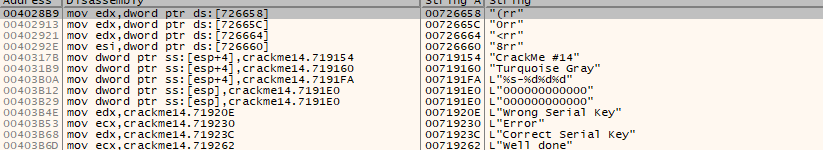


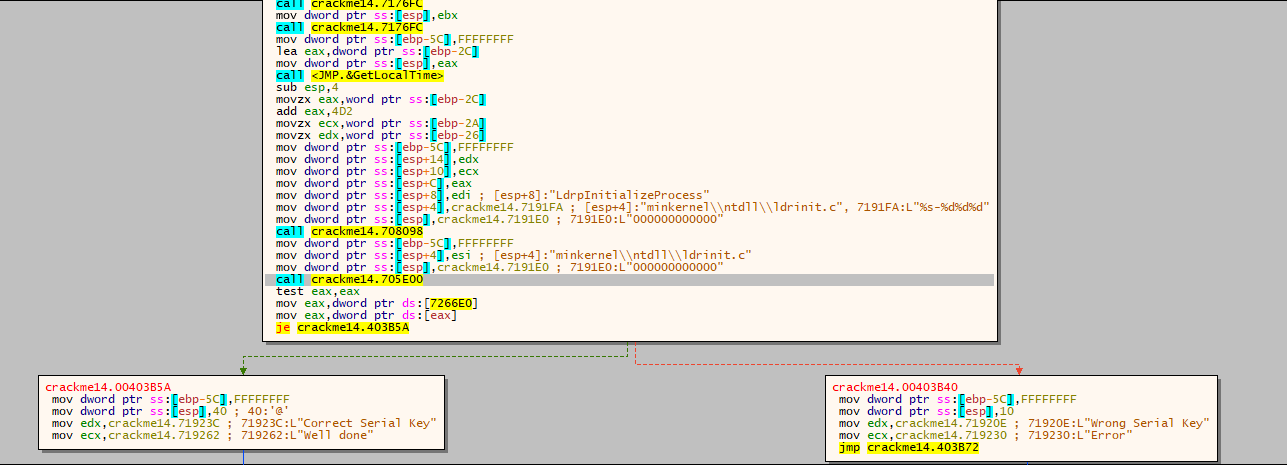
This challenge requires create a keygen

First, we find the logic of it

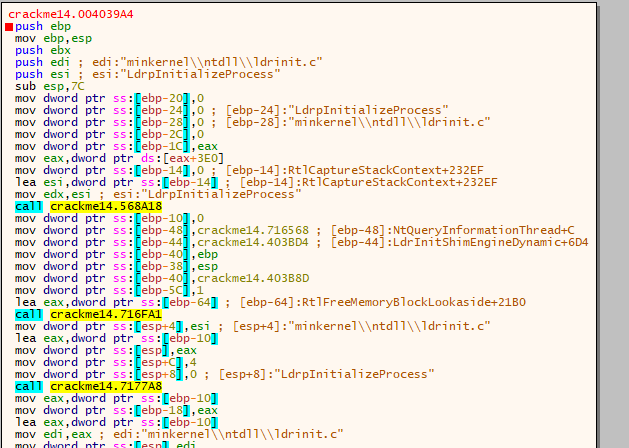
Throw into x32dbg, find reference strings



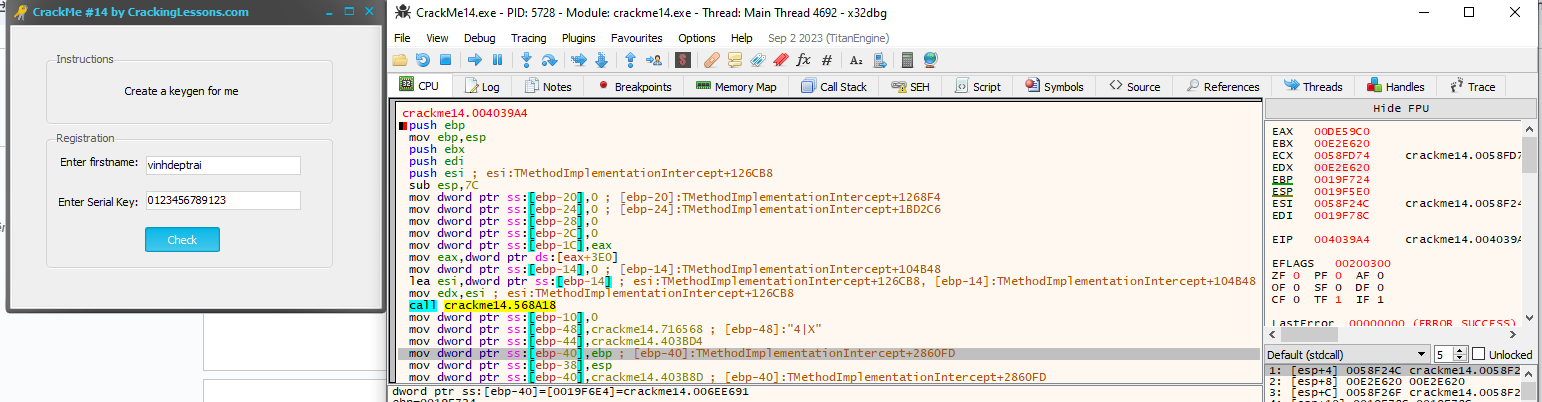
Go to “Correct Serial Key” and Well done”



Let’s find the where the function contain the code start by using calling convention x32 window, find where the stack of this function is create(push ebp + mov ebp, esp)

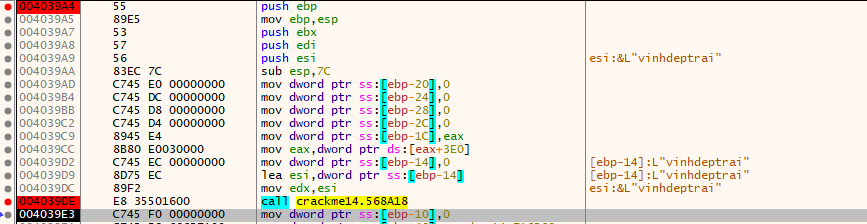
Here it’s

Set a breakpoint at the start of this function and see what does this function do before decide jump to goodboy or badboy



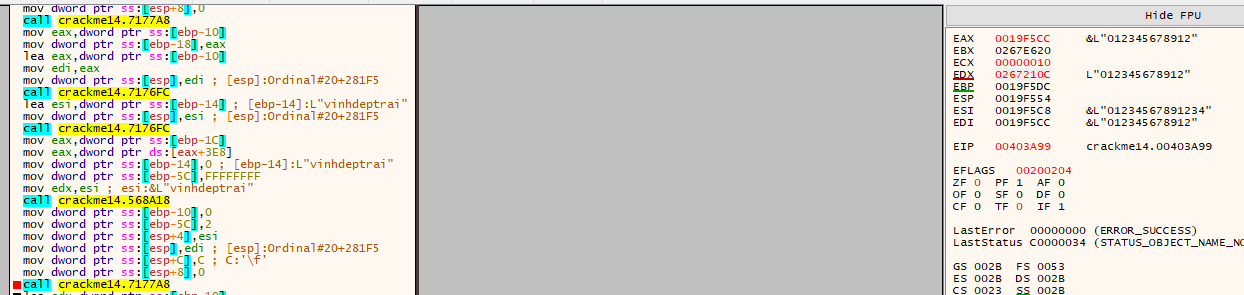
With the input, after pressing the Check button. We land on there - the start of function.

Tracing through each line of code of this function. I found some interesting things

After tracing through the function crackme14.568A18, I found the firstname we entered was get.



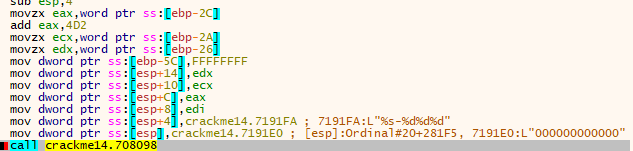
After that the name is passed into function crackme14.7177A8 with a parameter has value 4 and 0. Jump after this function, the value of the firstname only left 4 characters. So this function is used to get the first 4 characters of the firstname we entered. And in case it is less than 4 characters, it says the same as before.

Under are the same, the serial also read and pass into function crackme4.7177A8 but with value 0xc (12) so limit of serial is 12 character

Continue tracing.

We meet a GetLocalTime API, the result of it was store in

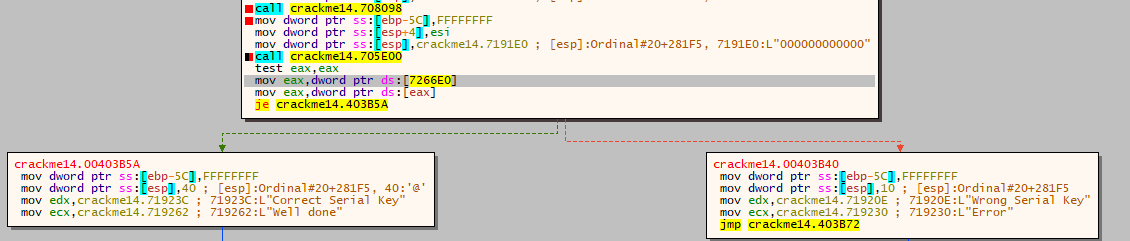
* eax: year + 0x4d2
* ecx: month
* edx: day

Next

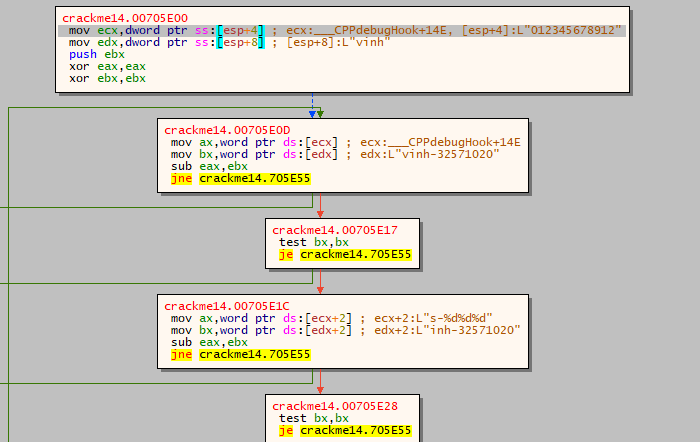
firstname(left then 5 characters) and year, month, day were pass into function crackme14.708098. After that function, they are concat into format firstname-yearmonthday

After that serial and the string was concat is passed into function crackme14.705E00

Result of it decide whether we jump into goodboy or badboy



Dig into this function

This function is like a strcmp function, it compare each chunk of two bytes, and return 0 if they are the same, other while, return 1

We want jump to goodboy, the result must be 0 so, two passed strings must be equal

======>

firstname(left then 5 character) + ‘-’ + (year + 0x4d2) + month + day = serial

