# book reviews

ELIZABETH ZWICKY, WITH SAM F. STOVER

## 97 THINGS EVERY SOFTWARE ARCHITECT SHOULD KNOW: COLLECTIVE WISDOM FROM THE EXPERTS

*Richard Monson-Haefel, editor*

O'Reilly, 2009. 195 pages.
ISBN 978-0-596-52269-8

This is a sweet collection of advice. As you might expect from a collection, some advice overlaps and some conflicts. That's OK. Actually, if I had to pick my top advice for software architects, there are some important apparent conflicts that appear very fast (for instance, always plan for the future, but not too far in the future, and don't expect it to actually work—all of which is better discussed in the book). If you can't handle balancing opposing and important concerns, don't try to architect anything.

This isn't going to teach you how to be a software architect. It's more a tool for software architects who want to improve their practice. The advice is mostly in the "simple but not easy" category, so it's the sort of book you want to read a little at a time, think on, come back to when you need a pick-me-up, argue with your colleagues about.

Plus, I'm glad it's 97 items. I hate it when people force their lists into round numbers. (Although I do have my suspicions that ending up with a prime number of items was not entirely accidental. It is possible that I hang out with too many people who notice this sort of thing.)

## NETWORK KNOW-HOW: AN ESSENTIAL GUIDE FOR THE ACCIDENTAL ADMIN

*John Ross*

No Starch Press, 2009. 251 pages.
ISBN 978-1-59327-191-6

Networking is complex, and yet most networks are not big enough to need a full-time network administrator. My home network is full-featured to an unusual extent (there aren't very many nodes, for a household of computer people, but a mix of expediency and curiosity leads to some baroque complexity). Even though we're running exotic feature-sets on routers purchased on eBay, most of the time the thing just works. This is even more true for most households and even most small businesses.

So what happens when new features are needed or, worse yet, it stops working? Well, my household is in good shape, but most networks aren't, so a book like this could be extremely useful.

And this book is OK. Instead of to troubleshooting, it's mostly devoted to setting things up, which I find is usually the easy part, although a bit of help understanding what's going on and how the pieces fit together is definitely useful. Some of its advice is purely mystifying: no, really, I asked around, and people don't usually spell out IP addresses number-by-number ("one nine two dot three five . . . " instead of "one ninety-two dot thirty-five . . . "). The author may say "why-fie" for Wi-Fi but I guess he says "why" differently than I do. No home network I know of changes WPA encryption keys once or twice a month. (Frankly, most people change them when they move. Yes, it would be safer to change them all the time, but then all my friends would be typing in new passwords every time they come over.) "Modem" is not a geeky term for "modulator-demodulator," but, rather, the other way around. Not that there's a non-geeky term. And honestly, I know that these things are very confusing and some skipping details is necessary and experts disagree on fine nuances, but a bridge is not a device that sits between two different networks, and it is not fair to say that NAT is a primary characteristic of a router.

All of this made me very cranky. Possibly unreasonably cranky; it's like listening to somebody singing slightly off-tune. The fact is, there's a lot of useful information here. The presentation is relatively accessible, suitable for people who are a bit technical but not network-literate, and there's practical advice for small networks with little or no support staff, which is hard to find elsewhere. The information on troubleshooting, while sparse, is

practical and accurate. It's not the book I was hoping for, but it's a lot better than nothing.

## PHOTOSHOP CS4 PHOTOGRAPHER'S HANDBOOK

*Stephen Laskevitch*

Rocky Nook, 2009. 258 pages.
ISBN 978-1-933952-42-0

If you're new to Photoshop and are interested in doing normal photograph things with it, this is a good starting point. It describes a good working process, firmly based in current Photoshop best practices (every pixel is sacred! never destroy data!). It does a quick but reasonable job of introducing you to the basics of pixel-based photographs, assuming very little about your knowledge of digital photography. It's not an advanced Photoshop technique manual, but it does cover the techniques you're likely to need to get the best out of your photos, plus the most popular fun tricks.

Oddly, the thing I liked least about this book was the layout. I found that navigation was sometimes tricky. The book actually covers three or four applications, depending on how you count—Photoshop, Bridge (which ships with Photoshop), Lightroom (which can be bundled with Photoshop but is a separate, extra-cost application), and Adobe Camera Raw (which is a plugin, but with all the features of a separate application). These applications overlap a lot, so almost every task can be undertaken in at least two of them. This means a lot of back and forth. There are handy little color blocks to tell you what application is being discussed, but it still changes every few paragraphs in some places. Couple this with the need to put in lots of screen shots and illustrations, and I found it hard to follow from time to time.

## THE MANGA GUIDE TO DATABASES

*Mana Takahashi, Shoko Asuma, and Trend-Pro Co., Ltd.*

No Starch Press, 2009. 208 pages.
ISBN 978-1-59327-190-9

This is a perfectly reasonable introduction to databases, including normal forms, and basic SQL queries. It's not particularly deep; you wouldn't want it to be your DBA's main text or anything, but a person who pays attention and does the exercises will be able to, for instance, understand what's so horrible about most of the SQL examples you see on www.thedailywtf.com, or what a DBA is talking about. It's enough to do some basic database work, if you're a reasonably technically oriented person to begin with.

I would recommend judging this book by the cover. If you look at the big-eyed fairy and think "Bleargh," really, it's not going to get any better. There's a princess, and a love interest. If you look at it and think, "Cute. That could make SQL bearable," then you're in the right place. (At least this time the love interest is not creepy.)

It's fatally easy to skim, so the unmotivated reader can easily come away with a feeling of virtue and not much actual knowledge. In some ways, it's like one of those girly cocktails; it's pink and fluffy, but it packs a concealed punch. Unfortunately, in this case you won't take it in without noticing. I found that I was periodically going back to re-read.

## UNIX AND LINUX FORENSIC ANALYSIS DVD TOOLKIT

*Chris Pogue, Cory Altheide, and Todd Haverkos*

Syngress, 2009. 230 pages.
ISBN: 978-1-59749-26-0

REVIEWED BY SAM STOVER
(SAM.STOVER@GMAIL.COM)

This little book was a pleasant surprise: well written, upfront about the targeted audience, and full of interesting information. When I first started reading, I immediately formed the "another Windows user who is amazed by basic *nix capabilities" opinion. While there is a little of this, it's not overwhelming, and the basics covered are solid. Since the forensic process touches just about everything hardware and software, this is a great book for someone who doesn't know much *nix but wants to learn, and that was what the author intended.

Weighing in at a lean 230 pages, the book contains eight chapters and an appendix. The first chapter, "Introduction," is very short and covers what is covered, what is not covered, and who the target audience is. I think this is a pretty important chapter for *nix geeks, because, unlike some other books, this one does a great job of laying out everything so the reader isn't taken by surprise as they read the book. If you find yourself considering this book for purchase, definitely read the Intro, which does a great job of telling you whether you'll benefit from it.

"Understanding Unix," the second chapter, it covers the expected *nix basics: differences between UNIX and Linux, some basic file system stuff, and an introduction to shells. The third chapter, "Live Response: Data Collection," starts to delve into the

forensic process a bit and how this differs from Windows to *nix. Someone with experience using EnCase, FTK, and other Windows forensic tools will find some familiar material here. Chapter 4, "Initial Triage and Live Response: Data Analysis," hits on numerous *nix commands that replace or augment the typical Windows forensic toolkit. I've said it before and I'll say it again, the majority of whiz-bang features included in most Windows forensic toolkits are simply commands that *NIX geeks have been using for years, and that becomes pretty clear in this chapter. I sincerely doubt that my target audience needs a refresher on more, less, and tail, so unless you want to see how they fit in the forensic process, you might be bored by Chapter 4.

Chapter 5 lists the "Hacking Top 10" tools, which, again, should be familiar to any self-respecting geek: netcat, nmap, nessus, nikto, wireshark, etc. Good intro chapter for the Windows user, but old hat to *nix folks.

Chapters 6 and 7 deal with "The /proc File System" and "File Analysis" respectively, and they do a really great job. While I wouldn't expect you to buy this book for two chapters alone, if you need a refresher on /proc, Chapter 6 is a good place to start. Since a lot of forensic analysis is actually file analysis, understanding the file system is pretty important, and these two chapters provide what you need. Chapter 8, entitled "Malware," actually deals more with anti-virus solutions (Panda and Clam) than actual malware—my only real gripe with the book. There is a pretty interesting discussion of malware on the *NIX platform, and it's not just the ubiquitous "Linux is more secure than Windows because of X, Y, and Z" but some well-thought-out points and expectations for the future.

This book might be a little too basic for the *nix maestro who wants to learn forensics, but I'd still recommend considering it. Also, while I don't think this was the intent of the author, I think this is a great introduction for any budding *nix enthusiast, because it deals with a lot of core and basic concepts inherent to *nix that anyone, not just a Windows forensic analyst, can learn from. A solid intro book.