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

3.4.6 配置方案

学习了 Wireshark 的参数配置后，有些时候会发现你在使用一种配置案但很快又要切换到另一种配置方案的应用场景。其实我们没必要每次都新手动设置这些选项，Wireshark 引入了个性化配置方案，让用户可以保一组配置。

一个配置方案储存了下面的设置。

- Preferences 参数选项。
- Capture filters 捕获过滤器。
- Display filters 显示过滤器。
- Coloring rules 着色规则。
- Disabled protocols 已禁用的协议。
- Forced decodes 强制解码。
- Recent settings 最近设置，比如窗格大小、菜单设置和列宽。
- Protocol-specific tables 针对特定协议的表格，例如 SNMP 用户和自定义 HTTP 头。

要查看配置方案列表，可以在主下拉菜单单击 Edit，并选择 Configuration Profiles 选项。另一种办法是在屏幕的右下角单击右键并选择 Manage Profiles 选项。当处在配置方案的那个窗口时，你将会看到 Wireshark 的预设配置方案，它包含了如图 3-11 所示的「缺省」、「蓝牙」和「经典」方案。其中「Latency Investigation」方案是我自定义的方案它被显示为正体，而其他系统全局或默认的方案被显示为斜体。

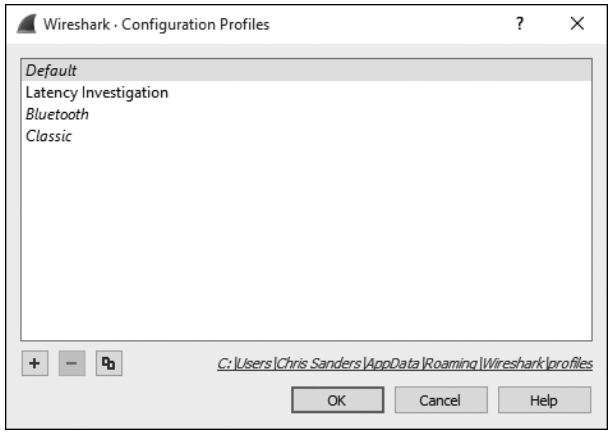

图 3-11　查看配置方案

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

配置方案窗口可以让你创建、复制、删除和应用配置方案。创建一个的配置方案是非常简单的。

（1）把 Wireshark 设置成你想要储存的配置。

（2）在主下拉菜单单击 Edit，并选择 Configuration Profiles 选项，调出配置方案窗口。

（3）单击加号（+）按钮并且给该方案取名。

（4）单击 OK。

当你想切换配置方案时，在配置方案窗口下选择方案名，然后单击 O即可。有一种更快的方法，就是在屏幕的右下角单击配置文件，然后直接择你想要的那个方案，如图 3-12 所示。

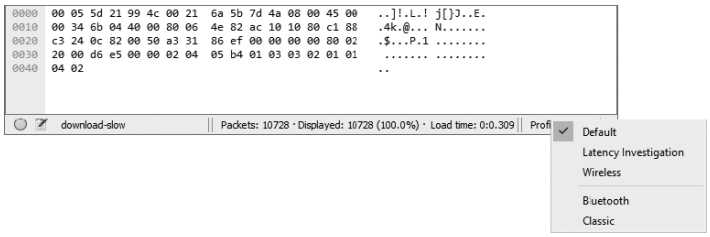

图 3-12　快速转换配置方案

其中一个特别有用的特性就是，每个配置方案都会储存在单独的目录中，这意味着你可以方便地备份和共享给其他人。在图 3-10 所示的 folde标签卡下提供了全局和个人配置文件的路径。你只要把那个配置方案的整目录复制到相同的路径下，就可以把当前配置共享给其他计算机了。

当继续往下读这本书的时候，你也许会需要去创建一些特别的配置方案，来解决常见问题、查找网络延迟的源头和调查安全问题。别被频繁切配置方案吓着。恰恰相反，这可是很省时间的技巧。我知道很多高手有一不同的配置方案用来应对不同的场景。

现在你的 Wireshark 应该已经安装好并运行起来了，你已经准备好进数据包的分析了。在下一章中，我们将详细讲述如何处理你所捕获的数据包。

---

[1]　肯塔基州是美国的一个内陆州。——译者注