Ocultando tu información privada a miradas indiscretas

HACK &BEERS *Tarragona*
Noviembre 2015

Rafael Páez
@fikih888

Presentación

Rafael Páez

- Ingeniero superior en informática
- Máster universitario de Seguridad en las Tecnologías de la Información y de las Comunicaciones (MISTIC)
- Offensive Security Certified Professional (OSCP)
- Cybersecurity Auditor
- Wargames and CTFs
- Twitter: @fikih888

Contenidos

1. ¿Qué es la esteganografía?
2. Historia de la esteganografía
3. Esteganografía en la actualidad
4. Técnicas de esteganografía
5. Least Significant Bit en profundidad
6. Dificultando el descubrimiento
7. Posibles usos

Contenidos

1. ¿Qué es la esteganografía?
2. Historia de la esteganografía
3. Esteganografía en la actualidad
4. Técnicas de esteganografía
5. Least Significant Bit en profundidad
6. Dificultando el descubrimiento
7. Posibles usos

¿Qué es la esteganografía?

Definición:

La esteganografía es la disciplina en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos, dentro de otros, de modo que no se perciba su existencia.

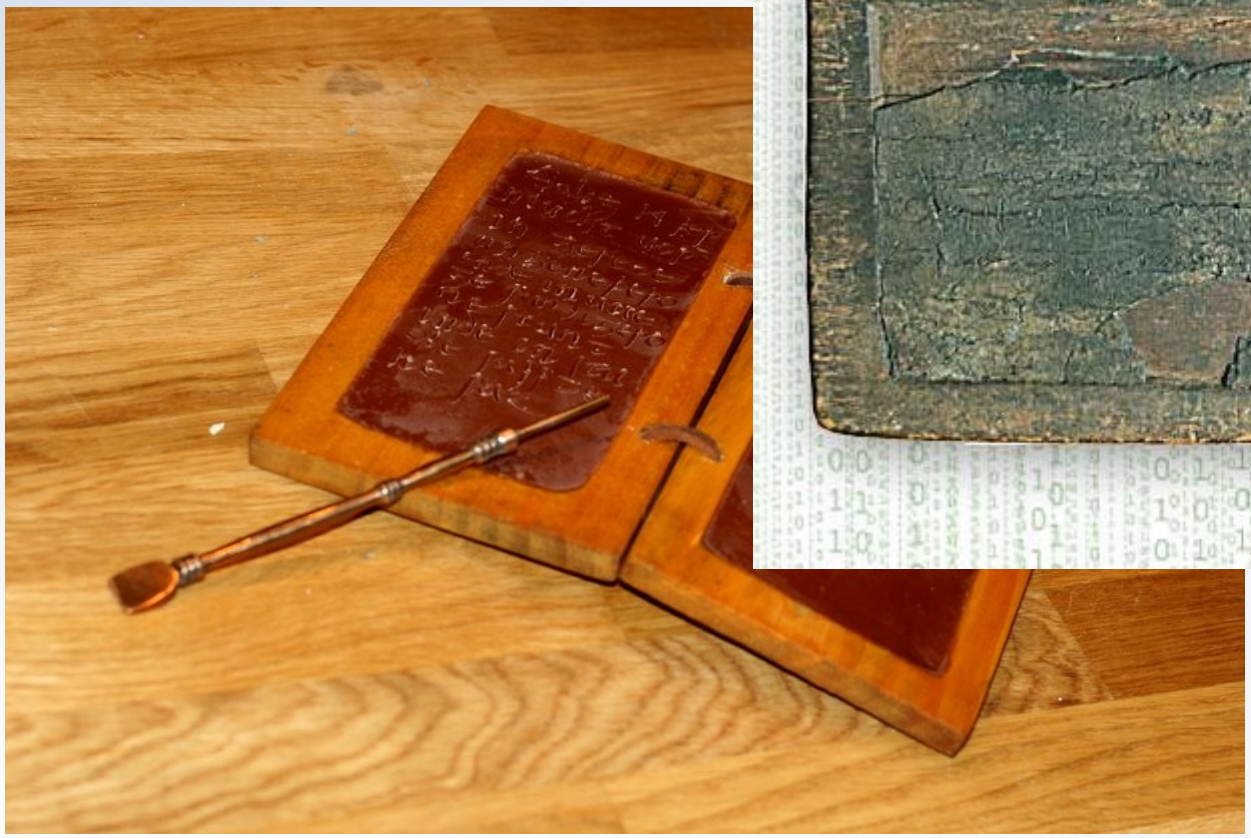
Contenidos

1. ¿Qué es la esteganografía?
2. Historia de la esteganografía
3. Esteganografía en la actualidad
4. Técnicas de esteganografía
5. Least Significant Bit en profundidad
6. Dificultando el descubrimiento
7. Posibles usos

Tablas de cera

Historia de la esteganografía

Tablas de cera

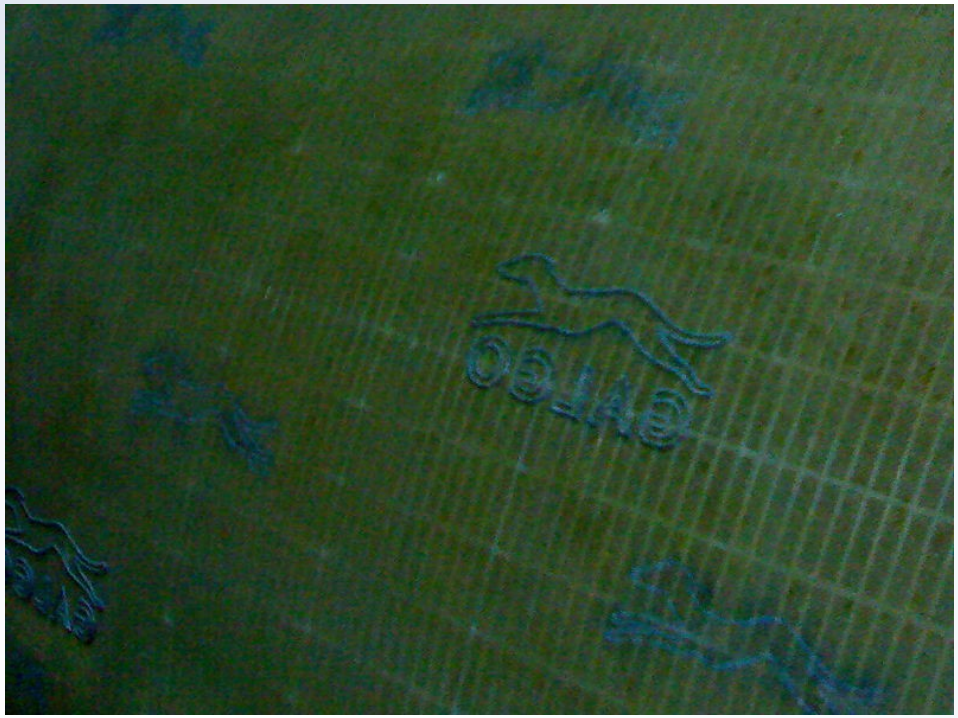


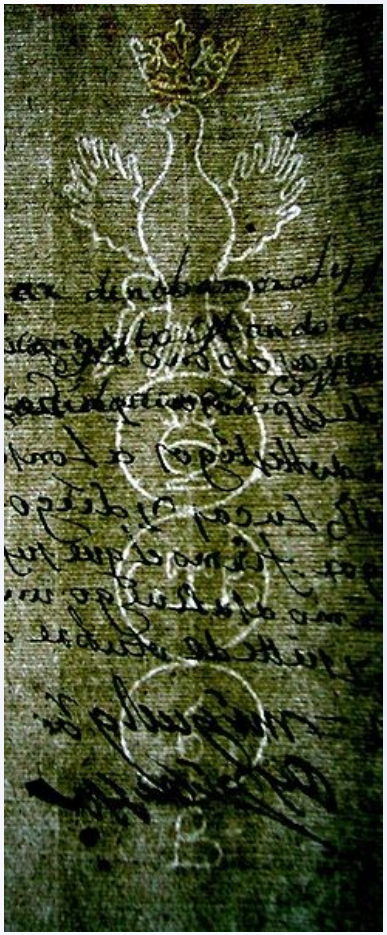
Historia de la esteganografía

Tablas de cera

Escritura en cuero cabelludo

Filigranas papel





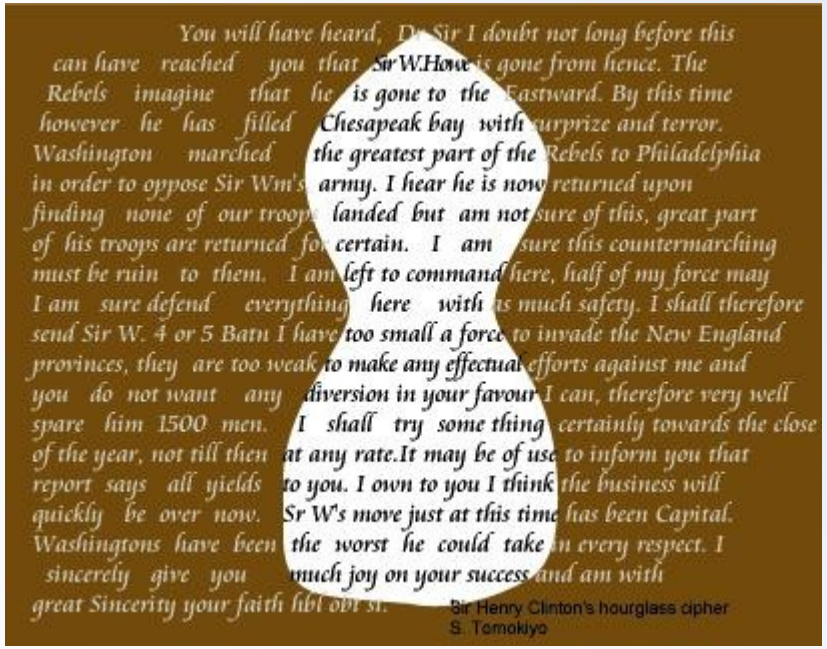
Tinta invisible

Tinta invisible

Tinta invisible

Historia de la esteganografía

Textos y libros



Contenidos

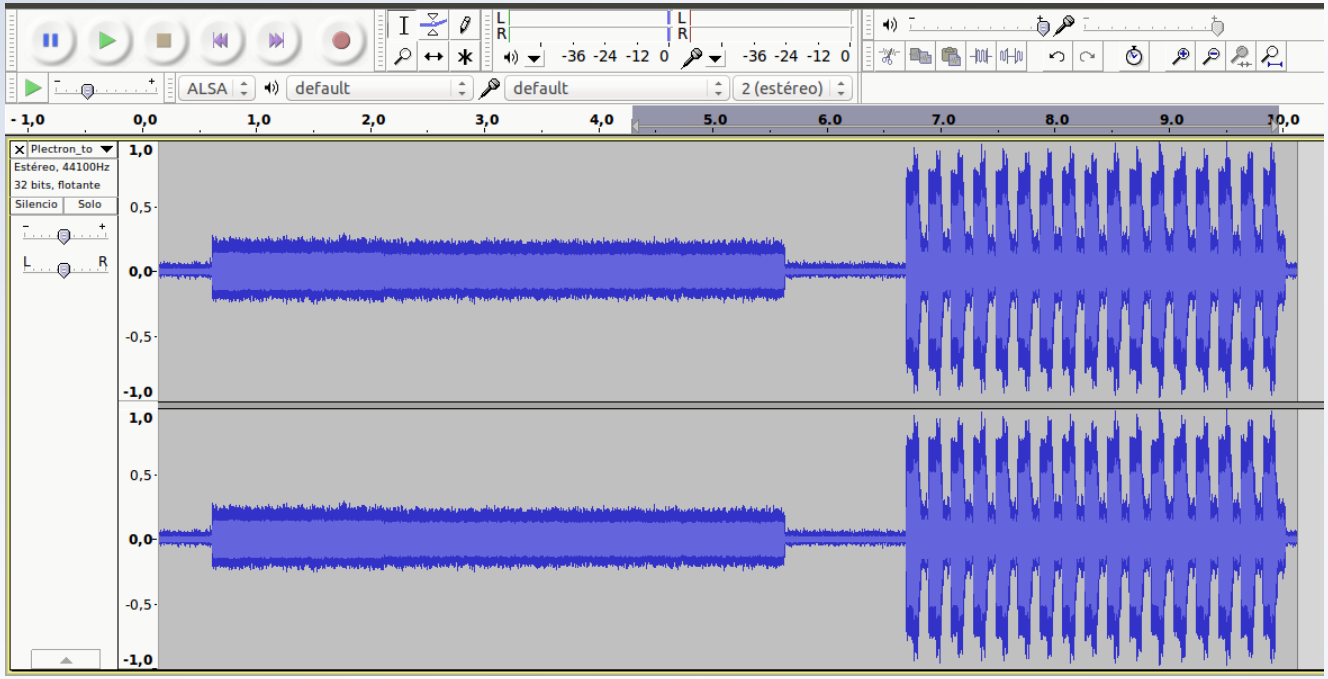
1. ¿Qué es la esteganografía?
2. Historia de la esteganografía
3. Esteganografía en la actualidad
4. Técnicas de esteganografía
5. Least Significant Bit en profundidad
6. Dificultando el descubrimiento
7. Posibles usos

Esteganografía en la actualidad

Imágenes

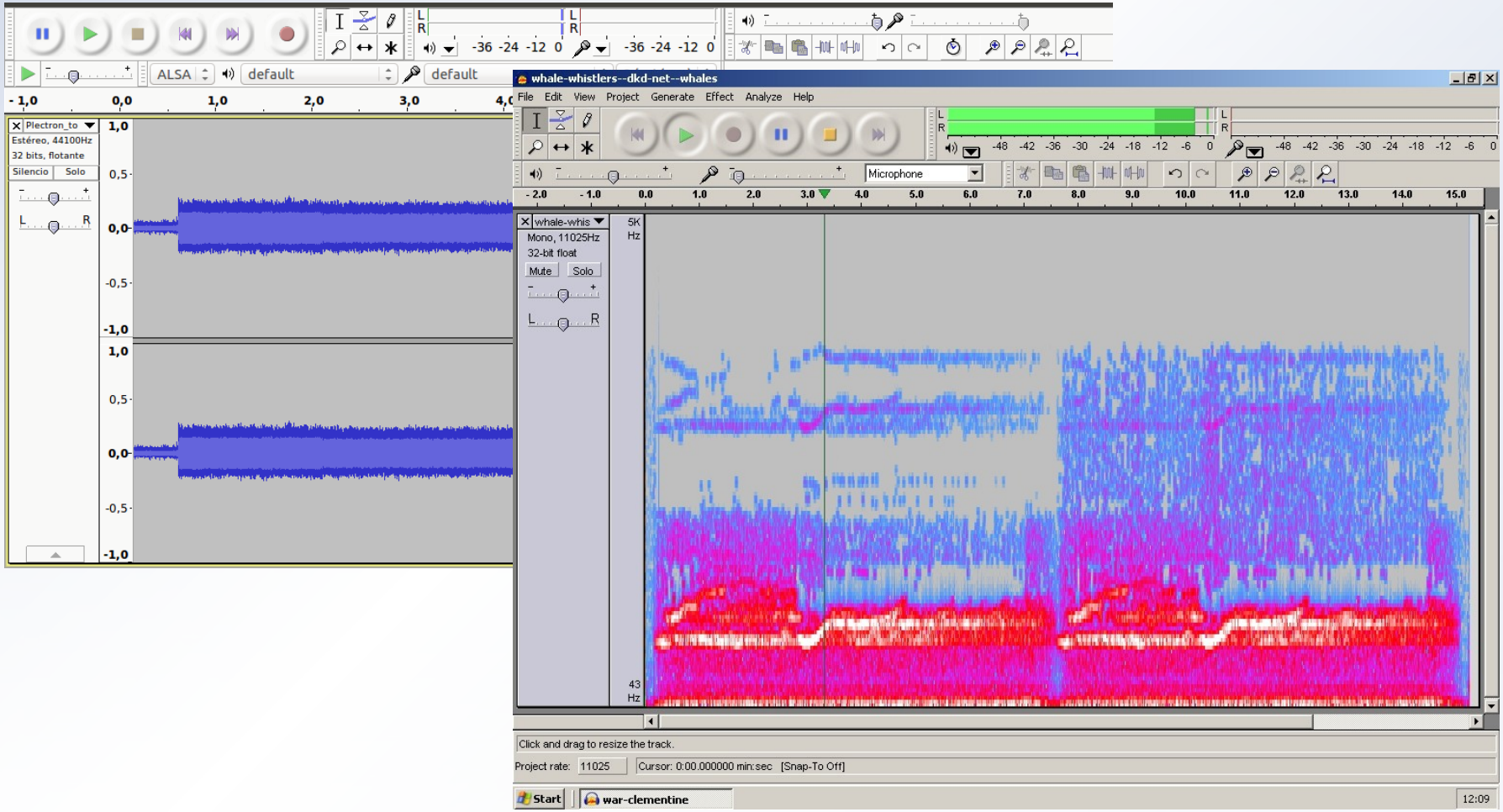
Esteganografía en la actualidad

Audio



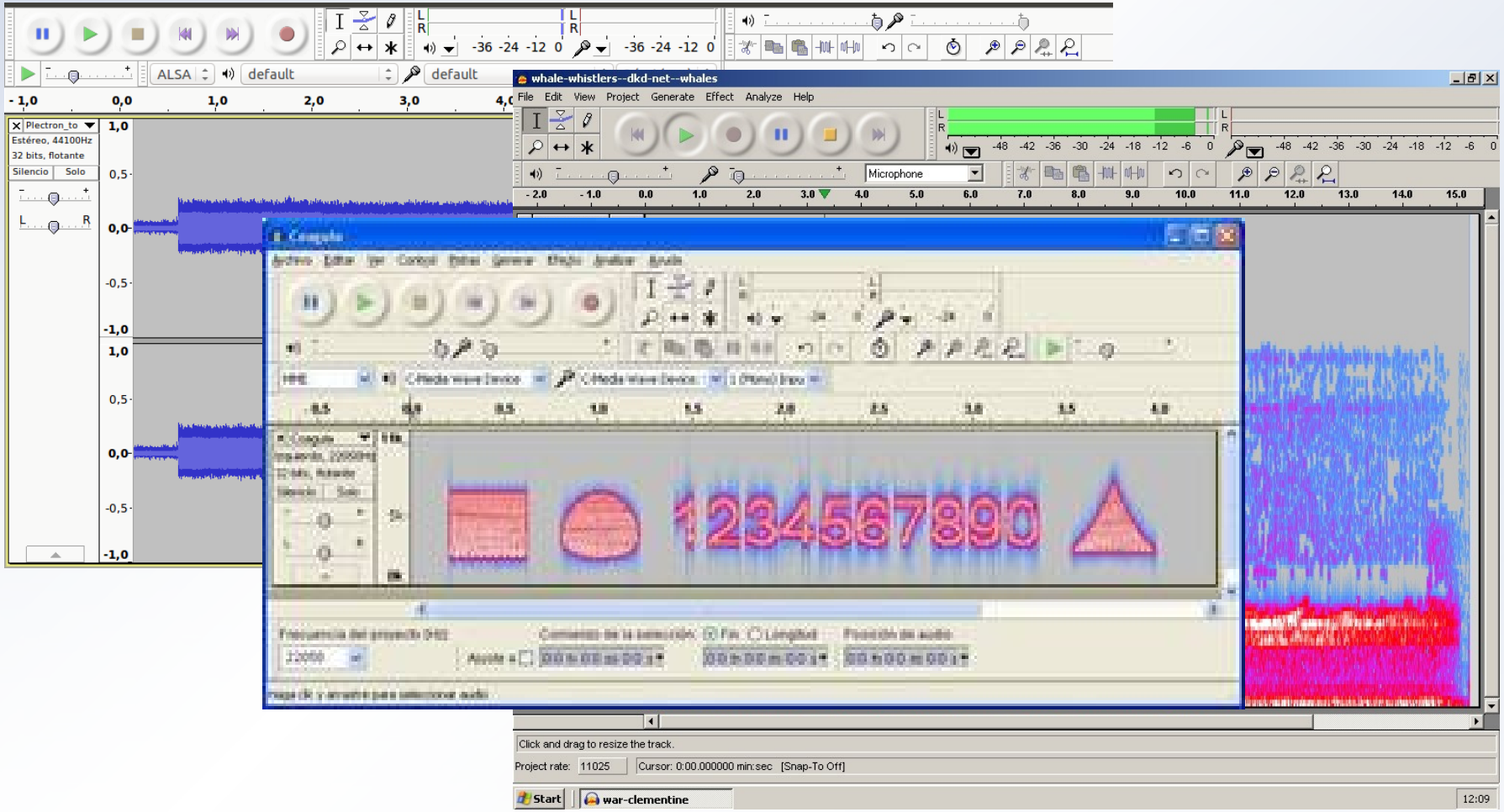
Esteganografía en la actualidad

Audio



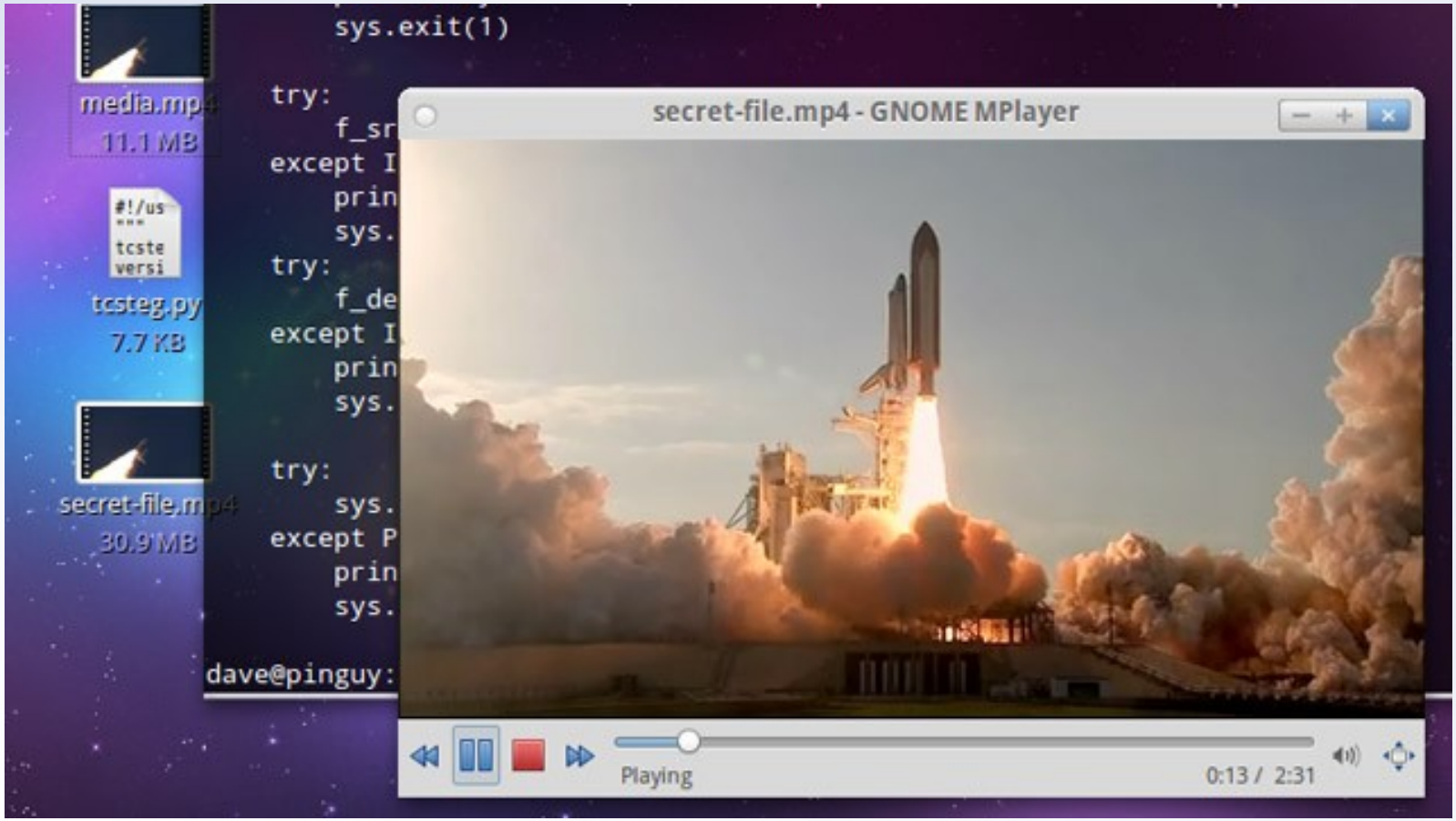
Esteganografía en la actualidad

Audio



Esteganografía en la actualidad

Vídeos



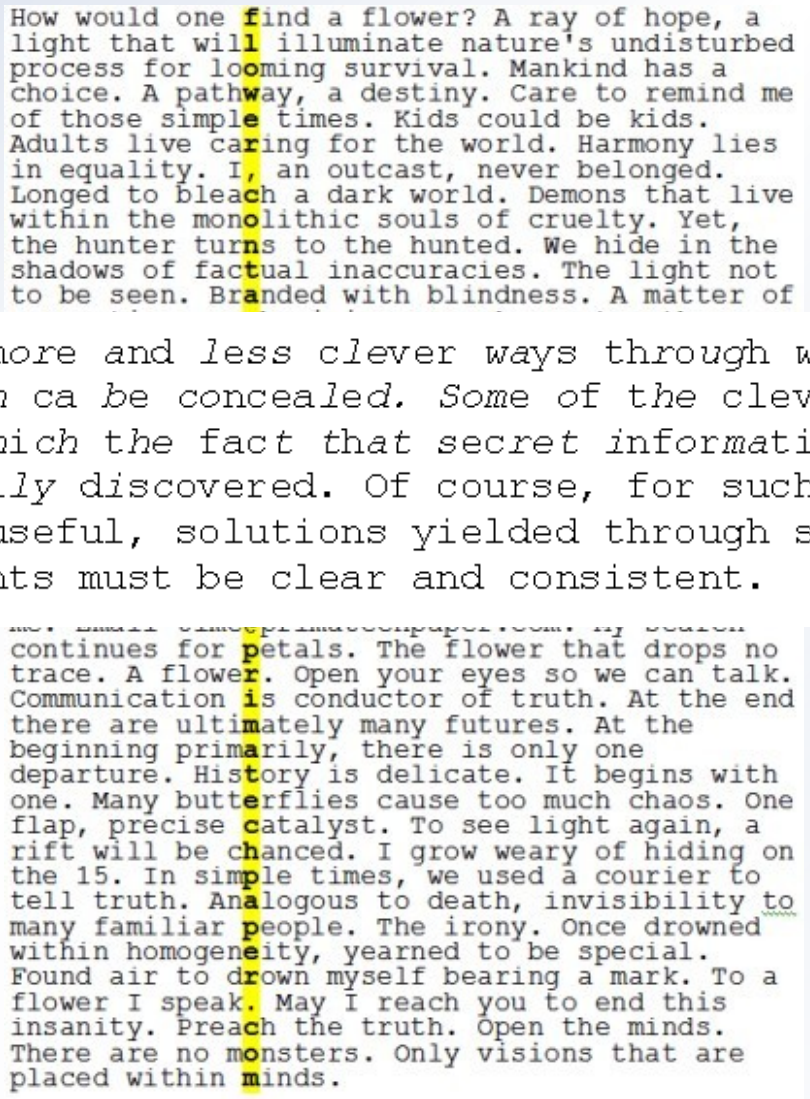
Esteganografía en la actualidad

Texto

How would one find a flower? A ray of hope, a light that will illuminate nature's undisturbed process for looming survival. Mankind has a choice. A pathway, a destiny. Care to remind me of those simple times. Kids could be kids. Adults live caring for the world. Harmony lies in equality. I, an outcast, never belonged. Longed to bleach a dark world. Demons that live within the monolithic souls of cruelty. Yet, the hunter turns to the hunted. We hide in the shadows of factual inaccuracies. The light not to be seen. Branded with blindness. A matter of perception, such visions speak greater than words. Pleasantly resolved, convenient for humanity. When will I be free? When will we be free? Fates timed to precision. We follow a path. It crosses with each other. Realize the moment. Awaken. Unite. Ambivalence is not a solution. Blackness is resolved with truth. Love. Beyond walls of hatred, lies purity. Prisoners of silence. Lacking a leader, we have common goals at the core. Trust no one. Fight to avenge and open the eyes of the beast. Prejudice spawns like spores. Find me. Reach me. Email time@primatechpaper.com. My search continues for petals. The flower that drops no trace. A flower. Open your eyes so we can talk. Communication is conductor of truth. At the end there are ultimately many futures. At the beginning primarily, there is only one departure. History is delicate. It begins with one. Many butterflies cause too much chaos. One flap, precise catalyst. To see light again, a rift will be chanced. I grow weary of hiding on the 15. In simple times, we used a courier to tell truth. Analogous to death, invisibility to many familiar people. The irony. Once drowned within homogeneity, yearned to be special. Found air to drown myself bearing a mark. To a flower I speak. May I reach you to end this insanity. Preach the truth. Open the minds. There are no monsters. Only visions that are placed within minds.

Esteganografía en la actualidad

Texto



How would one find a flower? A ray of hope, a light that will illuminate nature's undisturbed process for looming survival. Mankind has a choice. A pathway, a destiny. Care to remind me of those simple times. Kids could be kids. Adults live caring for the world. Harmony lies in equality. I, an outcast, never belonged. Longed to bleach a dark world. Demons that live within the monolithic souls of cruelty. Yet, the hunter turns to the hunted. We hide in the shadows of factual inaccuracies. The light not to be seen. Branded with blindness. A matter of

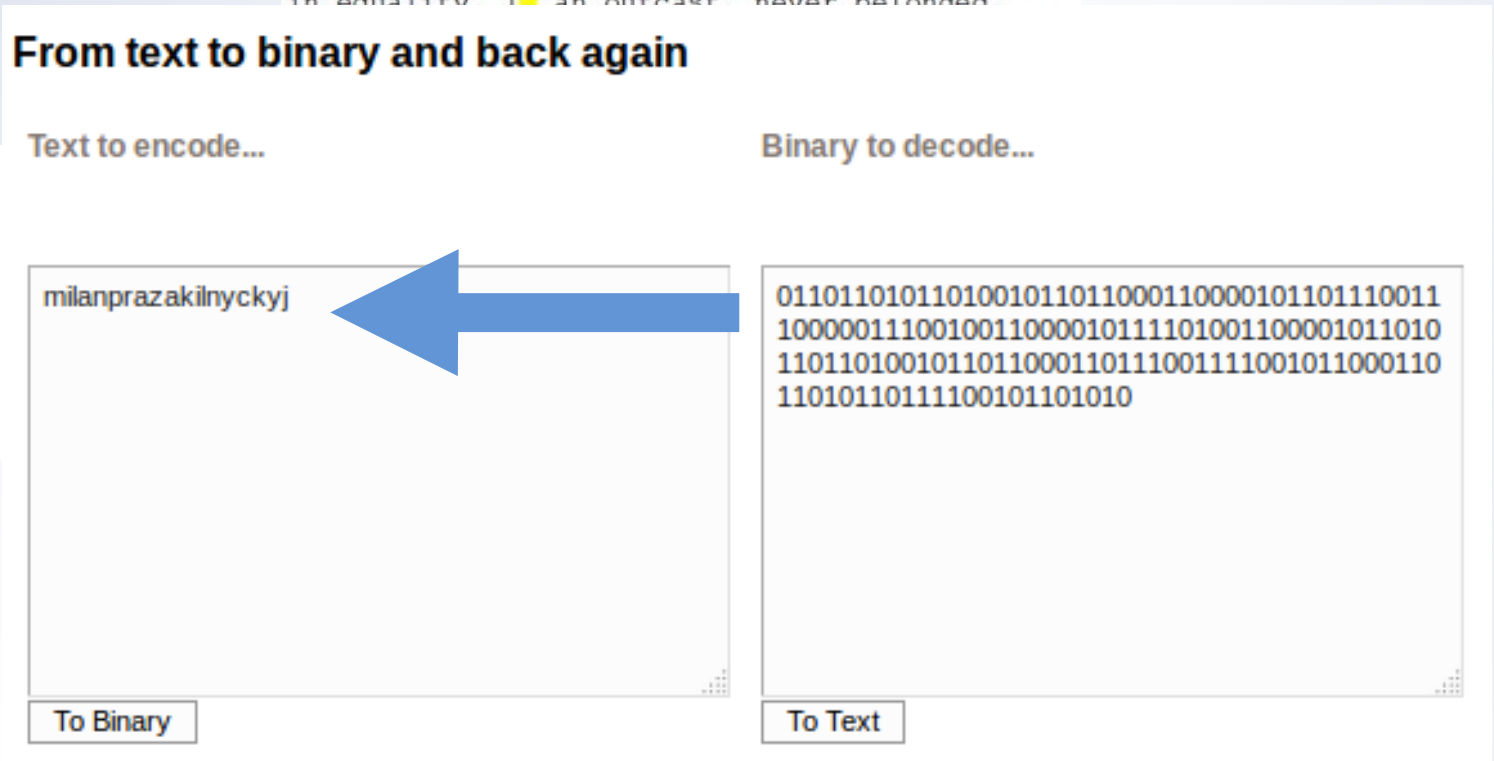
There are more and less clever ways through which information ca be concealed. Some of the cleverest are those in which the fact that secret information is present is not easily discovered. Of course, for such systems to be genuinely useful, solutions yielded through sensible decipherments must be clear and consistent.

continues for petals. The flower that drops no trace. A flower. Open your eyes so we can talk. Communication is conductor of truth. At the end there are ultimately many futures. At the beginning primarily, there is only one departure. History is delicate. It begins with one. Many butterflies cause too much chaos. One flap, precise catalyst. To see light again, a rift will be chanced. I grow weary of hiding on the 15. In simple times, we used a courier to tell truth. Analogous to death, invisibility to many familiar people. The irony. Once drowned within homogeneity, yearned to be special. Found air to drown myself bearing a mark. To a flower I speak. May I reach you to end this insanity. Preach the truth. Open the minds. There are no monsters. Only visions that are placed within minds.

Esteganografía en la actualidad

Texto

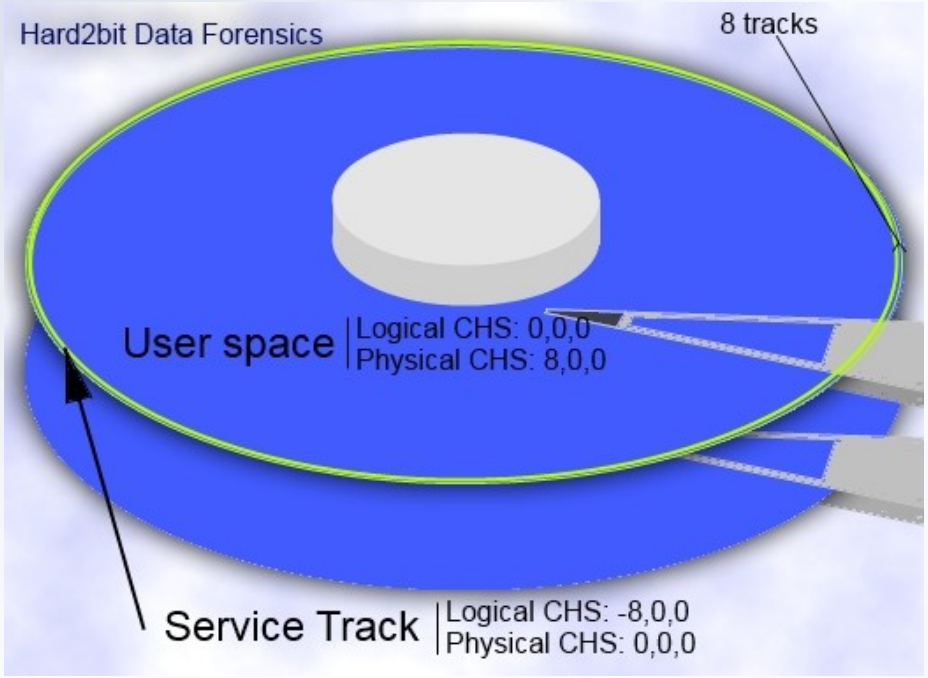
How would one find a flower? A ray of hope, a light that will illuminate nature's undisturbed process for looming survival. Mankind has a choice. A pathway, a destiny. Care to remind me of those simple times. Kids could be kids. Adults live caring for the world. Harmony lies in equality. I, an outcast, never belonged



within homogeneity, yearned to be special. Found air to drown myself bearing a mark. To a flower I speak. May I reach you to end this insanity. Preach the truth. Open the minds. There are no monsters. Only visions that are placed within minds.

Esteganografía en la actualidad

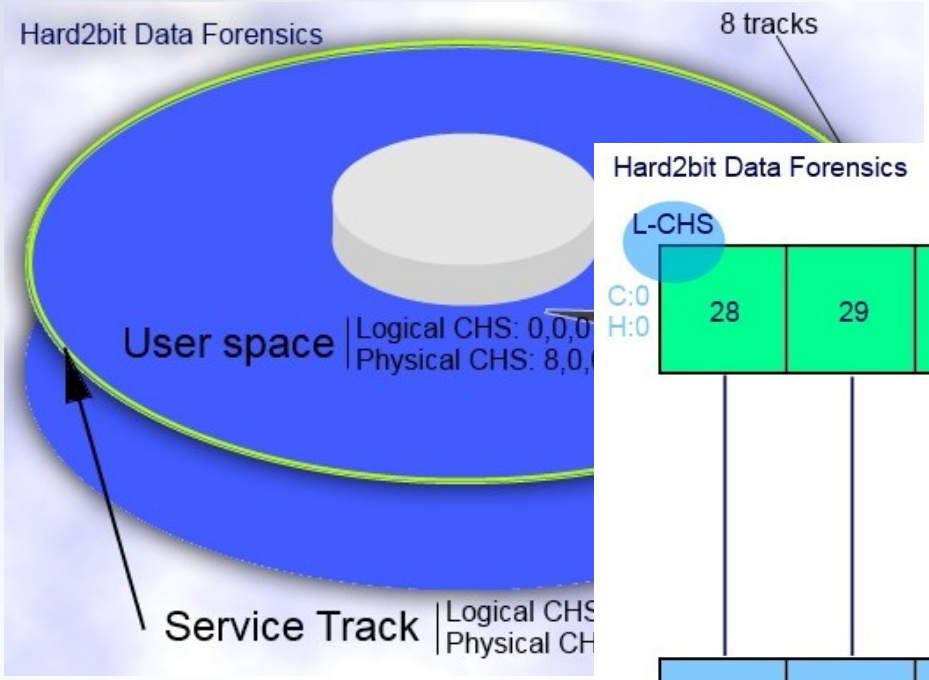
Discos duros

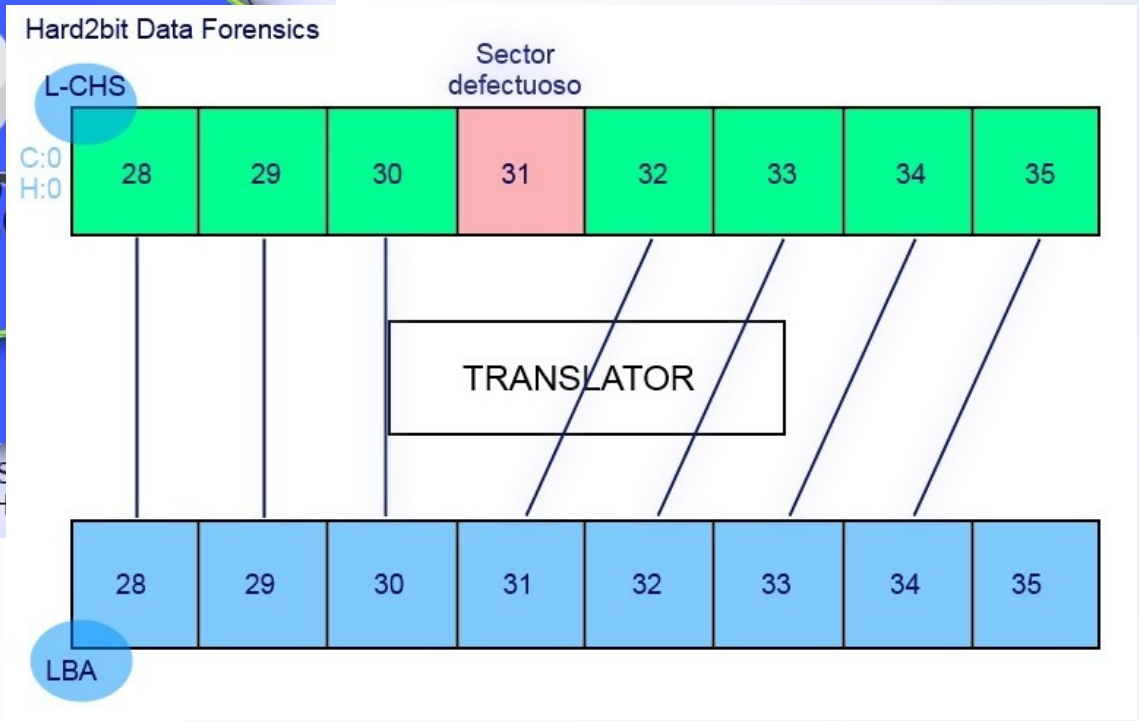


https://hard2bit.com/blog/como-ocultar-datos-en-un-disco-duro-de-casi-cualquier-pericial-informatico-forense-sin-usar-cifrado-ni-esteganografia/

Esteganografía en la actualidad

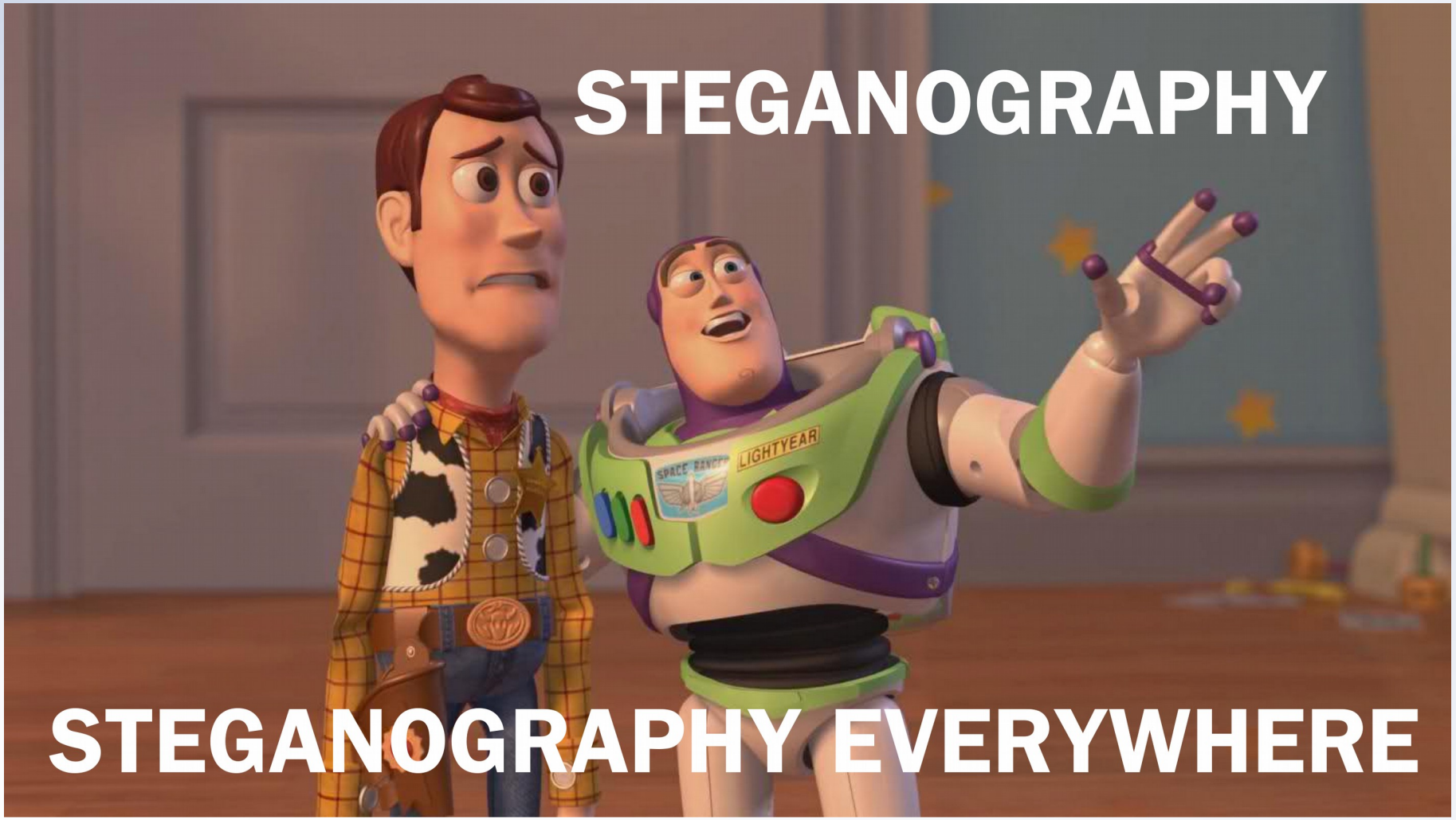
Discos duros





https://hard2bit.com/blog/como-ocultar-datos-en-un-disco-duro-de-casi-cualquier-pericial-informatico-forense-sin-usar-cifrado-ni-esteganografia/

Esteganografía en la actualidad



Contenidos

1. ¿Qué es la esteganografía?
2. Historia de la esteganografía
3. Esteganografía en la actualidad
4. Técnicas de esteganografía
5. Least Significant Bit en profundidad
6. Dificultando el descubrimiento
7. Posibles usos

Metadatos

Metadatos


fikih888@h&b_tgn $ exif meta2.jpg
Etiquetas EXIF en 'meta2.jpg' ('Intel' es el orden de bytes):
Etiqueta |Valor
Fabricante |CANON
Modelo |ThE p4Ssw0rd is: StEga0nO RockS!
Orientación |Superior izquierda
Resolución X |72
Resolución Y |72
Unidad de resolución|Pulgadas
Fecha y hora |2014:06:01 04:50:08
Fecha y hora (Origin|2014:06:01 04:50:08
Fecha y hora (Digita|2014:06:01 04:50:08
Configuración de com|Y Cb Cr -
Espacio de color |sRGB
Dimensión píxel X |2816
Dimensión píxel Y |2112
Versión Exif |Versión Exif 2.1
FlashPixVersion |FlashPix Version 1.0

Thumbnail

Thumbnail

Demo...

Thumbnail

End Of File (EOF)

Algo Más...

End Of File (EOF)

Algo Más...

Demo...

End Of File (EOF)

Algo Más...

Texto secreto:

Que buen sitio para ocultar informacion no? :)

End Of File (EOF)

Algo Más...

Texto secreto:

Que buen sitio para ocultar informacion no? :)

End Of File (EOF)

Algo Más...

Demo...

Texto secreto:

Que buen sitio para ocultar informacion no? :)

End Of File (EOF)

Algo Más...

Texto secreto:

Que buen sitio para ocultar informacion no? :)

Estructura de archivos

Can you see the secret?

Estructura de archivos

Can you see the secret?

header1_721x208.pgm

```
00000000 50 35 0A 23 20 66 69 6B 69 68 38 38 38 3A 20 43 61 6E 20 79 30 75 20 P5.# fikih888: Can y0u
00000017 73 33 33 20 74 68 34 20 73 33 63 52 65 74 3F 20 3A 50 0A 37 32 31 20 s33 th4 s3cRet? :P.721
0000002e 30 37 31 0A 32 35 35 0A 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 071.255.............
00000045 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F .....................
```

Estructura de archivos

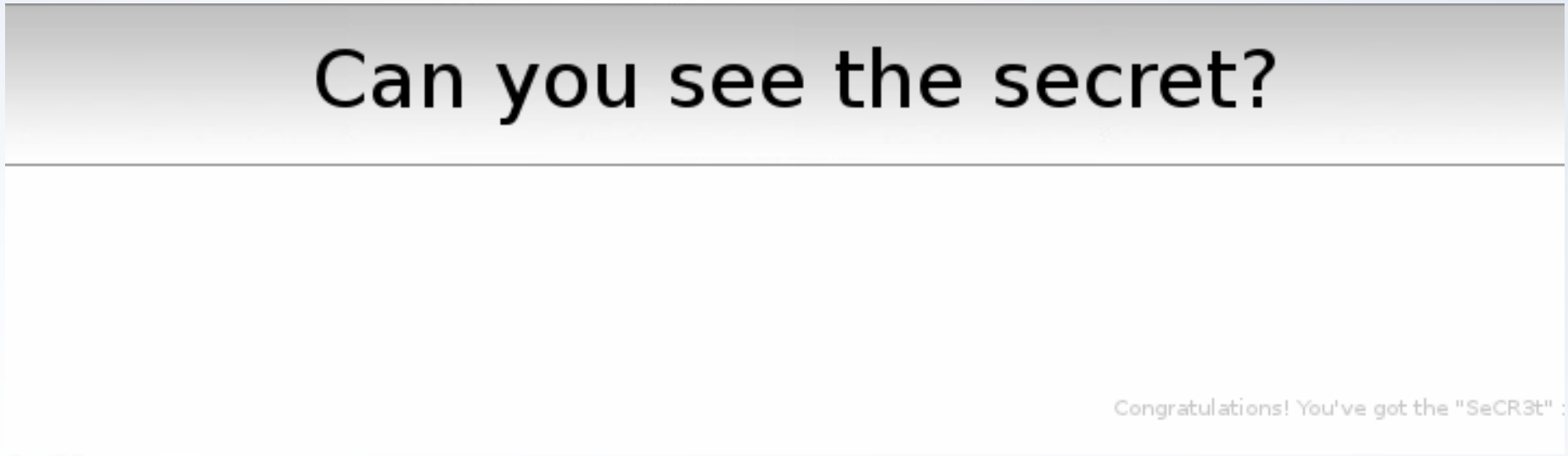
header1_721x208.pgm

```
00000000 50 35 0A 23 20 66 69 6B 69 68 38 38 38 3A 20 43 61 6E 20 79 30 75 20 P5.# fikih888: Can y0u
00000017 73 33 33 20 74 68 34 20 73 33 63 52 65 74 3F 20 3A 50 0A 37 32 31 20 s33 th4 s3cRet? :P.721
0000002e 30 37 31 0A 32 35 35 0A 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 208.255.............
00000045 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F .....................
```

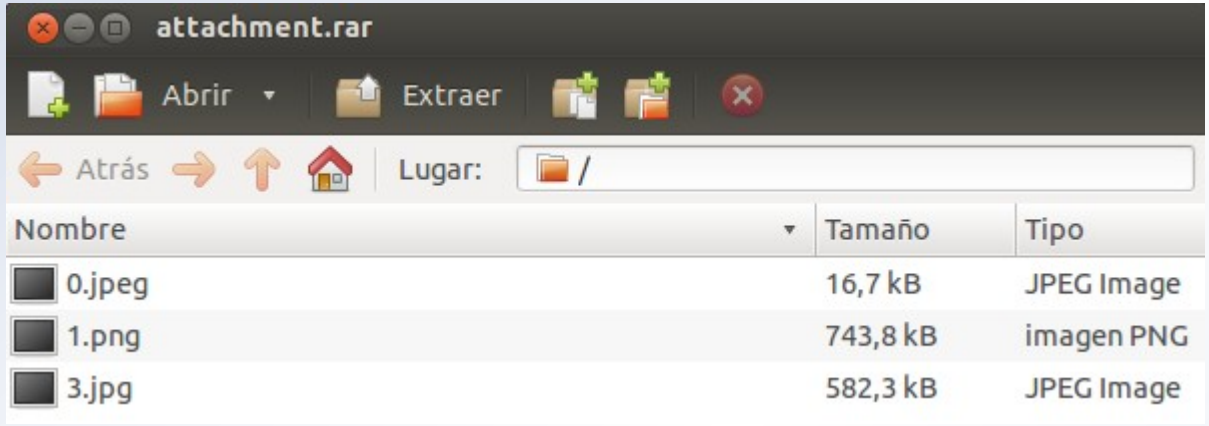
Estructura de archivos

header1_721x208.pgm

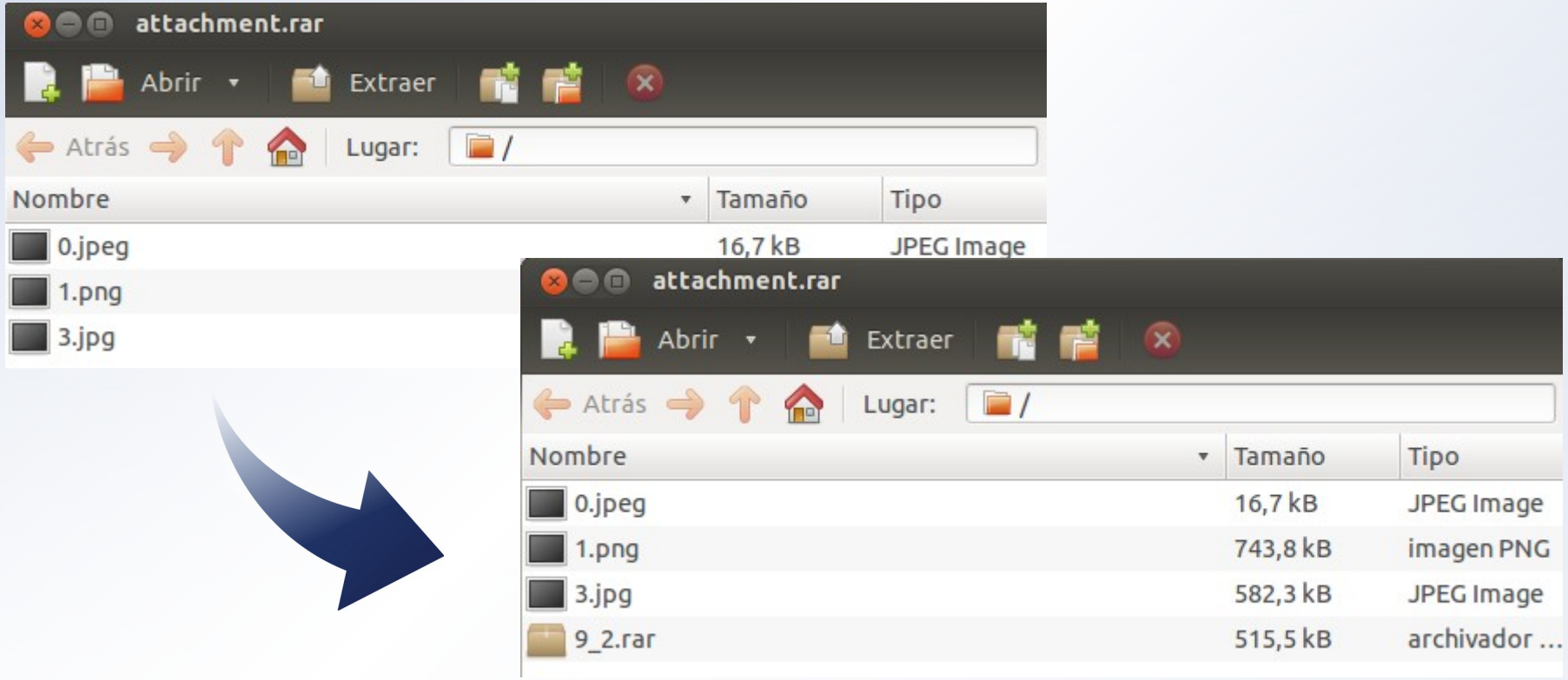
```
00000000 50 35 0A 23 20 66 69 6B 69 68 38 38 38 3A 20 43 61 6E 20 79 30 75 20 P5.# fikih888: Can y0u
00000017 73 33 33 20 74 68 34 20 73 33 63 52 65 74 3F 20 3A 50 0A 37 32 31 20 s33 th4 s3cRet? :P.721
0000002e 30 37 31 0A 32 35 35 0A 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 208.255.............
00000045 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F .....................
```



Hidden files in RAR



Hidden files in RAR



http://kthoom.googlecode.com/hg/docs/unrar.html#MHD_ENCRYPTVER

Hidden files in RAR

2 General Format of a .RAR File

Overall .RAR file format:

```
   signature              7 bytes    (0x52 0x61 0x72 0x21 0x1A 0x07 0x00)
   [1st volume header]
   ...
   [2nd volume header]
   ...
   ...
   [nth volume header]
   ...
```

In general, a modern single-volume RAR file has a MAIN_HEAD structure followed by multiple FILE_HEAD structures.

Hidden files in RAR

2.1 Volume Header Format

The Base Header Block is:

```
   header_crc              2 bytes
   header_type             1 byte
   header_flags            2 bytes
   header_size             2 bytes
```

The header_size indicates how many total bytes the header requires. The header_type field determines how the remaining bytes should be interpreted.

2.1.1 Header Type

The header type is 8 bits (1 byte) and can have the following values:

Value	Type
0x72	MARK_HEAD
0x73	MAIN_HEAD
0x74	FILE_HEAD
0x75	COMM_HEAD
0x76	AV_HEAD
0x77	SUB_HEAD
0x78	PROTECT_HEAD
0x79	SIGN_HEAD
0x7a	NEWSUB_HEAD
0x7b	ENDARC_HEAD

2.1.1.1 MARK_HEAD

TBD

2.1.1.2 MAIN_HEAD

The remaining bytes in the volume header for MAIN_HEAD are:

```
   HighPosAv               2 bytes
   PosAV                   4 bytes
   EncryptVer              1 byte (only present if MHD_ENCRYPTVER is set)
```

Hidden files in RAR

Demo...

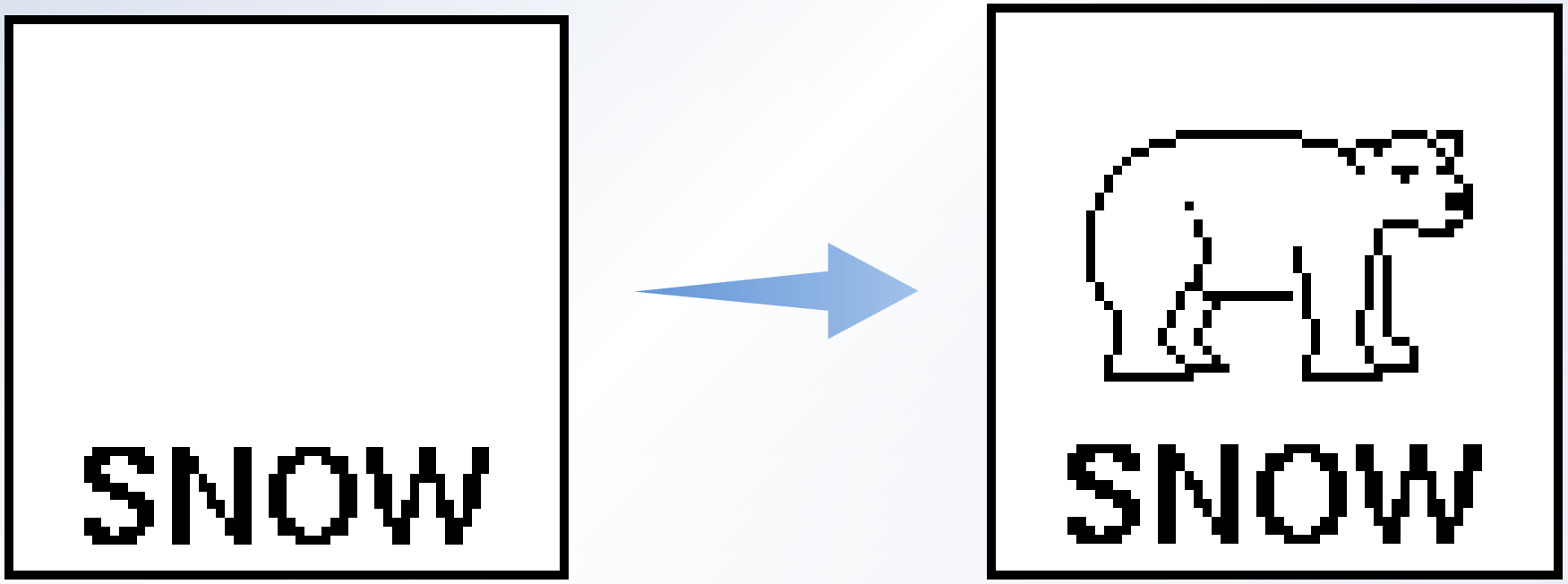
Colores semblantes

Colores semblantes

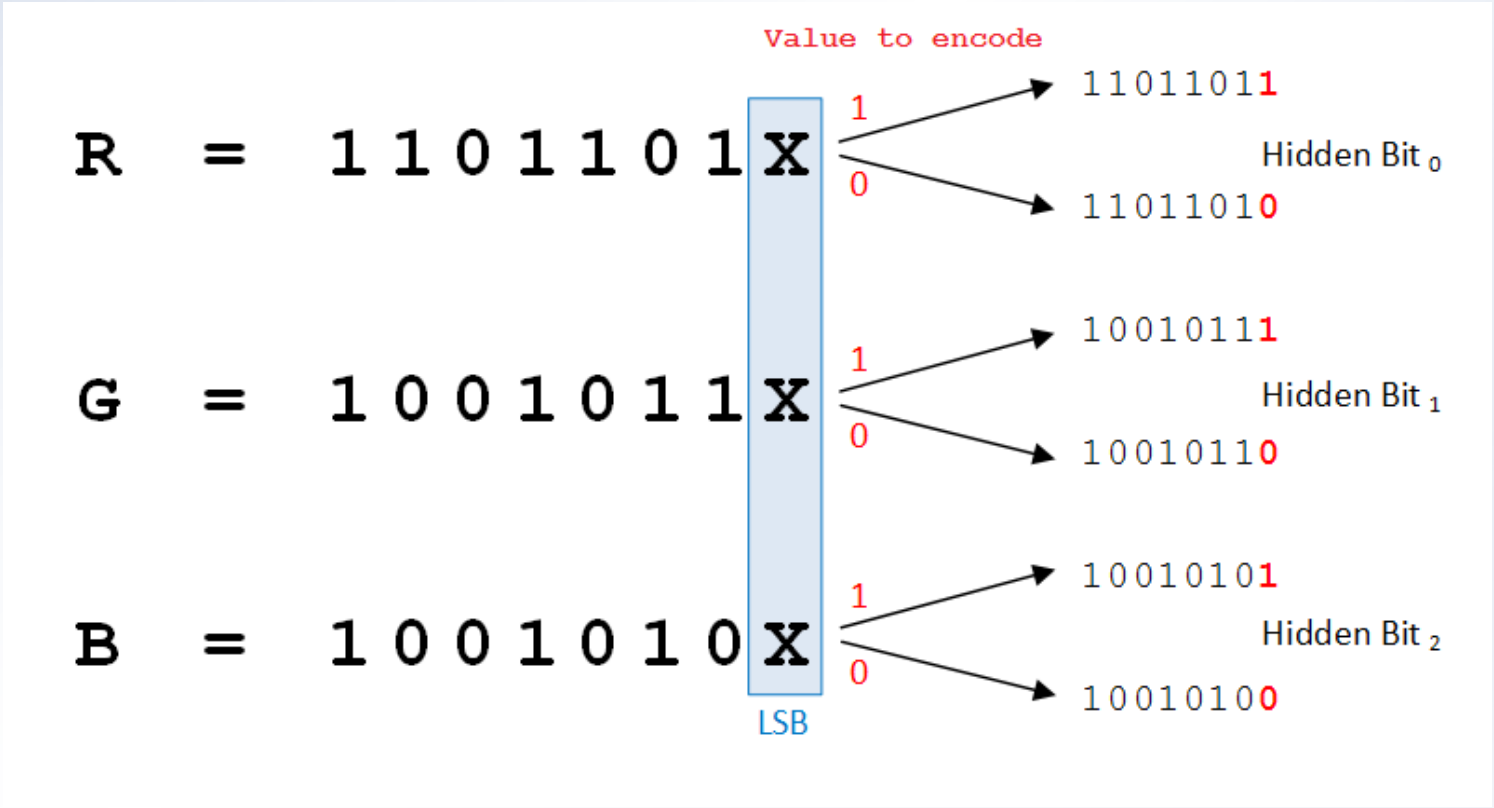
Colores semblantes

Demo...

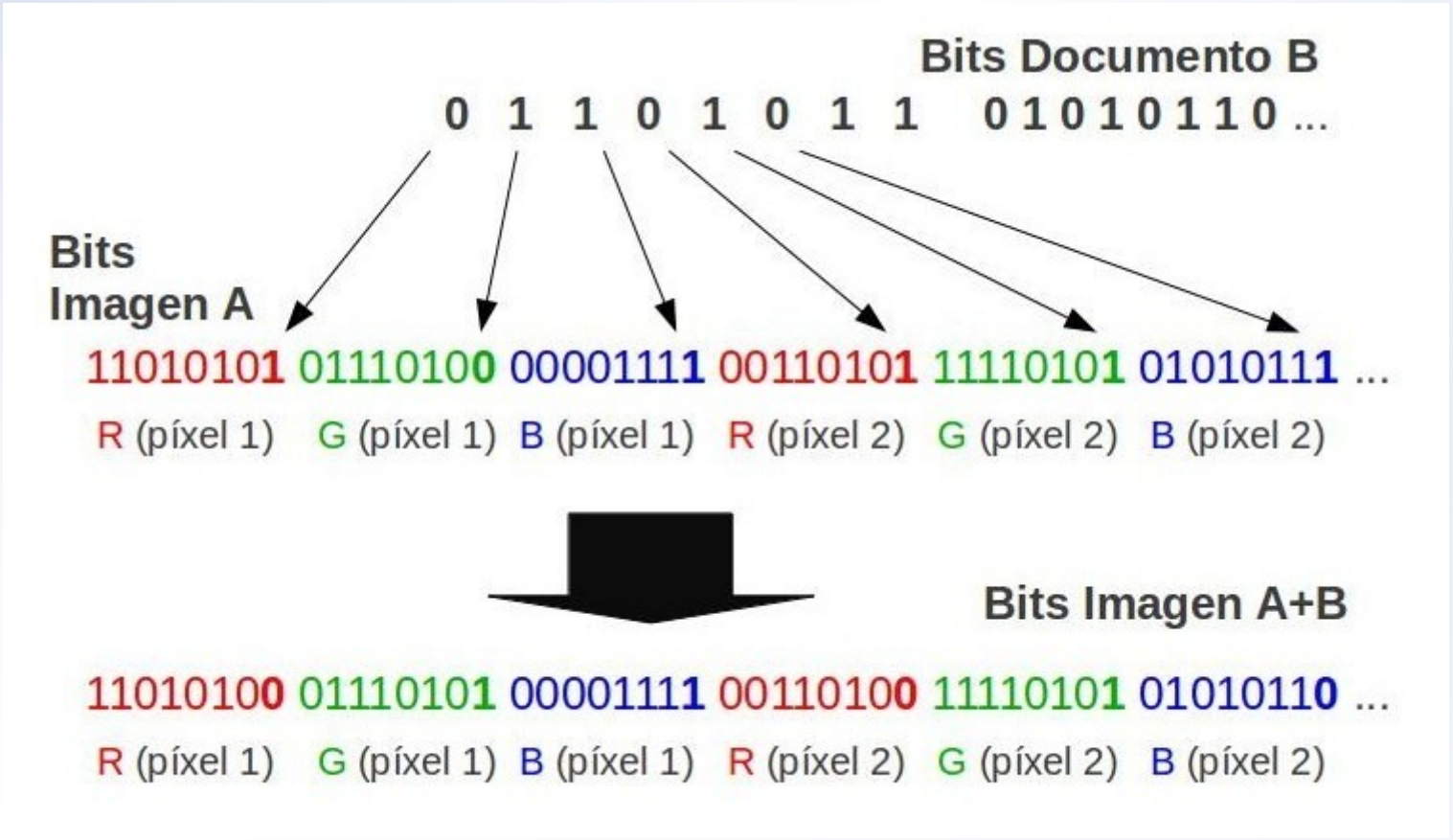
Colores semblantes



Least Significant Bit (LSB)



Least Significant Bit (LSB)



Contenidos

1. ¿Qué es la esteganografía?
2. Historia de la esteganografía
3. Esteganografía en la actualidad
4. Técnicas de esteganografía
5. Least Significant Bit en profundidad
6. Dificultando el descubrimiento
7. Posibles usos

Least Significant Bit en profundidad

Definición:

Procedimiento de esteganografía que consiste en la ocultación de información en los bits menos significativos.

Ejemplo

Least Significant Bit en profundidad

Pasos a seguir:

1. Elaborar un programa que lea cada píxel de la imagen.

2. Extraer el respectivo RGB de cada píxel.

3. Obtener el bit menos significativo de cada color y agrupar los bits de 8 en 8 para formar bytes.

4. Escribir todos los bytes en un fichero.

Least Significant Bit en profundidad

1. Leer cada píxel de la imagen
2. Extraer RGB de cada píxel
3. Obtener el LSB de cada píxel

```
//Leemos la imagen de entrada
$archivo_imagen=imagecreatefrompng($nombre_imagen);

//Obtenemos el tamano de la imagen
$xmax=imagesx($archivo_imagen);
$ymax=imagesy($archivo_imagen);

//Recorremos todos los pixeles de la imagen portadora por filas
for($y=0;$y<$ymax;$y++)
{
        for($x=0;$x<$xmax;$x++)
        {
                //Obtenemos el color rgb del pixel
                $rgb=imagecolorat($archivo_imagen, $x, $y);

                //Obtenemos el último bit de cada color
                $r_lsb=($rgb >> 16) & 1;
                $g_lsb=($rgb >> 8) & 1;
                $b_lsb=$rgb & 1;

                //Guardamos los 3 bits en una cadena
                $rgb_lsb .= $r_lsb.$g_lsb.$b_lsb;
        }
}
```

Least Significant Bit en profundidad

4. Agrupar los bits de 8 en 8 y copiarlos a un fichero

```
//////////////////////
// Procedemos a crear el archivo oculto

//Agrupamos los bits de 8 en 8
$longi = strlen($rgb_lsb);
for($i=0;$i<$longi;$i+=8)
{
        $aux = "";
        for($j=0;$j<8;$j++)
        {
                if(($i+$j)<$longi)
                {
                        $aux .= $rgb_lsb[$i+$j];
                }
        }
        $aux = bindec($aux);
        $aux = chr($aux);

        //volcamos cada "char" a un fichero
        fputs($archivo_salida, $aux);
}

//cerramos el fichero
fclose($archivo_salida);
```

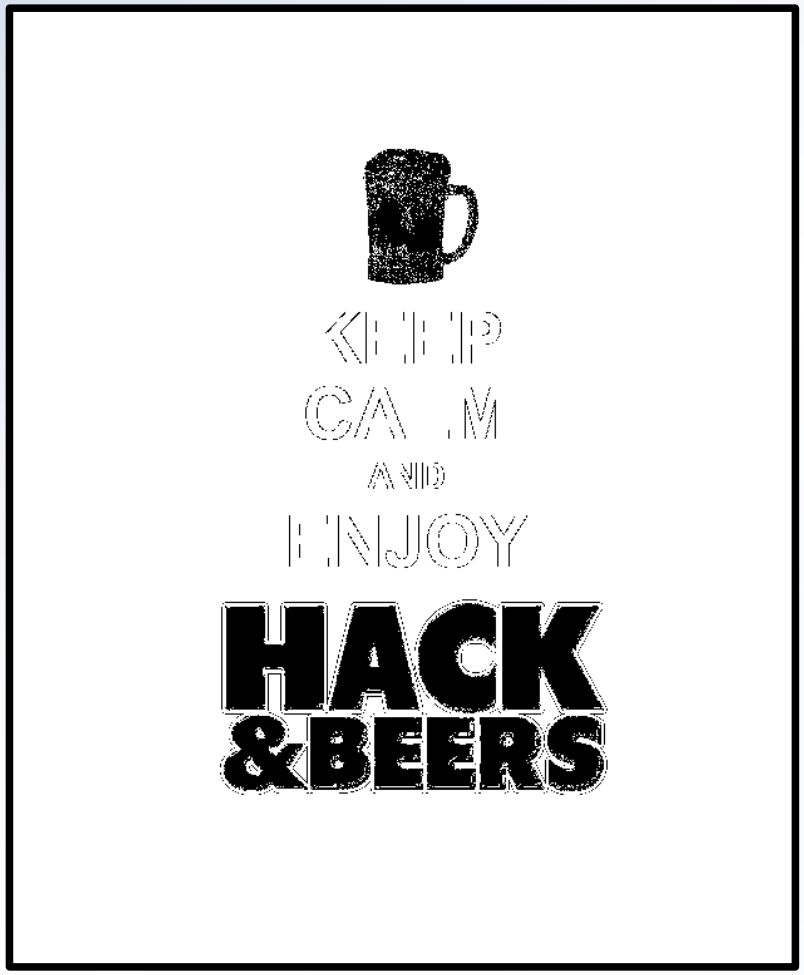
Least Significant Bit en profundidad

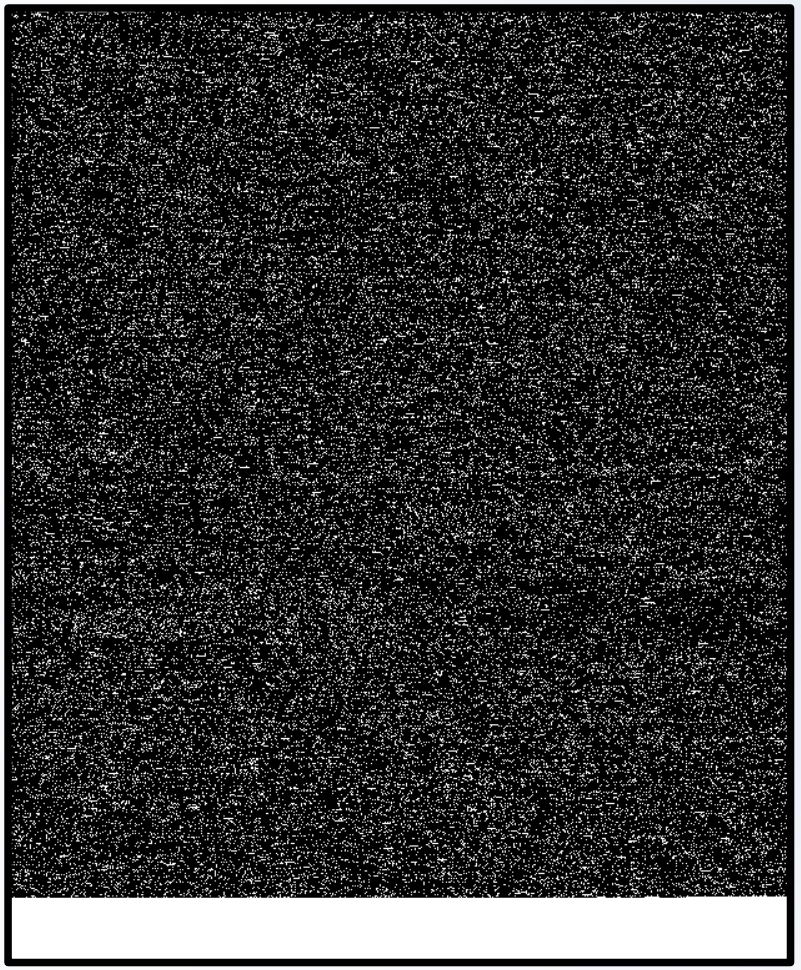
LSB Demo...

¿Diferencias?

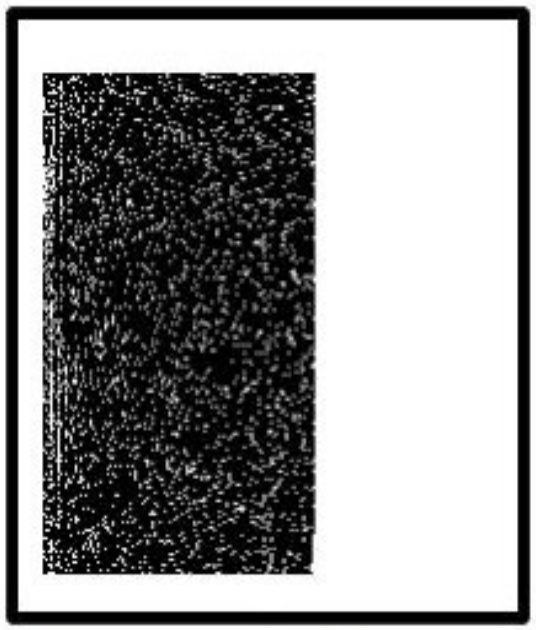
Least Significant Bit en profundidad

¿Diferencias?

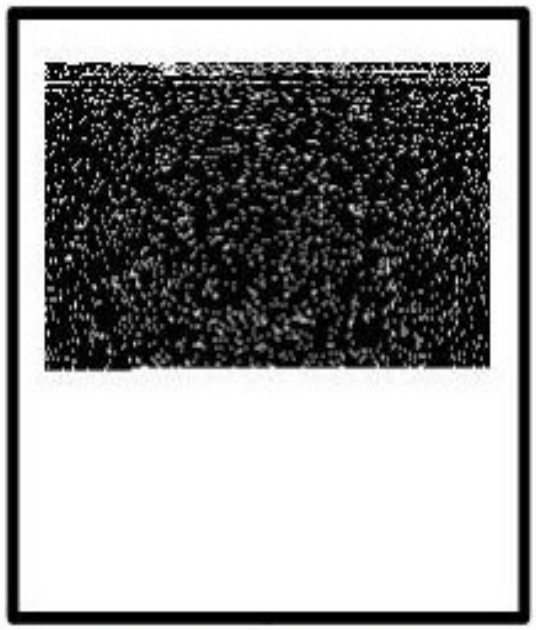




Detectando LSB en imágenes



LSB por columnas



LSB por filas

Contenidos

1. ¿Qué es la esteganografía?
2. Historia de la esteganografía
3. Esteganografía en la actualidad
4. Técnicas de esteganografía
5. Least Significant Bit en profundidad
6. Dificultando el descubrimiento
7. Posibles usos

Ejemplos

1. Modificación de cabeceras.
2. Alteración del orden de inserción en LSB.
3. Utilizar contraseñas.
4. Utilizar datos cifrados.

...

Contenidos

1. ¿Qué es la esteganografía?
2. Historia de la esteganografía
3. Esteganografía en la actualidad
4. Técnicas de esteganografía
5. Least Significant Bit en profundidad
6. Dificultando el descubrimiento
7. Posibles usos

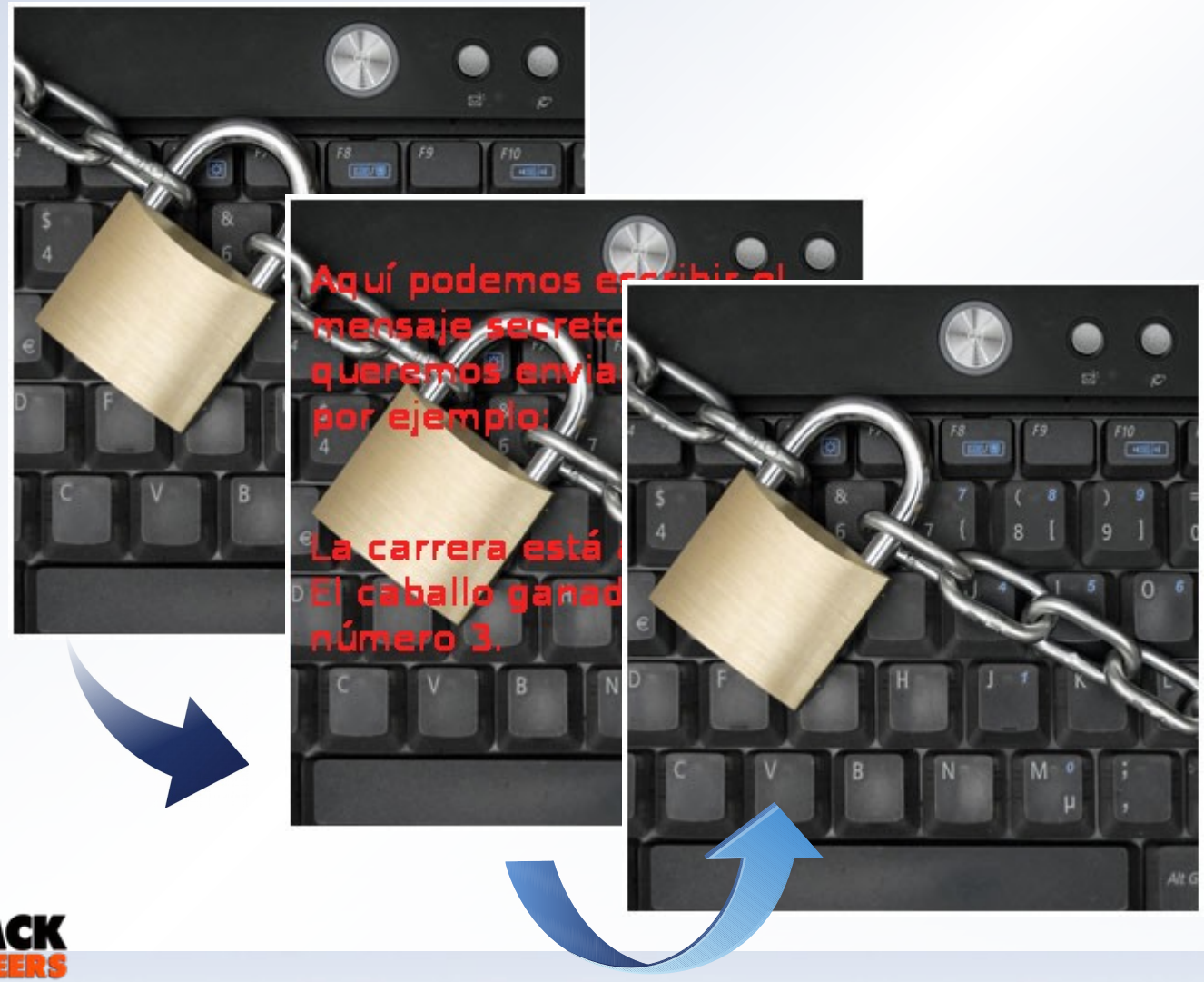
Posibles usos

Watermarking

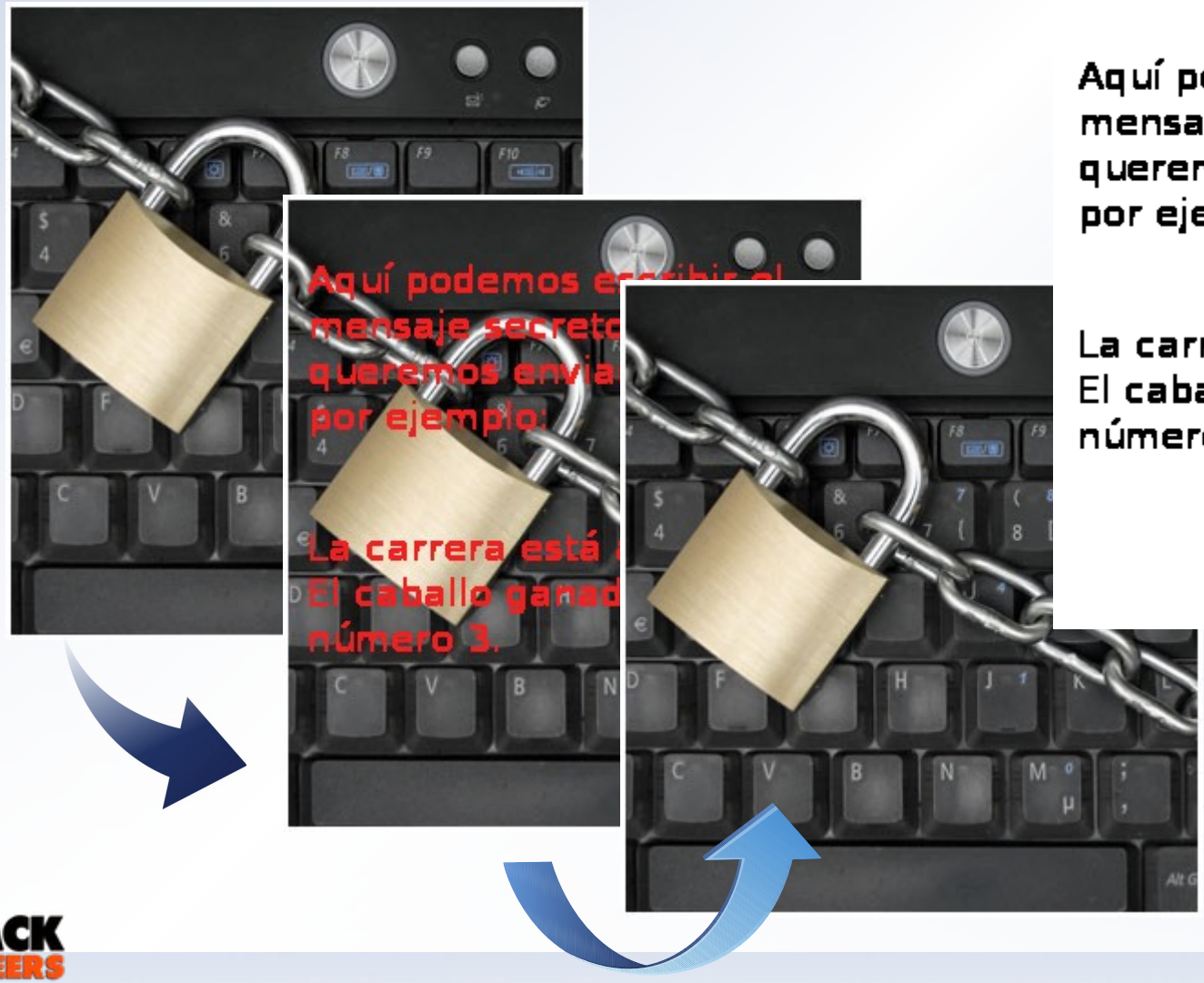
Watermarking

Posibles usos

Watermarking



Watermarking



Data Loss Prevention Bypass

Device inspection

Preguntas

¿Any questions?

Ocultando tu información privada a miradas indiscretas

HACK &BEERS *Tarragona*
Noviembre 2015

Rafael Páez
@fikih888