Windbg command

* Symbols

|  |  |
| --- | --- |
| sympath .SRV\*C::\sym\*http://msdl.microsoft.com.com/download/symbols/ | **.reload /f** |
| !sym noisy |  |

|  |  |
| --- | --- |
| **x modulename!symbolname** | search for function or symbols ; use \* wildcards |
| **$iment(module)** | Entry point of module |
| **!drobj <name>** | Find drive |
| **!devobj <name>** | Device object |
| **!devhandles <handle>** | App using driver |

* breakpoint

|  |  |
| --- | --- |
| **bp 0x<addr>** | Set breakpoint at addr |
| **bl** | Breakpoint |
| **bd<#>** | Disble breakpoint |
| **bc<#>** | Clear breakpoint |
| **be<#>** | Enable breakpoint |
| **ba[r|w|e] 1 0x<addr>** | Break on [read|break|execute] |
| **bu<symbolname>** | Break on symbol |
| **Sxe ld:dllname** | Break on module load |

* control

|  |  |  |  |
| --- | --- | --- | --- |
| Basic |  | T or F11 | Step into |
| G or F5 | Continue | Shift + F11 | Step out |
| P or F10 | Step over | wt | Trace and watch |
| Extra |  | Pt or tt | Setp to next return |
| Pa or ta 0x<addr> | Step to address | Pct or tct | Step to next return|call |
| Pc or tc | Step to next call |  |  |
| Session |  | **.detach** | Detach process |
| F6 or **.**attach | Attach to process | **.** | restart |
| q | quit |  |  |

* thread

|  |  |  |  |
| --- | --- | --- | --- |
| a | ~<a><b> | . | Current thread |
| \* | All thread | <#> | thread number |
| b | Empty list all | u | unfreeze |
| e | execute | n | suspend |
| f | freeze | m | resume |

* dump

|  |  |  |  |
| --- | --- | --- | --- |
| k | Dump all stack | !teb | Dump teb |
| r | Dump registers | !peb | Dump peb |
| !vadump | Dump mem pages/info | lm | List loaded modules |
| !dump heap |  |  |  |

|  |  |
| --- | --- |
| ln <addr> | List closest symbol at memory address |
| !idt | Interrupt descriptor table |
| dt modulename!symbolname 0x<addr> | Dump structure of symbol |

* code

|  |  |
| --- | --- |
| U 0x<addr> L <#> | Disassemble at addr L# instructions |

* memory

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| d\* 0x<addr> | a=ascii chars | U=Unicode | b=byte+ascii | w=word(2b)+ascii |
| d=dword(4b) | c=dword+ascii | q=qword(8b) | b=binary+byte | d=binary+dword |
| s=string struct | S=Unicode str | f=floating point(single precision – 4b | | |
| D=floating point(double precision -8b) | | | | |
|  | | | | |

|  |  |
| --- | --- |
| gflags /i <pocess name> +ust | Add allocation stack for this process |
| !address -summary | Show summery of memory by types |
| !heap -s | Show all heaps |
| !heap -stat -h <heap addr> | Show blocks of specific heap |
| !heap -flt s <block size> | Show addresses of memory blocks of specific size by heap |
| !heap -p -a <usrPtr> | Display allocation call stack for given block user ptr address |

* referncde

|  |  |  |  |
| --- | --- | --- | --- |
| dd\* | dq\* | dp\* | \*determine display |

* linked list

|  |
| --- |
| dl[b] 0x<addr> Max size |

* edit

|  |  |  |
| --- | --- | --- |
| e\* 0x<addr><value> \* | b=yte | w,d,q,f,D,u,a |
| Za=ascii string (Null – terminated) | zu=Unicode string (null – terminated) | |

* search

|  |  |
| --- | --- |
| s –[d|w|b|a] 0x00000000 L?0xffffffff <value | Search size start end value |

* process

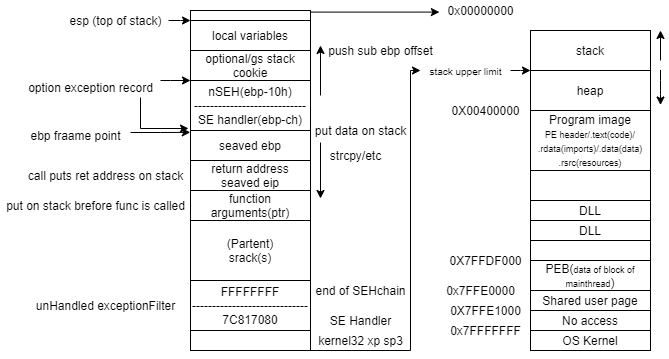
|  |  |
| --- | --- |
| **!process 0 0** | List all process |
| **!process 0 0 cmd.exe** | Find process |
| **!process -1 0** | Current process context |
| **.process /i <addr>** | Switch to usermode process |
| **!token <addr>** | Info about a process token |
| **!pte <addr>** | Convert VA to PA |

lock

|  |  |
| --- | --- |
| !syncblk [-all | <syncblkNumber>] | Show all sync blocks that are owned by the current thread but not thinlocks, use !DumpHeap -thinlock |
| !DumpHeap -thinlock | Show all the thin locks |
| !dlk [-d] | Displays deadlocks between SyncBlocks and/or ReaderWriterLocks, only managed (sosex) |
| !critlist | Get critical sections that threads are locked on (sieextpub) |
| !locks |  |
| !mlocks [-d] | Lists all managed lock objects and CriticalSections and their owning threads (sosex) |
| !mwaits [-d] | Lists all waiting threads and, if known, the locks they are waiting on (sosex) |
| !rwlock [objectAddr | -nd] | Displays all RWLocks or, if provided a RWLock address, details of the specified lock (sosex) |
| dt <lockAddr> |  |
| !handle <handleAddr> f | Show data on the handle, if mutex or event can show the owner (procId.ThreadId) |

Exceptions

|  |  |
| --- | --- |
| !analyze -v [-hang] | -v Very detailed exception data (SLOW), -hang Generates !analyze output. |
| !pe [<exceptionAddr>] | most recent exception data (don’t forget the external stack) |
| !dae | Dump all exception found (psscor) |



remote

|  |  |
| --- | --- |
| .server | Create a debugging server |
| .clients | List debugging clients connected to server |
| .envsrv | End a debugging server |
| .remote | Start a remote.exe server |
| .onshell | Prevent shell commands |