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

4.4 设定捕获选项

4.4.1 输入标签页

4.4.2 输出标签页

4.4.3 选项标签页

4.5 过滤器

4.5.1 捕获过滤器

4.5.2 显示过滤器

4.5.3 保存过滤器规则

4.5.4 在工具栏中增加显示过…

章 Wireshark 高级特性

5.1 端点和网络会话

5.1.1 查看端点统计

## 4.2.2 标记数据包

在找到那些符合搜索条件的数据包之后,你可以根据需要进行标记。 例来说,可能你希望将那些需要分开保存的数据包标记出来,或者根据颜 快速地查找它们。如图 4-5 所示,被标记的数据包会以黑底白字显示(例 可以仅仅将标记了的数据包选择出来,然后将其作为数据包捕获保存下来

图 4-5 被标记的数据包将在你的屏幕上高亮显示。在这个例子中, 第二个数据包被标记并且显示为深色

如果你想要标记一个数据包,那么可以右击 Packet List 面板,并在 出的菜单中选择 Mark Packet,或者在 Packet List 面板中选中一个数据包 然后按 Ctrl-M 组合键;如果想取消对一个数据包的标记,那么再按一次 Ctrl-M 组合键;就可以将其取消。在一次捕获中,你想标记多少个数据包 都可以;如果你想要在标记的数据包间前后切换,那么分别按 Shift-Ctrl-和 Shift-Ctrl-B 组合键即可。