PM3 Easy3.0 Quick start guide 3

Ⅰ. Hardware description 4

1. Installation of equipment : 4

A. Install the copper pillar first : 4

B. Install the upper plate : 5

C. Install low frequency antenna : 5

D. Attach a protective film : ....

2. IC high frequency card placement location : 6

3. ID low frequency card placement location : 7

4. Other parameters : 8

II. Driver Installation 9

Reasons for unsuccessful driver installation and solutions : 12

III. Quickly test basic functions 13

1. Antenna voltage test : 13

2. Read high frequency card test : 14

3. Read low frequency card test : 14

Ⅳ. Card basics 16

Common cards are : 16

M1 S50 card introduction 16

M1 UID card introduction 18

M1 FUID, CUID card introduction 19

ID, HID, card introduction 19

T5577 card introduction 19

Ⅴ. Card security test (whether it can be copied) 23

Overall process 23

IC card ideas : 24

1. Try to get any key in the 16 sectors of the card 24

2. Obtain all sector keys through known keys 32

3. Read the card data to the computer 34

4. Read the card data in the computer and write it to the UID card 34

5. Check the data and complete the clone 35

Ⅵ. Low frequency card operation : 35

1. Read ID, HID, INDALA and other cards : 35

2. Write different types to T5577 card to clone the card : 36

Clone into ID card : 36

Clone into HID card : 37

Clone into INDALA card : 37

Ⅶ. Software introduction : 38

Ⅷ. Matters needing attention : 38

1. Hardware matters : 38

2. Software matters : 39

a) PC software 39

b) Device firmware 40

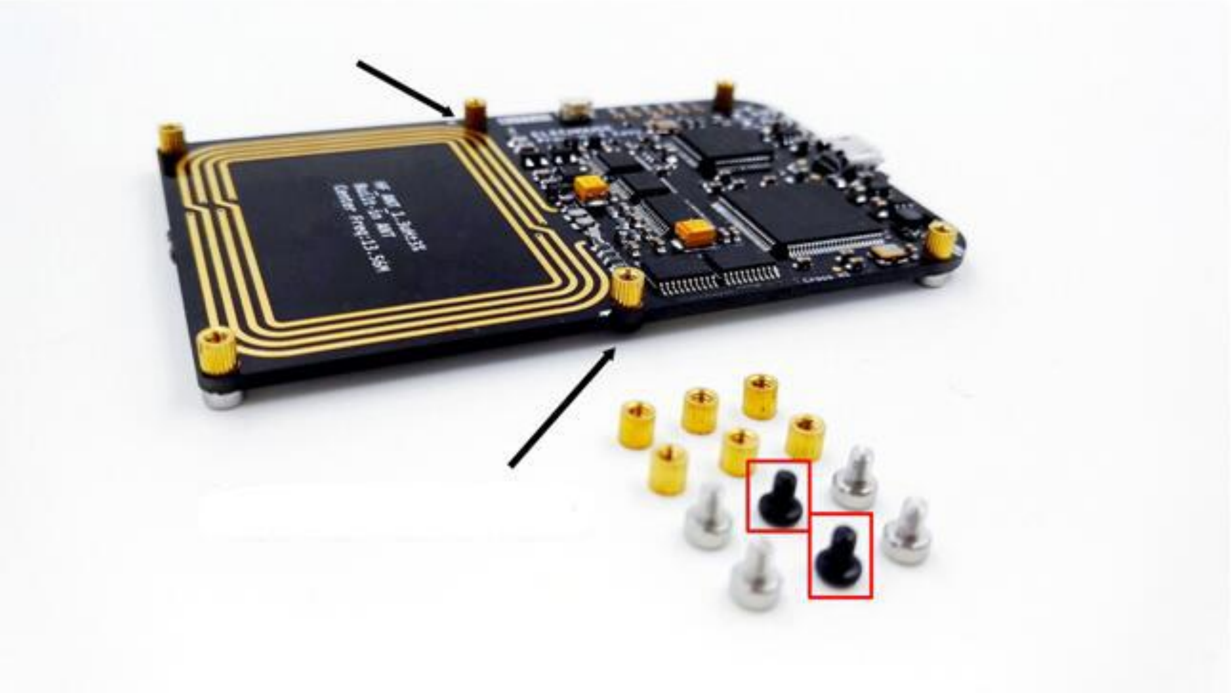
Ⅸ. Instruction introduction 40

PM3 Easy3.0 quick start guide

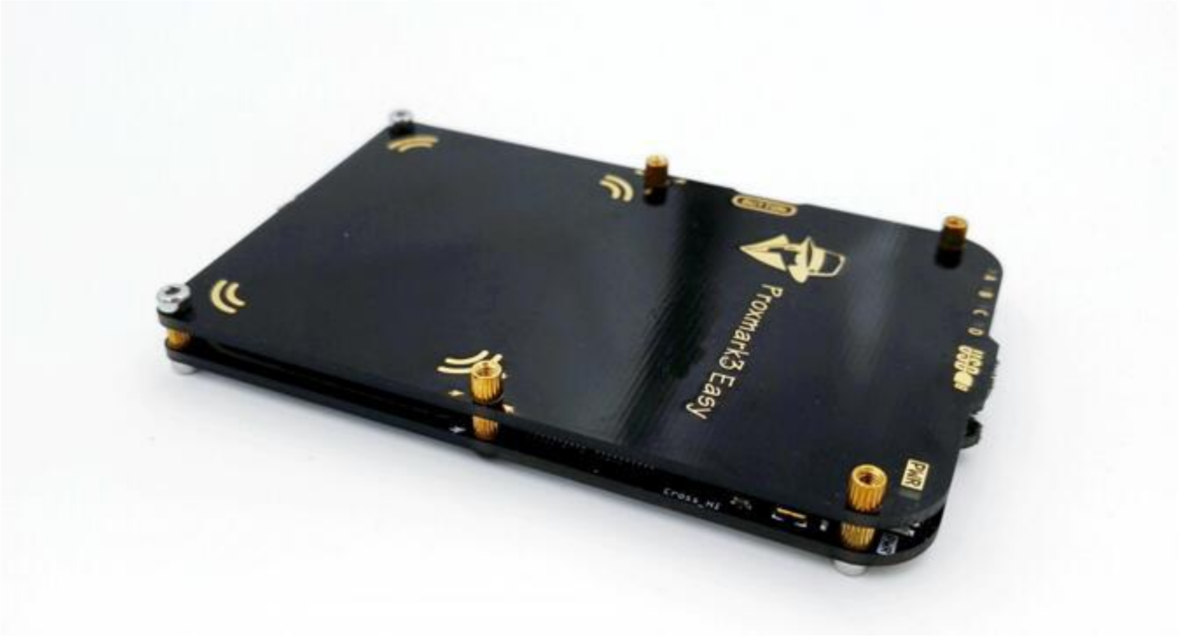
一 . Hardware description

1.1. Installation of equipment :

A. Install the copper pillar first :

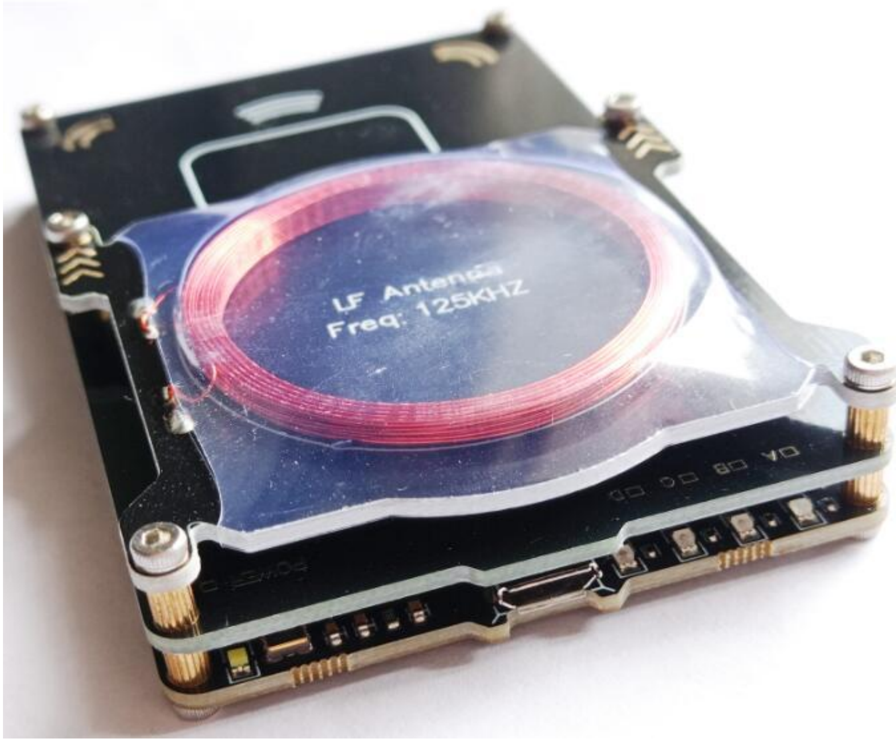


B. And then install the upper plate：



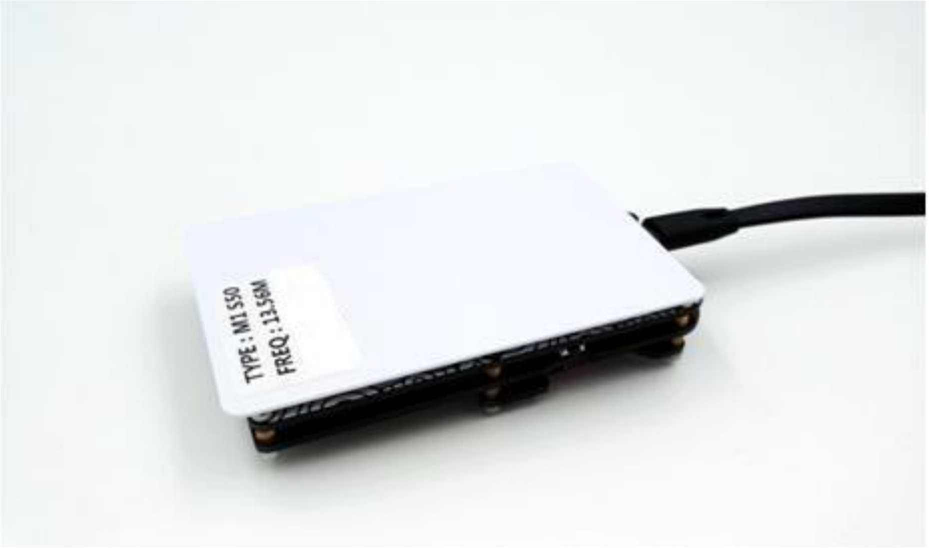
Screw the screws and lead copper posts on the upper plate

C.Install low frequency antenna：

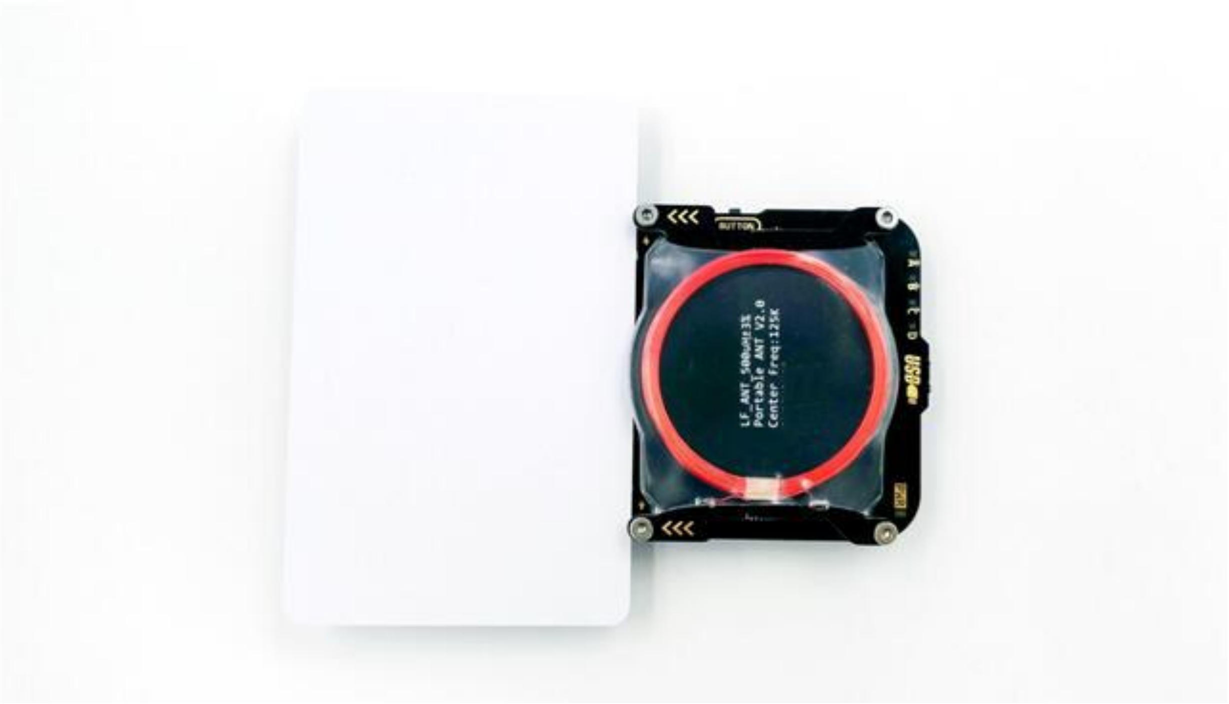


Tip: The low-frequency antenna can also be installed in four symmetrical positions on the top, bottom, left, and right, and you can choose according to your preferences. In the recommended way, the two antennas have the least influence on each other.

2. **IC HF card placement location：**



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



Place the card as shown in the picture above. Normally, there is no problem. In addition, please keep away from metal objects and metal tabletops. Individual keychains or small cards with poor signals can easily interrupt the reading and writing. At this time, you can read the card as shown in the figure below and 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 on the circular antenna

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

4.Other parameters :

(When the low-frequency antenna is installed on the right side)

# LF antenna: 29.84 V @ 125.00 kHz
# LF antenna: 32.31V @ 134.00 kHz
# HF antenna: 28.43V @ 13.56 MHz

(When the low-frequency antenna is installed on the left side)

# LF antenna: 43.86 V @ 125.00 kHz
# LF antenna: 24.48 V @ 134.00 kHz
# HF antenna: 25.13 V @ 13.56 MHz

Factory firmware version : 2.5

Operating Voltage

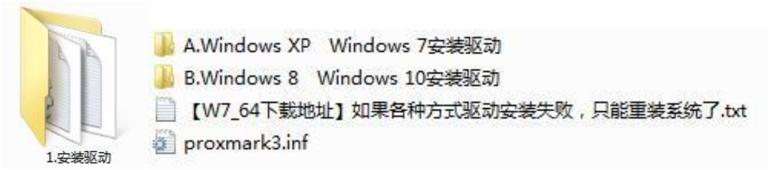
3.5-5.5V

Working current :

50-130Ma

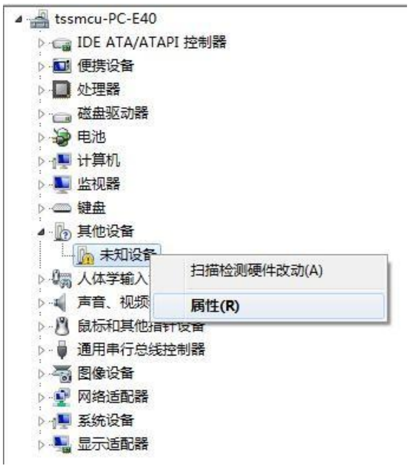
二．Driver Installation

The following is an example process of W7 64 installation. The installation of different systems is slightly different, please refer to the under this folder


1.安装驱动

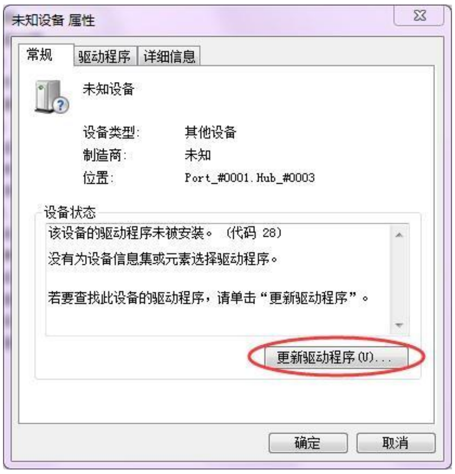
A.Windows XP　Windows 7安装驱动
B.Windows 8　Windows 10安装驱动
【W7_64下载地址】如果各种方式驱动安装失败，只能重装系统了.txt
proxmark3.inf

Guide to operate：


tssmcu-PC-E40
IDE ATA/ATAPI 控制器
便携设备
处理器
磁盘驱动器
电池
计算机
监视器
键盘
其他设备
未知设备
人体学输入
声音、视频
鼠标和其他指针设备
通用串行总线控制器
图像设备
网络适配器
系统设备
显示适配器

1. Connect PM3 to the computer, right-click the properties of the unknown device in the device manager

2.Click Update Driver



未知设备 属性

常规 | 驱动程序 | 详细信息

未知设备

设备类型: 其他设备
制造商: 未知
位置: Port_#0001.Hub_#0003

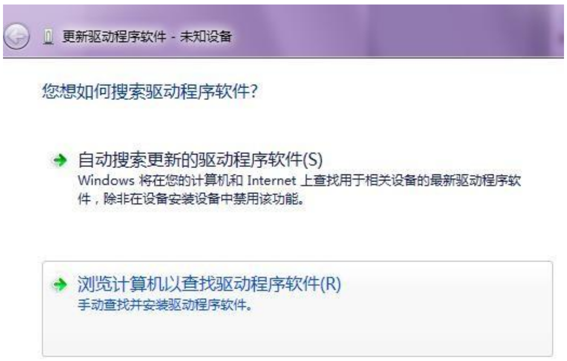
设备状态

该设备的驱动程序未被安装。 (代码 28)

没有为设备信息集或元素选择驱动程序。

若要查找此设备的驱动程序，请单击“更新驱动程序”。

2. Click below-- Browse the computer to find the driver software (R)



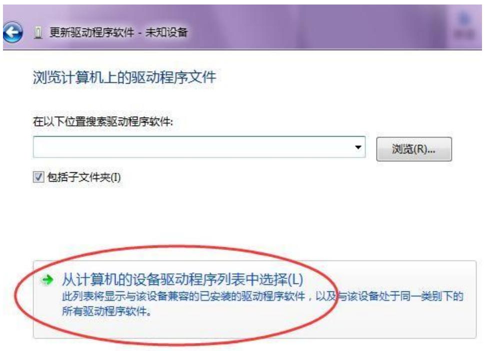
更新驱动程序软件 - 未知设备

您想如何搜索驱动程序软件?

自动搜索更新的驱动程序软件(S)
Windows 将在您的计算机和 Internet 上查找用于相关设备的最新驱动程序软件，除非在设备安装设备中禁用该功能。

浏览计算机以查找驱动程序软件(R)
手动查找并安装驱动程序软件。

3. Click below--Select from the computer's device driver list (L)



更新驱动程序软件 - 未知设备

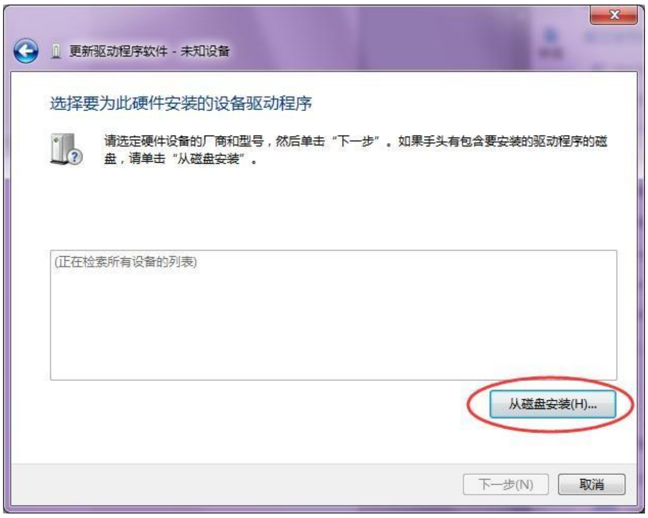
浏览计算机上的驱动程序文件

在以下位置搜索驱动程序软件:

☑ 包括子文件夹(I)

从计算机的设备驱动程序列表中选择(L)
此列表将显示与该设备兼容的已安装的驱动程序软件，以及与该设备处于同一类别下的所有驱动程序软件。

4. After the next step, install from disk

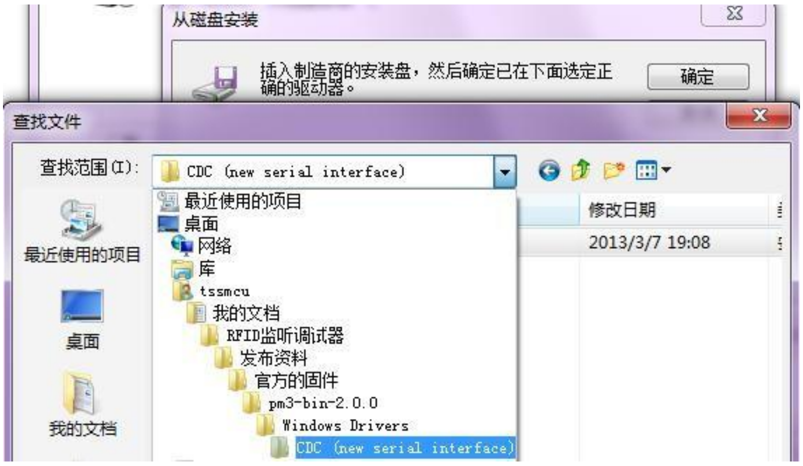


选择要为此硬件安装的设备驱动程序

请选定硬件设备的厂商和型号，然后单击“下一步”。如果手头有包含要安装的驱动程序的磁盘，请单击“从磁盘安装”。

(正在检索所有设备的列表)

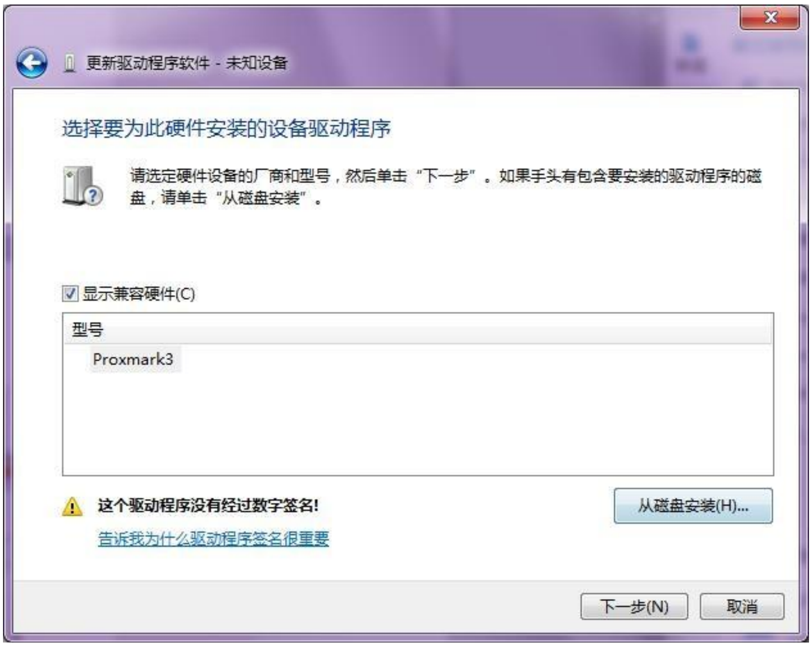
5. Select the drive directory, select the drive file



插入制造商的安装盘，然后确定已在下面选定正确的驱动器。

查找范围(I): CDC (new serial interface)

6. Next step



更新驱动程序软件 - 未知设备

选择要为此硬件安装的设备驱动程序

请选定硬件设备的厂商和型号，然后单击“下一步”。如果手头有包含要安装的驱动程序的磁盘，请单击“从磁盘安装”。

☑ 显示兼容硬件(C)

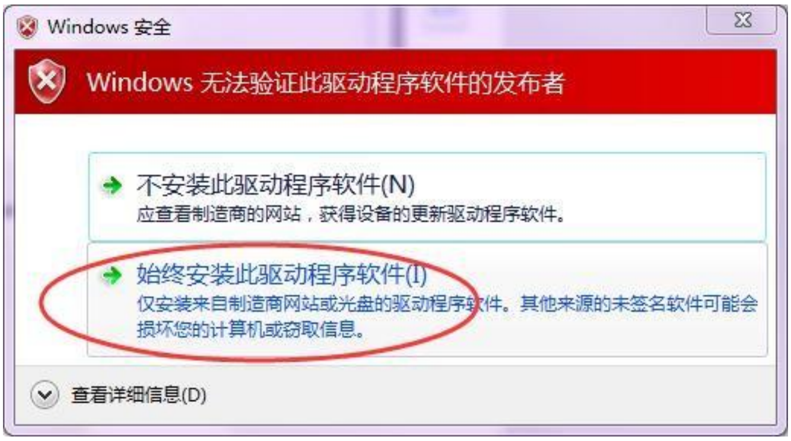
型号

Proxmark3

这个驱动程序没有经过数字签名!

告诉我为什么驱动程序签名很重要

7.Click below-- Always install this driver software (I)，finish drive install.



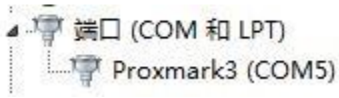
Windows 安全

Windows 无法验证此驱动程序软件的发布者

不安装此驱动程序软件(N)
应查看制造商的网站，获得设备的更新驱动程序软件。

始终安装此驱动程序软件(I)
仅安装来自制造商网站或光盘的驱动程序软件。其他来源的未签名软件可能会损坏您的计算机或窃取信息。

If everything is normal, a virtual serial port will appear. As shown below：



端口 (COM 和 LPT)
Proxmark3 (COM5)

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

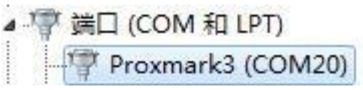
Reasons for unsuccessful driver installation and solutions：

1. The driver signature verification is not turned off, just turn off the driver signature verification.
2. WINDOWS may be a simplified version of GHOST.
3. Use a virtual machine to connect to the device.
4. The system lacks dependent files.
5. Try another computer or another USB port for a try

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

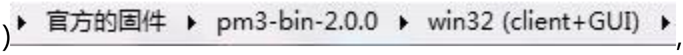
三 . Quickly test basic functions

First check the serial port number in the explorer :

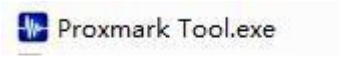


端口 (COM 和 LPT)
Proxmark3 (COM20)

Then open the file in the official firmware directory, (our fimeware is pm3-bin-V2.5) ,dauble click

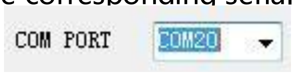


官方的固件 ▸ pm3-bin-2.0.0 ▸ win32 (client+GUI) ▸



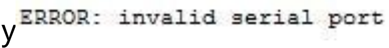
Proxmark Tool.exe

Select the corresponding serial port after opening If the bottom is blank, the connection is normal.



COM PORT COM20

If display Indicates that the connection is not normal。

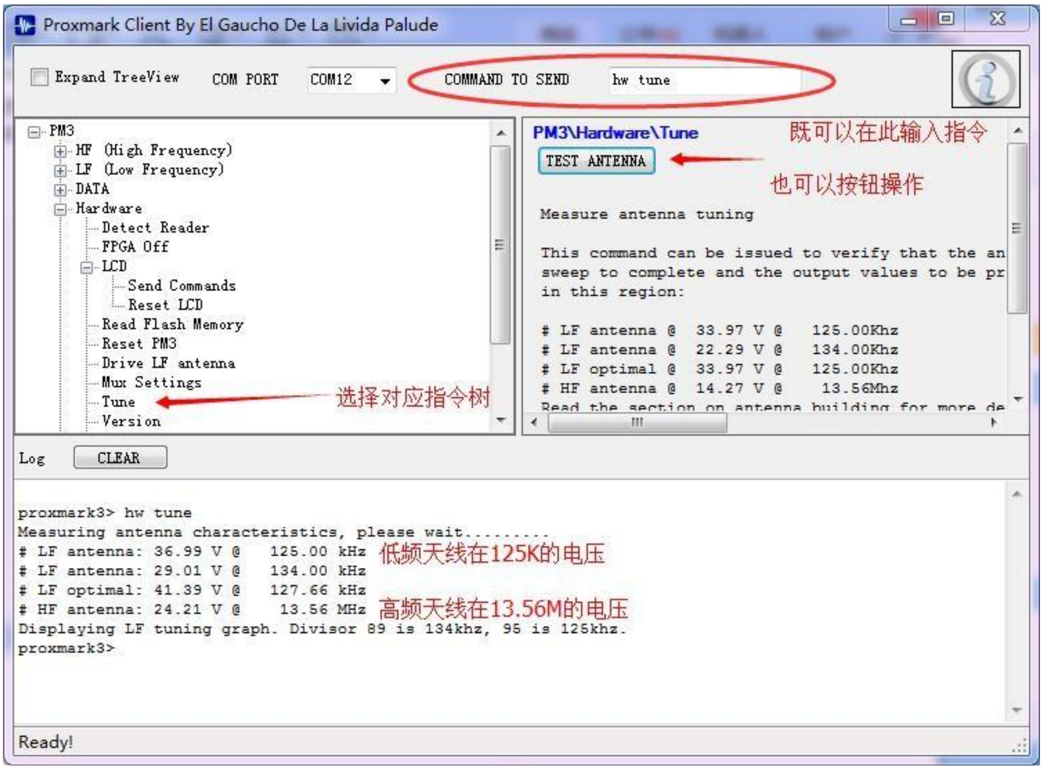


ERROR: invalid serial port

Try to plug and unplug the USB again, first select another serial port number, and then plug in the USB, and then select the correct serial port after the ding-dong sound.

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

1.Antenna voltage test:



既可以在此输入指令

也可以按钮操作

选择对应指令树

```
Measure antenna tuning

This command can be issued to verify that the an
sweep to complete and the output values to be pr
in this region:

# LF antenna @  33.97 V @   125.00Khz
# LF antenna @  22.29 V @   134.00Khz
# LF optimal @  33.97 V @   125.00Khz
# HF antenna @  14.27 V @    13.56Mhz
Read the section on antenna building for more de
```

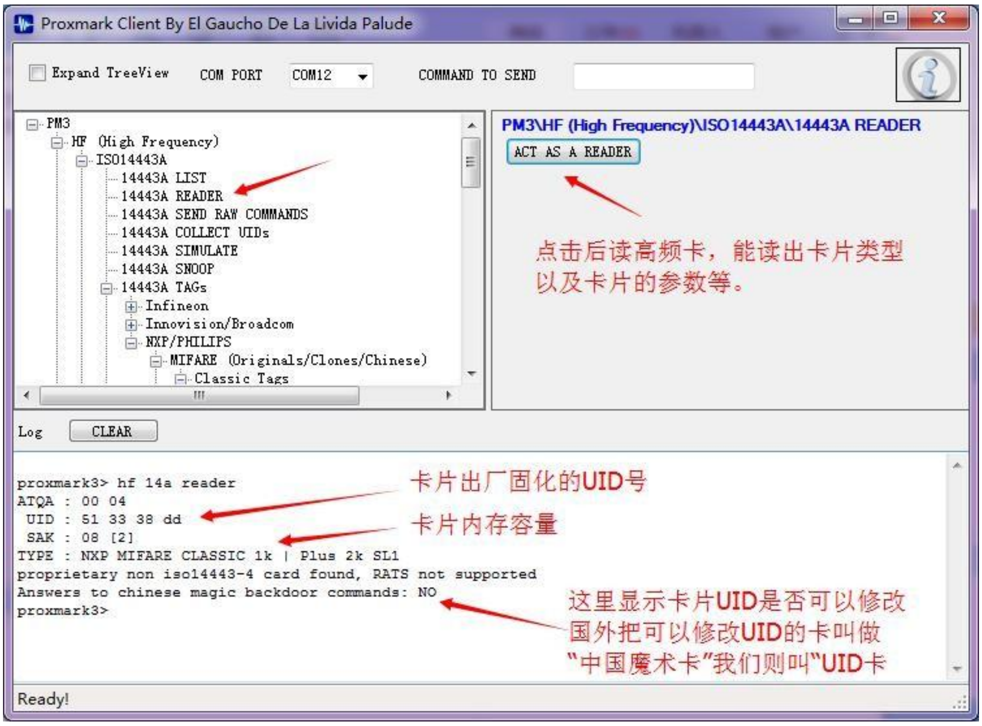
```
proxmark3> hw tune
Measuring antenna characteristics, please wait.........
# LF antenna: 36.99 V @    125.00 kHz
# LF antenna: 29.01 V @    134.00 kHz
# LF optimal: 41.39 V @    127.66 kHz
# HF antenna: 24.21 V @     13.56 MHz
Displaying LF tuning graph. Divisor 89 is 134khz, 95 is 125khz.
proxmark3>
```

低频天线在125K的电压

高频天线在13.56M的电压

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

1. Read the high frequency card test :



点击后读高频卡，能读出卡片类型以及卡片的参数等。

```
proxmark3> hf 14a reader
ATQA : 00 04
 UID : 51 33 38 dd
 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>
```

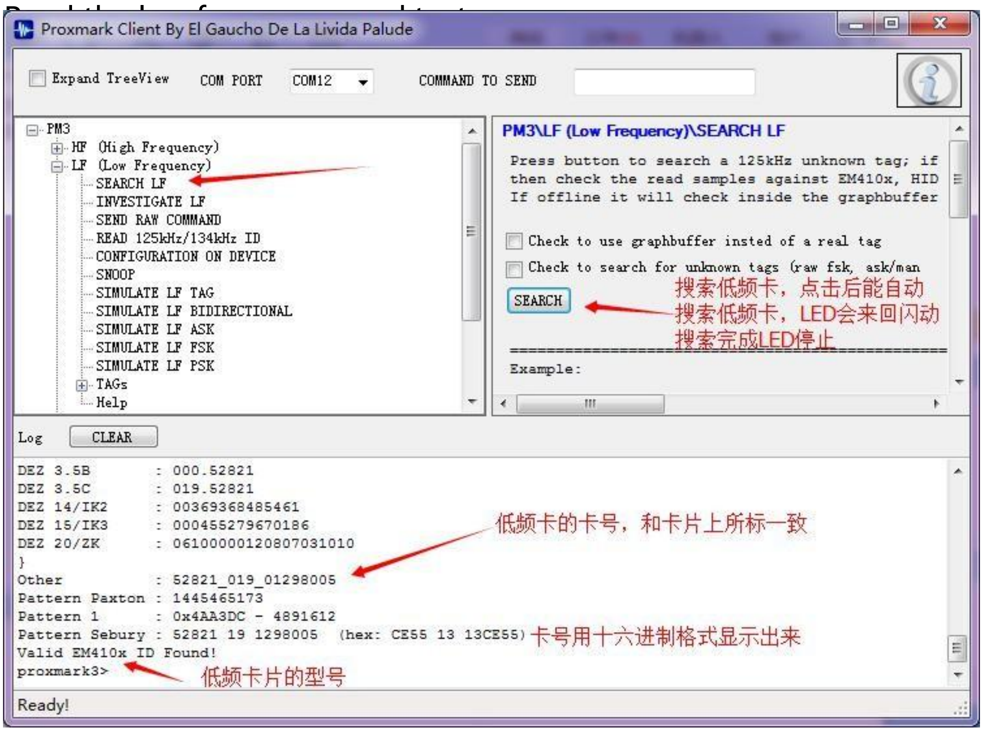
卡片出厂固化的UID号

卡片内存容量

这里显示卡片UID是否可以修改
国外把可以修改UID的卡叫做
"中国魔术卡"我们则叫"UID卡

You can try to test the cards by putting different cards "M1 S50" and "M1 UID" on the antenna.

2.



PM3\LF (Low Frequency)\SEARCH LF

```
Press button to search a 125kHz unknown tag; if
then check the read samples against EM410x, HID
If offline it will check inside the graphbuffer
```

□ Check to use graphbuffer insted of a real tag

□ Check to search for unknown tags (raw fsk, ask/man

搜索低频卡，点击后能自动搜索低频卡，LED会来回闪动搜索完成LED停止

```
DEZ 3.5B        : 000.52821
DEZ 3.5C        : 019.52821
DEZ 14/IK2      : 00369368485461
DEZ 15/IK3      : 000455279670186
DEZ 20/ZK       : 06100000120807031010
}
Other           : 52821_019_01298005
Pattern Paxton  : 1445465173
Pattern 1       : 0x4AA3DC - 4891612
Pattern Sebury  : 52821 19 1298005  (hex: CE55 13 13CE55)
Valid EM410x ID Found!
proxmark3>
```

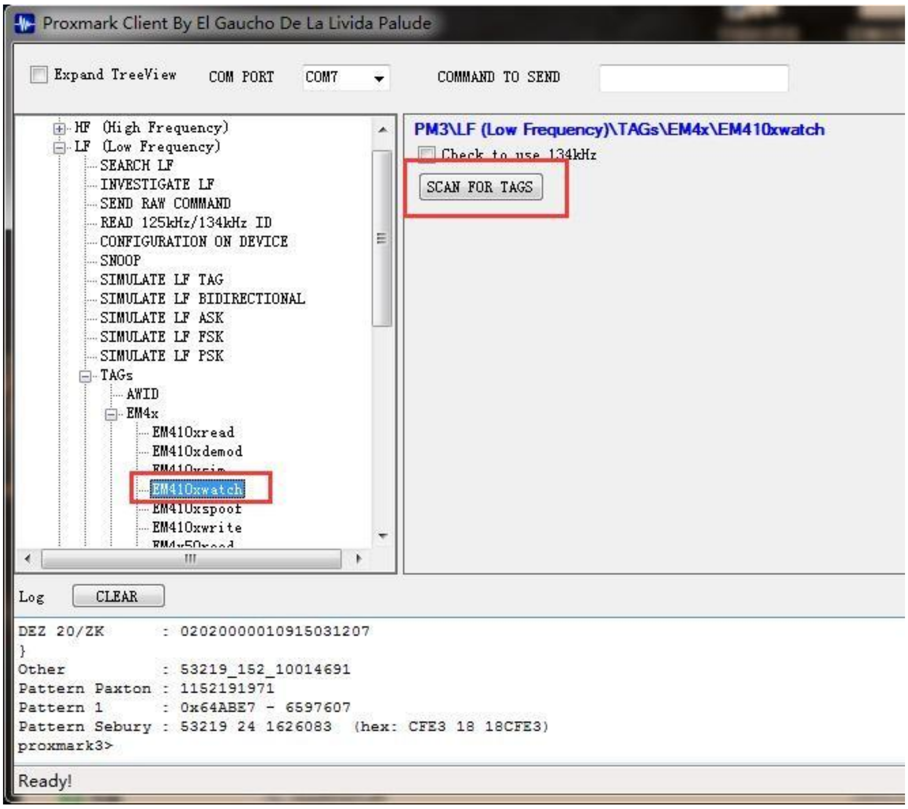
低频卡的卡号，和卡片上所标一致

卡号用十六进制格式显示出来

低频卡片的型号

You can try to test the card type by putting different cards "HID" and "T5577" on the antenna.

The sensitivity of this command to read the ID card is not good. When some cards cannot be read, you need to use another command to read, as shown in the figure below.

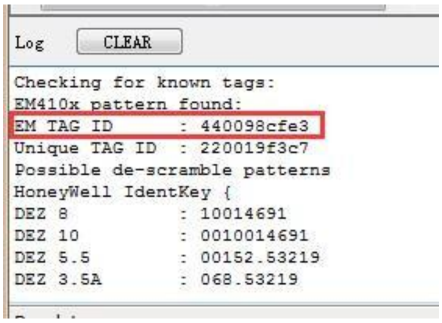


PM3\LF (Low Frequency)\TAGs\EM4x\EM410xwatch

□ Check to use 134kHz

```
DEZ 20/ZK       : 02020000010915031207
}
Other           : 53219_152_10014691
Pattern Paxton  : 1152191971
Pattern 1       : 0x64ABE7 - 6597607
Pattern Sebury  : 53219 24 1626083  (hex: CFE3 18 18CFE3)
proxmark3>
```

Page up after reading, as shown in the figure below, the red box is the ID card number :



```
Checking for known tags:
EM410x pattern found:
EM TAG ID      : 440098cfe3
Unique TAG ID  : 220019f3c7
Possible de-scramble patterns
HoneyWell IdentKey {
DEZ 8          : 10014691
DEZ 10         : 0010014691
DEZ 5.5        : 00152.53219
DEZ 3.5A       : 068.53219
```

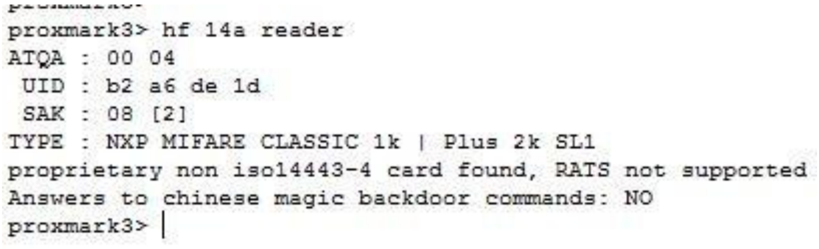
Note: Some T5577 empty cards cannot be read before they are initialized. We need to write the ID once to read them. Some cards have an ID number by default.

四．Four. Card basics

Common cards are:

Type	Frequency	Characteristic
Mifare S50(M1)	high frequency	The most common card, each card has a unique UID number, which can be stored Store modified data (student card, meal card, bus card, access card)
Mifare UltraLight(M0)	high frequency	Low-cost card, factory-cured UID, can store modified data (Metro card, bus card)
Mifare UID(Chinese magic card)（ UID card)	high frequency	Variant version of M1 card, UID can be modified, called China abroad Magic card, can be used to clone the data of M1 S50 completely
EM4XX(ID card)	high frequency	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 (Modifiable ID card)	Low frequency	It can be used to clone ID card, the factory is empty card, it can also have sectors inside Store data, and passwords can be set for individual sectors.
HID Prox II (HID)	Low frequency	Low-frequency card commonly used in the United States, rewritable, not used with other cartoons

M1 S50 card introduction.M1 S50 is the most commonly used card in China, also known as IC card.Developed by NXP, a subsidiary of Philips, domestically produced compatible cards are also available, but the card information cannot be determined. The card information is as follows:



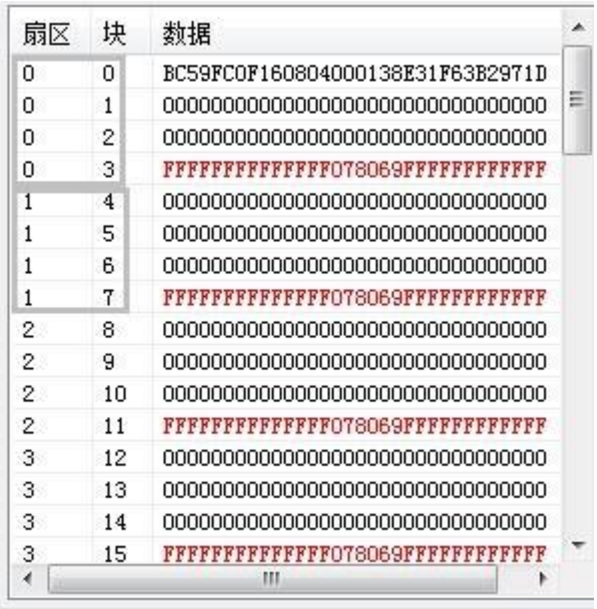
```
proxmark3> hf 14a reader
ATQA : 00 04
 UID : b2 a6 de 1d
 SAK : 08 [2]
TYPE : NXP MIFARE CLASSIC 1k | Plus 2k SL1
proprietary non iso14443-4 card found, RATS not supported
Answers to chinese magic backdoor commands: NO
proxmark3> |
```

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

It means this is an M1 S50 card.

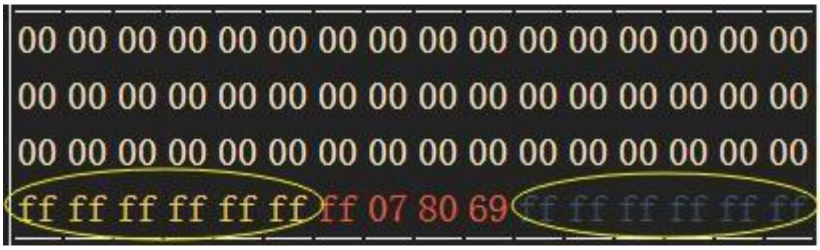
This kind of card is like a small-capacity U-disk, which is inherently mandatory to encrypt. The password cannot be cancelled.

The factory will set the password to the default password that everyone knows, FFFFFFFFFFFF. easy to use



扇区	块	数据
0	0	BC59FC0F160804000138E31F63B2971D
0	1	00000000000000000000000000000000
0	2	00000000000000000000000000000000
0	3	FFFFFFFFFFFFFF078069FFFFFFFFFFFF
1	4	00000000000000000000000000000000
1	5	00000000000000000000000000000000
1	6	00000000000000000000000000000000
1	7	FFFFFFFFFFFFFF078069FFFFFFFFFFFF
2	8	00000000000000000000000000000000
2	9	00000000000000000000000000000000
2	10	00000000000000000000000000000000
2	11	FFFFFFFFFFFFFF078069FFFFFFFFFFFF
3	12	00000000000000000000000000000000
3	13	00000000000000000000000000000000
3	14	00000000000000000000000000000000
3	15	FFFFFFFFFFFFFF078069FFFFFFFFFFFF

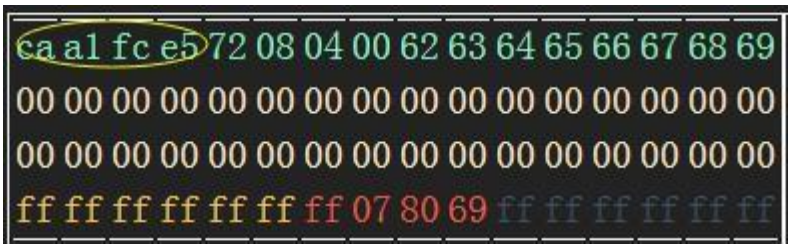
As shown in the figure above, it is the data structure of a card. There are 16 sectors in total, and each sector is composed of 4 blocks. The first three blocks of the 4 blocks are used to store data, and the last block is used to store passwords. Just like an encrypted small U disk, each sector has two passwords for common management. Screenshot of single sector data:



```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
ff ff ff ff ff ff ff 07 80 69 ff ff ff ff ff ff
```

It can be seen that there are four rows in this sector, each row is a block, and the first three blocks store data. The fourth block is to store the password. The two yellow circles are the A password and the B password. The middle four bytes are the control word, which is used to manage the password authority, just like the password setting option of the safe, which is used to set A and B Password function. When it is not modified by default, you can use the A password to read and write all data. Password A cannot be read out, password B can be read out with password A.

Although the password is stored there, the password is not necessarily readable. This is determined by the control word. Please refer to the [Card Information] folder for the detailed comparison table setting table.Except for the first sector in the M1 card, the structure of the other 15 sectors is exactly the same. The following figure shows the structure of the first sector:

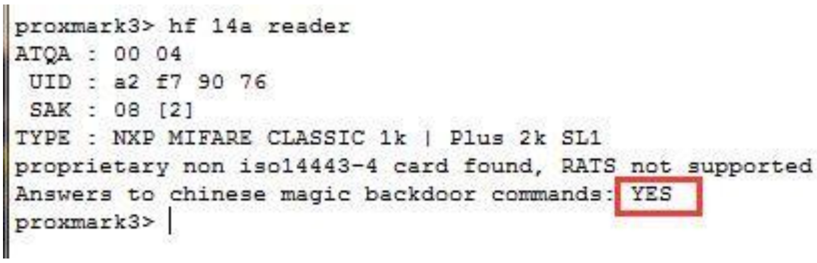


```
ca a1 fc e5 72 08 04 00 62 63 64 65 66 67 68 69
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
ff ff ff ff ff ff ff 07 80 69 ff ff ff ff ff ff
```

The red circle is not only the UID number of the card, but also a unique and unmodifiable 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 factory built-in, including manufacturer and card information. Can not be modified. Can only read.

M1 UID card introduction

The M1 UID card is a variant card specially made by the Chinese for the M1 S50 card. It is used exactly the same as the M1 S50 card, except that it has one more function, that is, the data of the 0 sector block can be modified at will. Therefore, the UID number can also be modified at will, and the manufacturer information can also be modified at will, hence the name of the 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” means it is a UID card. But some UID cards with poor compatibility will display NO , Cards with poor compatibility can be written with both software, but when reading data, the Chinese GUI cannot read the data, and the English GUI can read the incomplete data of the last block.

The advantage of this modification is that the M1 S50 card can be copied perfectly and the UID number is exactly the same. In this way, if the card reader has a verification UID number, there is no problem.

UID card modification 0 sector 0 block data is to enter the factory mode by instructions, you can directly edit any data of the whole card, you can read and write the card without a password, and you are not afraid of writing bad cards, even if you write wrong 0 blocks, write bad sectors The control word can also be repaired at any time without affecting the subsequent use, so it is widely used and won the hearts of the people.

But the disadvantage is that the new card reading system can detect the UID card by detecting the card's response to the special command, so it can deny the UID card's access to achieve the function of shielding the copy card. But after all, it is still a minority.

M1 FUID, CUID card introduction

The FUID card is optimized by the Chinese for the UID card. As mentioned above, the UID card will be detected and therefore blocked. The FUID card is a UID modifiable card without a backdoor. Its sector 0 data can only be modified once in a lifetime. Besides, it is exactly the same as the M1 standard card, so it is difficult to detect and block.

The CUID card is optimized for the FUID card. As mentioned above, because the block 0 can only be written once, it is difficult to write it wrong or it is difficult to reuse it.

Therefore, the CUID card can modify the block 0 repeatedly, but it and UID The difference of the card is that it does not have a backdoor, and can write 0 blocks by using conventional password verification. The other sectors are the same as the standard M1 card. The disadvantage is that there is still the possibility of being detected. At the same time, if the check digit of the UID number is accidentally written incorrectly, the card cannot be read. At this time, the card cannot be repaired, and the card can only be scrapped. Note that PM3 can write the above two types of cards, but the official English software can only write the cards one block at a time. Our Chinese GUI software can directly write the entire data file into the card, which is convenient to use.

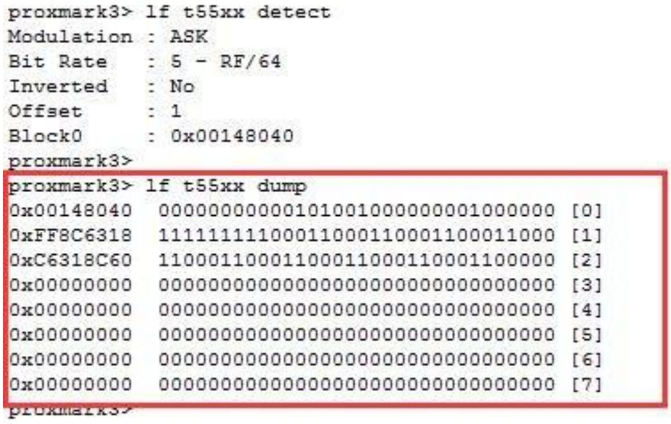
ID, HID, card introduction

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

T5577 card introduction

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

We first write the 5577 card into ID:1111111111, at this time 5577 has been transformed into an ID card, and then use the read 5577 full card data command to see the full card data



```
proxmark3> lf t55xx detect
Modulation : ASK
Bit Rate   : 5 - RF/64
Inverted   : No
Offset     : 1
Block0     : 0x00148040
proxmark3>
proxmark3> lf t55xx dump
0x00148040  00000000000101001000000001000000 [0]
0xFF8C6318  11111111100011000110001100011000 [1]
0xC6318C60  11000110001100011000110001100000 [2]
0x00000000  00000000000000000000000000000000 [3]
0x00000000  00000000000000000000000000000000 [4]
0x00000000  00000000000000000000000000000000 [5]
0x00000000  00000000000000000000000000000000 [6]
0x00000000  00000000000000000000000000000000 [7]
proxmark3>
```

As shown in the figure above, the first 3 blocks of the card will be automatically calculated by PM3 after ID is written, and the data will be written to achieve the transformation effect. Don't look at the 0 and 1 at the back, just look at the data at the front. There are 8 blocks in 5577, and each block can only store 8 digits. Block 0 is used to set the card type and modulation method, which determines whether the card is an ID card or an HID card. If you modify it at will, you will not be able to read the card. The last block of the seventh block is the data area when it is not encrypted. After encryption, its data becomes a password.

Note: Sometimes the 5577 card with the ID written into it does not respond after swiping, and the ID number cannot be read on the PM3 again. Explain that the card reader has a firewall, which is specially designed to prevent ID duplication of the card. In this case, you need to encrypt the 5577 before you can go through the firewall.

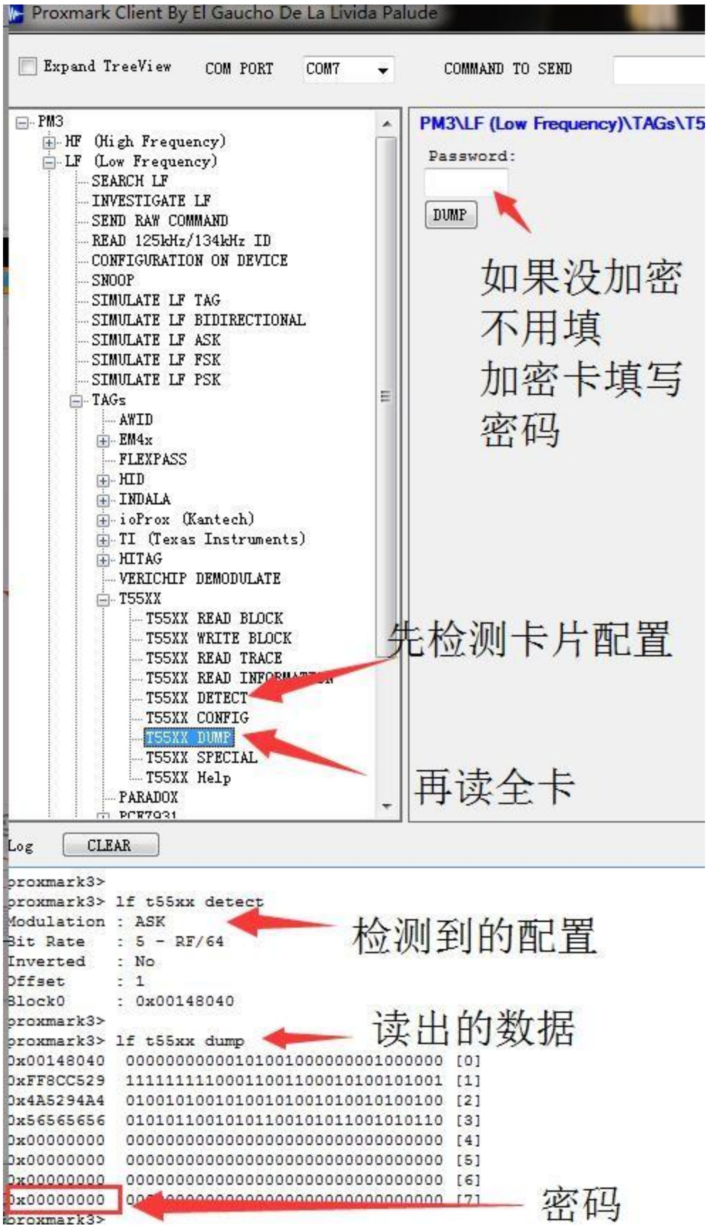
ID card: 0 block write: 00148040 no secret
00148050 encryption

HID card: 0 block write: 00107060 no secret
00107070 encryption

Steps to encrypt the ID card:

Write ID number → read 57 full card data (see password) → write 0 block data →Read the full card data again (verification)→Complete

PM3 read unencrypted 5577 full card data method：



如果没加密
不用填
加密卡填写
密码

先检测卡片配置

再读全卡

检测到的配置

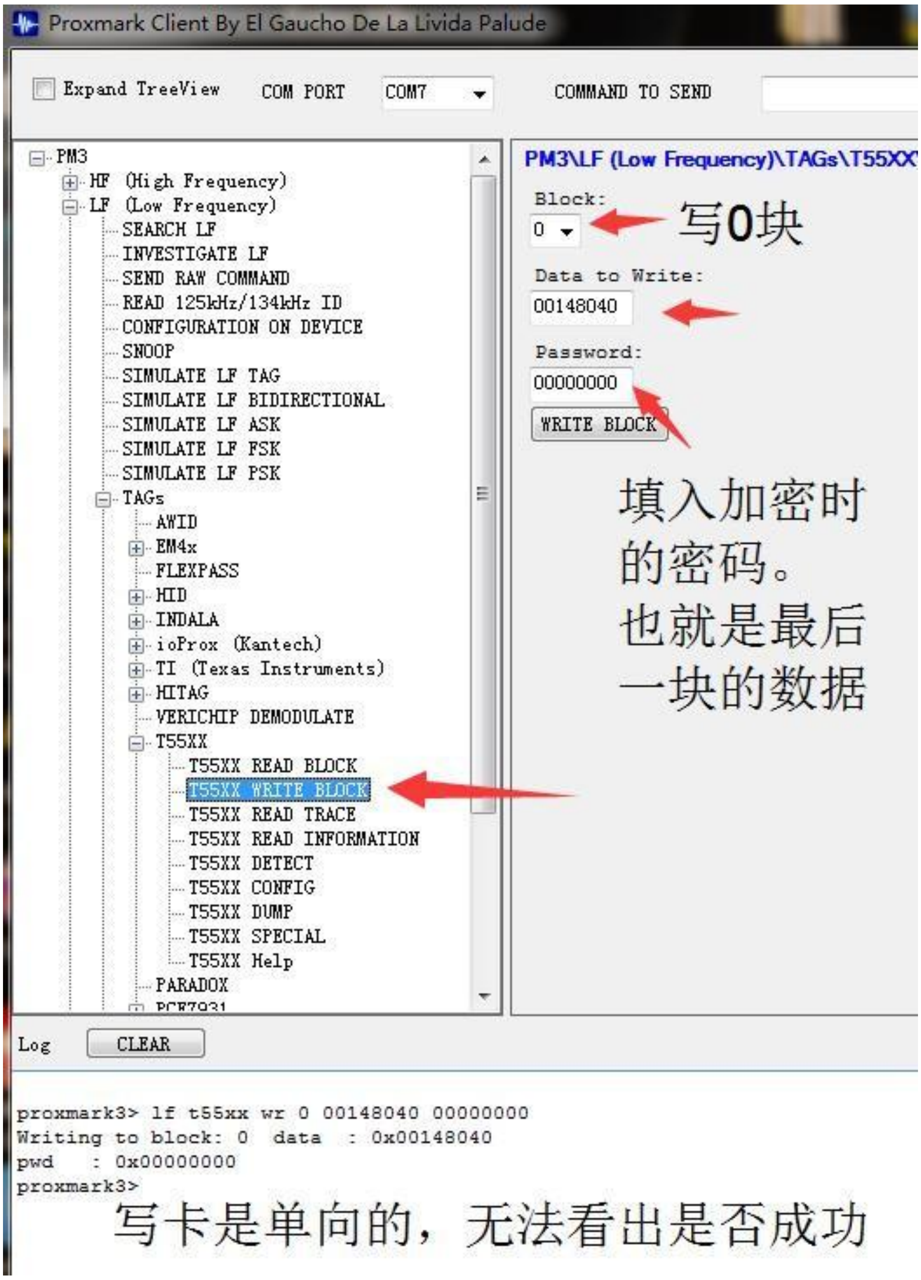
读出的数据

密码

```
proxmark3>
proxmark3> lf t55xx detect
Modulation : ASK
Bit Rate   : 5 - RF/64
Inverted   : No
Offset     : 1
Block0     : 0x00148040
proxmark3>
proxmark3> lf t55xx dump
0x00148040  00000000000101001000000001000000 [0]
0xFF8CC529  11111111100011001100010100101001 [1]
0x4A5294A4  01001010010100101001010010100100 [2]
0x56565656  01010110010101100101011001010110 [3]
0x00000000  00000000000000000000000000000000 [4]
0x00000000  00000000000000000000000000000000 [5]
0x00000000  00000000000000000000000000000000 [6]
0x00000000  00000000000000000000000000000000 [7]
proxmark3>
```

Note that if it is encrypted 5577, the configuration cannot be detected, or the read blocks are all the same data.

Write 5577 card when encryption is canceled:



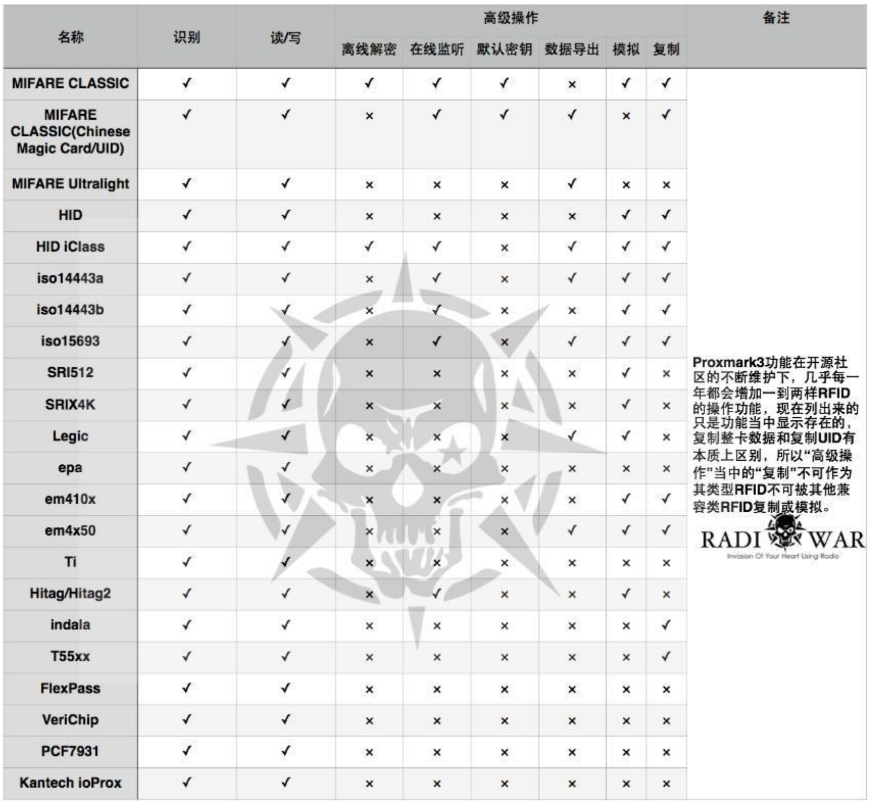
Block: 0

Data to Write: 00148040

Password: 00000000

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

The following table is from RADIOWAR and clearly shows PM3’ s support for cards



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	✓	✓	✓	✓	✓	×	✓	✓	Proxmark3功能在开源社区的不断维护下，几乎每一年都会增加一到两样RFID的操作功能，现在列出来的只是功能当中显示存在的，复制整卡数据和复制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。
MIFARE CLASSIC(Chinese Magic Card/UID)	✓	✓	×	✓	✓	✓	×	✓	
MIFARE Ultralight	✓	✓	×	×	×	✓	×	×	
HID	✓	✓	×	×	×	×	✓	✓	
HID iClass	✓	✓	✓	✓	×	✓	✓	✓	
iso14443a	✓	✓	×	✓	×	✓	✓	✓	
iso14443b	✓	✓	×	✓	×	×	✓	✓	
iso15693	✓	✓	×	✓	×	✓	✓	✓	
SRI512	✓	✓	×	×	×	×	✓	×	
SRIX4K	✓	✓	×	×	×	×	✓	×	
Legic	✓	✓	×	×	×	✓	✓	×	
epa	✓	✓	×	×	×	×	×	×	
em410x	✓	✓	×	×	×	×	✓	✓	
em4x50	✓	✓	×	×	×	✓	✓	✓	
Ti	✓	✓	×	×	×	×	×	×	
Hitag/Hitag2	✓	✓	×	✓	×	×	✓	×	
indala	✓	✓	×	×	×	×	×	✓	
T55xx	✓	✓	×	×	×	×	×	✓	
FlexPass	✓	✓	×	×	×	×	×	×	
VeriChip	✓	✓	×	×	×	×	×	×	
PCF7931	✓	✓	×	×	×	×	×	×	
Kantech ioProx	✓	✓	×	×	×	×	×	×	

This table is for reference only, most of the cards are rarely seen in China, so they have not been tested。

五．Card security test (whether it can be copied)

Overall process

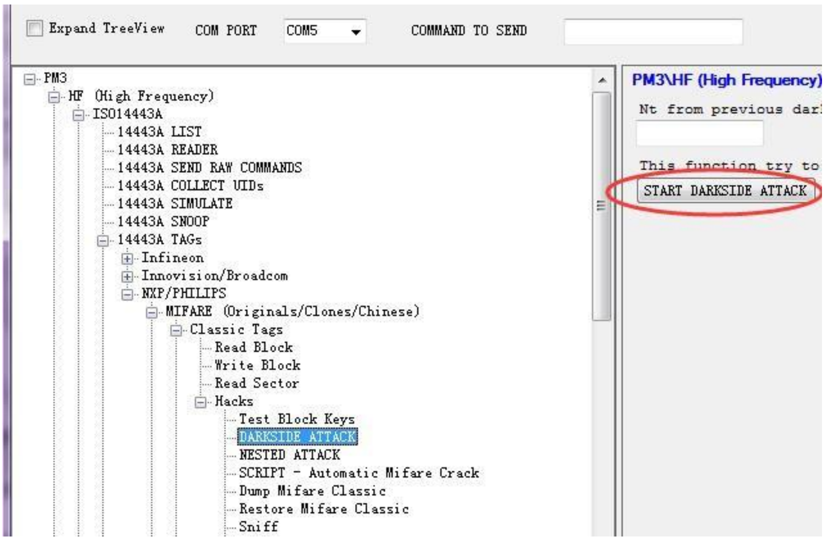
First read the card to determine the card type, whether it is an ID card or an IC card.

Note that the shape of the card has nothing to do with the model, the same chip can be packaged into a completely different shape

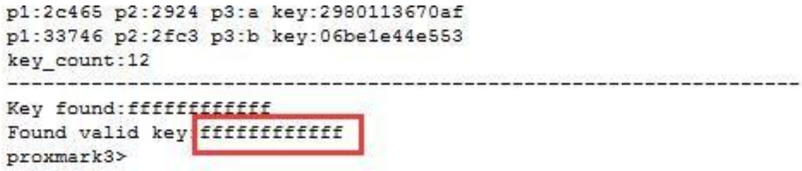
ID card: read the card ID number → replace the T5577 card → write the ID number into the card → complete
IC card: vulnerability decryption → read the entire card data → replace the UID card → write the data into the card → complete

Idea of IC card:
1. Obtain the key of any sector (any of the following can be used) a. 0 sector key for PRNG vulnerability attack
b. Scan the default password to get the key
c. Sniff the card reader and card interactive data to obtain the key
d. Simulate as M1 card and capture the key after swiping the card (picking the card reader, the compatibility is not good) 2. Using the MFOC vulnerability, use the known sector key to find all the sector keys
3. Use the cracked key to read out the card data 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 in the 16 sectors of the card
There are four ways, any one of which has obtained the key, you can proceed to the next step.
a) (Only the card is required) Through the PRNG vulnerability attack, the 0 sector key can be obtained unconditionally.
i. Send the command hf mf mifare, or click DARKSIDE ATTACK in the command tree



After clicking to start the attack, the card cannot be pasted in the middle of the antenna. You need to move to the edge until ABCD flashes, indicating that the card can be cracked, keep the position unchanged, and just 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:ffffffffffff
proxmark3>
```

i. After completion, the result as shown in the figure will be displayed, and the 0 sector key is in the red frame.

ii. If the card is not supported, or if the card is not put in, it will freeze after ten seconds, just reconnect PM3. You can use the complimentary M1 S50 to practice first.

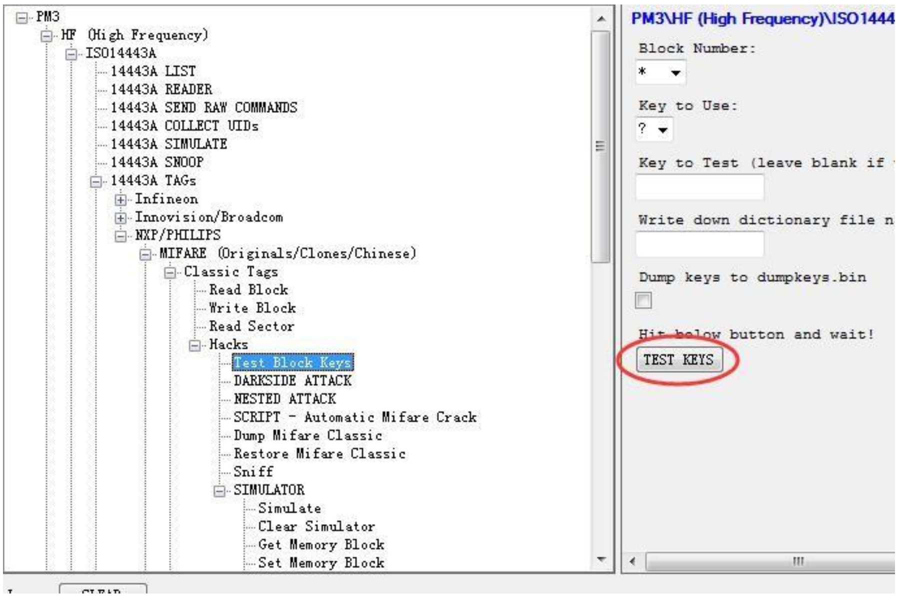
iii. Matters needing attention:

iv. Not all cards can be cracked smoothly, and sometimes it takes a chance.

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

b) Use the default passwords commonly used by the card manufacturers to test the card, and scan the sectors to see if there is a default key.

i. Send command: hf mf chk *?, or click in the command treeTest Block Keys



Block Number:
*

Key to Use:
?

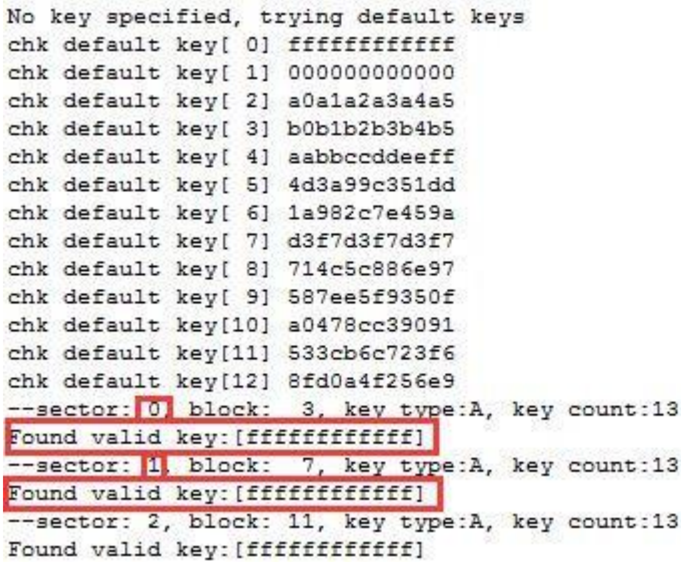
Key to Test (leave blank if

Write down dictionary file n

Dump keys to dumpkeys.bin
□

Hit below button and wait!

Put the card first, and scan the default password



```
No key specified, trying default keys
chk default key[ 0] ffffffffffff
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:[ffffffffffff]
--sector: 1, block:  7, key type:A, key count:13
Found valid key:[ffffffffffff]
--sector: 2, block: 11, key type:A, key count:13
Found valid key:[ffffffffffff]
```

ii. 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 "Found valid key:[ffffffffffff]" appears, it means that the corresponding key is found. The content of the key is "ffffffffffff", and the box above is the sector number corresponding to the key.

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

iv. Matters needing attention :

Sometimes there may be minor bugs in scanning the default key, so the results must be verified .

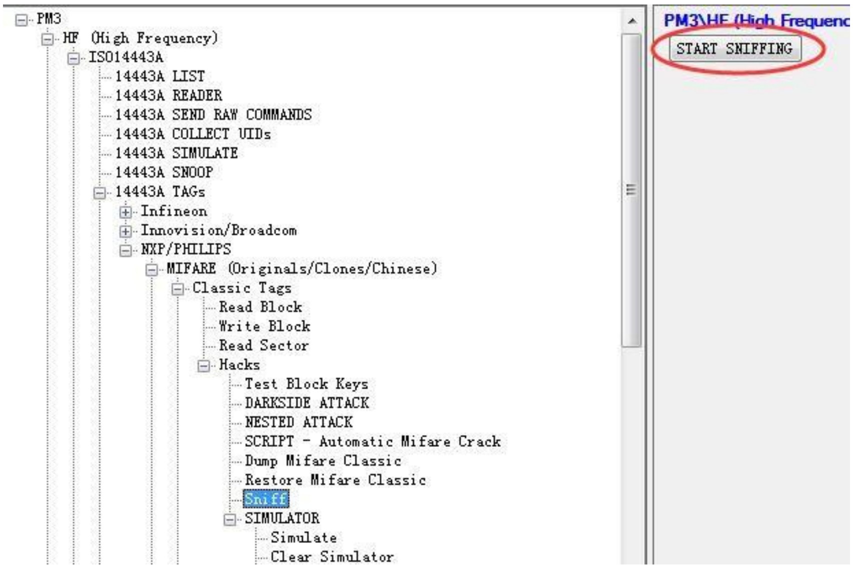
Principle

Pre-stored 12 sets of world-wide, factory default keys for the card, and test them one by one. The factory default of domestic cards is generally "ffffffffffff".

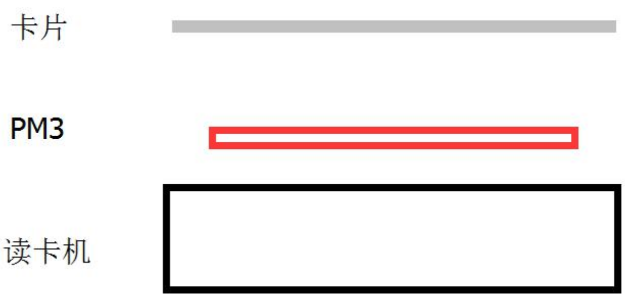
c) (Need to go to the scene) Put the antenna between the card and the card reader to sniff the communication data and extract a sector key.

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

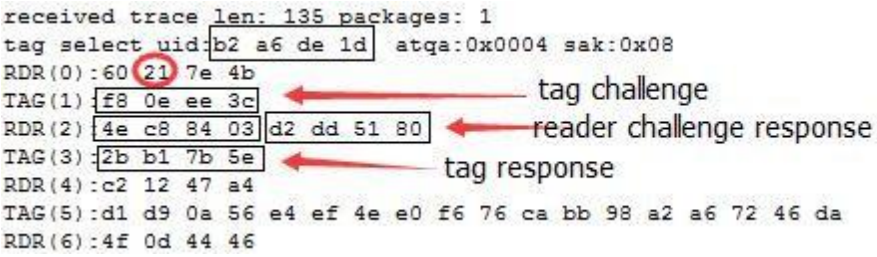
The password obtained by sniffing cannot be specified. It is the sector of the card that the card reader has accessed to obtain which code. When other codes cannot be obtained, only the data of these sectors can be used, and no copying is required. The data of the entire card.



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. None of the three should be placed too close, and there should be no metal shielding on both sides.



In general, you can first stick PM3 on the card reader very close to the position of PM3 and the card reader, and then swipe the card on top of PM3 several times to obtain the most stable data, but the card reading distance will be very close, if you read the card If the card cannot be recognized by the machine, you can gradually increase the distance between the PM3 and the card reader until the card can be swiped normally, the effect is the best. When sniffing, make adjustments according to the actual situation.



```
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
```

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

Pay attention to looking for the data starting with 60 or 61, 60 means to use A password to access, 61 means to use B password. At the beginning, RDR is the instruction issued by the card reader, and TAG is the instruction issued by the card.

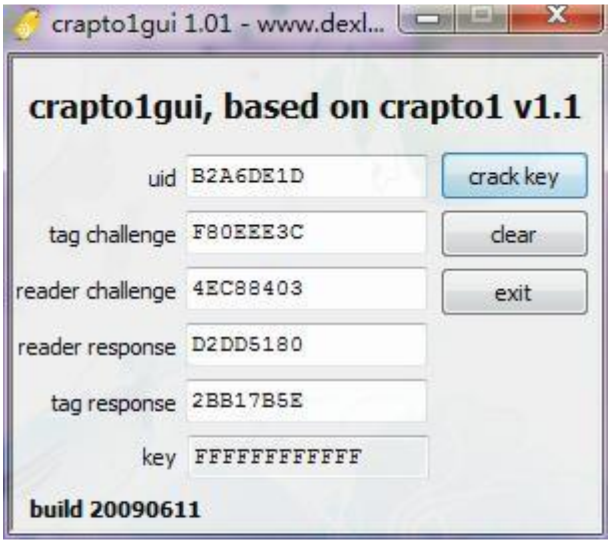
The red circle indicates that the card reader has accessed the 21st block. 21 is hexadecimal, converted to decimal is 33. The first box "b2a6de1d" is the UID of the card

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

The third box "4ec88403" is the reader challenge (the number of reader challenges), the fourth box "d2dd5180" is the reader respones (the number of reader responses), and

the fifth box "2bb17b5e" is the tag respones (card response) number)

Fill in the "crapto1gui.exe" software one by one. (In the "Gadgets" folder)



crapto1gui 1.01 - www.dexl...

crapto1gui, based on crapto1 v1.1

uid B2A6DE1D

tag challenge F80EEE3C

reader challenge 4EC88403

reader response D2DD5180

tag response 2BB17B5E

key FFFFFFFFFFFF

build 20090611

Click crak key to calculate the key. The conclusion is: the card reader uses A to access the 33rd block and the password used is FFFFFFFFFFFF

v. Matters needing attention

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

The card reader must be the one that usually reads this card, not necessarily a card issuer. If the key is not available, it may be that the card reader did not use the password to access the card sector, or it may be due to the poor signal of the card reader.

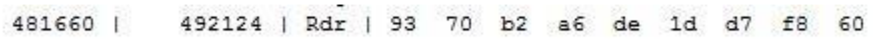
If it is not allowed to bring computers on site. When you want to sniff offline, you need to flash the firmware to version 816.

The command used under 816 is SNOOP instead of Sniff. After sending the command, turn on the power switch, unplug the USB, approach the card reader with the card, and swipe back and forth a few times until the A light goes out. Plug it back into the computer and use hf 14a list to view it. You may reset it first, but the data is still there. After waiting for a few seconds, send hf 14a list again to view the data. Never turn off the PM3 power switch, otherwise data will be lost. The following figure is a comparison of the difference between the two instruction

	848 firmware (old)		2.X.0 under firmware (new)	
	SNOOP order	**Sniff** order	**SNOOP** order	**Sniff** order
Features	Sniffing card readers and card integrity Interactive data	no	Sniffing card readers and card integrity Interactive data	Only show the key to decrypt the M1 card data
usage	Pre-stored in PM3, use hf 14a list Check	no	Pre-stored in PM3, use hf list 14a Check	Display the decrypted key data on the computer in real time
Record length	very short	no	very long	unlimited
Data integrity	Incomplete, easy Lost packets, pick the machine	no	Data is complete and clear Clear and clearly annotated	Data is complete and clear Clear and clearly annotated
Offline recording	support	no	Don’t support	Don’t support
Record object	Support 14443A Any card	no	Support 14443A Any card	Withdraw only M1 card Decrypt data

Need to pay attention to SNOOP, it will not pick automatically. Need to manually find out the valid data segment. Generally judged by similar data length and form。

As shown in the figure above, the beginning of 93 70 means that the card with the UID of b2 a6 de 1d is selected, and there will often be valid data behind. After the card reader selects the card, it is ready to access the card.



```
 481660 |     492124 | Rdr | 93  70  b2  a6  de  1d  d7  f8  60
```

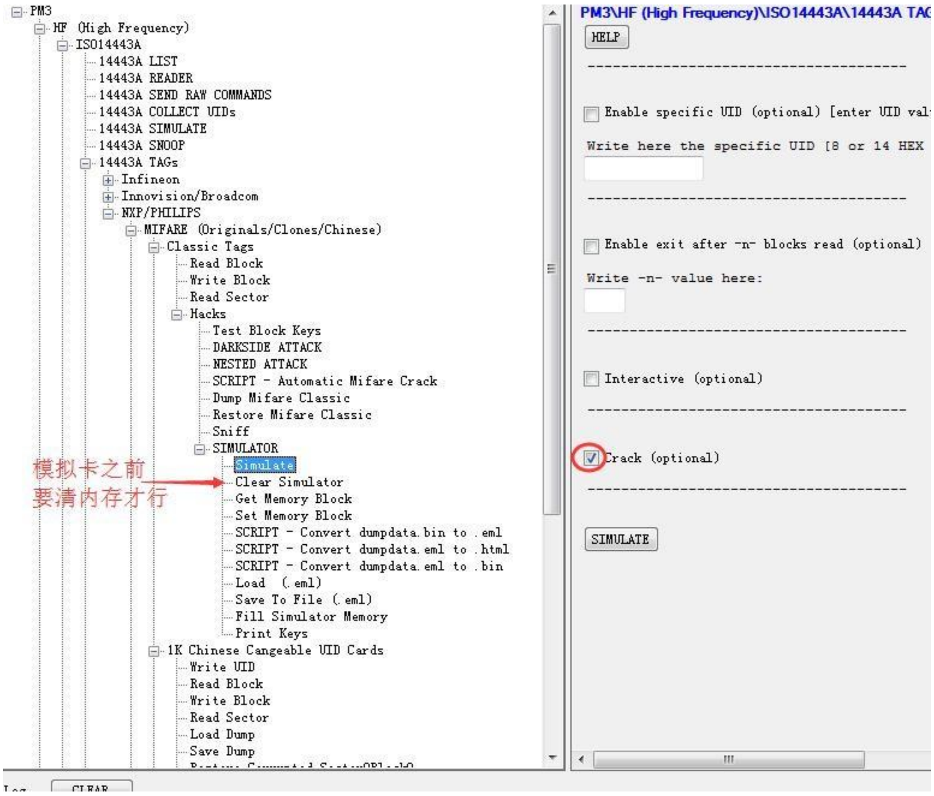
principle

The M1 card uses the crapto1 algorithm when the card reader and the card exchange data and passwords.

Even if the same card and the same password, the interaction data obtained by sniffing is random, but as long as the four sets of random arrays and UID mentioned above are obtained, the key can be reversed.

(Need to go to the scene) Simulate the antenna as an M1 card, induce the card reader to read the card, capture the data, and solve a sector key.

i. Send command: hf mf sim x, or click SIMULATOR in the command tree



模拟卡之前
要清内存才行

PM3\HF (High Frequency)\ISO14443A\14443A TAG

□ Enable specific UID (optional) [enter UID val

Write here the specific UID [8 or 14 HEX

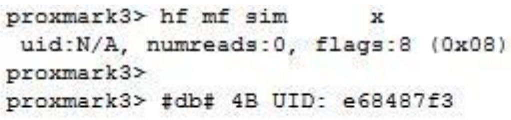
□ Enable exit after -n- blocks read (optional)

Write -n- value here:

□ Interactive (optional)

☑ Crack (optional)

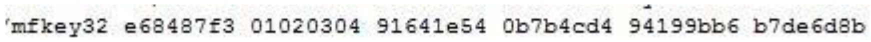
You can leave out the UID to be simulated on the right, PM3 will automatically select a default UID, as shown in the figure below



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

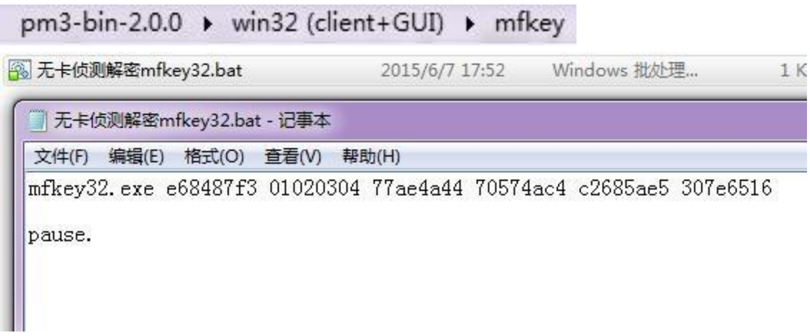
Then swipe the card near the card reader. After finishing press the button

to exit, it will automatically return to the data. Such as :



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

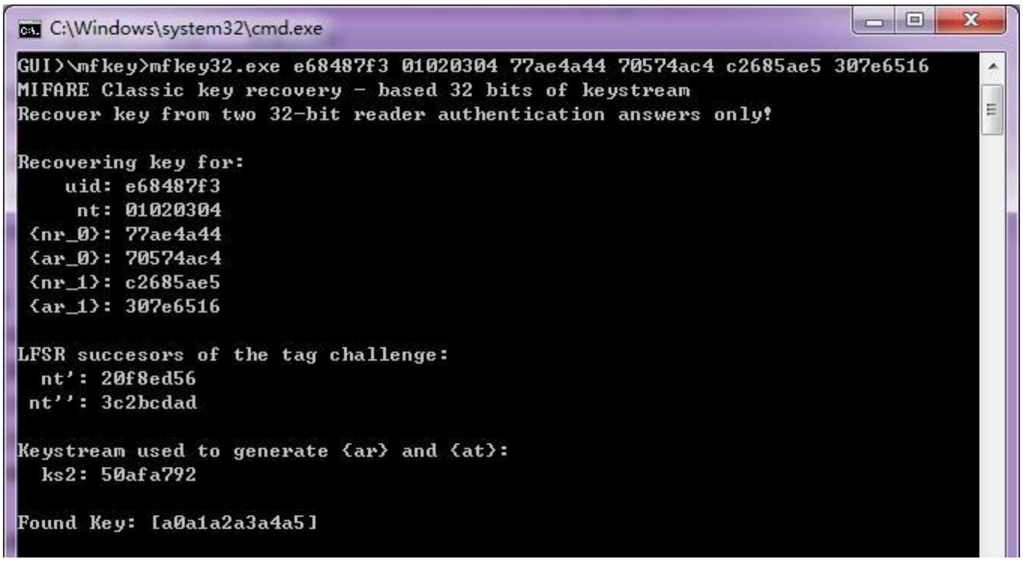
First open the following batch file, modify the data in it and replace it with your own data.


pm3-bin-2.0.0 ▸ win32 (client+GUI) ▸ mfkey
无卡侦测解密mfkey32.bat 2015/6/7 17:52 Windows 批处理... 1 K
无卡侦测解密mfkey32.bat - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
mfkey32.exe e68487f3 01020304 77ae4a44 70574ac4 c2685ae5 307e6516

pause.
```

After the replacement is complete, double-click to open the batch and get the result:



```
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 succesors of the tag challenge:
  nt': 20f8ed56
 nt'': 3c2bcdad

Keystream used to generate {ar} and {at}:
  ks2: 50afa792

Found Key: [a0a1a2a3a4a5]
```

v. **Matters needing attention**

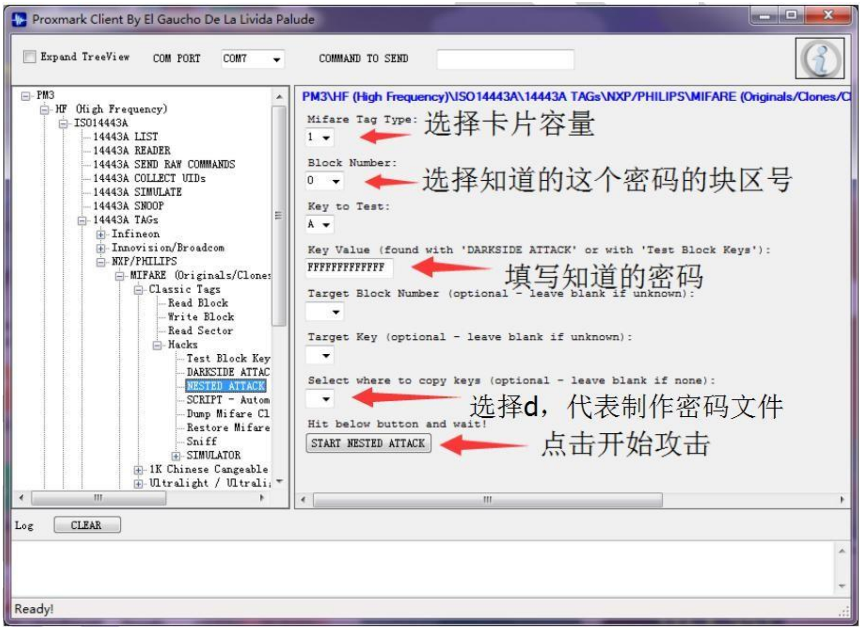
Note that this function is not 100%, and it is not compatible with some card readers and cannot be returned correctly.

1 **Obtain all sector keys through known keys**

Use the command, [hf mf nested 1 0 A ffffffffffff d] one password and more passwords

This is to use the nested authentication vulnerability to use the known key of any sector to obtain the keys of all sectors. This vulnerability has a higher success rate. In the example, it represents the A key ff of sector 0. You can see that a "d" has been added to the tail cone,

If d is not added, the key file will not be output. If d is added, the key will be saved to the file dumpkeys.BIN. When using nested, pay attention to choosing the correct card capacity. 1-4K.



PM3\HF (High Frequency)\ISO14443A\14443A TAGs\NXP/PHILIPS\MIFARE (Originals/Clones/C

Mifare Tag Type: 1 选择卡片容量

Block Number: 0 选择知道的这个密码的块区号

Key to Test: A

Key Value (found with 'DARKSIDE ATTACK' or with 'Test Block Keys'): FFFFFFFFFFFF 填写知道的密码

Target Block Number (optional - leave blank if unknown):

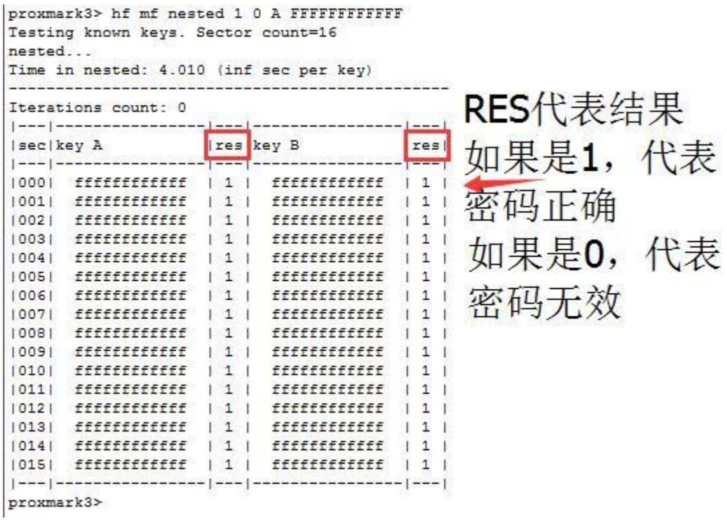
Target Key (optional - leave blank if unknown):

Select where to copy keys (optional - leave blank if none): 选择d，代表制作密码文件

Hit below button and wait!

START NESTED ATTACK 点击开始攻击

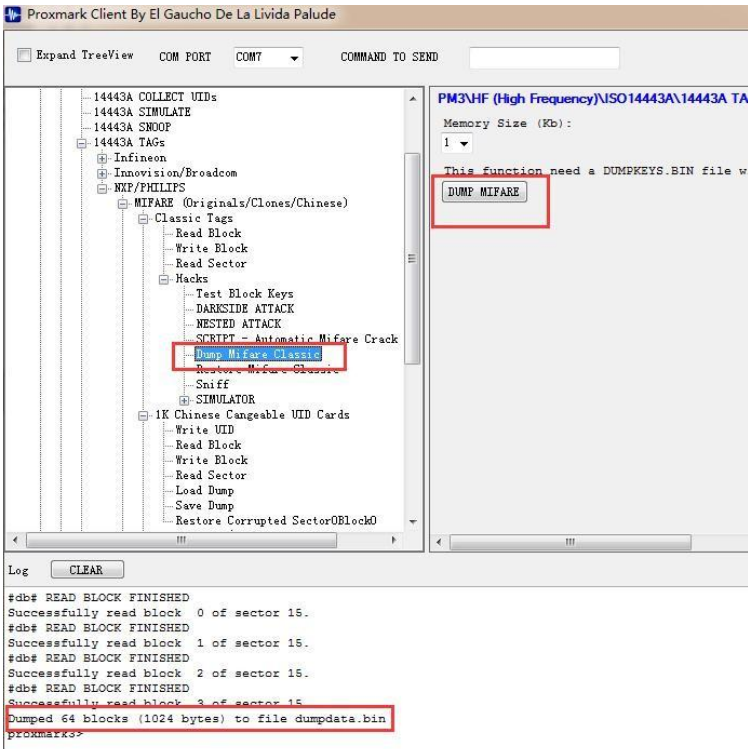
The picture below is a screenshot of a successful attack：



```
proxmark3> hf mf nested 1 0 A FFFFFFFFFFFF
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|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|001|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|002|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|003|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|004|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|005|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|006|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|007|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|008|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|009|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|010|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|011|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|012|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|013|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|014|  ffffffffffff  | 1 |  ffffffffffff  | 1 |
|015|  ffffffffffff  | 1 |  ffffffffffff  | 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

1.Read the card data to the computer



PM3\HF (High Frequency)\ISO14443A\14443A TA

Memory Size (Kb): 1

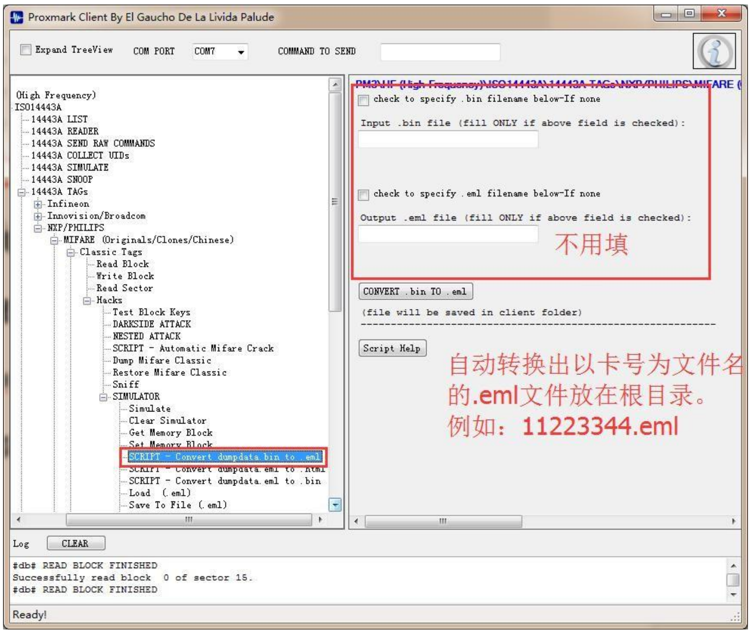
This function need a DUMPKEYS.BIN file w

```
#db# READ BLOCK FINISHED
Successfully read block  0 of sector 15.
#db# READ BLOCK FINISHED
Successfully read block  1 of sector 15.
#db# READ BLOCK FINISHED
Successfully read block  2 of sector 15.
#db# READ BLOCK FINISHED
Successfully read block  3 of sector 15.
Dumped 64 blocks (1024 bytes) to file dumpdata.bin
proxmark3>
```

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

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

First, we need to convert the dumpdata.bin file to the xxxxx.eml format. This format can be opened and viewed with Notepad before it can be retrieved and written into the UID card by PM3.。



PM3\HF (High Frequency)\ISO14443A\14443A TAGs\NXP/PHILIPS\MIFARE (

□ check to specify .bin filename below-If none

Input .bin file (fill ONLY if above field is checked):

□ check to specify .eml filename below-If none

Output .eml file (fill ONLY if above field is checked):

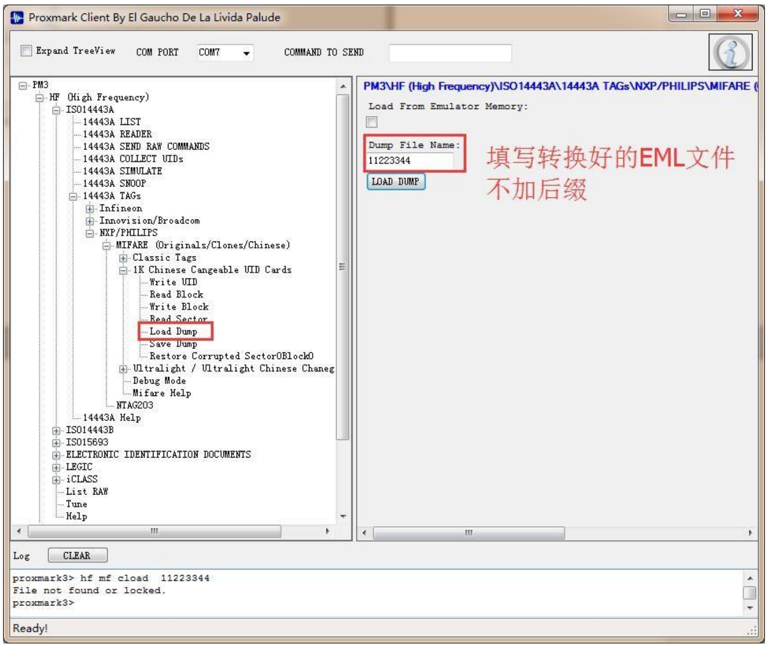
不用填

(file will be saved in client folder)

自动转换出以卡号为文件名的.eml文件放在根目录。
例如：11223344.eml

```
#db# READ BLOCK FINISHED
Successfully read block  0 of sector 15.
#db# READ BLOCK FINISHED
```

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



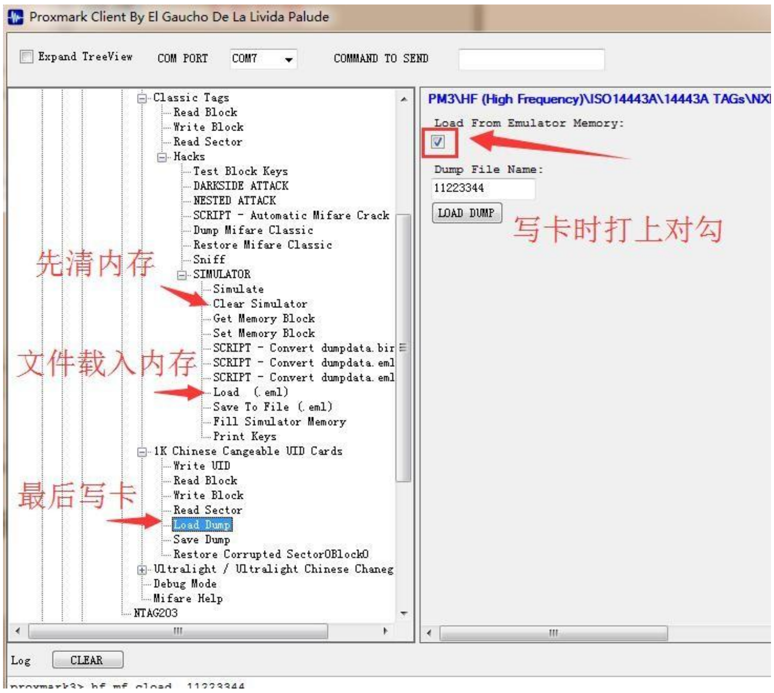
Load From Emulator Memory: □

Dump File Name: 11223344

填写转换好的EML文件
不加后缀

```
proxmark3> hf mf cload  11223344
File not found or locked.
proxmark3>
```

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



先清内存

文件载入内存

最后写卡

Load From Emulator Memory: ☑

Dump File Name: 11223344

写卡时打上对勾

```
proxmark3> hf mf cload  11223344
```

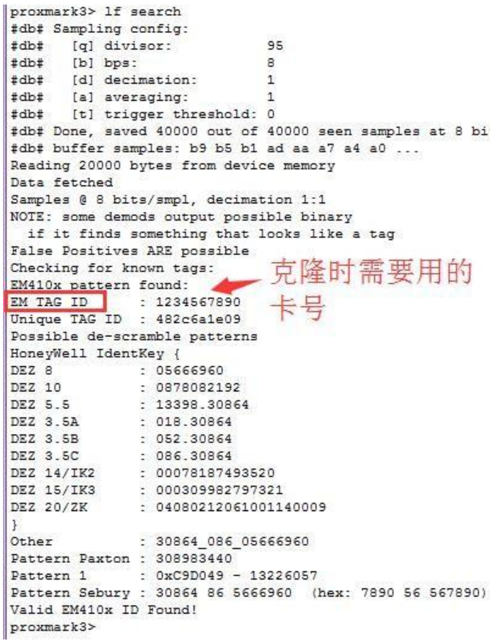
Check the data and complete the clone

Low frequency card operation:

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

First , EM4X is the chip of the ID card we often say. It is a low-frequency card and needs to be read by a circular antenna.

After reading the card, the following data will be displayed, "Valid EM410X ID Found!" means that the serial number of the ID card has been read.。



```
proxmark3> lf search
#db# Sampling config:
#db#   [q] divisor:           95
#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 bi
#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  : 482c6a1e09
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     : 00078187493520
DEZ 15/IK3     : 000309982797321
DEZ 20/ZK      : 04080212061001140009
}
Other          : 30864_086_05666960
Pattern Paxton : 308983440
Pattern 1      : 0xC9D049 - 13226057
Pattern Sebury : 30864 86 5666960  (hex: 7890 56 567890)
Valid EM410x ID Found!
proxmark3>
```

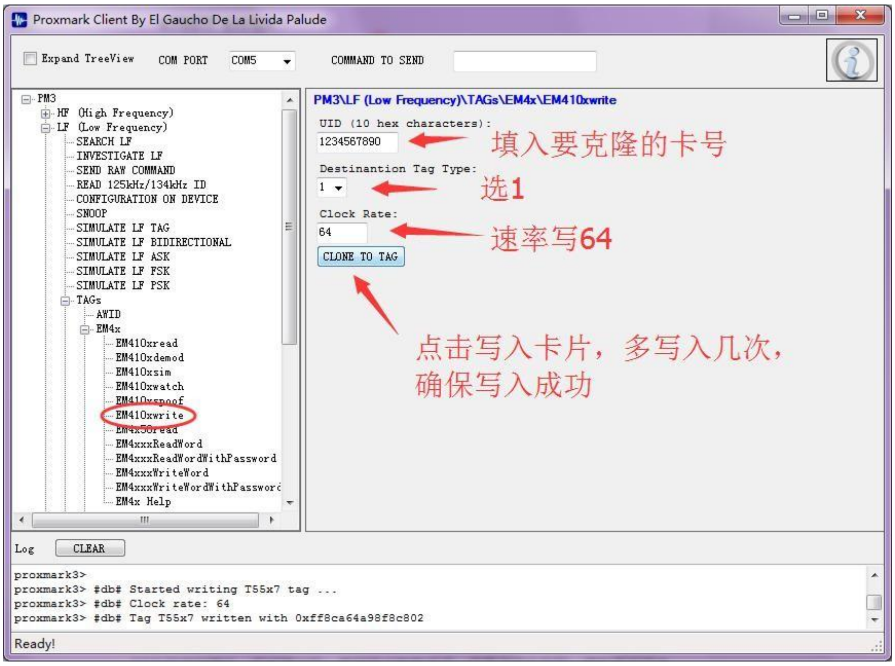
克隆时需要用的卡号

Record the serial number behind the EM TAG ID in the figure above, and that's it.

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

1. Write different types to T5577 card

to clone the card : Clone into ID card :



PM3\LF (Low Frequency)\TAGs\EM4x\EM410xwrite

UID (10 hex characters): 1234567890

Destinantion Tag Type: 1

Clock Rate: 64

填入要克隆的卡号

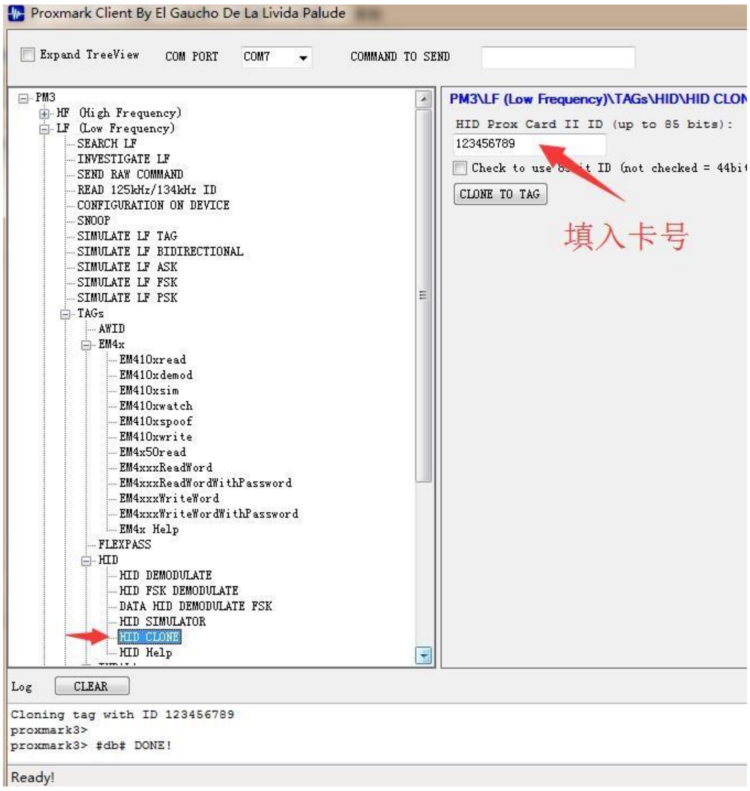
选1

速率写64

点击写入卡片，多写入几次，确保写入成功

```
proxmark3>
proxmark3> #db# Started writing T55x7 tag ...
proxmark3> #db# Clock rate: 64
proxmark3> #db# Tag T55x7 written with 0xff8ca64a98f8c802
```

Clone into HID card：

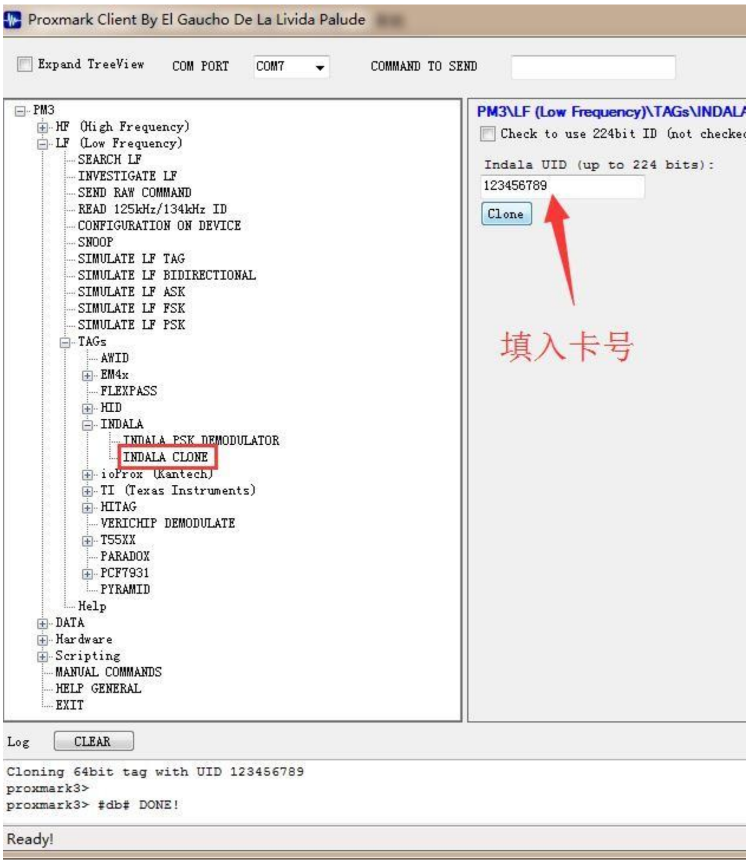


HID Prox Card II ID (up to 85 bits):
123456789

□ Check to use 64bit ID (not checked = 44bit

```
Cloning tag with ID 123456789
proxmark3>
proxmark3> #db# DONE!
```

Clone into INDALA card：

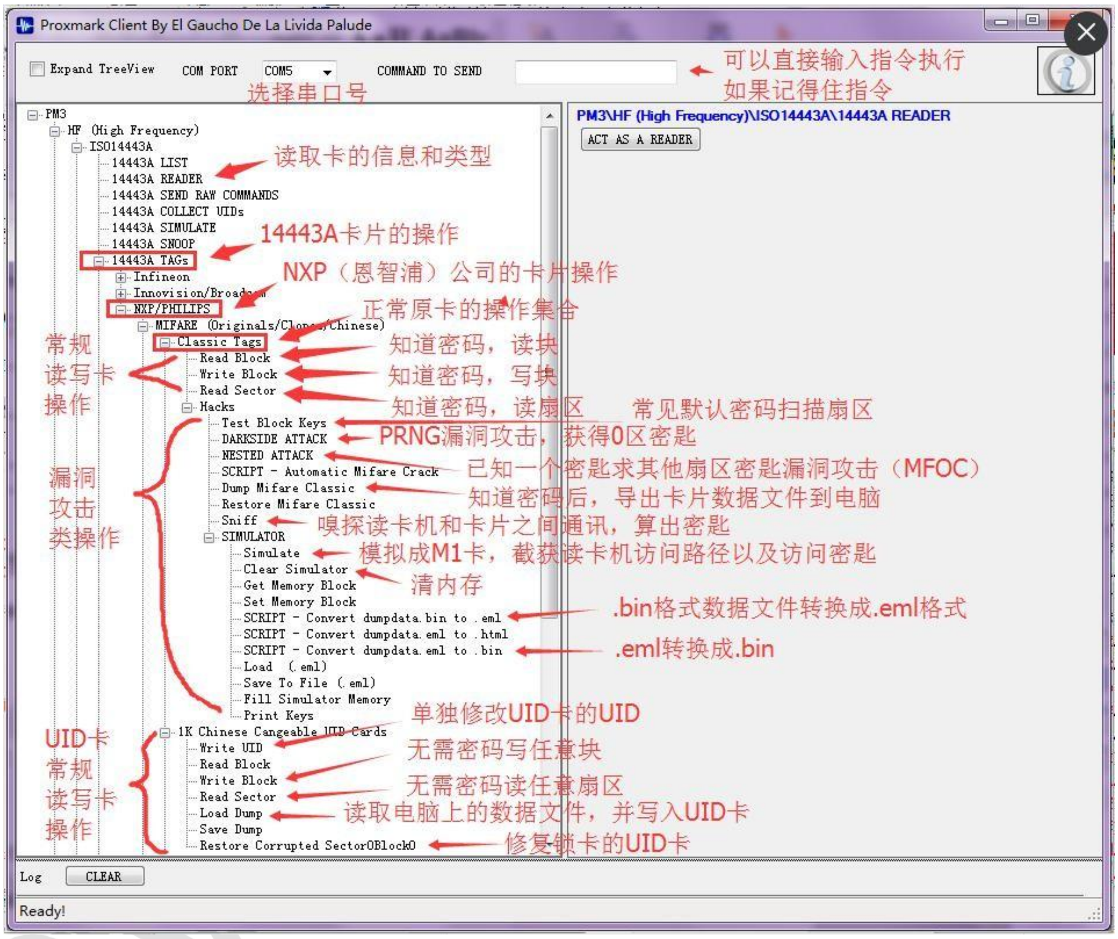


□ Check to use 224bit ID (not checked

Indala UID (up to 224 bits):
123456789

```
Cloning 64bit tag with UID 123456789
proxmark3>
proxmark3> #db# DONE!
```

七 . Software introduction：



The figure 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 restarting the software multiple times: PM3 often crashes when running some commands and needs to reconnect to the USB. Often the software also needs to be reopened. If you disconnect the USB, select the serial port to another number, plug in PM3, and then select the serial port to the correct number after the ding-dong sound. This can avoid the trouble of restarting the software every time.

八 . Note：

1. Hardware matters：

As PM3 is developed by hackers amateurs, it does not consider too much in terms of ease of use and humanization, so it often crashes, some commands do not have a clear success and failure response, and some details are not handled well.

Therefore, when the device is running the attack command, if the card does not support or does not put the card, it will directly crash. After the crash, the device needs to be plugged and unplugged at any time to force the computer's serial port to connect normally. During the decryption operation, the ABCD four LEDs on the device should be used as the operating basis. If the LED is flashing, it means it is in progress. If it is completely off or always on, it means the attack has failed. Waiting for all to be off means it has stopped running. Unplug and plug the device again.

2. Software matters :

Computer software

The software can use the CMD command line, the English GUI with the blue icon, or the Chinese GUI we opened.

	Official CMD command line （PM3 command console.bat）	GUI （Proxmark Tool.exe）	GUI （Proxmark3_EASY_GUI.exe）
principle	调用Proxmark3.exe	调用Proxmark3.exe	调用 Proxmark3.exe
Report poison	no	no	Will misidentify and report poison
Read and write UID card	Read and write, compatible with display ″NO″ UID card	Read and write, compatible with display ″NO″ UID card	Read and write, only compatible with reading and writing Good UID card
Read and write FUID/CUID	Read and write, need manual order Solo block	Read and write, need manual order Solo block	Read and write, after loading the file Write full card
Ease of use	Not easy to use, need to recite English Text instruction	Generally easy to use, need to watch English Text operation, comprehensive functions	Easy to use, extract frequently used functions Later, a small function was added
compatibility	High compatibility, cross-platform	Windows Good platform compatibility	Sometimes it will flash back when open, open Can be solved twice
Keychain card DUMP data	There is no automatic reread mechanism, Easy to interrupt and not smooth.	There is no automatic reread mechanism, Easy to interrupt and not smooth.	Added an automatic reread mechanism, The small card is also smoothly read

Device firmware

The firmware is arranged from the old to the new: r486→756→816→848→852→1.0.0→2.0.0→2.5.0 old firmware before entering hw version to directly see the version number.

After 1.0.0, only the date will be returned, and the version number will be judged by the date.

```
2.0.0： #db# bootrom: /-suspect 2015-04-02 15:12:04

        #db# os: /-suspect 2015-04-02 15:12:11

        #db# HF FPGA image built on 2015/03/09 at 08:41:42

2.5.0： bootrom: /-suspect 2015-11-19 10:08:02

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

        LF FPGA image built for 2s30vq100 on 2015/03/06 at 07:38:04

        HF FPGA image built for 2s30vq100 on 2015/11/ 2 at  9: 8: 8
```

九．Instruction introduction

【Hw tune】Antenna tuning voltage test

The command is used to test the antenna resonance voltage. When testing, the antenna should be upright, away from metal and away from the card, in order to obtain an accurate voltage. Sometimes the voltage may be lower than the nominal value. The voltage of the antenna does not affect any operation and function. In fact, it can be used normally if the high frequency exceeds 5V and the low frequency exceeds 10V. It's just that the higher the voltage, the farther the card reading distance will be.

【Hf 14a reader】Type of card reader
As a card reader, read the high-frequency card ID, test the type of the high-frequency card, put the card first, and then execute the command.

[Hf mf chk 0 A ffffffffffff] Check password
For M1 card, check whether the A password of sector 0 is ff....

[Hf mf chk *1? T] Check the default password
For M1 cards, check whether there are default passwords in all sectors, that is, automatically use the default passwords in the dictionary to verify 16 sectors.
(Most of the cards are used to modify the password of the used sector, the unused is the factory default password, the default password of individual manufacturers will be different, PM3 built-in more than ten common default passwords)

[Hf mf mifare] PRNG attack
This is a test for a PRNG vulnerability. The password of the first sector can be calculated directly through the vulnerability, which is also called blasting. Not all cards support this vulnerability. Sometimes the English "Can’ t select card" will be prompted during the process. This is a BUG prompt, please ignore it. If ABCD keeps flashing during operation, it means it can be cracked, just wait for the result.
For unsupported cards, no matter how you adjust the card position, the LED will not change, and PM3 will eventually reset and drop.

(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 1 0 A ffffffffffff d] One password has more passwords

This is to use the nested authentication vulnerability to use the known key of any sector to obtain the keys of all sectors. This vulnerability has a higher success rate. In the example, it represents the A key ff of sector 0. You can see that a "d" has been added to the tail cone,
If d is not added, the key file will not be output. If d is added, the key will be saved to the file dumpkeys.BIN. When using nested, pay attention to choosing the correct card capacity. 1-4K.

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

This command reads and saves the data of all sectors of the card in the binary file dumpdata.BIN on the premise of obtaining all the keys. Then you can use "UltraEdit" to open the file and cross-compare with other data. The UltraEdit installation package is in "Gadgets".

[Hf mf cload e dumpdata.eml] Clone data to UID card

Write dump data to UID card. Followed by the data file name "dumpdata.eml". The dumpdata.bin generated earlier cannot be imported directly, it needs to be converted to eml and then imported. The card data in Eml format must contain complete 64 rows of data. After the conversion is completed, the integrity of the dumpdata file needs to be confirmed. (The conversion format can be converted with its own script)

After cloning is completed, we can DUMP the UID card data again in the same way for comparison. Or read some sectors individually for comparison.

[Hf mf csetuid 1234bcdf] Modify the UID of the UID card

Modify the UID of the UID card to 1234bcdf, and the UID is four bytes.

【hf mf eclr】**Clear the cache**

Before monitoring the card reader without a card, be sure to clear the cache.

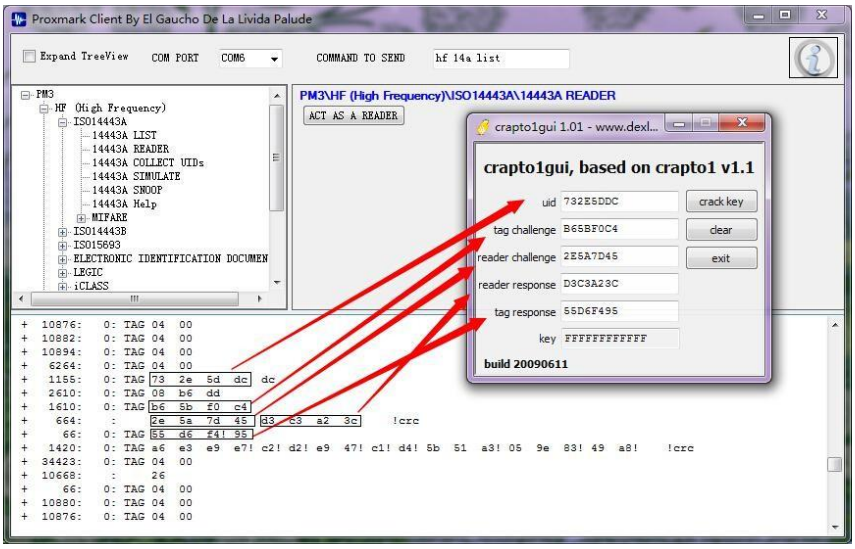
[Hf mf sim x] No card monitor card reader

The antenna of PM3 is simulated as a card, which induces the card reader to read the card, and captures the verification key issued by the card reader. Cannot operate offline, press the button to exit after monitoring.

[Hf 14a snoop] There is a card to monitor the card reader to get a secret

2.0.0 Firmware online monitoring:

Click SNOOP or enter the command directly to enter the monitoring mode. The antenna and the card are close to the card reader. The card reader can operate the card. The four LEDs will change. After the monitoring is completed, press the button to exit. The four LEDs will go out. Then send the command hf list 14a to view the monitoring results.



Proxmark Client By El Gaucho De La Livida Palude

☐ Expand TreeView   COM PORT: COM6   COMMAND TO SEND: hf 14a list

crapto1gui, based on crapto1 v1.1

uid: 732E5DDC
tag challenge: B65BF0C4
reader challenge: 2E5A7D45
reader response: D3C3A23C
tag response: 55D6F495
key: FFFFFFFFFFFF

build 20090611

```
+  10876:    0: TAG 04  00
+  10882:    0: TAG 04  00
+  10894:    0: TAG 04  00
+   6264:    0: TAG 04  00
+   1155:    0: TAG 73  2e  5d  dc  dc
+   2610:    0: TAG 08  b6  dd
+   1610:    0: TAG b6  5b  f0  c4
+    664:     :     2e  5a  7d  45  d3  c3  a2  3c      !crc
+     66:    0: TAG 55  d6  f4! 95
+   1420:    0: TAG a6  e3  e9  e7! c2! d2! e9  47! c1! d4! 5b  51  a3! 05  9e  83! 49  a8!    !crc
+  34423:    0: TAG 04  00
+  10668:     :     26
+     66:    0: TAG 04  00
+  10880:    0: TAG 04  00
+  10876:    0: TAG 04  00
```

Find the data structure group as shown in the figure above, and that's it. If there is no 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 password verification operations.
2. The signal of individual card readers is poor and no signal can be recorded.

3.The distance between the card and the PM3 antenna should be a certain distance, not too far nor too close, about one centimeter. The password can be calculated by entering the corresponding data into the gadget.

【lf em4x em410xwatch】**Read low frequency card ID**

This command is to read the ID of the low-frequency card. A low-frequency antenna is required. The command is executed first and then the card is released. Colleagues who record the ID need to pay attention to the value of the clock rate, which is generally 64.

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

[Lf em4x em410xwrite 12345bcdef 1 64] Write ID to T5577 card

Write the ID number into the T5577 card. The length is 10-bit hex. In the example, 12345bcdef is the ID, the following "1" is the card type of T55X7, and 64 is the clock rate.

All the above instructions can be found in the instruction tree on the left side of the host computer software. Move the mouse on the right side to the corresponding box, there are English prompts and user guides, and translations are not listed one by one.

Question collection:

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.A8cload.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

FCC WARNING

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.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: 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.

To maintain compliance with FCC’s RF Exposure guidelines, This equipment should be installed and operated with minimum 20cm distance between the radiator and your body: Use only the supplied antenna.