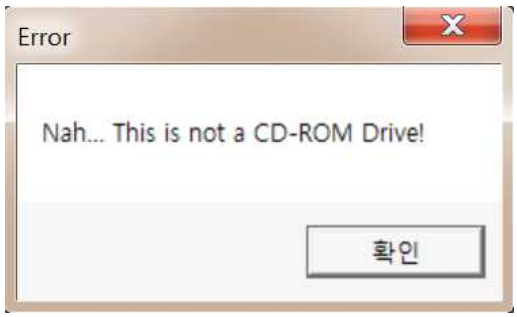
코드 엔진 Challenges: Basic 01

Author: abex
Korean: HDD를 CD-ROM으로 인식시키기 위해서는 GetDriveTypeA의 리턴값이 무엇이 되어야 하는가

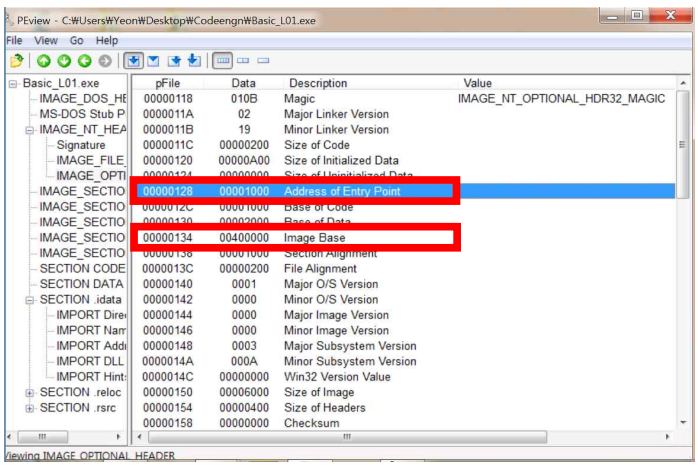
문제를 확인했으니 파일을 다운로드해서 실행해보도록 하자.



실행을 하면 "HDD를 CD-ROM으로 인식하게 하라" 라는 메시지 창이 나온다 . 그 후 확인 버튼 클릭 시 Error라는 타이틀의 "이것은 CD-ROM이 아니라"라는 메시지의 창이 나오고 프로그램은 종료된다.

프로그램을 확인했으니 리버싱을 위해 올리디버거로 파일을 열어보도록 한다.

그 전에 PEView를 이용해 문제의 EntryPoint와 사용하는 함수를 알아보자.

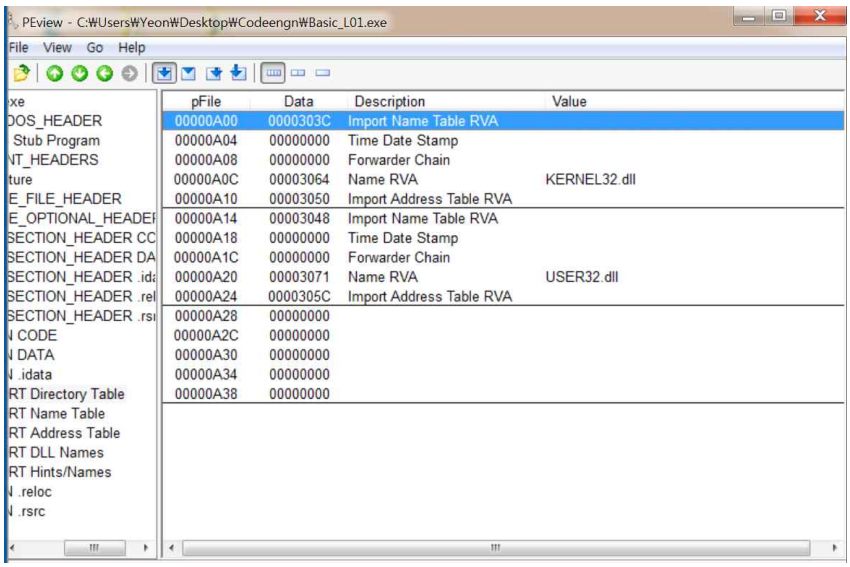


EntryPoint는 운영체제가 사용자 프로그램으로 최초로 제어를 넘기는 것으로 프로그래머가

만든 실행 코드가 최초로 실행되는 지점이다. PE구조의 모든 실행 파일은 헤더 영역에 엔트리 포인트가 상대주소(RVA)로 저장되어 있다. 프로그램은 로딩되면서 베이스 주소가 할당되고 메모리에 베이스 주소와 상대 주소가 더해진 위치에 (BaseAddress+RVA)데이터가 저장된다. PEView로 파일을 열었을 때 IMAGE_OPTIONAL_HEADER영역에 Address of Entry 항목에 데이터가 00001000을 볼 수 있는데 이는 메모리에 저장 될 때 사용될 상대 주소가 1000이라는 것을 의미한다 아래에 Image Base가 00400000로 저장되어 있으므로 엔트리 포인가 00401000이 된다는 것을 알 수 있다. (다음 보고서부터는 생략.)

이제 IAT(Iport Address Table)를 통해 실행 파일 안에 어떤 라이브러리에서 어떤 함수를 가져다 쓰는지 확인해보자. 로더는 PE 파일을 메모리로 로딩 할 때 IAT에 기록된 API 이름을 참조해서 프로그램이 사용할 수 있는 주소를 찾아 IAT안에 API를 가리키는 주소를 적어놓는다. 코드에서 라이브러리를 참조하는 부분은 IAT 내부에 있는 함수 주소를 사용한다.

IMPORT Directory Table은 참조하는 DLL을 알 수 있다. 이번 파일은 KERNELL32.dll과 USER32.dll을 참조하고 있다.



또한 INT(Import name Table)와 IAT(Import Address Table)에 대한 정보를 가진다. INT와 IAT는 PE파일에서 사용하는 외부라이브러리를 기록하는 핵심 영역이다. INT와 IAT는 참조하는 함수 이름을 가리키고 있다.

pFile	Data	Description	Value
00000A3C	0000307C	Hint/Name RVA	0000 GetDriveTypeA
00000A40	0000308C	Hint/Name RVA	0000 ExitProcess
00000A44	00000000	End of Imports	KERNEL32.dll
00000A48	0000309A	Hint/Name RVA	0000 MessageBoxA
00000A4C	00000000	End of Imports	USER32.dll

[INT Table]

pFile	Data	Description	Value
00000A50	0000307C	Hint/Name RVA	0000 GetDriveTypeA
00000A54	0000308C	Hint/Name RVA	0000 ExitProcess
00000A58	00000000	End of Imports	KERNEL32.dll
00000A5C	0000309A	Hint/Name RVA	0000 MessageBoxA
00000A60	00000000	End of Imports	USER32.dll

[IAT Table]

IAT와 INT테이블에서 0000307C, 0000308C, 0000309A가 들어있는 것을 확인할 수 있다. 이 해당 주소가 실제로 어떤 데이터를 가지리키고 있는지는 IMPORT Hints/Names 영역을 살펴보면되는데 실제 참조하는 함수의 이름의 ASCII코드 값이 들어가 있다.

RVA	Raw Data	Value
0000307C	00 00 47 65 74 44 72 69 76 65 54 79 70 65 41 00	..GetDriveTypeA.
0000308C	00 00 45 78 69 74 50 72 6F 63 65 73 73 00 00 00	..ExitProcess...
0000309C	4D 65 73 73 61 67 65 42 6F 78 41 00 00	MessageBoxA..

[Import Hints/Names 영역]

PE파일 상태에서는 IAT와 INT가 같은 값을 가지고 있지만 ,로더가 PE파일을 메모리로 로딩할 때 실제 참조해야하는 주소값을 가지고와서 IAT에 저장한다. PE 파일 내부에 있는 함수 이름을 가리키던 IAT 내부의 값은 함수를 가리키는 주소 값으로 변경된다. IAT의 RVA 값은 IMage Base값 40000000과 결합해서 디버거의 메모리영역에서 어떤 값이 저장되어 있는 확인할 수 있다. 주소 00003050에는 주소 75F98739가 저장되어 있는 것을 알 수 있다. 반면에 INT에는 PE파일에 저장된 값이 그대로 저장된다.

Address	Hex dump	ASCII
00403050	39 87 F9 75 4F 21 FB 75	9뇵u0!?
00403058	00 00 00 00 71 EA CC 75	....q圖u
00403060	00 00 00 00 4B 45 52 4E	....KERN
00403068	45 4C 33 32 2E 64 6C 6C	EL32.dll
00403070	00 55 53 45 52 33 32 2E	.USER32.
00403078	64 6C 6C 00 00 00 47 65	dll...Ge
00403080	74 44 72 69 76 65 54 79	tDriveTy
00403088	70 65 41 00 00 00 45 78	peA...Ex

[Memory 영역]

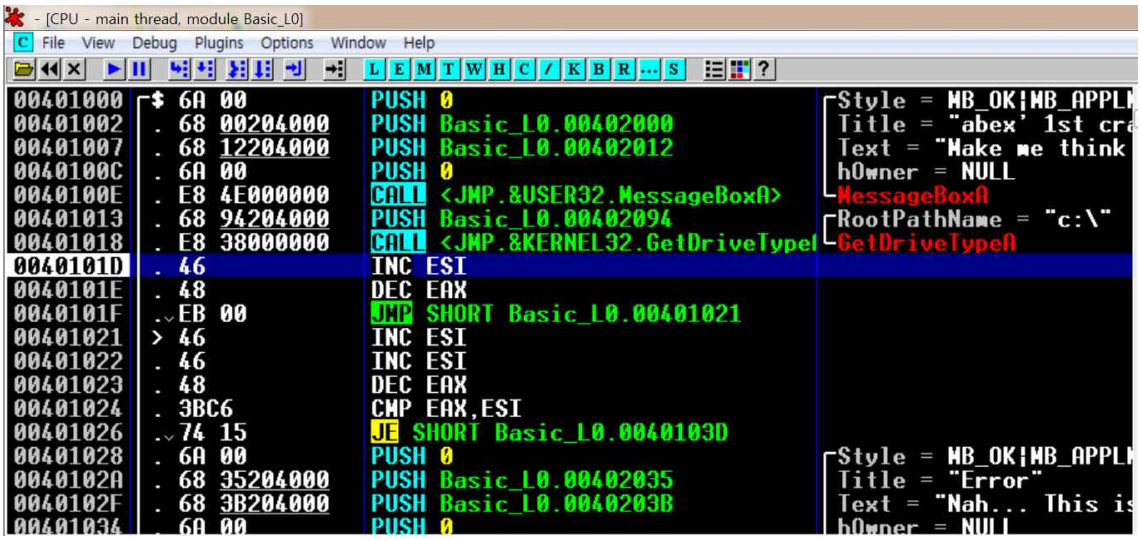
또한 실제 코드에서 참조하는 라이브러리 값도 확인할 수 있따. 디버거 코드 영역에서 주소 00401055를 보면 코드 JMP DWORD PTR DS[:<KERNEL32.GetDriveType>]을 확인할 수 있는데 외부라이브러리를 참조하는 코드이다.

```
0040104B   E8 11000000      CALL <JMP.&USER32.MessageBoxA>
00401050   E8 06000000      CALL <JMP.&KERNEL32.ExitProcess>
00401055  -FF25 50304000    JMP DWORD PTR DS:[<&KERNEL32.GetDriveTyp
0040105B  -FF25 54304000    JMP DWORD PTR DS:[<&KERNEL32.ExitProcess
```

[Code영역]

지금은 Level1이라 PE구조에 대해 자세히 살펴보고 설명했지만, 다음 보고서부터는 EntryPoint가 어디인지 어떤 함수를 참조하는지에 대해만 간략히 쓰고 넘어갈 것이다.

올리디버거를 통해 분석을 시작해 보면



-00401000~0040100E: MessageBox 함수를 호출해서 "Make Me Think your HD is a CD-ROM"을 출력하도록 하고 있다
-00401013~00401018: RootPathName을 인자값으로 넣고 GetDriceTypeA함수를 호출하고 있다.

다음 주소에 코드를 알아보기전에 함수 두가지를 알아보고 가자.

1.MessageBoxA함수

```
int messagebox{
  HWND hwnd,        //생성될 메시지 상자의 소유자 윈도우에 대한 핸들
  LPCSTR lptext,    //표시할 메시지
  LPTSTR lpCaption, //대화상자제목
  UINT uType;       //대화 상자의 내용과 동작
}
```

2.GetDriveTypeA
//아래와 같은 형태로 RootPathName값을 입력받아서 드라이브의 타입이 어떤 타입이지 확인하는 함수이다.

```
UINT WINAPI GetDriveType(
  _In_opt LPCSTR lpRootPathName //드라이브의 루트 디렉터리
);
```

리턴 값은 특정 정수값을 반환하는데 해당 값에 따라 드라이브 타입을 판단할 수 있는 것이다. 리턴 값의 종류는 아래와 같다.

Return Code	Value	Description
DRIVE_UNKNOWN	0	알 수 없음
DRIVE_NO_ROOT_DIR	1	최상의 경로가 없음
DRIVE_REMOVABLE	2	이동형 저장장치
DRIVE_FIXED	3	고정형 저장장치(HDD)
DRIVE_REMOTE	4	네트워크 드라이브
DRICE_CDROM	5	DVD/CD-ROM유형
DRICE_RAMDISK	6	램디스크

즉 우리가 GetDriveType 함수가 DVD/CD-ROM 유형으로 인식하게 하려면 반환값을 5로 바꾸면 된다는 것을 알 수 있을 것이다. 그러기 위해서는 반환값이 어디에 저장되는지 알 필요가 있다. 이를 알기위해서 0040101D에 BP를 설정하고 실행시키면 EAX 값에 3이라는 반환값이 저장된다는 것을 알 수 있다.

*EAX 함수 리턴값이 저장되는 레지스터로 사용되기도한다.

-0040101D~00401023주소를 살펴보면 ESI값은 3 ESI 값은 3 EAX 값은 1이된다.

-00401024에서 비교 연산인 CMP 연산을 하고

-00401026에서 앞에서 비교 연산을 한 결과를 이용한 JE명령을 하고 있다. 여기서 JE명령은 CMP 결과가 같으면 지정된 주소로 점프하는 연산이다. 결과값이 같아서 점프하는 주소는 0040103D이다. 즉 EAX값과 ESI 값이 같으면 0040103D주소로 가는 것이다.

-EAX값과 ESI같아 0040103D 주소로 가면 성공메시지가 나온다. 우리가 원하는데로 성공 메시지를 출력해주기위해서는 00401018 점프문을 JMP 0040103D로 수정해주어 메시지가 나오게 해주거나 EAX의 반환값을 ESI 와 같게 3으로 만들어주면된다.

-문제는 HDD를 CD-ROM으로 인식시키기 위해서는 GetDriveTypeA의 리턴값이 무엇이 되어야 하는가이니 5로 적어준다.