

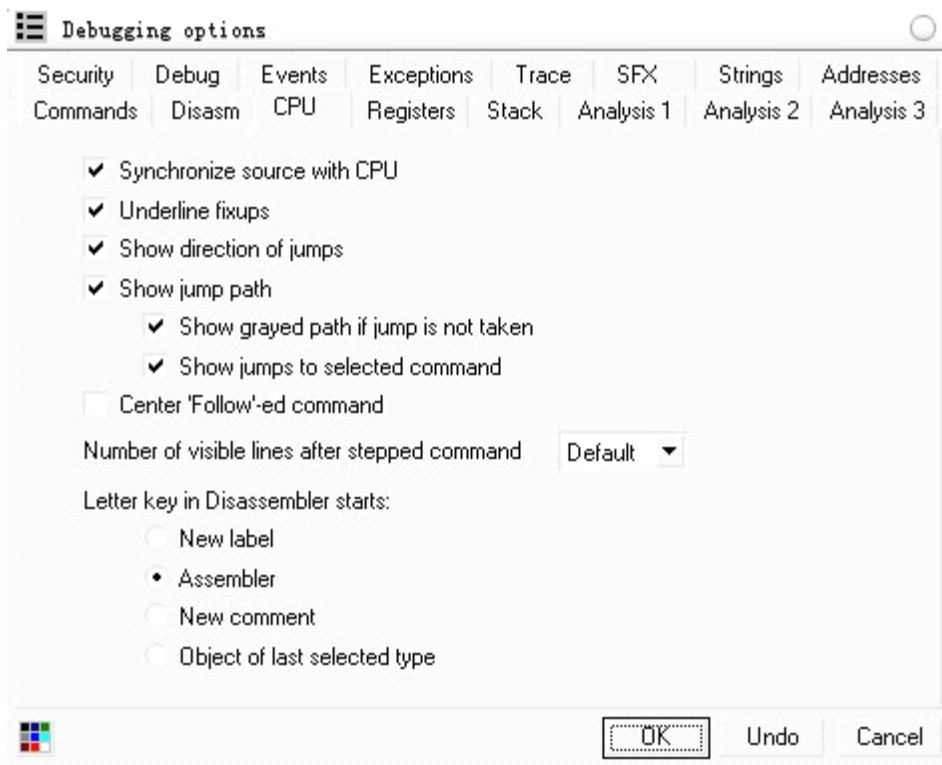
# 使用 **OllyDbg** 调试源代码级 C 程序

[wWw.Begin09.COM](http://wWw.Begin09.COM)  
Review

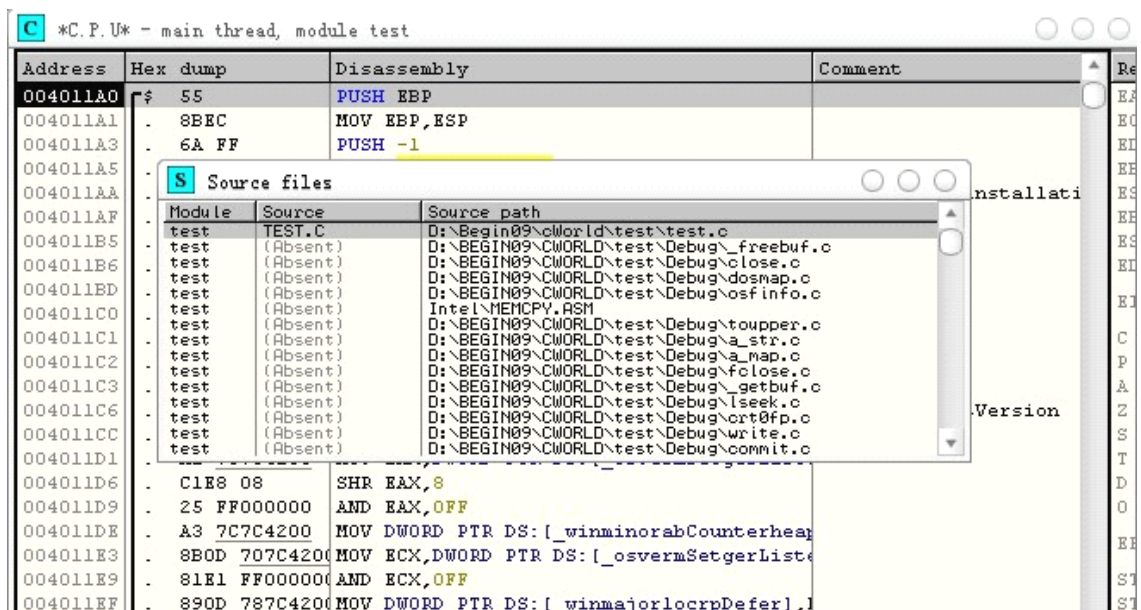


大家都知道 OllyDbg 是支持源代码级调试的，但是具体怎么设置，估计还有一部分人不知道，前两天又翻了翻看雪的《加密解密 3》，按照上面的介绍进行设置，果然很舒服，现在做给大家看看。

1. 首先打开 OllyDbg，检查 Options->debugging options ->CPU 选项卡下的 Synchronize source with CPU 选项是否选中



2. 载入要调试的程序，在 View->Source files 中选择源代码文件



### 3. 打开源代码文件后，就可以先在文件中下断点（F2）

The screenshot shows a debugger window with the following components:

- Disassembly Window:** Lists instructions with their addresses, hex dumps, and assembly mnemonics. The instruction at address 004011A0 is highlighted in blue: `PUSH EBP`.
- Source Code Window:** Shows the C source code for `test.c`. The line `nday = 364;` is highlighted in red, indicating a breakpoint is set there.
- Registers and Memory:** The bottom of the window shows the state of registers and memory addresses (e.g., `00401000` contains `CC CC CC CC CC E9 86 00 00 0`).

### 4. 然后回到 CPU 窗口，在标题栏 Comment 处，点击左键，将在 Comment -- Source -- Profile, 3 个选项中循环，将状态设定到 Source

Address	Hex dump	Disassembly	Source
004011A0	55	PUSH EBP	
004011A1	8BEC	MOV EBP,ESP	
004011A3	6A FF	PUSH -1	
004011A5	68 60214200	PUSH test.00422160	
004011AA	68 50424000	PUSH test.__except_handler31dBLOCK?9?D	
004011AF	64:A1 00000000	MOV EAX,DWORD PTR FS:[0]	
004011B5	50	PUSH EAX	
004011B6	64:8925 00000000	MOV DWORD PTR FS:[0],ESP	
004011BD	83C4 F0	ADD ESP,-10	
004011C0	53	PUSH EBX	
004011C1	56	PUSH ESI	
004011C2	57	PUSH EDI	

5. 现在按 F9，让程序跑起来，look...动人的时刻

Address	Hex dump	Disassembly	Source
00401036	. F3:AE	REP STOS DWORD PTR ES:[EDI]	
00401038	. C745 FC 1C20	MOV DWORD PTR SS:[EBP-4],OFFSET test.??	char * string = "Hello www.Begin09.Com";
0040103F	. C745 F8 6C01	MOV DWORD PTR SS:[EBP-8],16C	nday = 364;
00401046	. 8B45 F8	MOV EAX,DWORD PTR SS:[EBP-8]	nday++;
00401049	. 83C0 01	ADD EAX,1	
0040104C	. 8945 F8	MOV DWORD PTR SS:[EBP-8],EAX	
0040104F	. 8B4D F8	MOV ECX,DWORD PTR SS:[EBP-8]	output(string, nday);
00401052	. 51	PUSH ECX	
00401053	. 8B55 FC	MOV EDX,DWORD PTR SS:[EBP-4]	
00401056	. 52	PUSH EDX	
00401057	. E8 A9FFFFFF	CALL test.00401005	
0040105C	. 83C4 08	ADD ESP,8	
0040105F	. 33C0	XOR EAX,EAX	return 0;
00401061	. 5F	POP EDI	}
00401062	. 5E	POP ESI	
00401063	. 5B	POP EBX	
00401064	. 83C4 48	ADD ESP,48	
00401067	. 3BEC	CMP EBP,ESP	
00401069	. E8 72000000	CALL test._chkespleBuffers@4ingsW@4loc	
0040106E	. 8BE5	MOV ESP,EBP	
00401070	. 5D	POP EBP	

接下来就享受 OllyDbg,带来的美好时光吧！