

Memory Dump Analysis Anthology

Volume 9a

Dmitry Vostokov
Software Diagnostics Institute

Published by OpenTask, Republic of Ireland

Copyright © 2016 by Dmitry Vostokov

Copyright © 2016 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: 978-1-908043-35-1 (Paperback)

First printing, 2016

Table of Contents

Preface	7
About the Author	9
PART 1: Professional Crash Dump Analysis and Debugging	11
When realloc is not a realloc.....	11
WinDbg Shortcut !ddstack	12
PART 2: Crash Dump Analysis Patterns	15
Stack Trace Collection (CPUs)	15
Object Distribution Anomaly (.NET Heap)	19
Stack Trace Surface	22
Hidden Stack Trace	24
Evental Dumps	27
Active Thread (Windows).....	55
Clone Dump	59
Parameter Flow.....	63
Diachronic Module.....	67
PART 3: Pattern Interaction	69
Spiking Thread, Top Module, Module Hint, and Memory Fluctuation	69
PART 4: A Bit of Science and Philosophy	83
Quotes from Memoriarch	83
PART 5: Software Trace Analysis Patterns	85
Ruptured Trace	85
Sequence Repeat Anomaly	88
Adjoint Message	90
Coupled Activities	92
Error Powerset.....	94

Trace Dimension 96
Calibrating Trace 98
Data Interval 99
Identification Messages 101

PART 6: Fun with Debugging, Crash Dumps, and Traces..... 103

Dangerous Words 103
Debugging Slang..... 104

MOAN 104
LOG 104
Diplodoc..... 104
pMud..... 104
HLL 104
Success..... 105
FOOD..... 105
Tor-mented 105
Obsession 105
Literature 105
CLERK 105
Analysis Paralysis..... 106
3D Dump..... 106
Star Wars 106
Daily Standup..... 106

Debugging Curiosities 107

Hung vs. Hanged..... 107
Trace Messages 107
13 107
Similar Cases 107
Error 1917..... 108

Dump2Wave Update 109
Diagnostics and Debugging in Science Fiction 110
Suspicious Volume 9a 111
Music for Debugging 112

<i>Shpongle: Nothing Lasts But Nothing Is Lost</i>	112
PART 7: Linux Core Dump Analysis Patterns	113
NULL Pointer (Data)	113
Stack Trace	114
NULL Pointer (Code)	115
Spiking Thread	116
Dynamic Memory Corruption (process heap).....	118
Execution Residue	119
Coincidental Symbolic Information.....	121
Stack Overflow (user mode)	122
Divide by Zero (user mode).....	124
Local Buffer Overflow	125
C++ Exception	126
Paratext.....	127
Active Thread	129
Lateral Damage	130
Critical Region	131
PART 8: Software Diagnostics, Root Cause Analysis, Debugging	135
Workaround Patterns	135
<i>Axed Data</i>	135
Diagnostics, Forensics, Prognostics: The Copernican Revolution	137
Pattern Repertoire	140
Pattern-Oriented Software Internals: Pattern Paradigms and Software Internals	
Pattern Stack.....	142
Software Diagnostics Canvas	147
Software Traces and Logs as Proteins.....	149
Patterns-Based Root Cause Analysis Methodology	152
Teaching Complex Diagnostic Scenarios with Artificial Debugger (ArtDbg) and Pseudo-Memory Dumps	156
The Scope of Software Diagnostics	159
PART 9: Art and Photography	163

- W - I'M DEBUGGIN' IT® 163
- Coincidental Symbolic Information Pattern..... 164
- Pisa Fault System Model 165
- System Playing Tetris 166
- A Pattern of Zeroes 167
- Abnormal Structure 168
- Control Your Software Emissions! 169
- Component-Based Bug Architecture 170

- PART 10: Miscellaneous..... 171**

- Quotes..... 171
- World Software Diagnostics Day..... 173
- Train Journey 174

- Appendix 175**

- Crash Dump Analysis Checklist 175
- Pattern Changes..... 178

- Index of WinDbg Commands 179**