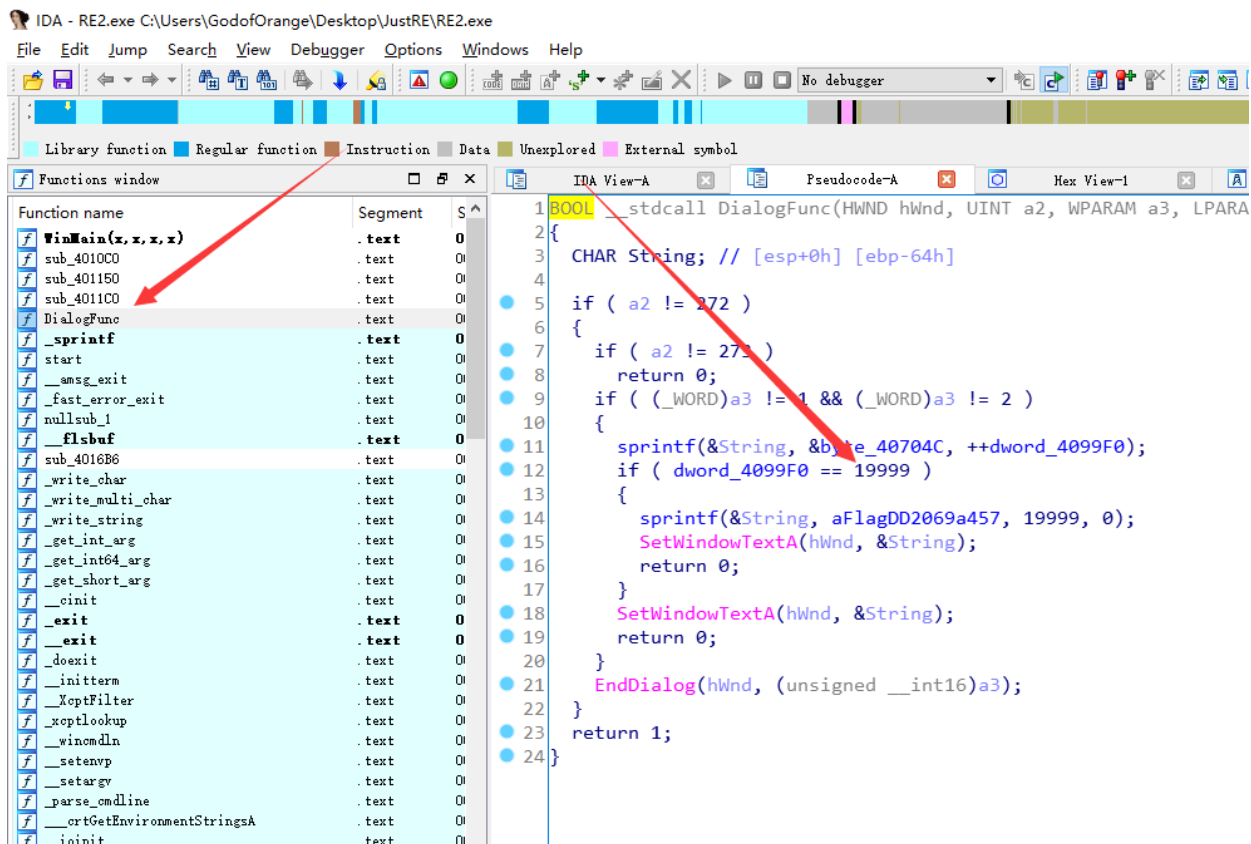
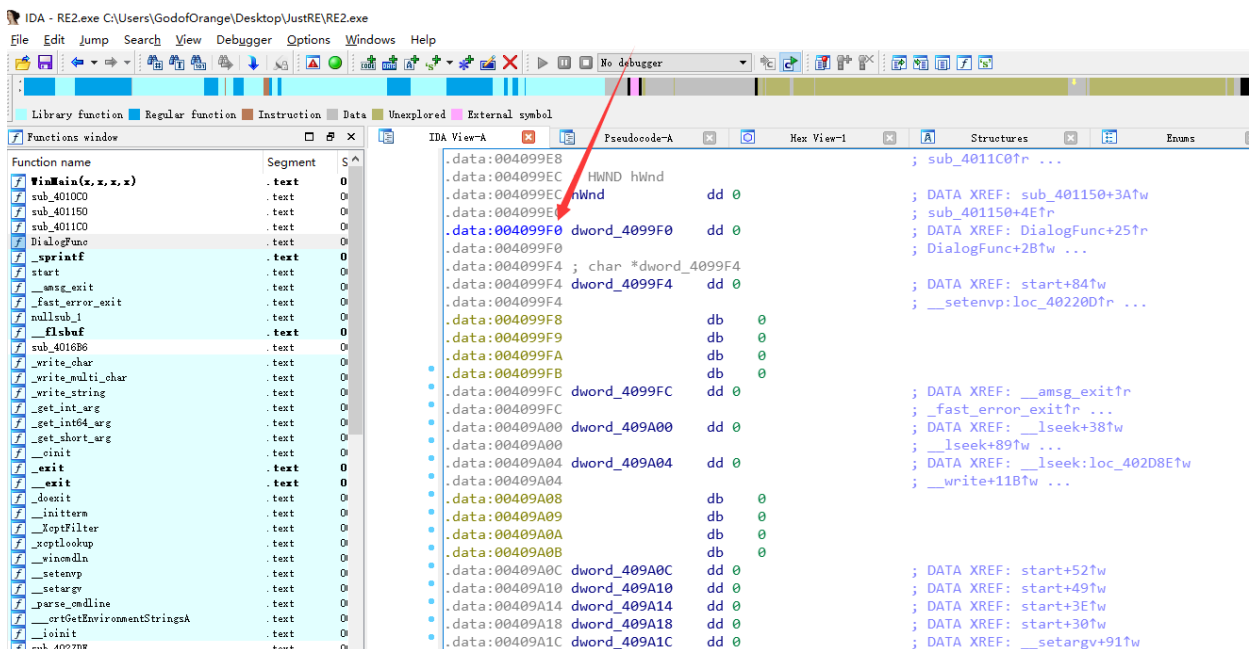


# 1、测试你得手速

## 1、用IDA打开程序



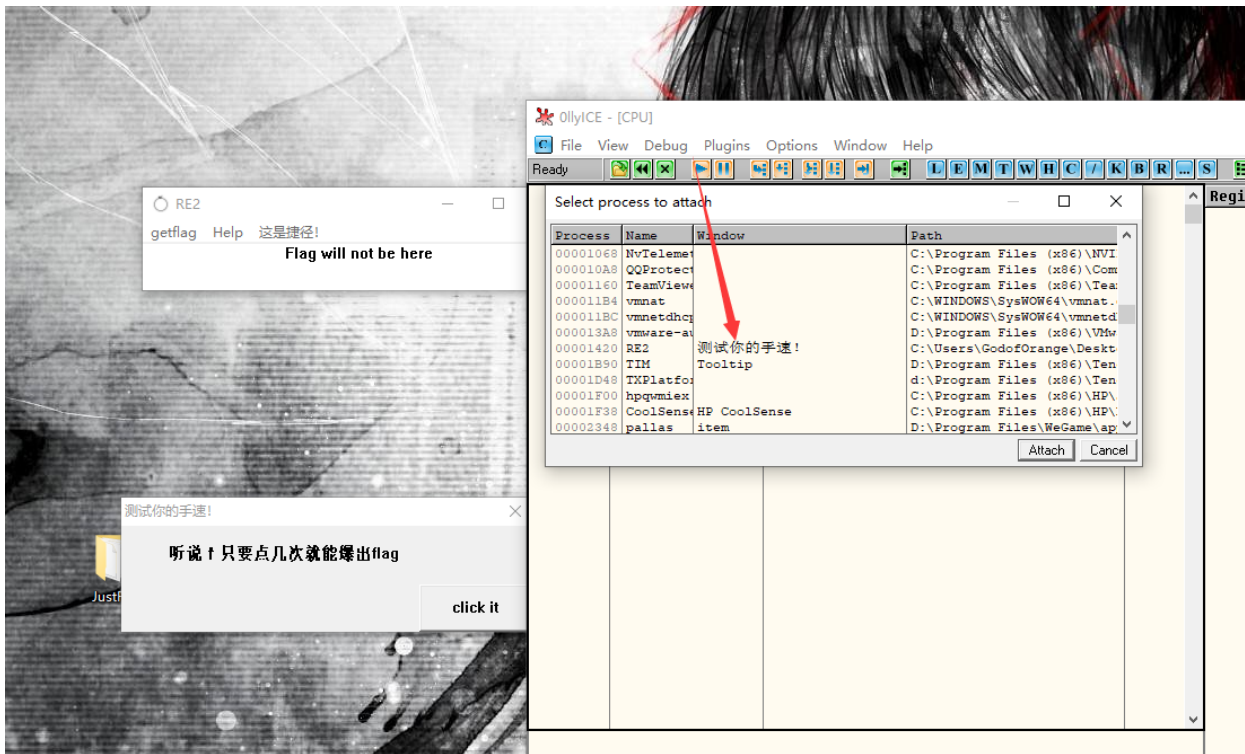
找到单击次数,



获取全局变量地址。

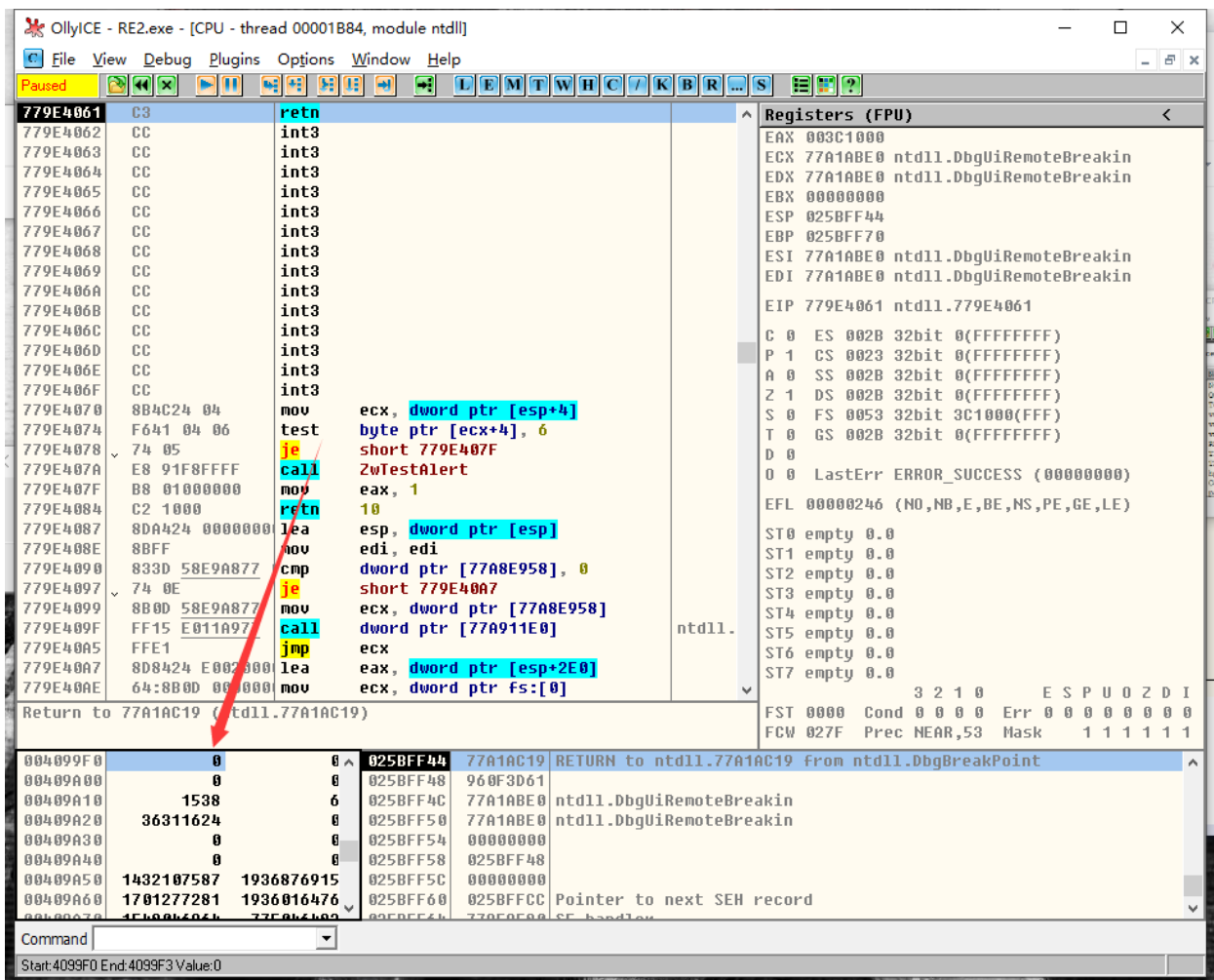
打开程序

打开OllyDbg



attach后在左下角按CTRL+N

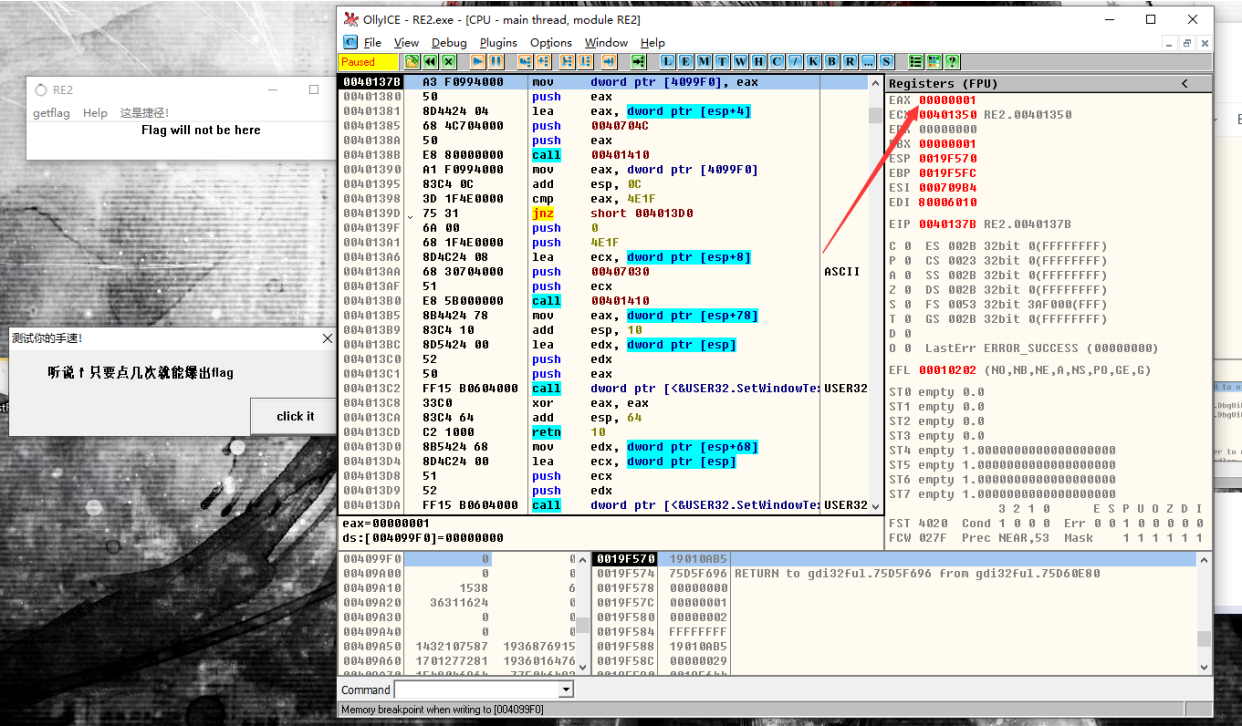
跳到004099F0内存地址



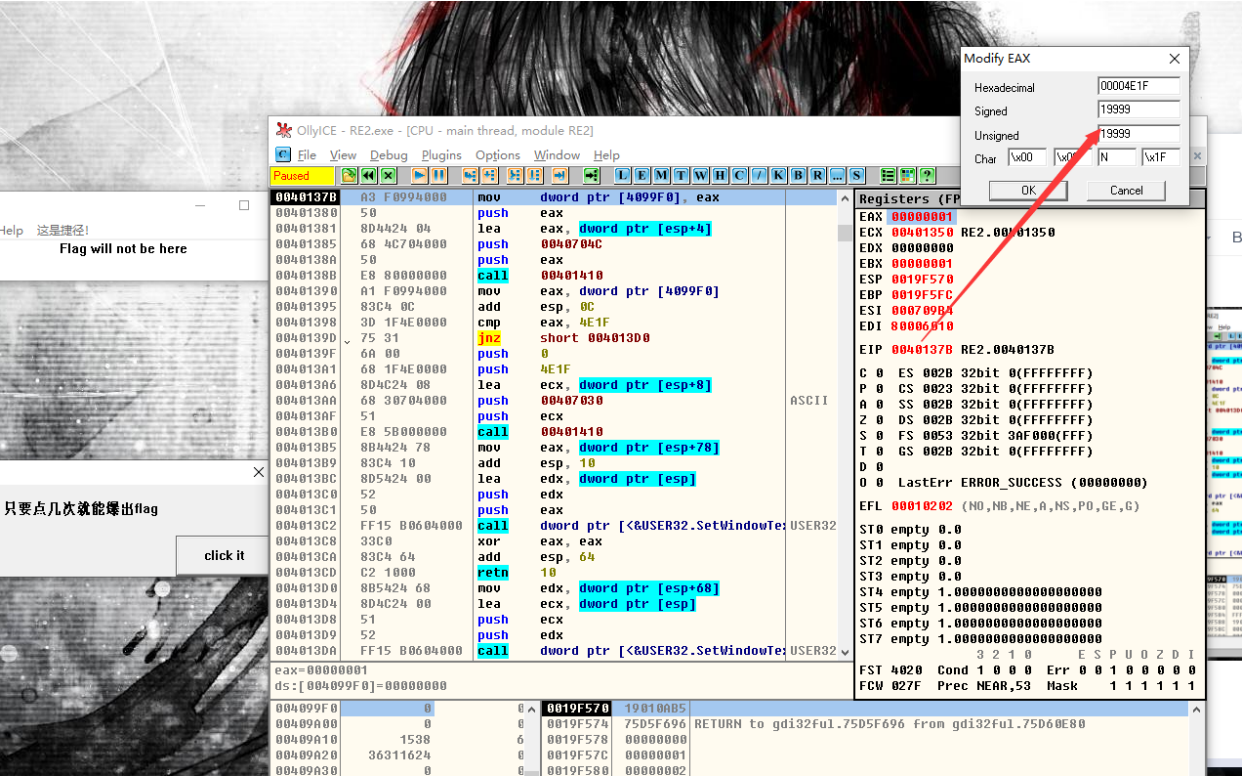
右击下硬件写入断点。

然后按F9运行

然后单击Click



将其改成19999的16进制



然后再摁F9

OlyICE - RE2.exe - [CPU - main thread, module RE2]

File View Debug Plugins Options Window Help

Running

RE2  
getflag Help 这是谁?  
Flag will not be here

flag(1999902069a45792d233ac)

听说！只要点几次就能爆出flag

click it

00401378 A3 F0994000 mov dword ptr [4099F0], eax  
00401380 50 push eax  
00401381 80424 04 lea eax, dword ptr [esp+4]  
00401385 68 4C704000 push 0040704C  
0040138A 50 push eax  
0040138B E8 80000000 call 00401410  
00401390 A1 F0994000 mov eax, dword ptr [4099F0]  
00401395 83C4 0C add esp, 0C  
00401398 3D 1F4E0000 cmp eax, 4E1F  
0040139D 75 31 jnz short 004013D0  
0040139F 6A 00 push 0  
004013A1 68 1F4E0000 push 4E1F  
004013A6 8D4C24 08 lea ecx, dword ptr [esp+8]  
004013AA 68 30704000 push 00407030  
004013AF 51 push ecx  
004013B0 E8 5B000000 call 00401410  
004013B5 8B424 78 mov eax, dword ptr [esp+78]  
004013B9 83C4 10 add esp, 10  
004013BC 8D5424 00 lea edx, dword ptr [esp]  
004013C0 52 push edx  
004013C1 50 push eax  
004013C2 FF15 B0604000 call dword ptr [&USER32.SetWindowTe: USER32  
004013C6 33C0 xor eax, eax  
004013CA 83C4 64 add esp, 64  
004013CD C2 1000 ret 10  
004013D0 8B5424 68 mov edx, dword ptr [esp+68]  
004013D4 8D4C24 00 lea ecx, dword ptr [esp]  
004013D8 51 push ecx  
004013D9 52 push edx  
004013DA FF15 B0604000 call dword ptr [&USER32.SetWindowTe: USER32  
004099F0 0 0 0010F570 190100B5  
004099A0 0 0 0019F574 75D5F696 RETURN to gdi32fu1.75D5F696 from gdi32fu1.75D60E8  
00409910 1538 6 0019F570 00000000  
00409A20 36311624 6 0019F57C 00000001  
00409A30 0 0 0019F580 00000002  
00409A40 0 0 0019F584 FFFFFFFF  
00409A50 1432107587 1936876915 0019F588 190100B5  
00409A60 1701277281 1936016476 0019F58C 00000029  
00409A70 4740817047 77F04400 0019F588 0010F588  
00409A80 77F04400 0010F588 0010F588 0010F588

Registers (FPU)  
EAX 00004E1F  
ECX 00401350 RE2.00401350  
EDX 00000000  
EBX 00000001  
ESP 0019F570  
EBP 0019F5FC  
ESI 000709B4  
EDI 80006010  
EIP 0040137B RE2.0040137B  
C 0 ES 002B 32bit 0(FFFFFFFF)  
P 0 CS 0023 32bit 0(FFFFFFFF)  
A 0 SS 002B 32bit 0(FFFFFFFF)  
Z 0 DS 002B 32bit 0(FFFFFFFF)  
S 0 FS 0053 32bit 3AF000(FE)  
T 0 GS 002B 32bit 0(FFFFFFFF)  
D 0  
O 0 LastErrr ERROR\_SUCCESS (EFL 00010202 (NO,NB,NE,A,NS,  
ST0 empty 0.0  
ST1 empty 0.0  
ST2 empty 0.0  
ST3 empty 0.0  
ST4 empty 1.0000000000000000  
ST5 empty 1.0000000000000000  
ST6 empty 1.0000000000000000  
ST7 empty 1.0000000000000000  
3 2 1 0  
FST 4020 Cond 1 0 0 0 Err  
FCW 027F Prec NEAR,53 Mask

Command