3.4.2 Wireshark 主窗口

Wireshark 的主窗口将你所捕获的数据包拆分并以更容易使人理解的式呈现出来，它也将是你花费时间较多的地方。我们使用刚刚捕获的数据来介绍一下 Wireshark 的主窗口，如图 3-5 所示。

主窗口的 3 个面板之间有着互相的联系。如果希望在 Packet Details 板中查看一个单独的数据包的具体内容，那么你必须在 Packet List 面板中单击选中那个数据包。在选中了数据包之后，你可以在 Packet Details 面中选中数据包的某个字段，从而在 Packet Bytes 面板中查看相应字段的字节信息。

> 注意
>
> 图 3-5 中的 Packet List 面板中列出了几种不同的协议，但这里并没有使用不同的层次来对不同的协议进行视觉上的区分，所有的数据包都是按照其在链路上接收到的顺序排列的。

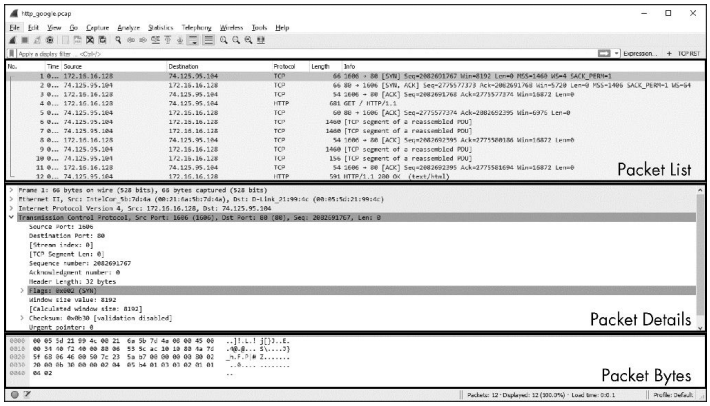

图 3-5　Wireshark 主窗口的设计使用了 3 个面板

下面介绍了每个面板的内容。

Packet List（数据包列表）：这个最上面的面板用表格显示了当前捕获文件中的所有数据包，其中包括了数据包序号、数据包被捕获时的相对时间、数据包的源地址和目标地址、数据包的协议以及在数据包中找到的概信息等列。

> 注意
>
> 当文中提到流量的时候，我通常是指 Packet List 面板中所有呈现出来的数据包，而当特别提到 DNS 流量时，我指的是 Packet List 面板中 DNS 协议的数据包。

Packet Details（数据包细节）；这个中间的面板分层次地显示了一个
据包中的内容，并且可以通过展开或是收缩来显示这个数据包中所捕获到
全部内容。

Packet Bytes（数据包字节）；这个最下面的面板可能是最令人困惑的
因为它显示了一个数据包未经处理的原始样子，也就是其在链路上传播时
样子。这些原始数据看上去一点都不舒服而且不容易理解。