Memory Dump Analysis Anthology

Volume 11

Dmitry Vostokov
Software Diagnostics Institute

OpenTask

Published by OpenTask, Republic of Ireland

Copyright © 2018 by Dmitry Vostokov

Copyright © 2018 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: 978-1-912636-11-2 (Paperback)

First printing, 2018

Revision 1.0 (October 2018)

Table of Contents

Preface **9**

About the Author **11**

PART 1: Crash Dump Analysis Patterns **13**

System Call 13
Data Correlation (CPU Times) 15
Stack Trace Race 17
Hyperdump 19
Disassembly Ambiguity 24
Hidden Exception (Managed Space) 25
Insufficient Memory (Stack) 28
Exception Reporting Thread 34

PART 2: Software Trace Analysis Patterns **35**

Ultrasimilar Messages 35
Hedges 37
Trace Field 39
Script Messages 41
Working Set 42
Trace Homotopy 44
Signal 45
Renormalization 47
Motivic Trace 48
Significant Interval 50
Random Data 52
Truncated Data 53
Time Scale 55
Trace Sharding 56
Phantom Activity 57

PART 3: Software Diagnostics, Root Cause Analysis, Troubleshooting, and Debugging **59**

The Most Important Skill in Software Diagnostics. 59
Pattern-Oriented Data Analysis Example 61
Diagnostic Operads 63
Mathematical Concepts in Software Diagnostics and Software Data Analysis .. 66
Software Diagnostics Engineering 69
Narrachain 71
Diagnostics-Driven Development 74
Integral Diamathics – Tracing the Road to Root Cause 75
Anolog.io 77
Meso-problem Solving using Meso-patterns 79
Lego Log Analysis 82
Artificial Chemistry Approach to Software Trace and Log Analysis 87

PART 4: Fun with Debugging, Crash Dumps, and Traces 93

Debugging Slang 93

QUICK 93
DREAM 93
DOSE 93
Fex 93
DANCE 94
CORPSE 94
Hi 94
SOS 94
GUT 94
Autopsy 95
FILOsophy and FILOlogy 95
Timesheets and Timeshits 95
Software Logomancy 95
RhaPSODy 95
Developer 96

Diagnostics and Debugging in Science Fiction 97
Russian-English Lexical Connection 98
Defects in Logs 98
A Space Makes a Difference 98
Digital Transformation 98
Pathology 98

Freemallocers 99
Double Layoff 99
Dump in Morse Code 99
Pushkin and Updates 99
Law of Misprints 99
SoftwareLog, MaintainLog, MountainLog 100
Cloud Patches 101
Puree Windows Cooking 102

An Edible CPU Chip 102

Trying on a Sherlock's Hat 103
The Reality is a Matrix 105
Problem Solving Exercises 106
Counting to 10 107
Music for Debugging 107
A Bug Climbs a Book 108
A Computer Crash 109
Traces on Roads 110
Lego Dump Analysis 112

PART 5: Art and Photography 113

Cyberspace Diagnostics 113
Chasing a Beautiful Bug 114
Diagnostics and Poetry 116
Diagnostics in a Wild 117
Interview Preparation Deque 118
Practicing Sorting Algorithms 119
The Open/Closed Principle 120
Microsoft Campus in Redmond 121
Soviet Glasses and Apple Hardware 123
Design/Testing Proportion 124

PART 6: Debugging Dictionary 125

7 125
8 128
Breakpoint 131

Crash 133
Hang 134
Kernel Space 135
Memory Dump 137
Memory Space 138
Physical Memory 139
Thread 140
User Space 141
Virtual Memory 143

PART 7: Tools 145

Dump2Picture Version 2.0 145
Window2Dump 149
WindowHistory 150
WindowHistory Mobile 155
MessageHistory 159
ScreenHistory 161
ProcessHistory 164
Using SSSL Principle to Design Support Tools 165
Repair Clipboard Chain 166
The Inception of Debugging Studio 168
Easter Egg 169

PART 8: Miscellaneous 171

Selected Crashes from My Computers 171
WinDbg Notes 211
Resume and CV as Memory Analysis Artifacts and General Traces 219
Quotes 220
My Road to Modern C++ 222
Algorithms for Breakfast 225
Applying API Wrapper Pattern 229
Clipboard Issues Explained 233
Inside Citrix - November 2006 238
Looking at Software Problems from a Different Angle 243
Me and "Windows NT/2000 Native API Reference" 244

Appendix 245

Curriculum Vitae 245
Resume in WinDbg Style 254
Resume in GDB Style 256
Windows Internals Certificate 258
Dump2Picture 2.2.3 Source Code 259
Dump2Wave 1.3.3 Source Code 262
Window2Dump 1.0 Source Code 265

Index of WinDbg Commands 273