3.4.4 数据包彩色高亮

如果你像我一样喜欢五颜六色的物体，那么你应该会对 Packet List 面板中那些不同的颜色感到兴奋。如图 3-7 所示（虽然图示是黑白的，但你该可以理解的），那些颜色看上去就像是随机分配给每一个数据包的，但其实并不是这样的。

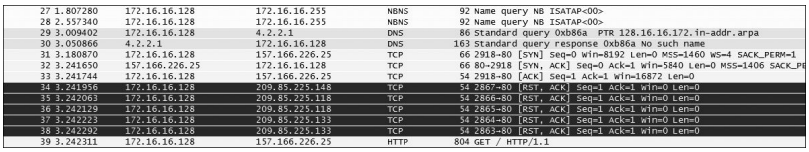

图 3-7　Wireshark 的彩色高亮有助于快速标识协议

每一个数据包的颜色都是有讲究的，这些颜色对应着数据包使用的协议。举例来说，所有的 DNS 流量都是蓝色的，而 HTTP 流量都是绿色的。将数据包进行彩色高亮，可以让你迅速将不同协议的数据包分开，而不需查看每个数据包的 Packet List 面板中的协议列。你会发现这样做在浏览较大的捕获文件时，可以极大地节省时间。

如图 3-8 所示，Wireshark 通过 Coloring Rules（着色规则）窗口可轻松地查看每个协议所对应的颜色。如果想要打开这个窗口，那么可以在下拉菜单中选择 View 并单击 Coloring Rules。

你可以创建你自己的着色规则，或者修改已有设置。举例来说，使用列步骤可以将 HTTP 流量绿色的默认背景改成淡紫色。

（1）打开 Wireshark，并且打开 Coloring Rules 窗口（View->Coloring Rules）。

（2）在着色规则的列表中找到 HTTP 着色规则并单击选中。

（3）单击 Edit 按钮，你会看到一个 Edit Color Filter 窗口，如图 3-9 示。

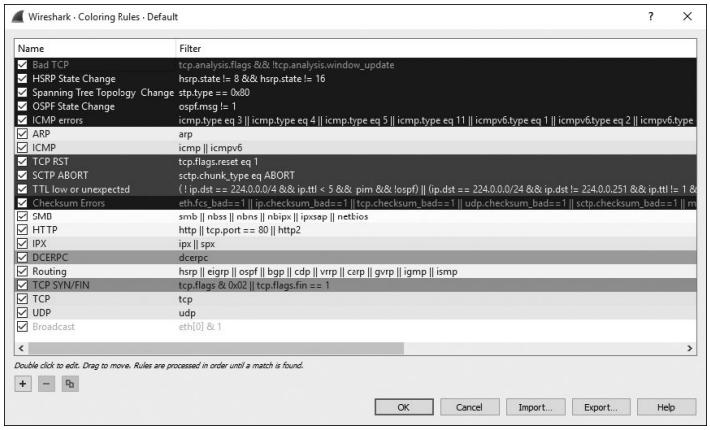

图 3-8　你可以在 Coloring Rules 窗口中查看并更改数据包的着色

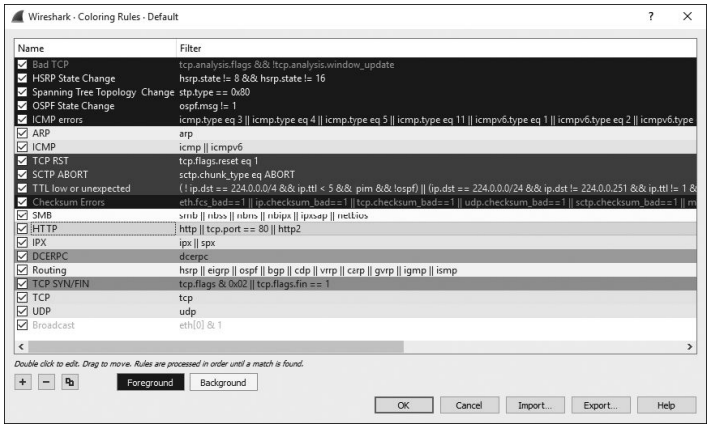

图 3-9　在编辑着色过滤器时，前景色和背景色都可以进行更改

（4）单击 Background Color 按钮。

（5）使用颜色滚轮选择一个你希望使用的颜色，然后单击 OK。

（6）再次单击 OK 来应用改变，并回到主窗口。主窗口此时应该已经载，并使用了更改过的颜色样式。

当在网络上使用 Wireshark 时，可能会发现你处理某个协议的工作要其他协议多得多。这时彩色高亮的数据包能让你的工作更加方便。举例来说，如果你觉得你的网络上有一个恶意的 DHCP 服务器在分发 IP，那么你可以简单地修改 DHCP 协议的着色规则，使其呈现明黄色（或者其他易于辨认的颜色）。这可以使你更快地找出所有 DHCP 流量，并让你的数据包析工作更具效率。你还可以通过基于定制的过滤器创建着色规则，来扩展些着色规则的使用。

> 注意
>
> 就在前不久，我在给本地一群学生展示 Wireshark 的着色规则时，有一名学生是色盲，但他通过修改着色规则分辨出了以前无法分辨出的协议。这说明了修改着色规则的功能对视觉残障人提供了一定程度上的可用性。