

Memory Dump Analysis Anthology

Volume 6

Dmitry Vostokov
Software Diagnostics Institute

Published by OpenTask, Republic of Ireland

Copyright © 2013 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: 978-1-908043-19-1 (Paperback)

ISBN-13: 978-1-908043-20-7 (Hardback)

First printing, 2013

Revision 2 (July 2015)

Summary of Contents

Preface	15
Acknowledgements.....	17
PART 1: Professional Crash Dump Analysis and Debugging.....	19
PART 2: Crash Dump Analysis Patterns	31
PART 3: Pattern Interaction	163
PART 4: Unified and Generative Debugging	171
PART 5: A Bit of Science and Philosophy.....	175
PART 6: Fun with Crash Dumps.....	189
PART 7: A Bit of Religion	235
PART 8: Software Trace Analysis.....	239
PART 9: Software Trace Analysis Patterns	243
PART 10: Software Troubleshooting and Debugging	255
PART 11: Software Victimology	263
PART 12: Art	265
PART 13: Miscellaneous	277
PART 14: Intelligence Analysis	289
Appendix	291
Index of WinDbg Commands	301
About the Author	304

Cover Images..... 305

Contents

Preface	15
Acknowledgements.....	17
PART 1: Professional Crash Dump Analysis and Debugging.....	19
Memory Dump Analysis Best Practices.....	19
Windows Debugging Expert System WinDbg Extension	20
Common Mistakes	21
Not Comparing to Reference Debugger Output	21
From Bugchecks to Patterns	23
Raw Stack from Laterally Damaged Memory Dumps	24
WinDbg Tips and Tricks: Getting the Bottom of a Stack Trace	26
PART 2: Crash Dump Analysis Patterns.....	31
Divide by Zero (Kernel Mode)	31
Fat Process Dump	33
Blocked Queue	34
Crash Signature	37
Invalid Parameter (Process Heap).....	40
Hooking Level.....	43
Embedded Comments.....	47
Well-Tested Module.....	48

String Parameter	49
Environment Hint	51
Dual Stack Trace	52
Blocking Module	54
Wait Chain (Window Messaging)	55
Wait Chain (Named Pipes)	60
Top Module	62
Dialog Box	63
Technology-Specific Subtrace (COM Interface Invocation)	67
Livelock	70
Semantic Structure (PID.TID)	73
Instrumentation Side Effect	77
Directing Module	80
Stack Overflow (Software Implementation)	82
Data Correlation	84
Truncated Stack Trace	86
Least Common Frame	87
Self-Diagnosis (Kernel Mode)	89
Technology-Specific Subtrace (Dynamic Memory)	90
Module Hint	92

Custom Exception Handler (Kernel Space).....	94
No Data Types	96
Cloud Environment	97
Version-Specific Extension	99
Multiple Exceptions (Managed Space).....	104
Blocking File	105
Quiet Dump.....	109
Pleiades	110
Thread Age	111
Unsynchronized Dumps	113
Coupled Modules	114
Managed Stack Trace	115
Problem Vocabulary.....	116
Activation Context.....	117
Stack Trace Set	120
Special Thread (.NET CLR)	123
Dynamic Memory Corruption (Managed Heap)	124
Stack Trace Collection (Managed Space)	127
Duplicate Extension	131
Deadlock (Managed Space).....	135

Caller-n-Callee	138
Handled Exception (User Space)	141
Handled Exception (.NET CLR).....	144
Execution Residue (Managed Space)	149
Annotated Disassembly (JIT .NET code)	151
Wait Chain (Mutex Objects).....	153
Inline Function Optimization (Managed Code)	155
Technology-Specific Subtrace (JIT .NET Code)	157
Double IRP Completion	160
PART 3: Pattern Interaction	163
Main Thread, Self-Diagnosis, Window Message Chain, Blocking Module, Ubiquitous Component, Dual Stack Trace, Pipe Wait Chain and Coupled Machines.....	163
Abridged Dump, Embedded Comment, Spiking Thread, Incorrect Stack Trace and Top Module.....	166
Stack Trace Collection, Message Box, Self-Diagnosis, Version-Specific Extension, Managed Stack Trace and Managed Code Exception	168
PART 4: Unified and Generative Debugging	171
A Periodic Table of Software Defects.....	171
Analysis, Architectural, Design, Implementation and Usage Debugging Patterns....	172
Generative Debugging	173
Metadefect Template Library	174
PART 5: A Bit of Science and Philosophy.....	175

On Memory Perspectives	175
Orbifold Memory Space	176
Notes on Memoidealism	177
M->analysis	178
Memiosphere.....	179
On Memory-Time vs. Space-Time	180
The Will to Be Memorized	181
The Trinity of Memory Worldview	182
Uses of Memoretics	183
Crossdisciplinary Memoretics as Interdisciplinary Science	184
Private Property on Memory Spaces	185
Coarse vs. Fine Grained DNA of Software Behavior.....	187
PART 6: Fun with Crash Dumps.....	189
Music for Debugging	189
555 Binary Threads	189
Out of Memory and Losing My Data (Comment Impact).....	190
Navigating the Long List	191
Debugging Joke	192
Memory Dump Barcodes	193
MessageBox at Dublin Zoo.....	194

CDB for Kids.....	195
Snow Spike Residue	196
Second Snowfall Spike in Dublin	197
MMXI.....	198
Happy New Year and Decade of Debugging 0x7DB - 0x7E4!.....	199
Do Security Professionals Dream?	204
Debugging Slang.....	205
Golden Bug.....	205
Beer Time	206
Finger Exercise	207
Resolution Rush	208
The Window of Opportunity	209
Dump.....	210
Pre-analysis	211
Tapping.....	212
Having Fun	213
Adult Debugging.....	214
Second Eye	215
Abscess.....	216
Finction	217

Mad OS and other Publishing Blunders	218
The Ultimate Debugger's Desk.....	221
Memceptions: Flags and Handles are Everywhere!.....	222
Computer Memory Monsters	223
On President's Daily Briefs (PDBs)	226
The First Evidence for Process Resurrection	227
Vacuum Pages.....	228
WinDbg Command on Certificate	230
Pleasing WinDbg SOS Extension.....	231
Airport Terminal Services Incident.....	232
Philosophical Self-Interview.....	233
PART 7: A Bit of Religion	235
Memory Creates God.....	235
Morality and Memorianity.....	236
On Natural Theology	237
PART 8: Software Trace Analysis.....	239
Pattern Interaction.....	239
Basic Facts, Periodic Error, and Defamiliarizing Effect.....	239
Close and Deconstructive Readings of a Software Trace	240
Software Tracing Best Practices	241

No Longer Seeing Nothing: The Advantage of Patterns.....	242
PART 9: Software Trace Analysis Patterns	243
Focus of Tracing	243
Event Sequence Order	244
Implementation Discourse.....	245
News Value	246
Master Trace	247
Gossip.....	248
Impossible Trace	249
Glued Activity.....	250
Message Invariant.....	251
UI Message.....	252
Original Message.....	253
PART 10: Software Troubleshooting and Debugging	255
Debugware Patterns	255
System Description Snapshot.....	255
Debugging in 2021: Trends for the Next Decade	256
The Way of Philip Marlowe: Abductive Reasoning for Troubleshooting and Debugging	257
Workaround Patterns	258
Fake API.....	258

User Interface Problem Analysis Patterns.....	259
Message Box	259
PART 11: Software Victimology	263
Function Activity Theory	263
PART 12: Art	265
No E-numbers Software Product Sticker	265
Paleo-debugging: Excavated Minidump.....	266
Stack Trace Art	267
Debugger’s Dream	268
Defect in Defect	269
Memorianity Cross.....	270
Memioart: The New Art Form.....	271
Clouded	272
Cloud Traces.....	273
What Is To Be Done?.....	274
PART 13: Miscellaneous	277
GI Index of Memory Dump Analysis.....	277
The New School of Debugging	279
TestWER Tool to Test Windows Error Reporting	280
Moving to ARM	283

The New School of Debugging: What’s New 284

A.C.P. Root Cause Analysis Methodology 285

TestWAER Tool to Test Windows Azure Error Reporting 286

PART 14: Intelligence Analysis 289

 Intelligence Analysis Patterns 289

 The Birth of Memory Intelligence Agency 290

Appendix 291

 Memory Analysis as a Service 291

 Stack Overflow Patterns 292

 .NET / CLR / Managed Space Patterns 293

 Stack Trace Patterns 294

 Symbol Patterns 295

 Analysis Compass 296

 Software Trace Analysis Checklist 297

 Crash Dump Analysis Checklist 298

Index of WinDbg Commands 301

About the Author 304

Cover Images 305