

Crash Dump Analysis

for System Administrators
(Windows edition)

Thomas Monahan
Dmitry Vostokov

Published by OpenTask, Republic of Ireland

Copyright © 2008 by Thomas Monahan, 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: 978-1-906717-02-5 (Paperback)

First printing, 2008

"Crash dumps are fossils"

Contents

Preface	7
Acknowledgements.....	9
About the Authors	11
Chapter 1: The Origin of Crash Dumps.....	13
Chapter 2: Getting Started	17
Chapter 3: Looking at Operating System Crashes.....	41
Chapter 4: Looking at Application Crashes.....	91
Chapter 5: A Word about Hangs.....	121
Chapter 6: Two Words about Spikes and Leaks.....	141
Chapter 7: Security Considerations.....	161
Appendixes	171
Index.....	175
Notes.....	177

