

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

3.3.2 在 Linux 系统中安装

Wireshark 可以在大部分基于 UNIX 的系统中运行。你可以通过系统管理器下载，并安装针对你的系统所适用的发行版本。我们在这里只介绍个常见的 Linux 发行版本的安装步骤。

一般来说，如果作为系统软件安装，你需要具有 root 权限；但如果通过编译源代码安装成为本地软件，那么通常就不需要 root 权限了。

1. 基于 RPM 的系统

对于类似红帽 Linux（Red Hat Linux）等使用 RPM 的 Linux 发行版比如 CentOS，很可能系统默认安装了 Yum 包管理器。如果是这样的话，你可以从发行版本的软件源中获取并快速安装 Wireshark。你需要做的是开一个控制台窗口，并输入以下命令：

```
$ sudo yum install wireshark
```

如果需要依赖组件，那么你将通过提示来安装它们。如果一切成功执行，你将可以使用命令行启动它并通过 GUI 来操作它。

2. 基于 DEB 的系统

对于类似于 Debian 和 Ubuntu 等使用 DEB 的 Linux 发行版，你可以用 APT 包管理工具安装 Wireshark。要从系统软件源中安装 Wireshark，打开一个控制台窗口并键入如下命令：

```
$ sudo apt-get install wireshark wireshark-qt
```

如果需要依赖组件，那么你将通过提示来安装它们。

3. 使用源代码编译

因为操作系统架构和 Wireshark 功能的改变，所以从源码安装的方法能也会随之变化，这也是建议从系统包管理器安装的一个原因。然而，如果你的 Linux 发行版没有自动安装包管理工具，那么安装 Wireshark 的一种有效的方法就是使用源代码编译。下面的步骤给出了安装方法。

(1) 从 Wireshark 网站下载源代码包。

(2) 键入下面的命令将压缩包解压（将文件名替换成你所下载的源文件的名称）：

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

```
$ tar -jxvf <file_name_here>.tar.bz2
```

(3) 在安装和设置 Wireshark 之前，可能需要安装一些依赖组件。比如，Ubuntu 14.04 需要一些额外的软件包才能让 Wireshark 工作。这些依赖组件可以用以下的命令进行安装（你可能需要使用 root 权限，你可以在命令前面添加 sudo）：

```
$ sudo apt-get install pkg-config bison flex qt5-default libgtk-3-dev libpcap-dev qttools5-dev-tools
```

(4) 进入解压缩后创建的文件夹。

(5) root 级别的用户使用 ./configure 命令配置源代码以便于其能正常编译。如果你不想使用默认的设置，那么你可以在这时指定安装选项；如果缺少相关软件支持，那么你应该会得到相关错误信息；如果安装成功了，那么你应该可以得到成功提示，如图 3-3 所示。

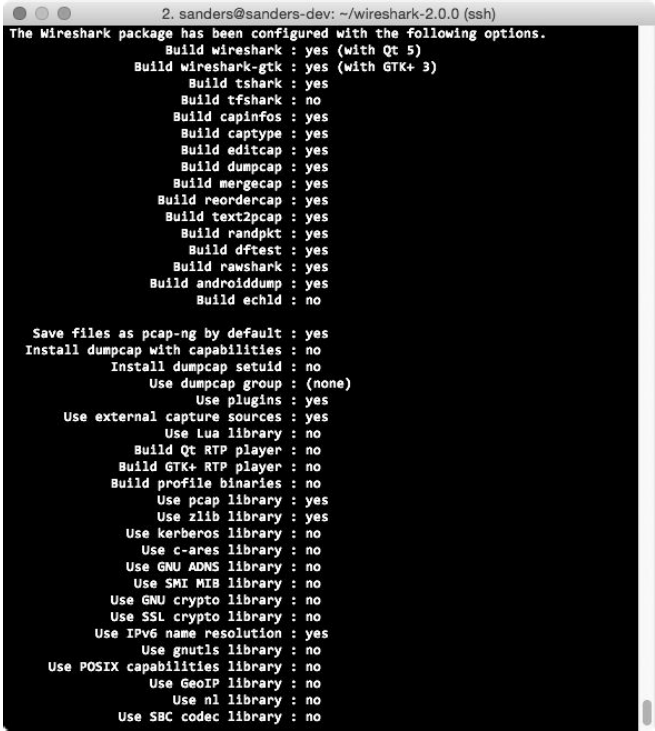


图 3-3 由 ./configure 命令得到的成功输出

- (6) 键入 make 命令将源代码编译成二进制文件。
- (7) 使用 sudo make install 命令完成最后的安装。
- (8) 运行 sudo/sbin/ldconfig 来结束安装。

注意

如果你按照以上步骤操作时出现了错误，那么你可能需要安装额外的软件包。

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