Software Trace and Log Analysis

Pattern Reference
Second Edition

Dmitry Vostokov
Software Diagnostics Institute

OpenTask

Published by OpenTask, Republic of Ireland

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

First printing, 2016

Table of Contents

[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” training[1]. The previous version was two years old, and Software Diagnostics Institute[2] 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 Library[3]. 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.