3.1 Wireshark 简史
3.2 Wireshark 的优点
3.3 安装 Wireshark
3.3.1 在微软 Windows 系统…
3.3.2 在 Linux 系统中安装
3.3.3 在 Mac OS X 系统中安装
3.4 Wireshark 初步入门
3.4.1 第一次捕获数据包
3.4.2 Wireshark 主窗口
3.4.3 Wireshark 首选项
3.4.4 数据包彩色高亮
3.4.5 配置文件
3.4.6 配置方案
章 玩转捕获数据包
4.1 使用捕获文件
4.1.1 保存和导出捕获文件
4.1.2 合并捕获文件
4.2 分析数据包
4.2.1 保存和导出捕获文件
4.2.2 标记数据包
4.2.3 打印数据包
4.3 设定时间显示格式和相对参考
4.3.1 时间显示格式
4.3.2 数据包的相对时间参考
4.3.3 时间偏移

3.4.3 Wireshark 首选项

Wireshark 提供一些首选项设定可以让你根据需要进行定制。如果需设定 Wireshark 首选项，那么需要在主下拉菜单中选择 Edit 并单击 Preferences，然后你便可以看到一个首选项的对话框，里面有一些可以定制的选项，如图 3-6 所示。

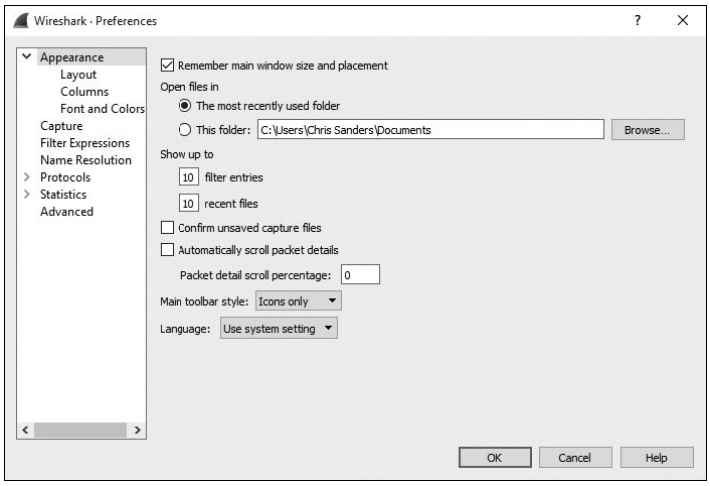

图 3-6　你可以使用 Preferences 对话框中的选项自定义 Wireshark 的配置

Wireshark 首选项分为 6 个主要部分，外加 1 个高级选项。

Appearance（外观）：这些选项决定了 Wireshark 将如何显示数据。可以根据个人喜好对大多数选项进行调整，比如是否保存窗口位置、3 个要窗口的布局、滚动条的摆放、Packet List 面板中列的摆放、显示捕获数据的字体、前景色和背景色等。

Capture（捕获）：这些选项可以让你对于自己捕获数据包的方式进行殊设定，比如你默认使用的设备、是否默认使用混杂模式、是否实时更新 Packet List 面板等。

Filter Expressions（过滤器表达式）：在之后的章节里我们将探讨 Wireshark 是如何让你基于设定标准去过滤流量的。这个部分中的选项可让你生成和管理这些过滤器。

Name Resolutions（名称解析）：通过这些设定，你可以开启 Wireshark 将地址（包括 MAC、网络以及传输名称解析）解析成更加容易分辨的名字这一功能，并且可以设定并发处理名称解析请求的最大数目。

3.1 Wireshark 简史
3.2 Wireshark 的优点
3.3 安装 Wireshark
3.3.1 在微软 Windows 系统…
3.3.2 在 Linux 系统中安装
3.3.3 在 Mac OS X 系统中安装
3.4 Wireshark 初步入门
3.4.1 第一次捕获数据包
3.4.2 Wireshark 主窗口
3.4.3 Wireshark 首选项
3.4.4 数据包彩色高亮
3.4.5 配置文件
3.4.6 配置方案
章 玩转捕获数据包
4.1 使用捕获文件
4.1.1 保存和导出捕获文件
4.1.2 合并捕获文件
4.2 分析数据包
4.2.1 保存和导出捕获文件
4.2.2 标记数据包
4.2.3 打印数据包
4.3 设定时间显示格式和相对参考
4.3.1 时间显示格式
4.3.2 数据包的相对时间参考
4.3.3 时间偏移

Protocols （协议）： 这个部分中的选项可以让你调整关于捕捉和显示
种 Wireshark 解码数据包的功能。虽然并不是针对每一个协议都可以进行
整，但是有一些协议的选项可以进行更改。除非你有特殊的原因去修改这
选项，否则最好保持它们的默认值。

Statistics （统计）： 这一部分提供了 Wireshark 中统计功能的设定选
在第 5 章节我们会对之进行更深入的学习。

Advanced （高级）： 在以上 6 个部分中没有做的设置会被归类到这里
通常这些设置只有 Wireshark 的高级用户才会去修改。