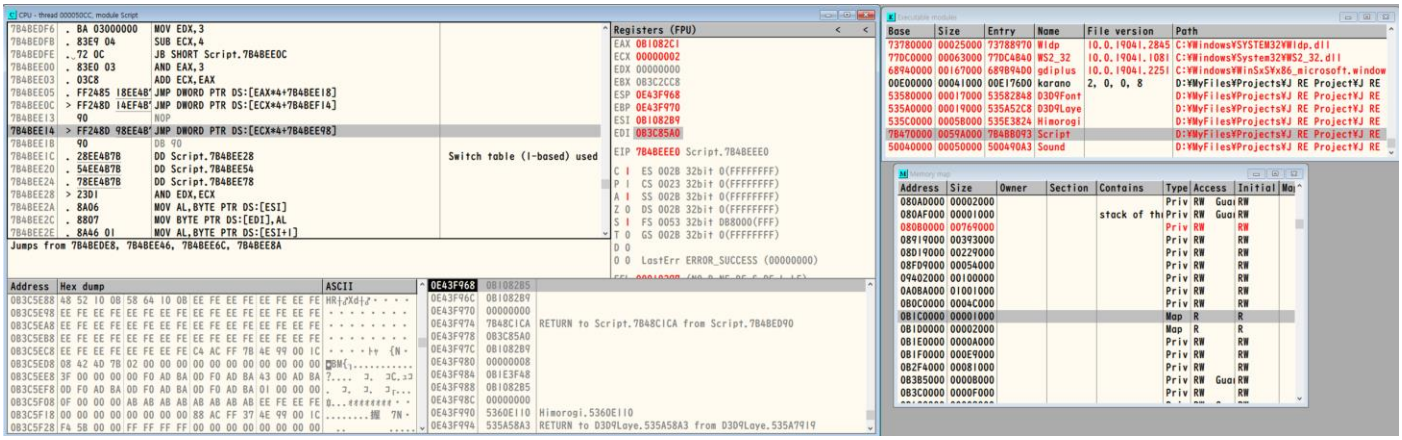
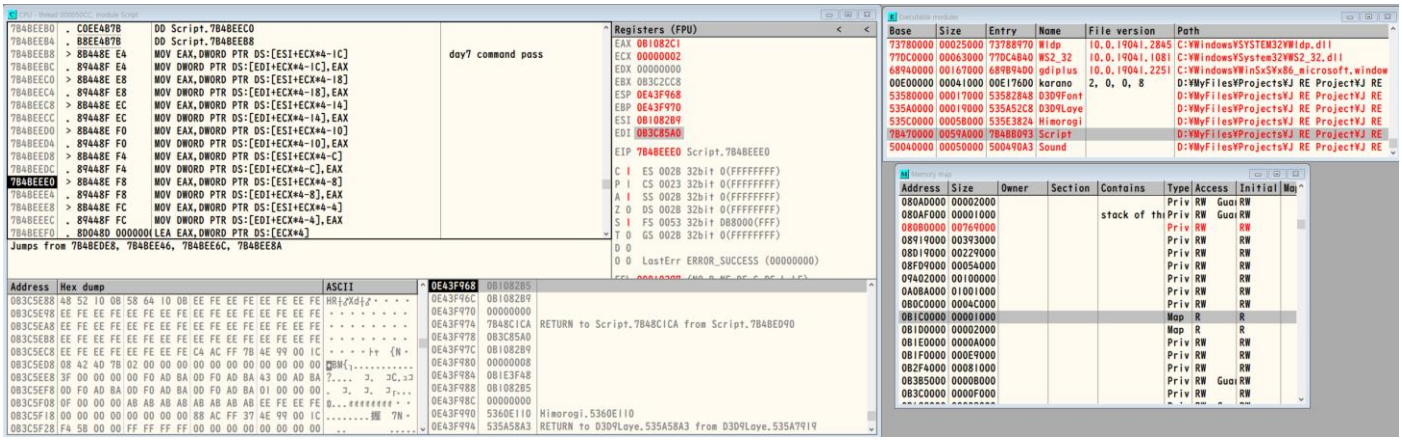
오늘은 학교과제를 해야하기 때문에 다음 후킹테스트를 해볼 지점만 저장해두고 마무리합니다.



7B4BEE14 – 7B470000 = 0004EE14

0x0004EE14

이곳에서는 ECX의 값이 중요합니다. 그 이유는 다음 사진에 바로 나와있습니다. 간단히 말하면, ECX는 문장의 길이와 관련되어 데이터를 얼마나 복사할지를 결정하는 값입니다.



이곳은 위의 7B4BEE14지점에서부터 점프해오는곳입니다.

문장, 명령어 등등 을 EDI에 무언가를 더한 지점에 Double WORD씩 저장합니다.

받아오려는 원본에 AABBCCDDEE라는 것이 있었다 가정하면, EAX에 AA BB CC DD라는 문장을 넣고, 이를 EDI+ECX*4-??에 넣는 느낌이지요. 복사 길이는 이곳으로 오기전에 저장된 ECX값이 결정합니다. 참고로 복사하는 값의 최소단위는 DWOD이므로 별로 상관없는 부분까지도 복사해올수도 있을 듯 합니다.

Hex dump를 보며 테스트해보면 쉽게 보입니다.