

Лабораторная работа 51.

Работа с пакетом стеганографии.

Изложенный материал является составной частью пособия¹ раздел 2.1 "Основные понятия и применения стеганографии" на странице 73.

2.1.1 Основные понятия и применение стеганографии

В большинстве случаев в практике обмена и передачи данных и сообщений нужно не столько зашифровать данные, сколько просто скрыть сам факт обмена и передачи сообщений. Этой темой полна литература «докомпьютерной» эпохи. Практика написания текста молоком между строк, с целью дальнейшего проявления и визуализации сообщения, тоже восходит к тем временам. Методы, использующие маскировку и сокрытие самого факта наличия сообщения и его передачи, изучает стеганография.

Что изменилось в стеганографии с появлением компьютеров, и как всё это работает с использованием компьютерных программ и данных? Принципы стеганографии в компьютерную эру подверглись минимальным изменениям и остались такими же простыми. Файл с данными, факт передачи которого вы хотите скрыть, может быть любым: это может быть текст, изображение, бинарный файл, мультимедийный объект. С другой стороны, эти данные специальным образом внедряются в так называемый файл-носитель (carrier file) — рисунок 1.

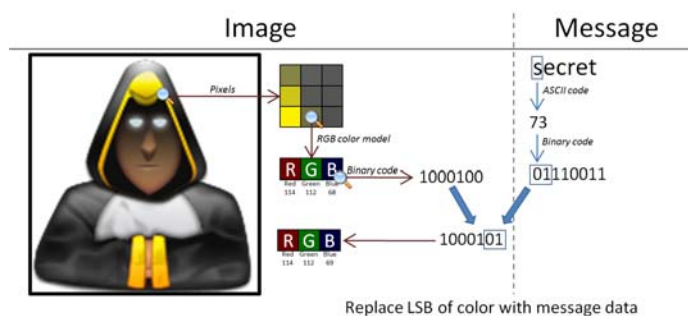


Рисунок 1 — Схема внедрения данных в файл-носитель

Естественно, файл-носитель внешне должен быть совершенно безобидным и не вызывать никаких подозрений у хакеров, нацеленных

¹ Ганжа В.А. Компьютерные сети. Информационная безопасность и сохранение информации / В.А. Ганжа [и др.]. — Минск : БГУИР, 2014. — 128 с.

вас атаковать, — рекламная картинка, текст песенки-шлягера, нейтральные фотографии цветов и домашних животных.

Второе требование к файлу-носителю — он должен быть “рыхлым”, то есть содержать достаточное количество избыточных данных. Такие файлы обычно очень хорошо упаковываются архиваторами. Форматы таких файлов известны — *.bmp, *.txt, *.html, *.pdf. Именно такие файлы используются в качестве файлов-носителей. Программа, осуществляющая все эти функции, подходит для нашей задачи. Такие программы обычно небольшие и имеются в свободном доступе в Интернете. Стоит вам набрать в любой поисковой системе “program steganography” и вы получите список из сотен названий.



Рисунок 2 — Первый шаг работы с программой SilentEye

Выполним некоторые практические задания, для этого используем программу SilentEye с открытым исходным кодом, которая написана программистом Anselm Choein и загружена с его web-странички <http://forge.silenteye.org/>.

2.1.2 Внедрение данных в файл-носитель программой SilentEye

Работа с программой состоит из ряда этапов.

Первый этап. На первом этапе запускаем программу и видим интерактивное окно (рисунок 2). При отсутствии загруженного файла кнопки выбора режима работы затенены. При выборе пункта главного меню, “? → About” программа сообщает: номер версии программы; сведения

об авторах разработчиках; некоторые сведения о себе; и GNU лицензию.

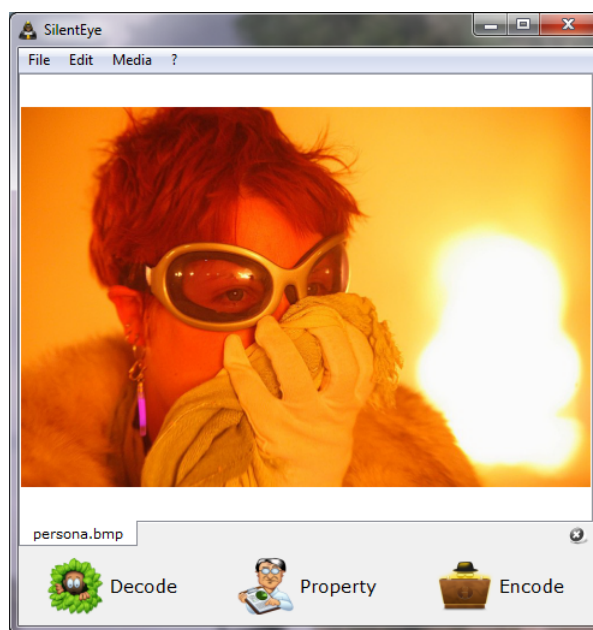


Рисунок 3 — Выбор режима работы программы SilentEye

Упражнение для самостоятельной работы 1. Выберите пункта главного меню, “? → About” и просмотрите сведения, которые хочет сообщить вам программа.

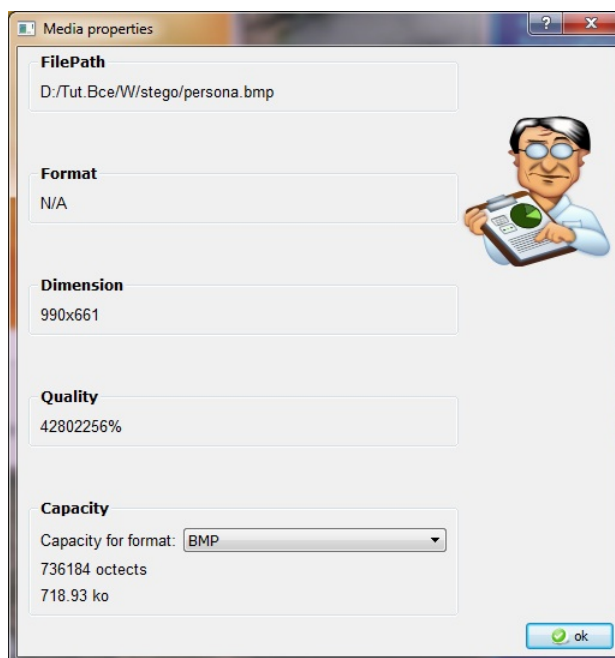


Рисунок 4 — Свойства файла носителя в окне программы SilentEye


Упражнение для самостоятельной работы 2. Выберите пункт главного меню, “Edit → Preferences” и просмотрите, доступ к каким настройкам

разрешает программа SilentEye. Обратите внимание, что в этом окне можно указать путь к каталогу с файлами, а также выбрать стандартные форматы по умолчанию.

Для выхода из программы, выберите пункт главного меню, “File → Quit”.

Второй этап. Открываем файл с которым вы будете работать: отправлять данные (внедрять — encode), либо получать данные (извлекать — decode) (рисунок 3). Обратите внимание интерфейсные кнопки Decode, Encode и Property стали активными.

Осуществим внедрение ваших конфиденциальных данных в файл носитель `persona.bmp`. Программа SilentEye позволяет посмотреть и контролировать свойства загруженного файла-носителя.

Перед началом работы полезно посмотреть свойства файла (рисунок 4): полный путь; размер; качество; формат и количественно оценить размер внедряемых данных. Для этого выбираем пункт главного меню, “Media → Property” (либо жмём кнопку  — Property).

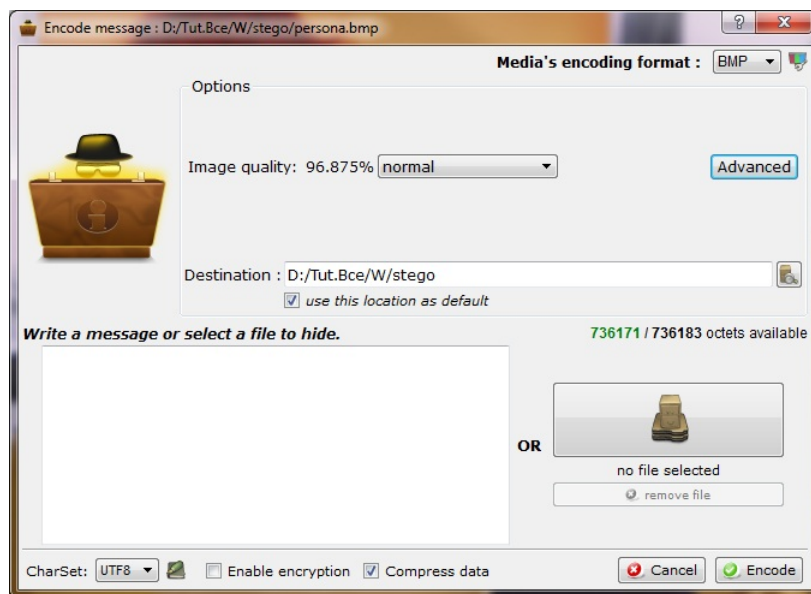



Рисунок 5 — Окно кодирования со стандартными настройками

Третий этап. Подготовка внедрения данных в файл носитель `persona.bmp`. Для этого выбираем пункт главного меню, “Media → Encode” (либо жмём кнопку  — Encode). Появляется окно программы с различными настройками (рисунок 5).

Необходимо сразу проверить содержимое поля Destination, где указывается место дислокации будущего файла с зашифрованными данными. Программа SilentEye к сожалению не даёт возможности переименовать этот файл в процессе шифрования, поэтому выход в том чтобы

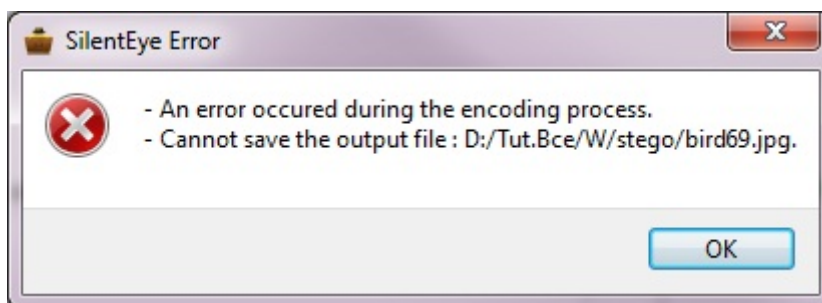


Рисунок 6 — Сообщение о сбое записи файла

поместить ваш новый файл (с тем же самым именем) в другой каталог, путь к которому вы должны ввести в поле Destination. Если этого не сделать программа SilentEye не перезапишет старый файл, но откажется работать и выдаст следующее сообщение (рисунок 6)

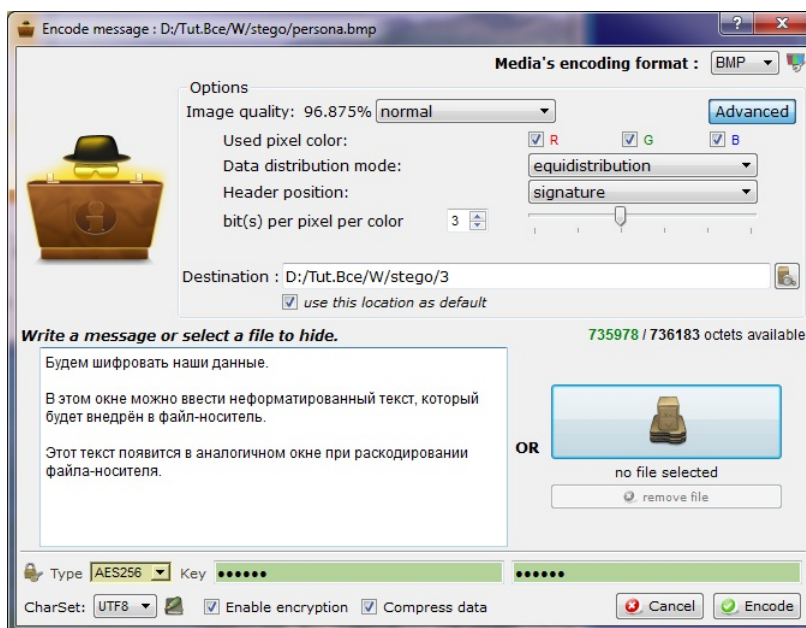


Рисунок 7 — Окно кодирования с расширенными настройками

Нажав кнопку Advanced можно перейти в окно с расширенными настройками (рисунок 7). В расширенных настройках программа предоставляет несколько дополнительных возможностей — распределять внедрённые данные в выходной файл (Data distribution mode) **равно-распределённо** — Equidistribution или Inline — **локализовано** в одно место (рисунок 8). Если вы уверены в структуре распределения данных

этого файла, отметьте Inline, но лучше положиться на программу, она разберётся, как распределить внедряемые вами данные в файле-носителе.

Рисунок 8 иллюстрирует в виде красных квадратиков две возможности: **Equidistribution** и **Inline** распределения данных по файлу

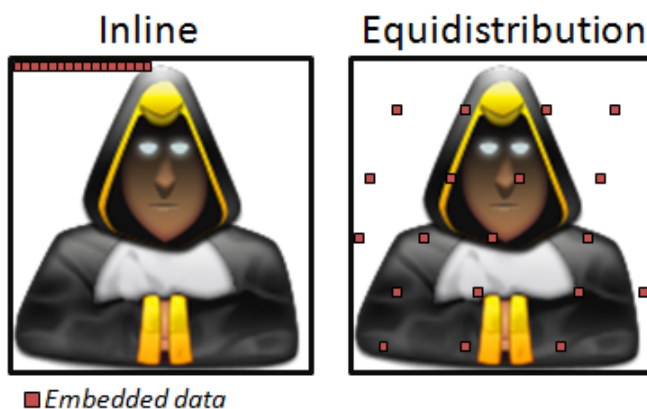


Рисунок 8 — Структура распределения данных в файле носителе

Пункт User pixel color позволяет задействовать для переноса данных различные цветовые пиксели (если вы отметили соответствующий флажок): красные — **R**, зелёные — **G** и голубые — **B**. Манипуляции с цветом оправданы, если в файле носителе преобладает один цветовой тон.

Следующая позиция Header position (рисунок 7) — указывает программе в каком месте картинке размещать служебные данные. На рисунке 9 они показаны зелёными символическими квадратиками.

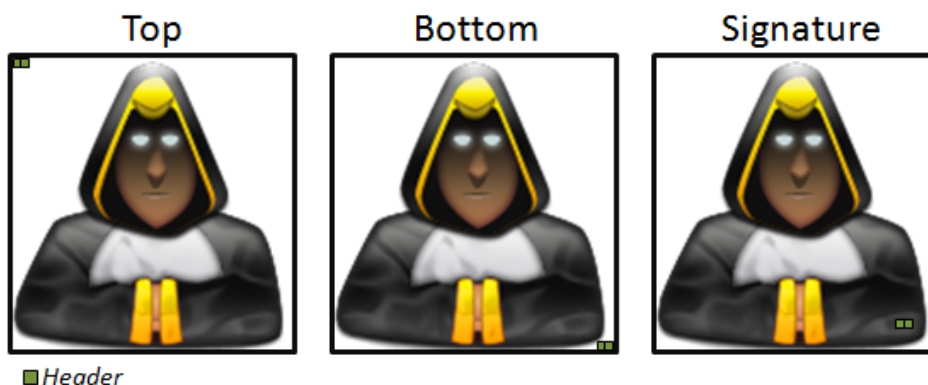


Рисунок 9 — Место дислокации служебных данных в файле носителе

Программе необходимо указать путь к файлу, данные которого будут внедрены в файл носитель, для указания этого пути к этому "секретно-

му" файлу нажимаем большую кнопку справа (рисунок 5), после чего появляется стандартное окно ввода файловой системы.

Четвёртый этап. Программа SilentEye по умолчанию не шифрует данные (рисунок 5). Для возможности шифровать внедряемые данные в файл носитель, необходимо активировать флажок Enable encryption, тогда внизу окна программы появятся два поля для ввода пароля (см. рисунок 7) и поле метода шифрования с длиной ключа. Программа SilentEye использует метод шифрования AES с длиной ключа 128 бит, либо 256 бит.

На рисунке 5 этот флажок не активен и полей нет. При активации функции Enable encryption, для работы программы SilentEye необходимо будет дважды ввести пароль. Если пароль в обоих полях совпал, то они окрашиваются в зелёный цвет как на рисунках 7 и 10.

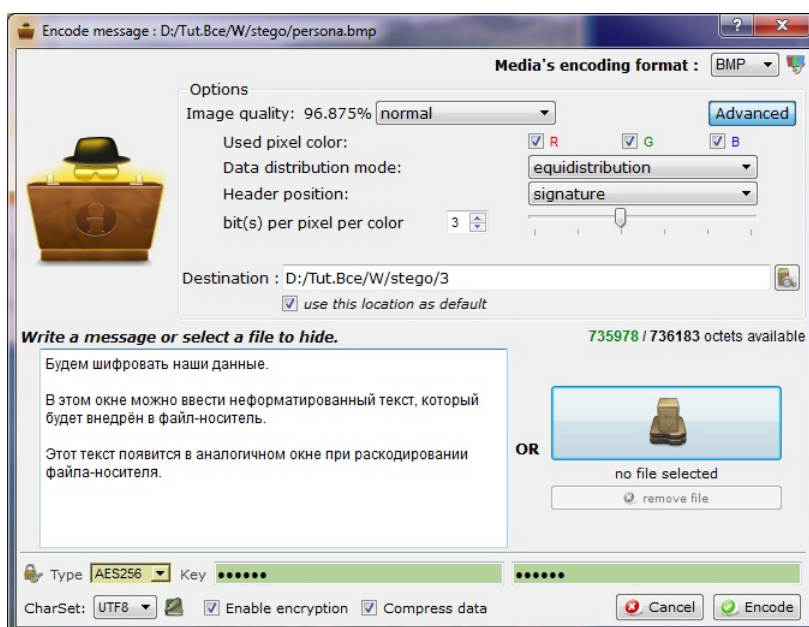


Рисунок 10 — Текст введенный с клавиатуры в окно сообщений

Программа SilentEye допускает альтернативную возможность внедрять не файл, а вводить данные прямо с клавиатуры. Внизу окна с установками кодирования (рисунок 10) имеется большое прямоугольное поле для ввода текста с клавиатуры, который будет внедрён в файл носитель. В окне ввода (рисунок 10) можно ввести неформатированный текст, который будет внедрён в файл носитель. Этот текст появится в аналогичном поле (рисунок 16) при раскодировании файла носителя.

Программа `SilentEye` не переименовывает файл-носитель при внедрении в него данных, поэтому предлагает указать другой каталог для обработанного файла.



Рисунок 11 — Зелёный индикатор сообщает о наличии свободного места в файле носителе

Необходимо учесть, что размеры файла-носителя и данных, которые вы хотели бы туда внедрить, коррелируют. Файл-носитель, конечно, «рыхлый», но не «резиновый» и естественное ограничение — его собственный размер. Данные, превосходящие по размеру файл-носитель, внедрить в него никак нельзя.



Рисунок 12 — Красный индикатор сигнализирует о превышении допустимого размера в файле носителе

Речь может идти только о какой-то части, о какой-то доле размера файла-носителя, обычно, не превышающей 50 %. Точных рецептов и точных аналитических формул для расчёта этого параметра нет. Общее правило такое: для сокрытия большого массива конфиденциальных данных нужен соответствующего большего размера файл-носитель.

Обсуждаемый параметр зависит от типа данных: наиболее «рыхлые» — чёрно-белые картинки формата `*.bmp`, минимум избыточных данных в формате `*.pdf`. Проверку обсуждаемого параметра осуществляет сама программа и вы можете увидеть сообщение, показанное на рисунке 11, который является фрагментом рисунка 5.

Если ваши данные предназначенные для сокрытия, не поместятся в файл-носитель, индикатор будет красного цвета и перед ним появится минус (см. рисунок 12).

При попытке всё-таки начать кодирование данных программа выдаст сообщение об ошибке, как на рисунке 13.

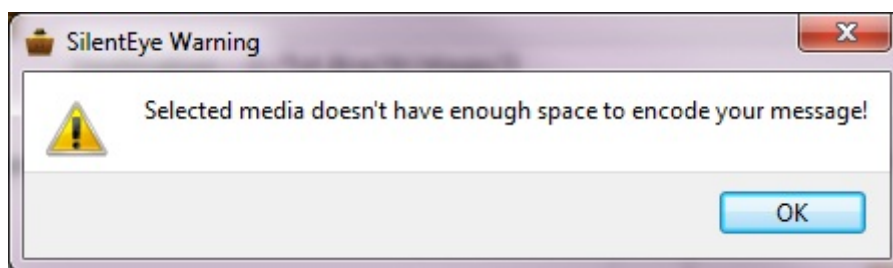


Рисунок 13 — Сообщение о превышении допустимого размера внедряемого сообщения

После описанных подготовительных операций в правом нижнем углу окна ввода нажимаем кнопку Encode. Если вы всё сделали правильно окно для ввода данных исчезнет, а в основном окне программы появится вторая закладка которая станет активной (рисунок 17). Тем самым программа информирует вас, что процесс шифрования данных и их внедрение в файл-носитель успешно завершён. К сожалению, программа SilentEye не даёт возможности присвоить новому файлу с внедрёнными данными другое имя.

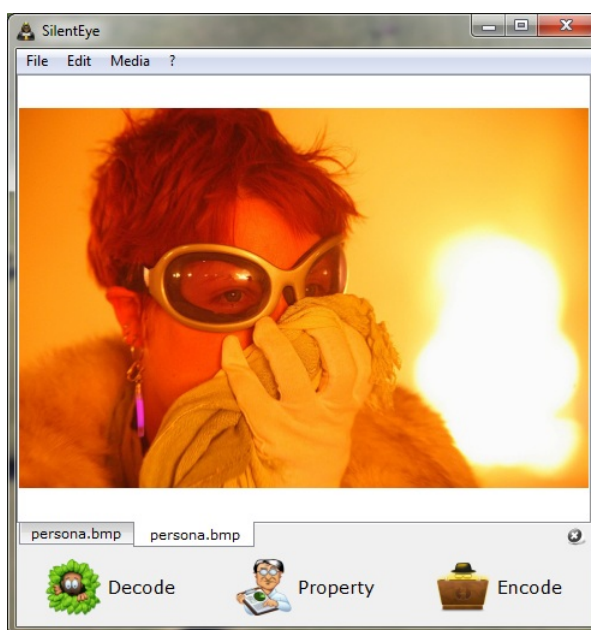


Рисунок 14 — Появление второй закладки — сигнал об успешном завершении работы программы

И пустой файл-носитель и файл с зашифрованными данными теперь имеют одинаковые имена, одинаковые размеры и "на глаз" их различить невозможно (хорошо, что они теперь хоть в разных каталогах).

Будьте внимательны и осторожны, переименуйте их самостоятельно, поскольку если вы установили опцию Image quality в ввысоке качество, то отличий файлов в разных закладках вы не найдёте, более того, размеры у этих файлов окажутся одинаковыми.

2.1.3 Извлечение данных из файла-носителя программой SilentEye

Для решения обратной задачи — извлечения данных из файла-носителя — последовательно выполняем несколько этапов.

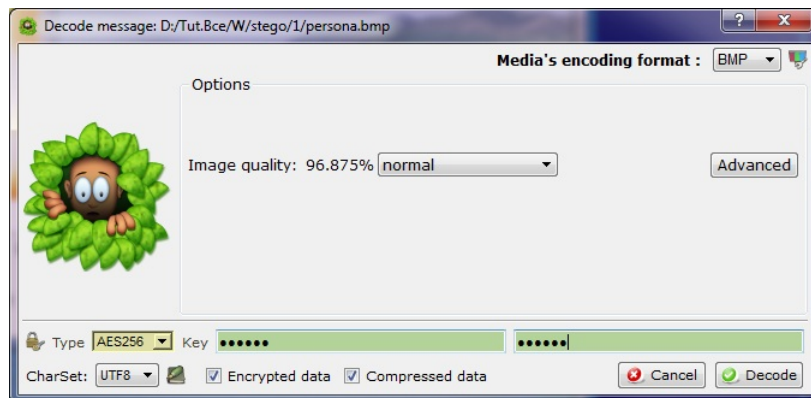



Рисунок 15 — Окно декодирования со стандартными настройками

Первый этап. Запускаем программу SilentEye (см. рисунок 2) и открываем в ней файл содержащий внедрённые данные. После этого выбираем пункт главного меню, “Media → Decode” (либо жмём кнопку  — Decode). Появляется окно программы с различными настройками (рисунок 15).

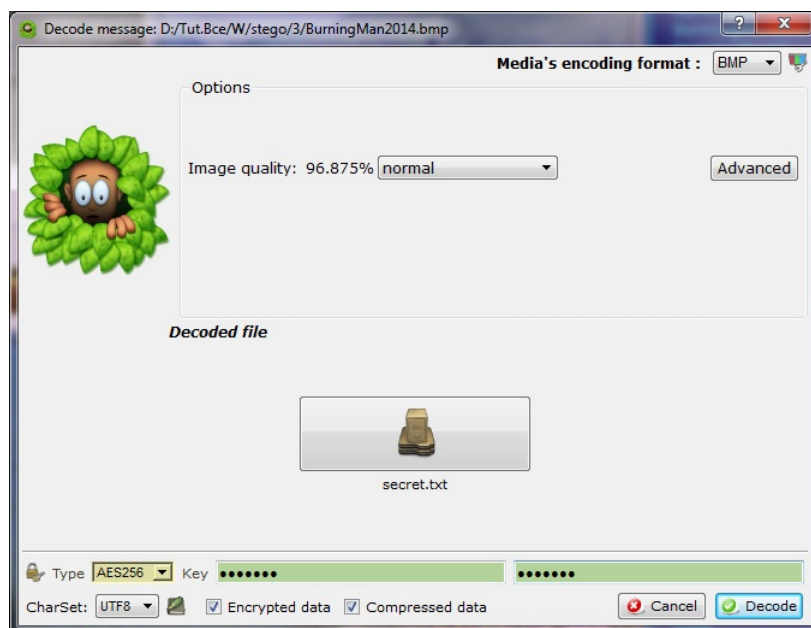


Рисунок 16 — Расшифрованный файл и его название

Для успешного процесса расшифровки необходимо внизу в соответствующих окнах дважды ввести пароль. Если это сделано безошибочно, то окна ввода позеленеют. Теперь нажимаем кнопку Decode в правом нижнем углу.

В случае успешной расшифровки файла-носителя появляется следующее окно (рисунок 16) с названием скрытого файла и с большущей кнопкой, нажав на которую появляется стандартное диалоговое окно ОС Windows со стандартным интерфейсом, с помощью которого вы указываете программе SilentEye куда извлечь расшифрованный секрет-файл.

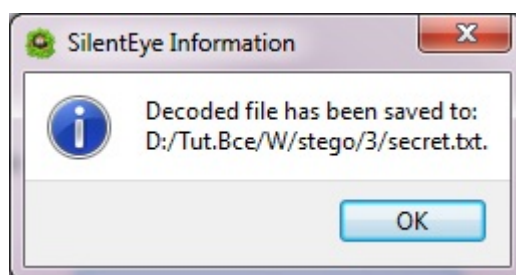


Рисунок 17 — Успешное завершения процесса декодирования

Произойдёт извлечение файла и запись его на жёсткий диск в ваш каталог. Если всё прошло успешно, программе SilentEye выводит окошко (рисунок 17) с последним сообщением о расшифровке и записью секрет-файла на жёсткий диск.

*

*

*

Упражнение для самостоятельной работы 3. Подготовьте ваши конфиденциальные данные и обработайте их программой *SilentEye*. В качестве носителей вам предлагается восемь файлов в каталоге `../network/51/v*` (см. Примечание). Эти восемь файлов содержат четыре графических изображения: четыре из них формата `*.bmp` и четыре — формата `*.jpg`.

Подберите для каждого из восьми файлов-носителей **максимальный** размер секрет-файла (файла с вашими конфиденциальными данными). Используйте сведения описанные в этом методическом пособии и информацию, показанную на рисунках 11, 12. Результат вашей работы о всех восьми файлах сведите в таблицу, содержащую следующие поля.

1. Порядковый номер

Файл-носитель

2. имя, из предложенного варианта (файлы не переименовывать)

3. формат

4. размер

Секрет-файл

5. формат (тип)

6. размер

7. Отношение максимального размера секрет-файла к размеру файла-носителя (в процентах)

8. Примечания о ходе выполнения (если сочтёте необходимым). В примечании отметьте также, использовалось ли сжатие и шифрование в процессе внедрения данных в файл-носитель.

Таблица 1 — Определение предельной вместимости файла-носителя в методе стеганографии

№	Файл-носитель			Секрет-файл		Отношение %	Примечание
	имя	формат	размер Кб	формат	размер Кб		
1	persona.bmp	bmp	984	chm	480	49	
2	persona.jpg	jpg	41	txt	7	17	
8							

Узнайте номер вашего варианта у преподавателя. После завершения работы сдайте заполненную таблицу преподавателю.

Примечание. На кафедральном сервере **ftp://192.168.1.15** имеется дистрибутив программы SilentEye, а также файлы с изображениями **.bmp** и **.jpeg** необходимые для выполнения упражнений. Дистрибутив SilentEye расположен в каталоге **../network/51/SilentEye**

варианты для выполнения упражнений:

../network/51/v01

.....

../network/51/v12

Успехов и удачи!