

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

3.3 安装 Wireshark

Wireshark 的安装过程极其简单，但在安装之前要确保你的机器满足下要求。

- 任意新型的 32 位或 64 位 CPU。
- 至少 400MB 可用内存（主要为了大型流量文件）。
- 至少 300MB 的可用存储空间（不包括捕获的流量文件）。
- 支持混杂模式的网卡。
- WinPcap 或 libpcap 驱动。

WinPcap 驱动是 Windows 对于 pcap 数据包捕获的通用程序接口（API）的实现，简单来说就是这个驱动能够通过操作系统捕捉原始数据包应用过滤器，并能够让网卡切入或切出混杂模式。

虽然你也可以单独下载安装 WinPcap，但一般最好使用 Wireshark 安装包中的 WinPcap。因为这个版本的 WinPcap 经过测试，能够和 Wireshark 一起工作。