第3章

Wireshark 入门

在第 1 章中，我们介绍了几种可以进行网络分析的数据包嗅探工具软件，但在本书中我们将只使用 Wireshark，并在此章进行简要的介绍。

3.1 Wireshark 简史

Wireshark 的历史相当久远，其最初的版本叫做 Ethereal，由毕业于密苏里大学堪萨斯城分校计算机科学专业的 Gerald Combs 出于项目需要而开发，并于 1998 年以 GNU Public Licence（GPL）开源许可证发布。

在发布了 Ethereal 8 年之后，Combs 辞职另谋高就，但是在那个时候他的雇主公司掌握着 Ethereal 的商标权，而 Combs 也没能和其雇主就取得 Ethereal 商标达成协议。于是 Combs 和整个开发团队在 2006 年中的时候将这个项目重新命名为 Wireshark。

Wireshark 随后迅速地取得了大众的青睐，而其合作开发团队也壮大到 500 人以上，然而之前的 Ethereal 项目却再没有前进过一步。

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——于本书截稿时 Wireshark 已提供了超过 850 种协议的支持。这些协议包括从最基础的 IP 协议和 DHCP 协议到高级的专用协议比如 AppleTalk 和 BitTorrent 等。由于 Wireshark 在开源模式下进行开发，每次更新都会增加一些对新协议的支持。

注意　在一些特殊情况下，如果 Wireshark 并不支持你所需要的协议，你还可以通过自己编写代码提供相应的支持，并提供给 Wirshark 的开发者，以便于使之能被包含在之后版本中（当然是在代码被采纳的情况下）。

用户友好度：Wireshark 的界面是数据包嗅探工具中最容易理解的工具之一。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，它还提供了不同协议的彩色高亮，以及通过图形展示原始数据细节等不同功能。与 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，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 Wireshark。

注意　尽管 Wireshark 是免费的，但是还是会有一些人不小心去“付费”购买它。如果你在 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，我正有些肯塔基的海边别墅以跳楼价出售（肯塔基州是美国的一个内陆州——译者注）。

程序支持：一个软件的成败通常取决于其程序支持的好坏。虽然像 Wireshark 这样的自由分发软件很少会有正式的程序支持，而是依赖于开源社区的用户群，但是幸运的是，Wireshark 社区是最活跃的开源项目社区之一。Wireshark 网页上给出了许多种程序支持的相关链接，包括在线文档、支持与开发 wiki、FAQ，并可以注册 Wireshark 开发者都关注的邮件列表。CACE Technologies 通过 SharkNet 项目也对外提供付费支持。

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 的主页上查询所有 Wireshark 支持的操作系统列表。

3.3 安装 Wireshark

Wireshark 的安装过程极其简单。但在你安装之前要确保你的机器满足如下要求。

- 400MHz 及以上的处理器
- 128MB 内存
- 至少 75MB 的可用存储空间
- 支持混杂模式的网卡
- WinPcap 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。

尽管你也可以单独下载安装 WinPcap（http://www.winpcap.org），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。

3.3.1 在微软 Windows 系统中安装

在 Windows 中安装 Wireshark 的第一步就是在 Wireshark 的官方网站

http://www.wireshark.org 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，遵照如下步骤进行安装。

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，并单击 **Next**。

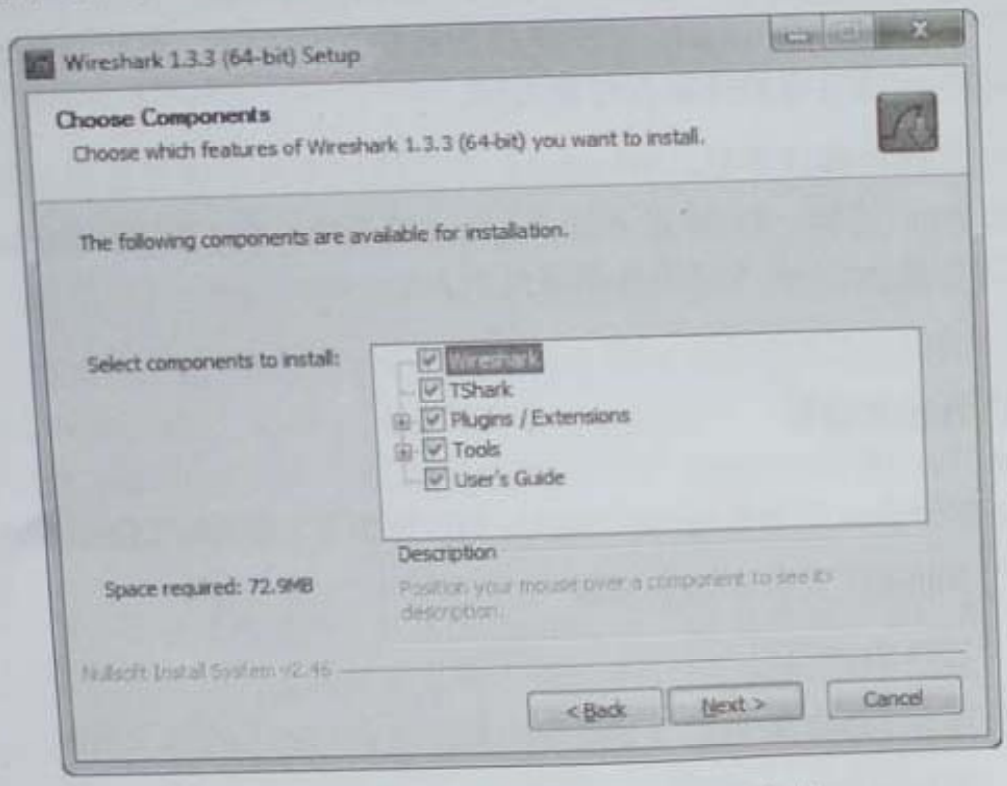

图 3-1 选择你想要安装的 Wireshark 组件

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**。安装过程便会随即开始。

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. WinPcap 应该已经安装到你的电脑上，在安装完成之后，单击 **Finish**。

9. Wireshark 应该已经安装到你的电脑上，在安装完成之后，单击 **Next**。

10. 在安装完成确认界面中，单击 **Finish**。

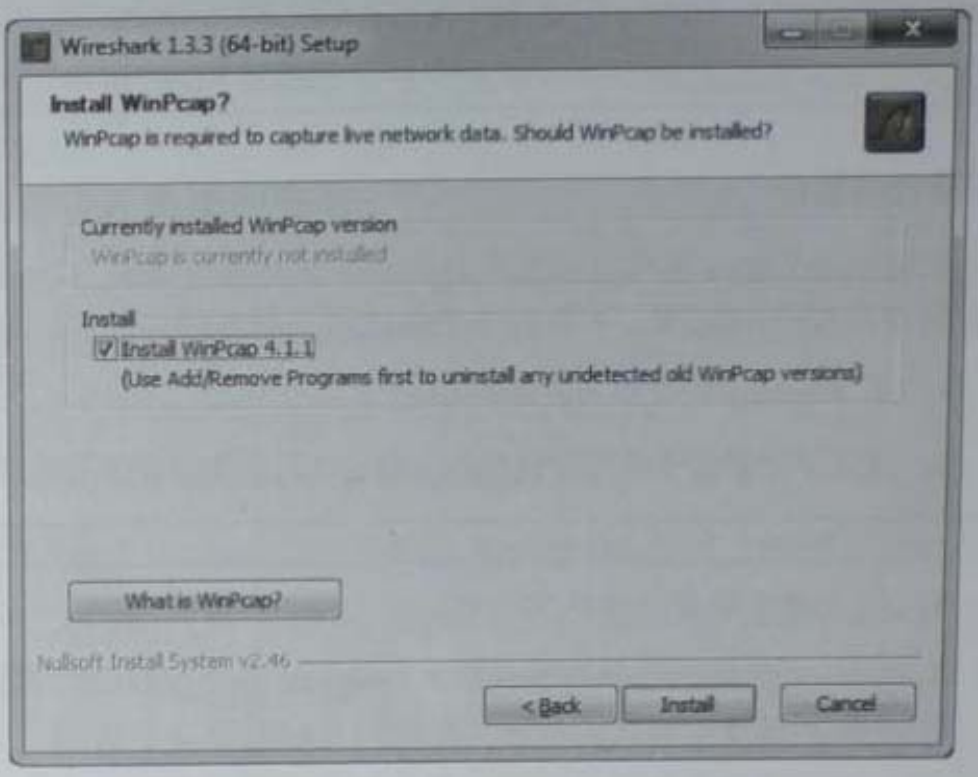

图 3-2　选中安装 WinPcap 驱动的选项

3.3.2　在 Linux 系统中安装

在 Linux 系统中安装 Wireshark 的第一步是先下载合适的安装包。由于 Wireshark 并不支持所有的 Linux 版本，所以你可能会发现并没有合适你的 Linux 版本对应的安装包可供下载。

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

使用 RPM 的系统

对于类似于红帽 Linux（Red Hat Linux）等使用 RPM 的 Linux 发行版，在从 Wireshark 网站上下载好合适的安装包之后，打开一个命令行程序并键入如下命令（将文件名替换成你所下载安装包的名称）：

```
rpm -ivh wireshark-0.99.3.i386.rpm
```

如果缺少相关程序支持，在安装好这些之后，再重新安装 Wireshark。

使用 DEB 的系统

对于类似与 Debian 和 Ubuntu 等使用 DEB 的 Linux 版本，你可以从系统源

中安装 Wireshark，打开一个命令行窗口并键入如下命令。

```
apt-get install wireshark
```

使用源代码编译

如果你的 Linux 没有自动安装包管理工具，那么安装 Wireshark 最高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源代码包的名称）。

```
tar -jxvf wireshark-1.2.2.tar.bz2
```

3. 进入解压缩后创建的文件夹。

4. 以 root 级别的用户身份使用**./configure** 命令配置源代码以便其能正常编译。如果你不想使用默认的设置，你可以这时指定安装选项。如果缺少相关软件支持，你应该会得到相关错误信息。如果安装成功了，你应该可以得到成功的提示，如图 3-3 所示。

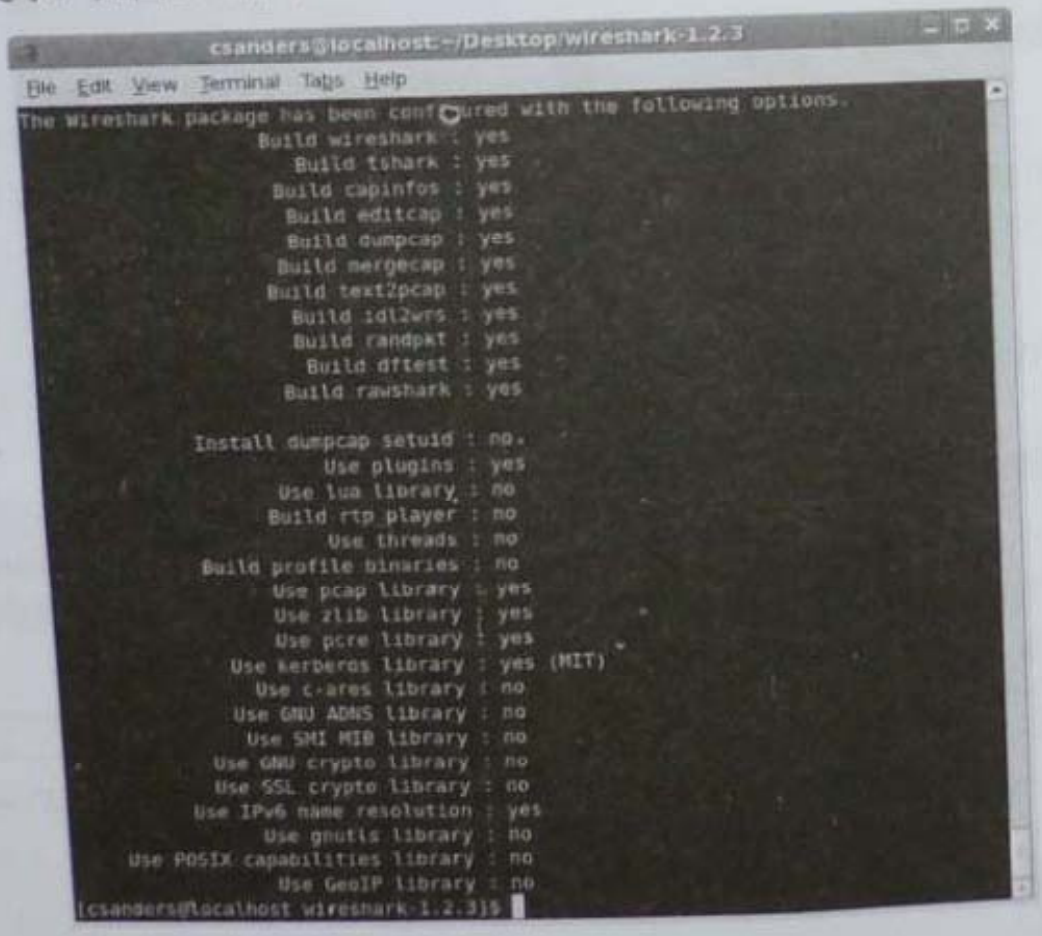

图 3-3　由./configure 命令得到的成功输出

5. 输入 **make** 命令将源代码编译成二进制文件。

6. 使用 **make install** 命令完成最后的安装。

3.3.3 在 Mac OS X 系统中安装

在 Mac OS X 雪豹系统中安装 Wireshark 有一些注意事项，但安装并不困难，我在这里罗列了所需的安装步骤。

1. 从 Wireshark 网站上下载 DMG 包。

2. 将 Wireshark.app 复制到 Applications 文件夹。

3. 打开 Utilities 文件夹中的 Wireshark.app。

4. 在 Finder 中单击 Go，选择 Go To Folder。输入**/usr/local/bin/**打开这个文件夹。

5. 将 Command Line 文件夹中的内容复制到/usr/local/bin/，这时你需要输入你的密码以完成操作。

6. 在 Utilities 文件夹中，将 ChmodBPF 文件夹复制到 StartupItems 文件夹，这时你需要再次输入你的密码以完成该操作。安装过程至此宣告结束。

3.4 Wireshark 初步入门

当你成功地在你的系统中装好了 Wireshark，你就可以开始熟悉它了。当你终于打开了这个功能强大的数据包嗅探器，却会发现你什么都看不见！

好吧，Wireshark 在刚打开的时候确实不太好玩，只有在拿到一些数据之后事情才会变得有趣起来。

3.4.1 第一次捕获数据包

为了能让 Wireshark 得到一些数据包，你可以开始你的第一次数据包捕获实验了。你可能会想：“当网络什么问题也没有的时候，怎么能捕获数据包呢？”

首先，网络总是有问题的。如果你不相信，那么你去给你网络上所有的用户发一封邮件，告诉他们一切都工作得非常好。

第二，做数据包分析并不一定要等到有问题的时候再做。事实上，大多数的数据包分析员在分析没有问题的网络流量上花的时间要比解决问题的时候

多。为了能高效地解决网络问题，你也同样需要得到一个基准来与之对比。举例来说，如果你想通过分析网络流量来解决关于 DHCP 的问题，你至少需要知道 DHCP 在正常工作时的数据流是什么样子的。

更广泛地讲，为了能够发现日常网络活动的异常，你必须对日常网络活动的情况有所掌握。当你的网络正常运行时，你以此作为基准，就能知道网络流量在正常情况下的样子。

闲言少叙，让我们来捕获一些数据包吧！

1. 打开 Wireshark。

2. 从主下拉菜单中选择 **Capture**，然后是 **Interface**。

这时你应该可以看到一个对话框，里面列出了你可以用来捕获数据包的各种设备，以及它们的 IP 地址。

3. 选择你想要使用的设备，如图 3-4 所示，然后单击 Start，或者直接单击欢迎画面中 Interface List 下的某一个设备。随后数据就会在窗口中呈现出来。

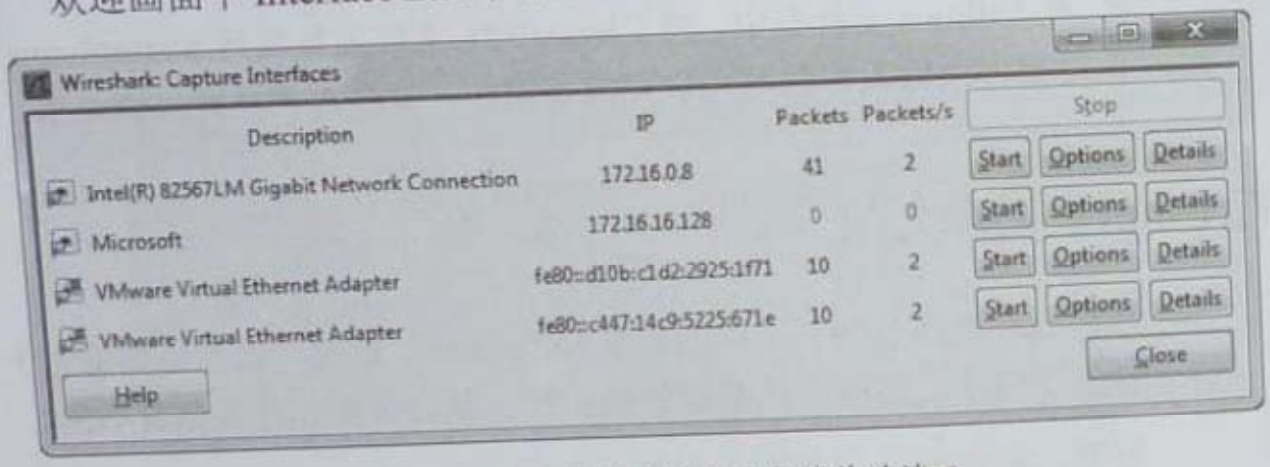

图 3-4　选择你想要进行数据包捕获的端口

4. 等上一分钟左右，当你打算停止捕获并查看你的数据时，在 Capture 的下拉菜单中单击 **Stop** 按钮即可。

当你做完了以上步骤并完成了数据包的捕获，Wireshark 的主窗口中应该已经呈现了相应的数据，但此时你可能已经对那些数据的规模感到头疼，这也就是为什么我们把 Wireshark 一整块的主窗口进行拆分的原因。

3.4.2　Wireshark 主窗口

Wireshark 的主窗口是将你所捕获的数据包显示或拆分成更容易使人理解的方式的地方，也将是你花费时间最多的地方。我们使用刚刚捕获的数据包来介

绍一下 Wireshark 的主窗口，如图 3-5 所示。

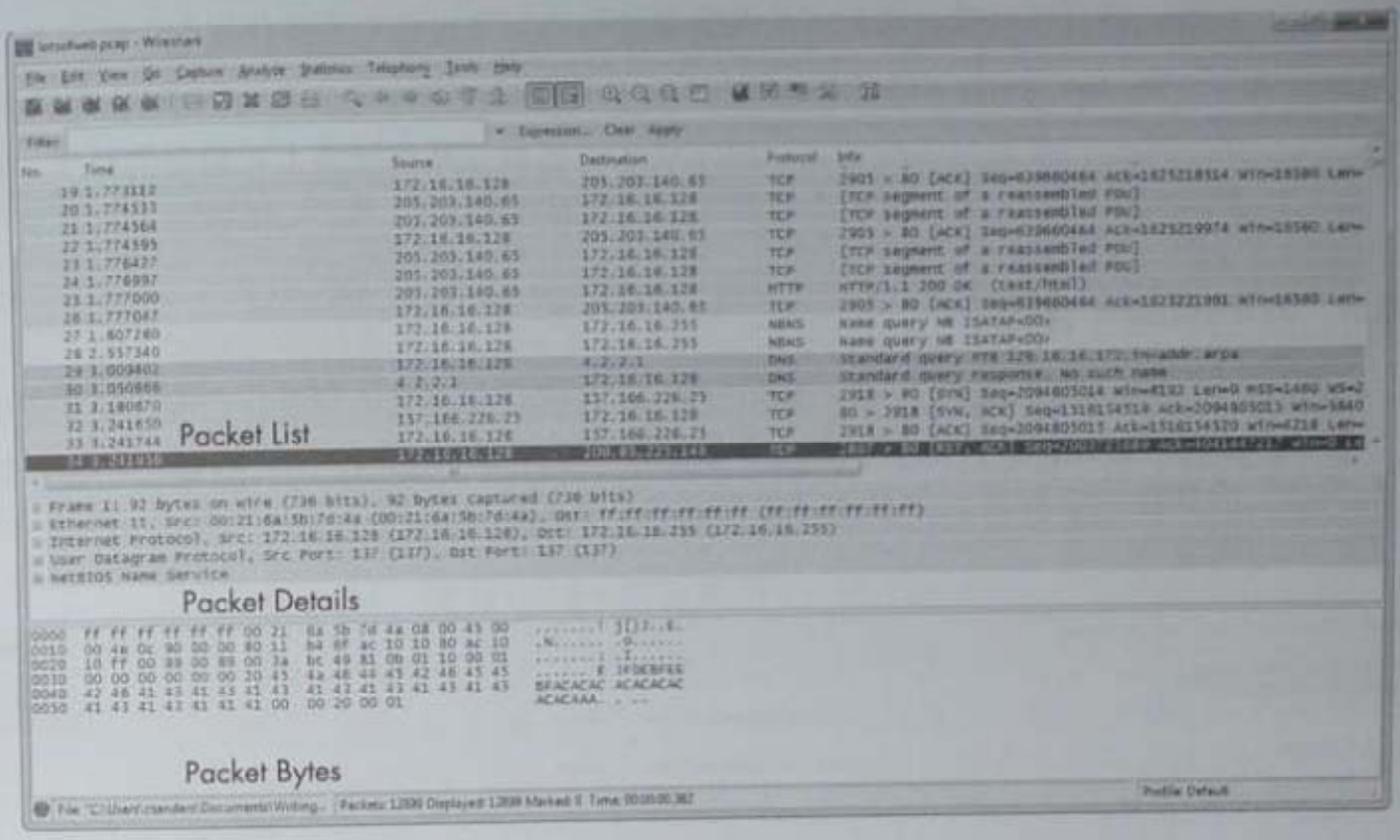

图 3-5　Wireshark 主窗口的设计使用了 3 个面板

主窗口的 3 个面板相互有着联系。如果希望在 Packet Details 面板中查看一个单独的数据包的具体内容，你必须现在 Packet List 面板中单击选中那个数据包。在你选中了数据包之后，你可以通过在 Packet Details 面板中选中数据包的某个字段，从而在 Packet Bytes 面板中查看相应字段的字节信息。

注意　在图 3-5 中的 Packet List 面板中列出了几种不同的协议，但这里并没有使用不同的层次来对不同的协议进行视觉上的区分，所有的数据包都是按照其在链路上接收到的顺序排列的。

下面介绍了每个面板的内容。

Packet List（数据包列表）：最上面的面板用表格显示了当前捕获文件中的所有数据包，其中包括了数据包序号、数据包被捕获的相对时间、数据包的源地址和目标地址、数据包的协议以及在数据包中找到的概况信息等列。

注意　当文中提到流量的时候，我通常是指 Packet List 面板中所有呈现出来的数据包，而当特别提到 DNS 流量时，我指的是 Packet List 面板中 DNS 协议的数据包。

Packet Details（数据包细节）：中间的面板分层次地显示了一个数据包中的内容，并且可以通过展开或是收缩来显示这个数据包中所捕获到的全部内容。

Packet Bytes（数据包字节）：最下面的面板可能是最令人困惑的，因为它显示了一个数据包未经处理的原始样子，也就是其在链路上传播时的样子。这些原始数据看上去一点都不舒服而且不容易理解。

3.4.3 Wireshark 首选项

Wireshark 提供了一些首选项设定，可以让你根据需要进行定制。如果需要设定 Wireshark 首选项，在主下拉菜单中选择 **Edit** 然后单击 **Preferences**，然后你便可以看到一个首选项的对话框，里面有一些可以定制的选项，如图 3-6 所示。

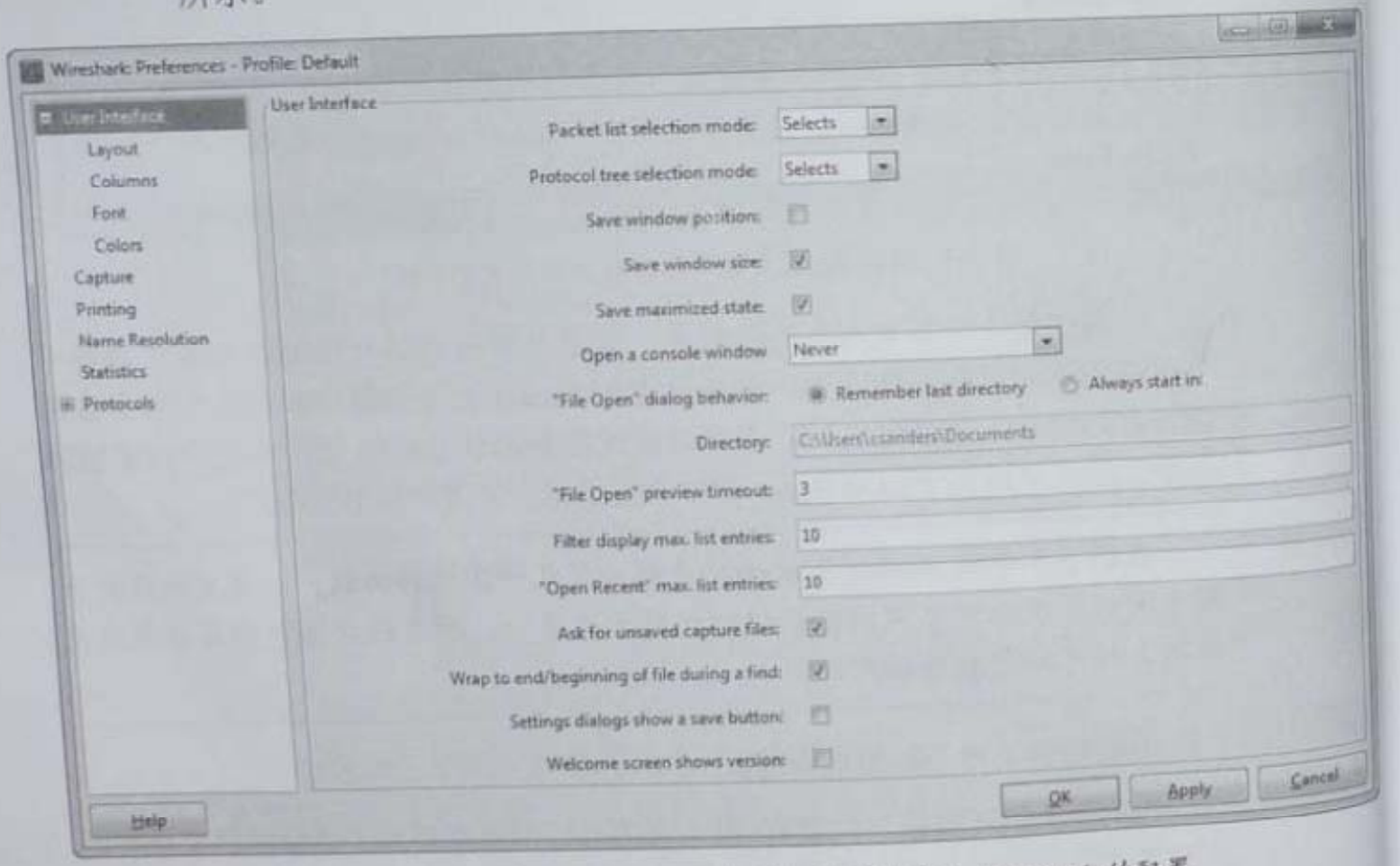

图 3-6　你可以使用 Preferences 对话框中的选项自定义 Wireshark 的配置

Wireshark 首选项分为 6 个主要部分。

User Interface（用户接口）：这些选项决定了 Wireshark 将如何显示数据。你可以根据你的个人喜好对大多数选项进行调整，比如是否保存窗口位置、

个主要窗口的布局、滚动条的摆放、Packet List 面板中列的摆放，以及显示捕获数据的字体、前景色和背景色等。

Capture（捕获）：这些选项可以让你对你捕获数据包的方式进行特殊的设定，比如你默认使用的设备、是否默认使用混杂模式、是否实时更新 Packet List 面板等。

Printing（打印）：这个部分中的选项可以让你对 Wireshark 如何打印你的数据进行各种特殊的设定。

Name Resolutions（名字解析）：通过这些设定，你可以开启 Wireshark 将地址（包括 MAC、网络以及传输名字解析）解析成更加容易分辨的名字这一功能，并且可以设定可以并发处理名字解析请求的最大数目。

Statistics（统计）：这一部分提供了一些 Wireshark 中统计功能的设定选项。

Protocols（协议）：这个部分中的选项与捕捉和显示各种 Wireshark 能够解码的数据包有关。并不是每一个协议都有配置选项，但是一些协议的某些选项则可以进行更改。除非你有特殊的原因去修改这些选项，否则最好保持它们的默认值。

3.4.4 数据包彩色高亮

如果你像我一样喜欢五颜六色的物体，那么你应该会对 Packet List 面板中那些不同的颜色感到兴奋。如图 3-7 所示（尽管图示是黑白的，但你应该可以理解），那些颜色看上去就像是随机分配给每一个数据包的，但其实并不是这样的。

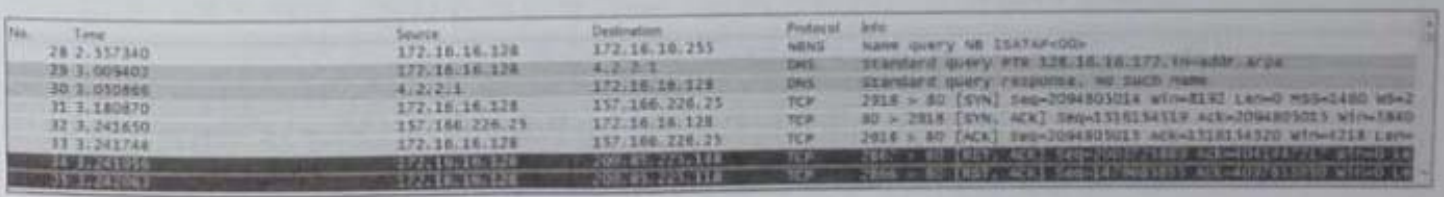

图 3-7 Wireshark 的彩色高亮有助于快速标识协议

每一个数据包的颜色都是有讲究的，这些颜色对应着数据包使用的协议。举例来说，所有的 DNS 流量都是蓝色的，而 HTTP 流量都是绿色的。将数据包进行彩色高亮，可以让你很快地将不同协议的数据包分开，而不需要对每个数据包都查看 Packet List 面板中的协议列。你会发现这样在浏览较大的捕获文件时，可以极大地节省时间。

如图 3-8 所示，Wireshark 通过 Coloring Rules（着色规则）窗口可以很容易地查看每个协议所对应的颜色。如果想要打开这个窗口，在主下拉菜单中选择 **View** 然后单击 **Coloring Rules**。

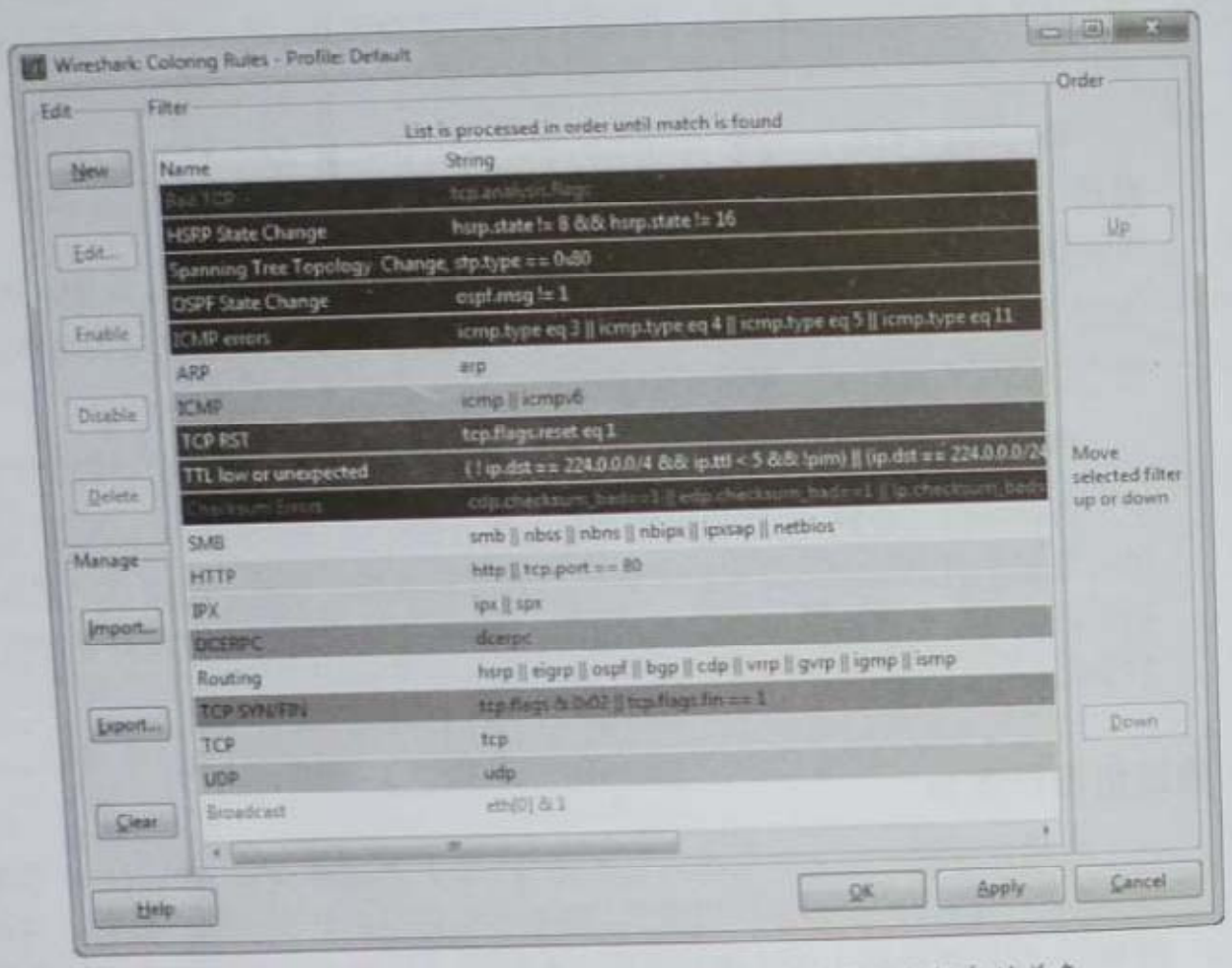

图 3-8　你可以在 Coloring Rules 窗口中查看并更改数据包的着色

你可以创建你自己的着色规则，或者修改已有设置。举例来说，使用下列步骤可以将 HTTP 流量绿色的默认背景改成淡紫色。

1. 打开 Wireshark，并且打开 Coloring Rules 窗口（**View**▸**Coloring Rules**）。
2. 在着色规则的列表中找到 HTTP 着色规则并单击选中。
3. 单击 **Edit** 按钮，你会看到一个 Edit Color Filter 窗口，如图 3-9 所示。
4. 单击 **Background Color** 按钮。
5. 使用颜色滚轮选择一个你希望使用的颜色，然后单击 **OK**。
6. 再次单击 **OK** 来应用改变，并回到主窗口。主窗口此时应该已经重载，并使用了更改过的颜色样式。

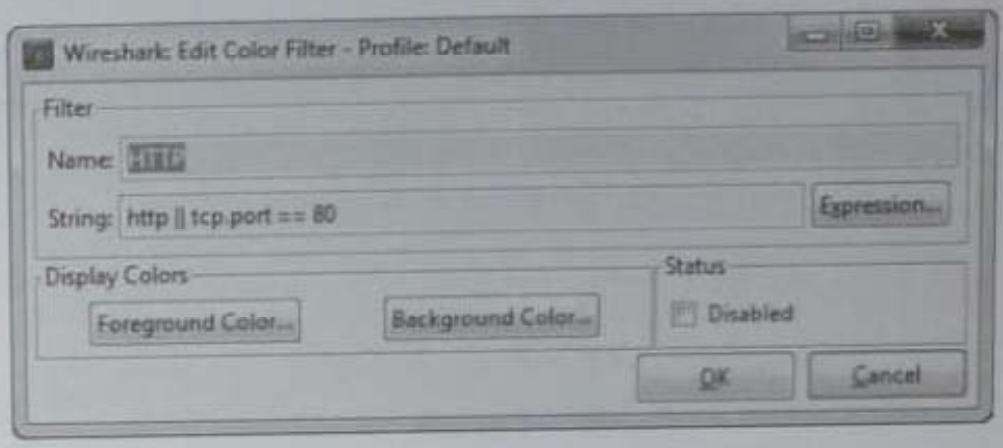

图 3-9　在编辑着色过滤器时，前景色和背景色都可以进行更改

当你在网络上使用 Wireshark 时，你可能会发现你处理某些协议比其他协议要多。这时彩色高亮的数据包就能让你工作得更加方便。举例来说，如果你觉得你的网络上有一个恶意的 DHCP 服务器在分发 IP，你可以简单地修改 DHCP 协议的着色规则，使其呈现明黄色（或者其他易于辨认的颜色）。这可以使你能够更快地找出所有 DHCP 流量，并让你的数据包分析工作更有效率。

你还可以通过基于你自己定制的过滤器创建着色规则，来扩展这些着色规则的用途。

现在你的 Wireshark 应该已经安装好并运行起来了，你已经准备好进行数据包的分析了。在下一章中，我们将详细讲述如何处理你所捕获的数据包。