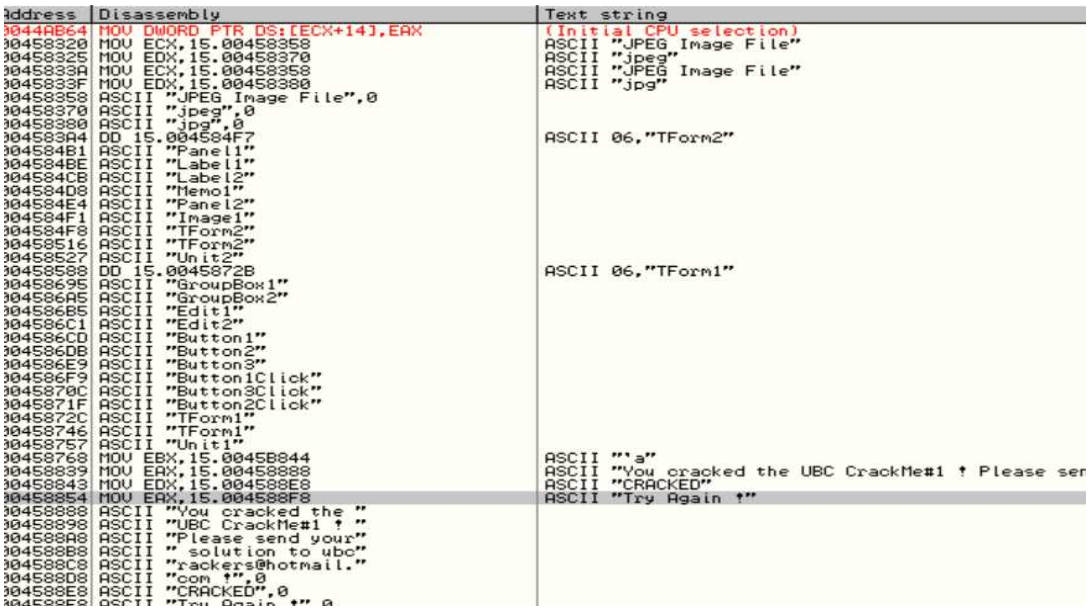
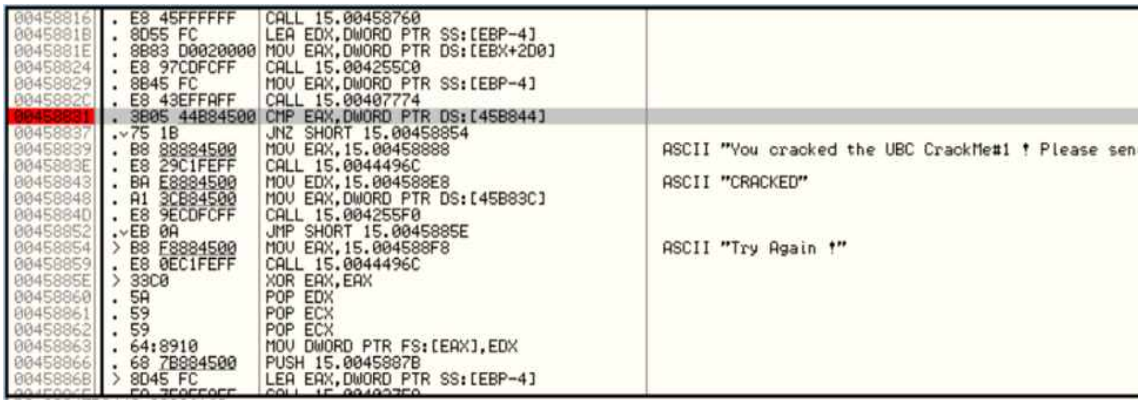
CodeEngn Basic RCE L15
: Name이 CodeEngn일때 Serial을 구하시오

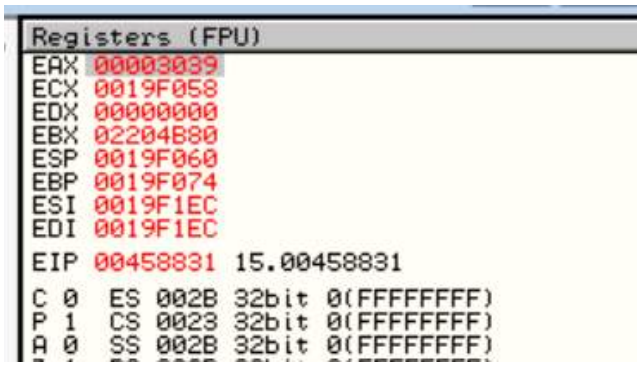
CodeEngn일 때의 시리얼 넘버를 찾는 것이기 때문에 시리얼 넘버에 아무거나 넣어주었고, Try again!이라는 에러메세지가 떴다. 올리디버거로 열어주었더니 따로 패킹이 되어 있지는 않아서, 오류 메세지를 찾기 위해 all text string을 찾아주었다.



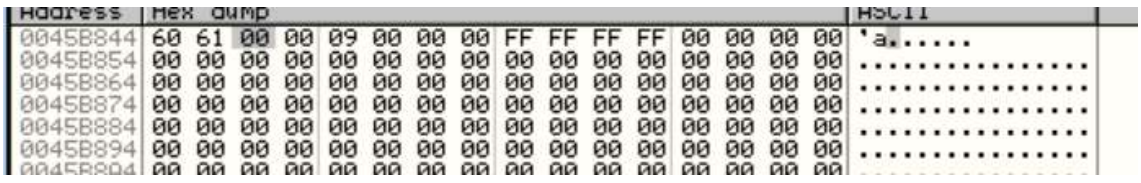
you cracked the UBC ~~~ 는 성공메세지로 추측된다. 해당 주소로 이동한다.



성공메세지 위쪽을 보면
CMP EAX, PTR ~~
JNZ 00458854가 나오는데, 14번 문제와 마찬가지로 EAX와 PTR ~~~를 비교해서 0이 아니라면 00458854로 이동해서 TRY AGAIN이라는 에러 메시지를 출력한다.
즉 EAX와 PTR ~~~~의 값이 같아야 한다. 따라서 CMP에 BP를 걸고 다시 실행해 주었다.
** DWORD PTR DS:[45B844] **
45B844 주소의 데이터 영역의 값->해당 줄 선택하여 FOLLOW IN DUMP를 수행해주어야함.



EAX의 값을 10진수로 바꾸어주면 12345이고, EAX 레지스터가 사용자의 입력값을 저장한다는 것을 알 수 있다. 그럼 앞서 말한것처럼 덤프따라가기로 밑 헥스 데이터를 확인해 보았다.



DWORD PTR DS:[45B844]는 45B844부터 4바이트 만큼의 값이기 때문에 00006160이다. (리틀 엔디안이라서 반대로 보아야함) 마찬가지로 10진수로 바꾸어 주면 24928이고, 이를 대입해보면


CrackMe#1 [UBC] by bRaINbuSY
You cracked the UBC CrackMe#1 ! Please send your solution to ubcrackers@hotmail.com !
OK

정답이다!!