

2019.02.21. CodeEngn Basic 17

Tree to Tree

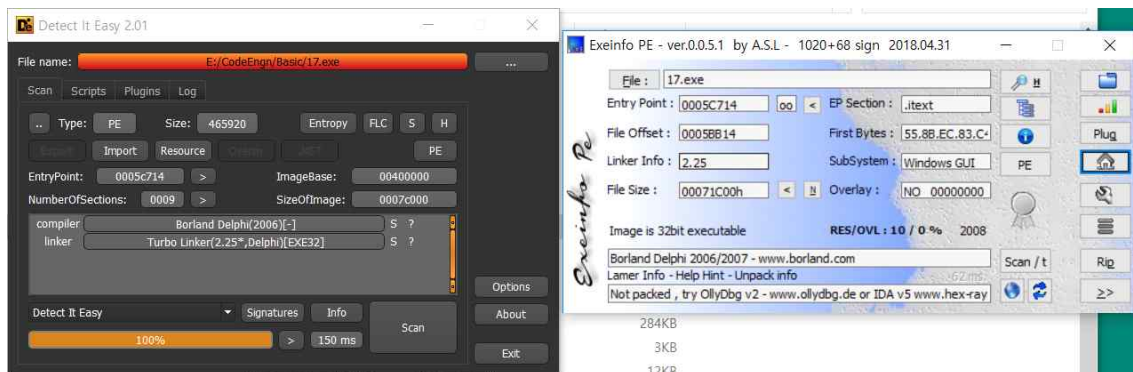
Basic RCE L17

Key 값이 BEDA-2F56-BC4F4368-8A71-870B 일때 Name은 무엇인가
힌트 : Name은 한자리인데.. 알파벳일수도 있고 숫자일수도 있고..
정답인증은 Name의 MD5 해쉬값(대문자)

— Author: WarRock
— File Password: codeengn

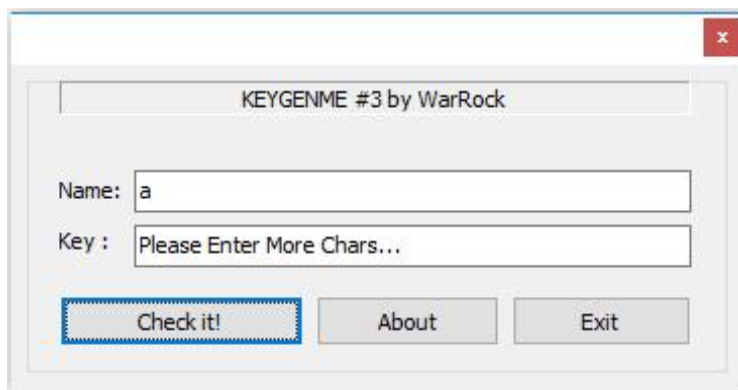


이번엔 Key값을 통해 아이디를 맞춰보자.

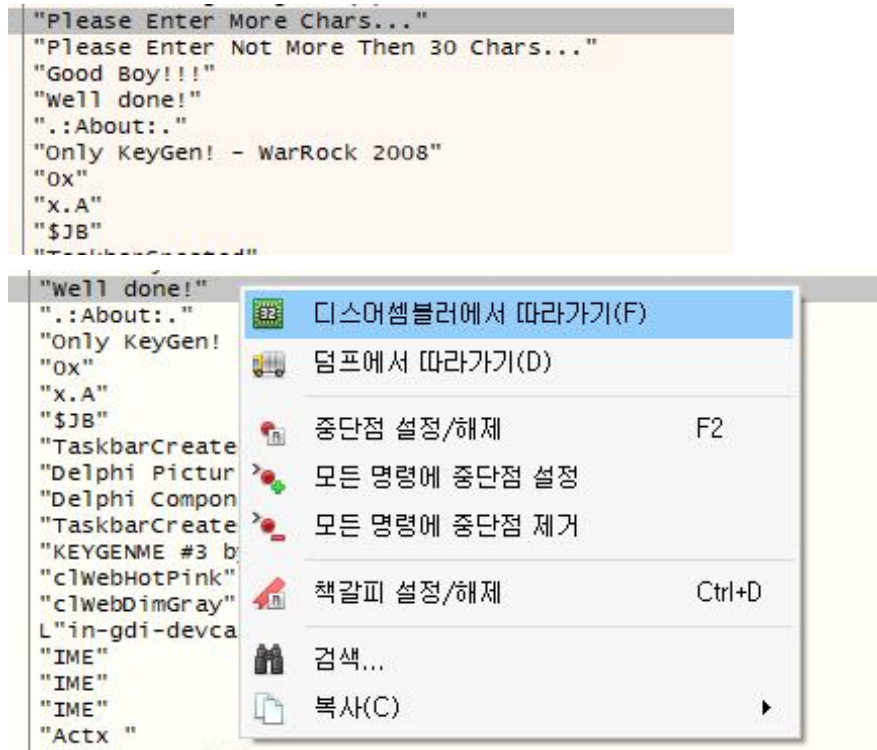


노 패킹

Name 문자열 길이 조건문이 있다.

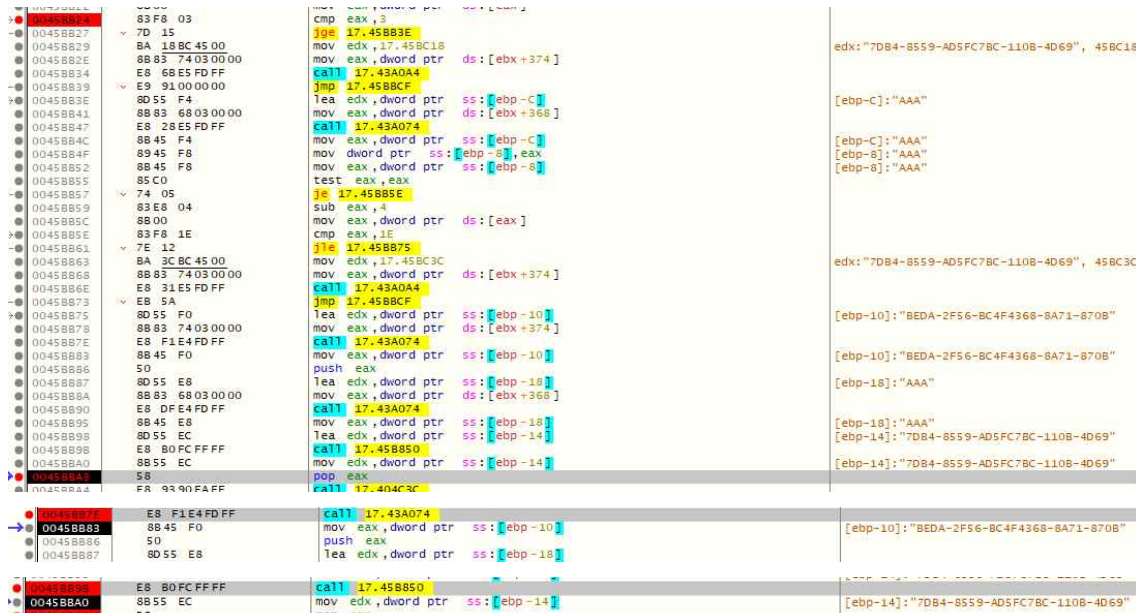


문자열을 찾으러 가서

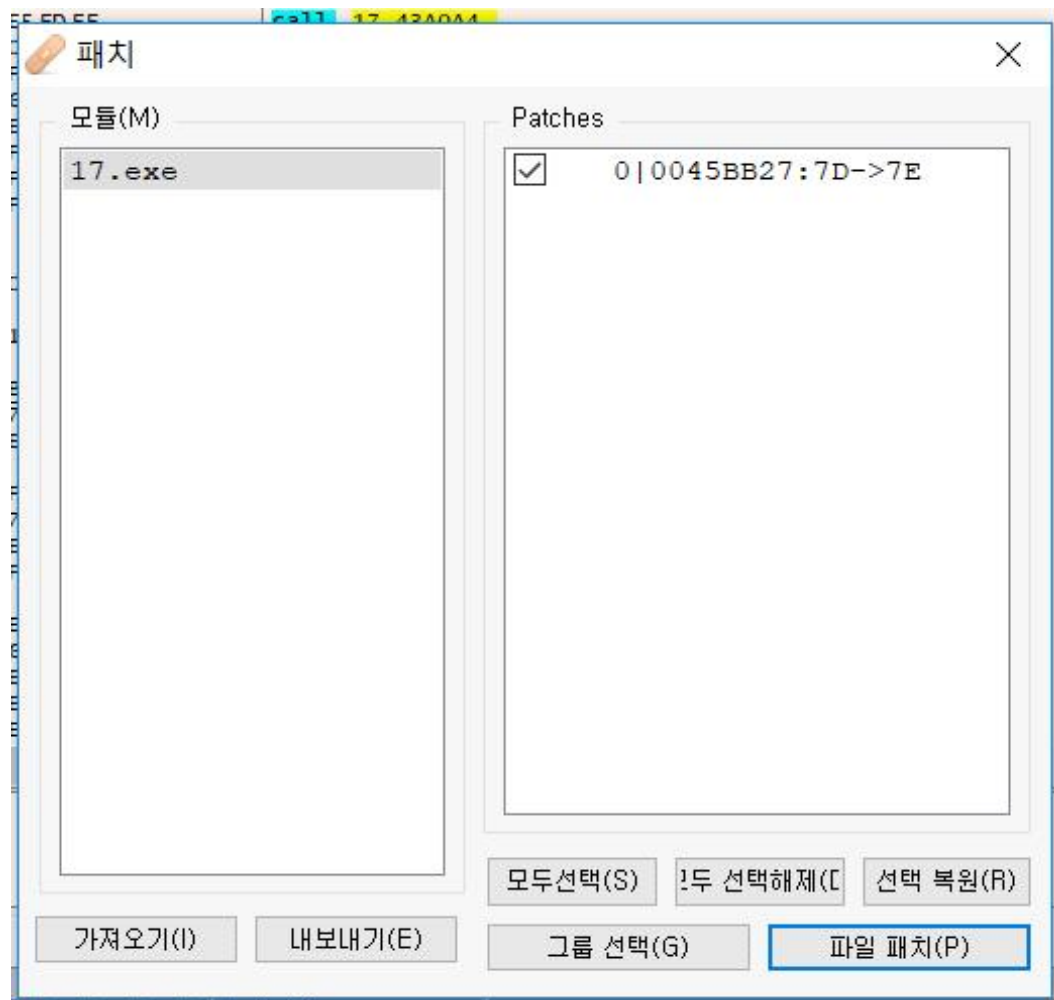
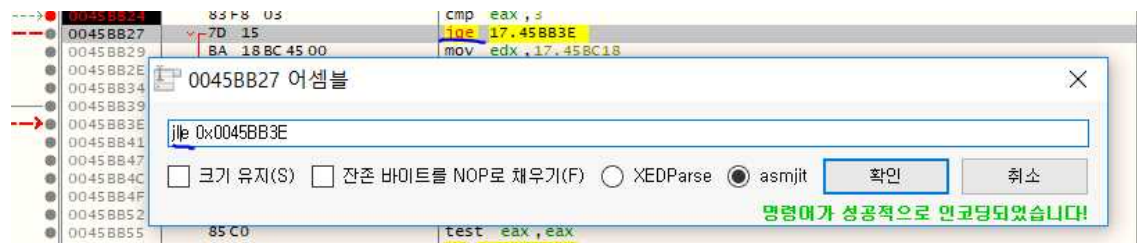


성공했을때의 문자열을 따라가봤다.

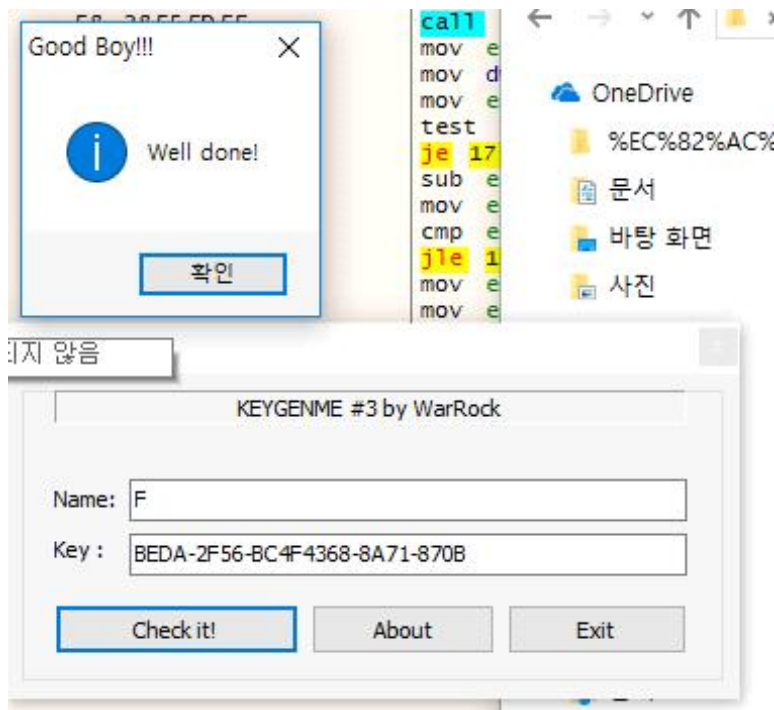
어떤 가공이 이뤄지고 시리얼 값을 비교한다.



시리얼 가공하는거 분석하는 것보다 0~9 a~Z까지 덱서너리 공격을 하는 것이 더 효율적이라고 판단하여 문자열 길이 조건문 패치
jge -> jle



0~9 a~Z까지 대입하는데 많은 시간이 걸리지 않았다.



이제 F를 MD5로 해쉬화하면

Your Hash: **800618943025315f869e4e1f09471012**

Your String: F

Use this generator to create an MD5 hash of a string:

800618943025315f869e4e1f09471012

Clear