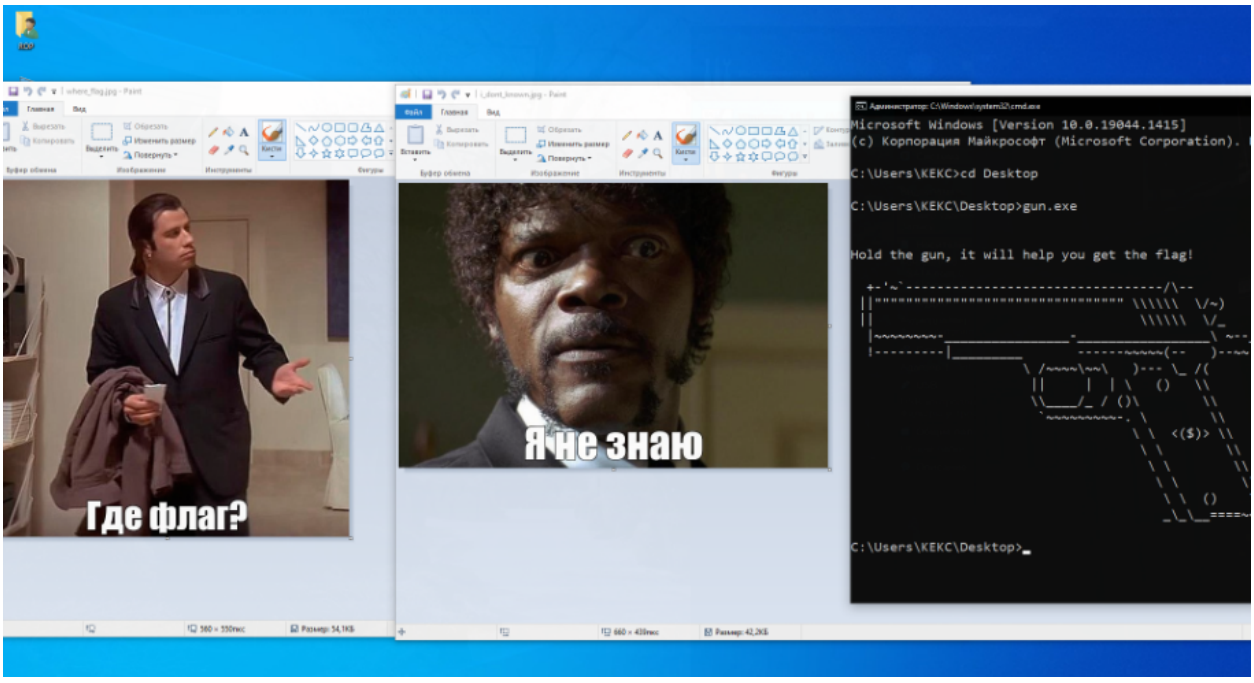
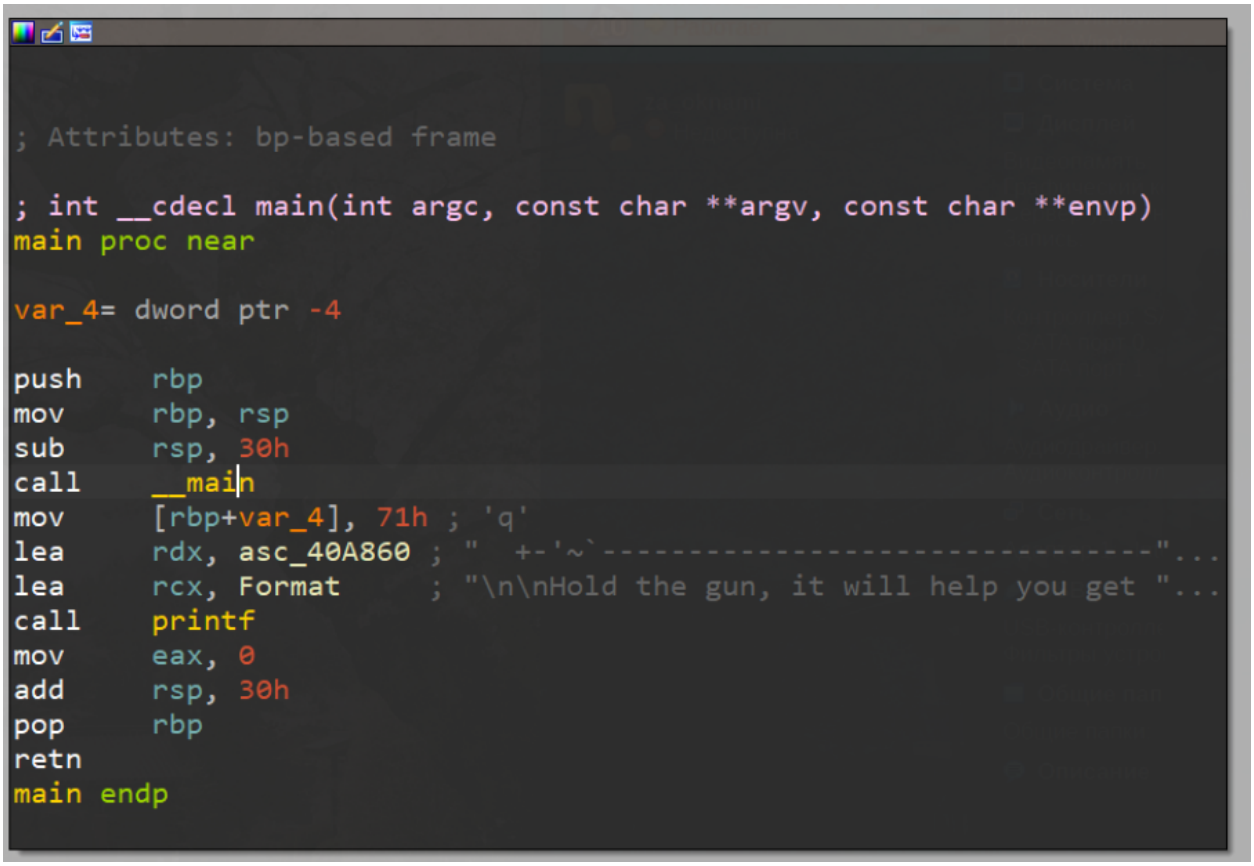
Название:	Где флаг?
Категория:	Реверс-инжиниринг
Уровень:	Средний
Очки:	400
Описание:	Я не знаю. Может быть ты сможешь найти его?
Теги:	C, патчинг
Автор:	ROP

Прохождение:

Распакуем архив, пробуем запустить.

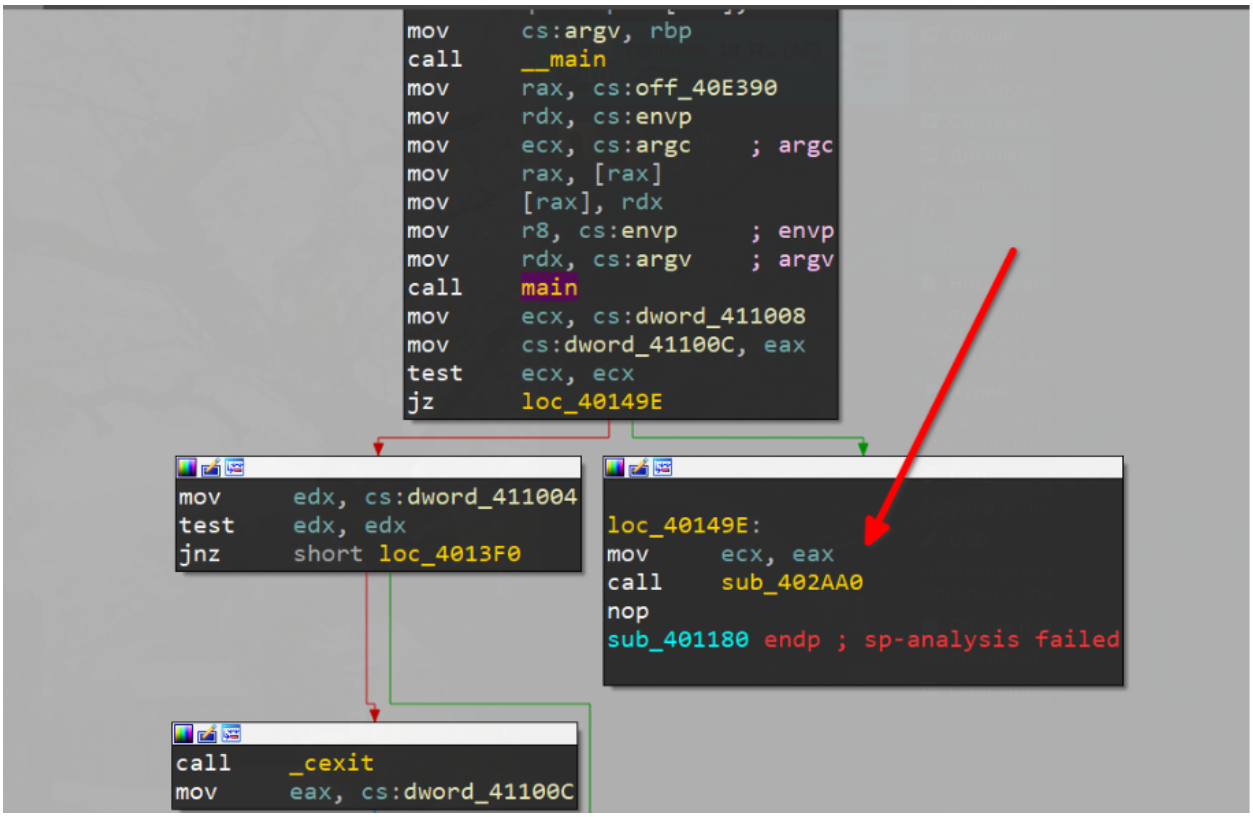


Ничего необычного. Изучим таск в IDA.

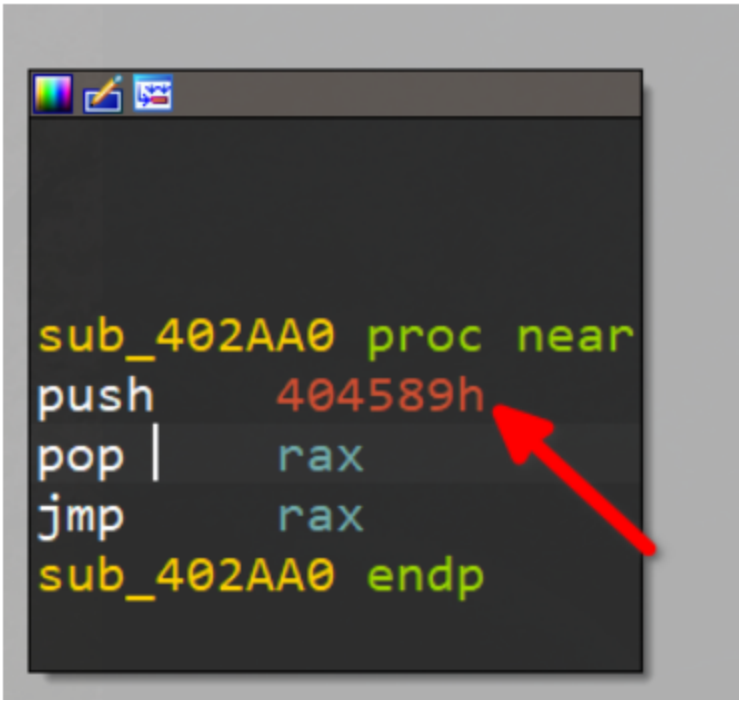


```
; Attributes: bp-based frame

; int __cdecl main(int argc, const char **argv, const char **envp)
main proc near

var_4= dword ptr -4

push    rbp
mov     rbp, rsp
sub     rsp, 30h
call    __main
mov     [rbp+var_4], 71h ; 'q'
lea     rdx, asc_40A860 ; "  +-'~`--------------------------------"...
lea     rcx, Format     ; "\n\nHold the gun, it will help you get "...
call    printf
mov     eax, 0
add     rsp, 30h
pop     rbp
retn
main endp
```

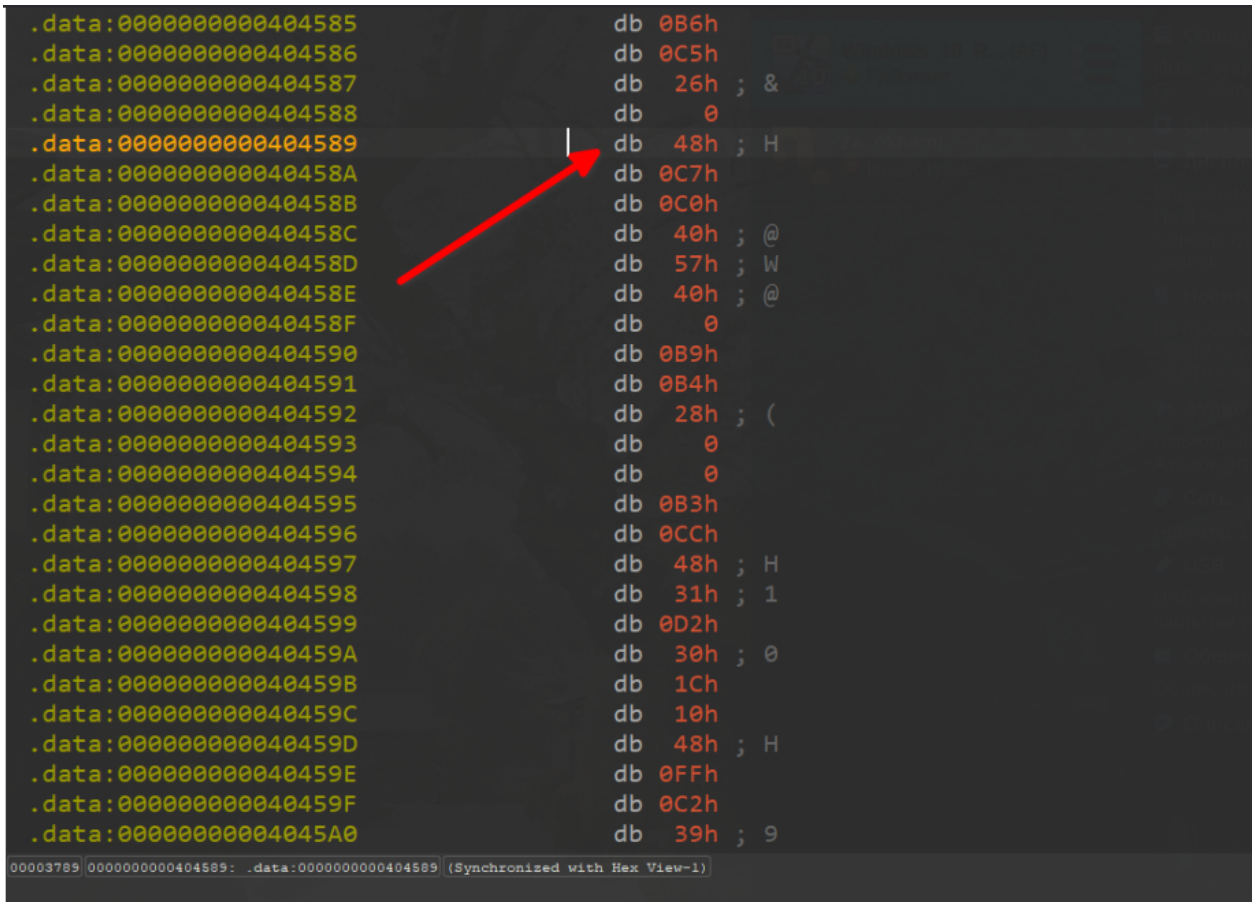
В `main` ничего необычного. Сам файл **не** статический, тоесть кода функций в нём нет. Проверим, что происходит после `main`.



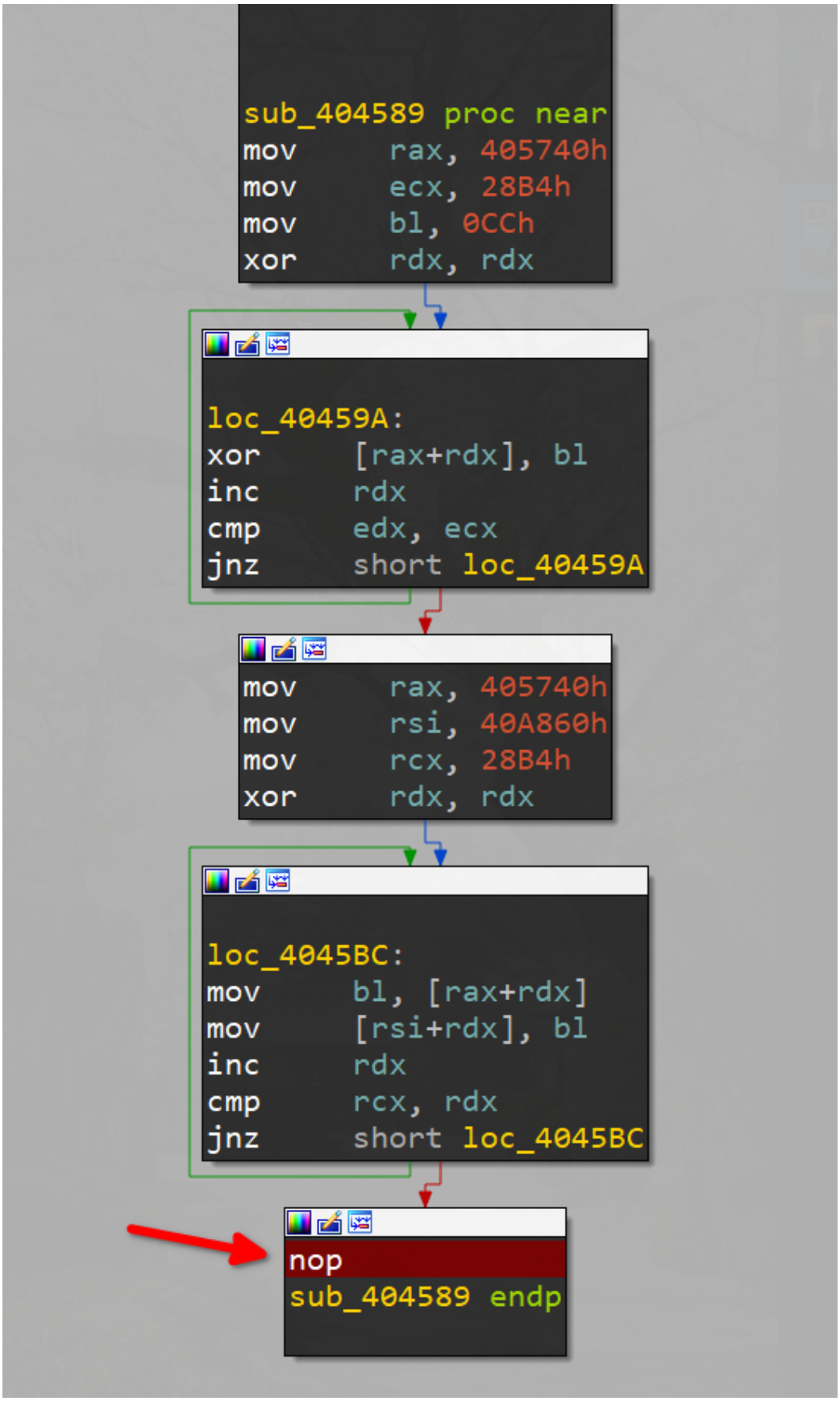
Тут должен быть `exit(0)`, но сейчас какая-то функция. Изучим её.



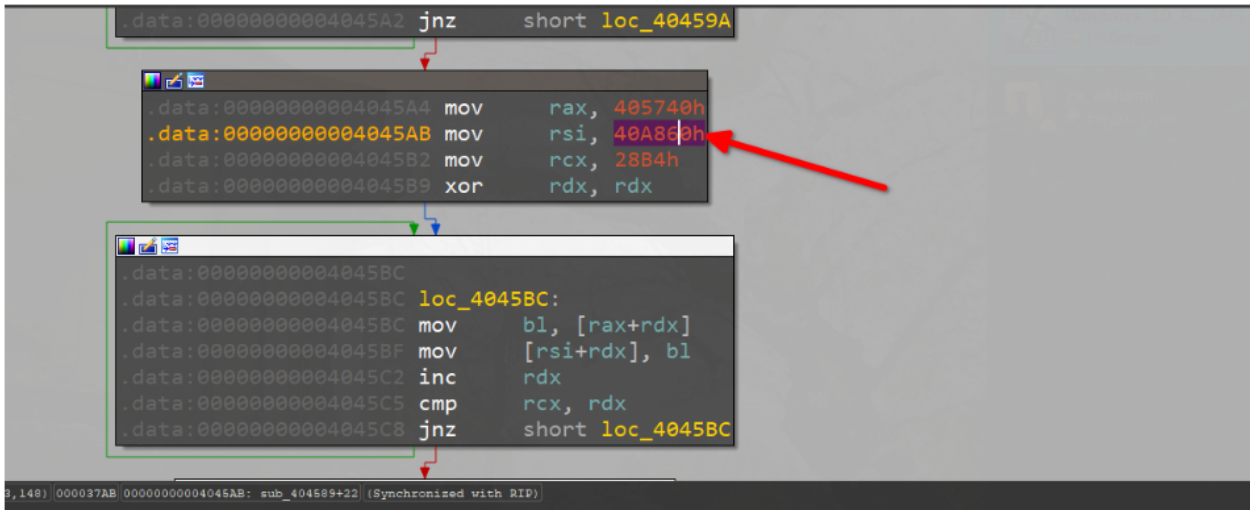
Переход по этому адресу через `jmp rax`. Смотрим, куда он ведёт.



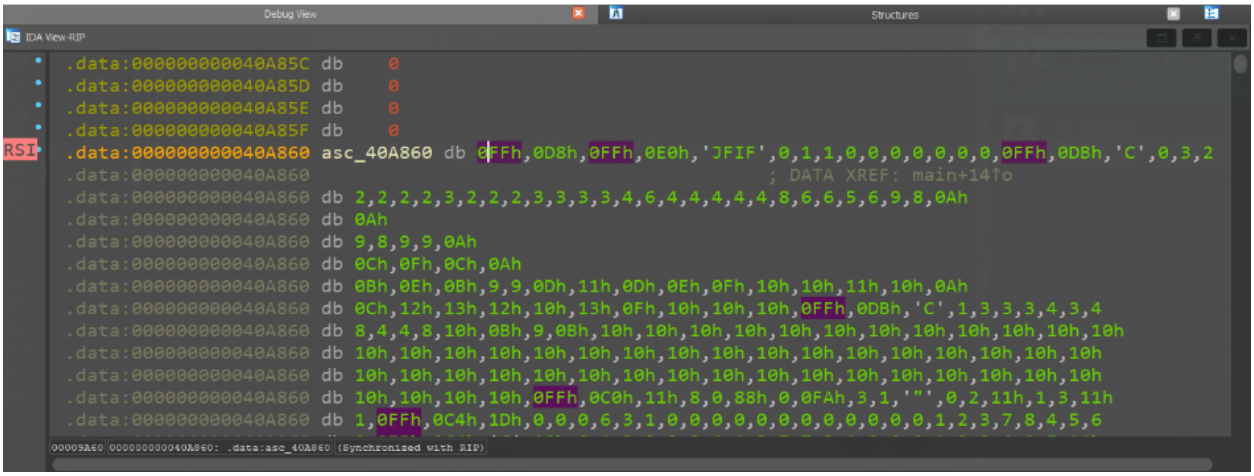
Поставим курсор сюда и нажмём C.


sub_404589 proc near
mov rax, 405740h
mov ecx, 28B4h
mov bl, 0CCh
xor rdx, rdx
loc_40459A:
xor [rax+rdx], bl
inc rdx
cmp edx, ecx
jnz short loc_40459A
mov rax, 405740h
mov rsi, 40A860h
mov rcx, 28B4h
xor rdx, rdx
loc_4045BC:
mov bl, [rax+rdx]
mov [rsi+rdx], bl
inc rdx
cmp rcx, rdx
jnz short loc_4045BC
nop
sub_404589 endp

Получили такой код. Он расшифровывает массив из секции `.data`. Поставим точку останова сюда и запустим отладчик.



Переходим по этому адресу - начало массива. В rcx будет его длина - 0x28B4.



Судя по тексту это файл формата JPEG. Сдампим его через Script Command (Shift+F2).

```
auto fname = "C:\\dump_mem.jpeg";
auto address = 0x40A860;  адрес начала
auto size = 0x28B4;  размер
auto file= fopen(fname, "wb");
savefile(file, 0, address, size);
fclose(file);
```

Открываем "C:\dump_mem.jpeg". Там флаг.