WIFI 最新的 BT5 以集成 16G 字典

卡王破解步骤一:
启动桌面上的卡王管理软件。切换到“可用网络”选项来调整天线角度，使目标路由位置最佳
卡王破解步骤二:
1,把下载下来的绿色版虚拟机解压，打开文件夹：
根据上面的提示按次序依次输入项目的序号 1-9,至完成。
如果安装当中出现硬件安装的对话框，如下图所示：
请选择“仍然继续”安装按钮
2,点 Vmware.exe 图标
开始新建虚拟机：
新建虚拟机步骤如下：
启动刚新建的虚拟机
在虚拟机的启动过程当中我们需要添加网卡，如下图所示，在虚拟机的可移动设备中的 usb 设备中的 realtek usb 设备打上勾。
我们点击左下角的图标，在弹出的对话框中输入 spoonwep 命令
，进入 BT3 系统，再点击左下角第二个图标开启一个命令窗口，输入：spoonwep，回车后十秒左右弹出 spoonwep2 程序：
NET CARD 网卡接口 选择 WLAN0(备注：带Ｎ的网卡此项选择ＲＡ0)
DRIVER 驱动 选择 NORMAL
MODE 模式 选择 UNKNOWN VICTIM
点击 NEXT 进入下一步
3.点击右上角 LAUNCH 按纽（点完后会变成ＡＢＯＲＴ），２０秒左右程序会扫描到周围无线信号。
ESSID 路由广播名称
MAC 路由的地址
CHAN 使用的频道
POW 信号强度
DATA　数据包
CLIS 空白代表无客户端,打钩则代表有客户端；
(备注：无线网卡搜索一陈后，被搜索到的无线信号的ＳＳＩＤ将会以列表显示。如果某加密无线信号的ＣＬＩＳ方框内有“勾”，表示该无线信号此刻拖有客户 端，这时破解会高效、快速一些。如果你选中了这样的无线信号，紧接着窗口的下方会显示出客户端列表，你应该把下方的客户端也选中一项参与破解。不要迷信一 定要带客户端才能破解，没有客户端的ＡＰ也可以破解，理论上ＰＯＷ值大于 18 的都可以破解)
有客户端模式比无客户端成功率要高，选中打算破解的路由，下面会显示当前所有连接到这个路由的客户端，选择一个 POWER PACKETS 都比较高的客户端(如上图)
然后点 SELECTION OK 转到 ATTACK PANEL 窗口:
第一个下拉菜单有四个选项，后面三个可作为无客户端攻击模式，其中：
APRREPLAY ATTACK　(有客户端时用)

P0841REPLAYATTACK (次次选)
CHOPCHOP & FORGEATTACK (次选)
FRAGMENTATION & FORGE A TTACK (首选)
第二个下拉菜单有 3 个选项,其中:
???LENGTH (不指定加密位数，首选)
128BITSLENGTH (指定 128 位加密，次次选)
64BITSLENGTH (指定 64 位加密,次选)
两个下拉菜单右边 InjRATE 是每秒发包数量，选默认的 600 既可。
选择好两个下拉菜单，点击左边 LAUNCH 按钮(点完后会变成 ABORT)，开始破解，一般十分钟内密码可以出来。
此时注意观察抓包窗口，如果 10 分钟内ＤＡＴＡ没有快速增长，则换一种攻击模式。
最下面的 wep key 既是破解出来的密码：AE07938C6F(无需输入冒号)