5.4.2 查看解析器源代码

开源软件的美妙之处就在于，当对正在进行的事情感到困惑时，你可以直接查看源代码来找到具体原因。当你想查明一个特定的协议没有被正确解析的原因时，这一点就变得非常顺手了。

在 Wireshark 网站上的 Develop 链接中，单击 Browse the Code，就可以直接查看协议解析器的源代码。这个链接直接指向 Wireshark 的代码仓库，里面有 Wireshark 的最新以及之前的发行版。单击 releases 文件夹，便能看见所有官方的 Wireshark（甚至包括 Ethereal）发行版，其中最新版将在最下面显示出来。在你选择了想要查看的发行版之后，在*epan/dissectors*文件夹下可以找到协议解析器。每一个解析器都以*packets-<protocolname>.c*（数据包-协议名称.c）的形式命名。

这些文件可能会很复杂，但你应该可以发现它们都遵循着同一个标准模板并有着详细的注释。你并不需要成为一个 C 语言专家，就可以理解每一个解析器的基本功能。如果你想深入理解在 Wireshark 中所看到的，我强烈建议你至少看一些简单协议的解析器。