

Introducción a la Esteganografía

Roberto Gómez Cárdenas

rogomez@itesm.mx

<http://cryptomex.org>

Otra opción a la criptografía...

ESTEGANOGRAFIA

Esteganografía

- Area similar a la de criptología.
- Viene del griego stegos (ocultar).
- Conjunto de técnicas que nos permiten ocultar o camuflar cualquier tipo de datos, dentro de información considerada como válida.
- La información puede esconderse de cualquier forma
 - diferentes métodos se han ido desarrollando



Algunos ejemplos históricos

- Herodoto:
 - 440 ac: Aristagoras de Milet usa esclavos calvos para la revuelta contra los persas
 - Demeratus envía mensaje (tablones cubiertos de cera) a Esparta para avisar de que Xerxes (rey de Persa) tenía intenciones de invadir Grecia.
- Tintas invisibles
 - Naturales: jugo limón, leche, orina, sal de amoniac
 - Química: alumbre y vinagre, traspasar cáscara huevo duro
- Chinos: texto escrito sobre seda china



Ejemplo de Null Cipher

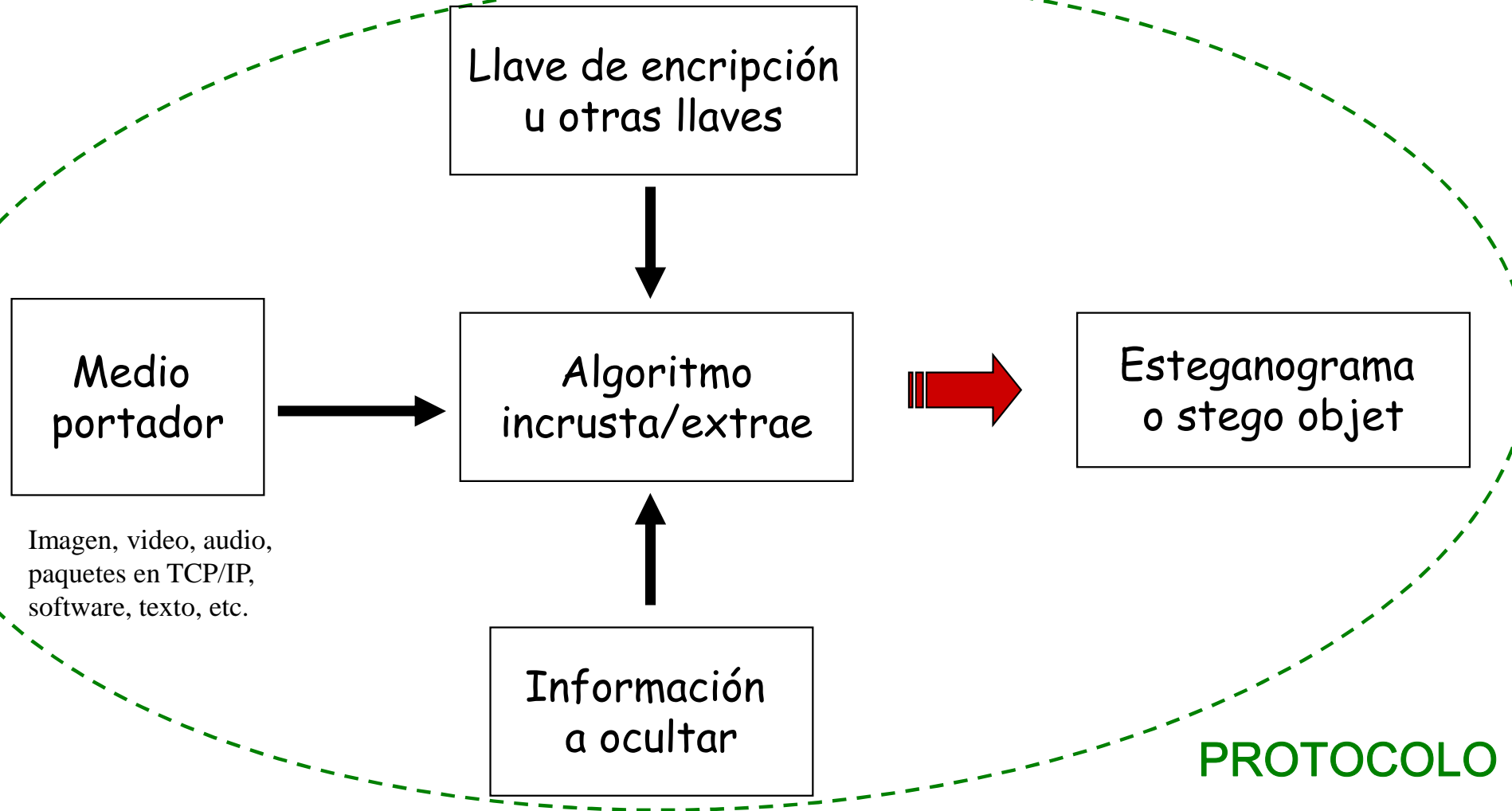
Tomando la primera letra de cada palabra

News Eight Weather: Tonight increasing snow.
Unexpected precipitation smothers eastern towns. Be
extremely cautious and use snowtires especially heading
east. The highways are knowingly slippery. Highway
evacuation is suspected. Police report emergency
situations in downtown ending near Tuesday.

Hidden Information !

Newt is upset because he thinks he is President.

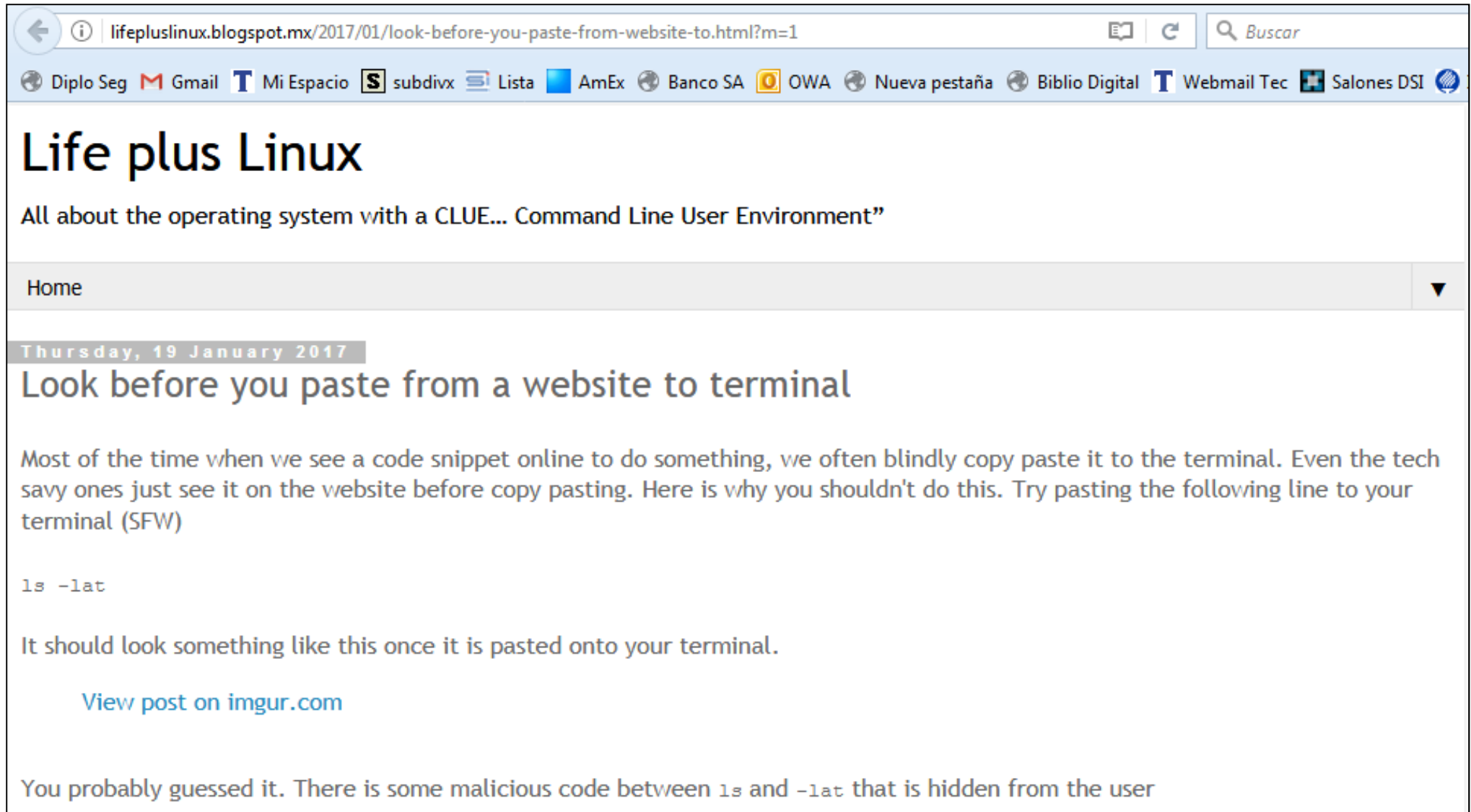
El proceso esteganográfico



Medios portadores

- Archivos de imágenes, sonido, texto, video
- Archivos ejecutables
- Archivos de música y de películas
- Páginas Web
- Campos no usados de paquetes de redes (TCP/IP)
- Espacio no utilizado del disco: slack space
- Particiones escondidas
- HTML
- ...

Un ejemplo interesante



lifepuslinux.blogspot.mx/2017/01/look-before-you-paste-from-website-to.html?m=1

Diplo Seg Gmail Mi Espacio subdivx Lista AmEx Banco SA OWA Nueva pestaña Biblio Digital Webmail Tec Salones DSI

Life plus Linux

All about the operating system with a CLUE... Command Line User Environment”

Home

Thursday, 19 January 2017

Look before you paste from a website to terminal

Most of the time when we see a code snippet online to do something, we often blindly copy paste it to the terminal. Even the tech savy ones just see it on the website before copy pasting. Here is why you shouldn't do this. Try pasting the following line to your terminal (SFW)

```
ls -lat
```

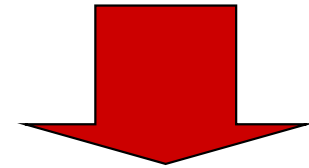
It should look something like this once it is pasted onto your terminal.

[View post on imgur.com](#)

You probably guessed it. There is some malicious code between `ls` and `-lat` that is hidden from the user

<http://lifepuslinux.blogspot.mx/2017/01/look-before-you-paste-from-website-to.html?m=1>

Usando imágenes digitales



```
FluxCat - Bloc de notas
Archivo Edición Búsqueda Ayuda
/* Copyright (C) 1996, MPEG Software Simulation Group. All Rights Reserved. */
/*
 * Disclaimer of Warranty]
 * These software programs are available to the user without any license fee or
 * royalty on an "as is" basis. The MPEG Software Simulation Group disclaims
 * any and all warranties, whether express, implied, or statutory, including any
 * implied warranties or merchantability or of fitness for a particular
 * purpose. In no event shall the copyright-holder be liable for any
 * incidental, punitive, or consequential damages of any kind whatsoever
 * arising from the use of these programs.
 *
 * This disclaimer of warranty extends to the user of these programs and user's
 * customers, employees, agents, transferees, successors, and assigns.
 *
 * The MPEG Software Simulation Group does not represent or warrant that the
 * programs furnished hereunder are free of infringement of any third-party
 * patents.
 *
 * Commercial implementations of MPEG-1 and MPEG-2 video, including shareware,
 * are subject to royalty fees to patent holders. Many of these patents are
 * general enough such that they are unavoidable regardless of implementation
 * design.
 */
```



Técnicas steganográficas

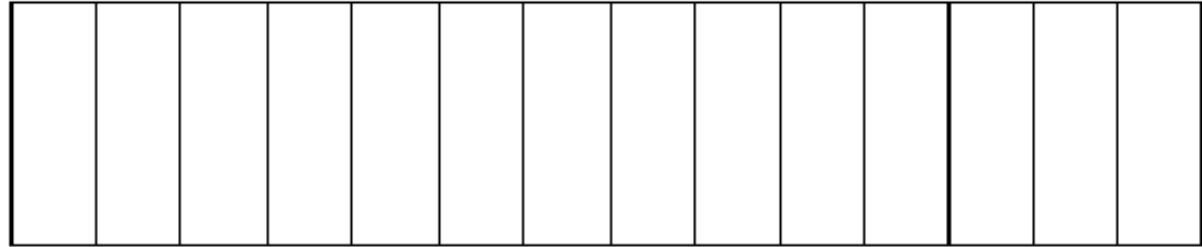
- Adición
 - Se oculta el mensaje secreto en las secciones del medio portador que pueden ser ignoradas por la aplicación que lo procesa
- Generación
 - Se crea el esteganograma a partir de la información secreta, sin contar con un medio portador previamente
- Susbtitución
 - Se modifican ciertos datos del medio portador por los datos del mensaje secreto

Ejemplo adición

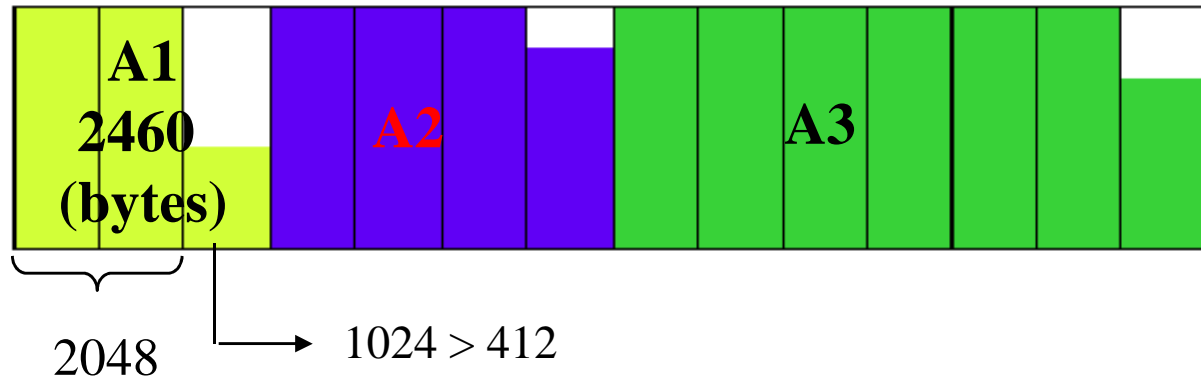
slack space

El slack space

14 clusters libres
c/cluster = 1024 bytes



Tres archivos:
A1, A2 y A3



Cluster = 512bytes



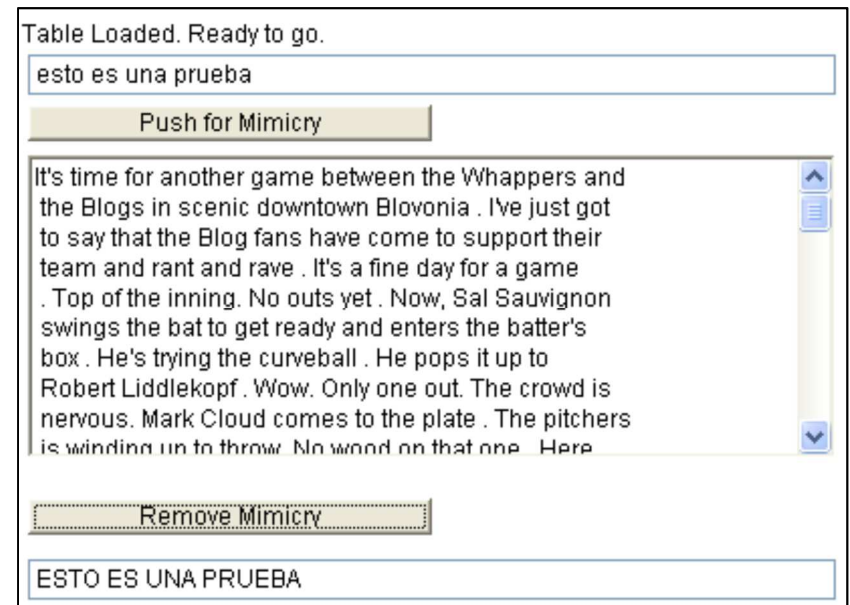
Ejemplos generación

funciones “mimic”

<http://www.wayner.org/books/discrypt2/bitlevel.php>

Ejemplos generación

- Mensaje a ocultar es la entrada de un generador de texto
- El generador produce un mensaje que incluye las palabras de la información a ocultar.
- Ejemplos
 - Narrador de baseball
 - <http://www.wayner.org/texts/mimic>
 - Spam Mimic
 - <http://www.spammimic.com/>
 - Lista de canciones
 - <http://www.wayner.org/books/discrypt2/sorted.php>



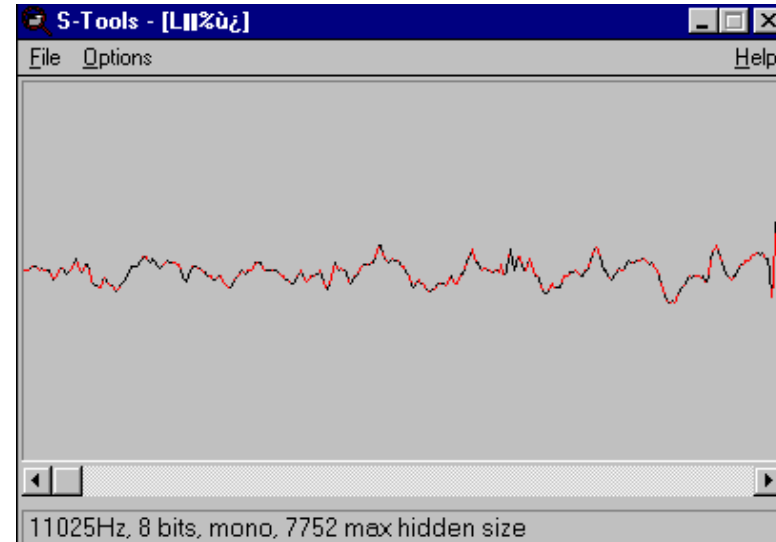
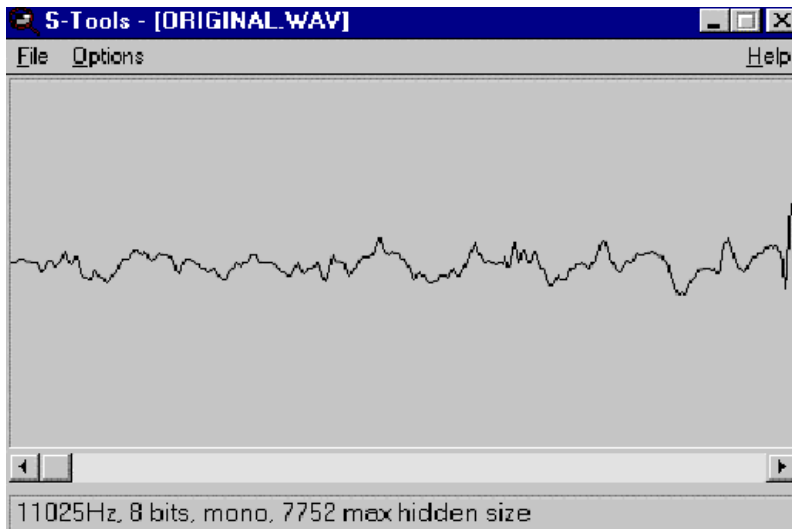
Ejemplos substitución

archivos digitales y Stools

Ejemplos Susbtitución

- Principales métodos
 - LSB: Least-Significant Bit
 - La transformación matemática de la información
 - Transformación discreta del coseno (DCT)
 - Transformación discreta de Fourier
 - Transformación de Wavelet
- Posibles medios medios portadores (archivos digitales)
 - archivos de música
 - archivos de imagenes

Esteganografía en música



Información: 132 134 137 141 121 101 74 38

**Binario: 10000100 10000110 10001001 10001101 01111001 01100101 01001010
00100110**

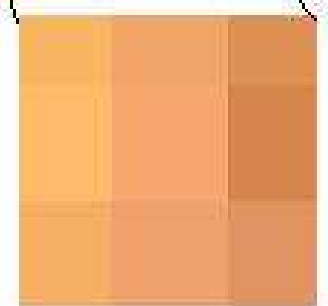
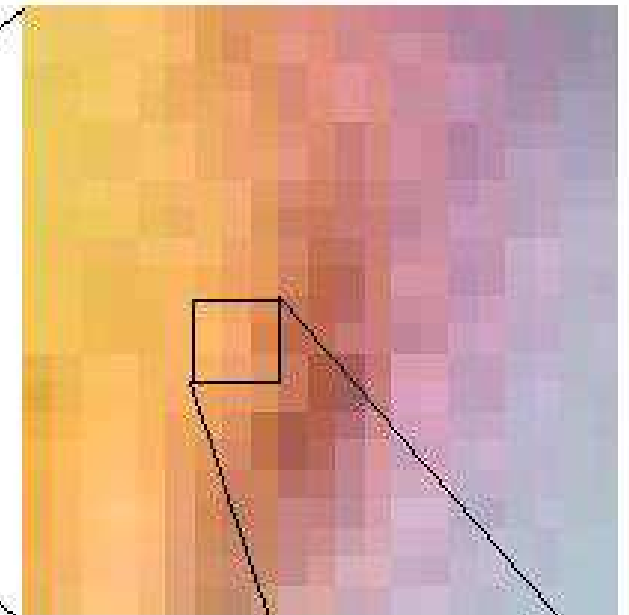
Información a esconder: 11010101 (213)

Resultado: 133 135 136 141 120 101 74 39

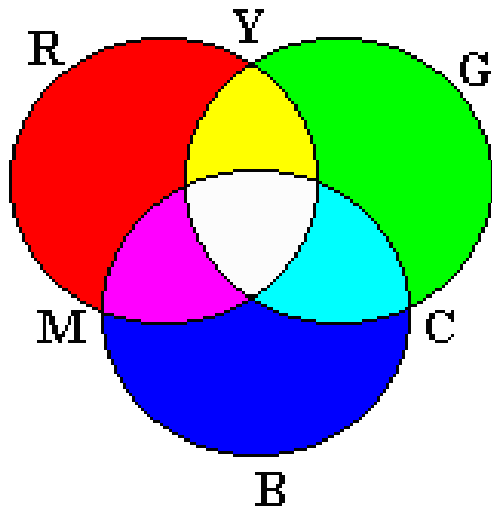
**Binario: 10000101 10000111 10001000 10001101 01111000 01100101
01001010 00100111**

Imágenes

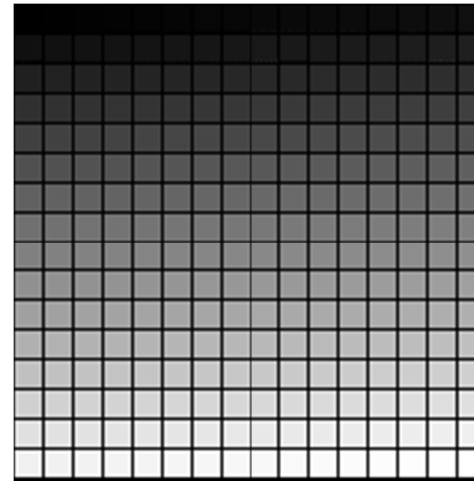
- Una imagen es una matriz de $M \times N$ Píxeles.
- Un Pixel es la unidad mínima de dibujo



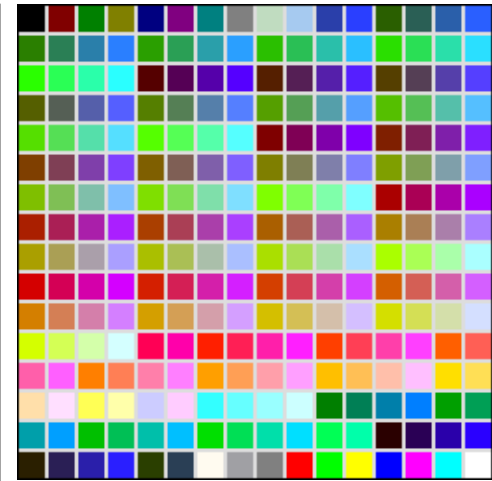
Los colores en las imágenes digitales



RGB



Paleta escala
de grises



Paleta escala
de colores



Modelo de Color RGB

- Emplea síntesis aditiva, es decir, suma colores para obtener nuevos colores.
 - el color de inicio es el negro y la suma de todos los colores da blanco.
- Los colores se representan con 24 bits
 - 8 para cada componente RGB.
- Cada componente 8 bits: 256 posibles niveles color
- Tres canales de color: Rojo (R), Verde (G), Azul (B)

1 0 0 0 1 1 0 0

Azul

1 0 0 0 1 1 0 0

Verde

1 0 0 0 1 1 0 0

Rojo

¿Qué pixels se pueden usar?



Bit más significativo



Segundo bit más significativo



Tercer bit más significativo



Cuarto bit más significativo



Quinto bit más significativo

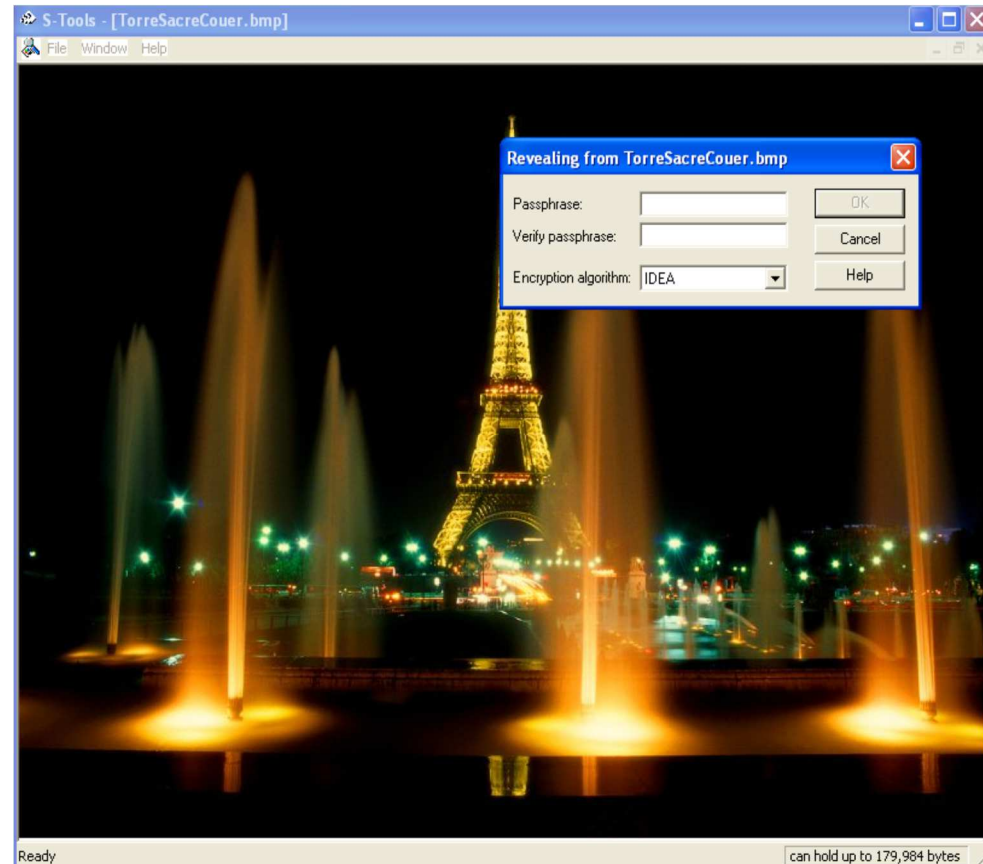


Sexto bit más significativo

<http://www.wayner.org/books/discrypt2/bitlevel.php>

¿Qué información podemos ocultar en una imagen?

- Dentro de una imagen podemos utilizar 1 ó 2 bits por cada canal de cada pixel.
 - Dichos bits pueden formar bytes
- Con bytes podemos almacenar cualquier tipo de información: texto, archivos de sonido, programas e incluso otras imágenes.
- Ejemplo herramienta:
 - Stools

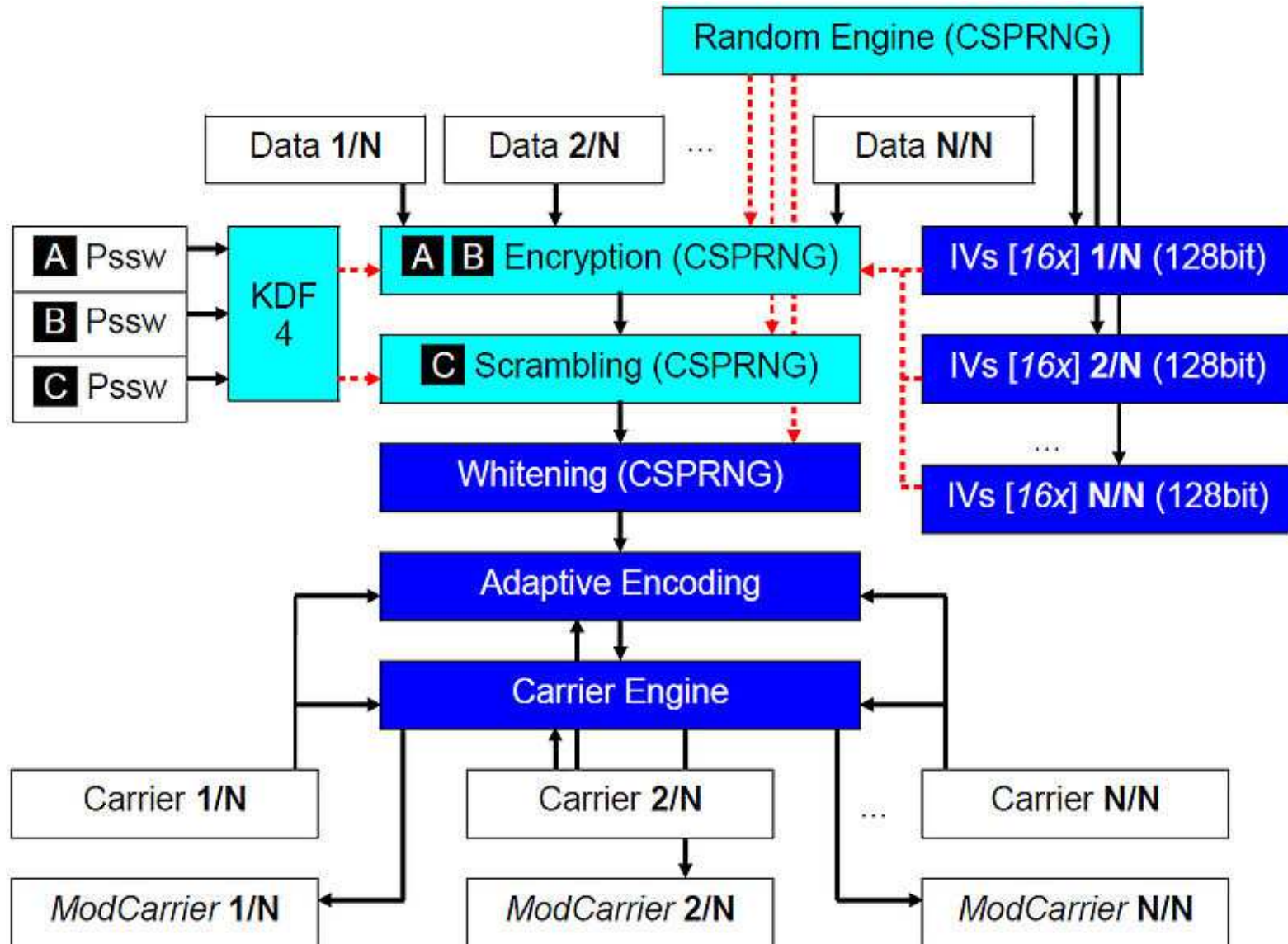


Otras herramientas esteganográficas

- Blindside
- BMP Secrets
- Covert.tcp
- dc-Steganograph
- EzStego
- FFEncode
- Gif-it-Up V1.0
- Gifshuffle
- Gzsteg
- Hide4 PGP
- Hide and Seek
- jpeg-jsteg
- MandelSteg
 - and GIF Extract
- MP3Stego
- MP3Stegz
- OpenPuff
- Outguess
- Paranoid
- PGE
 - Pretty Good Envelope
- PGPn123
- Publimark
- S-Tools
- Scytale
- Silent Eye
- Snow
- Stealth
- Steganos
- Steghide
- Stego
 - John Walker
- Stego
 - Romana Machado
- Stegonosaurus
- StegonoWav
- Stegodos
- Stegtunnel
- Texto
- wbStego
 - Werner Bailer
- WitnesSott
- Wnstorm
 - WhiteNoise Storm

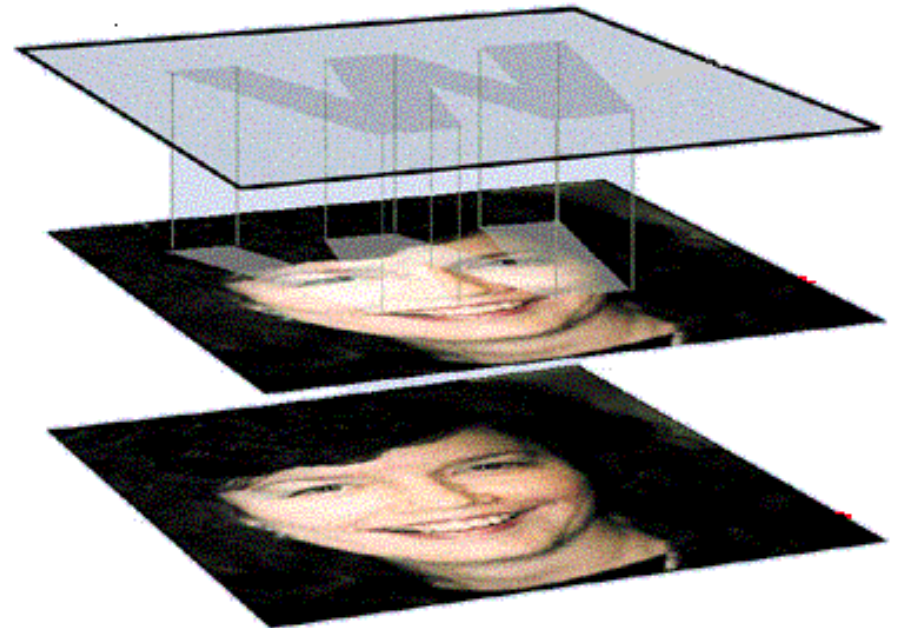
Fuentes: <http://www.jjtc.com/Security/stegtools.htm>
<http://www.jjtc.com/Steganography/toolmatrix.htm>
<http://stegano.net/tools>

Carrier chain (OpenPuff)



Esteganografía vs Watermarking

- Misma características esteganografía
- Robustez en contra de posibles ataques
 - esteganografía esta relacionada con la detección de un mensaje oculto, mientras que watermarking involucra el borrado/duplicación de un pirata
- Watermarking no siempre necesita estar oculto
- Tipos
 - invisible
 - visible



Marcas de agua visible e invisible



Imagen sin marca

+



Marca de agua

=



Imagen con marca

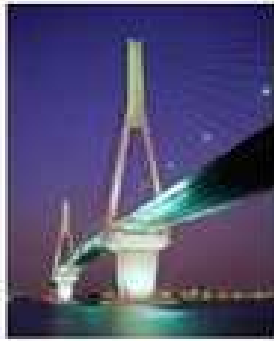


Imagen sin marca

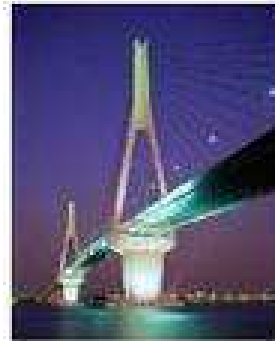


Imagen con marca



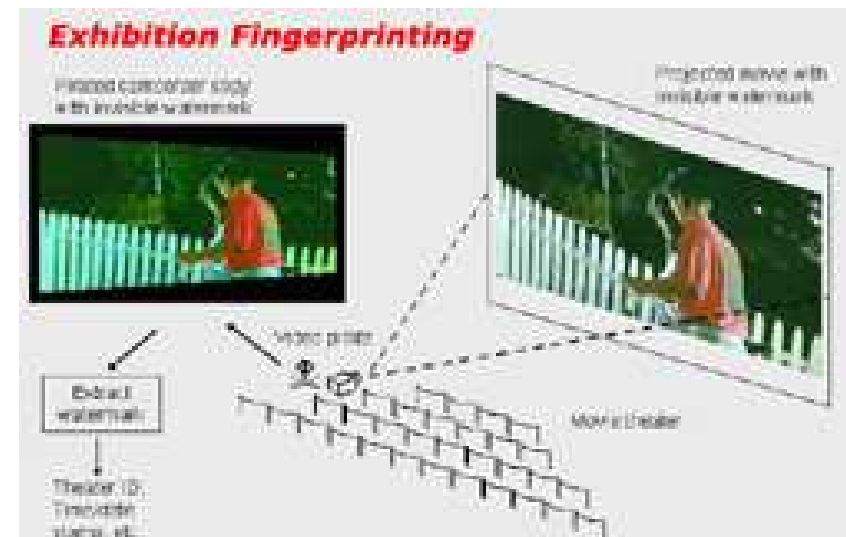
Marca de agua

Robustas vs frágiles

- Marcas de agua robustas
 - soportan un cierto grado de modificación, dependiendo de las necesidades de la aplicación.
 - tienen que considerar los ataques a los que pueden ser sometidas las imágenes marcadas
- Marcas de agua frágiles
 - son diseñadas para destruirse o modificarse ante cualquier distorsión sobre la imagen que la contiene, verificando así la integridad de la imagen.
 - algunas marcas de agua permiten localizar las áreas en el espacio que han sido afectadas, e incluso caracterizar cierto tipo de distorsión

Esteganografía vs Watermarking

- La información ocultada por un sistema de marca de agua, siempre se asocia al objeto digital a ser protegido.
- Comunicaciones esteganograficas son del tipo punto a punto, mientras que watermarking son del tipo punto-multipunto.
- Software
 - AiS Watermark Pictures Protector
 - Easy Watermark Creator
 - Alphatec Watermarking Suite 1.0
- Software de prueba
 - StirMark Benchmark 4 I
 - AudioStirMark
- Referencias:
 - <http://www.elis.ugent.be/~banckaer/watermarking.html>



Stegoanálisis

- Arte de descubrir y convertir los mensajes en no útiles.
- Ataques y análisis de información oculta pueden tomar diferentes formas:
 - Detección: solo detectar contenido esteganográfico
 - Extracción: quitar la información
 - Confusión: alteración, introducción, dejar inservible la información almacenada
 - Deshabilitación de la información oculta
- Muchos casos requieren contar con porciones del objeto encubierto (stego-object) y posibles porciones del mensaje.
 - Resultado: el stego-object

Métodos de detección Steganografía

- Detección Visual
 - JPEG, BMP, GIF, etc.
- Detección Auditiva
 - WAV, MPEG, etc.
- Detección estadística o análisis de histogramas
 - Cambios en los patrones de los píxeles o LSB
 - Histograma: resumen gráfico de la variación de un conjunto de datos
- Detección estructural: verificar propiedades/contenidos de archivos
 - Diferencia en el tamaño del archivo
 - Diferencias en tiempo y fecha
 - Modificaciones del contenido
 - Checksum

Detección estructural

- Comparar las propiedades de los archivos
- Propiedades:
 - 04/04/2003 05:25p 240,759 helmetprototype.jpg
 - 04/04/2003 05:26p 235,750 helmetprototype.jpg
- Checksum
 - C:\GNUTools>cksum a:\before\helmetprototype.jpg
3241690497 240759 a:\before\helmetprototype.jpg
 - C:\GNUTools>cksum a:\after\helmetprototype.jpg
3749290633 235750 a:\after\helmetprototype.jpg

Detección visual



Imagen original



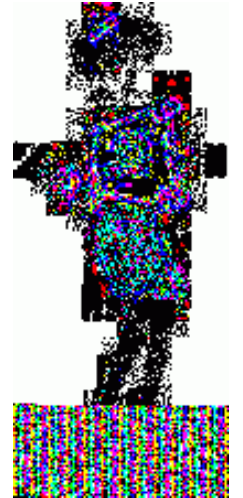
LSB resaltados
imagen pura



LSB resaltados
con 1KB de datos
aleatorios



LSB resaltados
con 5KB de datos
aleatorios



LSB resaltados
con poema "if"
(1.5 Kb)

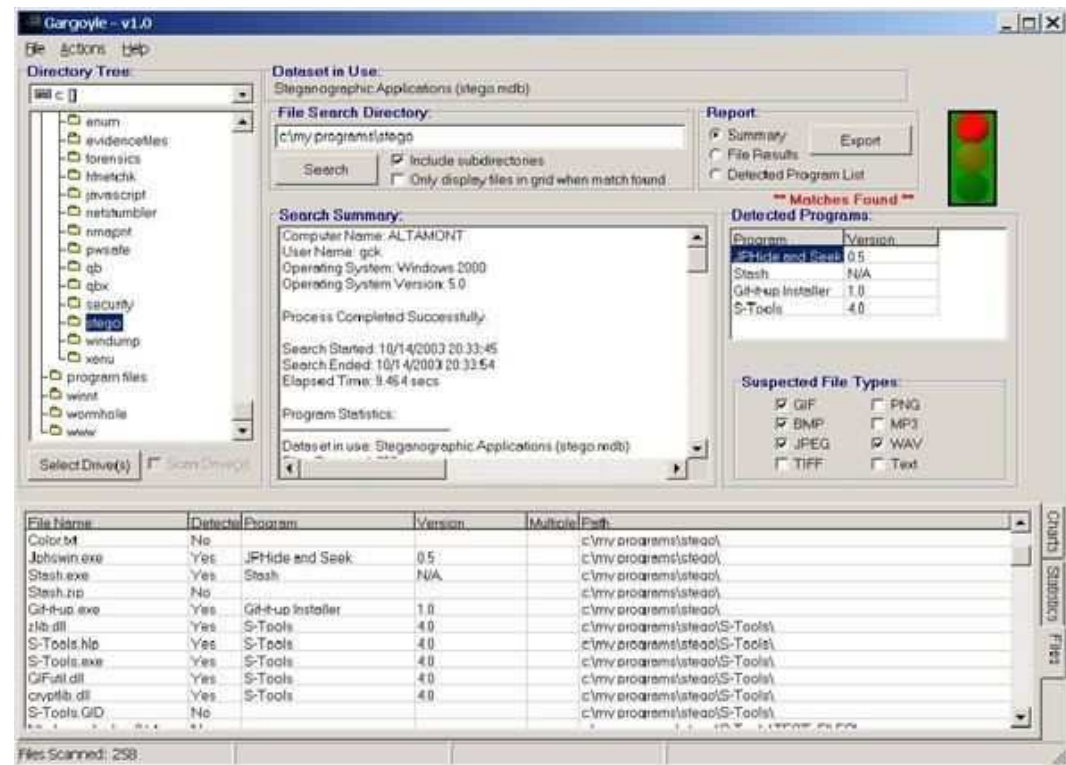
Fuente; <http://www.guillermi2.net>

Detección software esteganográfico

- Necesario saber si en la computadora existe software esteganográfico y cual es este.
- Una vez detectado se puede proceder a un análisis más dirigido de los archivos sospechosos.
- A tomar en cuenta
 - Software esteganográfico en un medio de almacenamiento portable.

Gargoyle (StegoDetect)

- Detección de software esteganográfico en base a un conjunto de datos (hash set) propietario de los archivos de software esteganográfico.
- También puede ser usado para detectar la presencia de otro tipo de software
 - Criptografía, SMS, cracks

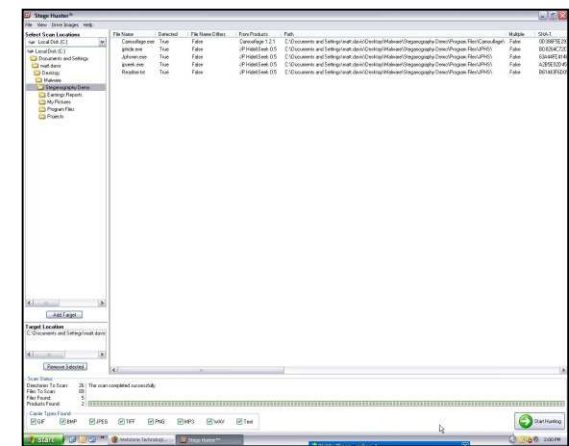
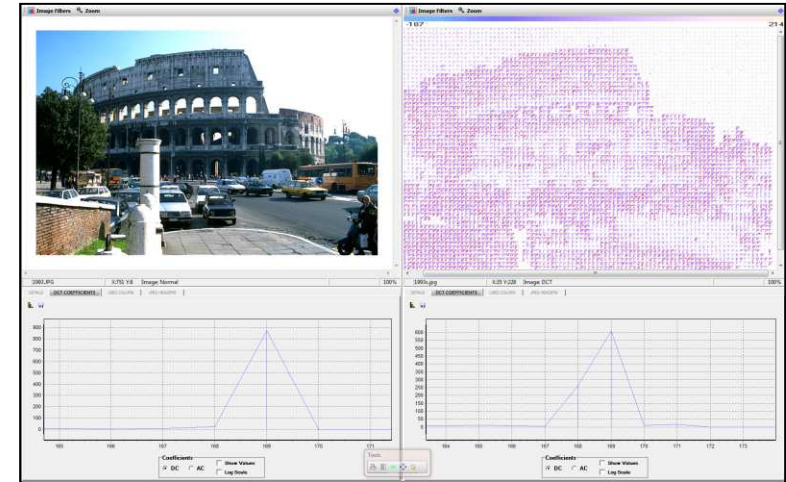


Forensic Toolkit y EnCase

- Detección de software esteganográfico
 - Pueden usar el HashKeeper, Maresware, y National Software Reference Library.
- A tomar en cuenta
 - Tamaño software esteganográfico en comparación con capacidad medios de almacenamiento temporal

Stego Suite = Stego Hunter

- Conjunto de herramientas para investigación forense
- Herramientas que se incluyen
 - Stego Hunter
 - Stego Analyst
 - Stego Break
- Producido por WetStone Technologies
 - <https://www.wetstonetech.com/>



Introducción a la Esteganografía

Roberto Gómez Cárdenas

rogomez@itesm.mx

<http://cryptomex.org>