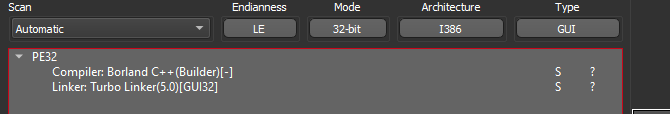
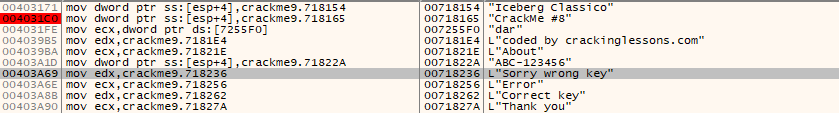
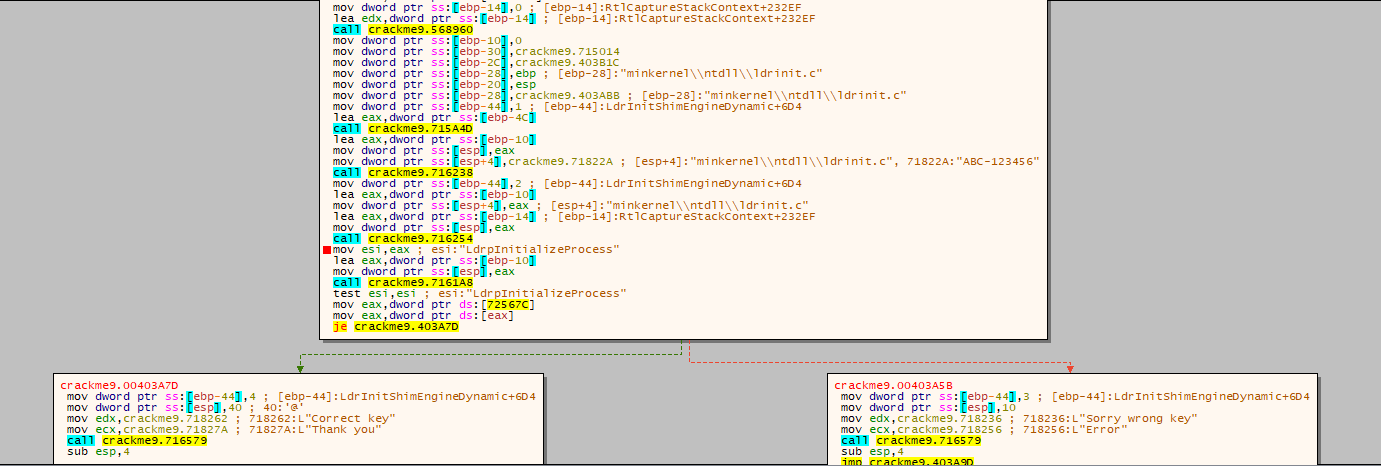


DiE: 32bit PE file

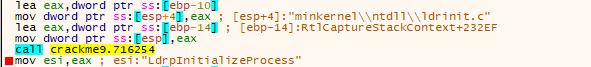


Find string references:



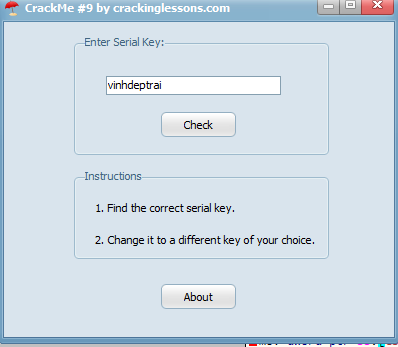
Go to there

we can see that the value at esi decides whether our key is correct or wrong, read the code, esi is the result from function crackme9.716254

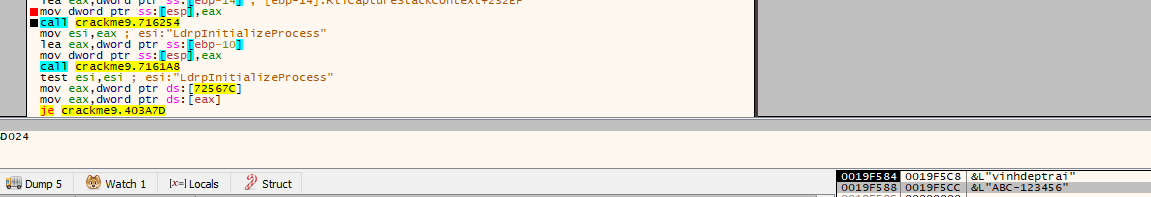


with two parameters are dword store at [ebp -10] and dword store at [ebp -14]

set breakpoint at the call and see what they are



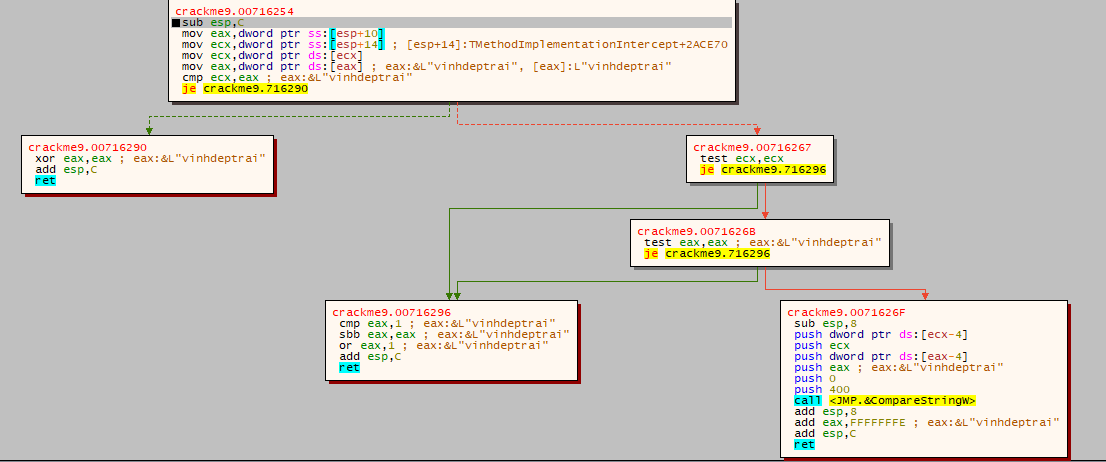
press check and it takes us jump to breakpoint



take a look on stack to see what they are

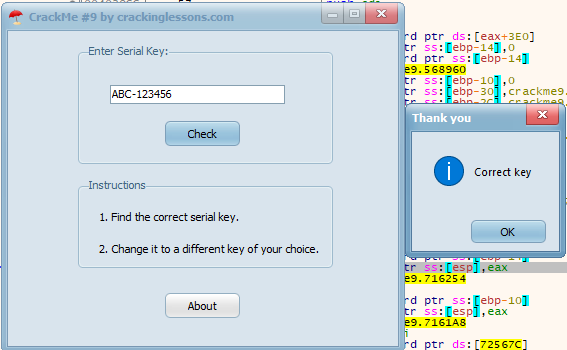
* One is our key: vinhdeptrai
* Other is a string: ABC-123456

Let go inside the function to see what do do with them



* first it compare address of two address of two input, it definitely different
* then it check whether one of them are null
* Finally,it call compareStringW with two input
* So we can conclude that **the key here is ABC-123456**

So test with input is ABC-123456



2. Change key to a different key

* We know where the ABC-123456
* Just jump there and patches it





===>

now check

