

Illydbg로

텍스트 박스 내용을

내가 원하는

문장으로

바꾸기





OllyDbg - HelloWorld.exe - [CPU - main thread, module HelloWor]

File View Debug Plugins Options Window Help

LEMTWHC/KBR...S

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
004011B0 . 81EC 28030000 SUB ESP,328
004011B6 . A3 58AD4000 MOV DWORD PTR DS:[40AD58],EAX
004011BB . 890D 54AD4000 MOV DWORD PTR DS:[40AD54],ECX
004011C1 . 8915 50AD4000 MOV DWORD PTR DS:[40AD50],EDX
004011C7 . 891D 4CAD4000 MOV DWORD PTR DS:[40AD4C],EBX
004011CD . 8935 48AD4000 MOV DWORD PTR DS:[40AD48],ESI
004011D3 . 893D 44AD4000 MOV DWORD PTR DS:[40AD44],EDI
004011D9 . 66:8C15 70AD4000 MOV WORD PTR DS:[40AD70],SS
004011E0 . 66:8C0D 64AD4000 MOV WORD PTR DS:[40AD64],CS
004011E7 . 66:8C1D 40AD4000 MOV WORD PTR DS:[40AD40],DS
004011EE . 66:8C05 3CAD4000 MOV WORD PTR DS:[40AD3C],ES
004011F5 . 66:8C25 38AD4000 MOV WORD PTR DS:[40AD38],FS
004011FC . 66:8C2D 34AD4000 MOV WORD PTR DS:[40AD34],GS
00401203 . 9C PUSHFD
00401204 . 8F05 68AD4000 POP DWORD PTR DS:[40AD68]
0040120A . 8B45 00 MOV EAX,DWORD PTR SS:[EBP]
0040120B . A3 5CAD4000 MOV DWORD PTR DS:[40AD5C],EAX
00401212 . 8B45 04 MOV EAX,DWORD PTR SS:[EBP+4]
00401215 . A3 60AD4000 MOV DWORD PTR DS:[40AD60],EAX
0040121A . 8B45 08 LEA EAX,DWORD PTR SS:[EBP+8]
0040121D . A3 6CAD4000 MOV DWORD PTR DS:[40AD6C],EAX
00401222 . 8B85 E0CFFFFF MOV EAX,DWORD PTR SS:[EBP-320]
00401228 . C705 A8AC4000 MOV DWORD PTR DS:[40AC88],10001
00401232 . A1 60AD4000 MOV EAX,DWORD PTR DS:[40AD60]
00401237 . A3 5CAD4000 MOV DWORD PTR DS:[40AC5C],EAX
0040123C . C705 58AC4000 MOV DWORD PTR DS:[40AC50],C0000409
00401246 . C705 54AC4000 MOV DWORD PTR DS:[40AC54],1
00401250 . A1 00AD4000 MOV EAX,DWORD PTR DS:[40AD00]
0040284C=HelloWor.0040284C

Registers (FPU)

EAX 00000000
ECX 0012FF80
EDX 7C90EB94 ntdll.KiFastSystemCallRet
EBX 7FFD5000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C910738 ntdll.7C910738
EIP 004011A1 HelloWor.<ModuleEntryPoint>

C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 1 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
D 0
I 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty -UNORM D0A8 01050104 00620064
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0

3 2 1 0 E S P U 0 2 0 1
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1

0012FFC4 7C816D4F RETURN to kernel32.7C816D4F
0012FFC8 7C910738 ntdll.7C910738
0012FFCC FFFFFFFF
0012FFD0 7FFD5000
0012FFD4 8054B038
0012FFD8 0012FFC8
0012FFDC FF93D8C0
0012FFE0 FFFFFFFF End of SEH chain
0012FFE4 7C8399F3 SE handler
0012FFE8 7C816D58 kernel32.7C816D58
0012FFEC 00000000
0012FFF0 00000000
0012FFF4 00000000
0012FFF8 004011A1 HelloWor.<ModuleEntryPoint>
0012FFFC 00000000

Address Hex dump ASCII
00400000 01 00 00 00 4E E6 40 8B |...NetB
00400008 01 19 0F 44 B7 15 40 00 |±0-00.
00400010 02 00 00 00 98 86 40 00 |...000.
00400018 08 00 00 00 6C 86 40 00 |...100.
00400020 09 00 00 00 40 86 40 00 |...000.
00400028 0A 00 00 00 A8 85 40 00 |...00.
00400030 10 00 00 00 7C 85 40 00 |...100.
00400038 11 00 00 00 4C 85 40 00 |...L00.
00400040 12 00 00 00 28 85 40 00 |...00.
00400048 13 00 00 00 FC 84 40 00 |...000.
00400050 18 00 00 00 C4 84 40 00 |...000.
00400058 19 00 00 00 9C 84 40 00 |...000.
00400060 1A 00 00 00 64 84 40 00 |...d00.
00400068 1B 00 00 00 2C 84 40 00 |...00.
00400070 1C 00 00 00 04 84 40 00 |...000.
00400078 1E 00 00 00 E4 83 40 00 |...300.
00400080 1F 00 00 00 8D 83 40 00 |...000.

Program entry point Paused

start odbg110 OllyDbg - HelloWorld ... C:\Documents and Se...

2:37 AM

Call : 함수로 이동

JMP: 함수로 이동

```
1 #include "windows.h"
2
3 int main(int argc, char* argv[])
4 {
5     MessageBox(NULL,
6                 L"Hello World!",
7                 L"www.reversecore.com",
8                 MB_OK);
9
10    return 0;
11 }
```

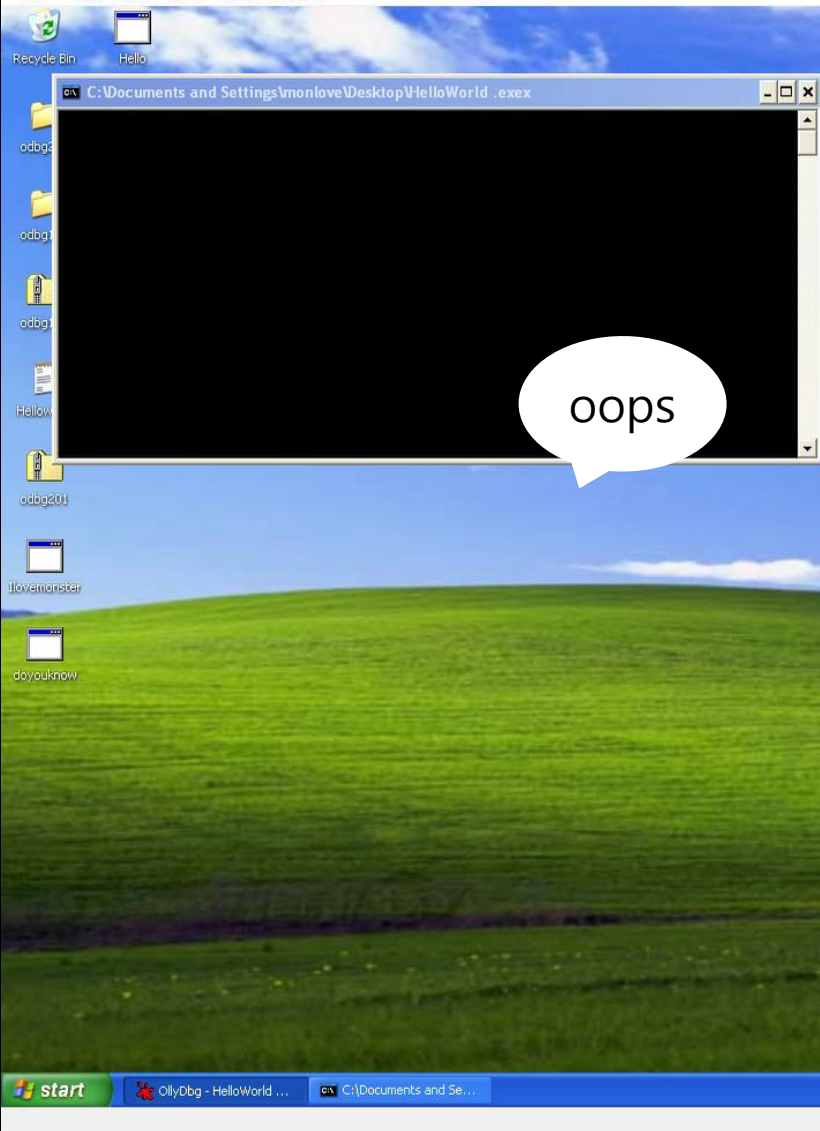
CALL



JMP



bye



OllyDbg - HelloWorld .exe

File View Debug Plugins Options Window Help

CPU - main thread, module HelloWor

004011A6 .E9 A4FFFFFF JMP HelloWorld.0040104F
004011A8 > 8BFF MOV EDI,EDI
004011AA . 55 PUSH EBP
004011AC . 8BEC MOV EBP,ESP
004011AE . 81EC 28030000 SUB ESP,328
004011B0 . A3 58AD4000 MOV DWORD PTR DS:[40AD58],EAX
004011B2 . 890D 54AD4000 MOV DWORD PTR DS:[40AD54],ECX
004011B4 . 8915 50AD4000 MOV DWORD PTR DS:[40AD50],EDX
004011B6 . 891D 4CAD4000 MOV DWORD PTR DS:[40AD4C],EBX
004011B8 . 8935 48AD4000 MOV DWORD PTR DS:[40AD48],ESI
004011BA . 893D 44AD4000 MOV DWORD PTR DS:[40AD44],EDI
004011BC . 66:8C15 70AD4 MOV WORD PTR DS:[40AD70],SS
004011BE . 66:8C0D 64AD4 MOV WORD PTR DS:[40AD64],CS
004011C0 . 66:8C1D 40AD4 MOV WORD PTR DS:[40AD40],DS
004011C2 . 66:8C05 3CAD4 MOV WORD PTR DS:[40AD3C],ES
004011C4 . 66:8C25 38AD4 MOV WORD PTR DS:[40AD38],FS
004011C6 . 66:8C2D 34AD4 MOV WORD PTR DS:[40AD34],GS
004011C8 . 9C PUSHFD
004011CA . 8F05 68AD4000 POP DWORD PTR DS:[40AD68]
004011CC . 8B45 00 MOV EAX,DWORD PTR SS:[EBP]
004011CE . A3 5CAD4000 MOV DWORD PTR DS:[40AD5C],EAX
004011D0 . 8B45 04 MOV EAX,DWORD PTR SS:[EBP+4]
004011D2 . A3 60AD4000 MOV DWORD PTR DS:[40AD60],EAX
004011D4 . 8D45 08 LEA EAX,DWORD PTR SS:[EBP+8]
004011D6 . A3 6CAD4000 MOV DWORD PTR DS:[40AD6C],EAX
004011D8 . 8B85 E0FCFFFF MOV EAX,DWORD PTR SS:[EBP-320]
004011DA . C705 A8AC4000 MOV DWORD PTR DS:[40AC8],10001
004011DC . A1 60AD4000 MOV EAX,DWORD PTR DS:[40AD60]
004011DE . A3 5CAC4000 MOV DWORD PTR DS:[40AC5C],EAX
004011E0 . C705 50AC4000 MOV DWORD PTR DS:[40AC50],C0000409
004011E2 . C705 54AC4000 MOV DWORD PTR DS:[40AC54],1
004011E4 . A1 04A04000 MOV EAX,DWORD PTR DS:[40A004]
004011E6 . 8985 D8ECFFFF MOV DWORD PTR SS:[EBP-328],EAX

Assemble at 004011A6

g

☒ Fill with NOPs Assemble Cancel

Registers

EAX 529B07
ECX 0012FF
EDX 7C900E
EBX 7FFDD6
ESP 0012FF
EBP 0012FF
ESI FFFFFFFF
EDI 7C9107
EIP 004011
C 0 ES 00
P 1 CS 00
A 0 SS 00
Z 0 DS 00
S 1 FS 00
T 0 GS 00
D 0
I 0 LastE
EFL 000002
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
FST 0000
FCW 027F

Address	Hex dump	UNIC
0040A000	01 00 00 00 43 3D 07 EE	...
0040A008	0C C2 28 11 87 15 40 00	...
0040A010	02 00 00 00 98 86 40 00	...
0040A018	08 00 00 00 6C 86 40 00	...
0040A020	09 00 00 00 40 86 40 00	...
0040A028	0A 00 00 00 A8 85 40 00	...
0040A030	10 00 00 00 7C 85 40 00	...
0040A038	11 00 00 00 4C 85 40 00	...
0040A040	12 00 00 00 28 85 40 00	...
0040A048	13 00 00 00 FC 84 40 00	...
0040A050	18 00 00 00 C4 84 40 00	...
0040A058	19 00 00 00 9C 84 40 00	...
0040A060	1A 00 00 00 64 84 40 00	...
0040A068	1B 00 00 00 2C 84 40 00	...
0040A070	1C 00 00 00 04 84 40 00	...
0040A078	1E 00 00 00 E4 83 40 00	...

0012FFC4 7C816D4F RETURN to kernel32.7C816D4F
0012FFC8 7C910738 ntdll.7C910738
0012FFCC FFFFFFFF
0012FFD0 7FFDD000
0012FFD4 80548358
0012FFD8 0012FFC8
0012FFDC FF94C2A0
0012FFE0 FFFFFFFF End of SEH chain
0012FFE4 7C8399F3 SE handler
0012FFE8 7C816D58 kernel32.7C816D58
0012FFEC 00000000
0012FFF0 00000000
0012FFF4 00000000
0012FFF8 004011A1 HelloWorld.<ModuleEntryPoint>
0012FFFC 00000000

Paused

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	. 75 06	JNZ SHORT HelloWor.0040115C
00401156	. 50	PUSH EAX
0040115A	. E8 2B040000	CALL HelloWor.004015A1
0040115D	. E8 4B040000	CALL HelloWor.004015DC
00401160	. 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	. 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 FEFFFF	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!

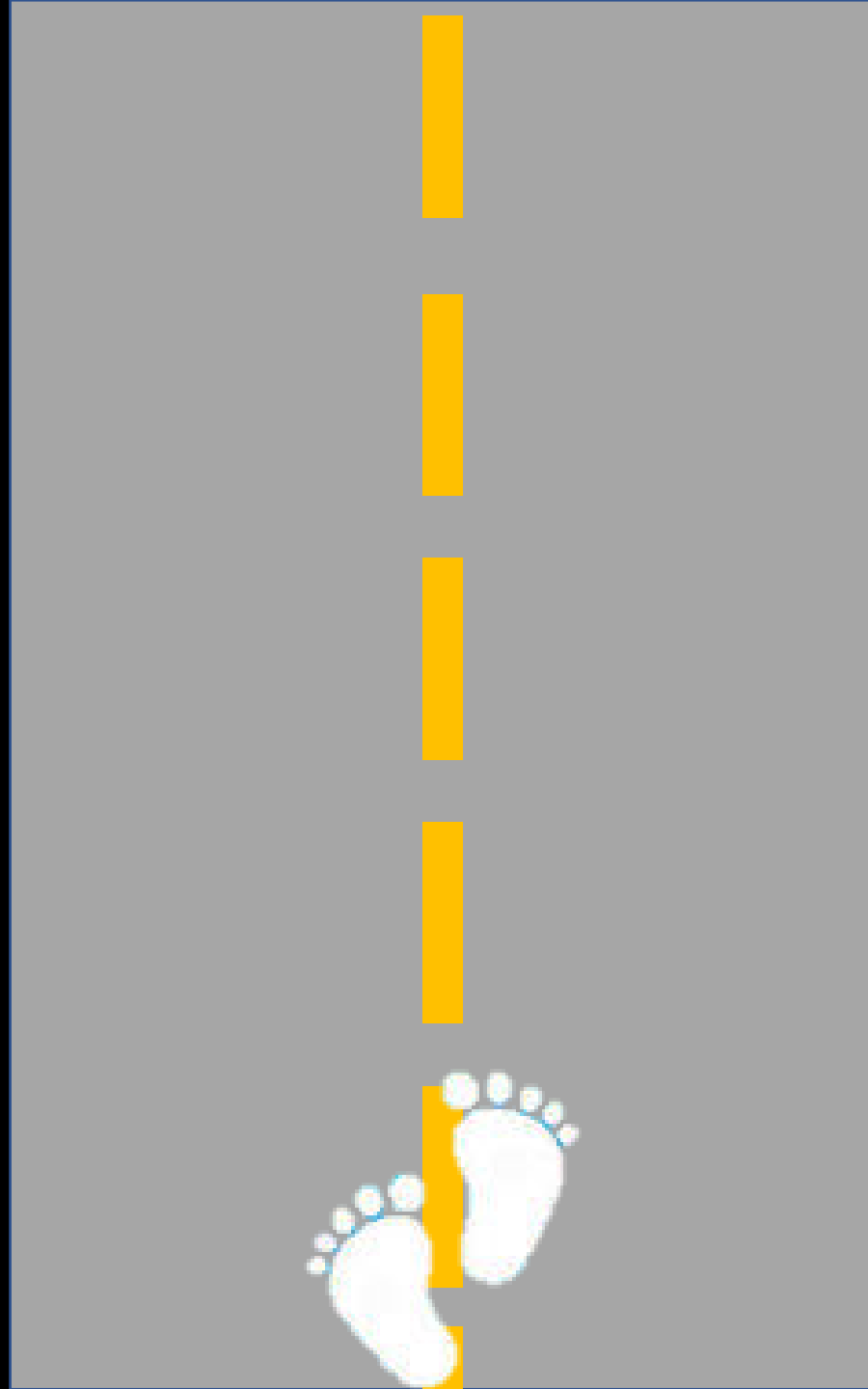
OK

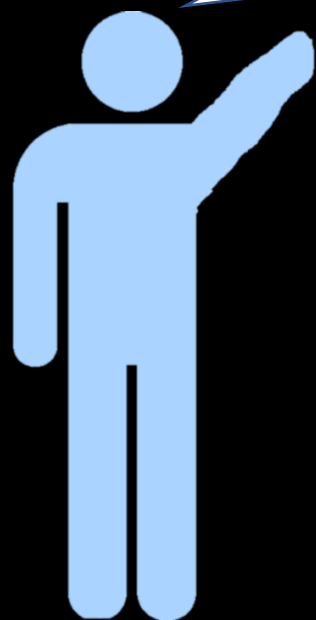
00401000	6A 00	PUSH 0
00401002	68 7C924000	PUSH HelloWor.0040927C
00401007	68 A4924000	PUSH HelloWor.004092A4
0040100C	6A 00	PUSH 0
0040100E	FF15 E8804000	CALL DWORD PTR DS:[<&USER32.MessageBoxW]
00401014	33C0	XOR EAX,EAX
00401016	C3	RETN

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 48 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)