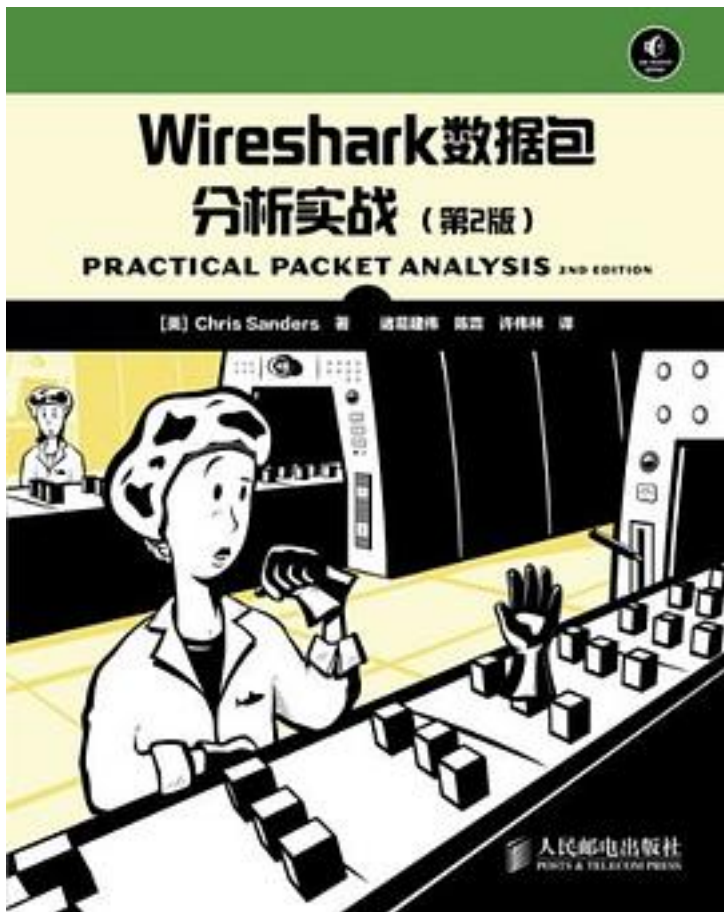


# Wireshark数据包分析实战



[Wireshark数据包分析实战\\_下载链接1](#)

著者:[美]Chris Sanders

出版者:人民邮电出版社

出版时间:2013-3

装帧:平装

isbn:9787115302366

《Wireshark数据包分析实战(第2版)》从网络嗅探与数据包分析的基础知识开始，渐进地介绍Wireshark的基本使用方法及其数据包分析功能特性，同时还介绍了针对不同协议层与无线网络的具体实践技术与经验技巧。在此过程中，作者结合一些简单易懂的实际网络案例，图文并茂地演示使用Wireshark进行数据包分析的技术方法，使读者能够

顺着本书思路逐步地掌握网络数据包嗅探与分析技能。最后，《Wireshark数据包分析实战(第2版)》使用网络管理员、IT技术支持、应用程序开发者们经常遇到的实际网络问题(包括无法正常上网、程序连接数据库错误、网速很卡，以及遭遇扫描渗透、ARP欺骗攻击等)，来讲解如何应用Wireshark数据包分析技术和技巧，快速定位故障点，并找出原因以解决实际问题。《Wireshark数据包分析实战(第2版)》覆盖了无线WiFi网络中的嗅探与数据包分析技术，同时也给出了嗅探与数据包分析领域丰富的参考技术文档、网站、开源工具与开发库等资源列表。

《Wireshark数据包分析实战(第2版)》适合网络管理员、安全工程师、软件开发工程师与测试人员，以及网络工程、信息安全等专业学生与网络技术爱好者阅读。

作者介绍:

Chris

Sanders，是一名计算机安全咨询顾问、作家和研究人员。他还是一名SANS导师，持有CISSP、GCIA、GCIH、GREM等行业证书，并定期在WindowsSecurity.com网站和自己的博客ChrisSanders.org发表文章。Sanders每天都会使用Wireshark进行数据包分析。他目前居住在美国南卡罗来纳州查尔斯顿，以国防承包商的身份工作。

目录: 目录

## 第1章 数据包分析技术与网络基础 1

### 1.1 数据包分析与数据包嗅探器 2

#### 1.1.1 评估数据包嗅探器 2

#### 1.1.2 数据包嗅探器工作原理 3

### 1.2 网络通信原理 4

#### 1.2.1 协议 4

#### 1.2.2 七层OSI参考模型 5

#### 1.2.3 数据封装 8

#### 1.2.4 网络硬件 10

### 1.3 流量分类 15

#### 1.3.1 广播流量 15

#### 1.3.2 多播流量 16

#### 1.3.3 单播流量 16

### 1.4 小结 17

## 第2章 监听网络线路 19

### 2.1 混杂模式 20

### 2.2 在集线器连接的网络中进行嗅探 21

### 2.3 在交换式网络中进行嗅探 23

#### 2.3.1 端口镜像 23

#### 2.3.2 集线器输出 25

#### 2.3.3 使用网络分流器 26

#### 2.3.4 ARP欺骗 29

### 2.4 在路由网络环境中进行嗅探 34

### 2.5 部署嗅探器的实践指南 36

## 第3章 Wireshark入门 39

### 3.1 Wireshark简史 39

### 3.2 Wireshark的优点 40

### 3.3 安装Wireshark 41

#### 3.3.1 在微软Windows系统中安装 41

- 3.3.2 在Linux系统中安装 43
- 3.3.3 在Mac OS X系统中安装 45
- 3.4 Wireshark初步入门 45
- 3.4.1 第一次捕获数据包 45
- 3.4.2 Wireshark主窗口 46
- 3.4.3 Wireshark首选项 48
- 3.4.4 数据包彩色高亮 49

## 第4章 玩转捕获数据包 53

- 4.1 使用捕获文件 53
- 4.1.1 保存和导出捕获文件 54
- 4.1.2 合并捕获文件 55
- 4.2 分析数据包 55
- 4.2.1 查找数据包 56
- 4.2.2 标记数据包 57
- 4.2.3 打印数据包 57
- 4.3 设定时间显示格式和相对参考 58
- 4.3.1 时间显示格式 58
- 4.3.2 数据包的相对时间参考 59
- 4.4 设定捕获选项 60
- 4.4.1 捕获设定 61
- 4.4.2 捕获文件设定 61
- 4.4.3 停止捕获选项 62
- 4.4.4 显示选项 62
- 4.4.5 名字解析选项 63
- 4.5 使用过滤器 63
- 4.5.1 捕获过滤器 63
- 4.5.2 显示过滤器 69
- 4.5.3 保存过滤器 72

## 第5章 Wireshark高级特性 75

- 5.1 网络端点和会话 75
- 5.1.1 查看端点 76
- 5.1.2 查看网络会话 77
- 5.1.3 使用端点和会话窗口进行问题定位 78
- 5.2 基于协议分层结构的统计数据 79
- 5.3 名字解析 81
- 5.3.1 开启名字解析 81
- 5.3.2 名字解析的潜在弊端 82
- 5.4 协议解析 82
- 5.4.1 更换解析器 82
- 5.4.2 查看解析器源代码 85
- 5.5 跟踪TCP流 85
- 5.6 数据包长度 86
- 5.7 图形展示 88
- 5.7.1 查看IO图 88
- 5.7.2 双向时间图 90
- 5.7.3 数据流图 91
- 5.8 专家信息 92

## 第6章 通用底层网络协议 95

- 6.1 地址解析协议 96
- 6.1.1 ARP头 97
- 6.1.2 数据包1: ARP请求 98

6.1.3 数据包2: ARP响应	99
6.1.4 无偿的ARP	100
6.2 互联网协议	101
6.2.1 IP地址	102
6.2.2 IPv4头	103
6.2.3 存活时间	104
6.2.4 IP分片	107
6.3 传输控制协议	109
6.3.1 TCP头	109
6.3.2 TCP端口	110
6.3.3 TCP的三次握手	113
6.3.4 TCP终止	116
6.3.5 TCP重置	117
6.4 用户数据报协议	118
6.5 互联网控制消息协议	119
6.5.1 ICMP头	119
6.5.2 ICMP类型和消息	120
6.5.3 Echo请求与响应	120
6.5.4 路由跟踪	122

第7章 常见高层网络协议	127
7.1 动态主机配置协议DHCP	127
7.1.1 DHCP头结构	128
7.1.2 DHCP续租过程	129
7.1.3 DHCP租约内续租	134
7.1.4 DHCP选项和消息类型	134
7.2 域名系统	135
7.2.1 DNS数据包结构	135
7.2.2 一次简单的DNS查询过程	136
7.2.3 DNS问题类型	138
7.2.4 DNS递归	139
7.2.5 DNS区域传送	142
7.3 超文本传输协议	145
7.3.1 使用HTTP浏览	145
7.3.2 使用HTTP传送数据	147
7.4 小结	149

第8章 基础的现实世界场景	151
8.1 数据包层面的社交网络	152
8.1.1 捕获Twitter流量	152
8.1.2 捕获Facebook流量	156
8.1.3 比较Twitter和Facebook的方法	158
8.2 捕获ESPN.com流量	159
8.2.1 使用会话窗口	159
8.2.2 使用协议分层统计窗口	160
8.2.3 查看DNS流量	161
8.2.4 查看HTTP请求	162
8.3 现实世界问题	163
8.3.1 无法访问Internet: 配置问题	163
8.3.2 无法访问Internet: 意外重定向	166
8.3.3 无法访问Internet: 上游问题	169
8.3.4 打印机故障	172
8.3.5 分公司之困	175
8.3.6 生气的开发者	179

## 8.4 小结 184

## 第9章 让网络不再卡 185

### 9.1 TCP的错误恢复特性 186

#### 9.1.1 TCP重传 186

#### 9.1.2 TCP重复确认和快速重传 189

### 9.2 TCP流控制 194

#### 9.2.1 调整窗口大小 195

#### 9.2.2 用零窗口通知停止数据流 196

#### 9.2.3 TCP滑动窗口实战 197

### 9.3 从TCP错误控制和流量控制中学到的 200

### 9.4 定位高延迟的原因 201

#### 9.4.1 正常通信 202

#### 9.4.2 慢速通信——线路延迟 202

#### 9.4.3 慢速通信——客户端延迟 203

#### 9.4.4 慢速通信——服务器延迟 204

#### 9.4.5 延迟定位框架 204

### 9.5 网络基线 205

#### 9.5.1 站点基线 206

#### 9.5.2 主机基线 207

#### 9.5.3 应用程序基线 208

#### 9.5.4 基线的其他注意事项 209

### 9.6 小结 209

## 第10章 安全领域的数据包分析 211

### 10.1 网络侦察 212

#### 10.1.1 SYN扫描 212

#### 10.1.2 操作系统指纹术 216

### 10.2 漏洞利用 219

#### 10.2.1 极光行动 219

#### 10.2.2 ARP缓存中毒攻击 225

#### 10.2.3 远程访问特洛伊木马 229

### 10.3 小结 236

## 第11章 无线网络数据包分析 237

### 11.1 物理因素 237

#### 11.1.1 一次嗅探一个信道 238

#### 11.1.2 无线信号干扰 239

#### 11.1.3 检测和分析信号干扰 239

### 11.2 无线网卡模式 240

### 11.3 在Windows上嗅探无线网络 242

#### 11.3.1 配置AirPcap 242

#### 11.3.2 使用AirPcap捕获流量 243

### 11.4 在Linux上嗅探无线网络 244

### 11.5 802.11数据包结构 246

### 11.6 在Packet List面板增加无线专用列 247

### 11.7 无线专用过滤器 248

#### 11.7.1 筛选特定BSS ID的流量 249

#### 11.7.2 筛选特定的无线数据包类型 249

#### 11.7.3 筛选特定频率 250

### 11.8 无线网络安全 251

#### 11.8.1 成功的WEP认证 251

#### 11.8.2 失败的WEP认证 253

#### 11.8.3 成功的WPA认证 253

11.8.4 失败的WPA认证 255

11.9 小结 256

附录A 延伸阅读 257

• • • • • [\(收起\)](#)

[Wireshark数据包分析实战\\_下载链接1](#)

标签

wireshark

网络分析

网络

抓包

TCP/IP

计算机网络

网络安全

计算机

评论

: TP393.09/7924

-----  
其实都可以当一本不错的计算机网络科普书了。因为围绕“抓包”话题，实操性也很强。对 TCP 拥塞控制的介绍尤其超预期。不过最后实操分析浏览器流量的章节有点过时，几个范例

网站都已经全面 HTTPS，书中并没有介绍如何做中间人证书，或者利用 Firefox 的开发者功能分享 TLS master key 给 Wireshark。

---

入门过一遍

---

入门书籍。推荐。后期应该再搭配一本wireshark工具书类型的，如cookbook

---

200多页的小书花专门两章讲 tcp/ip 协议栈基本原理是不是太奢侈了，集中讲 wireshark 就好了嘛

---

文章后面有一些攻击分析和参考资源。

---

思路和结构十分清晰，第一版的书评说：“各层次网络管理员必备手册。” “新手入门的最佳读物！”，说的没错。更难得的是，翻译的非常好。没什么好怕的，都只是一些数据包而已。

---

好玩，用Wireshark发现：当用网易邮箱大师登陆浙大邮箱的时候，可以抓到一个包，里面有明文的密码哈哈。看来邮箱大师和我校邮箱都不怎么样惹

---

讲的比较初级，工具这东西，还是要遇到问题实际去使用才能掌握

---

抓包经典

---

当用户手册看的，内容真的没什么，挺一般的吧

---

偏基础的入门科普书

---

抓包工具书

---

工具书

---

中文版的就是快 用了两个半天的实习时间就给finish了  
基本对wireshark有了框架性的了解 还是要实践才行  
不过感觉网络安全的大门就此打开了 日语也可以和几个日本哥们练习 实习还是不错的  
虽然很辛苦 论文压力很大 但是实习真的受益颇丰 因为只有少许补助  
所以心里上的压力算是没有的 接下来要好好读英文版的了

---

内容太少

---

流量题实在做不下去了回头补基础。还挺好的，对数通一窍不通的人也能够一口气阅读。  
看完之后就开始刷题啦！

---

1~7

---

好书，必读

---

最后两章没看，算是复习了一下计网的基本原理。第8章喜欢，跟破案故事一样哈哈  
。

---

[Wireshark数据包分析实战 下载链接1](#)



## 书评

首先说这本啦： <http://book.douban.com/subject/21691692/>

初学者必备，介绍了wireshark安装，嗅探网络流量，wireshark的基本使用，用wireshark分析了一圈常用的TCP，UDP协议，也简要分析了HTTP等应用层协议，概要介绍了一些TCP重传的机制，最后是无线分析 整个书定位应该是...

-----  
如果你手头宽裕，又想学习wireshark细节功能的话，这本书还是值得买的。  
关于wireshark监控网络流量作图问题，想来很多人都问过。这本书给出了作图的实例。  
TCP专家信息也有一些有用的监控。

-----  
这主要是一本工具书，可以在忘记怎么使用的时候翻翻，比起看英文的帮助文档会快一些。  
内容主要涉及：计算机网络的基础知识、如何在合理的位置抓包、wireshark配置、各种协议的数据格式以及它们在wireshark上的样子、最后两章节涉及到了网络安全、无线抓包。书中也有很...

-----  
值得购买 《wireshark 数据包分析实战》主要介绍了如何使用 wireshark 分析网络数据。该书既介绍了 wireshark 捕获捕获、保存、分析数据包的基本操作，也介绍了使用 wireshark 中 analysis 和 statics 分析网络情况的高级用法。既有 eth、arp、ip、tcp、udp、dns 等网络协议的...

-----  
[Wireshark数据包分析实战\\_下载链接1](#)