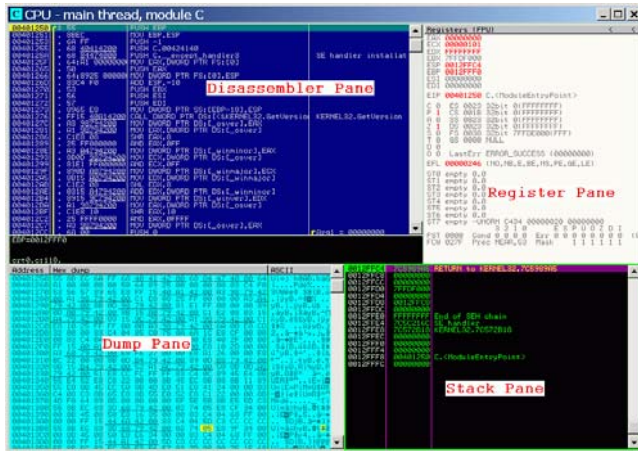


OllyDbg Quick Reference

Author: Jialong He

Jialong_he@yahoo.com

<http://tiger.la.asu.edu>



Introduction

OllyDbg is a machine code level debugger for 32-bit Windows. It is created by Oleh Yuschuk and downloadable from <http://www.ollydbg.de/>

Keyboard Shortcuts

Ctrl + F2	Restart debugged program
F2	Toggle breakpoint at the cursor line
F4 / F9	Run to the cursor / Run continually
F7 / F8	Step into / Step over
Alt + K	Open call stack trace window
Alt + B	Open breakpoint window
Alt + E	Open loaded modules window
Ctrl + A	Analysis code
Ctrl + B	Binary search memory
Ctrl + E	Edit current memory location
Ctrl + R	Find selected address xref
Ctrl + N	Display symbolic name
SPACE	Assemble an instruction

Debug Commands

To open the debug command window, type “**Alt + F1**”.

BP addr, [cond]	Set a break point at a specific address, optionally, specifying a condition. <i>bp 410010, EAX==WM_CLOSE</i> <i>bp Kernel32.GetProcAddress</i>
BPX label	Set a break points on each call to the label <i>Bpx GetwindowtextA</i>
MR addr1 [, addr2] MW addr1 [, addr2]	Set a memory READ/WRITE break point at an address range from [addr1] to [addr2]. <i>mr 041000, 0413ff</i>
MD	Delete memory READ/WRITE break point
HR addr HW addr HE addr HD addr	Set a hardware break point at a given address. HR – read, HW – write, HE – execute HD – remove break point <i>hr 041000</i>
DA addr DB addr DC addr DD addr DU addr	Dump memory content in various formats. DA – assembler DB – hex DC – ASCII DD – Address mode DU – UNICODE
ORIG / *	Set cursor to the current instruction (EIP)
Set reg = expr Set addr = expr	Change a register or memory location to a given value. <i>set EAX = 0</i> <i>set [BP + 2] = 8000001</i>
W expr	Add a watch point. The value of the expression is evaluated at each breakpoint or step. <i>w +[460030+ESI]</i>
A expr [, command]	Assemble at a given address. <i>A 41000, xor eax, eax</i>

Debug Standalone DLL

OllyDbg has the ability to run exported functions in a DLL file. First load the DLL file (press F3 or File -> Open). Then run the DLL file (press F9). This will run the initialization code in the DLL file. Then, from Debug menu, select “Call DLL export”. This will show all exported functions in this DLL file. Select a function you want to run and give correct parameters.