4.5.4 在工具栏中增加显示过滤器

如果你有一些经常用的过滤器，那么不妨把过滤器切换添加到包列表上面的过滤器栏中，这样方便你去调用。要实现这个功能，请依照下列步骤操作。

（1）在显示过滤器的条框里键入表达式，然后单击在条框右面的（+）按钮。

（2）一个新的条框会在下方出现，这时在 Label 区框里键入过滤器的名字（见图 4-19）。以该名字生成的标签将会在工具栏里代表这个过滤器。最后单击 OK，就可以把代表这个表达式的快捷标签加入工具栏。

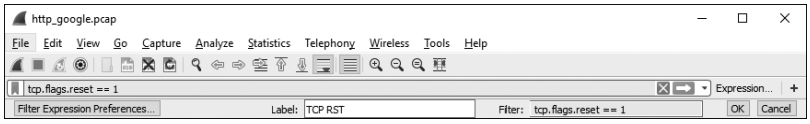

图 4-19　在过滤工具栏中增加过滤表达式标签

如图 4-20 所示，我们已经在过滤工具栏里制作了一个快捷标签，按下便可以迅速过滤出所有带 RST 标志位的 TCP 包。就像第 3 章介绍的那样，这些额外的快捷标签会保存在你个人的配置文档里。这个强大的功能极大地增强了你在不同抓包场景下找出问题的能力。

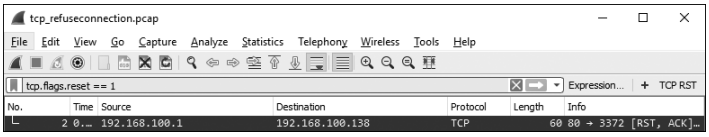

图 4-20　使用快捷标签来过滤

Wireshark 内置的许多过滤器可以作为过滤器规则范例。你在创建自己的过滤器时，可能会用到它们（可参考 Wireshark 帮助页面）。我们在整本书的例子中都会用到过滤器。

---

[1] Update list of packets in real time：实时更新数据包列表；Automatic scrolling in live capture：在当前捕获中进行自动滚动。——译者注