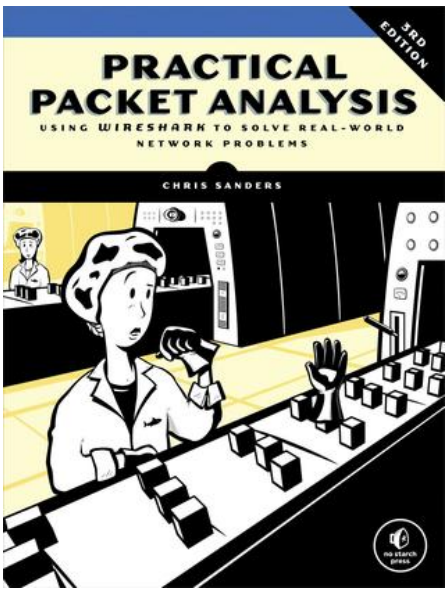

Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems

Chris Sanders

Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems

Chris Sanders

Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems Chris Sanders
It's easy to capture packets with Wireshark, the world's most popular network sniffer, whether off the wire or from the air. But how do you use those packets to understand what's happening on your network?

Updated to cover Wireshark 2.x, the third edition of *Practical Packet Analysis* will teach you to make sense of your packet captures so that you can better troubleshoot network problems. You'll find added coverage of IPv6 and SMTP, a new chapter on the powerful command line packet analyzers tcpdump and TShark, and an appendix on how to read and reference packet values using a packet map.

Practical Packet Analysis will show you how to:

Monitor your network in real time and tap live network communications

Build customized capture and display filters

Use packet analysis to troubleshoot and resolve common network problems, like loss of connectivity, DNS issues, and slow speeds

Explore modern exploits and malware at the packet level

Extract files sent across a network from packet captures

Graph traffic patterns to visualize the data flowing across your network

Use advanced Wireshark features to understand confusing captures

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

No matter what your level of experience is, *Practical Packet Analysis* will show you how to use Wireshark to make sense of any network and get things done.

Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems Details

Date	:	Published March 30th 2017 by No Starch Press (first published May 23rd 2007)
ISBN	:	9781593278021
Author	:	Chris Sanders
Format	:	Paperback 368 pages
Genre	:	Reference, Nonfiction, Computer Science, Computers, Science, Technology

From Reader Review Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems for online ebook

Tom Hinkle says

I liked the sections dealing with every day problems and how to use Wireshark to trace them to determine where the problem exits.

Peadar O'maoileoin says

This was one of the best "tech" books I've ever read. It really flows well, and the explanation is clear and concise. I'm blown away.

Lm says

great I love this book

Brandon Fulk says

Was able to get me up and running with some of the most useful Wireshark features while also giving some background into networking.

Dale Pearl says

This isn't a bad tech read. Chris keeps it simple and to the point. A book like this is more of less what I would call a temporary reference book. His examples are great,however, once you refer to them two or three times you will either have outgrown their usefullness or wireshark will have become outdated. Either way, I highly recommend this book for anyone who does networking for a living.

Shravan says

Great book for anyone who is interested in how the Internet and its different protocols work.
Highly recommend that you download the packet capture files from their website and try everything yourself as you read this book.
I'm sure I will keep coming back to this book over and over again.

Michael says

I really wanted to like this book.

The first few chapters give a quick summary of networking and TCP/IP basics. It's a subject which is difficult to cover so quickly. I'm not sure Sanders does it justice, to be honest--if you aren't already familiar with the concepts, I don't think this would be an adequate introduction.

The next few chapters discuss the mechanics of using the Wireshark program itself. I appreciate this section, as it taught me a few simple but very useful features of Wireshark that I had overlooked.

The bulk of the book presents a few packet capture use cases, and guides you through the analysis. You can download the .pcap files and follow along, and I encourage you to do that. Some of the examples can be puzzled out from the packet captures alone, and these are pretty fun. Unfortunately, a lot of the examples are only given a superficial treatment. I already knew that bittorrent traffic can consume a lot of bandwidth and will go all over the place, and the idea to look for the word bittorrent in the traffic itself is not all that insightful.

But the real letdown is the errors: the first printing has a ton of them. Things like the wrong diagram, or a packet trace that has obviously incorrect MAC addresses. On Amazon, the author says that many of these errors were corrected in later printings, but that doesn't help me. As of today, a year after he made that comment, there's still no errata for the first edition on the No Starch Press website.

Richard Lawrence says

Excellent resource for network analysts.

Soh Kam Yung says

Wireshark is one of the more useful tools available for people doing network packet analysis. But a tool is good if you know how to use it and this books show you how to use it in an easy to follow practical guide.

After going through an introduction to network packet analysis and using Wireshark, the book gets down to the nitty-gritty: using Wireshark to troubleshoot networks. You'll learn how to determine where a network problem might be happening and how to backup your analysis with evidence gathered using Wireshark.

One part that definitely needs more work is the section on wireless network analysis. This is an especially challenging part of a network to troubleshoot due to the difficulty of getting proper hardware to capture wireless packets, much less ensuring that you are getting the data you need to do proper analysis. What is covered in this book is enough to get you started in wireless network analysis but more coverage of this topic would be helpful.

Calvin Christopher says

Easy enough read for beginners while manages to get your feet wet In advanced topics.

Takedown says

Decent book if you're interested in packet analysis with Wireshark and looking for some practical examples. I would recommend that book for a beginner rather than a experienced professional since you're probably know most things already if you played with wireshark and do some analysis.

Kerszi says

Ksi??ka ma ju? par? lat, ale w wi?kszo?ci jest aktualna. W sumie internet, a tak naprawd? jego pocz?tki si?gaj? lat 60., ale protoko?y tcp/ip za bardzo si? nie zmieni?. Tak jak w tytule g?ówny nacisk jest nastawiony na Wireshark. Je?eli mia?e? styczno?? z sieci?, nie b?dzie to dla Ciebie problem.

Mohamed Nabil says

a simple but an important book that discusses how to monitor and analyze data packets using wireshark.

Steve says

The first half of this book reads like an extended help file. What makes up for it are the interesting case studies where the author shows you how to use Wireshark to solve real network crises.

Justin Andrusk says

Nice basic introduction to packet analysis using Wireshark.
