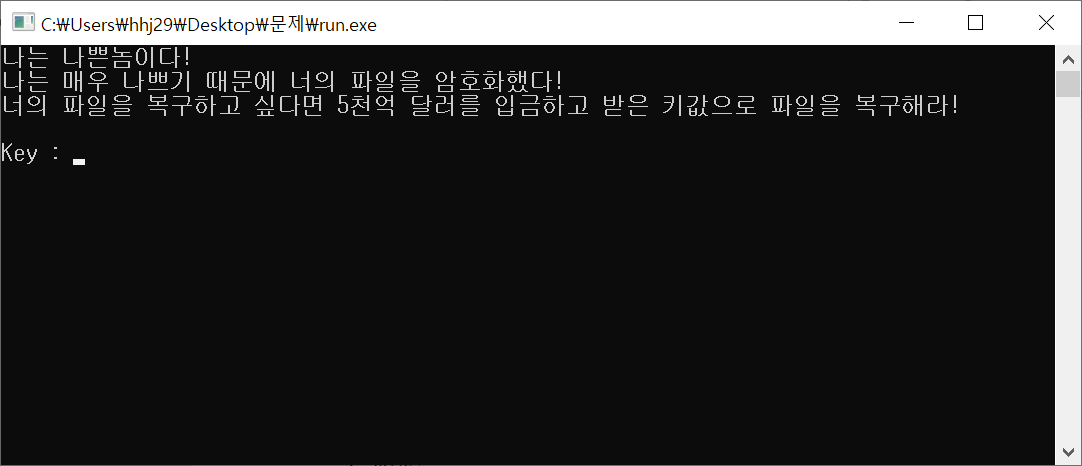
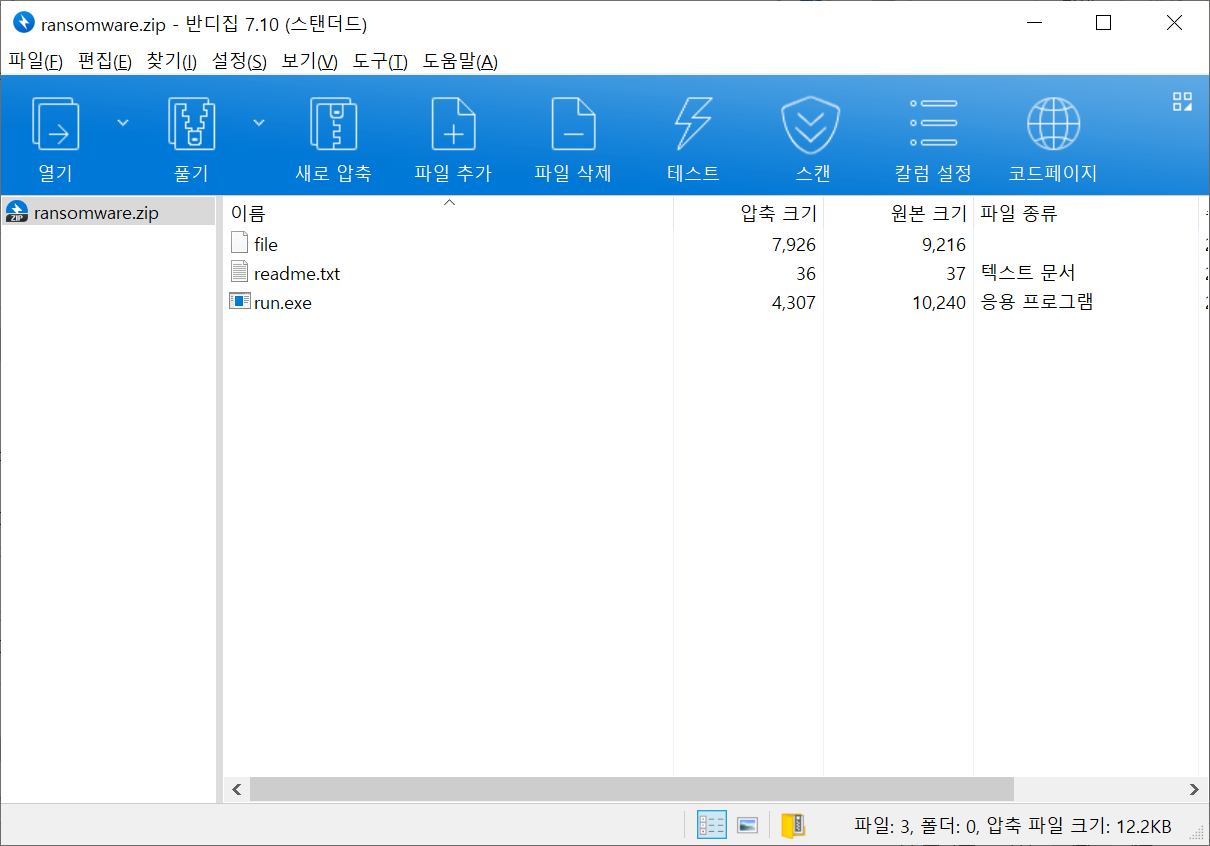
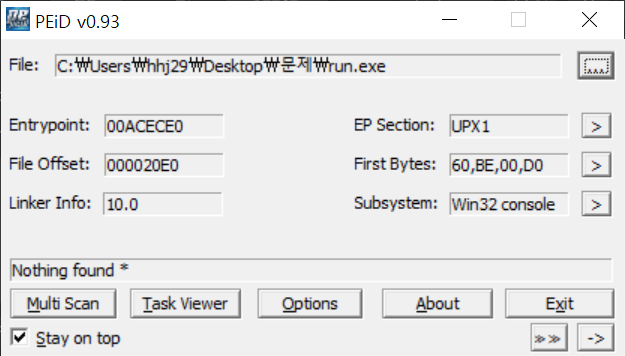
1. 문제 확인





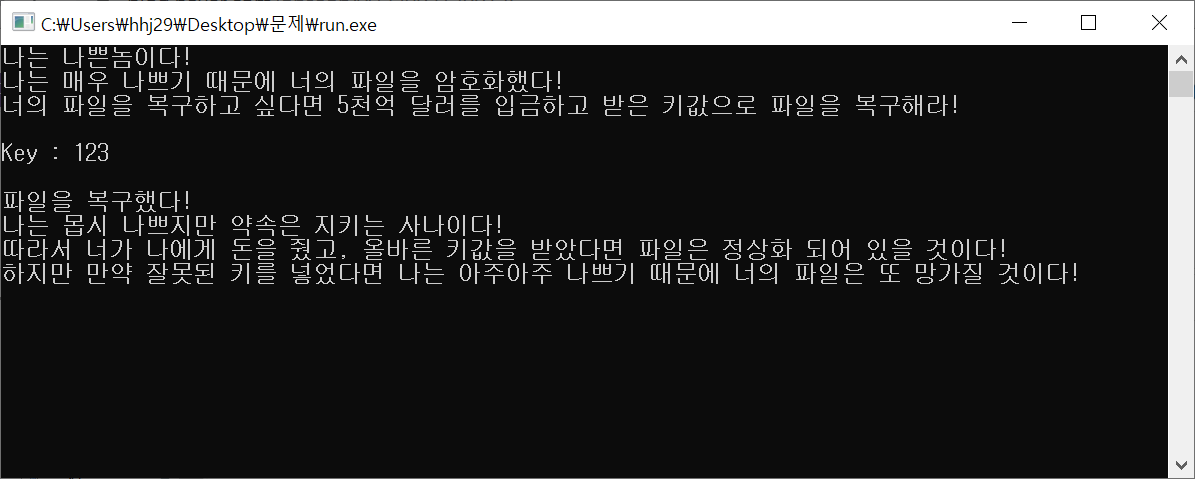
2. 과정

처음으로 패킹여부를 확인하기 위해 PEiD를 열었다.



UPX로 패킹 되어있다는 것을 확인하고 언패킹 해주었다.

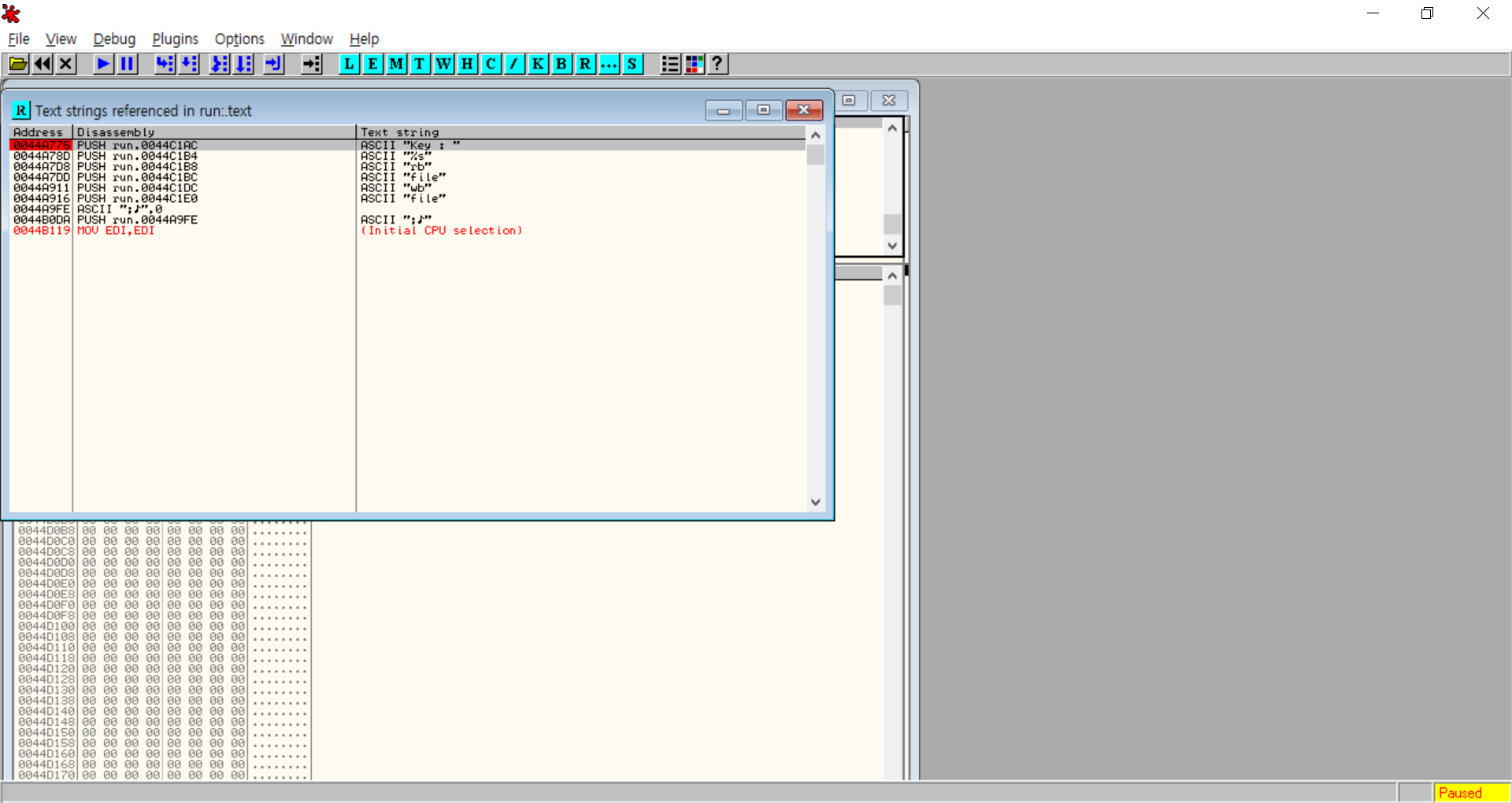
파일을 열어서 key 값을 입력해보니 이러한 문구창이 뜨는 걸 확인할 수 있었다.



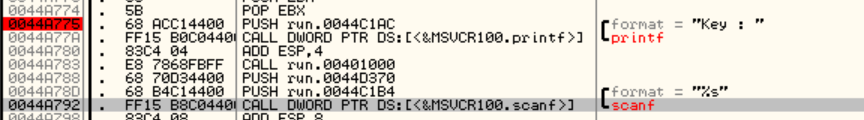
우선 올리디버거로 열어서 확인해보았다.

문자열이 나오는 부분 먼저 찾아보았다.

키를 입력하라는 문자열과 %s를 확인했다.

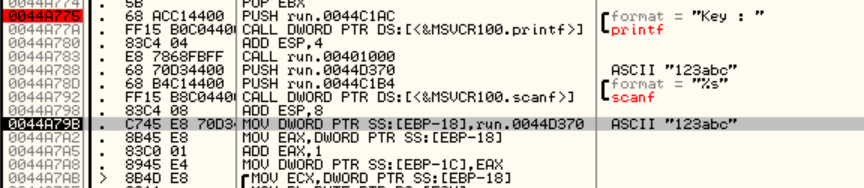


처음부터 하나씩 실행해보았다.

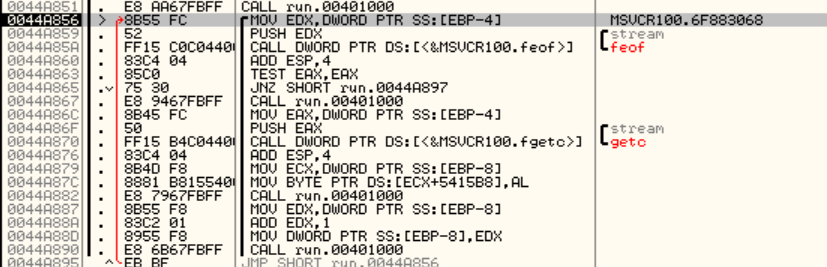


여기서 키 값을 입력 받도록 scanf가 실행되었다.

우선 123abc를 입력하고 계속 진행했다.

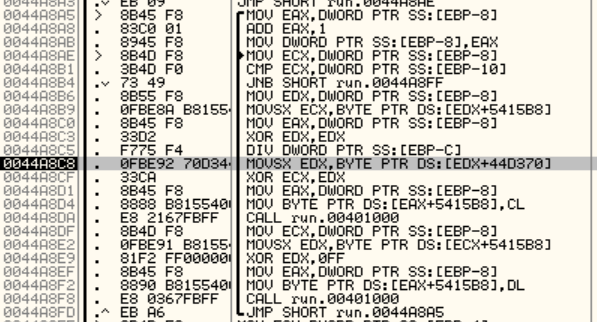


이 루프문에서는 어떤 파일을 불러와 하나씩 값을 5415B8에 저장하는 것 같다.



해당 루프문을 잠시 탈출하고 아래로 가보면 또 루프문이 존재하는데

여기서 내가 입력한 key 값과 어떤 값끼리 연산이 이루어지고 있다는 것을 발견했다.



여기서 식을 잘 찾으면 해결할 수 있는 값을 구할 수 있을 것 같다.

좀 헷갈리는 부분이 있어 다른 분의 풀이를 살펴가면서 진행했다.

44A8B9에서 EDX+5415B8 주소에서 불러온 값을 ECX에 넣는다.

44A8C8에서 내가 입력한 key 값을 하나씩 불러와 EDX에 넣는다.

ECX와 EDX를 XOR 한 후 저장한다.

위 ECX에 저장된 값을 EDX에 넣는다.

EDX와 0FF를 XOR 한 후 저장한다.

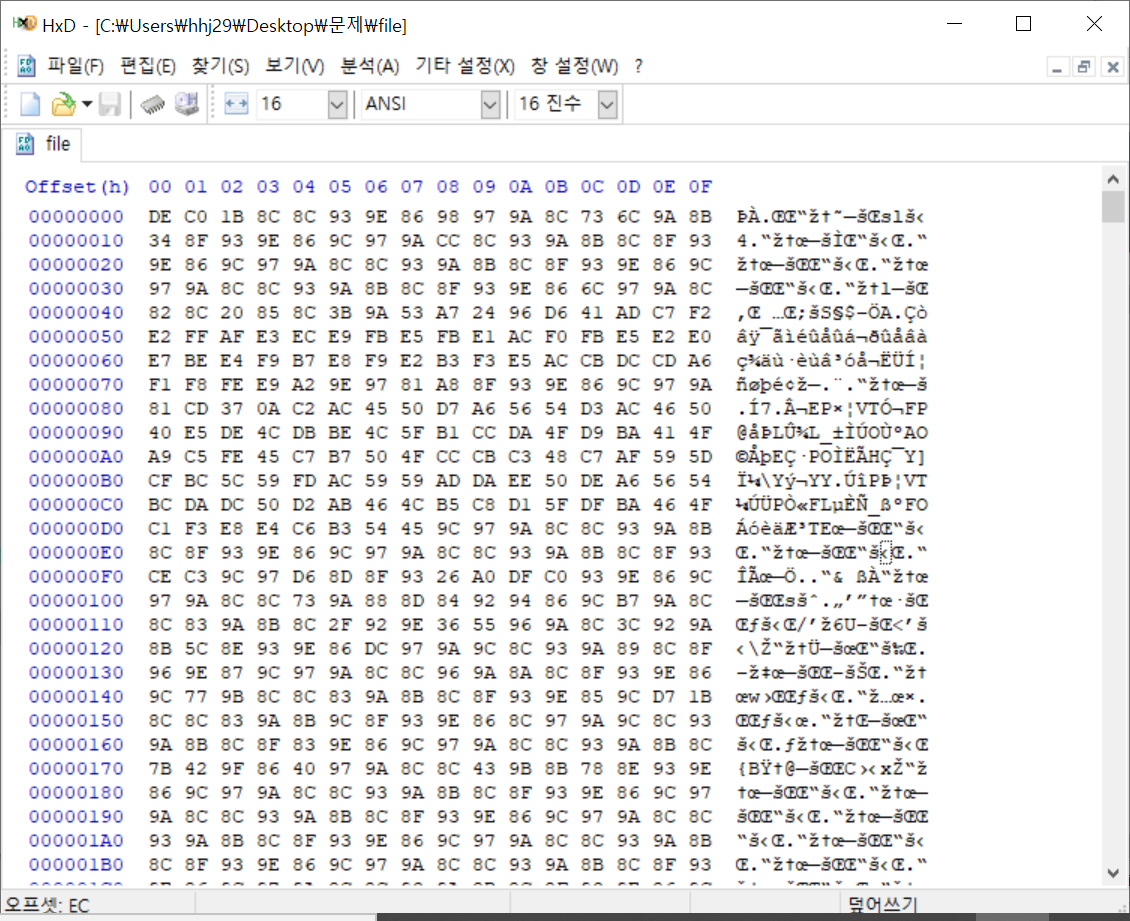
5415B8에 최종 값 넣는다.

결국 정리해보면

(처음 5415B8에 저장된 값) XOR (내가 입력한 key) XOR (OFF) = 최종 저장된 값

* Key = (처음 파일에 저장된 값) XOR (0FF) XOR (최종 저장된 값)

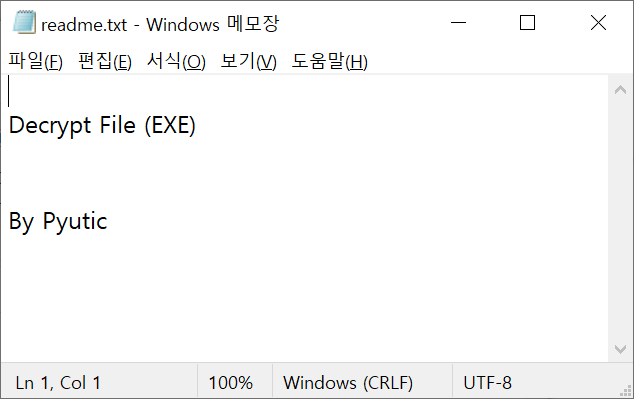
같이 받은 file을 HxD로 열어보았다.



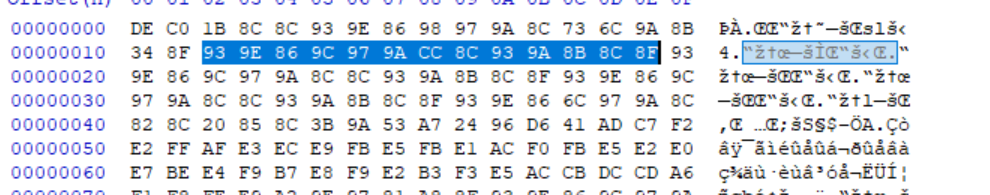
뭘 봐야하는 지 감이 전혀 안와서,,.

다른 분의 라업을 읽어보았다.

문제와 함께 있던 txt 파일이 힌트가 된다고 한다.



우선 file을 보면 일정한 길이로 반복되는 값을 확인할 수 있는데

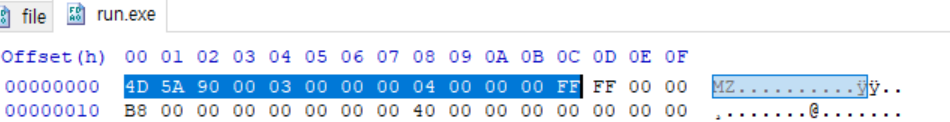


이 13자리가 반복되는 것을 보아 Key 값이 13자리인 것을 알 수 있다.

이걸 이용해 파일의 특정 위치에 있는 13자리 값과, 같은 위치 run.exe 파일의 13자리 값을 이용해 key를 구할 수 있다고 한다.

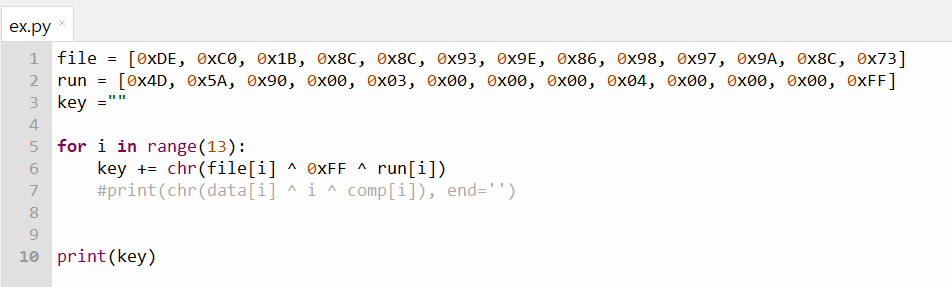


DE, C0, 1B, 8C, 8C, 93, 9E, 86, 98, 97, 9A, 8C, 73



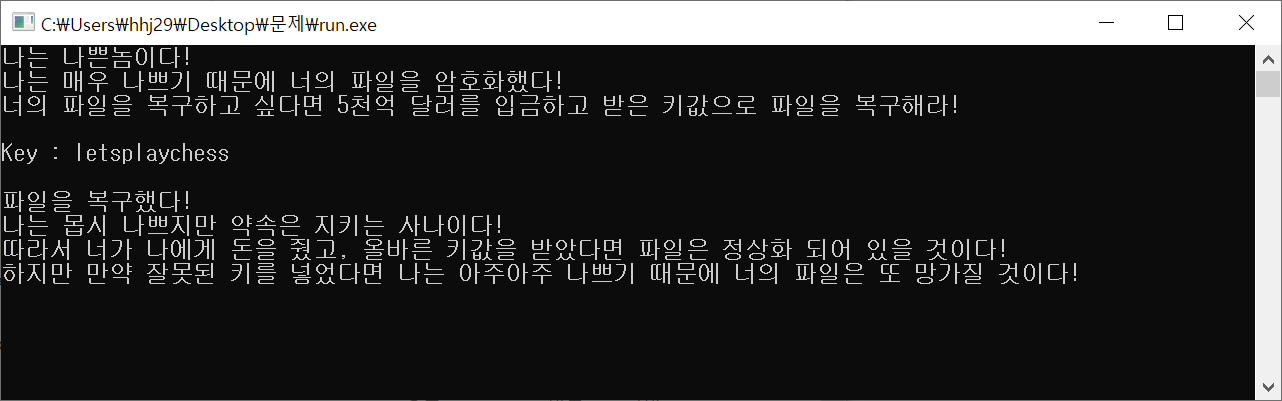
4D ,5A, 90, 00, 03, 00, 00, 00, 04, 00, 00, 00, FF

파이썬을 이용해 코드를 짜보았다.





키 값으로 letsplaychess가 나왔다.



여기가 아니라 file에 해야하는 것 같다.

File을 exe로 바꾸어 실행해보려 했는데 이상하게 이 컴퓨터에서 실행되지 않는다는 창이 떠서 확인할 수는 없었다.