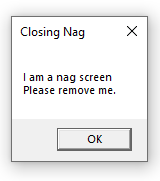
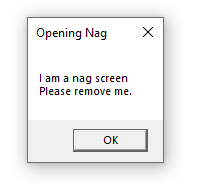
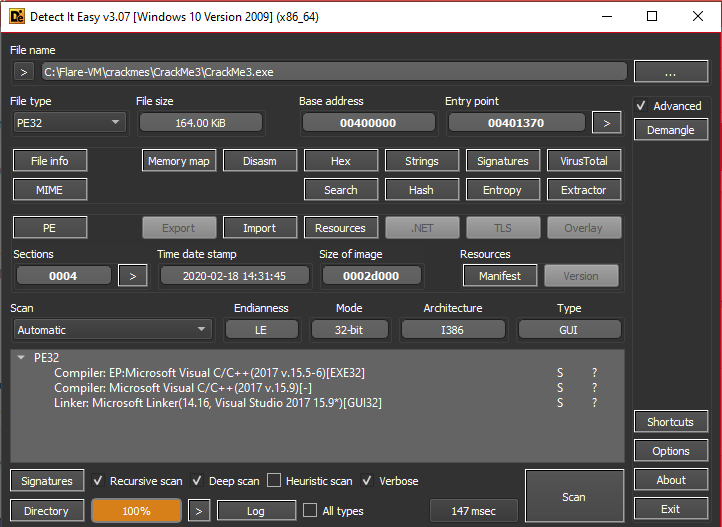


Run It:



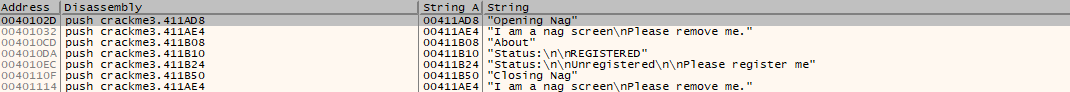
There are three nags above



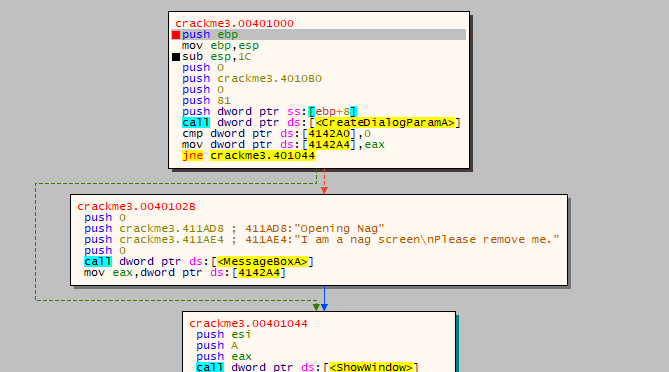
This a 32 bit PE file

1. Remove the opening nag

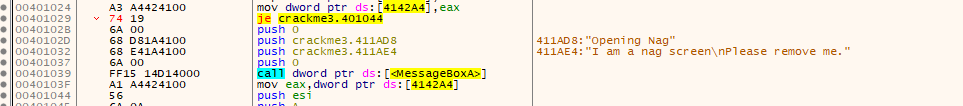
* Find all strings references:

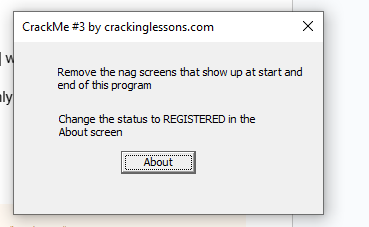


Go to place where Opening Nag is references



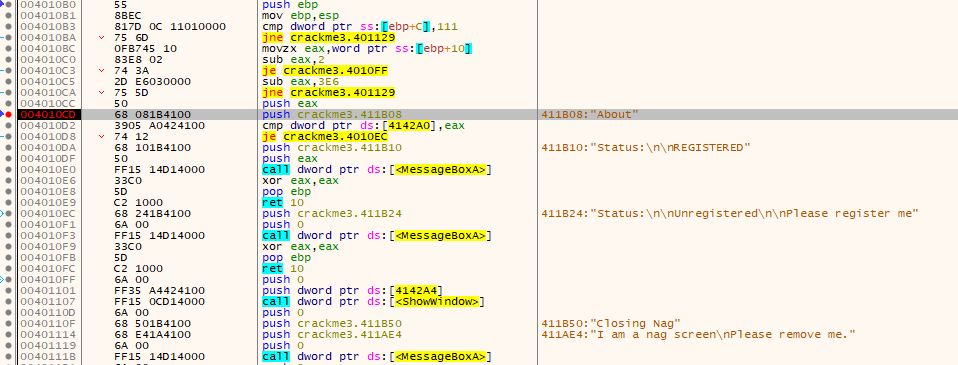
* Can easily see that it compare value at dword [4142A0] with 0, if it not equal, we jump through the nag
* Find all reference to dword[4142A0], we found that it only read y program, and default value is 0
* 
* So we just simple patch jump jne to je



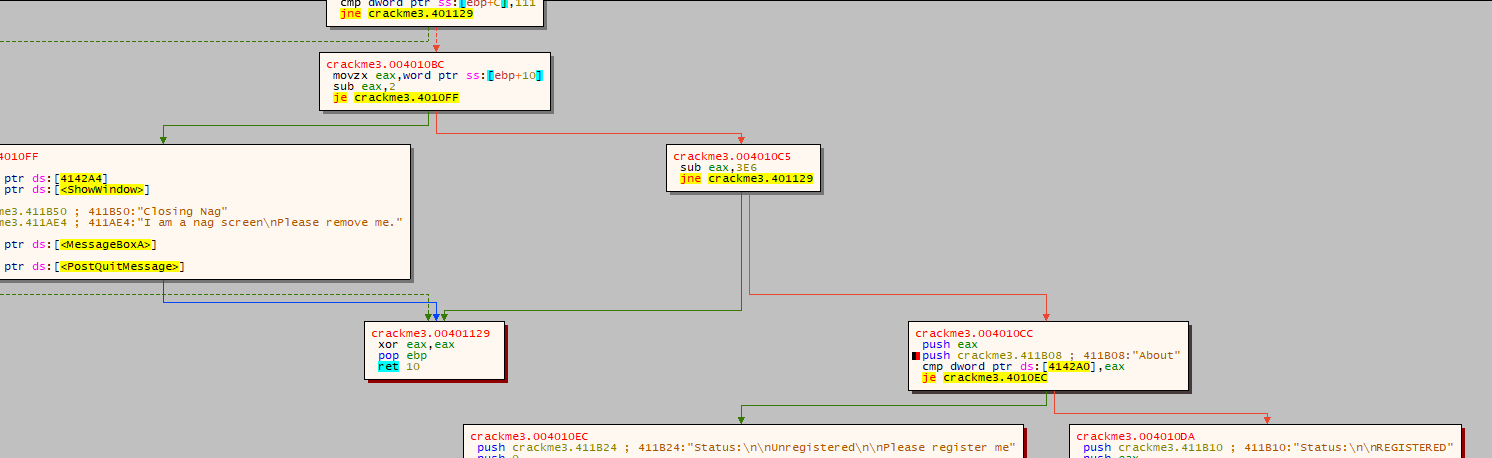
* Continue run program, see that no nag :)) and we jump immediate to
* 

1. Register

Set a breakpoint at “About” then go to app, press button About, we jump immediately to breakpoint

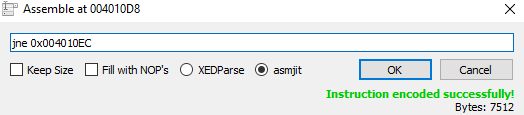


Press G to view in Graph mode

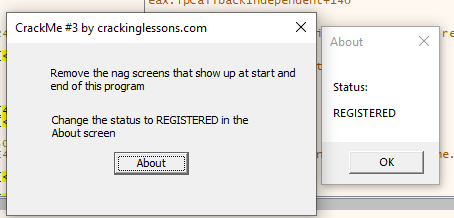


We can see that it continue compare dword[4142A0] with 0 (eax in this case equal 0)

if it not equal, we registered the crackme, other while commission fails. As mentions above, the value at this dword is default 0, and does not change in running time. So, we can simple patch je to jne

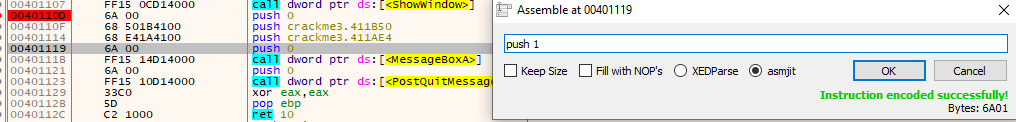


There is it



1. Remove the closing nag



Finally, to remove the closing nag, we found that the last parameter put into the API MessageBoxA is the window where the nag show, if this window not found, it not gonna show on screen, so we simple patch the last parameter to 1.

Press X on the top of About nag and continue run the program. No nag is shown

Check:

Run the patched program

