5.1.2 查看网络会话

打开 lotsofweb.pcapng 后，访问 Wireshark 的会话窗口（Statistics->Conversations）来显示所有在捕获文件中的会话，如图 5-3 所示。会话窗口和端点窗口看起来很像，但会话窗口展示的是一行两个地址组成的会话，以及每个设备发送或收到的数据包和字节数。地址 A 列代表着源端点，地址 B 列代表着目的端点。

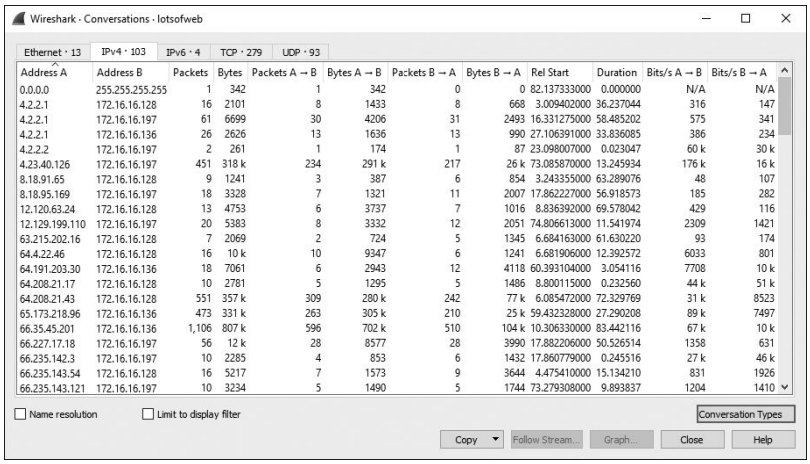

图 5-3　会话窗口可以让你与捕获文件中的每个会话进行交互

这个窗口中列出的会话以不同的协议分开。要查看针对一个协议的会话，可单击其中一个窗口顶部的选项卡进行切换或者在右下角增加一个其他的协议类型。就像在端点窗口里的操作一样，你可以使用名称解析、通过显示过滤器限制可见会话、右键单击一个特定的会话，来创建基于该会话的过滤器。基于会话的方式来过滤流量可以帮助你深入研究一些有趣的交互序列中的细节。