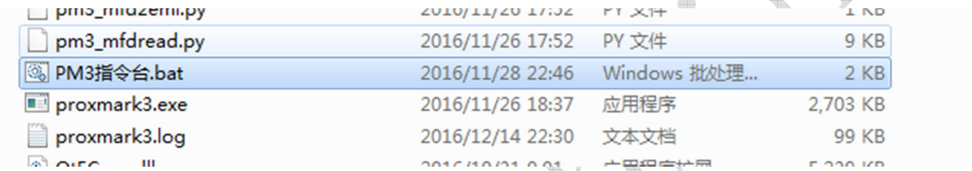
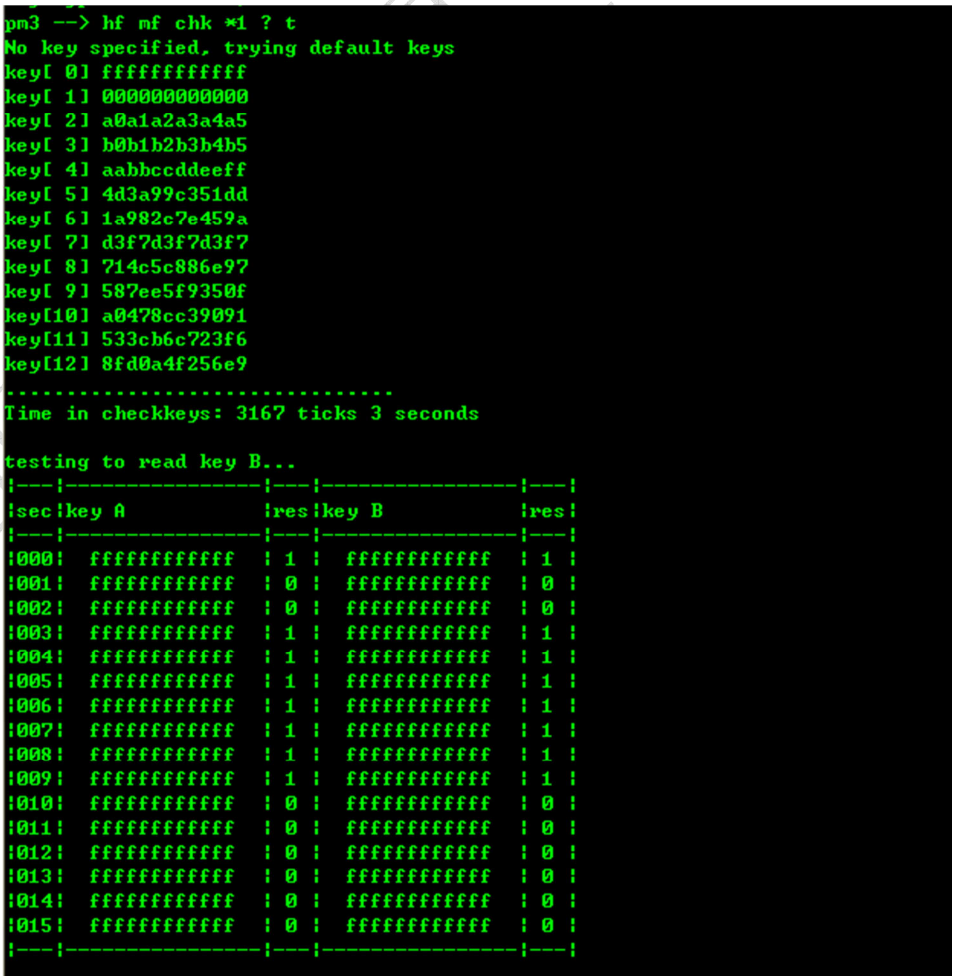
注意: Hardnested 指令针对的是扫描出默认密码，而解不出有密扇区的卡。对电脑配置要求较高，建议太老电脑就不要使用了。

1. 刷 iceman 固件

2. 进入 PM3 发布资料_DEC\官方软件固件\pm3-bin-iceman\client
打开



3. 扫描默认密码



4. 根据步骤 3，使用 hardnested 指令破解有密扇区

```
pm3 --> hf mf hardnested 0 A FFFFFFFFFFFF 4 A w
--target block no:  4, target key type:A, known target key: 0x000000000000 (not
set), file action: write, Slow: No, Tests: 0
Allocating memory for partial statelists...
Generating partial statelists...
Generating bitflip statelist...
```

解释：hf mf hardnested 0 A FFFFFFFFFFFF 4 A w

0：为默认密码的扇区块号，比如根据步骤 3，得知道 0 扇区是默认密码，那么 0 扇区 0 块肯定是这个密码，

A: 代表 0 块的 A 密码

FFFFFFFFFF： 为 0 块 A 密码

4：代表第四块区，即第 1 扇区，从步骤 3 的图可以看到第 1 扇区不是默认密码。如果要破解其他扇区的话，数字应该为设扇区号*4

A: 代表破解的是第四块区的 A 密码

5. 破解出密码

```
0 states...
.............Validating key search space
*
Time for bruteforce 9.2 seconds.

Found key: ffff93831077

Acquired a total of 12880 nonces in 136.9 seconds (5644 nonces/minute)

pm3 --> _
```

这个过程会根据卡的破解难易程度，耗费的时间不等，对计算机占用不较高，建议关闭其他的操作。

6. 记录每次破解的密码。有了密码就可以读出扇区内容。