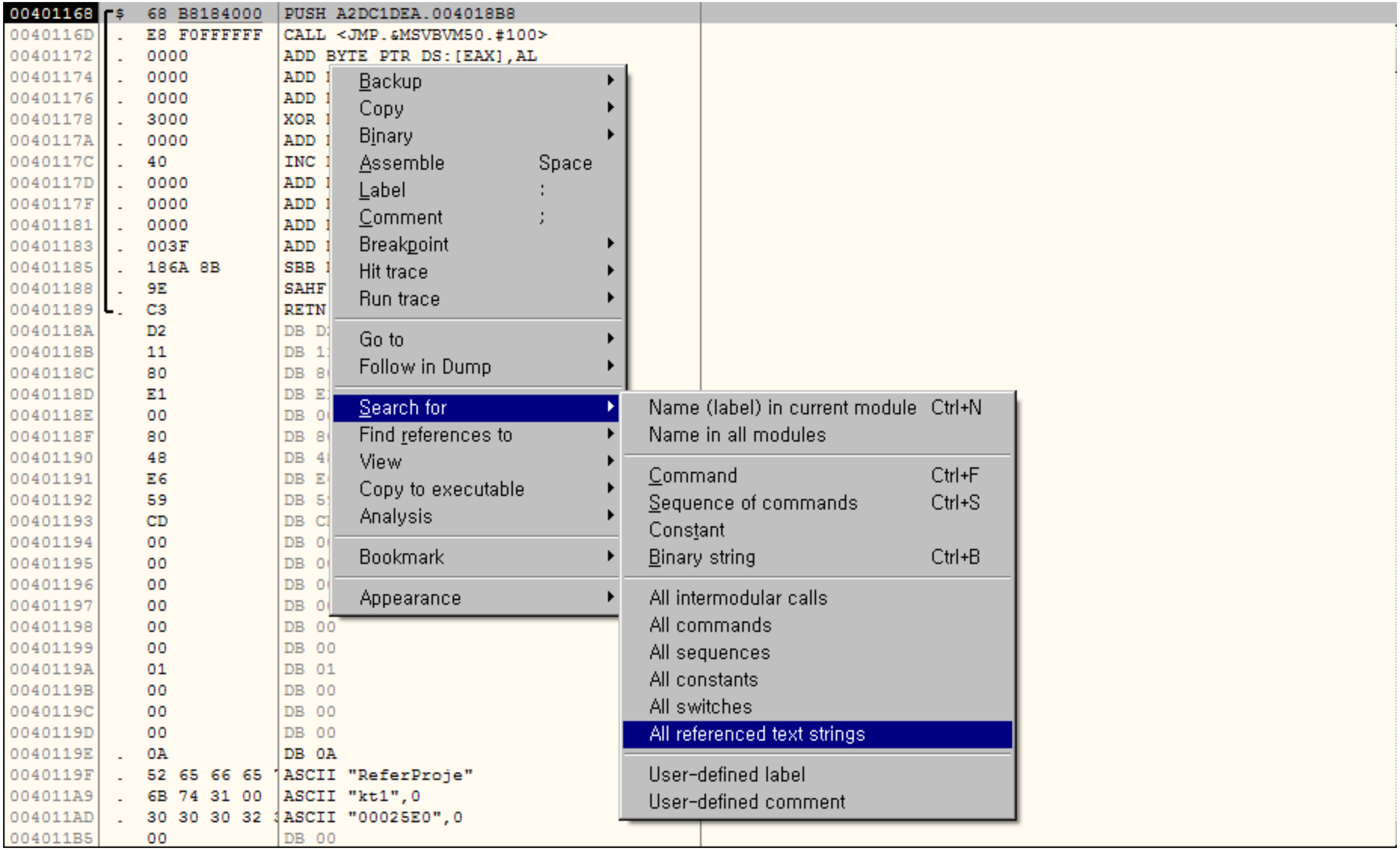
Reverseing No3

model9c@gmail.com

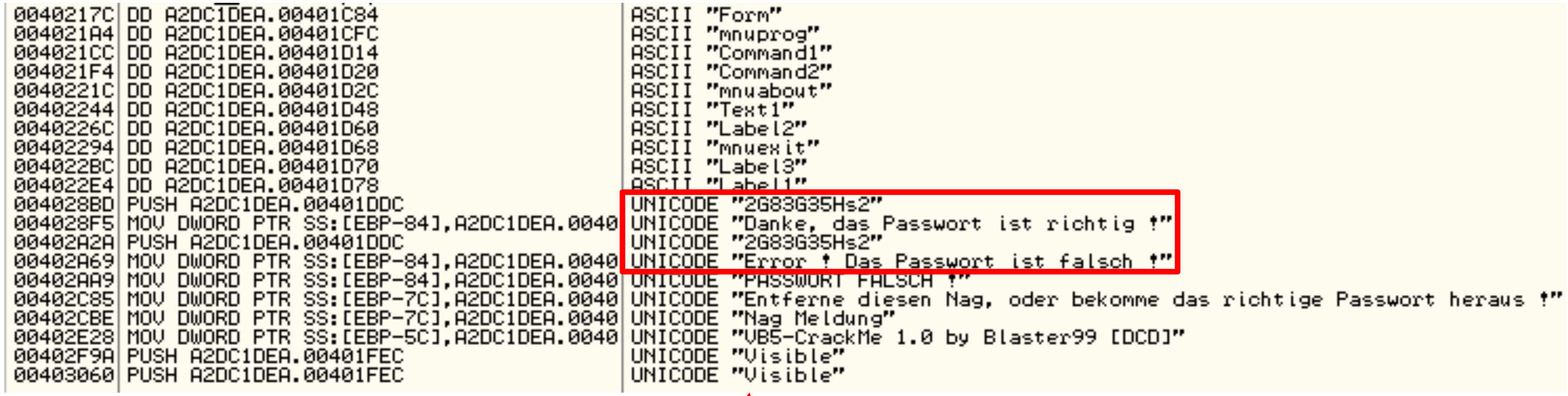
ID : bluetail



```
00401168 ┌$  68 B8184000   PUSH A2DC1DEA.004018B8
0040116D │.  E8 F0FFFFFF   CALL <JMP.&MSVBVM50.#100>
00401172 │.  0000          ADD BYTE PTR DS:[EAX],AL
00401174 │.  0000          ADD I
00401176 │.  0000          ADD I
00401178 │.  3000          XOR I
0040117A │.  0000          ADD I
0040117C │.  40            INC I
0040117D │.  0000          ADD I
0040117F │.  0000          ADD I
00401181 │.  0000          ADD I
00401183 │.  003F          ADD I
00401185 │.  186A 8B       SBB I
00401188 │.  9E            SAHF
00401189 └.  C3            RETN
0040118A     D2            DB D
0040118B     11            DB 1
0040118C     80            DB 8
0040118D     E1            DB E
0040118E     00            DB 0
0040118F     80            DB 8
00401190     48            DB 4
00401191     E6            DB E
00401192     59            DB 5
00401193     CD            DB C
00401194     00            DB 0
00401195     00            DB 0
00401196     00            DB 0
00401197     00            DB 0
00401198     00            DB 00
00401199     00            DB 00
0040119A     01            DB 01
0040119B     00            DB 00
0040119C     00            DB 00
0040119D     00            DB 00
0040119E  .  0A            DB 0A
0040119F  .  52 65 66 65   ASCII "ReferProje"
004011A9  .  6B 74 31 00   ASCII "kt1",0
004011AD  .  30 30 30 32   ASCII "00025E0",0
004011B5     00            DB 00
```

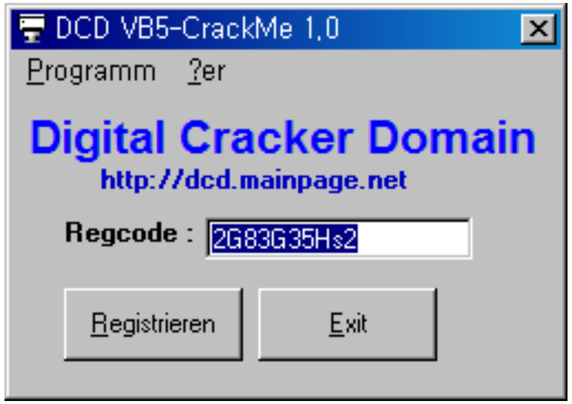
1. 프로그램에 사용된 문자열을 검색한다.

==우 클릭->Search for->All references text strings

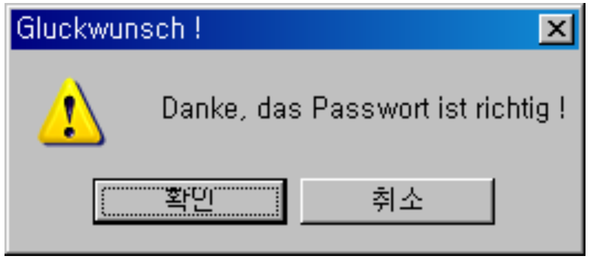


```
0040217C DD A2DC1DEA.00401C84                    ASCII "Form"
004021A4 DD A2DC1DEA.00401CFC                    ASCII "mnuprog"
004021CC DD A2DC1DEA.00401D14                    ASCII "Command1"
004021F4 DD A2DC1DEA.00401D20                    ASCII "Command2"
0040221C DD A2DC1DEA.00401D2C                    ASCII "mnuabout"
00402244 DD A2DC1DEA.00401D48                    ASCII "Text1"
0040226C DD A2DC1DEA.00401D60                    ASCII "Label2"
00402294 DD A2DC1DEA.00401D68                    ASCII "mnuexit"
004022BC DD A2DC1DEA.00401D70                    ASCII "Label3"
004022E4 DD A2DC1DEA.00401D78                    ASCII "Label1"
004028BD PUSH A2DC1DEA.00401DDC                  UNICODE "2G83G35Hs2"
004028F5 MOV DWORD PTR SS:[EBP-84],A2DC1DEA.0040 UNICODE "Danke, das Passwort ist richtig !"
00402A2A PUSH A2DC1DEA.00401DDC                  UNICODE "2G83G35Hs2"
00402A69 MOV DWORD PTR SS:[EBP-84],A2DC1DEA.0040 UNICODE "Error ! Das Passwort ist falsch !"
00402AA9 MOV DWORD PTR SS:[EBP-84],A2DC1DEA.0040 UNICODE "PASSWORT FALSCH !"
00402C85 MOV DWORD PTR SS:[EBP-7C],A2DC1DEA.0040 UNICODE "Entferne diesen Nag, oder bekomme das richtige Passwort heraus !"
00402CBE MOV DWORD PTR SS:[EBP-7C],A2DC1DEA.0040 UNICODE "Nag Meldung"
00402E28 MOV DWORD PTR SS:[EBP-5C],A2DC1DEA.0040 UNICODE "VB5-CrackMe 1.0 by Blaster99 [DCD]"
00402F9A PUSH A2DC1DEA.00401FEC                  UNICODE "Visible"
00403060 PUSH A2DC1DEA.00401FEC                  UNICODE "Visible"
```

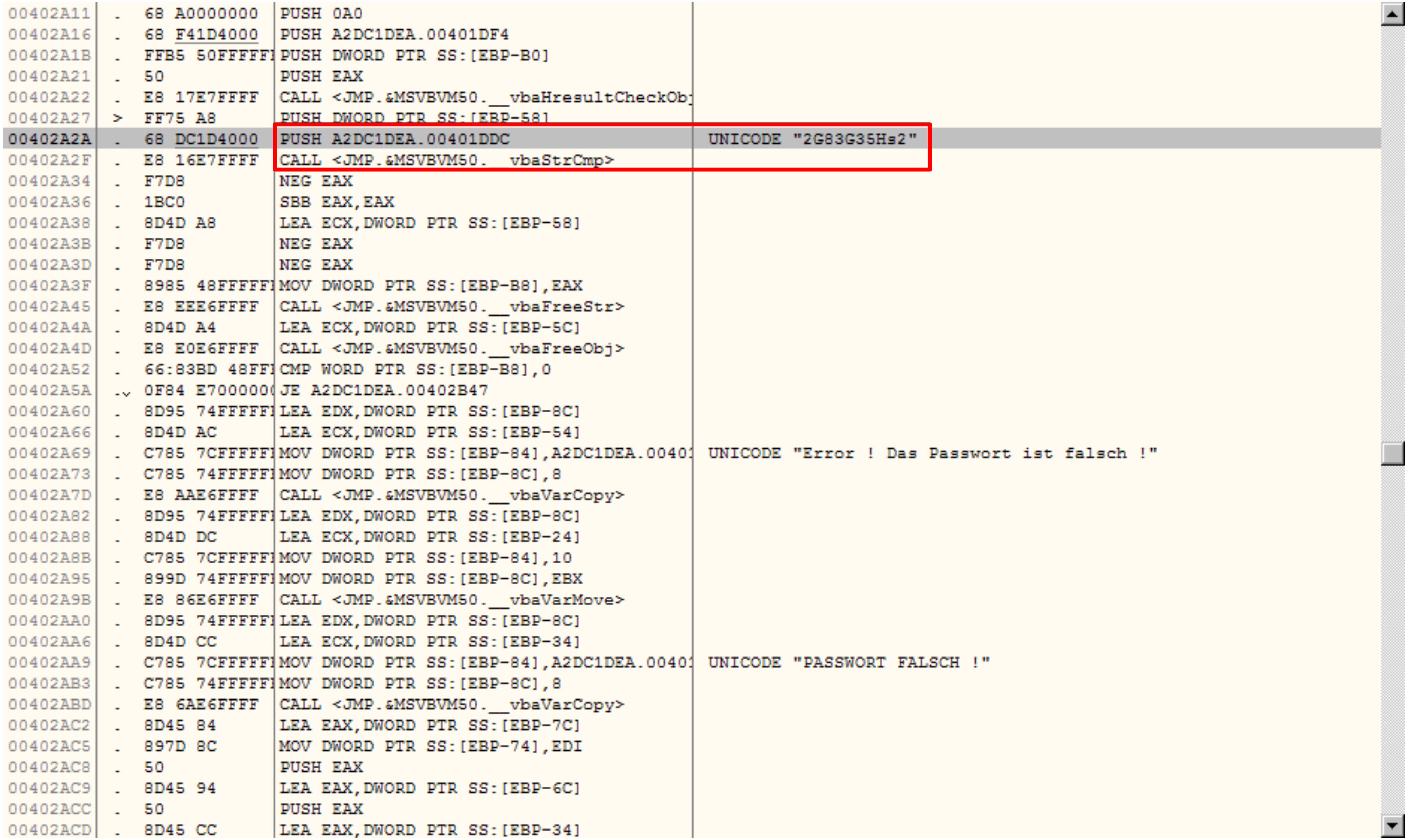
이 부분이 문자열을 비교하는 데 사용되는 것 같았다.
조건은 “2G83G35Hs2” 이고 이 문자열이 password.
즉 이 문자열이 어디서 사용되는지 찾아간다면
문자열을 비교하는 함수를 찾을 수 있다.



Regcode : 2G83G35Hs2



Danke, das Passwort ist richtig !



```
00402A11 .   68 A0000000  PUSH 0A0
00402A16 .   68 F41D4000  PUSH A2DC1DEA.00401DF4
00402A1B .   FFB5 50FFFFF PUSH DWORD PTR SS:[EBP-B0]
00402A21 .   50           PUSH EAX
00402A22 .   E8 17E7FFFF  CALL <JMP.&MSVBVM50.__vbaHresultCheckObj
00402A27 >   FF75 A8      PUSH DWORD PTR SS:[EBP-58]
00402A2A .   68 DC1D4000  PUSH A2DC1DEA.00401DDC                   UNICODE "2G83G35Hs2"
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 48FFFFF 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 48FF CMP WORD PTR SS:[EBP-B8],0
00402A5A .v  0F84 E700000 JE A2DC1DEA.00402B47
00402A60 .   8D95 74FFFFF LEA EDX,DWORD PTR SS:[EBP-8C]
00402A66 .   8D4D AC      LEA ECX,DWORD PTR SS:[EBP-54]
00402A69 .   C785 7CFFFFF MOV DWORD PTR SS:[EBP-84],A2DC1DEA.0040  UNICODE "Error ! Das Passwort ist falsch !"
00402A73 .   C785 74FFFFF MOV DWORD PTR SS:[EBP-8C],8
00402A7D .   E8 AAE6FFFF  CALL <JMP.&MSVBVM50.__vbaVarCopy>
00402A82 .   8D95 74FFFFF LEA EDX,DWORD PTR SS:[EBP-8C]
00402A88 .   8D4D DC      LEA ECX,DWORD PTR SS:[EBP-24]
00402A8B .   C785 7CFFFFF MOV DWORD PTR SS:[EBP-84],10
00402A95 .   899D 74FFFFF MOV DWORD PTR SS:[EBP-8C],EBX
00402A9B .   E8 86E6FFFF  CALL <JMP.&MSVBVM50.__vbaVarMove>
00402AA0 .   8D95 74FFFFF LEA EDX,DWORD PTR SS:[EBP-8C]
00402AA6 .   8D4D CC      LEA ECX,DWORD PTR SS:[EBP-34]
00402AA9 .   C785 7CFFFFF MOV DWORD PTR SS:[EBP-84],A2DC1DEA.0040  UNICODE "PASSWORT FALSCH !"
00402AB3 .   C785 74FFFFF MOV DWORD PTR SS:[EBP-8C],8
00402ABD .   E8 6AE6FFFF  CALL <JMP.&MSVBVM50.__vbaVarCopy>
00402AC2 .   8D45 84      LEA EAX,DWORD PTR SS:[EBP-7C]
00402AC5 .   897D 8C      MOV DWORD PTR SS:[EBP-74],EDI
00402AC8 .   50           PUSH EAX
00402AC9 .   8D45 94      LEA EAX,DWORD PTR SS:[EBP-6C]
00402ACC .   50           PUSH EAX
00402ACD .   8D45 CC      LEA EAX,DWORD PTR SS:[EBP-34]
```

위에서 보았던 문자열이 사용되어 비교하는 부분이 이 위치다.
바로 아래를 보면 vbaStrCmp라는 것이 보이는데 C언어에서 strcmp()함수는 문자열 비교함수인 것이 생각 났다.
아마 이 부분이 이 프로그램에서 문자열을 비교함수가 사용되어진 것 같다.