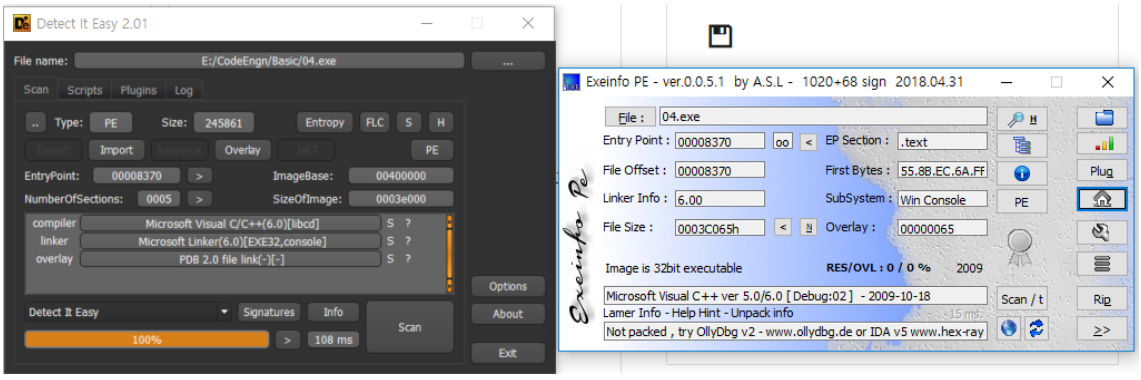
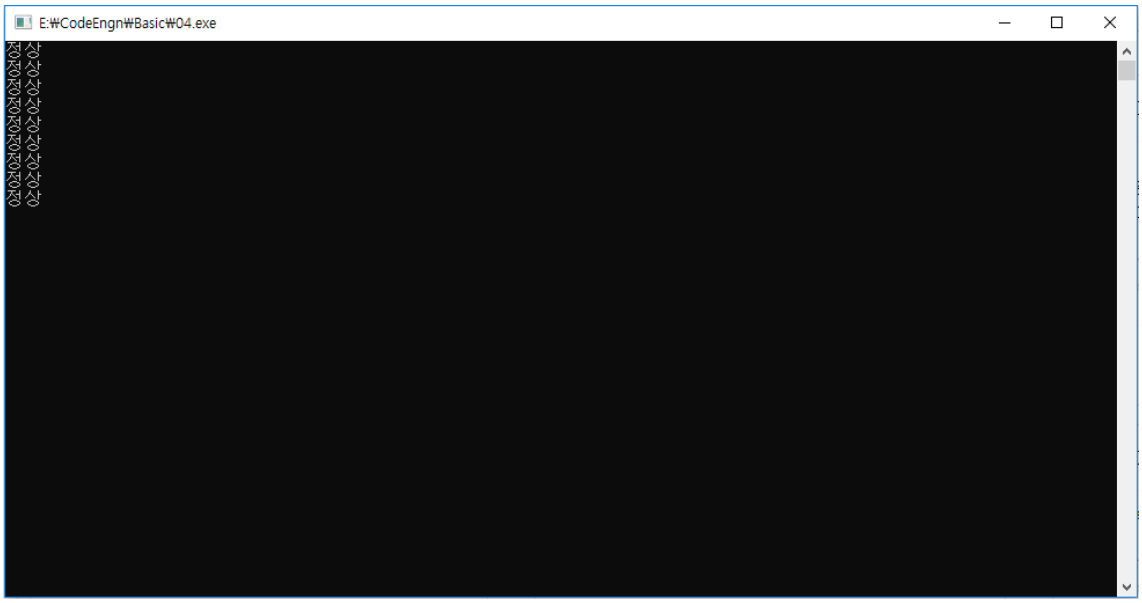
19.02.11 CodeEngn Basic RCE L04

Tree to Tree

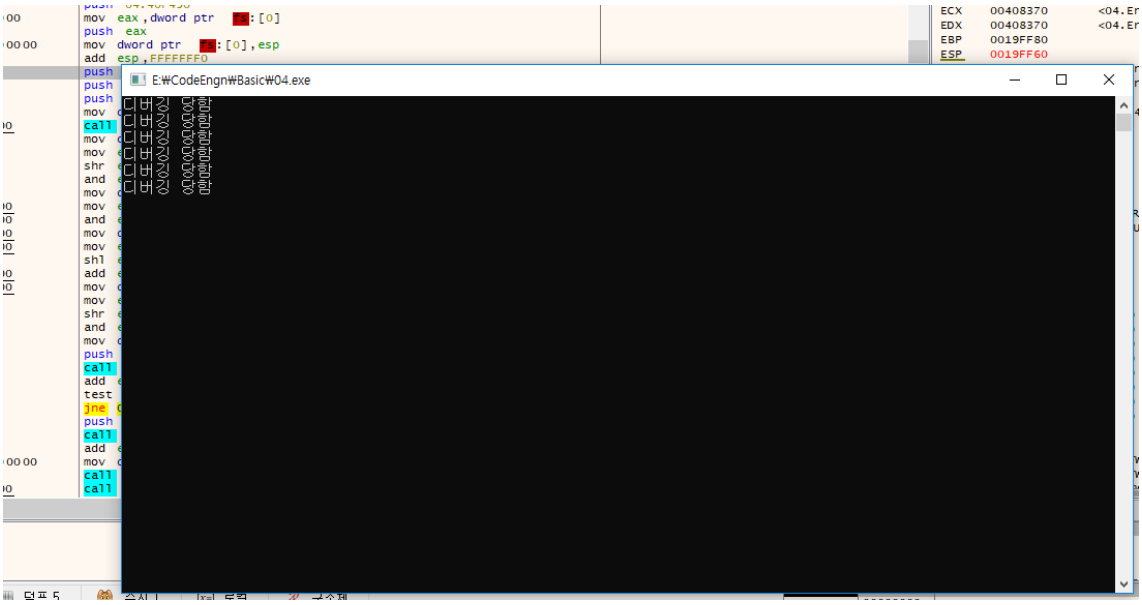
우선 PE분석기로 분석 해보니까 별다른 패킹은 되어있지 않다.



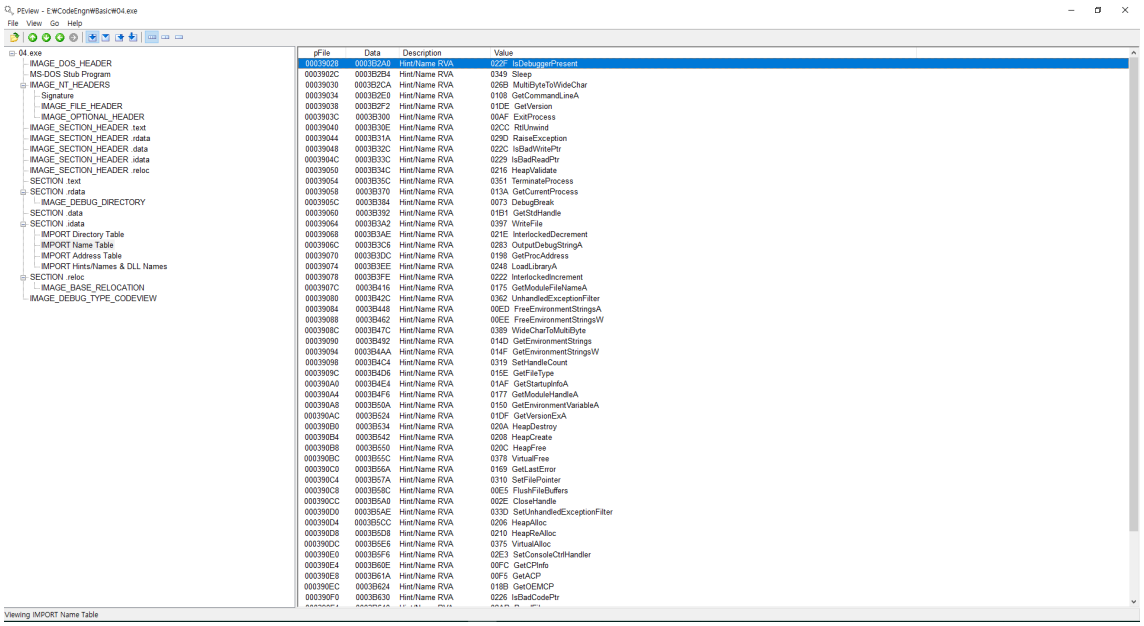
실행하니 정상이라는 문구가 계속 나옴
계속 체크한다는 것을 알 수 있음



디버거로 실행하니 디버깅 당함이라는 문구가 계속 나온다.

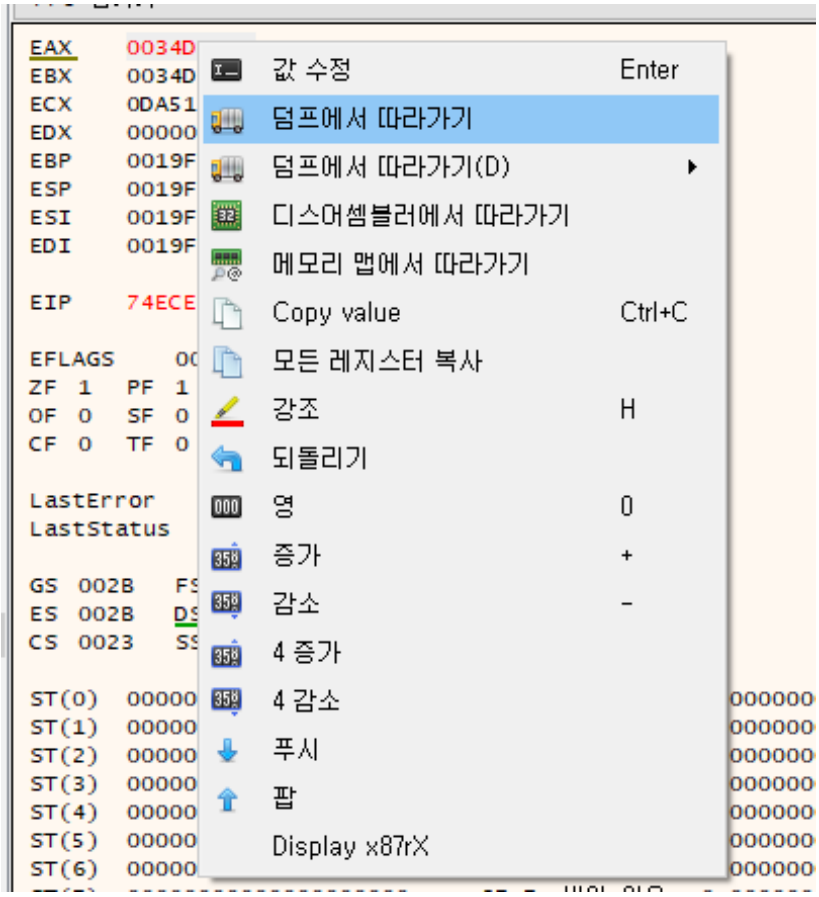


PE viewr로 Section .idata IMPORT Name Table을 보니
PEB값을 활용하는 기본 디버깅 API IsDebuggerPresent()가 보인다.

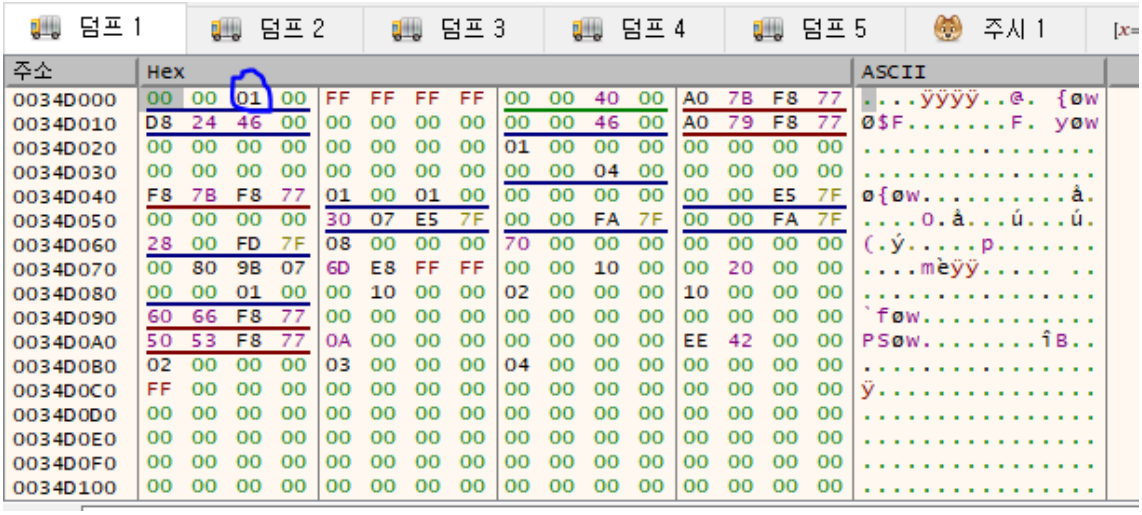


바로 따라가보자

PEB는 커널모드 디버거에서 자세한 사항이 나오지만 유저모드 디버거로도 찾아갈 수 있다.
IsDebuggerPresent를 따라가면 MOV eas, dword ptr fs:[30]이 보이는데
이주소가 PEB 구조체 접근 주소.
덤프해보면



파란색 동그라미 표시 해놓은 곳 01 PEB.BeingDebugged 멤버이다.
저 값이 0이면 디버깅 X 1이면 디버깅 O



PEB structure

12/05/2018 • 2 minutes to read

[This structure may be altered in future versions of Windows.]

Contains process information.

Syntax

C++ Copy

```
typedef struct _PEB {
  BYTE                          Reserved1[2];
  BYTE                          BeingDebugged;
  BYTE                          Reserved2[1];
  PVOID                         Reserved3[2];
  PPEB_LDR_DATA                 Ldr;
  PRTL_USER_PROCESS_PARAMETERS  ProcessParameters;
  PVOID                         Reserved4[3];
  PVOID                         AtlThunkSListPtr;
  PVOID                         Reserved5;
  ULONG                         Reserved6;
  PVOID                         Reserved7;
  ULONG                         Reserved8;
  ULONG                         AtlThunkSListPtr32;
  PVOID                         Reserved9[45];
  BYTE                          Reserved10[96];
  PPS_POST_PROCESS_INIT_ROUTINE PostProcessInitRoutine;
  BYTE                          Reserved11[128];
  PVOID                         Reserved12[1];
  ULONG                         SessionId;
} PEB, *PPEB;
```