跟踪 SSL 流

跟踪 TCP 和 UDP 流是一个简单的双击操作，但以可读的形式查看 SSL 流还需要额外的步骤，因为流量都是加密的，所以你必须提供与服务器加密所对应的私钥。获取私钥的方法取决于服务端所使用的技术，这不在本书的探讨范围内。但是一旦有了私钥，你就可以按照以下步骤把它加载到 Wireshark 里。

（1）单击 Edit->Preferences 进入 Wireshark 选项设置。

（2）展开协议（Protocols）部分并且选择 SSL 协议标题，如图 5-15 所示。

（3）单击加号（+）按钮。

（4）提供所需要的信息，包括加密服务器的 IP 地址、端口、协议、密钥文件地址和密钥文件所使用的密码（如果需要的话）。

（5）重启 Wireshark。

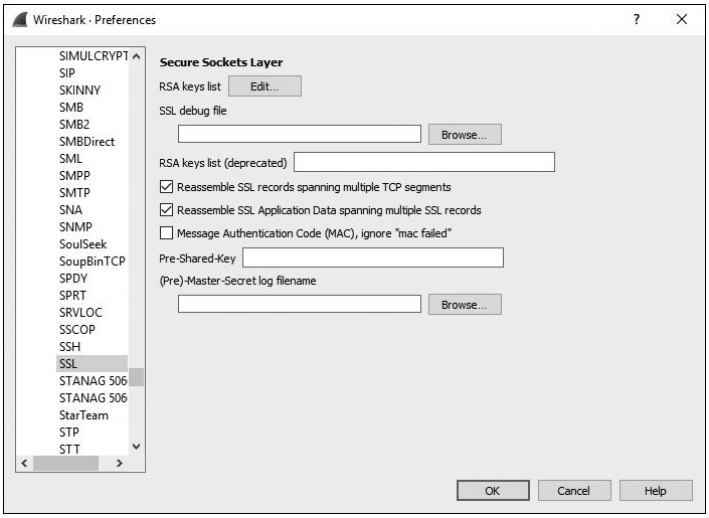

图 5-15　添加 SSL 解密信息

如果一切顺利的话，你就可以捕获客户端和服务器之间的加密流量了。右键单击一个 HTTPS 的包，然后单击 Follow SSL Stream，然后你就可以清晰地看到这一串 SSL 流的明文内容了。

查看数据包脚本是 Wireshark 中的一个常用的分析功能，你将依赖它来快速确定正在使用的特定协议。我们将在后面的章节中介绍几个其他的依赖于查看数据包脚本的方案。