



Windows Memory Dump Analysis **Accelerated**

Version 5.5

Part 2: Kernel and Complete Spaces

Dmitry Vostokov
Software Diagnostics Services

Published by OpenTask, Republic of Ireland

Copyright © 2022 by OpenTask

Copyright © 2022 by Software Diagnostics Services

Copyright © 2022 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.

Product and company names mentioned in this book may be trademarks of their owners.

OpenTask books and magazines 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: 978-1-912636-08-2 (Paperback)

Revision 5.50 (December 2021)

Contents

About the Author.....	5
Presentation Slides and Transcript.....	7
Practice Exercises	37
Exercise 0: Download, setup and verify your WinDbg or WinDbg Preview installation, or Docker image.....	42
Exercise K1: Analysis of a normal kernel dump (64-bit).....	60
Exercise K2: Analysis of a kernel dump with pool leak (64-bit).....	116
Exercise K3: Analysis of a kernel dump with pool corruption (64-bit)	132
Exercise K4: Analysis of a kernel dump with code corruption (64-bit)	138
Exercise K5: Analysis of a kernel dump with hang I/O (64-bit)	156
Exercise K6: Analysis of a kernel dump with stack overflow (64-bit).....	176
Exercise K7: Analysis of a kernel dump with stack overwrite (64-bit)	190
Exercise C1: Analysis of a normal complete dump (64-bit).....	208
Exercise C2: Analysis of a problem complete dump (64-bit).....	228
Exercise C3: Analysis of a problem complete dump (64-bit).....	262
Exercise C4: Analysis of a problem complete dump (64-bit).....	276
Application Source Code	309
AppA	311
AppB	313
AppC	315
AppE.....	317
AppK	319
Selected Q&A.....	321
Minidump Analysis	347
Scripts and WinDbg Commands	347
Component Identification	350
Raw Stack Data Analysis	355
Symbols and Images	364
Wait Chain (Executive Resources)	367