Memory Dump Analysis Anthology

Volume 10

Dmitry Vostokov
Software Diagnostics Institute

OpenTask

Published by OpenTask, Republic of Ireland

Copyright © 2017 by Dmitry Vostokov

Copyright © 2017 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: 978-1-908043-85-6 (Paperback)

First printing, 2017

Revision 1.03 (May 2017)

Table of Contents

Preface 7

About the Author 9

PART 1: Crash Dump Analysis Patterns 11

Quotient Stack Trace 11
Module Stack Trace 12
Foreign Module Frame 13
Unified Stack Trace 16
Mirror Dump Set 18
Memory Fibration 20
Aggregated Frames 21
Value Deviation (Structure Field) 22
Stack Trace (I/O Devices) 24
High Contention (.NET Heap) 26
Frame Regularity 30
Deadlock (.NET Finalizer) 34
Invalid Parameter (Runtime Function) 38
Wait Chain (SRW Lock) 40
Stack Trace Motif 42

PART 2: Linux Core Dump Analysis Pattern 43

Module Stack Trace 43

PART 3: Software Trace Analysis Patterns 45

Corrupt Message 45
Projective Space 47
Ornament 50
Poincaré Trace 52
De Broglie Trace Duality 55
Braid Group 57
Delay Dynamics 59
Activity Quantum 60

Trace Presheaf 61
Message Directory 63
Galois Trace 66
Singleton Trace 68
Braid of Activity 69
Tensor Trace 70
Unsynchronized Traces 72
Intrinsic ID 74
Combed Trace 75
Activity Packet 76

PART 4: Software Diagnostics, Root Cause Analysis, Troubleshooting, and Debugging 77

Topological Software Trace and Log Analysis 77
Is Your Security Healthy? 79
Software Diagnostic Space as a General Graph of Software Narratives 80
Software Diagnostics Metaphors 85

Software Diagnostics as Archaeology 85

Pattern-Oriented Diagnostic Analysis Process 86
Principles of Pattern-Oriented Software Data Analysis 88
Abstract Debugging Commands (ADC) Initiative 91
Reducing Analysis Pattern Complexity via Elementary Analysis Patterns 92
Categorical Foundations of Software Diagnostics 96
Existential Prognostics: Periodic Table of Diagnostic Patterns 98
Software Codiagnostics 100
The Unity of Pattern-Oriented Software Diagnostics 103

PART 5: A Bit of Science, Philosophy, and Religion 105

Quotes from Memoriarch 105
Notes on Memoidealism 105

PART 6: Fun with Debugging, Crash Dumps, and Traces 107

Debugging Slang 107

SCANDAL *107*
WTF *107*
UOP *107*
HOT *107*
HOME *107*
anOS *108*
theOS *108*
TCH *108*
Top NoTCH *108*

Problem Solving Techniques 109

Dissolution *109*

Software Temperature 109
Watson 109
Cosmic Rays in Memory 110
Area 51 113
Measuring Software Diagnostics 114
Cash and Crash 114
Debugging Law 114
Suggested Pool Tags 114
TOR 114
Attitude to Debugging 115
British vs. American Spelling 116
How I Became a Grandmaster 117
Memory Dumps and VAT 117
Updatician 117
Traces of Cyrillic Alphabet 117
Prolific Letter 118
Code and Edoc 118
The Three-Software Vendor Body Problem 118
Modem Troubleshooting and Putin 118
Bugs for Fireworks 119
Critical SnowLOB 120
Apotypomamnimisophobia 121
Schadenfreude of AI 121
Diagnostics and Debugging in Science Fiction 121
The Mozart of Diagnostics 122

Keyboard Problems 124

PART 7: Art and Photography 125

(t)ra(c)in(g) 125
Development Muses 126
Pattern Inside and Outside 127
Between Diagnostic Activities 128
Patched Bug Construction Kit 129
Russian Binary 130
Secret Russian Binary 131
Postanalysm 132

PART 8: Miscellaneous 135

Quotes 135
Is There Any Life Inside Windows? 137
The Condition of My Productivity 138
CyberSpace and the Solution to CyberProblems 139
VAX/VMS Debugging Artefact 141
Observing Patterns of Cloud Structure and Behavior 143

Appendix 145

Crash Dump Analysis Checklist 145

Volume Index 149

Memory Analysis Patterns 149
Trace and Log Analysis Patterns 161

Index of WinDbg Commands 167