Practical Packet Analysis, 3E: Using Wireshark To Solve Real-World Network Problems
Synopsis

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.

Book Information

Paperback: 368 pages
Publisher: No Starch Press; 3 edition (March 30, 2017)
Language: English
ISBN-10: 1593278020
Product Dimensions: 7.1 x 0.9 x 9.2 inches
Shipping Weight: 1.4 pounds (View shipping rates and policies)
Average Customer Review: 4.6 out of 5 stars 76 customer reviews

Customer Reviews

"A wealth of information. Smart, yet very readable, and honestly made me excited to read about packet analysis." --TechRepublic"I’d recommend this book to junior network analysts,
software developers, and the newly minted CSE/CISSP/etc.--folks that just need to roll up their sleeves and get started troubleshooting network (and security) problems." --Gunter Ollmann, former Chief Technical Officer of IOActive "The next time I investigate a slow network, I'll turn to Practical Packet Analysis. And that's perhaps the best praise I can offer on any technical book." --Michael W. Lucas, author of Absolute FreeBSD and Network Flow Analysis "An essential book if you are responsible for network administration on any level." --Linux Pro Magazine "A wonderful, simple-to-use, and well-laid-out guide." --ArsGeek.com "If you need to get the basics of packet analysis down pat, this is a very good place to start." --StateofSecurity.com "Very informative and held up to the key word in its title, practical. It does a great job of giving readers what they need to know to do packet analysis and then jumps right in with vivid real-life examples of what to do with Wireshark." --LinuxSecurity.com "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." --Free Software Magazine "Perfect for the beginner to intermediate." --Daemon News

Chris Sanders is a computer security consultant, researcher, and educator. He is the author of Applied Network Security Monitoring and blogs regularly at ChrisSanders.org. Chris uses packet analysis daily to catch bad guys and find evil.

This book is a great intro into packet analysis. Some knowledge of networking fundamentals would be useful for the reader to really get what's going on in some of the examples, but this book gives a great intro to both wire shark and packet analysis. I went through it in about 3 days, and now only wish it was longer and went into more depth or had more examples. Just a warning though, it may plant a bug in your head making you want to learn network forensics.

WireShark is a tool that most of us in the IT world know and have used at least once. This book takes the use of this tool to new levels. There are some uses that I had to question and there are some that are amazing. The book covers many different and real world scenarios that can be used as a building block for other purposes. In the beginning of the book, I found myself somewhat bored with the material, but towards the middle and end I very much enjoyed realizing how much more I could use WireShark for troubleshooting and saving time. I highly recommend this book for those who use wireshark, and those who troubleshoot both network and server/workstation related
problems.

Positives: Amazing Paper and Print Quality. Pretty good introduction to Protocols and their Headers [DHCP, ARP, TCP, UDP, DNS, HTTP to name few]. Introduction to latency measurement [Client/Wire/Server] through capture analysis is worth mention. Clear explanation related to TCP [Fast retransmission, Duplicate acks, RTO etc..] Enjoyed reading it and thanks to Chris for this good book on packet analysis. Expecting Many more.

Outstanding.

Thanks!

Enjoyable reading.

Good book with big reality background. Chris Sanders explains more aspects in network like bottleneck, how detect if lag is client or server side and how detect bad network activity... it’s realist still trying to understand all this, it's not the book. lol

Download to continue reading...
