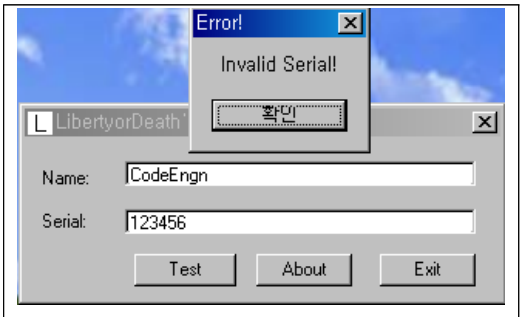
처음에 문제를 PE확인 툴로 봐보니 패커를 모른다고 나왔더군요.. 흐음..
하지만 올디로 열어서 트레이스 해보니 쉽게 OEP를 찾아서 언패킹을 할 수 있었습니다.
언패킹을 하고 난 후 올디로 열어본 처음 화면입니다.(코드를 1바이트씩 읽어서 잘못 읽는 경우 다시 읽도록 Analyse code해주면 됩니다~_~) 어떤 언패킹 방법 중에 있던거 같던데 기억이 않나네요 ^^;

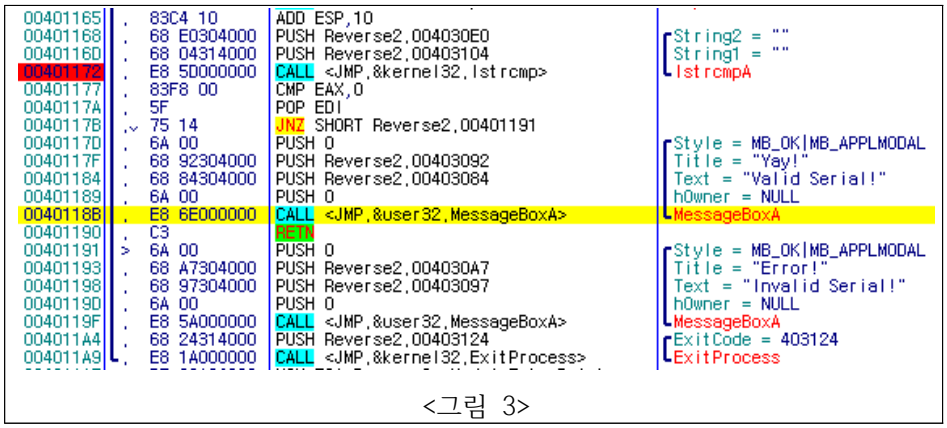
```
00401006  $  6A 00          PUSH 0                                  pModule = NULL
00401008  .  E8 C1010000    CALL <JMP.&kernel32.GetModuleHandleA>   GetModuleHandleA
0040100D  .  A3 BC304000    MOV DWORD PTR DS:[4030BC],EAX
00401012  .  6A 00          PUSH 0                                  lParam = NULL
00401014  .  68 36104000    PUSH Reverse2.00401036                  DlgProc = Reverse2.00401036
00401019  .  6A 00          PUSH 0                                  hOwner = NULL
0040101B  .  68 E9030000    PUSH 3E9                                pTemplate = 3E9
00401020  .  FF35 BC30400(  PUSH DWORD PTR DS:[4030BC]              hInst = NULL
00401026  .  E8 B5010000    CALL <JMP.&user32.DialogBoxParamA>      DialogBoxParamA
0040102B  .  A3 24314000    MOV DWORD PTR DS:[403124],EAX
00401030  .  50             PUSH EAX                                ExitCode
00401031  L. E8 92010000    CALL <JMP.&kernel32.ExitProcess>        ExitProcess
00401036  r. 55             PUSH EBP
00401037  .  8BEC           MOV EBP,ESP
00401039  .  817D 0C 1001(  CMP DWORD PTR SS:[EBP+C],110
00401040  .v 75 38          JNZ SHORT Reverse2.0040107A
00401042  .  68 D0070000    PUSH 7D0                                RsrcName = 2000.
00401047  .  FF35 BC30400(  PUSH DWORD PTR DS:[4030BC]              hInst = NULL
0040104D  .  E8 A6010000    CALL <JMP.&user32.LoadIconA>            LoadIconA
00401052  .  50             PUSH EAX                                lParam
00401053  .  6A 01          PUSH 1                                  wParam = 1
00401055  .  68 80000000    PUSH 80                                 Message = WM_SETICON
0040105A  .  FF75 08        PUSH DWORD PTR SS:[EBP+8]               hWnd
0040105D  .  E8 A2010000    CALL <JMP.&user32.SendMessageA>         SendMessageA
00401062  .  68 EA030000    PUSH 3EA                                ControlID = 3EA (1002.)
00401067  .  FF75 08        PUSH DWORD PTR SS:[EBP+8]               hWnd
0040106A  .  E8 7D010000    CALL <JMP.&user32.GetDlgItem>           GetDlgItem
0040106F  .  50             PUSH EAX                                hWnd
00401070  .  E8 95010000    CALL <JMP.&user32.SetFocus>             SetFocus
00401075  .v E9 94000000    JMP Reverse2.0040110E
```

<그림 1>
프로그램을 키고 어떻게 동작하는지 봐보겠습니다.



<그림 2>
유효하지 않은 시리얼이라고 친절히 팝업창을 띄워주네요.

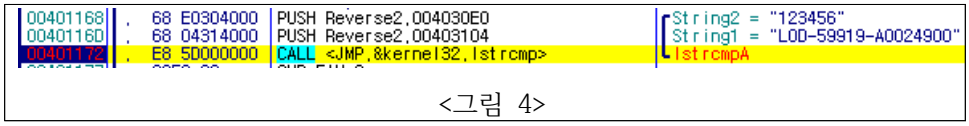
이번 문제는 3번 문제와 별 다른게 없어서 큰 설명을 제외하겠습니다.
방법만 말하면 먼저 해당 문자열("Invaild Serial!")을 찾아가겠습니다.



<그림 3>

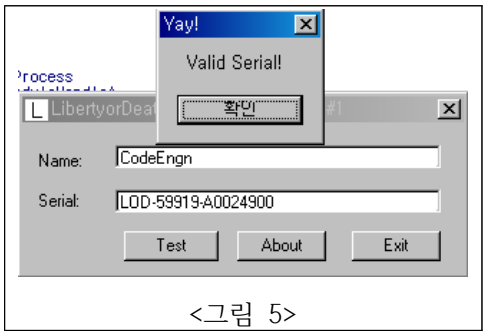
코드를 분석해 보면 두 문자열을 비교하고 있고 비교한 결과가 같으면 JNZ를 실행하지 않고 아래로 내려와 유효한 시리얼이라고 말하고 있고 아니면 점프를 해 유효하지 않은 시리얼을 출력하는 루틴으로 가게 될 것입니다.

이 문제는 특별한게 없는거 같네요.. :)



<그림 4>

답 : LOD-59919-A0024900



<그림 5>