



# Windows Memory Dump Analysis **Accelerated**

**Version 5.6**

**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](mailto:press@opentask.com).

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

ISBN-13: 978-1-912636-98-3 (Paperback)

Revision 5.60 (June 2022)

## Contents

About the Author.....	5
Presentation Slides and Transcript.....	7
Practice Exercises .....	37
Exercise 0: Download, setup, and verify your WinDbg Preview or WinDbg installation, or Docker image .....	42
Exercise K1: Analysis of a normal kernel dump (64-bit).....	59
Exercise K2: Analysis of a kernel dump with pool leak (64-bit).....	113
Exercise K3: Analysis of a kernel dump with pool corruption (64-bit) .....	128
Exercise K4: Analysis of a kernel dump with code corruption (64-bit) .....	134
Exercise K5: Analysis of a kernel dump with hang I/O (64-bit) .....	151
Exercise K6: Analysis of a kernel dump with stack overflow (64-bit).....	171
Exercise K7: Analysis of a kernel dump with stack overwrite (64-bit) .....	185
Exercise K8: Analysis of a kernel dump with blocked service process (64-bit) .....	192
Exercise C1: Analysis of a normal complete dump (64-bit).....	207
Exercise C2: Analysis of a problem complete dump (64-bit).....	226
Exercise C3: Analysis of a problem complete dump (64-bit).....	260
Exercise C4: Analysis of a problem complete dump (64-bit).....	273
Exercise C5: Analysis of a problem complete dump (64-bit).....	298
Application Source Code .....	313
AppA .....	315
AppB .....	317
AppC .....	319
AppE.....	321
AppK .....	323
ServiceA .....	324
Selected Q&A.....	327
Minidump Analysis .....	353
Scripts and WinDbg Commands .....	353
Component Identification .....	356
Raw Stack Data Analysis .....	361
Symbols and Images .....	370
Wait Chain (Executive Resources) .....	373