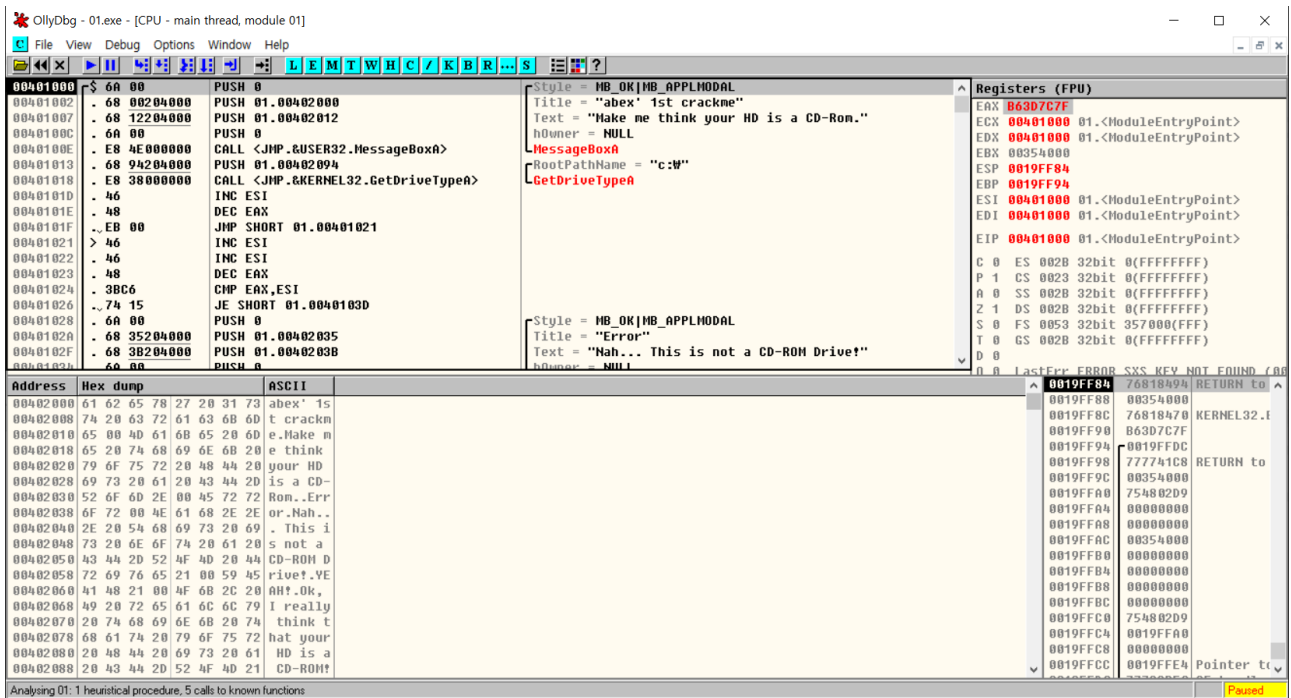

[CodeEngn]

Basic RCE L01

Basic RCE L01

HDD를 CD-Rom으로 인식시키기 위해서는 GetDriveTypeA의 리턴값이 무엇이 되어야 하는가



OllyDbg - 01.exe - [CPU - main thread, module 01]

File View Debug Options Window Help

Address Hex dump ASCII

00401000 6A 00 PUSH 0
00401002 68 00204000 PUSH 01.00402000
00401007 68 12204000 PUSH 01.00402012
0040100C 6A 00 PUSH 0
0040100E E8 4E000000 CALL <JMP.&USER32.MessageBoxA>
00401013 68 94204000 PUSH 01.00402094
00401018 E8 38000000 CALL <JMP.&KERNEL32.GetDriveTypeA>
0040101D 46 INC ESI
0040101E 48 DEC EAX
0040101F EB 00 JMP SHORT 01.00401021
00401021 46 INC ESI
00401022 46 INC ESI
00401023 48 DEC EAX
00401024 3BC6 CMP EAX,ESI
00401026 74 15 JE SHORT 01.0040103D
00401028 6A 00 PUSH 0
0040102A 68 35204000 PUSH 01.00402035
0040102F 68 3B204000 PUSH 01.0040203B
00401032 6A 00 PUSH 0

Style = MB_OK|MB_APPLMODAL
Title = "abex' 1st crackme"
Text = "Make me think your HD is a CD-Rom."
hOwner = NULL
MessageBoxA
RootPathName = "c:\\"
GetDriveTypeA

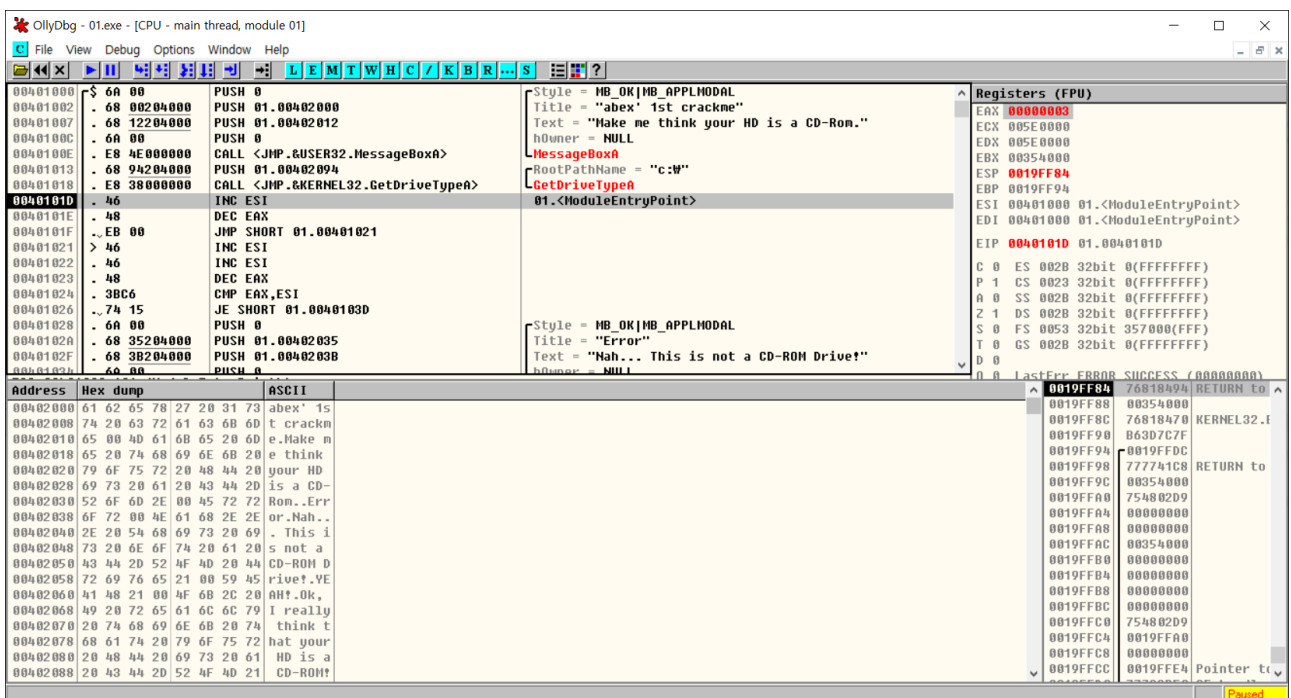
Registers (FPU)
EAX 00401000 01.<ModuleEntryPoint>
ECX 00401000 01.<ModuleEntryPoint>
EDX 00354000
EBX 0019FF84
ESP 00401000 01.<ModuleEntryPoint>
ESI 00401000 01.<ModuleEntryPoint>
EDI 00401000 01.<ModuleEntryPoint>
EIP 00401000 01.<ModuleEntryPoint>
C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 1 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 357000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
I 0 LastErr ERROR SXS KEY NOT FOUND (00000000)

0019FF84 76818A94 RETURN to
0019FF88 00354000
0019FF8C 76818A70 KERNEL32.I
0019FF90 B63D7C7F
0019FF94 0019FFDC
0019FF98 777741C8 RETURN to
0019FF9C 00354000
0019FFA0 754802D9
0019FFA4 00000000
0019FFA8 00000000
0019FFAC 00354000
0019FFB0 00000000
0019FFB4 00000000
0019FFB8 00000000
0019FFBC 00000000
0019FFC0 754802D9
0019FFC4 0019FFA0
0019FFC8 00000000
0019FFCC 0019FFE4 Pointer to

Analysing 01: 1 heuristic procedure, 5 calls to known functions

Paused

처음 프로그램을 실행 시켰을때 화면이다.



OllyDbg - 01.exe - [CPU - main thread, module 01]

File View Debug Options Window Help

Address Hex dump ASCII

00401000 6A 00 PUSH 0
00401002 68 00204000 PUSH 01.00402000
00401007 68 12204000 PUSH 01.00402012
0040100C 6A 00 PUSH 0
0040100E E8 4E000000 CALL <JMP.&USER32.MessageBoxA>
00401013 68 94204000 PUSH 01.00402094
00401018 E8 38000000 CALL <JMP.&KERNEL32.GetDriveTypeA>
0040101D 46 INC ESI
0040101E 48 DEC EAX
0040101F EB 00 JMP SHORT 01.00401021
00401021 46 INC ESI
00401022 46 INC ESI
00401023 48 DEC EAX
00401024 3BC6 CMP EAX,ESI
00401026 74 15 JE SHORT 01.0040103D
00401028 6A 00 PUSH 0
0040102A 68 35204000 PUSH 01.00402035
0040102F 68 3B204000 PUSH 01.0040203B
00401032 6A 00 PUSH 0

Style = MB_OK|MB_APPLMODAL
Title = "abex' 1st crackme"
Text = "Make me think your HD is a CD-Rom."
hOwner = NULL
MessageBoxA
RootPathName = "c:\\"
GetDriveTypeA

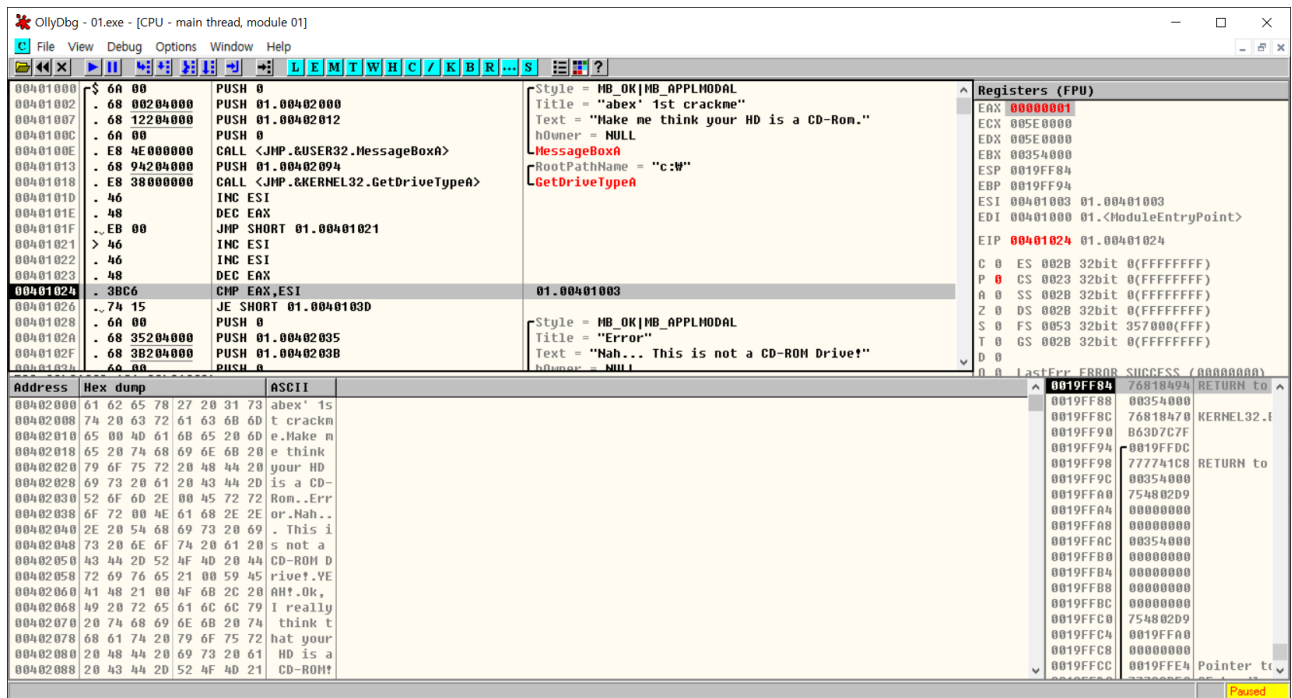
Registers (FPU)
EAX 00000003
ECX 005E0000
EDX 005E0000
EBX 00354000
ESP 0019FF84
EBP 0019FF94
ESI 00401000 01.<ModuleEntryPoint>
EDI 00401000 01.<ModuleEntryPoint>
EIP 0040101D 01.0040101D
C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 1 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 357000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
I 0 LastErr ERROR SUCCESS (00000000)

0019FF84 76818A94 RETURN to
0019FF88 00354000
0019FF8C 76818A70 KERNEL32.I
0019FF90 B63D7C7F
0019FF94 0019FFDC
0019FF98 777741C8 RETURN to
0019FF9C 00354000
0019FFA0 754802D9
0019FFA4 00000000
0019FFA8 00000000
0019FFAC 00354000
0019FFB0 00000000
0019FFB4 00000000
0019FFB8 00000000
0019FFBC 00000000
0019FFC0 754802D9
0019FFC4 0019FFA0
0019FFC8 00000000
0019FFCC 0019FFE4 Pointer to

Analysing 01: 1 heuristic procedure, 5 calls to known functions

Paused

현재 GetDriveTypeA 의 리턴값은 3 (EAX 에 3 이 들어갔음) 이다.



ESI = 401000, EAX = 3 이라는 값을 가지고 아래 명령어를 실행한다.

```
INC ESI
DEC EAX
INC ESI
INC ESI
DEC EAX
```

그리고 EAX 와 ESI 를 비교한다.

비교하고 ZF 가 1 이면 40103D 로 점프를 하고, 아니면 401028 로 가게 된다.

GetDriveTypeA 반환값에 대해서 알아보았다.

Return code/value	Description
<u>DRIVE_UNKNOWN</u> 0	The drive type cannot be determined.
<u>DRIVE_NO_ROOT_DIR</u> 1	The root path is invalid; for example, there is no volume mounted at the specified path.
<u>DRIVE_REMOVABLE</u> 2	The drive has removable media; for example, a floppy drive, thumb drive, or flash card reader.
<u>DRIVE_FIXED</u> 3	The drive has fixed media; for example, a hard disk drive or flash drive.
<u>DRIVE_REMOTE</u> 4	The drive is a remote (network) drive.
<u>DRIVE_CDROM</u> 5	The drive is a CD-ROM drive.
<u>DRIVE_RAMDISK</u> 6	The drive is a RAM disk.

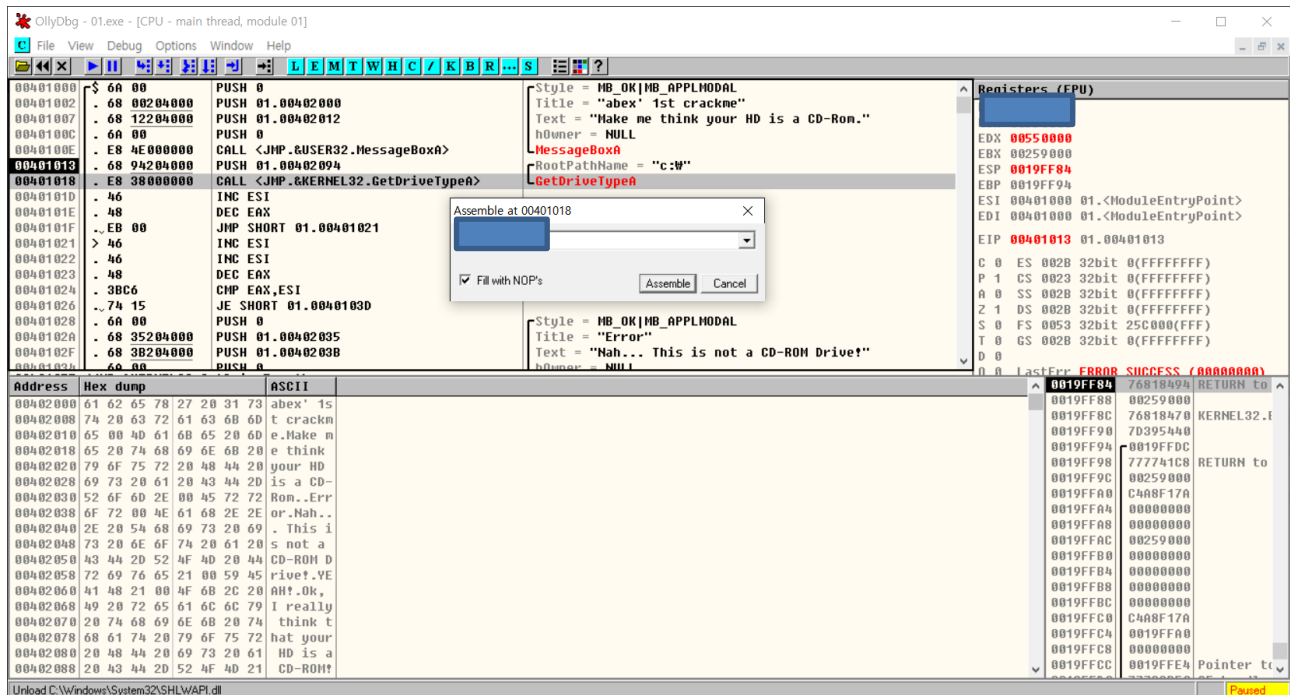
해당 드라이브가 하드디스크 또는 flash 드라이브라면, 반환값 3 이다.

해당 드라이브가 CD-ROM 드라이브라면 반환값 5 이다.

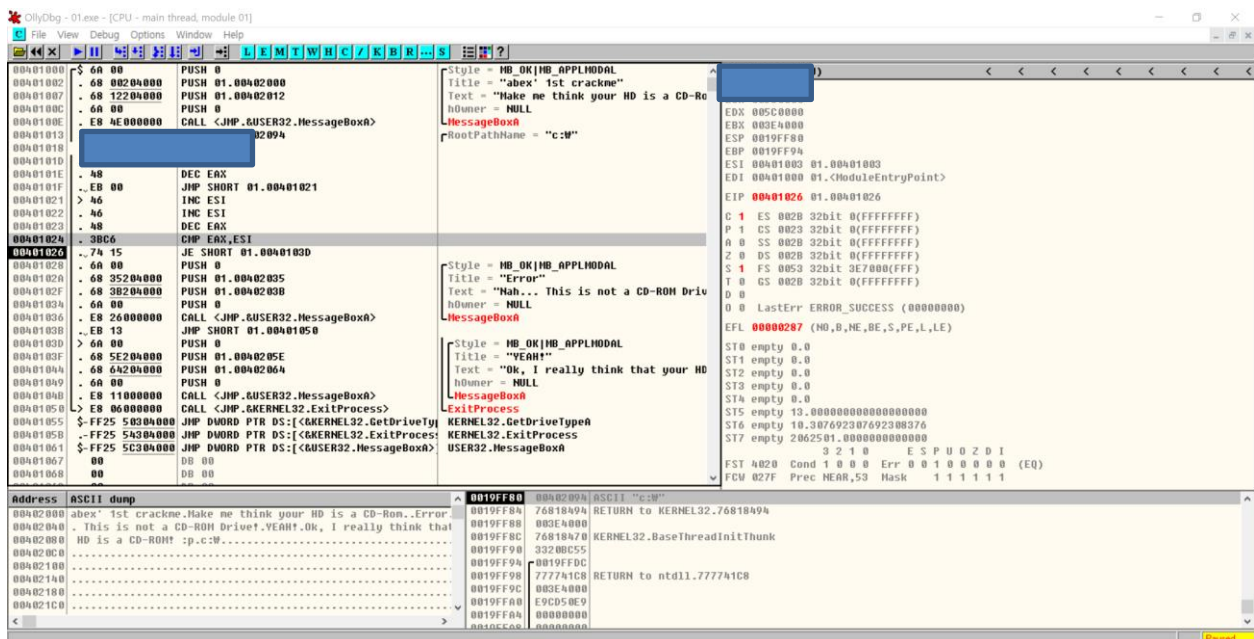
그럼 CD-ROM 으로 인식시키기 위해서는 반환값이 5 가 되어야한다.

= 변외편 =

하지만,



EAX 에 ? 를 넣고, 프로그램을 실행해본 결과이다.

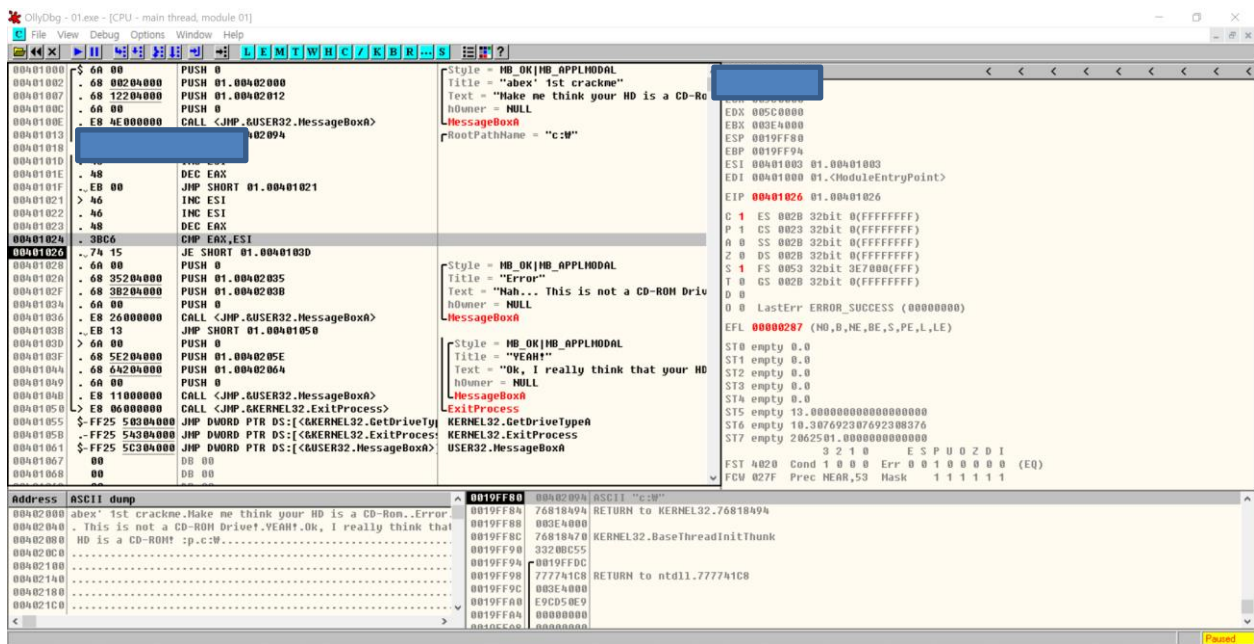


ZF 가 1 이 되지 않았다.

GetDriveTypeA 에 반환값이 ? 가 되었어도, 해당 프로그램은

“Ok, I really think that your HD is a CD-ROM! :p” 이 문구를 띄워주지 않는다.

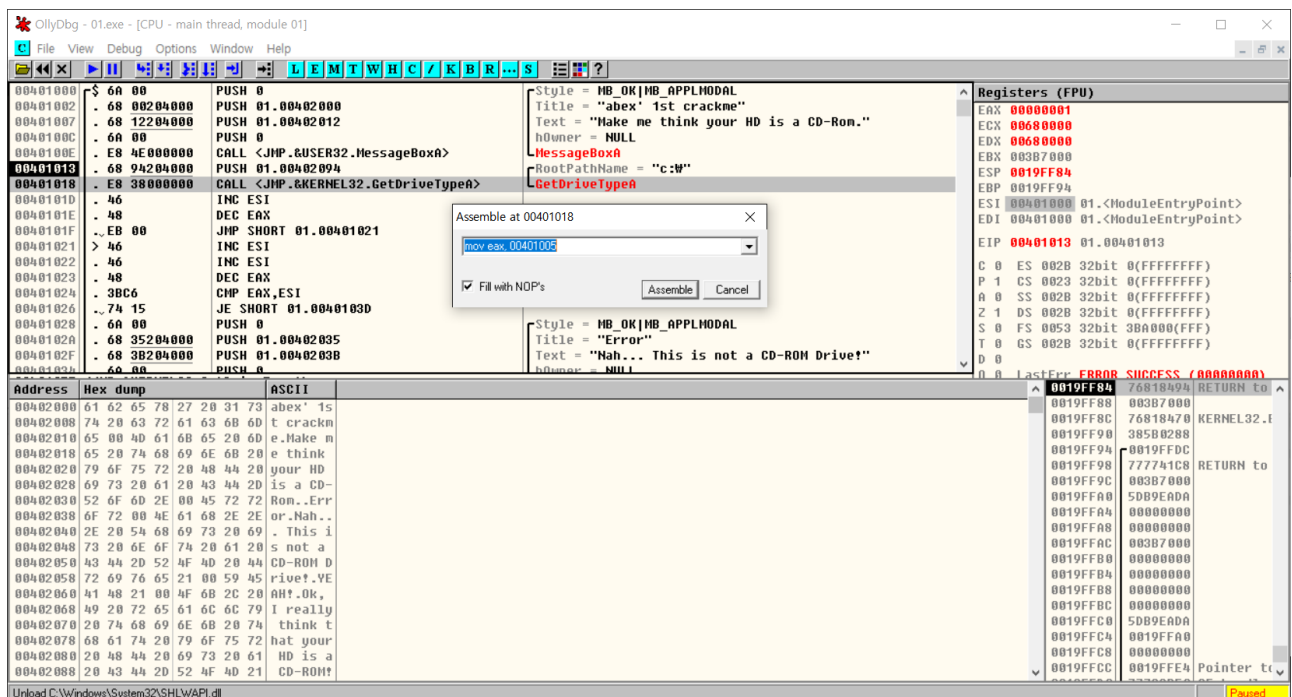
그러면 ZF 가 1 이 되기 위해서는 GetDriveTypeA 가 몇이 되야 될까?



CMP 에서 ESI 의 값은 401003 이다.

그래서, ZF 가 1 이 되려면, GetDriveTypeA 의 반환값이 401005 가 되어야 한다.

아래 사진들은 GetDriveTypeA 반환값을 401005 로 설정했을때 결과이다.



mov eax, 401005

OllyDbg - 01.exe - [CPU - main thread, module 01]

File View Debug Options Window Help

Assembly:

```

00401000 6A 00 PUSH 0
00401002 68 00204000 PUSH 01.00402000
00401007 68 12204000 PUSH 01.00402012
0040100C 6A 00 PUSH 0
0040100E E8 4E000000 CALL <JMP.&USER32.MessageBoxA>
00401013 68 94204000 PUSH 01.00402094
00401018 B8 05104000 MOV EAX,01.00401005
0040101D 46 INC ESI
0040101E 48 DEC EAX
0040101F EB 00 JMP SHORT 01.00401021
00401021 46 INC ESI
00401022 46 INC ESI
00401023 48 DEC EAX
00401024 3BC6 CMP EAX,ESI
00401026 74 15 JE SHORT 01.0040103D
00401028 6A 00 PUSH 0
0040102A 68 35204000 PUSH 01.00402035
0040102F 68 3B204000 PUSH 01.0040203B
00401034 6A 00 PUSH 0

```

Registers (FPU):

EAX 00401003 01.00401003
ECX 00680000
EDX 00680000
EBX 003B7000
ESP 0019FF80
EBP 0019FF94
ESI 00401003 01.00401003
EDI 00401000 01.<ModuleEntryPoint>
EIP 00401026 01.00401026
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 3BA000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
I 0 LastErr ERROR SUCCESS (00000000)

Address Hex dump ASCII

00402000	61 62 65 78 27 20 31 73	abex' 1s
00402008	74 20 63 72 61 63 68 6D	t crackme
00402010	65 00 4D 61 68 65 20 6D	e.Hake m
00402018	65 20 74 68 69 6E 68 20	e think
00402020	79 6F 75 72 20 A8 44 20	your HD
00402028	69 73 20 61 20 43 44 20	is a CD-
00402030	52 6F 6D 2E 00 45 72 72	Rom..Err
00402038	6F 72 00 4E 61 68 2E 2E	or.Nah..
00402040	2E 20 54 68 69 73 20 69	. This i
00402048	73 20 6E 6F 74 20 61 20	s not a
00402050	43 44 20 52 4F 4D 20 A4	CD-ROM D
00402058	72 69 76 65 21 00 59 45	rive?.VE
00402060	41 48 21 00 4F 68 2C 20	AH!.Ok,
00402068	49 20 72 65 61 6C 6C 79	I really
00402070	20 74 68 69 6E 68 20 74	think t
00402078	68 61 74 20 79 6F 75 72	hat your
00402080	20 48 44 20 69 73 20 61	HD is a
00402088	20 43 44 20 52 4F 4D 21	CD-ROM!

JE 를 하기 전에,ZF 가 1 이 된 것을 확인할 수 있다.

OllyDbg - 01.exe - [CPU - main thread, module 01]

File View Debug Options Window Help

Assembly:

```

0040103D 6A 00 PUSH 0
0040103F 68 5E204000 PUSH 01.0040205E
00401044 68 64204000 PUSH 01.00402064
00401049 6A 00 PUSH 0
0040104B E8 11000000 CALL <JMP.&USER32.MessageBoxA>
00401050 E8 06000000 CALL <JMP.&KERNEL32.ExitProcess>
00401055 FF25 5C304000 JMP DWORD PTR DS:[<&KERNEL32.GetDriveType>]
0040105B FF25 5C304000 JMP DWORD PTR DS:[<&KERNEL32.ExitProcess>]
00401061 00 DB 00
00401062 00 DB 00
00401063 00 DB 00
00401064 00 DB 00
00401065 00 DB 00
00401066 00 DB 00
00401067 00 DB 00
00401068 00 DB 00
00401069 00 DB 00
0040106A 00 DB 00
0040106B 00 DB 00
0040106C 00 DB 00
0040106D 00 DB 00
0040106E 00 DB 00
0040106F 00 DB 00
00401070 00 DB 00

```

Registers (FPU):

EAX 00000000
ECX 00000000
EDX 00000000
EBX 00800000
ESP 0019E5CC
EBP 0019E618
ESI 006A8878
EDI 006A87D0
EIP 7777A05C ntdll.7777A05C
C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 0 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 3BA000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
I 0 LastErr ERROR SUCCESS (00000000)

Address Hex dump ASCII

00402000	61 62 65 78 27 20 31 73	abex' 1s
00402008	74 20 63 72 61 63 68 6D	t crackme
00402010	65 00 4D 61 68 65 20 6D	e.Hake m
00402018	65 20 74 68 69 6E 68 20	e think
00402020	79 6F 75 72 20 A8 44 20	your HD
00402028	69 73 20 61 20 43 44 20	is a CD-
00402030	52 6F 6D 2E 00 45 72 72	Rom..Err
00402038	6F 72 00 4E 61 68 2E 2E	or.Nah..
00402040	2E 20 54 68 69 73 20 69	. This i
00402048	73 20 6E 6F 74 20 61 20	s not a
00402050	43 44 20 52 4F 4D 20 A4	CD-ROM D
00402058	72 69 76 65 21 00 59 45	rive?.VE
00402060	41 48 21 00 4F 68 2C 20	AH!.Ok,
00402068	49 20 72 65 61 6C 6C 79	I really
00402070	20 74 68 69 6E 68 20 74	think t
00402078	68 61 74 20 79 6F 75 72	hat your
00402080	20 48 44 20 69 73 20 61	HD is a
00402088	20 43 44 20 52 4F 4D 21	CD-ROM!

따라서 40103D 로 점프하게 되서, "Ok, I really think that your HD is a CD-ROM! :p" 문구가 나오게 되었다.