StarCTF2021-MISC-Writeup

原创

末 初 于 2021-01-20 23:25:48 发布 706 收藏 2

分类专栏： CTF_MISC_Writeup

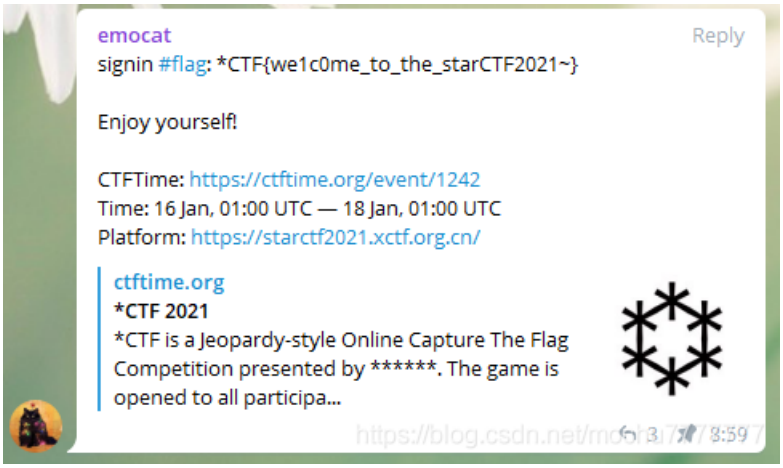
文章目录

signin
MineGame
little tricks
puzzle
Feedback

---

signin


```
Welcome to *CTF 2021, join telegram to get flag: https://t.me/starCTF
```




```
*CTF{we1c0me_to_the_starCTF2021~}
```

MineGame


```
If you love reverse, you can try it, otherwise, you must finish it as quickly as possible.
```

题目附件

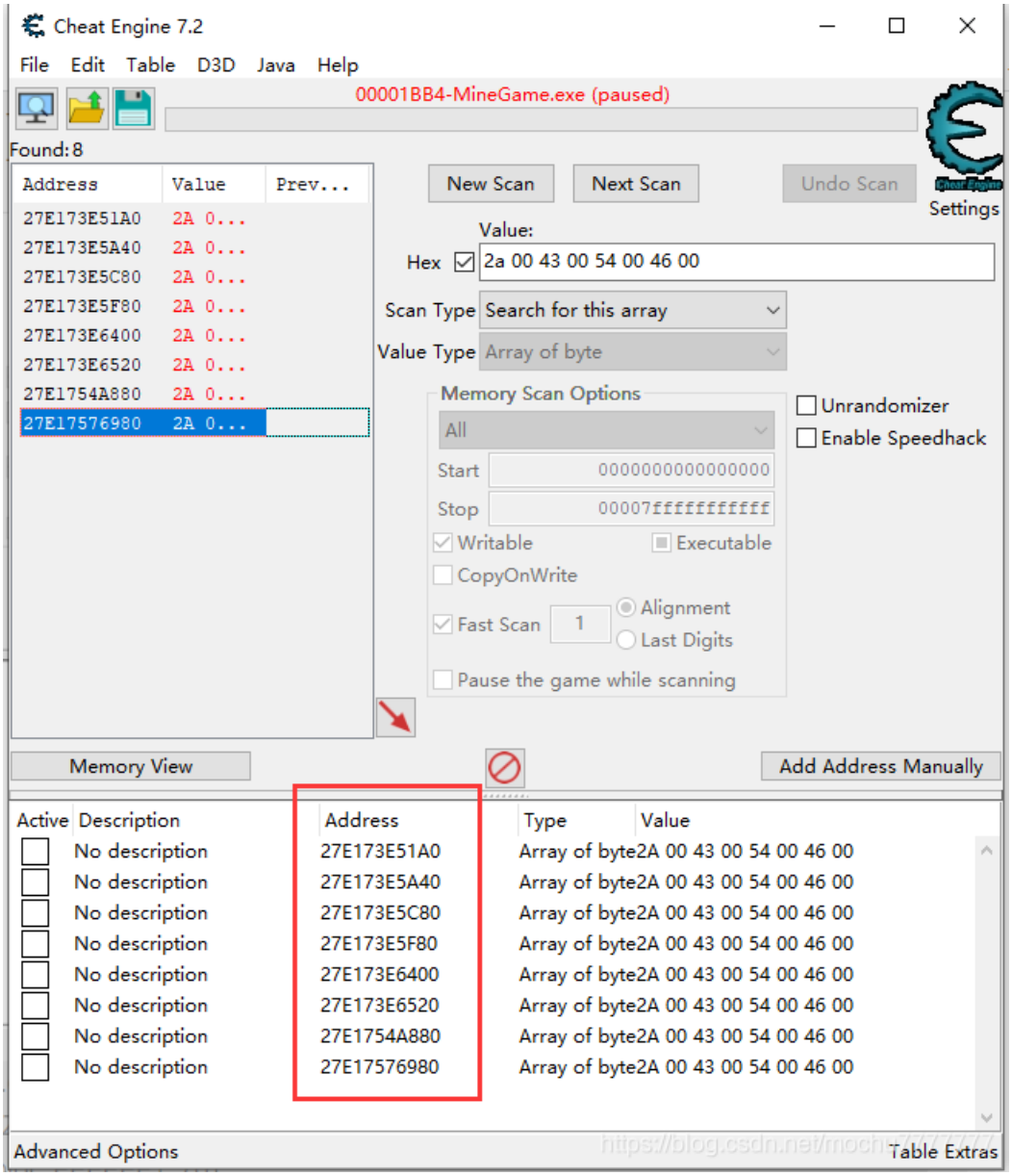
`readme.txt`

```
MineGame:

Verify that version 9.9 (R2020b) of the MATLAB Runtime is installed.
If not, you can run the MATLAB Runtime installer.
To find its location, enter

    >>mcrinstaller

at the MATLAB prompt.
NOTE: You will need administrator rights to run the MATLAB Runtime installer.

Alternatively, download and install the Windows version of the MATLAB Runtime for R2020b
from the following link on the MathWorks website:

    https://www.mathworks.com/products/compiler/mcr/index.html


If you can't use those ways above, you can download Runtime installer that the author has prepared for your Mine
Game from those site :


    https://drive.google.com/file/d/1HBxALAqETpEfT1tZSxbgMFVqv0v5pY3O/view?usp=sharing

     https://pan.baidu.com/s/130oOYBiWBwGX_HUfjuspXA    password:flag

HINT:
  1. The first time you run MineGame, it may be slow. You can try more times.
  2. Using computer with good performance may help you.
```

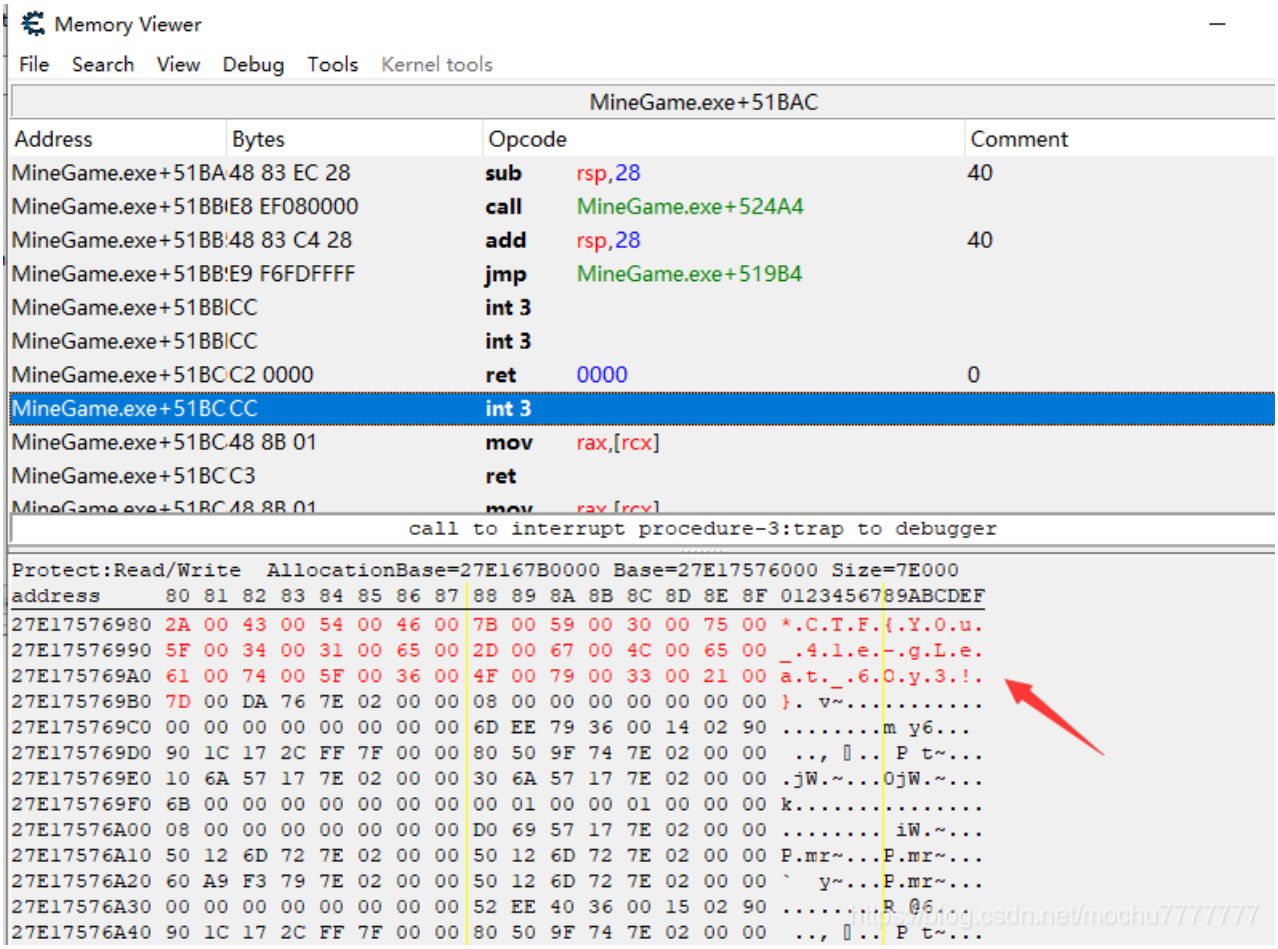
下载完`MATLAB`，之后运行`MineGame.exe`发现是扫雷，而且运行程序大概十秒后就会自动结束程序，首先运行`MineGame.exe`，然后使用`Cheat Engine`打开这个进程，然后点击左下角的`Advanced Options`暂停进程

然后利用`CE`可以在内存种搜索字符`*CTF`的Unicode编码

```
字符：*CTF
Unicode编码：2A 00 43 00 54 00 46 00
```



在内存中找到了好几个地址有该字符串，在`27E17576980`地址找到完整的flag

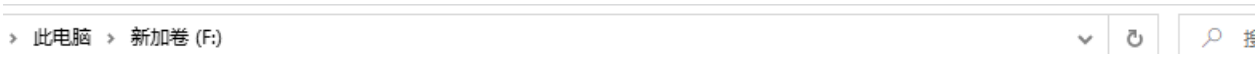



```
*CTF{Y0u_41e-gLeat_6Oy3!}
```

little tricks

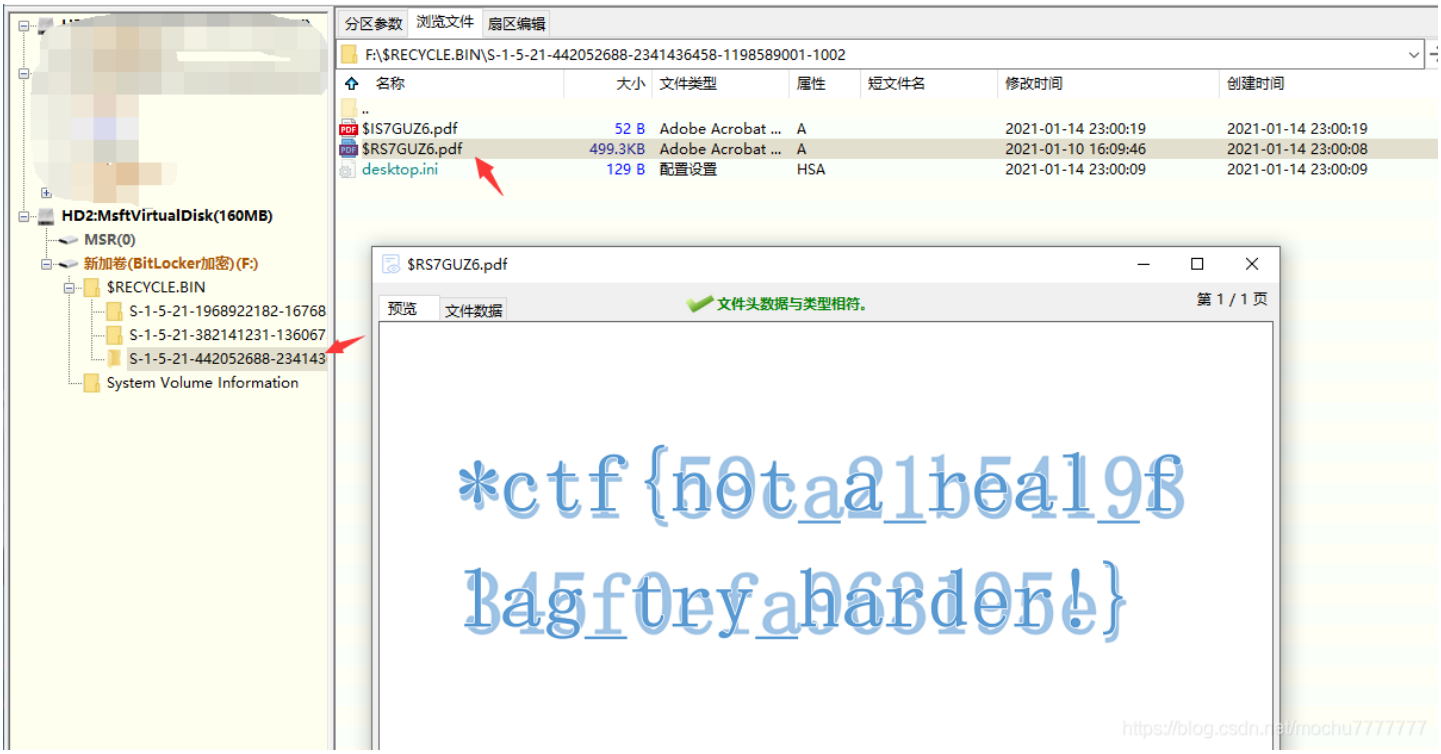
`ll2`用`file`一查看发现是windows磁盘镜像

尝试修改`vhdx`，然后尝试了下弱密码`12345678`就直接打开了，2333
里面只有个`password.txt`，并没发现其他的



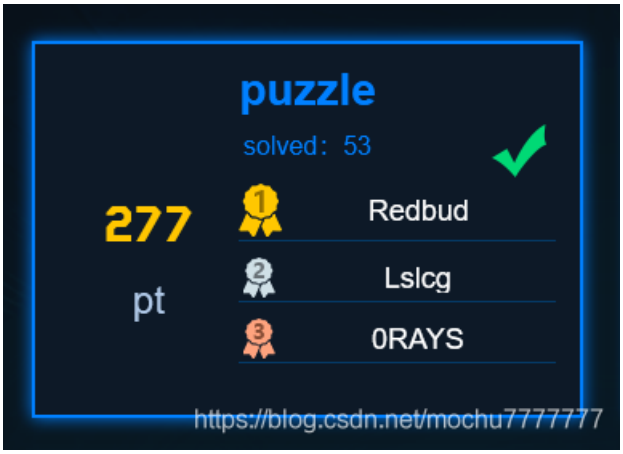
`DiskGenius`打开，发现两个`pdf`文件

直接打开较大的`pdf`，两个flag重叠了，上面的是假的，下面的是真的



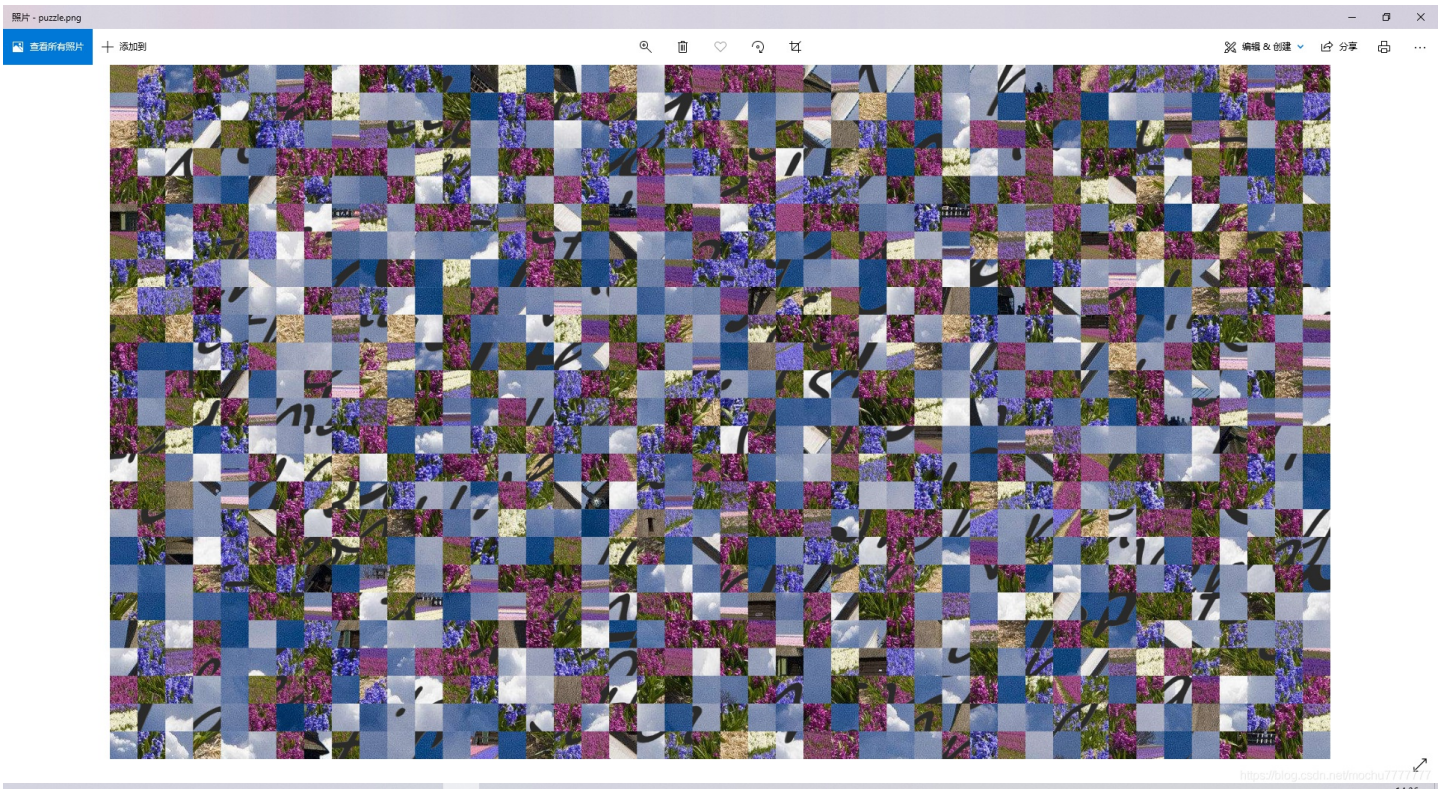

```
*ctf{59ca21b54198345f0efa963195e}
```

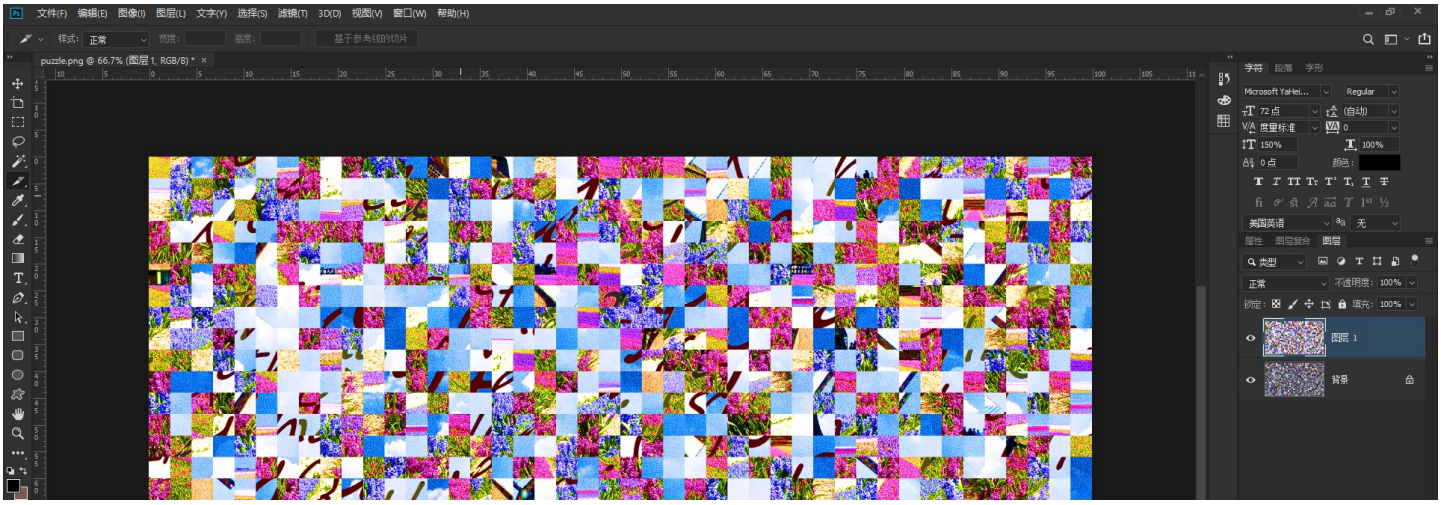
puzzle

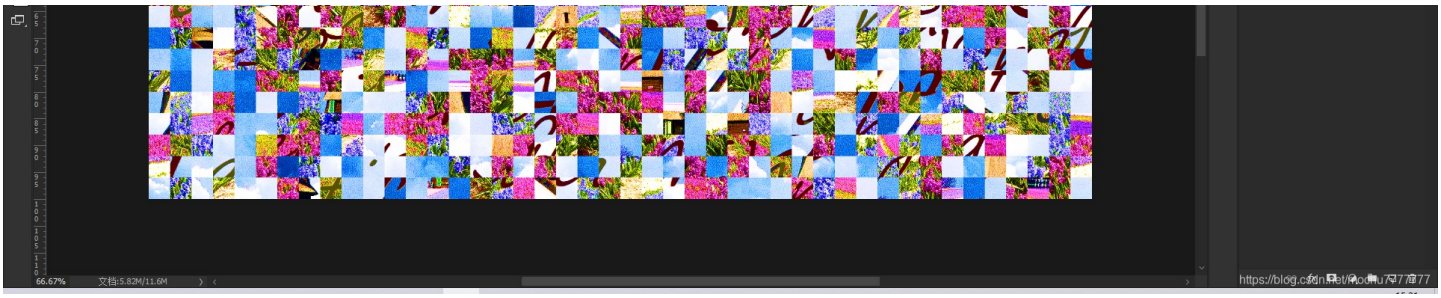


拼图游戏

每一块拼图`size=43`

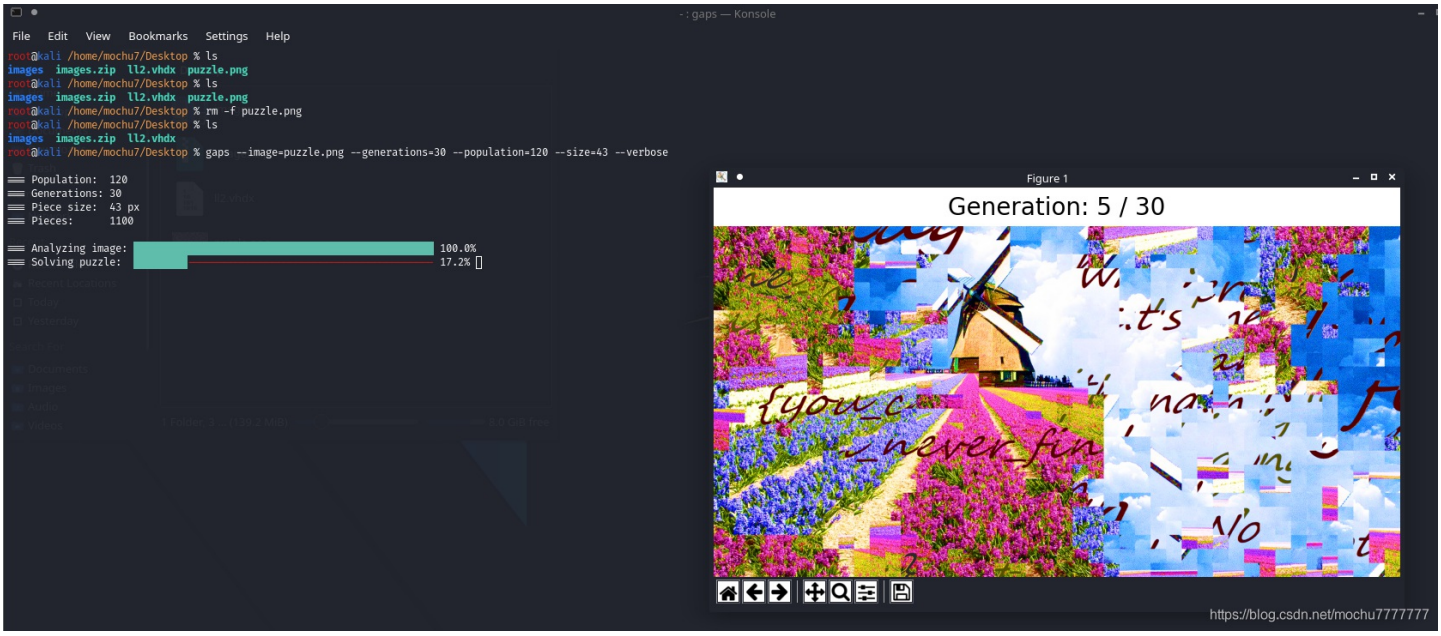


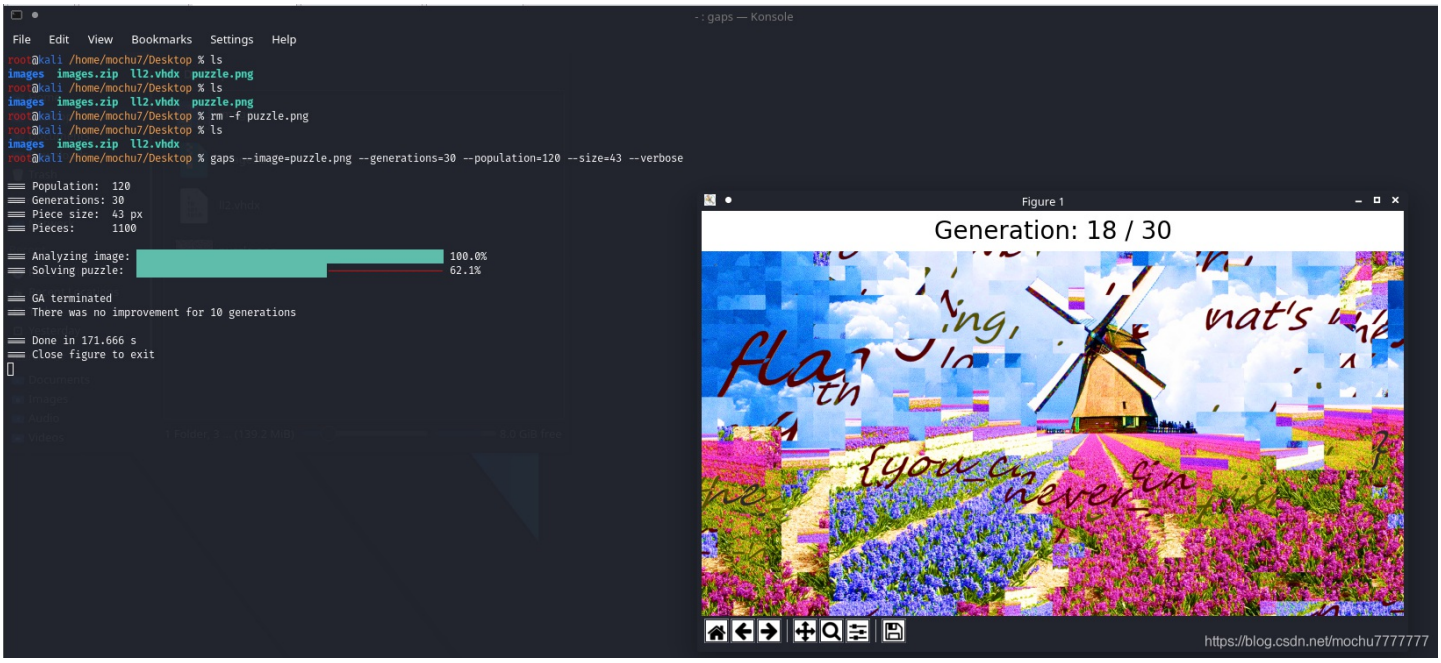




`PS` 调整饱和度、对比度、亮度
然后用`gaps`跑跑，看看每一代训练结果

```
gaps --image=puzzle.png --generations=30 --population=120 --size=43 --verbose
```



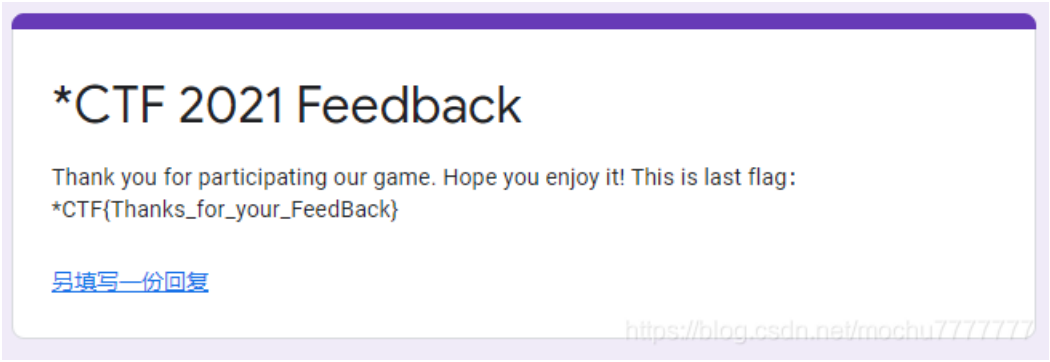


差不多就可以看出来`flag`
实在看不出来就用手工拼一下

```
flag{you_can_never_finish_the}
```

Feedback

```
We need your FeedBack!
https://forms.gle/UjK5RWBU7XA5DmHz5
```




```
*CTF{Thanks_for_your_FeedBack}
```