怎样破解 **WIFI** 密码（只要简单 **4** 步）

并非黑客专利 只要简单 **4** 步

现在利用 **WIFI** 无线上网已经成为了众多网友的上网方式，回到家打开笔记本轻松无线在网络畅游，但如果你经常闯南走北，**WIFI** 上网似乎利用的少之又少，因此许多人选择了 **3G** 无线上网，但 **3G** 的速度和价格实在不太给力，也许在线看个电影，几百元就没了，因此还是找到免费的 **WIFI** 比较靠谱，速度快还无限流量，重要的是不花钱。

身边的加密 **WIFI** 无处不在

之前我们的一篇文章《**WIFI** 信号遍地是**!**免费无线技巧揭秘》，就是传授了大家如何寻找身边的免费**“WIFI”**，并且免费**“**热点**”**信号速度快信号好如何选择的方法，十分实用，有效的解决燃眉之急，但

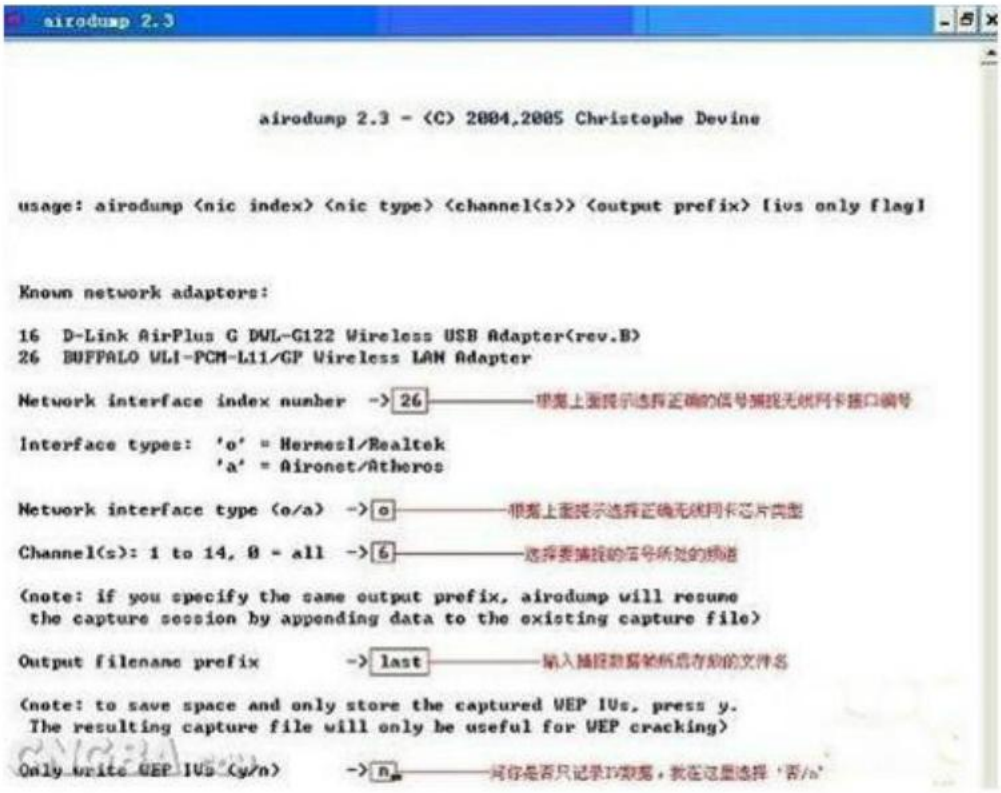
是也存在不方便之处，毕竟免费热点实在凤毛麟角，而身边加密的 **WIFI** 却无处不在，如在需要的时候**“**借用**”**一下，相信也情有可原，下面的文章中就教你简单几步破解身边的 **WIFI** 密码，但是基于道德，在使用他人 **WIFI** 时，不要进行 **BT** 或者在线视频的操作，简单的浏览网页或聊天，避免影响主人使用。**(**注：本教程来自网络达人，成功与否仍看人品**)**

破解静态 **WEP** 密码必备软件：**NetStumbler**（无线信号检测）、**airodump**（捕捉数据帧）与 **WinAircrack**（破解 **WEP** 密码）

静态 **WEP** 密码破解第一步：

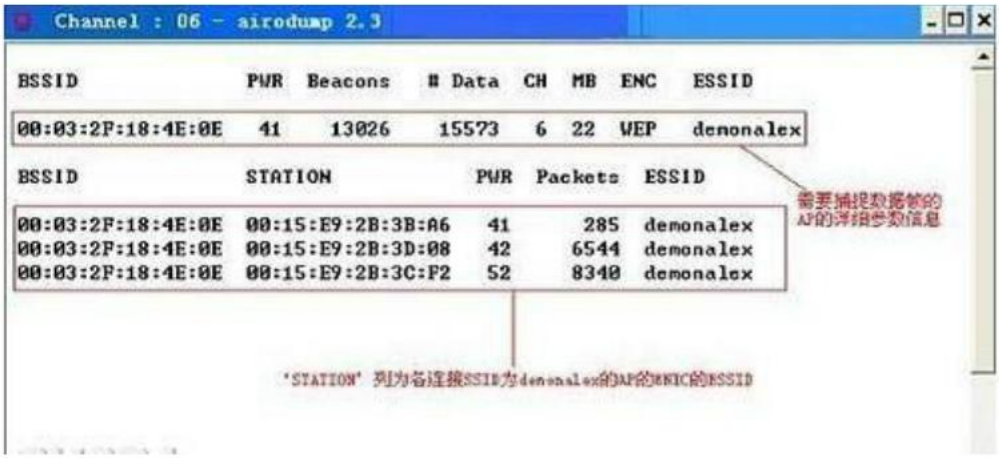
首先通过 **NetStumbler** 确认身边的热点，并通过 **WIFI** 信号的参数进行数据搜集，之后通过上图的红色框框部分内容确定该 **SSID** 名为 **demonalex** 的 **AP** 为 **802.11b** 类型设备，**Encryption** 属性为**‘**已加密**’**，根据 **802.11b** 所支持的算法标准，该算法确定为 **WEP**。有一点需要注意：**NetStumbler** 对任何有使用加密算法的无线站点都会在 **Encryption** 属性上标识为 **WEP** 算法，如上图中 **SSID** 为 **gzpia** 的 **AP** 使用的加密算法是 **WPA2-AES**。

静态 **WEP** 密码破解第二步：



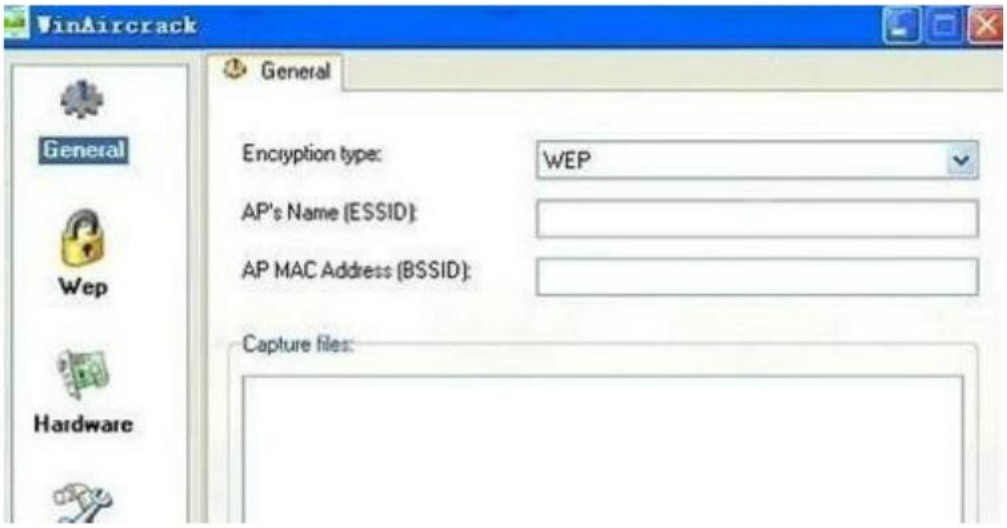
打开 **ariodump.exe** 程序，按照上述图中操作，首先程序会提示本机目前存在的所有无线网卡接口，并要求你输入需要捕捉数据帧的无线网卡接口编号，在这里我选择使用支持通用驱动的 **BUFFALOWNIC ---**编号**‘26’**；然后程序要求你输入该 **WNIC** 的芯片类型，目前大多国际通用芯片都是使用**‘HermesI/Realtek’**子集的，因此选择 **‘o’**；然后需要输入要捕捉的信号所处的频道，我们需要捕捉的 **AP** 所处的频道为**‘6’**；提示输入捕捉数据帧后存在的文件名及其位置，若不写绝对路径则文件默认存在在 **winaircrack** 的安装目录下，以**.cap** 结尾，我在上例中使用的是**‘last’**；最后 **winaircrack** 提示：**‘**是否只写入**/**记录 **IV[**初始化向量**]**到 **cap** 文件中去？**’**，我在这里选择**‘**否**/n’**；确定以上步骤后程序开始捕捉数据包。

静态 **WEP** 密码破解第三步：



第三步就是漫长的等待了，直至上表中**‘Packets’**列的总数为 **300000** 时即可满足实验要求。根据实验的经验所得：当该 **AP** 的通信数据流量极度频繁、数据流量极大时，**‘Packets’**所对应的数值增长的加速度越大。当程序运行至满足**‘Packets’=300000** 的要求时按 **Ctrl+C** 结束该进程。此时你会发现在 **winaircrack** 的安装目录下将生成 **last.cap** 与 **last.txt** 两个文件。

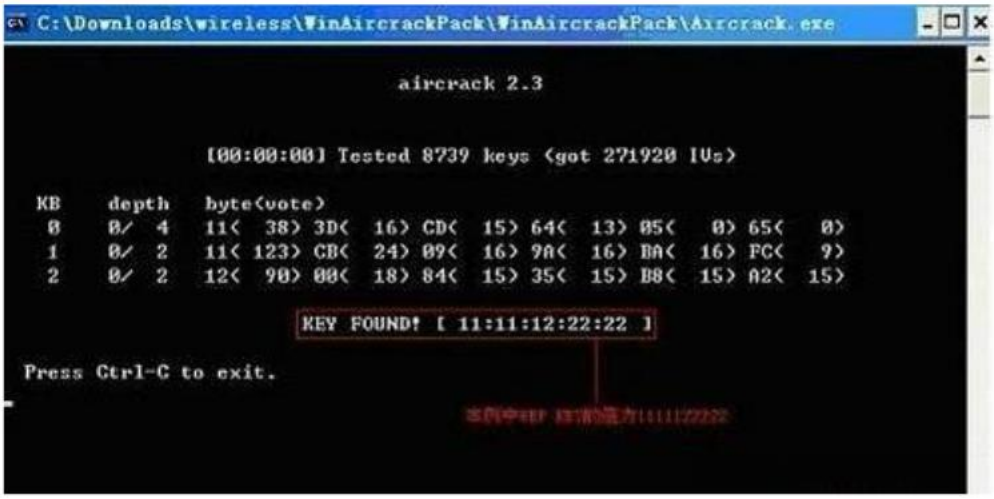
静态 **WEP** 密码破解第四步：



破解工作主要是针对 **last.cap** 进行，首先执行 **WinAirCrack.exe** 文件，单击上图红色框框部分的文件夹按钮，弹出***.cap** 选定对话框，

选择上面生成的 **last.cap** 文件，然后通过点击右方的**‘Wep’**按钮切换主界面至 **WEP** 破解选项界面。

选择**‘Key size’**为 **64**（目前大多数用户都是使用这个长度的 **WEPKEY**，因此这一步骤完全是靠猜测选定该值），最后单击主界面右下方的**‘Aircrack thekey…’**按钮，此时将弹出一个内嵌在 **cmd.exe** 下运行的进程对话框，并在提示得出 **WEP** 密码。



打开无线网卡的连接参数设置窗口，设置参数为： **SSID：demonalex** 频道：**6 WEP KEY：1111122222**（**64** 位） **OK**，现在可以享受免费 **WIFI** 了。虽非黑客专利，使用要讲道德!!