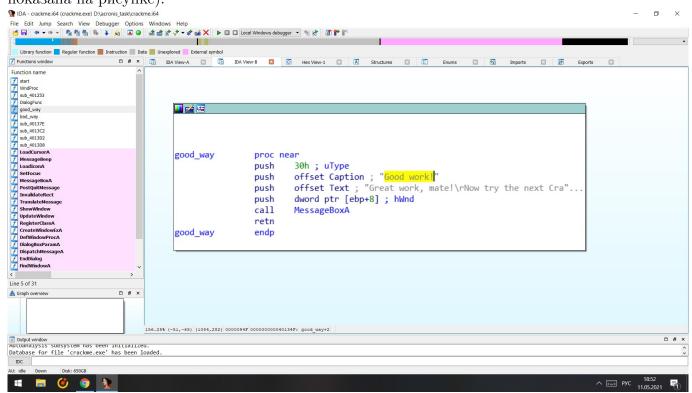
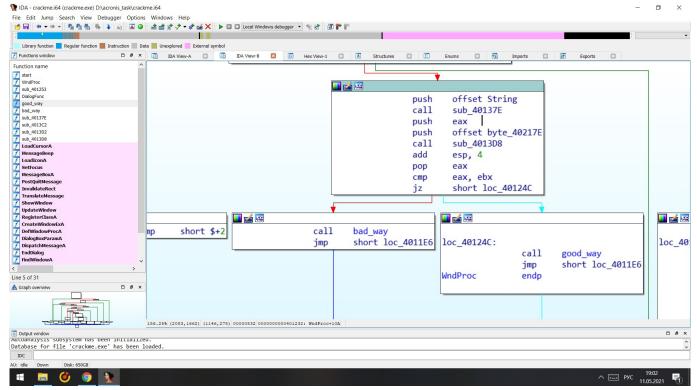
13 задача для поступления на базовую кафедру ТИПИ

Макаров Глеб Евгеньевич

Чтобы понять, что происходит в программе, дизассемблируем ее. Для этого я использую дизассемблер IDA. Открываем программу в IDA. Видим некоторое колво функций. Просматриваем их, находим 2 функции, которые выводят сообщения "No luck!"и "Good work!"(последняя показана на рисунке).



Перейдем в место, где вызываются эти функции. Они вызываются после сравнения еах и еbх.



Посмотрим, что происходит с этими регистрами до их сравнения. Т.к. еах пушится после вызова sub40137E, то скорее всего именно эта функция выдает тот еах, котрый мы будем сравнивать. Посмотрим, что в ней происходит. Запуская в режиме дебага, понимаем, что функция проходит по каждой букве логина. Если код какой-то буквы меньше чем 41, то есть буквы 'А', то неудача. Далее, если код больше 'Z', то из кода вычитается 0х20(если в логине только буквы, то эта опрецаия равносильна приведению всех букв к верхнему регистру). Дальше, когда мы прошли все буквы, функция вызывает функцю, которая складывает все буквы. И потом результат ксорится с 0х5678. Теперь аналогично анализируем функцию sub4013D8. Она по сути делает atoi(char* password), если в пароле одни цифры. И потом полученное число ксорится с 0х1234. Вот и все, теперь чтобы мы попали в хороший путь, нужно, чтобы еах и еbх были равны. На полученных знаниях легко написать саму программу.