

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

3.3.1 在微软 Windows 系统中安装

通过测试的当前 Wireshark 版本，能够在微软仍维护的 Windows 操作系统上运行，于本书截稿时包括 Windows Vista、Windows 7、Windows 8、Windows 10 和 Windows Servers 2003/2008/2012。虽然 Wireshark 也可以在一些其他版本的 Windows 中运行（比如 Windows XP），但这些版本不被官方支持。

在 Windows 中安装 Wireshark 的第一步就是在 Wireshark 的官方网站上找到 Download 页面，并选择一个镜像站点下载最新版的安装包。在下载好安装包之后，遵照如下步骤安装。

- (1) 双击.exe 文件开始进行安装，在介绍页面上单击 Next。
- (2) 阅读许可证条款，如果同意接受此条款，单击 I Agree。
- (3) 选择你希望安装的 Wireshark 组件，如图 3-1 所示。在本书中接受默认设置即可，然后单击 Next。

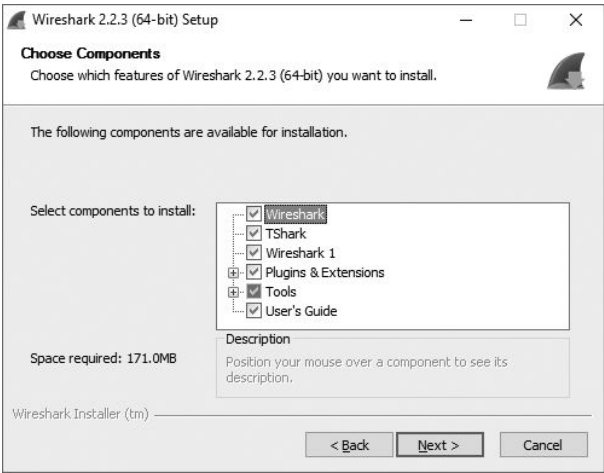


图 3-1 选择你想要安装的 Wireshark 组件

- (4) 在 Additional Tasks 窗口中单击 Next。
- (5) 选择 Wireshark 的安装位置并单击 Next。
- (6) 当弹出是否需要安装 WinPcap 的对话框时，务必确保 Install WinPcap 选项已被勾选，如图 3-2 所示，然后单击 Install。安装过程便随即开始。

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

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

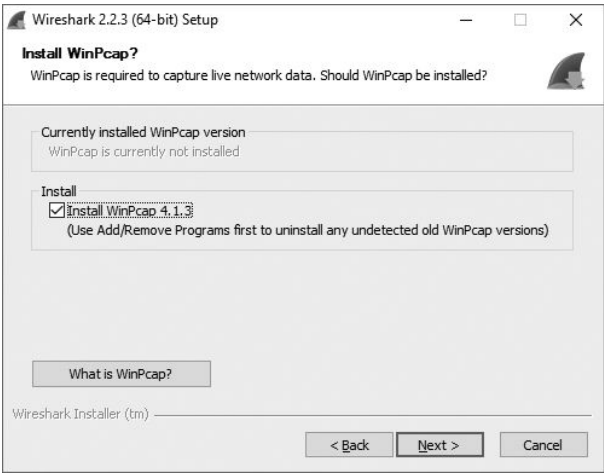


图 3-2 将安装 WinPcap 驱动选项选中

- (7) Wireshark 的安装过程进行了大约一半的时候，会开始安装 WinPcap。在介绍页面单击 Next 之后，请阅读许可协议并单击 I Agree。
- (8) 你将选择是否安装 USBPcap 选项。这是一个从 USB 设备中收集数据的工具。勾选你想要的复选框并单击 Next。
- (9) WinPcap 和 USBPcap（如果你在上一步勾选了的话）应该已经装到你的计算机上了，在安装完成之后，单击 Finish。
- (10) Wireshark 应该已经安装到你的计算机上了，在安装完成之后，单击 Finish。
- (11) 在安装确认界面中，单击 Finish。