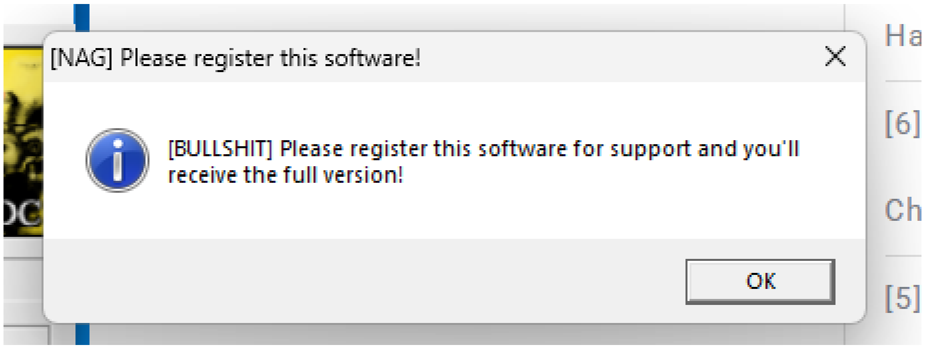
NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

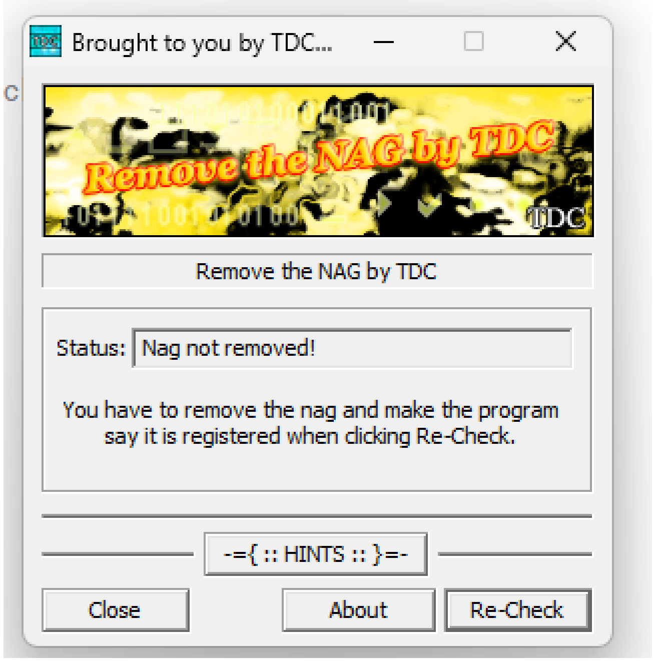
CRACK ME 6

1. Remove the starting Nag Screen
2. When the button Re-Check is clicked, a pop-up messagebox appears and you should set it to say “Thank you for registering this software”
3. Set the Status box text to: “Clean crack! Good Job!”



[NAG] Please register this software!

[BULLSHIT] Please register this software for support and you'll receive the full version!



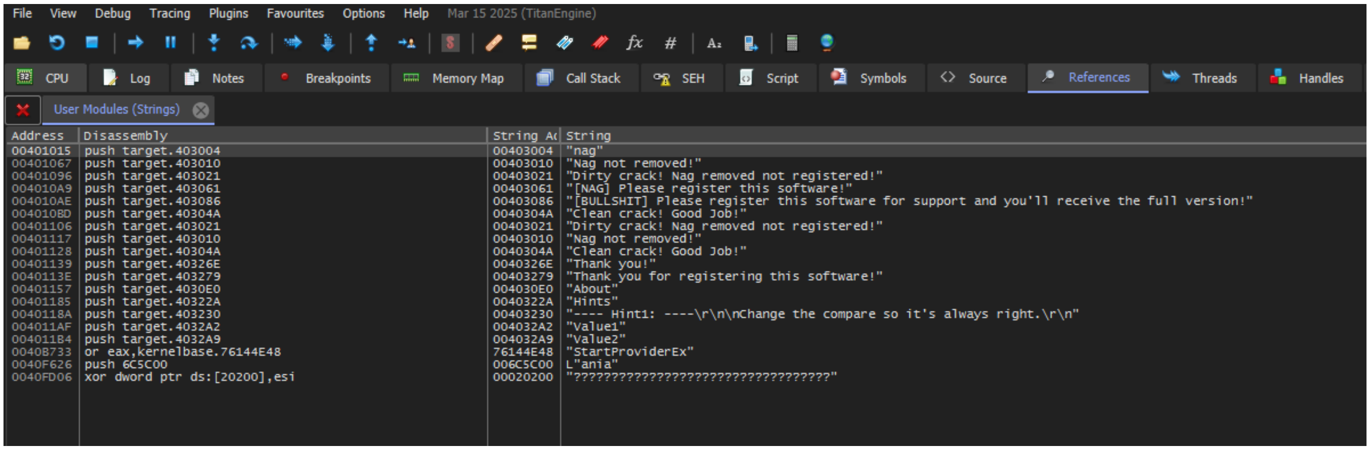
Brought to you by TDC...

Remove the NAG by TDC

Status: Nag not removed!

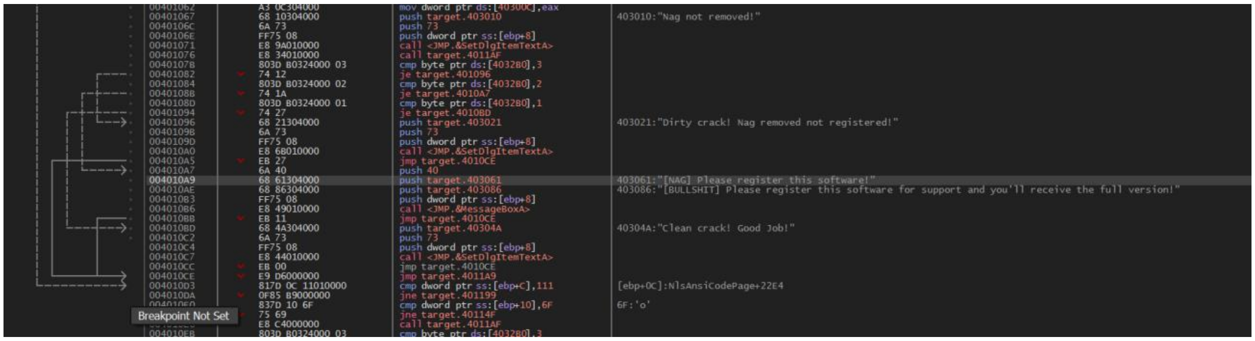
You have to remove the nag and make the program say it is registered when clicking Re-Check.

Go to String references to dig into notable string and its line of code.



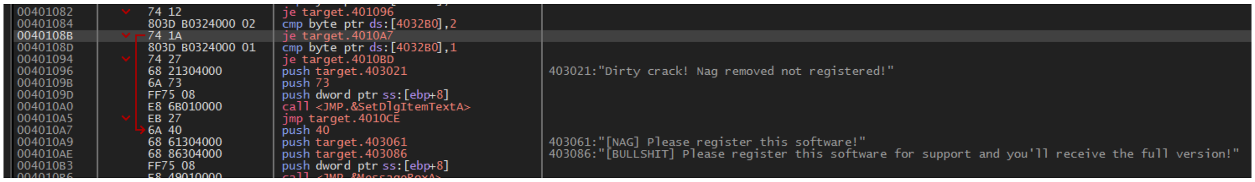
```
Address   Disassembly                       String Ad String
00401015  push target.403004                00403004  "nag"
00401067  push target.403010                00403010  "Nag not removed!"
00401096  push target.403021                00403021  "Dirty crack! Nag removed not registered!"
004010A9  push target.403061                00403061  "[NAG] Please register this software!"
004010AE  push target.403086                00403086  "[BULLSHIT] Please register this software for support and you'll receive the full version!"
004010BD  push target.40304A                0040304A  "Clean crack! Good Job!"
00401106  push target.403021                00403021  "Dirty crack! Nag removed not registered!"
00401117  push target.403010                00403010  "Nag not removed!"
00401128  push target.40304A                0040304A  "Clean crack! Good Job!"
00401139  push target.40326E                0040326E  "Thank you!"
0040113E  push target.403279                00403279  "Thank you for registering this software!"
00401157  push target.4030E0                004030E0  "About"
00401185  push target.40322A                0040322A  "Hints"
0040118A  push target.403230                00403230  "---- Hint1: ----\r\n\nChange the compare so it's always right.\r\n"
004011AF  push target.4032A2                004032A2  "Value1"
004011B4  push target.4032A9                004032A9  "Value2"
0040B733  or eax,kernelbase.76144E48        76144E48  "StartProviderEx"
0040F626  push 6C5C00                       006C5C00  L"ania"
0040FD06  xor dword ptr ds:[20200],esi      00020200  "??????????????????????????????????"
```

Click the string have [NAG] to see and analyze to remove it.

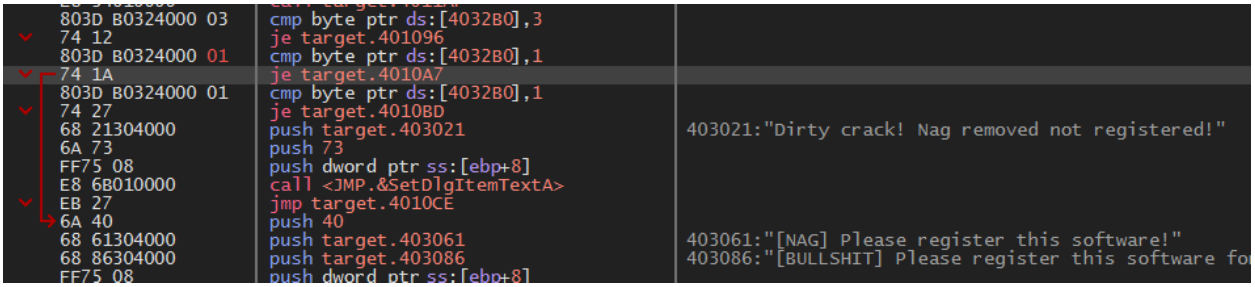


```
00401067   68 10304000         push target.403010                  403010:"Nag not removed!"
0040106C   6A 73               push 73
0040106E   FF75 08             push dword ptr ss:[ebp+8]
00401071   E8 9A010000         call <JMP.&SetDlgItemTextA>
00401076   E8 34010000         call target.4011AF
0040107B   803D B0324000 03    cmp byte ptr ds:[4032B0],3
00401082   74 12               je target.401096
00401084   803D B0324000 02    cmp byte ptr ds:[4032B0],2
0040108B   74 1A               je target.4010A7
0040108D   803D B0324000 01    cmp byte ptr ds:[4032B0],1
00401094   74 27               je target.4010BD
00401096   68 21304000         push target.403021                  403021:"Dirty crack! Nag removed not registered!"
0040109B   6A 73               push 73
0040109D   FF75 08             push dword ptr ss:[ebp+8]
004010A0   E8 6B010000         call <JMP.&SetDlgItemTextA>
004010A5   EB 27               jmp target.4010CE
004010A7   6A 40               push 40
004010A9   68 61304000         push target.403061                  403061:"[NAG] Please register this software!"
004010AE   68 86304000         push target.403086                  403086:"[BULLSHIT] Please register this software for support and you'll receive the full version!"
004010B3   FF75 08             push dword ptr ss:[ebp+8]
004010B6   E8 49010000         call <JMP.&MessageBoxA>
004010BB   EB 11               jmp target.4010CE
004010BD   68 4A304000         push target.40304A                  40304A:"Clean crack! Good Job!"
004010C2   6A 73               push 73
004010C4   FF75 08             push dword ptr ss:[ebp+8]
004010C7   E8 44010000         call <JMP.&SetDlgItemTextA>
004010CC   EB 00               jmp target.4010CE
004010CE   E9 D6000000         jmp target.4011A9
004010D3   817D 0C 11010000    cmp dword ptr ss:[ebp+C],111        [ebp+0C]:NlsAnsiCodePage+22E4
004010DA   0F85 B9000000       jne target.401199
004010E0   837D 10 6F          cmp dword ptr ss:[ebp+10],6F        6F:'o'
           75 69               jne target.40114F
           E8 C4000000         call target.4011AF
004010EB   803D B0324000 03    cmp byte ptr ds:[4032B0],3
```

Trace above the code to find how the NAG displayed. And I found that, this NAG is pushed and displayed by the address 00401084 and 00401084. These addresses have command to compare, if byte ptr ds:[4032B0] represent for variable of system equals with 2, the first NAG will be displayed (in this situation, it is always true). So I change the condition comparing with 2 to another number such as 1, to result false.

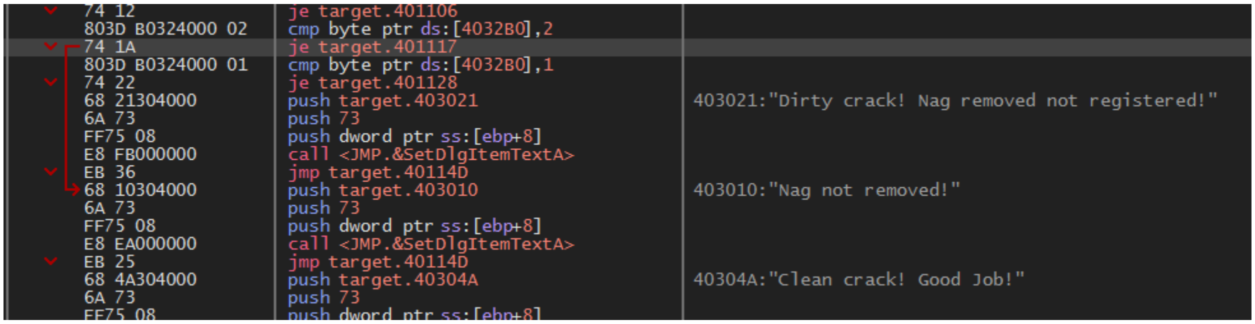


```
00401082   74 12               je target.401096
00401084   803D B0324000 02    cmp byte ptr ds:[4032B0],2
0040108B   74 1A               je target.4010A7
0040108D   803D B0324000 01    cmp byte ptr ds:[4032B0],1
00401094   74 27               je target.4010BD
00401096   68 21304000         push target.403021            403021:"Dirty crack! Nag removed not registered!"
0040109B   6A 73               push 73
0040109D   FF75 08             push dword ptr ss:[ebp+8]
004010A0   E8 6B010000         call <JMP.&SetDlgItemTextA>
004010A5   EB 27               jmp target.4010CE
004010A7   6A 40               push 40
004010A9   68 61304000         push target.403061            403061:"[NAG] Please register this software!"
004010AE   68 86304000         push target.403086            403086:"[BULLSHIT] Please register this software for support and you'll receive the full version!"
004010B3   FF75 08             push dword ptr ss:[ebp+8]
```



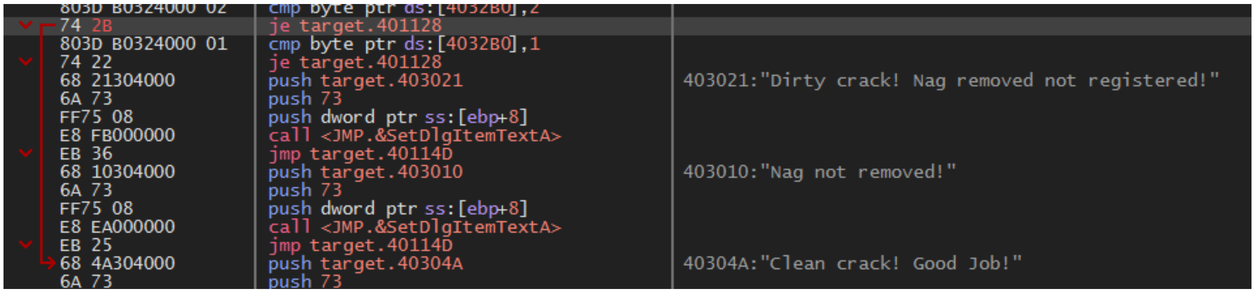
```
803D B0324000 03    cmp byte ptr ds:[4032B0],3
74 12               je target.401096
803D B0324000 01    cmp byte ptr ds:[4032B0],1
74 1A               je target.4010A7
803D B0324000 01    cmp byte ptr ds:[4032B0],1
74 27               je target.4010BD
68 21304000         push target.403021            403021:"Dirty crack! Nag removed not registered!"
6A 73               push 73
FF75 08             push dword ptr ss:[ebp+8]
E8 6B010000         call <JMP.&SetDlgItemTextA>
EB 27               jmp target.4010CE
6A 40               push 40
68 61304000         push target.403061            403061:"[NAG] Please register this software!"
68 86304000         push target.403086            403086:"[BULLSHIT] Please register this software fo
FF75 08             push dword ptr ss:[ebp+8]
```

After passing start NAG, we will change status “Nag not removed!” into “Clean crack! Good job!”. So I trace to the line of code having “Nag not removed!”. Tracing above code and found that, we have command “JE” to that string. So I convert Jump Equal to “Nag not removed!” into address of “Clean code…”



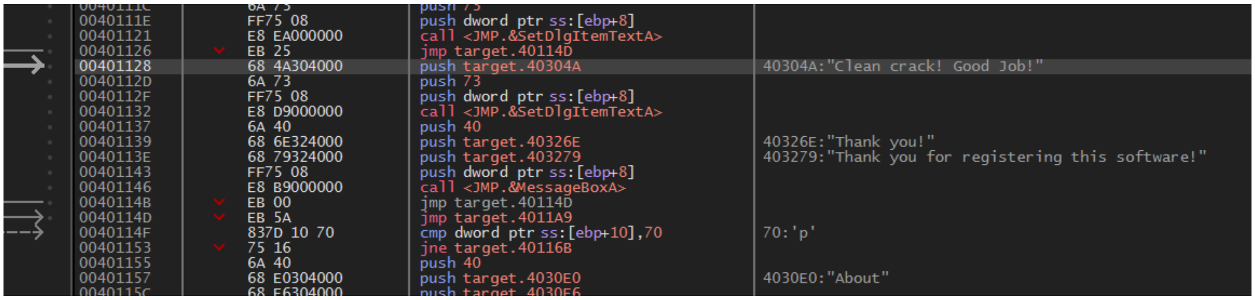
```
74 12              je target.401106
803D B0324000 02   cmp byte ptr ds:[4032B0],2
74 1A              je target.401117
803D B0324000 01   cmp byte ptr ds:[4032B0],1
74 22              je target.401128
68 21304000        push target.403021                   403021:"Dirty crack! Nag removed not registered!"
6A 73              push 73
FF75 08            push dword ptr ss:[ebp+8]
E8 FB000000        call <JMP.&SetDlgItemTextA>
EB 36              jmp target.40114D
68 10304000        push target.403010                   403010:"Nag not removed!"
6A 73              push 73
FF75 08            push dword ptr ss:[ebp+8]
E8 EA000000        call <JMP.&SetDlgItemTextA>
EB 25              jmp target.40114D
68 4A304000        push target.40304A                   40304A:"Clean crack! Good Job!"
6A 73              push 73
FF75 08            push dword ptr ss:[ebp+8]
```

Like below: 401117 => 401128.



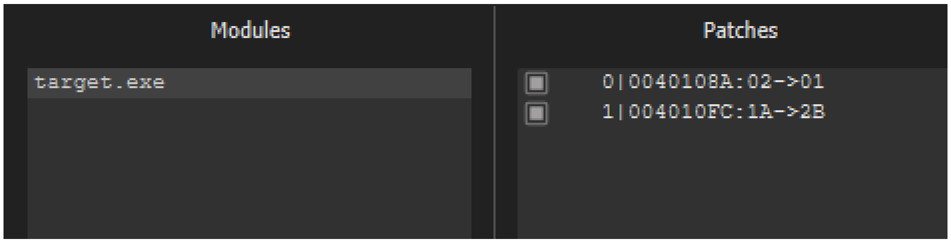
```
803D B0324000 02   cmp byte ptr ds:[4032B0],2
74 2B              je target.401128
803D B0324000 01   cmp byte ptr ds:[4032B0],1
74 22              je target.401128
68 21304000        push target.403021                   403021:"Dirty crack! Nag removed not registered!"
6A 73              push 73
FF75 08            push dword ptr ss:[ebp+8]
E8 FB000000        call <JMP.&SetDlgItemTextA>
EB 36              jmp target.40114D
68 10304000        push target.403010                   403010:"Nag not removed!"
6A 73              push 73
FF75 08            push dword ptr ss:[ebp+8]
E8 EA000000        call <JMP.&SetDlgItemTextA>
EB 25              jmp target.40114D
68 4A304000        push target.40304A                   40304A:"Clean crack! Good Job!"
6A 73              push 73
```

After changing status, I found that the code below will execute to automatically displaying NAG “Thank you! Thank you for registering this sofware!” if we press button Re-check.



```
0040111C   6A 73          push 73
0040111E   FF75 08        push dword ptr ss:[ebp+8]
00401121   E8 EA000000    call <JMP.&SetDlgItemTextA>
00401126   EB 25          jmp target.40114D
00401128   68 4A304000    push target.40304A              40304A:"Clean crack! Good Job!"
0040112D   6A 73          push 73
0040112F   FF75 08        push dword ptr ss:[ebp+8]
00401132   E8 D9000000    call <JMP.&SetDlgItemTextA>
00401137   6A 40          push 40
00401139   68 6E324000    push target.40326E              40326E:"Thank you!"
0040113E   68 79324000    push target.403279              403279:"Thank you for registering this software!"
00401143   FF75 08        push dword ptr ss:[ebp+8]
00401146   E8 B9000000    call <JMP.&MessageBoxA>
0040114B   EB 00          jmp target.40114D
0040114D   EB 5A          jmp target.4011A9
0040114F   837D 10 70     cmp dword ptr ss:[ebp+10],70    70:'p'
00401153   75 16          jne target.40116B
00401155   6A 40          push 40
00401157   68 E0304000    push target.4030E0              4030E0:"About"
0040115C   68 E6304000    push target.4030E6
```

So I patch this file and check the result.

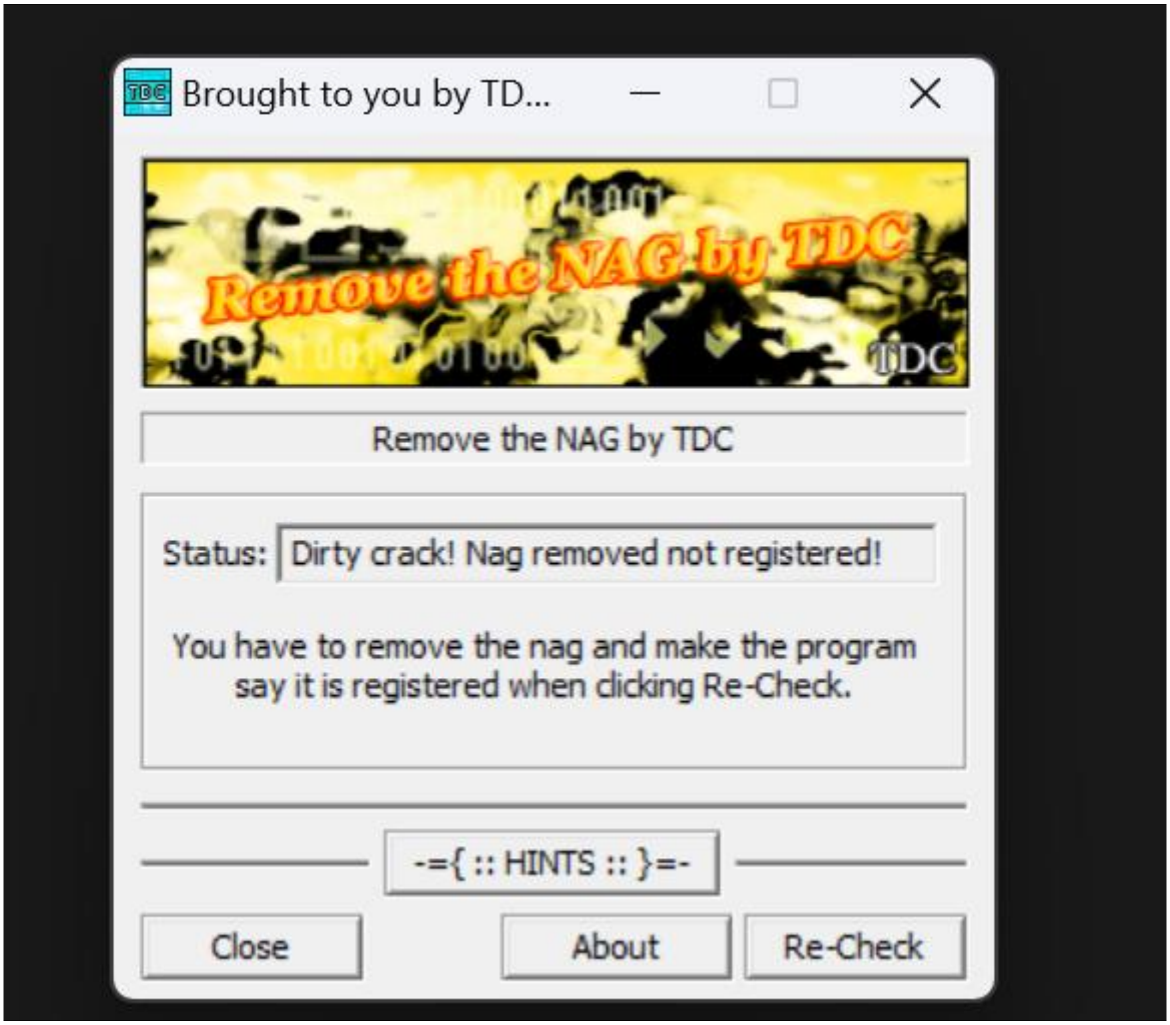


```
target.exe
```

```
0|0040108A:02->01
1|004010FC:1A->2B
```

The result:

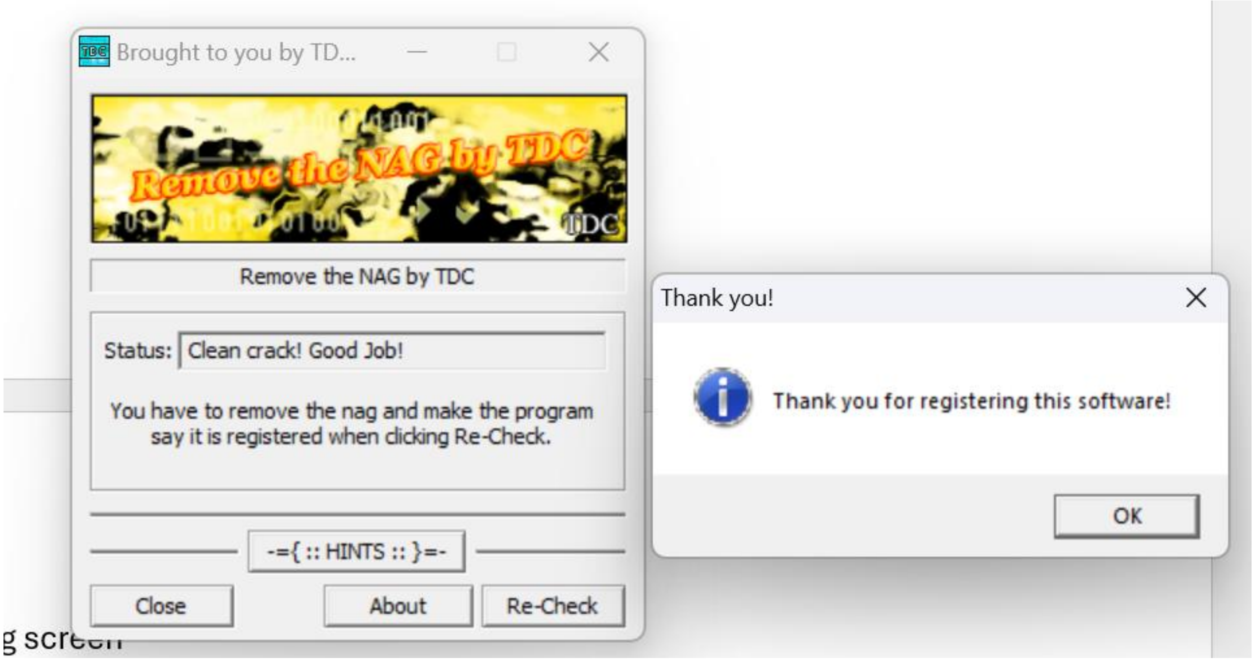
1.removing starting nag screen



Status: Dirty crack! Nag removed not registered!

You have to remove the nag and make the program say it is registered when clicking Re-Check.

2. When the button Re-Check is clicked, a pop-up messagebox appears and you should set it to say “Thank you for registering this software”
3. Set the Status box text to: “Clean crack! Good Job!”



Remove the NAG by TDC

Status: Clean crack! Good Job!

You have to remove the nag and make the program say it is registered when clicking Re-Check.

Thank you for registering this software!

DONE!!!