REPORT:

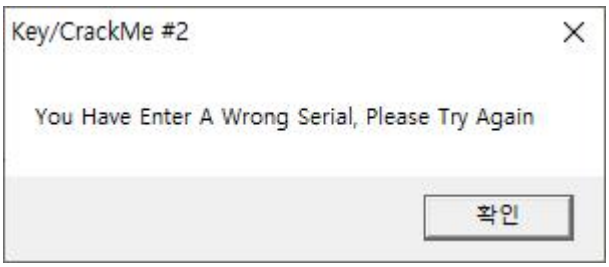
코드엔진 Basic RCE 14 Writeup

COLONY
1824275 정상지

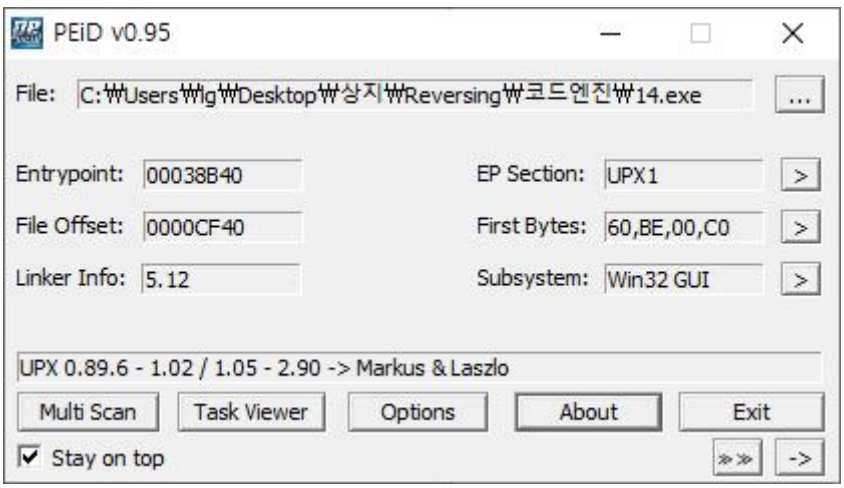
2021.07.24

Name이 CodeEngn 일때 Serial을 구하시오

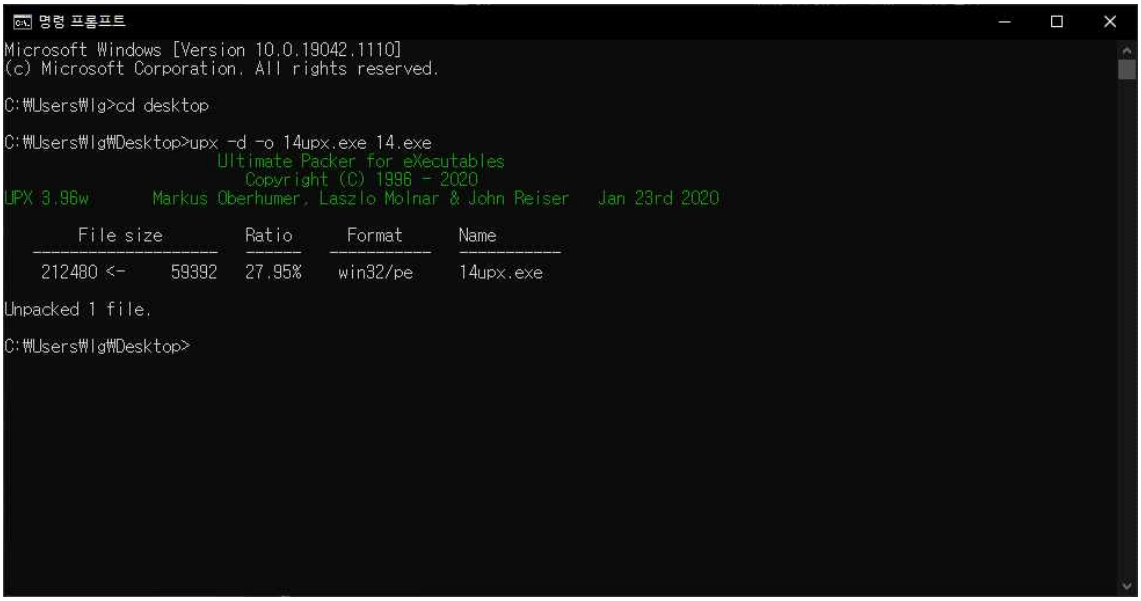
위와 같이 프로그램은 name과 key값을 적을 수 있는 공간으로 나누어져 있다



key값이 틀릴 경우 위와 같은 메시지 박스를 출력한다



14번 문제는 upx로 패킹이 되어있는 것을 알 수 있다

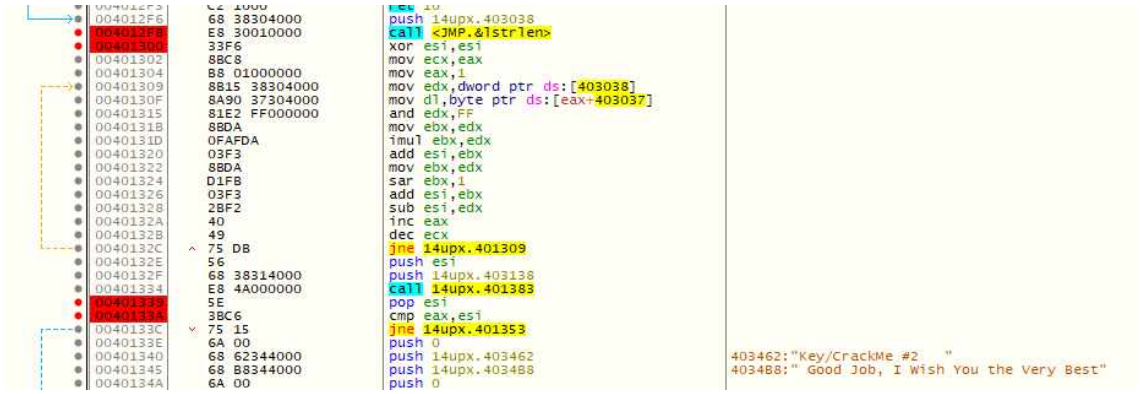


upx 언패킹을 진행한다

언패킹한 파일을 통해 디버깅한다

문자열 참조를 통하여 아까 전에 보았던 문자열의 위치를 확인한다

분기문에서 eax와 esi의 값을 비교하여 확인하는 것을 알 수 있다



분기문 이전의 함수에 중단점을 설정하여 해당 함수 및 분기문 이전의 메모리에 대해 확인한다

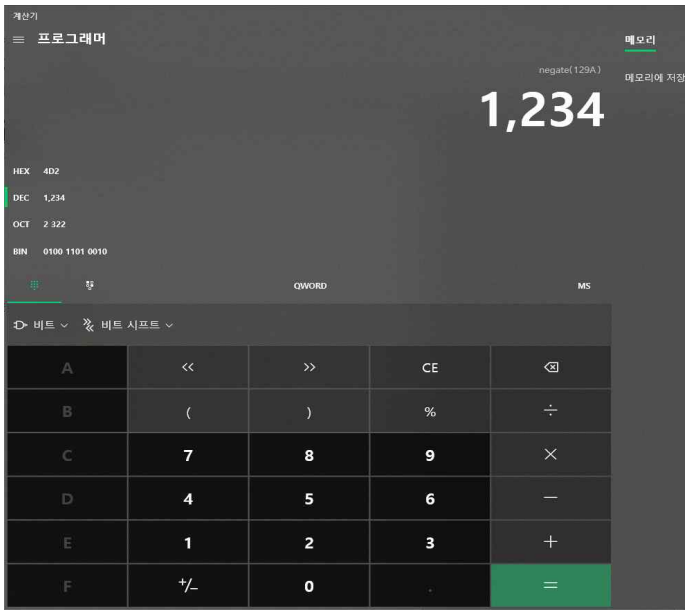
CodeEngn과 1234라는 Serial값을 입력하여 해당 함수의 동작을 확인한다

```
EAX   00000004
EBX   004011E2    14upx.004011E2
ECX   973ABED5
EDX   00000004
EBP   0019FA74
ESP   0019FA70    &"CodeEngn"
ESI   000507EE
EDI   00000111    L'đ'

EIP   004012FB    14upx.004012FB
```

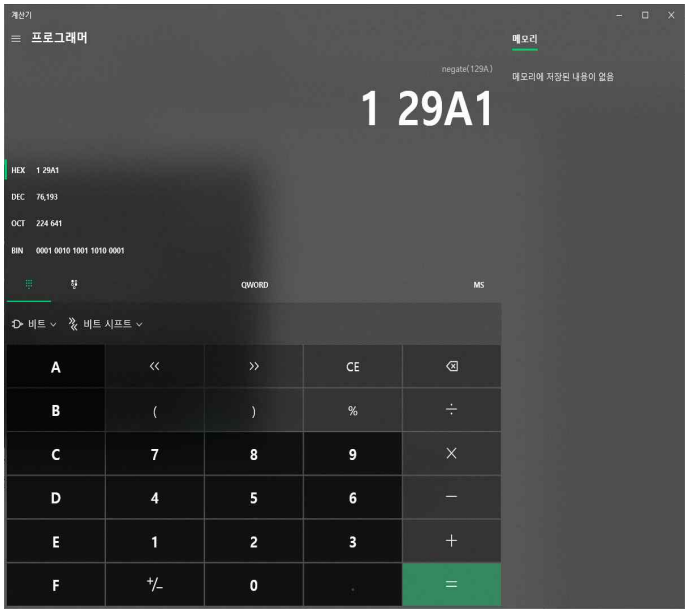
확인 시 EAX의 값이 Serial의 길이를 받아오는 것을 알수 있다

```
EAX   000004D2    L'Ä'
EBX   00000037    '7'
ECX   00000000
EDX   00403139    "234"
EBP   0019FA74
ESP   0019FA74
ESI   000129A1
EDI   00000111    L'đ'

EIP   0040133A    14upx.0040133A
```

분기문 이전의 레지스터의 값이다

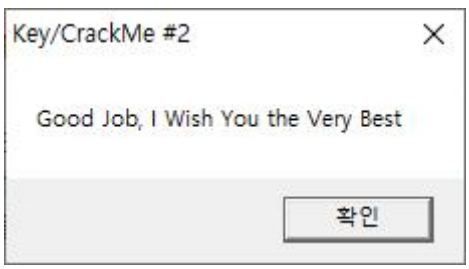


1234의 값이 HEX값으로 EAX에 저장되는 것을 알 수 있다
이 값이 ESI와 비교되므로 ESI에 저장되어있는 값을 DEC로 바꾼 값이 Serial임을 알 수 있다



129A1의 DEC값은 76193이다

해당 Serial을 넣고 check를 하면



위와 같이 성공한 것을 볼 수 있다

정답 : 76193