

# Memory Dump Analysis Anthology

---

## Volume 5

**Dmitry Vostokov**  
**Software Diagnostics Institute**

Published by OpenTask, Republic of Ireland

Copyright © 2011 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](mailto:press@opentask.com).

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

ISBN-13: 978-1-906717-96-4 (Paperback)

ISBN-13: 978-1-906717-97-1 (Hardback)

First printing, 2011

Revision 2 (June 2015)

To Memory.



## Summary of Contents

Preface .....	17
Acknowledgements.....	19
PART 1: Professional Crash Dump Analysis and Debugging.....	21
PART 2: Crash Dump Analysis Patterns .....	43
PART 3: Crash Dump Analysis AntiPatterns .....	129
PART 4: Pattern Interaction .....	133
PART 5: A Bit of Science and Philosophy.....	213
PART 6: Fun with Crash Dumps.....	231
PART 7: Software Trace Analysis.....	271
PART 8: Software Trace Analysis Patterns .....	281
PART 9: Models of Software Behaviour .....	311
PART 10: The Origin of Crash Dumps .....	335
PART 11: Structural Memory Patterns .....	343
PART 12: Memory Visualization .....	353
PART 13: Art .....	375
PART 14: Security and Malware Analysis .....	401
PART 15: Miscellaneous .....	411
Appendix.....	423
Index of WinDbg Commands .....	427

Notes..... 429

About the Author..... 430

Cover Images..... 431

## Contents

Preface .....	17
Acknowledgements.....	19
PART 1: Professional Crash Dump Analysis and Debugging.....	21
Common Mistakes .....	21
Not Double-Checking Symbolic Output .....	21
Not Looking Past the First Found Evidence.....	24
Not Recognizing Data as UNICODE or ASCII Fragments .....	26
Common Questions.....	28
What Service is this? .....	28
Complete Stack Traces from x64 System .....	30
Software Behavior Patterns .....	32
Crash and Hang Analysis Audit Service .....	33
Case Study: Extremely Inconsistent Dump and CPU Spike .....	34
Raw Stack Dump of All Thread Stacks .....	39
Architecture of CARE.....	41
PART 2: Crash Dump Analysis Patterns.....	43
Succession of Patterns .....	43
Wait Chain (Process Objects) .....	49

Coincidental Frames.....	55
Fault Context.....	59
Coupled Processes (Weak).....	60
Hooked Functions (Kernel Space) .....	63
Hardware Activity.....	66
Incorrect Symbolic Information .....	71
Message Hooks .....	76
Blocked Thread (Hardware) .....	79
Coupled Machines.....	81
High Contention (Processors) .....	82
Thread Starvation (Normal Priority) .....	85
Coupled Processes (Semantics).....	87
Abridged Dump .....	88
Exception Stack Trace .....	93
Wait Chain (RPC) .....	95
Distributed Spike.....	99
Instrumentation Information .....	108
Template Module.....	112
Invalid Exception Information.....	116
Shared Buffer Overwrite .....	120



Pervasive System.....	125
Problem Exception Handler .....	126
Deadlock (Self) .....	127
Same Vendor.....	128
PART 3: Crash Dump Analysis AntiPatterns .....	129
Wild Explanations.....	129
PART 4: Pattern Interaction .....	133
Inconsistent Dump, Stack Trace Collection, LPC, Thread, Process, Executive Resource Wait Chains, Missing Threads and Waiting Thread Time.....	133
Fault Context, Wild Code, and Hardware Error .....	137
Main Thread, Critical Section Wait Chains, Critical Section Deadlock, Stack Trace Collection, Execution Residue, Data Contents Locality, Self-Diagnosis and Not My Version .....	145
Strong Process Coupling, Stack Trace Collection, Critical Section Corruption and Wait Chains, Message Box, Self-Diagnosis, Hidden Exception and Dynamic Memory Corruption.....	158
IRP Distribution Anomaly, Inconsistent Dump, Execution Residue, Hardware Activity, Coincidental Symbolic Information, Not My Version, Virtualized System .....	169
Spiking Thread, Main Thread, Message Hooks, Hooked Functions, Semantic Split, Coincidental Symbolic Information and Not My Version.....	180
Stack Trace Collection, Special Process, LPC and Critical Section Wait Chains, Blocked Thread, Coupled Machines, Thread Waiting Time and IRP Distribution Anomaly....	188
ALPC Wait Chains, Missing Threads, Waiting Thread Time and Semantic Process Coupling .....	200
Insufficient Kernel Pool Memory, Spiking Thread, and Data Contents Locality.....	201

Incorrect Stack Trace, Stack Overflow, Early Crash Dump, Nested Exception, Problem Exception Handler and Same Vendor .....	206
PART 5: A Bit of Science and Philosophy.....	213
Memory Systems Language .....	213
Categories for the Working Software Defect Researcher .....	214
Collective Pointer .....	214
Notes on Memoidealism.....	217
Archaeological Foundations for Memory Analysis.....	218
On God and Miracles.....	220
Psychoanalysis of Software Troubleshooting and Debugging .....	221
Ontological and Epistemological Memoidealism .....	222
On Unconscious .....	223
Ruminations on Automated Debugging.....	224
General Memory Analysis .....	225
Notation for Memory and Trace Analysis .....	226
Category Theory and Troubleshooting .....	227
Software Chorography and Chorology: A Definition.....	229
PART 6: Fun with Crash Dumps.....	231
Music for Debugging .....	231
Retry, Abort, Escape.....	231
Debugging Slang.....	232

STUPID.....	232
On the Same Page .....	233
.SYS.....	234
PLOT .....	235
Freedom.....	236
Free Verse .....	237
BCE, BC, and CE .....	238
HCI.....	239
Blog .....	240
Inherit a Fortune .....	241
Dr. Watson’s Observational Patterns.....	242
Memory Dumps in Myths .....	245
Bus Debugging.....	246
Debugging the Debugger (16-bit) .....	247
Dr. DebugLove and Nature.....	249
Sailing Memory Spaces under an RGB Flag.....	253
Don’t Name Your Driver a “Missile” .....	254
Notepad Debugging .....	255
Ianalyze -vostokov .....	263
Contemplating Crash Dumps in Unicode .....	264

Memory Dump Analysis Services Cap and T-Shirt .....	266
Troubleshooting Poem in Six Stanzas .....	267
On the Interpretation of M-Theory.....	268
Check the Name of Your Driver in Reverse .....	269
PART 7: Software Trace Analysis.....	271
Pattern Interaction.....	271
Adjoint Threads, Discontinuity, and Time Delta .....	271
Basic Software PLOTS .....	272
Two Readings of a Software Trace.....	274
CDFMarker Tool .....	276
The Extended Software Trace .....	277
Presenting a Software Story.....	278
Adjoint Threading in Process Monitor .....	279
PART 8: Software Trace Analysis Patterns .....	281
Significant Event.....	281
Time Delta .....	282
Adjoint Thread of Activity .....	283
Trace Acceleration .....	284
Incomplete History.....	286
Background and Foreground Components .....	287

Defamiliarizing Effect .....	290
Anchor Messages .....	293
No Trace Metafile .....	296
No Activity .....	297
Trace Partition .....	299
Truncated Trace .....	301
Diegetic Messages .....	302
False Positive Error .....	303
Guest Component .....	304
Message Change .....	305
Layered Periodization .....	306
PART 9: Models of Software Behaviour .....	311
Multiple Exceptions Pattern .....	311
Memory Leak (Process Heap) Pattern .....	315
Message Hooks Pattern .....	326
Modeling C++ Object Corruption .....	330
PART 10: The Origin of Crash Dumps .....	335
More on Demystifying First-chance Exceptions .....	335
PART 11: Structural Memory Patterns .....	343
Memory Snapshot .....	343

Aggregate Snapshot .....	345
Snapshot Collection .....	346
Memory Region.....	347
Region Boundary.....	348
Memory Hierarchy .....	350
Anchor Region.....	351
PART 12: Memory Visualization .....	353
Memory Map Visualization Tools (Revised).....	353
Decomposing Memory Dumps via DumpFilter .....	355
Can a Memory Dump be Blue? .....	359
Virtual to Physical Memory Mapping.....	360
The Memory Visualization Question .....	363
PART 13: Art.....	375
Sweet Oil of Memory .....	375
Night Sky .....	376
Component Trace.....	377
Ana-Trace-Log-Lyzer and Closed Session .....	378
Computer Memory Gardens .....	380
Debugging Venue.....	381
Inside a Memory File.....	382

Fabric of Memory Dumps .....	383
Race Condition in a Kernel Pool .....	394
Memory Interfaces.....	395
Bleeding Memory.....	396
Picture Frame for Memory Dumps .....	398
Front Cover Glitch .....	399
Chance Exceptions in a Turing Machine.....	400
PART 14: Security and Malware Analysis .....	401
Crash Dumps and Password Exposure .....	401
Crash Dump Analysis of Defective Malware .....	406
PART 15: Miscellaneous .....	411
Native Script Debugging.....	411
Component Heap .....	414
Attached Processes .....	416
User/Kernel Diagramming Styles .....	419
Appendix .....	423
Contention Patterns.....	423
Raw Stack Analysis Scripts .....	424
Crash Dump Analysis Checklist.....	425
Index of WinDbg Commands .....	427

Notes..... 429

About the Author..... 430

Cover Images..... 431