**Министерство науки и высшего образования Российской Федерации**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий**

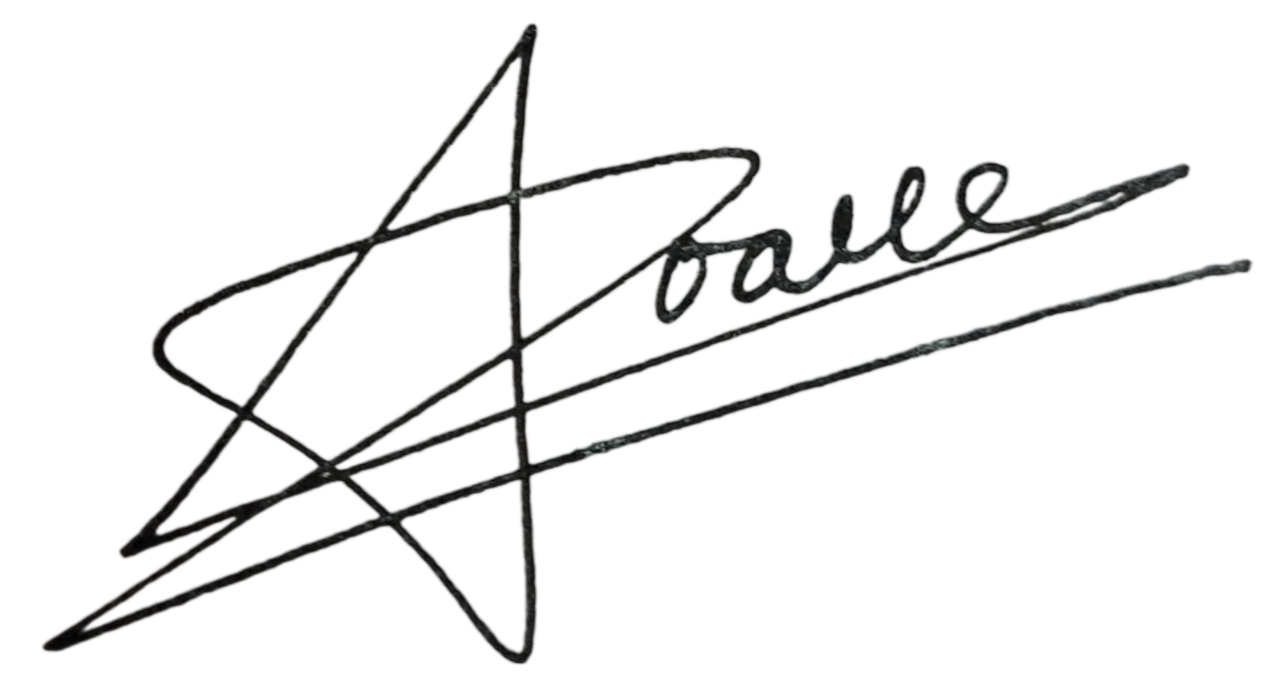
**Дисциплина:**

«Технологии и методы программирования»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №4**

**Выполнил:**

Чу Ван Доан – Студент группы N3347

*\_\_\_\_\_\_\_\_\_\_\_**\_\_\_*

(подпись)

**Проверил:**

Ищенко Алексей Петрович

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

Санкт-Петербург

2024 г.

**Содержание**

[**1. Задание 3**](#_heading=h.30j0zll)

[**2. Ход работы 3**](#_heading=h.1fob9te)

[**Заключение 6**](#_heading=h.3znysh7)

# Задание

**Задача:** Получить пароль от программы, используя индивидуальный секрет.

**Вариант**: 5zgw95y4

# Ход работы

* Чтобы получить пароль я использую приложение x32dbg.
* Введение и обзор применения x32dbg в качестве инструмента для анализа вредоносных программ. x32dbg — отладчик с открытым исходным кодом для Windows, который часто используется в качестве инструмента анализа вредоносных программ. Отладчик предназначен для пошагового выполнения кода, что позволяет отслеживать его действия. Отладчики необходимы для поиска и устранения ошибок, однако они также позволяют декомпилировать вредоносные программы
* Открыла приложение LabReverse в x32dbg и нажмите «Выпольнить» пока приложение не запустится (рисунок 1).

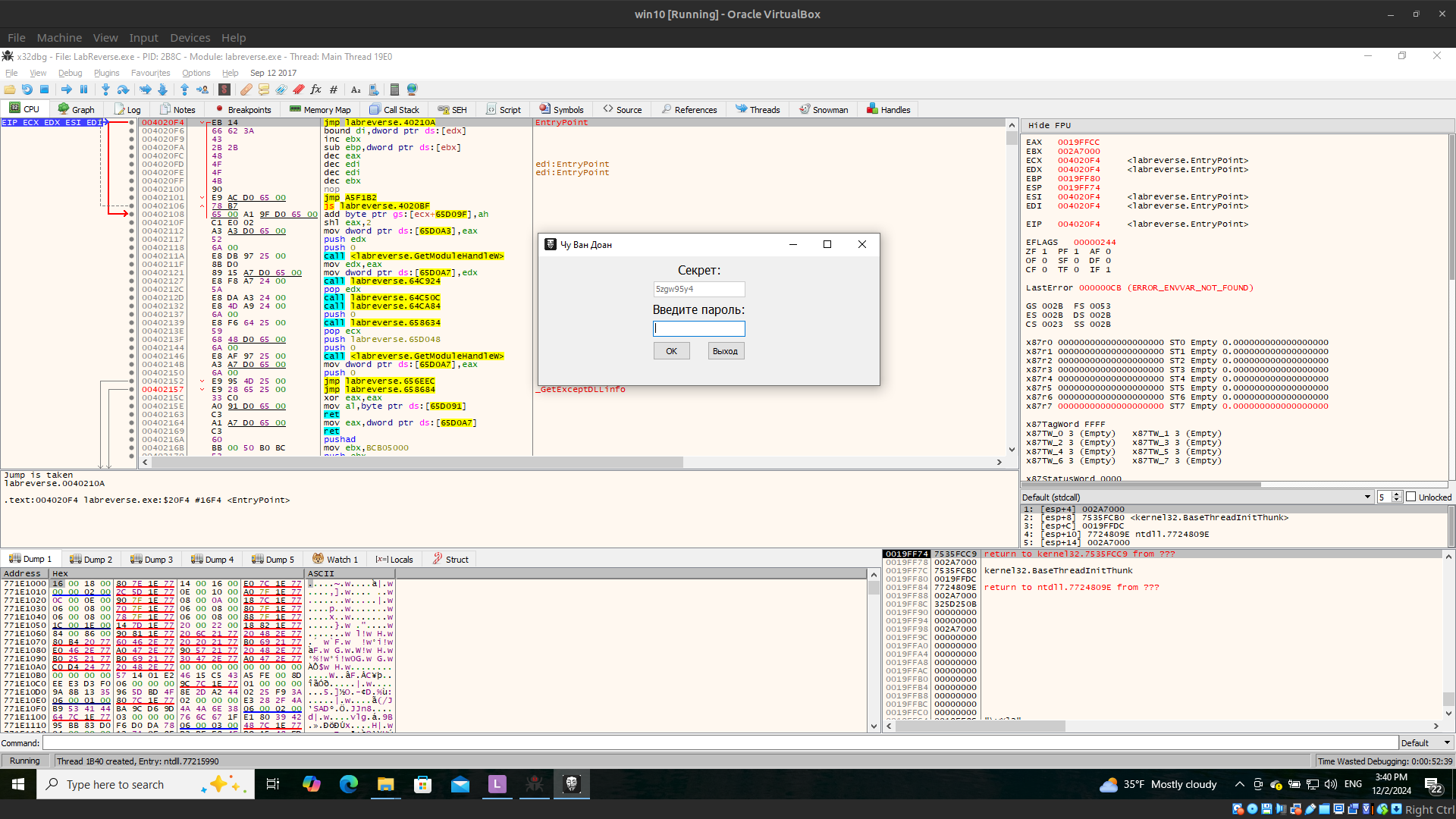


Рисунок 1 – LabReverse в x32dbg с вариантом Чу Ван Доан

Вводим пароль из 8 символов "password" и получил результат что пароль не правильный (рисунок 2).

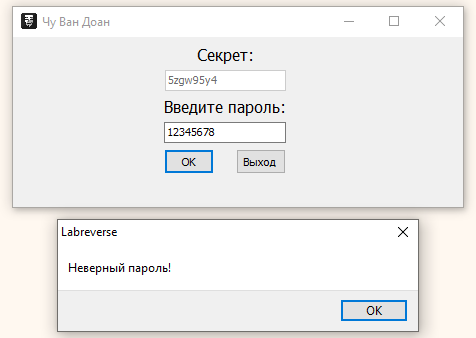


Рисунок 2 – Неверный пароль

Щелкнул правой кнопкой мыши, выбрал Search for –> Current module –> String reference.

Я пробовал много раз, и первая строка всегда была постоянной и кликнула по ней. (рисунок 3).

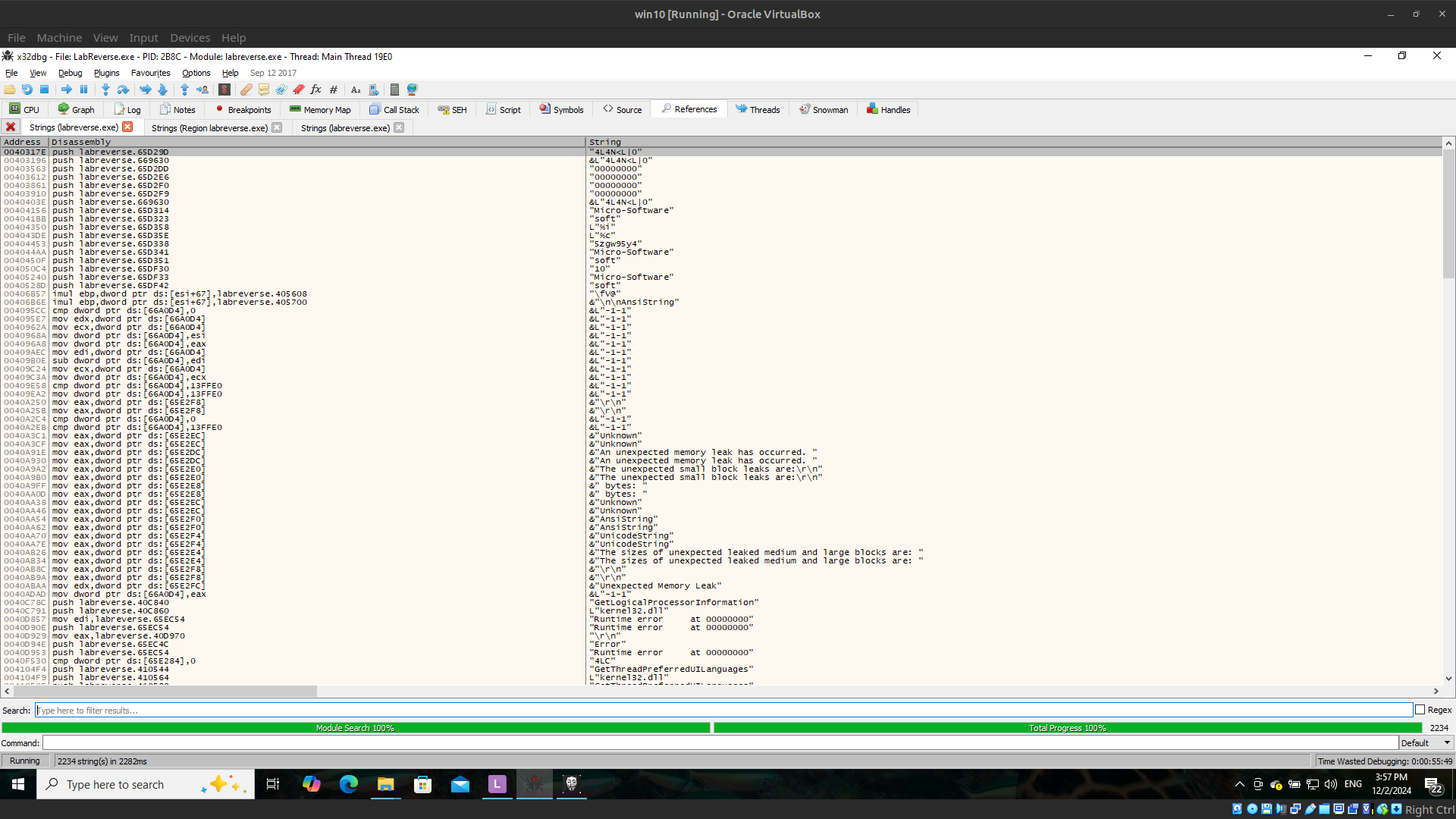


Рисунок 3 – Все модули (строки)

Затем дважды щелкнил по этой первой постоянной строке. Мы получим адрес этой строки (рисунок 4).

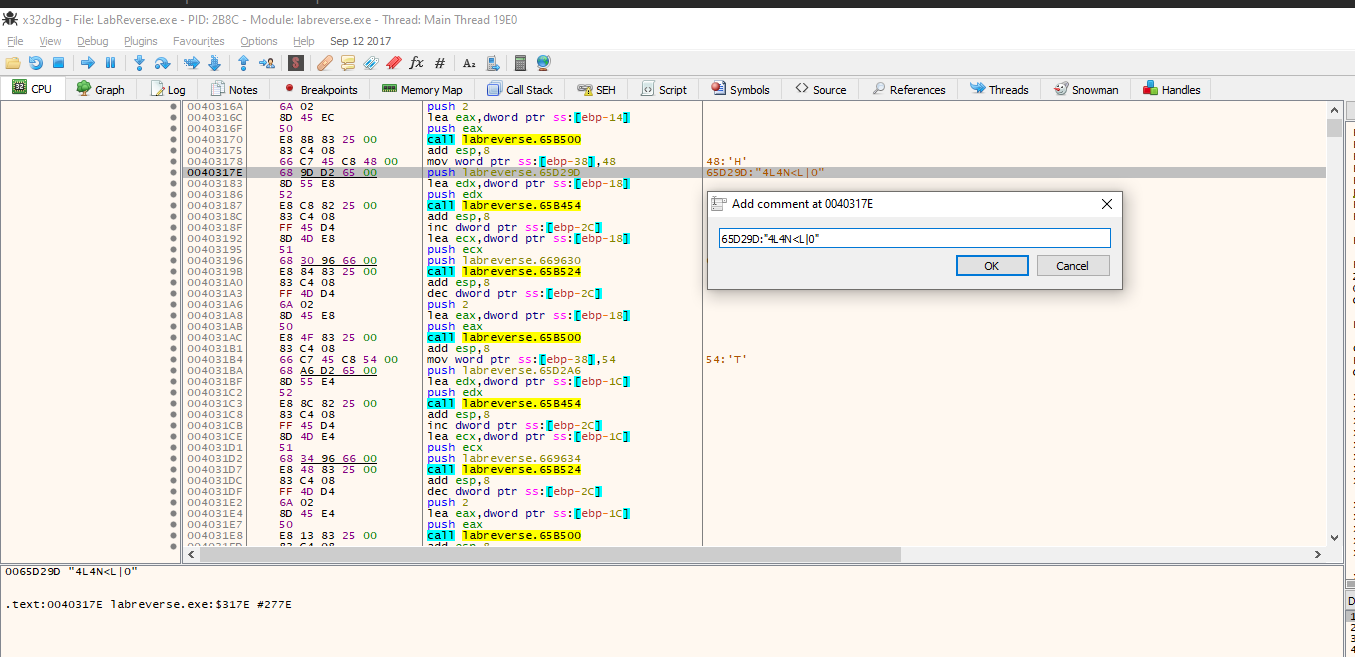


Рисунок 4 – Адрес этой строки

Я написал программу на Python, которая может взломать криптографические ключи

user = bytearray(b"5zgw95y4")

pwd = bytearray(b"4L4N<L|0")

for i in range(8):

d = user[i] ^ pwd[i]

if 48 <= d <= 59:

print(chr(d), end='')

continue

if 97 <= d <= 123:

print(chr(d), end='')

continue

if 80 <= d <= 89:

print(d - 80, end='')

continue

else:

print(chr(ord('a') - 1 + d), end='')

continue



Рисунок 5 – Python программа

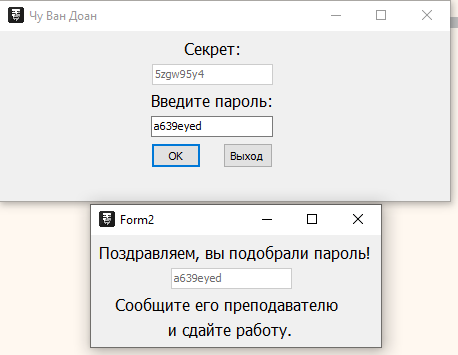


Рисунок 6 – Верный пароль

# 

# Заключение

В этой лаборатории я немного научился использовать программное обеспечение

x32dbg для обнаружения секретной строки в зашифрованном виде и успешно

расшифровал ее, создав программу на Python