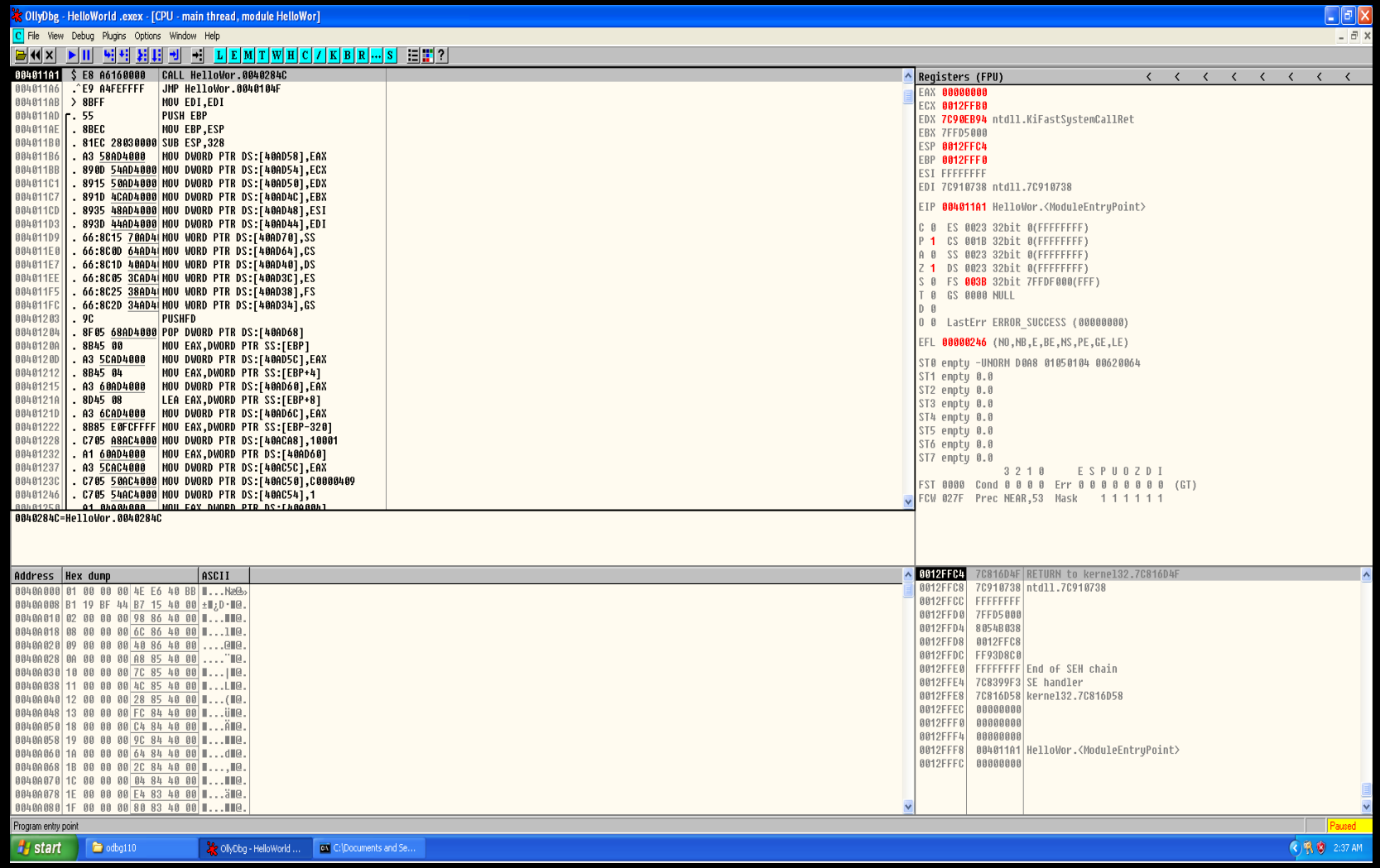
Ollydbg로

텍스트 박스 내용을

내가 원하는

문장으로

바꾸기

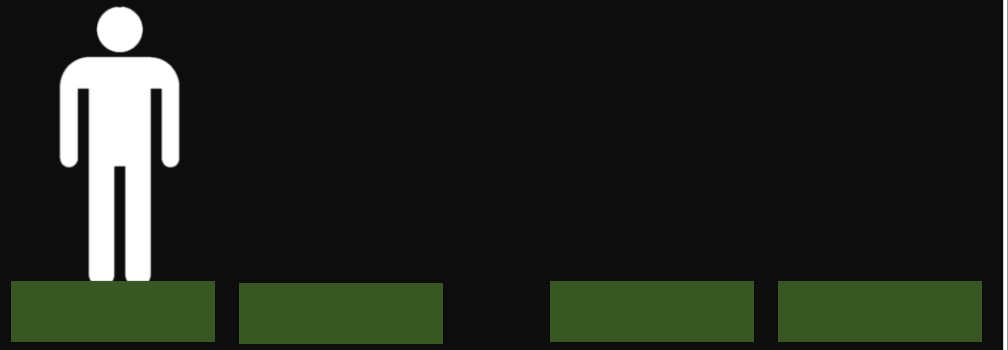


Call : 함수로 이동

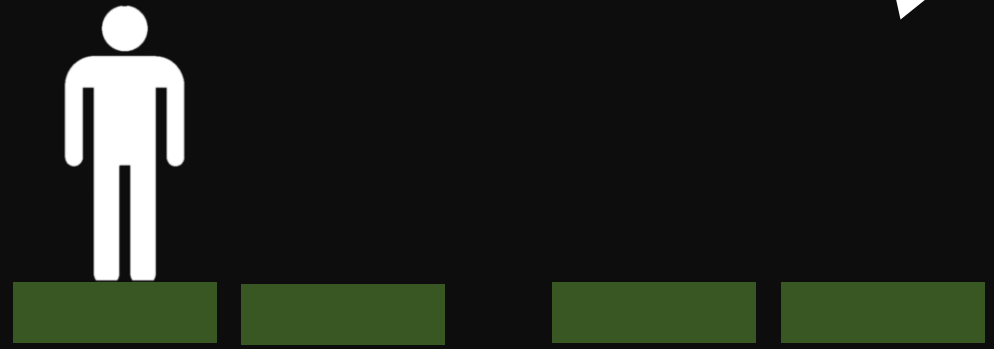
JMP: 함수로 이동

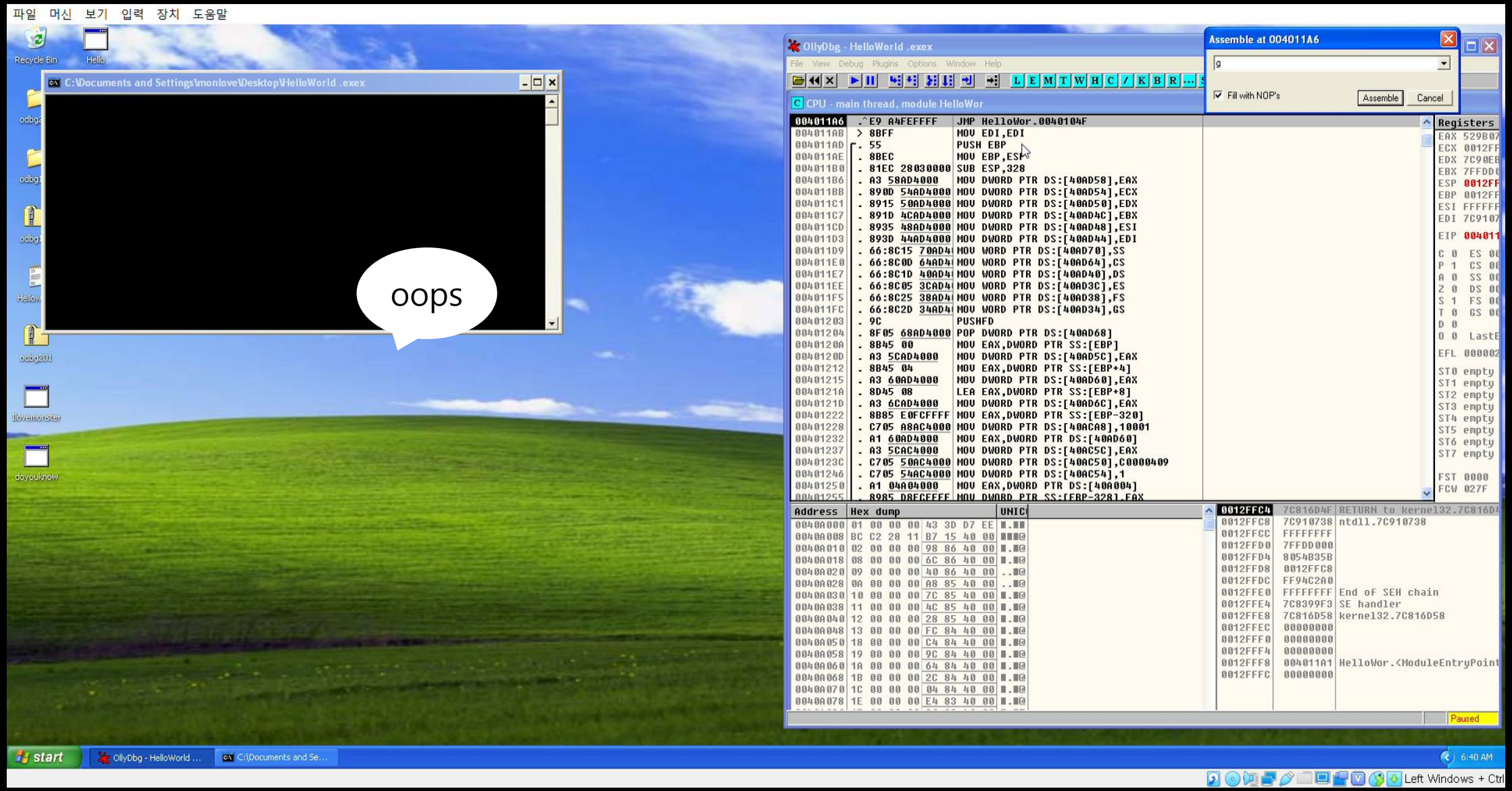
```c
#include "windows.h"

int main(int argc, char* argv[])
{
    MessageBox(NULL,
               L"Hello World!",
               L"www.reversecore.com",
               MB_OK);

    return 0;
}
```

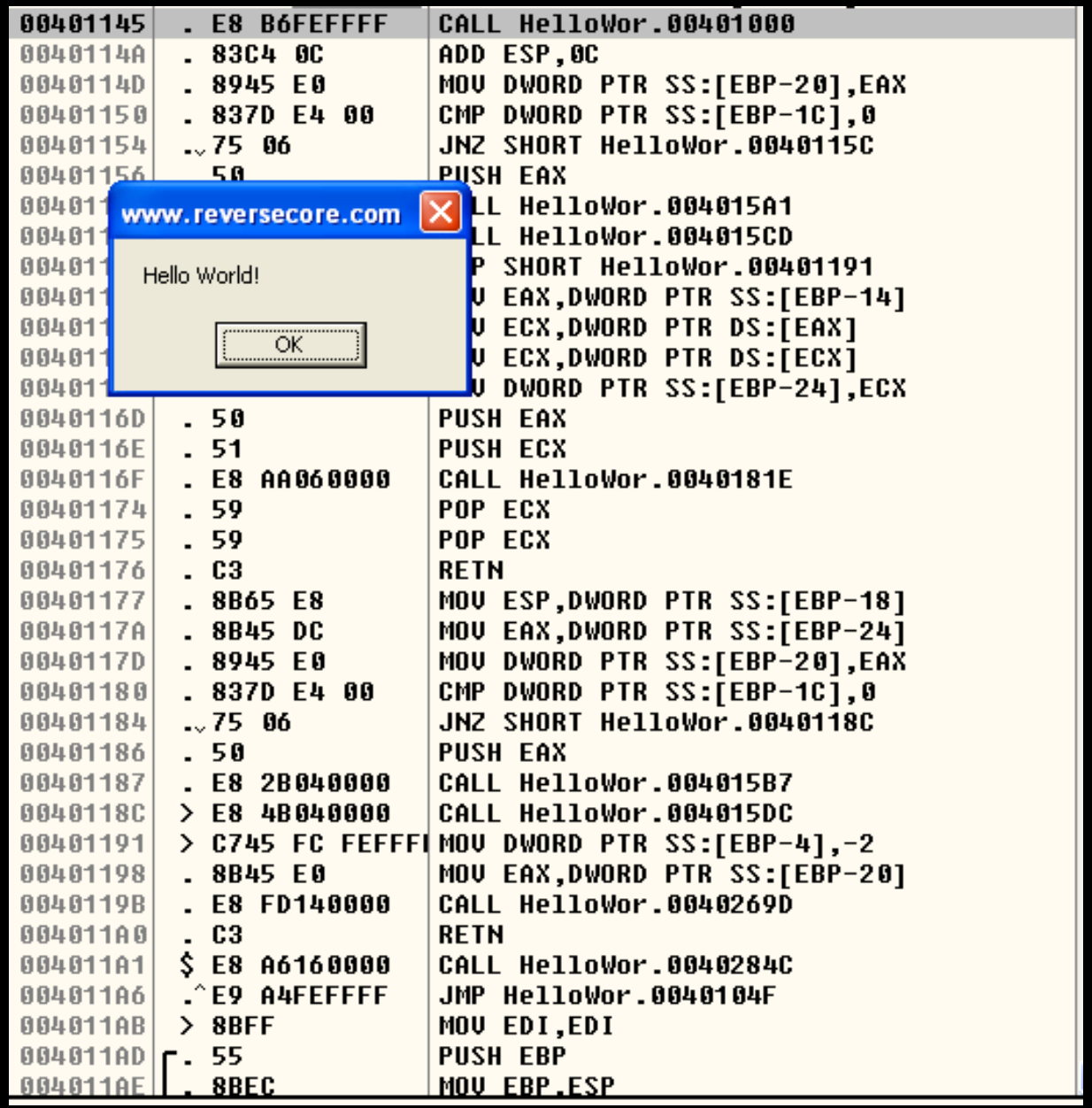
CALL



JMP



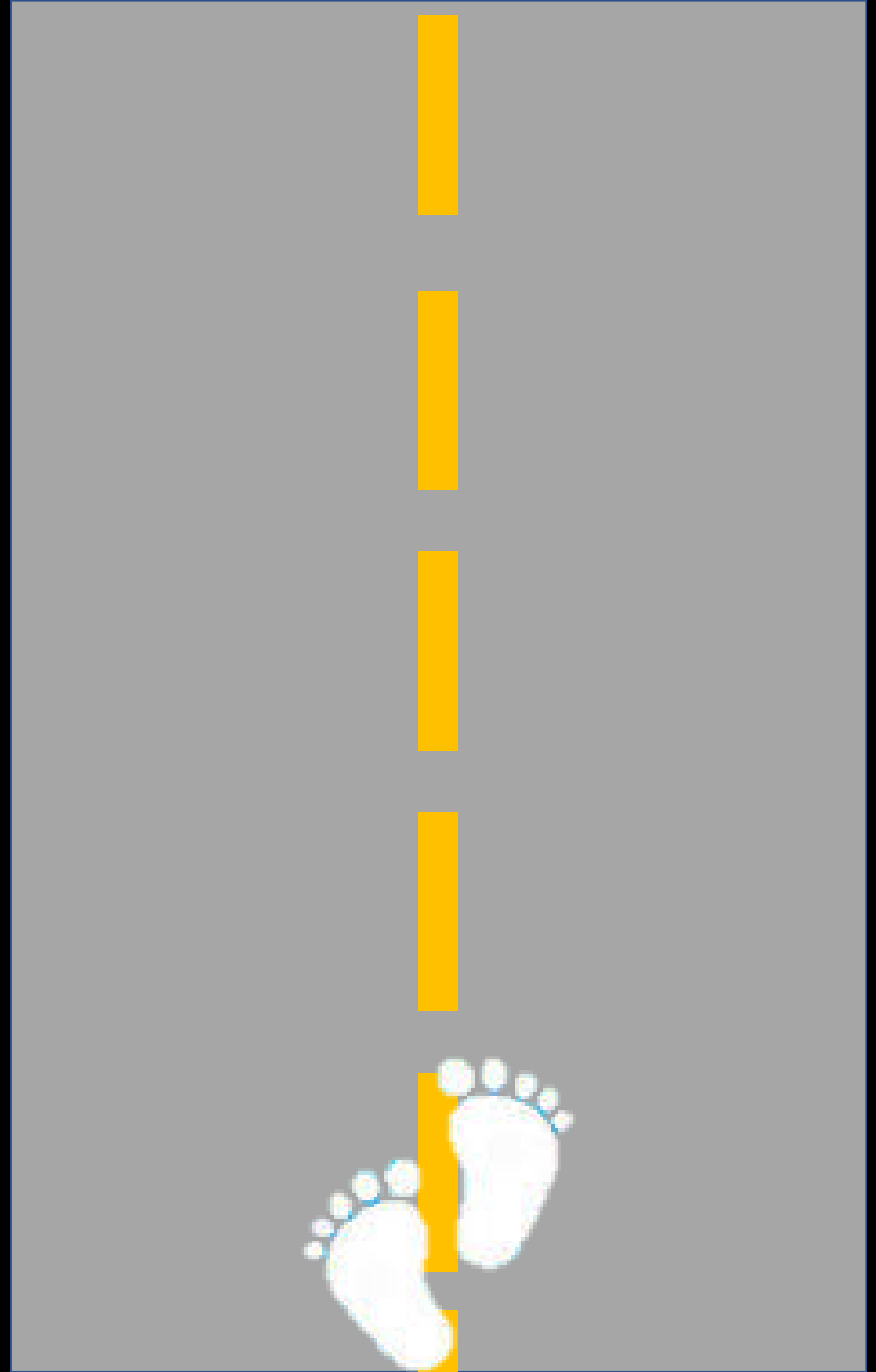

파일 머신 보기 입력 장치 도움말
Recycle Bin
Hello
C:\Documents and Settings\monlove\Desktop\HelloWorld .exex
oops
odbg201
lovemonster
doyouknow
OllyDbg - HelloWorld .exex
CPU - main thread, module HelloWor
Assemble at 004011A6
g
Fill with NOP's
Assemble
Cancel
Registers
Address
Hex dump
start
OllyDbg - HelloWorld ...
C:\Documents and Se...
6:40 AM
Left Windows + Ctrl


00401145 . E8 B6FEFFFF CALL HelloWor.00401000
0040114A . 83C4 0C ADD ESP,0C
0040114D . 8945 E0 MOV DWORD PTR SS:[EBP-20],EAX
00401150 . 837D E4 00 CMP DWORD PTR SS:[EBP-1C],0
00401154 .v 75 06 JNZ SHORT HelloWor.0040115C
00401156 . 50 PUSH EAX
00401 LL HelloWor.004015A1
00401 LL HelloWor.004015CD
00401 P SHORT HelloWor.00401191
00401 V EAX,DWORD PTR SS:[EBP-14]
00401 V ECX,DWORD PTR DS:[EAX]
00401 V ECX,DWORD PTR DS:[ECX]
00401 V DWORD PTR SS:[EBP-24],ECX
0040116D . 50 PUSH EAX
0040116E . 51 PUSH ECX
0040116F . E8 AA060000 CALL HelloWor.0040181E
00401174 . 59 POP ECX
00401175 . 59 POP ECX
00401176 . C3 RETN
00401177 . 8B65 E8 MOV ESP,DWORD PTR SS:[EBP-18]
0040117A . 8B45 DC MOV EAX,DWORD PTR SS:[EBP-24]
0040117D . 8945 E0 MOV DWORD PTR SS:[EBP-20],EAX
00401180 . 837D E4 00 CMP DWORD PTR SS:[EBP-1C],0
00401184 .v 75 06 JNZ SHORT HelloWor.0040118C
00401186 . 50 PUSH EAX
00401187 . E8 2B040000 CALL HelloWor.004015B7
0040118C > E8 4B040000 CALL HelloWor.004015DC
00401191 > C745 FC FEFFFI MOV DWORD PTR SS:[EBP-4],-2
00401198 . 8B45 E0 MOV EAX,DWORD PTR SS:[EBP-20]
0040119B . E8 FD140000 CALL HelloWor.0040269D
004011A0 . C3 RETN
004011A1 $ E8 A6160000 CALL HelloWor.0040284C
004011A6 .^ E9 A4FEFFFF JMP HelloWor.0040104F
004011AB > 8BFF MOV EDI,EDI
004011AD . 55 PUSH EBP
004011AE . 8BEC MOV EBP,ESP
www.reversecore.com
Hello World!
OK

```
00401000 ┌$ 6A 00          PUSH 0
00401002 |. 68 7C924000    PUSH HelloWor.0040927C
00401007 |. 68 A4924000    PUSH HelloWor.004092A4
0040100C |. 6A 00          PUSH 0
0040100E |. FF15 E8804000 CALL DWORD PTR DS:[<&USER32.MessageBoxW
00401014 |. 33C0          XOR EAX,EAX
00401016 L. C3            RETN
```

Address	Hex dump	UNIC
004092A4	48 00 65 00 6C 00 6C 00	Hell
004092AC	6F 00 20 00 57 00 6F 00	o Wo
004092B4	72 00 6C 00 64 00 21 00	rld!
004092BC	00 00 00 00 00 00 00 00	....
004092C4	00 00 00 00 00 00 00 00	....
004092CC	00 00 00 00 00 00 00 00	....
004092D4	00 00 00 00 00 00 00 00	....
004092DC	00 00 00 00 00 00 00 00	....
004092E4	00 00 00 00 00 00 00 00	....
004092EC	00 00 00 00 00 00 00 00	....
004092F4	00 00 00 00 00 00 00 00	....

Address	Hex dump	UNIC
004092A4	44 00 6F 00 20 00 79 00	Do y
004092AC	6F 00 75 00 20 00 4B 00	ou K
004092B4	6E 00 6F 00 77 00 20 00	now
004092BC	4D 00 6F 00 6E 00 73 00	Mons
004092C4	74 00 65 00 72 00 20 00	ter
004092CC	45 00 6E 00 65 00 72 00	Ener
004092D4	67 00 79 00 3F 00 00 00	gy?.
004092DC	00 00 00 00 00 00 00 00	....
004092E4	00 00 00 00 00 00 00 00	....




질문 있으신
가요??

만든이 : 송태현

실행환경 : window xp

출처 : 나뭇잎책

도와준 이: 흰색 사람 (테스트, 발자국)

하늘색 사람(Q&A)