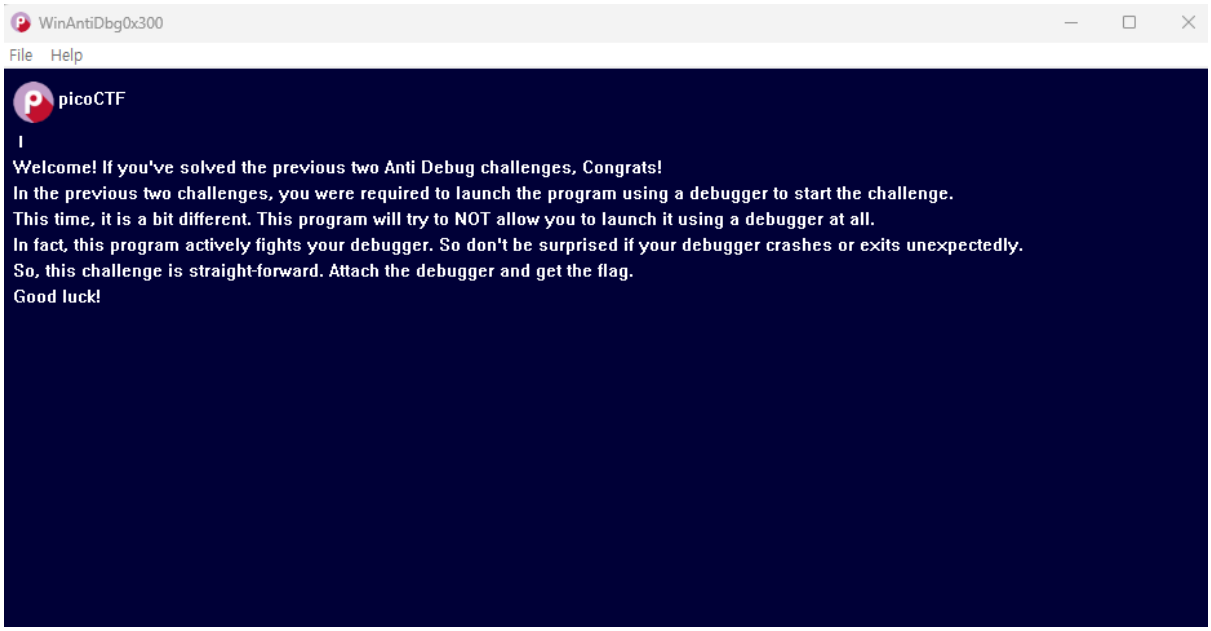
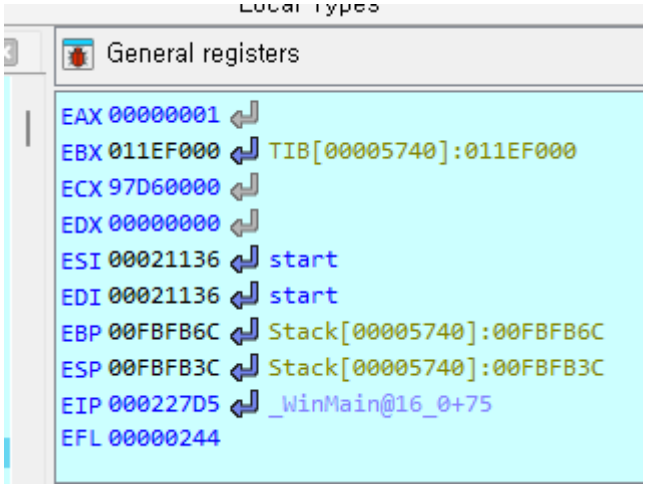
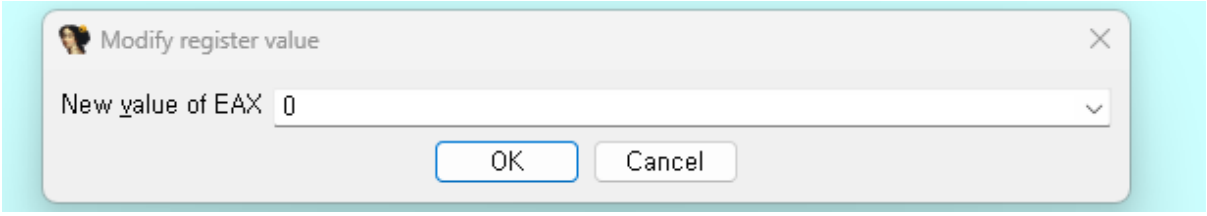


관리자 권한으로 실행해야 프로그램이 실행된다.

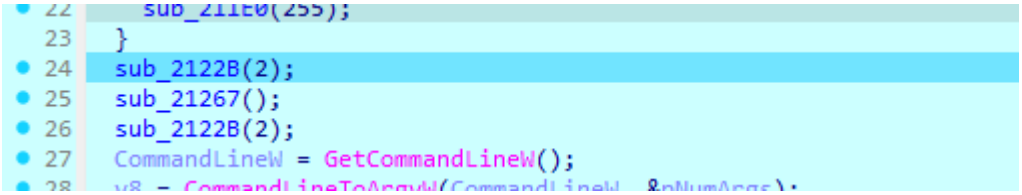
```
if ( !sub_401046() )
{
  MessageBoxW(hWnd, L"[FATAL ERROR] Error opening the 'config.bin' file. Challenge abort
  sub_4011E0(255);
}
sub_40122B(3);
if ( sub_401276() )
{
  MessageBoxW(hWnd, L"Oops! Debugger Detected. Challenge Aborted.", &Caption, 0x40u);
  sub_4011E0(255);
}
sub_40122B(2);
sub_401267();
```

Sub_401276함수에서 Debugger가 실행되었는지 탐지한다.

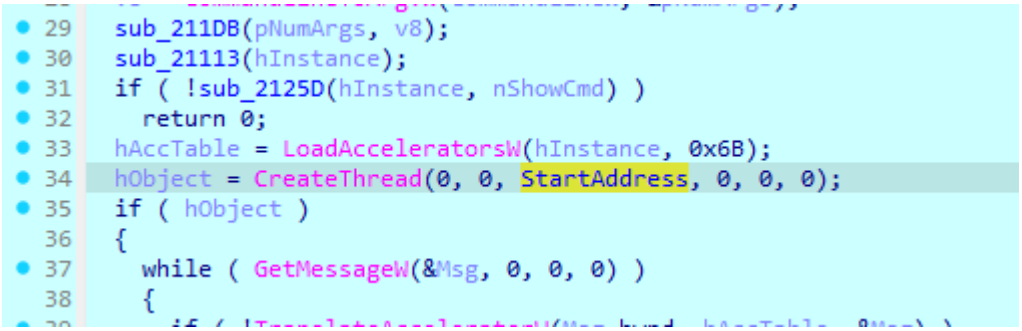




반환 값을 확인해보면 EAX가 1이 되고 에러 메시지를 출력하며 강제 종료가 될 것이기 때문에 EAX 값을 0으로 바꿔준다.



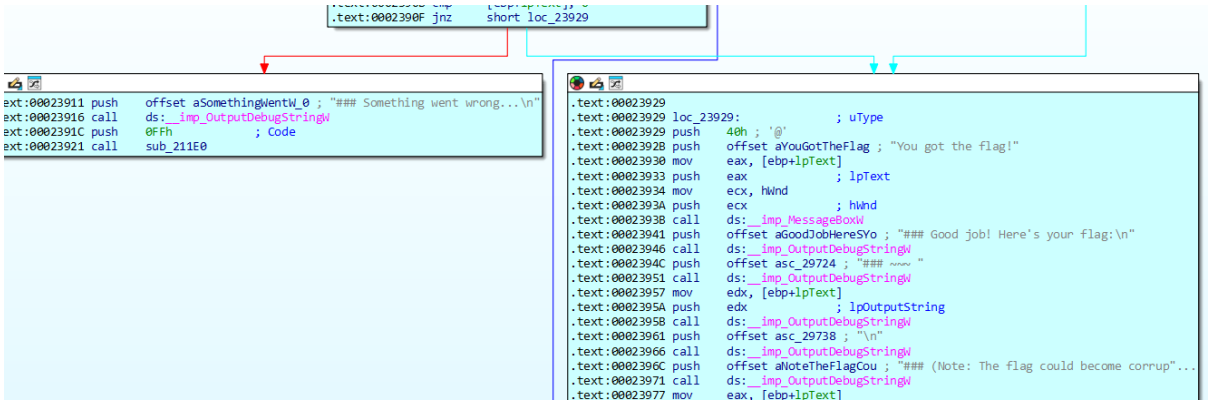
그리고 세개의 함수가 호출되는데, 2122B는 복호화를 수행하고 21267은 디버거가 admin 권한으로 실행되었는지 체크한다.



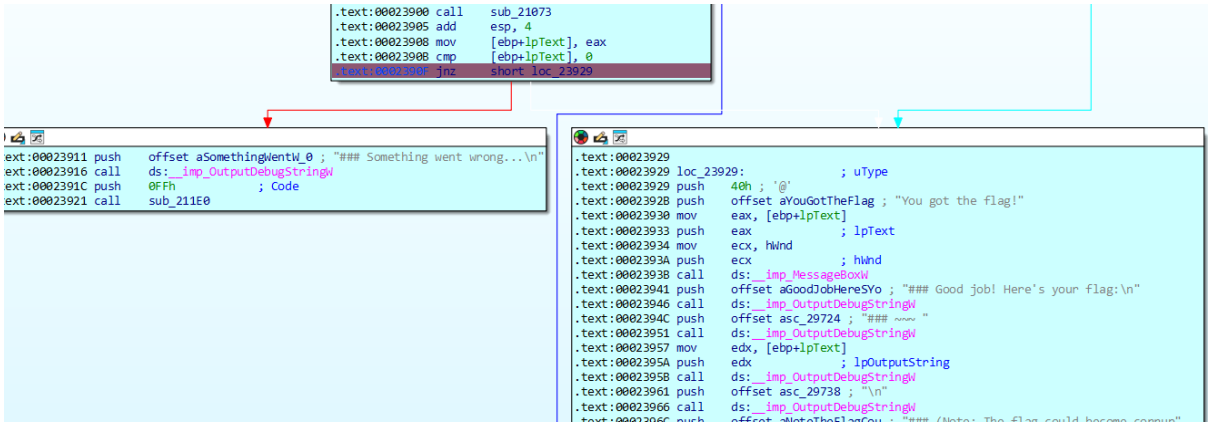
중요한 코드는 CreateThread 가 실행되는 부분이다.

```
1  void __stdcall __noreturn StartAddress_0(int a1)
2  {
3    WCHAR Filename[260]; // [esp+0h] [ebp-380h] BYREF
4    CHAR CommandLine[272]; // [esp+208h] [ebp-178h] BYREF
5    _STARTUPINFOA StartupInfo; // [esp+318h] [ebp-68h] BYREF
6    DWORD CurrentProcessId; // [esp+364h] [ebp-1Ch]
7    _PROCESS_INFORMATION ProcessInformation; // [esp+368h] [ebp-18h] BYREF
8    DWORD ExitCode; // [esp+37Ch] [ebp-4h] BYREF
9
10   memset(&StartupInfo, 0, sizeof(StartupInfo));
11   StartupInfo.cb = 68;
12   memset(&ProcessInformation, 0, sizeof(ProcessInformation));
13   ExitCode = 0;
14   CurrentProcessId = GetCurrentProcessId();
15   GetModuleFileNameW(0, Filename, 0x104u);
16   j__snprintf(CommandLine, 0x110u, "%ws %d", Filename, CurrentProcessId);
17   sub_2122B(2);
18   while ( CreateProcessA(0, CommandLine, 0, 0, 0, 0, 0, 0, &StartupInfo, &ProcessInformation) )
19   {
20     WaitForSingleObject(ProcessInformation.hProcess, 0xFFFFFFFF);
21     GetExitCodeProcess(ProcessInformation.hProcess, &ExitCode);
22     switch ( ExitCode )
23     {
24       case 0xFFu:
25         MessageBoxW(hWnd, L"Something went wrong. Challenge aborted.", &Caption, 0x10u);
26         sub_211E0(255);
27       case 0xFEu:
28         MessageBoxW(
29           hWnd,
30           L"The debugger was detected but our process wasn't able to fight it. Challenge aborted.",
31           &Caption,
32           0x10u);
33         sub_211E0(255);
34       case 0xFDu:
35         MessageBoxW(
36           hWnd,
37           L"Our process detected the debugger and was able to fight it. Don't be surprised if the debugger crashed.",
```

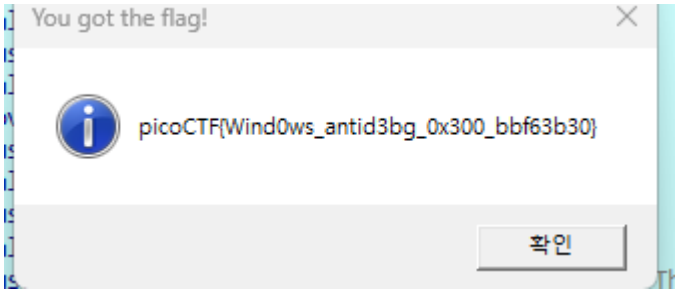
내부 로직을 보면 ExitCode에 따라 보여지는 에러 메시지가 다르다.



해당 함수의 코드를 디스어셈블 그래프로 살펴보면 디컴파일 했을 때와 다르게 숨겨진 로직이 하나 존재한다. 이 로직에서 flag를 출력시켜준다.



FLAG로 분기하기 위해서 각 FLAG값을 조작해주었다.



로직을 실행하면 FLAG가 출력된다.