JBU CTF

Reversing

SCP_이다영

문제

범인의 노트북

Emily와 Clay의 아파트

Reversing

범인의 노트북

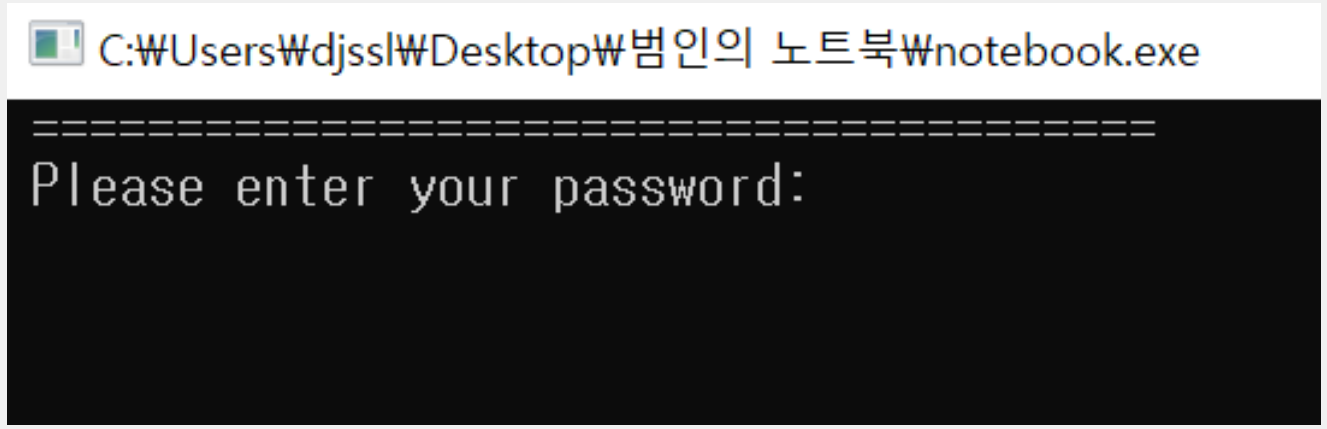
수사관인 당신은 범인을 뒤쫓던 중 범인의 노트북과 메모장을 발견하였다.

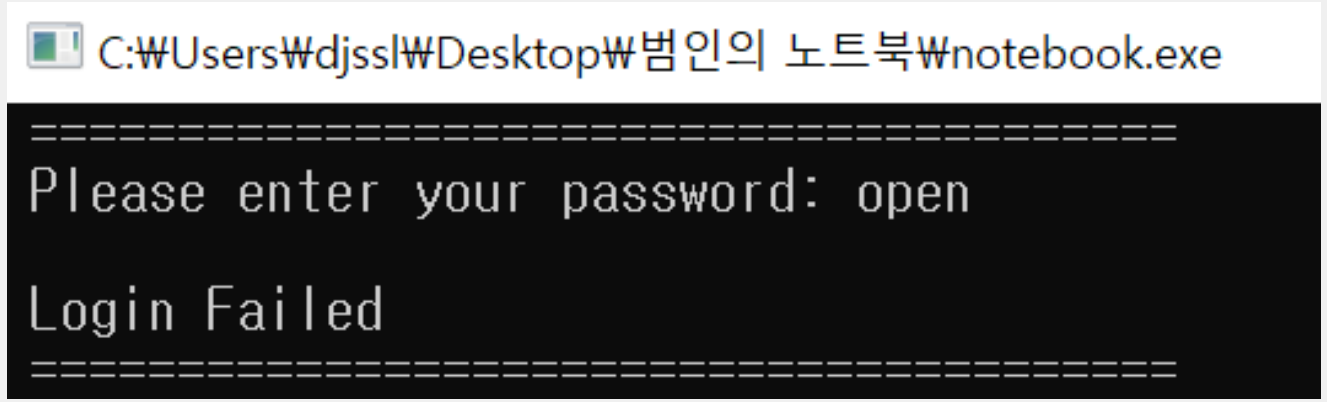
메모장에는 노트북 비밀번호로 추정되는 'open'이 적혀있다.

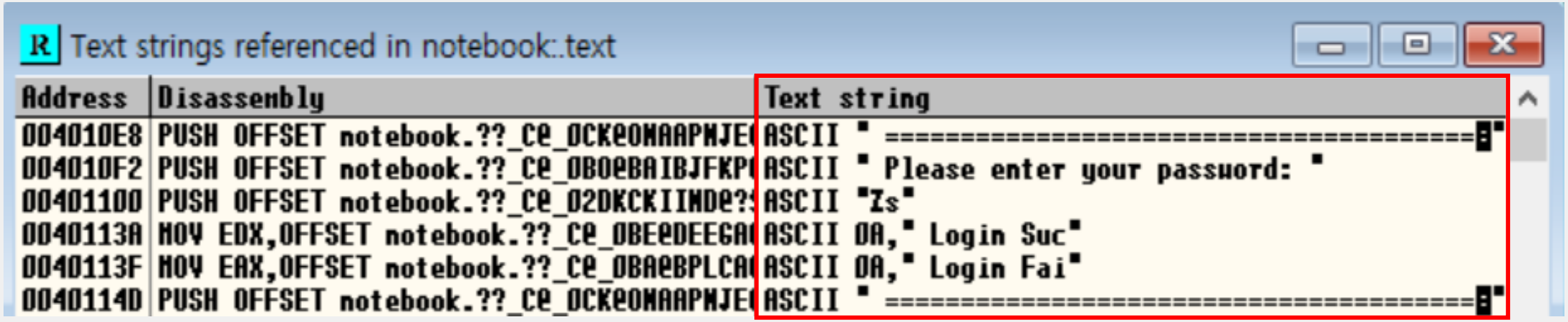
바로 입력해보았지만 올바른 비밀번호가 아니다.

하지만 open과 연관성이 있을 것이다.

시간이 없다! 얼른 진짜 비밀번호를 찾아보자!


C:₩Users₩djssl₩Desktop₩범인의 노트북₩notebook.exe
==========
Please enter your password:

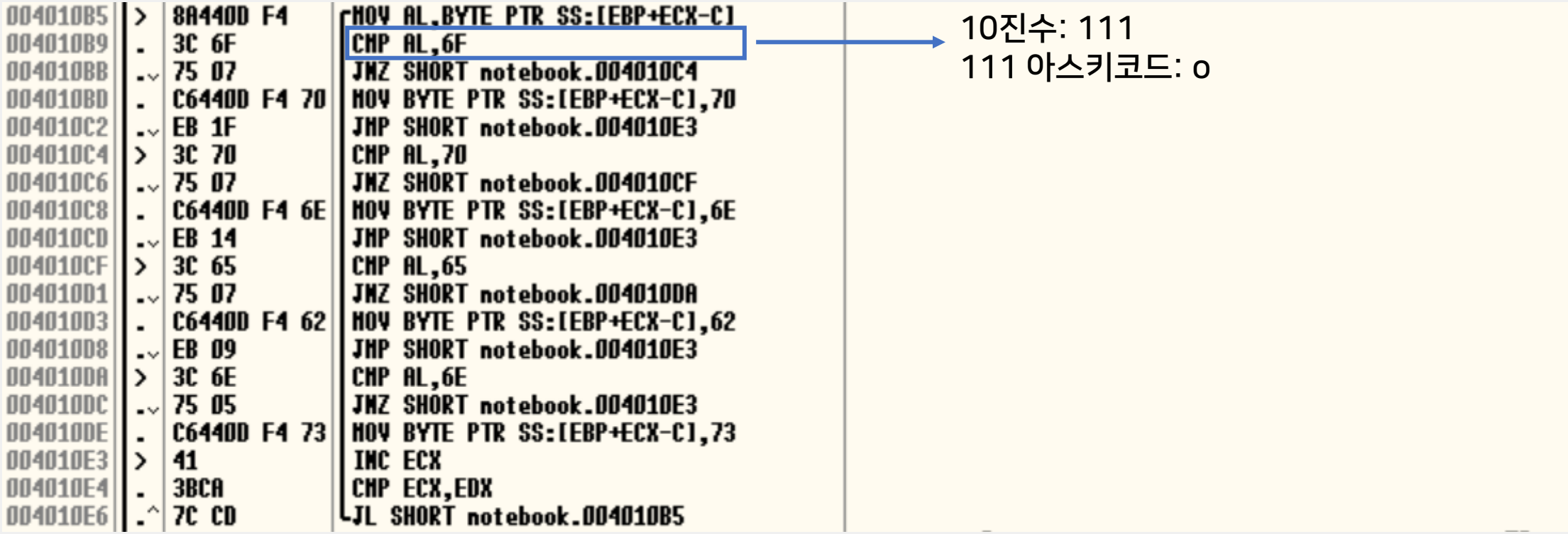

C:₩Users₩djssl₩Desktop₩범인의 노트북₩notebook.exe
==========
Please enter your password: open
Login Failed
==========

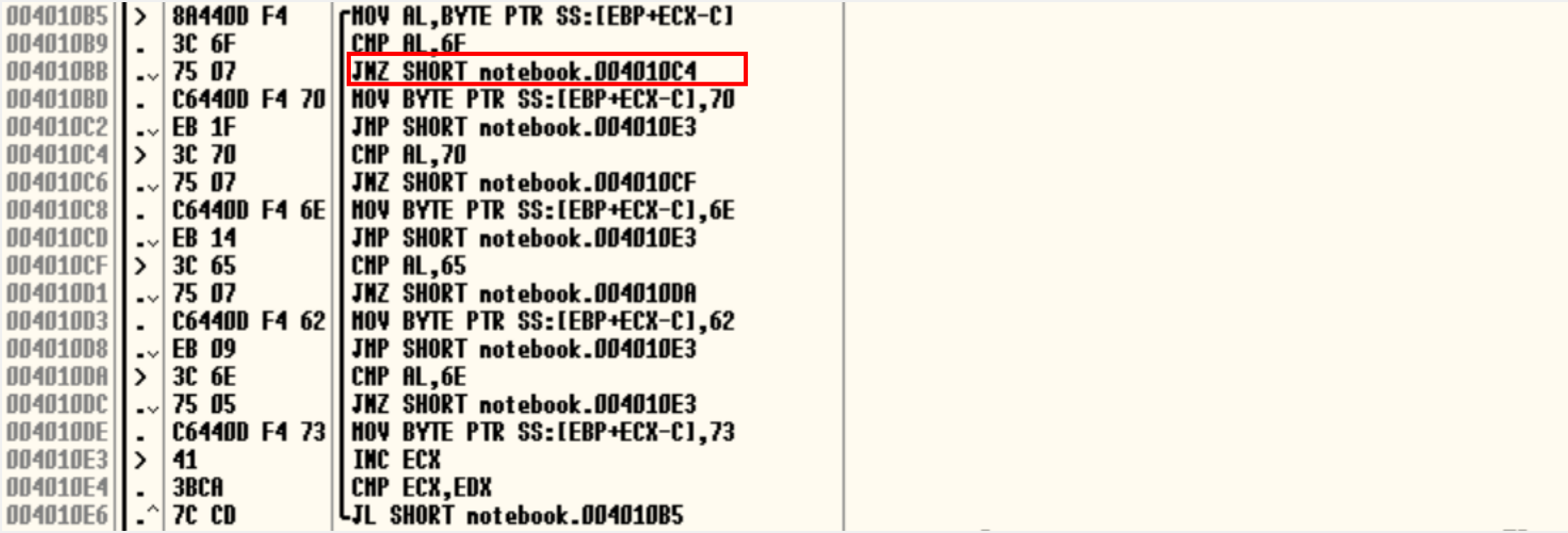

Text strings referenced in notebook:.text
Address
Disassembly
Text string
00401DE8 PUSH OFFSET notebook.??_C@_0CK@OMAAPMJE
ASCII " ==========="
00401DF2 PUSH OFFSET notebook.??_C@_0BO@BAIBJFKP
ASCII " Please enter your passuord: "
00401100 PUSH OFFSET notebook.??_C@_02DKCKIIMD@?
ASCII "Zs"
0040113A MOV EDX,OFFSET notebook.??_C@_0BE@DEEGA
ASCII 0A," Login Suc"
0040113F MOV EAX,OFFSET notebook.??_C@_0BA@BPLCA
ASCII 0A," Login Fai"
0040114D PUSH OFFSET notebook.??_C@_0CK@OMAAPMJE
ASCII " ==========="

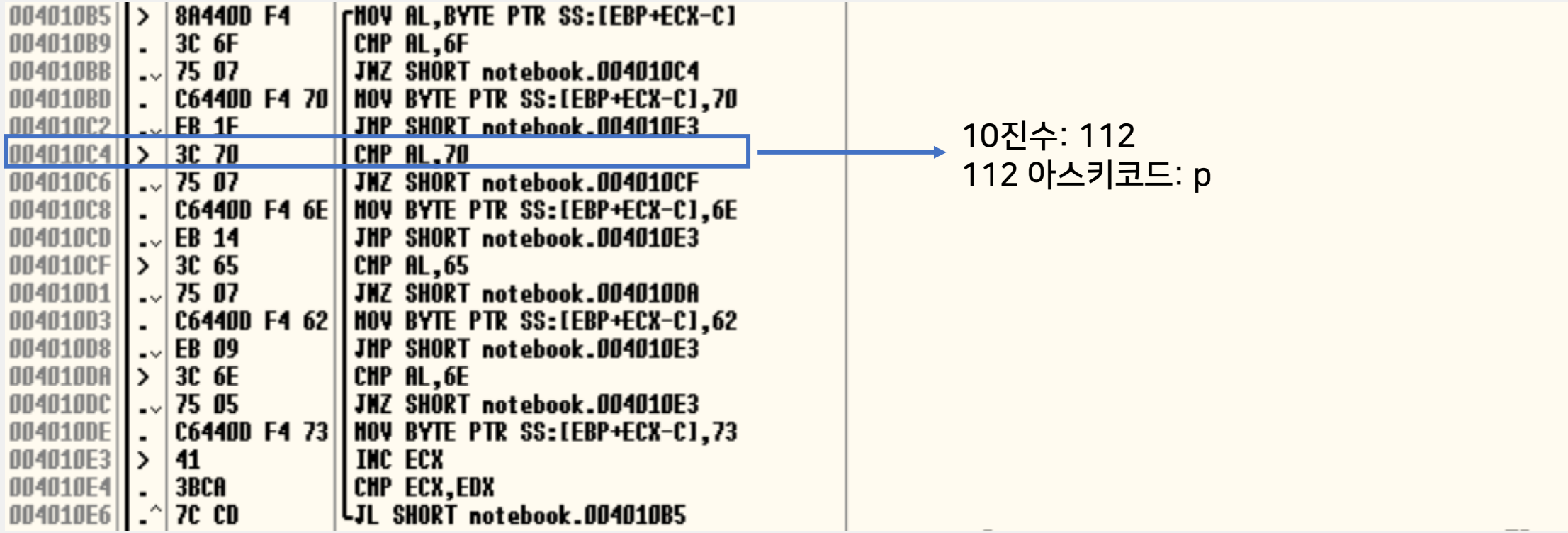
```
0040133D  .  56           PUSH ESI                          Arg2
0040133E  .  FF30         PUSH DWORD PTR DS:[EAX]           Arg1
00401340  .  E8 3BFDFFFF  CALL notebook.main                main
00401345  .  83C4 0C      ADD ESP,0C
00401348  .  8BF0         MOV ESI,EAX
```

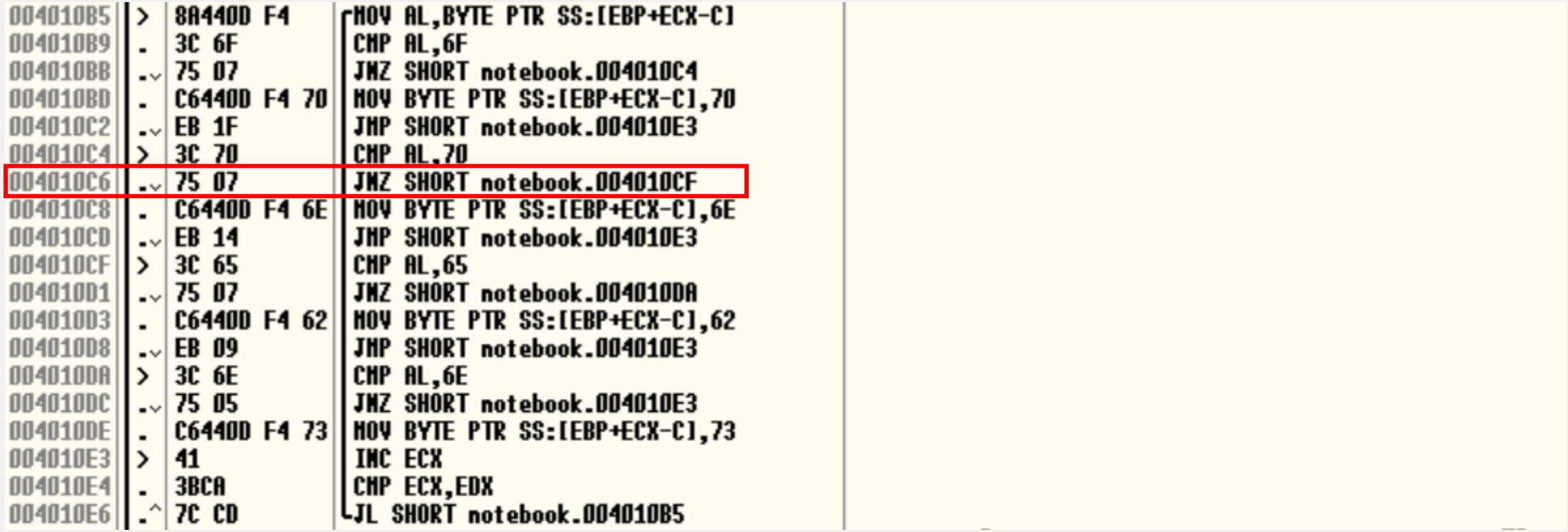
```
00401080  r$ 55           PUSH EBP
00401081  .  8BEC         MOV EBP,ESP
00401083  .  83EC 20      SUB ESP,20
00401086  .  A1 04304000  MOV EAX,DWORD PTR DS:[__security_cookie]
0040108B  .  33C5         XOR EAX,EBP
0040108D  .  8945 FC      MOV DWORD PTR SS:[EBP-4],EAX
00401090  .  A1 08214000  MOV EAX,DWORD PTR DS:[??_C@_04PMOCAHAAE@
00401095  .  8D55 F4      LEA EDX,DWORD PTR SS:[EBP-C]
00401098  .  8945 F4      MOV DWORD PTR SS:[EBP-C],EAX
```

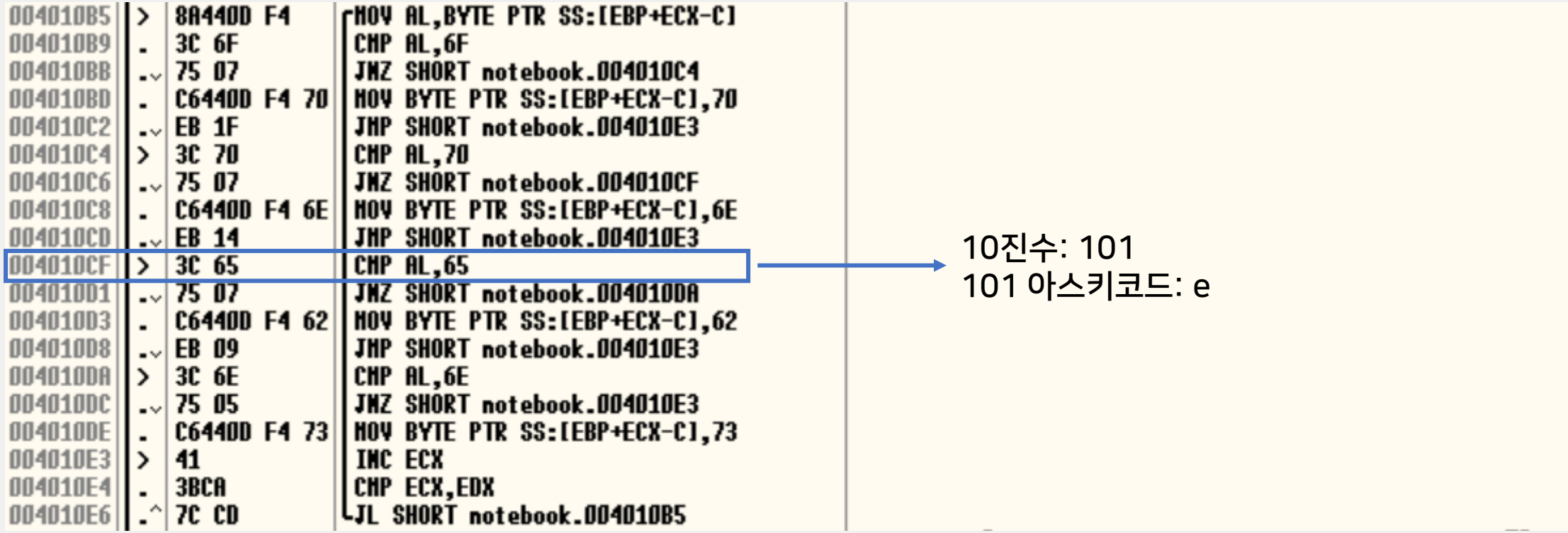
```
004010E8  >  68 10214000  PUSH OFFSET notebook.??_C@_0CK@OMAAPMJE@   format = " ========================================="
004010ED  .  E8 2EFFFFFF  CALL notebook.printf                      printf
004010F2  .  68 3C214000  PUSH OFFSET notebook.??_C@_0BO@EBAIBJFKP@  format = " Please enter your passuord: "
004010F7  .  E8 24FFFFFF  CALL notebook.printf                      printf
004010FC  .  8D45 E0      LEA EAX,DWORD PTR SS:[EBP-20]
```

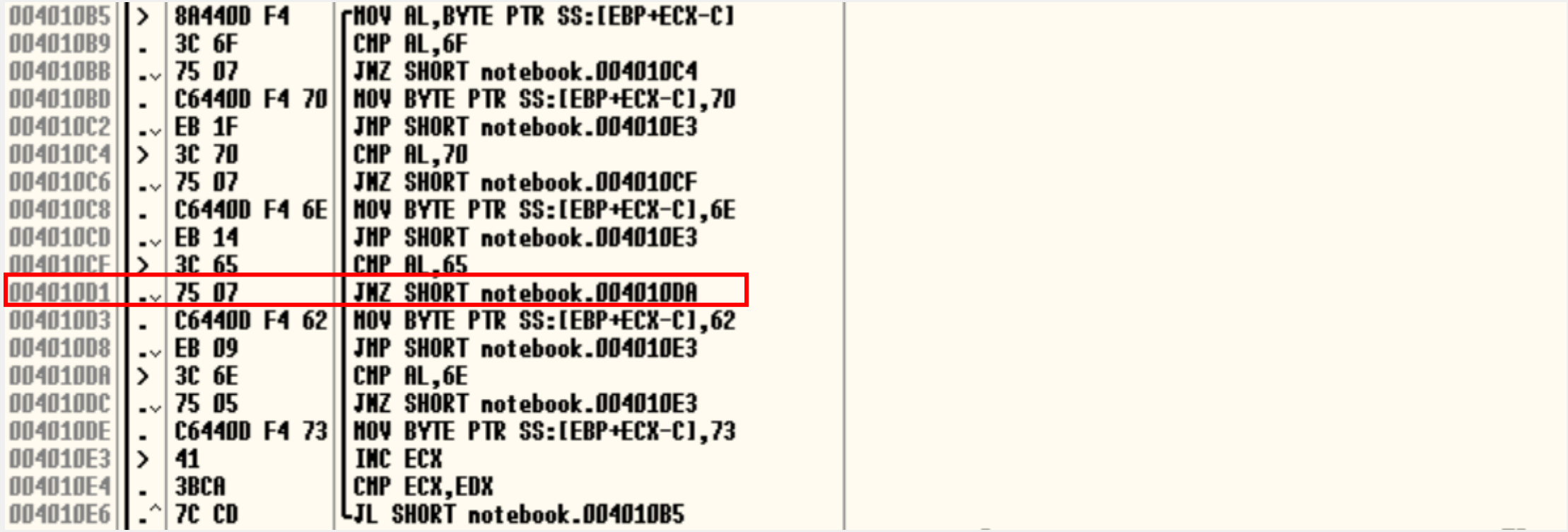

004010B5 > 8A440D F4 MOV AL,BYTE PTR SS:[EBP+ECX-C]
004010B9 . 3C 6F CMP AL,6F
004010BB .v 75 07 JNZ SHORT notebook.004010C4
004010BD . C6440D F4 70 MOV BYTE PTR SS:[EBP+ECX-C],70
004010C2 .v EB 1F JMP SHORT notebook.004010E3
004010C4 > 3C 70 CMP AL,70
004010C6 .v 75 07 JNZ SHORT notebook.004010CF
004010C8 . C6440D F4 6E MOV BYTE PTR SS:[EBP+ECX-C],6E
004010CD .v EB 14 JMP SHORT notebook.004010E3
004010CF > 3C 65 CMP AL,65
004010D1 .v 75 07 JNZ SHORT notebook.004010DA
004010D3 . C6440D F4 62 MOV BYTE PTR SS:[EBP+ECX-C],62
004010D8 .v EB 09 JMP SHORT notebook.004010E3
004010DA > 3C 6E CMP AL,6E
004010DC .v 75 05 JNZ SHORT notebook.004010E3
004010DE . C6440D F4 73 MOV BYTE PTR SS:[EBP+ECX-C],73
004010E3 > 41 INC ECX
004010E4 . 3BCA CMP ECX,EDX
004010E6 .^ 7C CD JL SHORT notebook.004010B5
10진수: 111
111 아스키코드: o

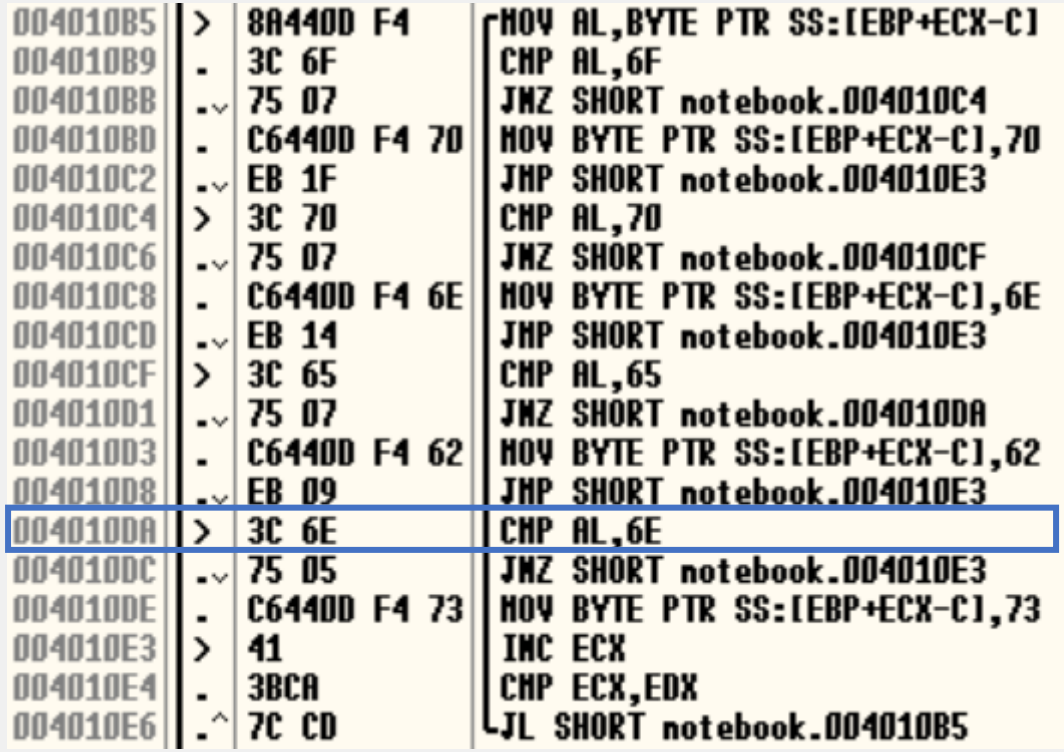

004010B5 > 8A440D F4 MOV AL,BYTE PTR SS:[EBP+ECX-C]
004010B9 . 3C 6F CMP AL,6F
004010BB .v 75 07 JNZ SHORT notebook.004010C4
004010BD . C6440D F4 70 MOV BYTE PTR SS:[EBP+ECX-C],70
004010C2 .v EB 1F JMP SHORT notebook.004010E3
004010C4 > 3C 70 CMP AL,70
004010C6 .v 75 07 JNZ SHORT notebook.004010CF
004010C8 . C6440D F4 6E MOV BYTE PTR SS:[EBP+ECX-C],6E
004010CD .v EB 14 JMP SHORT notebook.004010E3
004010CF > 3C 65 CMP AL,65
004010D1 .v 75 07 JNZ SHORT notebook.004010DA
004010D3 . C6440D F4 62 MOV BYTE PTR SS:[EBP+ECX-C],62
004010D8 .v EB 09 JMP SHORT notebook.004010E3
004010DA > 3C 6E CMP AL,6E
004010DC .v 75 05 JNZ SHORT notebook.004010E3
004010DE . C6440D F4 73 MOV BYTE PTR SS:[EBP+ECX-C],73
004010E3 > 41 INC ECX
004010E4 . 3BCA CMP ECX,EDX
004010E6 .^ 7C CD JL SHORT notebook.004010B5


004010B5 > 8A440D F4 MOV AL,BYTE PTR SS:[EBP+ECX-C]
004010B9 . 3C 6F CMP AL,6F
004010BB .v 75 07 JNZ SHORT notebook.004010C4
004010BD . C6440D F4 70 MOV BYTE PTR SS:[EBP+ECX-C],70
004010C2 .v EB 1F JMP SHORT notebook.004010E3
004010C4 > 3C 70 CMP AL,70
004010C6 .v 75 07 JNZ SHORT notebook.004010CF
004010C8 . C6440D F4 6E MOV BYTE PTR SS:[EBP+ECX-C],6E
004010CD .v EB 14 JMP SHORT notebook.004010E3
004010CF > 3C 65 CMP AL,65
004010D1 .v 75 07 JNZ SHORT notebook.004010DA
004010D3 . C6440D F4 62 MOV BYTE PTR SS:[EBP+ECX-C],62
004010D8 .v EB 09 JMP SHORT notebook.004010E3
004010DA > 3C 6E CMP AL,6E
004010DC .v 75 05 JNZ SHORT notebook.004010E3
004010DE . C6440D F4 73 MOV BYTE PTR SS:[EBP+ECX-C],73
004010E3 > 41 INC ECX
004010E4 . 3BCA CMP ECX,EDX
004010E6 .^ 7C CD JL SHORT notebook.004010B5
10진수: 112
112 아스키코드: p


004010B5 > 8A440D F4 MOV AL,BYTE PTR SS:[EBP+ECX-C]
004010B9 . 3C 6F CMP AL,6F
004010BB .v 75 07 JNZ SHORT notebook.004010C4
004010BD . C6440D F4 70 MOV BYTE PTR SS:[EBP+ECX-C],70
004010C2 .v EB 1F JMP SHORT notebook.004010E3
004010C4 > 3C 70 CMP AL,70
004010C6 .v 75 07 JNZ SHORT notebook.004010CF
004010C8 . C6440D F4 6E MOV BYTE PTR SS:[EBP+ECX-C],6E
004010CD .v EB 14 JMP SHORT notebook.004010E3
004010CF > 3C 65 CMP AL,65
004010D1 .v 75 07 JNZ SHORT notebook.004010DA
004010D3 . C6440D F4 62 MOV BYTE PTR SS:[EBP+ECX-C],62
004010D8 .v EB 09 JMP SHORT notebook.004010E3
004010DA > 3C 6E CMP AL,6E
004010DC .v 75 05 JNZ SHORT notebook.004010E3
004010DE . C6440D F4 73 MOV BYTE PTR SS:[EBP+ECX-C],73
004010E3 > 41 INC ECX
004010E4 . 3BCA CMP ECX,EDX
004010E6 .^ 7C CD JL SHORT notebook.004010B5

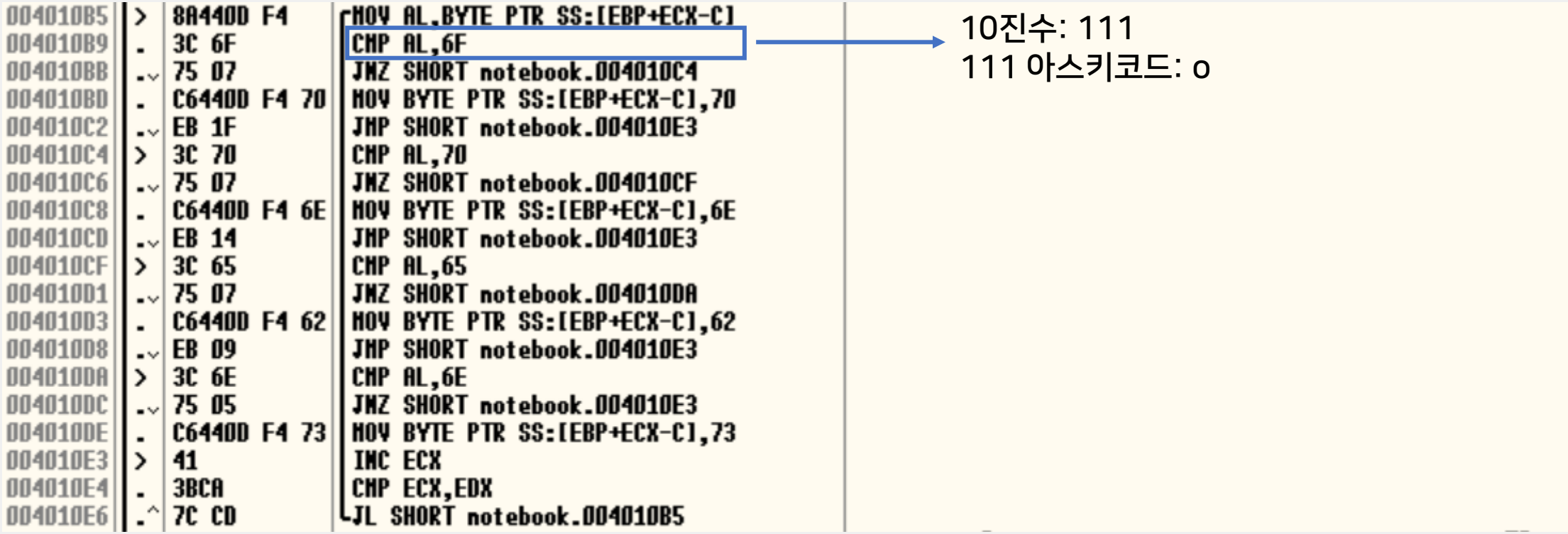

004010B5 > 8A440D F4 MOV AL,BYTE PTR SS:[EBP+ECX-C]
004010B9 . 3C 6F CMP AL,6F
004010BB .v 75 07 JNZ SHORT notebook.004010C4
004010BD . C6440D F4 70 MOV BYTE PTR SS:[EBP+ECX-C],70
004010C2 .v EB 1F JMP SHORT notebook.004010E3
004010C4 > 3C 70 CMP AL,70
004010C6 .v 75 07 JNZ SHORT notebook.004010CF
004010C8 . C6440D F4 6E MOV BYTE PTR SS:[EBP+ECX-C],6E
004010CD .v EB 14 JMP SHORT notebook.004010E3
004010CF > 3C 65 CMP AL,65
004010D1 .v 75 07 JNZ SHORT notebook.004010DA
004010D3 . C6440D F4 62 MOV BYTE PTR SS:[EBP+ECX-C],62
004010D8 .v EB 09 JMP SHORT notebook.004010E3
004010DA > 3C 6E CMP AL,6E
004010DC .v 75 05 JNZ SHORT notebook.004010E3
004010DE . C6440D F4 73 MOV BYTE PTR SS:[EBP+ECX-C],73
004010E3 > 41 INC ECX
004010E4 . 3BCA CMP ECX,EDX
004010E6 .^ 7C CD JL SHORT notebook.004010B5
10진수: 101
101 아스키코드: e

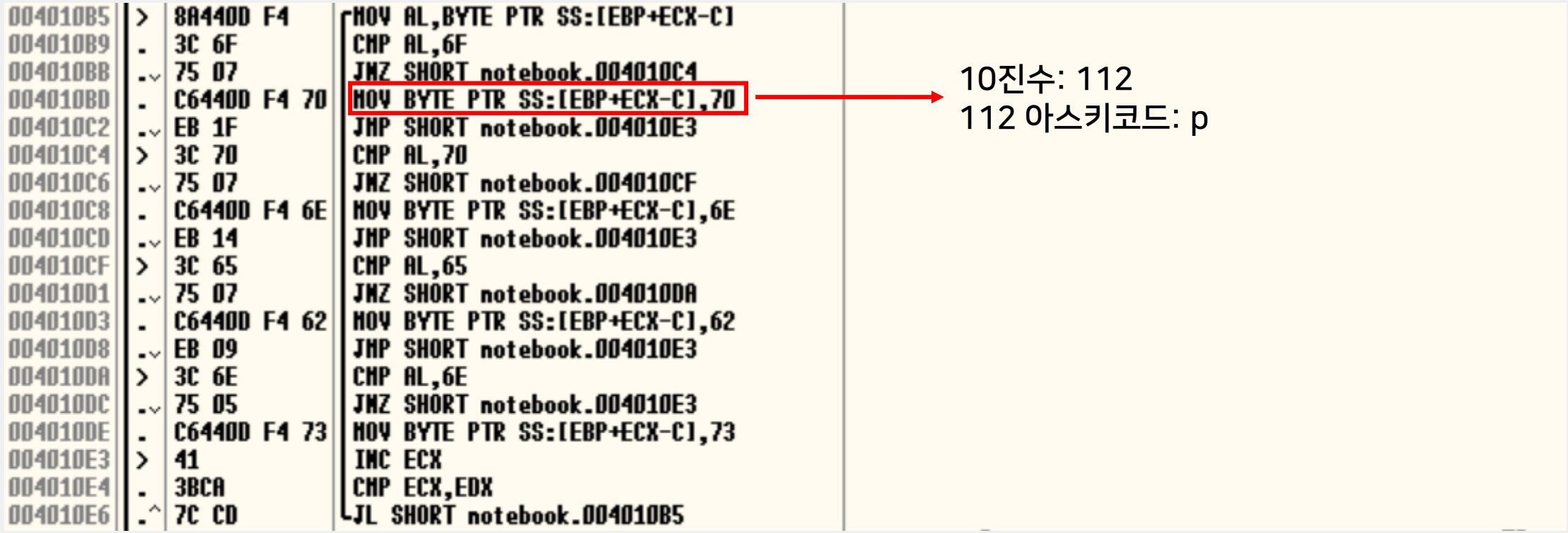

004010B5 > 8A440D F4 MOV AL,BYTE PTR SS:[EBP+ECX-C]
004010B9 . 3C 6F CMP AL,6F
004010BB .v 75 07 JNZ SHORT notebook.004010C4
004010BD . C6440D F4 70 MOV BYTE PTR SS:[EBP+ECX-C],70
004010C2 .v EB 1F JMP SHORT notebook.004010E3
004010C4 > 3C 70 CMP AL,70
004010C6 .v 75 07 JNZ SHORT notebook.004010CF
004010C8 . C6440D F4 6E MOV BYTE PTR SS:[EBP+ECX-C],6E
004010CD .v EB 14 JMP SHORT notebook.004010E3
004010CF > 3C 65 CMP AL,65
004010D1 .v 75 07 JNZ SHORT notebook.004010DA
004010D3 . C6440D F4 62 MOV BYTE PTR SS:[EBP+ECX-C],62
004010D8 .v EB 09 JMP SHORT notebook.004010E3
004010DA > 3C 6E CMP AL,6E
004010DC .v 75 05 JNZ SHORT notebook.004010E3
004010DE . C6440D F4 73 MOV BYTE PTR SS:[EBP+ECX-C],73
004010E3 > 41 INC ECX
004010E4 . 3BCA CMP ECX,EDX
004010E6 .^ 7C CD JL SHORT notebook.004010B5

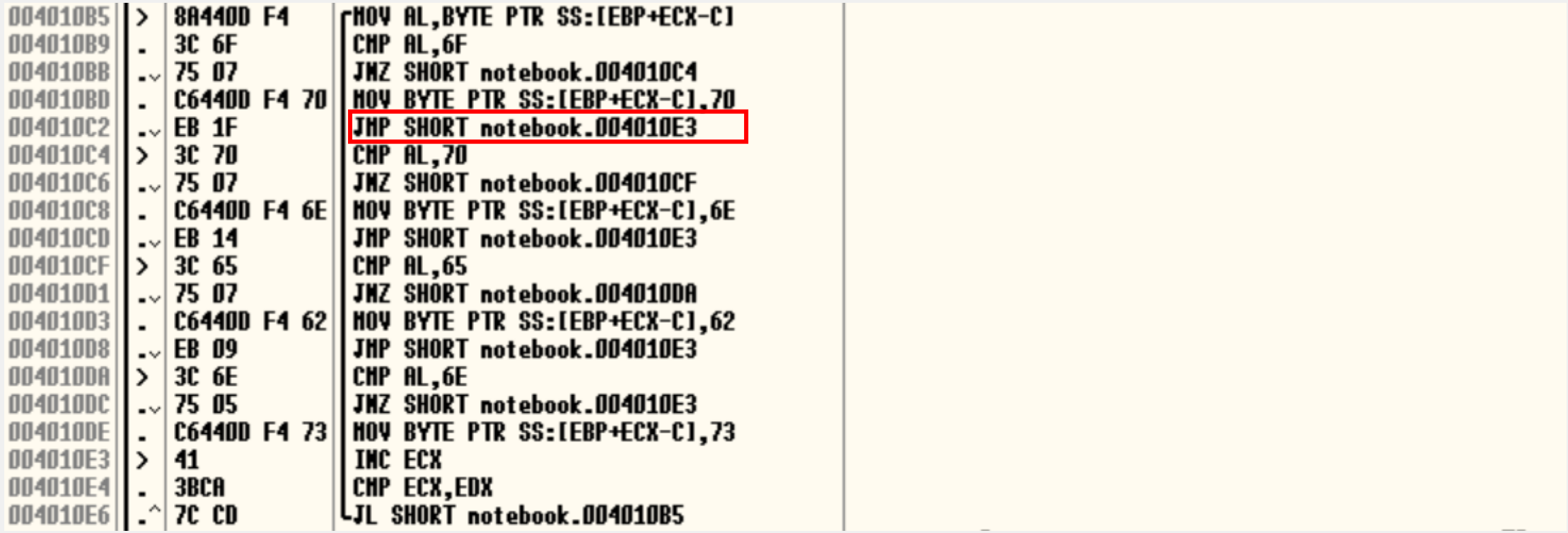


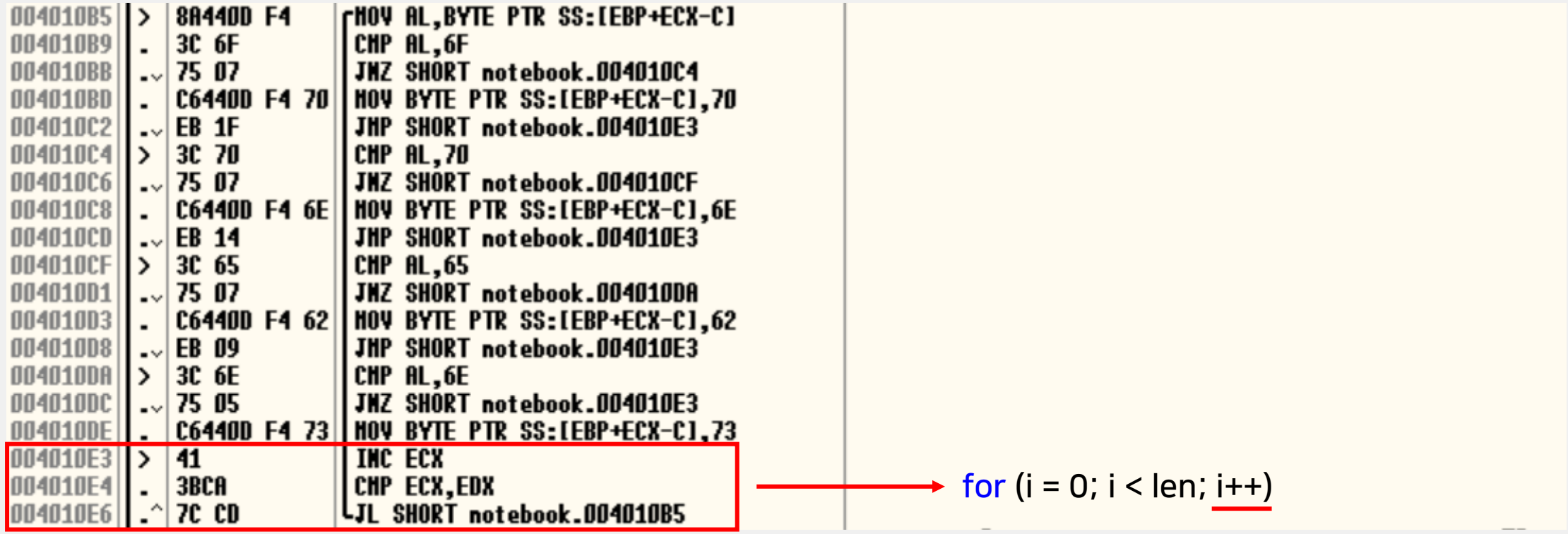
10진수: 110
110 아스키코드: n

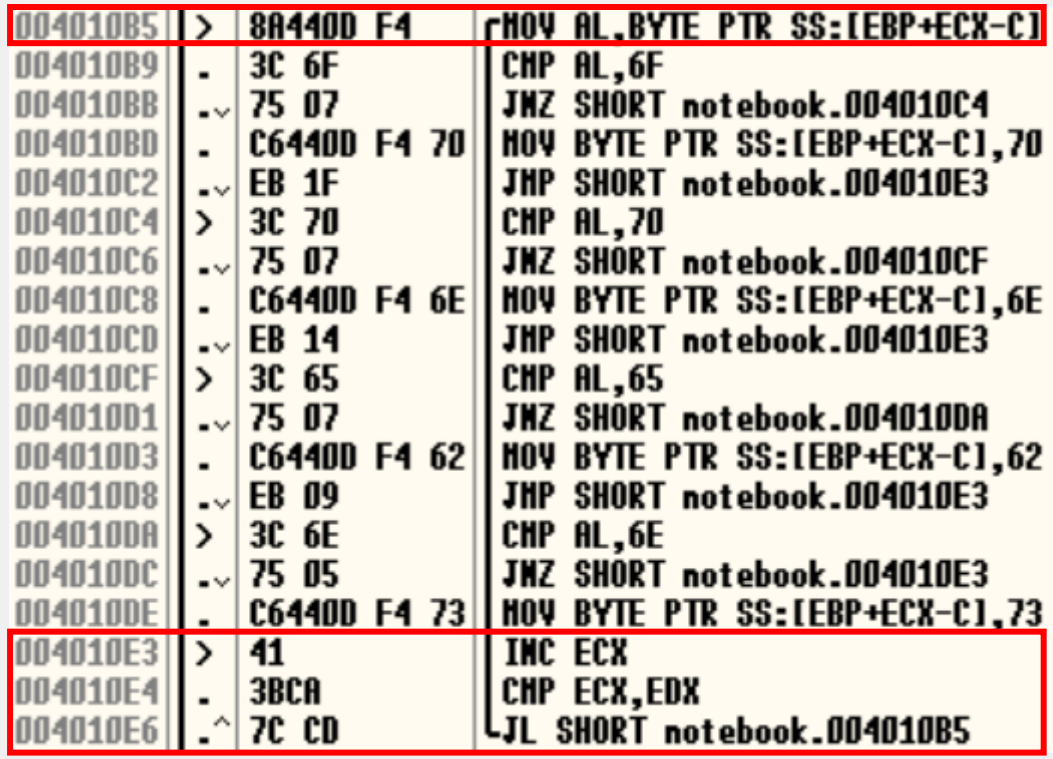
open


004010B5 > 8A440D F4 MOV AL,BYTE PTR SS:[EBP+ECX-C]
004010B9 . 3C 6F CMP AL,6F
004010BB .v 75 07 JNZ SHORT notebook.004010C4
004010BD . C6440D F4 70 MOV BYTE PTR SS:[EBP+ECX-C],70
004010C2 .v EB 1F JMP SHORT notebook.004010E3
004010C4 > 3C 70 CMP AL,70
004010C6 .v 75 07 JNZ SHORT notebook.004010CF
004010C8 . C6440D F4 6E MOV BYTE PTR SS:[EBP+ECX-C],6E
004010CD .v EB 14 JMP SHORT notebook.004010E3
004010CF > 3C 65 CMP AL,65
004010D1 .v 75 07 JNZ SHORT notebook.004010DA
004010D3 . C6440D F4 62 MOV BYTE PTR SS:[EBP+ECX-C],62
004010D8 .v EB 09 JMP SHORT notebook.004010E3
004010DA > 3C 6E CMP AL,6E
004010DC .v 75 05 JNZ SHORT notebook.004010E3
004010DE . C6440D F4 73 MOV BYTE PTR SS:[EBP+ECX-C],73
004010E3 > 41 INC ECX
004010E4 . 3BCA CMP ECX,EDX
004010E6 .^ 7C CD JL SHORT notebook.004010B5
10진수: 111
111 아스키코드: o

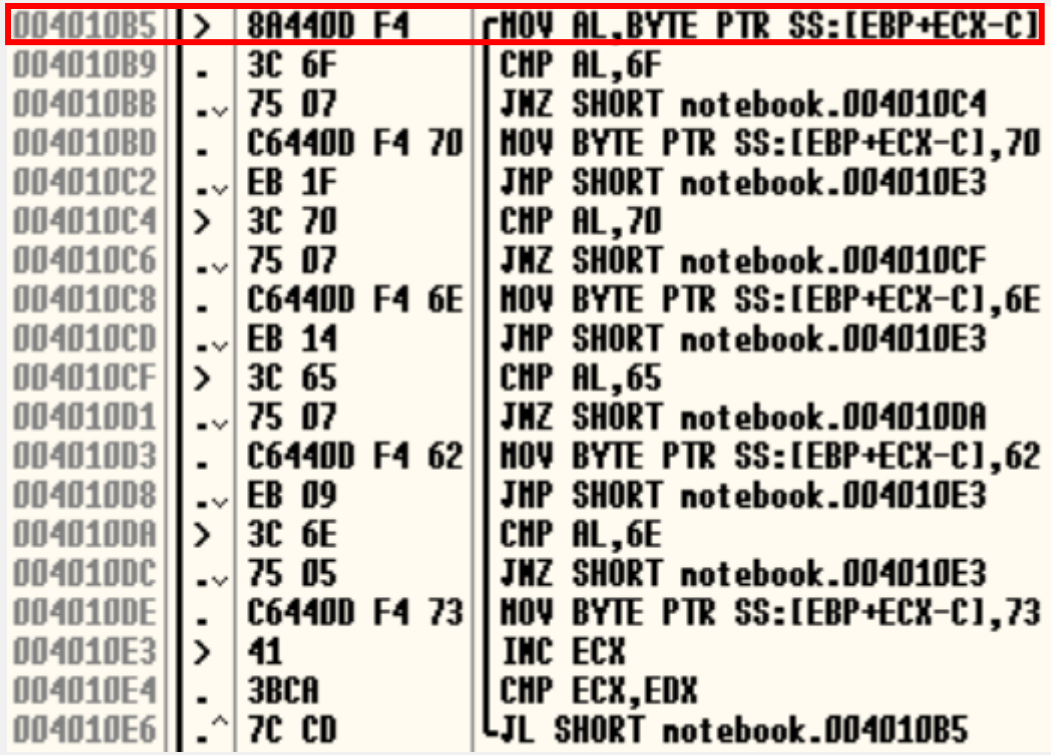

004010B5 > 8A440D F4 MOV AL,BYTE PTR SS:[EBP+ECX-C]
004010B9 . 3C 6F CMP AL,6F
004010BB .v 75 07 JNZ SHORT notebook.004010C4
004010BD . C6440D F4 70 MOV BYTE PTR SS:[EBP+ECX-C],70
004010C2 .v EB 1F JMP SHORT notebook.004010E3
004010C4 > 3C 70 CMP AL,70
004010C6 .v 75 07 JNZ SHORT notebook.004010CF
004010C8 . C6440D F4 6E MOV BYTE PTR SS:[EBP+ECX-C],6E
004010CD .v EB 14 JMP SHORT notebook.004010E3
004010CF > 3C 65 CMP AL,65
004010D1 .v 75 07 JNZ SHORT notebook.004010DA
004010D3 . C6440D F4 62 MOV BYTE PTR SS:[EBP+ECX-C],62
004010D8 .v EB 09 JMP SHORT notebook.004010E3
004010DA > 3C 6E CMP AL,6E
004010DC .v 75 05 JNZ SHORT notebook.004010E3
004010DE . C6440D F4 73 MOV BYTE PTR SS:[EBP+ECX-C],73
004010E3 > 41 INC ECX
004010E4 . 3BCA CMP ECX,EDX
004010E6 .^ 7C CD JL SHORT notebook.004010B5
10진수: 112
112 아스키코드: p


004010B5 > 8A440D F4 MOV AL,BYTE PTR SS:[EBP+ECX-C]
004010B9 . 3C 6F CMP AL,6F
004010BB .v 75 07 JNZ SHORT notebook.004010C4
004010BD . C6440D F4 70 MOV BYTE PTR SS:[EBP+ECX-C],70
004010C2 .v EB 1F JMP SHORT notebook.004010E3
004010C4 > 3C 70 CMP AL,70
004010C6 .v 75 07 JNZ SHORT notebook.004010CF
004010C8 . C6440D F4 6E MOV BYTE PTR SS:[EBP+ECX-C],6E
004010CD .v EB 14 JMP SHORT notebook.004010E3
004010CF > 3C 65 CMP AL,65
004010D1 .v 75 07 JNZ SHORT notebook.004010DA
004010D3 . C6440D F4 62 MOV BYTE PTR SS:[EBP+ECX-C],62
004010D8 .v EB 09 JMP SHORT notebook.004010E3
004010DA > 3C 6E CMP AL,6E
004010DC .v 75 05 JNZ SHORT notebook.004010E3
004010DE . C6440D F4 73 MOV BYTE PTR SS:[EBP+ECX-C],73
004010E3 > 41 INC ECX
004010E4 . 3BCA CMP ECX,EDX
004010E6 .^ 7C CD JL SHORT notebook.004010B5


004010B5 > 8A440D F4 MOV AL,BYTE PTR SS:[EBP+ECX-C]
004010B9 . 3C 6F CMP AL,6F
004010BB .v 75 07 JNZ SHORT notebook.004010C4
004010BD . C6440D F4 70 MOV BYTE PTR SS:[EBP+ECX-C],70
004010C2 .v EB 1F JMP SHORT notebook.004010E3
004010C4 > 3C 70 CMP AL,70
004010C6 .v 75 07 JNZ SHORT notebook.004010CF
004010C8 . C6440D F4 6E MOV BYTE PTR SS:[EBP+ECX-C],6E
004010CD .v EB 14 JMP SHORT notebook.004010E3
004010CF > 3C 65 CMP AL,65
004010D1 .v 75 07 JNZ SHORT notebook.004010DA
004010D3 . C6440D F4 62 MOV BYTE PTR SS:[EBP+ECX-C],62
004010D8 .v EB 09 JMP SHORT notebook.004010E3
004010DA > 3C 6E CMP AL,6E
004010DC .v 75 05 JNZ SHORT notebook.004010E3
004010DE . C6440D F4 73 MOV BYTE PTR SS:[EBP+ECX-C],73
004010E3 > 41 INC ECX
004010E4 . 3BCA CMP ECX,EDX
004010E6 .^ 7C CD JL SHORT notebook.004010B5
for (i = 0; i < len; i++)

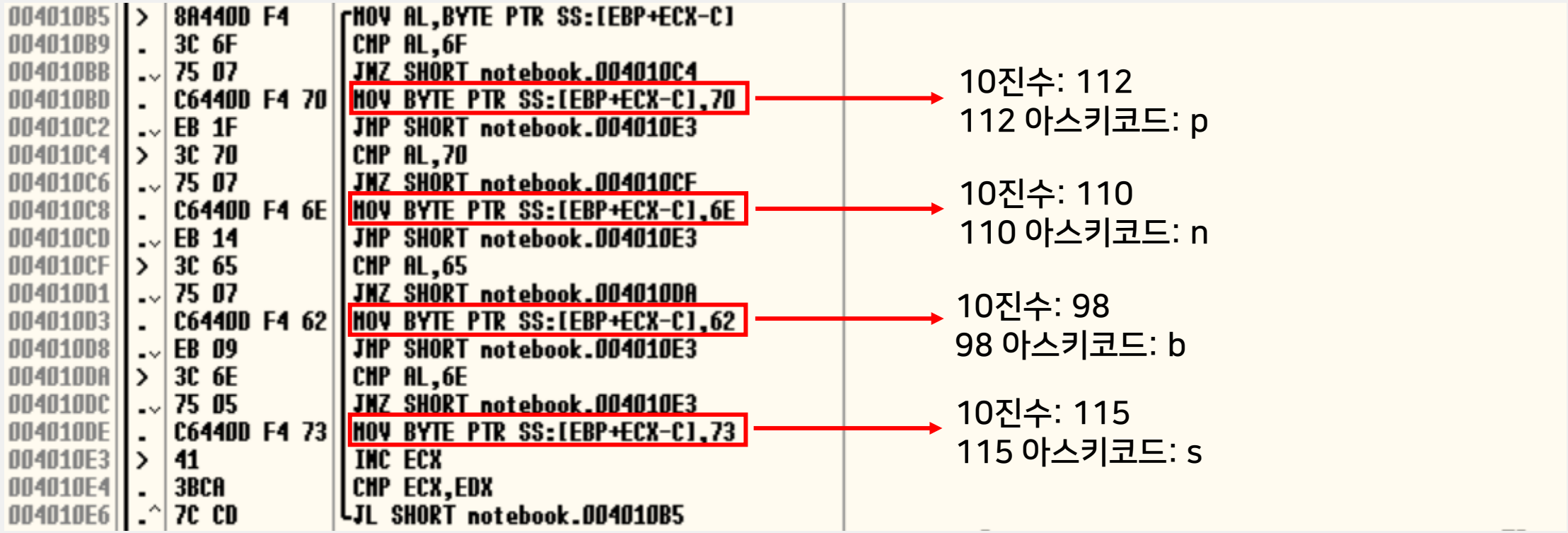

004010B5 > 8A440D F4 MOV AL,BYTE PTR SS:[EBP+ECX-C]
004010B9 . 3C 6F CMP AL,6F
004010BB .v 75 07 JNZ SHORT notebook.004010C4
004010BD . C6440D F4 70 MOV BYTE PTR SS:[EBP+ECX-C],70
004010C2 .v EB 1F JMP SHORT notebook.004010E3
004010C4 > 3C 70 CMP AL,70
004010C6 .v 75 07 JNZ SHORT notebook.004010CF
004010C8 . C6440D F4 6E MOV BYTE PTR SS:[EBP+ECX-C],6E
004010CD .v EB 14 JMP SHORT notebook.004010E3
004010CF > 3C 65 CMP AL,65
004010D1 .v 75 07 JNZ SHORT notebook.004010DA
004010D3 . C6440D F4 62 MOV BYTE PTR SS:[EBP+ECX-C],62
004010D8 .v EB 09 JMP SHORT notebook.004010E3
004010DA > 3C 6E CMP AL,6E
004010DC .v 75 05 JNZ SHORT notebook.004010E3
004010DE . C6440D F4 73 MOV BYTE PTR SS:[EBP+ECX-C],73
004010E3 > 41 INC ECX
004010E4 . 3BCA CMP ECX,EDX
004010E6 .^ 7C CD JL SHORT notebook.004010B5

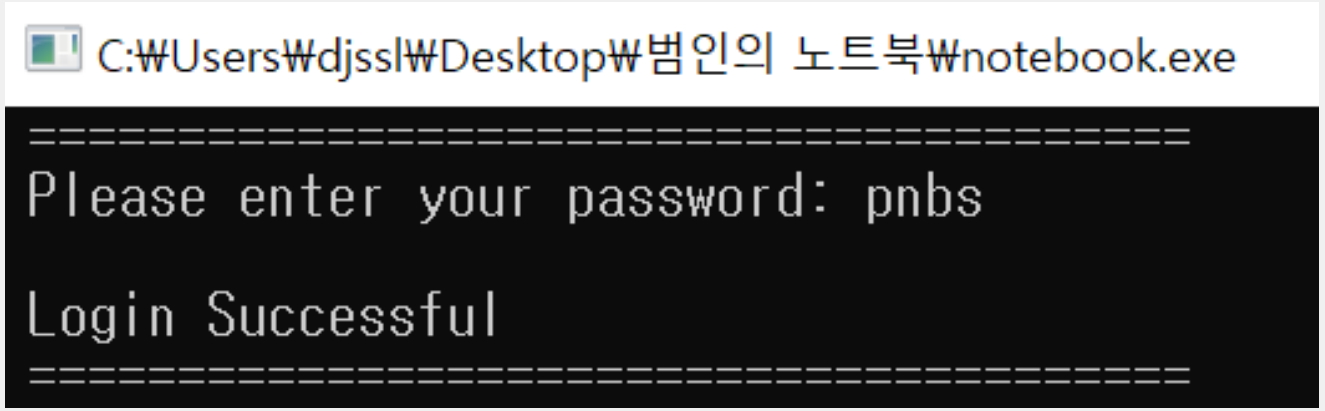
for (i = 0; i < len; i++)



```
004010B5  >  8A440D F4     MOV AL,BYTE PTR SS:[EBP+ECX-C]
004010B9  .  3C 6F         CMP AL,6F
004010BB  .v 75 07         JNZ SHORT notebook.004010C4
004010BD  .  C6440D F4 70  MOV BYTE PTR SS:[EBP+ECX-C],70
004010C2  .v EB 1F         JMP SHORT notebook.004010E3
004010C4  >  3C 70         CMP AL,70
004010C6  .v 75 07         JNZ SHORT notebook.004010CF
004010C8  .  C6440D F4 6E  MOV BYTE PTR SS:[EBP+ECX-C],6E
004010CD  .v EB 14         JMP SHORT notebook.004010E3
004010CF  >  3C 65         CMP AL,65
004010D1  .v 75 07         JNZ SHORT notebook.004010DA
004010D3  .  C6440D F4 62  MOV BYTE PTR SS:[EBP+ECX-C],62
004010D8  .v EB 09         JMP SHORT notebook.004010E3
004010DA  >  3C 6E         CMP AL,6E
004010DC  .v 75 05         JNZ SHORT notebook.004010E3
004010DE  .  C6440D F4 73  MOV BYTE PTR SS:[EBP+ECX-C],73
004010E3  >  41            INC ECX
004010E4  .  3BCA          CMP ECX,EDX
004010E6  .^ 7C CD         JL SHORT notebook.004010B5
```

for
if
else if
else if
else if


00401085 > 8A440D F4 MOV AL,BYTE PTR SS:[EBP+ECX-C]
00401089 . 3C 6F CMP AL,6F
0040108B .v 75 07 JNZ SHORT notebook.00401C4
0040108D . C6440D F4 70 MOV BYTE PTR SS:[EBP+ECX-C],70
00401092 .v EB 1F JMP SHORT notebook.004010E3
00401094 > 3C 70 CMP AL,70
00401096 .v 75 07 JNZ SHORT notebook.0040109F
00401098 . C6440D F4 6E MOV BYTE PTR SS:[EBP+ECX-C],6E
0040109D .v EB 14 JMP SHORT notebook.004010E3
0040109F > 3C 65 CMP AL,65
004010A1 .v 75 07 JNZ SHORT notebook.004010AA
004010A3 . C6440D F4 62 MOV BYTE PTR SS:[EBP+ECX-C],62
004010A8 .v EB 09 JMP SHORT notebook.004010E3
004010AA > 3C 6E CMP AL,6E
004010AC .v 75 05 JNZ SHORT notebook.004010E3
004010AE . C6440D F4 73 MOV BYTE PTR SS:[EBP+ECX-C],73
004010E3 > 41 INC ECX
004010E4 . 3BCA CMP ECX,EDX
004010E6 .^ 7C CD JL SHORT notebook.00401085
10진수: 112
112 아스키코드: p
10진수: 110
110 아스키코드: n
10진수: 98
98 아스키코드: b
10진수: 115
115 아스키코드: s


C:₩Users₩djssl₩Desktop₩범인의 노트북₩notebook.exe
==========
Please enter your password: pnbs
Login Successful
==========

scpCTF{pnbs}

Reversing

Emily와 Clay의 아파트

Emily와 Clay가 살고있는 아파트는 층수가 무려 100층까지 있다.

그렇다면 Emily의 집은 몇 층일지 아래 프로그램을 통해 맞춰보자.

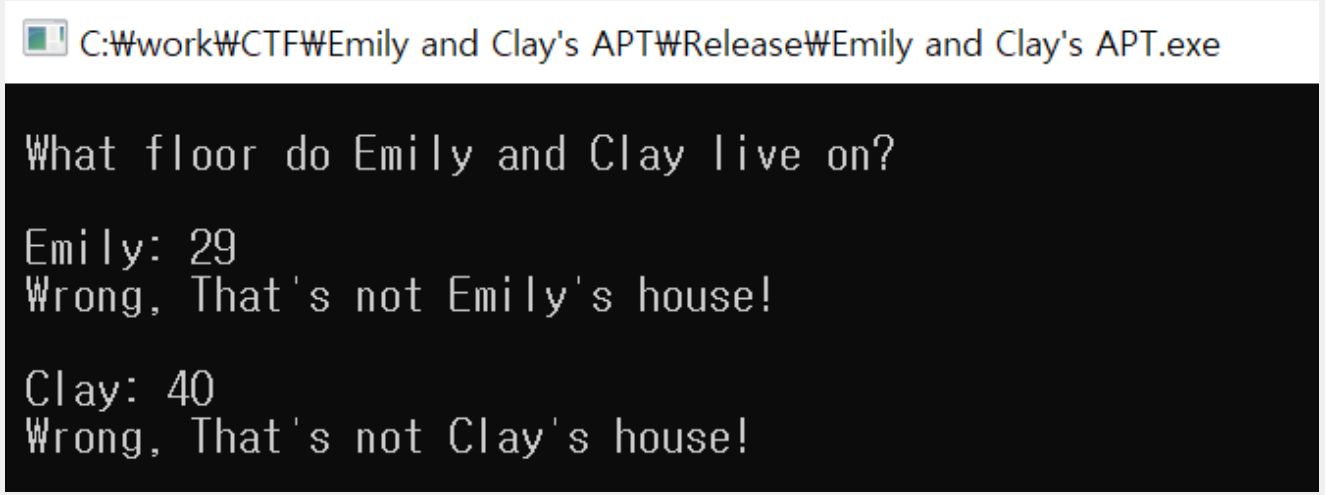
Clay는 내일 이사를 가므로, 맞는 층수를 입력했을 때 ' It's a wrong approach.'가

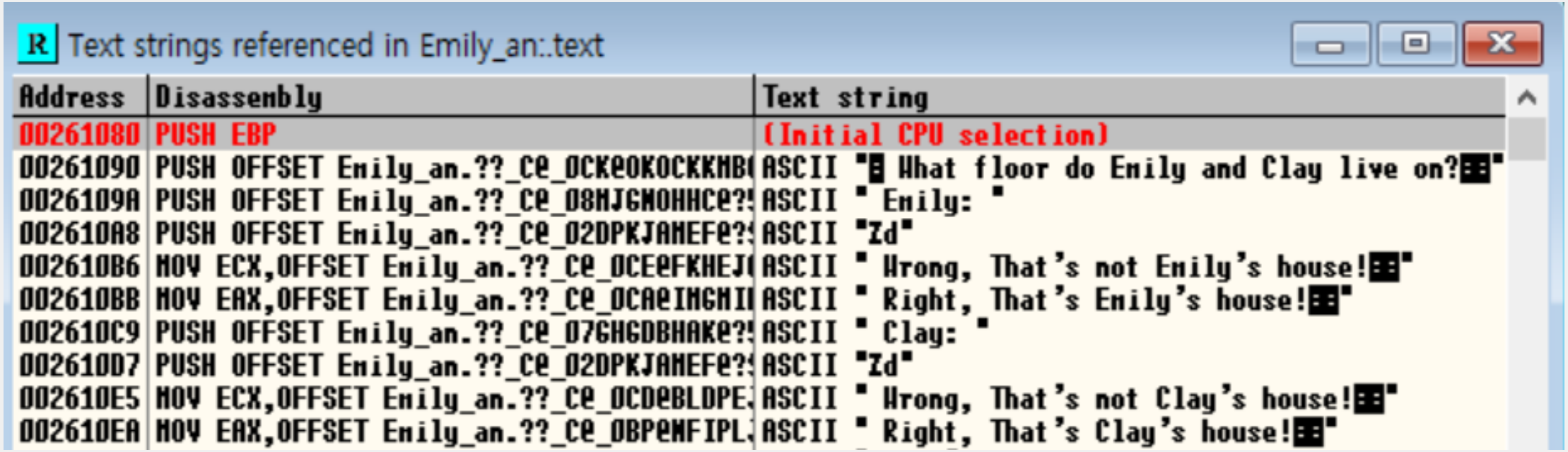
나오도록 HXD로 수정해보자.

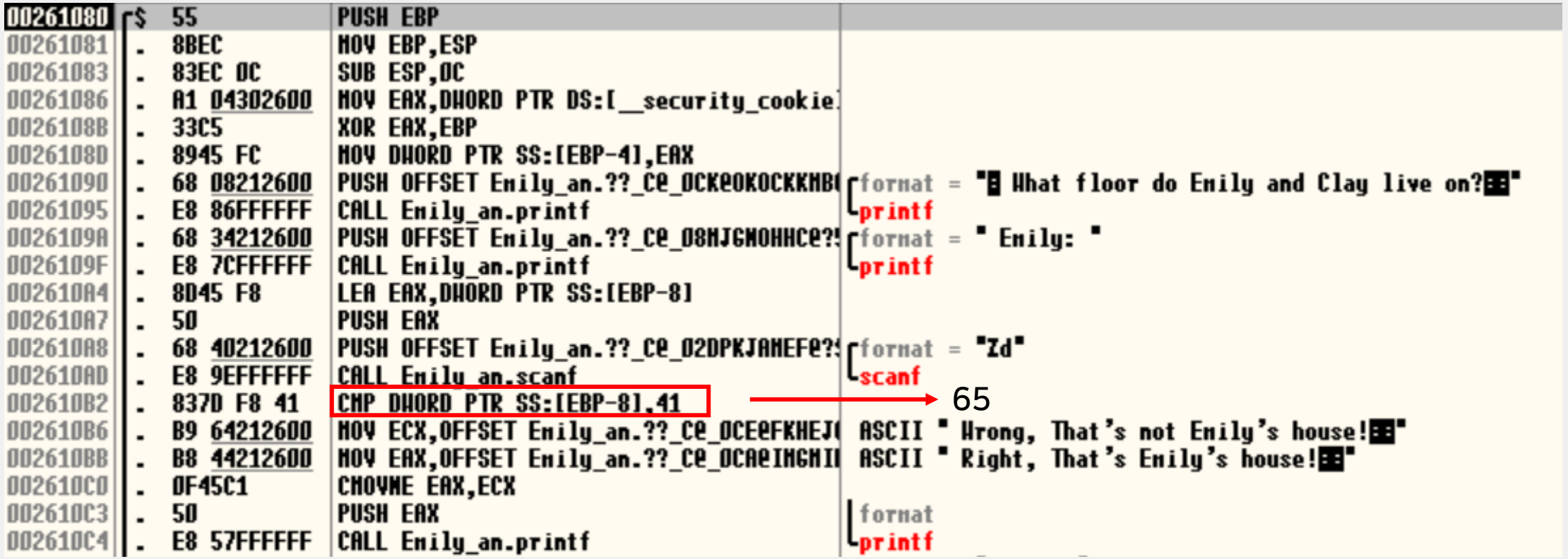
* 각 문장의 맨 앞은 무조건 공백이다.

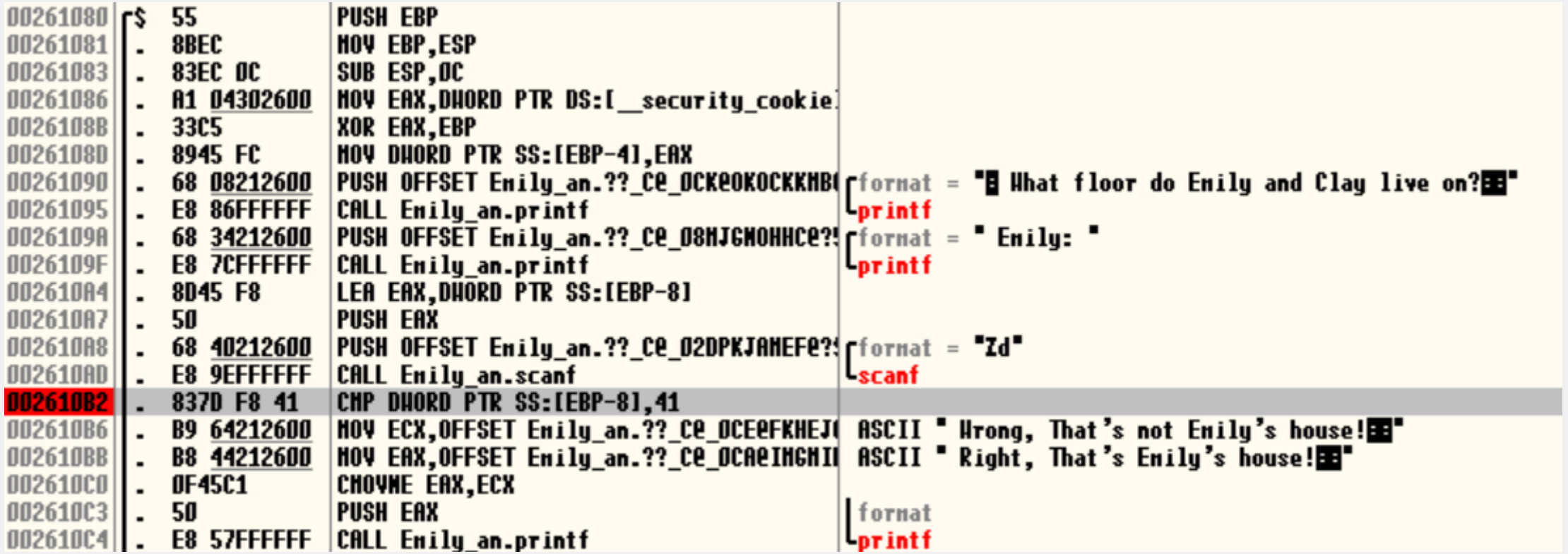
→ Emily가 사는 층 + 수정 완료한 영역의 끝 주소값

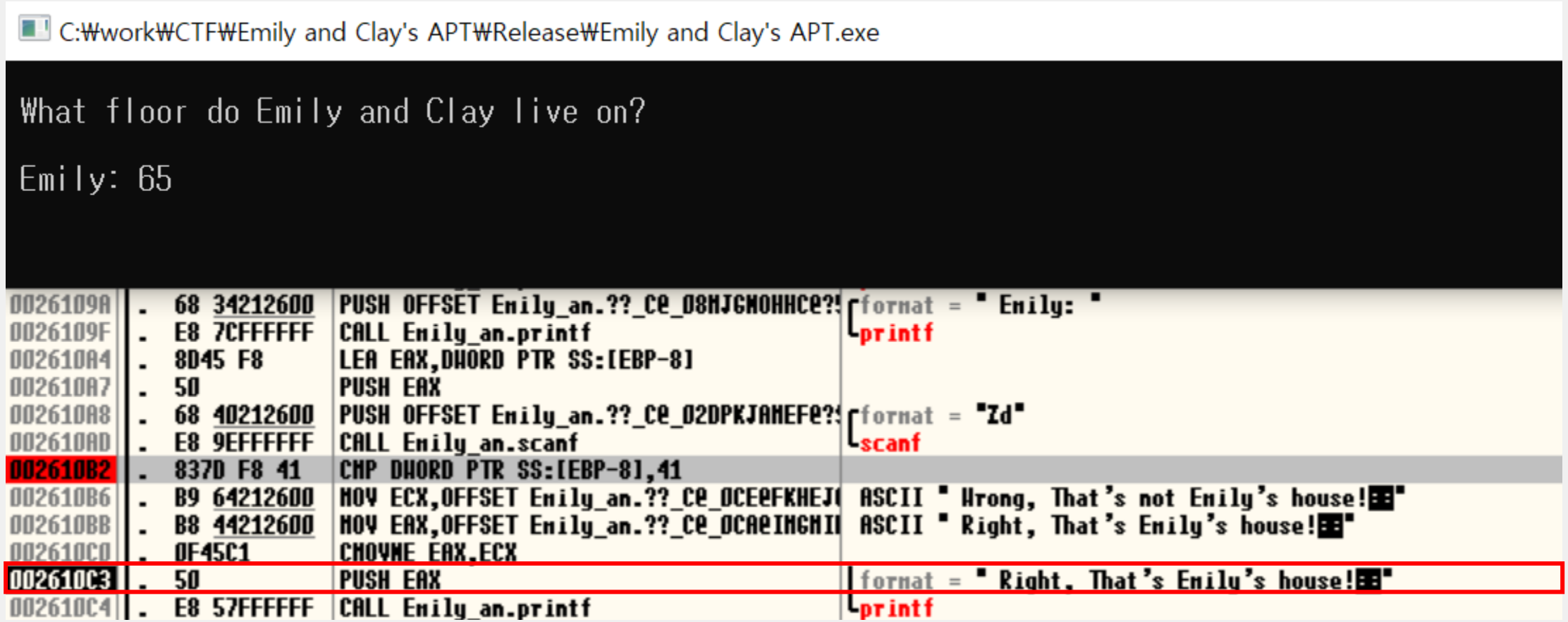
Ex) scpCTF{721524)

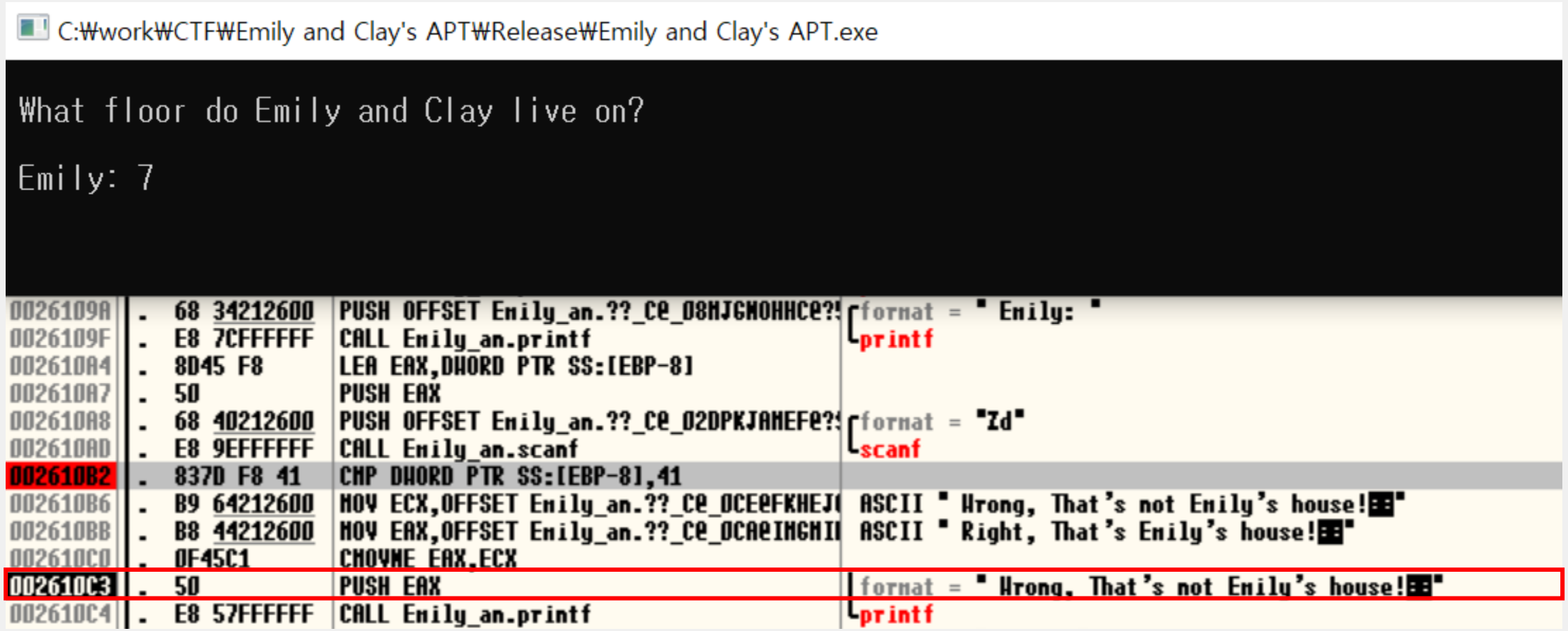

C:₩work₩CTF₩Emily and Clay's APT₩Release₩Emily and Clay's APT.exe
What floor do Emily and Clay live on?
Emily: 29
Wrong, That's not Emily's house!
Clay: 40
Wrong, That's not Clay's house!

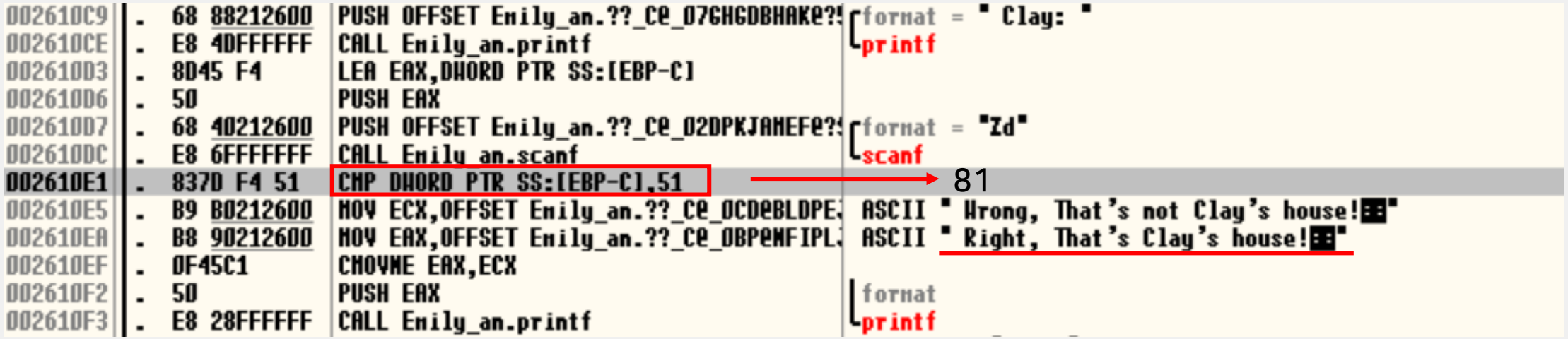

R Text strings referenced in Emily_an:.text
Address
Disassembly
Text string
00261080 PUSH EBP
(Initial CPU selection)
00261090 PUSH OFFSET Emily_an.??_C@_0CK@OKOCKKMB
ASCII "■ What floor do Emily and Clay live on?■■"
0026109A PUSH OFFSET Emily_an.??_C@_08MJGMOHHC@?
ASCII " Emily: "
002610A8 PUSH OFFSET Emily_an.??_C@_02DPKJAMEF@?
ASCII "Zd"
002610B6 MOV ECX,OFFSET Emily_an.??_C@_0CE@FKHEJ
ASCII " Wrong, That's not Emily's house!■■"
002610BB MOV EAX,OFFSET Emily_an.??_C@_0CA@IMGMI
ASCII " Right, That's Emily's house!■■"
002610C9 PUSH OFFSET Emily_an.??_C@_07GHGDBHAK@?
ASCII " Clay: "
002610D7 PUSH OFFSET Emily_an.??_C@_02DPKJAMEF@?
ASCII "Zd"
002610E5 MOV ECX,OFFSET Emily_an.??_C@_0CD@BLDPE
ASCII " Wrong, That's not Clay's house!■■"
002610EA MOV EAX,OFFSET Emily_an.??_C@_0BP@MFIPL
ASCII " Right, That's Clay's house!■■"

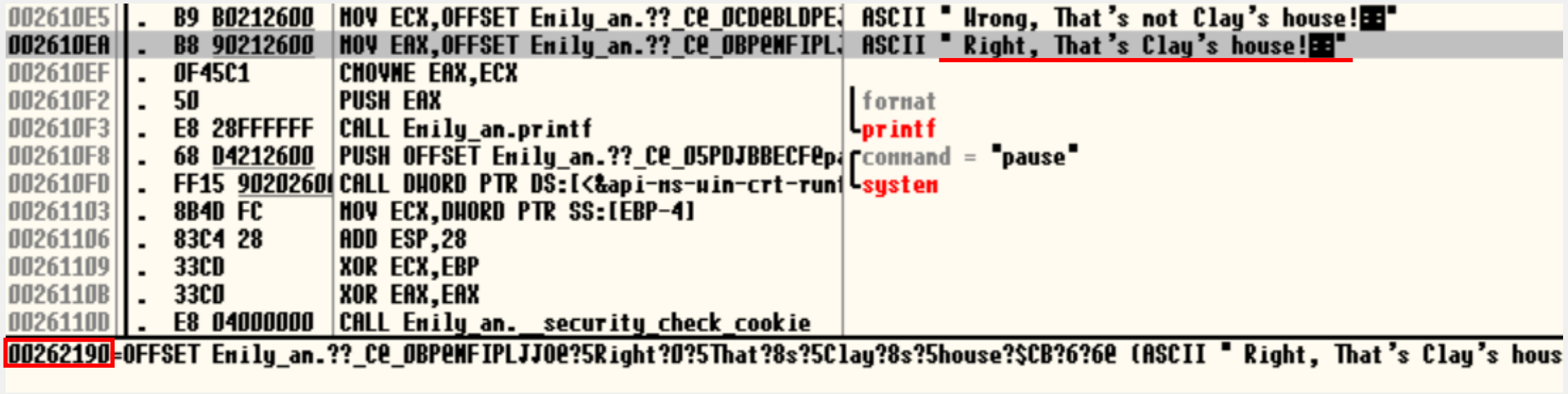

00261080 $ 55 PUSH EBP
00261081 . 8BEC MOV EBP,ESP
00261083 . 83EC 0C SUB ESP,0C
00261086 . A1 04302600 MOV EAX,DWORD PTR DS:[__security_cookie
0026108B . 33C5 XOR EAX,EBP
0026108D . 8945 FC MOV DWORD PTR SS:[EBP-4],EAX
00261090 . 68 08212600 PUSH OFFSET Enily_an.??_C@_0CK@OKOCKKMB
00261095 . E8 86FFFFFF CALL Enily_an.printf
0026109A . 68 34212600 PUSH OFFSET Enily_an.??_C@_08MJGMOHHC@?
0026109F . E8 7CFFFFFF CALL Enily_an.printf
002610A4 . 8D45 F8 LEA EAX,DWORD PTR SS:[EBP-8]
002610A7 . 50 PUSH EAX
002610A8 . 68 40212600 PUSH OFFSET Enily_an.??_C@_02DPKJAMEF@?
002610AD . E8 9EFFFFFF CALL Enily_an.scanf
002610B2 . 837D F8 41 CMP DWORD PTR SS:[EBP-8],41
002610B6 . B9 64212600 MOV ECX,OFFSET Enily_an.??_C@_0CE@FKHEJ
002610BB . B8 44212600 MOV EAX,OFFSET Enily_an.??_C@_0CA@IMGMI
002610C0 . 0F45C1 CMOVNE EAX,ECX
002610C3 . 50 PUSH EAX
002610C4 . E8 57FFFFFF CALL Enily_an.printf
format = "■ What floor do Enily and Clay live on?■■"
printf
format = " Enily: "
printf
format = "%d"
scanf
65
ASCII " Wrong, That's not Enily's house!■■"
ASCII " Right, That's Enily's house!■■"
format
printf


00261080 $ 55 PUSH EBP
00261081 . 8BEC MOV EBP,ESP
00261083 . 83EC 0C SUB ESP,0C
00261086 . A1 04302600 MOV EAX,DWORD PTR DS:[__security_cookie
0026108B . 33C5 XOR EAX,EBP
0026108D . 8945 FC MOV DWORD PTR SS:[EBP-4],EAX
00261090 . 68 08212600 PUSH OFFSET Enily_an.??_C@_0CK@OKOCKKMB
00261095 . E8 86FFFFFF CALL Enily_an.printf
0026109A . 68 34212600 PUSH OFFSET Enily_an.??_C@_08MJGMOHHC@?
0026109F . E8 7CFFFFFF CALL Enily_an.printf
002610A4 . 8D45 F8 LEA EAX,DWORD PTR SS:[EBP-8]
002610A7 . 50 PUSH EAX
002610A8 . 68 40212600 PUSH OFFSET Enily_an.??_C@_02DPKJAMEF@?
002610AD . E8 9EFFFFFF CALL Enily_an.scanf
002610B2 . 837D F8 41 CMP DWORD PTR SS:[EBP-8],41
002610B6 . B9 64212600 MOV ECX,OFFSET Enily_an.??_C@_0CE@FKHEJ
002610BB . B8 44212600 MOV EAX,OFFSET Enily_an.??_C@_0CA@IMGMI
002610C0 . 0F45C1 CMOVNE EAX,ECX
002610C3 . 50 PUSH EAX
002610C4 . E8 57FFFFFF CALL Enily_an.printf
format = "▪ What floor do Enily and Clay live on?▪▪"
printf
format = " Enily: "
printf
format = "%d"
scanf
ASCII " Wrong, That's not Enily's house!▪▪"
ASCII " Right, That's Enily's house!▪▪"
format
printf


C:₩work₩CTF₩Emily and Clay's APT₩Release₩Emily and Clay's APT.exe
What floor do Emily and Clay live on?
Emily: 65
00261099 . 68 34212600 PUSH OFFSET Emily_an.??_C@_08MJGMOHHC@?
format = " Emily: "
0026109F . E8 7CFFFFFF CALL Emily_an.printf
printf
002610A4 . 8D45 F8 LEA EAX,DWORD PTR SS:[EBP-8]
002610A7 . 50 PUSH EAX
002610A8 . 68 40212600 PUSH OFFSET Emily_an.??_C@_02DPKJAMEF@?
format = "%d"
002610AD . E8 9EFFFFFF CALL Emily_an.scanf
scanf
002610B2 . 837D F8 41 CMP DWORD PTR SS:[EBP-8],41
002610B6 . B9 64212600 MOV ECX,OFFSET Emily_an.??_C@_0CE@FKHEJ
ASCII " Wrong, That's not Emily's house!"
002610BB . B8 44212600 MOV EAX,OFFSET Emily_an.??_C@_0CA@IMGMI
ASCII " Right, That's Emily's house!"
002610C0 . 0F45C1 CMOVNE EAX,ECX
002610C3 . 50 PUSH EAX
format = " Right, That's Emily's house!"
002610C4 . E8 57FFFFFF CALL Emily_an.printf
printf


C:₩work₩CTF₩Emily and Clay's APT₩Release₩Emily and Clay's APT.exe
What floor do Emily and Clay live on?
Emily: 7
00261099 . 68 34212600 PUSH OFFSET Enily_an.??_C@_08MJGMOHHC@?
format = " Emily: "
0026109F . E8 7CFFFFFF CALL Enily_an.printf
printf
002610A4 . 8D45 F8 LEA EAX,DWORD PTR SS:[EBP-8]
002610A7 . 50 PUSH EAX
002610A8 . 68 40212600 PUSH OFFSET Enily_an.??_C@_02DPKJAMEF@?
format = "%d"
002610AD . E8 9EFFFFFF CALL Enily_an.scanf
scanf
002610B2 . 837D F8 41 CMP DWORD PTR SS:[EBP-8],41
002610B6 . B9 64212600 MOV ECX,OFFSET Enily_an.??_C@_0CE@FKHEJ
ASCII " Wrong, That's not Enily's house!"
002610BB . B8 44212600 MOV EAX,OFFSET Enily_an.??_C@_0CA@IMGMI
ASCII " Right, That's Enily's house!"
002610C0 . 0F45C1 CMOVNE EAX,ECX
002610C3 . 50 PUSH EAX
format = " Wrong, That's not Enily's house!"
002610C4 . E8 57FFFFFF CALL Enily_an.printf
printf

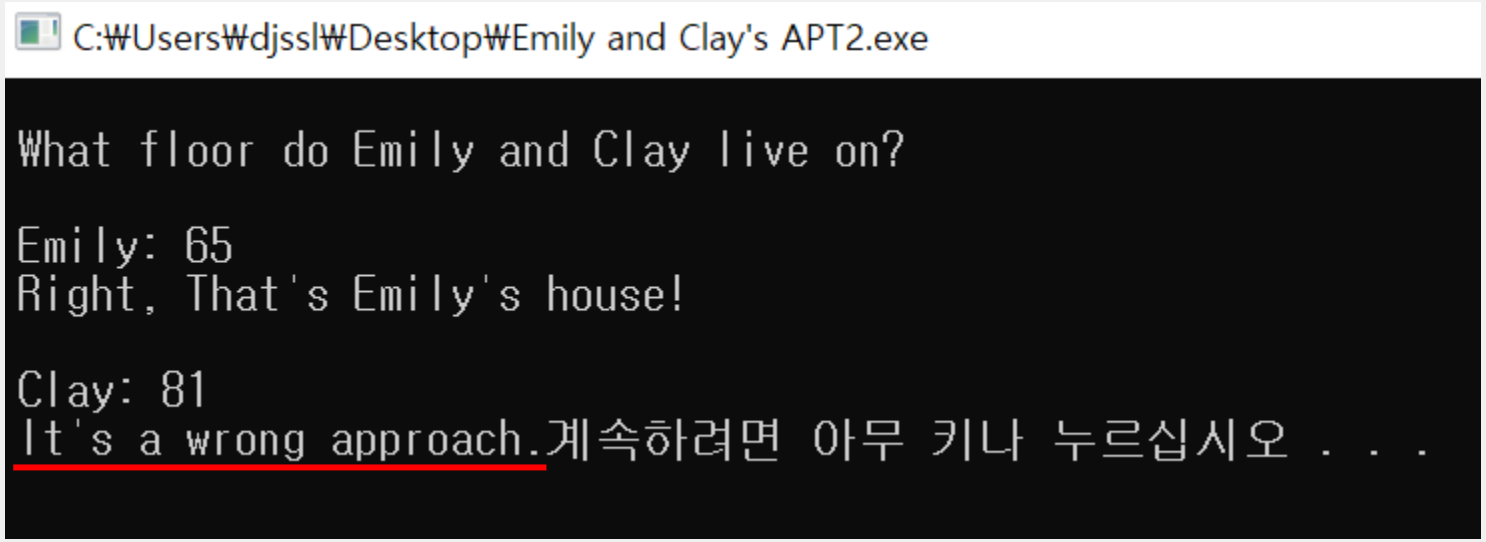

00261DC9 . 68 88212600 PUSH OFFSET Enily_an.??_C@_07GHGDBHAK@?
00261DCE . E8 4DFFFFFF CALL Enily_an.printf
00261DD3 . 8D45 F4 LEA EAX,DWORD PTR SS:[EBP-C]
00261DD6 . 50 PUSH EAX
00261DD7 . 68 40212600 PUSH OFFSET Enily_an.??_C@_02DPKJAMEF@?
00261DDC . E8 6FFFFFFF CALL Enily_an.scanf
00261DE1 . 837D F4 51 CMP DWORD PTR SS:[EBP-C],51
00261DE5 . B9 B0212600 MOV ECX,OFFSET Enily_an.??_C@_0CD@BLDPE
00261DEA . B8 90212600 MOV EAX,OFFSET Enily_an.??_C@_0BP@MFIPL
00261DEF . 0F45C1 CMOVNE EAX,ECX
00261DF2 . 50 PUSH EAX
00261DF3 . E8 28FFFFFF CALL Enily_an.printf
format = " Clay: "
printf
format = "%d"
scanf
81
ASCII " Wrong, That's not Clay's house!"
ASCII " Right, That's Clay's house!"
format
printf

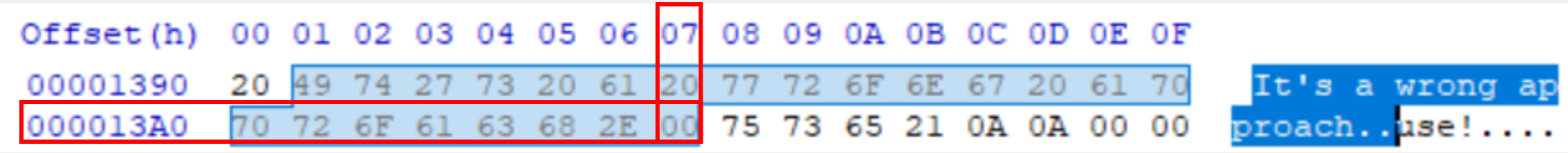

00261DE5 . B9 B0212600 MOV ECX,OFFSET Emily_an.??_C@_0CD@BLDPE ASCII " Wrong, That's not Clay's house!"
00261DEA . B8 90212600 MOV EAX,OFFSET Emily_an.??_C@_0BP@MFIPL ASCII " Right, That's Clay's house!"
00261DEF . 0F45C1 CMOVNE EAX,ECX
00261DF2 . 50 PUSH EAX
00261DF3 . E8 28FFFFFF CALL Emily_an.printf
00261DF8 . 68 D4212600 PUSH OFFSET Emily_an.??_C@_05PDJBBECF@pa
00261DFD . FF15 90202600 CALL DWORD PTR DS:[<&api-ms-win-crt-runt
00261E03 . 8B4D FC MOV ECX,DWORD PTR SS:[EBP-4]
00261E06 . 83C4 28 ADD ESP,28
00261E09 . 33CD XOR ECX,EBP
00261E0B . 33C0 XOR EAX,EAX
00261E0D . E8 04000000 CALL Emily_an.__security_check_cookie
format
printf
command = "pause"
system
00262190=OFFSET Emily_an.??_C@_0BP@MFIPLJJ0@?5Right?D?5That?8s?5Clay?8s?5house?$CB?6?6@ (ASCII " Right, That's Clay's hous

Address	Hex dump	ASCII
00262190	20 52 69 67 68 74 2C 20 54 68 61 74 27 73 20 43	Right, That's C
002621A0	6C 61 79 27 73 20 68 6F 75 73 65 21 0A 0A 00 00	lay's house!....
002621B0	20 57 72 6F 6E 67 2C 20 54 68 61 74 27 73 20 6E	Wrong, That's n
002621C0	6F 74 20 43 6C 61 79 27 73 20 68 6F 75 73 65 21	ot Clay's house!

```
00001370  27 73 20 6E 6F 74 20 45 6D 69 6C 79 27 73 20 68  's not Emily's h
00001380  6F 75 73 65 21 0A 0A 00 20 43 6C 61 79 3A 20 00  ouse!... Clay: .
00001390  20 52 69 67 68 74 2C 20 54 68 61 74 27 73 20 43   Right, That's C
000013A0  6C 61 79 27 73 20 68 6F 75 73 65 21 0A 0A 00 00  lay's house!....
000013B0  20 57 72 6F 6E 67 2C 20 54 68 61 74 27 73 20 6E   Wrong, That's n
000013C0  6F 74 20 43 6C 61 79 27 73 20 68 6F 75 73 65 21  ot Clay's house!
```

```
00001370  27 73 20 6E 6F 74 20 45 6D 69 6C 79 27 73 20 68  's not Emily's h
00001380  6F 75 73 65 21 0A 0A 00 20 43 6C 61 79 3A 20 00  ouse!... Clay: .
00001390  20 49 74 27 73 20 61 20 77 72 6F 6E 67 20 61 70   It's a wrong ap
000013A0  70 72 6F 61 63 68 2E 00 75 73 65 21 0A 0A 00 00  proach..use!....
000013B0  20 57 72 6F 6E 67 2C 20 54 68 61 74 27 73 20 6E   Wrong, That's n
000013C0  6F 74 20 43 6C 61 79 27 73 20 68 6F 75 73 65 21  ot Clay's house!
```


C:₩Users₩djssl₩Desktop₩Emily and Clay's APT2.exe
What floor do Emily and Clay live on?
Emily: 65
Right, That's Emily's house!
Clay: 81
It's a wrong approach.계속하려면 아무 키나 누르십시오 . . .



scpCTF{6513A7}

감사합니다 !