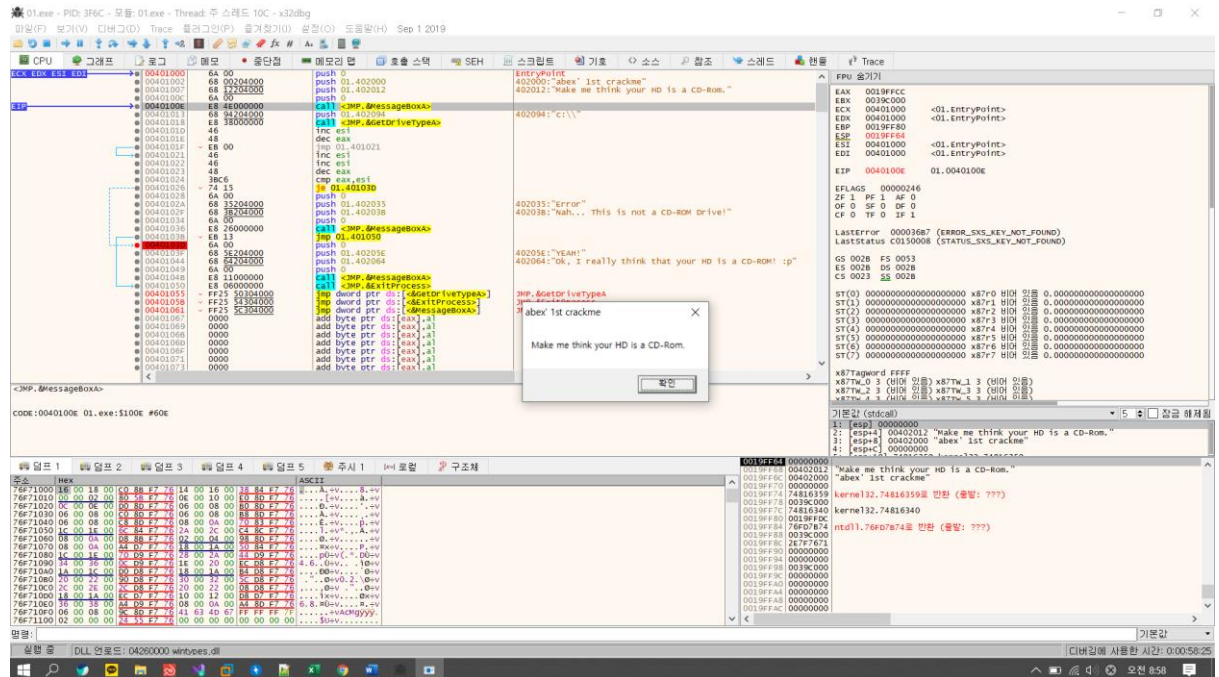
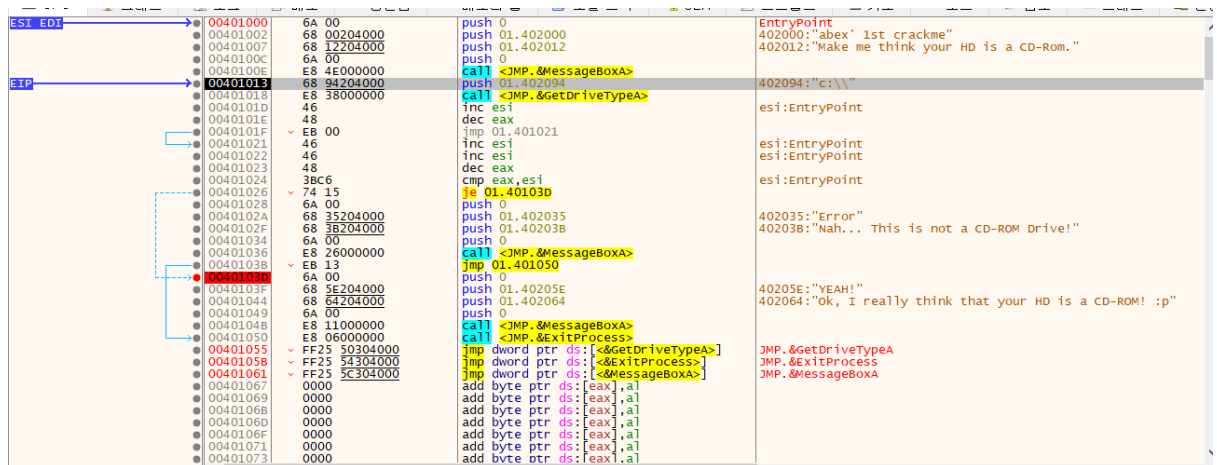


# 01.exe 풀이 해설



일단 프로그램을 구동 한 다음 구조를 살펴본다.



구조를 살펴보니 GetDriveTypeA를 실행 한 다음 리턴 값을 받고 비교를 하여 CD-Rom인지 아닌지를 확인 하는 프로그램 이다.

일단 작동이 시작 되면 메시지 박스를 출력한 다음 GetDriveTypeA API를 통해 리턴값을 eax에 저장을 하게 되는데 이때 인터넷 검색을 통해 어떤 리턴 값이 Cd-Rom 인지 찾아 보았다.

# Return Value

The return value specifies the type of drive, which can be one of the following values.

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

CD-ROM은 eax에 5를 리턴 받아야 한다는 사실을 알게 되었다.

그런 다음 GetDriveTypeA API를 실행 한다음의 레지스터값과 그다음에 실행되는 어셈블리어를 분석하였다.

```
00401000 6A 00          push 0
00401002 68 00204000   push 01.402000
00401007 68 12204000   push 01.402012
0040100C 6A 00          push 0
0040100E E8 4E000000   call <JMP.&MessageBoxA>
00401013 68 84204000   push 01.401094
00401018 E8 38000000   call <JMP.&GetDriveTypeA>
0040101D 46            inc esi
0040101F EB 00          jmp 01.401021
00401021 46            inc esi
00401022 46            inc esi
00401023 48            dec eax
00401024 3BC6          cmp eax,esi
00401026 74 15         je 01.40103D
00401028 6A 00          push 0
0040102A 68 35204000   push 01.402035
0040102F 68 3E204000   push 01.402038
00401034 6A 00          push 0
00401036 E8 26000000   call <JMP.&MessageBoxA>
0040103B 6A 00          push 0
0040103D EB 13          jmp 01.401050
0040103F 68 3E204000   push 01.40205E
00401044 68 3E204000   push 01.402064
00401049 6A 00          push 0
0040104B E8 11000000   call <JMP.&MessageBoxA>
00401050 E8 06000000   call <JMP.&ExitProcess>
00401055 FF25 50304000 jmp dword ptr ds:[<&GetDriveTypeA>]
00401058 FF25 54304000 jmp dword ptr ds:[<&ExitProcess>]
00401061 FF25 5C304000 jmp dword ptr ds:[<&MessageBoxA>]
00401067 0000          add byte ptr ds:[eax],al
00401069 0000          add byte ptr ds:[eax],al
0040106B 0000          add byte ptr ds:[eax],al
0040106D 0000          add byte ptr ds:[eax],al
0040106F 0000          add byte ptr ds:[eax],al
00401071 0000          add byte ptr ds:[eax],al
00401073 0000          add byte ptr ds:[eax],al

EntryPoint
402000:"abex' 1st crackme"
402012:"Make me think your HD is a CD-Rom."
402094:"c:\\\"
esi:EntryPoint
esi:EntryPoint
esi:EntryPoint
esi:EntryPoint
402035:"Error"
402038:"Nah... This is not a CD-ROM drive!"
40205E:"YEAH!"
402064:"Ok, I really think that your HD is a CD-ROM! :p"
JMP.&GetDriveTypeA
JMP.&ExitProcess
JMP.&MessageBoxA

FPU 보기
EAX 00000003
EBX 00225000
ECX 004E0000
EDX 004E0000
EBP 0019FF80
ESP 0019FF74
ESI 00401000 <01.EntryPoint>
EDI 00401000 <01.EntryPoint>
EIP 0040101D 01.0040101D
EFLAGS 00000244
ZF 1 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 0 IF 1
LastError 00000000 (ERROR_SUCCESS)
LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOUND)
GS 002B FS 0053
ES 002B DS 002B
CS 0023 SS 002B
DR0 00000000
DR1 00000000
DR2 00000000
DR3 00000000
DR6 00000000
DR7 00000000
```

GetDriveTypeA API의 리턴값은 3으로 반환을 받았다.

이때 CD-ROM의 리턴값은 5를 받아야 하기 때문에 EAX의 레지스터를 5로 수정 한다.

FPU 보기	
EAX	00000005
EBX	00225000
ECX	004E0000
EDX	004E0000
EBP	0019FF80
ESP	0019FF74
ESI	00401000 <01.EntryPoint>
EDI	00401000 <01.EntryPoint>

그다음 ESI를 1 증가시켜 401000 → 401001로 변경이 되었고

EAX를 1 다운 시켜 5 → 4로 변경이 되었다.

그 다음 JMP 401021로 이동한다.

그다음 ESI를 1씩 증가 두번을 하여 401001 → 401003으로 변경이 되었다.

그리고 EAX를 1를 다운 시켜 4 → 3으로 변경이 되었다.

이때 CMP를 하여 EAX와 ESI를 비교 하게 되는데

401003 과 3를 비교 하기 때문에 ZF는 0를 얻게 되고 CD-ROM이 아니라는 메시지가 출력 될것을 예상 하게 되었다.

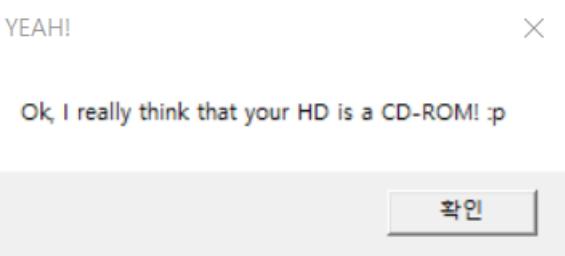
ESI의 초기값이 401000이라는 값이 오기 때문에 결국은 실제 "C:\ww"이 CD-ROM이여도 오작동 한다는 것을 알게 되었다.

고로 해결 방법은 여러가지 방법이 나오게 되는데 ESI또는EAX 둘중 하나를 같게 수정 하는 방법과

EAX	00000003
EBX	00225000
ECX	004E0000
EDX	004E0000
EBP	0019FF80
ESP	0019FF74
ESI	00000003
EDI	00401000

또는 CMP를 한다음 ZF를 1로 변경하여 JMP를 작동하게 만든다.

00401020	74 15	je 01.40103D	EFLAGS 00000246
00401028	6A 00	push 0	ZF 1 PF 1 AF 0
0040102A	68 35204000	push 01.402035	OF 0 SF 0 DF 0
0040102F	68 3B204000	push 01.40203B	CF 0 TF 0 IF 1
00401034	6A 00	push 0	
00401036	E8 26000000	call <JMP.&MessageBox>	
0040103B	EB 13	jmp 01.401050	LastError 00000000
0040103D	6A 00	push 0	LastStatus C0000034



그러면 최종적으로 이라는 화면을 볼수 있게 된다.

일단 이 문제를 제작자가 원하는 GetDriveTypeA의 리턴값은 5 이지만, 실제로 동작하도록 하는 리턴값은 401005이다.