*CTF2021 Misc部分wp

原创

MISC

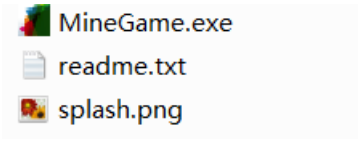
签到

签到就是下载一下推特，然后加群就得到flag


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

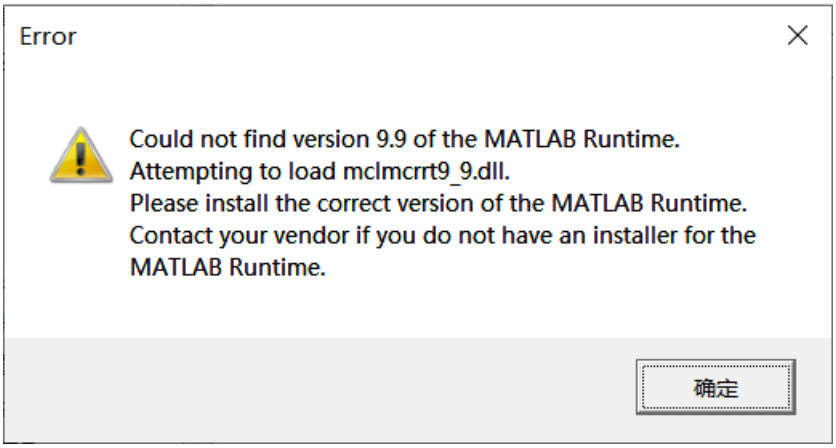
MineGame

下载附件



我们打开exe文件查看一下

发现报错



我们查看一下文本里面内容

```
# 大体意思就是让我们如果才能运行这个exe，按照txt中给的地址随便下载一个即可，下载完安装就能打开exe文件了

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.
```

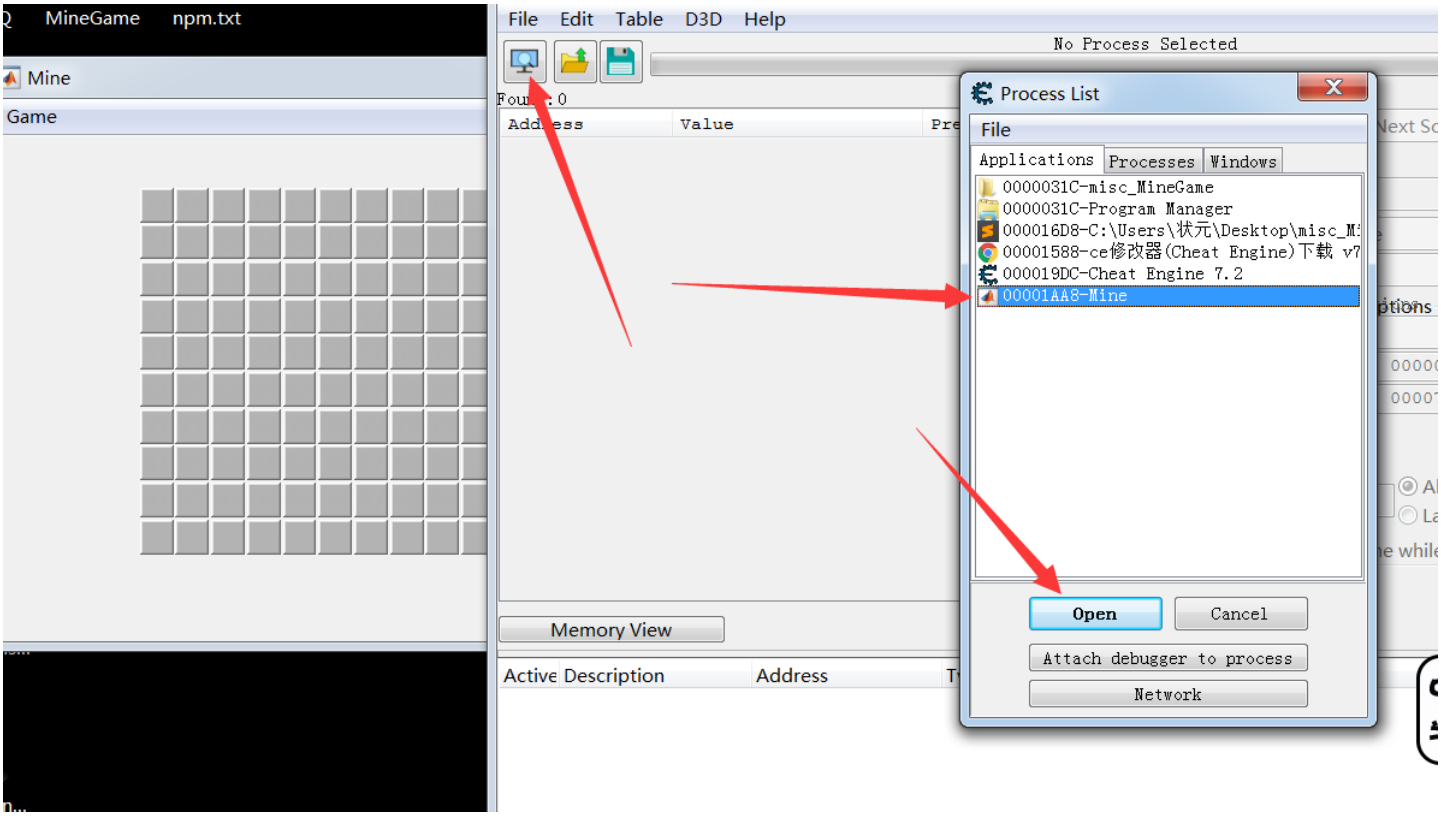
安装完后我们打开exe发现是一个扫雷，而且10后自动关闭。

我们使用`Cheat Engine`来打开这个进程

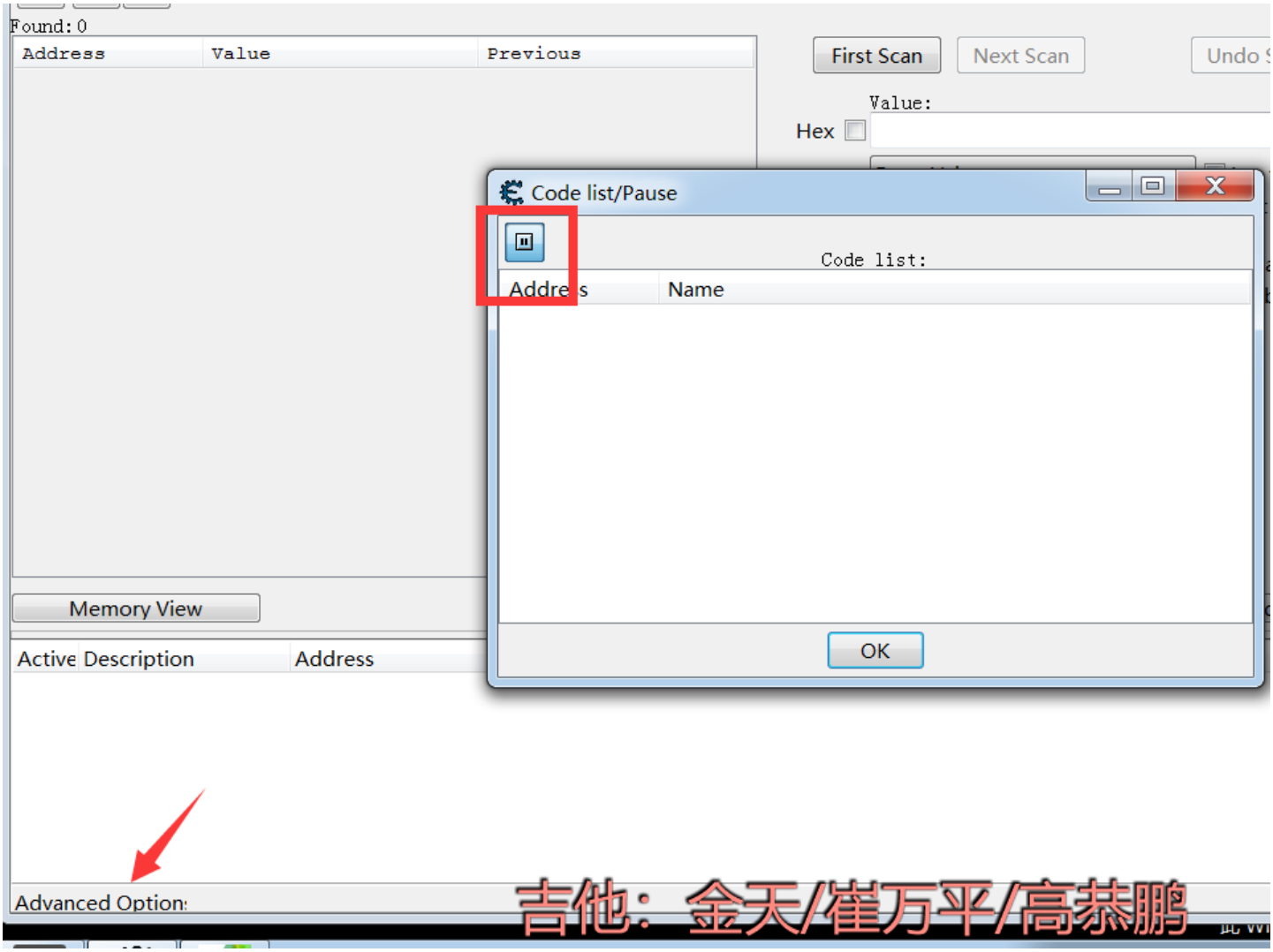
> Cheat Engine 下载地址：英文版https://www.cheatengine.org/ 中文版http://www.pc6.com/softview/SoftView_62186.html?_t_t_t=0.052645973079466335

首先打开这个软件，然后在打开exe文件

根据箭头指示按步骤点击



打开这个进程后再点击左下角的`Advanced Option`点开之后左上角有个暂停键，点开

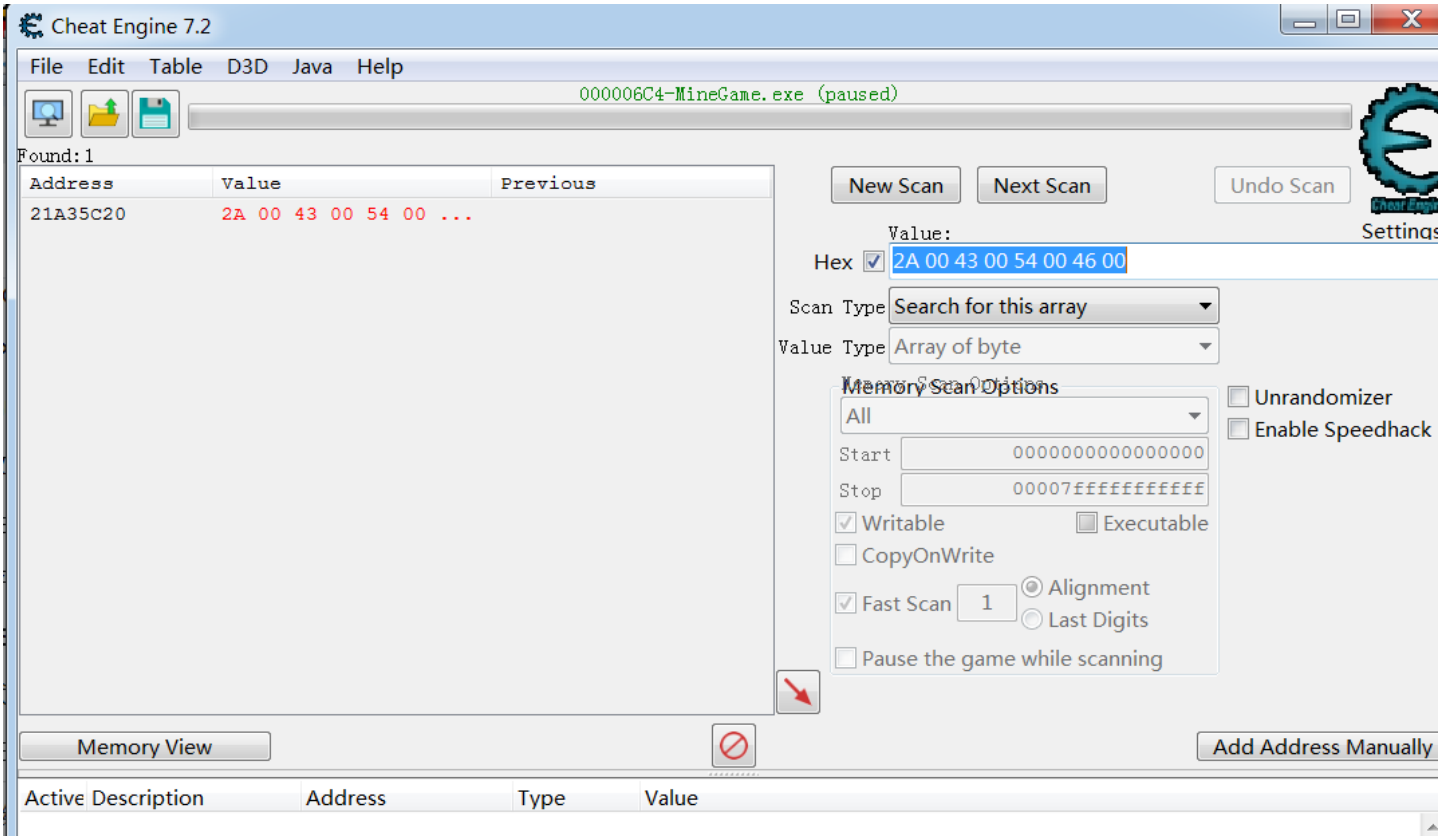


点开之后，将`Scan Type`和`Value Type`分别改成`Search for this array`和`Array of byte`

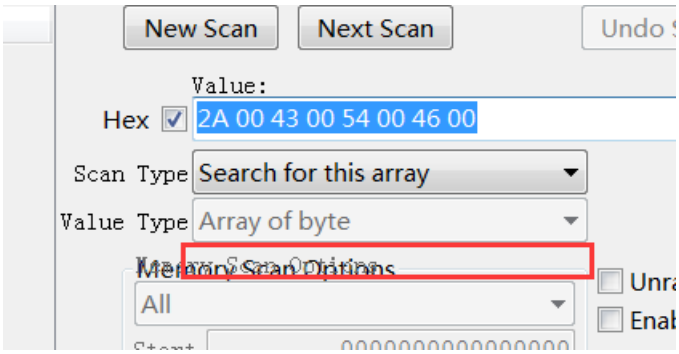
再将*CTF进行16进制加密

```
字符串：*CTF
16进制：2A435446
我们要将16进制写成以下格式
2A 00 43 00 54 00 46 00
```

然后进行`First Scan`

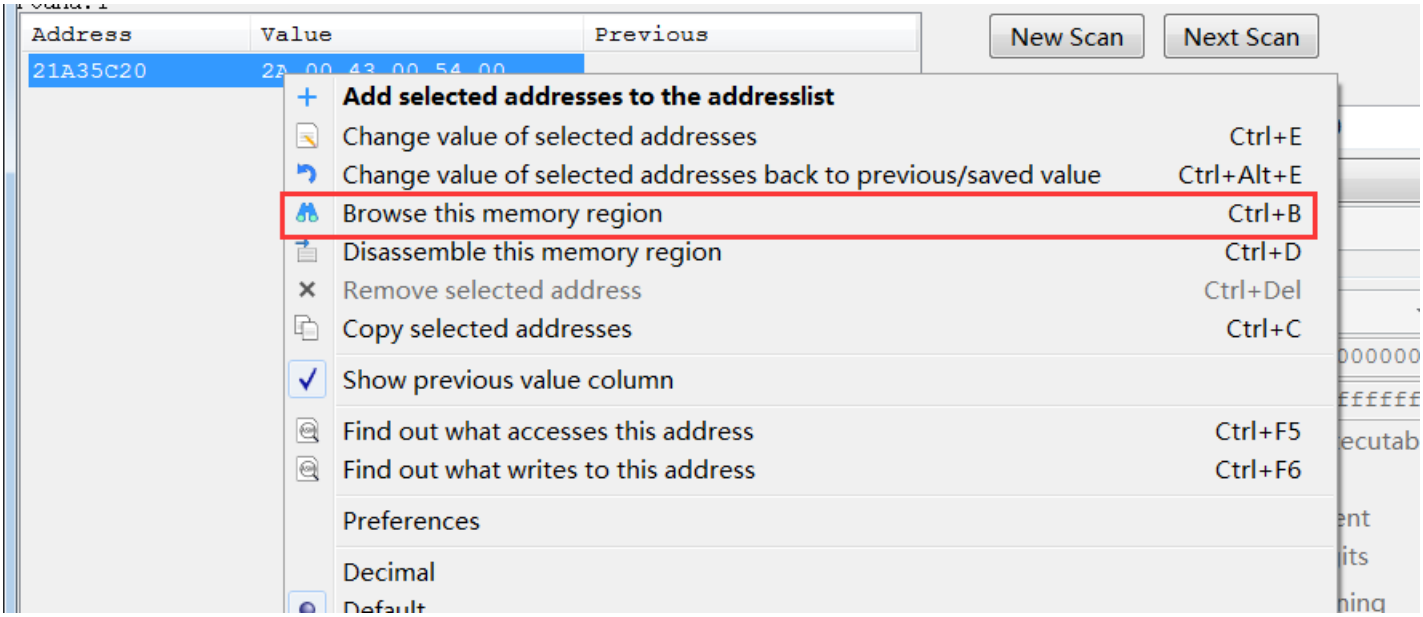


注意：如果第一次使用CE软件的话，一开始是不能更改`Scan Tyoe`和`Value Type`的，在红框的位置会有一个选框，勾选上就可以更改了，因为我们已经勾选了，所以这里不显示了。

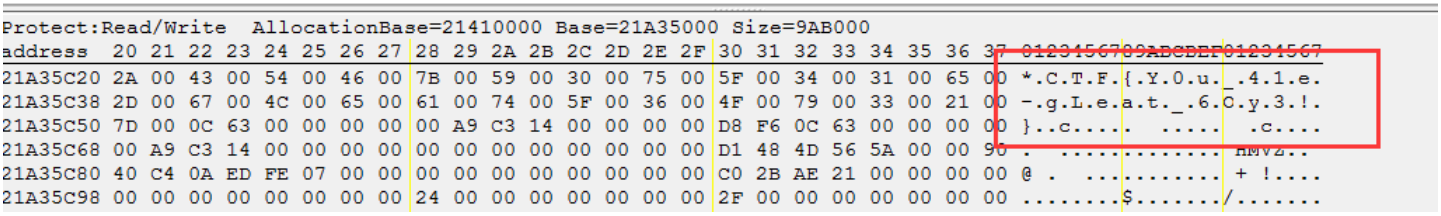


然后我们搜索和出来一个地址

右键选择红框这个选项

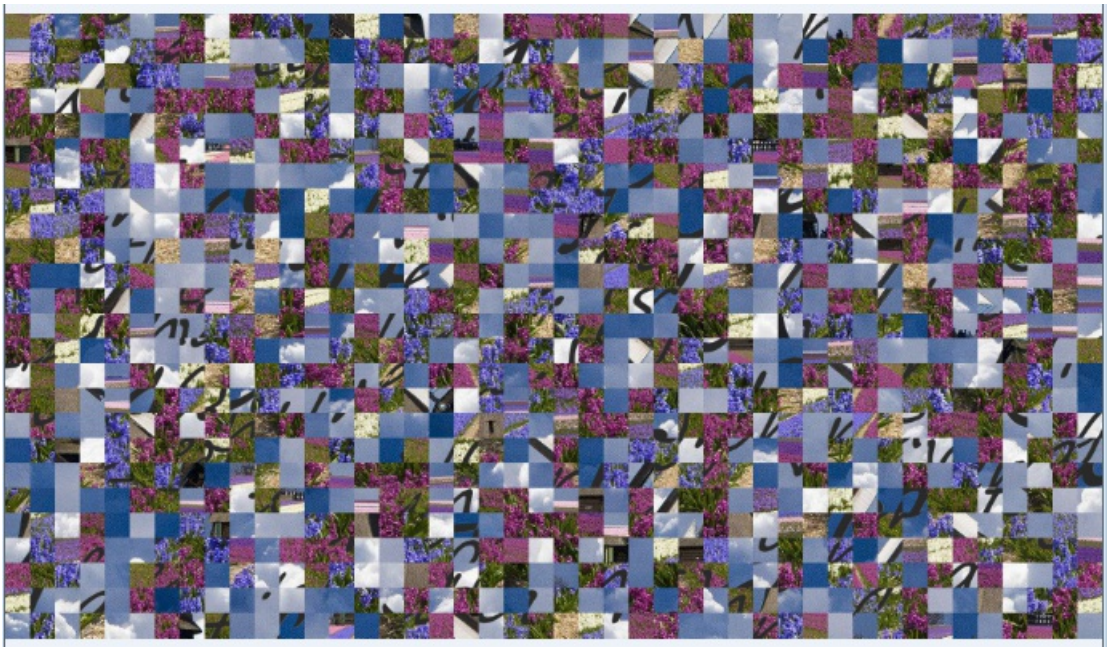


得到flag



puzzle

下载附件我们得到一个图片，看到图片我们就知道是拼图。



我们使用kali中的`gaps`来进行拼图

> 如果图片感觉亮度太低，可以用PS改一下亮度和饱和度等等。

命令如下：

```
gaps --image=puzzle1.png --generations=30 --population=120 --size=43 --verbose
```

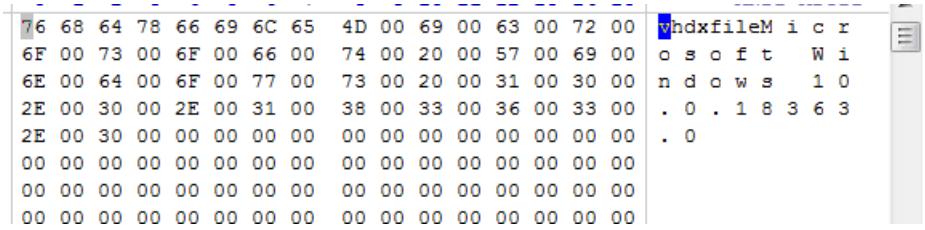
> 如果一次看不清就先将能看清的部分截图下来，然后取消再次执行命令。

这样我们根据上面图片得到了flag

```
flag{you_can_never_finish_the}
```

little tricks

下载附件得到一个ll2文件放到winhex中发现是vhdx文件。



改一下后缀挂载一下，发现是加密的。不知道密码

我们使用`bitlocker2john`查看一下

`bitlocker2john -i ll2`

得到一些哈希值

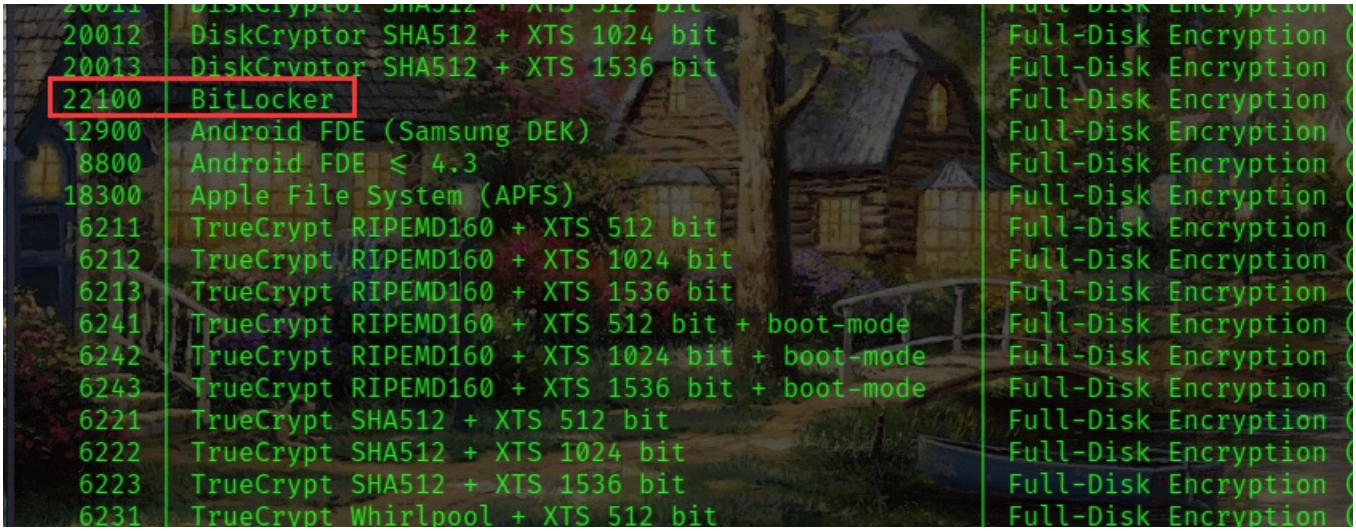
将中间一些没用的删除掉，得到以下内容

```
$bitlocker$0$16$212afe1afbb733f18b043338d85c4744$1048576$12$80ad0e8486ead60103000000$60$01c1f4b616a85eecbd9d090b
a2f0cbf5642f6591ff2abdf1df84e3fc33240b714e5fd280f03b7b4fbb8fe6f58dcea572f1258671c7d42748c76097ed
$bitlocker$1$16$212afe1afbb733f18b043338d85c4744$1048576$12$80ad0e8486ead60103000000$60$01c1f4b616a85eecbd9d090b
a2f0cbf5642f6591ff2abdf1df84e3fc33240b714e5fd280f03b7b4fbb8fe6f58dcea572f1258671c7d42748c76097ed
$bitlocker$2$16$b044a4ad4fc868f736d0baf7ef47a9ea$1048576$12$80ad0e8486ead60106000000$60$58fe021061ac9673d8925324
f7a3530433814456 79ab17420c05c408a728775c3fde50f1333b720a876dab4cc850e29078aa257dab9f4f690be0fb81
$bitlocker$3$16$b044a4ad4fc868f736d0baf7ef47a9ea$1048576$12$80ad0e8486ead60106000000$60$58fe021061ac9673d8925324
f7a3530433814456 79ab17420c05c408a728775c3fde50f1333b720a876dab4cc850e29078aa257dab9f4f690be0fb81
```

我们使用找一下对应的哈希类型

可以开到哈希类型是`$bitlocker`

```
hashcat --help
```

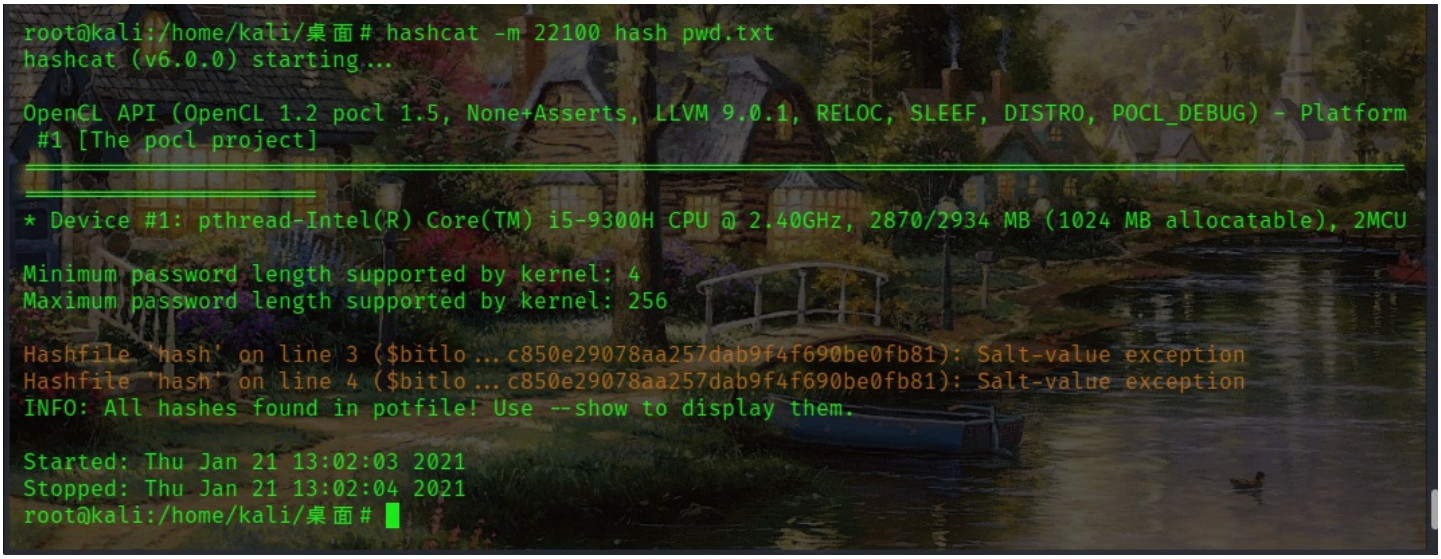


将之前跑的哈希值新建一个文件放进去。然后再找个一个弱口令的字典

使用一下命令，先执行一下

```
hashcat -m 22100 hash pwd.txt
```

> 我这是执行一遍了，所以显示这样

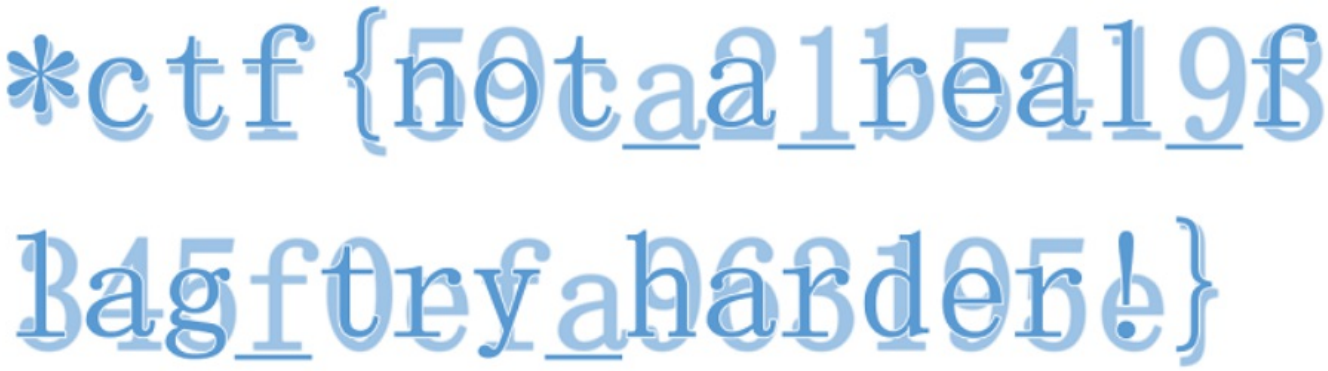


再在命令后面加上`--show`

```
hashcat -m 22100 hash pwd.txt --show
```

得到密码解密，发现里面只有一个password.txt

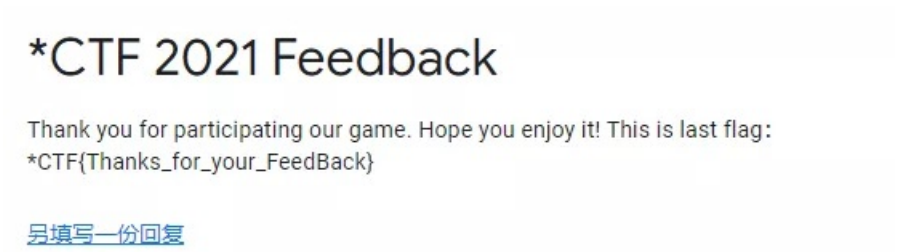
使用`DiskGenius`打开，得到两个PDF，打开大小最大的那个得到一个重叠的flag，颜色`浅`的是正确flag




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

Feedback

是个问卷，做完就给flag




```
*CTF{Thanks_for_your_FeedBack}
```