

2ND
EDITION

THE IDA PRO BOOK

THE UNOFFICIAL GUIDE TO THE
WORLD'S MOST POPULAR DISASSEMBLER

CHRIS EAGLE

*I wholeheartedly recommend The
IDA Pro Book to all IDA Pro users.
—Ilfak Gullfanov,
creator of IDA Pro*



The IDA Pro Book

Table of Contents

[PRAISE FOR THE FIRST EDITION OF THE IDA PRO BOOK](#)

[Acknowledgments](#)

[Introduction](#)

[I. Introduction to IDA](#)

1. Introduction to Disassembly

Disassembly Theory

The What of Disassembly

The Why of Disassembly

Malware Analysis

Vulnerability Analysis

Software Interoperability

Compiler Validation

Debugging Displays

The How of Disassembly

A Basic Disassembly Algorithm

Linear Sweep Disassembly

Recursive Descent Disassembly

Summary

2. Reversing and Disassembly Tools

Classification Tools

file

PE Tools

PEiD

Summary Tools

nm

ldd

objdump

otool

dumpbin

c++filt

Deep Inspection Tools

strings

Disassemblers

Summary

[3. IDA Pro Background](#)

[Hex-Rays' Stance on Piracy](#)

[Obtaining IDA Pro](#)

[IDA Versions](#)

[IDA Licenses](#)

[Purchasing IDA](#)

[Upgrading IDA](#)

[IDA Support Resources](#)

[Your IDA Installation](#)

[Windows Installation](#)

[OS X and Linux Installation](#)

[IDA and SELinux](#)

[32-bit vs. 64-bit IDA](#)

[The IDA Directory Layout](#)

[Thoughts on IDA's User Interface](#)

[Summary](#)

[II. Basic IDA Usage](#)

[4. Getting Started with IDA](#)

[Launching IDA](#)

[IDA File Loading](#)

[Using the Binary File Loader](#)

[IDA Database Files](#)

[IDA Database Creation](#)

[Closing IDA Databases](#)

[Reopening a Database](#)

[Introduction to the IDA Desktop](#)

[Desktop Behavior During Initial Analysis](#)

[IDA Desktop Tips and Tricks](#)

[Reporting Bugs](#)

[Summary](#)

5. IDA Data Displays

The Principal IDA Displays

[The Disassembly Window](#)

[The Functions Window](#)

[The Output Window](#)

Secondary IDA Displays

[The Hex View Window](#)

[The Exports Window](#)

[The Imports Window](#)

[The Structures Window](#)

[The Enums Window](#)

Tertiary IDA Displays

[The Strings Window](#)

[The Names Window](#)

[The Segments Window](#)

[The Signatures Window](#)

[The Type Libraries Window](#)

[The Function Calls Window](#)

[The Problems Window](#)

Summary

6. Disassembly Navigation

Basic IDA Navigation

Double-Click Navigation

Jump to Address

Navigation History

Stack Frames

Calling Conventions

Local Variable Layout

Stack Frame Examples

IDA Stack Views

Searching the Database

Text Searches

Binary Searches

Summary

7. Disassembly Manipulation

Names and Naming

Parameters and Local Variables

Named Locations

Register Names

Commenting in IDA

Regular Comments

Repeatable Comments

Anterior and Posterior Lines

Function Comments

Basic Code Transformations

Code Display Options

Formatting Instruction Operands

Manipulating Functions

Converting Data to Code (and Vice Versa)

Basic Data Transformations

Specifying Data Sizes

Working with Strings

Specifying Arrays

Summary

8. Datatypes and Data Structures

Recognizing Data Structure Use

[Array Member Access](#)

[Structure Member Access](#)

Creating IDA Structures

[Creating a New Structure \(or Union\)](#)

[Editing Structure Members](#)

[Stack Frames as Specialized Structures](#)

Using Structure Templates

Importing New Structures

[Parsing C Structure Declarations](#)

[Parsing C Header Files](#)

Using Standard Structures

IDA TIL Files

[Loading New TIL Files](#)

[Sharing TIL Files](#)

C++ Reversing Primer

[The this Pointer](#)

[Virtual Functions and Vtables](#)

[The Object Life Cycle](#)

[Name Mangling](#)

[Runtime Type Identification](#)

[Inheritance Relationships](#)

[C++ Reverse Engineering References](#)

Summary

9. Cross-References and Graphing

Cross-References

[Code Cross-References](#)

[Data Cross-References](#)

[Cross-Reference Lists](#)

[Function Calls](#)

IDA Graphing

[IDA External \(Third-Party\) Graphing](#)

[IDA's Integrated Graph View](#)

Summary

10. The Many Faces of IDA

Console Mode IDA

Common Features of Console Mode

Windows Console Specifics

Linux Console Specifics

OS X Console Specifics

Using IDA's Batch Mode

Summary

III. Advanced IDA Usage

11. Customizing IDA

Configuration Files

The Main Configuration File: ida.cfg

The GUI Configuration File: idagui.cfg

The Console Configuration File: idatui.cfg

Additional IDA Configuration Options

IDA Colors

Customizing IDA Toolbars

Summary

12. Library Recognition Using FLIRT Signatures

[Fast Library Identification and Recognition Technology](#)

[Applying FLIRT Signatures](#)

[Creating FLIRT Signature Files](#)

[Signature-Creation Overview](#)

[Identifying and Acquiring Static Libraries](#)

[Creating Pattern Files](#)

[Creating Signature Files](#)

[Startup Signatures](#)

[Summary](#)

13. Extending IDA's Knowledge

Augmenting Function Information

IDS Files

Creating IDS Files

Augmenting Predefined Comments with loadint

Summary

14. Patching Binaries and Other IDA Limitations

The Infamous Patch Program Menu

[Changing Individual Database Bytes](#)

[Changing a Word in the Database](#)

[Using the Assemble Dialog](#)

IDA Output Files and Patch Generation

[IDA-Generated MAP Files](#)

[IDA-Generated ASM Files](#)

[IDA-Generated INC Files](#)

[IDA-Generated LST Files](#)

[IDA-Generated EXE Files](#)

[IDA-Generated DIF Files](#)

[IDA-Generated HTML Files](#)

Summary

IV. Extending IDA's Capabilities

15. IDA Scripting

Basic Script Execution

The IDC Language

[IDC Variables](#)

[IDC Expressions](#)

[IDC Statements](#)

[IDC Functions](#)

[IDC Objects](#)

[IDC Programs](#)

[Error Handling in IDC](#)

[Persistent Data Storage in IDC](#)

Associating IDC Scripts with Hotkeys

Useful IDC Functions

[Functions for Reading and Modifying Data](#)

[User Interaction Functions](#)

[String-Manipulation Functions](#)

[File Input/Output Functions](#)

[Manipulating Database Names](#)

[Functions Dealing with Functions](#)

[Code Cross-Reference Functions](#)

[Data Cross-Reference Functions](#)

[Database Manipulation Functions](#)

[Database Search Functions](#)

[Disassembly Line Components](#)

IDA Scripting Examples

[Enumerating Functions](#)

[Enumerating Instructions](#)

[Enumerating Cross-References](#)

[Enumerating Exported Functions](#)

[Finding and Labeling Function Arguments](#)

[Emulating Assembly Language Behavior](#)

IDAPython

[Using IDAPython](#)

IDAPython Scripting Examples

[Enumerating Functions](#)

[Enumerating Instructions](#)

[Enumerating Cross-References](#)

Summary

16. The IDA Software Development Kit

SDK Introduction

[SDK Installation](#)

[SDK Layout](#)

[Configuring a Build Environment](#)

The IDA Application Programming Interface

[Header Files Overview](#)

[Netnodes](#)

[Useful SDK Datatypes](#)

[Commonly Used SDK Functions](#)

[Iteration Techniques Using the IDA API](#)

Summary

Writing a Plug-in

[The Plug-in Life Cycle](#)

[Plug-in Initialization](#)

[Event Notification](#)

[Plug-in Execution](#)

Building Your Plug-ins

[Installing Plug-ins](#)

[Configuring Plug-ins](#)

[Extending IDC](#)

[Plug-in User Interface Options](#)

[Using the SDK's Chooser Dialogs](#)

[Creating Customized Forms with the SDK](#)

[Windows-Only User Interface-Generation Techniques](#)

[User Interface Generation with Qt](#)

Scripted Plug-ins

[Summary](#)

18. Binary Files and IDA Loader Modules

[Unknown File Analysis](#)

[Manually Loading a Windows PE File](#)

[IDA Loader Modules](#)

[Writing an IDA Loader Using the SDK](#)

[The Simpleton Loader](#)

[Building an IDA Loader Module](#)

[A pcap Loader for IDA](#)

[Alternative Loader Strategies](#)

[Writing a Scripted Loader](#)

[Summary](#)

19. IDA Processor Modules

[Python Byte Code](#)

[The Python Interpreter](#)

[Writing a Processor Module Using the SDK](#)

[The processor_t Struct](#)

[Basic Initialization of the LPH Structure](#)

[The Analyzer](#)

[The Emulator](#)

[The Outputter](#)

[Processor Notifications](#)

[Other processor_t Members](#)

[Building Processor Modules](#)

[Customizing Existing Processors](#)

[Processor Module Architecture](#)

[Scripting a Processor Module](#)

[Summary](#)

V. Real-World Applications

20. Compiler Personalities

[Jump Tables and Switch Statements](#)

[RTTI Implementations](#)

[Locating main](#)

[Debug vs. Release Binaries](#)

[Alternative Calling Conventions](#)

[Summary](#)

21. Obfuscated Code Analysis

Anti-Static Analysis Techniques

Disassembly Desynchronization

Dynamically Computed Target Addresses

Imported Function Obfuscation

Targeted Attacks on Analysis Tools

Anti-Dynamic Analysis Techniques

Detecting Virtualization

Detecting Instrumentation

Detecting Debuggers

Preventing Debugging

Static De-obfuscation of Binaries Using IDA

Script-Oriented De-obfuscation

Emulation-Oriented De-obfuscation

Virtual Machine-Based Obfuscation

Summary

- [download online Changing My Mind: Occasional Essays](#)
- [click A Guide to Poetics Journal: Writing in the Expanded Field, 1982â€“1998 pdf, azw \(kindle\), epub, doc, mobi](#)
- [click Succubus Blues \(Georgina Kincaid, Book 1\) pdf, azw \(kindle\)](#)
- [Mathematics, Ideas and the Physical Real online](#)
- [download online Nelson the Commander book](#)
- [Building Military Dioramas, Volume 2 here](#)

- <http://metromekanik.com/ebooks/Magicians-of-the-Gods--The-forgotten-wisdom-of-earth-s-lost-civilisation.pdf>
- <http://www.freightunlocked.co.uk/lib/Hot-Springs.pdf>
- <http://www.khoi.dk/?books/The-Yoga-Sutras-of-Patanjali.pdf>
- <http://studystategically.com/freebooks/Mathematics--Ideas-and-the-Physical-Real.pdf>
- <http://deltaphenomics.nl/?library/Nelson-the-Commander.pdf>
- <http://www.gateaerospaceforum.com/?library/The-Politics-of-Inequality--A-Political-History-of-the-Idea-of-Economic-Inequality-in-America.pdf>