

# Documentación CTF






Estado inicial del reto.....	2
Primer paso: README.txt.....	2
Segundo paso: pista.bmp y video.mp4.....	4
Tercer paso: script.exe.....	5
Cuarto paso: mensaje.pcap.....	6
Quinto paso y final: OSINT.....	6
Bonus: caminos alternativos.....	7
Conclusiones.....	8

El reto Capture The Flag que se adjunta con este documento se ha realizado para afianzar conocimientos de esteganografía (ocultación de mensajes u objetos), criptografía (cifrado) y técnicas de OSINT (Open Source INTelligence).

Como bonus, la práctica se puede resolver mediante técnicas de ingeniería inversa de manera opcional, para aquellos participantes que quieran tomar un atajo en su resolución.

## Estado inicial del reto

El estado inicial del CTF cuenta con los siguiente archivos:

 pista.bmp	19/10/2024 19:16	Archivo BMP	1.201 KB
 premio.7z	19/10/2024 19:19	Archivo WinRAR	3.796 KB
 README.txt	23/10/2024 19:36	Documento de te...	1 KB
 script.exe	19/10/2024 20:21	Aplicación	11.559 KB
 video.mp4	19/10/2024 20:11	Archivo MP4	44.367 KB

## Primer paso: README.txt

Lo primero que debe hacer el participante es leer el archivo README.txt. Para ello, necesitará desenscriptar el texto que contiene haciendo uso de [rot13.com](https://rot13.com)

# rot13.com

[About ROT13](#)

```
vatravreín vairefn.  
Cnen pbzramne, gvrarf n gh qvfcbfvpvóa ybf nepuvibf cvfgn.ozc, cerzvb.7m,  
ivqrb.zc4 l fpevcg.rkr (Clguba), nqrzáf qr rfgr ERNQZR.  
Ry bowrgvib svany rf pbaftrhve yn pbagenfrñn qr cerzvb.7m, yn phny rf han  
cnynoen qr 12 pnenpgrerf.  
  
Cnen ryyb, qroreáf qrfphoeve ry abzoer qry crefbanwr snzbfb zrqvnagr cvfgn.ozc l  
ivqrb.zc4, l cbare fh srpun qr anpvzvragb (qq/zz/1111) ra ry fpevcg.rkr.  
Fv yn srpun rf pbeerpgn, erpvoveáf ha nepuvib pba rkgrafvóa cpnc. Chrgf noeve  
ry nepuvib pba Jverfunex cnen rapbagene yn cvfgn svany dhr gr yyrineá ny cerzvb.  
¡Ohran fhregr!
```



ROT13 ▼



```
¡Bienvenido al reto CTF!  
Para resolver este reto tendrás que utilizar técnicas de criptografía,  
esteganografía y OSINT. Opcionalmente también puedes resolverlo mediante  
ingeniería inversa.  
Para comenzar, tienes a tu disposición los archivos pista.bmp, premio.7z,  
video.mp4 y script.exe (Python), además de este README.  
El objetivo final es conseguir la contraseña de premio.7z, la cual es una  
palabra de 12 caracteres.  
  
Para ello, deberás descubrir el nombre del personaje famoso mediante pista.bmp y  
video.mp4, y poner su fecha de nacimiento (dd/mm/yyyy) en el script.exe.  
Si la fecha es correcta, recibirás un archivo con extensión pcap. Puedes abrir
```

El mensaje descryptado es el siguiente:

*¡Bienvenido al reto CTF!*

*Para resolver este reto tendrás que utilizar técnicas de criptografía, esteganografía y OSINT. Opcionalmente también puedes resolverlo mediante ingeniería inversa.*

*Para comenzar, tienes a tu disposición los archivos pista.bmp, premio.7z, video.mp4 y script.exe (Python), además de este README.*

*El objetivo final es conseguir la contraseña de premio.7z, la cual es una palabra de 12 caracteres.*

*Para ello, deberás descubrir el nombre del personaje famoso mediante pista.bmp y video.mp4, y poner su fecha de nacimiento (dd/mm/yyyy) en el script.exe.*

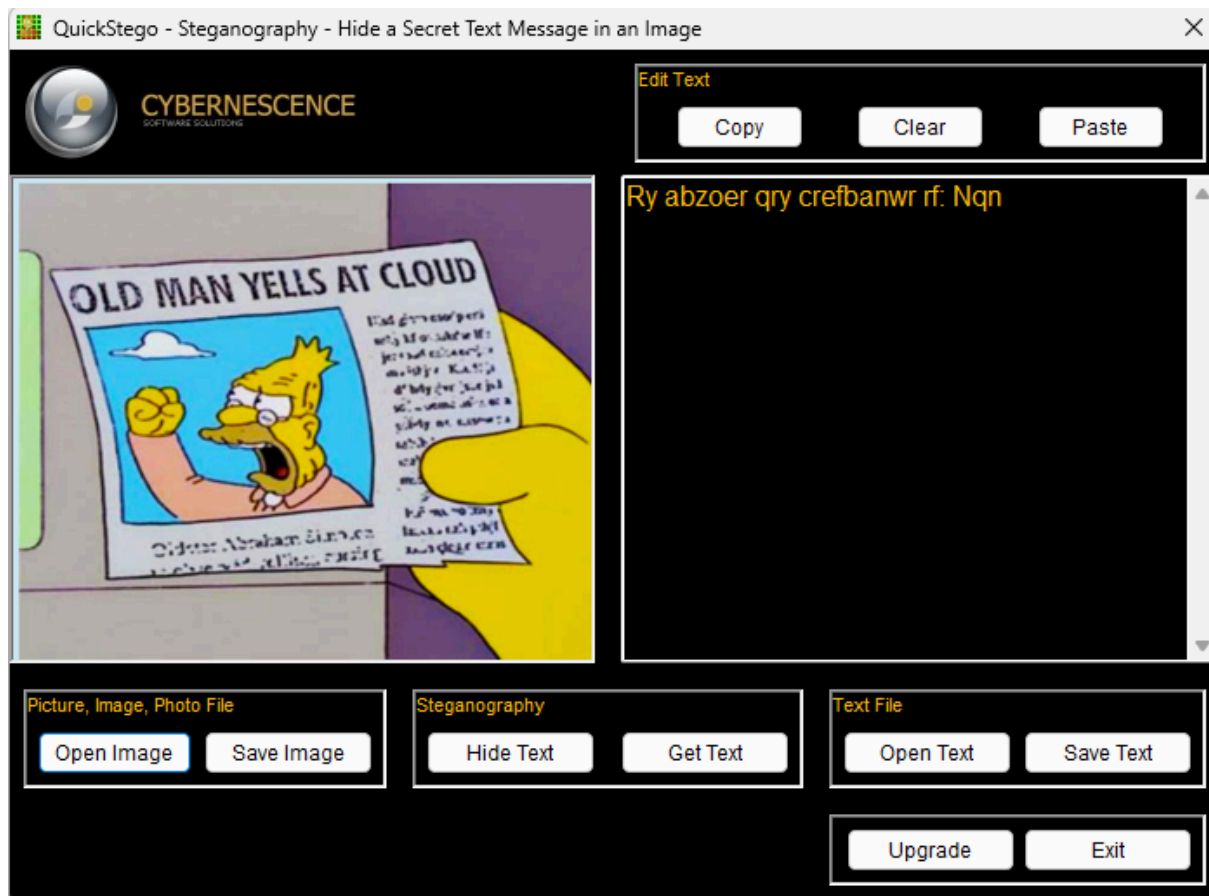
*Si la fecha es correcta, recibirás un archivo con extensión pcap. Puedes abrir el archivo con Wireshark para encontrar la pista final que te llevará al premio.*

¡Buena suerte!”

El texto contiene suficientes explicaciones para resolver todo el reto si se hace uso de las herramientas adecuadas.

## Segundo paso: pista.bmp y video.mp4

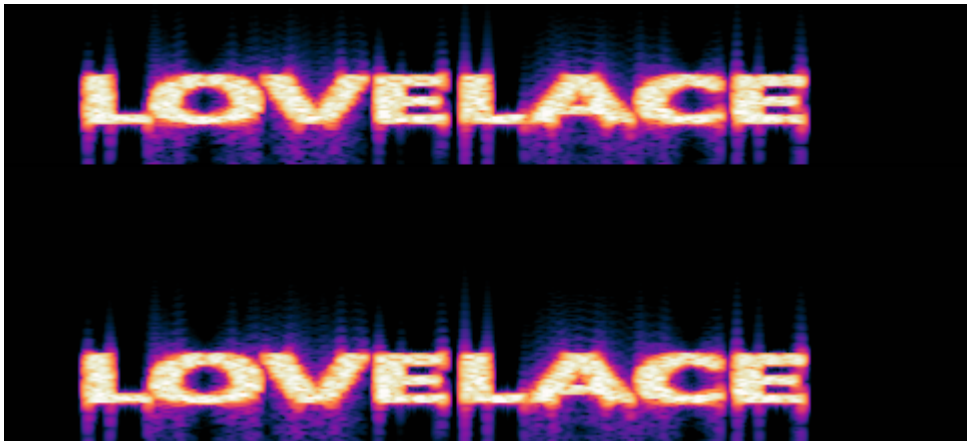
Lo siguiente a realizar es conseguir el nombre del personaje famoso mediante esteganografía. Para ello, la imagen pista.bmp debe ser analizada con Quick Stego, encontrando un texto encriptado:



Dicho texto, una vez desencriptado con la misma herramienta del paso 1, nos da el siguiente mensaje:

*“El nombre del personaje es: Ada”*

Aún necesitamos una pista más para resolver este segundo paso. Para ello, debemos separar el audio del video.mp4, el cual al revisar en el espectrograma de Audacity, nos da el apellido de nuestro personaje:



Así descubrimos el nombre completo del personaje: Ada Lovelace.

## Tercer paso: script.exe

El archivo script.exe ha sido generado con python, y pide una fecha de nacimiento en el formato dd/mm/yyyy para obtener acceso a un archivo pcap.

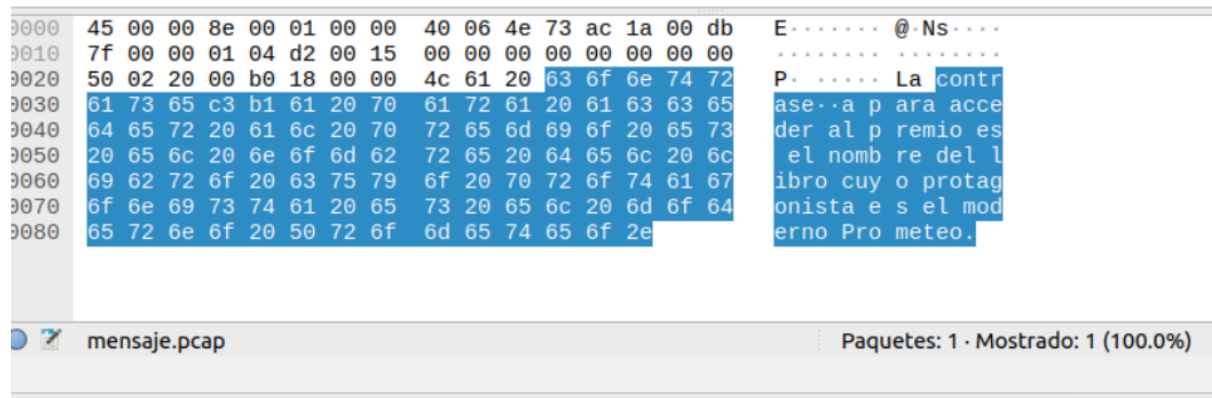
Para ello, tenemos que utilizar técnicas OSINT para obtener la fecha de nacimiento de Ada Lovelace. En este caso basta con una búsqueda en wikipedia para saber que la fecha es 10/12/1815.

```
C:\Users\Jorge Carrasco\Desktop X + v
WARNING: WinPcap is now deprecated (not maintained). Please use Npcap instead
Introduce la fecha (dd/mm/yyyy): 10/12/1815
Acceso autorizado
Dando acceso al archivo pcap. Dentro encontrarás la contraseña del premio.
Pulsa enter para salir
```

Una vez introducida, podemos analizar el archivo pcap.

## Cuarto paso: mensaje.pcap

El archivo pcap contiene la captura de unos datos enviados por la red. En este caso, al abrir el archivo con Wireshark, podemos ver el siguiente mensaje:



*“La contraseña para acceder al premio es el nombre del libro cuyo protagonista es el moderno Prometeo”*

## Quinto paso y final: OSINT

Por último, haciendo uso una vez más de técnicas OSINT, podemos averiguar que el nombre del libro es Frankenstein.

Al introducir dicha contraseña al descomprimir el zip, obtenemos acceso a nuestro premio.



## Bonus: caminos alternativos

Hay varios atajos que pueden ser utilizados para resolver el reto, algunos concretamente destinados a participantes más experimentados.

El archivo pcap puede ser abierto mediante un editor de texto, dando la misma información que si lo abrimos desde Wireshark.

El archivo script.exe, como alternativa, puede ser resuelto con técnicas de ingeniería inversa. Para ello, tenemos que utilizar la herramienta PyInstaller Extractor (<https://github.com/extremecoders-re/pyinstxtractor>) para extraer el bytecode de Python. Una vez tenemos el bytecode, podemos descompilarlo con uncompyle6 (<https://pypi.org/project/uncompyle6/>) y obtener directamente el mensaje del código de script.py:

```
1 from scapy.all import *
2
3 correct_password = "10/12/1815"
4
5 user_password = input("Introduce la fecha (dd/mm/yyyy): ")
6
7 if(user_password == correct_password):
8     print("Acceso autorizado")
9     print("Dando acceso al archivo pcap. Dentro encontrarás la contraseña del premio.")
10    pkt1 = IP(dst="127.0.0.1")/TCP(sport=1234, dport=21)/"La contraseña para acceder al premio es el nombre del libro cuyo protagonista es el moderno Prometeo."
11    wrpcap("mensaje.pcap", pkt1)
12    input("Pulsa enter para salir")
13 else:
14    print("Acceso no autorizado")
```

## Conclusiones

El CTF adjunto contiene las suficientes pruebas para testar los conocimientos de esteganografía, criptografía y OSINT del participante, además de poder ser resuelto por técnicas de ingeniería inversa para suponer un reto más avanzado para aquellos participantes que quieran intentarlo.