Panabit 应用协议样本抓包方法

（2008 年 2 月）

Panabit 自发布以来，得到了各位网友及用户的热心支持和帮助。为更好的提高 Panabit 在各用户网络中的作用与体验，对于您网络中存在的、Panabit 暂时尚未识别的应用，请按照本方法进行样本采集，通过邮件发送给 support@panabit.com。我们将尽快进行分析处理并发布更新特征库，以满足用户对这些未知应用的流量分析与管理需求，谢谢！（本方法同样适用于各合作伙伴在用户测试过程中遇到类似问题的技术人员）

一、工具软件：

推荐使用：WireShark

版本号： 0.99.6

官方下载地址：http://www.wireshark.org/download.html

二、抓包步骤：

1、 关闭所有可以访问网络的应用程序。

2、 打开 WireShark，开始抓包。操作步骤为：依次点击“Capture”---“Options”---在“Interface”行选择本机访问网络所使用的网卡名称--- “Start”(窗口右下角)。

3、 打开欲分析的应用软件，例如 Skype，捕捉一个会话的完整过程，包括“登陆 – 选择联系人 – 文字聊天或通话 – 退出”。

4、 Skype 正常应用过程中，打开 Windows 命令行程序 cmd.exe，执行 netstat –ano ，将结果拷贝到文本文件。（鼠标移入 cmd 窗口、右键“全选”、CTRL+C、创建新的 txt 文本文件、CTRL+V）

5、 点击 WireShark 窗口“Capture”下的“STOP”，停止抓包。

6、 点击 WireShark 窗口左上角“File”--- “Save As”保存文件。（文件后缀名为.cap，如 Skype-1.cap；并注意文件保存的位置。）

7、 换另一个帐号登陆 Skype，重复以上步骤。

8、 将 Skype-x.cap 各文件和步骤 4 中的文本文件同时发送邮件至：support@panabit.com

三、注意事项：

1、 多抓几次，要求提供不同帐号、不同访问/下载对象的完整过程包至少 3 个。

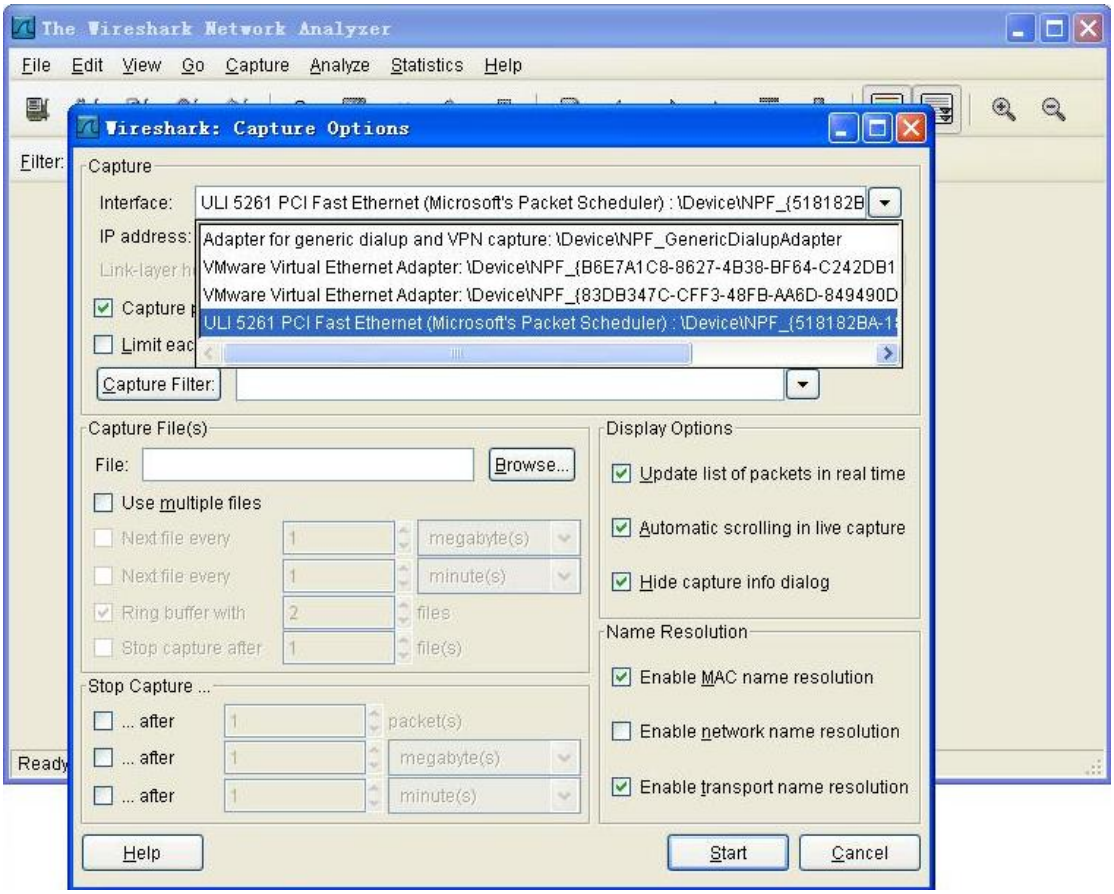
2、 抓包前关闭其他可以访问网络的程序，减少无关的干扰包。

3、 抓包后，为方便查看分析，请指定文件后缀名为 .cap 。

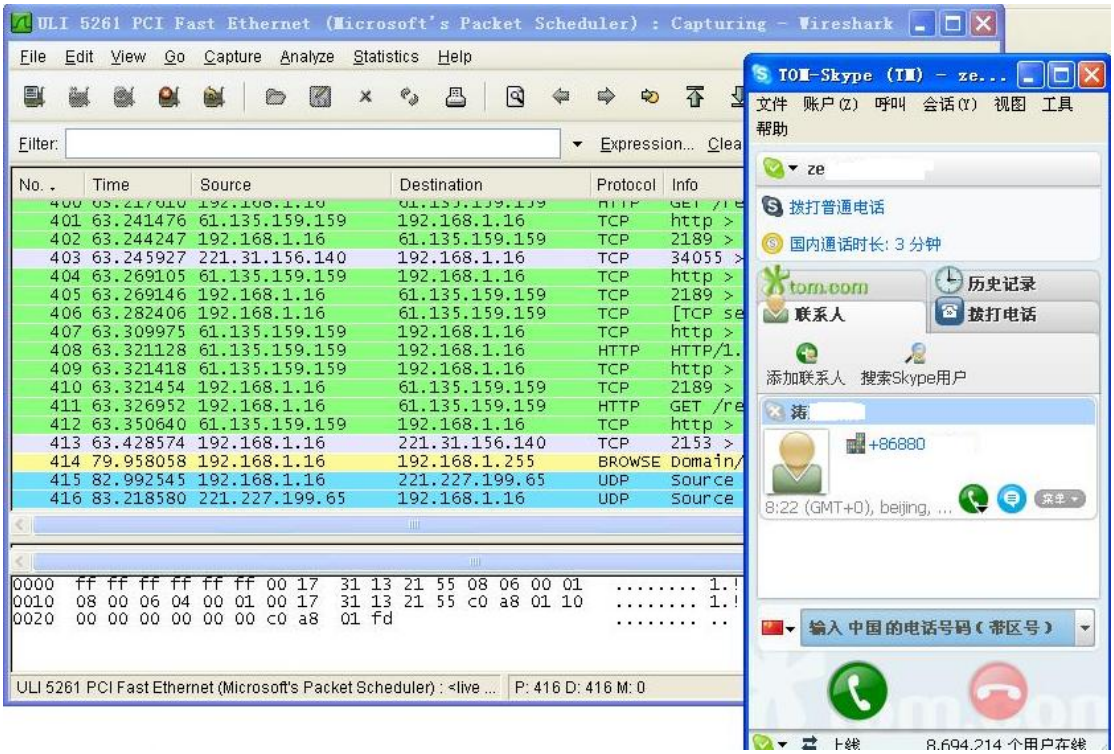
4、 保证抓包的完整性，即包括登陆 -- 正常应用 -- 退出全过程。

四、示例：Skype 抓包全过程：

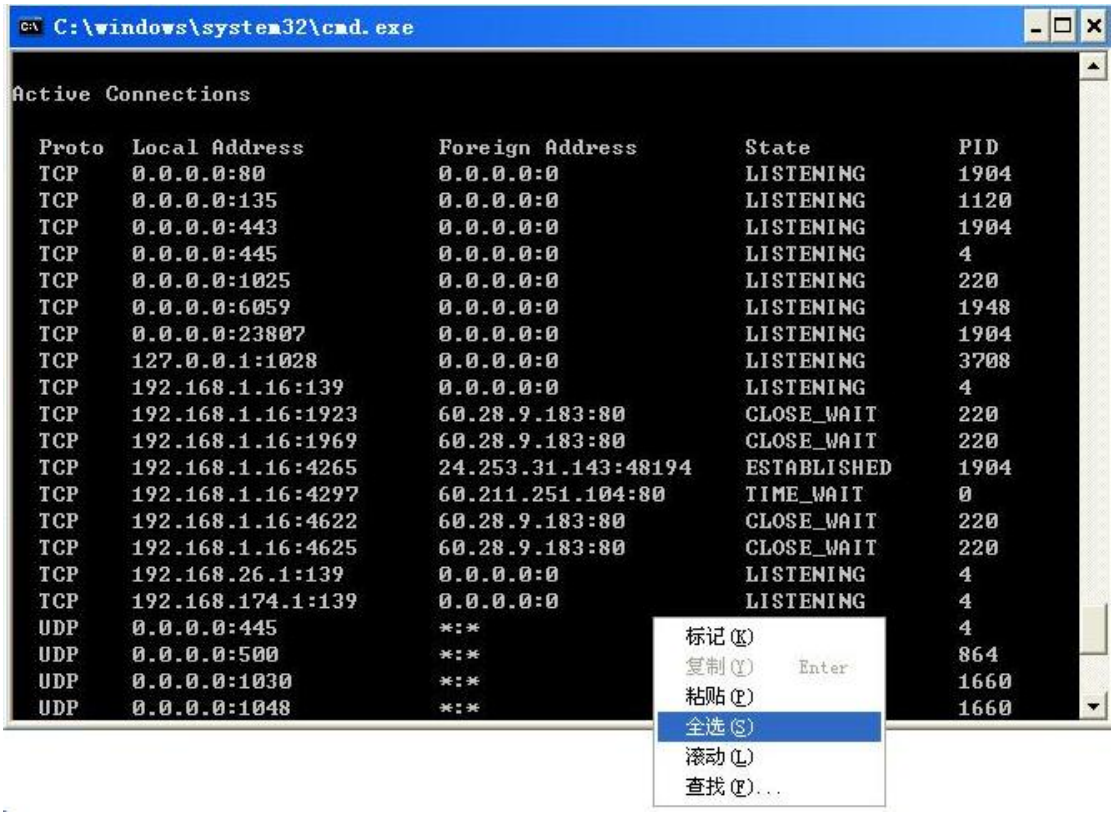
下图一、打开并执行 WireShark，依次点击“Capture”---“Options”，在最上一行“Interface”中选择本机访问网络所使用的网卡名称，点击窗口右下的“Start”。



下图二、打开 Skype，正常登陆、选中联系人、正常发送文字信息或打电话、退出。



下图三、Skype 正常登陆后的使用过程中，在 cmd 中执行 netstat –ano 并保存其信息。



下图四、将 WireShark 捕获的数据包保存为文件 Skype-1.cap。