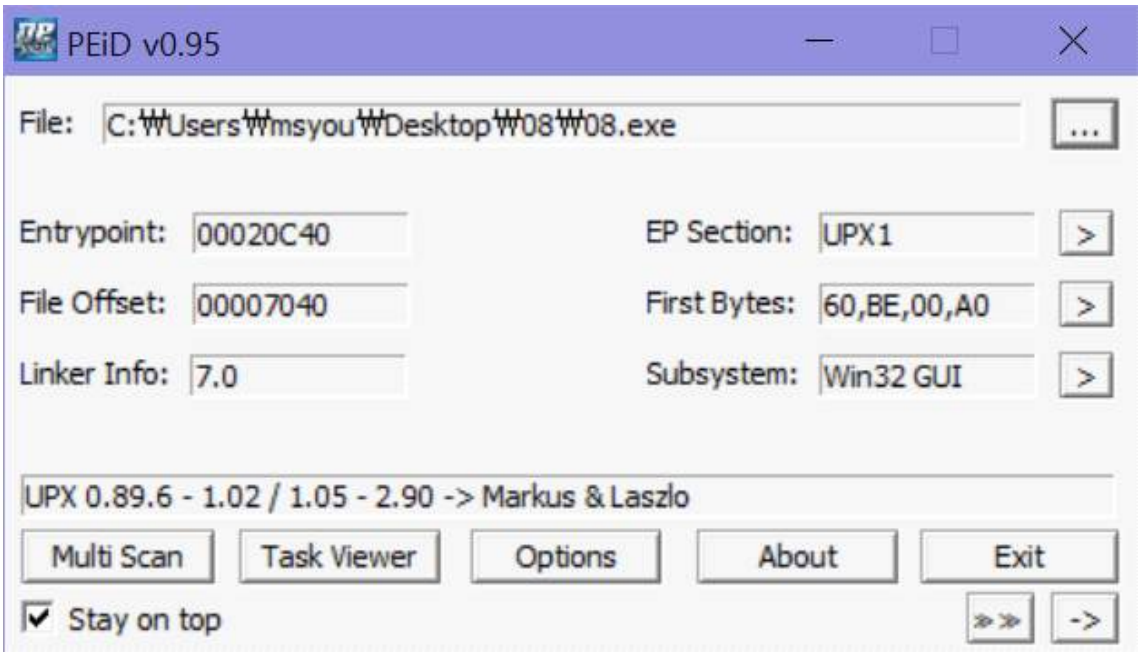
CodeEngn Basic RCE L08 Write up
: OEP를 구하시오 Ex) 00400000

이번 8번 문제는 OEP를 구하는 문제이다.
아직 EXE를 열어보지는 않았지만 OEP를 구하라는 걸로 보아 UPX로 패킹되어 있다고 짐작해 볼 수 있다.

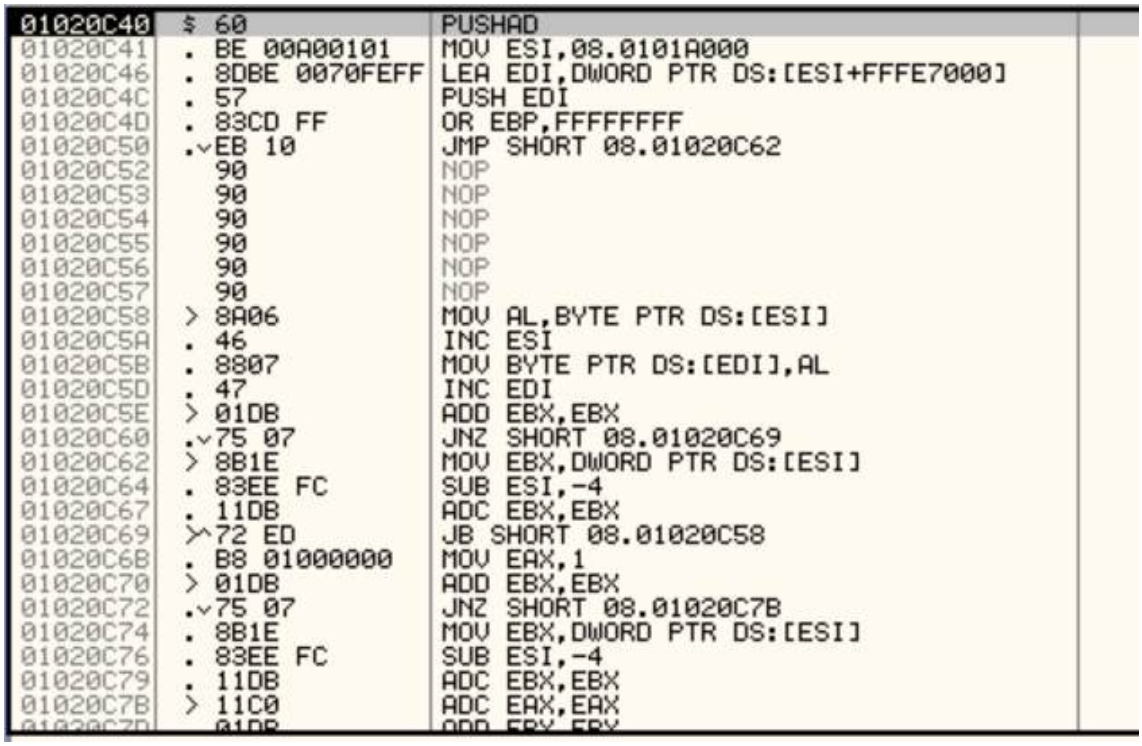
1. PEiD를 통해 UPX로 패킹되어 있는지 확인



EP SECTION에 보면 UPX1로 패킹되어있다는 것을 알 수 있다.

우선 이전 L05,06,07을 풀어본 결과 UPX로 패킹되어 있는 것은 PUSHAD -> POPAD를 찾고, POPAD 주변의 명령어를 보다보면 OEP 주소로 이동하라는 명령이 존재한다. 따라서 올리디버거에 올려서 이를 찾아보도록 하겠다.

2. OLLYDBG에 올려보기

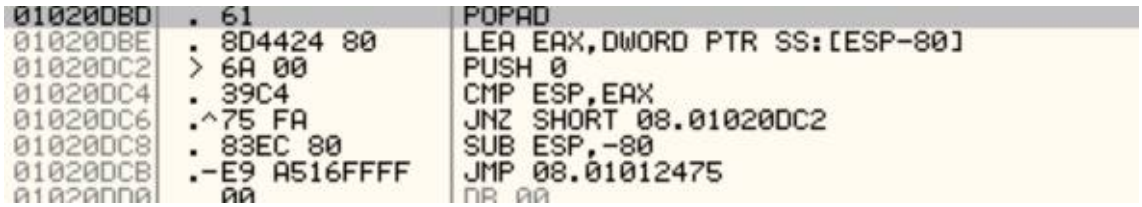


```
01020C40  $ 60            PUSHAD
01020C41  . BE 00A00101   MOV ESI,08.0101A000
01020C46  . 8DBE 0070FEFF LEA EDI,DWORD PTR DS:[ESI+FFFE7000]
01020C4C  . 57            PUSH EDI
01020C4D  . 83CD FF       OR EBP,FFFFFFFF
01020C50  .v EB 10        JMP SHORT 08.01020C62
01020C52    90            NOP
01020C53    90            NOP
01020C54    90            NOP
01020C55    90            NOP
01020C56    90            NOP
01020C57    90            NOP
01020C58  > 8A06          MOV AL,BYTE PTR DS:[ESI]
01020C5A  . 46            INC ESI
01020C5B  . 8807          MOV BYTE PTR DS:[EDI],AL
01020C5D  . 47            INC EDI
01020C5E  > 01DB          ADD EBX,EBX
01020C60  .v 75 07        JNZ SHORT 08.01020C69
01020C62  > 8B1E          MOV EBX,DWORD PTR DS:[ESI]
01020C64  . 83EE FC       SUB ESI,-4
01020C67  . 11DB          ADC EBX,EBX
01020C69  >^72 ED         JB SHORT 08.01020C58
01020C6B  . B8 01000000   MOV EAX,1
01020C70  > 01DB          ADD EBX,EBX
01020C72  .v 75 07        JNZ SHORT 08.01020C7B
01020C74  . 8B1E          MOV EBX,DWORD PTR DS:[ESI]
01020C76  . 83EE FC       SUB ESI,-4
01020C79  . 11DB          ADC EBX,EBX
01020C7B  > 11C0          ADC EAX,EAX
```

올리디버거에서 실행을 시키니 PUSHAD가 바로 보인다.

Address	Disassembly	Comment
0101D4DC	POPAD	
0102047E	POPAD	
010205B9	POPAD	
01020C40	PUSHAD	(Initial CPU selection)
01020DBD	POPAD	

마우스 오른쪽 클릭 - SEARCH FOR - ALL COMMANDS를 통해 POPAD를 검색하면, PUSHAD 아래에 있는 POPAD를 볼 수 있고, 이를 더블클릭하면 다음과 같은 어셈블리어들이 나온다.



```
01020DBD  . 61            POPAD
01020DBE  . 8D4424 80     LEA EAX,DWORD PTR SS:[ESP-80]
01020DC2  > 6A 00         PUSH 0
01020DC4  . 39C4          CMP ESP,EAX
01020DC6  .^75 FA         JNZ SHORT 08.01020DC2
01020DC8  . 83EC 80       SUB ESP,-80
01020DCB  .-E9 A516FFFF   JMP 08.01012475
```

01020DBE LEA EAX,DWORD PTR SS:[ESR-80] : EAX에 ESR-80의 주소값을 저장한다.

01020DC2 PUSH 0 : 0을 스택에 PUSH한다.

01020DC4 CMP ESP,EAX : ESP와 EAX를 비교한다.

01020DC6 JNZ SHORT 08.01020DC2 : ESP와 EAX가 같지 않으면 01020DC2로 이동한다.
* 같으면 밑의 명령어를 실행

01020DC8 SUB ESP,-80 : ESP-(-80) = ESP+80

01020DCB JMP 08.01012475 : 01012475로 이동한다.

이때 UPX 문제를 풀다가 공통점을 발견했는데 OEP 주소로 가기전 루프(LOOP)를 돈다는 것이다. 위에서도 01020DC6에서 같지 않으면 01020DC2로 이동하는데 해당 주소를 바로 위에, 위에 있는 PUSH 0이라는 것을 알 수 있다. 따라서 01020DC6인 OEP로 가는 주소가 아니라는 것을 추측할 수 있다.

그 밑에 있는 JMP가 OEP로 가게 하는 명령어이고, OEP의 주소는 01012475라는 것을 알 수 있다.