2008

WinDbg

A Reference Poster and Learning Cards

OpenTask
in association with
Dmitry Vostokov from DumpAnalysis.org

Published by OpenTask, Republic of Ireland

OpenTask books 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-13: 978-1-906717-29-2 (Paperback)

First printing, 2008

Card command mnemonic colors:

!black - extension

.black - user, kernel and complete space

.blue - user space

.red - kernel space

.green - scripting

Card command descriptions colors:

Black - live and crash dump sessions or extension or scripting

Blue - crash dump analysis only

Red - live debugging only

!acl <address> 1	.apply_dbp	.block	.breakin
.abandon	!acpiirqarb	!amli	!apicerr
!acpiinf	.asm	.bpsync 1	.bugcheck
.allow_exec_cmds	!address	!analyze	!arbinst
!acpicache	.attach	.break	.cache
!finddata	.exptr	!findfilelockowner	.exr
.srcnoisy	.unloadall	.srcpath	.unload
.allow_image_mapping	!ahcache	!apc	!arbiter
!frozen	!wudfext.*	!wsle	!wmitrace.*
!timer	!thread	!teb	!sysptes
!rtlavl	!rsdt	!rpcexts.*	!rellist

Switches to kernel-mode debugging	Groups commands and evaluates aliases	Applies bps to specified CONTEXT	Shows friendly contents of ACL
Shows APIC error log	ACPI Machine Language Interpreter debugger	Shows ACPI IRQ Arbiter structure	Ends debugging session only
Shows bugcheck code and args	Stops all threads upon a breakpoint	Sets format of disassembly output	Shows ACPI configuration and table location
Shows arbiter information	Information about exception or bugcheck	Shows memory region usage and attributes	Enables/ disables g, t and p
Sets the size and memory cache options	Works similar to *break* in C and C++	Attaches to a process	Shows ACPI tables cached by HAL
Shows exception record information	Finds an owner of a file lock	EXCEPTION_POINTERS structure	Shows cached data at a file offset
Unloads a debugging extension	Sets the source file search path	Unloads all extensions	Sets verbosity for source file loads
Shows resource arbiters and their ranges	Shows information about APC	Shows application compatibility cache	Sets module mapping
Event tracing extension	Shows working set list entries	User-mode driver framework extension	Shows the state of processors
Shows formatted system page table entries	Shows formatted thread environment block	Shows ETHREAD and a stack trace	Shows system timers
Shows a PnP relation list	RPC debugging extension	Shows ACPI Root System Description Table	Shows RTL_AVL_TABLE structure