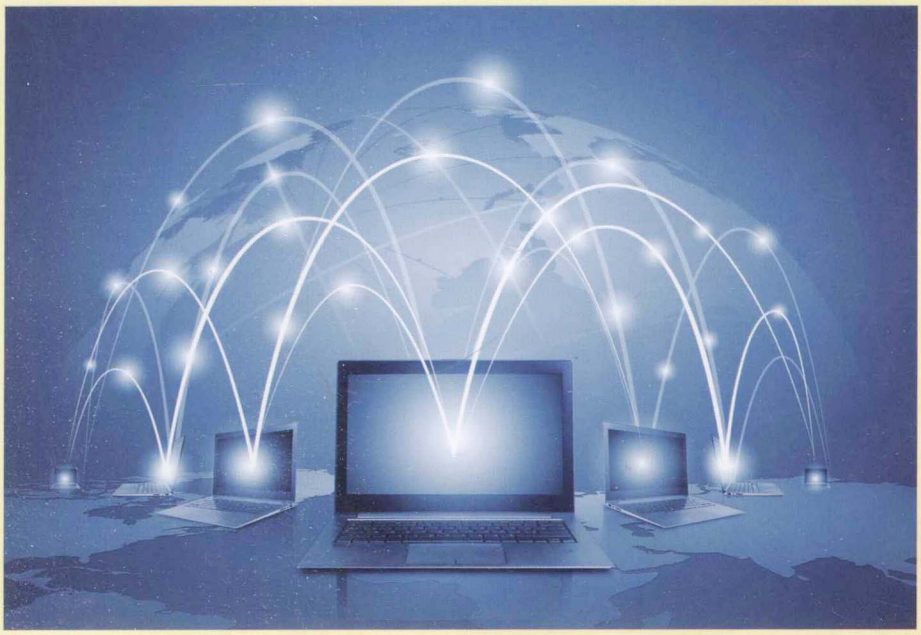
HZ BOOKS
华章教育

高等院校计算机课程设计指导丛书

Windows网络编程课程设计

刘琰 罗军勇 常斌 编著

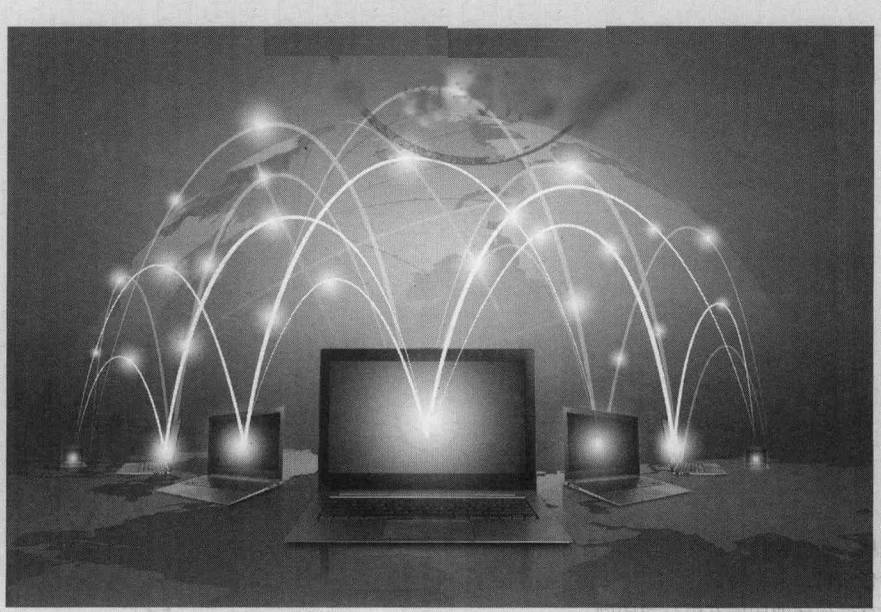


机械工业出版社
China Machine Press

高等院校计算机课程设计指导丛书

Windows网络编程课程设计

刘琰 罗军勇 常斌 编著



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

Windows 网络编程课程设计/刘琰，罗军勇，常斌编著. —北京：机械工业出版社，2013.11

（高等院校计算机课程设计指导丛书）

ISBN 978-7-111-44433-6

Ⅰ. W… Ⅱ. ①刘… ②罗… ③常… Ⅲ. Windows 操作系统-网络软件-程序设计-课程设计-高等学校-教材 Ⅳ. TP316.86

中国版本图书馆 CIP 数据核字（2013）第 246790 号

本书以 Visual Studio C ++作为实验环境，设计了有关 Windows 系统中网络编程的延续性单元实践和可扩展专题实践项目，将计算机网络的基本原理与应用紧密结合。本书给出了操作分析类、程序设计类和程序分析类 3 大类共 21 个实践项目，应用范围涵盖网络应用程序逆向分析、网络基本通信、网络通信框架设计、网络应用程序性能测量与分析、网络应用程序可靠性分析、网络异步操作和底层通信控制等。本书实践环节基于主流开发环境和开源代码软件，不需要特殊的软硬件平台投入，既方便学生课后练习，也可以供教师组织实践教学。

本书系统性较强、结构清晰、论述严谨，既突出基本原理和技术思想，也强调工程实践，适合作为网络工程、信息安全、计算机应用、计算机软件、通信工程等专业的本科生教材，也可供从事网络工程、网络应用开发和网络安全等工作的技术人员参考。

机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码 100037）

责任编辑：朱 劼

北京诚信伟业印刷有限公司印刷

2014 年 1 月第 1 版第 1 次印刷

185mm×260mm · 16 印张

标准书号：ISBN 978-7-111-44433-6

定 价：39.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

客服热线：（010）88378991 88361066 投稿热线：（010）88379604

购书热线：（010）68326294 88379649 68995259 读者信箱：hzjsj@hzbook.com

前　言

在信息化高度发展的今天，网络应用层出不穷，技术日新月异。越来越多的应用运行在网络环境下，这就要求程序员能够在最普及的 Windows 操作系统上开发网络应用程序。目前，国内大批专门从事网络技术开发与技术服务的研究机构和高科技企业需要网络基础扎实、编程技术精湛的专业技术人才。作为计算机网络课程体系的重要组成部分，网络编程相关课程已在国内各大高校开设。

网络应用程序具有理论与实践结合紧密、编程模型可复用、运行结果受环境影响大等特点。着眼于 Windows 网络编程基本技能的训练和强化，本书内容的组织充分考虑了教学过程的可实施性，设计了前后贯穿的延续性单元实践项目，突出编程方法的差异性；设计了由浅入深的可扩展专题实践项目，丰富实践内容，强化学习效果。通过本书内容的学习，读者可以深入实践 Windows 系统中网络编程的基本方法，系统掌握网络数据处理的原理和技术，为将来从事网络技术研究、网络应用程序开发和网络管理等工作打下坚实的基础。

本书共分 7 章，并在最后提供了一个附录，主要内容如下：

第 1 章利用 Windows 系统中的两个常用网络分析工具：网络流量捕获工具 Wireshark 和网络状态显示工具 Netstat，并选择邮件登录和迅雷软件下载两种常见的网络应用，完成软件运行过程分析工作，目的在于帮助学生熟悉常用的网络编程辅助工具，掌握网络应用程序的调试和分析技能。

第 2 章重点阐述 Windows Sockets 的基本组成和 Windows Sockets 编程接口的具体功能，通过主机 IP 地址获取的简单设计类项目来熟悉和掌握 Windows Sockets 编程基本方法，目的在于帮助学生熟悉 Windows Sockets 接口函数的具体功能，掌握使用 Windows Sockets 的基本配置和开发过程。

第 3 章阐述流式套接字编程的适用场合和基本方法，在此基础上，通过一系列项目来训练学生掌握循环方式和并发方式下的流式套接字编程、网络通信的框架设计、基于流式套接字的网络程序的故障分析、字节流处理的接收控制和效率提升等。

第 4 章阐述数据报套接字编程的适用场合和基本方法，在此基础上，设计了三个设计类实践项目，力图训练学生掌握数据报套接字编程、基于无连接传输服务的数据报套接字网络程序的故障分析等。

第 5 章阐述原始套接字编程的适用场合和基本方法，在此基础上，由简到繁设计了三个设计类实践项目，力图训练学生掌握原始套接字的基本使用方法和高级参数设置，帮助学生熟练使用原始套接字，灵活控制底层传输协议，实现更低层次的网络应用程序。

第 6 章选择三个在不同规模 I/O 环境下最常用的模型，即 I/O 复用模型、WSAAsyncSelect 模型和完成端口模型，设计了三个综合性较强的设计类项目进行训练，目的在于进一步拓展学生对 Windows 套接字的实践能力，在前面单元训练的基础上，对代码进行组合和改进，满足现

实应用对效率、处理规模等的需求。

第7章以WinPcap框架中wpcap.dll接口的使用为重点，设计了两个链路层数据通信的实践项目：ARP欺骗和用户级网桥，目的在于扩展学生对原始帧的接收与发送、网卡操控等的处理能力。

附录部分给出了Windows Sockets错误码和错误原因。

为了方便读者阅读和学习，编者根据本书内容另外提供了使用Visual Studio 2008开发的Visual C++应用程序源代码，读者可以登录华章网站（http://www.hzbook.com）免费下载。

本书由解放军信息工程大学网络空间安全学院组织编写，刘琰参与了本书全部章节的撰写和示例代码编码，罗军勇教授参与了部分内容的编写并审校了全书，常斌完成了本书教学资源的制作和整理。内蒙古医科大学王晓东老师参与了第6、7章的编写及相关工作。

本书是编者根据多年开发网络应用程序和研究相关课程教学的经验，并在多次编写的内部交流讲义的基础上修改而成的。由于网络技术的快速发展，再加之作者水平有限，疏漏和错误之处在所难免，恳请读者和有关专家不吝赐教。

编　者

2013年6月

教学和阅读建议

本课程的先修课程为“程序设计”、“计算机网络”、“网络协议分析”。本课程强调技能训练，在授课内容上注重知识的实用性和连贯性，建议实践学时为 30 学时，各章的教学内容可作如下安排。

第 1 章　网络应用程序运行分析（上机实践 2 学时）

实践内容：

- 网络流量捕获工具使用方法。
- 网络状态显示工具使用方法。
- 经典网络应用运行过程分析。

考核要求：

通过上机实践，学生应能熟悉常用的网络编程辅助分析工具，掌握网络应用程序的调试和分析技能。

第 2 章　Windows Sockets 编程基础（上机实践 2 学时）

实践内容：

- Windows Sockets 开发环境配置。
- Windows Sockets 相关数据结构定义。
- Windows Sockets 接口的基本函数使用。

考核要求：

通过上机实践，学生应能熟悉 Windows Sockets 的接口功能，掌握 Windows Sockets 开发环境配置，掌握 Windows Sockets DLL 的初始化和释放方法，熟悉 Windows Sockets 的常用数据结构。

第 3 章　基于流式套接字的网络程序设计（上机实践 8 学时）

实践内容：

- 基本流式套接字编程方法。
- 流式套接字的网络功能框架设计。
- 基于流式套接字的并发程序设计。
- 基于流式套接字的网络应用程序运行过程分析。
- 提高网络应用程序对数据流的处理能力。
- 提高网络应用程序的传输效率。

考核要求：

通过上机实践，学生应能掌握流式套接字编程模型和基本函数的使用，能够用简单的回射程序测试和分析网络应用常见的异常现象，对基于流式套接字的网络程序的可靠性保护有合理的处理方法，对基于流式套接字的网络程序的传输效率有客观的测量方法和改进思路，能够排除流式套接字编程中的常见错误。

第 4 章　基于数据报套接字的网络程序设计（上机实践 4 学时）

实践内容：

- 基本数据报套接字编程方法。
- 数据报套接字的网络功能框架设计。
- 无连接应用程序丢包率测试。

考核要求：

通过上机实践，学生应能掌握基于数据报套接字的网络程序设计方法，具备测试和分析网络传输异常现象的能力，重视基于数据报套接字网络程序的不可靠性问题，提高在网络应用程序设计过程中检查错误和排除错误的能力。

第 5 章　基于原始套接字的网络程序设计（上机实践 4 学时）

实践内容：

- 基本原始套接字编程方法。
- 原始套接字的网络功能框架设计。
- 基于原始套接字的通信报文构造和通信过程控制。

考核要求：

通过上机实践，学生应能掌握基于原始套接字的网络程序设计方法，具备测试和分析网络传输异常现象的能力，掌握协议首部构造和控制、网络数据分析的基本方法，提高在网络应用程序设计过程中检查错误和排除错误的能力。

第 6 章　网络 I/O 模型的应用（上机实践 6 学时）

实践内容：

- 基于 I/O 复用模型的网络应用程序设计。
- 基于 WSAAsyncSelect 模型的网络应用程序设计。
- 基于完成端口模型的网络应用程序设计。

考核要求：

通过上机实践，学生应能掌握 Windows I/O 操作的基本原理，掌握 I/O 复用模型、WSAAsyncSelect 模型和完成端口模型的程序设计方法，熟悉各种模型的优缺点，培养在各种应用场景下正确选择 I/O 模型的意识和能力，提高在网络应用程序设计过程中检查错误和排除错误的能力。

第 7 章　WinPcap 编程（上机实践 4 学时）

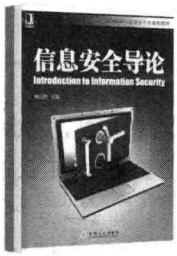
实践内容：

- 基于 WinPcap 的数据构造和发送。
- 基于 WinPcap 的数据接收和控制。

考核要求：

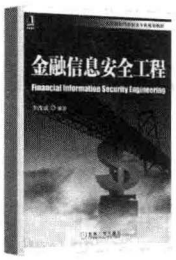
通过上机实践，学生应能掌握 WinPcap 的体系结构和编程开发的基本方法，掌握 WinPcap 编程环境的配置方法，掌握 wpcap.dll 接口库的基本功能，掌握链路层数据帧的构造和处理方法。

推荐阅读



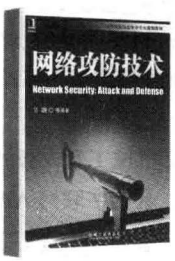
信息安全导论

作者：何泾沙 ISBN：978-7-111-36272-2 定价：33.00元



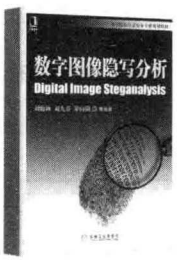
金融信息安全工程

作者：李改成 ISBN：978-7-111-28262-4 定价：35.00元



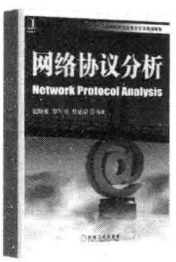
网络攻防技术

作者：吴灏 ISBN：978-7-111-27632-6 定价：29.00元



数字图像隐写分析

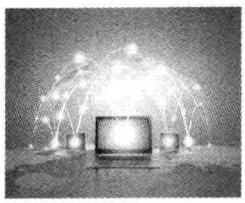
作者：刘粉林 刘九芬 罗向阳 ISBN：978-7-111-30517-07 定价：29.00元



网络协议分析

作者：寇晓蕤 罗军勇 蔡延荣 ISBN：978-7-111-26832-1 定价：33.00元

目　录



第 1 章
网络应用程序运行分析

随着计算机技术的发展和应用的深入，分布式网络应用程序的应用广为流行。这些程序借助网络与分布在不同地域、不同网络、不同系统中的其他应用程序交互。与传统桌面应用程序相比，在网络应用程序中，其数据的位置、访问方式、结构形态等发生了巨大的变化，这使得应用程序编制过程中的调试方法也有了很大区别。本章重点阐述 Windows 系统中的两个常用的网络分析工具：网络流量捕获工具 Wireshark 和网络状态显示工具 netstat，选择邮件登录和迅雷软件下载两种常见的网络应用，设计了软件运行过程分析实验，目的在于帮助读者熟悉常用的网络编程辅助工具，掌握网络应用程序的调试和分析技能。

1.1 实验目的

本章实验的目的是：

1）了解网络编程的常用辅助工具。

2）掌握 Wireshark 的基本操作方法，能够捕获、过滤和分析网络原始数据。

3）掌握 netstat 基本命令的使用。

4）掌握客户端/服务器模型和 P2P 模型的基本原理。

5）能够结合辅助工具逆向分析常用软件的运行过程。

1.2 网络流量捕获工具

1997 年，Gerald Combs 开发了 Ethereal（Wireshark 项目以前的名称），以进行网络问题的跟踪调试，并进一步学习网络知识。经过数次开发、补丁和 Bug 报告，在 1998 年 Ethereal 0.2.0 版诞生。此后不久 Gilbert Ramirez 发现了它的潜力，并为其提供了底层分析能力。1998 年 10 月，Guy Harris 开始对 Ethereal 进行改进，并提供分析；之后，正在进行 TCP/IP 教学的 Richard Sharpe 注意到它在课程教学中的作用，开始从事对 Ethereal 的分析及改进工作。

从那以后，参与 Ethereal 开发和改进的人越来越多，他们为 Ethereal 增加了更多尚不被支持的协议，并为团队提供了改进和回馈。2006 年，Ethereal 被重新命名为 Wireshark。目前，Wireshark 开发小组负责对该项目进一步开发和维护，通过查看 Wireshark 帮助菜单下的 About 选项，可以找到为 Wireshark 提供代码的人员名单。

Wireshark 是一个开源软件项目，发布遵循 GNU General Public Licence（GPL 协议），所有源代码可以在 GPL 框架下免费使用。

Wireshark 的源文件和二进制发行版可以从网站 http://www.wireshark.org.获得。

1.2.1　Wireshark 的安装和卸载

1. 安装 Wireshark

Wireshark 的安装文件可以从 http://www.wireshark.org/download.html#releases 下载，根据操作系统的不同，选择适合版本的安装文件，如图 1-1 所示。

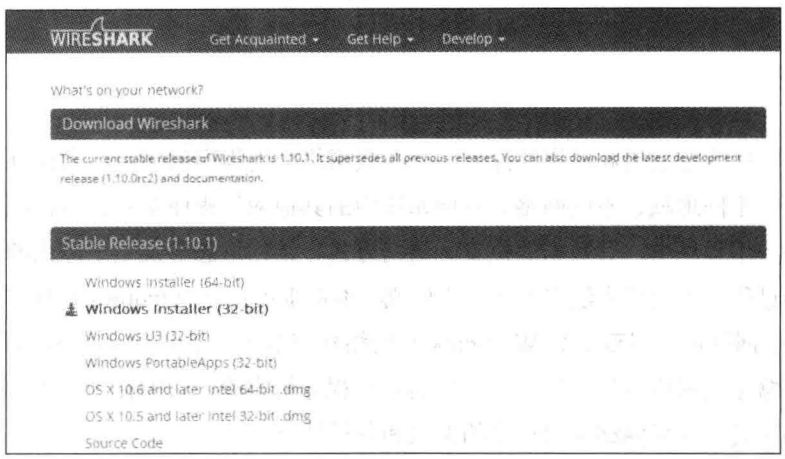


图 1-1　选择 Wireshark 的安装版本

Wireshark 的安装需执行下载的安装文件，以下以 Wireshark 1.10.1（32-bit）为例介绍安装过程，如图 1-2 所示。

单击“Next”按钮，进入授权许可页面，如图 1-3 所示。

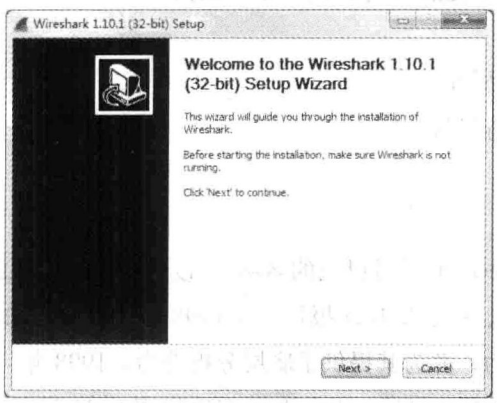


图 1-2　Wireshark 的初始安装界面

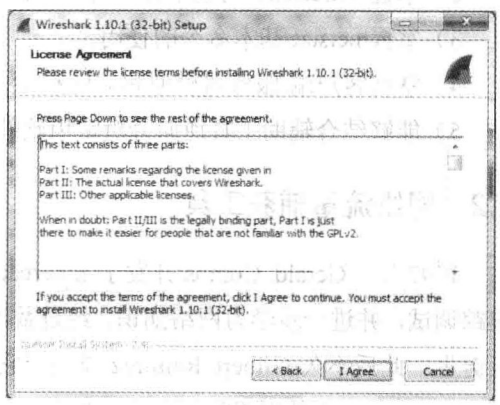


图 1-3　Wireshark 的授权许可页面

单击“I Agree”按钮，选择待安装的组件，如图 1-4 所示。

单击“Next”按钮，对软件快捷启动和文件关联进行配置，如图 1-5 所示。

单击“Next”按钮，选择 Wireshark 的安装目录，如图 1-6 所示。

单击“Next”按钮，Wireshark 安装包包含 WinPcap，WinPcap 是一个在 Windows 平台下访问网络中数据链路层的开源库，能够应用于网络数据帧的构造、捕获和分析。Wireshark 是基于 WinPcap 开发的，选择是否安装 WinPcap，如图 1-7 所示。

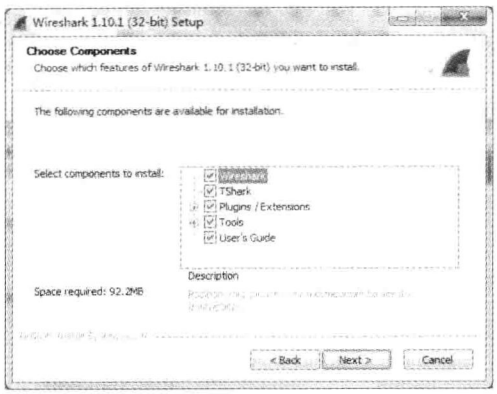


图 1-4　选择 Wireshark 的相关组件

图 1-5　设置 Wireshark 的快捷启动和文件关联

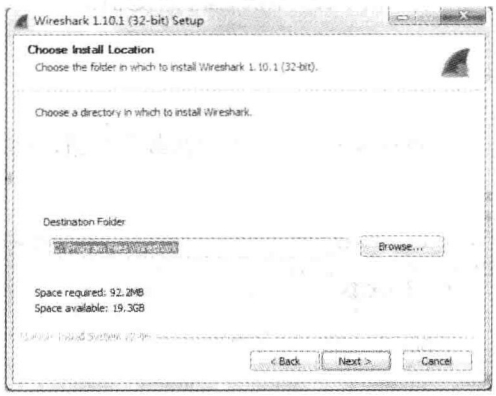


图 1-6　设置 Wireshark 的安装目录

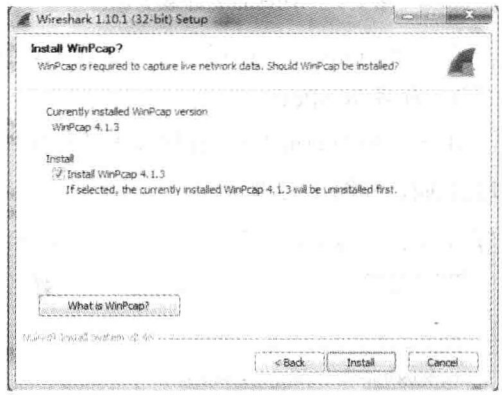


图 1-7　安装 WinPcap

最后，单击“Install”按钮，开始安装 Wireshark 到指定目录。

2. 卸载 Wireshark

进入“控制面板”>“卸载或更改程序”，选择“Wireshark 1.10.1（32-bit）”程序，单击“卸载”按钮，如图 1-8 所示。

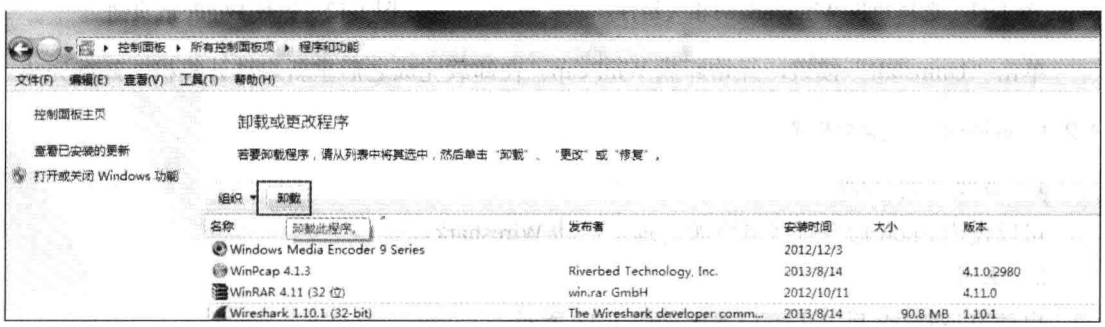


图 1-8　选择卸载 WinPcap

进入卸载页面，如图 1-9 所示。

单击“Next”按钮，显示即将卸载的 Wireshark 所在目录，如图 1-10 所示。

单击“Next”按钮，选择待卸载的已安装组件，如图 1-11 所示。默认配置是卸载核心组件，但保留个人设置和 WinPcap，这是因为其他类似 Wireshark 的程序有可能同样使用 WinPcap。

图 1-9　Wireshark 卸载页面

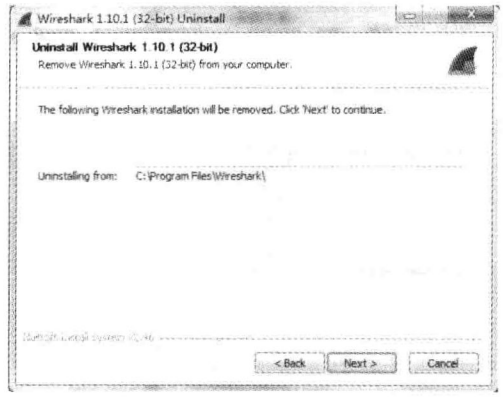


图 1-10　Wireshark 卸载路径

单击“Uninstall”按钮，开始卸载 Wireshark。

3. 卸载 WinPcap

进入“控制面板”>“卸载或更改程序”，选择“WinPcap 4.1.3”，单击“卸载”按钮，进入卸载页面，如图 1-12 所示。

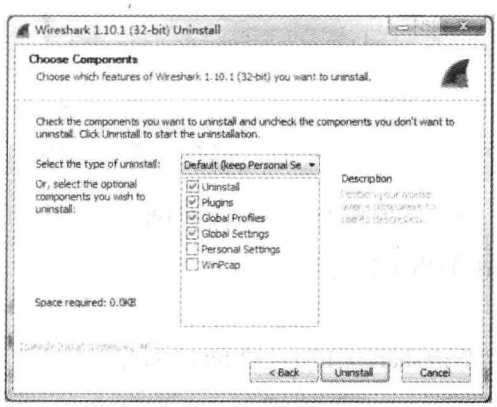


图 1-11　选择卸载 Wireshark 的相关组件

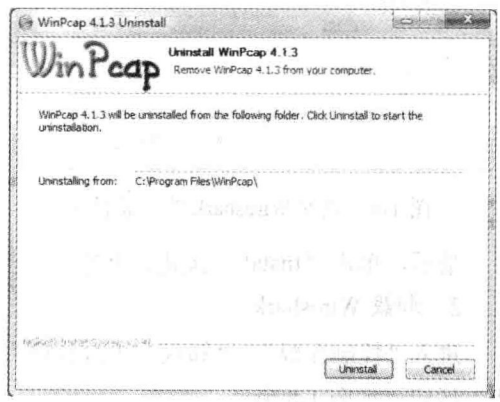


图 1-12　卸载 WinPcap 页面

单击“Uninstall”按钮，开始卸载 WinPcap。在卸载完成之后重新启动计算机，卸载完成。

1.2.2　Wireshark 用户界面

1. 启动 Wireshark

可以使用 Shell 命令行或者资源管理器启动 Wireshark。

2. 主窗口

启动 Wireshark 后，主窗口界面如图 1-13 所示。

Wireshark 主窗口由以下部分组成：

- 菜单：提供了对 Wireshark 进行配置的若干功能项目。
- 主工具栏：提供快速访问菜单中经常用到的项目功能。
- 过滤工具栏：提供处理当前显示过滤的方法。

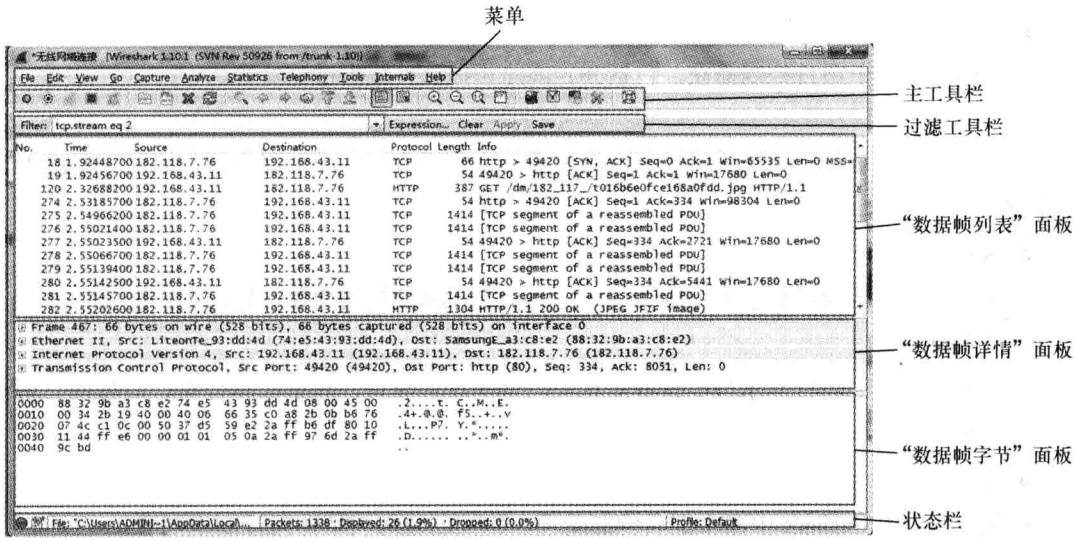


图 1-13　Wireshark 主窗口

- “数据帧列表”面板：显示打开文件的每个帧的摘要。单击面板中的每个条目，帧的其他情况将会显示在另外两个面板中。
- “数据帧详情”面板：显示在“数据帧列表”面板中所选帧的数据解析结果。
- “数据帧字节”面板：显示在“数据帧列表”面板中所选帧的原始数据，以及在“数据帧详情”面板高亮显示的字段。
- 状态栏：显示当前程序状态以及捕获数据的更多详情。

3. 主菜单

Wireshark 主菜单位于 Wireshark 窗口的最上方，图 1-14 显示了主菜单的基本界面。

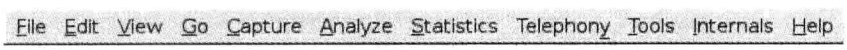


图 1-14　主菜单

主菜单包括以下几个项目：

- File

该菜单包括如下项目：打开、合并捕获文件，保存、打印、导出捕获文件的全部或部分内容，以及退出 Wireshark 等。

- Edit

该菜单包括如下项目：剪切、复制、粘贴、查找帧、时间参考、标记一个或多个帧、设置预设参数。

- View

该菜单包含若干项目控制捕获数据的显示方式，包括颜色、字体缩放，将数据帧显示在分离的窗口，展开或收缩“数据帧详情”面板的树状节点等。

- Go

该菜单包含若干项目设置跳转条件，并根据条件定位到特定数据帧。

- Capture

该菜单包含若干项目控制捕获，包括开始或停止捕获、编辑过滤器等。

- Analyze

该菜单包含若干项目处理显示过滤，允许或禁止分析协议，配置用户指定解码和追踪 TCP 流等功能。

- Statistics

该菜单包含若干项目显示多个统计窗口，包括关于捕获帧的摘要、协议层次统计等。

- Telephony

该菜单包含若干项目显示与电话业务相关的若干统计窗口，包括媒体分析、流程图、协议层次统计等。

- Tools

该菜单包含 Wireshark 中多个工具的启动项，比如创建防火墙访问控制规则等。

- Internals

该菜单包含 Wireshark 内部信息的若干启动项，比如罗列 Wireshark 支持的协议等。

- Help

该菜单包含一些辅助用户的参考内容，如访问一些基本的帮助文件、支持的协议列表、用户手册，在线访问一些网站、程序相关信息等。

4. “File” 菜单

WireShark 的 “File” 菜单包含的项目如图 1-15 所示，其菜单功能如表 1-1 所示。

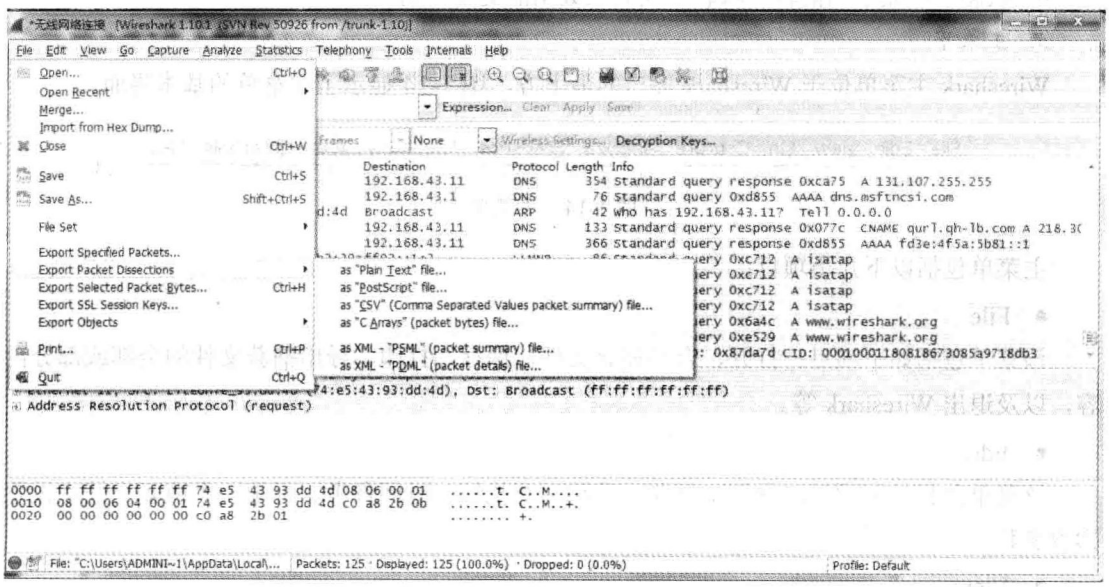


图 1-15 “File” 菜单

5. “Edit” 菜单

WireShark 的 “Edit” 菜单包含的项目如图 1-16 所示，其菜单功能如表 1-2 所示。