Abex crackme #2 풀이

SCP 20학번 박준형

목차 table of contents

1 프로그램 동작 방식 이해

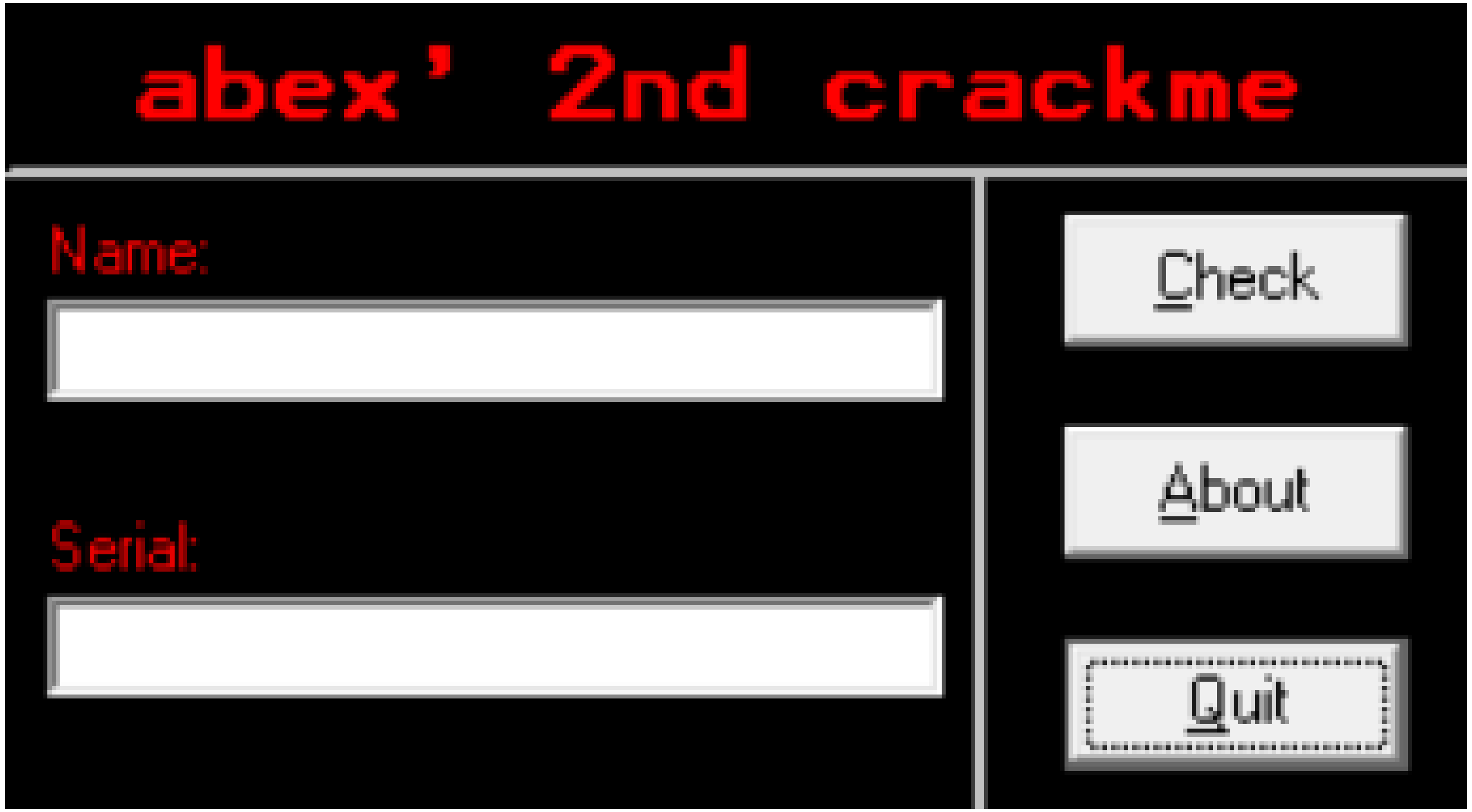
2 문자열 검색

3 스택 분석

4 문제 풀이

프로그램 동작 방식 이해

프로그램 동작 방식 이해



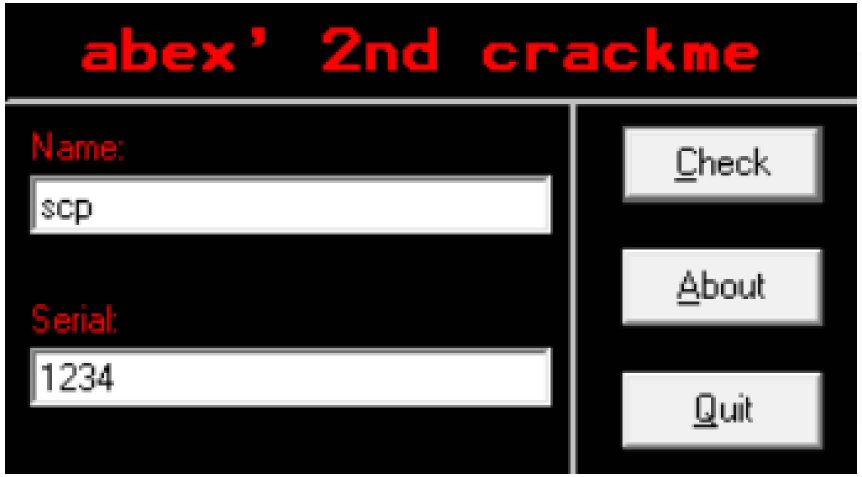
abex' 2nd crackme

Name:

Serial:

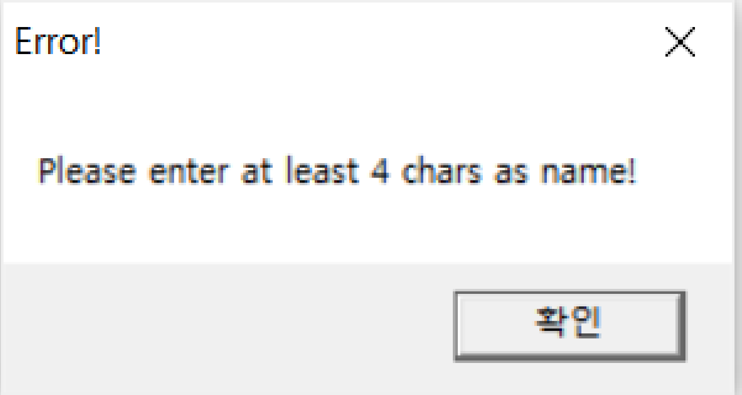
Part 1 프로그램 동작 방식 이해

(이름이 4자리 보다 작을 때)


abex' 2nd crackme

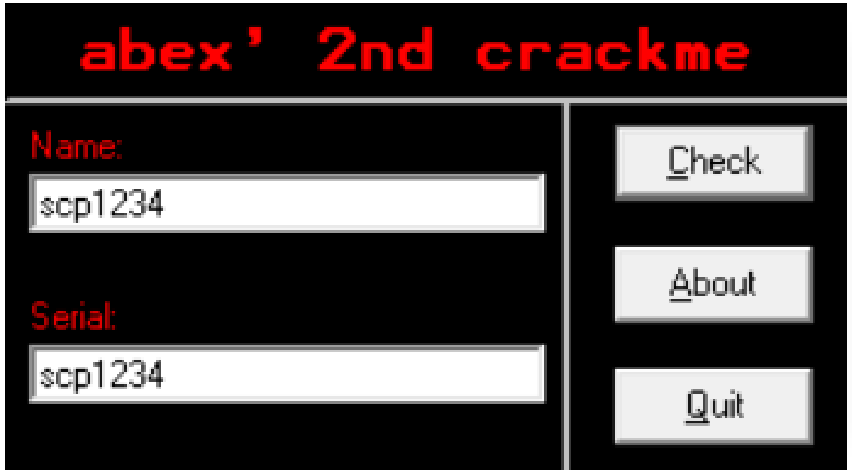
Name: scp

Serial: 1234


Error!

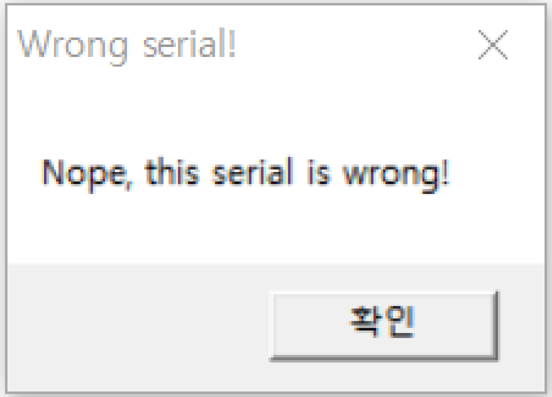
Please enter at least 4 chars as name!

(일련번호가 틀렸을 때)


abex' 2nd crackme

Name: scp1234

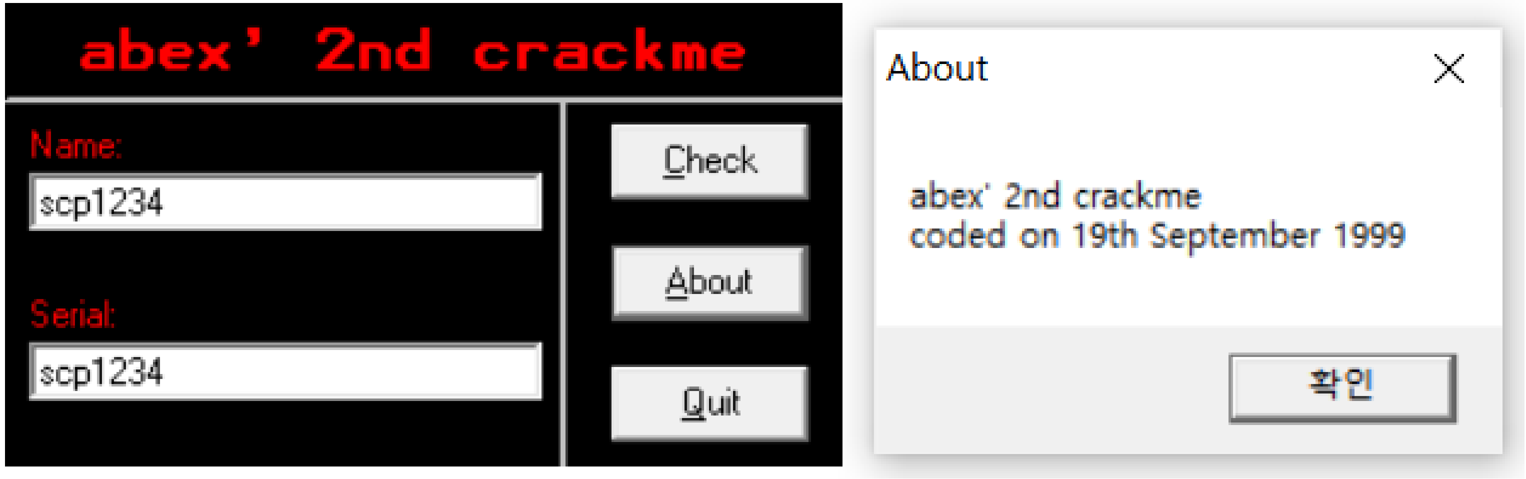
Serial: scp1234


Wrong serial!

Nope, this serial is wrong!

Part 1 프로그램 동작 방식 이해

(About 버튼 눌렀을 때)



Name: scp1234

Serial: scp1234

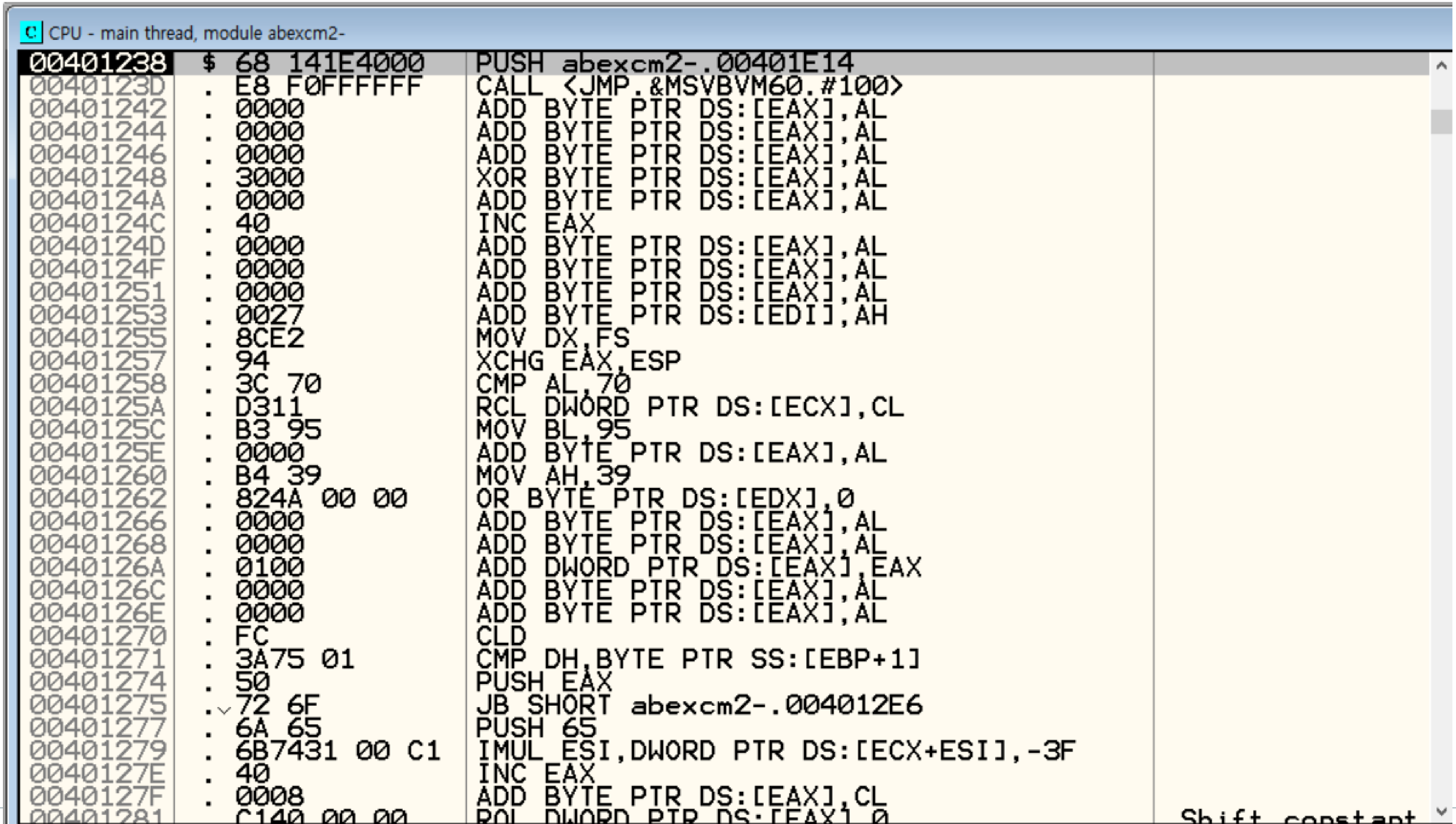
About

abex' 2nd crackme
coded on 19th September 1999

(Quit 버튼 눌렀을 때는 프로그램이 즉시 종료됨)

문자열 검색

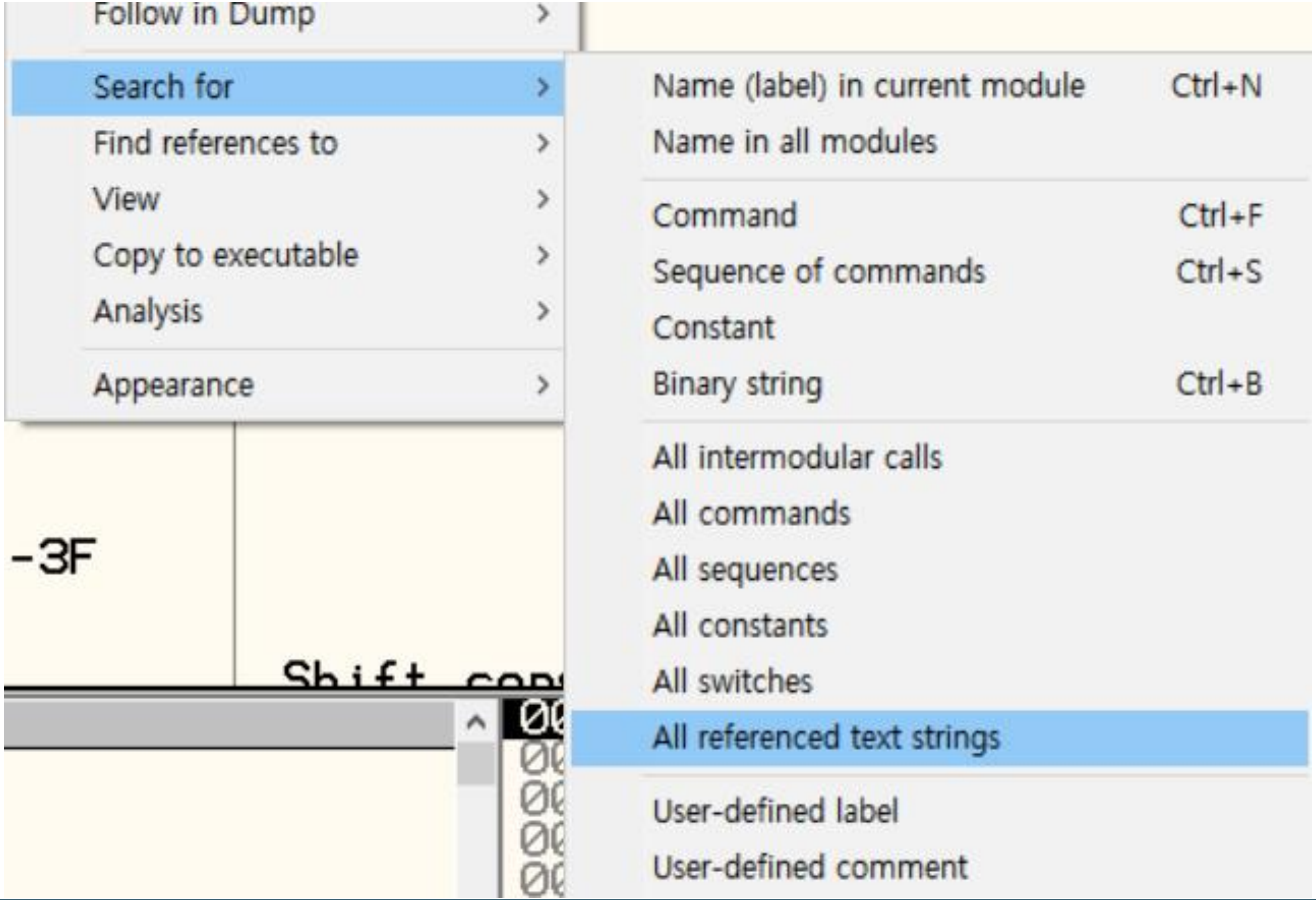
Part 2 문자열 검색



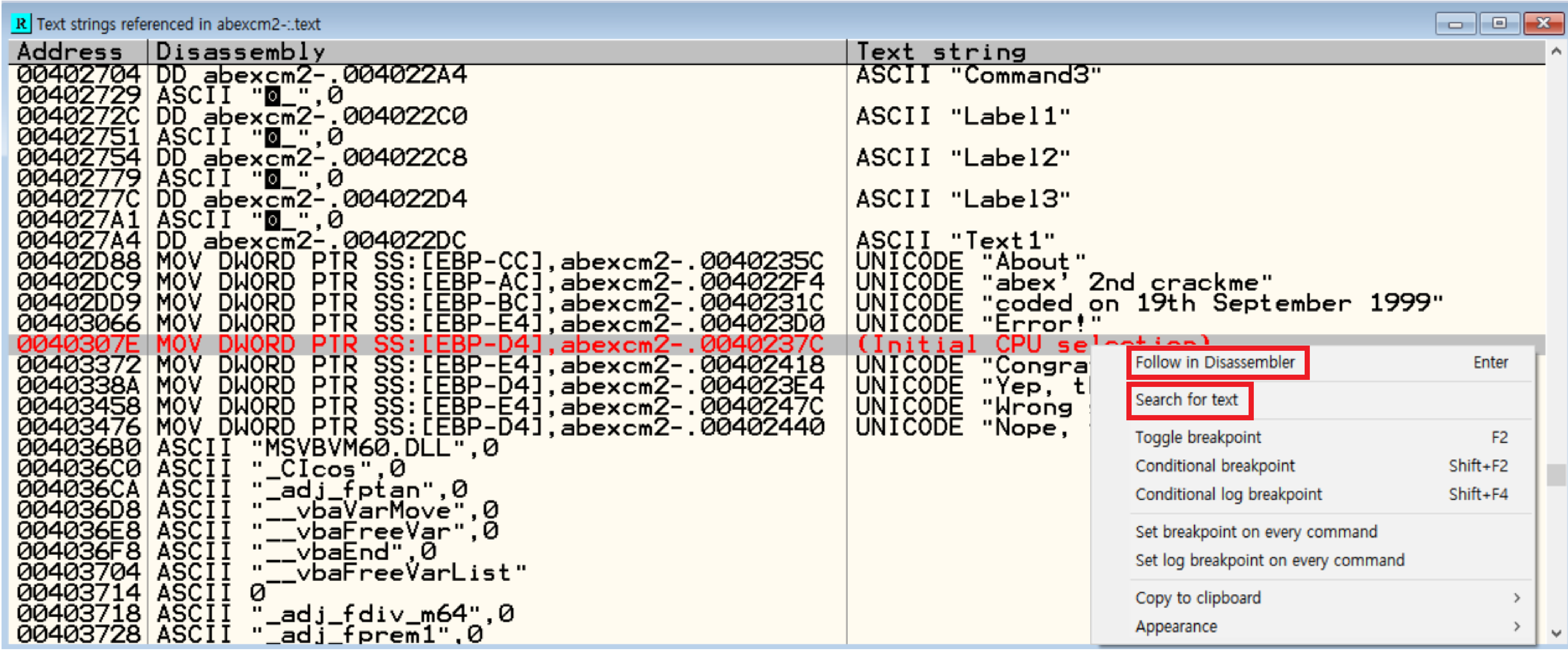
CPU - main thread, module abexcm2-

```
00401238  $ 68 141E4000     PUSH abexcm2-.00401E14
0040123D  . E8 F0FFFFFF     CALL <JMP.&MSVBVM60.#100>
00401242  . 0000            ADD BYTE PTR DS:[EAX],AL
00401244  . 0000            ADD BYTE PTR DS:[EAX],AL
00401246  . 0000            ADD BYTE PTR DS:[EAX],AL
00401248  . 3000            XOR BYTE PTR DS:[EAX],AL
0040124A  . 0000            ADD BYTE PTR DS:[EAX],AL
0040124C  . 40              INC EAX
0040124D  . 0000            ADD BYTE PTR DS:[EAX],AL
0040124F  . 0000            ADD BYTE PTR DS:[EAX],AL
00401251  . 0000            ADD BYTE PTR DS:[EAX],AL
00401253  . 0027            ADD BYTE PTR DS:[EDI],AH
00401255  . 8CE2            MOV DX,FS
00401257  . 94              XCHG EAX,ESP
00401258  . 3C 70           CMP AL,70
0040125A  . D311            RCL DWORD PTR DS:[ECX],CL
0040125C  . B3 95           MOV BL,95
0040125E  . 0000            ADD BYTE PTR DS:[EAX],AL
00401260  . B4 39           MOV AH,39
00401262  . 824A 00 00      OR BYTE PTR DS:[EDX],0
00401266  . 0000            ADD BYTE PTR DS:[EAX],AL
00401268  . 0000            ADD BYTE PTR DS:[EAX],AL
0040126A  . 0100            ADD DWORD PTR DS:[EAX],EAX
0040126C  . 0000            ADD BYTE PTR DS:[EAX],AL
0040126E  . 0000            ADD BYTE PTR DS:[EAX],AL
00401270  . FC              CLD
00401271  . 3A75 01         CMP DH,BYTE PTR SS:[EBP+1]
00401274  . 50              PUSH EAX
00401275  .v72 6F           JB SHORT abexcm2-.004012E6
00401277  . 6A 65           PUSH 65
00401279  . 6B7431 00 C1    IMUL ESI,DWORD PTR DS:[ECX+ESI],-3F
0040127E  . 40              INC EAX
0040127F  . 0008            ADD BYTE PTR DS:[EAX],CL
00401281  . C140 00 00      ROL DWORD PTR DS:[EAX],0                 Shift constant
```

Part 2 문자열 검색


Follow in Dump
Search for
Find references to
View
Copy to executable
Analysis
Appearance
Name (label) in current module Ctrl+N
Name in all modules
Command Ctrl+F
Sequence of commands Ctrl+S
Constant
Binary string Ctrl+B
All intermodular calls
All commands
All sequences
All constants
All switches
All referenced text strings
User-defined label
User-defined comment
-3F
Shift con

Part 2 문자열 검색

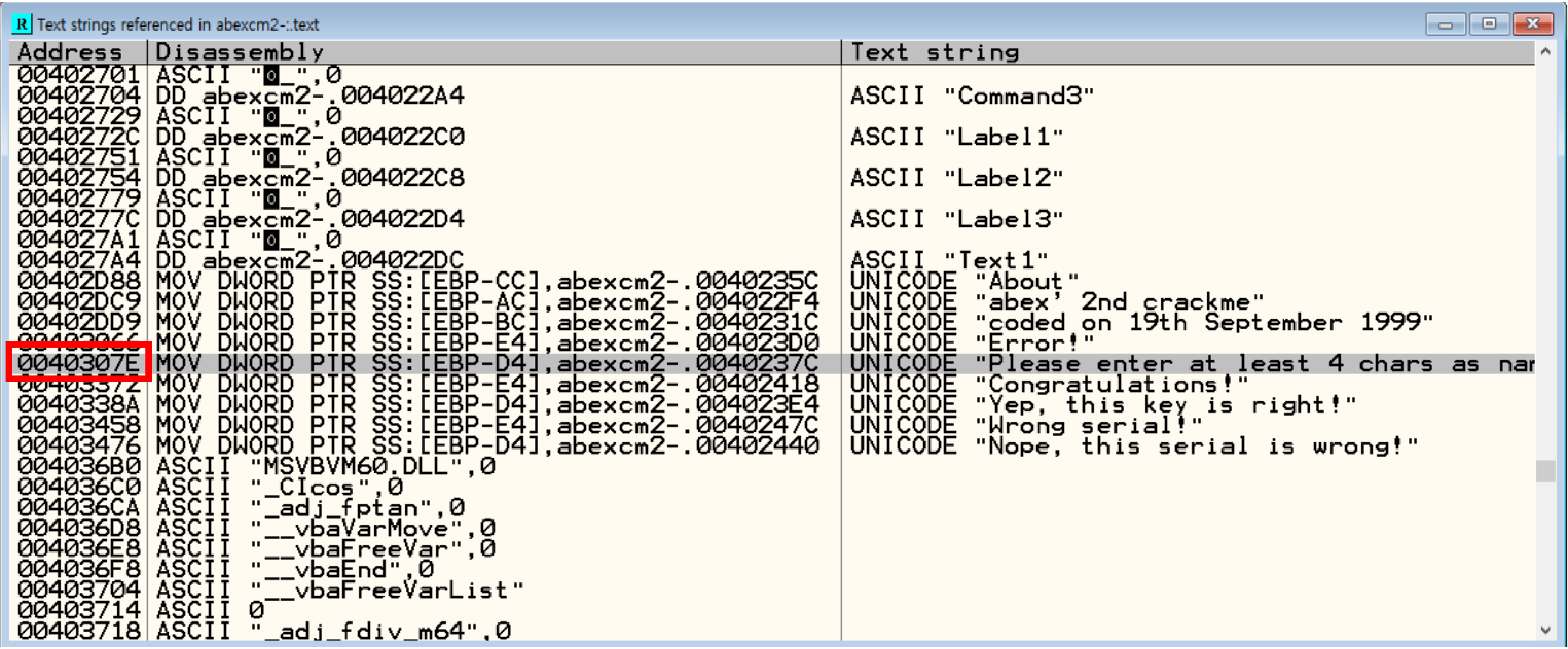


Text strings referenced in abexcm2-:.text

```
Address   Disassembly                                      Text string
00402704  DD abexcm2-.004022A4                             ASCII "Command3"
00402729  ASCII "■_",0
0040272C  DD abexcm2-.004022C0                             ASCII "Label1"
00402751  ASCII "■_",0
00402754  DD abexcm2-.004022C8                             ASCII "Label2"
00402779  ASCII "■_",0
0040277C  DD abexcm2-.004022D4                             ASCII "Label3"
004027A1  ASCII "■_",0
004027A4  DD abexcm2-.004022DC                             ASCII "Text1"
00402D88  MOV DWORD PTR SS:[EBP-CC],abexcm2-.0040235C      UNICODE "About"
00402DC9  MOV DWORD PTR SS:[EBP-AC],abexcm2-.004022F4      UNICODE "abex' 2nd crackme"
00402DD9  MOV DWORD PTR SS:[EBP-BC],abexcm2-.0040231C      UNICODE "coded on 19th September 1999"
00403066  MOV DWORD PTR SS:[EBP-E4],abexcm2-.004023D0      UNICODE "Error!"
0040307E  MOV DWORD PTR SS:[EBP-D4],abexcm2-.0040237C      (Initial CPU selection)
00403372  MOV DWORD PTR SS:[EBP-E4],abexcm2-.00402418      UNICODE "Congra
0040338A  MOV DWORD PTR SS:[EBP-D4],abexcm2-.004023E4      UNICODE "Yep, t
00403458  MOV DWORD PTR SS:[EBP-E4],abexcm2-.0040247C      UNICODE "Wrong
00403476  MOV DWORD PTR SS:[EBP-D4],abexcm2-.00402440      UNICODE "Nope,
004036B0  ASCII "MSVBVM60.DLL",0
004036C0  ASCII "_CIcos",0
004036CA  ASCII "_adj_fptan",0
004036D8  ASCII "__vbaVarMove",0
004036E8  ASCII "__vbaFreeVar",0
004036F8  ASCII "__vbaEnd",0
00403704  ASCII "__vbaFreeVarList"
00403714  ASCII 0
00403718  ASCII "_adj_fdiv_m64",0
00403728  ASCII "_adj_fprem1",0
```

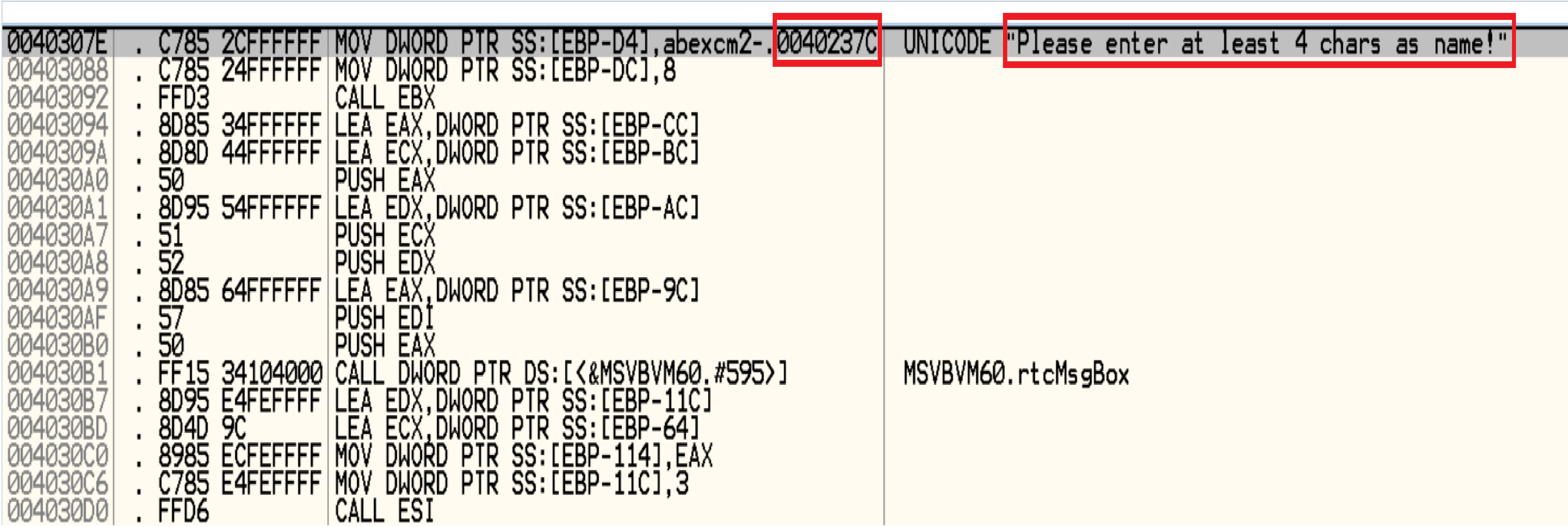
Follow in Disassembler Enter
Search for text
Toggle breakpoint F2
Conditional breakpoint Shift+F2
Conditional log breakpoint Shift+F4
Set breakpoint on every command
Set log breakpoint on every command
Copy to clipboard
Appearance

Part 2 문자열 검색



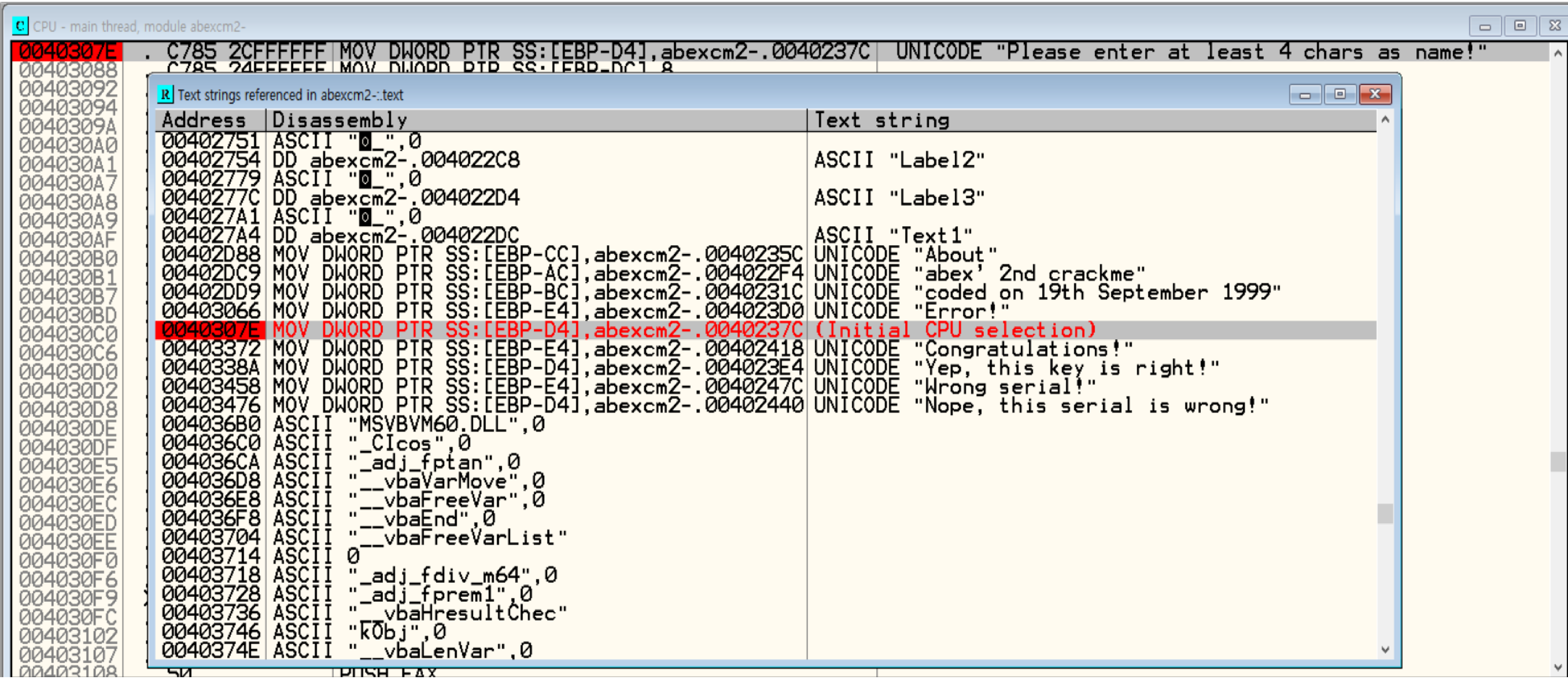
```
Address  Disassembly                                       Text string
00402701 ASCII "■_",0
00402704 DD abexcm2-.004022A4                              ASCII "Command3"
00402729 ASCII "■_",0
0040272C DD abexcm2-.004022C0                              ASCII "Label1"
00402751 ASCII "■_",0
00402754 DD abexcm2-.004022C8                              ASCII "Label2"
00402779 ASCII "■_",0
0040277C DD abexcm2-.004022D4                              ASCII "Label3"
004027A1 ASCII "■_",0
004027A4 DD abexcm2-.004022DC                              ASCII "Text1"
00402D88 MOV DWORD PTR SS:[EBP-CC],abexcm2-.0040235C       UNICODE "About"
00402DC9 MOV DWORD PTR SS:[EBP-AC],abexcm2-.004022F4       UNICODE "abex' 2nd crackme"
00402DD9 MOV DWORD PTR SS:[EBP-BC],abexcm2-.0040231C       UNICODE "coded on 19th September 1999"
00403066 MOV DWORD PTR SS:[EBP-E4],abexcm2-.004023D0       UNICODE "Error!"
0040307E MOV DWORD PTR SS:[EBP-D4],abexcm2-.0040237C       UNICODE "Please enter at least 4 chars as nar
00403372 MOV DWORD PTR SS:[EBP-E4],abexcm2-.00402418       UNICODE "Congratulations!"
0040338A MOV DWORD PTR SS:[EBP-D4],abexcm2-.004023E4       UNICODE "Yep, this key is right!"
00403458 MOV DWORD PTR SS:[EBP-E4],abexcm2-.0040247C       UNICODE "Wrong serial!"
00403476 MOV DWORD PTR SS:[EBP-D4],abexcm2-.00402440       UNICODE "Nope, this serial is wrong!"
004036B0 ASCII "MSVBVM60.DLL",0
004036C0 ASCII "_CIcos",0
004036CA ASCII "_adj_fptan",0
004036D8 ASCII "__vbaVarMove",0
004036E8 ASCII "__vbaFreeVar",0
004036F8 ASCII "__vbaEnd",0
00403704 ASCII "__vbaFreeVarList"
00403714 ASCII 0
00403718 ASCII "_adj_fdiv_m64",0
```

Part 2 문자열 검색



```
0040307E  . C785 2CFFFFFF MOV DWORD PTR SS:[EBP-D4],abexcm2-.0040237C  UNICODE "Please enter at least 4 chars as name!"
00403088  . C785 24FFFFFF MOV DWORD PTR SS:[EBP-DC],8
00403092  . FFD3          CALL EBX
00403094  . 8D85 34FFFFFF LEA EAX,DWORD PTR SS:[EBP-CC]
0040309A  . 8D8D 44FFFFFF LEA ECX,DWORD PTR SS:[EBP-BC]
004030A0  . 50            PUSH EAX
004030A1  . 8D95 54FFFFFF LEA EDX,DWORD PTR SS:[EBP-AC]
004030A7  . 51            PUSH ECX
004030A8  . 52            PUSH EDX
004030A9  . 8D85 64FFFFFF LEA EAX,DWORD PTR SS:[EBP-9C]
004030AF  . 57            PUSH EDI
004030B0  . 50            PUSH EAX
004030B1  . FF15 34104000 CALL DWORD PTR DS:[<&MSVBVM60.#595>]         MSVBVM60.rtcMsgBox
004030B7  . 8D95 E4FEFFFF LEA EDX,DWORD PTR SS:[EBP-11C]
004030BD  . 8D4D 9C       LEA ECX,DWORD PTR SS:[EBP-64]
004030C0  . 8985 ECFEFFFF MOV DWORD PTR SS:[EBP-114],EAX
004030C6  . C785 E4FEFFFF MOV DWORD PTR SS:[EBP-11C],3
004030D0  . FFD6          CALL ESI
```

문자열 검색



CPU - main thread, module abexcm2-

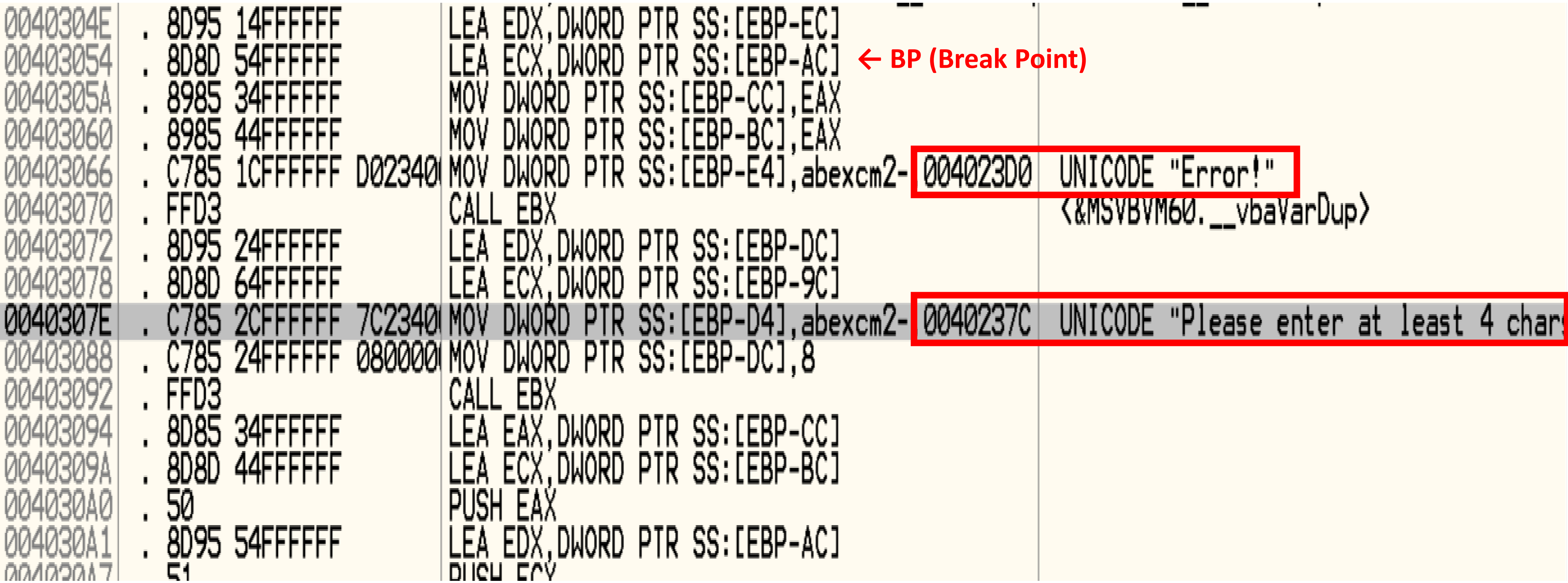
```
0040307E  . C785 2CFFFFFF  MOV DWORD PTR SS:[EBP-D4],abexcm2-.0040237C  UNICODE "Please enter at least 4 chars as name!"
00403088    C785 24FFFFFF  MOV DWORD PTR SS:[EBP-DC],8
00403092
00403094
0040309A
004030A0
004030A1
004030A7
004030A8
004030A9
004030AF
004030B0
004030B1
004030B7
004030BD
004030C0
004030C6
004030D0
004030D2
004030D8
004030DE
004030DF
004030E5
004030E6
004030EC
004030ED
004030EE
004030F0
004030F6
004030F9
004030FC
00403102
00403107
00403108    50             PUSH EAX
```

Text strings referenced in abexcm2-:.text

```
Address   Disassembly                                    Text string
00402751  ASCII "■_",0
00402754  DD abexcm2-.004022C8                           ASCII "Label2"
00402779  ASCII "■_",0
0040277C  DD abexcm2-.004022D4                           ASCII "Label3"
004027A1  ASCII "■_",0
004027A4  DD abexcm2-.004022DC                           ASCII "Text1"
00402D88  MOV DWORD PTR SS:[EBP-CC],abexcm2-.0040235C   UNICODE "About"
00402DC9  MOV DWORD PTR SS:[EBP-AC],abexcm2-.004022F4   UNICODE "abex' 2nd crackme"
00402DD9  MOV DWORD PTR SS:[EBP-BC],abexcm2-.0040231C   UNICODE "coded on 19th September 1999"
00403066  MOV DWORD PTR SS:[EBP-E4],abexcm2-.004023D0   UNICODE "Error!"
0040307E  MOV DWORD PTR SS:[EBP-D4],abexcm2-.0040237C   (Initial CPU selection)
00403372  MOV DWORD PTR SS:[EBP-E4],abexcm2-.00402418   UNICODE "Congratulations!"
0040338A  MOV DWORD PTR SS:[EBP-D4],abexcm2-.004023E4   UNICODE "Yep, this key is right!"
00403458  MOV DWORD PTR SS:[EBP-E4],abexcm2-.0040247C   UNICODE "Wrong serial!"
00403476  MOV DWORD PTR SS:[EBP-D4],abexcm2-.00402440   UNICODE "Nope, this serial is wrong!"
004036B0  ASCII "MSVBVM60.DLL",0
004036C0  ASCII "_CIcos",0
004036CA  ASCII "_adj_fptan",0
004036D8  ASCII "__vbaVarMove",0
004036E8  ASCII "__vbaFreeVar",0
004036F8  ASCII "__vbaEnd",0
00403704  ASCII "__vbaFreeVarList"
00403714  ASCII 0
00403718  ASCII "_adj_fdiv_m64",0
00403728  ASCII "_adj_fprem1",0
00403736  ASCII "__vbaHresultChec"
00403746  ASCII "kÖbj",0
0040374E  ASCII "__vbaLenVar",0
```

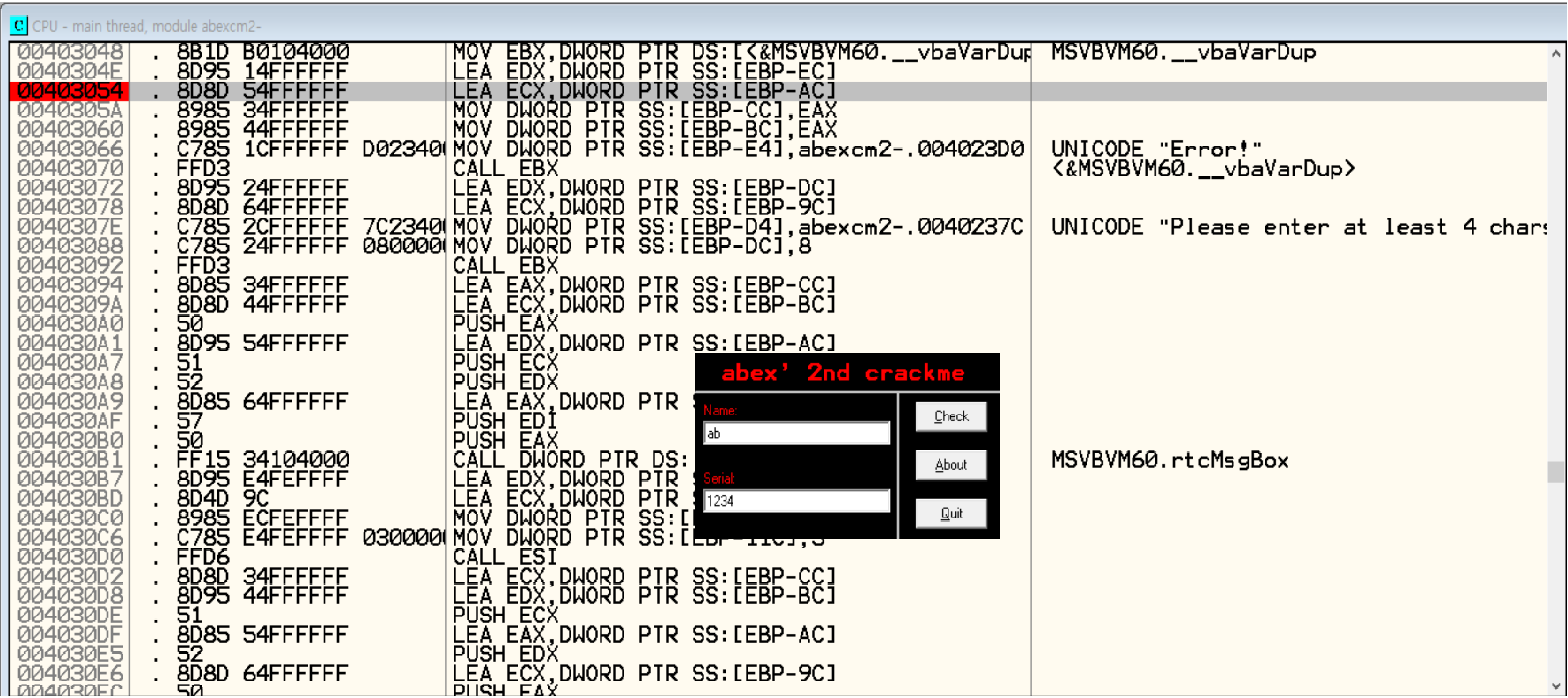
스택 분석

Part 3 스택 분석



```
0040304E  . 8D95 14FFFFFF         LEA EDX,DWORD PTR SS:[EBP-EC]
00403054  . 8D8D 54FFFFFF         LEA ECX,DWORD PTR SS:[EBP-AC]
0040305A  . 8985 34FFFFFF         MOV DWORD PTR SS:[EBP-CC],EAX
00403060  . 8985 44FFFFFF         MOV DWORD PTR SS:[EBP-BC],EAX
00403066  . C785 1CFFFFFF D02340  MOV DWORD PTR SS:[EBP-E4],abexcm2-004023D0  UNICODE "Error!"
00403070  . FFD3                  CALL EBX                                     <&MSVBVM60.__vbaVarDup>
00403072  . 8D95 24FFFFFF         LEA EDX,DWORD PTR SS:[EBP-DC]
00403078  . 8D8D 64FFFFFF         LEA ECX,DWORD PTR SS:[EBP-9C]
0040307E  . C785 2CFFFFFF 7C2340  MOV DWORD PTR SS:[EBP-D4],abexcm2-0040237C  UNICODE "Please enter at least 4 char
00403088  . C785 24FFFFFF 080000  MOV DWORD PTR SS:[EBP-DC],8
00403092  . FFD3                  CALL EBX
00403094  . 8D85 34FFFFFF         LEA EAX,DWORD PTR SS:[EBP-CC]
0040309A  . 8D8D 44FFFFFF         LEA ECX,DWORD PTR SS:[EBP-BC]
004030A0  . 50                    PUSH EAX
004030A1  . 8D95 54FFFFFF         LEA EDX,DWORD PTR SS:[EBP-AC]
004030A7  . 51                    PUSH ECX
```

← BP (Break Point)



CPU - main thread, module abexcm2-

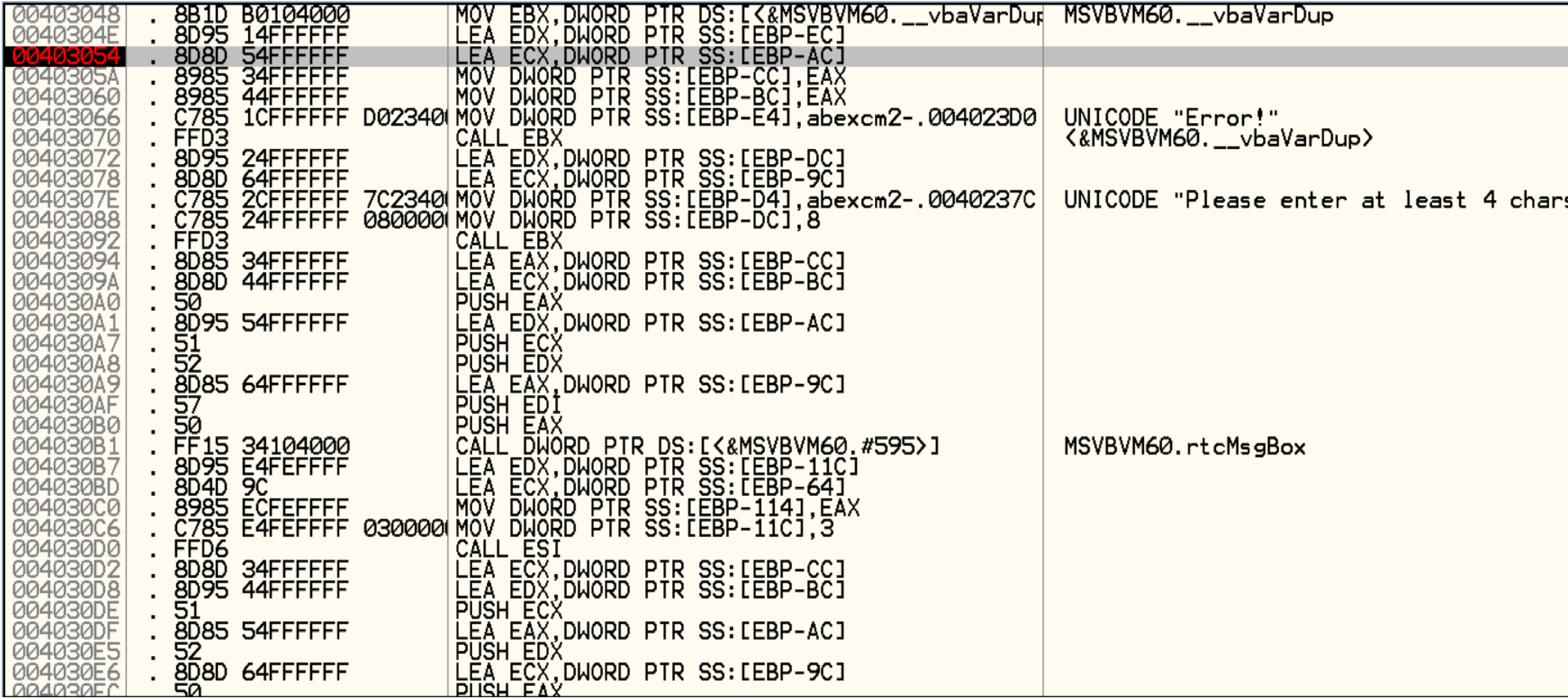
```
00403048  . 8B1D B0104000     MOV EBX,DWORD PTR DS:[<&MSVBVM60.__vbaVarDup  MSVBVM60.__vbaVarDup
0040304E  . 8D95 14FFFFFF     LEA EDX,DWORD PTR SS:[EBP-EC]
00403054  . 8D8D 54FFFFFF     LEA ECX,DWORD PTR SS:[EBP-AC]
0040305A  . 8985 34FFFFFF     MOV DWORD PTR SS:[EBP-CC],EAX
00403060  . 8985 44FFFFFF     MOV DWORD PTR SS:[EBP-BC],EAX
00403066  . C785 1CFFFFFF D02340 MOV DWORD PTR SS:[EBP-E4],abexcm2-.004023D0  UNICODE "Error!"
00403070  . FFD3              CALL EBX                                      <&MSVBVM60.__vbaVarDup>
00403072  . 8D95 24FFFFFF     LEA EDX,DWORD PTR SS:[EBP-DC]
00403078  . 8D8D 64FFFFFF     LEA ECX,DWORD PTR SS:[EBP-9C]
0040307E  . C785 2CFFFFFF 7C2340 MOV DWORD PTR SS:[EBP-D4],abexcm2-.0040237C  UNICODE "Please enter at least 4 char
00403088  . C785 24FFFFFF 080000 MOV DWORD PTR SS:[EBP-DC],8
00403092  . FFD3              CALL EBX
00403094  . 8D85 34FFFFFF     LEA EAX,DWORD PTR SS:[EBP-CC]
0040309A  . 8D8D 44FFFFFF     LEA ECX,DWORD PTR SS:[EBP-BC]
004030A0  . 50                PUSH EAX
004030A1  . 8D95 54FFFFFF     LEA EDX,DWORD PTR SS:[EBP-AC]
004030A7  . 51                PUSH ECX
004030A8  . 52                PUSH EDX
004030A9  . 8D85 64FFFFFF     LEA EAX,DWORD PTR
004030AF  . 57                PUSH EDI
004030B0  . 50                PUSH EAX
004030B1  . FF15 34104000     CALL DWORD PTR DS:                            MSVBVM60.rtcMsgBox
004030B7  . 8D95 E4FEFFFF     LEA EDX,DWORD PTR
004030BD  . 8D4D 9C           LEA ECX,DWORD PTR
004030C0  . 8985 ECFEFFFF     MOV DWORD PTR SS:[
004030C6  . C785 E4FEFFFF 030000 MOV DWORD PTR SS:[EBP-11C],3
004030D0  . FFD6              CALL ESI
004030D2  . 8D8D 34FFFFFF     LEA ECX,DWORD PTR SS:[EBP-CC]
004030D8  . 8D95 44FFFFFF     LEA EDX,DWORD PTR SS:[EBP-BC]
004030DE  . 51                PUSH ECX
004030DF  . 8D85 54FFFFFF     LEA EAX,DWORD PTR SS:[EBP-AC]
004030E5  . 52                PUSH EDX
004030E6  . 8D8D 64FFFFFF     LEA ECX,DWORD PTR SS:[EBP-9C]
004030EC  . 50                PUSH EAX
```

abex' 2nd crackme

Name: ab

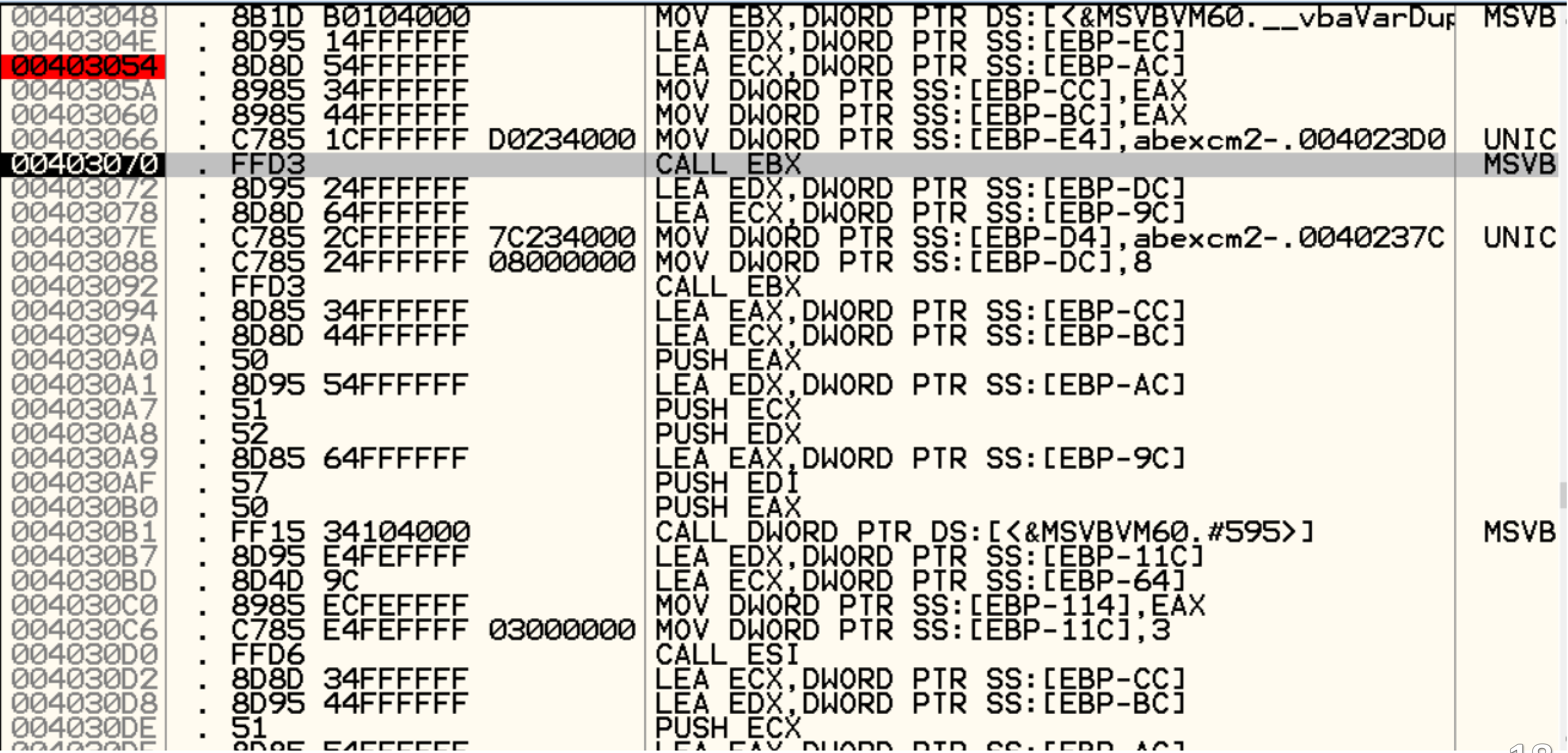
Serial: 1234

Part 3 스택 분석



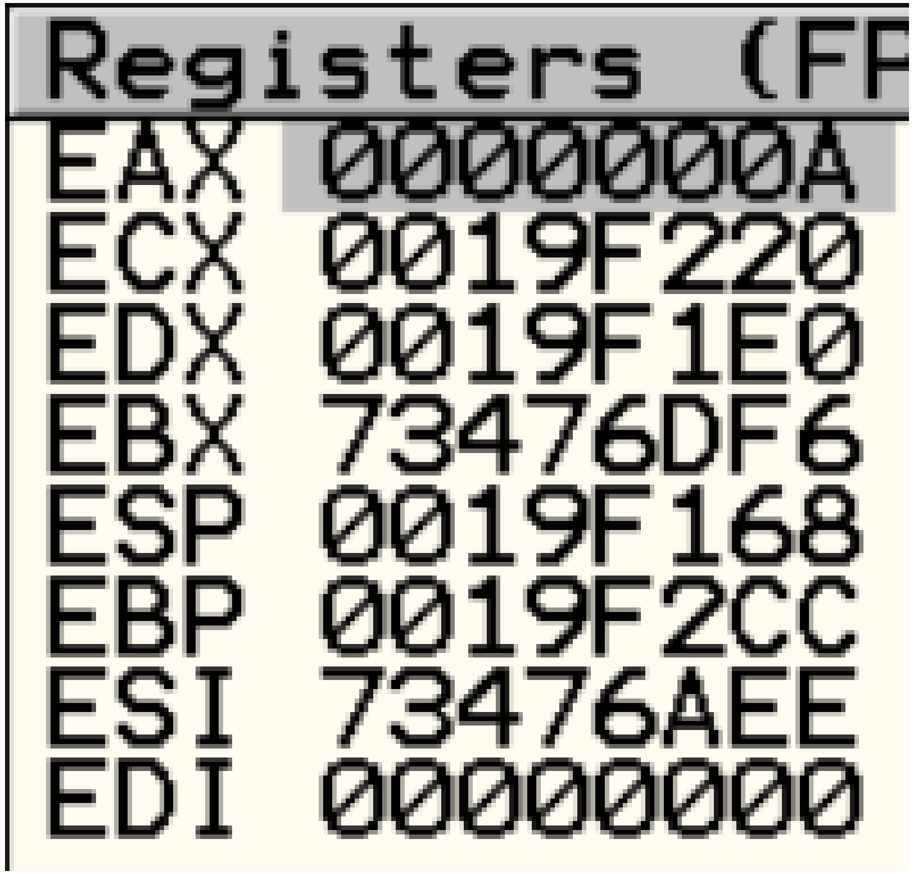
```
00403048  .  8B1D B0104000        MOV EBX,DWORD PTR DS:[<&MSVBVM60.__vbaVarDup   MSVBVM60.__vbaVarDup
0040304E  .  8D95 14FFFFFF        LEA EDX,DWORD PTR SS:[EBP-EC]
00403054  .  8D8D 54FFFFFF        LEA ECX,DWORD PTR SS:[EBP-AC]
0040305A  .  8985 34FFFFFF        MOV DWORD PTR SS:[EBP-CC],EAX
00403060  .  8985 44FFFFFF        MOV DWORD PTR SS:[EBP-BC],EAX
00403066  .  C785 1CFFFFFF D02340 MOV DWORD PTR SS:[EBP-E4],abexcm2-.004023D0   UNICODE "Error!"
00403070  .  FFD3                 CALL EBX                                       <&MSVBVM60.__vbaVarDup>
00403072  .  8D95 24FFFFFF        LEA EDX,DWORD PTR SS:[EBP-DC]
00403078  .  8D8D 64FFFFFF        LEA ECX,DWORD PTR SS:[EBP-9C]
0040307E  .  C785 2CFFFFFF 7C2340 MOV DWORD PTR SS:[EBP-D4],abexcm2-.0040237C   UNICODE "Please enter at least 4 chars
00403088  .  C785 24FFFFFF 080000 MOV DWORD PTR SS:[EBP-DC],8
00403092  .  FFD3                 CALL EBX
00403094  .  8D85 34FFFFFF        LEA EAX,DWORD PTR SS:[EBP-CC]
0040309A  .  8D8D 44FFFFFF        LEA ECX,DWORD PTR SS:[EBP-BC]
004030A0  .  50                   PUSH EAX
004030A1  .  8D95 54FFFFFF        LEA EDX,DWORD PTR SS:[EBP-AC]
004030A7  .  51                   PUSH ECX
004030A8  .  52                   PUSH EDX
004030A9  .  8D85 64FFFFFF        LEA EAX,DWORD PTR SS:[EBP-9C]
004030AF  .  57                   PUSH EDI
004030B0  .  50                   PUSH EAX
004030B1  .  FF15 34104000        CALL DWORD PTR DS:[<&MSVBVM60.#595>]           MSVBVM60.rtcMsgBox
004030B7  .  8D95 E4FEFFFF        LEA EDX,DWORD PTR SS:[EBP-11C]
004030BD  .  8D4D 9C              LEA ECX,DWORD PTR SS:[EBP-64]
004030C0  .  8985 ECFEFFFF        MOV DWORD PTR SS:[EBP-114],EAX
004030C6  .  C785 E4FEFFFF 030000 MOV DWORD PTR SS:[EBP-11C],3
004030D0  .  FFD6                 CALL ESI
004030D2  .  8D8D 34FFFFFF        LEA ECX,DWORD PTR SS:[EBP-CC]
004030D8  .  8D95 44FFFFFF        LEA EDX,DWORD PTR SS:[EBP-BC]
004030DE  .  51                   PUSH ECX
004030DF  .  8D85 54FFFFFF        LEA EAX,DWORD PTR SS:[EBP-AC]
004030E5  .  52                   PUSH EDX
004030E6  .  8D8D 64FFFFFF        LEA ECX,DWORD PTR SS:[EBP-9C]
004030EC  .  50                   PUSH EAX
```

Part 3 스택 분석



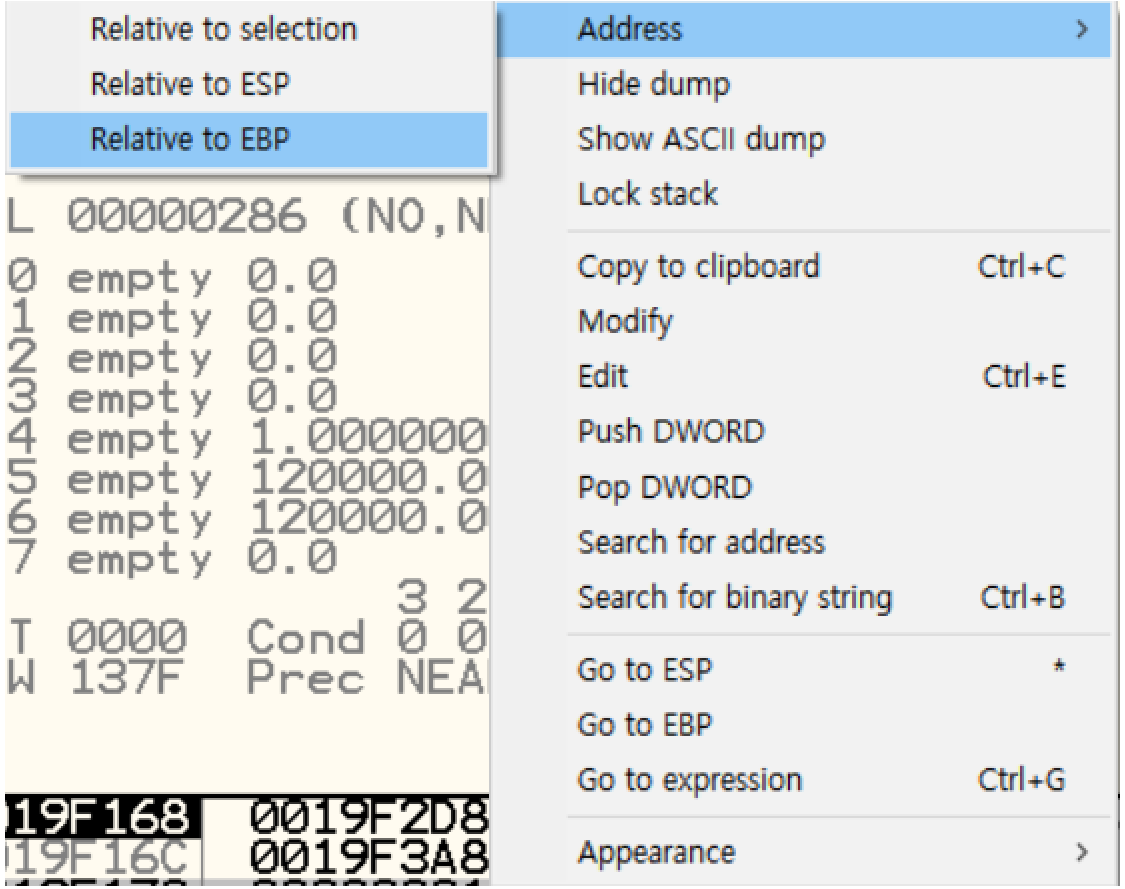
```
00403048  .  8B1D B0104000          MOV EBX,DWORD PTR DS:[<&MSVBVM60.__vbaVarDup  MSVB
0040304E  .  8D95 14FFFFFF          LEA EDX,DWORD PTR SS:[EBP-EC]
00403054  .  8D8D 54FFFFFF          LEA ECX,DWORD PTR SS:[EBP-AC]
0040305A  .  8985 34FFFFFF          MOV DWORD PTR SS:[EBP-CC],EAX
00403060  .  8985 44FFFFFF          MOV DWORD PTR SS:[EBP-BC],EAX
00403066  .  C785 1CFFFFFF D0234000 MOV DWORD PTR SS:[EBP-E4],abexcm2-.004023D0  UNIC
00403070  .  FFD3                   CALL EBX                                      MSVB
00403072  .  8D95 24FFFFFF          LEA EDX,DWORD PTR SS:[EBP-DC]
00403078  .  8D8D 64FFFFFF          LEA ECX,DWORD PTR SS:[EBP-9C]
0040307E  .  C785 2CFFFFFF 7C234000 MOV DWORD PTR SS:[EBP-D4],abexcm2-.0040237C  UNIC
00403088  .  C785 24FFFFFF 08000000 MOV DWORD PTR SS:[EBP-DC],8
00403092  .  FFD3                   CALL EBX
00403094  .  8D85 34FFFFFF          LEA EAX,DWORD PTR SS:[EBP-CC]
0040309A  .  8D8D 44FFFFFF          LEA ECX,DWORD PTR SS:[EBP-BC]
004030A0  .  50                     PUSH EAX
004030A1  .  8D95 54FFFFFF          LEA EDX,DWORD PTR SS:[EBP-AC]
004030A7  .  51                     PUSH ECX
004030A8  .  52                     PUSH EDX
004030A9  .  8D85 64FFFFFF          LEA EAX,DWORD PTR SS:[EBP-9C]
004030AF  .  57                     PUSH EDI
004030B0  .  50                     PUSH EAX
004030B1  .  FF15 34104000          CALL DWORD PTR DS:[<&MSVBVM60.#595>]          MSVB
004030B7  .  8D95 E4FEFFFF          LEA EDX,DWORD PTR SS:[EBP-11C]
004030BD  .  8D4D 9C                LEA ECX,DWORD PTR SS:[EBP-64]
004030C0  .  8985 ECFEFFFF          MOV DWORD PTR SS:[EBP-114],EAX
004030C6  .  C785 E4FEFFFF 03000000 MOV DWORD PTR SS:[EBP-11C],3
004030D0  .  FFD6                   CALL ESI
004030D2  .  8D8D 34FFFFFF          LEA ECX,DWORD PTR SS:[EBP-CC]
004030D8  .  8D95 44FFFFFF          LEA EDX,DWORD PTR SS:[EBP-BC]
004030DE  .  51                     PUSH ECX
004030DF  .  8D85 54FFFFFF          LEA EAX,DWORD PTR SS:[EBP-AC]
```

스택 분석

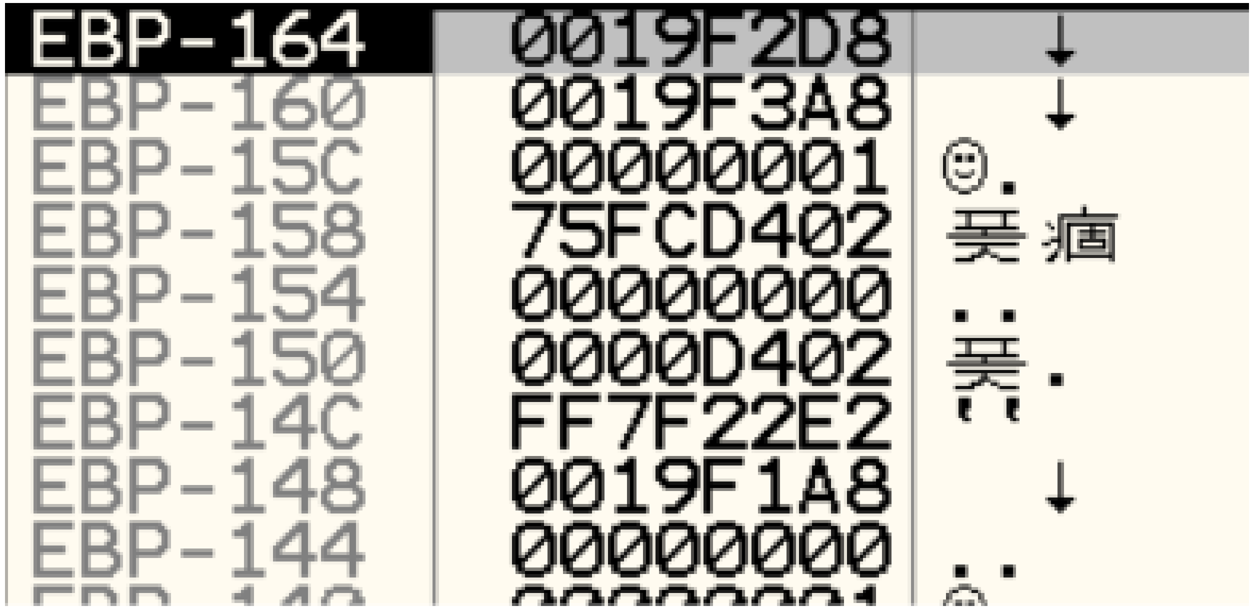


```
Registers (FP
EAX 0000000A
ECX 0019F220
EDX 0019F1E0
EBX 73476DF6
ESP 0019F168
EBP 0019F2CC
ESI 73476AEE
EDI 00000000
```

Part 3 스택 분석



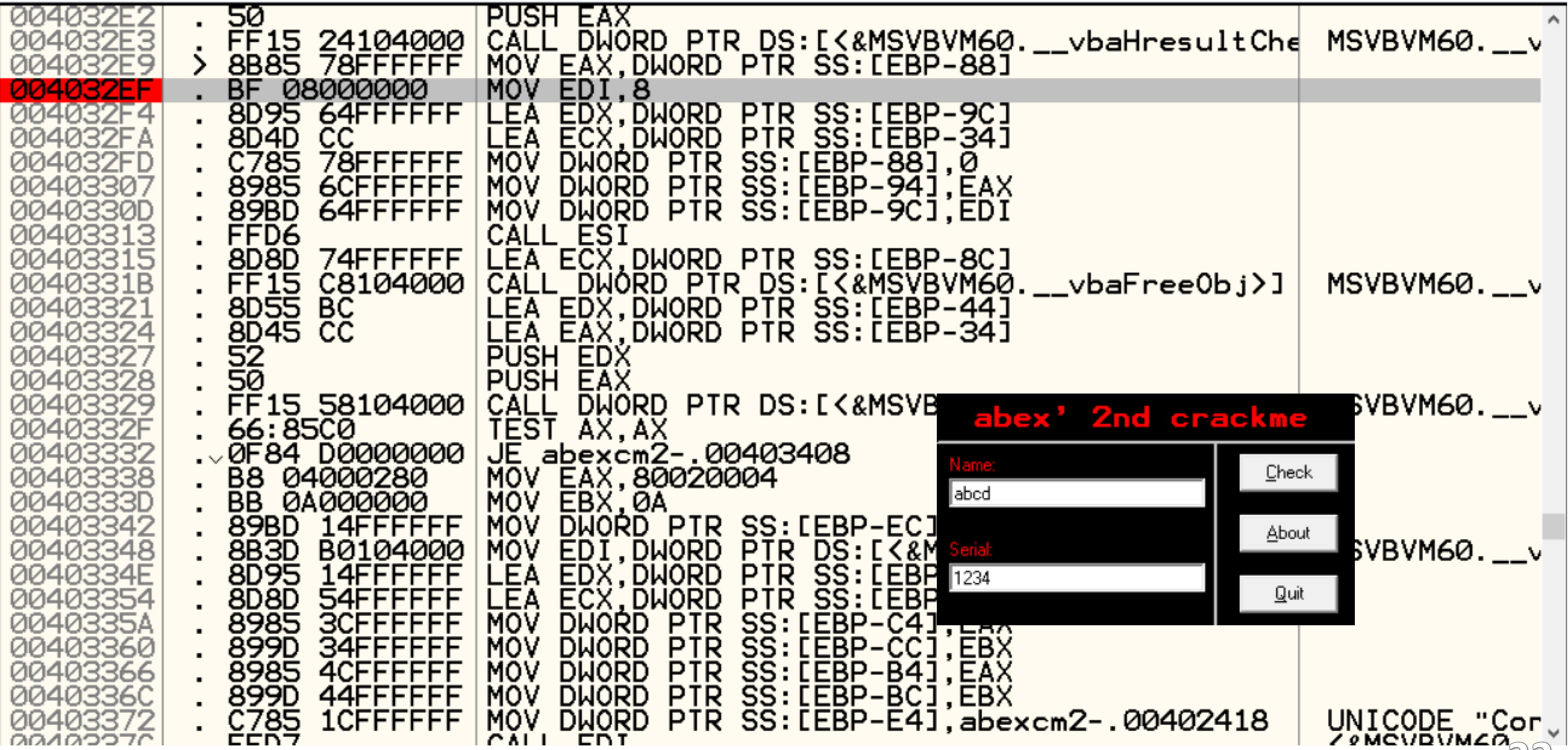
```
L 00000286 (NO,N
0 empty 0.0
1 empty 0.0
2 empty 0.0
3 empty 0.0
4 empty 1.000000
5 empty 120000.0
6 empty 120000.0
7 empty 0.0
                3 2
T 0000   Cond 0 0
W 137F   Prec NEA
19F168   0019F2D8
19F16C   0019F3A8
```



```
EBP-164   0019F2D8   ↓
EBP-160   0019F3A8   ↓
EBP-15C   00000001  ☺.
EBP-158   75FCD402  昊 酒
EBP-154   00000000  ..
EBP-150   0000D402  昊.
EBP-14C   FF7F22E2
EBP-148   0019F1A8   ↓
EBP-144   00000000  ..
```

문제해결

Part 4 문제해결



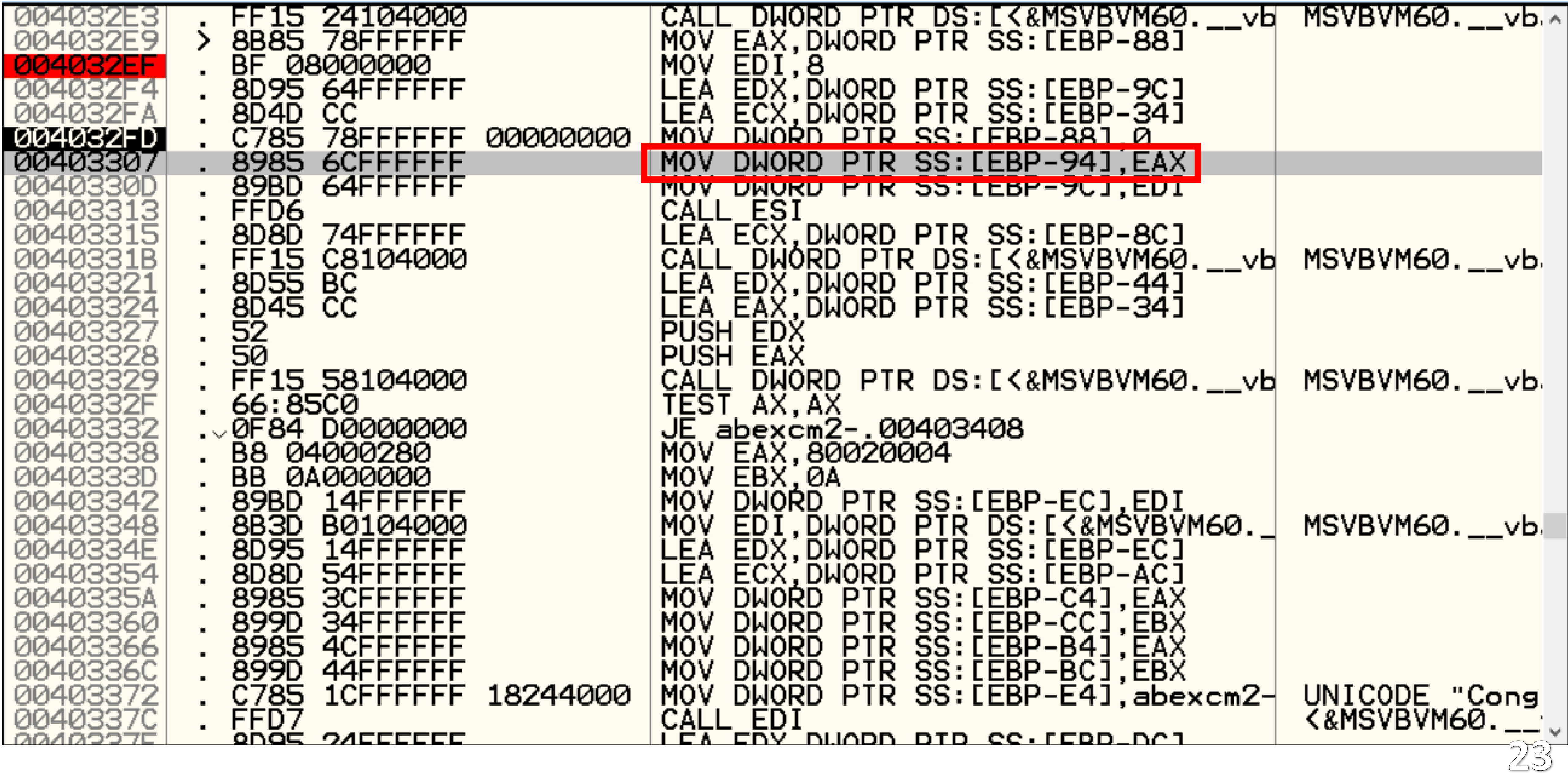
```
004032E2  .  50             PUSH EAX
004032E3  .  FF15 24104000  CALL DWORD PTR DS:[<&MSVBVM60.__vbaHresultChe   MSVBVM60.__v
004032E9  >  8B85 78FFFFFF  MOV EAX,DWORD PTR SS:[EBP-88]
004032EF  .  BF 08000000    MOV EDI,8
004032F4  .  8D95 64FFFFFF  LEA EDX,DWORD PTR SS:[EBP-9C]
004032FA  .  8D4D CC        LEA ECX,DWORD PTR SS:[EBP-34]
004032FD  .  C785 78FFFFFF  MOV DWORD PTR SS:[EBP-88],0
00403307  .  8985 6CFFFFFF  MOV DWORD PTR SS:[EBP-94],EAX
0040330D  .  89BD 64FFFFFF  MOV DWORD PTR SS:[EBP-9C],EDI
00403313  .  FFD6           CALL ESI
00403315  .  8D8D 74FFFFFF  LEA ECX,DWORD PTR SS:[EBP-8C]
0040331B  .  FF15 C8104000  CALL DWORD PTR DS:[<&MSVBVM60.__vbaFreeObj>]    MSVBVM60.__v
00403321  .  8D55 BC        LEA EDX,DWORD PTR SS:[EBP-44]
00403324  .  8D45 CC        LEA EAX,DWORD PTR SS:[EBP-34]
00403327  .  52             PUSH EDX
00403328  .  50             PUSH EAX
00403329  .  FF15 58104000  CALL DWORD PTR DS:[<&MSVB                        SVBVM60.__v
0040332F  .  66:85C0        TEST AX,AX
00403332  .v 0F84 D0000000  JE abexcm2-.00403408
00403338  .  B8 04000280    MOV EAX,80020004
0040333D  .  BB 0A000000    MOV EBX,0A
00403342  .  89BD 14FFFFFF  MOV DWORD PTR SS:[EBP-EC]
00403348  .  8B3D B0104000  MOV EDI,DWORD PTR DS:[<&M                        SVBVM60.__v
0040334E  .  8D95 14FFFFFF  LEA EDX,DWORD PTR SS:[EBP
00403354  .  8D8D 54FFFFFF  LEA ECX,DWORD PTR SS:[EBP
0040335A  .  8985 3CFFFFFF  MOV DWORD PTR SS:[EBP-C4],EAX
00403360  .  899D 34FFFFFF  MOV DWORD PTR SS:[EBP-CC],EBX
00403366  .  8985 4CFFFFFF  MOV DWORD PTR SS:[EBP-B4],EAX
0040336C  .  899D 44FFFFFF  MOV DWORD PTR SS:[EBP-BC],EBX
00403372  .  C785 1CFFFFFF  MOV DWORD PTR SS:[EBP-E4],abexcm2-.00402418   UNICODE "Cor
0040337C  .  FFD7           CALL EDI                                      <&MSVBVM60
```

abex' 2nd crackme

Name: abcd

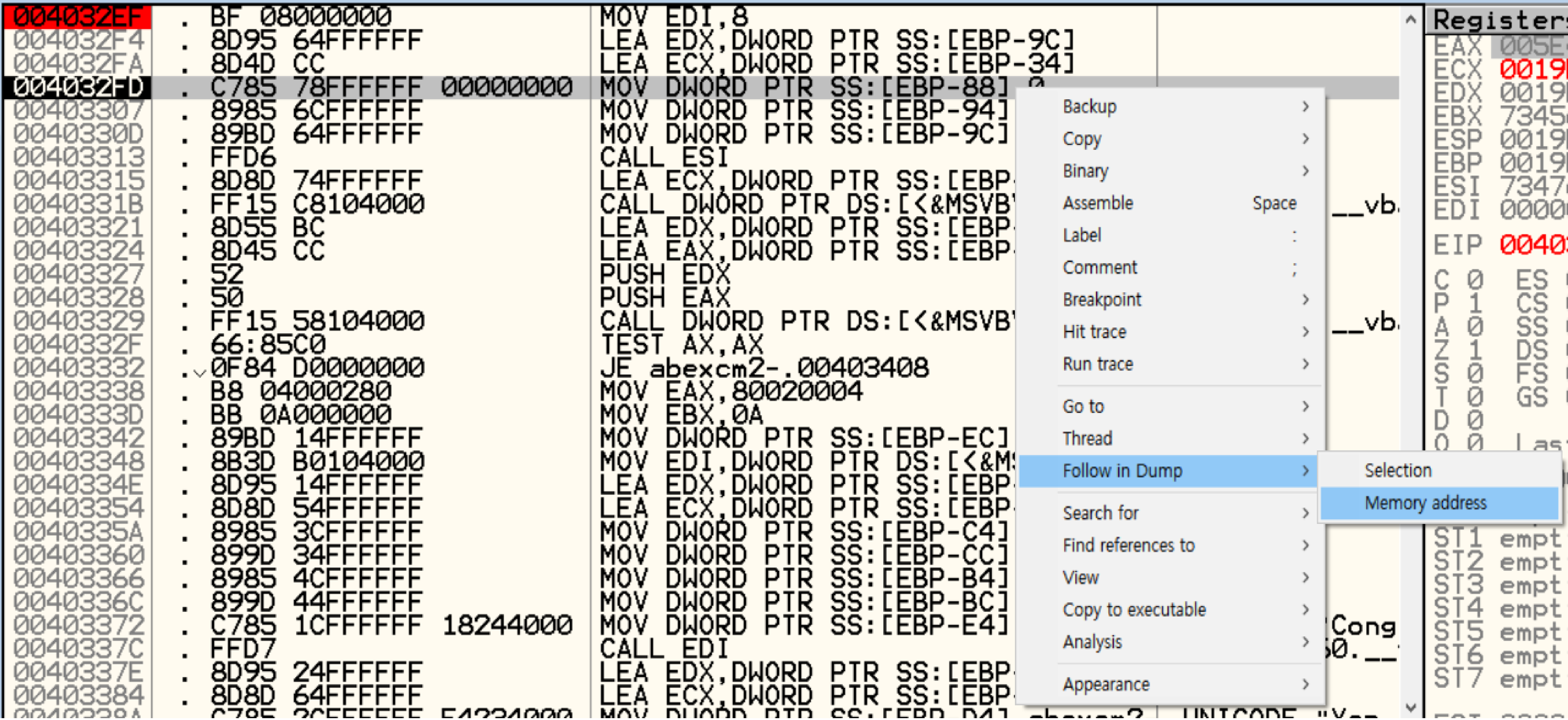
Serial: 1234

Part 4 문제해결



```
004032E3  .  FF15 24104000      CALL DWORD PTR DS:[<&MSVBVM60.__vb   MSVBVM60.__vb.
004032E9  >  8B85 78FFFFFF      MOV EAX,DWORD PTR SS:[EBP-88]
004032EF  .  BF 08000000        MOV EDI,8
004032F4  .  8D95 64FFFFFF      LEA EDX,DWORD PTR SS:[EBP-9C]
004032FA  .  8D4D CC            LEA ECX,DWORD PTR SS:[EBP-34]
004032FD  .  C785 78FFFFFF 00000000  MOV DWORD PTR SS:[EBP-88],0
00403307  .  8985 6CFFFFFF      MOV DWORD PTR SS:[EBP-94],EAX
0040330D  .  89BD 64FFFFFF      MOV DWORD PTR SS:[EBP-9C],EDI
00403313  .  FFD6               CALL ESI
00403315  .  8D8D 74FFFFFF      LEA ECX,DWORD PTR SS:[EBP-8C]
0040331B  .  FF15 C8104000      CALL DWORD PTR DS:[<&MSVBVM60.__vb   MSVBVM60.__vb.
00403321  .  8D55 BC            LEA EDX,DWORD PTR SS:[EBP-44]
00403324  .  8D45 CC            LEA EAX,DWORD PTR SS:[EBP-34]
00403327  .  52                 PUSH EDX
00403328  .  50                 PUSH EAX
00403329  .  FF15 58104000      CALL DWORD PTR DS:[<&MSVBVM60.__vb   MSVBVM60.__vb.
0040332F  .  66:85C0            TEST AX,AX
00403332  .v 0F84 D0000000      JE abexcm2-.00403408
00403338  .  B8 04000280        MOV EAX,80020004
0040333D  .  BB 0A000000        MOV EBX,0A
00403342  .  89BD 14FFFFFF      MOV DWORD PTR SS:[EBP-EC],EDI
00403348  .  8B3D B0104000      MOV EDI,DWORD PTR DS:[<&MSVBVM60._   MSVBVM60.__vb.
0040334E  .  8D95 14FFFFFF      LEA EDX,DWORD PTR SS:[EBP-EC]
00403354  .  8D8D 54FFFFFF      LEA ECX,DWORD PTR SS:[EBP-AC]
0040335A  .  8985 3CFFFFFF      MOV DWORD PTR SS:[EBP-C4],EAX
00403360  .  899D 34FFFFFF      MOV DWORD PTR SS:[EBP-CC],EBX
00403366  .  8985 4CFFFFFF      MOV DWORD PTR SS:[EBP-B4],EAX
0040336C  .  899D 44FFFFFF      MOV DWORD PTR SS:[EBP-BC],EBX
00403372  .  C785 1CFFFFFF 18244000  MOV DWORD PTR SS:[EBP-E4],abexcm2-   UNICODE "Cong
0040337C  .  FFD7               CALL EDI                             <&MSVBVM60.__
0040337E  .  8D95 24FFFFFF      LEA EDX,DWORD PTR SS:[EBP-DC]
```

문제해결



```
004032EF  .  BF 08000000           MOV EDI,8
004032F4  .  8D95 64FFFFFF         LEA EDX,DWORD PTR SS:[EBP-9C]
004032FA  .  8D4D CC               LEA ECX,DWORD PTR SS:[EBP-34]
004032FD  .  C785 78FFFFFF 00000000 MOV DWORD PTR SS:[EBP-88],0
00403307  .  8985 6CFFFFFF         MOV DWORD PTR SS:[EBP-94]
0040330D  .  89BD 64FFFFFF         MOV DWORD PTR SS:[EBP-9C]
00403313  .  FFD6                  CALL ESI
00403315  .  8D8D 74FFFFFF         LEA ECX,DWORD PTR SS:[EBP
0040331B  .  FF15 C8104000         CALL DWORD PTR DS:[<&MSVB'     __vb.
00403321  .  8D55 BC               LEA EDX,DWORD PTR SS:[EBP
00403324  .  8D45 CC               LEA EAX,DWORD PTR SS:[EBP
00403327  .  52                    PUSH EDX
00403328  .  50                    PUSH EAX
00403329  .  FF15 58104000         CALL DWORD PTR DS:[<&MSVB'     __vb.
0040332F  .  66:85C0               TEST AX,AX
00403332  .v 0F84 D0000000         JE abexcm2-.00403408
00403338  .  B8 04000280           MOV EAX,80020004
0040333D  .  BB 0A000000           MOV EBX,0A
00403342  .  89BD 14FFFFFF         MOV DWORD PTR SS:[EBP-EC]
00403348  .  8B3D B0104000         MOV EDI,DWORD PTR DS:[<&M
0040334E  .  8D95 14FFFFFF         LEA EDX,DWORD PTR SS:[EBP
00403354  .  8D8D 54FFFFFF         LEA ECX,DWORD PTR SS:[EBP
0040335A  .  8985 3CFFFFFF         MOV DWORD PTR SS:[EBP-C4]
00403360  .  899D 34FFFFFF         MOV DWORD PTR SS:[EBP-CC]
00403366  .  8985 4CFFFFFF         MOV DWORD PTR SS:[EBP-B4]
0040336C  .  899D 44FFFFFF         MOV DWORD PTR SS:[EBP-BC]
00403372  .  C785 1CFFFFFF 18244000 MOV DWORD PTR SS:[EBP-E4]     'Cong
0040337C  .  FFD7                  CALL EDI                       0.__
0040337E  .  8D95 24FFFFFF         LEA EDX,DWORD PTR SS:[EBP
00403384  .  8D8D 64FFFFFF         LEA ECX,DWORD PTR SS:[EBP
```

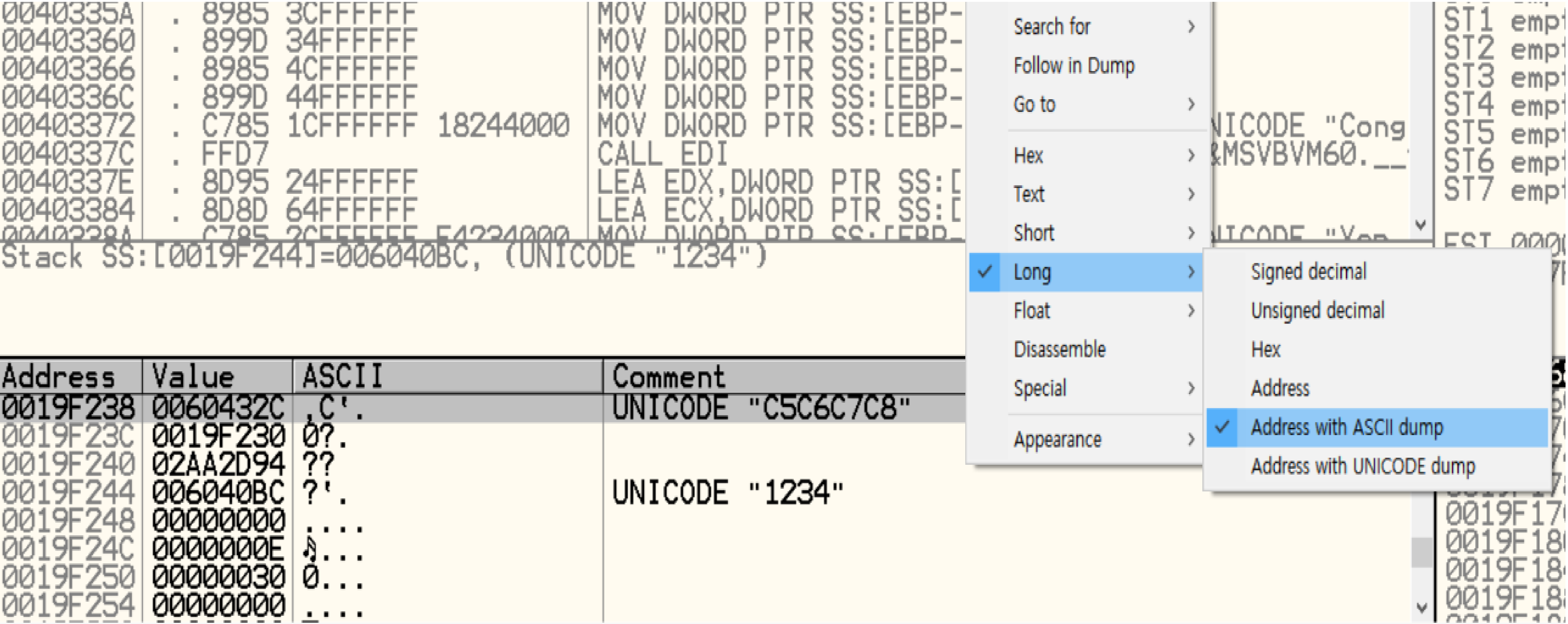
```
Registers
EAX 005E
ECX 0019
EDX 0019
EBX 7345
ESP 0019
EBP 0019
ESI 7347
EDI 0000

EIP 0040

C 0  ES
P 1  CS
A 0  SS
Z 1  DS
S 0  FS
T 0  GS
D 0
O 0  Las

ST1 empt
ST2 empt
ST3 empt
ST4 empt
ST5 empt
ST6 empt
ST7 empt
```

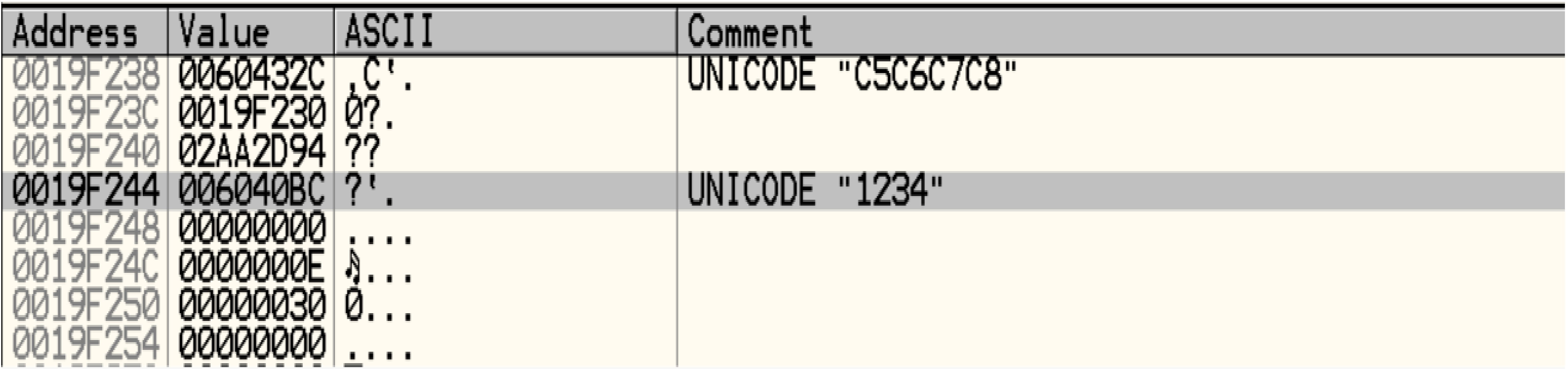
Part 4 문제해결



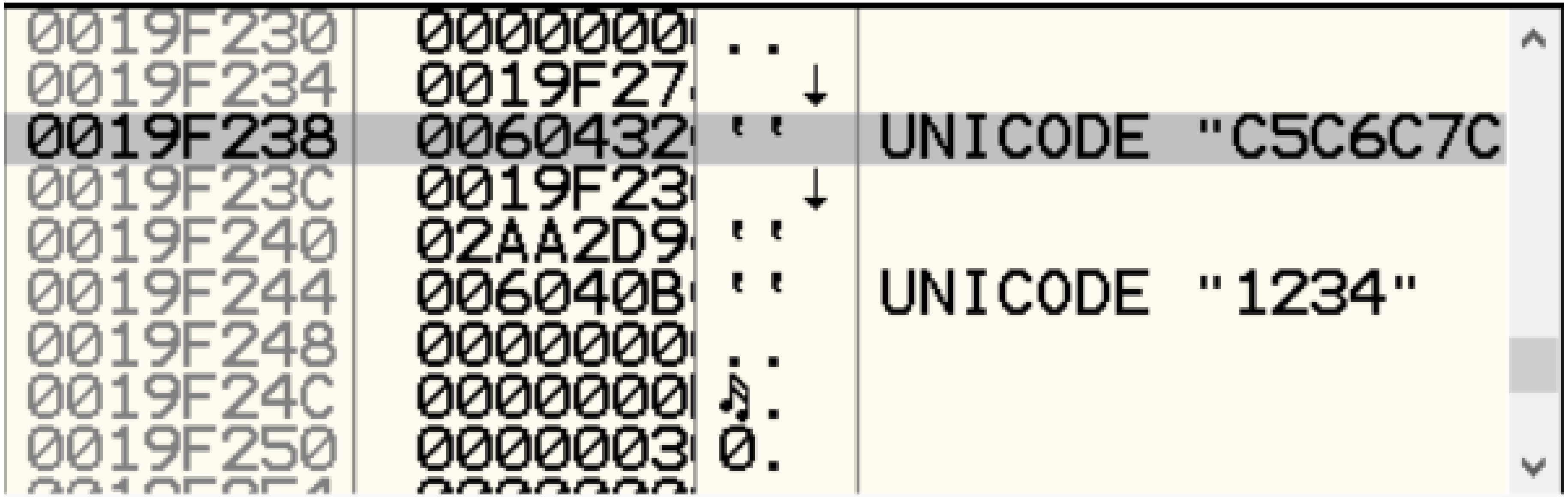
```
0040335A  .  8985 3CFFFFFF           MOV DWORD PTR SS:[EBP-
00403360  .  899D 34FFFFFF           MOV DWORD PTR SS:[EBP-
00403366  .  8985 4CFFFFFF           MOV DWORD PTR SS:[EBP-
0040336C  .  899D 44FFFFFF           MOV DWORD PTR SS:[EBP-
00403372  .  C785 1CFFFFFF 18244000  MOV DWORD PTR SS:[EBP-     NICODE "Cong
0040337C  .  FFD7                    CALL EDI                   &MSVBVM60.__
0040337E  .  8D95 24FFFFFF           LEA EDX,DWORD PTR SS:[
00403384  .  8D8D 64FFFFFF           LEA ECX,DWORD PTR SS:[
Stack SS:[0019F244]=006040BC, (UNICODE "1234")
```

```
ST1 empt
ST2 empt
ST3 empt
ST4 empt
ST5 empt
ST6 empt
ST7 empt
```

```
Address   Value     ASCII  Comment
0019F238  0060432C  ,C'.   UNICODE "C5C6C7C8"
0019F23C  0019F230  0?.
0019F240  02AA2D94  ??
0019F244  006040BC  ?'.    UNICODE "1234"
0019F248  00000000  ....
0019F24C  0000000E  ♫...
0019F250  00000030  0...
0019F254  00000000  ....
```

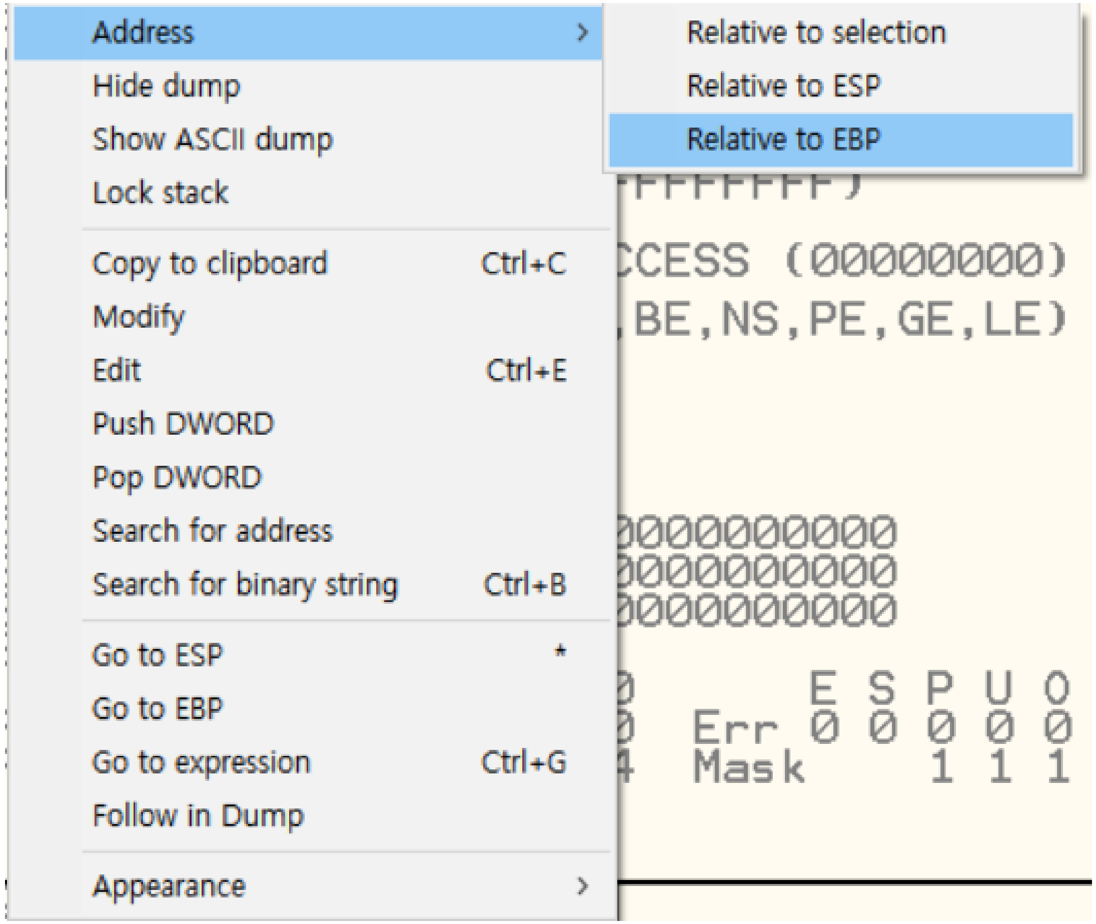


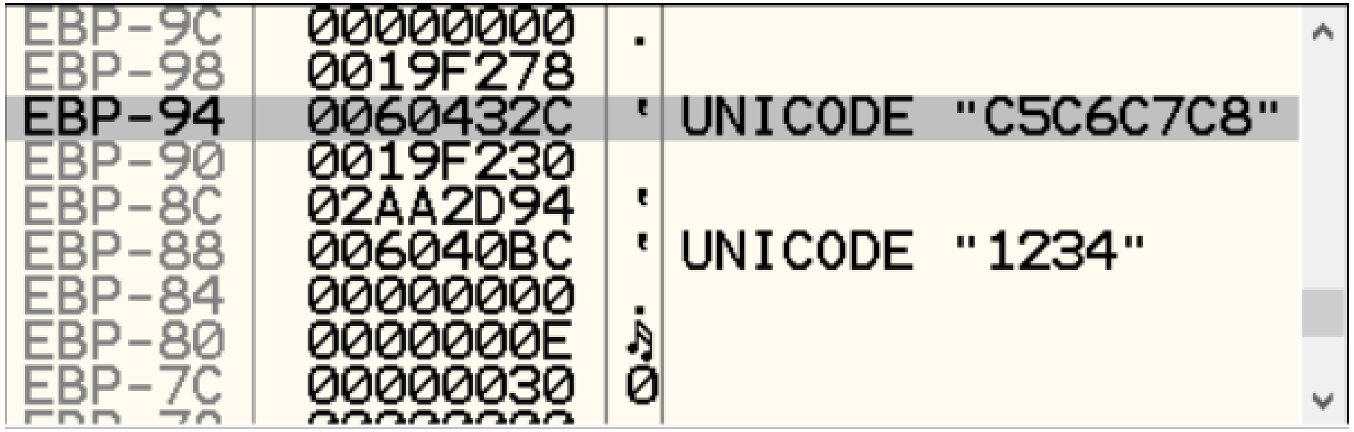
```
Address   Value     ASCII    Comment
0019F238  0060432C  ,C'.     UNICODE "C5C6C7C8"
0019F23C  0019F230  0?.
0019F240  02AA2D94  ??
0019F244  006040BC  ?'.      UNICODE "1234"
0019F248  00000000  ....
0019F24C  0000000E  ♪...
0019F250  00000030  0...
0019F254  00000000  ....
```



```
0019F230   0000000   ..
0019F234   0019F27     ↓
0019F238   0060432   ''   UNICODE "C5C6C7C
0019F23C   0019F23     ↓
0019F240   02AA2D9   ''
0019F244   006040B   ''   UNICODE "1234"
0019F248   0000000   ..
0019F24C   0000000  ♪.
0019F250   0000003  0.
```

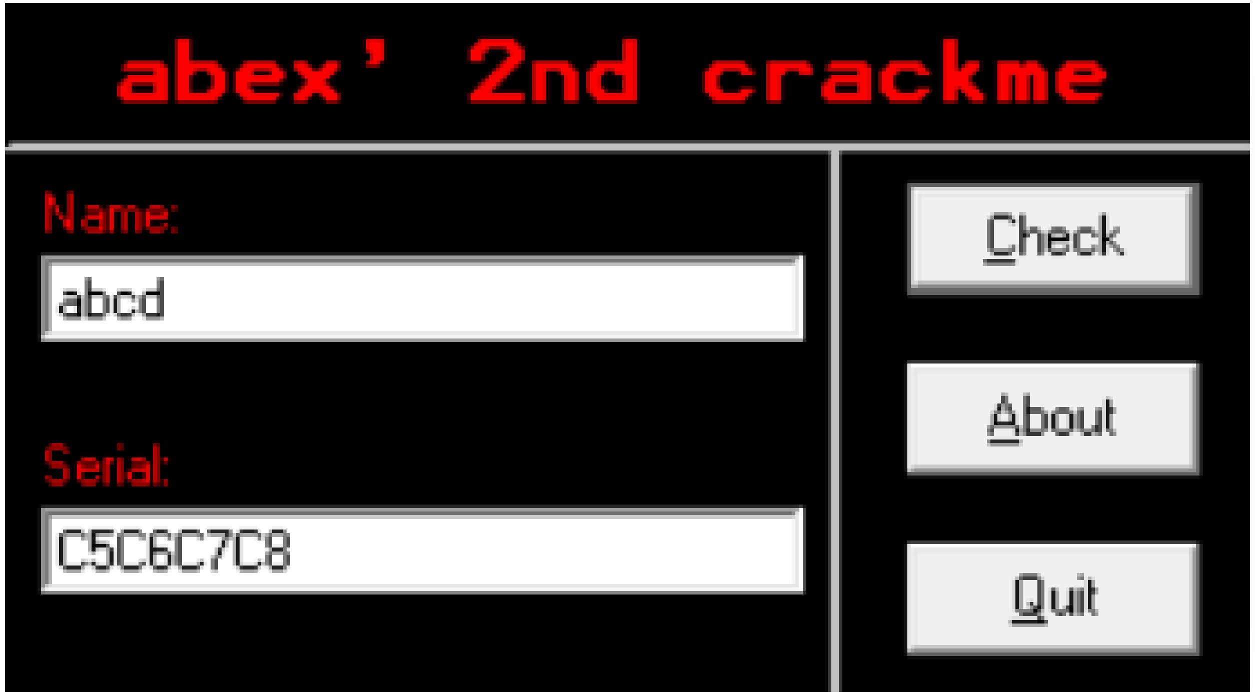
Part 4 문제해결





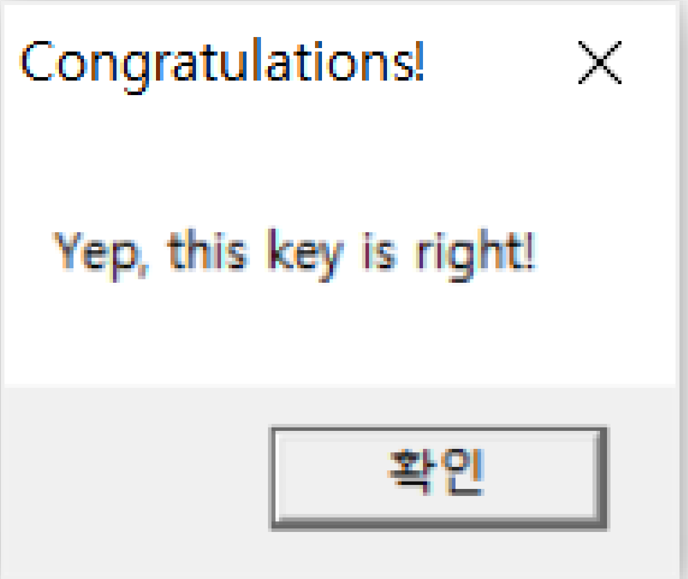
```
EBP-9C   00000000  .
EBP-98   0019F278
EBP-94   0060432C  '  UNICODE "C5C6C7C8"
EBP-90   0019F230
EBP-8C   02AA2D94  '
EBP-88   006040BC  '  UNICODE "1234"
EBP-84   00000000  .
EBP-80   0000000E  ♫
EBP-7C   00000030  0
```

Part 4 문제해결


abex' 2nd crackme

Name: abcd

Serial: C5C6C7C8


Congratulations!

Yep, this key is right!

Q&A