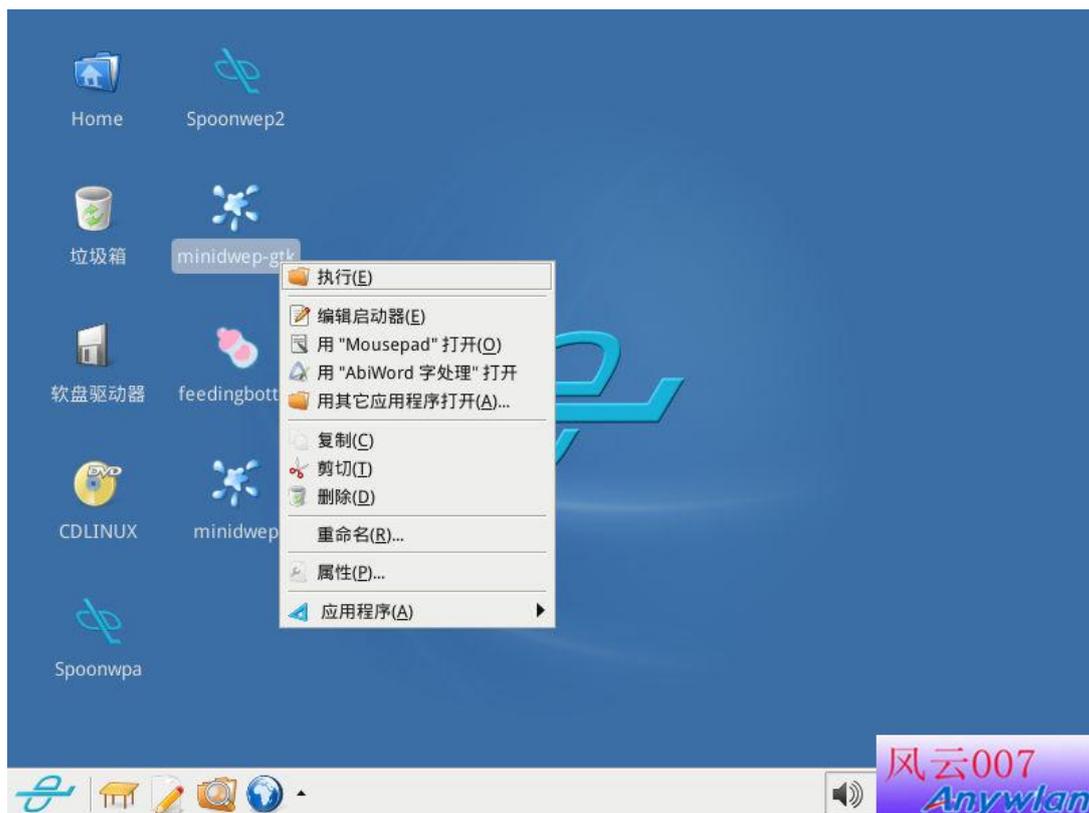


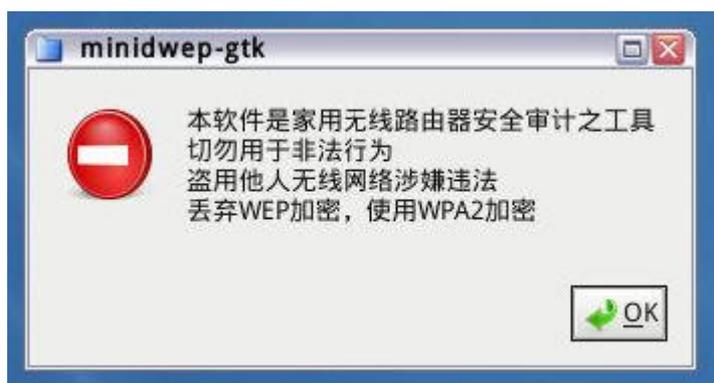
minidwep-gtk 破 WPA 全攻略

- 1、CDlinux 下使用 minidwep-gtk 获取握手包并使用自带的字典破解
- 2、自带的字典破解不出密码时使用 U 盘外挂字典继续暴力破解密码
- 3、将握手包拷贝到 Windows 系统下使用 ewsa 工具高速破解密码
- 4、破解 WPA 加密“握手包”字典的制作

一、CDlinux 下使用 minidwep-gtk 获取握手包并使用自带的字典破解
插好网卡，在 minidwep-gtk 上面点鼠标右键选择执行。



跳出警告的对话框点 OK 就可以了。



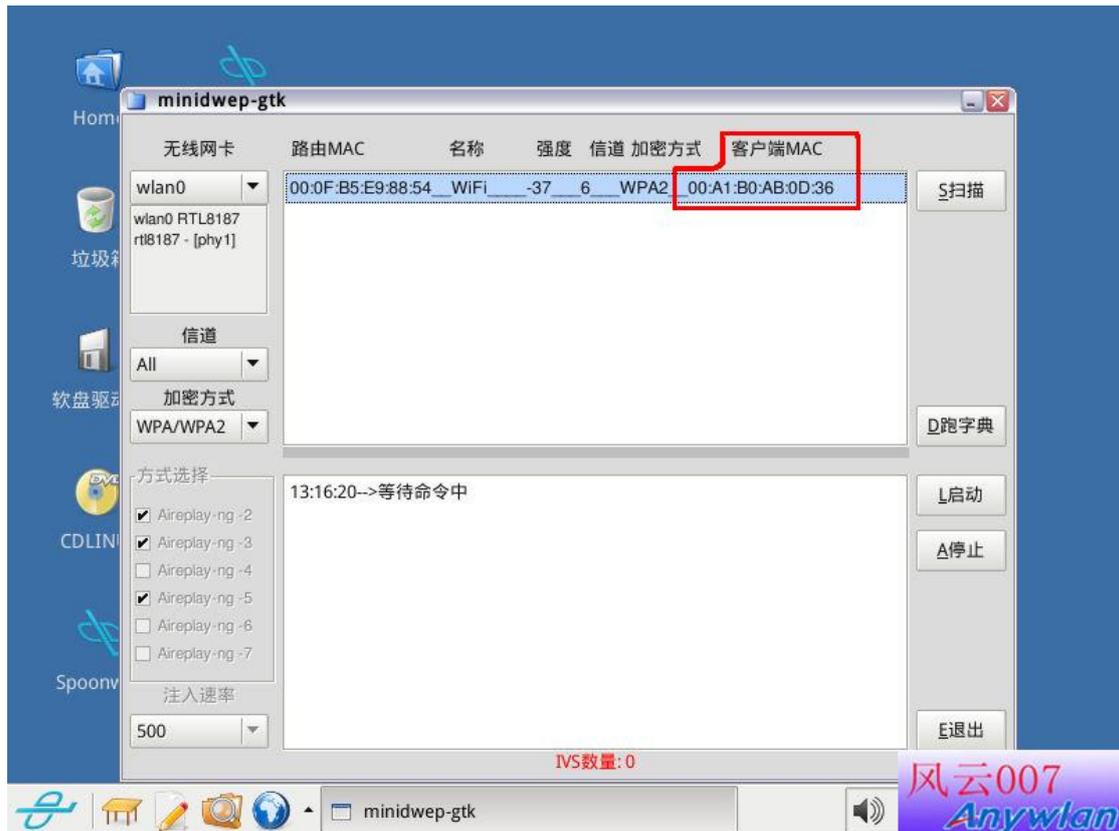
点 OK 后出现设置的窗口



把加密方式修改为“WPA/WPA2”，然后点“扫描”。

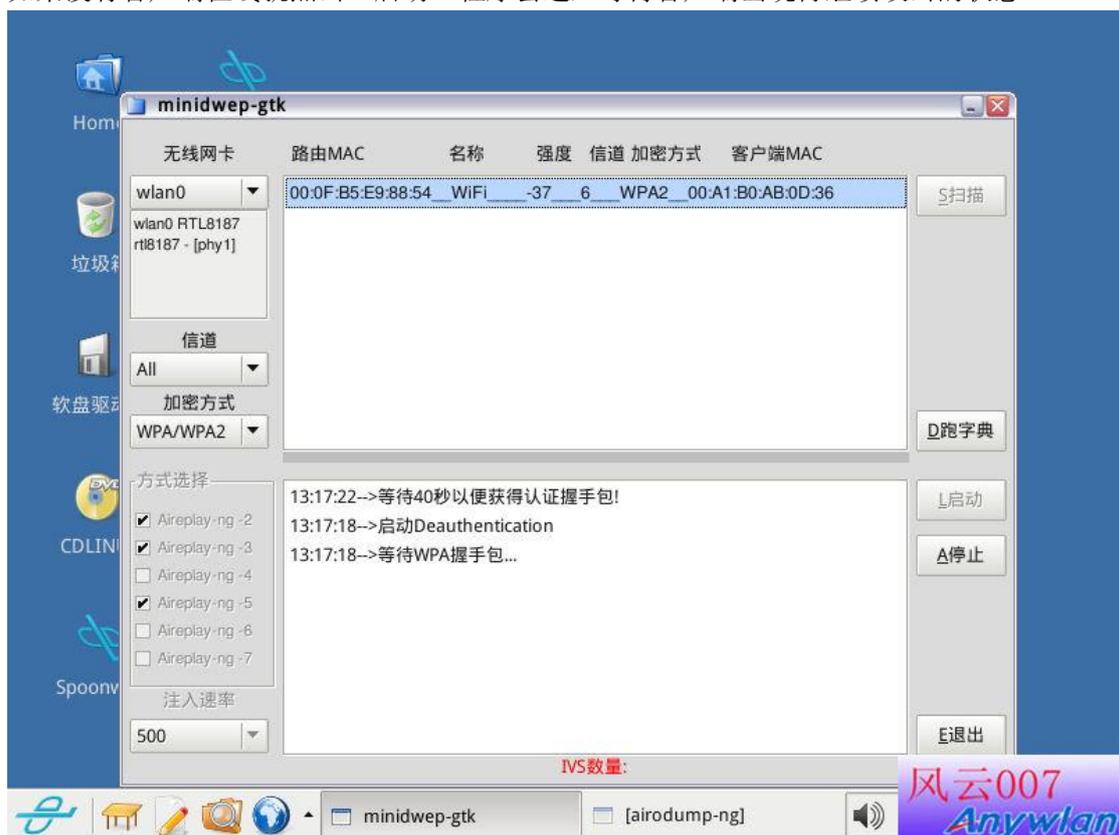


扫描到一个 WPA2 的信号并且有一个无线客户端在线。

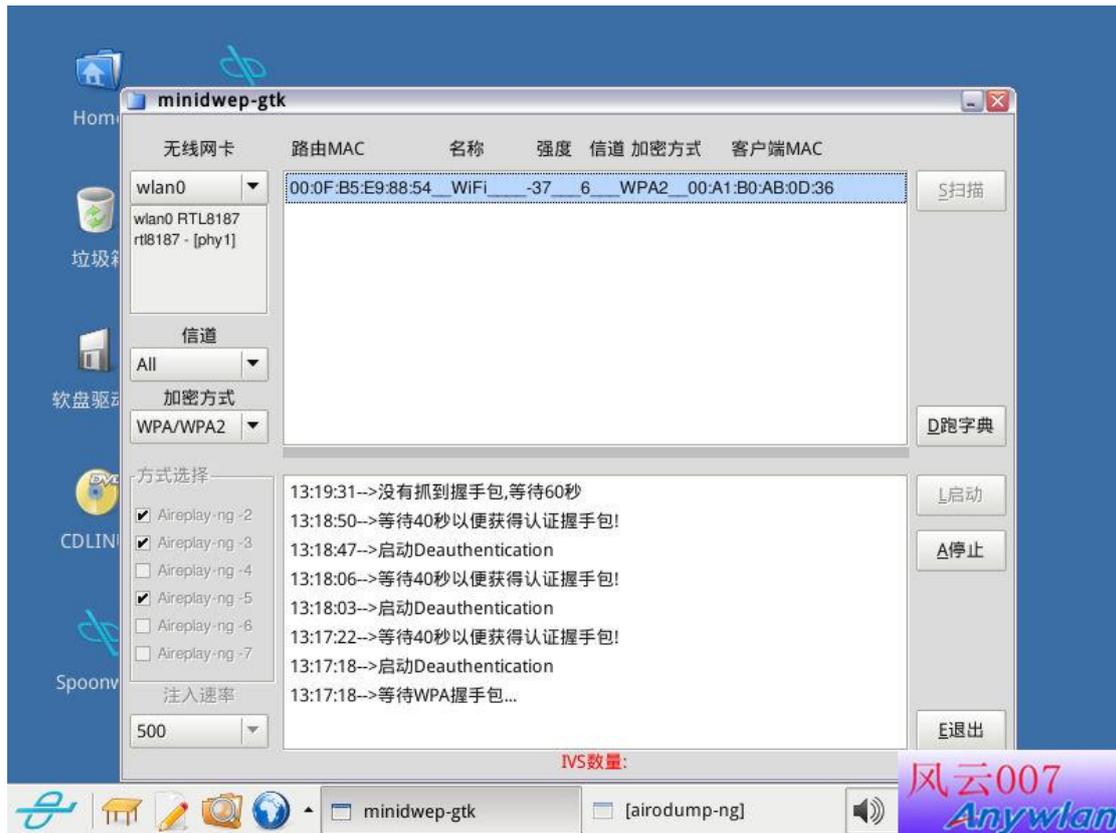


点击“启动”开始攻击无线客户端.....

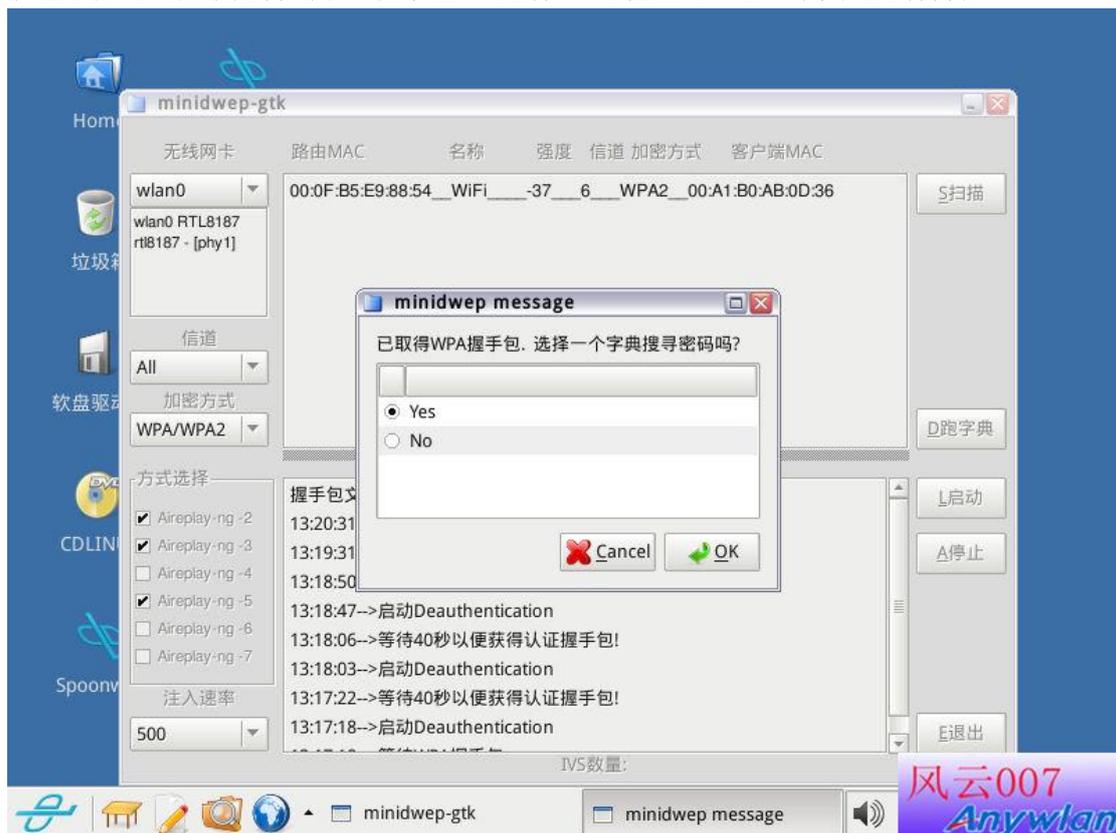
如果没有客户端在线就点击“启动”程序会进入等待客户端出现再继续攻击的状态。



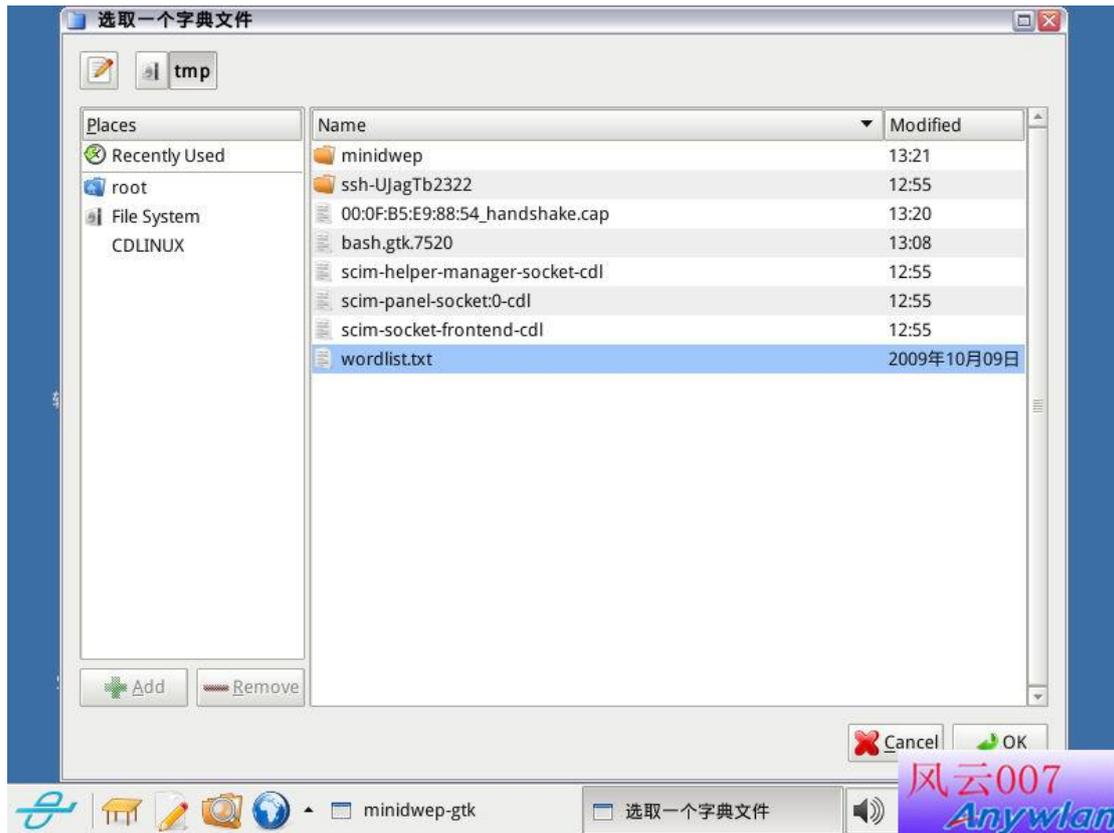
攻击中.....



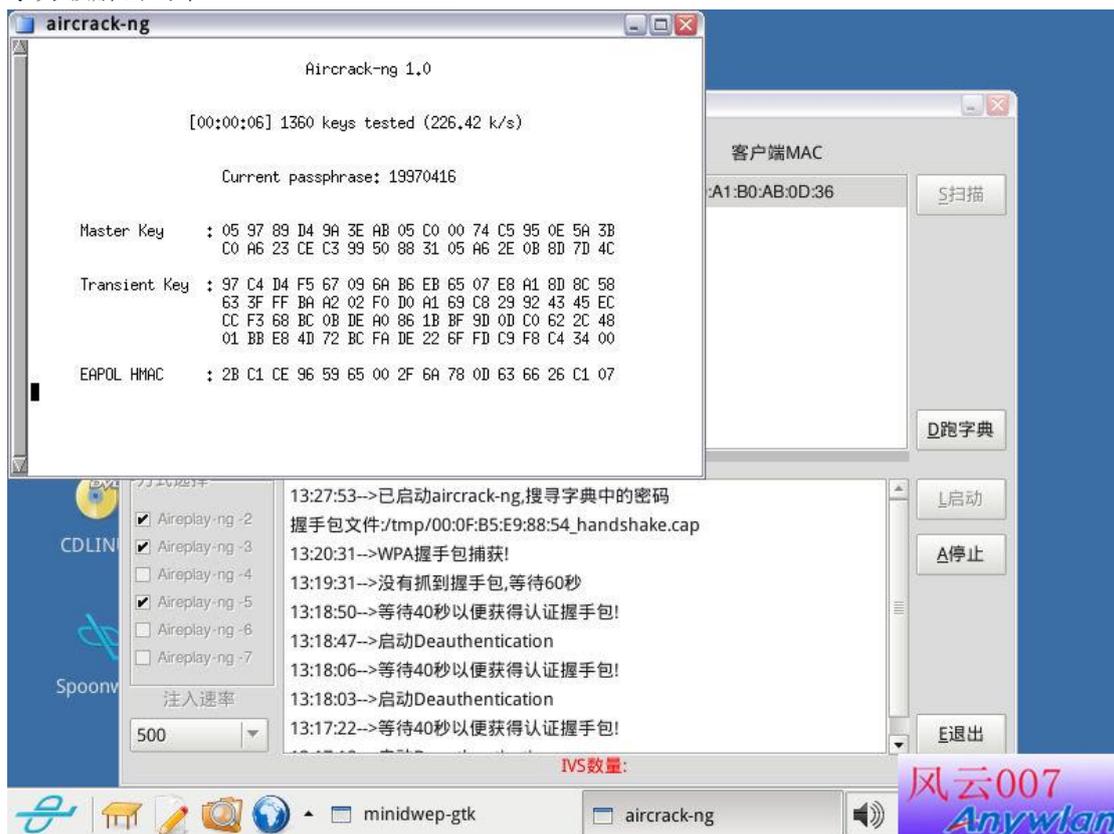
攻击到客户端断线在自动连接就可以获取到“握手包”了。
跳出下面的画面就是得到了“握手包”，选择 YES 在点 OK 进入字典的选择界面。



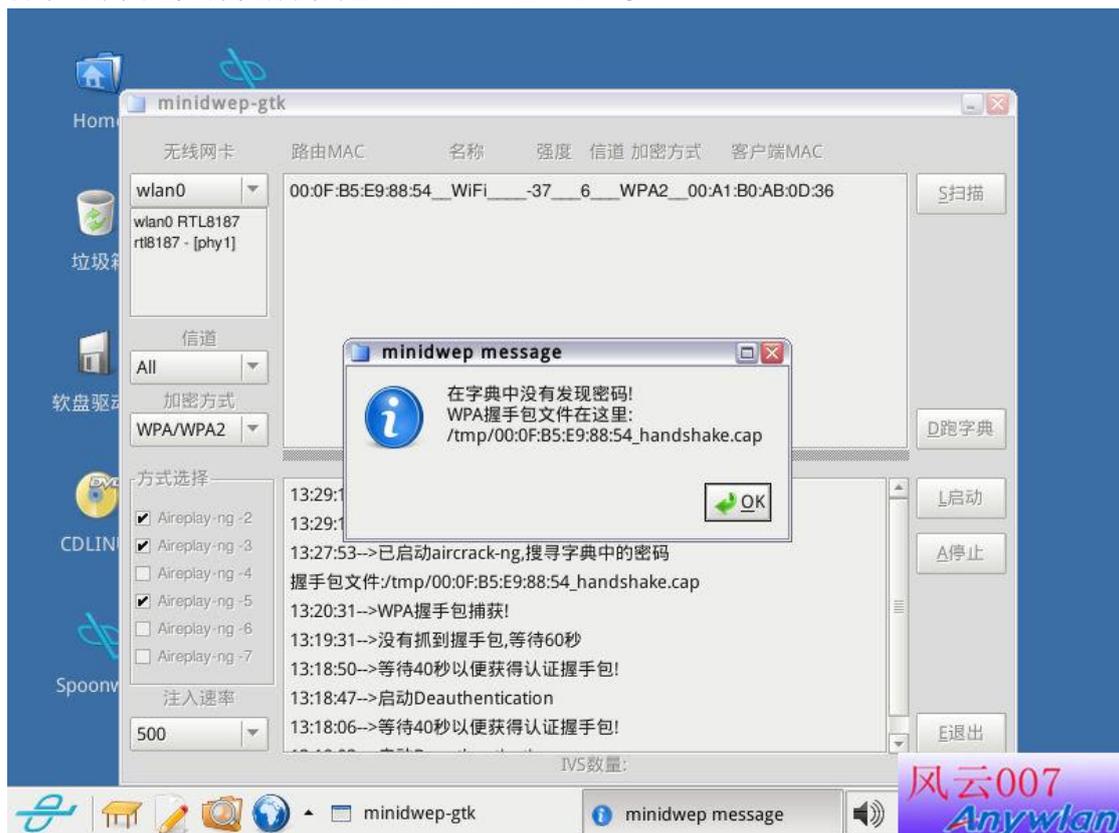
wordlist.txt 就是工具自带的字典，选择后点 OK 开始暴力破解密码。



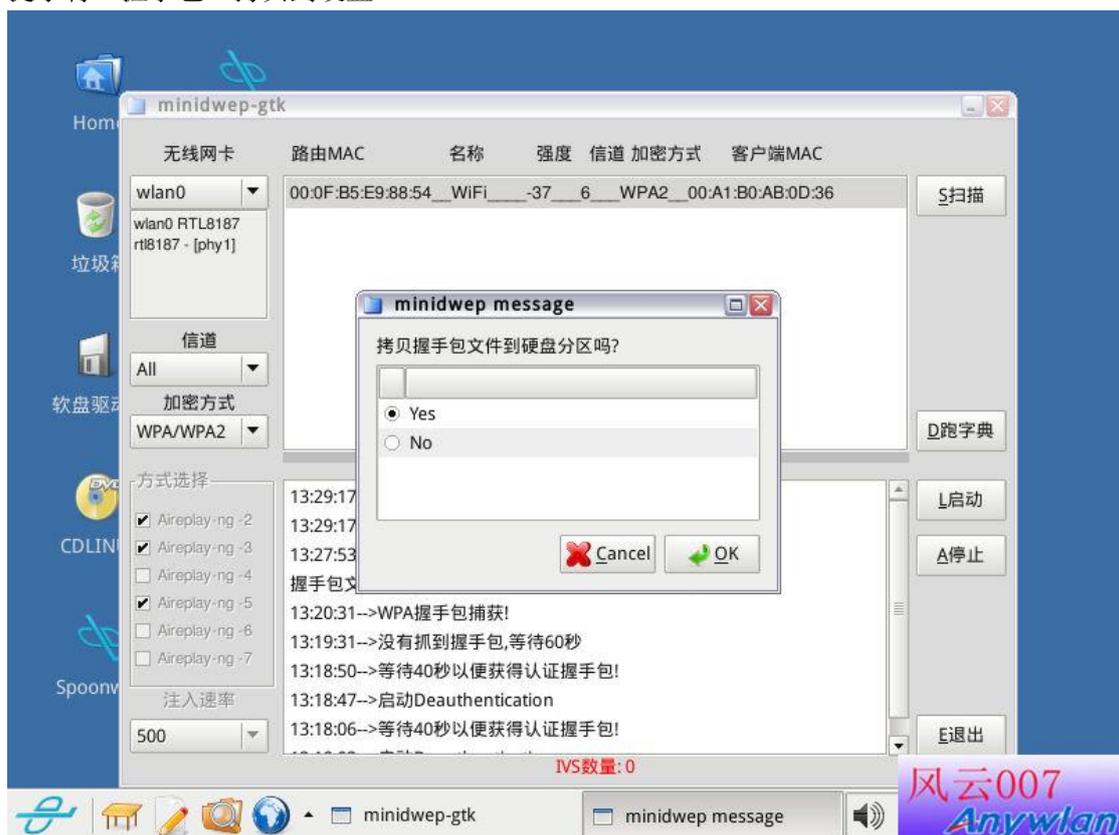
暴力破解密码中.....



时间的长短与字典的大小和字典中是否有正确的密码有关系。
自带的字典跑完都没有找到密码，点 OK 进入下一步。

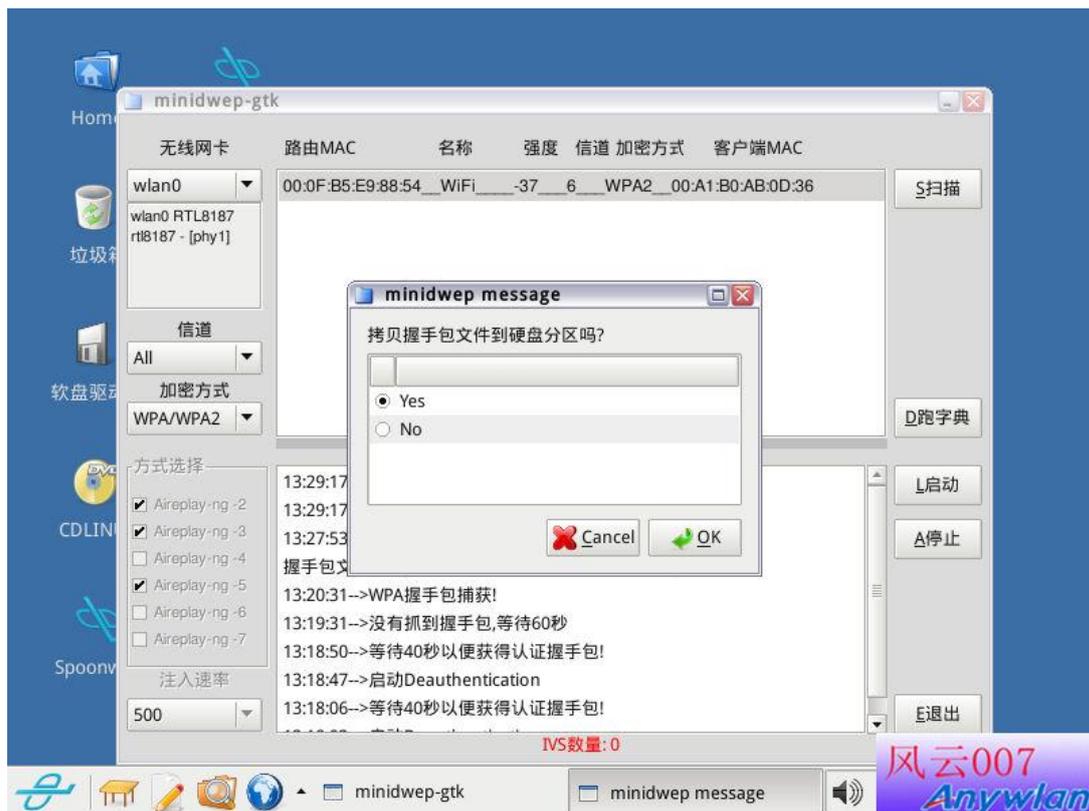


提示将“握手包”拷贝到硬盘。



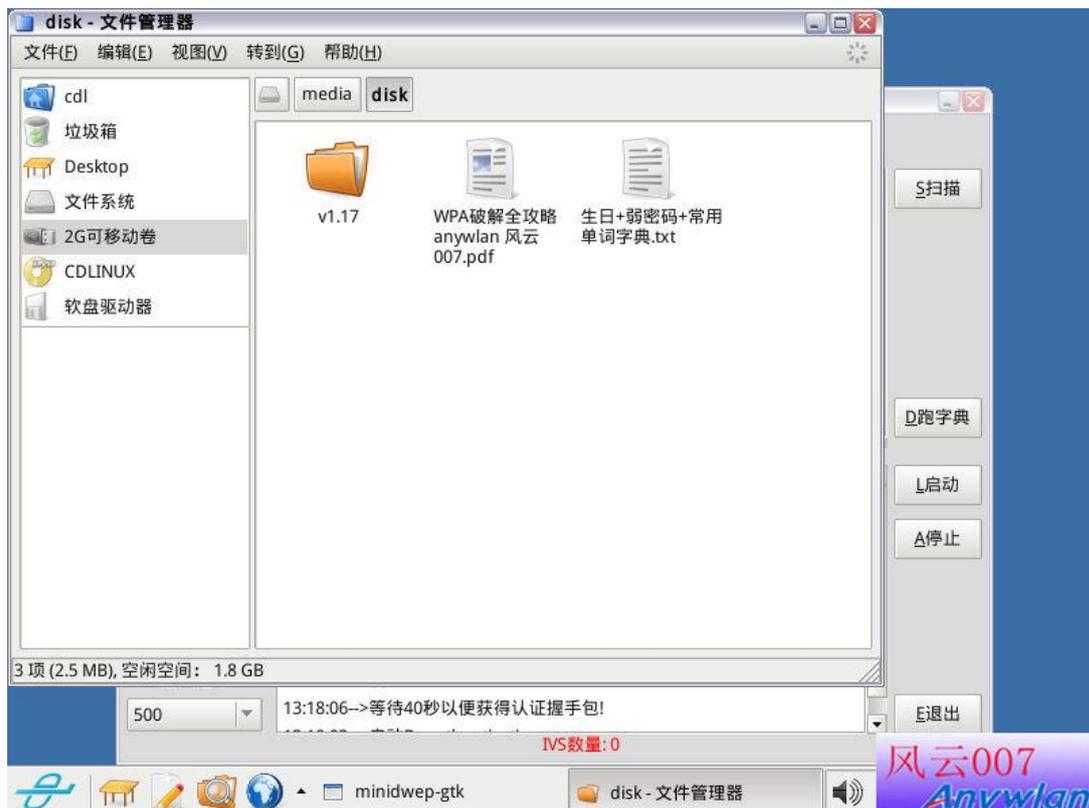
二、使用 U 盘外挂字典继续暴力破解密码

关闭拷贝“握手包”的提示



插入 U 盘，CDlinux 自动打开 U 盘里的根目录。关闭 U 盘的文件管理器。

如果是虚拟机启动要在“虚拟机→可移动设备”里面加载 U 盘并选择自动安装 USB 驱动

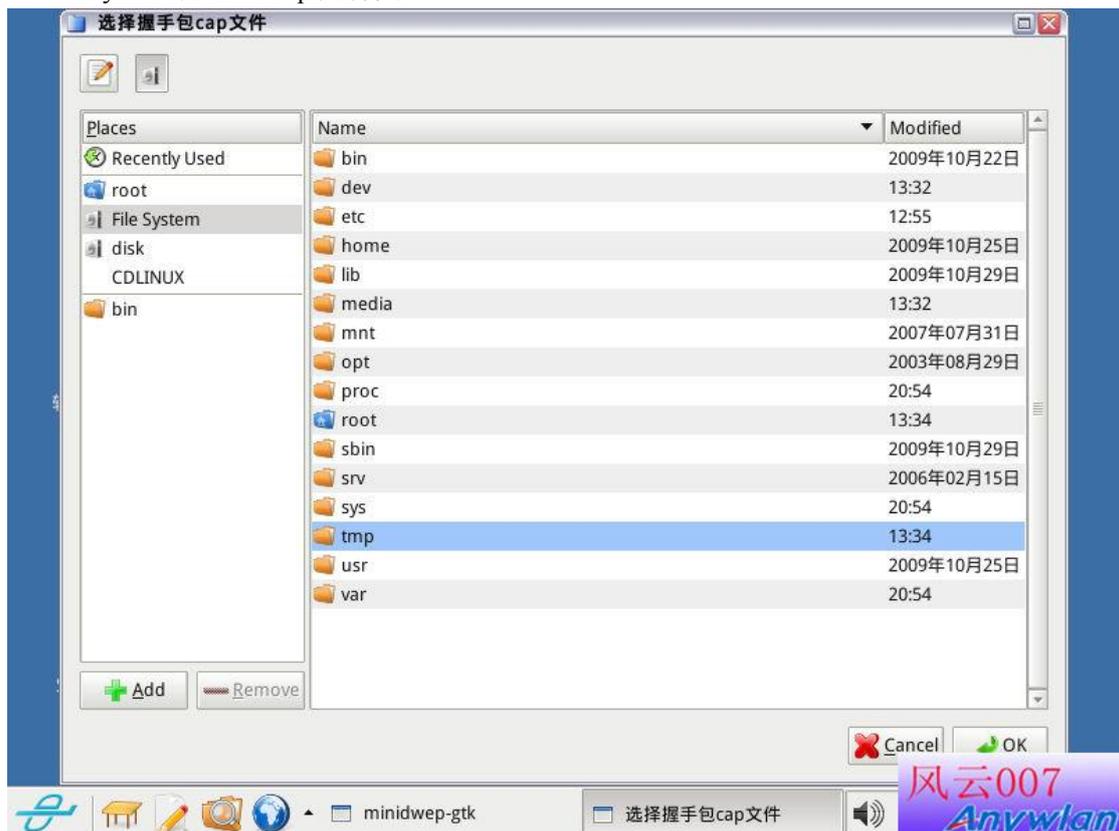


准备好后点击“跑字典”

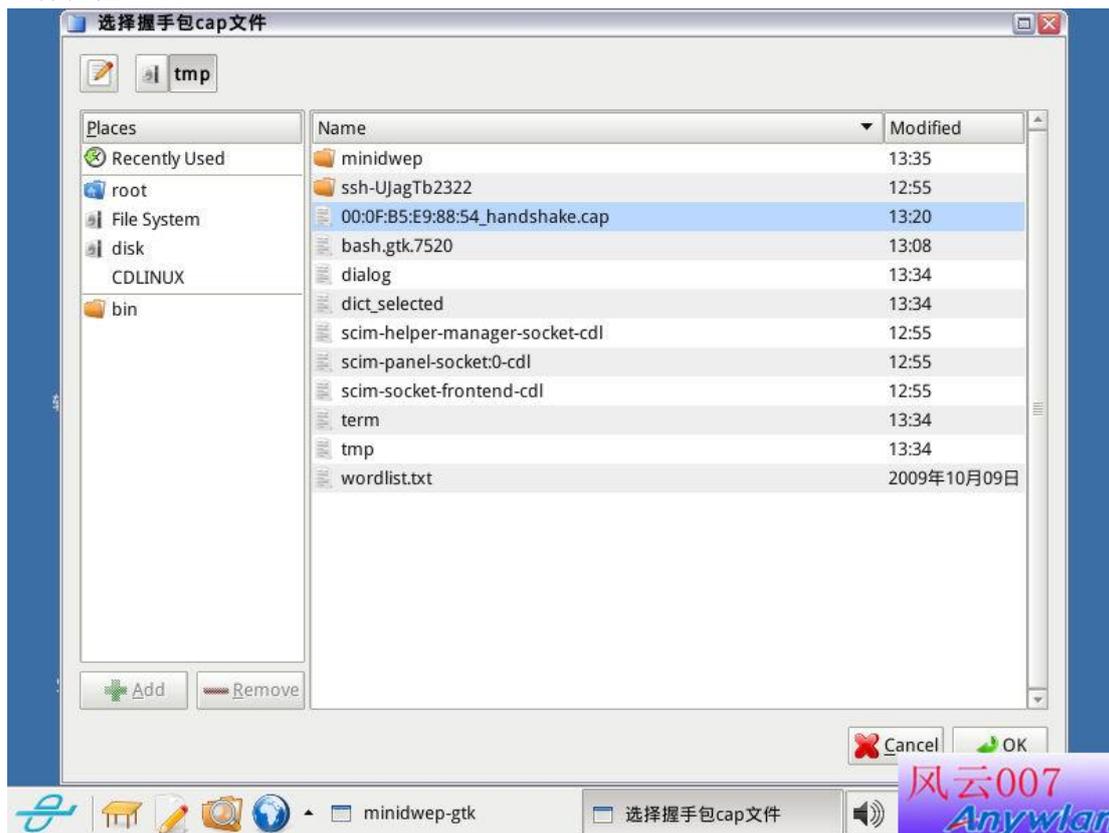


出现选择“握手包”的界面，就是我们先抓到的握手包。

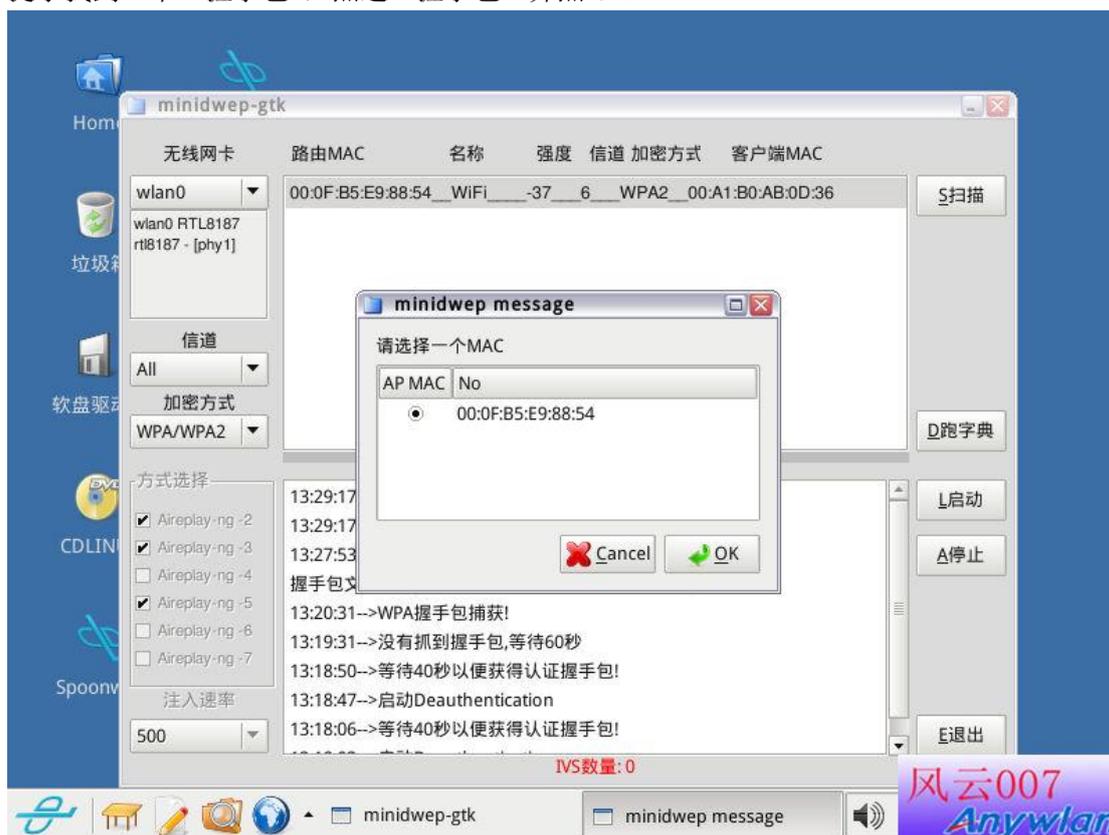
点 file System 再进入 tmp 文件夹



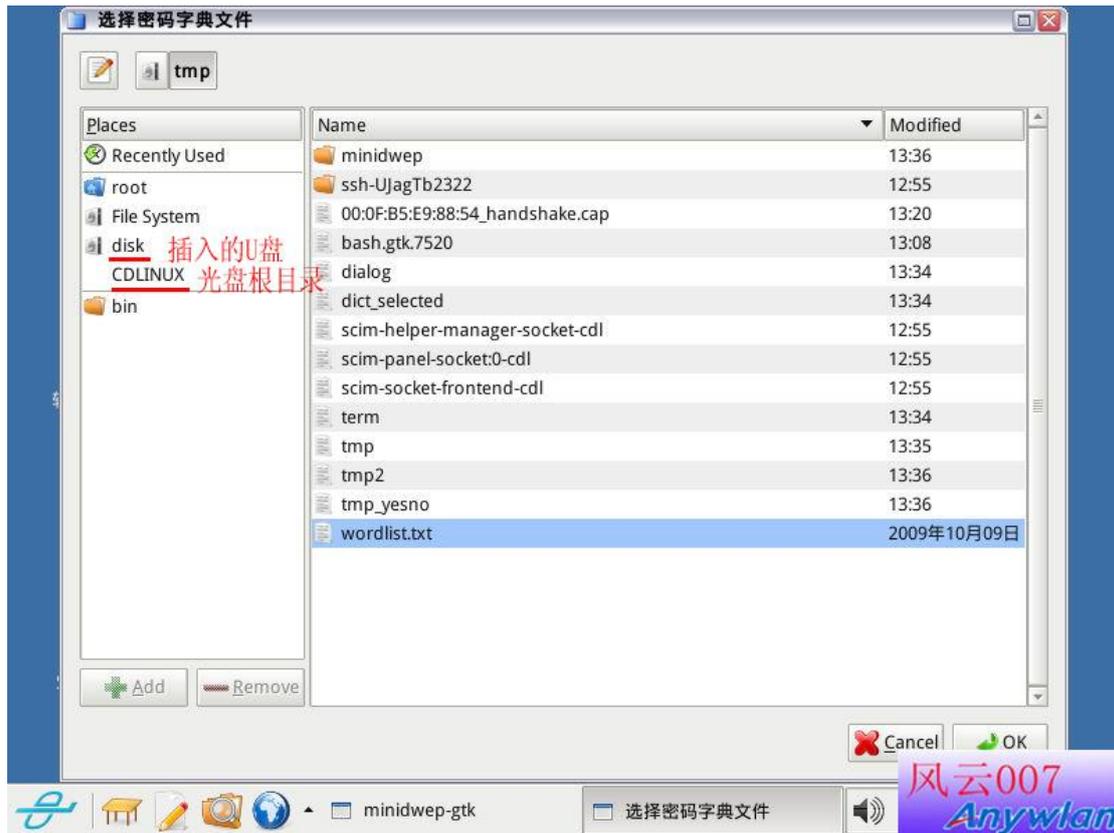
00: 0F: B5: E9: 88: 54-handshake.cap 就是我们先抓到的“握手包”
选择他在点 OK



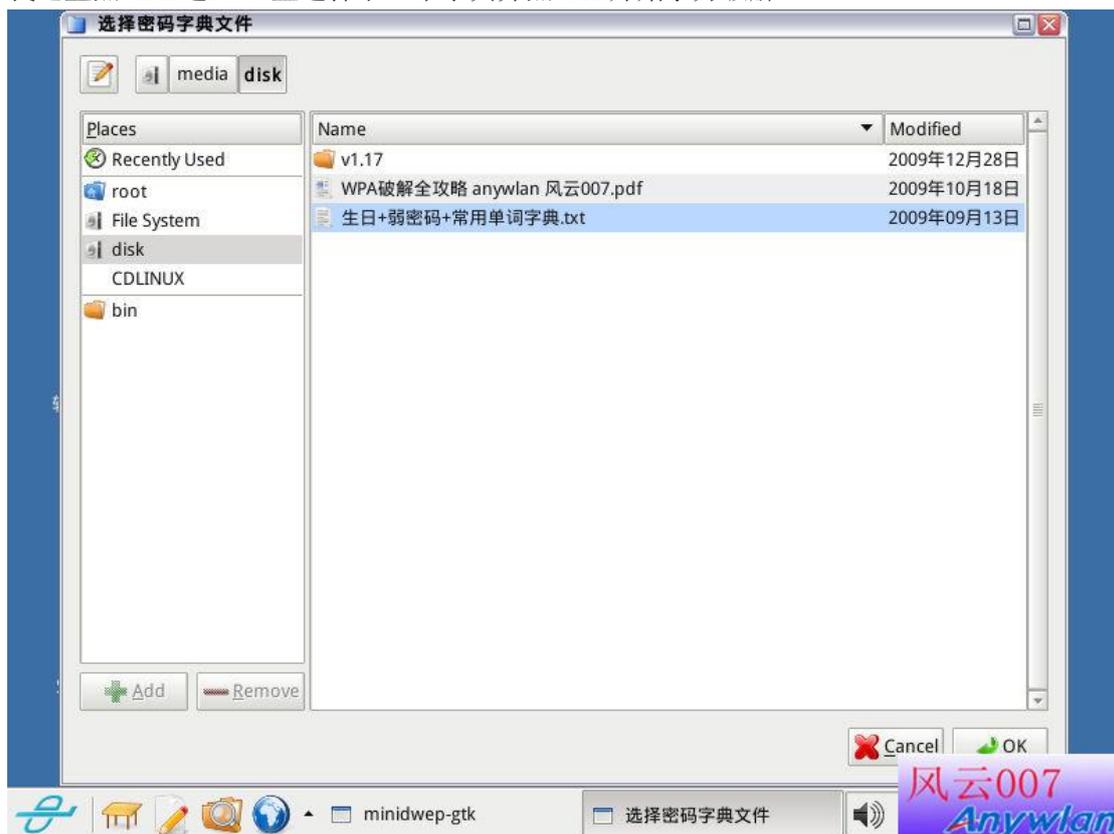
提示找到一个“握手包”，点选“握手包”并点 OK



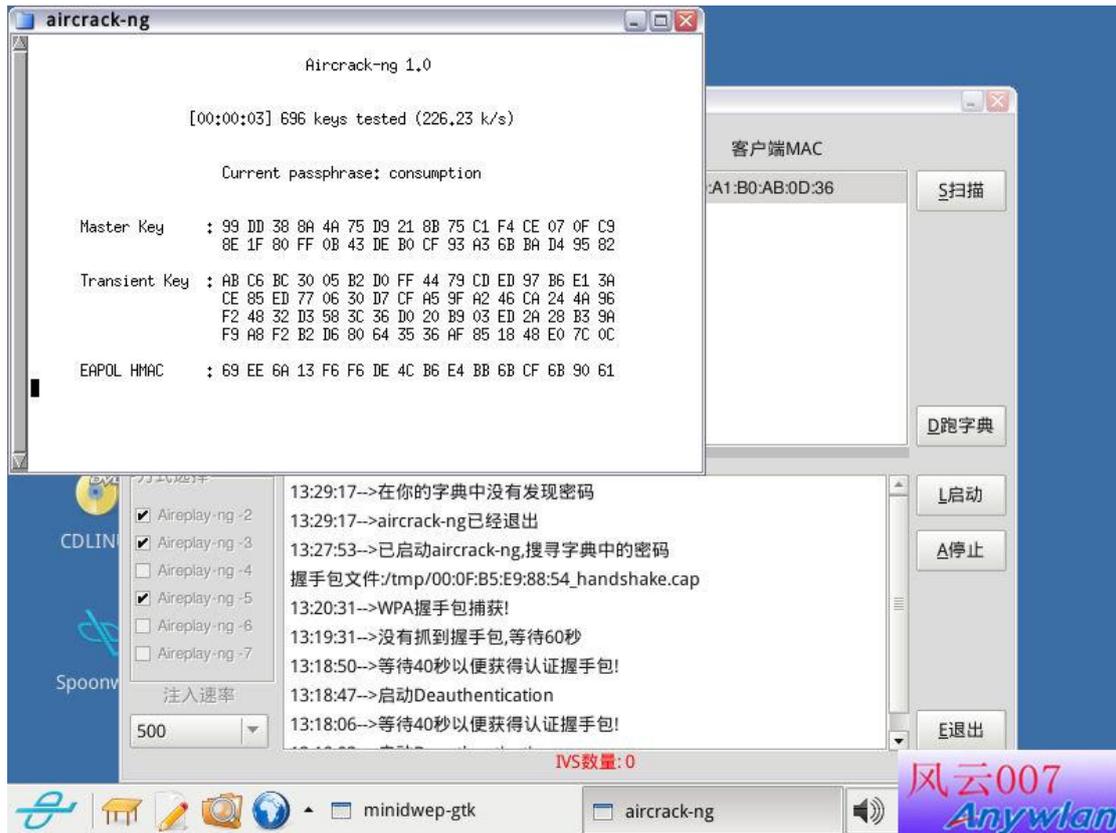
跳出选择字典的界面：选择 U 盘的字典就点 **disk** 、选择光盘里的字典就选择 **CDLINUX**



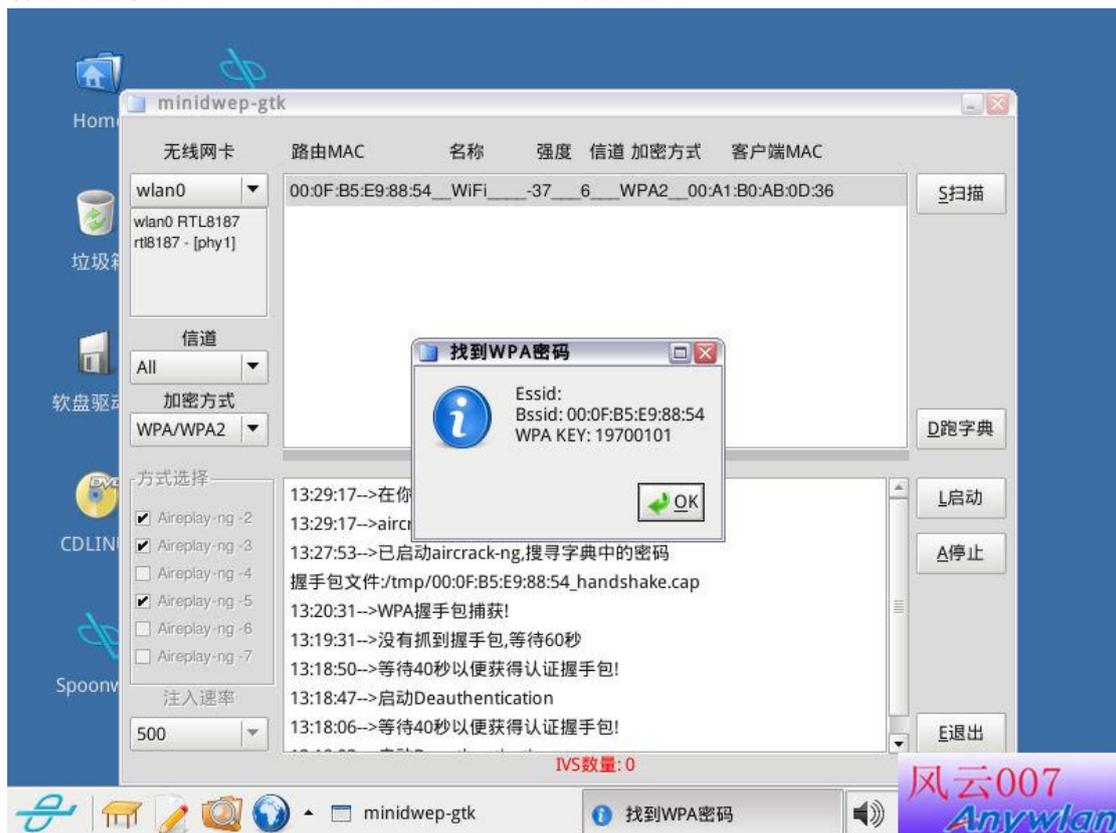
我这里点 **disk** 进入 U 盘选择了一个字典并点 **OK** 开始暴力破解



暴力破解中.....

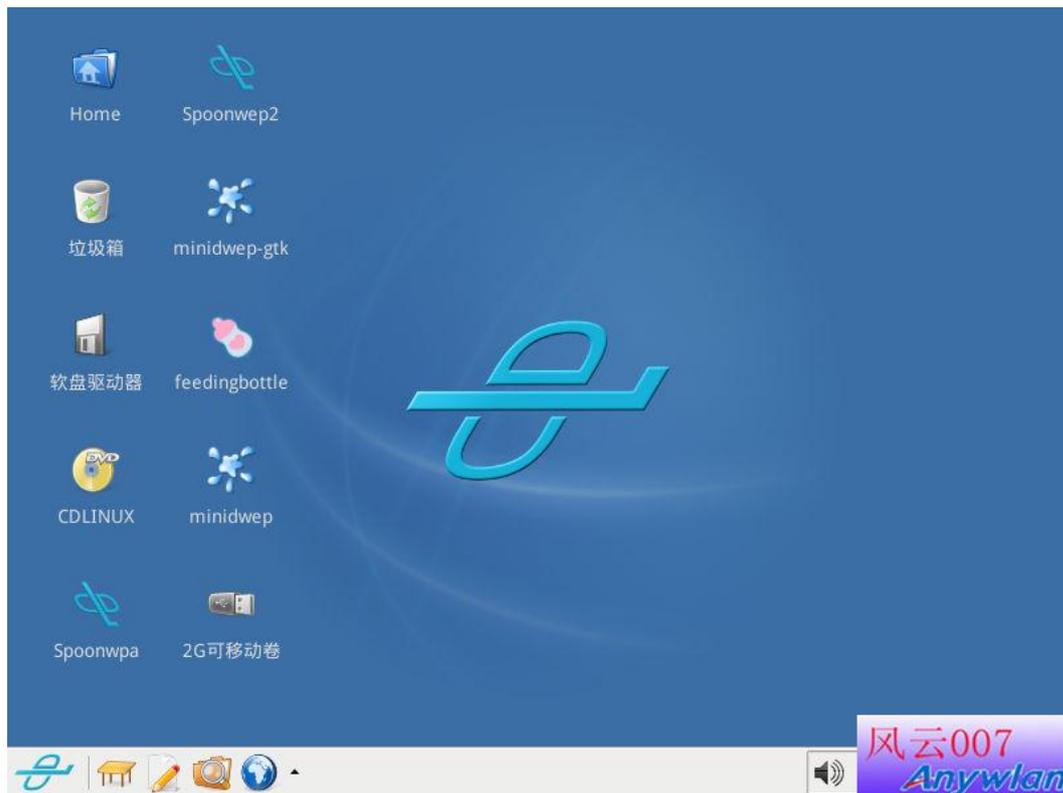


破解速度和字典的大小直接关系，只要字典中有正确的密码存在就一定可以破解出来的。看密码出来了，WPA KEY: 后面的 19700101 就是密码

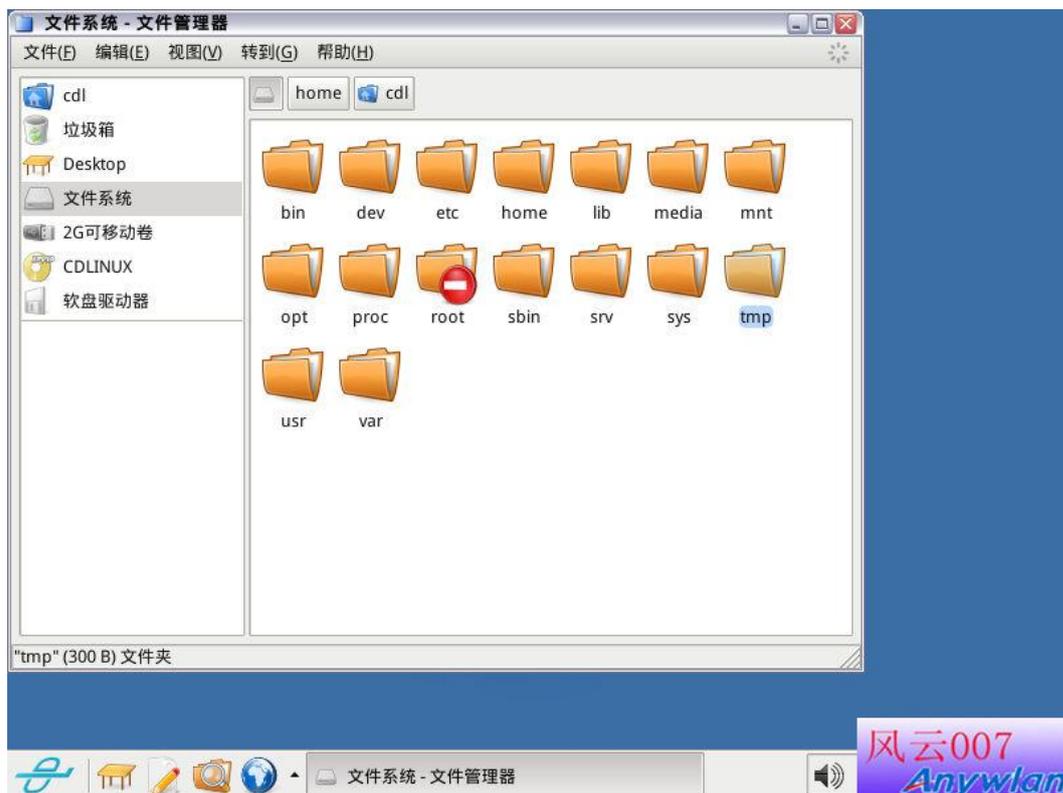


三、将握手包拷贝到 Windows 系统下使用 ewsa 工具高速破解密码

关闭所有的窗口回到桌面，点 Home 打开文件管理器。



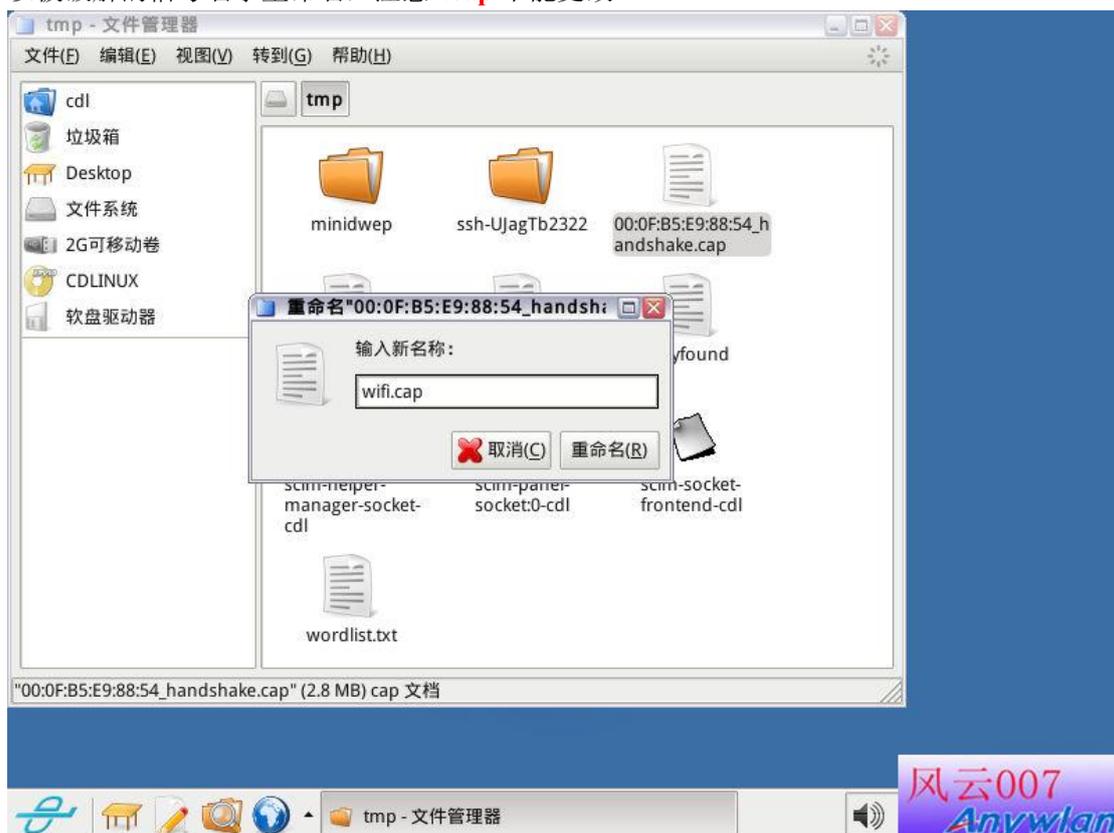
点“文件系统→tmp 文件夹”进入“握手包”的目录。



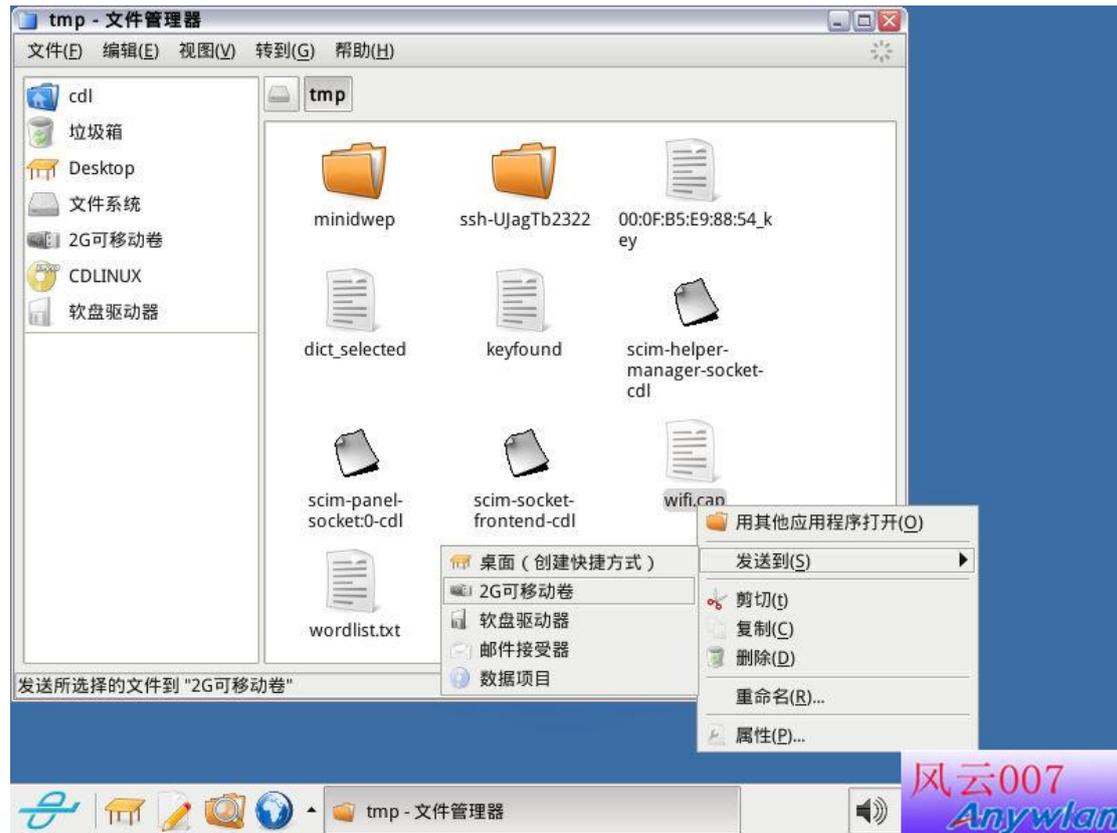
在“握手包”上点鼠标的右键选择“重命名”
因为这个文件名在 Windows 系统下是不允许的，将无法拷贝这个文件到 U 盘。



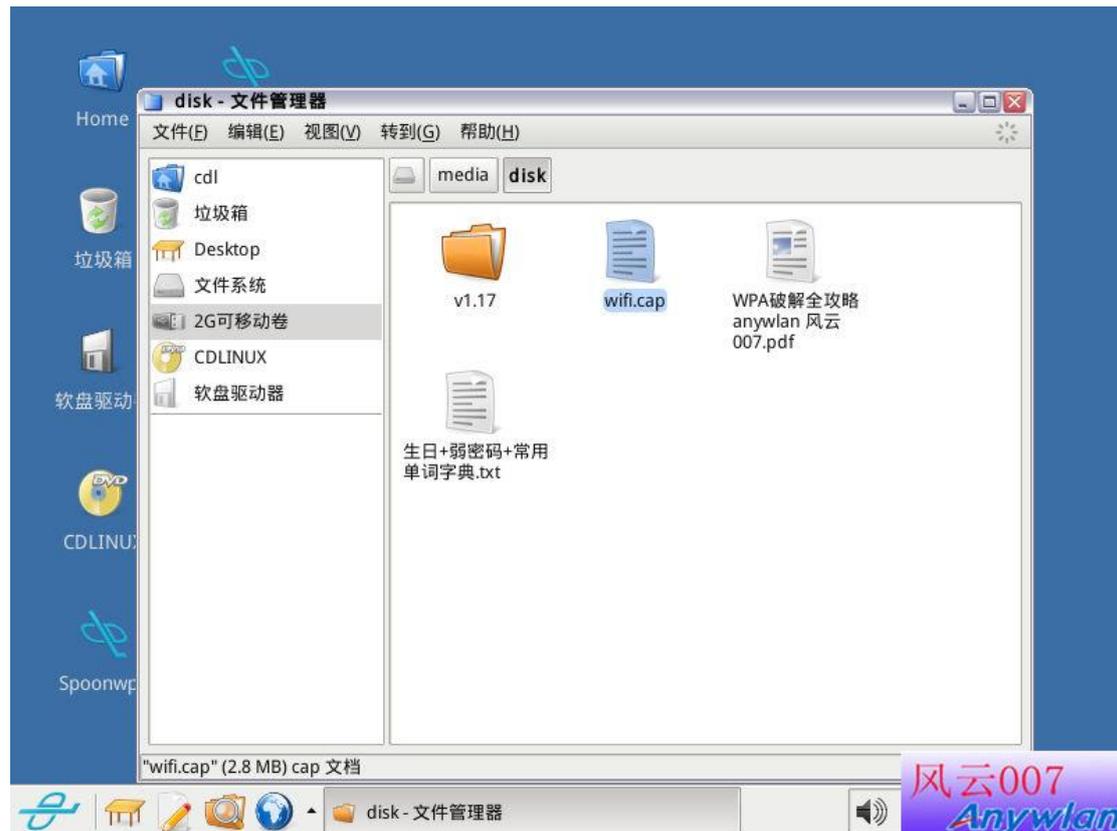
以被破解的信号名字重命名，注意 .cap 不能更改。



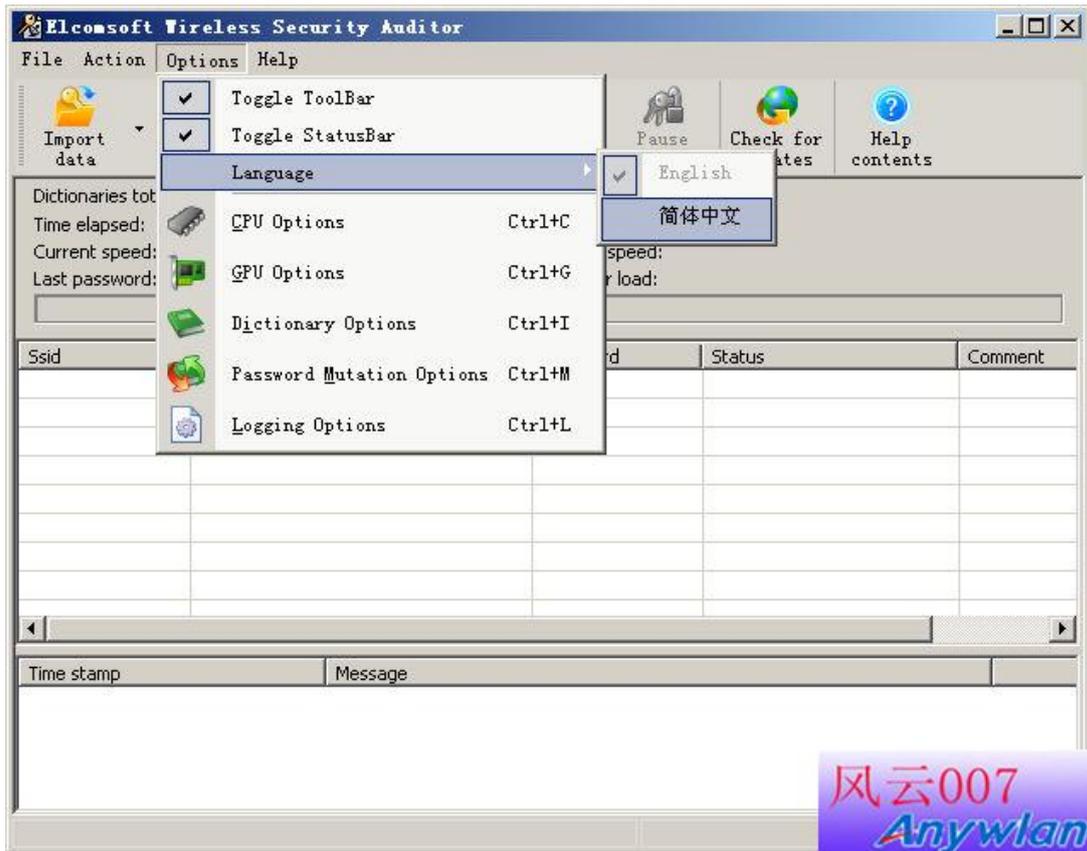
在改好名字的“握手包”上点鼠标的右键选择“发送到→U 盘”



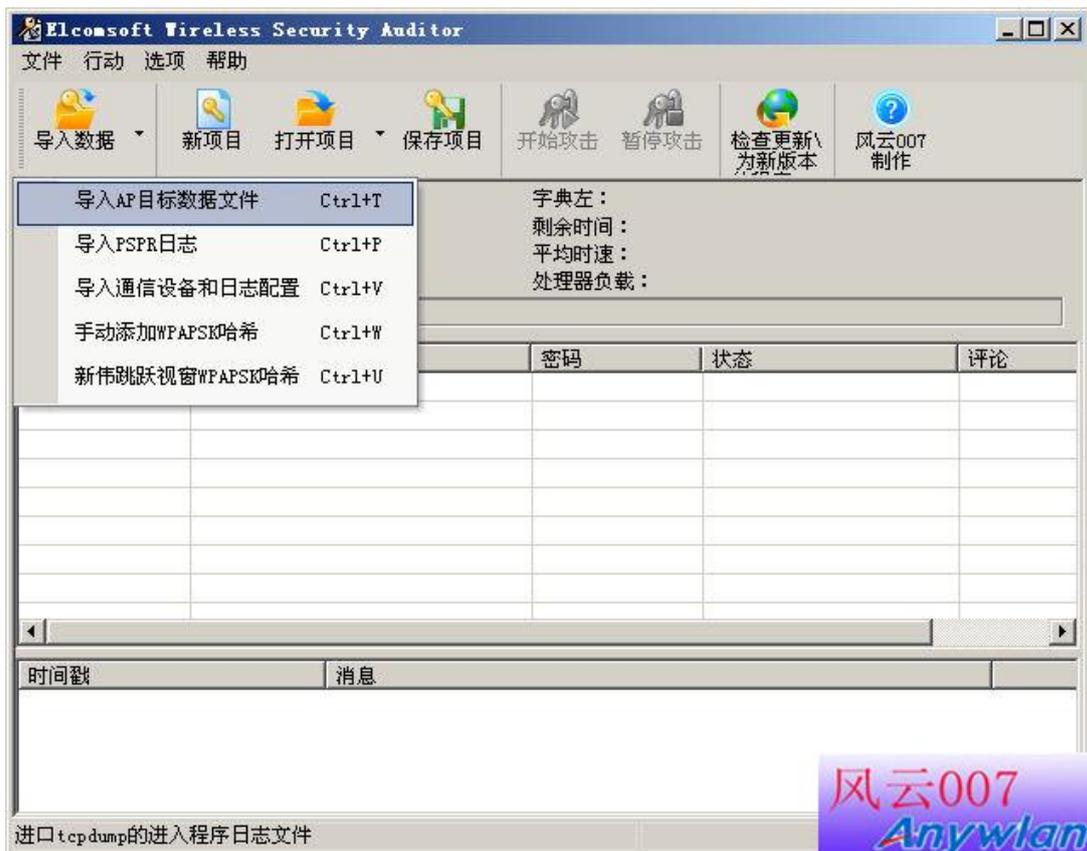
点击桌面的 U 盘图标查看是否保存成功



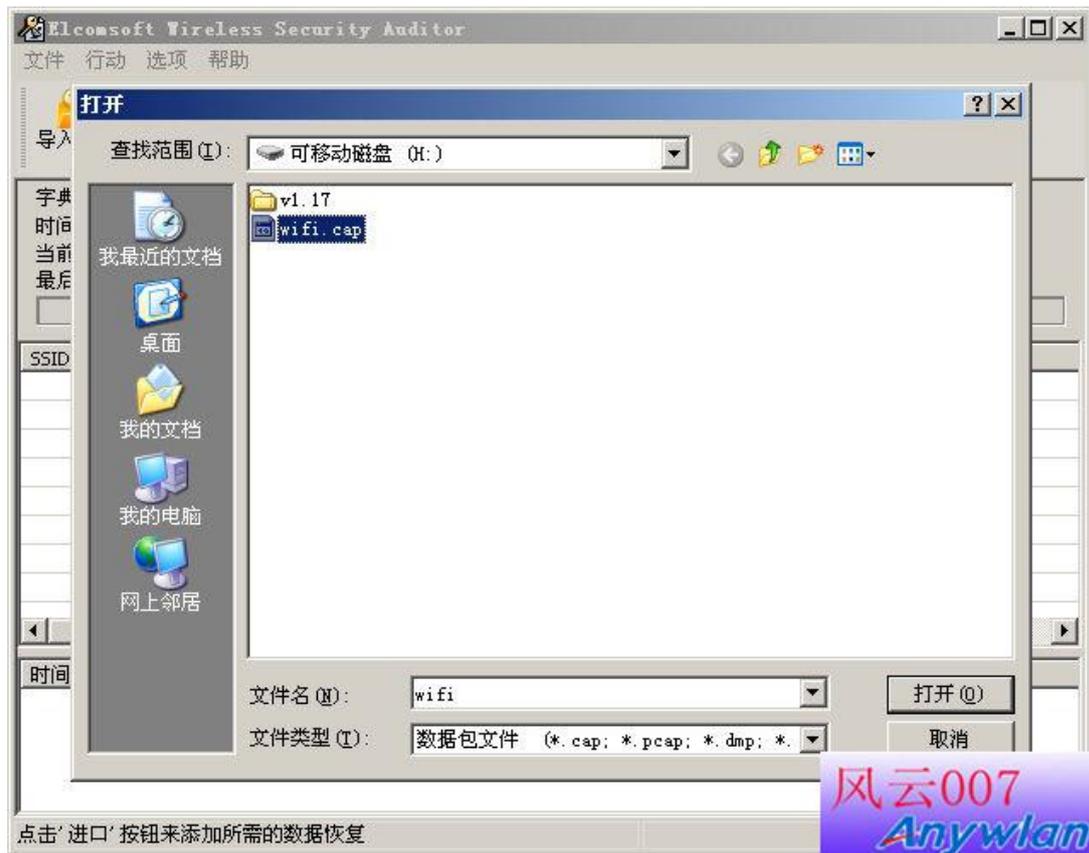
启动 ewsa 并设置为中文



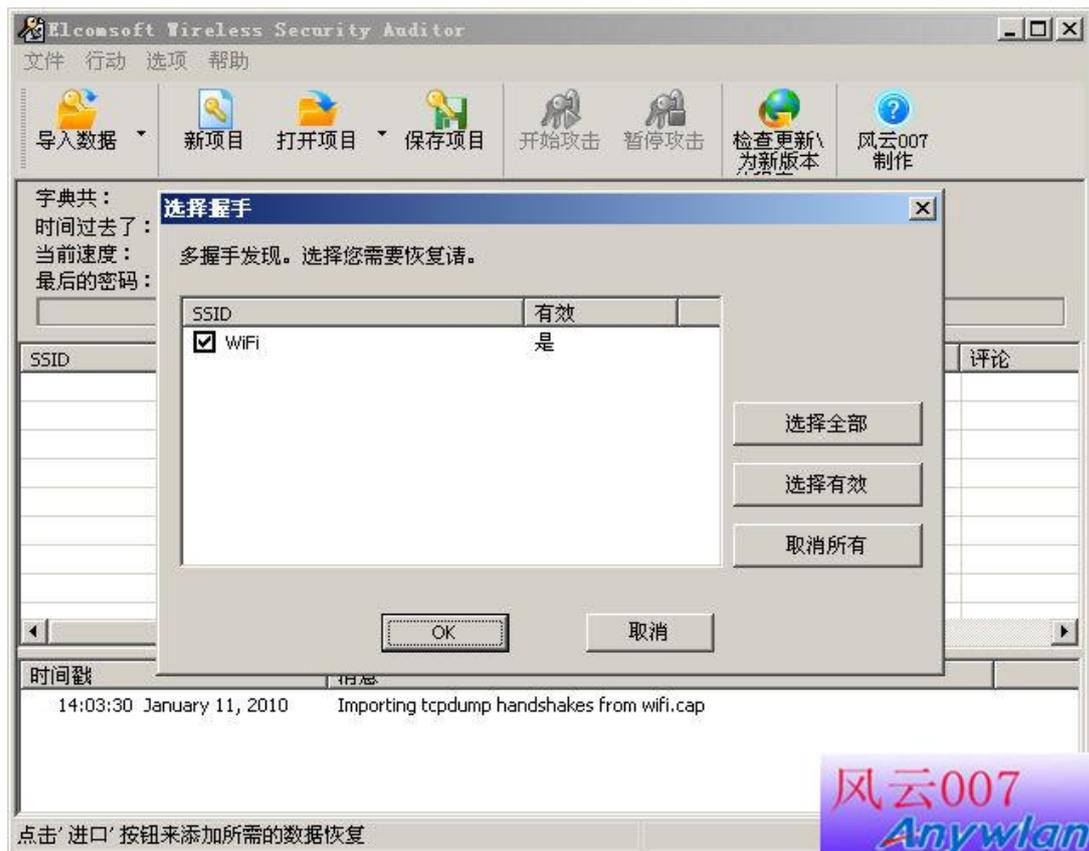
点导入数据→导入 AP 目标数据文件



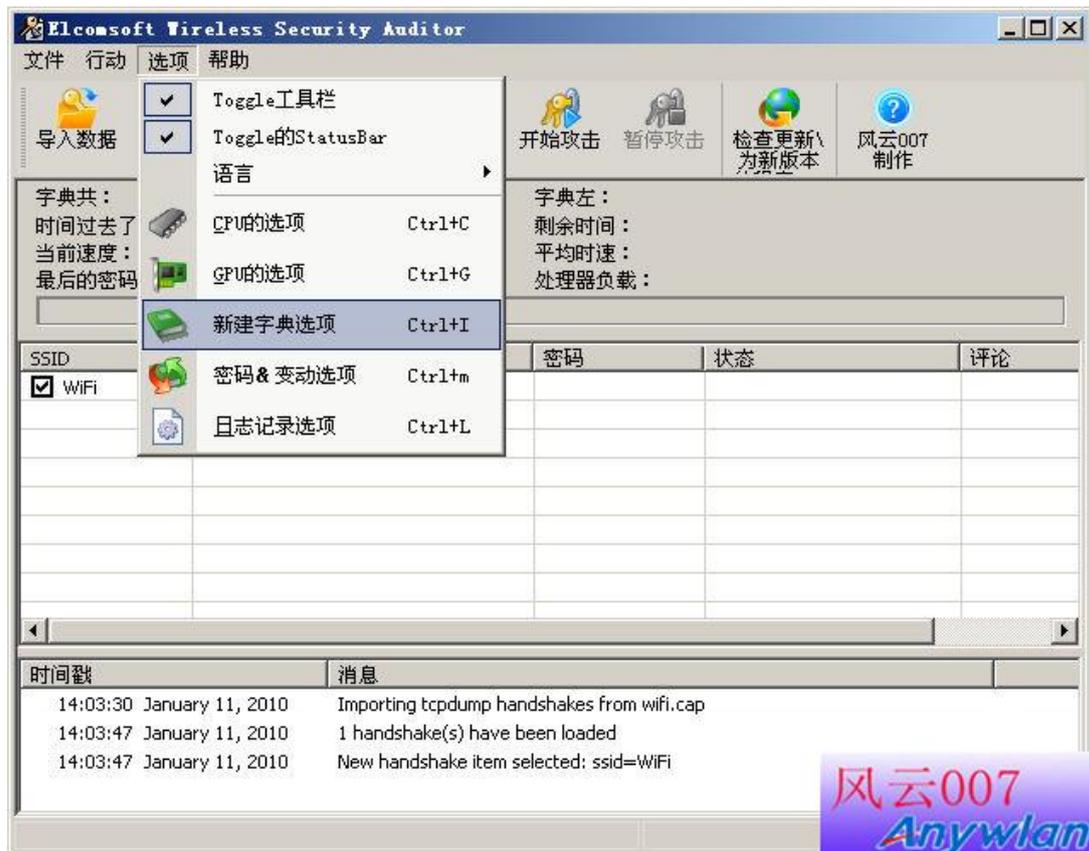
选择刚才 U 盘里面拷贝出来的“握手包”点打开。



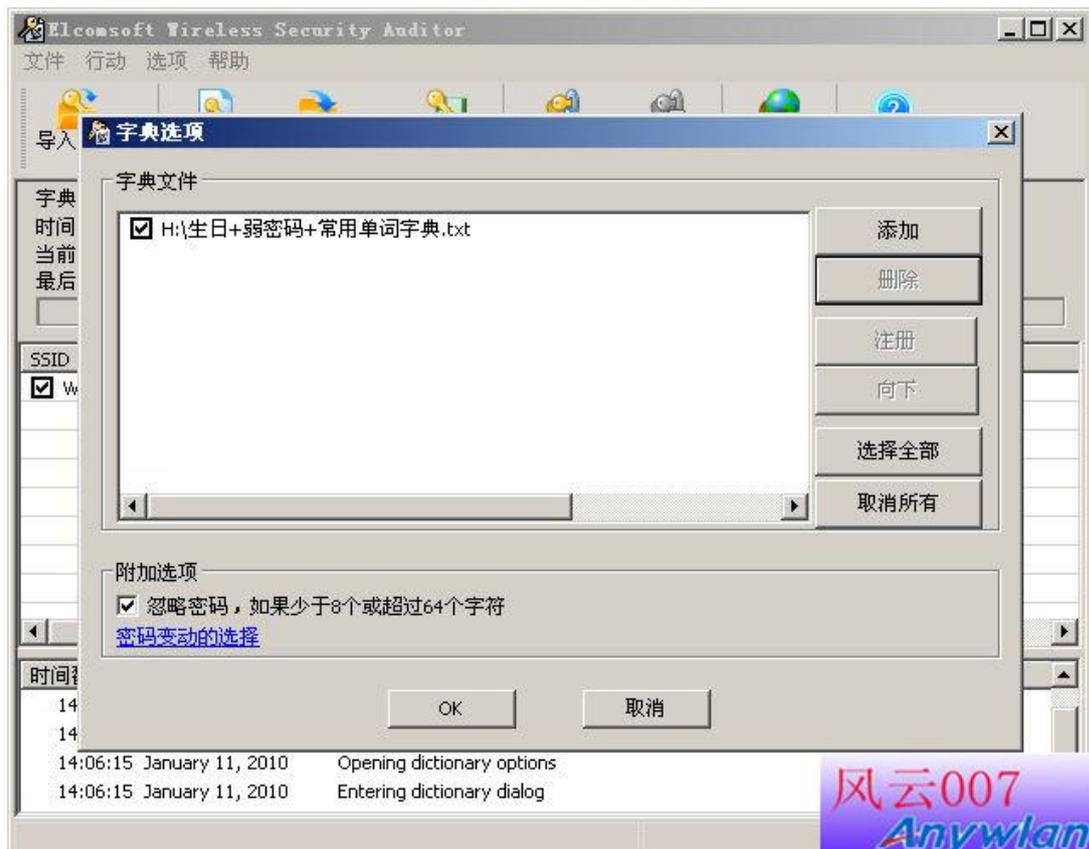
打开后“握手包”再点 OK



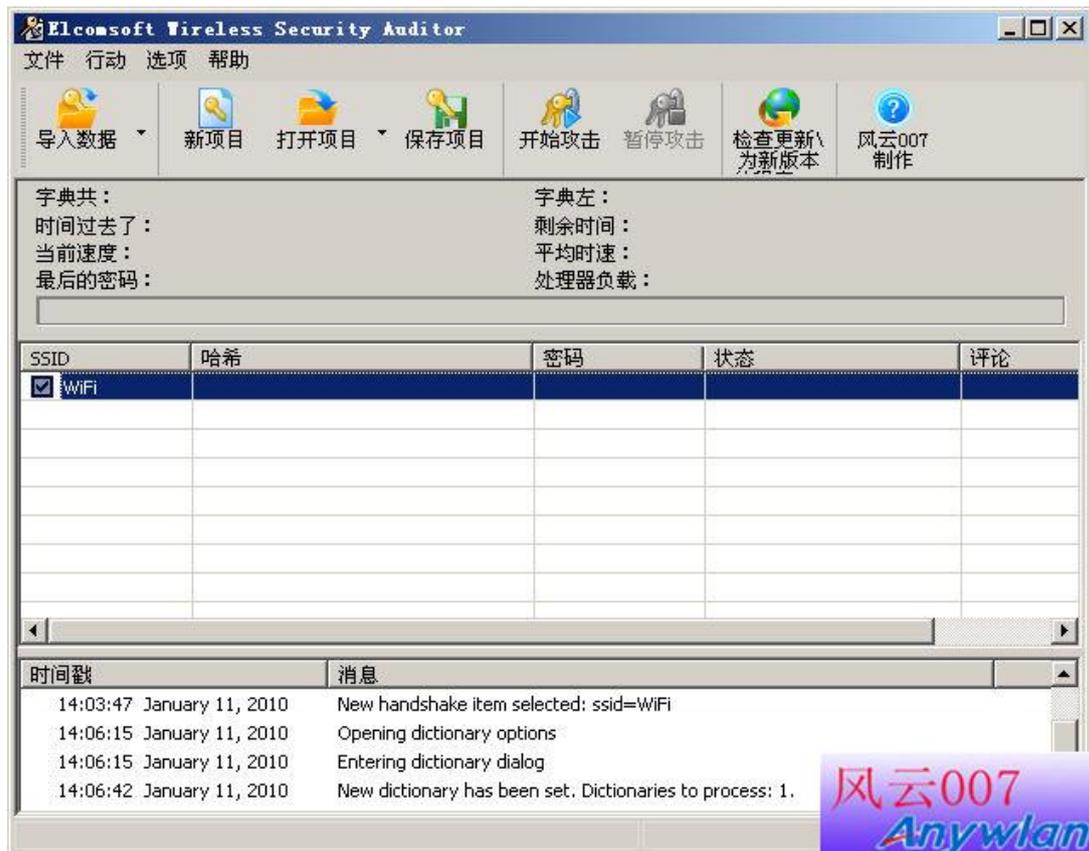
点选项→新建字典选项



添加一部字典也可以是多部字典后点 OK



选择要暴力破解的“握手包”并点开始攻击

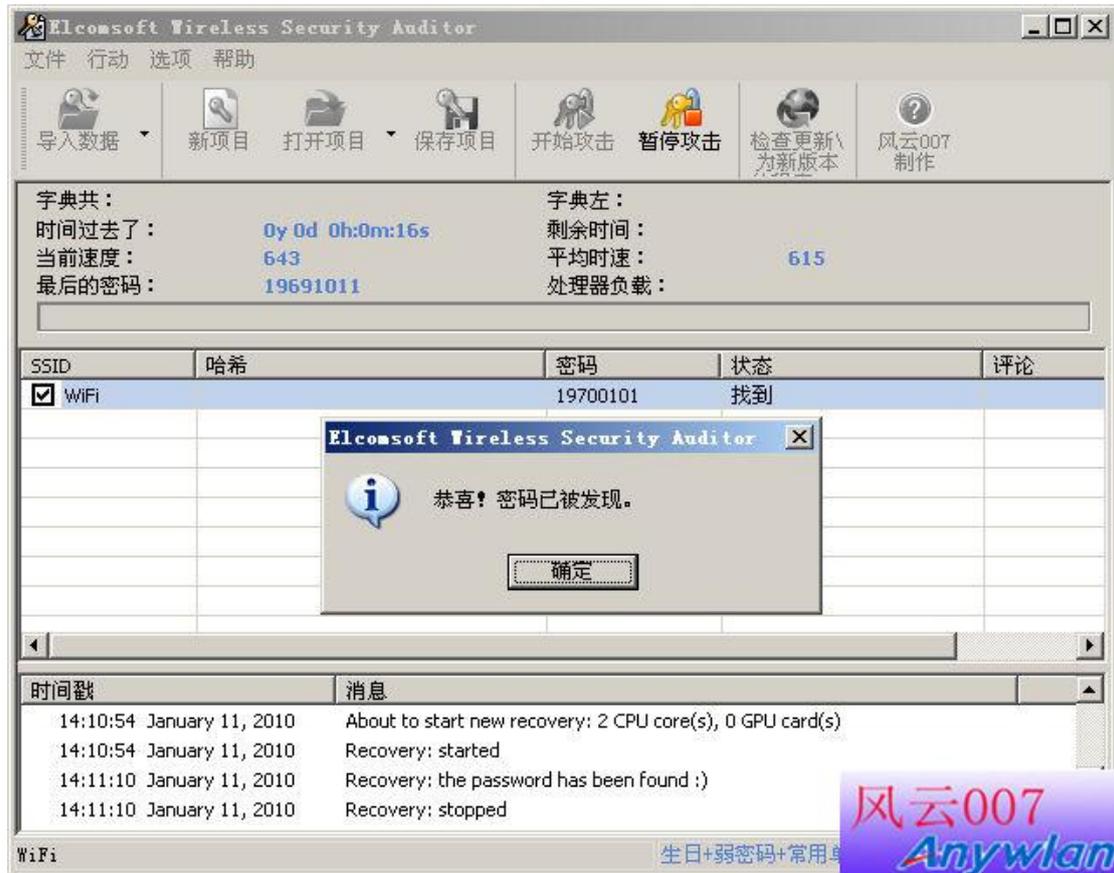


正在暴力破解中.....



密码出来了.....呵呵！

我的破电脑显卡不被软件支持只是纯 CPU 跑的速度已经很快了，如果是 4 核 CPU 加一块好显卡每秒跑字典的速度可以达到一万以上。



Elcomsoft Wireless Security Auditor

ElcomSoft 是一家俄罗斯软件公司，出品过不少密码破解软件，涉及 Office、SQL、PDF、EFS 等等。近日 ElcomSoft 又推出了“Wireless Security Auditor”，号称可以利用 GPU 的运算性能快速攻破无线网络密码，运算速度相比使用 CPU 可提高最多上百倍。本软件的工作方式很简单，就是利用词典去暴力破解无线 AP 上的 WPA 和 WPA2 密码，还支持字母大小写、数字替代、符号顺序变换、缩写、元音替换等 12 种变量设定，在 ATI 和 NVIDIA 显卡上均可使用。

它还通过尝试恢复对 Wi-Fi 通信进行加密的 WPA/WPA2 PSK 初始密码来帮助系统管理员实现对无线网络安全监控。通过运用由两大显卡制造商 ATI 和 NVIDIA 提供的硬件加速技术，Elcomsoft Wireless Security Auditor 已逐渐成为市场上最快速且最具成本效益的 Wi-Fi 密码恢复和无线安全监控工具之一。

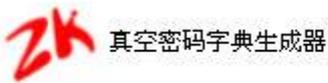
说通俗点就是用 EWSA 加载“握手包”并通过电脑的 CPU 和 GPU 来跑字典快速完成暴力破解

四、破解 WPA 加密“握手包”字典的制作

根据上面的实战大家可以看出 WPA 的加密只要有合理的字典一样可以很快就破掉的，所以我们只要根据中国人特点生成有针对性的字典就可以了！

- 1、一般有常用的弱密码如 1234567890 和常用的英文单词
- 2、生日密码也是大家用的最多的密码
- 3、在就是手机号和座机号码做密码（根据当地电话号码段生成）
手机号码段查询：<http://mobile.tool.la/sheng/>

给大家提供 3 个好用的字典生成工具



黑刀超级字典生成器.exe
黑刀超级字典生成器



万能钥匙字典生成工具(强).exe
XKey1.0 (VC++6)

真空密码字典生成器 - 升级版

系统 制作模式 修改模式 帮助

Flash小游戏 Q我去吧 www.q578.com 我也要玩

制作模式 修改模式 离开程序

生日字典 字符字典 电话密码 拼音密码 高级密码

电话号码格式：
 固定电话 移动电话

设置电话号码
请选择固定的号码段，“*”代表全部，“×”代表空白

<input checked="" type="checkbox"/> 全部号段	<input checked="" type="checkbox"/> 130	<input type="checkbox"/> 153	<input type="checkbox"/> 135	<input type="checkbox"/> 139	<input type="checkbox"/> 158
	<input type="checkbox"/> 131	<input type="checkbox"/> 155	<input type="checkbox"/> 136	<input type="checkbox"/> 150	<input type="checkbox"/> 159
	<input type="checkbox"/> 132	<input type="checkbox"/> 156	<input type="checkbox"/> 137	<input type="checkbox"/> 151	
	<input type="checkbox"/> 133	<input type="checkbox"/> 134	<input type="checkbox"/> 138	<input type="checkbox"/> 157	

电话号码 1 2 3 4 5 6 7 8

预览： 13012345678

查看上次操作结果 开始制作字典

正在进行的操作： 准备制作电话密码 2010-1-11 下午 09:28:02





欢迎光临我的淘宝小店交流

<http://shop61442600.taobao.com>