

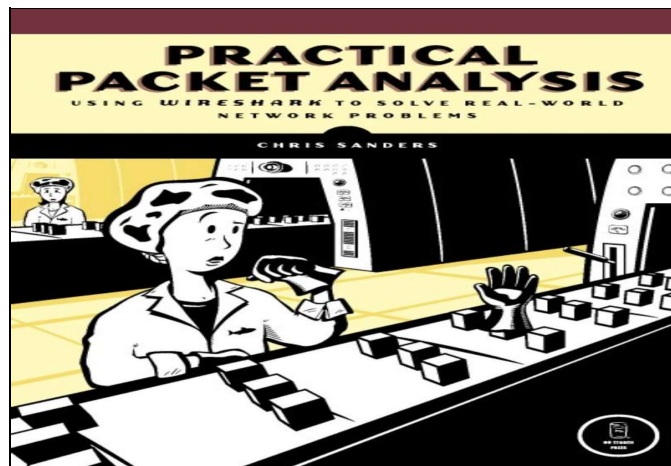


Published on Free Software Magazine (<http://www.freesoftwaremagazine.com>)

Book review: Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems by *Chris Sanders*

By Brian Turner

Knowing what information is traveling across your network is what keeps you out of trouble. Are there unknown hosts chatting away with each other? Is my machine talking to strangers? You need a packet sniffer to really find the answers to these questions. Wireshark is one of the best tools to do this job and this book is one of the best ways to learn about that tool. Chris Sanders, the author of this handy book, brings you the information cleanly and clearly. His style is to show you—to walk you through exactly what to do. This method works well and the book is quite readable.



The book's cover

I've been using Wireshark, formerly Ethereal, for many years. My first impression of this book is that there is an awful lot of networking background material provided. But as I started to dig more deeply, I found out that this background material taught me a few things too. There are many ways to approach a problem and the author showed me some fresh ways. I also remembered that many folks will be using this tool for the very first time and it started to look a little more balanced. The author brings the reader along at a good pace and I found myself learning new tips quickly. He explains different physical network layouts and how to best use Wireshark in each one. This information alone will be valuable to the new user, but there is much more contained in these pages.

“Practical Packet Analysis shows how to use Wireshark to capture and then analyze packets...”

The contents

The book is not thick or heavy, nor does it need to be. With only 216 pages total measuring out at 7 x 9.25 inches, (18 x 23.5cm), it's easy to slip the book in a desk drawer and keep close by. No Starch Press used RepKover for this book as well. RepKover allows you to lay the book flat and have it stay that way. This

feature keeps you from having to wedge the book under the lip of a keyboard to keep your pages turned. When you've had to use a few books to troubleshoot something under pressure or in a crisis situation, you really start to appreciate this little feature. The book takes you through network basics, tapping into the wires, capturing packets, and points out some common protocols. You'll want to keep this book open too; the practical examples are excellent. Following the examples will not only teach you about the tool but may also solve some immediate problems on your network. The reader is shown some typical network slowdown issues and how to perform a security analysis. A good section on wireless is also included.

Who's this book for?

This book is aimed at those who need to know how to perform packet analysis right now. Whether you are simply looking to understand how your machine "talks" with a website, debug the behavior of a new network device, troubleshoot your new network application or perhaps perform a security check, this book is going to have something to help you. As the title states, this is a "practical" book and it will tell you how to get the job done. Let me correct that, it will *show* you how to get the job done.

Relevance to free software

This book is all about free software. Wireshark is released under the GNU General Public License. The software will run on Windows, Mac OS X, and certainly on GNU/Linux. Installation is addressed for these three operating systems. Packages are available for most operating systems and you always have access to the source code as well. Most importantly though, this book will help you *open* up what is typically a *closed* system—the wire itself. Users who equate information with freedom will want to grab this book and see what's happening on those wires.

"Wireshark has become the world's most popular network sniffing application."

Pros

You should buy this book because you need to know what is happening on your network. Just for fun, start up Wireshark and then load your favorite website. I dare say you'll be surprised at just how much network traffic is generated by a typical website. Take a look at the DNS traffic and you might even be surprised at who is generating it. If you are responsible for the security or performance of your network and have not been using this tool yet, now is the time to get started. Even if you have been using this tool for years, this book has some tips to help you pull useful information from raw data even faster.

Cons

It has been said that ignorance is bliss. Knowing what sort of data is traveling about on your network may be a bit of a shock and might destroy that blissful feeling.

Title	Practical Packet Analysis
Author	Chris Sanders
Publisher	No Starch Press
ISBN	1593271492
Year	2007

Pages 216
CD included Yes/No
FS Oriented 10
Over all score 10

In short

Biography

Brian Turner (/user/14825" title="View user profile.): After 18 years supporting communication networks, satellite and microwave, I've discovered some fun on the PC again. GNU/Linux, Mac OS X and MS Windows all have their uses, but GNU/Linux is where the fun is at.

Copyright information

This article is made available under the "Attribution" Creative Commons License 2.5 available from <http://creativecommons.org/licenses/by/2.5/>.

Source URL:

http://www.freesoftwaremagazine.com/articles/book_review_practical_packet_analysis
