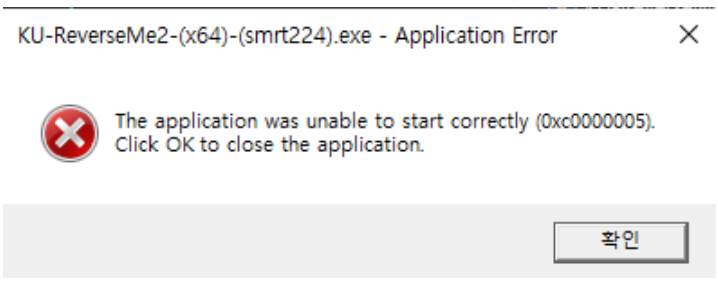
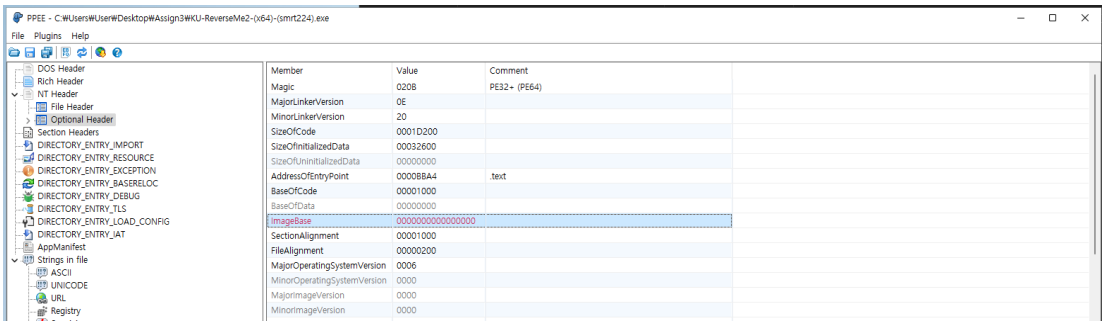
[2022-RE]-[2021350027]-[강재현]

[1] Execute the target PE file properly. How did you do that?

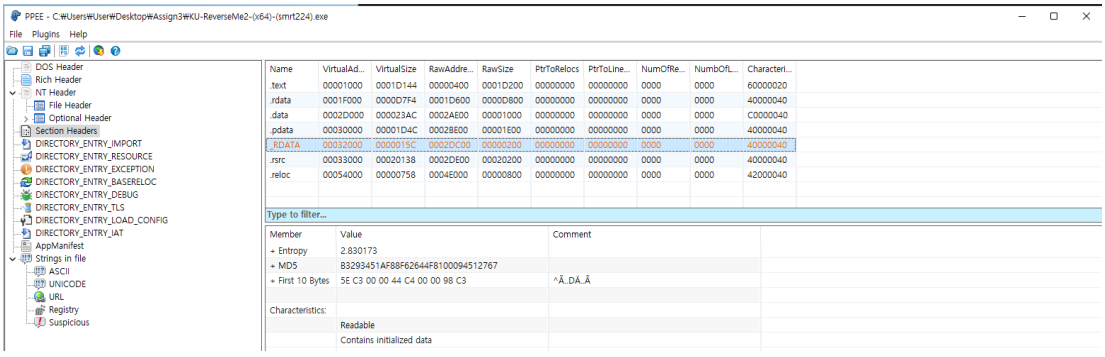
- 파일을 실행시키면 아래와 같이 오류가 뜬다. 0xc0000005오류는 메모리 손상이나 시스템 파일의 손상으로 인해 나타나는 오류라고 한다.



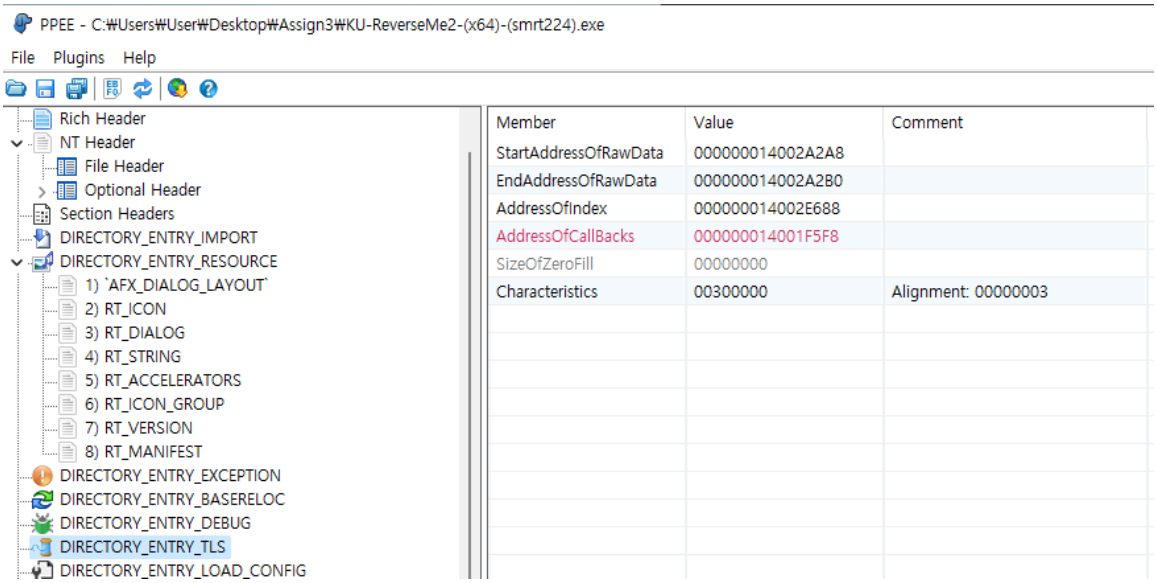
- PE파일의 format 부분에서 문제가 있다고 하셨으니, 먼저 PPEE로 파일을 열어봤다.
  - Optional Header 부분에서 빨간색으로 되어있는 ImageBase가 0으로 되어있는 것을 발견했다.



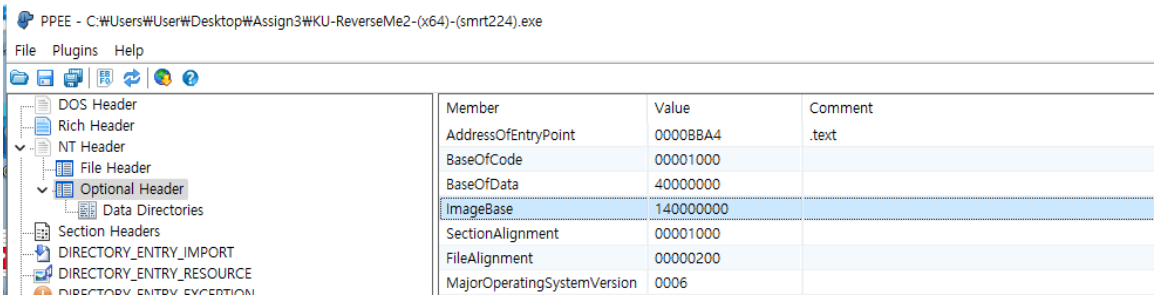
  - Section Header의 주황색으로 되어있는 _RDATA부분도 수정이 된 것 같다.



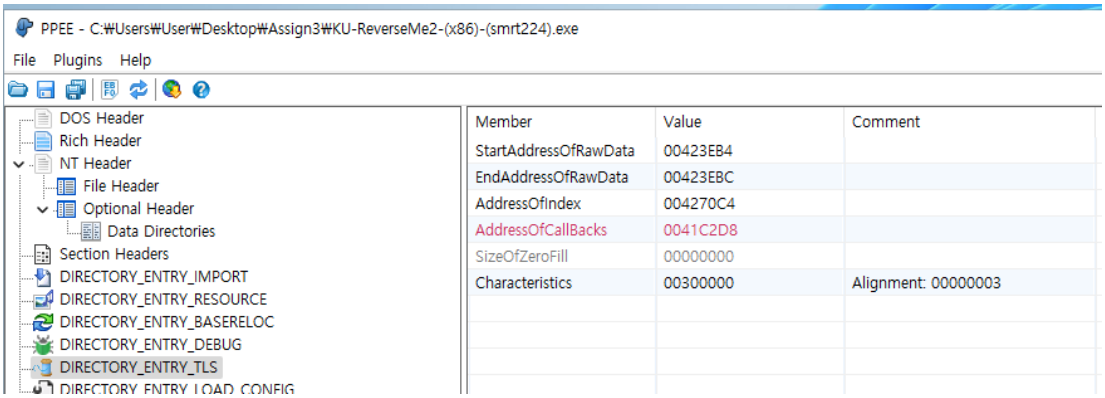
- 먼저 ImageBase 문제부터 알아보도록 하겠다.
  - ImageBase가 0이 아닌 다른 값이어서 이런 문제가 생긴것 같은데, 원래 ImageBase값을 어떻게 찾을 수 있을까?



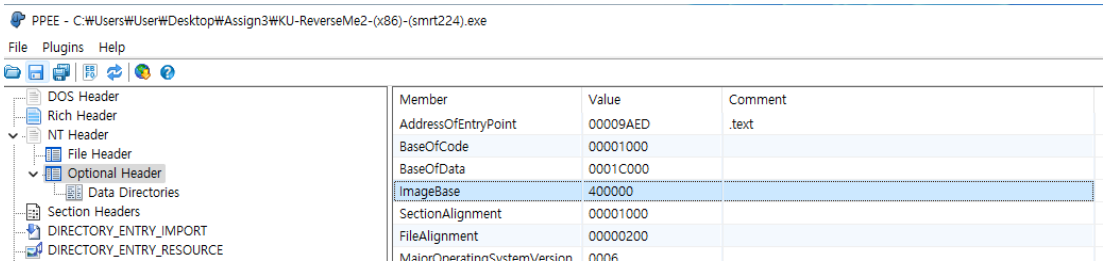
- 그냥 PPEE를 돌아다니다가, DIRECTORY_ENTRY_TLS에서 ImageBase를 유추할 수 있지 않을까 싶었다 RawData에 대한 address를 가지고 있기 때문에, ImageBase 기반의 주소이기 때문이다. `140000000`이 워낙 큰 수이기도 해서, 일단 그 값으로 **ImageBase**를 `0x140000000`으로 수정시켜 보겠다....



- 성공했다! 실행시키면 아무 일도 일어나지 않는다.
  - x64파일은 수정이 됐지만, x86은계속 `140000000`이 아닌 `40000000`으로 수정이 되었다. 계속 고민을 해보니, x86파일의 ImageBase는 x64와 달랐던 것이었다!



- 따라서 x86파일의 DIRECTORY_ENTRY_TLS에 기반해서, `ImageBase=0x400000`으로 수정했더니 오류가 뜨지 않았다.



결론

- x64파일의 **ImageBase**를 `0x140000000`으로 수정한다.
- x86파일의 **ImageBase**를 `0x400000`으로 수정했다.