Cheatography

windbg1111 Cheat Sheet

by GA11 via cheatography.com/142828/cs/30680/

符号

.reload /f	.sympath .SRV *C:\sym*http://msdl.microsoft.com/download/symbols/
x modulename!symbolname	search for function or symbols
$iment(module)	entry point of module
!drvobjt <name>	find drive
!devobj <name>	device object
!devhandles <handle>	app using drive

Brakpoints

bp 0x<addr>	set breakpoint at address
bl	brakpoints
bd <#>	disable breakpoint#
bc <#>	clear brakpoint#
be <#>	enable breakpoint #
ba [r|w|e] 0x<addr>	break on [read|write|execute]
bu <symbolname>	break on symbol
sxe ld:dllname	break on module load

Control

g or F5	continue
p or F10	step over
t or F11	step into
Shift + F11	step out
wt	trace and watch
pa or ta 0x<addr>	step to address
pc or tc	step to next call
pt or tt	step to next return
pct or tct	step to next call or return
ph or th	step to next branch
F6 or .attach	attach to process
.detach	detach to process
.restart	retstart
q	quit

Thread

a	~<**a**><b>
*	all threads
.	current threads
<#>	thread ordinal number
b	~<a><**b**>
e	exectue
f	freeze
u	ufreeze
n	supsend
m	resume
empty lists threads	

Dump Structures

k	dump all stack
r	dmp registers
!teb	dump TEB
!peb	dump PEB
!vadump	dump mem pages/info
!heap	dump heap
lm	list loaded modules
ln	list close symbol at memory address
!idt	interrupt descriptor table
dt modulename!symbolname 0x<addr>	dump structure for symbol

CODE

u 0x<addr> L<addr>	disassemble at addr L# instructions

Memory

d* 0x<addr>	
a	ascii chars
u	