WinDBG Cheat Sheet

Breakpoint Examples

Set breakpoint at offset in function. Dump bytes (**db**) and ascii chars of address stored in EAX, print stack trace (**kv**) and continue (**gc**).

```
bp gcl!clsPsCommCli::WriteReq + 0x42 "db eax; kv; gc"
```

Dump contents of dereferenced pointer (**poi**) stored at address stored in EBP+18 (**da**) and dump first 98 ASCII characters stored at dereferenced address. Continue (**gc**),

```
bp sloggerclient!hsc_LogMessage + 0xe "da /c 98 poi(ebp+18);gc
```

Set breakpoint (**bp**), print "str_part_1" (**.echo**), then dump value of eax (**r**), continue (**g**).

```
bp 0044ab66 ".echo 'str_part_1'; r ecx; gc"
```

Set breakpoint (**bp**), dump Unicode values at address pointed to by ECX (**du**). Continue (**gc**).

```
bp 0044ab59 "du ecx; gc"
```

Other Commands

Print loaded modules for program that start with the letter s.

```
lm m s*
```

Find all symbols for functions in gcl module:

```
x gcl!*
```

Find all symbols for functions in gcl modules that start with f:

```
x gcl!x*
```

List breakpoints:

```
bl
```

Clear all breakpoints:

```
bc *
```

Clear breakpoint (use bl command to get number):

```
bc <id>
```

Enable / Disable breakpoints:

```
# disable breakpoint
bd <id>

# enabled breakpoint
be <id>
```

Show memory map:

```
!address
```

View threads:

```
!thread
```

View process information:

```
!process
```

Disassemble:

```
# disassemble function
uf <fn name>
```