

The IDA Pro Book

Review by Ryan Linn, CISSP, MCSE, GPEN

After attending DEFCON in August and seeing the overwhelming interest in this book, I was eager to dive into The IDA Pro Book by Chris Eagle. Chris Eagle's team, School of Root, won the "Capture the Flag" event at DEFCON this year and Chris gave a presentation on CollabREate, a tool that integrates with IDA Pro to allow collaboration in reverse engineering (RE). All of that together - with the fact that the book sold out - screamed that this book should quickly make it to the top of my list.

Once I had the book in-hand, the cover alone offered some insight into what was to come. The quote on the front of the book is an endorsement from the creator of IDA Pro. The image on the front is a throwback to the Operation game by Milton Bradley, which reminds me of how I felt when I got started doing reverse engineering. I am not a professional Reverse Engineer or Malware Analyst, however, my coding background and my current position as a security professional at SAS affords the opportunity to dabble. This puts me in the perfect middle ground of being able to understand the material as well as assess its ability to teach.

Free Sample Chapter Available Below

"Chapter 12: Library Recognition Using FLIRT Signatures"

del.icio.us

Discuss in Forums {mos_smf_discuss:Book Reviews}

[Click Here to download "Chapter 12: Library Recognition Using FLIRT Signatures"](#)

The IDA Pro Book is broken up into a number of different "Parts" each having several chapters and its own goal. Even if the content appears to be beyond your level of knowledge in a certain area, I highly recommend that you keep reading. It may also be handy to point out the fact that the book is 640 pages. So this lends itself to being more of a reference guide than a book read straight through from cover to cover.

I should also mention at this point that the book is about the 5.X tree of IDA Pro, and not the freeware version. There is a demo that you can download off of the IDA Pro Website if you aren't able to purchase the full version right away. In addition, there is a reference at the back discussing how the freeware version differs from the commercial version, so as long as you are ok with those restrictions while you are learning, this book still should be very handy.

One of the most important sections of Chris's book is found in "Introduction to IDA." The author discusses disassembly and the challenges that go with it, the tools involved with reverse engineering and disassembly, and a general breakdown of how these tools approach the binaries that they are analyzing. He also references other tools that are handy alongside IDA Pro, and outlines how they fit into the reverse engineering process. Finally information about IDA Pro licensing and installation is discussed, and the base information that you will need for the rest of your IDA Pro adventure is laid out.

Once the basics of RE have been covered, the author addresses the fundamentals of using IDA Pro. Unlike some other books, this book does a great job of letting you know where you should be looking when it lays out a block of assembly code. The references are well laid out as well. "Part II: Basic IDA Usage" progresses logically and eases you into the interface. It does a great job helping you figure out what all the new windows are doing, and how to get to the information that IDA Pro is providing. The content moves from basic skills such as finding the disassembly into manipulating the disassembly to be more meaningful then to optimizing the disassembly process. It shows you how to navigate the code, and how to incorporate other knowledge that you have about the binary you are disassembling, such as what headers or what libraries might have been used in order to obtain the most useful disassembly possible and facilitate the disassembly of the binary.

"Part III: Advanced IDA Usage" gets deeper into using IDA Pro, including utilizing the Fast Library Identification and Recognition Technology (FLIRT) signatures and custom files in order to suck the most information possible out of a binary before analysis. You also get a glimpse into how to modify the pieces of the application which can be modified only through config files. It concludes by explaining the patch capabilities of IDA Pro and discussing what the limitations and expectations should be. This Part provides insight into creating your own signatures for custom libraries that might not be available in IDA Pro, so, as you start working on real life applications, you can tailor IDA Pro to be able to recognize libraries that you frequently encounter.

After the basics of using the application have been covered, the author explains how to extend the capabilities of IDA Pro in Parts III and IV. He discusses in depth the scripting engine and how to build plug-ins and modules. Throughout this Part numerous examples are given of how the scripting and plug-ins fit into the application. Short detailed examples are used to illustrate how to accomplish some tasks that would be useful for a reverse engineer including listing out function information. The beginning of the chapter was great. As a beginning Reverse Engineer, I was able to clearly see how this information would apply. For the stuff that was beyond my current knowledge level, it was easy to see that as my knowledge progresses in the future, I would be back to re-visit this information.

Throughout the entire fifth Part are goodies focusing on the real-world applications of IDA Pro. It goes into the different types of binaries that you might encounter while doing reverse engineering. This chapter also goes into two large areas where IDA Pro is used such as obfuscated code analysis and vulnerability analysis. After reading this Part, you should have some handy scripts and a series of applications and plug-ins to aid in your RE adventures. The author discusses a number of those plug-ins in-depth including adding in bindings for Python and Ruby. At the end of this chapter, I hadn't learned an incredible amount more about IDA Pro, however I definitely knew more about how to approach the problems I might encounter and how to extend IDA Pro's capabilities in order to tackle real world tasks.

The final Part of the book is on the IDA Debugger. The debugging features of IDA Pro were an afterthought and aren't the primary focus of IDA Pro. Chris Eagle goes into what to expect from the debugger, how it's used, and then finally how to integrate the information obtained from the debugger into the overall RE process. He concludes with a discussion of how to automate debugging tasks with scripts and plug-ins and discusses some of the real-world problems that people might encounter, such as dealing with UPX packing that has been modified. This chapter also goes into remote debugging, where you can be running a binary on one machine and having it come back to a GUI on another. Knowing this information is especially useful if you are doing analysis across multiple platforms. The Windows GUI is the only non-console GUI in the IDA Pro supported platforms.

Chris Eagle's The IDA Pro Book provides a significantly better understanding not of just IDA Pro itself, but of the entire RE process. There are little gems littered throughout the book that bring in real-life experience and knowledge that you don't always get from other books instructing you in the use of an application. Although it is impossible to absorb everything in this book due to its size, it helped greatly in overcoming some of the initial hurdles of understanding a highly technical topic. As I continue down my reverse engineering path, I'm confident that I will use this book repeatedly as a reference.

If you are interested in getting deep into the assembly and figuring out what applications are doing when you don't have the source, then I would highly recommend this book to get you started with IDA Pro, it won't turn you into a reverse engineering expert, but it certainly will provide you with a major tool that will help you along the way.

Ryan Linn, CISSP, MCSE, GPEN - Ryan is currently an Information Security Engineer at SAS Institute. Employed in the computer industry since 1997, he has held positions ranging from web developer to Unix Systems Programmer at a large university to his current position in Information Security. Ryan has been responsible for working with large scale deployments of various flavors of *nix, high availability web and database clusters, as well as for application programming in high availability environments. In the past few years, Ryan has incorporated Windows security into his responsibilities, and is now part of the team responsible for information security globally in one of the largest privately held software companies in the world.