

目录

1 认识 Proxmark3 Easy	2
2 安装客户端	2
3 升级固件	2
4 复制卡	3

1 认识 Proxmark3 Easy

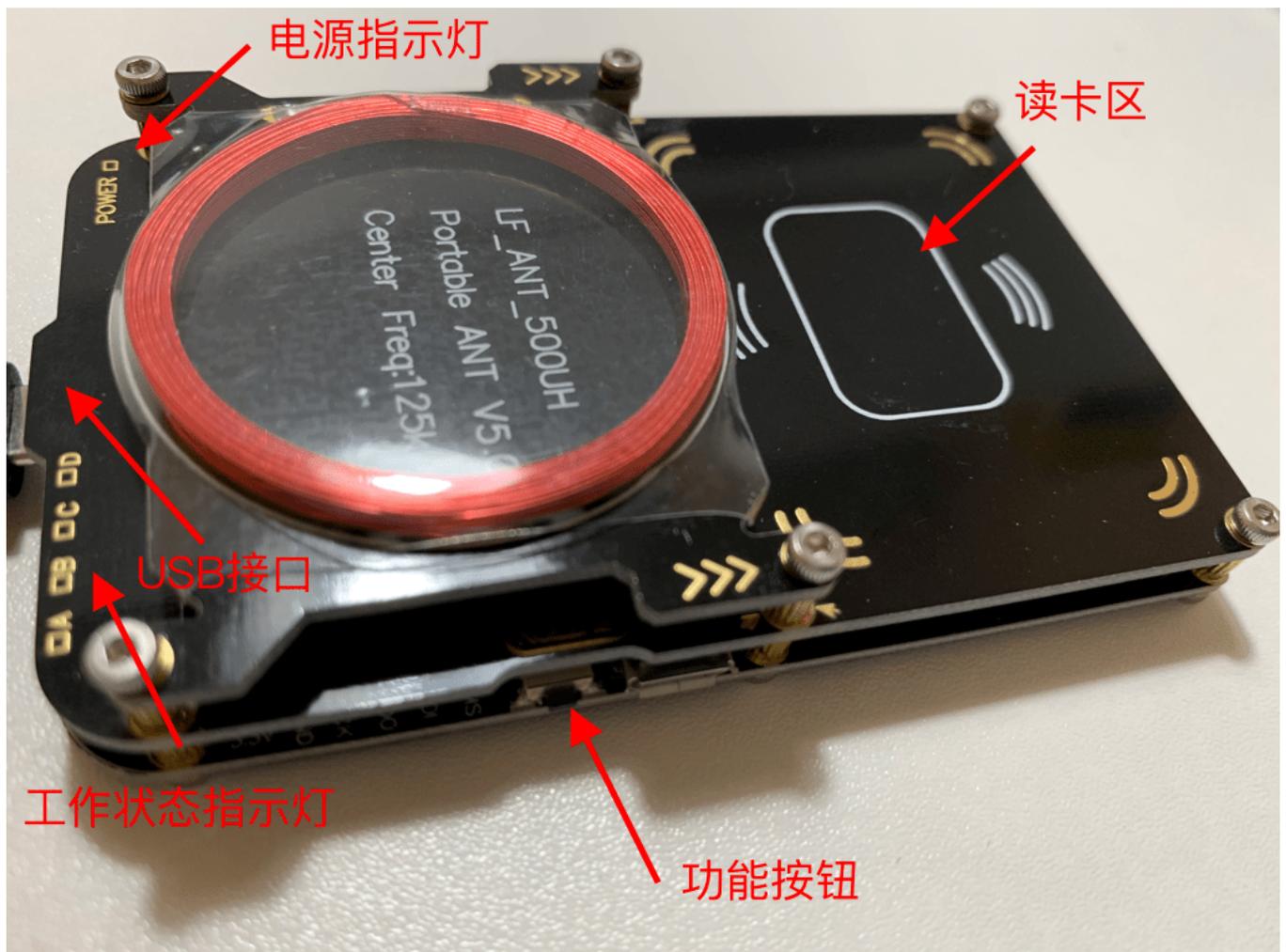


Figure 1: Proxmark3 Easy

2 安装客户端

使用 Homebrew 安装 proxmark3 客户端

```
brew tap proxmark/proxmark3  
brew install --HEAD proxmark3
```

3 升级固件

拿到手的 proxmark3 的固件比较旧，一般没有办法直接破解卡 Key。

电脑上插上 Proxmark3，查看设备 `/dev/tty.usbmodem*****`

```
git clone https://github.com/Proxmark/proxmark3.git  
cd proxmark3  
make clean  
make
```

```
./client/flasher /dev/tty.usbmodem***** -b bootrom/obj/bootrom.elf  
↪ armsrc/obj/fullimage.elf
```

注意更新固件之后，设备的名称会发生变化，查看新的设备名称
proxmark3 /dev/tty.usbmodem*****

4 复制卡



Figure 2: ID、IC 卡

在读卡区放上原卡

```
proxmark3> hf 14a read  
UID : e5 2c 98 f0  
ATQA : 00 04  
SAK : 08 [2]  
Field dropped.  
proxmark3> hf mf chk 0 A  
--chk keys. sectors: 1, block no: 0, key type:A, eml:n, dmp=n checktimeout=471 us  
No key specified, trying default keys  
chk default key[ 0] ffffffffffffff  
chk default key[ 1] 000000000000  
chk default key[ 2] a0a1a2a3a4a5  
chk default key[ 3] b0b1b2b3b4b5  
chk default key[ 4] aabbccddeeff
```

```

chk default key[ 5] 1a2b3c4d5e6f
chk default key[ 6] 123456789abc
chk default key[ 7] 010203040506
chk default key[ 8] 123456abcdef
chk default key[ 9] abcdef123456
chk default key[10] 4d3a99c351dd
chk default key[11] 1a982c7e459a
chk default key[12] d3f7d3f7d3f7
chk default key[13] 714c5c886e97
chk default key[14] 587ee5f9350f
chk default key[15] a0478cc39091
chk default key[16] 533cb6c723f6
chk default key[17] 8fd0a4f256e9
    
```

```

|---|-----|-----|
|sec|key A          |key B          |
|---|-----|-----|
|000| ffffffff        | ?             |
|---|-----|-----|
    
```

```

proxmark3> hf mf nested 1 0 A ffffffff d
--nested. sectors:16, block no: 0, key type:A, eml:n, dmp=y checktimeout=471 us
Testing known keys. Sector count=16
nested ...
    
```

```

-----
Nested statistic:
Iterations count: 0
Time in nested: 0.328 (inf sec per key)
|---|-----|---|-----|---|
|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 |
|---|-----|---|-----|---|
    
```

Printing keys to binary file dumpkeys.bin...

```
proxmark3> hf mf dump
|-----|
|----- Reading sector access bits ... -----|
|-----|
#db# READ BLOCK FINISHED
|-----|
|----- Dumping all blocks to file ... -----|
|-----|
#db# READ BLOCK FINISHED
Successfully read block 0 of sector 0.
#db# READ BLOCK FINISHED
Successfully read block 1 of sector 0.
#db# READ BLOCK FINISHED
Successfully read block 2 of sector 0.
#db# READ BLOCK FINISHED
Successfully read block 3 of sector 0.
#db# READ BLOCK FINISHED
Successfully read block 0 of sector 1.
#db# READ BLOCK FINISHED
Successfully read block 1 of sector 1.
#db# READ BLOCK FINISHED
Successfully read block 2 of sector 1.
#db# READ BLOCK FINISHED
Successfully read block 3 of sector 1.
#db# READ BLOCK FINISHED
Successfully read block 0 of sector 2.
#db# READ BLOCK FINISHED
Successfully read block 1 of sector 2.
#db# READ BLOCK FINISHED
Successfully read block 2 of sector 2.
#db# READ BLOCK FINISHED
Successfully read block 3 of sector 2.
#db# READ BLOCK FINISHED
Successfully read block 0 of sector 3.
#db# READ BLOCK FINISHED
Successfully read block 1 of sector 3.
```

```
#db# READ BLOCK FINISHED
Successfully read block 2 of sector 3.
#db# READ BLOCK FINISHED
Successfully read block 3 of sector 3.
#db# READ BLOCK FINISHED
Successfully read block 0 of sector 4.
#db# READ BLOCK FINISHED
Successfully read block 1 of sector 4.
#db# READ BLOCK FINISHED
Successfully read block 2 of sector 4.
#db# READ BLOCK FINISHED
Successfully read block 3 of sector 4.
#db# READ BLOCK FINISHED
Successfully read block 0 of sector 5.
#db# READ BLOCK FINISHED
Successfully read block 1 of sector 5.
#db# READ BLOCK FINISHED
Successfully read block 2 of sector 5.
#db# READ BLOCK FINISHED
Successfully read block 3 of sector 5.
#db# READ BLOCK FINISHED
Successfully read block 0 of sector 6.
#db# READ BLOCK FINISHED
Successfully read block 1 of sector 6.
#db# READ BLOCK FINISHED
Successfully read block 2 of sector 6.
#db# READ BLOCK FINISHED
Successfully read block 3 of sector 6.
#db# READ BLOCK FINISHED
Successfully read block 0 of sector 7.
#db# READ BLOCK FINISHED
Successfully read block 1 of sector 7.
#db# READ BLOCK FINISHED
Successfully read block 2 of sector 7.
#db# READ BLOCK FINISHED
Successfully read block 3 of sector 7.
#db# READ BLOCK FINISHED
Successfully read block 0 of sector 8.
#db# READ BLOCK FINISHED
Successfully read block 1 of sector 8.
#db# READ BLOCK FINISHED
Successfully read block 2 of sector 8.
#db# READ BLOCK FINISHED
Successfully read block 3 of sector 8.
#db# READ BLOCK FINISHED
Successfully read block 0 of sector 9.
#db# READ BLOCK FINISHED
Successfully read block 1 of sector 9.
#db# READ BLOCK FINISHED
Successfully read block 2 of sector 9.
#db# READ BLOCK FINISHED
```

```
Successfully read block 3 of sector 9.  
#db# READ BLOCK FINISHED  
Successfully read block 0 of sector 10.  
#db# READ BLOCK FINISHED  
Successfully read block 1 of sector 10.  
#db# READ BLOCK FINISHED  
Successfully read block 2 of sector 10.  
#db# READ BLOCK FINISHED  
Successfully read block 3 of sector 10.  
#db# READ BLOCK FINISHED  
Successfully read block 0 of sector 11.  
#db# READ BLOCK FINISHED  
Successfully read block 1 of sector 11.  
#db# READ BLOCK FINISHED  
Successfully read block 2 of sector 11.  
#db# READ BLOCK FINISHED  
Successfully read block 3 of sector 11.  
#db# READ BLOCK FINISHED  
Successfully read block 0 of sector 12.  
#db# READ BLOCK FINISHED  
Successfully read block 1 of sector 12.  
#db# READ BLOCK FINISHED  
Successfully read block 2 of sector 12.  
#db# READ BLOCK FINISHED  
Successfully read block 3 of sector 12.  
#db# READ BLOCK FINISHED  
Successfully read block 0 of sector 13.  
#db# READ BLOCK FINISHED  
Successfully read block 1 of sector 13.  
#db# READ BLOCK FINISHED  
Successfully read block 2 of sector 13.  
#db# READ BLOCK FINISHED  
Successfully read block 3 of sector 13.  
#db# READ BLOCK FINISHED  
Successfully read block 0 of sector 14.  
#db# READ BLOCK FINISHED  
Successfully read block 1 of sector 14.  
#db# READ BLOCK FINISHED  
Successfully read block 2 of sector 14.  
#db# READ BLOCK FINISHED  
Successfully read block 3 of sector 14.  
#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
```

换上一张新的空白卡，等待写入成功就可以了

```
proxmark3> mf 14a read  
proxmark3> restore
```