whaleCTF-30days-隐写【第二期】-踢踏舞-writeup

原创

sec小玖 于 2018-07-24 14:47:34 发布 438 收藏
分类专栏： CTF 隐写 文章标签： CTF 隐写 敲击密码 摩斯电码 二维码批量读取

本文链接：https://blog.csdn.net/afuzong4267/article/details/81183770

提示：

> 踢踏舞太美了，忍不住我就用图片记录了舞蹈的过程，请告诉我这段舞蹈表达了什么~

得到一张二维码图片，打开发现由89张二维码构成。

这里使用zbar-tools工具中的zbarimg命令批量扫描二维码。

```
sec@sec-pc:~/1/new$ zbarimg gifn.gif
QR-Code:two
QR-Code:parts
QR-Code:parts
QR-Code:parts
QR-Code:parts
QR-Code:all
QR-Code:all
QR-Code:all
QR-Code:lower
QR-Code:lower
QR-Code:lower
QR-Code:lower
QR-Code:add
QR-Code:add
QR-Code:add
QR-Code:add
QR-Code:9447{
```

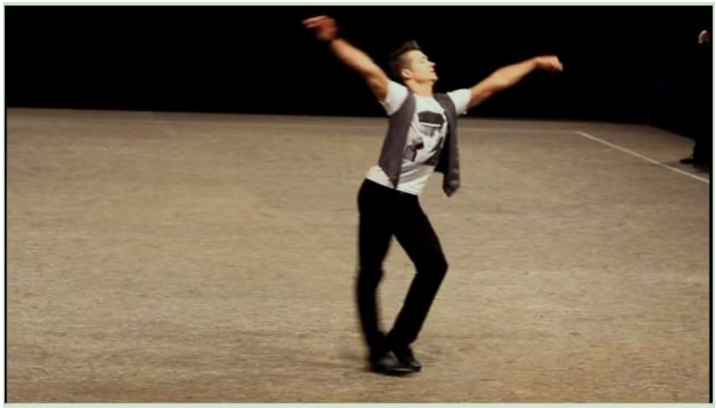
QR-Code:9447{
QR-Code:9447{
QR-Code:9447{
QR-Code:to
QR-Code:start
QR-Code:start
QR-Code:start
QR-Code:start
QR-Code:and
QR-Code:and
QR-Code:and
QR-Code:{
QR-Code:{
QR-Code:{
QR-Code:{
QR-Code:to
QR-Code:to
QR-Code:to
QR-Code:the
QR-Code:the
QR-Code:the
QR-Code:the
QR-Code:end
QR-Code:end
QR-Code:end
QR-Code:end
QR-Code:first
QR-Code:first
QR-Code:first
QR-Code:first
QR-Code:looks
QR-Code:like
QR-Code:like
QR-Code:like
QR-Code:like
QR-Code:'7do'
QR-Code:'7do'
QR-Code:'7do'
QR-Code:cut
QR-Code:cut
QR-Code:cut
QR-Code:cut
QR-Code:off
QR-Code:off
QR-Code:off
QR-Code:off
QR-Code:450ms
QR-Code:450ms
QR-Code:450ms
QR-Code:450ms
QR-Code:second
QR-Code:like
QR-Code:like
QR-Code:like
QR-Code:like
QR-Code:https://www.youtube.com/watch?v=5xxTkB5bGy4
QR-Code:https://www.youtube.com/watch?v=5xxTkB5bGy4
QR-Code:https://www.youtube.com/watch?v=5xxTkB5bGy4
QR-Code:https://www.youtube.com/watch?v=5xxTkB5bGy4
QR-Code:https://www.youtube.com/watch?v=5xxTkB5bGy4

```
QR-Code:https://www.youtube.com/watch?v=5xxTkB5bGy4
QR-Code:like
QR-Code:like
QR-Code:like
QR-Code:like
QR-Code:faucet
QR-Code:faucet
QR-Code:faucet
QR-Code:faucet
QR-Code:script
QR-Code:script
QR-Code:script
QR-Code:script
scanned 89 barcode symbols from 89 images in 0.56 seconds
```

发现有重复项，去除重复项：

```
sec@sec-pc:~/1/new$ zbarimg gifn.gif | uniq
QR-Code:two
QR-Code:parts
QR-Code:all
QR-Code:lower
QR-Code:add
QR-Code:9447{
QR-Code:to
QR-Code:start
QR-Code:and
QR-Code:{
QR-Code:to
QR-Code:the
QR-Code:end
QR-Code:first
QR-Code:looks
QR-Code:like
QR-Code:'7do'
QR-Code:cut
QR-Code:off
QR-Code:450ms
QR-Code:second
QR-Code:like
QR-Code:https://www.youtube.com/watch?v=5xxTkB5bGy4
QR-Code:like
QR-Code:faucet
QR-Code:script
scanned 89 barcode symbols from 89 images in 0.57 seconds
```

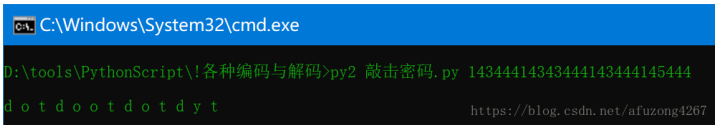
根据字母提示，由两部分组成，全是小写字母，开头部分添加9447{，并且{一直到结尾第一部分类似7do，每450ms截取一下，第二部分像视频中的faucet script？没搞懂。观看视频发现是一个踢踏舞，想到敲击码和摩斯密码。



提示每隔450ms截取一帧，我们首先看一下截取到的二维码的帧数，也就是重复的二维码数，利用 | uniq -c 进行统计：

```
sec@sec-pc:~/1/new$ zbarimg gifn.gif | uniq -c
      1 QR-Code:two
      4 QR-Code:parts
      3 QR-Code:all
      4 QR-Code:lower
      4 QR-Code:add
      4 QR-Code:9447{
      1 QR-Code:to
      4 QR-Code:start
      3 QR-Code:and
      4 QR-Code:{
      3 QR-Code:to
      4 QR-Code:the
      4 QR-Code:end
      4 QR-Code:first
      1 QR-Code:looks
      4 QR-Code:like
      3 QR-Code:'7do'
      4 QR-Code:cut
      4 QR-Code:off
      4 QR-Code:450ms
      1 QR-Code:second
      4 QR-Code:like
      5 QR-Code:https://www.youtube.com/watch?v=5xxTkB5bGy4
      4 QR-Code:like
      4 QR-Code:faucet
scanned 89 barcode symbols from 89 images in 0.59 seconds
```

发现数量都不超过5，使用敲击密码试一下，1434441434344414344414544：



所以得到第二部分的密码：dotdootdotdyt

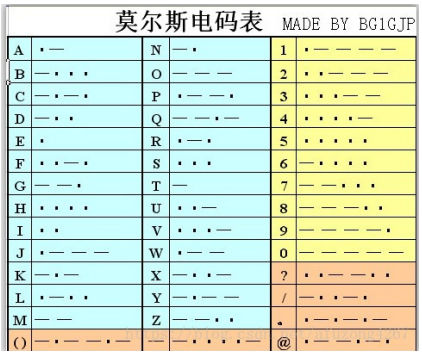
上面查看了帧数，下面再查看一下时间，使用identify工具检查图片的时长，命令：

```
sec@sec-pc:~/1/new$ identify -format "%s %T\n" gifn.gif
0 50
1 40
2 40
3 50
4 50
5 50
6 50
7 50
8 40
9 40
。。。
```

发现只有40 和 50， 联想到摩斯密码，将40替换为. ，50 替换为- ，另一组将40替换为 -，将50替换为 .

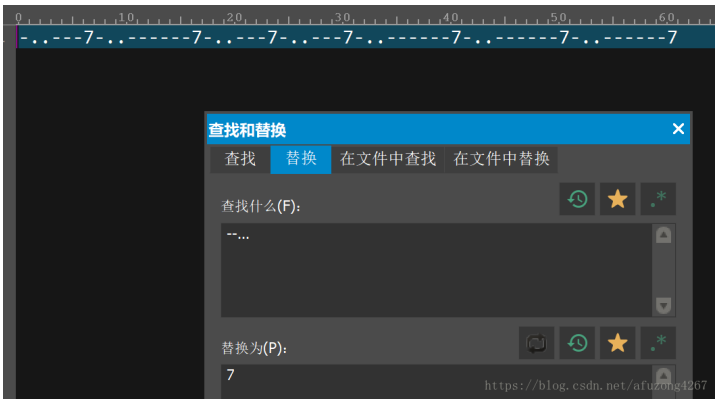
```
sec@sec-pc:~/1/new$ identify -format "%T" gifn.gif | tr -d 0 | tr '4' '.'| tr '5' '-'
-..-----...-..--------...-..-----...-..-----...-..----------...-..--------...-..--------...
sec@sec-pc:~/1/new$ identify -format "%T" gifn.gif | tr -d 0 | tr '4' '-'| tr '5' '.'
.--.....---.--.........---.--.........---.--.....---.--.........---.--.........---.--.........---
```

发现并没有空格分隔。联想到 7do，查找摩斯电码对照表，其中7对应--.. ； d对应 -.. ； o对应 ---



莫尔斯电码表		MADE BY BG1GJP			
A	·—	N	—·	1	·————
B	—···	O	———	2	··———
C	—·—·	P	·——·	3	···——
D	—··	Q	——·—	4	····—
E	·	R	·—·	5	·····
F	··—·	S	···	6	—····
G	——·	T	—	7	——···
H	····	U	··—	8	———··
I	··	V	···—	9	————·
J	·———	W	·——	0	—————
K	—·—	X	—··—	?	··——··
L	·—··	Y	—·——	/	—··—·
M	——	Z	——··	.	·—·—·—
()	—·——·—			@	·——·—·

对比后发现第二条开头就不匹配了，因此对第一条尝试进行替换，使用UE进行替换，这里需要先替换7，再替换d，否则7中的部分编码也会变成d：



依次替换后，得到：do7doo7do7do7doo7doo7doo7

将三部分拼接起来： 9447{do7doo7do7do7doo7doo7doo7dotdootdotdyt}，得到flag！