2013

Code Engn Basic 10

4.Z320

elttzero@gmail.com

Challenges : Basic 10

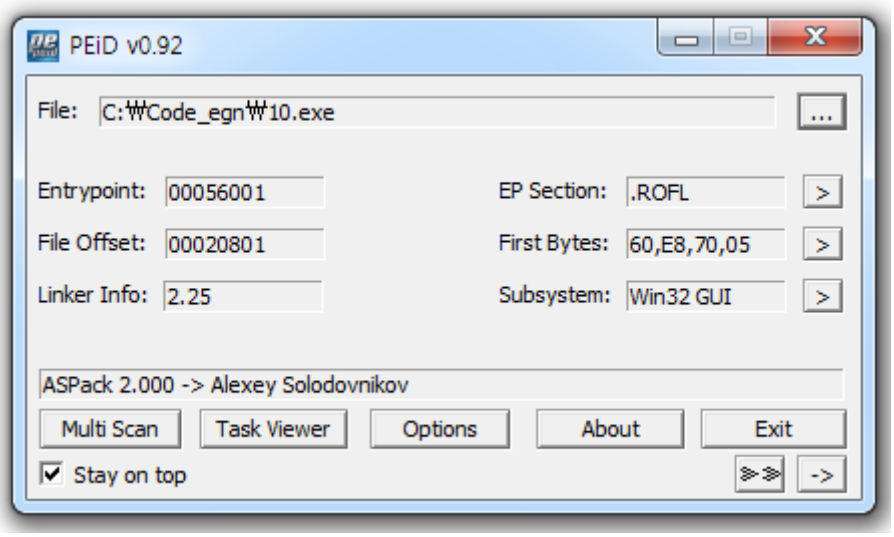
Author : ArturDents

Korea :
OEP를 구한 후 "등록성공"으로 가는 분기점의 OPCODE를 구하시오. 정답인증은 OEP + OPCODE
EX) 00400000EB03

English :
After finding the OEP, find the OPCODE of the branch instruction going to the "goodboy routine"
The solution should be in this format : OEP + Serial
EX) 00400000EB03

Download

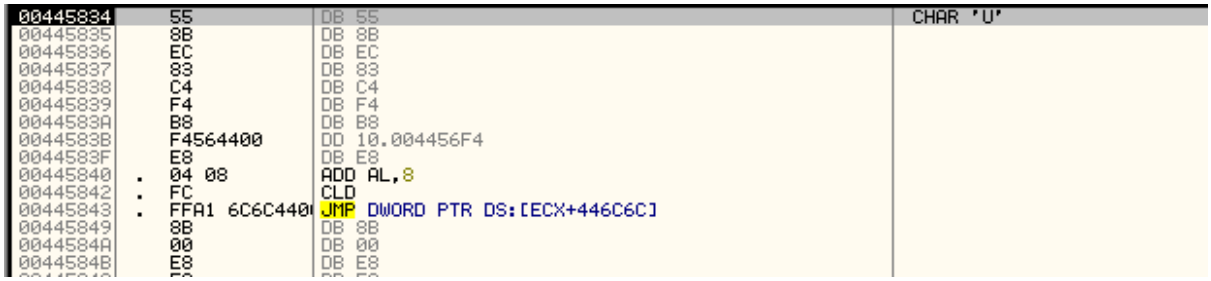
OEP 및 등록성공 으로 가는 분기점을 구하는 문제입니다.



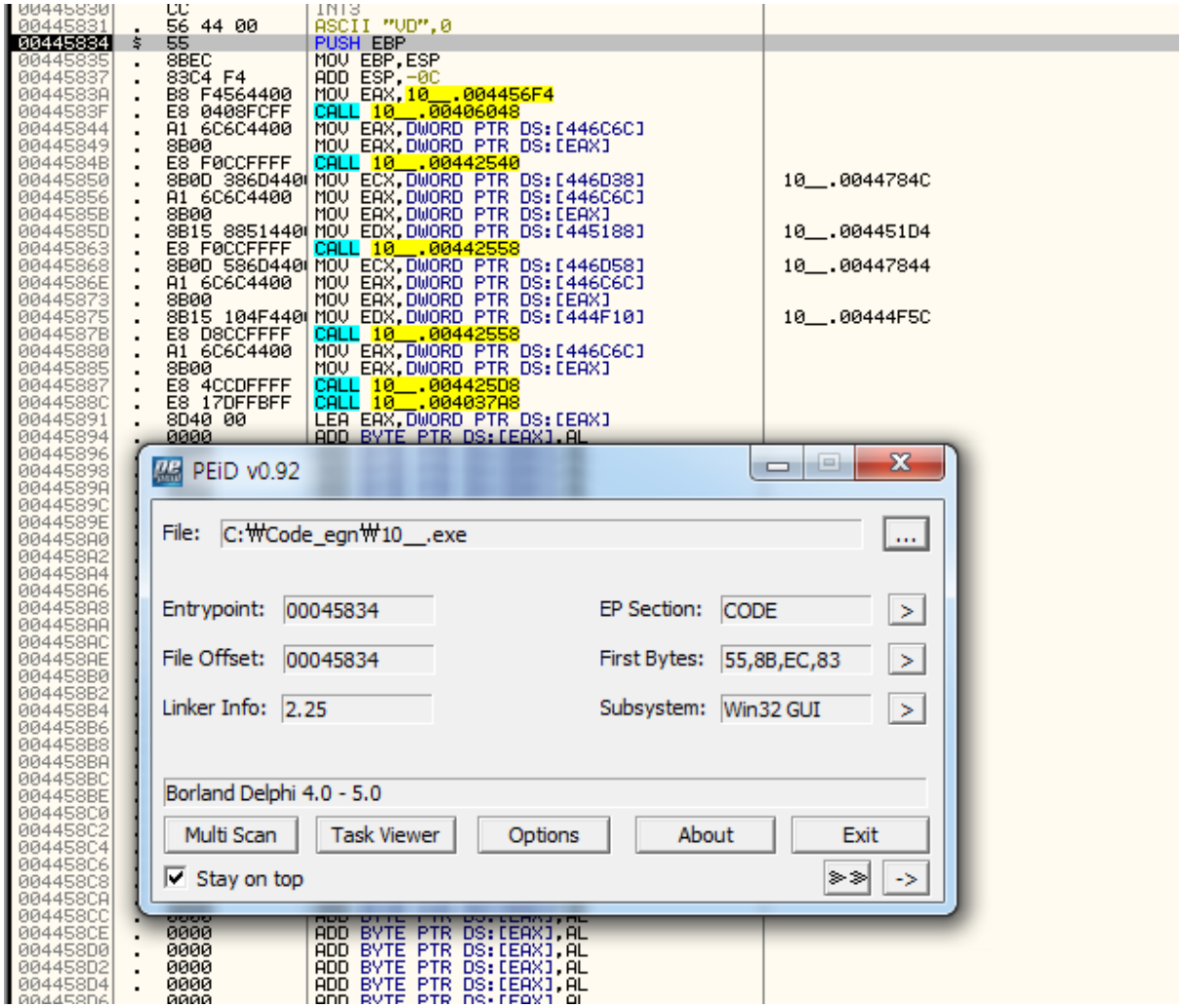
PEiD 로 확인해 보니 ASPack 이 되어 있음을 확인할 수 있습니다.

```
004564E2   0385 04484400   ADD EAX,DWORD PTR SS:[EBP+444804]
004564E8   59              POP ECX
004564E9   0BC9            OR ECX,ECX
004564EB   8985 A13E4400   MOV DWORD PTR SS:[EBP+443EA1],EAX
004564F1   61              POPAD
004564F2 v 75 08           JNZ SHORT 10.004564FC
004564F4   B8 01000000     MOV EAX,1
004564F9   C2 0C00         RETN 0C
004564FC   68 00000000     PUSH 0
00456501   C3              RETN
00456502   8B85 08484400   MOV EAX,DWORD PTR SS:[EBP+444808]
00456508   8D8D 41484400   LEA ECX,DWORD PTR SS:[EBP+444841]
0045650E   51              PUSH ECX
0045650F   50              PUSH EAX
00456510   FF95 14494400   CALL DWORD PTR SS:[EBP+444914]
```

프로그램의 언패킹이 끝나고 돌아가는 부분을 찾아서 안으로 들어가면 OEP 를 찾을 수 있습니다.

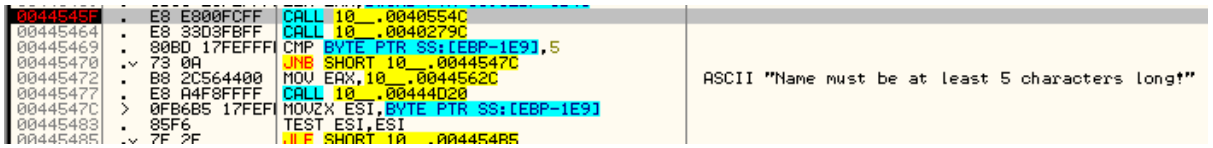


찾아낸 OEP 에서 OllyDbg 의 플러그인을 이용하여 수동 Dump 하여 Unpack 합니다.

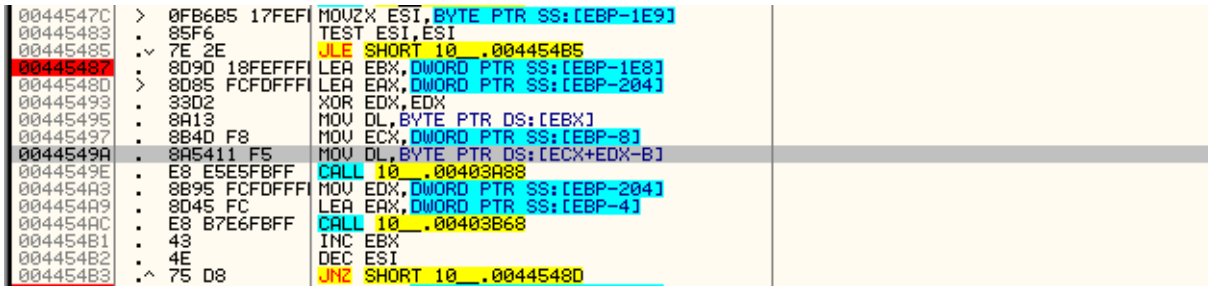


제대로 실행이 되는것으로 OEP 를 잘 찾아 Unpack 하였음을 알 수 있습니다.

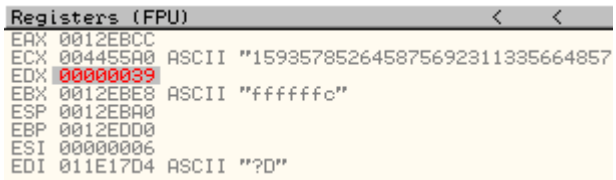
이 프로그램은 cm5.dat 파일을 불러와서 시리얼을 비교함을 알 수 있습니다만



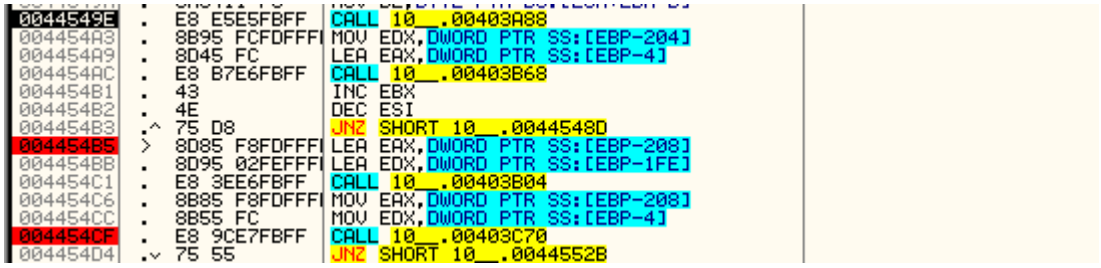
안의 파일의 첫번째 문장의 글자수가 5 글자 이하이면 에러메세지를 띄우게 되어 있습니다.



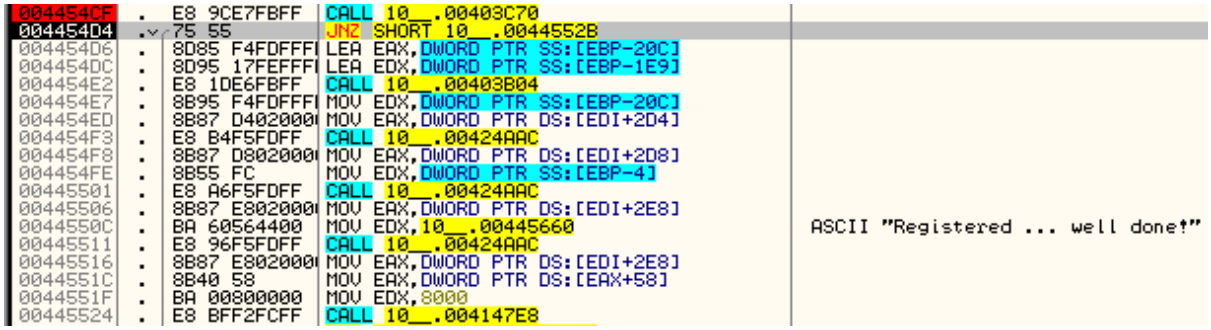
이후 글자의 길이를 ESI 에 넣은 뒤 루프의 카운터로 쓰게 되고 ECX 에 기본적으로 들어있던 숫자열의 주소를, EDX 에는 읽어들인 NAME 의 첫번째 글자를 읽어오게 됩니다.



이후 ECX 의 문자열 중에서 첫번째 글자의 ASCII Code 값 - B 만큼 이동한 곳의 숫자를 읽어온 뒤 EDX 레지스터에 저장하게 됩니다. 그리고 이것이 시리얼 값이 됩니다.



그후 만들어진 시리얼 값을 스택 [EBP – 4]에 저장하게 되고 cm5.dat 에서 다음 문장을 저장해 둔 곳인 [EBP – 208]의 값을 읽어온 뒤 만들어진 시리얼 값과 한글자씩 비교하게 됩니다. 이때 [EBP – 208]에 있는 문장의 길이는 NAME 값과 같아야 합니다.



만약 비교하여 서로의 문자열 값이 같다면 아래의 분기점인 JNZ 에 걸리지 않게 되고 Registered 구문을 만날 수 있게 됩니다. 즉 정답으로 가는 분기점의 OPCODE 는 JNZ 인 7555 가 되게 됩니다.

이번 문제의 OEP 는 00445834 이며 OPCODE 는 7555 이므로 정답은 004458347555 가 되게 됩니다.