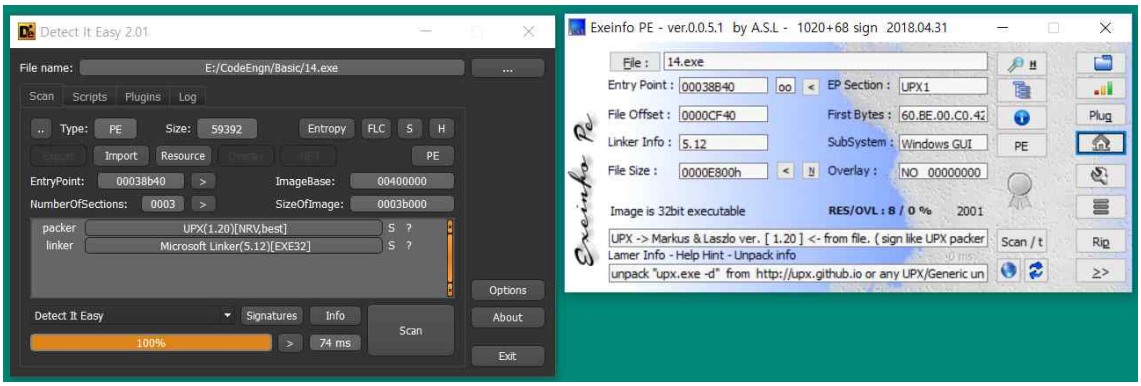
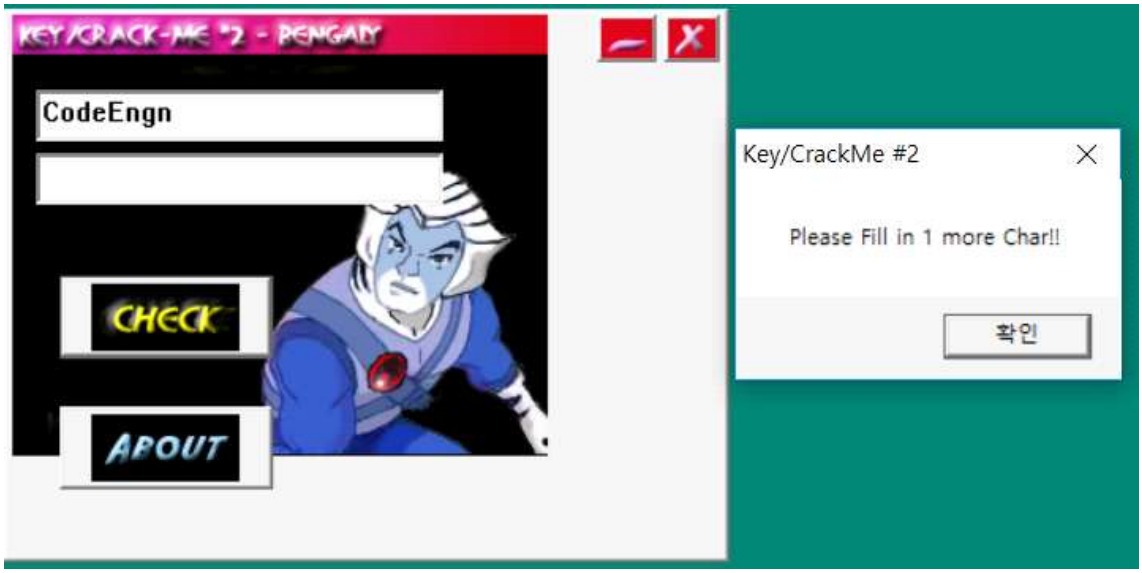
2019.02.17. CodeEngn Basic RCE L14

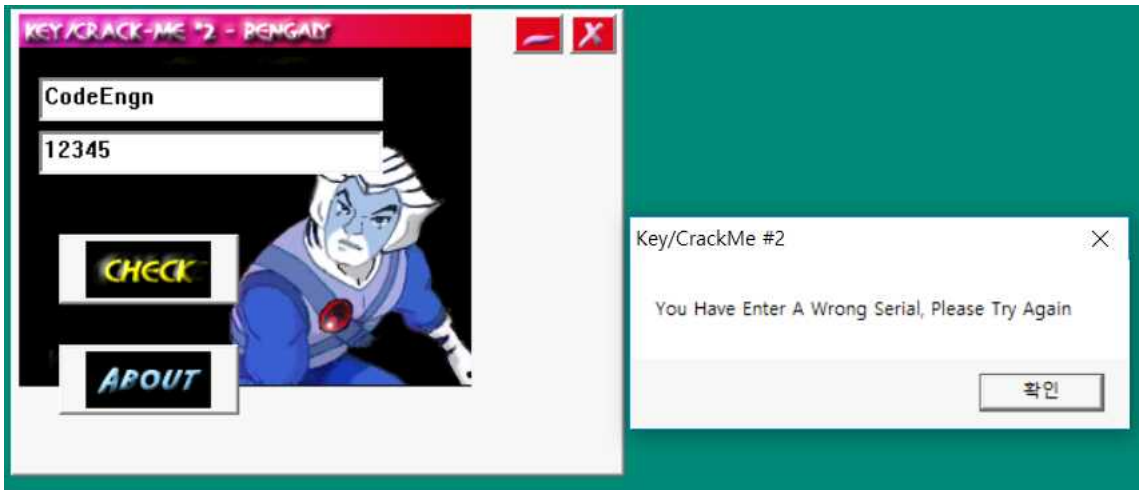
Tree to Tree

PE분석기로 보니 UPX패커로 패킹되어있다.



일반적으로 실행했을 때 문자열들을 확인했고 칸을 꼭 채워야 한다.





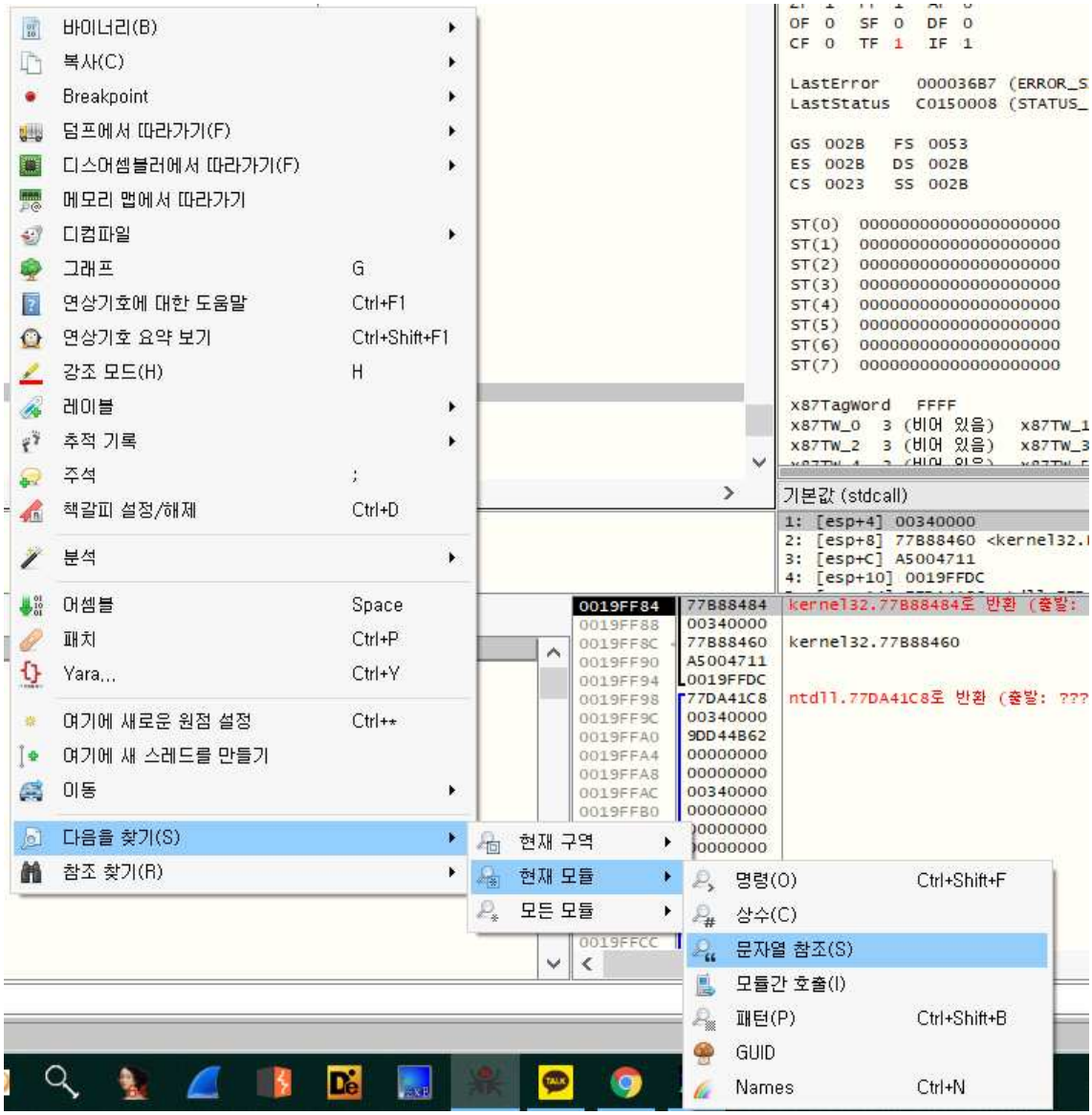
브레이크 포인트로 pushad와 popad바로 하단 jmp문에 걸고

유형	주소	Module/Label/Exception	상태	디스어셈블리
소프트웨어				
	00438B40	<14.exe.EntryPoint>	One-time	pushad
	00438C8F	14.exe	활성화됨	jmp 14.401000

OEP를 발견 00401000
덤프했는데...

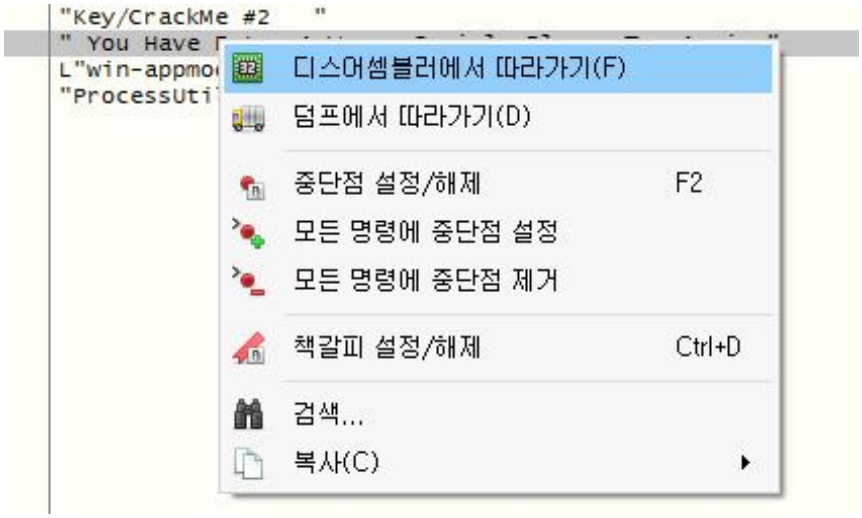
악성코드??
Trojan/Win32.Ruftar.C138568
망했다 이미 실행시켰는데..
악성코드 분석으로 바꿔야하는거 아닌가요..?

우선 문제를 풀기위해 OEP지점에서 현재모듈 문자열들을 살펴봤습니다.



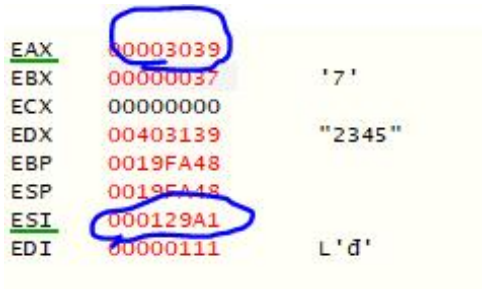
성공문구가보입니다.

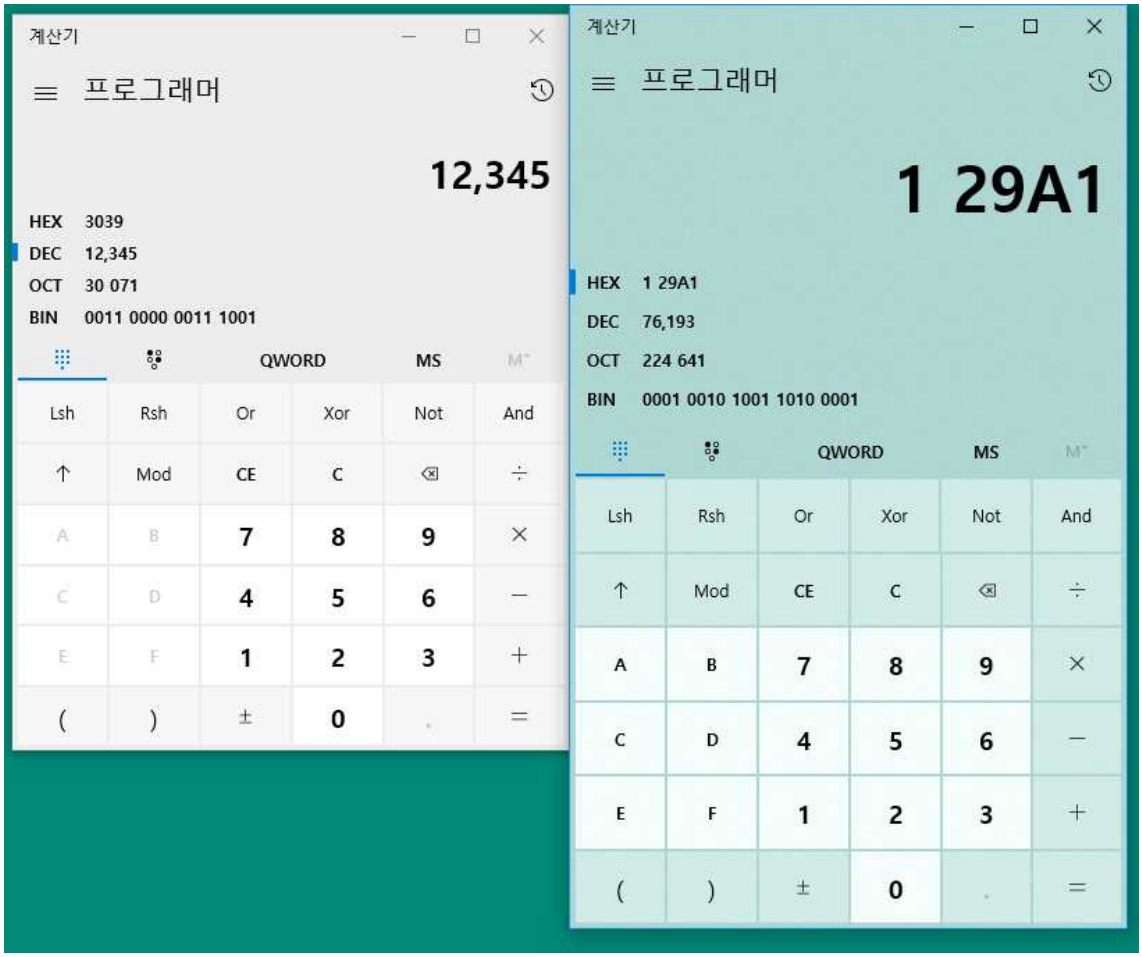
바로 디스어셈블러에서 따라가기



분기문 바로 위쪽 비교구문에서 레지스터의 변화를 관찰해보면

입력값 “12345“가 문자열 -> 숫자로 변환 16진수 3039 EAX
비교하는 값은 16진수 129A1이므로
정답은 10진수 76193으로 예상





CodeEngn과 76193을 넣어보니

Clear.... 그나저나 악성코드.....