

# RFID 系列之入门篇

By:欧欧

Email:Admin@hkmjj.com

咳咳，其实设备早发过来了。由于一系列问题，所以才拖到现在给大家做个小小小基本文档。设备到手，马上去官方下载了驱动。

官 方: <http://www.acs.com.hk>

驱动地址: [http://www.acs.com.hk/drivers/eng/ACR122USAM\\_MSI\\_Winx86\\_1120\\_P.zip](http://www.acs.com.hk/drivers/eng/ACR122USAM_MSI_Winx86_1120_P.zip)

工具列表: <http://www.acs.com.hk/index.php?pid=tools>

这东西开源的，所以大家自由发挥，因为设备来了。所以先给大家演示一下基本内容，个人感觉关注这些的国内不多，所以也是从基本开始吧。。。。。

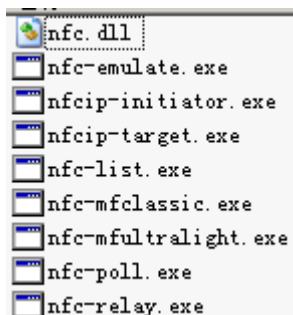
首先 Show 下设备。



感觉还不错吧，因为以前接触的是 ID 卡，也就是门卡。。想深入了解，必须凑齐一些设备。

如同前辈的一句话：一把瑞士军刀都有相同的特点，为什么要集成那么多 very Good!!

介绍下工具吧如图所示：

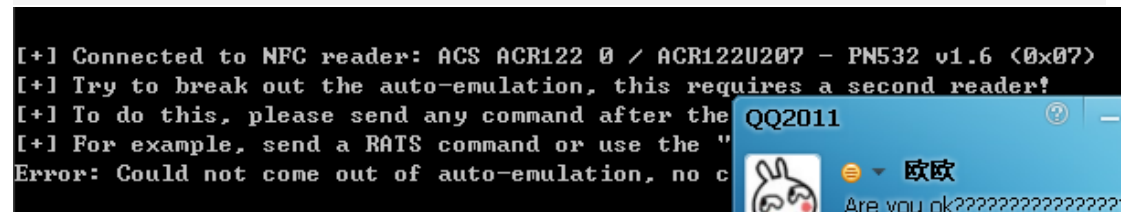


来介绍一下各种功能吧。

Nfc.dll→属于核心物品，必不可少的。。

Nfc-emulate→ 属于模仿必备良品。大家应该也知道，模仿一个东西很简单，不过你不了解里面的核心东西，那么有什么用呢？？？等下在介绍复制 模仿 克隆 读写的关系吧。。

```
[+] Connected to NFC reader: ACS ACR122 0 / ACR122U207 - PN532 v1.6 (0x07)
[+] Try to break out the auto-emulation, this requires a second reader!
[+] To do this, please send any command after the
[+] For example, send a RATS command or use the "
Error: Could not come out of auto-emulation, no c
```

A screenshot of a terminal window with a black background and white text. The text shows the process of connecting to an NFC reader (ACS ACR122 0 / ACR122U207 - PN532 v1.6 (0x07)) and attempting to break out of auto-emulation. The process fails with the error "Error: Could not come out of auto-emulation, no c". In the foreground, there is a QQ chat window titled "QQ2011" with a blue header. It shows a chat bubble with a rabbit icon and the text "Are you ok????????????????????".

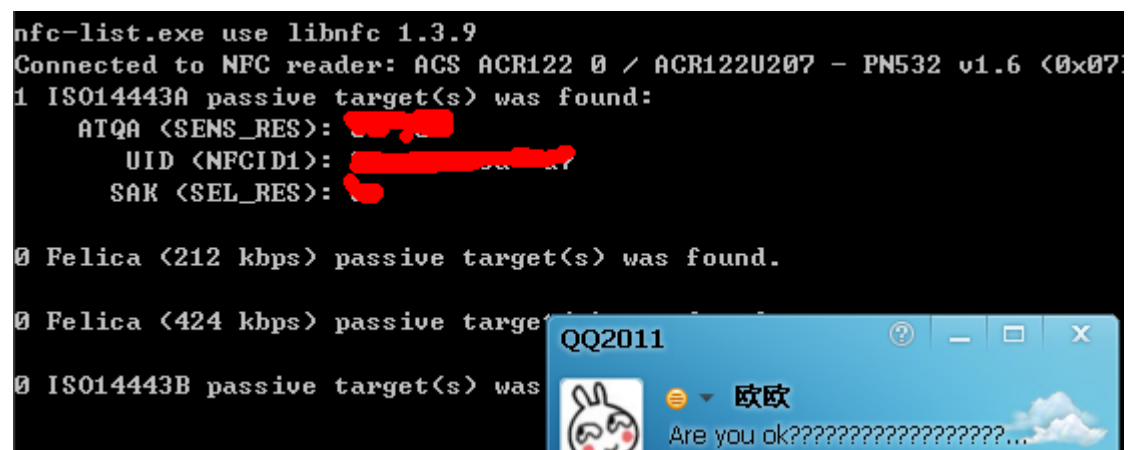
Nfcip-initiator.exe→ 这个东西我也不知道是啥玩意，似乎是啥初始化什么什么东西来着。。不详。。

nfcip-target.exe→ 同上。初始化程序玩意。

nfc-list.exe→ 这个就是读取卡里面的 UID SAK 以及一些基本信息并不是卡里面的核心内容

```
nfc-list.exe use libnfc 1.3.9
Connected to NFC reader: ACS ACR122 0 / ACR122U207 - PN532 v1.6 (0x07)
1 ISO14443A passive target(s) was found:
  ATQA (SENS_RES): 
  UID (MFCID1): 
  SAK (SEL_RES): 

0 Felica (212 kbps) passive target(s) was found.
0 Felica (424 kbps) passive target(s) was found.
0 ISO14443B passive target(s) was found.
```

A screenshot of a terminal window with a black background and white text. The text shows the output of the nfc-list.exe command, indicating that it is using libnfc 1.3.9 and is connected to the same NFC reader. It reports finding three types of passive targets: 1 ISO14443A, 0 Felica (212 kbps), and 0 Felica (424 kbps). The details for the ISO14443A target are shown, with some fields (ATQA, UID, SAK) redacted with red boxes. In the foreground, there is a QQ chat window titled "QQ2011" with a blue header. It shows a chat bubble with a rabbit icon and the text "Are you ok????????????????????...".

nfc-mfclassic.exe→ 进行读取或写入。。

```
Usage: nfc-mfclassic.exe r!w a!b <dump.mfd> [<keys.mfd>]
  r!w          - Perform read from <r> or write to <w> card
  a!b          - Use A or B keys for action
  <dump.mfd>   - MiFare Dump <MFD> used to write <card to MFD> or <MFD to card>

  <keys.mfd>   - MiFare Dump <MFD> that contain the keys <optional>
Or: nfc-mfclassic.exe x <dump.mfd> <payload.bin>
  x            - Extract payload <data blocks> from MFD
  <dump.mfd>   - MiFare Dump <MFD> that contains wanted payload
  <payload.bin> - Binary file where payload will be extracted
```

nfc-mfultralight.exe→ 这个就同上了，意思差不多写入或读取卡片。

```
nfc-mfultralight.exe r!w <dump.mfd>

r!w          - Perform read from or write to card
<dump.mfd>   - MiFare Dump <MFD> used to write <card to MFD> or <MFD to card>
```

nfc-poll.exe→ 这个就是 nfc-list.exe 差不多啦，读取基本信息

```
Connected to NFC reader: ACS ACR122 0 / ACR122U207 - PN532 v1.6 (0x07)
PN53x will poll during 6000 ms
1 target(s) have been found.
T1: targetType=10, targetData:
  ATQA <SENS_RES>: 00 04
  UID <NFCID1>: 3e 80 6a a7
  SAK <SEL_RES>: 08
```

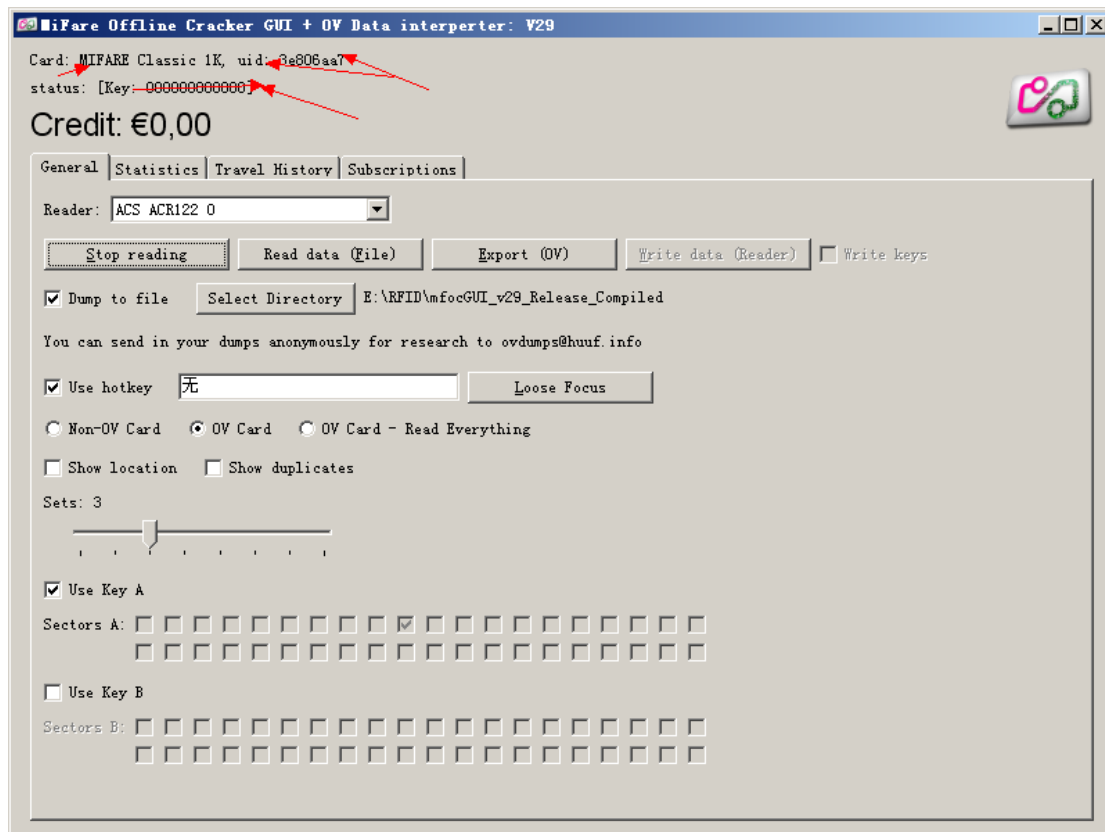
nfc-relay.exe—>未知

---

---

介绍完毕了，现在介绍一下 Gui 的工具吧。

mfocGUI—>这个玩意怎么说呢，可以说是爆破的把，不过不是遍历，而是根据一些默认密码进行爆破。在 Keys 文件夹里面生成一个.dump 的文件。



这个大家应该可以看出来吧。

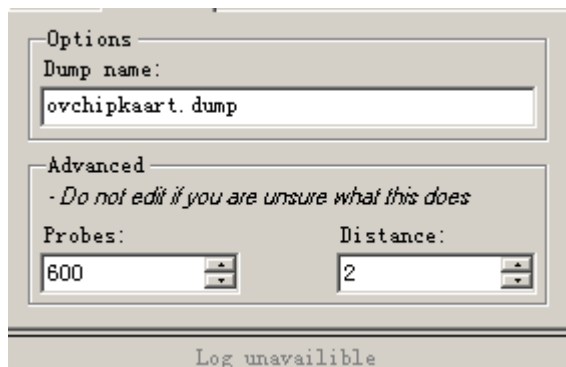
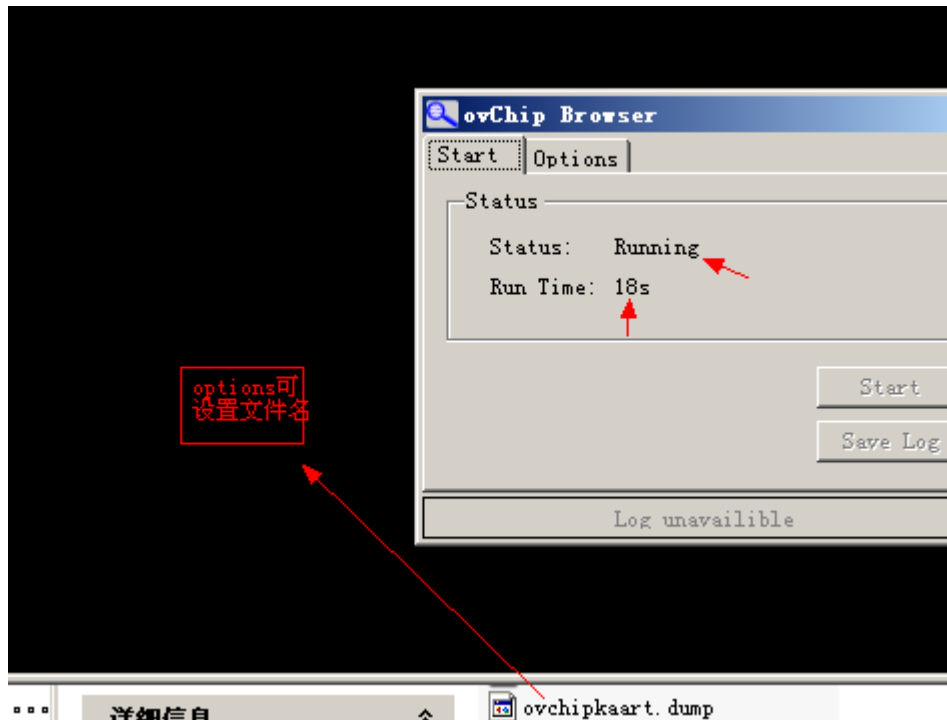
会生成一个这样的文件



用 C32 打开看。可以发现一些信息。。或者载入到其他工具里面，看扇区。如金额。时间。次数。等信息。。。

例外还有一款。

ovChip 也是一个非常不错的工具，不过依赖 nfc.dll 所以要 Copy 到 Nfc.dll 目录下哦。他和 mfocGUI 一样。一样会生成一个.Dump 的文件，意思和上面的解释一样。。如果还问，有了 mfocGUI 为什么还要用 ovchip，那么请参考本文档的第十行。。。



线程文件名等一些简单的设置。。

Over 之后，

EasyKey.exe—>可用 122u 里面的一个自带的程序试试密匙是否正确

Reader Connection
Serial
USB
PC/SC

READER NAME  
ACS ACR122 0

Current Login Parameters
Login Type: Key A
Sector (Decimal): 0
Stored No. (Decimal): 0
Key (Hexadecimal): FF FF FF FF FF FF
Manual Input
Volatile Memory

New Key A  
(Hexadecimal)  
FF FF FF FF FF FF

New Option Bits  
(Hexadecimal)  
FF 07 80 69

New Key B  
(Hexadecimal)  
FF FF FF FF FF FF

Data Block 0
Data Block 1
Data Block 2
Security Block

| Access condition for                     |         |           |                       | Application             |
|--|---------|-----------|-----------------------|-------------------------|
| Read                                     | Write   | Increment | Dec/Transfer, Restore |                         |
| <input checked="" type="radio"/> Key A/B | Key A/B | Key A/B   | Key A/B               | Transport configuration |
| <input type="radio"/> Key A/B            | Never   | Never     | Never                 | Read/Write Block        |
| <input type="radio"/> Key A/B            | Key B   | Never     | Never                 | Read/Write Block        |
| <input type="radio"/> Key A/B            | Key B   | Key B     | Key A/B               | Value Block             |
| <input type="radio"/> Key A/B            | Never   | Never     | Key A/B               | Value Block             |
| <input type="radio"/> Key B              | Key B   | Never     | Never                 | Read/Write Block        |
| <input type="radio"/> Key B              | Never   | Never     | Never                 | Read/Write Block        |
| <input type="radio"/> Never              | Never   | Never     | Never                 | Read/Write Block        |

Login to sector: 0 | Login Type: Key A
Keys: FF FF FF FF FF FF
Write Data to Block: 3
Data:
FF D6 00 03 10 FF FF FF FF FF FF 07 80 69 FF
FF FF FF FF FF

Format Sector 0
Clear Log
Analyze Option Bits
About
Close

我记得前辈还说过，个人认为这也是个方法，那卡去消费一次，和以前的对比，看数据哪里出现了变化。所以。。。你懂的。。。

对比修改完成之后，可以用 nfc-mfclassic.exe 导入。

读取：所谓的读取如同名字一般。读取里面的内容。

复制：也和名字一样。简简单单的复制。未曾对里面的数据进行修改和更新

写入：就和复制相反了，可进行修改，更新。以及作弊。。。

克隆：记录卡上某一样 xx 号进行模仿克隆仿照。

总结一下：以前了解过，差不多了就弄了几个设备玩玩。感觉兴趣来了，挺不错的。写此文章也是为了让大家对 **RFID** 多多了解一些。也是给一些想接触的朋友看的。所以一些“大牛”“不爱看，或者觉得水。那么就请 **Del...**告知：我也是新手，写的不好。希望大家多多”指点”

有待开发。请尽情期待。