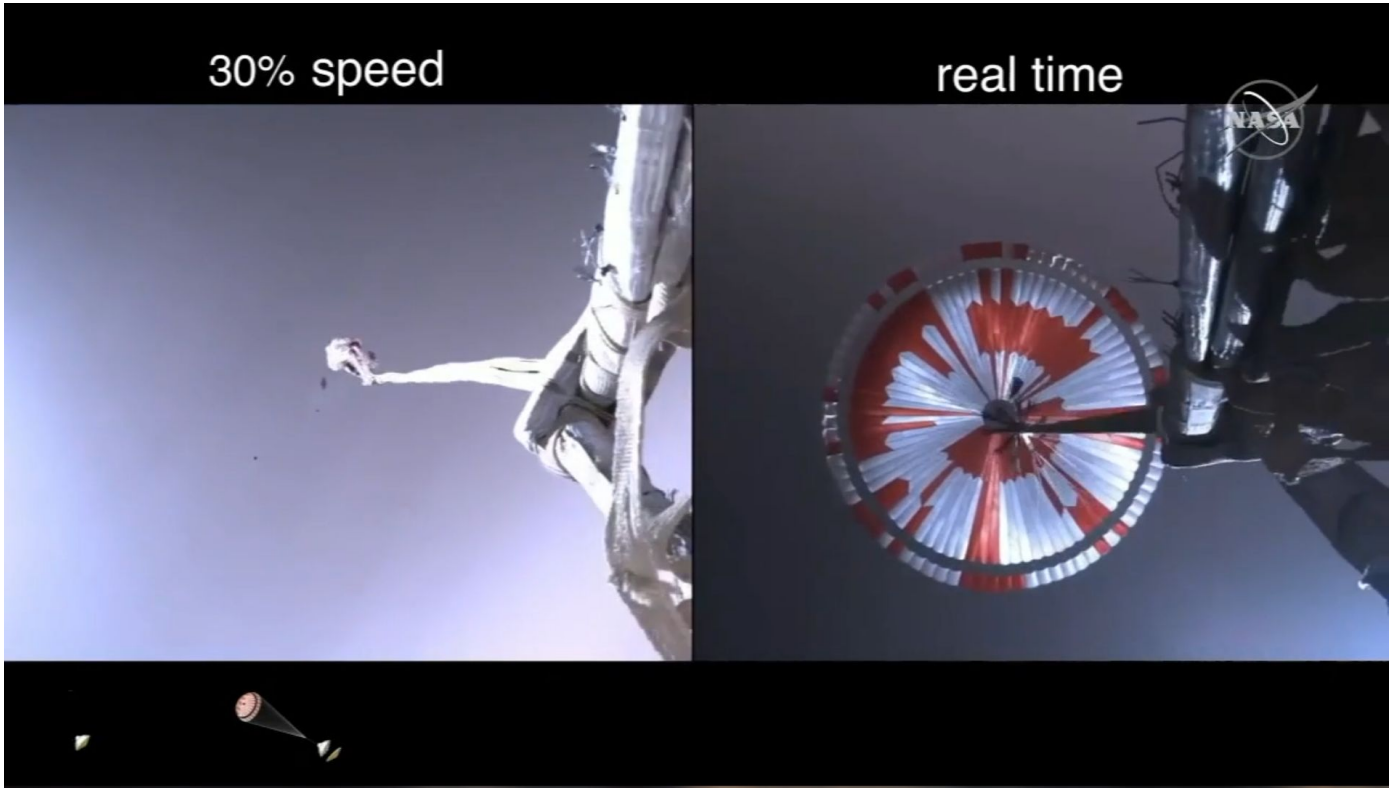
Esteganografía
Parte 2: Stego en texto, imágenes y sonido.

CC5325 - Taller de Hacking Competitivo

¿Stego?



¿Stego?

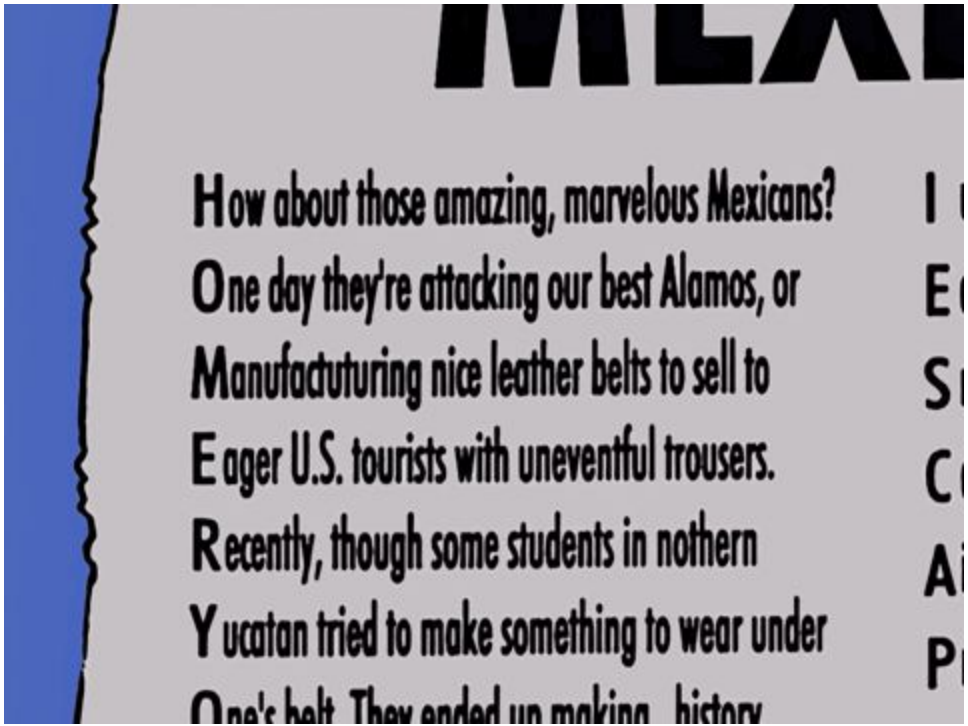
0	0	1	0	1	1	1	→ 23 →	W

Stego en Texto

- **Archivos de texto:** Poco espacio para esconder información.
  - El contenido completo del archivo es mostrado por un visor de archivos de texto.
    - No hay headers
    - No hay metainformación
    - No hay forma de cortar la lectura del archivo antes de su término

Stego en texto

- **Acrósticos:** Mensajes ocultos en las primeras (n) letras de cada palabra, oración o párrafo de un texto.



GIF de Los Simpsons S12E02

Stego en Texto

Caracteres Invisibles: Con 2 caracteres invisibles podemos escribir mensajes en binario:

- **Tabs/Espacios al final de cada línea**
- **Zero-Width Joiner (ZWJ) y Zero-Width Non-Joiner (ZWNJ)** al final o al medio del texto

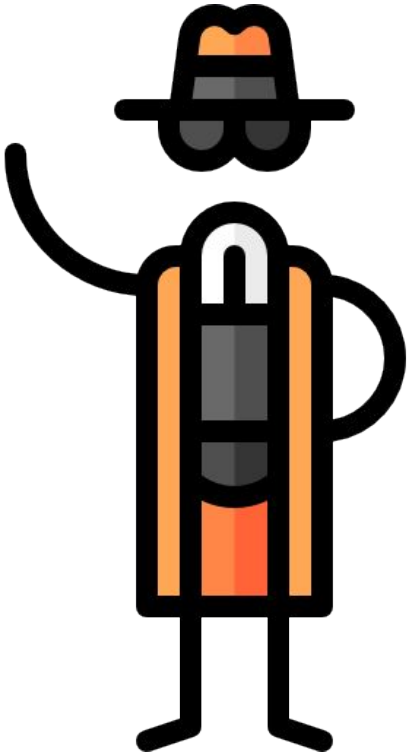
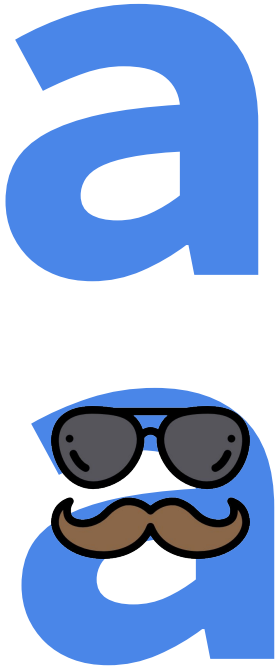


Imagen de freepik en https://flaticon.com

Stego en Texto

Tenemos secuestrado tu computador. Envia 1 bitcoin a esta dirección y te lo devolveremos 88

- **Caracteres homoglifos Unicode**
  - **Muy parecidos a originales:**
    - **Pasar desapercibidos.**
    - **Se puede comprobar revisando valor hexadecimal de cada caracter.**
  - **No tan parecidos, pero legible**
    - **Efecto "Nota de Secuestro"**
    - **Más variedad de posibles sustitutos, por lo que mensajes contenedores pueden ser más cortos.**

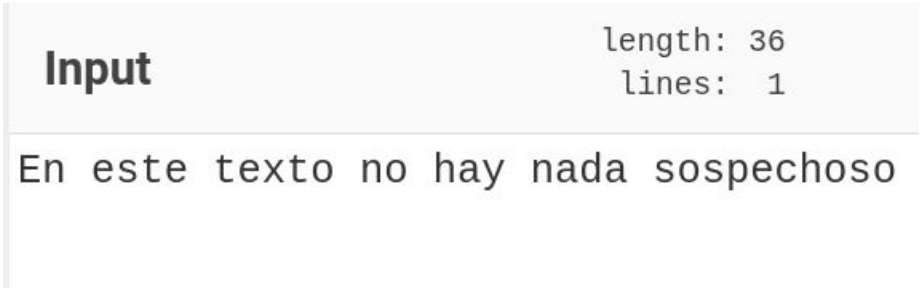


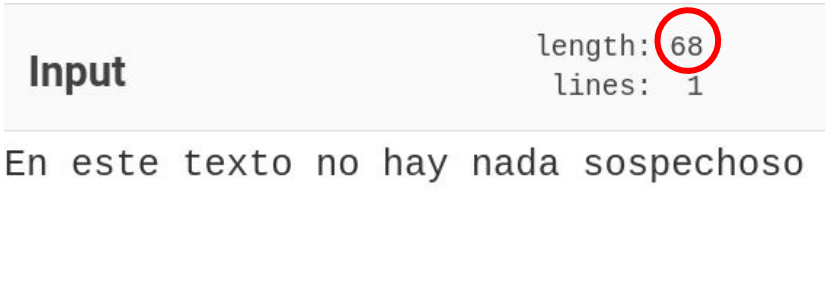
https://www.irongeek.com/i.php?page=security/unicode-steganography-homoglyph-encoder

Imagen de freepik en https://flaticon.com

Stego en texto: Recomendaciones

Comparar largo de texto visible con largo reportado por algún editor de texto:

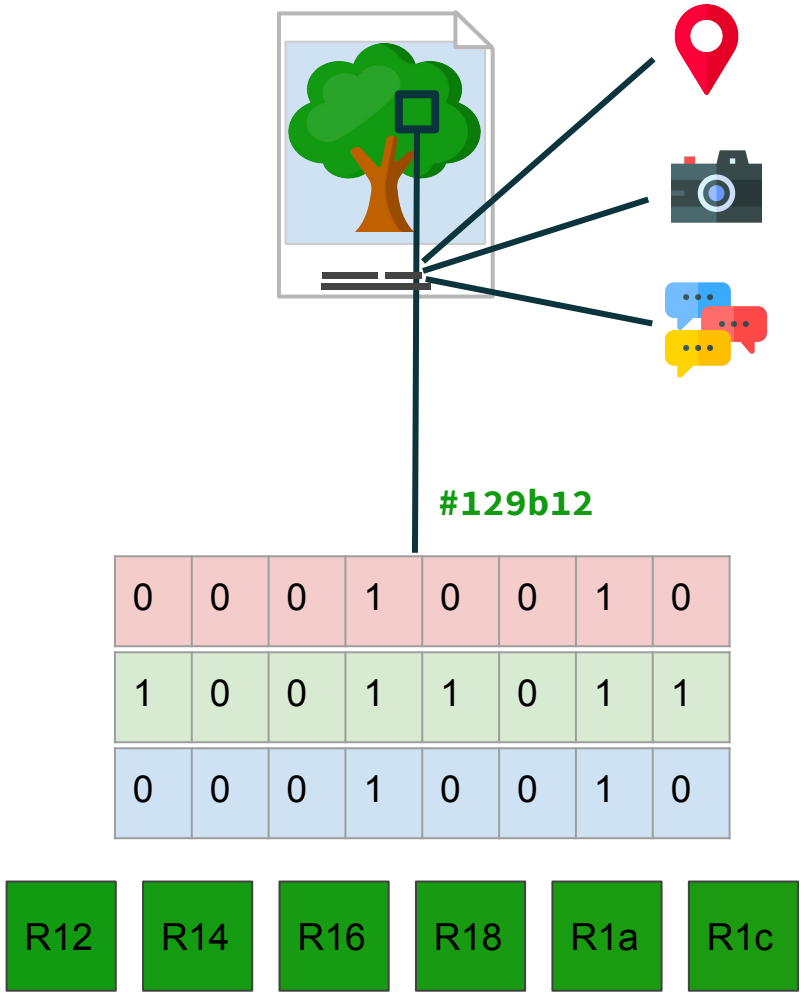




Stego en Imágenes

Imágenes son archivos más grandes y pesados que texto.

- Pueden guardar metadatos.
- Es posible tener dos imágenes aparentemente idénticas, pero compuestas por bytes distintos
- Formatos comunes: JPEG, PNG, GIF, WEBP



Imágenes de freepik en https://flaticon.com

Stego en imágenes

- **LSB (least significant bit):**
  - **Colores cercanos se ven muy parecidos**
  - **Podemos usar últimos n bits de cada color para codificar información (texto u otro archivo)**
  - **Es más, podemos cifrar la información oculta con una llave para que cueste más identificarla.**

hola => 8 15 17 1 => 001000 001111 010001 000001
Si tomo 1 LSB de cada componente de cada color, puedo escribir un mensaje en algo aparentemente verde (#129c12):

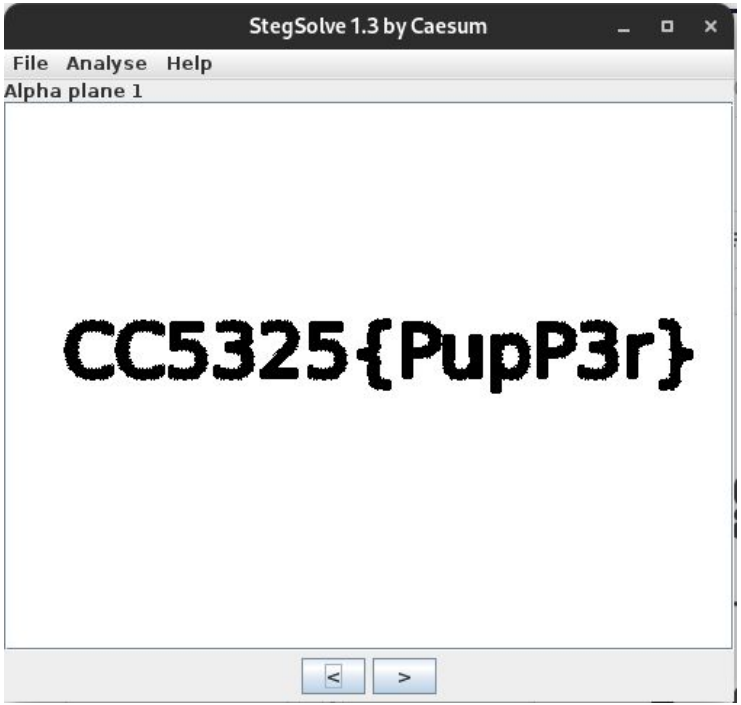
0 0 1	0 0 0	0 0 1	1 1 1	0 1 0	0 0 1	0 0 0	0 0 1
#129c13	#129c12	#129c13	#139d13	#129d12	#129c13	#129c12	#129c13

Stego en imágenes

- **Canal de color (RGBA):**
  - **Modificar un canal de color ligeramente, de forma de que al aislar la capa de color se muestre un mensaje visual.**
  - **A veces se hace con el canal Alpha (transparencia).**

Stego en imágenes

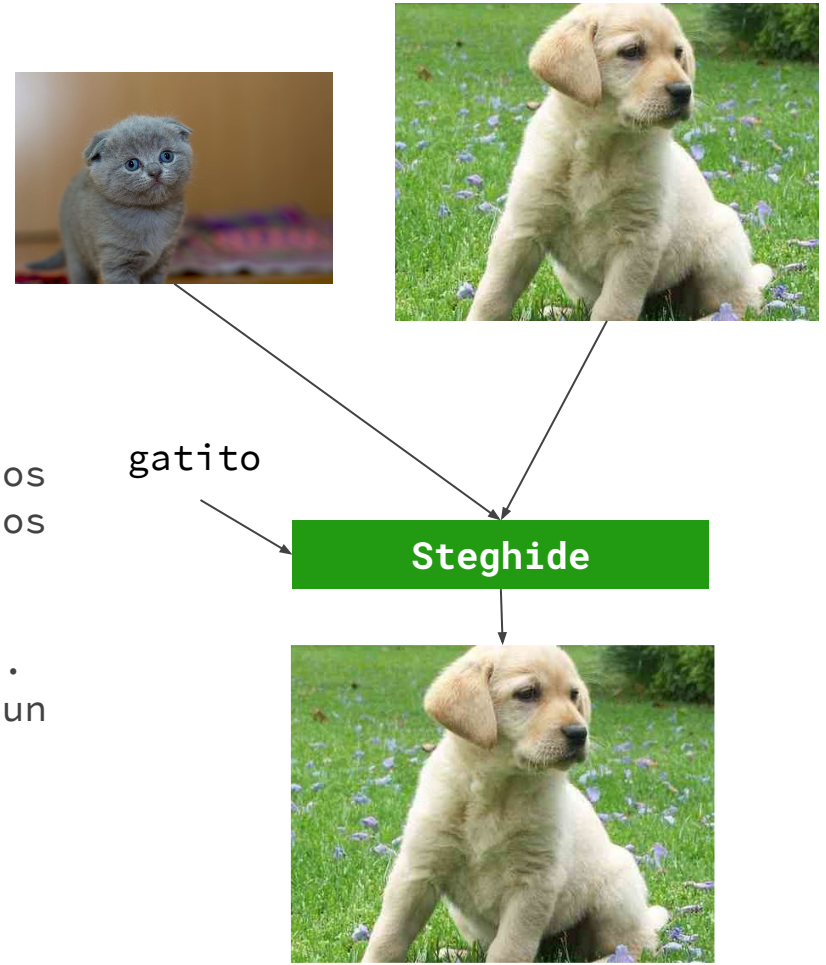
- **Canal de color (RGBA):**
  - **Modificar un canal de color ligeramente, de forma de que al aislar la capa de color se muestre un mensaje visual.**
  - **A veces se hace con el canal Alpha (transparencia).**



Stego en imágenes

Programas especiales:

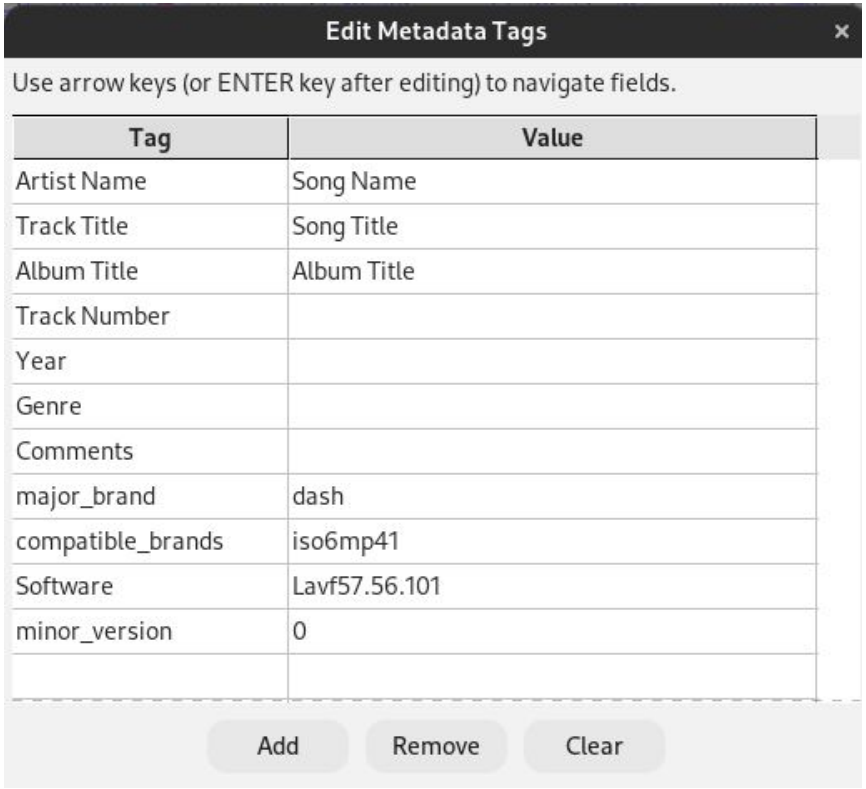
- **Ejemplo: Steghide**
  - Permite esconder otros archivos en imágenes y audios de ciertos tipos.
  - Es posible asignarles una contraseña para su extracción. La contraseña suele estar en un archivo extra o en metadatos.
- Si no hay contraseña: **Stegforce** + wordlist



Stego en audios

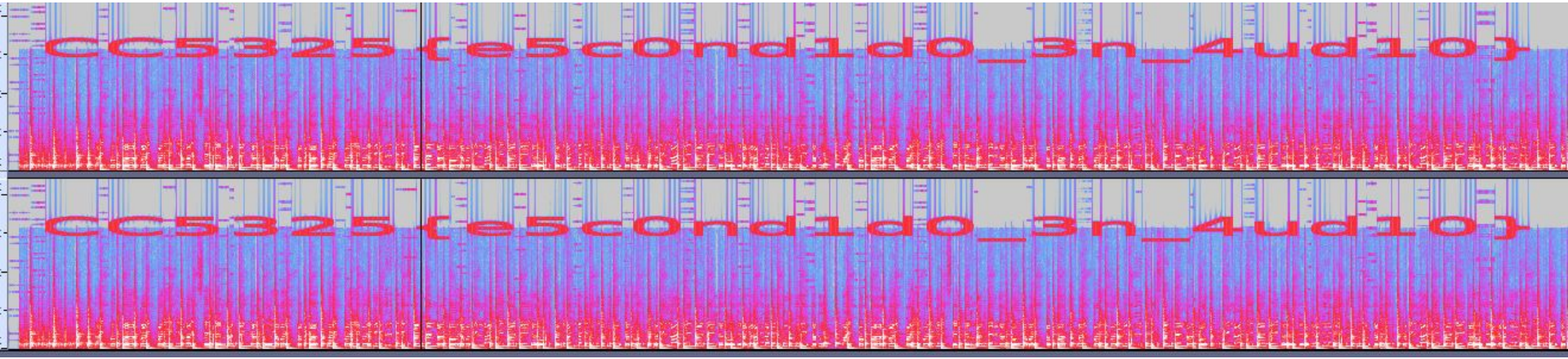
Metadatos:

- **ID3:** Archivos MP3 permiten guardar como metadato
    - Texto (Artista, título, álbum, etc)
    - Portada de disco (imagen)



Stego en audios

Espectrograma de Frecuencia
(https://github.com/solusipse/spectrology)



Stego en audios

Datos por audio

Existen codificaciones conocidas para transmitir datos en audio:

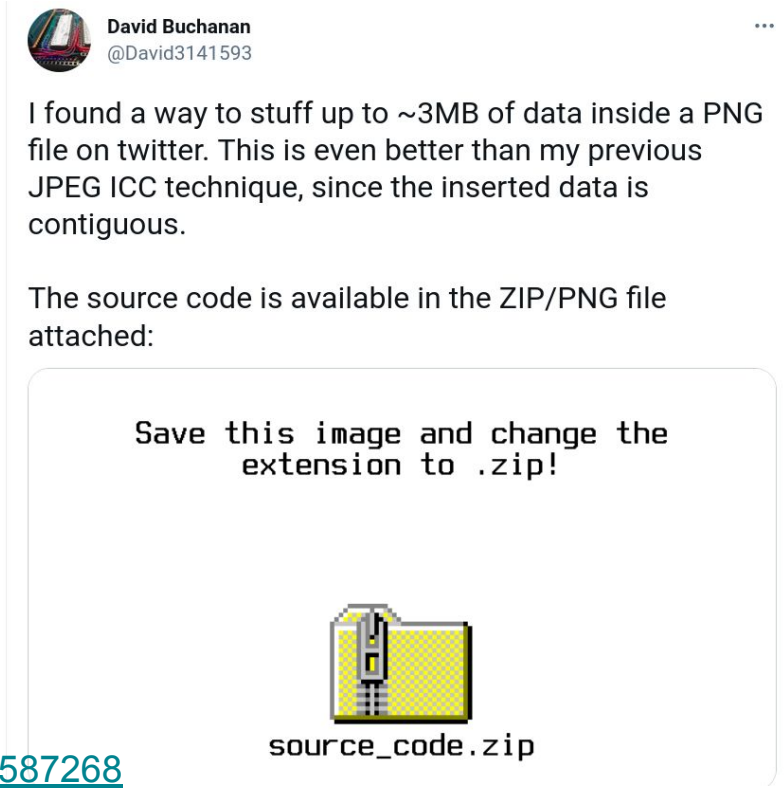
- **Modems (Datos binarios en sonido)**
- **Programas (Commodore 64)**
- **DTMF (tonos)**

DTMF keypad frequencies (with sound clips)

	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

Stego en Archivos Binarios en General

- **Binwalk:** Permite detectar archivos concatenados con nuestro archivo principal (y extraerlos)
- **Texto entre medio:** Una forma de detectarlo es con **GNU Strings** sobre el binario. Puede estar codificado.
- **Archivos especiales**



https://twitter.com/David3141593/status/1371974874856587268