每天都能看到有不少网友在回复论坛之前发布的一篇破解 WiFi 密码的帖子，并伴随各种疑问。今天流云就为大家准备一篇实战型的文章吧，详细图文从思维 CDlinux U 盘启动到中文设置，如何进行路由 SSID 扫描、WPA 密码类型该如何破解、字典该怎样做（WEP 加密的密码貌似可以直接破解不用字典）效果比 BT8 要强悍很多！这是一篇详细介绍 WiFi 密码破解的文章，准备好了吗？

好了，先说下提前要准备的东东吧：

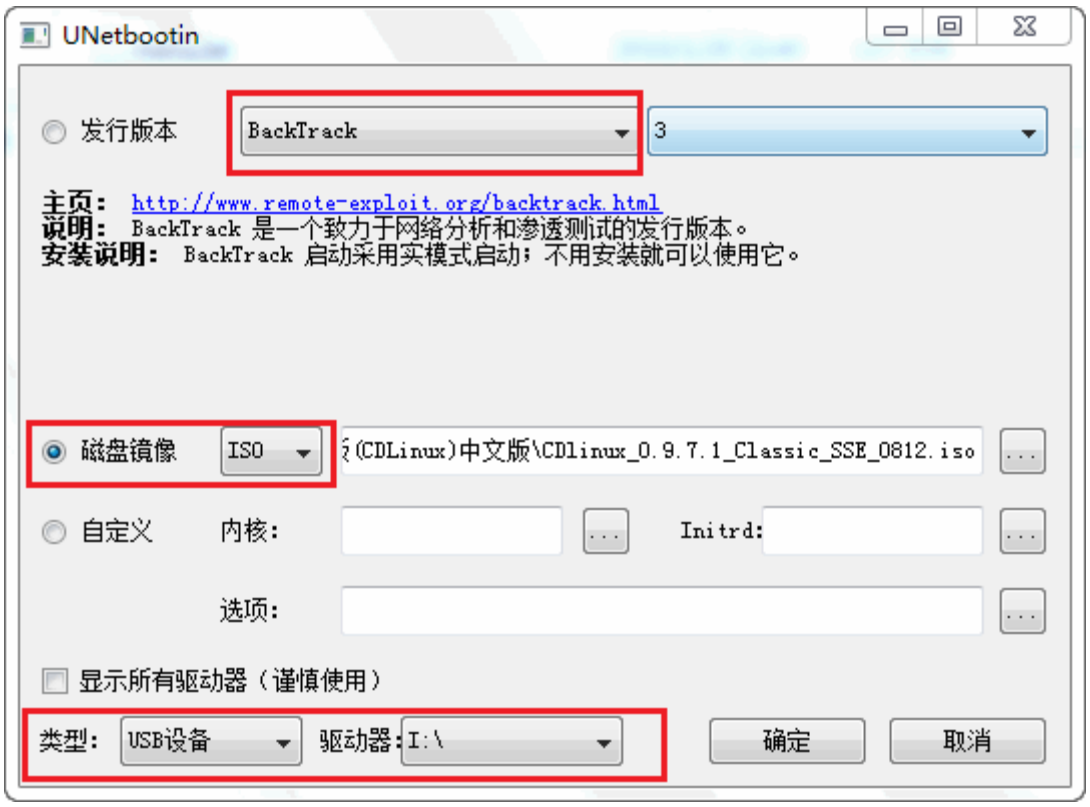
1、U 盘一枚，最小 1G 空间。需进行格式化操作，提前保存内部文件。

2、CDlinux 镜像。我会提供一枚 8 月最新修改版，共 135M。

1、CDlinux U 盘启动

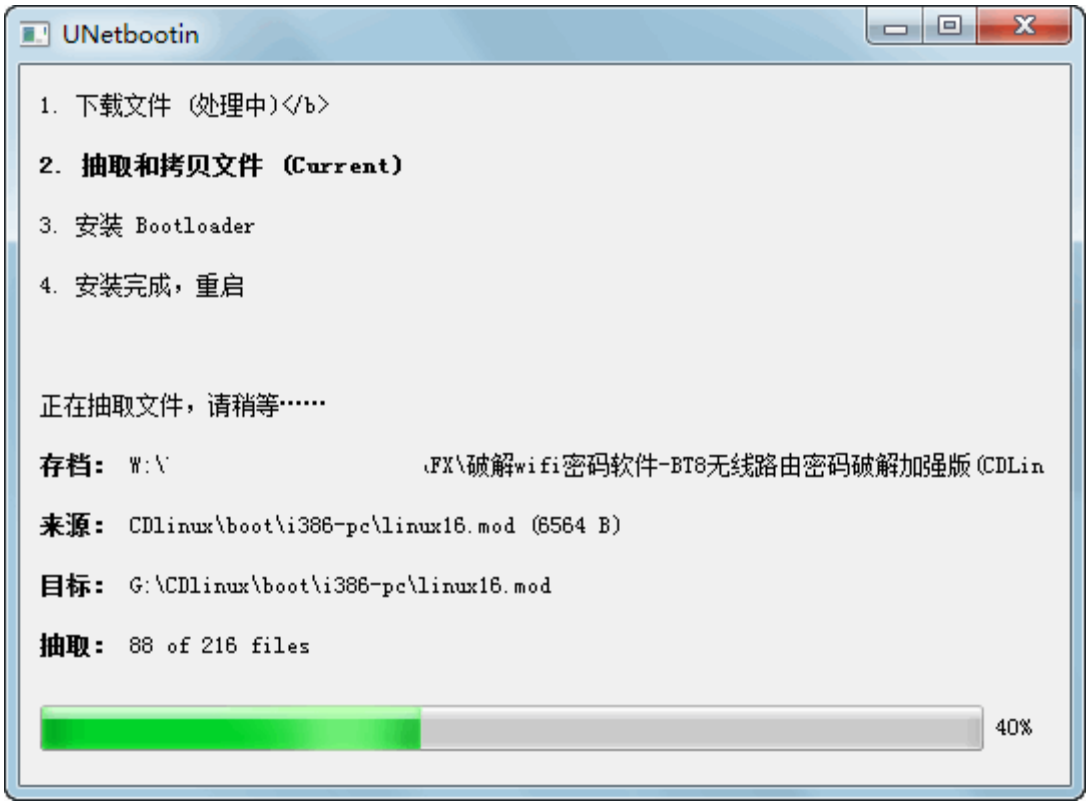
在这一步上废了不少功夫，因为 CDlinux 不支持内置网卡在虚拟机中进行破解，如果你的机器上有外置网卡的话，后面会提供一种方法来介绍该如何操作！

经过测试了 grub 等各种方法之后，感觉下面这个方法更适合大家，并且制作工具特别小巧，绿色免安装！特点就是利用它将 CDlinux 安装到 U 盘上。运行 Unetbootin 程序。按下图设置：

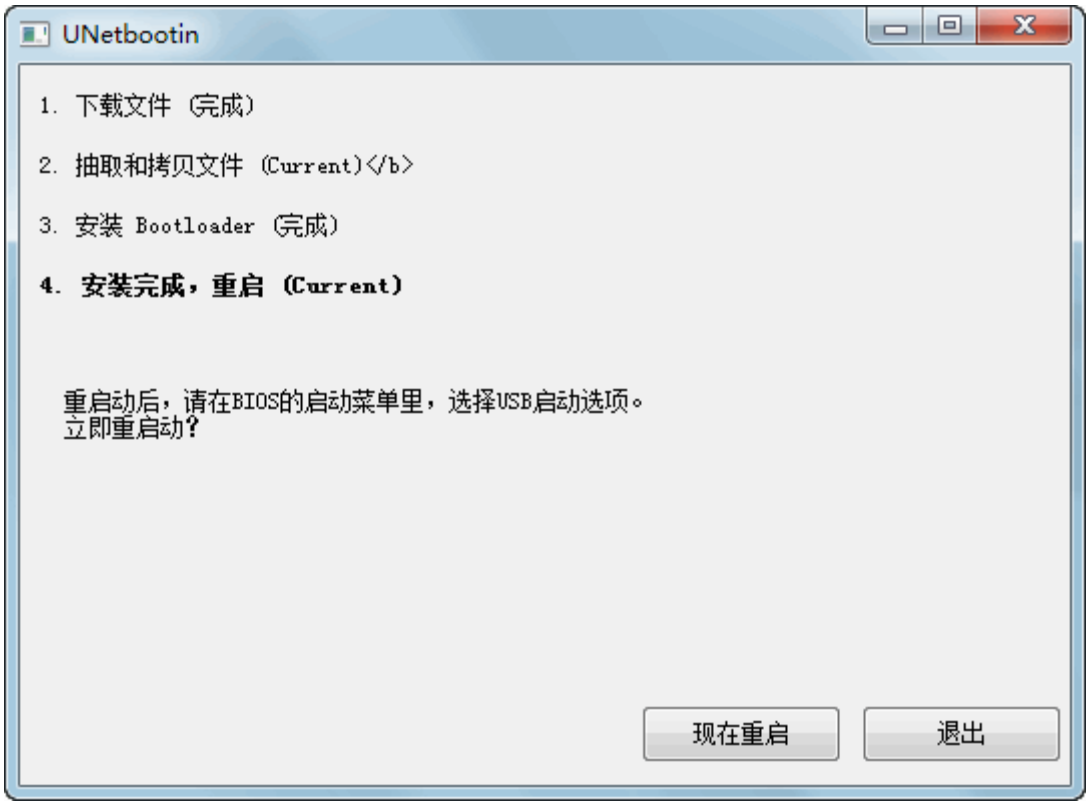


发行版本上选择 BackTrack，该版本就为适合我们的 CDlinux 运行环境，之后选择下载好的 CDlinux 镜像，最后选择我们的 U 盘盘符，记住别选错哈！

点击确定，程序开始制作，这些都是自动的，我们要做的只有等待就成了！



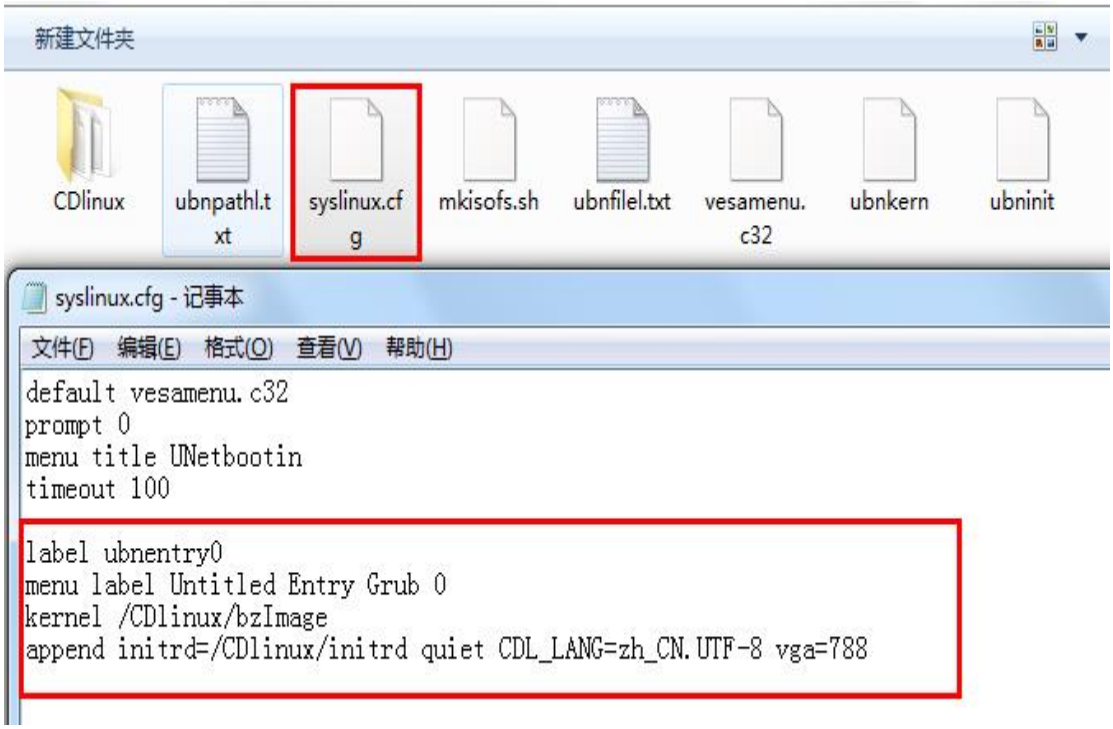
制作完成后，会提示重启，这里我们点退出。暂不重启。



2、中文语言设置

这点做成后启动的时候让我头疼了下，因为源镜像是多国语言的，经过上面的工作做完后自动进入了英语，跳过了选择项，所以我们需要设置下。设置方法很简单。

打开刚刚做好的 U 盘，找到下图 syslinux.cfg 文件，用记事本打开，将原有代码删除替换为红框内的。附件会提供文件下载，到时大家直接覆盖即可！

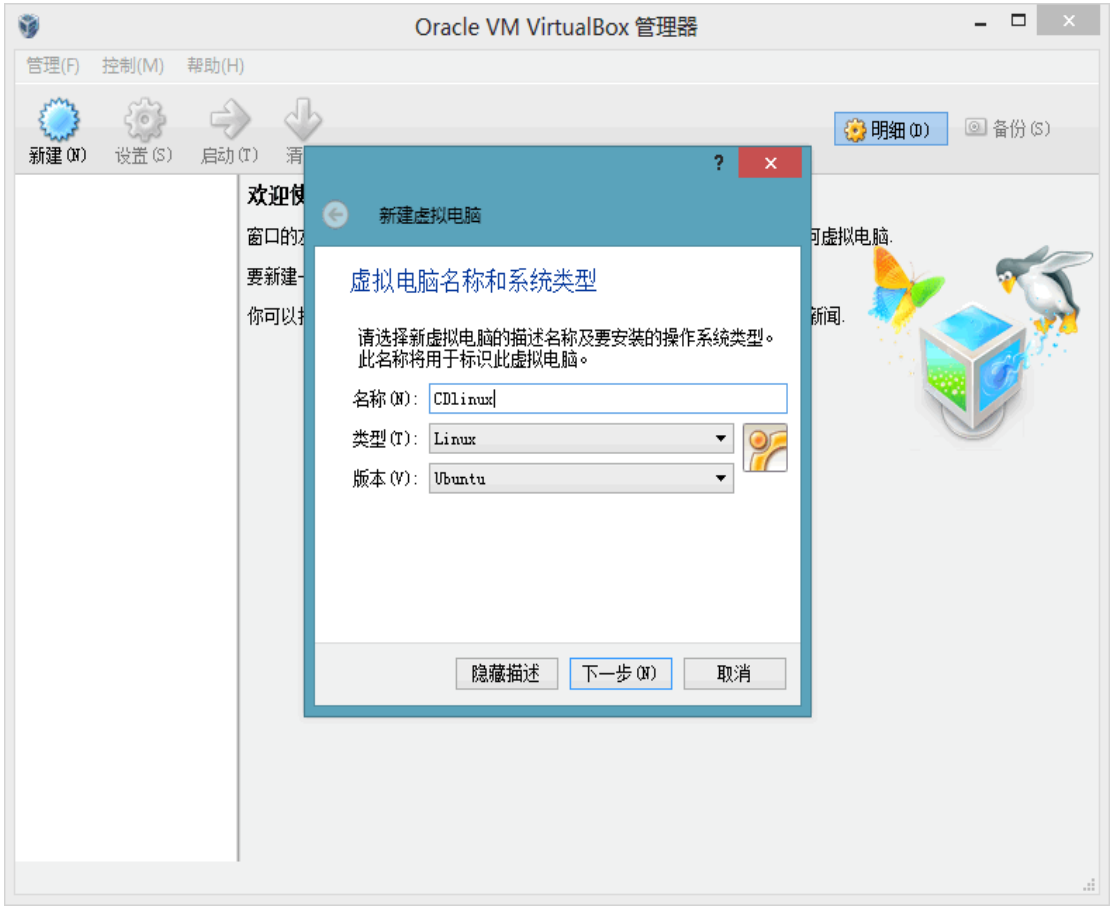


无外置网卡的朋友请直接跳过这一步

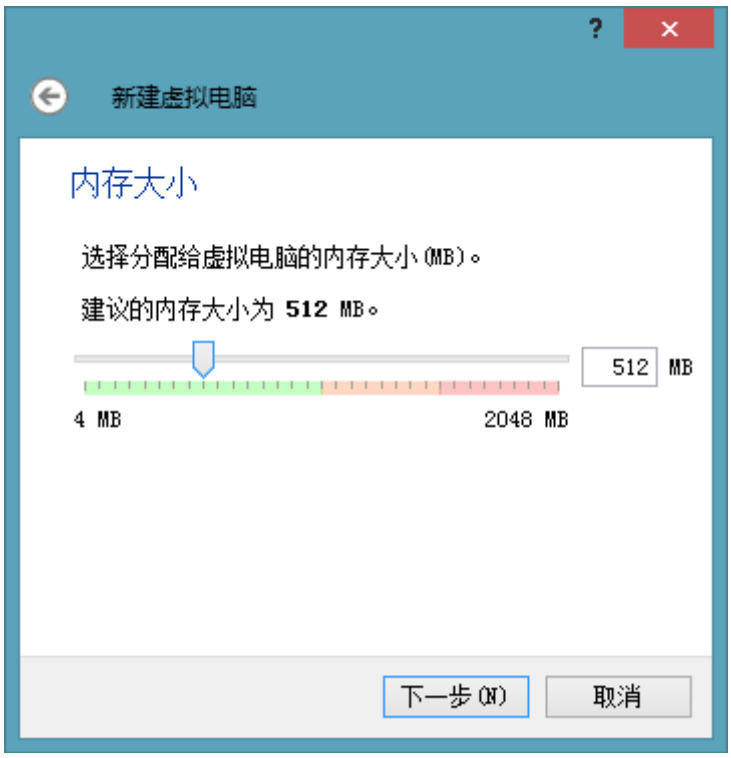
下面说下有外置无线网卡的朋友该怎样不做 U 盘的情况下来安装镜像：

首先我们需要一个虚拟机，这里以 VirtualBox 为例(点我下载)，不到 100m，多国语言，免费开源不用破解，附件都会提供的别急！

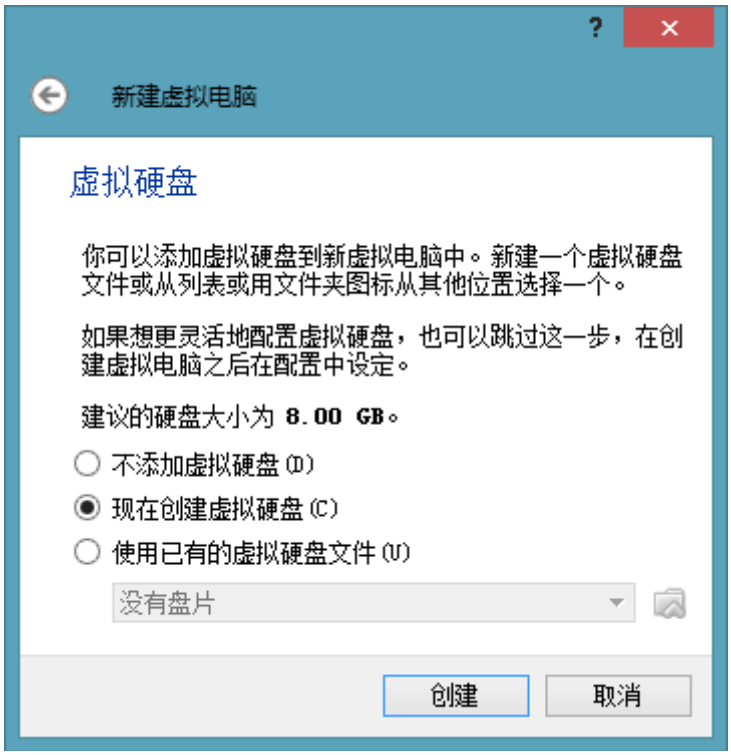
安装完之后（虽然安装界面是英文的），点击左上角的“新建”按钮，然后选择“类型”选择 Linux，名称随意，其他不用动。



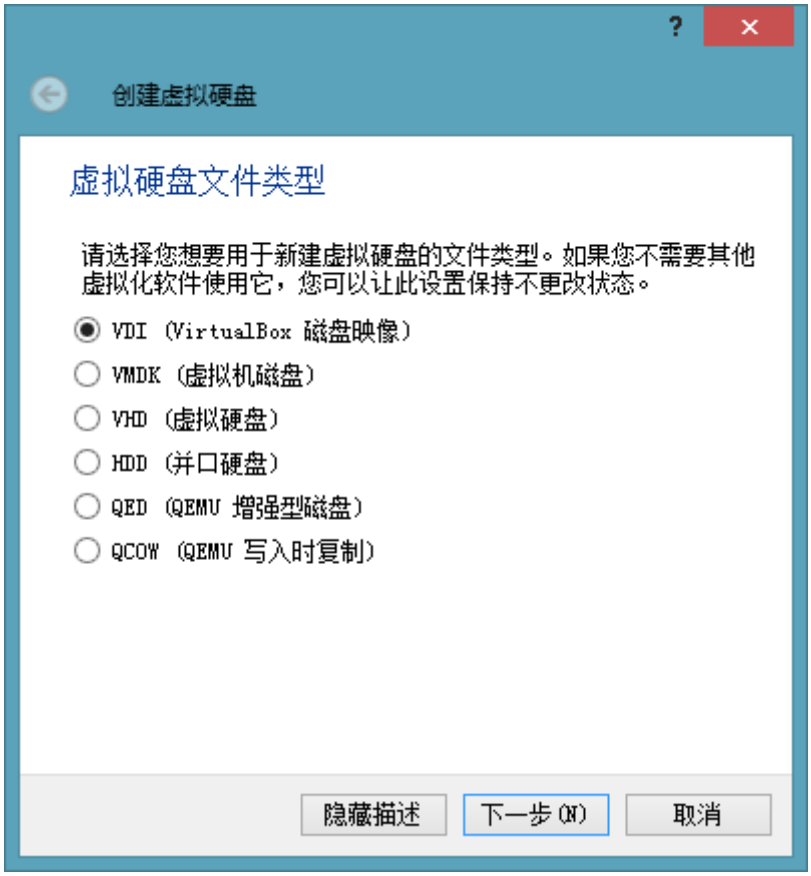
点击下一步，默认 512 足够了，继续下一步。



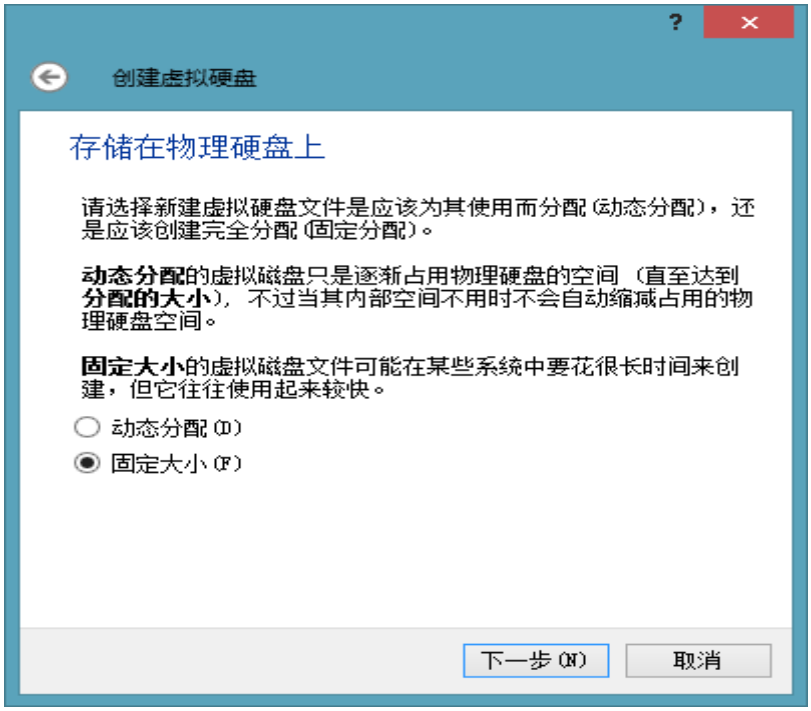
第一次用，按默认的创建虚拟硬盘。



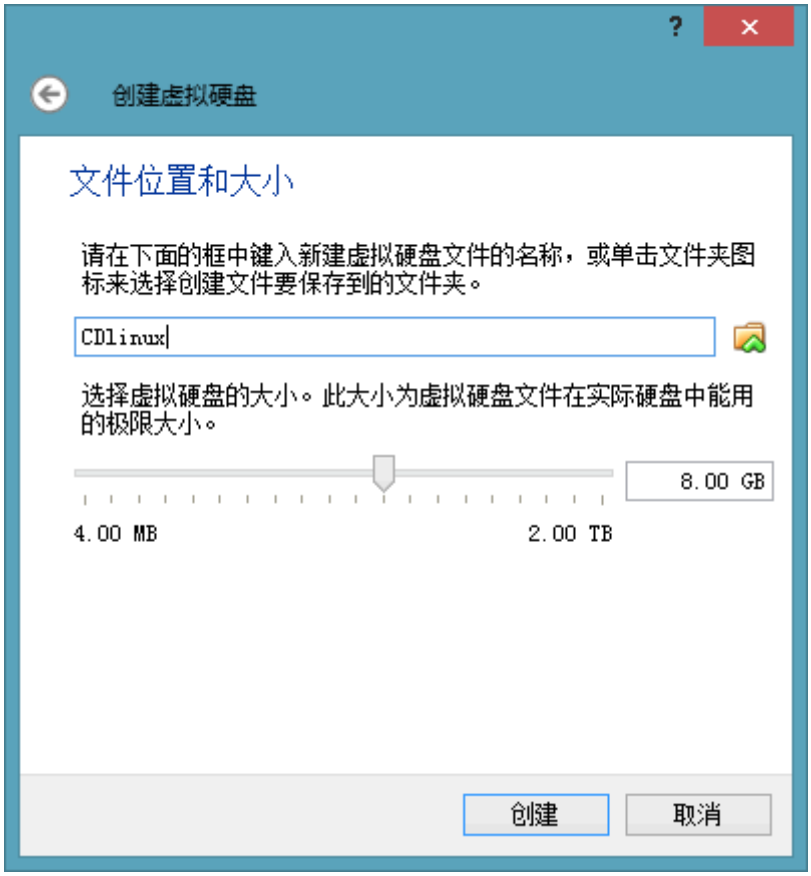
默认 VDI 类型。



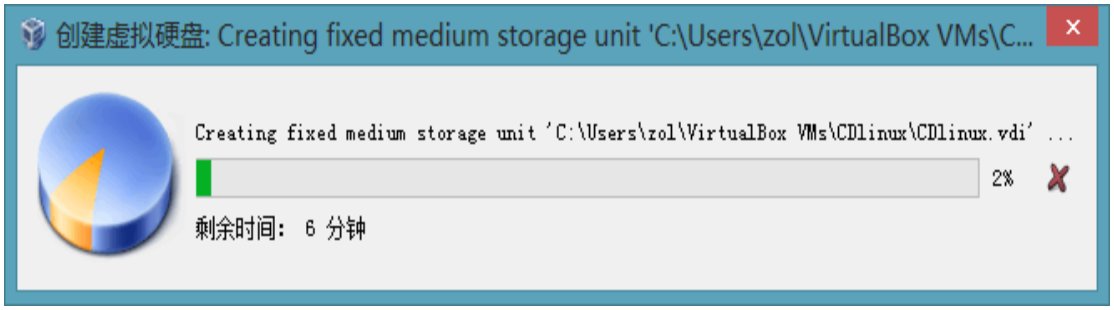
存在物理硬盘上的，建议选择“固定大小”。



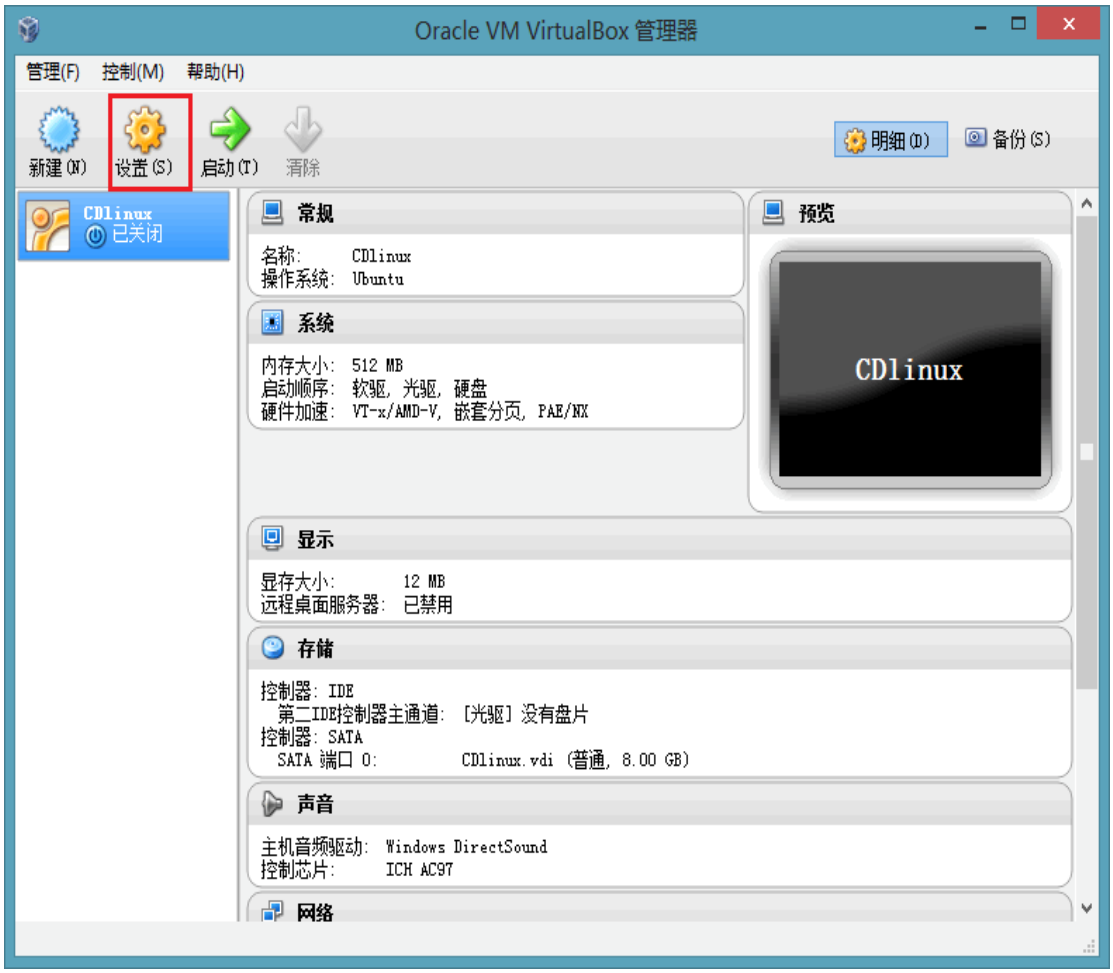
下面这一步是选择我们创建的 VDI 文件存放位置，默认存放虚拟机安装位置，这里需要设置的，点击文件夹图标更改即可。



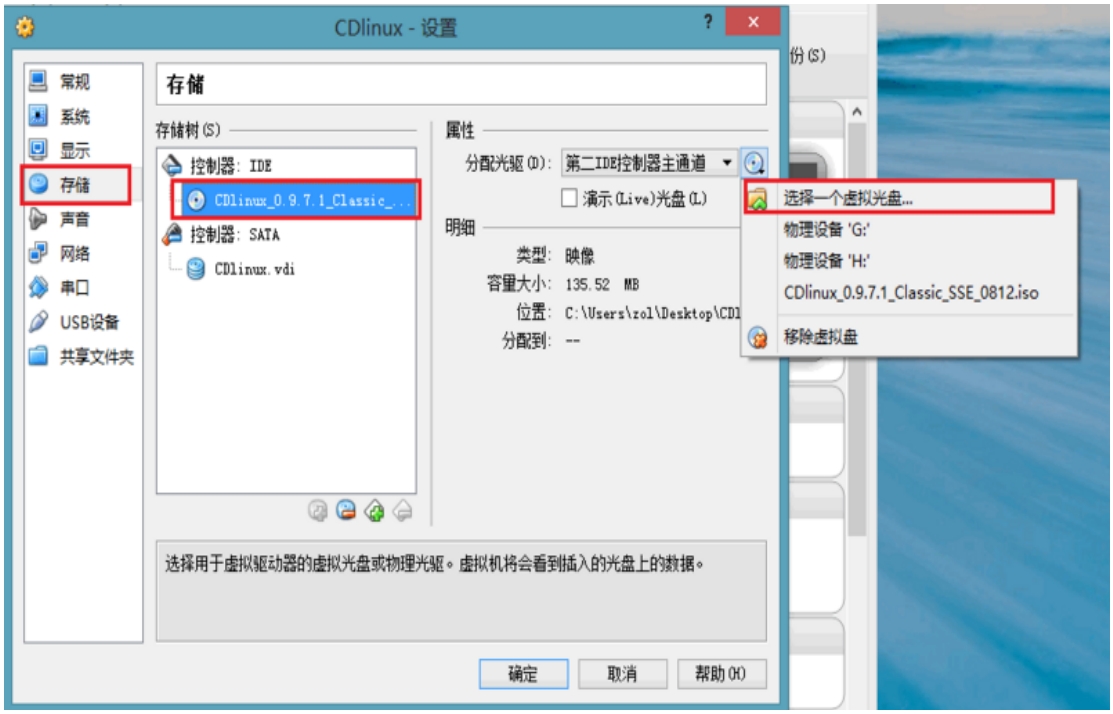
点击创建，虚拟磁盘就开始创建了。



稍等几分钟我们创建的 CDlinux 就出来了，点击左上角的设置。



在左边选择“存储”，控制器那选择此贴提供的镜像文件。

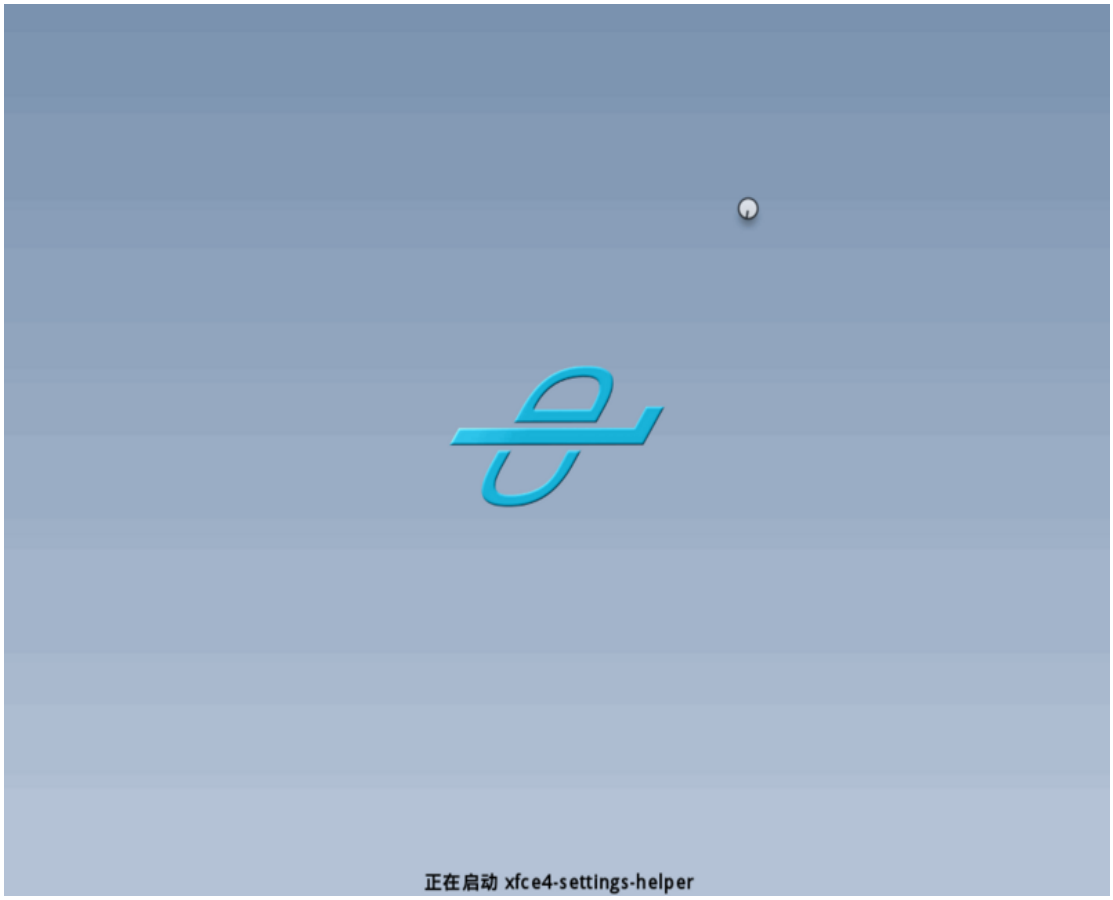


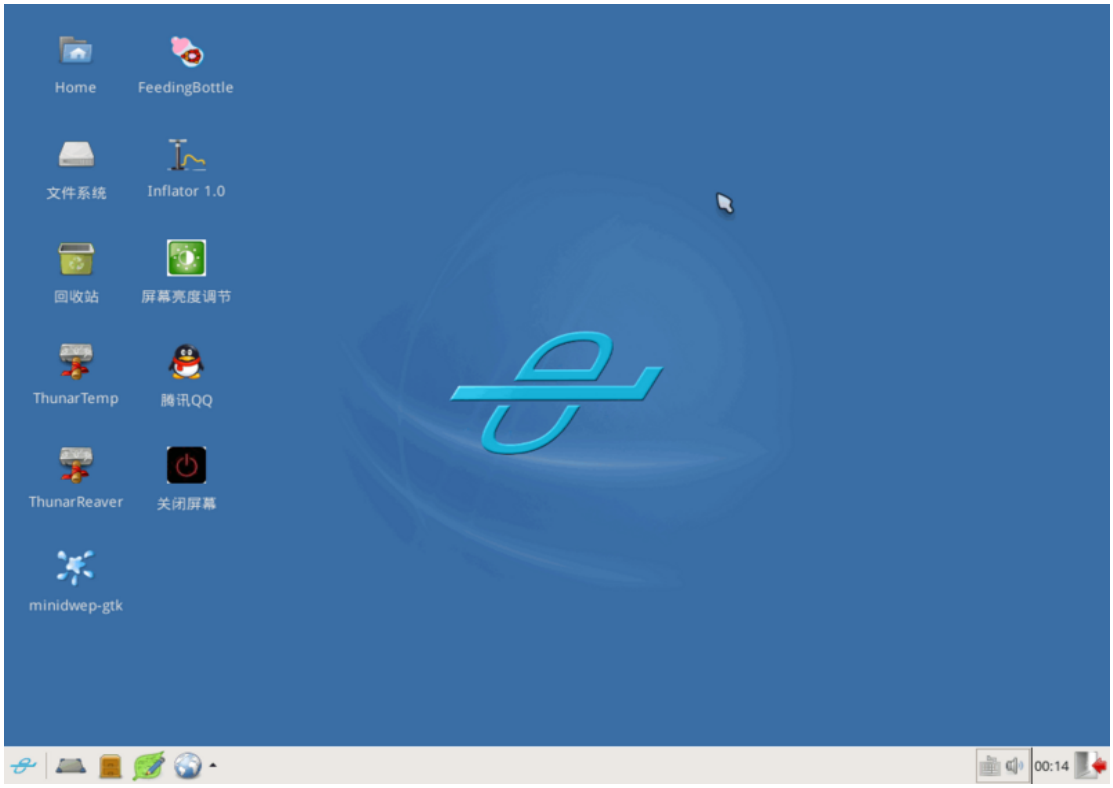
然后确定，回到主界面就可以启动了。

3、路由密码扫描

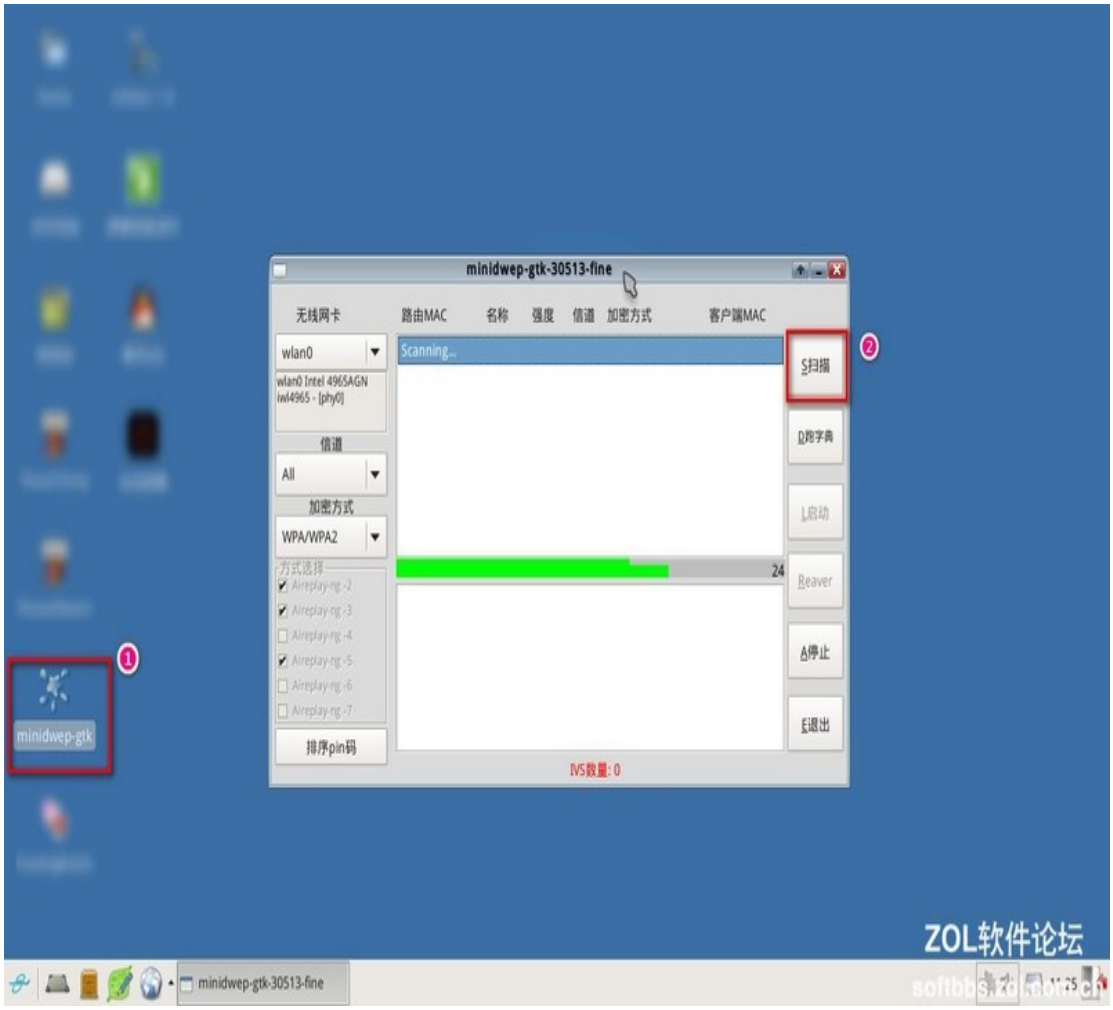
让没有外置网卡的朋友久等了。

我们将制作好的 U 盘插入电脑，修改 bios 为 U 盘启动：

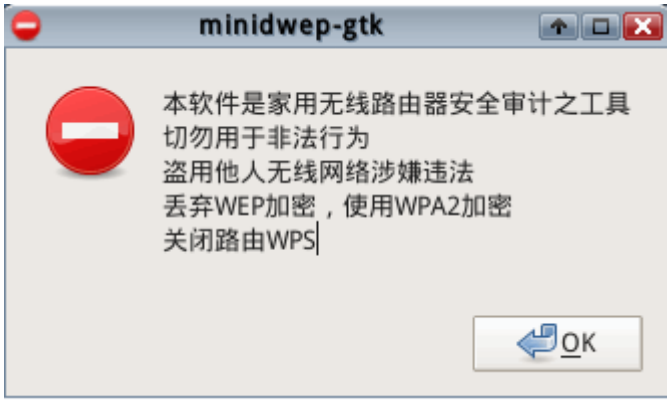




双击文件名为“minidwep-gtk”程序：

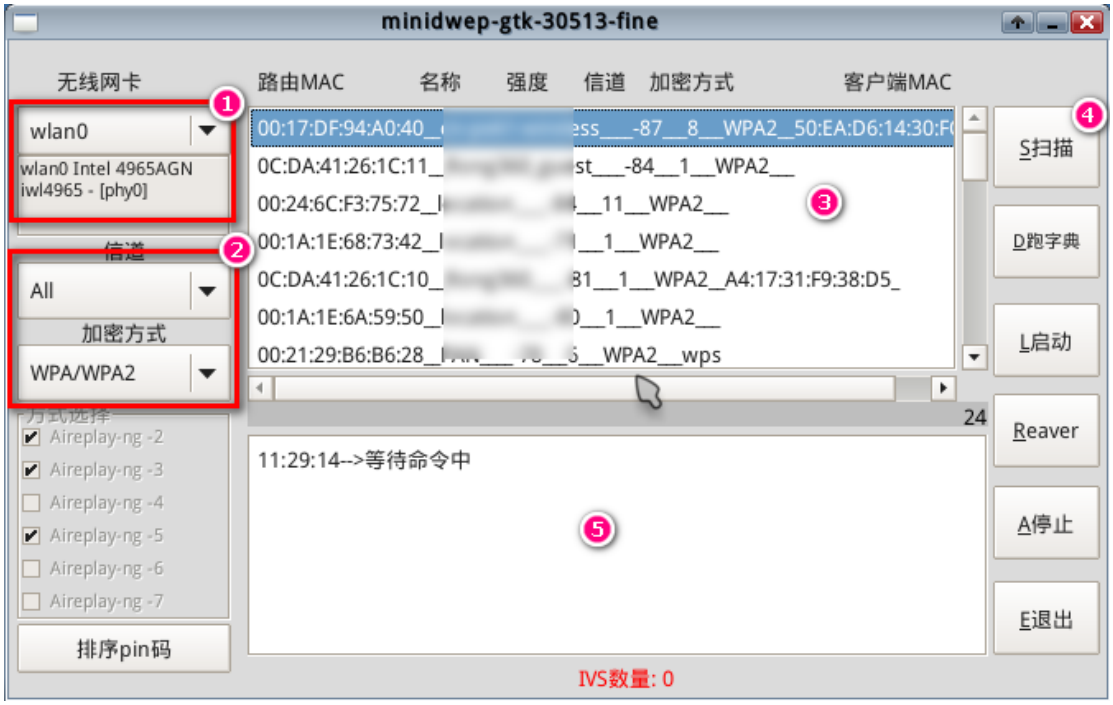


每次运行都会弹出一个提示窗口：



上面的说明，大家都懂的！切勿用于非法用户。。

下面详细介绍下该工具的主界面：



1）无线网卡 wlan0。这里显示自己的无线网卡信息。

2）信道，加密方式。信道就默认选 All 全部，加密方式分 WEP、WPA/WPA2 两种。下面的方式选择选择默认吧。

3）显示路由的 mac 地址、名称、强度、信道、加密方式等。

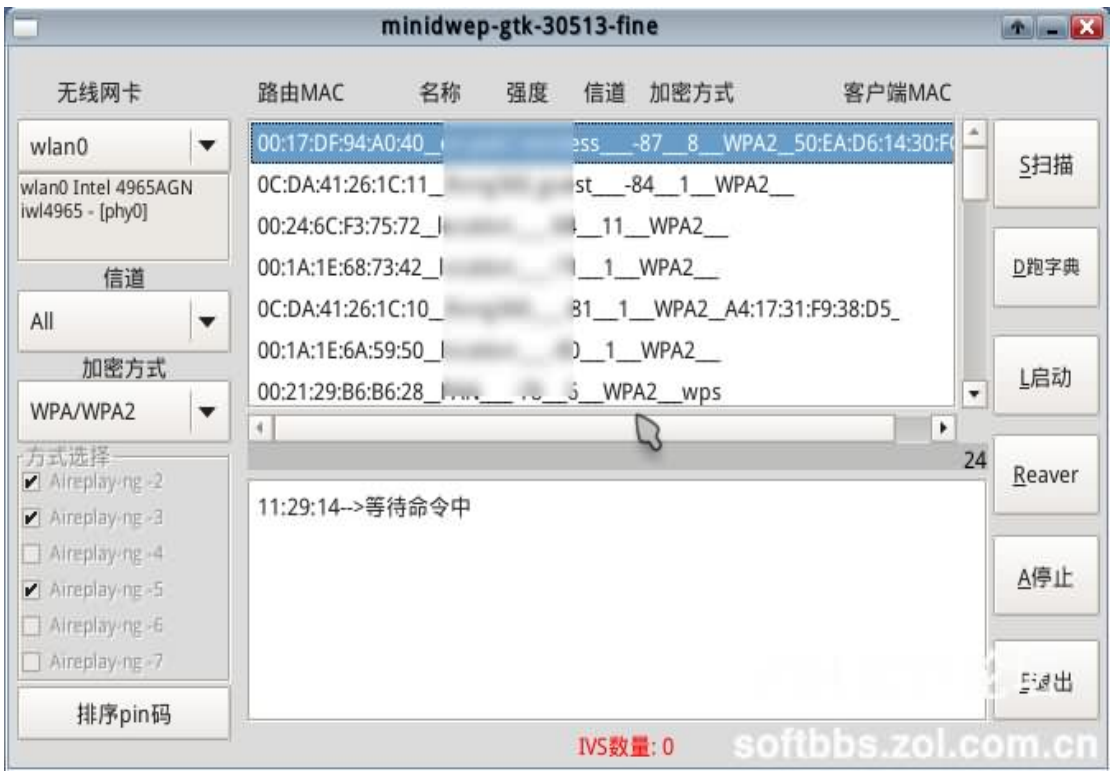
4）这一竖条都是功能按钮，点击实现相关功能。

5）这里扫描的时候相关状态进度显示。

看到界面之后，直接点上图 4 中的扫描按钮，就会看到中间的进度条再走了。

稍等片刻，就能看到路由的 MAC、名称、强度、信道、加密方式等。

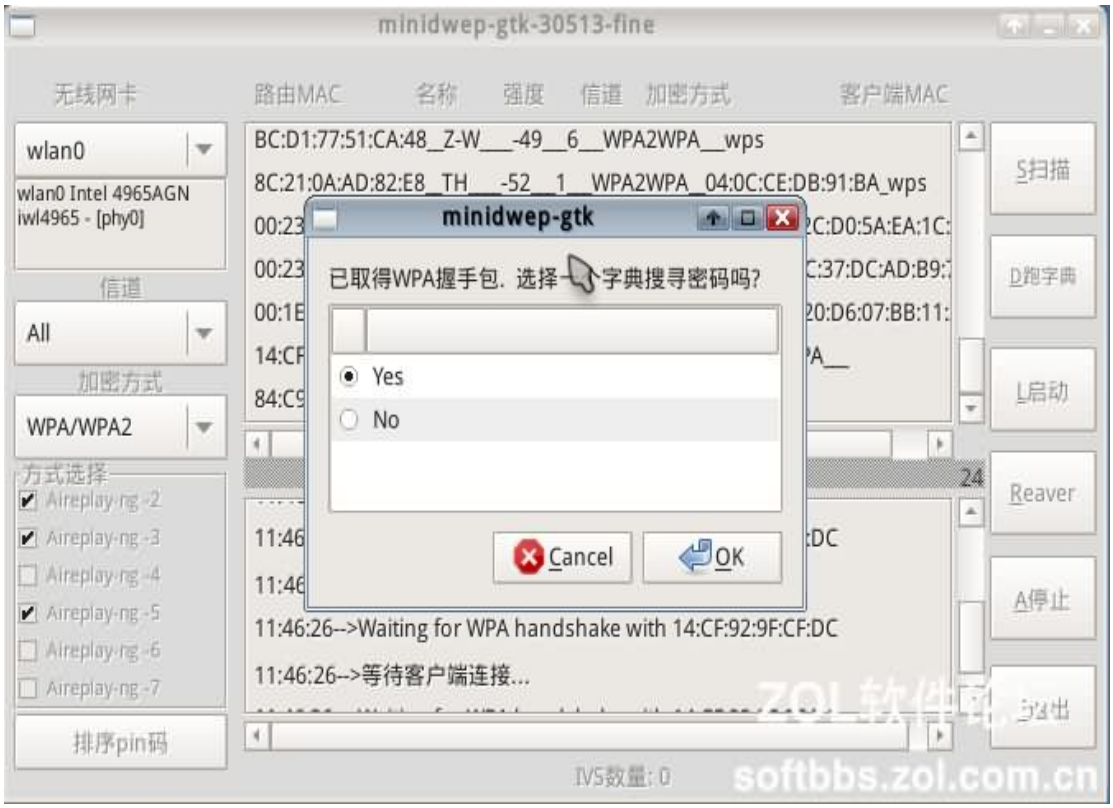
这里以加密方式为 WPA/WPA2 为例，WEP 后面再说（因为更容易破）。



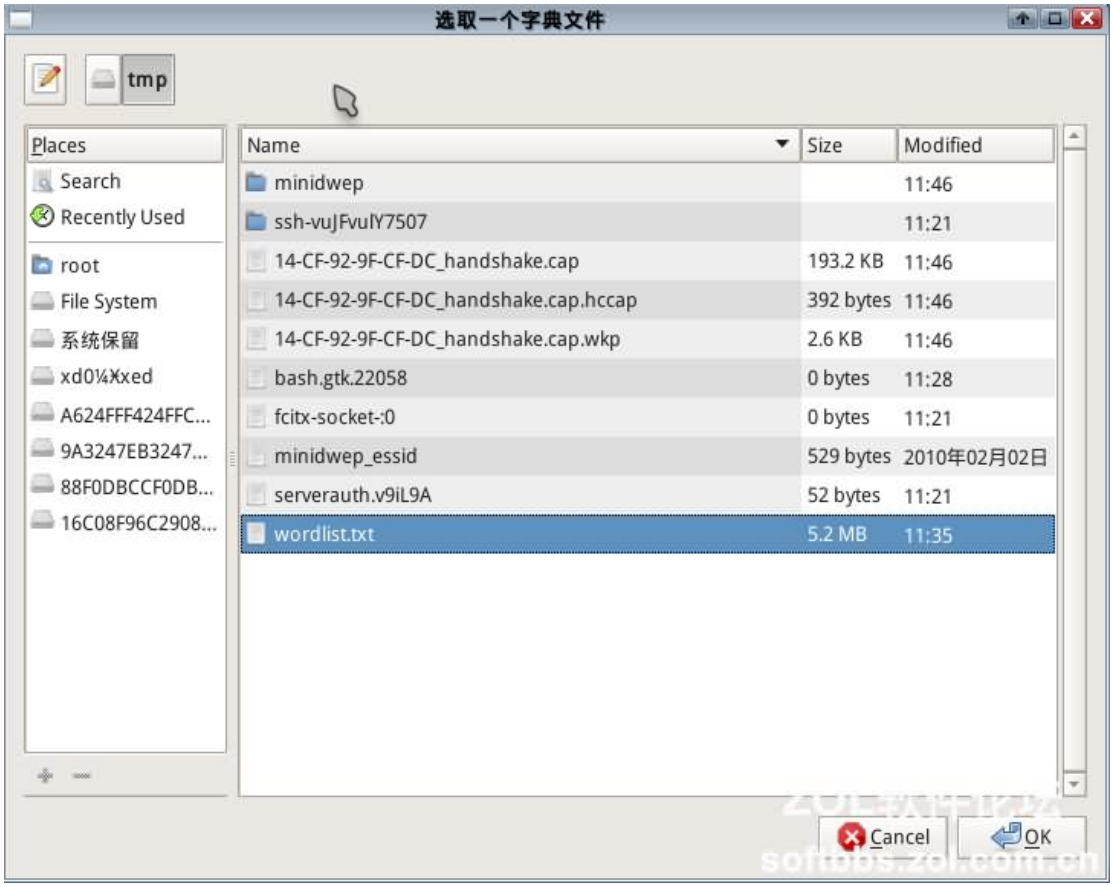
点击我们需要破解的路由名称，点右侧的启动，下放就会进行“握手”操作了，不停的与路由进行连接，这个过程是自动的，视路由及信号相关强度绝对时间的长短。

当“握手”成功后，就会你相关提示，看到下图，就说明我们离成功更进一步了。

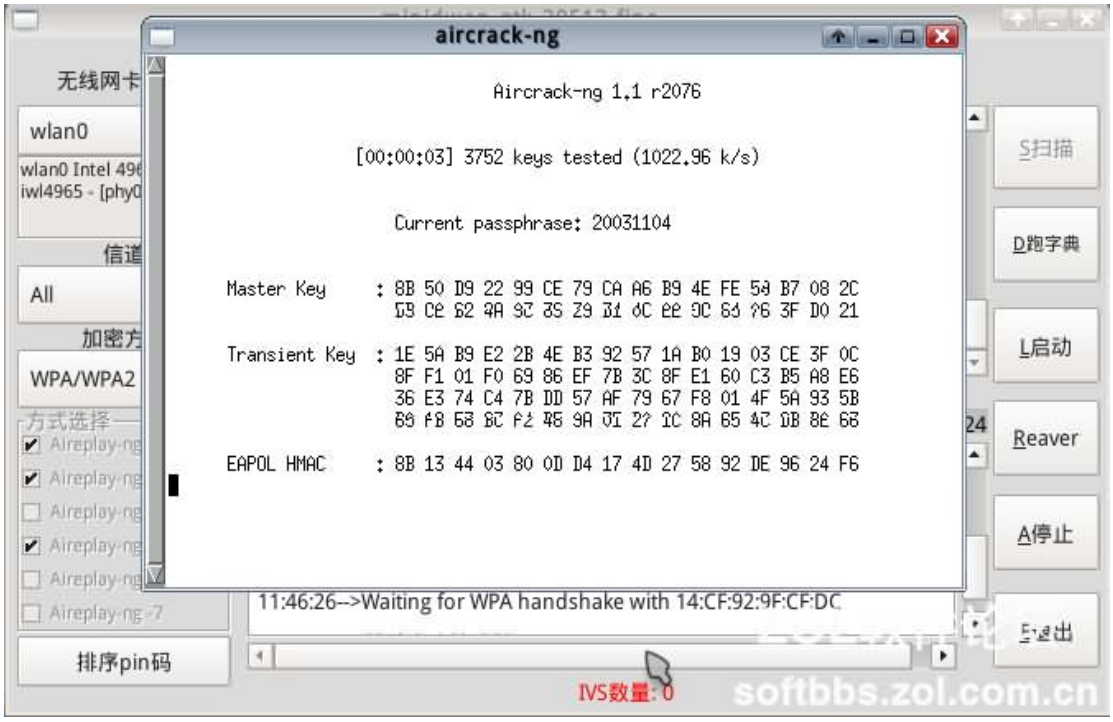
再稍等片刻，就会提示获取到握手包了。问我们是否选择一个字典来搜寻密码，点“Yes”之后再点“OK”。



选择弹出窗口中的“wordlist.txt”这个是此镜像附带的，选中点击右下角“OK”。

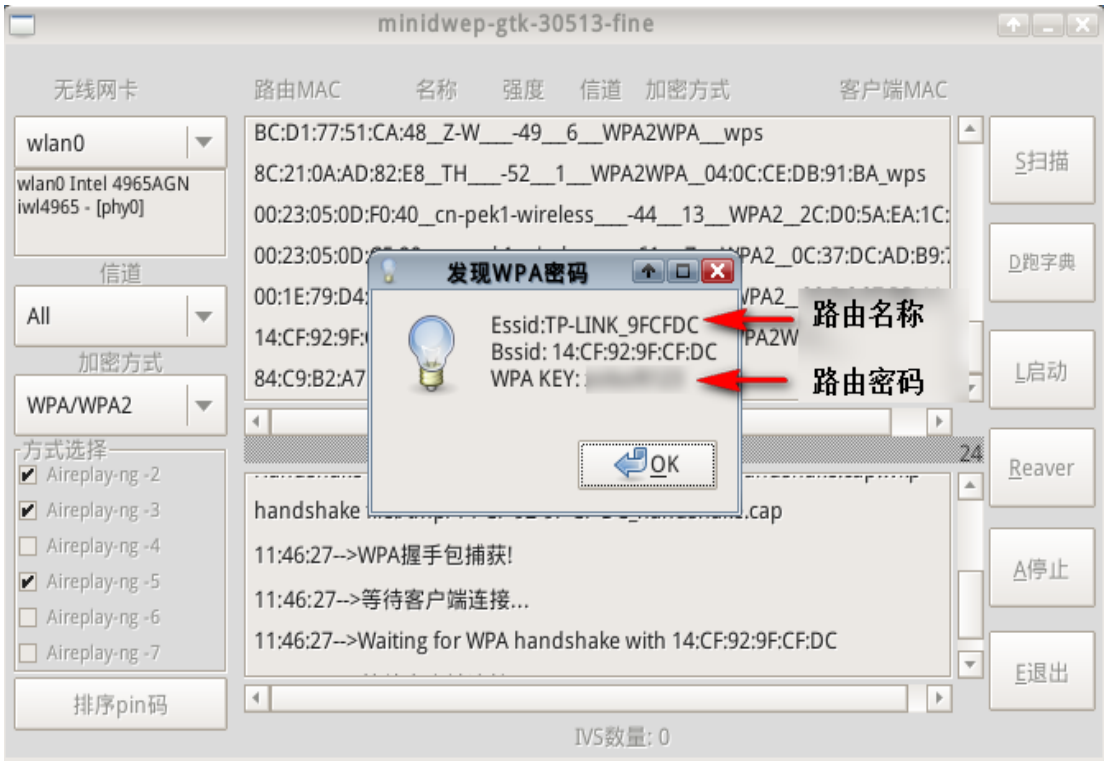


之后就是密码破解过程了，这个看运气和字典强度了。曾经有人分享给 3G 大小的密码包，按照这速度，一顿饭差不多能出结果了，如果不是特别 BT 的密码的话！

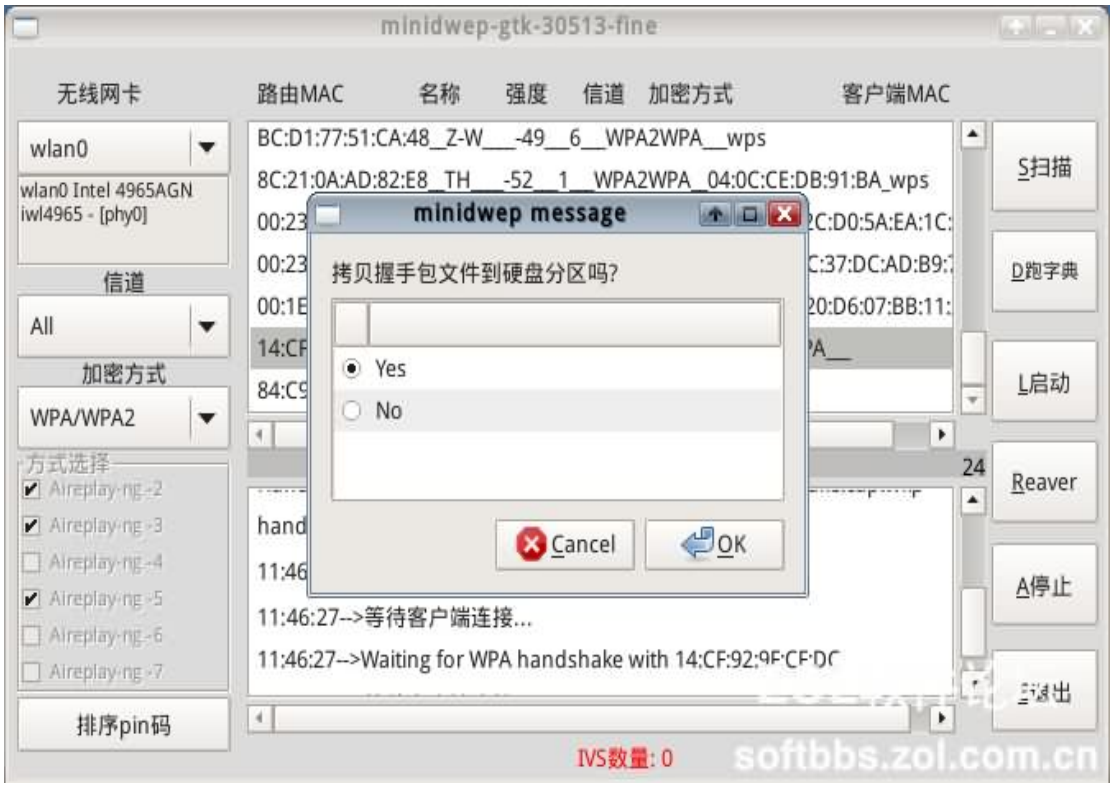


这次运气还算是比较好的，当软件自动扫描到密码后，会自动弹出的，这点真心赞一下！太人性化了！

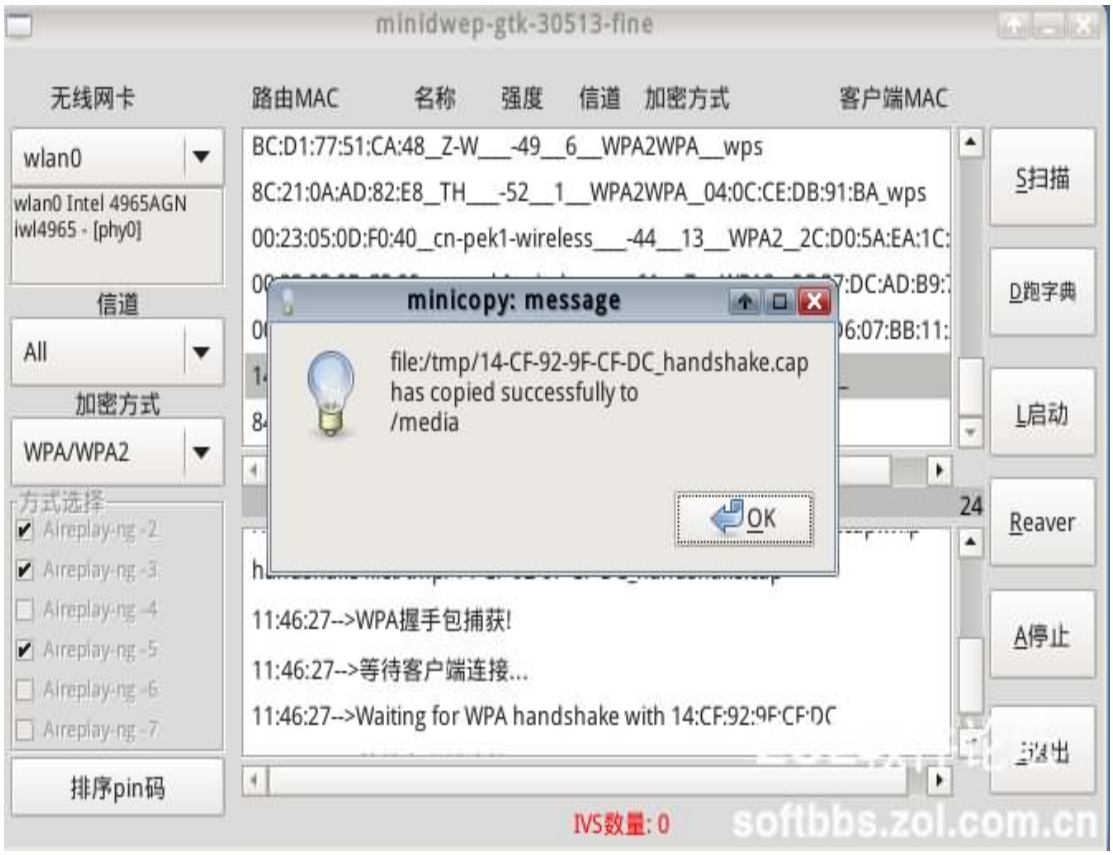
弹出窗口显示详细的路由名称（SSID），密码信息。



记录下破解出来的密码，然后软件会提示是否记录握手信息包到硬盘分区。



选择完保存路径之后就可以保存了。



这样一个路由的密码就算是破解出来了。看似简单的一篇图文详细教程，也废了流云好大力气，CDlinux U 盘启动用了很多种方法，格式化数次 U 盘才选中这一种曲线救国而又异常方便的方法，希望大家也能成功破解出自己希望破解的路由密码！WiFi 密码破解详细图文

教程也就到这里了，希望能看明白吧！后续有什么新东西也会不定期更新在这个帖子里，没事多来看看哈，说不定有什么惊喜呢！

防御这类型的破解方法有两种：含特殊符号和 Mac 地址绑定！不过貌似自己周围这样的设置比较少，所以大家成功率还是很高的！祝你好运 :)

关于贴子的方法有朋友回复稍显复杂，其实大部分跳过虚拟机那步即可，做一个 U 盘来进行也是非常不错的。

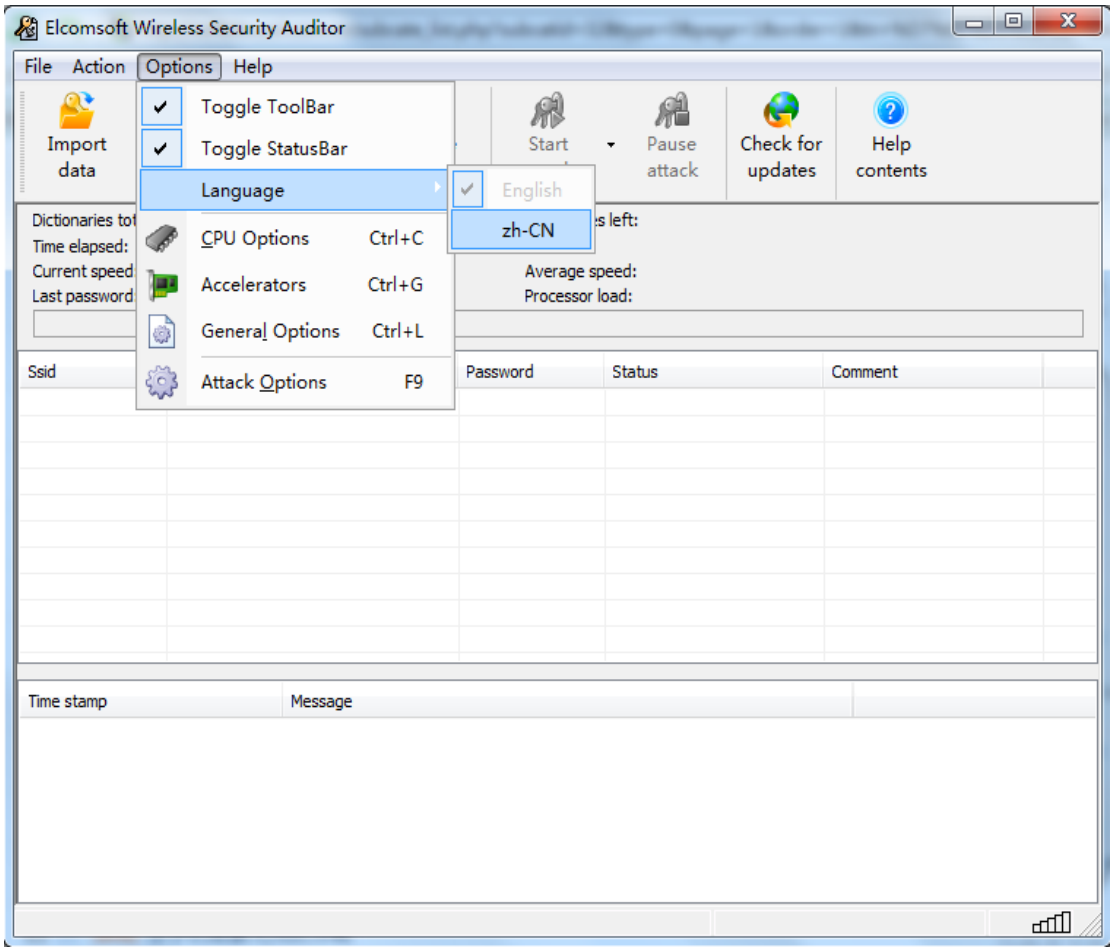
9 月 5 日更新 Windows 下破解方法：

感谢村长给提交 ZOL 首页焦点图推荐，不少网友回复这个方法较浅，不够深，还有就是速度可能较 GPU 破解来说，稍慢。所以加上一款可以再 Windows 下利用 GPU 破解的工具吧：Elcomsoft Wireless Security Auditor（简称 EWSA 附件有特别版下载 你懂的）。

EWSA 其他介绍及字典下载：http://softbbs.zol.com.cn/1/32_8011.html

这里提供给大家的是一款修改过的，关闭无广告弹出的版本（你懂的那种版本）。因为隶属于黑客类工具，杀软报警啥的，是常见的，请自行决定是否使用！

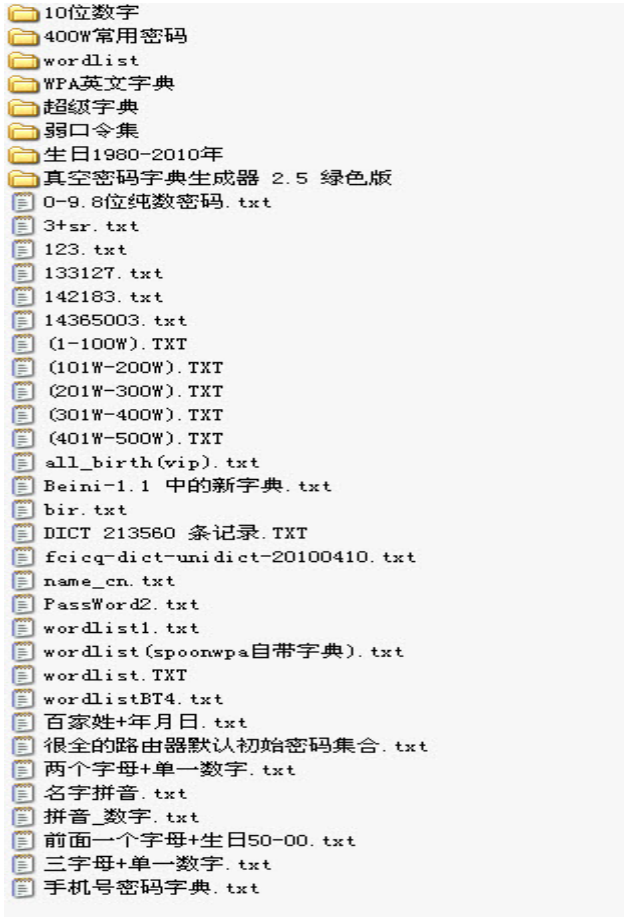
软件加入了中文语言包，通过下图来进行选择，Options——Language——zh-CN。



其他的都是中文了，估计大家都用的，不过它需要我们上面保存到的握手包，导入即可！（CDlinux 下，保存握手包的方法就是上传到网盘，那个镜像自带火狐浏览器的，登陆网盘上传上去，用 Windows 电脑下载回来用这个软件跑就可以了）

因为 GPU 的强大运算能力真心是 CPU 比拟不了的，SO 性子急的就选用 Windows 跑吧（CDlinux 下也别停哈，这样更快）。

9 月 7 日更新较为强大的字典包：



文中相关软件下载：

CDlinux 镜像下载：地址 1 备用 2

U 盘和硬盘启动安装工具（unetbootin 工具）：网盘下载

本地备份：U 盘和硬盘启动安装工具.rar(大小 4298k,下载次数:8687)

syslinux.cfg 文件下载：syslinux.cfg(大小 1k,下载次数:7079)　网盘备份：地址 1

Elcomsoft Wireless Security Auditor（EWSA 中文修改特别版）：地址 1

9 月 7 日更新的密码包下载：网盘地址 1　备用 2