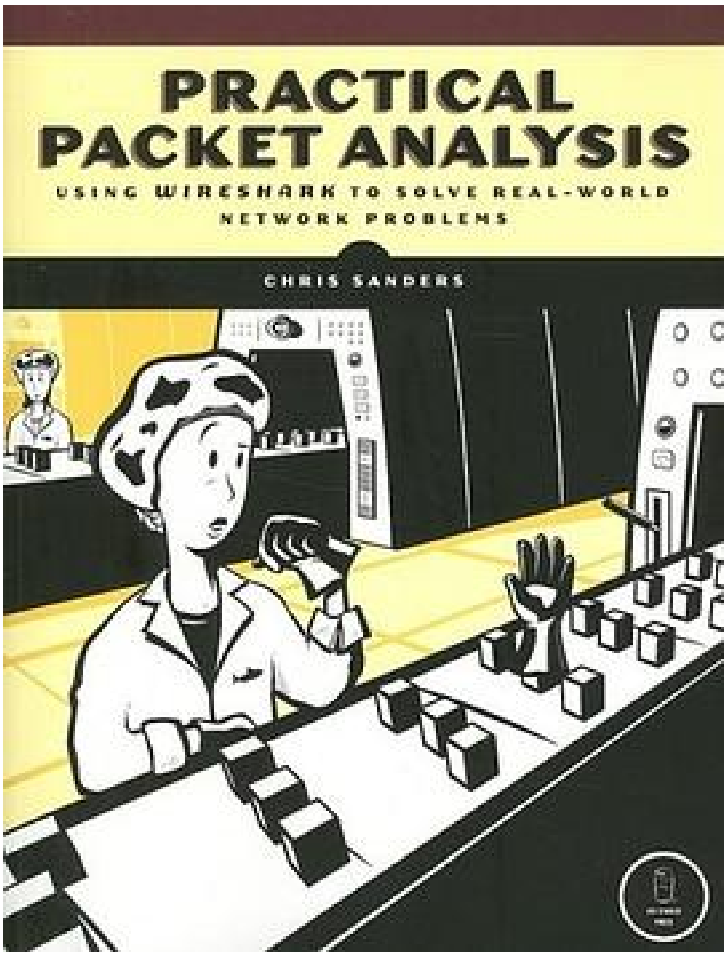
Practical Packet Analysis


PRACTICAL PACKET ANALYSIS
USING WIRESHARK TO SOLVE REAL-WORLD NETWORK PROBLEMS
CHRIS SANDERS

Practical Packet Analysis_下载链接1_

著者:Chris Sanders

出版者:No Starch Press

出版时间:2007-05-23

装帧:Paperback

isbn:9781593271497

Product Description

It's easy enough to install Wireshark and begin capturing packets off the wire--or from the air. But how do you interpret those packets once you've captured them? And how can those packets help you to better understand what's going on under the hood of your network? Practical Packet Analysis shows how to use Wireshark to capture and then analyze packets as you take an indepth look at real-world packet analysis and network troubleshooting. The way the pros do it.

Wireshark (derived from the Ethereal project), has become the world's most popular network sniffing application. But while Wireshark comes with documentation, there's not a whole lot of information to show you how to use it in real-world scenarios. Practical Packet Analysis shows you how to:

* Use packet analysis to tackle common network problems, such as loss of connectivity, slow networks, malware infections, and more

* Build customized capture and display filters

* Tap into live network communication

* Graph traffic patterns to visualize the data flowing across your network

* Use advanced Wireshark features to understand confusing packets

* Build statistics and reports to help you better explain technical network information to non-technical users

Because net-centric computing requires a deep understanding of network communication at the packet level, Practical Packet Analysis is a must have for any network technician, administrator, or engineer troubleshooting network problems of any kind.

Technical review by Gerald Combs, creator of Wireshark.

作者介绍:

About the Author

Chris Sanders is the network administrator for the Graves County Schools in Kentucky, where he manages more than 1,800 workstations, 20 servers, and a user base of nearly 5,000. His website, ChrisSanders.org, offers tutorials, guides, and technical commentary, including the very popular Packet School 101. He is also a staff writer for WindowsNetworking.com and WindowsDevCenter.com. He uses Wireshark for packet analysis almost daily.

目录:

Practical Packet Analysis_下载链接1_

标签

网络

networking

计算机网络

计算机

wireshark

sa

network

评论

初级内容，新手看看比较有帮助。

没想象中的好。前五章像是说明文档，后几章是结合实际案例讲的，感觉一般。

内容较浅，适合入门

Practical Packet Analysis_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...

Practical Packet Analysis_下载链接1_