**ЛАБОРАТОРНА РОБОТА №1**

**Мета роботи:**

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

**1.Робота з S-Tools**

Програма S-Tools дозволяє шифрувати і ховати файли в будь-які файли зображень формату GIF і BMP, а також в аудіозаписи формату WAV. При цьому, працездатність файлів, використовуваних в якості контейнера, зберігається. Тобто, фотографії із захованими в них даними будуть відкриватися комп'ютером, як ні в чому не бувало, аудіозаписи-контейнери також будуть відтворюватися.

Позитивним моментом є також і те, що S-Tools не вимагає установки (портативна програма).

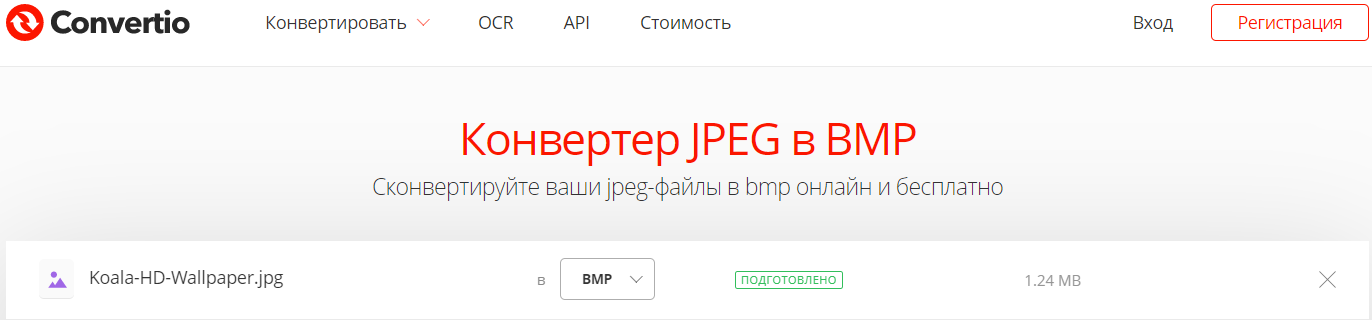
Але використовувати її в повсякденному житті все-таки не дуже зручно. Найбільшим мінусом цього способу захисту даних є те, що використовувані в якості контейнерів файли є не більшими. Відповідно, заховати в них багато інформації неможливо.

Програму S-Tools можна використовувати для надійного захисту якогось невеликого текстового файлу, наприклад, файлу з паролями або інший схожою інформацією.

*Як користуватися S-Tools*

1. Упаковка файлу

Спочатку потрібно приготувати майбутній контейнер - зображення форматів GIF, BMP або аудіофайл формату WAV. Це не найпоширеніші формати. Якщо в наявності таких бракуватиме - потрібно переконвертувати в них файли інших форматів.Якщо ви не знайшли файл потрібного формату ви завжди можете конвертувати зображення будь-якого формату за допомогою онлайн сервісів



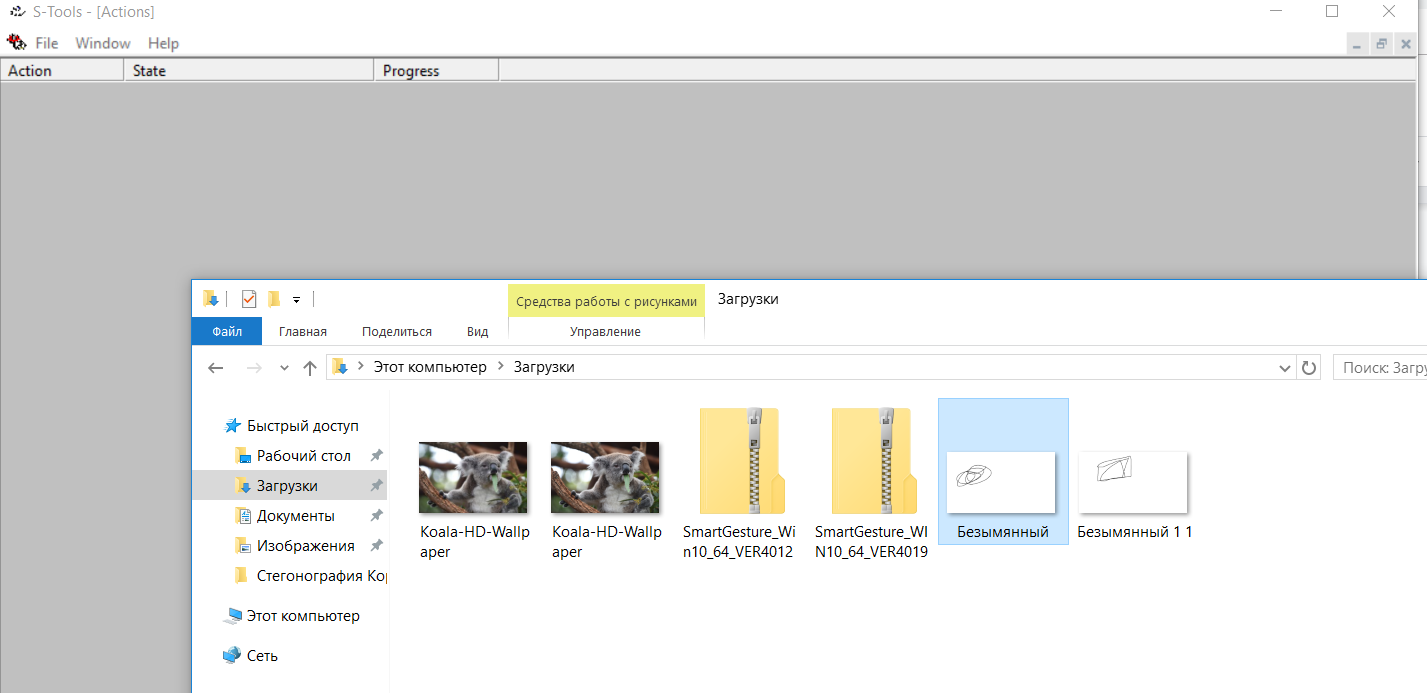
Запускаємо S-Tools. Перетягуємо мишкою файл-контейнер у вікно утиліти. Там цей файл відкриється у вигляді окремого вікна. У це вікно таким же чином перетягуємо файл, який потрібно сховати. Через кілька секунд S-Tools запропонує ввести пароль і вибрати метод шифрування. Вводимо пароль в поле «Passphrase» і повторюємо його в поле «Verify Passphrase». Тиснемо кнопку ОК. Через деякий час у вікні S-Tools з'явиться ще одне вікно з назвою hidden ... Це і є вже упакований контейнер. Для збереження результатів потрібно клацнути по цьому вікну правою кнопкою мишки, в контекстному меню, яке відкриється, вибрати пункт Save as ..., вказати куди зберегти файл, його ім'я і натиснути кнопку «Зберегти».

Буває, що S-Tools під час збереження результатів «з'їдає» розширення файлу. Якщо створений контейнер комп'ютером автоматично не розпізнає як зображення або аудіофайл, розширення потрібно дописати вручну - клацаємо правою кнопкою мишки по файлу, в контекстному меню вибираємо «перейменувати» і в кінці назви файлу додаємо .bmp, .gif або .wav (в залежності від того , який тип файлу використовувався в якості контейнера).

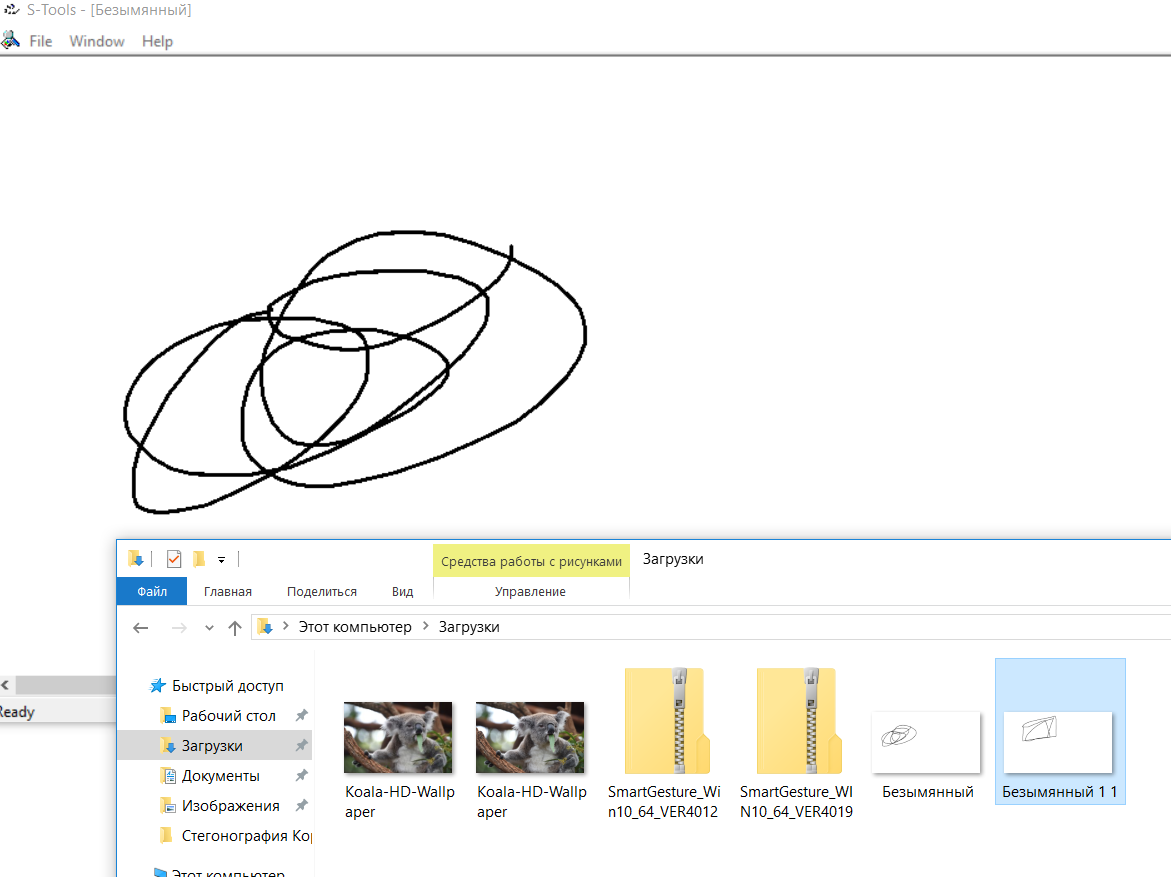
2. Витяг файлу

Запускаємо S-Tools, мишкою перетягуємо в вікно утиліти файл-контейнер. Відкриється вікно цього файлу. Клацаємо по ньому правою кнопкою мишки, в контекстному меню вибираємо Reveal ... Потім вводимо пароль і метод шифрування, зазначені при упаковці, тиснемо ОК. Відкриється ще одне вікно з назвою «Revealed Archive», в якому буде відображатися захований файл. Клік правою кнопкою мишки по цьому файлу, вибираємо пункт «Save as», вказуємо куди витягти файл, тиснемо «Зберегти».

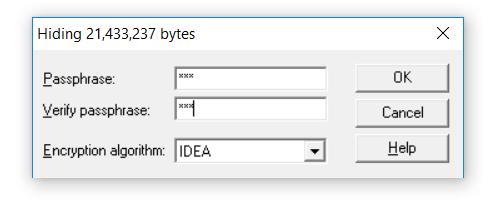
Обираємо файл-контейнер



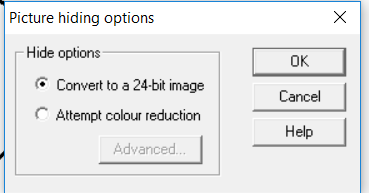
Перетягуємо файл призначений для приховування на вікно.

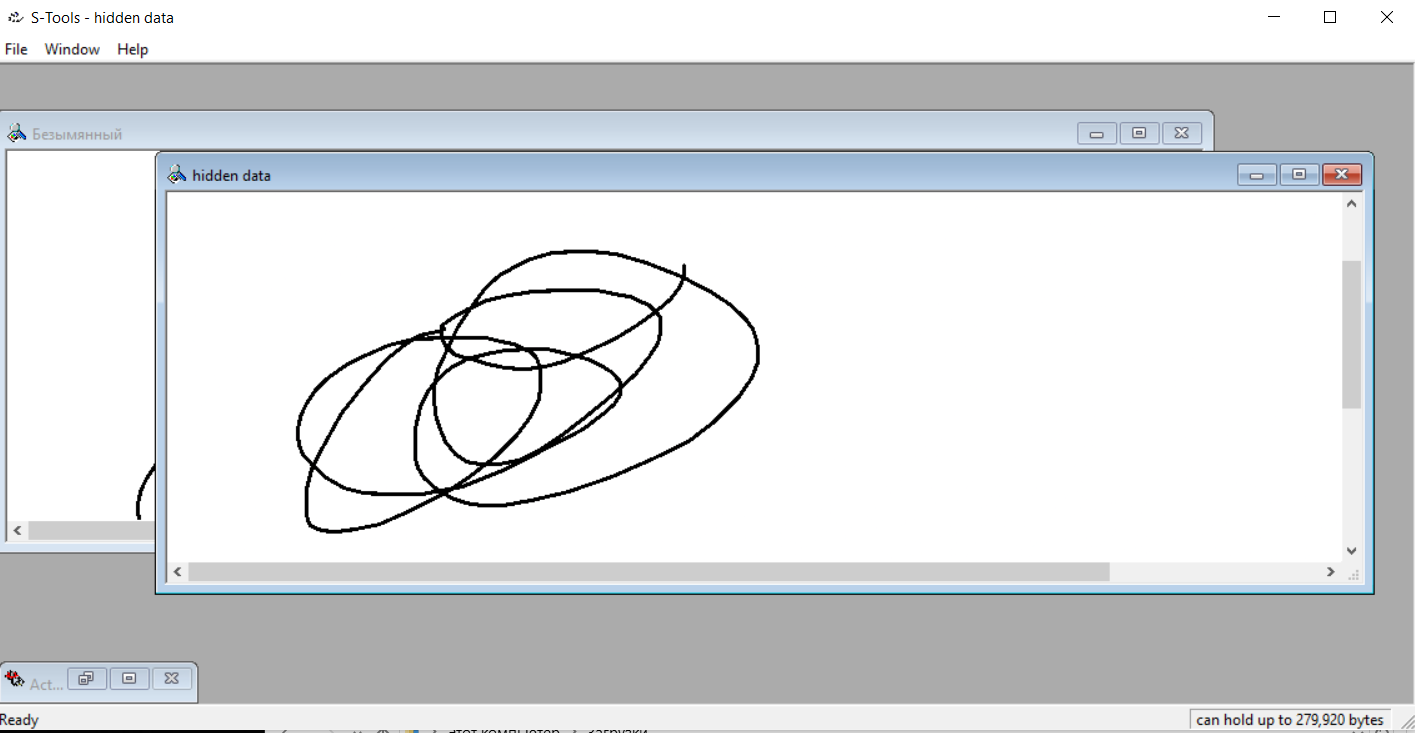


Вводимо пароль і вибираємо алгоритм шифрування

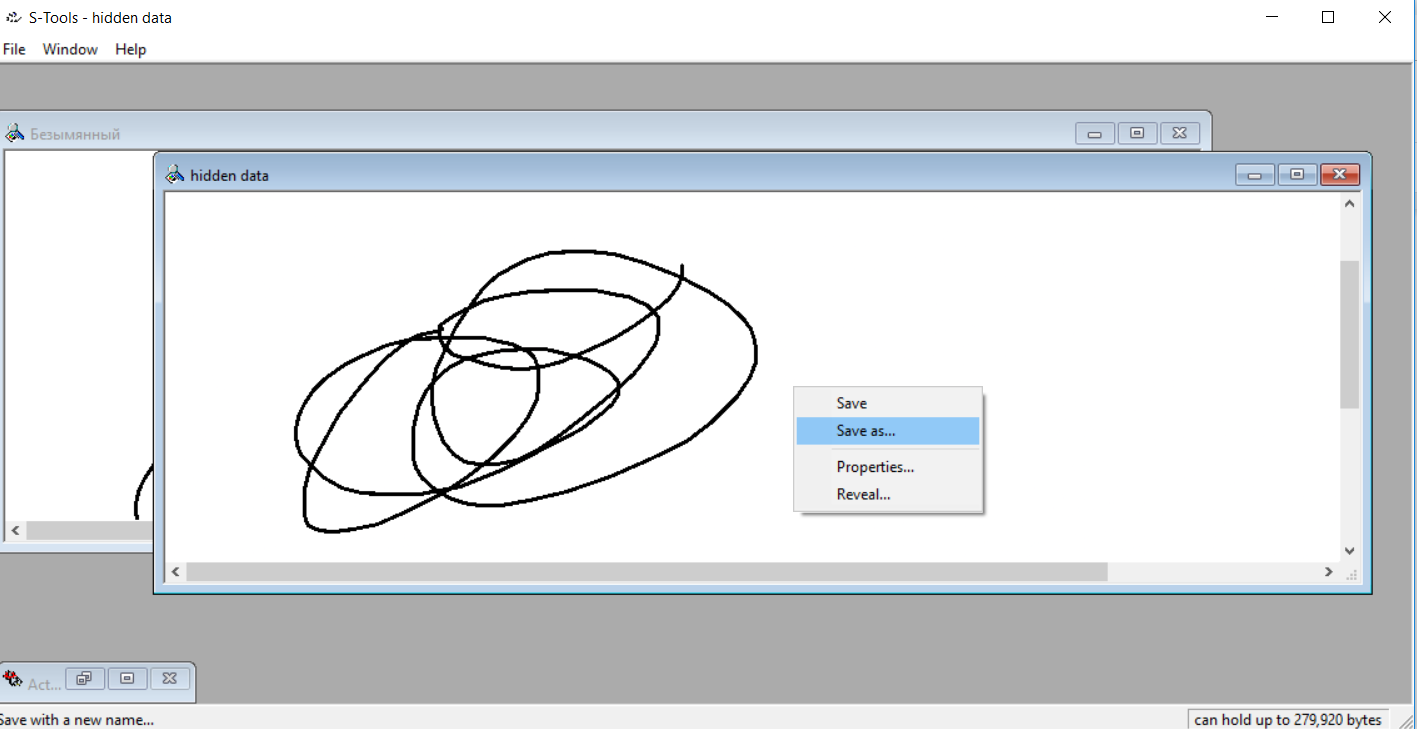


Вибираємо опції перетворення кольору



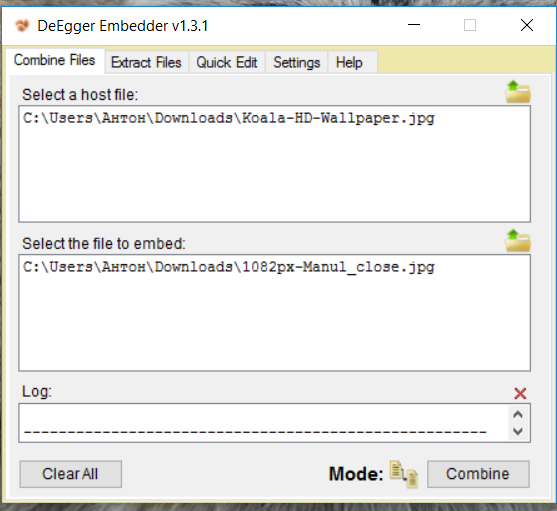


Зберігаємо файл з прихованою в ньому інформацією

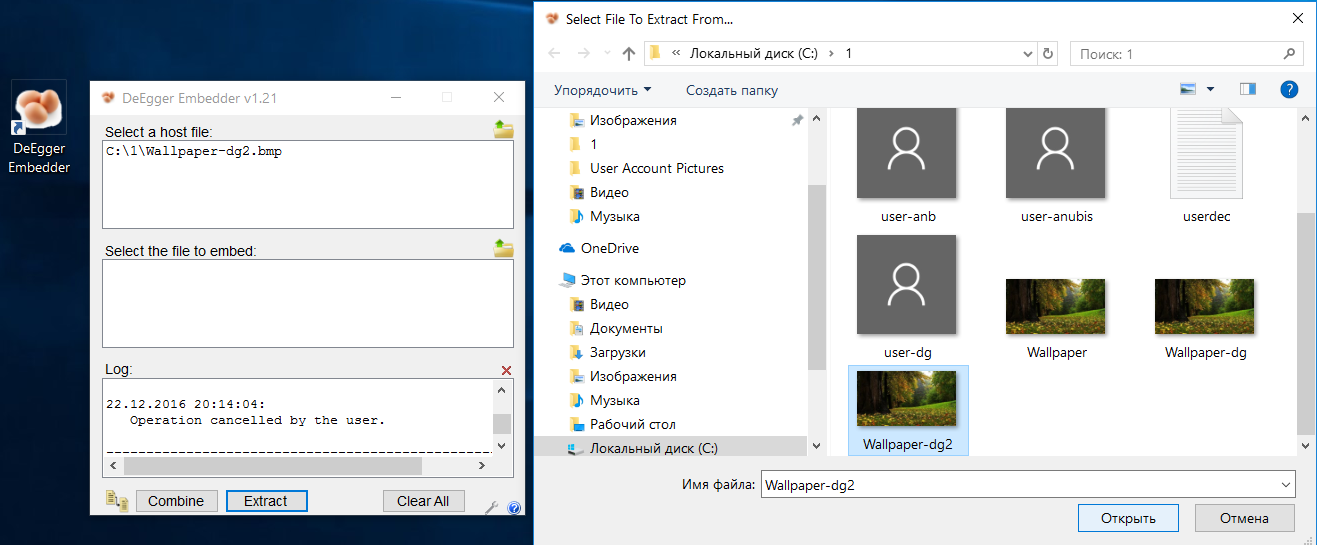


**2.DeEgger Embedder**

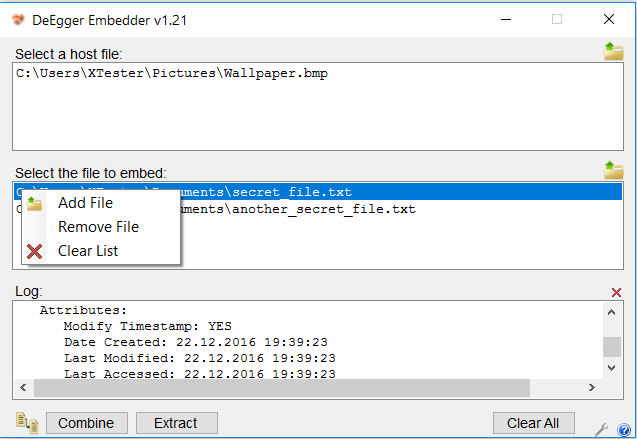
DeEgger Embedder - ще одна маленька програма для стеганографії. У ній реалізований вже більший набір функцій, але його використання вимагає установки .NET Framework 3.5. Крім рідко використовуваних сьогодні картинок BMP, програма підтримує в якості контейнерів PNG, JPG, відеофайли AVI і музичні MP3. Утиліта веде докладний лог своїх дій, який відображається прямо в головному вікні.



Кнопка запуску алгоритму називається Combine, а не Encrypt, що більш точно відображає процес впровадження файлів. Витягуються приховувані файли (стегосообщенія) з мультимедійних контейнерів натисканням єдиної кнопки Extract. Ніякого захисту пін-кодом тут немає.

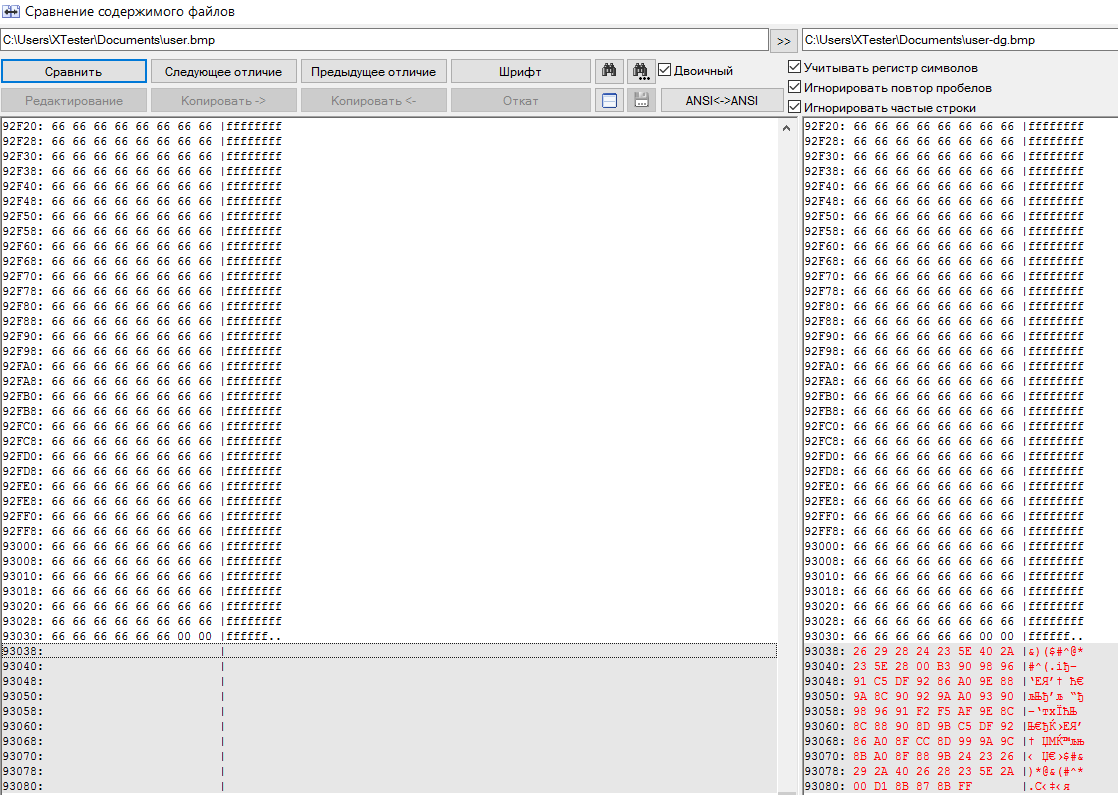
Комбайн и экстракт

Зате програма може обробляти кілька файлів відразу. Можна помістити кілька повідомлень в один контейнер або одне в різні контейнери.

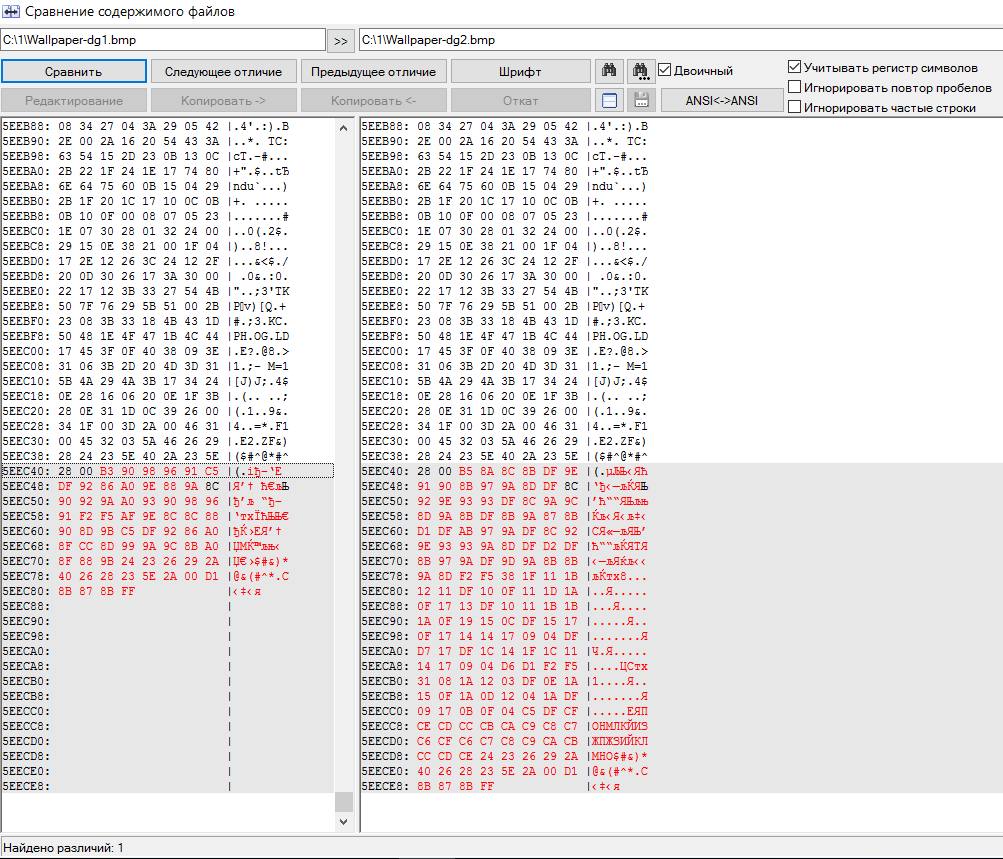


Після обробки в DeEgger утиліти для порівняння зображень вважають ідентичними вихідний і кінцевий файли BMP. Реально ж це порожній і заповнений контейнер в термінології стеганографії.

Зробимо побайтное порівняння. Знайома картина? Так само як і Anubis, утиліта DeEgger Embedder дописала стегосообщеніе в кінець файлу-контейнера. У зображенні user.bmp багато однотонних областей, тому такий апендикс виглядає особливо помітно.



На перший погляд, тут немає явних покажчиків, за якими можна зробити пошук файлів, що містять певну рядок. Однак придивимося уважніше. Для цього зробимо ще один контейнер з іншим повідомленням і з рівним вже два заповнених контейнера між собою.

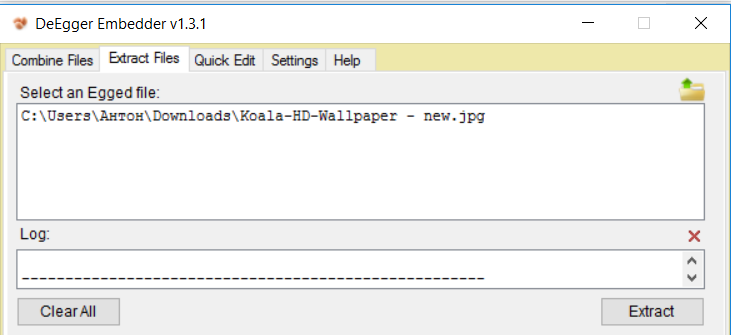


Знаходимо покажчик впровадженого файлу

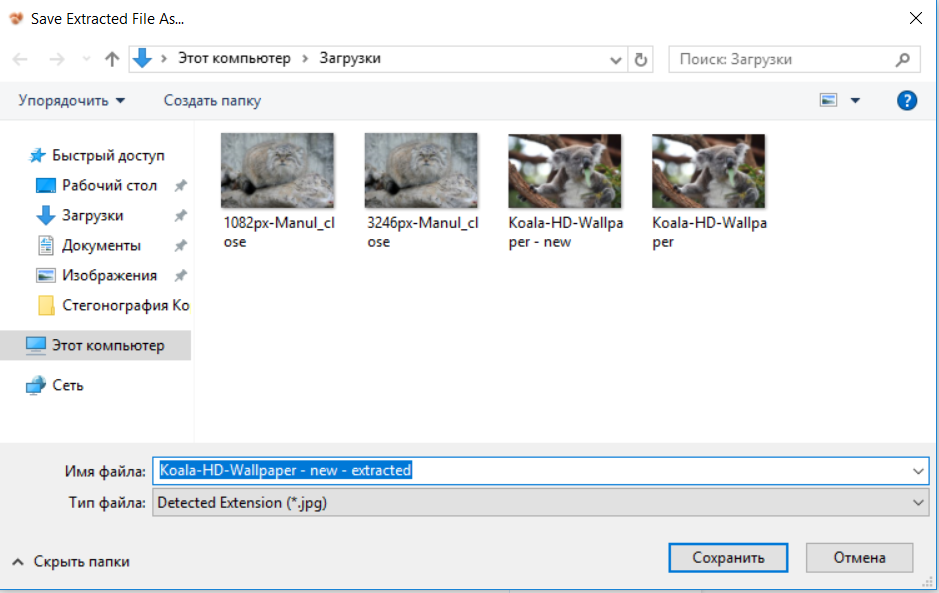
Ось однаковий ділянку в шістнадцятковому вигляді: 24 23 26 29 2A 40 26 28 23 5E 2A 00 D1 8B 87 8B FF.

Як бачите, незважаючи на підтримку більшої кількості форматів, DeEgger недалеко пішов від Anubis. Приховувані файли так само записуються в кінець файлу-контейнера і мають характерний вигляд, по якому їх легко виявити.

Вилучення інформації з зашифрованою картинки можна зробити в другому пункті шапки програми.



Отримуємо приховуваний файл



**3.TrueCrypt**

Ця програма захищає не безпосередньо самі файли. Вона дозволяє створювати спеціальні контейнери, в які можна поміщати будь-яку інформацію (документи, відео, фото та ін.). Вся інформація в такому контейнері зберігається в закріптованном вигляді. Для доступу до контейнера користувач повинен знати пароль. В якості додаткового захисту крім пароля можна використовувати також ключовий файл, без наявності якого відкрити контейнер неможливо.

В якості контейнера програма може використовувати спеціально створений файл або ж якийсь пристрій цілком (флешку, логічний розділ жорсткого диска).

Доступ до зашифрованого контейнера здійснюється шляхом його віртуального перетворення в окремий логічний розділ (монтування). Щоб змонтувати (відкрити) контейнер, користувач повинен запустити програму TrueCrypt, вказати на цей контейнер, ввести пароль, після чого в переліку запам'ятовуючих пристроїв комп'ютера (в розділі «Мій комп'ютер») з'явиться додаткове пристрій. Це і буде наш контейнер. З ним можна працювати як зі звичайним запам'ятовуючим пристроєм - копіювати, видаляти, створювати файли, переглядати, перейменовувати, коригувати їх і т.д. При цьому, дані, що зберігаються в змонтованому контейнері, крипти програмою «на льоту». Користувач цього навіть не помічає.

Відключивши контейнера він перестане відображатися в списку запам'ятовуючих пристроїв комп'ютера.

Як вже було сказано, програма TrueCrypt може створювати контейнери двох основних видів:

1. У вигляді окремого файлу будь-якого розміру (вказується користувачем). Розмір цього файлу буде розміром контейнера. Примітно, що файлу-контейнера можна привласнити будь-яку назву і розширення, наприклад, «avatar.avi». Такий файл на диску візуально буде виглядати як фільм «Аватар» і за замовчуванням (якщо двічі клацнути по ньому мишкою) буде відкриватися програмою-програвачем. Ніякого кіно, природно, при цьому не буде. Вилетить повідомлення про несправності файлу.

2. У вигляді цілого пам'яті (флешки, портативного жорсткого диска, логічного розділу жорсткого диска комп'ютера). Програма TrueCrypt дозволяє зашифрувати весь простір пам'яті (в тому числі разом з уже знаходяться на ньому файлами). Якщо такий пристрій спробувати відкрити звичайним способом (подвійним клацанням мишки), з'явиться повідомлення про те, що носій неформатований.

Таким чином, програма TrueCrypt реалізує два рівня захисту.

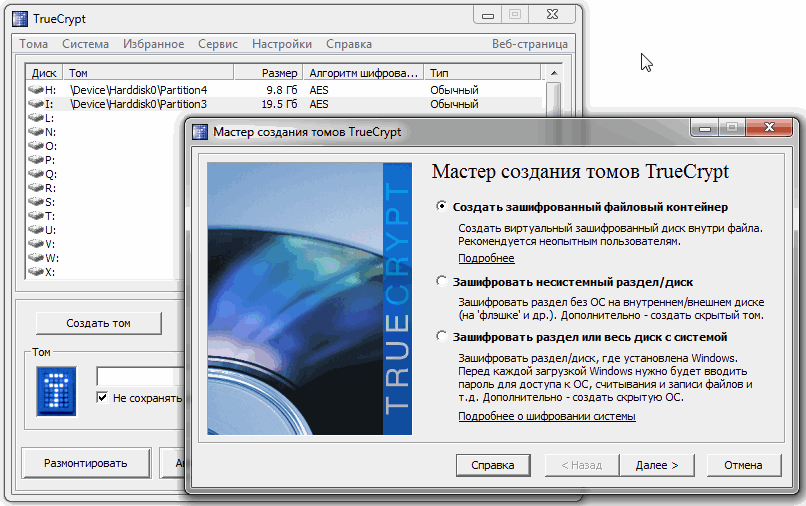
По-перше, вона ховає файли візуально, поміщаючи їх у середину іншого файлу або на носій, який на перший погляд здається неформатованим. Якщо контейнер навіть і потрапить в руки не обізнаного людини, той, швидше за все, просто видалить його, навіть і не здогадуючись про його дійсному призначення.

По-друге, дані, що зберігаються в контейнері, добре крипти. Зламати такий контейнер в звичайних умовах практично неможливо.

Ще однією важливою особливістю програми TrueCrypt є можливість криптування системного логічного розділу комп'ютера, тобто, розділу, в якому встановлена ​​операційна система. Пароль для доступу до нього буде запитуватися комп'ютером відразу після його включення (ще до початку завантаження Windows). Це дуже корисна можливість, оскільки вона гарантує надійний захист інформації навіть в тому випадку, якщо комп'ютер буде завантажений зловмисниками зі знімного носія (Live CD) або ж якщо жорсткий диск або SSD комп'ютера буде ними знятий і приєднаний до іншого комп'ютера. Зашифрований розділ при цьому буде орієнтуватися як неформатований.

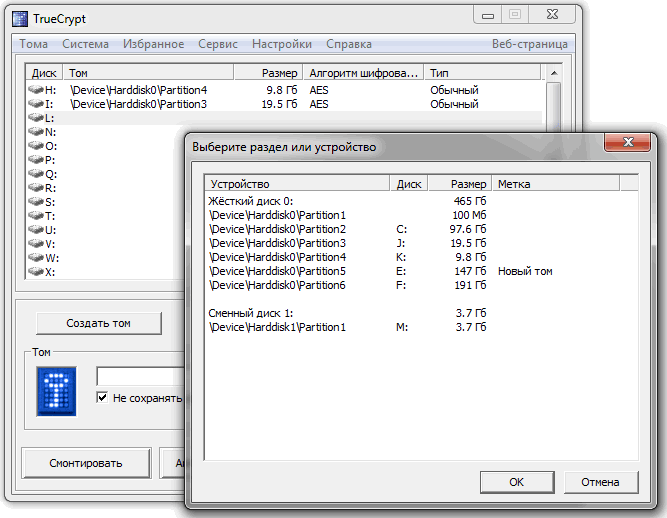
Користуватися програмою TrueCrypt не складно, в ній все зрозуміло на інтуїтивному рівні. Але про всяк випадок ось інформація про порядок здійснення основних операцій:

1. Для створення зашифрованого контейнера - запустити програму, натиснути кнопку «Створити те», вибрати один з варіантів створення контейнера і далі відповідати на питання майстра створення томи (див. Зображення);



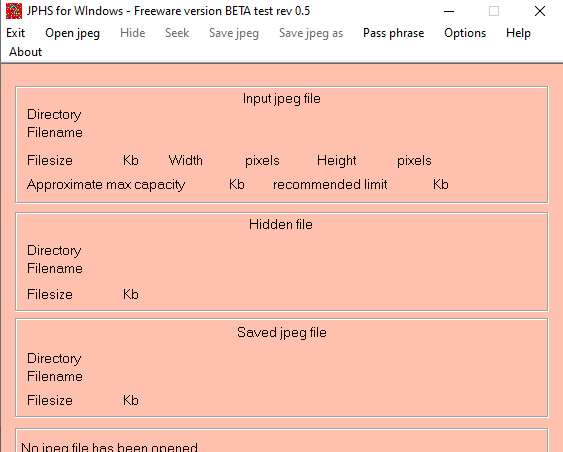
2. Щоб змонтувати контейнер - запустити програму, в основному віконці виділити букву пристрою, в вигляді якого буде змонтовано контейнер, потім натиснути кнопку «Пристрій» або «Файл» (в залежності від типу контейнера) і вказати на контейнер. Після цього натиснути кнопку «Змонтувати», ввести пароль, вказати на ключовий файл (якщо такий спосіб захисту був обраний для монтируемого контейнера) і натиснути кнопку «ОК».

3. Щоб демонтувати контейнеру повинна здійснюватися відкрити вікно програми, в основному віконці вибрати змонтоване пристрій і натиснути кнопку «Розмонтувати».



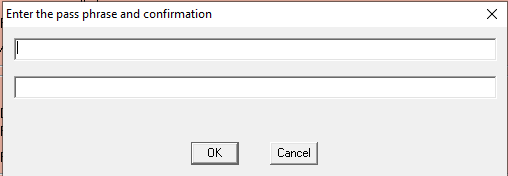
**4.JPHIDE, JPSEEK**

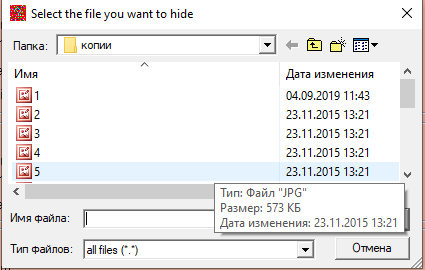
**JPHIDE, JPSEEK -** програми які дозволяють Вам приховувати файл в jpeg зображенні. Є велика кількість версій подібних програм, доступних в internet, але JPHIDE і JPSEEK досить специфічні. Їх головна мета - не приховати файл, а скоріше зробити це таким способом, щоб було неможливо довести, що ведучий файл містить невидимий файл.



Open jpeg-файл контейнер

Hide- Enter the pass phrase and confirmation- Введіть пароль і підтвердження



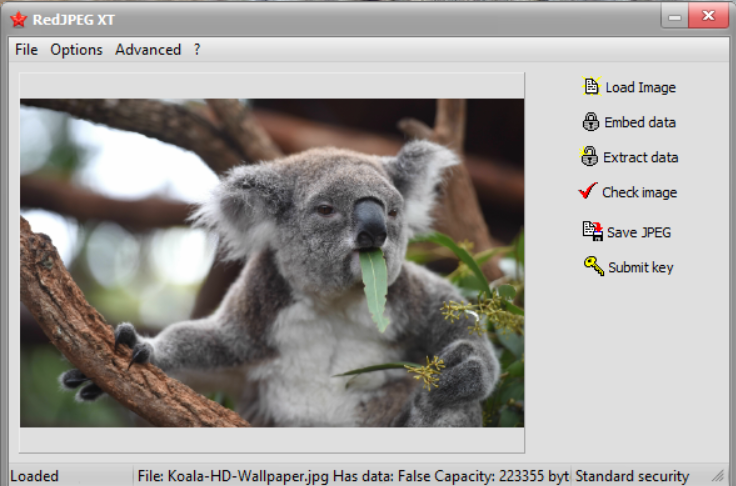


Вибрати файл для приховування і записати файл jpeg.

Процес дешифрування проходить в зворотному порядку.

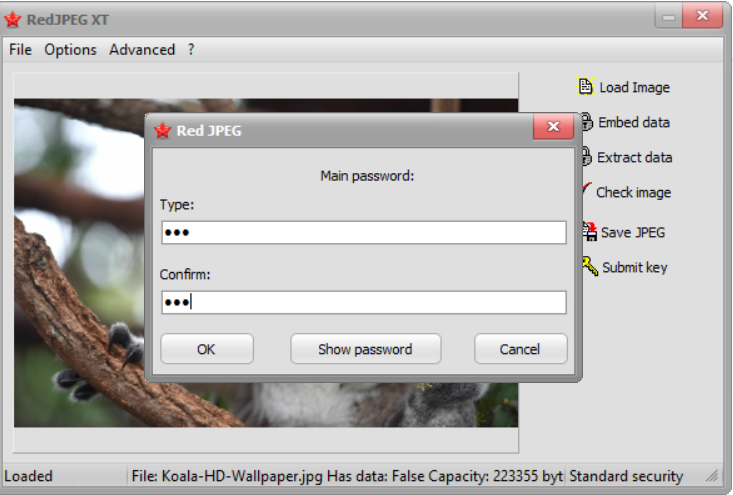
**5. Red JPEG XT**

Потужний плагін для стеганографічного приховування в JPEG зображенні довільних даних з використанням авторського методу. Рішення включає відкриті криптографічні алгоритми (AMPRNG rev.1.1, Cartman Cipher 2.DDP.4) і ефективне LZMA стиснення. Саме зображення змінюється лише незначно, без спотворень. Модифікацію практично не розрізнити візуально, не маючи перед очима оригіналу. Дані надійного захищені призначеним для користувача паролем, який попередньо хешіруется. На відміну від безлічі аналогів і поширених методик, в програмі використовується реальна стеганографія, яка полягає в незначній модифікації самого зображення. Ємність окремого графічного файлу залежить від його характеристик (кольоровості, яскравості і контрасту, набору варіацій пікселів). Дані попереднього стискаються і шифруються надійним потоковим криптоалгоритмом. Під час вилучення перевіряється коректність і цілісність архіву, правильність введення пароля шляхом підрахунку контрольної суми. Розширена версія з додатковою функцією маскування факту впровадження і посиленою процедурою ініціалізації поточного шифру на основі ряду характеристик конкретного зображення. Включає алгоритм випадкового секретного розподілу.

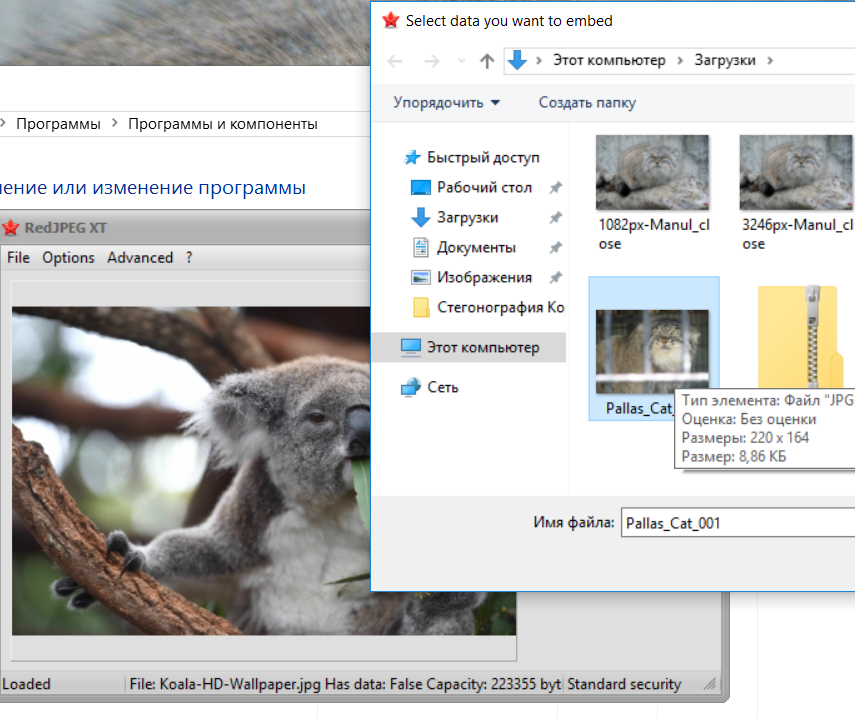


Інтерфейс програми

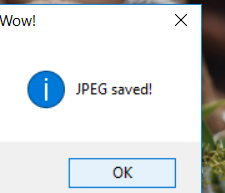
Перед тим як шифрувати дані ми повинні назначити пароль



Після чого за пунктом "Embed data" вибираємо файл для шифрування



Зберігаємо наш файл



Вилучення зашифрованої інформації відбувається за допомогою пункту меню “Extract Data”

Оформити лабораторну роботу з скріншотами використання програмних продуктів і зробити висновки по роботі.