3.4.1 第一次捕获数据包

为了能让 Wireshark 得到一些数据包，你可以开始第一次数据包捕获验了。你可能会想：「当网络什么问题也没有的时候，怎么能捕获数据包呢?」

第一，网络总是有问题的。如果你不相信，那么请给你网络上所有的户发一封邮件，告诉他们一切都工作得非常好。

第二，数据包分析并不一定要等到有问题的时候再做。事实上，大多的数据包分析员在分析没有问题的网络流量上花费的时间要比解决问题的间多。为了能高效地解决网络问题，你也同样需要得到一个基准来与之对比。举例来说，如果你想通过分析网络流量来解决关于 DHCP 的问题，那么你至少需要知道 DHCP 在正常工作时的数据流是什么样子的。

更广泛地讲，为了能够发现日常网络活动的异常，你必须对日常网络动的情况有所掌握。当你的网络正常运行时，以此作为基准，就能知道网流量在正常情况下的样子。

闲言少叙，让我们来捕获一些数据包吧!

（1）打开 Wireshark。

（2）从主下拉菜单中选择 Capture，然后是 Interface。

这时你应该可以看到一个对话框，里面列出了你可以用来捕获数据包各种设备，以及它们的 IP 地址。

（3）选择你想要使用的设备，如图 3-4 所示，然后单击 Start，或者接单击欢迎画面中 Interface List 下的某一个设备。随后数据就会在窗口中呈现出来。

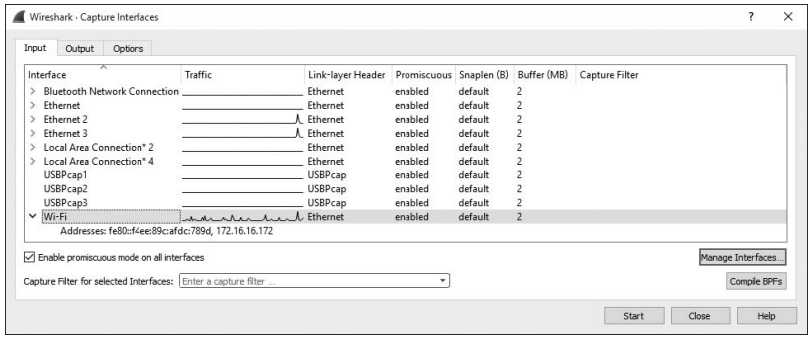

图 3-4　选择你想要进行数据包捕获的端口

（4）等上 l min 左右，当你打算停止捕获并查看你的数据的时候，在 Capture 的下拉菜单中单击 Stop 按钮即可。

当你做完了以上步骤并完成了数据包的捕获时，Wireshark 的主窗口应该已经呈现了相应的数据，但此时你可能对于那些数据的规模感到头疼这也就是我们把 Wireshark 一整块的主窗口进行拆分的原因。