Wireshark
数据包分析实战详解

王晓卉　李亚伟　编著

通过80个实例，详细讲解了Wireshark数据包分析实施的8大类技巧
基于Wireshark抓取的数据包，层层剥茧地剖析了12种常见网络协议的构成

- 全面涵盖Wireshark基础知识和应用技巧，以及使用Wireshark对网络协议进行分析
- 遵循规范，从专业的角度循序渐进地讲解了Wireshark抓包及分析的实施流程
- 针对海量数据问题，详细讲解了捕获过滤器、显示过滤器和着色规则等专业技巧
- 以图表结合的形式直观地展示了协议报结构，帮助读者快速掌握各种抽象的网络协议
- 对抓取的数据包按照协议层次，逐层讲解了各个协议在数据包中的体现

清华大学出版社

Wireshark
数据包分析实战详解

王晓卉　李亚伟　编著

清华大学出版社
北　京

内 容 简 介

本书由浅入深，全面系统地介绍了 Wireshark 数据抓包和数据包分析。本书提供了大量实例，供读者实战演练 Wireshark 的各项功能。同时，对抓取的数据包按照协议层次，逐层讲解各个协议在数据包中的体现。这样，读者就可以掌握数据包抓取到信息获取的每个环节。

本书共分 3 篇。第 1 篇介绍 Wireshark 的各项功能，包括基础知识、Wireshark 的定制、捕获过滤器和显示过滤器的使用、数据包的着色、导出和重组等；第 2 篇介绍基于 Wireshark 对 TCP/IP 协议族中常用协议的详细分析，如 ARP、IP、UDP、TCP、HTTP、HTTPS 和 FTP 等；第 3 篇介绍借助 Wireshark 分析操作系统启动过程中的网络通信情况。

本书涉及面广，内容包括工具使用、网络协议和应用。本书适合各类读者群体，如想全面学习 Wireshark 的初学者、网络管理员、渗透测试人员及网络安全专家等。对于网络数据分析人士，本书更是一本不可多得的案头必备参考书。

图书在版编目（CIP）数据

Wireshark 数据包分析实战详解 / 王晓卉，李亚伟编著. —北京：清华大学出版社，2015
ISBN 978-7-302-38871-5

Ⅰ. ①W…　Ⅱ. ①王…　②李…　Ⅲ. ①统计数据－统计分析－应用软件　Ⅳ. ①O212.1-39

中国版本图书馆 CIP 数据核字（2015）第 004772 号

责任编辑：杨如林
封面设计：欧振旭
责任校对：徐俊伟
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京嘉实印刷有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：26.25　　**字　　数**：656 千字
版　　次：2015 年 3 月第 1 版　　**印　　次**：2015 年 3 月第1 次印刷
印　　数：1～3000
定　　价：79.00 元

产品编号：062969-01

前　言

网络的普及给人们的生活带来了极大的便利，同时网络的安全问题也成为公众热点。网络数据抓包和分析作为网络管理和监控最有效的措施，越来越受到网络管理人员和网络安全人员的重视。

Wireshark 作为一款开源的专业数据抓包和分析工具，深受业内人士欢迎。它提供了强大的数据抓取功能和丰富的数据分析方式。面对 Wireshark 强大的功能和海量的数据包，初学者往往无从下手。

笔者结合网络数据传输及安全方面存在的各种问题，经过分析及总结，编写了本书。本书通过专业的数据抓包流程，逐步讲解 Wireshark 各项强大的功能。同时，基于 Wireshark 抓取的数据包，以层层剥茧的形式，讲解常见的各种网络协议。这样读者可以更直接地掌握各种协议类型的数据包。

通过本书的学习，读者不仅可以轻松掌握 Wireshark 的使用，踏入网络数据分析的大门，还可以更为直观地理解 TCP/IP 各个协议，以及这些协议在数据包中的表现。掌握这些技术，再加以充分的练习，就可以轻松应对网络数据分析等各项工作。

本书特色

1. 内容全面、系统、深入

本书介绍了 Wireshark 的基础知识、捕获过滤器和显示过滤器的使用、对数据包进行导出或重组等。然后，介绍了使用 Wireshark 对各种协议的详细分析。最后，还详细分析了操作系统启动过程的数据包。

2. 贴近实际，专业讲解

本书按照 Wireshark 专业使用流程，对其功能进行详细讲解，帮助读者掌握最高效的数据抓包、分析技术，以解决各种复杂的网络问题。同时，针对围绕海量数据包处理问题，本书详细介绍相关技术，如抓取过滤器、显示过滤器、着色规则等功能。

3. 直观讲解网络协议

对于网络数据包涉及的网络协议，本书给以最直观的讲解。首先分析协议的工作原理以及相关数据包的构成，然后对照 Wireshark 数据包视图进行逐条比对，帮助读者以最直观的形式学习和掌握各个网络协议。

4. 提供多种学习和交流的方式

为了方便大家学习和交流，我们提供了多种方式。读者可以在论坛 www.wanjuanchina.

net 上发帖讨论 Wireshark 相关技术；也可以通过 QQ 群 336212690 转入对应的 Wireshark 技术群；还可以就图书阅读中遇到的问题致信 book@wanjuanchina.net 或 bookservice2008@163.com，以获得帮助。

本书内容及体系结构

第1篇　Wireshark应用篇（第1～9章）

本篇主要内容包括：Wireshark 的基础知识、设置 Wireshark 视图、捕获过滤器技巧、显示过滤器技巧、着色规则和数据包导出、构建图表、重组数据、添加注释等。通过本篇的学习，读者可以掌握 Wireshark 的基本操作，灵活地使用捕获过滤器和显示过滤器，并可以对 Wireshark 中的数据进行重组构建图表等。

第2篇　网络协议分析篇（第10～20章）

本篇主要内容包括：ARP 协议抓包分析、互联网协议（IP）抓包分析、UDP 协议抓包分析、TCP 协议抓包分析、ICMP 协议抓包分析、DHCP 数据抓包分析、DNS 抓包分析、HTTP 协议抓包分析、HTTPS 协议抓包分析、FTP 协议抓包分析和电子邮件抓包分析。通过本篇的学习，读者可以掌握 TCP/IP 协议族中每层中包括的协议、协议的格式及传输的数据等。

第3篇　实战篇（第21章）

本篇主要内容包括：操作系统启动过程抓包分析。通过本篇的学习，读者可以掌握一个操作系统启动过程中会自动开启哪些服务、获取地址的过程及启动的一些应用程序等。

本书配套资源获取方式

本书涉及的源程序、工具及接线图等资源需要读者自行下载。请登录清华大学出版社的网站 http://www.tup.com.cn，搜索到本书页面后按照提示下载即可。另外，读者也可以到 www.wanjuanchina.net 社区的相关版块下载。

本书读者对象

- Wireshark 初学者；
- 想全面学习 Wireshark 的人员；
- 各种兴趣爱好者；
- 网络管理员；
- 专业的安全渗透测试人员；
- 大中专院校的学生；
- 社会培训班学员。

本书作者

本书由王晓卉、李亚伟编写，其中营口职业技术学院的王晓卉负责编写第 1～9 章，李亚伟负责编写第 10～21 章。其他参与编写的人员有陈刚、陈世琼、黄点点、黄海力、黄绍斌、蒋春蕾、李国良、李俊娜、李晓娜、刘永纯、王书勇、王挺、王文强、张伟、张小华、胡丹萍、王以荣、徐阳。

阅读本书的过程中若有任何疑问，都可以发邮件或者在论坛和 QQ 群里提问，会有专人为您解答。最后顺祝各位读者读书快乐！

编者

目　录

第 1 篇　Wireshark 应用篇

第 2 篇 网络协议分析篇

第 3 篇 实战篇

第 1 篇　Wireshark 应用篇

第 1 章　Wireshark 的基础知识

Wireshark（前称 Ethereal）是一个网络包分析工具。该工具主要是用来捕获网络包，并显示包的详细情况。本章将介绍 Wireshark 的基础知识。

1.1　Wireshark 的功能

在学习 Wireshark 之前，首先介绍一下它的功能。了解它的功能，可以帮助用户明确借助该工具能完成哪些工作。本节将介绍 Wireshark 的基本功能。

1.1.1　Wireshark 主窗口界面

在学习使用 Wireshark 之前，首先需要了解该工具主窗口界面中每部分的作用。Wireshark 主窗口界面如图 1.1 所示。

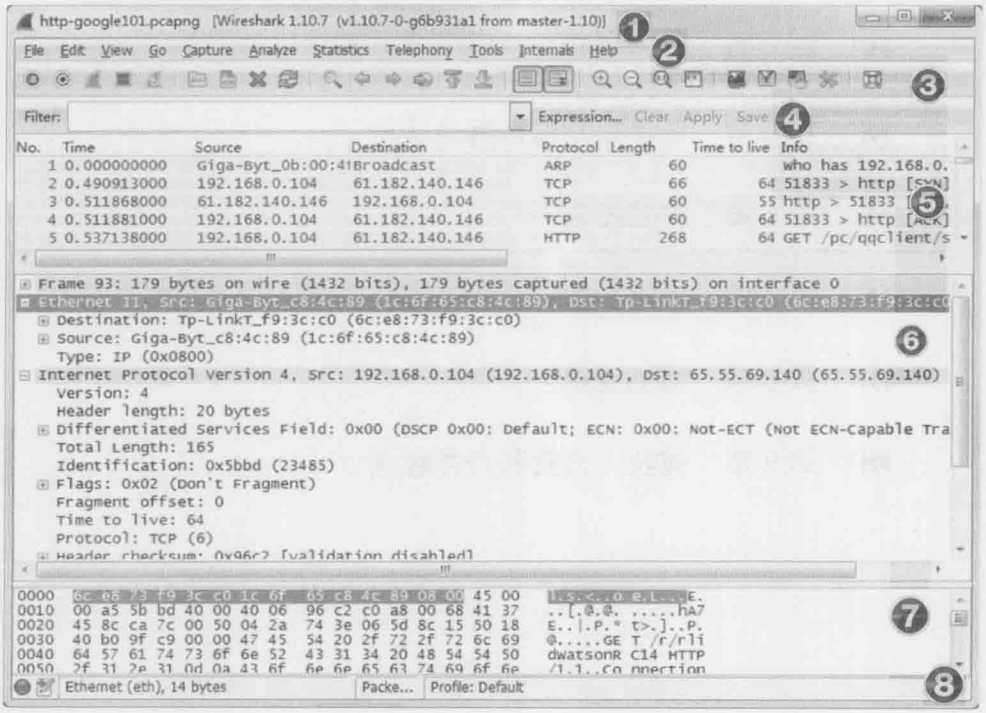

图 1.1　Wireshark 主窗口界面

在图 1.1 中，以编号的形式已将 Wireshark 主窗口每部分标出。下面分别介绍每部分的含义，如下所示。

- ① 标题栏——用于显示文件名称、捕获的设备名称和 Wireshark 版本号。
- ② 菜单栏——Wireshark 的标准菜单栏。
- ③ 工具栏——常用功能快捷图标按钮。
- ④ 显示过滤区域——减少查看数据的复杂度。
- ⑤ Packet List 面板——显示每个数据帧的摘要。
- ⑥ Packet Details 面板——分析封包的详细信息。
- ⑦ Packet Bytes 面板——以十六进制和 ASCII 格式显示数据包的细节。
- ⑧ 状态栏——专家信息、注释、包数和 Profile。

1.1.2　Wireshark 的作用

Wireshark 是一个广受欢迎的网络数据包分析软件。网络数据包分析软件的功能是截取网络数据包，并尽可能显示出最为详细的网络数据包数据。它是一个最知名的开源应用程序安全工具。Wireshark 可以运行在 Windows、MAC OS X、Linux 和 UNIX 操作系统上，它甚至可以作为一个 Portable App 运行。本小节将介绍 Wireshark 的常用功能。使用 Wireshark 可以快速分析一些任务，如下所示。

1. 一般分析任务

- 找出在一个网络内发送数据包最多的主机。
- 查看网络通信。
- 查看某个主机使用了哪些程序。
- 基本正常的网络通信。
- 验证特有的网络操作。
- 了解尝试连接无线网络的用户。
- 同时捕获多个网络的数据。
- 实施无人值守数据捕获。
- 捕获并分析到/来自一个特定主机或子网的数据。
- 通过 FTP 或 HTTP 查看和重新配置文件传输。
- 从其他捕获工具导入跟踪文件。
- 使用最少的资源捕获数据。

2. 故障任务

- 为故障创建一个自定义的分析环境。
- 确定路径、客户端和服务延迟。
- 确定 TCP 问题。
- 检查 HTTP 代理问题。
- 检查应用程序错误响应。
- 通过查看图形显示的结果，找出相关的网络问题。