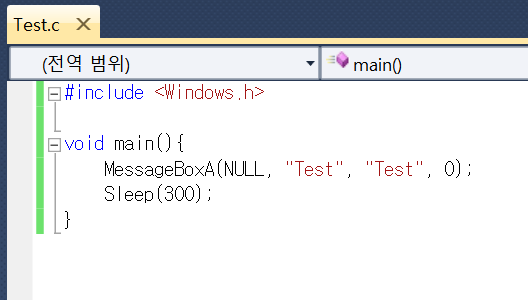
실습보고서6 2016111566 이나경

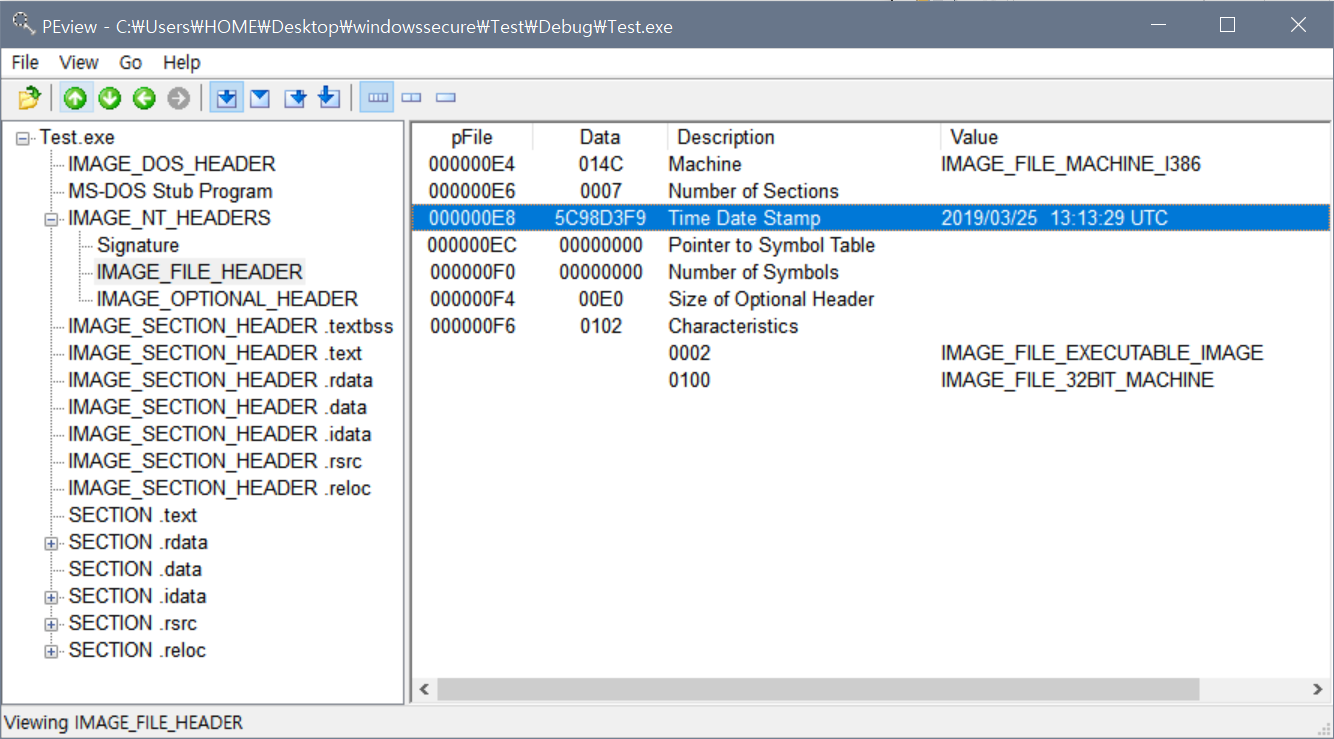
실습환경 : Windows XP(VMware 가상머신)

Tool : OllyDbg

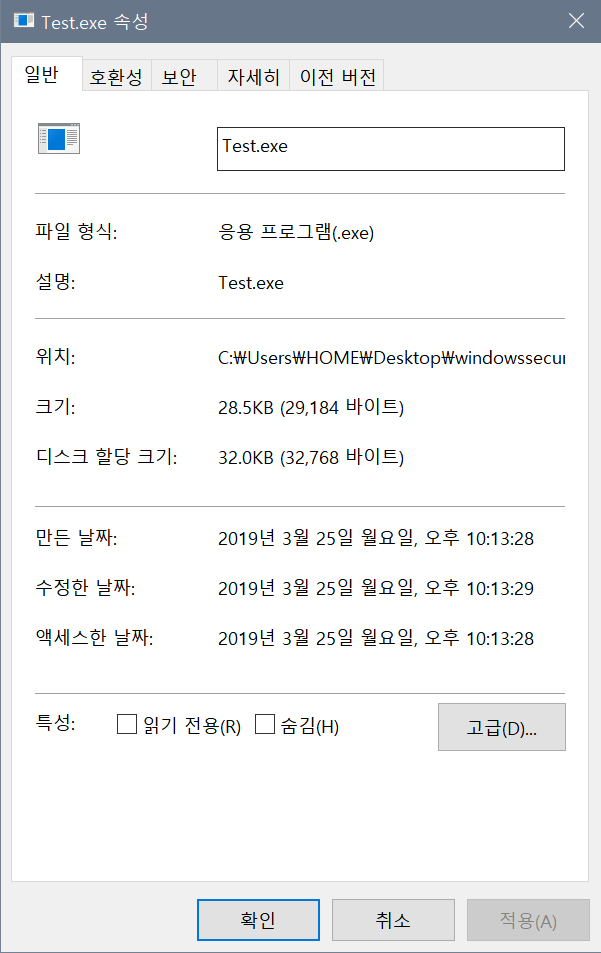
<PE정보 확인>



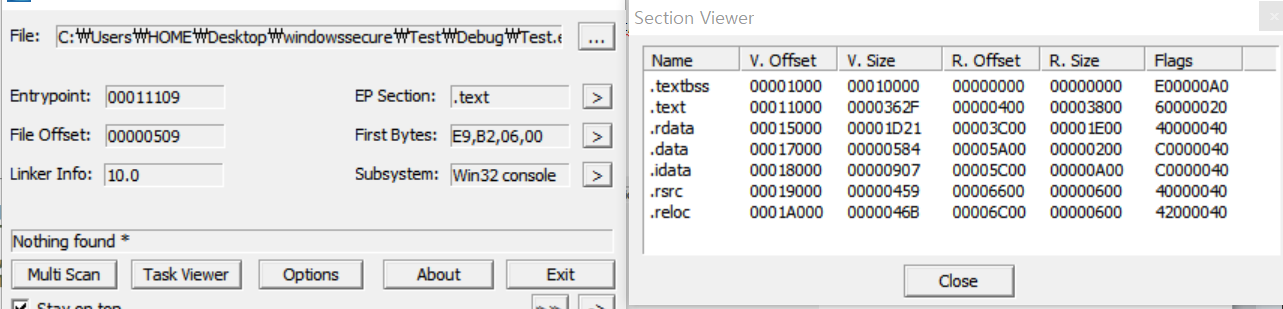
간단한 윈도우 실행파일을 작성해 PEview로 분석해보았다



생성 시점은 3월 25일 13시 13분이며



파일 종류는 응용프로그램(exe)이고



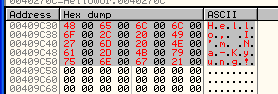
PEiD로 확인한 결과 섹션은 7개이다

<문자열 버퍼 직접 수정>

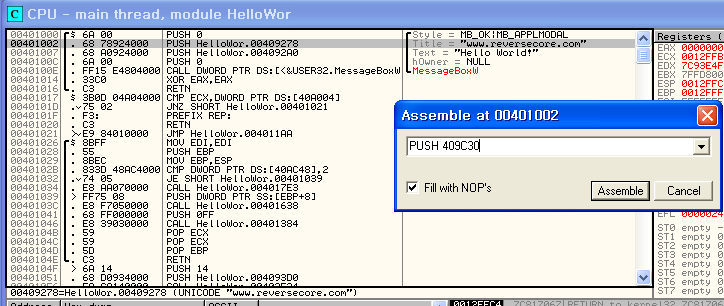
-> Hello.exe 첨부

<다른 메모리 영역에 새로운 문자열 생성 전달>

NULL Padding 영역에 문자열 입력

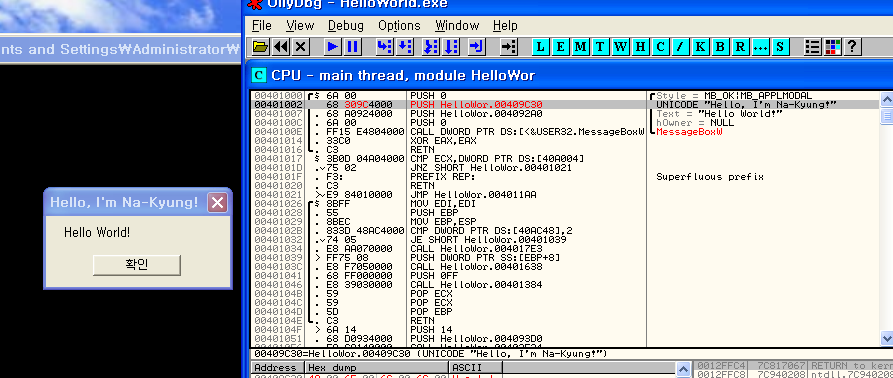


00409C30부터 문자열을 입력한다.



그 후 401002에 Assemble

“PUSH 409C30”



실행버튼을 누르면 Title이 수정된 것을 볼 수 있다.