802.11 无线

抓包教程

V3.0

目录

1. 驱动安装

1.1. 安装说明

驱动文件分为 32 位和 64 位，请根据电脑系统对应选择合适驱动文件，驱动安装请一定根据以下说明安装。

1.2. 驱动安装

将网卡插入电脑 USB 接口中，打开电脑的“设备管理器”，找到网卡所对应的选项，有些电脑可能会显示“802.11ac Wireless LAN Card”或“802.11n WLAN”等，或者通过拔插网卡来判断设备管理器中哪一个对应的是网卡，如下图：

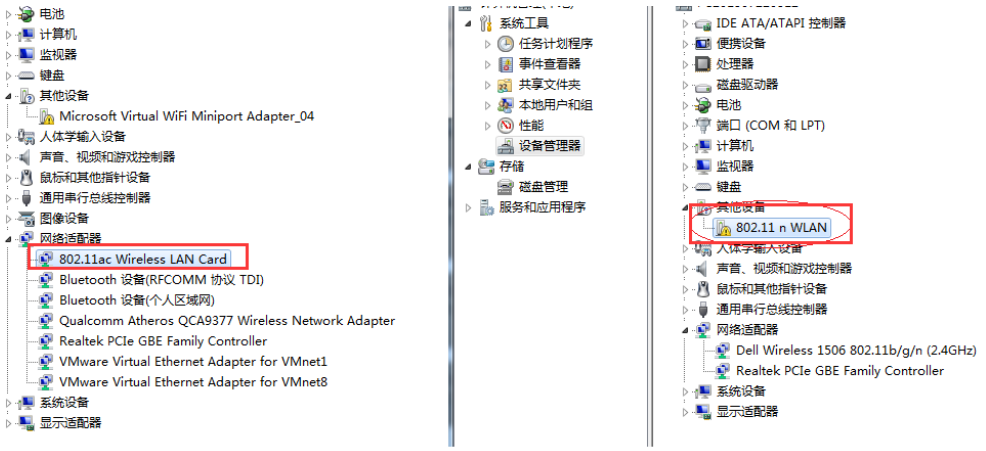


图 1

部分电脑可能会自动安装驱动，点击关闭或等待安装结束即可。

选中网卡点击右键“更新驱动程序软件”，选择“浏览计算机以查找驱动程序软件”：

图 2

选择“从计算机的设备驱动程序列表中选择”，请不要选择“浏览”，选择浏览按钮安装可能成功，也可能会失败：

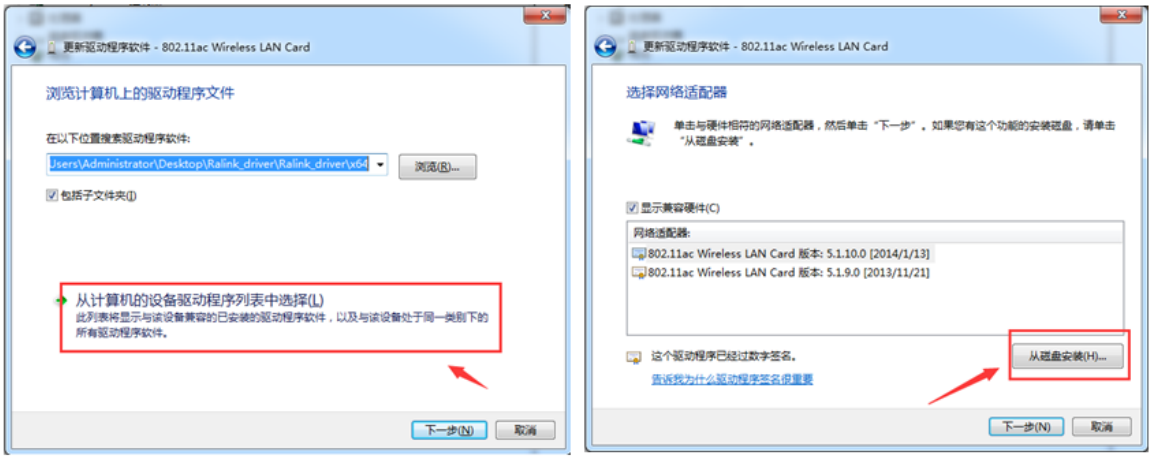


图 3

选择对应的驱动文件：

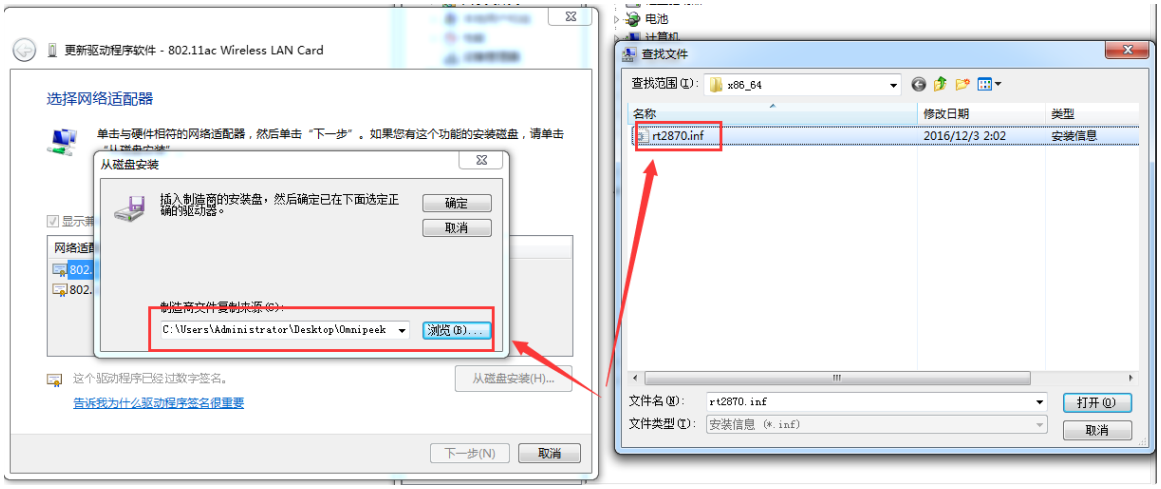


图 4

点击下一步开始安装：

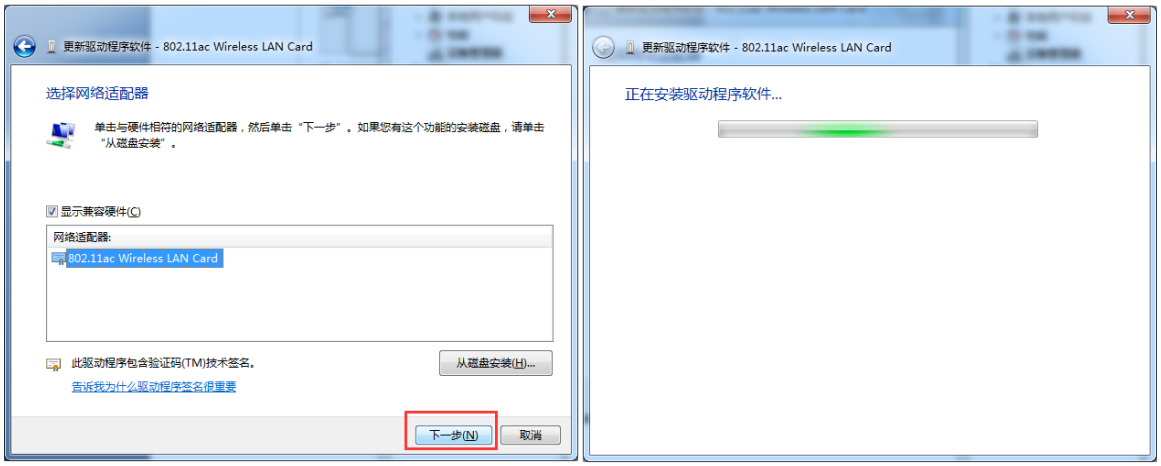


图 5

安装过程会提示警告，请选择继续安装，等待安装成功：

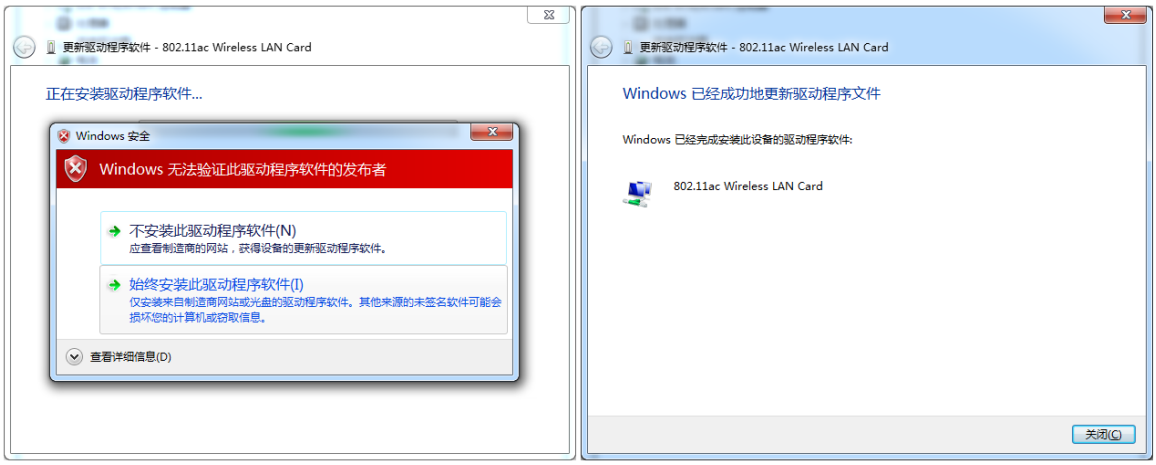
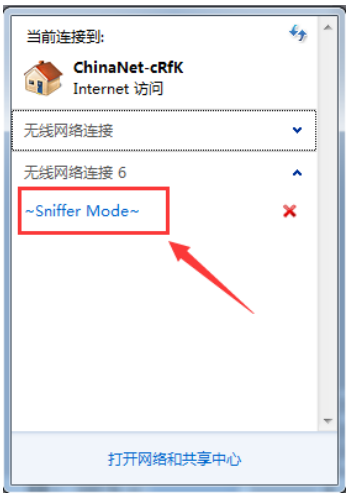
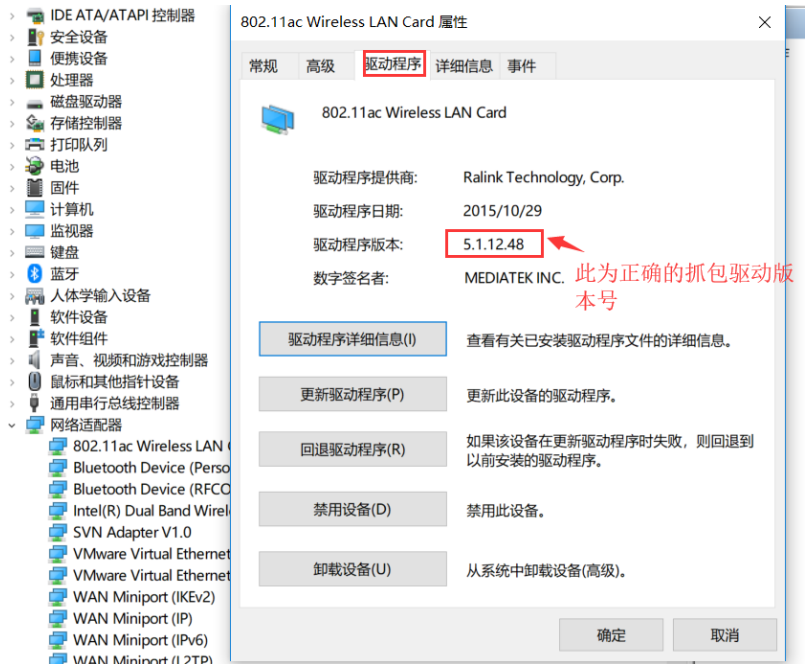


图 6

至此驱动安装完成，完成后点击 Windows 下网络标志可以看到一个“Sniffer Mode”的网卡，说明抓包驱动安装正确，如下图：



少部分电脑安装完后设备列表中名字不是“802.11ac Wireless LAN Card“或者没有”Sniffer Mode“，最好的方式是通过设备管理器中右键->属性查看驱动程序版本号，正确的抓包驱动版本号为”5.1.12.48“，如果是此版本说明驱动安装成功。



注意：

如果在设备管理器中网卡前面有一个黄色感叹号或者提示您驱动签名有问题，请参考“相关文档“文件夹下的《5、驱动提示数字签名问题》中的解决方法解决。

1.3. 驱动切换

网卡模式说明：网卡支持 **抓包** 和 **普通上网** 两种模式，普通上网模式就是可以连接路由器进行上网的，文档中安装说明默认安装的是抓包驱动。

判断网卡所在模式：点击电脑右下角网络标志，出现如下图所示“sniffer mode”说明网卡处于抓包模式，右下角如果出现下图的“无线网络连接”说明网卡处于普通上网模式，如下图：

或者通过驱动版本号来判断，如果是“5.1.12.48“则是抓包驱动，其他为上网驱动。详细的说明可以请参考“相关文档“文件夹下的《1、当作普通网卡上网》中的《网卡驱动切换说明.pdf》。

2. 软件安装

2.1. 安装说明

Wilpacket omnipeek 已更名为 Savvius Omnipeek， 从 7.8 版本开始支持 802.11ac 协议，下文讲述如何在 Win7 64 位电脑上安装 Omnipeek 10.0.1。

部分电脑安装 Omnipeek 10.0.1 可能会提示安装 CRT、SHA-2、Microsoft .NET Framework 4.0 等，根据提示安装即可。

提示需要安装 CRT：请参考“相关文档“文件夹下的《3、安装 Omnipeek 提示更新 CRT》中的解决方法解决，安装后请重启电脑。

2.2. 软件安装

打开资料包，解压文件，选择对应电脑系统版本的文件夹，找到安装软件，然后双击 Omnipeek10_x64.msi 开始安装：

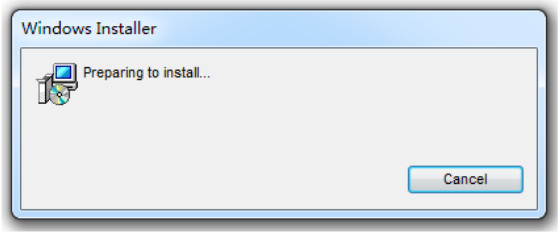


图 7

等待初始化完成，点击 Next，在第二步 Product Activation 中选择“Manual：generates your activation key via a web page”，然后点击 Next：

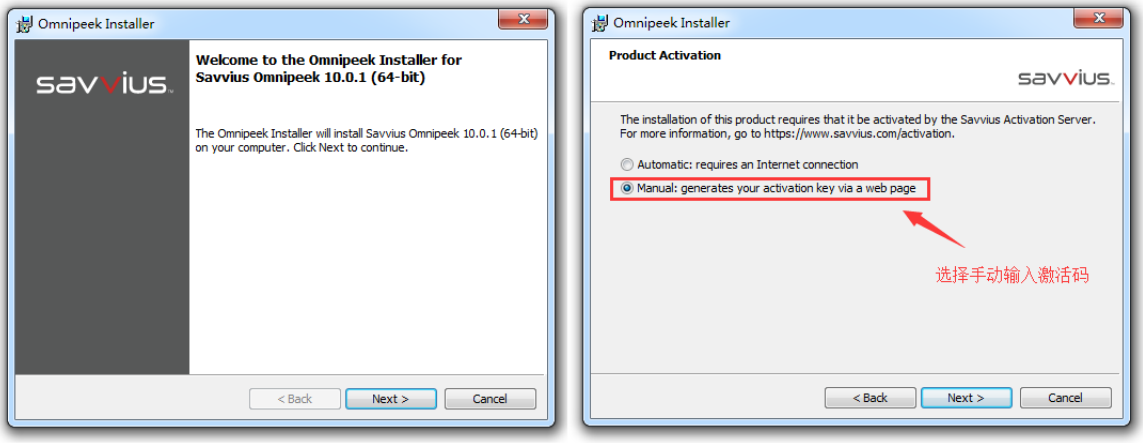


图 8

双击打开秘钥生成工具，Product 选择“OmniPeek Ent. with Enh. Voice Opt.”，Product Version 改为“100”，点击“Generate”生成，请注意区分“Serial Number”和“Activation Key”，如果您系统的杀毒软件会删除密钥生成工具或者电脑无法运行密钥生成工具，请联系我们帮您生成，或者参考“相关文档“文件夹下的《7、无法运行密钥生成工具》中的说明。

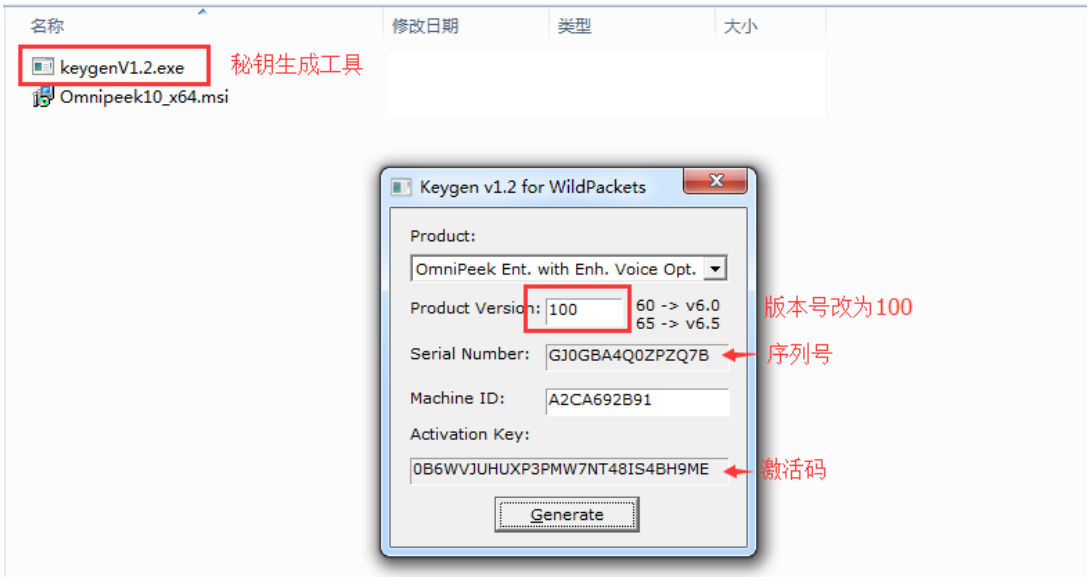


图 9

将序列号拷贝至安装软件，Omnipeek Installer 中的“User Name”、“Company Name”和“Email”可随意填写，点击 Next：

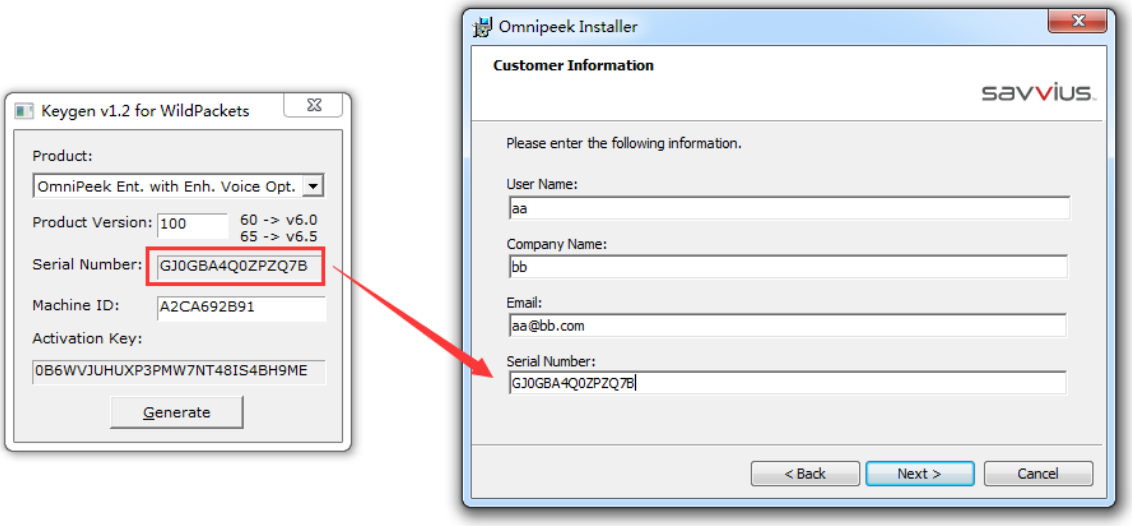


图 10

点击 Next，拷贝激活码，再点击 Next：

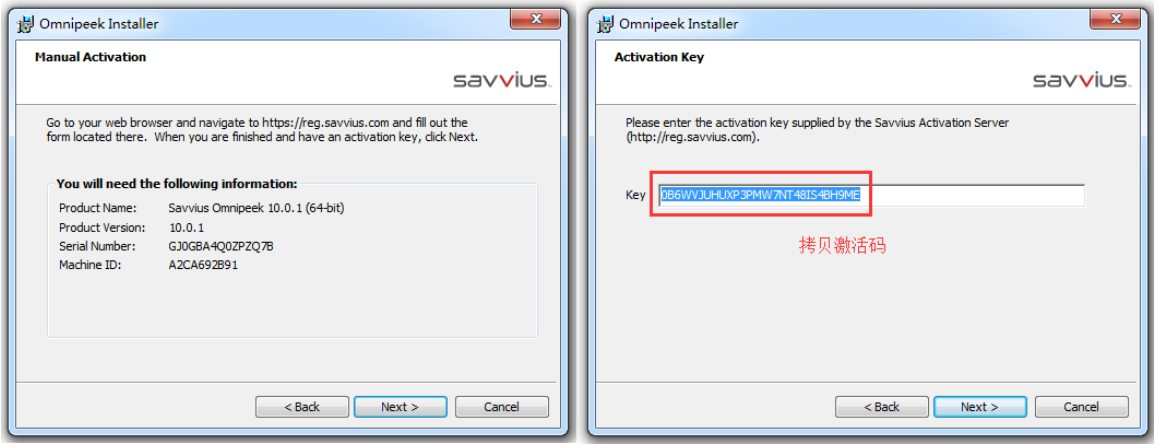


图 11

选择“accept”点击 Next，选择“Default location”，点击 Next：

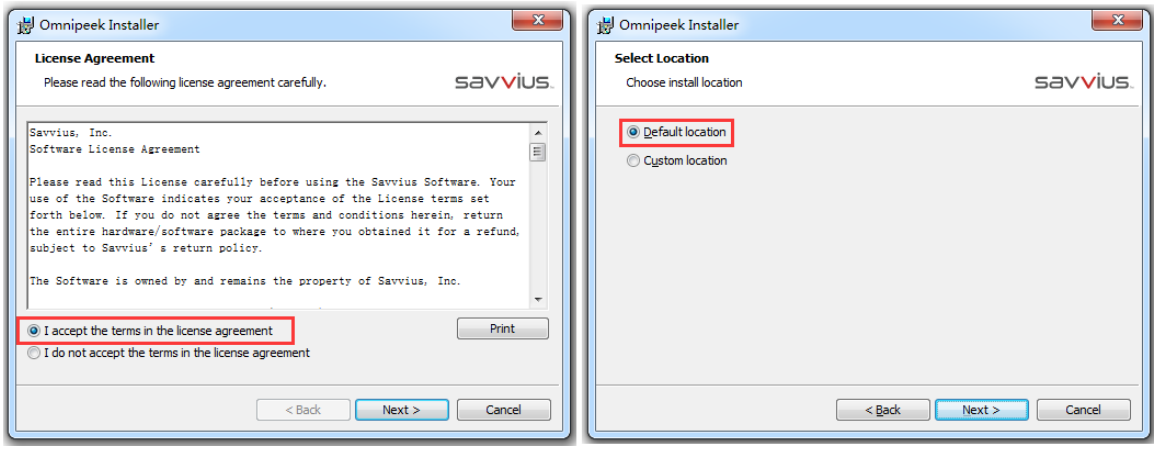


图 12

选择语言，如果以前安装过其他版本 Omnipeek 会提示是否卸载，本文选择卸载，如果没有安装过请忽略这步：

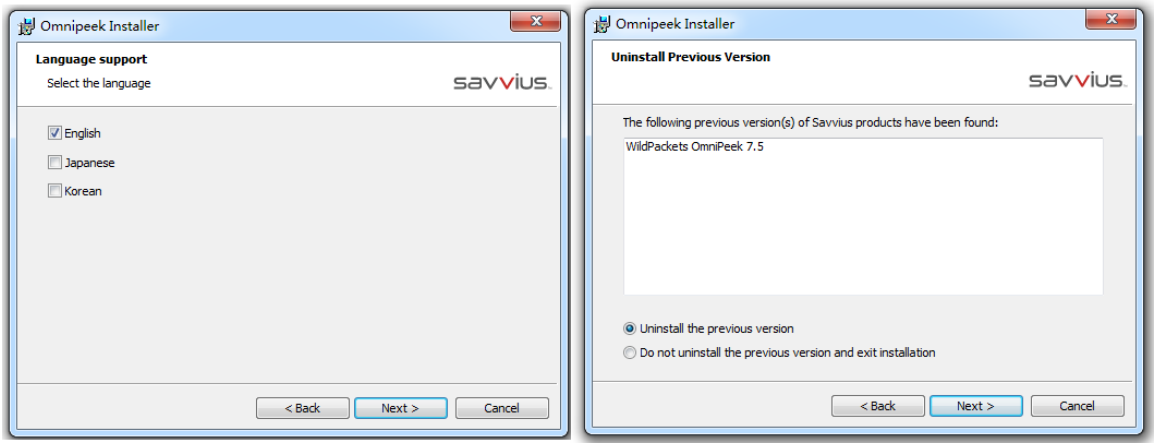


图 13

点击 Install 开始安装，等待安装成功，安装过程中 360 等安全软件可能会报警，点击允许即可。

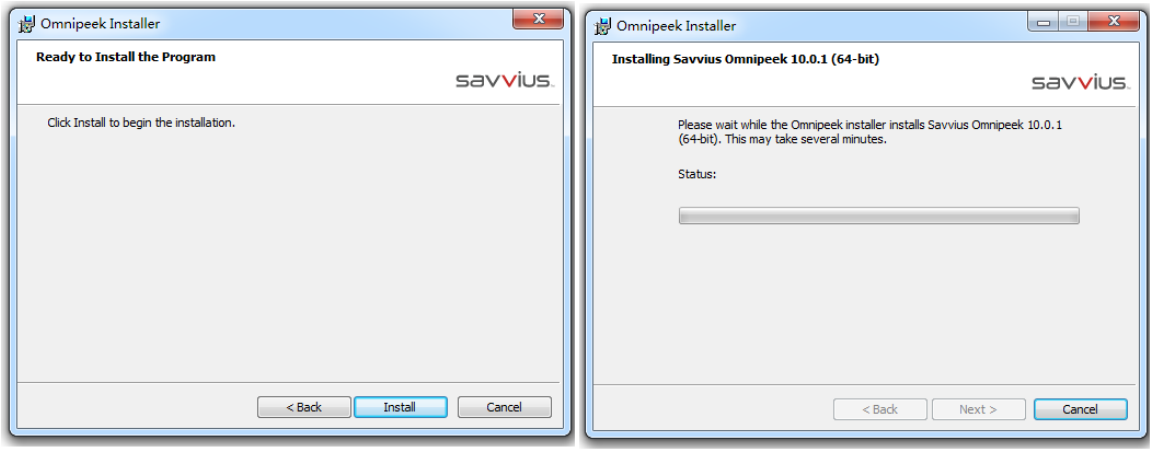
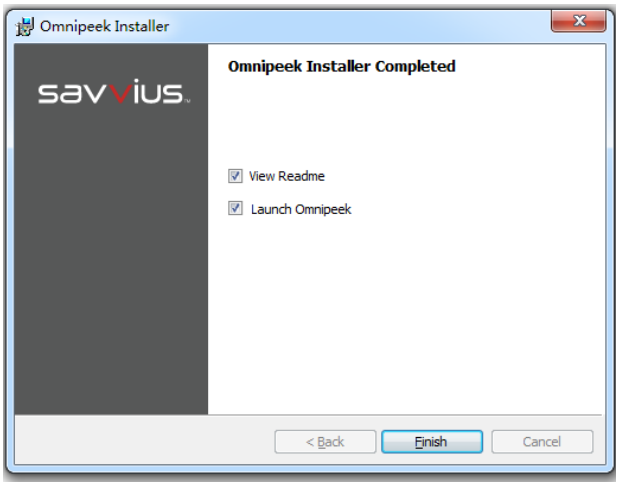


图 14



2.3. 常见问题

1. 序列号密钥错误

如果进入软件直接显示密钥错误，那是上一次序列号输错引起的，解决办法：

打开注册表，找到下面目录，把目录下的三个注册信息全部删除，然后重新打开 Omnipeek 软件，可以继续输入序列号了！

Win XP 的目录是：

HKEY_LOCAL_MACHINE\SOFTWARE\WildPackets\OmniPeek\6.3\UserInfo

Win 7 的目录是：

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\WildPackets\OmniPeek\6.3\UserInfo

部分电脑可能不在上述目录下，可以搜索关键字“OmniPeek”、“WildPackets”查找注册表项。

2.运行 Omnipeek 软件闪退或者蓝屏

参考“相关文档“文件夹下的《6、其他版本 Omnipeek》中的说明安装 7.9.1 版本 Omnipeek 软件或者使用虚拟机的方式。

3. 开始抓包

3.1 运行软件

点击运行“Savvius Omnipeek”软件，初次运行可能会设置一下注册表，请允许；打开软件后点击“New Capture”：

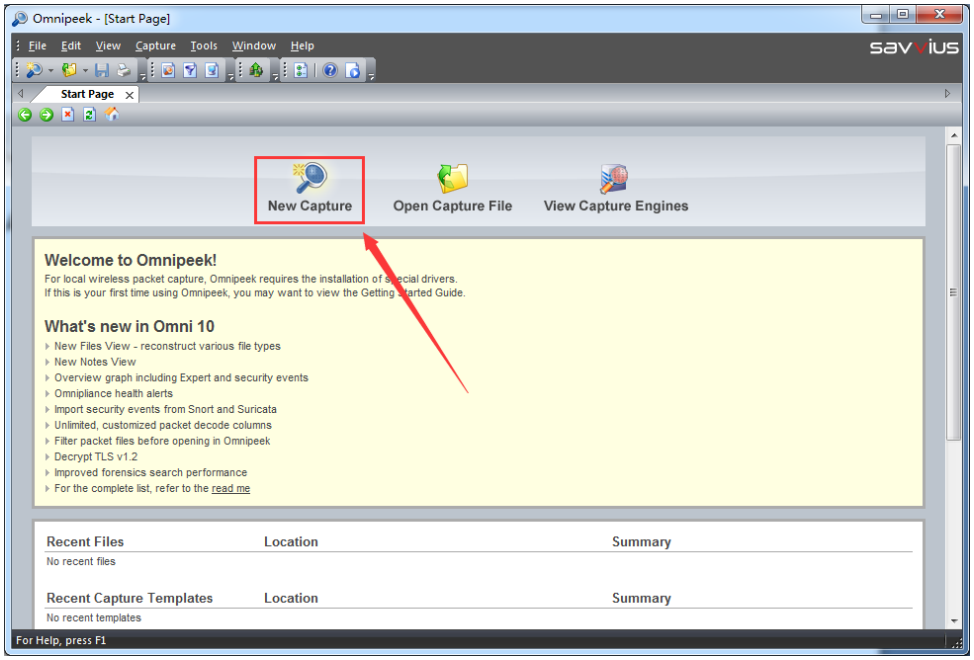


图 15

左侧菜单“Adapter”选择刚刚安装的网卡适配器，部分电脑在安装驱动后可能需要重启，选择后可以看到“Omnipeek API”为 Yes 则表示驱动安装正确，可以正常抓包：

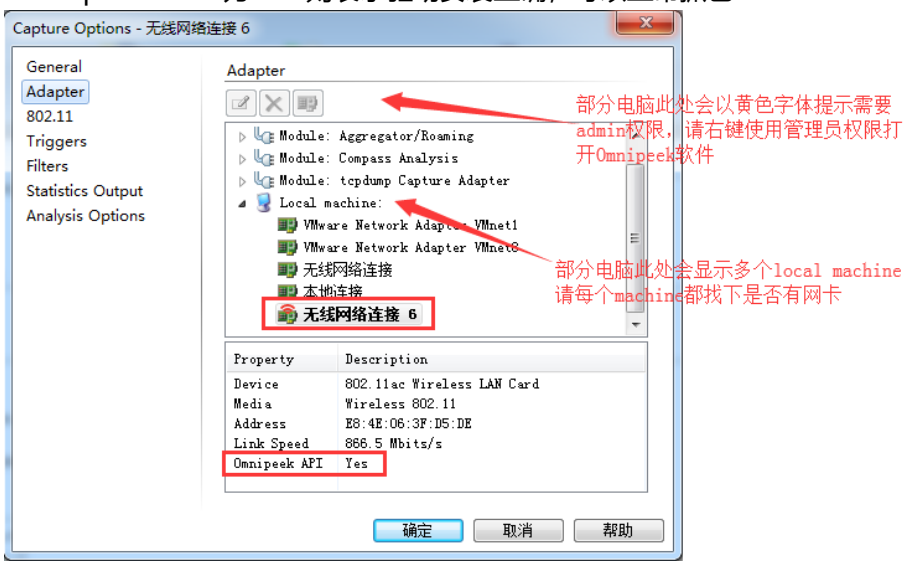


图 16

左侧菜单“802.11”选择需要抓包的信道，网卡只能在固定的信道上抓包；如果选择“scan”模式，则网卡处于多个信道轮询抓包，这种情况下漏包会很多；设置完后点击确定：

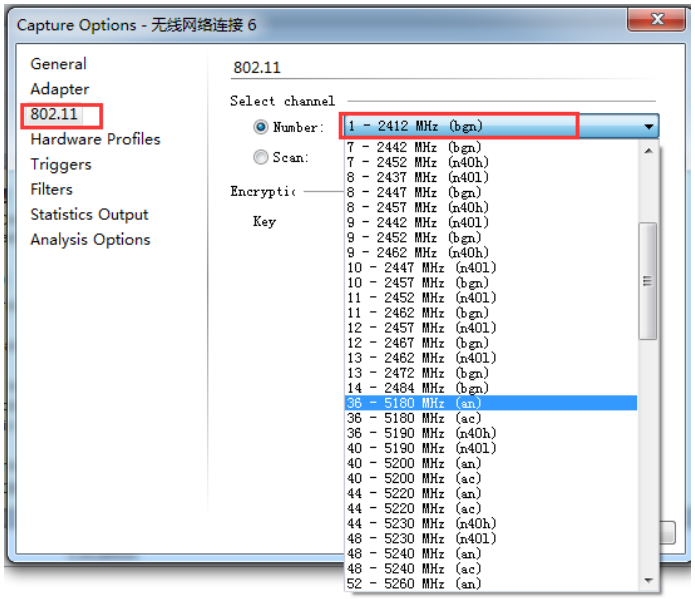


图 17

如果您需要同时抓 2 个信道，请参考“相关文档“文件夹下的《10、如何同时抓 2 个信道的数据》中的说明。

点击“Start Capture”开始抓包，点击左侧“Packets”菜单可以看到抓包的数据包，单击选中某个数据包可以看到数据包的具体内容：

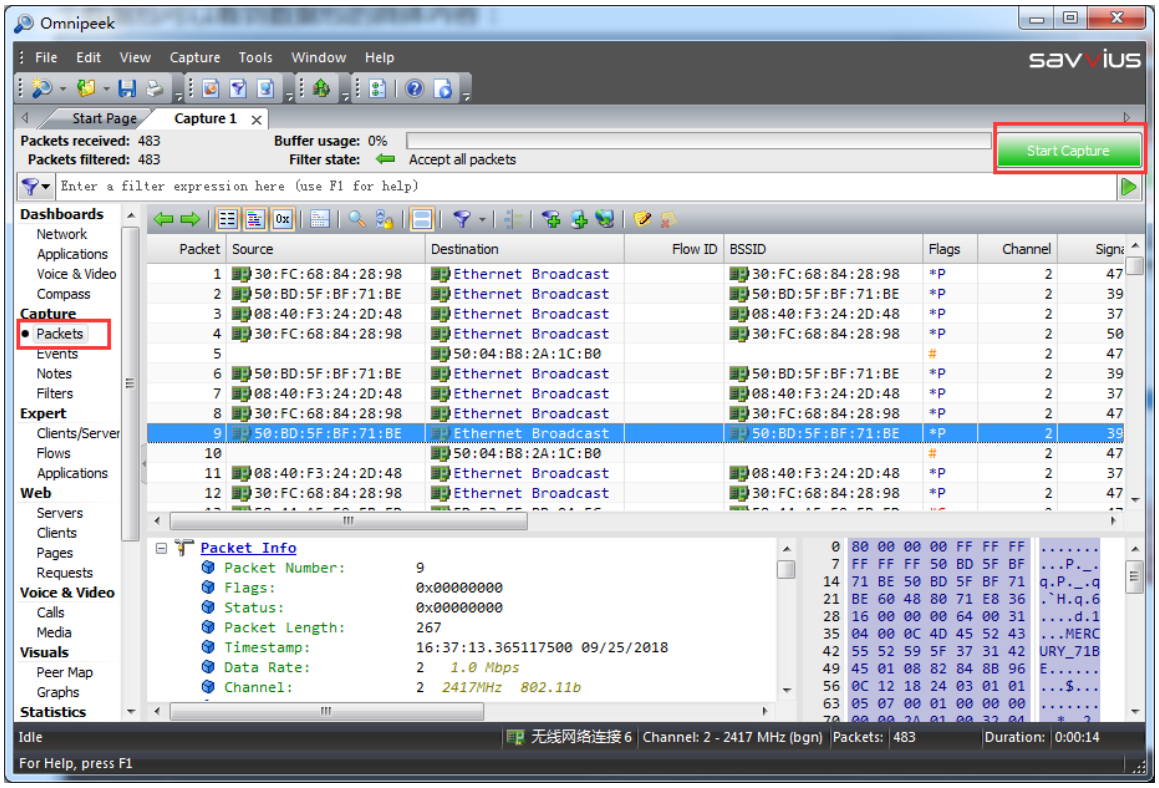


图 18

3.2 设置过滤

由于空中数据包很多，可以通过设置 filter 过滤获取想要的数据包，点击左侧菜单“Filters”：

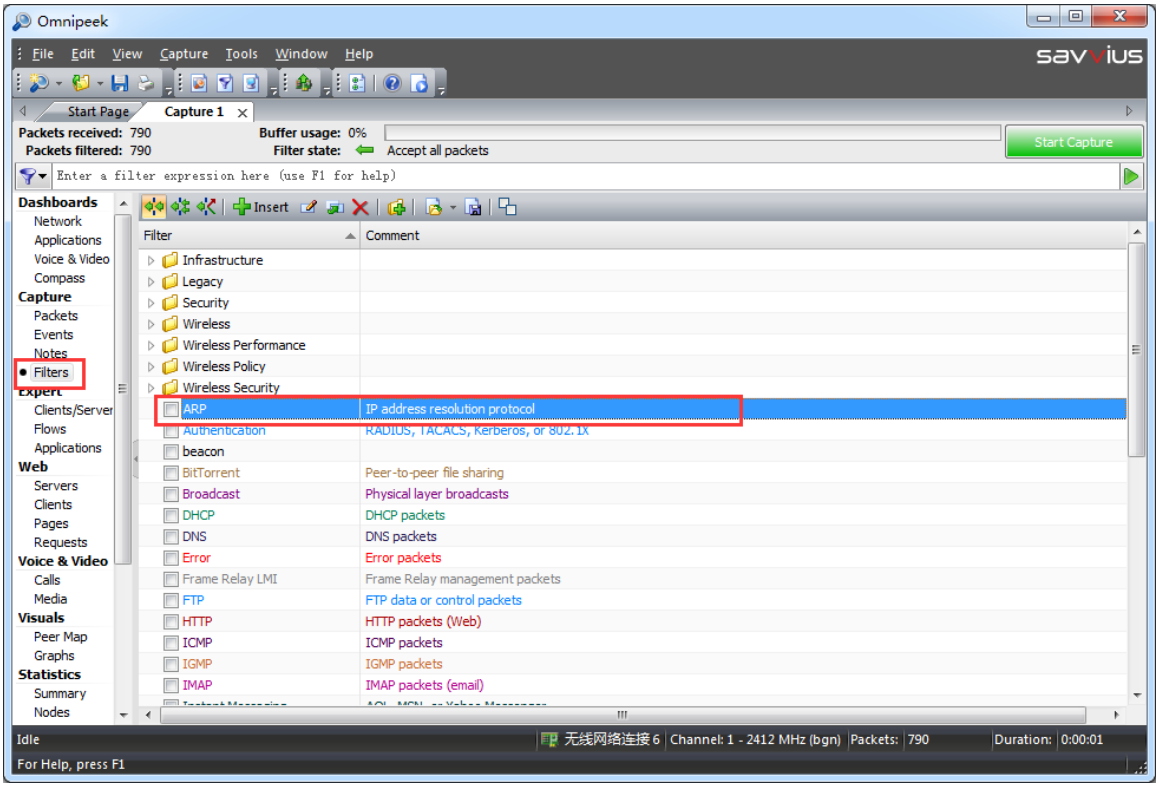


图 19

双击打开任意一个 filter，可以通过“Address”、“Protocol”和“Port”进行简单过滤，也可点击右上角 Type 切换为 Advanced 模式：

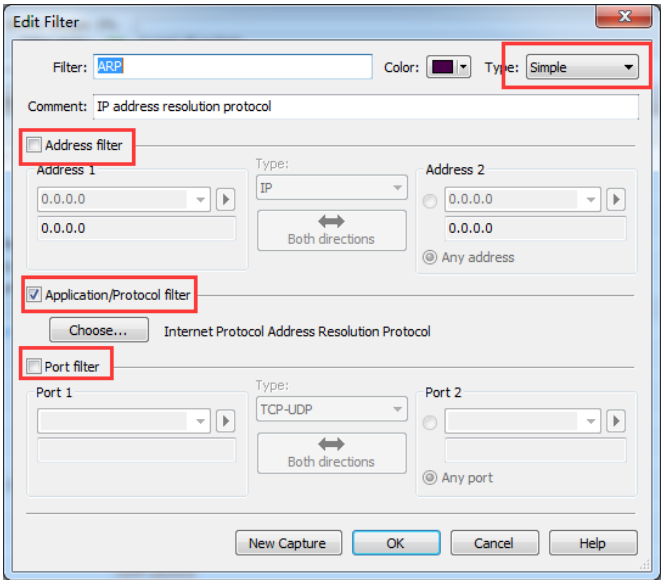


图 20

Advanced 模式下，可以通过“与或非”三种逻辑写出复杂的过滤条件：

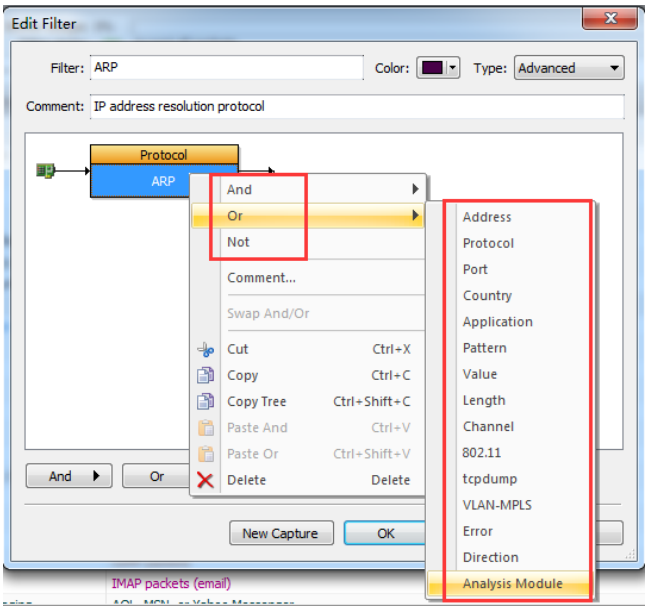


图 21

过滤条件书写完成后，勾选前面的方框应用 filter：

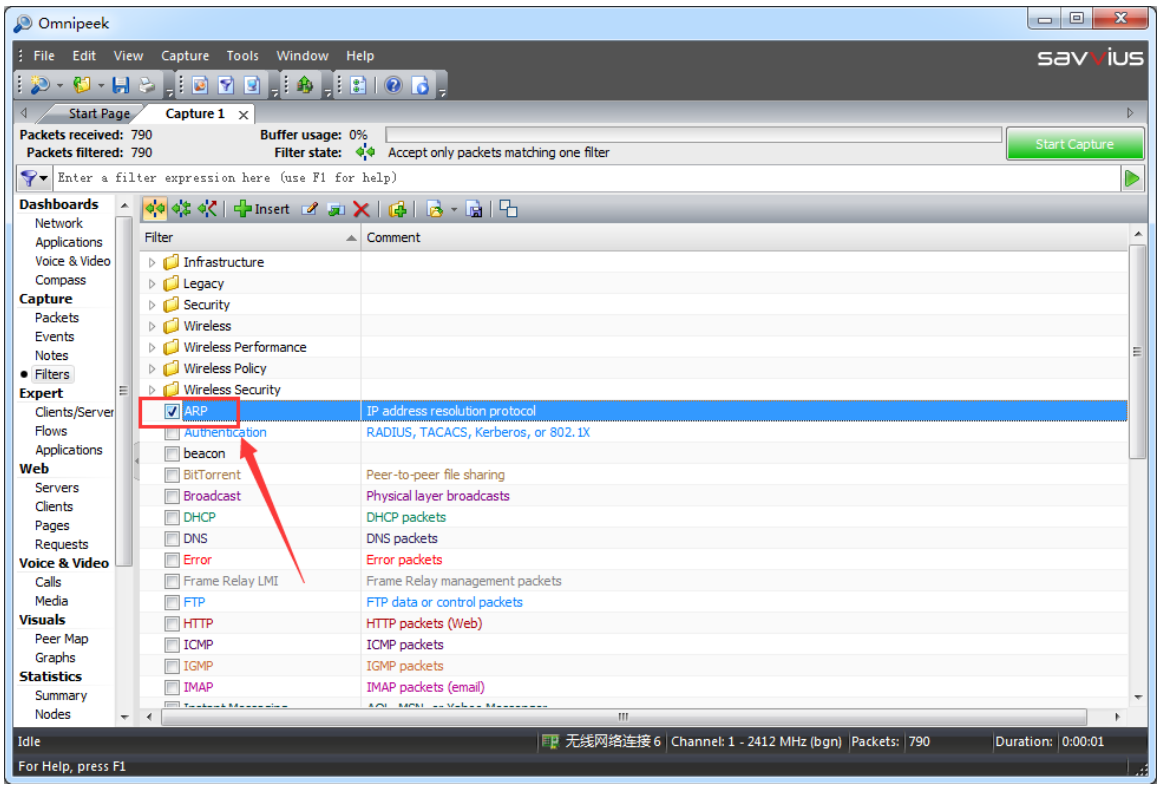


图 22

注意：如果是加密的路由器抓包软件抓到的数据包都是加密的，所以无法判断是不是 TCP 等，所以需要协议和端口判断的请把路由器设置成没有加密。

3.3 热点扫描

Omnipeek 可以扫描空间范围内的所有热点状态，将 802.11 设置为 scan 模式，然后设置需要扫描的信道和单信道扫描时间，然后开始抓包一段时间，时间需要大于 信道个数*单信道扫描时间；

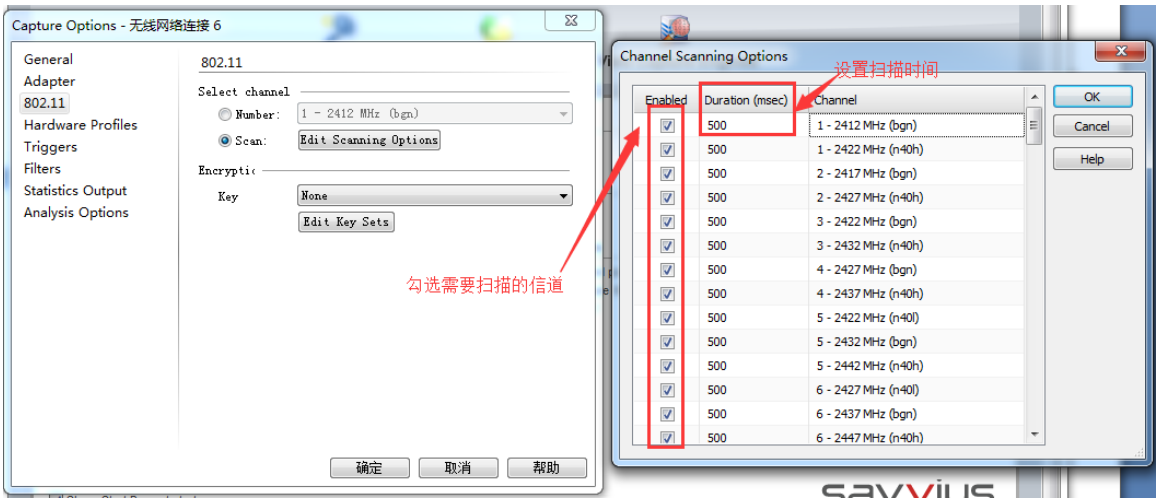


图 23

扫描结束后点击左侧菜单的“WLAN”可以看到空中所有热点的状态，如下图：

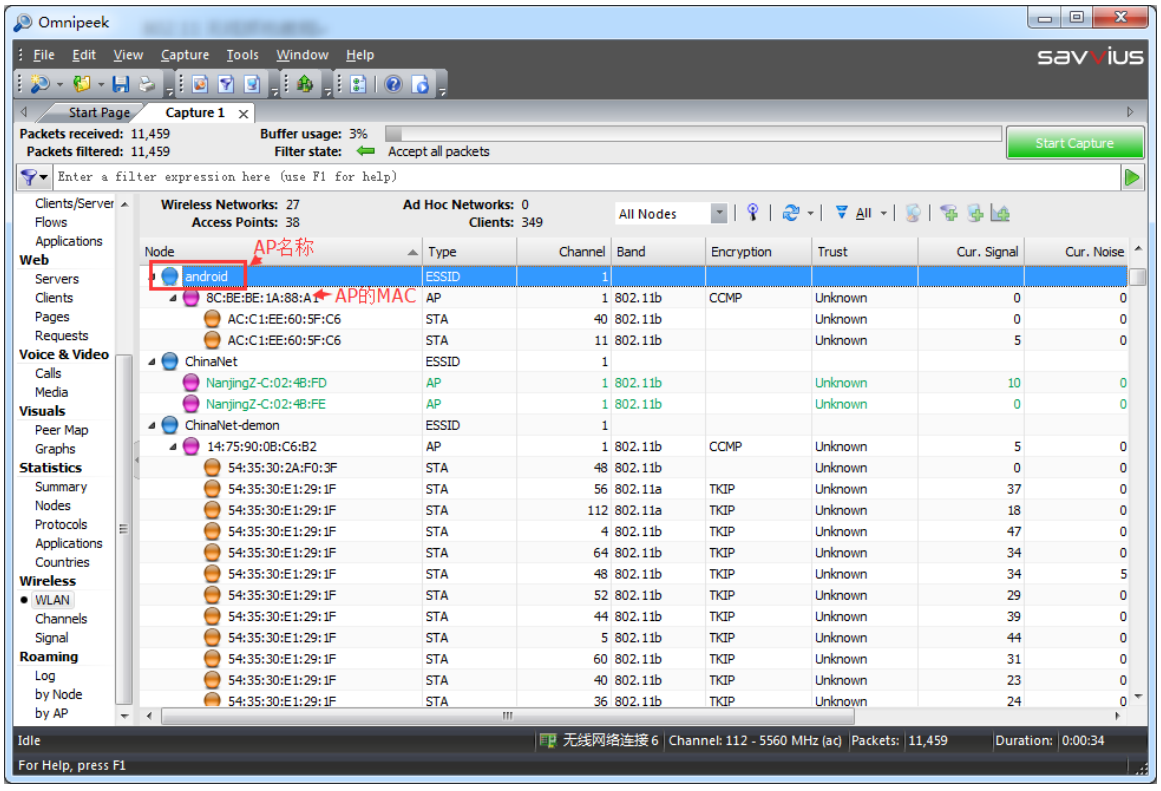


图 24

3.4 抓包实时保存到硬盘

实际应用中可能需要长时间抓包来复现问题，Omnipeek 一旦抓包到百分百后就会停止，为了解决这个问题可以设置将 omnipeek 抓到的包实时保存到电脑硬盘中。

在启动 Omnipeek 时打开 General 选项，勾选“Capture to disk”,设置相关的保存条件，然后 Omnipeek 软件会自动将抓到的数据包保存到硬盘中，如下图：

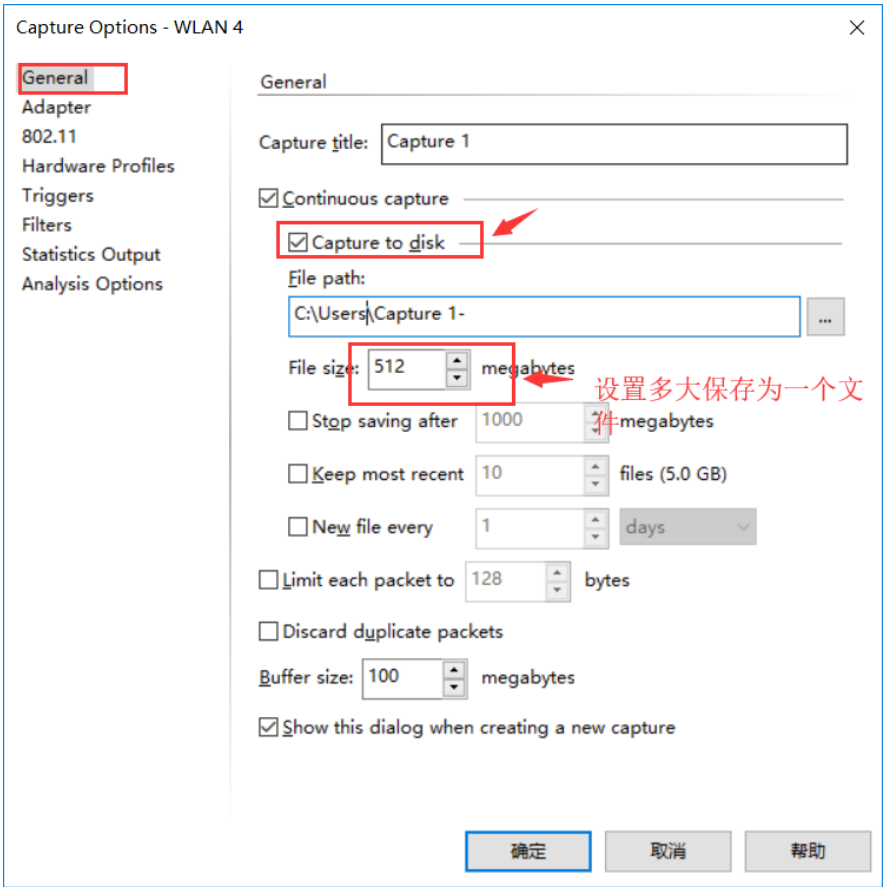


图 25

3.5 小技巧-快速定位到包

如何在大量的包中快速的定位到自己想要的包，有两种常用的方法：

方法一：在 Filter 中设置一个过滤条件，然后在 Packets 中点击  标志选择 filter，则会过滤出符合的数据包；

方法二：通过右键 Select Related Packets 的方法过滤出数据包。