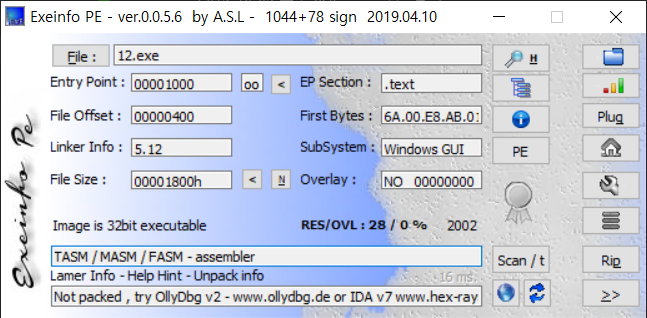
**12.exe -** Key를 구한 후 입력하게 되면 성공메시지를 볼 수 있다

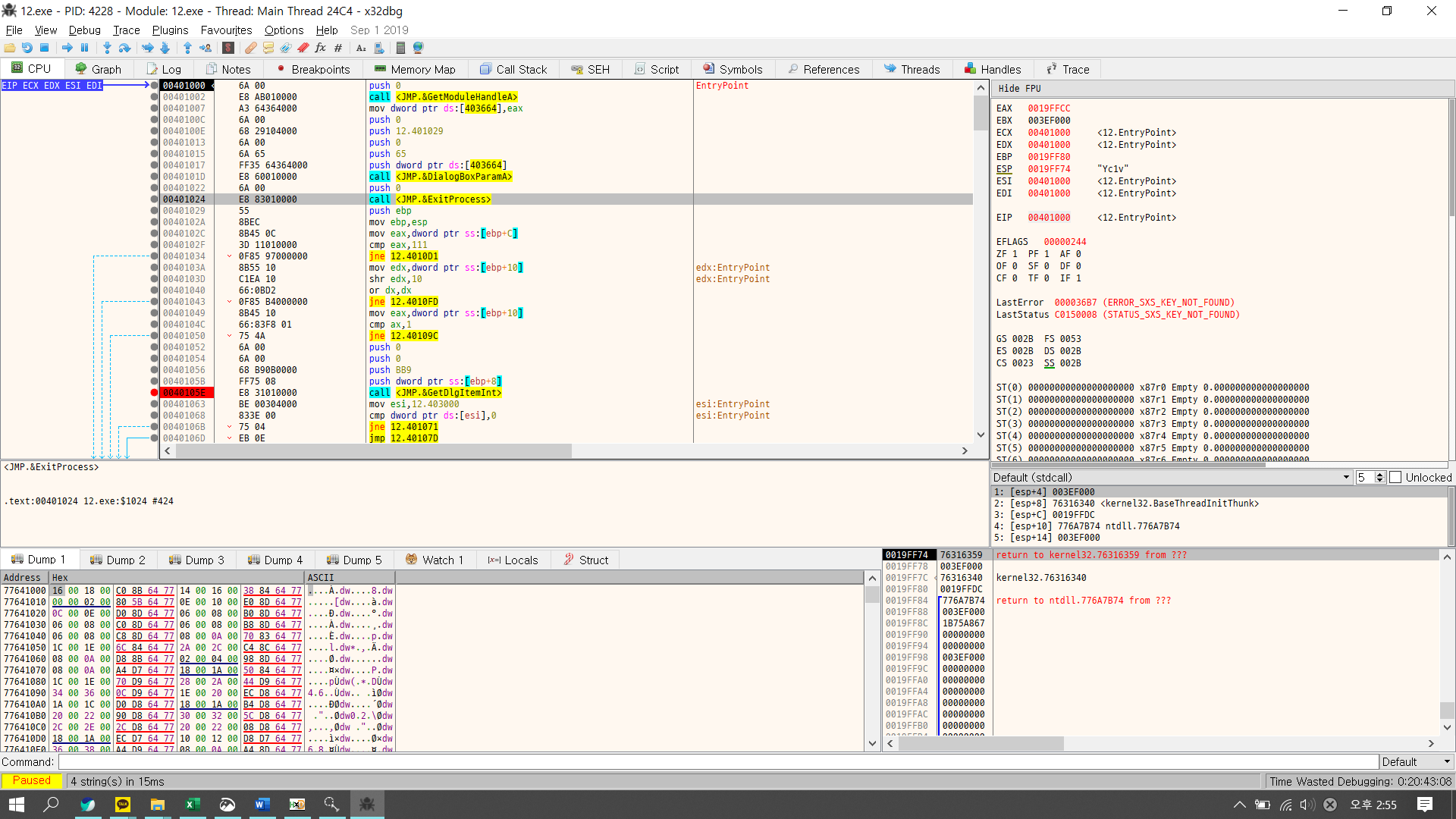
이때 성공메시지 대신 Key 값이 MessageBox에 출력 되도록 하려면 파일을 HexEdit로 오픈 한 다음 0x???? ~ 0x???? 영역에 Key 값을 overwrite 하면 된다.

문제 : Key값과 + 주소영역을 찾으시오 Ex) 7777777????????

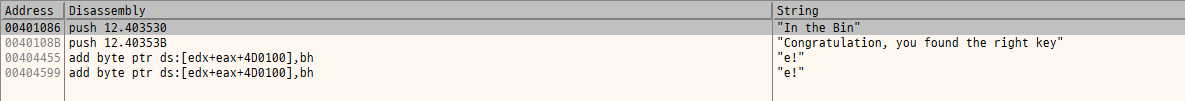


PE 분석을 통해 Packing이 되지 않았다는 것을 확인할 수 있다.

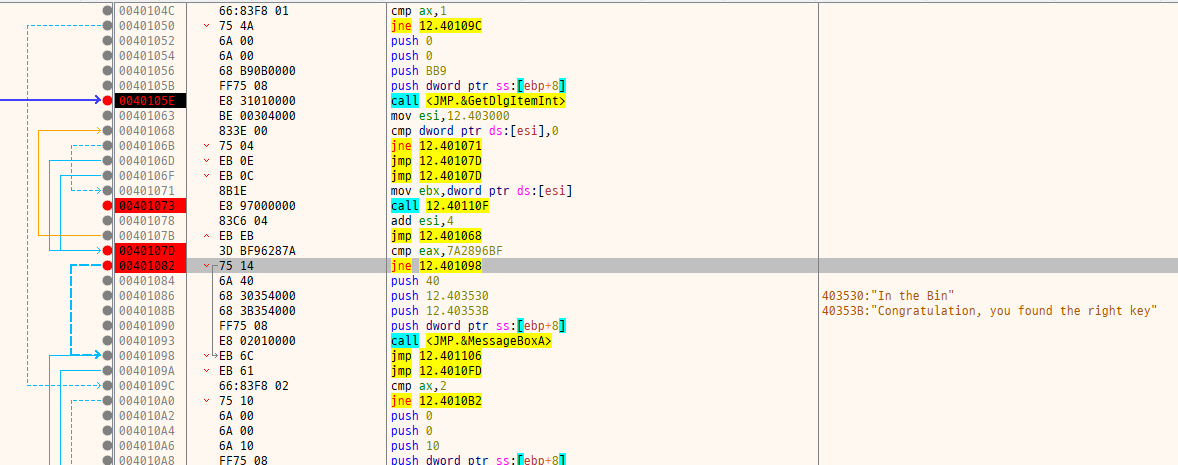
이제 X32DBG를 통해 분석을 해본다.



이제 여기서 문자열 검색을 통해 분석을 해본다.



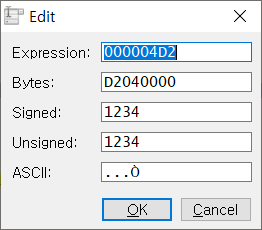
검색을 통해 성공 메세지를 발견했다. 이때 메시지 주소로 들어가 분석을 해본다.



Jne를 통해 성공 메시지를 출력 하는지에 대해 분기점이 갈리고 있는데 이때 위의 cmp eax.7A2896BF를 통해 비교 하여 키 값을 체크 하고 있는 것을 볼 수가 있다.

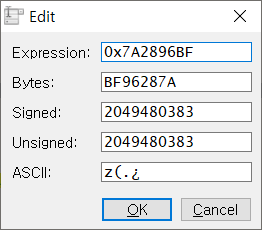


이때 EAX의 값을 확인해본다.



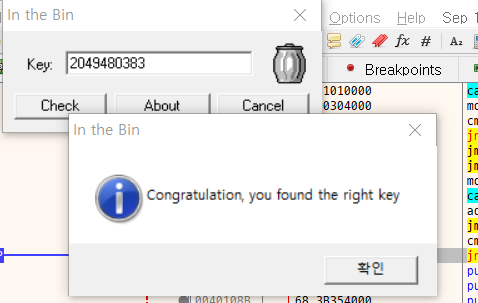
테스트를 위해 입력한 키 값인 1234가 16진수로 인코딩 되어 저장되어 있는 것을 알 수가 있다.

이때 cmp를 하는 7A2896BF를 10진수로 바꾸어 확인해 본다.



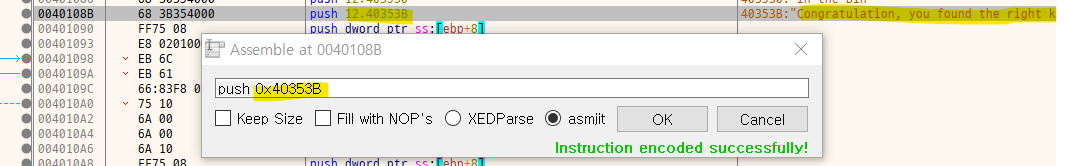
이때 키 값은 2049480383라는 것을 알 수가 있다.

이제 이 찾은 키 값이 정확한지 체크를 해본다.

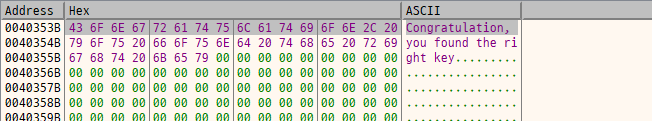


그 결과 정확한 키 값을 찾았다는 것을 확인할 수가 있다.

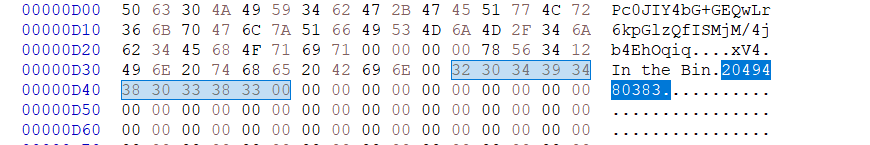
이제 문제로 돌아와 성공 메세지 부분에 키 값을 넣어서 수정을 해본다.



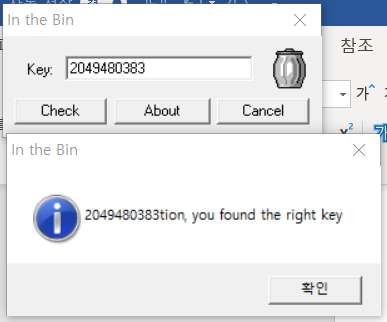
문자열을 PUSH 하는 주소를 확인하여 성공 메시지를 참조하는 주소를 확인하고



덤프를 확인하여 offset 주소를 구하여 수정을 진행해본다.



Offset 주소를 가지고 수정을 하여 성공 시리얼 키 값을 삽입한다.

****

수정한 파일을 실행해서 정상적을 동작하는 것을 확인할 수가 있다.

**정답: 20494803830D3B0D45**