Breakpoints / Execution / Exceptions

U .breakin	Break to the Kernel Debugger
U .ecxr	Exception Context Record
U ~F	Freeze Thread
U ~U	Unfreeze Thread
U ~N	Suspend Thread
U ~M	Resume Thread
U ~S	Set Current Thread
U |S	Set Current Process
U ||S	Set Current System
G BA	Break on Access
G BC	Breakpoint Clear
G BD	Breakpoint Disable
G BE	Breakpoint Enable
G BL	Breakpoint List
G BP BU BM	Set Breakpoint
G AH AH(bcdi)	Assertion Handling
G SX SX(DEIN)	Set Exceptions
G !exchain	Exception handler chain
G .exr	Exception Record
G G	Go
G GH	Go with Exception Handled
G Gn GN	Go with Exception Not Handled
G P	Step
G PA	Step to Address
G PC	Step to Next Call
G T	Trace
G TA	Trace to Address
G TB	Trace to Next Branch
G TC	Trace to Next Call
G WT	Trace and Watch Data
G .fiber	Set Fiber Context
G .record_branches	(AMD64) Enable Branch Recording
K !bpid	Cause a process to break
K !ubc	Clear a user-space breakpoint
K !ubd	Disable a user-space breakpoint
K !ube	Enable a user-space breakpoint
K !ubl	Lists all user-space breakpoints
K !ubp	Sets a breakpoint in user space
K .trap	Trap Frame
K ~S	Change Current Processor
K .thread	Set Register Context

Crash Dump

G .dump	Create Dump File
G .dumpcab	Create Dump File CAB
G !analyze -v	Analyze bugcheck
G .opendump	Open Dump File
G !findxmldata	XML from a kernel Small Memory Dump CAB
K .bugcheck	Display Bug Check Data
K .crash	Force System Crash
K .reboot	Reboot Target Computer
K !bugdump	Bug check callback buffers
K .enumtag	Enumerate Secondary Callback Data

Control Flow

G $<	Run Script File
G AD	Delete Alias
G AL	List Aliases
G AS	Set Alias
G J	Execute If - Else
G Z	Execute While
G !for_each_frame	Execute for each frame in the stack
G !for_each_local	Execute for each local variable
G !for_each_module	Execute for each loaded module
G !list	Execute for every element in a linked list

.foreach .do .for .while .if .elsif
.else .catch .break .continue .leave See help :)

Modules / Symbols

G LM	List Loaded Modules
G !chkimg	Detects corruption of images
G !dh	Display the headers of an image
G !dlls	Display list all used modules
G !imgreloc	Original base address of each module
G !lmi	Display information about a module
G !imggp	Global pointer GP for a 64-bit image
G LD	Load Symbols
G .reload /u	Reload Modules
G DT –b –v	Display Type Ex: nt!* nt!_IRP
G LN	List Nearest Symbols
G .fnent	Display Function Data
G LS LSA	List Source Lines
G LSC	List Current Source
G LSF LSF-	Load or Unload Source File
G LSP	Set Number of Source Lines
G Dds DPs DQs	Display Words and Symbols
G L+ L-	Set Source Options
G X /t /v	Examine Symbols Ex: Drv!*g_*
G .exepath	Set Executable Path
G .lines	Toggle Source Line Support
G .open	Open Source File
G .srcnoisy	Noisy Source Loading
G .srcpath .lsrcpath	Set Source Path
G .symfix	Set Symbol Store Path
G .symopt	Set Symbol Options
G .sympath	Set Symbol Path
G !sym	Controls noisy symbol loading and prompts
G !symsrv close	Closes the symbol server client
G .fpo	Control FPO Overrides

Processes and threads

U ||	System Status
U |	Process Status
U ~	Thread Status
U ~E	Thread-Specific Command
U .abandon	Abandon Process
U .attach	Attach to Process
U .childdbg	Debug Child Processes
U .create	Create Process
U .createdir	Set Created Process Directory
U .restart	Restart Target Application
U .ttime	Display Thread Times
U !runaway	Display the time consumed by each thread
U !threadtoken	Thread's impersonation state
U !locks	ntsdexts.dll, process' critical sections
U .tlist	List Process IDs
G .cxr	Display Context Record
G .detach	Detach from Process
G .kill	Kill Process
G !gle	Last error value for the current thread
G !peb	Process environment block PEB
G !teb	Thread environment block TEB
K .context	Set User-Mode Address Context
K .process /p	Set Process Context
K .restart	Restart Kernel Connection
K !process	One or all processes
K !ready	READY threads
K !running	List all running threads
K !sprocess	Session processes
K !thread	Thread
K !zombies	"Zombie" processes or threads
K .tss	Display Task State Segment

Modifications / Memory

U !dphdump	Debug page heap
U !dphfind	Find a debug page heap
U !dphflags	Set or display the global page heap flags
U !dphhogs	Debug page heap hogs
U !vadump	Virtual memory ranges and their protection
U !vprot	Display virtual memory protection
G A	Assemble
G U	Unassemble
G #	Search for Disassembly Pattern
U !igrep	Search for a pattern in disassembly
G C	Compare Memory
G D(ABCdDFPQUW) DY(bd)	Disp Memory
G DdP DPP DQP	Referenced Memory
G E(ABdDFPQUW)	Edit Memory
G F FP	Fill Memory
G M	Move Memory
G S	Search Memory
G .holdmem	Hold and Compare Memory
G .writemem	Write Memory to File
G !heap	Breakpoints, leaks; search for blocks
G !kuser	Shared user-mode page KUSER_SHARED_DATA
K .ignore_missing_pages	Suppress Missing Page Errors
K .pagein	Page In Memory
K !d(bcdpuw)	Data at physical address
K !eb !ed	Write to a physical address
K !pool	Pool(s)
K !poolfind	Find pool tag in nonpaged or paged pools
K !poolused	Memory use, based on the pool tag
K !poolval	Analyzes a pool page and find corruptions
K !frag	Pool memory fragmentation
K !spoolused	Session's paged pool use
K !lookaside	Display or modify look-aside lists
K !sysptes	System page table entries PTEs
K !vm	Virtual memory use statistics
K !vtop	Virtual to physical; page table and directory
K !pfn	Page(s) frame(s) database
K !pte	Adress' page table entry PTE and PDE
K !ptov	Physical-to-virtual map for a process
K !vad	Adress' virtual address descriptor VAD
K !memusage	Physical memory use

OEM Support Tools

http://support.microsoft.com/?kbid&ID=253066
(If needed)

!apc!dpc	Dump APC/DPC or all APCs/DPCs
!ethread/!kthread	Display thread structure
!idt	Dump information about IDT and handlers
!ip	Dissection and dump of IP packets
!kqueue	Display queue of worker thread
!lastlivetime	Display system last live time
!list,!singlelist	Chain display of LIST_ENTRY/SINGLE_LIST_ENTRY
!s	Cool searching capability
!smb	Display SMB structure from header
!stack	Stack analysis
!strct	Dump most structures in ntddk.h
!xpool	Prints maps of pool usage

Console / Help

G ;	Command Separator
G ?	Command Help
G .help	Meta-Command Help
G .hh	Open HTML Help File
G !help	Help for the extension commands
G *	Comment
G N	Set Number Base
G SO	Set Kernel Debugging Options
G SQ	Set Quiet Mode
G SS	Set Symbol Suffix
G Q QQ	Quit
G QD	Quit and Detach
G vercommand	Debugger Command Line
G version	Debugger Version
G vertarget	Target Version
G .asm	Disasm Opt: no_code_bytes ignore_output_width
G .cls	Clear Screen
G .echo	Echo Comment
G .echotimestamps	Show Time Stamps
G .enable_long_status	Enable Long Integer Display
G .enable_unicode	Enable Unicode Display
G .expr /s masm/c++	Choose Expression Evaluator
G .force_radix_output	Use Radix for Integers
G .force_tb	Forcibly Allow Branch Tracing
G .formats	Show Number Formats
G .logappend	Append Log File
G .logclose	Close Log File
G .logfile	Display Log File Status
G .logopen	Open Log File
G .noshell	Prohibit Shell Commands
G .noversion	Disable Version Checking
G .ocommand	Expect Commands from Target
G .ofilter	Filter Output
G .pcmd	Set Prompt Command
G .shell	Command Shell
G .sleep	Pause Debugger
G .time	Display System Time
G .wake	Wake Debugger
G .wtitle	Set Window Title
G .write_cmd_hist [file]	Writes the history to file
K !dbgprint	Previously sent string to the DbgPrint buffer

Hardware

G !cpuid	Processors
G UR	Unassemble Real Mode BIOS
G !psr	(Itanium) Status word PSR
K UX	Unassemble x86 BIOS
K RDMSR	Read MSR
K WRMSR	Write MSR
K !dma	DMA subsystem, and the Driver Verifier
K !ecb !ecd !ecw	Write to the PCI configuration space
K !cbreg	CardBus informations and registers
K !cpuinfo	CPU
K !exca	CardBus ExCA registers
K !fwver	Itanium firmware
K !mca	x86, Machine check architecture MCA registers
K !mca	Itanium, MCA error record
K !mps	BIOS Intel Multiprocessor Specification MPS
K !mtrr	Display the MTRR register
K !pci	Status of the PCI buses and devices attached
K !pcitree	PCI/Cardbus device objects and child buses
K !pcr	Processor's processor Control Region PCR
K !prcb	Display the processor control block PRCB
K !srb	Display a SCSI Request Block SRB
K !urb	Display a USB request block URB
K !wdmaud	WDM Audio WDMAud structures

Informations

U !critsec	CRITICAL_SECTION
U !cs	Critical sections tree
U .closehandle	Close Handle
U !dreg	Registry information
U !evlog	Display, changes, or backs up the event log
U !gatom	Global atom table
U !avrf	Application Verifier and its outputs
G !elog_str	Adds a string to the event log
G !atom	Atom table
G ?	Evaluate Expression
G ??	Evaluate C++ Expression
G !error	Explain an error value
G DS Ds	Display String
G !ustr	UNICODE_STRING
G !str	ANSI_STRING or OEM_STRING
G DV	Display Local Variables
G DG	Display Selector
G R	Registers
G Rm	Register Mask
G K(BDPpV)	Display Stack Backtrace
G DL	Display Linked List
G !slist	Singly-linked list SList
G .frame	Set Local Context
G .lastevent	Display Last Event
G .kframes [N]	Set Stack Length
G !gflag	Set or display the global flags
G !handle	Handle(s)
G !htrace	Stack trace for one or more handles
G !owner	Owner of a module or function
G !obja	Object of Object Manager
G !acl	Access control list ACL
G !sd	Security descriptor
G !sid	Security identifier SID
G !tls	Thread local storage TLS
G !token	Security token object
K !npx	Floating-point register save area
K !dflink	Linked list in the forward direction
K !dblink	Linked list in the backward direction
K .echocpunum	Show CPU Number
K !apc	Asynchronous procedure calls APCs
K !timer	Display all system timer use
K !blockeddrv	List of blocked drivers
K !ca	Control area for the specified section
K !callback	Thread's trap's callback data
K !cmreslist	Device object's CM_RESOURCE_LIST
K !deadlock	Deadlocks found by Driver Verifier
K !defwrites	Variables of the Cache Manager
K !devext	Bus-specific device extension for devices
K !devnode	Node in the device tree
K !devobj	DEVICE_OBJECT
K !devstack	Device stack associated with a device object
K !drvobj	DRIVER_OBJECT
K !drivers	List all drivers loaded with their memory use
K !pnpevent	Plug and Play device event queue
K !rellist	Plug and Play relation list
K !pocaps	Power capabilities
K !popolicy	Power policy
K !diskspace	Free space on a hard disk
K !object	System object
K !qlocks	State of all queued spin locks
K !reg	Display and searches through registry data
K !regkcb	Registry key control blocks
K !session	Controls or display the session context(s)
K !stacks	Kernel stacks
K !vpb	Volume parameter block VPB
K !wsle	Display all working set list entries WSLE
K !arbiter	System resource arbiters and arbitrated range
K !errlog	Pending entries in the I/O system's error log
K !exqueue	Queued items in the ExWorkerQueue work queues
K !filecache	System file cache memory and PTE use
K !filelock	Display a file lock
K !gentable	RTL_GENERIC_TABLE
K !hidppd	HIDP_PREPARSED_DATA
K !bushnd	HAL BUS_HANDLER
K !ioresdes	IO_RESOURCE_DESCRIPTOR
K !ioreslist	IO_RESOURCE_REQUIREMENTS_LIST
K !irp	I/O request packet IRP
K !irpfind	Finds I/O request packets IRP
K !irql	Current interrupt request level IRQL
K !job	job object
K !locks	kdextx86.dll, kdexts.dll, ERESOURCE locks

```
K !lpc              Local procedure call LPC ports and messages
K !verifier         Display the status of Driver Verifier
K !ahcache          Application compatibility cache
```

Misc / Never Used (By me :)

```
U .endsrv           End Debugging Server
G .endpsrv          End Process Server
G .chain            List Debugger Extensions
G .clients          List Debugging Clients
G .load             Load Extension DLL
G .unload           Unload Extension DLL
G .unloadall        Unload All Extension DLLs
G .locale           Set Locale
G .quit_lock        Prevent Accidental Quit
G .remote           (KD or CDB) Create Remote.exe Server
G .remote_exit      (KD or CDB) Exit Debugging Client
G .send_file        Send File
G .server           Create Debugging Server
G .servers          List Debugging Servers
G .setdll           Set Default Extension DLL
K IB ID IW          Input from Port
K OB OD OW          Output to Port
K .cache            Set Cache Size
K .kdfiles          Set Driver Replacement Map
K .secure           Activate Secure Mode
K !processfields    EPROCESS fields
K !tokenfields      TOKEN fields
K !threadfields     ETHREAD fields
CTRL+A              Toggle Baud Rate
CTRL+B              Quit Local Debugger
CTRL+C              Break
CTRL+D              Toggle Debug Info
CTRL+F              Break to KD
CTRL+K              Change Post-Reboot Break State
CTRL+P              Debug Current Debugger
CTRL+R              Re-synchronize
CTRL+V              Toggle Verbose Mode
CTRL+W              Show Debugger Version
U !dp               In ntsdexts.dll, display a CSR process
U !dt               Display information about a CSR thread
G !net_send         Sends a message over LAN
G !version          Display the version for the extension DLL
G !logexts.help     logexts.dll "Windows API Logging Extensions"
G !rpcexts.help     rpcexts.dll "RPCDBG"
K !calldata         Call's performance from the named table
K !vpdd             Process' physical, virtual, content memory
K !ndiskd.help      ndiskd.dll "NDIS"
K !acpikd.help      acpikd.dll "ACPI"
K !gdikdx.verifier Driver Verifier verifying a graphics driver

Debug a piped session:
-k com:pipe,port=\\.\pipe\Name,resets=0 -ee c++ -QSY -QY -W Test
-b -k com:port=com1,baud=115200 -QSY -QY -W Remote

Debugging tools for Windows:
http://www.microsoft.com/whdc/ddk/debugging/default.mspx
```