МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки

**Звіт до лабораторної роботи № 13**

на тему “ Дослідження методів цифрової стеганографії ”

Виконав студент(ка) Борщ Дмитро

Група КБ-01

Перевірила Лаврик Т.В

**Суми 2022**

**ЗВІТ 13**

**Завдання і порядок виконання роботи.**

1. Дослідити основні понять цифрової стеганографії та заповнити таблиці.

1.1 Основні поняття:

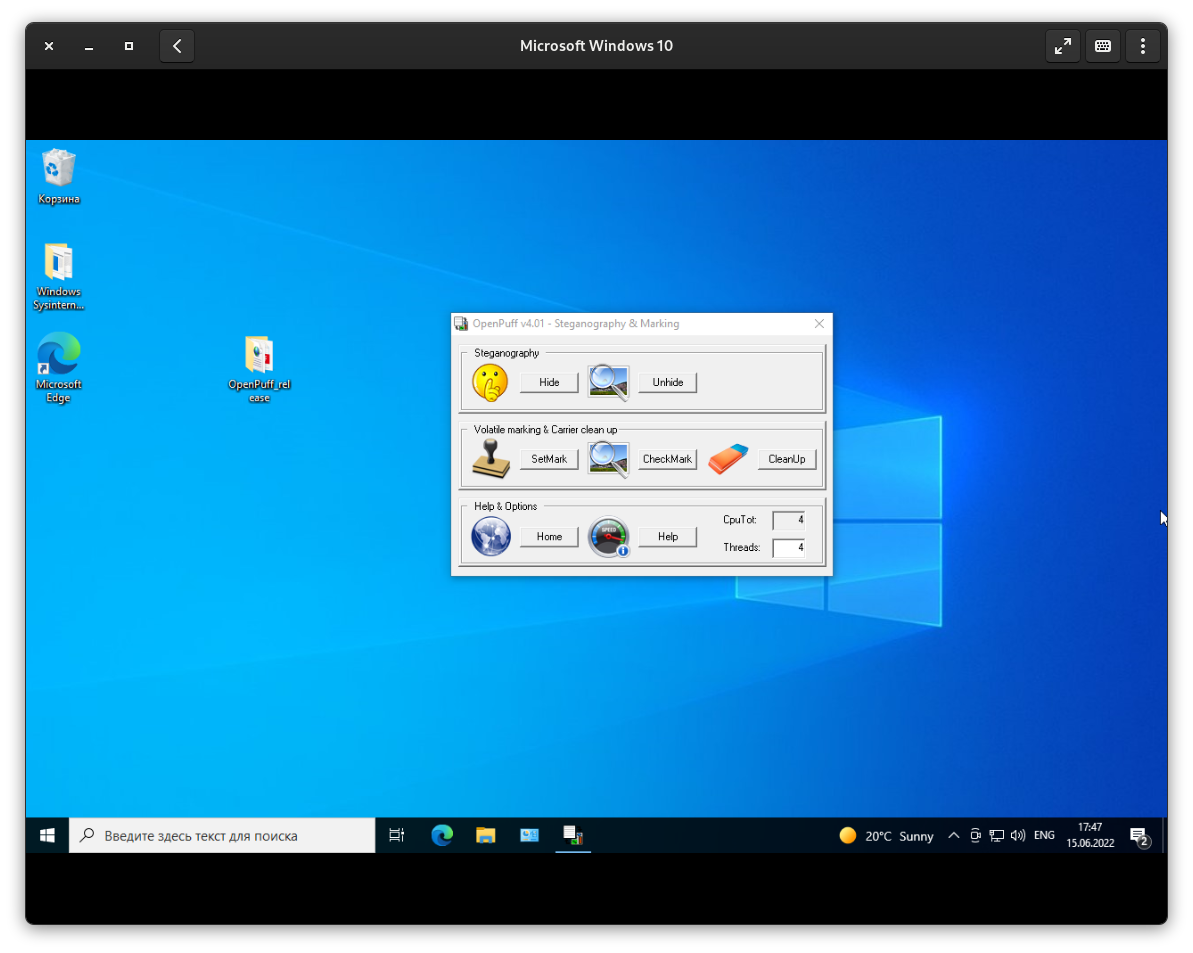
|  |  |
| --- | --- |
| **Контейнер** | будь-яка інформація, яка використовується для приховування таємного повідомлення. |
| **Вбудоване повідомлення** | загальна назва прихованої інформації, що передається, будь то лист з написами молоком, голова раба або цифровий файл. |
| **Стеганографічний канал** | канал передачі стегоконтейнера. |
| **Ключ** | секретний ключ, необхідний приховування стегоконтейнера. Ключі в стегосистемах бувають двох типів: закриті (секретні) та відкриті. Якщо стегосистема використовує закритий ключ, він має бути створено або початку обміну повідомленнями, або переданий по захищеному каналу. Стегосистема, що використовує відкритий ключ, повинна бути влаштована таким чином, щоб неможливо було отримати з нього закритий ключ. У цьому випадку відкритий ключ можна передавати незахищеним каналом. |
| **Види контейнерів** | * Порожній контейнер - контейнер, який не містить секретного послання. * Заповнений контейнер (стегоконтейнер) – контейнер, що містить секретне послання. |

* 1. Методи стеганографії:

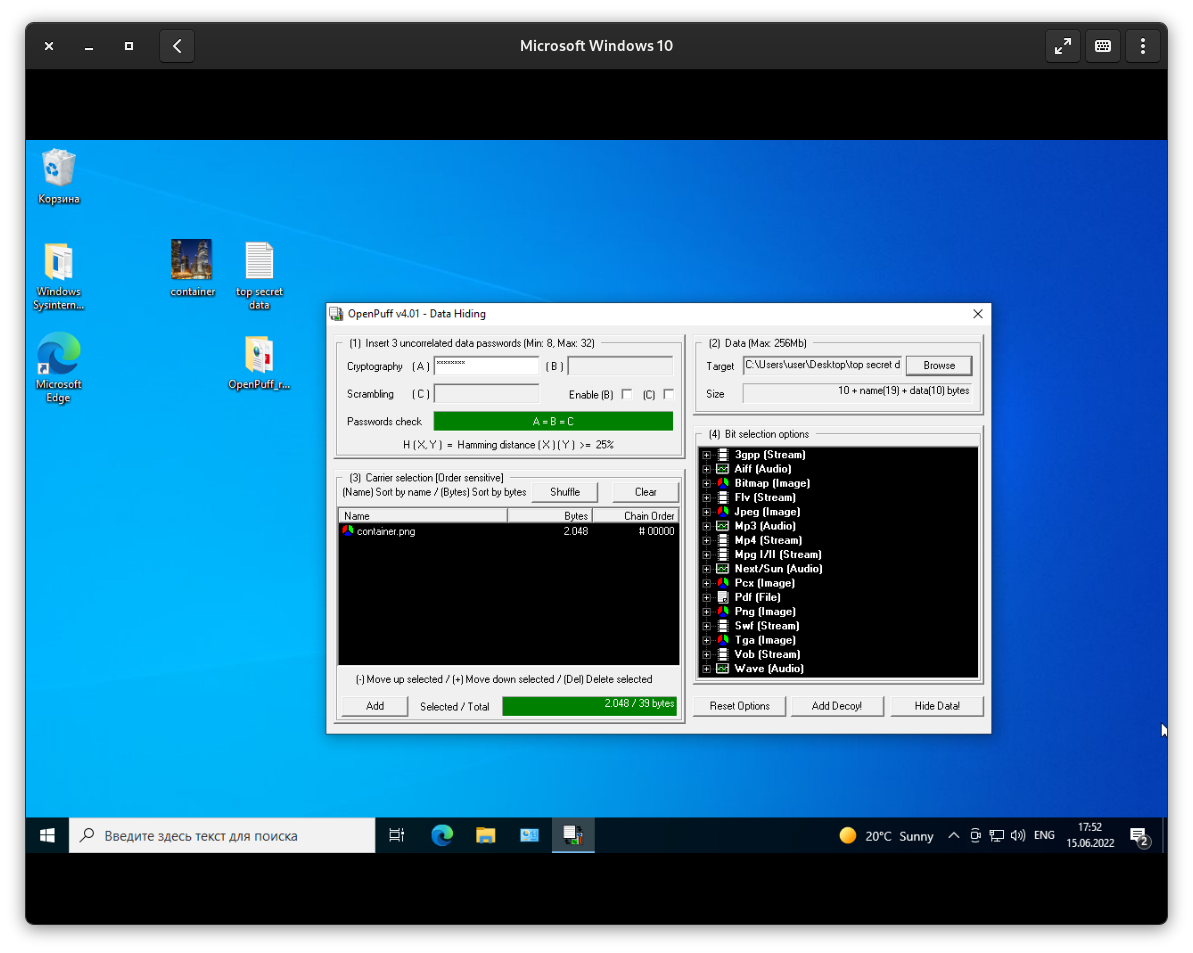
|  |  |  |
| --- | --- | --- |
| № | Назва методу | Короткий опис методу |
| 1. | Метод заміни молодших бітів (Least Significant Bit) | Суть методу полягає у заміні кількох молодших біт у байтах даних. Він застосовується у графічних файлах, що використовують для формування кольору кожного елемента зображення (піксела) значення деяких складових (наприклад, значення складових основних кольорів – червоного, зеленого та синього), або у звукових файлах, що використовують для формування звуку значення дискретизованих амплітуд сигналу. |
| 2. | Метод заміни палітри кольорів. | Метод заснований на використанні специфічних особливостей формату файла-контейнера та призначений для приховування текстової інформації у графічних файлах, що використовують палітри кольорів. |
| 3. | Метод сортування палітри кольорів. | Метод заснований як у використанні особливостей формату контейнера, і на використанні психофізичних особливостей сприйняття кольору людиною. При цьому методі як контейнер використовуються файли з індексованими кольорами, що містять монохромне (зазвичай градації сірого) зображення. Суть методу полягає у спеціальній попередньої підготовці файла-контейнера. |
| 4. | Методи комп'ютерної стеганографії у JPEG-файлах. | Кольорові зображення, представлені у цифровій формі, досить великі і займають великий обсяг пам'яті (до кількох мегабайт). Тому для їх стиснення існує низка методів. Так, формати BMP та GIF використовують алгоритми стиснення без втрат, що забезпечують точне відновлення вихідного зображення. |
| 5. | Комп'ютерна стеганографія у PRN-файлах. | Файли друку кольорових графічних зображень на принтерах, що підтримують точковий вивід, містять опис бітової картки відбитка. Процедура друку передбачає отримання бітових карт відбитків, кодування їх мовою керування принтером (PRN-файли) та пересилання на принтер для безпосереднього отримання відбитка. В цьому випадку як контейнер стегосистеми може бути використана бітова карта відбитка. |

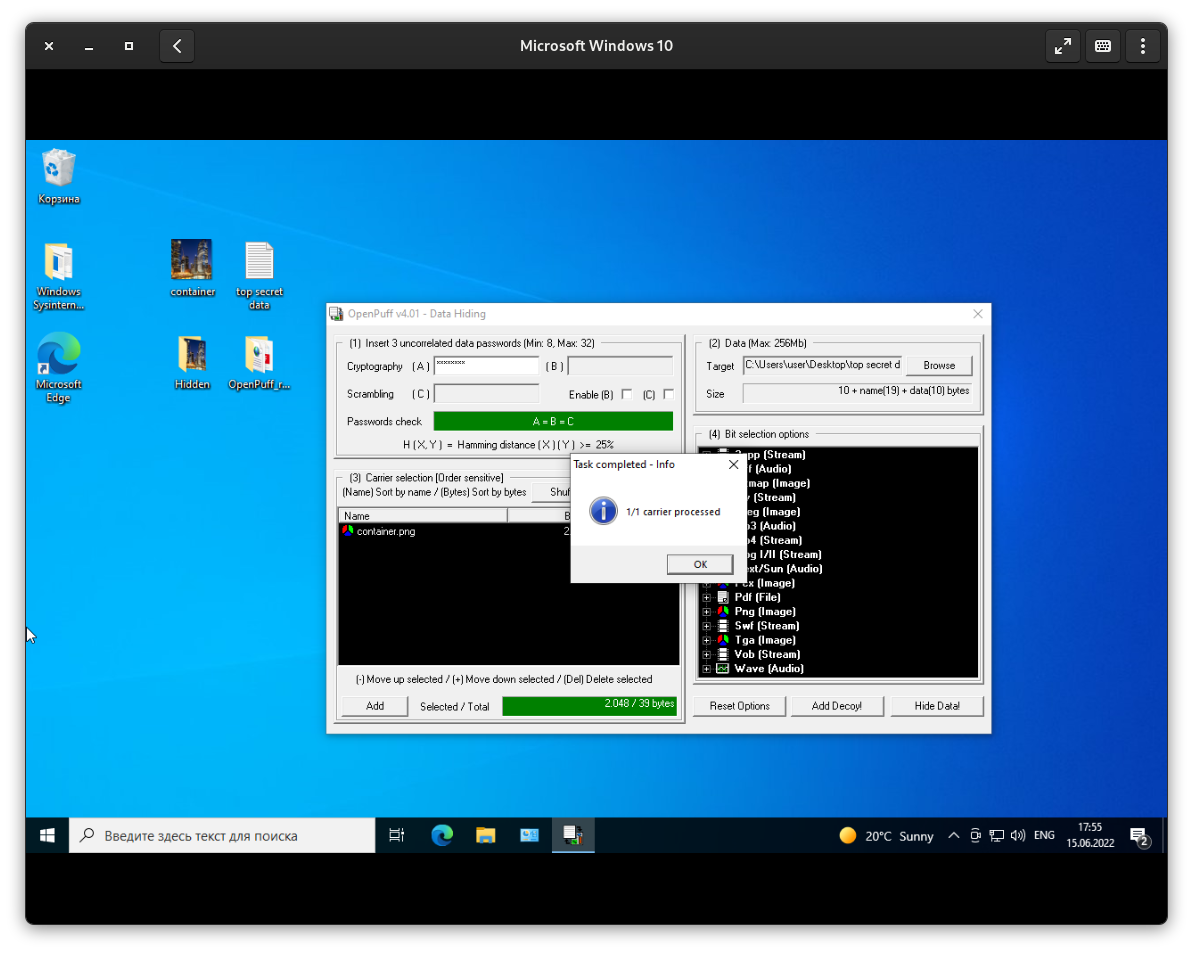
1. Результати роботи з програмою OpenPuff.

***Примітка:*** Усі дії, що виконуються, у звіті мають супроводжуватися скріншотами і текстовими поясненнями.

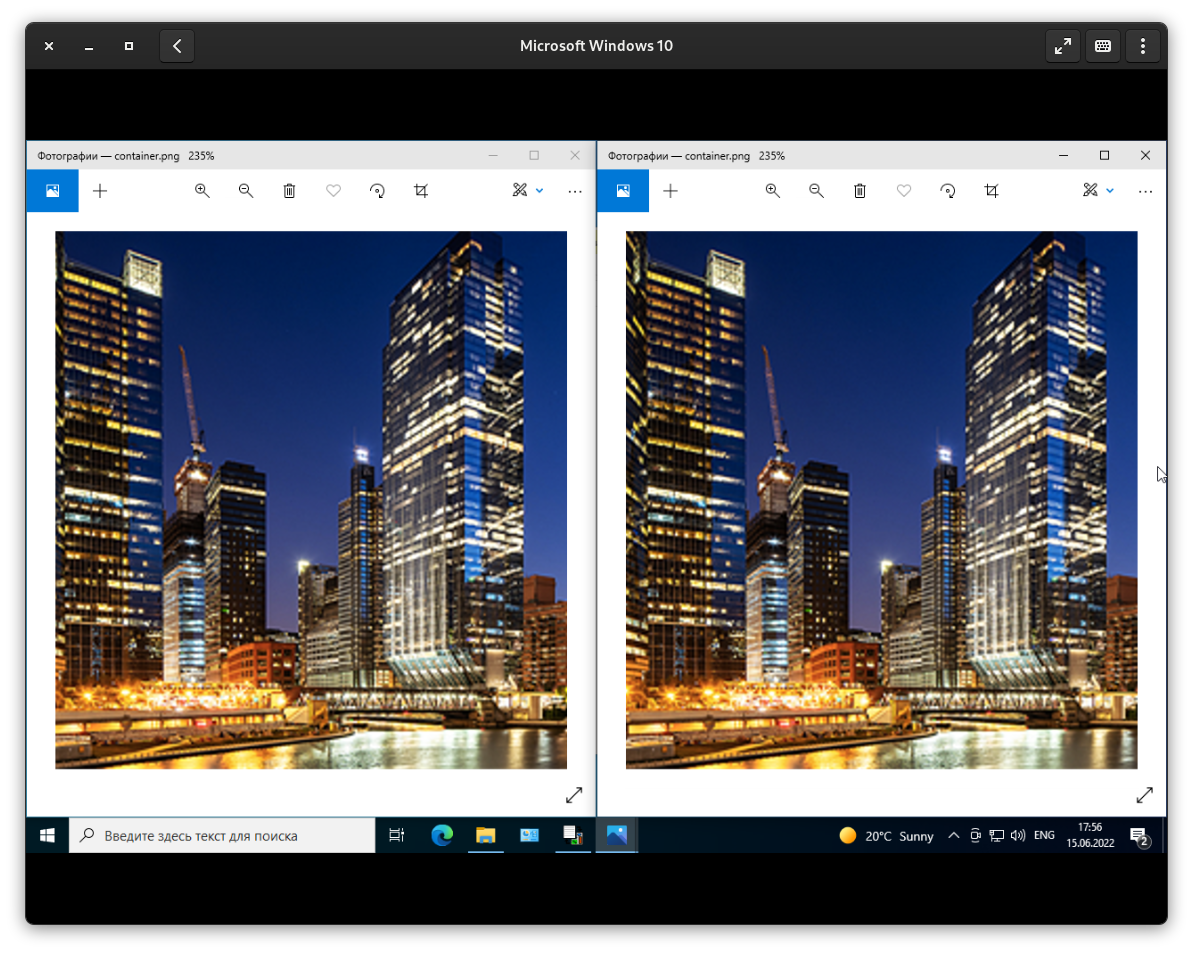
Рис. 1 — Інтерфейс програми OpenPuff.

Проведемо приховування даних за допомогою OpenPuff. За методичними вказівками обираємо пароль, файл-контейнер, та файл-ціль.

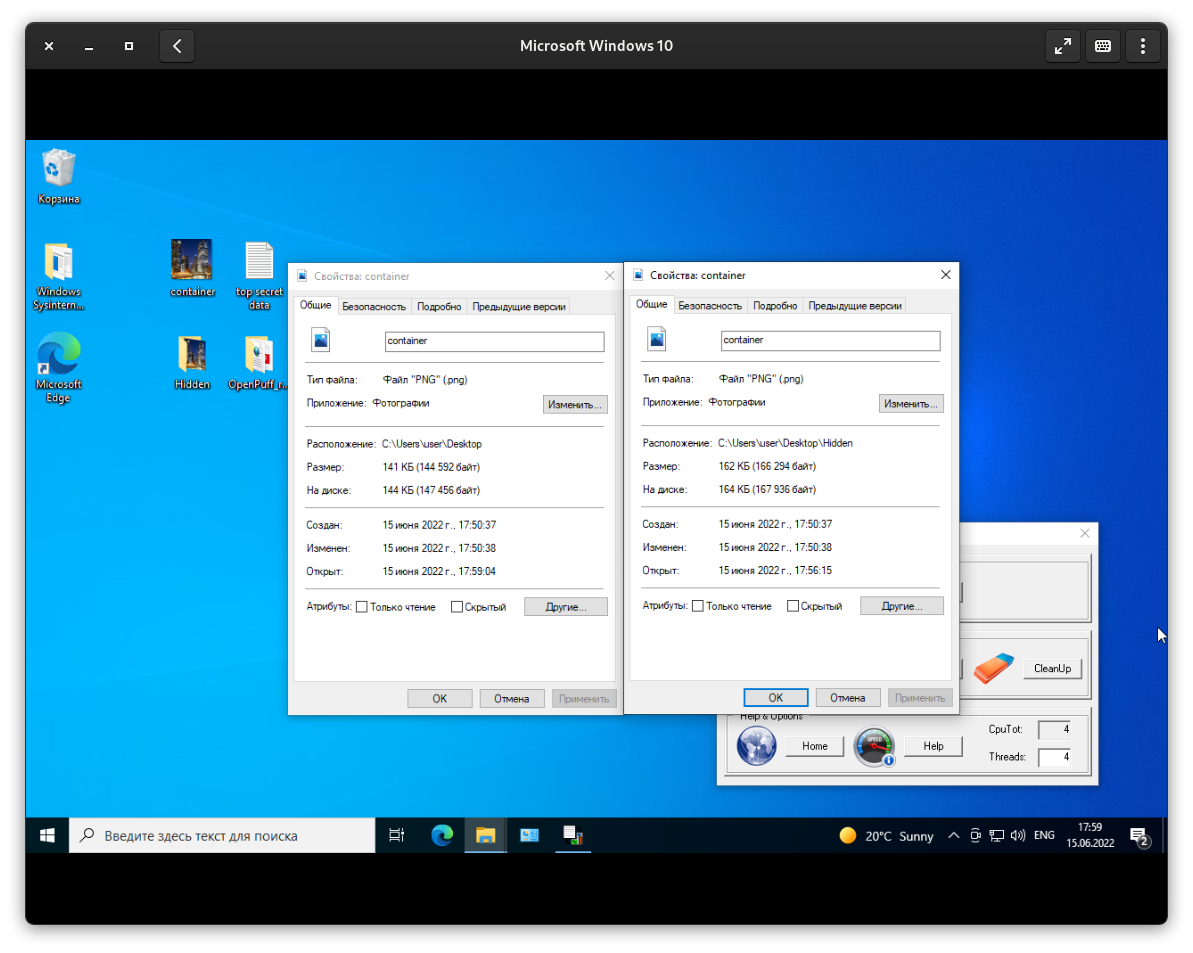
Рис. 2 — Обрані необхідні параметри для програми OpenPuff.

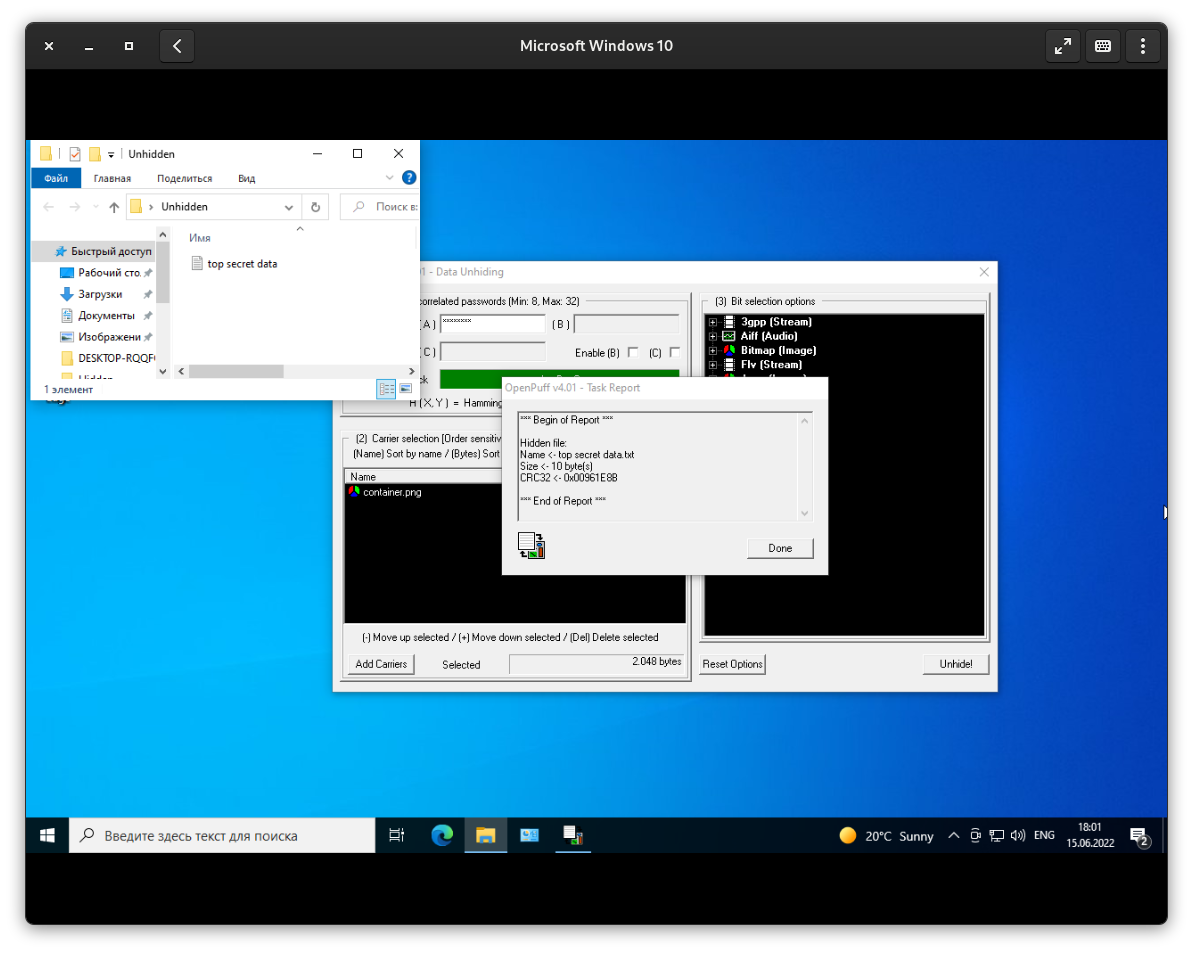
Рис. 3 — Успішне приховування даних.

Так як обсяг інформації був досить не великий, то візуально абослютно не можливо знайти присутність певної інформації на зображенні.

Рис. 4 — Порівняння початкового контейнеру та стегоконтейнеру.

Помітне лише незначне збільшення розміру файлу.

Рис. 5 — Порівняння початкового файлу-контейнеру та стегоконтейнеру.

Рис. 6 — Успішне вилучення файлу зі стегоконтейнеру.

***Висновки.***

Зробіть висновок. Надайте відповіді на такі питання:

1) Які типи файлів можуть виступати у якості контейнерів?

*У якості контейнерів можуть бути використані файли будь-яких типів. Потрібно лише щоб їх розмір дозволяв приховати необхідну кількість інформації.*

2) Чи може обсяг прихованого файлу перевищувати обсяг контейнеру?

*Такий алгоритм можливо реалізувати, але це буде небезпечно.*

3) У чому відмінність стеганографічних методів захисту від криптографічних?

*На відміну від криптографії, стеганографія займається приховуванням факту передачі інформації, а не захистом самого повідомлення.*