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

4.1.1 保存和导出捕获文件

如果想要保存数据包的捕获,那么可以选择 File->Save As,之后你愿 该能看见 Save File As 对话框,如图 4-1 所示。对话框会询问你想要保存数据包捕获的位置,以及你希望保存的格式。如果你不选择一个文件格式那么 Wireshark 会默认使用.pcapng 文件格式。

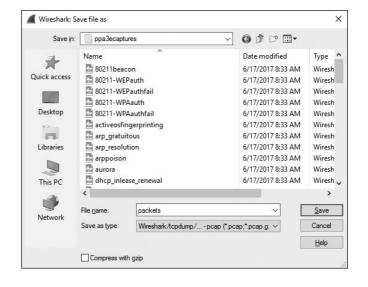


图 4-1 Save File As 对话框可以让你保存你的数据包捕获

Save File As 对话框的一个更强大的功能是你可以指定需要保存的数i包范围,选择 File->Export Specified Packets,如图 4-2 所示。这是一1让「胖」捕获文件变「瘦」的好方法。你可以选择只保存一定序号范围的数据包、标记了的数据包,或者经过过滤器筛选后显示出来的数据包等(标记的数据包和过滤器会在这一章后面进行讨论)。

你可以将你的 Wireshark 捕获数据导出到几种不同格式的文件中,以于在其他媒体中查看,或是导入到其他的数据包分析工具中。这些格式包文本文件、PostScript、逗号分隔值(CSV)和 XML。如果想要导出你的据包捕获,那么可以选择 File->Export Packet Dissections,并选择你想导出的文件格式。你将会看到一个包含着相应文件格式选项的 Save As 对框。

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

4.1.1 保存和导出捕获文件 - Wireshark 数据包分析实战(第 3 版) - 知乎书店

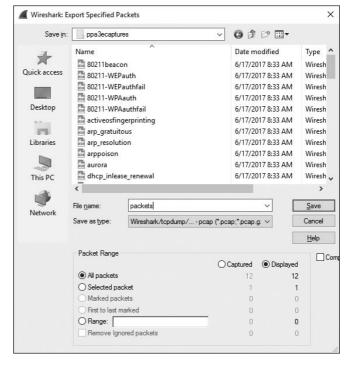


图 4-2 Export Specified Packets 对话框让你针对要保存的流量包有更多的粒度制