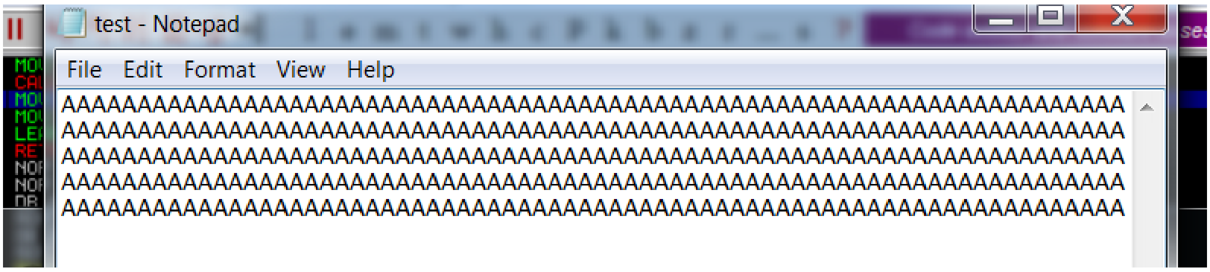
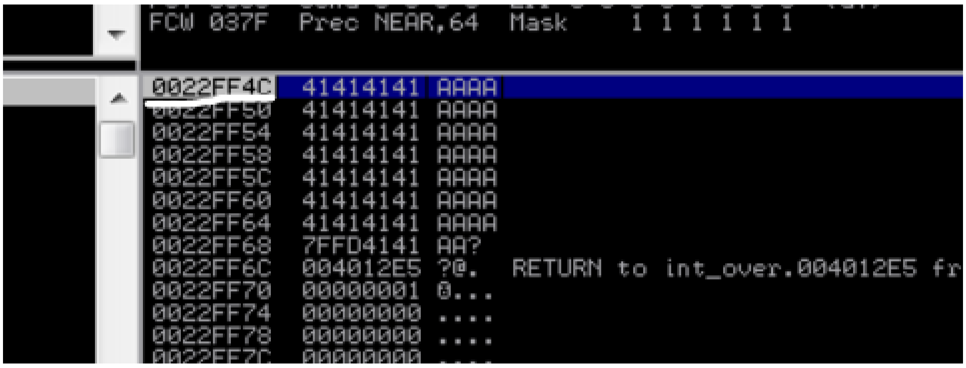
1. A의 개수 구하기



A가 350개 있는 test.txt 파일을 이용해 exe 파일을 디버거로 실행해보았다.

Main 함수를 찾아서 들어간 후 return 까지 실행하여 ret 주소가 저장되는 곳을 확인한다.



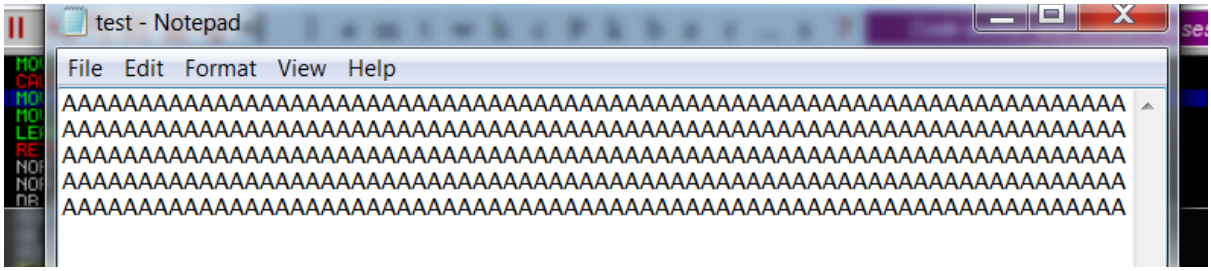
0022FF4C 위치에 RET 값 (EBP 값)이 저장되는 것을 알 수 있다.

이번 argument로 준 파일의 길이가 350이였는데 파일 마지막에 주소를 넣어서 ebp 주소를 조작하려면 350에서 길이를 30만큼 줄여야한다는 것을 알 수 있다.

따라서 320개만큼 A를 넣고 + 원하는 주소를 넣으면 ebp 주소 조작이 가능해진다.

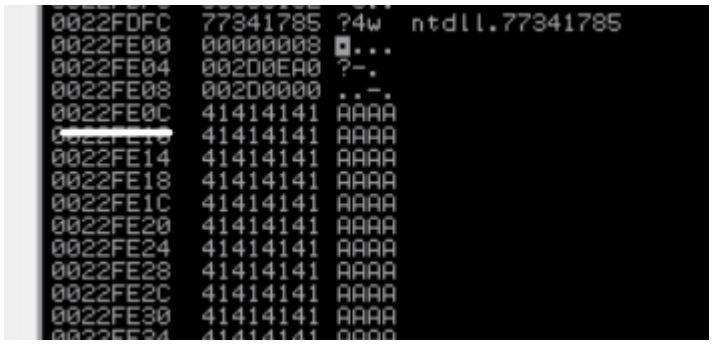
즉 해당 함수(main) 함수에서 return 후 원하는 주소로 가도록 하게 된다는 의미이다.

2. BUF에 들어가는 주소값을 추출하는 방법



A가 350개 있는 test.txt 파일을 이용해 exe 파일을 디버거로 실행해보았다.

Main 함수를 찾아서 들어간 후 memcpy까지 실행하여 contents 변수의 값이 메모리 상에 어디에 저장되는지 확인한다.



0022FE0C 부분부터 A가 저장된 것을 알 수 있다.

따라서 argument로 받은 파일의 내용을 0022FE0C 위치에 저장한다는 의미이다.

쉘코드에서 해당 주소로 가도록 ebp 주소를 조작한 후 해당 주소에는 파일에 원하는 동작을 하는 함수를 저장하면(기계어로) 원하는 동작을 가능하게 한다.