

Навчально-науковий інститут інформаційних технологій
Харківський національний економічний університет
імені Семена Кузнеця

Звіт

З Виконання лабораторної роботи №1

за дисципліною: “Основи стеганографічного захисту інформації”

Виконав: студент кафедри
Кібербезпеки та інформаційних
технологій

4 курсу, спец. Кібербезпека,
групи 6.04.125.010.21.2

Бойко Вадим Віталійович

Перевірила:

Венгріна Олена Сергіївна

ХНЕУ ім. С. Кузнеця

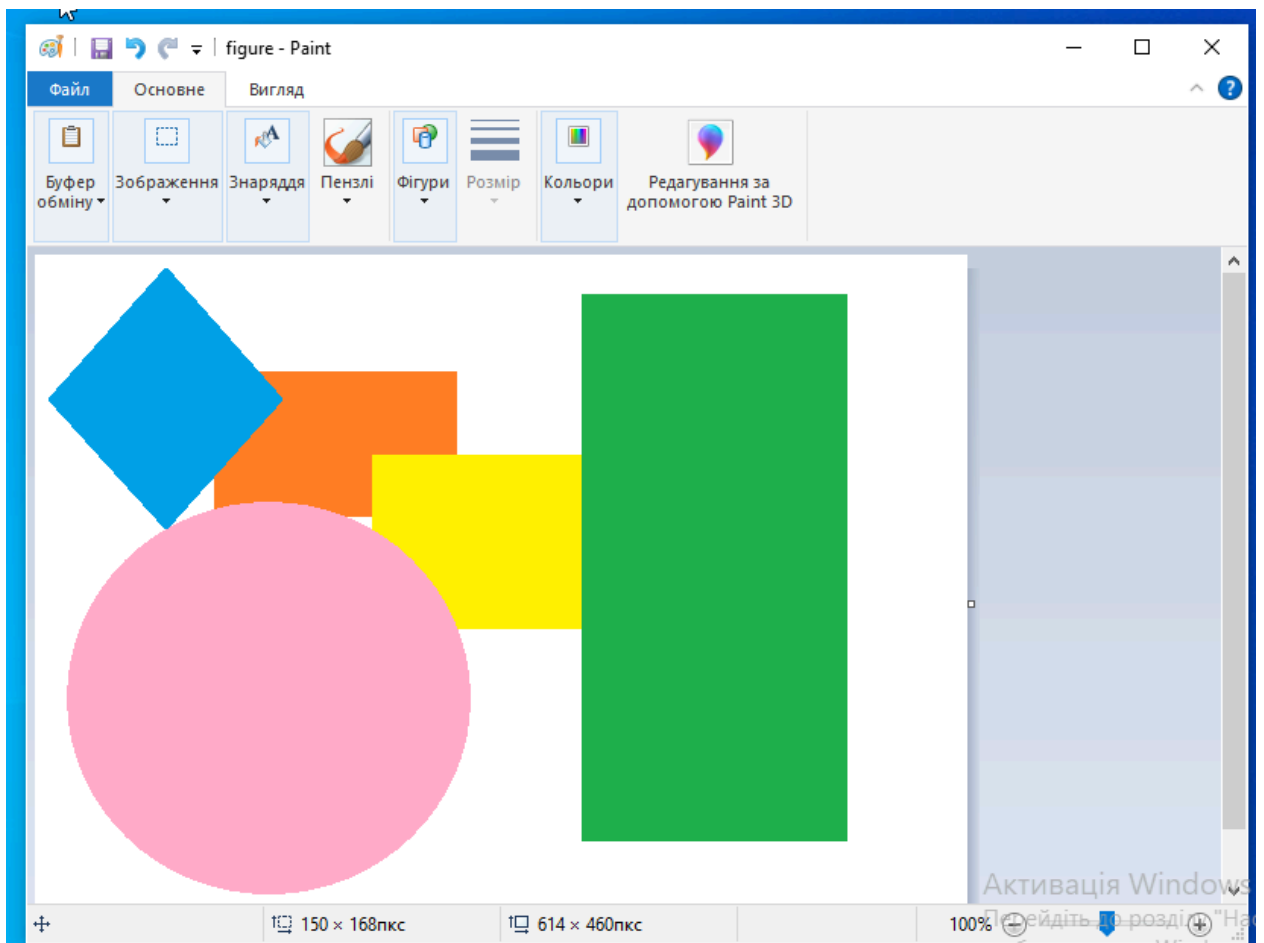
2024

Мета: Ознайомлення з поняттям стеганографії, її базовими принципами, використовуваними форматами контейнерів, способами упаковки приховується, найбільш популярними програмами стеганографії

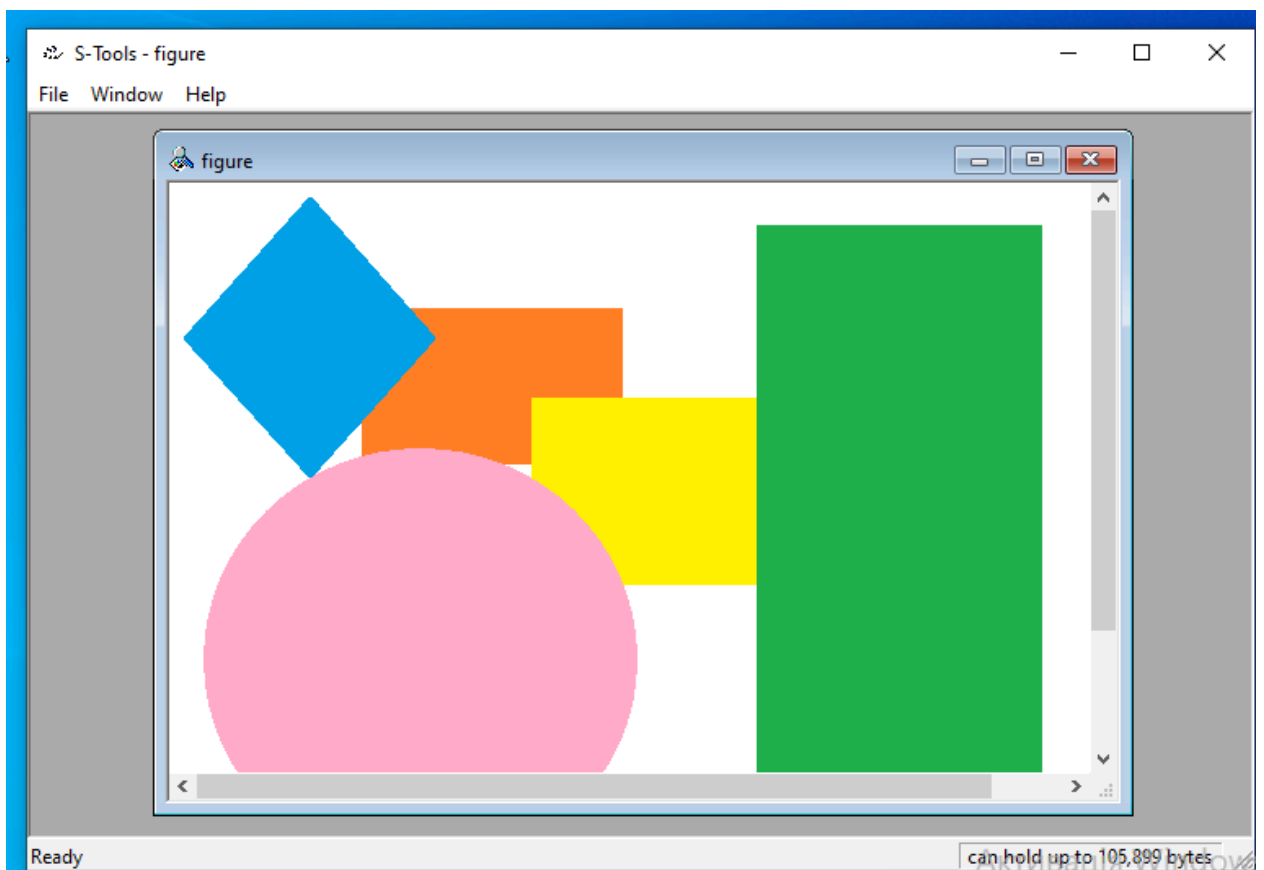
Хід роботи:

1. Робота з S-Tools

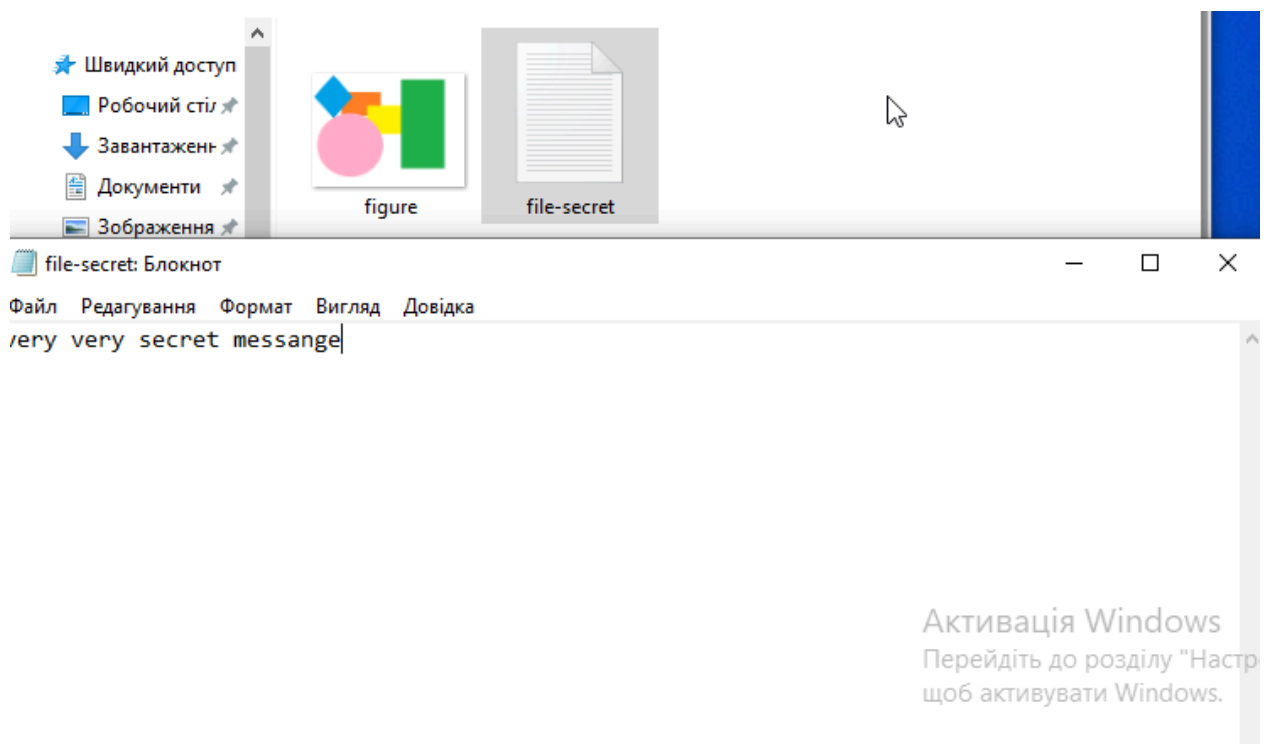
Підготую зображення для використання як контейнер



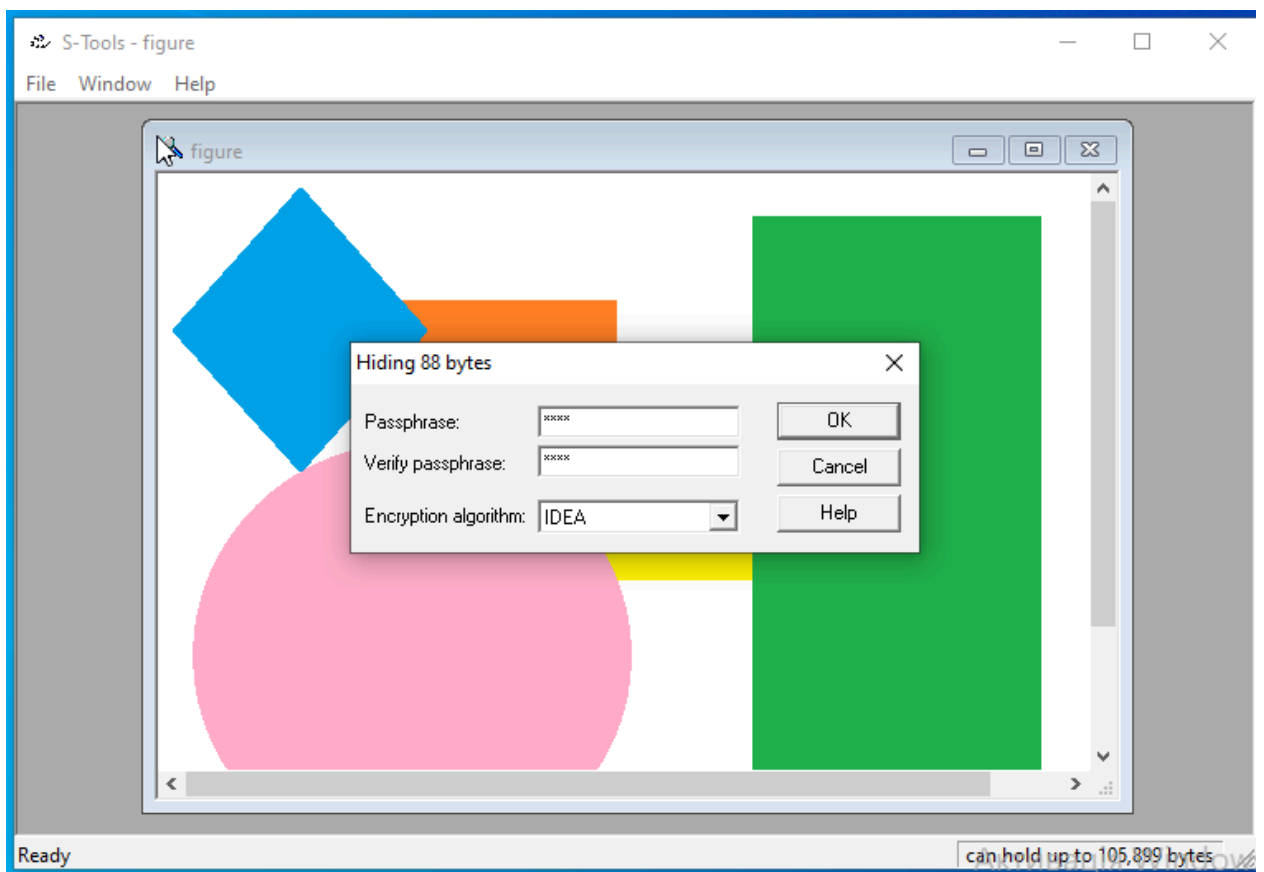
Додам зображення до програми



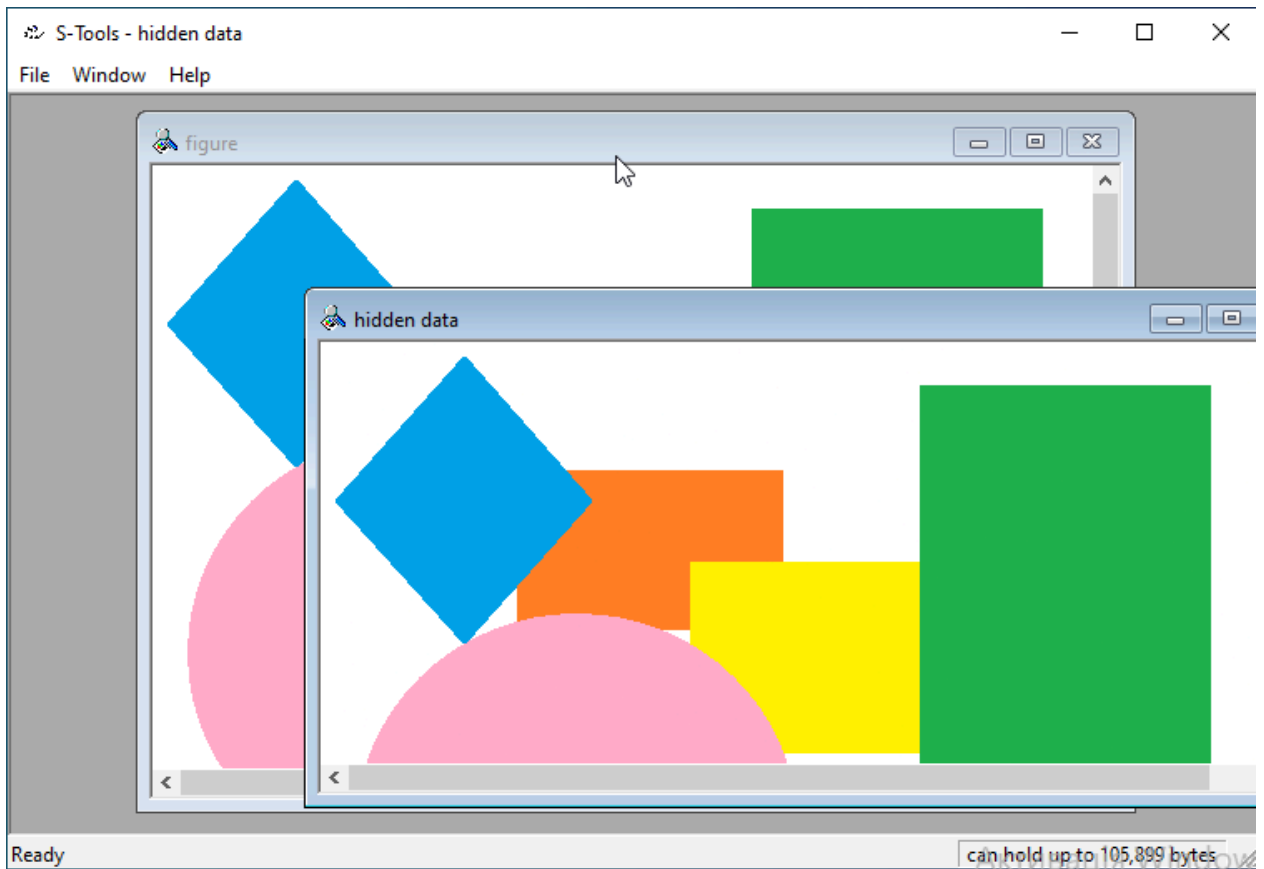
Створю файл який буду ховати у контейнері



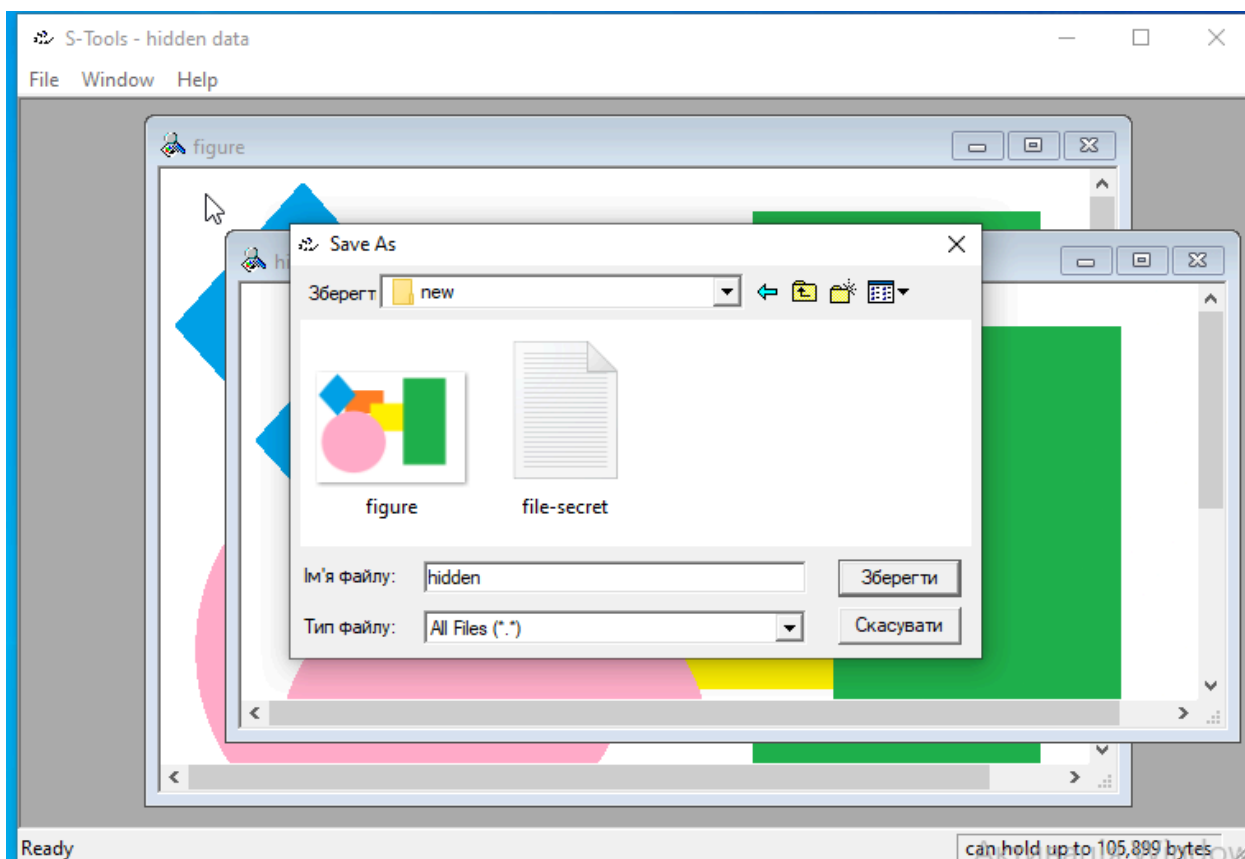
Додам ключ до файлу-контейнеру для ховання інформації



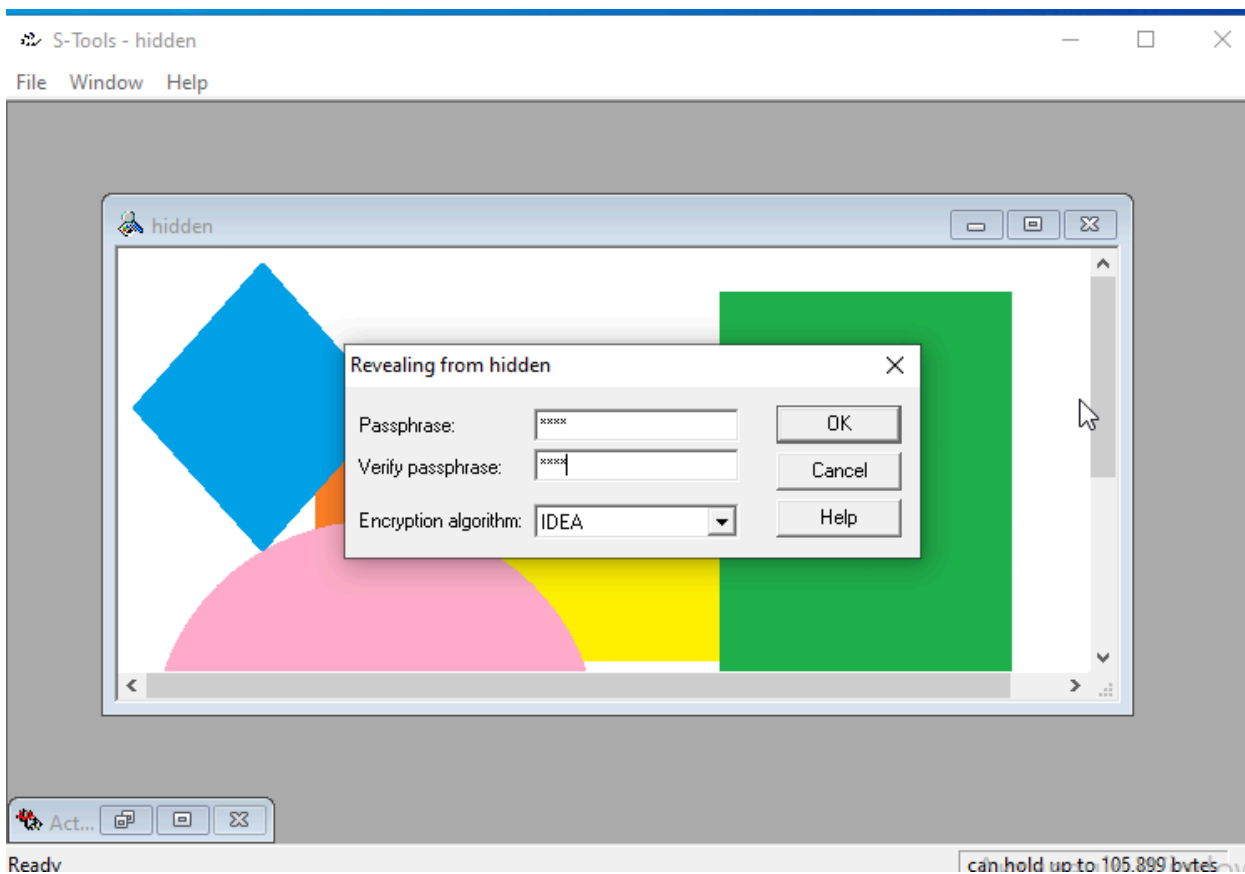
В результаті отримую новий файл з прихованою інформацією



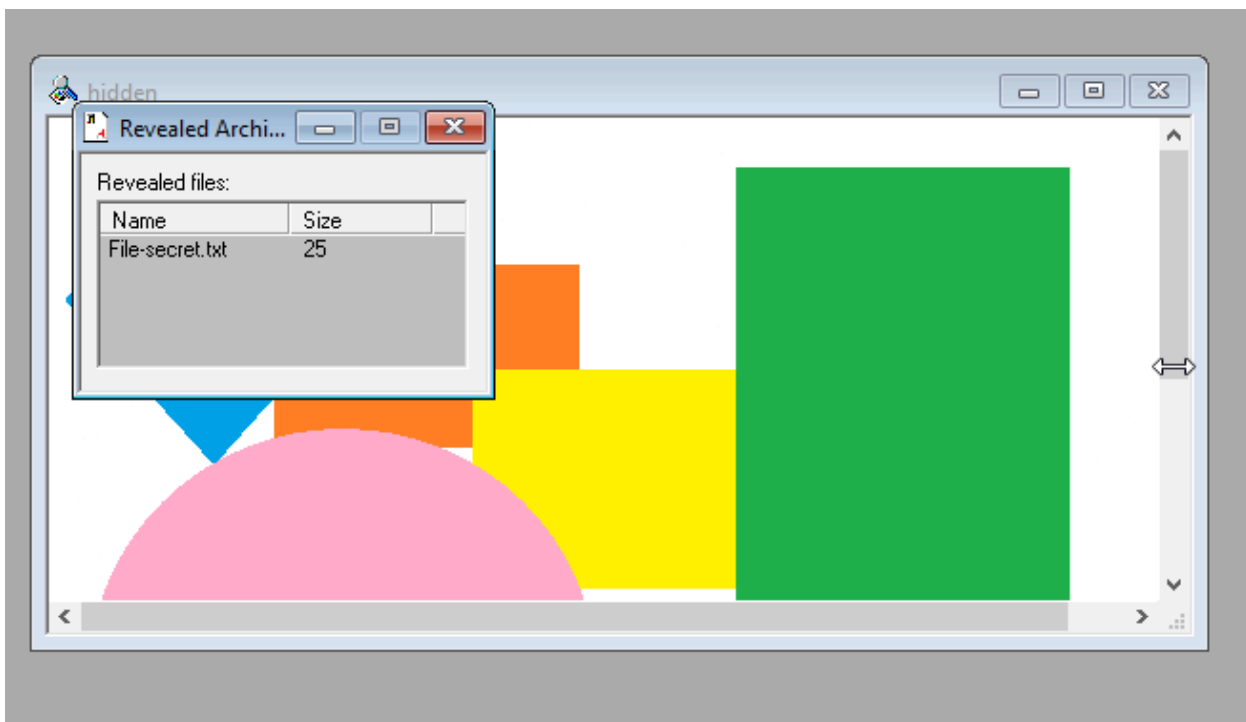
Та збережу файл з прихованими даними



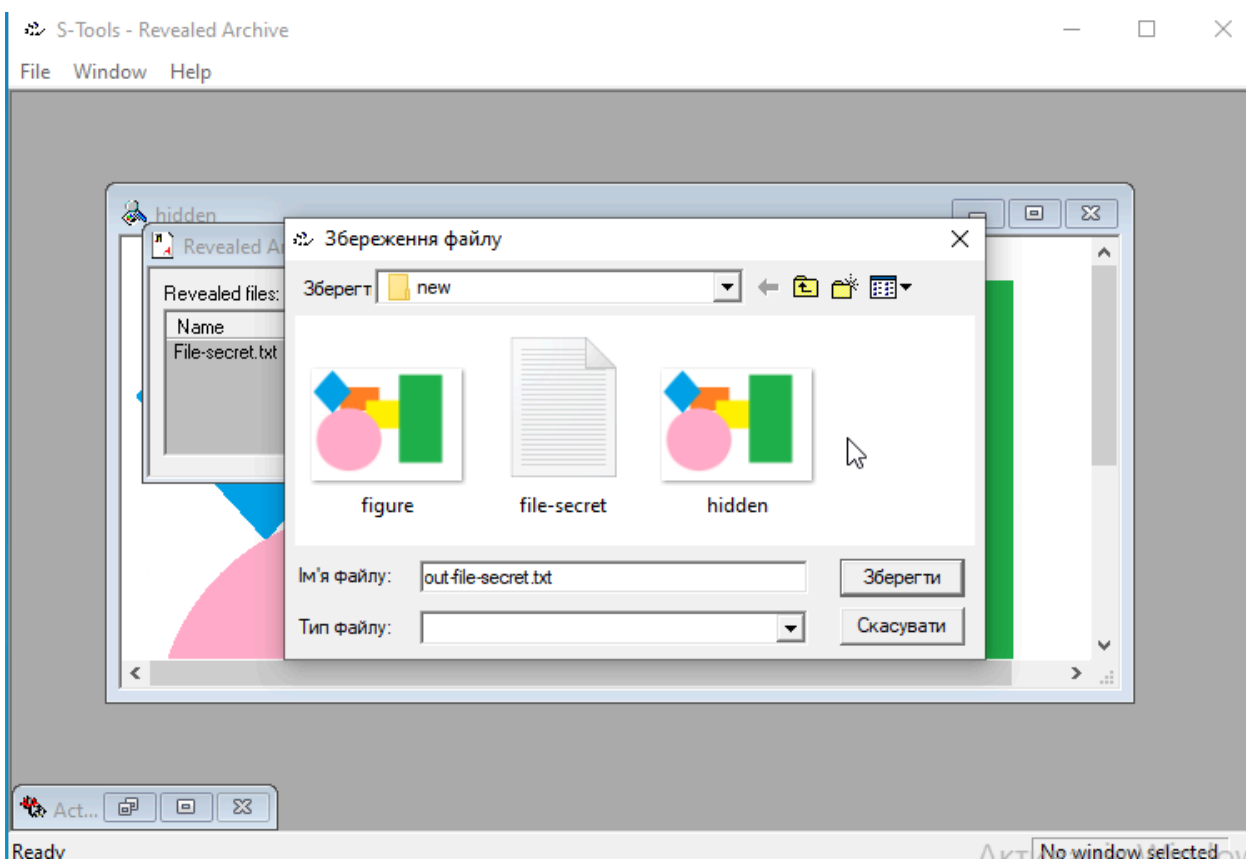
Наступним кроком перевірю прихований файл



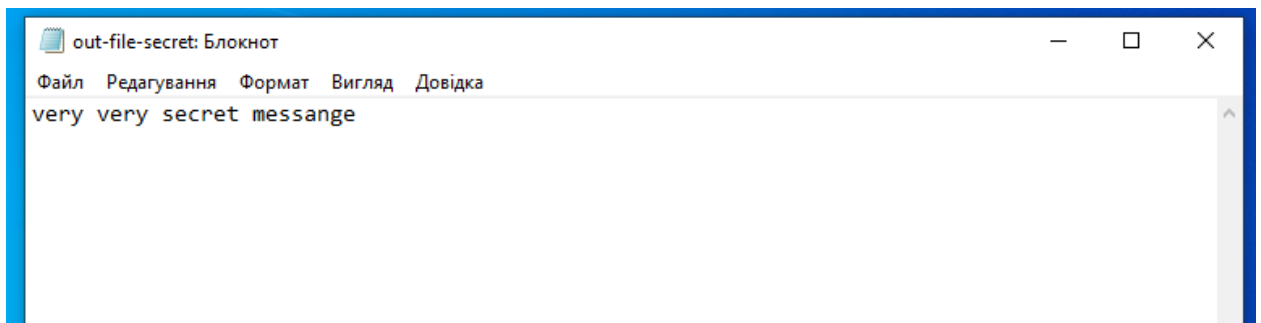
в результаті отримую дані, які були приховані



Й можу зберегти дан, які було отримано

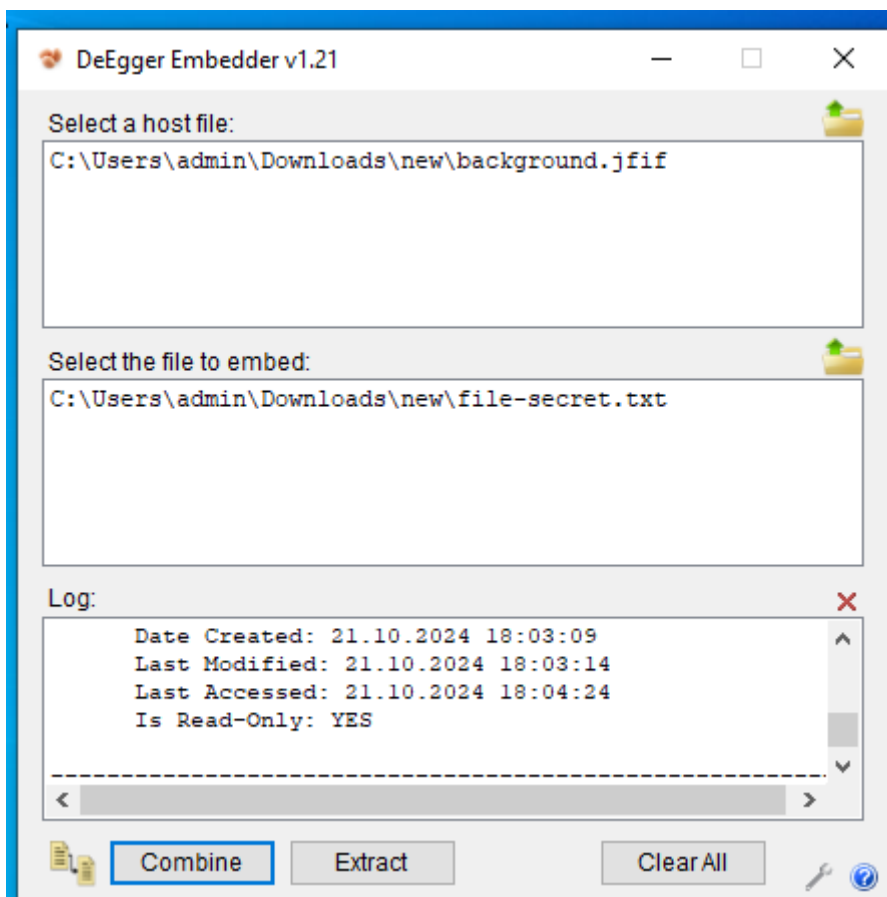


Й відкривши файл можна побачити, що повідомлення таке саме, як й було приховане

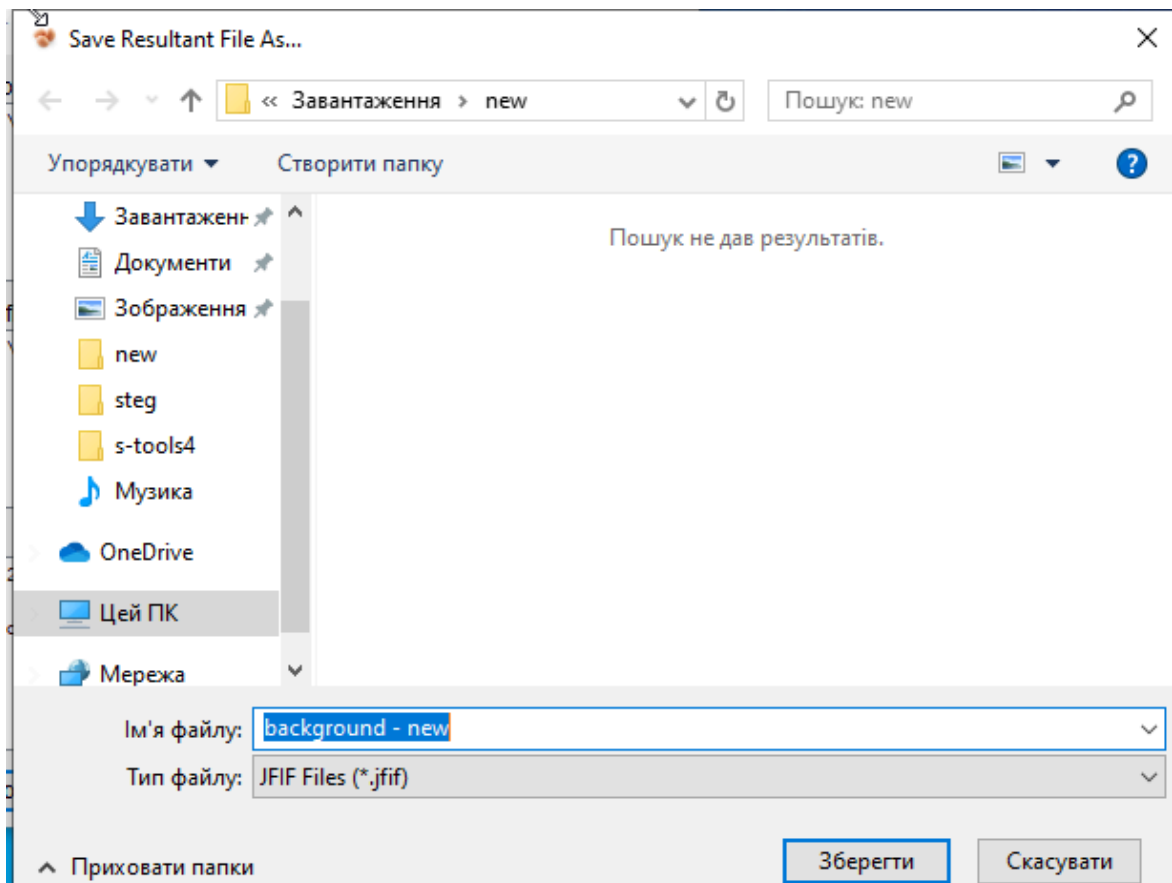


2. DeEgger Embedder

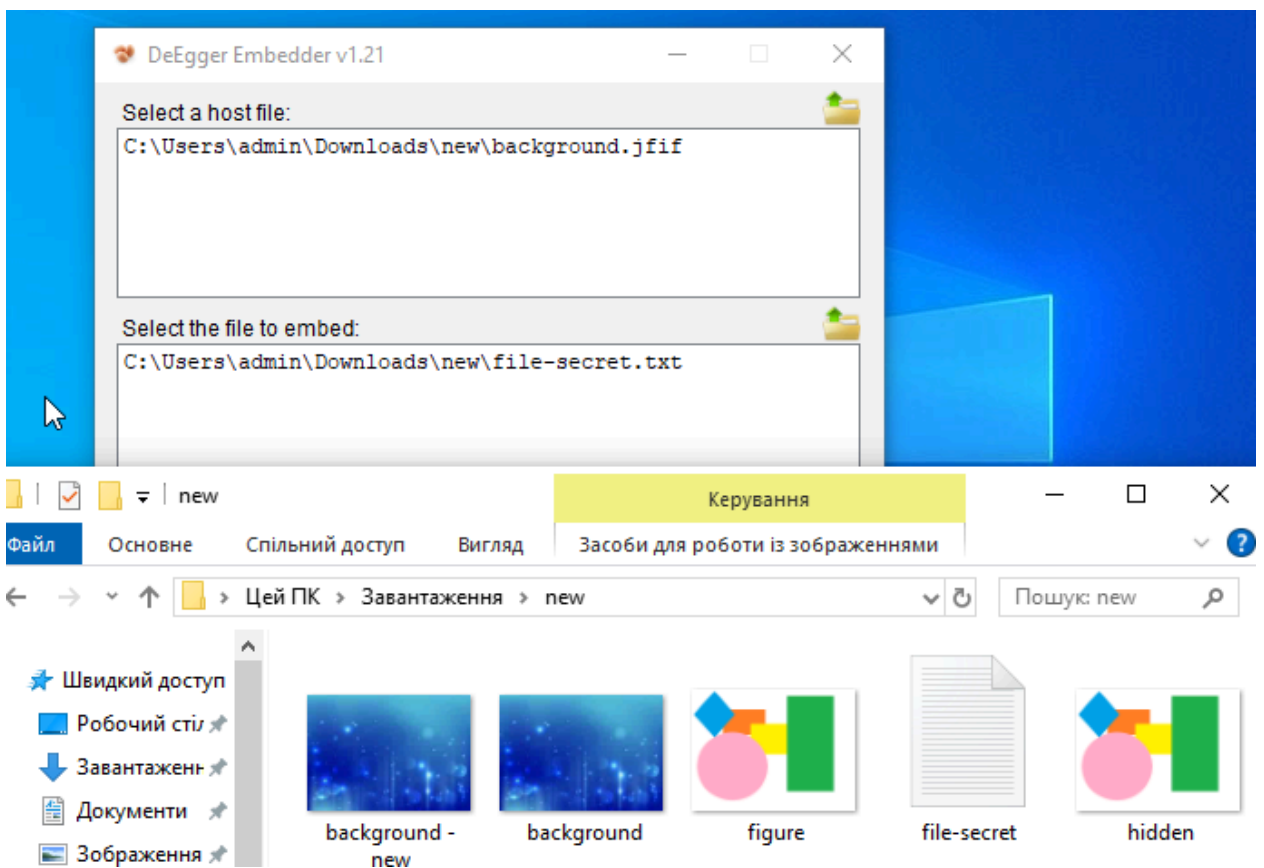
Успішне додавання даних



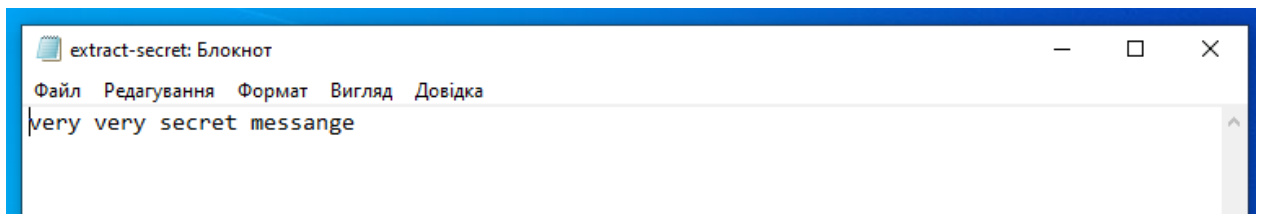
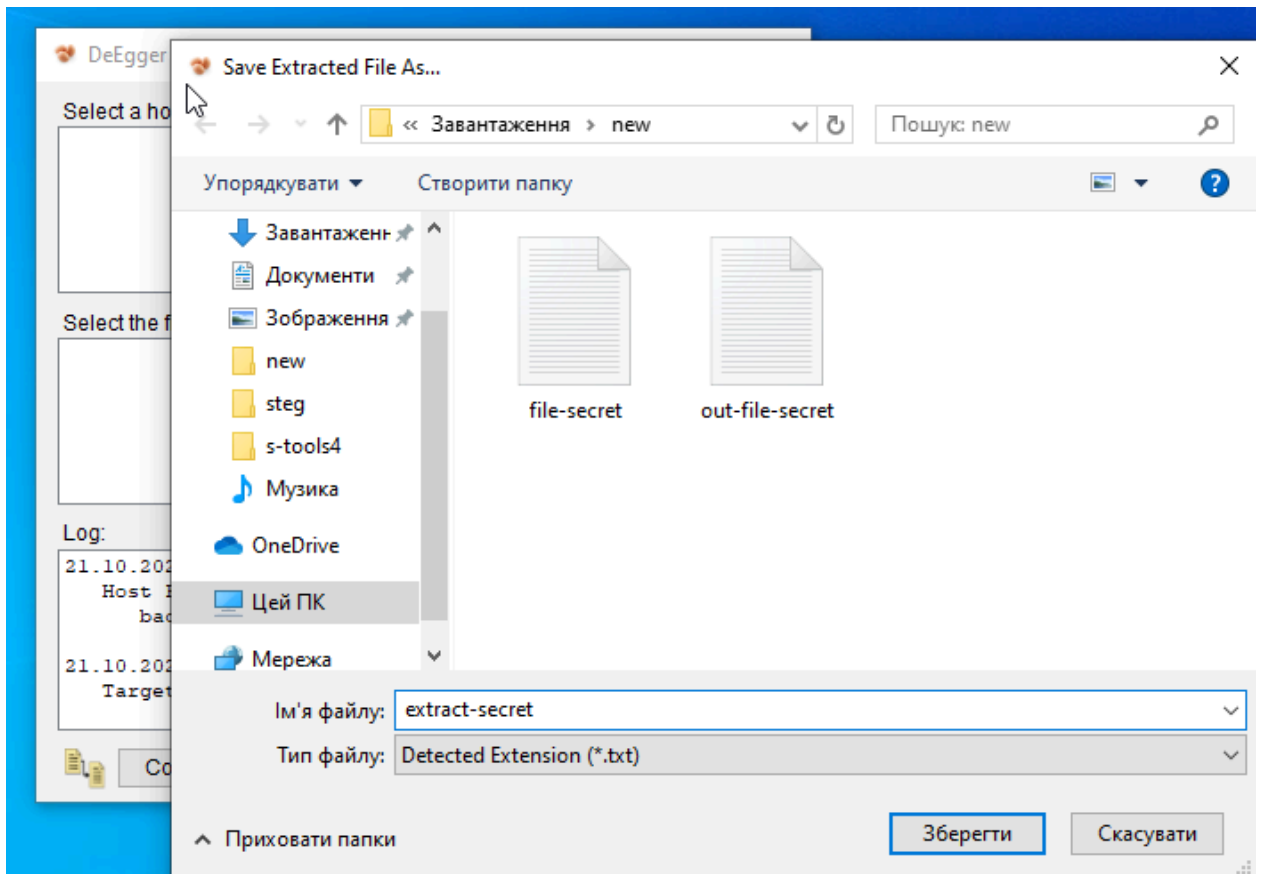
Обираю куди завантажити файл



В результаті файл було створено

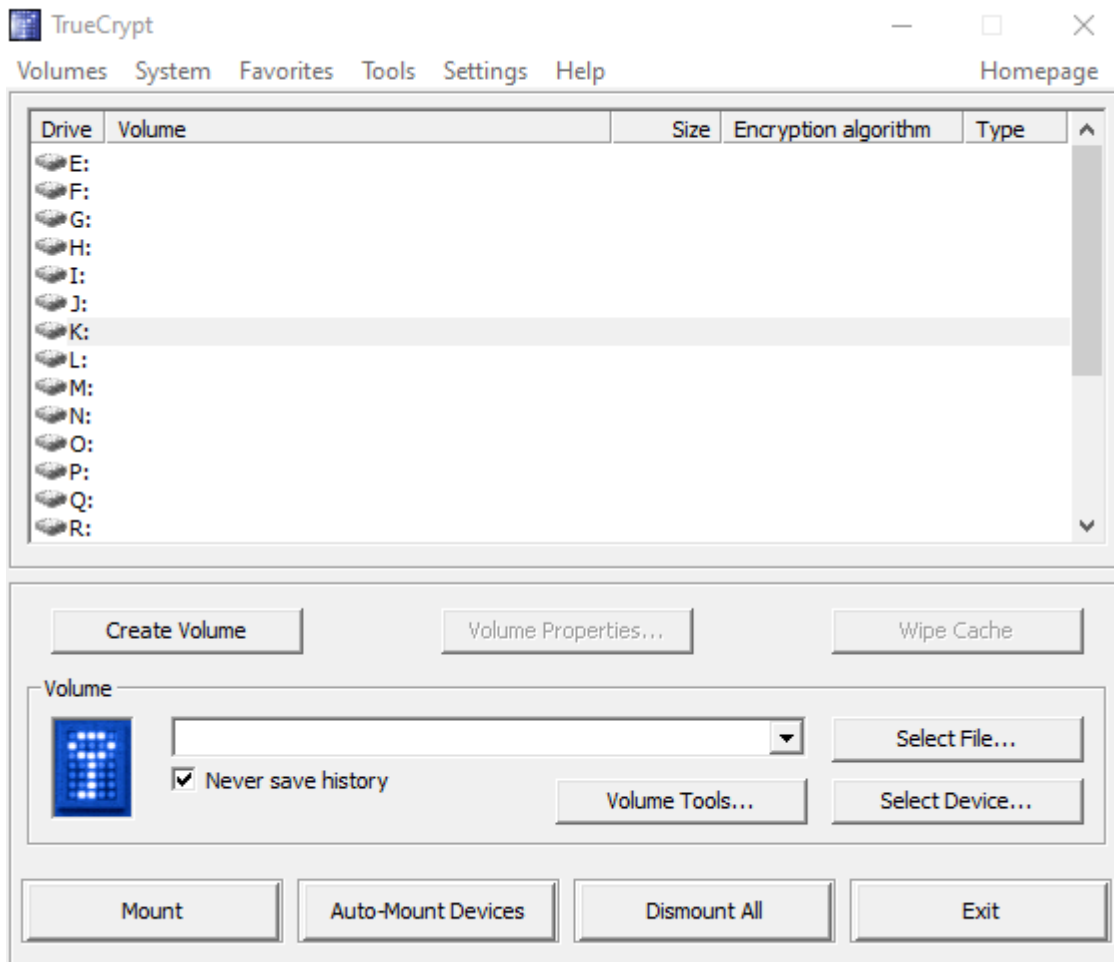


Й при вилученні інформації повідомлення таке саме, як й спочатку

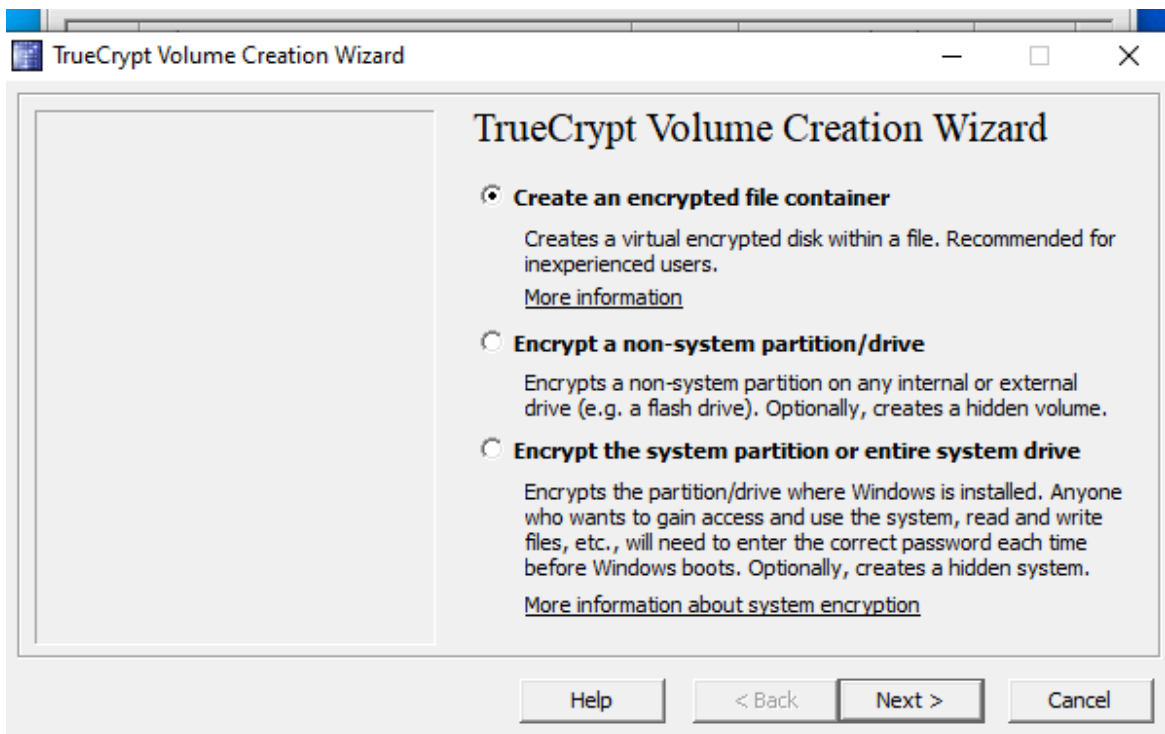


TrueCrypt

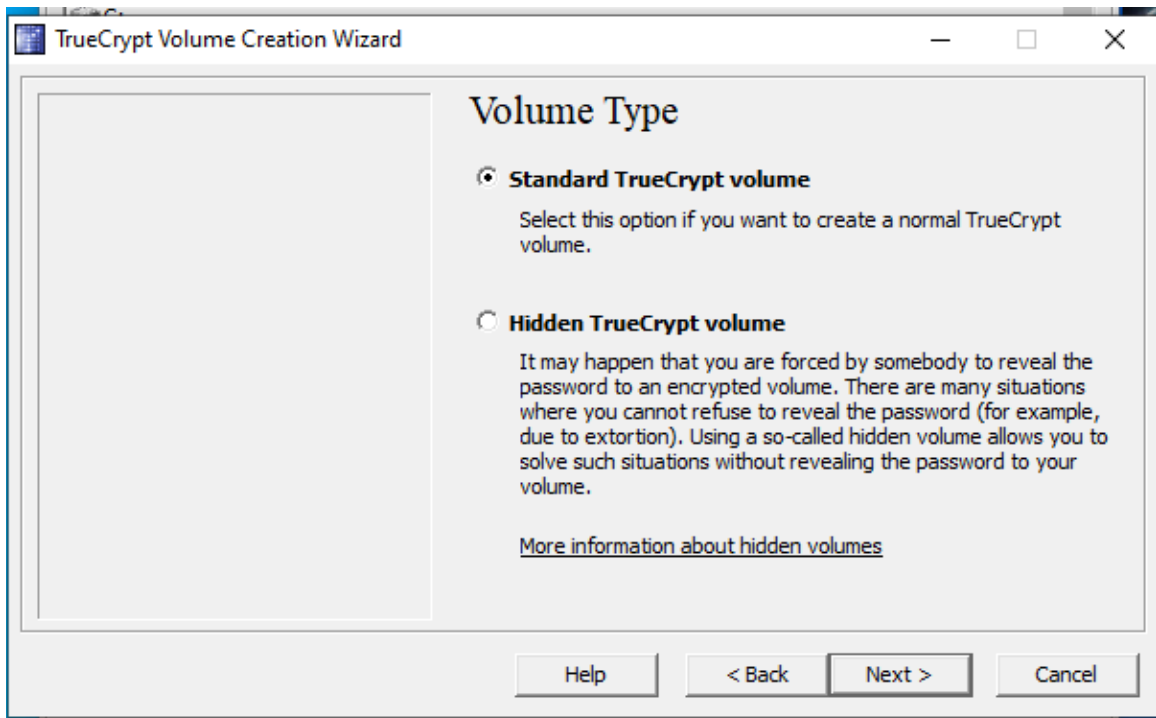
Стартове вікно програми



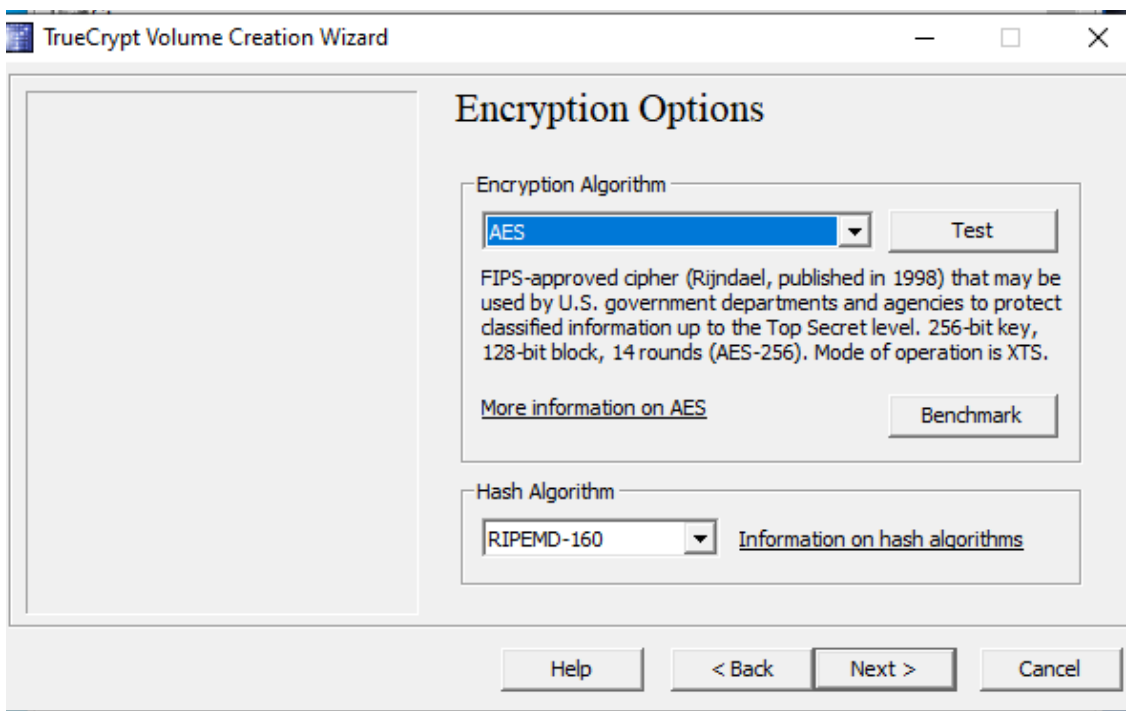
Створю розділ



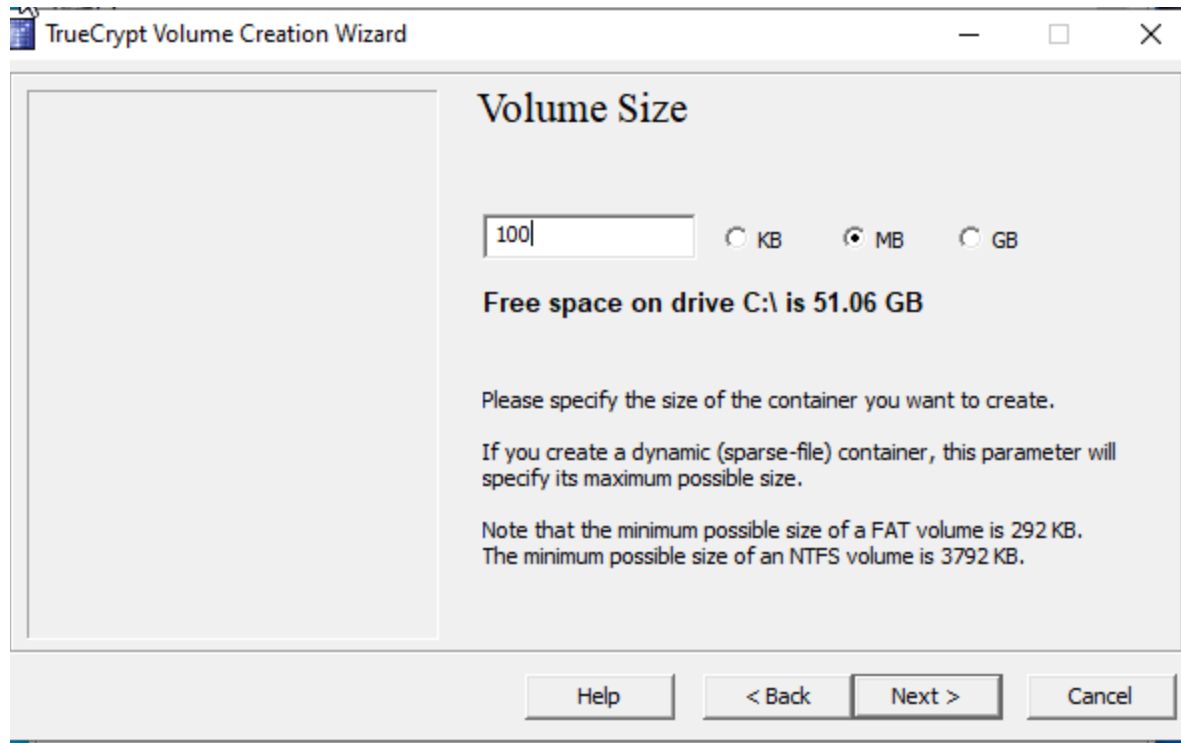
Обиру тип розділу



Обираю тип шифрування



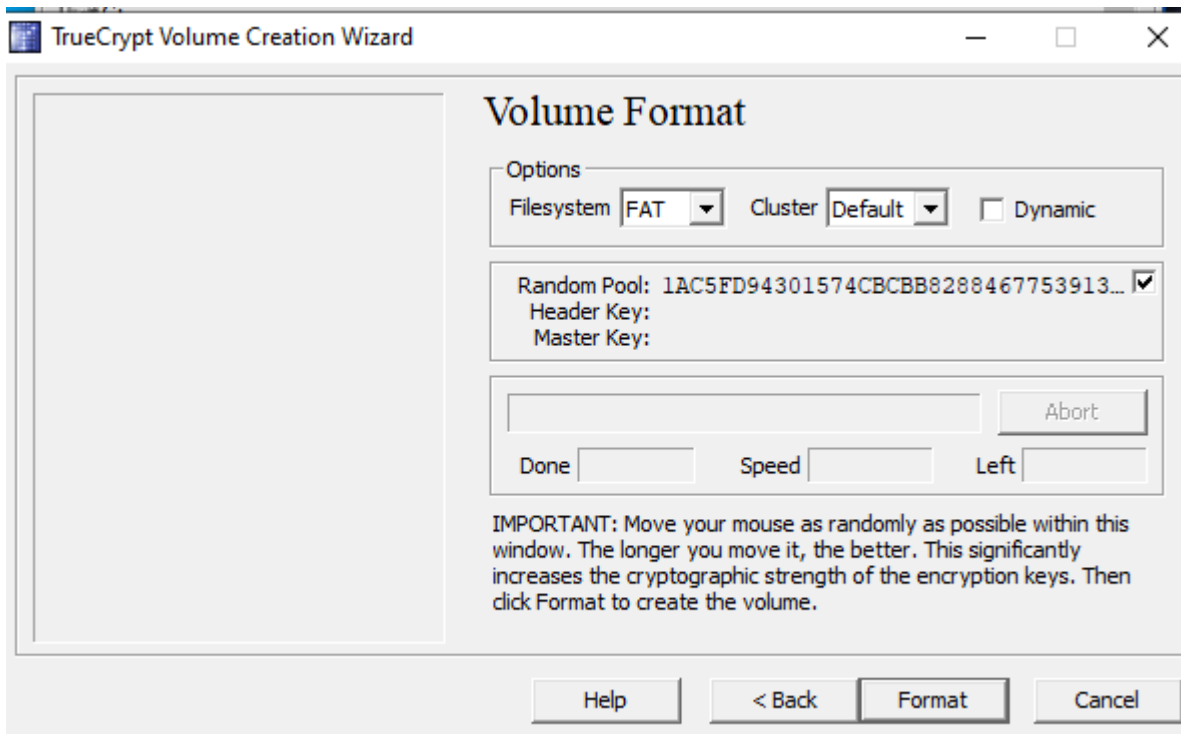
Обираю розмір розділу



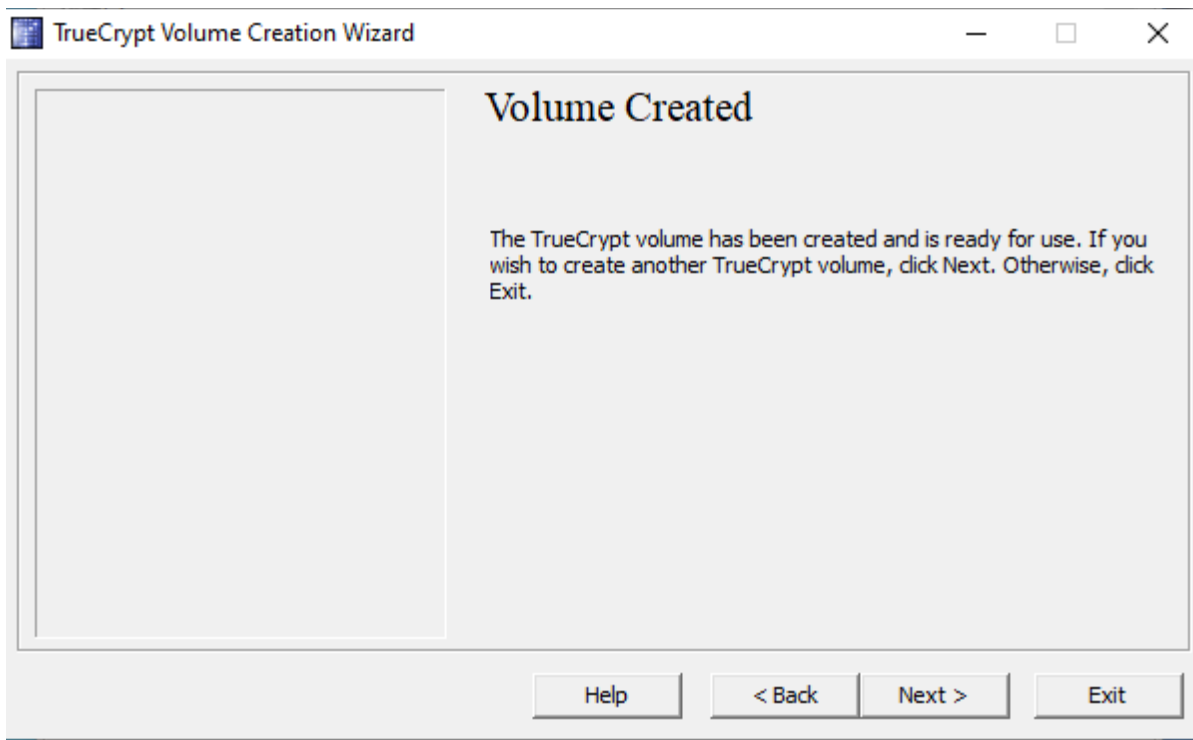
Встановлюю пароль на розділ



Обираю формат розділу



Й в результаті успішне створення розділу

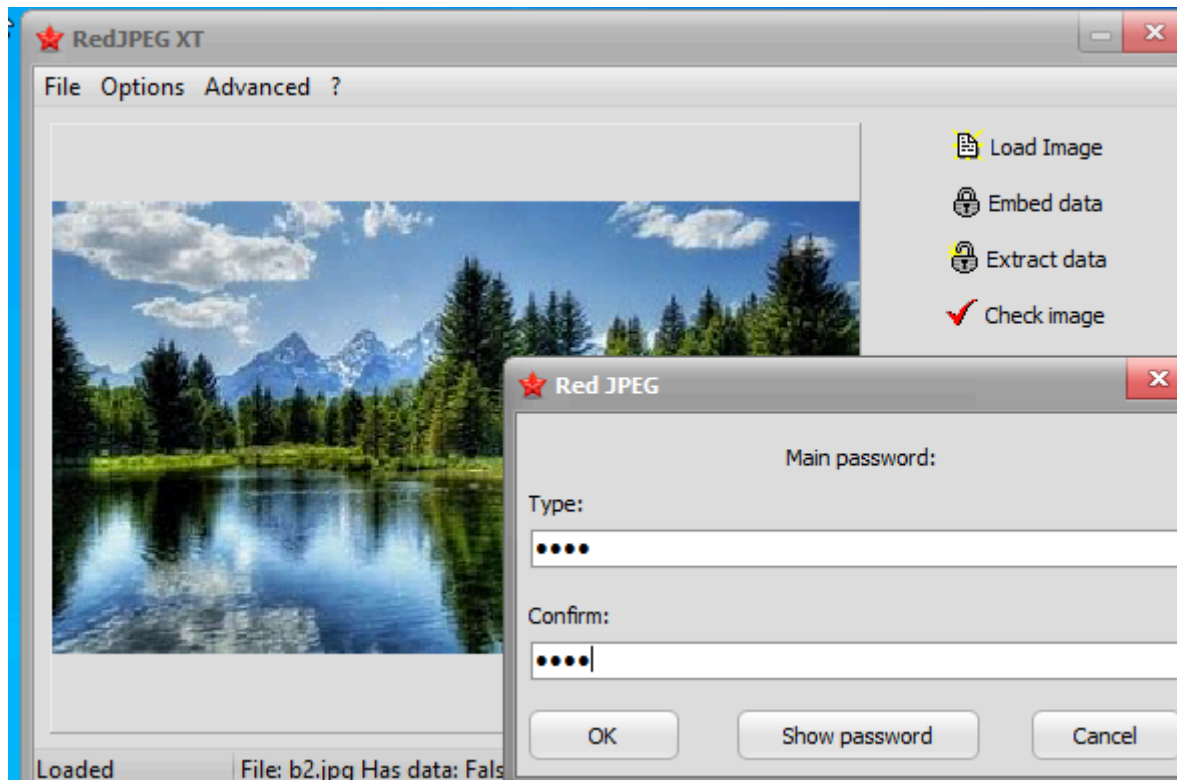


JPHide, JPSeek.

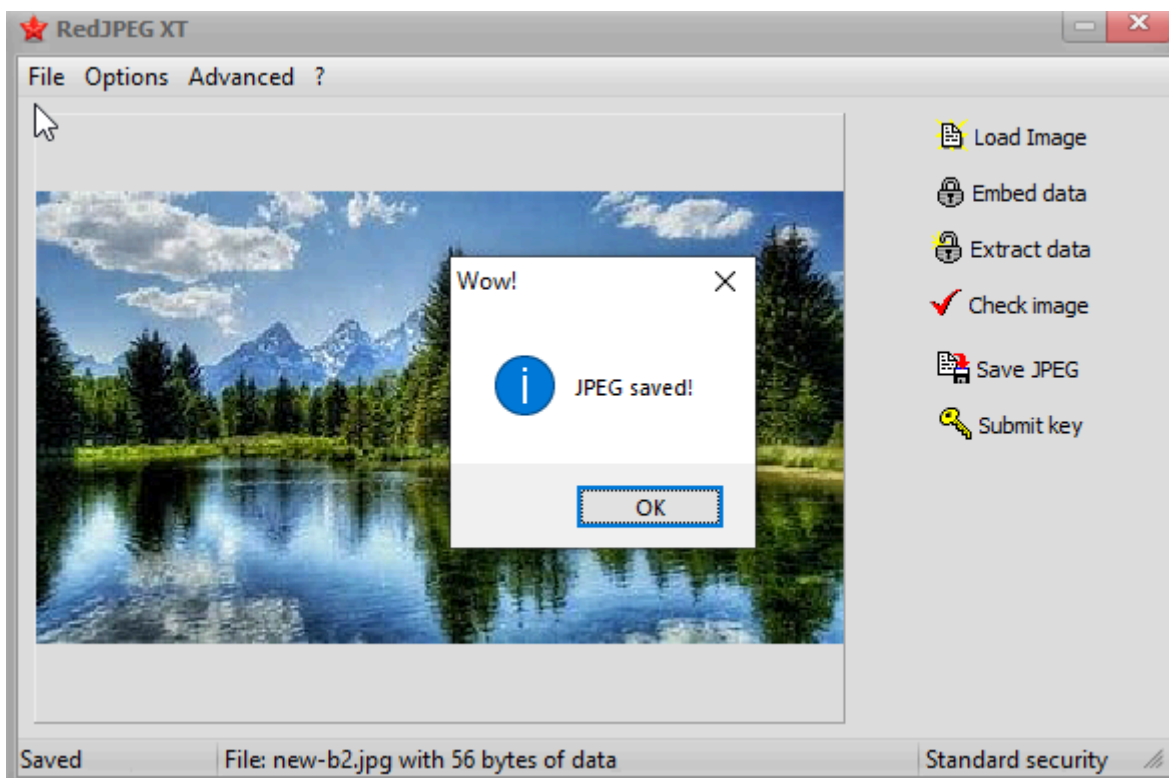
На зараз дані програми застаріли і вже не працюють і перевірка архівів видає, що файли небезпечні, тому робота з даними інструментами не було проведено!

Red JPEG XT

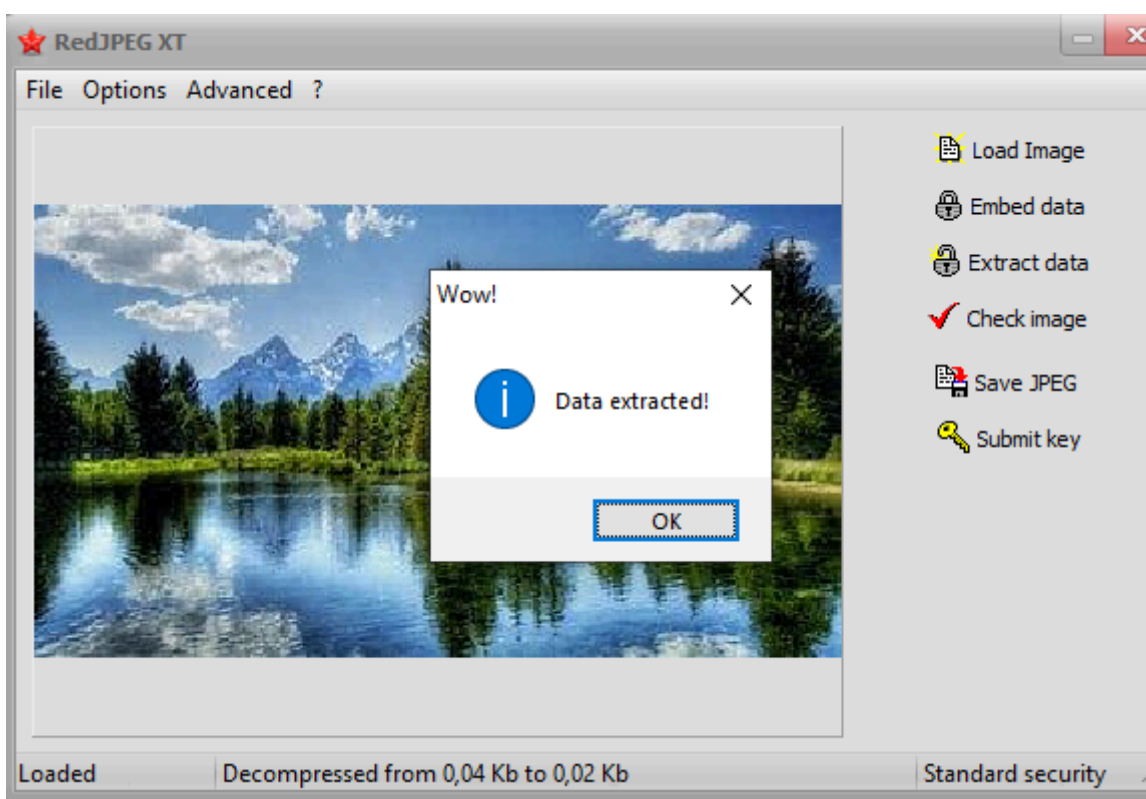
Додам зображення та встановлю пароль



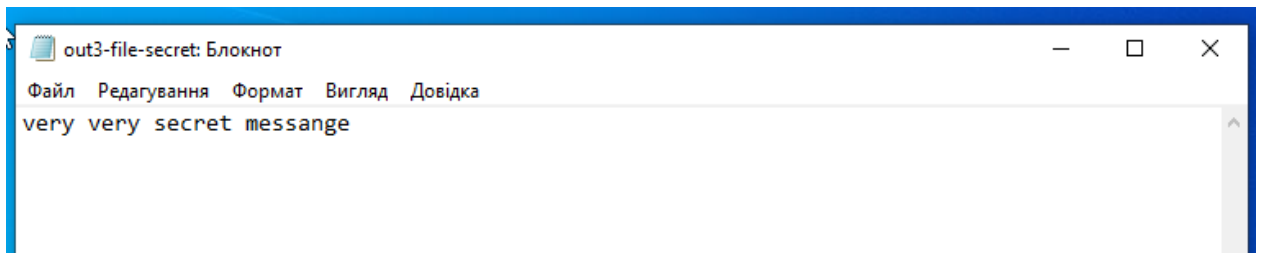
В результаті при прихованні файлу зображення було збережено коректно



Та при вилученні даних також успіх



Вилучені дані



Висновок: В даній лабораторній роботі я ознайомився з поняттям стеганографії, її базовими принципами, використовуваними форматами контейнерів, способами упаковки приховування, найбільш популярними програмами стеганографії