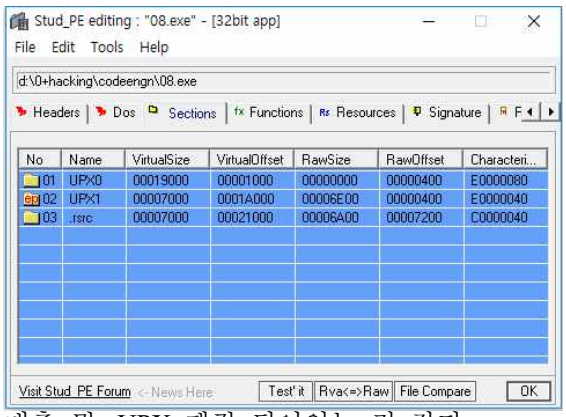
문제 : Basic RCE L08　　OEP를 구하시오 Ex) 00400000

8번 프로그램을 실행시켜보면...

그냥 계산기 프로그램이다.

StudPE로 보자.

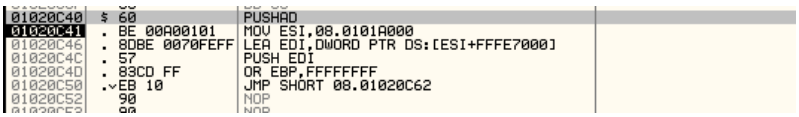


대충 뭐...UPX 패킹 되어있는 것 같다.

[UPX 패킹] -> OEP가 바로 나오지 않는 것이 특징.

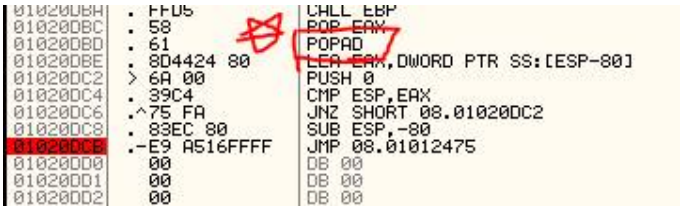
1. PUSHAD
2. 반복문을 통한 패킹과정 진행
3. POPAD
4. JMP OEP
5. 끝.

그러니까 우리는 PUSHAD, POPAD 위치만 찾으면 된다. 그 중간에 Packing 과정은 볼 필요 없음.



PUSHAD 찾음.

여기서 스크롤다운해서 좀만 내려보자...



좀만 내리니 나왔다.
그럼 POPAD 다음에 JMP OEP 니까...
8번 문제는 OEP 주소 찾는 것이 문제.

즉 정답은 아마도 01012475 일 것이다.

과연?

정답!