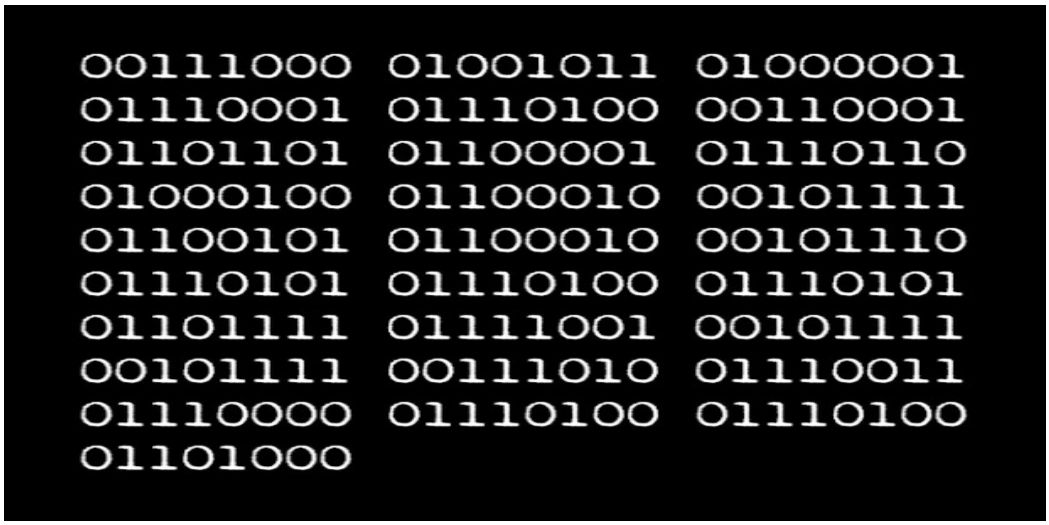
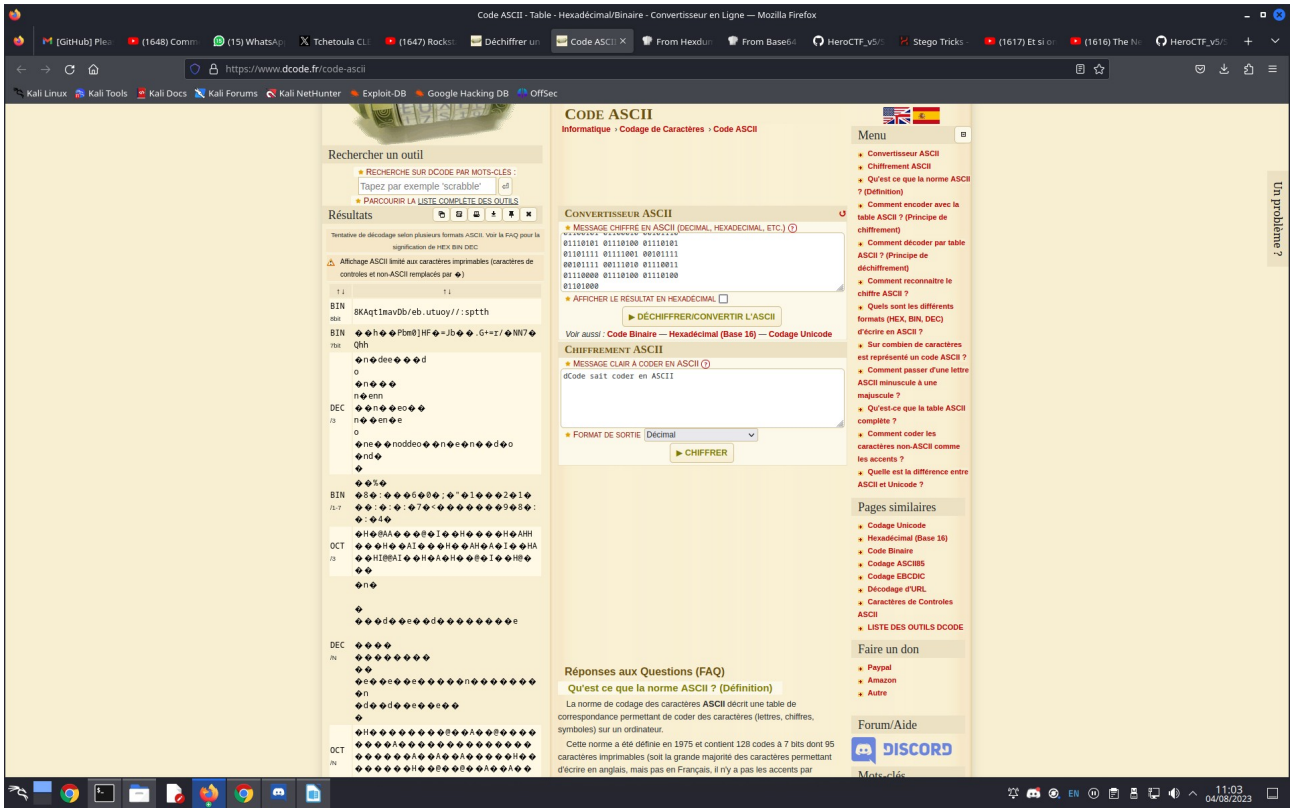
# Writeup

**Challenge:** Hèviosso nou gué
**Auteur:** charliepy
**Mon equipe:** Nekketsu


Pour ce challenge, il a ete mis a notre disposition une video nommee Teaser HACKERLAB 2023. Suite au visionnage de cette video on aperçoit du binaire a 2min30s de la video. Le premier reflexe a ete de dechiffrer ce binaire.



Lorsqu’on essaie de dechiffrer le code ASCII avec decode, on obtient le lien 8KAqt1mavDb/eb.utuoy//:sptth qui est visiblement a l’envers.




Apres traitement donne le lien suivant: https://youtu.be/bDvam1tqAK8.

Ce lien nous a amene sur une video youtube dont le titre etait IRXSA6LPOUQHGZLFEBWWKPY=. Ce titre est chiffre en base 32 ce qui donne « Do you see me? »apres dechiffrement. On comprend donc qu’on nous demande si on voit ce qui est dans la video.

Grace au challenge Subliminal du HeroCTF_v5 qu’on avait eu a fait, on a vite compris qu’il y a avait une image cachee dans la video. La vidéo est divisée en images et chaque image contient une partie de 20x20 pixels de l'image du message. Pour récupérer le message , nous devons inverser le processus.  Nous avions donc utilise le code ci-dessous pour le faire.

```python
import cv2
import numpy as np

def retrieve_image(video_path, output_path):
    video = cv2.VideoCapture(video_path)
    width = int(video.get(3))
    height = int(video.get(4))

    image = np.zeros((height, width, 3), np.uint8)

    i = 0
    while True:

        ret, frame = video.read()
        if not ret:
            break


        x = i % (width // 20) * 20
        y = i // (width // 20) * 20
        image[y:y+20, x:x+20] = frame[y:y+20, x:x+20]
        i += 1

    cv2.imwrite(output_path, image)
    video.release()


retrieve_image('IRXSA6LPOUQHGZLFEBWWKPY=.mp4','output_flag.png')

```

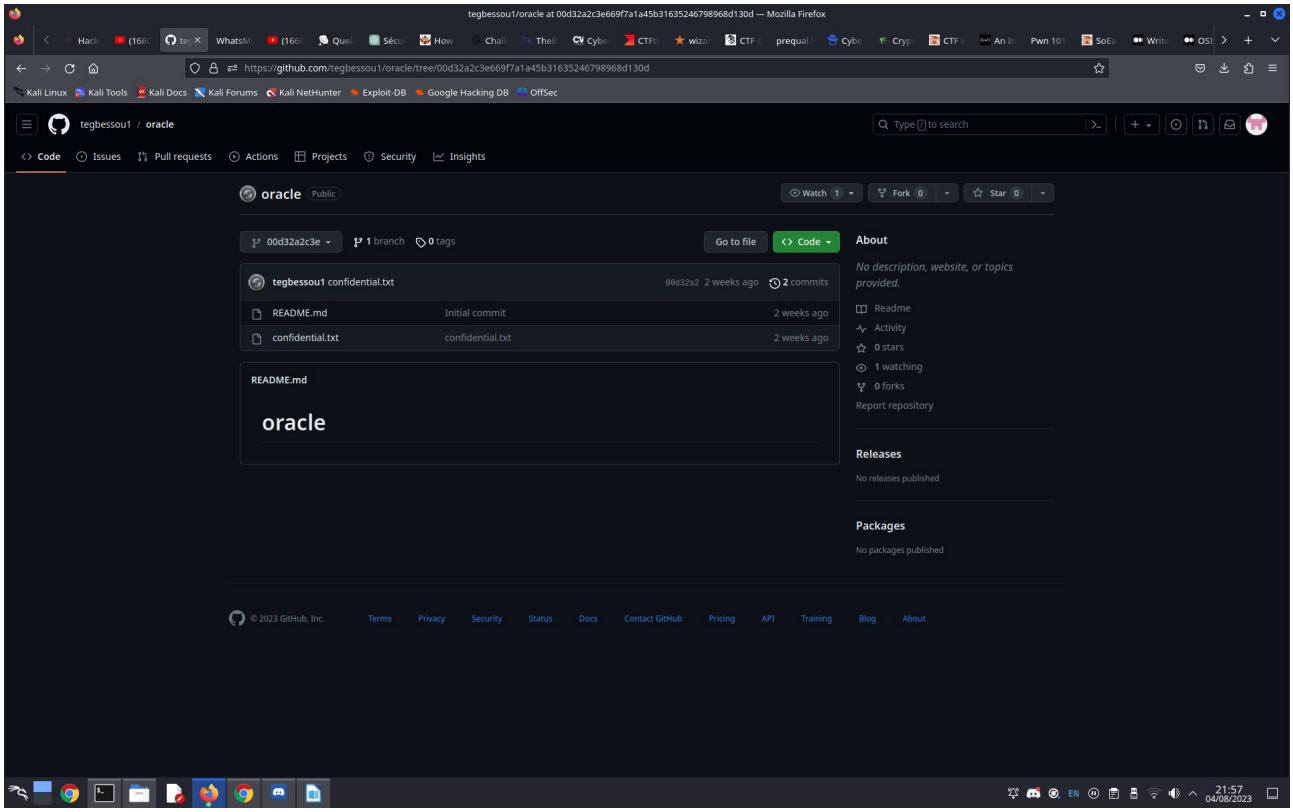
On obtient finalement l’image ci-dessous:


Lorsqu’on dechiffre ce qu’on a on obient AuthorÒ @tegbessou1. On a donc compris qu’il s’agissait d’un username et qu’il nous fallait faire de l’OSINT avec @tegbessou1.

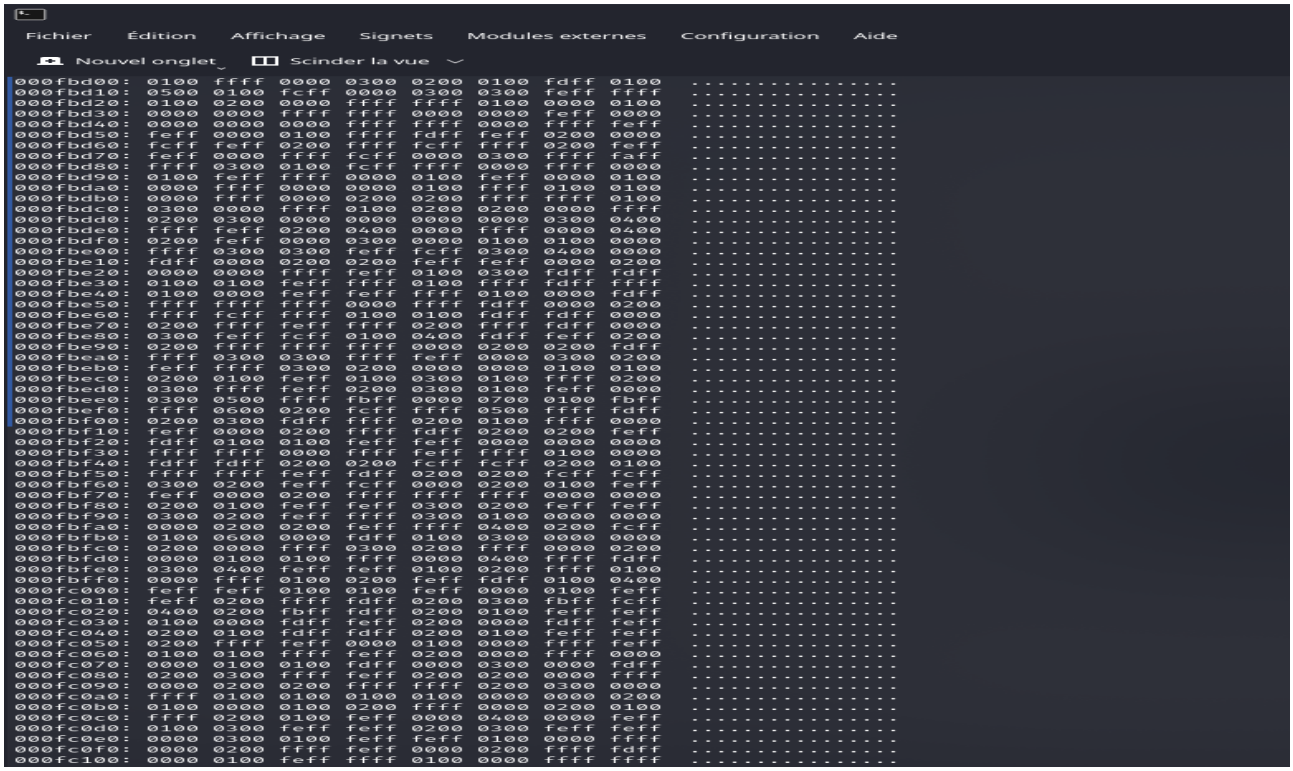
Nous avions donc utilise le puissant outil Sherlock pour trouver la liste des comptes utilisant tegbessou1 sur les reseaux sociaux.

```
┌──([redacted])-[~/sherlock]
└─$ python3 sherlock tegbessou1
[*] Checking username tegbessou1 on:

[+] CNET: https://www.cnet.com/profiles/tegbessou1/
[+] Enjin: https://www.enjin.com/profile/tegbessou1
[+] G2G: https://www.g2g.com/tegbessou1
[+] GitHub: https://www.github.com/tegbessou1
[+] GunsAndAmmo: https://forums.gunsandammo.com/profile/tegbessou1
[+] IRL: https://www.irl.com/tegbessou1
[+] Quizlet: https://quizlet.com/tegbessou1
[+] Speedrun.com: https://speedrun.com/user/tegbessou1
[+] Twitch: https://www.twitch.tv/tegbessou1
[+] Twitter: https://twitter.com/tegbessou1
[+] Venmo: https://account.venmo.com/u/tegbessou1
[+] ebio.gg: https://ebio.gg/tegbessou1

[*] Search completed with 12 results
```

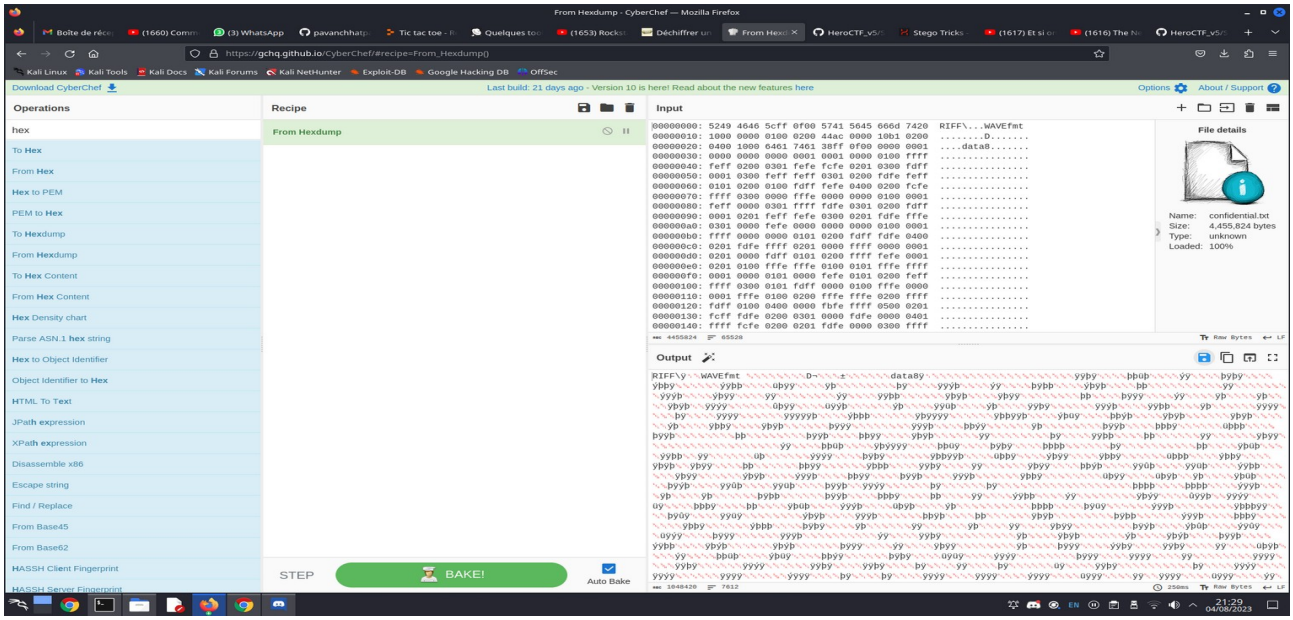
Un tour sur github nous a permis de constater que le compte a joint github il y a de cela 3 semaines, ce qui a attire notre attention.




On a donc clone le repo nomme oracle qui est d'ailleurs le seul sur ce compte. Apres clonnage on a constate qu'il y avait un fichier nomme confidentiel.txt. Un cat sur ce fichier nous a donc permis de dire qu'il s'agissait d'un fichier audio en se basant aussi sur le nom  du repositorie qui est oracle.



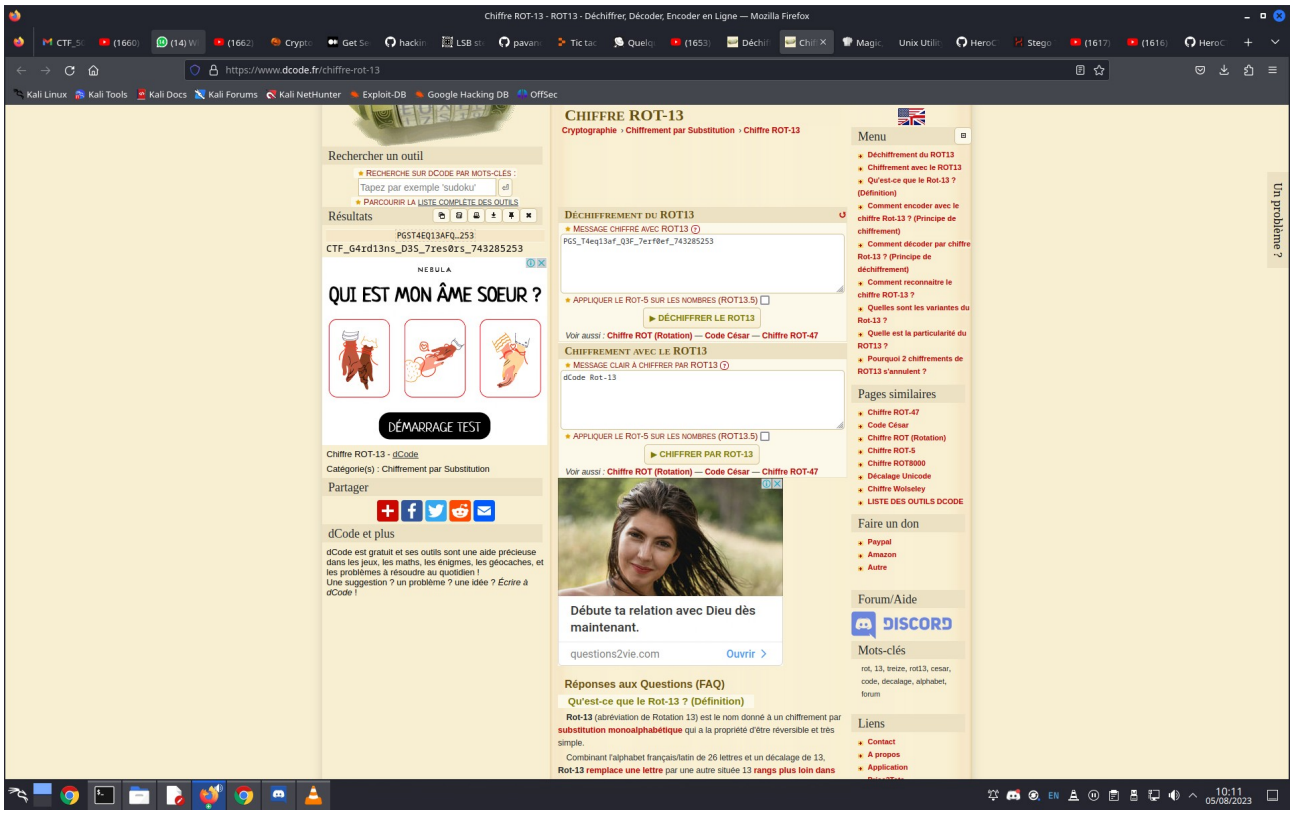

Lorqu'on regarde l'entete du fichier on constate qu'il s'agit en fait d'un fichier wav (**RIFF???? WAVE**) .
Cependant un wavSteg sur le fichier nous donne une erreur. L'erreur disait que l'entete RIFF n'est pas retrouve. Apres quelques heures de reflexions on a donc compris qu'il faillait dechiffrer le fichier de l'hexdump.



Avec cyberchef nous avions pu avoir le bon fichier wav en dechiffrant le contenu du fichier confidentiel.txt depuis l'hexdump. Lorqu'on ecoute le fichier wav on entend une sorte de sonnerie. Nous avions donc utilise l'outil Stegolsb pour voir si l'on pouvait extraire des donnees du fichier wav.

```
┌──(gojo㉿kali)-[~/Téléchargements/oracle-00d32a2c3e669f7a1a45b31635246798968d130d]
└─$ stegolsb wavsteg -r -i download1.wav -o output.txt -n 1 -b 1000
Files read                    in 0.00s
Recovered 1000 bytes          in 0.00s
Written output file           in 0.00s

┌──(gojo㉿kali)-[~/Téléchargements/oracle-00d32a2c3e669f7a1a45b31635246798968d130d]
└─$
```

On a constate que le fichier contenant un message qui disait «Find my e-mail address and send me a message with the TIC-TAC-TOE challenge answer in the subject line.»
On a donc cherché le mail associé au compte github tegbessou1. Ce mail était «th3t0ul41960@gmail.com».
Comme le message le demandait, nous avions envoyé la reponse du challenge Tic-Tac-Toe au mail et nous avions en retour recu un mail contenant le flag mais chiffré en Rot-13 que nous avions décodé avec decode.




# Flag: CTF_G4rd13ns_D3S_7res0rs_743285253