5.1.1 查看端点统计

当分析流量时，你也许会察觉到可以将问题定位到网络中的一个特定端点上去。举例来说，依次打开捕获文件*lotsofweb.pcapng*和 Wireshark 的 Endpoints 窗口（Statistics->Endpoints）。这个窗口给出了各个端点的许多有用的统计数据，如图 5-2 所示，包括每个端点的地址、传输发送数据包的数量和字节数。

这个窗口顶部的选项卡（TCP、Ethernet、IPv4、IPv6 和 UDP）根据协议将当前捕获文件中所有支持和被识别的端点进行分类。单击其中一个选项卡，就可以只显示针对一个具体协议的端点。单击窗口右下角的 EndpointTypes 多选框，就可以添加额外的协议过滤标签。勾选 Name resolution 多选框，可以开启名称解析功能来查看端点地址。如果你在处理大流量且需要过滤出所显示的端点数据，那么你可以事先在 Wireshark 主窗口里应用显示过滤器，然后在端点窗口勾选 Limit to display filter 多选框。这个选项会让端点窗口只显示与显示过滤器相匹配的端点。

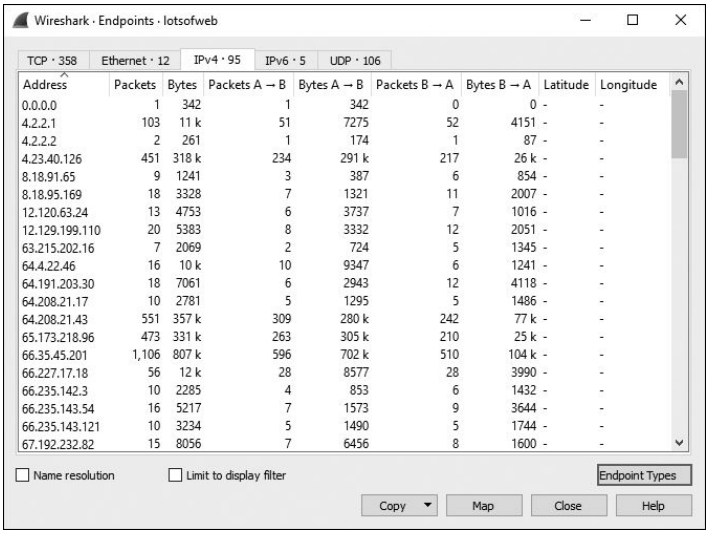

图 5-2　端点窗口可以让你查看一个捕获文件里的每个端点

另一个便利的功能就是你可以使用端点窗口将特定的数据包过滤出来，使其显示在 Packet List 面板中。这是快速锁定某个端点相关数据包的方法。右键单击一个特定的端点，可以看到许多选项，包括创建过滤器以显示只与这个端点关联的流量，或者与选定端点无关的所有流量。你还可以在下拉菜单里选择着色（Colorize）选项，这会直接把当前端点地址转化为一条着色规则（着色规则在第 4 章有所讨论）。用这种方法，你可以批量高亮与一个端点有关的包，以便于你在后续分析中可以很快地定位到它们。