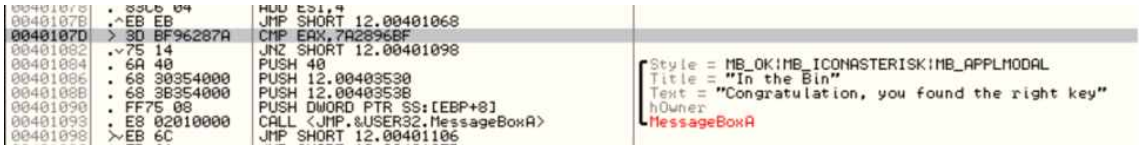
CodeEngn Basic RCE L12
: Key를 구한 후 입력하게 되면 성공메시지를 볼 수 있다
이때 성공메시지 대신 Key 값이 MessageBox에 출력 되도록 하려면 파일을 HexEdit로 오픈한 다음 0x???? ~ 0x???? 영역에 Key 값을 overwrite 하면 된다.
문제 : Key값과 + 주소영역을 찾으시오

Ex) 7777777?????????

1. key 값 구하기



올리디버거로 열어 실행 시킨 화면이고, 우리는 키 값을 알아야 하기 때문에 "Congratulation, you foung the right key" 앞에서 어떤 명령어들이 있는지를 유심하게 보아야 한다.

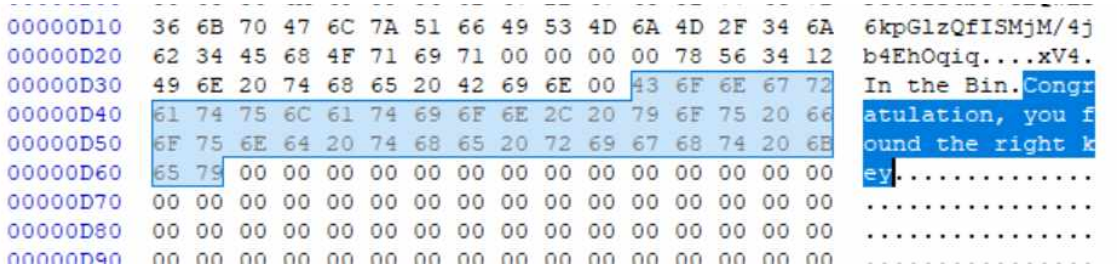
CMP EAX,7A2896BF
JNZ 00401098
-> EAX의 값에서 7A2896BF를 마이너스한 결과가 0이 아니면 00401098로 점프하라 !

즉, 올바른 키 값을 찾았다는 메세지가 뜨기 위해서는 EAX와 7A2896BF가 같아야 한다. 왜냐하면 EAX - 7A2896BF가 0이어야 JNZ에서 가리킨 주소로 점프하지 않고 그대로 메세지 박스를 출력하기 때문이다.

그럼 사용자가 입력하는 키 값이 EAX에 저장이 되고, 7A2896BF와 같아야 하므로, 키 값은 7A2896BF인것을 알 수 있다. 근데 올리디버거 상에서 프로그램을 올려봤을 때 7A2896BF는 16진수를 사용하고 있으므로 10진수로 바꾸어주면 2049480383 인것을 알 수 있다.

따라서 키 값은 2049480383 이다.

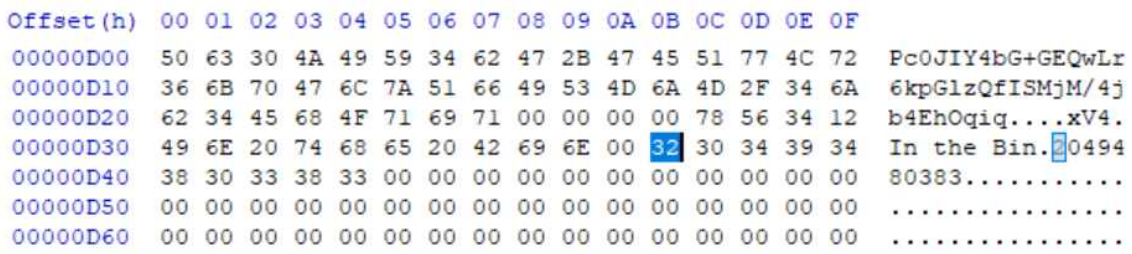
2. HexEdit 으로 키 값을 메세지 박스에 출력하기



HEXEDIT을 다운 받아서 DATA 부분을 살펴보면 성공메세지가 있는 부분이 보이는데, 문제에서 여기서 overwrite해서 키 값이 나오도록 하라고 했기 때문에, 43 6F 6E 67 72 ~~~~ 79의 부분을 지우고 키 값을 넣어주어야 한다.

2049480383을 16진수 아스키코드로 바꾸어 넣어줘야 하는데 그렇다고 7A2896BF를 넣으면 안된다 *** 구글에서 16진수 아스키코드를 검색하면 이미지 탭에서 쉽게 찾아 볼 수 있다.

2는 표에서 32,
0 - > 30
4 - > 34
9 - > 39
4 - > 34
8 - > 38
0 - > 30
3 - > 33
8 - > 38
3 - > 33
이므로 32 30 34 39 34 38 30 33 38 33을 붙여넣어주면 된다.



```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000D00   50 63 30 4A 49 59 34 62 47 2B 47 45 51 77 4C 72   Pc0JIY4bG+GEQwLr
00000D10   36 6B 70 47 6C 7A 51 66 49 53 4D 6A 4D 2F 34 6A   6kpGlzQfISMjM/4j
00000D20   62 34 45 68 4F 71 69 71 00 00 00 00 78 56 34 12   b4EhOqiq....xV4.
00000D30   49 6E 20 74 68 65 20 42 69 6E 00 32 30 34 39 34   In the Bin.20494
00000D40   38 30 33 38 33 00 00 00 00 00 00 00 00 00 00 00   80383...........
00000D50   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000D60   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

overwrite 해주었더니 data에서 2049280383으로 잘 출력되고 있다는 것을 확인할 수 있다!!
이때 문제에서 0x??????의 주소 값을 원하기 때문에 내가 덮어씌운 주소 값의 시작인 00000D3B ~ 00000D45 이다.
이때 00000D44가 끝이라고 생각할 수 있는데, 문자열은 그 끝을 알리는 NULL값이 항상 존재를 하고, 이는 16진수 아스키코드에서 00으로 표시되기 때문에 0D45가 마지막이 되는 것이다.

따라서 답은 20494803830D3B0D45 이다.