Command line plugin: Preliminary description

Welcome. I'm glad to present you the first version of command line plugin, with very limited capabilities but completely functional. Its source code is free, so you can add any commands and modify functionality of existing. Plugin uses new and undocumented OllyDbg functions. I plan to describe them in details in the next "full" release 1.08. Note that plugin does not work with any OllyDbg version prior to 1.08 (beta 1).

Shortcut for command line plugin: **Alt+F1**. Currently, it supports following commands:

Expressions	
CALC expression	Calculate value of expression
? expression	Ditto
expression (first character is not letter)	Ditto
WATCH expression	Add watch
W expression	Ditto
Disassembler	
AT expression	Follow address in Disassembler
FOLLOW expression	Ditto
ORIG	Go to actual EIP
*	Ditto
Dump and stack	
D expression	Follow address in dump
DUMP expression	Ditto
DA [expression]	Dump in assembler format
DB [expression]	Dump in hex byte format
DC [expression]	Dump as ASCII text
DD [expression]	Dump as addresses (stack format)
DU [expression]	Dump as UNICODE text
DW [expression]	Dump in hex word format
STK expression	Follow address in stack
Assembling	
A expression [,command]	Assemble at address
Labels and comments	
L expression, label	Assign symbolic label to address
C expression, comment	Set comment at address
Breakpoint commands	
BP expression [,condition]	Set INT3 breakpoint at address
BPX label	Set breakpoint on each call to external 'label' within the current module
BC expression	Delete breakpoint at address
MR expression1 [,expression2]	Set memory breakpoint on access to range
MW expression1 [,expression2]	Set memory breakpoint on write to range
MD	Remove memory breakpoint
HR expression	Set 1-byte hardware breakpoint on access to address
HW expression	Set 1-byte hardware breakpoint on write to address
HE expression	Set hardware breakpoint on execute at address
HD [expression]	Remove hardware breakpoint(s) at address

Tracing commands

STOP	Pause execution
PAUSE	Ditto
RUN	Run program
G [expression]	Run till address
GE [expression]	Pass exception to handler and run till address
S	Step into
SI	Ditto
SO	Step over
T [expression]	Trace in till address
TI [expression]	Ditto
TO [expression]	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	Close OllyDbg
QUIT	Ditto
OPEN [filename]	Open executable file for debugging
CLOSE	Close debugged program
RST	Restart current program
HELP	Show this help
HELP OllyDbg	Show OllyDbg help
HELP APIfunction	Show help on API function

Commands are not case-sensitive, parameters in brackets are optional. 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:

- **2+2** - calculate value of this expression;
- **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.

You can find full description of expressions supported by OllyDbg in the OllyDbg help.

How to add new command

To add new command, first you must register it in the array cmdlist[]. Elements of this array are structures of type t_command. First element is the command in uppercase, second element describes its operands. Current version of plugin supports only three types of operands:

A - address expression with value in address. Plugin checks that it points to allocated memory.
a - same as A but optional. If expression is absent, address is set to 0.

V - expression of any type in value. If you expect integer expression, check that value.dtype is DEC_DWORD and use contents of value.u.
v - same as V but optional. If expression is absent, value.dtype is DEC_UNKNOWN and value.u is 0.

S - ASCII string in string, may be empty.

Third element is a constant that will be passed to command procedure, and the fourth one is the address of procedure that executes the command:

```
typedef int t_exefunc(char *answer,ulong parm);
```

If all operands of the recognized command are parsed and estimated correctly, plugin calls this procedure. First argument, answer, is the pointer to string 256 bytes long. Its contents will be displayed in the command line window after command is executed. Second argument is the parameter from cmdlsit[]. If function returns 0, command is considered correct and will be added to the history list.