



# Windows Memory Dump Analysis **Advanced**

**with Data Structures**

Dmitry Vostokov  
Memory Dump Analysis Services

Published by OpenTask, Republic of Ireland

Copyright © 2012 by OpenTask

Copyright © 2012 by Memory Dump Analysis Services

Copyright © 2012 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.

You must not circulate this book in any other binding or cover and you must impose the same condition on any acquirer.

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 catalogue record for this book is available from the British Library.

ISBN-13: 978-1-908043-34-4 (Paperback)

First printing, 2012

## Contents

Presentation Slides and Transcript.....	5
Practice Exercises .....	10
Exercise 0: Download, setup and verify your WinDbg installation .....	14
Exercise C1: Stack Trace Collection (64-bit) .....	21
Exercise C2: Memory Search (64-bit) .....	45
Exercise C3: Linked Lists (64-bit) .....	61
Exercise C4: Scripting (64-bit).....	96
Exercise C5: Registry (64-bit).....	114
Exercise C6: Module Variables (64-bit) .....	124
Exercise C7: System Objects (64-bit) .....	130
Exercise C8: Network (64-bit).....	139
Exercise C9: Device Drivers (64-bit).....	150
Exercise C10: Window Messaging (64-bit) .....	165
Selected Q&A.....	177