




# 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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/mochu7777777/article/details/112794962>

版权



[CTF\\_MISC\\_Writeup](#) 专栏收录该内容

246 篇文章 46 订阅

订阅专栏

## 文章目录

[signin](#)

[MineGame](#)

[little tricks](#)

[puzzle](#)

[Feedback](#)

## signin



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

emocat Reply  
signin #flag: \*CTF{we1c0me\_to\_the\_starCTF2021~}

Enjoy yourself!

CTFTime: <https://ctftime.org/event/1242>  
Time: 16 Jan, 01:00 UTC — 18 Jan, 01:00 UTC  
Platform: <https://starctf2021.xctf.org.cn/>

[ctftime.org](https://ctftime.org)  
\*CTF 2021  
\*CTF is a Jeopardy-style Online Capture The Flag Competition presented by \*\*\*\*\*. The game is opened to all participa...



<https://blog.csdn.net/mochu7777777>

\*CTF{we1c0me\_to\_the\_starCTF2021~}

## MineGame



MineGame

solved: 53 ✓

277	1st Lord of rings	Lord of
pt	2nd 天璇Merak	天璇Mer:
	3rd Oops	

<https://blog.csdn.net/mochu7777777>

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/1HBxALaQETpEft1tZSxbgMFVqv0v5pY30/view?usp=sharing

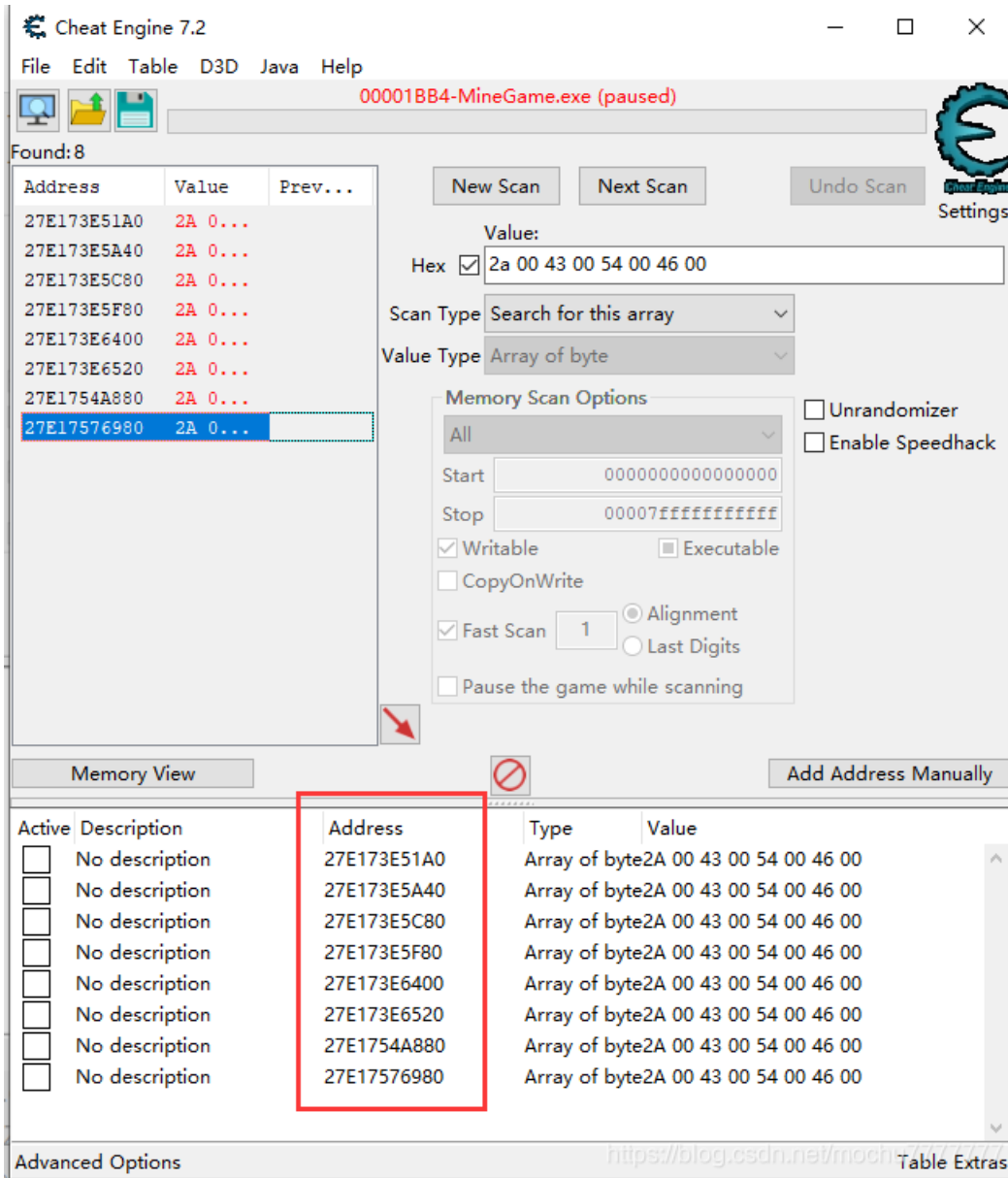
    https://pan.baidu.com/s/130oOYBiWBwGX_HUfjuspXA    password:flag

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

Memory Viewer

File Search View Debug Tools Kernel tools

MineGame.exe+51BAC

Address	Bytes	Opcode	Comment
MineGame.exe+51BA48 83 EC 28		sub rsp,28	40
MineGame.exe+51BBE8 EF080000		call MineGame.exe+524A4	
MineGame.exe+51BB48 83 C4 28		add rsp,28	40
MineGame.exe+51BBE9 F6FDFFFF		jmp MineGame.exe+519B4	
MineGame.exe+51BBCC		int 3	
MineGame.exe+51BBCC		int 3	
MineGame.exe+51BCC2 0000		ret 0000	0
MineGame.exe+51BCCC		int 3	
MineGame.exe+51BC48 8B 01		mov rax,[rcx]	
MineGame.exe+51BCC3		ret	
MineGame.exe+51BC48 8B 01		mov rax,[rcx]	
call to interrupt procedure-3:trap to debugger			

Protect:Read/Write AllocationBase=27E167B0000 Base=27E17576000 Size=7E000

address	80 81 82 83 84 85 86 87	88 89 8A 8B 8C 8D 8E 8F	0123456789ABCDEF
27E17576980	2A 00 43 00 54 00 46 00	7B 00 59 00 30 00 75 00	*.C.T.F.{.Y.O.u.
27E17576990	5F 00 34 00 31 00 65 00	2D 00 67 00 4C 00 65 00	_.4.l.e.-.g.L.e.
27E175769A0	61 00 74 00 5F 00 36 00	4F 00 79 00 33 00 21 00	a.t._.6.O.y.3.!
27E175769B0	7D 00 DA 76 7E 02 00 00	08 00 00 00 00 00 00 00	}. v~.....
27E175769C0	00 00 00 00 00 00 00 00	6D EE 79 36 00 14 02 90	.....m y6...
27E175769D0	90 1C 17 2C FF 7F 00 00	80 50 9F 74 7E 02 00 00	.., [].. P t~...
27E175769E0	10 6A 57 17 7E 02 00 00	30 6A 57 17 7E 02 00 00	.jW.~...OjW.~...
27E175769F0	6B 00 00 00 00 00 00 00	00 01 00 00 01 00 00 00	k.....
27E17576A00	08 00 00 00 00 00 00 00	D0 69 57 17 7E 02 00 00	..... iW.~...
27E17576A10	50 12 6D 72 7E 02 00 00	50 12 6D 72 7E 02 00 00	P.mr~...P.mr~...
27E17576A20	60 A9 F3 79 7E 02 00 00	50 12 6D 72 7E 02 00 00	` y~...P.mr~...
27E17576A30	00 00 00 00 00 00 00 00	52 EE 40 36 00 15 02 90	.....R @6...
27E17576A40	90 1C 17 2C FF 7F 00 00	80 50 9F 74 7E 02 00 00	.., [].. P t~...

\*CTF{Y0u\_41e-gLeat\_60y3!}

## little tricks

little tricks

solved: 62

246 pt

1 Kap0K

2 rak 天璇Merak

3 TimeKeeper

<https://blog.csdn.net/mochu777777>

112 用 file 一查看发现是windows磁盘镜像

```
root@mochu7-pc:/mnt/c/Users/Administrator/Desktop/StarCTF# file 112
112: Microsoft Disk Image extended, by Microsoft Windows 10.0.18363.0, sequence 0x14, NO Log Signature; region, 2 entries, id BAT, at 0x300000, Required 1, id Metadata, at 0x200000, Required 1
root@mochu7-pc:/mnt/c/Users/Administrator/Desktop/StarCTF#
```

尝试修改 vhdx ，然后尝试了弱密码 12345678 就直接打开了，2333

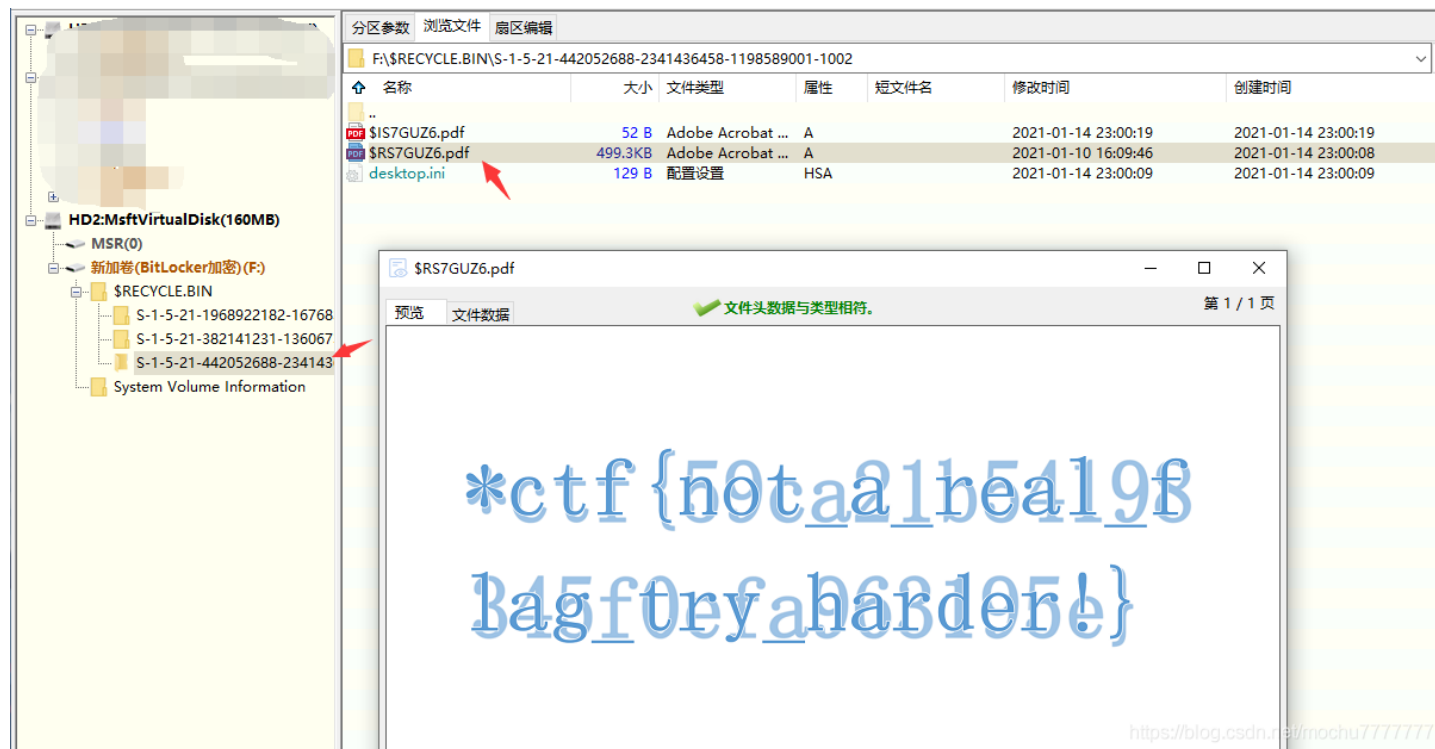
里面只有个 password.txt ，并没发现其他的



DiskGenius is opened, and two pdf files are found

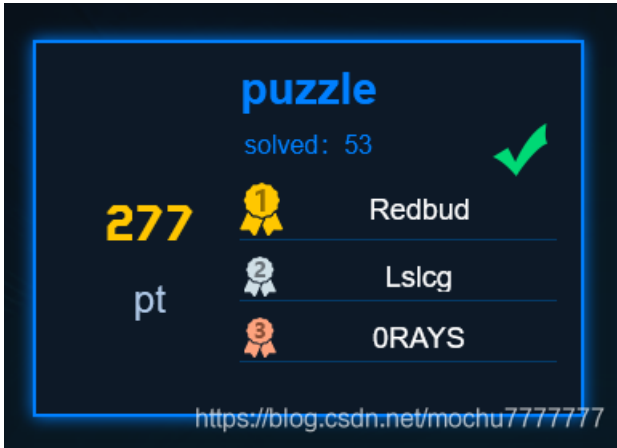


Directly open the larger pdf, the two flags overlap, the top one is fake, the bottom one is real



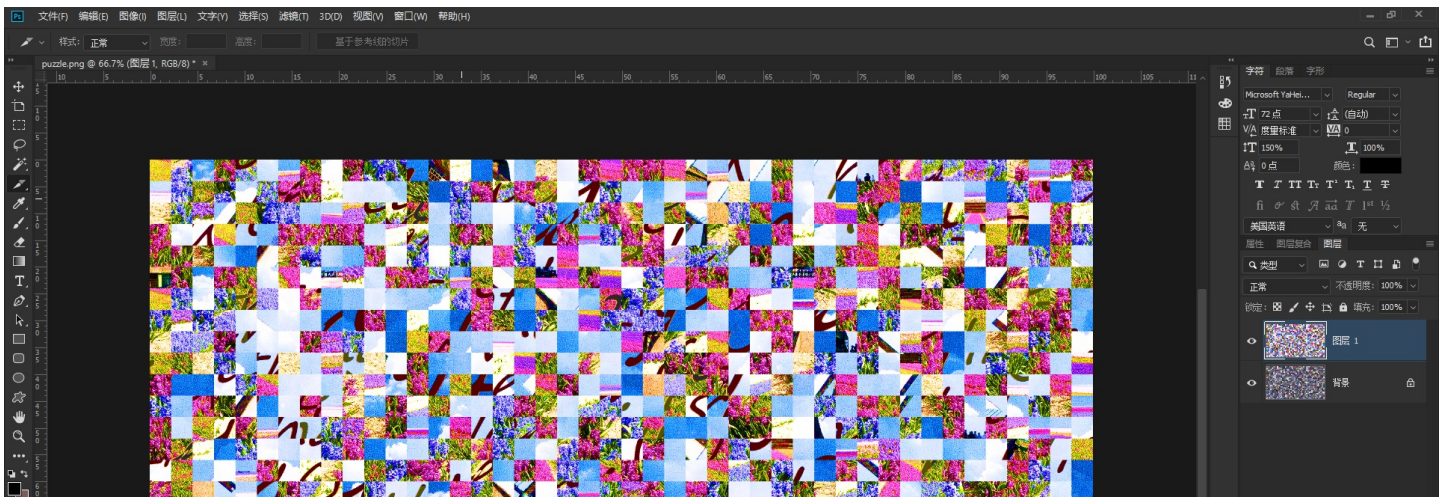
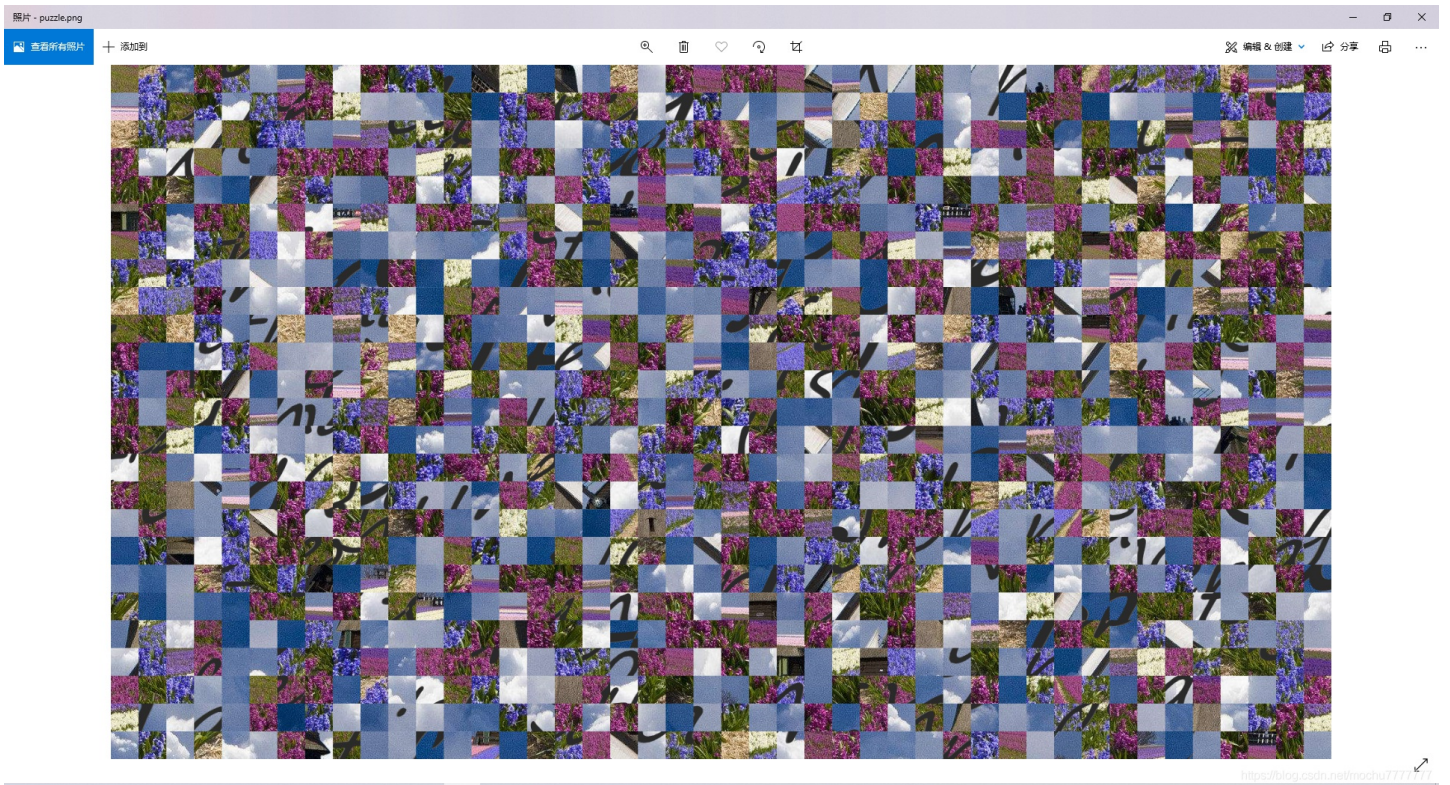
\*ctf{59ca21b54198345f0efa963195e}

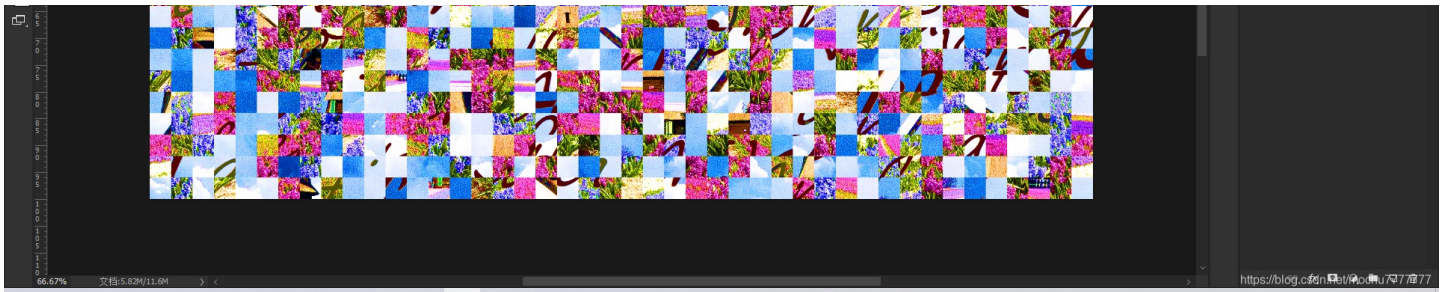
# puzzle



拼图游戏

每一块拼图 size=43



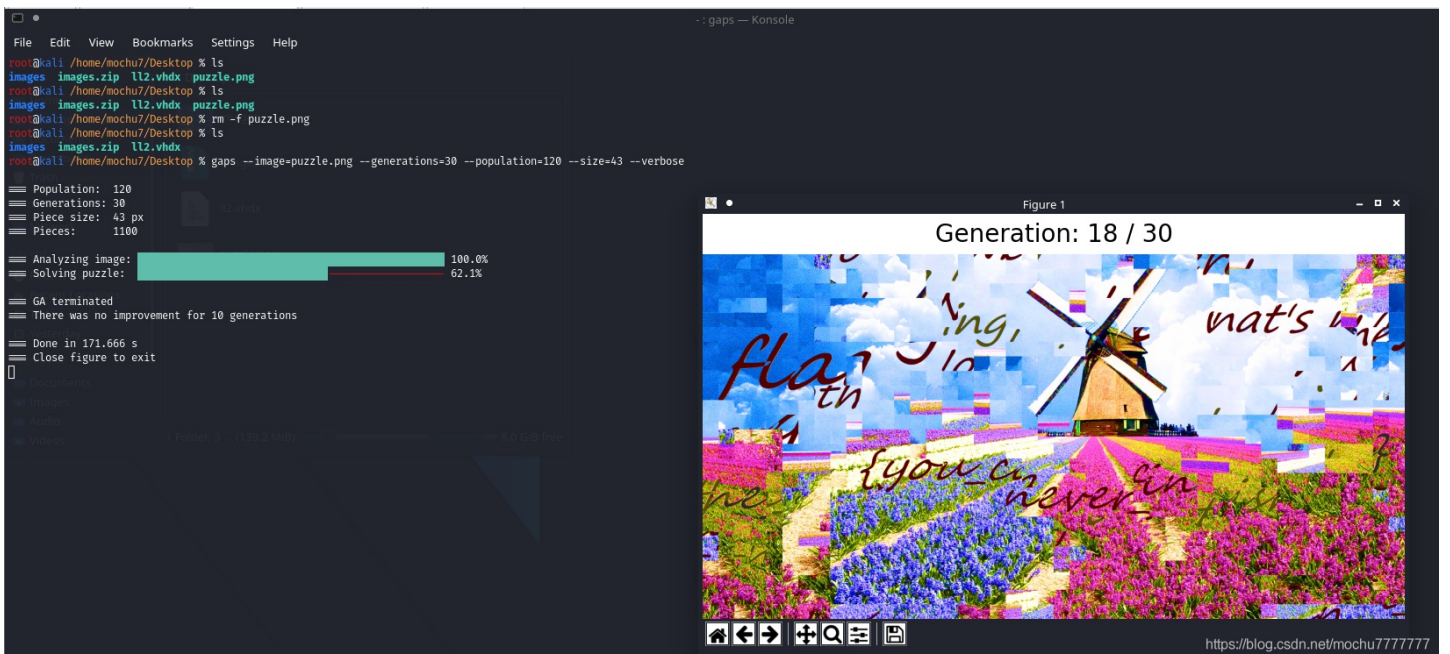
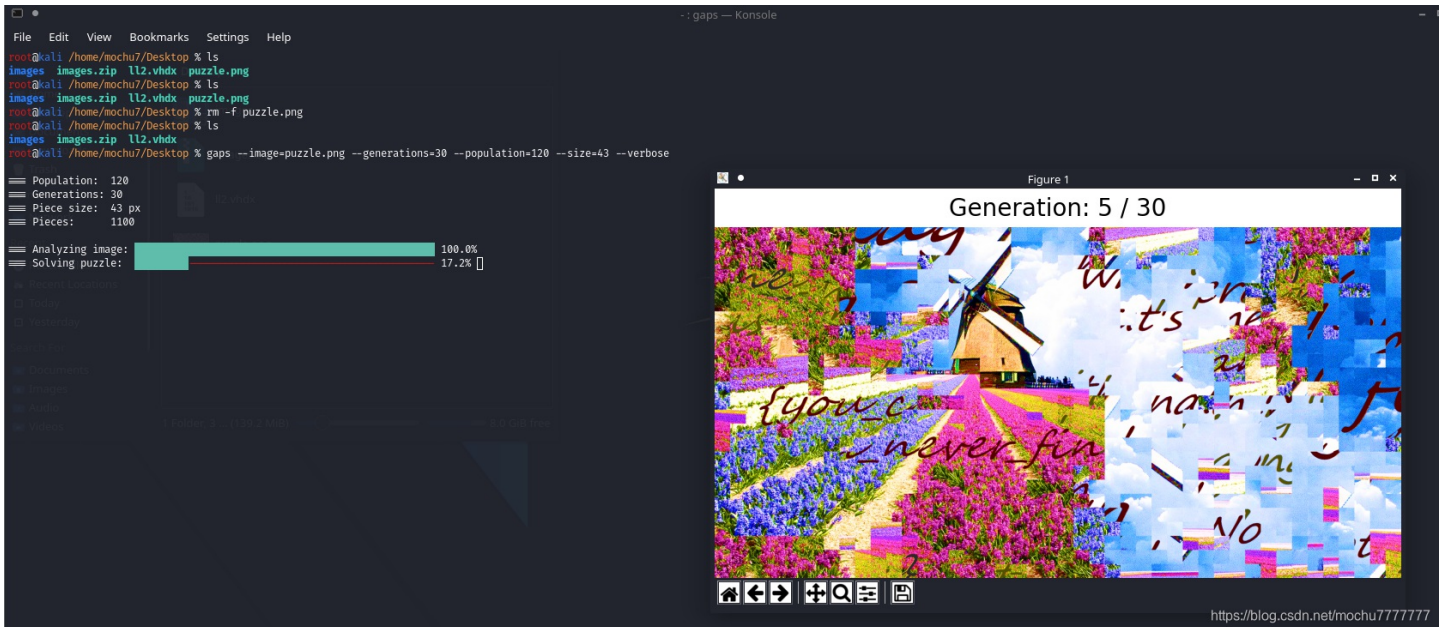


PS 调整饱和度、对比度、亮度

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 2021 Feedback

Thank you for participating our game. Hope you enjoy it! This is last flag:

\*CTF{Thanks\_for\_your\_FeedBack}

[另填写一份回复](#)

<https://blog.csdn.net/mochu7777777>

\*CTF{Thanks\_for\_your\_FeedBack}