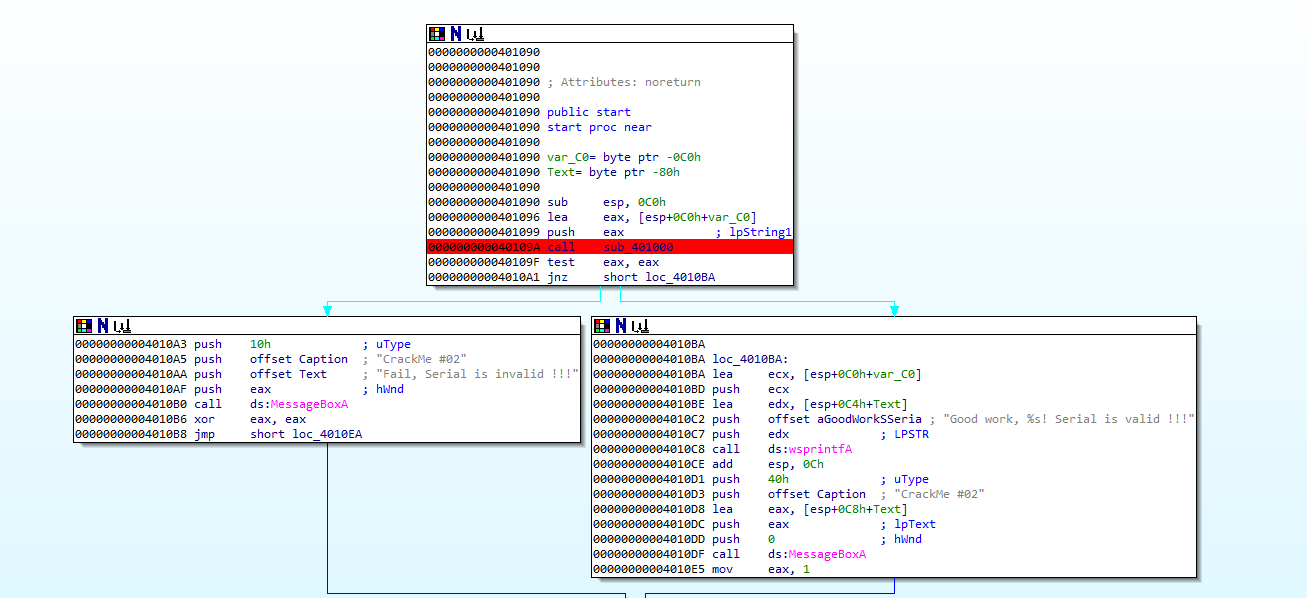
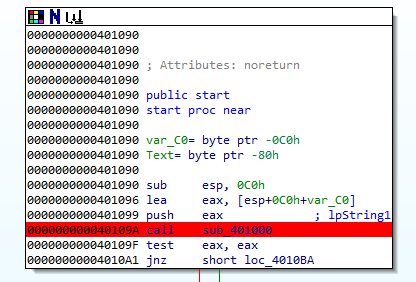
1. Для успешного выполнения задания необходимо попасть на инструкцию по адресу 0x004010BA, с которой начинается выполнение кода, отображающего окно об успешном завершении работы:



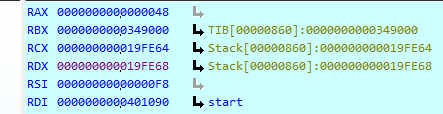
1. В данной программе вызывается функция, которая открывает файл с именем crackme02.key и кладет его содержимое на стек (адрес вызова функции 0x0040109A):



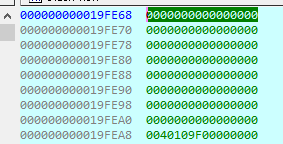
1. Данная функция (call\_401000) открывает файл и сохраняет его содержимое, вызывая WinAPI функцию ReadFile, на стеке по адресу, переданному функции ReadFile в параметре lpBuffer (передача параметра с адресом для начала записи содержимого файла - инструкция по адресу 0x0040103D):



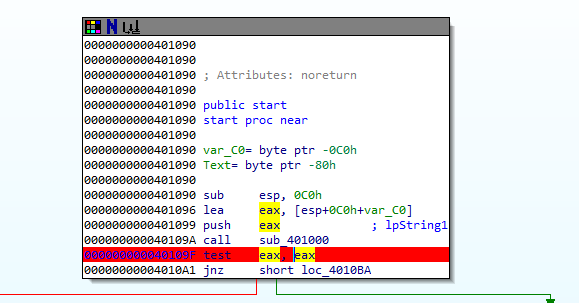
1. Перейдя в режим отладки, выясняем, что адрес на стеке, куда сохраняется содержимое файла crackme02.key – это значение, хранящееся в регистре Rdx, в данном случае, это 0x0019FE68:



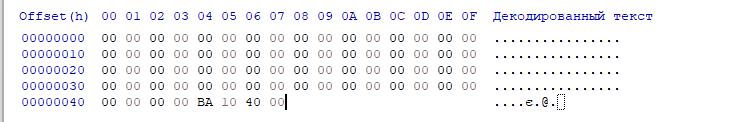
1. В стеке ищем значения по этому адресу:



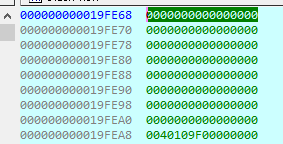
1. Видим, что по смещению 0x0019FEAB лежит адрес возврата функции call\_401000 из п.2, он указывает на инструкцию “test eax, eax” (0x0040109F):



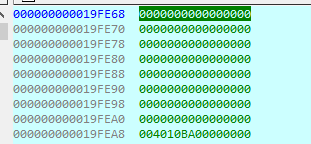
1. Нам необходимо5 перезаписать этот адрес возврата на адрес (0x004010BA) инструкции из п.1, для этого необходимо создать файл crackme02.key со следующим содержимым:



Как раз содержимое файла начнет считываться по адресу 0x0019FE68 и последние четыре байта содержимого файла перезапишут адрес возврата на нужный (68 байт нулевых значений и последние 4 байта – адрес инструкции, где начинается вывод сообщения об успехе см. п. 1)



Результат чтения файла:



1. Вывод сообщения об успехе:  
   