Memory Dump Analysis Anthology

Volume 8a

Dmitry Vostokov
Software Diagnostics Institute

OpenTask

Published by OpenTask, Republic of Ireland

OpenTask books are available through booksellers and distributors worldwide. For further information or comments send requests to press@opentask.com.

A CIP catalog record for this book is available from the British Library.

ISBN-13: 978-1-908043-53-5 (Paperback)

First printing, 2014

Revision 2.0 (July 2015)

Table of Contents

Preface **7**

About the Author **9**

PART 1: Professional Crash Dump Analysis and Debugging **11**

Software Diagnostics Professional Certification 11
Three Roads to Kernel Space 13

PART 2: Crash Dump Analysis Patterns **15**

Design Value 15
Hidden IRP 16
Tampered Dump 17
Wait Chain (RTL_RESOURCE) 29
Memory Fluctuation (Process Heap) 35
Last Object 37
Rough Stack Trace 39
Past Stack Trace 43
Stack Trace (I/O Request) 46
Stack Trace (File System Filters) 48
Stack Trace (Database) 51
Wait Chain (Modules) 56
Insufficient Memory (Stack Trace Database) 57
Insufficient Memory (Region) 63
Memory Leak (Regions) 65
Invalid Handle (Managed Space) 69
Ghost Thread 77
Dry Weight 79
Exception Module 80

PART 3: Memory Forensics **83**

Memory Forensics Professional Certification 83
Native Memory Forensics 84

PART 4: A Bit of Science and Philosophy 85

Memory Symmetry Breaking 85
Memoevolutionism 86
Entropy as Memory and Memory as Entropy 87
Notes on Memoidealism 88
Welcome to Memorianism 89
United Memory Lands, Memorianites, EthnOS 90
Quotes from Memoriarch 91
Pattern-Oriented Philosophy 92

PART 5: Software Trace Analysis Patterns 93

Hidden Facts 93
Back Trace 95
Blackout 97
Missing Message 99
Use Case Trail 101
Event Sequence Phase 103
Milestones 105
File Size 107
Singleton Event 108
Visitor Trace 110

PART 6: Fun with Crash Dumps 111

Debugging Slang and Proverbs 111

PUS 111
Coollect 111
Dump-out 111
LOGIC 111
DiagNose 112
Consolidation 112
No Pass a Run! 112
ID IoT Zone 112
Putty in Someone's Hands 112
DisPatched vs. DESPatched 112
Programmatica Nervosa 113

GOTCHA *113*
Pan-o-RAM-ic *113*
VLSI *113*
Debugging Proverb *113*

Space Opera 114
If Programmers Were Writers 115
My Computer Celebrates Halloween 116
Look, there's a Bug! 117
Diagnostics in Science Fiction 118
Hard Copy Natives 119

PART 7: Software Narratology 121

Malnarratives 121
Higher-Order Pattern Narratives (Analyzing Diagnostic Analysis) 123

PART 8: Software Diagnostics, Troubleshooting, and Debugging 127

A Pattern Language for Performance Analysis 127
The Timeless Way of Diagnostics 128
Pattern-Oriented Debugging Process 130

PART 9: Art and Visualization 133

Café WoW 133
Bang Debugging 134
Bug Hunter 135
Glass of Water Dump 136
Memory Dump Analysis 137
Organic Incidents and Bad Stench 138

PART 10: Miscellaneous 139

Book Discovery 139
Quotes 140

Appendix 143

Crash Dump Analysis Checklist 143

Index of WinDbg Commands 147

Notes 149