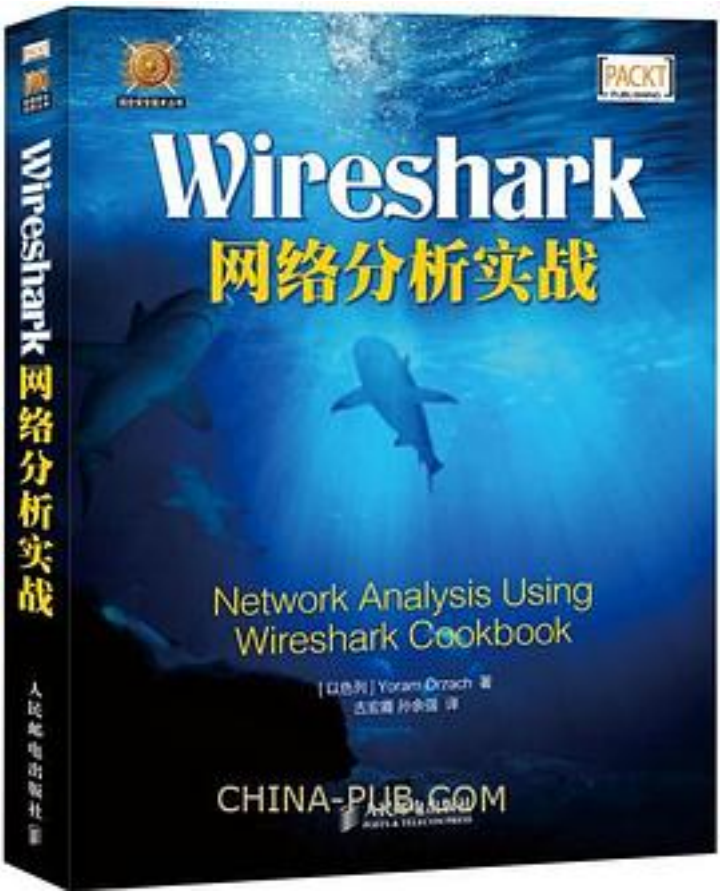
Wireshark网络分析实战



Wireshark网络分析实战_下载链接1_

著者:[以色列 Yoram Orzach

出版者:人民邮电出版社

出版时间:2015-1

装帧:平装

isbn:9787115377715

本书采用步骤式为读者讲解了一些使用Wireshark来解决网络实际问题的技巧。

本书共分为14章，其内容涵盖了Wireshark的基础知识，抓包过滤器的用法，显示过滤器的用法，基本/高级信息统计工具的用法，Expert

Info工具的用法，Wiresahrk在Ethernet、LAN及无线LAN中的用法，ARP和IP故障分析，TCP/UDP故障分析，HTTP和DNS故障分析，企业网应用程序行为分析，SIP、多媒体和IP电话，排除由低带宽或高延迟所引发的故障，认识网络安全等知识。

本书适合对Wireshark感兴趣的网络从业人员阅读，还适合高校网络相关专业的师生阅读。

作者介绍:

Yoram Orzach 毕业于色列技术学院（Israel Institute of Technology），持有该校科学学士学位。1991-1995年，以系统工程师的身份就职于Bezeq公司，从事传输及接入网相关工作。1995年，从Leadcom集团（Leadcom group）加盟Netplus公司，并转型为技术管理者。自1999年起，开始担任NDI通信公司（NDI Communications，http://www.ndi-com.com/）的CTO，负责并参与该公司在全球范围内的数通网络的设计、实施及故障排除工作。Yoram对大型企业网络、服务提供商网络及Internet服务提供商网络极有心得，Comverse、Motorola、Intel、 Ceragon networks、Marvel以及HP等公司都接受过他提供的服务。Yoram在网络设计、实施及故障排除方面浸淫多年，在研发（R&D）、工程、IT团队的培训方面也有丰富的经验。

目录: 第1章 Wireshark简介 1
1.1 Wireshark简介 1
1.2 安置Wireshark（程序或主机） 2
1.3 开始抓包 9
1.4 配置启动窗口 14
1.5 配置时间参数 20
1.6 定义配色规则 22
1.7 数据文件的保存、打印及导出 24
1.8 通过Edit菜单中的Preferences菜单项，来配置Wireshark主界面 28
1.9 配置Preferences窗口中的Protocol选项 33
第2章 抓包过滤器的用法 37
2.1 简介 37
2.2 配置抓包过滤器 38
2.3 配置Ethernet过滤器 42
2.4 配置主机和网络过滤器 46
2.5 配置TCP/UDP及端口过滤器 50
2.6 配置复合型过滤器 53
2.7 配置字节偏移和净载匹配型过滤器 55
第3章 显示过滤器的用法 58
3.1 简介 58
3.2 配置显示过滤器 59
3.3 配置Ethernet、ARP、主机和网络过滤器 67
3.4 配置TCP/UDP过滤器 71
3.5 配置协议所独有的显示过滤器 78
3.6 配置字节偏移型过滤器 81
3.7 配置显示过滤器宏 82
第4章 基本信息统计工具的用法 84
4.1 简介 84
4.2 Statistics菜单中Summary工具的用法 85
4.3 Statistics菜单中Protocol Hierarchy工具的用法 87
4.4 Statistics菜单中Conversation工具的用法 90

4.5 Statistics菜单中Endpoints工具的用法 94
4.6 Statistics菜单中HTTP工具的用法 96
4.7 配置Flow Graph（数据流图），来查看TCP流 101
4.8 生成与IP属性有关的统计信息 103
第5章 高级信息统计工具的用法 107
5.1 简介 107
5.2 配置与显示过滤器结合使用的IO Graphs工具，来定位与网络性能有关的问题 108
5.3 用IO Graphs工具测算（链路的）吞吐量 112
5.4 IO Graphs工具的高级配置方法（启用Y轴Unit参数的Advanced选项） 117
5.5 TCP StreamGraph菜单项中Time-Sequence (Stevens)子菜单项的用法 125
5.6 TCP StreamGraph菜单项中Time-Sequence (tcp-trace)子菜单项的用法 128
5.7 TCP StreamGraph菜单项中Throughput Grap子菜单项的用法 131
5.8 TCP StreamGraph菜单项中Round Trip Time Graph子菜单项的用法 133
5.9 TCP StreamGraph菜单项中Window Scaling Graph子菜单项的用法 135
第6章 Expert Info工具的用法 137
6.1 简介 137
6.2 如何使用Expert Info工具执行排障任务 137
6.3 认识Errors事件 145
6.4 认识Warnings事件 147
6.5 认识Notes事件 149
第7章 Ethernet、LAN交换及无线LAN 152
7.1 简介 152
7.2 发现广播及错包风暴 152
7.3 生成树协议分析 159
7.4 VLAN和VLAN tagging故障分析 168
7.5 无线LAN（WiFi）故障分析 172
第8章 ARP和IP故障分析 177
8.1 简介 177
8.2 与ARP有关的连通性网络故障分析 178
8.3 IP流量分析工具的用法 186
8.4 利用GeoIP来查询IP地址的归属地 189
8.5 发现IP包分片问题 192
8.6 路由选择故障分析 197
8.7 发现IP地址冲突 200
8.8 DHCP故障分析 204
第9章 UDP/TCP故障分析 208
9.1 简介 208
9.2 配置Preferences窗口内protocol选项下的UDP和TCP协议参数，为排除排障做准备 209
9.3 TCP连接故障 213
9.4 TCP重传现象——源头及原因 219
9.5 重复确认（duplicate ACKs）和快速重传（fast retransmissions）现象 229
9.6 TCP报文段失序现象 232
9.7 TCP Zero Window、Window Full、Window Change以及其他包含Window字样的提示信息 235
9.8 TCP重置（reset）及原因 240
第10章 HTTP和DNS 242
10.1 简介 242
10.2 筛选DNS流量 243
10.3 分析DNS协议的常规运作机制 247
10.4 DNS故障分析 252
10.5 筛选HTTP流量 260
10.6 配置Preferences窗口中protocol选项下的HTTP协议参数 263
10.7 HTTP故障分析 266

10.8 导出HTTP对象 272
10.9 HTTP数据流分析及Follow TCP Stream窗口 274
10.10 HTTPS协议流量分析——SSL/TLS基础 277
第11章 企业网应用程序行为分析 286
11.1 简介 286
11.2 摸清流淌于网络中的流量的类型 287
11.3 FTP故障分析 289
11.4 E-mail协议（POP、IMAP、SMTP）流量及故障分析 295
11.5 MS-TS 和Citrix故障分析 305
11.6 NetBIOS协议故障分析 308
11.7 数据库流量及常见故障分析 317
第12章 SIP、多媒体和IP电话 322
12.1 简介 322
12.2 使用内置于Wireshark 的IP电话及多媒体流量专用分析工具 323
12.3 SIP故障分析 330
12.4 RTP/RTCP故障分析 341
12.5 视频及视频监控应用排障场景 349
12.6 IPTV应用排障场景 353
12.7 视频会议应用排障场景 354
12.8 排除RTSP协议故障 356
第13章 排除由低带宽或高延迟所引发的故障 361
13.1 简介 361
13.2 测量通信链路的总带宽 361
13.3 测量每个用户及每种应用所占用的通信链路的带宽 366
13.4 借助Wireshark，获悉链路上的延迟及抖动状况 367
13.5 发现因高延迟/高抖动所引发的应用程序故障 370
第14章 认识网络安全 377
14.1 简介 377
14.2 发现异常流量模式 378
14.3 发现基于MAC地址和基于ARP的攻击 384
14.4 发现ICMP和TCP SYN/端口扫描 385
14.5 发现DoS/DDoS攻击 393
14.6 发现高级TCP攻击 397
14.7 发现暴力破解（brute-force）攻击 400
附录 链接、工具及阅读资料 405
・・・・・・・(收起)

Wireshark网络分析实战_下载链接1_

标签

网络

wireshark

计算机

Wireshark

抓包

协议

web

逆向工程

评论

这本书的译者我觉得太可爱了，书里面有不少译者的吐槽，吐槽作者的文笔和技术能力，所以读了之后我得出了一个结论：译者的语言实力和技术实力在作者之上。。哈哈

译者吐槽一绝

书两颗星，一颗星给翻译。

---
wireshark的使用、capture/display filter、统计、分析、TCP/IP各层的典型问题、排查思路，这些讲得比较全面，对于初/中级的troubleshooting足够了。不足的地方是协议原理略浅，尤其是TCP。

---
wireshark基础知识

将常见的网络问题和排查思路写的比较清晰，同时也补充了不少协议栈原理的知识，挺好的。 不过我觉得没有林沛满的书写的好!

图书馆借的，草草读了一遍。开发人员了解一下即可

粗粗读完。 译者的吐槽很是有意思。
“原文不忍卒读”“要骂就骂作者”“掠过不表”“原文不入流”“完全是外行的写法”“真替作者着急”，如此种种...
其实当初接任务就一句敬谢不敏的事儿，非给自己罪受，学术圈氛围，可见一斑

书还是很不错的，感觉译者戾气比较重。

Wireshark网络分析实战_下载链接1_

书评

很久以前同事和我说过，同一个题材的书籍，读外文翻译的书籍比国内的要好，倒不是因为外国书的整体质量高，而是因为在外文编辑那里烂书都被过滤掉了。
这本书的内还可以，当然，要我说其实还是不够贴近实战，而且文章的组织也不是很好，这点译者已经多次吐槽，我就不多说了。 ...

Wireshark网络分析实战_下载链接1_