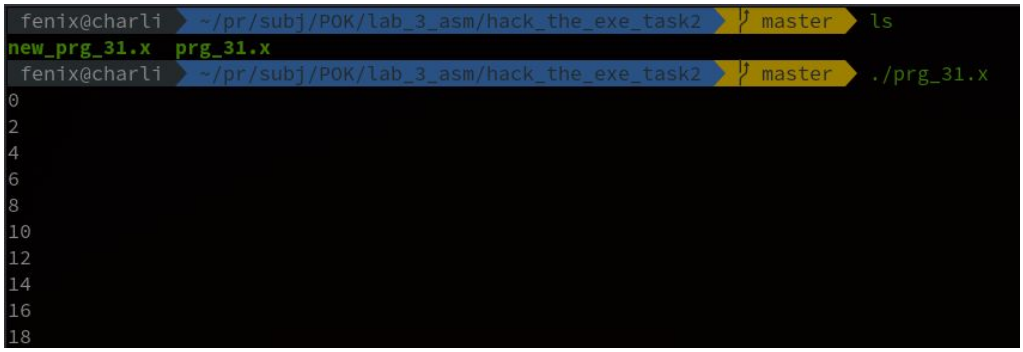
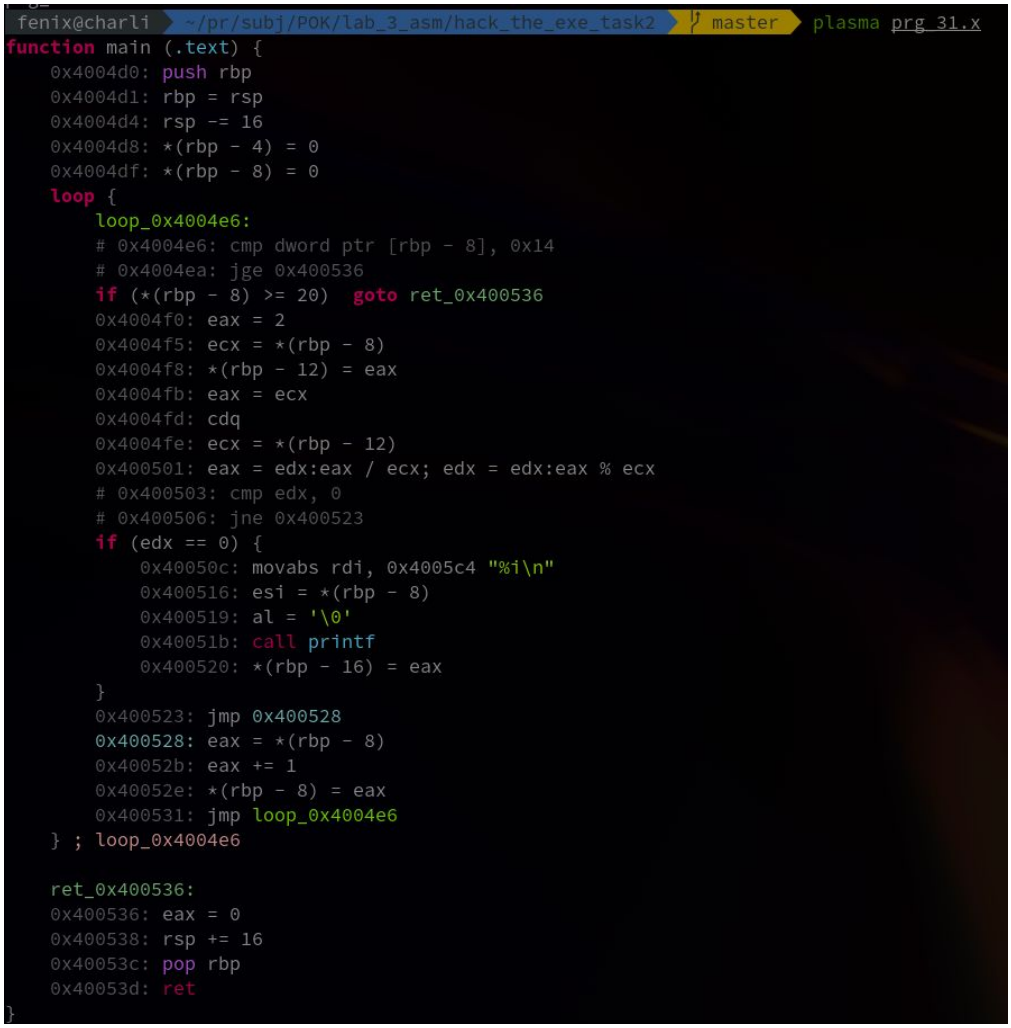
**Задача 31: Програма виводить парні числа в інтервалі [1, 19). Зробіть, щоб виводила їх в інтервалі [4-19).**

1) Скачав і створив копію ELF
2) Запустив ELF визначив що воно прінтує починаючи з 0 а не з 1 (оскільки парні то навіть з 2)

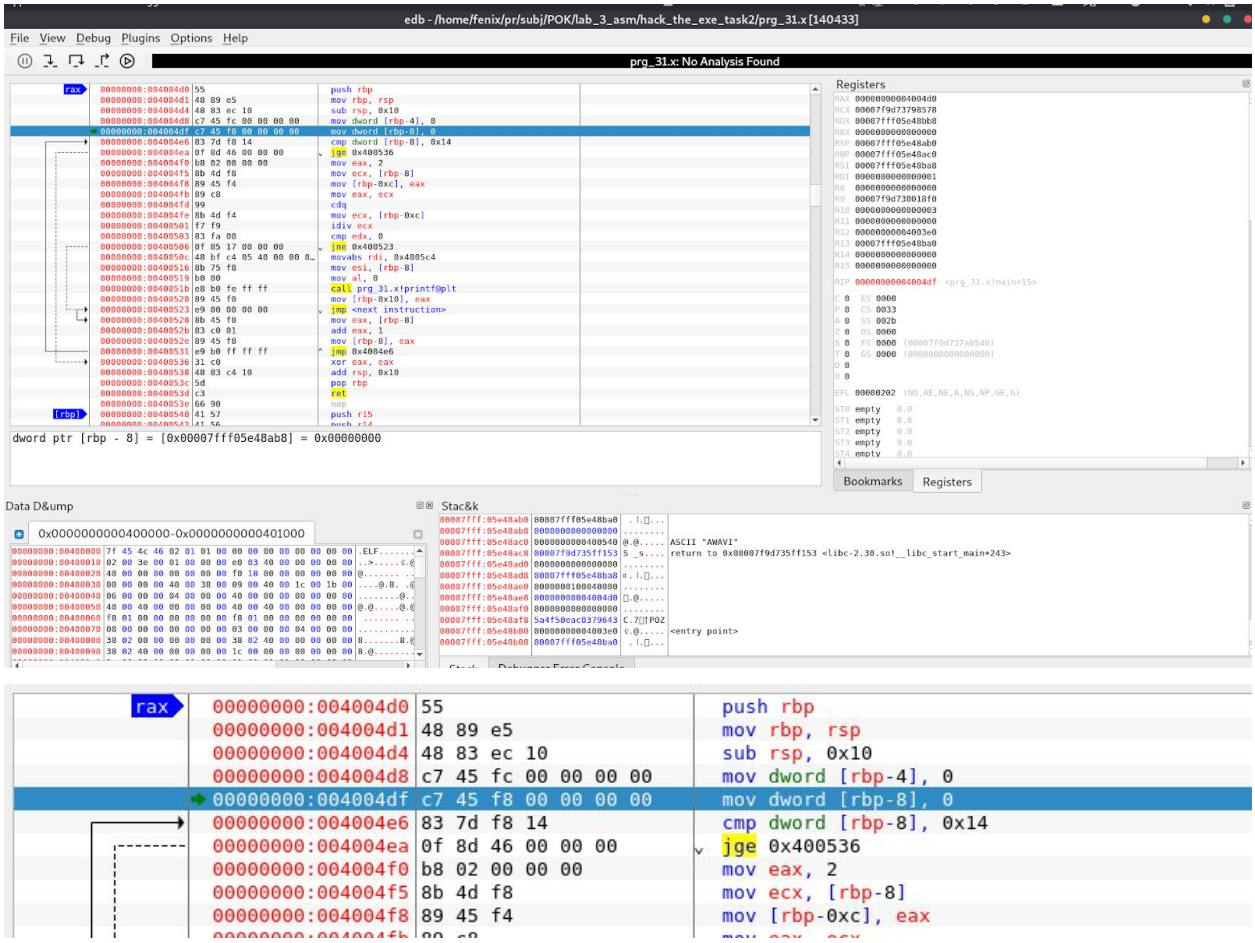



Деасемблював за допомогою ‘plasma’ і проаналізував як працює код.




Зробив висновок, що виводиться значення з пам’яті за адресою rbp-8 якщо воно парне. Цикл закінчується коли значення за адресою rbp-8 >= 20. Отже, якщо змінити початкове значення, яке присвоюється комірці за адресою rbp-8 на 4, то отримаємо бажаний результат.

3) Відкрив ELF в дебагері edb. Запустив програму і дійшов до присвоєння комірці значення.

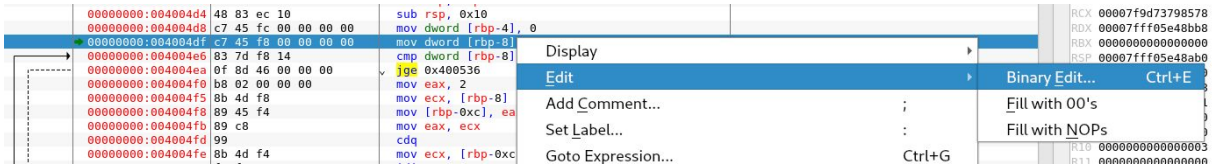


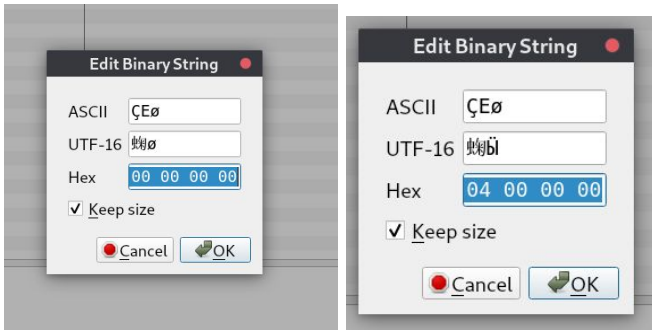




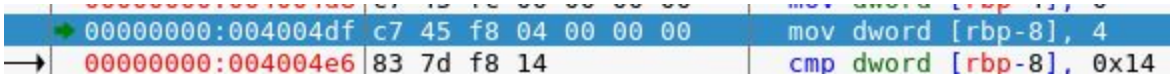
Чітко видно, в області машинного коду, де присвоюється значення 0 розміру подвійного машинного слова (4 байти) області в пам'яті.

4) Перевірив чи це дійсно те що потрібно змінити

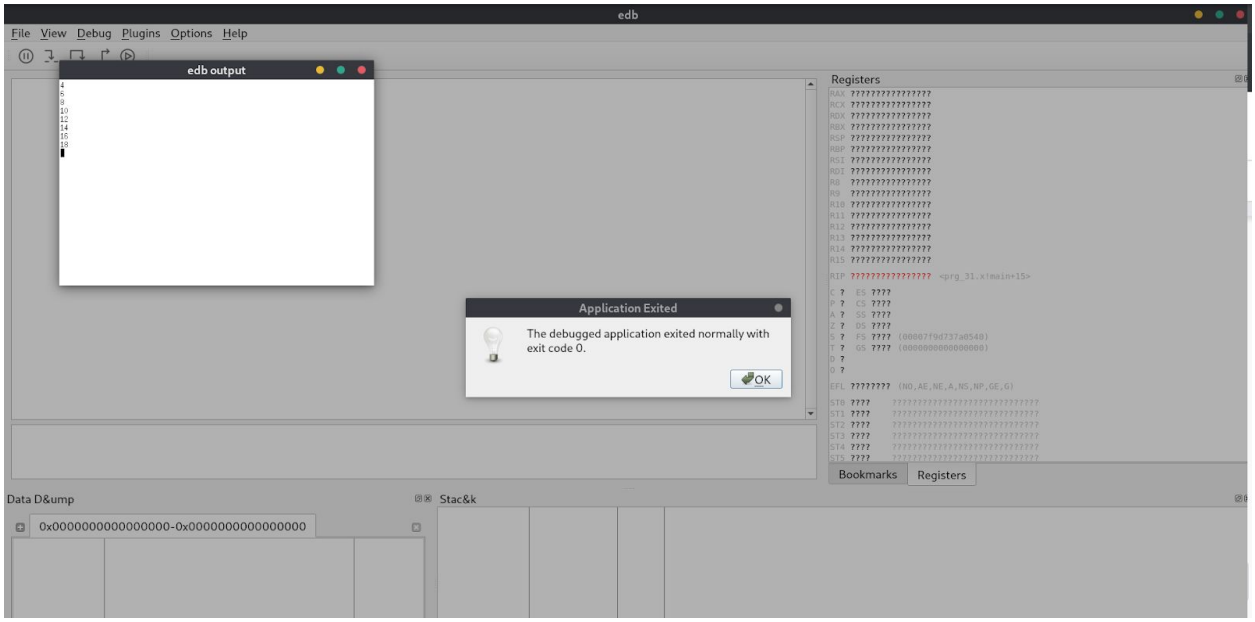


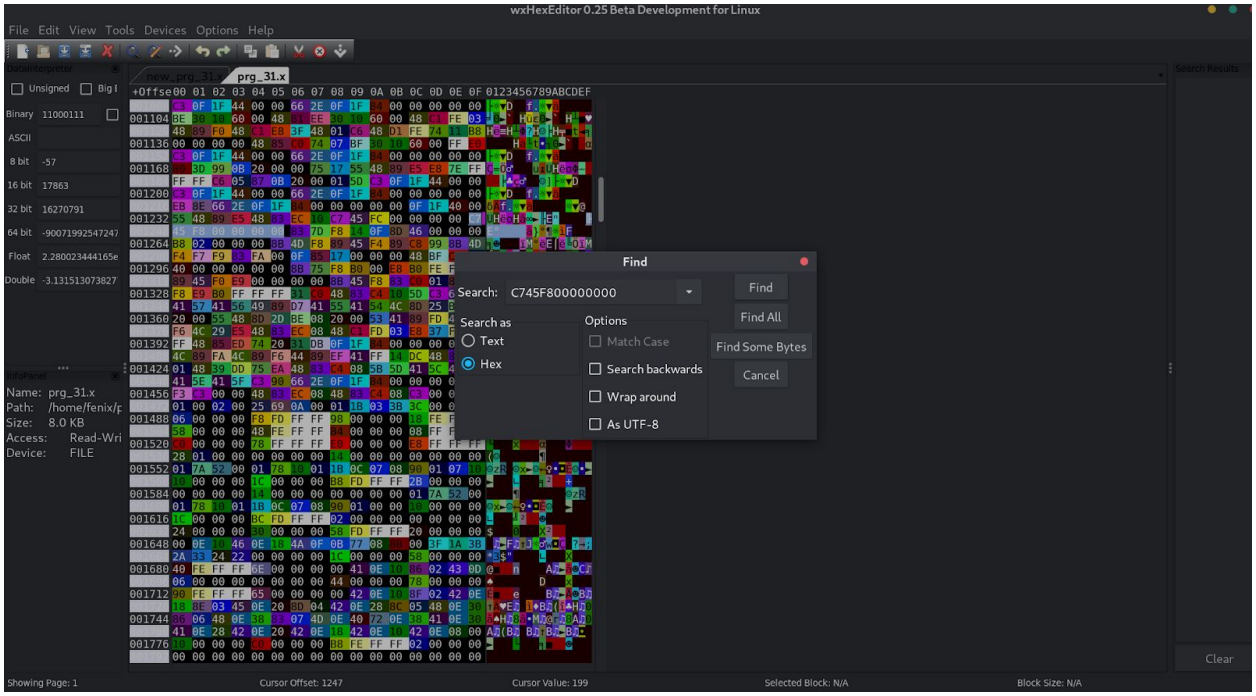

Оскільки значення зберігаються за принципом little-endian. Потрібно змінити перший лівий байт на 04 щоб отримати початкове значення "counter" 4.

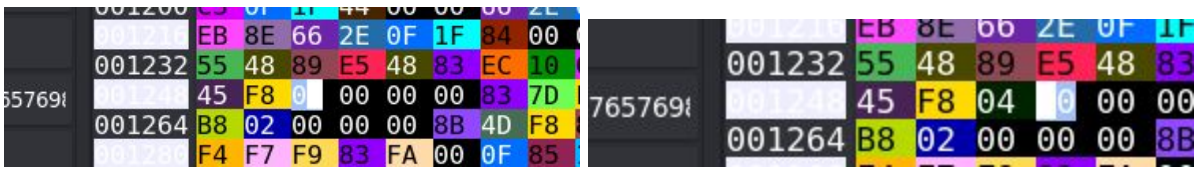


Запустивши програму до кінця отримав підтвердження, що програма працює так як треба.

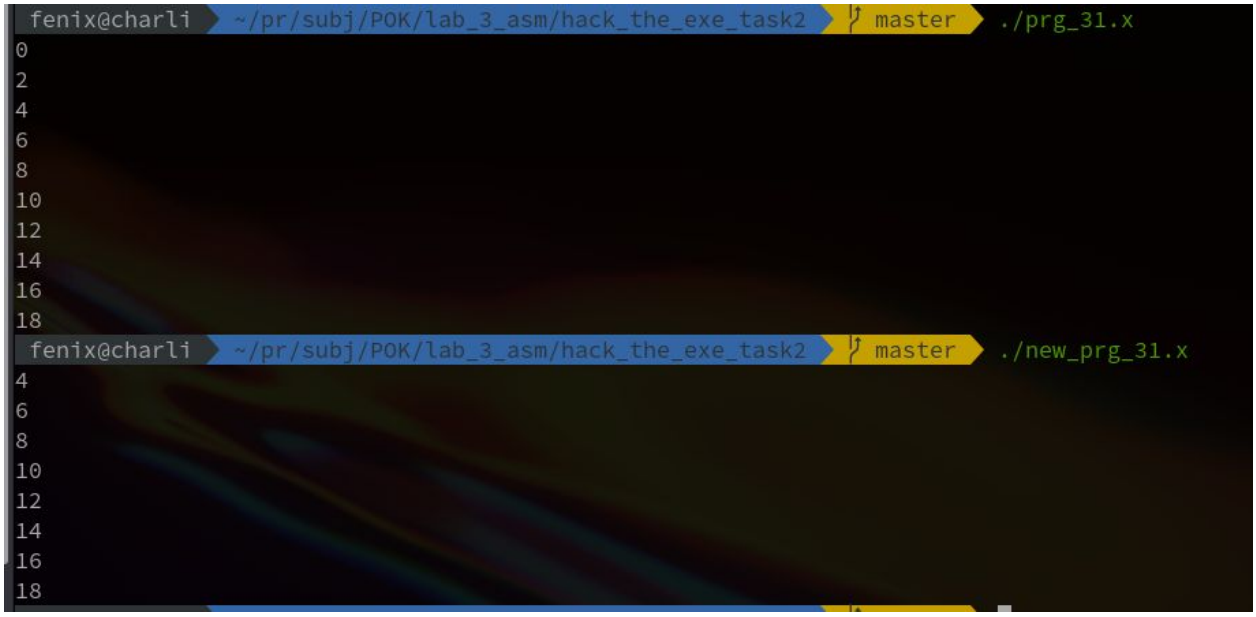



5) Тоді зайшов в бінарний редактор wxHexEditor і задавши в пошук достатньо довгу послідовність байт (c7 45 f8 00 00 00 00) знайшов необхідне місце для редагування.




Змінив один байт (номер якого 19972). Зберіг новоутворений ELF як new_prg_31.x і перевірив справність.


fenix@charli ~/pr/subj/POK/lab_3_asm/hack_the_exe_task2 master ./prg_31.x
0
2
4
6
8
10
12
14
16
18
fenix@charli ~/pr/subj/POK/lab_3_asm/hack_the_exe_task2 master ./new_prg_31.x
4
6
8
10
12
14
16
18