

PM3Easy3.0 Quick start guide	3
I. Hardware description	4
1. Installation of equipment:	4
A. First install the copper column:	4
B. Install the board again:	5
C. Installation of low frequency antenna:	5
D. Apply protective film:.....	6
2. IC high frequency card placement:	6
3. Placement of low-frequency ID card:	7
4. Other parameters:.....	8
2. Drive installation	9
Reasons for unsuccessful drive installation and solutions:.....	12
Three. Quick test basic functions	13
1. Antenna voltage test:.....	13
2. Read high frequency card test:	14
3. Read low frequency card test:.....	14
Four. Basic knowledge of cards	16

Common cards include:.....	16
M1 S50 Introduction of the card	16
M1UID Introduction of the card	18
M1FUID Introduction of CUID card	19
Introduction of ID, HID and card.....	19

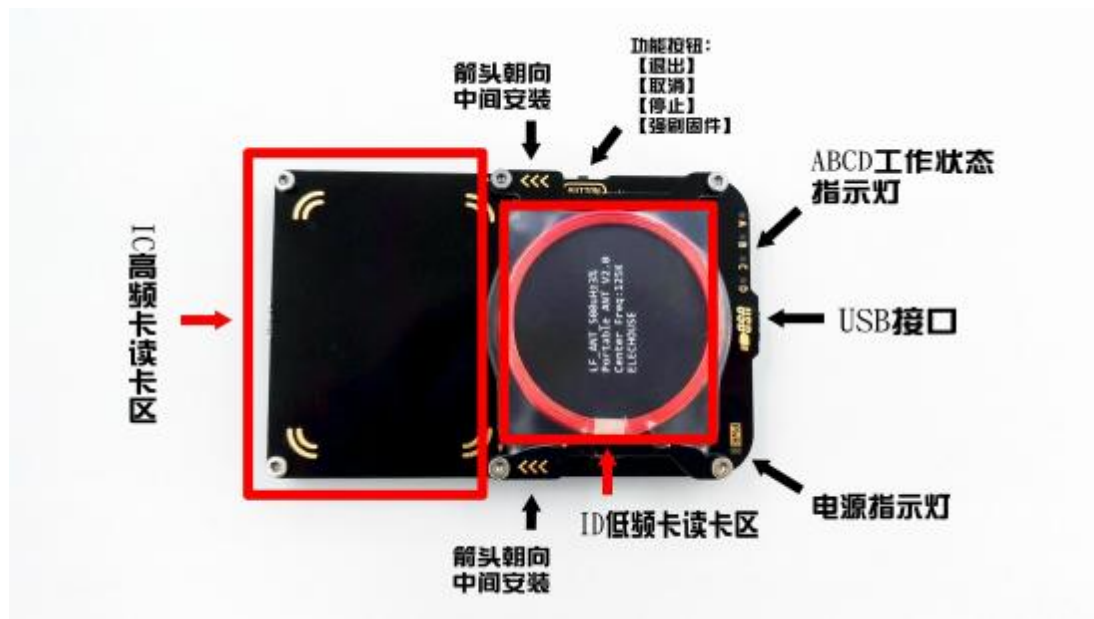
T5577 Introduction of the card	19
Card security test (can it be copied)	23
Overall process.....	23
IC card idea:.....	24
1 . Try to get any key from one of the 16 sectors on the card	24
2 . All sector keys are obtained from the known key	32
3 . Read the card data into the computer.....	34
4 . Read the card data from the computer and write it to the UID card	34
5 . Check the data and complete the cloning.....	35
VI. Operation of low-frequency card:	35
1 . Read ID, HID, INDALA, etc. cards:	35
2 . Write different types to T5577 cards to clone the card:	36
Clone as ID card:.....	36
Clone into HID card:.....	37
Clone into a INDALA card:	37
VII. Software Introduction:	38
VIII. Precautions:	38

1. Hardware matters:	38
2. Software matters:	39
a) Computer software	39
b) Device firmware	40
IX. Introduction to the Directive	40

Ten. Firmware upgrade and replacement	45
Refer to the document "Firmware Burn-in Guide V1.0.pdf"	45
Compile the firmware	45

PM3Easy3.0 Quick Start Guide

I. Hardware description



Tip: The low-frequency antenna can also be installed in the four symmetrical positions of the top, bottom, left and right, and can be selected according to your preference. In the recommended way, the two antennas have the least mutual influence.

2.IC high frequency card placement location:



The IC card is recommended to be placed on the back of the device, and the position aligned with the device is the most stable.



You can also place the card as shown above, usually no problem, and be careful to stay away from metal objects and metal tables.

Some keychains or small cards with poor signal are easy to interrupt when reading and writing. In this case, you can use the method shown in the figure below to read the card. Put the low-frequency antenna under the high-frequency antenna to solve the problem.



3.ID. Low frequency card placement location:



Just stick the card to the circular antenna

Some ID cards have poor signal, so you can install the circular antenna on the left side, and the sensitivity of reading cards will be improved

4. Other parameters:

(When installed on the right side of the low frequency antenna)

LF antenna: 29.84 V@ 125.00 kHz

LF antenna:32.31V @ 134.00 kHz

HF antenna: 28.43V @ 13.56 MHz

**(when installed on the left side of
the low-frequency antenna)**

LF antenna: 43.86 V@ 125.00

kHz # LF antenna:24.48 V @ 134.00

**kHz # HF antenna: 25.13 V@ 13.56
MHz**

Working voltage: 3.5-5.5V

Working current:50-130mA

Length and width: 54mm*86.6mm

Size and thickness: 6.2mm (thinnest) 9.8mm (with screws) 15.8

(with low frequency antenna). Firmware version at factory:

2.0.0

Drive installation

The following is an example of the installation process for W7 64. The installation may vary slightly from system to system. Please refer to the folder below

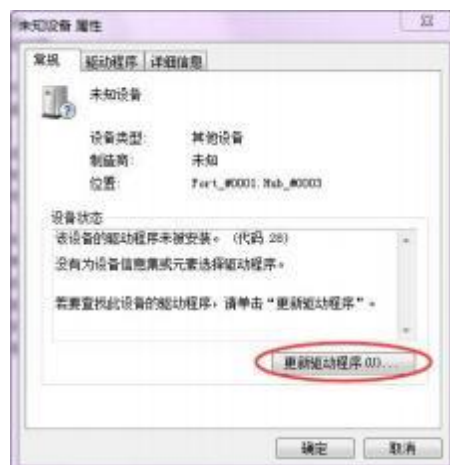


Guidance for operation.

1. Connect PM3 to the computer, right-click on unknown device in the Device Manager and click Properties



2. Click Update Driver





3. Click below

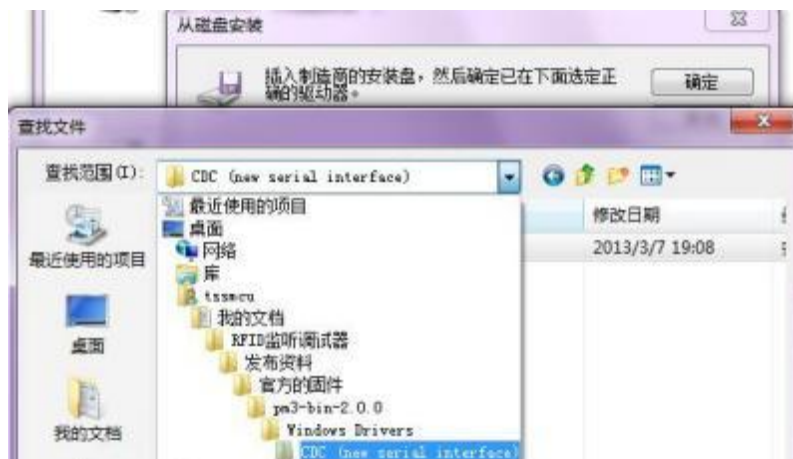
4. Click below



5. Next, install from the disk



6. Select the drive directory and select the drive file





8. Click below to complete the driver installation



If all is well, a virtual serial port will appear as shown in the following figure:

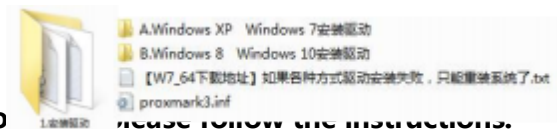


COM5 can be any number, and the driver installation is complete.

Reasons for unsuccessful drive installation and solutions:

1. The driver signature authentication is not turned off. Turn off the driver signature authentication.
2. WINDOWS may be a reduced GHOST version.
3. Virtual machines and other methods are used to connect devices.
4. The system lacks dependent files.
5. Change your computer, or try a different USB port.

If you encounter the above pro



Please follow the instructions.

PM3 compatible system: XP/W7/W7 64/W8/W10/LINUX/Android (knowledge required)

Three. Quick test basic functions

First, view the serial port in the resource manager:



Then open the file in this directory:

官方的固件 > pm3-bin-2.0.0 > win32 (client+GUI) >

double click





Open and select the corresponding serial port

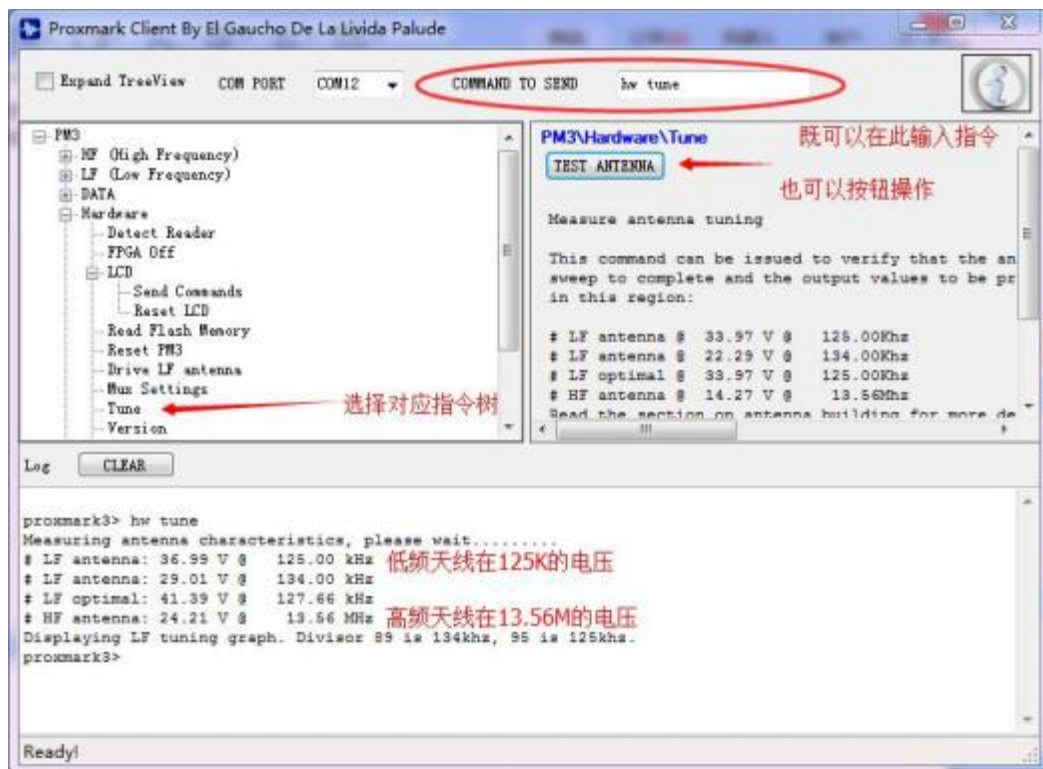
If the bottom is blank, the connection is normal.

If displayed `ERROR: invalid serial port` Indicates that the connection is not normal.

Try to reinsert the USB, select another serial port first, then plug in the USB, ding dong sound, and then select the correct serial port.

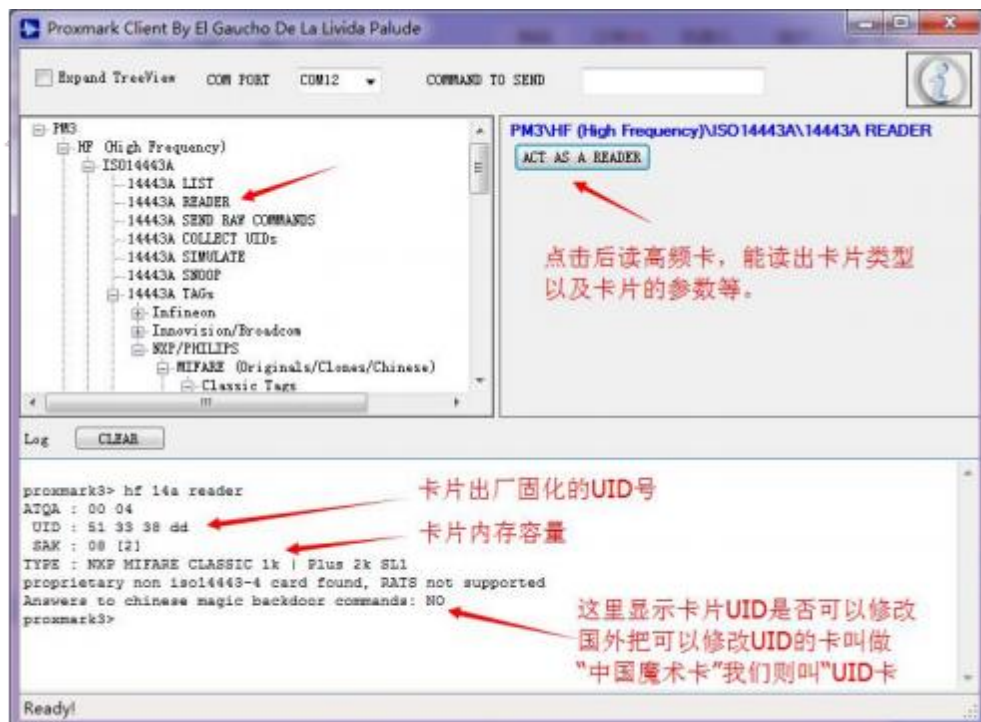
Note that if the serial port cannot be opened several times in a row, you need to close the "Proxmark3.exe" process in task manager

1. Antenna voltage test:



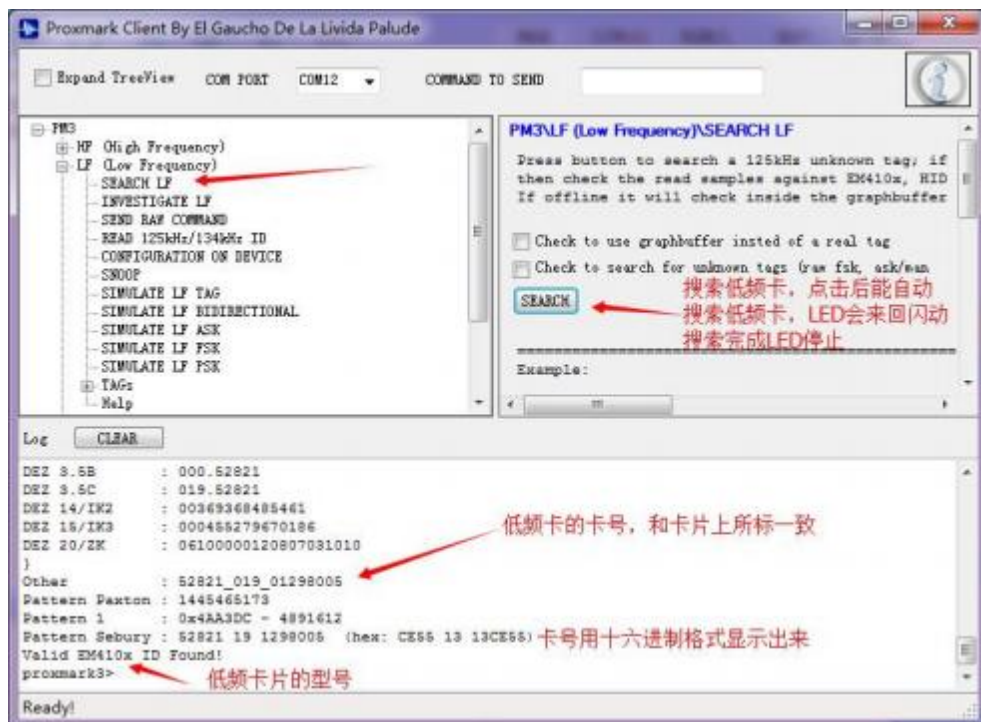
When testing the resonant voltage of the antenna, do not place cards or metals around the antenna, otherwise the measurement result will be low.

2. Read high frequency card test:



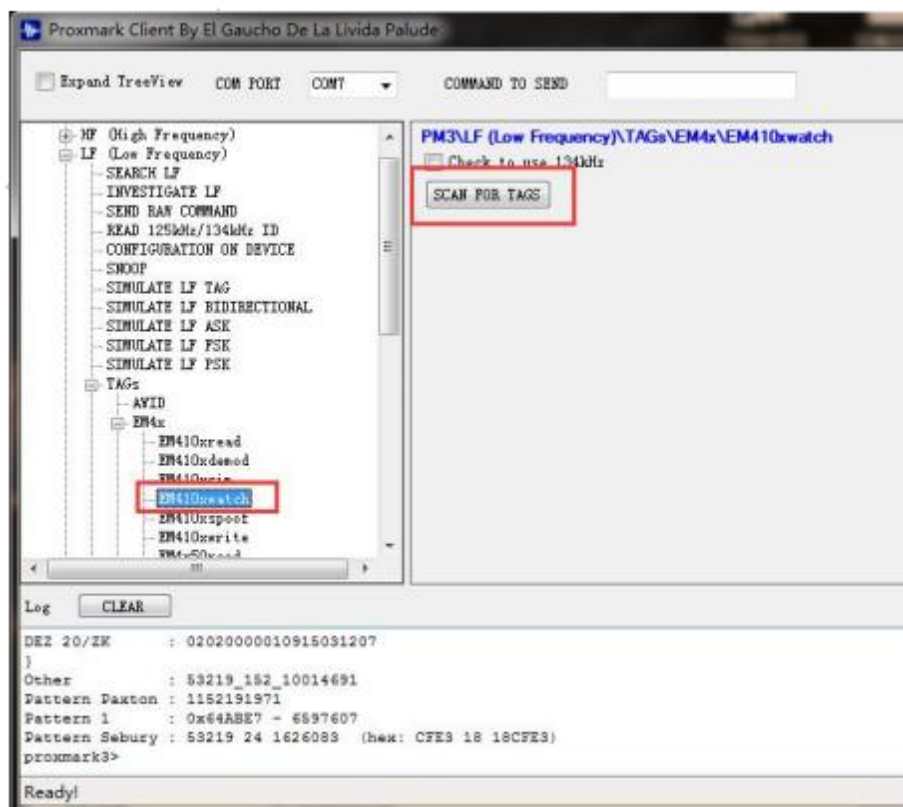
Try placing different cards such as "M1 S50" and "M1UID" on the antenna to test the cards.

3. Read low frequency card test:

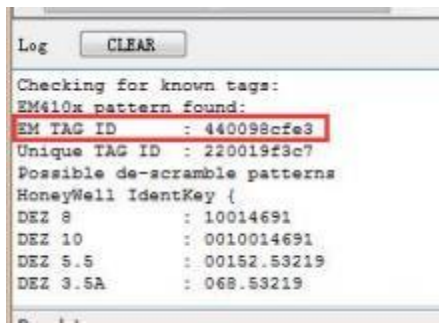


You can try to put different cards such as "HID" and "T5577" on the antenna to test the card type.

This instruction reads the ID card sensitivity is not good, some cards can not be read, you need to use another instruction to read, as shown in the figure below:



After reading it, turn the page up. As shown in the figure below, the red box is the ID card number:



Note: Some T5577 cards cannot be read before they are not initialized. We need to write an ID once, and then we can read them. Some cards have an ID number by default.

Card basics

Common cards include:

type	frequency	characteristic
Mifare S50 (M1 for short)	high frequency	The most common card, each card has a unique UID number, can store and modify data (student card, meal card, bus card, access card)
Mifare UltraLight (short for M0)	high frequency	Low cost card, factory solidified UID, can store modified data (subway card, bus card)
MifareUID (Chinese magiccard) (short for UID card)	high frequency	A variant of the M1 card that can modify the UID is called the Chinese magic card abroad and can be used to fully clone the data of the M1 S50
EM4XX (ID card)	LF	Commonly used solidified ID card, factory solidified ID, can only read but not write (low cost access card, community access card, parking lot access card)
T5577 (referred to as a modifiable ID card)	LF	It can be used to clone ID cards. The factory is empty card, and there are sectors that can also store data. Some sectors can be set with passwords.

HID ProxII (short for HID)	LF	Low frequency cards commonly used in the United States can be erased and written, but are not compatible with other cards
----------------------------	----	---

M1 S50 Introduction of the card.

M1 S50 is the most commonly used card in China, which is commonly known as IC card.

Developed by NXP (NXP) under Philips, there is also a compatible card in China, but the card information cannot be determined. The card information is as follows:

```
proxmark3> hf 14a reader
ATQA : 00 04
UID : b2 a6 de 1d
SAK : 08 [2]
TYPE : NXP MIFARE CLASSIC 1k | Plus 2k SL1
proprietary non iso14443-4 card found, RATS not supported
Answers to chinese magic backdoor commands: NO
proxmark3> |
```

When you see TYPE: NXP MIFARE CLASSIC 1k | Plus 2k SL1,

it means this is an M1S50 card.

The card is like a small U disk, inherently encrypted. The password cannot be canceled.

The factory will set the password to the default password that everyone knows, FFFFFFFF. It is convenient to use.

扇区	块	数据
0	0	BC59FC0F160804000138E31F63B2971D
0	1	00000000000000000000000000000000
0	2	00000000000000000000000000000000
0	3	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFFFF
1	4	00000000000000000000000000000000
1	5	00000000000000000000000000000000
1	6	00000000000000000000000000000000
1	7	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFFFF
2	8	00000000000000000000000000000000
2	9	00000000000000000000000000000000
2	10	00000000000000000000000000000000
2	11	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFFFF
3	12	00000000000000000000000000000000
3	13	00000000000000000000000000000000
3	14	00000000000000000000000000000000
3	15	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFFFF

As shown above, this is a data structure of a card. There are 16 sectors in total, and each sector consists of 4 blocks. The first three blocks are used to store data, and the last block is used to store the password. Just like an encrypted small U disk, each sector has two passwords to manage together.

Screenshot of single sector data:



You can see that there are four rows in this sector, and each row is a block, and the first three blocks are for storing data.

The fourth block stores the passwords. The two yellow circles represent Password A and Password B, respectively. The four bytes in the middle are control words used to manage password permissions, similar to the password settings options in a safe, which are used to set up functions for Password A and Password B. By default, if not modified, all data can be read and written using Password A. Password A cannot be read out, but Password B can be used with Password A

The password was read out.

Although the password is stored there, the password may not be readable, which is determined by the control word. See the detailed comparison table Settings Table in the [Card Information] folder.

Except for the first sector, which is slightly different, the other 15 sectors are exactly the same. The following figure shows the structure of the first sector:



The red circle is the card UID number, which is a unique and unchangeable ID sequence for each card. It can be read without a password. The rest of the data in block 0 of the first sector is built-in by the manufacturer, including the manufacturer and card information. It cannot be modified. It can only be read.

M1UID Introduction of the card

M1UID Card is a variant card specially designed for M1S50 Card by Chinese people. It works exactly like M1S50 Card, except it has an additional feature: the data in Block 0 can be modified at will. Therefore, the UID number and manufacturer information can also be changed at will, which is why it is called a UID card.

```
proxmark3> hf 14a reader
ATQA : 00 04
UID : a2 f7 90 76
SAK : 08 [2]
TYPE : NXP MIFARE CLASSIC 1k | Plus 2k SL1
proprietary non iso14443-4 card found, RATS not supported
Answers to chinese magic backdoor commands: YES
proxmark3> |
```

As shown in the figure, "YES" indicates that it is a UID card. However, some UID cards with poor compatibility will show NO. The cards with poor compatibility can be written by both kinds of software, but when reading data, the Chinese GUI cannot read it, while the English GUI can read the incomplete data of the last block.

The advantage of this modification is that you can perfectly copy the M1 S50 card and make the UID number exactly the same. Read this way

If the card is jammed, there is no problem if the UID number is verified.

The data of the card modification 0 sector 0 block is entered into the factory mode by instructions, and any data on the whole card can be edited directly. The card can be read and written without a password, and it is not afraid of writing the card wrong. Even if the 0 block or the sector control word is written incorrectly, it can be repaired at any time without affecting subsequent use. Therefore, it is widely used and deeply loved by people.

However, the disadvantage is that the new card reading system can detect UID cards by detecting the response of the card to special instructions, so it can refuse the access of UID cards to achieve the function of shielding copy cards. However, after all, it is still a minority.

M1FUID Introduction of CUID card

The FUID card is an optimized version of the UID card made by Chinese people. As mentioned above, the UID card is detected and thus blocked. The FUID card is a non-backdoor, modifiable UID card. Its 0th sector, 0th block data can only be modified once in its lifetime. Apart from this, it is identical to the M1 standard card, making it difficult to detect and block.

The CUID card is an optimized version of the FUID card. As mentioned above, since it can only write to block 0 once, if written incorrectly or reused, it becomes very difficult. Therefore, the CUID card allows for repeated modifications to block 0. However, unlike the UID card, it has no backdoor and can be written to block 0 using regular password verification methods. Other sectors are identical to those

on a standard M1 card. The downside is that there is still a possibility of detection. Additionally, if the verification bit of the UID number is accidentally written incorrectly, leading to an inability to read the card, the card cannot be repaired and must be scrapped.

Note that PM3 can write the above two cards, but the official English software can only manually write the card one by one, while our Chinese GUI software can directly write the data file into the card, which is convenient for use.

ID, HID, card introduction

The ID card is our common name. The full name of the internal chip is called EM4100 or EM41XX, which is a low-frequency card. Each card has a unique ID number when it leaves the factory and cannot be rewritten. The HIDProxcard card is similar.

T5577 Introduction of the card

T5577 A card is a low-frequency card that can be written with data and encrypted. The most special thing is that writing an ID number can turn it into an ID card, writing an HID number can turn it into an HID card, and writing a Indala card number can turn it into a Indala card.

Lets first write 5577 into ID: 11 11111111, at this time 5577 has been transformed into an ID card, and then use the read 5577 full card data instruction to see the full card data:

```
proxmark3> lf t55xx detect
Modulation : ASK
Bit Rate   : 5 - RF/64
Inverted    : No
Offset      : 1
Block0      : 0x00148040
proxmark3> lf t55xx dump
0x00148040  000000000000101001000000001000000 [0]
0xFF8C6318  11111111100011000110001100011000 [1]
0xC6318C60  11000110001100011000110001100000 [2]
0x00000000  00000000000000000000000000000000 [3]
0x00000000  00000000000000000000000000000000 [4]
0x00000000  00000000000000000000000000000000 [5]
0x00000000  00000000000000000000000000000000 [6]
0x00000000  00000000000000000000000000000000 [7]
```

As shown in the figure above, after writing the ID, the first three blocks of the card will be automatically calculated by PM3 and written to achieve the transformation effect.

Do not look at the 0s and 1s at the back; only look at the data in front. 5577 consists of 8 blocks, each capable of storing only 8 digits. The 0th block is used to set the card type and modulation method, determining whether it is an ID card or a HID card. Any arbitrary modification will result in the card being unreadable. The 7th and final block, when unencrypted, is the data area; after encryption, its data becomes the password.

Note: Sometimes the 5577 card does not respond after writing the ID, and the ID number cannot be read back on the PM3. This indicates that the card reader has a firewall, which is specially designed to prevent ID duplication. In this case, the 5577 card must be encrypted before passing through the firewall.

ID card: 0 block write: 00148040 no
password

00148050
Encryption

HID card: 0 block write:

00107060 no
password
00107070
encryption

Encryption steps for ID card:

Write ID number-> read 57 full card data (see
password) -> write 0 block data-> read full card
data again (verification) -> complete

The method to read the unencrypted 5577 full card data with PM3:

The screenshot shows the Proxmark Client software interface. The left pane displays a tree view of commands under the 'PM3' category, with 'T55XX DUMP' selected. The right pane shows the 'PM3\LF (Low Frequency)\TAGs\T5' section with a 'Password:' field and a 'DUMP' button. A red arrow points to the 'DUMP' button with the text '如果没加密 不用填 加密卡填写 密码' (If not encrypted, no need to fill; for encrypted cards, fill in the password). Another red arrow points to 'T55XX DUMP' in the tree view with the text '先检测卡片配置' (First detect card configuration). A third red arrow points to the 'T55XX DUMP' command in the command list with the text '再读全卡' (Then read the full card). The bottom pane shows the command log with the following text:

```
proxmark3>
proxmark3> if t55xx detect
Modulation : ASK
Bit Rate   : 5 - RF/64
Inverted    : No
Offset     : 1
Block0     : 0x00148040
proxmark3>
proxmark3> if t55xx dump
0x00148040 0000000000001010010000000001000000 [0]
0xFF8CC529 1111111100011001100010100101001 [1]
0x4A5294A4 01001010010100101001010010100100 [2]
0x56565656 01010110010101100101011001010110 [3]
0x00000000 000000000000000000000000000000 [4]
0x00000000 000000000000000000000000000000 [5]
0x00000000 000000000000000000000000000000 [6]
0x00000000 000000000000000000000000000000 [7]
proxmark3>
```

Red arrows point to the log output with the following text:

- '检测到的配置' (Detected configuration) points to the 'if t55xx detect' command and its output.
- '读出的数据' (Read data) points to the 'if t55xx dump' command and its output.
- '密码' (Password) points to the last line of the dump output, '0x00000000 000000000000000000000000000000 [7]'.

Note that if encryption 5577 is not detected, or all blocks read are identical data.

Remove encryption write 5577 card:

Proxmark Client By El Gaucho De La Livia Palude

Expand TreeView COM PORT COM7 COMMAND TO SEND

PM3

- HF (High Frequency)
- LF (Low Frequency)
 - SEARCH LF
 - INVESTIGATE LF
 - SEND RAW COMMAND
 - READ 125kHz/134kHz ID
 - CONFIGURATION ON DEVICE
 - SNOOP
 - SIMULATE LF TAG
 - SIMULATE LF BIDIRECTIONAL
 - SIMULATE LF ASK
 - SIMULATE LF FSK
 - SIMULATE LF PSK
- TAGs
 - AWID
 - EM4x
 - FLEXPASS
 - MID
 - INDALA
 - ioProx (Kantech)
 - TI (Texas Instruments)
 - MITAG
 - VERICHIP DEMODULATE
 - T55XX
 - T55XX READ BLOCK
 - T55XX WRITE BLOCK**
 - T55XX READ TRACE
 - T55XX READ INFORMATION
 - T55XX DETECT
 - T55XX CONFIG
 - T55XX DUMP
 - T55XX SPECIAL
 - T55XX Help
 - PARADOX
 - PCF7931

PM3\LF (Low Frequency)\TAGs\T55XX

Block: 0

Data to Write: 00148040

Password: 00000000

WRITE BLOCK

填入加密时的密码。
也就是最后一块的数据

Log CLEAR

```
proxmark3> lf t55xx wr 0 00148040 00000000
Writing to block: 0 data : 0x00148040
pwd : 0x00000000
proxmark3>
```

写卡是单向的，无法看出是否成功

The following table from RADIOWAR clearly shows the support for cards by PM3

名称	识别	读/写	高级操作						备注
			离线解密	在线监听	默认密钥	数据导出	模拟	复制	
MIFARE CLASSIC	✓	✓	✓	✓	✓	×	✓	✓	
MIFARE CLASSIC(Chinese Magic Card/UID)	✓	✓	×	✓	✓	✓	×	✓	
MIFARE Ultralight	✓	✓	×	×	×	✓	×	×	
HID	✓	✓	×	×	×	×	✓	✓	
HID iClass	✓	✓	✓	✓	×	✓	✓	✓	
iso14443a	✓	✓	×	✓	×	✓	✓	✓	
iso14443b	✓	✓	×	✓	×	×	✓	✓	
iso15693	✓	✓	×	✓	×	✓	✓	✓	
SR1512	✓	✓	×	×	×	×	✓	×	
SR1X4K	✓	✓	×	×	×	×	✓	×	
Legic	✓	✓	×	×	×	✓	✓	×	
epa	✓	✓	×	×	×	×	×	×	
em410x	✓	✓	×	×	×	×	✓	✓	
em4x50	✓	✓	×	×	×	✓	✓	✓	
Ti	✓	✓	×	×	×	×	×	×	
Hitag/Hitag2	✓	✓	×	✓	×	×	✓	×	
Indala	✓	✓	×	×	×	×	×	✓	
T55xx	✓	✓	×	×	×	×	×	✓	
FlexPass	✓	✓	×	×	×	×	×	×	
VeriChip	✓	✓	×	×	×	×	×	×	
PCF7931	✓	✓	×	×	×	×	×	×	
Kantech ioProx	✓	✓	×	×	×	×	×	×	

Proxmark3功能在开源社区的不断维护下，几乎每年都会增加一些新的RFID的操作功能，现在列出来的只是功能当中显示存在的。复制卡数据和复制UID有本质上区别，所以“高级操作”当中的“复制”不可作为其类型RFID不可被其他兼容类RFID复制或模拟。

RADIOWAR
Professional RF Tools and Software

This table is only for reference. Most cards are rarely seen in China, so they have not been tested.

Card security test (can it be copied)

Overall process

Read the card to determine whether it is an ID card or an IC card.

Note that the shape of the card is independent of the model, and the same chip can be packaged into completely different shapes:



ID card: read the ID number of the card → replace it with a T5577 card → write the ID number into the card → complete

IC card: decrypt the vulnerability-> read all the data of the card-> replace with UID card-> write the data into the card-> complete

IC card idea:

1. Obtain the key to any sector (any of the following is acceptable)

A PRNG vulnerability allows an attacker to obtain the key to a sector

b. The key is obtained by scanning the default password

c. The sniffing card reader and the card interact with each other to obtain the key

d. Capture the key after simulating the card swiping on M1 card (pick reading card machine, poor compatibility)

2. Use the MFOC vulnerability to find all the sector keys with known sector keys. 3. Read the card data with the cracked keys and import it into the computer

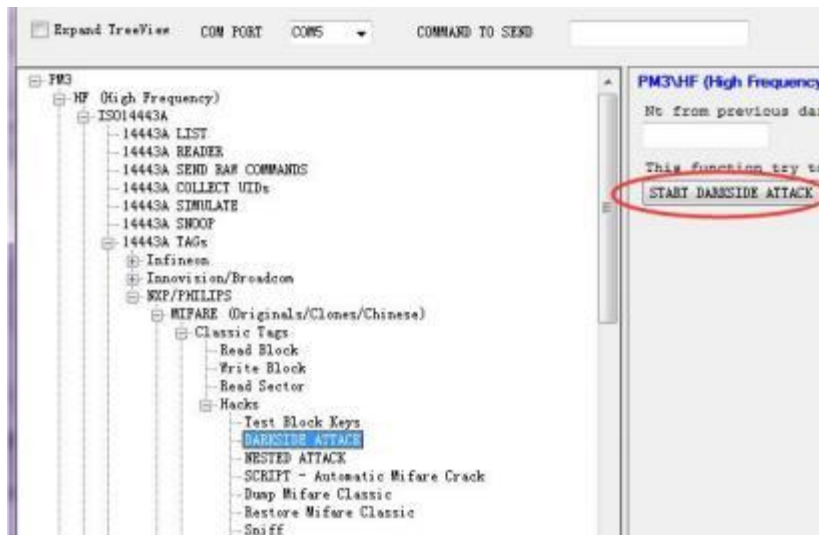
4. Put the empty UID card and write the data in the computer into the card

1. Try to obtain any key from one of the 16 sectors of the card

There are four ways, and any one of them can proceed to the next step if the key is obtained.

A) (Only the card is required) Access to the 0 sector key is obtained unconditionally through the PRNG vulnerability attack.

i. Send the instruction hf mf mifare, or click on the instruction tree in DARKSIDE ATTACK



After clicking to start the attack, the card cannot be attached to the middle of the antenna, it needs to move to the edge until ABD flashes, indicating that the card can be cracked, keep the position unchanged, and wait.

```
p1:2c465 p2:2924 p3:a key:2980113670af
p1:33746 p2:2fc3 p3:b key:06be1e44e553
key_count:12
-----
Key found:ffffffffffff
Found valid key ffffffffffffff
proxmark3>
```

After completion, the result shown in the figure will be displayed. The key of sector 0 is in the red box.

If the card does not support, or does not put the card, after ten seconds, the card will crash, and you can reconnect PM3. You can practice with the free M1 S50 first.

ii. matters need attention:

Not all cards can be cracked, sometimes you have to take a chance.

The UID card does not support cracking, nor does it need cracking. The data can be read directly without a password.

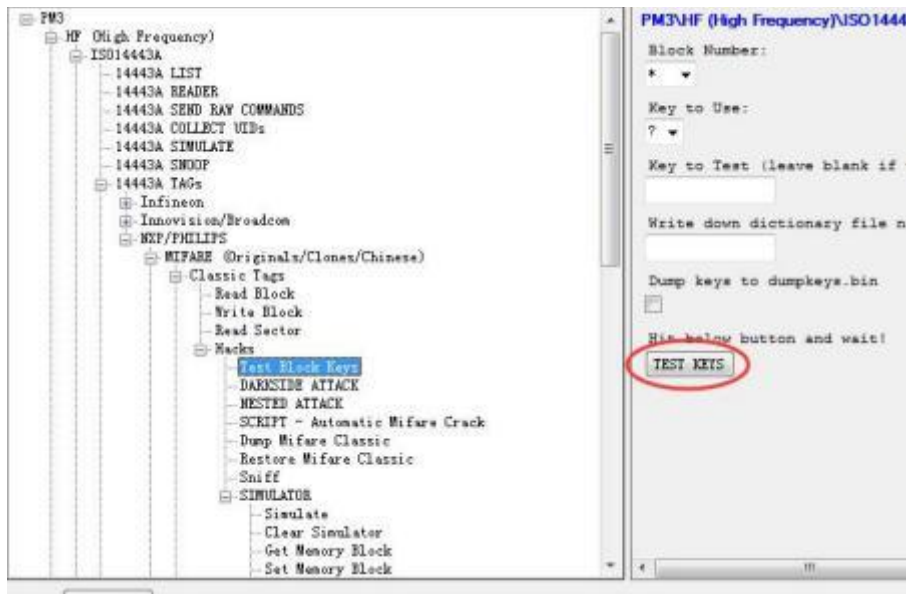
iii. principle:

首先（**PRNG安全缺陷**），国外的安全研究人员发现，MIFARE Classic采用的是Crypto-1私有加密算法，其算法的特点就是对称式的密码算法或者说是私钥密码系统。其主要组成部分是伪随机数发生器（PRNG）、48位的线性反馈移位寄存器（LFSR）以及非线性函数。由于算法当中的Filter Function的设计出现缺陷，导致改变线性反馈移位寄存器的后8位数值就有可能得到所对应的Keystream。这个缺陷类似于802.11b WEP算法，不同的明文有极高的可能性被相同的Keystream，使得整个加密算法出现了漏洞。

If you are interested in understanding the cracking mechanism, you can refer to the paper "The-MIFARE-Hack-1.PDF", which is very detailed.

b) Use the default password commonly used by the card manufacturer to test the card and scan the sector to see if there is a default key.

i. Send instruction: hf mf chk *? , Or click on the Test Block Keys in the instruction tree



Place the card first and scan the default password

```
No key specified, trying default keys
chk default key[ 0] ffffffff
chk default key[ 1] 000000000000
chk default key[ 2] a0a1a2a3a4a5
chk default key[ 3] b0b1b2b3b4b5
chk default key[ 4] aabbccddeeff
chk default key[ 5] 4d3a99c351dd
chk default key[ 6] 1a982c7e459a
chk default key[ 7] d3f7d3f7d3f7
chk default key[ 8] 714c5c886e97
chk default key[ 9] 587ee5f9350f
chk default key[10] a0478cc39091
chk default key[11] 533cb6c723f6
chk default key[12] 8fd0a4f256e9
--sector: 0, block: 3, key type:A, key count:13
Found valid key:[ffffffff]
--sector: 1, block: 7, key type:A, key count:13
Found valid key:[ffffffff]
--sector: 2, block: 11, key type:A, key count:13
Found valid key:[ffffffff]
```

As shown in the figure, the top 12 common default passwords recorded in the dictionary will be used to verify the card in turn. If the red box shows "Found validkey: [ffffffff]" it means that the corresponding key has been found, and the key content is "ffffffff", and the square above is the sector number corresponding to the key.

If the card does not have a default key, there will be no such prompt.

ii. matters need attention:

Sometimes the default key scan may have a small BUG, so be sure to verify the results before trusting them.

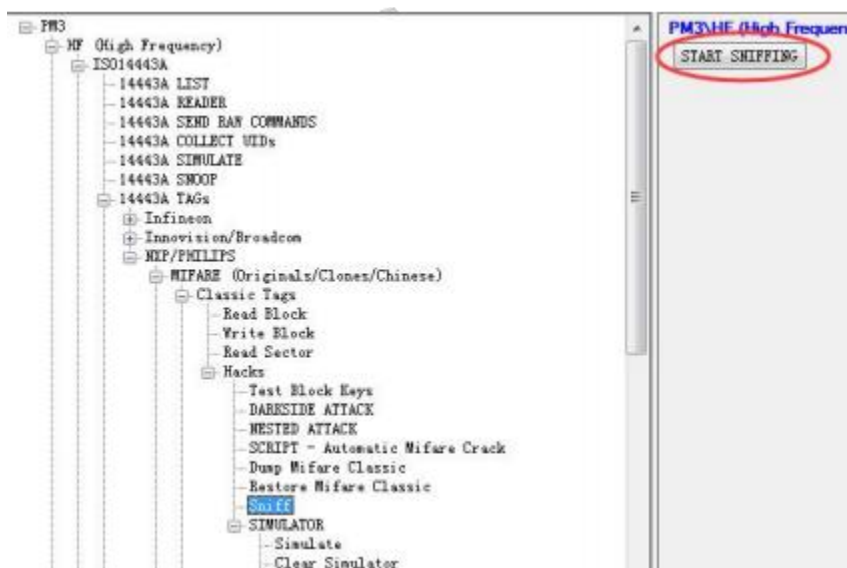
iii. principle

12 sets of default keys for cards manufactured worldwide are stored and tested in sequence. The default value for domestic cards is generally "ffffffffffff".

c) (On-site) Place the antenna between the card and the card reader to sniff the communication data and solve a sector key.

i. Send the command: hf mf sniff, or click Sniff or SNOOP in the command tree

The password obtained by sniffing cannot be specified. Only when the card reader accesses which sector of the card can it obtain which password. When other passwords cannot be obtained, only the data of these sectors need to be copied for use, without copying the whole card data.



After clicking to start sniffing, the PM3 high-frequency card reading area is sandwiched between the card and the card reader, and then the card is swiped. The three cannot be too close to each other, and there should be no metal shielding on both sides.



In general, you can first place the PM3 very close to the card reader, keeping the positions of PM3 and the card reader unchanged. Then, repeatedly swipe the card above PM3 to obtain the most stable data. However, this will bring the card reader very close to the card. If the card reader cannot detect the card, gradually increase the distance between PM3 and the card reader until you can swipe the card normally, which will yield the best results. Adjust according to the actual situation during sniffing.

```

received trace len: 135 packages: 1
tag select uid:b2 a6 de 1d atqa:0x0004 sak:0x08
RDR(0):60 21 7e 4b
TAG(1):f8 0e ee 3c
RDR(2):4e c8 84 03 d2 dd 51 80
TAG(3):2b b1 7b 5e
RDR(4):c2 12 47 a4
TAG(5):d1 d9 0a 56 e4 ef 4e e0 f6 76 ca bb 98 a2 a6 72 46 da
RDR(6):4f 0d 44 46
  
```

Diagram illustrating the data flow during a card swipe. Red arrows indicate the direction of communication:

- From RDR(0) to TAG(1): tag challenge
- From TAG(1) to RDR(2): reader challenge response
- From RDR(2) to TAG(3): tag response

As shown above, after swiping the card once, take it away and wait for a few seconds, and the computer will return the sniffed data.

Pay attention to the data starting with 60 or 61. 60 means access using A password, 61 means access using B password. The instructions starting with RDR are issued by the card reader, and the instructions starting with TAG are issued by the card.

The red circle indicates that the card reader has accessed block 21.21 is hexadecimal, which converts to decimal 33. The first box "b2a6de1d" is the card UID

The second box "f80eee3c" is the tag challenge (card challenge number)

The third box "4ec88403" is reader challenge (Reader Challenge number) the fourth box "d2dd5180" is readerresponses (Reader Response number) and the fifth box "2bb17b5e" is tagresponses (Card Response number)

Add "crpto1gui.exe" to the software in turn. (In the "Tools" folder)



Click crackkey to calculate the key. The conclusion is that the card reader uses

A to access the 33rd block and the password used is FFFFFFFFFF

ii. matters need attention

When sniffing, the antenna must be between the card and the reader. If the order is wrong, the complete data will not be obtained.

The card reader must be the machine that reads the card on a regular basis, not necessarily the card issuing machine. If you cannot get the key, it may be that the card reader does not use the password to access the card sector, or it may be that the signal of the card reader is poor.

If you are not allowed to bring a computer on site, you need to flash the firmware to version 816 if you want to sniff offline.

The command used below is SNOOP instead of Sniff. After sending the command, turn on the power switch, unplug the USB, and bring the card close to the card reader several times until the A light turns off. Plug it back into the computer and use hf 14a list to view the data. It may reset first, but the data is still there. Wait a few seconds for the computer to beep, then

resend the hf 14a list to view the data. Never turn off the PM3 power switch, as this will result in data loss. The following figure compares the differences between the two commands.

	848 firmware down (old)		2.X.0 firmware down (new)	
	SNOOP instruct	Sniff instruct	SNOOP instruct	Sniff instruct
function	The sniffing card reader and the card complete the interaction data	not have	Sniff card reader And the card is intact Interact with data	Only decrypt is displayed The key to the M1 card data
use	Pre-empted in PM3 and used hf 14a list look over	not have	Pre-empted in PM3 and used hf list 14a look over	Its real-time on the computer It shows the decryption Key data
length	Very short	not have	fairly long	infinite
data integrity	Incomplete, easy to lose packets, pick up machines	not have	The data is complete, clear and annotated clearly	The data is complete, clear and annotated clearly
Offline records	support	not have	nonsupport	nonsupport
Record object	Supports any card for 14443A	not have	Supports any card for 14443A	Only the M1 card decryption data is extracted

Note that SNOOP does not automatically pick out the data segments. It requires manual identification of valid data segments, usually similar ones

Judging by the length and shape of the data.

481660I 492124IRd il 9370 bz a de 1 d d 7E860

As shown in the figure above, 93 70 means that the card with UID b2 a6 de1d is selected, and there are often valid data behind it. After the card reader selects the card, it is ready to access the card.

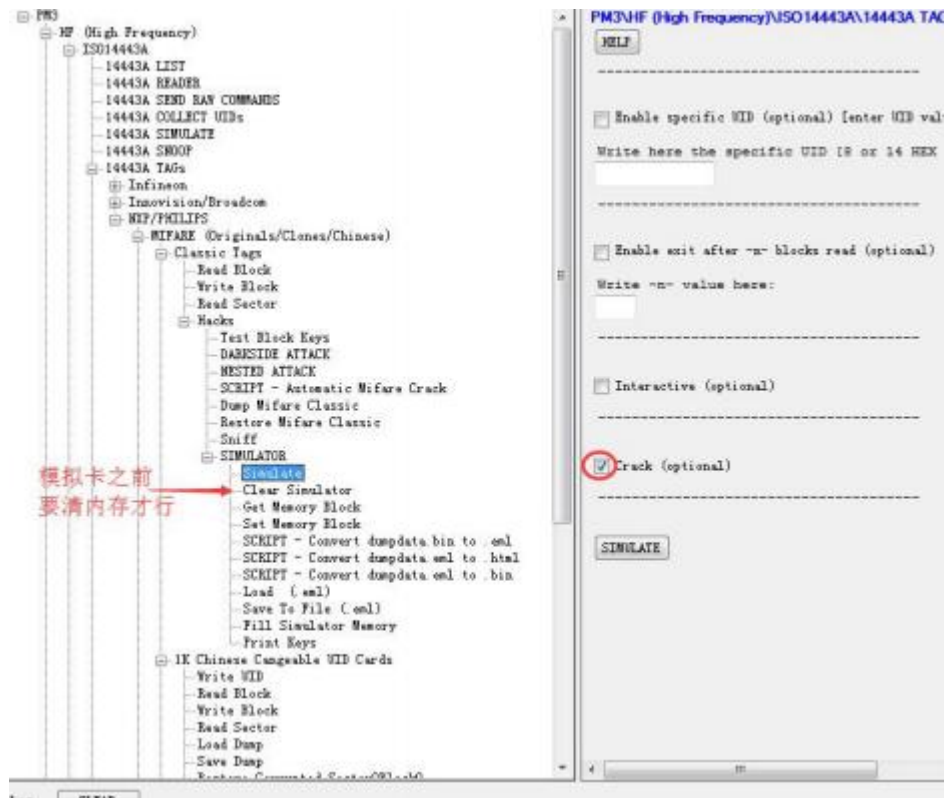
iii. principle

The M1 uses the crpto1 algorithm when the card reader and the card interact with data and passwords.

Even with the same card and the same password, the sniffed interaction data is random, but as long as you have the four sets of random arrays mentioned above, as well as the UID, you can reverse the key.

D) (On-site is required) Simulate the antenna into an M1 card, induce the card reader to read the card, capture the data, and solve a sector key.

i. Send the instruction: hf mf sim x, or click on the instruction tree for SIMULATOR



You do not need to fill in the UID that needs to be simulated on the right. PM3 will automatically select a default UID, as shown in the figure below

```
proxmark3> hf mf sim      x
uid:N/A, numreads:0, flags:8 (0x08)
proxmark3>
proxmark3> #db# 4B UID: e68487f3
```

Then approach the card reader and swipe your card. After that, press the button to exit and the data will be returned automatically. For example:

```
'mfkey32 e68487f3 01020304 91641e54 0b7b4cd4 94199bb6 b7de6d8b
```

The password can be solved by using the plug-in.

First, open the following batch file and replace the data in it with your own data.



After the replacement is completed, double click to open the batch processing and get the results:

```
C:\Windows\system32\cmd.exe
GUI>\mfkey>mfkey32.exe e68487f3 01020304 77ae4a44 70574ac4 c2685ae5 307e6516
MIFARE Classic key recovery - based 32 bits of keystream
Recover key from two 32-bit reader authentication answers only!

Recovering key for:
  uid: e68487f3
  nt: 01020304
  <nr_0>: 77ae4a44
  <ar_0>: 70574ac4
  <nr_1>: c2685ae5
  <ar_1>: 307e6516

LFSR successors of the tag challenge:
  nt': 20f8ed56
  nt'': 3c2bcdad

Keystream used to generate <ar> and <at>:
  ks2: 50afa792

Found Key: [a0a1a2a3a4a5]
```

ii. matters need attention

Note that this function is not 100%, and some card readers are not compatible, and the correct return cannot be obtained.

iii. principle

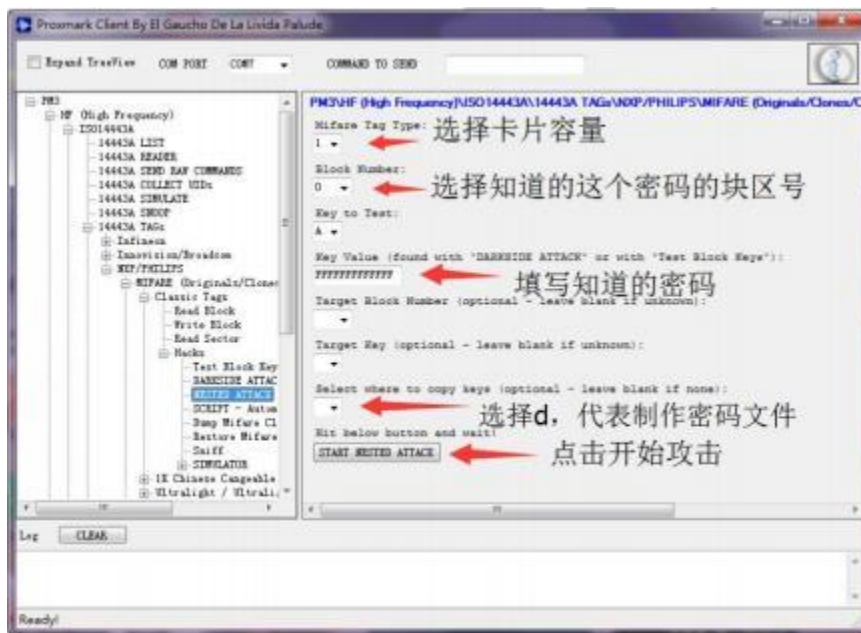
summary

2. Obtain the key of all sectors through the known key

Use the instruction, [hf mf nested 10 A ffffffff d] one password more than the other

This exploits the nested authentication vulnerability by using a known key for any sector to obtain keys for all sectors, making this vulnerability highly successful. In the example, it represents the A key ff.... for sector 0, where you can see that a "d" is added to the end. Without the "d," the key file will not be output; with the "d," the key is saved to file dumpkeys.BIN.

When using nested, be sure to choose the right card capacity. 1-4K.



The following is a screenshot of the successful attack:

```
proxmark3> hf mf nested 1 0 A FFFFFFFF
Testing known keys. Sector count=16
nested...
Time in nested: 4.010 (inf sec per key)

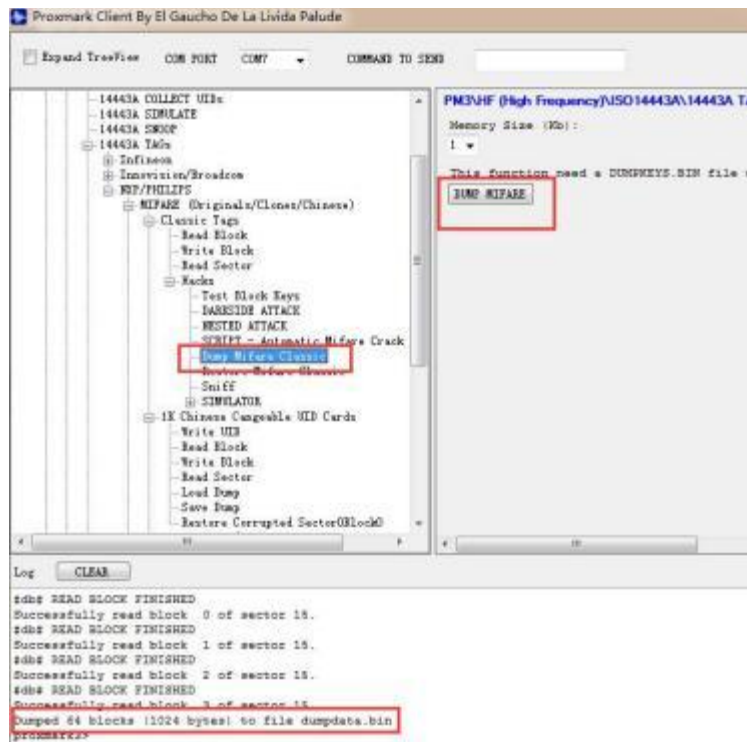
Iterations count: 0
```

sec	key A	res	key B	res
000	FFFFFFFF	1	FFFFFFFF	1
001	FFFFFFFF	1	FFFFFFFF	1
002	FFFFFFFF	1	FFFFFFFF	1
003	FFFFFFFF	1	FFFFFFFF	1
004	FFFFFFFF	1	FFFFFFFF	1
005	FFFFFFFF	1	FFFFFFFF	1
006	FFFFFFFF	1	FFFFFFFF	1
007	FFFFFFFF	1	FFFFFFFF	1
008	FFFFFFFF	1	FFFFFFFF	1
009	FFFFFFFF	1	FFFFFFFF	1
010	FFFFFFFF	1	FFFFFFFF	1
011	FFFFFFFF	1	FFFFFFFF	1
012	FFFFFFFF	1	FFFFFFFF	1
013	FFFFFFFF	1	FFFFFFFF	1
014	FFFFFFFF	1	FFFFFFFF	1
015	FFFFFFFF	1	FFFFFFFF	1

```
proxmark3>
```

RES代表结果
如果是1, 代表
密码正确
如果是0, 代表
密码无效

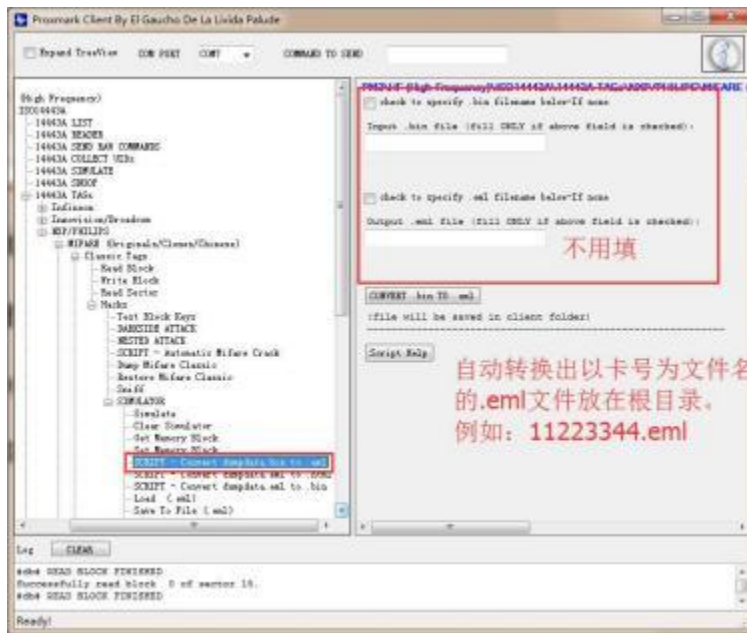
3. Read the card data to the computer



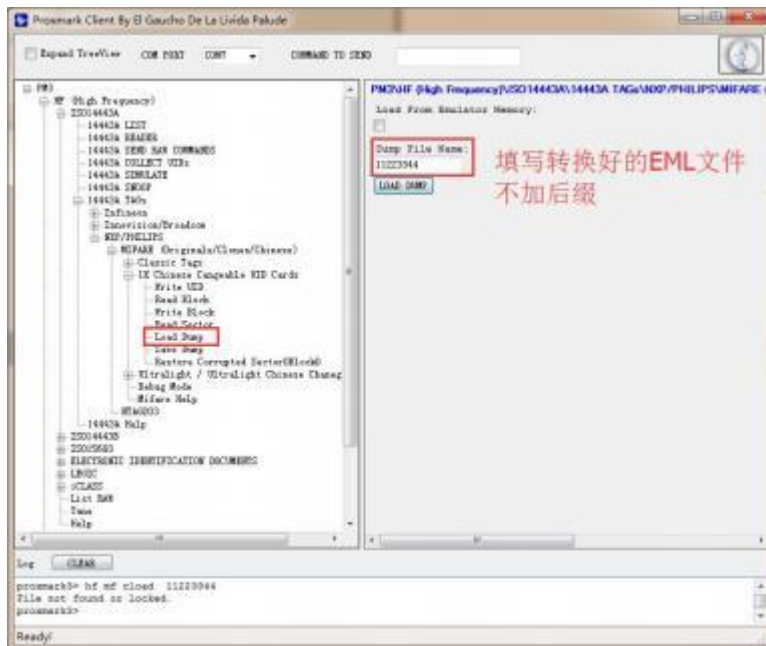
Use the above instructions. The card data file read is saved in the root directory, dumpdata.bin

4. Read the card data in the computer and write it into the UID card

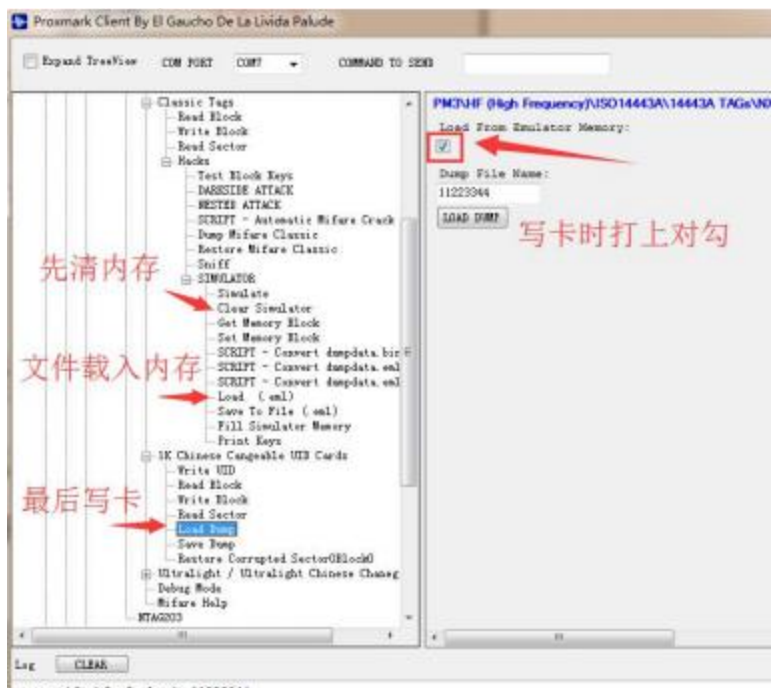
First, we need to convert the dumpdata.bin file to xxxxx.eml format, which can be opened and viewed in notepad before being retrieved and written to the UID card by PM3.



As shown in the figure below, retrieve the eml file and write it to the UID card.
The cloning is complete.



If the card cannot be read after writing, or the
data is corrupted, you can use the following
methods to reliably write:



**5. Check the data
and complete the
operation of cloning 6.**

Low-frequency card:

1. Read ID, HID, INDALA and other cards:

First of all, EM4X is the chip of the ID card, which belongs to the low frequency card and should be placed on a circular antenna for reading.

After reading the card, the following data will be displayed: "Valid EM410X I D Found!" indicates that the ID card number has been read.

```
prommark3> if search
#db# Sampling config:
#db# [q] divisor:      35
#db# [b] bps:          8
#db# [d] decimation:    1
#db# [a] averaging:     1
#db# [t] trigger threshold: 0
#db# Done, saved 40000 out of 40000 seen samples at 8 b1
#db# buffer samples: b9 b5 b1 ad aa a7 a4 a0 ...
Reading 20000 bytes from device memory
Data fetched
Samples @ 8 bits/smpl, decimation 1:1
NOTE: some demods output possible binary
      if it finds something that looks like a tag
False Positives ARE possible
Checking for known tags:
EM410x pattern found:
EM TAG ID       : 1234567890
Unique TAG ID   : 482c6ale09
Possible de-scramble patterns
HoneyWell IdentKey {
DEZ 8           : 05666960
DEZ 10          : 0878082192
DEZ 5.5         : 13398.30864
DEZ 3.5A        : 018.30864
DEZ 3.5B        : 052.30864
DEZ 3.5C        : 086.30864
DEZ 14/IK2      : 00078187498520
DEZ 15/IK3      : 000309882797821
DEZ 20/ZK       : 04080212061001140009
}
Other           : 30864_086_05666960
Pattern Paxton  : 308983440
Pattern 1       : 0xC9D043 - 13226057
Pattern Sebury  : 30864 86 5666960 (hex: 7890 56 567890)
Valid EM410x ID Found!
prommark3>
```

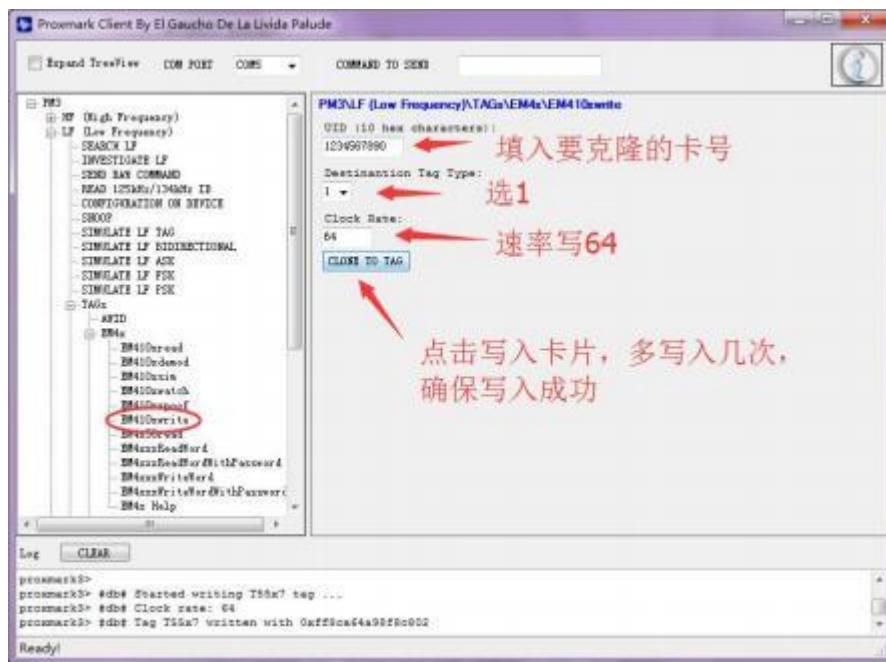
克隆时需要用的
卡号

Just write down the number behind EM TAG ID in the figure above.

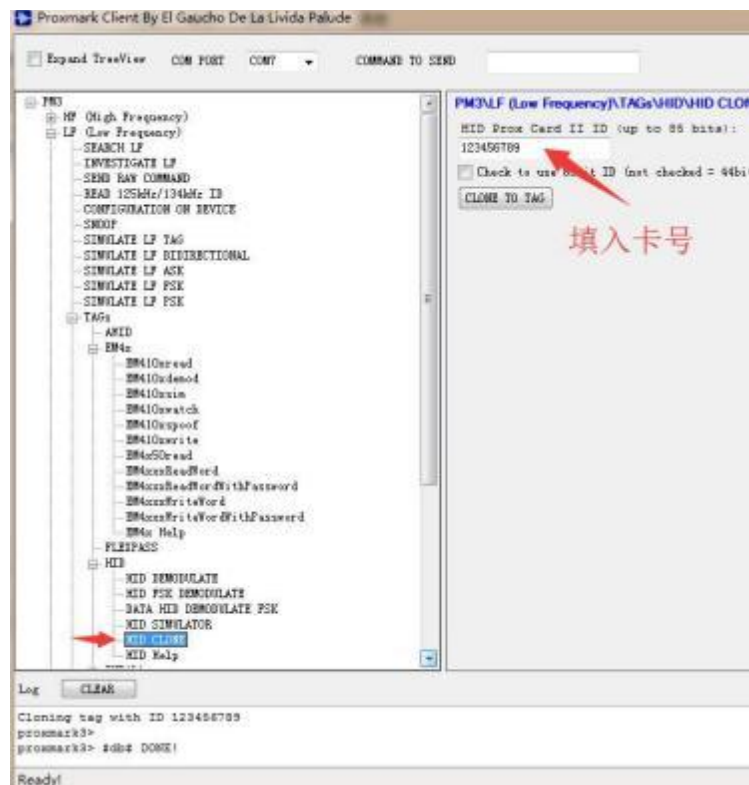
If it is an HID card, it will display [HID]. If it is an INDALA, it will display [INDALA].

2. Write different types of T5577 cards

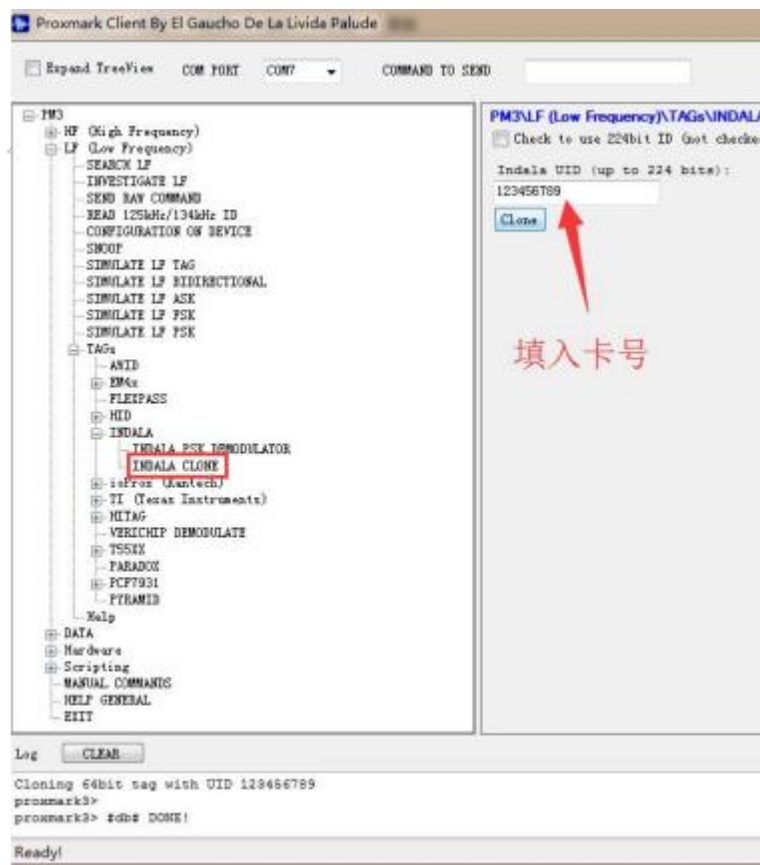
to clone the card: Clone into ID card:



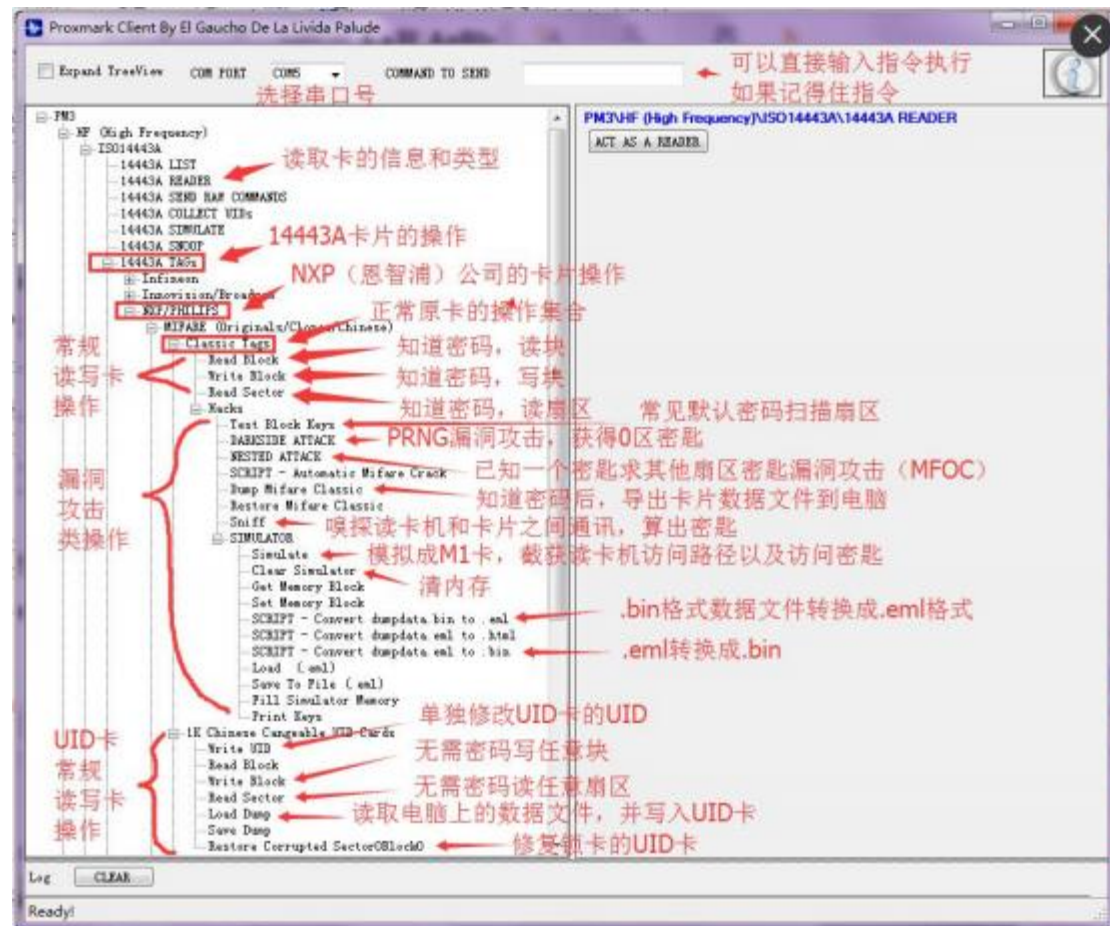
Clone as HID card:



Clone into a INDALA card:



VII. Software Introduction:



The following is a preliminary translation and description of the software interface to help understand the meaning of the software instruction tree.

How to Avoid the Trouble of Rebooting Software Multiple Times: The PM3 often crashes when running certain commands, requiring a reconnection of the USB. The software usually needs to be restarted as well. If you disconnect the USB and select another serial port number, then plug in the PM3, after the beep sound, switch the serial port back to the correct number. This way, you can avoid the hassle of restarting the software each time.

VIII. Notes:

1. Hardware matters:

PM3 is developed by foreign hackers in their spare time, so it does not consider much about usability and humanization. Therefore, it often crashes, some instructions do not have clear success or failure responses, and some details are not well handled.

Therefore, when the device is running an attack command, if the card does not support it or is not inserted, it will directly crash. After a crash, the device needs to be unplugged and reinserted at any time to force the computers serial port connection to function normally. During decryption and operation, use the four LEDs on the device, labeled ABCD, as indicators of progress. If the LEDs are flashing, it means the process is ongoing. If they are completely off or always on, it indicates a failed attack. Wait until all LEDs are off to confirm that the operation has stopped, then simply reinsert the device.

2. Software Matters:

A) Computer software

The software can use the CMD command line, the English GUI with blue icons, or our Chinese GUI.

	Official CMD command line (PM3 command console.bat)	Official English GUI (Proxmark Tool.exe)	Chinese GUI of this store (Proxmark3_EA SY_GUI.exe)
principle	Call Proxmark3.exe	Call Proxmark3.exe	Call Proxmark3.exe
Drug trafficking	not have	not have	It will misidentify the virus
Read and write UID cards	Read/write and compatible with UID cards displaying "NO"	Read and write, compatible with UID cards displaying "NO"	Read and write only compatible UID cards that can be read and written
read- write FUID/CUID	Read and write, you need to write blocks	Read and write, you need to write blocks	Read and write, automatically write the

	individually by hand	individually by hand	whole card after loading the file	
Ease of use	It is difficult to use the English instructions, but the operation is easy	Generally easy to use, see English Wind text operation, comprehensive functions	It is easy to use. After extracting the function, small functions are added	
compatibility				
The keychain card dumps the data	High compatibility and cross-platform	Windows Good platform for Tai zho u compati bility	Sometimes the screen opens and flashes back, but two hits will fix it	ope n
	Without an automatic re- reading mechanism, it is easy to interrupt and become unsmooth.	Without an automatic re- reading mechanism, it is easy to interrupt and not smooth.	, Added an automatic rereader card that can also read smoothly	make ,

b) Device firmware

Firmware is arranged from old to new:

r486→756→816→848→852→1.0.0→2.0.0→2.5.0 Before the old

firmware input hw version you can directly see the version number.

After 1.0.0, only the date is returned, and the version number is determined by the date.

2.0.0: #db#bootrom: /-suspect 2015-04-

0215:12:04#db# os: /-suspect 2015-04-

0215:12:11

#db# HF FPGA image built on 2015/03/09 at08:41:42

2.5.0: bootrom: /-suspect 2015-11-1910:08:02

os: /-suspect 2015-11-19 10:08:09

LF FPGA image built for 2s30vq100 on 2015/03/06 at07:38:04

HF FPGA imagebuilt for 2s30vq100 on 2015/11/ 2at 9: 8: 8

It is recommended to use 2.0.0 firmware. The latest 2.5.0 firmware has been tested.

One secret can easily produce ERROR. Some new features in the new firmware are not available, but it is often necessary to patch the wall by breaking the east wall, which will affect the old features.

IX. Introduction to the Directive

[hw tune] Antenna tuning voltage test

The command is used to test the antennas resonant voltage. When testing, the antenna should be upright, with no metal or cards around it, to obtain accurate voltage readings. Sometimes the voltage may be slightly lower than the nominal value. The antennas voltage has no impact on any operation or function; in fact, high frequencies above 5V and low frequencies above 10V can still be used normally.

Its just that the higher the voltage, the farther away the card is.

[hf 14areader] Types of card reading

As a card reader, read the high frequency card ID, test the type of high frequency card, put the card first, and then execute the command.

[hf mf c hk0 A ffffffff] Check the password

For the M1 card, check if the A password in sector 0 is ff....

【hf mf c hk*1 ? T】 Check the default password

For the M1 card, check whether there is a default password for all sectors, that is, automatically use the default password in the dictionary to verify 16 sectors.

(For most cards, the password is modified for the used sector, and the password is factory default for the unused sector. The default password may vary from manufacturer to manufacturer, and PM3 has more than ten common default passwords.)

[hf mfmifare] PRNG attack

This is a test of the PRNG vulnerability, which can directly calculate the password for the first sector through the vulnerability, also known as a hack. Not all cards support this vulnerability. Sometimes it will prompt "Cant select card" in

English, which is a BUG warning, please ignore it. If ABCD keeps flashing during operation, it indicates that it can be cracked, just wait for the result.

For unsupported cards, no matter how the card position is adjusted, the LED will not change, and finally PM3 will reset and drop the line.

(PRNG, vulnerability introduction:

<http://radiowar.org/security/%e4%bb%8e%e4%b9%8c%e4%ba%91%e7%9a%84%e9%94%99%e8%af%af%e6%bc%8f%e6%b4%9e%e5%88%86%e6%9e%90%e7%9c%8bmifare-classic%e5%ae%89%e5%85%a8.html>)

[hf mf nested 10 A ffffffff ffffd] One password is more than one password

This exploits a nested authentication vulnerability by using the known key of any sector to obtain the keys of all sectors, making this vulnerability highly successful. In the example, it represents the A key ff.... for sector 0, where you can see that a "d" is added to the end. Without the "d," the key file will not be output; with the "d," the key is saved to file dumpkeys.BIN.

When using nested, be sure to choose the right card capacity. 1-4K.

[hf mf dump] Read the card data and save it in dumpdata.BIN

This command reads out all the data from all the sectors of the card and saves it in a binary file dumpdata.BIN, provided that all the keys are obtained. Then you can use "UltraEdit" to open the file and cross-reference it with other data. The UltraEdit installation package is in the "utilities" section.

[hf mf c load e dumpdata.eml] Clone data to UID card

Write the dumpdata to the UID card. Follow it with the data file name "dumpdata.eml". The dumpdata.bin generated earlier cannot be directly imported; it needs to be converted into eml before importing. The card

data in eml format must contain a complete 64-line set of data. After conversion, confirm the integrity of the dumpdata file.

(The conversion format can be converted using the built-in script)

 `SCEIPT-convert dump data.b into .eml`

After cloning is complete, we can use the same way to dump the UID card again, and compare the data. Or we can read some sectors separately for comparison.

`[hf mf csetuid1234bcd] Modify the UID of the`

UID card Modify the UID of the UID card to

1234bcd. UID is four bytes.

[hf mf eclr] Clear the cache

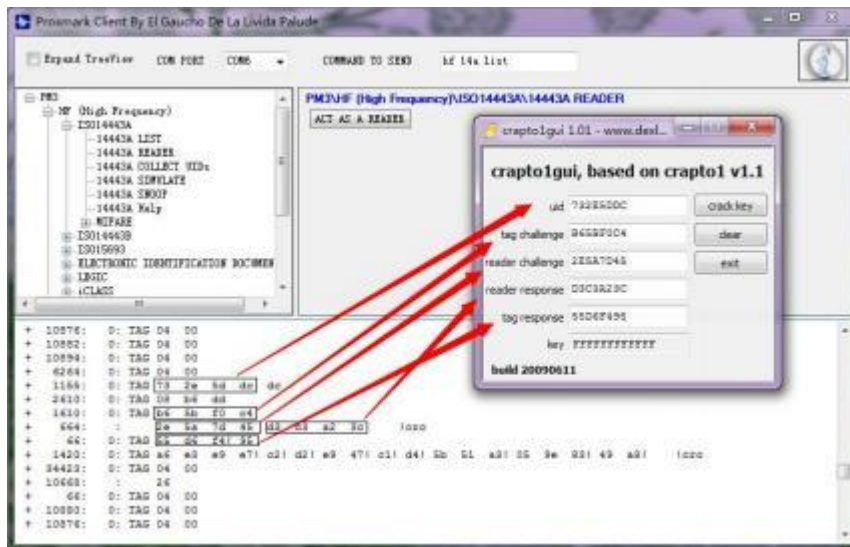
Be sure to clear the cache before using a cardless reader.

[hf mf sim x] Cardless listening card reader

The antenna of PM3 is simulated into a card, which induces the card reader to read the card, and captures the verification key issued by the card reader. It cannot be operated offline, and the button is pressed and exited after listening.

[hf 14a snoop] The card reader has obtained a 2.0.0 firmware for online monitoring:

Click SNOOP or enter the command directly to enter listening mode. Place the antenna and card close to the card reader; the card reader will operate on the card. The four LEDs will change, indicating that listening is complete. Press the button to exit. The four LEDs will turn off. Then send the command hf list 14a to view the listening results.



If you find the data structure group as shown in the figure above, you are done. If you do not have the data structure group as shown in the figure above, there may be the following reasons: 1. The card reader only reads the UID of the card without performing the password verification operation.

2. Some card readers have poor signals and cannot record signals.

3. The card and PM3 antenna should be a certain distance away, not too far or too close, about one centimeter. The data corresponding to the input into the gadget can be calculated to calculate the password.

[If em4x em410xwatch] Read the low frequency card ID

This command is used to read the ID of the low-frequency card. The low-frequency antenna is required. The command is executed first and the card is placed. While recording the ID, it is important to record the value of clock rate, which is usually 64.

(Knowledge: em4x is the chip model of most fixed ID low-frequency cards. Generally, a string of numbers printed on the card is a fixed ID card, which has a unique ID number solidified at the factory and cannot be modified.)

[If em4x em410xwrite 12345bcd ef164] Write the ID to the T5577 card

Write the ID number into the T5577 card. The length is 10 hex. In the example, 12345bcdef is the ID, followed by "1" which is the T55X7 card type, and 64 is the clockrate.

All the above instructions can be found in the instruction tree on the left side of the upper computer software. On the right, the mouse moves to the corresponding box, and there are English prompts and instructions for use, which will not be listed one by one.

Problem collection:

[http://wiki.radiowar.org/%E9%97%AE%E9%A2%98%E6%B1%87%E9%9B%86#.](http://wiki.radiowar.org/%E9%97%AE%E9%A2%98%E6%B1%87%E9%9B%86#.E4.B8.BA.E4.BB.80.E4.B9.88.E4.BD.BF.E7.94.A8cloud.E5.AF.BC.E5.85.A5.E6.95.B0.E6.8D.AE.E7.9A.84.E6.97.B6.E5.80.99.EF.BC.8C.E6.8F.90.E7.A4.BA.E6.89.BE.E4.B8.8D.E5.88.B0.E6.96.87.E4.BB.B6)

[E4.B8.BA.E4.BB.80.E4.B9.88.E4.BD.BF.E7.94.A8cloud.E5.AF.BC.E5.85.A5.E6.95.B0.E6.8D.AE.E7.9A.84.E6.97.B6.E5.80.99.EF.BC.8C.E6.8F.90.E7.A4.BA.E6.89.BE.E4.B8.8D.E5.88.B0.E6.96.87.E4.BB.B6](http://wiki.radiowar.org/%E9%97%AE%E9%A2%98%E6%B1%87%E9%9B%86#.E4.B8.BA.E4.BB.80.E4.B9.88.E4.BD.BF.E7.94.A8cloud.E5.AF.BC.E5.85.A5.E6.95.B0.E6.8D.AE.E7.9A.84.E6.97.B6.E5.80.99.EF.BC.8C.E6.8F.90.E7.A4.BA.E6.89.BE.E4.B8.8D.E5.88.B0.E6.96.87.E4.BB.B6)

Instruction set reference:

<http://wiki.radiowar.org/Proxmark3%E5%91%BD%E4%BB%A4%E5%B8%AE%E5%8A%A9>

Use case reference:

<http://wiki.radiowar.org/Proxmark3%E4%BD%BF%E7%94%A8%E6%A1%88%E4%BE%8B>

Ten. Firmware upgrade and replacement

Refer to the document "Firmware Burn-in Guide V1.0.pdf"

Compile the firmware

Compile the firmware to produce elf, s19 and other files required for burning.

This is not a necessary operation. If you want to compile the latest firmware by yourself, refer to the "data of Yimeng Technology" or wiki for the process.

The data provides compiled firmware that can be burned directly.

FCC Warning:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: Any changes or modifications to this device not explicitly approved by manufacturer could void your authority to operate this equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.