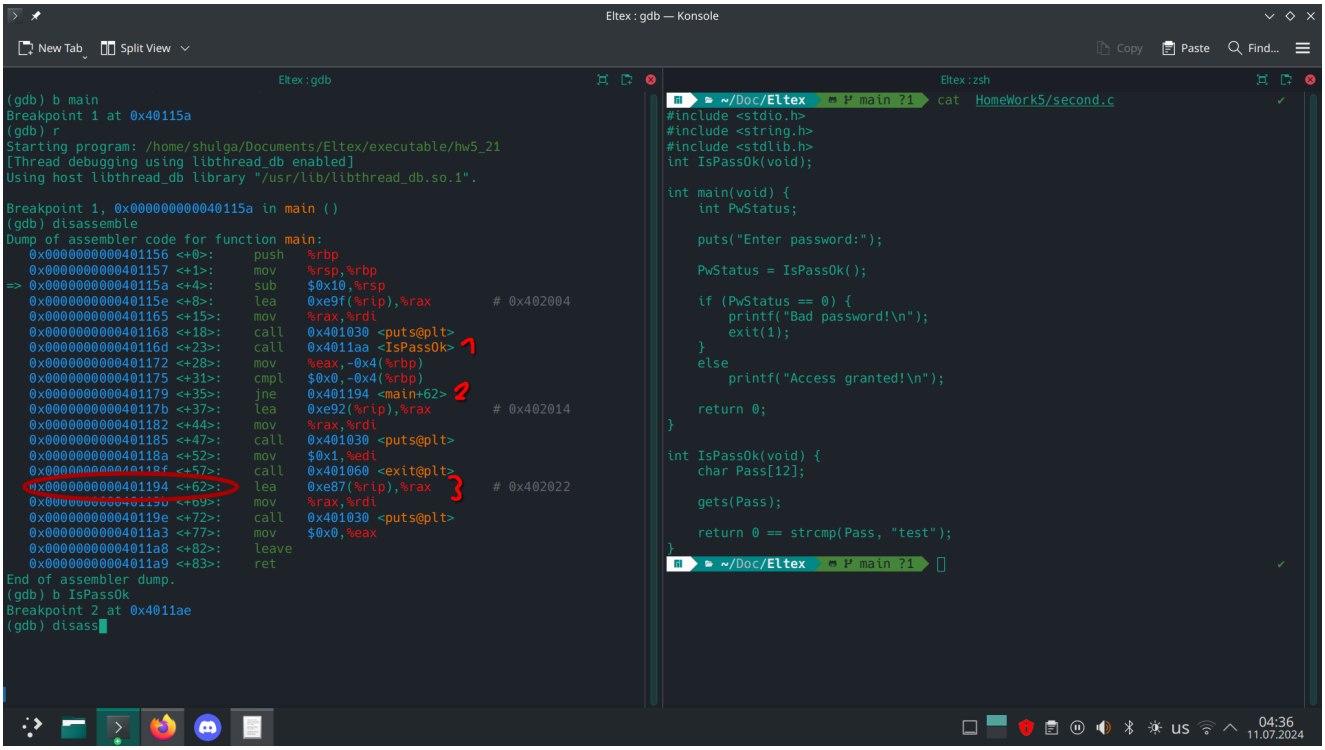
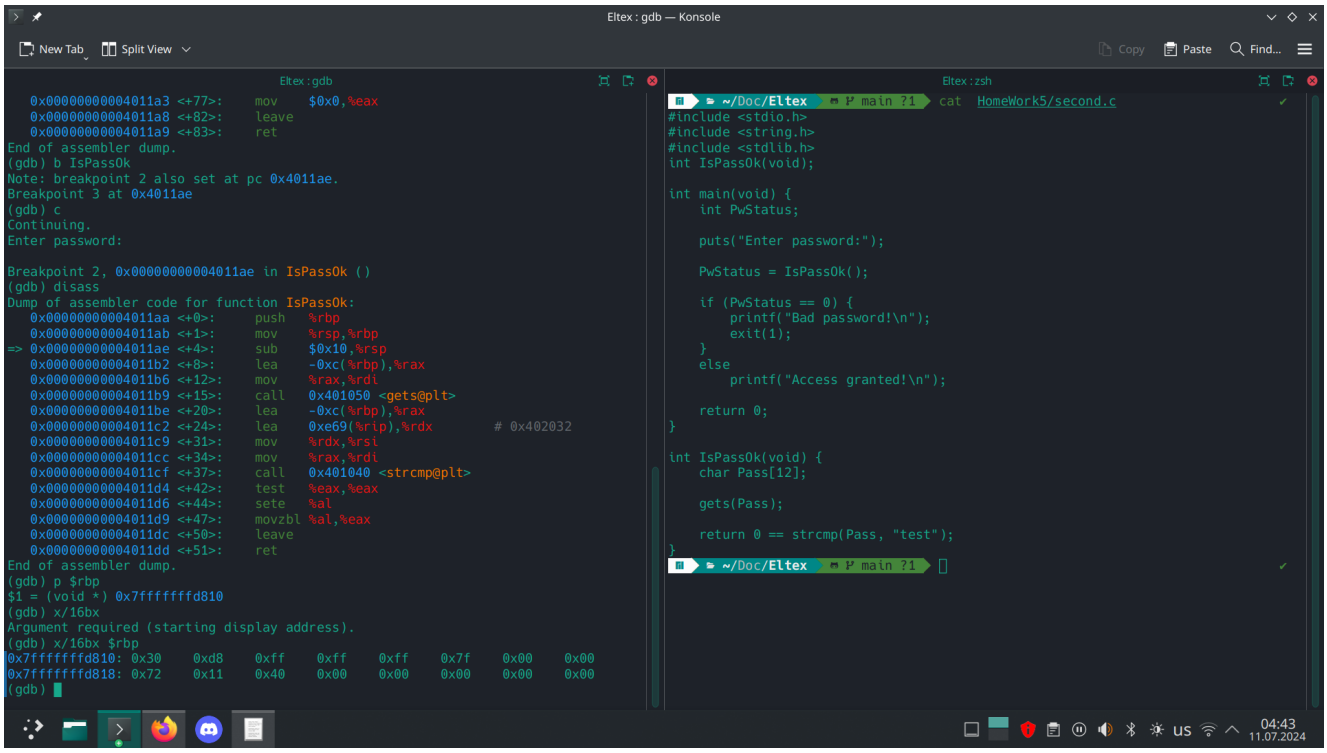
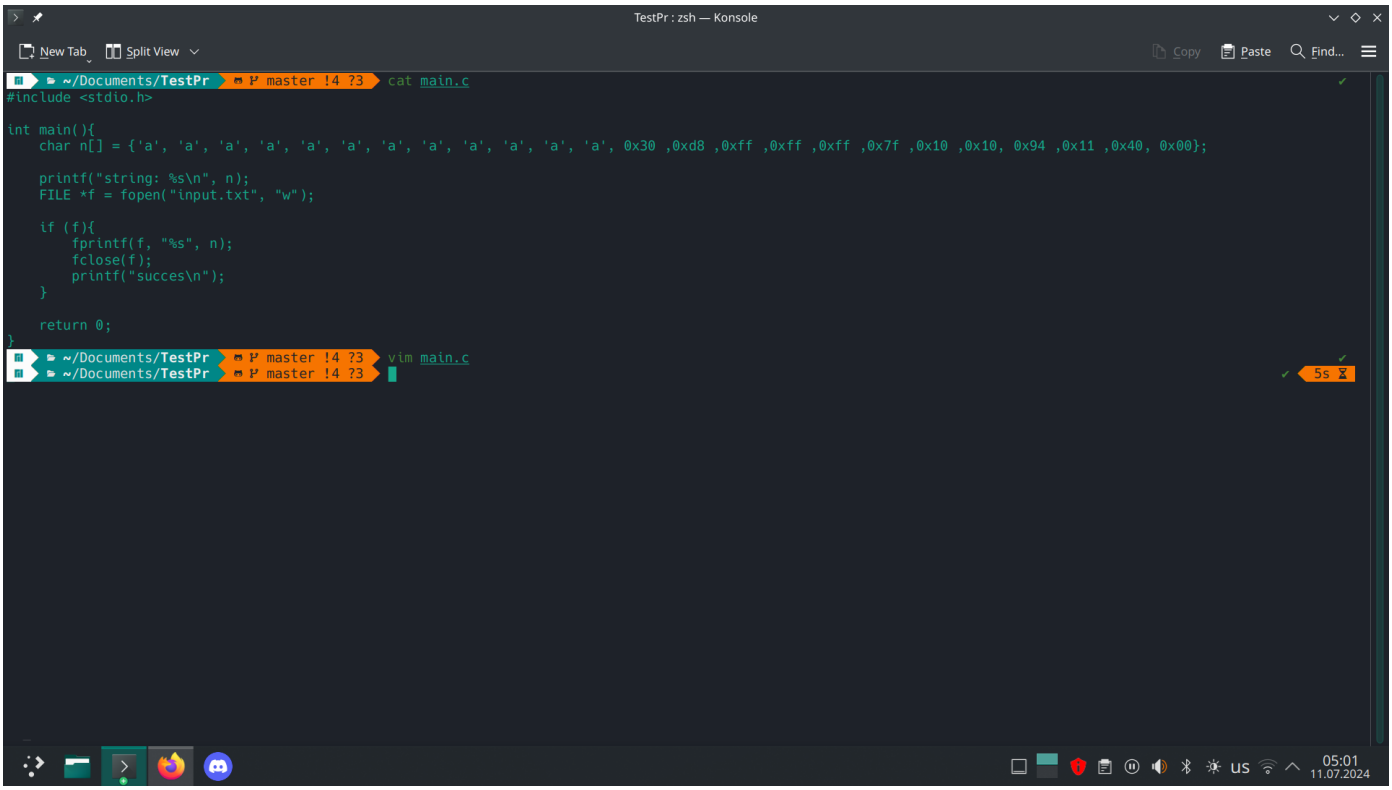


1 - узнаю название фунции проверки пароля
2 - команда jne отвечает за проверку условия и ведет на <main+62>.
тк в первой ветки условия есть ф-я <exit@plt>, то нужная ветка находится по адресу 0x401194, туда и буду "прыгать"
3 - искомая ф-я для возврата



disass для IsPassOk

нахожу адрес rbp и вывожу кусок памяти 16 байт от этого регистра, это мне даст информацию, что адрес возврата идет правильно
также вижу инструкцию для выделения эфективной памяти (lea) на 12 байт =>
массив вмещает в себя 12 элементов типа char, сразу после rbp
далее сохраню все нужные мне адреса и вычисляю нужное кол-во байт для переполнения (12+8+8) и перехожу к написанию файла ввода.



Эта программа создает файл и вводит туда 12 символов 'a' для массива,
8 мусорных сивмолов для rbp, 3 байта для изменения адреса возврата на <main+62>
и нулевой символ конца файла.