本文只作技术研究之用，请勿用于非法用途，否则后果自负。

如今网络上能找到RFID安全类的信息非常的少，原因我就不说了，大家也明白。大家如果要研究RFID安全可以去[RadioWar](http://radiowar.org/" \o "" \t "_blank)或者[Freebuf](http://www.freebuf.com/" \o "" \t "_blank)多看看相关的文章，我在后面也会放出一些相关的资料供大家下载研究，资料大多数是外语资料，所以说外语一定要学好！

这次案例的主角是某学校可怜的水卡（热水卡），先小小地上镜一下先。

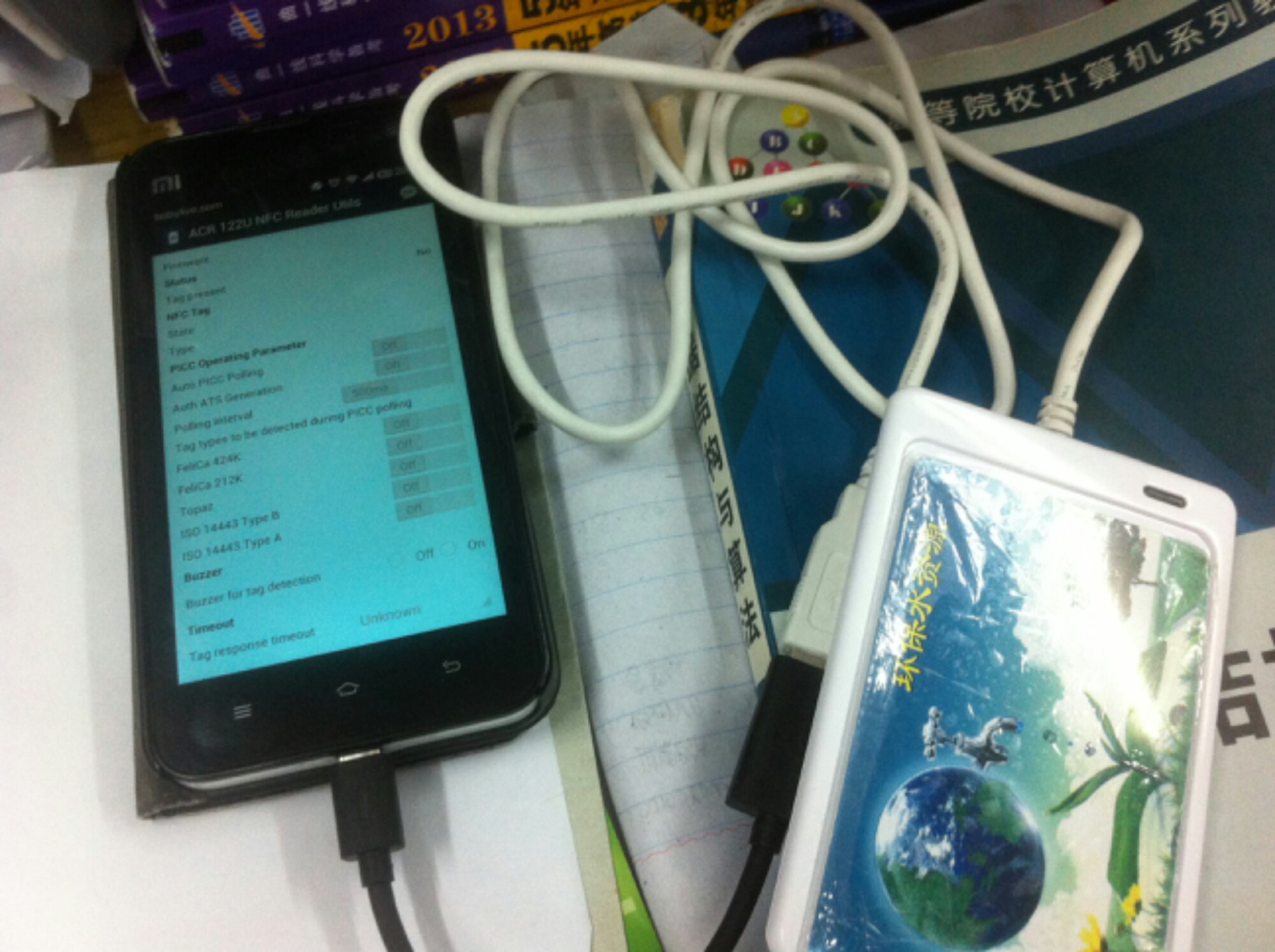
[](http://cdn.bobylive.com/wp-upload/wpid-IMG_20131122_195631.jpg)

[](http://cdn.bobylive.com/wp-upload/wpid-IMG_20131122_195646.png)

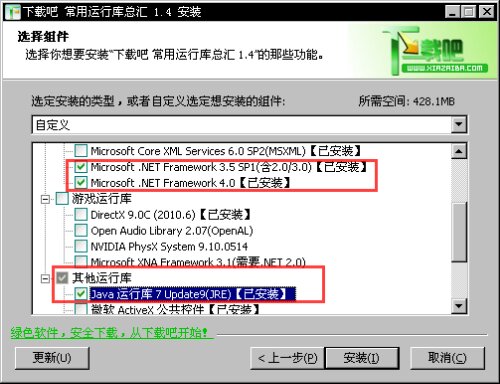
用NFC手机上安装的[MCT(Mifare Classic Tool)](http://pan.baidu.com/share/link?shareid=1802710180&uk=436466797" \o "" \t "_blank)查看，水卡的确是Mifare Classic 1k类型的。

[](http://cdn.bobylive.com/wp-upload/wpid-Screenshot_2013-11-22-20-10-46.png)

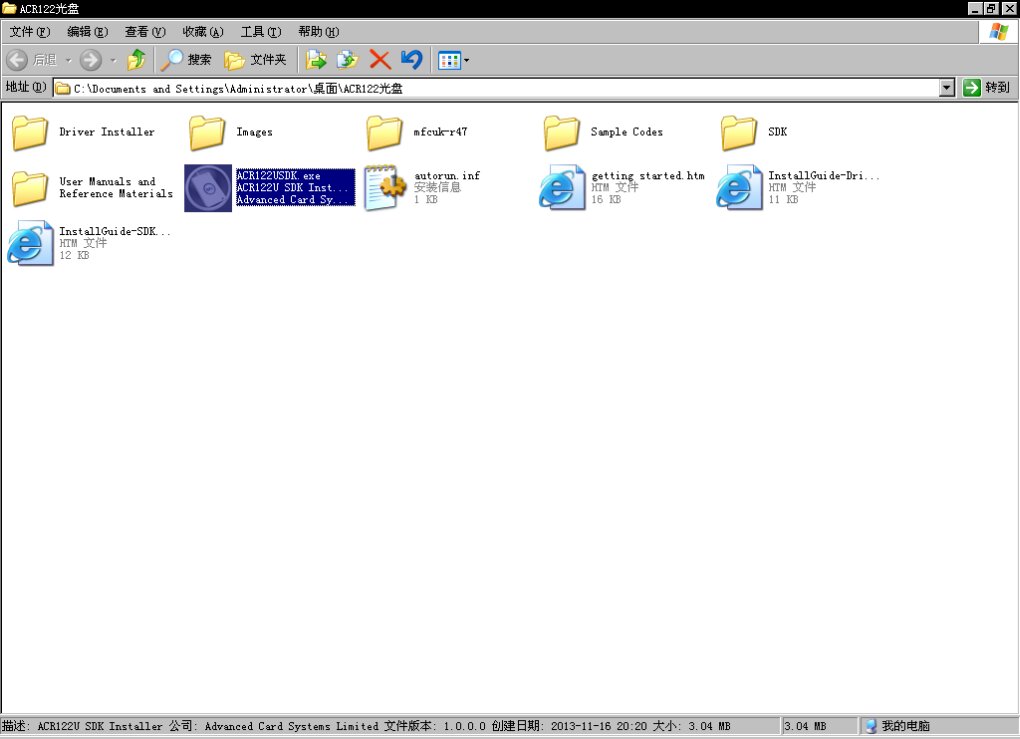
此次破解用到的工具有：电脑一台，ACR122U一台，带NFC功能的手机一台，水卡一张

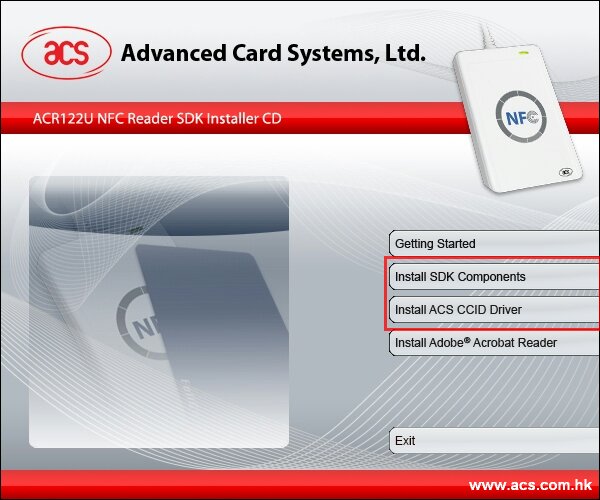
[](http://cdn.bobylive.com/wp-upload/wpid-rfid-2-hardware2.jpg)

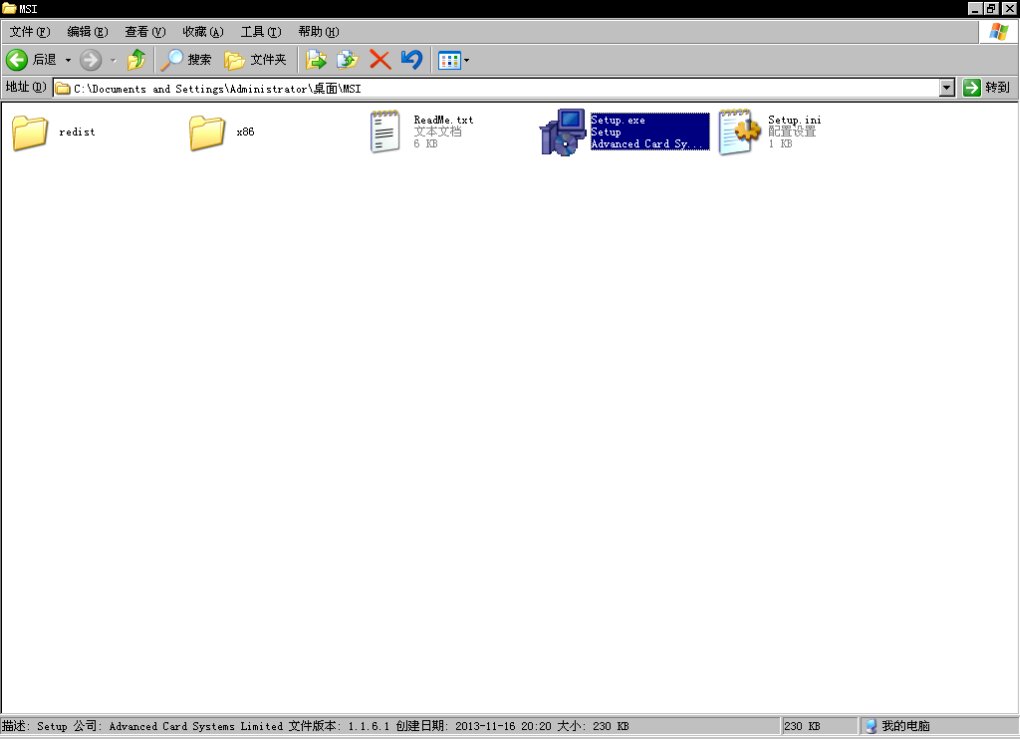
在进行破解工作之前，我们要为电脑搭建相应的环境，大家需要在电脑上安装.NET Farmwork 4以及Java，请自行上网下载安装，后面用到的软件依赖这两个运行库。

[](http://cdn.bobylive.com/wp-upload/wpid-rfid-2-1.png)

安装完运行库之后就需要安装ACR122U的驱动了（[驱动下载（百度云）](http://pan.baidu.com/share/link?shareid=3622525845&uk=436466797" \o "" \t "_blank) ，[SDK下载（百度云）](http://pan.baidu.com/share/link?shareid=3640062626&uk=436466797" \o "" \t "_blank) ），为了方便后续的开发，我将SDK也一并安装。

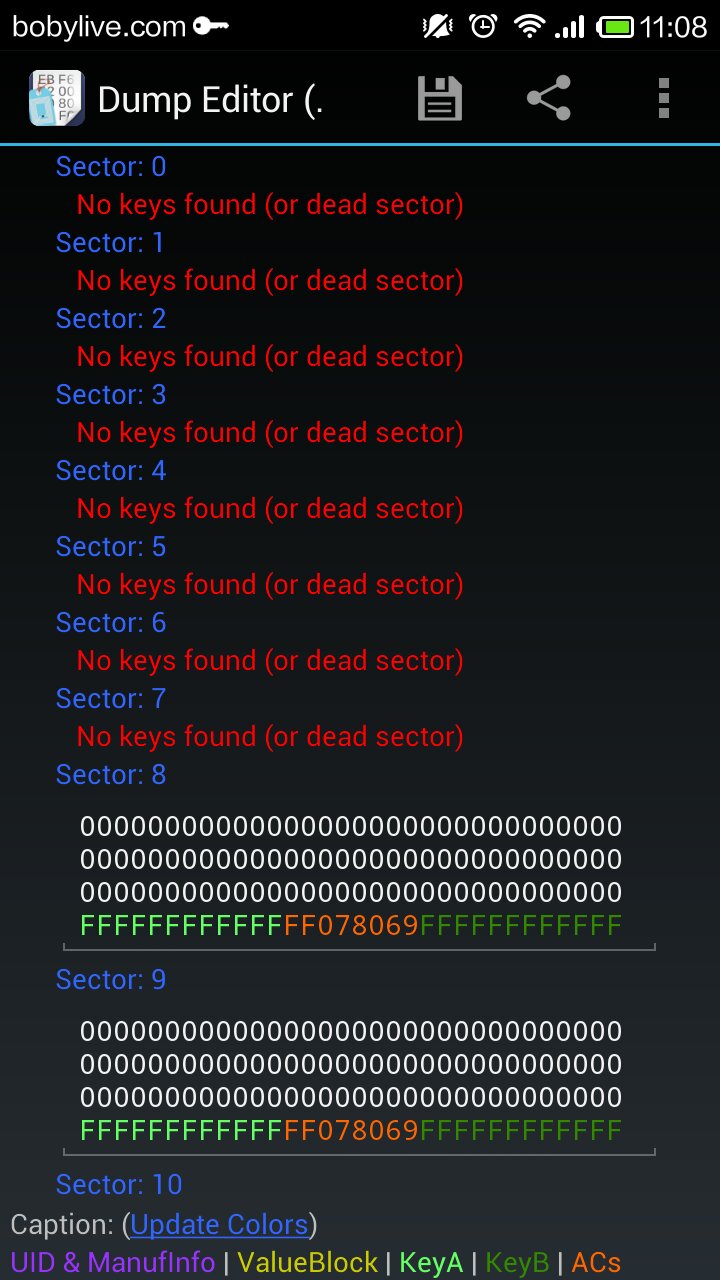
[](http://cdn.bobylive.com/wp-upload/wpid-rfid-2-3.png)

[](http://cdn.bobylive.com/wp-upload/wpid-rfid-2-4.png)

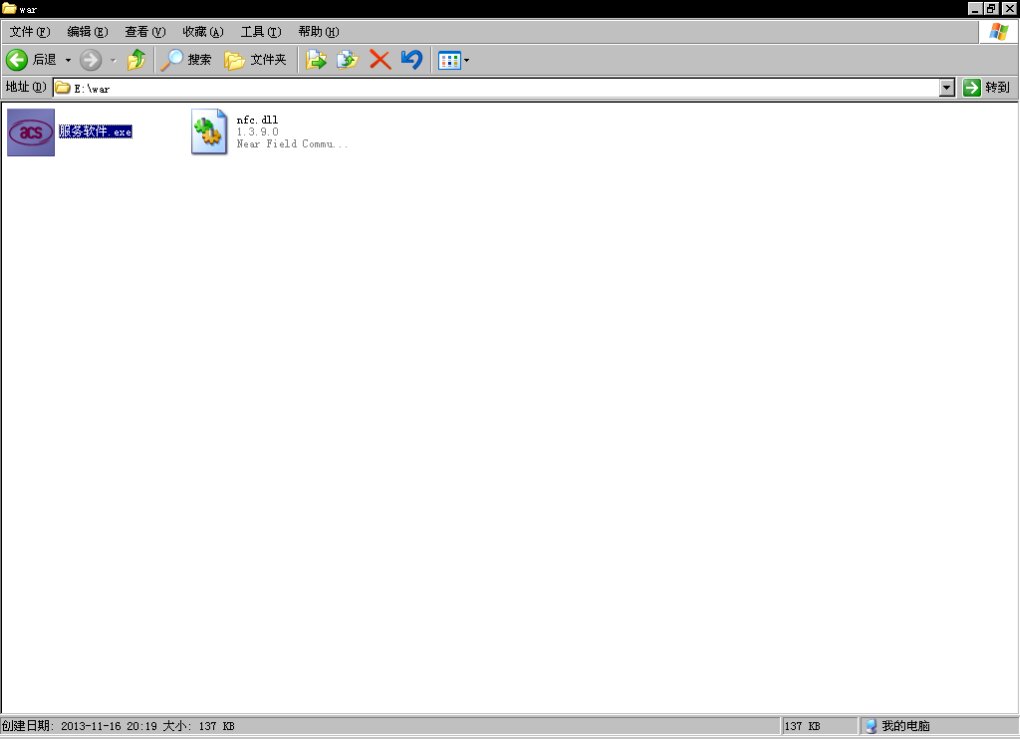
[](http://cdn.bobylive.com/wp-upload/wpid-rfid-2-2.png)

安装完驱动和SDK之后，把ACR122U连接电脑，设备就能正常工作了。把我们的水卡放上去，ACR122U的蜂鸣器就会响并且LED的颜色也会改变。

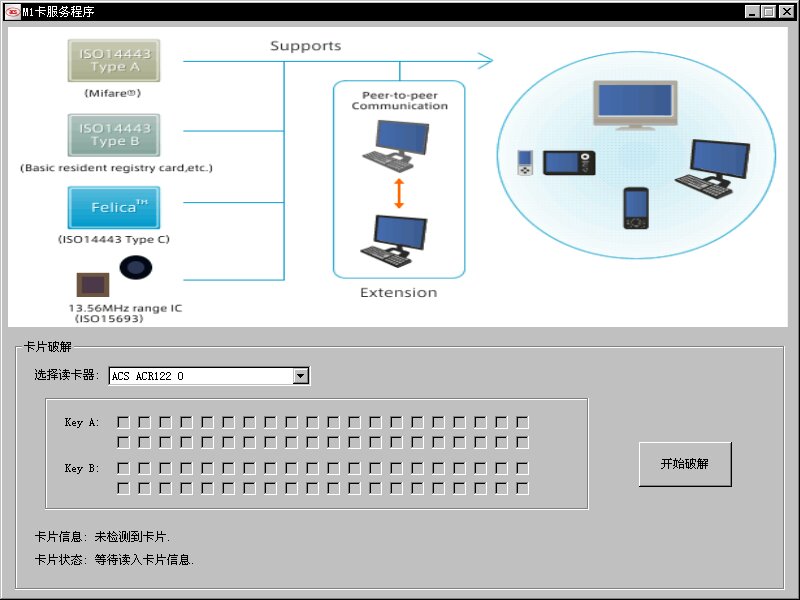
在此之前我已经尝试过用MCT自带的常见的密钥去访问水卡，发现有部分扇区使用的不是默认密钥，被加密了，对于这种不是所有扇区加密的卡，我们可以采用验证漏洞把其他扇区密码破解出来。

[](http://cdn.bobylive.com/wp-upload/wpid-Screenshot_2013-11-23-11-08-52.png)

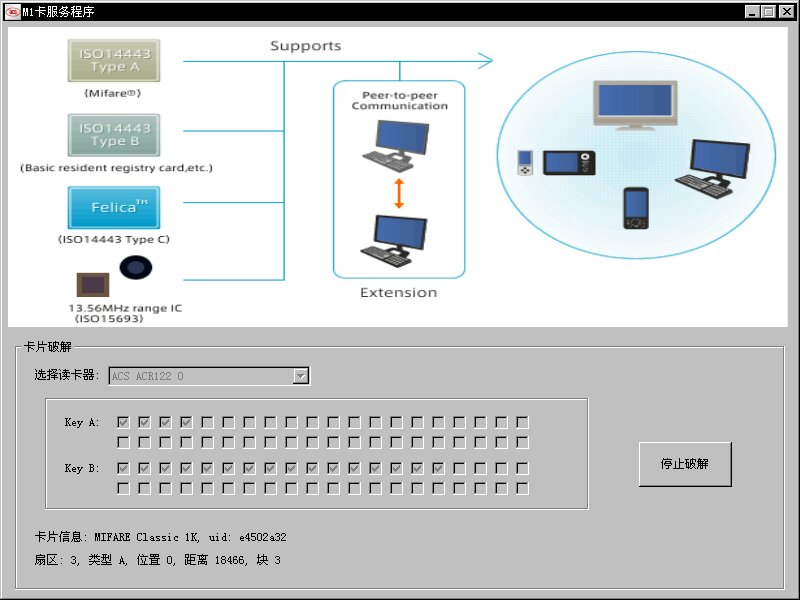
验证漏洞可利用的程序是mfoc，mfoc在Windows上的版本叫mfocgui，但mfocgui对于刚刚接触RFID安全的同学来说有点麻烦，所以这次直接采用[M1卡服务程序](http://file.bobylive.com/rfid/mfocgui_lite.zip" \o "" \t "_blank)（其实就是简化版的mfocgui）。

[](http://cdn.bobylive.com/wp-upload/wpid-rfid-2-5.png)

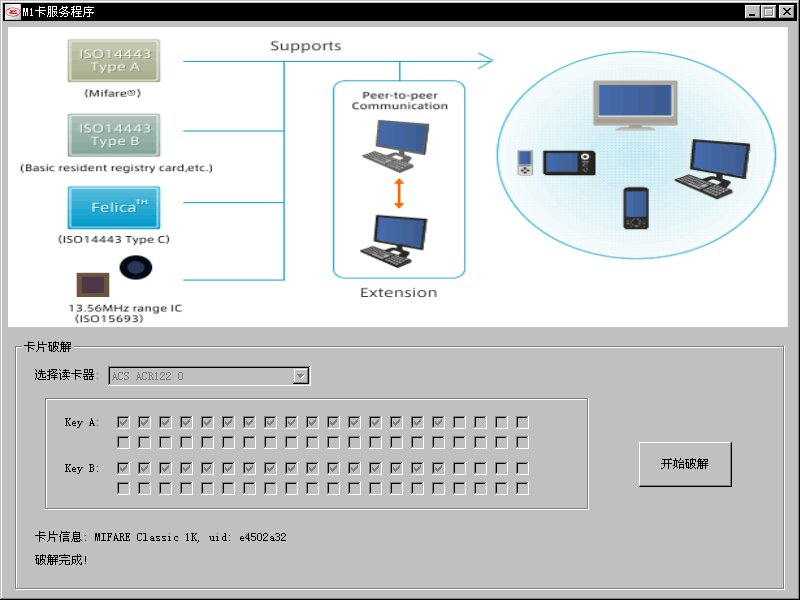
打开之后，程序界面非常简洁，只有一个按钮，就是开始破解。在读卡器列表那我已经见到我的ACR122U了，所以直接按开始破解就可以。

[](http://cdn.bobylive.com/wp-upload/wpid-rfid-2-6.png)

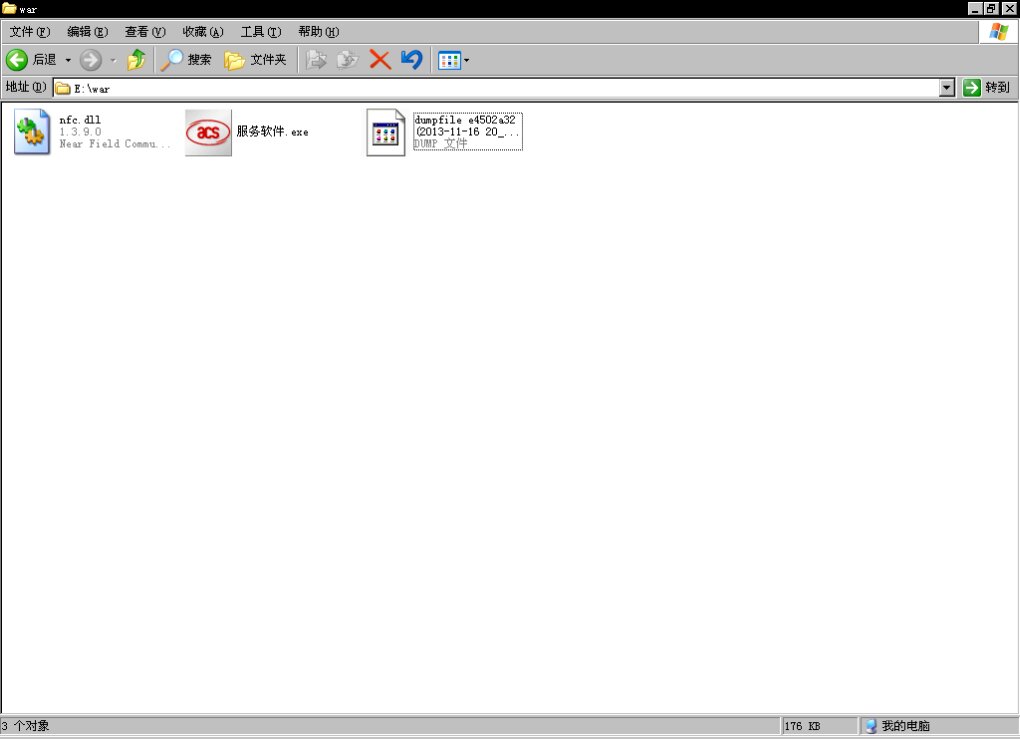
然后接下来就等待程序自己破解密钥。

[](http://cdn.bobylive.com/wp-upload/wpid-rfid-2-7.png)

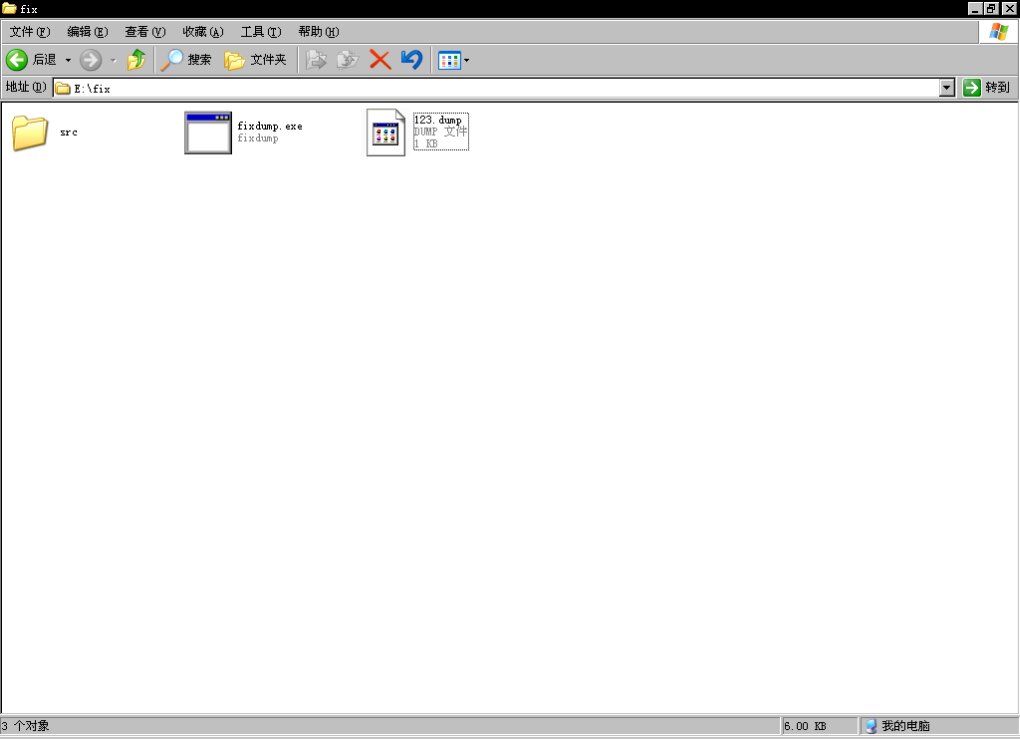
不用很久，就看到所有扇区都被打勾了，破解成功了。

[](http://cdn.bobylive.com/wp-upload/wpid-rfid-2-8.png)

破解成功后根目录就生成了这张卡的dump文件了，大小是1kb，整张卡就被读取出来了。

[](http://cdn.bobylive.com/wp-upload/wpid-rfid-2-9.png)

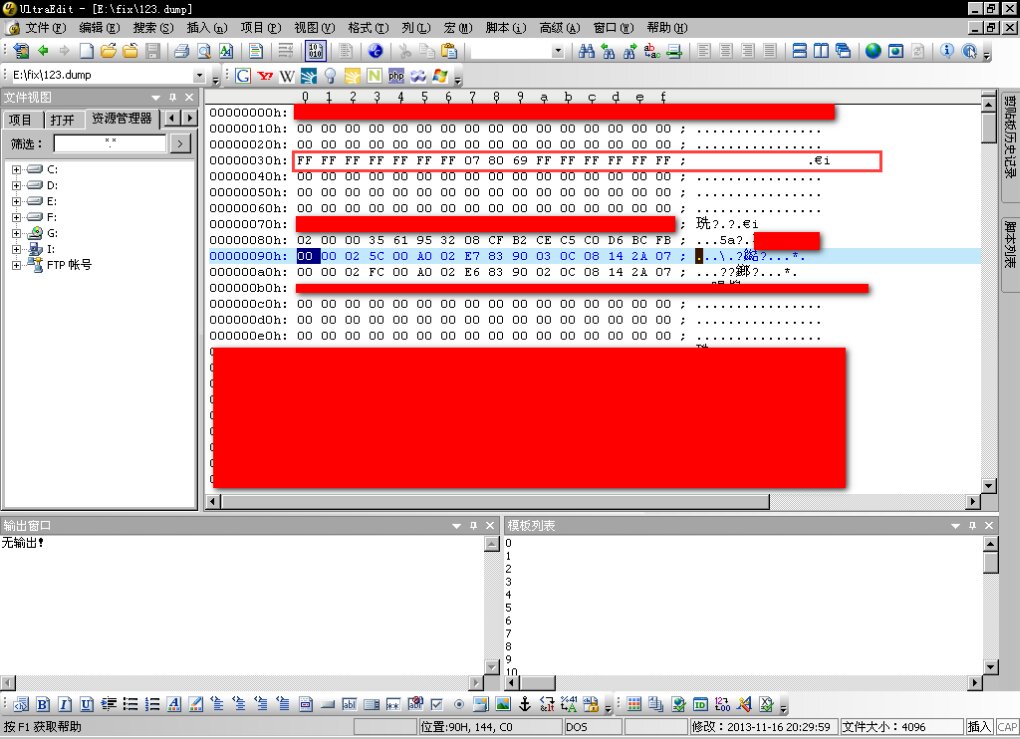
但mfoc原本是运行在Linux环境下的，移植到Windows下的mfocgui生成的dump文件是并不能直接使用的，还需要一个修复工具fixdump（[下载fixdump](http://file.bobylive.com/rfid/fixdump.zip)），将1kb的dump文件修复成4kb的dump文件才行。

[](http://cdn.bobylive.com/wp-upload/wpid-rfid-2-10.png)

fixdump是命令行操作，并且必须安装了.NET Farmwork 4运行库才可以使用，为了方便命令操作，我们将dump文件拷贝到fixdump的目录里，打开cmd进行修复。命令很简单，直接“fixdump ”就可以，生成的文件会直接覆盖源文件。

[](http://cdn.bobylive.com/wp-upload/wpid-rfid-2-11.png)

修复完成后，用[UltraEdit](http://pan.baidu.com/s/1kT7fcIN)或者[WinHex](http://pan.baidu.com/s/1kTFS9fD)之类的十六进制编辑器打开，就可以看到dump文件的数据了。

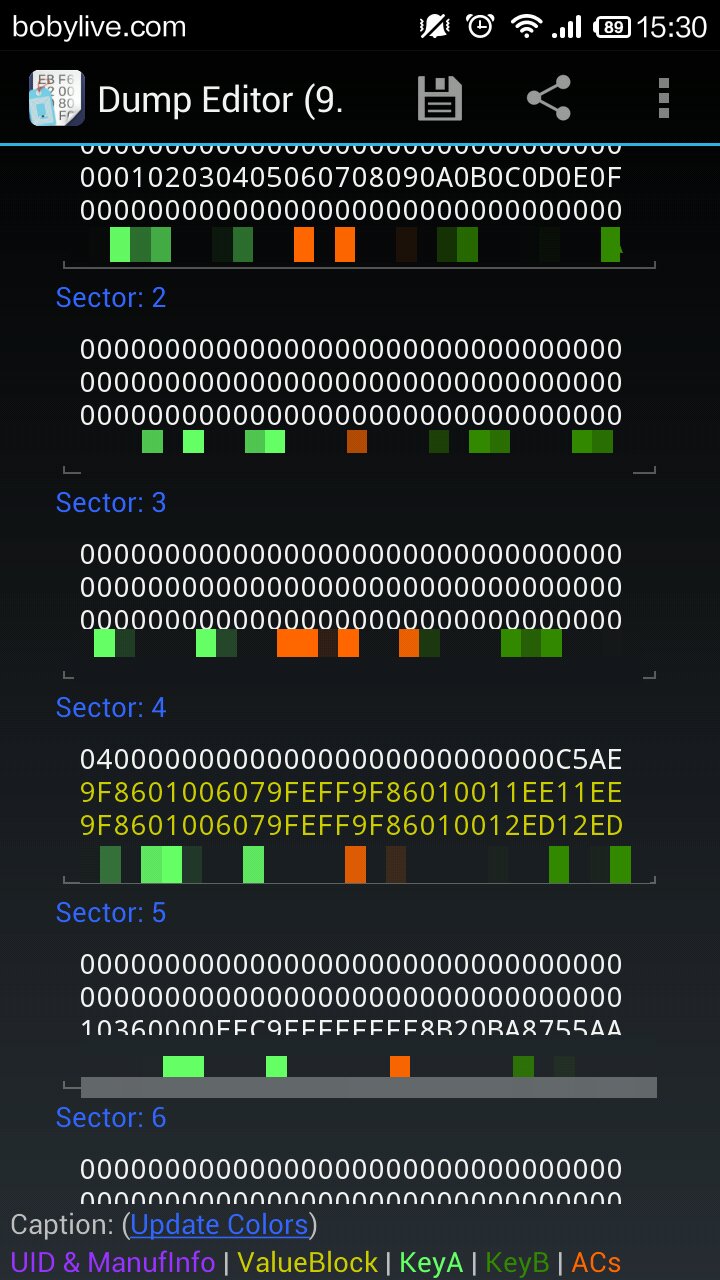
[](http://cdn.bobylive.com/wp-upload/wpid-rfid-2-12.png)

看到上图我用方框框着的数据了吗？这就是卡扇区的控制段，其中前6字节和后6字节的FFFFFFFFFFFF就是这个扇区的密码，中间的FF078069就是控制位，还不清楚M1卡的结构的可以去看看这篇介绍[M1卡结构](http://bobylive.com/static/1491)文章。

知道密码之后，我将密码导入MCT中，开始读取卡片的数据了。

[](http://cdn.bobylive.com/wp-upload/wpid-Screenshot_2013-11-23-15-13-42.png)

由于MCT自带数据高亮的功能，我们可以清楚的看到4扇区中有两行值块，我卡中现在的余额是32.31，我们根据值块的计算规矩进行计算，不清楚值块的还请去看看介绍[M1卡结构](http://bobylive.com/static/1491)的文章。值块的数值是两次不取反一次取反，并且保存在最低的地址里面的。看到第一个值块，9F0C，因为计算机数据是倒序存入的，所以就是真正的数据就是0C9F，换成十进制就是3231。中间那段的60F3是取反保存的，60F3倒序一次是F360，换成二进制就是1111001101100000， 取反一次就是0000110010011111，换成十进制就是3231。最后一段9F0C跟第一段一样，都是不取反保存，直接倒序一次转换即可。末端的11和EE就是地址，可以忽略不计，只要后面记得地址保持一致就可以。到此为止，卡的数据因为并没有采取任何加密导致被破解，现在我将卡的钱修改成999.99试试，999.99元应该是十进制99999，十六进制就是01869F，倒序一次结果就是9F8601 ，其他几位一样原理计算， 或者我们可以用MCT自带的值块计算工具计，最终算出结果如下图。

[](http://cdn.bobylive.com/wp-upload/wpid-Screenshot_2013-11-23-15-30-18.png)

将数据写入到卡里，现在就是去机器实践的时候了。

[](http://cdn.bobylive.com/wp-upload/wpid-IMG_20131123_161423.jpg)

破解大完满结束，总耗时5小时。

如果有什么问题欢迎留言或者邮件咨询和交流。

本条目发布于[2013/11/17](http://bobylive.com/static/1493)。属于[RFID](http://bobylive.com/static/category/technology-research/geek/rfid)、[极客](http://bobylive.com/static/category/technology-research/geek)分类，被贴了 [ACR122U](http://bobylive.com/static/tag/acr122u)、[IC卡](http://bobylive.com/static/tag/icka)、[M1](http://bobylive.com/static/tag/m1)、[Mifare](http://bobylive.com/static/tag/mifare)、[RFID](http://bobylive.com/static/tag/rfid)、[S50](http://bobylive.com/static/tag/s50)、[极客](http://bobylive.com/static/tag/geek)、[水卡](http://bobylive.com/static/tag/shui-ka)、[热水卡](http://bobylive.com/static/tag/re-shui-ka)、[破解](http://bobylive.com/static/tag/po-jie)、[黑客](http://bobylive.com/static/tag/hei-ke) 标签。