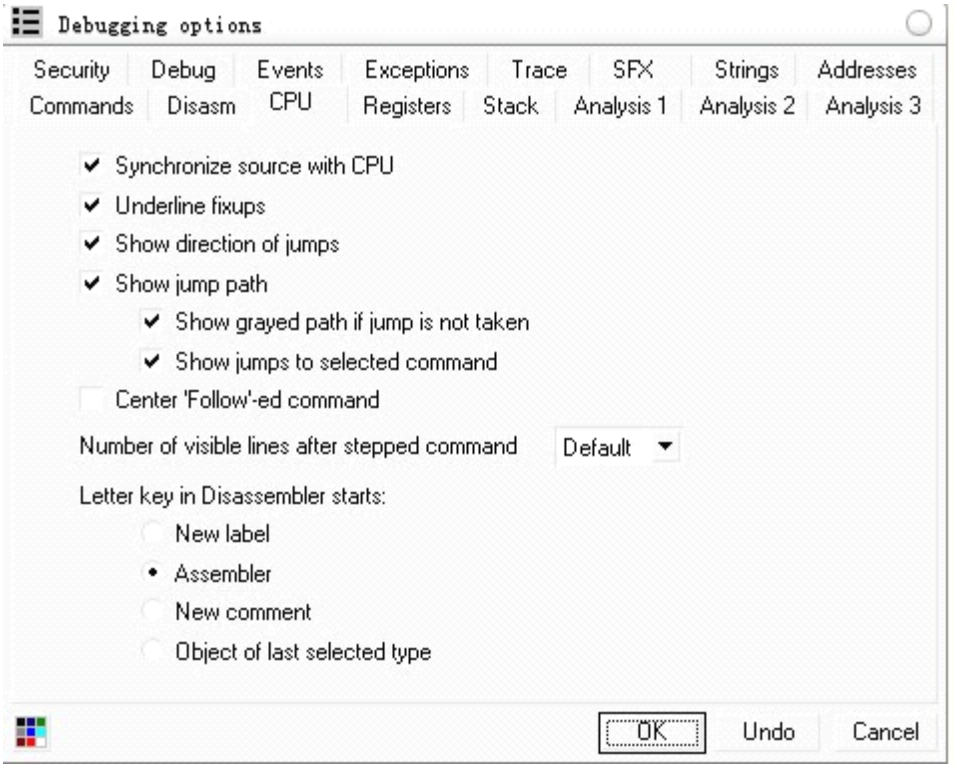
# 使用 OllyDbg 调试源代码级 C 程序

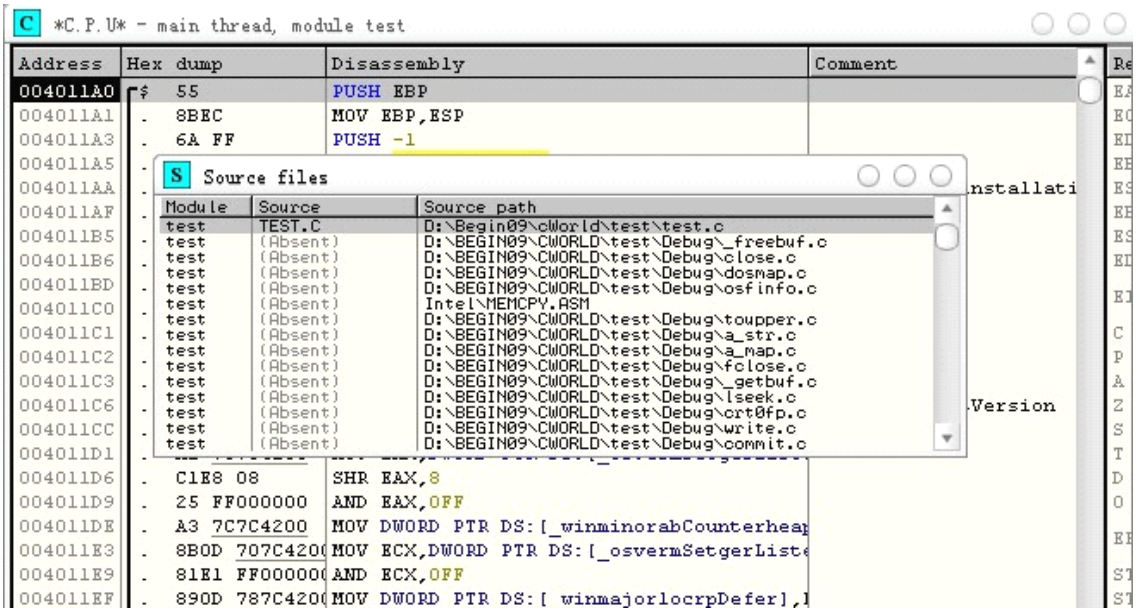
wWw.Begin09.COM
Review

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。

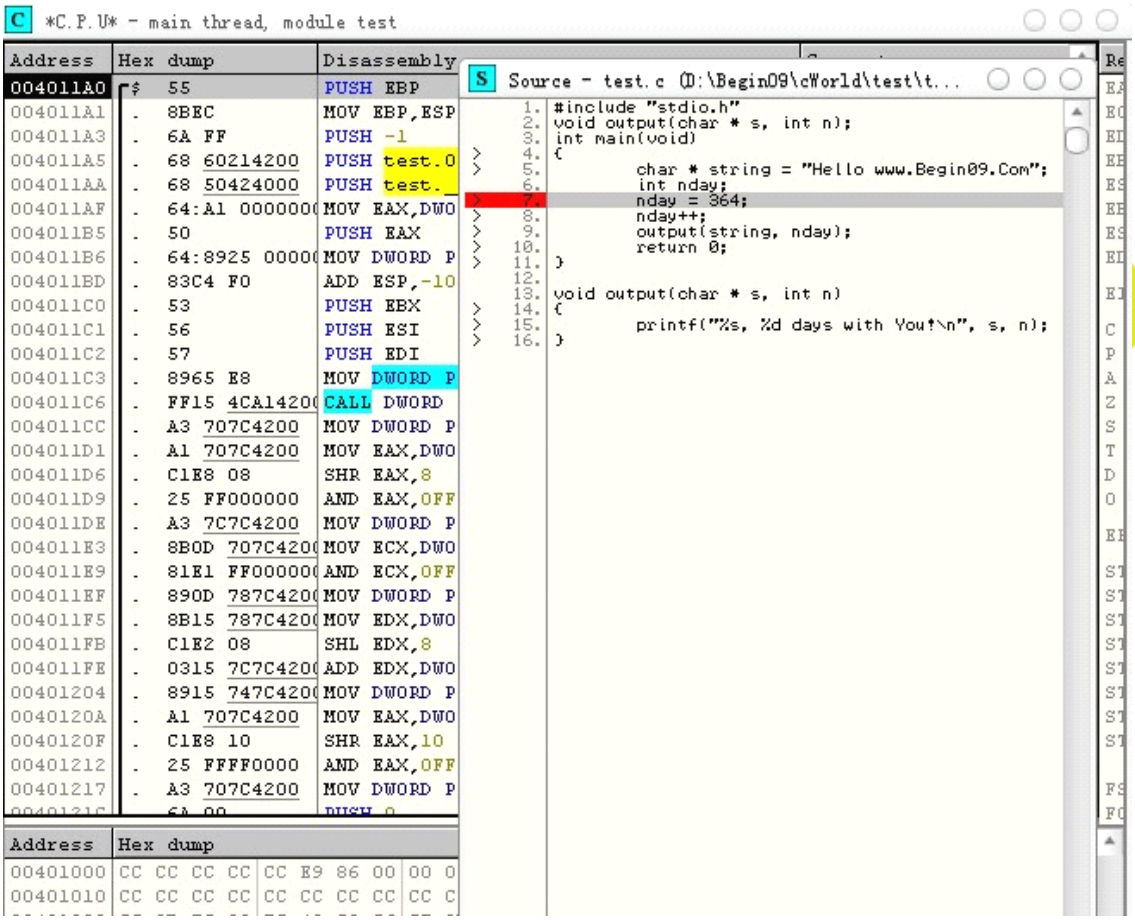
1. 首先打开 OllyDbg，检查 Options->debugging options ->CPU 选项卡下的 Synchronize source with CPU 选项是否选中



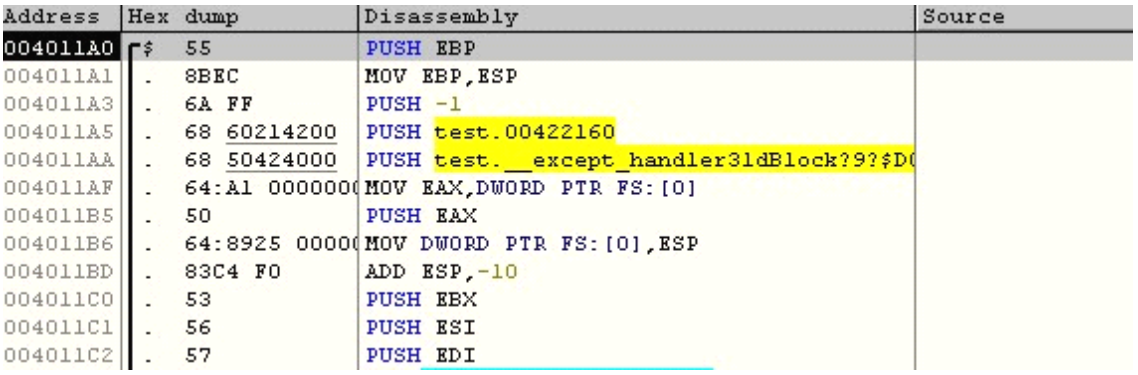

2. 载入要调试的程序，在 View->Source files 中选择源代码文件



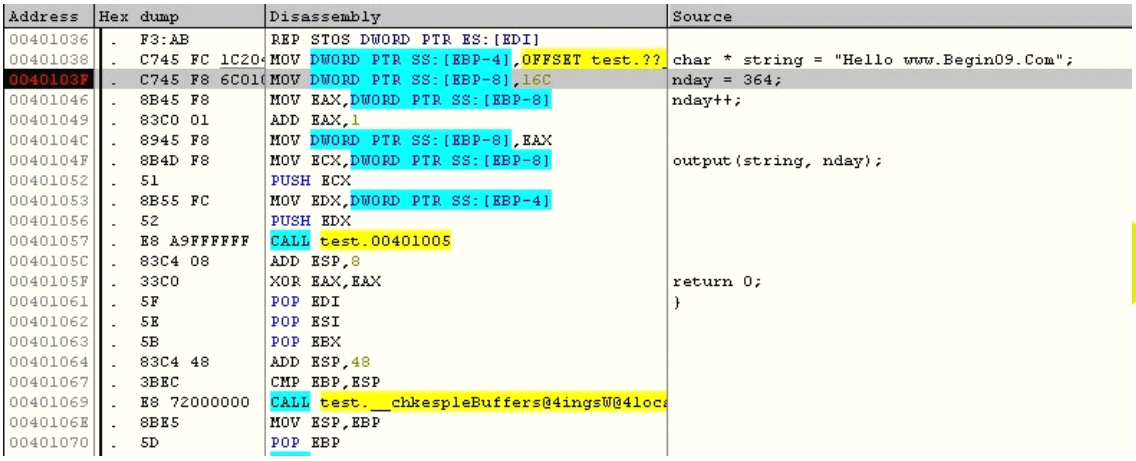
3. 打开源代码文件后，就可以先在文件中下断点（F2）




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



5. 现在按 F9，让程序跑起来，look....动人的时刻



| Address | Hex dump | Disassembly | Source |
|---|---|---|---|
| 00401036 | F3:AB | 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！