# Omnipeek 10.0.1 配合 EWSA 跑包破解路由器密码教程

# 目录

# 1. 使用 Omnipeek 抓包

## 1.1. 安装相关软件和驱动

提前安装 Omnipeek 软件和抓包驱动，可以参看相关教程。

## 1.2. 运行软件开始抓包

以管理员身份运行 Omnipeek 软件；

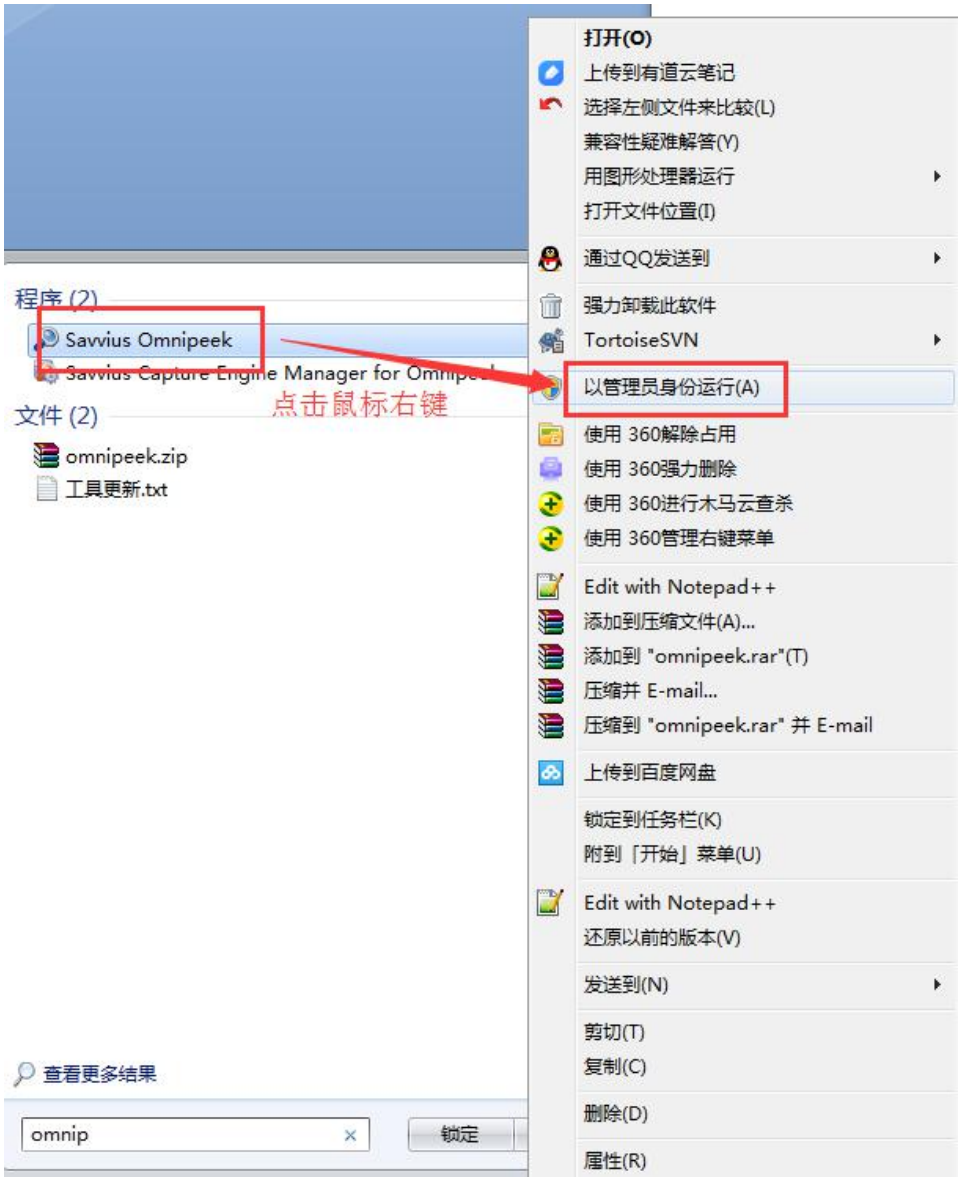


图 1

点击“New Capture”开始

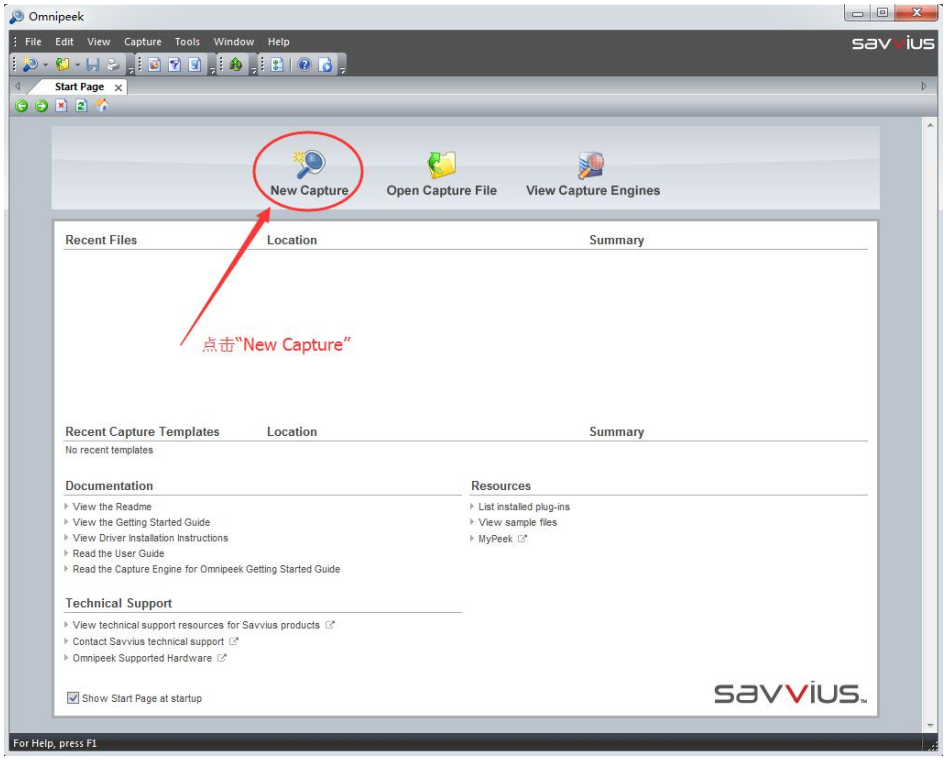


图 2

点击“Adapter”选择 Local machine 下支持 Omnipeek API：Yes 的网卡，有些电脑可能有多个 Local machine，每个都需要查找；

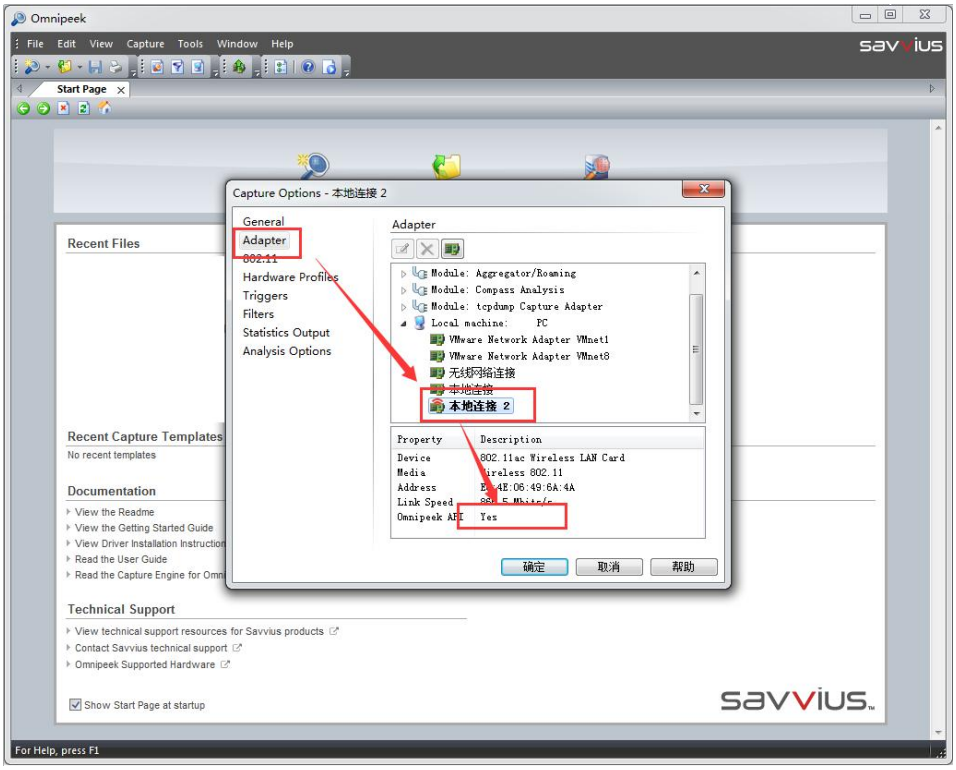


图 3

点击“802.11”选择“scan”，点击“Edit Scanning Options”勾上 1-14 的所有信道；

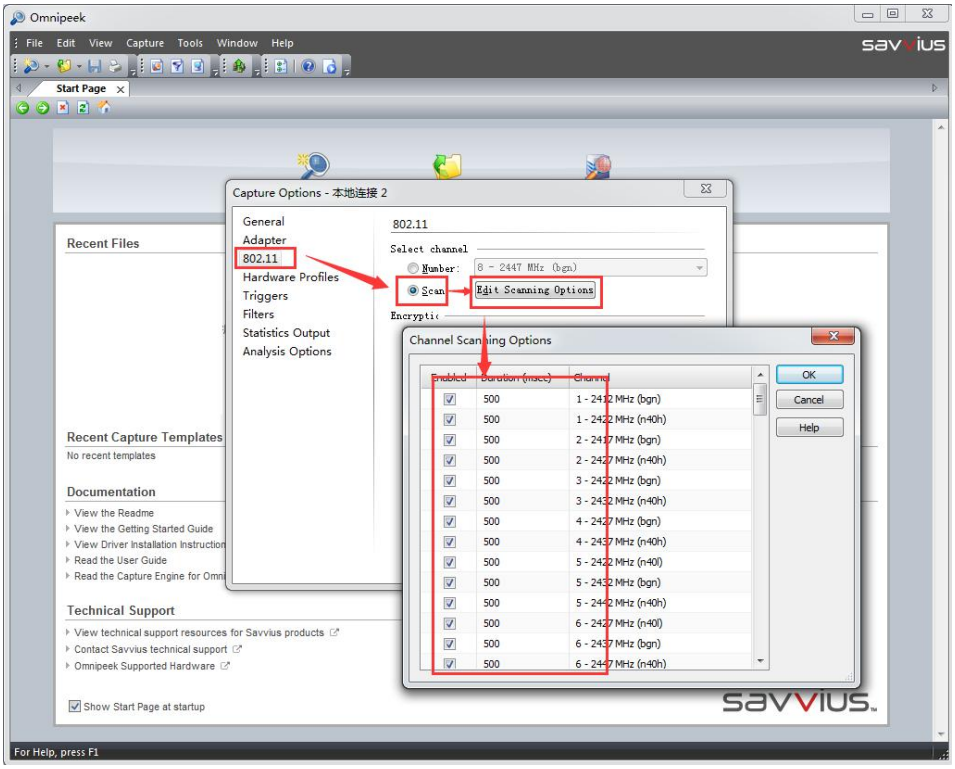


图 4

设置结束后，点击 “确认”；

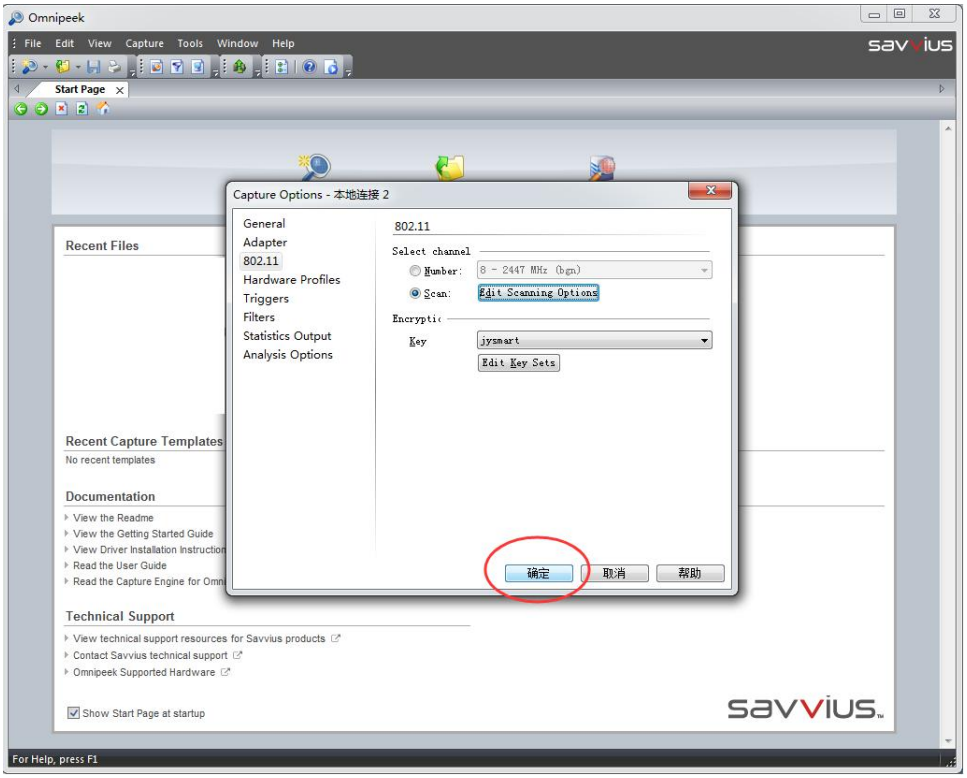


图 5

点击“Start Capture”开始抓包 1 分钟左右；

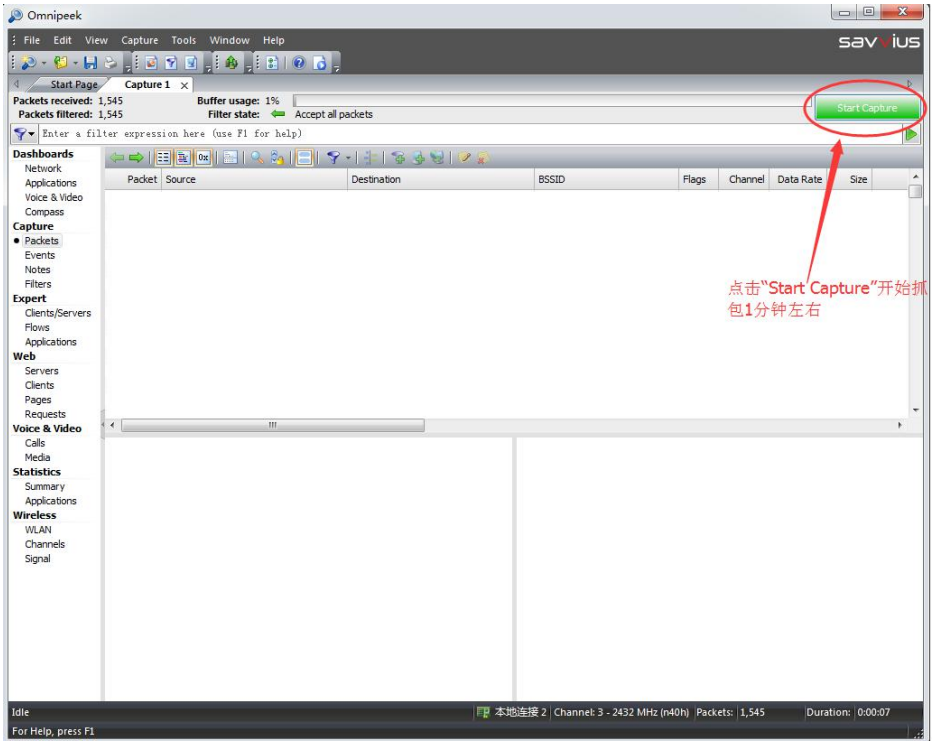


图 6

点击“WLAN”查看空中无线网络情况，选择自己需要抓包的路由器，记录好路由器的 mac 地址和信道，举例：名为“XY”的 MAC 地址为“A4:56:02:93:D9:A3”，信道是 11；

确认后点击“Stop Capture”停止抓包；

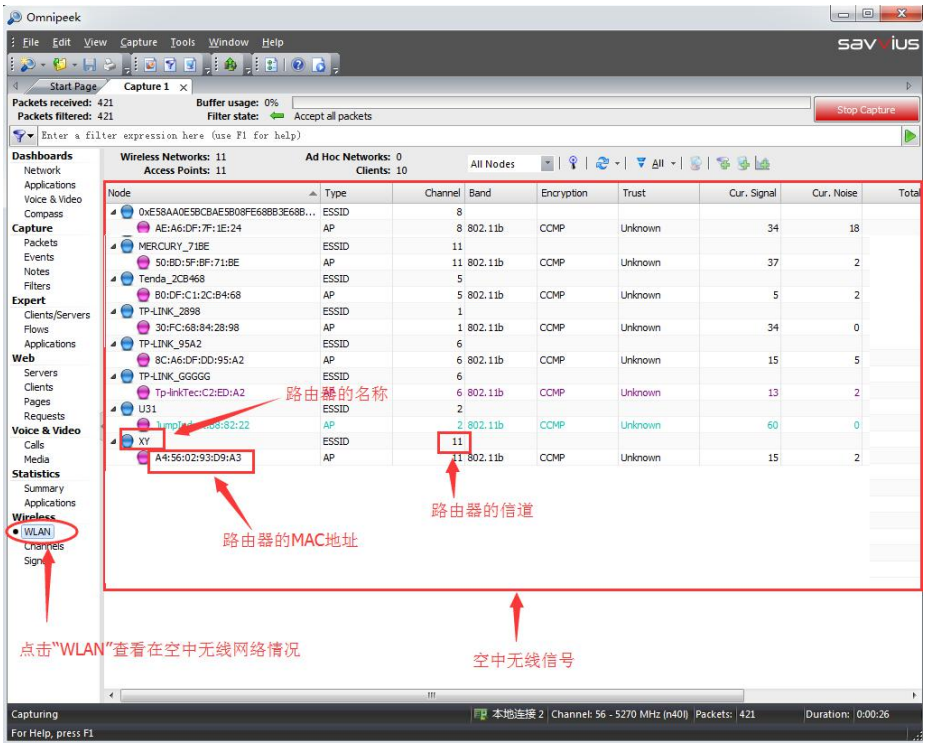


图 7

点击“Capture->Capture Options”；

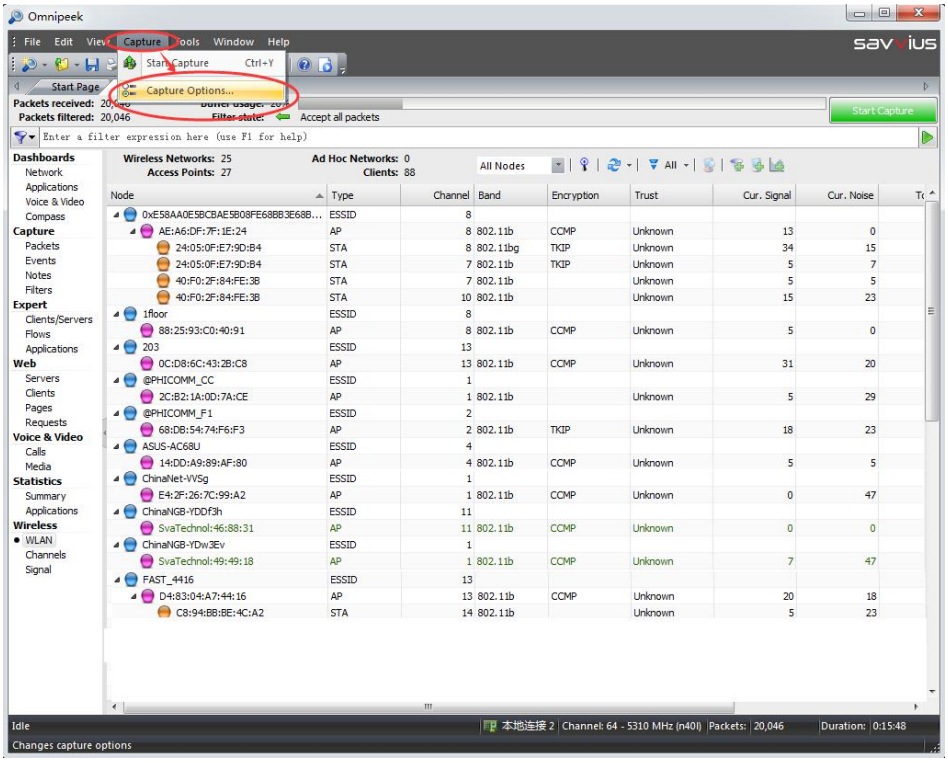


图 8

点击“802.11”->“Number”选择之前记录的信道号，举例：信道 11

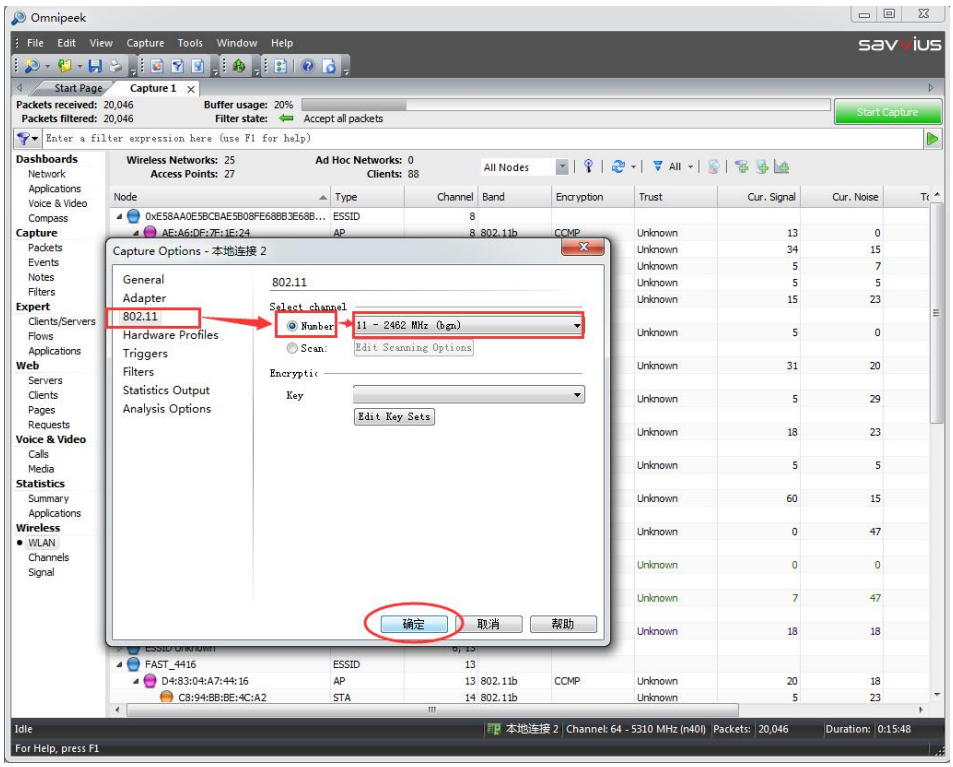


图 9

点击“Filters”右键“Import”导入“802.11Handshake Packet.flt”；

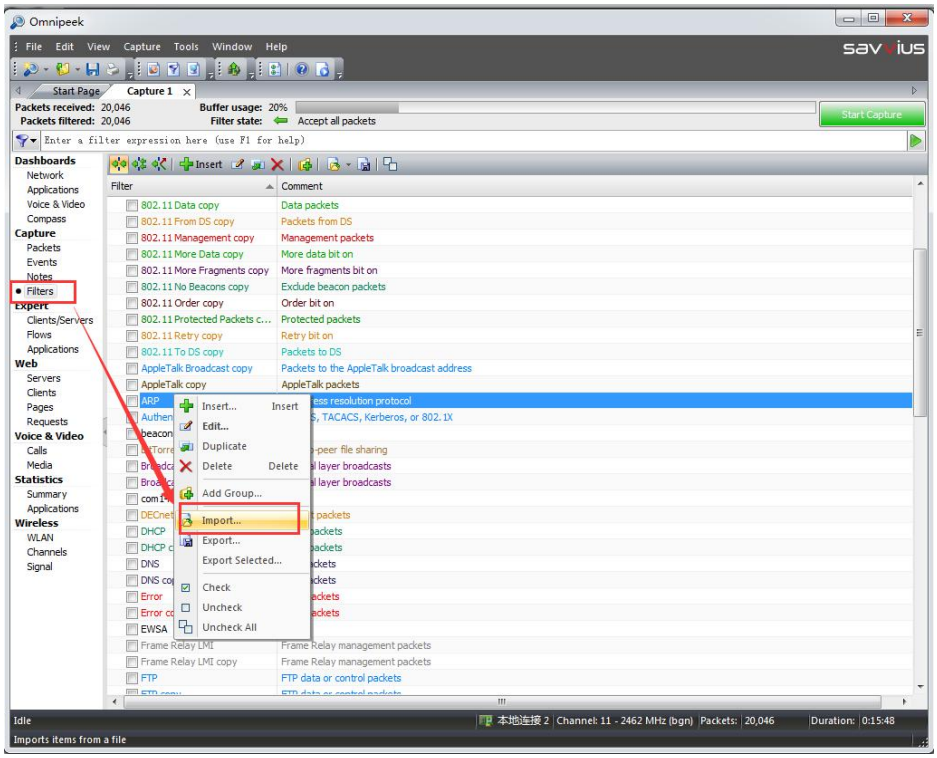


图 11

双击“EWSA”，双击“Address”，修改地址为之前记录的 MAC 地址，举例：A4:56:02:93:D9:A3

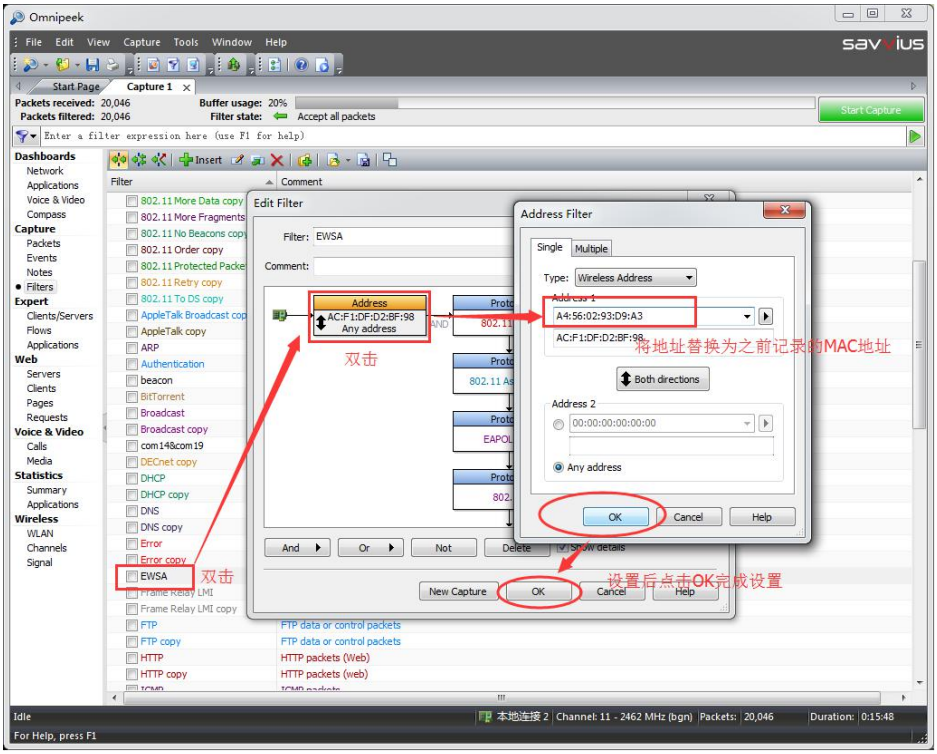


图 12

勾选“EWSA”，点击“Packets”，点击“Start Capture”开始继续抓包；

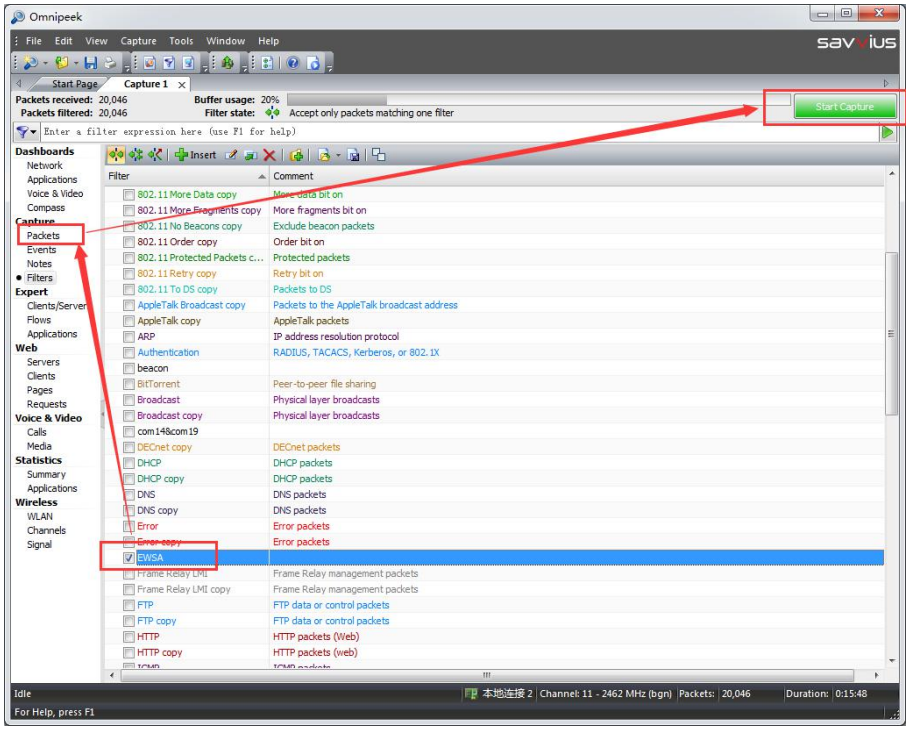


图 13

等待抓到“EAPOL-Key”这种握手包，握手包只有在设备连接路由器的时候才会出现，可能需要长时间抓包才能抓到；

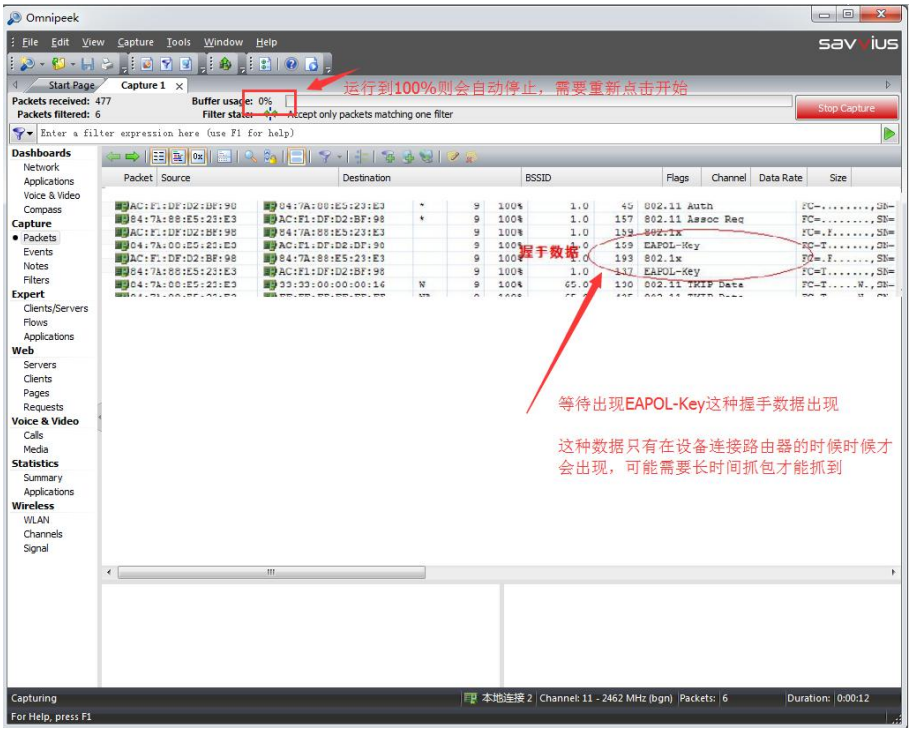


图 14

抓到握手包后，点击“File->Save All Packets”保存数据包；

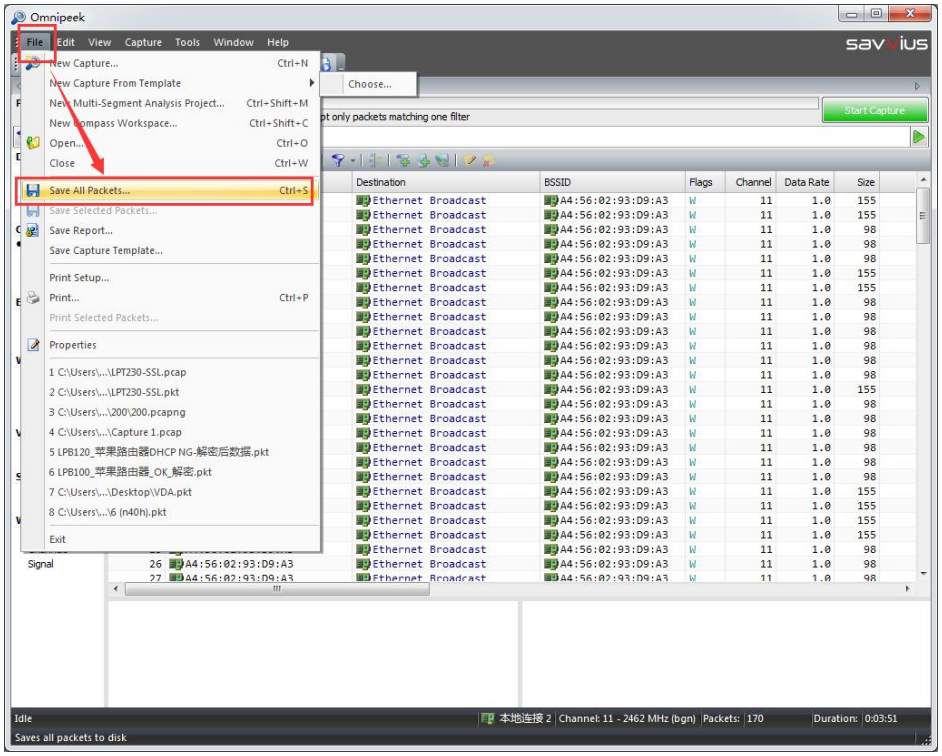


图 15

选择保存为“Libpcap”格式；

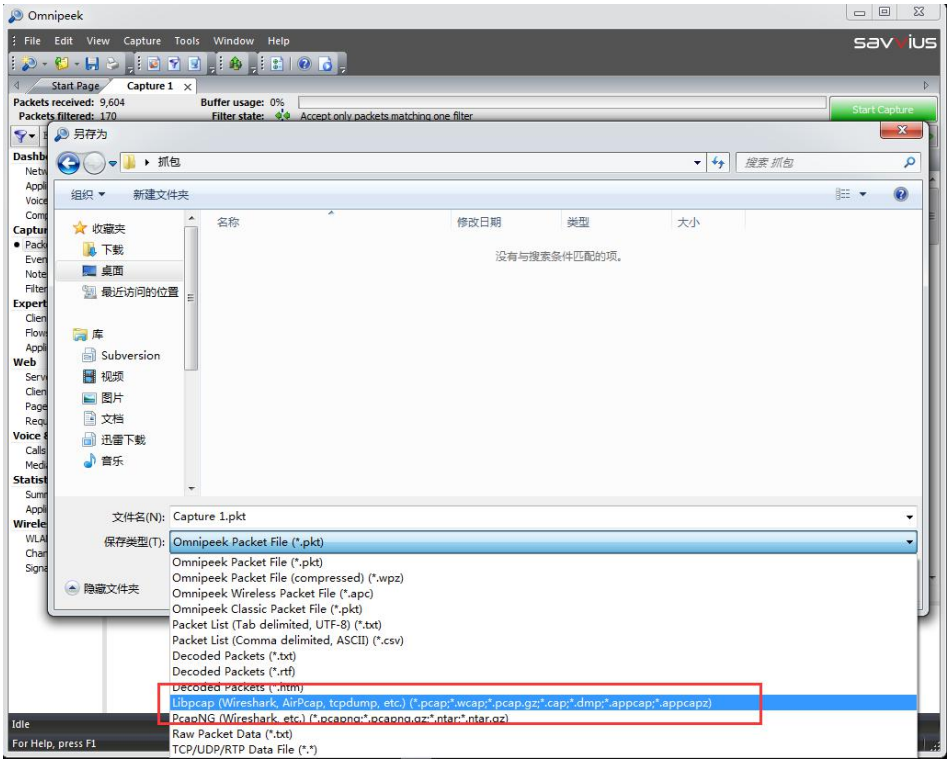


图 16

至此抓包结束。

# 2. 使用 EWSA 跑包解密

## 2.1. 运行 EWSA 软件

打开 EWSA.exe 软件，点击“导入数据->导入 Tcpdump 文件”，选择之前保存的文件；

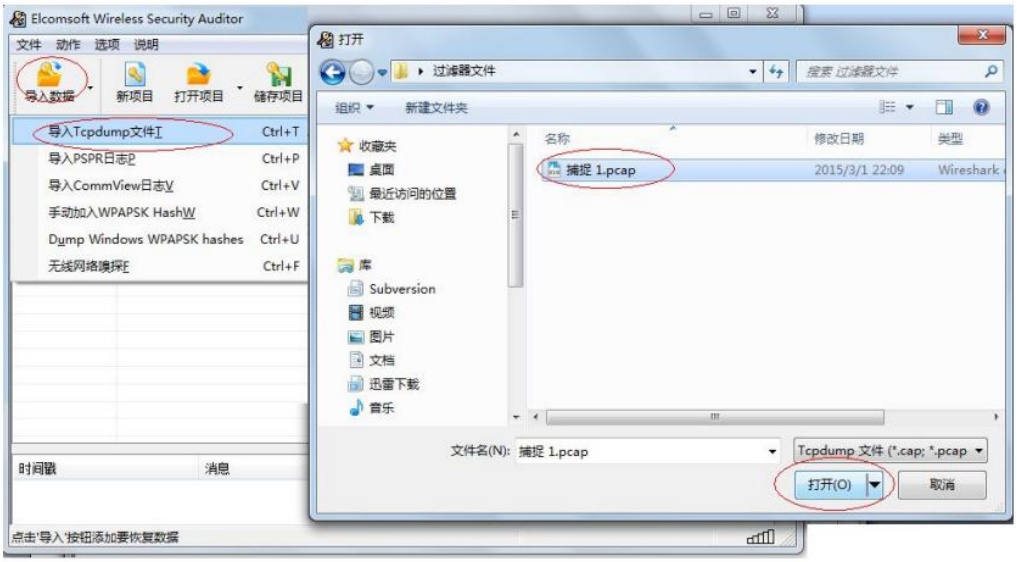


图 17

确认打开后可以看到抓包数据包中的有效握手包，选择需要破解的那一个，点击“确认”；

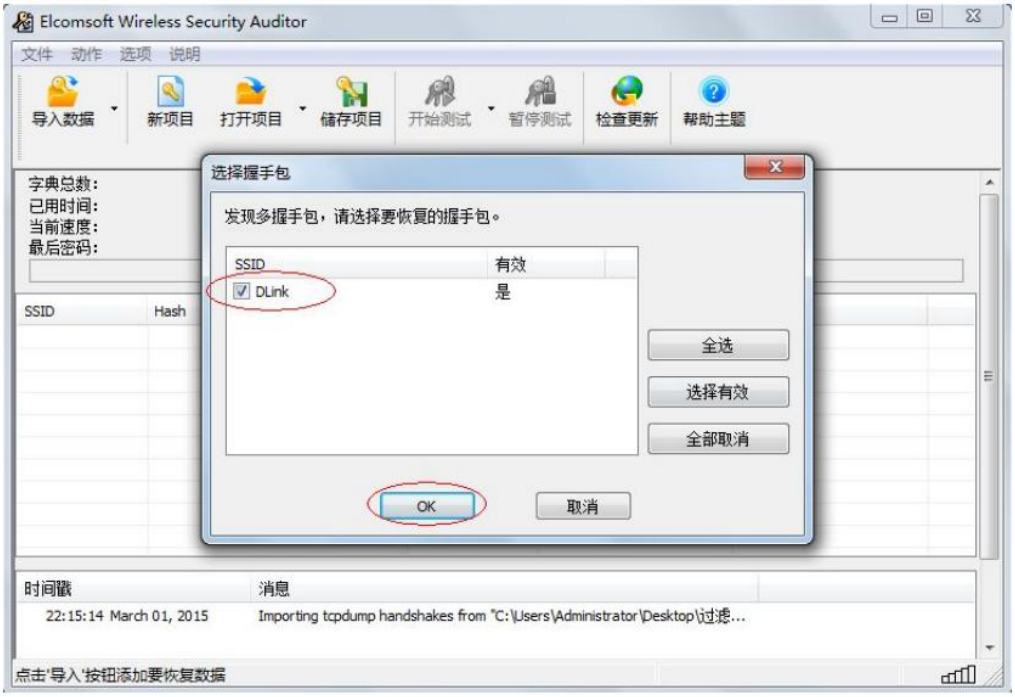


图 18

点击“开始测试”，如果是第一次打开需要设置一下字典，字典为同目录下的“english.dic”文件，设置好后点击开始测试；软件会显示解密的过程，当密码被找到后会提示：

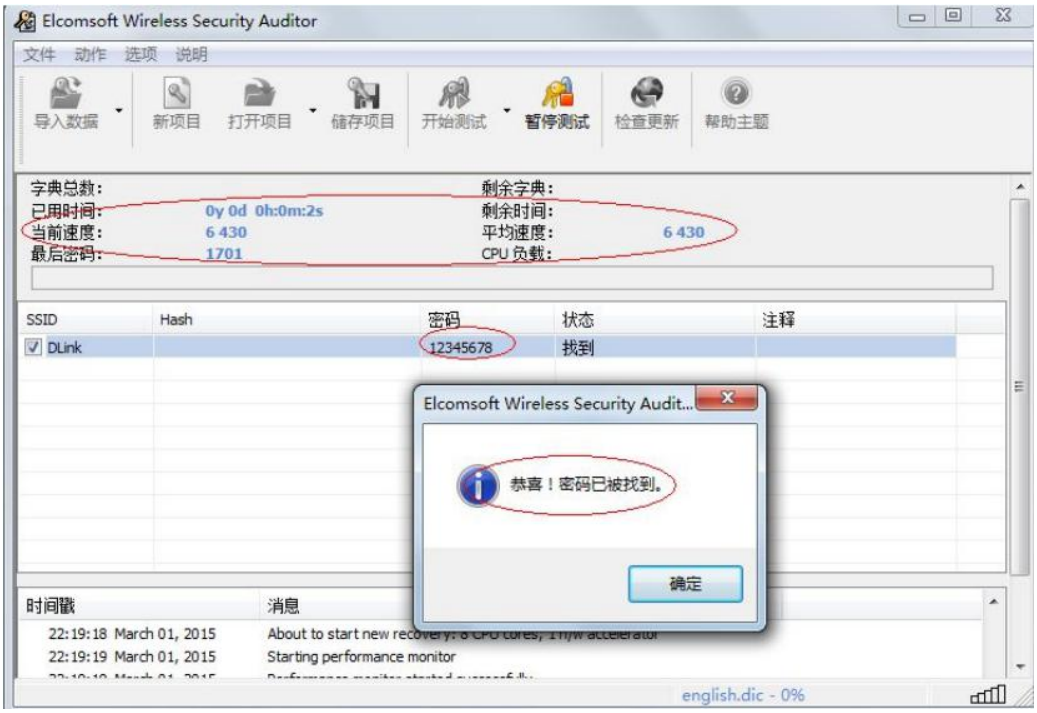


图 19

**注意：当字典跑完后还是没有成功破解，可以换一下几个字典跑跑，字典越大跑的时间越长！**