

CONTENTS IN DETAIL

FOREWORD by Pierre Vandevenne	xix
ACKNOWLEDGMENTS	xxi
INTRODUCTION	xxiii

PART I INTRODUCTION TO IDA

1	
INTRODUCTION TO DISASSEMBLY	3
Disassembly Theory	4
The What of Disassembly	5
The Why of Disassembly	6
Malware Analysis	6
Vulnerability Analysis	6
Software Interoperability	7
Compiler Validation	7
Debugging Displays	7
The How of Disassembly	7
A Basic Disassembly Algorithm	8
Linear Sweep Disassembly	9
Recursive Descent Disassembly	11
Summary	14
2	
REVERSING AND DISASSEMBLY TOOLS	15
Classification Tools	16
file	16
PE Tools	18
PEiD	19
Summary Tools	20
nm	20
ldd	22
objdump	23
otool	24
dumppbin	25
c++filt	25
Deep Inspection Tools	27
strings	27
Disassemblers	28
Summary	29

3	IDA PRO BACKGROUND	31
	Hex-Rays' Stance on Piracy	32
	Obtaining IDA Pro	32
	IDA Versions	33
	IDA Licenses	33
	Purchasing IDA	33
	Upgrading IDA	34
	IDA Support Resources	34
	Your IDA Installation	35
	Windows Installation	36
	OS X and Linux Installation	37
	The IDA Directory Layout	37
	Thoughts on IDA's User Interface	39
	Summary	39

PART II

BASIC IDA USAGE

4	GETTING STARTED WITH IDA	43
	Launching IDA	44
	IDA File Loading	46
	Using the Binary File Loader	47
	IDA Database Files	49
	IDA Database Creation	50
	Closing IDA Databases	52
	Reopening a Database	53
	Introduction to the IDA Desktop	54
	Desktop Behavior During Initial Analysis	56
	IDA Desktop Tips and Tricks	58
	Reporting Bugs	58
	Summary	59

5	IDA DATA DISPLAYS	61
	The Principal IDA Displays	62
	The Disassembly Window	62
	The Names Window	68
	The Message Window	69
	The Strings Window	70
	Secondary IDA Displays	71
	The Hex View Window	72
	The Exports Window	73
	The Imports Window	73

The Functions Window	74
The Structures Window	74
The Enums Window	75
Tertiary IDA Displays	75
The Segments Window	75
The Signatures Window	76
The Type Libraries Window	77
The Function Calls Window	77
The Problems Window	78
Summary	79

6

DISASSEMBLY NAVIGATION **81**

Basic IDA Navigation	82
Double-Click Navigation	82
Jump to Address	84
Navigation History	84
Stack Frames	85
Calling Conventions	87
Local Variable Layout	91
Stack Frame Examples	91
IDA Stack Views	95
Searching the Database	100
Text Searches	101
Binary Searches	101
Summary	102

7

DISASSEMBLY MANIPULATION **103**

Names and Naming	104
Parameters and Local Variables	104
Named Locations	105
Register Names	107
Commenting in IDA	108
Regular Comments	109
Repeatable Comments	109
Anterior and Posterior Lines	110
Function Comments	110
Basic Code Transformations	110
Code Display Options	111
Formatting Instruction Operands	114
Manipulating Functions	115
Converting Data to Code (and Vice Versa)	121
Basic Data Transformations	122
Specifying Data Sizes	123
Working with Strings	124
Specifying Arrays	126
Summary	128

8	DATATYPES AND DATA STRUCTURES	129
Recognizing Data Structure Use	131	
Array Member Access	131	
Structure Member Access	136	
Creating IDA Structures	142	
Manual Structure Layout	143	
Using Structure Templates	147	
Importing New Structures	150	
Parsing C Structure Declarations	150	
Parsing C Header Files	151	
Using Standard Structures	152	
IDA TIL Files	155	
Loading New TIL Files	155	
Sharing TIL Files	155	
C++ Reversing Primer	156	
The this Pointer	156	
Virtual Functions and Vtables	157	
The Object Life Cycle	160	
Name Mangling	162	
Runtime Type Identification	163	
Inheritance Relationships	164	
C++ Reverse Engineering References	165	
Summary	166	
9	CROSS-REFERENCES AND GRAPHING	167
Cross-References	168	
Code Cross-References	169	
Data Cross-References	171	
Cross-Reference Lists	173	
Function Calls	175	
IDA Graphing	176	
Legacy IDA Graphing	176	
IDA's Integrated Graph View	184	
Summary	186	
10	THE MANY FACES OF IDA	187
Console Mode IDA	188	
Common Features of Console Mode	188	
Windows Console Specifics	189	
Linux Console Specifics	190	
OS X Console Specifics	192	
Using IDA's Batch Mode	195	
GUI IDA on Non-Windows Platforms	196	
Summary	198	

PART III ADVANCED IDA USAGE

11		
CUSTOMIZING IDA		201
Configuration Files		201
The Main Configuration File: ida.cfg		202
The GUI Configuration File: idagui.cfg		203
The Console Configuration File: idatui.cfg		206
Additional IDA Configuration Options		207
IDA Colors		207
Customizing IDA Toolbars		208
Summary		210
12		
LIBRARY RECOGNITION USING FLIRT SIGNATURES		211
Fast Library Identification and Recognition Technology		212
Applying FLIRT Signatures		212
Creating FLIRT Signature Files		216
Signature-Creation Overview		217
Identifying and Acquiring Static Libraries		217
Creating Pattern Files		219
Creating Signature Files		221
Startup Signatures		224
Summary		225
13		
EXTENDING IDA'S KNOWLEDGE		227
Augmenting Function Information		228
IDS Files		230
Creating IDS Files		232
Augmenting Predefined Comments with loadint		234
Summary		236
14		
PATCHING BINARIES AND OTHER IDA LIMITATIONS		237
The Infamous Patch Program Menu		238
Changing Individual Database Bytes		238
Changing a Word in the Database		239
Using the Assemble Dialog		239
IDA Output Files and Patch Generation		241
IDA-Generated MAP Files		242
IDA-Generated ASM Files		242
IDA-Generated INC Files		243
IDA-Generated LST Files		243

IDA-Generated EXE Files	243
IDA-Generated DIF Files	244
IDA-Generated HTML Files	245
Summary	245

PART IV EXTENDING IDA'S CAPABILITIES

15 SCRIPTING WITH IDC 249

Basic Script Execution	250
The IDC Language	251
IDC Variables	251
IDC Expressions	252
IDC Statements	252
IDC Functions	253
IDC Programs	254
Error Handling in IDC	255
Persistent Data Storage in IDC	256
Associating IDC Scripts with Hotkeys	258
Useful IDC Functions	258
Functions for Reading and Modifying Data	259
User Interaction Functions	260
String-Manipulation Functions	261
File Input/Output Functions	261
Manipulating Database Names	262
Functions Dealing with Functions	263
Code Cross-Reference Functions	264
Data Cross-Reference Functions	265
Database Manipulation Functions	265
Database Search Functions	266
Disassembly Line Components	267
IDC Scripting Examples	267
Enumerating Functions	268
Enumerating Instructions	268
Enumerating Cross-References	269
Enumerating Exported Functions	272
Finding and Labeling Function Arguments	272
Emulating Assembly Language Behavior	274
Summary	277

16 THE IDA SOFTWARE DEVELOPMENT KIT 279

SDK Introduction	280
SDK Installation	281
SDK Layout	281
Configuring a Build Environment	283

The IDA Application Programming Interface	284
Header Files Overview	284
Netnodes	288
Useful SDK Datatypes	296
Commonly Used SDK Functions	298
Iteration Techniques Using the IDA API	304
Summary	308

17 THE IDA PLUG-IN ARCHITECTURE 309

Writing a Plug-in	310
The Plug-in Life Cycle	312
Plug-in Initialization	313
Event Notification	315
Plug-in Execution	316
Building Your Plug-ins	318
Plug-in Installation	322
Plug-in Configuration	323
Extending IDC	324
Plug-in User Interface Options	327
Building Interface Elements with the SDK	327
Summary	336

18 BINARY FILES AND IDA LOADER MODULES 337

Unknown File Analysis	338
Manually Loading a Windows PE File	339
IDA Loader Modules	347
Writing an IDA Loader	348
The Singleton Loader	350
Building an IDA Loader Module	355
A pcap Loader for IDA	355
Alternative Loader Strategies	361
Summary	362

19 IDA PROCESSOR MODULES 363

Python Byte Code	364
The Python Interpreter	365
Writing a Processor Module	366
The processor_t Struct	366
Basic Initialization of the LPH Structure	367
The Analyzer	371
The Emulator	376
The Outputter	380
Processor Notifications	385
Other processor_t Members	386

Building Processor Modules	389
Customizing Existing Processors	393
Processor Module Architecture	395
Summary	396

PART V REAL-WORLD APPLICATIONS

20 COMPILER VARIATIONS 399

Jump Tables and Switch Statements	400
RTTI Implementations	404
Locating main	405
Debug vs. Release Binaries	412
Alternative Calling Conventions	414
Summary	415

21 OBFUSCATED CODE ANALYSIS 417

Anti-Static Analysis Techniques	418
Disassembly Desynchronization	418
Dynamically Computed Target Addresses	421
Imported Function Obfuscation	428
Targeted Attacks on Analysis Tools	432
Anti-Dynamic Analysis Techniques	433
Detecting Virtualization	433
Detecting Instrumentation	435
Detecting Debuggers	435
Preventing Debugging	436
Static De-obfuscation of Binaries Using IDA	438
Script-Oriented De-obfuscation	438
Emulation-Oriented De-obfuscation	443
Summary	455

22 VULNERABILITY ANALYSIS 457

Discovering New Vulnerabilities with IDA	458
After-the-Fact Vulnerability Discovery with IDA	465
IDA and the Exploit-Development Process	469
Stack Frame Breakdown	470
Locating Instruction Sequences	472
Finding Useful Virtual Addresses	473
Analyzing Shellcode	475
Summary	477

23	REAL-WORLD IDA PLUG-INS	479
Hex-Rays		480
IDAPython		481
IDARub		484
IDA Sync		485
collabREate		488
ida-x86emu		492
mIDA		492
Summary		494

PART VI THE IDA DEBUGGER

24	THE IDA DEBUGGER	497
Launching the Debugger		498
Basic Debugger Displays		501
Process Control		504
Breakpoints		505
Tracing		508
Stack Traces		511
Watches		511
Automating Debugger Tasks		512
Scripting Debugger Actions with IDC		512
Automating Debugger Actions with IDA Plug-ins		517
Summary		520

25	DISASSEMBLER/DEBUGGER INTEGRATION	521
Background		522
IDA Databases and the IDA Debugger		523
Debugging Obfuscated Code		525
Simple Decryption and Decompression Loops		526
Import Table Reconstruction		530
Hiding the Debugger		533
Dealing with Exceptions		538
Summary		544

26	LINUX, OS X, AND REMOTE DEBUGGING WITH IDA	545
Console-Mode Debugging		545
Remote Debugging with IDA		547
Exception Handling During Remote Debugging		550
Using Scripts and Plug-ins During Remote Debugging		550
Summary		550

A	
USING IDA FREEWARE 4.9	551
Restrictions on IDA Freeware	552
Using IDA Freeware	553
B	
IDC/SDK CROSS-REFERENCE	555
C	
WHAT'S NEW IN IDA 5.3	573
Redesigned Debugger	574
Type Library Support	574
New IDC Functions	574
New API/SDK Functionality	574
Summary	575
INDEX	577