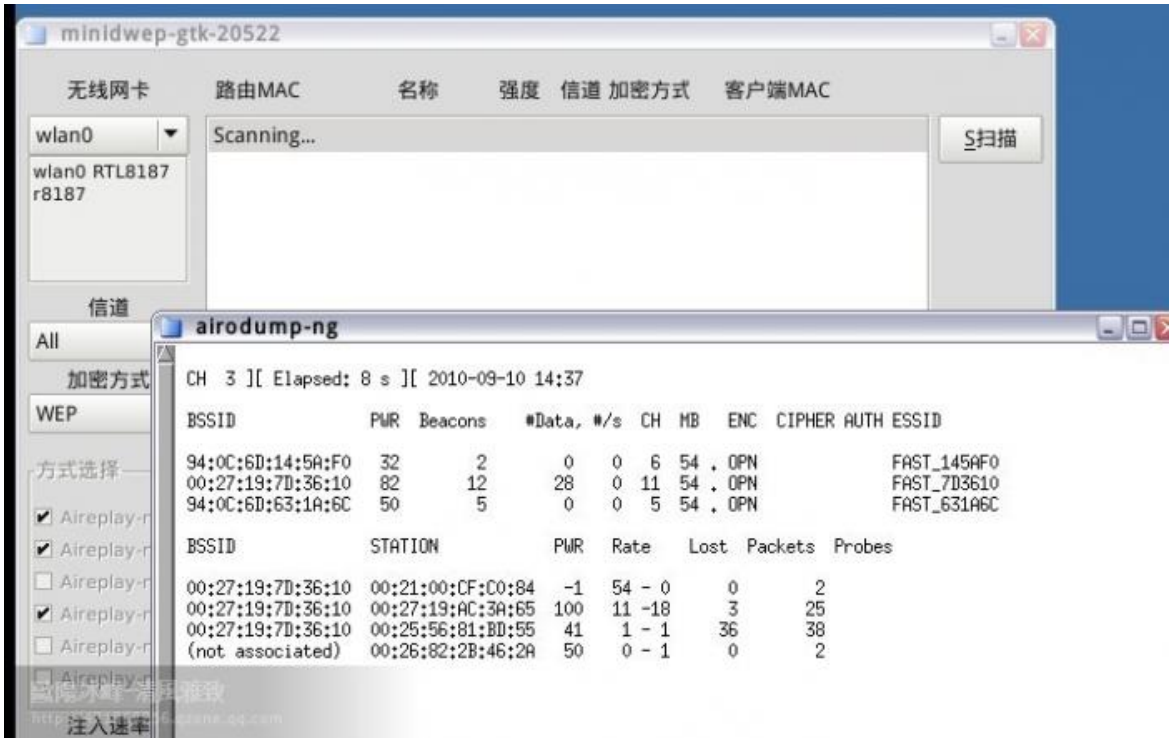
无线宝 bt5 来破解 wpa wpa2 加密

此教程为使用 无线宝**bt5 来破解wpa加密、wpa2 加密**，请勿使用在非法途径，其主要目的供测试您自己家无线路由是否安全。请自行参考内部教程打开bt5 程序。

1、系统启动啦，这就是桌面！咋样？熟悉吧？很像win的！很容易上手
2、然后打开第二排的第一个软件minidwep-gtk~~出现此对话框，直接点ok！就过去了

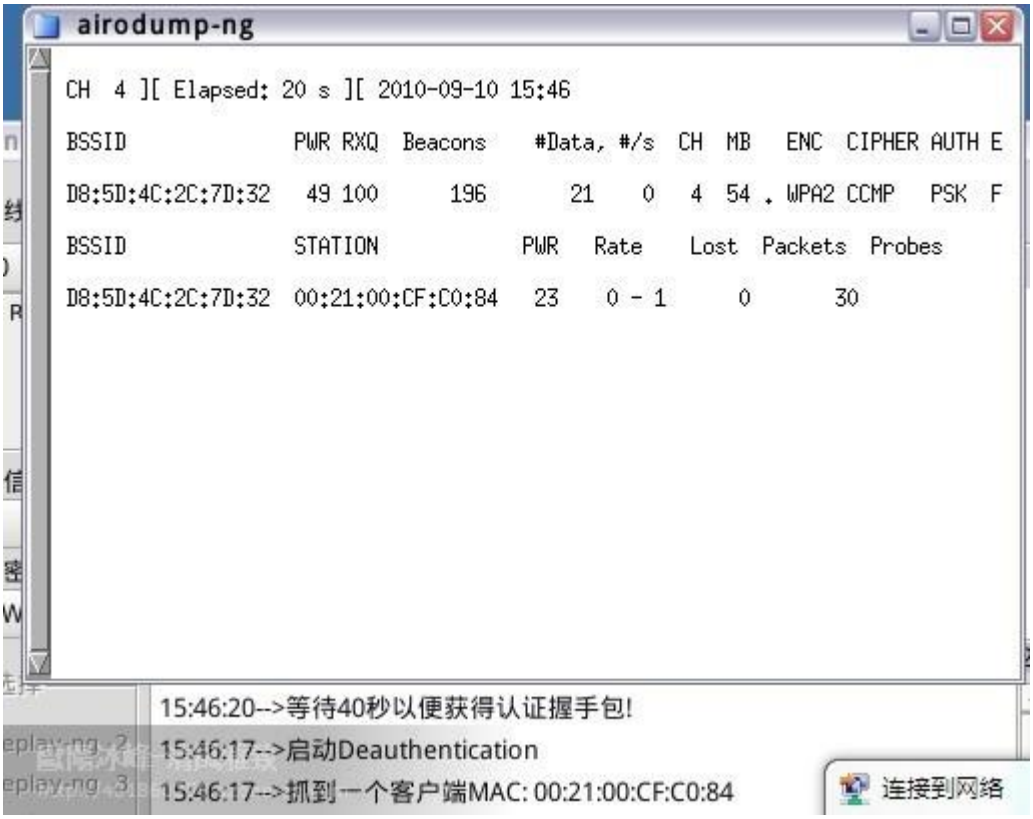
3、看左上角那个下拉菜单，找到自己的网卡！！！然后右上角！！扫描！！！然后就开始激动人心了！~



4、够激动吧？看到没有？

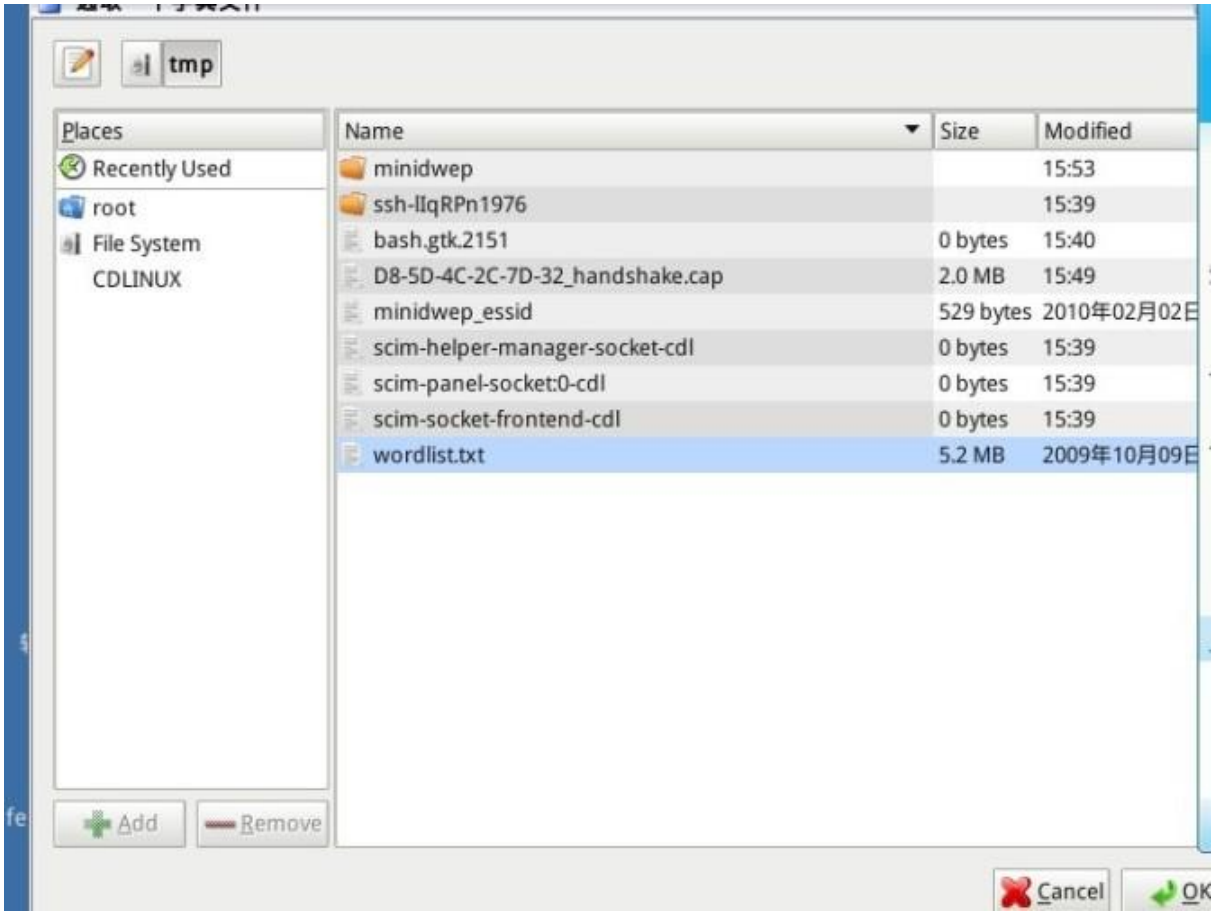
sssid--- 就是扫描到无线接入点的mac地址 pwr：信号强度 data：这句是所谓的数据包 最后面的essid就知道了吧？那就是你扫描到的路由名称！这样就明白了吧？当然了，如果没有数据包的话，你还是省省吧！毕竟是破解！没有数据包代表抓不 到握手包，抓不到握手包怎样破解呢？所以还是需要数据量的！然后抓到握手包以后就开始破解啦！

5、 怎么样？嘿嘿，看到了吧？软件已经搜索到了wpa2 加密的方式的路由器！当然了，软件的搜索方式是一起搜索，也就是wep，wpa2 一起搜索，看看软件左 边栏的“加密方式”你选择wep就会显示wep方式加密的路由，你选择wpa2 就会显示wpa2 方式加密的路由，咱们这儿讲的是破解wpa2 加密方式的路 由！所以wep一笔带过！如果是破解wep的路由，直接右边栏的“启动”按钮，剩下的几乎不用动手自动搜索密码（前提是有数据包哦！）



6、接下来开始抓取握手包，看图片最后面一行字，抓到一个握手包，正在等待认证，等待认证后就会给你提示！告诉你已经抓到一个握手包，然后就可以破解啦!（当然，抓取握手包是需要耐心的，有时候rp暴增，没准上来就能抓到，我这儿抓了十几分钟才抓到）

7、基本上已经成功，剩下的就是破解啦！这里开始进入破解第一部，跑包，开始测试密码！



8、接下来，把你的字典贡献给minidwep-gtk！嘿嘿，这个都会了吧？我给他一个默认的字典，就是最后一个wordlist.txt。你可以根据情况来选择字典，其实我上藏了 3g多的字典呢！嘿嘿，不过这个路由是弱口令的！所以这个字典足够了！

9、这下子就解密啦，成功啦！！！嘿嘿，哈哈！！！看见wpakey：0123456789 这就是密码！这个密码牛屄吧？够弱智吧？！哈哈哈

10、昨天写的仓促，忘了告诉的大家，虚拟机运行cd是不支持内置网卡的，所以需要设置一下的！很简单，我就不上图了！打开vm以后，看上面菜单栏里面有个“虚拟机”然后下来看到“可移动设备”，然后看到你的usb网卡，然后打上对勾就ok了！简单吧！嘿嘿

嘿嘿，同志们别拍砖，别骂！破解wpa不是开玩笑！关键是你的机器是否够强悍！字典是不是够多！！！
如 果你的机器够强悍，跑包跑到几十万的话！字典收藏几百G，估计你不能破解的密码不多了！有很多“大侠”告诉我说破解不了，说我骗人的！后来问人家，你字典多大？人家说了，我字典超牛逼！！！有 3m的txt文件作字典！！！！同志们啊！！！这样的“大侠啊”您觉得他能破解吗？

本次教程所使用软件下载地址：

VMware6.0.rar(本教程所用软件)http://u.115.com/file/f758c8914b

VMware7.0：http://bbs.yowao.com/read.php?tid=26

EWSA.rar：http://u.115.com/file/f37ce4a120#Download

cdlinux_-0.9.6.1_ISO无线破解系统.iso 传说中的奶瓶：
http://u.115.com/file/f3651329a9#Download

Beini-1.2.1 集成 500W密码增强版.iso 附上我收藏的字典：压缩后 80 多mb，解压缩后 3g空间！
http://u.115.com/file/f7d8f179da

wpa2 破解字典（解压后 3g文件）：http://u.115.com/file/f3d90f8b9f

all_birth(vip).rar：http://u.115.com/file/f3168451ef

Beini-1.1_中的新字典.rar
http://u.115.com/file/f33b6b3771

http://u.115.com/file/f760ed169e
14365003.rar

http://u.115.com/file/f742663269
142183.rar

http://u.115.com/file/f7bc03925f
133127.rar

http://u.115.com/file/f7533611f
0-9.8 位纯数密码.rar

http://u.115.com/file/f7d077303a
3+sr.rar

http://u.115.com/file/f76a7b09c8
生日 1980-2010 年.rar

http://u.115.com/file/f74d658ab6
弱口令集.rar

http://u.115.com/file/f7cd77abab
超级字典.rar

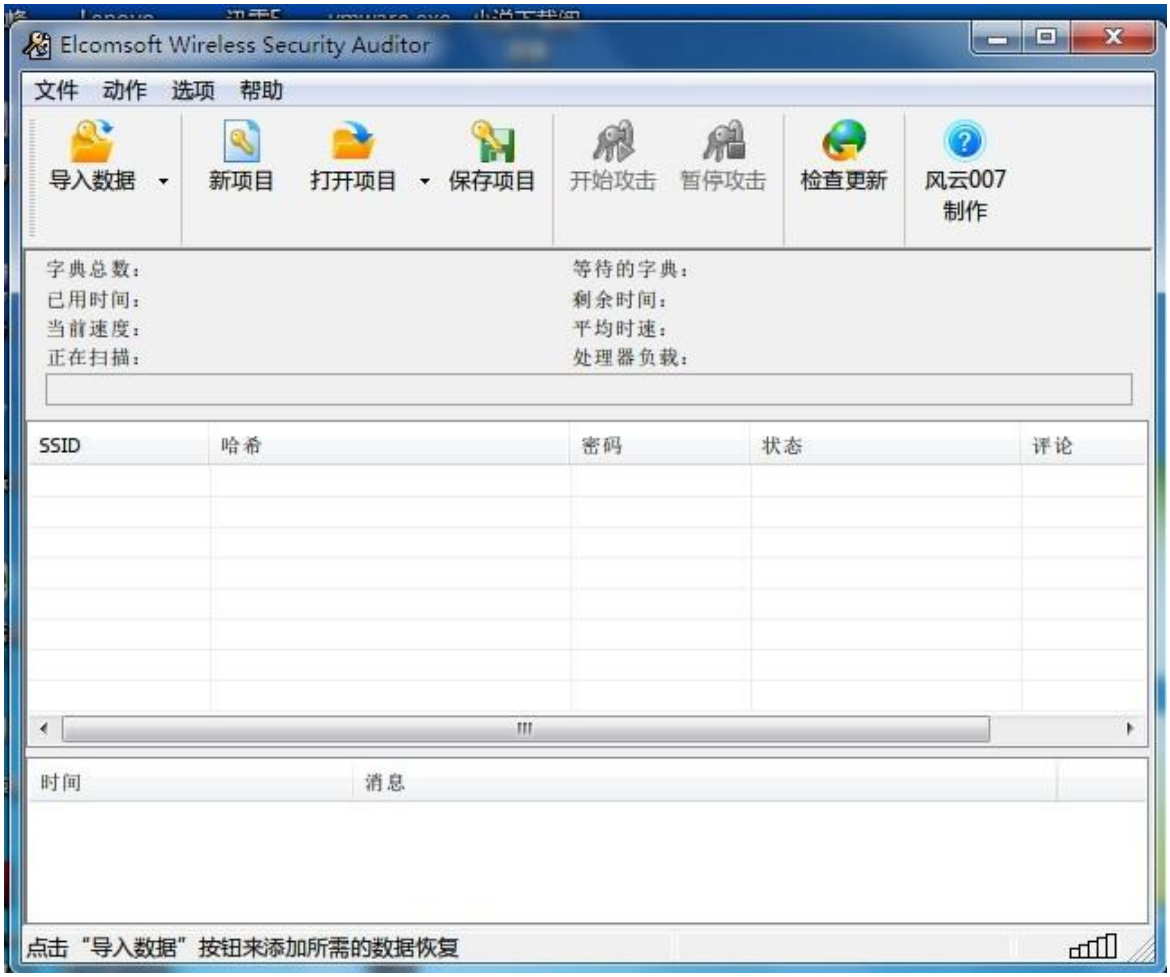
http://u.115.com/file/f7e9e85619
WPA英文字典.rar

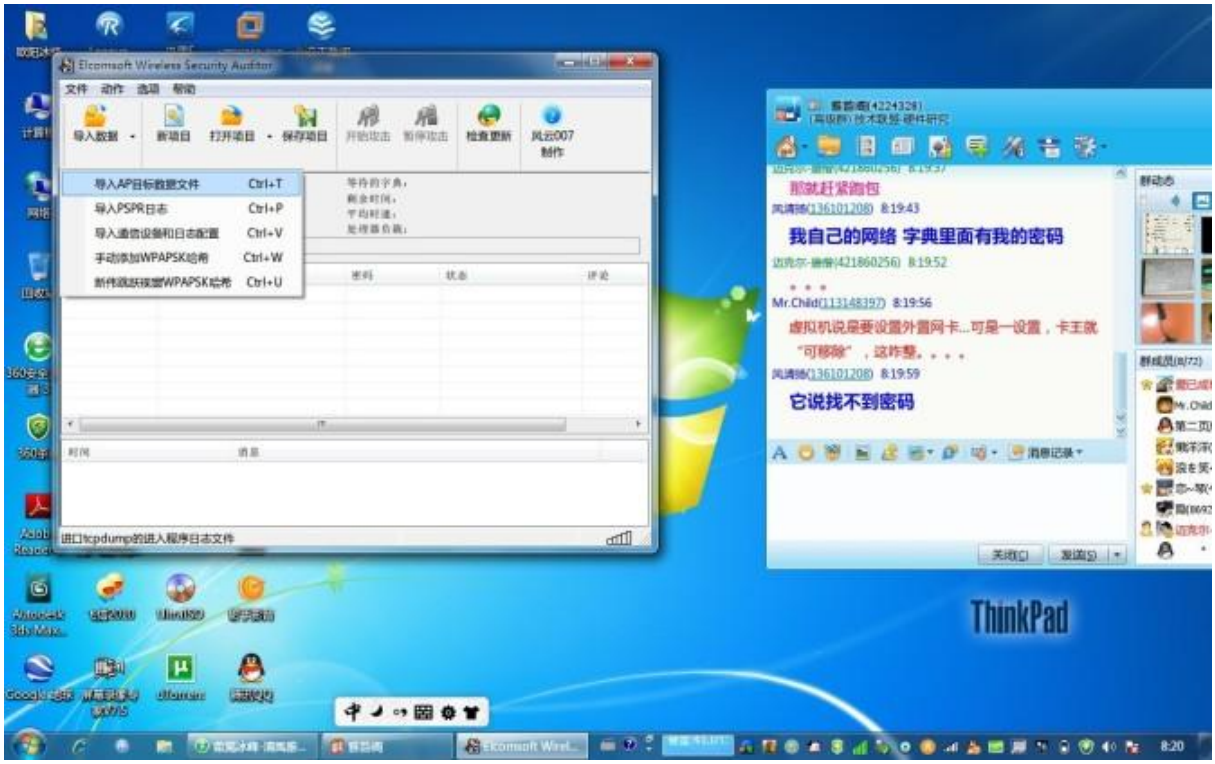
http://u.115.com/file/f720ee3656
wordlist.rar

http://u.115.com/file/f7a42521bf
10 位数字.rar

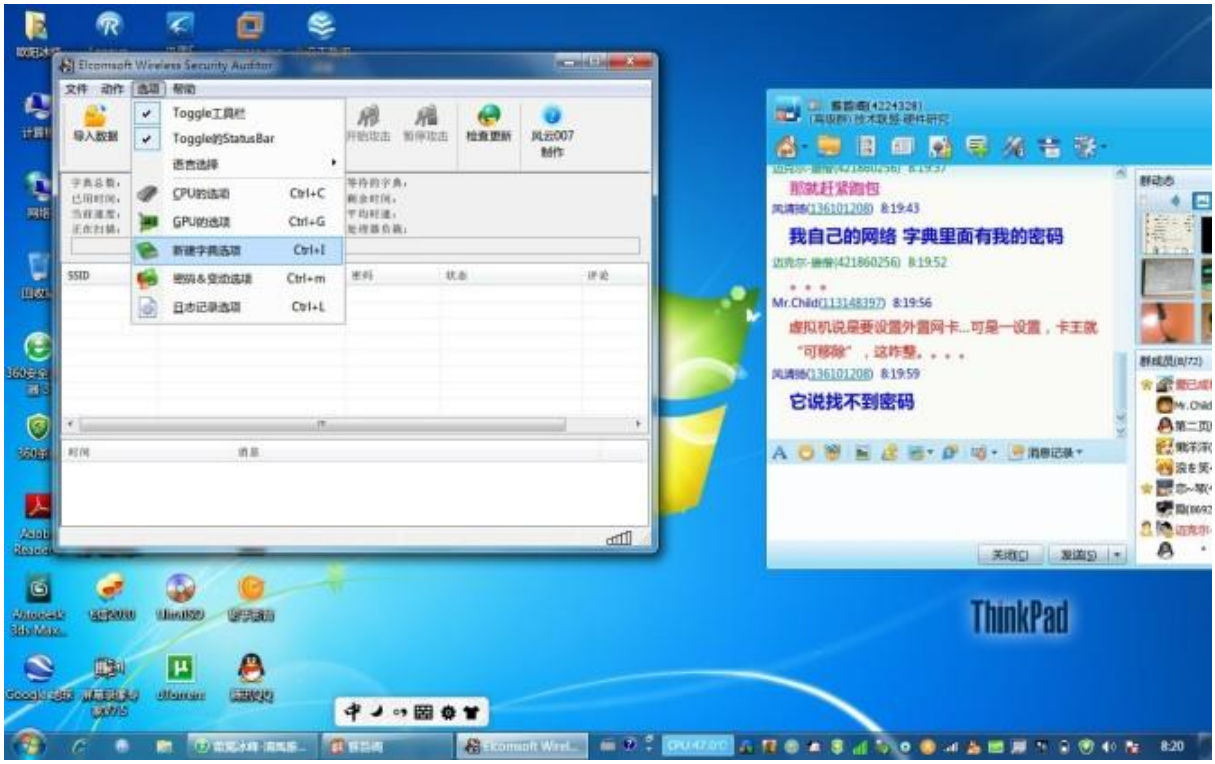
关于破解字典

其实破解是最简单却也是最复杂的，简单的是只需要几个步骤设置好以后就可以暴力破解，复杂的是需要极好的耐心与运气才能破解成功，机器配置越高，字典越 多，你跑包的速度就越快，你破解的几率就越高，所以不要问我多久能破解一个wpa2，我是回答不了的，因为破解有很多因素的吗！下面开始告诉大家如何在 win下跑包！
首先需要准备的软件：EWSA（老规矩，懒得下载的后面留言，我发送）字典若干
首先打开EWSA

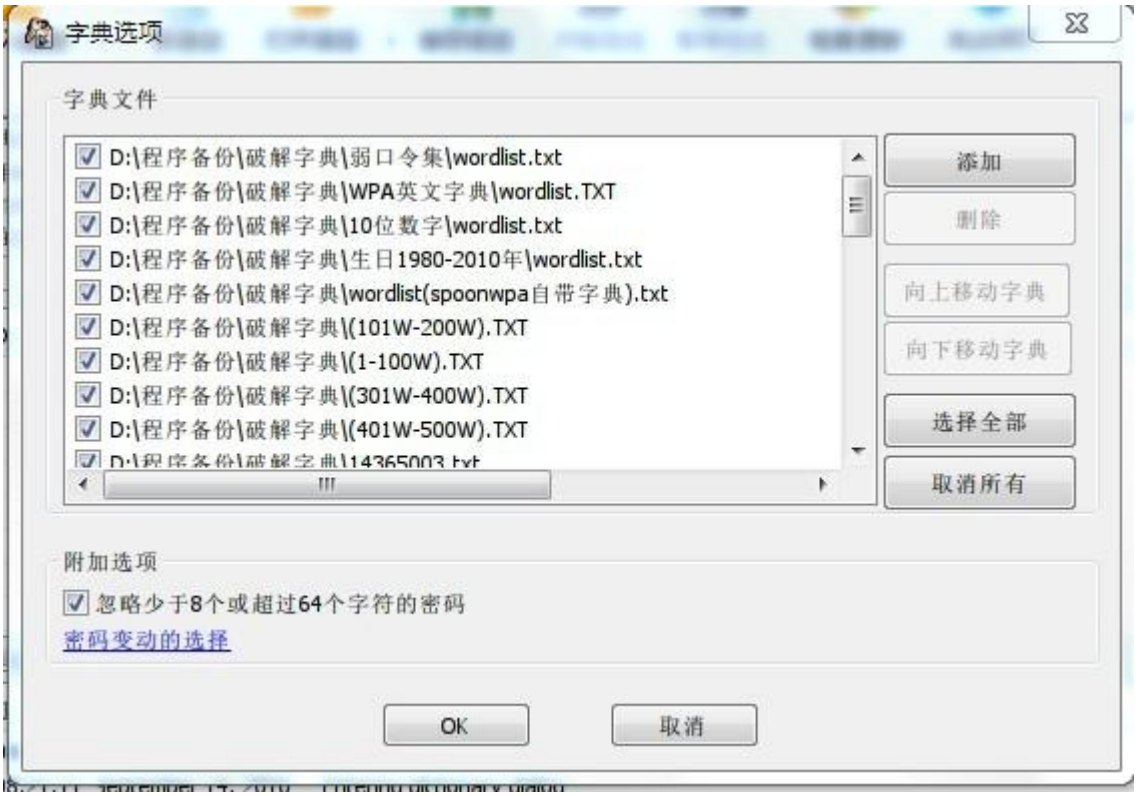




然后导入你抓到的握手包



然后新建字典选项



然后添加你字典所在路径
然后ok就可以开始攻击握手包进行破解了

当然，除了**无线宝bt5 来破解wpa加密、wpa2 加密** 您还可能感兴趣的是： 无线宝可以蹭哪些网？ - 全向天线和定向雷达的区别