

*CTF2021 Misc部分wp

原创

置顶 [PoisOn#](#) 于 2021-01-21 14:18:42 发布 1367 收藏 4

分类专栏: [misc](#)

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/qq_49354488/article/details/112941546

版权



[misc](#) 专栏收录该内容

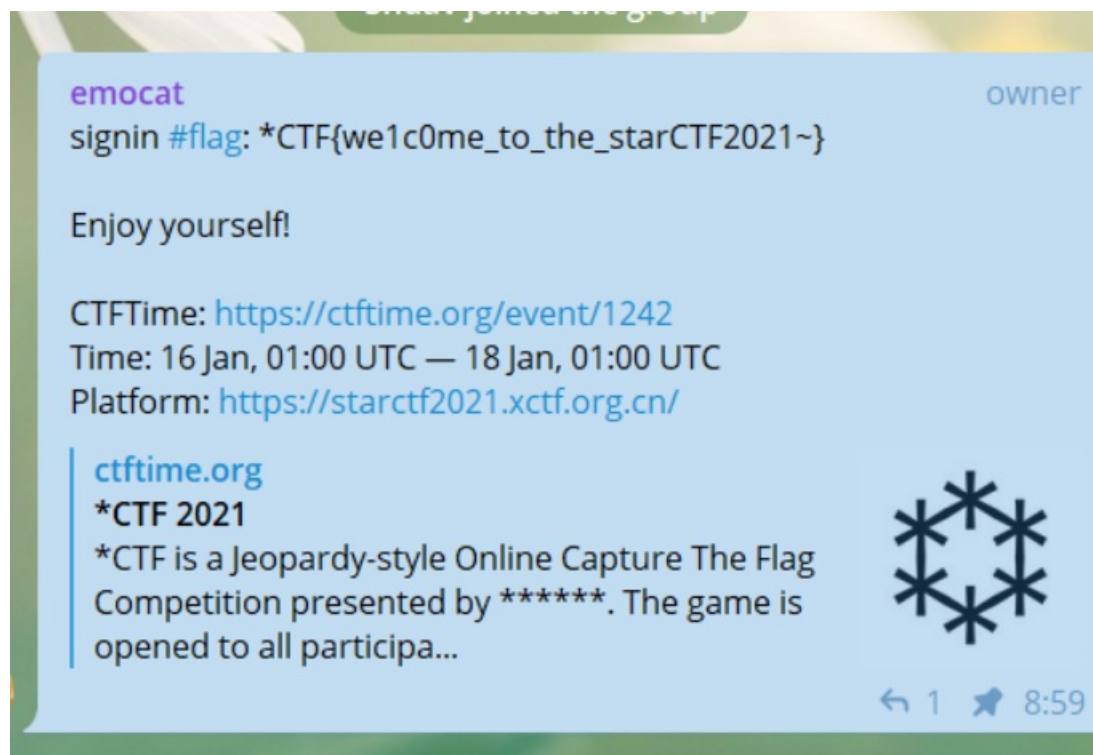
6 篇文章 0 订阅

订阅专栏

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

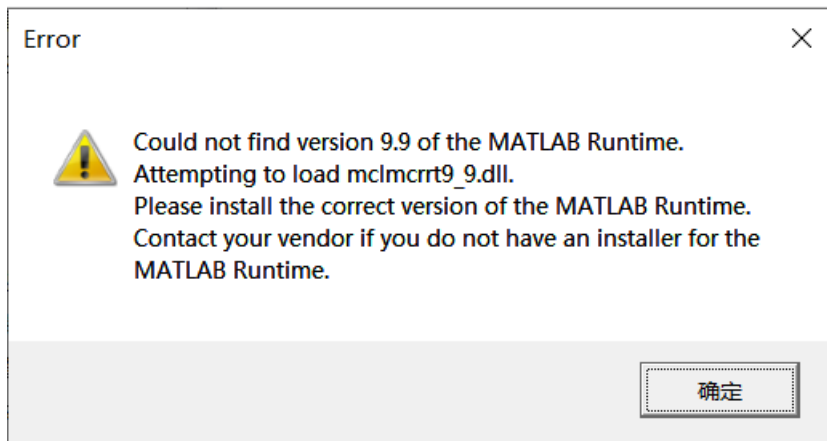
MineGame.exe

readme.txt

splash.png

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/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.

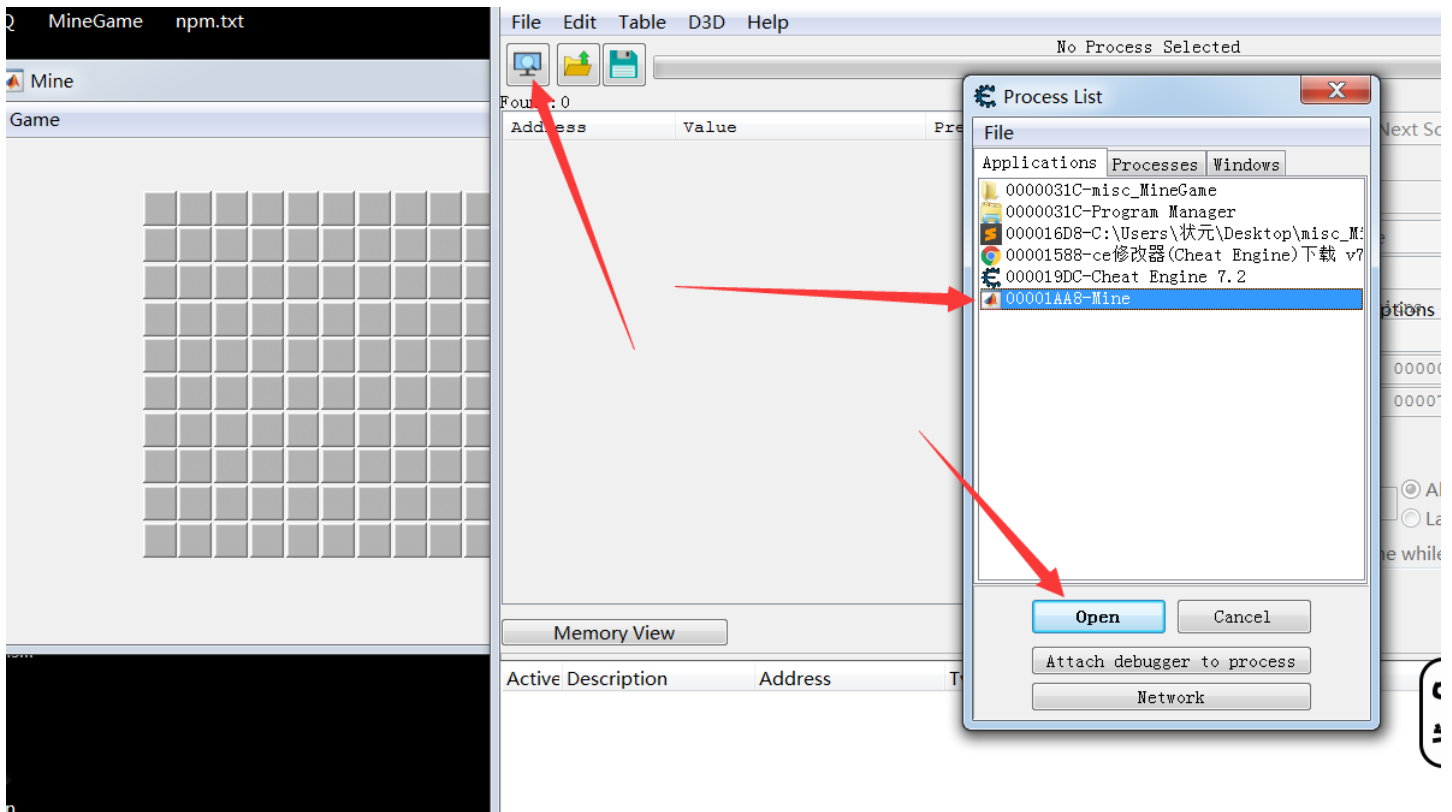
安装完后我们打开exe发现是一个扫雷，而且10后自动关闭。

我们使用 **Cheat Engine** 来打开这个进程

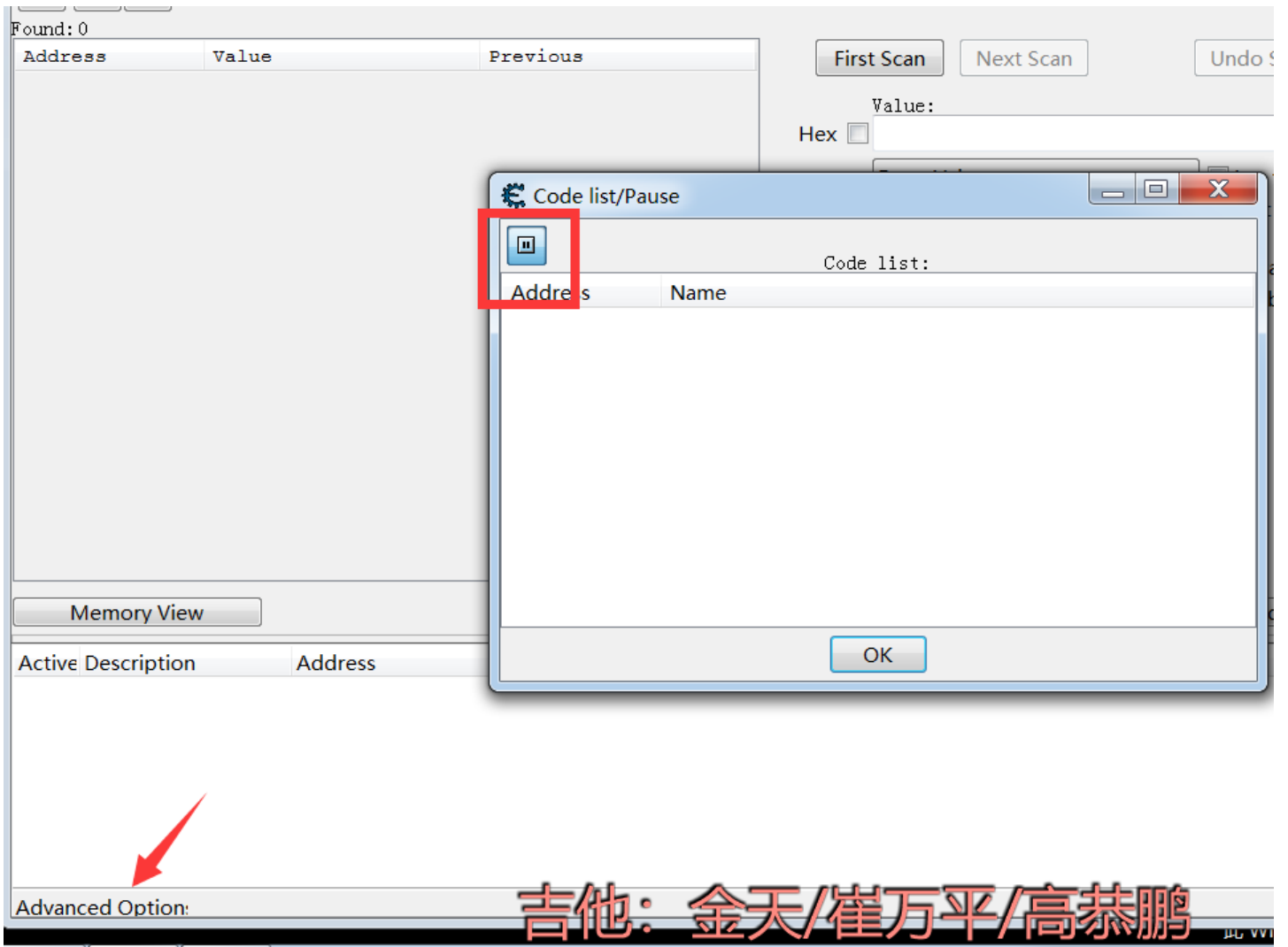
Cheat Engine 下载地址：英文版<https://www.cheatengine.org/> 中文版http://www.pc6.com/softview/SoftView_62186.html?_t_t_t=0.052645973079466335

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

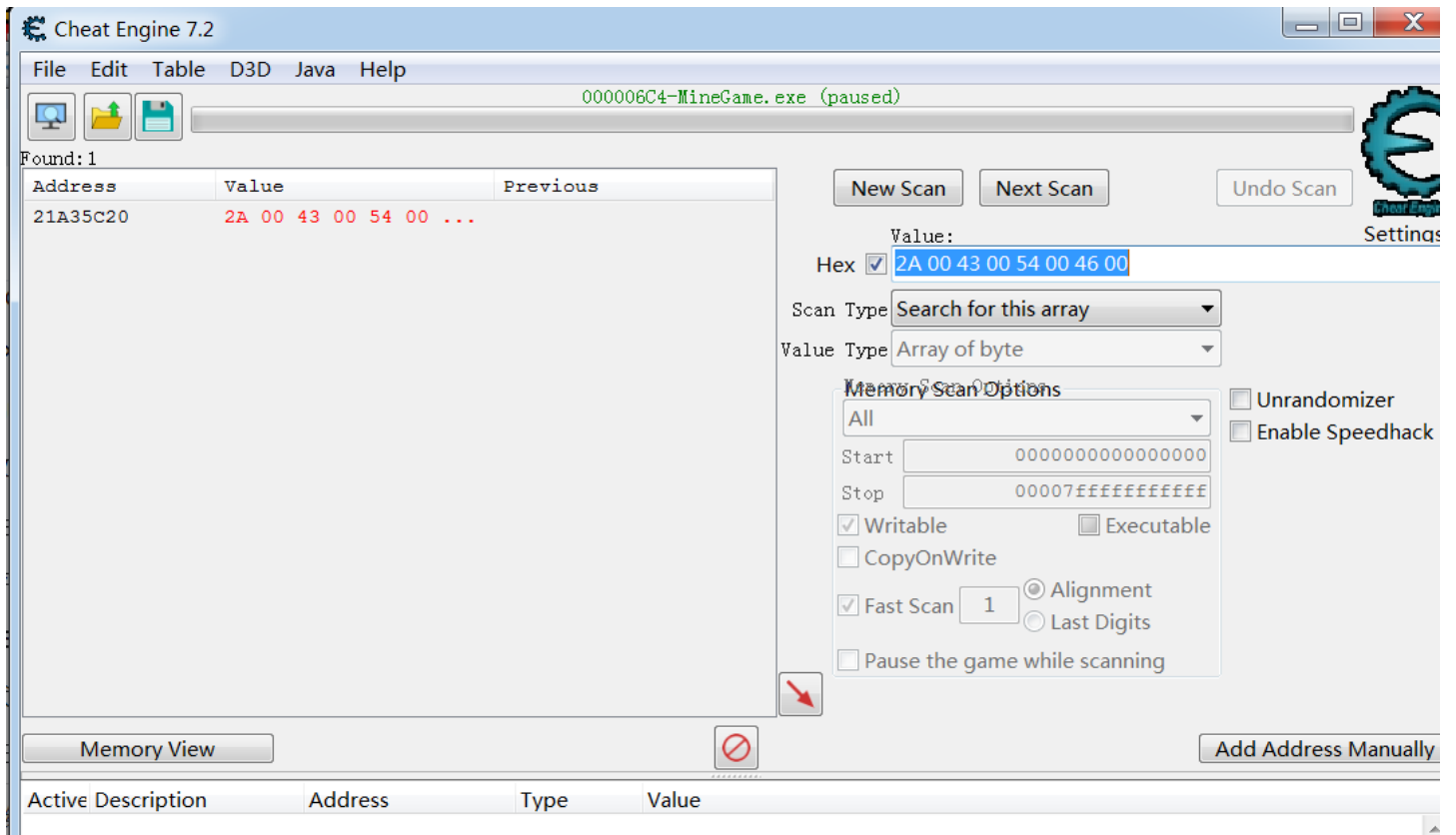
字符串: *CTF

16进制: 2A435446

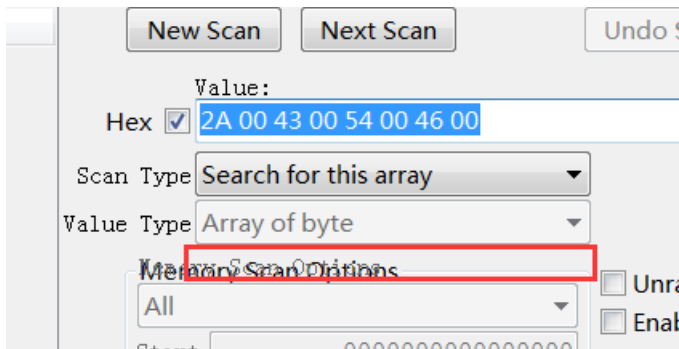
我们要将16进制写成以下格式

```
2A 00 43 00 54 00 46 00
```

然后进行 `First Scan`

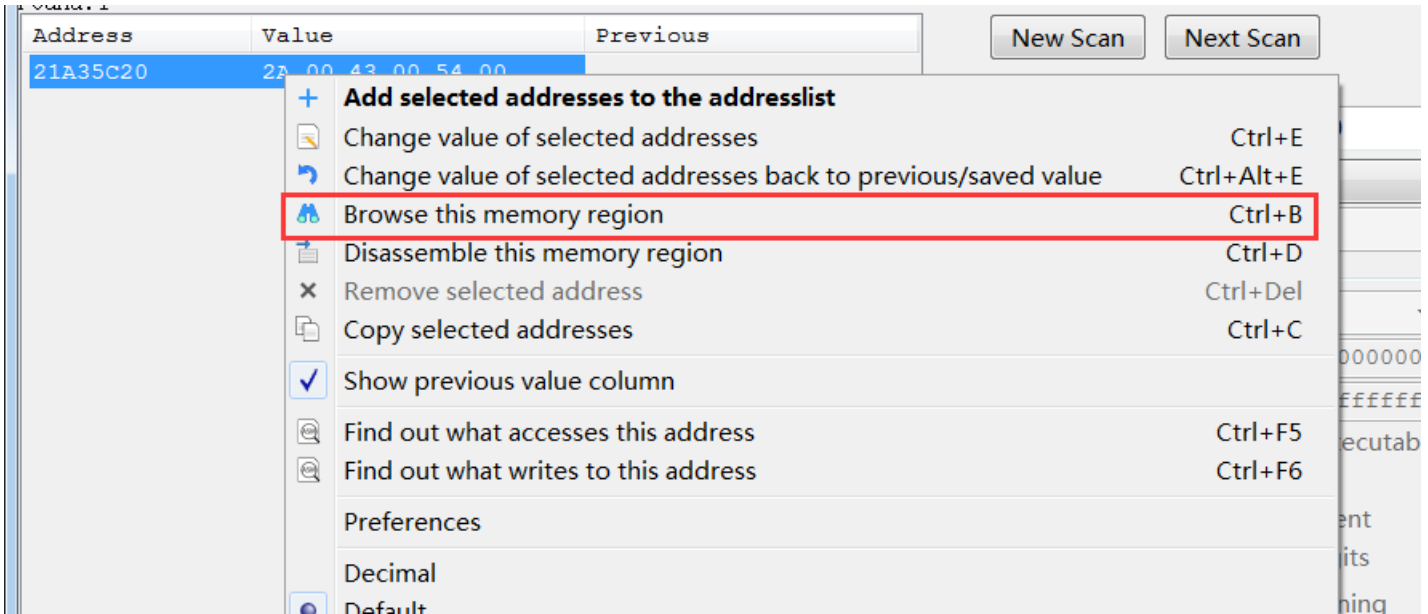


注意：如果第一次使用CE软件的话，一开始是不能更改 **Scan Tyoe** 和 **Value Type** 的，在红框的位置会有一个选框，勾选上就可以更改了，因为我们已经勾选了，所以这里不显示了。



然后我们搜索和出来一个地址

右键选择红框这个选项

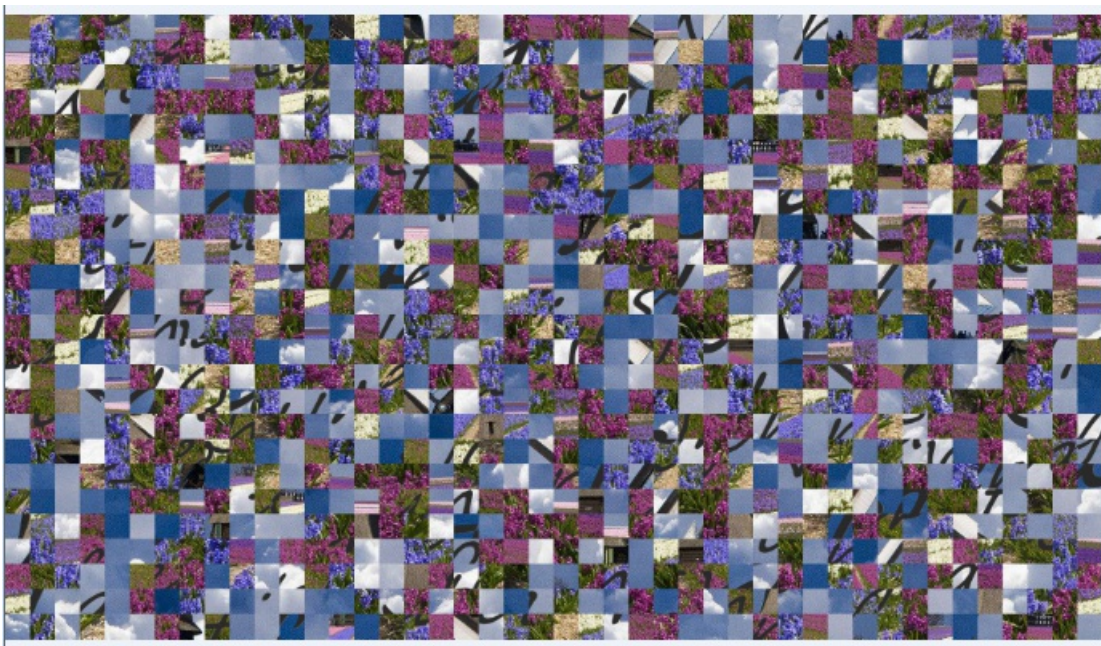


得到flag

Protect:Read/Write	AllocationBase=21410000	Base=21A35000	Size=9AB000																						
address	20	21	22	23	24	25	26	27	28	29	2A	2B	2C	2D	2E	2F	30	31	32	33	34	35	36	37	0123456789ABCDEF01234567
21A35C20	2A	00	43	00	54	00	46	00	7B	00	59	00	30	00	75	00	5F	00	34	00	31	00	65	00	*.C.T.F.{.Y.O.u.}.4.1.e.
21A35C38	2D	00	67	00	4C	00	65	00	61	00	74	00	5F	00	36	00	4F	00	79	00	33	00	21	00	-.g.L.e.a.t._.6.C.y.3.!
21A35C50	7D	00	0C	63	00	00	00	00	00	A9	C3	14	00	00	00	00	D8	F6	0C	63	00	00	00	00	}..c..... .c....
21A35C68	00	A9	C3	14	00	00	00	00	00	00	00	00	00	00	00	00	D1	48	4D	56	5A	00	00	90 hmvz...
21A35C80	40	C4	0A	ED	FE	07	00	00	00	00	00	00	00	00	00	00	C0	2B	AE	21	00	00	00	00	@ + !....
21A35C98	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	2F	00	00	00	00	00	00	00\$...../.....

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能将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I12文件放到winhex中发现是vhdx文件。

```
76 68 64 78 66 69 6C 65 4D 00 69 00 63 00 72 00 vhdxfileM i c r
6F 00 73 00 6F 00 66 00 74 00 20 00 57 00 69 00 o s o f t W i
6E 00 64 00 6F 00 77 00 73 00 20 00 31 00 30 00 n d o w s 1 0
2E 00 30 00 2E 00 31 00 38 00 33 00 36 00 33 00 . 0 . 1 8 3 6 3
2E 00 30 00 00 00 00 00 00 00 00 00 00 00 00 . 0
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

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` 看一下

```
bitlocker2john -i ll2
```

得到一些哈希值

```
User Password hash:
$bitlocker$0$16$212afe1afbb733f18b043338d85c4744$1048576$12$80ad0e8486ead60103000000$60$01c1f4b616a85ee
cbd9d090ba2f0cbf5642f6591ff2abdf1df84e3fc33240b714e5fd280f03b7b4fbb8fe6f58dcea572f1258671c7d42748c76097
ed
Hash type: User Password with MAC verification (slower solution, no false positives)
$bitlocker$1$16$212afe1afbb733f18b043338d85c4744$1048576$12$80ad0e8486ead60103000000$60$01c1f4b616a85ee
cbd9d090ba2f0cbf5642f6591ff2abdf1df84e3fc33240b714e5fd280f03b7b4fbb8fe6f58dcea572f1258671c7d42748c76097
ed
Hash type: Recovery Password fast attack
$bitlocker$2$16$b044a4ad4fc868f736d0baf7ef47a9ea$1048576$12$80ad0e8486ead60106000000$60$58fe021061ac967
3d8925324f7a353043381445679ab17420c05c408a728775c3fde50f1333b720a876dab4cc850e29078aa257dab9f4f690be0fb
81
Hash type: Recovery Password with MAC verification (slower solution, no false positives)
$bitlocker$3$16$b044a4ad4fc868f736d0baf7ef47a9ea$1048576$12$80ad0e8486ead60106000000$60$58fe021061ac967
3d8925324f7a353043381445679ab17420c05c408a728775c3fde50f1333b720a876dab4cc850e29078aa257dab9f4f690be0fb
81
root@kali:/home/kali/桌面#
```

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
f7a353043381445679ab17420c05c408a728775c3fde50f1333b720a876dab4cc850e29078aa257dab9f4f690be0fb81
$bitlocker$3$16$b044a4ad4fc868f736d0baf7ef47a9ea$1048576$12$80ad0e8486ead60106000000$60$58fe021061ac9673d8925324
f7a353043381445679ab17420c05c408a728775c3fde50f1333b720a876dab4cc850e29078aa257dab9f4f690be0fb81
```

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
```


20011	DiskCryptor SHA512 + XTS 512 bit	Full-Disk Encryption (
20012	DiskCryptor SHA512 + XTS 1024 bit	Full-Disk Encryption (
20013	DiskCryptor SHA512 + XTS 1536 bit	Full-Disk Encryption (
22100	BitLocker	Full-Disk Encryption (
12900	Android FDE (Samsung DEK)	Full-Disk Encryption (
8800	Android FDE ≤ 4.3	Full-Disk Encryption (
18300	Apple File System (APFS)	Full-Disk Encryption (
6211	TrueCrypt RIPEMD160 + XTS 512 bit	Full-Disk Encryption (
6212	TrueCrypt RIPEMD160 + XTS 1024 bit	Full-Disk Encryption (
6213	TrueCrypt RIPEMD160 + XTS 1536 bit	Full-Disk Encryption (
6241	TrueCrypt RIPEMD160 + XTS 512 bit + boot-mode	Full-Disk Encryption (
6242	TrueCrypt RIPEMD160 + XTS 1024 bit + boot-mode	Full-Disk Encryption (
6243	TrueCrypt RIPEMD160 + XTS 1536 bit + boot-mode	Full-Disk Encryption (
6221	TrueCrypt SHA512 + XTS 512 bit	Full-Disk Encryption (
6222	TrueCrypt SHA512 + XTS 1024 bit	Full-Disk Encryption (
6223	TrueCrypt SHA512 + XTS 1536 bit	Full-Disk Encryption (
6231	TrueCrypt Whirlpool + XTS 512 bit	Full-Disk Encryption (

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

```
root@kali:/home/kali/桌面# hashcat -m 22100 hash pwd.txt
hashcat (v6.0.0) starting...

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEP, DISTRO, POCL_DEBUG) - Platform
#1 [The pocl project]

-----
* Device #1: pthread-Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz, 2870/2934 MB (1024 MB allocatable), 2MCU

Minimum password length supported by kernel: 4
Maximum password length supported by kernel: 256

Hashfile 'hash' on line 3 ($bitlo...c850e29078aa257dab9f4f690be0fb81): Salt-value exception
Hashfile 'hash' on line 4 ($bitlo...c850e29078aa257dab9f4f690be0fb81): Salt-value exception
INFO: All hashes found in potfile! Use --show to display them.

Started: Thu Jan 21 13:02:03 2021
Stopped: Thu Jan 21 13:02:04 2021
root@kali:/home/kali/桌面# █
```

再在命令后面加上 `--show`

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

```
Stopped: Thu Jan 21 13:02:04 2021
root@kali:/home/kali/桌面# hashcat -m 22100 hash pwd.txt --show
Hashfile 'hash' on line 3 ($bitlo... c850e29078aa257dab9f4f690be0fb81): Salt-value exception
Hashfile 'hash' on line 4 ($bitlo... c850e29078aa257dab9f4f690be0fb81): Salt-value exception
$bitlocker$0$16$212afe1afbb733f18b043338d85c4744$1048576$12$80ad0e8486ead60103000000$60$01c1f4b616a85ee
cbd9d090ba2f0cbf5642f6591ff2abdf1df84e3fc33240b714e5fd280f03b7b4fbb8fe6f58dcea572f1258671c7d42748c76097
ed:12345678
root@kali:/home/kali/桌面#
```

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 {n0t_aa1b5419f
B4g_f0r_ya_h4r_d05e}

*ctf{59ca21b54198345f0efa963195e}

Feedback

是个问卷，做完就给flag

*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](#)

*CTF{Thanks_for_your_FeedBack}