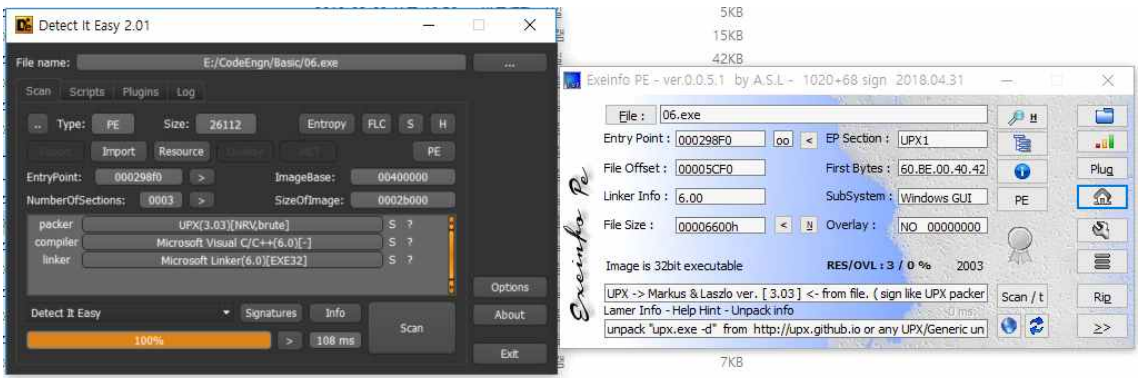
19.02.13 CodeEngn Basic RCE L06
Tree to Tree

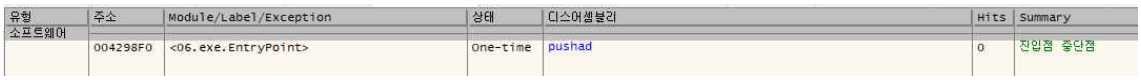
Unpack을 한 후 Serial을 찾는문제



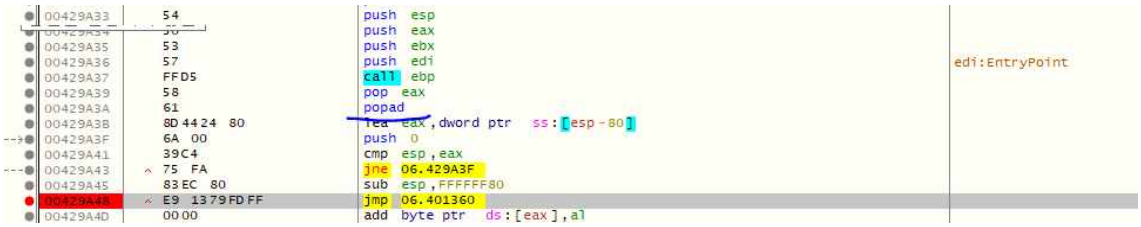
Detect It Easy로 보니 5번문제와 같은 UPX로 팩되어있는거 확인

그냥 실행시켰을 때 모습
아무 문자나 쳐봤다.

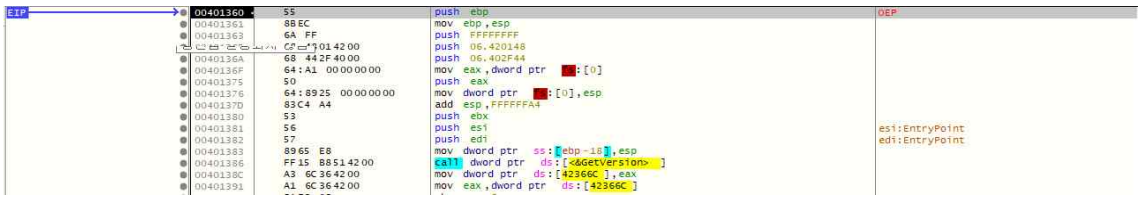
이제 문제 5 unpack한것과 같이 먼저 pushad지점에 breakpoint를 걸고



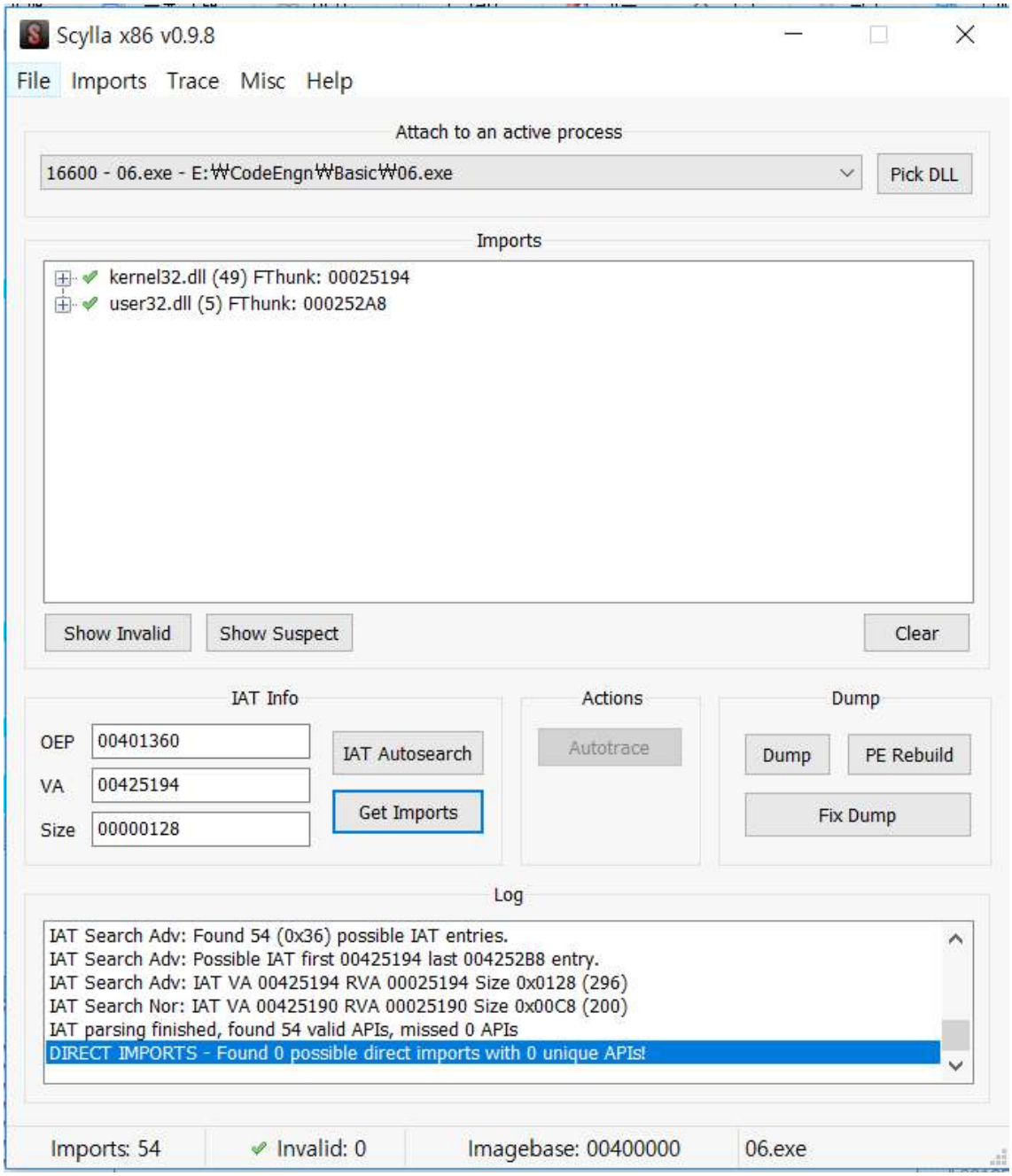
popad부분을 찾으러 내려간다.
찾고나면 jmp하는곳에 break포인트를 걸고 실행시킨 후

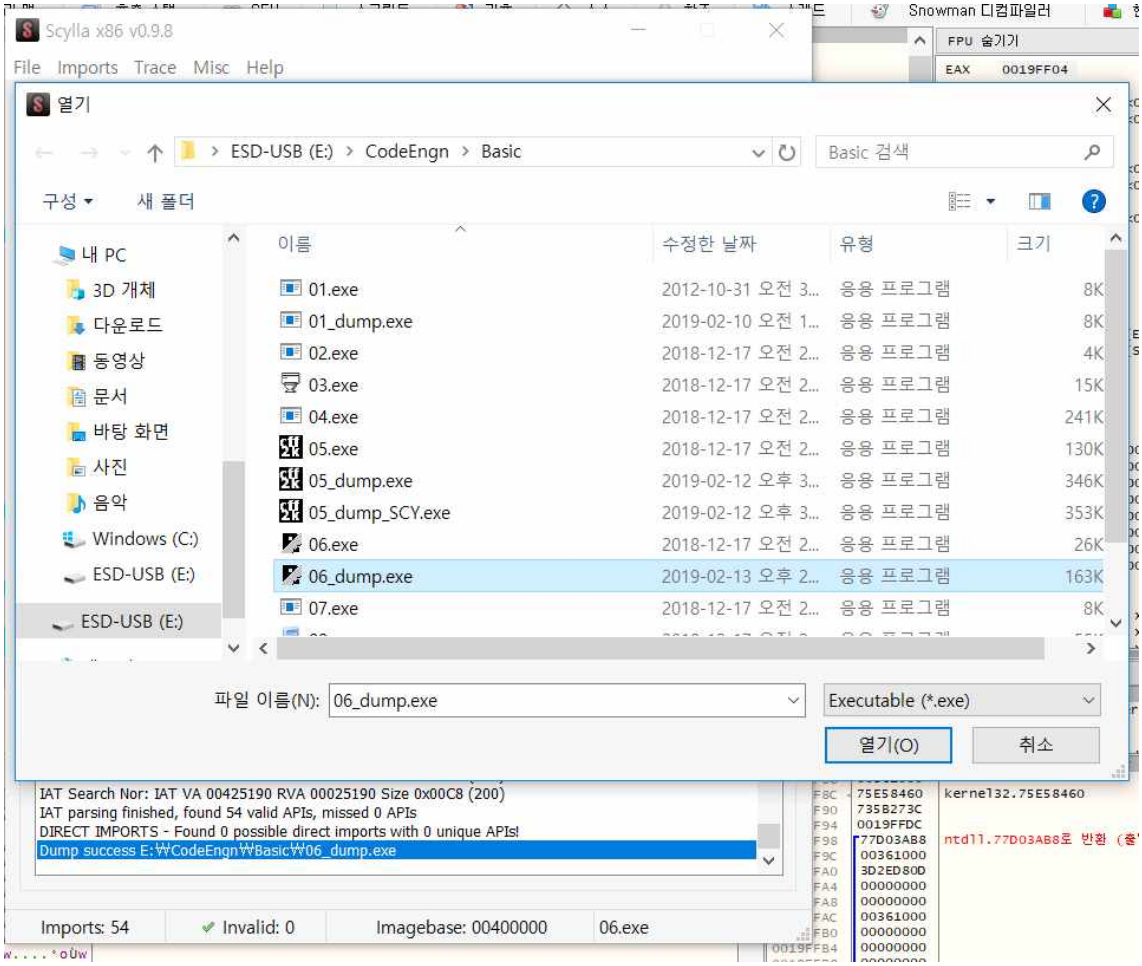


한스텝만 실행시키면 OEP에 도달한다.

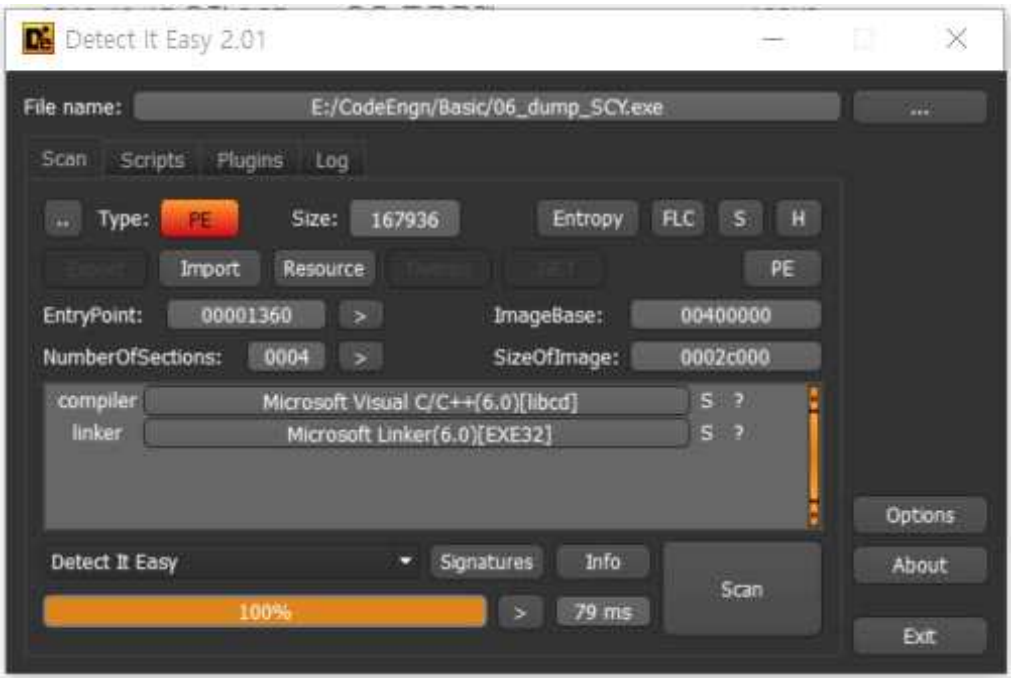


Scylla x86을 이용하여 덤프, Fix dump해주면





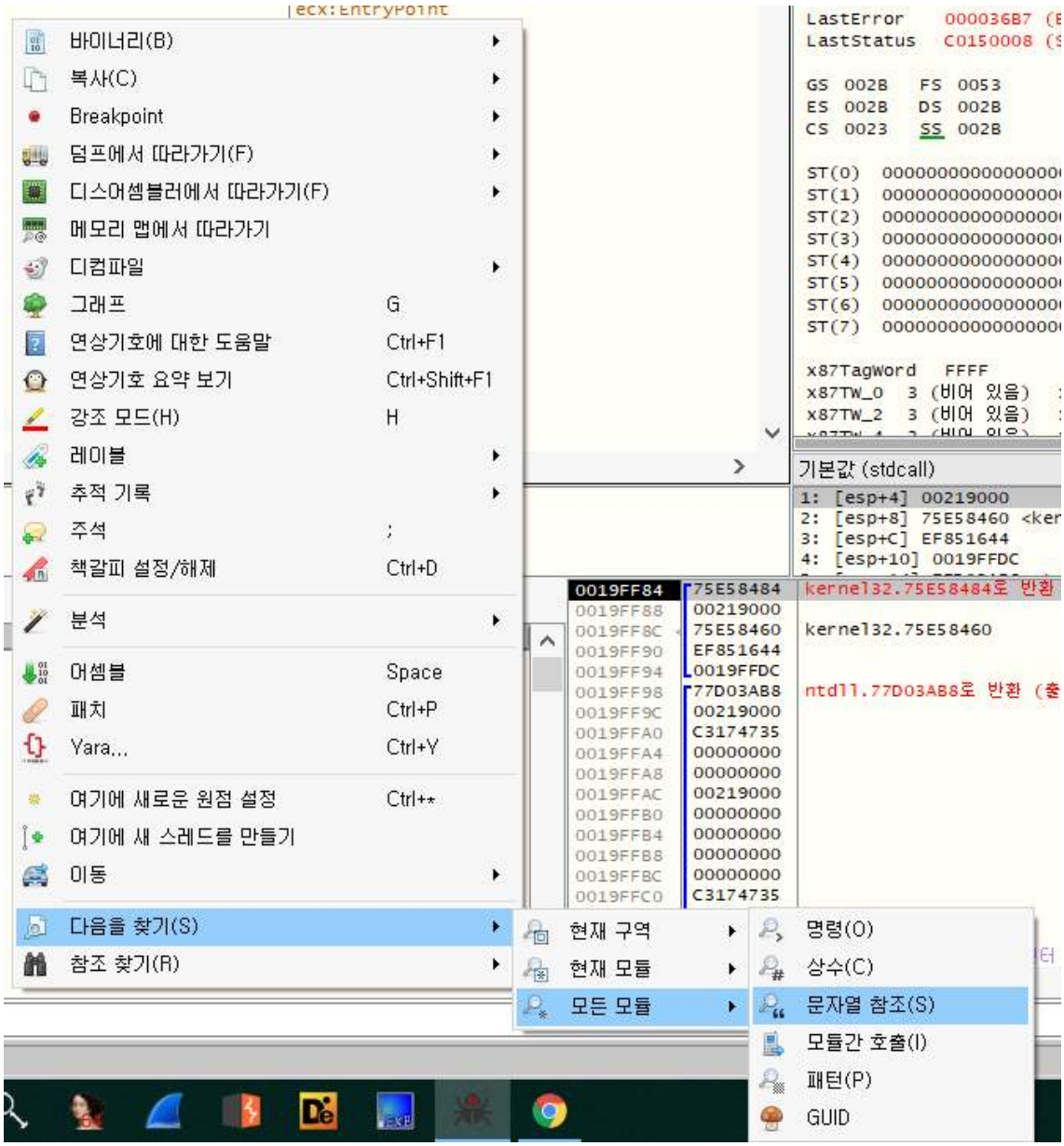
unpack된 06_dump_SCY.exe 파일을 볼수 있다.



이제 Sserial 코드를 찾기위해서
언팩된 실행파일을 실행시키면 정상적인 EP에 Breakpoint가 걸려있다.

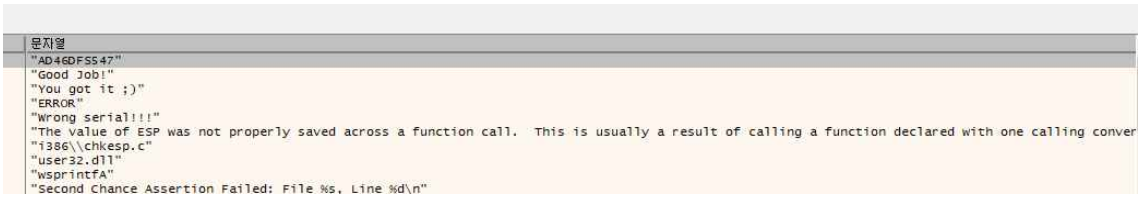
유형	주소	Module/Label/Exception	상태	디스어셈블리	Hits	Summary
소프트웨어	00401360	<06_dump_scy.exe.EntryPoint>	One-time	push ebp	0	진입점 중단점

먼저 문자열을 찾아준다.



d

이번에도 5번문제와같이 문자열에 시리얼 코드가 들어있다.



넣어주면

Clear