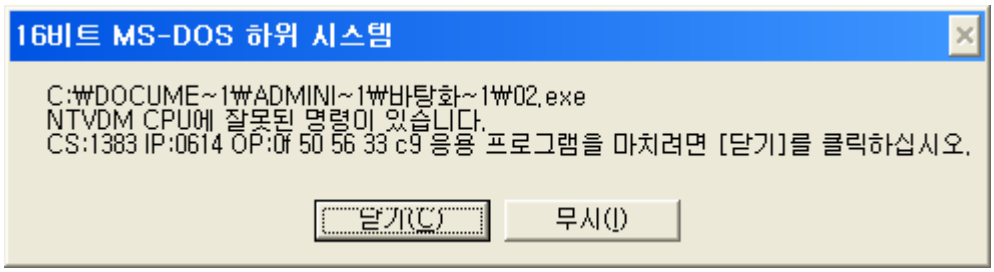
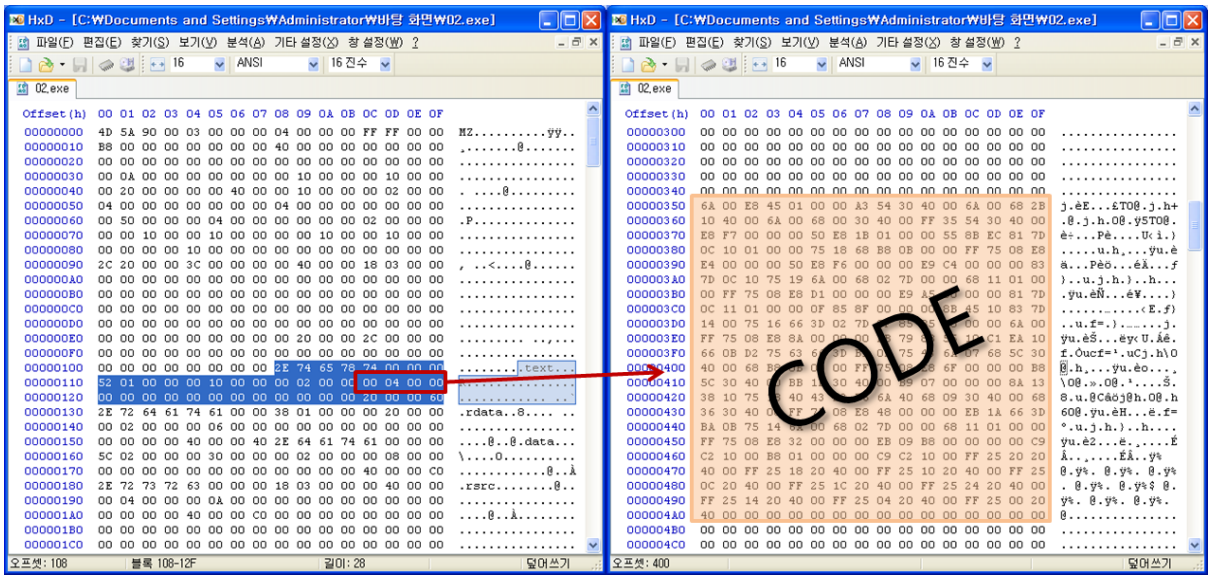
Q. 패스워드로 인증하는 실행파일이 손상되어 실행이 안 되는 문제가 생겼다. 패스워드가 무엇인지 분석하시오.

파일이 손상되어 실행이 불가능하다.

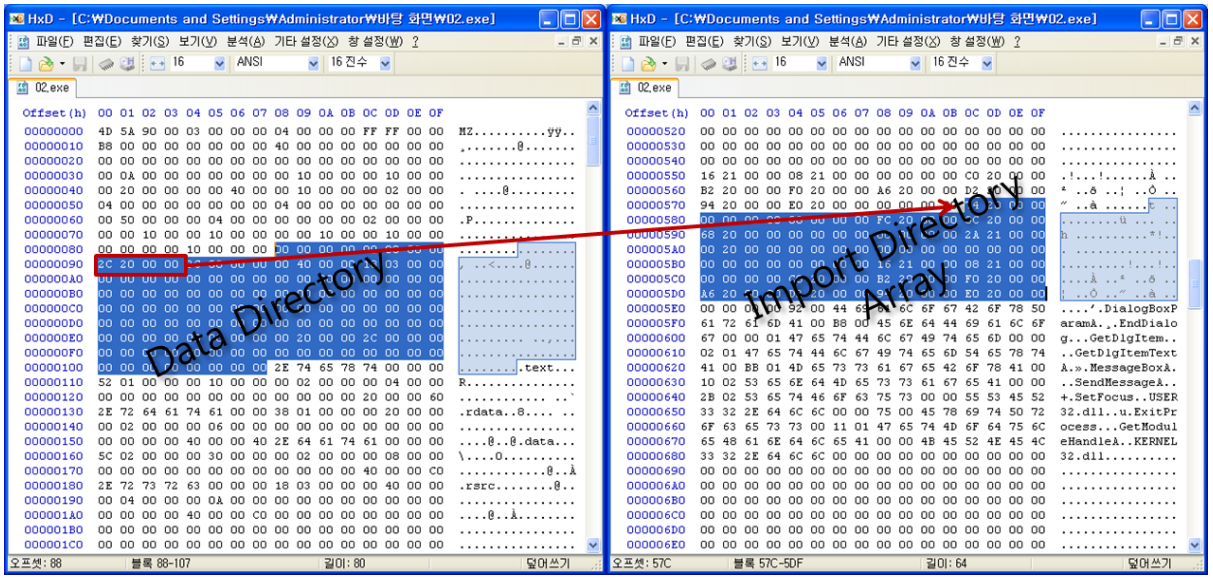


파일의 어떤 부분이 손상되었는지 확인하기 위해 헥사값을 확인하던 도중 섹션헤더 부분은 손상되지 않고 남아있는 것을 볼 수 있었다.



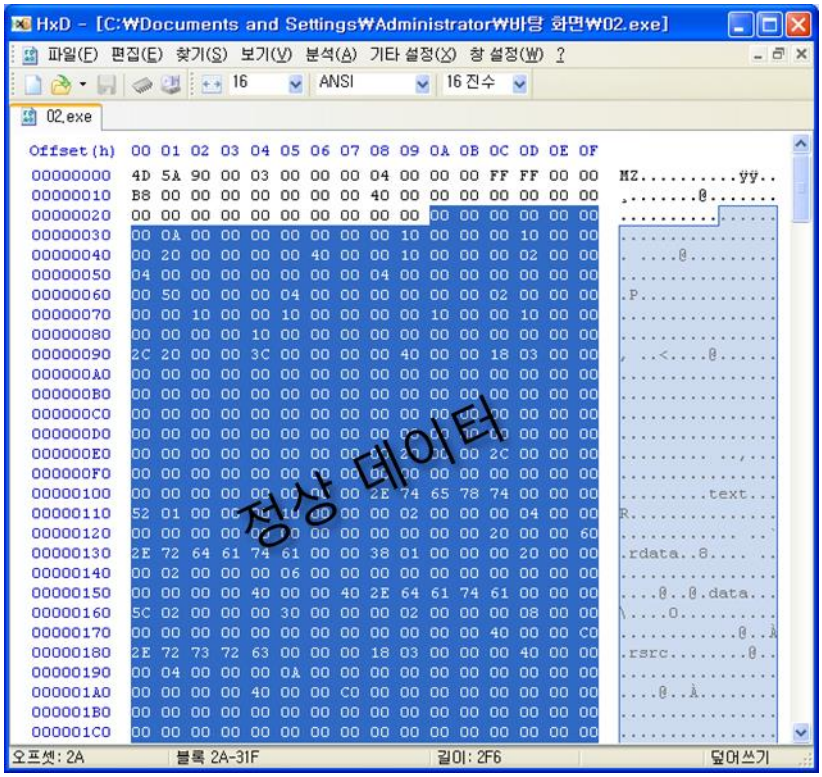
text섹션의 PointerToRawData는 0x400을 가리키고 있는데, 0x350부터 코드가 존재하는 것을 볼 수 있다. 적어도 PE 헤더의 0xB0만큼은 손상되어 사라진 것으로 추측이 가능하다.

DataDirectory를 확인해보면 0x10만큼의 배열이 잘 자리잡고 있는 것을 확인할 수 있다. 정확히 들어맞는지 확인하기 위해 Import Directory를 찾아가 계산하여 보았다.

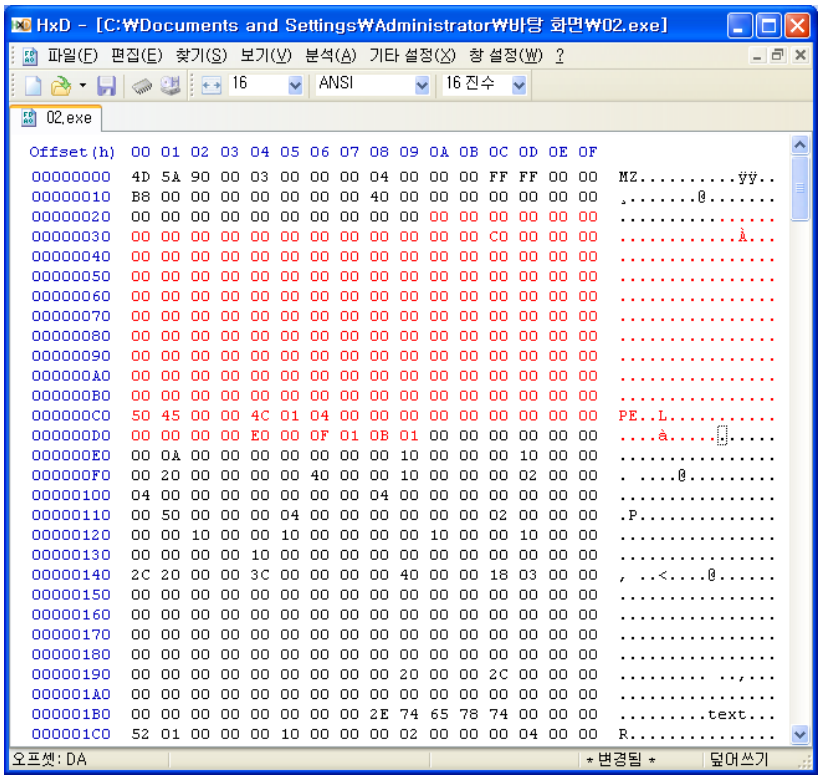


Import Directory의 RVA값은 0x202C이므로, RAW를 계산하면 0x62C이다. 여기서 손상되었을 것으로 추측되는 0xB0만큼을 더 뺀 값인 0x57C로 가면 실제 Import Directory 배열을 확인할 수 있다. 각 필드의 값도 확인해 봄으로써 DataDirectory가 맞다고 확신할 수 있었다..

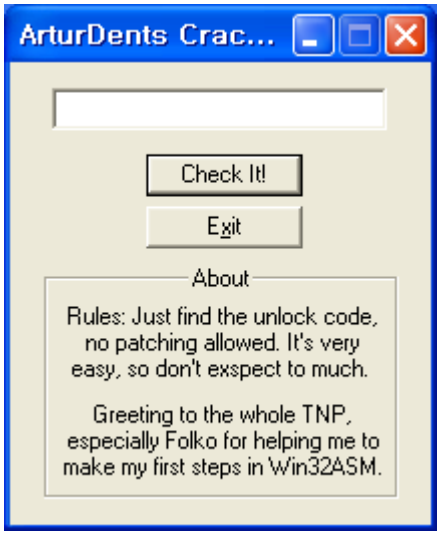
가변 필드인 DataDirectory를 확인했으므로 이 앞의 데이터들을 뒤에서부터 하나씩 보면서 위치를 찾아 손실된 데이터를 삽입하기만 하면 복원할 수 있을 것이다. 실제로 OptionalHeader의 Magic 필드 이후부터 구조를 잘 따르고 있었으며, 실제로 복구해야하는 필드의 범위를 알 수 있다.



실제 손실 된 부분은 IMAGE_DOS_HEADER의 일부(e_lfanew 포함), Dos Stub구간, NT Header의 시그니처, IMAGE_FILE_HEADER의 magic 필드였다. PE 로더가 읽지않는 필드는 전부 0으로 채우고, 실행에 필요한 부분만 채워넣었다.



저장하고 실행하면 어떤 창이 생성된다.



이 창으로 무언가 할 수 있는 것은 없으며, 패스워드를 입력해도 결과창은 나타나지 않는다. 패스워드는 어딘가 저장되어있을 것이고, 복호화 루틴이 없는 점, 네트워크 통신 관련 코드가 없는 점을 생각해보면, 결국 패스워드로 추측가능한 문자열은 Data섹션의 JK3FJZh를 제외하고는 없다.