OllyDbg Command Line Cheat Sheet

Expressions [expr]	
[CALC/?] expr	Calculate value of expression
expr	Ditto (first character is not letter)
W[ATCH] expr	Add watch
Assignments	
[SET] reg=expr	Writes value of expr to 8/16/32-bit general register
SET memory=expr	Writes to 8/16/32-bit memory
Disassembler	
AT / FOLLOW expr	Follow address in Disassembler
ORIG / *	Go to actual EIP
Assembling	
A expr [,command]	Assemble at address
Dump and stack	
D[UMP] expr	Follow address in dump
DA [expr]	Dump in assembler format
DB [expr]	Dump in hex byte format
DC [expr]	Dump as ASCII text
DD [expr]	Dump as addresses (stack format)
DU [expr]	Dump as UNICODE text
DW [expr]	Dump in hex word format
STK expr	Follow address in stack
Breakpoint commands	
BP expr [,condition]	Set INT3 breakpoint at address
BPX label	Set breakpoint on each call to external 'label' within the current module
BC expr	Delete breakpoint at address
MR expr1 [,expr2]	Set memory breakpoint on access to range
MW expr1 [,expr2]	Set memory breakpoint on write to range
MD	Remove memory breakpoint
HR expr	Set 1-byte hardware breakpoint on access to address
HW expr	Set 1-byte hardware breakpoint on write to address
HE expr	Set hardware breakpoint on execute at address
HD [expr]	Remove hardware breakpoint(s) at address

Labels and comments	
L expr, label	Assign symbolic label to address
C expr, comment	Set comment at address
Tracing commands	
STOP / PAUSE	Pause execution
RUN	Run program
G [expr]	Run till address
GE [expr]	Pass exception to handler and run till address
S / SI	Step into
SO	Step over
T[I] [expr]	Trace in till address
TO [expr]	Trace over till address
TC condition	Trace in till condition
TOC condition	Trace over till condition
TR	Execute till return
TU	Execute till user code
OllyDbg windows	
LOG	View Log window
MOD	View Executable modules
MEM	View Memory window
CPU	View CPU window
CS	View Call Stack
BRK	View Breakpoints window
OPT	Edit options
Miscellaneous commands	
EXIT / QUIT	Close OllyDbg
OPEN [filename]	Open executable file for debugging
CLOSE	Close debugged program
RST	Restart current program
HELP	Show help on command line plugin
HELP OllyDbg	Show OllyDbg help
HELP APIfunction	Show help on API function

Expressions may include constants, registers and memory references and support all standard arithmetical and boolean functions. By default, all constants are hexadecimal. To mark constant as **decimal**, follow it with decimal point.

Examples:

- **AT [EAX+10]** - disassemble at address that is the contents of memory doubleword at address EAX+0x10;
- **BP KERNEL32.GetProcAddress** - set breakpoint on API function. Note that you can set breakpoint in system DLL only in NT-based operating systems;
- **BPX GetProcAddress** - set breakpoint on every call to external function GetProcAddress in the currently selected module;
- **BP 412010,EAX==WM_CLOSE** - set conditional breakpoint at address 0x412010. Program pauses when EAX is equal to WM_CLOSE.