

# REVESING

**99999999**

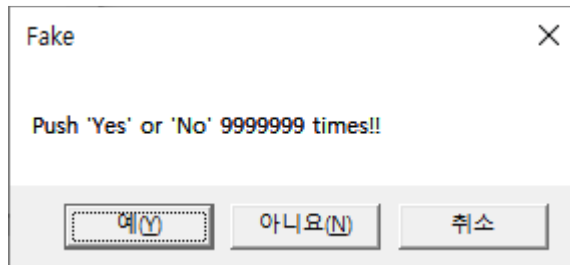
인공지능사이버보안학과

2017270706 김호영

9999999

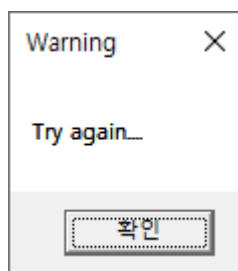
WRITE UP

문제 파일을 실행해보면 다음과 같은 창이 나온다.

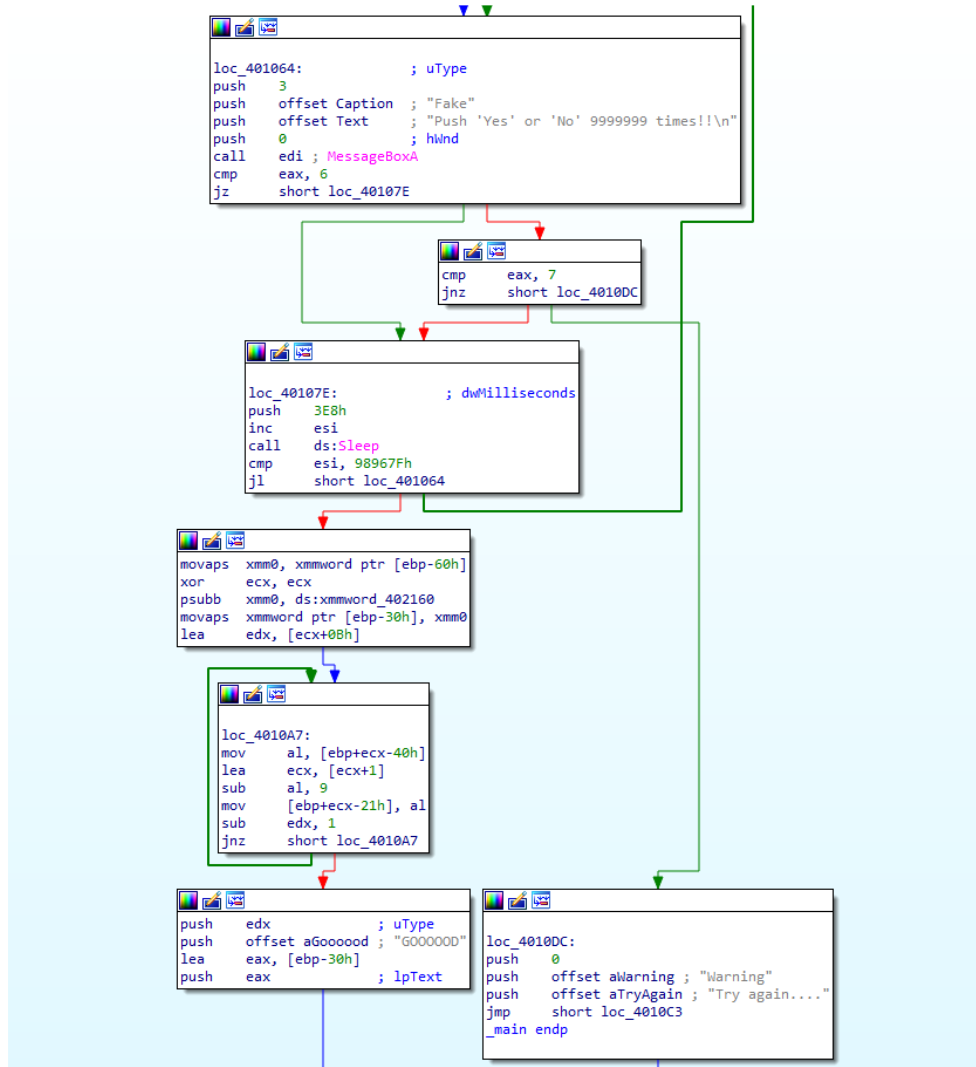


‘예’ 와 ‘아니오’ 버튼을 9999999 번 누르면 플래그를 주는 문제인 것 같다.

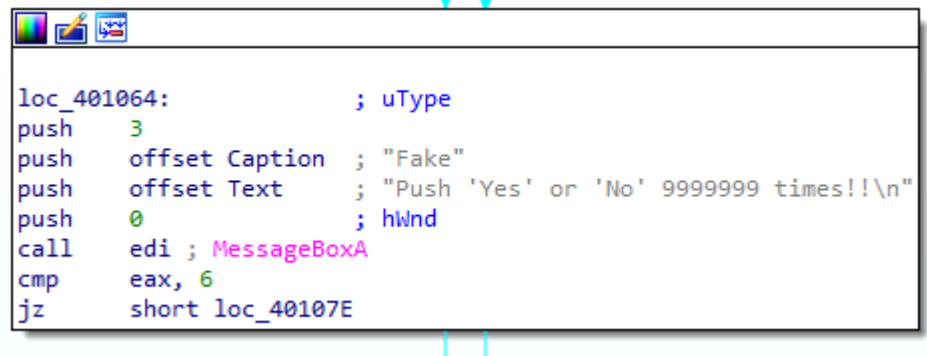
‘예’ 와 ‘아니오’ 버튼을 누르면 창이 다시 나오고, 취소 버튼을 누르면 다음과 같은 창이 나오면서 프로그램이 종료된다.



해당 파일을 IDA 로 열어보면 다음과 같은 구조로 나온다.



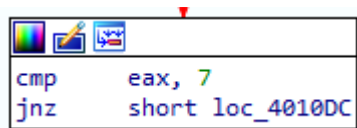
하나씩 자세히 살펴보면, 먼저 메시지 박스가 출력되는 부분



```

loc_401064:                ; uType
push    3
push    offset Caption    ; "Fake"
push    offset Text       ; "Push 'Yes' or 'No' 9999999 times!!\n"
push    0                  ; hWnd
call    edi ; MessageBoxA
cmp     eax, 6
jz      short loc_40107E
  
```

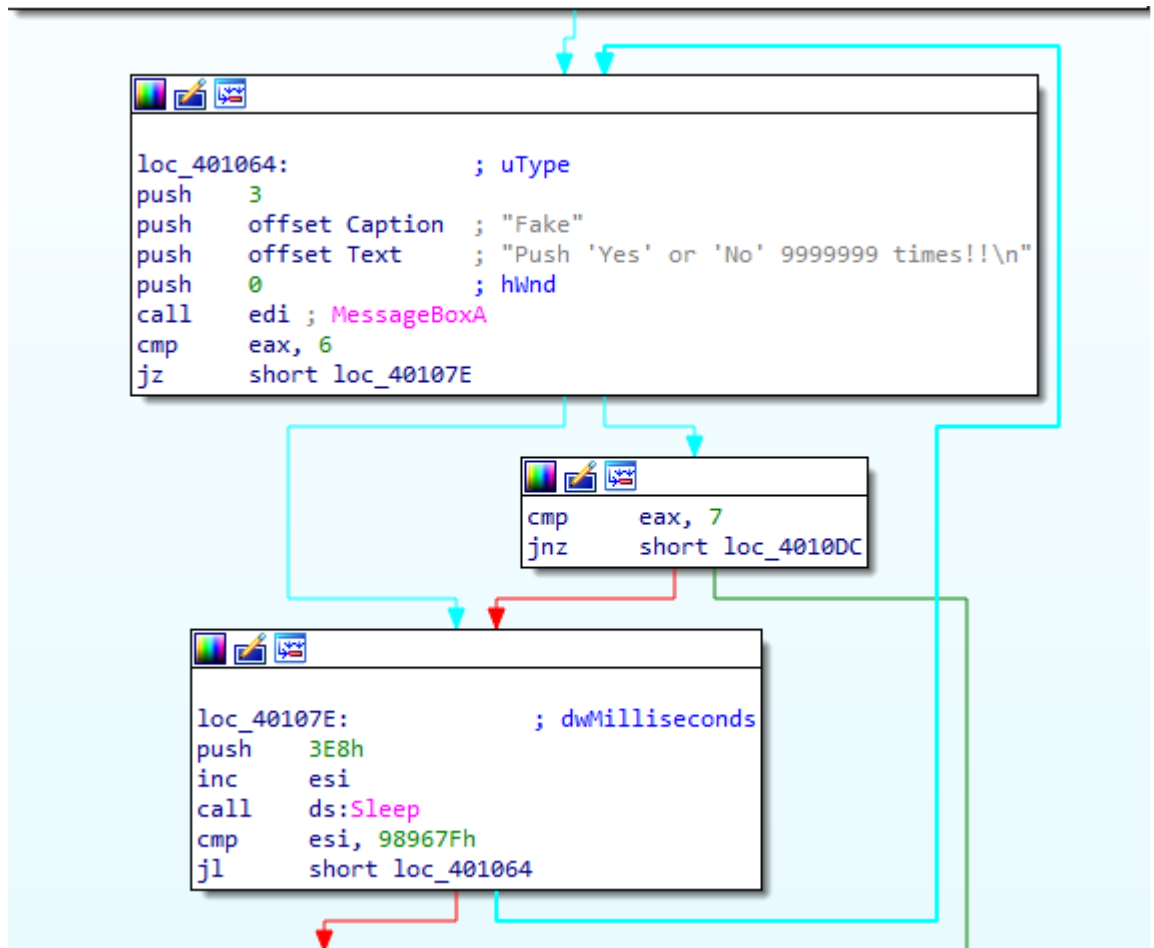
메시지 박스를 누르고 난 뒤의 값을 비교하는 부분이다. 해당 값이 7 이 나오면 취소문구로 가는 걸로 보아, 취소 버튼을 누르면 7 을 리턴해준다는 것을 알 수 있다.



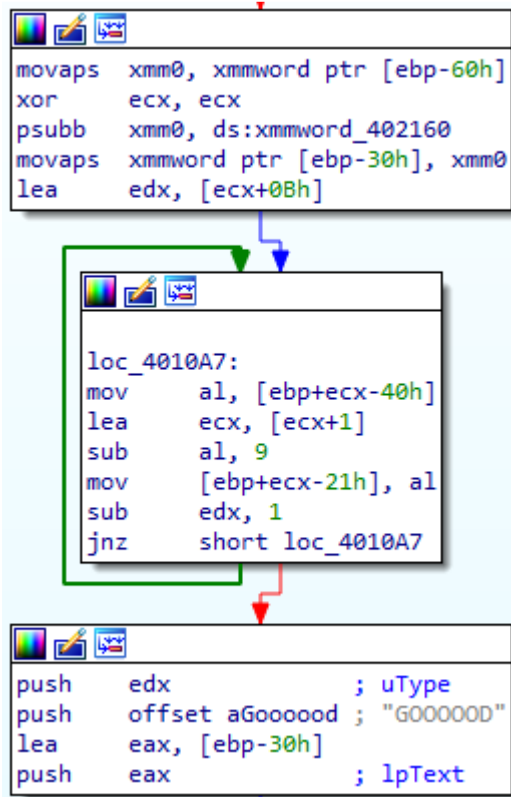
```

cmp     eax, 7
jnz     short loc_4010DC
  
```

Loc\_40107E 부분을 확인해보면 esi 값을 증가시키고 esi 값을 0x98967F(9999999)와 비교하는 것을 알 수 있다. 즉, 반복문이라는 것을 확인할 수 있다. 디버거를 이용해서 esi 값을 0x98967F(9999999)로 변경해주면, 해당 반복문을 넘어가는 것을 확인할 수 있다.



Loc\_40107E 를 통과하고 나면 다음과 같은 블록이 나온다. 해당 반복문은 플래그를 출력해주는 반복문으로 반복문이 끝나면 플래그가 출력된다.



#### FLAG

