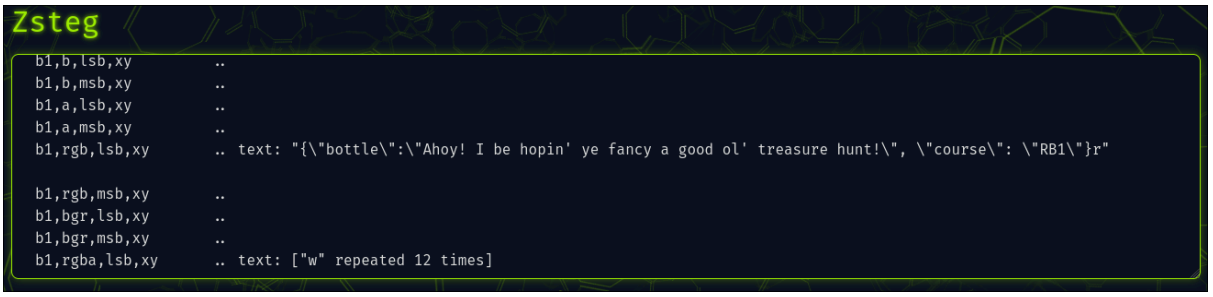
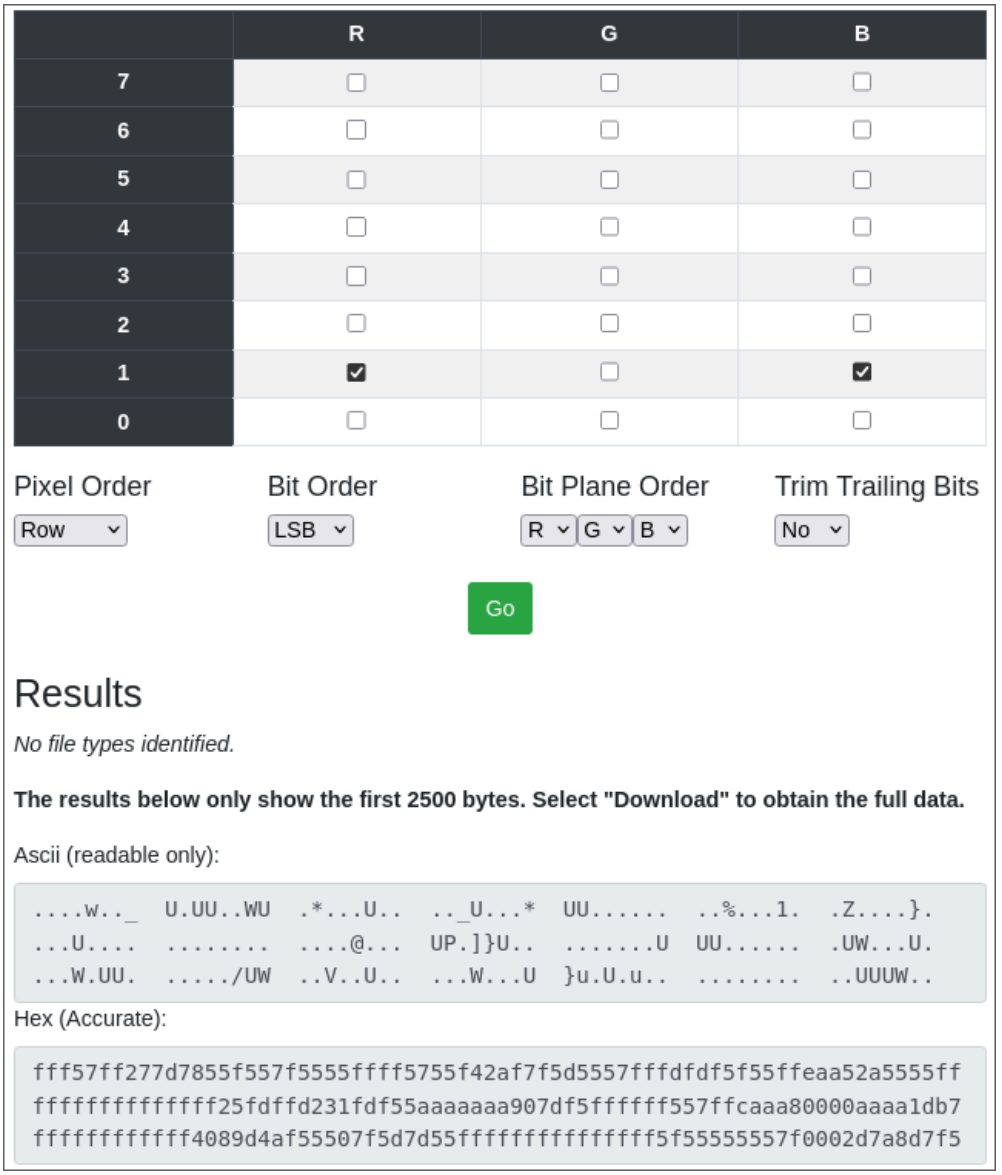
After I uploaded the image on Aperi'Solve, I saw this message at **zsteg** :



Immediately I knew I had to use LSB, on **https://www.georgeom.net/StegOnline/upload** or **https://cyberchef.io/.**

After a lot of research, I will leave you every step, as briefly as possible because they are a lot of steps :

1. Upload the image on **https://www.georgeom.net/StegOnline/upload**, go to **Extract Files/Data**, use **RB1 :**



Now I got a **data** file, so I used find out a hidden message using **strings** :

strings -n 7 flag.dat

The output :

WUZUUZR
UUUUUU]
*WZUx5_
b pRz/_r
_UUUU_wi
EIZBLVE
~V@uhl6
u_UUUUU
Mm3!H6[
U+{"bottle":"Arrr, the great Cap
n Red Beard be sailin' the Seven Seas in search o
the almighty flag!", "course": "R2"}
…

Now it's clear, we have to apply the same algorithms for every message we find.

2. Upload **AGAIN** the image on **https://www.georgeom.net/StegOnline/upload**. **Get out after the website** and upload your picture **again**. It is a bug in which the LSB does not work properly if we use the first load. That's why we better recharge the picture on the website. Go to **Extract Files/Data**, use **R1.** Command :

   strings -n 7 flag.dat

   # The message :

   {"bottle":"He sailed long 'n' far from shore to shore aboard the mighty Stormsailor...", "course": "BG3"}

3. Upload the image on **https://cyberchef.io/.** because we have to use **BG3** and save the file. There is **no** such option on **StegOnline** :

Command :

strings -n 7 download.dat

The message :

{"bottle":"Till one fateful day, he did find th' flag!", "course": "GB2"}

4. Upload **AGAIN** the image on **https://www.georgeom.net/StegOnline/upload**. Extract **GB2.** Command :

   strings -n 7 flag.dat

   # The message :

   {"bottle":"It be on a wee island, with naught but his fav'rite fruit tree standin' tall.", "course": "B1"}

5. Upload **AGAIN** the image on **https://www.georgeom.net/StegOnline/upload**. Extract **B1.** Command :

   strings -n 7 flag.dat

   # The message :

   {"bottle":"Th' fruit be sweet as treasure, not sour at all, shaped like a crescent moon.", "course": "R3"}

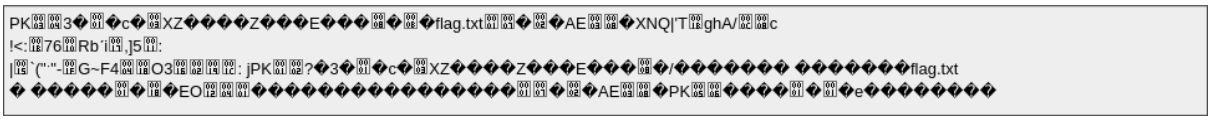
6. Upload **AGAIN** the image on **https://www.georgeom.net/StegOnline/upload**. Extract **R3.** Command :

   strings -n 7 flag.dat

   # The last message :

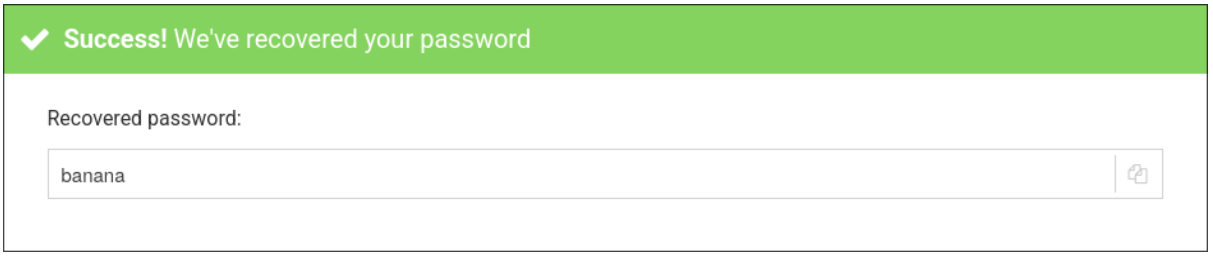
{"bottle":"Now, tell me, ye scallywag, what fruit did that tree bear?", "treasure": "UEsDBDMAAQBjAAO9WFoAAAAAWgAAAEUAAAAIAAsAZmxhZy50eHQBmQcAAgBBRQMIAFhOyFF8J1TyG2doQcYvrgzortHSCGMNxMshPDobNzagEPb3jVJi8820aRecsizN1F01EToNfBXNYLUo7v4irZDLka8iLR9HfkY0xgT+GE/9MxamvglZHDogaIBLAQI/ADMAAQBjAAO9WFoAAAAAWgAAAEUAAAAIAC8AAAAAAAAAIAAAAAAAAABmbGFnLnR4dAoAIAAAAAAAAQAYAEVPEqsEh9sBAAAAAAAAAAAAAAAAAAAAAAAAGZBwACAEFFAwgAUEsFBgAAAAABAAEAZQAAAIsAAAAAAA=="}

Now, if we use a Base64 decoder for **treasure** we will see :



This is an Archive. Upload the text on **https://cyberchef.io/** and extract the file :

Now if we want to extract the archive, we will see that the archive it's protected with a password. Upload the archive on **https://www.lostmypass.com/try/ :**



Command :

7z x download.zip
Enter password (will not be echoed): banana
cat flag.txt

THE FLAG :
CTF{1f8915fa52fbf862ba636d69f39427dd8aeb4a9e7b28afc5a36fd70d6db580ac}
~Z4que