



Auditoría y Legislación Informática

Resuelve y construye tu CTF



ÍNDICE

INTRODUCCIÓN DEL RETO.....	3
CONSTRUCCIÓN DEL RETO	4
• ARCHIVOS UTILIZADOS.....	4
• CREACIÓN DEL RETO	7
RESOLUCIÓN RETO COMPAÑERO	12

INTRODUCCIÓN DEL RETO

Bienvenidos al CTF "Investigación del Ataque de Phishing". En este desafío, los participantes se adentrarán en el mundo oscuro y engañoso del ciberdelito, donde tendrán la oportunidad de demostrar sus habilidades de ciberseguridad y resolver un misterio que amenaza la seguridad de una empresa ficticia llamada "TechSecure". Como investigadores de ciberseguridad, su misión es desentrañar un sofisticado ataque de phishing y proteger la valiosa información de esta empresa.

LA HISTORIA:

La empresa "TechSecure" se encuentra en una situación crítica. Un ataque de phishing ha comprometido su seguridad cibernética y su información confidencial está en peligro. Como un equipo de investigadores de ciberseguridad contratado para resolver este misterio, su tarea es descubrir quién está detrás del ataque, recuperar información crítica y ayudar a TechSecure a fortalecer su seguridad.

EL DESAFÍO:

En su investigación, descubrirán cuatro imágenes relacionadas con el ataque: un intento de registro de usuario, un inicio de sesión falso, el retorcido código fuente de la página de inicio de sesión y detalles de pago maliciosamente enmarañados. Cada imagen contiene pistas ocultas que los guiarán a través del laberinto de engaño hacia la reconstrucción de un código QR dividido en partes.

EL OBJETIVO:

El objetivo final es descubrir el orden correcto para ensamblar las partes del código QR. Cuando descifren este código QR y lo escaneen, serán conducidos a coordenadas geográficas. Estas coordenadas actuarán como la clave que les permitirá acceder a un informe de seguridad valioso y crucial para TechSecure. Proteger esta información es esencial para garantizar la seguridad de la empresa y prevenir futuros ataques de phishing.

SU MISIÓN:

Con su astucia y conocimientos en ciberseguridad, tienen la responsabilidad de resolver este misterio en línea y desentrañar la verdad detrás del ataque de phishing. La empresa TechSecure confía en ustedes para proteger su información crítica. ¿Están listos para enfrentar el desafío y demostrar sus habilidades de ciberseguridad? ¡Comencemos la investigación del ataque de phishing!".

CONSTRUCCIÓN DEL RETO

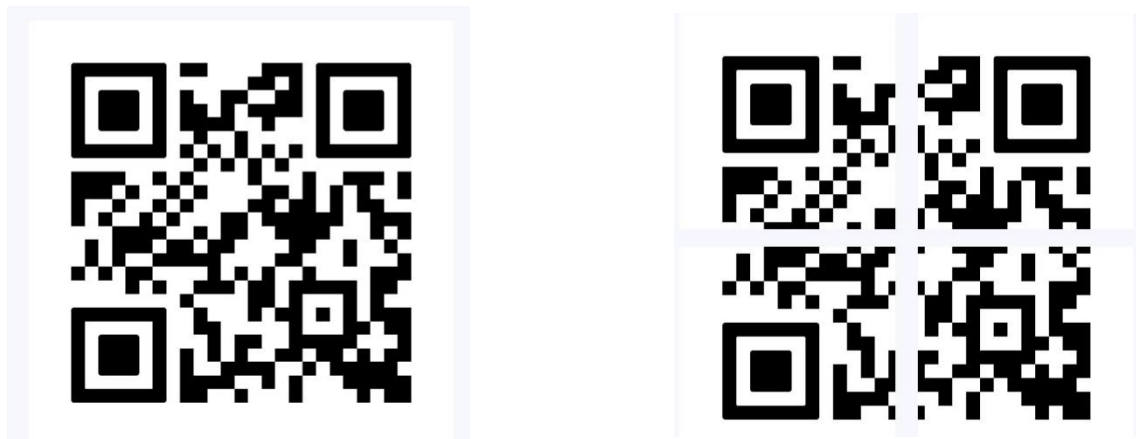
En este paso, se describen los archivos utilizados como base para el CTF "Investigación del Ataque de Phishing". Se incluyen imágenes correspondientes a un registro de usuario, un inicio de sesión, el código fuente de la página de inicio de sesión y un proceso de pago en una web de phishing. A continuación, se detallan los archivos y su función en el CTF:

ARCHIVOS UTILIZADOS

Este equipo > Documentos > Universidad > Ingeniería Software_3ºAño > Auditoria y Legislacion (ALI) > Practica2_Lab >				
	Nombre	Fecha	Tipo	Tamaño
	codigoFuenteWeb	24/10/2023 22:24	Archivo BMP	46.751 KB
	Descripción_CTF	25/10/2023 11:39	Documento de texto	1 KB
	inicioSesion	24/10/2023 22:23	Archivo BMP	46.751 KB
	Premio	25/10/2023 0:04	Archivo WinRAR ZIP	13.242 KB
	procesoPago	24/10/2023 22:23	Archivo BMP	46.751 KB
	web	24/10/2023 22:23	Archivo BMP	46.751 KB

Archivo: "codigo_qr.png"

Descripción: Este es el elemento central del CTF. Contiene las coordenadas geográficas que servirán como contraseña para acceder al archivo ZIP que contiene el premio final. El código QR se dividió en cuatro partes y se ocultó en las imágenes de phishing. Los participantes deberán ensamblar el código QR en el orden correcto para obtener las coordenadas.



Este código QR desempeña un papel crucial en la resolución del CTF, ya que es el objetivo final que los participantes deben descubrir y ensamblar para acceder al premio. Cada parte del código QR se oculta en las imágenes de phishing y se relaciona con pistas y desafíos que guían a los jugadores en la reconstrucción correcta

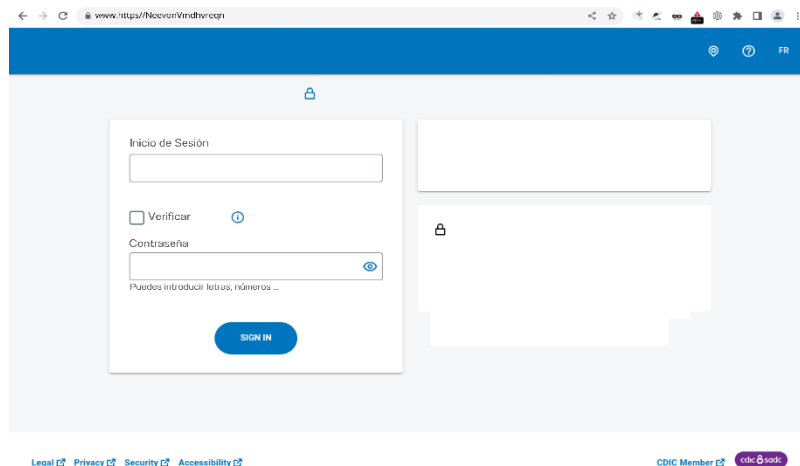
Archivo: "web.bmp"

Descripción: Esta imagen representa un intento de registro de usuario en un sitio web de phishing. Contiene pistas visuales y textuales relacionadas con el orden correcto de las partes del código QR.



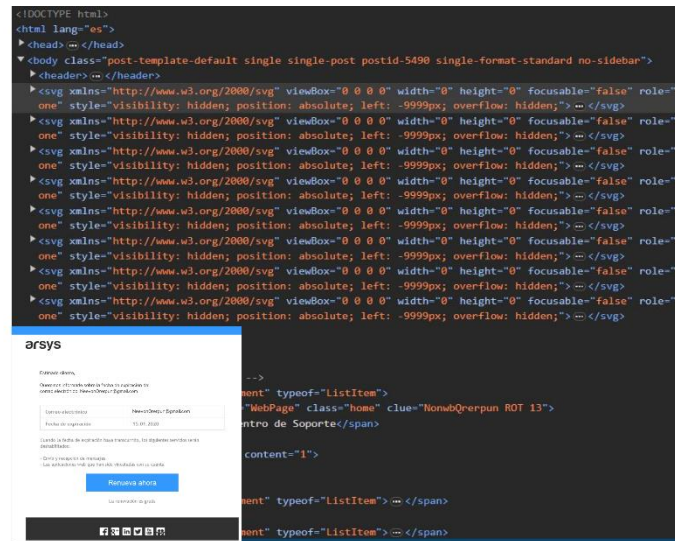
Archivo: "inicioSesion.bmp"

Descripción: Esta imagen simula una trampa de inicio de sesión en un sitio web falso. Contiene pistas que indican su posición en el orden del código QR.



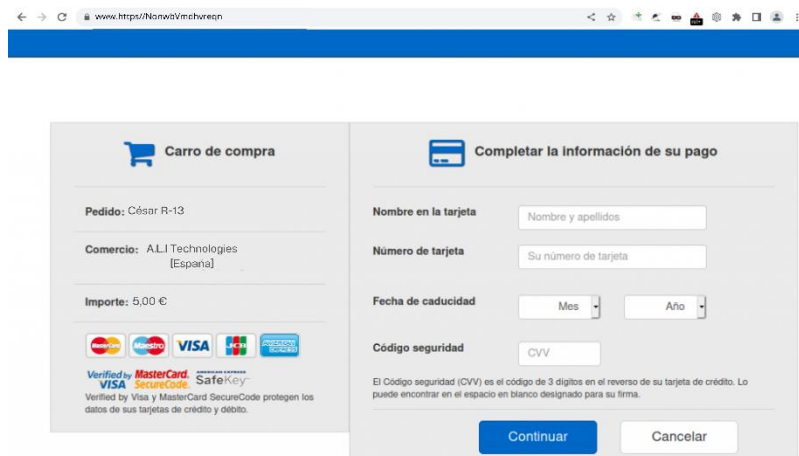
Archivo: "codigoFuenteWeb.bmp"

Descripción: En esta imagen se muestra el código fuente de la página de inicio de sesión falsa. Proporciona pistas visuales y textuales sobre el orden de las partes del código QR.



Archivo: "proceso_de_pago.png"

Descripción: Representa detalles de pago maliciosamente enmarañados en un sitio web de phishing. Incluye pistas que indican su posición en el orden del código QR.

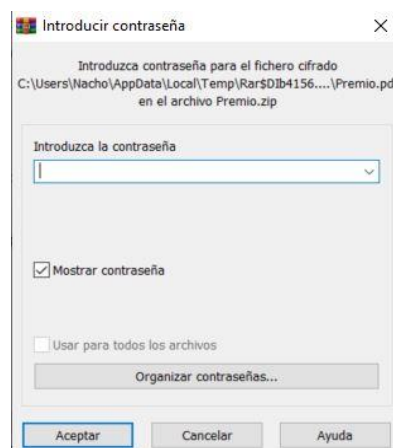
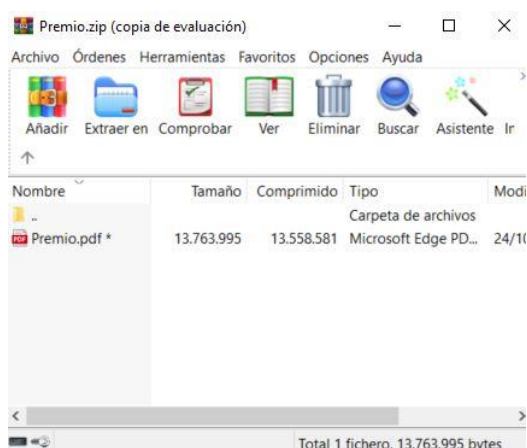


Estas imágenes servirán como elementos clave en la construcción del CTF y proporcionarán pistas visuales y textuales para los participantes mientras intentan descifrar el orden correcto de las partes del código QR. Cada imagen contiene información relevante que guiará a los jugadores a través del desafío.

En los siguientes pasos, se explicará cómo estas imágenes se utilizan para ocultar las partes del código QR y cómo se crean pistas relacionadas con el orden correcto. También se describirán las herramientas y técnicas utilizadas para lograr esto.

Archivo: "premio.zip"

Descripción: El archivo ZIP contiene el premio final (archivo: "premio.pdf") que los participantes del CTF buscan desbloquear. Las coordenadas geográficas obtenidas al escanear el código QR llevan a averiguar la contraseña para acceder a este archivo ZIP.



CREACIÓN DEL RETO

En este paso, se explican los conceptos y herramientas clave utilizados en la creación del CTF "Investigación del Ataque de Phishing". Se describen de manera clara y concisa, junto con los pasos a seguir para crear el reto.

Creación y División del Código QR:

Creación: El código QR se creó como un componente clave del CTF. Representa la información final que los participantes deben descubrir para acceder al premio. El código QR se generó utilizando una herramienta en línea de generación de códigos QR (<https://www.qr-code-generator.com/>). Contiene las coordenadas geográficas que servirán como contraseña para acceder al archivo ZIP que posee el premio final.

División en Cuatro Partes: El código QR se dividió en cuatro partes iguales para aumentar la dificultad del CTF. El QR fue dividido gracias a la utilización de la herramienta (<https://splitter.imageonline.co/es>). Cada parte del código QR se ocultó en una de las cuatro imágenes base. La división en cuatro partes tenía la finalidad de que los participantes debieran encontrar y ensamblar las partes del código QR en el orden correcto.



Esteganografía:

Concepto: La esteganografía es la práctica de ocultar información dentro de otros archivos o medios de manera que no sea evidente a simple vista. En el CTF, se utilizó para ocultar pistas de la ordenación y colocación de las diferentes partes del QR en las imágenes proporcionadas.

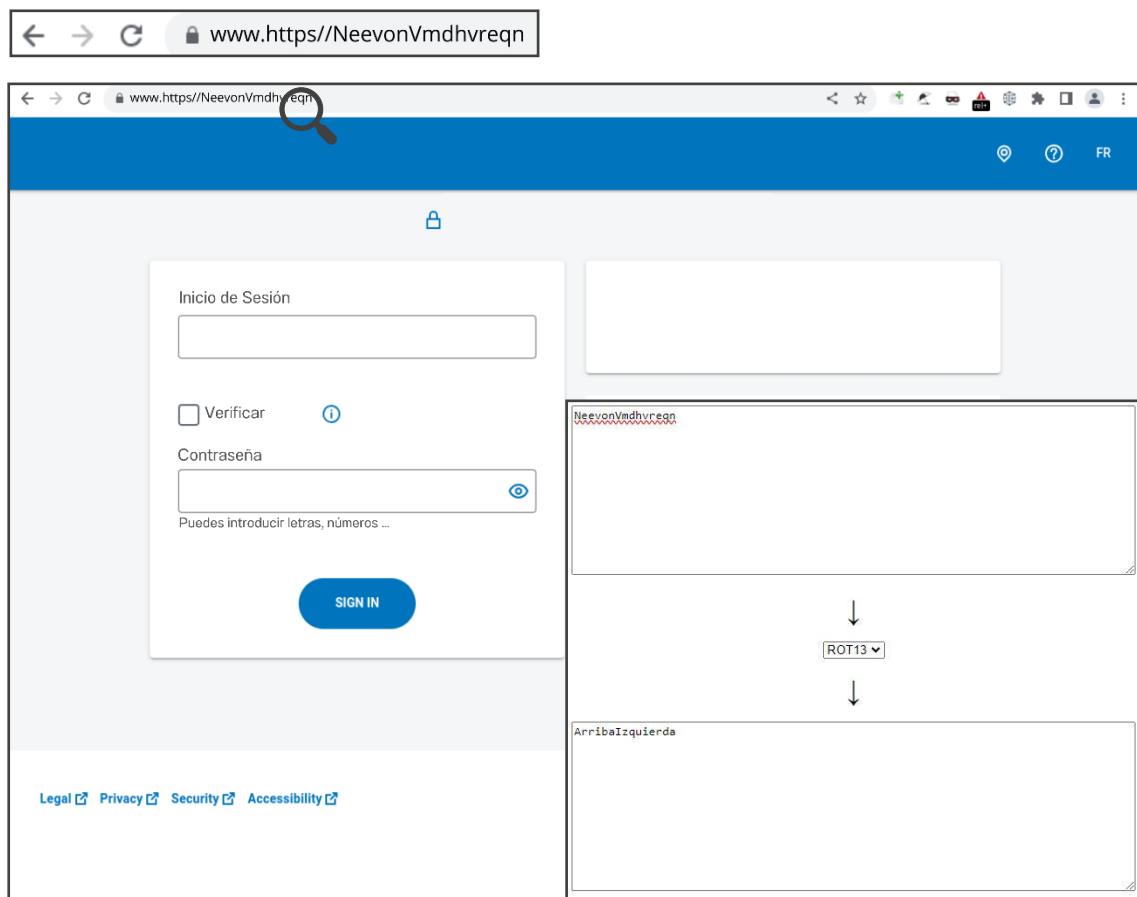
Herramientas: Para ocultar las pistas en las imágenes, se utilizó una herramienta de edición de imágenes en línea, como Canva (<https://www.canva.com/>).

Criptografía:

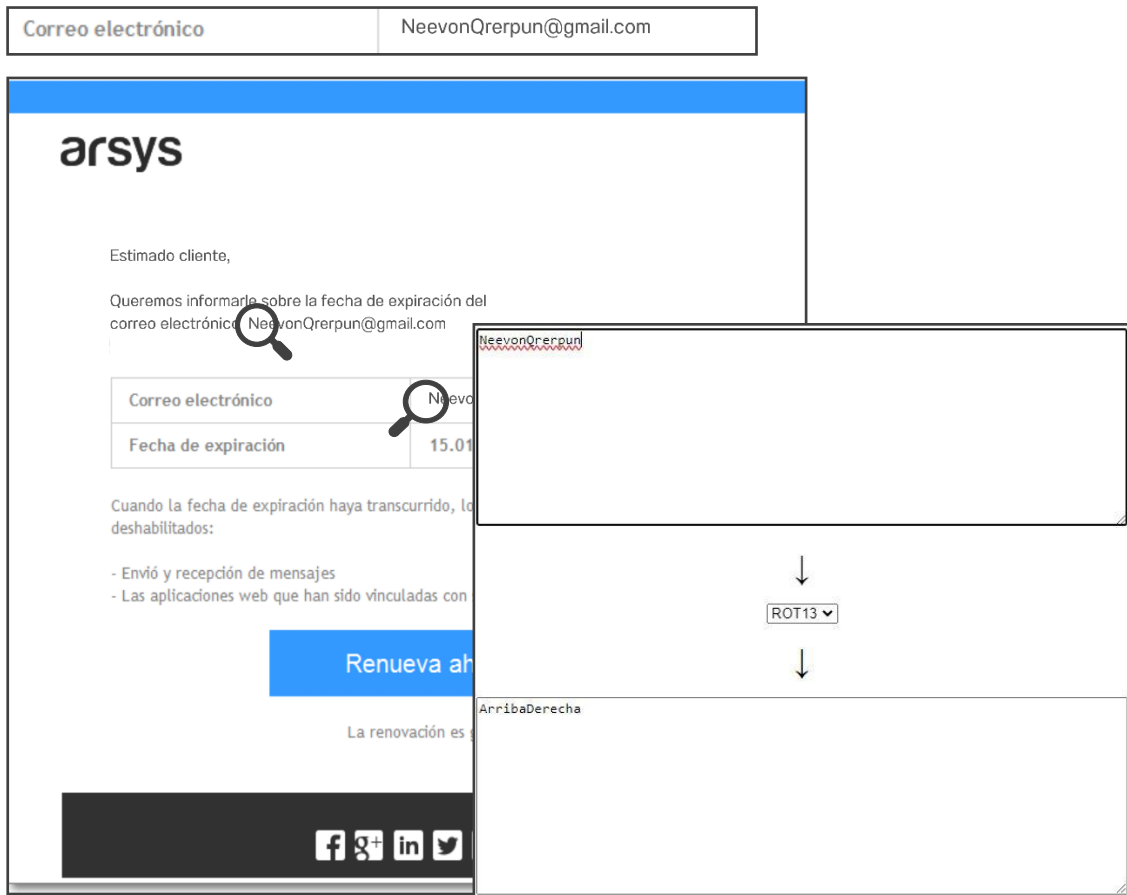
Concepto: La criptografía implica el uso de técnicas de cifrado para proteger la información. En el CTF, se aplicó la criptografía mas concretamente se utilizó el cifrado César con un desplazamiento de 13 caracteres para cifrar las pistas ocultas en las imágenes.

Herramientas: Para cifrar las pistas se uso un cifrado simple como el César R-13 gracias a la web Rot13 (<https://rot13.com/>).

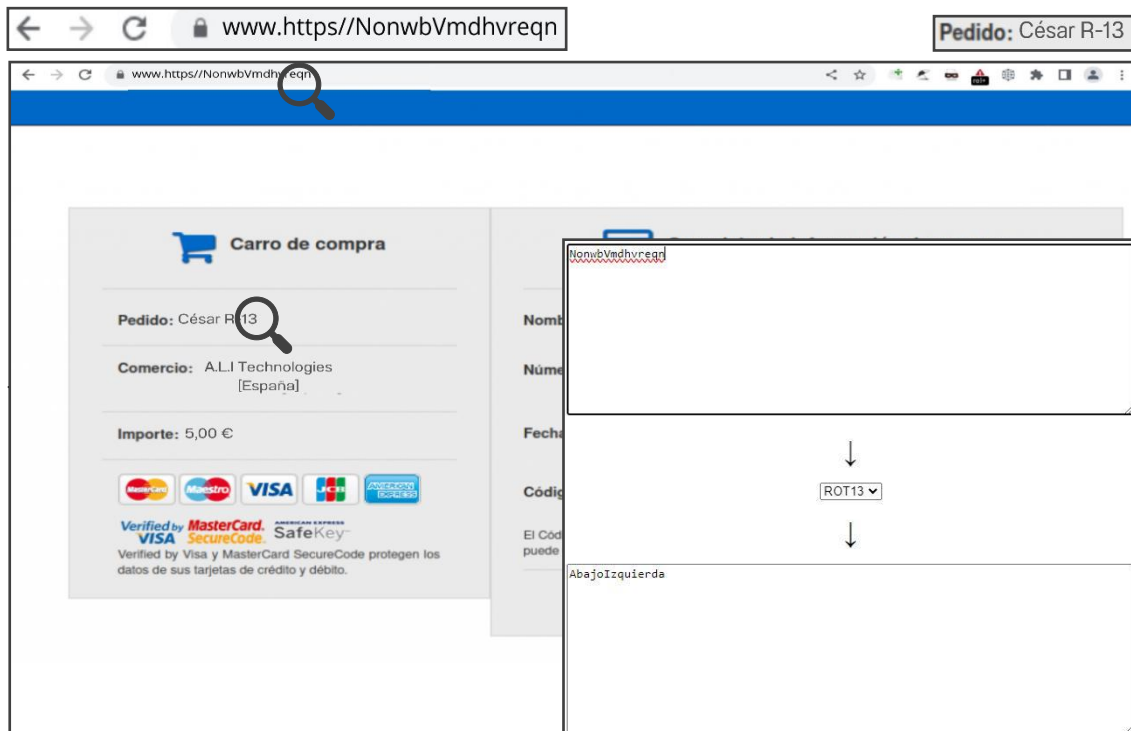
Pista1. Archivo: "inicioSesion.bmp" = NeevonVmdhvreqn



Pista2. Archivo: "web.bmp" = NeevonQrerpun



Pista3. Archivo: "procesoPago.bmp" = NonwbVmdhvreqn, César R-13



Pista4. Archivo: "códigoFuenteWeb.bmp" = NonwbQrerpun

The image shows a screenshot of a web page source code and a diagram illustrating a ROT13 cipher. The source code is in Spanish and includes a header with the class "home" and the clue "NonwbQrerpun ROT 13". The code also contains several SVG elements with hidden styles. The diagram shows a box labeled "NonwbQrerpun" with a downward arrow pointing to a box labeled "ROT13", which then points to a box labeled "AbajoDerecha".

```
class="home" clue="NonwbQrerpun ROT 13">
```

```
<!DOCTYPE html>
<html lang="es">
  <head>
    <meta charset="UTF-8">
    <title>NonwbQrerpun ROT 13</title>
  </head>
  <body class="post-template-default single single-post postid-1">
    <div class="page-container">
      <div class="header">
        <h1>NonwbQrerpun</h1>
      </div>
      <div class="content">
        <div class="post">
          <div class="post-content">
            <div class="post-text">
              <p>Estimado cliente,</p>
              <p>Queremos informarle sobre la fecha de expiración del</p>
              <p>correo electrónico NonwbQrerpun@gmail.com</p>
              <p>Fecha de expiración: 15.01.2020</p>
              <p>Cuando la fecha de expiración haya transcurrido, los siguientes servicios serán</p>
              <p>desactivados:</p>
              <ul>
                <li>- Envío y recepción de mensajes</li>
                <li>- Las aplicaciones web que han sido vinculadas con su cuenta</li>
              </ul>
              <p><button>Renueva ahora</button></p>
              <p>La renovación es gratis</p>
              <p><img alt="Social media icons" data-bbox="218 471 281 481"/></p>
            </div>
          </div>
        </div>
      </div>
    </div>
  </body>
</html>
```

Técnicas de OSINT:

Concepto: Las técnicas de OSINT se utilizan para recopilar información de fuentes abiertas y públicas en línea. En el CTF, se utilizaron para diseñar una narrativa realista que involucra a la empresa ficticia "TechSecure" y un ataque de phishing.

Herramientas: No se requirió el uso de herramientas de OSINT específicas, pero se realizó una investigación básica en línea para recopilar información de referencia sobre seguridad cibernética y phishing.

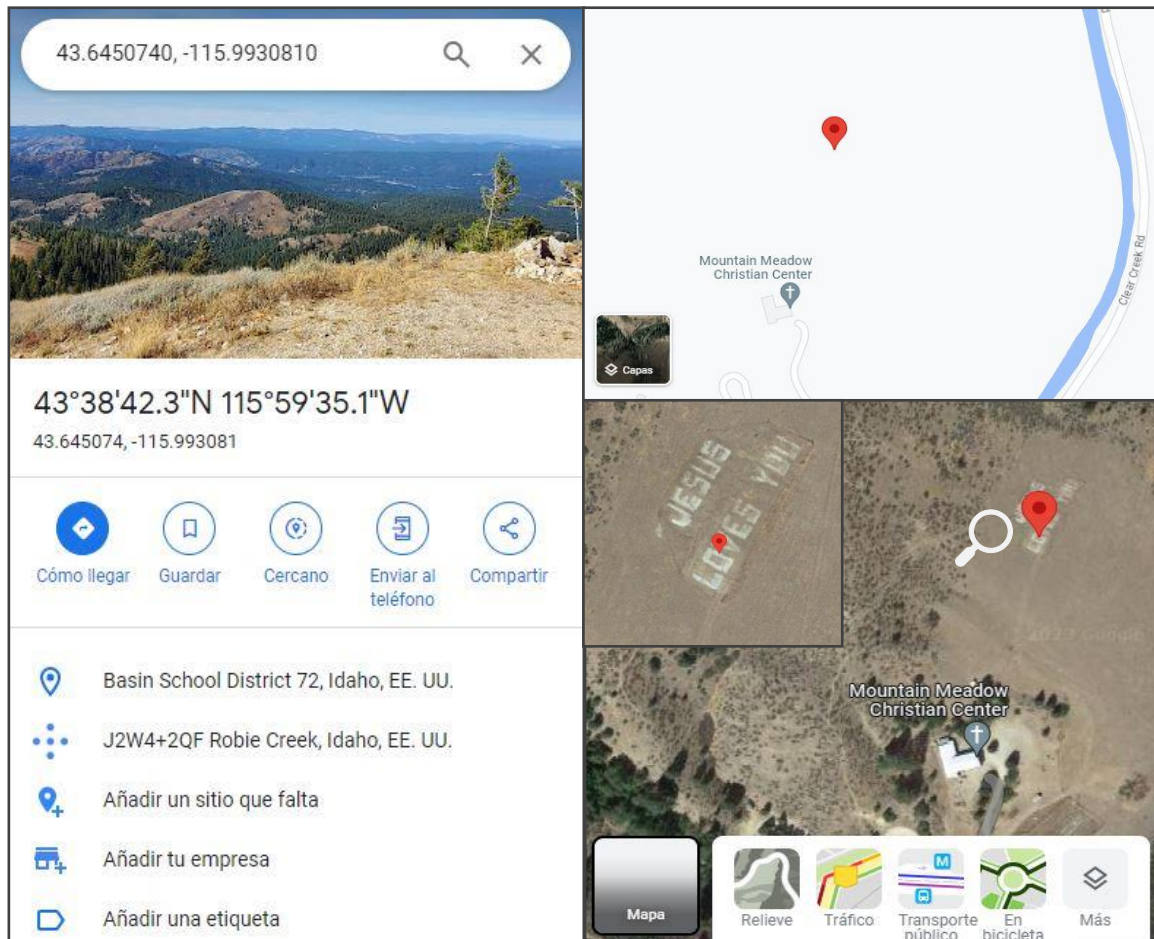
Geocaching:

Concepto: El Geocaching es una actividad recreativa en la que las personas utilizan coordenadas GPS para buscar tesoros o contenedores escondidos en ubicaciones específicas en todo el mundo. En el CTF, se empleó una variación de esta técnica. Los participantes debían utilizar Google Maps en modo relieve y hacer zoom para encontrar una palabra escrita en la tierra que actúa como la contraseña para desbloquear el archivo ZIP con el premio final.

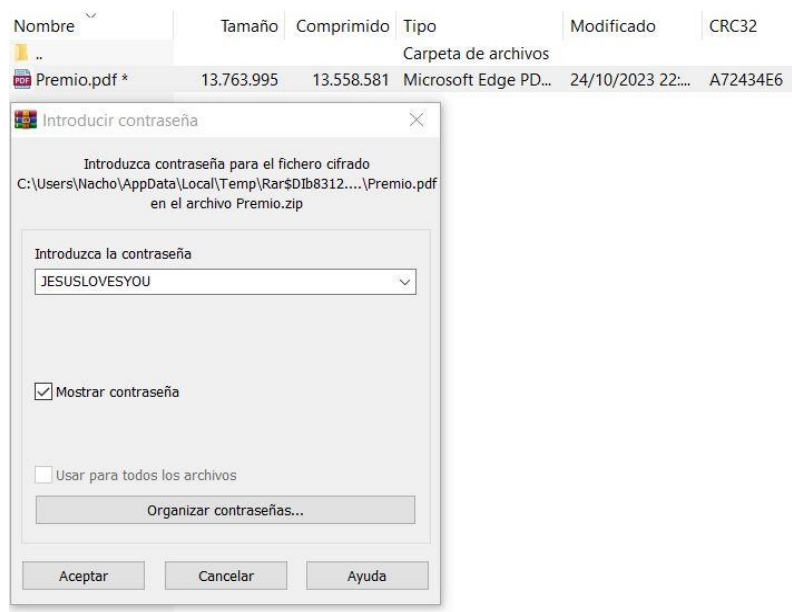
Herramientas: Para esta técnica, se utilizó Google Maps (<https://www.google.com/maps>) como plataforma para buscar la ubicación geográfica con la palabra escrita en la tierra. No se necesitaron herramientas adicionales, ya que se aprovechó una función estándar de Google Maps.

Esta técnica añade un elemento de búsqueda en el mundo real a la resolución del CTF, lo que hace que el proceso sea más interactivo y desafiante para los participantes. El uso de Google Maps y la búsqueda de coordenadas geográficas reales agregan un toque único y emocionante al CTF.

Contraseña del archivo (premio.zip) = JESUSLOVESYOU

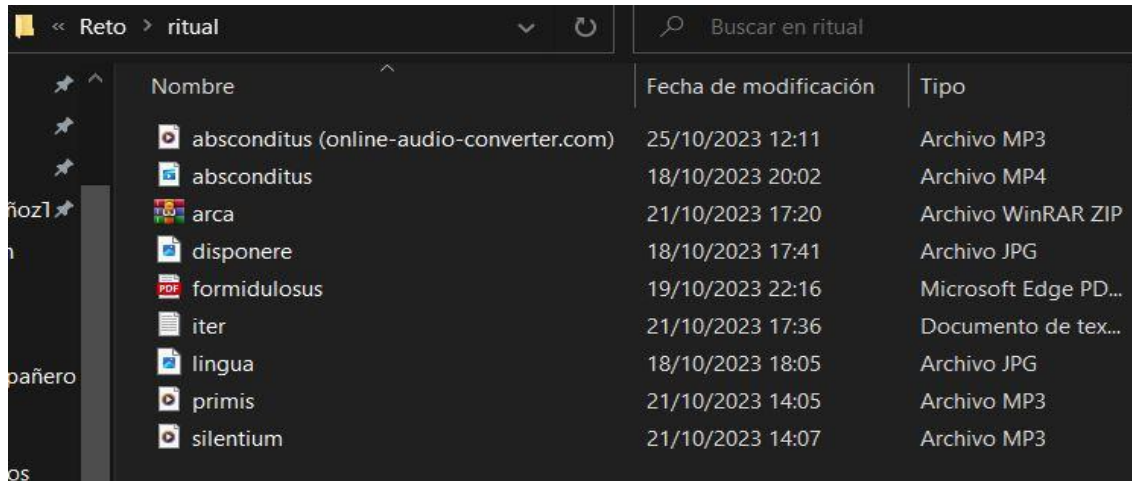


Premio final:



RESOLUCIÓN RETO COMPAÑERO

A continuación voy a resolver el reto de mi compañero. En mi caso fue asignado el CTF de Rubén Vázquez Angamarca.

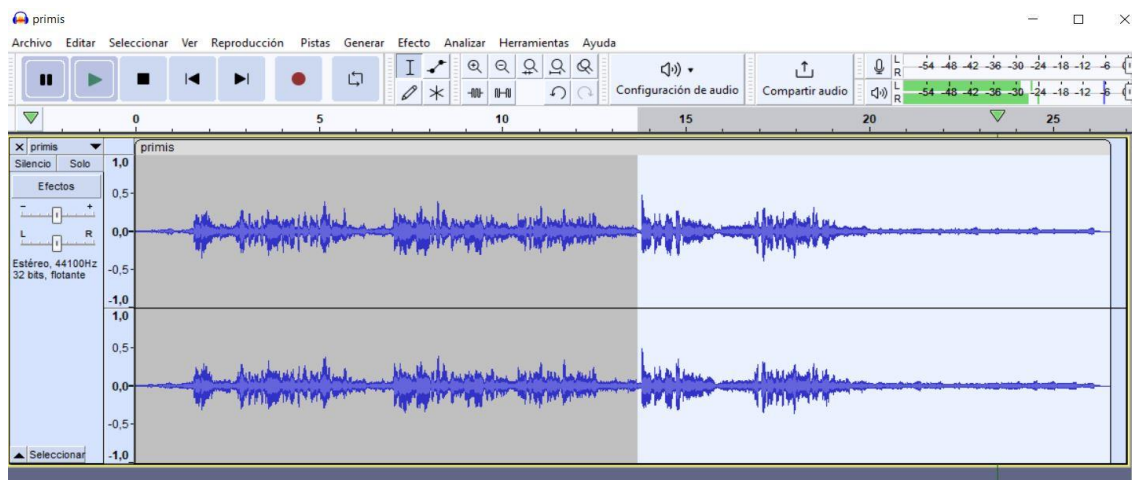


The screenshot shows a Windows File Explorer window with the address bar set to 'Reto > ritual'. The search bar contains 'Buscar en ritual'. The main area displays a list of files with columns for 'Nombre', 'Fecha de modificación', and 'Tipo'.

Nombre	Fecha de modificación	Tipo
absconditus (online-audio-converter.com)	25/10/2023 12:11	Archivo MP3
absconditus	18/10/2023 20:02	Archivo MP4
arca	21/10/2023 17:20	Archivo WinRAR ZIP
disponere	18/10/2023 17:41	Archivo JPG
formidulosus	19/10/2023 22:16	Microsoft Edge PD...
iter	21/10/2023 17:36	Documento de tex...
lingua	18/10/2023 18:05	Archivo JPG
primis	21/10/2023 14:05	Archivo MP3
silentium	21/10/2023 14:07	Archivo MP3

El primer paso consistía en abrir `primis.mp3` utilizando la herramienta de edición de audio Audacity. Al escuchar el contenido del archivo, se podía notar que había modificado. La pista de audio presentaba alguna alteración.

Para abordar este problema, se procedió a revertir la pista de audio en un intento de restablecer su estado original.



La modificación en la pista de audio llevó a la necesidad de realizar ajustes para entender el mensaje oculto, como cambios en la velocidad del audio.

Mensaje oculto en el audio:

“Si estas escuchando esto significa que el ritual ha comenzado. El demonio solamente ataca a aquellos que no sean informáticos, así que tendrás que demostrar de lo que eres capaz. Hay información oculta en el silencio. Recuerda lo que has aprendido en ALI para obtenerla. El camaleón puede reparar imágenes.”

El segundo paso implicó el uso de QuickStego para extraer información oculta del archivo de audio "silentum.mp3".



El mensaje extraditado contenía la siguiente información: "La foto con el demonio es 1 y la foto sin el demonio es 0. Los textos en iter.txt son posibles soluciones al valor desconocido en https://drive.google.com/file/d/_____/view"

Siguiendo las indicaciones extraídas, se procedió a analizar el video "abscoditus.mp4". La pista reveló que el demonio estaba presente en ciertas partes del video, y el objetivo era contar sus apariciones.

Se reprodujo el video "abscoditus.mp4" y se contaron las apariciones del demonio según las indicaciones dadas en el mensaje extraído. Se obtuvo el número binario "101000" como resultado del conteo de las apariciones del demonio en el video.

Introduzca el número binario:

Convertir Binario a Decimal

Número Decimal:

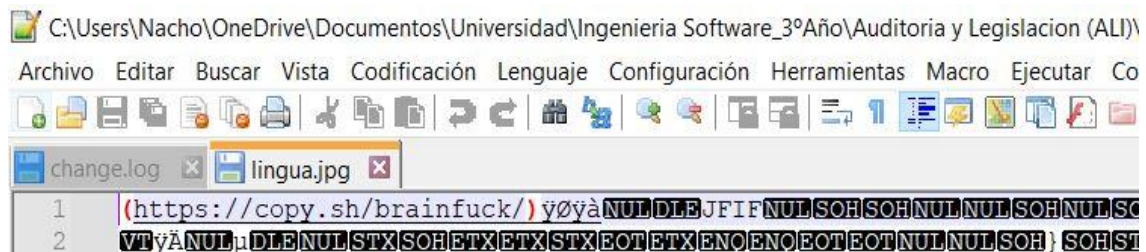
El archivo "iter.txt" contenía un extenso listado de códigos aparentemente codificados. Se relacionó el valor "40" con el enlace https://drive.google.com/file/d/_____/view. Este paso sirvió como conexión entre el código en "iter.txt" y el enlace proporcionado

```
35 - iCdvmPL0HLAtL5eCvq9wUnZ96eAkPLiKH
36 - ee1ktnVr8Wegj1BJWdu9K96N1fFi0Mp1D
37 - b7YAjaWSPK53MAiPjzUivcMdATw9KULy2
38 - ZFFzwf88e7CDEtdjkjXQr20iAH28GuZR4
39 - J04yNJzj4c1rPCM2ZmE1nUFuRqmt3CGhD
40 - 1kWRjJxoBj-F4z2fcKCclj9ZpGkzdxgOC
41 - WanyL0z3ErFfiCXD518vNay16BpAGPtXG
42 - 5bAryHgwHCPMif6eXxwcMXvcaP5nWSEf4
43 - wkVJATvbQathzYbdixiL4A7n86zKjBRnG
44 - A9ByJiFwjxcgCehiZiRNSvenLn3Rv3Nzr
45 - 6tPzA8jqHtRWYu76wEDuEZd00XTndypyf
```

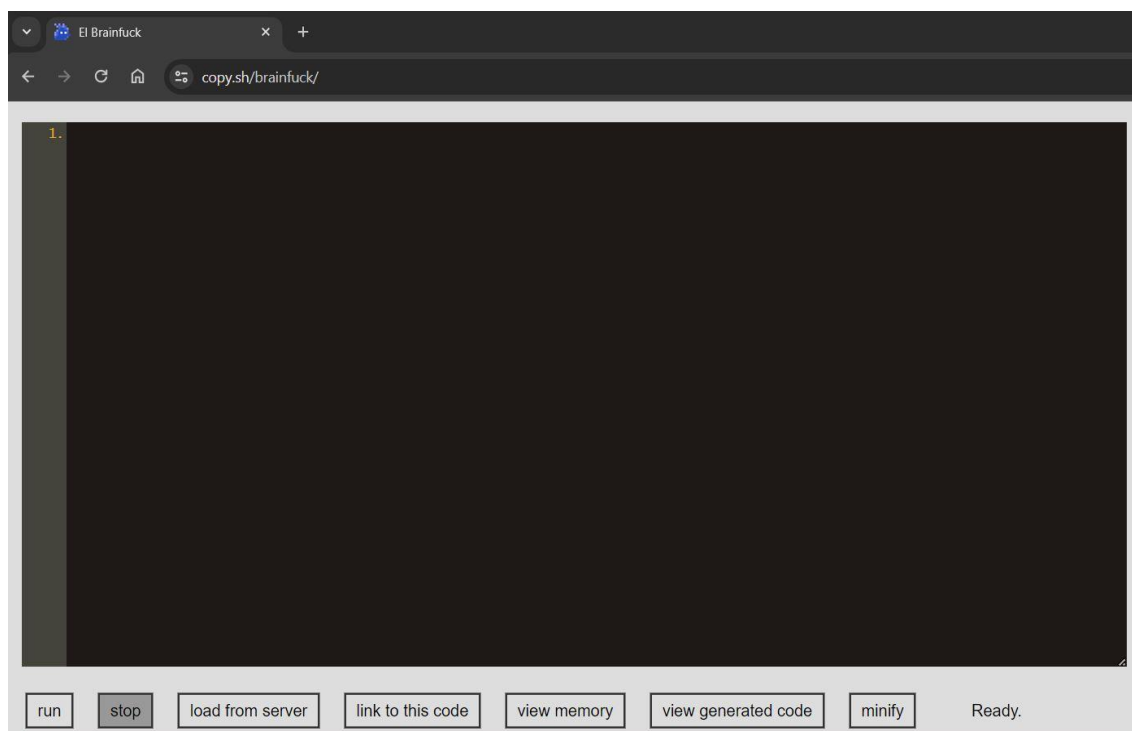

EL enlace completo: <https://drive.google.com/file/d/1kWRjJxoBj-F4z2fcKCclj9ZpGkzdxgOC/view>



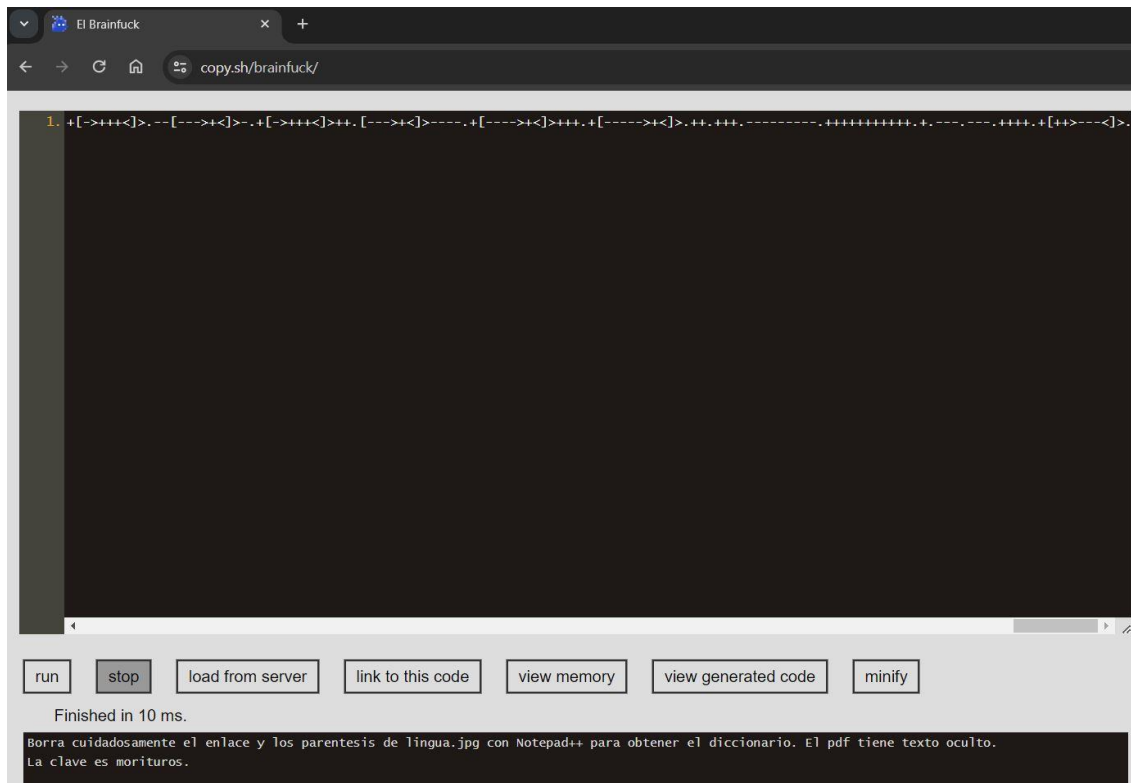
En este paso, se abordó el problema de compatibilidad con el archivo "lingua.jpg" haciendo referencia a la pista proporcionada en el archivo de audio "primis.mp3", que sugería la descarga de una aplicación relacionada con un camaleón. Tras investigar y determinar que se refería a Notepad++, se procedió a abrir el archivo con esta herramienta.



Accedemos a través de un navegador al enlace descubierto: <https://copy.sh/brainfuck>



Introducimos el mensaje descubierto nuntius.txt y ejecutamos el intérprete:

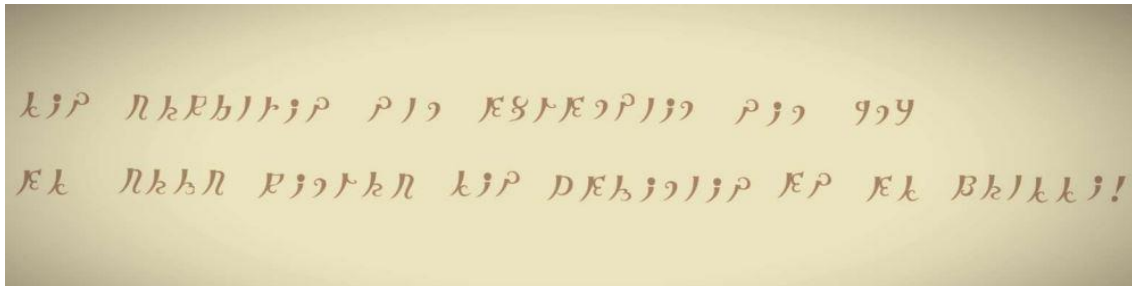


El intérprete de Brainfuck ejecutó el código y reveló el mensaje: "Borra cuidadosamente el enlace y los parentesis de lingua.jpg con Notepad++ para obtener el diccionario. El pdf tiene texto oculto. La clave es morituros."

Tal y como revelo la pista, se procedió a borrar cuidadosamente el enlace y los paréntesis de "lingua.jpg" utilizando Notepad++ y se guardó el archivo resultante. Después de realizar las acciones especificadas, el archivo "lingua.jpg" ahora se puede abrir sin problemas de compatibilidad de formatos.



“El pdf tiene texto oculto”, referido al archivo formidulosus.pdf. Al abrir el archivo, se encontró un texto encriptado que requería el uso del diccionario previamente obtenido para avanzar en el desafío.

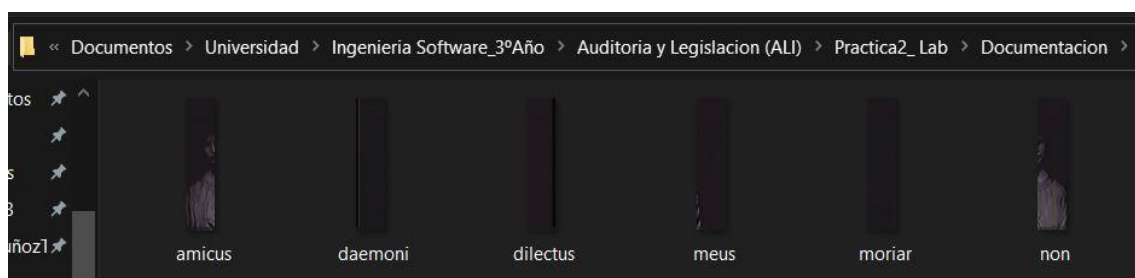


El mensaje oculto revelado fue: "Los archivos sin extensión son png. ¡El arma contra los demonios es el brillo!"

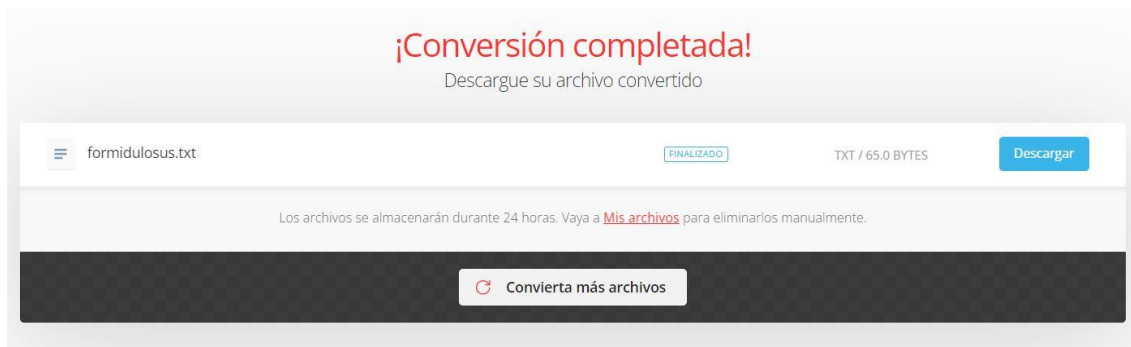
Durante los pasos anteriores, se descubrió una clave, "morituros", asociada con el archivo ZIP "arca.zip". Se procedió a descomprimir este archivo utilizando la clave proporcionada. Al descomprimir el archivo ZIP, se obtuvieron varios archivos.

Nombre	Fecha de modificación	Tipo	Tamaño
amicus	19/10/2023 14:29	Archivo	67 KB
daemoni	19/10/2023 14:29	Archivo	19 KB
dilectus	19/10/2023 14:29	Archivo	9 KB
meus	19/10/2023 14:29	Archivo	20 KB
moriar	19/10/2023 14:29	Archivo	12 KB
non	19/10/2023 14:29	Archivo	65 KB
z	20/10/2023 18:05	Documento de tex...	1 KB

Siguiendo las indicaciones reveladas, se determinó que todos los archivos obtenidos de la descompresión debían tener la extensión PNG para ser visibles. Esto condujo a la obtención de las imágenes siguientes:



Una pista adicional sugería que el PDF "formidulosus.pdf" contenía texto oculto. Para verificar esto, fue empleada la aplicación web convertora de pdf a txt: <https://convertio.co/es>

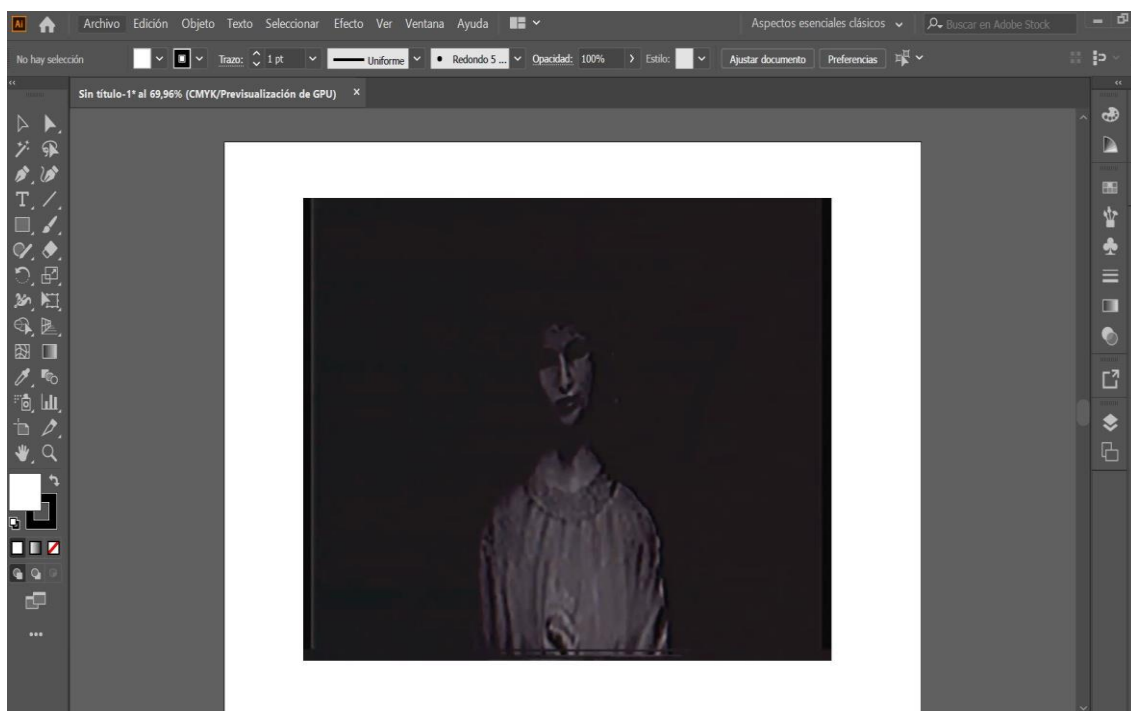


Al examinar el texto convertido, se descubrió que los nombres de las imágenes contenidas en el archivo "arca.zip" estaban asociados a números, siguiendo un orden específico.

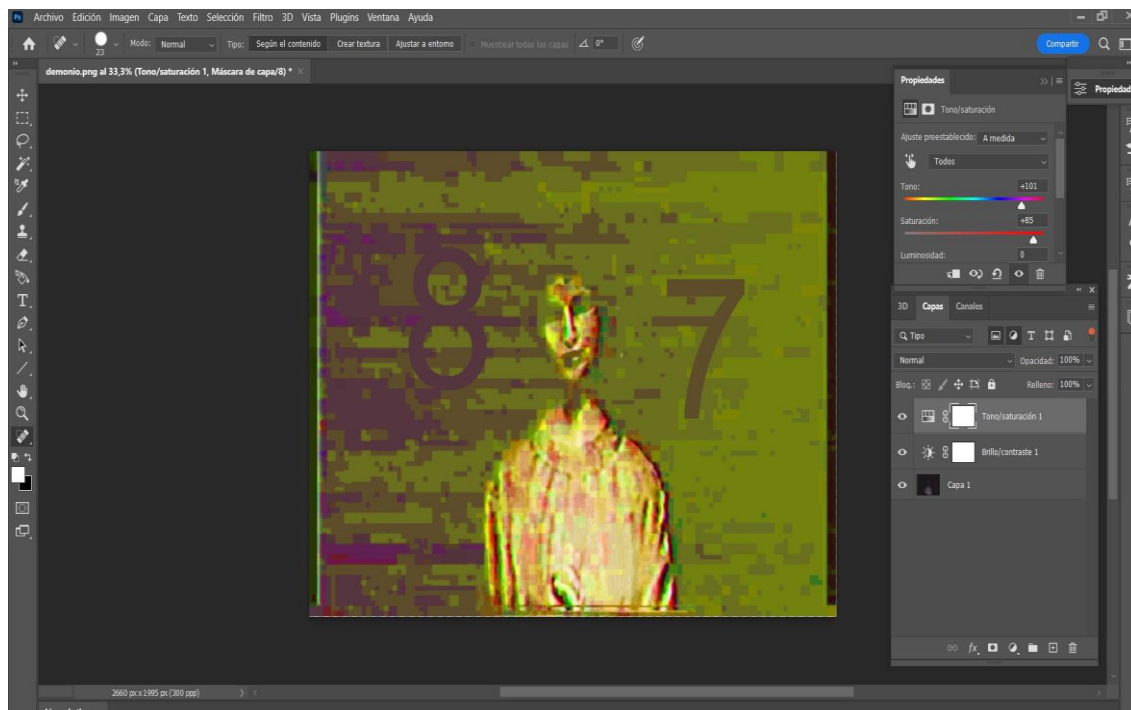
```
formidulosus: Bloc de notas
Archivo Edición Formato Ver Ayuda
daemoni 1
^moriar 2
^amicus 3
^non 4
^meus 5
^dilectus 6
^^
```

Según el orden establecido por los números asociados a los nombres de las imágenes en el archivo "arca.zip", se procedió a unir las diferentes imágenes utilizando un editor de imágenes, en este caso, Adobe Illustrator (<https://www.adobe.com/es/products/illustrator>).

Las imágenes se organizaron según el orden establecido por los números descubiertos:



Anteriormente, se descubrió una pista que indicaba: "El arma contra los demonios es el brillo". Para cambiar los valores de brillo en las imágenes y buscar información oculta se hizo uso de Adobe Photoshop (<https://www.adobe.com/es/products/photoshop.html>).



Durante la manipulación de la imagen, se identificó el número 87. Este número estaba relacionado con el archivo "iter.txt" y un código asociado.

```
84 - kWQyeQhVYPSzuXB1PzSm35b0KKzRitDBk
85 - W6BpYtfZG9QKuKMwYZXv140zdGL7YvRKC
86 - 1HTAADtTN1SUvNRzLnuPK2Zz3cJ3K3xDy
87 - 18x1sWhSvuTssA8vp_hwhH61KIag6MX_5
88 - k2r56AgA3wqbG1zmky7aZX6DJy5893BMS
89 - 4477H4n8iVh9VfVCCJW7F2F0BCN9iKpHg
90 - SXUUVK14fyzBfjSwWmkRPrixSquAveFSP
91 - TgmmW1MzUpS7fPdtYiyv3hUXV1Y4UPm8L
92 - WKNVhSHiPY50X7z3tUrrNEPKr9a5rdfR3
```

Se intentó acceder al enlace generado por el número 87 en el navegador ("18x1sWhSvuTssA8vp_hwhH61KIag6MX_5"). Sin embargo, esto llevó a una página no existente.

Durante los pasos, nos habíamos olvidado de una pista esencial "z.txt", contenida en el archivo ZIP "arca.zip".

```
z: Bloc de notas
Archivo Edición Formato Ver Ayuda
El número de la bestia oculta el mensaje final.
```

“El numero de la bestia oculta el mensaje final”. En la mayoría de los manuscritos del Nuevo Testamento y en las traducciones al español de la Biblia, el número de la Bestia es el 666. Gracias a esa pista se determinó que el enlace del premio final estaba cifrado según el código César con un factor de 666.

Se utilizó un decodificador César con factor 666 para descifrar el enlace y obtener la ubicación del premio final.



The image shows a web-based Caesar cipher decoder interface. At the top, under the heading "Cambio:", there is a text input field containing the number "666". Below this, there are two tabs: "Texto:" (selected) and "Cifrado César:". Under the "Texto:" tab, a large text area contains the encoded string "18h1cGrCfeDccK8fz_rgrR61USkq6WH_5". Under the "Cifrado César:" tab, a large text area contains the decoded string "18x1sWhSvuTssA8vp_hwhH61Klag6MX_5".

Obteniendo así el enlace del premio final ((18x1sWhSvuTssA8vp_hwhH61Klag6MX_5):
https://drive.google.com/file/d/18h1cGrCfeDccK8fz_rgrR61USkq6WH_5/view

