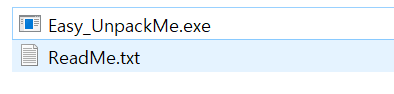
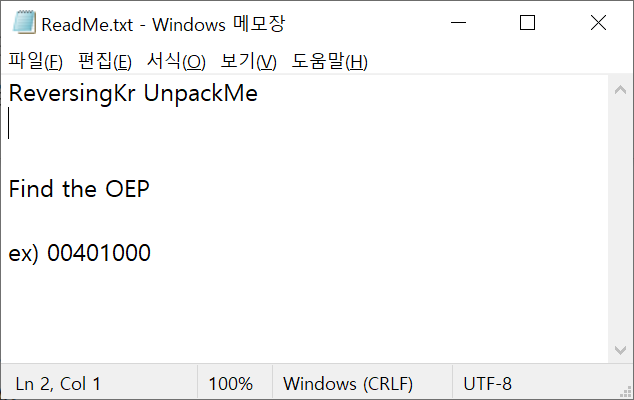
1. 문제 확인





2. 과정

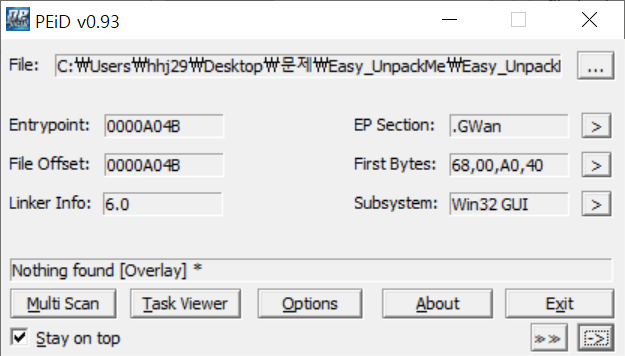
우선 OEP는 원본 파일을 디버깅 했을 때 시작위치라고 한다..

패킹된 파일을 디버깅 하면 언패킹된 순간을 찾을 수 있는데 그곳이 OEP

언패킹된 파일이 계속 실행되다가 마지막에는 원본 코드의 EP로 점프하게 되는데

결국은 OEP로 분기하는 부분만 찾으면 된다고 한다.

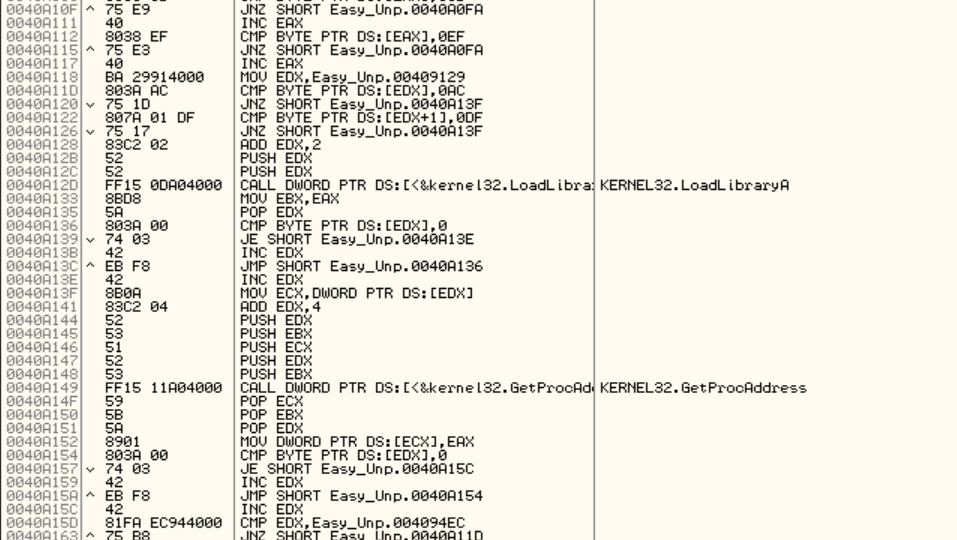
패킹여부를 확인해보았다.



GWan이 무엇인지 검색해봤지만 제대로 된 내용이 없었다.

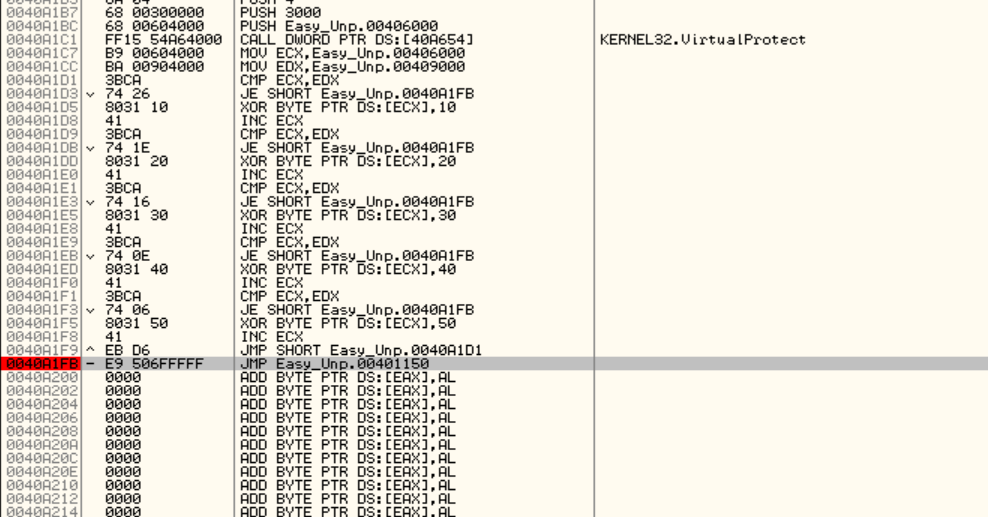
뭘로 패킹 되어 있는지 알 수 없다.

일단 올리디버거를 열어 확인해보았다.

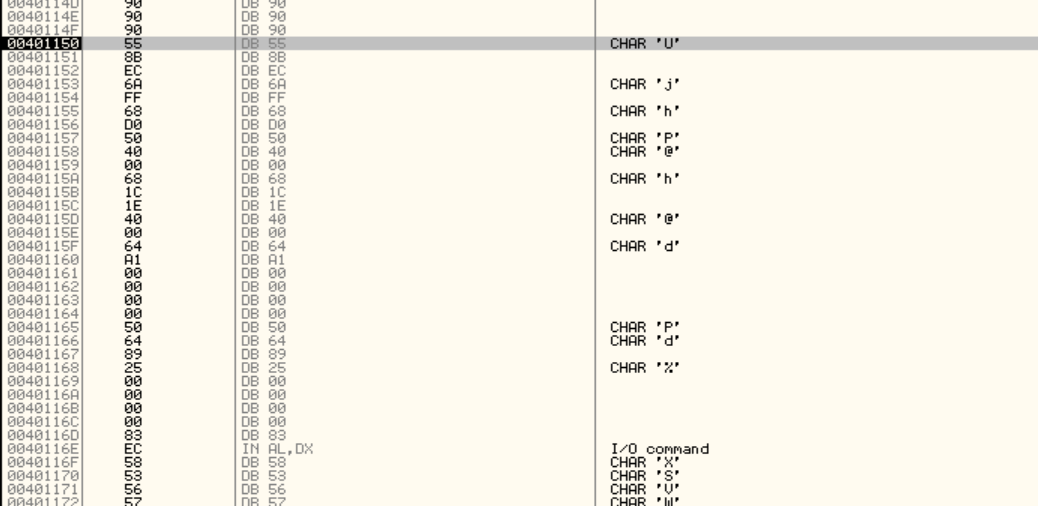


무슨 JNZ, JE, PUSH 등 많은 코드가 실행되다가

이렇게 마지막 부분에 점프문이 있는 것을 발견했다.

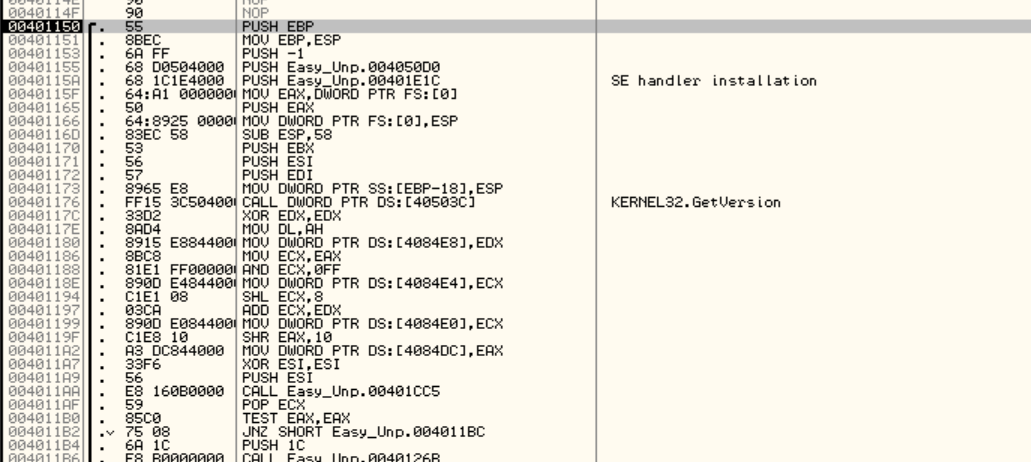


느낌이 여기일 것 같아서 bp를 걸고 F7을 눌러 확인해봤는데



이런 곳으로 넘어갔다.

코드 분석을 누르니까 PYSH EBP를 찾을 수 있었다.



따라서 OEP는 00401150

3. 결과

