



Windows Memory Dump Analysis **Accelerated**

Version 5.6

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: 978-1-912636-97-6 (Paperback)

Revision 5.60 (May 2022)

Contents

About the Author	5
Presentation Slides and Transcript.....	7
Practice Exercises.....	33
Exercise 0: Download, setup, and verify your WinDbg Preview or WinDbg installation, or Docker image	38
Exercise P1: Analysis of a normal application process dump (64-bit notepad).....	55
Exercise P2: Analysis of a normal application process dump (32-bit notepad).....	65
Exercise P3: Analysis of a normal application process dump (64-bit Microsoft Edge).....	67
Exercise P4: Analysis of an application process dump (64-bit AppK, no symbols)	91
Exercise P5: Analysis of an application process dump (64-bit AppK, with application symbols).....	101
Exercise P6: Analysis of an application process dump (AppL, 64-bit).....	106
Exercise P7: Analysis of an application process dump (AppL2, 64-bit)	115
Exercise P8: Analysis of an application process dump (AppM, 64-bit).....	129
Exercise P9: Analysis of an application process dump (AppN, 64-bit)	139
Exercise P10: Analysis of an application process dump (AppO, 64-bit).....	149
Exercise P11: Analysis of an application process dump (AppP, 64-bit)	158
Exercise P12: Analysis of an application process dump (AppR2, 64-bit)	170
Exercise P13: Analysis of an application process dump (AppA, WOW64).....	189
Exercise P14: Analysis of an application process dump (AppS, 64-bit)	208
Exercise P15: Analysis of an application process dump (notepad, 32-bit)	230
Exercise P16: Analysis of an application process dump (notepad, 64-bit)	235
Exercise P17: Analysis of an application process dump (AppQ, 32-bit).....	243
Exercise P18: Analysis of an application process dump (AppQ, 64-bit).....	255
Exercise P19: Analysis of an application process dump (AppT, 64-bit).....	265
Exercise P20: Analysis of a service process dump (ServiceA, 64-bit)	280
Application Source Code.....	289
AppA.....	291
AppK.....	293
AppL.....	294
AppL2	295
AppM.....	296
AppN	297
AppO.....	298
AppP.....	300
AppR2.....	301

AppS	302
AppQ.....	304
AppT.....	308
ServiceA.....	310
Selected Q&A	313
Triple Dereference	349
Large Heap Allocations.....	352