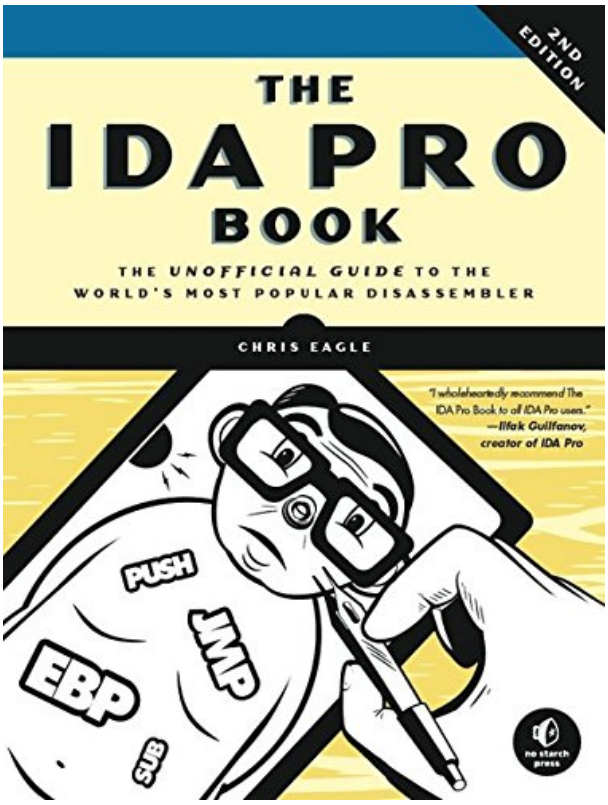
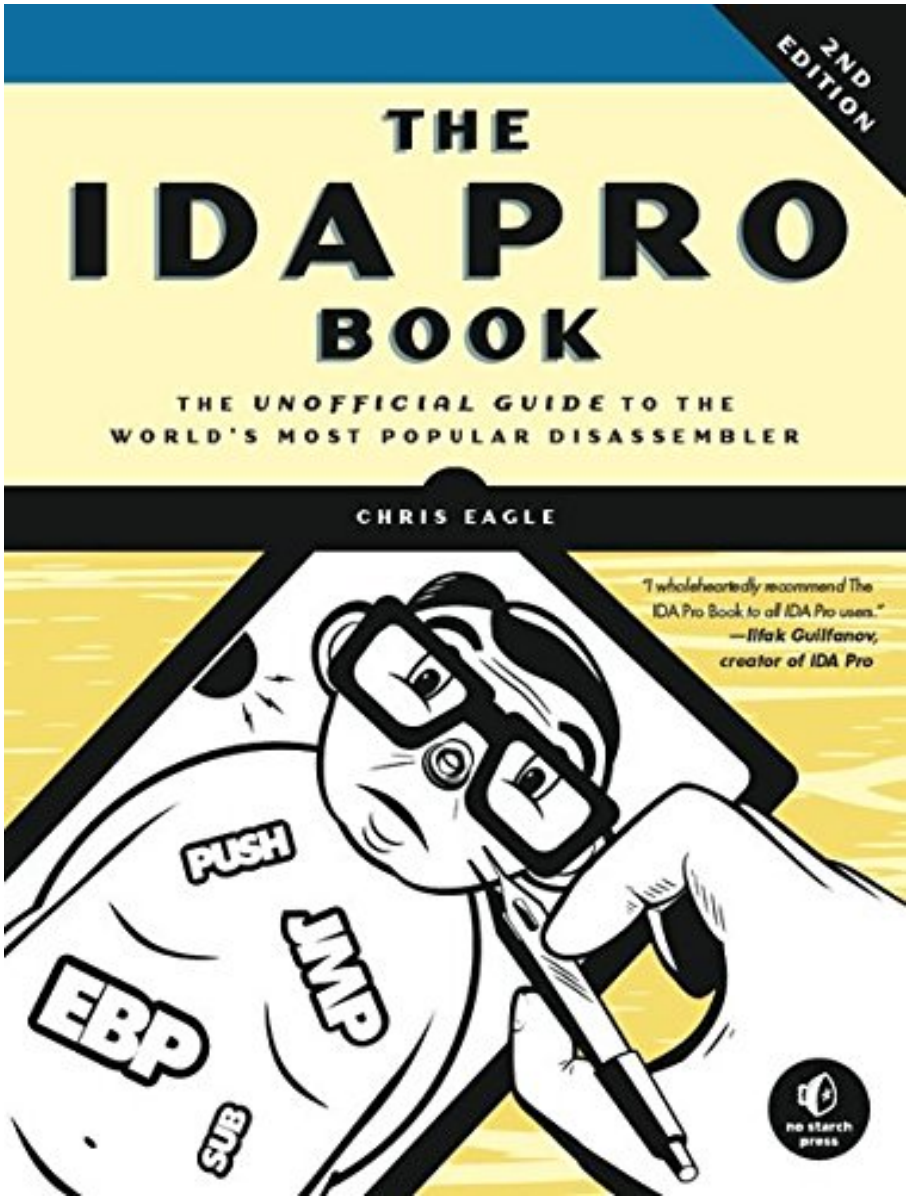
THE IDA PRO BOOK: THE UNOFFICIAL GUIDE TO THE WORLD'S MOST POPULAR DISASSEMBLER BY CHRIS EAGLE





THE IDA PRO BOOK: THE UNOFFICIAL GUIDE TO THE WORLD'S MOST POPULAR DISASSEMBLER BY CHRIS EAGLE PDF

Some people may be chuckling when taking a look at you reading **The IDA Pro Book: The Unofficial Guide To The World's Most Popular Disassembler By Chris Eagle** in your leisure. Some could be admired of you. As well as some may really want resemble you that have reading hobby. Just what regarding your personal feel? Have you really felt right? Reading The IDA Pro Book: The Unofficial Guide To The World's Most Popular Disassembler By Chris Eagle is a need and also a leisure activity at the same time. This problem is the on that particular will make you feel that you have to read. If you know are seeking the book entitled The IDA Pro Book: The Unofficial Guide To The World's Most Popular Disassembler By Chris Eagle as the choice of reading, you can discover here.

About the Author

Chris Eagle is a Senior Lecturer of Computer Science at the Naval Postgraduate School in Monterey, CA. He is the author of many IDA plug-ins, co-author of Gray Hat Hacking, and has spoken at numerous security conferences, including Black Hat, Defcon, ToorCon, and ShmooCon.

THE IDA PRO BOOK: THE UNOFFICIAL GUIDE TO THE WORLD'S MOST POPULAR DISASSEMBLER BY CHRIS EAGLE PDF

Locate the key to boost the quality of life by reading this **The IDA Pro Book: The Unofficial Guide To The World's Most Popular Disassembler By Chris Eagle** This is a type of book that you require currently. Besides, it can be your favorite publication to review after having this publication The IDA Pro Book: The Unofficial Guide To The World's Most Popular Disassembler By Chris Eagle Do you ask why? Well, The IDA Pro Book: The Unofficial Guide To The World's Most Popular Disassembler By Chris Eagle is a publication that has different characteristic with others. You may not need to understand which the writer is, exactly how widely known the work is. As sensible word, never judge the words from that talks, yet make the words as your inexpensive to your life.

Getting the books *The IDA Pro Book: The Unofficial Guide To The World's Most Popular Disassembler By Chris Eagle* now is not kind of challenging way. You can not simply going for publication shop or collection or loaning from your close friends to read them. This is an extremely easy way to exactly obtain guide by on the internet. This online book The IDA Pro Book: The Unofficial Guide To The World's Most Popular Disassembler By Chris Eagle could be among the choices to accompany you when having extra time. It will certainly not waste your time. Think me, the book will show you brand-new point to review. Just invest little time to open this on the internet e-book The IDA Pro Book: The Unofficial Guide To The World's Most Popular Disassembler By Chris Eagle as well as review them wherever you are now.

Sooner you obtain the book The IDA Pro Book: The Unofficial Guide To The World's Most Popular Disassembler By Chris Eagle, sooner you could enjoy reading the publication. It will be your rely on keep downloading and install the publication The IDA Pro Book: The Unofficial Guide To The World's Most Popular Disassembler By Chris Eagle in provided web link. This way, you could actually make a selection that is offered to obtain your very own e-book on the internet. Here, be the very first to obtain the publication qualified The IDA Pro Book: The Unofficial Guide To The World's Most Popular Disassembler By Chris Eagle and be the initial to understand just how the writer indicates the message and knowledge for you.

THE IDA PRO BOOK: THE UNOFFICIAL GUIDE TO THE WORLD'S MOST POPULAR DISASSEMBLER BY CHRIS EAGLE PDF

No source code? No problem. With IDA Pro, the interactive disassembler, you live in a source code-optional world. IDA can automatically analyze the millions of opcodes that make up an executable and present you with a disassembly. But at that point, your work is just beginning. With The IDA Pro Book, you'll learn how to turn that mountain of mnemonics into something you can actually use.

Hailed by the creator of IDA Pro as "profound, comprehensive, and accurate," the second edition of The IDA Pro Book covers everything from the very first steps to advanced automation techniques. You'll find complete coverage of IDA's new Qt-based user interface, as well as increased coverage of the IDA debugger, the Bochs debugger, and IDA scripting (especially using IDAPython). But because humans are still smarter than computers, you'll even learn how to use IDA's latest interactive and scriptable interfaces to your advantage.

Save time and effort as you learn to:

- Navigate, comment, and modify disassembly
- Identify known library routines, so you can focus your analysis on other areas of the code
- Use code graphing to quickly make sense of cross references and function calls
- Extend IDA to support new processors and filetypes using the SDK
- Explore popular plug-ins that make writing IDA scripts easier, allow collaborative reverse engineering, and much more
- Use IDA's built-in debugger to tackle hostile and obfuscated code

Whether you're analyzing malware, conducting vulnerability research, or reverse engineering software, a mastery of IDA is crucial to your success. Take your skills to the next level with this 2nd edition of The IDA Pro Book.

- Sales Rank: #55975 in Books
- Brand: Brand: No Starch Press
- Published on: 2011-07-14
- Original language: English
- Number of items: 1
- Dimensions: 9.00" h x 1.56" w x 7.00" l, 2.68 pounds
- Binding: Paperback
- 672 pages

Features

- Used Book in Good Condition

About the Author

Chris Eagle is a Senior Lecturer of Computer Science at the Naval Postgraduate School in Monterey, CA. He is the author of many IDA plug-ins, co-author of Gray Hat Hacking, and has spoken at numerous security conferences, including Black Hat, Defcon, ToorCon, and ShmooCon.

Most helpful customer reviews

29 of 29 people found the following review helpful.
The IDA Pro Book Review
By E. Hulse
Second Edition Review:
If you are considering any other book about IDA Pro Don't bother, as The IDA Pro Book Second Edition is the only book on IDA Pro that you will need.

The overall structure of the Second Edition is unchanged, which is not a bad thing. The structure Chris Eagle uses allows for inexperienced users to get spun up on the basics of IDA Pro while allowing experienced users to jump into more advanced topics.

The author has an excellent method of elaborating concepts. A Novice user can easily follow the examples and build knowledge as they dive deeper into the book. Experienced users should not be put off by this, the first half of the book may be aimed at the Novice, but the second half is packed with much deeper information on more advanced topics.

If you've read the first edition and take a look at the table of contents for the second edition you may be deceived into thinking very little has changed. In fact, you'd be wrong as the second edition offers much more coverage of IDA Python. The second edition also brings users up to speed on the latest editions to IDA Pro to include Scriptable Plugins, Loader Modules and Scriptable Processor Modules. The Second Edition has an increased number of examples using IDA Python, whereas the examples from the first editions were largely only in C using IDC /SDK.

The Likes & Dislikes of the book remain the same as my review for the first edition. Although, after considering my only dislike I must admit that my suggestion is somewhat beyond the scope of the book.

Bottom line on the Second Edition: If you are new to IDA Pro you NEED this book. If you are experienced with IDA Pro I still suggest picking it up!

First Edition Review:
I was able to pick up a pre-released copy of The IDA Pro book at Defcon in the vendor area, thanks to Adam from No Starch. This book is not an introduction to reverse engineering, its a hard core manual for IDA Pro. IDA Pro is a critical weapon in any reverser's arsenal, so proficiency in this tool is paramount to your success in reverse engineering. If you are new to IDA Pro you need this book, even if you've been working with IDA for a while you will more than likely learn quite a few things after reading it. Unlike the two other books I've read on IDA Pro this book has no fluff or filler, its solid information! The funny thing when comparing it to the other two IDA books is its thicker than both combined, and contains an exponentially larger amount of information.

The author takes time to explain things in a very clear manner as you walk through from an introduction to the tool to more advanced usage such as customizing, extending IDA, debugging, and dealing with

obfuscated code. The author answered questions I had been spent weeks asking and searching the Internet for.

Likes:

Just about everything. The author walks you through plenty of code and discusses scenarios where you could apply the information he is giving you. The fact that he took his time to elaborate on why, and when you might use a piece of information is unlike many authors whom will give you information and leave the reader wondering "What would I use that for".

This book does not just talk about Win32 and Portable Executable format, ELF binaries have a continual guest appearance throughout the book, and firmware/binaries are mentioned in numerous chapters.

Side bar elaboration is kept to a minimum, I often find in texts that an author will go on about background information that does not add anything significant to what I am reading. Chris Eagle keeps this to a minimum adding small side bars when necessary but only take up a small amount of real estate.

Dislikes

My only dislike of this book was the use of PE format as the example in chapter 18 - Binary Files and Ida Loader modules. Despite the use of a well known format chosen for this example the concepts were clearly displayed. I think it would have made it more interesting if the author had used a lesser known format, or do as the author of "Reversing, Secrets of Reverse Engineers" did and create his own binary.

10 of 10 people found the following review helpful.
A good book for advanced users and an excellent book for beginners.
By Albert Sweigart
IDA Pro is a tool that I always tentatively held at arms length. The magnitude of its complexity and lack of accessible documentation (in the form of vague web tutorials, advanced technical docs that were over my head, and half-remembered bits of advice) kept me from fully embracing this useful tool. Chris Eagle's book is the book I wish I had years ago.

The IDA Pro Book is the first book you should read if you are interested in IDA Pro, or disassembly and reverse engineering in general. It is also a book that intermediate and expert IDA Pro users can learn something new from as well.

The book focuses on IDA Pro, while delving into other related topics (assembly, binary formats, variations between compilers, etc.) to give the reader a general understanding but not so much as to be distracting. There is little fluff material, but plenty of concise, practical examples and scenarios.

As much as I enjoyed The Shellcoder's Handbook and Reversing: Secrets of Reverse Engineering, I would say reading The IDA Pro Book first would be an excellent primer.

12 of 13 people found the following review helpful.
s/Unofficial/Definitive/
By Happy Cat
IDA Pro is the world's most popular disassembler. This book is for you if you are a beginner or intermediate reverser and you do not already own the first edition of The IDA Pro Book. Much of the second edition is similar, or identical in some places, to the first edition. The IDA Pro Book 2nd Edition does a great job using IDA Pro as the enabling tool for discussing specific techniques of reverse engineering. It is more of a book

about reverse engineering rather than a user manual for IDA.

Part I

Reverse engineering may be illegal in certain situations, but the author, Chris Eagle, gives solid explanations of reasons for reversing. Some of the reasons are obvious and maybe a bit scary, such as malware analysis and vulnerability analysis. Other reasons are more related to traditional computer science such as software interoperability and compiler/assembler validation. Like the first edition of the IDA Pro book, my favorite part of the chapter is still the explanations on disassembly algorithms. The author again does an excellent job highlighting the advantages and disadvantages of linear sweep and recursive descent, as well as explaining their differences and intricacies.

Chapter two is spent enumerating tools that supplement IDA in reversing. This is pretty much the same chapter as the first edition, and legitimately so. Beginners and first-time readers will likely find the chapter's contents to be helpful in working alongside IDA. It's worth noting for the chapter that one of the tools mentioned is PEiD, an application to help identify protections and other attributes of a PE. PEiD, however, is no longer developed or maintained as of April 4th, 2011. Instead, I would have liked to see a different comparable tool mentioned, perhaps ProtectionID and/or ExEinfo. No big deal, as stated in the intro, tools change faster than the book can be published. Maybe NoStarch can add a note in the Errata.

Part II

Part II starts by easing the user into working with IDA. Chapter 5 reminds the reader that there is no undo in IDA. This is disappointing for IDA, but an important aspect to keep in mind while diligently assessing a target. It's good to be reminded the easy way as opposed to inadvertently sabotaging a project on which you've spent countless hours. This fifth chapter contains some good tidbits on the user interface. One of my favorite user interface tweaks that I learned from The IDA Pro Book is that virtual addresses can be displayed in graph mode. This helped me combine the effectiveness of visualizing a target's code flow with the benefits of having some good insight into where to look while examining the disassembly. Some of the displays have changed tiers, for example the Strings Window which was a Primary IDA Display in the first edition is now a Tertiary Display with the new UI covered by the second edition of the book.

While much of Part II carried over from the first edition, it was a nice refresher to read the C++ Reversing Primer again. Developers know that C++ has additional features not found in C, such as the 'this' pointer, objects, and virtual functions. Under the hood, a reverse engineer adept at analyzing C applications may not be familiar with the data structures or intricacies used by C++. Chapter 8, Datatypes and Data Structures, does a great job taking the reverse engineer through reversing the aforementioned aspects of C++, as well as name mangling (or name decoration), runtime type identification (RTTI), and inheritance relations, an essential aspect of OOP.

Part II also discusses some of the new graphing functionality in the IDA 6.1 release. As of IDA 6.1, all versions of IDA can now use qwingraph, a cross-platform Qt port of wingraph32. This helps bring a unified look to graphing across all versions of IDA. The new external graphing functionality can still generate the five types of graphs: function flowchart, call graph for the entire binary, cross-references to a symbol, cross-references from a symbol, and a customized cross-reference graph; they just all look a little bit smoother, in my opinion, with qwingraph.

Part III

Part III begins by showing the user different ways to customize IDA. Aspects such as the configuration files, color schemes, and the toolbars are covered in Chapter 11, with much of the information carrying over from the first edition. My favorite portion of Part III, however, is the chapter on library recognition.

When developing software, code can be stored in libraries external to the main program. Sometimes the code in those libraries can also be linked in place into the main program. When this happens, it can add extra work or wasted time if the reverser is analyzing unnecessary functions. For example, most people don't really need to know the nitty gritty details of how MessageBoxA does its thing, but they might end up finding out unwittingly if the function were statically linked. To address this issue, IDA utilizes a signature-based approach with two features: FLAIR and FLIRT. FLAIR is the Fast Library Acquisition for Identification and Recognition, a toolset distributed by Hex-Rays, which can quickly create signatures for libraries and their functions. IDA can then scan the target binary with FLIRT, Fast Library Identification and Recognition Technology, using signatures generated by FLAIR. This way, functions that have already been identified can be recognized and labeled saving the reverser the time and effort of manually analyzing the function.

Chris Eagle does a great job explaining FLAIR and FLIRT, as well as walking the reader through how to use the two features in conjunction. Additionally noted are some cases where identifying the library can be rather difficult; for example, a binary that's been stripped during linking will lack symbols/function names. Chris discusses some different approaches that can be used to figure out the libraries statically linked into the target binary such that FLAIR and FLIRT can then be effectively utilized.

Part IV

Part IV looks into the internals of IDA where intermediate and advanced users will find core functionality to automate tasks and assist with analysis. Chapter 15 examines IDC, the original language used in scripting for IDA. New to this edition are IDC Objects, which, like objects in C++ and Java, allow for more complex data types. IDC Objects support single inheritance, but do not use access specifiers; in essence, all class members are effectively public. The IDC section of this chapter is valuable for both its reference content on IDC, as well as the listing of examples that are provided. The IDA Pro Book 2nd Edition does not come up short on examples.

One of the new parts in The IDA Pro Book 2nd Edition that was fun to read was "Writing a Scripted Loader" in Chapter 18. IDA 5.6 introduced the ability to implement loaders with IDC or Python, in addition to the previous offering of using the SDK. This is great for using IDA to analyze files whose format is not already supported and may be more flexible than what the SDK allows. A perfect example of this is the Portable Document Format, or PDF. PDF is an extremely flexible format that can tolerate all sorts of manipulations to its layout and still work properly in certain reader programs. This presented a challenge to loader authors who could only use the SDK. However, Python provides an adequate feature-set to parse and handle the creation of a PDF loader in IDA. It's also worth noting that processor modules can now be scripted, as well. The scriptable processor modules are covered in Chapter 19.

Part V

Chapter 21, "Obfuscated Code Analysis" contains a nice addition on analyzing virtualized code obfuscation. With virtualized code, think more along the lines of an intermediate language byte code, like a JVM with a .class file. This section covers using functionality, added to IDA after the book's first edition, which makes the reverser's work a bit less stressful. This short new section talks about customizing processor modules, as well as specifying custom formats with scripts and/or plug-ins, to automate the parsing of embedded code. The end result is that both native code and disassembled intermediate code can be displayed coherently.

Chapter 22, "Vulnerability Analysis" examines aspects of determining vulnerable function usage, potential vulnerabilities, and developing exploits, all with the help of IDA. One of the new sections focuses on using PatchDiff2, an open source project that can enumerate differences between two versions of a binary (two databases). Knowing what code was patched in response to a security advisory can significantly help with identifying a vulnerability and developing an exploit in a timely manner.

Part VI

The IDA Pro Book 2nd Edition includes a new chapter on additional debugger features. This chapter starts with remote debugging in IDA, which is a powerful feature if you are debugging code at kernel mode, or if you are debugging a remote target that requires a specific environment in which to function. The chapter then moves into debugging with Bochs, an open source x86 emulation environment. Lastly, the chapter examines Appcall, a feature of the debugger to allow IDC or IDAPython to call any function of the active process from a script. This is an interesting component as Appcall could be used in a variety of manners such as fuzzing functions, DLL injection, and manipulating the target's virtual memory space, just to name a few. In the past, I've mainly used gdb, kd, and WinDbg for remote debugging; but after reading this chapter, I'll need to give remote debugging with IDA another consideration.

Conclusion

Chris Eagle does an excellent job discussing many facets of reverse engineering using IDA Pro. If you are interested in reversing, or are already a beginner or intermediate reverser and do not own the first edition of this book, The IDA Pro Book 2nd Edition is absolutely a must-own.

See all 29 customer reviews...

THE IDA PRO BOOK: THE UNOFFICIAL GUIDE TO THE WORLD'S MOST POPULAR DISASSEMBLER BY CHRIS EAGLE PDF

It will have no uncertainty when you are visiting select this book. This impressive **The IDA Pro Book: The Unofficial Guide To The World's Most Popular Disassembler By Chris Eagle** publication can be read entirely in particular time relying on how often you open up and also review them. One to bear in mind is that every publication has their own production to obtain by each reader. So, be the excellent visitor as well as be a much better person after reviewing this book The IDA Pro Book: The Unofficial Guide To The World's Most Popular Disassembler By Chris Eagle

About the Author

Chris Eagle is a Senior Lecturer of Computer Science at the Naval Postgraduate School in Monterey, CA. He is the author of many IDA plug-ins, co-author of Gray Hat Hacking, and has spoken at numerous security conferences, including Black Hat, Defcon, ToorCon, and ShmooCon.

Some people may be chuckling when taking a look at you reading **The IDA Pro Book: The Unofficial Guide To The World's Most Popular Disassembler By Chris Eagle** in your leisure. Some could be admired of you. As well as some may really want resemble you that have reading hobby. Just what regarding your personal feel? Have you really felt right? Reading The IDA Pro Book: The Unofficial Guide To The World's Most Popular Disassembler By Chris Eagle is a need and also a leisure activity at the same time. This problem is the on that particular will make you feel that you have to read. If you know are seeking the book entitled The IDA Pro Book: The Unofficial Guide To The World's Most Popular Disassembler By Chris Eagle as the choice of reading, you can discover here.