

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

```
Zsteg <
b1,b,lsb,xy ..
b1,b,msb,xy ..
b1,a,lsb,xy ..
b1,a,msb,xy ..
b1,rgb,lsb,xy .. text: "{ \"bottle\": \"Ahoy! I be hopin' ye fancy a good ol' treasure hunt!\", \"course\": \"RB1\"}r"

b1,rgb,msb,xy ..
b1,bgr,lsb,xy ..
b1,bgr,msb,xy ..
b1,rgba,lsb,xy .. text: ["w" repeated 12 times]
```

# 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** :

	R	G	B
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pixel Order  
Row ▾

Bit Order  
LSB ▾

Bit Plane Order  
R ▾ G ▾ B ▾

Trim Trailing Bits  
No ▾

Go

### Results

No file types identified.

The results below only show the first 2500 bytes. Select "Download" to obtain the full data.

Ascii (readable only):

```
....w._ U.UU..WU .*...U.. .._U...* UU..... ..%...1. .Z....}.
...U.... ..... ....@... UP.]}U.. .....U UU..... .UW...U.
...W.UU. .... /UW ..V..U.. ...W...U }u.U.u.. ..... .UUUW..
```

Hex (Accurate):

```
fff57fff277d7855f557f5555ffff5755f42af7f5d5557fffd5f55fffeaa52a5555ff
fffffffd231fd55aaaaaa907df5fffff557ffcaaa80000aaaa1db7
fffffffd4089d4af55507f5d7d55ffffffffff55555557f0002d7a8d7f5
```

# Now I got a **data** file, so I used find out a hidden message using **strings** :  
**strings -n 7 flag.dat**

# The output :

```
WUZUZR
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"}
...
```

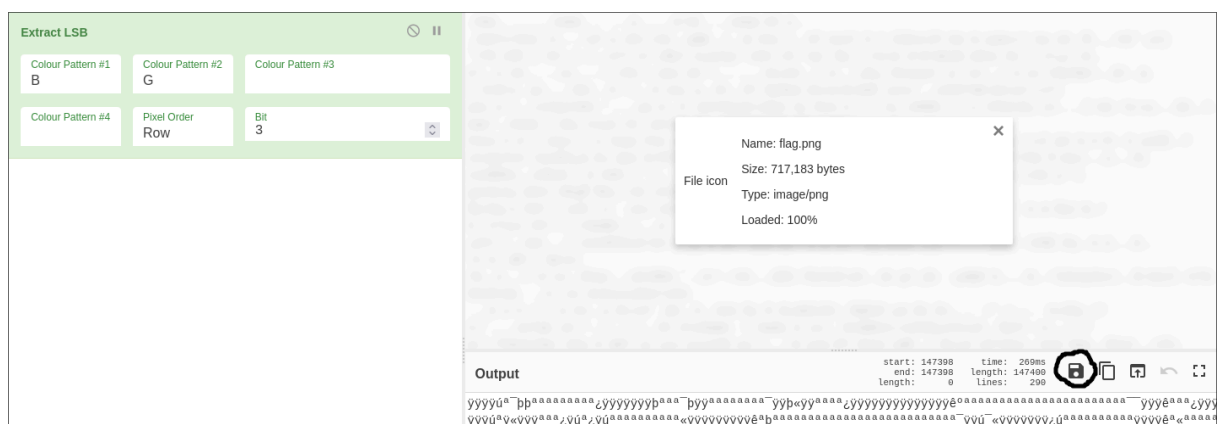
# Now it's clear, we have to apply the same algorithms for every message we find.

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":  
"UEsDBDMAAQBjAAO9WFOAAAAAWgAAAEUAAAAIAAsAZmxhZy50eHQBmQcAAgB  
BRQMIAFhOyFF8J1TyG2doQcYvrgzortHSCGMNxMshPDobNzagEPb3jVJi8820aRecsiz  
N1F01EToNfBXNYLUo7v4irZDLka8iLR9HfkY0xgT+GE/9MxamvgiZHDogaIBLAQI/ADMA  
AQBjAAO9WFOAAAAAWgAAAEUAAAAIAC8AAAAAAAAAAAAAAAAAABmbGFnLnR  
4dAoAIAAAAAAAAAQAYAEVPEqsEh9sBAAAAAAAAAAAAAAAAAAAGZBwACAE  
FFAwgAUEsFBgAAAAABAAEAZQAAAlsAAAAAAAA=="}  
}**

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

```
PK3cXZEEflag.txtAEXNQJThghA/c  
!<76Rb'i.j5:  
j["G~F4O3: jPK?3cXZEE/flag.txt  
EOEAEPKPe
```

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

From Base64

Alphabet

A-Za-z0-9+/=

☒ Remove non-alphabet chars

**Input**

length: 352  
lines: 1

+

```

UESDBDMAAQBJAA09WFOAAAAAwgAAAEUAAAAIAAsAZmxhZy50eHQBMQcAAgBBRQMIAFh0yFF8J1TyG2doQcYvrgzortHSCGMNxMshPDobNzagEPb
3jVJi8820aRecsizN1F01ETonFBXNYLUo7v4irZDLka8iLR9HfkY0xgT+GE/9MxamvgIZHDoga1BLAQI/
ADMAAQBJAA09WFOAAAAAwgAAAEUAAAAIAC8AAAAAAAAIAAAAAAAAAABmbGFnLnR4dAoAIAAAAAAAAAQAYAEVPEqsEh9sBAAAAAAAAAAAAAAAA
AAAGZBwACAEFFAwgAUESFBgAAAAABAAEAZQAAAI sAAAAAA==

```

**Output**

time: 1ms  
length: 262  
lines: 2

```

PK...3...c...%XZ...Z...E.....flag.txt.....AE...XNÈQ|'Tò.ghAÆ/®.è®Ñ0.c
ÄÈ!<.:.76 .ò÷.Rbóí'í..²,í0]5.:
|.í`µ(ip"..È."-.G~F4Æ.p.0ý3.}%...: jPK..?.3...c...%XZ...Z...E.../.....flag.txt
. ....EO.«..Û.....AE...PK.....e.....

```

# 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/> :

✓ Success! We've recovered your password

Recovered password:

banana

# Command :

7z x download.zip

# Enter password (will not be echoed): banana

cat flag.txt

THE FLAG :

CTF{1f8915fa52fbf862ba636d69f39427dd8aeb4a9e7b28afc5a36fd70d6db580ac}

~Z4que