



Auditoría y Legislación Informática

Análisis Forense de Discos



Auditoría y Legislación Informática

1. Descripción del reto

Este reto se compone de varias fases, cada una diseñada para aplicar distintos conceptos y habilidades de resolución.

En la primera fase, se ha utilizado la esteganografía para ocultar información en un video llamado **Aqui comienza todo.mp4**. También se ha ocultado información cifrada con pistas en la imagen **No hay nada oculto aquí.bmp**.

Además, en el propio vídeo se encuentra el enlace que permite acceder a la segunda fase.

En la segunda fase, se presentan tres archivos distintos: **programita.jar**, **fruta**, y **No tengo nada**. Entre estos archivos tenemos el llamado **no tengo nada**, que contiene una imagen con un enlace al archivo **No se puede pasar** de la fase 3. Además con Ingeniería inversa hemos creado el **programita.jar** con contraseña. Esta contraseña se obtiene al resolver un desafío en **fruta**, que proporciona la clave para acceder al archivo **programita.jar**. Este archivo, al ser ejecutado, permite obtener la siguiente contraseña necesaria para avanzar y la primera letra de la clave final.

En la tercera fase, el participante accede a un código QR que enlaza directamente al archivo final **premio.zip**.

Adicionalmente, se proporciona un archivo PDF sin extensión, el cual incluye la pista para deducir la última parte de la contraseña final que permitirá abrir **premio.zip** y acceder al contenido que constituye el premio del reto.

Este flujo de resolución como hemos indicado, introduce conceptos clave de esteganografía, criptografía e ingeniería inversa, guiando al participante paso a paso en el uso de herramientas y técnicas necesarias para desentrañar el desafío completo y acceder al premio final.

Para ello se facilita una carpeta comprimida **Materiales.rar** cuyo tamaño es de 35,4 MB la cual da paso a la fase 1 como se observa en el Figura 1

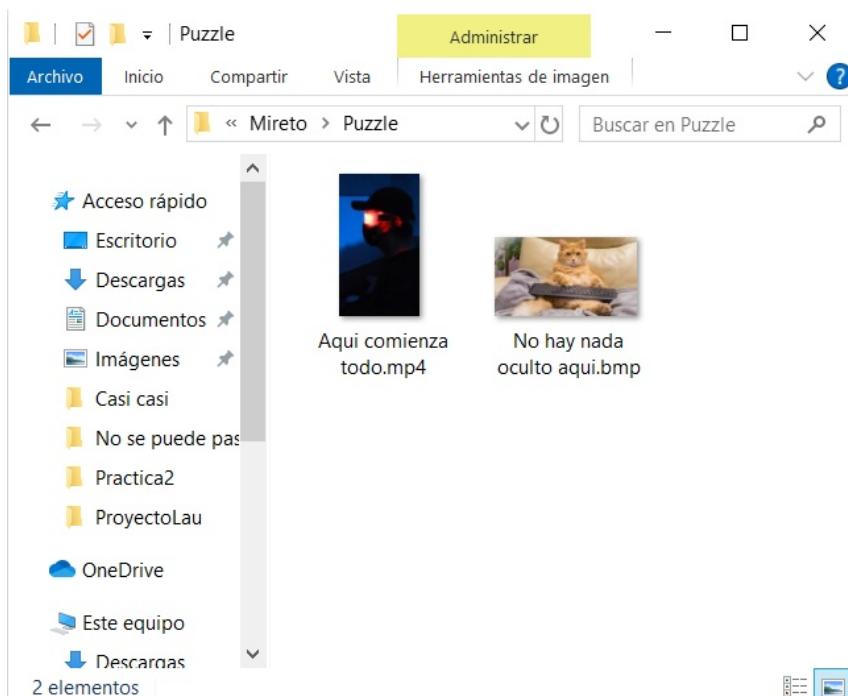


Figura 1: Imagen donde se muestra el contenido del archivo Materiales.rar

2. Pasos para la creación del reto

Para la creación de este reto se tienen que seguir varios pasos los cuales tendrá que resolver el usuario para la obtención del premio.

2.1 Creación de mensaje, instrucciones o pistas

Lo primero que se debe tener claro es el mensaje y las pistas a proporcionar. Es sumamente importante que las instrucciones queden lo suficientemente claras. La dificultad del reto no se debe encontrar en ocultar información que indique como se resuelve si no en el proceso de resolución.

Para obtener el archivo protegido **premio.zip**, primero necesitas descubrir que se encuentra alojado en la nube, específicamente en el siguiente enlace de Google Drive:

<https://drive.google.com/file/d/1nzZQRgbfTsjPxn1dNKDPMCrliwWJTC0/view?usp=sharing>

La contraseña para desbloquear el archivo **PREMIO.zip** es "**quieroAprobar**", generada en pasos anteriores como parte del reto. Para facilitar el acceso, puedes escanear un código QR que te llevará directamente a este enlace de Drive, donde se encuentra el archivo.

En la **Figura 2** se muestra la imagen denominada **PREMIO.zip**, que representa el premio del desafío. Esta imagen fue comprimida en el archivo **PREMIO.zip** y está protegida con la contraseña mencionada, la cual simboliza el logro de completar el reto.



Figura 2. Imagen "Conseguido.jpg" protegida por la contraseña "quieroAprobar"

Para poder acceder al archivo **premio.zip**, primero deberás completar una serie de fases y retos. A lo largo de estos desafíos, obtendrás la primera parte de la contraseña, que es "**quiero**". Posteriormente, tras resolver algunos retos adicionales, obtendrás la segunda parte de la contraseña, "**Aprobar**".

2.2 Fase 1 del reto: Esteganografía y ocultación de información cifrada

En la esteganografía se va a ocultar el enlace para acceder al archivo de la fase 2.

- Se procede a ocultar el siguiente enlace <https://drive.google.com/file/d/1TLuUxo4aU-yGJDQ2IHgFWCpLEQgLWaOT/view?usp=sharing>

2.2.1 Ocultar información en espectrograma sonido “Aqui comienza todo.mp4”

Los primero que he hecho para introducir el enlace en el espectrograma de un audio ha sido crear una imagen con el mensaje que se desea incrustar con un formato .bmp. Para crear esta imagen con el enlace he usado Paint, como se muestra en la Figura 3

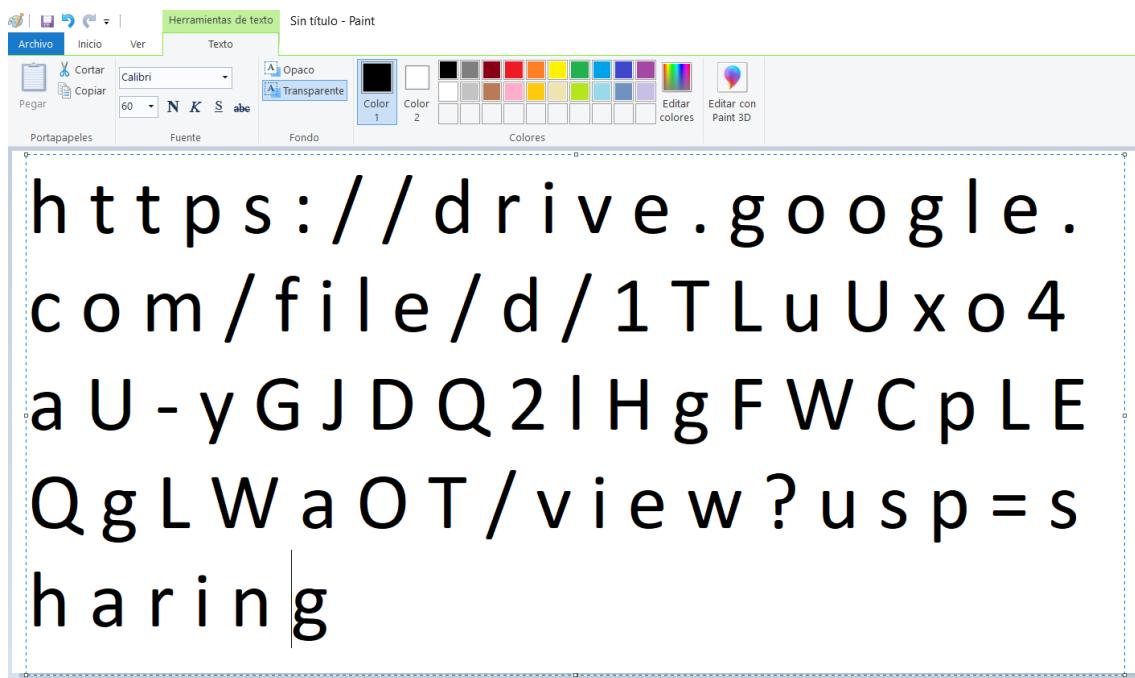


Figura 3: Imagen donde se muestra la creación del “.bmp” con el enlace a Google drive

Después, se procede a utilizar la aplicación *Coagula Light* para importar la imagen “drive.bmp” para transforma en un sonido y añadirla después al video como muestra la Figura 4 .



Figura 4: Imagen donde se muestra la creación del “.wav” para la introducción en el video

Una vez convertida la imagen a formato “.wav” guardaremos el archivo y procederemos a comprobar si se ha realizado de manera correcta analizando el espectrograma con la herramienta *Audacity* para revelar el contenido y posteriormente añadirlo al video. En la Figura 5 y 6 podemos observar el proceso del espectrograma:

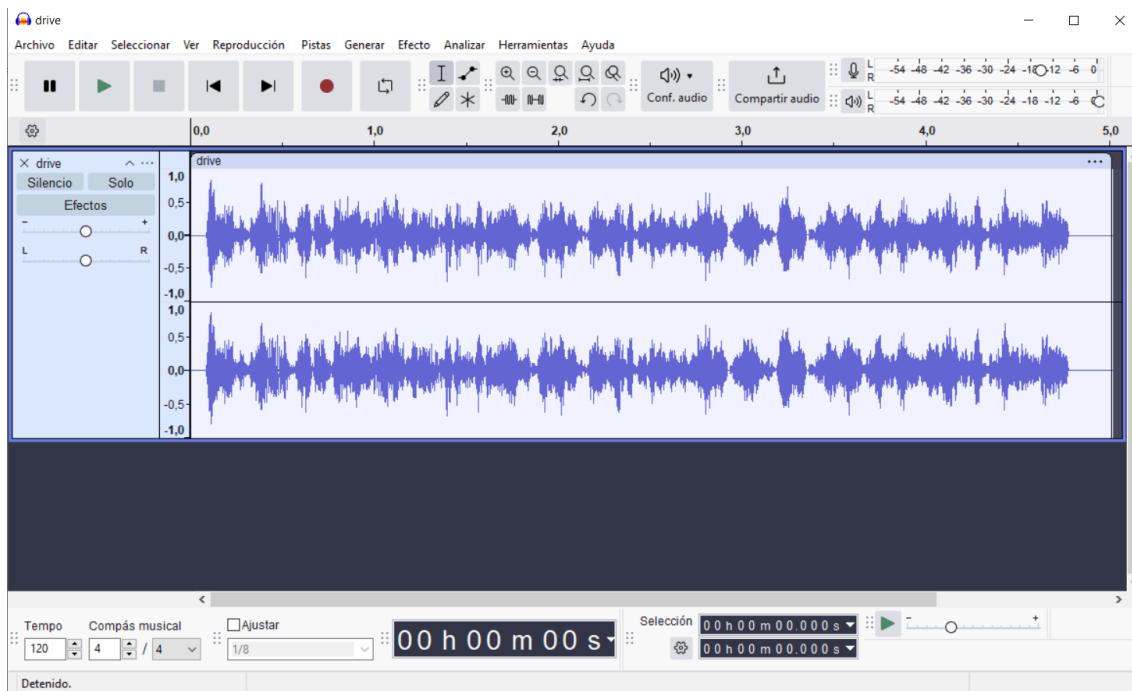


Figura 5: Imagen donde se muestra el archivo “.wav” en Audacity

En la *Figura 6* podemos observar en el espectrograma el siguiente enlace:

[“<https://drive.google.com/file/d/1TLuUxo4aU-yGJDQ2IHgFWCpLEQgLWaOT/view?usp=sharing>”](https://drive.google.com/file/d/1TLuUxo4aU-yGJDQ2IHgFWCpLEQgLWaOT/view?usp=sharing)

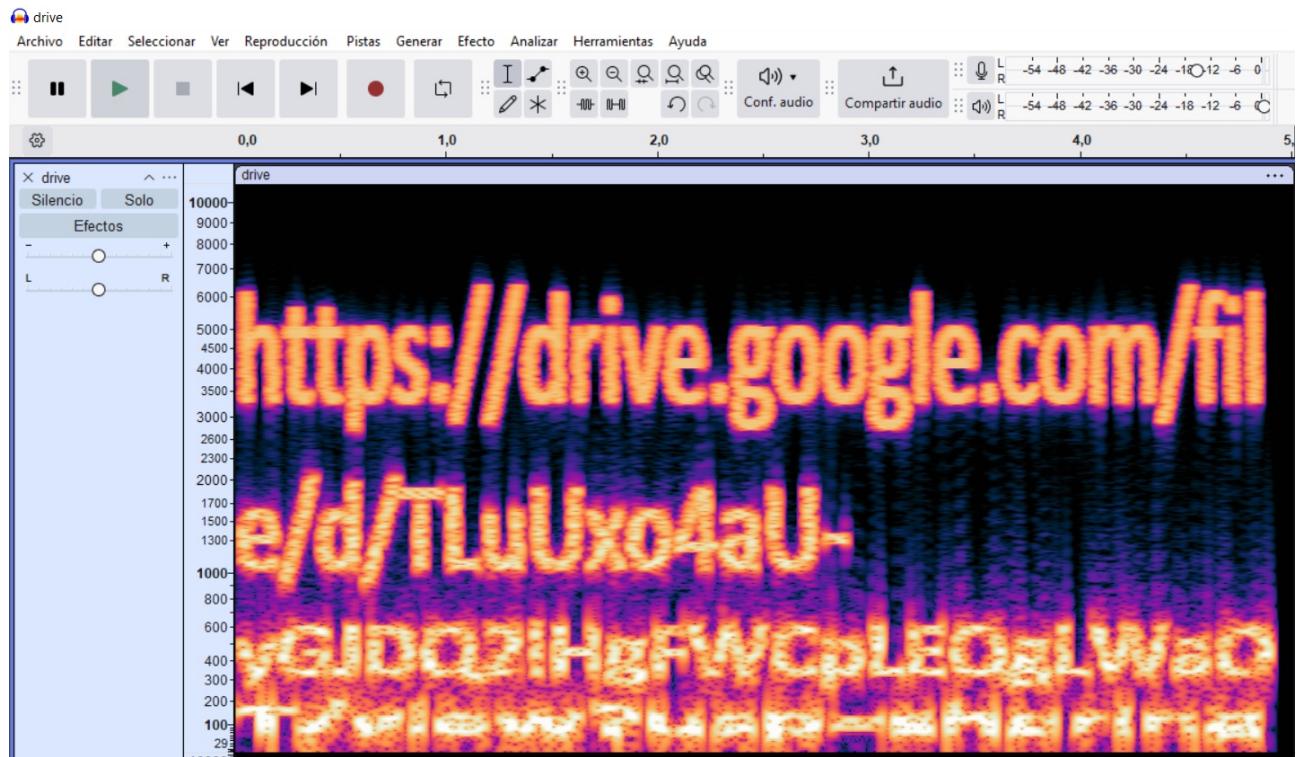


Figura 6: Imagen donde se muestra el espectrograma del archivo “drive.wav” en Audacity

Después de crear este audio lo añadiremos al video **Aqui comienza todo.mp4** con la herramienta de edición de video “Microsoft Clipchamp”, la cual nos va a permitir modificar y añadir el audio del video. Como se muestra la *Figura 7* primero importaremos el audio **drive.wav** y el video **Aqui comienza todo.mp4**.

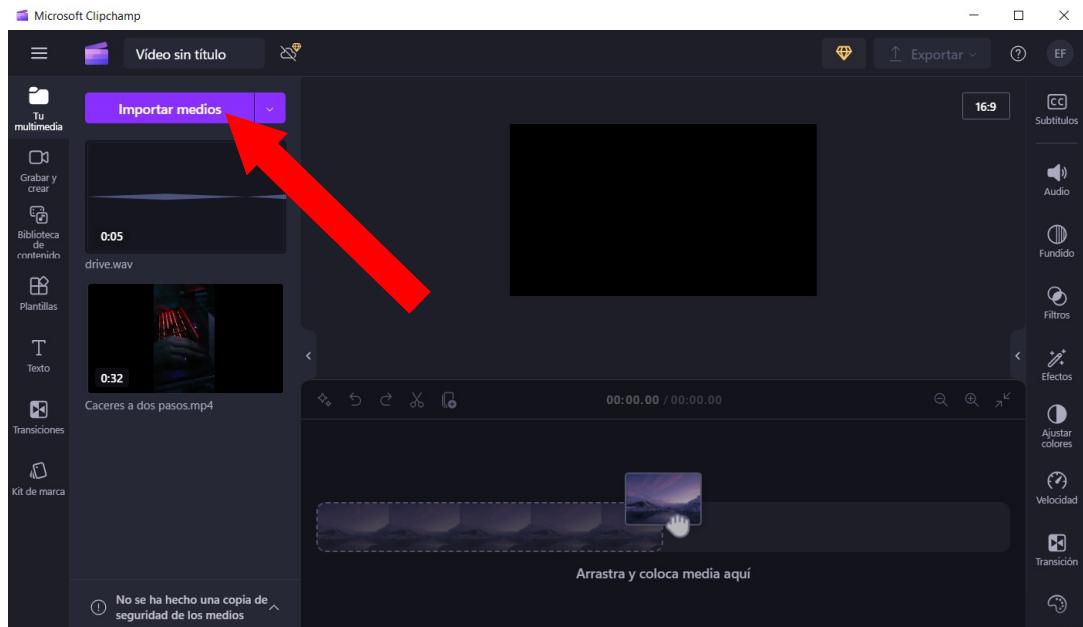


Figura 7: Imagen donde se muestra como importar medios en “Microsoft Clipchamp”.

En la *Figura 8* se observa como eliminamos parte del audio del video original para dar paso al nuevo audio y así poder tener la información oculta guardada.

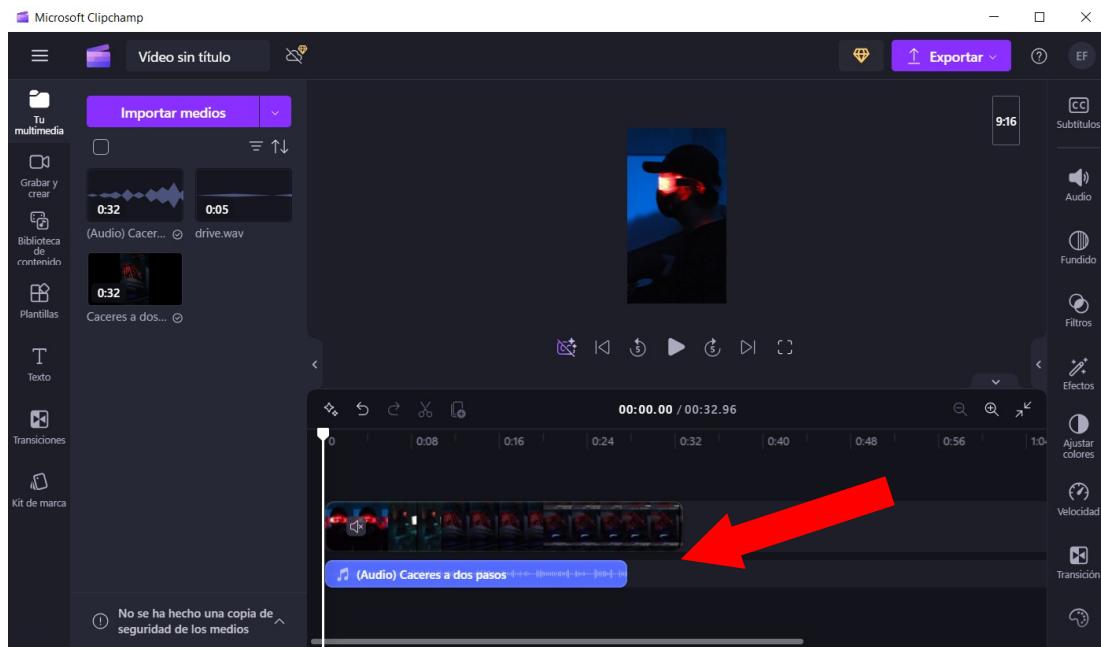


Figura 8: Imagen donde se elimina parte del audio del video.

En la *Figura 9* se muestra como añadimos el audio de drive.wav y así tenemos la información oculta en el video.

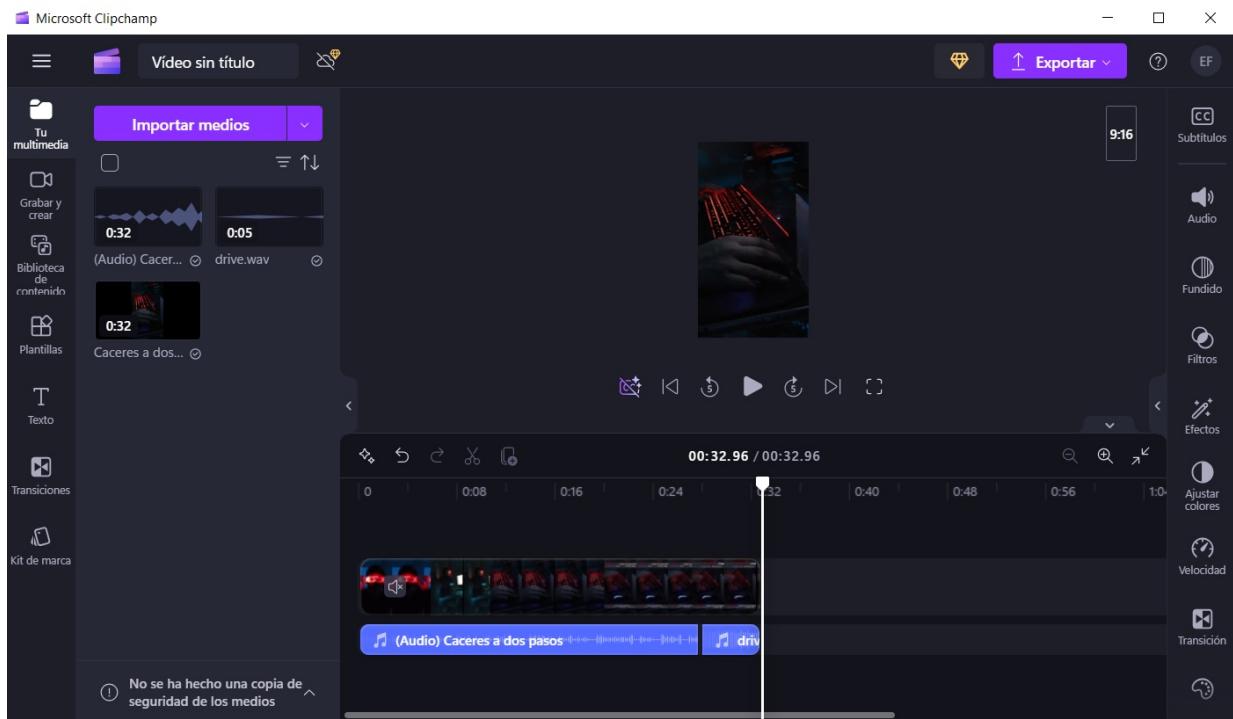


Figura 9 : Imagen donde hemos añadido el audio drive.wav al video.

Por ultimo en la *Figura 10* observamos como podemos exportar el video con el audio modificado y así obtener el video con la información oculta en el audio.

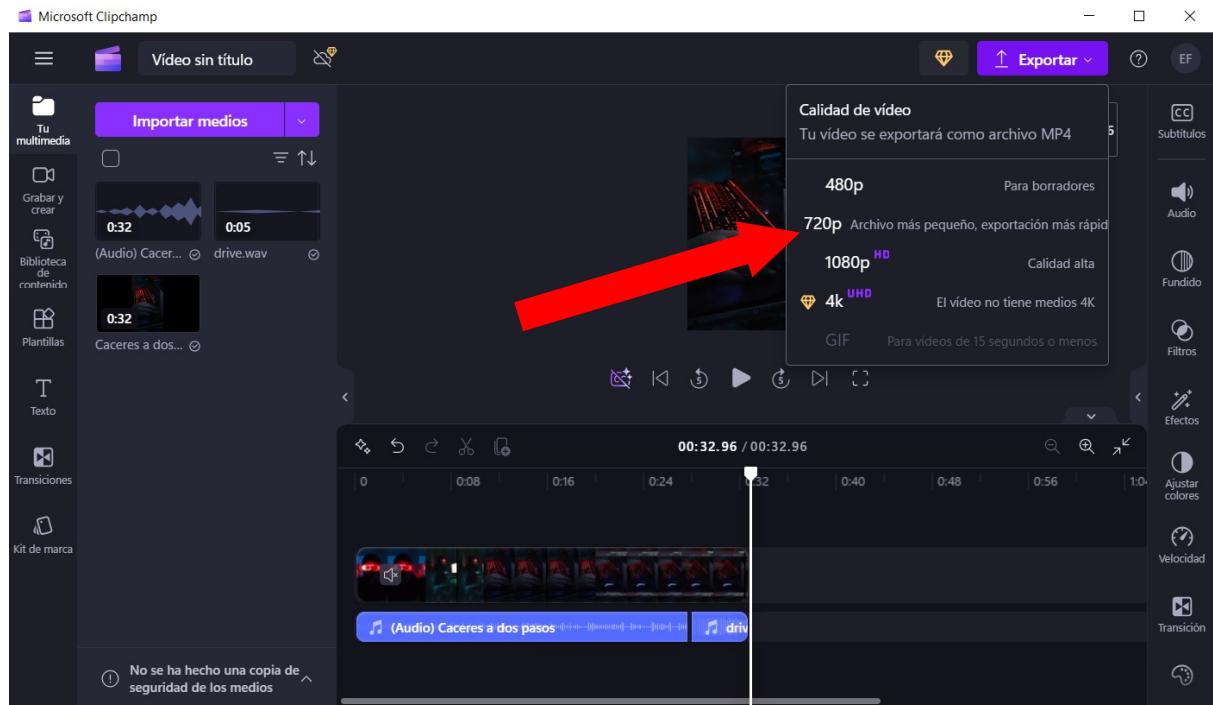


Figura 10 : Imagen donde observamos como podemos exportar el video ya modificado.

Para terminar con la fase 1 también he añadido información encriptada en rot13 para dar pistas sobre como continuar. El texto que he cifrado en rot13 y después guardado en la imagen **No hay nada oculto aquí.bmp** es el siguiente:

Al final si que había algo oculto. Como premio de resolver este primer paso tan difícil, te diré que la contraseña para abrir el tesoro consta de dos palabras, las cuales tendrás que obtener siguiendo los pasos. ¡Suerte!

Que fijándonos en la *Figura 11* podemos observar como ha sido el proceso de cifrado con la pagina web rot13.com

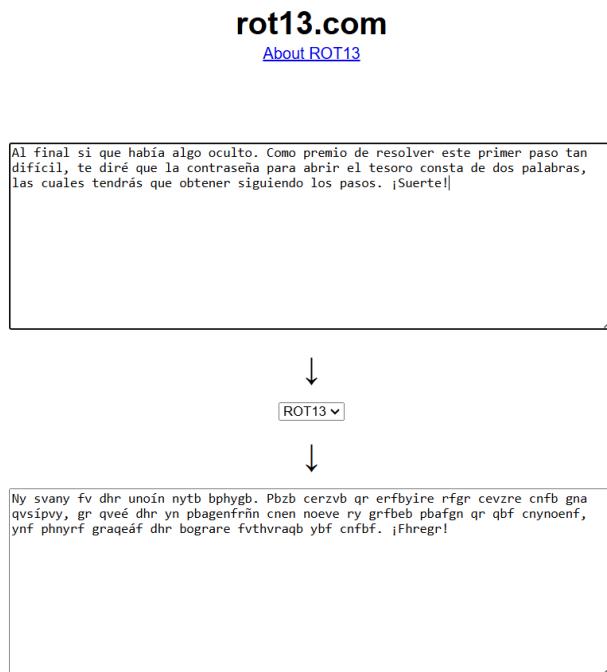


Figura 11 : Se muestra la pagina web usado para el cifrado de la pista.

Para poder guardar el texto encriptado en la imagen he usado la herramienta *QuickStego* la cual te permite abrir una imagen para ver si tiene o no información de texto guardada en ella y también para poder esconder texto en la imagen elegida.

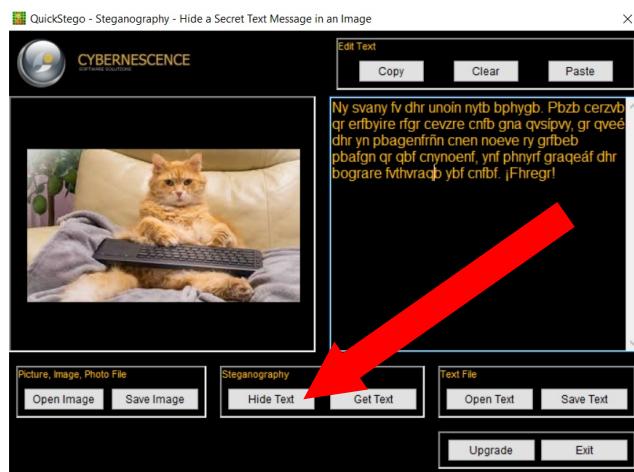


Figura 12 : Se muestra la herramienta QuickEstego y como se oculta el texto en la imagen.

2.3 Fase 2 del reto: Ingeniería inversa

Para la creación del fichero denominado “Programita” cuyo tamaño es de 3 kb en formato .jar se escribe un pequeño programa en Java que se compila siguiendo los siguientes pasos:

1- Compilar clase

javac Aqui tampoco hay nada.java



2- Generar JAR

Jar cfm IngenierialInversa.jar Manifest.txt IngenierialInversa.class

3- Ejecutar JAR

java -jar IngenierialInversa.jar

Este proceso lo he realizado en la herramienta de windows *Windows PowerShell* como se muestra en el *Figura 13*

```
PS C:\Users\Ernesto\Desktop\UNI 24-25\Primer cuatri\ALI\Practica2\MaterialesConstruccion\CreacionProgramita> ls

Directorio: C:\Users\Ernesto\Desktop\UNI 24-25\Primer cuatri\ALI\Practica2\MaterialesConstruccion\CreacionProgramita

Mode          LastWriteTime      Length Name
----          -----        -----
-a---  23/10/2024  10:31       2986 Aqui tampoco hay nada.java
-a---  23/10/2024  10:21        31 manifest.txt

PS C:\Users\Ernesto\Desktop\UNI 24-25\Primer cuatri\ALI\Practica2\MaterialesConstruccion\CreacionProgramita> javac "Aqui tampoco hay nada.java"
PS C:\Users\Ernesto\Desktop\UNI 24-25\Primer cuatri\ALI\Practica2\MaterialesConstruccion\CreacionProgramita> ls

Directorio: C:\Users\Ernesto\Desktop\UNI 24-25\Primer cuatri\ALI\Practica2\MaterialesConstruccion\CreacionProgramita

Mode          LastWriteTime      Length Name
----          -----        -----
-a---  23/10/2024  10:31       2986 Aqui tampoco hay nada.java
-a---  10/11/2024  19:11       3279 IngenieriaInversa.class
-a---  23/10/2024  10:21        31 manifest.txt

PS C:\Users\Ernesto\Desktop\UNI 24-25\Primer cuatri\ALI\Practica2\MaterialesConstruccion\CreacionProgramita> Jar cfm IngenieriaInversa.jar Manifest.txt IngenieriaInversa.class
PS C:\Users\Ernesto\Desktop\UNI 24-25\Primer cuatri\ALI\Practica2\MaterialesConstruccion\CreacionProgramita> ls

Directorio: C:\Users\Ernesto\Desktop\UNI 24-25\Primer cuatri\ALI\Practica2\MaterialesConstruccion\CreacionProgramita

Mode          LastWriteTime      Length Name
----          -----        -----
-a---  23/10/2024  10:31       2986 Aqui tampoco hay nada.java
-a---  10/11/2024  19:11       3279 IngenieriaInversa.class
-a---  10/11/2024  19:11       2424 IngenieriaInversa.jar
-a---  23/10/2024  10:21        31 manifest.txt

PS C:\Users\Ernesto\Desktop\UNI 24-25\Primer cuatri\ALI\Practica2\MaterialesConstruccion\CreacionProgramita>
```

Figura 13 : Muestra el proceso de compilación y creación de “Programita.jar”.

En la Figura 14 y la Figura 15 podemos ver el código en java usado en **Aqui tampoco hay nada.java**

```
import java.awt.datatransfer.Clipboard;
import java.awt.datatransfer.ClipboardOwner;
import java.awt.datatransfer.Transferable;
import java.awt.datatransfer.StringSelection;
import java.awt.event.ActionEvent;
import java.awt.Component;
import javax.swing.JPanel;
import java.awt.Dimension;
import java.awt.Toolkit;
import javax.swing.JLabel;
import javax.swing.JTextField;
import javax.swing.JButton;
import javax.swing.JFrame;
import java.awt.event.ActionListener;
class IngenieriaInversa implements ActionListener
{
    JFrame frame;
    JButton send;
    JTextField tf;
    JLabel result;

    IngenieriaInversa() {
        this.frame = new JFrame();
        this.send = new JButton("Enviar");
        this.tf = new JTextField(10);
        this.result = new JLabel("", 0);
        this.prepareGUI();
        this.buttonProperties();
    }

    public void prepareGUI() {
        this.frame.setTitle("ALI 2021-22");
        this.frame.setVisible(true);
        final Dimension dimension = Toolkit.getDefaultToolkit().getScreenSize();
        final int x = (int)((dimension.getWidth() - this.frame.getWidth()) / 2.0);
        final int y = (int)((dimension.getHeight() - this.frame.getHeight()) / 2.0);
        this.frame.setBounds(x - 150, y - 75, 300, 150);
        this.frame.setDefaultCloseOperation(3);
    }

    public void buttonProperties() {
        final JPanel panel = new JPanel();
        this.send.setActionCommand("send");
        this.send.addActionListener(this);
        final JLabel label = new JLabel("Clave");
        panel.add(label);
        panel.add(this.tf);
        panel.add(this.send);
        this.frame.getContentPane().add("North", panel);
        this.frame.getContentPane().add("Center", this.result);
        this.frame.setVisible(true);
    }
}
```

Figura 14 : Se muestra la primera parte del código de **Aqui tampoco hay nada.java** .

```

@Override
public void actionPerformed(final ActionEvent e) {
if (e.getActionCommand().equals("send")) {
if (this.tf.getText().equals("BANANA")) {
final JButton copy = new JButton("Copiar en el portapapeles");
copy.setActionCommand("copy");
copy.addActionListener(this);
this.frame.getContentPane().add("South", copy);

this.result.setText("TXV5IGJpZW4sIG1lIGhhcyBzb3JwcmVuZGlkbywgbmFkaWUgaGFiw61hIGNvbnNlZ3VpZG8gbGxI2FyIGEgZXN0ZSE
")
else {
this.result.setText("Vuelve a intentarlo!!");
}
}

else if (e.getActionCommand().equals("copy")) {
final StringSelection stringSelection = new StringSelection(this.result.getText());
final Clipboard clipboard = Toolkit.getDefaultToolkit().getSystemClipboard();
clipboard.setContents(stringSelection, null);
this.result.setText("Copiado correctamente");
}
}

public static void main(final String[] args) {
new IngenieriaInversa();
}
}

```

*Figura 15 : Se muestra la segunda parte del código de **Aqui tampoco hay nada.java** .*

En la *Figura 15* podemos que se establece una contraseña a **Programita.jar** la cual es “BANANA” y ademas se pone que cuando se ponga la contraseña correcta muestre el siguiente texto cifrado:

TXV5IGJpZW4sIG1lIGhhcyBzb3JwcmVuZGlkbywgbmFkaWUgaGFiw61hIGNvbnNlZ3VpZG8gbGxI2FyIGEgZXN0ZSBwYXN
vIGFudGVyaW9ybWVudGUsIGNvbW8gcHJlbWlvIHRIIGRhcsOplGxhIHByaW1lcmEgcGFsYWJyYSBkZSBsYSBjb21iaW5hY2
nDs24gZmluYWwulExhIHByaW1lcmEgbGV0cmEgZW1waWV6YSBwb3lglnEilHkgdGVybWluYSBwb3lglnVpZXJvli4gcGFyY
SBjb250aW51YXlgdGVuZHLDoXMgcXVIHNhY2FyIGVsIHNpZ3VpZW50ZSBhcmNoaXzvIHkgcG9uZXlgbGEgcHJpbWVvYSB
sZXRyYSBkZSBsYSBjb250cmFzZcOxYSBmaW5hbCA6KQ==

El cual esta codificado en base 64 con la pagina web: <https://www.base64encode.org/es/>

The screenshot shows a web form titled "Codifique en formato Base64". It contains a text area with the message: "Muy bien, me has sorprendido, nadie había conseguido llegar a este paso anteriormente, como premio te daré la primera palabra de la combinación final. La primera letra empieza por "q" y termina por "uiero". para continuar tendrás que sacar el siguiente archivo y poner la primera letra de la contraseña final :)"

Below the text area, there are several configuration options:

- Para codificar binarios (como imágenes, documentos, etc.) utilice el formulario de carga de archivos que encontrará un poco más abajo en esta página.
- UTF-8 (selected) Conjunto de caracteres de destino.
- LF (Unix) Separador de nueva línea de destino.
- Codifique cada linea por separado (útil cuando tiene varias entradas).
- Divida las líneas en trozos de 76 caracteres de largo (útil para MIME).
- Realice una codificación URL segura (utiliza el formato Base64URL).
- Modo en directo DESACTIVADO Codifica en tiempo real mientras escribe o pega (sólo admite el juego de caracteres UTF-8).

A button labeled "CODIFICAR" with a right-pointing arrow is present, followed by the instruction "Codifica sus datos en la zona de abajo."

The bottom of the form shows the encoded output: TXV5IGJpZW4sIG1lGhhecyBzb3JwcmVuZGlkbywgbmFkaWUgaGFiw61hGNvbnNlZ3VpZG8gbGxtZ2FyIGEgZXN0ZSBwYXNvIGFudGVyaW9ybWVudGUslGNvbW8gcHJlbWvIhRlIGRhcsOpIGxHlHByaW1cmEgGFsYWJyYSBkZSBsYSBjb21aW5hY2nDs24gZmluYWwulExhIHByaW1cmEgbGV0cmEgZ2W1waW6YSBwb3iglneIiHkgdGVybWluYSBwb3iglVpZXJvl4gcGFYYSbjb250aW51YXigdGVuZHLDoXmgXVIIHNhY2FyIGVsIhNpZ3VpZW50ZSBhcmNoaXzvIhgCg9uZxIgbGEgCHJpbWVvYSBsZXRsYYSBkZSBsYSBjb250cmFzZcOxYSBmaWShbCA6KQ==

Figura 16 : Muestra el proceso de cifrado en base64.

El texto sin codificar indica la contraseña para poder acceder al comprimido de la fase 3 ("q") y ademas indica la primera palabra de la contraseña final, siendo una gran recompensa. El texto es el siguiente:

Muy bien, me has sorprendido, nadie había conseguido llegar a este paso anteriormente, como premio te daré la primera palabra de la combinación final. La primera letra empieza por "q" y termina por "uiero". para continuar tendrás que sacar el siguiente archivo y poner la primera letra de la contraseña final :)

En la Figura 17 y la Figura 18 podemos ver la ejecución de Programita.jar



Figura 17 : Muestra el Programita.jar cuando se ejecuta.

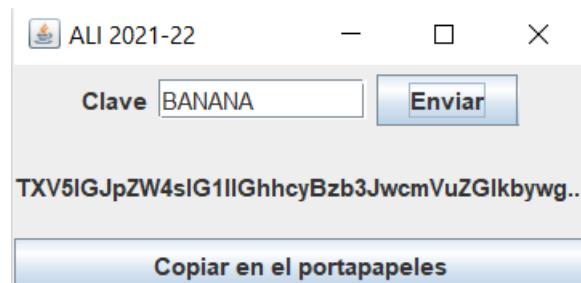


Figura 18 : Muestra el resultado que da Programita.jar cuando pones la contraseña.

Para poder obtener la contraseña del reto hay un archivo “pdf” llamado **Fruta** el cual esta sin extensión y es el propio usuario quien tendrá que obtenerla, añadiéndole un poco mas de dificultad. Dentro de este archivo hay un acertijo sencillo con indicaciones sobre como poner y obtener la contraseña de **Programita.jar**.

BANANA



¡Excelente, pequeño minion! Has llegado hasta aquí, y eso es todo un logro. Espero que no hayas encontrado demasiadas complicaciones en el camino, pero si estás aquí, significa que vas en la dirección correcta.

Como puedes ver, aún necesitas una contraseña secreta para avanzar. Recuerda, es crucial completar cada paso al 100% para evitar cualquier posible enredo. ¡Tu atención a los detalles marcará la diferencia!

Ahora, aquí va la siguiente pista: para desbloquear la siguiente fase del desafío, debes escribir en MAYÚSCULAS el nombre de la fruta que más aman los minions, esa fruta deliciosa que siempre los vuelve locos.

¡Buena suerte y no te rindas, pequeño minion!

Figura 19 : Muestra el resultado que da Programita.jar cuando pones la contraseña.

Por ultimo, para pasar a la siguiente fase se ha guardado el comprimido de la fase 3 en la nube, y su enlace para continuar esta en el archivo **No tengo nada**, el cual es una imagen sin extensión, por lo que el usuario tendrá que adquirir la extensión de esta y encontrar el enlace en su interior con alguna herramienta como *QuickStego*.

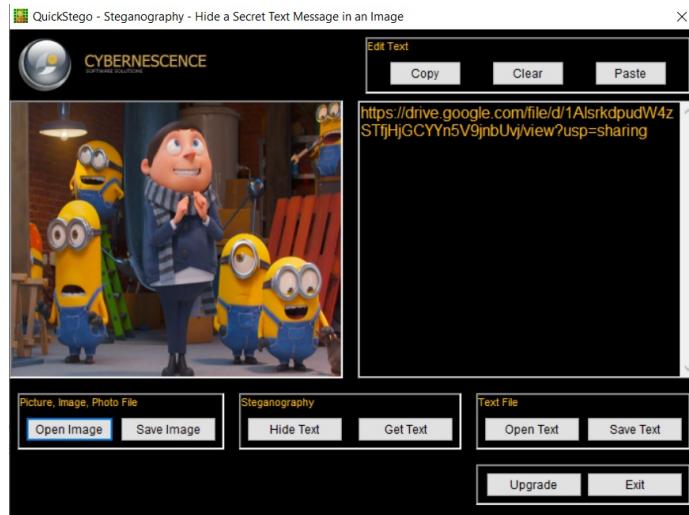


Figura 20 : Podemos observar como el enlace a la fase 3 esta oculto en el archivo **No tengo nada** con formato .bmp.

2.4 Fase 3 del reto: Creación y troceado del QR

En esta fase he creado un código QR con el enlace al archivo **PREMIO.zip** gracias a la pagina web <https://www.codigos-qr.com/generador-de-codigos-qr/> la cual simplemente poniendo el enlace puedes crear el código QR

The screenshot shows the "Códigos QR" website. The top navigation bar includes links for GENERADOR QR, LECTORES QR, OTROS GENERADORES, SOPORTE, HERRAMIENTAS, BLOG, and ESPAÑOL. The main section is titled "Generador de Códigos QR". It features a toolbar with icons for URL, WhatsApp, SMS, Teléfono, Email, Texto, VCard, Geolocalización, Evento, and WiFi. Below this is a field labeled "Código QR para una dirección Web" containing the URL "https://drive.google.com/file/d/1nzZQRgbfTsjPxn1dNKDPMCrliwWJTC0_/view?usp=sharing". There are dropdown menus for "Tamaño" (set to "Pequeño") and "Redundancia" (set to "Media"). A red button at the bottom left says "GENERAR CÓDIGO QR".

Figura 21 : Se puede observar como es la generación del código QR

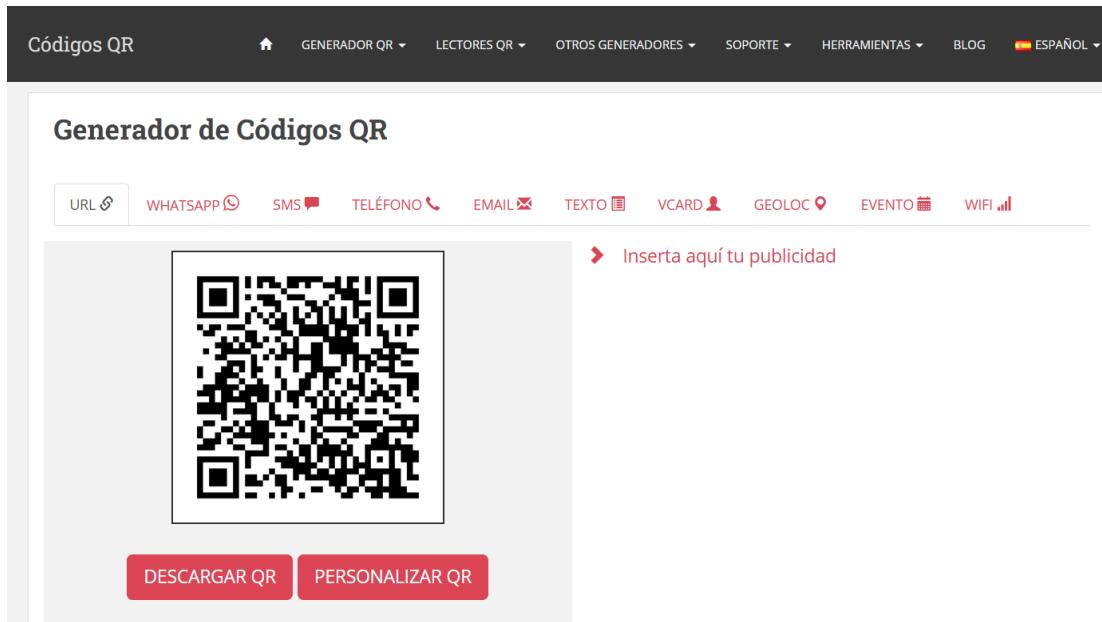


Figura 22 : Se puede observar el resultado de la generación del código QR

Por ultimo en esta fase esta el archivo **Se termina**, que es una archivo el cual contiene un reto con operaciones aritméticas simples y con pistas adquieres que cada resultado corresponde con la posición de una letra del alfabeto, obteniendo al final la letra “aprobar”, correspondiente la segunda palabra de la contraseña final, que junto con la primera palabra “quiero” y la pista de como tienes que poner la palabra que viene en ese mismo archivo, obtienes que la contraseña para poder conseguir el PREMIO.bmp es “quieroAprobar”.

;Felicitaciones! Has logrado superar el reto, pero aún te queda un último desafío. Solo necesitas descubrir la última contraseña. Para ello, tendrás que resolver un pequeño enigma final. ¡Mucho ánimo y buena suerte!

$$\begin{aligned}
 &(5 \times 2) - 9 = \\
 &(3 \times 3) + (4 \div 2) = \\
 &(6 \times 4) - 6 = \\
 &(7 \times 3) - 6 = \\
 &(5 \div 5) + 1 = \\
 &(9 - 7) - 1 = \\
 &(8 \times 3) - 6 =
 \end{aligned}$$

Para poder convertir esta secuencia de números que has obtenido en la palabra de la contraseña, tendrás que averiguarlo con la siguiente pista. Por ultimo, una vez tengas la segunda palabra de la contraseña final, tendrás que ponerla a continuación y con la primera letra en mayúsculas, por ejemplo: quieroMinions, quieroGatos, quieroComida... Mucha suerte con la pista :)

A	B	C	D	E	F	G	H	I
J	K	L	M	N	Ñ	O	P	Q
R	S	T	U	V	W	X	Y	Z
<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>	<i>f</i>	<i>g</i>	<i>h</i>	<i>i</i>
<i>j</i>	<i>k</i>	<i>l</i>	<i>m</i>	<i>n</i>	<i>ñ</i>	<i>o</i>	<i>p</i>	<i>q</i>
<i>r</i>	<i>s</i>	<i>t</i>	<i>u</i>	<i>v</i>	<i>w</i>	<i>x</i>	<i>y</i>	<i>z</i>

Figura 23 : Contenido del archivo **Se termina.pdf** con el reto y la pista para poner la contraseña final

3.Pasos para la resolución de mi reto

3.1 Materiales

En la Figura 24 se pueden observar los materiales al iniciales para el comienzo del reto:

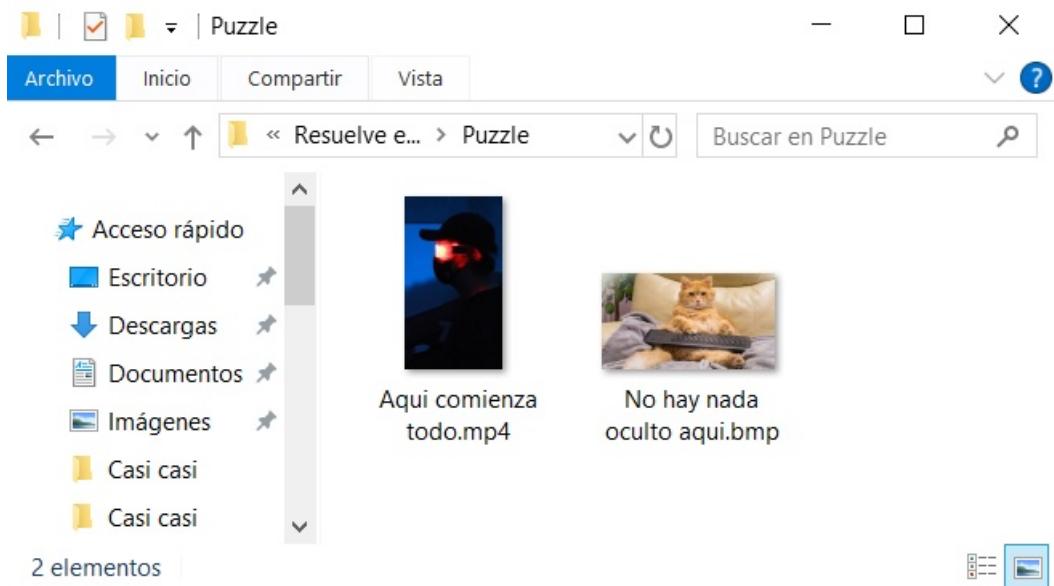


Figura 24 : Se observa el fichero **Aqui comienza todo.mp4** y el archivo **No hay nada oculto aquí.bmp**

Descripción de los ficheros:

- Un archivo denominado "**Aqui comienza todo.mp4**" cuyo tamaño es de 36,1 MB y su extensión es .mp4
- Una imagen denominada "**No hay nada oculto aquí.bmp**" cuyo tamaño es de 147 KB y su extensión es .bmp

3.2 Fase 1: Análisis de la imagen y del video

El primer paso es analizar la imagen **No hay nada oculto aquí.bmp** con la herramienta QuickEstego, para comprobar si hay información oculta en ella.



Figura 25 : Se observa el contenido oculto de la imagen

Podemos ver entonces que la imagen el siguiente texto cifrado:

Ny svany fv dhr unoín nytb bphygb. Pbzb cerzvb qr erfbyire rfgr cevzre cnfb gna qvsípyv, gr qveé dhr yn pbagenfrñn cnen noeve ry grfbef pbafgn qr qbf cnynoenf, ynf phnyrf graqeáf dhr bograre fvthvraqb ybf cnfbf. ¡Fhregr!

Usaremos una pagina web para identificar el tipo de cifrado del texto. Para ello usamos "dcode.fr"

<https://www.dcode.fr/identificador-cifrado>. Con esta web, podemos introducir el texto y después de darle al botón de analizar nos mostrara en resultados el cifrado que es, como se muestra en la Figura 26

Figura 26 : Se el proceso de identificar el cifrado

Una vez que obtenemos el cifrado usamos la pagina web “rot13” <https://rot13.com/> para obtener su contenido.

Figura 27 : Observamos el descifrado del texto.

Podemos el texto ya descifrado, el cual nos da una pista de que la contraseña que necesitaremos al final se compone de dos palabras.

Al final si que había algo oculto. Como premio de resolver este primer paso tan difícil, te diré que la contraseña para abrir el tesoro consta de dos palabras, las cuales tendrás que obtener siguiendo los pasos. ¡Suerte!

Ahora pasamos ha analizar el video **Aqui comienza todo.mp4**, el cual, una vez que lo escuchamos notamos un ruido raro en el audio, por lo que procederemos ha separar el audio del video y después analizar ese audio para ver si se ha introducido alguna información por esteganografía.

Para separar el audio del video usaremos una pagina web llamada “[moravi.com](https://www.movavi.com/es/support/how-to/how-to-extract-audio-from-video.html)”

<https://www.movavi.com/es/support/how-to/how-to-extract-audio-from-video.html>

The screenshot shows the Movavi video converter interface. At the top, there is a navigation bar with the Movavi logo, a search bar, and language selection (ES). Below the navigation bar, there are links for VÍDEO, TODOS LOS PRODUCTOS, TIENDA, AYUDA, and TUTORIALES. A blue banner at the top right says "NUEVA VERSIÓN". The main area is titled "Archivos añadidos" and shows a single file: "Aqui comienza todo.mp4". To the right of the file name, it shows "37 MB" and "MP3" with a dropdown arrow. There is also a gear icon for settings. At the bottom of the list is a large blue button labeled "Convertir". Above the file list, there is a link to "Volver a la página principal".

Figura 28 : Se muestra el proceso de pasar de .mp4 a .mp3

Una vez tengamos el audio, lo analizaremos con la herramienta *Audacity*, la cual nos permitirá ver su espectrograma y así poder ver si hay información oculta.

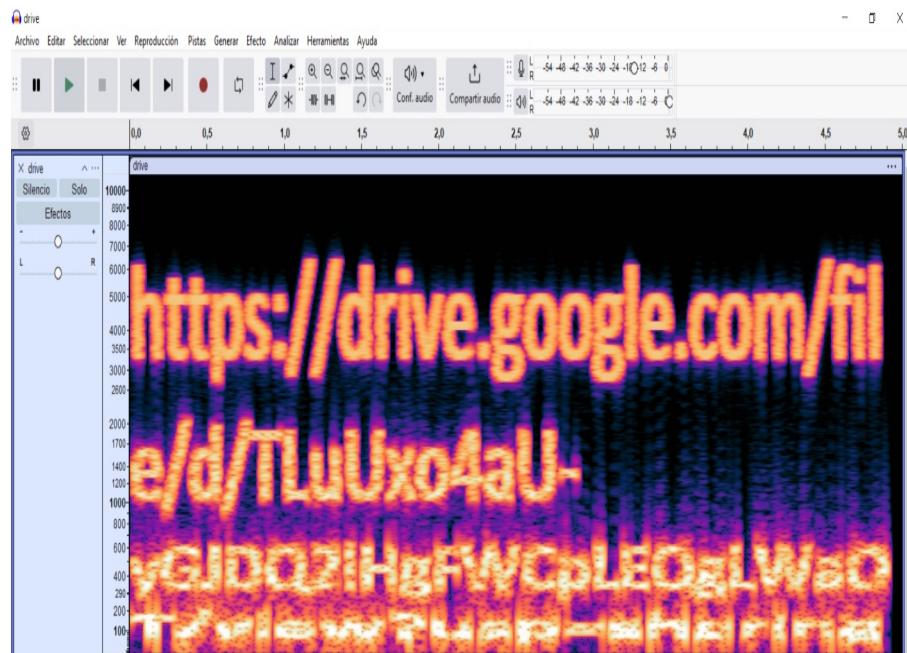


Figura 29 : podemos ver el espectrograma del audio de **Aqui comienza todo.mp4**.

Gracias al espectrograma podemos distinguir el siguiente enlace:

[“<https://drive.google.com/file/d/1LuUxo4aU-yGJDQ2IHgFWCpLEQgLWaOT/view?usp=sharing>”](https://drive.google.com/file/d/1LuUxo4aU-yGJDQ2IHgFWCpLEQgLWaOT/view?usp=sharing)

Donde podremos descargar el archivo **Casi casi.zip** con tamaño de 6 MB como observamos en la Figura 30

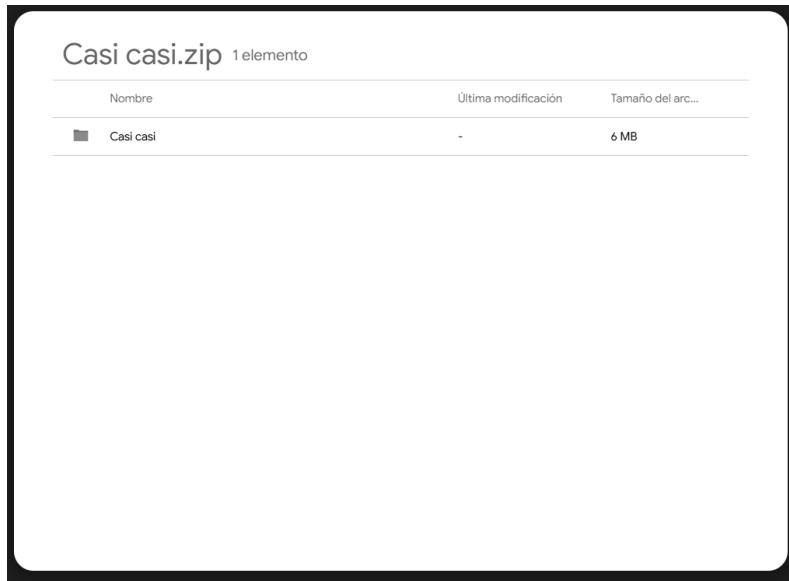


Figura 30 : Vemos el contenido del enlace.

3.3 Fase 2: Análisis de archivos sin extensión y de programa java

Dentro del archivo **Casi casi.zip** podemos sacar tres archivos, dos sin extension y uno llamado **Programita.jar** con extensión .jar, como podemos ver en la *Figura 31*:

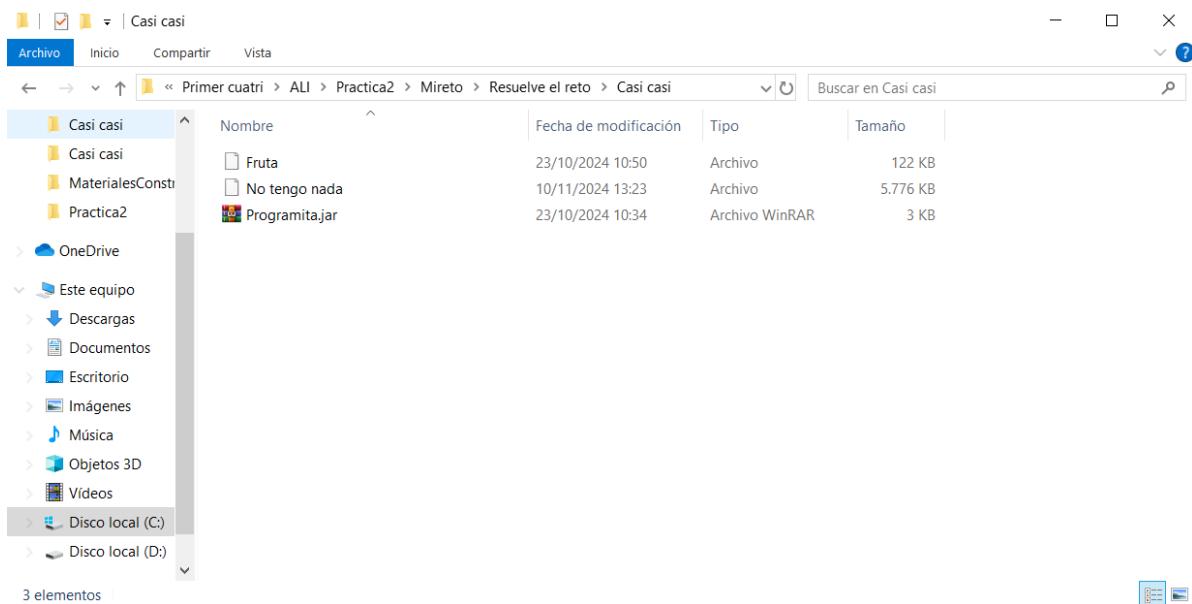


Figura 31 : Podemos observar el contenido de la carpeta Casi casi

El primer paso sera obtener las extensiones de los archivos para poder analizarlos, para ello usaremos la pagina web <https://mark0.net/onlinetrid.html> donde podremos subir los archivos y este nos indicara la extensión, como podemos observar en la *Figura 32* y la *Figura 33*.

The screenshot shows the homepage of Marco Pontello's website. On the left, there is a sidebar with various links: Home, Old News, Contacts Info (which is highlighted in blue), Privacy, Software, Awards, TrID (which is also highlighted in blue), PBTracer, Extra Redcode Kit, Screenshots, SendMex, and PEDu. The main content area has a dark background with a banner for 'TrID File Identifier'. Below the banner, it says '(Powered by TrIDEEngine/Py v1.0, 18403 definitions)'. There is a section titled 'Online TrID File Identifier' with the heading 'Identification results:' and a note 'File size: 121KB'. A table shows the analysis results:

Match	Ext	File type	MIME type	Related URL	Def's author
100.00%	PDF	Adobe Portable Document Format application/pdf	http://en.wikipedia.org/wiki/Pdf	Marco Pontello	

Figura 32 : Vemos el resultado de analizar el archivo Fruta

Marco Pontello's Home Page

(Last updated: 07/11/24)

Software

- Awards
- TrID**
- TrIDNet
- Online TrID
- TrIDBot
- TrIDScan
- File extension defs
- PBTracer
- Extra Redcode Kit**
- Screenshots
- SendMex
- PEDu
- BDLScan**
- MiniDumper
- Online Hex Dump
- RTFFStrip
- MPCBitsGUI
- Twin
- LeakOut
- PFCEEx
- BitmapRip
- BubbleRand
- mpcABX

Online TrID File Identifier

Identification results:

File size: 5775KB

Match	Ext	File type	MIME type	Related URL	Def's author
50.00%	BMP RLE	DIB	Windows Bitmap (generic)	image/bmp https://en.wikipedia.org/wiki/BMP_file_format	Joerg Jenderek
50.00%	BMP	Windows Bitmap (v3)	image/bmp	https://en.wikipedia.org/wiki/BMP_file_format	Joerg Jenderek
This variant with 40 byte DIB header (Windows 3.x)					

Figura 33 : Vemos el resultado de analizar el archivo **No tengo nada**

En conclusión obtenemos que el archivo **Fruta** tiene formato .pdf y el archivo **No tengo nada** tiene formato .bmp y ademas poder intuir que esta imagen tiene información oculta, ya que indica que el 50% es un Bitmap.

Procedemos ha analizar la imagen con *QuickEstego* como en la Fase 1 y abriremos el archivo .pdf, dándonos los siguientes resultados que vemos en la Figura 34 y la Figura 35



¡Excelente, pequeño minion! Has llegado hasta aquí, y eso es todo un logro. Espero que no hayas encontrado demasiadas complicaciones en el camino, pero si estás aquí, significa que vas en la dirección correcta.

Como puedes ver, aún necesitas una contraseña secreta para avanzar. Recuerda, es crucial completar cada paso al 100% para evitar cualquier posible enredo. ¡Tu atención a los detalles marcará la diferencia!

Ahora, aquí va la siguiente pista: para desbloquear la siguiente fase del desafío, debes escribir en MAYÚSCULAS el nombre de la fruta que más aman los minions, esa fruta deliciosa que siempre los vuelve locos.

¡Buena suerte y no te rindas, pequeño minion!

Figura 34 : Vemos el contenido de **Fruta.pdf**

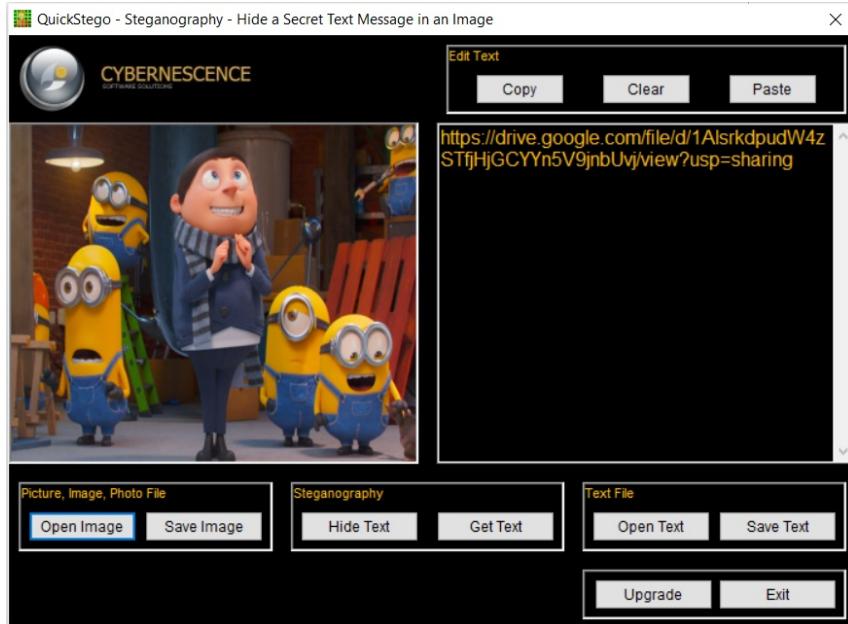


Figura 34 : Vemos el contenido oculto de **No tengo nada.bmp**

Como hemos podido ver, el archivo .pdf contiene un reto para obtener la contraseña que nos pedirá el **Programita.jar** y la imagen .bmp tiene oculto un enlace a un archivo para continuar a la fase 3, pero como en **Fruta.pdf** nos indica que completaremos el 100% antes de continuar procederemos a ejecutar el Programita.jar e introducir la contraseña “BANANA”, ya que esta es la fruta preferida de los minions y ademas nos indica que tiene que estar escrita todo con mayúsculas, tras introducir la contraseña nos da el siguiente resultado, el cual, podemos observar en la Figura 35.

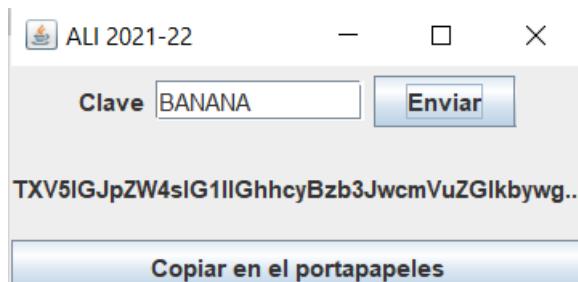


Figura 35 : Ejecución y resolución de **Programita.jar**

Nos da el siguiente texto cifrado, que con la pagina web “dcode.fr” <https://www.dcode.fr/identificador-cifrado> que hemos usado antes, obtenemos que esta cifrado en base64 el siguiente texto:

```
TXV5IGJpZW4sIG1lIGhhcyBzb3JwcmVuZGlkbywg...  
bmFkaWUgaGFiw61hIGNvbnNlZ3VpZG8gbGxI2FyIGEgZXN0ZSBwYXN  
vIGFudGVyaW9ybWVudGUslGNvbW8gcHJlbWlvIHRIIGRhcsOpIGxhIHByaW1lc  
mEgcGFsYWJyYSBkZSBsYSBjb21iaW5hY2  
nDs24gZmluYWwuExhIHByaW1lcEgbGV0cmEgZW1waWV6YSBwb3lglnEilHkgdGVybWluYSBwb3lglnVpZXJvI4gcGFyY  
SBjb250aW51YXlgdGVuZHLDoXMgcXVIHNhY2FyIGVsIHNPZ3VpZW50ZSBhcmNoaXzvIHkgcG9uZXlgbGEgcHJpbWVYYSB  
sZXRyYSBkZSBsYSBjb250cmFzZcOxYSBmaW5hbCA6KQ==
```

Para poder descifrarlo usaremos la pagina web <https://www.base64decode.org/> donde podremos sacar el siguiente texto descifrado:

Muy bien, me has sorprendido, nadie había conseguido llegar a este paso anteriormente, como premio te daré la primera palabra de la combinación final. La primera letra empieza por "q" y termina por "uiero". para continuar tendrás que sacar el siguiente archivo y poner la primera letra de la contraseña final :)

Decode from Base64 format

Simply enter your data then push the decode button.

```
TXV5IGJpZW4slG1lGhhcyBzb3JwcmVuZGlkbwgbmFkaWUgaGFiw6hlGNvbnNlZ3VpZG8gbGxI2FylGEgZXN0ZSBwYXNvlGFudGVyaW9ybWVudGUslGNvbW8gcHJlbWlviHRIlGRhcsOplGxhiHByaW1lcmeGcGFsYWJyYSBkZSBsYSBjb21iaW5hY2nDs24gZmluYWwulExhlHByaW1lcmeGbGV0cmEgZW1waWV6YSBwb3lglnEilHkgdGVybWlUYSBwb3lglnVpZXJvli4gcGFyYSBjb250aW51YXlglGVuZHLDoXMgcXVIIHNhY2FylGVsIHNPZ3VpZW50ZSBhcmNoaXzvlIkcgG9uZXlgbGEgchJpbWVvYSBsZXRxYYSBkZSBsYSBjb250cmFzCoxYSBmaW5hbCA6KQ==
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

AUTO-DETECT ▾ Source character set. Detected: UTF-8

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

Muy bien, me has sorprendido, nadie había conseguido llegar a este paso anteriormente, como premio te daré la primera palabra de la combinación final. La primera letra empieza por "q" y termina por "uiero". para continuar tendrás que sacar el siguiente archivo y poner la primera letra de la contraseña final :)

Figura 36 : Proceso de descifrar el texto devuelto por **Programita.jar**

Este texto nos da la primera palabra de la contraseña final y ademas nos indica que el siguiente archivo que nos proporciona el enlace que venia en la imagen **No tengo nada.bmp** necesita de una contraseña la cual sera la “q”

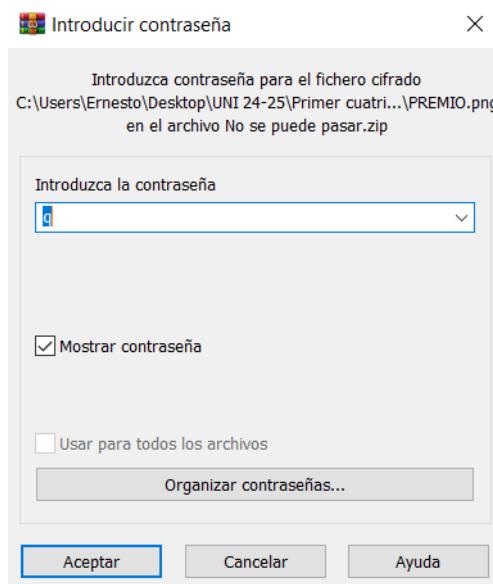


Figura 36 : Proceso de poner la contraseña “q” en **No puedes pasar.zip**

3.4 Fase 3: Código QR y obtención del PREMIO.bmp

En el archivo **No se puede pasar.zip** de tamaño 166 KB podemos encontrar un código QR con formato .png y un archivo sin extensión, como vemos en la *Figura 37*

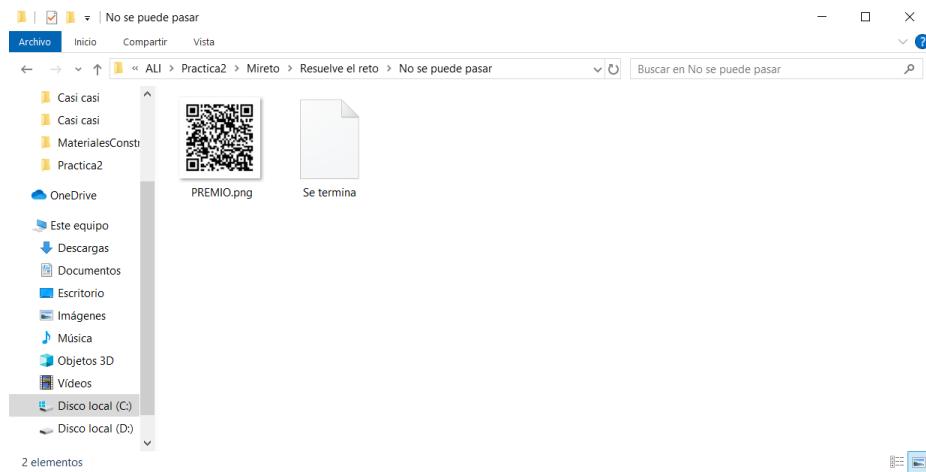


Figura 37 : Contenido del archivo No puedes pasar.zip

El primer paso es obtener la extensión del archivo Se termina con la página web que usamos anteriormente <https://mark0.net/onlinetrid.html> la cual nos da que se trata de un archivo .pdf, donde podemos ver el reto para obtener la segunda y última palabra de la contraseña final además de indicarnos como hay que escribirla.

¡Felicitaciones! Has logrado superar el reto, pero aún te queda un último desafío. Solo necesitas descubrir la última contraseña. Para ello, tendrás que resolver un pequeño enigma final. ¡Mucho ánimo y buena suerte!

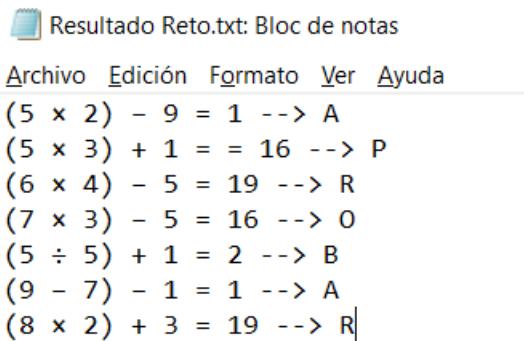
(5 × 2) – 9 =
(5 × 3) + 1 =
(6 × 4) – 5 =
(7×3) – 5 =
(5 ÷ 5) + 1 =
(9 – 7) – 1 =
(8 × 2) + 3 =

Para poder convertir esta secuencia de números que has obtenido en la palabra de la contraseña, tendrás que averiguarlo con la siguiente pista. Por último, una vez tengas la segunda palabra de la contraseña final, tendrás que ponerla a continuación y con la primera letra en mayúsculas, por ejemplo: quieroMinions, quieroGatos, quieroComida... Mucha suerte con la pista :)

A B C D E F G H I
J K L M N Ñ O P Q
R S T U V W X Y Z
*a b c d e f g h i j k l m n ñ
o p q r s t u v w x y z*

Figura 38 : Contenido del archivo Se termina.pdf

Gracias a las pistas se puede intuir que hay que resolver las operaciones aritméticas y que el numero resultante corresponde a la posición de una letra del alfabeto, dándonos como resultado la ultima palabra de la contraseña.



```
Archivo Edición Formato Ver Ayuda
(5 × 2) - 9 = 1 --> A
(5 × 3) + 1 = = 16 --> P
(6 × 4) - 5 = 19 --> R
(7 × 3) - 5 = 16 --> O
(5 ÷ 5) + 1 = 2 --> B
(9 - 7) - 1 = 1 --> A
(8 × 2) + 3 = 19 --> R
```

Figura 38 : Resultado de las operaciones aritméticas y su letra correspondiente en el alfabeto

Por lo tanto podemos ver que la segunda palabra de la contraseña final es “APROBAR” y según las indicaciones, la del reto, la contraseña final es “quieroAprobar”. Por ultimo nos falta escanear el código QR, descargar el archivo **Premio.zip** y poner la contraseña para obtener el premio y terminar el reto.

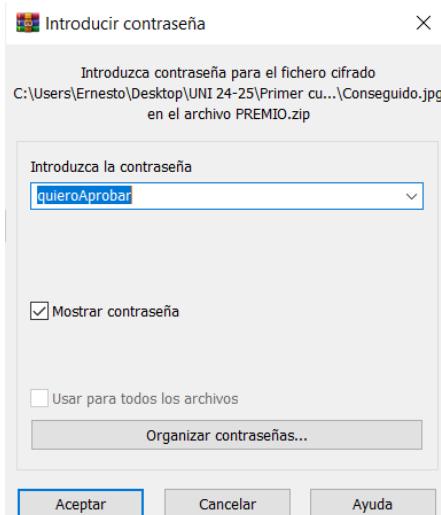


Figura 39 : Proceso de colocar la contraseña final tras escanear el codigo QR y descargar el archivo **Premio.zip**



Figura 40 : Obtención del premio final del reto, llamado **Conseguido.jpg**

4 Resolución del reto del compañero

4.1 Materiales

La compañera me ha facilitado la carpeta comprimida **Materiales.zip** cuyo tamaño es de 72,514 KB. Al descomprimir la carpeta aparecen tres ficheros, una carpeta “**x_continua**”, una archivo **flores.bmp** con tamaño 1,219 KB y un archivo **RuidoBlanco.mp4**:

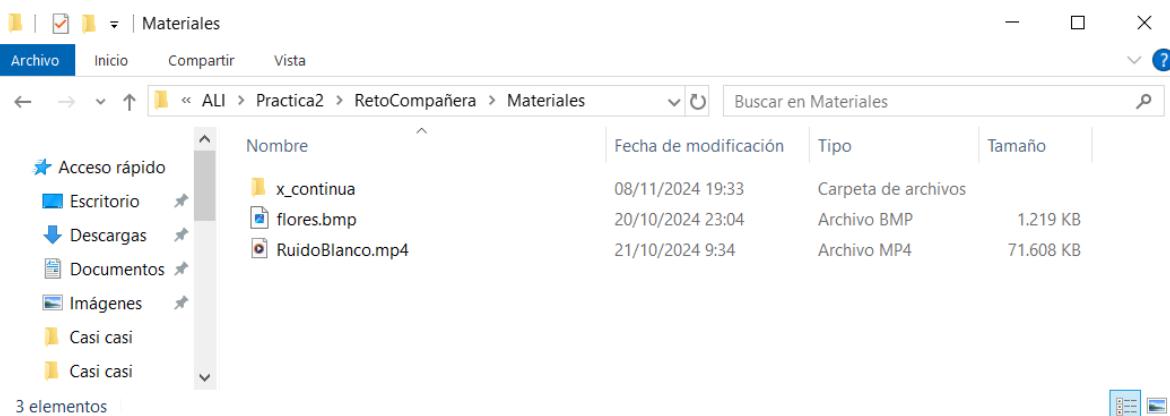


Figura 41 : Se puede observar el contenido del archivo **Materiales.zip**

Primero aplicaremos la esteganografía para ver si hay información oculta tanto en la imagen **flores.bmp** como en el sonido **RuidoBlanco.mp4**, ya que en este ultimo suenan interferencias por lo que puede ser una señal de información oculta. Para comprobar si hay información oculta en la imagen usare la herramienta *QuickStego* y para ver si en el audio hay oculta información oculta revisando con la herramienta *Audacity* su espectrograma

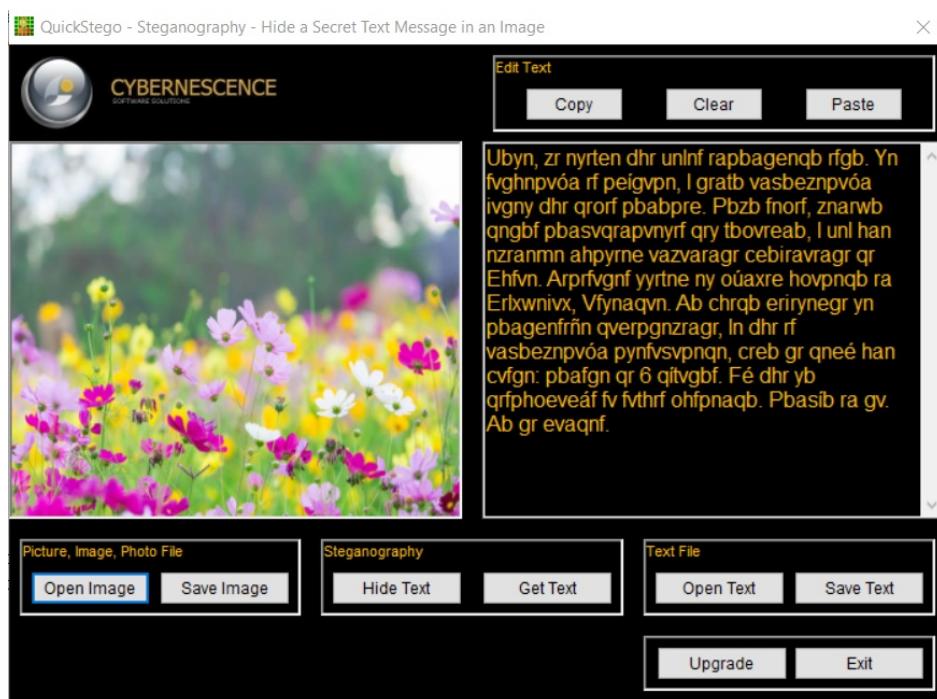


Figura 41 : Se puede observar el contenido del archivo **Materiales.zip**

Podemos observar que en la imagen había oculto un texto cifrado, el cual introduciremos en la página web <https://www.dcode.fr/identificador-cifrado> para que nos indique de qué tipo de cifrado se trata. El texto cifrado es el siguiente:

Ubyn, zr nyten dhr unlfrapbagenqb rfgb. Yn fvghnpvúa rf peígvpn, l gratb vasbeznpvúa ivgny dhr qrorf pbabpre. Pbzb fnorf, znarwb qngbf pbasvqrapvnyrf qry tbovreab, l unl han nzranmn ahpyrne vazvaragr cebiravragr qr Ehfvn. Arprfvgnf yyrtne ny ouáxre hovpnqb ra Erlxwnivx, Vfyngvn. Ab chrb eriryneqr yn pbagenfrñ qverpgnzragr, In dhr rf vasbeznpvúa pynfsvpnqn, creb gr qneé han cvfgn: pbafgn qr 6 qítvgbf. Fé dhr yb qrfphoeáfv fv fvtchrh ofhpnaqb. Pbasib ra gv. Ab gr evaqnf.

Figura 42 : Se puede observar el tipo de cifrado del texto.

Figura 43 : Se puede observar el contenido del texto descifrado

Por lo tanto hemos podido observar que el texto oculto estaba cifrado en rot13 y usando la pagina web <https://rot13.com/> hemos podido obtener su contenido, quedándonos el siguiente texto:

Hola, me alegra que hayas encontrado esto. La situación es crítica, y tengo información vital que debes conocer. Como sabes, manejo datos confidenciales del gobierno, y hay una amenaza nuclear inminente proveniente de Rusia. Necesitas llegar al búnker ubicado en Reykjavik, Islandia. No puedo revelarte la contraseña directamente, ya que es información clasificada, pero te daré una pista: consta de 6 dígitos. Sé que lo descubrirás si sigues buscando. Confío en ti. No te rindas.

El texto nos da una pista sobre la contraseña final, indicándonos que consta de 6 dígitos. Ahora analizaremos el audio de **RuidoBlanco.mp4** para ver si podemos obtener mas información oculta, para ello el primer paso sera obtener únicamente el audio, convirtiendo el archivo de formato .mp4 a formato .mp3, por tanto, usaremos la siguiente pagina web <https://convertio.co/es/mp4-mp3/>.



Figura 44 : Podemos ver el proceso para convertir de .mp4 a .mp3

Ahora procederemos como he indicado anteriormente a analizar el audio con la herramienta Audacity



Figura 45 : Proceso de análisis del archivo .mp3

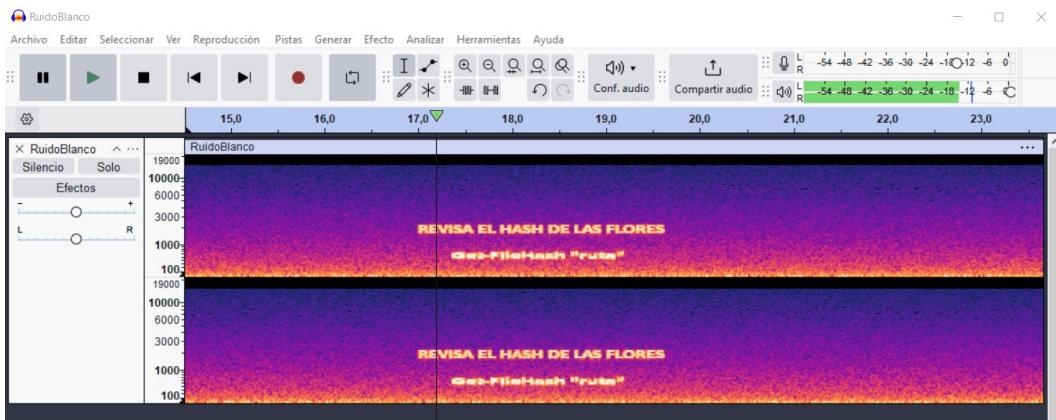


Figura 46 : Análisis del espectrograma del archivo .mp3

Como podemos observar también había información oculta en el archivo **RuidoBlanco.mp4** la cual hemos podido obtener revisando el espectrograma de su audio. Ahora voy a pasar a revisar el hash de la imagen de las flores como me indica en la información oculta. Con el comando `Get-FileHash "ruta"` como se nos indica, dándonos el resultado que nos muestra la Figura 47

PS C:\Users\Ernesto> Get-FileHash "C:\Users\Ernesto\Desktop\UNI 24-25\Primer cuatri\ALI\ResolucionCompañera\Materiales\flores.bmp"
Algorithm Hash Path

SHA256 9AE14BA0EB62FE17AA3D49D527C881D56776F9789CC9BB05AAB2715E907CE4FB C:\Users\Ernesto\Desktop\UNI ...

Como aun no se nos ha indicado que hacer con el hash

"9AE14BA0EB62FE17AA3D49D527C881D56776F9789CC9BB05AAB2715E907CE4FB" seguiremos viendo la carpeta **x_continua**. En ella podemos encontrar un archivo **sigue**, el cual no tenemos extensión y la obtendremos con la pagina web <https://mark0.net/onlinetrid.html>

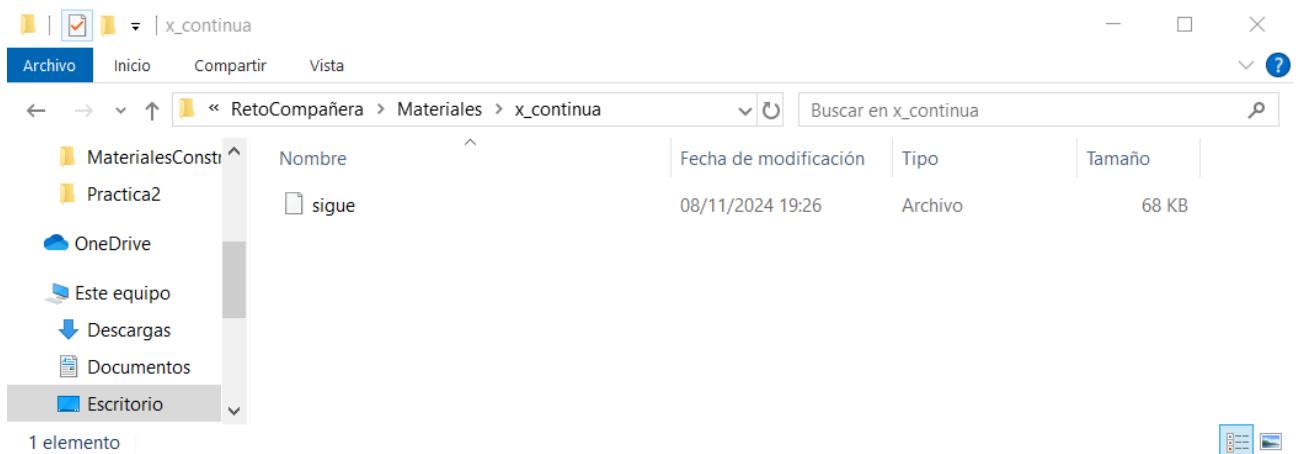


Figura 47 : Se muestra el contenido de la carpeta x_continua

Marco Pontello's Home Page

Home
Old News
Contacts Info
Privacy
Software
Awards
TrID
TrIDNet
Online TrID
TrIDBot
TrIDScan
File extension defs
PBTracer
Extra Redcode Kit
Screenshots
SendMex
PEDu
BDLLScan
MiniDumper
Online Hex Dump

(Last updated: 07/11/24)


(Powered by TrIDEEngine/Py v1.0, 18403 definitions) Share 212

Online TrID File Identifier

Identification results:

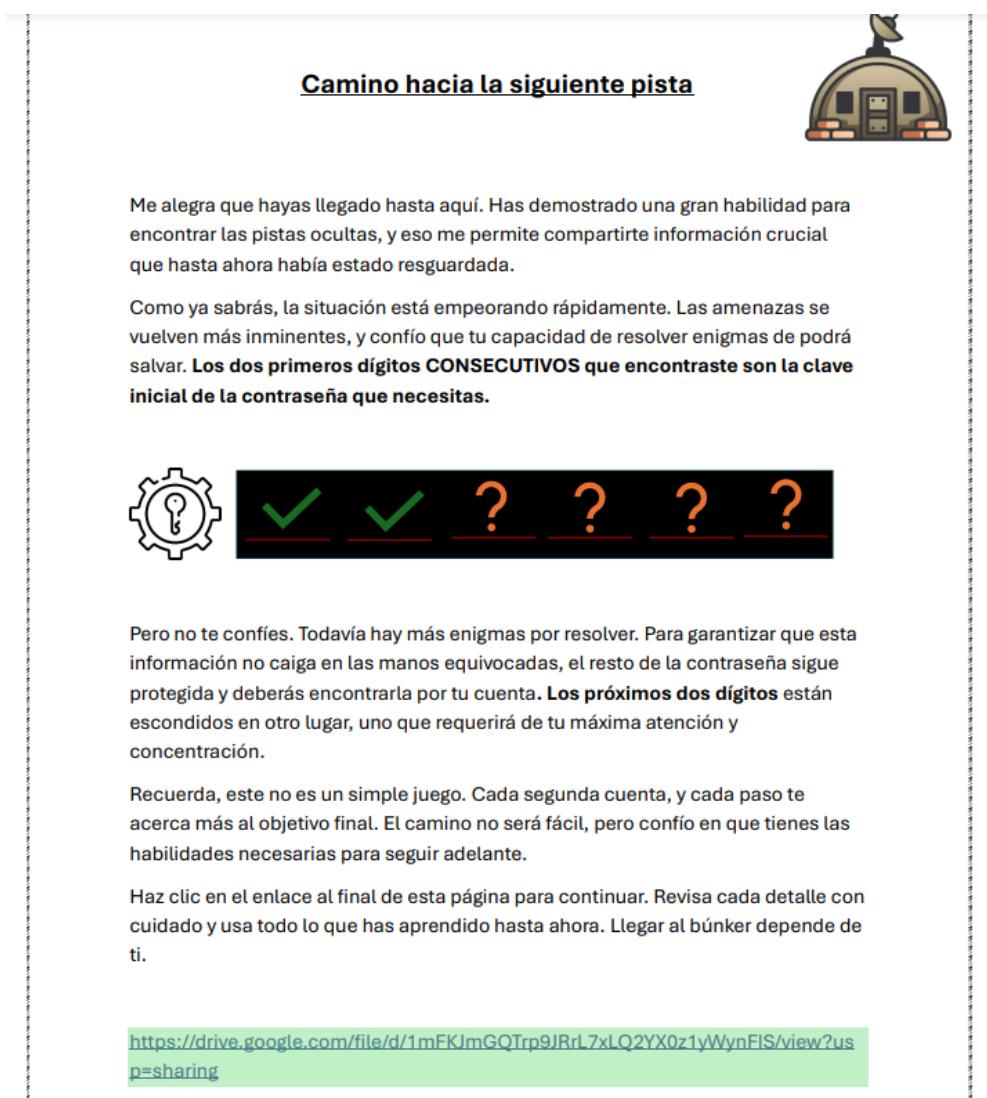
File size: 67KB

Match	Ext	File type	MIME type	Related URL	Def's author
100.00%	PDF	Adobe Portable Document Format application/pdf	http://en.wikipedia.org/wiki/Pdf	Marco Pontello	

Not satisfied with the result? It doesn't seem right? You know more about this kind of file? You can help improving TrID accuracy! Click the "Help TrID" link to send a mail with some notes about this file! Thanks!

Figura 48 : Se muestra el resultado del análisis del archivo **sigue**

Como podemos ver el archivo **sigue** es de tipo “pdf” por lo que podremos ver su contenido


Camino hacia la siguiente pista

Me alegra que hayas llegado hasta aquí. Has demostrado una gran habilidad para encontrar las pistas ocultas, y eso me permite compartirte información crucial que hasta ahora había estado resguardada.

Como ya sabrás, la situación está empeorando rápidamente. Las amenazas se vuelven más inminentes, y confío que tu capacidad de resolver enigmas de podrá salvar. **Los dos primeros dígitos CONSECUTIVOS que encontraste son la clave inicial de la contraseña que necesitas.**

Pero no te confies. Todavía hay más enigmas por resolver. Para garantizar que esta información no caiga en las manos equivocadas, el resto de la contraseña sigue protegida y deberás encontrarla por tu cuenta. **Los próximos dos dígitos** están escondidos en otro lugar, uno que requerirá de tu máxima atención y concentración.

Recuerda, este no es un simple juego. Cada segunda cuenta, y cada paso te acerca más al objetivo final. El camino no será fácil, pero confío en que tienes las habilidades necesarias para seguir adelante.

Haz clic en el enlace al final de esta página para continuar. Revisa cada detalle con cuidado y usa todo lo que has aprendido hasta ahora. Llegar al búnker depende de ti.

<https://drive.google.com/file/d/1mFKJmGQTrp9JRrl7xLQ2YX0z1yWynFIS/view?usp=sharing>

Figura 49 : Se muestra el contenido del archivo **sigue**

El archivo nos indica que los dos primeros dígitos de la contraseña son el “1” y el “4” ya que son los dos primeros dígitos consecutivos y ademas nos proporciona un enlace para poder continuar el reto.

<https://drive.google.com/file/d/1mFKJmGQTrp9JRrl7xLQ2YX0z1yWynFIS/view>

Este enlace lleva a un archivo **Titulares.zip** el cual descomprimimos y podemos observar que en su interior tiene un archivo **Desconocido** sin extensión y un archivo **Noticias.html** como muestra la *Figura 50*.

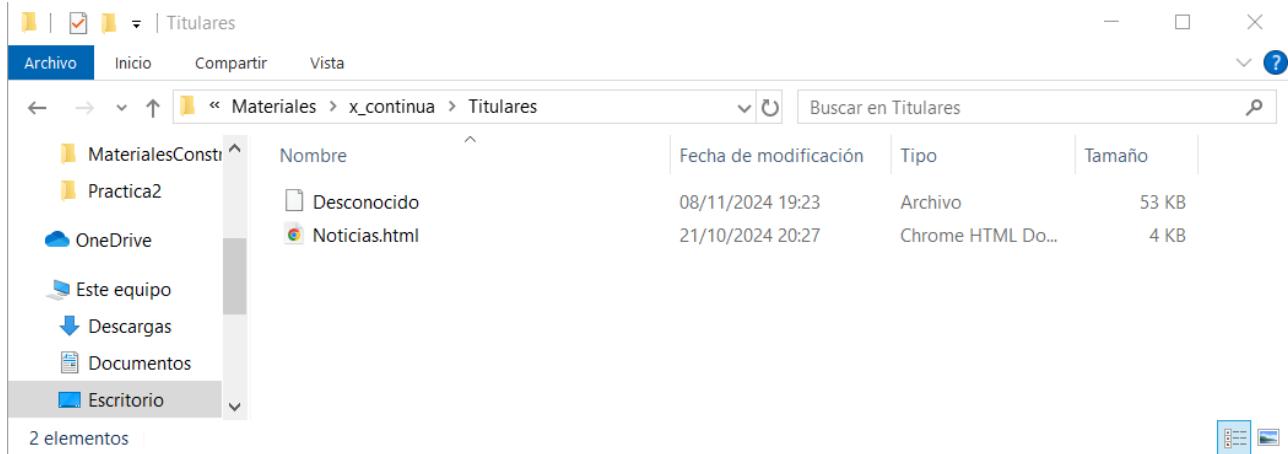


Figura 50 : Se muestra el contenido del la carpeta Titulares

Dado estas pistas analizaremos la extensión del archivo **Desconocido** como antes, dándonos el siguiente resultado:

Match	Ext	File type	MIME type	Related URL	Def's author
100.00%	PDF	Adobe Portable Document Format	application/pdf	http://en.wikipedia.org/wiki/Pdf	Marco Pontello

Figura 51 : Se muestra la extensión de archivo Desconocido

Una vez tenemos la extensión tenemos el fichero y obtenemos un mensaje cifrado y otro enlace a drive para seguir con el reto, como antes, usaremos la página web para ver que tipo de cifrado es y luego lo descifraremos.

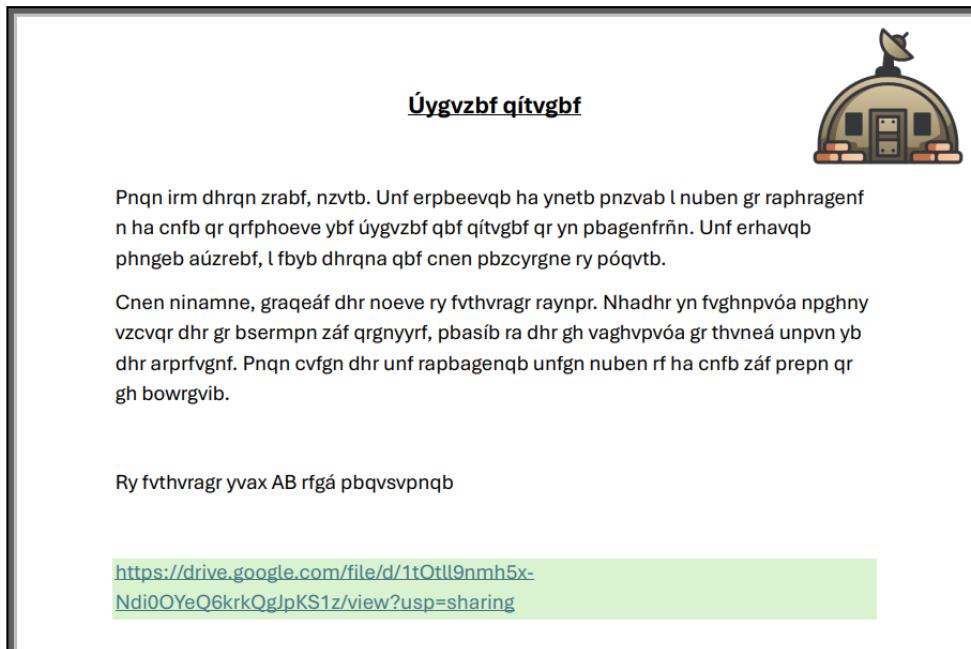


Figura 52 : Se muestra el contenido del fichero **Desconocido.pdf**

The screenshot shows the Cryptool website interface. On the left, there's a search bar for tools and a sidebar with links like 'ROT-13 Cipher_us', 'Substitution Cipher_us', etc. The main area is titled 'IDENTIFICADOR DE CIFRADO' and contains sections for 'IDENTIFICAR UN MENSAJE CODIFICADO' and 'IDENTIFICADOR DE SÍMBOLOS'. It displays analysis results for the message 'Ry fvthvragr yvax AB rfgá pbqvsvpnqb', including 'PISTAS/PALABRAS CLAVE (OPCIONAL)' and a button to 'ANALIZAR'. A summary sidebar on the right lists various topics related to cryptography.

Figura 53 : Se obtiene el resultado del tipo de cifrado que es.

Úygvzbf qítvgbf
Pnqn irm dhrqn zrabf, nzytb. Unf erpbeevqb ha ynetb pnzvab l nuben gr raphragenf
n ha cnfb qr qrfphoeve ybf úygvzbf qbf qítvgbf qr yn pbagenfrñ. Unf erhavqb
phngeb aúzrebf, l fbyb dhrqna qbf cnen pbzcyrge ry póqvtb.
Cnen minamne, graqeáf dhr noeve ry fvthvragr raynpr. Nhadhr yn fvghnpvúa npghny
vzcvqr dhr gr bsermpn záf qrgnyyrf, pbasisb ra dhr gh vaghvpvúa gr thvneá unpvn yb
dhr arprfvgnf. Pnqn cvfgn dhr unf rapbagenaó unfen nuben rf ha cnfb záf prepñ gr
gh bowrgvib.
Ry fvthvragr vyax AB rfgá pbqysvpnqab



ROT13 ▾



Últimos dígitos
Cada vez queda menos, amigo. Has recorrido un largo camino y ahora te encuentras
a un paso de descubrir los últimos dos dígitos de la contraseña. Has reunido
cuatro números, y solo quedan dos para completar el código.
Para avanzar, tendrás que abrir el siguiente enlace. Aunque la situación actual
impide que te ofrezca más detalles, confío en que tu intuición te guiará hacia lo
que necesitas. Cada pista que has encontrado hasta ahora es un paso más cerca de
tu objetivo.
El siguiente link NO está codificado

Figura 54 : Se obtiene el texto descifrado.

El texto descifrado nos indica que pasemos al siguiente paso, pero antes buscaremos en el código de **Noticias.html** alguna pista más.

Noticias del Día

Actualidad Global



En el día de hoy, múltiples temas han dominado los titulares de todo el mundo. Entre las noticias más destacadas se encuentra la situación económica global, así como los avances tecnológicos que están redefiniendo el futuro de las telecomunicaciones.

Tendencias en Tecnología

Figura 55 : Se observa el contenido de **Noticias.html**

```

► <p>...</p>
<!-- ===== -->
<!--    !!ATENCION!!    -->
<!-- ===== -->
<!--    SIGUIENTE PISTA    -->
<!--    Los siguientes dos digitos de la contraseña son: 79    -->
► <div class="hidden-hint">...</div>
</main>
► <footer>...</footer>
</body>

```

Figura 56 : Se observa el código fuente de **Noticias.html**

Observando el código fuente de la página nos dan los dos siguientes números de la contraseña, quedándonos la contraseña final “1479**” faltandonos dos dígitos. Después de terminar de analizar todas las pistas continuamos con el enlace a drive que nos dio en el archivo **Desconocido.pdf**.

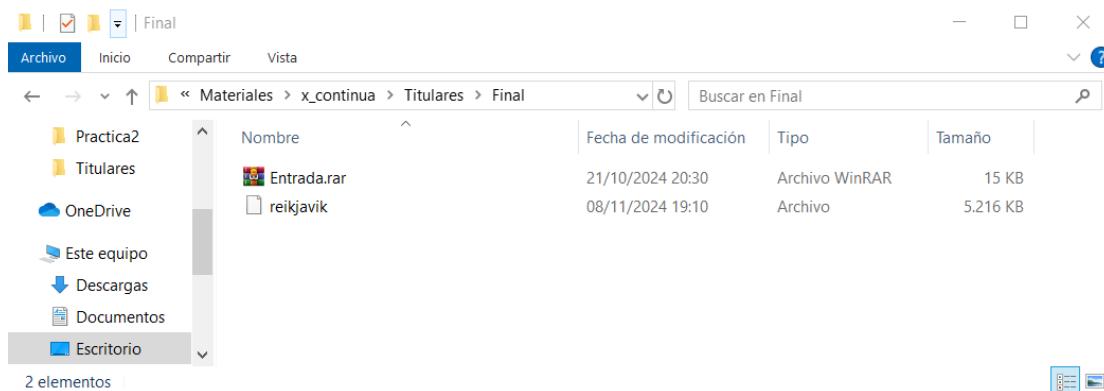


Figura 57 : Se muestra el contenido de la carpeta **Final**

En esta carpeta tenemos un archivo **Entrada.rar** y un archivo sin extensión, del cual la sacaremos como anteriormente. Analizando su extensión observamos que tiene formato .bmp y que tiene el 50% formato Bitmap por lo que se intuye que puede tener información oculta en su interior.

Match	Ext	File type	MIME type	Related URL	Def's author
50.00%	BMP RLE	DIB	image/bmp	Windows Bitmap (generic)	Joerg Jenderek
				RLE is sometimes used for run length encoded variants; OS2 is sometimes used for OS/2 system variants; HCP is sometimes used by hardcopy tool; POG is used for PowerQuest PartitionMagic graphic; SPG is used for some Infineon Logo; SYS is used for Windows 9M boot messages; WBF is used for Epson printer water mark	
				This variant with 40 byte DB header (Windows 3.x)	Joerg Jenderek
				https://en.wikipedia.org/wik/BMP_file_format	

Figura 58 : Se muestra el análisis de la extensión del archivo **reikjavik**

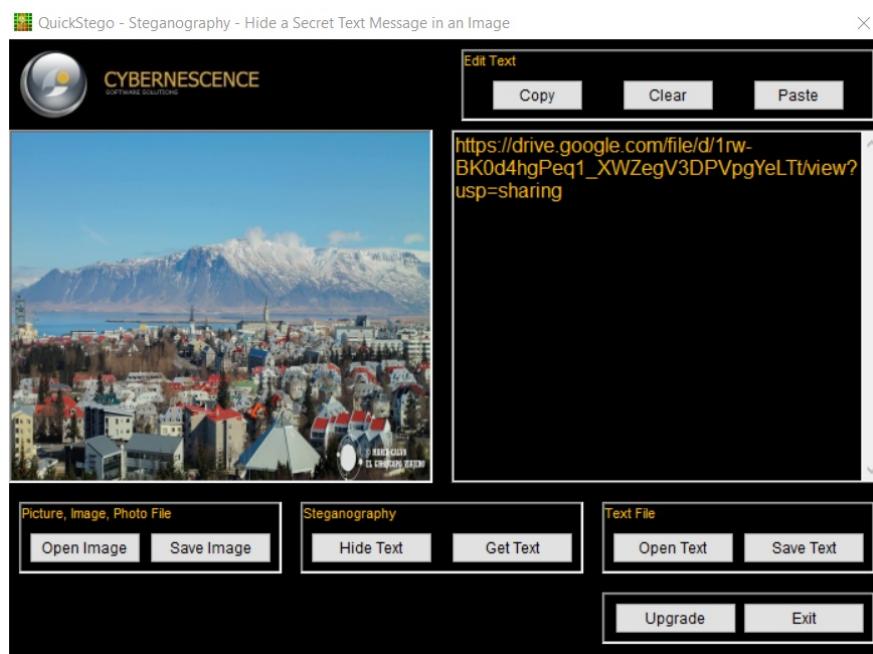


Figura 59 : Se muestra el análisis de la imagen **reikjavik.bmp** con QuickStego



Figura 60 : Se muestra el resultado del enlace que contenía oculta la imagen **reikjavik.bmp**

← Resultado del escaneo



Texto

Felicitaciones, amigo!
Estás a punto de alcanzar la clave del refugio.
Estoy asombrado de que estés aquí. Te mereces
conocer los últimos dos dígitos de la contraseña.
Recuerda: la X va antes que la Y.

No iba a hacerte el final tan fácil. Aquí tienes un
pequeño reto:
 $3x + 5 = 20$
 $4y - 6 = 10$

Figura 61 : Se muestra el resultado del escaneo

Dáandonos un resultado de 5 y 4 siendo los dos últimos dígitos de la contraseña. Quedando que la contraseña final es “147954”, el cual introduciremos en la contraseña que pide **Entrada.rar**.

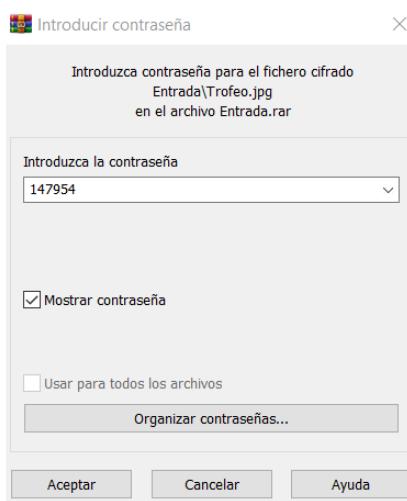


Figura 62 : Se muestra como se pone la contraseña del final

Una vez desbloqueado la contraseña final obtenemos el premio como se muestra en la *Figura 63*



Figura 63 : Se muestra el trofeo final