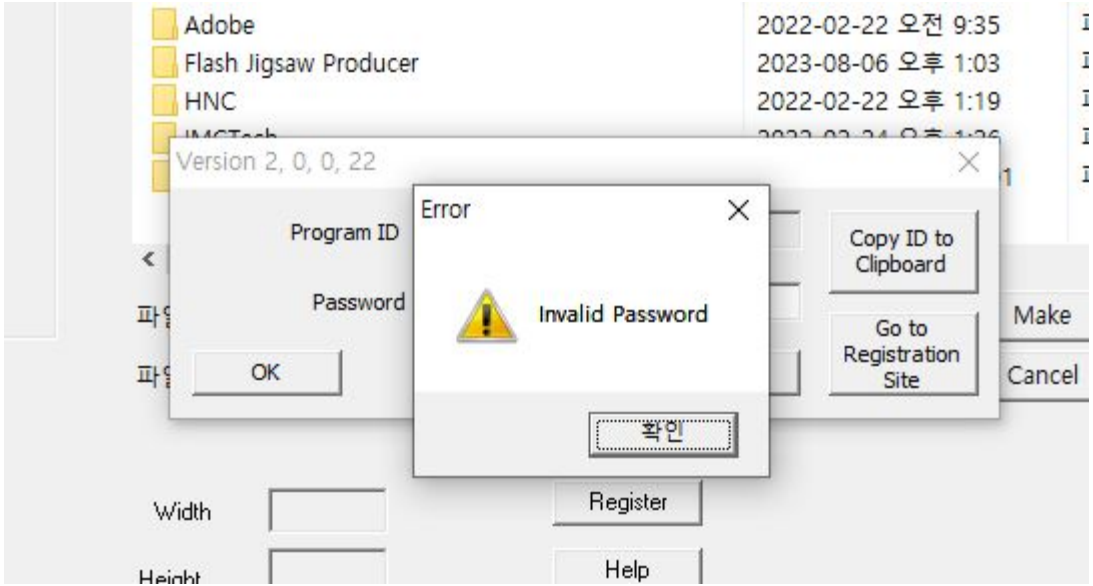
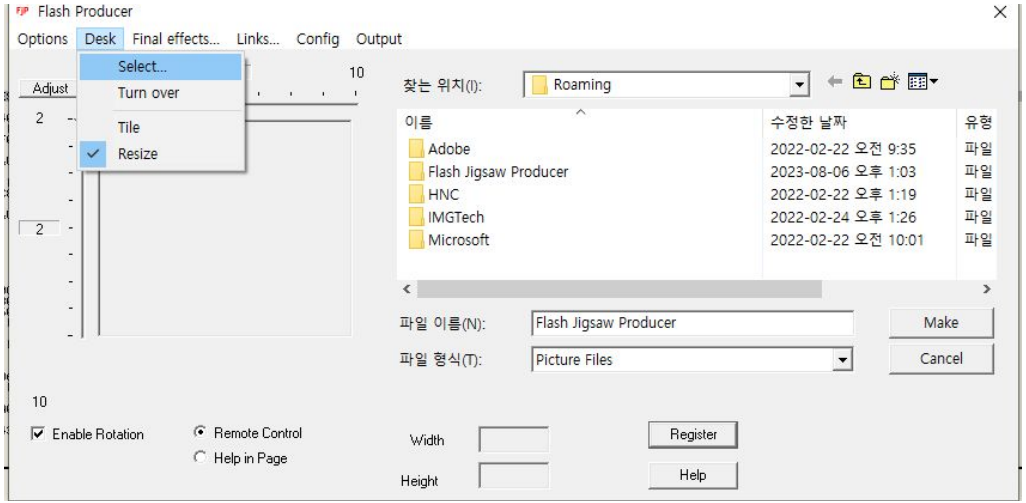


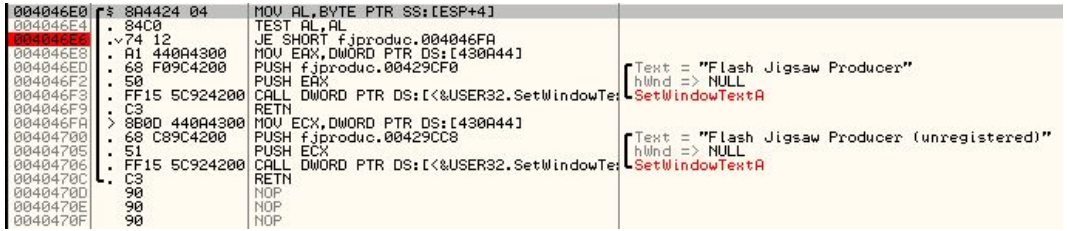
이번 튜토리얼의 목적은 pane windows를 이용한 중급 패치이다.

이전 프로그램과 다르지 않게 register하는건데, 레지스터 키를 직접 찾아 등록하지 않고, register하는게 이번 튜토리얼의 목적이다.

이 그림은 register 실패 시 보이는 오류이다.



desk -> select 버튼을 누르면 등록한 사람만 사용할 수 있다고, 나온다. 이번 패치를 통해 이 기능을 사용할 수 있게 하는것이 목적이다.



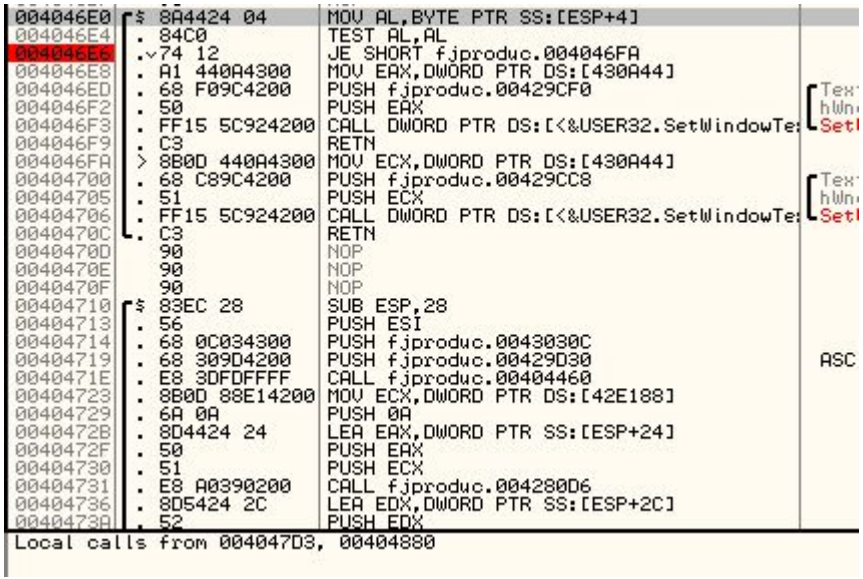
프로그램 실행시 윈도우 바에 원래 unregister라는 문자열이 있는데, 이 프로그램에서는 보이지 않아 있다고 가정하에 분석을 진행한다.

이전 분석과 다를바 없이 문자열 검색으로 unregistered 문자열을 호출하는 영역으로 이동한다.

그럼 다음과 같이 두개의 SetWindowsText API가 나온다.

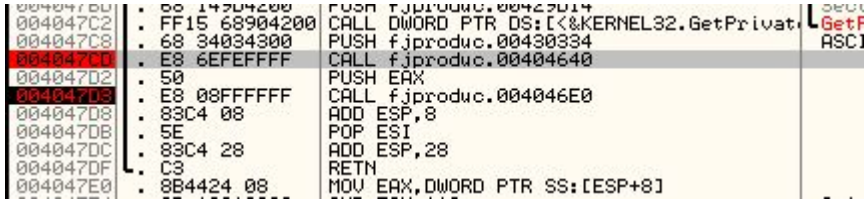
bp가 걸린 분기문을 통해 보여지는 문자열이 다르다.

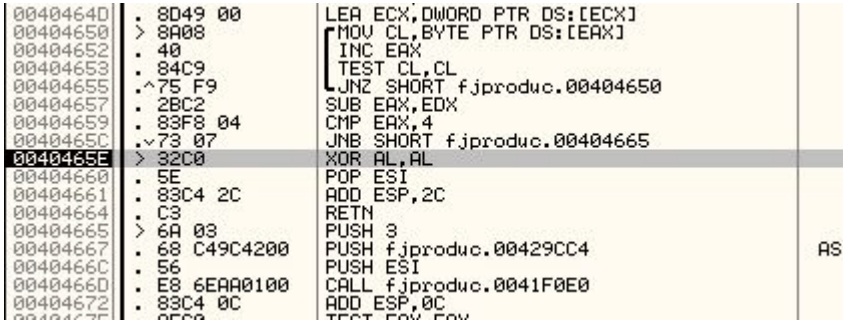
위에 보면 AL 레지스터에 ESP+4 주소에 있는 값을 집어넣는데, 이 부분의 값이 어디서 결정되는지 위에서 살펴보도록 한다.

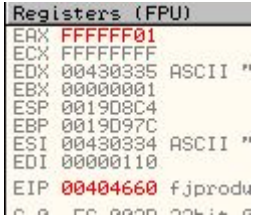


위 MOV AL... 부분을 클릭해 보면 어디서 호출하는지 알 수 있다. 이 부분이 바로 pane windows다.

해당 주소로 이동하여 bp를 건 후 다시 실행한다.







그럼 해당 주소에서 호출하는 걸 볼 수 있다. 그 전에 AL에 값을 집어넣는 PUSH EAX 함수가 보인다. 아마 그전 함수에 의해 AL 값이 결정되는걸로 보인다. 4047CD 주소에 bp를 걸고 함수를 분석해본다.

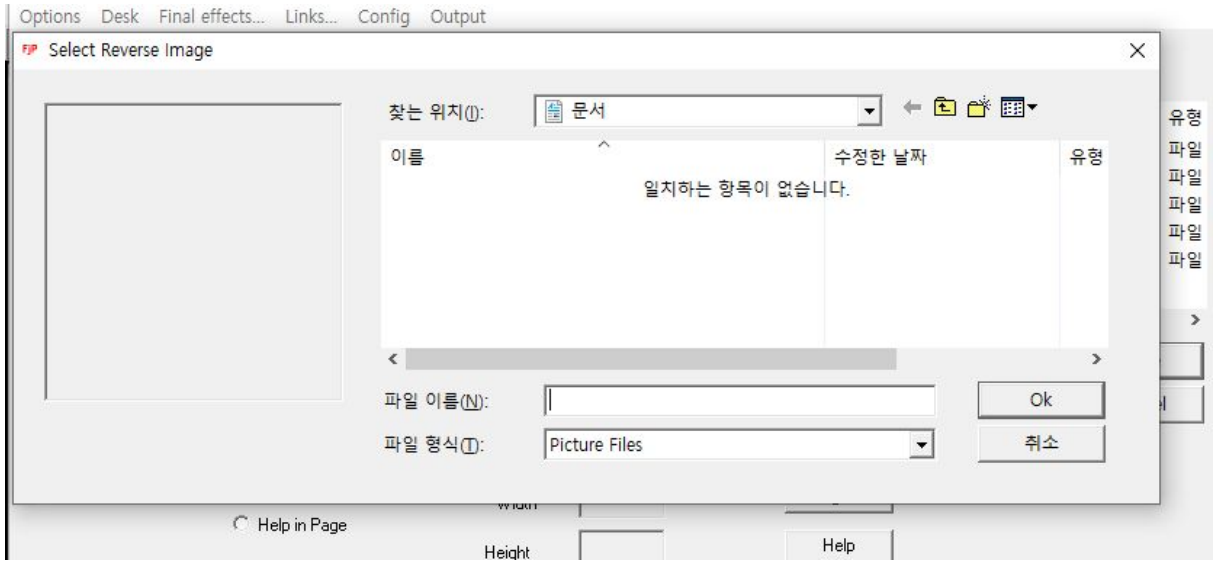
안에 보면 내가 입력한 레지스터 값과 글자수를 비교한다. 여기 보니 총 4글자를 입력하라고 나온다.

그리고 해당 주소에서 XOR AL, AL을 통해 값을 결정하는걸 알 수 있다.

이 명령을 MOV AL, 1로 바꿔 AL 값이 1이 되게 한다.

그럼 AL값이 1로 바뀐걸 볼 수 있다.

그러면 아까 TEST AL, AL값이 1이 되고, JE도 성립되지 않아 unregistered문자열이 호출 안되는걸 볼 수 있다.



그리고 실행해보면 아까 못썼던 select기능이 잘 실행되고, 등록할 때 나왔던 오류 메시지도 안뜨게 된다.