



**NO STARCH
PRESS**

FOR IMMEDIATE RELEASE

Contact: camille@nostarch.com
+1 415.863.9900 x303

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

April 26, 2007, San Francisco—In network parlance, "Packets" are packages of data that carry information. Capture them with a software tool like Wireshark or Ethereal and you can peer inside them, reassemble them, and use them to really understand network communication from the inside out. But what do you do with those packets once you've collected them? And how can they help you to better understand what's going on under the hood of your network?

Like many No Starch Press readers, publisher Bill Pollock wanted to know what to do with the packets he captured with Wireshark. After a bit of searching he happened upon Chris Sanders' "Packet School 101" on the net and **Practical Packet Analysis** (No Starch Press, May 2007, <http://www.nostarch.com/packet.htm>), was the result. Here is a book that shows anyone interested in troubleshooting a network or understanding network communication how to use Wireshark to capture and analyze packets. This is real-world packet analysis and network troubleshooting, the way the pros do it.

"Wireshark is a snap to install and I can point-and-click just as well as the next guy," said Pollock. "But pointing and clicking didn't help me to do anything with the packets I captured. I wanted to get information from those packets. Chris Sanders offers that answer with his **Practical Packet Analysis**."

Readers of **Practical Packet Analysis** learn how to:

- Use packet analysis to tackle common network problems, such as loss of connectivity, slow networks, and malware
- Build customized capture and display filters
- Tap into and view live network communication
- Graph traffic patterns to visualize the data flowing across a network
- Use advanced Wireshark features to understand confusing packets

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 administrator or engineer troubleshooting network problems of any kind.

Additional Resources:

Table of Contents: www.nostarch.com/packet_toc.htm

Sample Chapter: Chapter 6: Common Protocols, http://www.nostarch.com/download/ppa_ch06.pdf

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 userbase 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.

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

Chris Sanders, May 2007, 192 pp., ISBN 978-1-59327-149-7, US\$39.95

Available at fine bookstores everywhere, from www.oreilly.com/nostarch, or directly from No Starch Press (www.nostarch.com, orders@nostarch.com, 800.420.7240).

ABOUT NO STARCH PRESS: Founded in 1994, No Starch Press is one of the few remaining independent computer book publishers publishing unique books on technology, with a focus on Open Source, security, hacking, programming, and alternative operating systems. No Starch Press titles have personality, their authors are passionate, and their books tackle topics that people care about. No Starch Press titles have been included in the prestigious Communication Arts Design Annual and STEP inside 100 competition, and have won the Ippy Award from Independent Publisher magazine. See www.nostarch.com for more information and a complete catalog. (And most No Starch Press books use RepKover, a lay-flat binding that won't snap shut.)

###