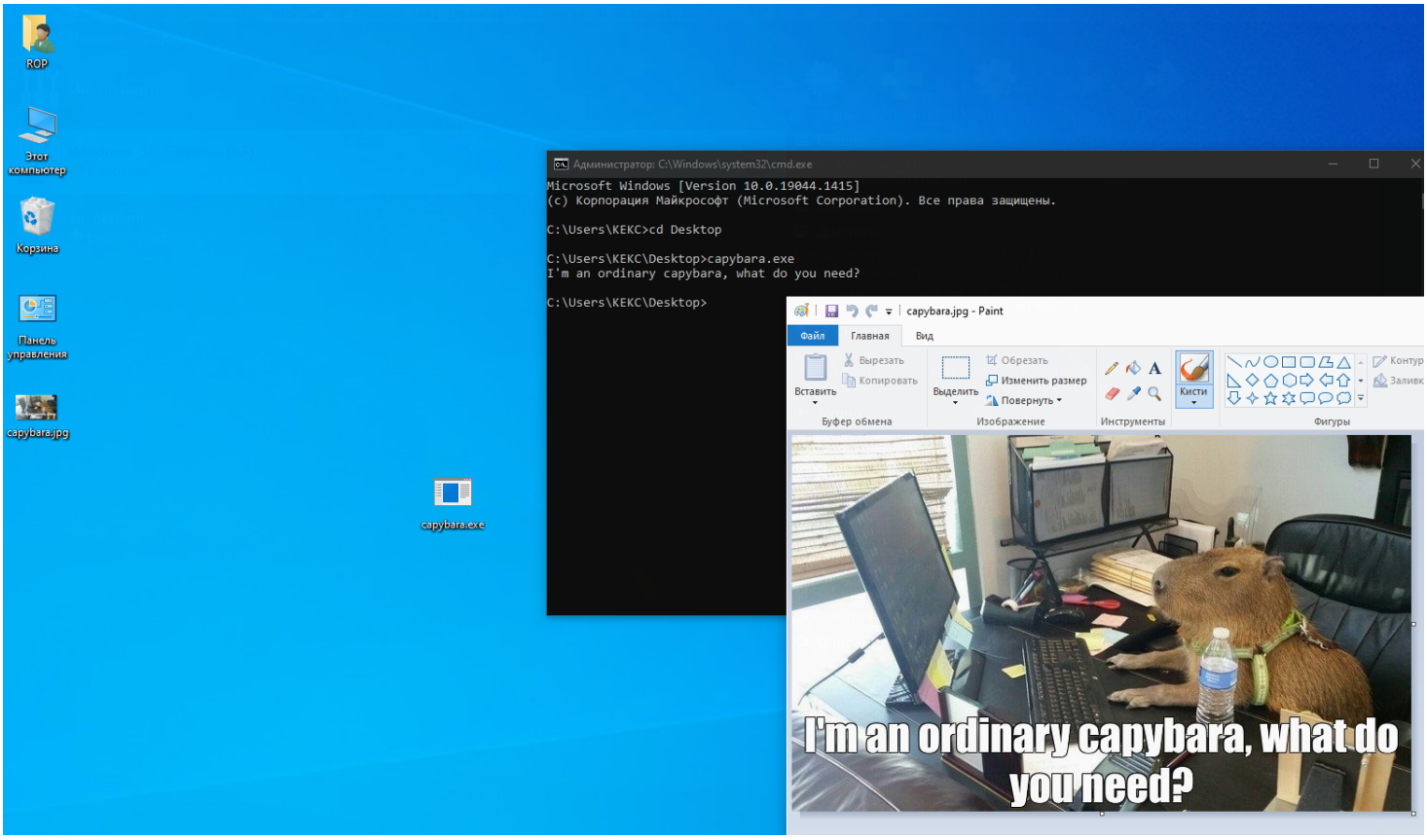
Обычная капибара

ⓘ Краткая информация

Название: Обычная капибара
Описание: Что такое, это обычная капибара.
Категория: Реверс-инжиниринг
Сложность: Средняя
Очки: 450
Мероприятие/ивент: Киберколизей
Флаг: `CODEBY{qqq_wE_l2ve_C@pYbaRa_1n_EXE}`

Райтап

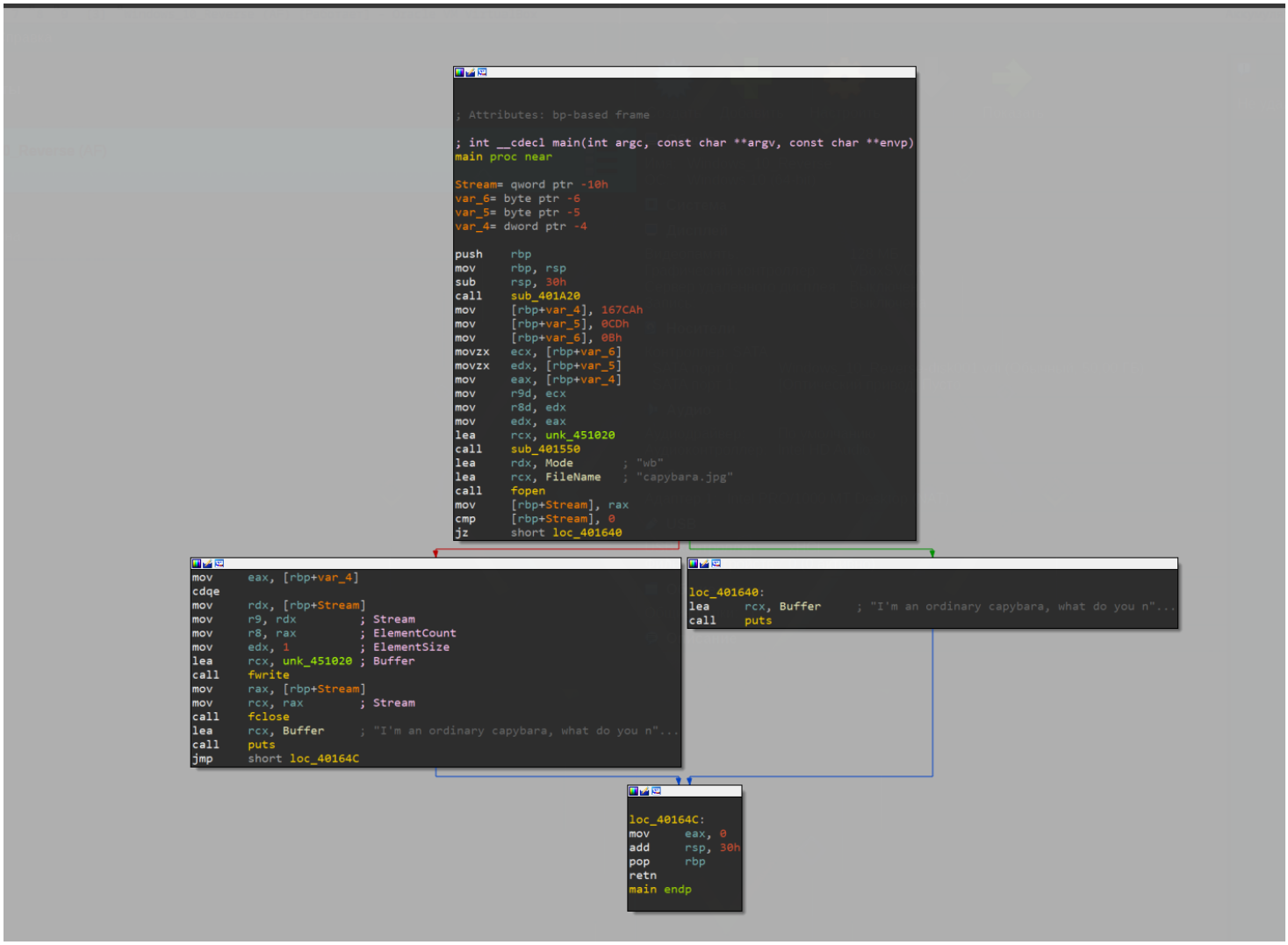
Распакуем архив и попробуем запустить EXE.



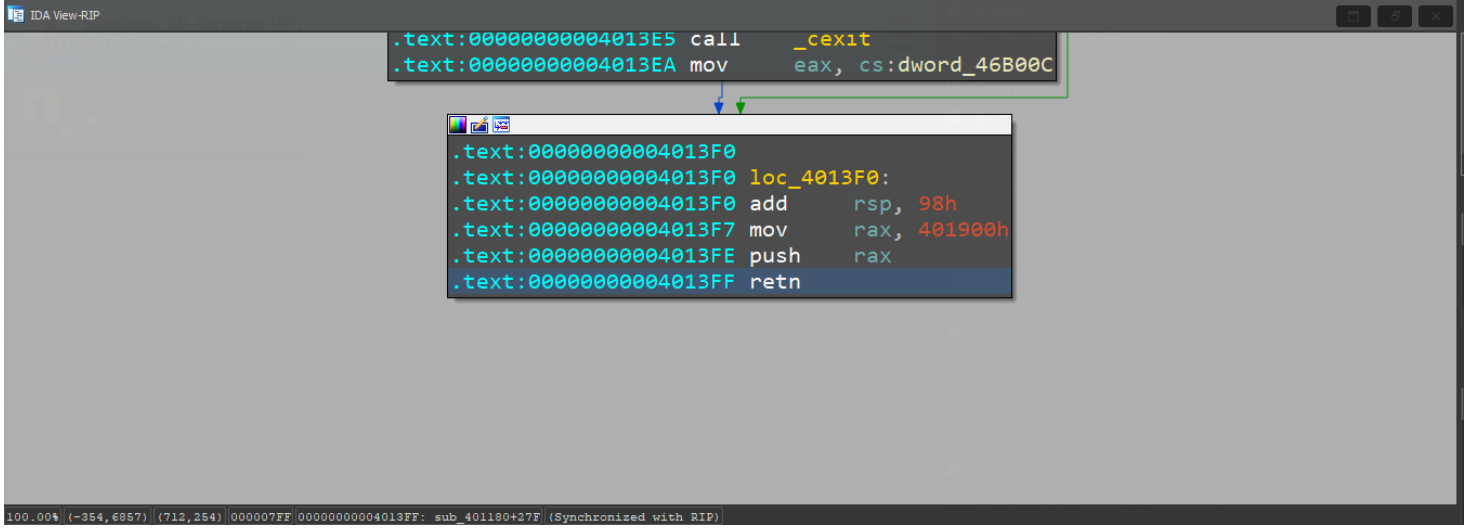
Создаётся картинка на рабочем столе.

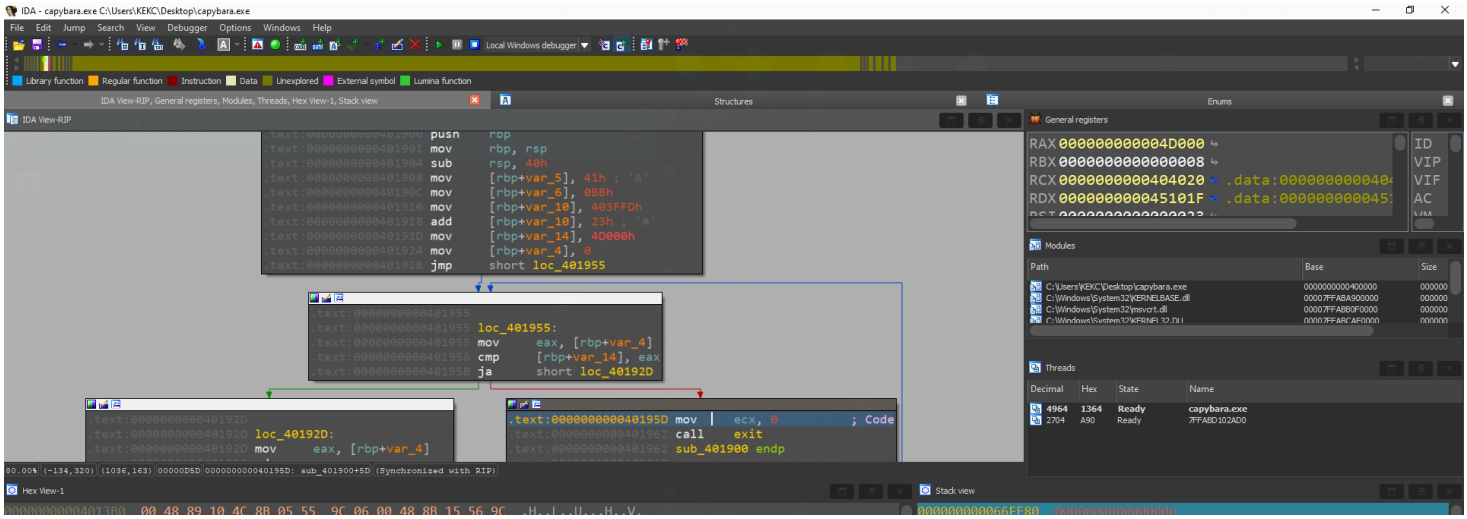
Через UPX распакуем файл.

```
Администратор: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19044.1415]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\KEKC\Desktop\upx-4.0.2-win64>upx.exe -d capybara.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2023
UPX 4.0.2       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 30th 2023

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    424448 <-    307712   72.50%    win64/pe     capybara.exe

Unpacked 1 file.

C:\Users\KEKC\Desktop\upx-4.0.2-win64>
```



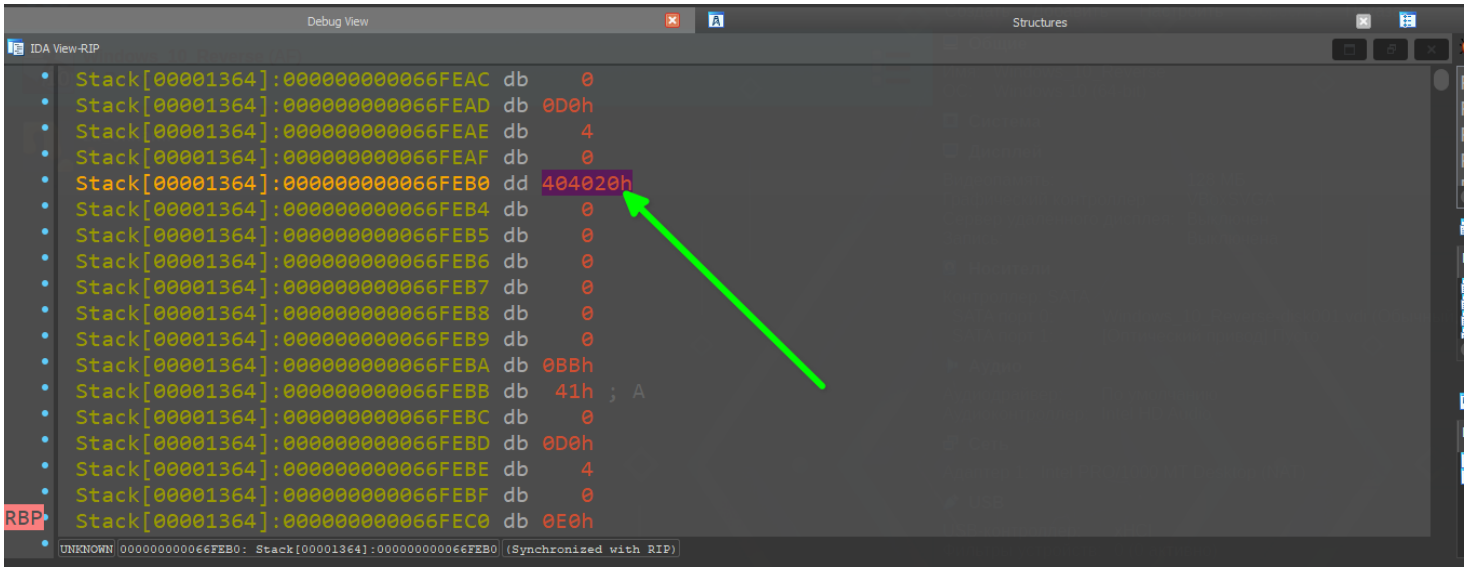
Это всё ложный вектор. Во время отладки доходим до сюда.

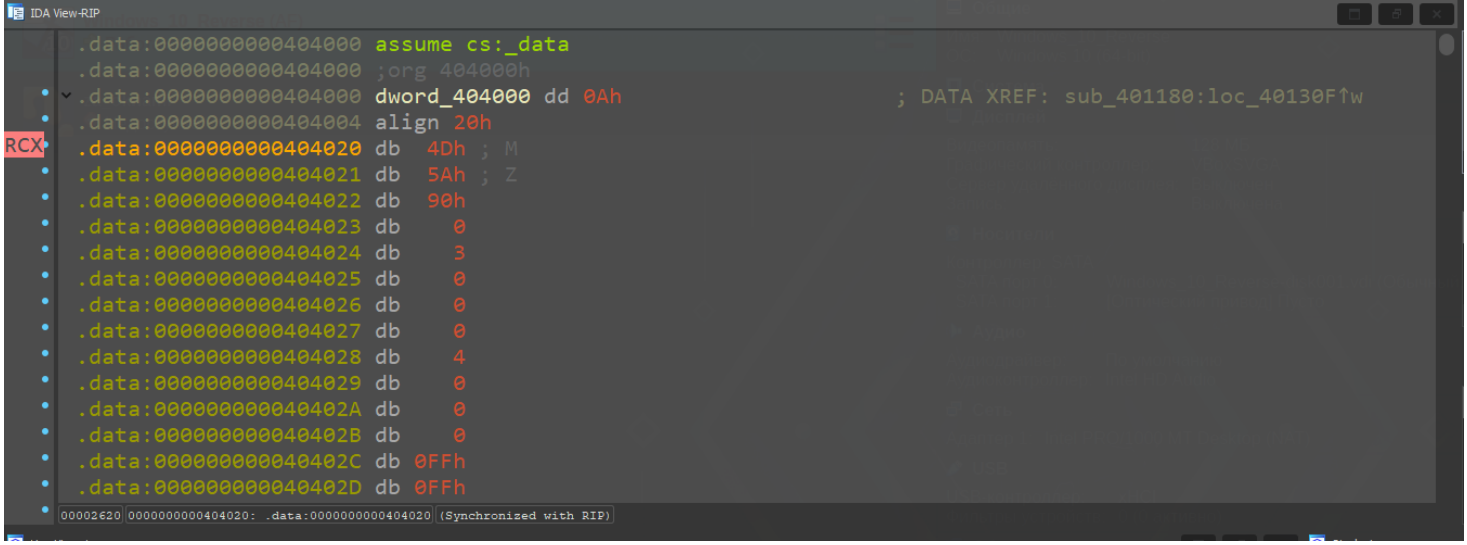




Далее выполняем код до сюда.

Переходим в `var_10`, затем по адресу из него.

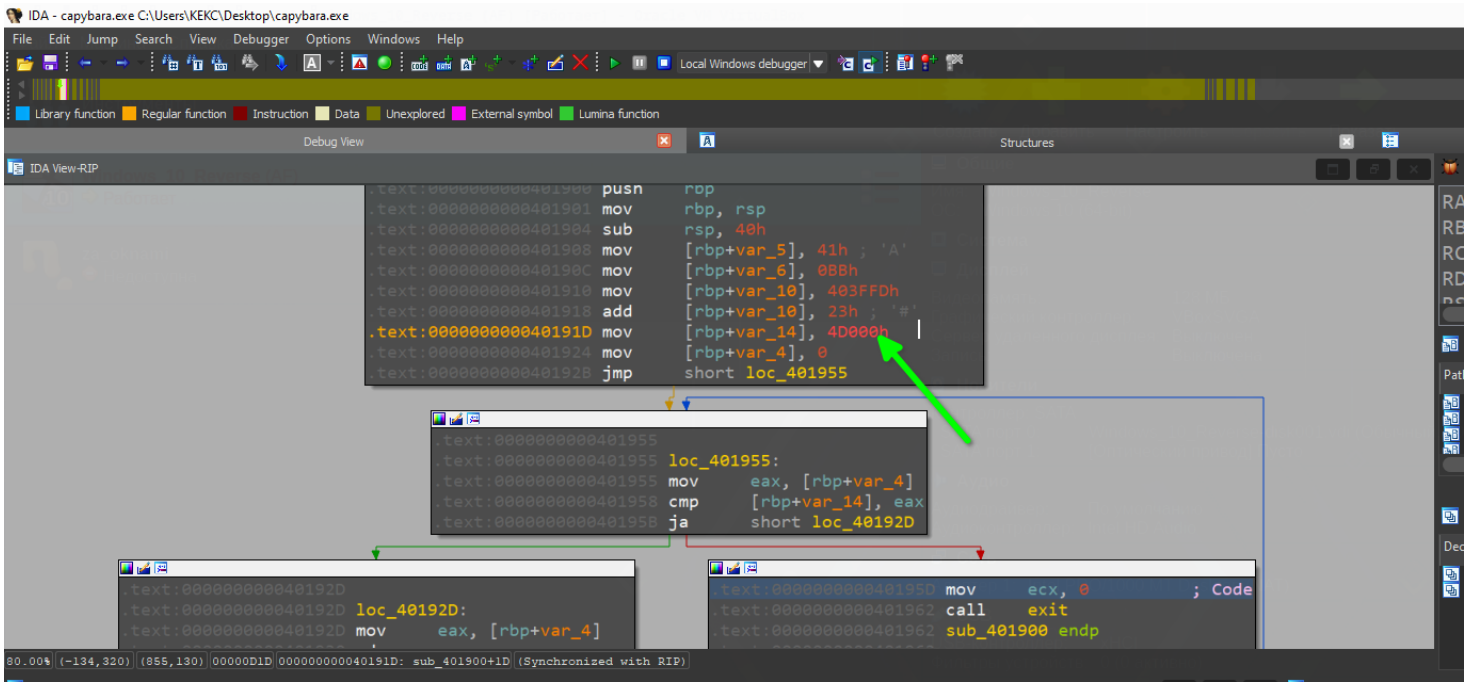




Ставим курсор на 0x402020 и нажимаем Shift+F2. Используем этот скрипт, чтобы сдампить программу из памяти.

```
auto fname = "C:\\dump.exe";
auto address = 0x404020;
auto size = 0x4D000;
auto file= fopen(fname, "wb");

savefile(file, 0, address, size);
fclose(file);
```

Размер узнали тут.



У нас будет файл `dump.exe` в диске C. Запустим его и получим новую картинку.

Флаг: `CODEBY{qqq_wE_l2ve_C@pYbaRa_1n_EXE}`