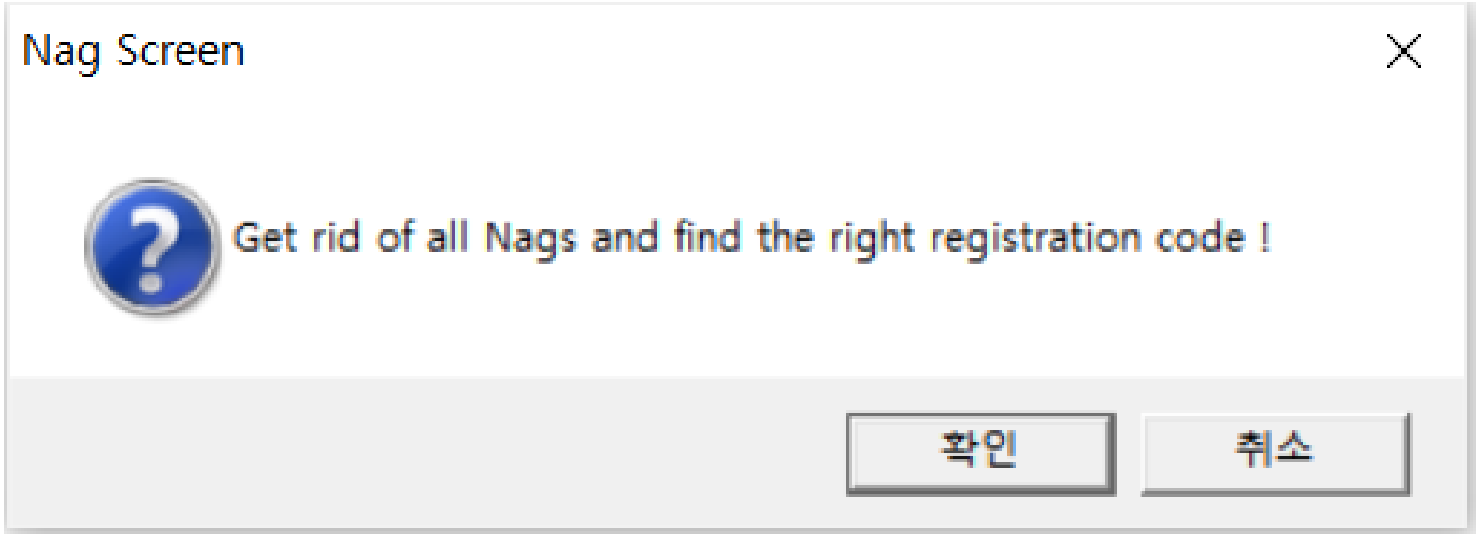
Lena’s Reversing for Newbies

SCP 20학번 박준형

목차 table of contents

프로그램 목표 찾기

Part 1 프로그램 목표찾기

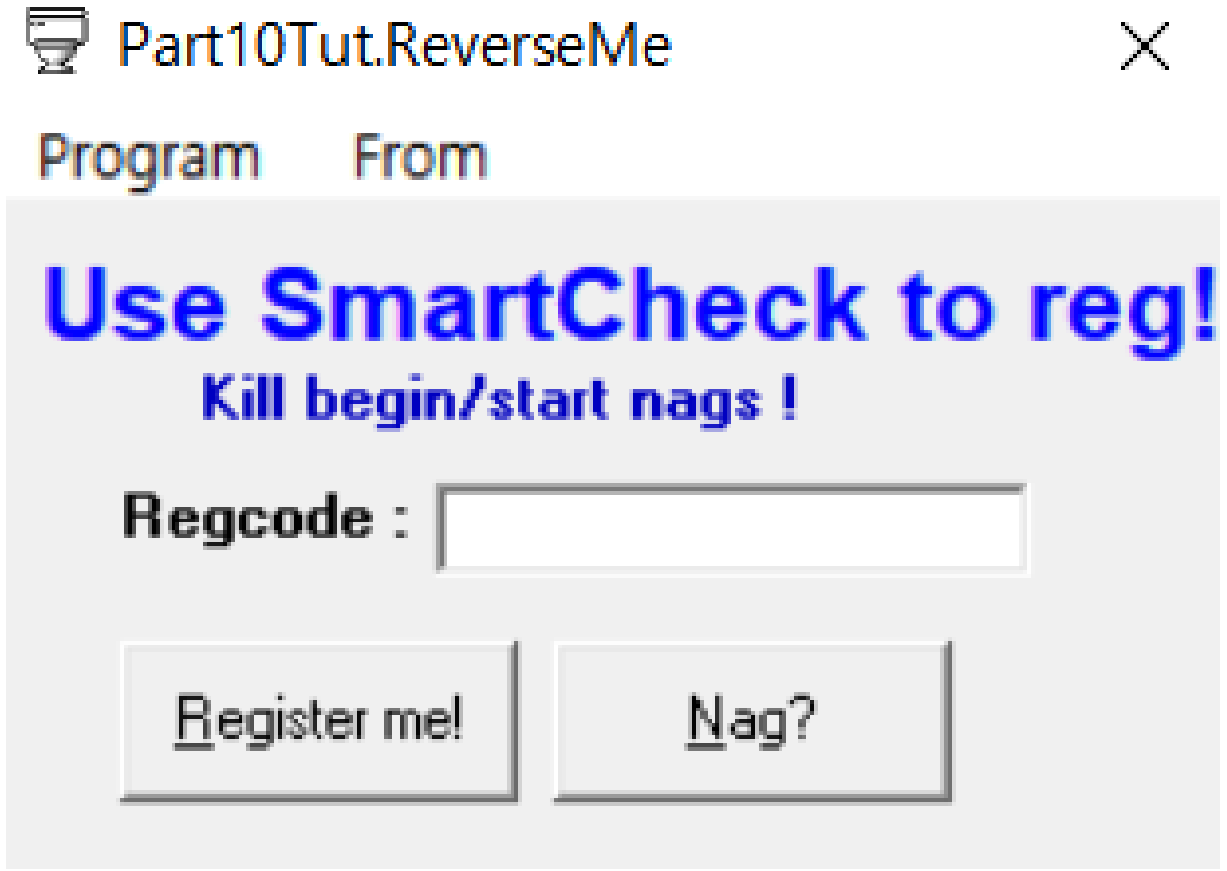


(목표)

•모든 성가신 Nags(잔소리)를 없애라

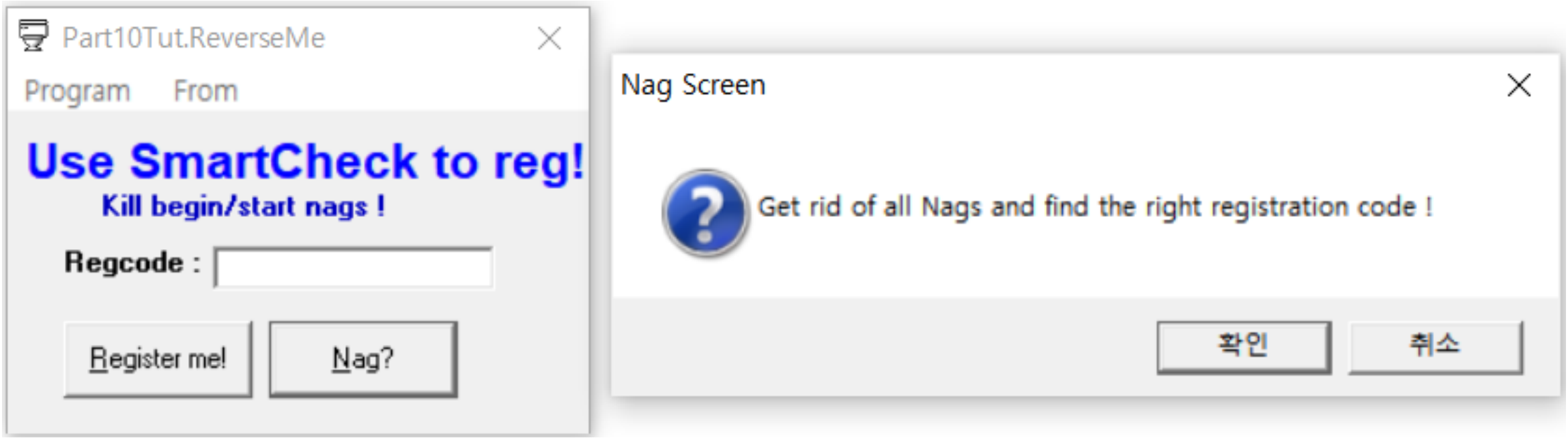
•registration code(등록 코드)를 찾아라

Part 1 프로그램 목표 찾기



목표(1) - 메시지 박스 제거

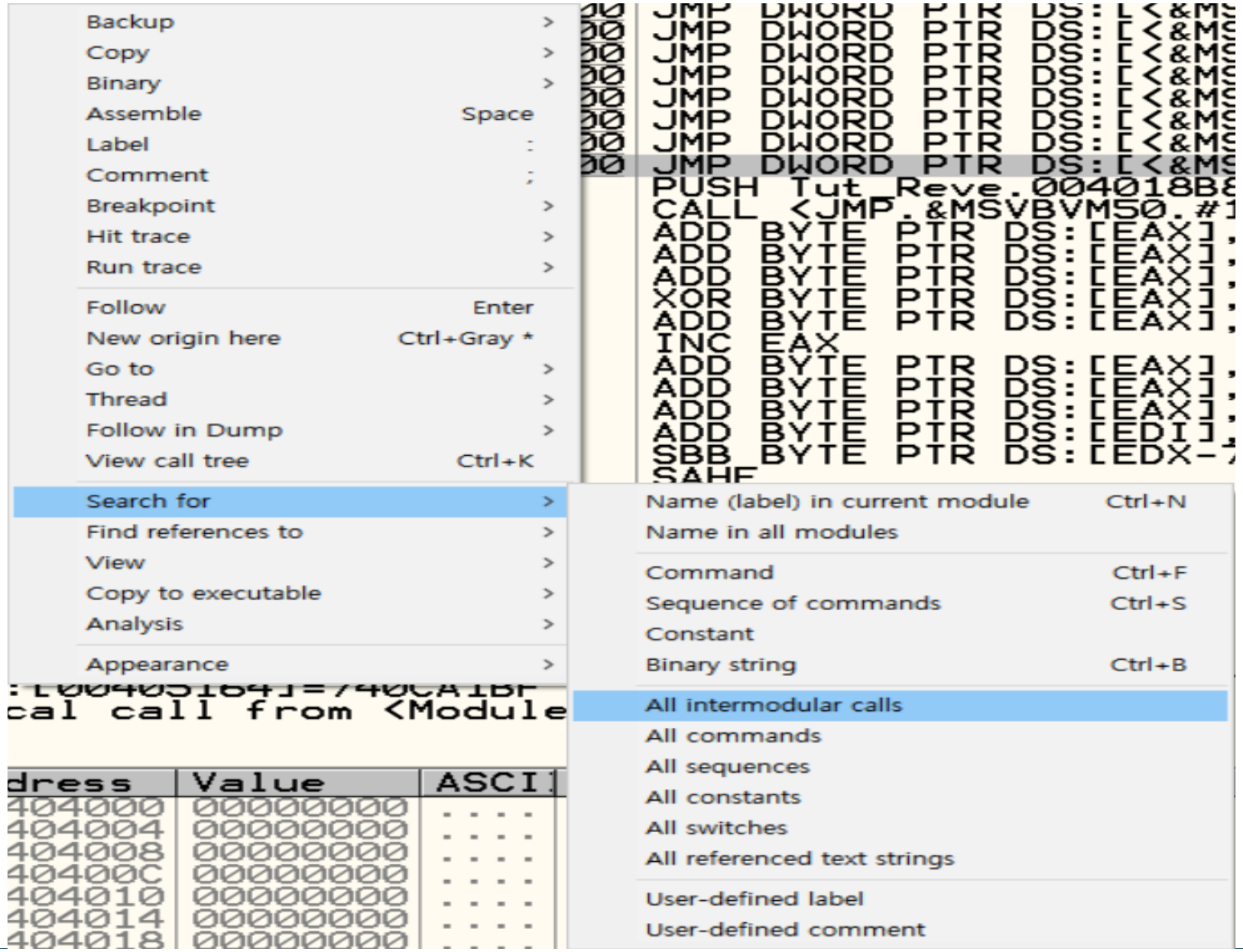
Part 2 목표(1) - 메시지 박스 제거



Part 2 목표(1) - 메시지 박스 제거

```
00401138   $-FF25 84514000  JMP DWORD PTR DS:[<&MSVBVM50.__vbaFreeSt  MSVBVM50.__vbaFreeStr
0040113E   $-FF25 FC504000  JMP DWORD PTR DS:[<&MSVBVM50.__vbaHresu  MSVBVM50.__vbaHresultCheckObj
00401144   $-FF25 08514000  JMP DWORD PTR DS:[<&MSVBVM50.__vbaObjSet  MSVBVM50.__vbaObjSet
0040114A   $-FF25 24514000  JMP DWORD PTR DS:[<&MSVBVM50.__vbaStrCmp  MSVBVM50.__vbaStrCmp
00401150   .-FF25 3C514000  JMP DWORD PTR DS:[<&MSVBVM50.EVENT_SINK_  MSVBVM50.EVENT_SINK_QueryInterface
00401156   .-FF25 20514000  JMP DWORD PTR DS:[<&MSVBVM50.EVENT_SINK_  MSVBVM50.EVENT_SINK_AddRef
0040115C   .-FF25 34514000  JMP DWORD PTR DS:[<&MSVBVM50.EVENT_SINK_  MSVBVM50.EVENT_SINK_Release
00401162   $-FF25 64514000  JMP DWORD PTR DS:[<&MSVBVM50.#100>]       MSVBVM50.ThunRTMain
00401168  ┌$  68 B8184000   PUSH Tut_Reve.004018B8
0040116D  │.  E8 F0FFFFFF   CALL <JMP.&MSVBVM50.#100>
00401172  │.  0000          ADD BYTE PTR DS:[EAX],AL
00401174  │.  0000          ADD BYTE PTR DS:[EAX],AL
00401176  │.  0000          ADD BYTE PTR DS:[EAX],AL
00401178  │.  3000          XOR BYTE PTR DS:[EAX],AL
0040117A  │.  0000          ADD BYTE PTR DS:[EAX],AL
0040117C  │.  40            INC EAX
0040117D  │.  0000          ADD BYTE PTR DS:[EAX],AL
0040117F  │.  0000          ADD BYTE PTR DS:[EAX],AL
00401181  │.  0000          ADD BYTE PTR DS:[EAX],AL
00401183  │.  003F          ADD BYTE PTR DS:[EDI],BH
00401185  │.  186A 8B       SBB BYTE PTR DS:[EDX-75],CH
00401188  │.  9E            SAHF
00401189  └.  C3            RETN
0040118A      D2            DB D2
0040118B      11            DB 11
0040118C      80            DB 80
0040118D      E1            DB E1
0040118E      00            DB 00
0040118F      80            DB 80
00401190      48            DB 48                                   CHAR 'H'
```

Part 2 목표(1) - 메시지 박스 제거

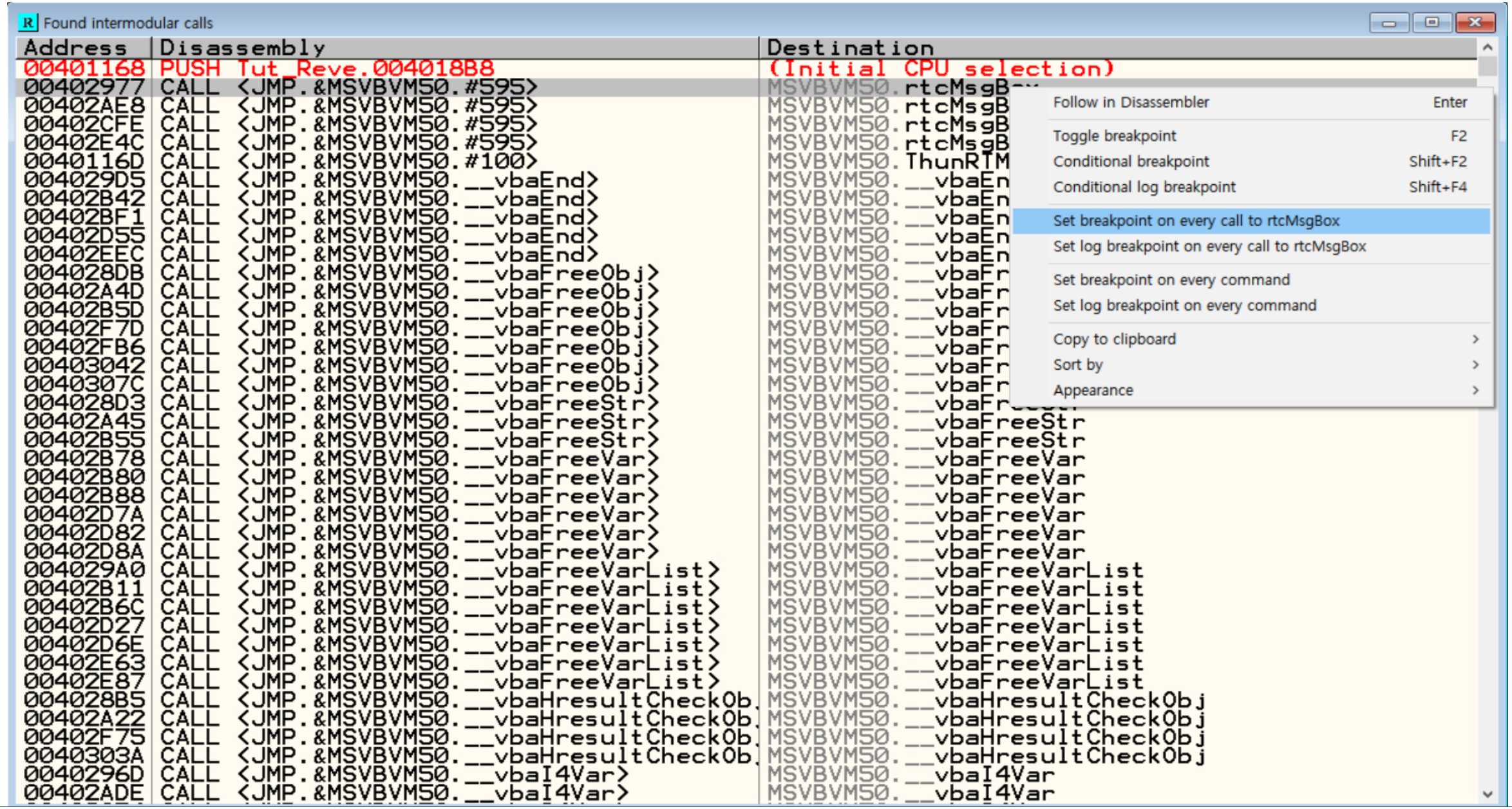


Part 2 목표(1) - 메시지 박스 제거

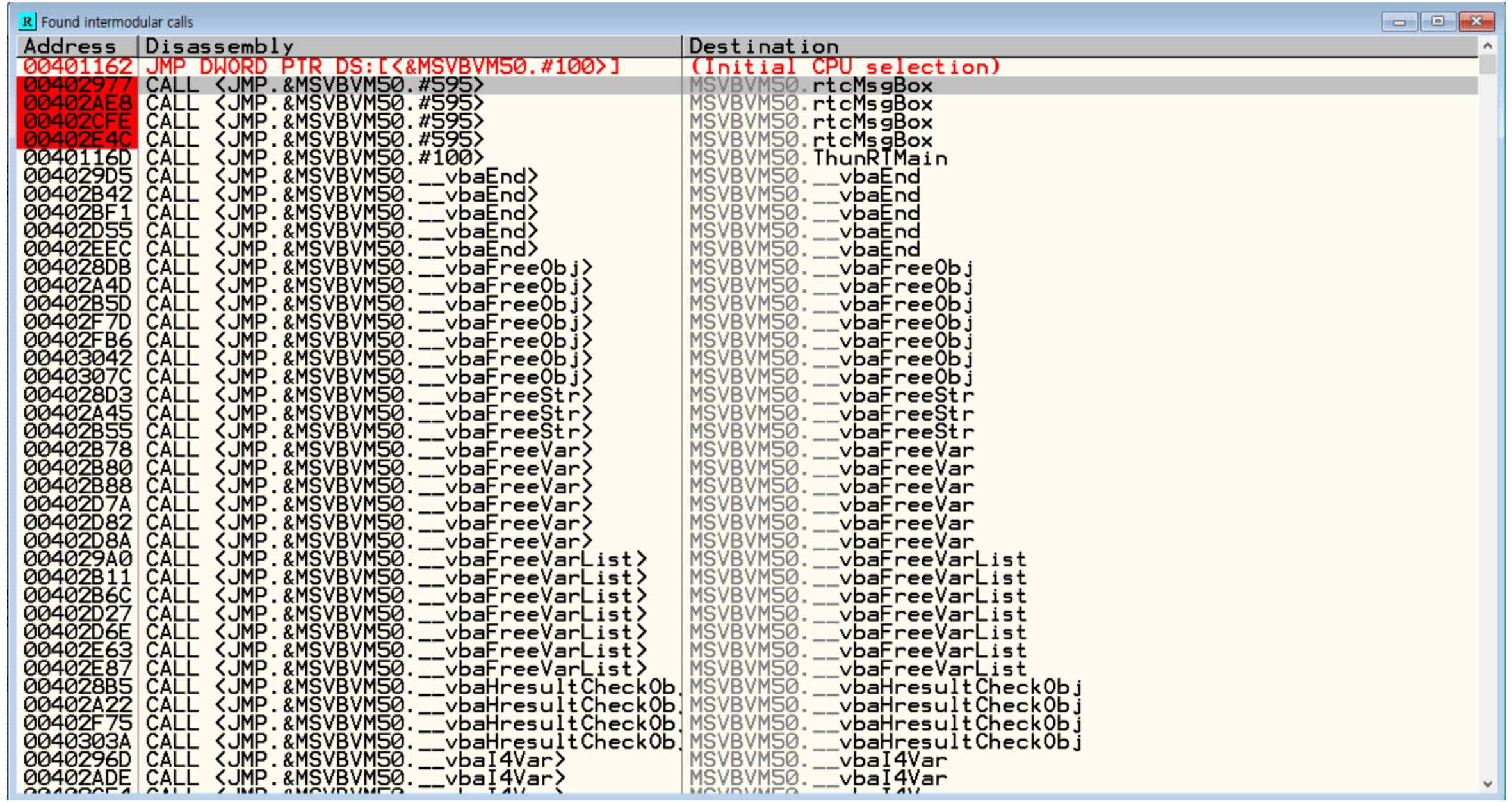
Found intermodular calls

Address	Disassembly	Destination
00401162	JMP DWORD PTR DS:[<&MSVBVM50.#100>]	(Initial CPU selection)
00402977	CALL <JMP.&MSVBVM50.#595>	MSVBVM50.rtcMsgBox
00402AE8	CALL <JMP.&MSVBVM50.#595>	MSVBVM50.rtcMsgBox
00402CFE	CALL <JMP.&MSVBVM50.#595>	MSVBVM50.rtcMsgBox
00402E4C	CALL <JMP.&MSVBVM50.#595>	MSVBVM50.rtcMsgBox
00401160	CALL <JMP.&MSVBVM50.#100>	MSVBVM50.ThunRTMain
004029D5	CALL <JMP.&MSVBVM50.__vbaEnd>	MSVBVM50.__vbaEnd
00402B42	CALL <JMP.&MSVBVM50.__vbaEnd>	MSVBVM50.__vbaEnd
00402BF1	CALL <JMP.&MSVBVM50.__vbaEnd>	MSVBVM50.__vbaEnd
00402D55	CALL <JMP.&MSVBVM50.__vbaEnd>	MSVBVM50.__vbaEnd
00402EEC	CALL <JMP.&MSVBVM50.__vbaEnd>	MSVBVM50.__vbaEnd
004028DB	CALL <JMP.&MSVBVM50.__vbaFreeObj>	MSVBVM50.__vbaFreeObj
00402A4D	CALL <JMP.&MSVBVM50.__vbaFreeObj>	MSVBVM50.__vbaFreeObj
00402B5D	CALL <JMP.&MSVBVM50.__vbaFreeObj>	MSVBVM50.__vbaFreeObj
00402F7D	CALL <JMP.&MSVBVM50.__vbaFreeObj>	MSVBVM50.__vbaFreeObj
00402FB6	CALL <JMP.&MSVBVM50.__vbaFreeObj>	MSVBVM50.__vbaFreeObj
00403042	CALL <JMP.&MSVBVM50.__vbaFreeObj>	MSVBVM50.__vbaFreeObj
0040307C	CALL <JMP.&MSVBVM50.__vbaFreeObj>	MSVBVM50.__vbaFreeObj
004028D3	CALL <JMP.&MSVBVM50.__vbaFreeStr>	MSVBVM50.__vbaFreeStr
00402A45	CALL <JMP.&MSVBVM50.__vbaFreeStr>	MSVBVM50.__vbaFreeStr
00402B55	CALL <JMP.&MSVBVM50.__vbaFreeStr>	MSVBVM50.__vbaFreeStr
00402B78	CALL <JMP.&MSVBVM50.__vbaFreeVar>	MSVBVM50.__vbaFreeVar
00402B80	CALL <JMP.&MSVBVM50.__vbaFreeVar>	MSVBVM50.__vbaFreeVar
00402B88	CALL <JMP.&MSVBVM50.__vbaFreeVar>	MSVBVM50.__vbaFreeVar
00402D7A	CALL <JMP.&MSVBVM50.__vbaFreeVar>	MSVBVM50.__vbaFreeVar
00402D82	CALL <JMP.&MSVBVM50.__vbaFreeVar>	MSVBVM50.__vbaFreeVar
00402D8A	CALL <JMP.&MSVBVM50.__vbaFreeVar>	MSVBVM50.__vbaFreeVar
004029A0	CALL <JMP.&MSVBVM50.__vbaFreeVarList>	MSVBVM50.__vbaFreeVarList
00402B11	CALL <JMP.&MSVBVM50.__vbaFreeVarList>	MSVBVM50.__vbaFreeVarList
00402B6C	CALL <JMP.&MSVBVM50.__vbaFreeVarList>	MSVBVM50.__vbaFreeVarList
00402D27	CALL <JMP.&MSVBVM50.__vbaFreeVarList>	MSVBVM50.__vbaFreeVarList
00402D6E	CALL <JMP.&MSVBVM50.__vbaFreeVarList>	MSVBVM50.__vbaFreeVarList
00402E63	CALL <JMP.&MSVBVM50.__vbaFreeVarList>	MSVBVM50.__vbaFreeVarList
00402E87	CALL <JMP.&MSVBVM50.__vbaFreeVarList>	MSVBVM50.__vbaFreeVarList
004028B5	CALL <JMP.&MSVBVM50.__vbaHresultCheckOb	MSVBVM50.__vbaHresultCheckObj
00402A22	CALL <JMP.&MSVBVM50.__vbaHresultCheckOb	MSVBVM50.__vbaHresultCheckObj
00402F75	CALL <JMP.&MSVBVM50.__vbaHresultCheckOb	MSVBVM50.__vbaHresultCheckObj
0040303A	CALL <JMP.&MSVBVM50.__vbaHresultCheckOb	MSVBVM50.__vbaHresultCheckObj
0040296D	CALL <JMP.&MSVBVM50.__vbaI4Var>	MSVBVM50.__vbaI4Var
00402ADE	CALL <JMP.&MSVBVM50.__vbaI4Var>	MSVBVM50.__vbaI4Var

Part 2 목표(1) - 메시지 박스 제거



Part 2 목표(1) - 메시지 박스 제거

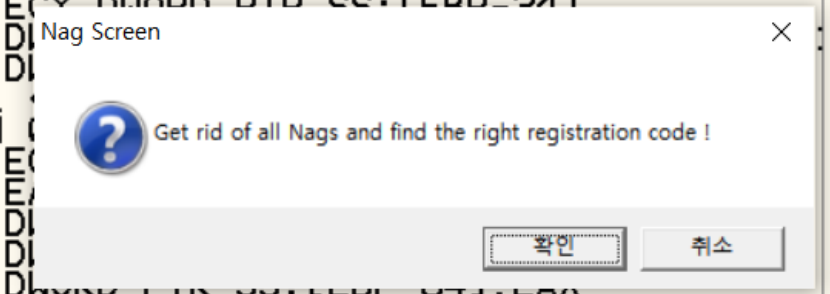


Part 2 목표(1) - 메시지 박스 제거

```
00402C7C   . 8975 8C        MOV DWORD PTR SS:[EBP-74],ESI
00402C7F   . 89B5 5CFFFFFF  MOV DWORD PTR SS:[EBP-A4],ESI
00402C85   . C745 84 F01E40 MOV DWORD PTR SS:[EBP-7C],Tut_Reve.00401  UNICODE "Get rid of all Nags and find
00402C8C   . 899D 7CFFFFFF  MOV DWORD PTR SS:[EBP-84],EBX
00402C92   . E8 95E4FFFF    CALL <JMP.&MSVBVM50.__vbaVarCopy>
00402C97   . 6A 03          PUSH 3
00402C99   . 8D95 7CFFFFFF  LEA EDX,DWORD PTR SS:[EBP-84]
00402C9F   . 5F             POP EDI
00402CA0   . 8D4D DC        LEA ECX,DWORD PTR SS:[EBP-24]
00402CA3   . C745 84 210000 MOV DWORD PTR SS:[EBP-7C],21
00402CAA   . 89BD 7CFFFFFF  MOV DWORD PTR SS:[EBP-84],EDI
00402CB0   . E8 71E4FFFF    CALL <JMP.&MSVBVM50.__vbaVarMove>
00402CB5   . 8D95 7CFFFFFF  LEA EDX,DWORD PTR SS:[EBP-84]
00402CBB   . 8D4D CC        LEA ECX,DWORD PTR SS:[EBP-34]
00402CBE   . C745 84 781F40 MOV DWORD PTR SS:[EBP-7C],Tut_Reve.00401  UNICODE "Nag Screen "
00402CC5   . 899D 7CFFFFFF  MOV DWORD PTR SS:[EBP-84],EBX
00402CCB   . E8 5CE4FFFF    CALL <JMP.&MSVBVM50.__vbaVarCopy>
00402CD0   . 6A 0A          PUSH 0A
00402CD2   . B9 04000280    MOV ECX,80020004
00402CD7   . 58             POP EAX
00402CD8   . 894D 94        MOV DWORD PTR SS:[EBP-6C],ECX
00402CDB   . 8945 8C        MOV DWORD PTR SS:[EBP-74],EAX
00402CDE   . 8945 9C        MOV DWORD PTR SS:[EBP-64],EAX
00402CE1   . 8D45 8C        LEA EAX,DWORD PTR SS:[EBP-74]
00402CE4   . 894D A4        MOV DWORD PTR SS:[EBP-5C],ECX
00402CE7   . 50             PUSH EAX
00402CE8   . 8D45 9C        LEA EAX,DWORD PTR SS:[EBP-64]
00402CEB   . 50             PUSH EAX
00402CEC   . 8D45 CC        LEA EAX,DWORD PTR SS:[EBP-34]
00402CEF   . 50             PUSH EAX
00402CF0   . 8D45 DC        LEA EAX,DWORD PTR SS:[EBP-24]
00402CF3   . 50             PUSH EAX
00402CF4   . E8 21E4FFFF    CALL <JMP.&MSVBVM50.__vbaI4Var>
00402CF9   . 50             PUSH EAX
00402CFA   . 8D45 AC        LEA EAX,DWORD PTR SS:[EBP-54]
00402CFD   . 50             PUSH EAX
00402CFE   . E8 1DE4FFFF    CALL <JMP.&MSVBVM50.#595>
00402D03   . 8D95 5CFFFFFF  LEA EDX,DWORD PTR SS:[EBP-A4]
00402D09   . 8D4D BC        LEA ECX,DWORD PTR SS:[EBP-44]
00402D0C   . 8985 64FFFFFF  MOV DWORD PTR SS:[EBP-9C],EAX
```

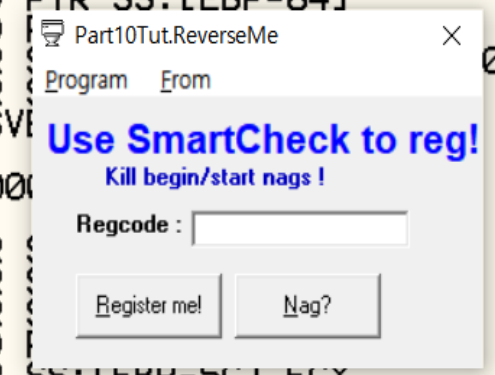
Part 2 목표(1) - 메시지 박스 제거

```
00402C7C   .  8975 8C        MOV DWORD PTR SS:[EBP-74],ESI
00402C7F   .  89B5 5CFFFFFF  MOV DWORD PTR SS:[EBP-A4],ESI
00402C85   .  C745 84 F01E40 MOV DWORD PTR SS:[EBP-7C],Tut_Reve.00401  UNICODE "Get rid of all Nags anc
00402C8C   .  899D 7CFFFFFF  MOV DWORD PTR SS:[EBP-84],EBX
00402C92   .  E8 95E4FFFF    CALL <JMP.&MSVBVM50.__vbaVarCopy>
00402C97   .  6A 03          PUSH 3
00402C99   .  8D95 7CFFFFFF  LEA EDX,DWORD PTR SS:[EBP-84]
00402C9F   .  5F             POP EDI
00402CA0   .  8D4D DC        LEA ECX,DWORD PTR SS:[EBP-24]
00402CA3   .  C745 84 210000 MOV DWORD PTR SS:[EBP-7C],21
00402CAA   .  89BD 7CFFFFFF  MOV DWORD PTR SS:[EBP-84],EDI
00402CB0   .  E8 71E4FFFF    CALL <JMP.&MSVBVM50.__vbaVarMove>
00402CB5   .  8D95 7CFFFFFF  LEA EDX,DWORD PTR SS:[EBP-84]
00402CBB   .  8D4D CC        LEA ECX,DWORD PTR SS:[EBP-34]
00402CBE   .  C745 84 781F40 MOV DI                          UNICODE "Nag Screen "
00402CC5   .  899D 7CFFFFFF  MOV DI
00402CCB   .  E8 5CE4FFFF    CALL
00402CD0   .  6A 0A          PUSH
00402CD2   .  B9 04000280    MOV EC
00402CD7   .  58             POP EA
00402CD8   .  894D 94        MOV DI
00402CDB   .  8945 8C        MOV DI
00402CDE   .  8945 9C        MOV DWORD PTR SS:[EBP-64],EAX
00402CE1   .  8D45 8C        LEA EAX,DWORD PTR SS:[EBP-74]
00402CE4   .  894D A4        MOV DWORD PTR SS:[EBP-5C],ECX
00402CE7   .  50             PUSH EAX
00402CE8   .  8D45 9C        LEA EAX,DWORD PTR SS:[EBP-64]
00402CEB   .  50             PUSH EAX
00402CEC   .  8D45 CC        LEA EAX,DWORD PTR SS:[EBP-34]
00402CEF   .  50             PUSH EAX
00402CF0   .  8D45 DC        LEA EAX,DWORD PTR SS:[EBP-24]
00402CF3   .  50             PUSH EAX
00402CF4   .  E8 21E4FFFF    CALL <JMP.&MSVBVM50.__vbaI4Var>
00402CF9   .  50             PUSH EAX
00402CFA   .  8D45 AC        LEA EAX,DWORD PTR SS:[EBP-54]
00402CFD   .  50             PUSH EAX
00402CFE   .  E8 1DE4FFFF    CALL <JMP.&MSVBVM50.#595>
00402D03   .  8D95 5CFFFFFF  LEA EDX,DWORD PTR SS:[EBP-A4]
00402D09   .  8D4D BC        LEA ECX,DWORD PTR SS:[EBP-44]
00402D0C   .  8985 64FFFFFF  MOV DWORD PTR SS:[EBP-9C],EAX
```



Part 2 목표(1) - 메시지 박스 제거

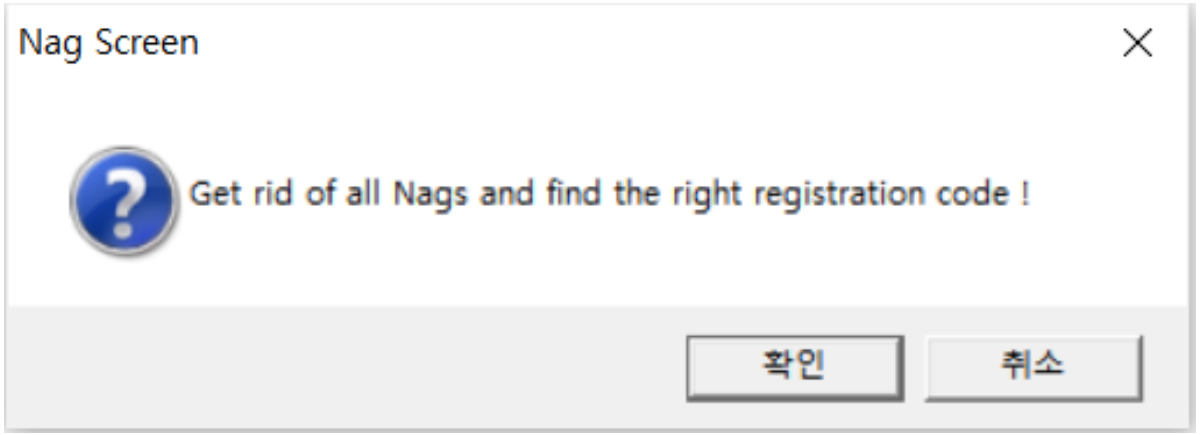
```
00402C7C   . 8975 8C        MOV DWORD PTR SS:[EBP-74],ESI
00402C7F   . 89B5 5CFFFFFF  MOV DWORD PTR SS:[EBP-A4],ESI
00402C85   . C745 84 F01E40 MOV DWORD PTR SS:[EBP-7C],Tut_Reve.00401  UNICODE "Get rid of all Nags and find
00402C8C   . 899D 7CFFFFFF  MOV DWORD PTR SS:[EBP-84],EBX
00402C92   . E8 95E4FFFF    CALL <JMP.&MSVBVM50.__vbaVarCopy>
00402C97   . 6A 03          PUSH 3
00402C99   . 8D95 7CFFFFFF  LEA EDX,DWORD PTR SS:[EBP-84]
00402C9F   . 5F             POP EDI
00402CA0   . 8D4D DC        LEA ECX,DWORD PTR SS:[EBP-24]
00402CA3   . C745 84 210000 MOV DWORD PTR SS:[EBP-7C],21
00402CAA   . 89BD 7CFFFFFF  MOV DWORD PTR SS:[EBP-84],EDI
00402CB0   . E8 71E4FFFF    CALL <JMP.&MSVBVM50.__vbaVarMove>
00402CB5   . 8D95 7CFFFFFF  LEA EDX,DWORD PTR SS:[EBP-84]
00402CBB   . 8D4D CC        LEA ECX,DWORD P
00402CBE   . C745 84 781F40 MOV DWORD PTR S                    0040  UNICODE "Nag Screen "
00402CC5   . 899D 7CFFFFFF  MOV DWORD PTR S
00402CCB   . E8 5CE4FFFF    CALL <JMP.&MSVB
00402CD0   . 6A 0A          PUSH 0A
00402CD2   . B9 04000280    MOV ECX,8002000
00402CD7   . 58             POP EAX
00402CD8   . 894D 94        MOV DWORD PTR S
00402CDB   . 8945 8C        MOV DWORD PTR S
00402CDE   . 8945 9C        MOV DWORD PTR S
00402CE1   . 8D45 8C        LEA EAX,DWORD P
00402CE4   . 894D A4        MOV DWORD PTR SS:[EBP-5C],ECX
00402CE7   . 50             PUSH EAX
00402CE8   . 8D45 9C        LEA EAX,DWORD PTR SS:[EBP-64]
00402CEB   . 50             PUSH EAX
00402CEC   . 8D45 CC        LEA EAX,DWORD PTR SS:[EBP-34]
00402CEF   . 50             PUSH EAX
00402CF0   . 8D45 DC        LEA EAX,DWORD PTR SS:[EBP-24]
00402CF3   . 50             PUSH EAX
00402CF4   . E8 21E4FFFF    CALL <JMP.&MSVBVM50.__vbaI4Var>
00402CF9   . 50             PUSH EAX
00402CFA   . 8D45 AC        LEA EAX,DWORD PTR SS:[EBP-54]
00402CFD   . 50             PUSH EAX
00402CFE   . E8 1DE4FFFF    CALL <JMP.&MSVBVM50.#595>
00402D03   . 8D95 5CFFFFFF  LEA EDX,DWORD PTR SS:[EBP-A4]
00402D09   . 8D4D BC        LEA ECX,DWORD PTR SS:[EBP-44]
00402D0C   . 8985 64FFFFFF  MOV DWORD PTR SS:[EBP-9C],EAX
```

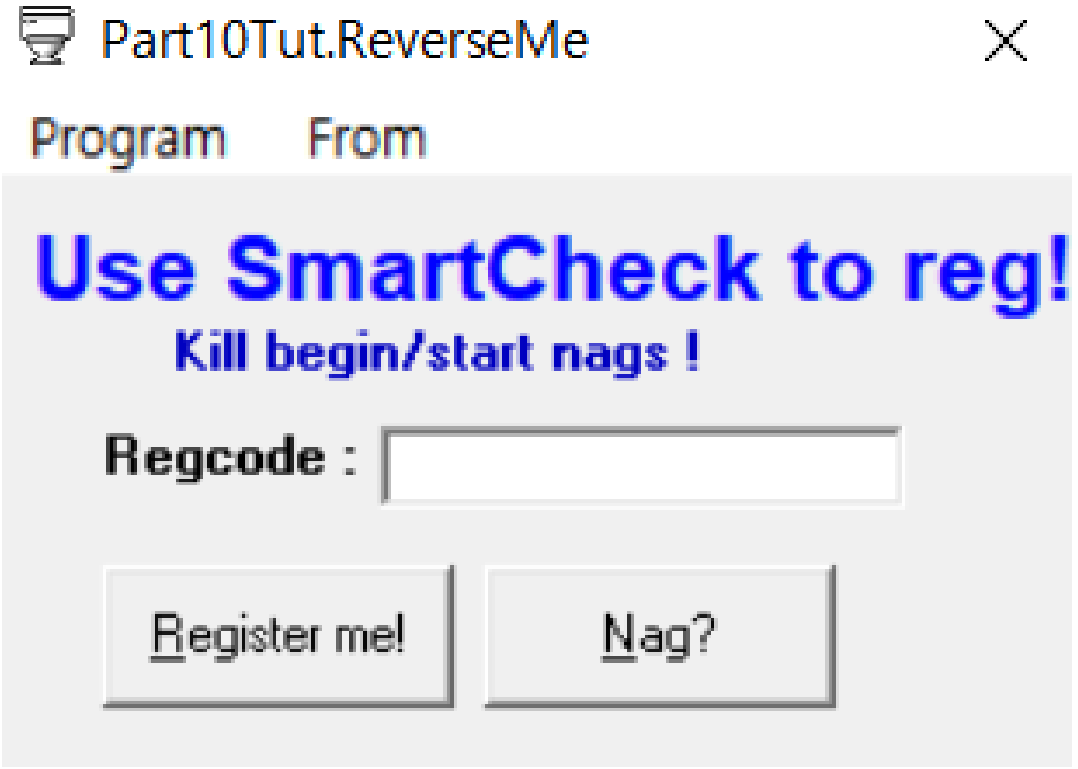


Part 2 목표(1) - 메시지 박스 제거

```
00402CA3  . C745 84 210000 MOV DWORD PTR SS:[EBP-7C],21
00402CAA  . 89BD 7CFFFFFF MOV DWORD PTR SS:[EBP-84],EDI
00402CB0  . E8 71E4FFFF   CALL <JMP.&MSVBVM50.__vbaVarMove>
00402CB5  . 8D95 7CFFFFFF LEA EDX,DWORD PTR SS:[EBP-84]
00402CBB  . 8D4D CC       LEA ECX,DWORD PTR SS:[EBP-34]
00402CBE  . C745 84 781F40 MOV DWORD PTR SS:[EBP-7C],Tut_Reve.00401  UNICODE "Nag Screen "
00402CC5  . 899D 7CFFFFFF MOV DWORD PTR SS:[EBP-84],EBX
00402CCB  . E8 5CE4FFFF   CALL <JMP.&MSVBVM50.__vbaVarCopy>
00402CD0  . 6A 0A         PUSH 0A
00402CD2  . B9 04000280   MOV ECX,80020004
00402CD7  . 58            POP EAX
00402CD8  . 894D 94       MOV DWORD PTR SS:[EBP-6C],ECX
00402CDB  . 8945 8C       MOV DWORD PTR SS:[EBP-74],EAX
00402CDE  . 8945 9C       MOV DWORD PTR SS:[EBP-64],EAX
00402CE1  . 8D45 8C       LEA EAX,DWORD PTR SS:[EBP-74]
00402CE4  . 894D A4       MOV DWORD PTR SS:[EBP-5C],ECX
00402CE7  . 50            PUSH EAX
00402CE8  . 8D45 9C       LEA EAX,DWORD PTR SS:[EBP-64]
00402CEB  . 50            PUSH EAX
00402CEC  . 8D45 CC       LEA EAX,DWORD PTR SS:[EBP-34]
00402CEF  . 50            PUSH EAX
00402CF0  . 8D45 DC       LEA EAX,DWORD PTR SS:[EBP-24]
00402CF3  . 50            PUSH EAX
00402CF4  . E8 21E4FFFF   CALL <JMP.&MSVBVM50.__vbaI4Var>
00402CF9  . 50            PUSH EAX
00402CFA  . 8D45 AC       LEA EAX,DWORD PTR SS:[EBP-54]
00402CFD  . 50            PUSH EAX
00402CFE  . E8 1DE4FFFF   CALL <JMP.&MSVBVM50.#595>
00402D03  . 8D95 5CFFFFFF LEA EDX,DWORD PTR SS:[EBP-A4]
00402D09  . 8D4D BC       LEA ECX,DWORD PTR SS:[EBP-44]
```

Part 2 목표(1) - 메시지 박스 제거

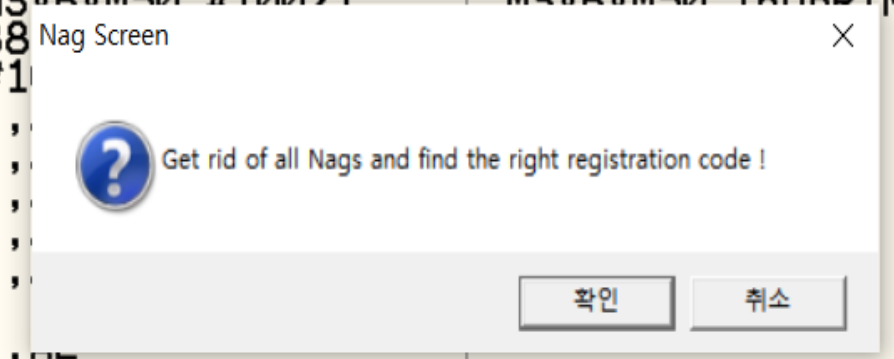




둘 다 같은 코드에서 실행

Part 2 패치(1) - ADD ESP,XXXX 형태로 변경

```
00401120  $-FF25 0C514000 JMP DWORD PTR DS:[<&MSVBVM50.#595>]     MSVBVM50.rtcMsgBox
00401126  $-FF25 E4504000 JMP DWORD PTR DS:[<&MSVBVM50.__vbaVarMov  MSVBVM50.__vbaVarMove
0040112C  $-FF25 70514000 JMP DWORD PTR DS:[<&MSVBVM50.__vbaVarCop  MSVBVM50.__vbaVarCopy
00401132  $-FF25 88514000 JMP DWORD PTR DS:[<&MSVBVM50.__vbaFreeOb  MSVBVM50.__vbaFreeObj
00401138  $-FF25 84514000 JMP DWORD PTR DS:[<&MSVBVM50.__vbaFreeSt  MSVBVM50.__vbaFreeStr
0040113E  $-FF25 FC504000 JMP DWORD PTR DS:[<&MSVBVM50.__vbaHresu  MSVBVM50.__vbaHresultCh
00401144  $-FF25 08514000 JMP DWORD PTR DS:[<&MSVBVM50.__vbaObjSet  MSVBVM50.__vbaObjSet
0040114A  $-FF25 24514000 JMP DWORD PTR DS:[<&MSVBVM50.__vbaStrCmp  MSVBVM50.__vbaStrCmp
00401150  .-FF25 3C514000 JMP DWORD PTR DS:[<&MSVBVM50.EVENT_SINK_  MSVBVM50.EVENT_SINK_Que
00401156  .-FF25 20514000 JMP DWORD PTR DS:[<&MSVBVM50.EVENT_SINK_  MSVBVM50.EVENT_SINK_Add
0040115C  .-FF25 34514000 JMP DWORD PTR DS:[<&MSVBVM50.EVENT_SINK_  MSVBVM50.EVENT_SINK_Re
00401162  $-FF25 64514000 JMP DWORD PTR DS:[<&MSVBVM50.#100>]     MSVBVM50.ThunRTMain
00401168  ┌$ 68 B8184000    PUSH Tut_Reve.004018B8
0040116D  │. E8 F0FFFFFF   CALL <JMP.&MSVBVM50.#1
00401172  │. 0000          ADD BYTE PTR DS:[EAX],
00401174  │. 0000          ADD BYTE PTR DS:[EAX],
00401176  │. 0000          ADD BYTE PTR DS:[EAX],
00401178  │. 3000          XOR BYTE PTR DS:[EAX],
0040117A  │. 0000          ADD BYTE PTR DS:[EAX],
0040117C  │. 40            INC EAX
0040117D  │. 0000          ADD BYTE PTR DS:[EAX],
0040117F  │. 0000          ADD BYTE PTR DS:[EAX],AL
00401181  │. 0000          ADD BYTE PTR DS:[EAX],AL
00401183  │. 003F          ADD BYTE PTR DS:[EDI],BH
00401185  │. 186A 8B       SBB BYTE PTR DS:[EDX-75],CH
00401188  │. 9E            SAHF
00401189  └. C3            RETN
0040118A     D2            DB D2
0040118B     11            DB 11
0040118C     80            DB 80
0040118D     E1            DB E1
0040118E     00            DB 00
0040118F     80            DB 80
```



Part 2 패치(1) - ADD ESP,XXXX 형태로 변경

```
7419410F   33FF              XOR EDI,EDI
74194111   66:397D FC        CMP WORD PTR SS:[EBP-4],DI
74194115   0F84 B6000000     JE MSVBVM50.741941D1
7419411B   66:397D FE        CMP WORD PTR SS:[EBP-2],DI
7419411F   0F84 AC000000     JE MSVBVM50.741941D1
74194125   33C0              XOR EAX,EAX
74194127   897D E8           MOV DWORD PTR SS:[EBP-18],EDI
7419412A   85F6              TEST ESI,ESI
7419412C   75 03            JNZ SHORT MSVBVM50.74194131
7419412E   8D75 FA           LEA ESI,DWORD PTR SS:[EBP-6]
74194131   85DB              TEST EBX,EBX
74194133   75 0A            JNZ SHORT MSVBVM50.7419413F
74194135   66:837D F6 00     CMP WORD PTR SS:[EBP-A],0
7419413A   75 03            JNZ SHORT MSVBVM50.7419413F
7419413C   8D5D FA           LEA EBX,DWORD PTR SS:[EBP-6]
7419413F   6A 01             PUSH 1
74194141   50                PUSH EAX
74194142   57                PUSH EDI
74194143   FF75 0C           PUSH DWORD PTR SS:[EBP+C]
74194146   53                PUSH EBX
74194147   56                PUSH ESI
74194148   E8 A61FFDFF       CALL MSVBVM50.741660F3
7419414D   FF75 EC           PUSH DWORD PTR SS:[EBP-14]
74194150   66:8BF8           MOV DI,AX
74194153   FF15 88190C74     CALL DWORD PTR DS:[<&OLEAUT32.#6>]     OLEAUT32.SysFreeString
74194159   FF75 F0           PUSH DWORD PTR SS:[EBP-10]
7419415C   FF15 88190C74     CALL DWORD PTR DS:[<&OLEAUT32.#6>]     OLEAUT32.SysFreeString
74194162   FF75 E8           PUSH DWORD PTR SS:[EBP-18]
74194165   FF15 88190C74     CALL DWORD PTR DS:[<&OLEAUT32.#6>]     OLEAUT32.SysFreeString
7419416B   0FBFC7            MOVSX EAX,DI
7419416E   5F                POP EDI
7419416F   5E                POP ESI
74194170   5B                POP EBX
74194171   8BE5              MOV ESP,EBP
74194173   5D                POP EBP
74194174   C2 1400           RETN 14
74194177   66:C745 FC 0000   MOV WORD PTR SS:[EBP-4],0
7419417D   E9 02FFFFFF       JMP MSVBVM50.74194084
74194182   66:C745 FE 0000   MOV WORD PTR SS:[EBP-2],0
74194188   E9 17FFFFFF       JMP MSVBVM50.741940A4
```

Part 2 패치(1) - ADD ESP,XXXX 형태로 변경

(수정 전)

```
00402CFA  .  8D45 AC        LEA EAX,DWORD PTR SS:[EBP-54]
00402CFD  .  50             PUSH EAX
00402CFE  .  E8 1DE4FFFF    CALL <JMP.&MSVBVM50.#595>
00402D03  .  8D95 5CFFFFFF  LEA EDX,DWORD PTR SS:[EBP-A4]
00402D09  .  8D4D BC        LEA ECX,DWORD PTR SS:[EBP-44]
00402D0C  .  8985 64FFFFFF  MOV DWORD PTR SS:[EBP-9C],EAX
00402D12  .  89BD 5CFFFFFF  MOV DWORD PTR SS:[EBP-A4],EDI
```

(수정 후)

```
00402CFA  .  8D45 AC        LEA EAX,DWORD PTR SS:[EBP-54]
00402CFD  .  50             PUSH EAX
00402CFE     83C4 14        ADD ESP,14
00402D01     90             NOP
00402D02     90             NOP
00402D03     8D95 5CFFFFFF  LEA EDX,DWORD PTR SS:[EBP-A4]
00402D09  .  8D4D BC        LEA ECX,DWORD PTR SS:[EBP-44]
```

Part 2 패치(2) –RETN 형태로 변경

```
00402C0B  |. 64:890D 000000( MOV DWORD PTR FS:[0],ECX
00402C12  |. 5B              POP EBX
00402C13  |. C9              LEAVE
00402C14  |. C2 0400         RETN 4
00402C17  > 55              PUSH EBP
00402C18  . 8BEC            MOV EBP,ESP
00402C1A  . 83EC 0C         SUB ESP,0C
00402C1D  . 68 66104000     PUSH <JMP.&MSVBVM50.__vbaExceptHandler>  SE handler installatior
00402C22  . 64:A1 00000000( MOV EAX,DWORD PTR FS:[0]
00402C28  . 50              PUSH EAX
00402C29  . 64:8925 000000( MOV DWORD PTR FS:[0],ESP
00402C30  . 81EC 98000000   SUB ESP,98
00402C36  . 8B45 08         MOV EAX,DWORD PTR SS:[EBP+8]
00402C39  . 8365 08 FE      AND DWORD PTR SS:[EBP+8],FFFFFFFE
00402C3D  . 83E0 01         AND EAX,1
00402C40  . C745 F8 181040( MOV DWORD PTR SS:[EBP-8],Tut_Reve.004010
00402C47  . 53              PUSH EBX
00402C48  . 8945 FC         MOV DWORD PTR SS:[EBP-4],EAX
00402C4B  . 8B45 08         MOV EAX,DWORD PTR SS:[EBP+8]
00402C4E  . 56              PUSH ESI
00402C4F  . 57              PUSH EDI
00402C50  . 8B08            MOV ECX,DWORD PTR DS:[EAX]
00402C52  . 8965 F4         MOV DWORD PTR SS:[EBP-C],ESP
00402C55  . 50              PUSH EAX
00402C56  . FF51 04         CALL DWORD PTR DS:[ECX+4]
00402C59  . 6A 08           PUSH 8
00402C5B  . 33F6            XOR ESI,ESI
00402C5D  . 5B              POP EBX
00402C5E  . 89B5 7CFFFFFF   MOV DWORD PTR SS:[EBP-84],ESI
00402C64  . 8D95 7CFFFFFF   LEA EDX,DWORD PTR SS:[EBP-84]
00402C6A  . 8D4D AC         LEA ECX,DWORD PTR SS:[EBP-54]
00402C6D  . 8975 DC         MOV DWORD PTR SS:[EBP-24],ESI
00402C70  . 8975 CC         MOV DWORD PTR SS:[EBP-34],ESI
00402C73  . 8975 BC         MOV DWORD PTR SS:[EBP-44],ESI
00402C76  . 8975 AC         MOV DWORD PTR SS:[EBP-54],ESI
00402C79  . 8975 9C         MOV DWORD PTR SS:[EBP-64],ESI
00402C7C  . 8975 8C         MOV DWORD PTR SS:[EBP-74],ESI
00402C7F  . 89B5 5CFFFFFF   MOV DWORD PTR SS:[EBP-A4],ESI
00402C85  . C745 84 F01E40( MOV DWORD PTR SS:[EBP-7C],Tut_Reve.0040  UNICODE "Get rid of al
00402C8C    899D 7CFFFFFF   MOV DWORD PTR SS:[EBP-84],EBX
```

Part 2 패치(2) –RETN 형태로 변경

```
00402C12   . 5B          POP EBX
00402C13   . C9          LEAVE
00402C14   . C2 0400     RETN 4
00402C17   > 55          PUSH EBP                ← BP 설정
00402C18   . 8BEC        MOV EBP,ESP
00402C1A   . 83EC 0C     SUB ESP,0C
00402C1D   . 68 66104000 PUSH <JMP.&MSVBVM50.__vbaExceptHandler>  SE handler installation
```

(실행 후 스택값)

↙ 리턴 주소

```
0019F2A8   740DE5A9  RETURN to MSVBVM50.740DE5A9
0019F2AC   00650129  ASCII "B@"
0019F2B0   0019F2C0
0019F2B4   00402649  Tut_Reve.00402649
0019F2B8   00650168
0019F2BC   00000001
0019F2C0   0019F2DC
0019F2C4   740DE583  RETURN to MSVBVM50.740DE583 from
0019F2C8   00402649  Tut_Reve.00402649
0019F2CC   0019F388
0019F2D0   00000002
0019F2D4   00000001
0019F2D8   0019F3BC
```

Part 2 패치(2) –RETN 형태로 변경

```
740DE5A3  8BFC          MOV EDI,ESP
740DE5A5  F3:A5         REP MOVS DWORD PTR ES:[EDI],DWORD PTR DS
740DE5A7  FFD0          CALL EAX
740DE5A9  8BE5          MOV ESP,EBP
740DE5AB  5D            POP EBP
740DE5AC  8945 FC       MOV DWORD PTR SS:[EBP-4],EAX
740DE5AF  8B45 FC       MOV EAX,DWORD PTR SS:[EBP-4]
```

Part 2 패치(2) –RETN 형태로 변경

```
740DE5A3  8BFC      MOV EDI,ESP
740DE5A5  F3:A5     REP MOVS DWORD PTR ES:[EDI],DWORD PTR DS
740DE5A7  FFD0      CALL EAX                                  Tut_Reve.00402656
740DE5A9  8BE5      MOV ESP,EBP
740DE5AB  5D        POP EBP
740DE5AC  8945 FC   MOV DWORD PTR SS:[EBP-4],EAX
740DE5AF  8B45 FC   MOV EAX,DWORD PTR SS:[EBP-4]
```

CALL EAX 실행 전

```
Registers (MMX)
EAX 00402656 Tut_Reve.00402656
ECX 00000000
EDX 00000006
EBX 0226A374
ESP 0019FAB8
EBP 0019FABC
ESI 0019FB98
EDI 0019FABC

EIP 740DE5A7 MSVBVM50.740DE5A7
```

CALL EAX 실행 후

```
Registers (MMX)
EAX 00000000
ECX 0019FF58
EDX 00000090
EBX 022EA374
ESP 0019FABC
EBP 0019FABC
ESI 0019FB98
EDI 0019FABC

EIP 740DE5A9 MSVBVM50.740DE5A9
```

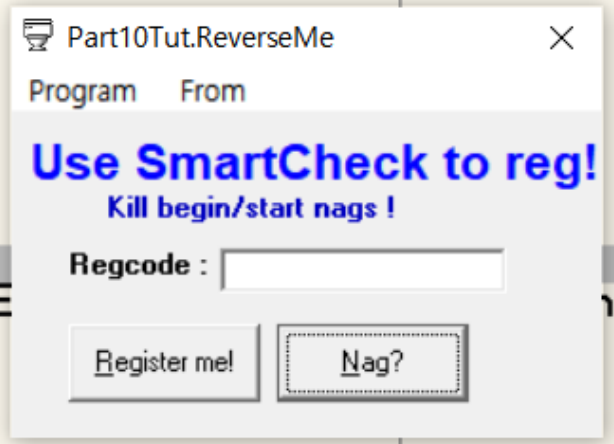
19FABC
- 19FAB8

4

(C가 16진수에서 12를 나타냄)

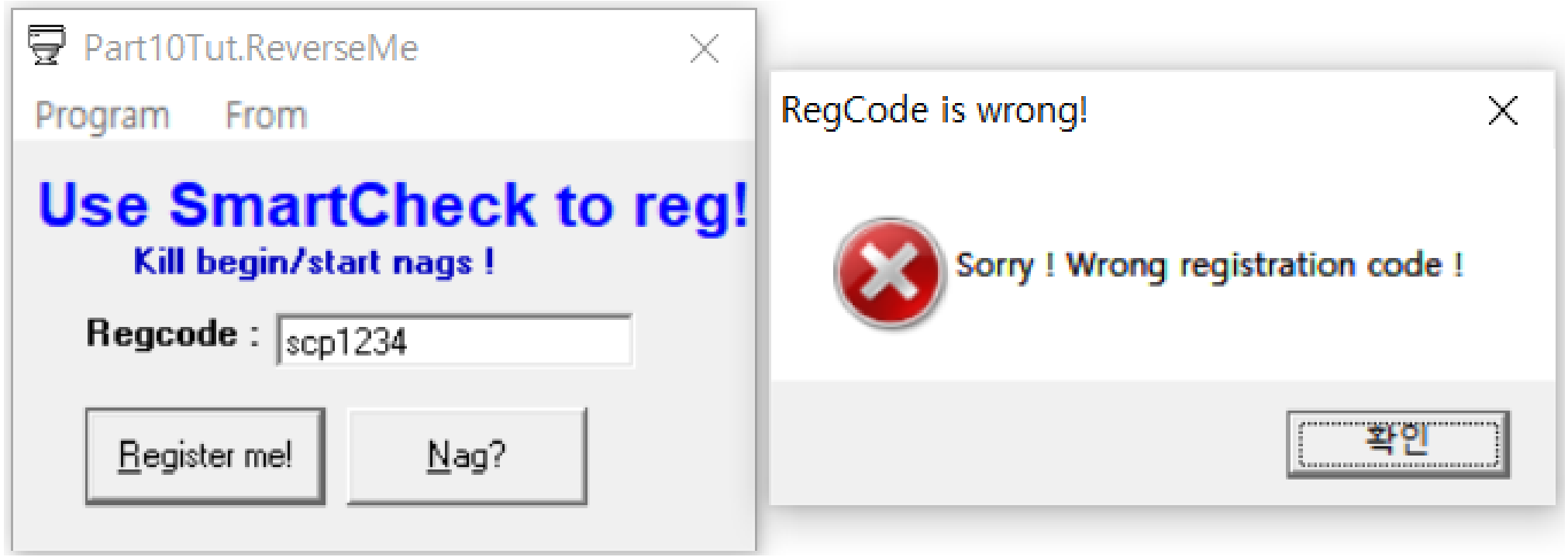
Part 2 패치(2) –RETN 형태로 변경

```
00402BF1  .  E8 12E5FFFF    CALL <JMP.&MSVBVM50.__vbaEnd>
00402BF6  .  8365 FC 00     AND DWORD PTR SS:[EBP-4],0
00402BFA  .  8B45 08        MOV EAX,DWORD PTR SS:[EBP+8]
00402BFD  .  50             PUSH EAX
00402BFE  .  8B08           MOV ECX,DWORD PTR DS:[EAX]
00402C00  .  FF51 08        CALL DWORD PTR DS:[ECX+8]
00402C03  .  8B4D EC        MOV ECX,DWORD PTR SS:[EBP-14]
00402C06  .  8B45 FC        MOV EAX,DWORD PTR SS:[EBP-4]
00402C09  .  5F             POP EDI
00402C0A  .  5E             POP ESI
00402C0B  .  64:890D 000000 MOV DWORD PTR FS:[0],ECX
00402C12  .  5B             POP EBX
00402C13  .  C9             LEAVE
00402C14  .  C2 0400        RETN 4
00402C17     C2 0400        RETN 4
00402C1A  .  83EC 0C        SUB ESP,0C
00402C1D  .  68 66104000    PUSH <JMP.&MSVBVM50.__vbaE                    ndler installation
00402C22  .  64:A1 00000000 MOV EAX,DWORD PTR FS:[0]
00402C28  .  50             PUSH EAX
00402C29  .  64:8925 000000 MOV DWORD PTR FS:[0],ESP
00402C30  .  81EC 98000000  SUB ESP,98
00402C36  .  8B45 08        MOV EAX,DWORD PTR SS:[EBP+8]
00402C39  .  8365 08 FE     AND DWORD PTR SS:[EBP+8],FFFFFFFE
00402C3D  .  83E0 01        AND EAX,1
00402C40  .  C745 F8 181040 MOV DWORD PTR SS:[EBP-8],Tut_Reve.004010
```

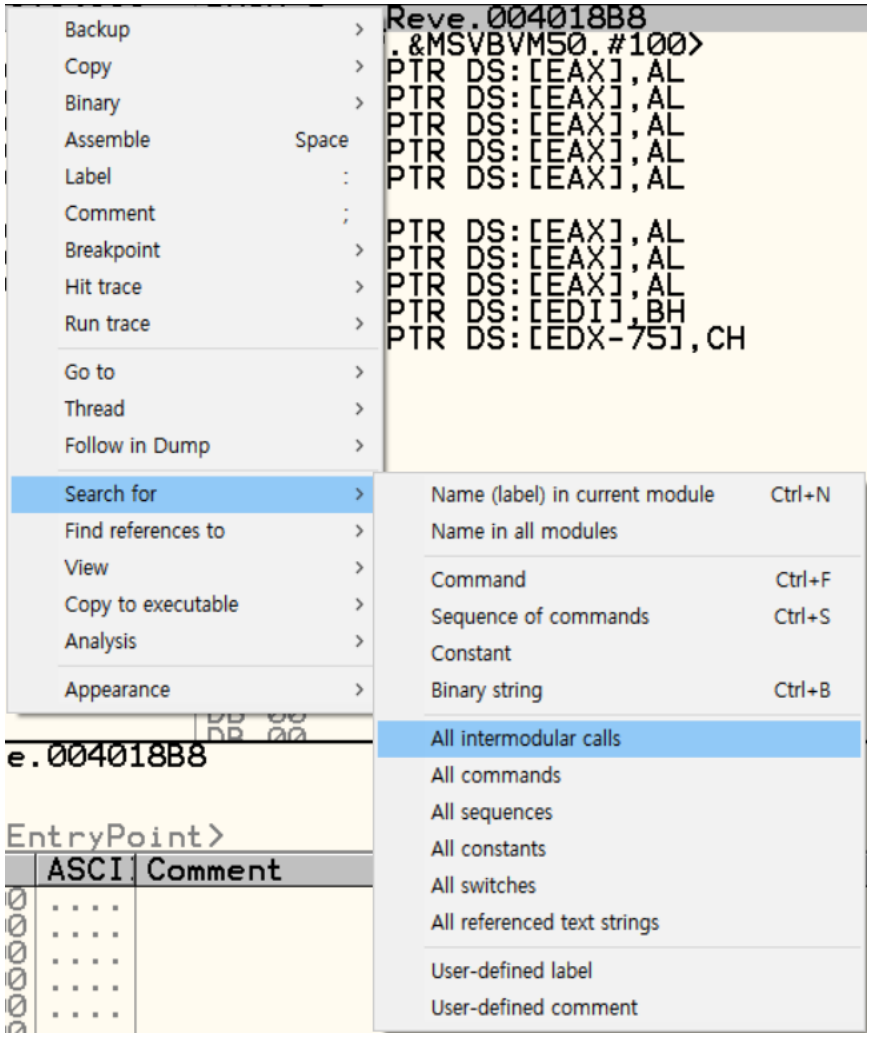


목표(2) – Registraion Code 찾기

Part 2 목표 (2) – Restration Code 찾기



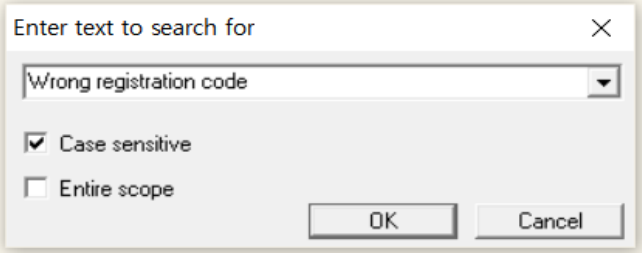
Part 2 목표 (2) – Restration Code 찾기



Part 2 목표 (2) – Restration Code 찾기

Text strings referenced in Tut_Reve:.text

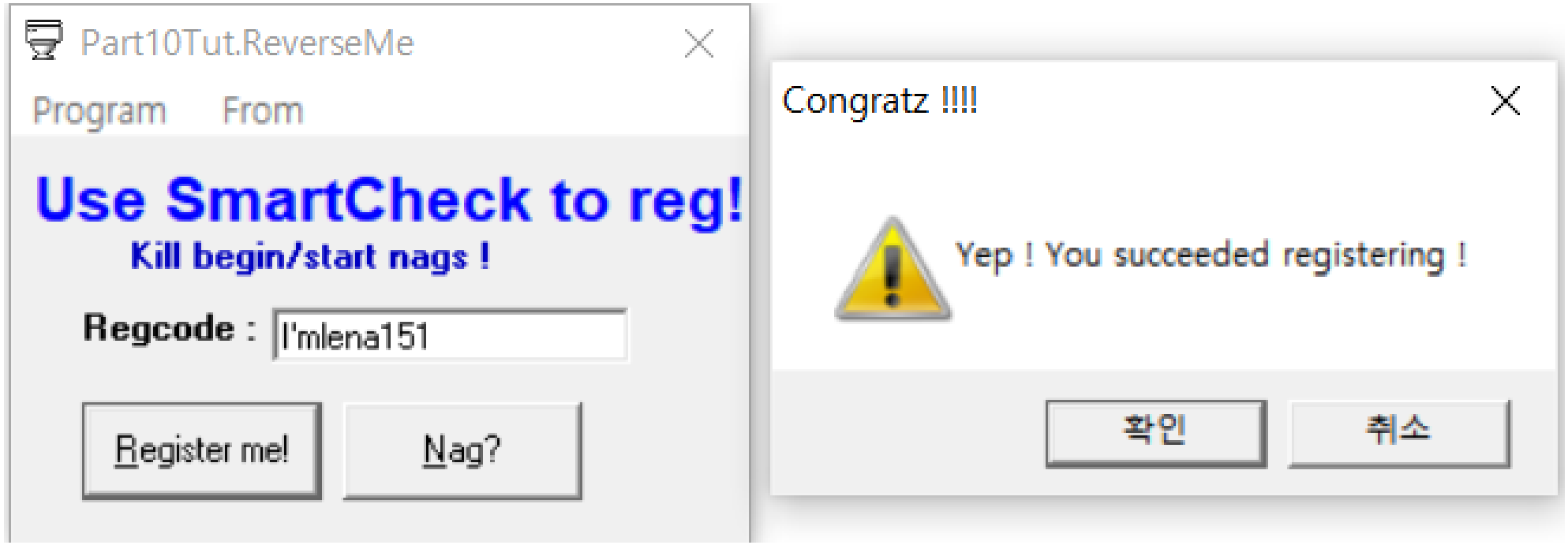
Address	Disassembly	Text string
00401FC4	UNICODE "0 lena15"	
00401FD4	UNICODE "1 ",0	
00401FEC	UNICODE "Visible",0	
00401FFC	ASCII "VBA5.DLL",0	
00402008	ASCII "__vbaObjVar",0	
00402014	ASCII "__vbaLateMemSt",0	
00402024	ASCII "__vbaVarDup",0	
00402030	ASCII "__vbaEnd",0	
0040203C	ASCII "__vbaVarTstEq",0	
0040204C	ASCII "__vbaFreeVarList"	
0040205C	ASCII 0	
00402060	ASCII "__vbaI4Var",0	
0040206C	ASCII "__vbaVarMove",0	
0040207C	ASCII "__vbaVarCopy",0	
0040208C	ASCII "__vbaFreeObj",0	
0040209C	ASCII "__vbaFreeStr",0	
004020AC	ASCII "__vbaHresultChec"	
004020BC	ASCII "kObj",0	
004020C4	ASCII "__vbaObjSet",0	
004020D0	ASCII "__vbaStrCmp",0	
0040217C	DD Tut_Reve.00401C84	ASCII "Form"
004021A4	DD Tut_Reve.00401CFC	ASCII "mnuprog"
004021CC	DD Tut_Reve.00401D14	ASCII "Command1"
004021F4	DD Tut_Reve.00401D20	ASCII "Command2"
0040221C	DD Tut_Reve.00401D2C	ASCII "mnuabout"
00402244	DD Tut_Reve.00401D48	ASCII "Text1"
0040226C	DD Tut_Reve.00401D60	ASCII "Label2"
00402294	DD Tut_Reve.00401D68	ASCII "mnuexit"
004022BC	DD Tut_Reve.00401D70	ASCII "Label3"
004022E4	DD Tut_Reve.00401D78	ASCII "Label1"
004028BD	PUSH Tut_Reve.00401DDC	UNICODE "I'mlena151"
004028F5	MOV DWORD PTR SS:[EBP-84],Tut_Reve.0040	UNICODE "Yep ! You succeeded registering !"
00402934	MOV DWORD PTR SS:[EBP-84],Tut_Reve.0040	UNICODE "Congratz !!!!"
00402A2A	PUSH Tut_Reve.00401DDC	UNICODE "I'mlena151"
00402A69	MOV DWORD PTR SS:[EBP-84],Tut_Reve.0040	UNICODE "Sorry ! Wrong registration code !"
00402AA9	MOV DWORD PTR SS:[EBP-84],Tut_Reve.0040	UNICODE "RegCode is wrong!"
00402C85	MOV DWORD PTR SS:[EBP-7C],Tut_Reve.0040	UNICODE "Get rid of all Nags and find the right
00402CBE	MOV DWORD PTR SS:[EBP-7C],Tut_Reve.0040	UNICODE "Nag Screen "
00402E28	MOV DWORD PTR SS:[EBP-5C],Tut_Reve.0040	UNICODE "ReverseMe Tutorial Part10 lena151 "
00402F9A	PUSH Tut_Reve.00401FEC	UNICODE "Visible"



Part 2 목표 (2) – Restration Code 찾기

```
00402A0F  .v7D 16          JGE SHORT Tut_Reve.00402A27
00402A11  . 68 A0000000    PUSH 0A0
00402A16  . 68 F41D4000    PUSH Tut_Reve.00401DF4
00402A1B  . FFB5 50FFFFFF  PUSH DWORD PTR SS:[EBP-B0]
00402A21  . 50             PUSH EAX
00402A22  . E8 17E7FFFF    CALL <JMP.&MSVBVM50.__vbaHresultCheckOb
00402A27  > FF75 A8        PUSH DWORD PTR SS:[EBP-58]
00402A2A  . 68 DC1D4000    PUSH Tut_Reve.00401DDC                   UNICODE "I'mlena151"
00402A2F  . E8 16E7FFFF    CALL <JMP.&MSVBVM50.__vbaStrCmp>
00402A34  . F7D8           NEG EAX
00402A36  . 1BC0           SBB EAX,EAX
00402A38  . 8D4D A8        LEA ECX,DWORD PTR SS:[EBP-58]
00402A3B  . F7D8           NEG EAX
00402A3D  . F7D8           NEG EAX
00402A3F  . 8985 48FFFFFF  MOV DWORD PTR SS:[EBP-B8],EAX
00402A45  . E8 EEE6FFFF    CALL <JMP.&MSVBVM50.__vbaFreeStr>
00402A4A  . 8D4D A4        LEA ECX,DWORD PTR SS:[EBP-5C]
00402A4D  . E8 E0E6FFFF    CALL <JMP.&MSVBVM50.__vbaFreeObj>
00402A52  . 66:83BD 48FFFF CMP WORD PTR SS:[EBP-B8],0
00402A5A  .v0F84 E7000000  JE Tut_Reve.00402B47
00402A60  . 8D95 74FFFFFF  LEA EDX,DWORD PTR SS:[EBP-8C]
00402A66  . 8D4D AC        LEA ECX,DWORD PTR SS:[EBP-54]
00402A69  . C785 7CFFFFFF  MOV DWORD PTR SS:[EBP-84],Tut_Reve.0040  UNICODE "Sorry ! Wrong regis
00402A73  . C785 74FFFFFF  MOV DWORD PTR SS:[EBP-8C],8
00402A7D  . E8 AAE6FFFF    CALL <JMP.&MSVBVM50.__vbaVarCopy>
00402A82  . 8D95 74FFFFFF  LEA EDX,DWORD PTR SS:[EBP-8C]
00402A88  . 8D4D DC        LEA ECX,DWORD PTR SS:[EBP-24]
00402A8B  . C785 7CFFFFFF  MOV DWORD PTR SS:[EBP-84],10
00402A95  . 899D 74FFFFFF  MOV DWORD PTR SS:[EBP-8C],EBX
00402A9B  . E8 86E6FFFF    CALL <JMP.&MSVBVM50.__vbaVarMove>
```

Part 2 목표 (2) – Restration Code 찾기



Q&A