



# Esteganografía: Exfiltración de datos sin ser descubierto en el intento

Mayo 2018

Rafael Páez Jaime  
@fikih888

# Who Am I?

## Rafael Páez Jaime

- ✓ Ingeniero superior en informática
- ✓ Máster universitario de Seguridad en las Tecnologías de la Información y de las Comunicaciones (MISTIC)
- ✓ Offensive Security Certified Professional (OSCP)
- ✓ Certified Ethical Hacking (CEH)
- ✓ Cybersecurity Consultant and Pentester @ KPMG
- ✓ Participante de CTFs (PKTeam)
- ✓ Twitter: @fikih888

# Contenido

1. ¿Qué nos impide extraer datos?
2. Esteganografía en la historia
3. Ocultación en ficheros de audio
4. Ocultación en documentos de texto
5. Ocultación en protocolos de red
6. Dificultando el descubrimiento
7. Bibliografía

- 
1. ¿Qué nos impide extraer datos?
  2. Esteganografía en la historia
  3. Ocultación en ficheros de audio
  4. Ocultación en documentos de texto
  5. Ocultación en protocolos de red
  6. Dificultando el descubrimiento
  7. Bibliografía

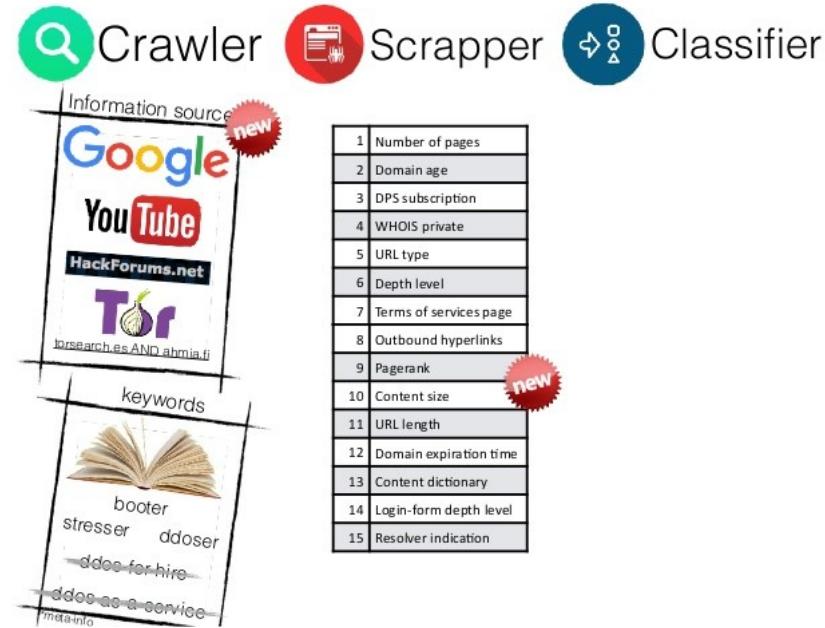
# 1. ¿Qué nos impide extraer datos?

## Firewall



# 1. ¿Qué nos impide extraer datos?

Firewall  
URL Whitelist/Blacklist



# 1. ¿Qué nos impide extraer datos?

Firewall

URL Whitelist/Blacklist

**Puertos USB deshabilitados**



# 1. ¿Qué nos impide extraer datos?

Firewall

URL Whitelist/Blacklist

Puertos USB deshabilitados

**HIDS/NIDS**



# 1. ¿Qué nos impide extraer datos?

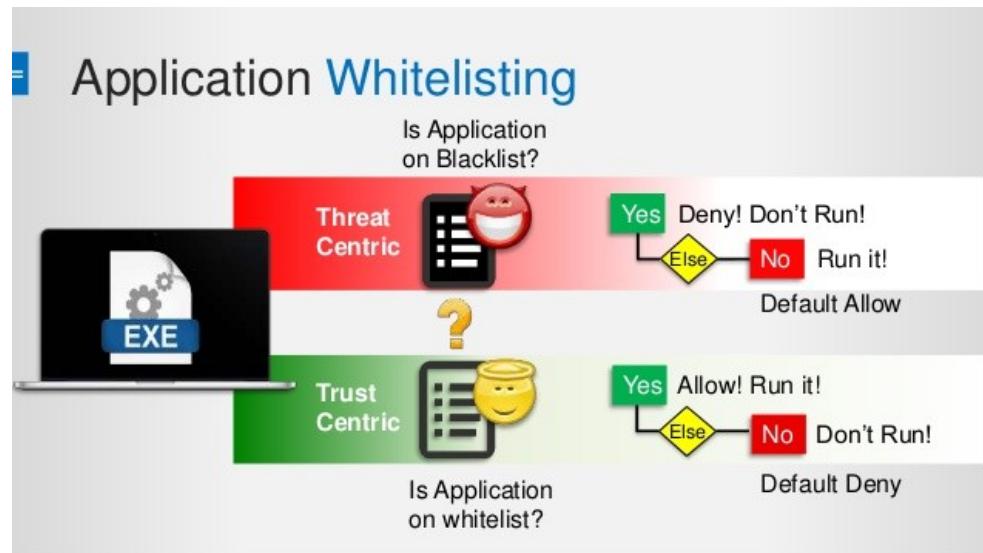
Firewall

URL Whitelist/Blacklist

Puertos USB deshabilitados

HIDS/NIDS

**Aplicaciones específicas**



# 1. ¿Qué nos impide extraer datos?

Firewall

URL Whitelist/Blacklist

Puertos USB deshabilitados

HIDS/NIDS

Aplicaciones específicas

**Device inspection**

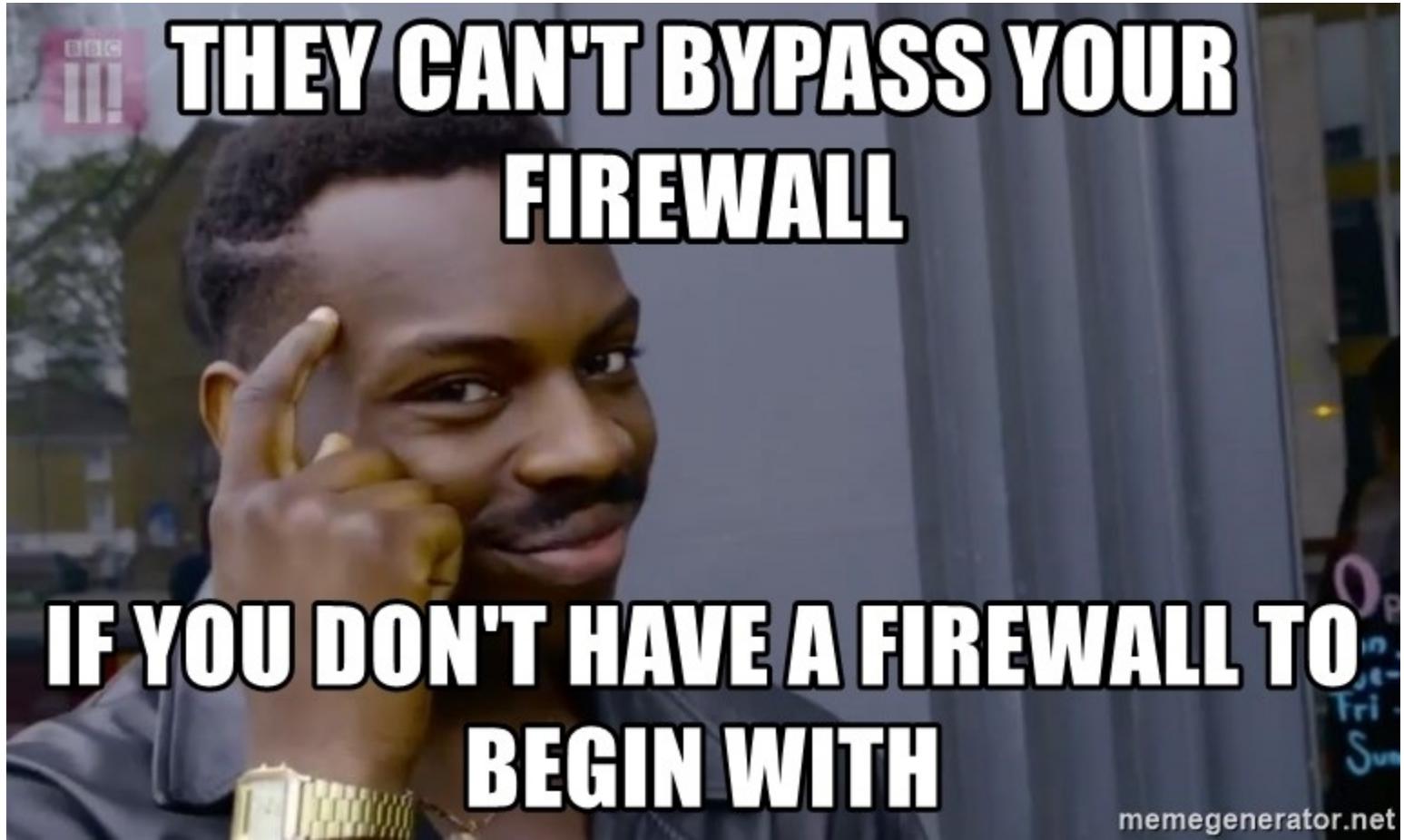


# 1. ¿Qué nos impide extraer datos?

Firewall  
URL Whitelist/Blacklist  
Puertos USB deshabilitados  
HIDS/NIDS  
Aplicaciones específicas  
Device inspection  
**DLP (Data Loss Prevention)**



# 1. ¿Qué nos impide extraer datos?



memegenerator.net

- 
1. ¿Qué nos impide extraer datos?
  2. Esteganografía en la historia
  3. Ocultación en ficheros de audio
  4. Ocultación en documentos de texto
  5. Ocultación en protocolos de red
  6. Dificultando el descubrimiento
  7. Bibliografía

## 2. Esteganografía en la historia

### 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.

## 2. Esteganografía en la historia

Tablas de cera



## 2. Esteganografía en la historia

### Tablas de cera



## 2. Esteganografía en la historia

### Tablas de cera



## 2. Esteganografía en la historia

### Escritura en cuero cabelludo



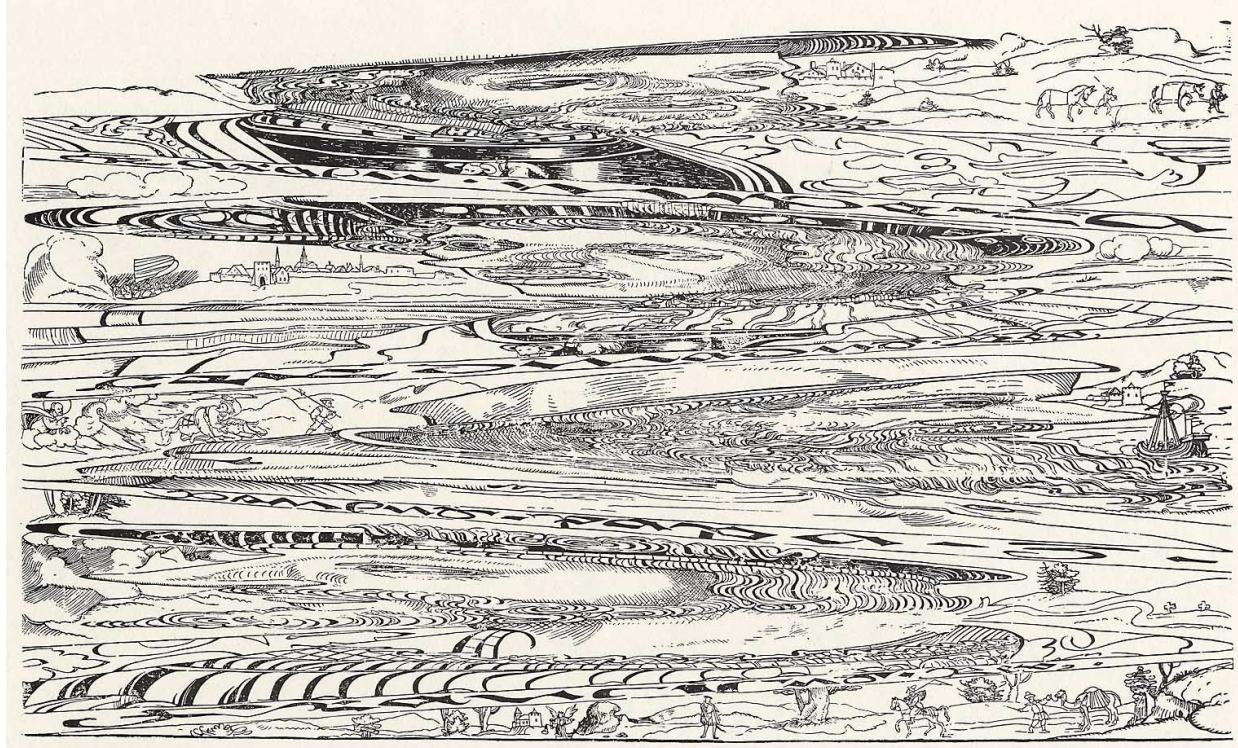
## 2. Esteganografía en la historia

Anamorfosis – Vexierbild por Erhard Schön (1535)



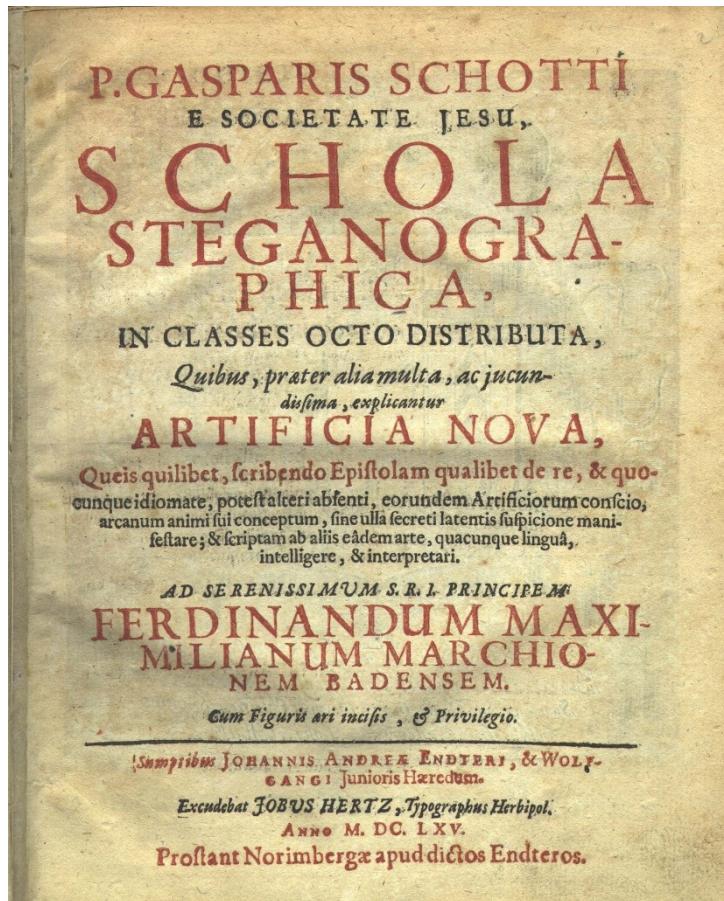
## 2. Esteganografía en la historia

Anamorfosis – Vexierbild por Erhard Schön (1535)



## 2. Esteganografía en la historia

### Schola Steganographica (1665)



## 2. Esteganografía en la historia

### Schola Steganographica (1665)



Classis IX. 323

que secretum significant. In sequenti Schemate notarum quantitates ac sedes, significant literas directè infrà subjectas.

b a c | d e f | g h i | k l | m n o | y z r | s t u | v w x q p

Per has notas, earumque quantitates ac sedes, docet citatus Auctor secretum Germanicis verbis conceptum, ut quis clavum magnum ac firmum frangere possit manibus, sine malleo, forcipe, aut alio manuali instrumento, prout sequitur. In Schemate Auctoris nota non occupant loca debita; quare restituenda fuere.

Nim z vvei vvischdichlein,  
wickel s umb den nagel, eins  
oben, das ander unden, eins

Ss 2 2M

RIS SCHOTTI  
IETATE JESU.  
**H O L A  
A N O G R A -  
H I C A .**

OCTO DISTRIBUTA,  
atēr alia multa, ac juncun-  
lissima, explicantur

**I C I A N O V A ,**

ndo Epistolam qualibet de re, & quo-  
eri absenti, corundem Artificiorum conscio-  
rum, sine illa secreti latentis suspicione mani-  
ab aliis eadē arte, quacunque lingua,  
illigere, & interpretari.

SSIMUM S. R. L. PRINCIPEM  
**A N D U M M A X I -  
I U M M A R C H I O -  
I B A D E N S E M .**

ris ari incisis, & Privilegio.

NIS ANDREA ENDTERI, & WOLFGANGI Junioris Hereditus.

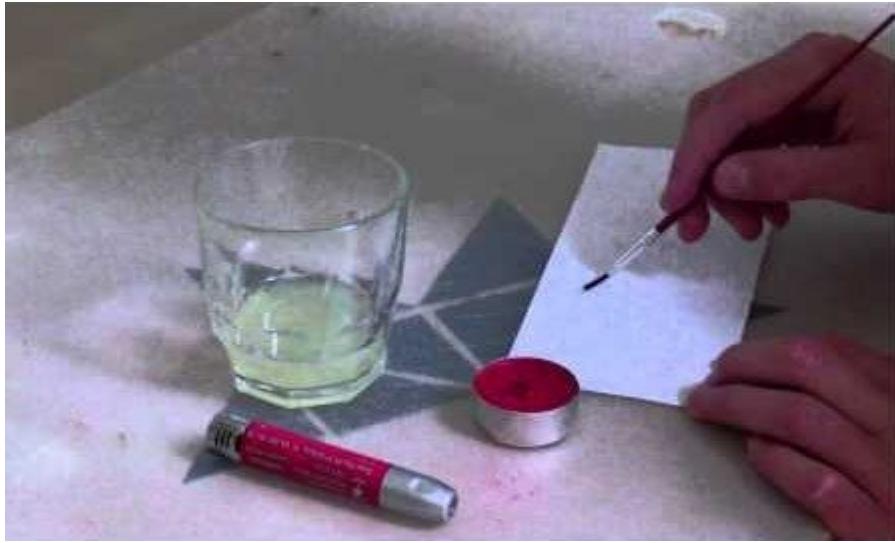
US HERTZ, Typographus Herbol.

Anno M. DC. LXV.

imbergæ apud dictos Endteros.

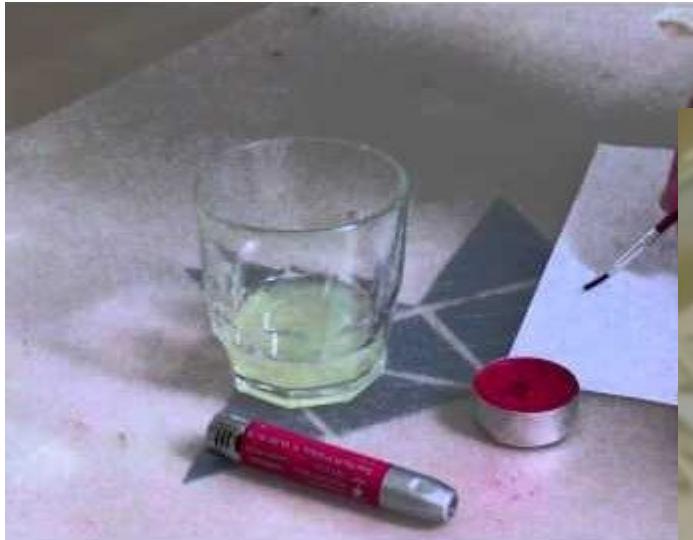
## 2. Esteganografía en la historia

### Tinta invisible



## 2. Esteganografía en la historia

Tinta invisible



## 2. Esteganografía en la historia

Tinta invisible



# 2. Esteganografía en la historia

## Illegal Primes

485650789657397829309841894694286137707442087351357924019652073668698513401047237446968797  
43992611751097377701027447528049058831384037549709987909653955227011712157025974666993240  
226834596619606034851742497735846851885567457025712547499964821941846557100841190862597169  
479707991520048667099759235960613207259737979936188606316914473588300245336972781813914797  
955513399949394882899846917836100182597890103160196183503434489568705384520853804584241565  
482488933380474758711283395989685223254460840897111977127694120795862440547161321005006459  
820176961771809478113622002723448272249323259547234688002927776497906148129840428345720146  
348968547169082354737835661972186224969431622716663939055430241564732924855248991225739466  
548627140482117138124388217717602984125524464744505583462814488335631902725319590439283873  
764073916891257924055015620889787163375999107887084908159097548019285768451988596305323823  
490558092032999603234471140776019847163531161713078576084862236370283570104961259568184678  
59653310077017991614674472549272833486916000647585917462781212690073518309241530106302893  
295665843662000800476778967984382090797619859493646309380586336721469695975027968771205724  
996666980561453382074120315933770309949152746918356593762102220068126798273445760938020304  
479122774980917955938387121000588766689258448700470772552497060444652127130404321182610103  
591186476662963858495087448497373476861420880529443

# 2. Esteganografía en la historia

## Illegal Primes - CSS Descramblers

485650789657397829309841894694286137707442087351357924019652073668698513401047237446968797  
43992611751097377701027447528049058831384037549709987909653955227011712157025974666993240  
226834596619606034851742497735846851885567457025712547499964821941846557100841190862597169  
479707991520048667099759235960613207259737979936188606316914473588300245336972781813914797  
955513399949394882899846917836100182597890103160196183503434489568705384520853804584241565  
482488933380474758711283395989685223254460840897111977127694120795862440547161321005006459  
820176961771809478113622002723448272249323259547234688002927776497906148129840428345720146  
348968547169082354737835661972186224969431622716663939055430241564732924855248991225739466  
548627140482117138124388217717602984125524464744505583462814488335631902725319590439283873  
764073916891257924055015620889787163375999107887084908159097548019285768451988596305323823  
490558092032999603234471140776019847163531161713078576084862236370283570104961259568184678  
59653310077017991614674472549272833486916000647585917462781212690073518309241530106302893  
295665843662000800476778967984382090797619859493646309380586336721469695975027968771205724  
996666980561453382074120315933770309949152746918356593762102220068126798273445760938020304  
479122774980917955938387121000588766689258448700470772552497060444652127130404321182610103  
591186476662963858495087448497373476861420880529443

# 2. Esteganografía en la historia

## Buscaminas



## 2. Esteganografía en la historia

### Imágenes



## 2. Esteganografía en la historia

### Vídeos

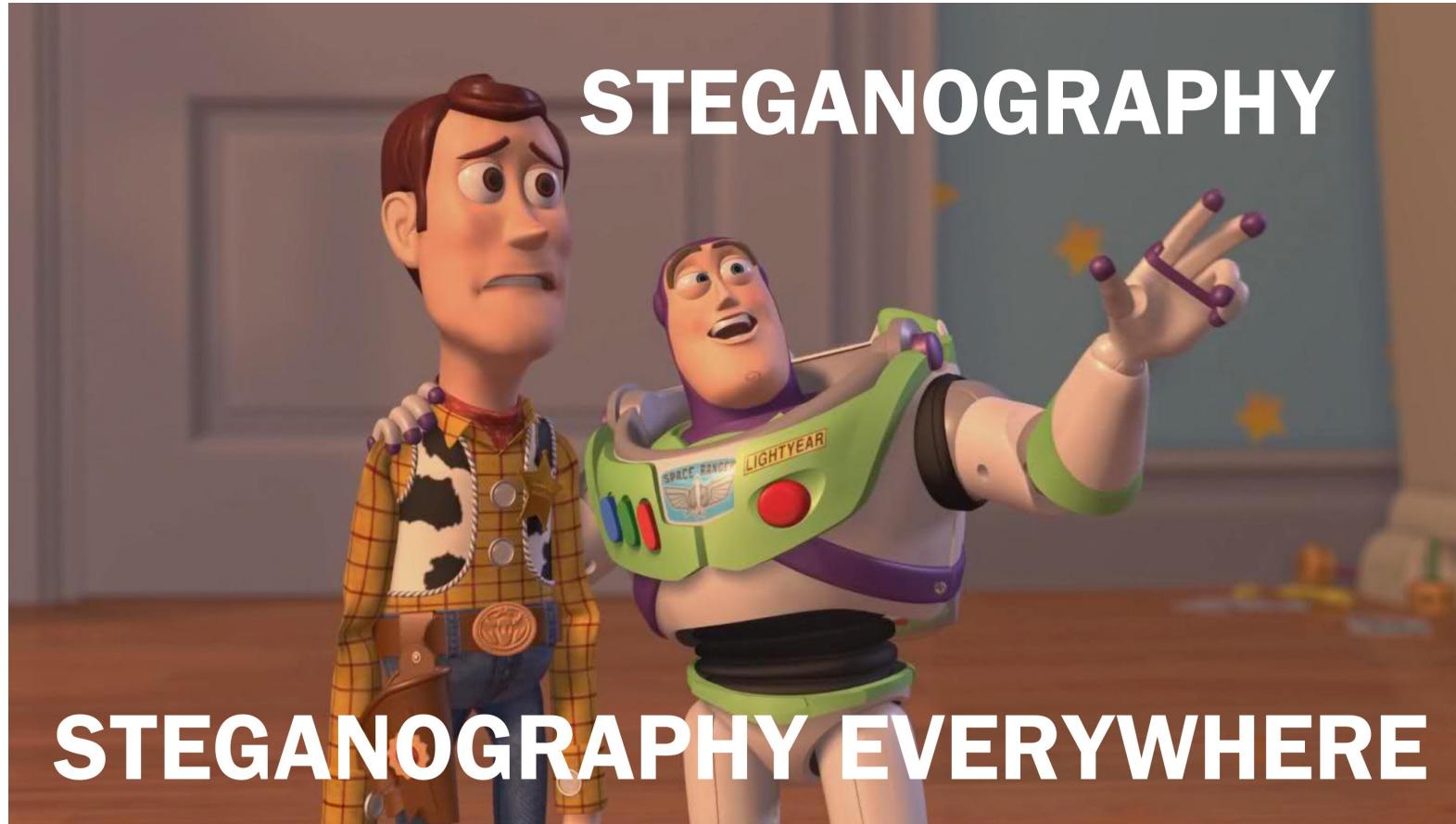
#### Steganography: how al-Qaeda hid secret documents in a porn video

Digital steganography hides files in plain sight, concealed in image and media files.

SEAN GALLAGHER - 5/2/2012, 2:02 PM



## 2. Esteganografía en la historia



- 
1. ¿Qué nos impide extraer datos?
  2. Esteganografía en la historia
  3. Ocultación en ficheros de audio
  4. Ocultación en documentos de texto
  5. Ocultación en protocolos de red
  6. Dificultando el descubrimiento
  7. Bibliografía

# 3. Ocultación en ficheros de audio

Least Significant Byte (LSB)

## Wav File Format

Start Byte	Len	Name
0	12	RIFF Header
12	24	Wav Format Subchunk
36	8	Data Subchunk (ID and Size)
44	*	Data

# 3. Ocultación en ficheros de audio

## Least Significant Byte (LSB)

### Wav File Format

Start Byte	Len	Name
0	12	RIFF Header
12	24	Wav Format Subchunk

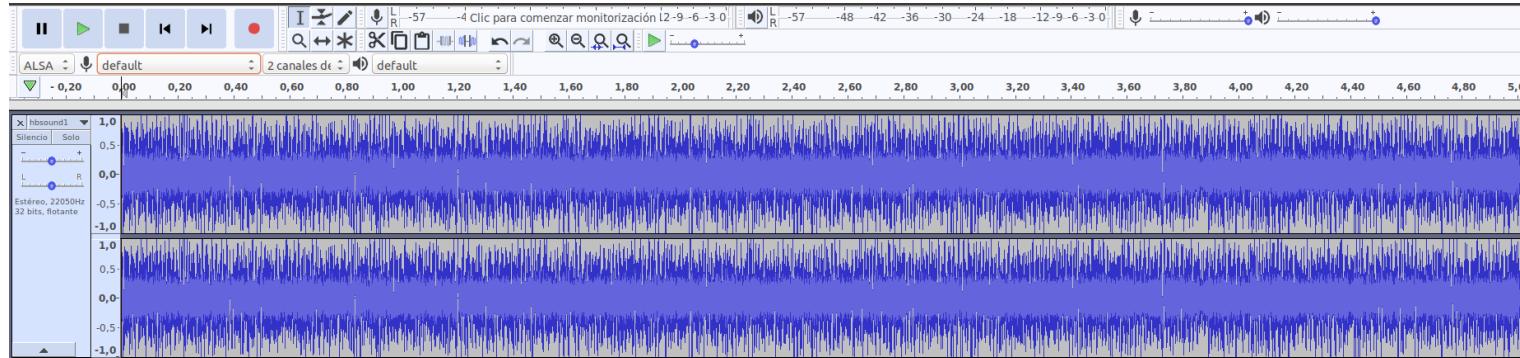
### WavSteg

WavSteg uses least significant bit steganography to hide a file in the samples of a .wav file.

For each sample in the audio file, we overwrite the least significant bits with the data from our file.

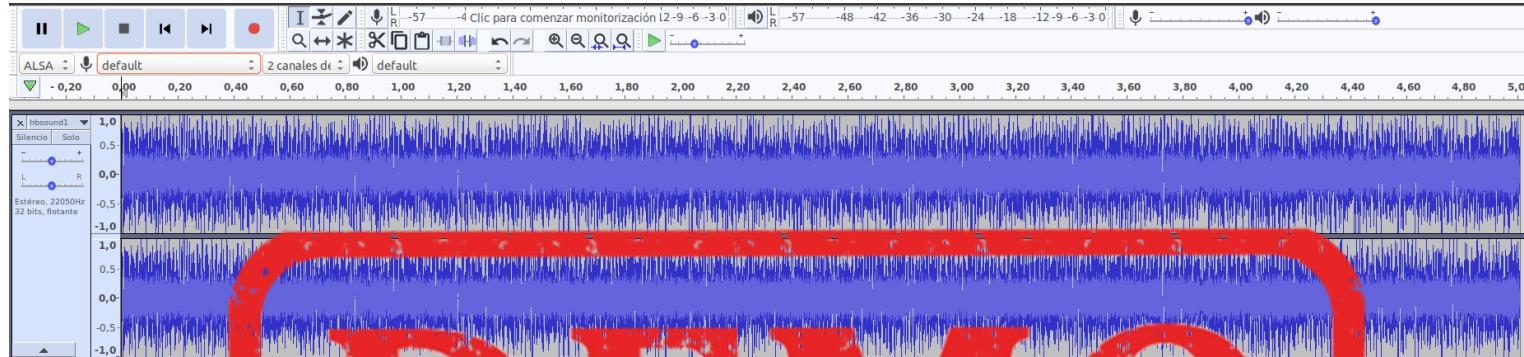
# 3. Ocultación en ficheros de audio

Coagula



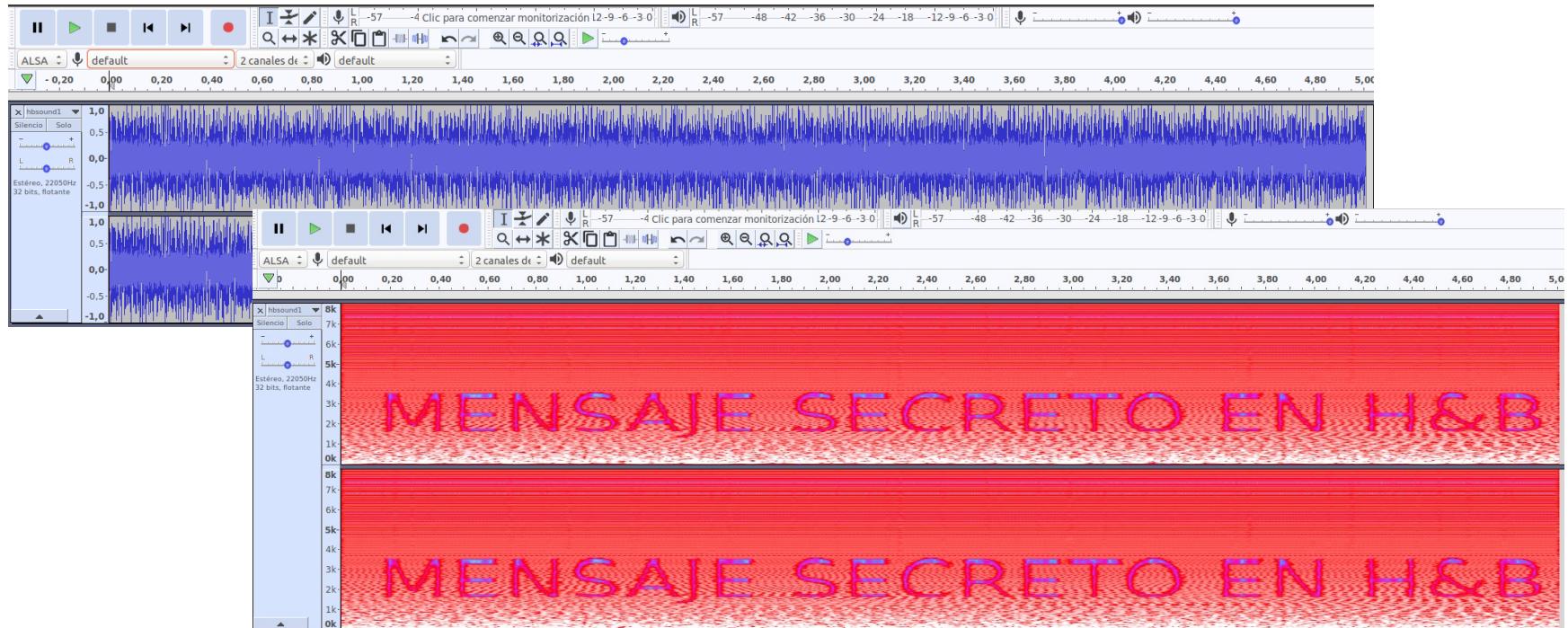
# 3. Ocultación en ficheros de audio

Coagula



# 3. Ocultación en ficheros de audio

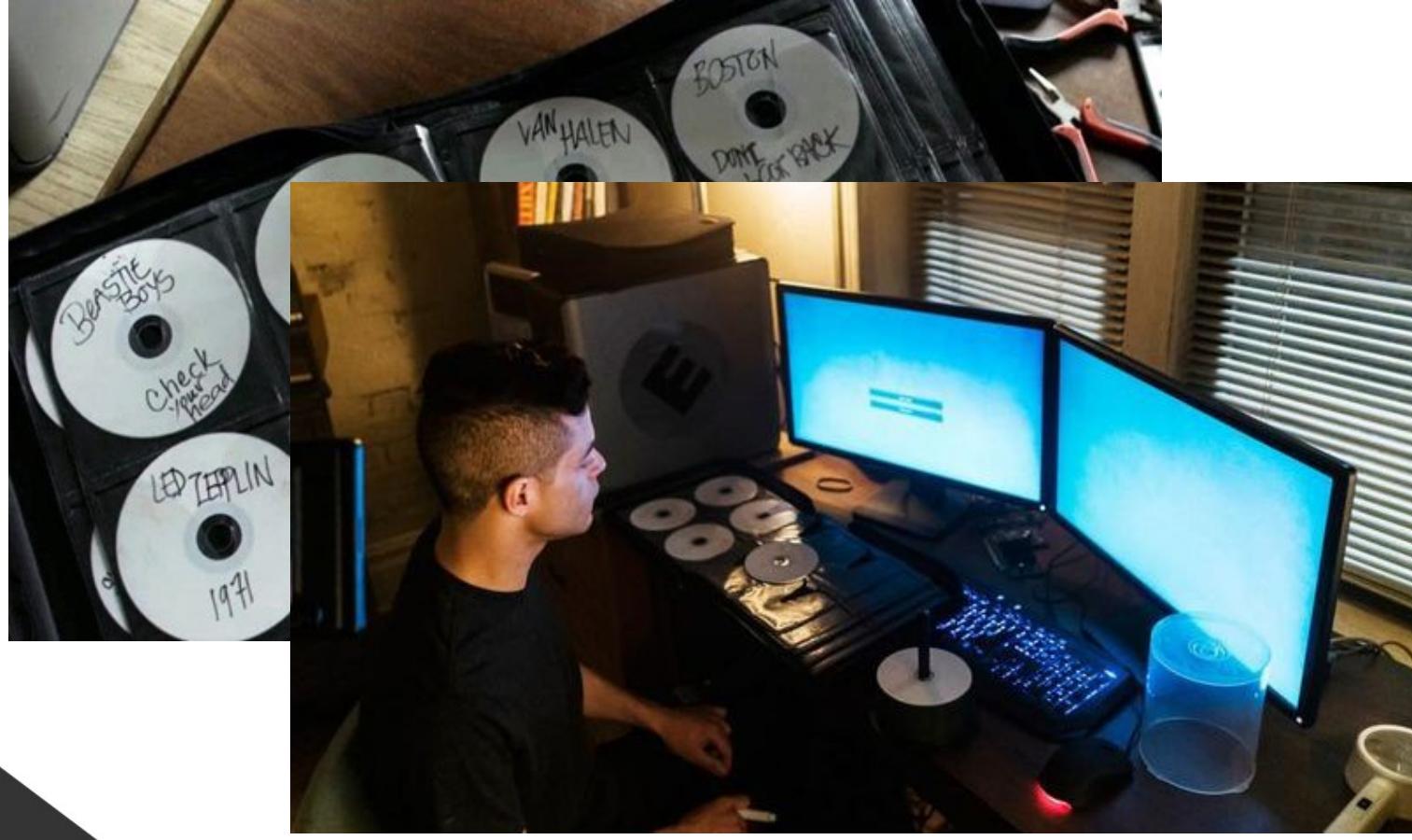
## Coagula



# 3. Ocultación en ficheros de audio



# 3. Ocultación en ficheros de audio



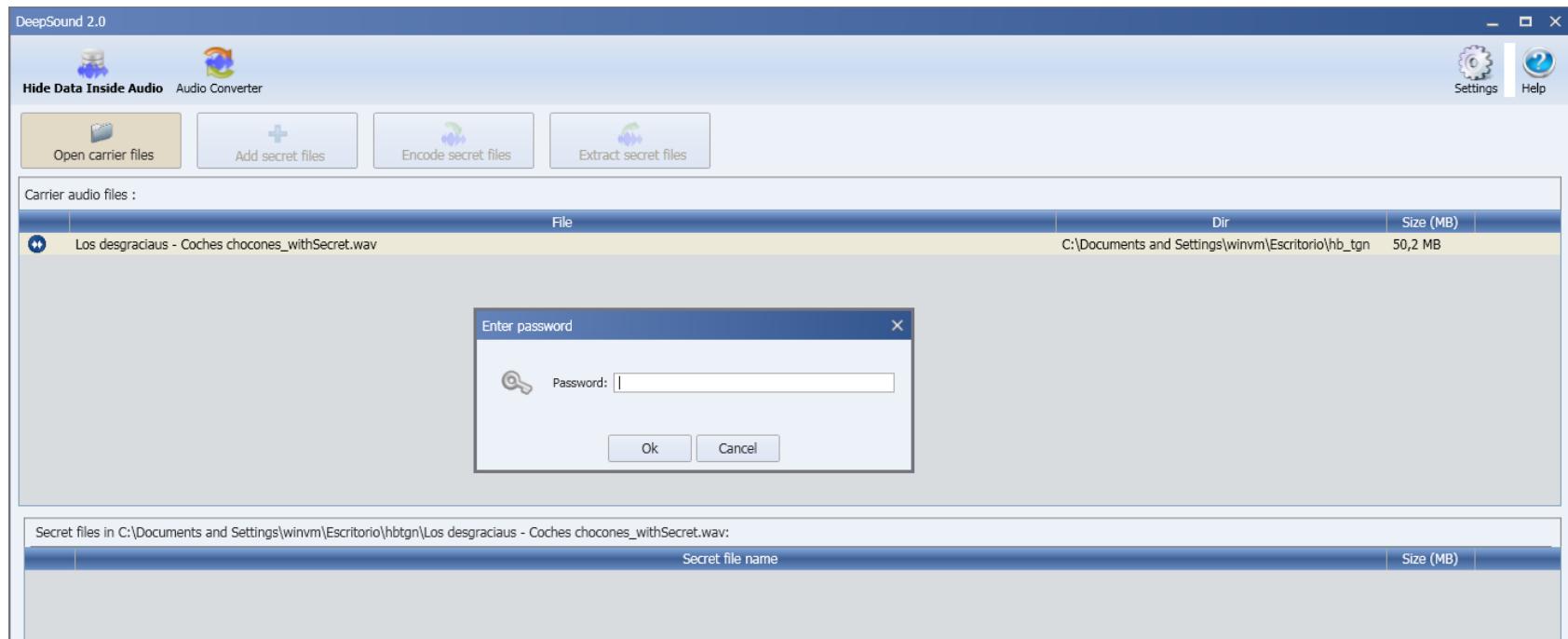
# 3. Ocultación en ficheros de audio

DeepSound

**DEMO**

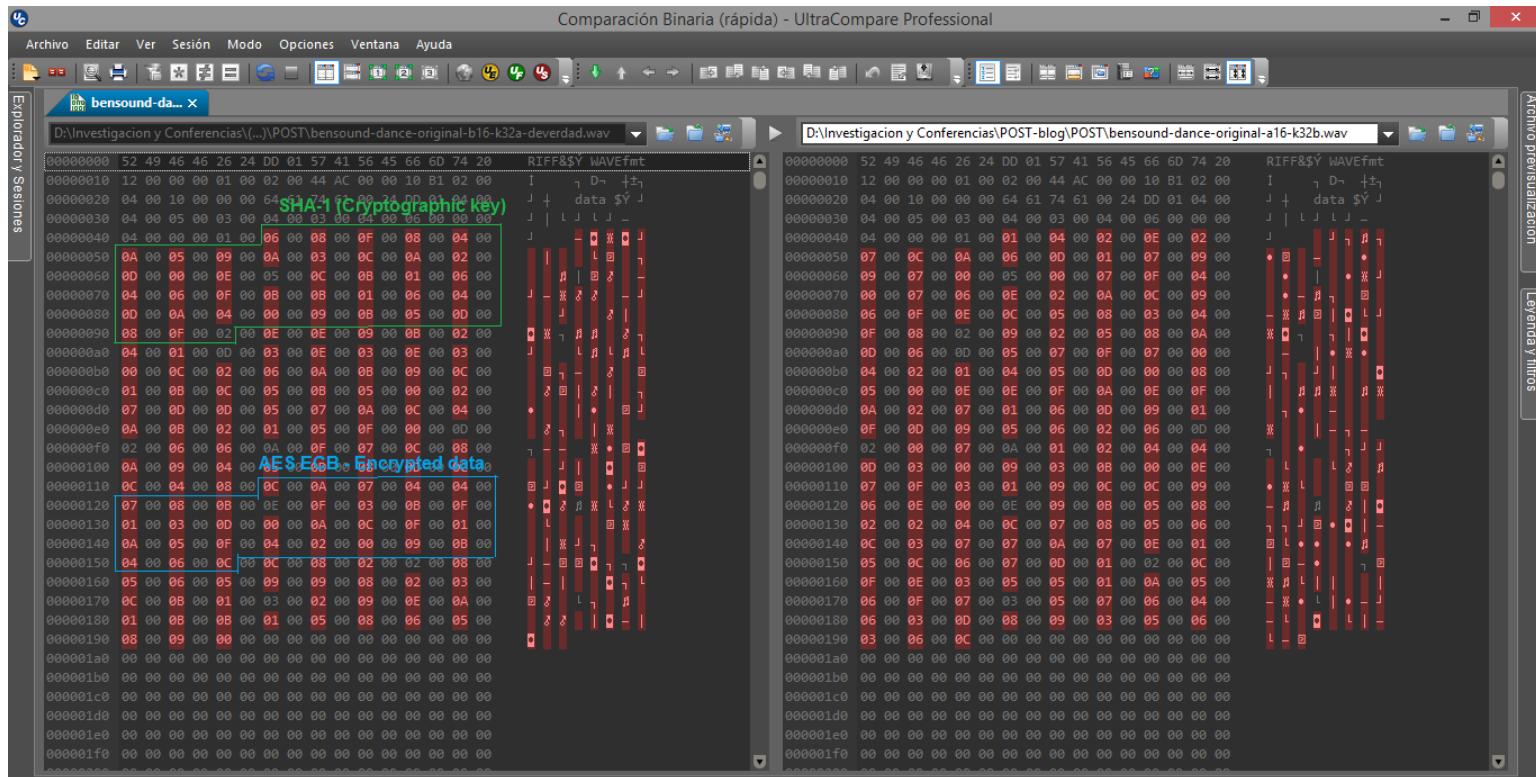
# 3. Ocultación en ficheros de audio

## DeepSound



# 3. Ocultación en ficheros de audio

## DeepSound



<https://cryptonibbles.blogspot.com.es/2016/05/why-mr-robot-does-not-know-steganography.html>

**HACK  
&BEERS**

#hbTarragona

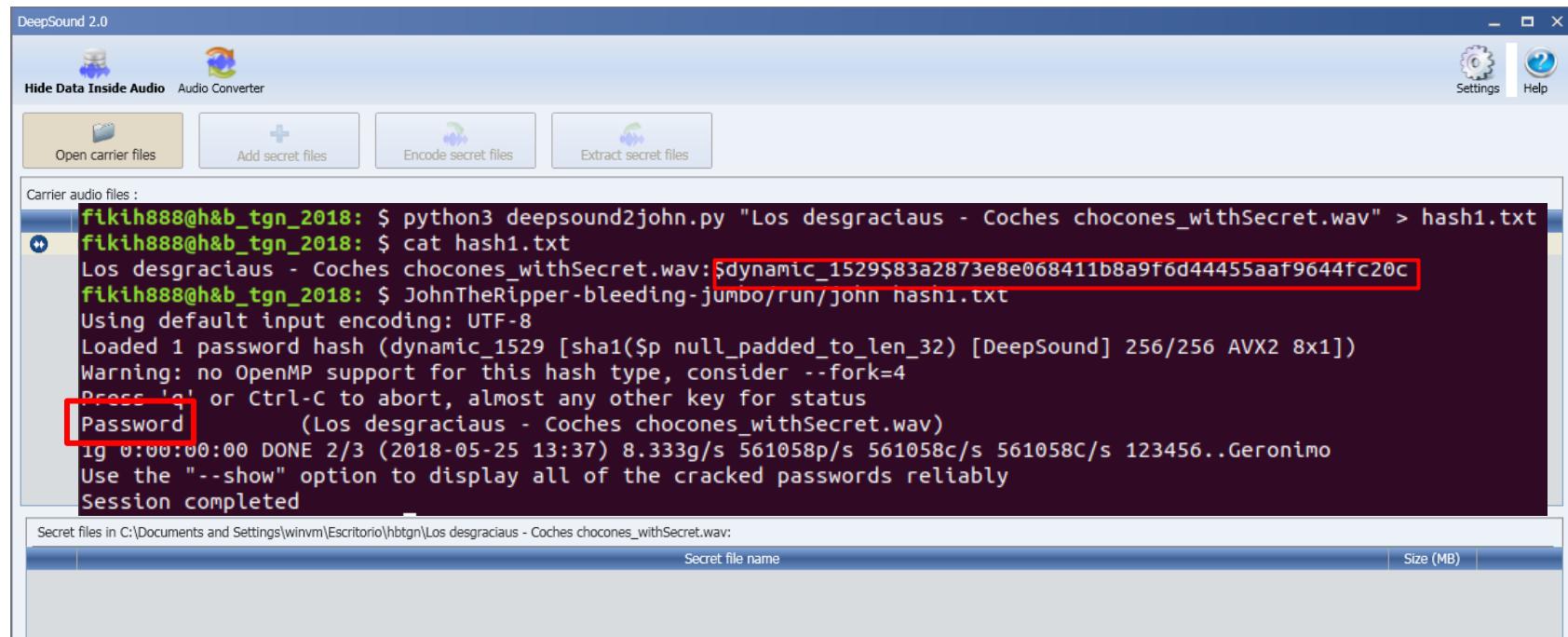
### 3. Ocultación en ficheros de audio

DeepSound

**DEMO**

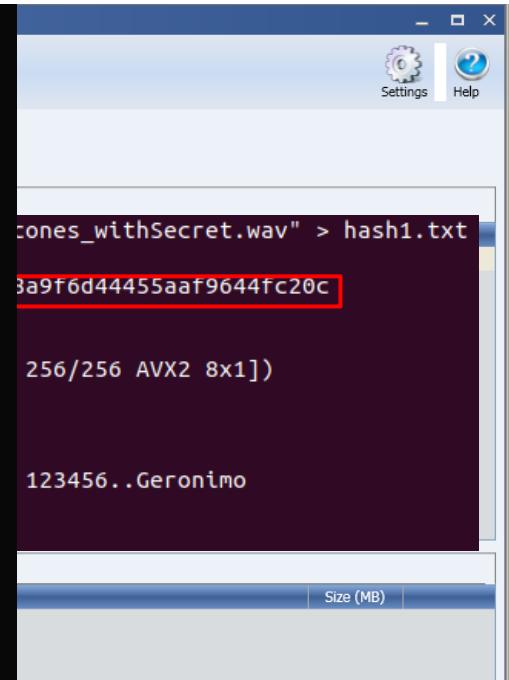
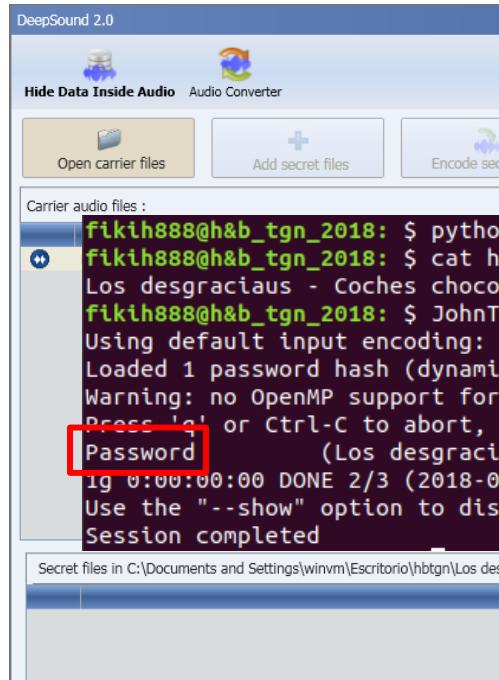
# 3. Ocultación en ficheros de audio

## DeepSound



# 3. Ocultación en ficheros de audio

## DeepSound

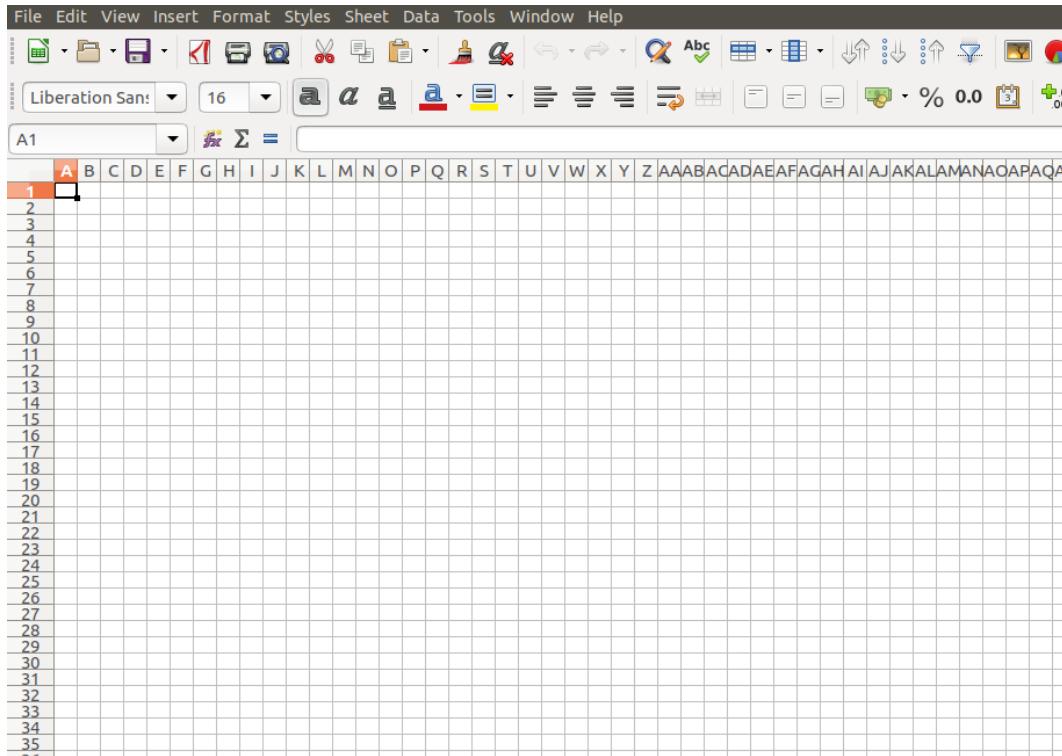


**HACK  
&BEERS**  
#hbTarragona

- 
1. ¿Qué nos impide extraer datos?
  2. Esteganografía en la historia
  3. Ocultación en ficheros de audio
  - 4. Ocultación en documentos de texto**
  5. Ocultación en protocolos de red
  6. Dificultando el descubrimiento
  7. Bibliografía

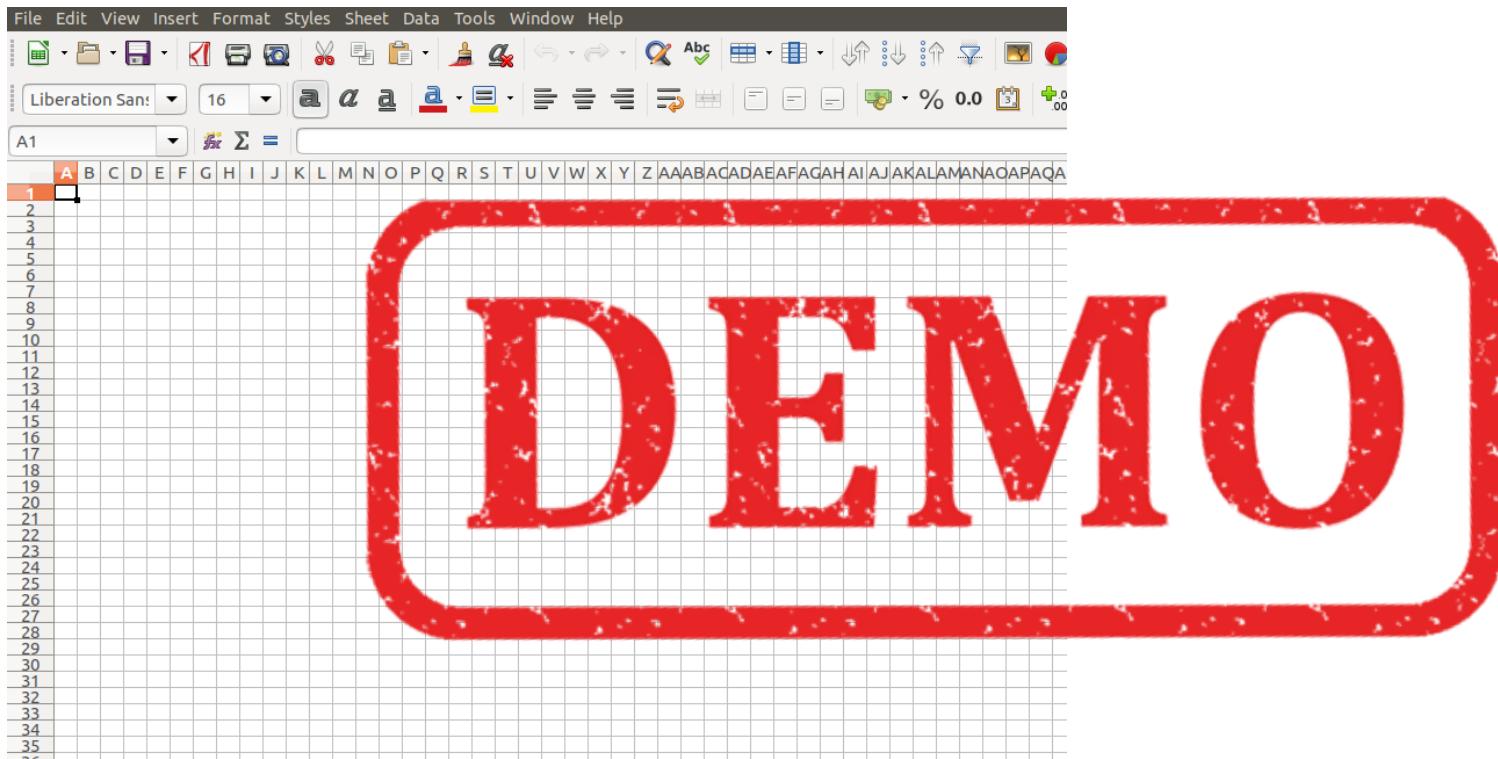
# 4. Ocultación en ficheros de texto

## Spreadsheet cells



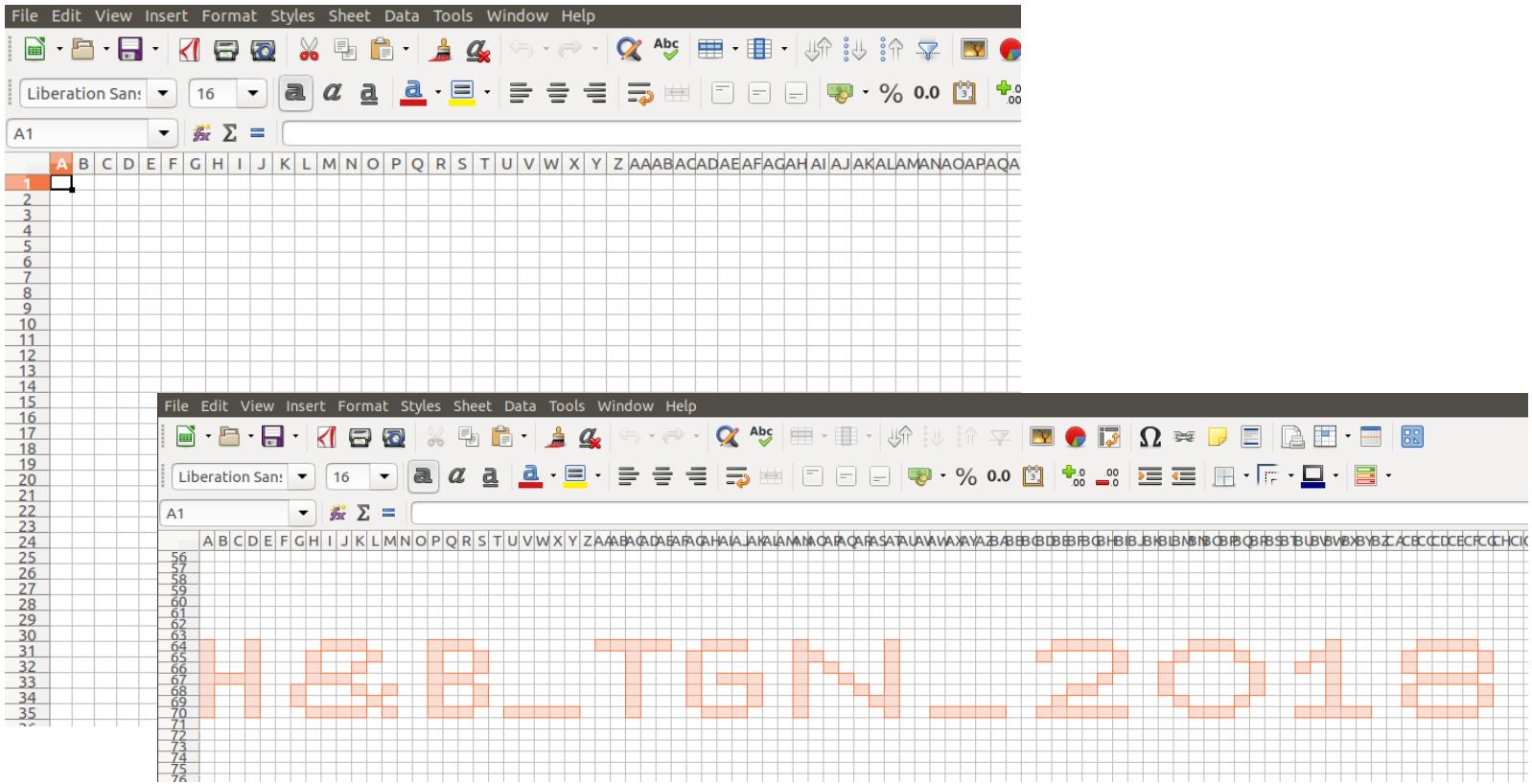
# 4. Ocultación en ficheros de texto

## Spreadsheet cells



# 4. Ocultación en ficheros de texto

## Spreadsheet cells



# 4. Ocultación en ficheros de texto

# HACK & BEERS

# 4. Ocultación en ficheros de texto

DEMO

# HACK & BEERS

# 4. Ocultación en ficheros de texto

# AsciiArt

HACK  
& BEERS

# 4. Ocultación en ficheros de texto

## Cloakify

Nail	Dende	Freezer
Dr. Gero	Vegeta	Yakon
Slug	Nappa	Son Goten
Broly	Slug	Bardock
Son Gohan	Lunch	Recoom
Tapion	Son Goten	King Cold
C-17	Turles	Puar
Recoom	C-17	Zarbon
Son Goten	King Cold	C-16
Turles	Puar	Oolong
C-16	Kamisama	Krilin
King Cold	Nail	Nappa
Krilin	Shenron	Slug
Yakon	Vegeta	Lunch
C-17	Tenshinhan	Son Goten
Uub	C-17	Bardock
Vegeta	Uub	King Cold
Kamisama	Piccolo	Shenron
Shenron	Zarbon	Vegeta
Cell	Bra	Cell
Vegeta	Porunga	C-16
Hildegan	Dodoria	Uub
Baby	Zarbon	Son Goku
Dende	Son Goten	Nappa
Son Gohan	Dende	Bra
Bardock	Dodoria	Lunch
Freezer	Tapion	Son Goten
Raditz	C-17	Ranfan
Dodoria	Pilaf	Bulma
Nappa	Dodoria	Karin
Cell	Hildegan	C-18
Ranfan	Bra	Dende
Chichi	Popo	Bibidi
Kamisama	Son Gohan	Bibidi
Garlick	Bardock	

<https://github.com/TryCatchHCF/Cloakify>

# 4. Ocultación en ficheros de texto

Cloakify

Nail	Dende	Freezer
Dr. Gero	Vegeta	Yakon
Slug	Nappa	Son Goten
Broly	Slug	Bardock
Son Gohan	Lunch	Recoom
Tapion	Son Goten	King Cold
C-17	Turles	Puar
Recoom	C-17	Zarbon
Son Goten	King Cold	C-16
Turles	Puar	Oolong
	Kai	Kai
King Cold	Nai	Nap
Kai	She	Lu
Y	Vega	Zun
C-17	Ten	Son Goten
U	C-17	Bardock
Ve	Utu	King Cold
Kai	Pi	Sh
Shenron	Zarbon	Vegeta
Cell	Bra	Cell
Vegeta	Porunga	C-16

Baby	Zarbon	Son Goku
Dende	Son Goten	Nappa
Son Gohan	Dende	Bra
Bardock	Dodoria	Lunch
Freezer	Tapion	Son Goten
Raditz	C-17	Ranfan
Dodoria	Pilaf	Bulma
Nappa	Dodoria	Karin
Cell	Hildegan	C-18
Ranfan	Bra	Dende
Chichi	Popo	Bibidi
Kamisama	Son Gohan	Bibidi
Garlick	Bardock	



# 4. Ocultación en ficheros de texto

## Cloakify

Nail	Dende	Freezer
Dr. Gero	Vegeta	Yakon
Slug	Nappa	Son Goten
Broly	Slug	Bardock
Son Gohan	Lunch	Recoom
Tapion	Son Goten	King Cold
C-17	Turles	Puar
Recoom	C-17	Zarbon
Son Goten	King Cold	C-16
Turles	Puar	Oolong
C-16	Kamisama	Krilin
King Cold	Nail	Nappa
Krilin	Shenron	Slug
Yakon	Vegeta	Lunch
C-17	Tenshinhan	Son Goten
Uub	C-17	Bardock

```
fikih888@h&b_tgn_2018: $ python decloakify.py hidden1.txt ciphers/dragonBall
Goku y sus amigos también nos pueden ayudar a ocultar nuestros mensajes :P
fikih888@h&b_tgn_2018: $
```

C-17	Bra	C-17
Vegeta	Porunga	C-16
Hildegan	Dodoria	Uub
Baby	Zarbon	Son Goku
Dende	Son Goten	Nappa
Son Gohan	Dende	Bra
Bardock	Dodoria	Lunch
Freezer	Tapion	Son Goten
Raditz	C-17	Ranfan
Dodoria	Pilaf	Bulma
Nappa	Dodoria	Karin
Cell	Hildegan	C-18
Ranfan	Bra	Dende
Chichi	Popo	Bibidi
Kamisama	Son Gohan	Bibidi
Garlick	Bardock	

<https://github.com/TryCatchHCF/Cloakify>

# 4. Ocultación en ficheros de texto

DOCX File format



# 4. Ocultación en ficheros de texto

DOCX File format



# 4. Ocultación en ficheros de texto

DOCX File format

A screenshot of a file manager window titled 'Informe1.docx.zip'. The window shows a list of files within the zip archive. The first file, 'Archivo\_ultrasecreto.txt', is highlighted with a red box. The table below lists the file details.

Nombre	Tamaño	Tipo	Modificado
Archivo_ultrasecreto.txt	67 bytes	documento...	24 mayo 2018, 00:45
document.xml.rels	2,7 kB	desconocido	24 mayo 2018, 15:49

# 4. Ocultación en ficheros de texto



En un lugar de la Mancha, de cuyo nombre no quiero acordarme, no ha mucho tiempo que vivía un hidalgo de los de lanza en astillero, adarga antigua, rocin flaco y galgo corredor. Una olla de algo más vaca que carnero, salpicón las más noches, duelos y quebrantos los sábados, lentejas los viernes, algún palomino de añadidura los domingos, consumían las tres partes de su hacienda. El resto della concluian sayo de velarte, calzas de velludo para las fiestas con sus pantuflos de lo mismo, los días de entre semana se honraba con su yellori de lo más fino. Tenía en su casa una ama que pasaba de los cuarenta, y una sobrina que no llegaba a los veinte, y un mozo de campo y plaza, que así ensilaba el rocin como tomaba la podadera. Frisaba la edad de nuestro hidalgo con los cincuenta años, era de complección recia, seco de carnes, enjuto de rostro; gran madrugador y amigo de la caza. Quieren decir que tenía el sobrenombe de Quijada o Quesada (que en esto hay alguna diferencia en los autores que deste caso escriben), aunque por conjecturas verosímiles se deja entender que se llama Quijana; pero esto importa poco a nuestro cuento; basta que en la narración déj no se salga un punto de la verdad.

Es, pues, de saber, que este sobredicho hidalgo, los ratos que estaba ocioso (que eran los más del año) se daba a leer libros de caballerías con tanta afición y gusto, que olvidó casi de todo punto el ejercicio de la caza, y aun la administración de su hacienda; y llegó a tanto su curiosidad y desatino en esto, que vendió muchas haneges de tierra de sembradura, para comprar libros de caballerías en leer; y así llevó a su casa todos cuantos pudo haber de ellos; y de todos ningunos le parecían tan bien como los que compuso el famoso Feliciano de Silva: porque la claridad de su prosa, y aquellas intrincadas razones suyas, le parecían de perlas; y más cuando llegaba a leer aquellos requiebros y cartas de desafío, donde en muchas partes hallaba escrito: *la razón de la sinrazón que a mi razón se hace, de tal manera mi razón enflaquece, que con razón me quejo de la vuestra fermosura*, y también cuando leía: *los altos cielos que de vuestra divinidad divinamente con las estrellas se fortifican, y os hacen merecedora del merecimiento que merece la vuestra grandeza*. Con estas y semejantes razones perdía el pobre caballero el juicio, y desvelabase por entenderlas, y desentrañarles el sentido, que no se lo sacara, ni las entendiera el mismo Aristóteles, si resucitara para solo ello. No estaba muy bien con las heridas que don Belianis daba y recibía, porque se imaginaba que por grandes maestros que le hubiesen curado, no dejaría de tener el rostro y todo el cuerpo lleno de cicatrices y sefiales, pero con todo alababa en su autor aquél acabar su libro con la promesa de aquella inacabable aventura, y muchas veces le vino deseo de tomar la pluma, y darle fin al pie de la letra como allí se promete; y sin duda alguna lo hiciera, y aun saliera con ello, si otros mayores y continuos pensamientos no se lo estorbaran.

Tuvo muchas veces competencia con el cura de su lugar (que era hombre docto graduado en Sigüenza), sobre cuál había sido mejor caballero, Palmerín de Inglatera o Amadís de Gaula; mas maese Nicolás, barbero del mismo pueblo, decía que ninguno llegaba al caballero del Febo, y que si alguno se le podía comparar, era don Galor, hermano de Amadís de Gaula, porque tenía muy acomodada condición para todo; que no era caballero melindroso, ni tan hlorón como su hermano, y que en lo de la valentía no le iba en zaga.

En resolución, él se enfascó tanto en su lectura, que se le pasaban las noches leyendo de claro en claro, y los días de turbio en turbio, y así, del poco dormir y del mucho leer, se le secó el cerebro, de manera que vino a perder el juicio. Llenósele la fantasía de todo aquello que leía en los libros, así de encantamientos, como de pendencias, batallas, desafíos, heridas, requiebros, amores, tormentas y disparates imposibles, y asentósele de tal modo en la imaginación que era verdad toda aquella máquina de aquellas soñadas invenciones que leía, que para él no había otra historia más cierta en el

# 4. Ocultación en ficheros de texto



En un lugar de hidalgo de los más vaca que ciernes, algún resto della conmismo, los dia que pasaba de que así ensillat cincuenta años de la caza. Qui diferencia en le entender que si déi no se salga

Es, pues, de sa año) se daba a ejercicio de la en esto, que ve que leer; y así bien como los intrincadas raz cartas de desaf hace, de tal ma también cuand fortifican, y os semejantes raz desentrañarles para sólo ello. imaginaba que cuerpo lleno de promesa de aq fin al pie de la otros mayores

Tuvo muchas y Sigüenza), sob maese Nicolás, alguno se le po acomodada co que en lo de la

En resolución, claro, y los dia manera que vir encantamiento: disparates impi máquina de aq

En un lugar de la Mancha, de cuyo nombre no quiero acordarme, no ha mucho tiempo que vivía un hidalgo de los de lanza en astillero, adarga antigua, rocin flaco y galgo corredor. Una olla de algo más vaca que carnero, salpicón las más noches, duelos y quebrantos los sábados, lentejas los viernes, algún palomino de añadidura los domingos, consumían las tres partes de su hacienda. El resto della concluyan sayo de velarte, calzas de velludo para las fiestas con sus pantuflas de lo mismo, los días de entre semana se honraba con su yellori de lo más fino. Tenía en su casa una ama que pasaba de los cuarenta, y una sobrina que no llegaba a los veinte, y un mozo de campo y plaza, que así ensillaba el rocin como tomaba la podadera. Frisaba la edad de nuestro hidalgo con los cincuenta años, era de complexión recia, seco de carnes, enjuto de rostro; gran madrugador y amigo de la caza. Quieren decir que tenía el sobrenombre de Quijada o Quesada (que en esto hay alguna diferencia en los autores que este caso escriben), aunque por conjuraciones verosímiles se deja entender que se llama Quijana; pero esto importa poco a nuestro cuento; basta que en la narración del no se salga un punto de la verdad.

Es, pues, de saber, que este sobredicho hidalgo, los ratos que estaba ocioso (que eran los más del año) se daba a leer libros de caballerías con tanta afición y gusto, que olvidó casi de todo punto el ejercicio de la caza, y aun la administración de su hacienda; y llegó a tanto su curiosidad y desatino en esto, que vendió muchas hanegas de tierra de sembradura, para comprar libros de caballerías en que leer; y así llevó a su casa todos cuantos pudo haber dellos; y de todos ningunos le parecían tan bien como los que compuso el famoso Feliciano de Silva: porque la claridad de su prosa, y aquellas intrincadas razones suyas, le parecían de perlas; y más cuando llegaba a leer aquellos requiebros y cartas de desafío, donde en muchas partes hallaba escrito: *la razón de la sinrazón que a mi razón se hace, de tal manera mi razón enflaquece, que con razón me queja de la vuestra fermezura*, y también cuando leía: *los altos cielos que de vuestra divinidad divinamente con las estrellas se fortifican, y os hacen merecedora del merecimiento que merece la vuestra grandeza*. Con estas y semejantes razones perdía el pobre caballero el juicio, y desvelábase por entenderlas, y desentrañarles el sentido, que no se lo sacara, ni las entendiera el mismo Aristóteles, si resucitara para sólo ello. No estaba muy bien con las heridas que don Belianis daba y recibía, porque se

# 4. Ocultación en ficheros de texto

## Interlineado

En un lugar de la Mancha, de cuyo nombre no quiero acordarme, no ha mucho tiempo que vivía un hidalgo de los de lanza en astillero, adarga antigua, rocin flaco y galgo corredor. Una olla de algo más vaca que carnero, salpicón las más noches, duelos y quebrantos los sábados, lentejas los viernes, algún resto de la misma, los días que pasaba de que así ensillaba el rocio. Quienes iban en la ería, que si de la caza, que de la salga

Este caballero se acostumbraba a leer en la noche, que veía leer; y así bien como los intrincadas razas de cartas de desafío, hace, de tal modo también cuando

desentrañarles para solo ello. imaginaba que cuerpo lleno de promesa de aquél fin al pie de la otros mayores

Tuvo muchas y Sigüenza), sobrino maese Nicolás, alguno se le puso acomodada con que en lo de la

En resolución, claro, y el día manera que vir encantamiento: disparates impidió máquina de aquél

En un lugar de la Mancha, de cuyo nombre no quiero acordarme, no ha mucho tiempo que vivía un hidalgo de los de lanza en astillero, adarga antigua, rocin flaco y galgo corredor. Una olla de algo más vaca que carnero, salpicón las más noches, duelos y quebrantos los sábados, lentejas los viernes, algún palomino de añadidura los domingos consumían las tres partes de su hacienda. El hidalgo concluía su velarte, calzando para las fiestas los zapatos de lo mismo, los días de que se honraba el albor de la noche, Tenía en su casa una amiga que se acostumbraba a los sobrinos que iban a los viernes y un mozo de la villa y plaza, que ensillaba el rocio que iba a la caza, y se trataba la noche de nuestro hidalgo de los de lanza, era el compañero de secuaces, enjundia y destro; gran madruga y amigo de la caza. Quieren decir que se acostumbraba a leer en la noche, Quijada, que es la señora (que en esto no hay ninguna diferencia en los autores que yo he visto) que describen que por su belleza era verosímil a la Virgen. Entendido que se llamaba Quijanga; pero esto importa poco a nuestro tema, basta que la narración sea larga y que sea la verdad.

Es, pues, de saber, que este sobredicho hidalgo, los ratos que estaba ocioso (que eran los más del día) se acostumbraba a leer en la noche, con tanto alimento y gusto, que olvidó casi de todo punto el ejercicio de la caza, y aun la administración de su hacienda; y llegó a tanto su curiosidad y desatino en esto, que vendió muchas hanegas de tierra de sembradura, para comprar libros de caballerías en que leer; y así llevó a su casa todos cuantos pudo haber de ellos; y de todos ningunos le parecían tan bien como los que compuso el famoso Feliciano de Silva: porque la claridad de su prosa, y aquellas intrincadas razones suyas, le parecían de perlas; y más cuando llegaba a leer aquellos requiebros y cartas de desafío, donde en muchas partes hallaba escrito: *la razón de la sinrazón que a mi razón se hace, de tal manera mi razón enfaquece, que con razón me quejo de la vuestra fermezura*, y

también cuando leía: *los altos cielos que de vuestra divinidad divinamente con las estrellas se fortifican, y os hacen merecedora del merecimiento que merece la vuestra grandeza*. Con estas y semejantes razones perdía el pobre caballero el juicio, y desvelaba por entenderlas, y

desentrañarles el sentido, que no se lo sacara, ni las entendiera el mismo Aristóteles, si resucitara para solo ello. No estaba muy bien con las heridas que don Belianis daba y recibía, porque se

# 4. Ocultación en ficheros de texto

## Interlineado



```
1 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2 <w:document xmlns:o="urn:schemas-microsoft-com:office:office" xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships" xmlns:v="urn:schemas-microsoft-com:xml" xmlns:w="http://schemas.openxmlformats.org/wordprocessingml/2006/main" xmlns:wp="http://schemas.openxmlformats.org/drawingml/2006/wordprocessingDrawing"><w:body><w:p>
3 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="240" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t></w:t></w:r></w:pPr></w:r><w:t>un
lugar de la Mancha, de cuya nombre no querlo acordarme, no ha mucho tiempo que vivia un</w:t></w:r></w:p><w:p>
4 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="241" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>hidalgo de los de lanza en astillero, adarga
antigua, rocin flaco y galgo corredor. Una olla de algo</w:t></w:r></w:p><w:p>
5 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="241" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>mas vaca que carnero, salpicón las más
noches, duelos y quebrantos los sábados, lentejas los</w:t></w:r></w:p><w:p>
6 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="240" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>viernes, algún palomino de añadura los
domingos, consumían las tres partes de su hacienda. El</w:t></w:r></w:p><w:p>
7 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="241" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>resto della concluijan sayo de velarate, calzas
de velludo para las fiestas con sus pantuflos de los</w:t></w:r></w:p><w:p>
8 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="240" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>mismo, los días de entre semana se honraba
con su vellor de lo más fino. Tenta en su casa una ama</w:t></w:r></w:p><w:p>
9 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="240" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>que pasaba de los cuarenta, y una sobrina que
no llegaba a los veinte, y un mozo de campo y plaza,</w:t></w:r></w:p><w:p>
10 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="240" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>que así ensillaba el rocin como tombaba la
podadera. Frisaba la edad de nuestro hidalgo con los</w:t></w:r></w:p><w:p>
11 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="240" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>cincuenta años, era de compleción recia, seco
de carnes, enjuto de rostro; gran madrugador y amigo</w:t></w:r></w:p><w:p>
12 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="240" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>de la caza. Quieren decir que tenia el
sobrenombre de Quijada o Quesada (que en este hay alguna</w:t></w:r></w:p><w:p>
13 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="241" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>diferencia en los autores que deste caso
escriben), aunque por conjecturas verosímiles se dejó</w:t></w:r></w:p><w:p>
14 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="240" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>entender que se llama Quijana; pero esto
importa poco a nuestro cuento; basta que en la narración</w:t></w:r></w:p><w:p>
15 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="240" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>xdél no se salga un punto
de la verdad. </w:t></w:r></w:p><w:p>
16 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="241" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>de saber, que este sobredicho
hidalgo, los ratos que estaba ocioso (que eran los más del</w:t></w:r></w:p><w:p>
17 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="241" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>año) se daba a leer libros de caballerías con
tanta afición y gusto, que olvidó casi de todo punto el</w:t></w:r></w:p><w:p>
18 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="240" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>ejercicio de la caza, y aun la administración
de su hacienda; y llegó a tanto su curiosidad y desatino</w:t></w:r></w:p><w:p>
19 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="241" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>en esto, que vendió muchas hanegas de tierra
de sembradura, para comprar libros de caballerías en</w:t></w:r></w:p><w:p>
20 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="241" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>que leer; y así llevó a su casa todos cuantos
pudo haber de ellos; y de todos ningunos le parecian tan</w:t></w:r></w:p><w:p>
21 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="240" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>bien como los que compuso el famoso Feliciano
de Silva; porque la claridad de su prosa, y aquellas</w:t></w:r></w:p><w:p>
22 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="240" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>intrincadas razones suyas, le parecian de
perlas; y más cuando llegaba a leer aquellos requiebros y</w:t></w:r></w:p><w:p>
23 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="240" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>cartas de desafío,
donde en muchas partes hallaba escrito: </w:t></w:r></w:p><w:p>
24 <w:p><w:pStyle w:val="Cuerpodetexto"/><w:spacing w:lineRule="auto" w:lin="241" :before="0" w:after="0"/><w:rPr></w:pPr><w:r><w:t>hace, de tal manera mi razón
y vos, y os hacen merecedora del merecimiento que merece la vuestra graneza. Con estas y
semejantes razones perdía el pobre caballero el juicio, y desvelabase por entenderlas, y
```

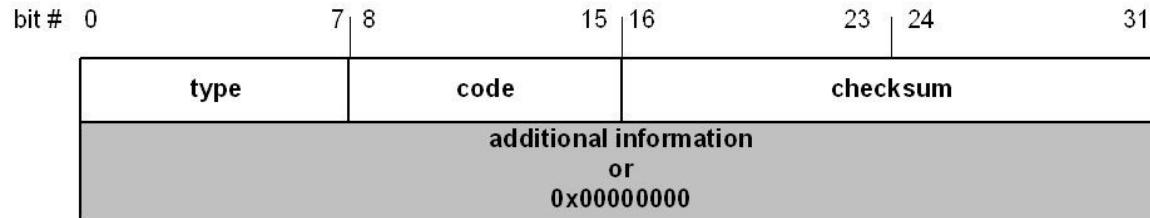
desentrañarles el sentido, que no se lo sacara, ni las entendiera el mismo Aristóteles, si resucitara para solo ello. No estaba muy bien con las heridas que don Belianis daba y recibía, porque se

- 
1. ¿Qué nos impide extraer datos?
  2. Esteganografía en la historia
  3. Ocultación en ficheros de audio
  4. Ocultación en documentos de texto
  - 5. Ocultación en protocolos de red**
  6. Dificultando el descubrimiento
  7. Bibliografía

# 5. Ocultación en protocolos de red



## ICMP message format



### 4 byte header:

- **Type (1 byte):** type of ICMP message
- **Code (1 byte):** subtype of ICMP message
- **Checksum (2 bytes):** similar to IP header checksum.  
Checksum is calculated over entire ICMP message

If there is no additional data, there are 4 bytes set to zero.  
→ each ICMP messages is at least 8 bytes long

# 5. Ocultación en protocolos de red

## ICMP

No.	Time	Source	Destination	Protocol	Length	Info
6971	143.958857	10.136.255.127	45.58.48.13	ICMP	42	Unknown ICMP (obsolete or malformed?)
6972	144.024776	10.136.255.127	45.58.48.13	ICMP	42	Unknown ICMP (obsolete or malformed?)
6973	144.096759	10.136.255.127	45.58.48.13	ICMP	42	Unknown ICMP (obsolete or malformed?)
6974	144.156829	10.136.255.127	45.58.48.13	ICMP	42	Unknown ICMP (obsolete or malformed?)
6975	144.208854	10.136.255.127	45.58.48.13	ICMP	42	Unknown ICMP (obsolete or malformed?)
6976	144.269928	10.136.255.127	45.58.48.13	ICMP	42	Unknown ICMP (obsolete or malformed?)
6977	144.344760	10.136.255.127	45.58.48.13	ICMP	42	Unknown ICMP (obsolete or malformed?)
6978	144.4088762	10.136.255.127	45.58.48.13	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, ttl=64
6979	144.480817	10.136.255.127	45.58.48.13	ICMP	42	Photuris (Bad SPI)
6980	144.540757	10.136.255.127	45.58.48.13	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, ttl=64
6981	144.620750	10.136.255.127	45.58.48.13	ICMP	42	Unknown ICMP (obsolete or malformed?)
6982	144.689171	10.136.255.127	45.58.48.13	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, ttl=64
6983	144.756835	10.136.255.127	45.58.48.13	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, ttl=64

► Frame 6971: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)  
► Ethernet II, Src: Cybertan\_7a:f3:47 (c8:3d:d4:7a:f3:47), Dst: All-HSRP-routers\_01 (00:00:0c:07:ac:01)  
► Internet Protocol Version 4, Src: 10.136.255.127, Dst: 45.58.48.13

▼ Internet Control Message Protocol  
Type: 8 (Unknown ICMP (obsolete or malformed?))  
Code: 0  
Checksum: 0xb8ff [correct]  
[Checksum Status: Good]

0000 00 00 0c 07 ac 01 c8 3d d4 7a f3 47 08 00 45 00 .....= .z.G..E.  
0010 00 1c 00 01 00 00 40 01 13 92 0a 88 ff 7f 2d 3a .....@. ....-:  
0020 30 0d 47 00 b8 ff 00 00 00 00 00 00 00 00 00 00 00 0.G.....

# 5. Ocultación en protocolos de red

## ICMP

No.	Time	Source	Destination	Protocol	Length	Info
697	143.958857	10.136.255.127	45.58.48.13	ICMP	42	Unknown ICMP (obsolete or malformed?)
69	144.024776	10.136.255.127	45.58.48.13	ICMP	42	Unknown ICMP (obsolete or malformed?)
69	144.0968	10.136.255.127	45.58.48.13	ICMP	42	Unknown ICMP (obsolete or malformed?)
69	144.1568	10.136.255.127	45.58.48.13	ICMP	42	Unknown ICMP (obsolete or malformed?)
69	144.2088	10.136.255.127	45.58.48.13	ICMP	42	Unknown ICMP (obsolete or malformed?)
69	144.2699	10.136.255.127	45.58.48.13	ICMP	42	Unknown ICMP (obsolete or malformed?)
69	144.3447	10.136.255.127	45.58.48.13	ICMP	42	Unknown ICMP (obsolete or malformed?)
69	144.4087	10.136.255.127	45.58.48.13	ICMP	42	(ping) request id=0000, seq=0/0, ttl=64
69	144.4808	10.136.255.127	45.58.48.13	ICMP	42	Transmis (Base SPI)
69	144.5407	10.136.255.127	45.58.48.13	ICMP	42	Echo (ping) request id=0000, seq=0/0, ttl=64
69	144.6207	10.136.255.127	45.58.48.13	ICMP	42	Unknown ICMP (obsolete or malformed?)
69	144.6891	10.136.255.127	45.58.48.13	ICMP	42	Echo (ping) reply id=0000, seq=0/0, ttl=64
69	144.756835	10.136.255.127	45.58.48.13	ICMP	42	Echo (ping) reply id=0000, seq=0/0, ttl=64

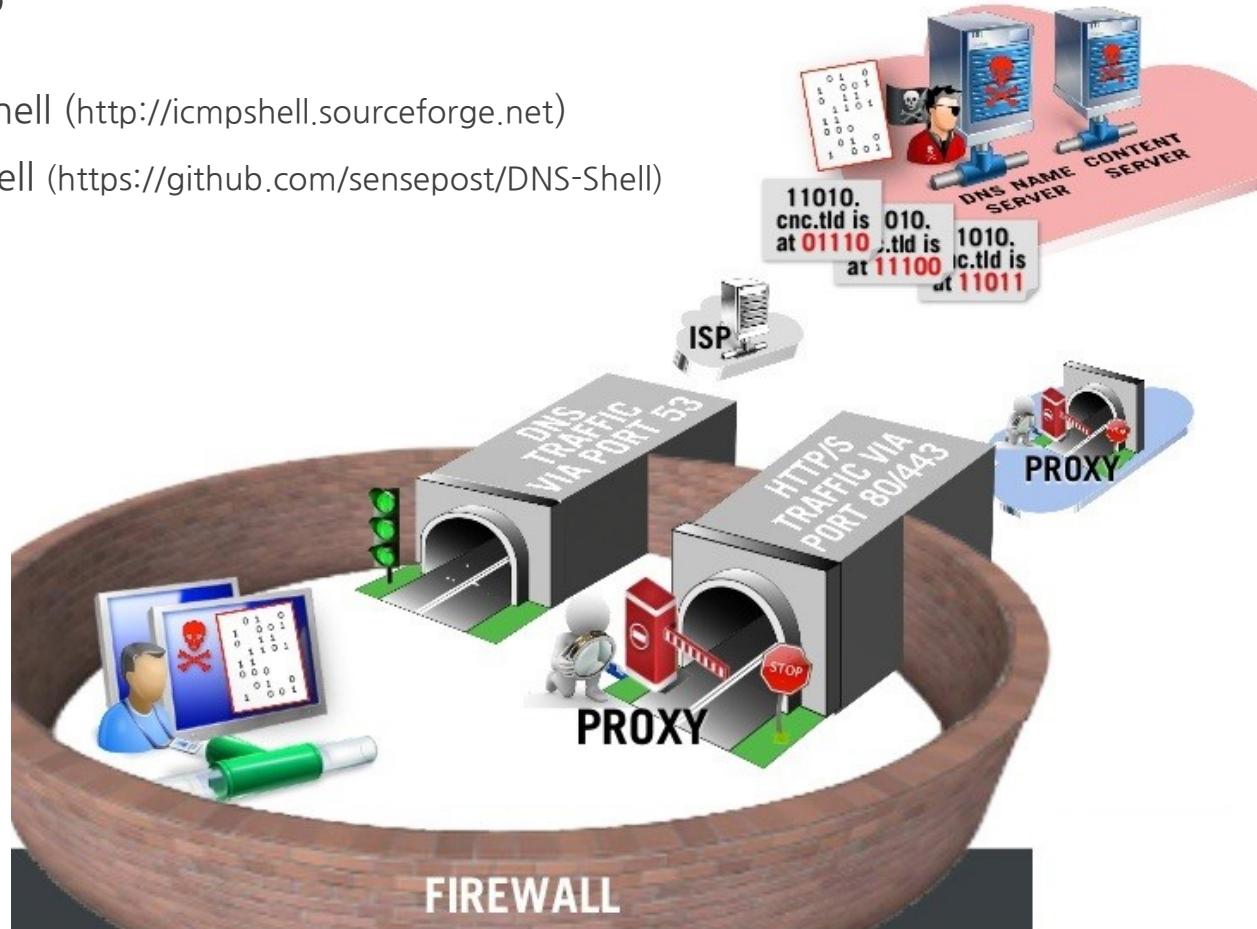
► Frame 6971: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)  
► Ethernet II, Src: Cybertan\_7a:f3:47 (c8:3d:d4:7a:f3:47), Dst: All-HSRP-routers\_01 (00:00:0c:07:ac:00)  
► Internet Protocol Version 4, Src: 10.136.255.127, Dst: 45.58.48.13  
▼ Internet Control Message Protocol (ICMP)  
    Type: 71 (Unknown ICMP (obsolete or malformed?))  
    Code: 0  
    Checksum: 0xb8ff [correct]  
    [Checksum Status: Good]

0000 00 00 0c 07 ac 01 c8 3d d4 7a f3 47 08 00 45 00 .....=.z.G..E.  
0010 00 1c 00 01 00 00 40 01 13 92 0a 88 ff 7f 2d 3a .....@.....-:  
0020 30 0d 47 00 b8 ff 00 00 00 00 00 00 00 00 00 00 00 0.G.....

# 5. Ocultación en protocolos de red

## Tunneling

- ICMP Shell (<http://icmpshell.sourceforge.net>)
- DNS Shell (<https://github.com/sensepost/DNS-Shell>)
- ...



# Contenido

1. ¿Qué nos impide extraer datos?
2. Esteganografía en la historia
3. Ocultación en ficheros de audio
4. Ocultación en documentos de texto
5. Ocultación en protocolos de red
- 6. Dificultando el descubrimiento**
7. Bibliografía

# 6. Dificultando el descubrimiento

## Ejemplos

Modificación de cabeceras

Alteración del orden de inserción en LSB

Utilizar contraseñas

Utilizar datos cifrados/codificados

No repetir siempre la misma técnica o patrón

...

# 6. Dificultando el descubrimiento

No ser demasiado obvios

# 6. Dificultando el descubrimiento

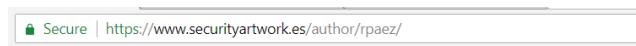
No ser demasiado obvios



- 
1. ¿Qué nos impide extraer datos?
  2. Esteganografía en la historia
  3. Ocultación en ficheros de audio
  4. Ocultación en documentos de texto
  5. Ocultación en protocolos de red
  6. Dificultando el descubrimiento
  7. **Bibliografía**

# 7. Bibliografía / Enlaces

## Artículos del blog - <https://www.securityartwork.es/author/rpaez/>



### Esteganografía: Ocultando el uso de LSB

7 de marzo de 2013 by Rafael Páez

Después de haber hablado en varias ocasiones sobre la esteganografía, volvemos al tema ampliando un poco más la técnica de LSB (Ocultando archivos en otros – LSB, Ocultando archivos en otros – LSB II)... [Leer Más](#)



### Reto: ¿Dónde será el encuentro? – Solución

19 de febrero de 2013 by Rafael Páez

Hace unos días propusimos un [nuevo reto en el blog](#), el cual consistía en obtener el lugar exacto donde se reuniría la banda que se había estado investigando desde hacía unos meses gracias la obtención de un archivo que había sido enviado a uno de los componentes y dos SMS guardados en el teléfono móvil de la banda. El reto consistía en descifrar el archivo que había sido detenido recientemente. Así que en esta ocasión, toca explicar la s

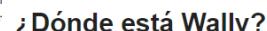


En este nuevo reto, partímos de la siguiente imagen... [Leer Más](#)

### Reto: ¿Dónde será el encuentro?

13 de febrero de 2013 by Rafael Páez

Después de un tiempo sin proponer ningún reto, volvemos con nuestro equipo de investigación para presentaros el paso de conocer el siguiente punto de encuentro de la banda que llevan investigando.



10 de septiembre de 2012 by Rafael Páez

Después de un tiempo sin poner ningún reto en el blog, aquí os traemos uno nuevo :). [Leer Más](#)

### ¿Rojo, azul o amarillo? Pues va a ser...

26 de marzo de 2012 by Rafael Páez

Para este nuevo reto de esteganografía, partímos de la siguiente imagen la cual sabíamos que contenía el color del cable que conseguía desactivar la detonación de la bomba en caso de una emergencia. Color que era la solución al reto.... [Leer Más](#)



### ¿Rojo, azul o amarillo?

20 de marzo de 2012 by Rafael Páez

(N.d.E. A partir de ahora gracias al volumen y calidad de las colaboraciones de Rafa, pueden encontrar todas sus entradas, futuras y pasadas, en el menú de autores ubicado en el lateral de la derecha.)... [Leer Más](#)



### Ocultando archivos en otros – LSB (II)

28 de febrero de 2012 by Rafael Páez

Rafa Páez, al que [podéis encontrar en su twitter](#), acaba la serie sobre el método LSB para ocultar información en imágenes con un ejemplo práctico.

Para comprender mejor la [técnica de esteganografía comentada en la entrada del viernes](#), he realizado una serie de scripts en PHP que nos permiten realizar todo este procedimiento de manera automática, simplemente indicando los archivos a utilizar.... [Leer Más](#)

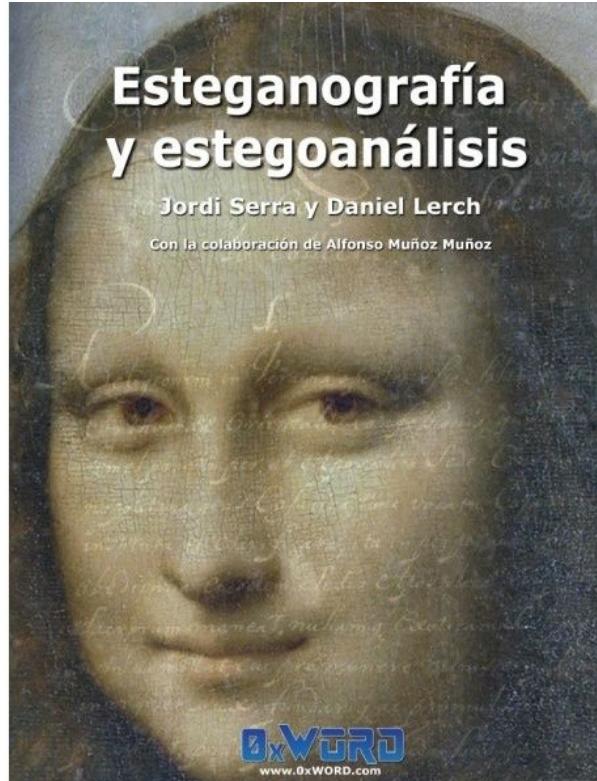


# 7. Bibliografía / Enlaces

## Esteganografía y estegoanálisis

Jordi Serra y Daniel Lerch

0xWORD

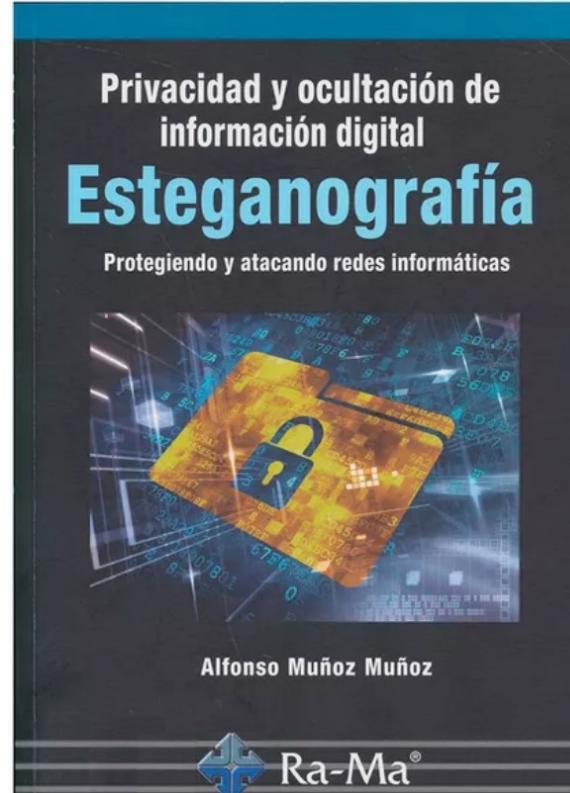


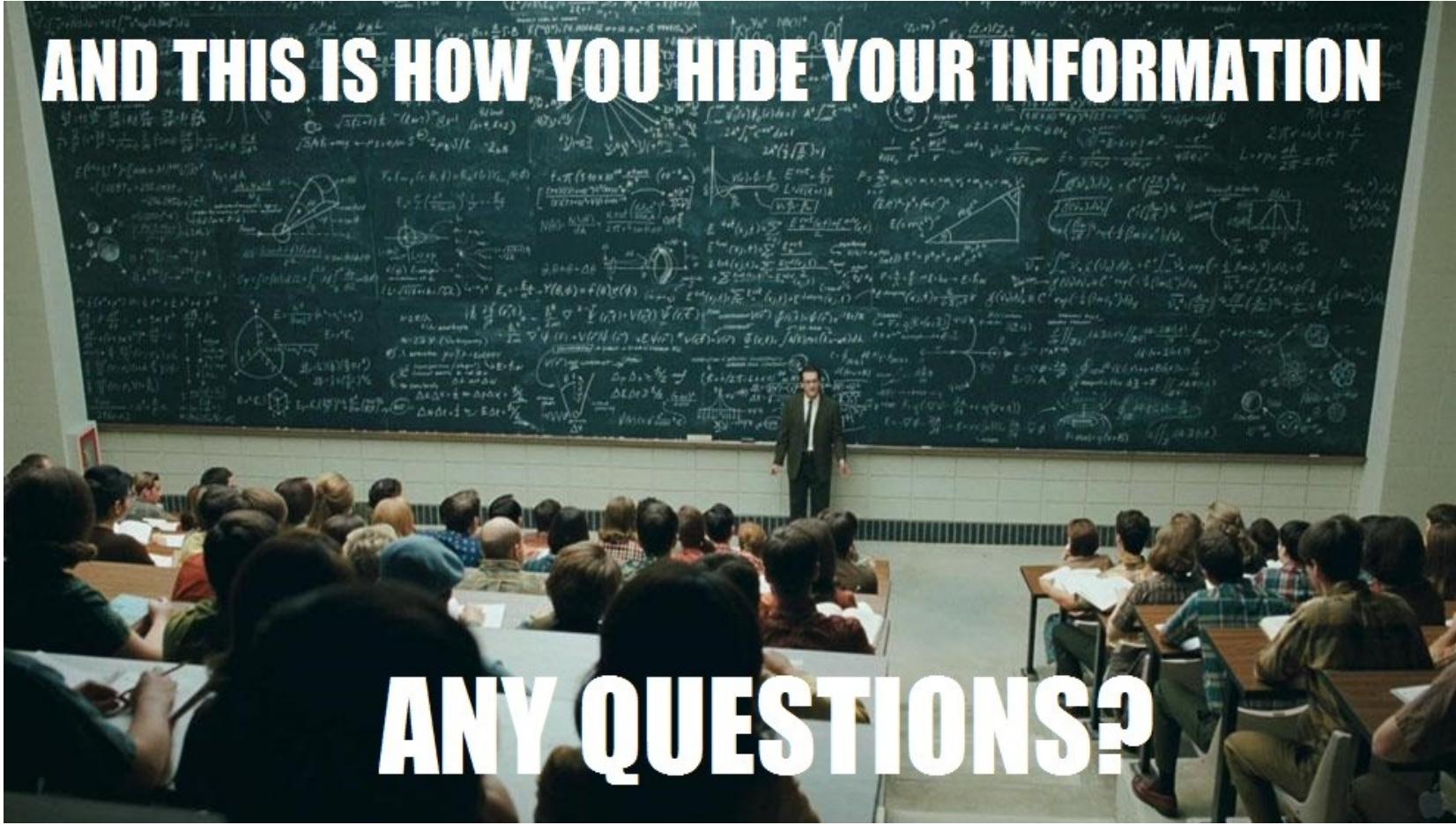
# 7. Bibliografía / Enlaces

Privacidad y ocultación de información digital

Alfonso Muñoz Muñoz

Ra-Ma





**AND THIS IS HOW YOU HIDE YOUR INFORMATION**

**ANY QUESTIONS?**

# HACK &BEERS

#hbTarragona



Esteganografía: Exfiltración de datos sin ser descubierto en el intento

Rafael Páez Jaime  
@fikih888