

Software Trace and Log Analysis

Pattern Reference
Second Edition

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: 978-1-908043-82-5 (Paperback)

First printing, 2016

Table of Contents

Preface to the Second Edition	13
Preface	14
About the Author	15
A	17
<i>Abnormal Value</i>	17
<i>Activity Disruption</i>	18
<i>Activity Divergence</i>	20
<i>Activity Overlap</i>	21
<i>Activity Region</i>	23
<i>Activity Theatre</i>	24
<i>Adjoint Message</i>	25
<i>Adjoint Space</i>	27
<i>Adjoint Thread of Activity</i>	30
<i>Anchor Messages</i>	35
B	38
<i>Back Trace</i>	38
<i>Background and Foreground Components</i>	39

<i>Basic Facts</i>	42
<i>Bifurcation Point</i>	43
<i>Blackout</i>	45
<i>Break-in Activity</i>	47
C	48
<i>Calibrating Trace</i>	48
<i>Characteristic Message Block</i>	49
<i>Circular Trace</i>	52
<i>Correlated Discontinuity</i>	53
<i>Corrupt Message</i>	54
<i>Counter Value</i>	55
<i>Coupled Activities</i>	56
D	57
<i>Data Association</i>	57
<i>Data Flow</i>	58
<i>Data Interval</i>	59
<i>Data Reversal</i>	60
<i>Data Selector</i>	62
<i>Declarative Trace</i>	63

	5
<i>Defamiliarizing Effect</i>	64
<i>Density Distribution</i>	66
<i>Dialogue</i>	67
<i>Diegetic Messages</i>	70
<i>Discontinuity</i>	71
<i>Dominant Event Sequence</i>	72
E	73
<i>Empty Trace</i>	73
<i>Error Distribution</i>	74
<i>Error Message</i>	75
<i>Error Powerset</i>	76
<i>Error Thread</i>	77
<i>Event Sequence Order</i>	78
<i>Event Sequence Phase</i>	79
<i>Exception Stack Trace</i>	81
F	83
<i>Factor Group</i>	83
<i>False Positive Error</i>	85
<i>Fiber Bundle</i>	86

<i>Fiber of Activity</i>	88
<i>File Size</i>	89
<i>Focus of Tracing</i>	90
<i>Fourier Activity</i>	91
G	93
<i>Glued Activity</i>	93
<i>Gossip</i>	94
<i>Guest Component</i>	95
H	96
<i>Hidden Error</i>	96
<i>Hidden Facts</i>	97
I	98
<i>Identification Messages</i>	98
<i>Implementation Discourse</i>	100
<i>Impossible Trace</i>	101
<i>Incomplete History</i>	102
<i>Indexical Trace</i>	103
<i>Indirect Facts</i>	104
<i>Indirect Message</i>	105

<i>Inter-Correlation</i>	110
<i>Interspace</i>	112
<i>Intra-Correlation</i>	113
L	116
<i>Last Activity</i>	116
<i>Layered Periodization</i>	117
<i>Linked Messages</i>	120
M	121
<i>Macrofunction</i>	121
<i>Marked Message</i>	122
<i>Master Trace</i>	123
<i>Message Change</i>	124
<i>Message Context</i>	125
<i>Message Cover</i>	126
<i>Message Interleave</i>	127
<i>Message Invariant</i>	128
<i>Message Pattern</i>	129
<i>Message Set</i>	130
<i>Message Space</i>	131

<i>Meta Trace</i>	132
<i>Milestones</i>	133
<i>Missing Component</i>	134
<i>Missing Data</i>	135
<i>Missing Message</i>	136
<i>Motif</i>	137
N	138
<i>News Value</i>	138
<i>No Activity</i>	140
<i>No Trace Metafile</i>	142
O	143
<i>Opposition Messages</i>	143
<i>Original Message</i>	144
P	145
<i>Palimpsest Messages</i>	145
<i>Periodic Error</i>	147
<i>Periodic Message Block</i>	148
<i>Piecewise Activity</i>	149
<i>Pivot Message</i>	151

<i>Punctuated Activity</i>	155
Q	156
<i>Quotient Trace</i>	156
R	157
<i>Recovered Messages</i>	157
<i>Relative Density</i>	158
<i>Resume Activity</i>	159
<i>Ruptured Trace</i>	161
S	163
<i>Sequence Repeat Anomaly</i>	163
<i>Shared Point</i>	164
<i>Sheaf of Activities</i>	165
<i>Significant Event</i>	167
<i>Silent Messages</i>	168
<i>Singleton Event</i>	170
<i>Small DA+TA</i>	171
<i>Sparse Trace</i>	173
<i>Split Trace</i>	174
<i>State and Event</i>	175

<i>State Dump</i>	177
<i>Statement Density and Current</i>	178
<i>Surveyor</i>	180
T	181
<i>Thread of Activity</i>	181
<i>Time Delta</i>	184
<i>Timeout</i>	185
<i>Trace Acceleration</i>	188
<i>Trace Dimension</i>	189
<i>Trace Extension</i>	191
<i>Trace Frames</i>	192
<i>Trace Mask</i>	194
<i>Trace Partition</i>	196
<i>Trace Viewpoints</i>	198
<i>Traces of Individuality</i>	200
<i>Translated Message</i>	201
<i>Truncated Trace</i>	203
U	204
<i>UI Message</i>	204

	11
<i>Use Case Trail</i>	205
V	206
<i>Visibility Limit</i>	206
<i>Visitor Trace</i>	207
<i>Vocabulary Index</i>	208
W	209
<i>Watch Thread</i>	209
Index of Patterns	211
Bibliography	217
Notes	219

[This page intentionally left blank]

Preface to the Second Edition

33 new trace and log analysis patterns have been discovered since the publication of the first edition almost two years ago. Memory Dump Analysis Anthology has also grown to 3,800 pages with the publication of volumes 8b, 9a, and 9b. Significant advances were made in software diagnostics theory that is reflected in the added analysis patterns. This edition also features better index, minor corrections to the patterns from the first edition, and one pattern from the forthcoming volume 10a.

In addition to previous contact details, please also refer to Facebook trace analysis page, DA+TA group, and The Software Diagnostics Group on LinkedIn:

<http://www.facebook.com/TraceAnalysis>

<http://www.facebook.com/groups/dumpanalysis>

<http://www.linkedin.com/groups/8473045>

Preface

The need for this reference book arose when we started working on the next version of “Accelerated Windows Software Trace Analysis” training¹. The previous version was two years old, and Software Diagnostics Institute² had already added 40 more trace and log analysis patterns to their catalog. All of them (almost 100 patterns in total) were scattered among 3,300 pages of various Memory Dump Analysis Anthology volumes (3 – 7, 8a), and a few found only in Software Diagnostics Library³. So we decided to reprint all these patterns and their illustrations in one small book and full color for easy reference. During editing, we also corrected various mistakes.

If you encounter any error, please contact me using this form

<http://www.dumpanalysis.org/contact>

Alternatively, send me a personal message using this contact e-mail:

dmitry.vostokov@dumpanalysis.org

Alternatively, via Twitter @ [DumpAnalysis](#)

About the Author



Dmitry Vostokov is an internationally recognized expert, speaker, educator, scientist and author. He is the founder of pattern-oriented software diagnostics, forensics and prognostics discipline and Software Diagnostics Institute (DA+TA: DumpAnalysis.org + TraceAnalysis.org). Vostokov has also authored more than 30 books on software diagnostics, forensics and problem-solving, memory dump analysis, debugging, software trace and log analysis, reverse engineering, and malware analysis. He has more than 20 years of experience in software architecture, design, development and maintenance in a variety of industries including leadership, technical and people management roles. Dmitry also founded DiaThings, Logtellect, OpenTask Iterative and Incremental Publishing (OpenTask.com), Software Diagnostics Services (former Memory Dump Analysis Services) PatternDiagnostics.com and Software Prognostics. In his spare time, he presents various topics on Debugging.TV and explores Software Narratology, an applied science of software stories that he pioneered, and its further development as Narratology of Things and Diagnostics of Things (DoT). His current area of interest is theoretical software diagnostics.