Correction du challenge 052 Stegseek

Pour rappel :
Voici les commandes à effectuer lors de la configuration

```
ubuntu@ubuntuVM:~/Documents/Projet/challenge_stegseek$ docker-compose build
challenge_052-syd-academy-stegseek uses an image, skipping
ubuntu@ubuntuVM:~/Documents/Projet/challenge_stegseek$ docker-compose up -d
Creating challenge_052-syd-academy-stegseek ... done
ubuntu@ubuntuVM:~/Documents/Projet/challenge_stegseek$ docker exec -ti challenge_052-syd-academy-stegseek /bin/bash
root@de57dfbeefdb:/home/Stegseek#
```

```
root@31f1da5712c1:/home/Stegseek# apt install ./stegseek_0.6-1.deb
```

Le challenge se déroule en 9 étapes :

1. Lister les fichiers présents dans le répertoire courant

```
root@de1959ee07ae:/home/Stegseek# ls
audio.wav  image.jpg  image2.jpg  stegseek_0.6-1.deb  worldlist.txt
```

On remarque que ce répertoire contient :
- 3 fichiers steghide (2 images et un audio)
- une worldlist contenant un grand nombre de mot de passe commun
- fichier d'installation de stegseek

2. On utilise stegseek sur l'image1 à l'aide de la worldlist pour récupérer les données cachées.

```
root@de57dfbeefdb:/home/Stegseek# stegseek image.jpg worldlist.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "optic"

[i] Original filename: "message.txt".
[i] Extracting to "image.jpg.out".
root@de57dfbeefdb:/home/Stegseek#
```

3. On affiche les données cachées

```
root@de57dfbeefdb:/home/Stegseek# cat image.jpg.out
Ne plus rien attendre en retour
Et pourtant t'aimer pour toujours

Merci pour me l'avoir fait découvrir

On peut penseer que le temps et la distance
Unient permettent de changer le présent en souvenir
Bienvenue dans mon âme, ce n'est pas ce que j'en pense
L'amour est un sentiment sans frontière ni durée
Il ne faut pas m'en vouloir, je veux simplement t'aimer
Et pour cela je n'ai besoin de rien

Pas même ta présence, puisque tu ne peux plus me voir
Alors simplement lis moi et écoute moi sans fin
Si tu pouvais ne rien me donner mais accepter de recevoir

Je voudrais que tu me comprennes

Et malgré tout ce qui s'est passé, que
X est l'inconnu de l'équation, toi plus moi même
Il faut que découvres que le résultat
Si même tu te protèges, que
Tout ce qui ne tues pas rend plus fort
Encore plus qu'avant, car mes sentiments n'ont pas de limites.
```

4. On utilise stegseek sur l'image2 à l'aide de la worldlist

```
root@de57dfbeefdb:/home/Stegseek# stegseek image2.jpg worldlist.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Progress: 99.27% (132.5 MB)
[!] error: Could not find a valid passphrase.
```

On remarque que le mot de passe ne figure pas dans la worldlist → il semble complexe.

5. OPTIONNELLE : on veut obtenir quelques informations supplémentaires

```
root@de57dfbeefdb:/home/Stegseek# stegseek --seed image2.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Progress: 52.22% (2242655000 seeds)
i] Found (possible) seed: "e2b605a8"
        Plain size: 738.0 Byte(s) (compressed)
        Encryption Algorithm: rijndael-128
        Encryption Mode:      cbc
```

6. On utilise une seconde commande de stegseek en indiquant un mdp précis.

Lorsque l'on regarde correctement le message caché, on remarque que les premières lettres de chaque vers forment un mot : NEMOUBLIEPASJEXISTE.
→ il s'agit du mdp utilisé sur l'image2.

cf Acrostiche

```
root@de57dfbeefdb:/home/Stegseek# cat image.jpg.out
Ne plus rien attendre en retour
Et pourtant t'aimer pour toujours

Merci pour me l'avoir fait découvrir

On peut penseer que le temps et la distance
Unient permettent de changer le présent en souvenir
Bienvenue dans mon âme, ce n'est pas ce que j'en pense
L'amour est un sentiment sans frontière ni durée
Il ne faut pas m'en vouloir, je veux simplement t'aimer
Et pour cela je n'ai besoin de rien

Pas même ta présence, puisque tu ne peux plus me voir
Alors simplement lis moi et écoute moi sans fin
Si tu pouvais ne rien me donner mais accepter de recevoir

Je voudrais que tu me comprennes

Et malgré tout ce qui s'est passé, que
X est l'inconnu de l'équation, toi plus moi même
Il faut que découvres que le résultat
Si même tu te protèges, que
Tout ce qui ne tues pas rend plus fort
Encore plus qu'avant, car mes sentiments n'ont pas de limites.
```

Puis, on lance une autre commande de stegseek permettant de spécifier le mot de passe. Celle-ci permet d'afficher directement dans bash ou invite de commande le message secret caché dans le second fichier.

```
root@de1959ee07ae:/home/Stegseek# stegseek --extract -sf image2.jpg -xf - -p "NEMOUBLIEPASJEXISTE"
########################################################################
Salut XXXX, je viens d'écrire ce magnifique poème, en réponse du tien
########################################################################
Titre : XXX_poeme_version1

Les mots sont des oiseaux qui volent dans le ciel,
Leur chant doux et léger est un appel éternel,
Ils portent nos pensées, nos rêves les plus fous,
Et les transforment en vers, en poèmes en mots doux.

Mais parfois, les mots sont lourds, difficiles à porter,
Et notre plume peine à les couchers sur le papier.
Alors, nous cherchons des astuces, des façons de les dire,
Et c'est là que la base64 peut nous offrir un empire.

Cette méthode de codage, complexe et mystérieuse,
Transforme les mots en chiffres, en une suite harmonieuse.
Et si cela peut sembler ardu, presqu'impossible à déchiffrer,
Cela offre une beauté unique, un langage à explorer.

Ainsi, laissez-vous emporte par la magie des mots,
Et n'ayez pas peur de leur donner des ailes, même en code.
Car chaque lettre, chaque signe, chaque accent,
Peut devenir une oeuvre d'art, un poème fascinant.

Alors prenez votre clavier, et laissez votre créativité s'envoler,
Car avec la base64, les mots peuvent toujours nous étonner.


########################################################################
Ps : il serait préférable de communiquer de façon plus sécurisée.
########################################################################
```

7. On réessaie de récupérer le message caché du dernier fichier steghide (audio) avec la première commande (étape 2)

```
root@de57dfbeefdb:/home/Stegseek# stegseek audio.wav worldlist.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Progress: 98.42% (131.3 MB)
[!] error: Could not find a valid passphrase.
```

8. On regarde correctement le message secret de l'image2.

On remarque une information importante : XXX_poeme_version1
Puis le texte fait allusion à la base64. Peut-être que le mot de passe renseigné dans le fichier audio est codé en base64.

On regarde des tutoriels sur Internet et la commande pour coder un String en base64 est :

```
root@de1959ee07ae:/home/Stegseek# echo -n "XXX_poeme_version1" | base64
WFhYX3BvZW1lX3ZlcnNpb24x
```

9. On utilise la seconde commande de stegseek (étape 6)

```
root@de1959ee07ae:/home/Stegseek# stegseek --extract -sf audio.wav -xf - -p "WFhYX3BvZW1lX3ZlcnNpb24x"
X_STEG{100k$_MISSION_PASSED_;-)}
```

On obtient le flag.