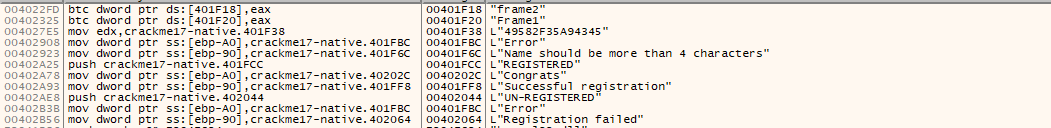


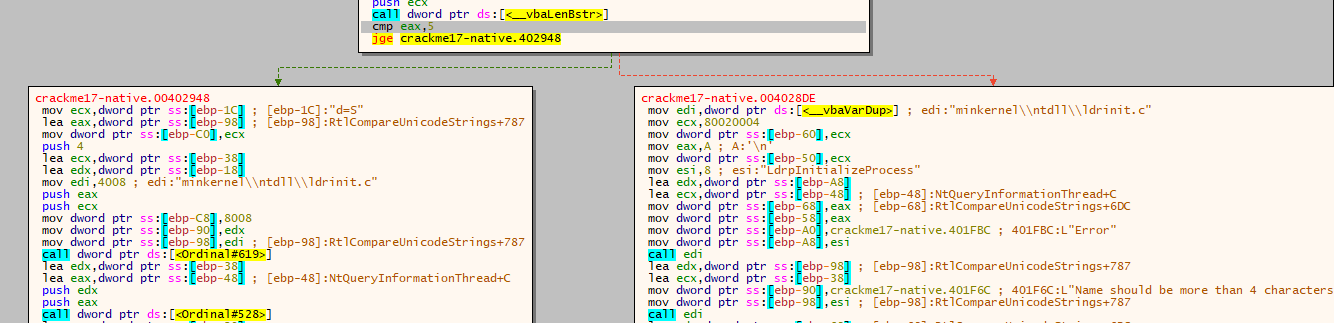
1. Patch the file

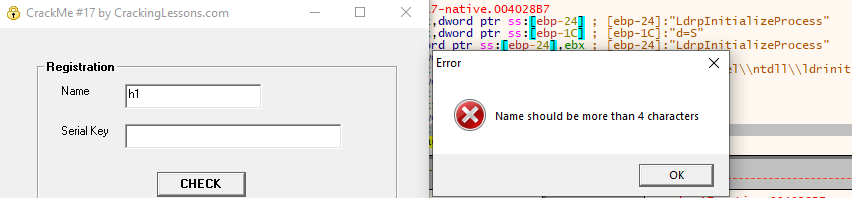


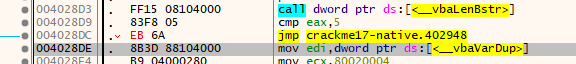
In reference string, we found something:

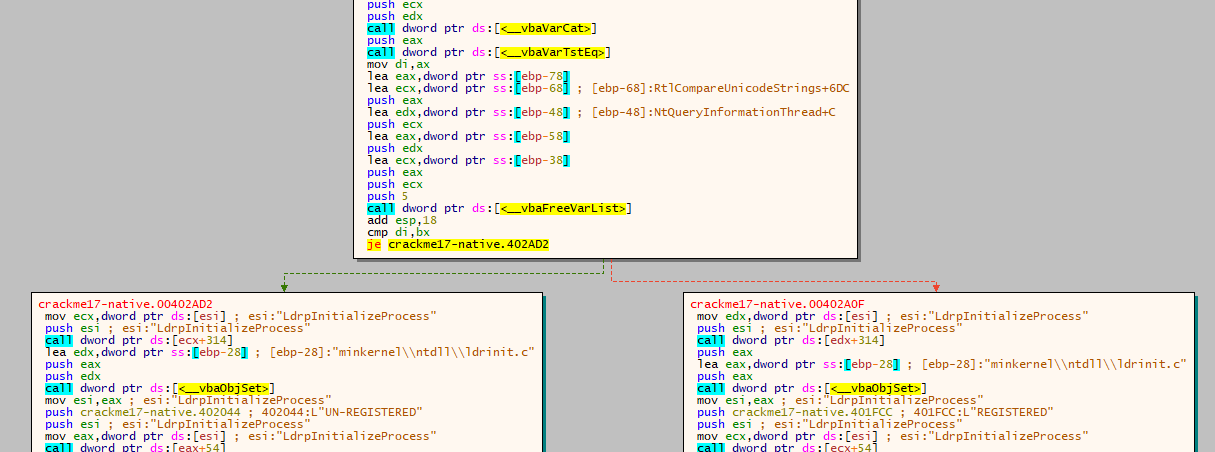
* Name should be more than 4 characters
* "49582F35A94345”
* REGISTERED
* UNREGISTERED

First Run crackme, If input less than 5 characters, crackme will show a nag: “Name should be more than 4 characters”

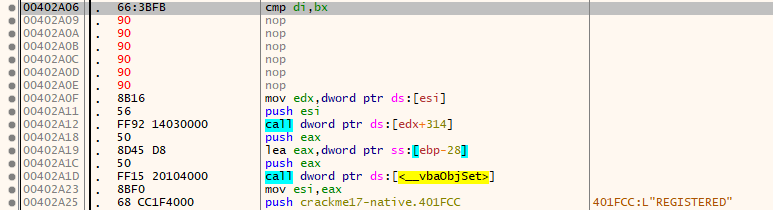
To bypass this check, we jump to where the nag is call 

We see that crackme call lenBStr function to calculate len of name, and compare result with 5, if result >= 5 it jump to continue block else, it run show nag code which show us 

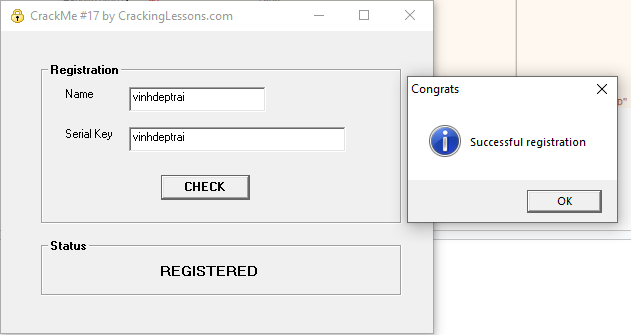
To bypass this check, we patch jge into jmp to alway jump no matter the length of it.

Next We jump to to next block, 

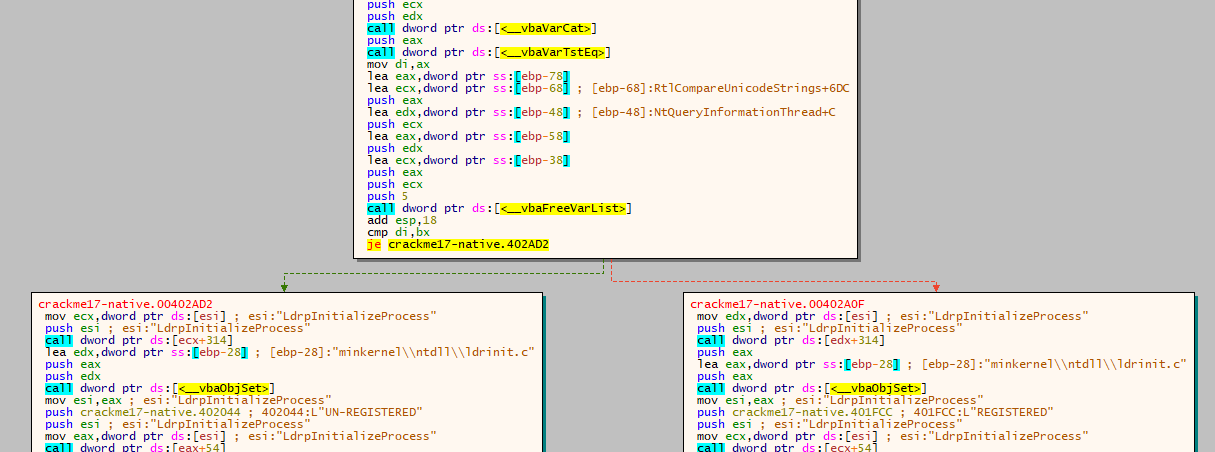
Have a je instruction which je to UNREGISTER BLOCK, to bypass this, we can patch je into nop, so it will always jump into register block.



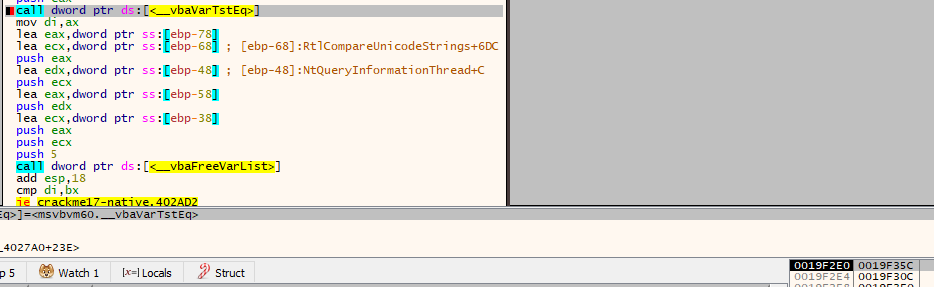
Test



1. Keygen



We see a VarTstEq() function, which is used to compare two strings.Let find which two strings are compared.

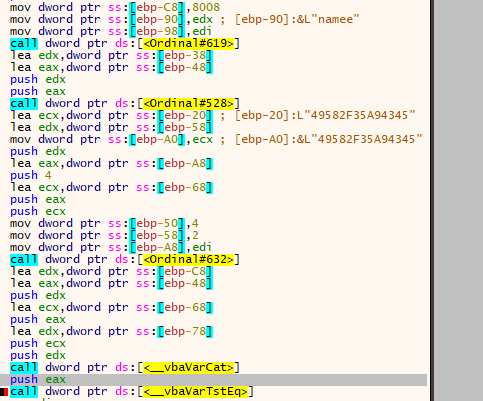


Follow address in stack, i found two string is compare is



AND

which is our serial and a strange “AMEE82F3”

Look above this code, we see some function

Ordinal#619 is Right() function in VBA

Ordinal#528 is Ucase function in VBA

Ordinal#632 is Mid function in VBA

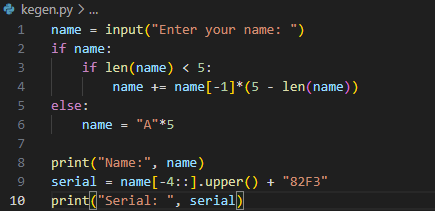
* The Right() function is used to get characters from the right of string, in our case, input is our input name and 4 which mean, it takes 4 rightmost character of input name
* The Ucase() function use to get uppercase of string, in our case, it is the 4 rightmost character we get from previous Right() function
* The Mid() function is used to get characters in a range, in our case input is string "49582F35A94345” and 4 and 4 which mean it takes 4 characters from index 4 of this string. Which output is “82F3” (string index in VBA is 1 - index)

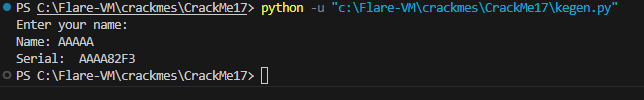
The we see, crackme call VarCat function which concat two strings which are 4 rightmost character in uppercase format and “82F3”

So, logic here is:

Crackme require user enter name and serial, name must be more than 4 characters, and serial is 4 rightmost character is name uppercase then concat with string “82F3”

So i write this keygen





Check

