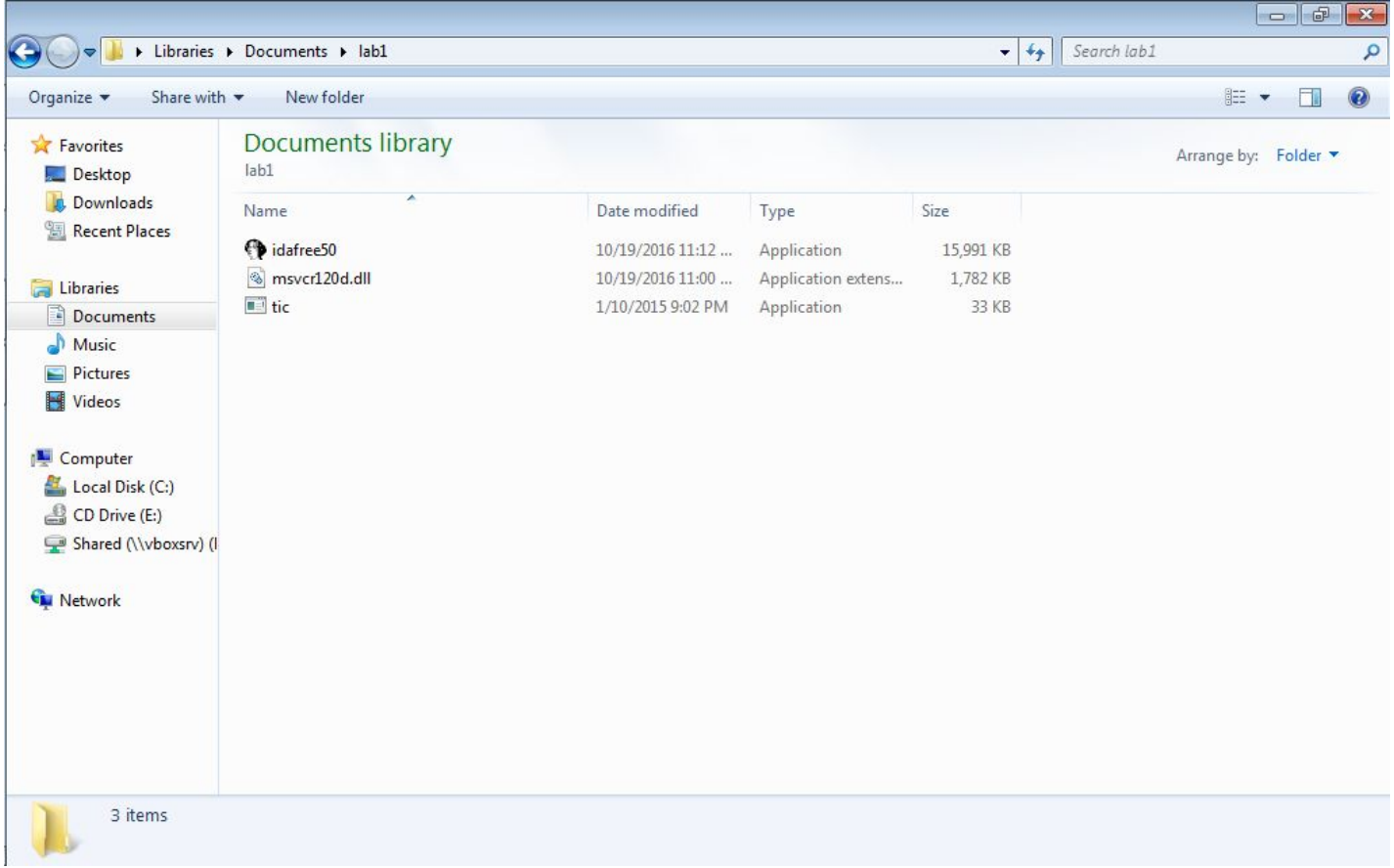
Анализ машинного кода

IDA

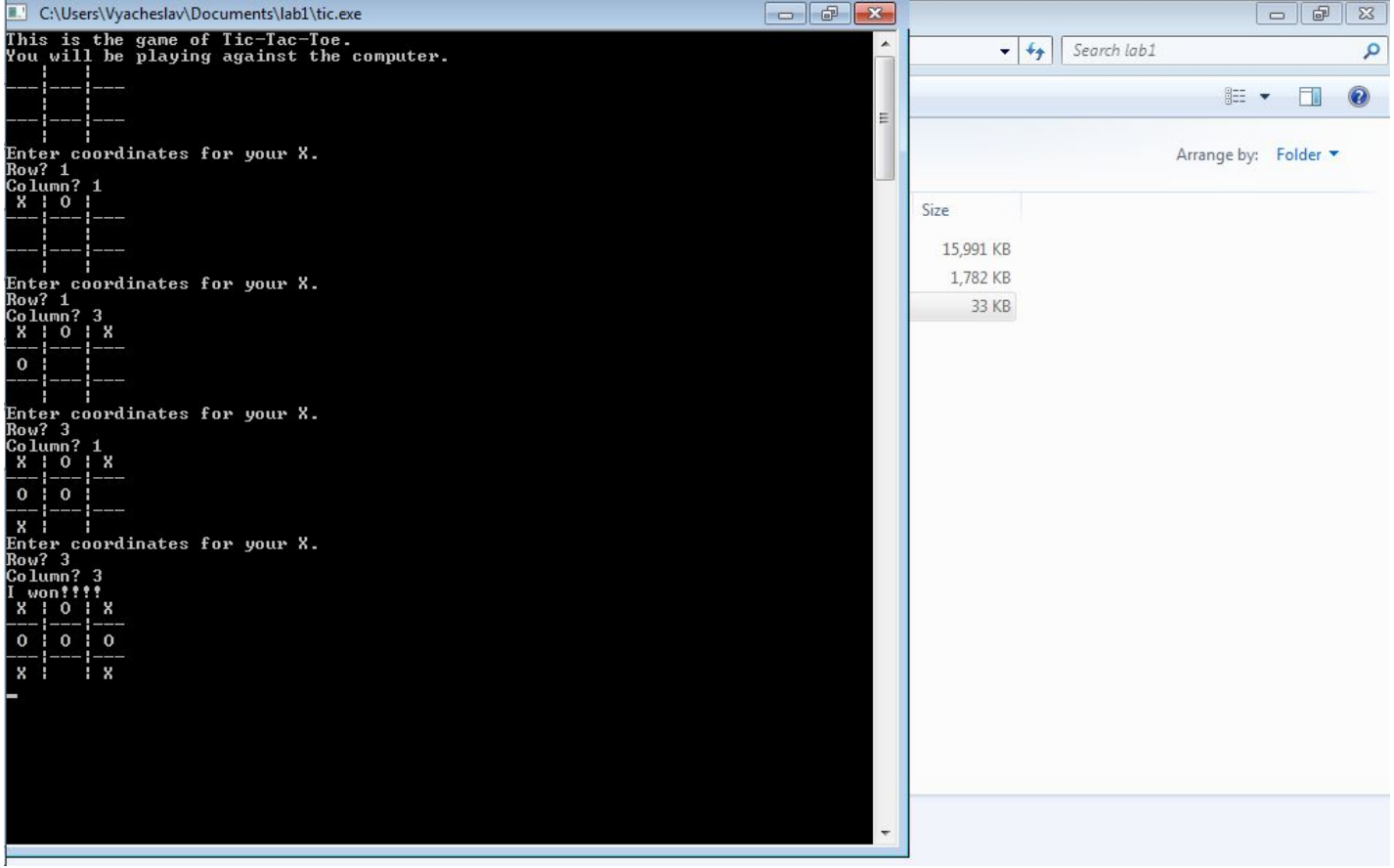
IDA

A disassembler

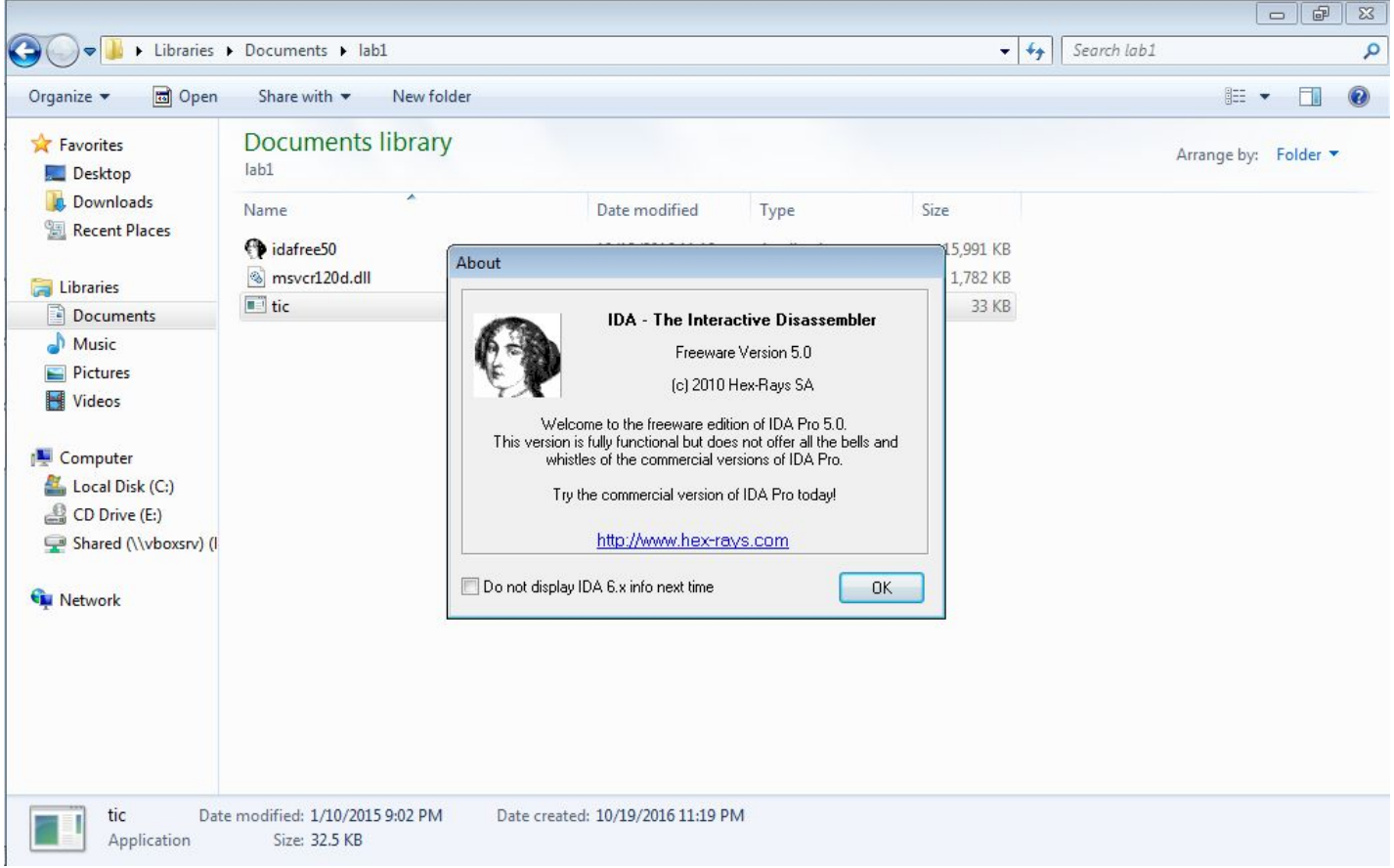
- Имеется программа
- Исходный код недоступен
- Как внести изменения?



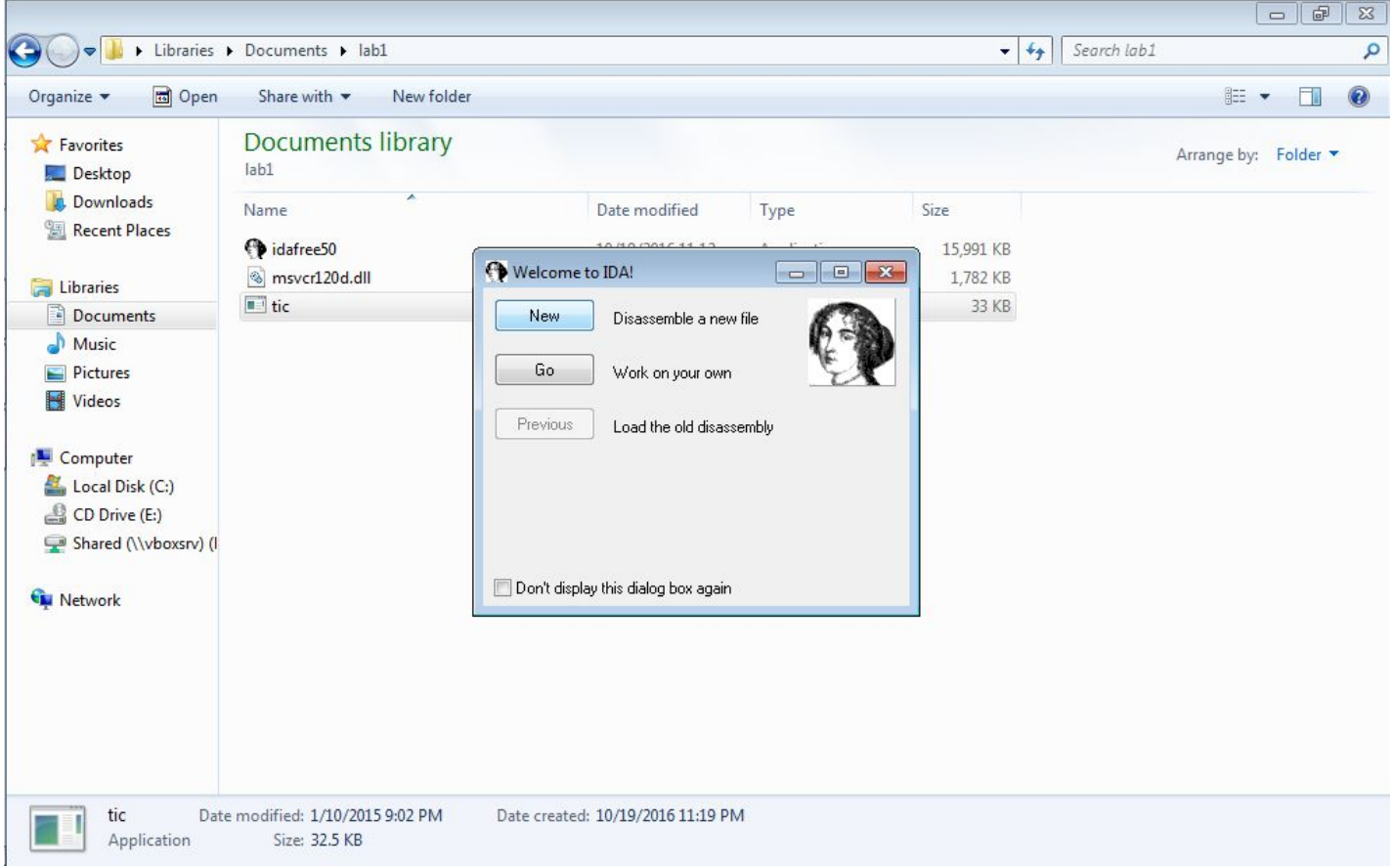
Есть программа без исходного кода



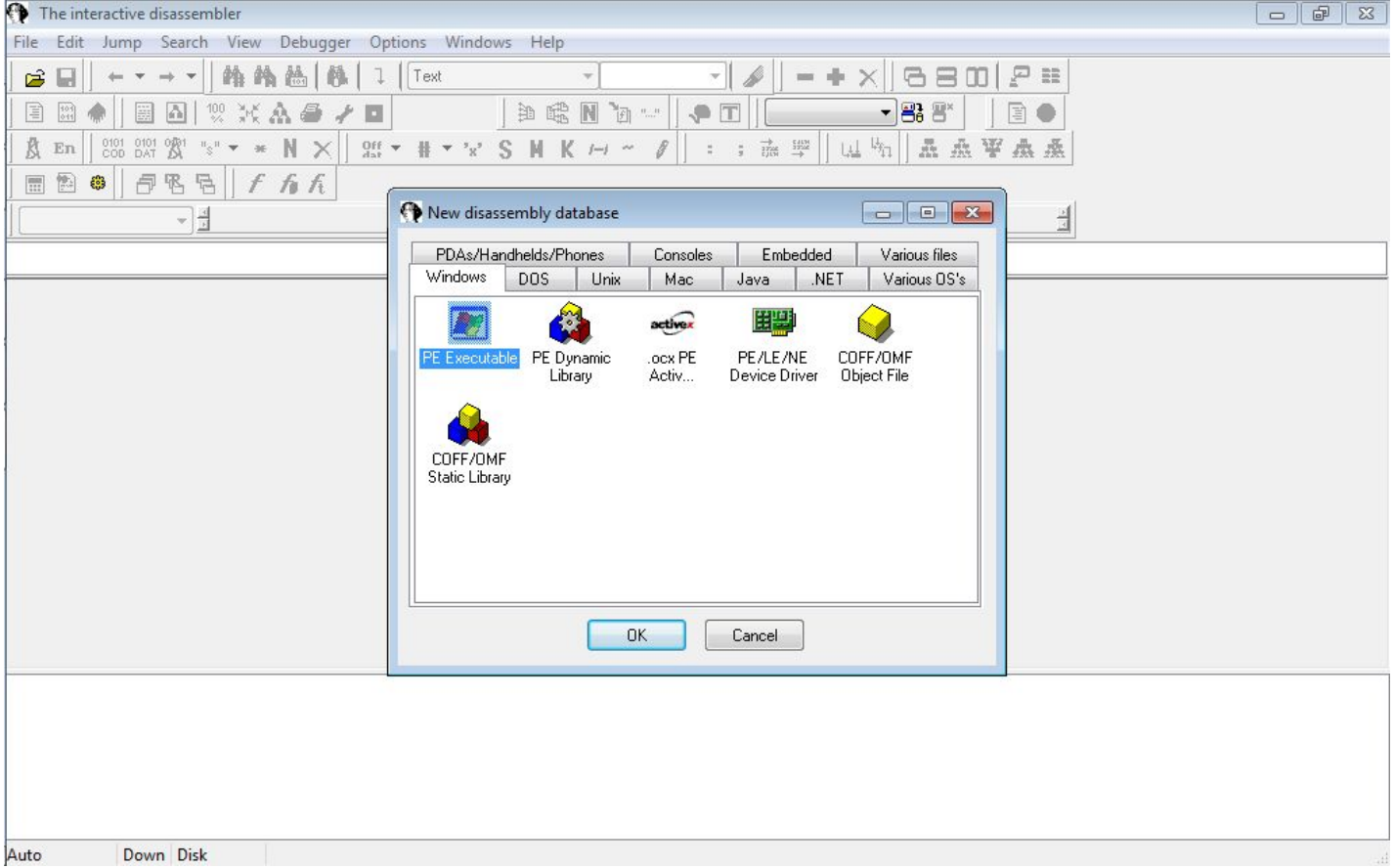
Работает корректно



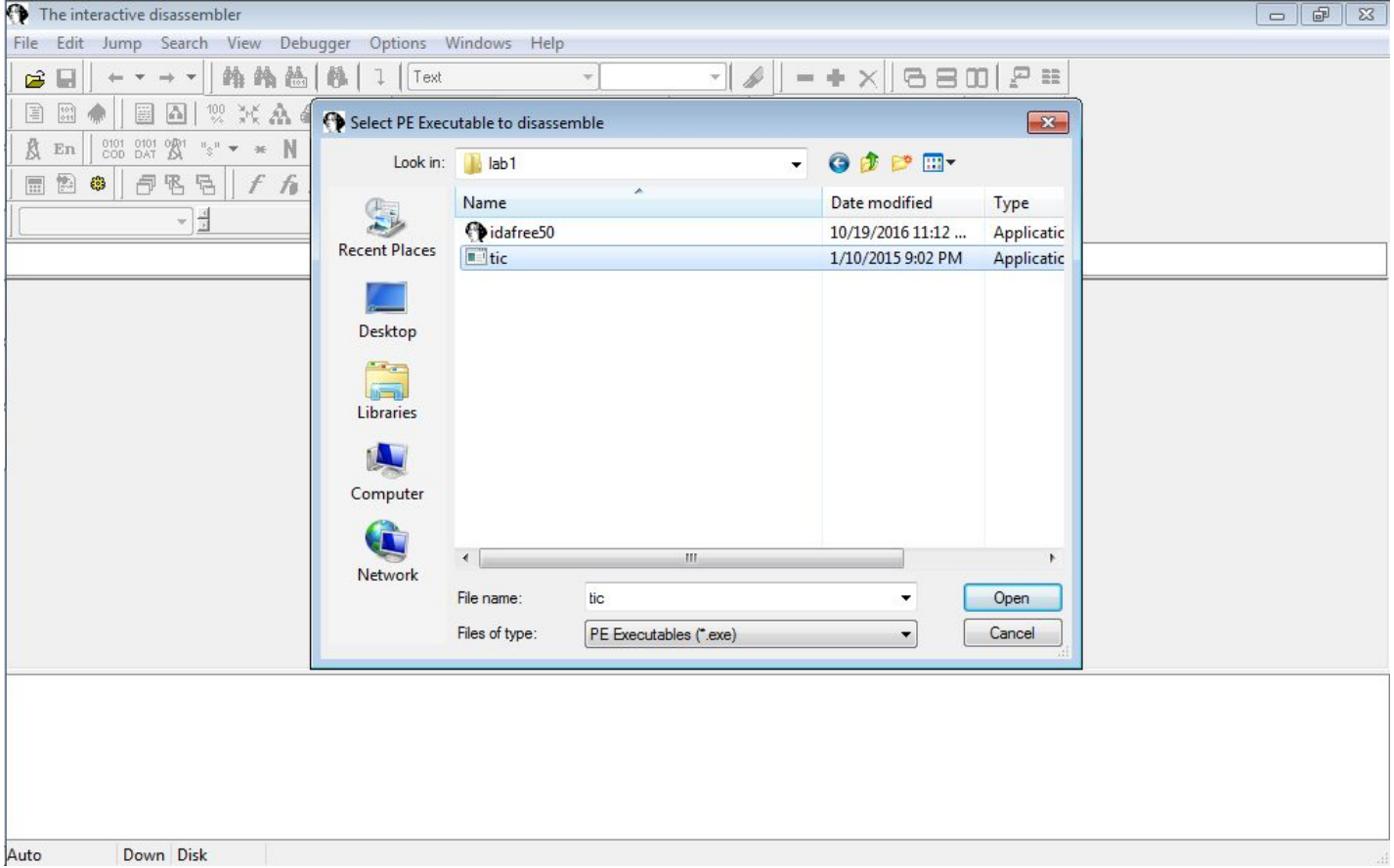
Изменим поведение на желаемое



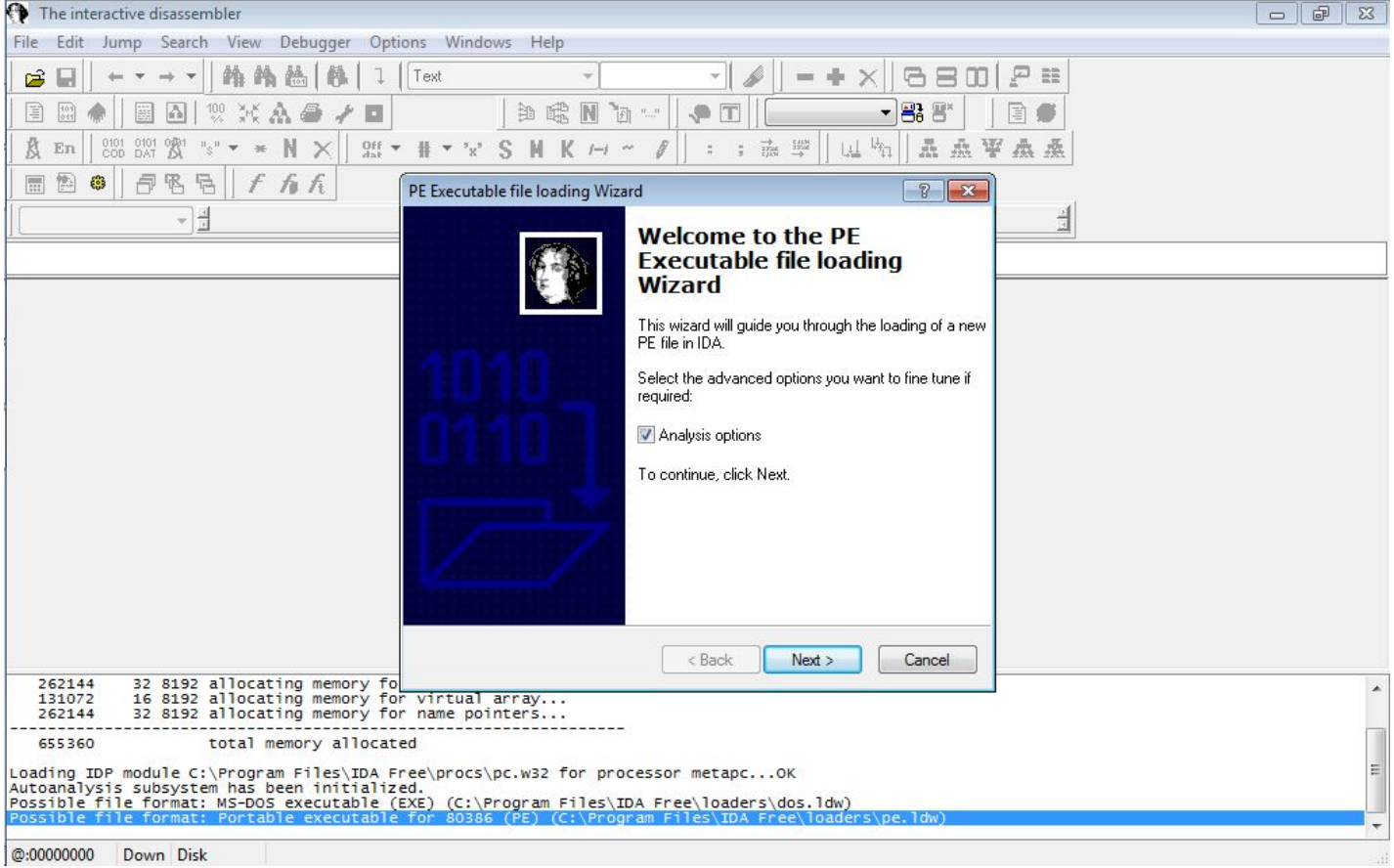
Исследуем машинные инструкции



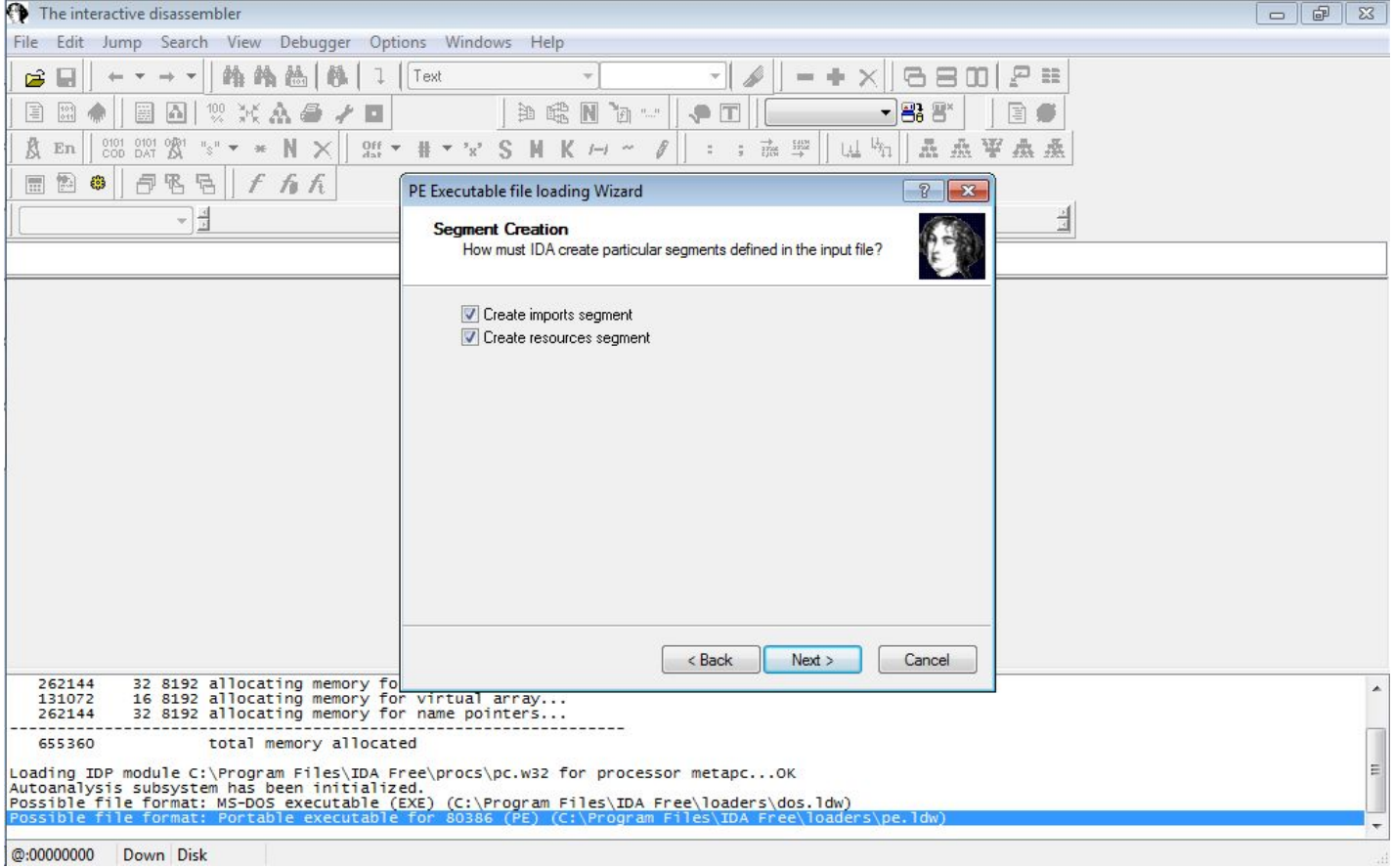
Добавим новую базу



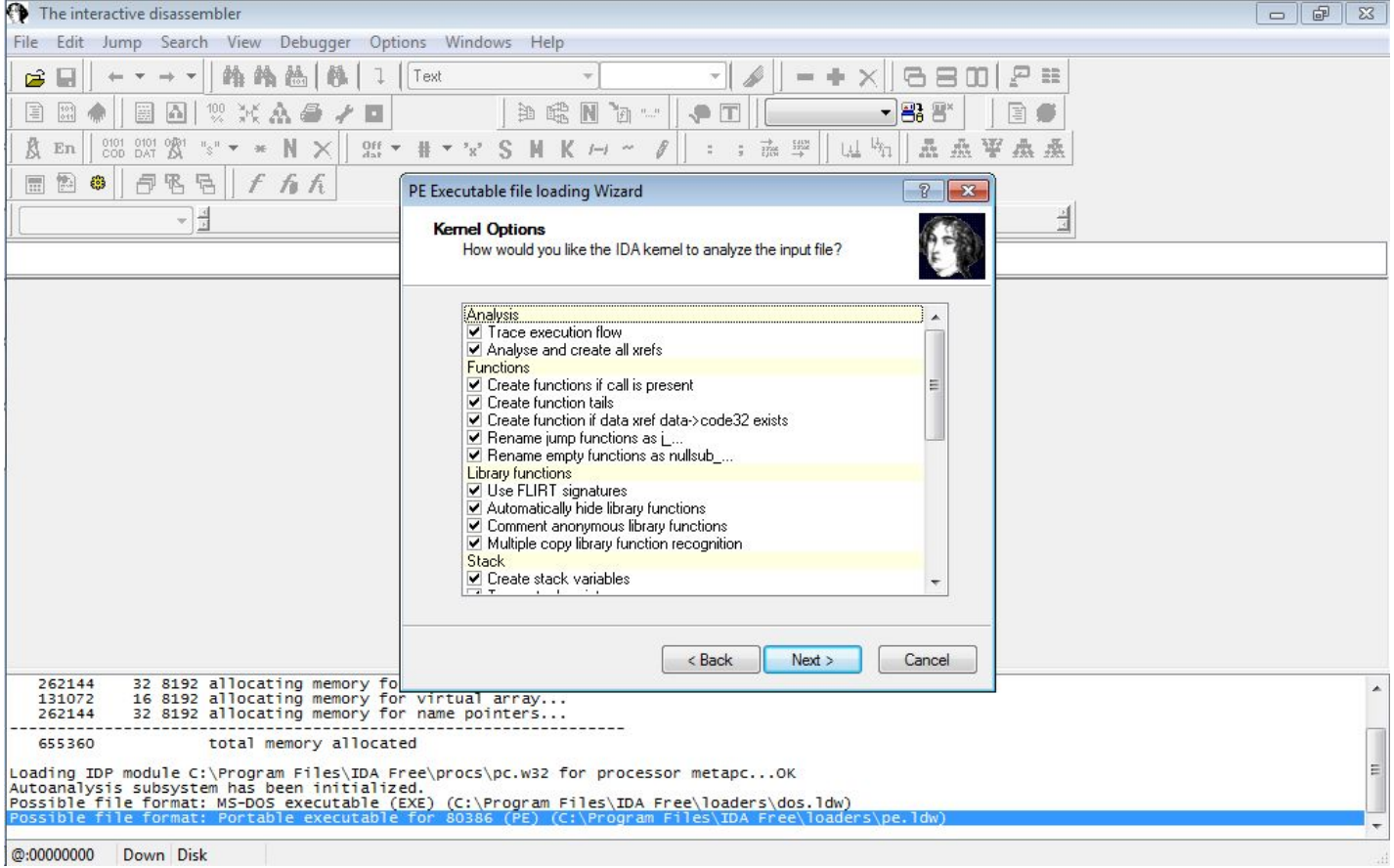
Загрузим исполняемый файл в IDA



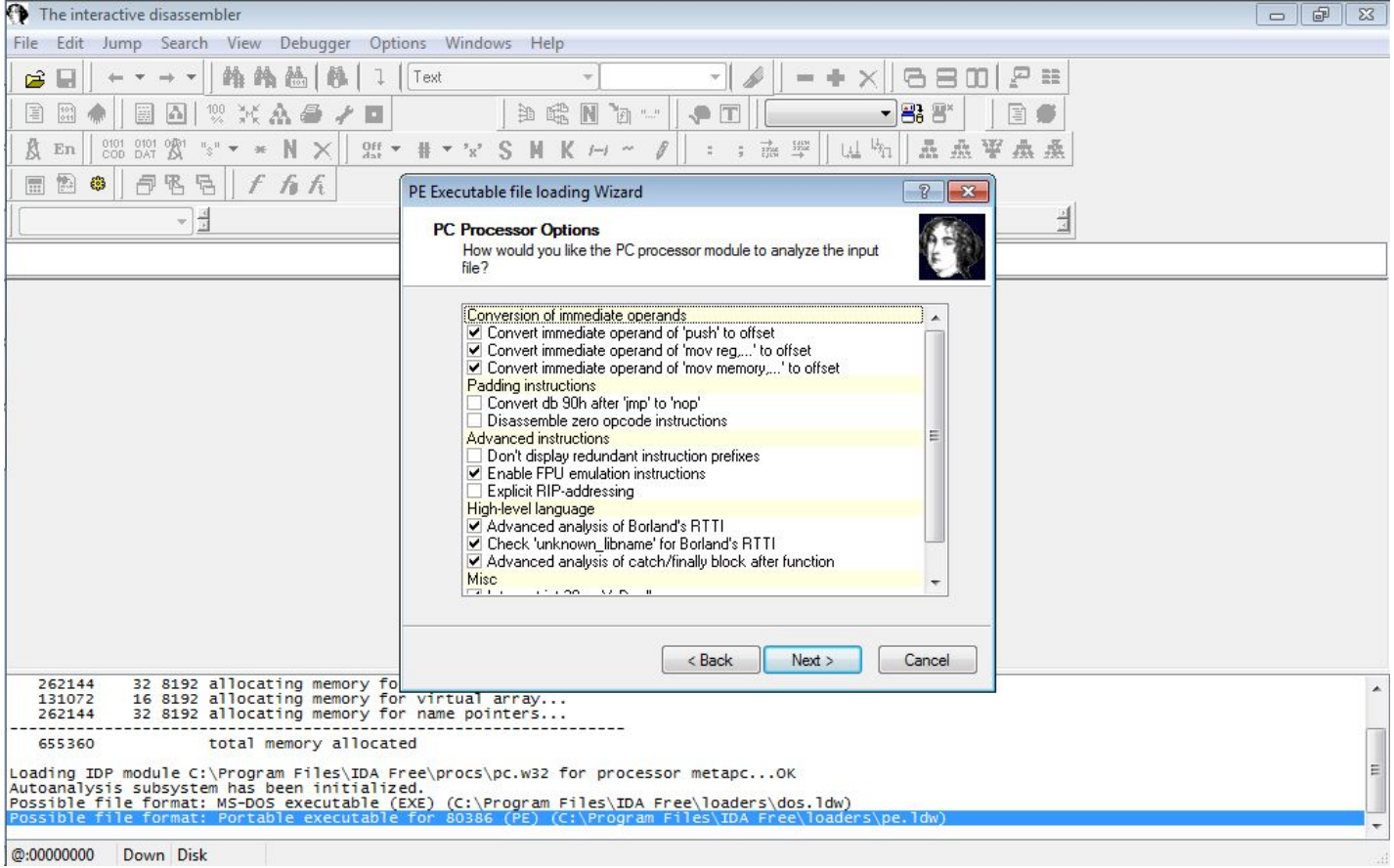
Мастер загрузки



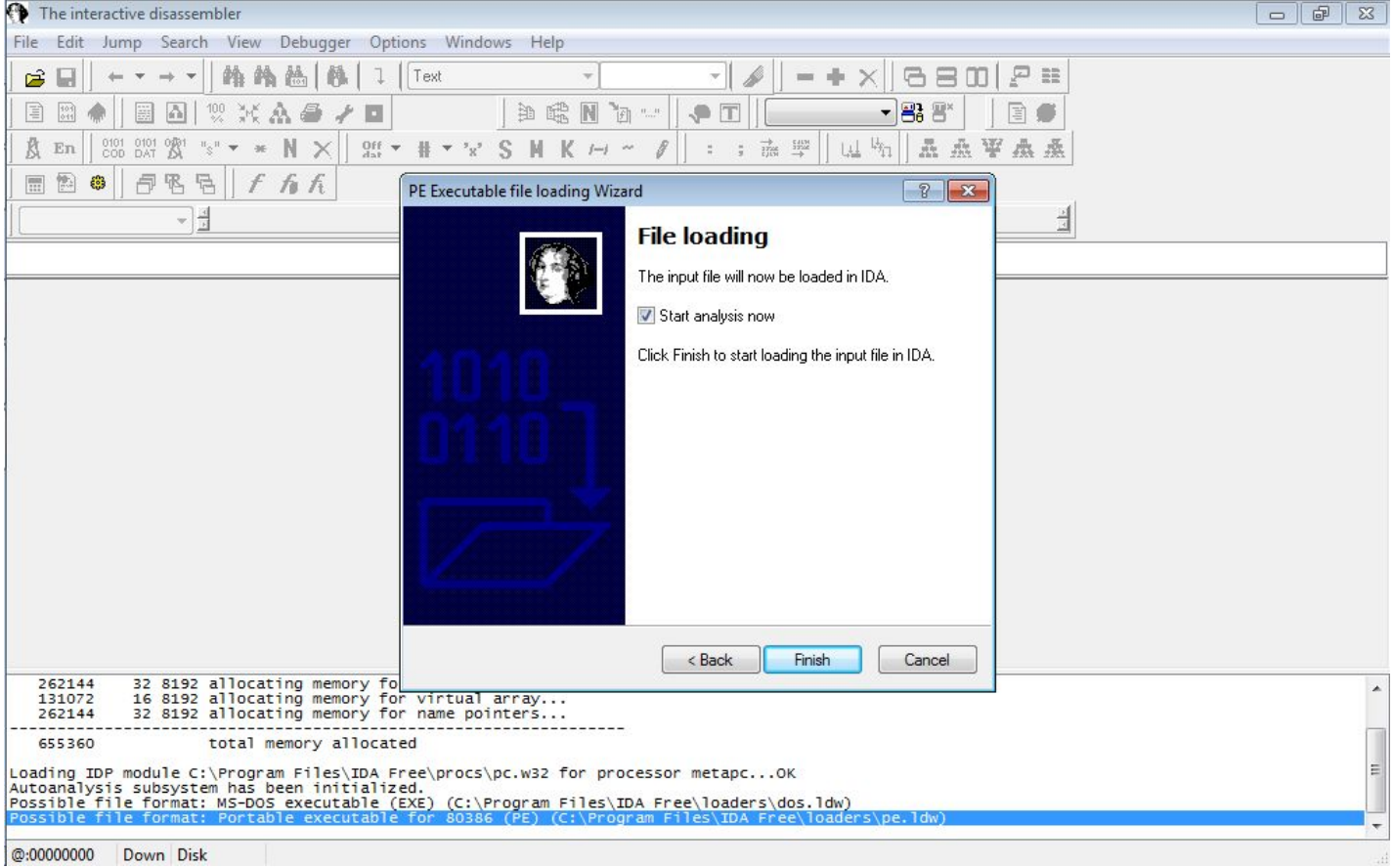
Создаем нужные сегменты



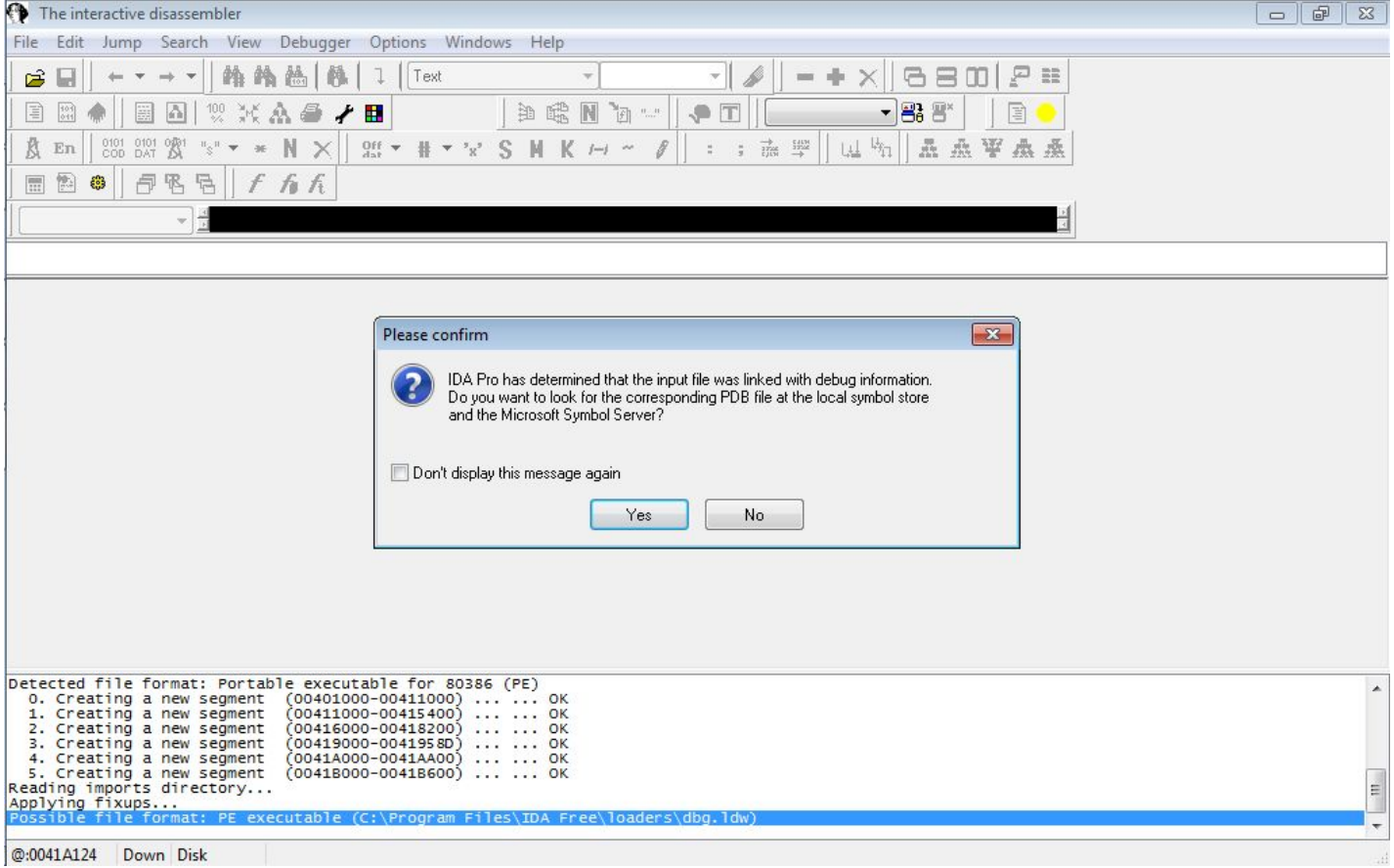
Опции IDA kernel



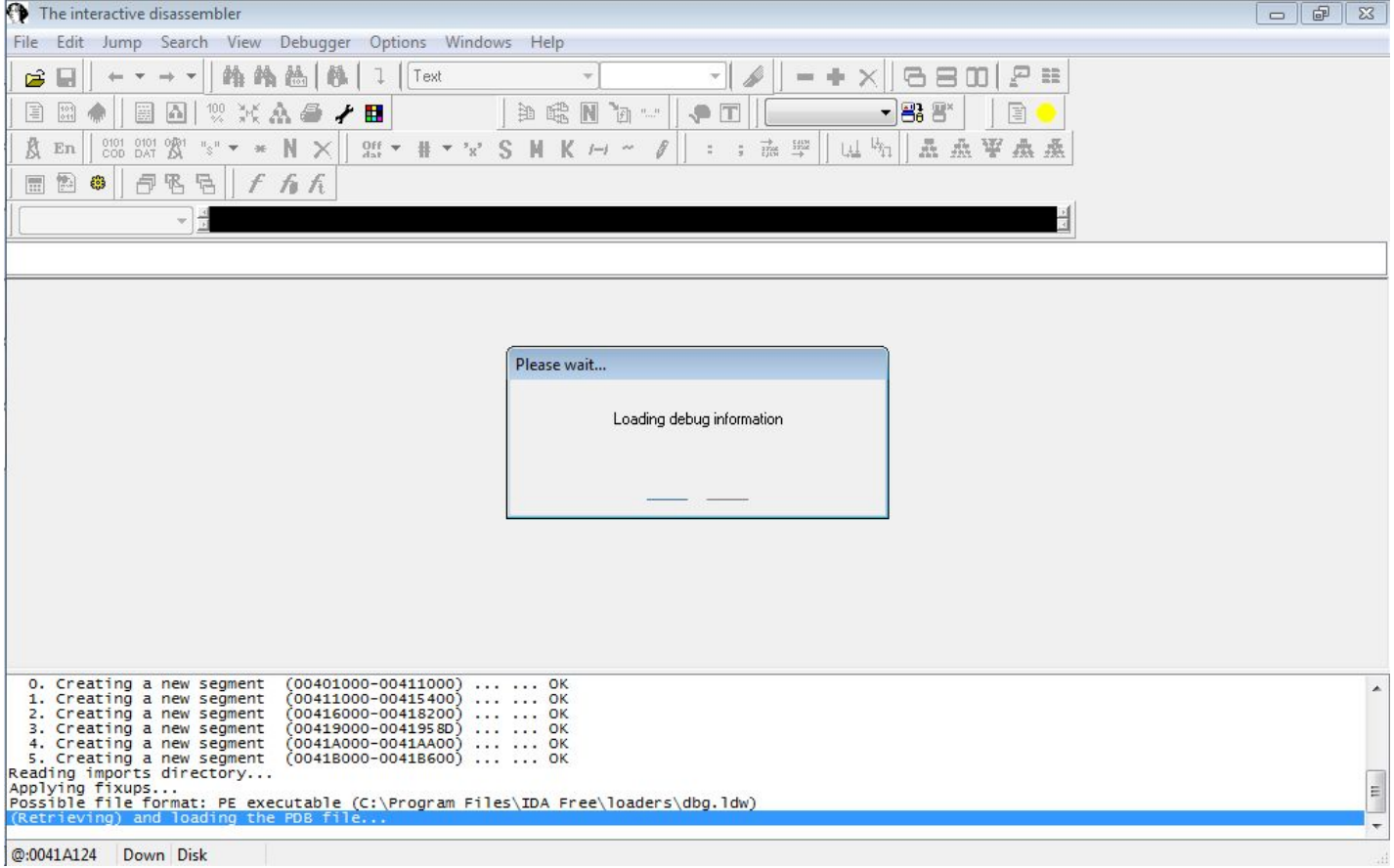
Опции PC processor



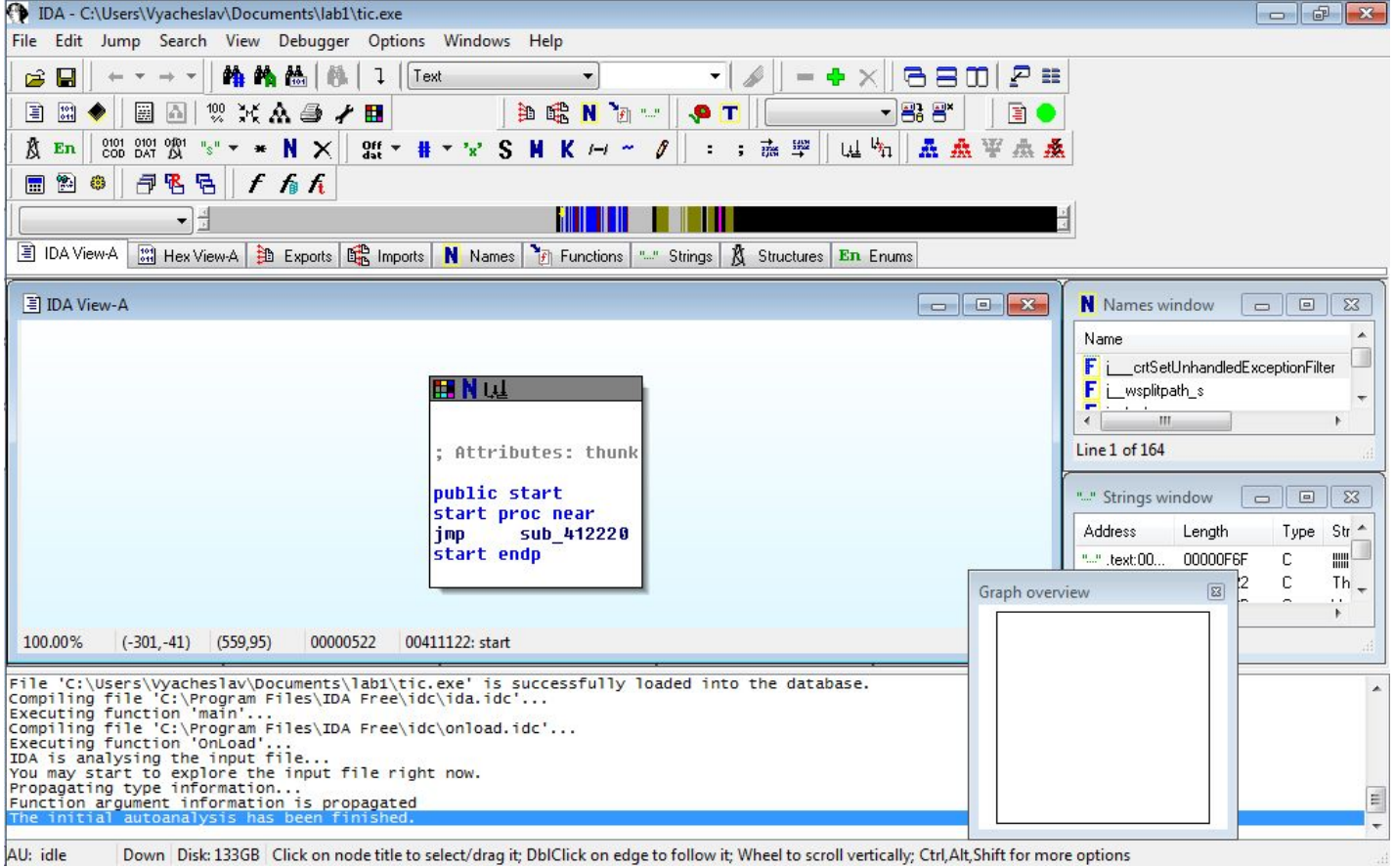
Запуск дизассемблирования



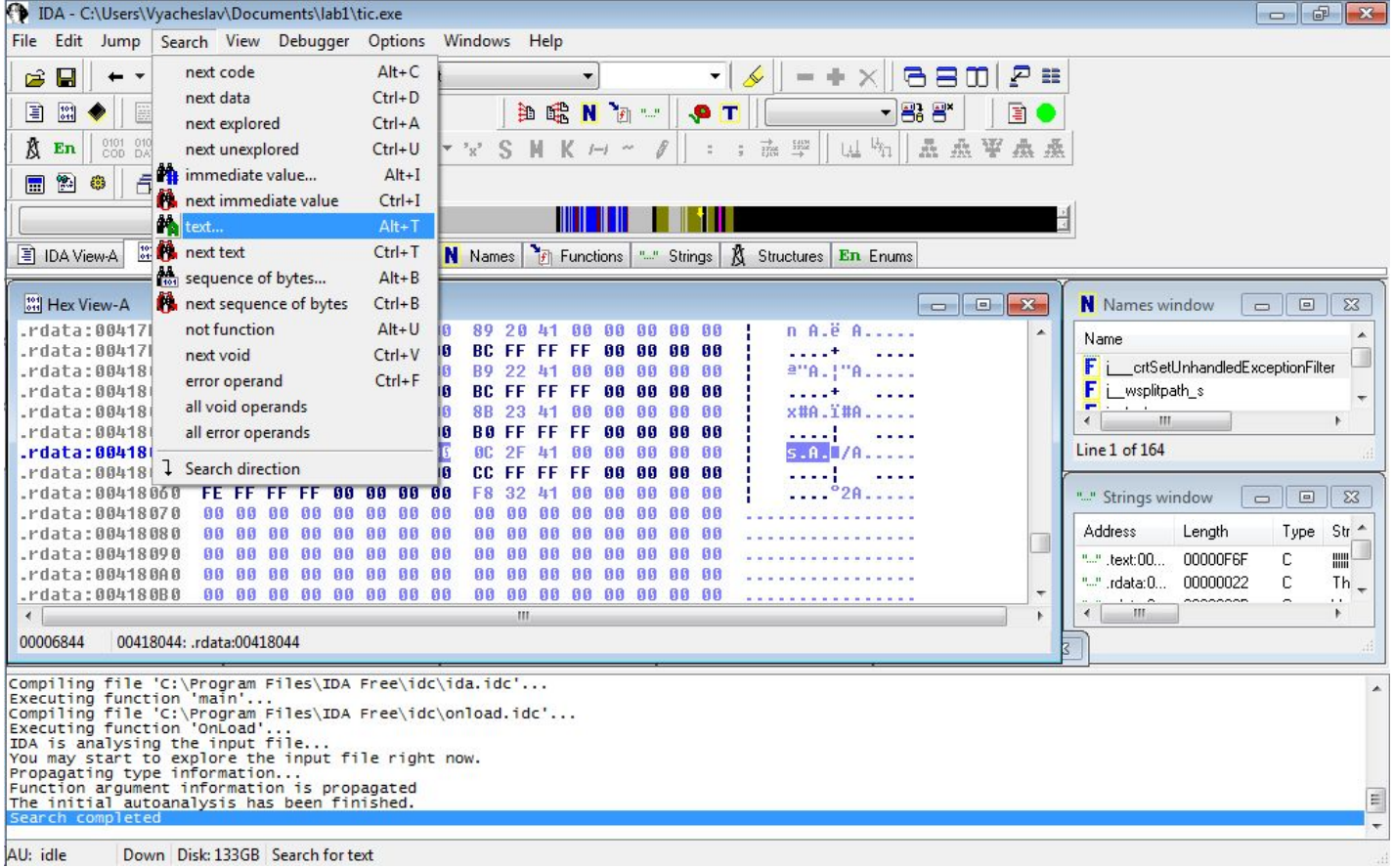
IDA сообщает о зависимостях



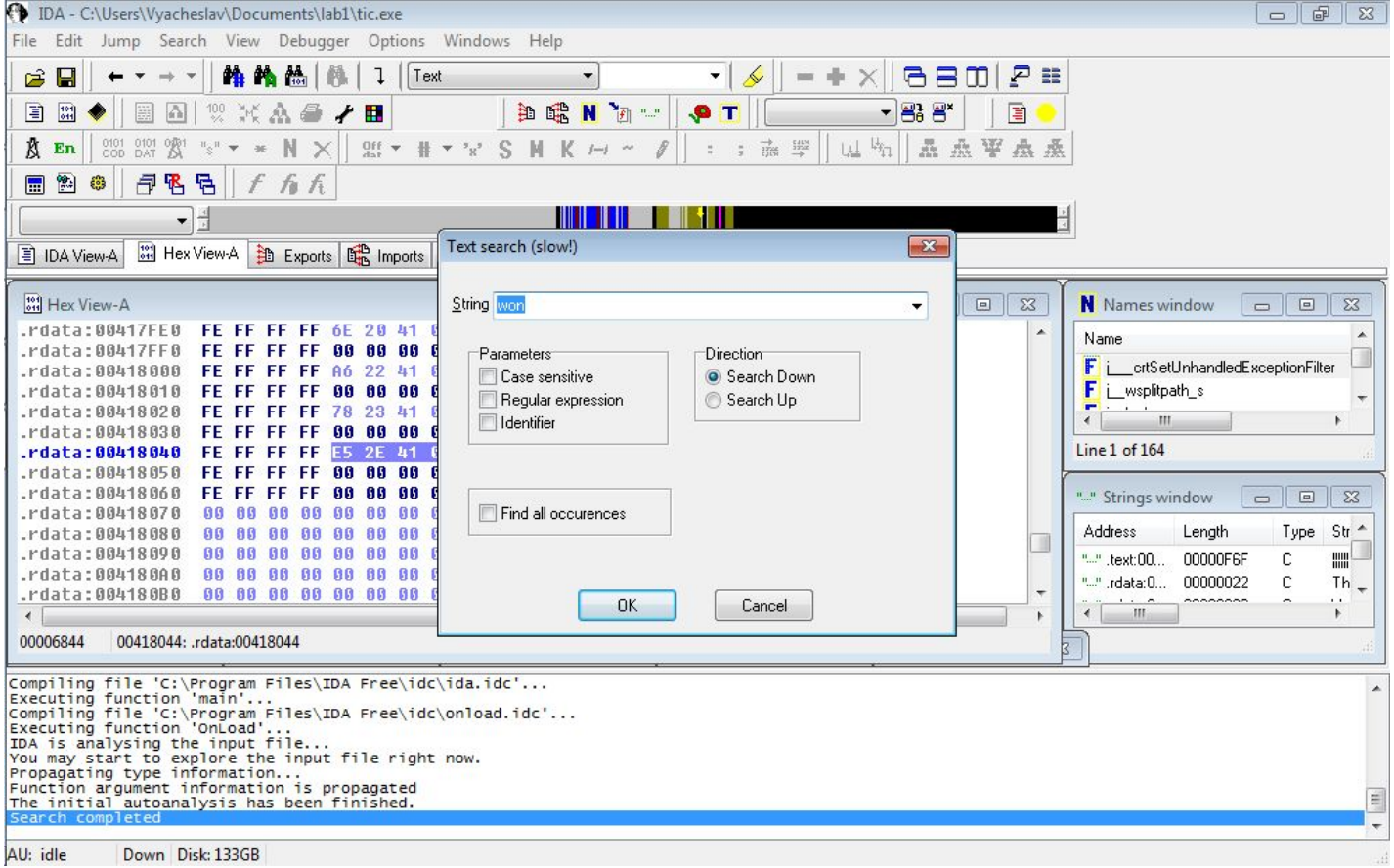
Подгрузка символов с сервера



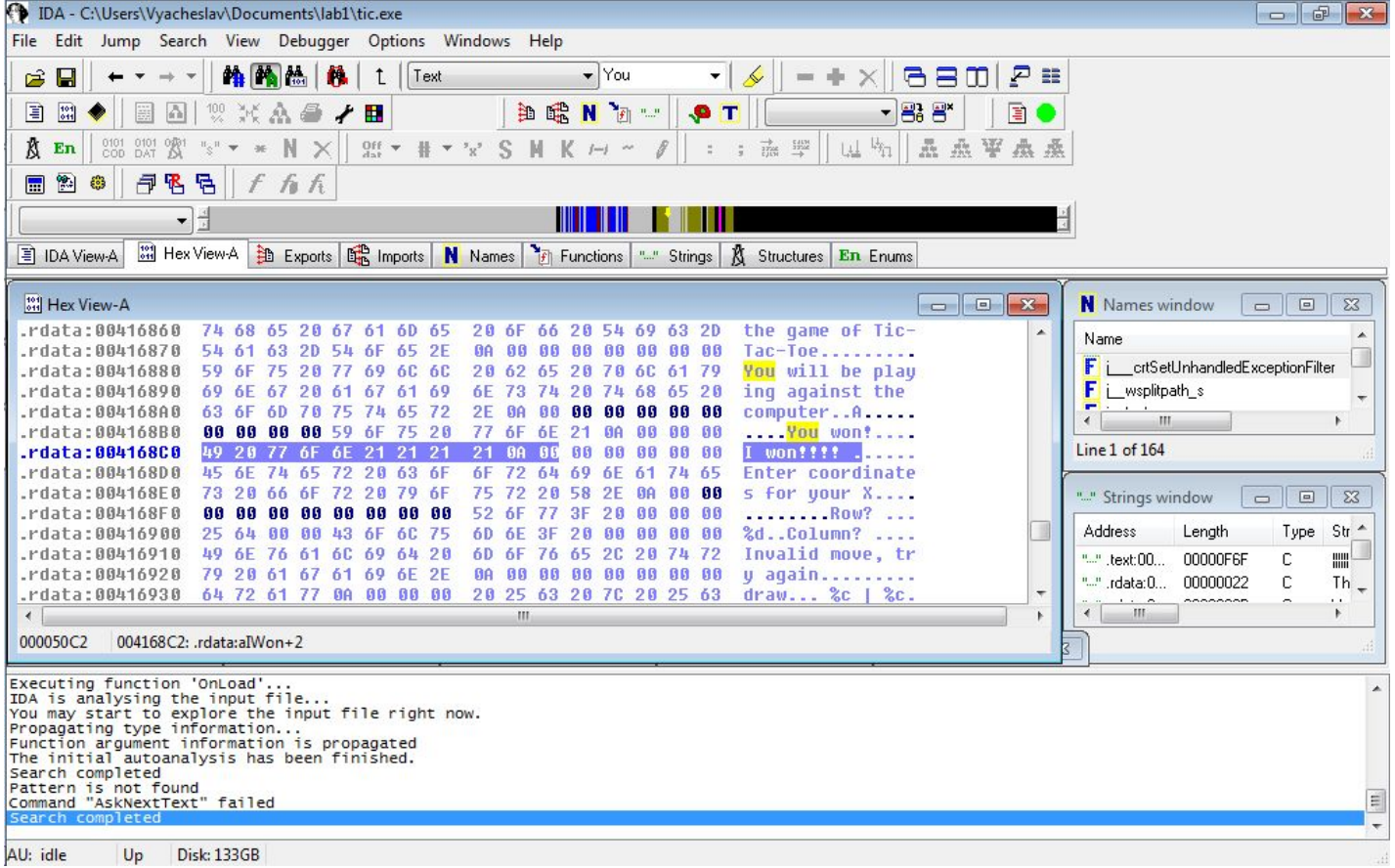
Интерфейс IDA



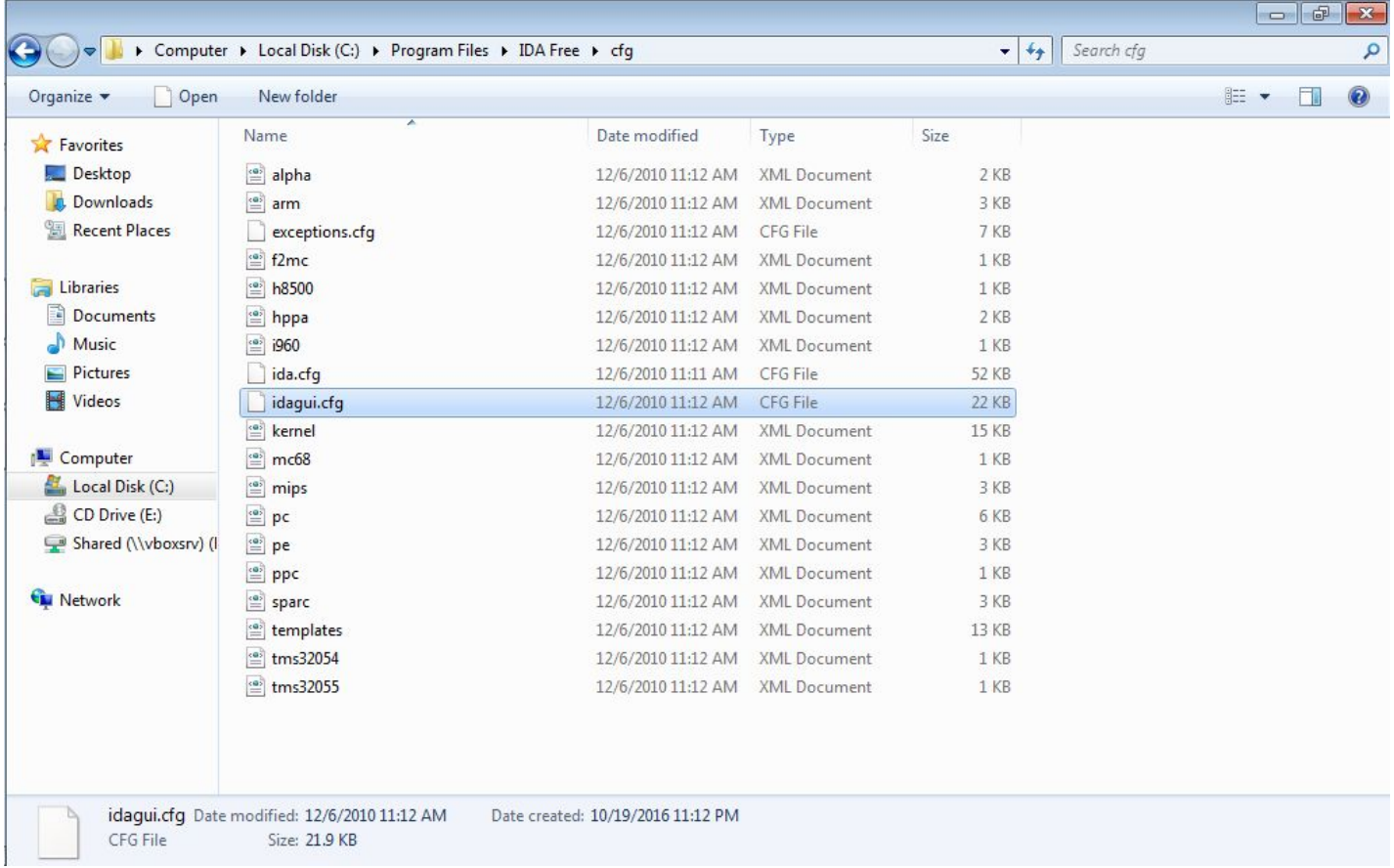
Текстовый поиск



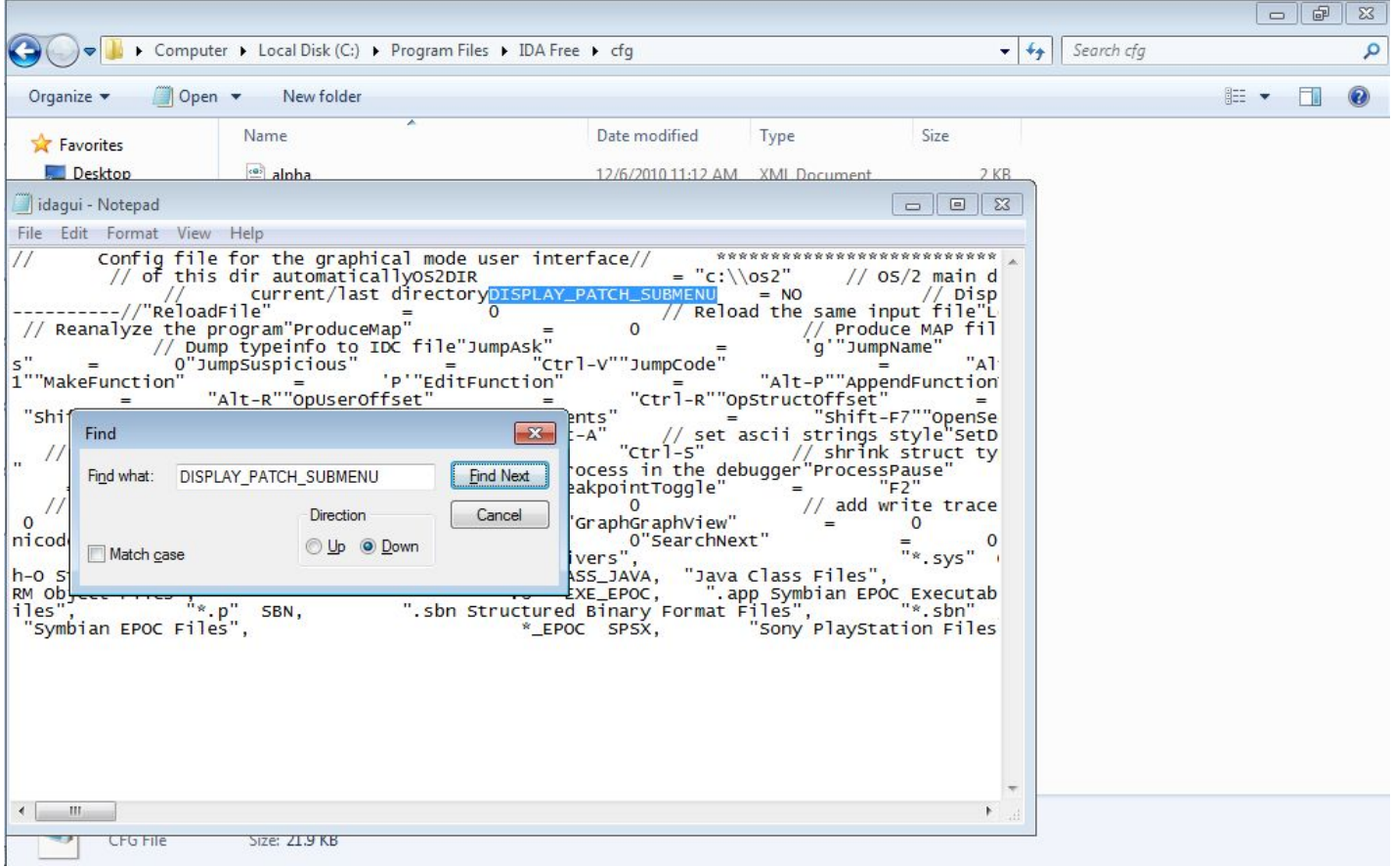
Ищем сообщение о результате



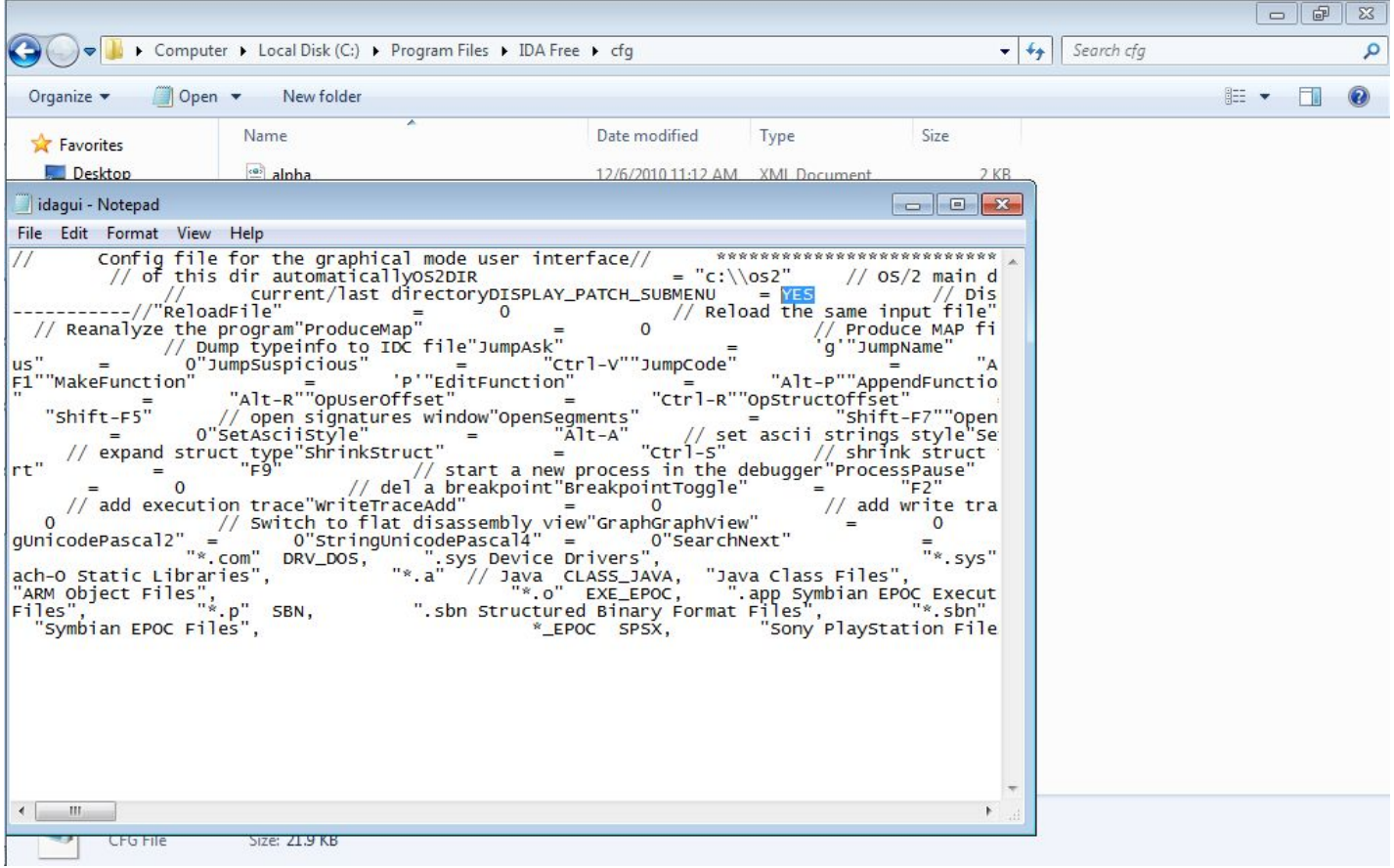
Сообщение в секции ресурсов



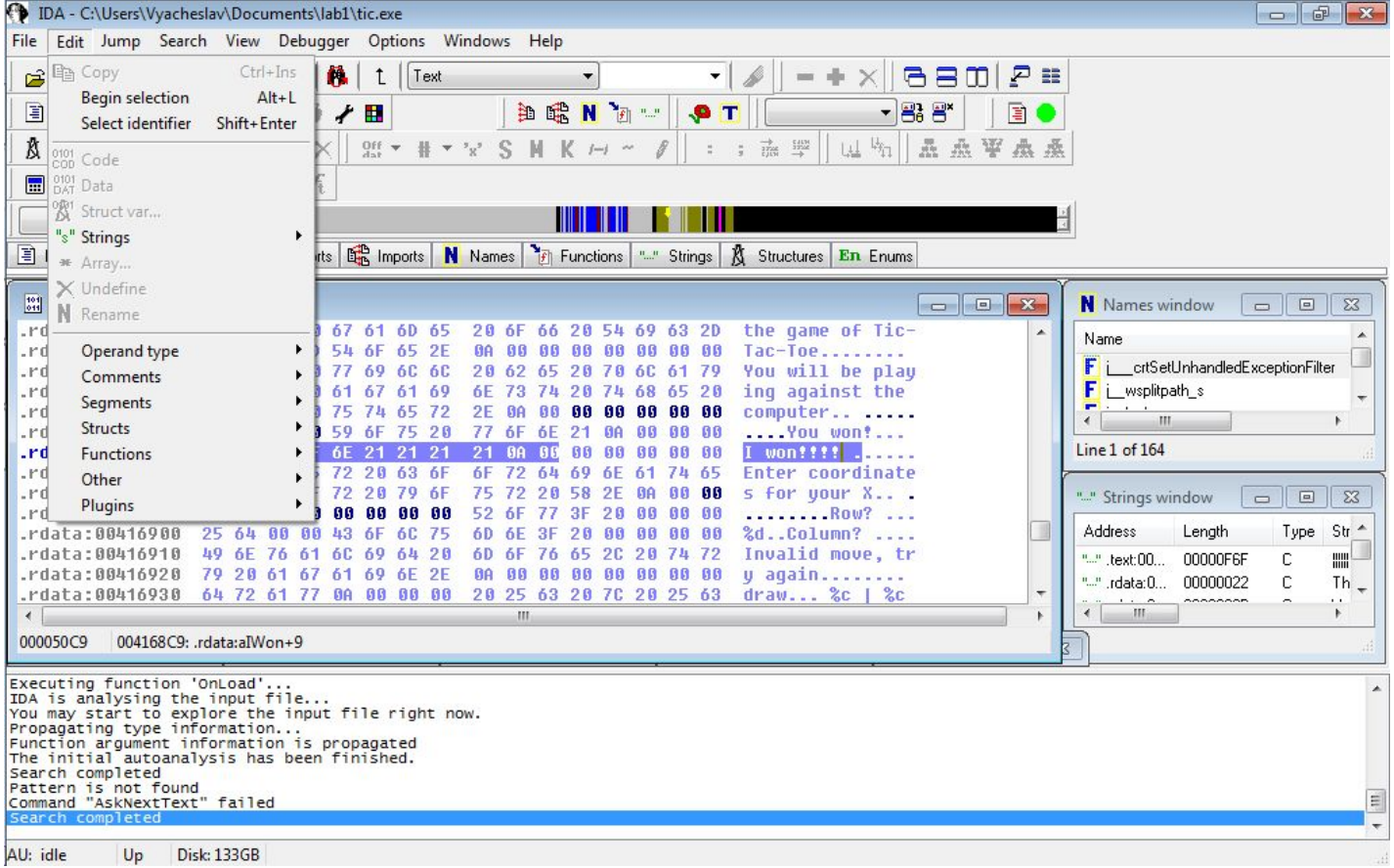
Настроим IDA для патчинга



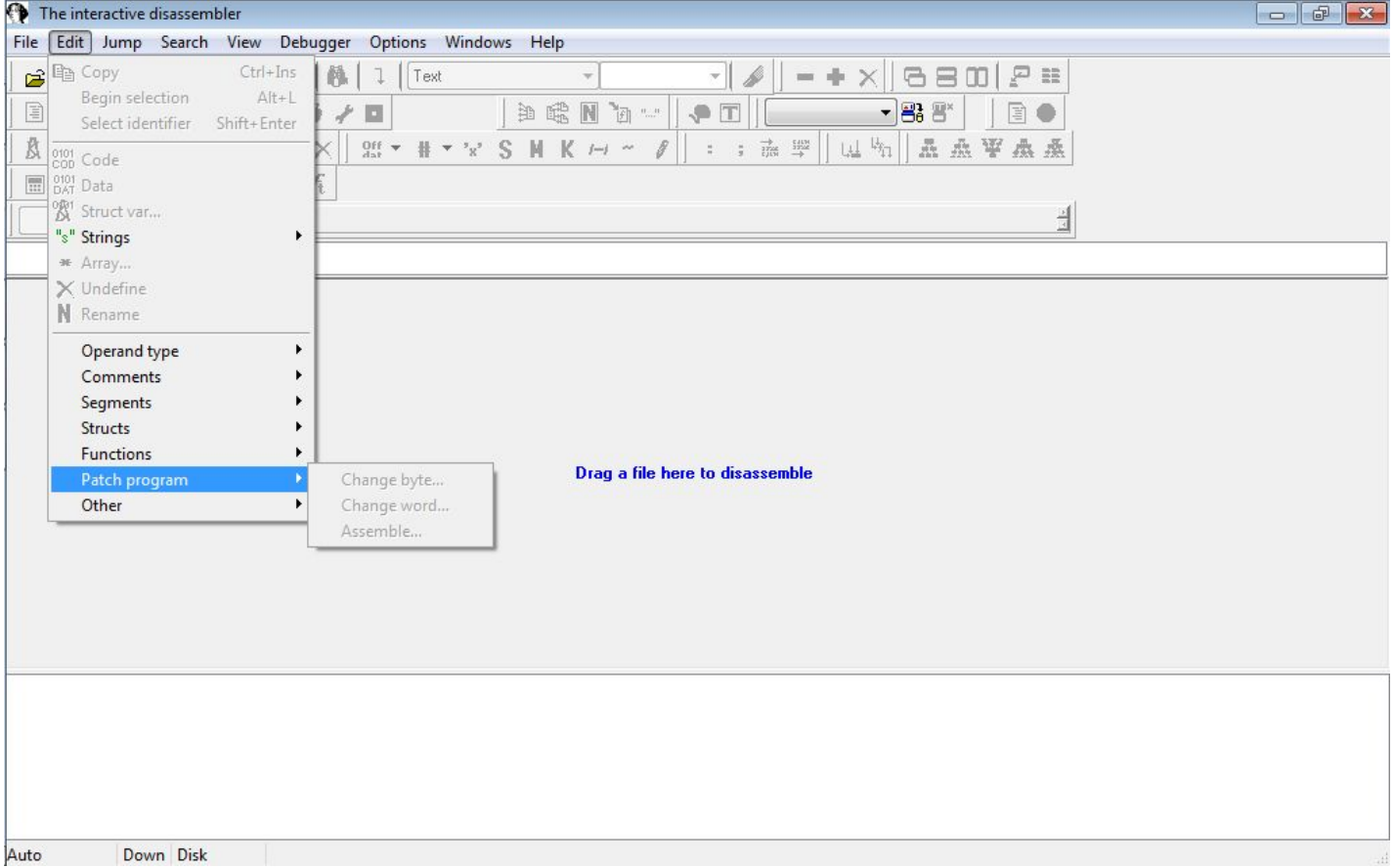
Активируем пункт меню



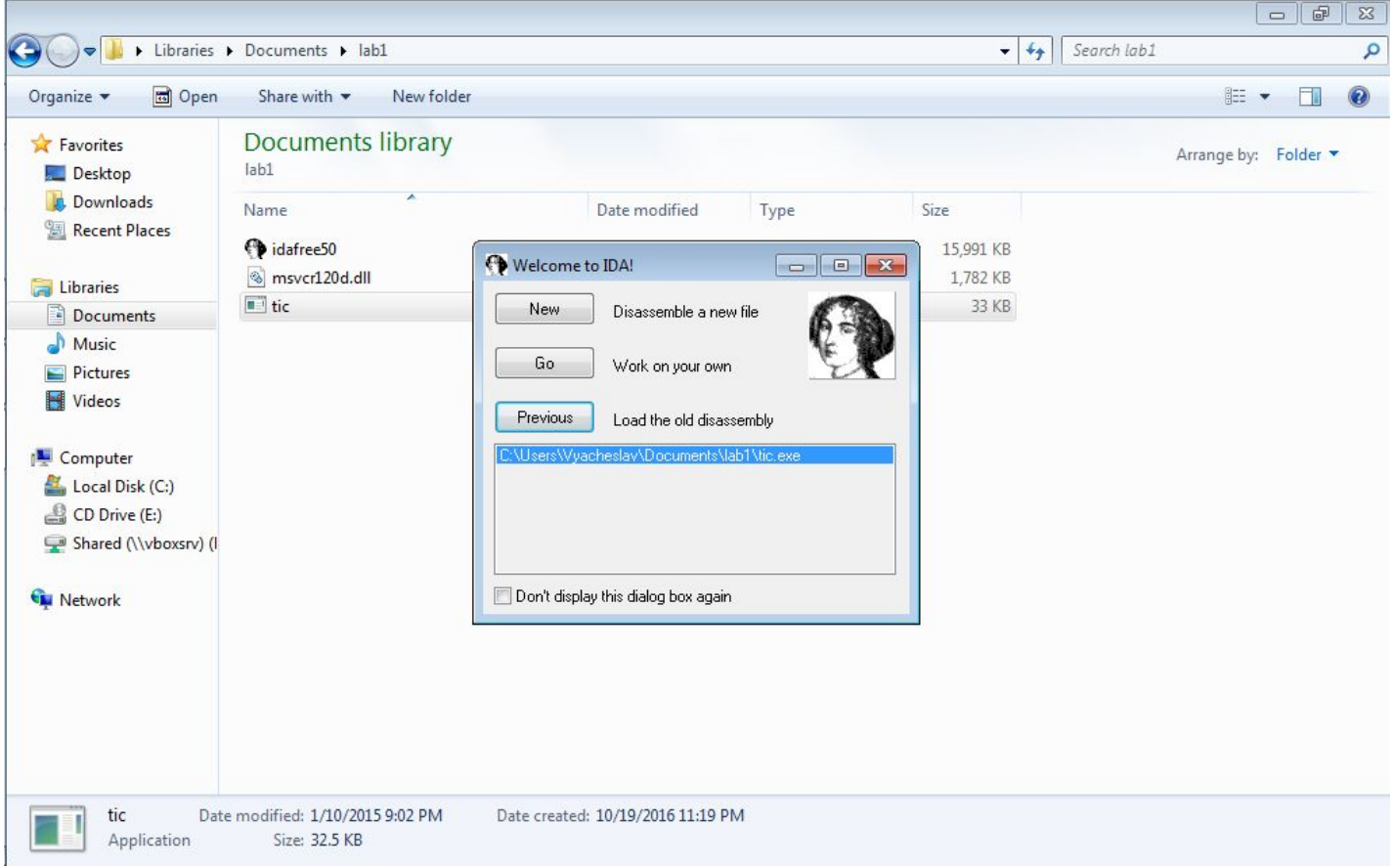
Сохраним изменения



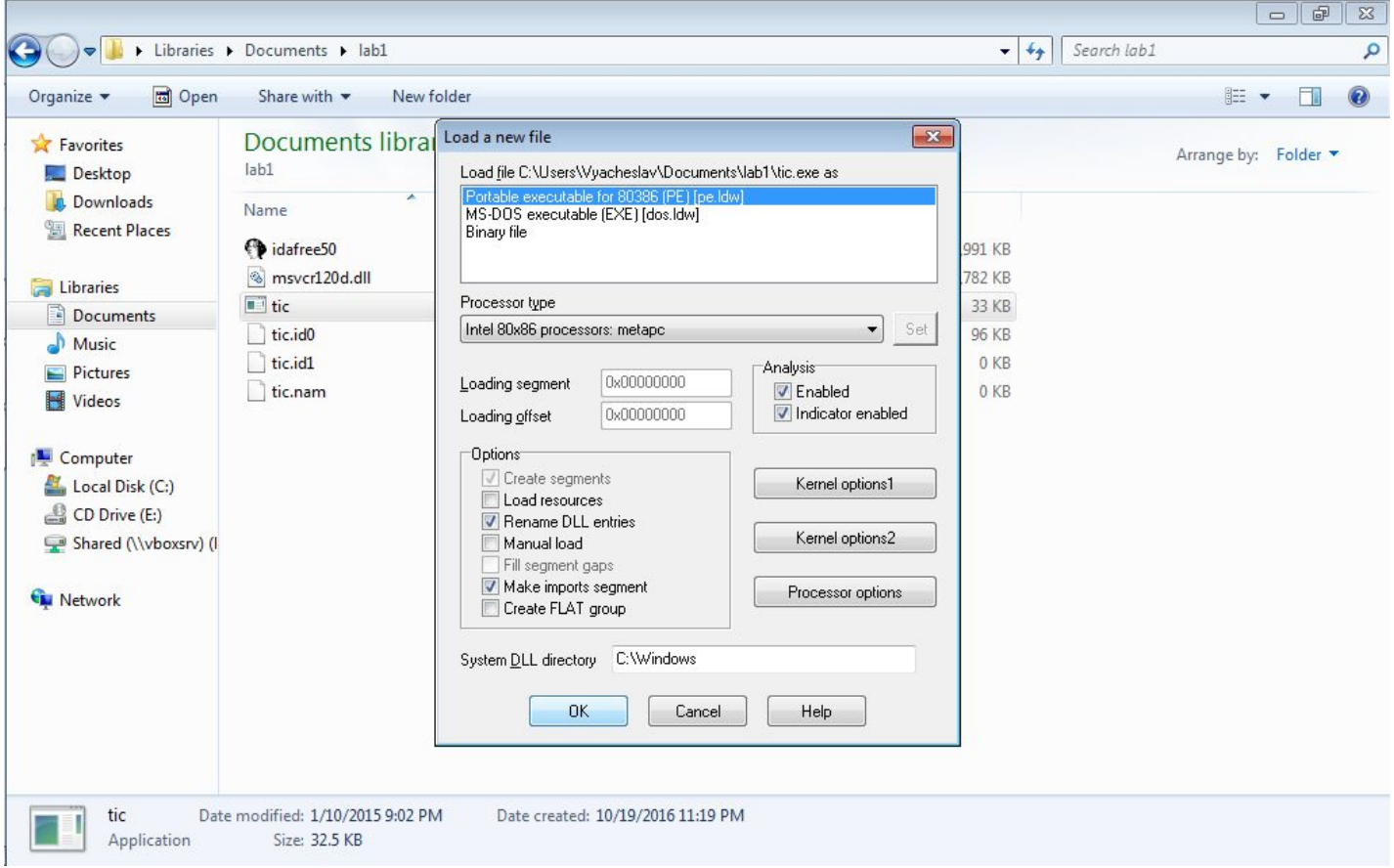
Меню Edit до изменения конфига



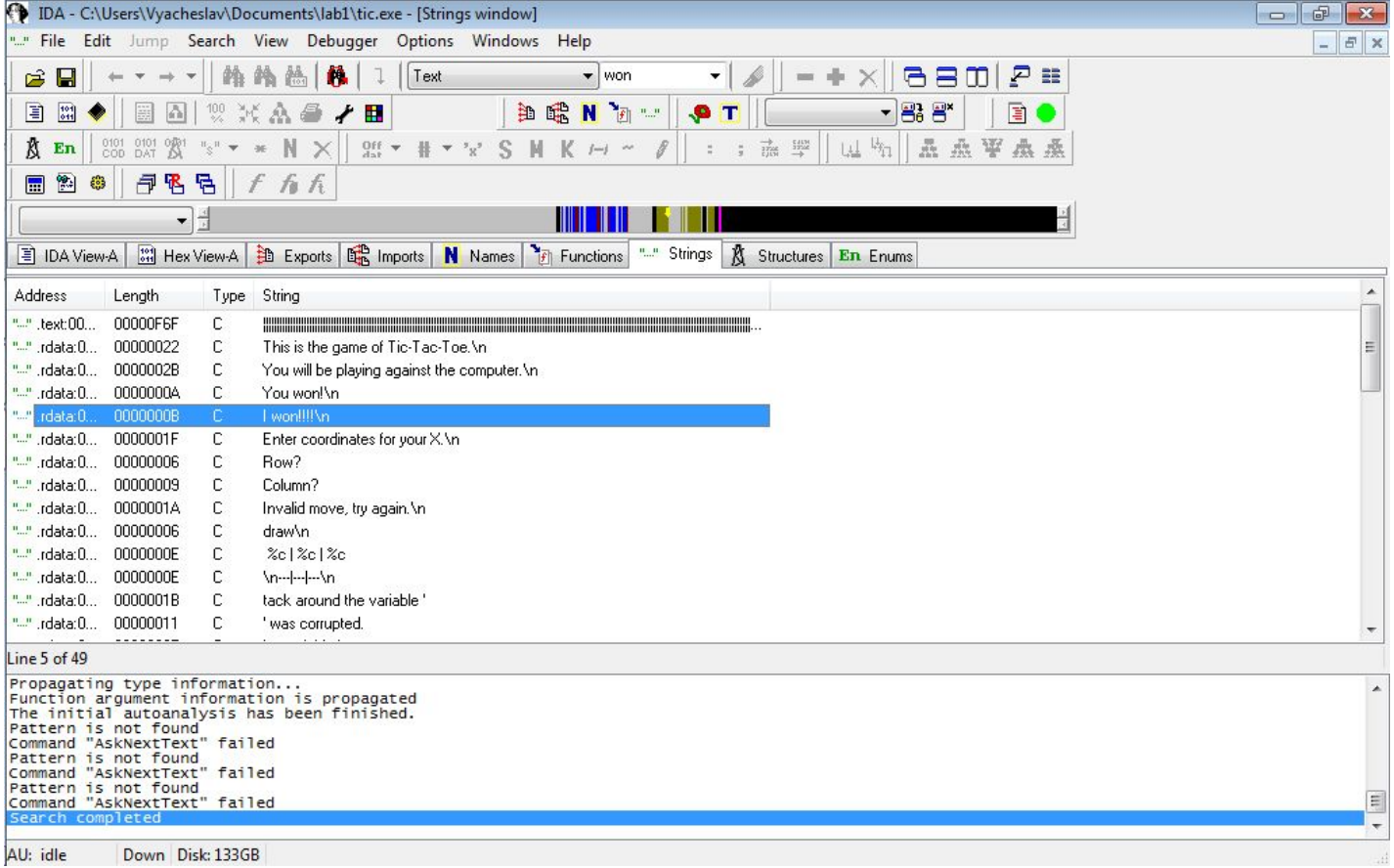
Меню Edit после (нужен перезапуск)



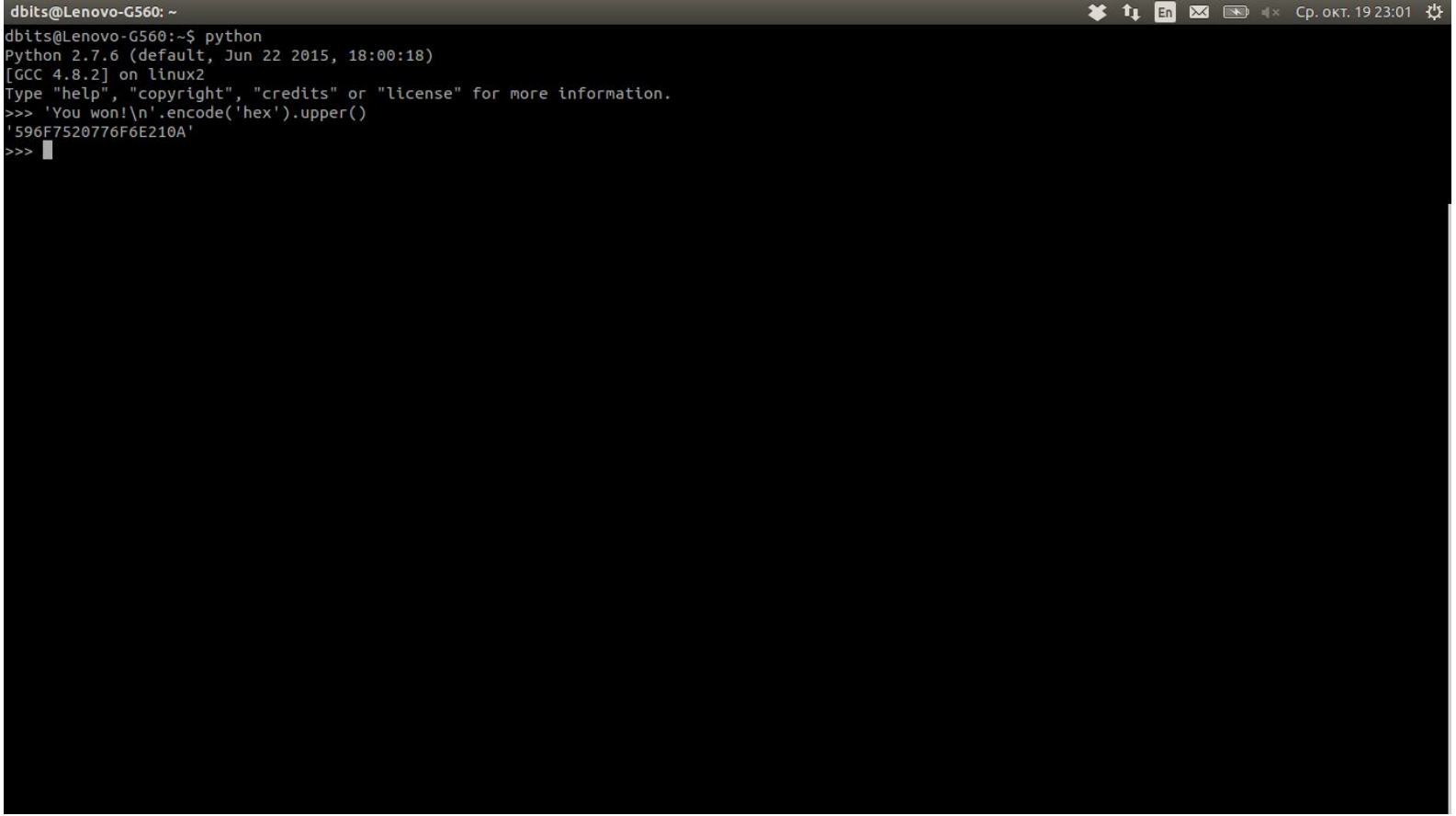
Перезапускаем прежнюю сессию



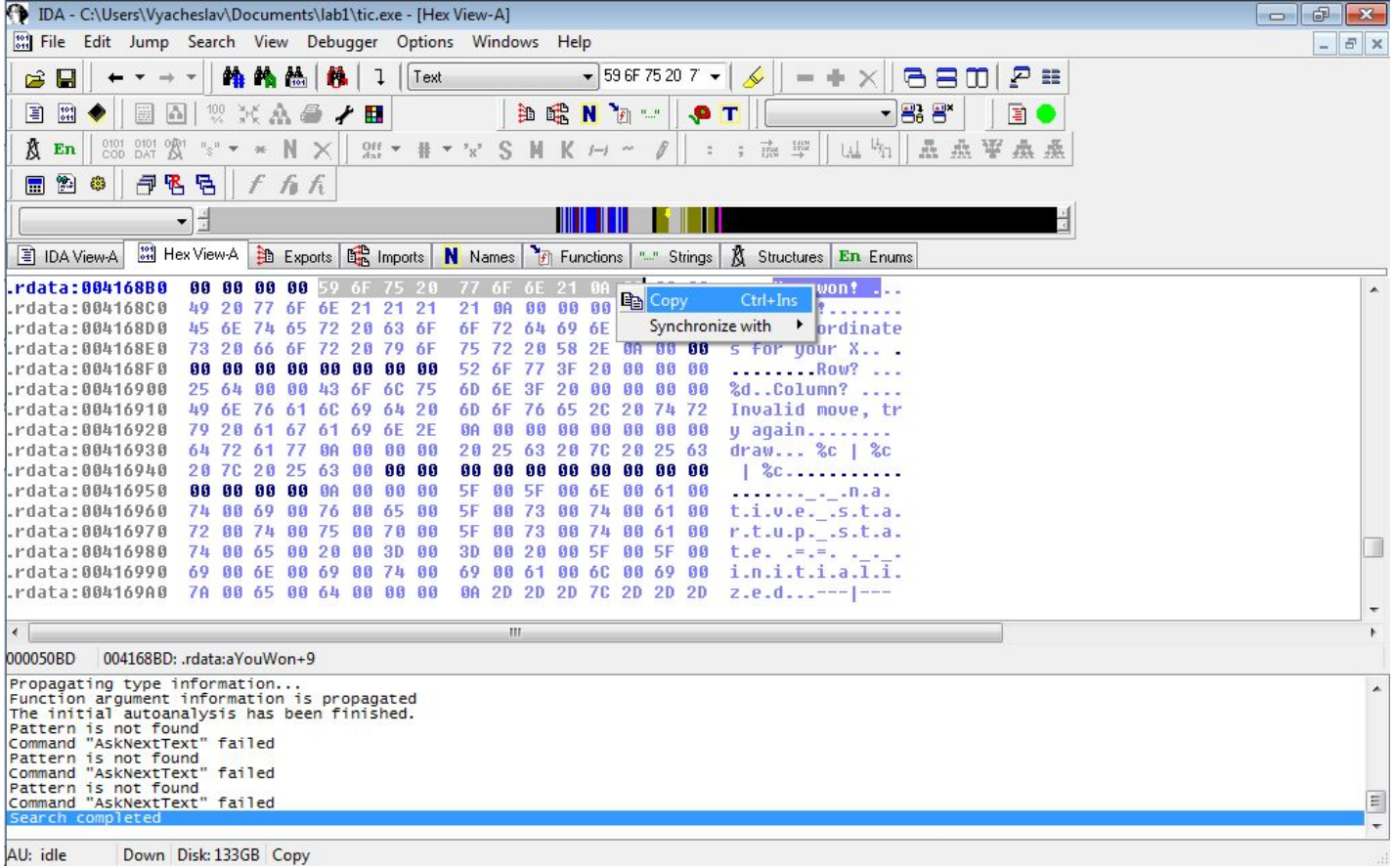
Настройка загрузки



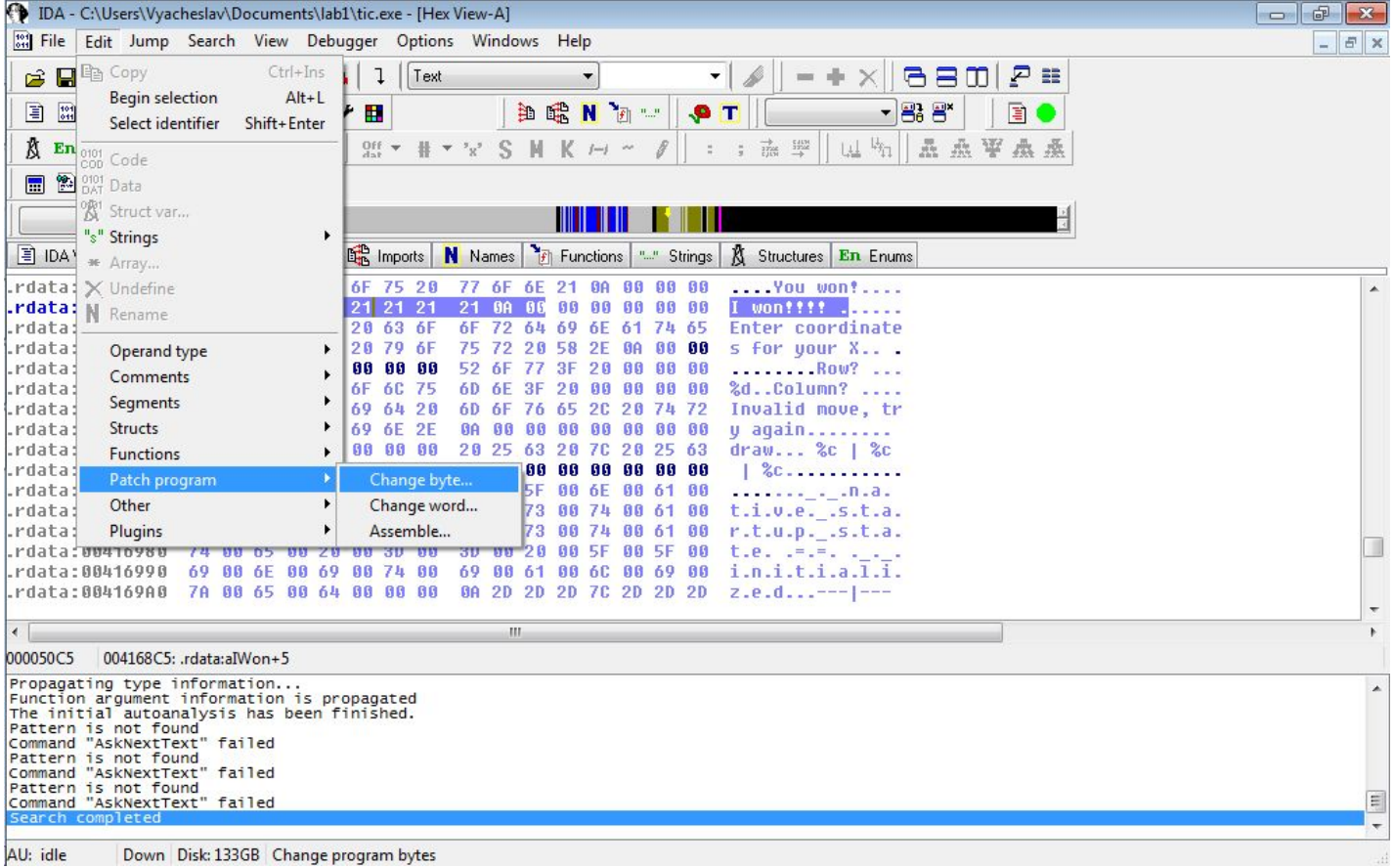
Вкладка Strings



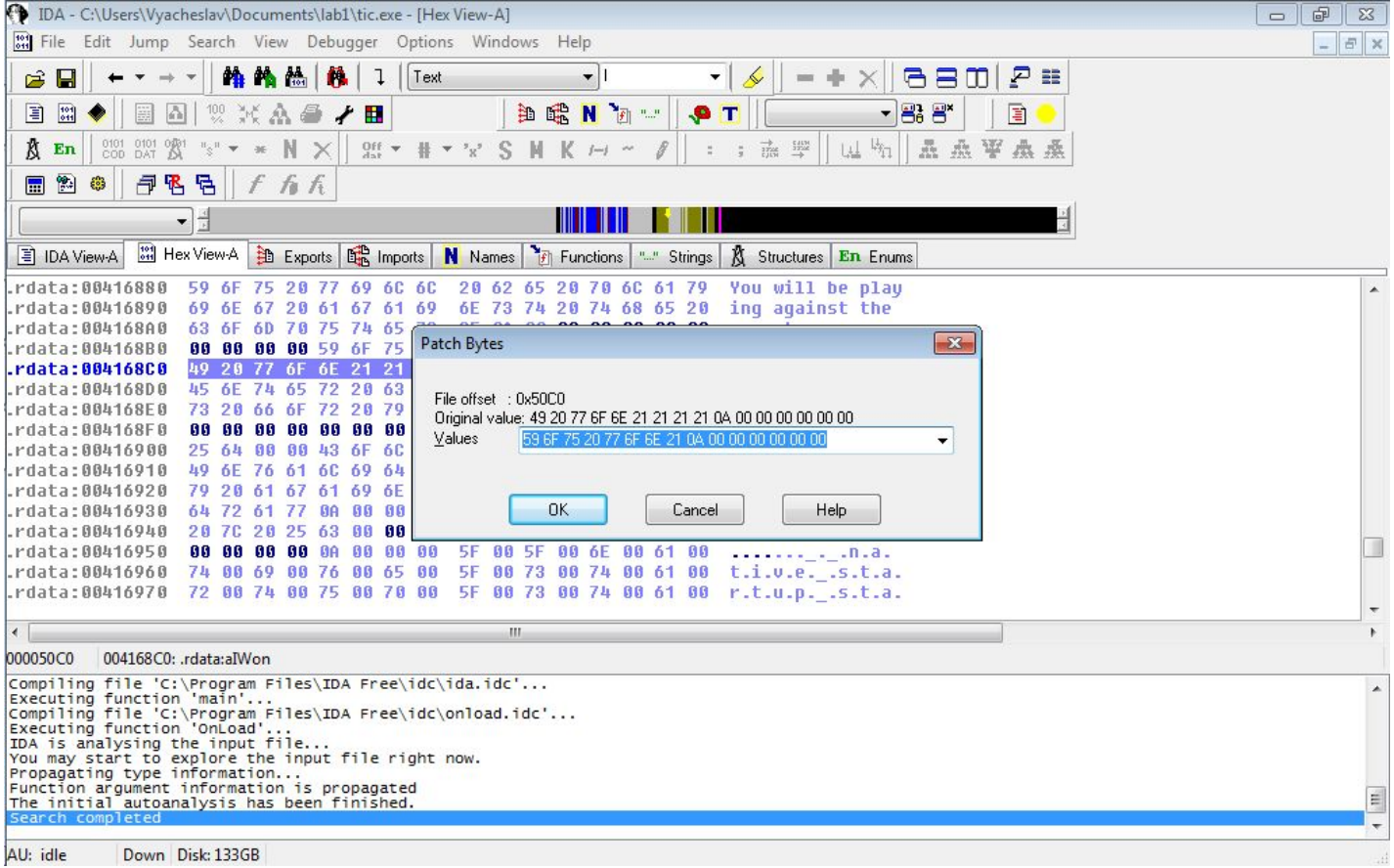
Получим в Python 16-ричный вид



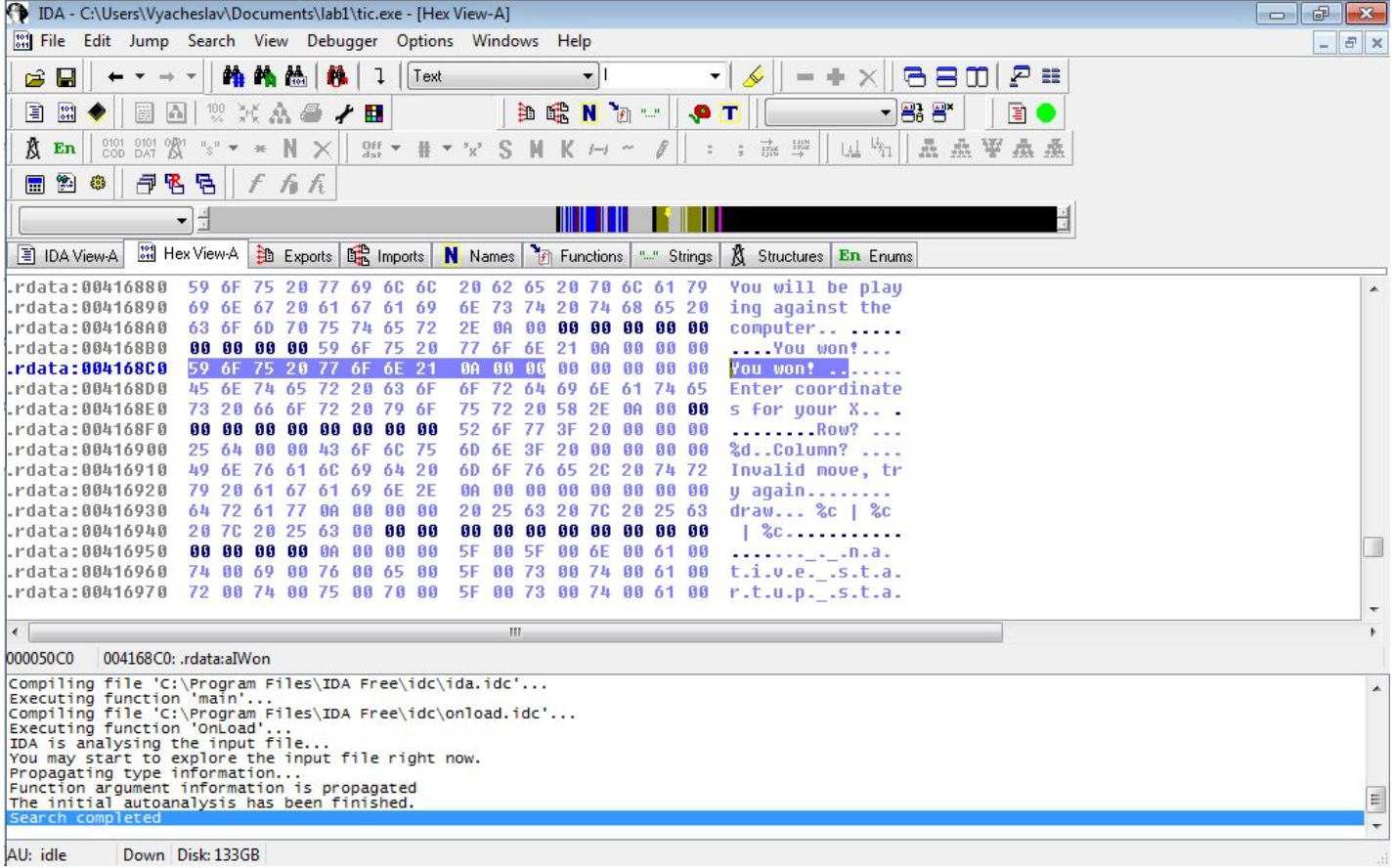
Либо скопируем из ресурсов



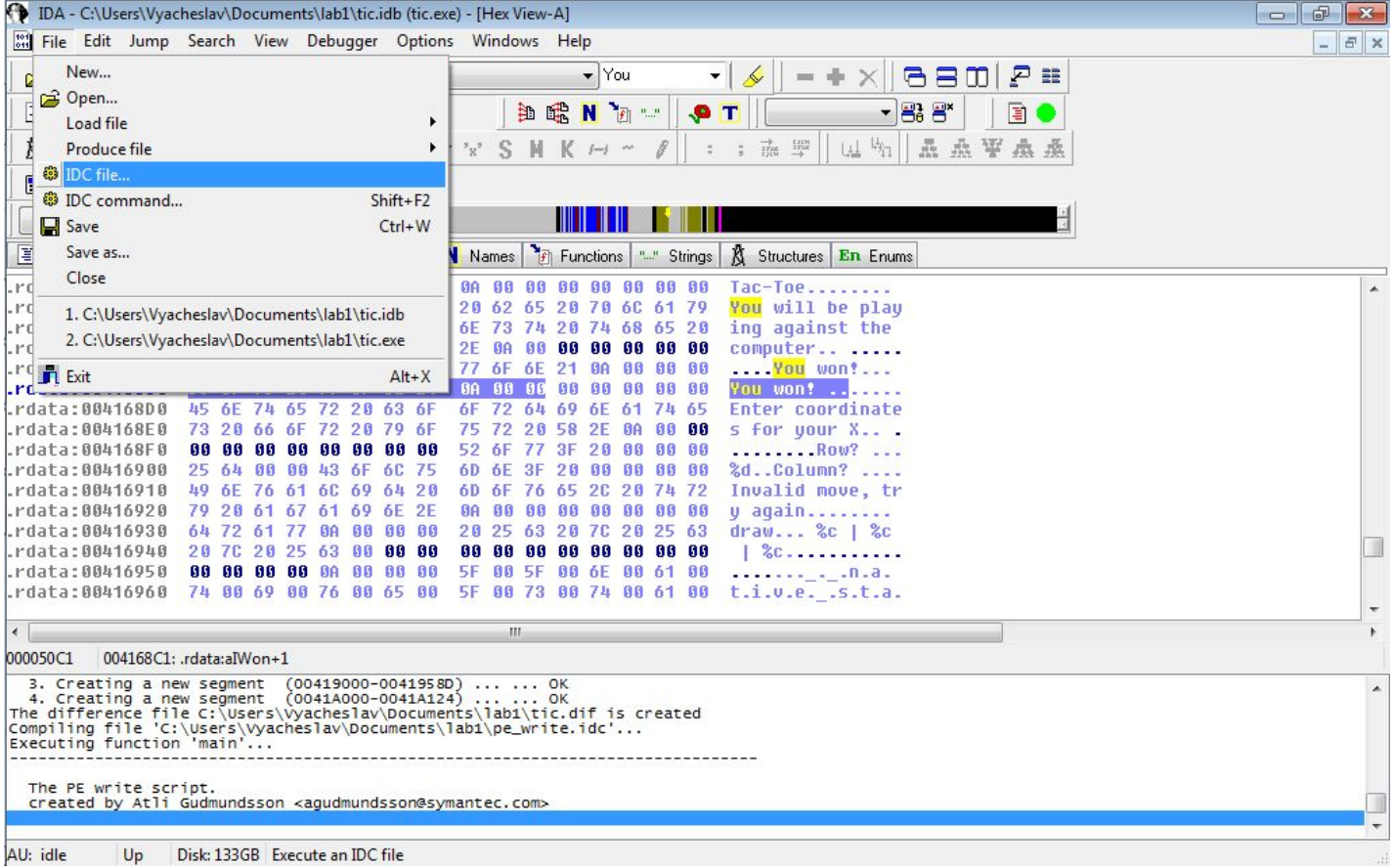
Изменим строку



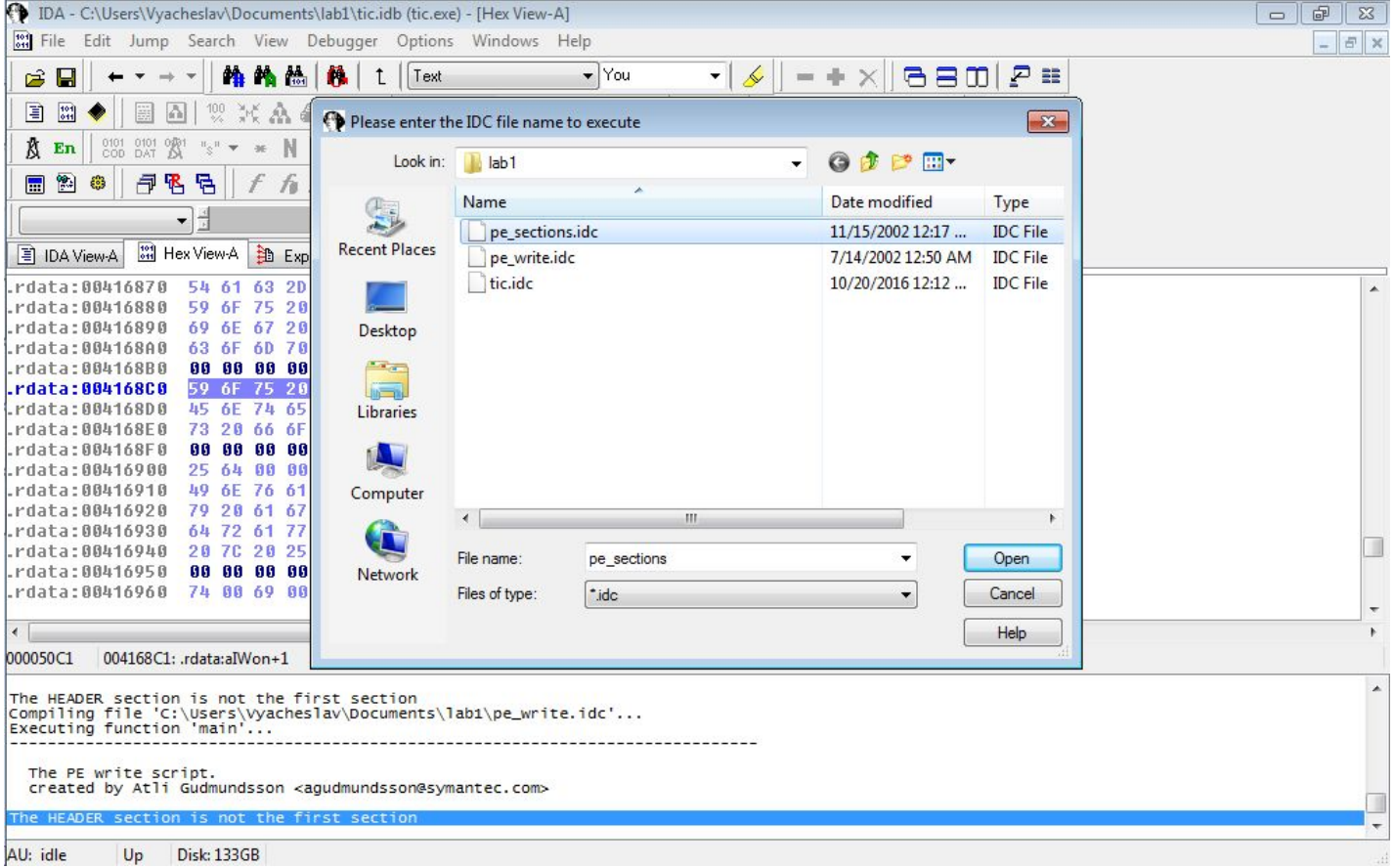
Подставим полученное значение



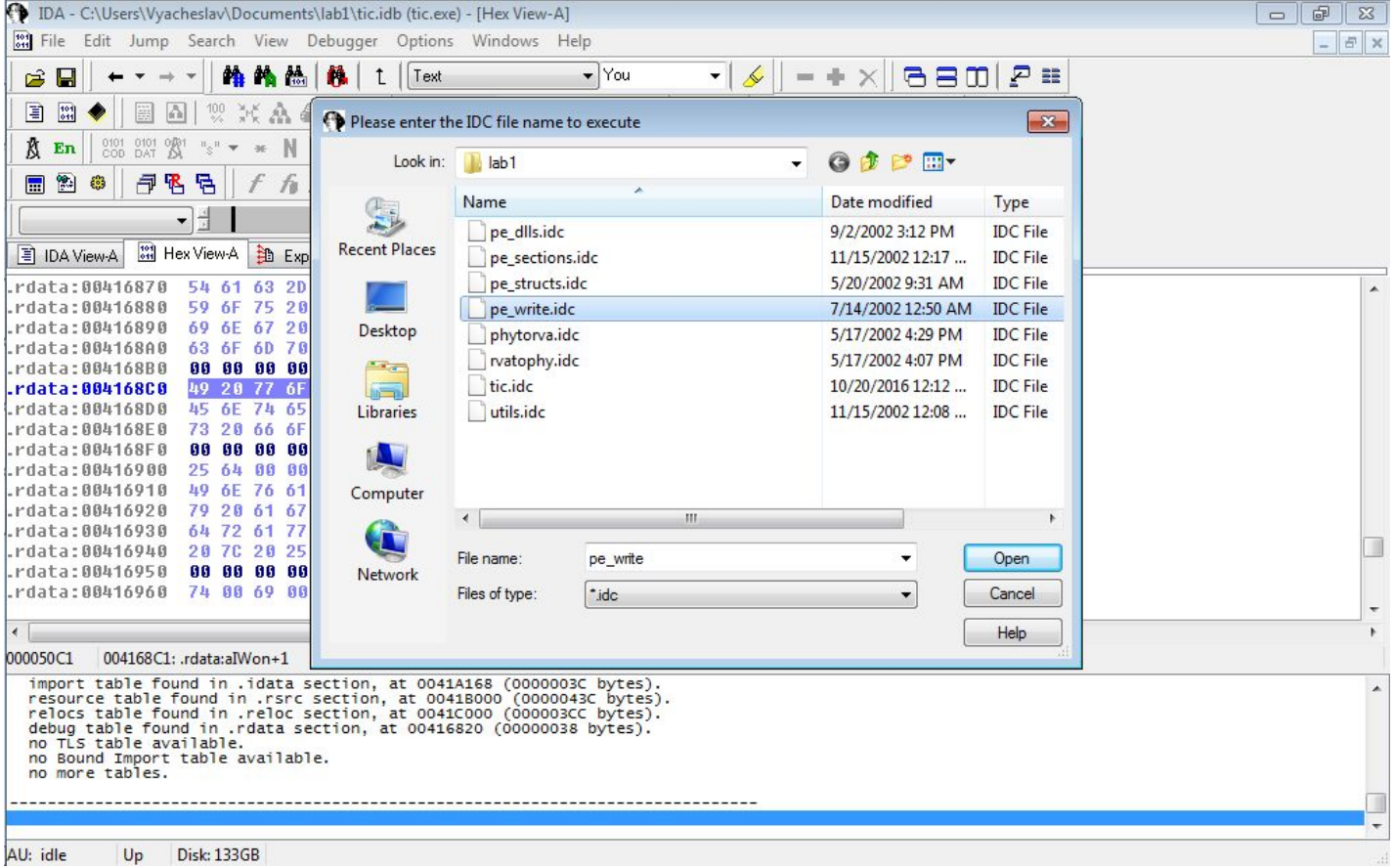
Значение строки изменилось



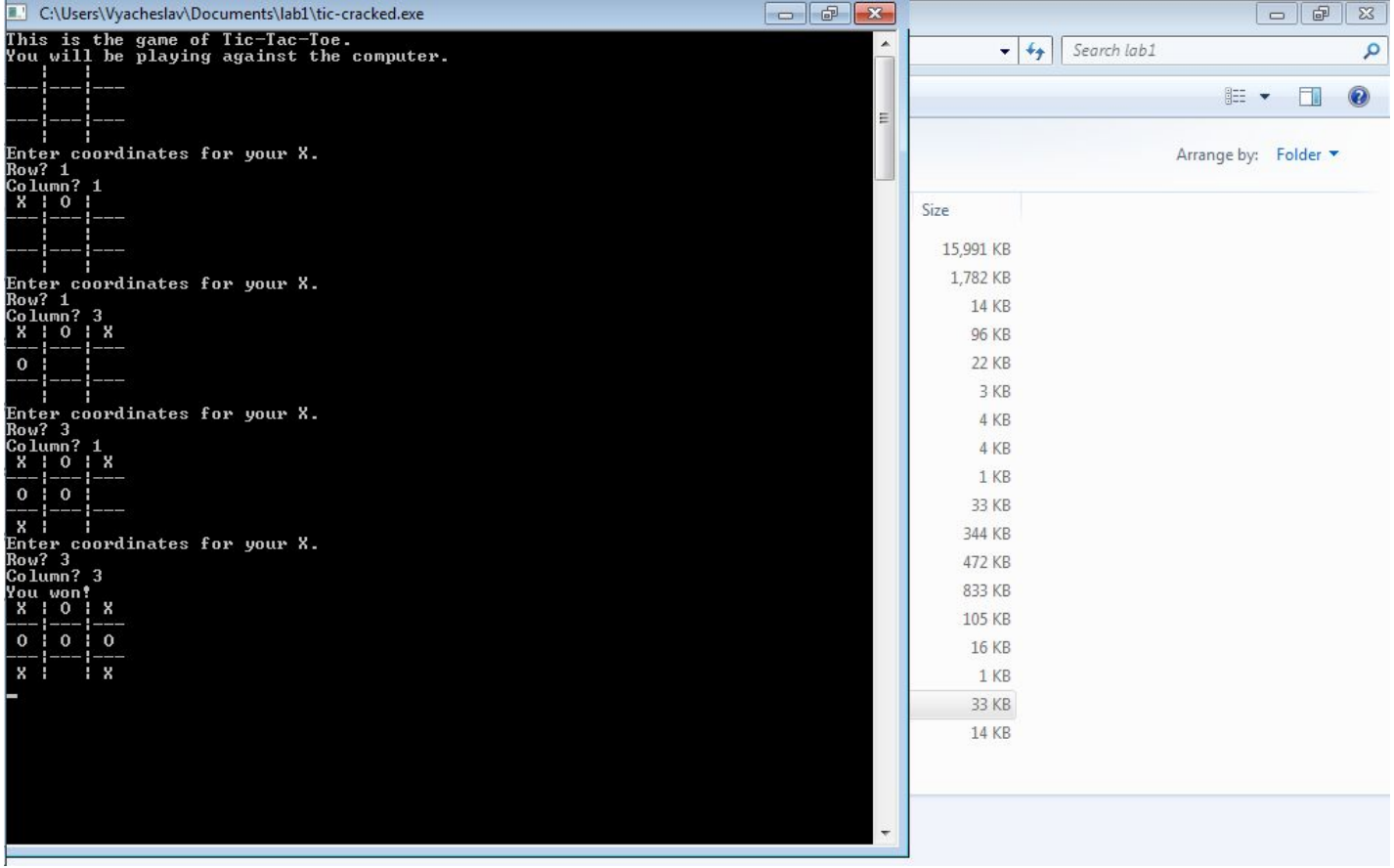
Сохраним изменения



Сохраним секции



Сохраним исполняемый файл



Программа взломана

Спасибо за внимание

mailto: vyacheslav.bezborodov@gmail.com