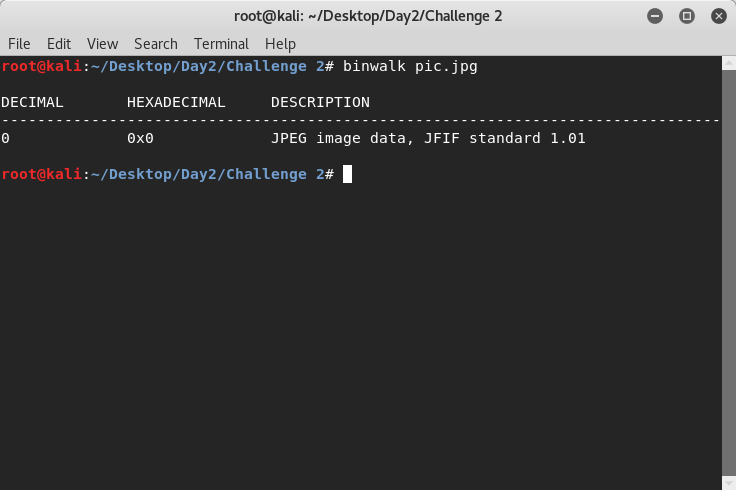
**Challenge 2 Day 2 – Harambe**

By team Bingsu Strawberry from IIUM

Step 1:

We received a picture of type .jpg which mean this is definitely going to be easier than the first challenge which involved a .png file. Whew. We zoomed in to check for any hidden text and found nothing. Moving onto the more complex stages.

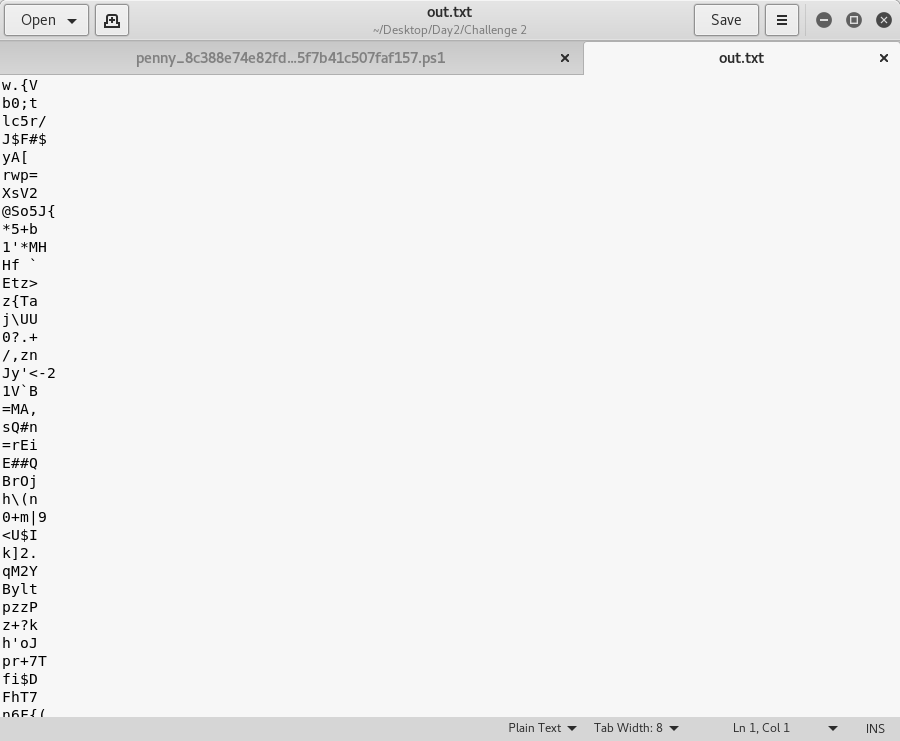
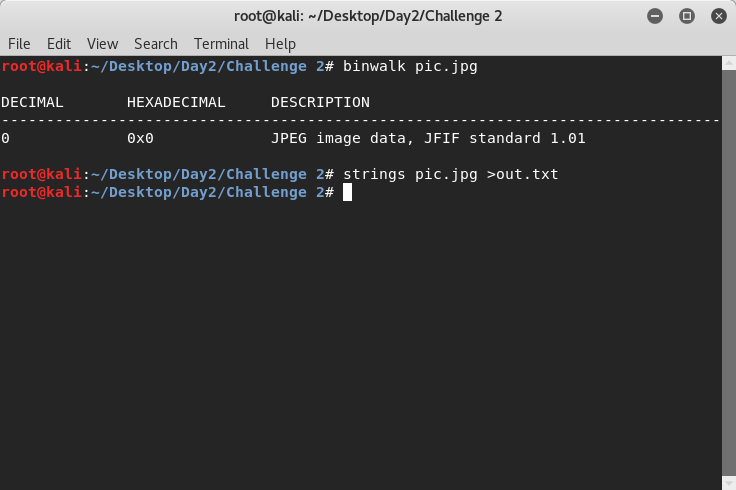
Step 2:

Moving onto the next step, we tried using binwalk on the image to check for any hidden zip file. 

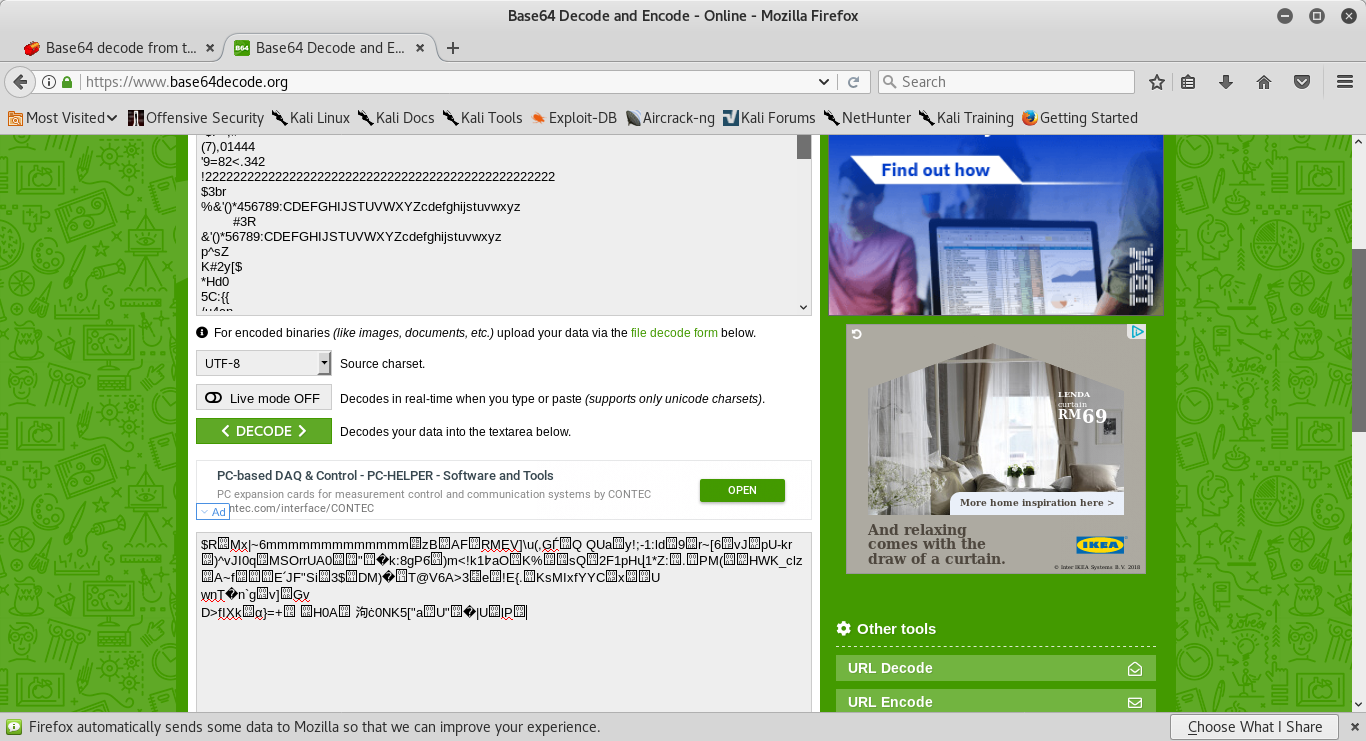
Nothing hidden here inside the image.

Step 3:

We tried using the strings tool to check whether its hidden there.



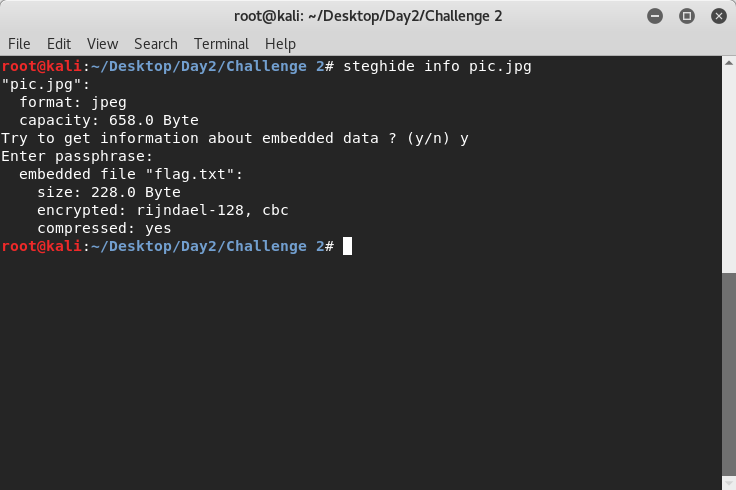
This is the text result. It looks kind of like its encoded with base64 with the weird O sign and abundance of = signs.

We tried decoding it using a base64 decoder online 

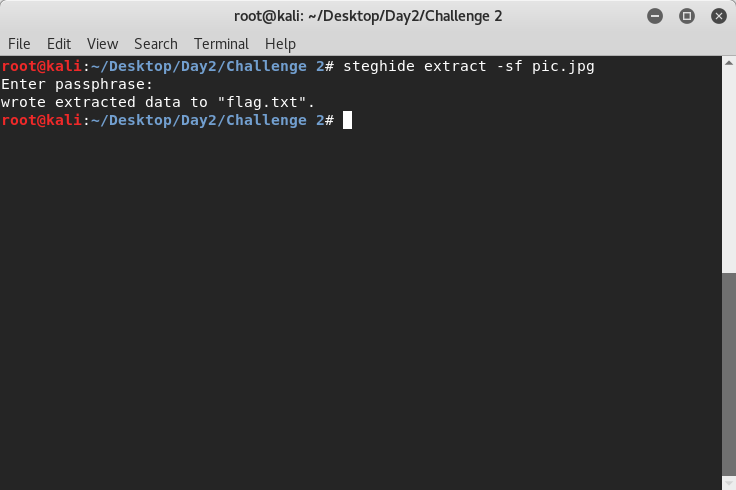
This is definitely not the flag :P.

Step 4:

Time to use some common steganography tools we can find. First up, steghide!

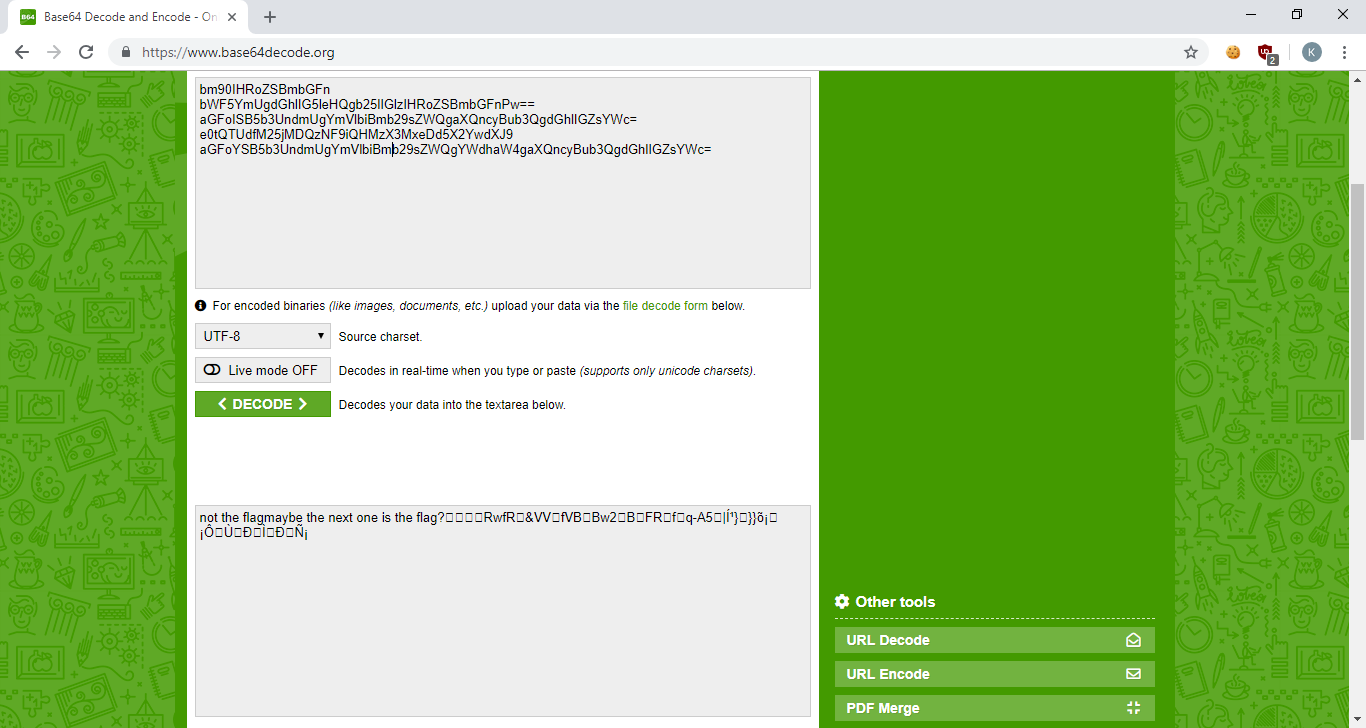


Bingo! We found the flag! We can now go to class peacefully :D . We extract the file out.





Now this definitely encoded using base64 . Run it through a base64 decoder and we should find the flag I hope.



Running it all at once doesn’t provide us the flag but it gave us a hint. Maybe we should run it one by one.

The fourth line gave us the flag! e0tQTUdfM25jMDQzNF9iQHMzX3MxeDd5X2YwdXJ9 deocded to {KPMG\_3nc0434\_b@s3\_s1x7y\_f0ur} and this is our flag!

Flag = {KPMG\_3nc0434\_b@s3\_s1x7y\_f0ur}