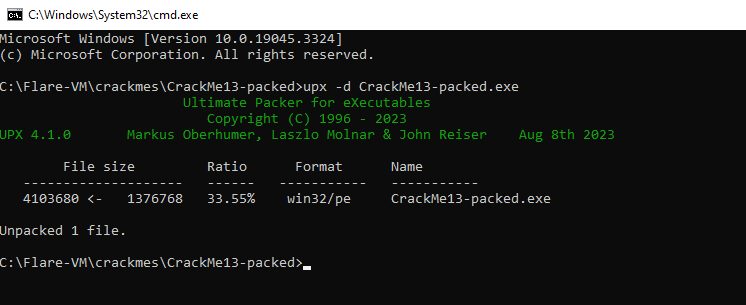
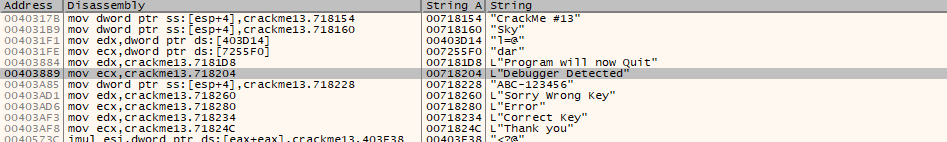


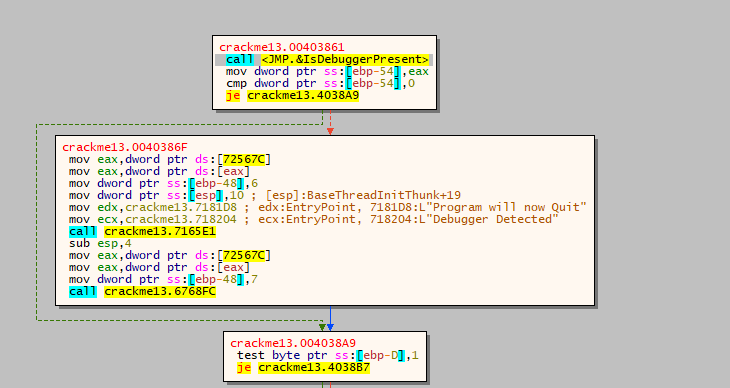
1. Unpack

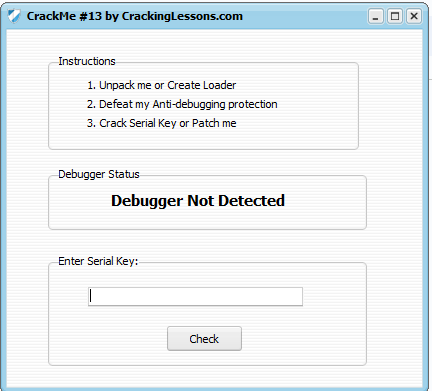
* This crackme is packed by upx, so unpack by upx

1. Defeat Anti-debug

In this part, i will practice on unpacked crackme

In reference strings, “Debugger Detected”. Jump there

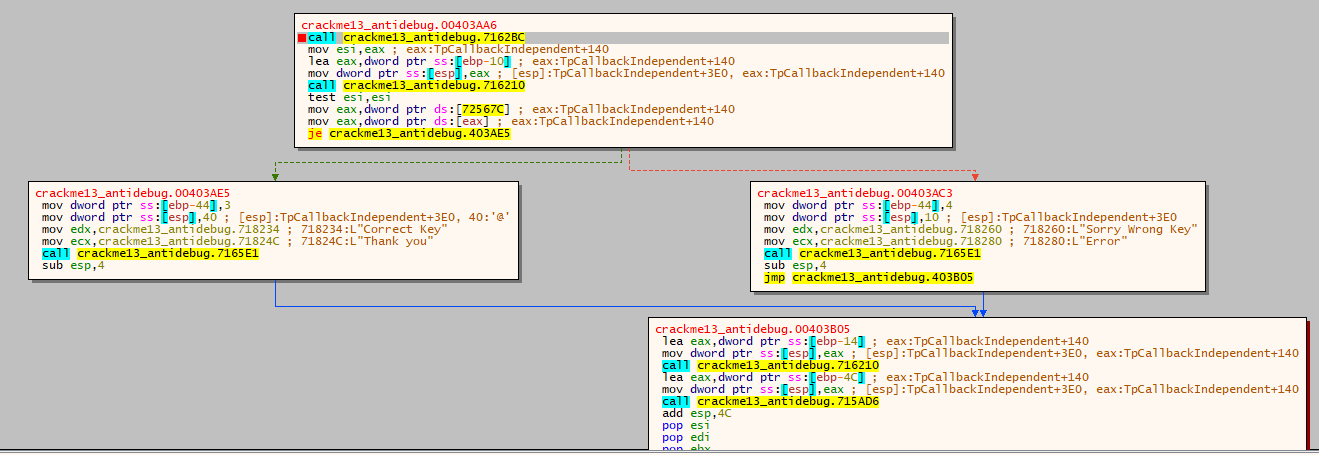


Using IsDebuggerPresent to detect debugger, we can patch the je to bypass this anti-debug technique

1. Crack Serial and Patch

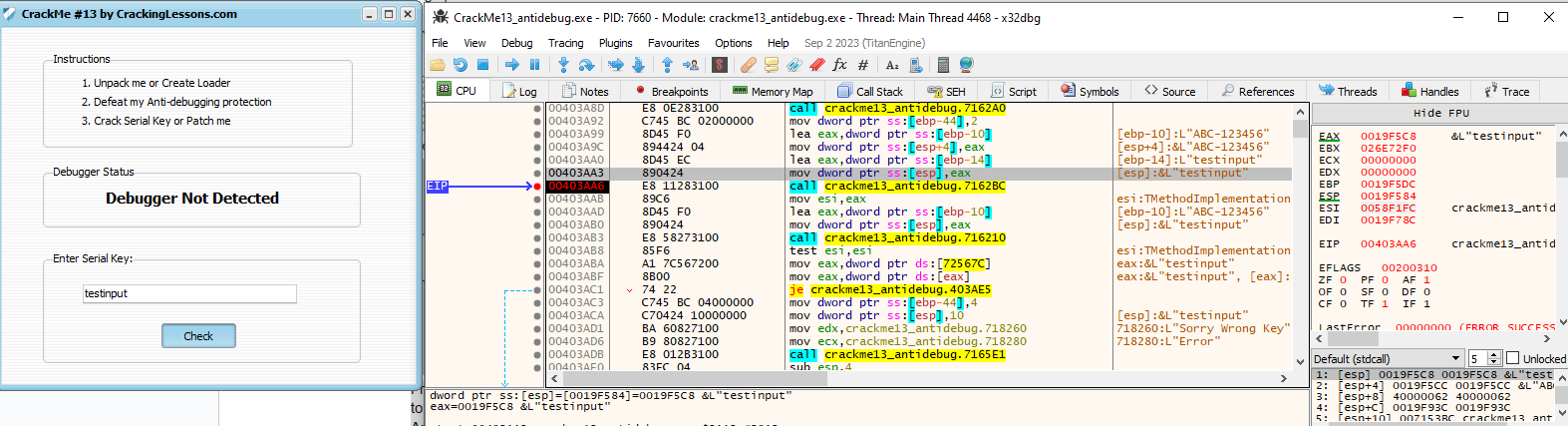
In this part, i will practice on patched anti debug crackme

In the reference string, we also found Correct Key!

Jump there

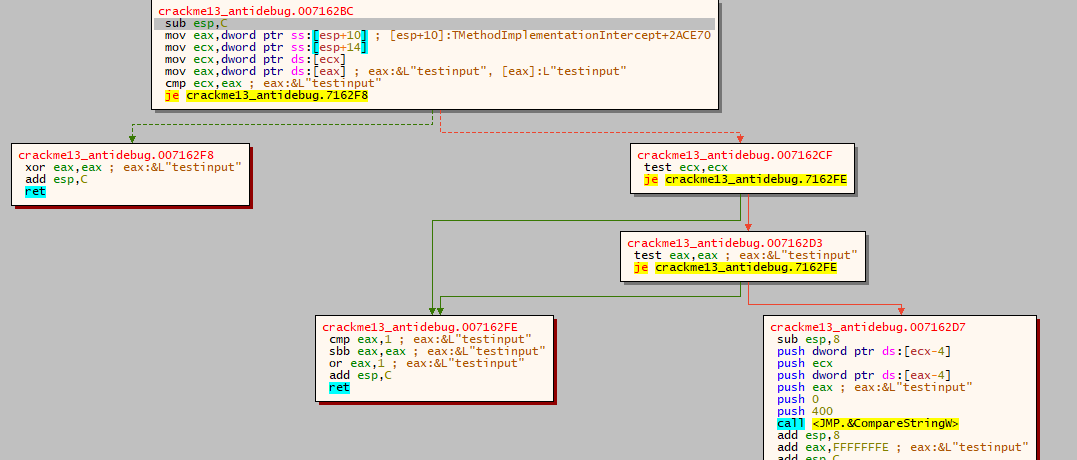
From the code, we can determine that value at ESI decides whether we jump to bad boy or goog boy.

And value at ESI was set by eax at very first, eax is the result of the first call, so set a breakpoint at this call to see what are passed into it and what it does.



So values of parameters passed into this function is input and a default string “ABC-123456”

Let’s dig into this function to see what happen



This function compares two parameters passed into through the CompareStringW function.

So, we can conclude that the valid input for this crackme is **ABC-123456**

Check:

