

Memory Dump Analysis Anthology

Volume 4

Dmitry Vostokov
Software Diagnostics Institute

Published by OpenTask, Republic of Ireland

Copyright © 2010 by Dmitry Vostokov

Copyright © 2015 by Software Diagnostics Institute

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, without the prior written permission of the publisher.

You must not circulate this book in any other binding or cover, and you must impose the same condition on any acquirer.

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

Product and company names mentioned in this book may be trademarks of their owners.

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

ISBN-13: 978-1-906717-86-5 (Paperback)

ISBN-13: 978-1-906717-87-2 (Hardback)

First printing, 2010

Revision 2 (June, 2015)

Crash Dump is a double buzzword.

Summary of Contents

Preface	17
Acknowledgements.....	19
PART 1: Professional Crash Dump Analysis and Debugging.....	21
PART 2: Crash Dump Analysis Patterns.....	93
PART 3: Crash Dump Analysis AntiPatterns	167
Part 4: Pattern Interaction	169
PART 5: A Bit of Science and Philosophy.....	235
PART 6: Fun with Crash Dumps.....	261
PART 7: Software Troubleshooting	303
PART 8: Software Trace Analysis.....	327
PART 9: Software Trace Analysis Patterns	335
PART 10: The Origin of Crash Dumps	353
PART 11: Memory Visualization	361
PART 12: Art	391
PART 13: Miscellaneous	401
Appendix	417
Index of WinDbg Commands	419
Notes.....	421
About the Author.....	422

Cover Images..... 423

Contents

Preface	17
Acknowledgements.....	19
PART 1: Professional Crash Dump Analysis and Debugging.....	21
Common Mistakes	21
Not Using Checklists.....	21
Not Paying Attention to All Aspects of Default Analysis	23
Not Paying Attention to Context.....	26
Raw Stack Dump of WOW64 Process	31
On Space and Mode.....	35
Registry Corruption: A Case Study	36
Wild Code and Partial Stack Reconstruction.....	39
Manual Parameter Reconstruction on x64 Windows Systems	42
Counterfactual Debugging	46
Dereference Fixpoints.....	46
Data Ordering.....	48
Clean Raw Stack Execution Residue.....	64
Essential and Derived Properties	71
Software Defect Researcher: A New Profession	74

WinDbg Shortcuts	75
Imu and Imk	75
.opendump.....	80
Live Kernel Debugging of System Freeze	82
Mode-Independent WinDbg Scripts	91
PART 2: Crash Dump Analysis Patterns	93
Succession of Patterns	93
Ubiquitous Component.....	94
Nested Offender	120
Hunting for a Driver	124
Virtualized System.....	131
Effect Component	137
Well-Tested Function	144
Mixed Exception.....	145
Random Object	150
Not My Version (Hardware).....	153
Missing Process.....	154
Platform-Specific Debugger	156
Value Deviation (Stack Trace)	159
CLR Thread	163

Insufficient Memory (Control Blocks)	166
PART 3: Crash Dump Analysis AntiPatterns	167
Habitual Reply	167
Part 4: Pattern Interaction	169
Null Data Pointer, Pass-Through Functions, and Platformorphic Fault	169
Stack Trace Collection, Message Box, Hidden Exception, Nested Offender, Insufficient Memory, C++ Exception, Heap Leak and Ubiquitous Component	172
Blocked LPC Thread, Coupled Processes, Stack Trace Collection and Blocked GUI Thread	181
Virtualized Process, Incorrect Stack Trace, Stack Trace Collection, Multiple Exceptions, Optimized Code and C++ Exception	182
WOW64 Process, NULL Data Pointer, Stack Overflow, Main Thread, Incorrect Stack Trace, Nested Exceptions, Hidden Exception, Manual Dump, Multiple Exceptions and Virtualized System	189
NULL Data Pointer, Stack Trace, Inline Function Optimization and Platformorphic Fault	201
Stack Trace Collection, Suspended Threads, Not My Version, Special Process, Main Thread and Blocked LPC Chain Threads	204
Truncated Dump, Stack Trace Collection, Waiting Thread Time and Wait Chains ...	212
ALPC Wait Chain, Missing Threads, Message Box, Zombie and Special Processes ...	214
Critical Section High Contention and Wait Chains, Blocked Threads and Periodic Error: Memory Dump and Trace Analysis Pattern Cooperation	220
Statement Current, Coupled Processes, Wait Chain, Spiking Thread, Hidden Exception, Message Box and Not My Version	223

Stack Trace Collection, Missing Threads, Waiting Thread Time, Critical Section and LPC Wait Chains	226
Wait Chain, Blocked Thread, Waiting Thread Time, IRP Distribution Anomaly and Stack Trace Collection	231
PART 5: A Bit of Science and Philosophy.....	235
Memory Exponentiation (PowerSet)	235
Memory Dump View of Artificial Intelligence	236
Memoidealism as Monistic Aspect Pluralism.....	237
Memory Dumps as Posets.....	239
Metaphorical Bijectionism: A Method of Inquiry.....	241
Notes on Memoidealism	246
Panmemorism	247
Cubic Memory Representation	248
Manifold Memory Space.....	250
Ars Recordatio.....	252
Categories for the Working Software Defect Researcher	253
MemD Category	253
Operating Closure of Memory	256
Memoidealism Defined.....	258
Memuon: A Definition	259
PART 6: Fun with Crash Dumps.....	261

Music for Debugging	261
THE ALL MIGHTY DEBUGGER	261
Memory Space Music.....	262
The Duet of Threads.....	263
The Memory Dump of the Dead	264
Ancient Computations and a Vision of the New Dump	265
The Meaning of DUMP	266
Memory Analysis Ritual	267
The Intelligent Memory Movement.....	268
Moving towards the Psi Point	269
Experiments on Poor Bugs	270
Exception Processing Of Crash Hypothesis (EPOCH).....	271
Debugging Slang.....	272
SAD Events	272
BoBo Address	273
Mad Day	274
Bug-sistential and Bug-sistentialism	275
Debugging Spy Network.....	276
Games for Debugging: Go	277
The Tsar of Memory Dump Analysis	278

DNA and RNA of Ruptured Computation	279
BAD0B0B0 Address: Childhood Memories.....	280
Bugs in Passing	281
Named Process: Vostokov.exe	283
Memory Analysts and Debuggers Day	286
After Volume 3	287
Crash, Core and Memory Dumps in Science Fiction and Fantasy	288
Reasoning with a Bug	301
PART 7: Software Troubleshooting	303
RADII and SDSD	303
Epistemic Troubleshooting and Debugging	304
RADII Process Illustrated	305
Debugware Patterns	307
Trace Expert	307
Troubleshooting Unit of Work	308
Checklist	309
Supporting Module	310
Span Differentiator	311
Self-Extractor	312
A Case Study.....	314

Can Software Tweet?	319
The Law of Simple Tools.....	320
Workaround Patterns	321
Hidden Output	321
Frozen Process	324
Axed Code	325
PART 8: Software Trace Analysis.....	327
CDFAnalyzer for Analysis of CDF (ETW) Traces	327
There ought to be a Planet at that Location!.....	328
Software Trace: Bird's Eye View.....	329
Extending Multithreading to Multibraiding (Adjoint Threading)	330
PART 9: Software Trace Analysis Patterns	335
Statement Density and Current	335
Exception Stack Trace	337
Thread of Activity.....	339
Discontinuity	341
Missing Component	342
Bifurcation Point	343
Characteristic Message Block.....	345
Activity Region	348

Vocabulary Index.....	349
Inter-Correlation	350
PART 10: The Origin of Crash Dumps	353
Full Page Heap Settings on x64 Windows	353
Memory Dumps from Hyper-Virtualized Windows	354
Fiber Bundle of Memory Space.....	357
On Self Dumps of Secure String API	358
PART 11: Memory Visualization	361
Pictures from Memory Space.....	361
Large-scale Structure of Memory Space	363
Advanced Memory Visualization	365
3D Memory Visualization	376
Memory Map Visualization Tools	389
PART 12: Art	391
Opcodism: The Art of Opcodes	391
Memory Dump and Minidumps.....	394
Hot Issues from Physicalist Artist Perspective	395
Memory Dumps from Physicalist Artist Perspective.....	396
Memory Hot Spot and the Illusion of Fix	397
Shared Section	398

Memory Space Road to the Ultimate Fix	399
Structure and Noise	400
PART 13: Miscellaneous	401
Assembling Code in WinDbg	401
Free Stack Traces	403
Stack Space and Program Database Types.....	405
The Longest Stack Trace.....	409
Software Victimology.....	414
Debugger as a Shut up Application	415
2 Great Windows Software Engineering Magazines	416
Appendix.....	417
Crash Dump Analysis Checklist.....	417
Index of WinDbg Commands	419
Notes.....	421
About the Author.....	422
Cover Images.....	423