REPORT:

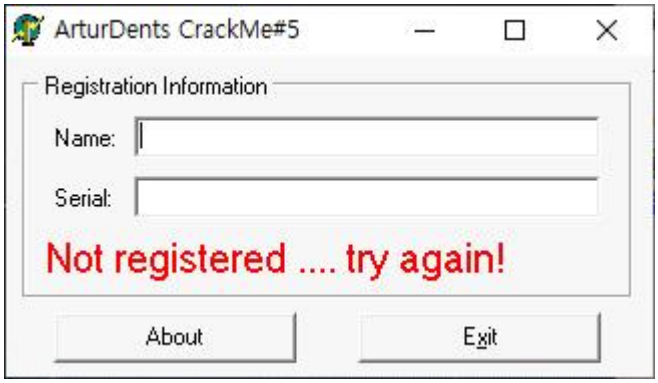
코드엔진 Basic RCE 10 Writeup

COLONY
1824275 정상지

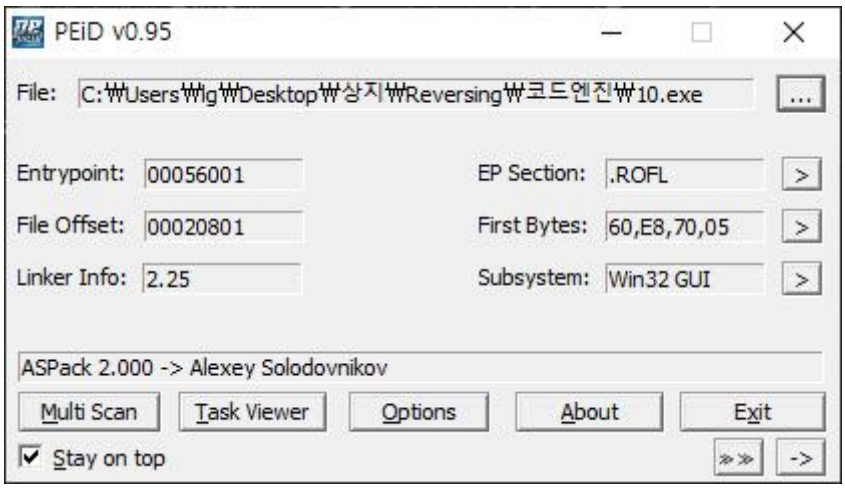
2021.05.30

OEP를 구한 후 '등록성공' 으로 가는 분기점의 OPCODE를 구하시오.

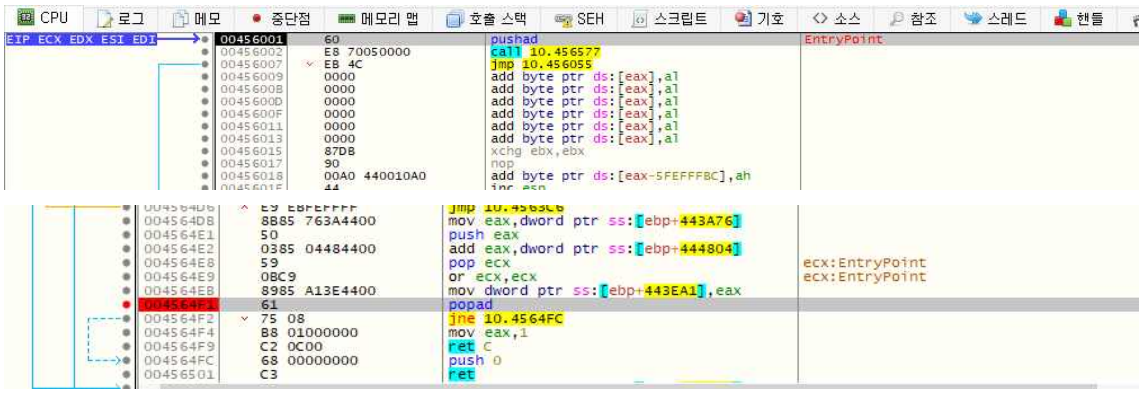
프로그램 실행



해당 프로그램은 ASpack으로 패킹되어있는 것을 확인할 수 있다

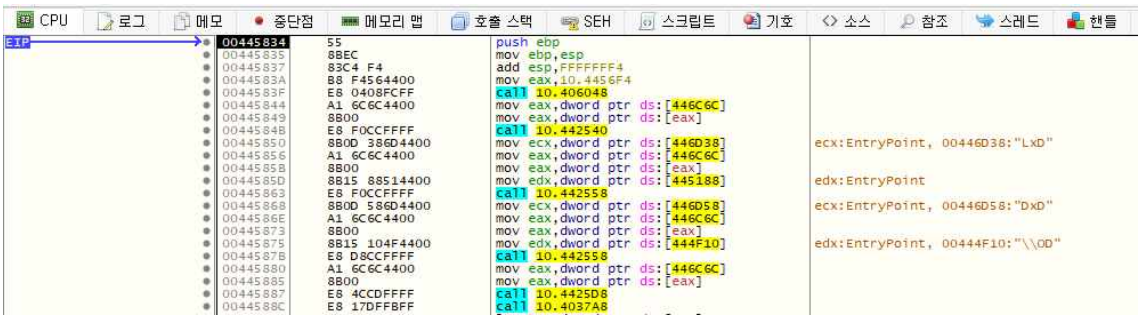


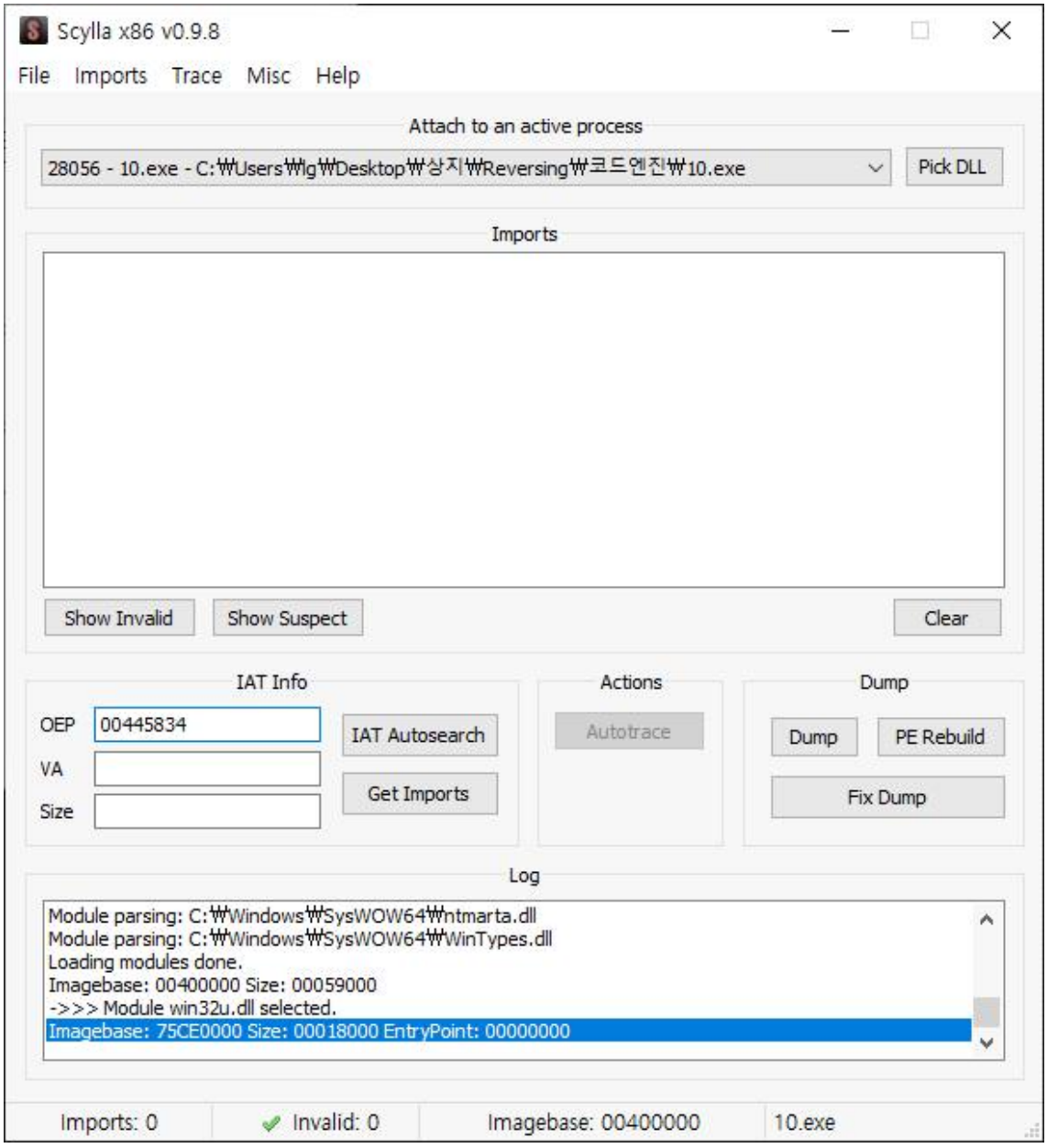
pushad에서부터 popad까지 패킹과정이므로



popad에서 breakpoint를 걸고 디버깅

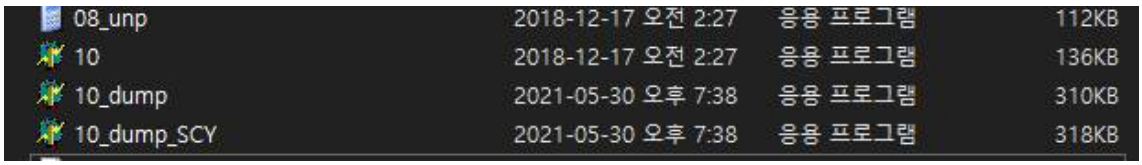
ret 호출 불러진 곳이 oep ->00445834



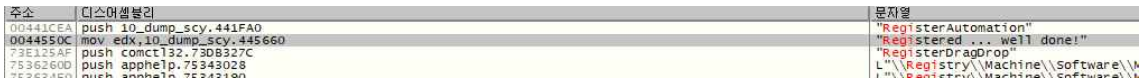


해당 파일을 Scylla 플러그인을 통해 IAT autosearch 및 get imports를 시키고 Dump를 만든 후에 fix dump로 저장한다

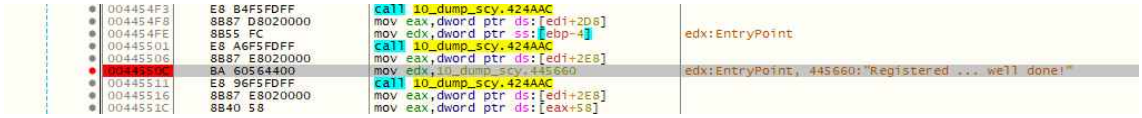
아래와 같이 10_dump_SCY라는 exe파일이 생성되었으며 해당 프로그램을 디버깅한다



성공했을 때의 메시지 주소가 0044550C이므로



해당 주소를 cpu에서 찾아간다



해당 break point 위에 분기문이 있는 것이므로 확인해본다

jne분기문을 통해서 확인할 수 있다

정답은 004458347755