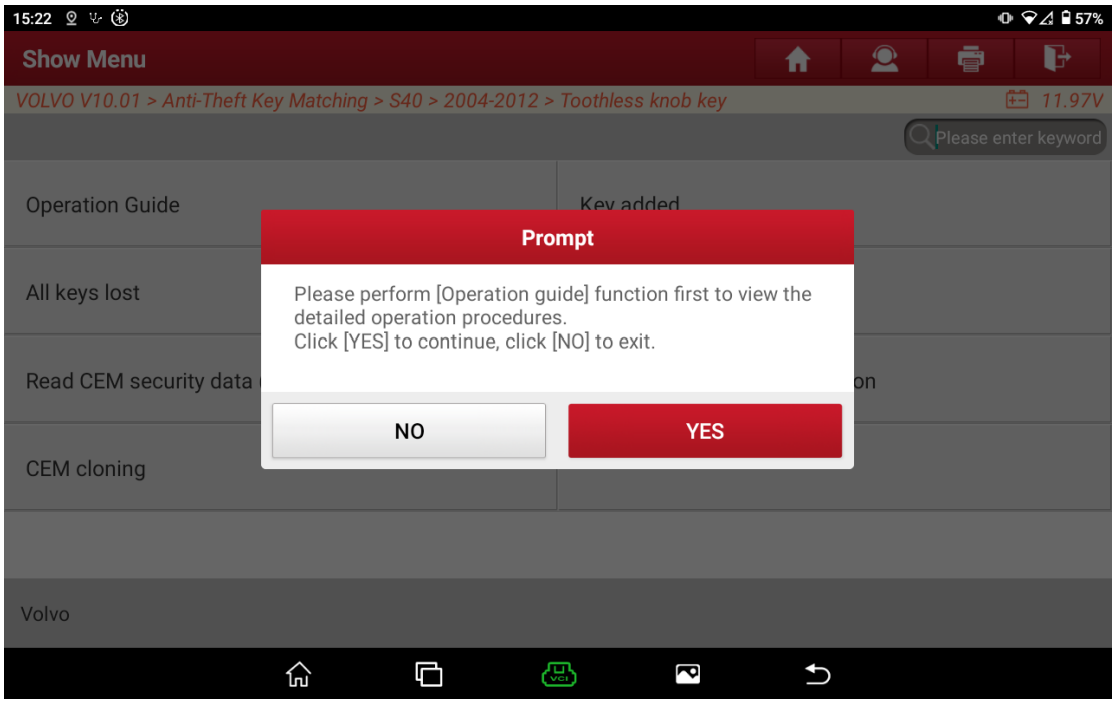


Figure 30

2) **After completing the operation as prompted, click [OK] to proceed to the next step.**

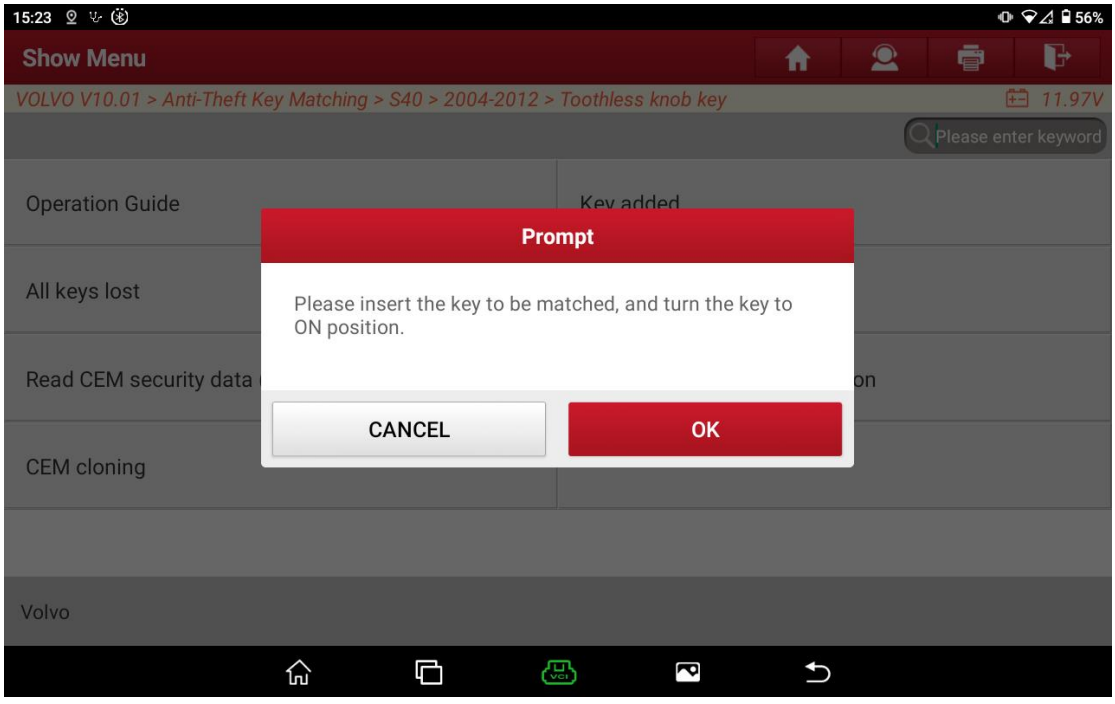


Figure 31

3) A prompt is displayed to load two copies of CEM security data, click [OK] to load the anti-theft data.

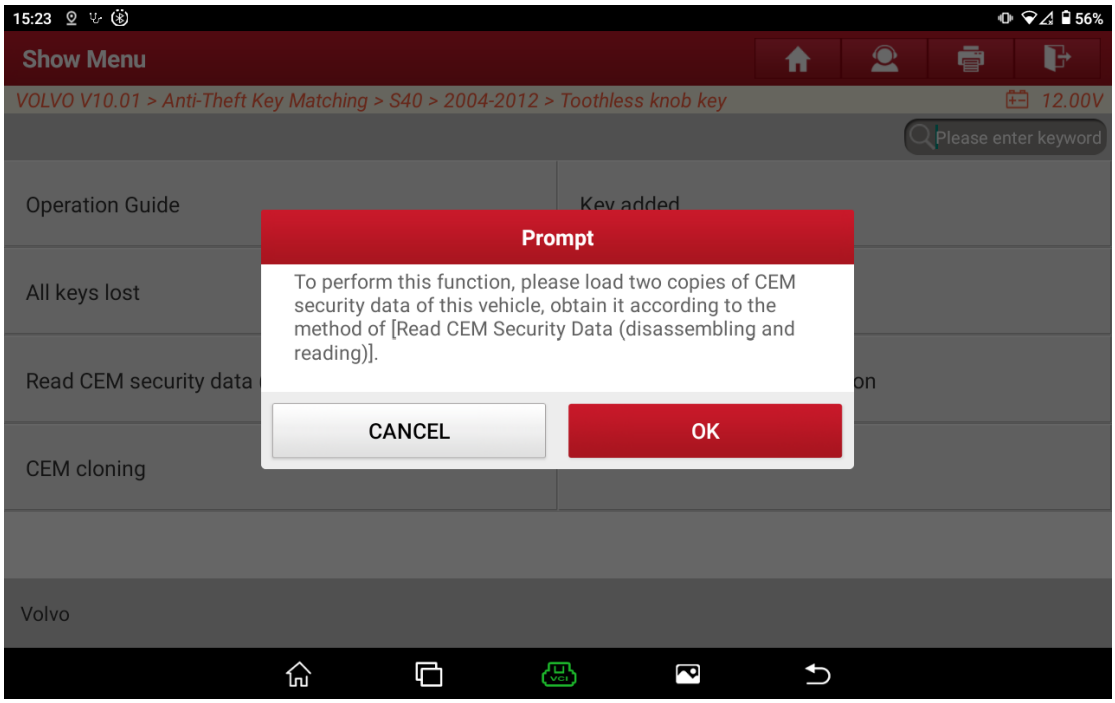


Figure 32

4) Select the first read data file, here we select file S40_MC9S12DG128.bin.

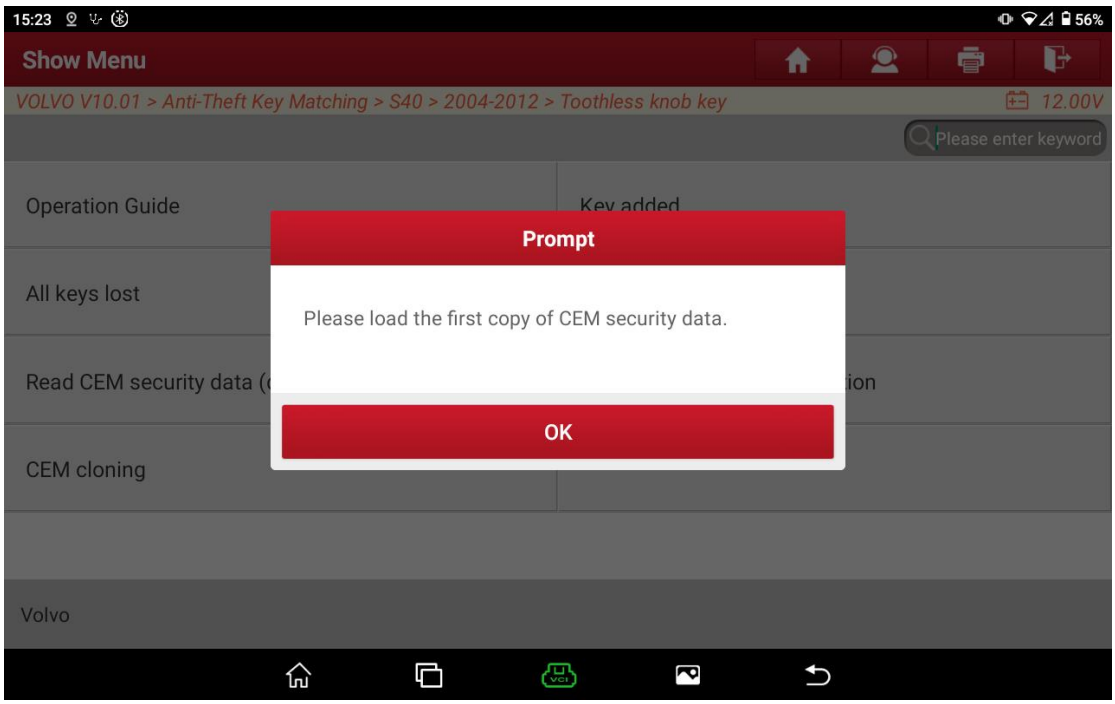


Figure 33

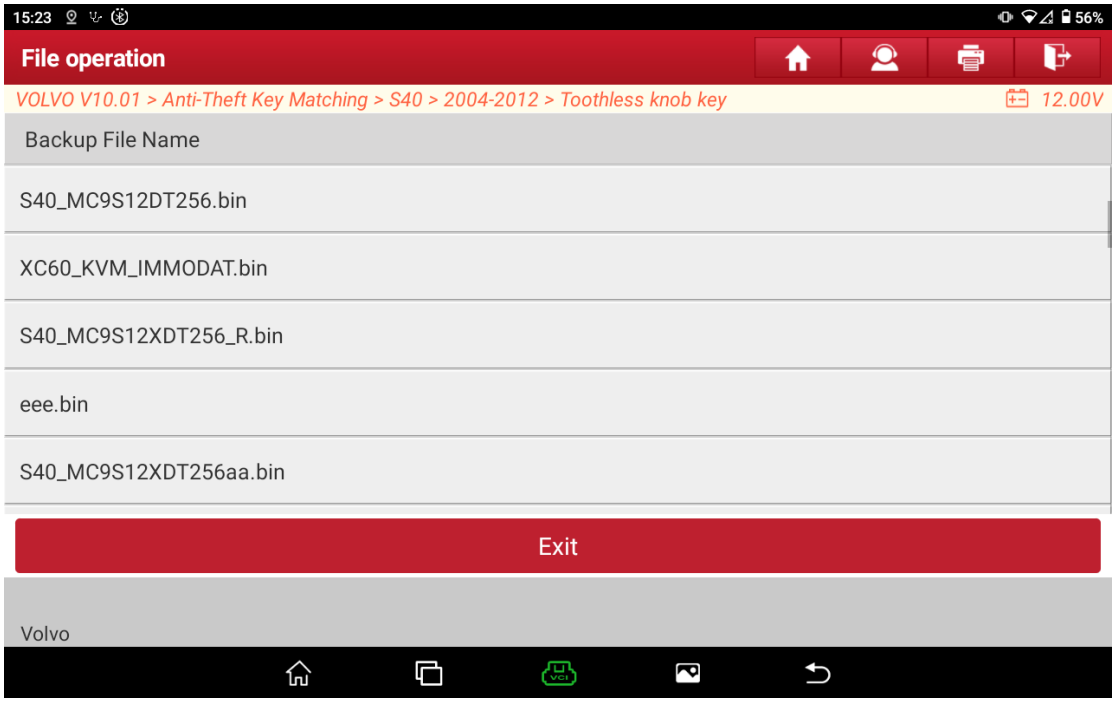
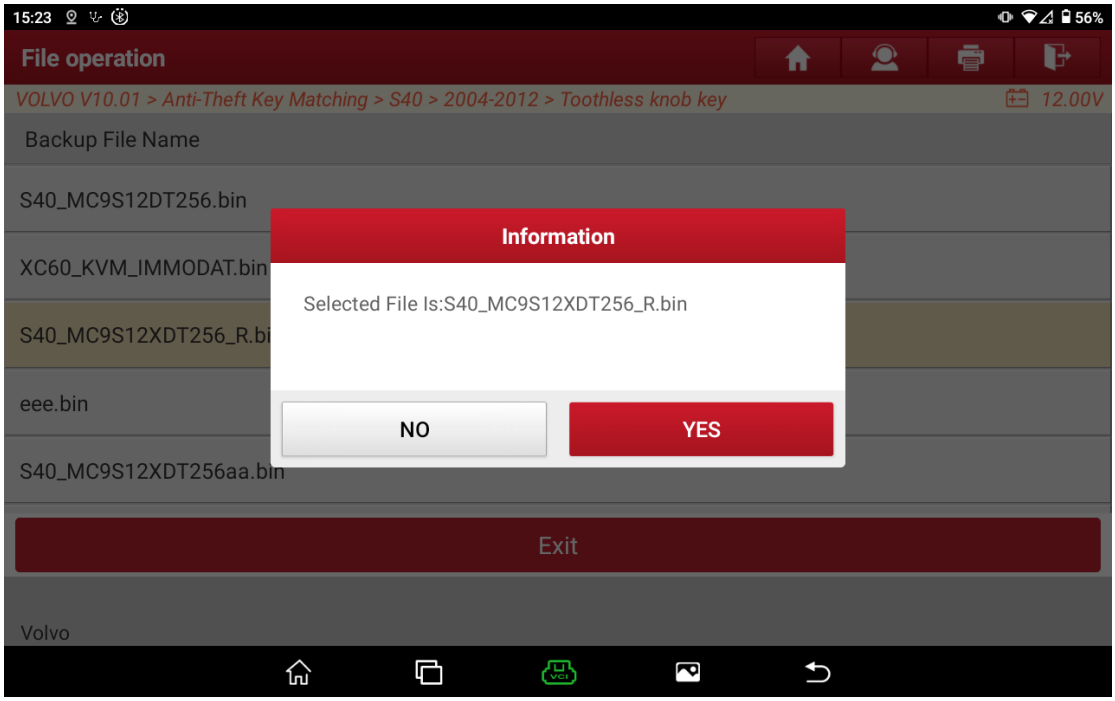


Figure 34



5) **Select the second read data file, here we select file S40_MC9S12DT256. bin.**

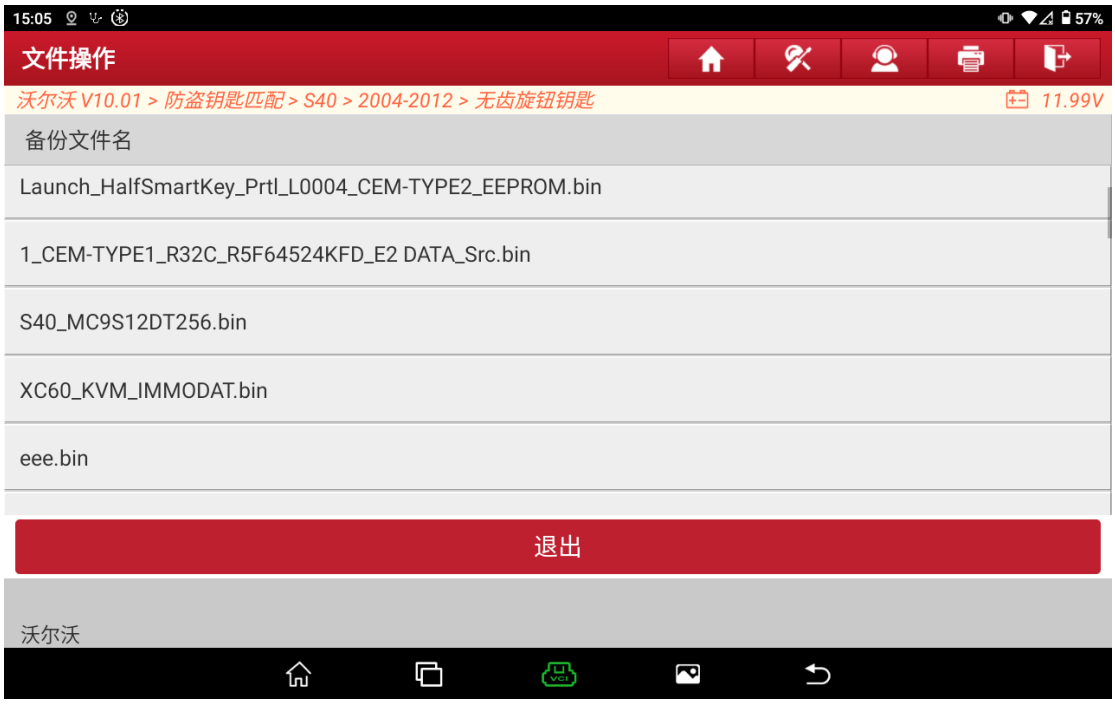
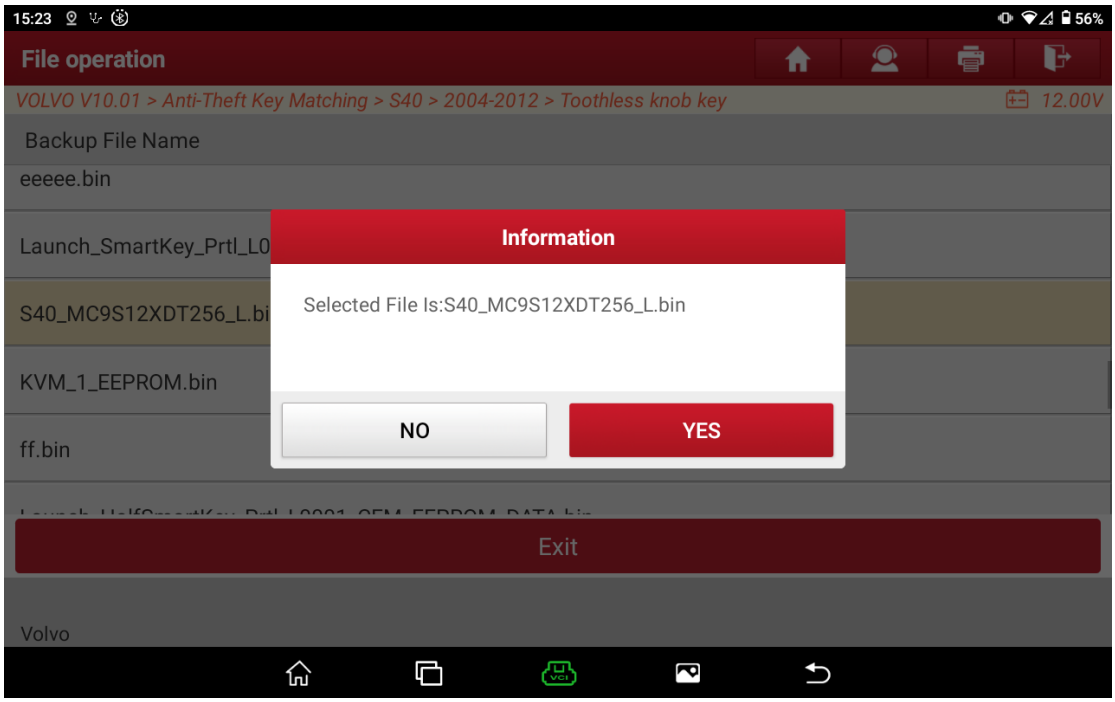


Figure 36



6) **Input the 8-digit remote control ID (The remote control ID and remote control data are on the key packaging shell when the key is purchased).**

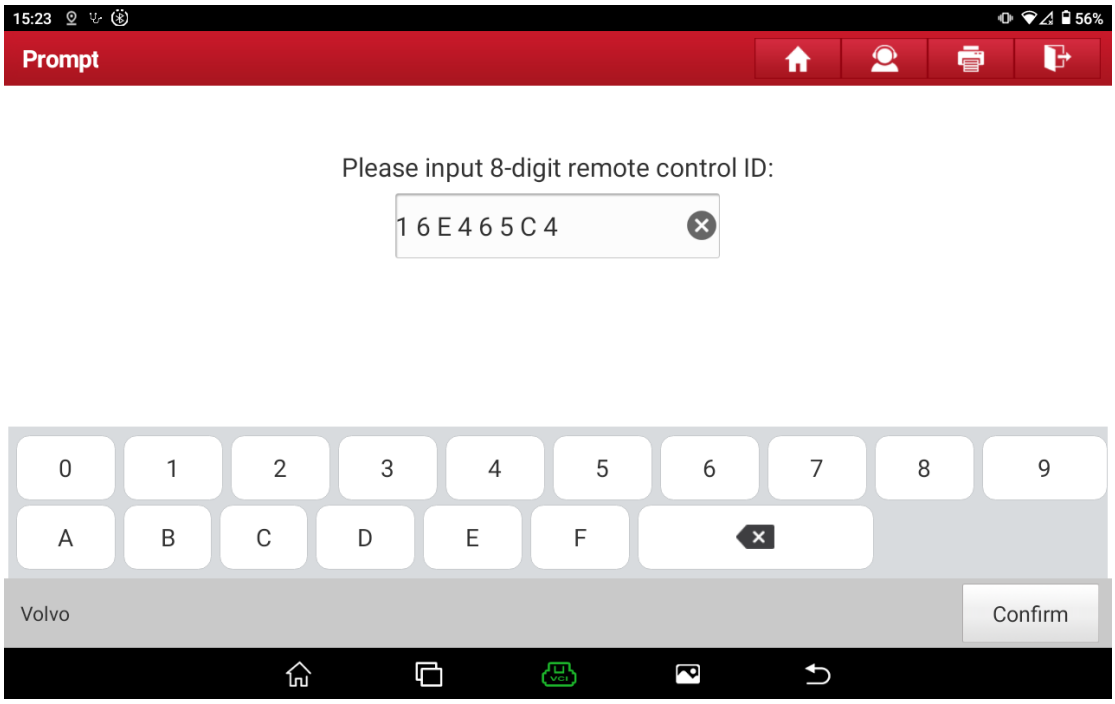


Figure 38

7) **Input the 24-digit remote control data (The example model is a 24-digit remote control, please select the key according to the actual situation), click [OK] to proceed to the next step.**

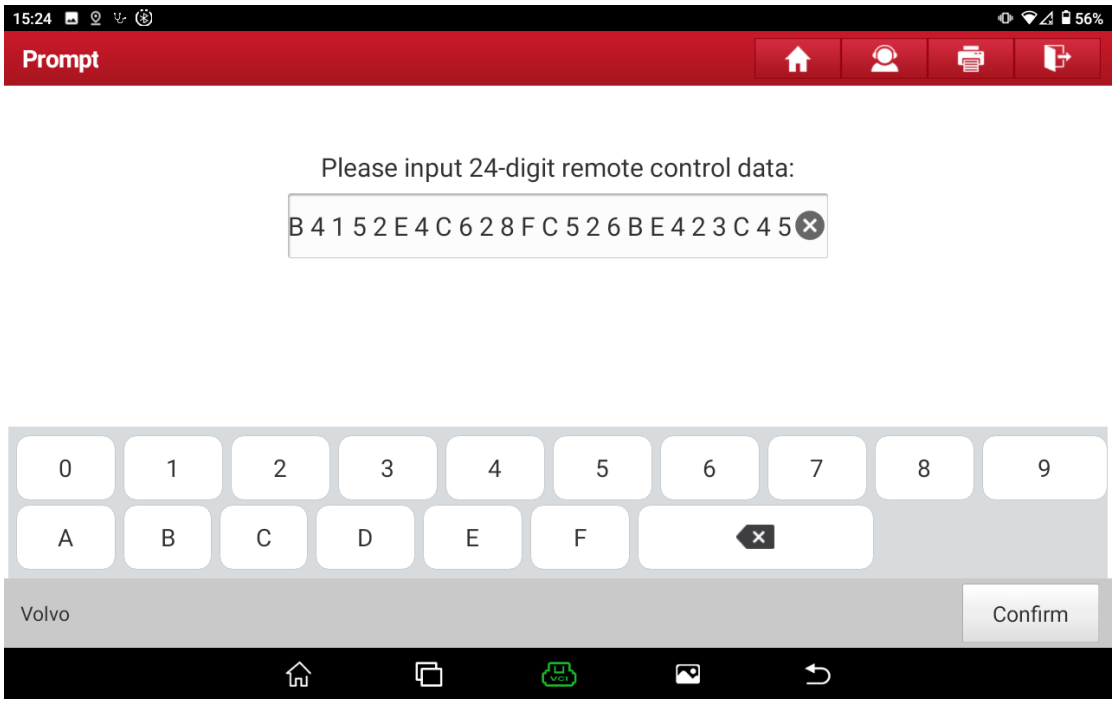


Figure 39

8) **Wait for key matching, which takes about 1 minute.**

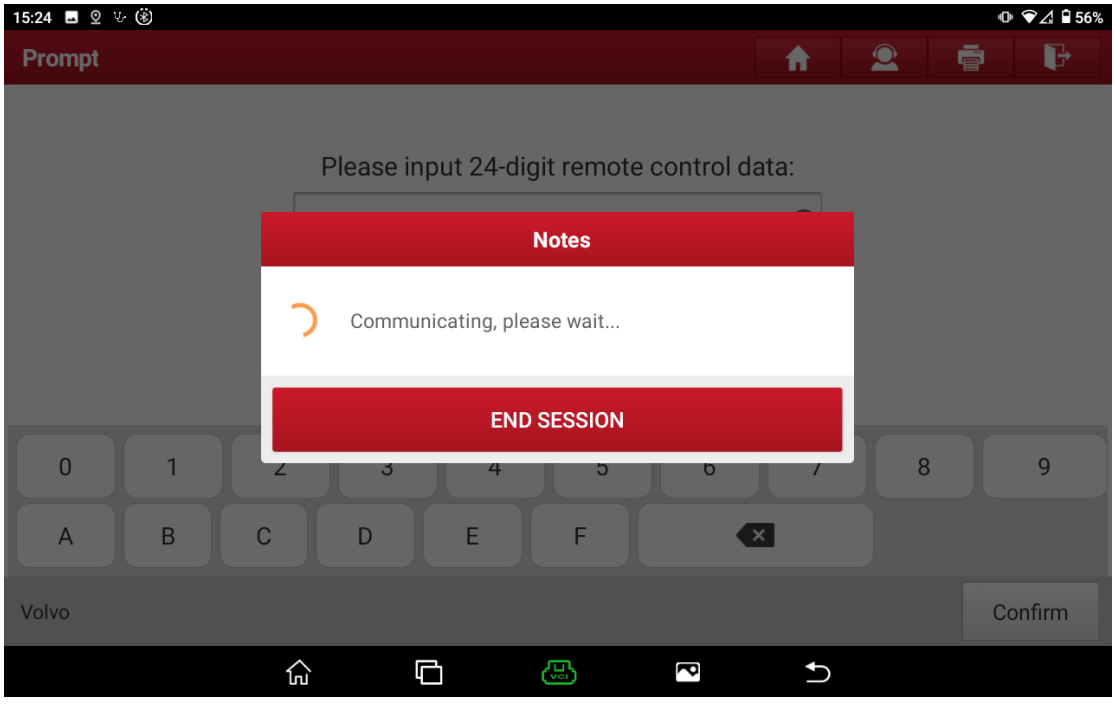
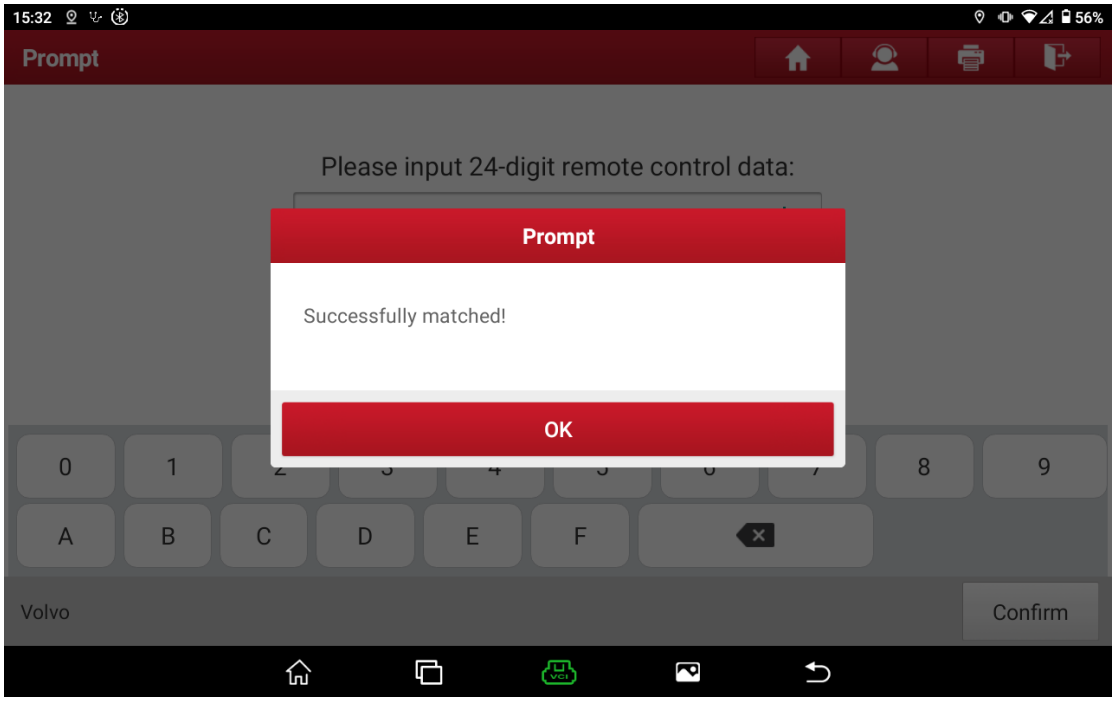


Figure 40



3.半智能钥匙/智能钥匙防盗系统

3.1Model Coverage

The anti-theft process of the following models is basically the same, but different vehicles need to read vehicle module data in different ways, which can be divided into the following three categories (each color represents one) :

Brand	Model	Year	Key type
VOLVO	S60	2010-2018	Smart Key/Half-Smart Key
VOLVO	S60 Cross Country	2016-2018	Smart Key/Half-Smart Key
VOLVO	S60L	2014-2018	Smart Key/Half-Smart Key
VOLVO	S80	2010-2016	Smart Key/Half-Smart Key
VOLVO	S80L	2010-2015	Smart Key/Half-Smart Key
VOLVO	V60	2011-2018	Smart Key/Half-Smart Key
VOLVO	V60 Cross Country	2015-2018	Smart Key/Half-Smart Key
VOLVO	V70	2009-2016	Smart Key/Half-Smart Key
VOLVO	XC60	2010-2018	Smart Key/Half-Smart Key
VOLVO	XC70	2011-2016	Smart Key/Half-Smart Key
VOLVO	S80	2007-2009	Smart Key/Half-Smart Key
VOLVO	S80L	2008-2009	Smart Key/Half-Smart Key
VOLVO	XC60	2006-2009	Smart Key/Half-Smart Key
VOLVO	XC70	2008-2010	Smart Key/Half-Smart Key

VOLVO	V40	2012-2018	Smart Key/Half-Smart Key
VOLVO	V40 Cross Country	2013-2018	Smart Key/Half-Smart Key

3.2Requirements

1.Launch IMMO PRO/IMMO PAD (professional version).
2. As for the compliance smart keys/semi-smart keys used for anti-theft matching, it is recommended to use the original factory key, because some secondary factory keys may have no intelligence after matching.
3. The difference between the semi-smart key and the smart key is that the matching process of the smart key contains KVM data disassembling & reading and data decryption steps. Other matching processes are basically the same as those of the smart key.

3.3Procedure

This operation process demonstration takes Volvo 2016 XC60 smart key as an example.

Vehicle series entry

Select [Volvo] -> [Automatic scan] -> [XC60] -> [2010-2018] -> [Smart key] (See Figure 1, Figure 2, Figure 3, Figure 4, Figure 5, Figure 6 and Figure 7 for the process steps)

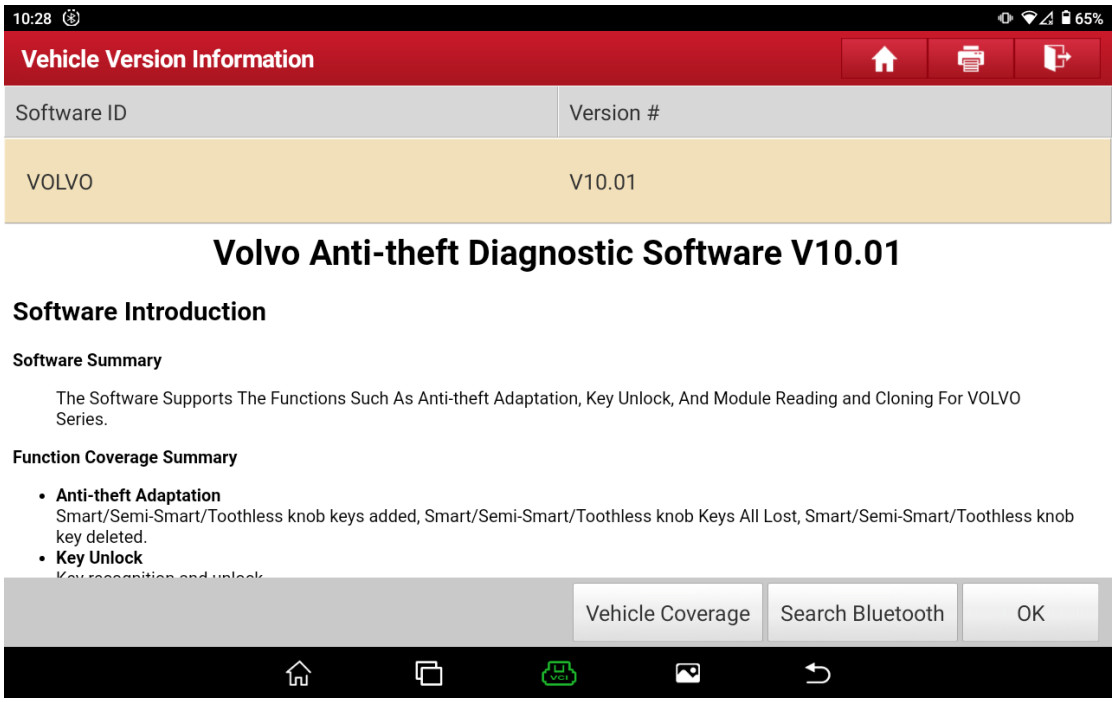


Figure 1

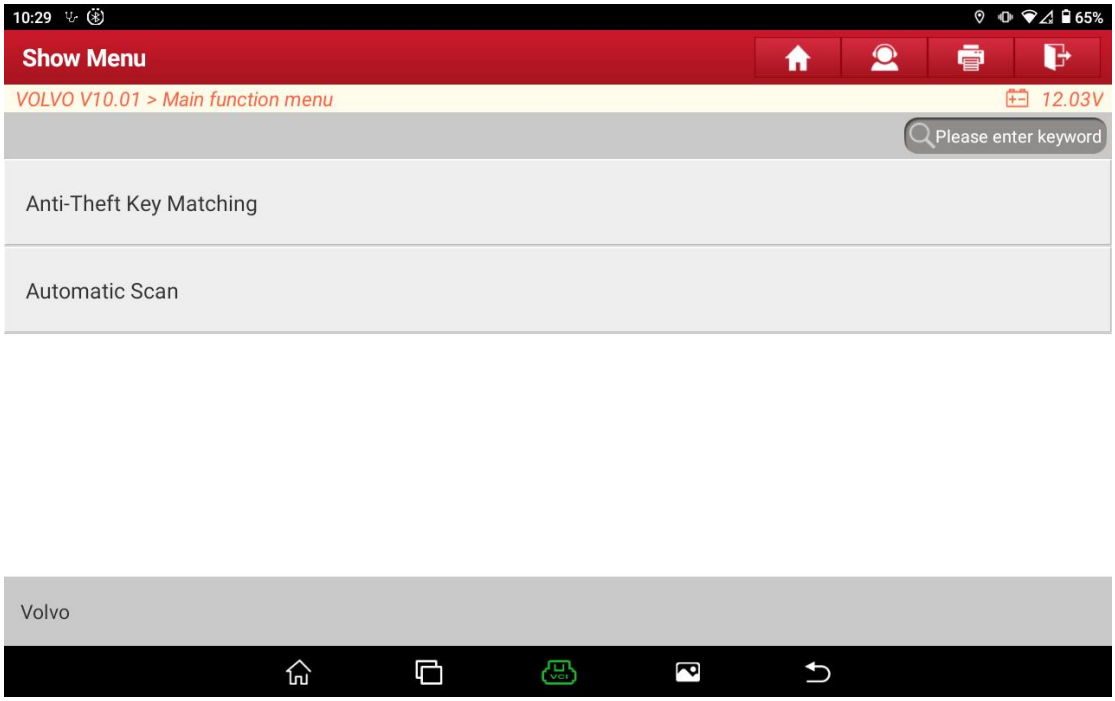


Figure 2

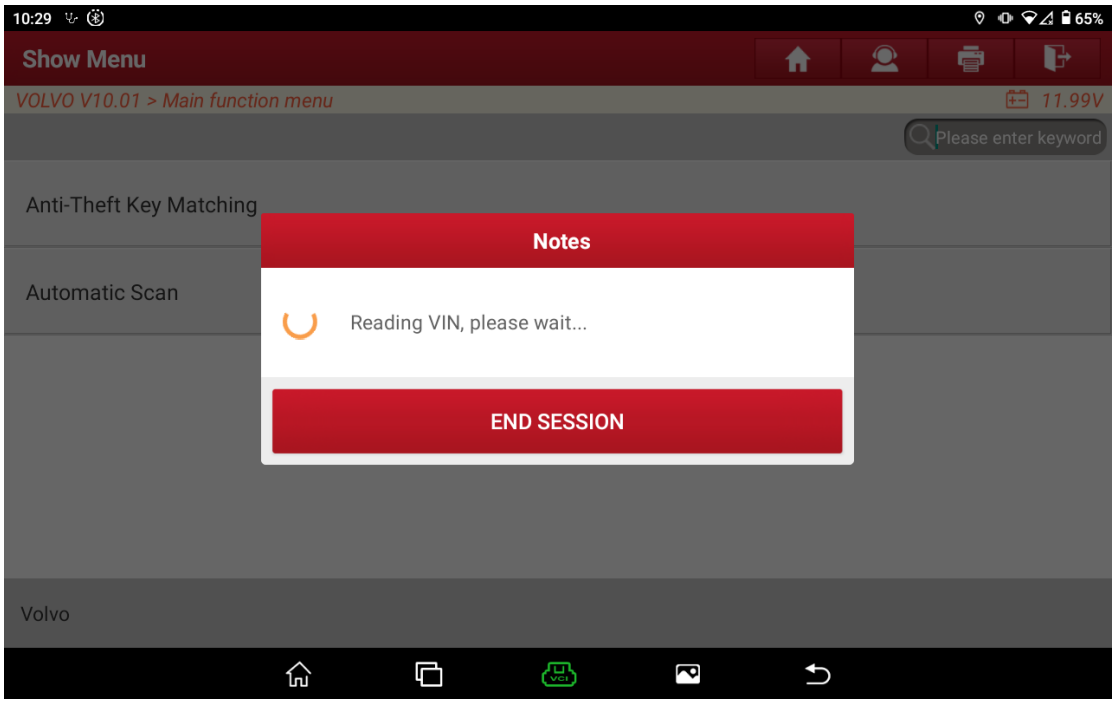


Figure 3

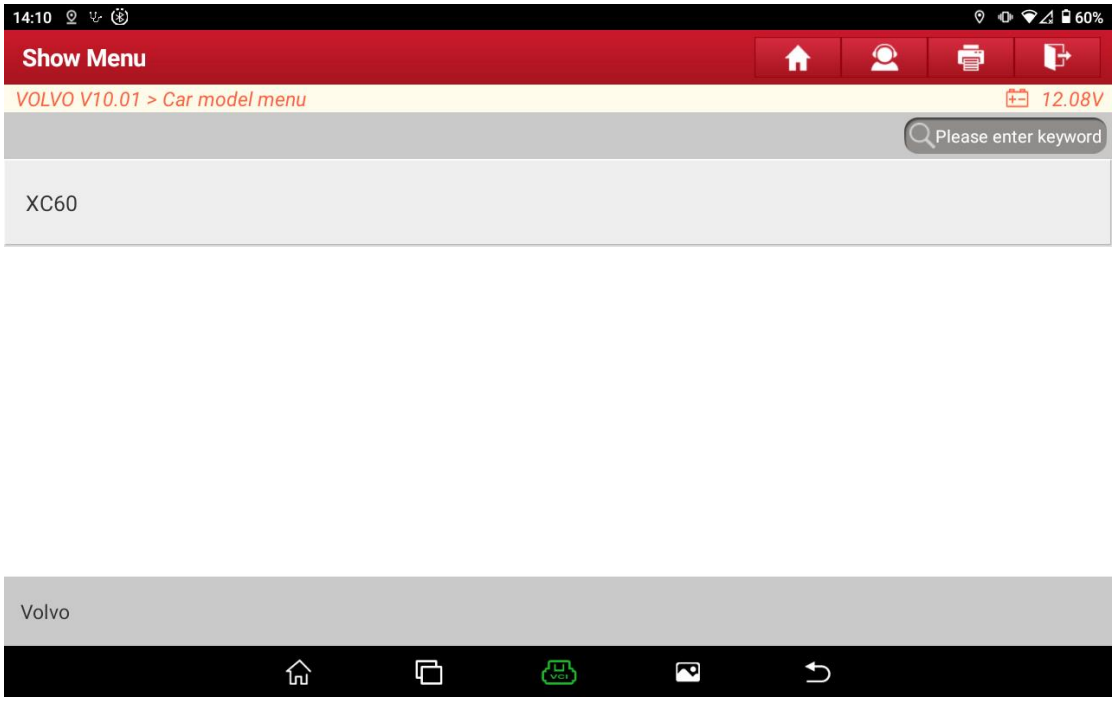


Figure 4

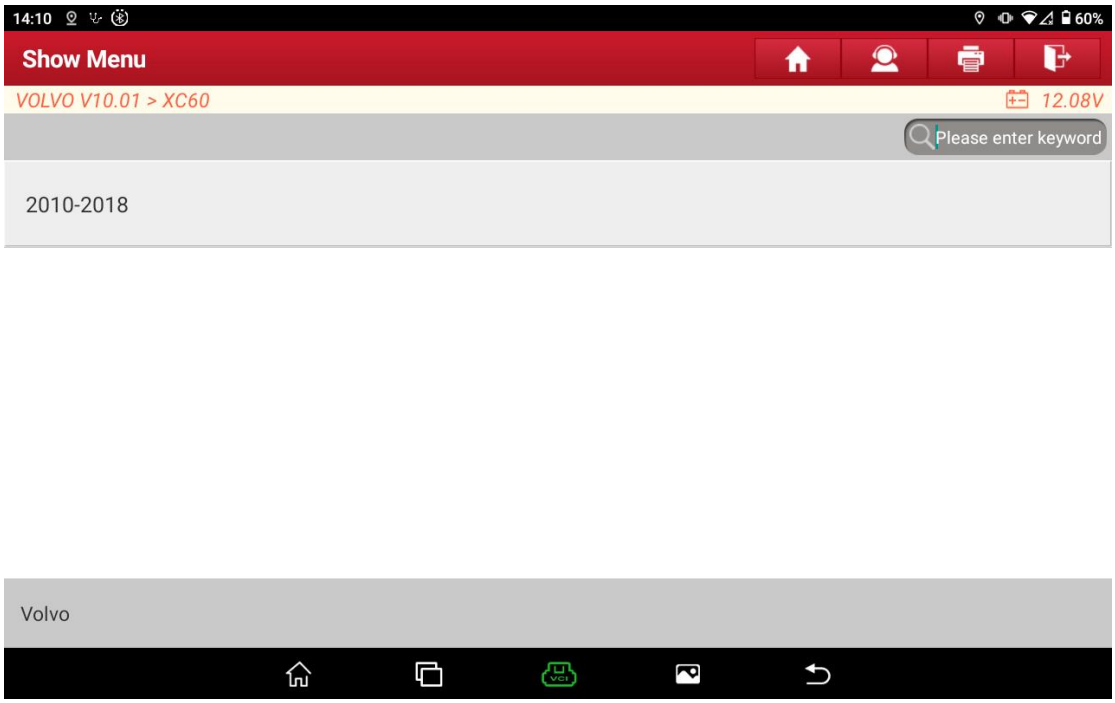


Figure 5

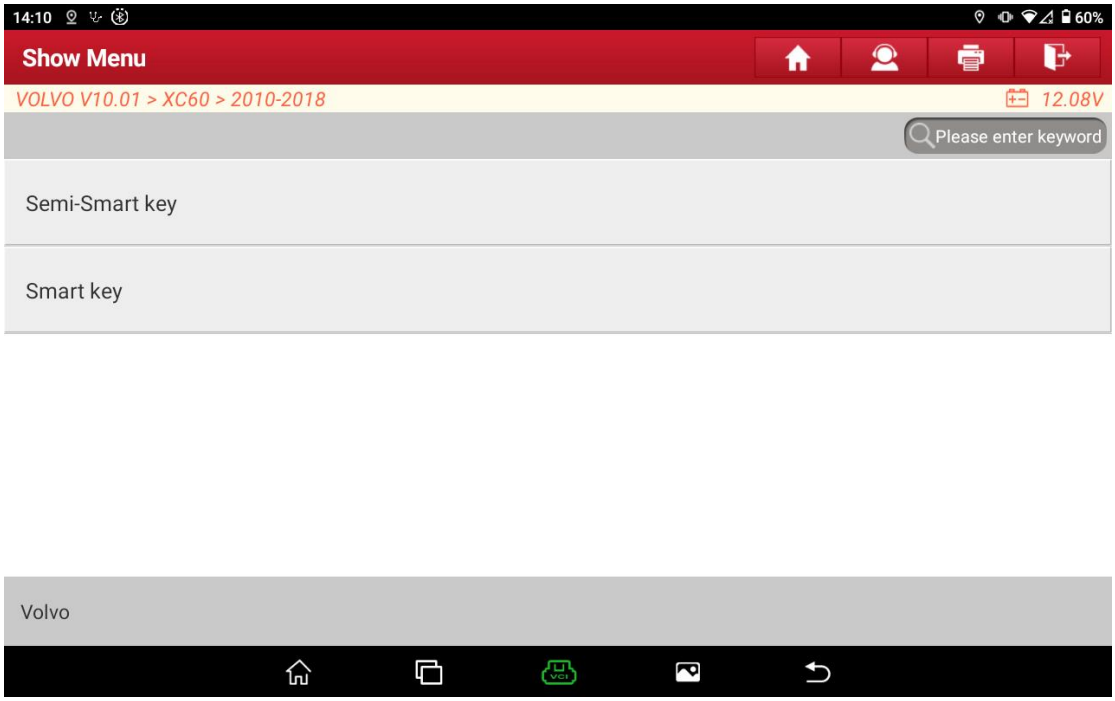


Figure 6

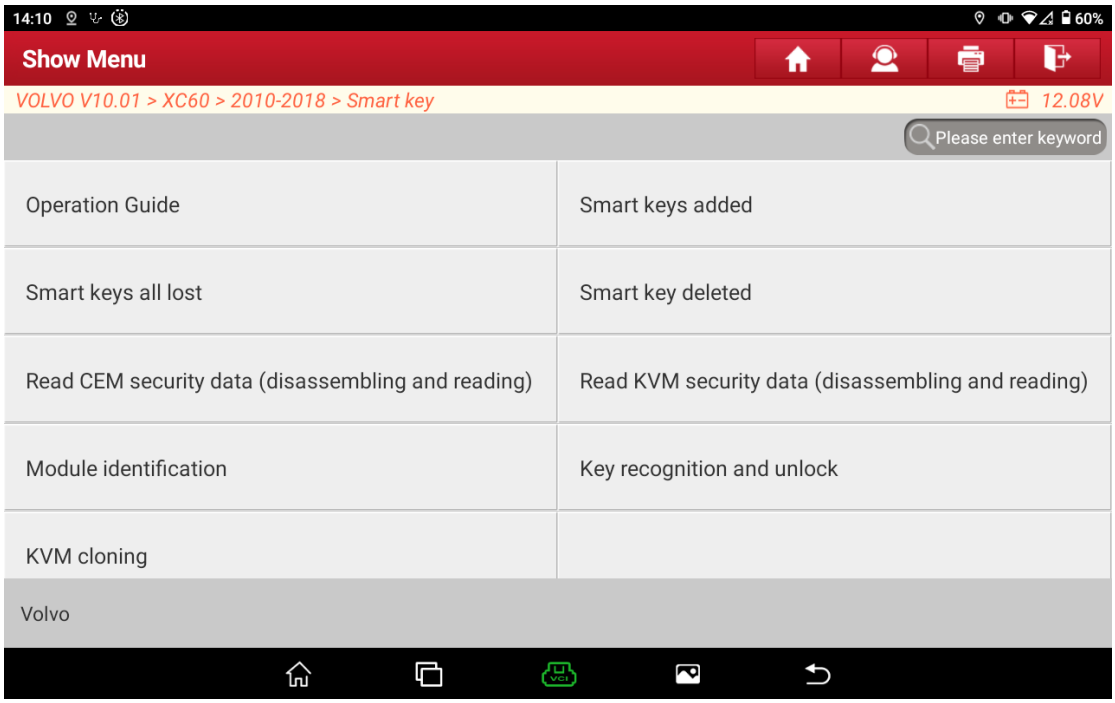


Figure 7

2. [Operation Guide]

Check the basic steps and precautions of the anti-theft matching process. (See Figure 8, Figure 9, Figure 10, and Figure 11 for the process steps)

1) Select the [Operation Guide] function to view the operation guide document.

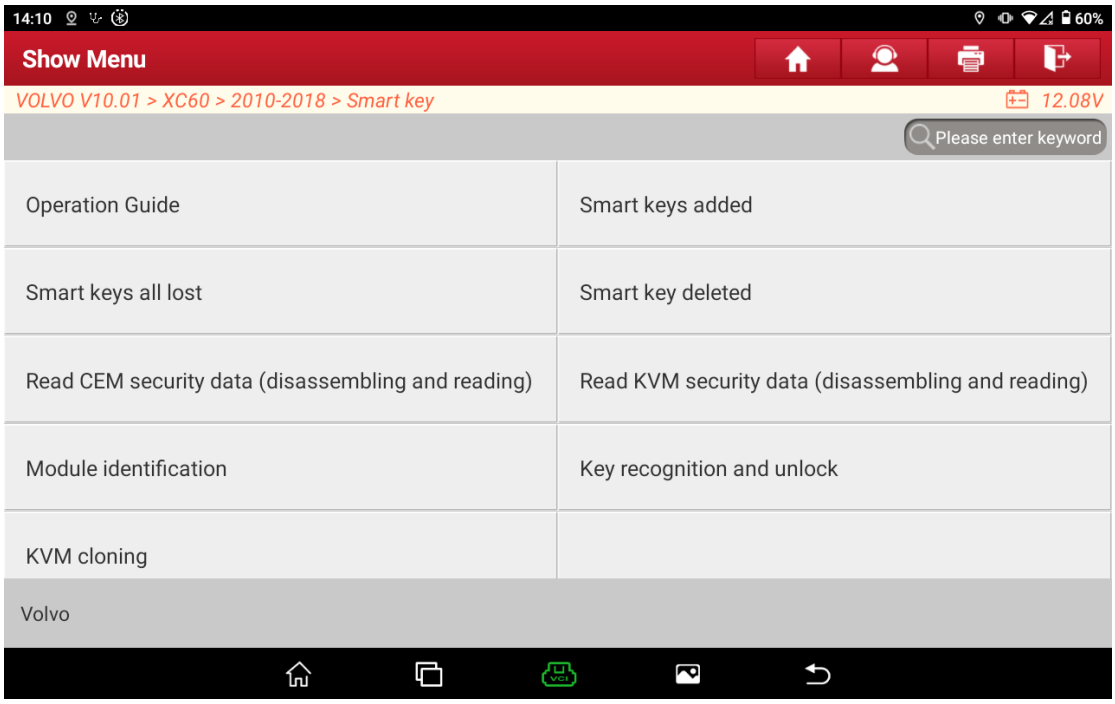


Figure 8

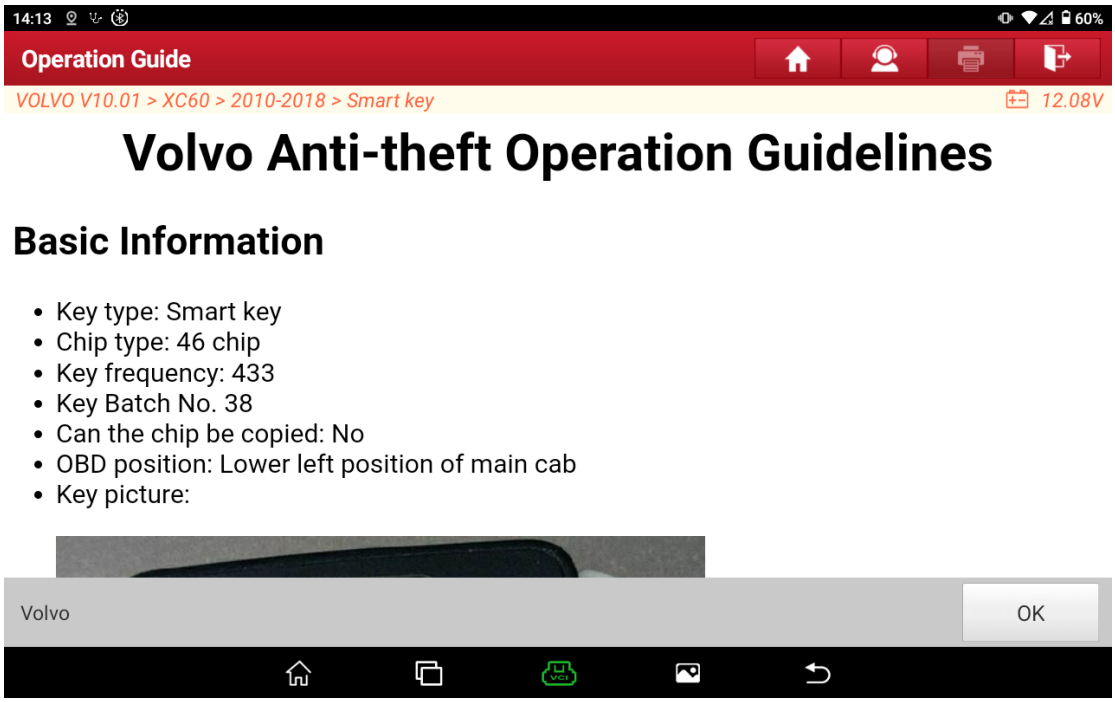


Figure 9

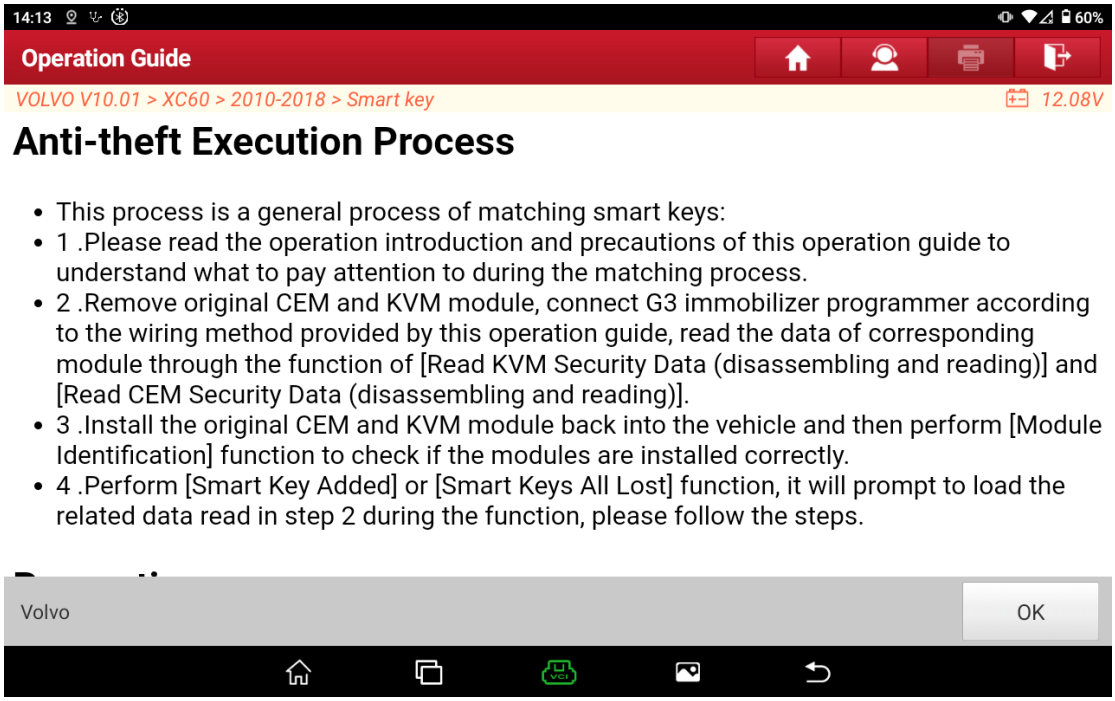


Figure 10

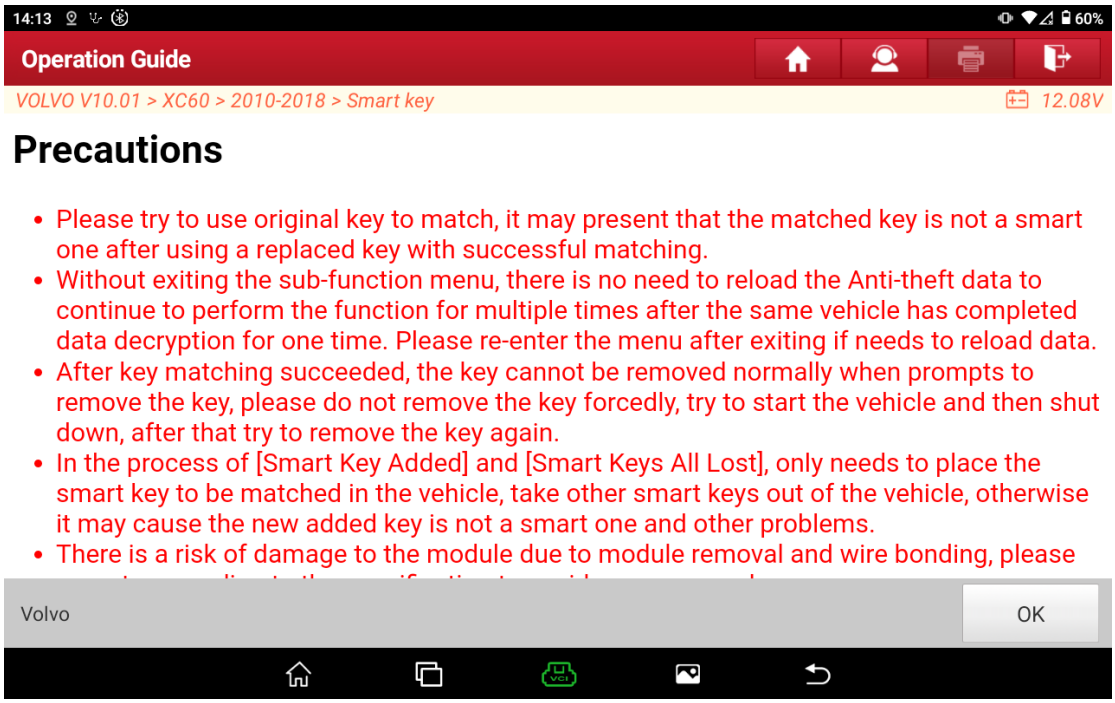


Figure 11

3. [Read KVM security data (disassembling and reading)]

After reading the operation document of the function of [Operation Guide], the MCU Cable V1 harness of the G3 programmer should be used to connect the disassembled vehicle module, and then the MCU V2 adapter should be used to connect the G3

programmer to the vehicle module. Finally, the function [Read KVM security data (disassembling and reading)] should be selected to read the anti-theft data of the vehicle module. (The module location and connection method are detailed in the [Operation Guide], which will not be detailed in this document. The procedure is as follows.)

1) The connection diagram is as follows:

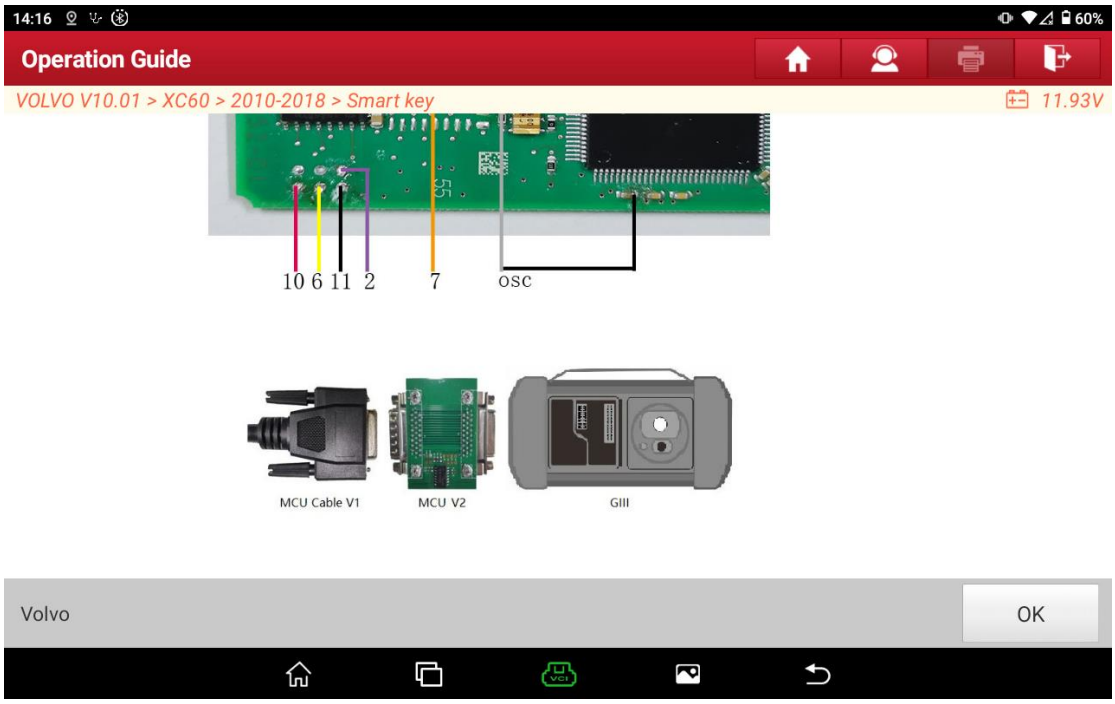


Figure 12

2) Select [Read KVM security data (disassembling and reading)] function

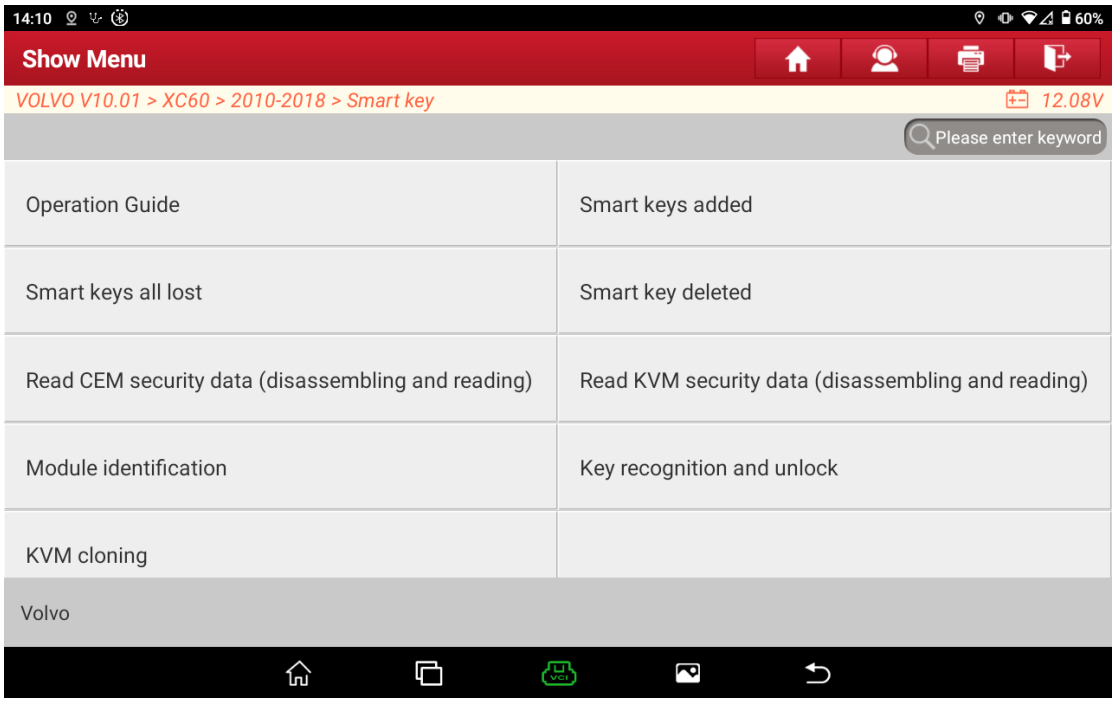


Figure 13

3) Prompt to view the [Operation Guide] function and click [YES] to proceed to the next step.

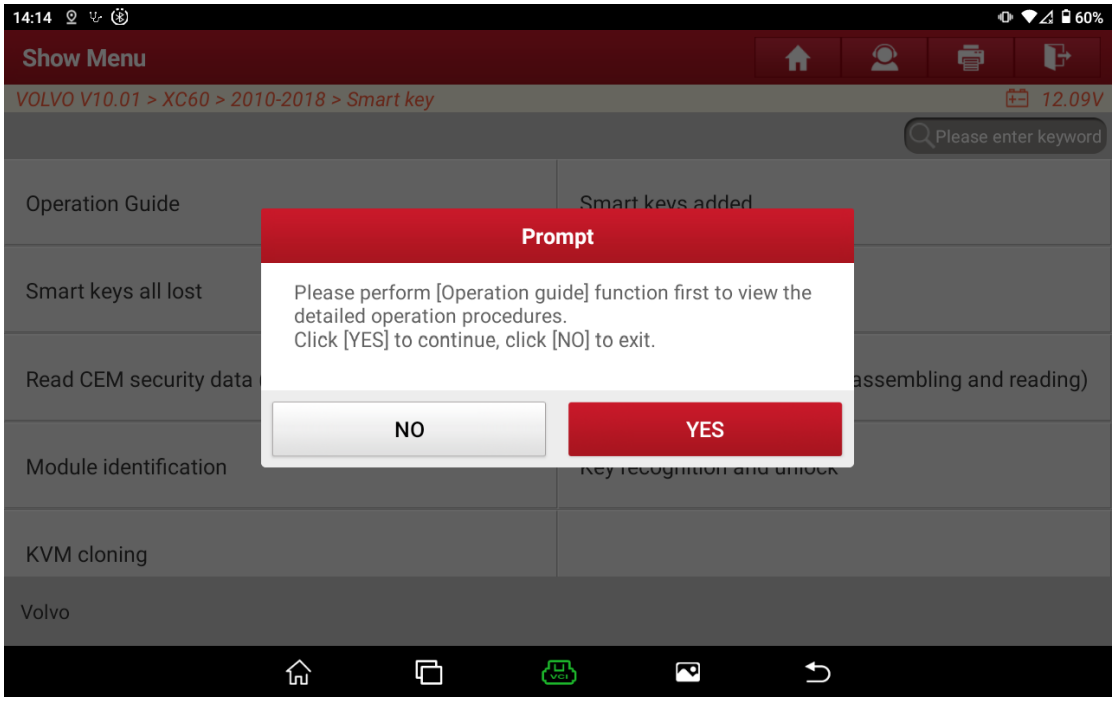


Figure 14

4) **Connect G3 programmer. Connect anti-theft device, programmer and vehicle module according to [Operation guide]. Click [Yes] to proceed to the next step.**

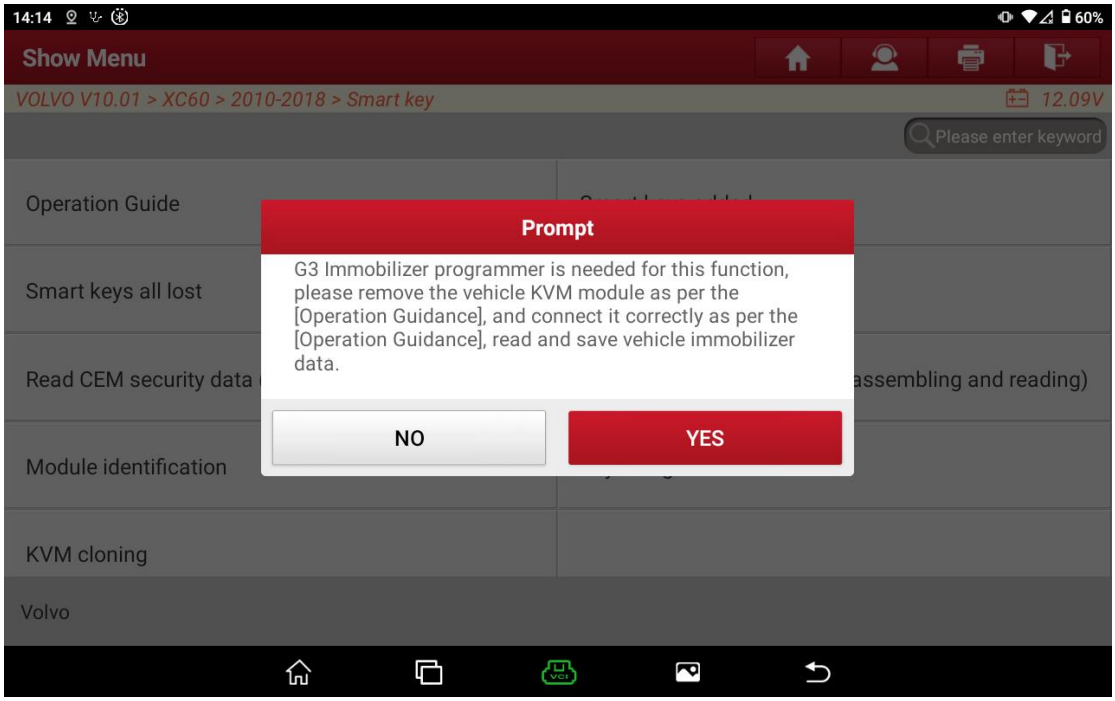


Figure 15

5) **It is indicated that anti-theft data is being read. The reading time is about 1 minute, during which no operation is required. Do not move the device to avoid data reading failure.**

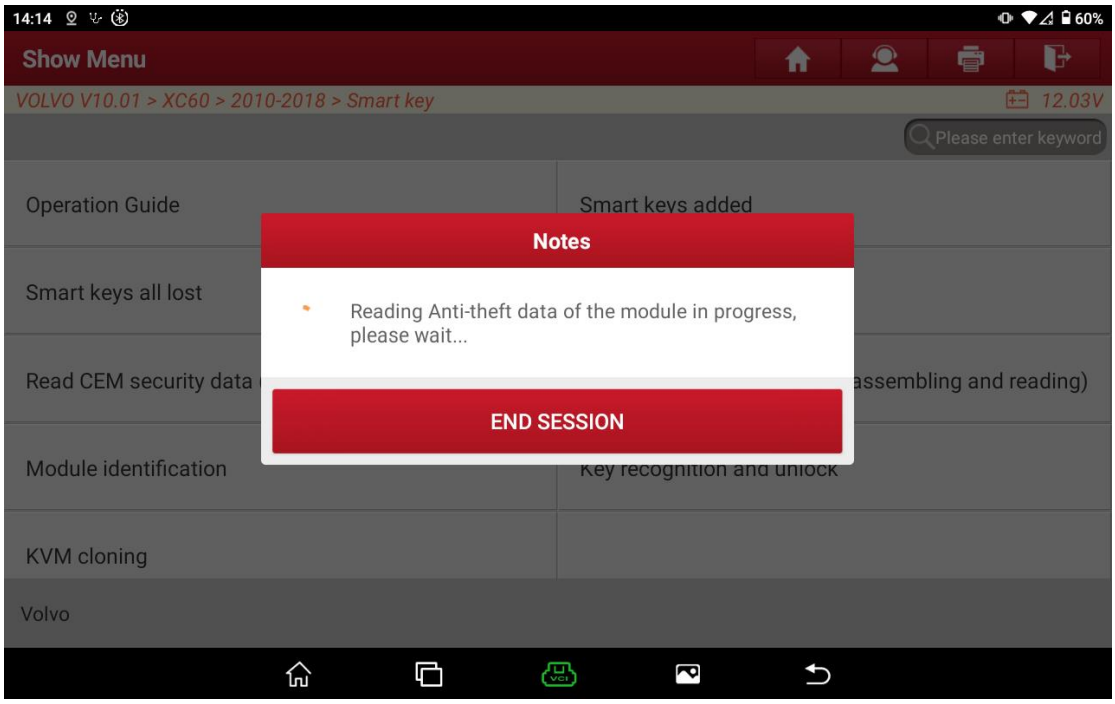


Figure 16

6) **After the anti-theft data is read successfully, it is prompted that the data is read successfully and the data is saved. After the successful saving, the function execution is completed.**

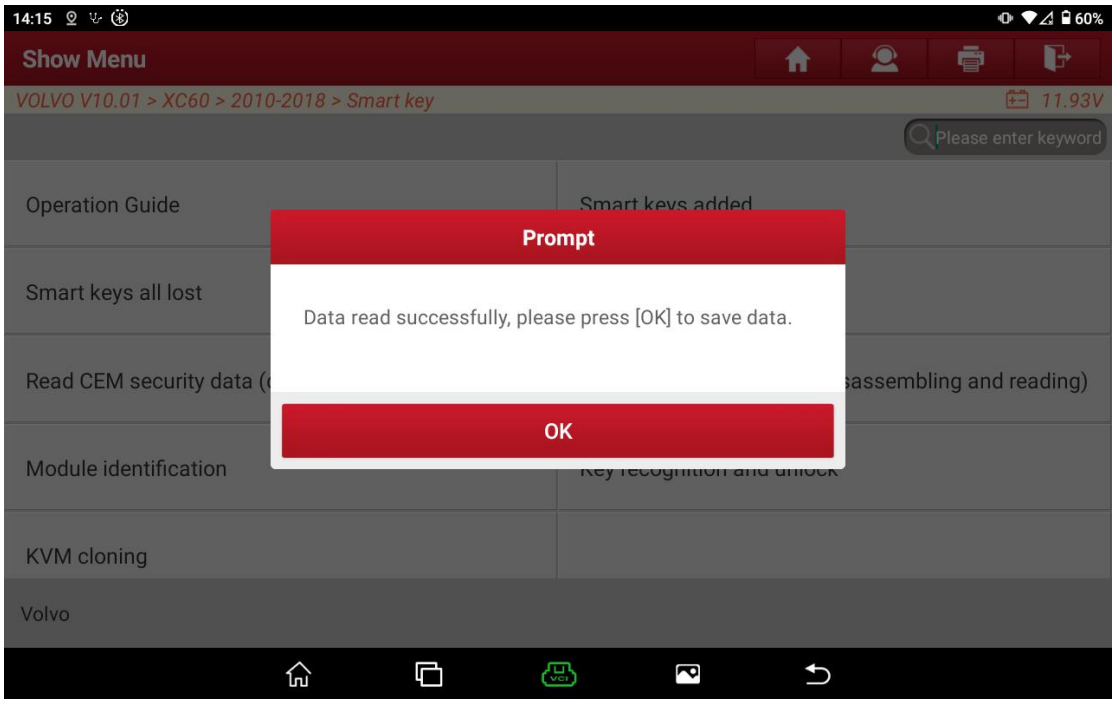


Figure 17

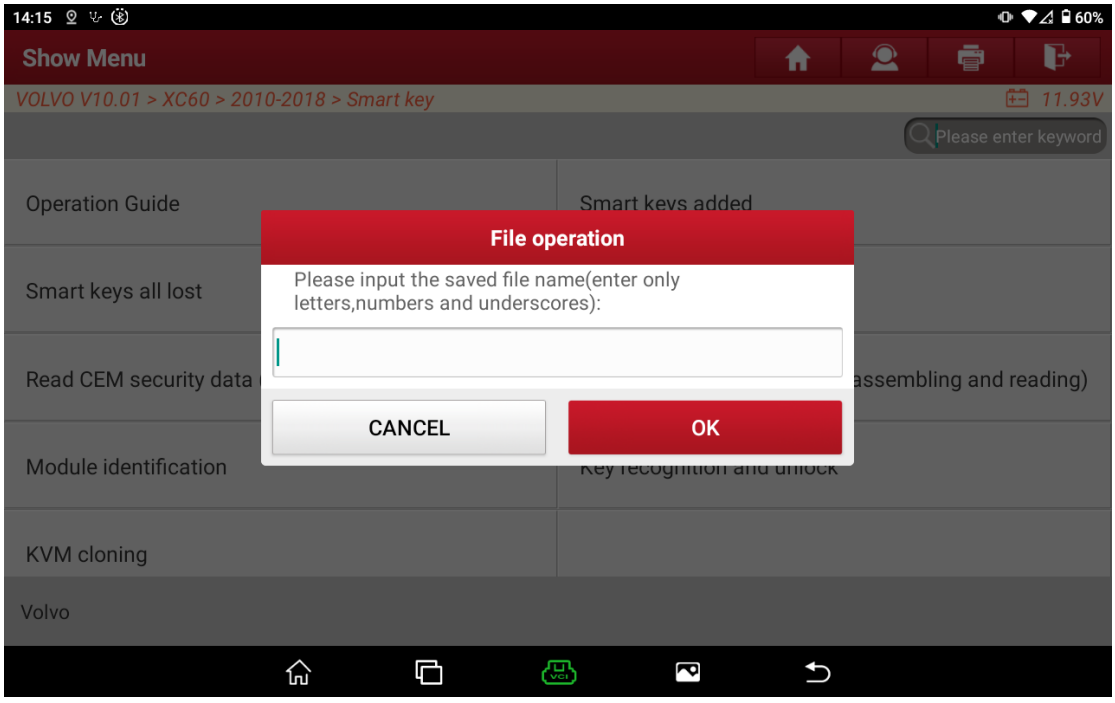


Figure 18

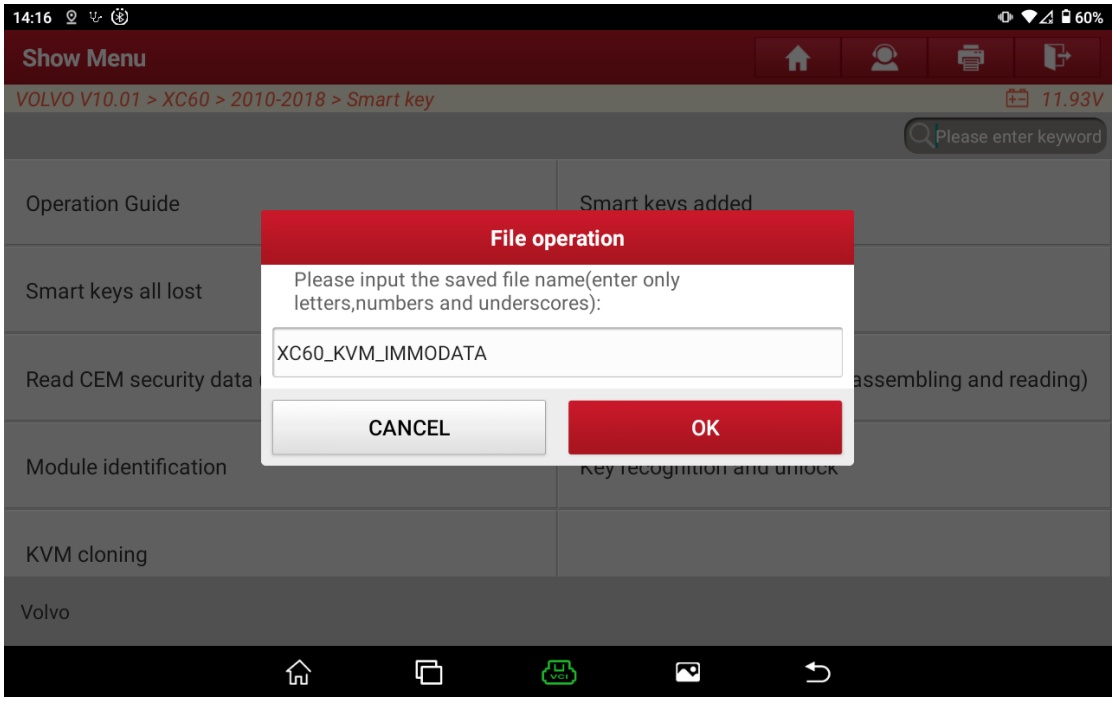


Figure 19

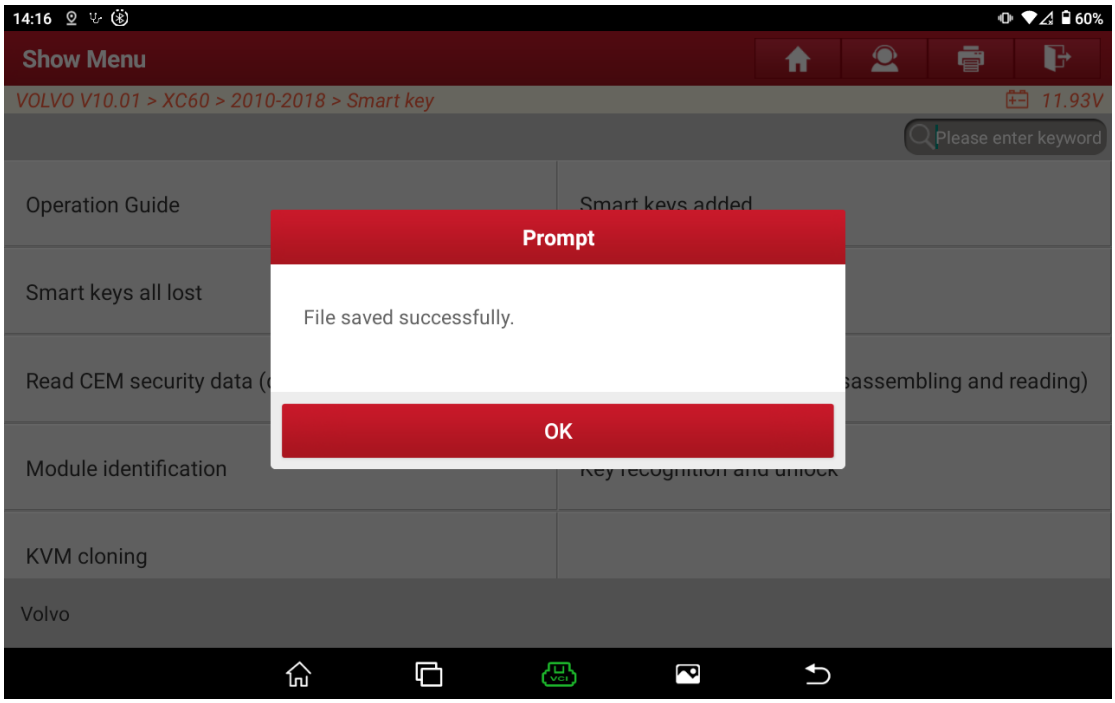


Figure 20

4. [Read CEM security data (disassembling and reading)]

By reading the operation document of the function of [Operation Guidance], the MCU Cable V1 harness of G3 programmer should be used to connect the disassembled vehicle module, and then the MCU V2 adapter should be used to connect the G3 programmer to the vehicle module. Finally, the function [Read CEM

security data (disassembling and reading)] should be selected to read the anti-theft data of the vehicle module. (The module location and cable connection are detailed in the [Operation Guide]. This document will not describe this part in detail. The procedure is as follows)

1) The connection diagram is as follows:

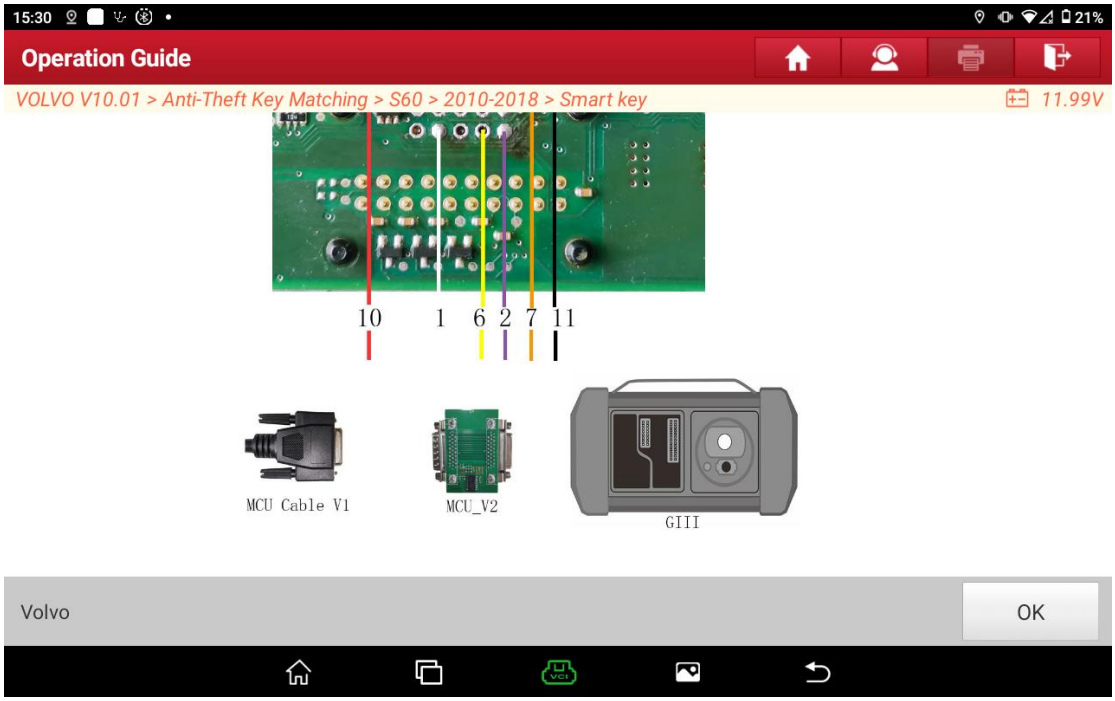


Figure 21

2) Select [Read CEM security data (disassembling and reading)] function

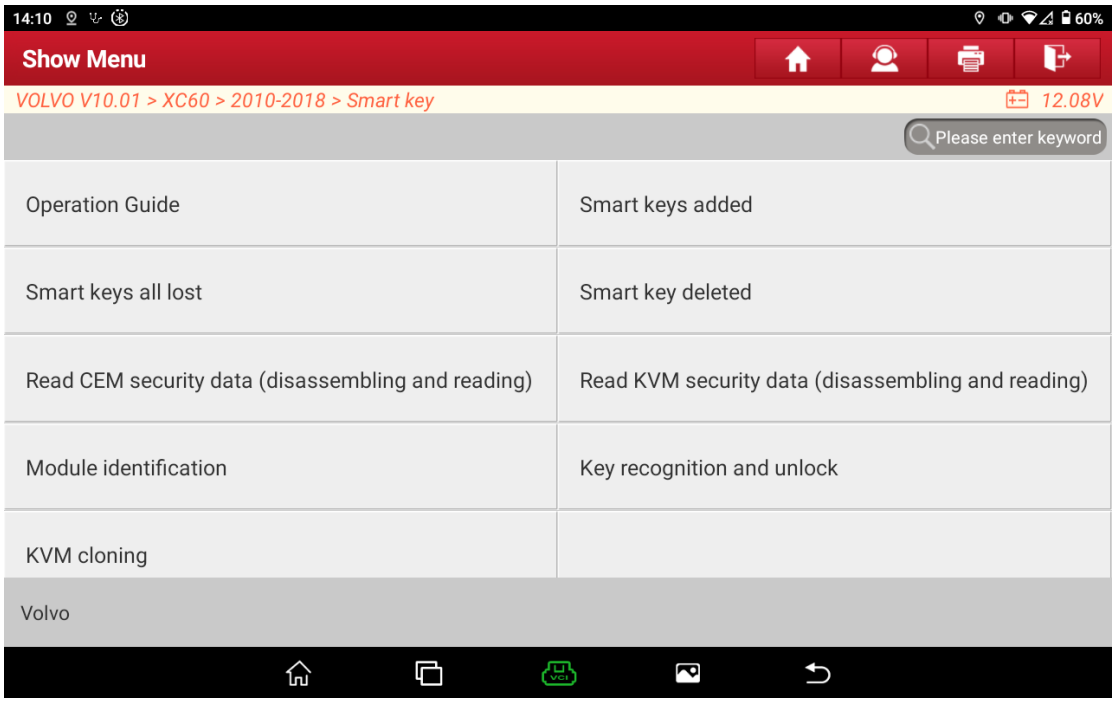


Figure 22

3) Prompt to view [Operation guide] function, click [YES] to proceed to the next step.

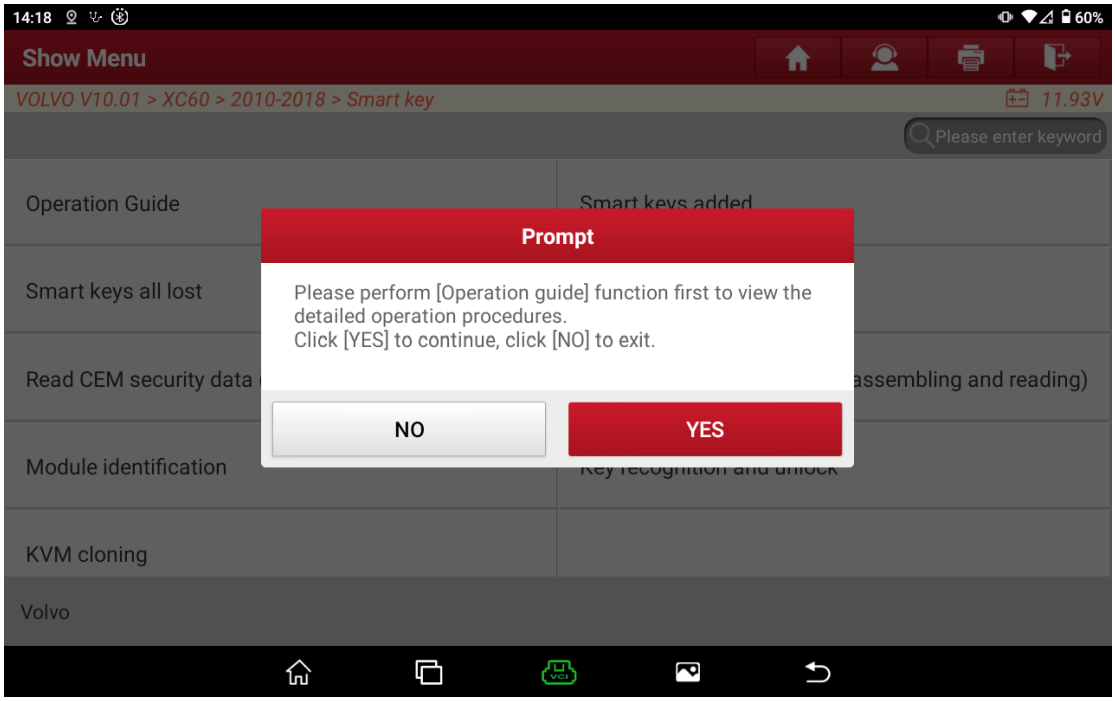


Figure 23

4) **Connect G3 programmer, connect anti-theft device, programmer and vehicle module according to [Operation Guide], and click [YES] to go to the next step.**

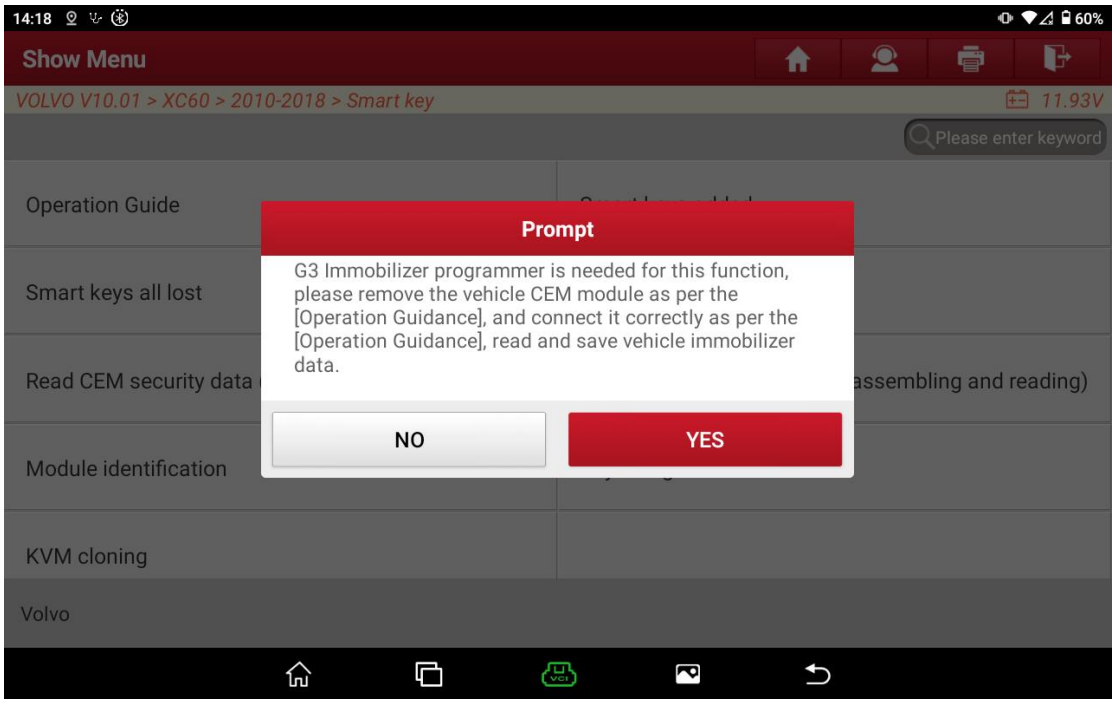


Figure 24

5) **It is suggested that anti-theft data is being read, and the reading time is about 1-2 minutes. During this period, no operation is required. Do not move the device to avoid data reading failure.**

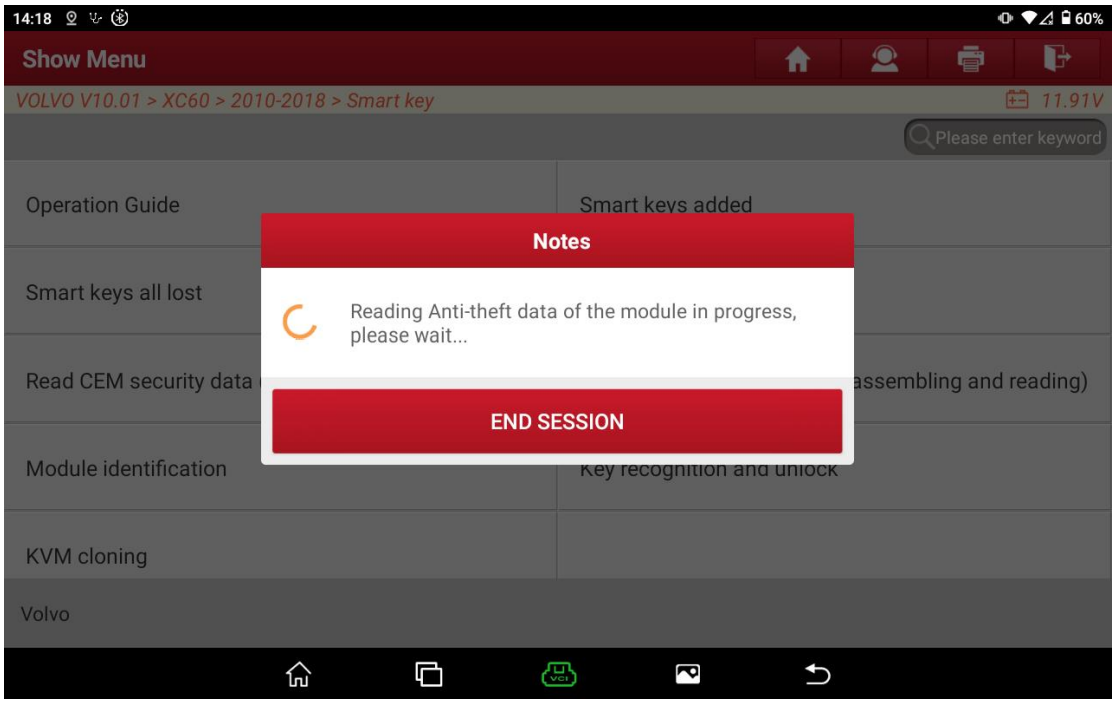


Figure 25

6) **After the anti-theft data is read successfully, it is prompted that the data is read successfully and the data is saved. After the successful saving, the function execution is completed.**

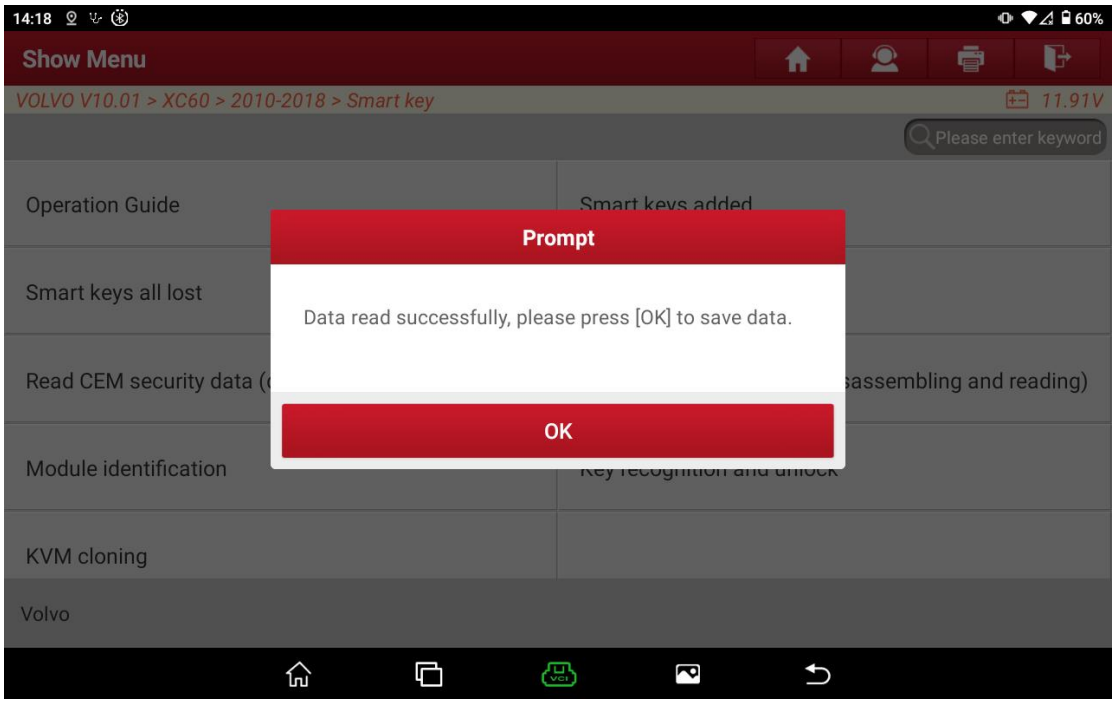


Figure 26

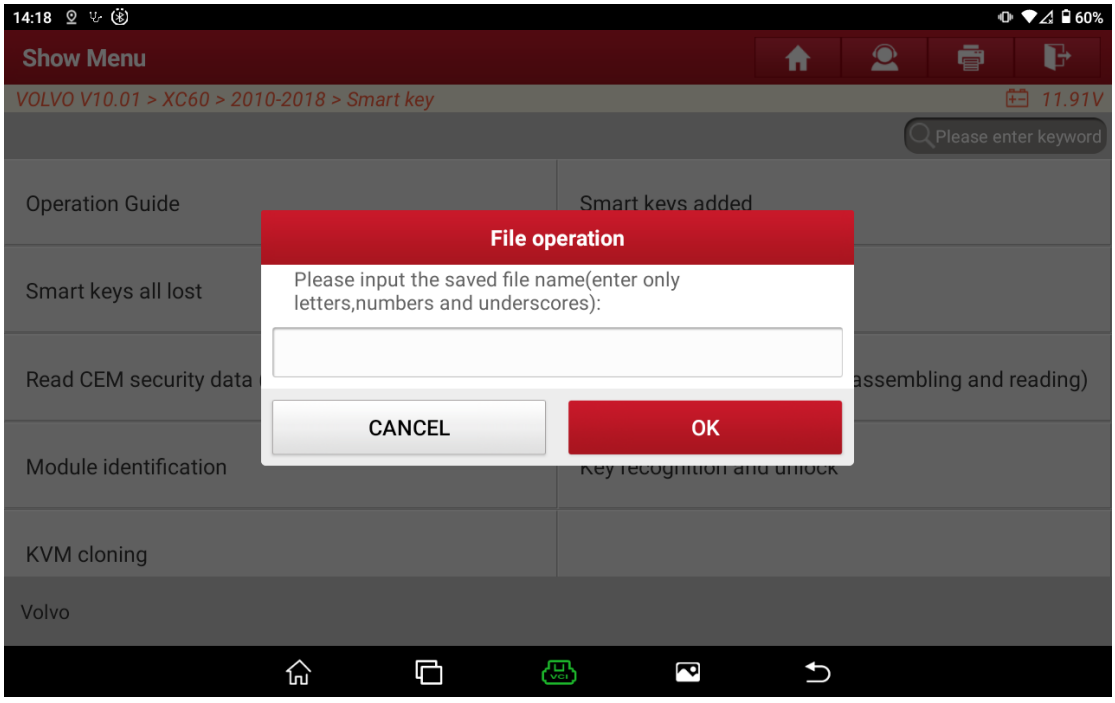


Figure 27

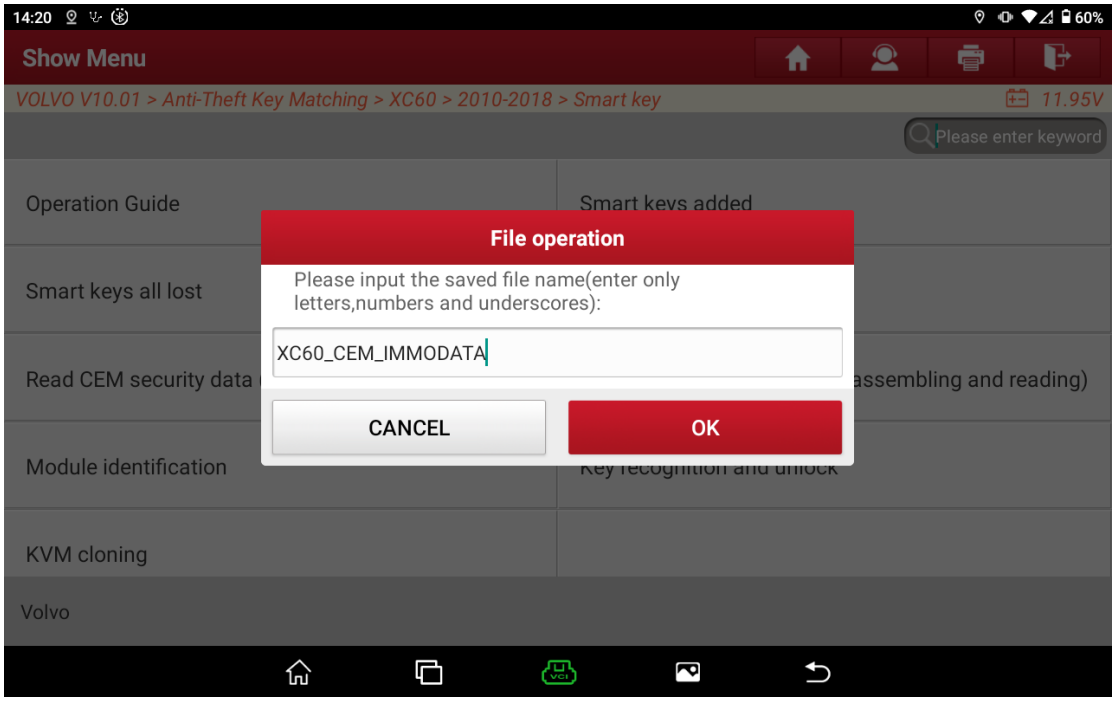


Figure 28

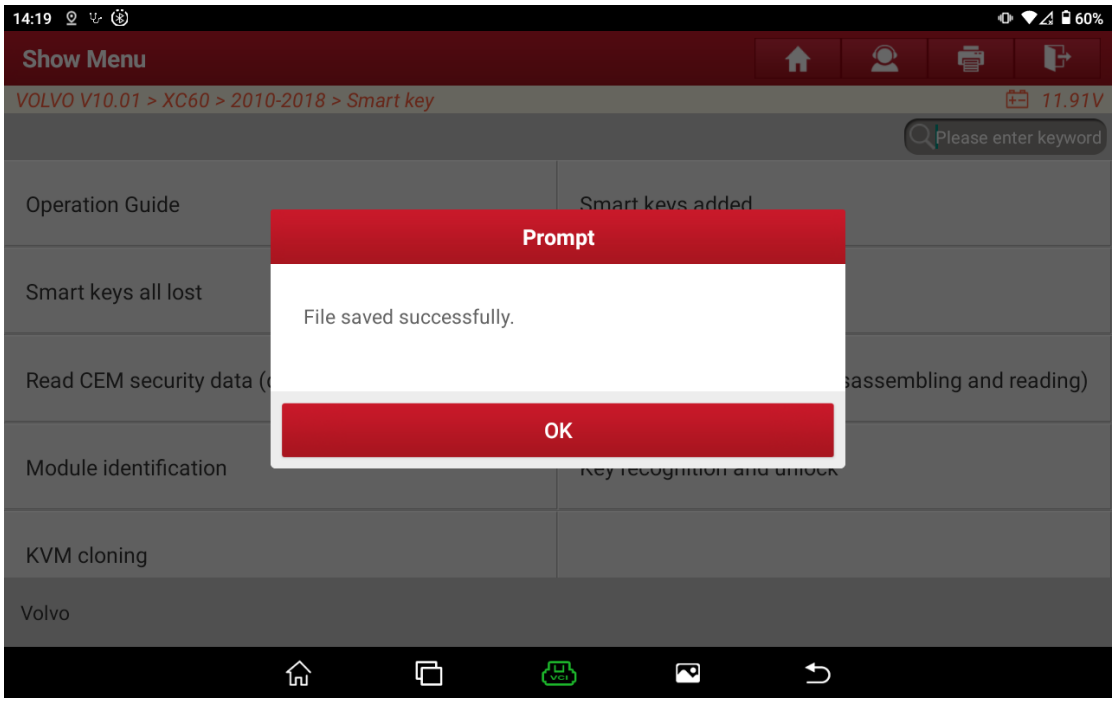


Figure 29

5. [Smart keys added]

The [Smart keys added] function is used to add keys to the vehicle without deleting the original car keys. The [Smart keys all lost] function is used to add keys to the vehicle after deleting all the original car keys. After deleting the original car keys, the original car keys need

to be re-matched before they can be used again. The [Smart key deleted] function is used to delete all the original car keys. Please select a function based on actual requirements. This document takes [Smart keys added] as an example:

1) Select [Smart keys added] function, it's prompted to view the [Operation guide] function and click [YES] to perform the next step.

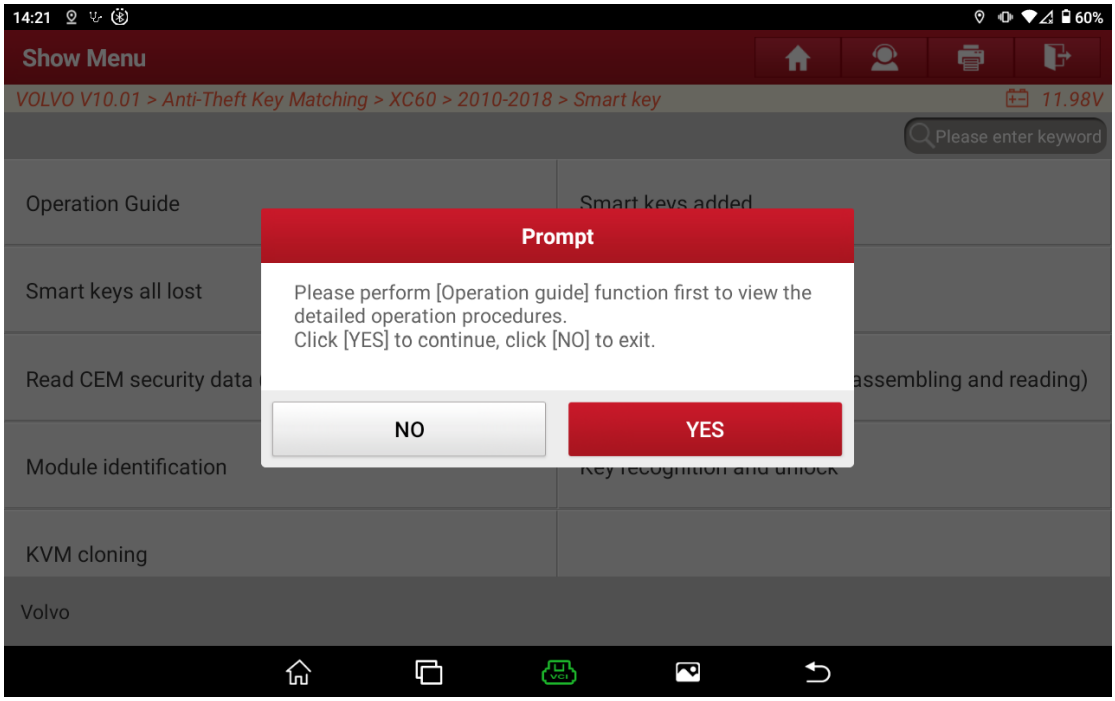


Figure 30

2) **After completing the action 'Press the START button', click [OK] to perform the next step.**

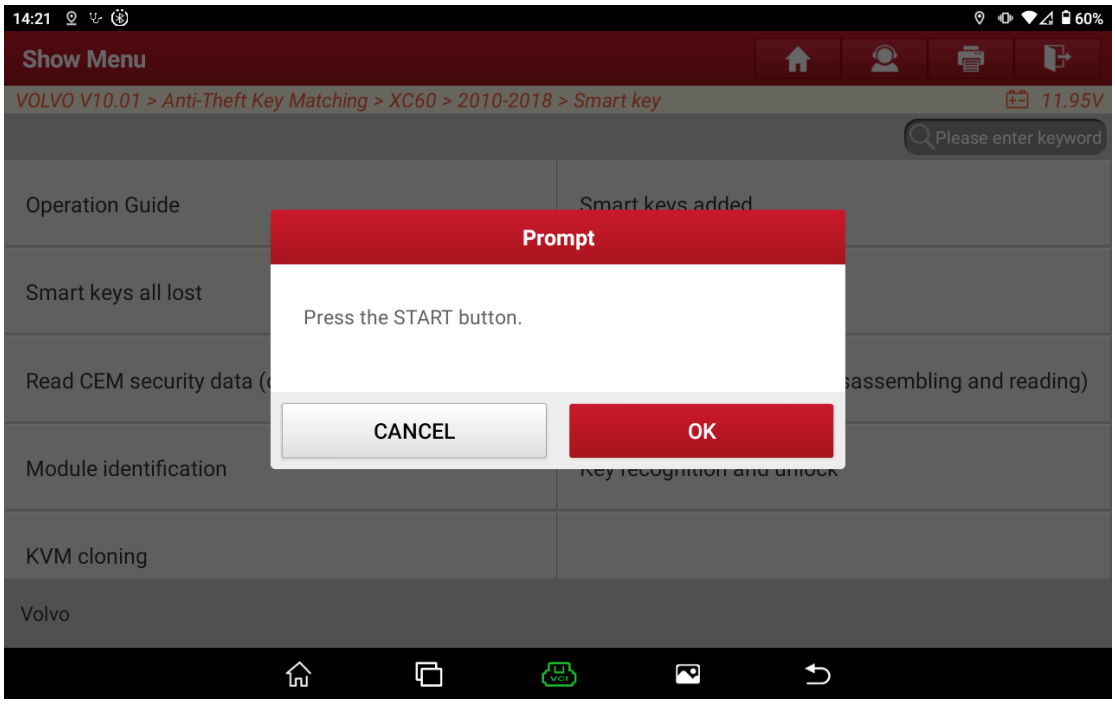


Figure 31

3) **It's prompted to load CEM security data, click [OK] to load the anti-theft data.**

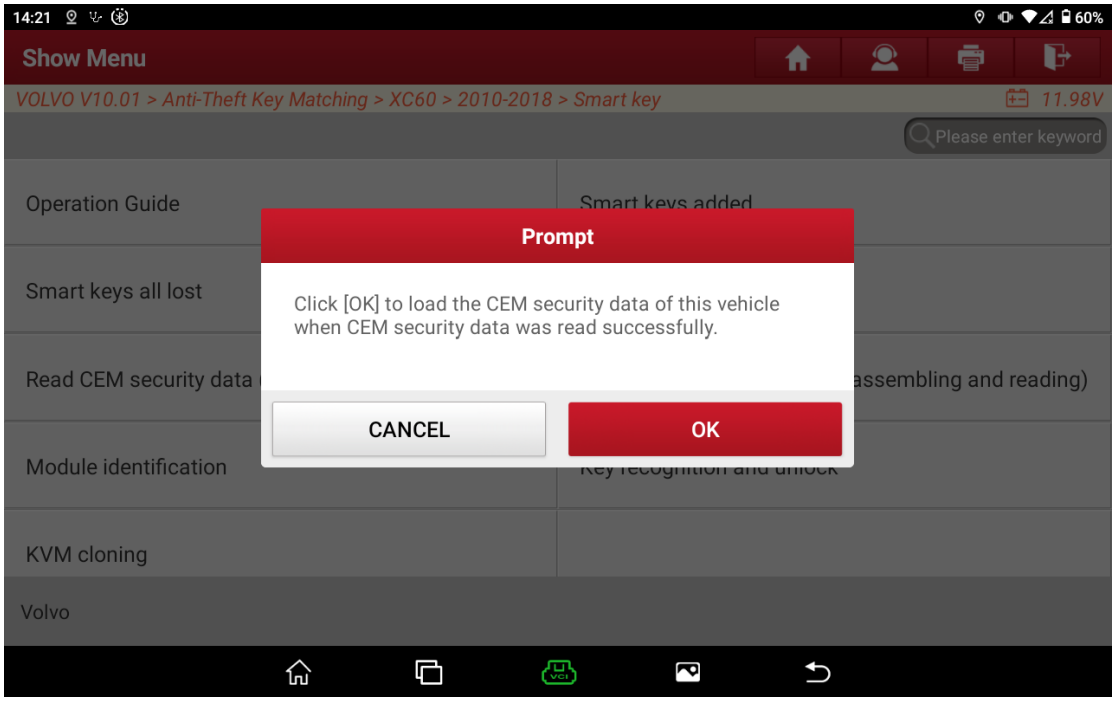


Figure 32

4) Select the read data file, here we select file XC60_CEM_IMMODATA.bin.

Figure 33

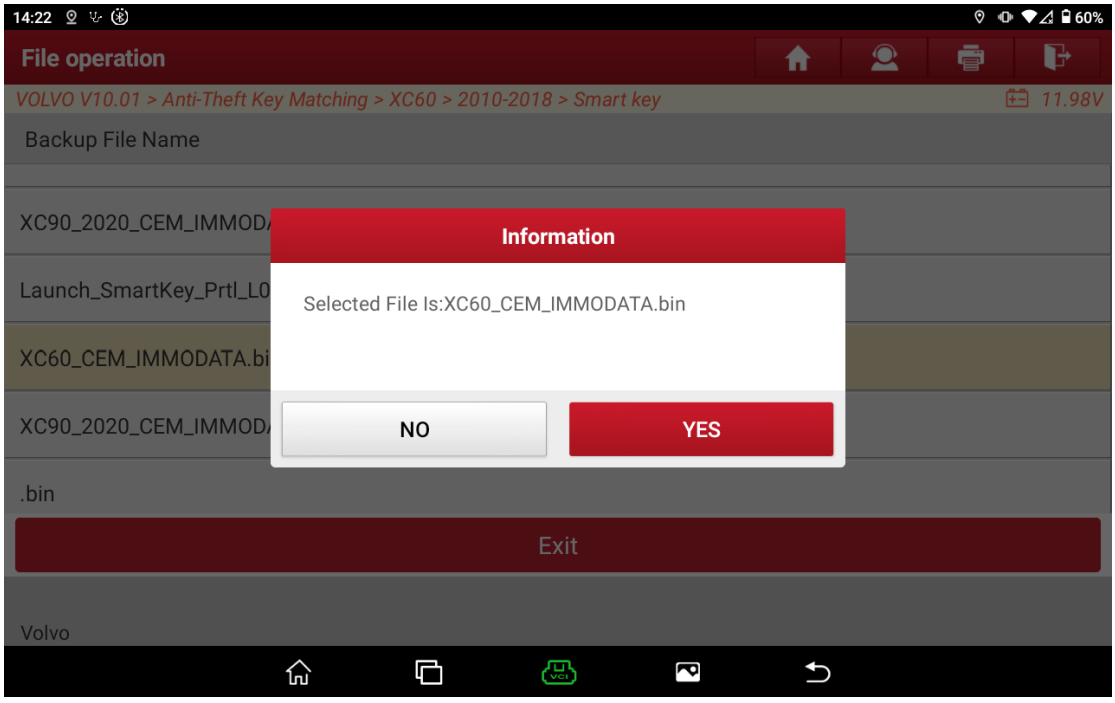


Figure 34

5) **It's prompted to load KVM security data, click [OK] to load the anti-theft data.**

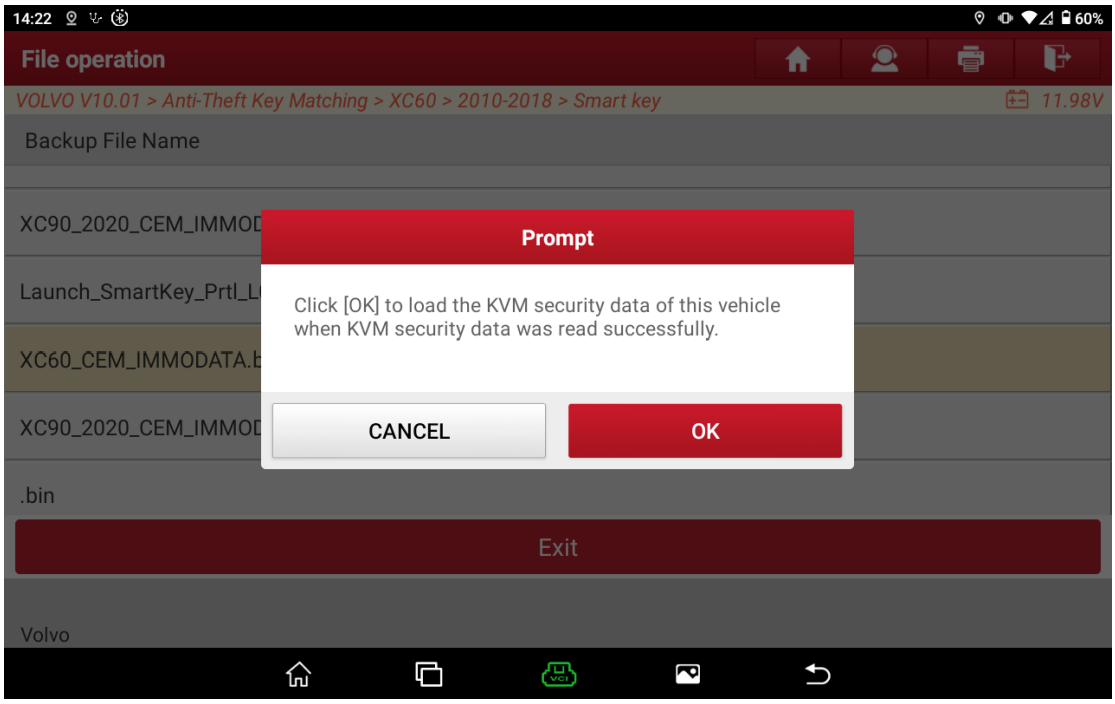


Figure 35

6) **Select the read data file, here we select file XC60_KVM_IMMODATA.bin.**

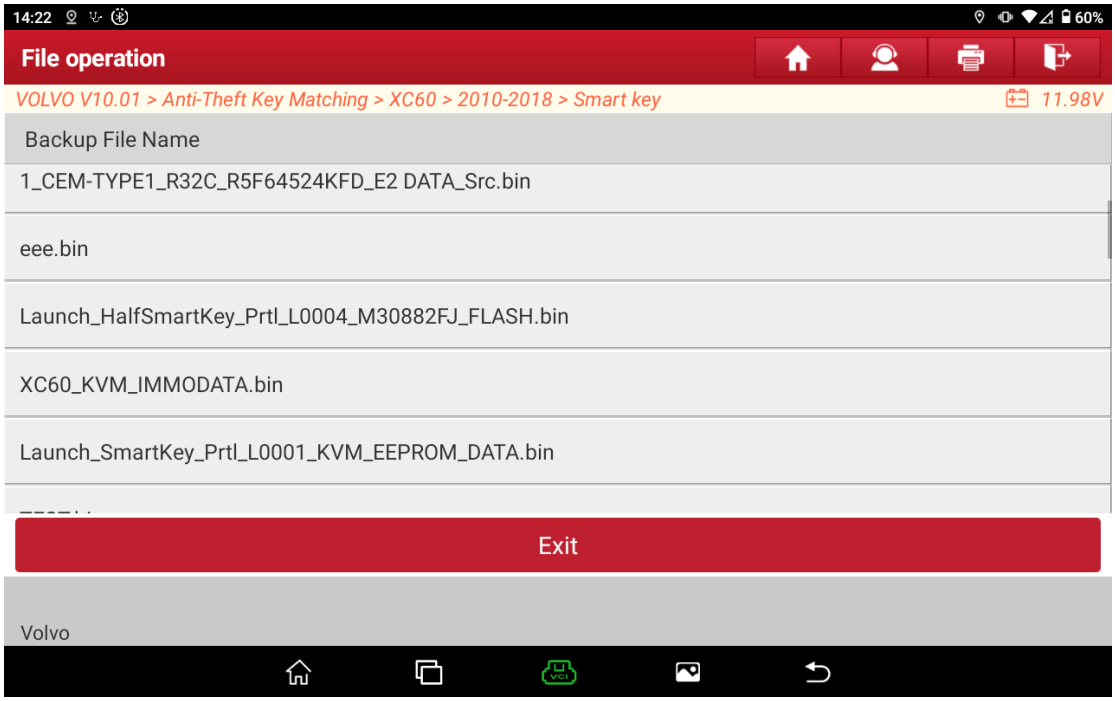


Figure 36

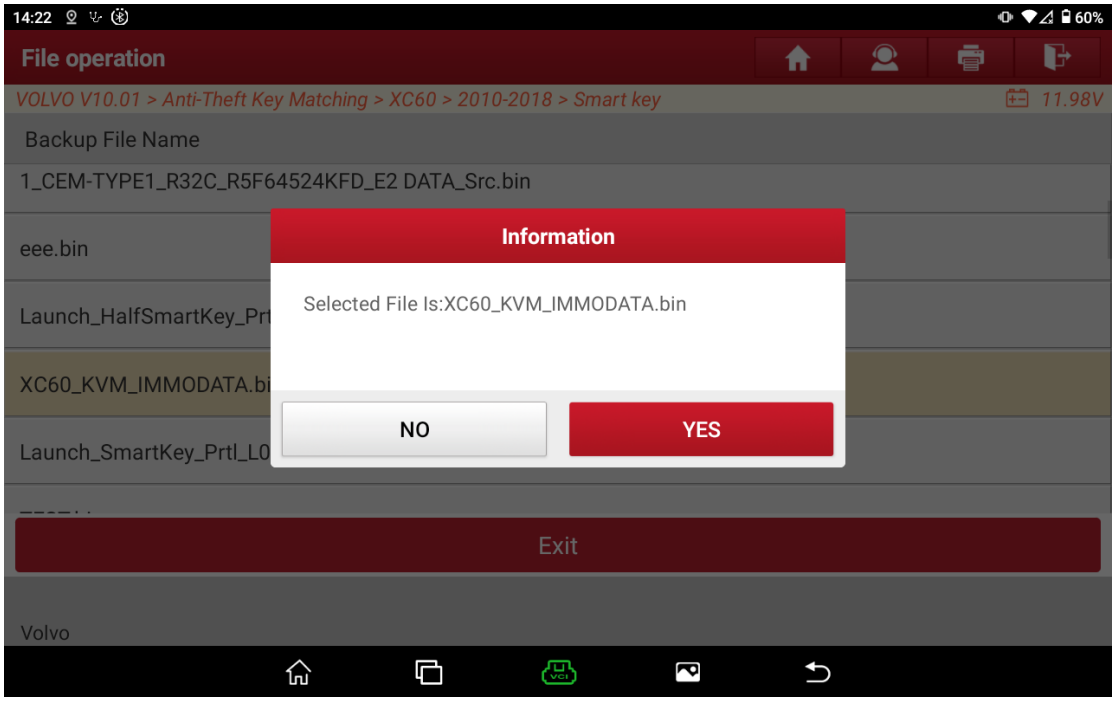


Figure 37

7) Confirm the key is correct and then click [YES] to perform the next step.

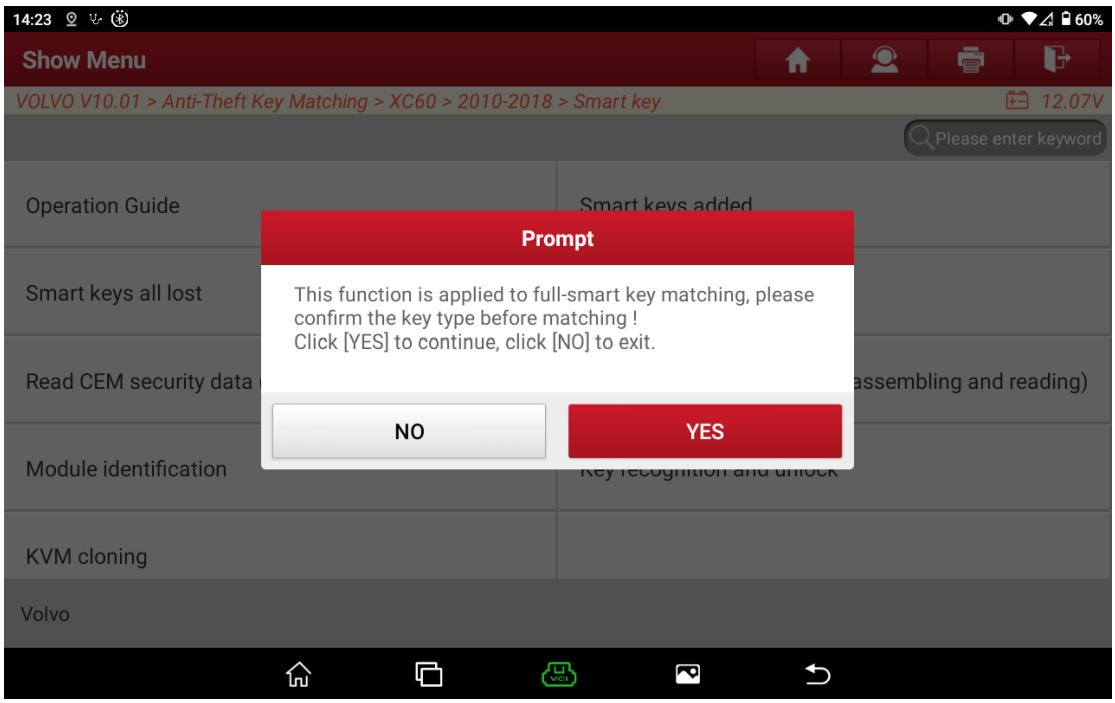


Figure 38

8) Turn off the ignition switch and click [OK] to perform the next step.

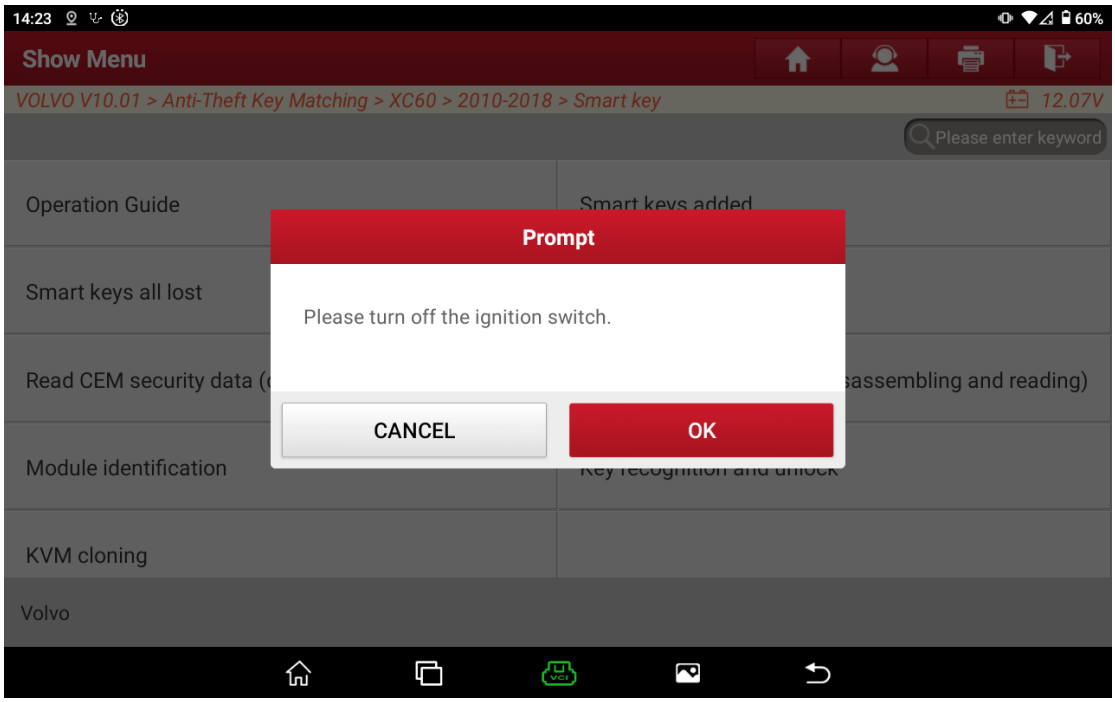


Figure 39

9) Confirm the number of keys and then click [OK] to perform the next step.

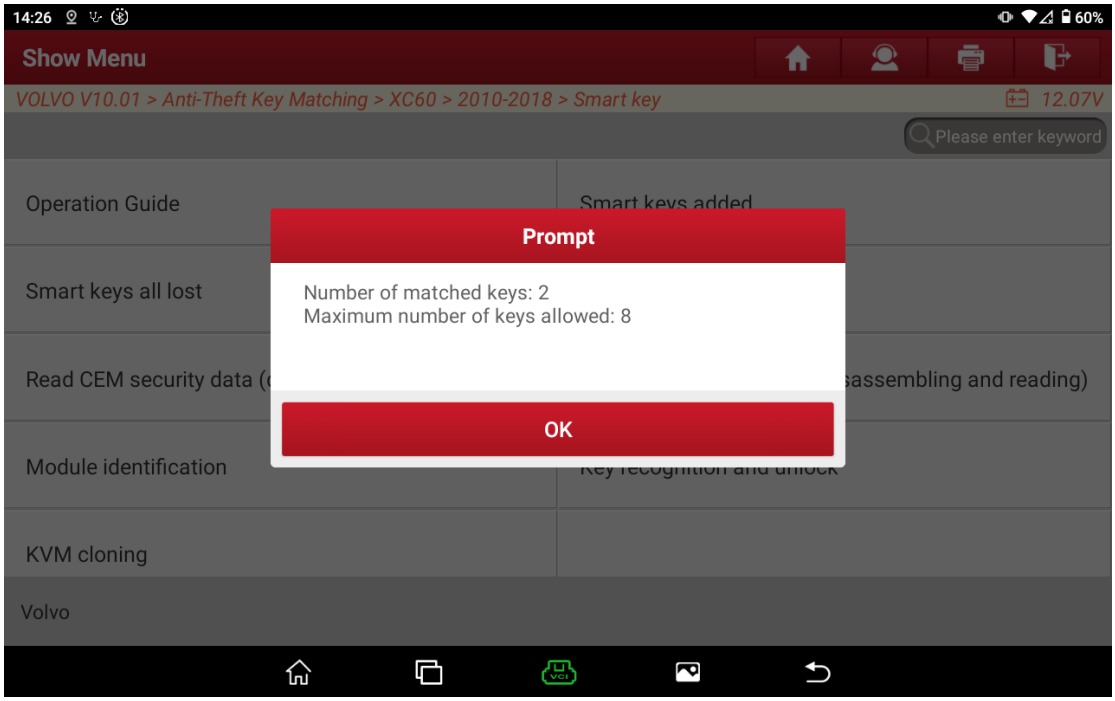


Figure 40

10) Insert the key into the card slot according to the prompts, select subsequent operations according to whether the key will be ejected. Click [CANCEL] to perform the next step when the key is ejected, click [OK] to perform the next step when the key is not ejected (generally ejected key is a rare case).

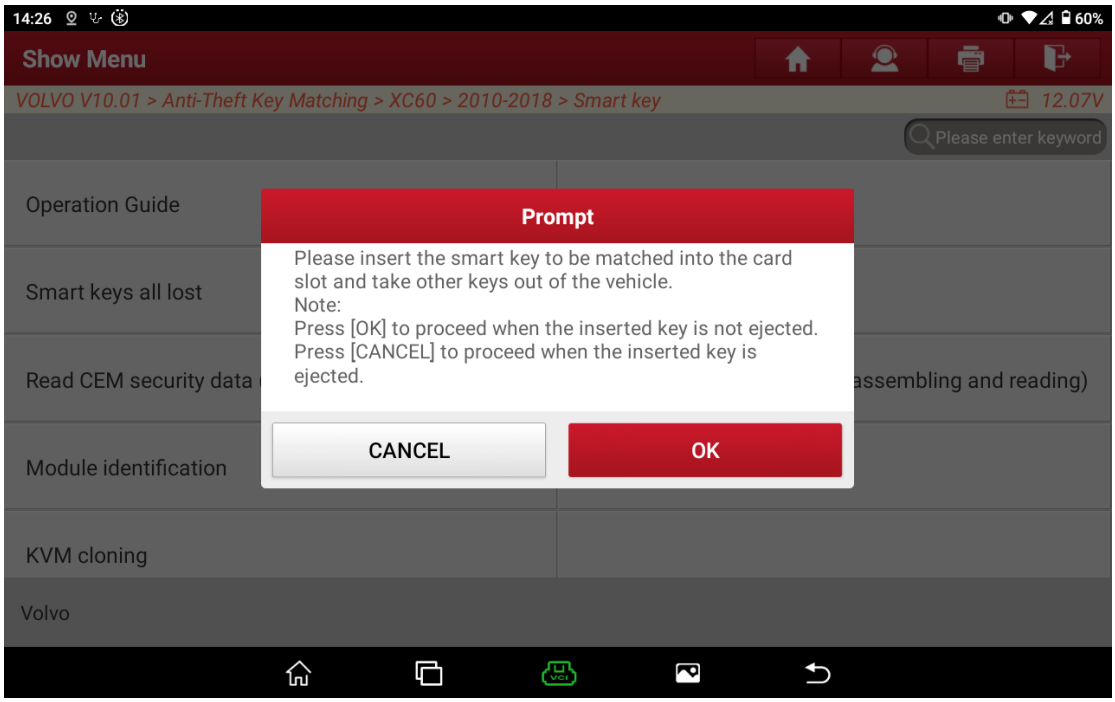


Figure 41

11) According to the prompts, click [OK] to complete the matching.

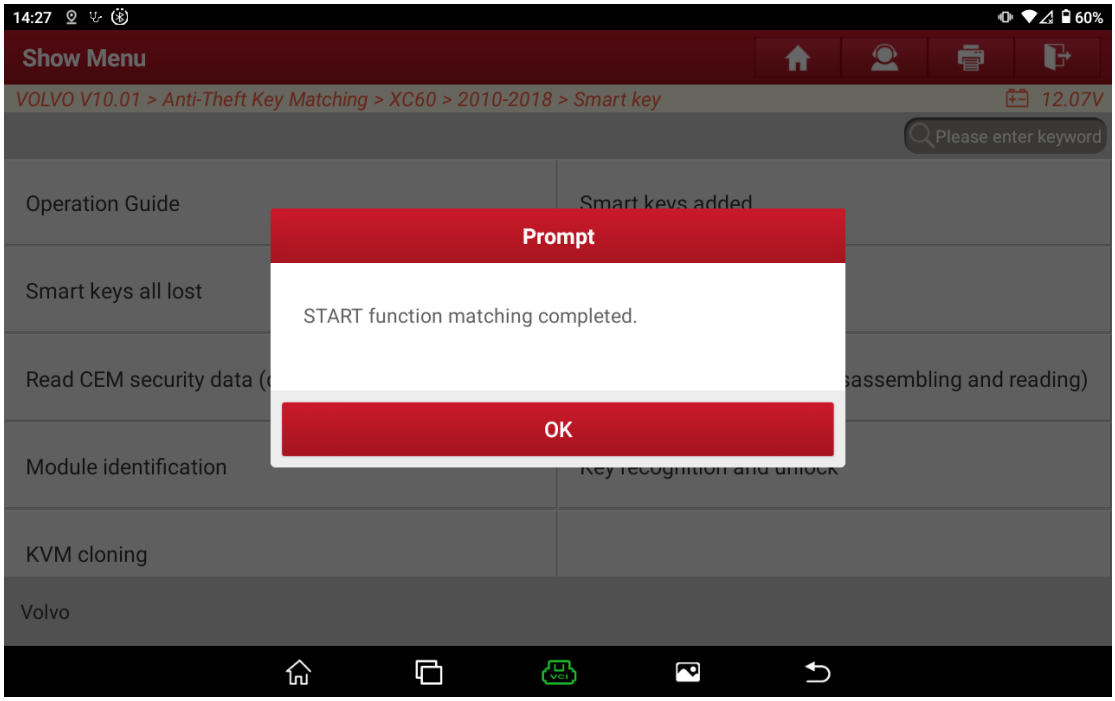


Figure 42

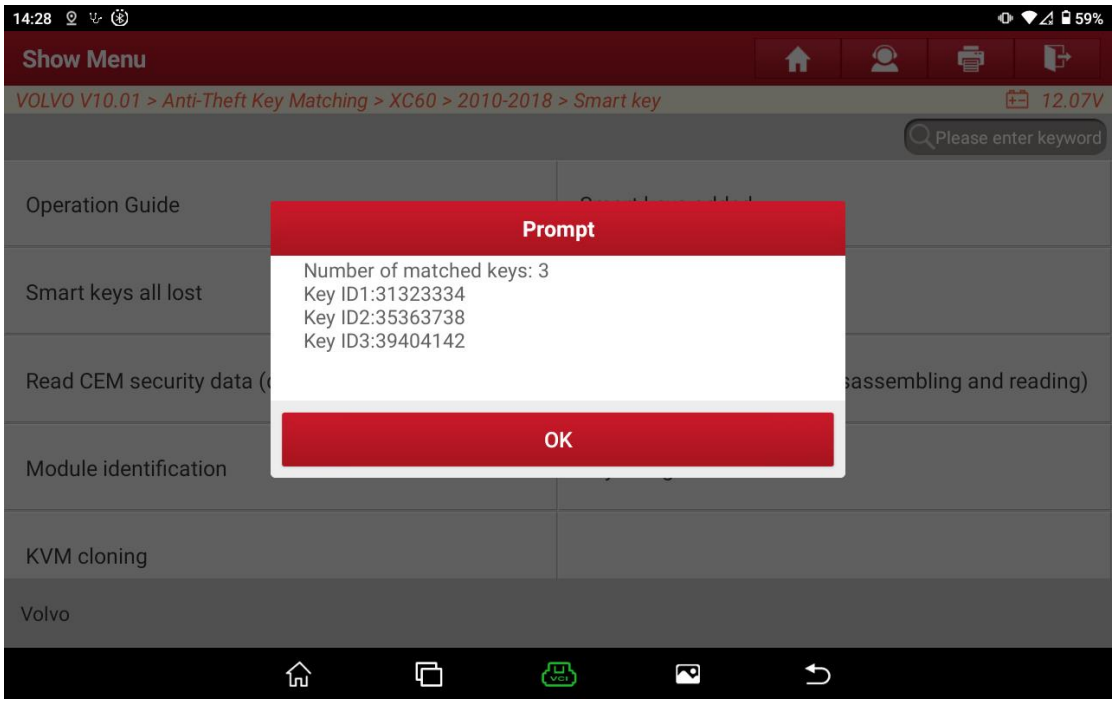


Figure 43

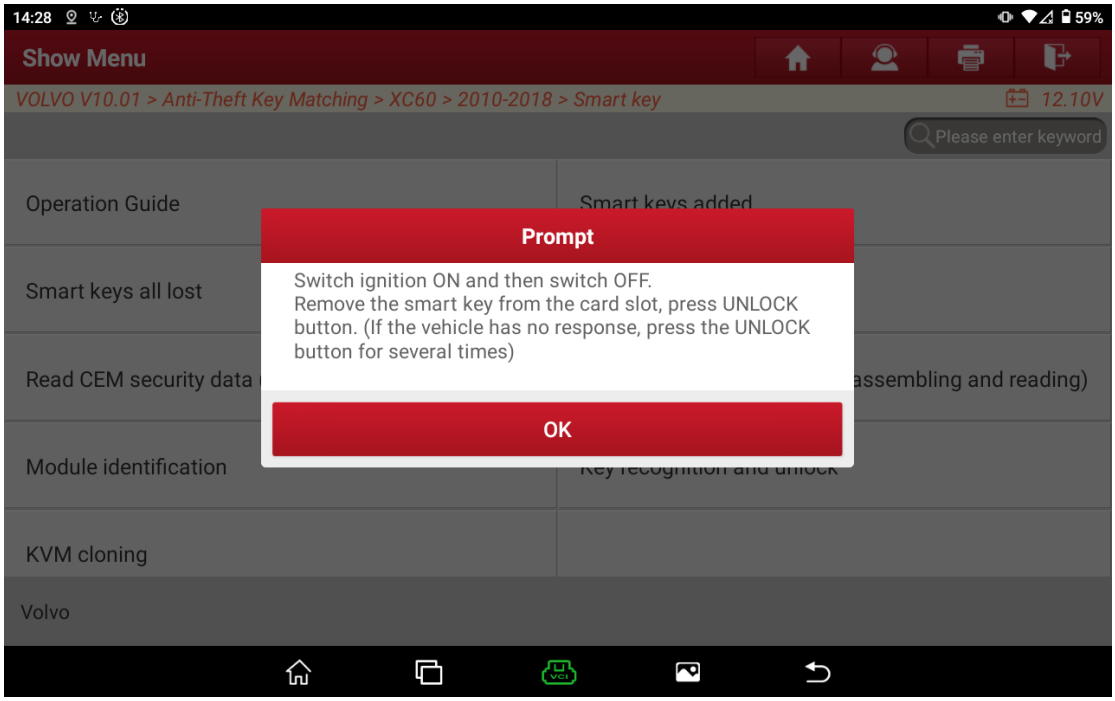


Figure 44

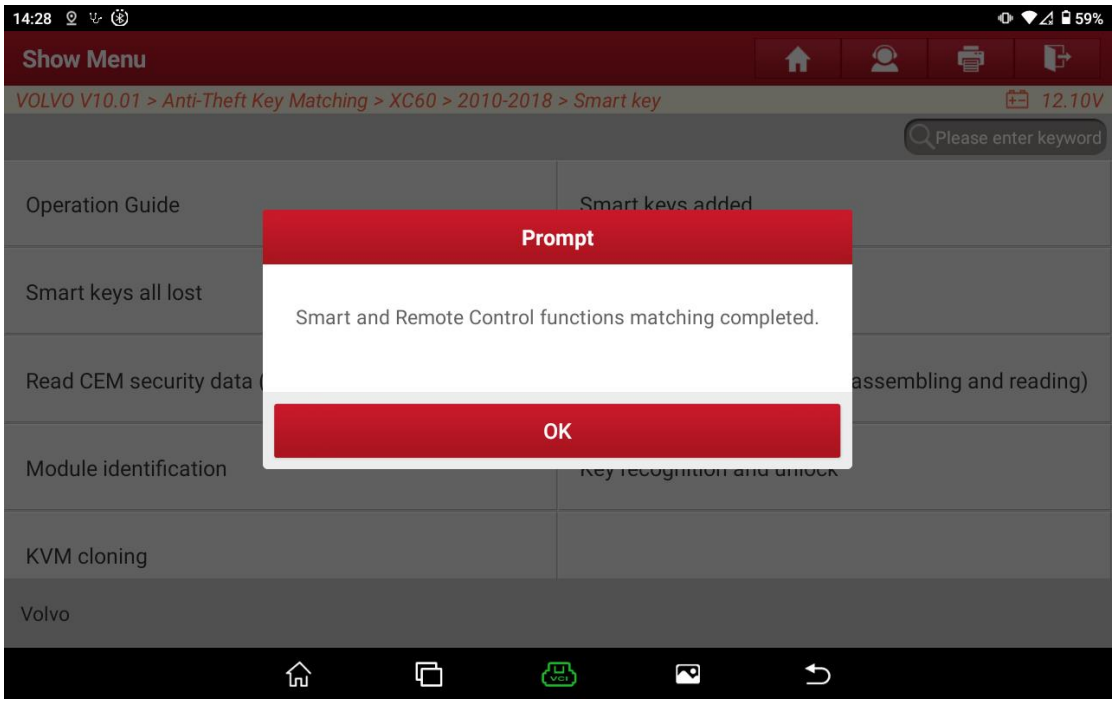


Figure 45

2020 年后防盗 Procedure

2.1Model Coverage：

Make	Vehicle	Year	Key Type
VOLVO	S60	2019-2021	Smart Key
VOLVO	S60 Hybrid	2018-2021	Smart Key
VOLVO	S90	2016-2021	Smart Key
VOLVO	S90 Hybrid	2019-2021	Smart Key
VOLVO	V60	2019-2021	Smart Key
VOLVO	V90	2017-2021	Smart Key
VOLVO	XC40	2018-2021	Smart Key
VOLVO	XC40 BEV	2021	Smart Key
VOLVO	XC60	2018-2021	Smart Key
VOLVO	XC60 Hybrid	2018-2021	Smart Key
VOLVO	XC90	2016-2021	Smart Key
VOLVO	XC90 Hybrid	2016-2021	Smart Key

2.2Requirements

1.Launch IMMO PRO/IMMO PAD (professional version)
2. As for the compliance smart keys used for anti-theft matching, it is recommended to use the original factory key, because some secondary factory keys may have no intelligence after matching.

2.3Procedure

This operation process demonstration takes Volvo 2020 XC90 smart key as an example.

Anti-theft operation process

This operation process demonstration takes Volvo 2020 XC90 smart key as an example.

1. Vehicle series entry

Select [Volvo] -> [Automatic Scan] -> [XC90] -> [2016-2021] -> [Smart key](See Figure 1, Figure 2, Figure 3, Figure 4, Figure 5, Figure 6 and Figure 7 for the process steps)

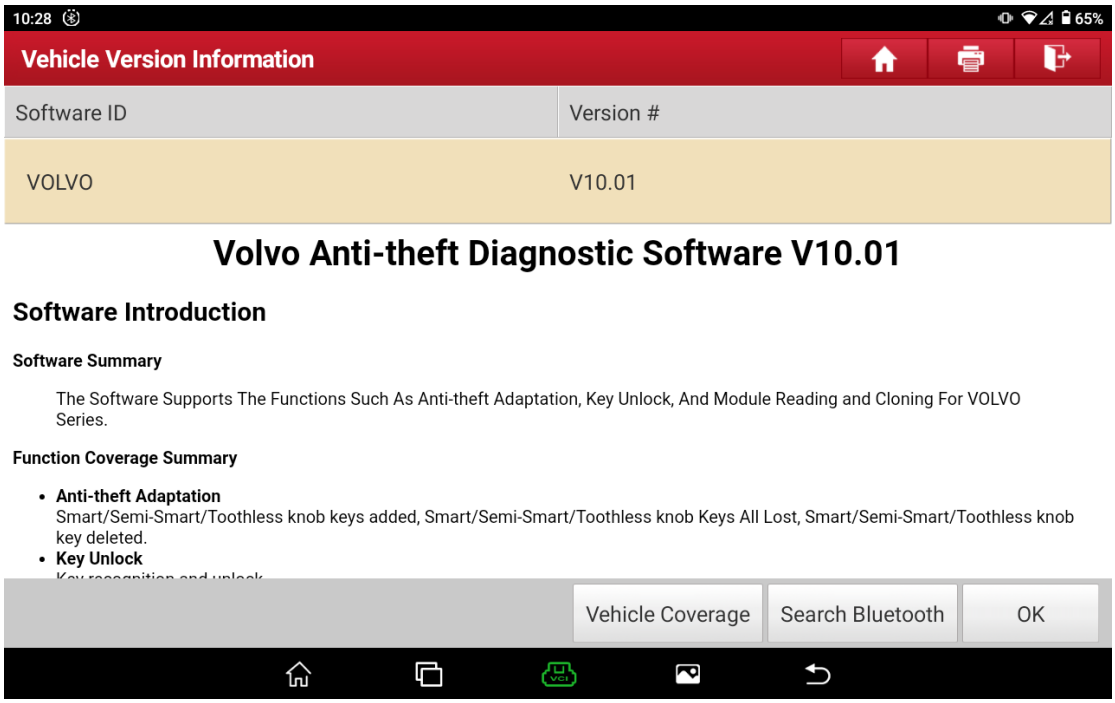


Figure 1

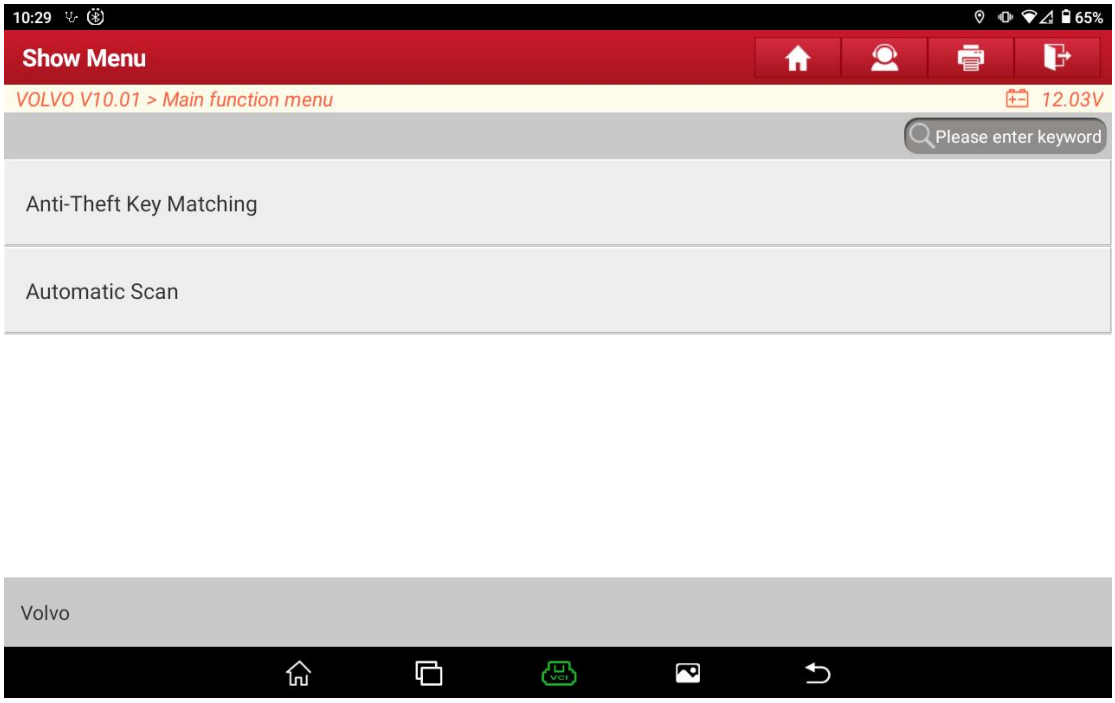


Figure 2

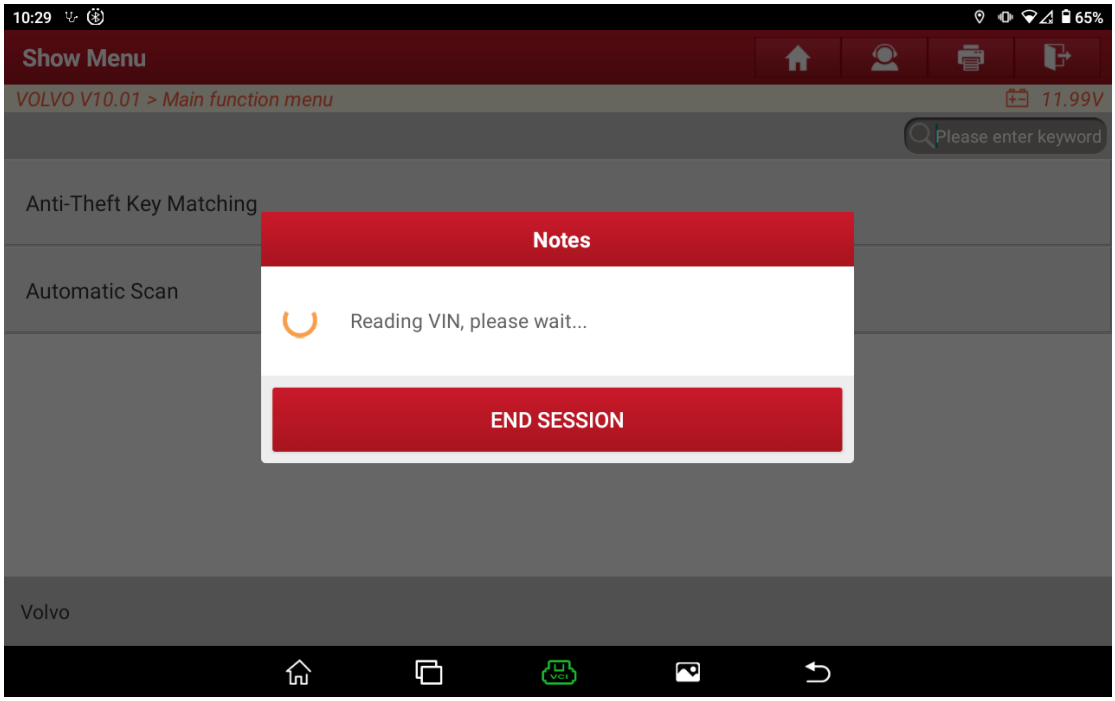


Figure 3

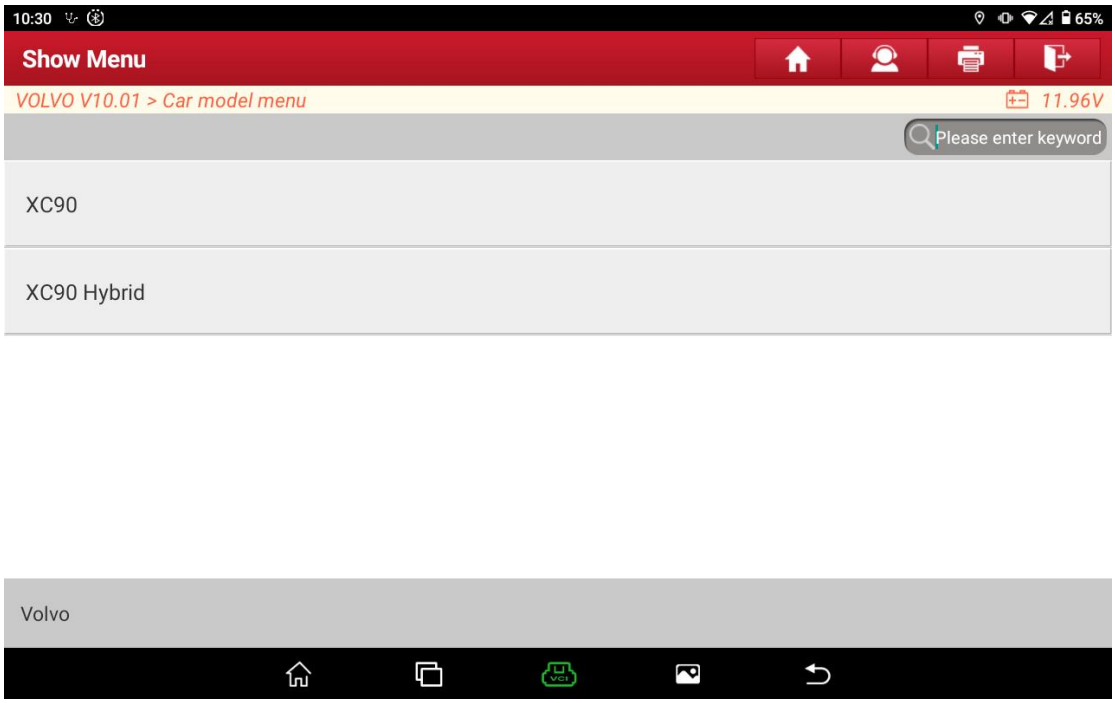


Figure 4

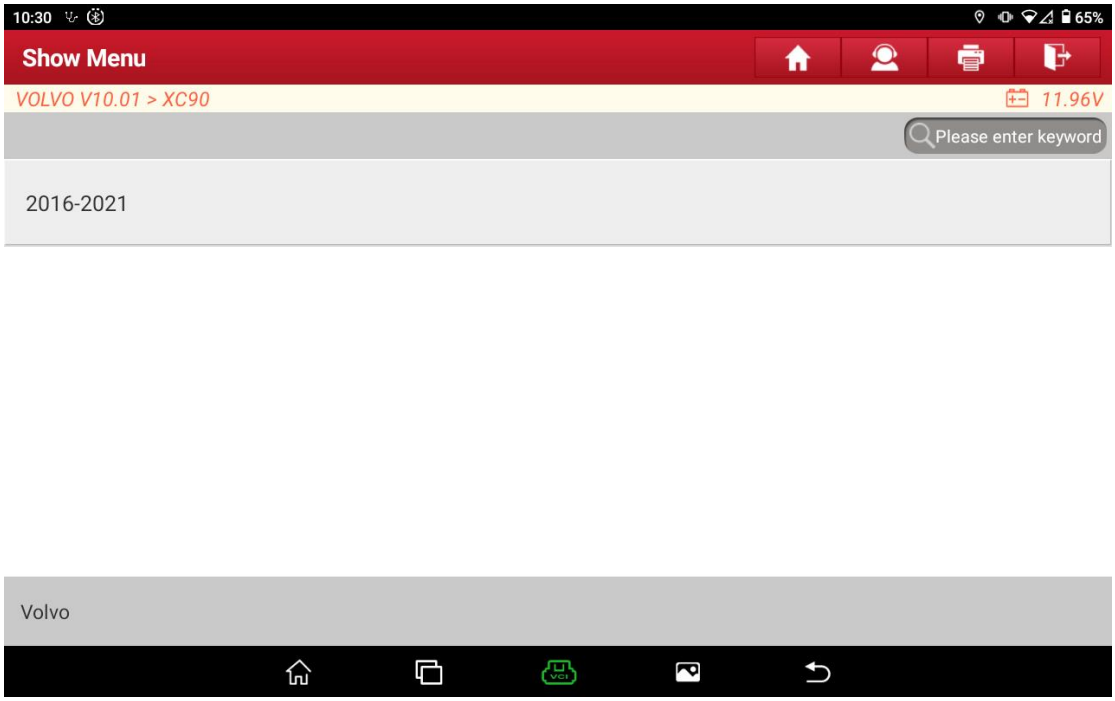


Figure 5

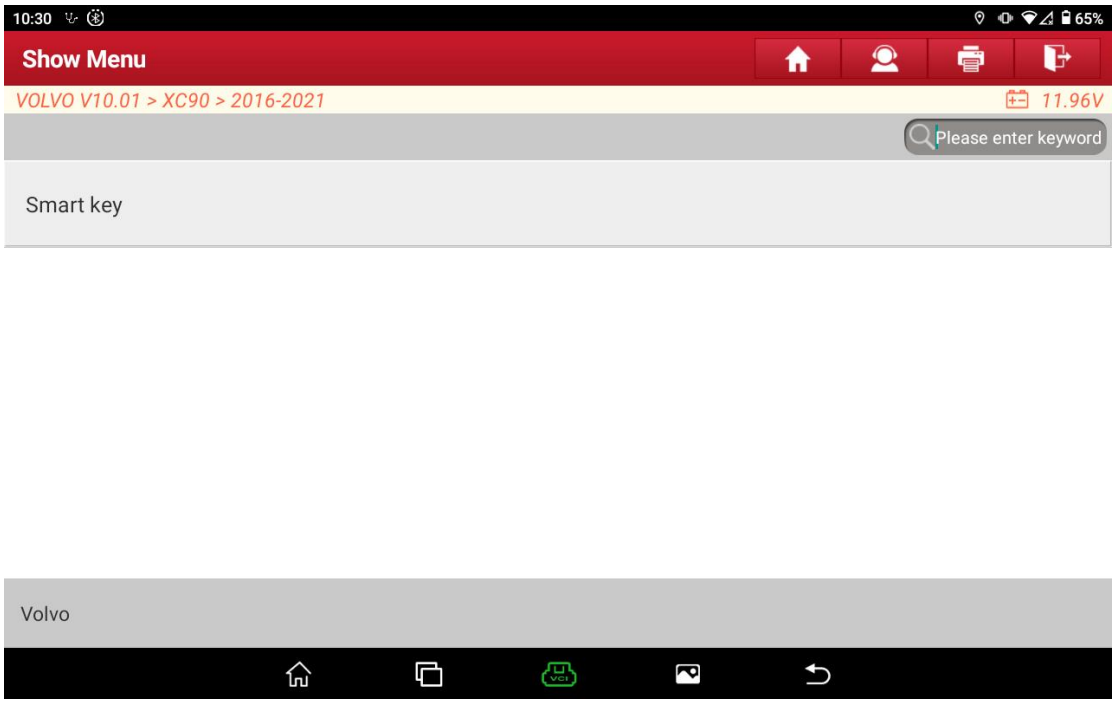


Figure 6

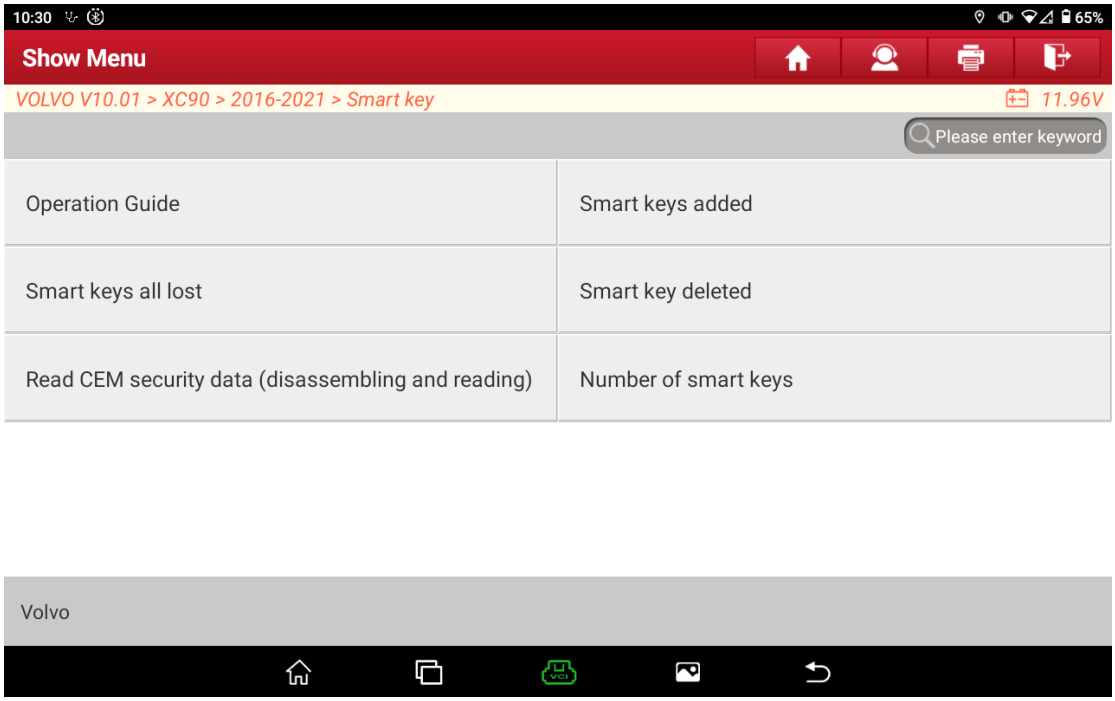


Figure 7

2. [Operation Guide]

Check the basic steps and precautions of the anti-theft matching process. (See Figure 8, Figure 9, Figure 10, and Figure 11 for the process steps)

1) Select the [Operation Guide] function to view the operation guide document.

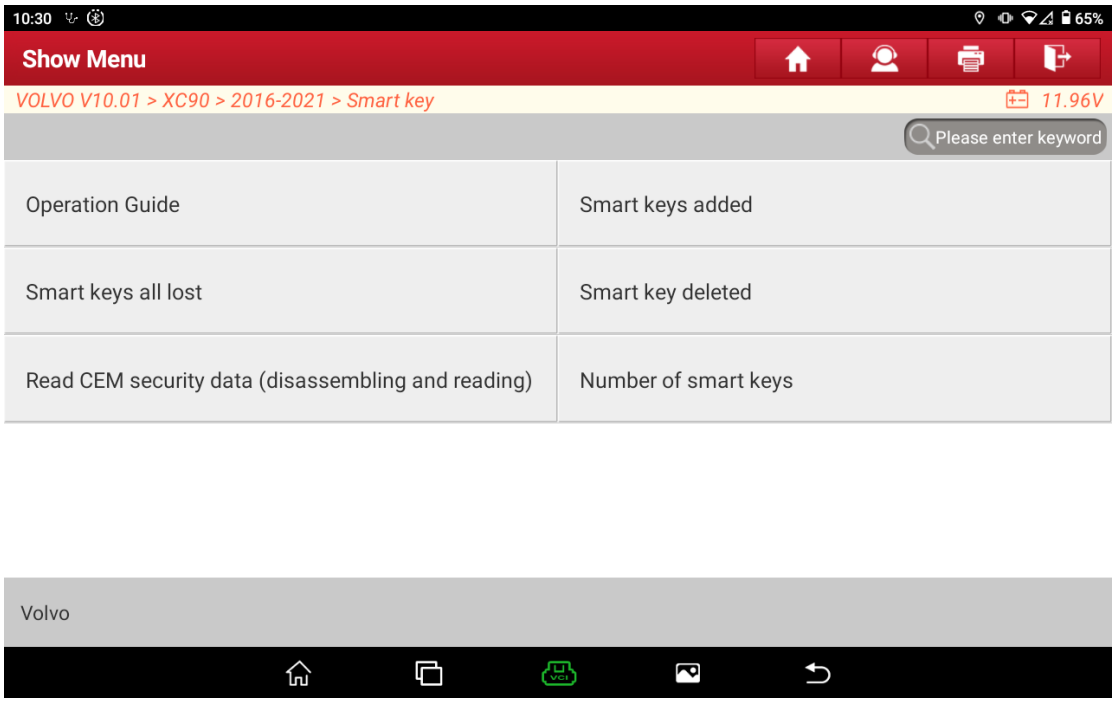


Figure 8

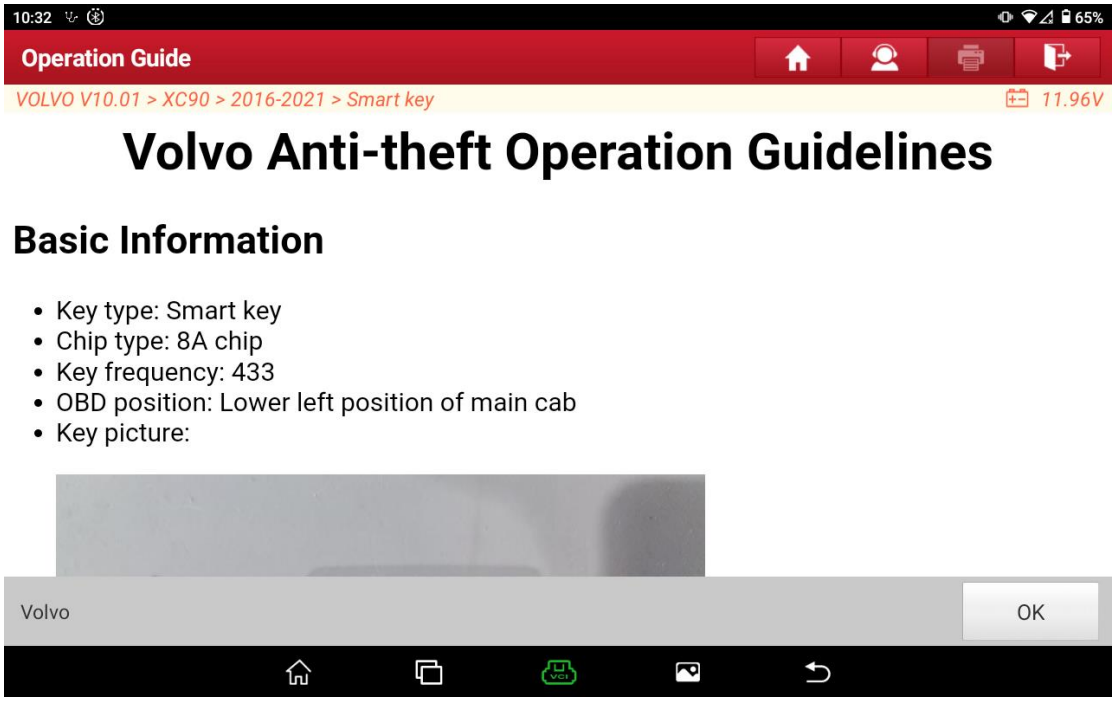


Figure 9

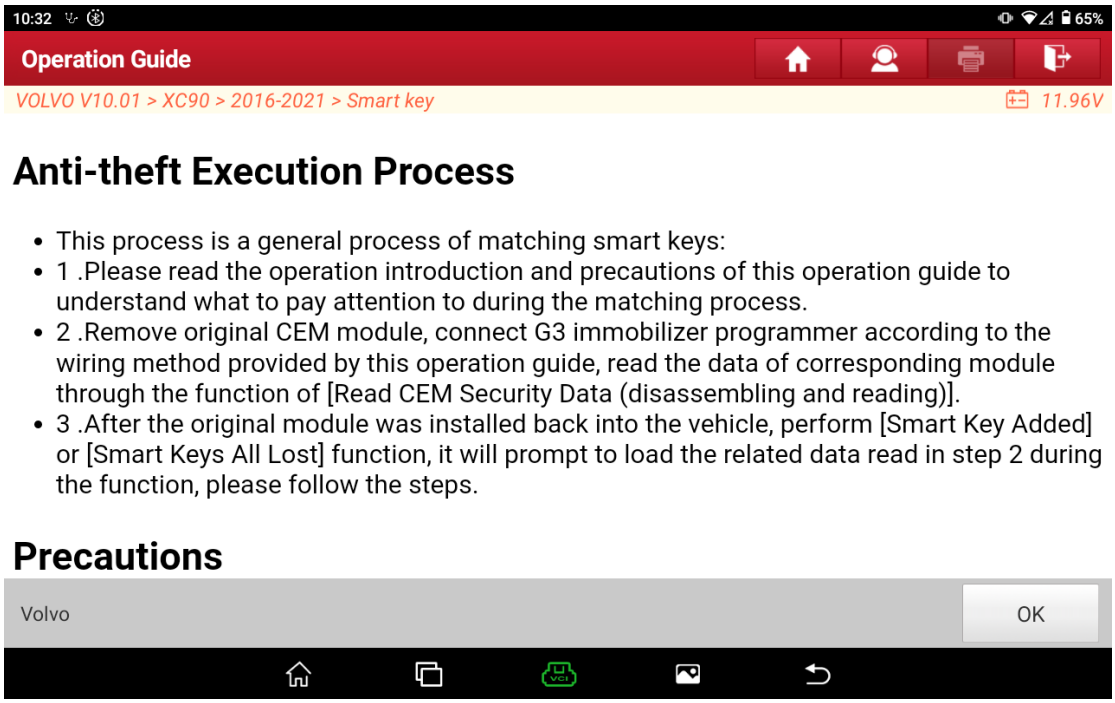


Figure 10

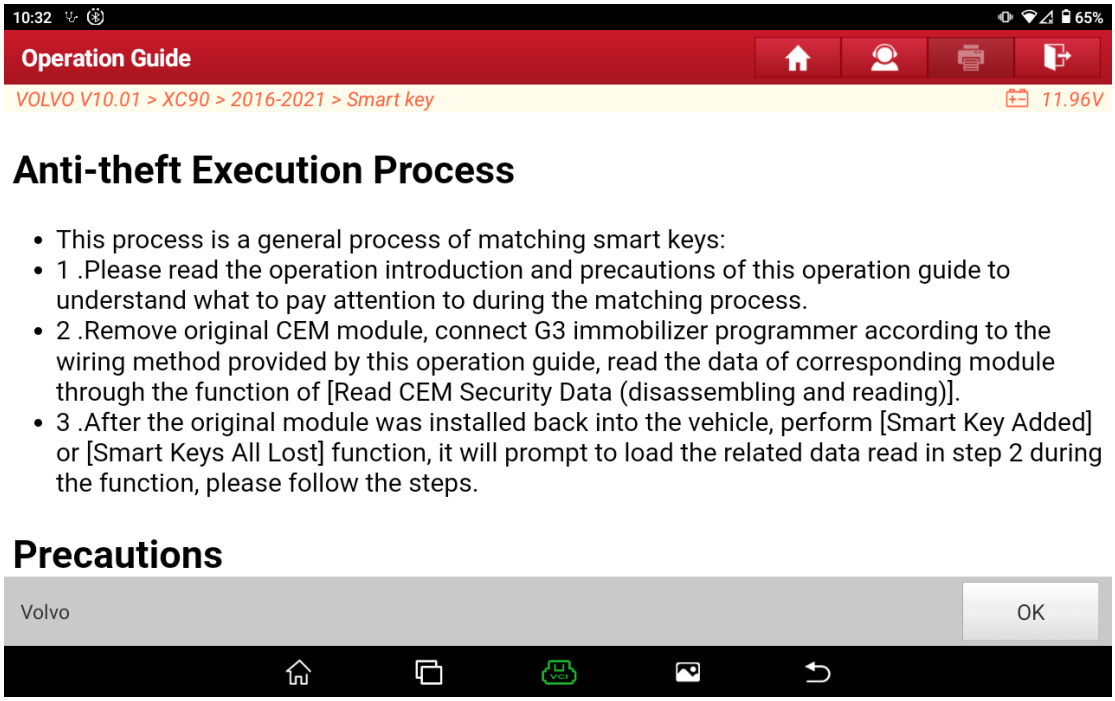


Figure 11

3. [Read CEM security data (disassembling and reading)]

By reading the operation document of the function of [Operation Guide], the MCU Cable V1 harness of G3 programmer should be used to connect the disassembled vehicle module, and then the MCU V1 adapter board should be used to connect the G3 programmer to the vehicle module. Finally, the function [Read CEM security data (disassembling and reading)] should be selected to read the anti-theft data of the vehicle module. (The module position and connection method are detailed in [Operation Guide], which will not be detailed in this document. See Figure 12, Figure 13 and Figure 14 for the process steps)

1) The connection diagram is as follows:

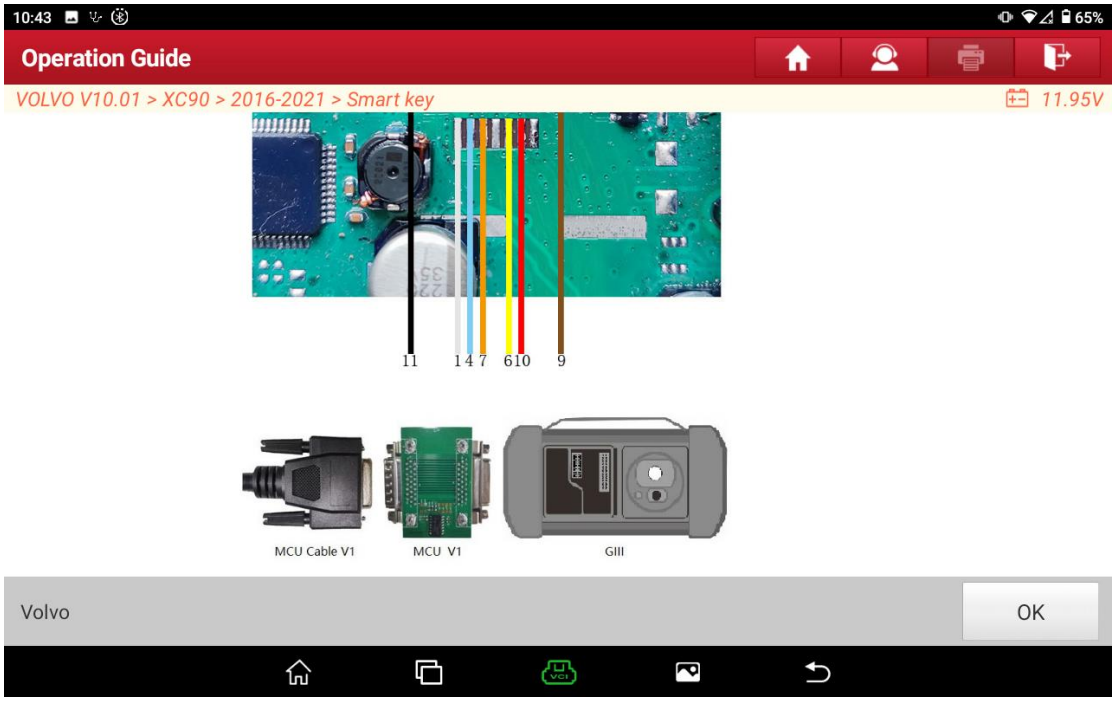


Figure 12

2) Select [Read CEM security data(disassembling and reading)] function

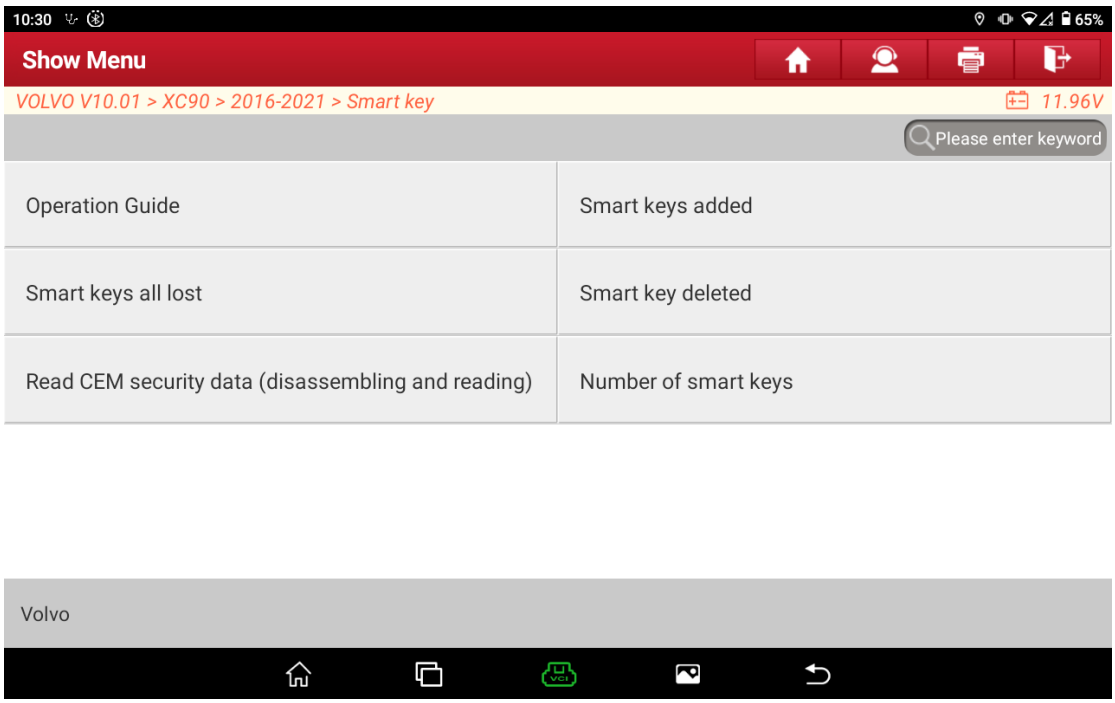


Figure 13

3) Prompt to view the [Operation Guide] function and click [YES] to proceed to the next step.

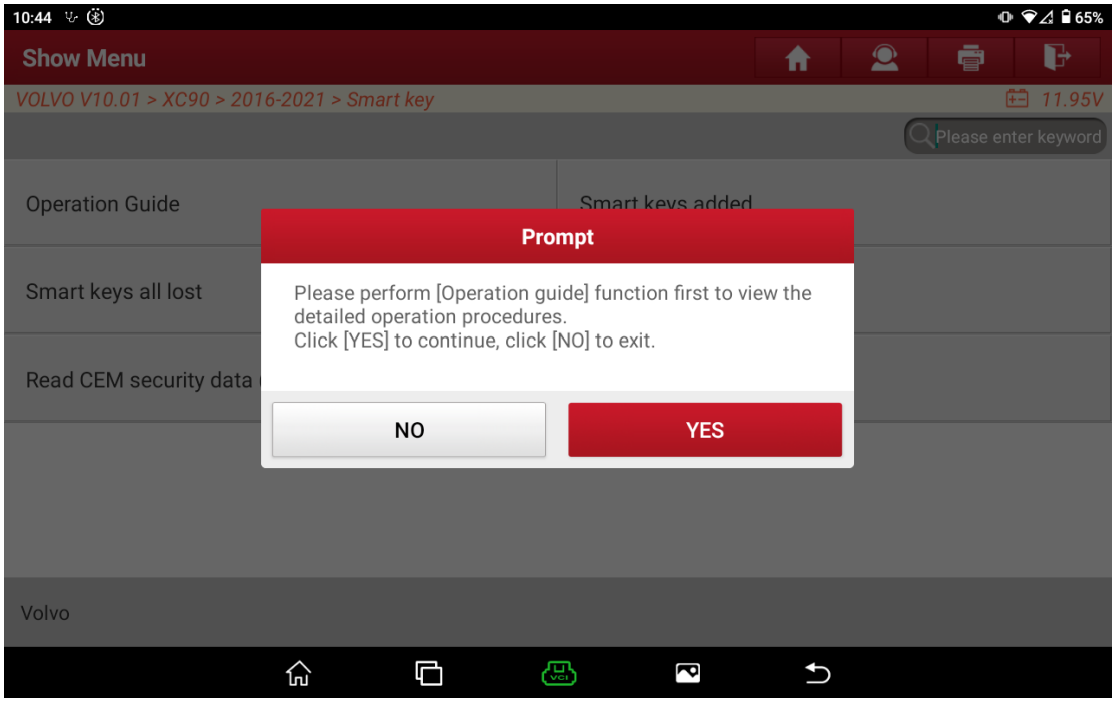


Figure 14

4) Connect G3 programmer. Connect anti-theft device, programmer and vehicle module according to [Operation guide]. Click [Yes] to proceed to the next step.

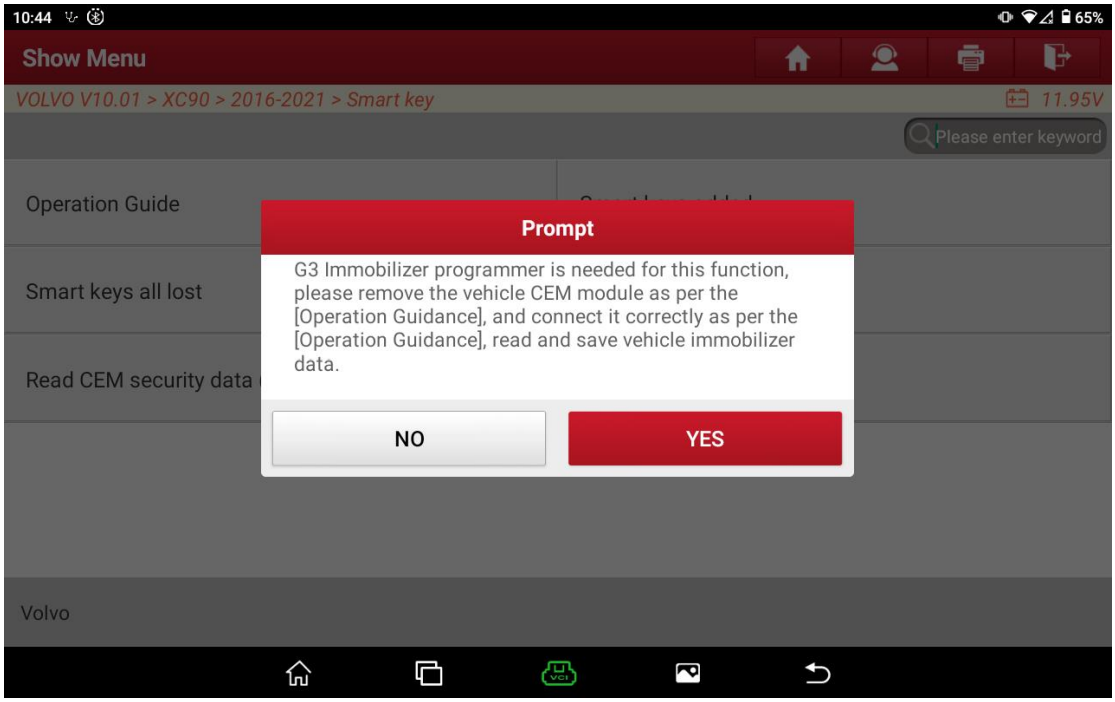


Figure 15

5) Select [SPC5748G] menu to proceed to the next step.

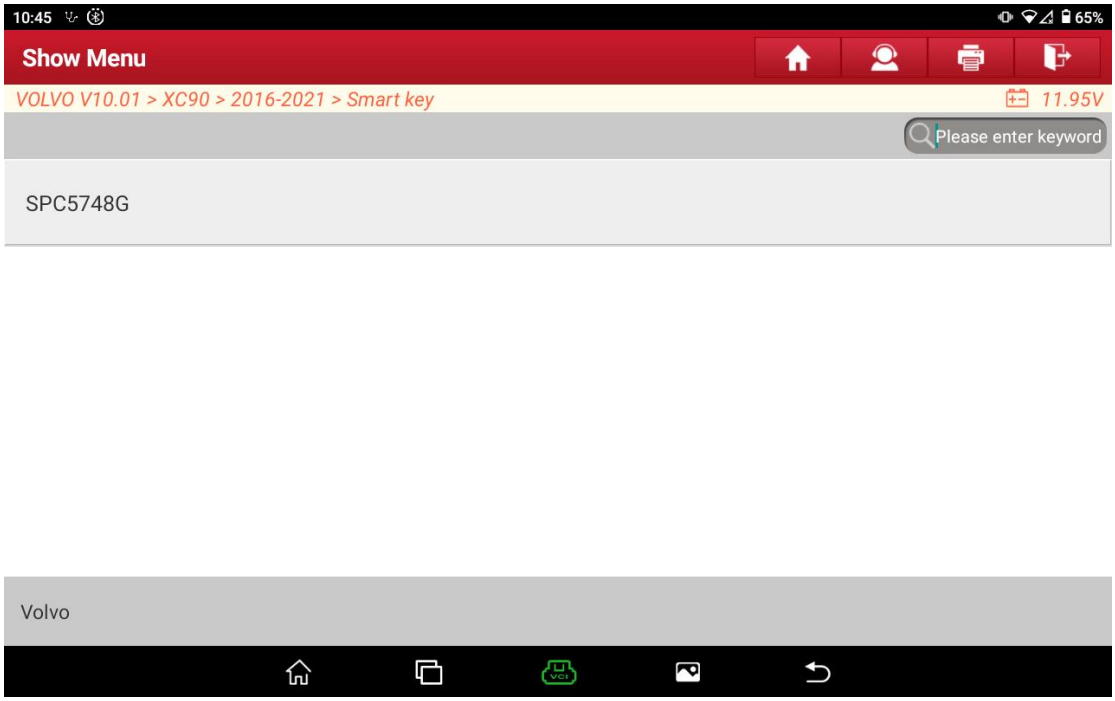


Figure 16

6) It is indicated that anti-theft data is being read. The reading time is about 2-3 minutes, during which no operation is required. Do not move the device to avoid data reading failure.

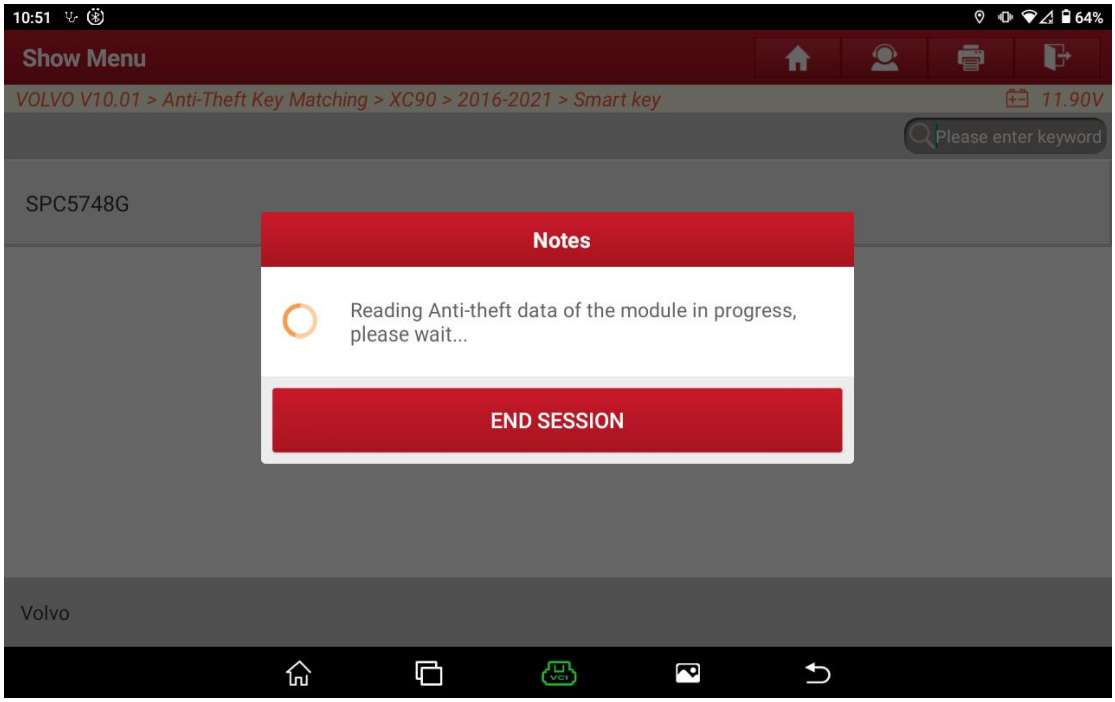


Figure 17

7) After the anti-theft data is read successfully, it is prompted that the data is read successfully and the data is saved. After the successful saving, the function execution is completed.

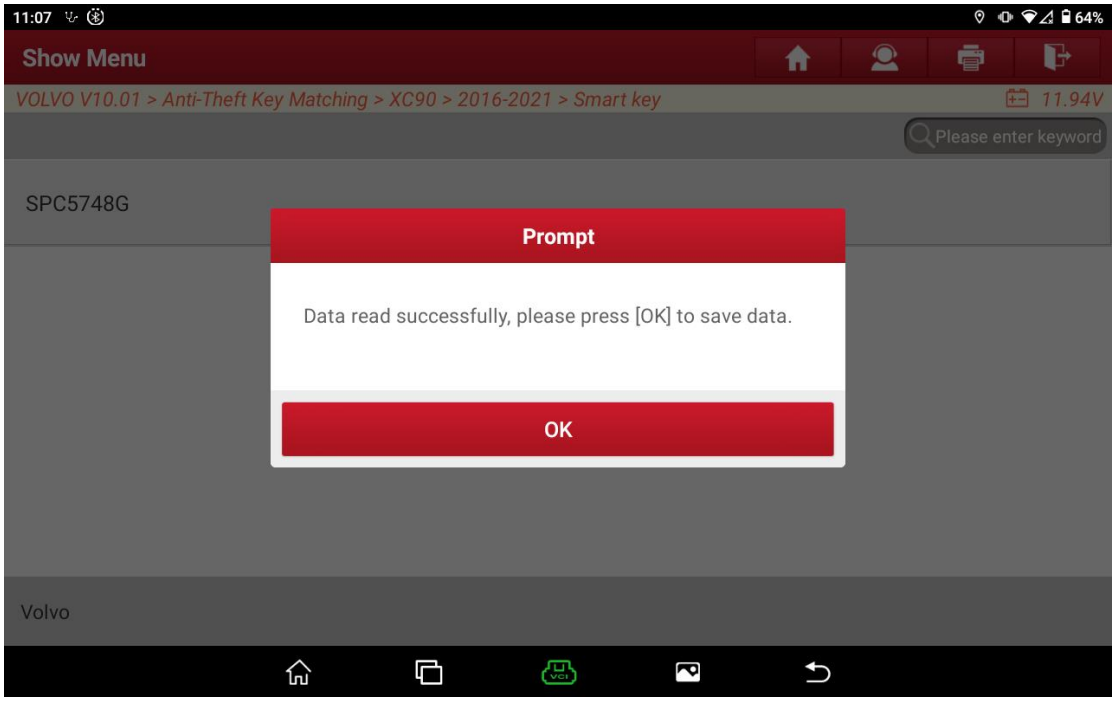


Figure 18

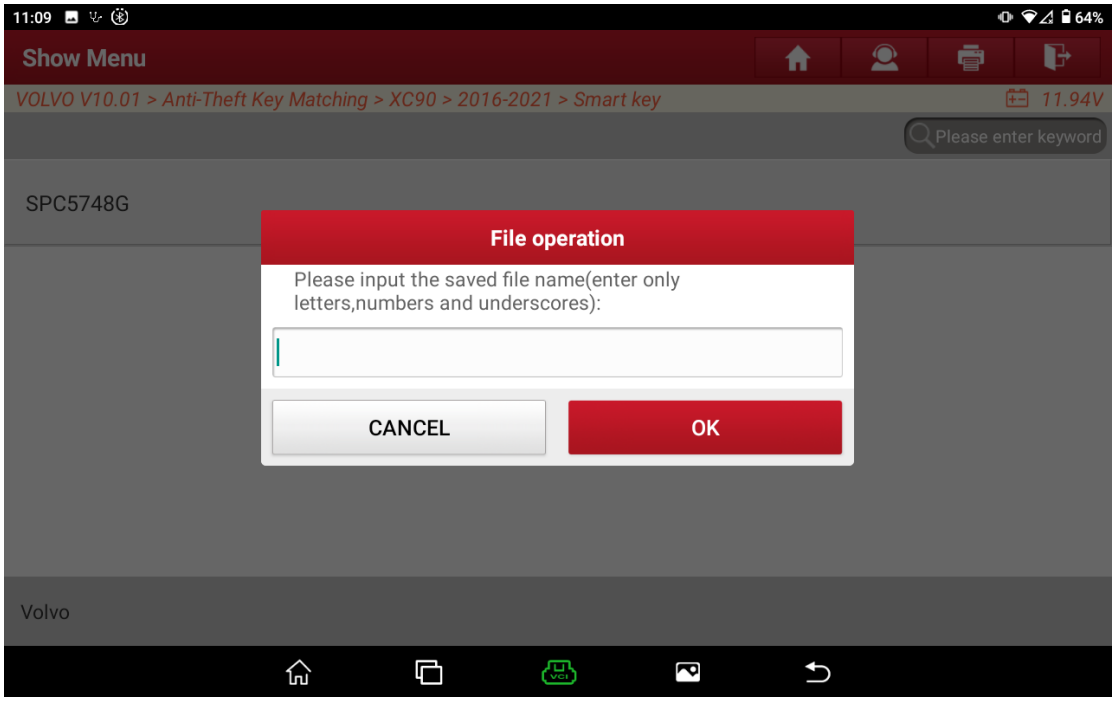


Figure 19

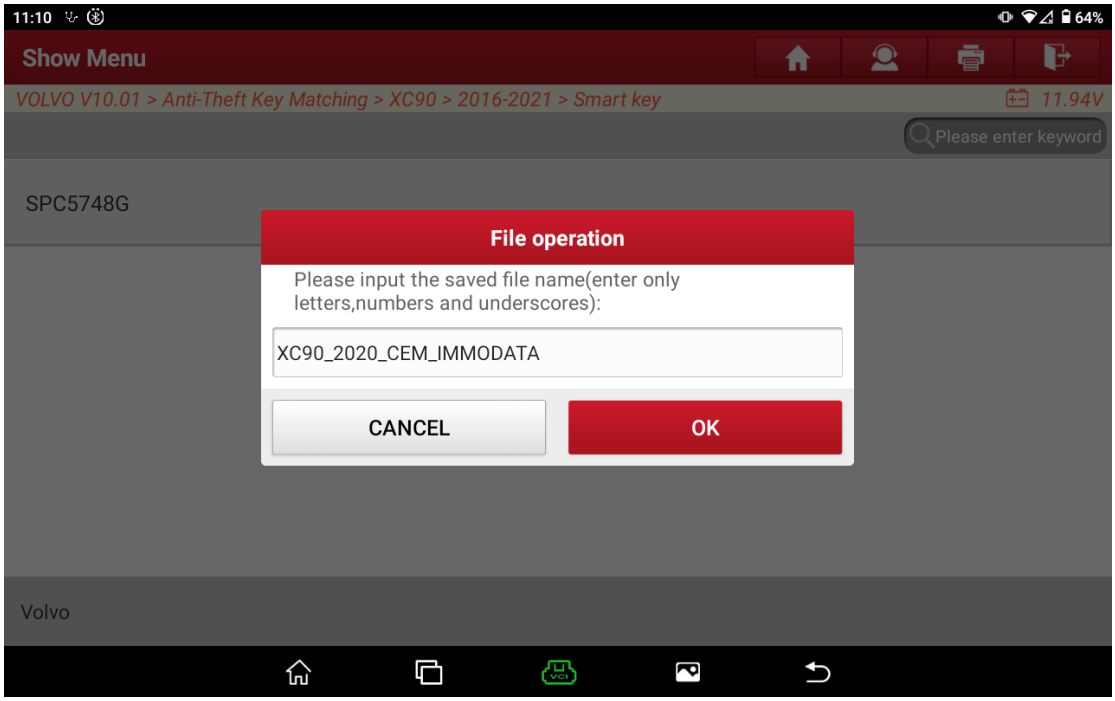


Figure 20

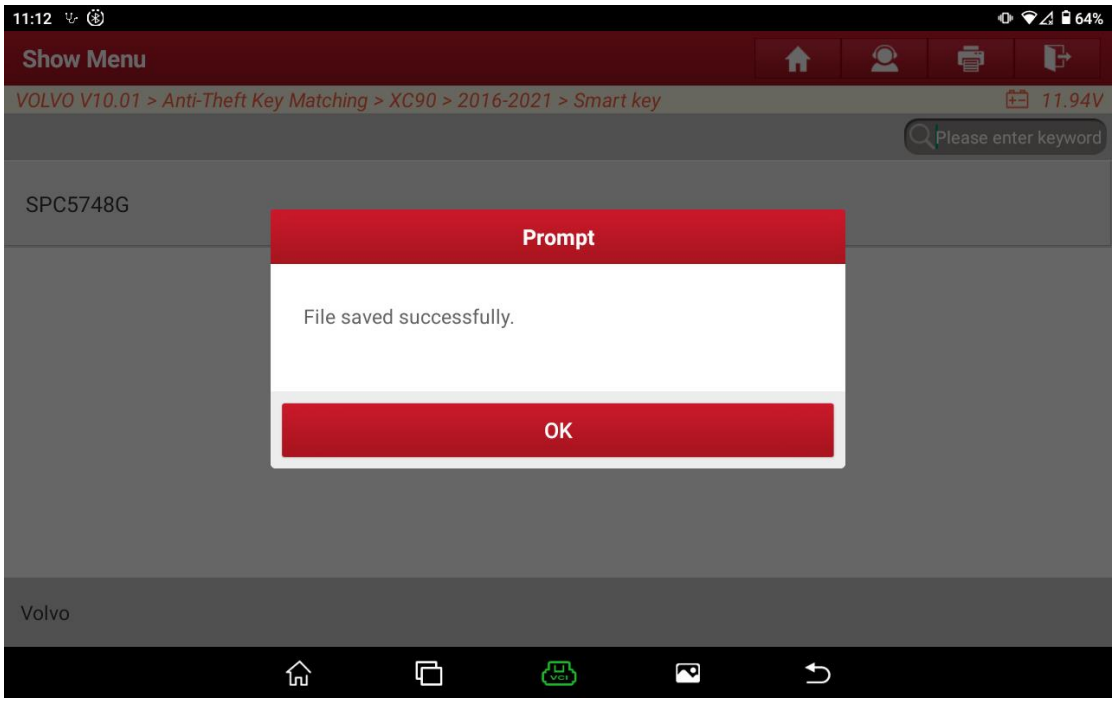


Figure 21

4. [Smart keys added]

The [Smart keys added] function is used to add keys to the vehicle without deleting the original car keys. The [Smart key all lost] function is used to add keys to the vehicle after deleting all the original car keys. After deleting the original car keys, the original car keys need to be re-matched before they can be used again. The

[Smart key deleted] function is used to delete all the original car keys. Please select a function based on actual requirements. This document uses [Smart keys added] as an example:

1) Select [Smart keys added] function, and the prompt is displayed to view the [Operation guide] function, click [YES] to proceed to the next step.

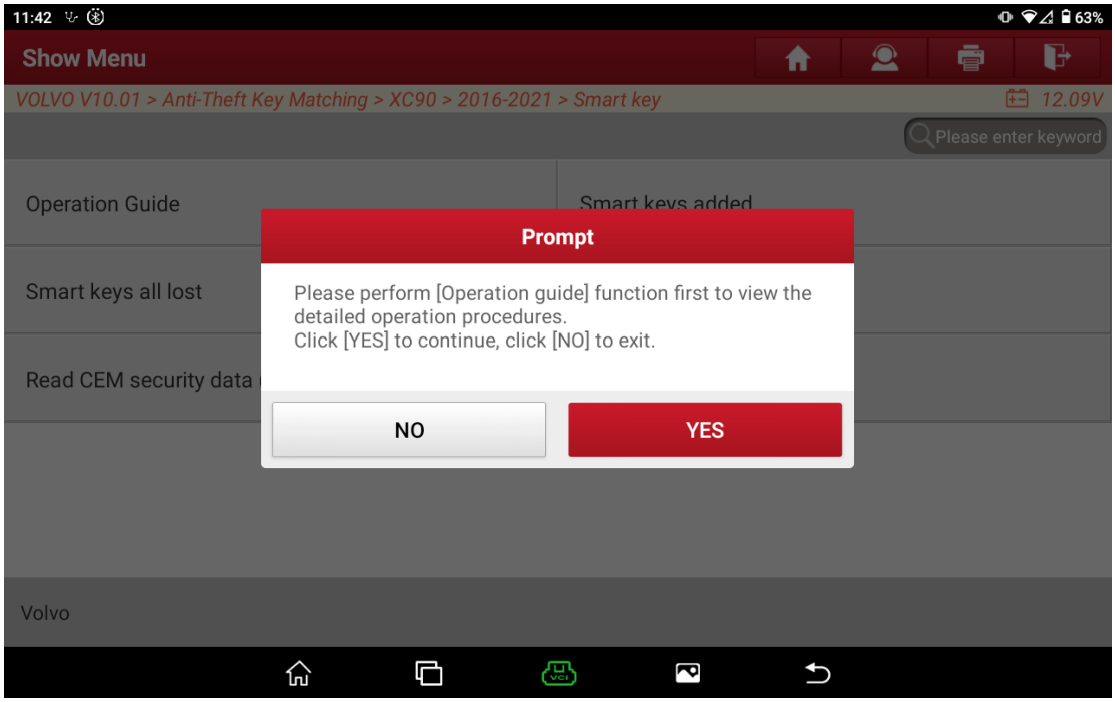


Figure 22

2) After completing the action 'Turn the START knob to the right for one time and then release it', click [OK] to go to the next step.

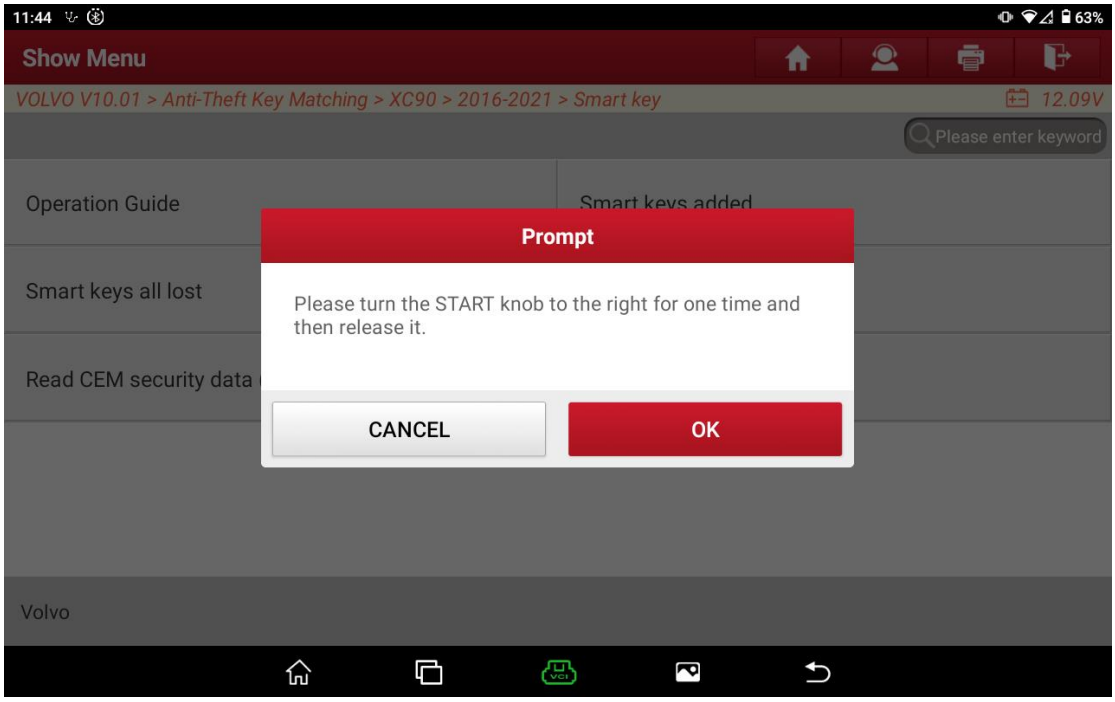


Figure 23

3) A prompt is displayed to load CEM security data, click [OK] to load the anti-theft data.

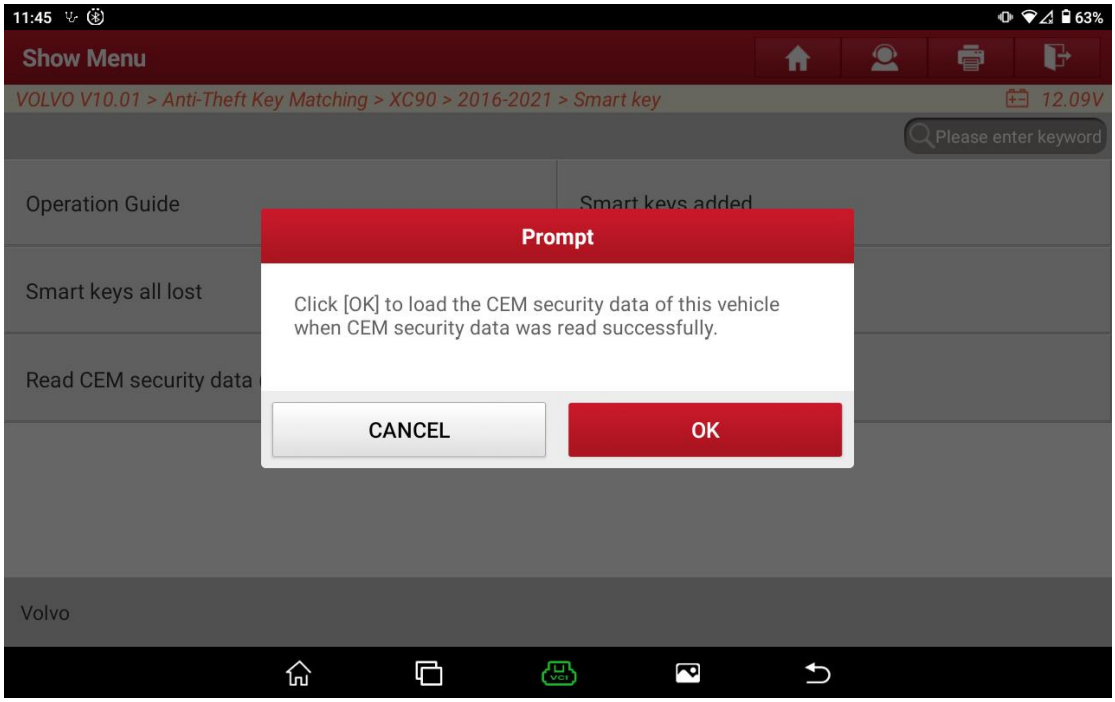


Figure 24

4) Select the read data file, here we select file XC90_2020_CEM_IMMODATA.bin(see Figure 25, Figure 26

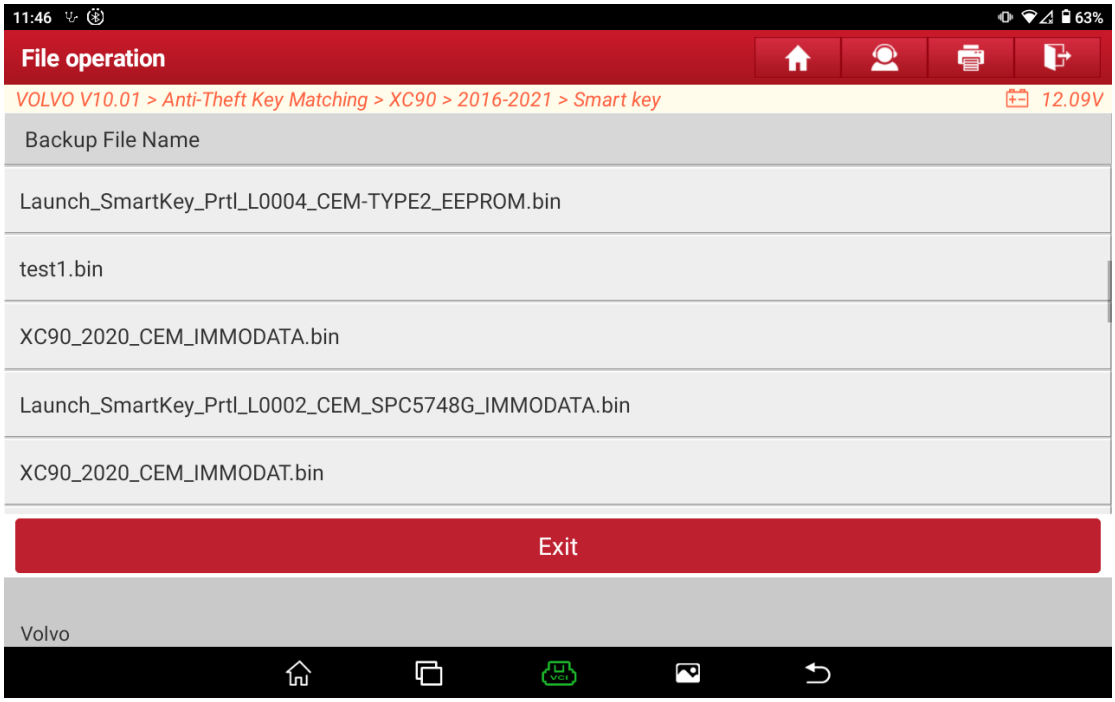


Figure 25

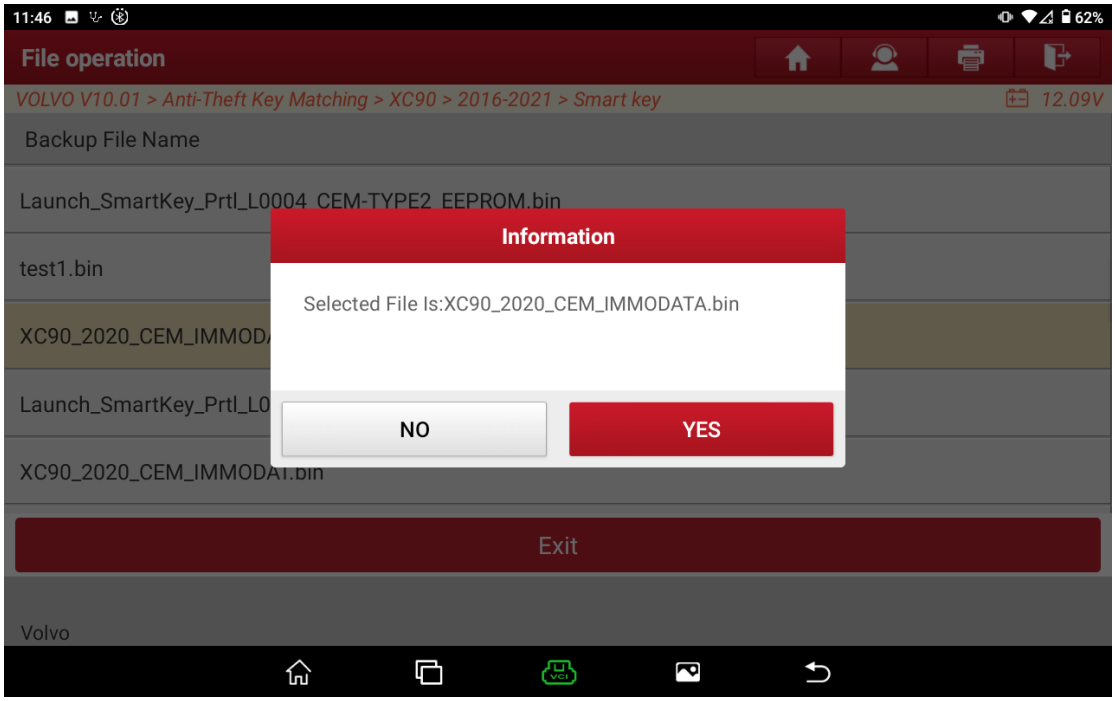


Figure 26

5) It's prompted to put the key to be matched into the induction area, and other intelligent keys are taken out of the car. Click [OK] to perform the next step.

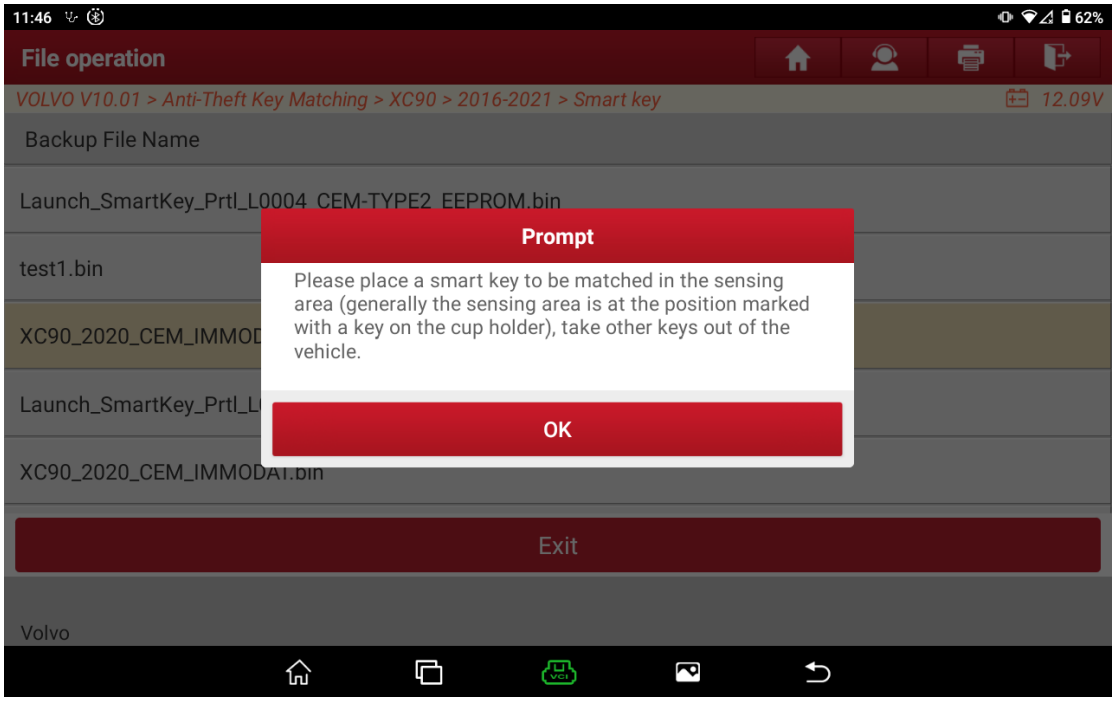


Figure 27

6) Wait for the key to be matched. If the key is matched successfully, a message will be displayed indicating that the key is matched successfully. If you need to continue to match the new key, click [OK] and perform Step 5). If not, please click [CANCEL] to exit (See Figure 28, Figure 29)

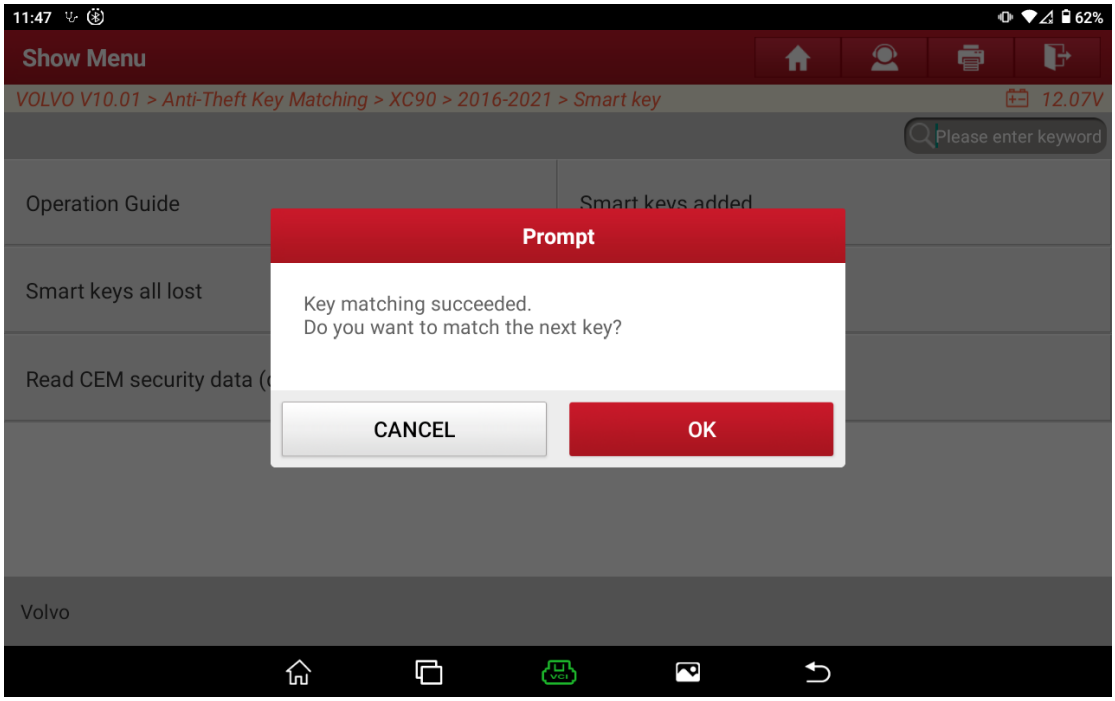


Figure 28

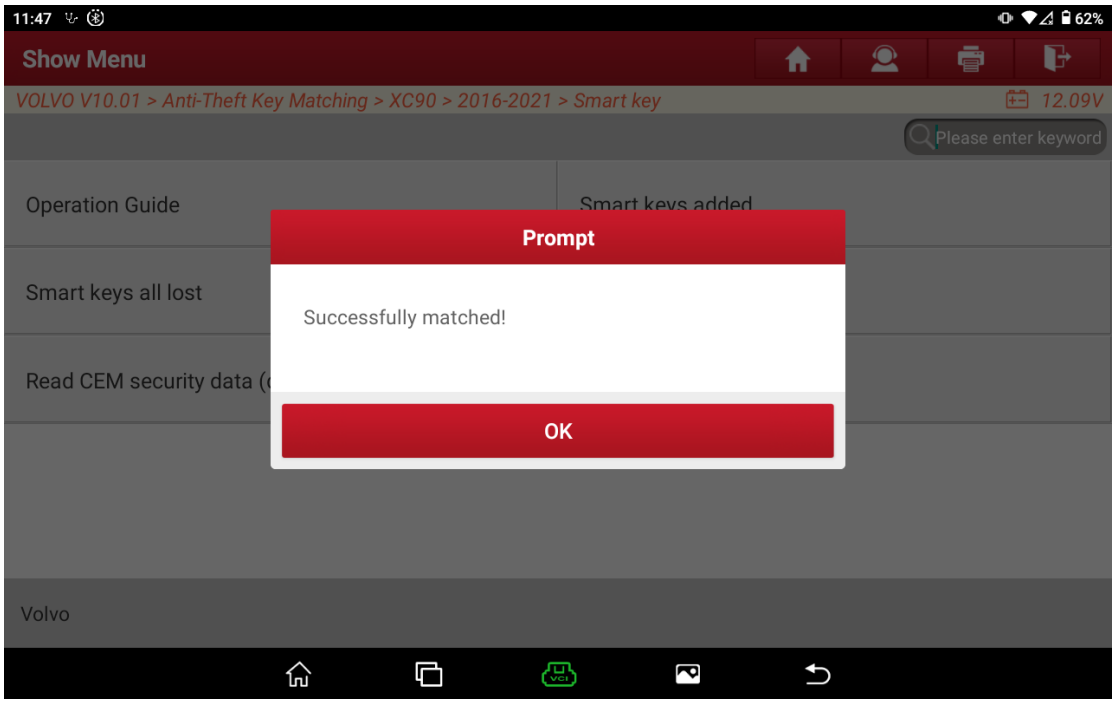


Figure 29

Statement: