**운영체제 – 숙제 5, 힙 영역에 코드 넣기**

**2013210111 남세현**

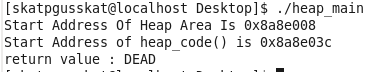
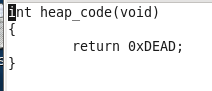
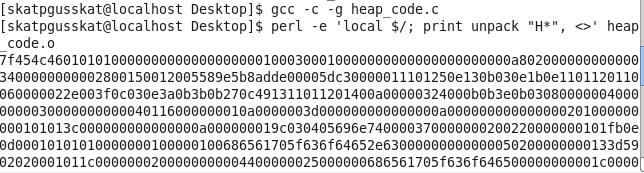


Figure - 실행 결과

숙제의 재미를 더하기 위해서, 7777의 값을 return하지 않고, 0xDEAD 값을 return하도록 하였습니다.

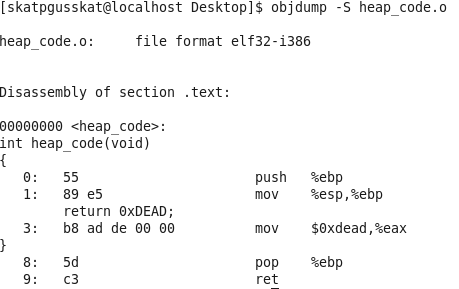


위 코드를 heap\_code.c에 작성하고, gcc로 오브젝트 파일로 컴파일 하면 아래와 같은 heap\_code.o 파일이 나옵니다.



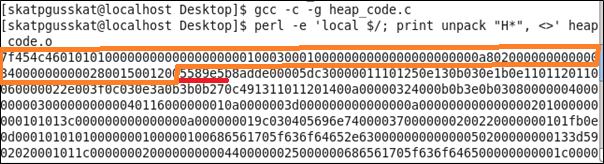
오브젝트 파일은 바이너리 데이터인데, 함수의 시작을 바로 알 수 없습니다.

그러므로 Objdump를 이용해서 역어셈블링을 하면



위 결과창에 나온 것 처럼, 처음 함수의 instruction들이 55, 89, e5로 시작됨을 알 수 있습니다.

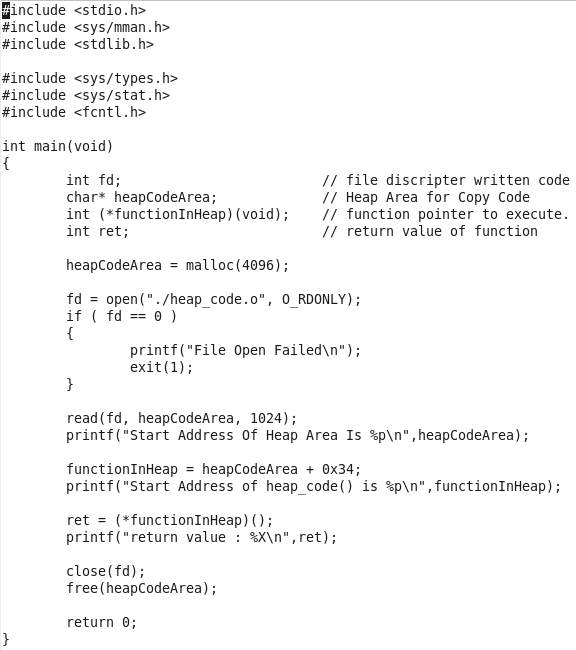
저 바이너리 데이터에서 55, 89, e5가 나오는 시점을 확인한 후, 거기까지의 offset을 확인합니다.



빨강색을 줄 쳐진 곳에 55, 89, e5가 확인됩니다. 그 앞으로 기타 데이터가 총 52Byte가 있었습니다.

그러므로, 최종적으로 실행한 코드 Heap\_main.c 에서는

1. Heap\_code.o를 읽어서 힙 영역에 복사해놓고
2. 함수포인터를 그 힙 영역의 첫 부분 + offset(52Byte) 를 가리키도록 셋팅한 후 함수포인터로 함수를 실행



숙제를 하면서 어려웠던 점은 없었습니다.