

Memory Dump Analysis Anthology

Volume 14

Dmitry Vostokov
Software Diagnostics Institute

Published by OpenTask, Republic of Ireland

Copyright © 2021 by Dmitry Vostokov

Copyright © 2021 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.

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

ISBN-13: 978-1-912636-14-3 (Paperback)

Revision 1.00 (August 2021)

Table of Contents

Preface	6
Acknowledgments	7
About the Author	8
PART 1: Crash Dump Analysis Patterns	9
False Frame	9
Procedure Call Chain	11
C++ Object	12
COM Exception	16
Structure Sheaf	19
Saved Exception Context (.NET)	20
Rough Stack Trace (Managed Space)	25
PART 2: Pattern Interaction	27
Exception Reporting Thread, Stored Exception, Exception Stack Trace, Exception Module, Foreign Module Frame, and Stack Trace Motif	27
PART 3: Software Trace Analysis Patterns	35
Flag	35
Strand of Activity	36
Cord of Activity	37
Text Trace	39
Weave of Activity	41
Multidimensional Message	43
Message Metadata	44
Trace Quilt	46
Feature of Activity	48
Trace Schema	50
Definition Trace	52
Serial Trace	53
Container Trace	55

Trace Join 56

PART 4: Cloud Analysis Patterns..... 57

Introducing Methodology and System of CAPS 57

PART 5: Software Diagnostics, Root Cause Analysis, Troubleshooting, and Debugging 67

The Fractal Nature of Software Traces and Logs 67

General Architecture of Analysis Pattern Networks 68

PART 6: Software Narratology..... 73

Exercises in Tracing Style 73

Prologue..... 73

Literary Theory Terms..... 75

Ab ovo, in medias res, flashback, abridged edition..... 75

Abstract, accent, act, action, adaptation, address 76

PART 7: Fun with Debugging, Crash Dumps, and Traces 79

Reading Capital 79

INSECuriTy..... 79

Desperate AI 79

Imperator 79

Buratino and Security 79

Two Types of Dump Analysis Jobs 79

Debugging Slang..... 80

POET..... 80

ijit..... 80

DREAM..... 80

Logistics 80

Poorrific..... 80

PART 8: Art and Photography.....	81
Chasing a Trace	81
Love of Logs	82
When Anomaly Detection is Your Bread.....	83
Observability of Traces	84
Array[T]	85
Old Card Bookmark.....	86
Cloud Tea Break	87
Fiber Bundle in the Wild	88
 PART 9: A Bit of Science, Philosophy, and Religion.....	 89
Plotinus on Overflow	89
Ereignis and Error.....	90
 PART 10: Miscellaneous	 91
WinDbg Notes.....	91
Quotes	95
My Favorite Category Theory Books (Continuation)	96
Data Pathology.....	101
FP Police.....	102
The Seed of Trace and Log Analysis Patterns.....	103
My Number Theory Book Collection (Continuation)	104
Artifacts for Lockdown.....	110
Books that Influenced Me.....	111
Streaming Architecture of Pattern-Oriented Software Diagnostics Publications	178
 Appendix.....	 179
My IT Reading List in 2006	179
 Index of WinDbg Commands.....	 189