

Memory Dump Analysis Anthology

Color Supplement for Volumes 1-3

Dmitry Vostokov

Published by OpenTask, Republic of Ireland

Copyright © 2010 by Dmitry Vostokov

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.

Microsoft, MSDN, Visual C++, Visual Studio, Win32, Windows, Windows Server and Windows Vista are registered trademarks of Microsoft Corporation. Citrix is a registered trademark of Citrix Systems. Other product and company names mentioned in this book may be trademarks of their owners.

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

ISBN-13: 978-1-906717-69-8 (Paperback)

First printing, 2010

Preface	5
Acknowledgements	7
Volume 1	9
<i>Crash Dumps Depicted</i>	9
<i>Crashes Explained</i>	10
<i>X86 Interrupts</i>	13
<i>IRQL_NOT_LESS_OR_EQUAL</i>	20
<i>KERNEL_MODE_EXCEPTION_NOT_HANDLED</i>	25
<i>SYSTEM_THREAD_EXCEPTION_NOT_HANDLED</i>	27
<i>Threads as Braided Strings in Abstract Space</i>	33
<i>Crash Dump Analysis Card</i>	36
<i>Visualizing Memory Dumps</i>	37
<i>Visualizing Memory Leaks</i>	49
<i>Picturing Computer Memory</i>	61
<i>Unicode Illuminated</i>	64
<i>Teaching Binary to Decimal Conversion</i>	65
<i>Reverse Engineering Citrix ThinWire</i>	66
<i>Memory Dump Analysis Using Excel</i>	69
<i>SystemDump</i>	70

Volume 2	73
<i>Stack Trace</i>	73
<i>Memory Search Revisited</i>	75
<i>First-order and Second-order Memory Leaks</i>	83
<i>Memory Analysis Album</i>	88
<i>Thinking Out of the Box</i>	90
<i>Colorimetric Computer Memory Dating</i>	91
<i>Physics of Debugging</i>	93
<i>The Hidden Tomb in Pyramid of Software Change</i>	94
<i>Bugchecks: SYSTEM_SERVICE_EXCEPTION</i>	95
Volume 3	99
<i>Memory Dump Analysis Walks</i>	99
<i>T&D Labyrinth</i>	101
<i>Visualizing Secondary Storage</i>	103
<i>Pictures from Memory Space</i>	104