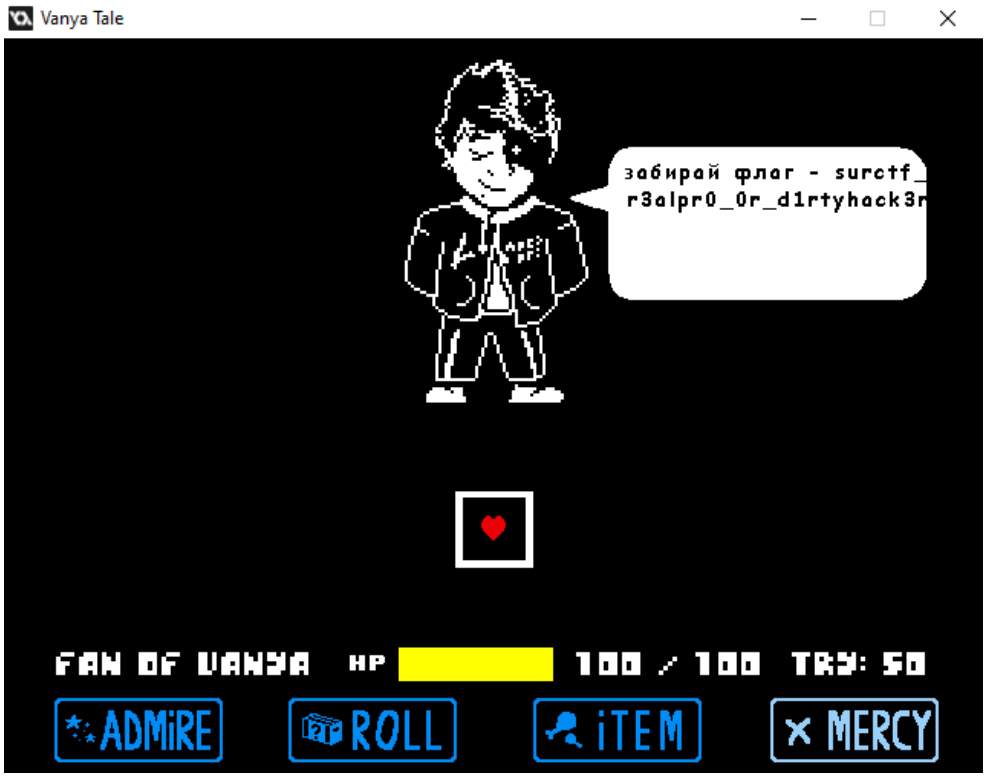
1. Vanyatale

Для получения флага нужно пройти игру до конца (довести «хп» Вани до минимума).

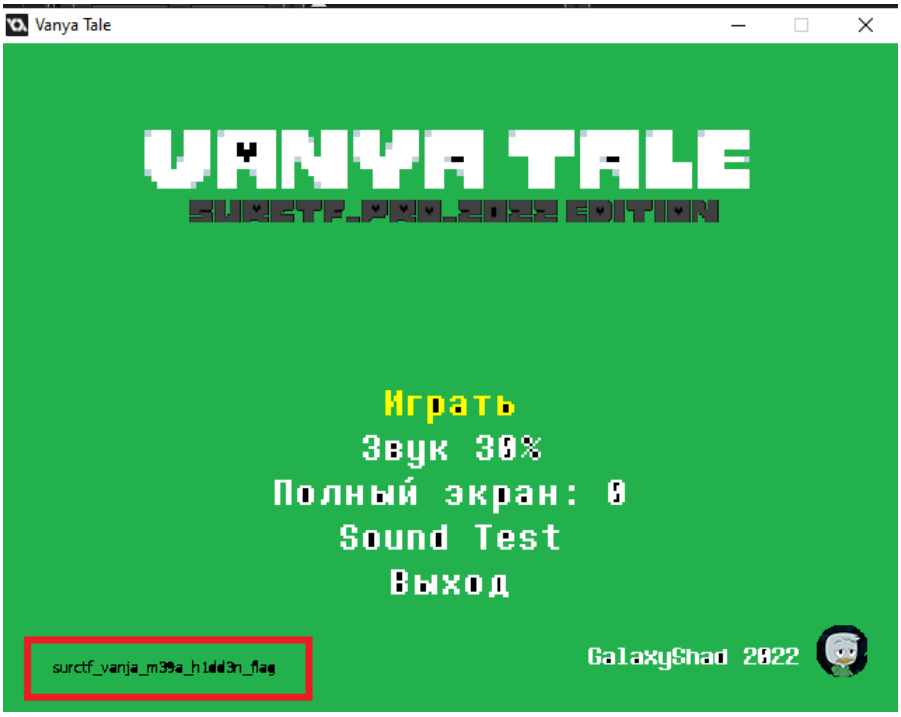
Круто, если сделать все это на скиле, но никто и не запрещал накрутить себе, к примеру, ХП через тот же Cheat Engine или уменьшить ХП босса.

В конечном диалоги Ваня сообщит флаг.



2. Vanyatale_y3t_dark3r

Флаг находится в главном меню. Для того, чтобы его увидеть, необходимо осветлить изображение. Ну или просто тыкнуть пипеткой в Paint по черному фону :D.



3. Vanyatale_hidden_snd

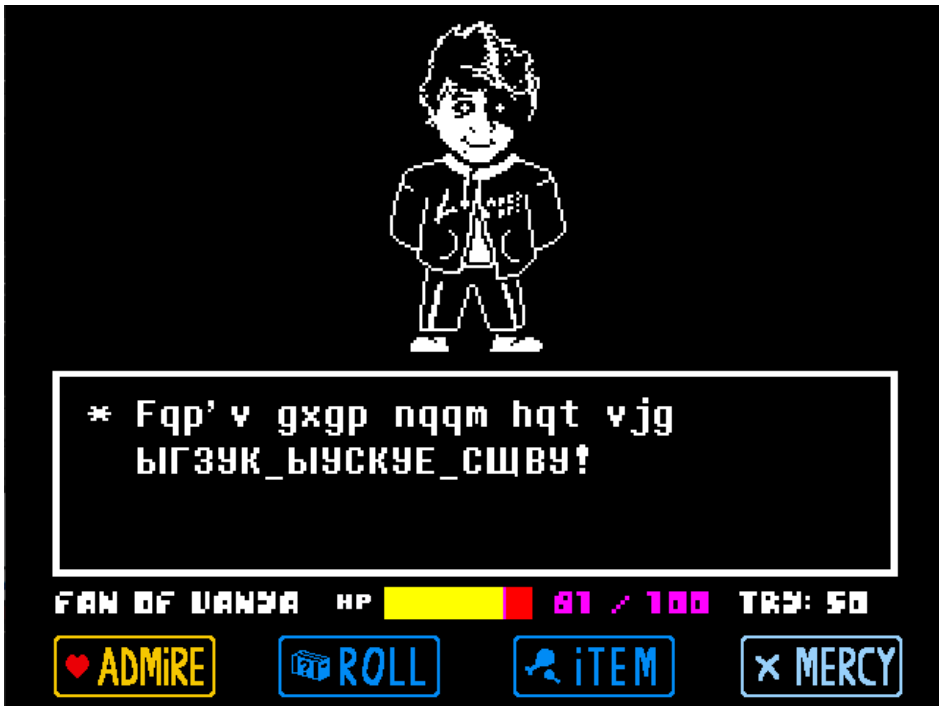
Заходим в SoundTest, листаем до 13 записи «T3L3PH0N3_CA77», содержащую DTMF запись - звуки клавиш кнопочных телефонов, где каждая клавиша имеет свое уникальное звучание.

Записываем это аудио любым способом и декодируем DTMF декодером. На месте пауз между звуками расставляем _, а также не забываем дописать перед полученной последовательностью цифр surctf_.

surctf_777_169_609_01_111

4. Vanyatale_cursed_image

Играя в игру, можно встретить следующее сообщение:



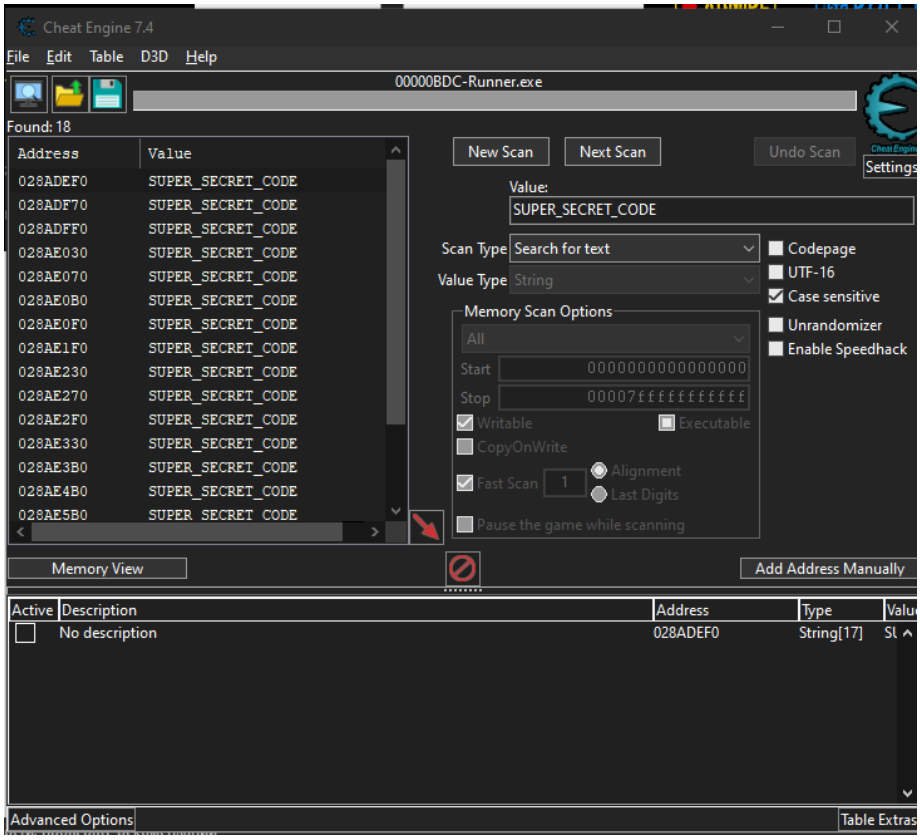
Первая его часть зашифрована шифром Цезаря (ROT24), расшифровав получим:

Don't even look for the ЫГЗУК_ЫУСКУЕ_СЩВУ!

Последние 3 слова написаны русской раскладкой, нужно восстановить английские буквы, в итоге получится:

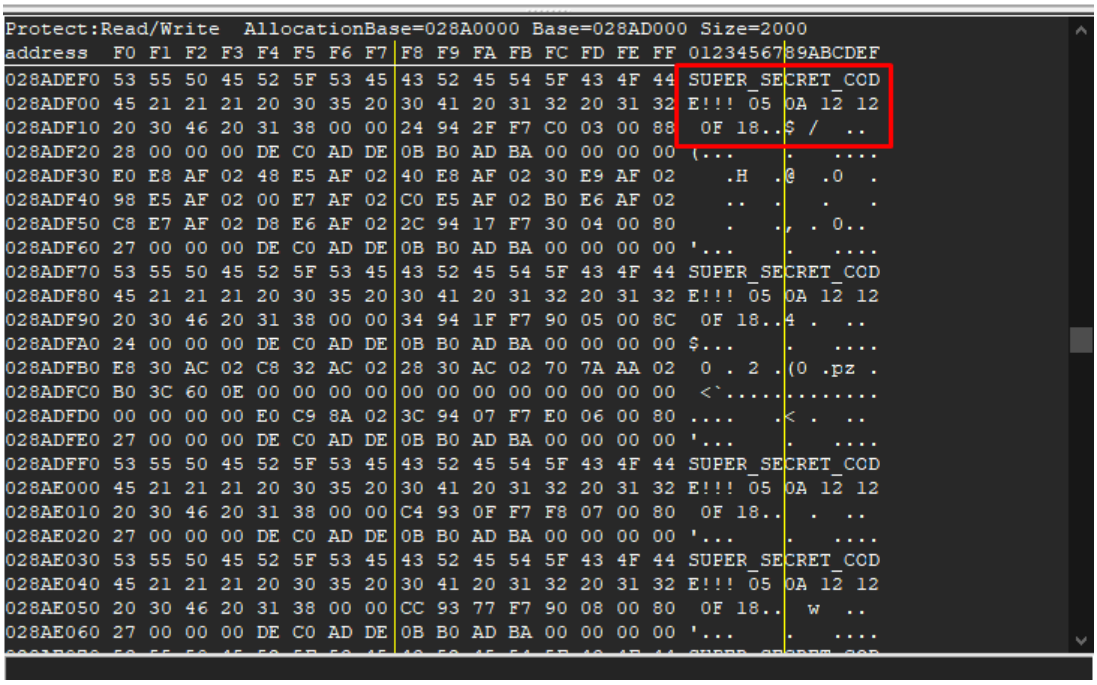
Don't even look for the SUPER_SECRET_CODE!

Открываем **CheatEngine**, ставим режим поиска String и вставляем в поле наше полученное значение.

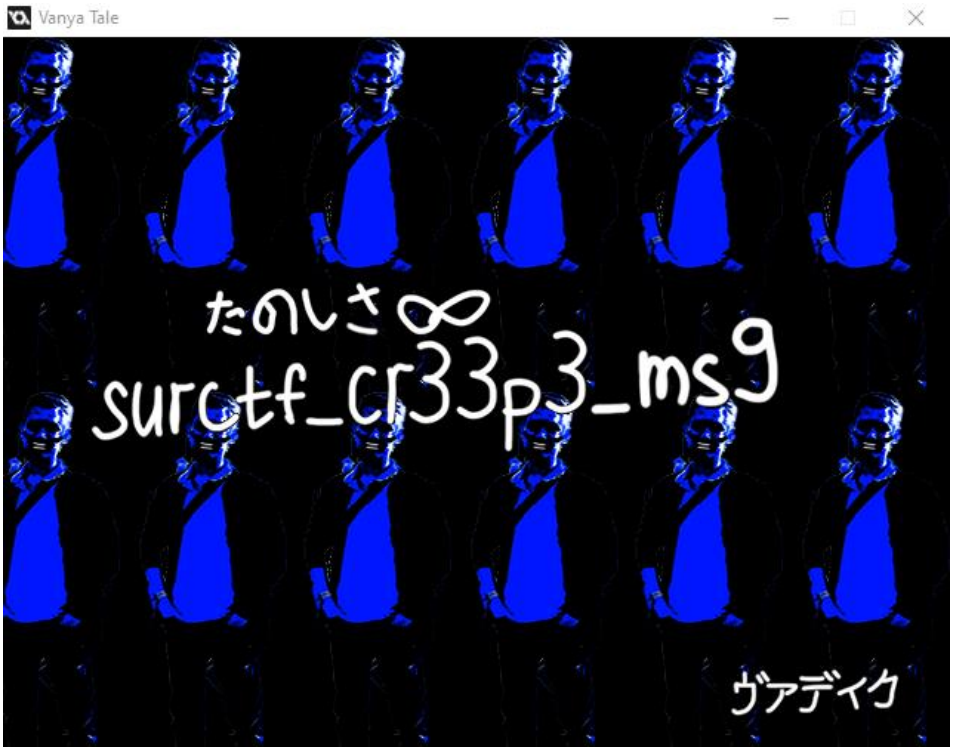


Выбираем любой из найденных адресов и жмем *Browse This Memory Region.* Видим последовательность значений в шестнадцатеричном формате.

05 0A 12 12 0F 18



Для получения изображения с флагом нужно по порядку проиграть песни в SoundTeste с кодами из полученной последовательности.

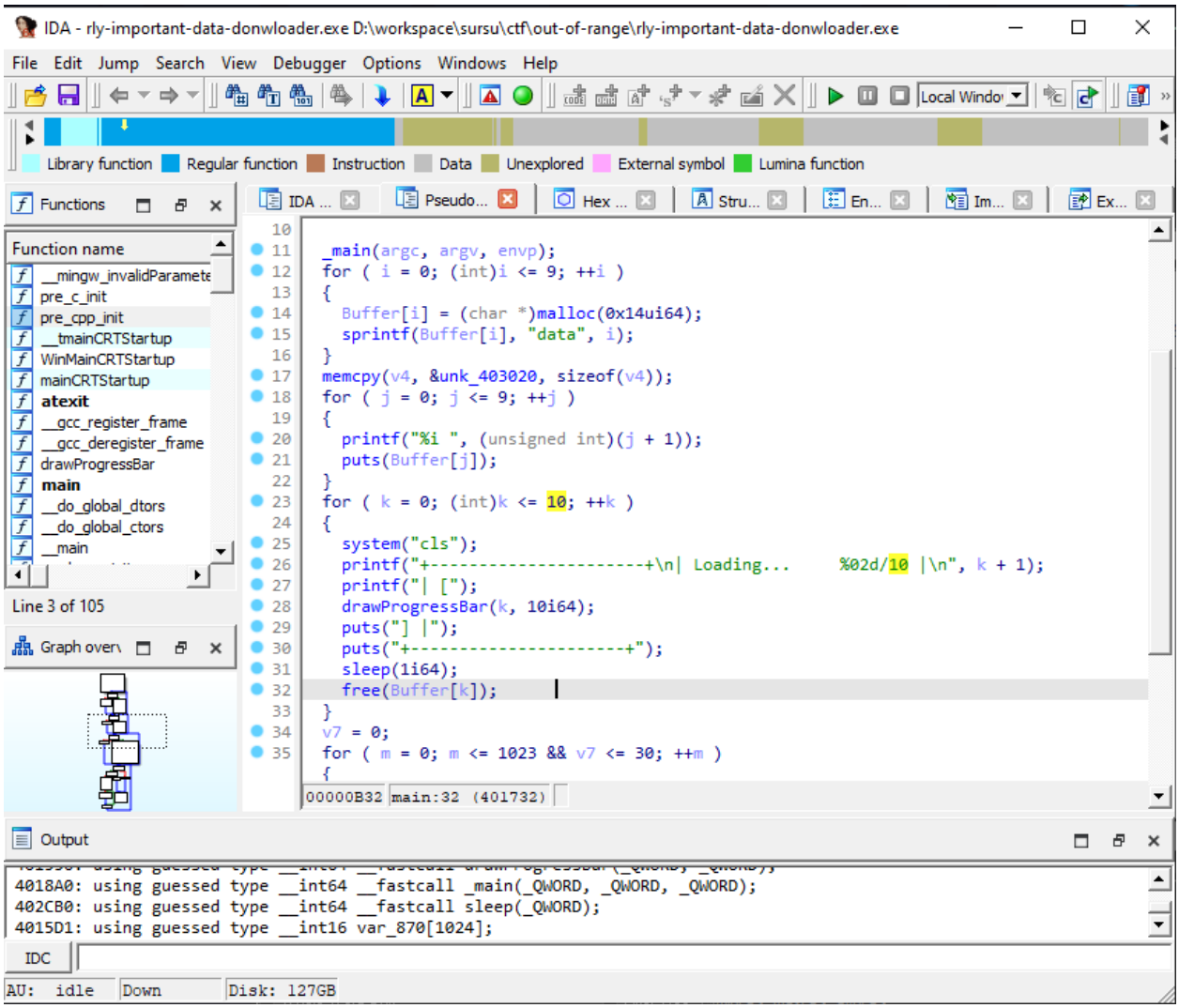


(Отсылка на https://youtu.be/idheGtky7os)

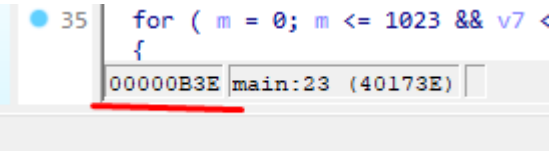
5. loading

Как можно догадаться, программа падает из-за выхода за пределы массива. Если это не очевидно, подсказка есть в одном из диалогов Vanyatale))

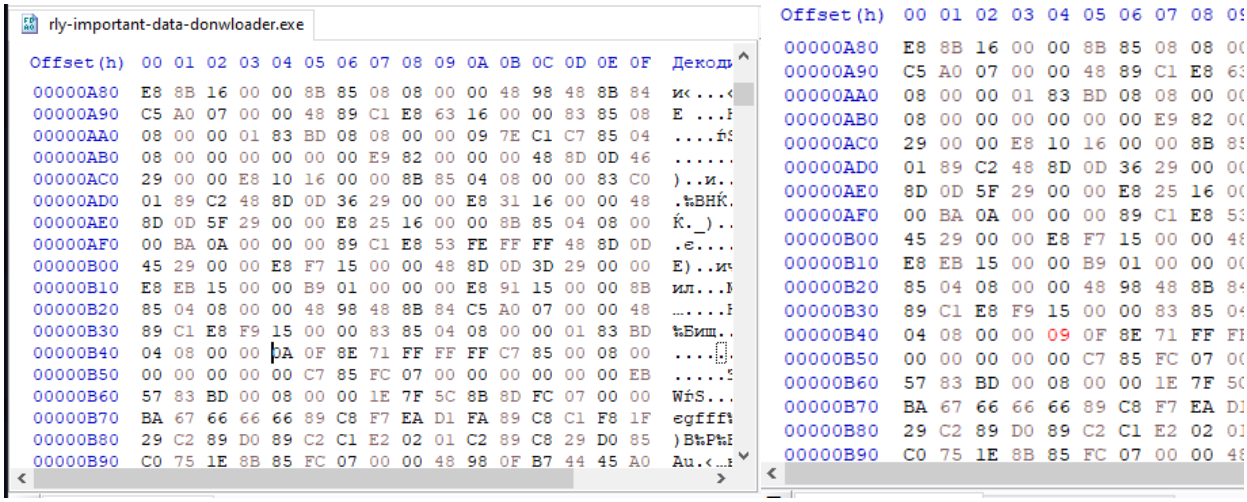
Открываем любую тулзу по декомпиляции. К примеру IDA. Находим там косячный цикл:



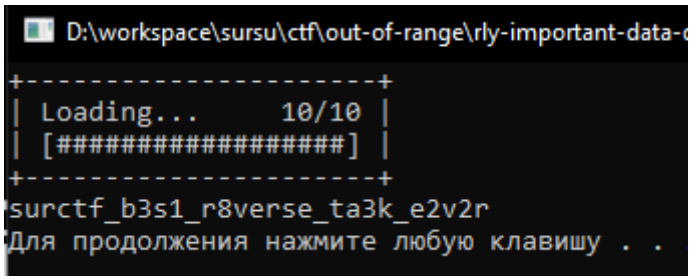
Узнаем примерный адрес неправильного значения в экзешнике – 0xB3E:



Идем в любой удобный редактор, к примеру HxD, находим там требуемое значение и меняем его с 0x0A (10) на 0x09 (9):



Сохраняем, запускаем программу и получаем флаг:



by GalaxyShad 2022

telegram: @galaxyshad
github: https://github.com/GalaxyShad
vk: https://vk.com/galaxyshad
youtube: https://www.youtube.com/@GalaxyShad102