Practical Packet Analysis: 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? With an expanded discussion of network protocols and 45 completely new scenarios, this extensively revised second edition of the best-selling Practical Packet Analysis will teach you how to make sense of your PCAP data. You'll find new sections on troubleshooting slow networks and packet analysis for security to help you better understand how modern exploits and malware behave at the packet level. Add to this a thorough introduction to the TCP/IP network stack and you're on your way to packet analysis proficiency. Learn how to: Use packet analysis to identify and resolve common network problems like loss of connectivity, DNS issues, sluggish speeds, and malware infectionsBuild customized capture and display filtersMonitor your network in real-time and tap live network communicationsGraph traffic patterns to visualize the data flowing across your networkUse advanced Wireshark features to understand confusing capturesBuild statistics and reports to help you better explain technical network information to non-techies Practical Packet Analysis is a must for any network technician, administrator, or engineer. Stop guessing and start troubleshooting the problems on your network.

**Book Information**

Paperback: 280 pages
Publisher: No Starch Press; 2 edition (July 9, 2011)
Language: English
ISBN-10: 1593272669
Product Dimensions: 7 x 0.8 x 9.2 inches
Shipping Weight: 1.4 pounds (View shipping rates and policies)
Average Customer Review: 4.5 out of 5 stars  See all reviews (79 customer reviews)

**Customer Reviews**

The book starts out with some requisite background knowledge about networking needed to understand the packets that will be analyzed. This will not make you a networking expert, but it is
very informative for the newcomer and a great refresher for the oldies. After learning about the basics of networking and comparing layer 1, 2, and 3 devices, the book explains techniques for successfully sniffing traffic. The author does not steer clear of the valuable (but sometimes controversial) ARP Cache Poisoning and flood attacks that frequently work for sniffing through a switch. The author also compares Wireshark (the selected sniffing tool) to some of the others, and clearly explains why he made the choice to use Wireshark. Time is spent familiarizing the reader with using Wireshark, covering installation and usage. The author also discusses how to write filters for capturing and displaying, which is essential to properly use the tool to wade through all the clutter. Finally, the packets that are typically found on a network are discussed and analyzed. The author points out many useful things that can be discovered by zeroing in on things like client/server latency (at different points throughout the TCP handshake) DNS abnormalities, and strange packets. Also Security implications and intrusion detection are discussed, which I found to be extremely informative for the typical network administrator. Finally some real world scenarios are presented, at which point we examine real life packets to determine the cause of the network problems. This exercise was very helpful to tie in the previous knowledge with a practical hands on approach. Also much appreciated were the example packets.

Download to continue reading...