SETUP

To set windbg as your default post-mortem debugger (run on crash of programs),
simply run windbg from the command line with the -I option:

```
C:\wherever\windbg.exe -I
```

CONTROL FLOW

```
g                   - go / continue / run
p                   - step over
t                   - step into
```

(All further commands also work as ta, tc, tt, tct, th - stepping in insted of over)

```
pa 0xaddress        - step to address
pc                  - step to next call
pt                  - step to next return
pct                 - step to next call or return
ph                  - step to next branching instruction
```

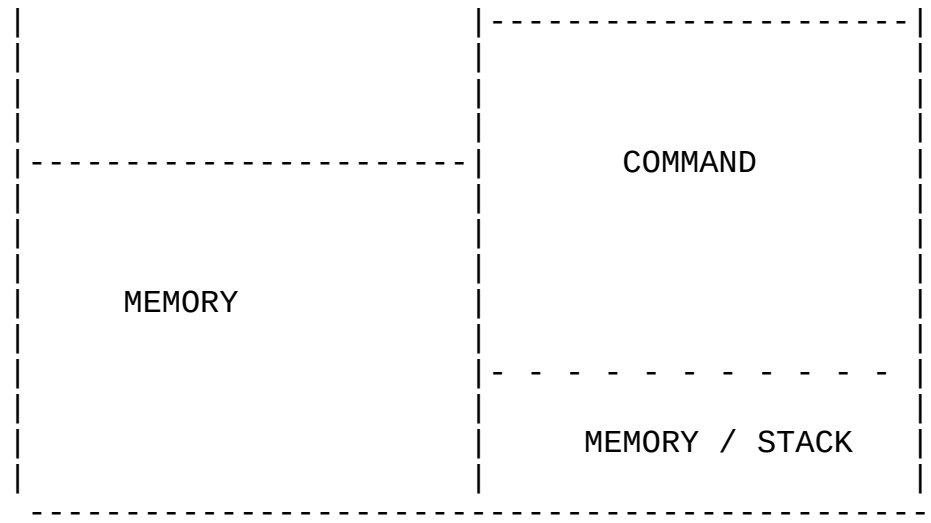
BREAKPOINTS

```
bp 0xaddress            - Set breakpoint
bl                      - List breakpoints
bd num                  - disable breakpoint num
bc num                  - clear breakpoitn num
ba [e|r|w] 1 0xaddress  - break on access [execution|read|write] size address

sxe ld:dllname          - Break on load of module dllname
```

DUMP MEMORY

```
d[d|w|b|a] 0xaddress    - dump [dword|word|byte|ascii] at address
d[d|w|b|a] 0xaddress L5 - option L argument defines how many of them to dump
dd register             - dump contents of a register
ddp 0xaddress           - dump contents of address, and whatever it points to
dda 0xaddress           - dump contents of address, and print the string if it exists
u 0xaddress L5          - disassemble at 0xaddress, L instructions
```

```
------------------------------------------------------
EDIT MEMORY

e[d|w|b] 0xaddress newbytes     - edit memory

------------------------------------------------------
SEARCH MEMORY

s -[d|w|b|a] 0x00000000 L?0xffffffff searchval
                    - first option is size (dword, word, byte,
ascii string)
                    - second option is start address
                    - third option is end address
                    - last option is the value to search for
                        - ex dword: 0x41414141
                        - ex word 0x4241
                        - ex byte ff e3 (can be as many as you
like!)
                        - ex ascii: avacado!

------------------------------------------------------
SYMBOL SETUP -  to dump symbols in C:\sym

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

------------------------------------------------------
DUMP STRUCTURES

!teb                    - dump thread environment block
!peb                    - dump process environment block
!vadump                 - dump list of memory pages and info
!lmi modulename         - dump the info for module modulename
lm                      - show loaded modules
k                       - show call stack
r                       - show registers
dt structName 0xaddress - display a structure in proper format
if you have symbols

------------------------------------------------------
SUGGESTED SETUP

 ---------------------------------------------
|                        |                    |
|                        |                    |
|                        |                    |
|                        |                    |
|    DISASSEMBLY         |       REGISTERS    |
|                        |                    |
```



MEMORY - Virtual: set to esp to show the stack
If you want a generic memdump AND a constant stack, put another memory window under
command - yes, you can have as many as you like

REGISTERS - I usually check both boxes in the configuration - changes show up on top and
in red