Міністерство освіти і науки України

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Кафедра Обчислювальна техніка та програмування

Звіт з лабораторной роботи з дисциплиі « Реверсне програмування »

Лабораторна робота 4

Виконав ст.гр. КІТ–36

Надірян Г.О.

Перевірив

Челак В.В.

Харків 2019

**Лабораторна робота 4**

**Тема**: «Впровадження коду. Додавання нової секції»

##### Мета: Набути практичних навичок виправлення помилок в програмному забезпеченні, яке знаходиться в експлуатації; створення нової функціональності, використовуючи неявне в експлуатації програмне забезпечення для платформи х64 в середовищі masm64.

##### Постановка задачі

##### Виконати завдання в кілька етапів:

##### 1.Написати програму в середовищі masm64 відповідно до завдання. На початку програми здійснити перевірку можливості мікропроцесора підтримувати команди AVX і AVX2. Про що вивести функціями MessageBox відповідні повідомлення. В кінці програми вивести отримані результати через функцію MessageBox, а також номер варіанта, назва лабораторної роботи, шифр групи, прізвище виконавця.

##### 2.Проізвесті підрахунок вільного місця в секції коду.

##### 3.Добавіть нову секцію коду, в яку здійснити впровадження функції виведення повідомлень MessageBox з висновком тесту «інфікованих. ПІБ, номер групи ». Цей висновок здійснити після виведення повідомлення про перевірку можливості мікропроцесора підтримувати команди AVX і AVX2 і перед виведенням спрощеного вікна з основними результатами програми.

##### Завдання

##### Відповідно до номером студента в групі вибрати варіант завдання і написати в середовищі masm64 на асемблері програму. Числа а є {a1, a2, a3, a4} задані масивом.

##### *a/cd – √e + b*

Результат виконання програми до впровадження

наведено на рис.1.

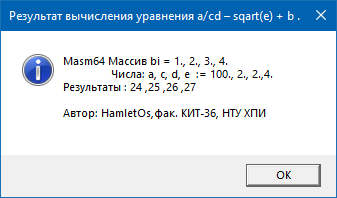


Рисунок 1- Результат виконання програми наведено на рис.1.

Додаємо нову секцію коду. Для цього в програмі-аналізаторі РЕ-коду LordPE виконуємо дії:

- натискаємо на кнопку меню Sections

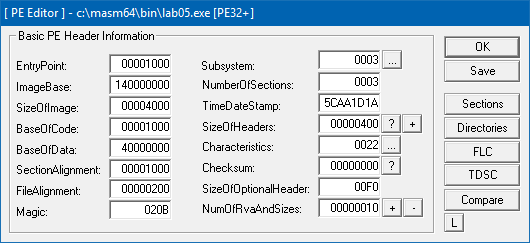


Рисунок 2 - Натискаємо на кнопку меню Sections

- Виділяємо будь-яку секцію і додаємо нову секцію за допомогою кнопки меню add section header (рис. 6.3);

- У вікні виділяємо нову секцію і для зміни властивостей нової секції натискаємо на кнопку меню edit section header ... При цьому необхідно запам'ятати зміщення roffset нової секції. В даному випадку воно дорівнює 0000 0а00h;

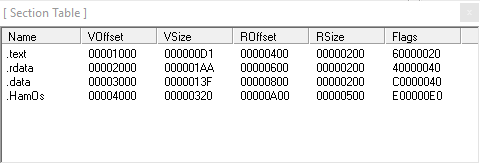


Рисунок 3 – Нова секция

Заповнюємо осередки нового блоку нулями.

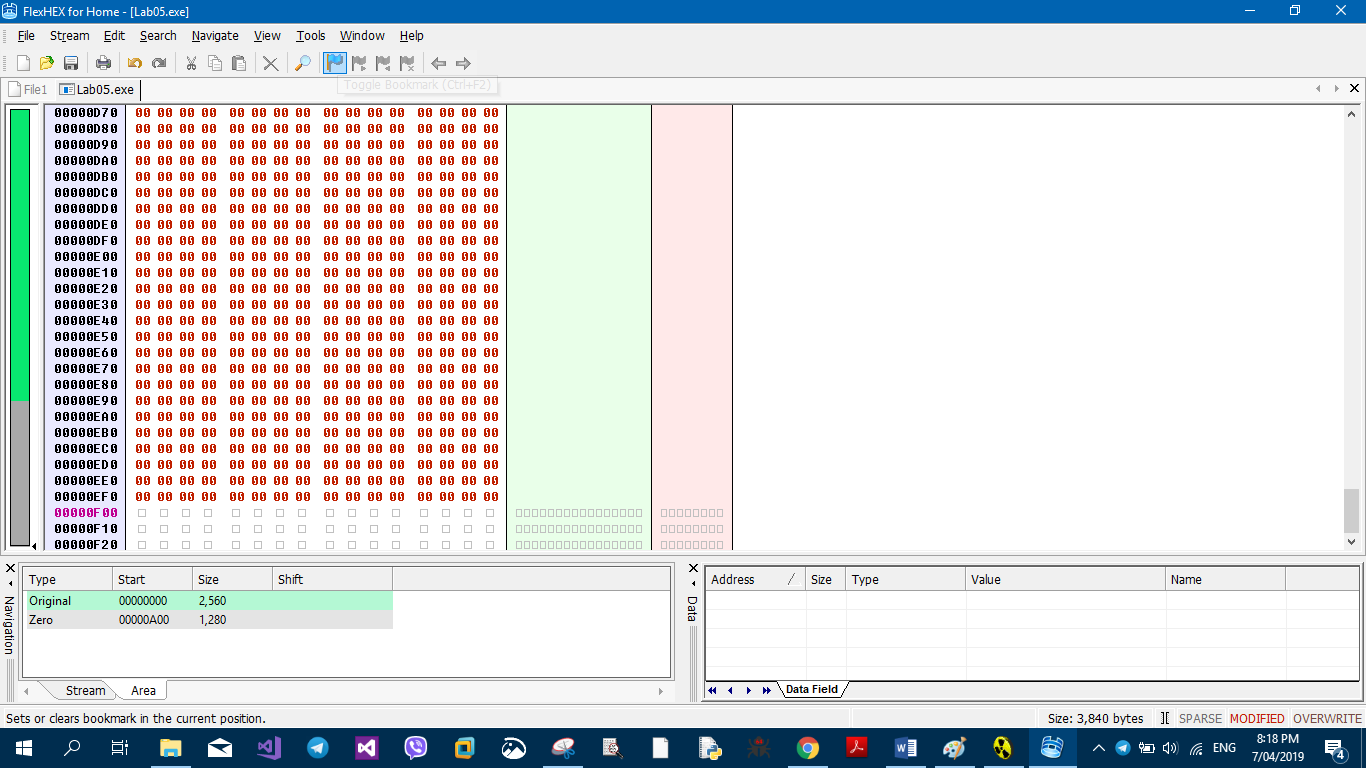


Рисунок 4 - Заповнюємо осередки нового блоку нулями.

Перевірка нової секції

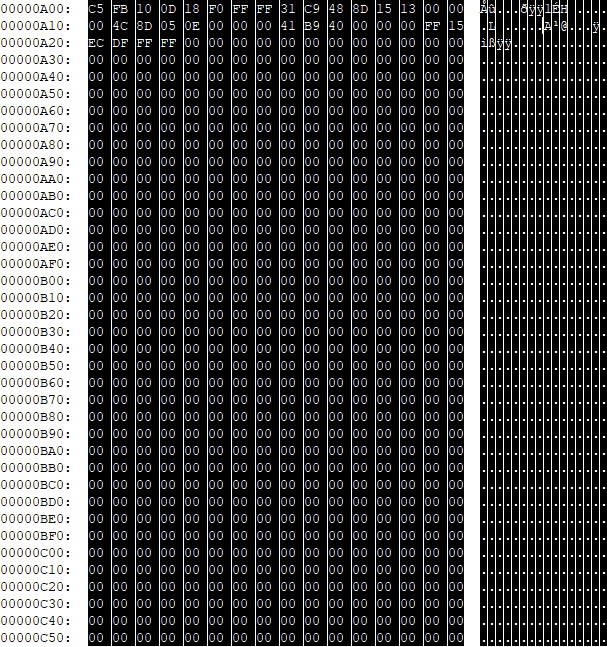


Рисунок 4 - Перевірка нової секції

Вносимо зміни в код, використовуючи відладчик x64Dbg.

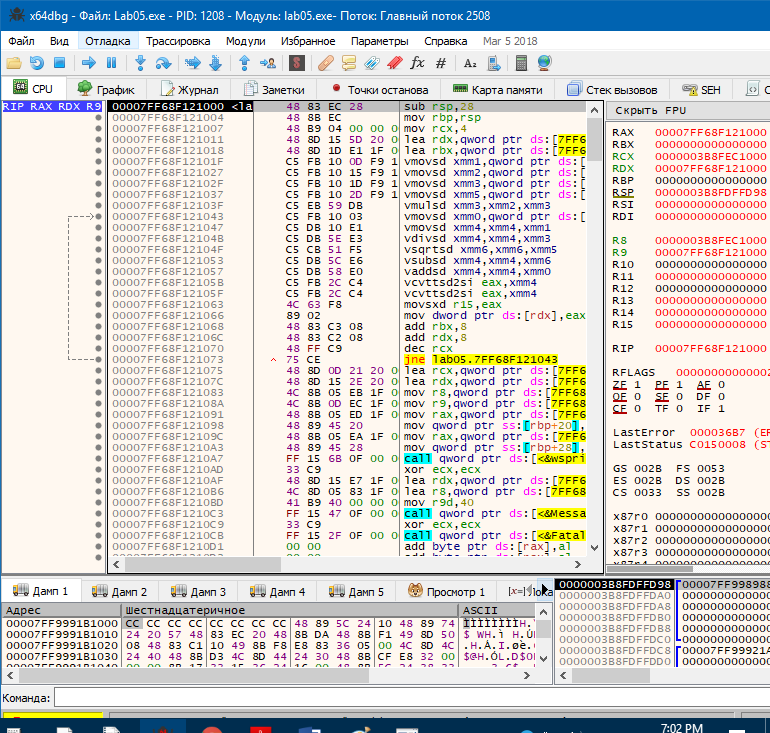


Рисунок 5 - Зовнішній вигляд коду

Звільнимо місце для команди jmp. виберемо команду. Двічі виділяємо цей рядок (рис. 6.) і її копіюємо.

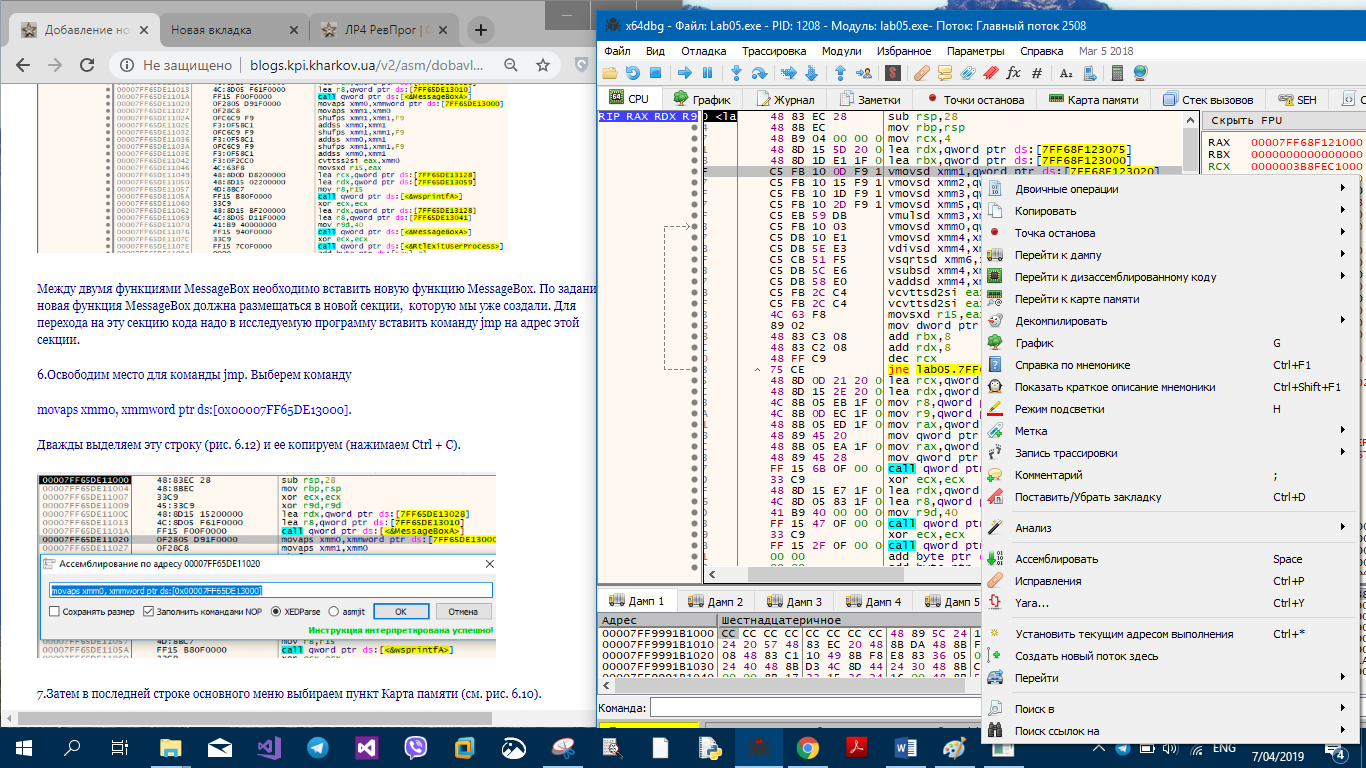


Рисунок 6 - Звільнимо місце для команди jmpс

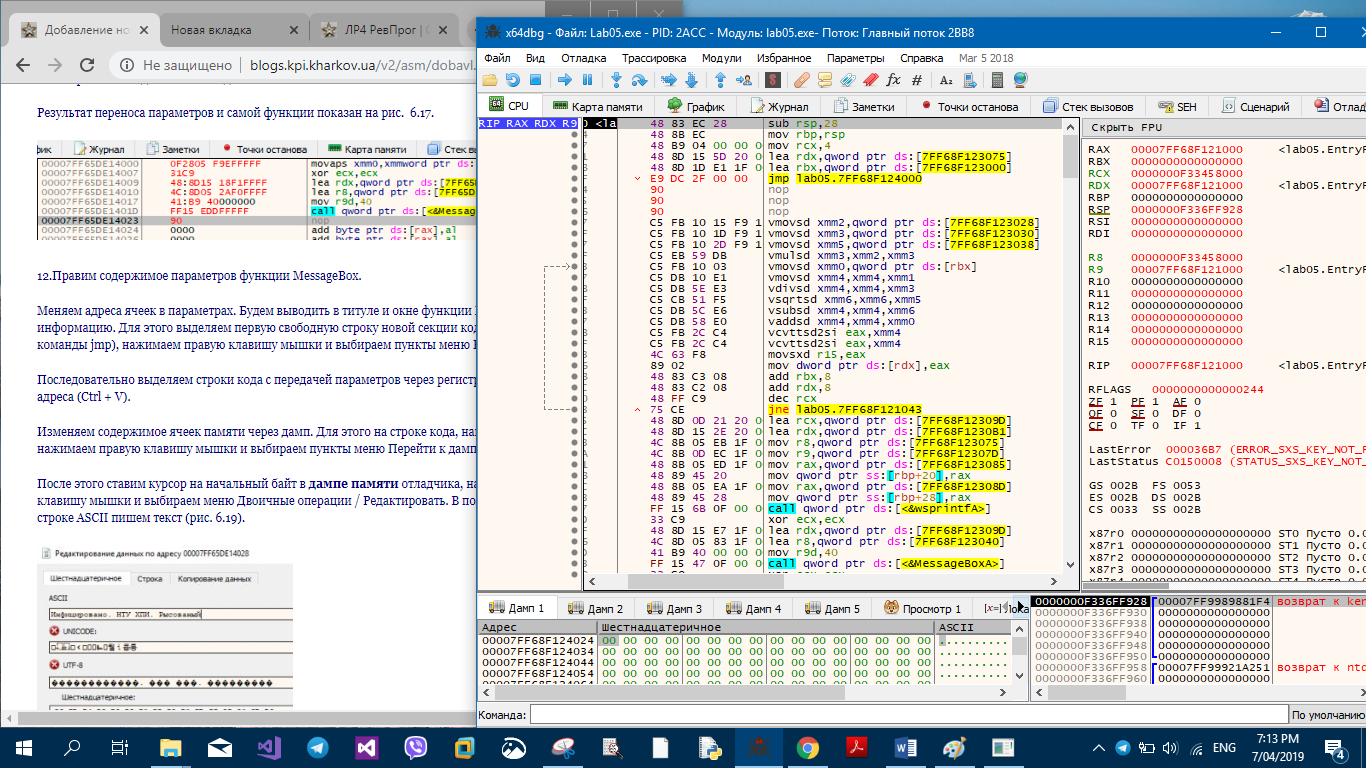


Рисунок 7 – jmp на адрес нової секції



Рисунок 8 – Нова секція

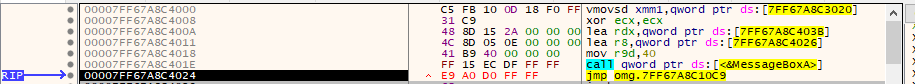
Результат перенесення параметрів і самої функції показан на рис.9. 

Рисунок 9 - Результат перенесення параметрів і самої функції

Правимо вміст параметрів функції MessageBox.

Міняємо адреси осередків в параметрах. Будемо виводити в титулі функції MessageBox “Hamlet Nadirian”

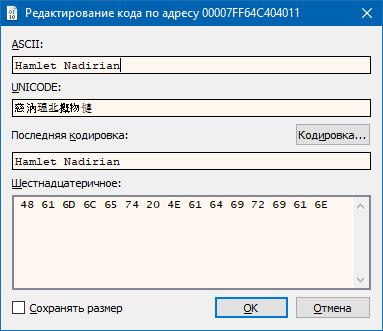


Рисунок 10 - Міняємо вміст регистру rdx

Міняємо адреси осередків в параметрах. Будемо виводити у вікні функції “Инфицировано Гамлет”

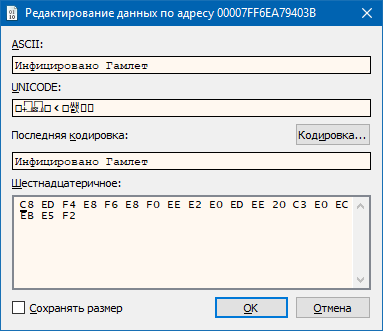


Рисунок 11 - Міняємо вміст регистру r8

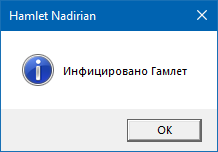


Рисунок 12 - Результат роботи після впровадження коду в ехе-файл в кінець секції з додаванням API-функцій

**Висновок**

Впровадили код. Додали нову секцію. Набули практичні навичкии виправлення помилок в програмному забезпеченні, яке знаходиться в експлуатації; створили нові функціональності, використовуючи неявне в експлуатації програмне забезпечення для платформи х64 в середовищі masm64.