

Book Review: Wireshark Network Analysis: The Official WCNA Study Guide

Book Review by Andrew Johnson, CISSP, CISA, GPEN, et al

Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide was written by Laura Chappell, a name that should be familiar to even the most casual Wireshark user. She is without a doubt the most well-known Wireshark trainer and has many years of experience producing and delivering Wireshark training. All of that knowledge and experience has culminated in this definitive resource.

The most important thing to do when considering purchasing a book like Wireshark Network Analysis is to understand what it is, what it isn't, and adjust your expectations accordingly. Given the vast breadth of material this book covers in its 700+ pages, it is impossible to be an authoritative resource on everything it touches upon. It is first and foremost a book written specifically for the Wireshark certification, and it covers the Wireshark application inside-and-out. This book also does an excellent job of introducing network analysis in general and explains key aspects of many common network protocols. However, it is not a comprehensive guide on all those topics (but isn't that what the RFCs are for anyway?).

One of the first things you will likely notice when reading this book is that it was written to be fun. If you were one of the lucky few that preordered a copy, you had the option of getting a signed copy. The inscription in mine instructs me to, "Enjoy every bit!!" The inscriptions in coworkers' copies contained various other network-based puns. There are countless humorous touches that will likely bring a smile to your face throughout the course of this book. For example, the "Acknowledgements" section is aptly entitled, "ACKs." This book contains a lot of cute humor that is reminiscent of Shon Harris' All-In-One CISSP book. I personally found it enjoyable and felt that it made an extremely technical book much more readable.

Discuss in Forums {mos_smf_discuss:Book Reviews}

My favorite aspect of this book is that it's practical. Each chapter ends with at least one case-study, and 45 are covered throughout the course of the book. You can instantly see how the material you just learned about is applicable in real-world scenarios. Most chapters also include corresponding trace files that can be analyzed in Wireshark. This book also strives to reinforce the material by including review questions at the end of each chapter. This is a certification guide after all, so there is special attention paid to knowledge retention.

One thing that was immediately evident in regards to the writing style was the classy manner in which the book was written. It genuinely exemplifies the free and open nature of Wireshark. The author doesn't discount other tools, such as tcpdump, but instead shows the pros and cons of each and describes how they can work cooperatively. This book is also remarkably error free. No technical book is perfect, but this guide definitely seems to be one of the better ones in terms of accuracy and attention to detail. A list of errata is maintained on the book's website for the few errors that have been discovered.

While this book is not written as an entry-level text, it isn't wholly inaccessible to novices either. A basic understanding of networking and TCP/IP would be a good baseline for audiences interested in this book. Even though a basic level of knowledge is expected, Laura still does an excellent job of explaining the nitty-gritty details. Anyone who performs any sort of network analysis is obviously the ideal candidate. Server administrators should also consider this text, because an understanding of what's happening at the network level can be used to identify problems and improve performance. Whether you do network analysis professionally, or you just need to try to troubleshoot your grandma's slow internet connection, this book will be beneficial for you.

I don't have any major complaints with this book. The book is in grayscale, and some of the graphs and diagrams would have benefited from color. However, all the trace files are available online, and they can simply be loaded as needed. Some people might have benefited from a CD containing a portable PDF version of the book and the sample trace files. This is not a small book, and an electronic companion copy would have been a nice perk for more mobile individuals. The trace files are publicly available on the book's website. While downloading hundreds of megabytes will not likely be a problem for most people, it might be somewhat problematic for individuals who have slow or limited internet connections. These complaints are clearly logistical and do not take away from the stellar content contained within the book.

Another quasi-complaint (that is no fault of Ms. Chappell – it's just the way things had to be done), is that it takes a while to get to the meat-and-potatoes of the book. I would wager that most people get excited about this book, because they want to dive into the bits and actually perform some sort of analysis. Unfortunately, the first simple trace file isn't analyzed until nearly 200 pages in, and the in-depth protocol analysis doesn't begin until another 100 after that. However, as with anything, it's important to understand the fundamentals before moving on to more advanced concepts. The application-specific content that is covered initially provides the necessary foundation for how to get the most out of Wireshark.

The book consists of 33 chapters and an appendix that details the online resources available. Chapters 1-13 focus on the Wireshark application itself and provide the aforementioned foundation for the rest of the book. Chapters 14 – 27 dive into protocol analysis, detail common LAN and internet protocols, and conclude with an introduction to VOIP and WLAN protocols. Chapters 28 – 32 bring it all together and cover more comprehensive items such as how to baseline traffic, identify suspicious traffic, and perform forensics. The last chapter shows how to make effective use of the command-line tools that are included in the Wireshark suite of utilities.

The book retails for \$99.95. Some people may balk at that price, but, rest assured, it is absolutely worth every penny. I have recommended this book to numerous acquaintances and coworkers, and I have received nothing but positive feedback. I highly recommend this book to anyone who is interested or concerned about what’s going on down at the wire. More information about the book and certification can be found at <http://www.wiresharkbook.com/>.

Andrew Johnson is an information security analyst who regularly performs penetration testing, risk assessments, IT audits, social engineering, and security awareness training. He has over five years of extensive experience working with information technology and information security. His notable certifications include CISSP, CISA, GPEN, GSEC, CEH, CCNA:S, CWSP, MCITP:EA, and MCSE:S. He is a mentor for the SANS 401 and 560 courses and has also recently started participating in GIAC exam development. You can find sporadic musings at www.infosiege.net or @infosiege.