



# MEMORY DUMP ANALYSIS

## VOLUME 3

### REVISED EDITION

DMITRY VOSTOKOV

# Memory Dump Analysis Anthology Volume 3

---

Revised Edition

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

Published by OpenTask, Republic of Ireland

Copyright © 2020 by Dmitry Vostokov

Copyright © 2020 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.

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

OpenTask books are available through booksellers and distributors worldwide. For further information or comments, send requests to [press@opentask.com](mailto:press@opentask.com).

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

ISBN-13: 978-1912636235 (Paperback)

Revision 3.01 (July 2020)

Memory dumps are facts.



## Summary of Contents

|  |     |
|--|-----|
| Preface .....                                  | 17  |
| Acknowledgments .....                          | 19  |
| About the Author .....                         | 20  |
| PART 1: Professional Crash Dump Analysis.....  | 21  |
| PART 2: Crash Dump Analysis Patterns.....      | 77  |
| PART 3: Crash Dump Analysis AntiPatterns ..... | 137 |
| PART 4: Pattern Interaction .....              | 141 |
| PART 5: A Bit of Science and Philosophy.....   | 295 |
| PART 6: Fun with Crash Dumps.....              | 313 |
| PART 7: Software Troubleshooting .....         | 335 |
| PART 8: Software Trace Analysis.....           | 341 |
| PART 9: Software Trace Analysis Patterns ..... | 343 |
| PART 10: The Origin of Crash Dumps.....        | 351 |
| PART 11: Memory Visualization .....            | 367 |
| PART 12: Miscellaneous .....                   | 375 |
| Appendix A.....                                | 383 |
| Appendix B .....                               | 385 |
| Appendix C .....                               | 389 |
| Index of WinDbg Commands .....                 | 391 |

Cover Images..... 394

## Contents

|  |    |
|--|----|
| Preface .....  | 17 |
| Acknowledgments .....                                    | 19 |
| About the Author .....                                   | 20 |
| PART 1: Professional Crash Dump Analysis.....            | 21 |
| Sparse Complete x64 Memory Dumps.....                    | 21 |
| Common Mistakes .....                                    | 24 |
| Not Looking at All Stack Traces .....                    | 24 |
| Dump Analysis on Windows 7.....                          | 28 |
| 32-bit Stack Traces from x64 Complete Memory Dumps ..... | 43 |
| Debugger Log Reading Technique.....                      | 48 |
| Variable Kernel Stack in Vista and W2K8 .....            | 49 |
| Advanced Local Procedure Call WinDbg Extension.....      | 52 |
| !cs vs. !ntsdexts.locks.....                             | 54 |
| Copyright as Timestamp .....                             | 55 |
| NULL Data Pointer Pattern: Case Study .....              | 56 |
| Looking for Abnormal: Case Study.....                    | 60 |
| Raw Stack Dump of All Threads .....                      | 62 |
| Comparative Memory Dump Analysis: CPU Spikes.....        | 63 |



|  |     |
|--|-----|
| Graphical Notation for Memory Dumps .....    | 68  |
| Exception Addresses from Event Logs .....    | 71  |
| The Importance of Symbols .....              | 72  |
| Platformorphism .....                        | 75  |
| PART 2: Crash Dump Analysis Patterns .....   | 77  |
| Data Alignment (Page Boundary) .....         | 77  |
| Multiple Exceptions (Kernel Mode) .....      | 78  |
| C++ Exception .....                          | 84  |
| Deadlock (Mixed Objects, Kernel Space) ..... | 85  |
| Wait Chain (Thread Objects) .....            | 92  |
| Divide by Zero (User Mode) .....             | 96  |
| Wait Chain (LPC/ALPC) .....                  | 97  |
| Insufficient Memory (Physical Memory) .....  | 104 |
| Swarm of Shared Locks .....                  | 107 |
| Process Factory .....                        | 112 |
| Paged Out Data .....                         | 118 |
| Semantic Split .....                         | 120 |
| Pass-Through Function .....                  | 129 |
| NULL Pointer (Data) .....                    | 131 |
| JIT Code (.NET) .....                        | 132 |

|  |     |
|--|-----|
| PART 3: Crash Dump Analysis AntiPatterns .....   | 137 |
| No Question .....  | 137 |
| Missing Space.....   | 138 |
| PART 4: Pattern Interaction .....  | 141 |
| Early Crash Dump, Blocked Thread, Not My Version, and Lost Opportunity.....  | 141 |
| Lateral Damage, Stack Overflow, and Execution Residue .....  | 144 |
| Truncated Dump, Spiking Thread, Not My Version, and Hooked Functions.....  | 149 |
| Stack Trace Collection, Hidden Exception, and NULL Code Pointer.....   | 155 |
| WOW64, Blocked Threads, and Coupled Processes .....  | 160 |
| Invalid Handle, Stack Trace Collection, Multiple Exceptions, Invalid Pointer, Data Alignment on Page Boundary, Dynamic Memory Corruption, and Not My Version | 163 |
| Wait Chain and Spiking Thread .....  | 167 |
| Blocked GUI Thread, Wait Chain, and Virtualized Process.....   | 170 |
| Insufficient Memory, Handle Leak, Wait Chain, Deadlock, Inconsistent Dump, and Overaged System .....   | 175 |
| Memory Leak, Spiking Threads, Wait Chain, High Critical Section Contention, and Module Variety .....   | 181 |
| NULL Code Pointer, Changed Environment, Hooked Functions, and Execution Residue .....  | 196 |
| Swarm of Shared Locks, Blocked Threads, and Waiting Time.....  | 201 |
| Stack Trace Collection, Blocked Thread, and Coupled Processes .....  | 205 |
| Insufficient Memory, Handle Leak, Process Factory, High Contention, and Busy System .....  | 209 |

|   |     |
|---|-----|
| Busy System, Blocked Threads, Wait Chains, and Deadlock .....   | 215 |
| Manual Dump, Dynamic Memory Corruption, Blocked Threads, Stack Trace Collection, Multiple Exceptions, Wait Chains and Deadlock.....                                       | 224 |
| Coupled Processes, Wait chains, Message Box, Waiting Thread Time, Paged Out Data, Incorrect Stack Trace, Hidden Exception, Unknown Component, and Execution Residue ..... | 228 |
| Manual Dump, Wait Chain, Blocked Thread, Dynamic Memory Corruption, and Historical Information .....  | 236 |
| Blocked Threads, Message Box, and Self-Diagnosis.....   | 240 |
| Manual and Early Crash Dump, Stack Trace Collection, Main Thread, Blocked Threads, and Pass-Through Functions .....   | 241 |
| Blocked Thread, Historical Information, Execution Residue, Hidden Exception, Dynamic Memory Corruption, Incorrect Stack Trace, and Not My Version .....                   | 245 |
| Null Data Pointer, Incorrect Stack Trace, Changed Environment, Hooked Functions, and Coincidental Symbolic Information .....  | 248 |
| Heap Corruption, Module Variety, Execution Residue, Coincidental Symbolic Information, and Critical Section Corruption .....  | 255 |
| Stack Trace Collection, Blocked Threads, Pass-Through Functions, and Main Thread .....  | 262 |
| Stack Trace, Invalid Code Pointer, and Hooked Functions.....  | 264 |
| Manual Dump, Virtualized Process, Stack Trace Collection, Multiple Exceptions, Optimized Code, Wild Code Pointer, Incorrect Stack Trace, and Hidden Exception             | 268 |
| Main Blocked Thread, Missing Component, Execution Residue, and Data Contents Locality .....   | 275 |
| Inconsistent Dump, Blocked Threads, Wait Chains, Incorrect Stack Trace, and Process Factory .....   | 279 |

|   |     |
|---|-----|
| Invalid Pointer, Incorrect Stack Trace, Multiple Exceptions, Insufficient Memory, and Memory Leak ..... | 288 |
| PART 5: A Bit of Science and Philosophy.....  | 295 |
| Universal Memory Dump: A Definition.....  | 295 |
| The Source of Intuition about Infinite.....   | 296 |
| Geometrical Debugging .....   | 297 |
| Riemann Programming Language .....  | 299 |
| Is Memory Dump Analysis a Science?.....   | 300 |
| My Dangerous Idea: Parameterized Science .....  | 301 |
| Unique Events and Historical Narratives.....  | 302 |
| Notes on Memoidealism.....  | 303 |
| A Copernican Revolution in Debugging.....   | 305 |
| On Subjectivity of Software Defects .....   | 306 |
| Memory Field Theories of Memuonics .....  | 307 |
| Software Trace: A Mathematical Definition.....  | 308 |
| Quantum Memory Dumps .....  | 309 |
| Chemistry of Virtual Memory .....   | 310 |
| PART 6: Fun with Crash Dumps.....   | 313 |
| Music for Debugging .....   | 313 |
| Bugs Never Disappear .....  | 313 |
| Horrors of Computation.....   | 314 |

|   |            |
|---|------------|
| Passion, Intellect, and Expression .....      | 315        |
| Headphones for Debugging .....                | 316        |
| In the Memory Dump File .....                 | 317        |
| Bugteriology .....                            | 318        |
| Implausible Debugging Book Titles .....       | 319        |
| Build Date Astrology .....                    | 320        |
| Breaking Technical Barrier .....              | 321        |
| Occult Debugging .....                        | 322        |
| The Year of Dump Analysis! .....              | 323        |
| Stack Traces and Poetry .....                 | 324        |
| Debugging Slang.....                          | 326        |
| Memory Dump Analysis Walks .....              | 327        |
| E-Acheri .....                                | 329        |
| The Meaning of DATA .....                     | 330        |
| Irish Government on Dumps .....               | 331        |
| Memory Dumps as Relics .....                  | 332        |
| The Ghost of Adelphi Training Center.....     | 333        |
| <b>PART 7: Software Troubleshooting .....</b> | <b>335</b> |
| I'm RARE.....                                 | 335        |
| To Bugcheck or Not To Bugcheck.....           | 336        |

|  |     |
|--|-----|
| T&D Labyrinth .....                            | 337 |
| Efficient vs. Effective: DATA View .....       | 339 |
| PART 8: Software Trace Analysis.....           | 341 |
| Tracing Best Practices .....                   | 341 |
| Software Narratology: A Definition.....        | 342 |
| PART 9: Software Trace Analysis Patterns ..... | 343 |
| Introduction .....                             | 343 |
| Periodic Error .....                           | 344 |
| Basic Facts .....                              | 345 |
| Circular Trace .....                           | 346 |
| Intra-Correlation .....                        | 347 |
| PART 10: The Origin of Crash Dumps.....        | 351 |
| Hide, Seek, and Dump.....                      | 351 |
| OSMOSIS Memory Dumps .....                     | 353 |
| Tools.....                                     | 356 |
| Crash2Hang.....                                | 356 |
| MTCrash .....                                  | 358 |
| Where did the Crash Dump Come from?.....       | 363 |
| FinalExceptionHandler .....                    | 364 |
| PART 11: Memory Visualization .....            | 367 |

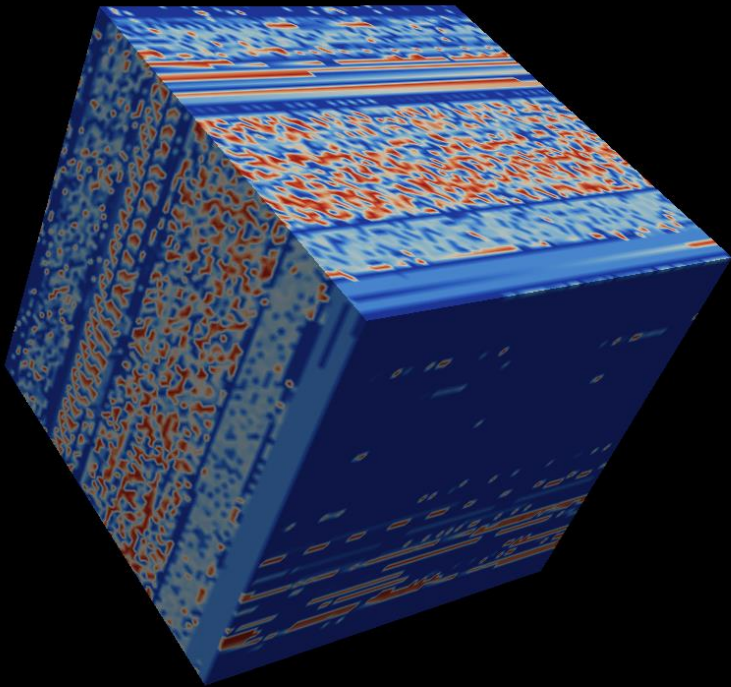
|  |     |
|--|-----|
| The Art of Memory Corruption .....                                 | 367 |
| Visualizing Secondary Storage .....                                | 368 |
| Pictures from Memory Space.....                                    | 369 |
| PART 12: Miscellaneous .....                                       | 375 |
| Hexadecimal/Decimal Chaos.....                                     | 375 |
| The Measure of Debugging and Memory Dump Analysis Complexity ..... | 376 |
| How To Simulate a Process Hang? .....                              | 377 |
| A Windows Case for Delta Debugging.....                            | 378 |
| Sentinel Pointers .....  | 380 |
| Collapsed Stack Trace.....   | 381 |
| Appendix A.....  | 383 |
| Crash Dump File Examples .....                                     | 383 |
| Appendix B .....   | 385 |
| Crash Dump Analysis Checklist.....                                 | 385 |
| Appendix C .....   | 389 |
| Memory Dump Analysis Pattern: A Definition .....                   | 389 |
| Wait Chain Patterns .....  | 389 |
| DLL Link Patterns.....   | 389 |
| Insufficient Memory Patterns .....                                 | 390 |
| Dynamic Memory Corruption Patterns.....                            | 390 |

Deadlock Patterns ..... 390

Index of WinDbg Commands ..... 391

Cover Images..... 394





ISBN 978-1-912636-23-5



9 781912 636235