CÁTEDRA DE CIBERSEGURIDAD CIBERUGR, INCIBE-UGR

Nombre	Protected File
Categoría	MISC (CRIPTO + FORENSE)
Dificultad	MEDIA
Puntos	300

DESCRIPCIÓN DEL RETO

Un cliente nos ha enviado un archivo protegido con contraseña, pero no nos han proporcionado la clave para ver el contenido de este. ¿Serás capaz de recuperar el contenido que se encuentra dentro del archivo?

WRITEUP

1. Inicialmente, al leer la descripción del reto se nos proporciona un fichero adjunto. Este fichero se trata de un zip con contraseña.
2. Para ello, vamos a intentar conseguir la contraseña a través de ataques de fuerza bruta, usando "zip2john" para sacar el hash del zip y "john" para crackearlo.
3. Sacamos el hash del zip usando zip2john.

zip2john Protected_File.zip > hash.txt

```
└$ zip2john Protected_File.zip > hash.txt
ver 2.0 efh 5455 efh 7875 Protected_File.zip/file_transfer_protoco
l.pcapng PKZIP Encr: TS_chk, cmplen=43574, decmplen=115656, crc=17
25AD31 ts=5A2B cs=5a2b type=8
```

4. Usamos la herramienta "John the Ripper" y el diccionario "rockyou.txt" para crackear la contraseña de este zip.

john hash.txt –wordlist=/usr/share/wordlists/rockyou.txt

```
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
!!!secret!!!     (Protected_File.zip/file_transfer_protocol.pcapng
)
1g 0:00:00:00 DONE (2024-04-24 17:35) 1.923g/s 27583Kp/s 27583Kc/s
 27583KC/s "2parrow"..*7¡Vamos!
Use the "--show" option to display all of the cracked passwords re
liably
Session completed.
```

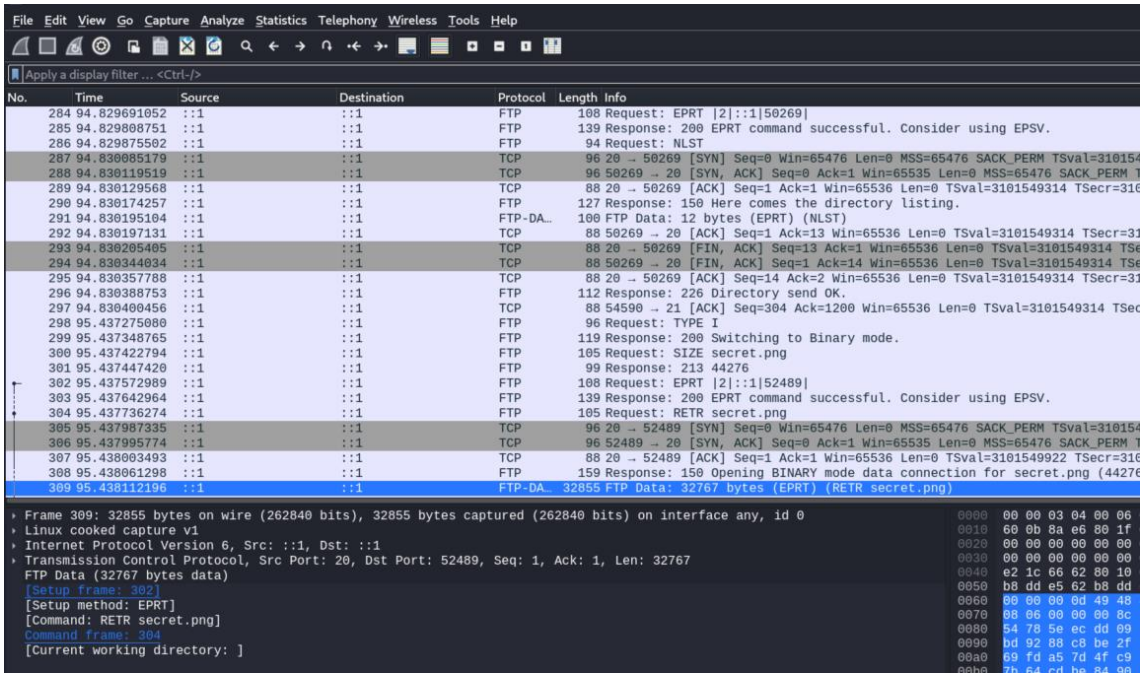
5. Ahora que tenemos la contraseña "**!!!secret!!!**" vamos a descomprimir el archivo. **NOTA**: Es necesario escapar los caracteres especiales como en este caso son todas las exclamaciones.

---

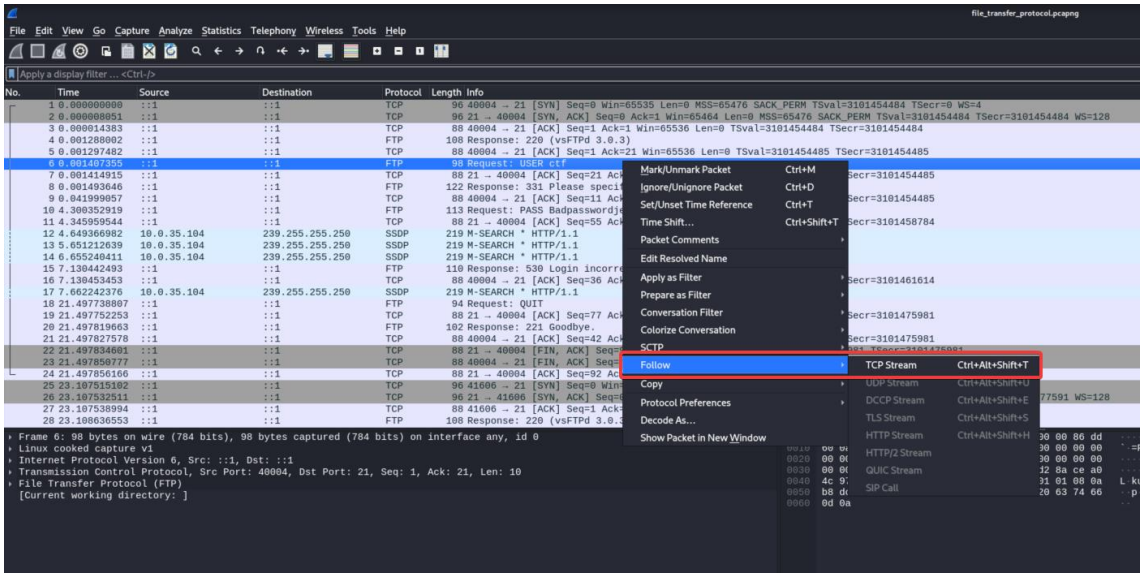
unzip -P \!\!\!secret\!\!\! Protected_File.zip

```
└─$ unzip -P \!\!\!secret\!\!\! Protected_File.zip
Archive:  Protected_File.zip
  inflating: file_transfer_protocol.pcapng
```

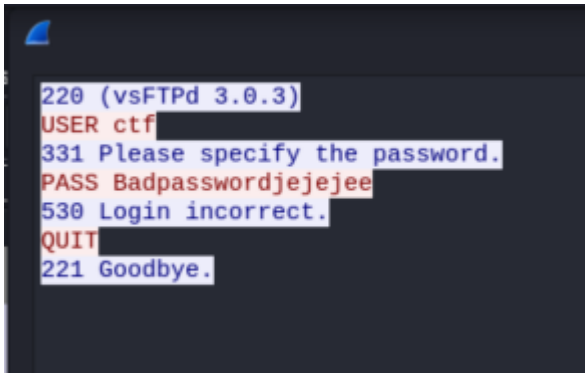
6. Una vez hemos descomprimido el zip, vamos a ver qué es lo que contiene dentro.
7. En este caso vemos un archivo pcap, el cual se trata de una captura de tráfico.
8. Abrimos el pcap usando "Wireshark".



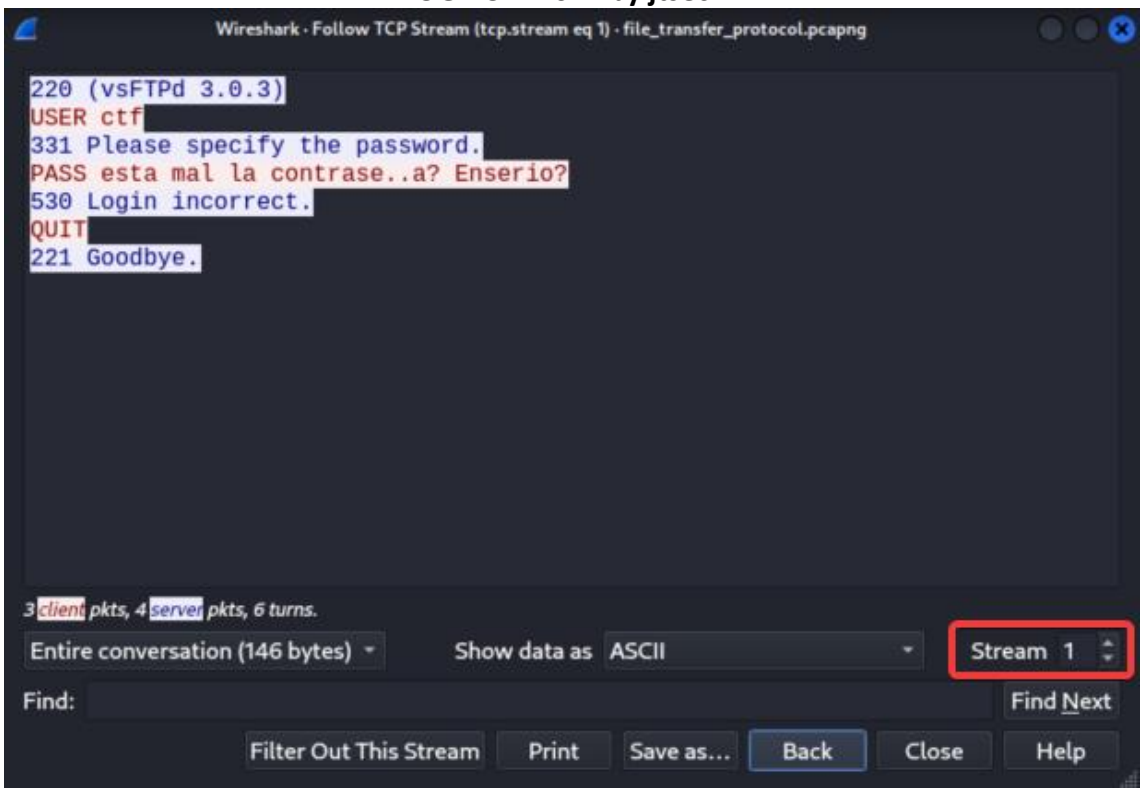
9. Al abrir la captura de tráfico, se ve bastante tráfico FTP, por lo tanto, es necesario hacerle un análisis para identificar que es lo que está pasando en esta comunicación. **NOTA**: Para analizarlo, podemos seguir el flujo TCP.



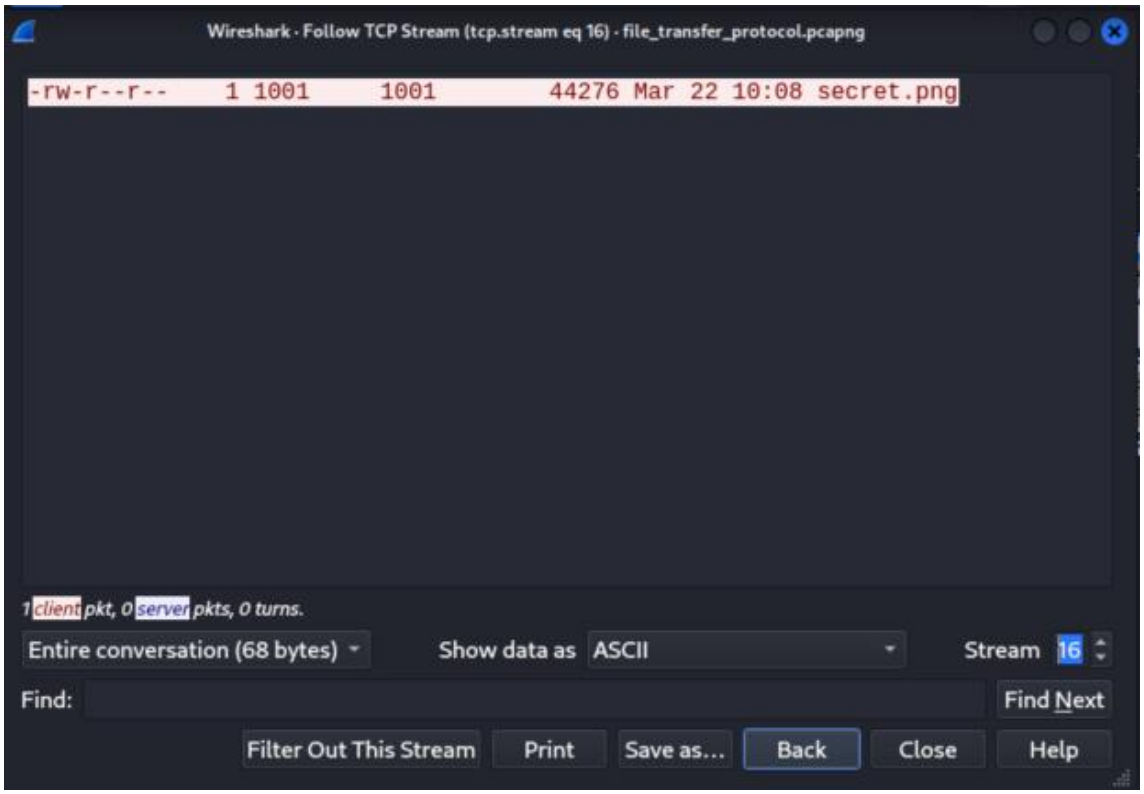
10. En el primer paquete, se ve como el usuario “ctf” se ha intentado autenticar con una contraseña invalida.



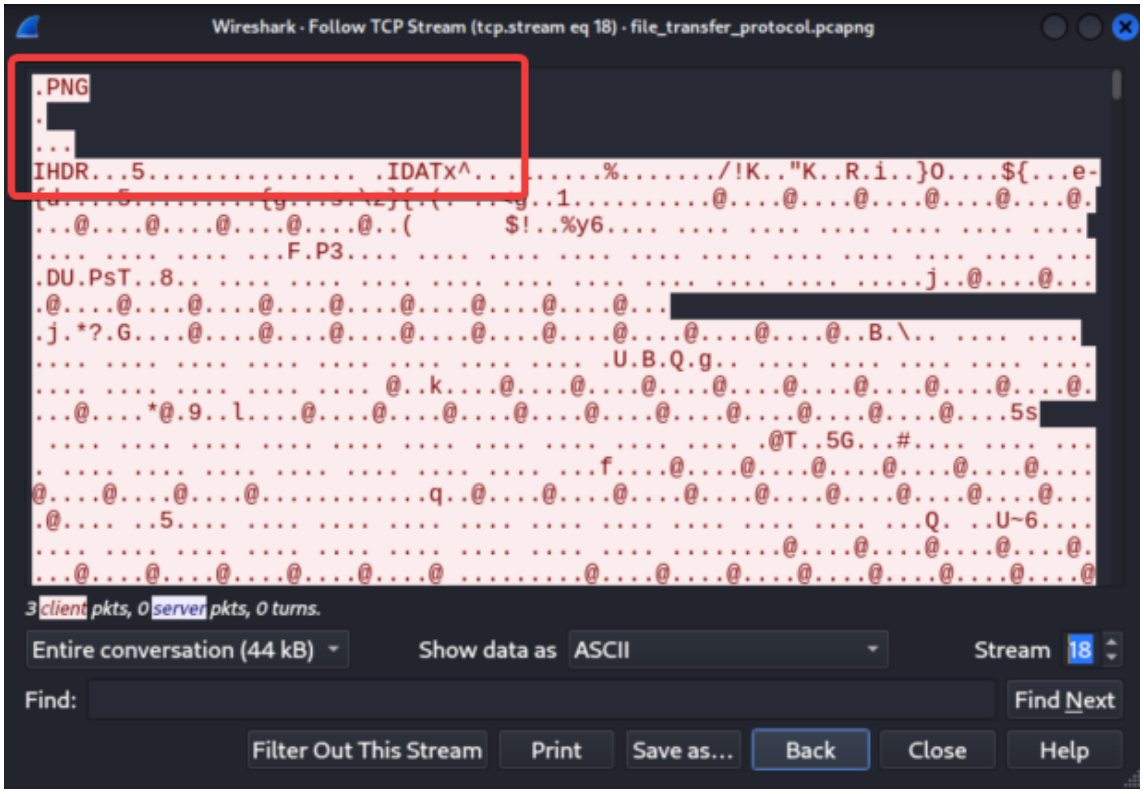
11. Para seguir viendo las comunicaciones podemos ir aumentando el valor de “stream”.



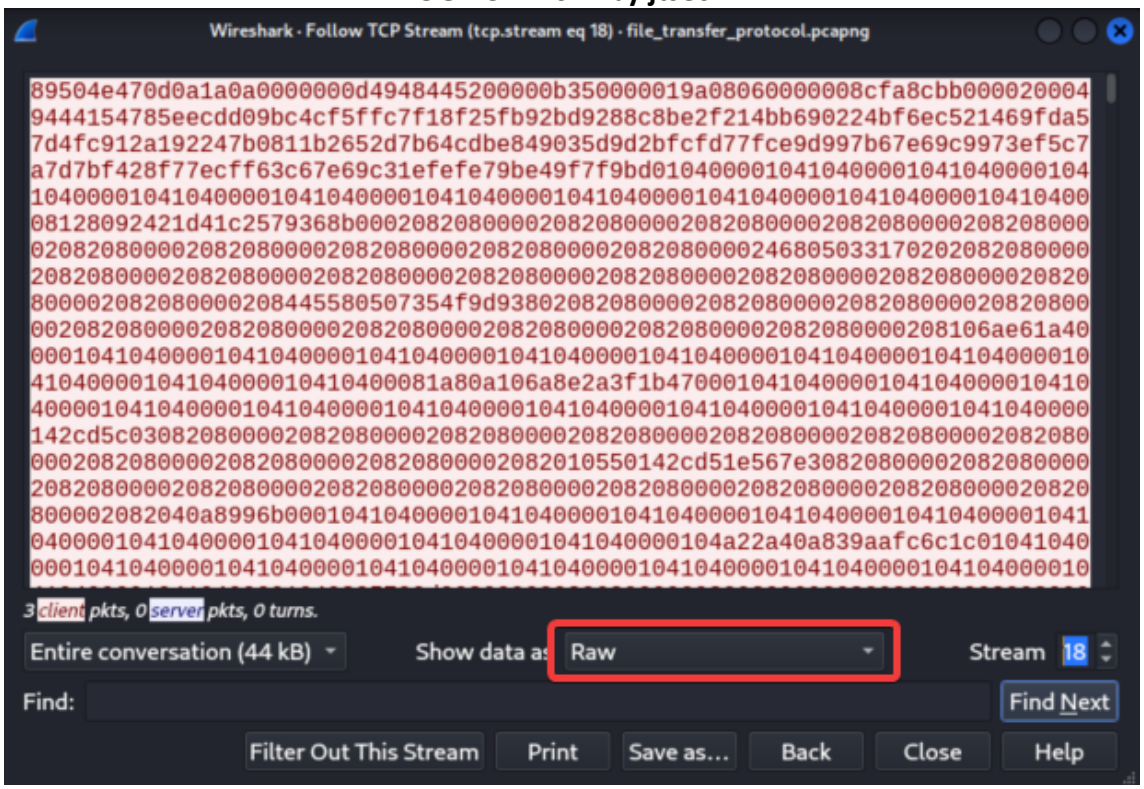
12. En el flujo 16 podemos observar como el usuario ha listado un directorio en el que se encuentra un PNG con el nombre de secret.png.



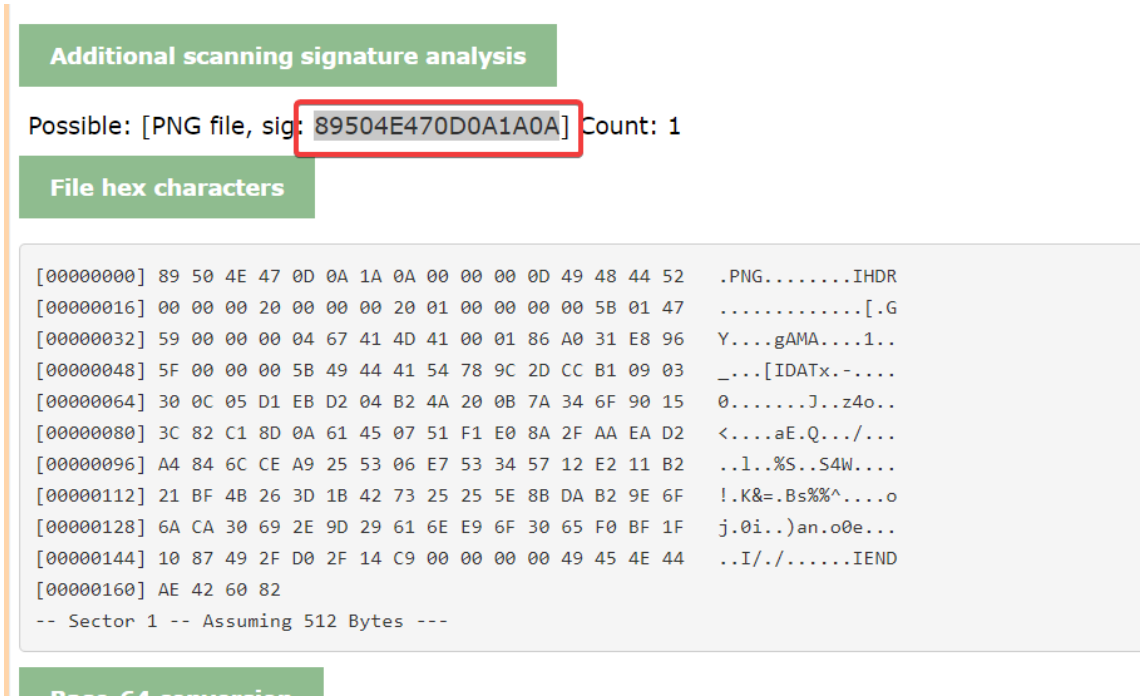
13. Si seguimos aumentando el “stream” hasta el número 18, se puede observar la estructura de un PNG, el cual tiene todo el sentido que sea el PNG que se ha listado anteriormente, secret.png.



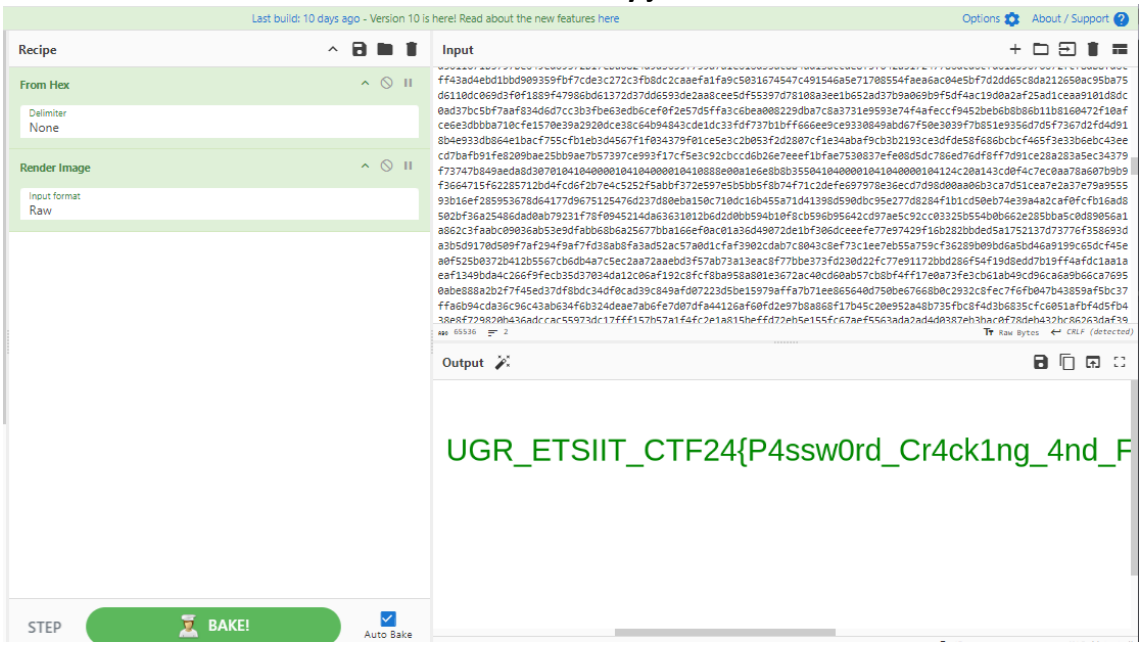
14. Pasamos el contenido de este paquete a raw, para ver si los *magic bytes* coinciden con los de un PNG.



15. Comparamos los primeros bytes de la imagen con los *magic bytes* de un PNG, en este caso coinciden, por lo que ya podemos asumir que esto es un PNG.



16. Por último, podemos ver la imagen usando CyberChef (https://gchq.github.io/CyberChef/), aplicando el “from Hex” y como sabemos que es una imagen, añadimos el “Render Image”, para finalmente poder visualizar la imagen que contiene la *flag*.



Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
UNIVERSIDAD DE GRANADA