리버싱 입문

SCP 신입부원 20학번 박준형

목차 table of contents

1 리버싱 이란?

2 동적분석과 정적분석

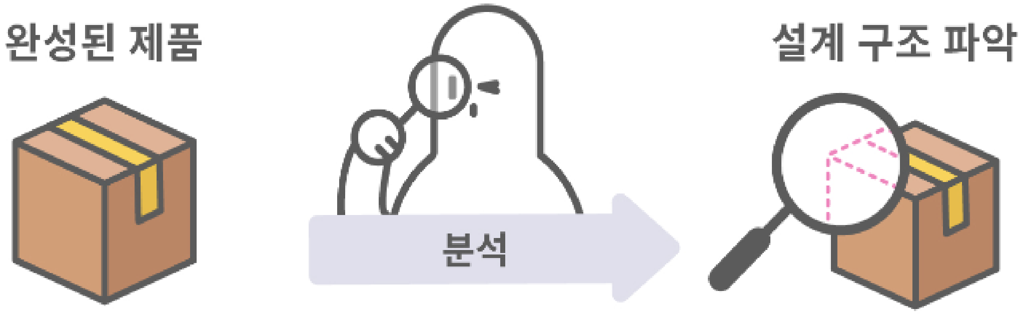
3 Ollydbg 실습

4 느낀점 및 Q&A

리버싱 이란?

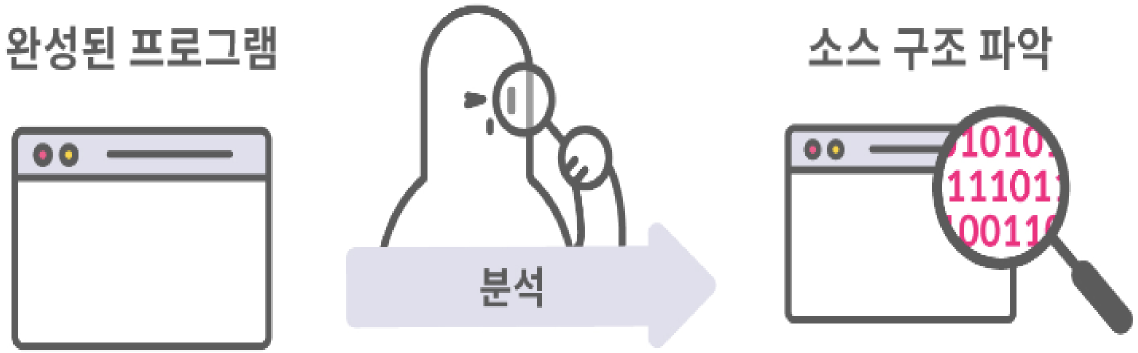
Part 1 리버싱(리버스엔지니어링)이란?

물건이나 기계장치 혹은 시스템
등의 구조, 기능, 동작 등을 분석하여
그 원리를 이해하며 단점을 보완하고
새로운 아이디어를 추가하는 일련의 작업



소프트웨어에서의 리버싱

개발된 소프트웨어나 하드웨어의 동작
원리나 디자인을 분석하여 이해하고,
그것을 복제하거나 수정하는 과정



정적 분석

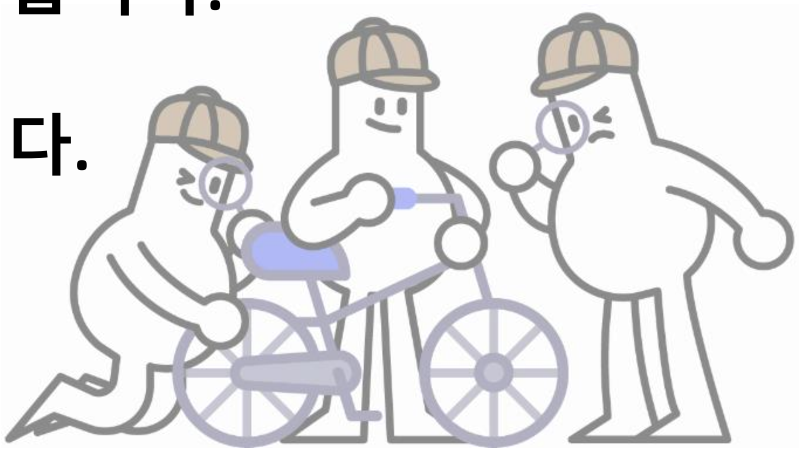
Vs

동적 분석

Part 2 정적 분석 vs 동적 분석

👍

정적 분석을 사용하면 프로그램의 전체구조를 파악하기 쉽습니다.
분석 환경의 제약에서도 비교적 자유롭습니다.
바이러스와 같은 악성 프로그램의 위협으로부터 안전합니다.



👎

난독화(Obfuscation)가 적용되면 분석이 매우 어려워집니다.

→ 난독화가 적용되면 프로그램의 코드가 심하게 변형돼서 이를 읽고,
실행 흐름을 파악하기가 어려워집니다.

Part 2

정적 분석 vs 동적 분석

👍

코드를 자세히 분석해보지 않고도 프로그램의 개략적인 동작을 파악할 수 있습니다.

→ 어떤 입력에 대한 개별 함수 또는 프로그램의 출력을 빠르게 확인할 수 있으므로, 이 출력값들을 기반으로 동작을 추론해 볼 수 있습니다

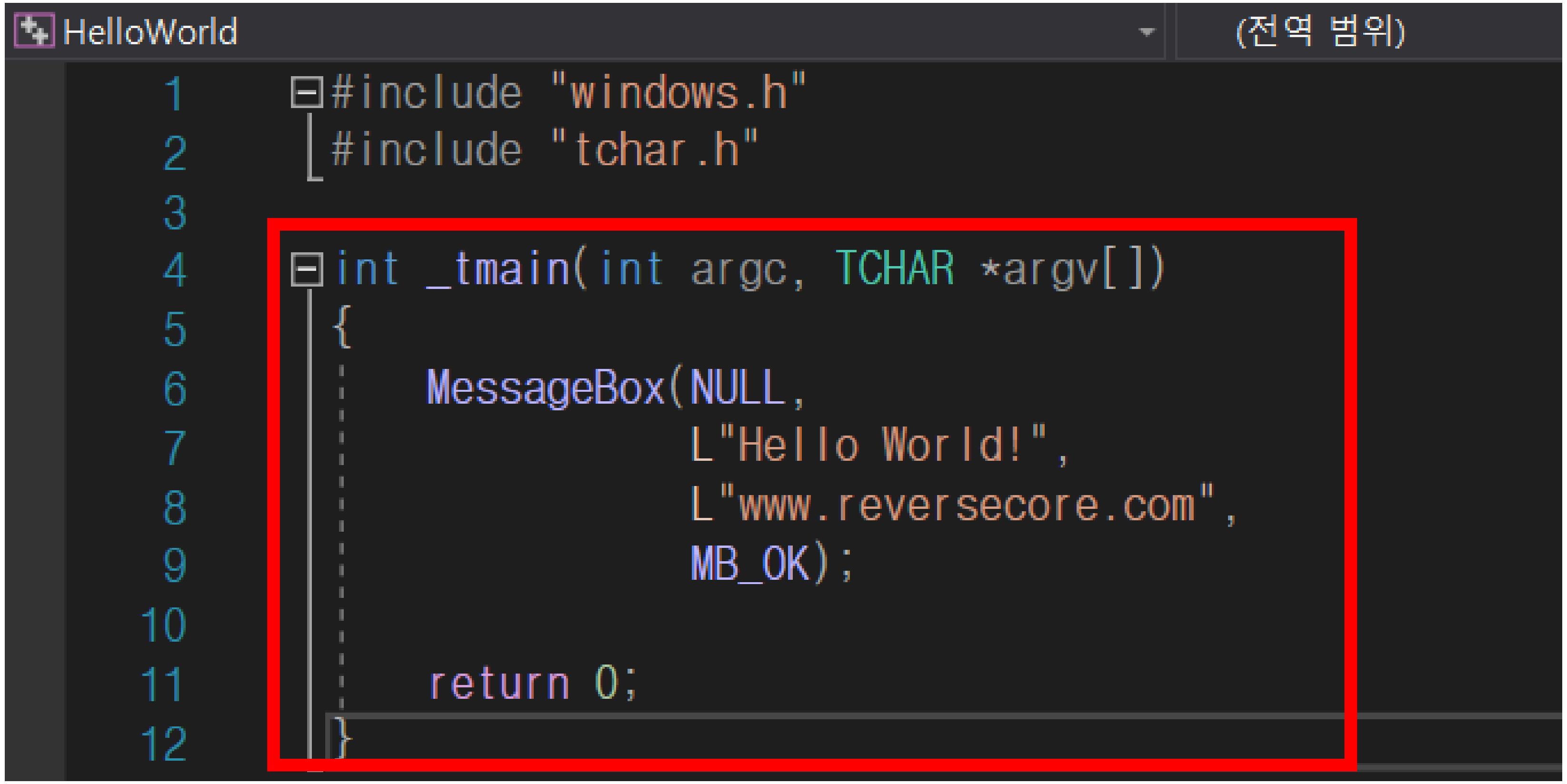
👎

분석 환경을 구축하기 어려울 수 있습니다.

→ 프로그램을 실행하면서 분석하는 것이므로, 프로그램을 실행하지 못하면 동적 분석을 진행할 수 없기 때문

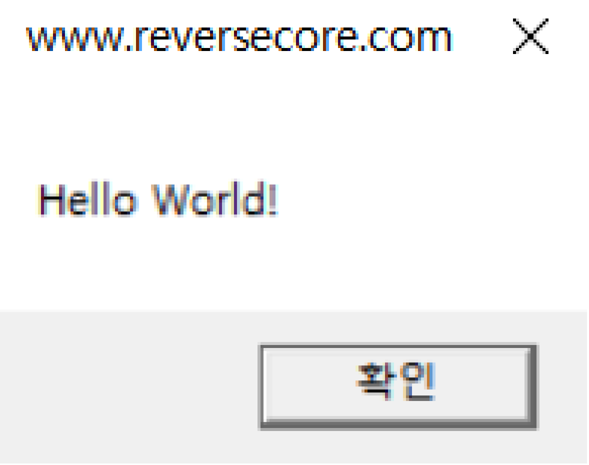
Ollydbg 실습(동적분석)

Part 3 Ollydbg 실습



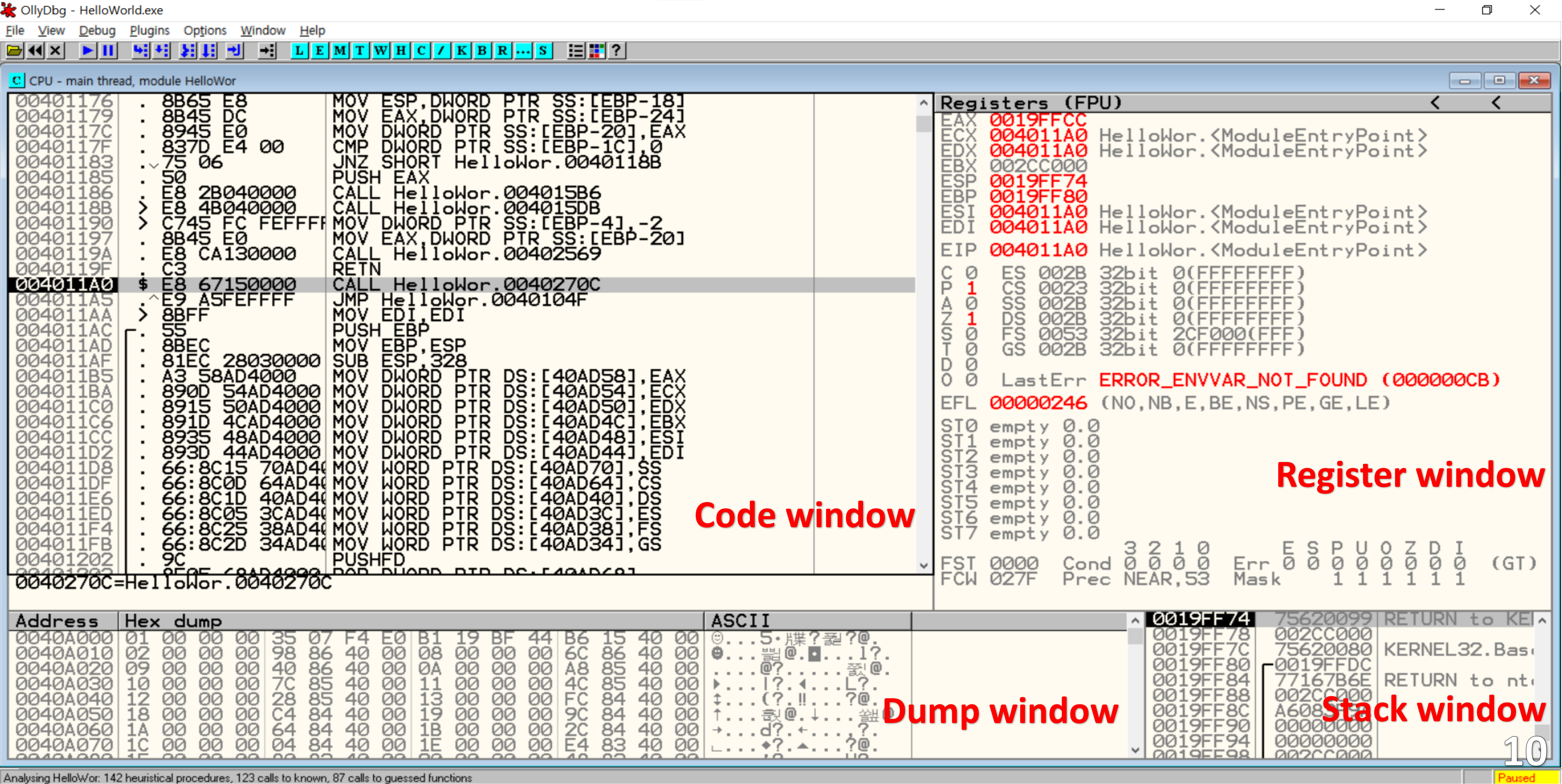
```
#include "windows.h"
#include "tchar.h"

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

    return 0;
}
```

build


www.reversecore.com

Hello World!

Part 3 Ollydbg 실습(ollydbg 메인 화면 설명)


OllyDbg - HelloWorld.exe
File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S
C CPU - main thread, module HelloWor

```
00401176  .  8B65 E8        MOV ESP,DWORD PTR SS:[EBP-18]
00401179  .  8B45 DC        MOV EAX,DWORD PTR SS:[EBP-24]
0040117C  .  8945 E0        MOV DWORD PTR SS:[EBP-20],EAX
0040117F  .  837D E4 00     CMP DWORD PTR SS:[EBP-1C],0
00401183  .v 75 06          JNZ SHORT HelloWor.0040118B
00401185  .  50             PUSH EAX
00401186  .  E8 2B040000    CALL HelloWor.004015B6
0040118B  >  E8 4B040000    CALL HelloWor.004015DB
00401190  >  C745 FC FEFFFF MOV DWORD PTR SS:[EBP-4],-2
00401197  .  8B45 E0        MOV EAX,DWORD PTR SS:[EBP-20]
0040119A  .  E8 CA130000    CALL HelloWor.00402569
0040119F  .  C3             RETN
004011A0  $  E8 67150000    CALL HelloWor.0040270C
004011A5  .^ E9 A5FEFFFF    JMP HelloWor.0040104F
004011AA  >  8BFF           MOV EDI,EDI
004011AC  r. 55             PUSH EBP
004011AD  |. 8BEC           MOV EBP,ESP
004011AF  |. 81EC 28030000  SUB ESP,328
004011B5  |. A3 58AD4000    MOV DWORD PTR DS:[40AD58],EAX
004011BA  |. 890D 54AD4000  MOV DWORD PTR DS:[40AD54],ECX
004011C0  |. 8915 50AD4000  MOV DWORD PTR DS:[40AD50],EDX
004011C6  |. 891D 4CAD4000  MOV DWORD PTR DS:[40AD4C],EBX
004011CC  |. 8935 48AD4000  MOV DWORD PTR DS:[40AD48],ESI
004011D2  |. 893D 44AD4000  MOV DWORD PTR DS:[40AD44],EDI
004011D8  |. 66:8C15 70AD4( MOV WORD PTR DS:[40AD70],SS
004011DF  |. 66:8C0D 64AD4( MOV WORD PTR DS:[40AD64],CS
004011E6  |. 66:8C1D 40AD4( MOV WORD PTR DS:[40AD40],DS
004011ED  |. 66:8C05 3CAD4( MOV WORD PTR DS:[40AD3C],ES
004011F4  |. 66:8C25 38AD4( MOV WORD PTR DS:[40AD38],FS
004011FB  |. 66:8C2D 34AD4( MOV WORD PTR DS:[40AD34],GS
00401202  |. 9C             PUSHFD
0040270C=HelloWor.0040270C
```

```
Registers (FPU)
EAX 0019FFCC
ECX 004011A0 HelloWor.<ModuleEntryPoint>
EDX 004011A0 HelloWor.<ModuleEntryPoint>
EBX 002CC000
ESP 0019FF74
EBP 0019FF80
ESI 004011A0 HelloWor.<ModuleEntryPoint>
EDI 004011A0 HelloWor.<ModuleEntryPoint>

EIP 004011A0 HelloWor.<ModuleEntryPoint>

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 2CF000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_ENVVAR_NOT_FOUND (000000CB)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
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 O Z D I
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
```

```
Address  Hex dump                                         ASCII
0040A000 01 00 00 00 35 07 F4 E0 B1 19 BF 44 B6 15 40 00 ☺...5•牒?줄?@.
0040A010 02 00 00 00 98 86 40 00 08 00 00 00 6C 86 40 00 ☻...뭚@.◘...l?.
0040A020 09 00 00 00 40 86 40 00 0A 00 00 00 A8 85 40 00 ....@?....쭯@.
0040A030 10 00 00 00 7C 85 40 00 11 00 00 00 4C 85 40 00 ►...|?.◄...L?.
0040A040 12 00 00 00 28 85 40 00 13 00 00 00 FC 84 40 00 ↕...(?.‼...?@.
0040A050 18 00 00 00 C4 84 40 00 19 00 00 00 9C 84 40 00 ↑...쾨@.↓...쐢@.
0040A060 1A 00 00 00 64 84 40 00 1B 00 00 00 2C 84 40 00 →...d?.←...,?.
0040A070 1C 00 00 00 04 84 40 00 1E 00 00 00 E4 83 40 00 ∟...♦?.▲...?@.
```

```
0019FF74   75620099  RETURN to KE
0019FF78   002CC000
0019FF7C   75620080  KERNEL32.Bas
0019FF80  r0019FFDC
0019FF84  |77167B6E  RETURN to nt
0019FF88  |002CC000
0019FF8C  |A608
0019FF90  |00000000
0019FF94  |00000000
```

```
Analysing HelloWor: 142 heuristical procedures, 123 calls to known, 87 calls to guessed functions
```

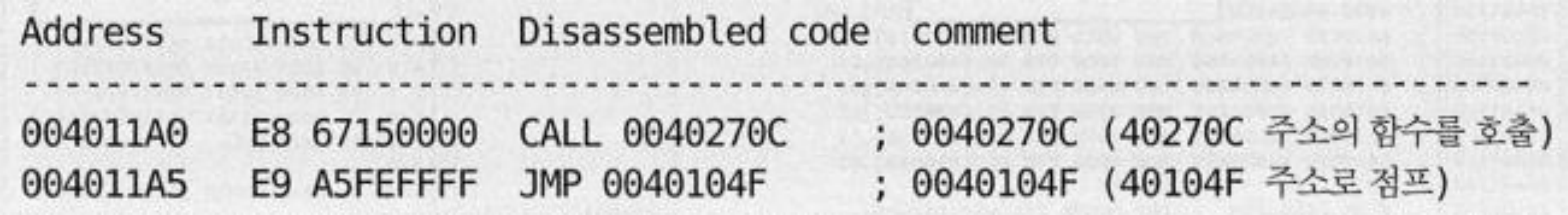
Code window

Register window

Dump window

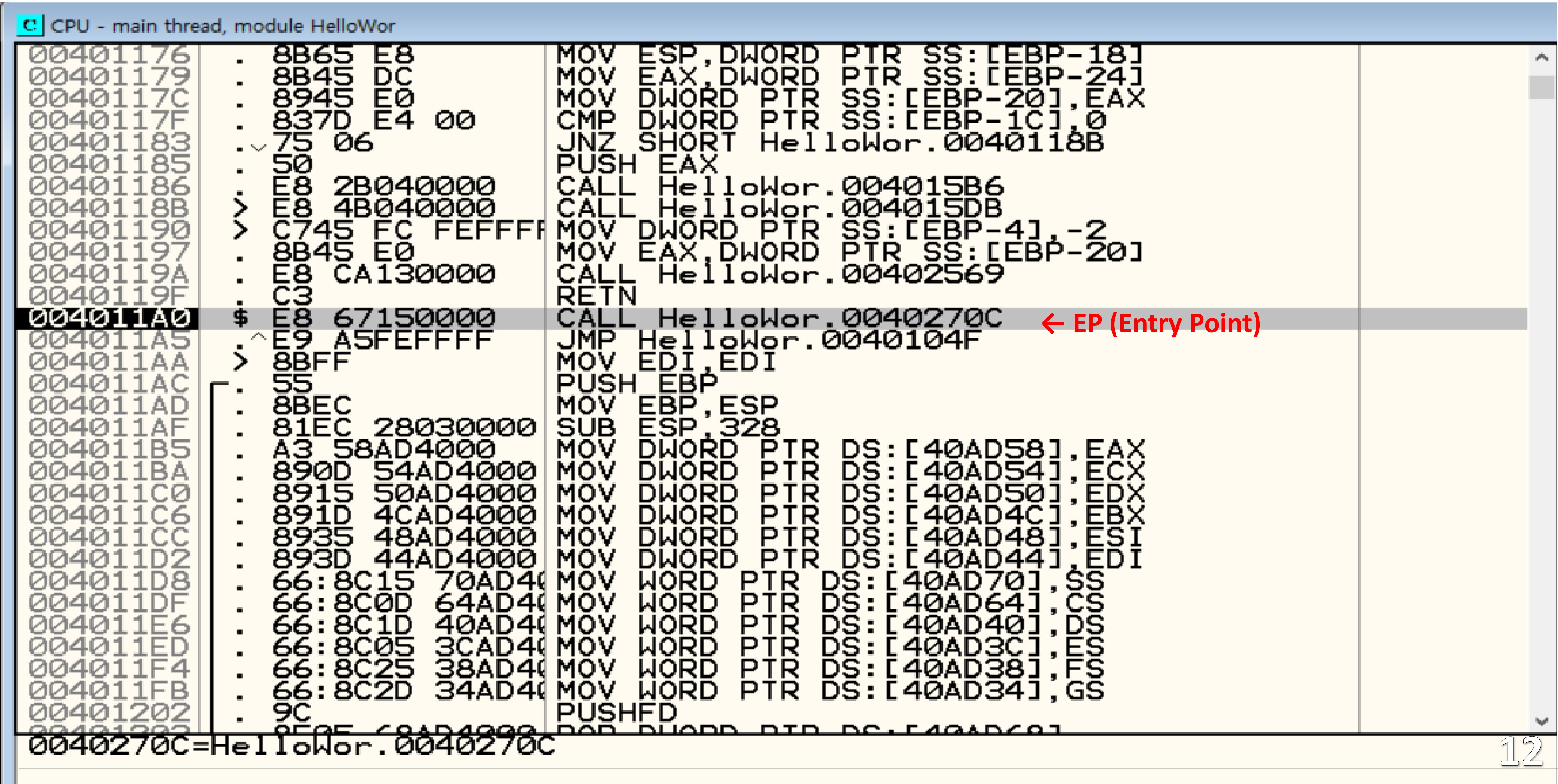
Stack window

Part 3 Ollydbg 실습(EntryPoint)



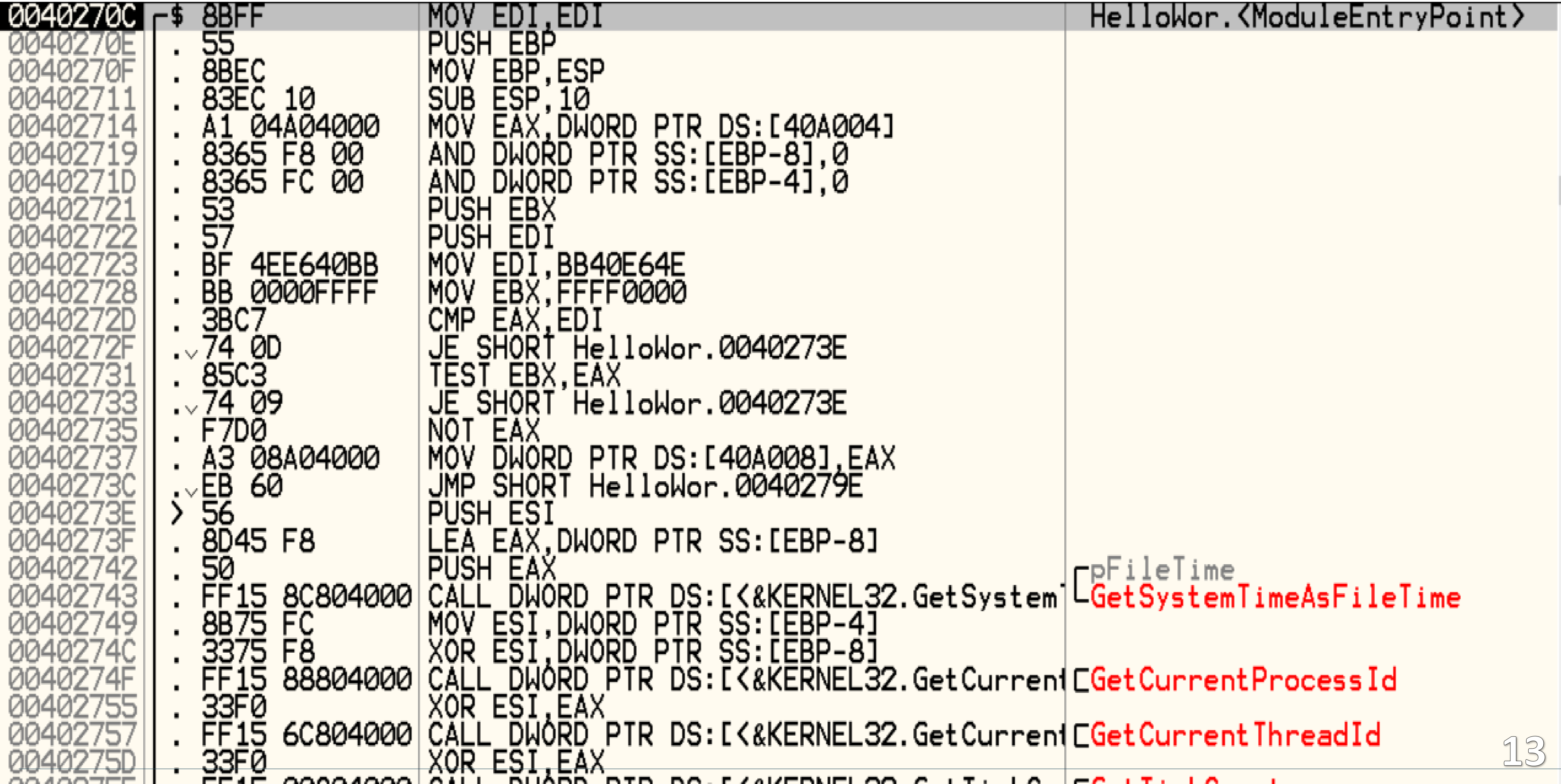
```
Address     Instruction  Disassembled code  comment
--------------------------------------------------------------------------
004011A0    E8 67150000  CALL 0040270C      ; 0040270C (40270C 주소의 함수를 호출)
004011A5    E9 A5FEFFFF  JMP 0040104F       ; 0040104F (40104F 주소로 점프)
```

Part 3 Ollydbg 실습(Restart, Step Into, Step Over, Execute till Return 만으로 main() 함수 찾기)



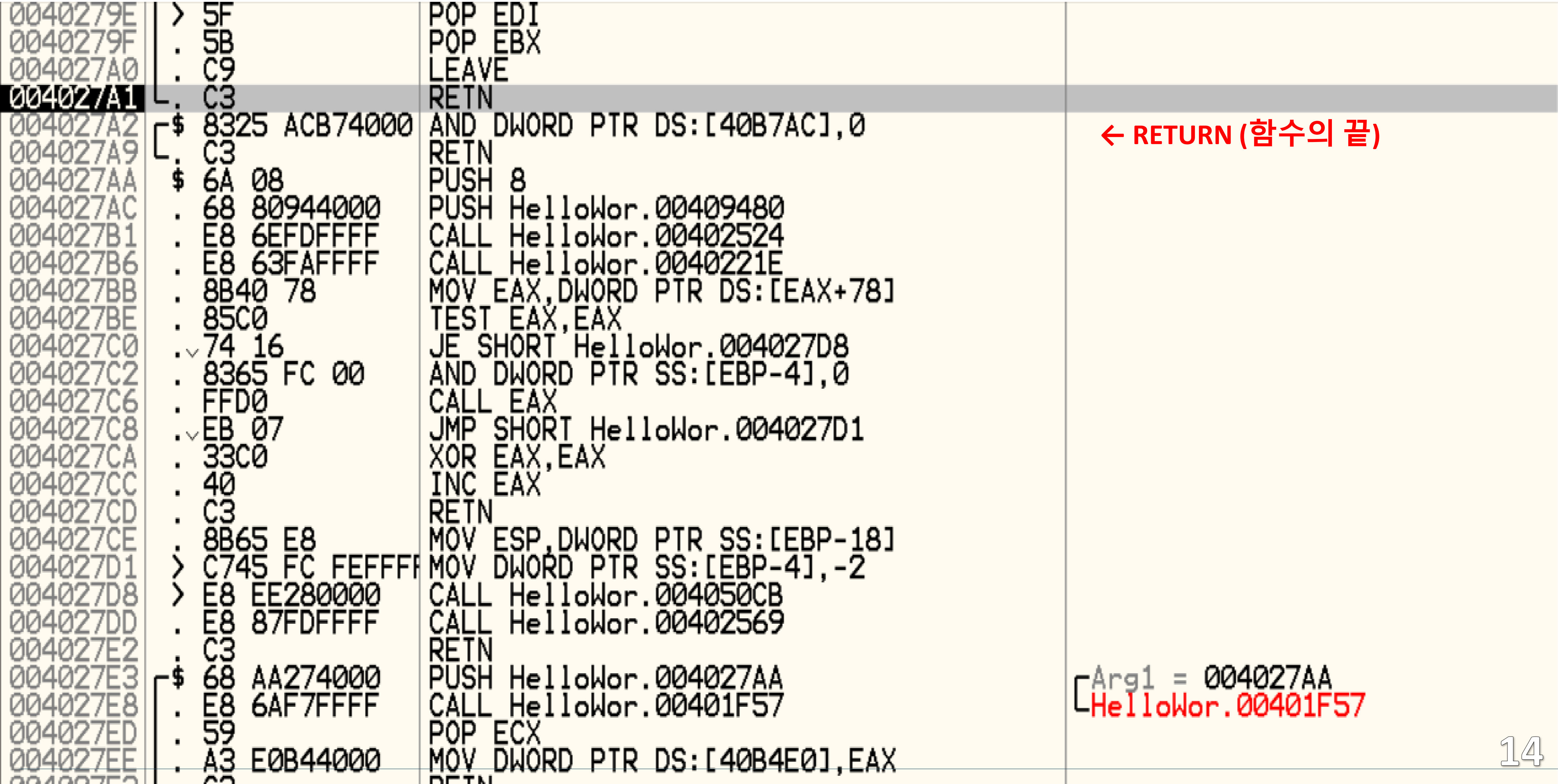
```
00401176  .  8B65 E8          MOV ESP,DWORD PTR SS:[EBP-18]
00401179  .  8B45 DC          MOV EAX,DWORD PTR SS:[EBP-24]
0040117C  .  8945 E0          MOV DWORD PTR SS:[EBP-20],EAX
0040117F  .  837D E4 00       CMP DWORD PTR SS:[EBP-1C],0
00401183  .v 75 06            JNZ SHORT HelloWor.0040118B
00401185  .  50               PUSH EAX
00401186  .  E8 2B040000      CALL HelloWor.004015B6
0040118B  >  E8 4B040000      CALL HelloWor.004015DB
00401190  >  C745 FC FEFFFF   MOV DWORD PTR SS:[EBP-4],-2
00401197  .  8B45 E0          MOV EAX,DWORD PTR SS:[EBP-20]
0040119A  .  E8 CA130000      CALL HelloWor.00402569
0040119F  .  C3               RETN
004011A0  $  E8 67150000      CALL HelloWor.0040270C          ← EP (Entry Point)
004011A5  .^ E9 A5FEFFFF      JMP HelloWor.0040104F
004011AA  >  8BFF             MOV EDI,EDI
004011AC  .  55               PUSH EBP
004011AD  .  8BEC             MOV EBP,ESP
004011AF  .  81EC 28030000    SUB ESP,328
004011B5  .  A3 58AD4000      MOV DWORD PTR DS:[40AD58],EAX
004011BA  .  890D 54AD4000    MOV DWORD PTR DS:[40AD54],ECX
004011C0  .  8915 50AD4000    MOV DWORD PTR DS:[40AD50],EDX
004011C6  .  891D 4CAD4000    MOV DWORD PTR DS:[40AD4C],EBX
004011CC  .  8935 48AD4000    MOV DWORD PTR DS:[40AD48],ESI
004011D2  .  893D 44AD4000    MOV DWORD PTR DS:[40AD44],EDI
004011D8  .  66:8C15 70AD4    MOV WORD PTR DS:[40AD70],SS
004011DF  .  66:8C0D 64AD4    MOV WORD PTR DS:[40AD64],CS
004011E6  .  66:8C1D 40AD4    MOV WORD PTR DS:[40AD40],DS
004011ED  .  66:8C05 3CAD4    MOV WORD PTR DS:[40AD3C],ES
004011F4  .  66:8C25 38AD4    MOV WORD PTR DS:[40AD38],FS
004011FB  .  66:8C2D 34AD4    MOV WORD PTR DS:[40AD34],GS
00401202  .  9C               PUSHFD
00401203  .  8F05 68AD4000    POP DWORD PTR DS:[40AD68]
0040270C=HelloWor.0040270C
```

Part 3 Ollydbg 실습(Restart, Step Into, Step Over, Execute till Return 만으로 main() 함수 찾기)



```
0040270C  r$ 8BFF           MOV EDI,EDI                              HelloWor.<ModuleEntryPoint>
0040270E  |. 55             PUSH EBP
0040270F  |. 8BEC           MOV EBP,ESP
00402711  |. 83EC 10        SUB ESP,10
00402714  |. A1 04A04000    MOV EAX,DWORD PTR DS:[40A004]
00402719  |. 8365 F8 00     AND DWORD PTR SS:[EBP-8],0
0040271D  |. 8365 FC 00     AND DWORD PTR SS:[EBP-4],0
00402721  |. 53             PUSH EBX
00402722  |. 57             PUSH EDI
00402723  |. BF 4EE640BB    MOV EDI,BB40E64E
00402728  |. BB 0000FFFF    MOV EBX,FFFF0000
0040272D  |. 3BC7           CMP EAX,EDI
0040272F  |.v74 0D          JE SHORT HelloWor.0040273E
00402731  |. 85C3           TEST EBX,EAX
00402733  |.v74 09          JE SHORT HelloWor.0040273E
00402735  |. F7D0           NOT EAX
00402737  |. A3 08A04000    MOV DWORD PTR DS:[40A008],EAX
0040273C  |.vEB 60          JMP SHORT HelloWor.0040279E
0040273E  |> 56             PUSH ESI
0040273F  |. 8D45 F8        LEA EAX,DWORD PTR SS:[EBP-8]
00402742  |. 50             PUSH EAX                                 rpFileTime
00402743  |. FF15 8C804000  CALL DWORD PTR DS:[<&KERNEL32.GetSystem  LGetSystemTimeAsFileTime
00402749  |. 8B75 FC        MOV ESI,DWORD PTR SS:[EBP-4]
0040274C  |. 3375 F8        XOR ESI,DWORD PTR SS:[EBP-8]
0040274F  |. FF15 88804000  CALL DWORD PTR DS:[<&KERNEL32.GetCurrent [GetCurrentProcessId
00402755  |. 33F0           XOR ESI,EAX
00402757  |. FF15 6C804000  CALL DWORD PTR DS:[<&KERNEL32.GetCurrent [GetCurrentThreadId
0040275D  |. 33F0           XOR ESI,EAX
```

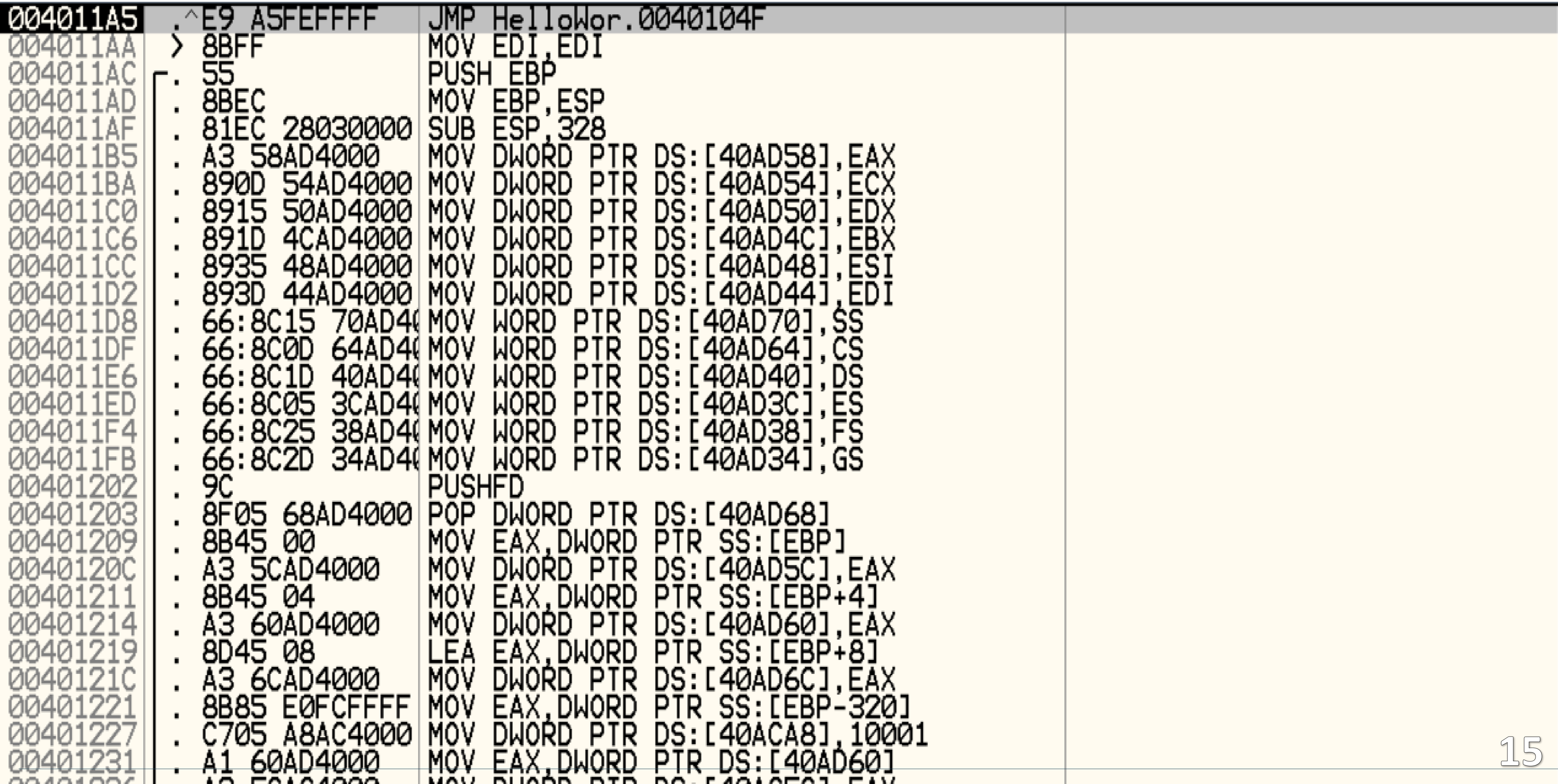
Part 3 Ollydbg 실습(Restart, Step Into, Step Over, Execute till Return 만으로 main() 함수 찾기)



```
0040279E  |> 5F             POP EDI
0040279F  |. 5B             POP EBX
004027A0  |. C9             LEAVE
004027A1  \. C3             RETN
004027A2  /$ 8325 ACB74000  AND DWORD PTR DS:[40B7AC],0
004027A9  \. C3             RETN
004027AA   $ 6A 08          PUSH 8
004027AC   . 68 80944000    PUSH HelloWor.00409480
004027B1   . E8 6EFDFFFF    CALL HelloWor.00402524
004027B6   . E8 63FAFFFF    CALL HelloWor.0040221E
004027BB   . 8B40 78        MOV EAX,DWORD PTR DS:[EAX+78]
004027BE   . 85C0           TEST EAX,EAX
004027C0   .v74 16          JE SHORT HelloWor.004027D8
004027C2   . 8365 FC 00     AND DWORD PTR SS:[EBP-4],0
004027C6   . FFD0           CALL EAX
004027C8   .vEB 07          JMP SHORT HelloWor.004027D1
004027CA   . 33C0           XOR EAX,EAX
004027CC   . 40             INC EAX
004027CD   . C3             RETN
004027CE   . 8B65 E8        MOV ESP,DWORD PTR SS:[EBP-18]
004027D1   > C745 FC FEFFFF MOV DWORD PTR SS:[EBP-4],-2
004027D8   > E8 EE280000    CALL HelloWor.004050CB
004027DD   . E8 87FDFFFF    CALL HelloWor.00402569
004027E2   . C3             RETN
004027E3  /$ 68 AA274000    PUSH HelloWor.004027AA                  /Arg1 = 004027AA
004027E8  |. E8 6AF7FFFF    CALL HelloWor.00401F57                  \HelloWor.00401F57
004027ED  |. 59             POP ECX
004027EE  |. A3 E0B44000    MOV DWORD PTR DS:[40B4E0],EAX
```

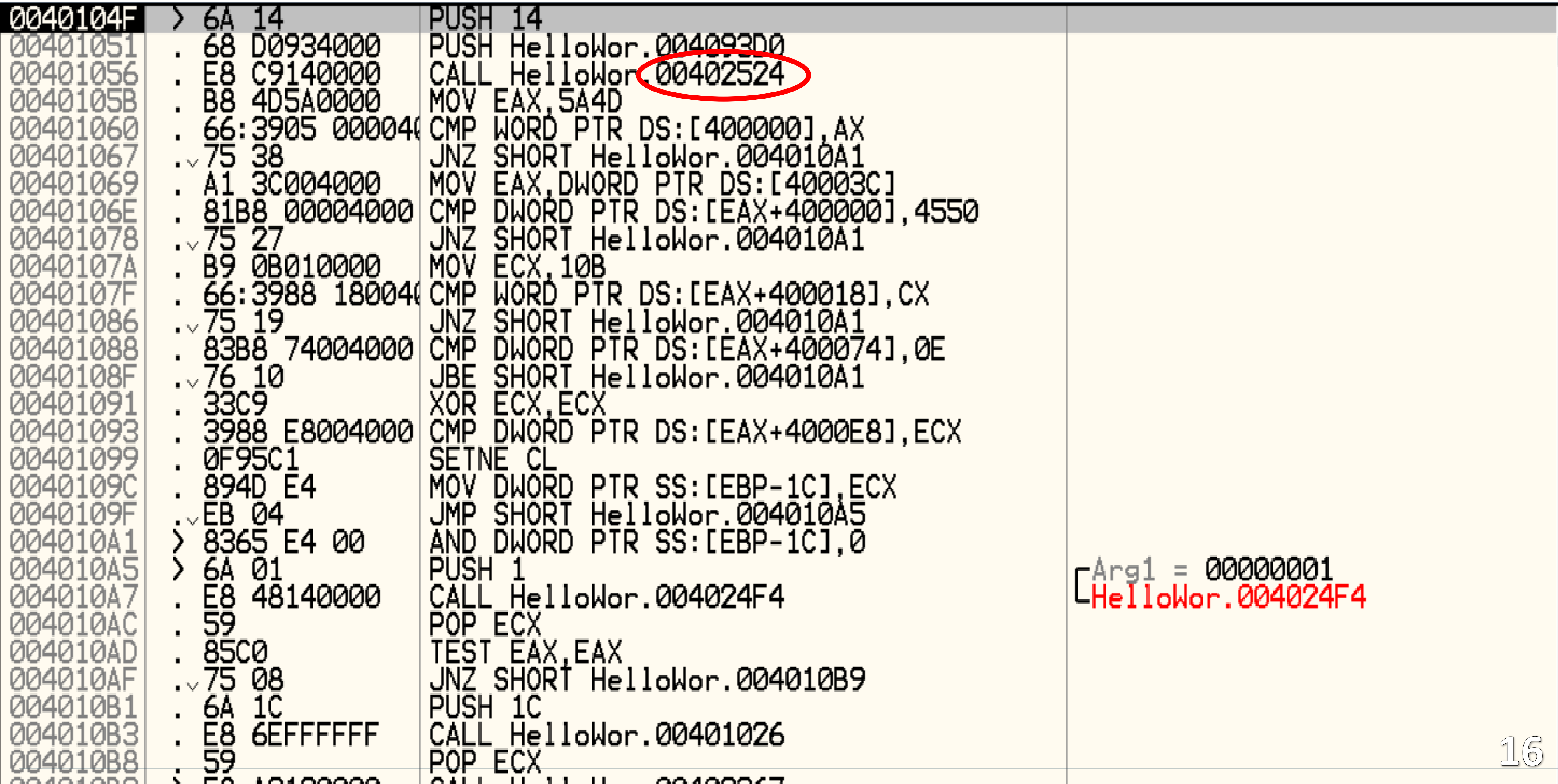
← RETURN (함수의 끝)

Part 3 Ollydbg 실습(Restart,Step Into,Step Over,Execute till Return 만으로 main() 함수 찾기)



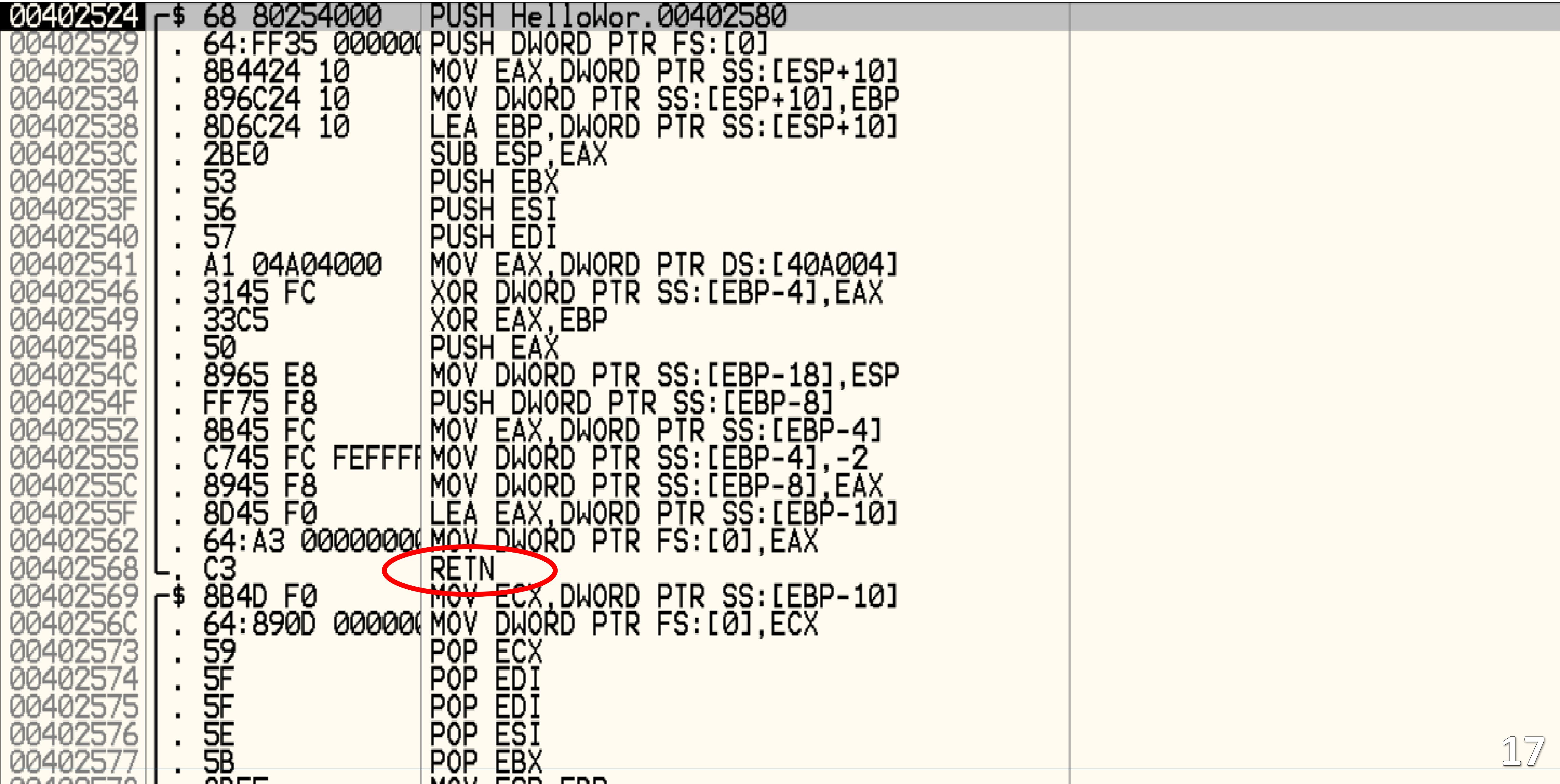
```
004011A5   .^E9 A5FEFFFF    JMP HelloWor.0040104F
004011AA   > 8BFF           MOV EDI,EDI
004011AC  ┌. 55             PUSH EBP
004011AD  │. 8BEC           MOV EBP,ESP
004011AF  │. 81EC 28030000  SUB ESP,328
004011B5  │. A3 58AD4000    MOV DWORD PTR DS:[40AD58],EAX
004011BA  │. 890D 54AD4000  MOV DWORD PTR DS:[40AD54],ECX
004011C0  │. 8915 50AD4000  MOV DWORD PTR DS:[40AD50],EDX
004011C6  │. 891D 4CAD4000  MOV DWORD PTR DS:[40AD4C],EBX
004011CC  │. 8935 48AD4000  MOV DWORD PTR DS:[40AD48],ESI
004011D2  │. 893D 44AD4000  MOV DWORD PTR DS:[40AD44],EDI
004011D8  │. 66:8C15 70AD4  MOV WORD PTR DS:[40AD70],SS
004011DF  │. 66:8C0D 64AD4  MOV WORD PTR DS:[40AD64],CS
004011E6  │. 66:8C1D 40AD4  MOV WORD PTR DS:[40AD40],DS
004011ED  │. 66:8C05 3CAD4  MOV WORD PTR DS:[40AD3C],ES
004011F4  │. 66:8C25 38AD4  MOV WORD PTR DS:[40AD38],FS
004011FB  │. 66:8C2D 34AD4  MOV WORD PTR DS:[40AD34],GS
00401202  │. 9C             PUSHFD
00401203  │. 8F05 68AD4000  POP DWORD PTR DS:[40AD68]
00401209  │. 8B45 00        MOV EAX,DWORD PTR SS:[EBP]
0040120C  │. A3 5CAD4000    MOV DWORD PTR DS:[40AD5C],EAX
00401211  │. 8B45 04        MOV EAX,DWORD PTR SS:[EBP+4]
00401214  │. A3 60AD4000    MOV DWORD PTR DS:[40AD60],EAX
00401219  │. 8D45 08        LEA EAX,DWORD PTR SS:[EBP+8]
0040121C  │. A3 6CAD4000    MOV DWORD PTR DS:[40AD6C],EAX
00401221  │. 8B85 E0FCFFFF  MOV EAX,DWORD PTR SS:[EBP-320]
00401227  │. C705 A8AC4000  MOV DWORD PTR DS:[40ACA8],10001
00401231  │. A1 60AD4000    MOV EAX,DWORD PTR DS:[40AD60]
```

Part 3 Ollydbg 실습(Restart,Step Into,Step Over,Execute till Return 만으로 main() 함수 찾기)



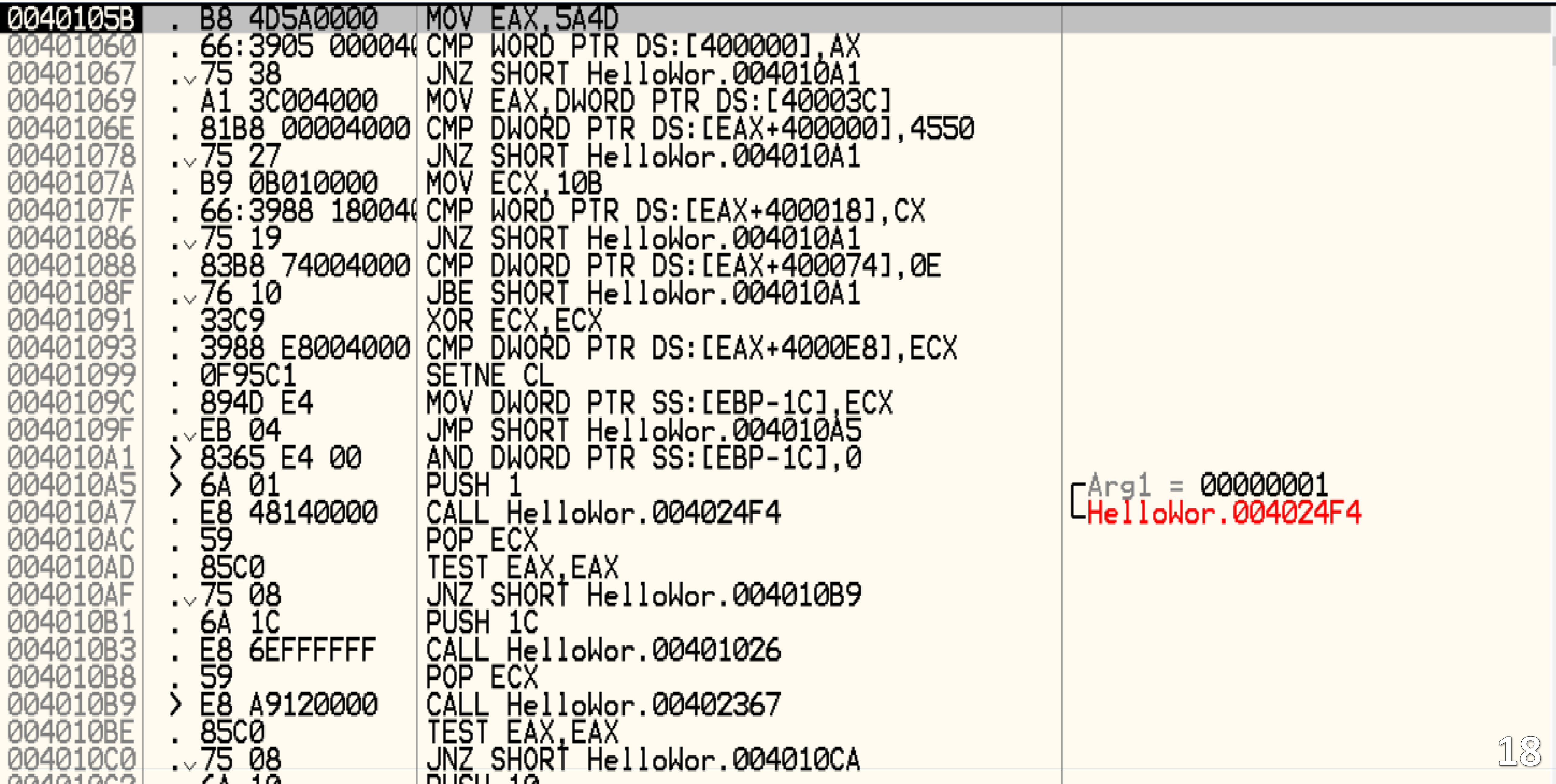
```
0040104F  > 6A 14          PUSH 14
00401051  . 68 D0934000    PUSH HelloWor.004093D0
00401056  . E8 C9140000    CALL HelloWor.00402524
0040105B  . B8 4D5A0000    MOV EAX,5A4D
00401060  . 66:3905 000040 CMP WORD PTR DS:[400000],AX
00401067  .v75 38          JNZ SHORT HelloWor.004010A1
00401069  . A1 3C004000    MOV EAX,DWORD PTR DS:[40003C]
0040106E  . 81B8 00004000  CMP DWORD PTR DS:[EAX+400000],4550
00401078  .v75 27          JNZ SHORT HelloWor.004010A1
0040107A  . B9 0B010000    MOV ECX,10B
0040107F  . 66:3988 180040 CMP WORD PTR DS:[EAX+400018],CX
00401086  .v75 19          JNZ SHORT HelloWor.004010A1
00401088  . 83B8 74004000  CMP DWORD PTR DS:[EAX+400074],0E
0040108F  .v76 10          JBE SHORT HelloWor.004010A1
00401091  . 33C9           XOR ECX,ECX
00401093  . 3988 E8004000  CMP DWORD PTR DS:[EAX+4000E8],ECX
00401099  . 0F95C1         SETNE CL
0040109C  . 894D E4        MOV DWORD PTR SS:[EBP-1C],ECX
0040109F  .vEB 04          JMP SHORT HelloWor.004010A5
004010A1  > 8365 E4 00     AND DWORD PTR SS:[EBP-1C],0
004010A5  > 6A 01          PUSH 1                                    [Arg1 = 00000001
004010A7  . E8 48140000    CALL HelloWor.004024F4                    [HelloWor.004024F4
004010AC  . 59             POP ECX
004010AD  . 85C0           TEST EAX,EAX
004010AF  .v75 08          JNZ SHORT HelloWor.004010B9
004010B1  . 6A 1C          PUSH 1C
004010B3  . E8 6EFFFFFF    CALL HelloWor.00401026
004010B8  . 59             POP ECX
004010B9  > E8 A9120000    CALL HelloWor.00402367
```

Part 3 Ollydbg 실습(Restart, Step Into, Step Over, Execute till Return 만으로 main() 함수 찾기)



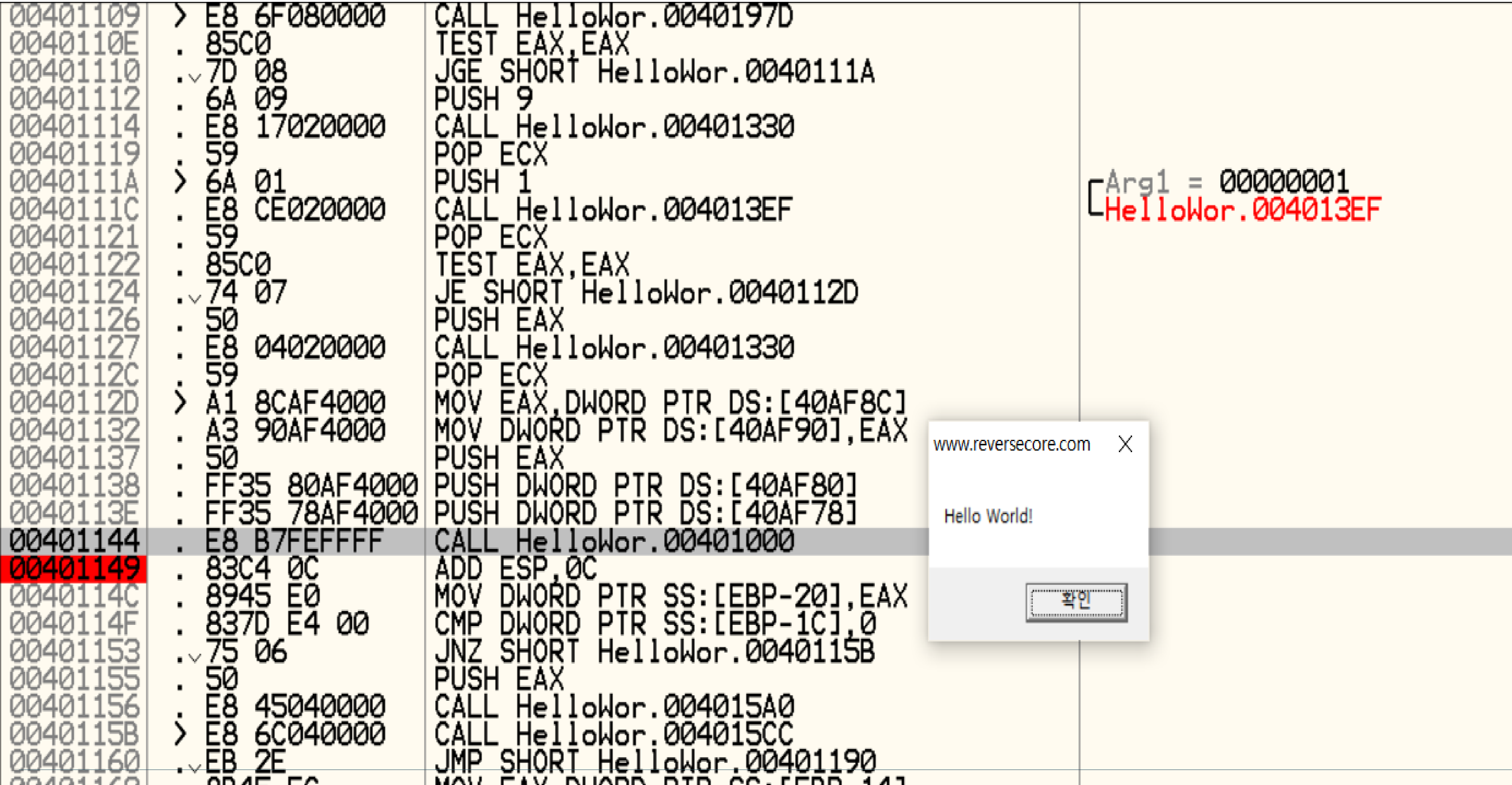
```
00402524 ┌$ 68 80254000        PUSH HelloWor.00402580
00402529 │. 64:FF35 000000     PUSH DWORD PTR FS:[0]
00402530 │. 8B4424 10          MOV EAX,DWORD PTR SS:[ESP+10]
00402534 │. 896C24 10          MOV DWORD PTR SS:[ESP+10],EBP
00402538 │. 8D6C24 10          LEA EBP,DWORD PTR SS:[ESP+10]
0040253C │. 2BE0               SUB ESP,EAX
0040253E │. 53                 PUSH EBX
0040253F │. 56                 PUSH ESI
00402540 │. 57                 PUSH EDI
00402541 │. A1 04A04000        MOV EAX,DWORD PTR DS:[40A004]
00402546 │. 3145 FC            XOR DWORD PTR SS:[EBP-4],EAX
00402549 │. 33C5               XOR EAX,EBP
0040254B │. 50                 PUSH EAX
0040254C │. 8965 E8            MOV DWORD PTR SS:[EBP-18],ESP
0040254F │. FF75 F8            PUSH DWORD PTR SS:[EBP-8]
00402552 │. 8B45 FC            MOV EAX,DWORD PTR SS:[EBP-4]
00402555 │. C745 FC FEFFFF     MOV DWORD PTR SS:[EBP-4],-2
0040255C │. 8945 F8            MOV DWORD PTR SS:[EBP-8],EAX
0040255F │. 8D45 F0            LEA EAX,DWORD PTR SS:[EBP-10]
00402562 │. 64:A3 0000000      MOV DWORD PTR FS:[0],EAX
00402568 └. C3                 RETN
00402569 ┌$ 8B4D F0            MOV ECX,DWORD PTR SS:[EBP-10]
0040256C │. 64:890D 000000     MOV DWORD PTR FS:[0],ECX
00402573 │. 59                 POP ECX
00402574 │. 5F                 POP EDI
00402575 │. 5F                 POP EDI
00402576 │. 5E                 POP ESI
00402577 │. 5B                 POP EBX
00402578 │. 8BE5               MOV ESP,EBP
```

Part 3 Ollydbg 실습(Restart, Step Into, Step Over, Execute till Return 만으로 main() 함수 찾기)



```
0040105B   .  B8 4D5A0000     MOV EAX,5A4D
00401060   .  66:3905 000040  CMP WORD PTR DS:[400000],AX
00401067   .v 75 38           JNZ SHORT HelloWor.004010A1
00401069   .  A1 3C004000     MOV EAX,DWORD PTR DS:[40003C]
0040106E   .  81B8 00004000   CMP DWORD PTR DS:[EAX+400000],4550
00401078   .v 75 27           JNZ SHORT HelloWor.004010A1
0040107A   .  B9 0B010000     MOV ECX,10B
0040107F   .  66:3988 180040  CMP WORD PTR DS:[EAX+400018],CX
00401086   .v 75 19           JNZ SHORT HelloWor.004010A1
00401088   .  83B8 74004000   CMP DWORD PTR DS:[EAX+400074],0E
0040108F   .v 76 10           JBE SHORT HelloWor.004010A1
00401091   .  33C9            XOR ECX,ECX
00401093   .  3988 E8004000   CMP DWORD PTR DS:[EAX+4000E8],ECX
00401099   .  0F95C1          SETNE CL
0040109C   .  894D E4         MOV DWORD PTR SS:[EBP-1C],ECX
0040109F   .v EB 04           JMP SHORT HelloWor.004010A5
004010A1   >  8365 E4 00      AND DWORD PTR SS:[EBP-1C],0
004010A5   >  6A 01           PUSH 1                              [Arg1 = 00000001
004010A7   .  E8 48140000     CALL HelloWor.004024F4              [HelloWor.004024F4
004010AC   .  59              POP ECX
004010AD   .  85C0            TEST EAX,EAX
004010AF   .v 75 08           JNZ SHORT HelloWor.004010B9
004010B1   .  6A 1C           PUSH 1C
004010B3   .  E8 6EFFFFFF     CALL HelloWor.00401026
004010B8   .  59              POP ECX
004010B9   >  E8 A9120000     CALL HelloWor.00402367
004010BE   .  85C0            TEST EAX,EAX
004010C0   .v 75 08           JNZ SHORT HelloWor.004010CA
004010C2   .  6A 10           PUSH 10
```

Part 3 Ollydbg 실습(Restart, Step Into, Step Over, Execute till Return 만으로 main() 함수 찾기)

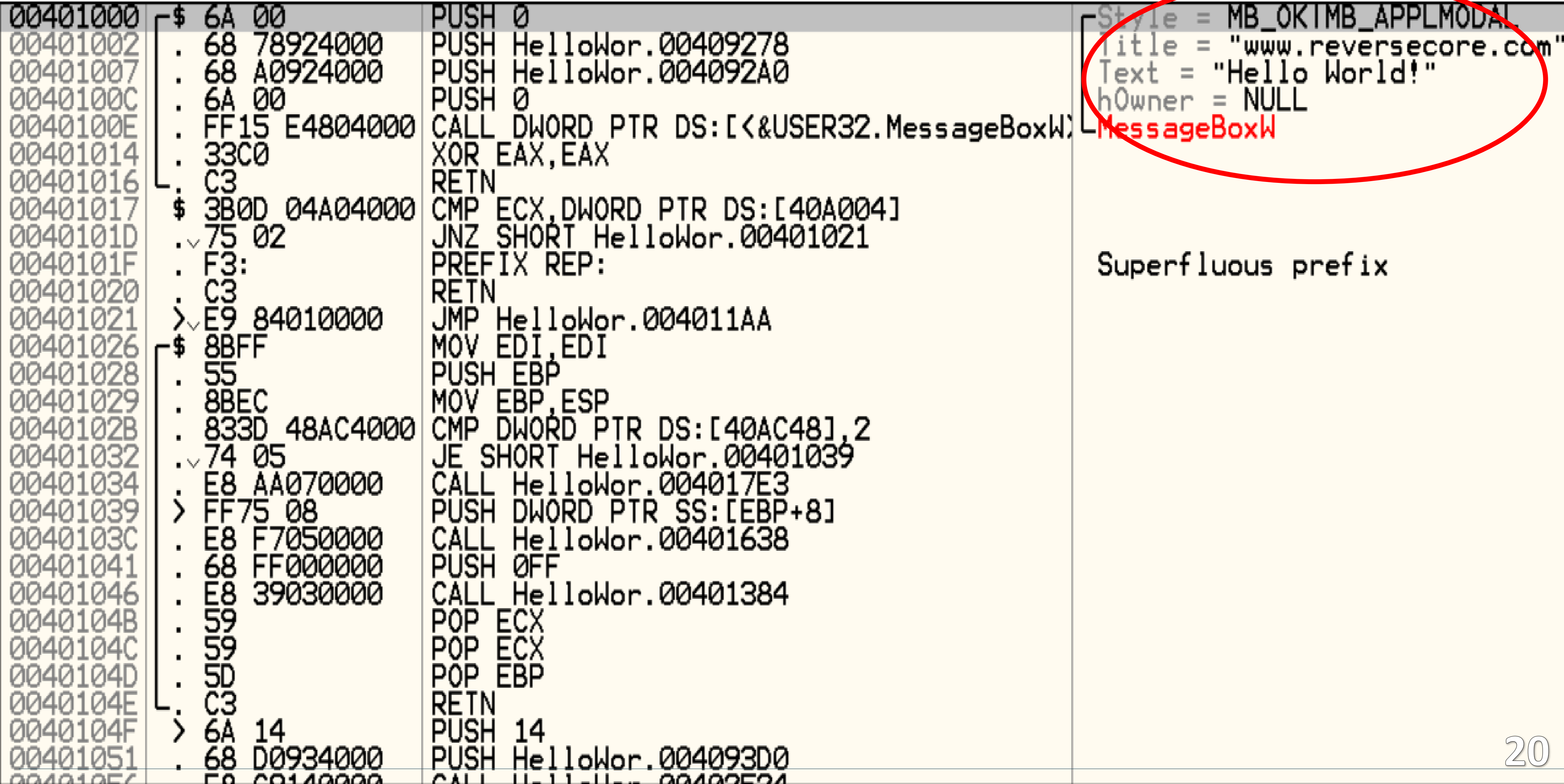


```
00401109  > E8 6F080000     CALL HelloWor.0040197D
0040110E  . 85C0            TEST EAX,EAX
00401110  .v7D 08           JGE SHORT HelloWor.0040111A
00401112  . 6A 09           PUSH 9
00401114  . E8 17020000     CALL HelloWor.00401330
00401119  . 59              POP ECX
0040111A  > 6A 01           PUSH 1                                   ┌Arg1 = 00000001
0040111C  . E8 CE020000     CALL HelloWor.004013EF                   └HelloWor.004013EF
00401121  . 59              POP ECX
00401122  . 85C0            TEST EAX,EAX
00401124  .v74 07           JE SHORT HelloWor.0040112D
00401126  . 50              PUSH EAX
00401127  . E8 04020000     CALL HelloWor.00401330
0040112C  . 59              POP ECX
0040112D  > A1 8CAF4000     MOV EAX,DWORD PTR DS:[40AF8C]
00401132  . A3 90AF4000     MOV DWORD PTR DS:[40AF90],EAX
00401137  . 50              PUSH EAX
00401138  . FF35 80AF4000   PUSH DWORD PTR DS:[40AF80]
0040113E  . FF35 78AF4000   PUSH DWORD PTR DS:[40AF78]
00401144  . E8 B7FEFFFF     CALL HelloWor.00401000
00401149  . 83C4 0C         ADD ESP,0C
0040114C  . 8945 E0         MOV DWORD PTR SS:[EBP-20],EAX
0040114F  . 837D E4 00      CMP DWORD PTR SS:[EBP-1C],0
00401153  .v75 06           JNZ SHORT HelloWor.0040115B
00401155  . 50              PUSH EAX
00401156  . E8 45040000     CALL HelloWor.004015A0
0040115B  > E8 6C040000     CALL HelloWor.004015CC
00401160  .vEB 2E           JMP SHORT HelloWor.00401190
```

www.reversecore.com

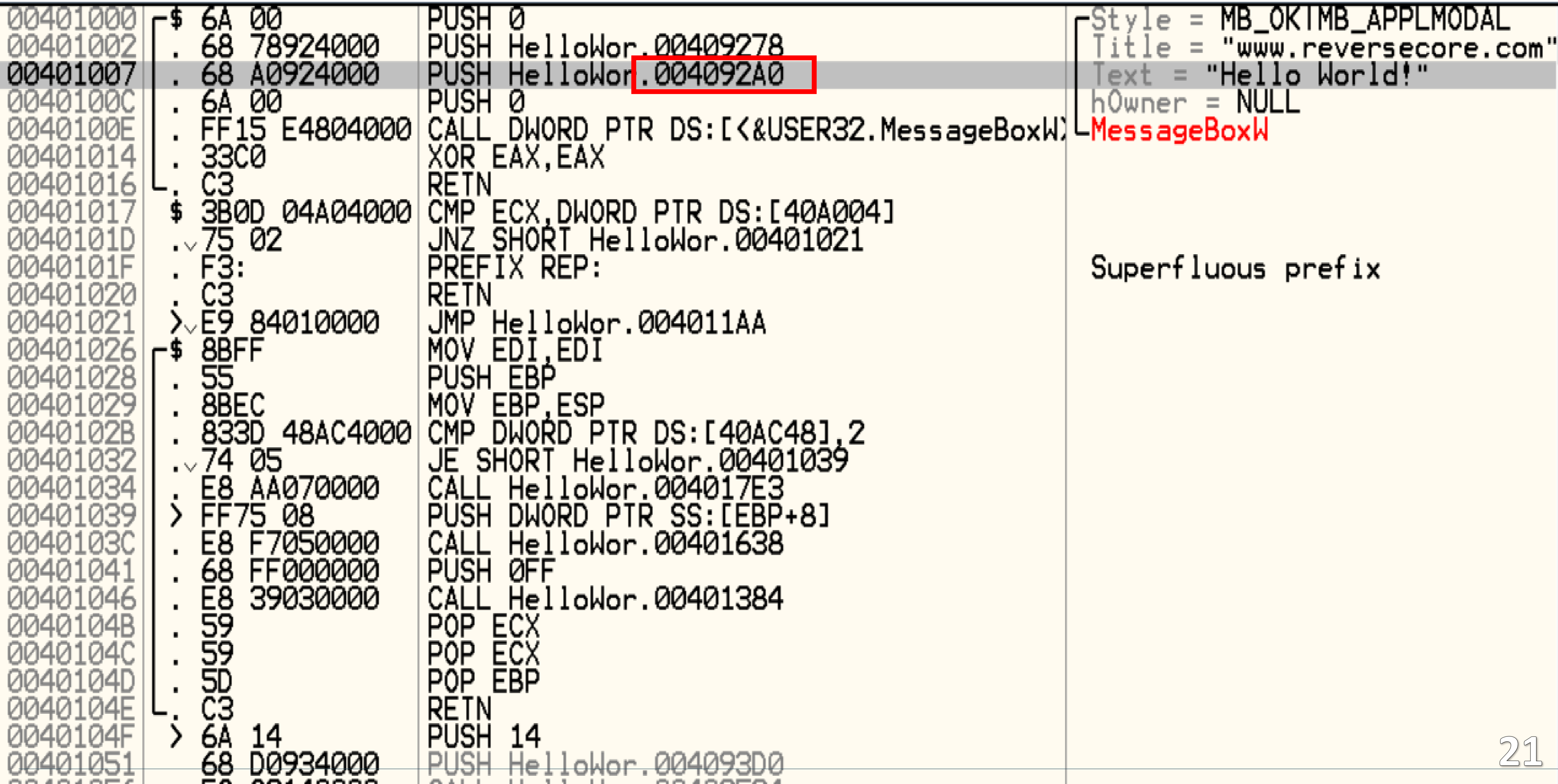
Hello World!

Part 3 Ollydbg 실습(Restart,Step Into,Step Over,Execute till Return 만으로 main() 함수 찾기)



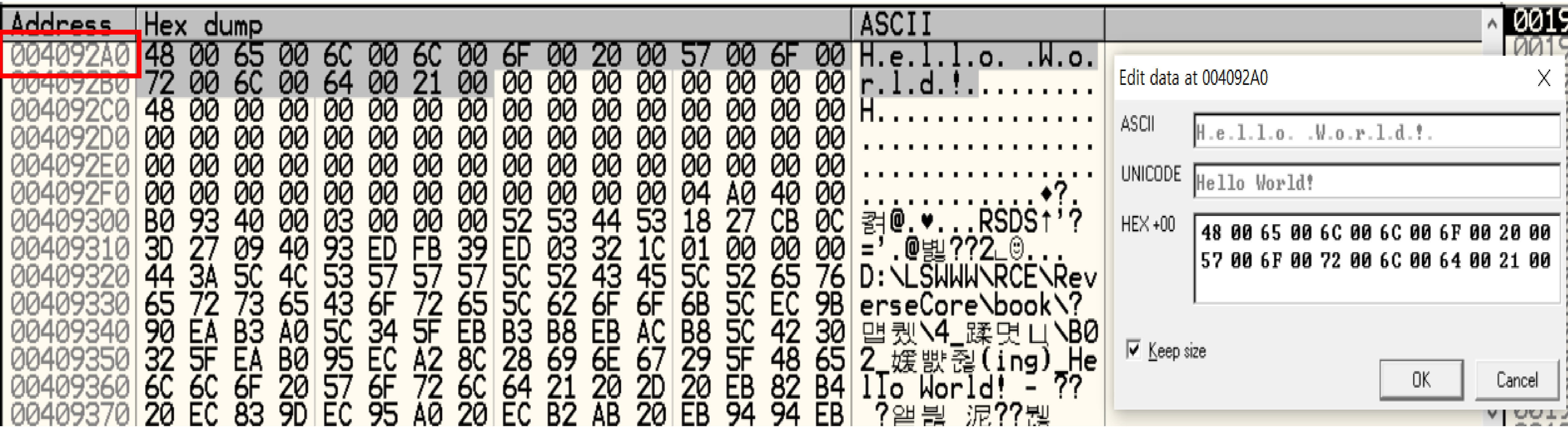
```
00401000 ┌$ 6A 00          PUSH 0                                     ┌Style = MB_OK|MB_APPLMODAL
00401002 │. 68 78924000    PUSH HelloWor.00409278                     │Title = "www.reversecore.com"
00401007 │. 68 A0924000    PUSH HelloWor.004092A0                     │Text = "Hello World!"
0040100C │. 6A 00          PUSH 0                                     │hOwner = NULL
0040100E │. FF15 E4804000  CALL DWORD PTR DS:[<&USER32.MessageBoxW>   └MessageBoxW
00401014 │. 33C0           XOR EAX,EAX
00401016 └. C3             RETN
00401017  $ 3B0D 04A04000  CMP ECX,DWORD PTR DS:[40A004]
0040101D  .v75 02          JNZ SHORT HelloWor.00401021
0040101F  . F3:            PREFIX REP:                                 Superfluous prefix
00401020  . C3             RETN
00401021  >vE9 84010000    JMP HelloWor.004011AA
00401026 ┌$ 8BFF           MOV EDI,EDI
00401028 │. 55             PUSH EBP
00401029 │. 8BEC           MOV EBP,ESP
0040102B │. 833D 48AC4000  CMP DWORD PTR DS:[40AC48],2
00401032 │.v74 05          JE SHORT HelloWor.00401039
00401034 │. E8 AA070000    CALL HelloWor.004017E3
00401039 │> FF75 08        PUSH DWORD PTR SS:[EBP+8]
0040103C │. E8 F7050000    CALL HelloWor.00401638
00401041 │. 68 FF000000    PUSH 0FF
00401046 │. E8 39030000    CALL HelloWor.00401384
0040104B │. 59             POP ECX
0040104C │. 59             POP ECX
0040104D │. 5D             POP EBP
0040104E └. C3             RETN
0040104F  > 6A 14          PUSH 14
00401051  . 68 D0934000    PUSH HelloWor.004093D0
```

Part 3 Ollydbg 실습(Restart, Step Into, Step Over, Execute till Return 만으로 main() 함수찾기)



```
00401000  ┌$ 6A 00          PUSH 0                                      ┌Style = MB_OK|MB_APPLMODAL
00401002  │. 68 78924000    PUSH HelloWor.00409278                      │Title = "www.reversecore.com"
00401007  │. 68 A0924000    PUSH HelloWor.004092A0                      │Text = "Hello World!"
0040100C  │. 6A 00          PUSH 0                                      │hOwner = NULL
0040100E  │. FF15 E4804000  CALL DWORD PTR DS:[<&USER32.MessageBoxW>    └MessageBoxW
00401014  │. 33C0           XOR EAX,EAX
00401016  └. C3             RETN
00401017   $ 3B0D 04A04000  CMP ECX,DWORD PTR DS:[40A004]
0040101D   .v75 02          JNZ SHORT HelloWor.00401021
0040101F   . F3:            PREFIX REP:                                  Superfluous prefix
00401020   . C3             RETN
00401021   >vE9 84010000    JMP HelloWor.004011AA
00401026  ┌$ 8BFF           MOV EDI,EDI
00401028  │. 55             PUSH EBP
00401029  │. 8BEC           MOV EBP,ESP
0040102B  │. 833D 48AC4000  CMP DWORD PTR DS:[40AC48],2
00401032  │.v74 05          JE SHORT HelloWor.00401039
00401034  │. E8 AA070000    CALL HelloWor.004017E3
00401039  │> FF75 08        PUSH DWORD PTR SS:[EBP+8]
0040103C  │. E8 F7050000    CALL HelloWor.00401638
00401041  │. 68 FF000000    PUSH 0FF
00401046  │. E8 39030000    CALL HelloWor.00401384
0040104B  │. 59             POP ECX
0040104C  │. 59             POP ECX
0040104D  │. 5D             POP EBP
0040104E  └. C3             RETN
0040104F   > 6A 14          PUSH 14
00401051   . 68 D0934000    PUSH HelloWor.004093D0
```

Part 3 Ollydbg 실습(Restart,Step Into,Step Over,Execute till Return 만으로 main() 함수 찾기)



```
Address   Hex dump                                          ASCII
004092A0  48 00 65 00 6C 00 6C 00 6F 00 20 00 57 00 6F 00  H.e.l.l.o. .W.o.
004092B0  72 00 6C 00 64 00 21 00 00 00 00 00 00 00 00 00  r.l.d.!.........
004092C0  48 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  H...............
004092D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004092E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004092F0  00 00 00 00 00 00 00 00 00 00 00 00 04 A0 40 00  ............♦?.
00409300  B0 93 40 00 03 00 00 00 52 53 44 53 18 27 CB 0C  쿼@.♥...RSDS↑'?
00409310  3D 27 09 40 93 ED FB 39 ED 03 32 1C 01 00 00 00  ='.@뷀??2∟☺...
00409320  44 3A 5C 4C 53 57 57 57 5C 52 43 45 5C 52 65 76  D:\LSWWW\RCE\Rev
00409330  65 72 73 65 43 6F 72 65 5C 62 6F 6F 6B 5C EC 9B  erseCore\book\?
00409340  90 EA B3 A0 5C 34 5F EB B3 B8 EB AC B8 5C 42 30  맵췘\4_蹂몃ㄴ\B0
00409350  32 5F EA B0 95 EC A2 8C 28 69 6E 67 29 5F 48 65  2_媛뺤쥪(ing)_He
00409360  6C 6C 6F 20 57 6F 72 6C 64 21 20 2D 20 EB 82 B4  llo World! - ??
00409370  20 EC 83 9D EC 95 A0 20 EC B2 AB 20 EB 94 94 EB   ?앸븘 泥??뷀
```

Edit data at 004092A0

ASCII: H.e.l.l.o. .W.o.r.l.d.!.

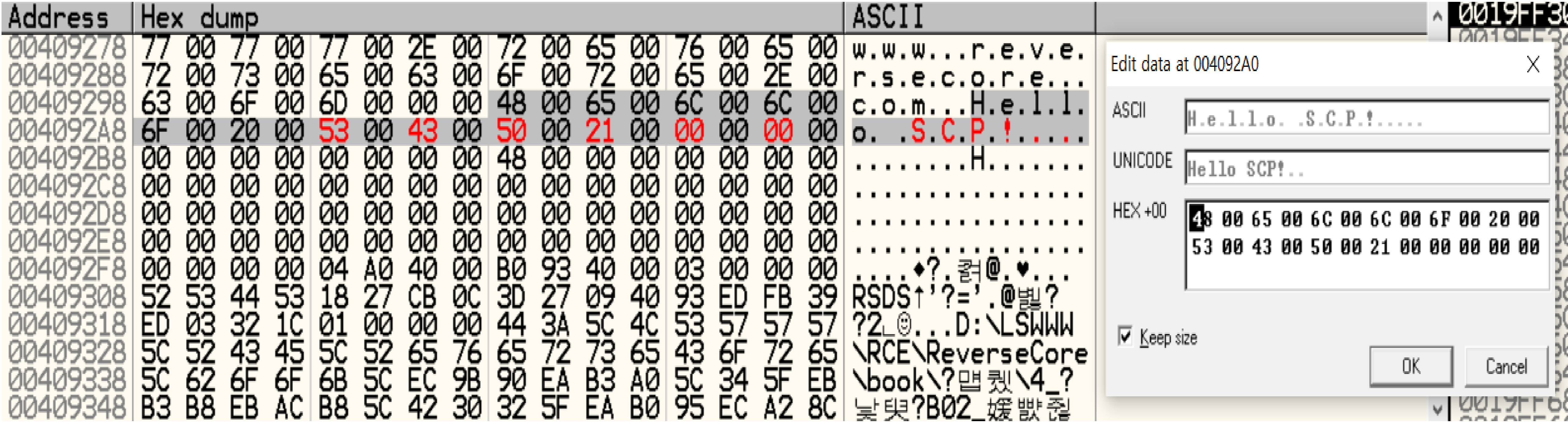
UNICODE: Hello World!

HEX +00:
```
48 00 65 00 6C 00 6C 00 6F 00 20 00
57 00 6F 00 72 00 6C 00 64 00 21 00
```

☑ Keep size

응용) HELLO WORLD!를 HELLO SCP!로 만들어보기

Part 3 Ollydbg 실습(HELLOWORLD!를 HELLOSCP!로 만들어 보기)



```
Address   Hex dump                                          ASCII
00409278  77 00 77 00 77 00 2E 00 72 00 65 00 76 00 65 00  w.w.w...r.e.v.e.
00409288  72 00 73 00 65 00 63 00 6F 00 72 00 65 00 2E 00  r.s.e.c.o.r.e...
00409298  63 00 6F 00 6D 00 00 00 48 00 65 00 6C 00 6C 00  c.o.m...H.e.l.l.
004092A8  6F 00 20 00 53 00 43 00 50 00 21 00 00 00 00 00  o. .S.C.P.!.....
004092B8  00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00  ........H.......
004092C8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004092D8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004092E8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004092F8  00 00 00 00 04 A0 40 00 B0 93 40 00 03 00 00 00  ....♦?.쥠@.♥...
00409308  52 53 44 53 18 27 CB 0C 3D 27 09 40 93 ED FB 39  RSDS↑'?='.@벨?
00409318  ED 03 32 1C 01 00 00 00 44 3A 5C 4C 53 57 57 57  ?2∟☺...D:\LSWWW
00409328  5C 52 43 45 5C 52 65 76 65 72 73 65 43 6F 72 65  \RCE\ReverseCore
00409338  5C 62 6F 6F 6B 5C EC 9B 90 EA B3 A0 5C 34 5F EB  \book\?맵켔\4_?
00409348  B3 B8 EB AC B8 5C 42 30 32 5F EA B0 95 EC A2 8C  놓 뵛?B02_媛 뻜 좰
```

Edit data at 004092A0

ASCII: H.e.l.l.o. .S.C.P.!.....

UNICODE: Hello SCP!..

HEX +00:
```
48 00 65 00 6C 00 6C 00 6F 00 20 00
53 00 43 00 50 00 21 00 00 00 00 00
```

☑ Keep size

Part 3 **Ollydbg 실습**(HELLOWORLD!를 HELLOSCP!로 만들어 보기)

직접 보여드리겠습니다!

(참고)

dreamhack

악성 코드 분석가의 리버싱 이야기

리버싱 핵심원리

이승원 지음 | 인사이트

느낀 점 및 Q&A

단순하게 설명할 수 없다면 제대로 이해하지 못한 것이다.

아인슈타인