**Down the Wormhole**

***Forensics***

**Challenge:**

An explosive chase with a UFO led us to a wormhole!

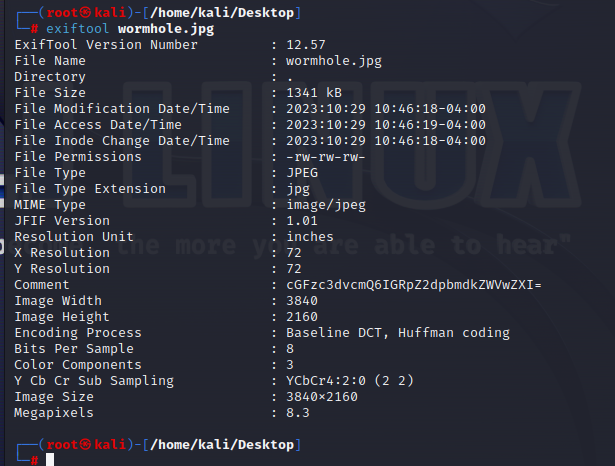
Make sure you have your bases covered before you head in and find the secrets hiding inside!

Attached - wormhole.jpg

**Approach:**

This one was a multi step challenge and it was fun solving this.

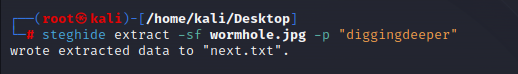
Firstly we perform exiftool on it to get this data:



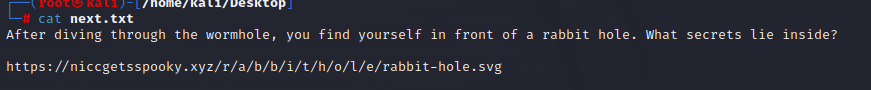
We decode this comment to get:

password: diggingdeeper

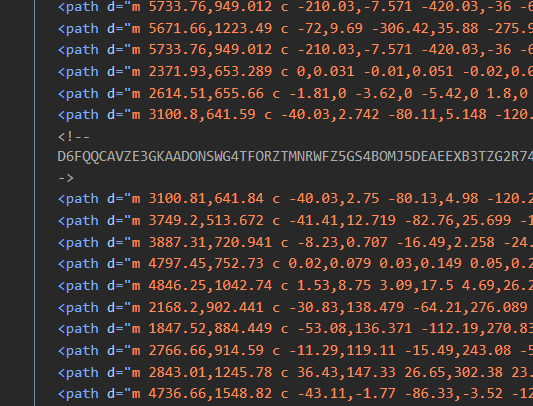
Okay…now this password could be used for anything, but since we don’t have much to go with, maybe it has to go with the image? We use this password with steghide and see there was a file hidden in it:



The content of next.txt read as follows:



Heading over to the website, on one look there’s nothing much to it. We open developer tools and scroll down a bit to reveal a comment:



We copy this weird string in cyberchef and see that it is base32 text of a whole zip file, damn!

We download the zip file and extract it to see that there’s a file named secrets666.zip.bz2. If we open it we’ll see more zips in it. Now I've solved this type of question before. It basically requires you to create a bash script to unzip the zip files. I analyzed the different zips used to craft my bash script:

#!/bin/bash

for ((i=666 ; i >=1 ; i--));

do

gzip -d secrets${i}.zip.bz2.gz

bzip2 -d secrets${i}.zip.bz2

unzip secrets${i}.zip

rm -rf secrets${i}.zip

done

In about less than 5 minutes, it solved all my trouble and handed me the flag.txt file which read:

**Flag: NICC{TH3-UF0S-4R3-UP-N0T-D0WN-50-WHY-4R3-Y0U-D0WN-H3R3}**

Congrats!!

Happy Hacking!