windows下抓取802.11管理包

2015年7月9日

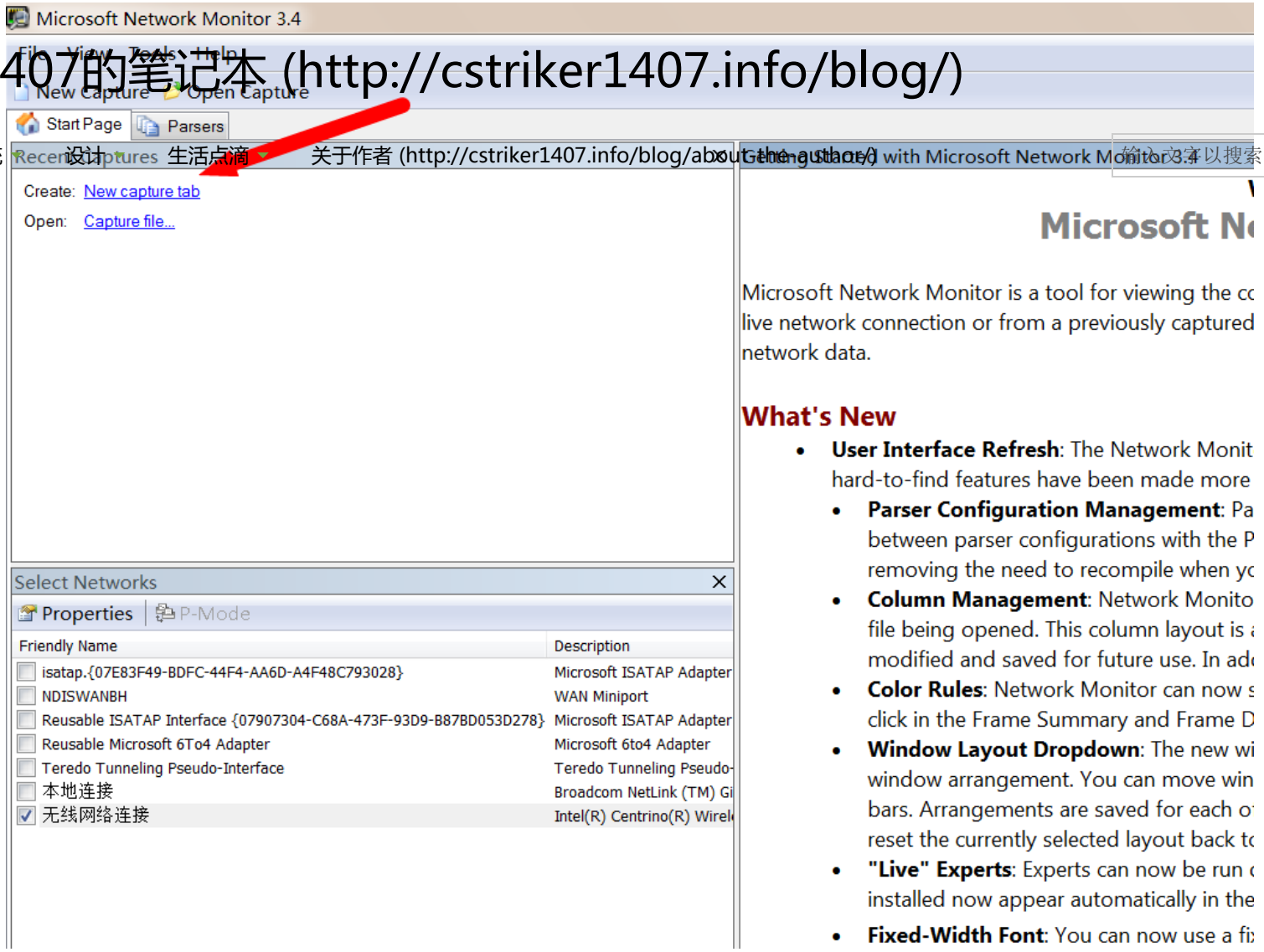
在ubuntu下抓取可以参考【 ubuntu下使用airmon-ng和wireshark抓取802.11管理包 (http://cstriker1407.info/blog/ubuntu-airmon-ng-wireshark-802-11/) 】，在windows下比较麻烦一点，这里作者个人比较喜欢第一种方式。

Contents [hide]

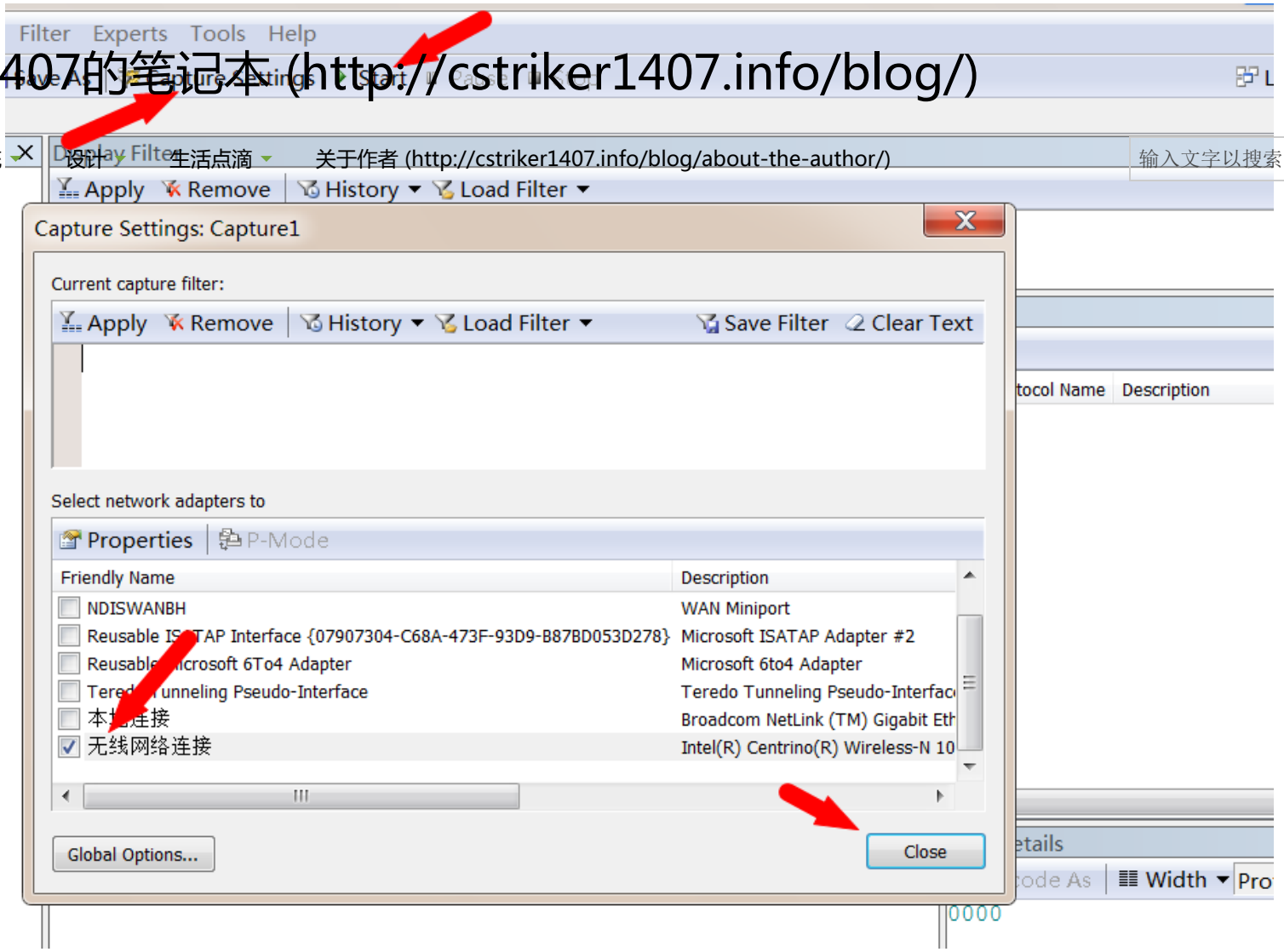
使用microsoft network monitor来抓包

MNM是微软提供的一个免费的检测工具，下载地址为【 http://www.microsoft.com/en-us/download/details.aspx?id=4865 (http://www.microsoft.com/en-us/download/details.aspx?id=4865) 】

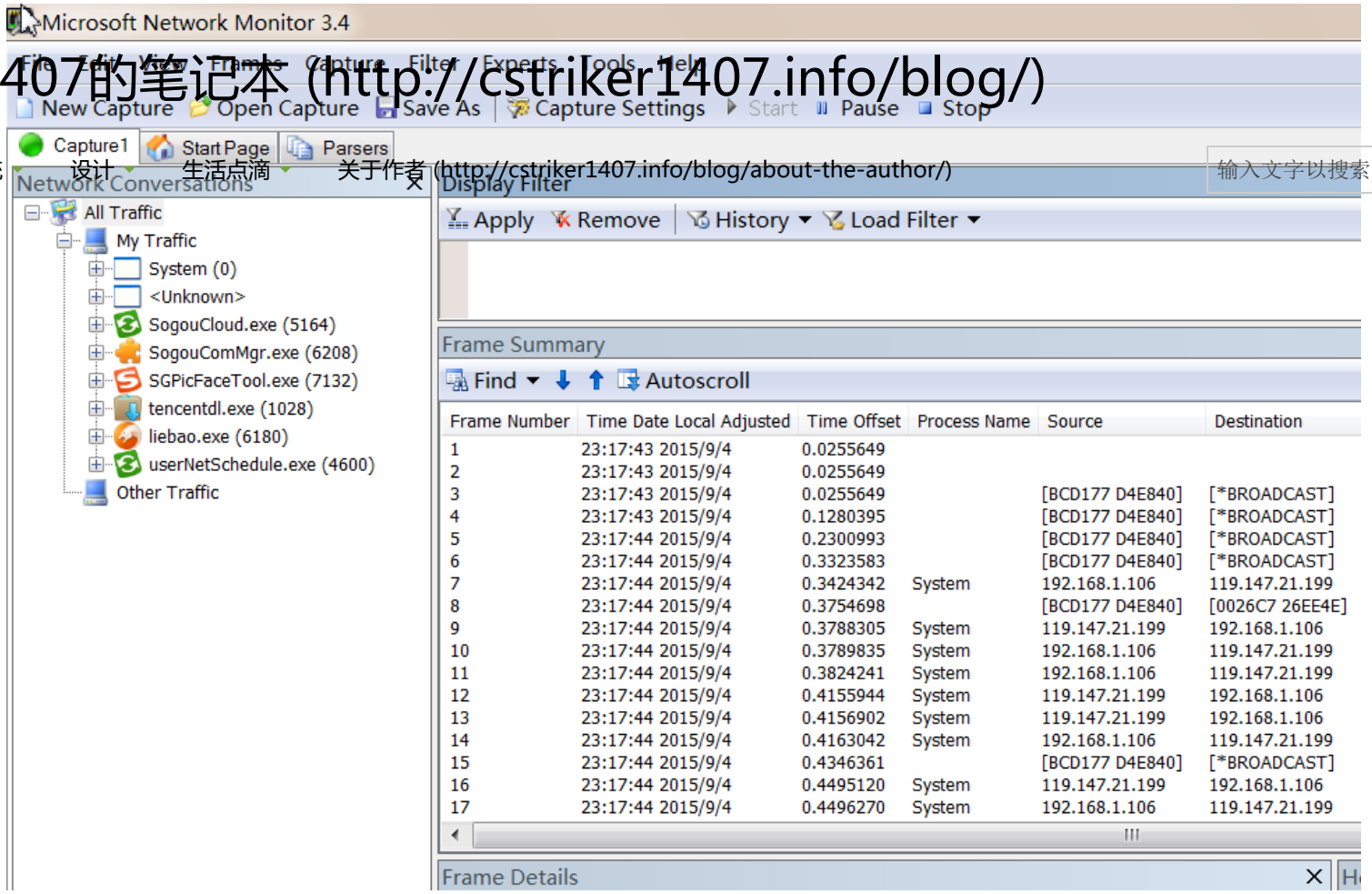
使用很简单，安装好之后打开，如果没有显示绑定的网卡，需要**退出重新登录windows**，重新登录后打开软件，如下图，就可以看到左下角有当前可用的网卡。



新建一个capture tab,然后选择【 Capture Settings 】，选择好需要抓包的网卡，然后点击【 Start 】就可以了。这里也可以先预设过滤器。如下图：



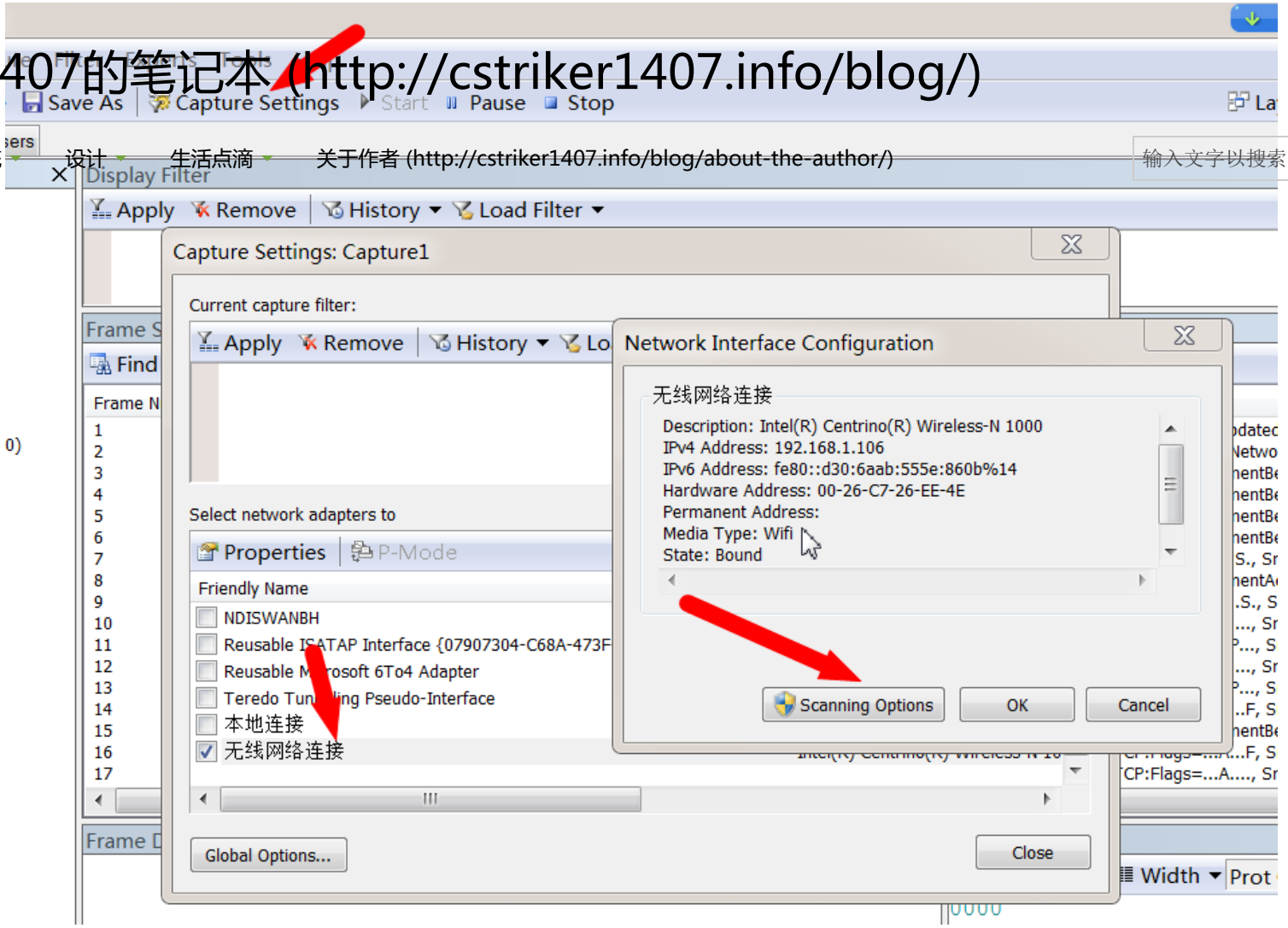
开始抓包后，如下图，可以发现该软件功能还是很强大的。可以看到每个进程访问网络的状态。



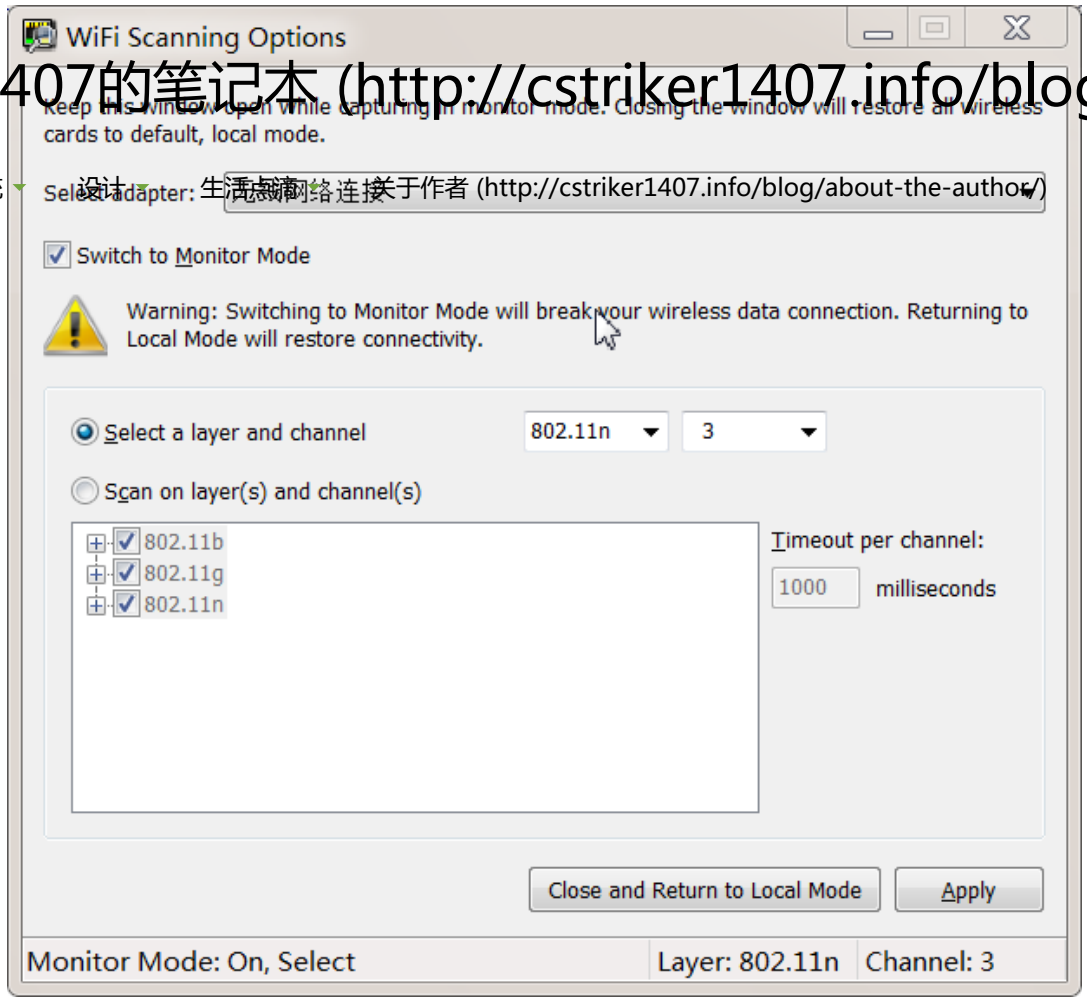
下面笔记下如何抓取802.11管理帧。
使用无线网卡抓取802.11管理帧需要启用monitor模式。由于此时会断网，WNM对该功能管理的比较严格。

首先要正常的抓包，和前面配置的一样。

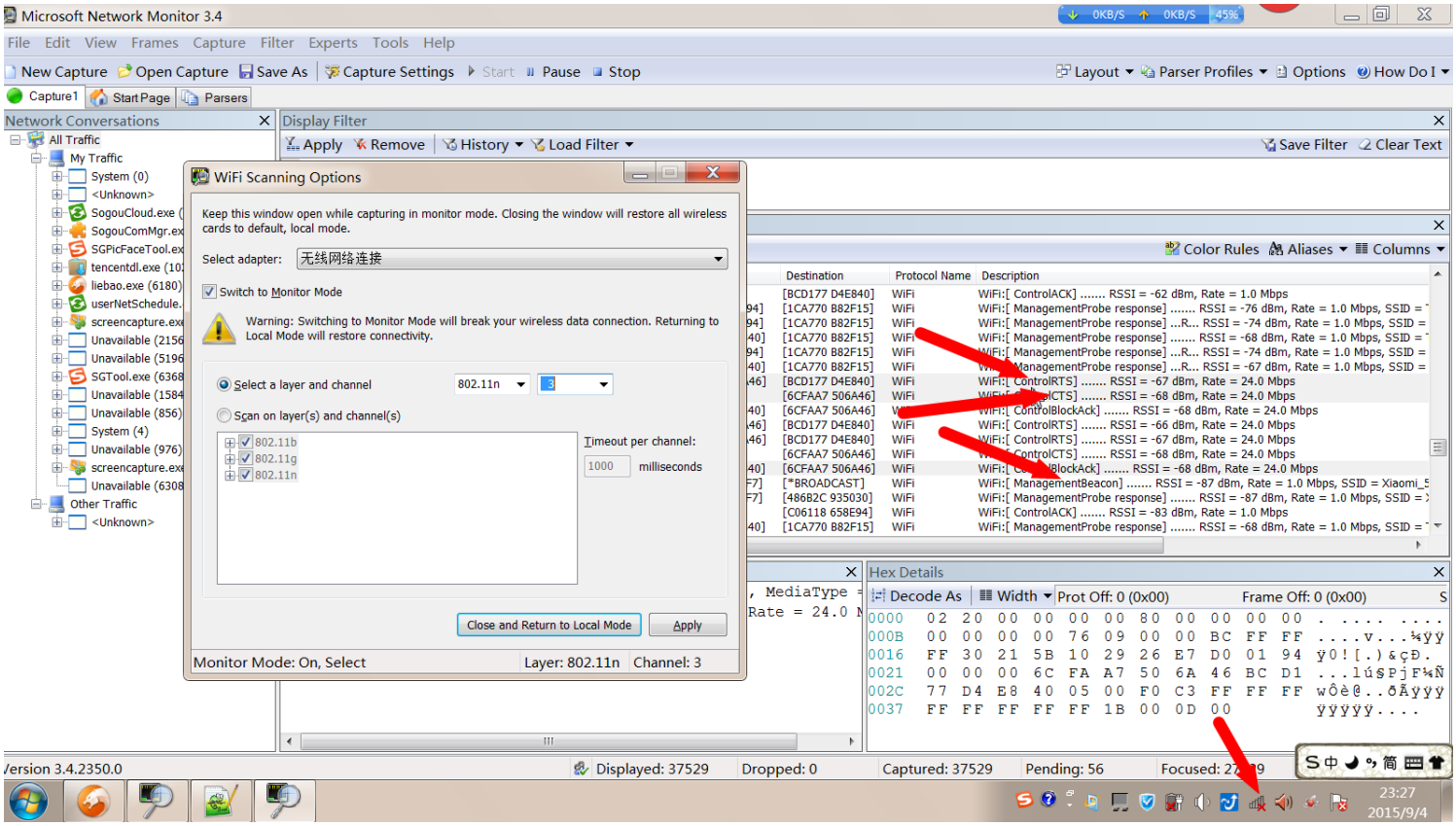
然后在抓包过程中选择【 Capture Settings 】，然后双击要修改的无线网卡【 无线网络连接 】，然后选择【 Scanning Options 】，如下图：



此时会打开高级选项，在这里可以配置无线网卡为Monitor模式，并且可以自定义的选择扫描的信道。**这里需要注意，该对话框不能关闭，如果关闭了，会自动关闭掉monitor模式**，如下图：



由于要保持该对话框关闭，**这里我们可以关闭掉其他的对话框，只保留该对话框。如果要退出monitor模式，关闭该对话框即可。**如下图：

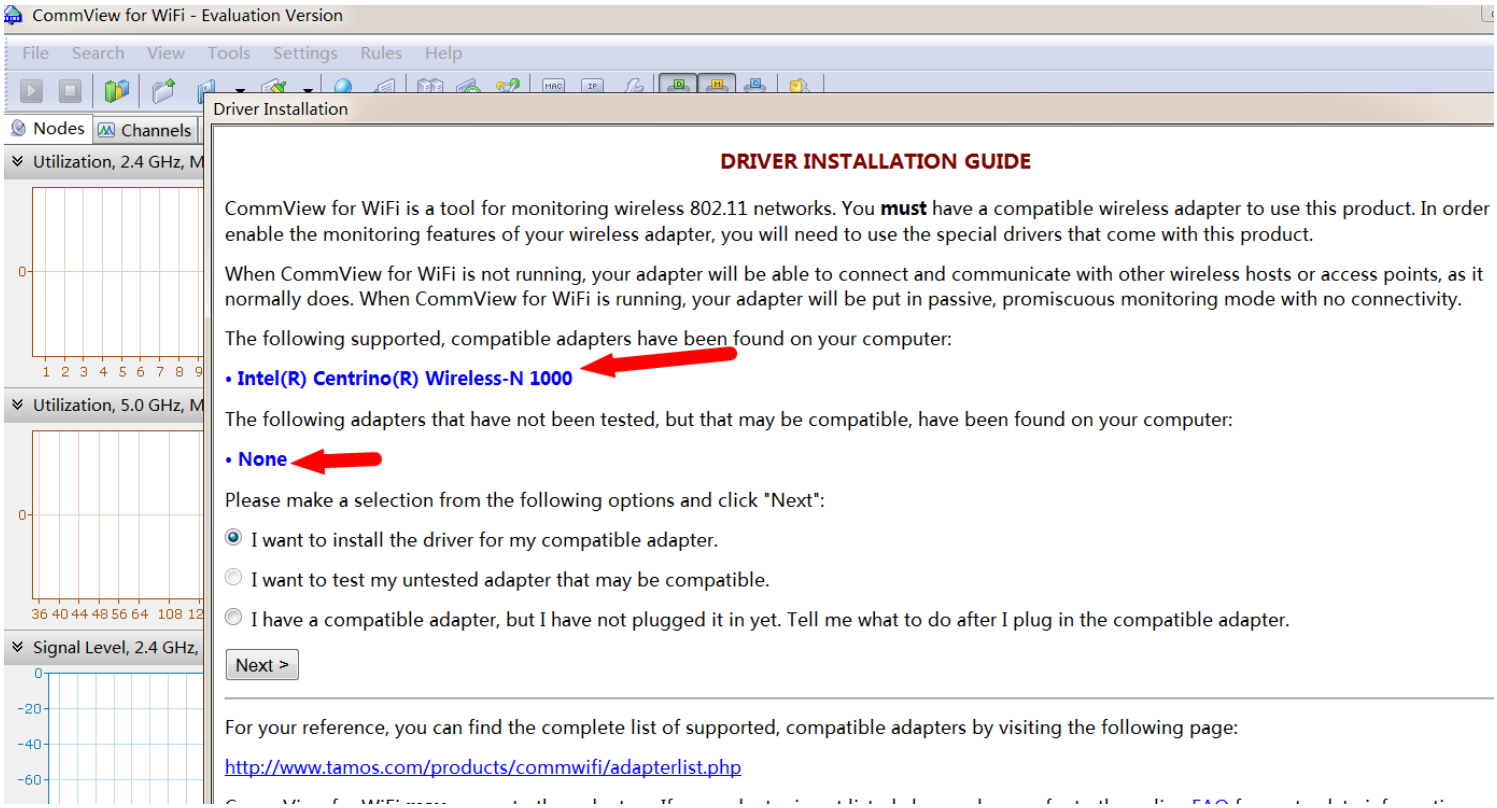


使用omnipeek

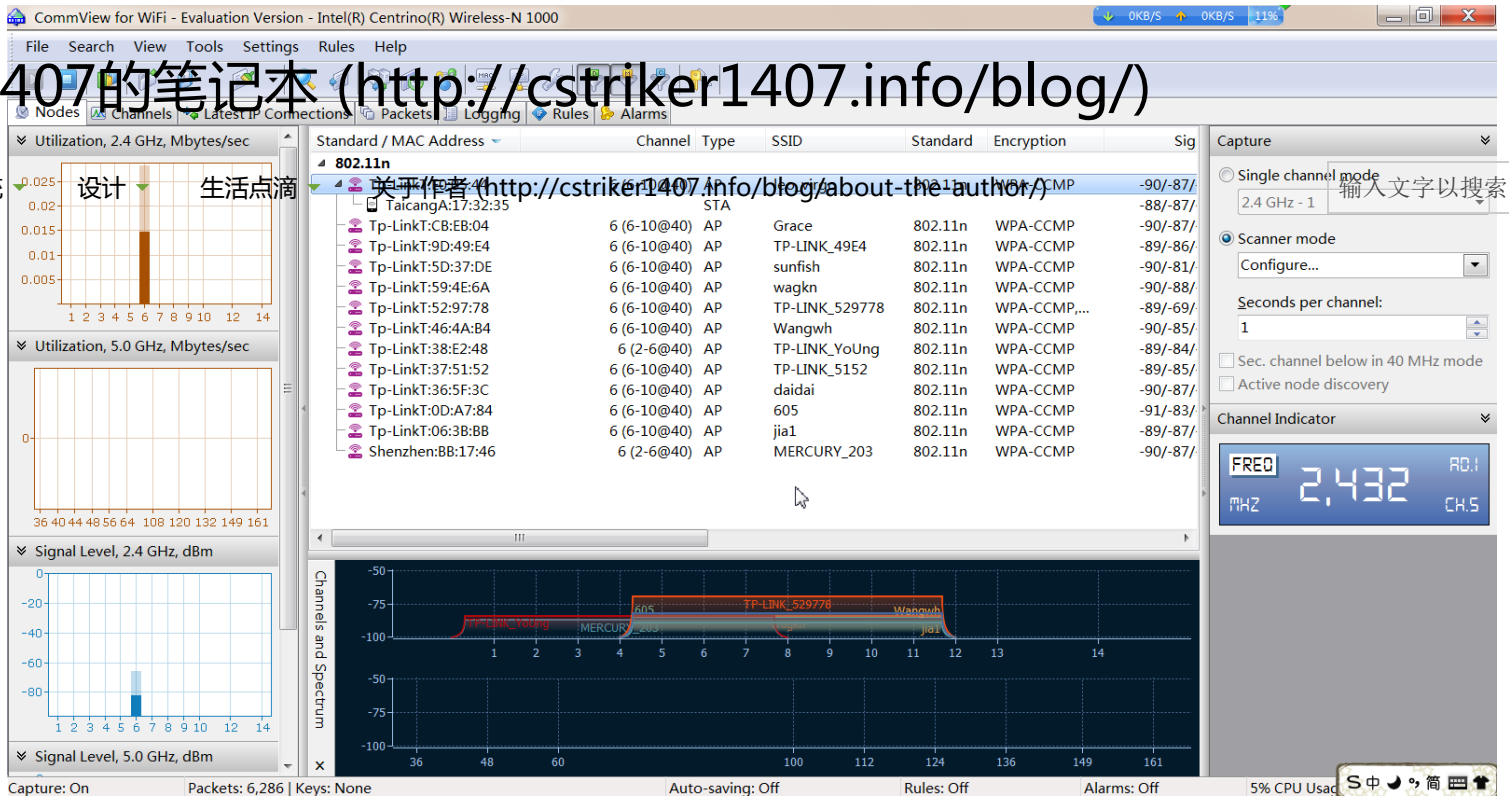
使用commview for WiFi

下载地址：http://www.tamos.cn/content/download/ (http://www.tamos.cn/content/download/)
这个软件有试用版本，是专门分析WIFI信号的，但是不知道为什么，作者没有在里面找到RTS/CTS包。

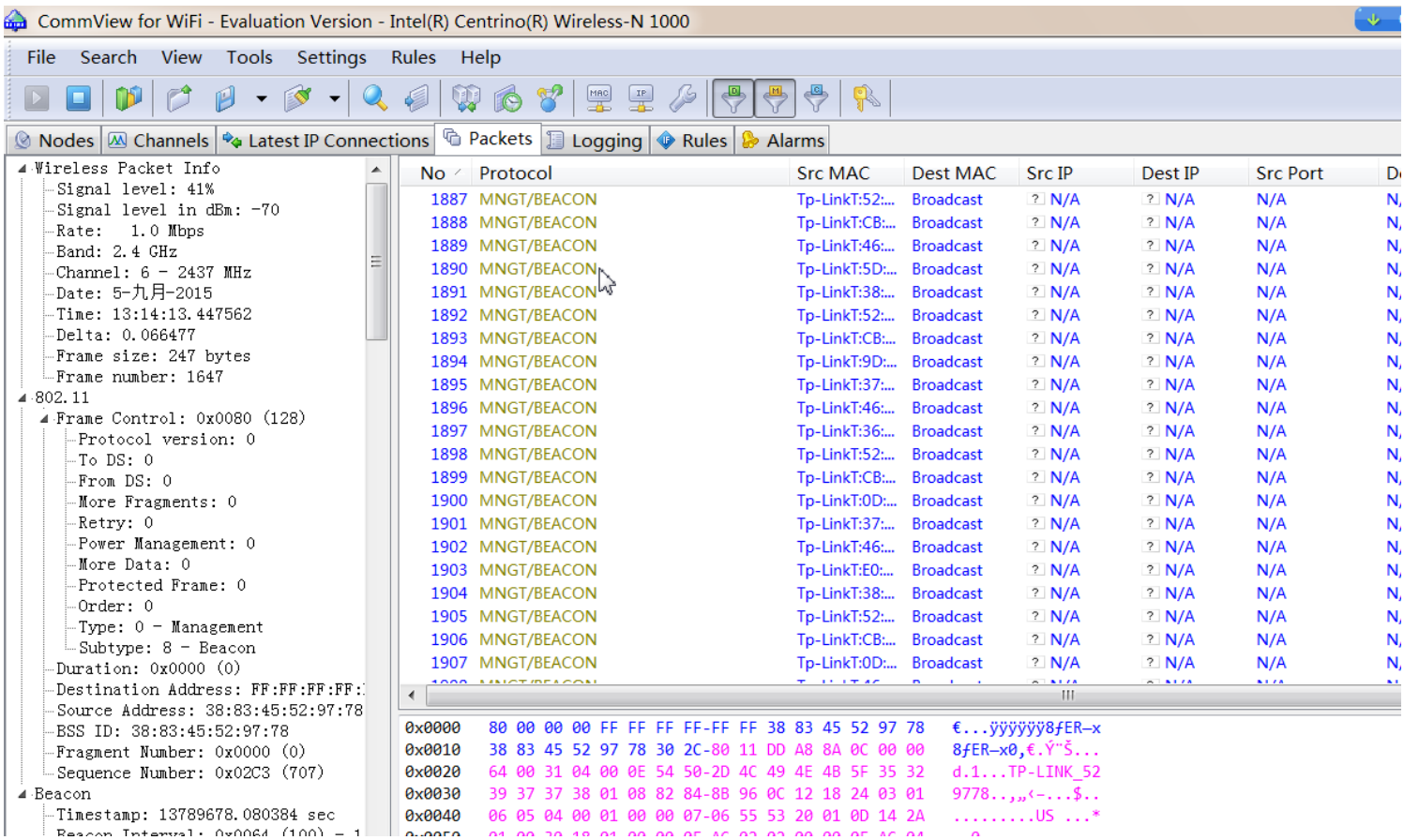
安装好之后会提示安装驱动，如下图：



使用截图如下：



和



使用aircrack-ng

在windows下使用aricrack-ng比较麻烦，而且用的人估计都是程网的。这里就简单的笔记下吧。

首先解压aircrack-ng，安装好commview，然后百度一个commview.dll拷贝到aircrack-ng的bin目录下，将commview目录下的ca2k.dll拷贝到aircrack-ng的bin目录下。管理员权限打开CMD，就可以使用airserv-ng了。

作者尝试使用wireshark来抓指定端口包，但是没有成功，也就作罢了。

相关
网络抓包工具整理 (http://cstriker1407.info/blog/network-caught-tool-finishing/)
2014年4月26日
在“安全”中

ubuntu下使用airmon-ng和wireshark抓取802.11管理包 (http://cstriker1407.info/blog/ubuntu-airmon-ng-wireshark-802-11/)
2015年8月11日
在“linux”中

kali下使用burpsuite暴力破解DVWA (http://cstriker1407.info/blog/use-kali-burpsuite-brute-dvwa/)
2014年4月26日
在“安全”中

分类 : 操作系统 (http://cstriker1407.info/blog/category/operationsystem/)

标签 : 802.11 (http://cstriker1407.info/blog/tag/802-11/)

本文链接地址：http://cstriker1407.info/blog/windows-80211-frame/ (http://cstriker1407.info/blog/windows-80211-frame/)