PM3 MAX

1.Product feature

1.1 Comes with two fully functional USB ports. Both the TYPE-C and MICRO ports can be connected to a computer.

1.2 A brand new chip model, although it cannot flash RDv4 firmware, it can flash Iceman firmware with consistent functionality.

1.3 FPC connector with 9-pin, supports modification of Bluetooth module, extended USB interface, SAM card module, etc.

1.4 512KB memory, all functions are retained without deletion.

1.5 Reserve low-frequency coil solder joints for easy modification by users.

1.6 There are 4 solder joints on the back, which can switch between card reading mode and sniffing mode. When disconnected, it is card reading mode, stable card reading, and moderate sniffing. When short circuiting (using materials such as soldering iron, wire, conductive tape, etc.), switching the sniffing mode greatly improves the sniffing ability, and the distance is even slightly farther than RDV4.

1.7 The low-frequency antenna is processed with PCB hollowing out and supports multiple installation methods, making it an added advantage in some low-frequency sniffing situations. For example, hitag2 (PCF9736...)

1.8 Offline sniffing mode, can sniff without an app. Just power up the product and press and hold the three second button to enter the sniffing mode (green light on). At this time, card sniffing can be performed. After sniffing, the log will be stored inside the chip and can be extracted from the computer GUI. It also supports offline continuous sniffing, and the log will be added on its own. Theoretically, it can support up to 50 sniffing attempts.

1.9 With the offline password storage feature, frequently used passwords can be saved inside the chip via the GUI. Even after changing computers, these passwords can still be retrieved through the GUI. This offers a convenient way to store passwords without the need for an internet connection. In theory, up to1000+ passwords can be stored offline.

1.10 Equipped with free computer GUI software and English APP. The APP supports both OTG and Bluetooth connection.When using the computer GUI, it is necessary to flash the PC firmware，When using the APP, it is necessary to flash the APP firmware

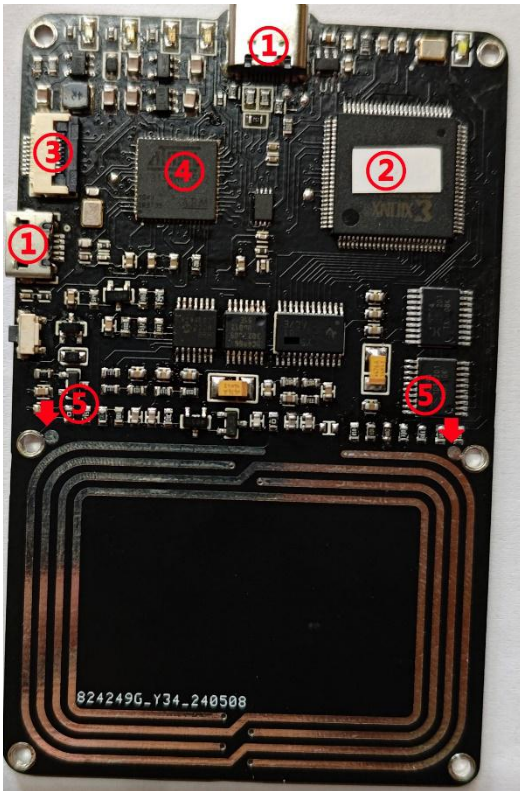
1.11 Continuously updated, with features consistent with the official Iceman. If you need to flash other firmware, please add the parameter=PM3ICOPYX during compilation

1.12 https://github.com/rfidreadermaker/proxmark3-max

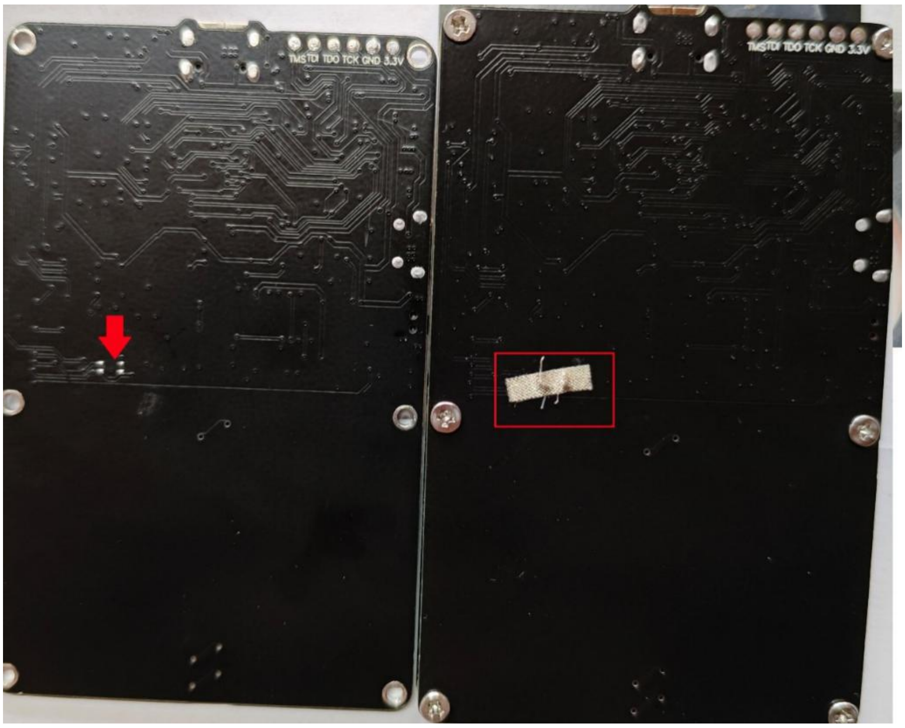
1.13 https://www.youtube.com/watch?v=X790z43Bdg0

2.Product images

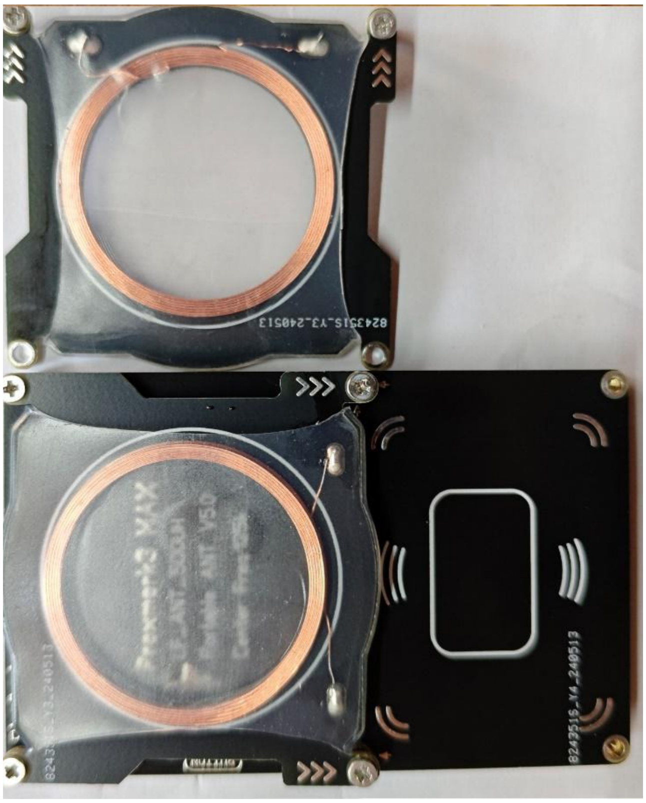
2.1Front view



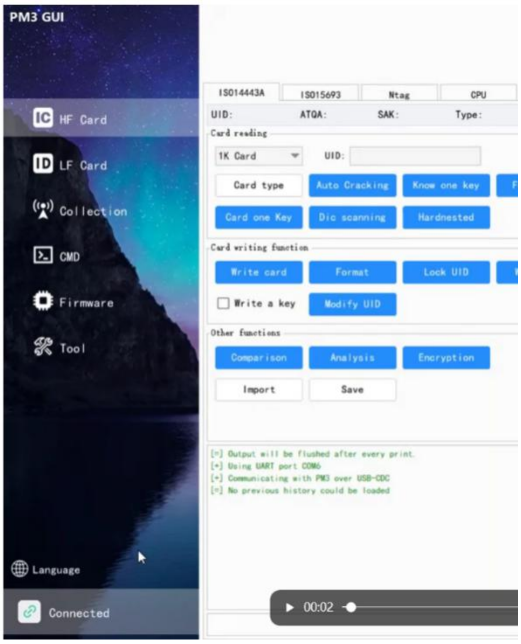
2.2Back view



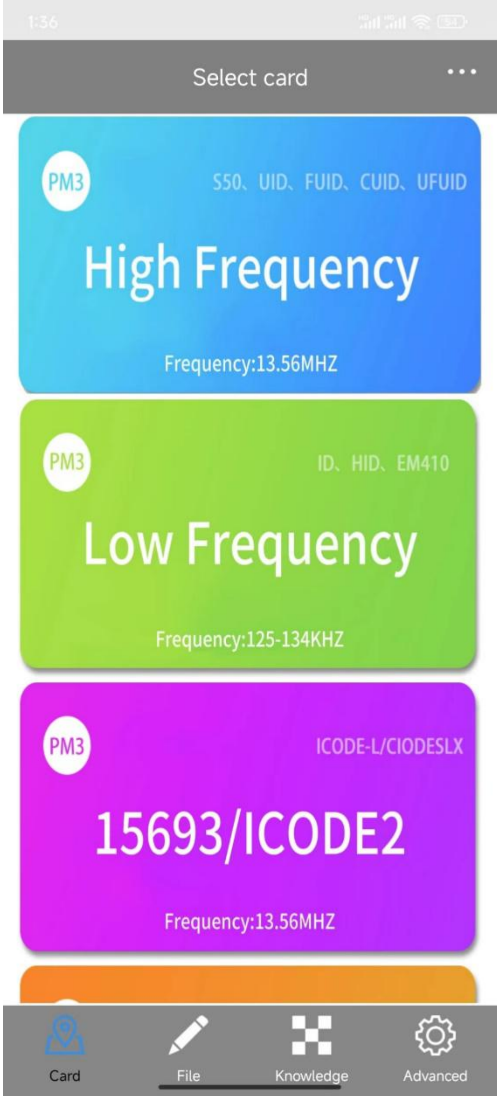
2.3Low frequency antenna hollowing treatment and various installation methods



2.4Free computer GUI and APP



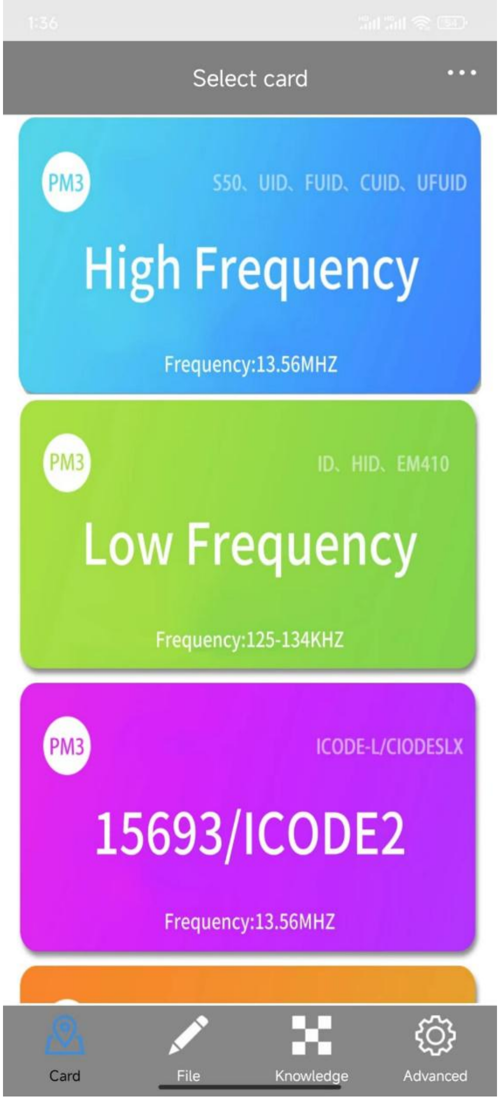
```
[=] Output will be flushed after every print.
[+] Using UART port COM6
[+] Communicating with PM3 over USB-CDC
[=] No previous history could be loaded
```


Select card

PM3 S50、UID、FUID、CUID、UFUID
High Frequency
Frequency:13.56MHZ

PM3 ID、HID、EM410
Low Frequency
Frequency:125-134KHZ

PM3 ICODE-L/CIODESLX
15693/ICODE2
Frequency:13.56MHZ



1:36

Select card

PM3 S50、UID、FUID、CUID、UFUID

High Frequency

Frequency:13.56MHZ

PM3 ID、HID、EM410

Low Frequency

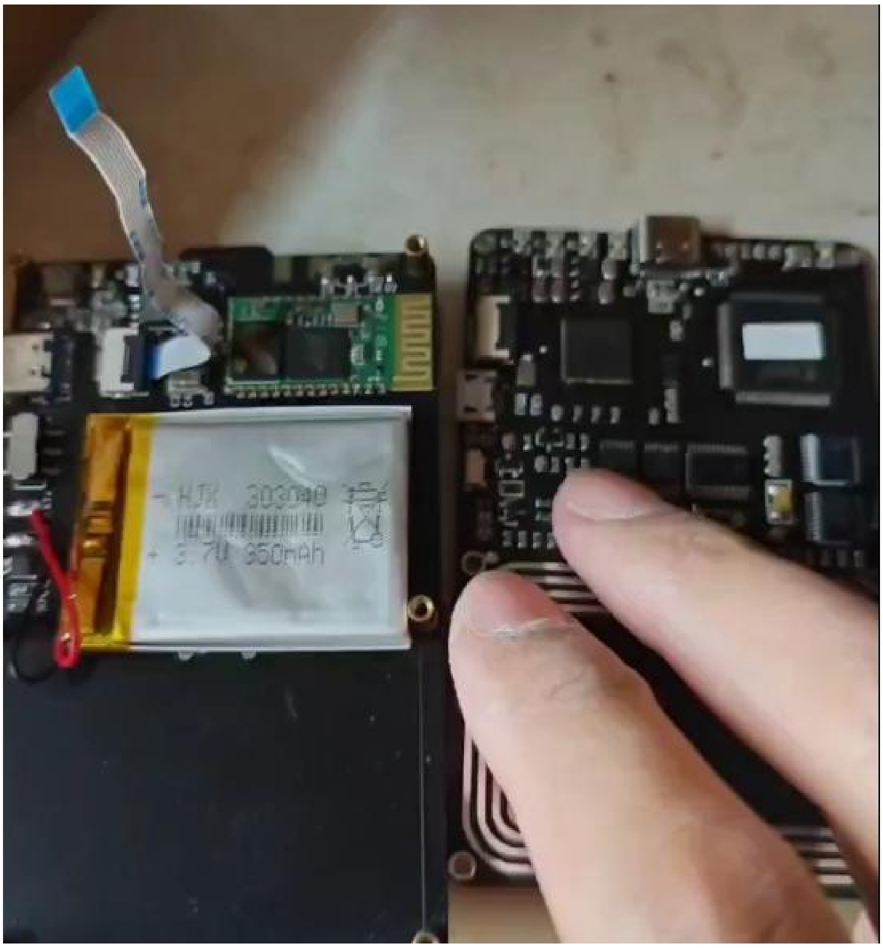
Frequency:125-134KHZ

PM3 ICODE-L/CIODESLX

15693/ICODE2

Frequency:13.56MHZ

2.5Bluetooth module modification



2.6FPC connector -9PIN

9.VCC

8.ARM 47(for sim card)

7.ARM 35(for sim card)

6.ARM 32(for sim card)

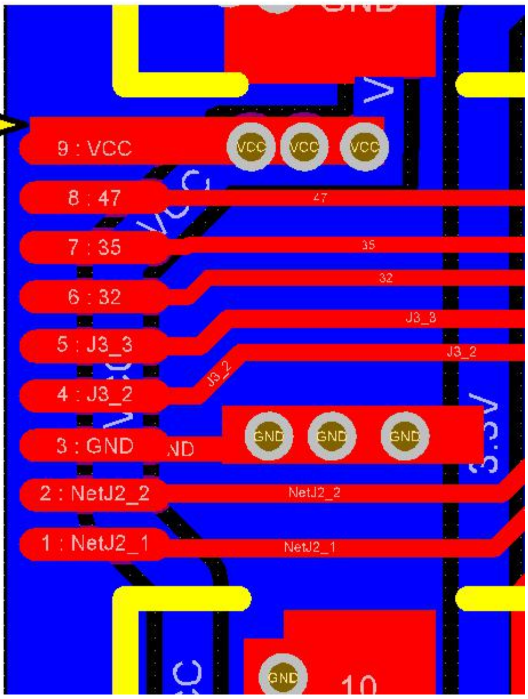
5.USB D+

4.USB D-

3.GND

2.ARM 14 TX (for Bluetooth)

1.ARM 11 RX (for Bluetooth)



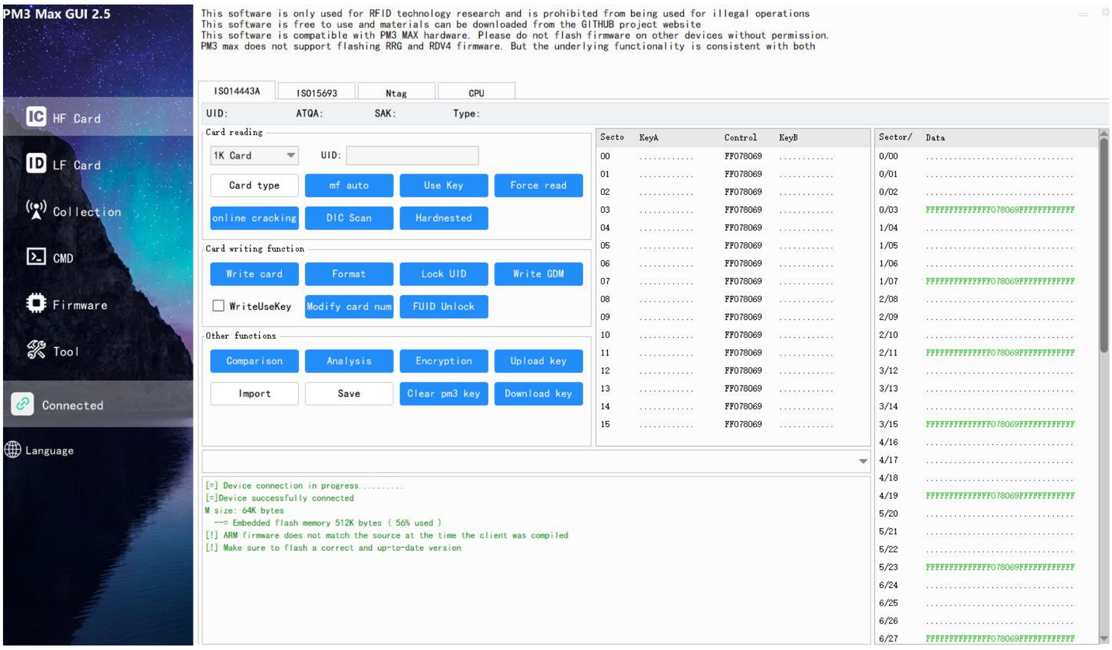
3.GUI introduce

3.1 Download link ：

https://github.com/rfidreadermaker/proxmark3-max

The GUI is completely non-toxic, but the operations of saving and importing data may be considered risky by Microsoft. Therefore, there may be risk warnings when downloading software, but there is no need to worry. Just add trust to the software. If you are really worried, you can also use the underlying code of the RRG team to link devices.

3.2 connet PM3



This software is only used for RFID technology research and is prohibited from being used for illegal operations
This software is free to use and materials can be downloaded from the GITHUB project website
This software is compatible with PM3 MAX hardware. Please do not flash firmware on other devices without permission.
PM3 max does not support flashing RRG and RDV4 firmware. But the underlying functionality is consistent with both

☐ WriteUseKey

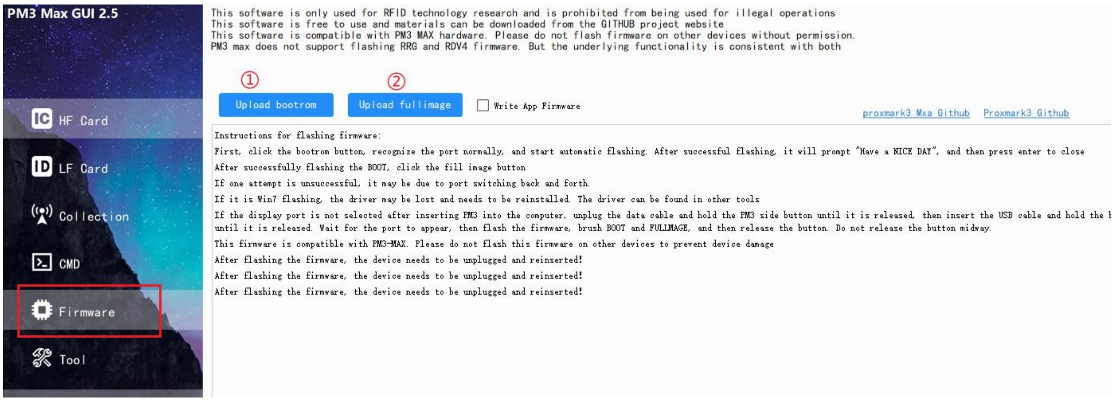
Secto	KeyA	Control	KeyB
00	....	FF078069	....
01	....	FF078069	....
02	....	FF078069	....
03	....	FF078069	....
04	....	FF078069	....
05	....	FF078069	....
06	....	FF078069	....
07	....	FF078069	....
08	....	FF078069	....
09	....	FF078069	....
10	....	FF078069	....
11	....	FF078069	....
12	....	FF078069	....
13	....	FF078069	....
14	....	FF078069	....
15	....	FF078069	....

Sector/	Data
0/00	....
0/01	....
0/02	....
0/03	FFFFFFFFFFFFFF078069FFFFFFFFFFFF
1/04	....
1/05	....
1/06	....
1/07	FFFFFFFFFFFFFF078069FFFFFFFFFFFF
2/08	....
2/09	....
2/10	....
2/11	FFFFFFFFFFFFFF078069FFFFFFFFFFFF
3/12	....
3/13	....
3/14	....
3/15	FFFFFFFFFFFFFF078069FFFFFFFFFFFF
4/16	....
4/17	....
4/18	....
4/19	FFFFFFFFFFFFFF078069FFFFFFFFFFFF
5/20	....
5/21	....
5/22	....
5/23	FFFFFFFFFFFFFF078069FFFFFFFFFFFF
6/24	....
6/25	....
6/26	....
6/27	FFFFFFFFFFFFFF078069FFFFFFFFFFFF

```
[=] Device connection in progress..........
[=]Device successfully connected
M size: 64K bytes
  --= Embedded flash memory 512K bytes ( 56% used )
[!] ARM firmware does not match the source at the time the client was compiled
[!] Make sure to flash a correct and up-to-date version
```

```
[!] ARM firmware does not match the source at the time the client was compiled
[!] Make sure to flash a correct and up-to-date version
```

If this prompt appears, it means that the firmware does not match, and we need to flash the corresponding firmware before we can use
it.

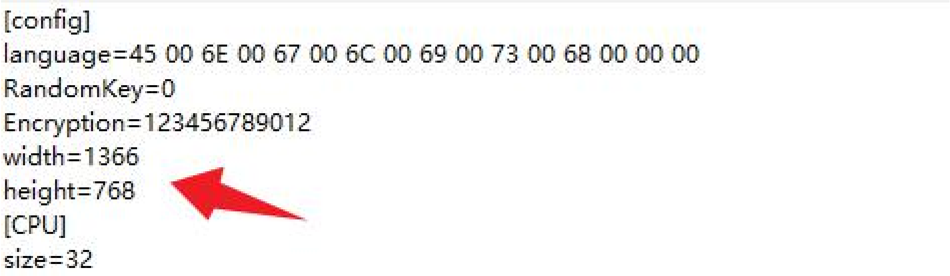


This software is only used for RFID technology research and is prohibited from being used for illegal operations
This software is free to use and materials can be downloaded from the GITHUB project website
This software is compatible with PM3 MAX hardware. Please do not flash firmware on other devices without permission.
PM3 max does not support flashing RRG and RDV4 firmware. But the underlying functionality is consistent with both

Instructions for flashing firmware:
First, click the bootrom button, recognize the port normally, and start automatic flashing. After successful flashing, it will prompt "Have a NICE DAY", and then press enter to close
After successfully flashing the BOOT, click the fill image button
If one attempt is unsuccessful, it may be due to port switching back and forth.
If it is Win7 flashing, the driver may be lost and needs to be reinstalled. The driver can be found in other tools
If the display port is not selected after inserting PM3 into the computer, unplug the data cable and hold the PM3 side button until it is released, then insert the USB cable and hold the b
until it is released. Wait for the port to appear, then flash the firmware, brush BOOT and FULLMAGE, and then release the button. Do not release the button midway.
This firmware is compatible with PM3-MAX. Please do not flash this firmware on other devices to prevent device damage
After flashing the firmware, the device needs to be unplugged and reinserted!
After flashing the firmware, the device needs to be unplugged and reinserted!
After flashing the firmware, the device needs to be unplugged and reinserted!

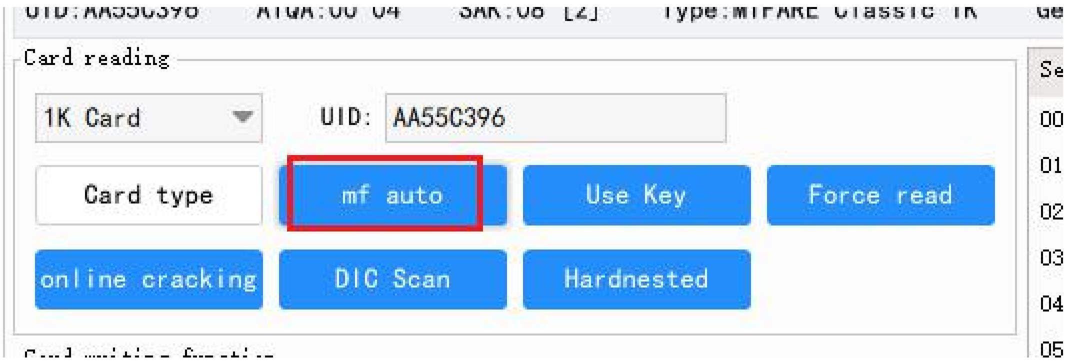
After you finish flashing the firmware, you must unplug the device and reinsert it.
The following video will quickly help you understand how to use the software
https://www.youtube.com/watch?v=YrIBbIoSKWg

If your screen resolution is not large enough, causing the software to display incompletely, you can use the following parameters to scale the software.
Open the 'config. ini' file in the 'Config' folder and add the following code width=1366 height=768 like this



```
[config]
language=45 00 6E 00 67 00 6C 00 69 00 73 00 68 00 00 00
RandomKey=0
Encryption=123456789012
width=1366
height=768
[CPU]
size=32
```

3.3 Introduction to some buttons



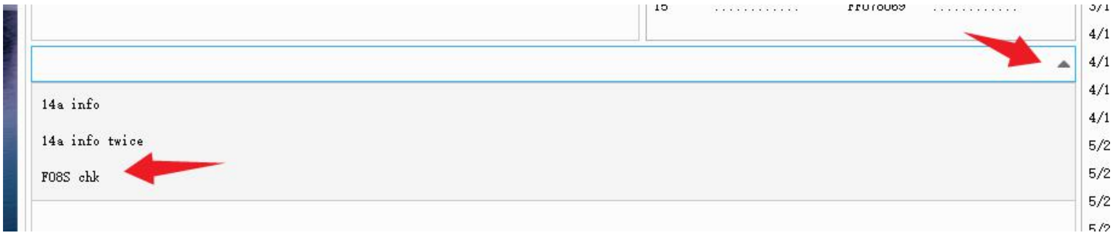
UID: AA55C396

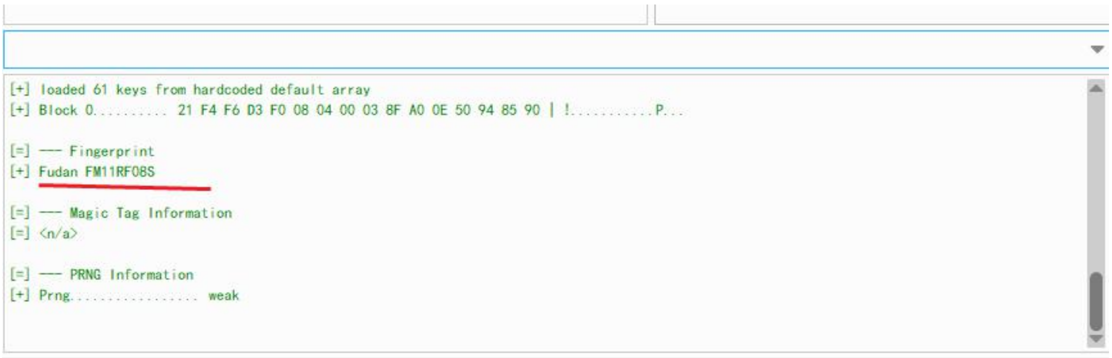
3.3.1The Mf auto button,

when clicked with the left mouse button, is equivalent to inputting the command 'hf mf auto'.

If you encounter a card that cannot be cracked by left clicking, such as F08S, right-click on "MF AUTO" to enter the F08S card cracking process. The whole process takes a long time, please be patient. If the cracking fails, you can choose to eliminate electromagnetic interference or change the position where the card is placed.

You can use the F08S CHK in the dropdown list of the command bar to check if the card is F08S. You can add more shortcut commands in the command. txt file.





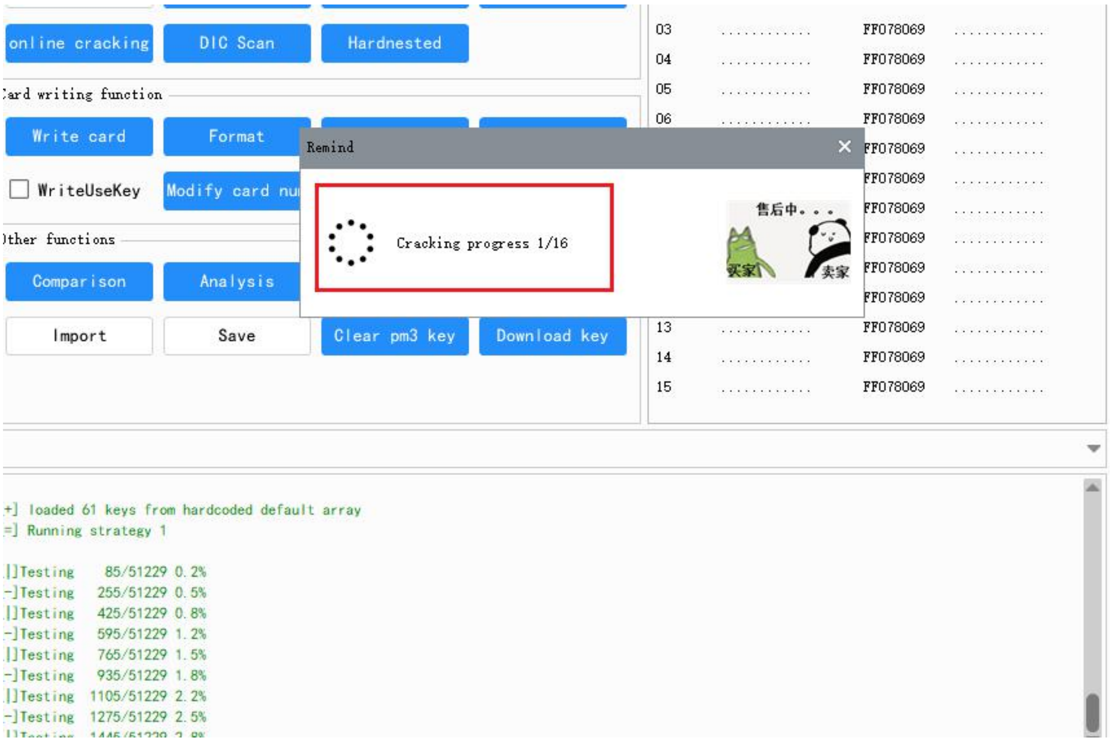
```
[+] loaded 61 keys from hardcoded default array
[+] Block 0.......... 21 F4 F6 D3 F0 08 04 00 03 8F A0 0E 50 94 85 90 | !..........P...

[=] --- Fingerprint
[+] Fudan FM11RF08S

[=] --- Magic Tag Information
[=] <n/a>

[=] --- PRNG Information
[+] Prng................. weak
```

The following interface shows the progress prompt when cracking
F08S



Cracking progress 1/16

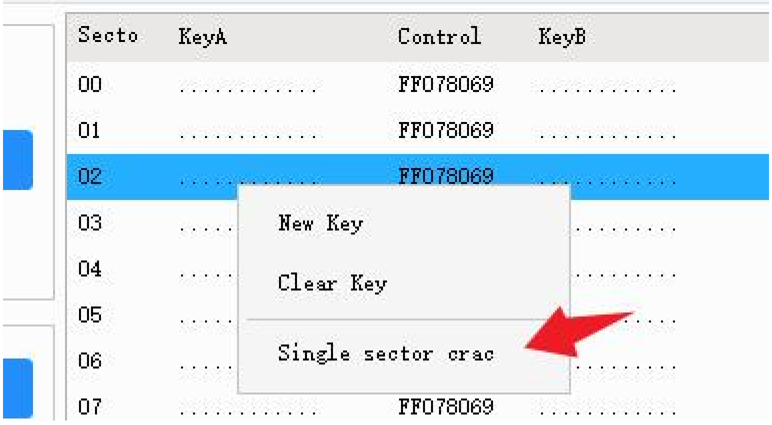
```
03   ............   FF078069   ............
04   ............   FF078069   ............
05   ............   FF078069   ............
06   ............   FF078069   ............
                    FF078069   ............
                    FF078069   ............
                    FF078069   ............
                    FF078069   ............
                    FF078069   ............
                    FF078069   ............
13   ............   FF078069   ............
14   ............   FF078069   ............
15   ............   FF078069   ............
```

```
+] loaded 61 keys from hardcoded default array
=] Running strategy 1

|]Testing    85/51229 0.2%
-]Testing   255/51229 0.5%
|]Testing   425/51229 0.8%
-]Testing   595/51229 1.2%
|]Testing   765/51229 1.5%
-]Testing   935/51229 1.8%
|]Testing  1105/51229 2.2%
-]Testing  1275/51229 2.5%
```

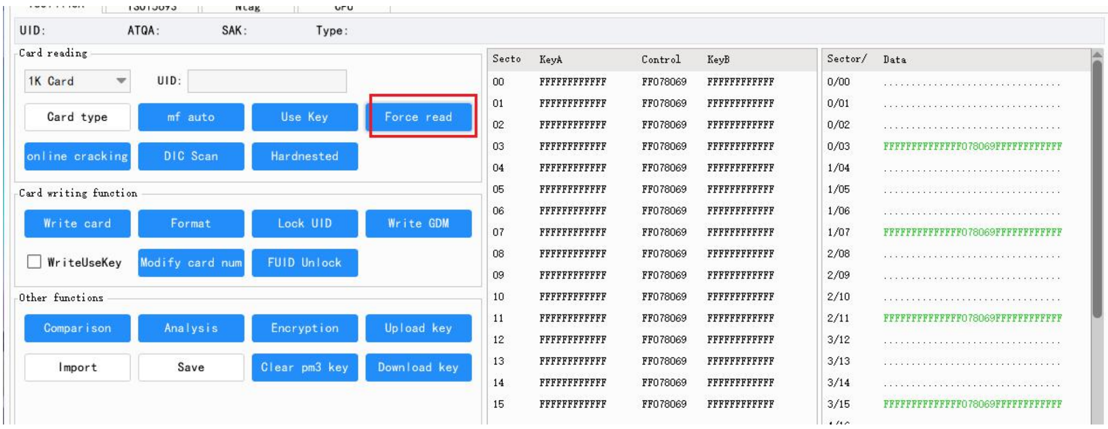
If you need to crack a sector separately, you can left click on the corresponding password area, then right-click on the password area and click this button to crack a sector separately.

This operation will only crack the password of the specified sector



Secto	KeyA	Control	KeyB
00	....	FF078069	....
01	....	FF078069	....
02	....	FF078069	....
03	.....		....
04	.....		....
05	.....		.....
06	.....		....
07	....	FF078069	....

3.3.2force read

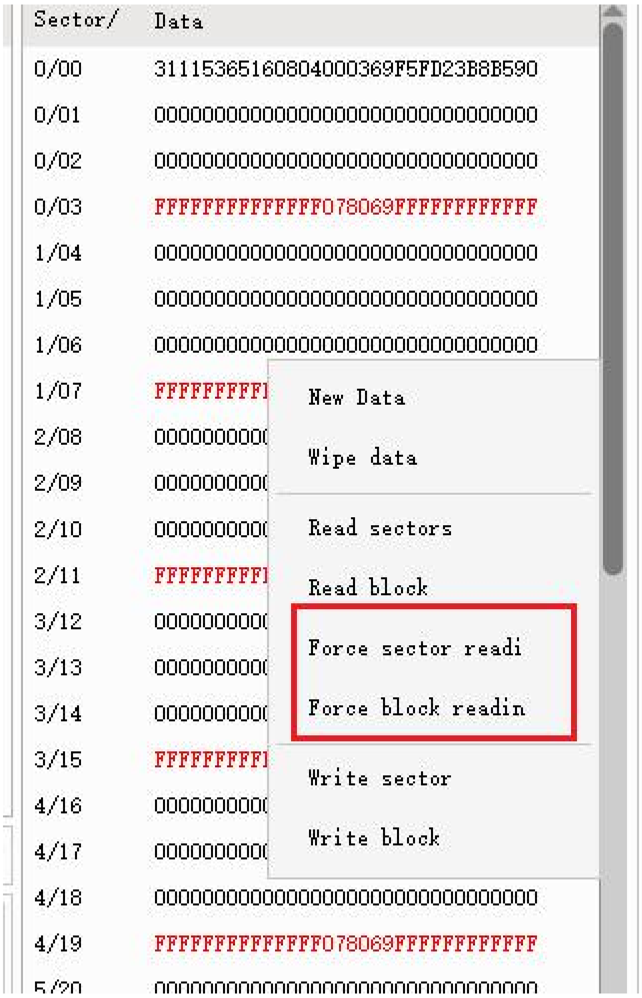


Secto	KeyA	Control	KeyB
00	FFFFFFFFFFFF	FF078069	FFFFFFFFFFFF
01	FFFFFFFFFFFF	FF078069	FFFFFFFFFFFF
02	FFFFFFFFFFFF	FF078069	FFFFFFFFFFFF
03	FFFFFFFFFFFF	FF078069	FFFFFFFFFFFF
04	FFFFFFFFFFFF	FF078069	FFFFFFFFFFFF
05	FFFFFFFFFFFF	FF078069	FFFFFFFFFFFF
06	FFFFFFFFFFFF	FF078069	FFFFFFFFFFFF
07	FFFFFFFFFFFF	FF078069	FFFFFFFFFFFF
08	FFFFFFFFFFFF	FF078069	FFFFFFFFFFFF
09	FFFFFFFFFFFF	FF078069	FFFFFFFFFFFF
10	FFFFFFFFFFFF	FF078069	FFFFFFFFFFFF
11	FFFFFFFFFFFF	FF078069	FFFFFFFFFFFF
12	FFFFFFFFFFFF	FF078069	FFFFFFFFFFFF
13	FFFFFFFFFFFF	FF078069	FFFFFFFFFFFF
14	FFFFFFFFFFFF	FF078069	FFFFFFFFFFFF
15	FFFFFFFFFFFF	FF078069	FFFFFFFFFFFF

Sector/	Data
0/00	....
0/01	....
0/02	....
0/03	FFFFFFFFFFFFFF078069FFFFFFFFFFFF
1/04	....
1/05	....
1/06	....
1/07	FFFFFFFFFFFFFF078069FFFFFFFFFFFF
2/08	....
2/09	....
2/10	....
2/11	FFFFFFFFFFFFFF078069FFFFFFFFFFFF
3/12	....
3/13	....
3/14	....
3/15	FFFFFFFFFFFFFF078069FFFFFFFFFFFF

When left clicking with the mouse, the software will use the password in the password area to read this card. You can import the password manually by filling in or dragging the data file.

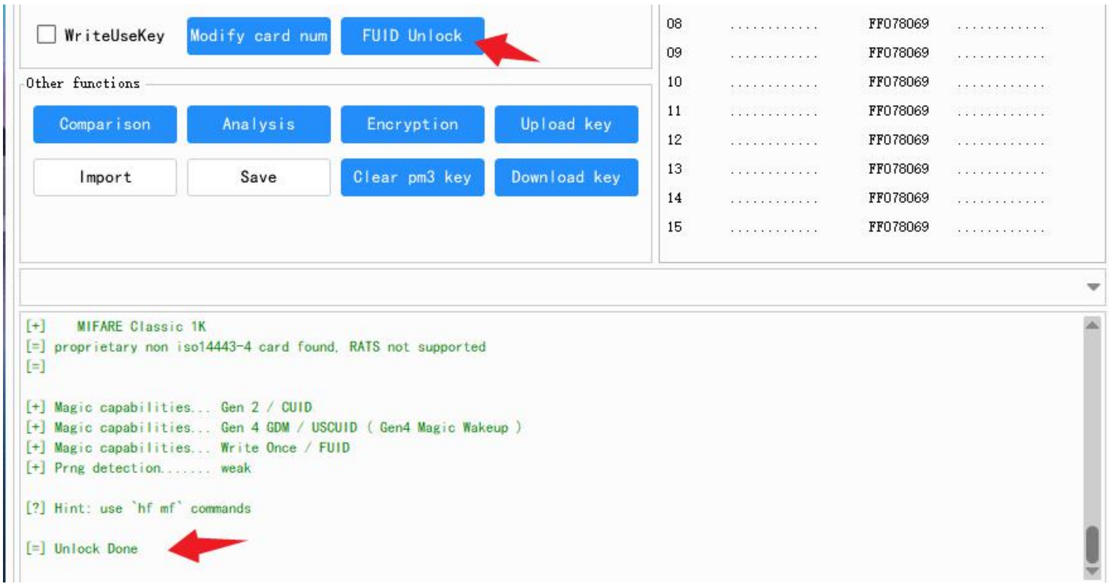
When right clicking with the mouse, the software will exploit the backdoor vulnerability of F08S to force the reading of card data and mark the encrypted sector password in red. Note: The right mouse button is only applicable to F08S cards. If partial sector reading fails, you can right-click on the data area and read a specific sector or block separately.



Sector/	Data
0/00	31115365160804000369F5FD23B8B590
0/01	00000000000000000000000000000000
0/02	00000000000000000000000000000000
0/03	FFFFFFFFFFFFFF078069FFFFFFFFFFFF
1/04	00000000000000000000000000000000
1/05	00000000000000000000000000000000
1/06	00000000000000000000000000000000
1/07	FFFFFFFFF
2/08	0000000000
2/09	0000000000
2/10	0000000000
2/11	FFFFFFFFF
3/12	0000000000
3/13	0000000000
3/14	0000000000
3/15	FFFFFFFFF
4/16	0000000000
4/17	0000000000
4/18	00000000000000000000000000000000
4/19	FFFFFFFFFFFFFF078069FFFFFFFFFFFF
5/20	00000000000000000000000000000000

3.3.3 unlock fuid

For locked FUIDs, you can use this button to unlock them. Note that FUIDs have two different chips, and some chips cannot be unlocked



08	....	FF078069	....
09	....	FF078069	....
10	....	FF078069	....
11	....	FF078069	....
12	....	FF078069	....
13	....	FF078069	....
14	....	FF078069	....
15	....	FF078069	....

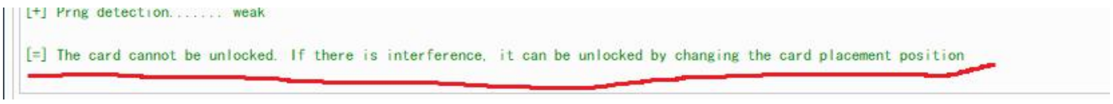
```
[+]    MIFARE Classic 1K
[=] proprietary non iso14443-4 card found, RATS not supported
[=]

[+] Magic capabilities... Gen 2 / CUID
[+] Magic capabilities... Gen 4 GDM / USCUID ( Gen4 Magic Wakeup )
[+] Magic capabilities... Write Once / FUID
[+] Prng detection....... weak

[?] Hint: use `hf mf` commands

[=] Unlock Done
```

For cards that cannot be unlocked, there will be the following prompt

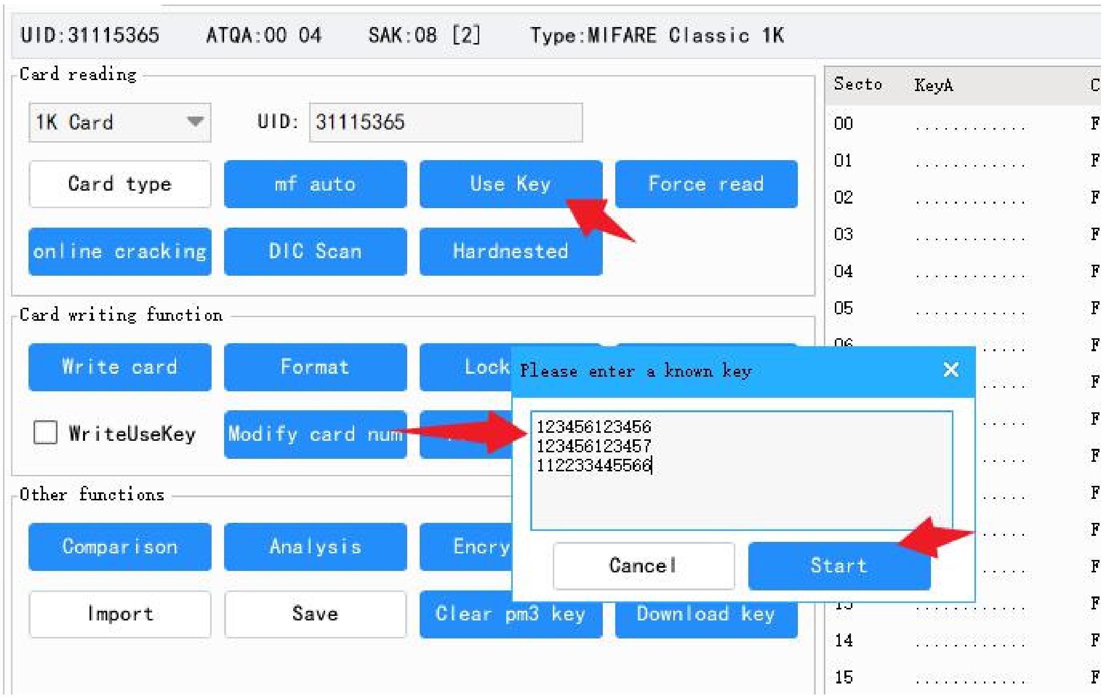


```
[+] Prng detection....... weak

[=] The card cannot be unlocked. If there is interference, it can be unlocked by changing the card placement position
```

3.3.4 USE key

Left click on 'USE KEY' and enter a known password to crack the card. Multiple passwords can be entered using the enter key



UID:31115365 ATQA:00 04 SAK:08 [2] Type:MIFARE Classic 1K

UID: 31115365

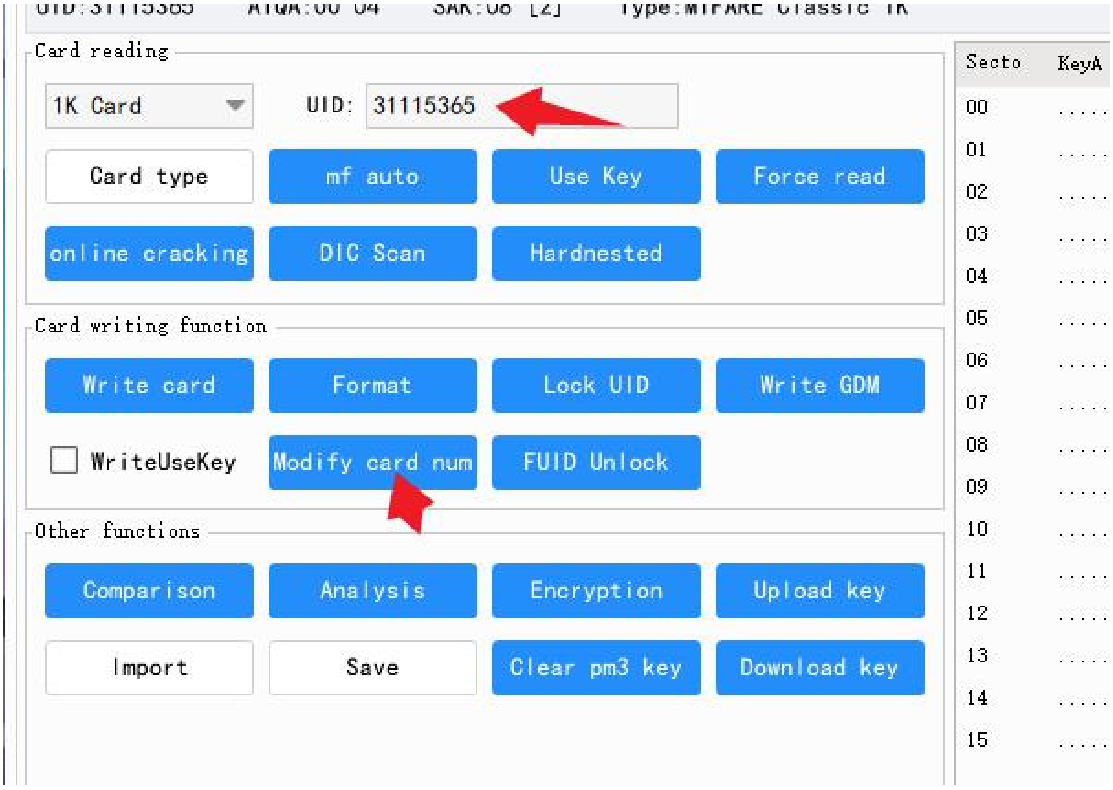
Please enter a known key

```
123456123456
123456123457
112233445566
```

Secto	KeyA	C
00	....	F
01	....	F
02	....	F
03	....	F
04	....	F
05	....	F
06	.....	F
	.....	F
	.....	F
	.....	F
	.....	F
	.....	F
	.....	F
13	....	F
14	....	F
15	....	F

3.3.5 Modify card num

First, enter the card to be modified, which must be four bytes long. Then click the button to modify the card number of UID \ UID \ FUID \ UFUID card



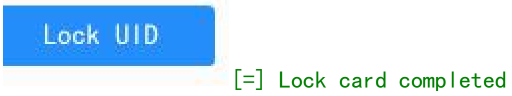
```
UID:31115365   ATQA:00 04   SAK:08 [2]   Type:MIFARE Classic 1K
```

UID: 31115365

Secto	KeyA
00	.....
01	.....
02	.....
03	.....
04	.....
05	.....
06	.....
07	.....
08	.....
09	.....
10	.....
11	.....
12	.....
13	.....
14	.....
15	.....

3.3.6 LOCK uid

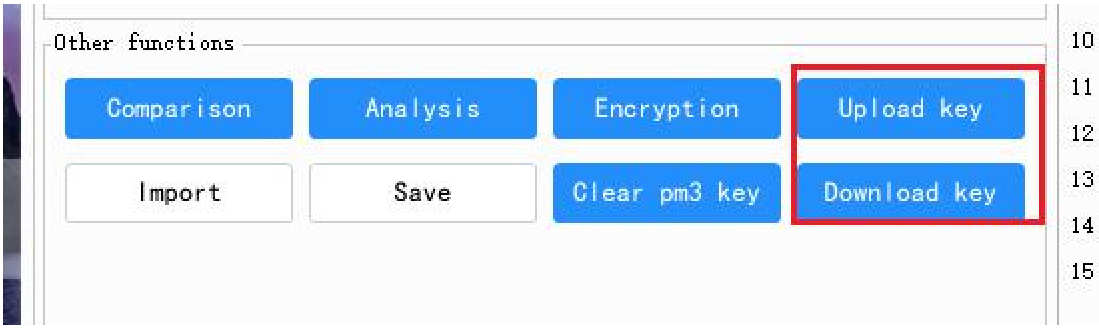
If you have used UFUID, you can lock it by clicking this button after modifying the card number



```
[=] Lock card completed
```

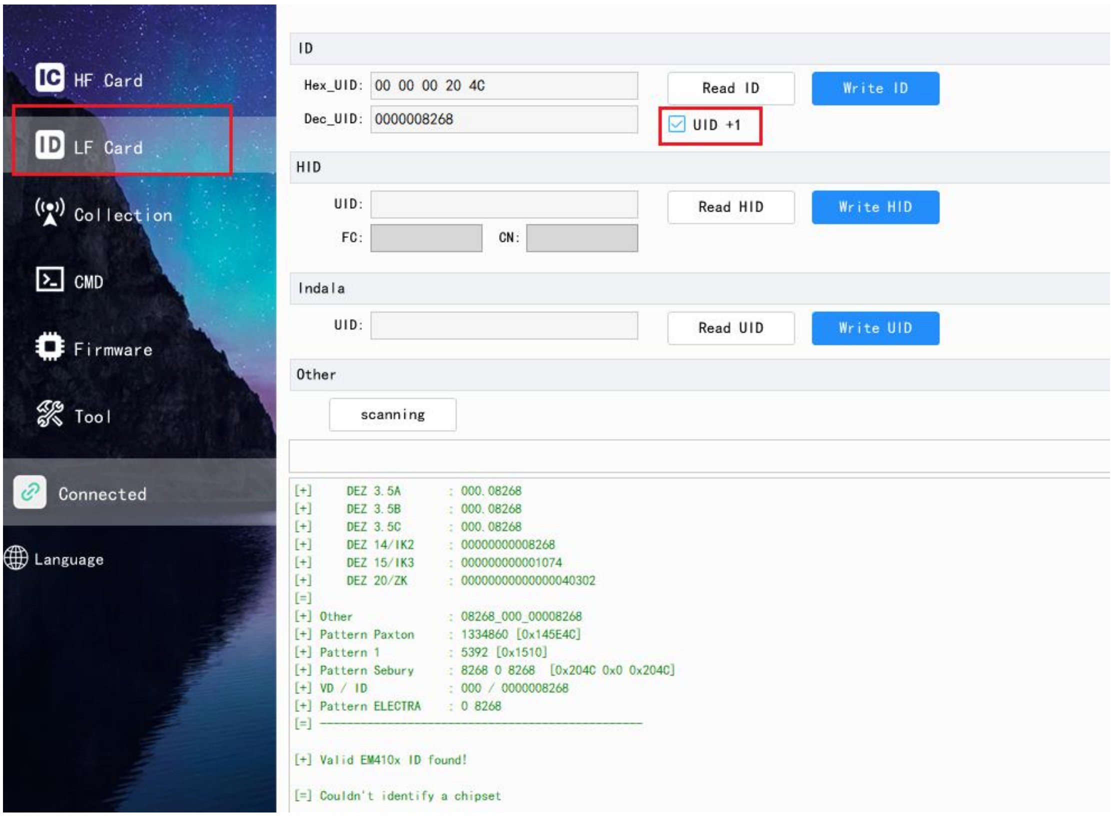
3.3.7 Upload and download keys

When you click the UPLOAD KEY button, the software will back up all passwords in the user folder and store them in the FLASH chip. When you need to download, click the Download key button, and the downloaded password will be saved in the key.dic file in the user folder. You can click the DIC scan button to scan the dictionary



3.3.8 LF CARD

For the EM4100 card, the software supports cloning the EM4100 using 5200, 5577, 8211, 8310, and 8268. If you select UID+1, the card number will automatically+1 each time it is written



Hex_UID: 00 00 00 20 4C

Dec_UID: 0000008268

☑ UID +1

UID:

FC: CN:

UID:

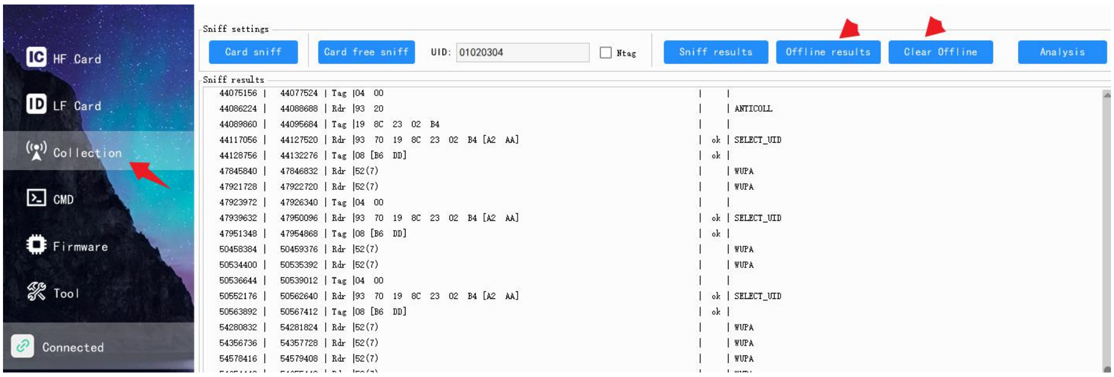
```
[+]     DEZ 3.5A         : 000.08268
[+]     DEZ 3.5B         : 000.08268
[+]     DEZ 3.5C         : 000.08268
[+]     DEZ 14/IK2       : 00000000008268
[+]     DEZ 15/IK3       : 000000000001074
[+]     DEZ 20/ZK        : 00000000000000040302
[=]
[+] Other                : 08268_000_00008268
[+] Pattern Paxton       : 1334860 [0x145E4C]
[+] Pattern 1            : 5392 [0x1510]
[+] Pattern Sebury       : 8268 0 8268  [0x204C 0x0 0x204C]
[+] VD / ID              : 000 / 0000008268
[+] Pattern ELECTRA      : 0 8268
[=] ------------------------------------------------------------

[+] Valid EM410x ID found!

[=] Couldn't identify a chipset
```

3.3.9 SNIFFING

In addition to online sniffing, the firmware of the device supports offline sniffing of 14A cards. After sniffing, sniffing records can be extracted. If you need to clear the records, you can click the clear button. Unplug the device and power it on. Press and hold the side button for three seconds. When the four different colored lights start flashing, release the button. At this time, the green light will remain on, and offline sniffing can begin. After sniffing is complete, press the side button once, the green light will flash three times, disconnect the power, go back to the computer software, reconnect the device, and extract sniffing records.

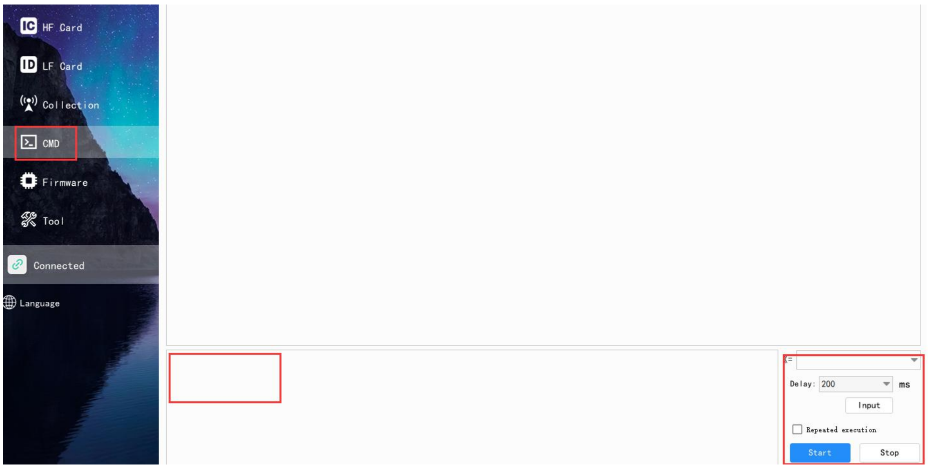


UID: 01020304

```
44075156 |  44077524 | Tag |04  00                                  |    |
44086224 |  44088688 | Rdr |93  20                                  |    | ANTICOLL
44089860 |  44095684 | Tag |19  8C  23  02  B4                      |    |
44117056 |  44127520 | Rdr |93  70  19  8C  23  02  B4 [A2  AA]     | ok | SELECT_UID
44128756 |  44132276 | Tag |08 [B6  DD]                             | ok |
47845840 |  47846832 | Rdr |52(7)                                   |    | WUPA
47921728 |  47922720 | Rdr |52(7)                                   |    | WUPA
47923972 |  47926340 | Tag |04  00                                  |    |
47939632 |  47950096 | Rdr |93  70  19  8C  23  02  B4 [A2  AA]     | ok | SELECT_UID
47951348 |  47954868 | Tag |08 [B6  DD]                             | ok |
50458384 |  50459376 | Rdr |52(7)                                   |    | WUPA
50534400 |  50535392 | Rdr |52(7)                                   |    | WUPA
50536644 |  50539012 | Tag |04  00                                  |    |
50552176 |  50562640 | Rdr |93  70  19  8C  23  02  B4 [A2  AA]     | ok | SELECT_UID
50563892 |  50567412 | Tag |08 [B6  DD]                             | ok |
54280832 |  54281824 | Rdr |52(7)                                   |    | WUPA
54356736 |  54357728 | Rdr |52(7)                                   |    | WUPA
54578416 |  54579408 | Rdr |52(7)                                   |    | WUPA
```

3.4 CMD Instructions and macros

You can set different parameters to let the software loop through certain instructions.

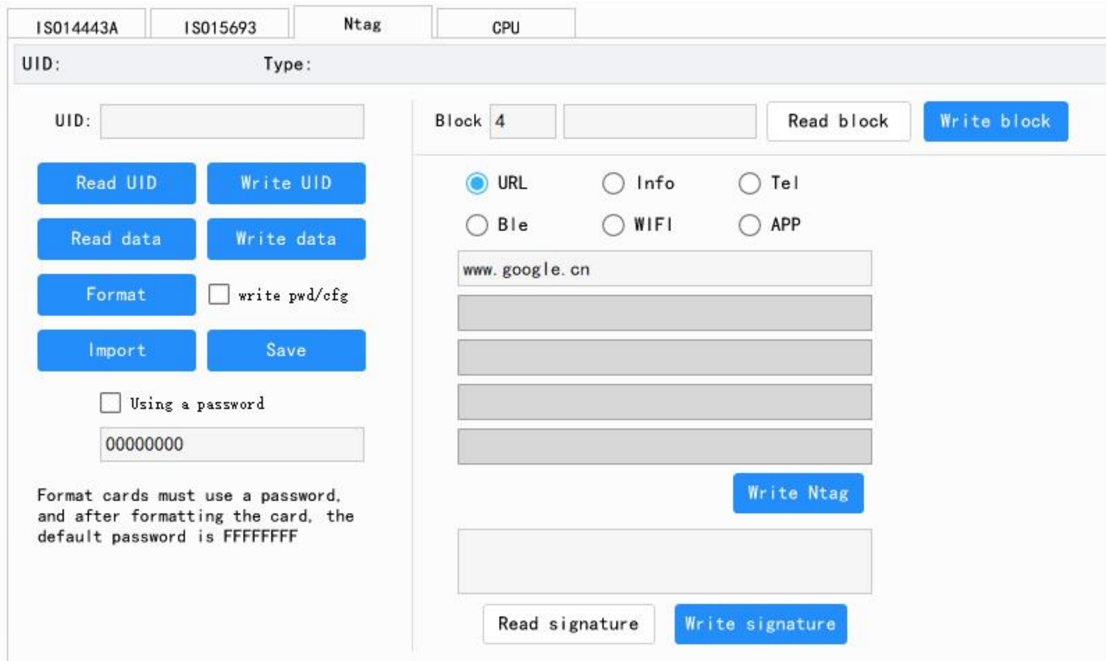


Delay: 200 ms

□ Repeated execution

3.5 NTAG CRAD

The software supports reading and writing the signature of NTAG cards. Please note that modifying the signature and card number requires using "Copy Card". And it supports writing website addresses, phone numbers, and other information



UID: Type:

UID:

Block 4

● URL ○ Info ○ Tel

○ Ble ○ WIFI ○ APP

www.google.cn

□ write pwd/cfg

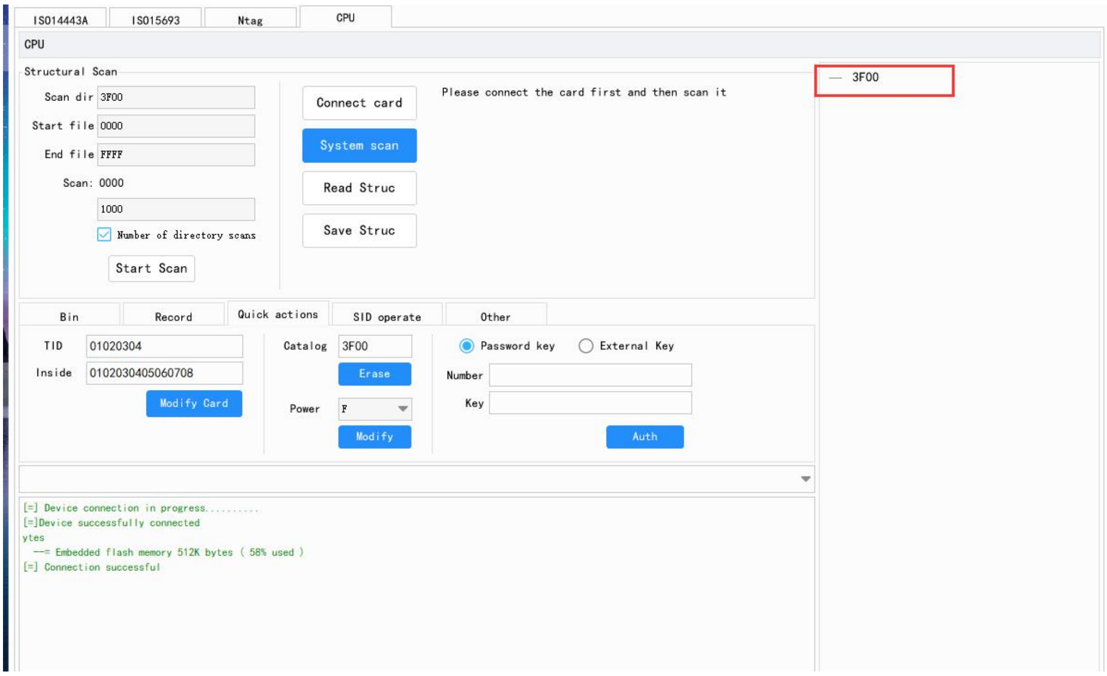
□ Using a password

00000000

Format cards must use a password, and after formatting the card, the default password is FFFFFFFF

3.6 fudan 1208-10/9

To read and write CPU cards, you need to first link the card. Start scan can scan the directory of the card. After scanning the directory and files, double-click the file name on the right side to enter the corresponding file and read the data. However, if you want to use this function, we recommend reading the technical documentation of Fudan 1208-10/9. The software supports sending APDU commands and TID/BOMB/SID cards. If you are using a new card, after linking the card, erase the directory and click on "3F00" on the right to customize the creation of a directory or file.



Scan dir 3F00

Start file 0000

End file FFFF

Scan: 0000

1000

☑ Number of directory scans

Please connect the card first and then scan it

TID 01020304

Inside 0102030405060708

Catalog 3F00

Power F

● Password key ○ External Key

Number

Key

```
[=] Device connection in progress..........
[=]Device successfully connected
ytes
  --= Embedded flash memory 512K bytes ( 58% used )
[=] Connection successful
```