WinDbg Cheat Sheet

1. 일반 명령

자주 쓰는 일반 명령어

r : 레지스터 상태 보기 / 변경

d : 메모리 내용 보기

e : 메모리 내용 변경

bp : 브레이크 포인트 걸기

p, t : 브레이크 포인트가 걸린 다음 명령들을 한 줄씩 수행

대표적 일반 명령어

A(Assemble), U(Unassemble)
BL(Breakpoint List), BC(Breakpoint Clear)
BD(Breakpoint Disable), BE(Breakpoint Enable)
BA(Break on Access)
BP, BU(Set Breakpoint)
D, DA, DB, DW, DD(Display Memory)
Dds(Display Words and Symbols)
DL(Display Linked List) LIST_ENTRY or SINGLE_LIST_ ...
DS, Ds(Display String)
DT(Display Type)
DV(Display Local Variable)
K, KB, KD, KP, KV (Display Stack Backtrace)
E, EA, EB, Ed, EW, EU (Enter Values)
S(Search Memory)
R(Register)
LD(Load Symbol)
LM(List Loaded Symbols)
LN(List Nearest Symbols)
G(Go), P(Step), PC(Step to Next Call)
T(Trace), TB(Trace to Next Branch), TC(Trace to Next Call)
WT(Trace and Watch Data)

2. 메타 명령 (디버거 자체를 제어) (.으로 시작)

자주 쓰는 명령어

.attach : 특정 프로세스를 디버깅할 때 사용

.cls : WinDbg 명령 창에 출력된 모든 내용을 지우기

.sympath : 현재 WinDbg 에 설정된 심볼 경로 확인 / 설정

.reload : 심볼 경로를 설정한 후에 WinDbg 가 심볼을 다시 로드하게 하기

대표적 메타 명령어

.bugcheck (Display Bug Check Data)
.cls (Clear Screen)
.ofilter (Filter Target Output)
.enable_unicode (Enable Unicode Display)
.crash (Force System Crash)
.dump (Create Dump File)
.reboot (Reboot Target Computer)
.cxr (Display Context Record)
.exr (Display Exception Record)
.ecxr (Display Exception Context Record)
.trap (Display Trap Frame)
.exepath (Set Executable Path)
.srcpath (Set Source Path)
.sympath (Set Symbol Store Path)
.symfix (Set Symbol Store Path)
.reload (Reload Module)
.context (Set User-Mode Address Context)
.process (Set Process Context)
.thread (Set Register Context)
.tss (Display Task State Segment)
.load (Load Extension DLL)

3. 확장 명령

자주 쓰는 확장 명령어

!process : 현재 프로세스의 정보를 보거나 현재 윈도우 운영체제에서 실행 중인 모든 프로세스의 정보를 보여주는 명령

!gle : GetLastError 의 약자로 Win32 API 인 GetLastError()와 같이 마지막으로 설정된 Win32 Code 를 보여주는 명령이다.

!error : Win32 Error Code 나 NTSTATUS Code 를 해석해 문자열로 보여주는 명령이다.

!analyze : 덤프 파일을 열었을 때 자동으로 분석을 하는 데 사용하는 명령이다.

대표적인 확장 명령어

!analyze : displays information about the current bug check
!cpuid : displays information about the processors on the system
!error : decodes and displays information about an error value
!gle : displays the last error value for the current thread
!obja : displays the attributes of an object in the object manager
!peb : displays a formatted view of the information in the process environment block(PEB)
!teb : displays a formatted view of the information in the thread environment block (TEB)
!token : displays a formatted view of a security token object
!process : displays information about the specified process or all
!stacks : displays information about the current kernel stacks
!thread : displays summary information about a thread
!zombies : displays all dead ("zombie") processes or threads
!drivers : displays a list of all drivers loaded
!devnode : displays information about a node in the device tree
!devobj : displays detailed information about a DEVICE_OBJECT
!devstack : displays a formatted view of the device stack
!drvobj : displays detailed information about a DRIVER_OBJECT

출처 문헌 : WinDbg 로 쉽게 배우는 Windows Debugging