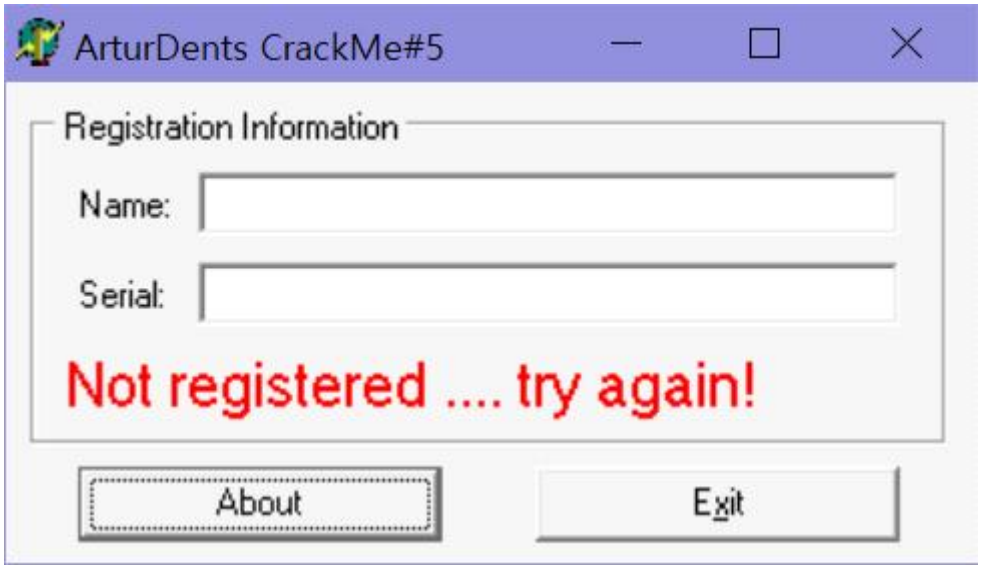
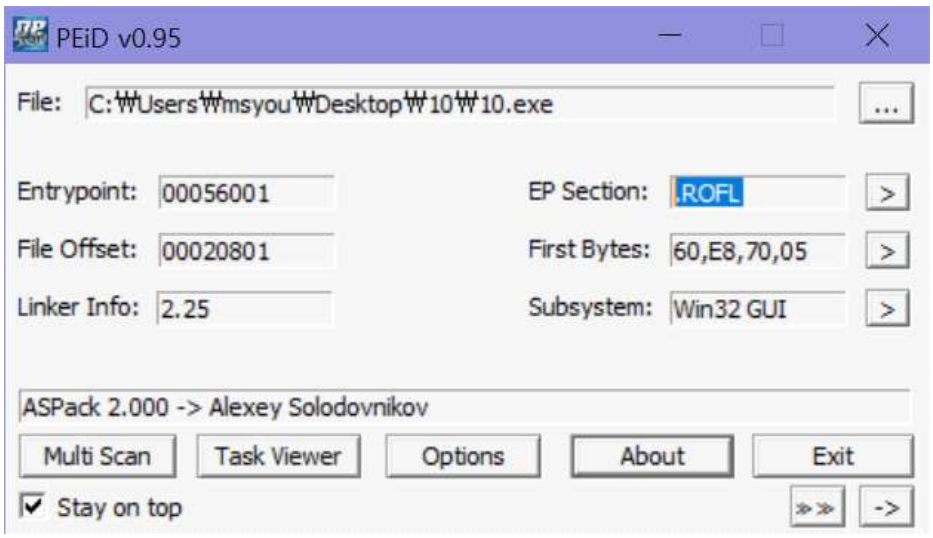
CodeEngn Basic RCE L10 Write up
:OEP를 구한 후 '등록성공' 으로 가는 분기점의 OPCODE를 구하시오.
정답인증은 OEP + OPCODE
EX) 00400000EB03



10.EXE 실행 시 위와 같이 뜬다!

문제에서는 등록성공으로 가는 OPCODE를 찾으라 했으므로 NAME과 SERIAL입력시 등록성공을 띄우게 하는 코드를 찾아야 하는 것 같다.

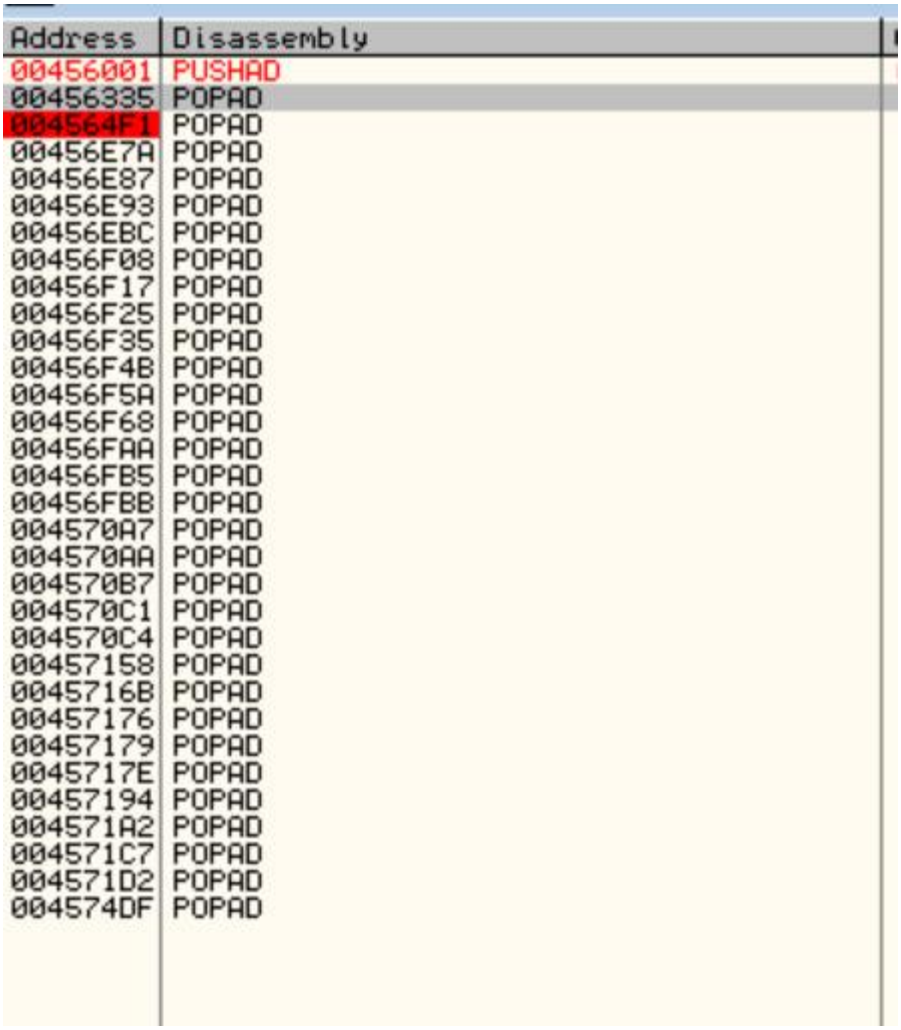
1. PEiD로 구조 분석하기



이번에도 OEP 코드를 구하라 하길래 PEiD로 조회 시 UPX로 패킹 되어있을 것이라고 생각했는데 ASPack으로 패킹되어 있는 것을 알 수 있다.

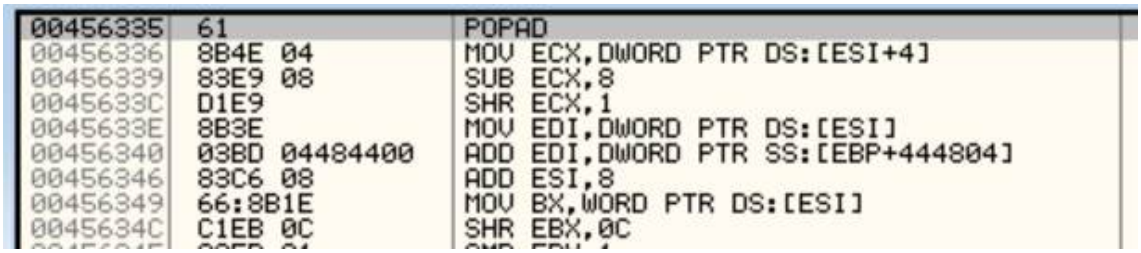
2. OLLYDBG로 분석하기

키고 실행 몇번 눌러누면 바로 PUSHAD가 보인다.

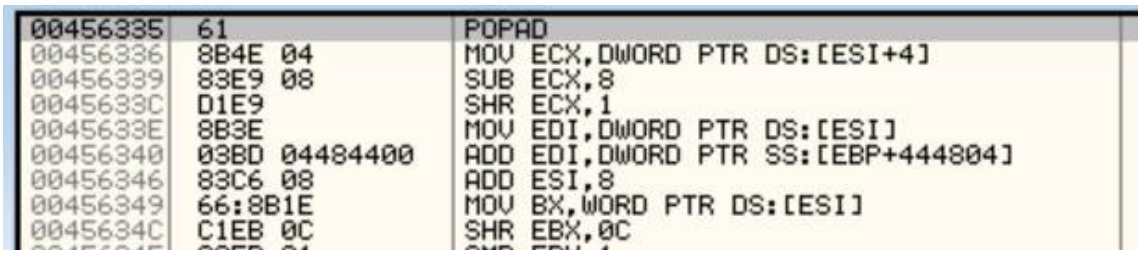


Address	Disassembly
00456001	PUSHAD
00456335	POPAD
004564F1	POPAD
00456E7A	POPAD
00456E87	POPAD
00456E93	POPAD
00456EBC	POPAD
00456F08	POPAD
00456F17	POPAD
00456F25	POPAD
00456F35	POPAD
00456F4B	POPAD
00456F5A	POPAD
00456F68	POPAD
00456FAA	POPAD
00456FB5	POPAD
00456FBB	POPAD
004570A7	POPAD
004570AA	POPAD
004570B7	POPAD
004570C1	POPAD
004570C4	POPAD
00457158	POPAD
0045716B	POPAD
00457176	POPAD
00457179	POPAD
0045717E	POPAD
00457194	POPAD
004571A2	POPAD
004571C7	POPAD
004571D2	POPAD
004574DF	POPAD

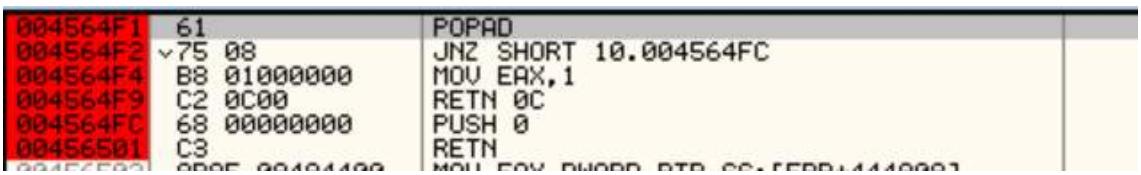
POPAD를 찾기 위해 이번에도 SEARCH FOR로 검색하였다.



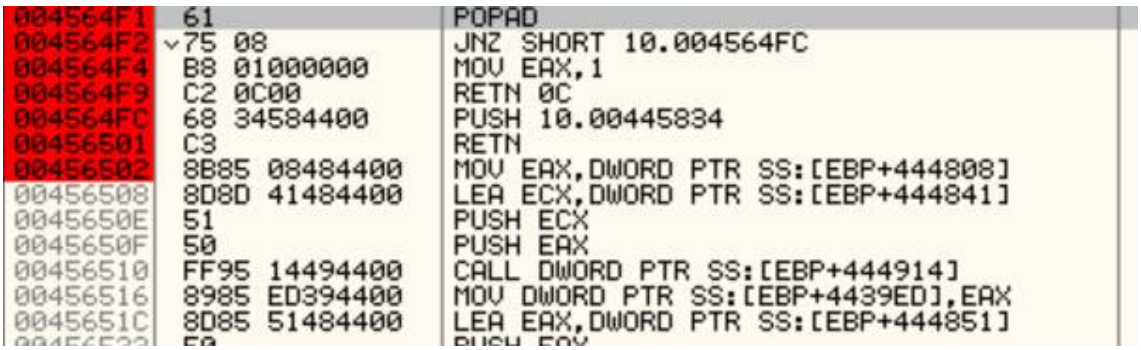
그랬더니 정말 많은 POPAD가 나온다. 일단 PUSHAD와 제일 가까운 것부터 살펴보기로 하고 00456335 주소의 POPAD를 더블클릭하였다.



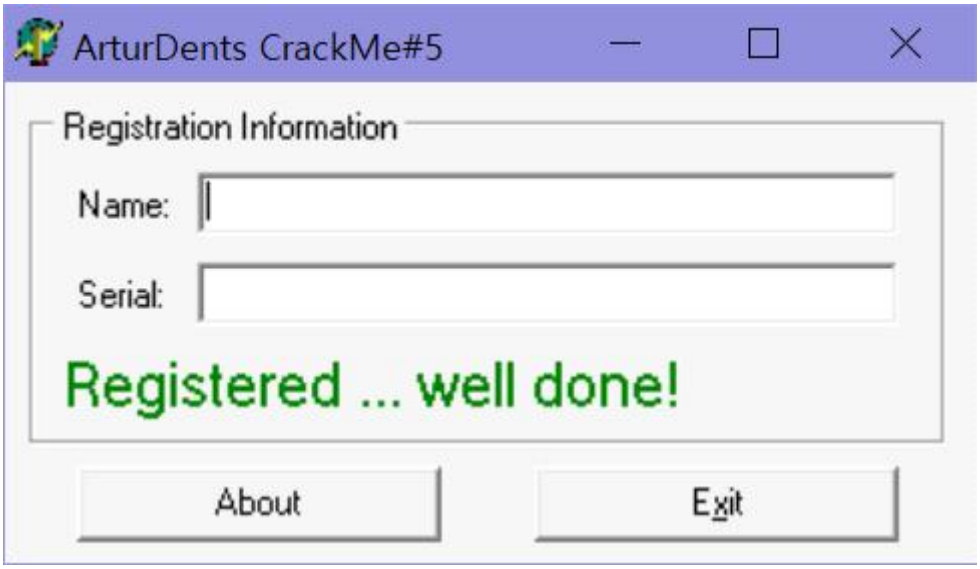
밑으로 이동시키는 명령어를 찾아보려 스크롤을 내렸는데 00456335 주소가 없어진다.
왜 이런건지는 모르겠지만 서치한 결과 이전 POPAD 검색 시 나왔던 목록에서 제외하고 살펴보라고 나와있어서, 두번째 POPAD 주소, 004564F1로 이동해 보았다.



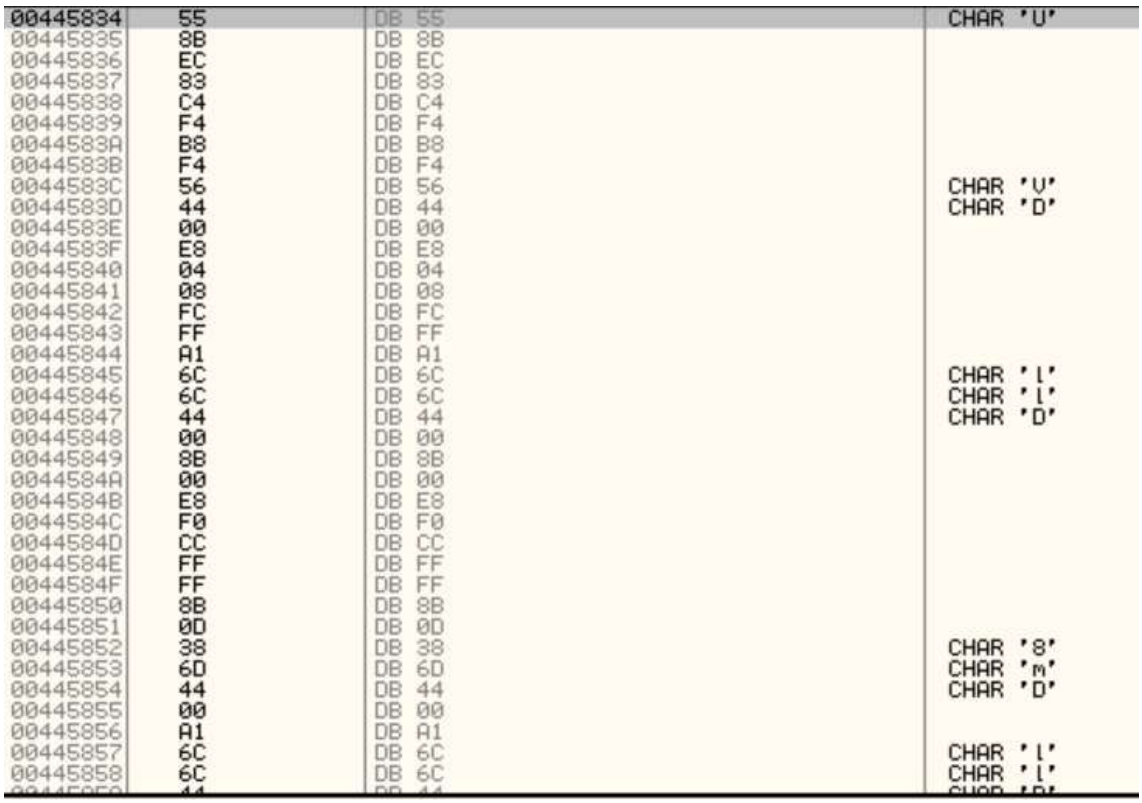
한줄씩 BP를 걸고 수행하면



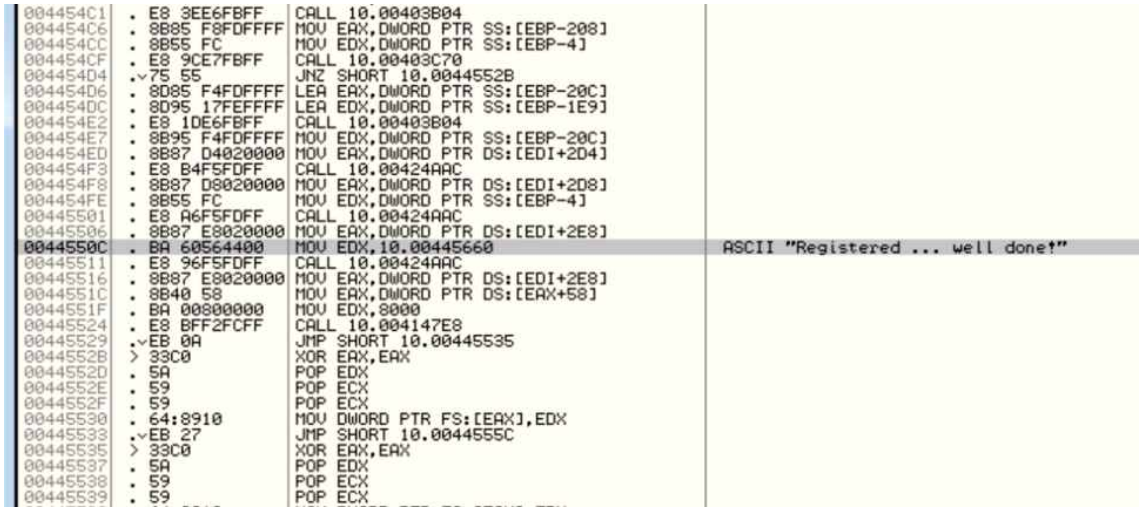
004564FC에서 PUSH되는 값이 00000000 -> 00445834로 바뀌고,
00456501 이후 프로그램이 실행되며, 아래와 같은 화면이 뜨게 되는 것을 알 수 있다.



프로그램이 실행되면서 등록 성공이라는 메시지가 뜬다.
즉 PUSH명령어에서 주소를 스택에 넣고 그것을 리턴하면 등록성공이라는 메세지가 나오기 때문에, OEP주소는 00445834라는 것을 알 수 있다.



해당 OEP 주소로 들어가보면 아직 OEP인것을 인식하지 못한다고 한다. CTRL+A를 누르면 제대로 인식한다.



CTRL+A 를 누르고, SEARCH FOR -> STRING 찾기로 EXE파일의 "Registered ... well done!"을 찾을 수 있다. 문제에서 구하라고 했던 opcode는 주소와 어셈블리어 사이에 있는 기계어코드를 말하는데, 등록성공으로 가는 분기문의 OPCODE는 위쪽의 꺽새가 있는 75 55 를 말한다.

답은 0044583475555이다.