



Windows Memory Dump Analysis **Accelerated**

Version 5.5

Part 1: Process User Space

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: 978-1-912636-05-1 (Paperback)

Revision 5.50 (December 2021)

Contents

About the Author.....	5
Presentation Slides and Transcript.....	7
Practice Exercises.....	33
Exercise 0: Download, setup and verify your WinDbg or WinDbg Preview installation, or Docker image.....	38
Exercise P1: Analysis of a normal application process dump (64-bit notepad).....	54
Exercise P2: Analysis of a normal application process dump (32-bit notepad).....	78
Exercise P3: Analysis of a normal application process dump (64-bit Microsoft Edge).....	80
Exercise P4: Analysis of an application process dump (64-bit AppK, no symbols).....	120
Exercise P5: Analysis of an application process dump (64-bit AppK, with application symbols).....	134
Exercise P6: Analysis of an application process dump (AppL, 64-bit).....	140
Exercise P7: Analysis of an application process dump (AppL2, 64-bit).....	154
Exercise P8: Analysis of an application process dump (AppM, 64-bit).....	174
Exercise P9: Analysis of an application process dump (AppN, 64-bit).....	184
Exercise P10: Analysis of an application process dump (AppO, 64-bit).....	198
Exercise P11: Analysis of an application process dump (AppP, 64-bit).....	208
Exercise P12: Analysis of an application process dump (AppR2, 64-bit).....	224
Exercise P13: Analysis of an application process dump (AppA, WOW64).....	254
Exercise P14: Analysis of an application process dump (AppS, 64-bit).....	264
Exercise P15: Analysis of an application process dump (notepad, 32-bit).....	284
Exercise P16: Analysis of an application process dump (notepad, 64-bit).....	290
Exercise P17: Analysis of an application process dump (AppQ, 32-bit).....	298
Exercise P18: Analysis of an application process dump (AppQ, 64-bit).....	312
Exercise P19: Analysis of an application process dump (AppT, 64-bit).....	326
Application Source Code.....	347
AppA.....	349
AppK.....	351
AppL.....	352
AppL2.....	353
AppM.....	354
AppN.....	355
AppO.....	356

AppP.....	358
AppR2.....	359
AppS.....	360
AppQ.....	362
AppT.....	366
Selected Q&A.....	369
Triple Dereference.....	405
Large Heap Allocations.....	408