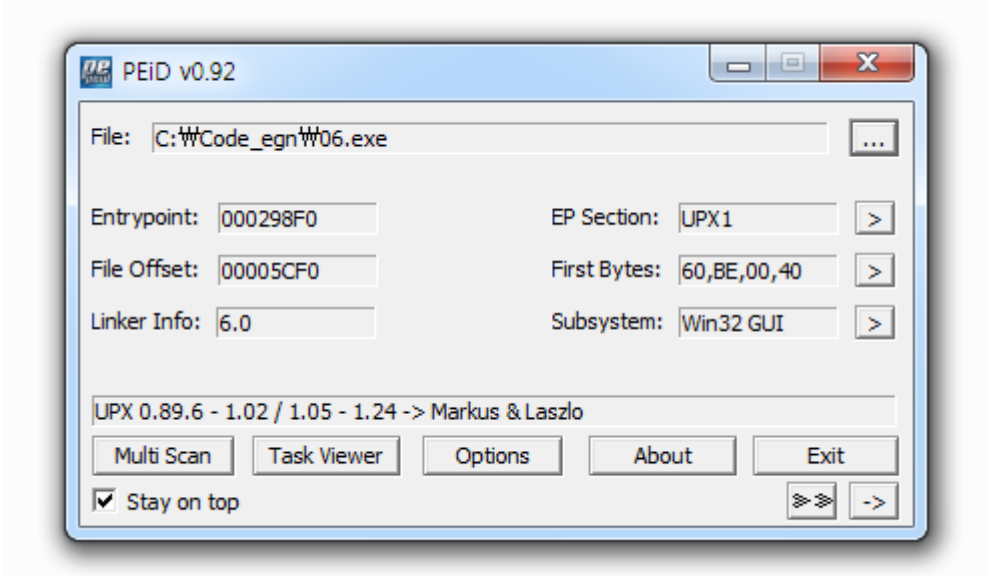
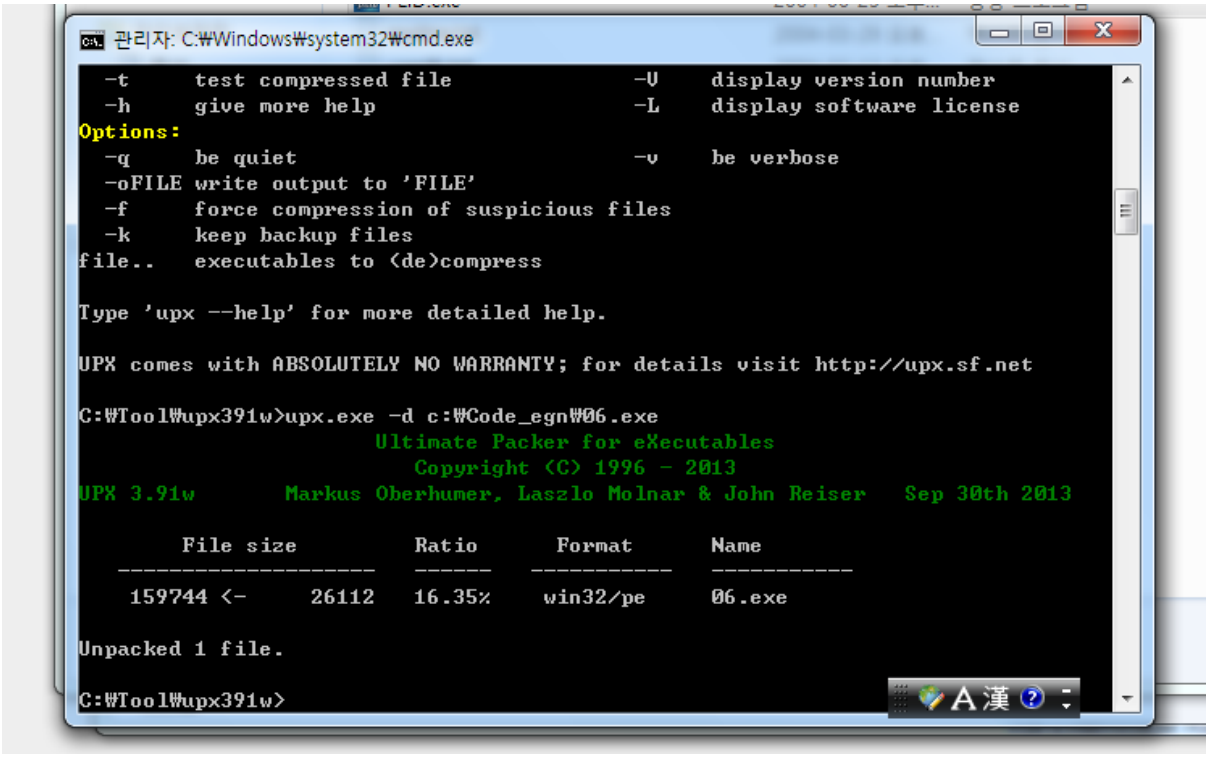
2013

Code Engn Basic 6

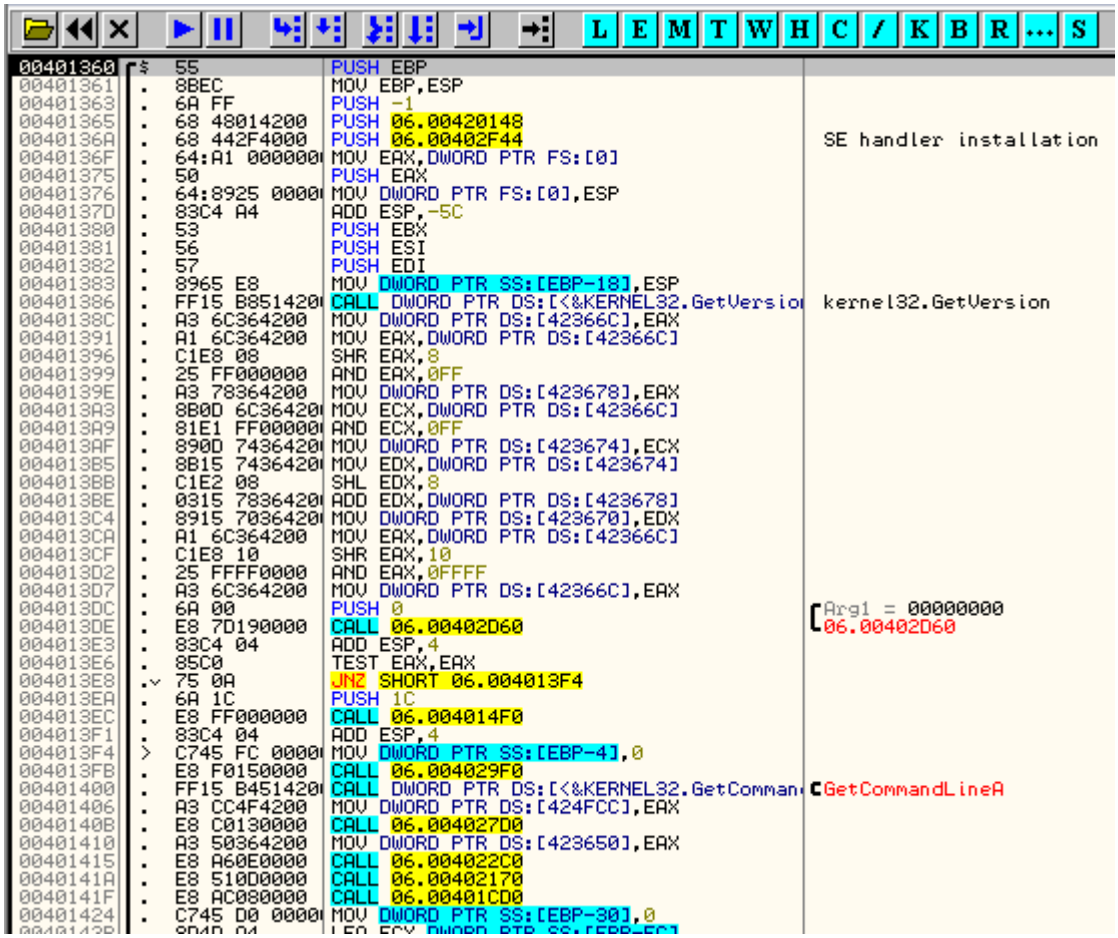
4.Z320



PEiD로 확인 시 UPX 패킹이 되어 있는것을 확인할 수 있습니다.



UPX를 이용, 디컴프레스 합니다.

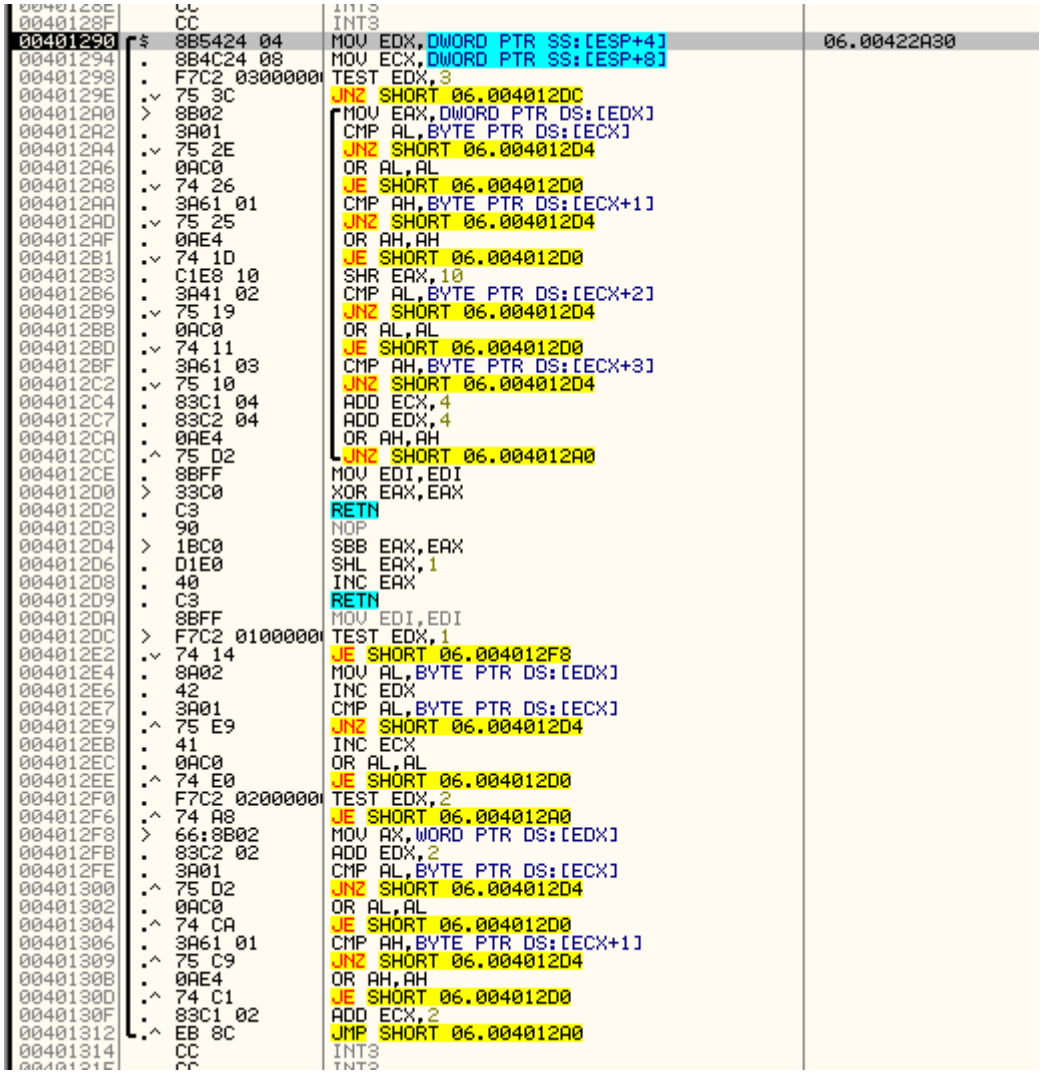


여기서 OEP가 00401360임을 확인할 수 있습니다.

문자열을 입력받은 후 메세지 박스를 출력하는 함수가 보입니다.

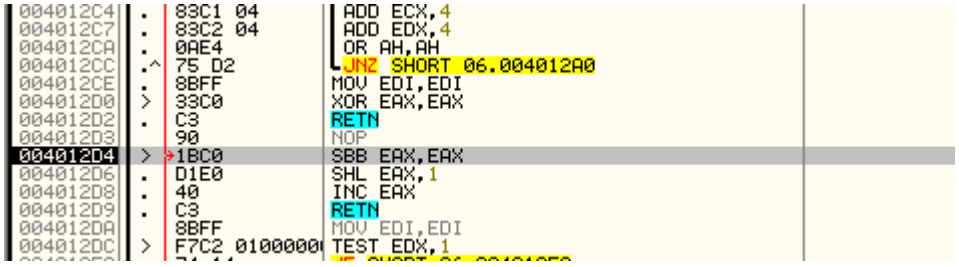
그리고 무언가 정해진 ASCII값과 사용자가 입력한 ASCII값을 PUSH 후 함수를 호출함을 볼 수 있습니다.

그리고 아래에는 Good Job이라는 제목과 ERROR이라는 제목을 가진 메세지 박스가 나오는것으로 보아 TEST명령의 결과에 따라 성공과 실패가 나눠지는것을 확인할 수 있습니다.



EDX에 프로그램 내에 있던 값을, ECX에는 사용자가 입력한 값을 넣은 뒤 루프문 안으로 들어갑니다.

EAX에 문자열 4byte를 넣은 뒤 사용자가 입력한 값 한글자 한글자와 서로 비교를 하기 시작합니다. 그리고 비교하여 값이 다를 경우에는 004012D4로 점프, EAX값을 1로 만든 뒤에 리턴 함을 확인할 수 있습니다. 이때 위에서 TEST EAX EAX의 결과값에 따라 메세지박스의 내용이 달라짐으로 보아 004012D4는 실패의 메세지를 띄우게 하기 위한 주소값임을 알 수 있습니다.

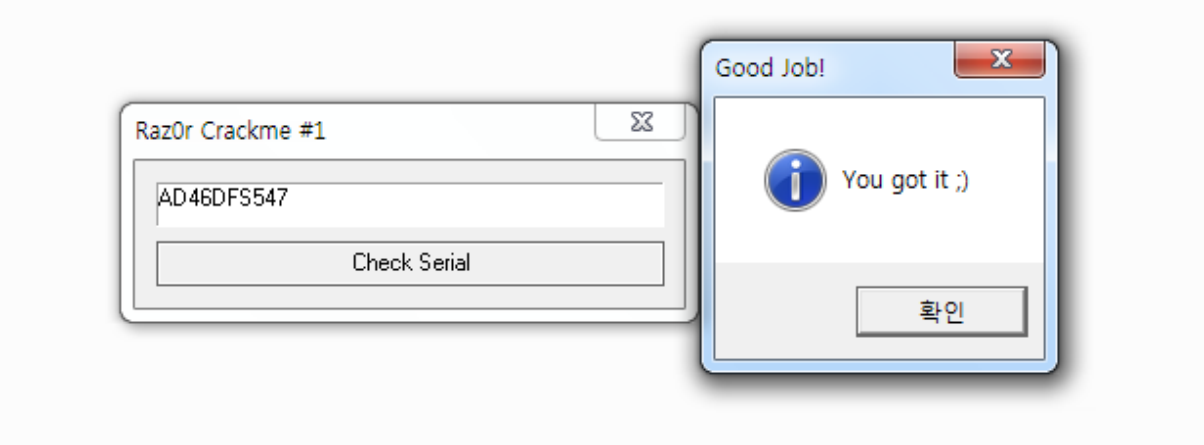


비교를 계속하다 널 문자열을 만나게 되면 OR AL(AH) AL(AH) 구문에서 ZF가 설정되므로 004012D0로 빠져나오게 되며 EAX값이 0으로 셋팅된 채로 RETN하게 됩니다.

```
00401069  .  68 D4354200  PUSH 06.004235D4                  ASCII "AAAAAAAAAA"
0040106E  .  68 302A4200  PUSH 06.00422A30                  ASCII "AD46DFS547"
00401073  .  E8 18020000  CALL 06.00401290
00401078  .  83C4 08      ADD ESP,8
0040107B  .  85C0         TEST EAX,EAX
0040107D  .v 75 24        JNZ SHORT 06.004010A3
0040107F  .  8BF4         MOV ESI,ESP
00401081  .  6A 40        PUSH 40                          Style = MB_OK|MB_ICONASTERISK|MB_APPLMODAL
00401083  .  68 48004200  PUSH 06.00420048                 Title = "Good Job!"
00401088  .  68 38004200  PUSH 06.00420038                 Text = "You got it ;)"
0040108D  .  8B0D 3836420 MOV ECX,DWORD PTR DS:[423638]
00401093  .  51           PUSH ECX                         hOwner => 00060638 ('Raz0r Crackme #1',class='#32770')
00401094  .  FF15 B452420 CALL DWORD PTR DS:[<&USER32.Mes MessageBoxA
0040109A  .  3BF4         CMP ESI,ESP
0040109C  .  E8 7F020000  CALL 06.00401320
004010A1  .v EB 22        JMP SHORT 06.004010C5
```

그리고 TEST문에서 ZF가 설정되지 않으므로 Good Job 부분으로 갈 수가 있게 됩니다.

즉 프로그램 내에 있는 문자열 값이 키값이라 볼 수 있는 것입니다.



그리고 이를 입력하게 되면 맞는 답임을 알리는 메세지 박스가 나오는 것을 확인할 수 있습니다.

따라서 6번 문제의 답은 OEP인 00401360과 키 값인 AD46DFS547를 합한 00401360AD46DFS547가 되게 됩니다.