Command :

```
❯ exiftool Gandalf.jpg
ExifTool Version Number         : 13.36
File Name                       : Gandalf.jpg
Directory                       : .
File Size                       : 15 kB
File Modification Date/Time     : 2025:12:03 12:57:14+02:00
File Access Date/Time           : 2025:12:03 13:02:24+02:00
File Inode Change Date/Time     : 2025:12:03 12:57:21+02:00
File Permissions                : -rwxrwxrwx
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Comment                         : Q1RGbGVhcm57eG9yX2lzX3lvdXJfZnJpZW5kfQo=.
Image Width                     : 225
Image Height                    : 225
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 225x225
Megapixels                      : 0.051
```

FromBase64(Q1RGbGVhcm57eG9yX2lzX3lvdXJfZnJpZW5kfQo=) = CTFlearn{xor_is_your_friend}

Command :

```
❯ strings Gandalf.jpg
JFIF
+Q1RGbGVhcm57eG9yX2lzX3lvdXJfZnJpZW5kfQo=
+xD6kfO2UrE5SnLQ6WgESK4kvD/Y/rDJPXNU45k/p
+h2riEIj13iAp29VUPmB+TadtZppdw3AuO7JRiDyU
"1!%*+...
383-7(-.+
+---+------+----------------+-------+------++----
"AQa
…
```

Python script to “”decrypt the flag :

```python
import base64

part1 = base64.b64decode("xD6kfO2UrE5SnLQ6WgESK4kvD/Y/rDJPXNU45k/p")
part2 = base64.b64decode("h2riEIj13iAp29VUPmB+TadtZppdw3AuO7JRiDyU")

flag = ""

for i in range(len(part1)) :
    flag += str( chr(part1[i] ^ part2[i]) )
print(flag)
```

THE FLAG : CTFlearn{Gandalf.BilboBaggins}
~Z4que