Forensics : Pretty Peculiar Pokemon

Value : 150 Pts

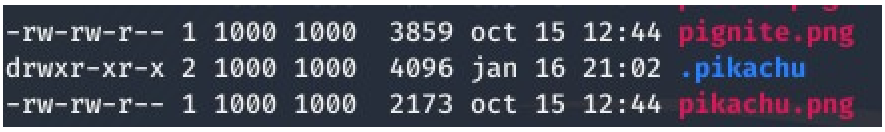
Description : Ash is on his mission to become world's best pokemon master. On his way he finds an amazing pokemon named charlizard, which he intends to catch in his pokeball. But he finds out that the last pokeball he had was missing. Maybe some pokemon took it. Can you help ash to find that hidden pokemon to get his pokeball back?
Here's a file you will need on this mission.
But try to find the perfect path, it can be a "timewaste", i assure you.

Attachment : Challenge.zip

Solution

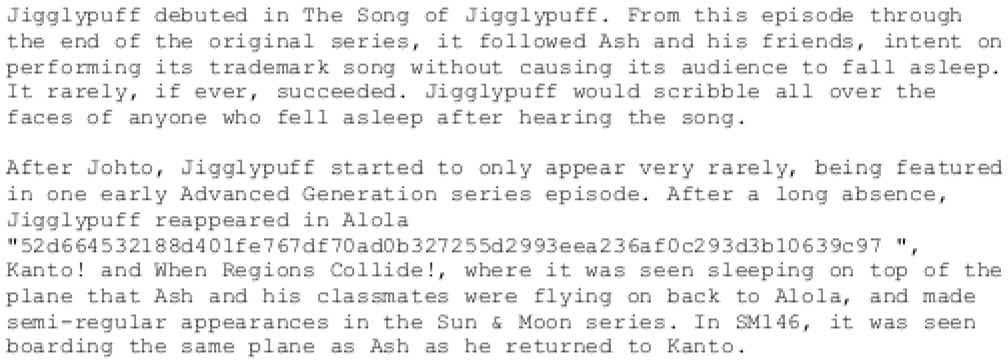
First download the attachment file «**Challenge.zip**» and extract his content. Inside it, we find a directory with many pokemon picture (png and jpg). And we get a pdf password protected «**pokemondata.pdf**».

As said the challenge description «**Try to find the perfect path, it can be a «timewaste»**». So i started to look for hidden folders. Running «ls -la» inside the images folder, and i find a directory called «**.pikachu**» .



```
-rw-rw-r-- 1 1000 1000  3859 oct 15 12:44 pignite.png
drwxr-xr-x 2 1000 1000  4096 jan 16 21:02 .pikachu
-rw-rw-r-- 1 1000 1000  2173 oct 15 12:44 pikachu.png
```

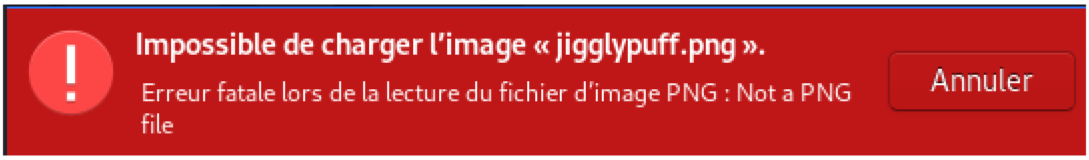
Inside this folder we get a pdf password protected named «may.pdf», guessing the password «**pikachu**» unlocked the pdf and show his content.



```
Jigglypuff debuted in The Song of Jigglypuff. From this episode through
the end of the original series, it followed Ash and his friends, intent on
performing its trademark song without causing its audience to fall asleep.
It rarely, if ever, succeeded. Jigglypuff would scribble all over the
faces of anyone who fell asleep after hearing the song.

After Johto, Jigglypuff started to only appear very rarely, being featured
in one early Advanced Generation series episode. After a long absence,
Jigglypuff reappeared in Alola
"52d664532188d401fe767df70ad0b327255d2993eea236af0c293d3b10639c97 ",
Kanto! and When Regions Collide!, where it was seen sleeping on top of the
plane that Ash and his classmates were flying on back to Alola, and made
semi-regular appearances in the Sun & Moon series. In SM146, it was seen
boarding the same plane as Ash as he returned to Kanto.
```

We get an hash inside this text, but i was unable to decrypt it actually. So i looked at the pokemon image of «**jigglypuff**» and see something strange.



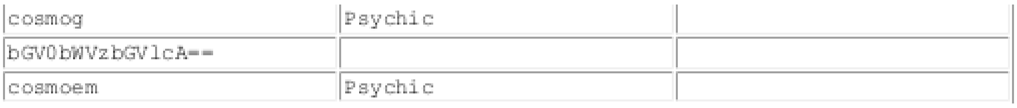
Impossible de charger l'image « jigglypuff.png ».

Erreur fatale lors de la lecture du fichier d'image PNG : Not a PNG file

Trying to open the picture i get an error message who told me its not a «PNG» so i looked the file type with the «**file**» command. Change his extension from «.png» to «.jpg» and i can open the picture. But nothing usefull.

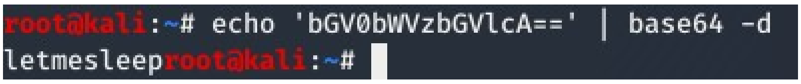
After a lot of time, approximatively 6-8hours on it, i come back to the description, and tried «**timewaste**» as password for the pokemondata.pdf and it worked ! YEAH ! IT WAS REALLY A TIME WASTE !

In the last page of the pdf, we can find a base64 string.



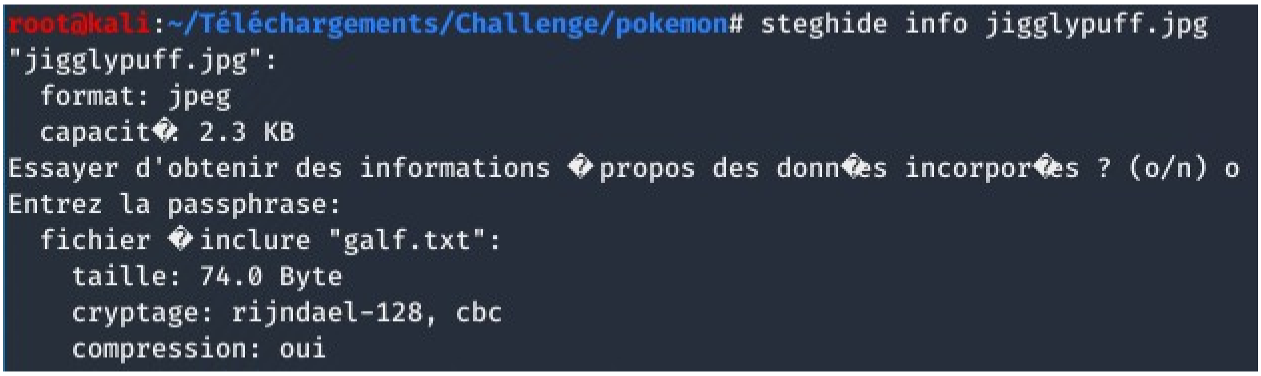
cosmog	Psychic	
bGV0bWVzbGVlcA==		
cosmoem	Psychic	

Decode it.



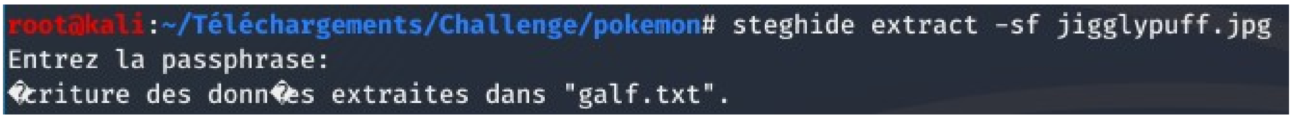
```
root@kali:~# echo 'bGV0bWVzbGVlcA==' | base64 -d
letmesleeproot@kali:~# 
```

And we get as result «**letmesleep**», i thinking about a steghide password for «**jigglypuff.jpg**» and tried it.



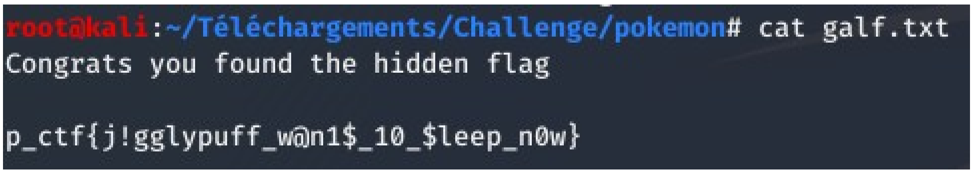
```
root@kali:~/Téléchargements/Challenge/pokemon# steghide info jigglypuff.jpg
"jigglypuff.jpg":
  format: jpeg
  capacit�: 2.3 KB
Essayer d'obtenir des informations �propos des donn�es incorpor�es ? (o/n) o
Entrez la passphrase:
  fichier �inclure "galf.txt":
    taille: 74.0 Byte
    cryptage: rijndael-128, cbc
    compression: oui
```

The password worked, and it discovered an embed file «**galf.txt**». Extract it with steghide and the password «**letmesleep**».



```
root@kali:~/Téléchargements/Challenge/pokemon# steghide extract -sf jigglypuff.jpg
Entrez la passphrase:
�criture des donn�es extraites dans "galf.txt".
```

Then read the extracted text file.



```
root@kali:~/Téléchargements/Challenge/pokemon# cat galf.txt
Congrats you found the hidden flag

p_ctf{j!gglypuff_w@n1$_10_$leep_n0w}
```

And we get our flag.

Flag : p_ctf{j!gglypuff_w@n1$_10_$leep_n0w}