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

## 4.3.2 数据包的相对时间参考

数据包的相对时间参考,允许你以一个数据包作为基准,而之后的数 包都以此计算相对时间戳。当你检查在捕获文件之外的某个点触发的一系 连续事件时,这个功能会变得非常好用。

如果希望将某一个数据包设定为时间参考,那么可以在 Packet List 顶板中选择作为相对参考的数据包,然后右键选择 Set/Unset Time Reference。如果希望取消一个数据包的相对时间参考,则重复刚才的操即可。选择完参考数据包后,你也可以按下组合键 Ctrl-T 达到一样的效果

在你将一个数据包设定为时间参考之后,Packet List 面板中这个数据的 Time 列就会显示为 *REF* ,如图 4-8 所示。

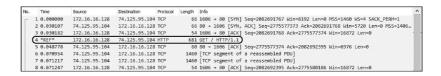


图 4-8 开启了数据包相对时间参考的一个数据包

只有当捕获的时间显示格式设定为与捕获开始相对的时间时,设定数 包时间参考才有用处。使用其他设定都不会生成有用的结果,并且其产生 一堆时间会很令人迷惑。