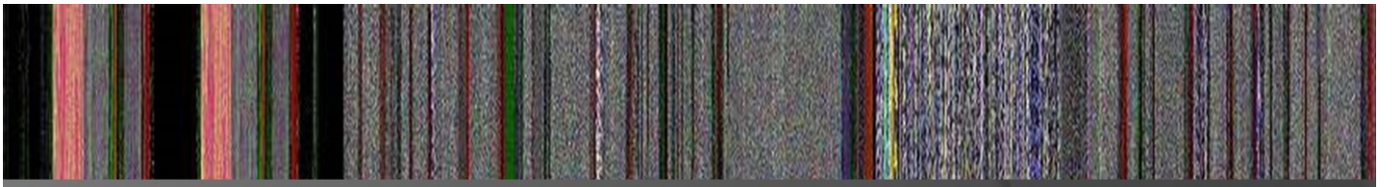

Windows RT Memory Dump Analysis Advanced

ARM Version

Dmitry Vostokov
Software Diagnostics Services

Published by OpenTask, Republic of Ireland

Copyright © 2014 by OpenTask

Copyright © 2014 by Software Diagnostics Services

Copyright © 2014 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.

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

ISBN-l3: 978-1-908043-73-3 (Paperback)

Version 1, 2014

Contents

Presentation Slides and Transcript 5

Practice Exercises 11

Exercise 0 (ARM): Download, setup and verify your WinDbg installation 16

Exercise C1: Stack Trace Collection (ARM) 23

Exercise C2: Memory Search (ARM) 54

Exercise C3: Linked Lists (ARM) 66

Exercise C4: Scripting (ARM) 107

Exercise C5: Registry (ARM) 136

Exercise C6: Module Variables (ARM) 145

Exercise C7: System Objects (ARM) 150

Exercise C8: Network (ARM) 163

Exercise C9: Device Drivers (ARM) 174