

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

第 4 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

3.2 Wireshark 的优点

Wireshark 在日常应用中具有许多优点，无论你是初学者还是数据包分析专家，Wireshark 都能通过丰富的功能来满足你的需要。在第 1 章中，我们为挑选数据包嗅探工具提出过一些重要的判断特征，让我们来检查一下 Wireshark 是否具有这些特征。

**支持的协议：**Wireshark 在支持协议的数量方面是出类拔萃的——于书截稿时 Wireshark 已提供了超过 1000 种协议的支持。这些协议从最基础的 IP 协议和 DHCP 协议到高级的专用协议，比如 DNP3 和 BitTorrent 等。由于 Wireshark 是在开源模式下进行开发的，因此每次更新都会增加一些新协议的支持。

**注意**

在一些特殊情况下，如果 Wireshark 并不支持你所需要的协议，那么你还可以自己编写代码提供相应的支持，并提供给 Wireshark 的开发者，以便他们考虑是否将之包含在以后的版本中。可以在 Wireshark 的项目网站上找到更多的相应信息。

**用户友好度：**Wireshark 的界面是数据包嗅探工具中一种很容易理解界面。它基于 GUI，并提供了清晰的菜单栏和简明的布局。为了增强实用性，它还提供了类似于不同协议的彩色高亮，以及通过图形展示原始数据字节等不同功能。与类似于 Tcpdump 使用复杂命令行的那些数据包嗅探工具相比，Wireshark 的图形化界面对于那些数据包分析的初学者而言，是十分方便的。

**价格：**由于 Wireshark 是开源的，因此它在价格上面是无以匹敌的。Wireshark 是遵循 GPL 协议发布的自由软件，任何人无论出于私人还是商业目的，都可以下载并且使用。

**注意**

虽然 Wireshark 是免费的，但是仍然会有一些人不小心去「付费」购买它。如果在 eBay 搜索「数据包嗅探」，你会惊讶地发现会有如此多的人想以 \$39.95 的跳楼价向你出售 Wireshark 的「专业企业级许可证」。显而易见，这些都是骗人的把戏。但是如果你执意想要购买这些所谓的「许可证」，不如给我打个电话，我正好有些肯塔基的海边别墅要以跳楼价出售。<sup>[1]</sup>

**软件支持：**一个软件的成败取决于其后期支持的好坏。虽然像 Wireshark 这样自由分发的软件很少会有官方正式的支持，它依赖于开源区的用户群提供帮助。但幸运的是，Wireshark 社区是最活跃的开源项目

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

第 4 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

区之一。Wireshark 网站上给出了很多种软件帮助的相关链接，包括在线文档、支持与开发 wiki、FAQ。很多顶尖的开发者也都注册并关注着 Wireshark 的邮件列表。Riverbed Technology 也提供了对 Wireshark 的免费支持。

**源码访问：**因为 Wireshark 是开源软件，所以你可以在任何时间访问其源码。这对查找程序的 Bug、理解协议解释器的工作原理或自己贡献代码都有很大帮助。

**支持的操作系统：**Wireshark 对主流的操作系统都提供了支持，其中包括 Windows、Mac OS X 以及基于 Linux 的系统。你可以在 Wireshark 的页面上查询所有 Wireshark 支持的操作系统列表。