5.7.1 查看 IO 图

Wireshark 的 IO 图窗口允许你对网络上的吞吐量进行绘图。你可以利用这些图，找到数据吞吐的峰值，找出不同协议中的性能时滞，以及比较实时数据流。

打开 download-fast.pcapng，单击任意一个 TCP 数据包并将其高亮，然后选择 Statistics->IO Graphs，就可以看到一台计算机在从互联网上下载文件时的 IO 图的例子。

这个 IO 图窗口显示了数据流随时间变化的一个图形化视图。在图 5-17 这个例子中所显示的下载量可知，每个周期大约有 500 个数据包，其过程中在一定程度上保持不变并在最后逐渐减少。

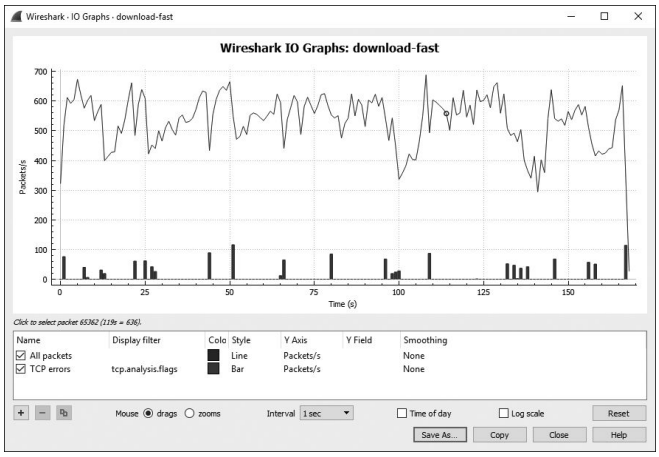

图 5-17　快速下载的 IO 图基本上是稳定的

我们可以将它与一个较慢的下载过程做比较。不要关闭当前这个文件，然后另外再启动一个 Wireshark 并打开 download-slow.pcapng。打开这个下载过程的 IO 图，如图 5-18 所示，便可以看到与之前大为不同。

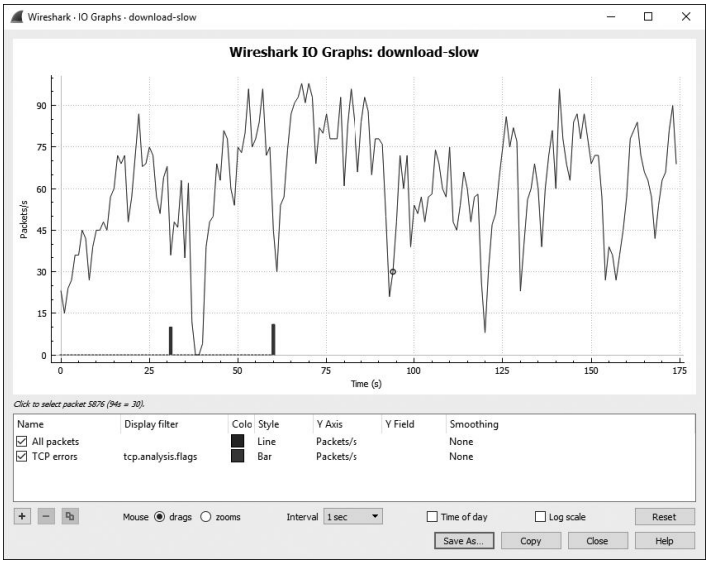

图 5-18　慢速下载的 IO 图特别不稳定

这个下载过程每秒传输的数据包为 0～100 个，并且浮动很大，其中也曾暂时接近每秒 0 个数据包。如果你将这两个捕获文件的 IO 并排放置，就能更清楚地看到这些浮动（见图 5-19）。当比较两幅图时，注意正确地比较 x 轴和 y 轴的值。图中的缩放比例会自动按照包和/或数据的传输量来调整，这也是图 5-19 中左右两幅图的主要区别。下载速度较慢的程序显示 0～100 个数据包/秒，下载较快的程序显示 0～700 个数据包/秒。

你应该可以注意到这个窗口的下面有一些配置选项。你可以创建多个不同的过滤器（使用与显示或者捕获过滤器相同的语法），并为这些过滤器指定显示的颜色。例如，你可以把特定的 IP 过滤出来，并且给它们分配独特的颜色，以查看每个设备不同的吞吐量。让我们来试一试吧。

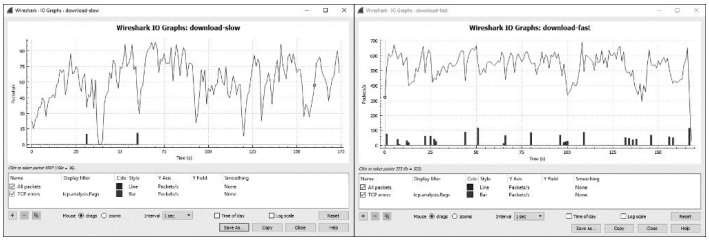

图 5-19　并排查看多个 IO 图有助于发现它们之间的差异

打开 http_espn.pcapng，这是在一个设备访问 ESPN[1]主页时捕获的。如果观察会话窗口，你会看到有着最大用量的外网 IP 是 205.234.218.129。我们可以由此推断，这台主机就是当访问 ESPN 时数据的主要提供源。然而，也有一些其他 IP 参与到通信中，这有可能是因为一部分内容从其他外网内容提供者或广告商处下载而来。我们使用图 5-20 所示的 IO 图可以识别出第一和第三方内容提供者的不同。

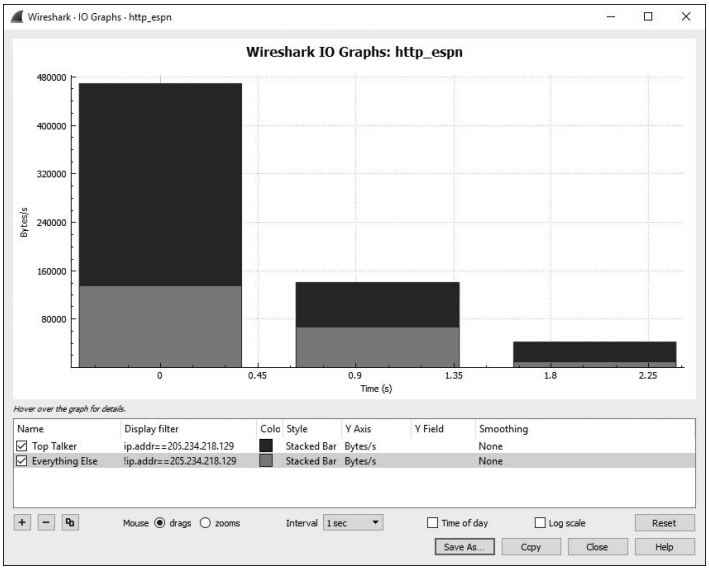

图 5-20　显示两个不同设备的 IO 图

图中所应用的两个过滤器，以行的形式在窗口下方表示。名为 Top Talker 的过滤器只显示 IP 地址为 205.234.218.129（主要内容提供者）的 IO 情况，在图中用黑色的条形柱表示。第二个名为 Everything Else 的过滤器只显示除去 205.234.218.129 外的所有 IO（第三方内容提供者）情况，在图中用红色条形柱表示（在这里是灰色）。注意，我们把 y 轴单位变成了字节每秒。这个单位能让我们非常容易地看到第一和第三方内容提供者 IO 的差异。你可以在经常访问的网站上做一做这个有趣的练习，这也是一项比较不同网络主机间 IO 的有用策略。