无线破解工具（奶瓶）Beini_1.2.2_集成 600W 密码！附使用教程（图文视频）！

适合破解 WPA 和 WPE 信号！

现在我们需要的是一个 U 盘，别小于 128MB 就行。

将其格式化

先把它格式化了，需要注意的是，一定要选择 FAT 格式，这点一定要记住，否则下面就没办法继续进行了。格式化完成之后，下面就让我们向着周围的路由器们发起进攻吧。

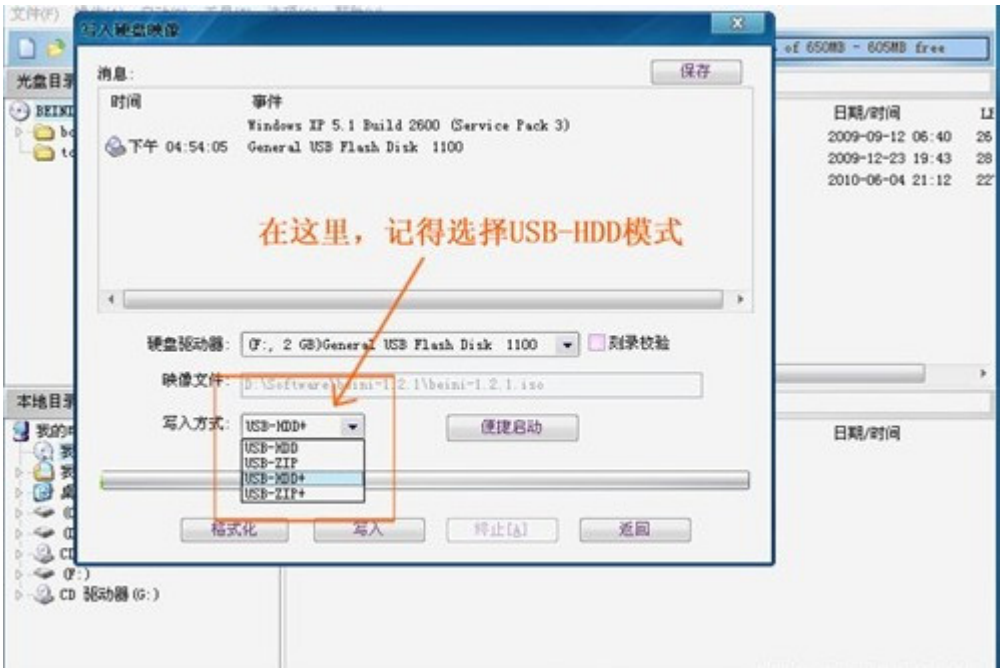
绰号“奶瓶”的 Linux 系统

奶 瓶这个系统，相信玩无线的朋友应该都会知道。这是一款基于 Tiny Core Linux 搭建的无线网络安全测试系统，当然由于它是用来安全测试的系统，因此在安全方面自然有着强大的功能。而且，这个系统非常简便易学，因此现在已经逐渐的取代 BT3、BT4 之类的工具，而逐渐成为了无线网络安全研究的主流系统。今天，我们就要应用这个系统来完成后面的事情。第 2 页：制作“奶瓶”启动 U 盘

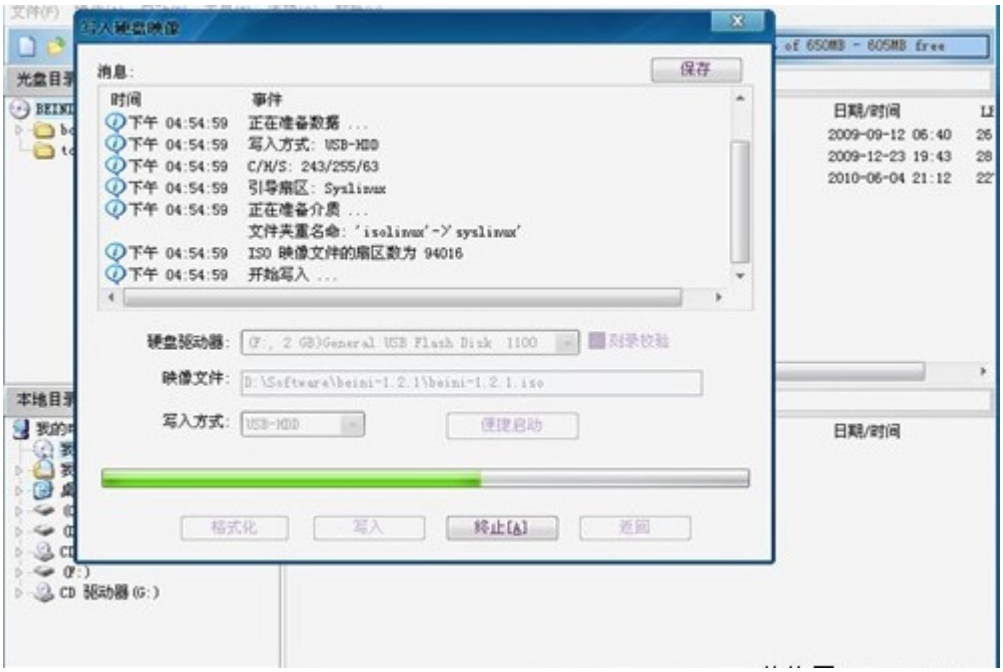
相比于其它的系统，“奶瓶”最大的优点除了操作简便易懂之外，还有一个优点就是制作 U 盘启动盘非常容易，而且成功率较高。

UltraISO 软件界面

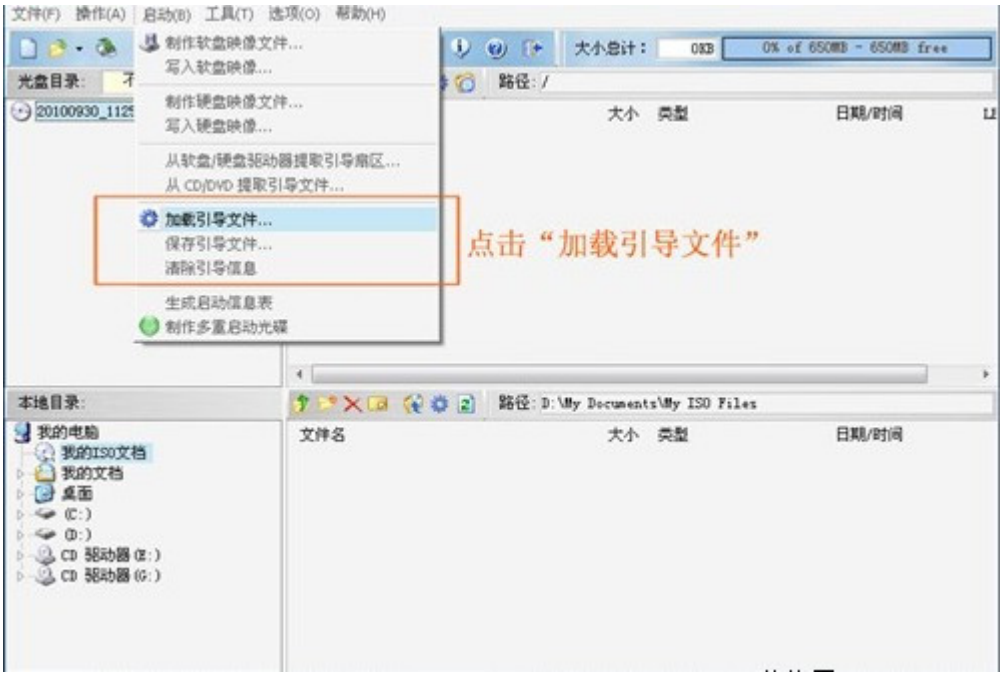
下载好的“奶瓶”系统是一个.iso 文件，而大小只有 40MB 左右，因此我们可以轻易的使用镜像软件将其写入 U 盘。这里，我们使用了 UltraISO 这款软件，相比其它的同类型软件，这款显得要简便易懂很多。



导入镜像文件之后，选择写入方式

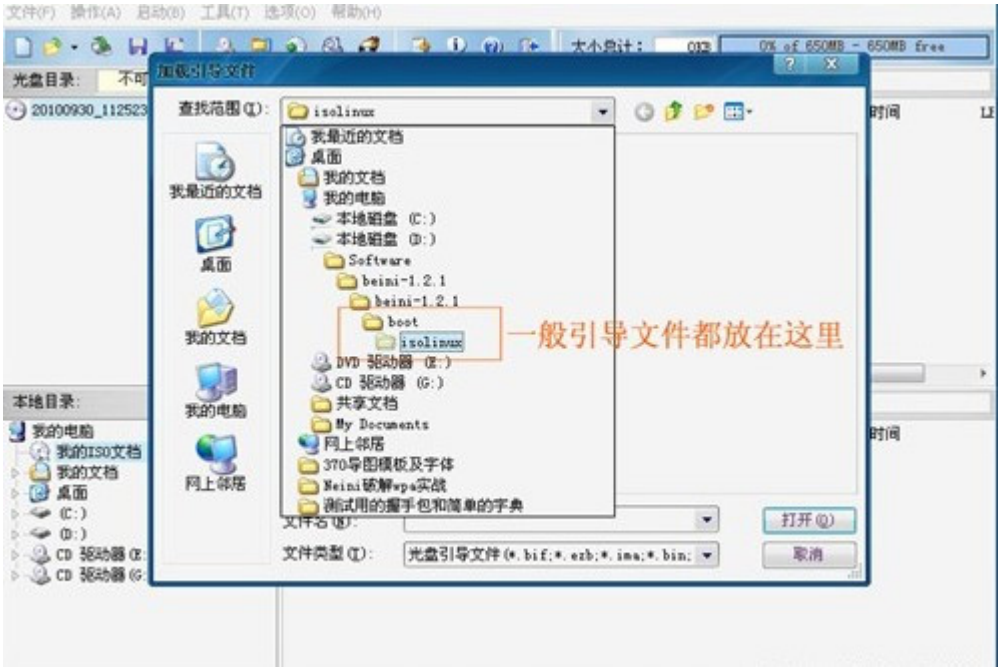


写入速度很快，一分钟不到



加载引导文件

但是有时候选择直接写入之后，电脑并不能成功从 U 盘启动“奶瓶”。因此如果制作不成功之后，我们还需要选择手工加载引导文件。



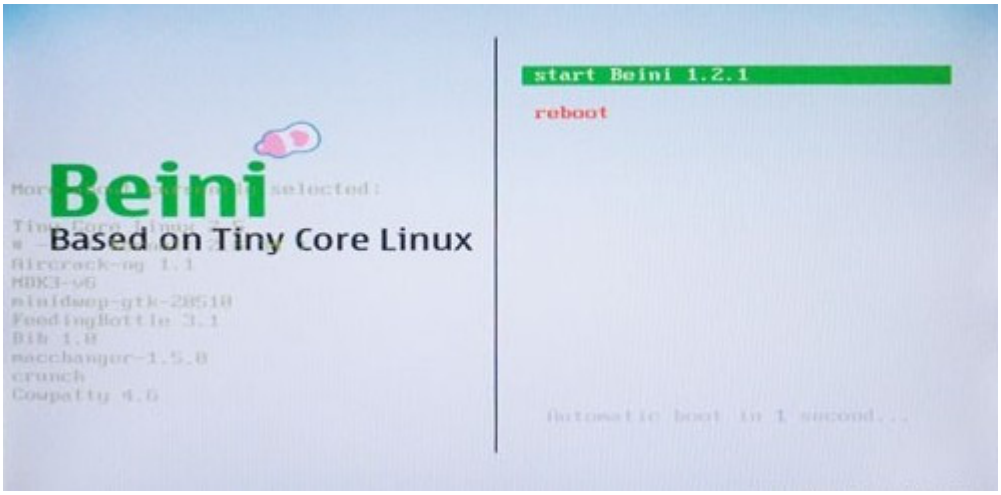
引导文件位置

我们首先需要将下载的“奶瓶”的.iso 文件解压缩，然后在如上图所示的目录中找到引导文件，然后再进行加载，如此操作之后，再进行 U 盘的写入。

第 3 页：进入“奶瓶”系统

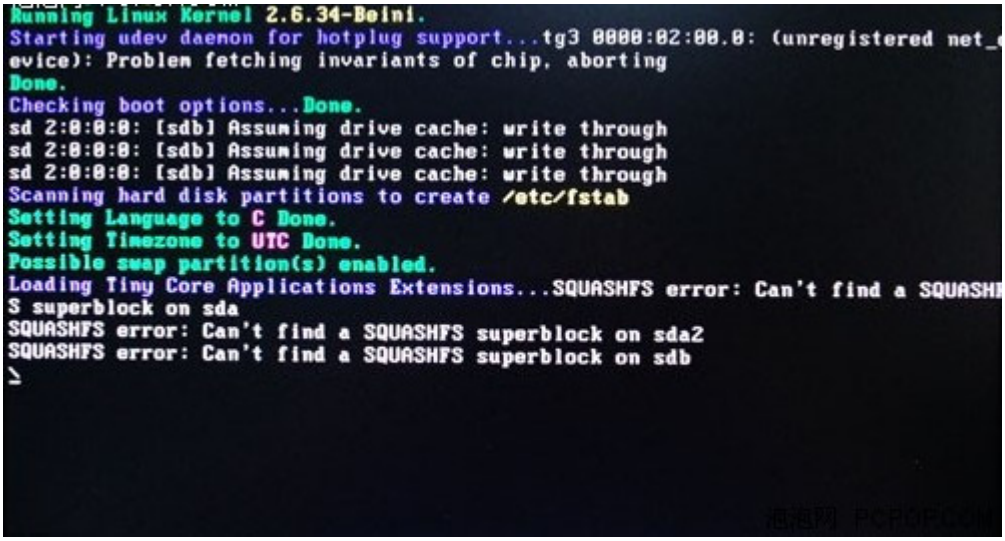
修改 BIOS 设置

重启电脑之后，按 DEL 键进入 BIOS 设置界面，在这里我们要选择从 U 盘启动，以让电脑从“奶瓶”系统启动。

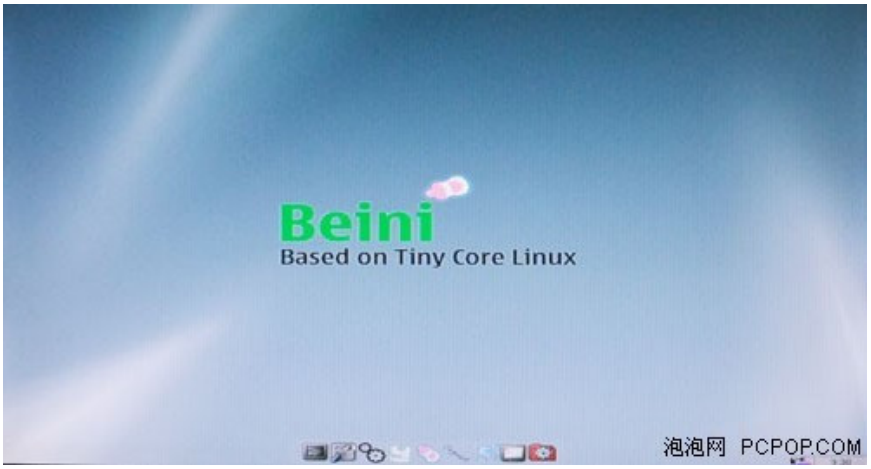


“奶瓶”的启动界面

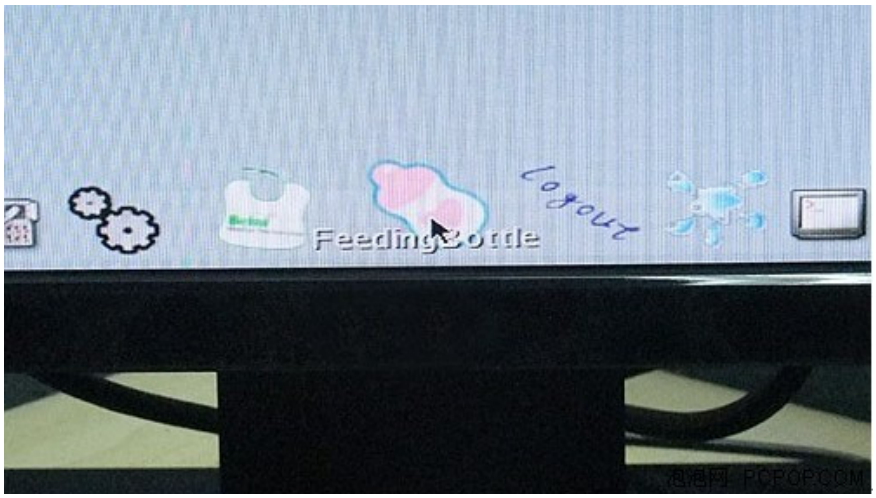
如果你能看到上面的这个画面，那 U 盘启动盘就制作成功了，稍后片刻，我们即可进入“奶瓶”中。



正在启动“奶瓶”



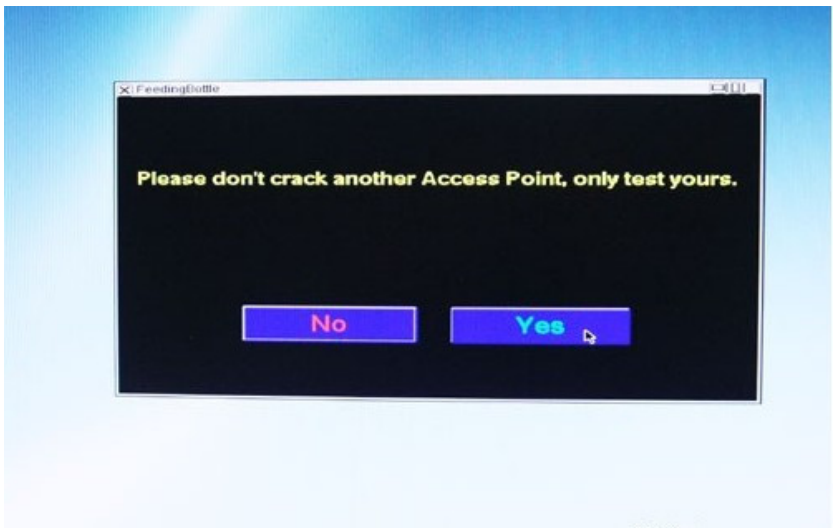
“奶瓶”的桌面，很清爽



点击位于最下端 Dock 上的“奶瓶”图标，即可开始我们的破解旅程

第 4 页：扫描网络信号

通常在我们的周围，都会同时开着很多台路由器，因此我们的电脑上也会显示多个连接信号。在“奶瓶”上搜索这些信号，则是一件非常简单的事情。



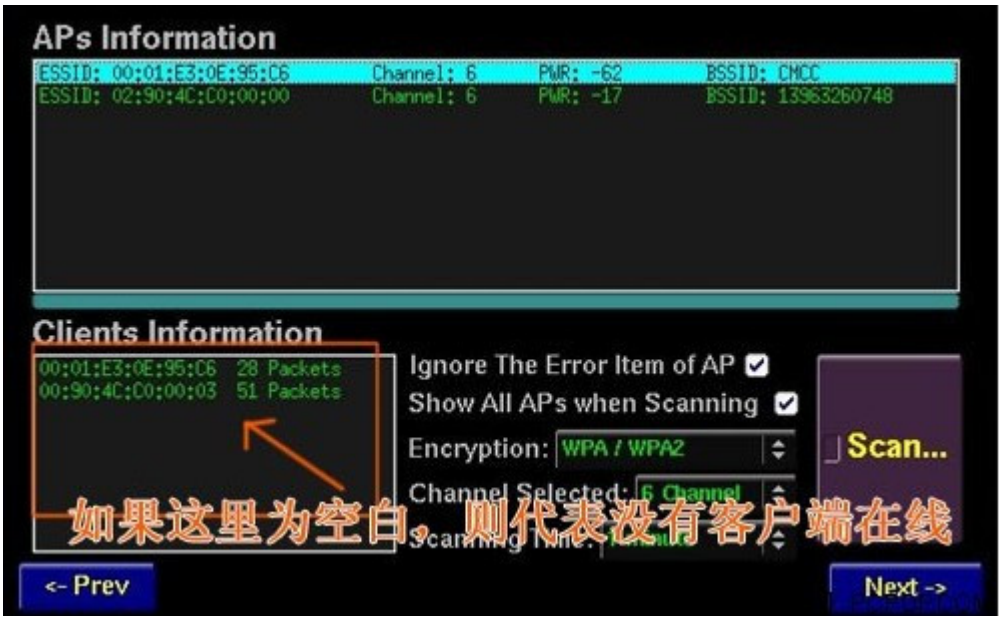
点击 YES，开始扫描

点击“奶瓶”图标之后，系统就会跳出上图这个界面，在这里点击 YES 按钮，即可启动网路信号扫描。

选择网卡之后，开始监听网络信号

画面中的 Encryption 选项可以选择加密类型

正在扫描网络



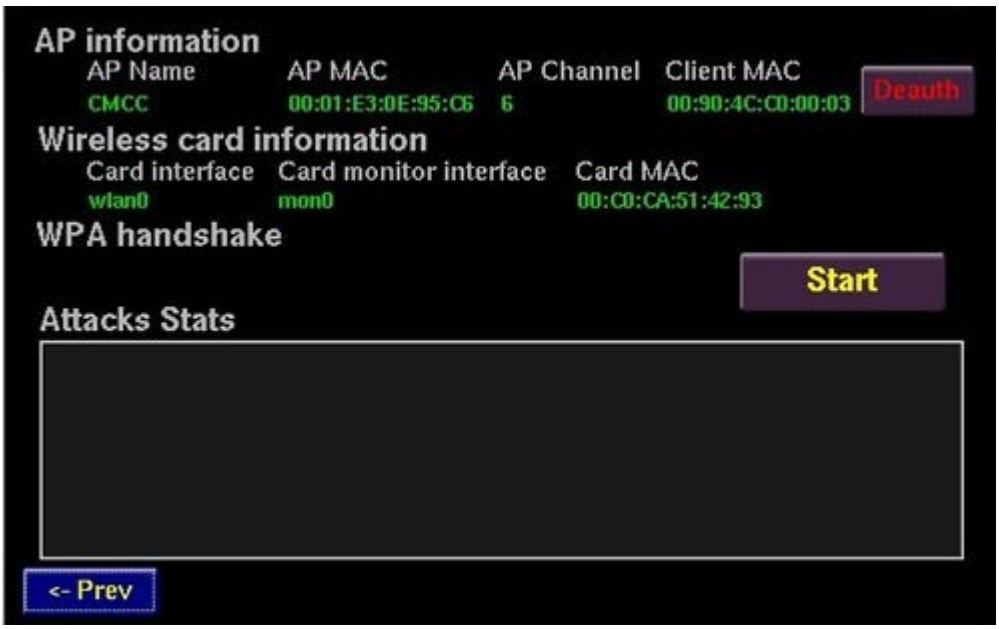
扫描完毕，搜索到两个无线网络

首先说一下客户端，这里说的客户端，即代表所扫描到的路由器正在通过客户端上网，因此我们完全可以向其发起攻击。而至于只有信号，而没有客户端在线的情 况，我们将在今后再抽时间来讨论。大家注意，由于 WEP 加密模式已经完全被破解掉，我所在的小区所能收到的网络信号，基本上都采取了 WAP/WAP2 的模 式，这点上大家都做的很好，只是，WAP/WAP2 也并不是完全安全的，让我们继续往下看。

当然，有客户端的情况下，还是非常容易破解的。如果真的没有客户端，记不起来是哪位网友说的话了：“没有耐心守候猎物的猎人不是一个好猎人。”这话不错，选择晚上进行守候，相信肯定会收获颇丰。

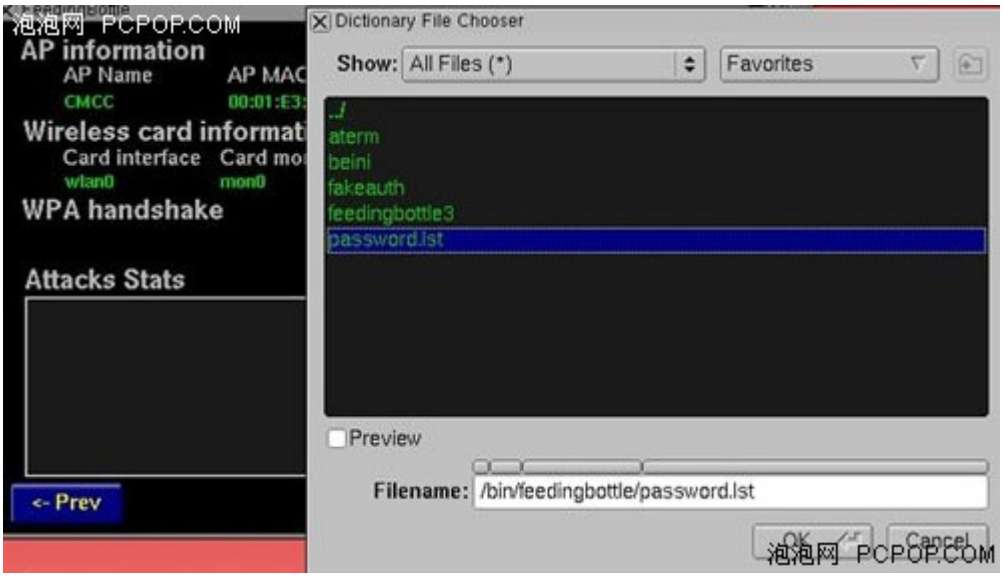
第 5 页：握手包，无线网络的死穴

先让我们来看一下什么是握手包。握手包就是网卡和路由器之间进行信息匹配验证的数据包，在这里面会含有无线网络的密码信息，因此，我们只要抓取到对方网络的握手包，那么破解密码也就只是一个时间问题了。

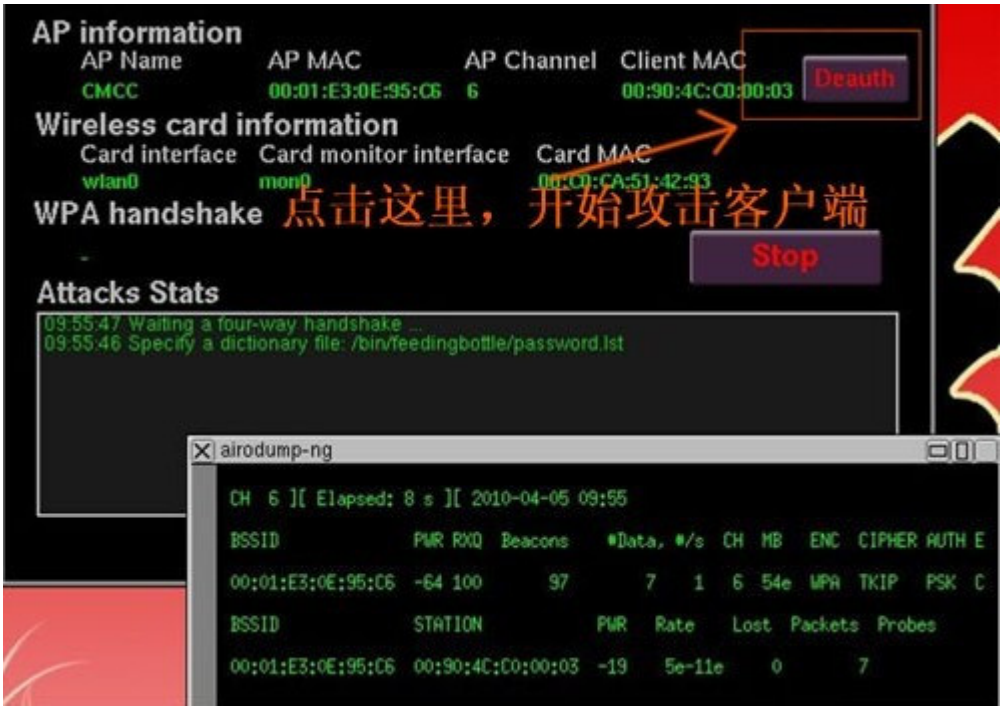


“奶瓶”的抓包界面

扫描完毕之后，我们点击 NEXT 按钮，即可进入到抓包界面。在图右上角的 Client MAC 则是我们将要进行抓包客户端的 MAC 地址。点击 Start 按钮，让我们开始抓包。

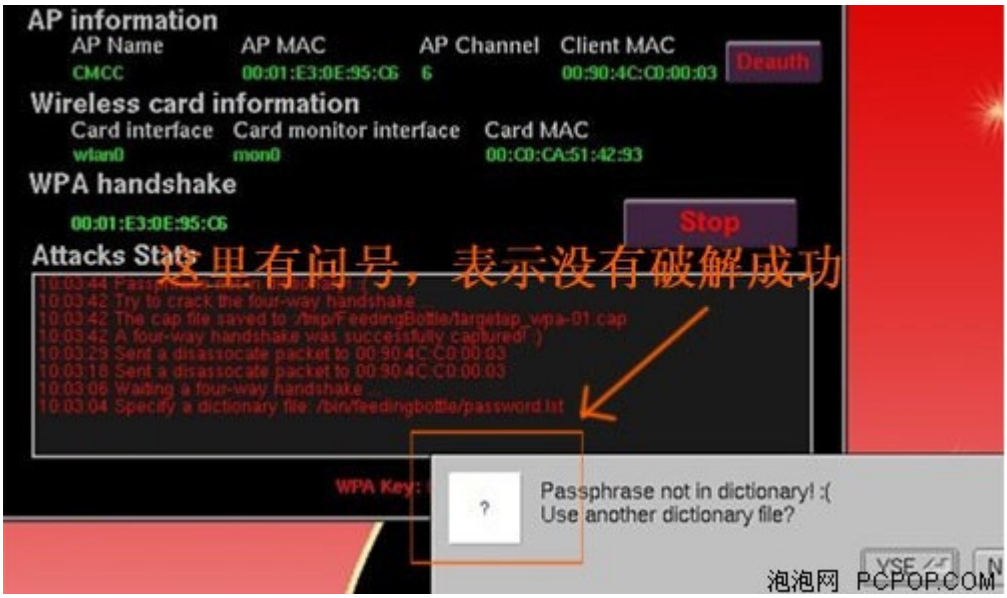


抓包之前，先挂好密码字典，一会抓到就能直接破解



点击 Deauth，攻击对方客户端

点击 Deauth 之后，系统就会对对方客户端发起攻击，迫使对方客户端和路由器断开链接。而当对方网络链接断开之后，路由器就会和客户端互传握手包，而 这正是我们需要的。抓取握手包是快慢，需要视我们与对方路由器以及 AP 之间的距离，信号越强，抓取成功越快，反之则越慢，甚至抓取不到。



自带密码字典没有破解成功

一般情况下，我们利用“奶瓶”自带的字典是破解不了所抓取的握手包的。因此，我们还需要将握手包导出，拿到 Windows 系统下，运用另外一款暴力软件进行破解。

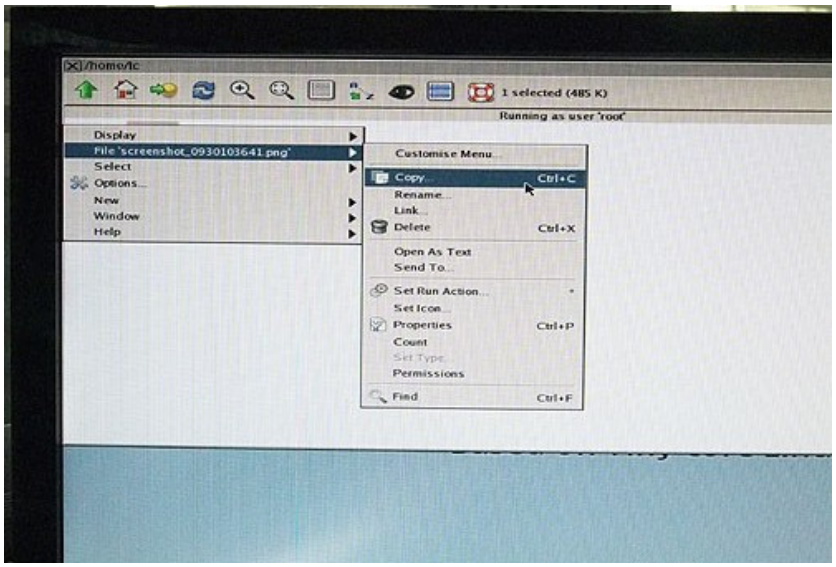
第 6 页：导出握手包

由于“奶瓶”是 Linux 系统，因此在文件的存储方式以及文件的操作方式上与我们日常的操作方法有着一定的不同。

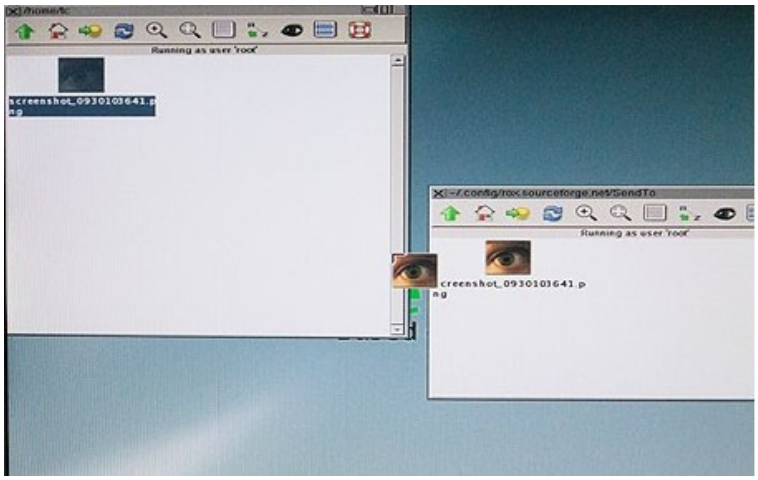
rox-filer 即相当于“我的电脑”

“奶瓶”中的磁盘列表

rox-filer 打开之后，点击左上角的绿色箭头，然后进入 mnt 目录之后，即可看到上图中的磁盘列表。只是由于没有明显的盘符现实，因此我们需要一个个去试了之后才能确定这些个图标分别对应哪个磁盘。

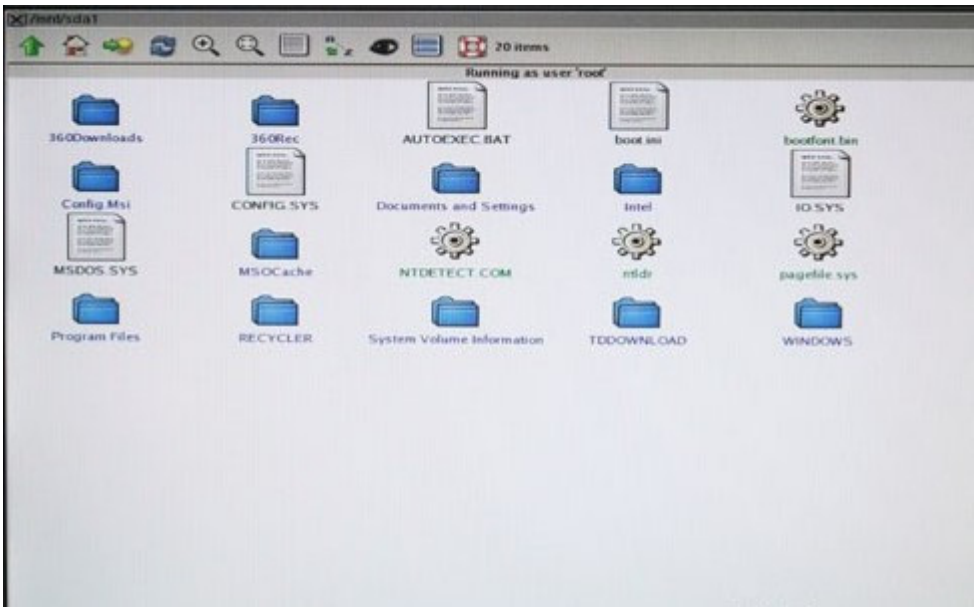


文件操作之：右键选择“COPY”



文件操作之：拖拽

文件的操作方式跟 Windows 下面一样，而我们抓取到的握手包的地址是：**rox-filer/tmp/feedingbotlle/targe/xxxxx.cap** 握手包文件是以.cap 为后缀名。



“奶瓶”下浏览 Windows 系统文件

握手包我们可以将其导入 U 盘中，也可以直接放到 Windows 系统文件夹中。然后，我们就重启电脑，进入 Windows 中，另一位主角将要登场。

第 7 页：EWSA 暴力破解机器

好了，终于回到了熟悉的 Windows 中，让我们请出另外一位主角吧，这就是来自俄罗斯的 Elcomsoft Wireless Security Auditor，简称 EWSA。

软件支持中文

导入抓到的握手包

GPU 的加入，让运算速度更快

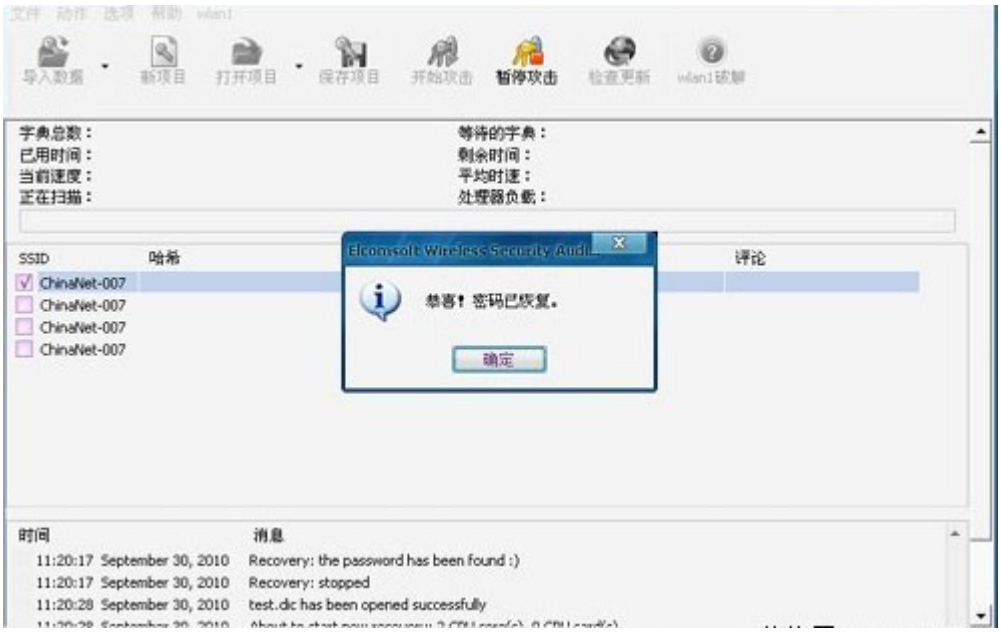
这款软件号称可以利用 GPU 的运算性能快速攻破无线网络密码，运算速度相比使用 CPU 可提高最多上百倍。它的工作方式很简单，就是利用词典去暴力 P 解无 线 AP 上的 WPA 和 WPA2 密码，还支持字母大小写、数字替代、符号顺序变换、缩写、元音替换等 12 种变量设定，在 ATI 和 NVIDIA 显卡上均可使用。

选择需要破解的握手包

加载字典文件

想要顺利的破解握手包，一个好的字典文件是必选的。好在目前网络上优秀的字典文件很多，因此我们在破解的时候有着多种多样的选择。不过总结下来，这些字 典文件无外乎以下几种：生日、单词、常见人名、纪念日、数字。因此，只要我们在设置密码的时候可以绕开这些字典文件的范围，那我们的网络安全性将得到极大 的提升。

开始破解，时间根据密码的复杂性以及字典文件的大小来决定


文件 动作 选项 帮助 wlan1
导入数据
新项目
打开项目
保存项目
开始攻击
暂停攻击
检查更新
wlan1破解
字典总数：
已用时间：
当前速度：
正在扫描：
等待的字典：
剩余时间：
平均时速：
处理器负载：
SSID
哈希
评论
ChinaNet-007
ChinaNet-007
ChinaNet-007
ChinaNet-007
Elcomsoft Wireless Security Audi...
恭喜！密码已恢复。
确定
时间
消息
11:20:17 September 30, 2010 Recovery: the password has been found :)
11:20:17 September 30, 2010 Recovery: stopped
11:20:28 September 30, 2010 test.dic has been opened successfully

破解完成


文件 动作 选项 帮助 wlan1
导入数据
新项目
打开项目
保存项目
重新启动 attack
暂停攻击
检查更新
wlan1破解
字典总数：
已用时间：
当前速度：
正在扫描：
等待的字典：
剩余时间：
平均时速：
处理器负载：
SSID
哈希
密码
状态
评论
ChinaNet-007
19760810
找到
ChinaNet-007
ChinaNet-007
ChinaNet-007
密码在这里
时间
消息
11:20:17 September 30, 2010 Recovery: the password has been found :)
11:20:17 September 30, 2010 Recovery: stopped
11:20:28 September 30, 2010 test.dic has been opened successfully