i春秋ctf训练营writeup-Recreators

原创

Gun__ 于 2020-05-20 15:31:08 发布 501 收藏 2

文章标签： 其他

本文链接：https://blog.csdn.net/bbszhenshuai/article/details/106236813

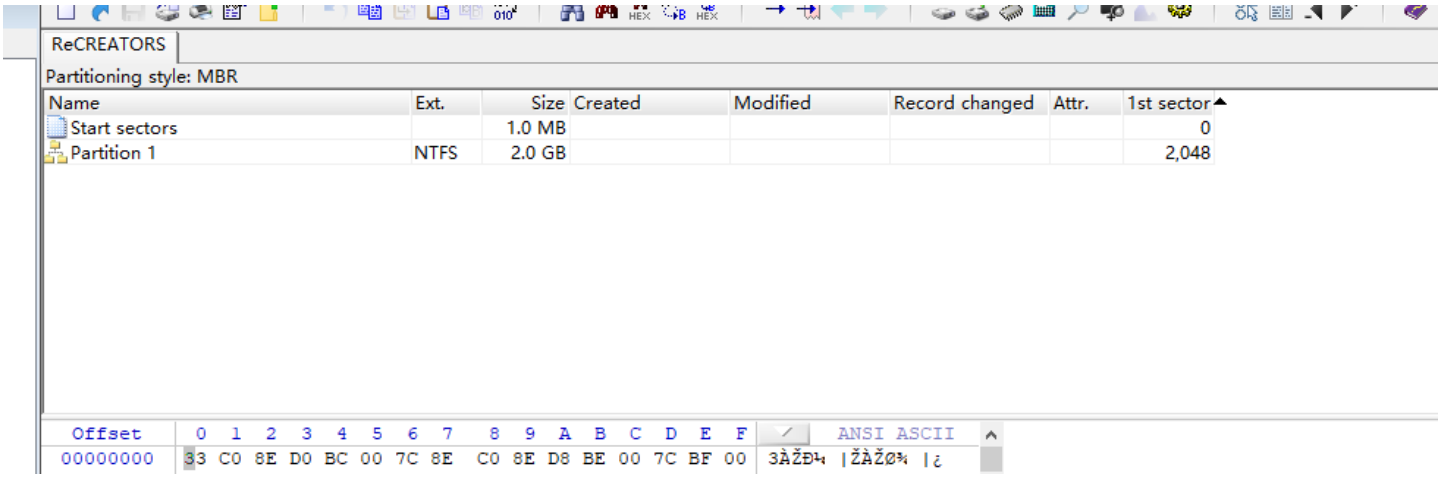
Recreators

首先下载并解压，可以看到没有拓展名

直接winhex打开看看

```
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
23 20 44 69 73 6B 20 44  65 73 63 72 69 70 74 6F  # Disk Descripto
72 46 69 6C 65 0A 76 65  72 73 69 6F 6E 3D 31 0A  rFile version=1
43 49 44 3D 30 30 32 39  34 38 32 33 0A 70 61 72  CID=00294823 par
65 6E 74 43 49 44 3D 66  66 66 66 66 66 66 66 0A  entCID=ffffffff
63 72 65 61 74 65 54 79  70 65 3D 22 6D 6F 6E 6F  createType="mono
6C 69 74 68 69 63 53 70  61 72 73 65 22 0A 0A 23  lithicSparse"  #
20 45 78 74 65 6E 74 20  64 65 73 63 72 69 70 74   Extent descript
69 6F 6E 0A 52 57 20 34  31 39 34 33 30 34 20 53  ion RW 4194304 S
50 41 52 53 45 20 22 6D  69 73 63 2E 76 6D 64 6B  PARSE "misc.vmdk
22 0A 0A 23 20 54 68 65  20 44 69 73 6B 20 44 61  "  # The Disk Da
74 61 20 42 61 73 65 20  0A 23 44 44 42 0A 0A 64  ta Base  #DDB  d
64 62 2E 76 69 72 74 75  61 6C 48 57 56 65 72 73  db.virtualHWVers
69 6F 6E 20 3D 20 22 36  22 0A 64 64 62 2E 67 65  ion = "6" ddb.ge
6F 6D 65 74 72 79 2E 63  79 6C 69 6E 64 65 72 73  ometry.cylinders
20 3D 20 22 32 36 31 22  0A 64 64 62 2E 67 65 6F   = "261" ddb.geo
6D 65 74 72 79 2E 68 65  61 64 73 20 3D 20 22 32  metry.heads = "2
35 35 22 0A 64 64 62 2E  67 65 6F 6D 65 74 72 79  55" ddb.geometry
2E 73 65 63 74 6F 72 73  20 3D 20 22 36 33 22 0A  .sectors = "63"
64 64 62 2E 61 64 61 70  74 65 72 54 79 70 65 20  ddb.adapterType
3D 20 22 69 64 65 22 0A  00 00 00 00 00 00 00 00  = "ide"
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```


由这里可以看出该文件应该是一个VMware虚拟磁盘镜像，那么修改拓展名为.vmdk，再用winhex打开。



```
00000010  06 B9 00 02 FC F3 A4 50  68 1C 06 CB FB B9 04 00   ¹  üó¤Ph  Ëû¹
00000020  BD BE 07 80 7E 00 00 7C  0B 0F 85 0E 01 83 C5 10  ½¾ €~  |  …  ƒÅ
00000030  E2 F1 CD 18 88 56 00 55  C6 46 11 05 C6 46 10 00  âñÍ ˆV UÆF  ÆF
00000040  B4 41 BB AA 55 CD 13 5D  72 0F 81 FB 55 AA 75 09  ´A»ªUÍ ]r  ûUªu
00000050  F7 C1 01 00 74 03 FE 46  10 66 60 80 7E 10 00 74  ÷Á  t þF f`€~  t
00000060  26 66 68 00 00 00 00 66  FF 76 08 68 00 00 68 00  &fh     fÿv h  h
00000070  7C 68 01 00 68 10 00 B4  42 8A 56 00 8B F4 CD 13  |h  h  ´BŠV ‹ôÍ
00000080  9F 83 C4 10 9E EB 14 B8  01 02 BB 00 7C 8A 56 00  ŸƒÄ žë ¸  » |ŠV
00000090  8A 76 01 8A 4E 02 8A 6E  03 CD 13 66 61 73 1C FE  Šv ŠN Šn Í fas þ
000000A0  4E 11 75 0C 80 7E 00 80  0F 84 8A 00 B2 80 EB 84  N u €~ € „Š ²€ë„
000000B0  55 32 E4 8A 56 00 CD 13  5D EB 9E 81 3E FE 7D 55  U2äŠV Í ]ëž >þ}U
000000C0  AA 75 6E FF 76 00 E8 8D  00 75 17 FA B0 D1 E6 64  ªunÿv è  u ú°Ñæd
000000D0  E8 83 00 B0 DF E6 60 E8  7C 00 B0 FF E6 64 E8 75  èƒ °ßæ`è| °ÿædèu
000000E0  00 FB B8 00 BB CD 1A 66  23 C0 75 3B 66 81 FB 54  û¸ »Í f#Àu;f ûT
000000F0  43 50 41 75 32 81 F9 02  01 72 2C 66 68 07 BB 00  CPAu2 ù  r,fh »
00000100  00 66 68 00 02 00 00 66  68 08 00 00 00 66 53 66   fh    fh    fSf
00000110  53 66 55 66 68 00 00 00  00 66 68 00 7C 00 00 66  SfUfh    fh |  f
00000120  61 68 00 00 07 CD 1A 5A  32 F6 EA 00 7C 00 00 CD  ah   Í Z2öê |  Í
00000130  18 A0 B7 07 EB 08 A0 B6  07 EB 03 A0 B5 07 32 E4   · ë ¶ ë  µ 2ä
00000140  05 00 07 8B F0 AC 3C 00  74 09 BB 07 00 B4 0E CD    ‹ð¬< t »  ´ Í
00000150  10 EB F2 F4 EB FD 2B C9  E4 64 EB 00 24 02 E0 F8  ëòôëý+Éädë $ àø
00000160  24 02 C3 49 6E 76 61 6C  69 64 20 70 61 72 74 69  $ ÃInvalid parti
00000170  74 69 6F 6E 20 74 61 62  6C 65 00 45 72 72 6F 72  tion table Error
00000180  20 6C 6F 61 64 69 6E 67  20 6F 70 65 72 61 74 69   loading operati
00000190  6E 67 20 73 79 73 74 65  6D 00 4D 69 73 73 69 6E  ng system Missin
000001A0  67 20 6F 70 65 72 61 74  69 6E 67 20 73 79 73 74  g operating syst
000001B0  65 6D 00 00 00 63 7B 9A  E2 6B 64 58 00 00 80 20  em   c{šâkdX  €
000001C0  21 00 07 15 50 05 00 08  00 00 00 F8 3F 00 00 00  !   P       ø?
```

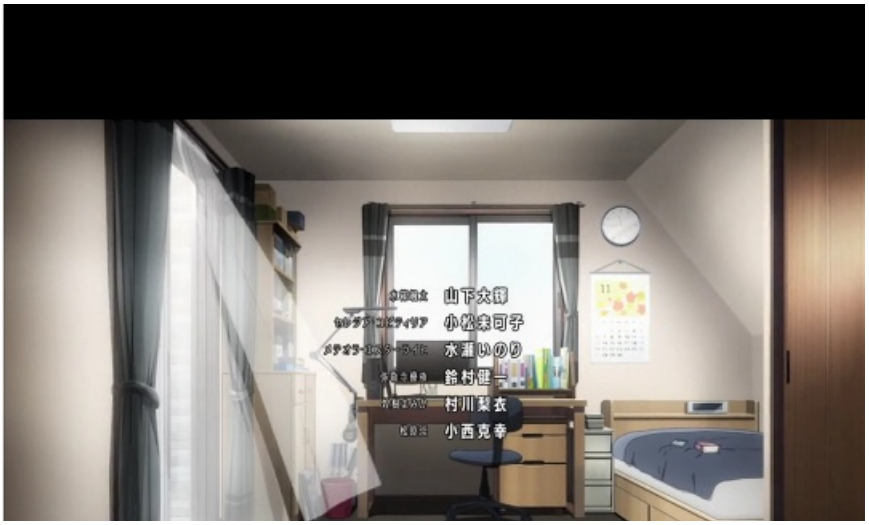

可以看到，winhex是由对vmdk格式的解析的。

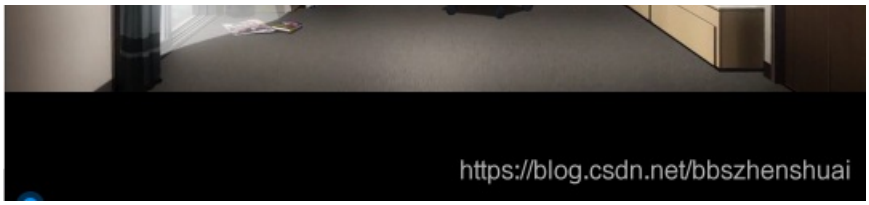
ReCREATORS | ReCREATORS, P1

\

Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
$Extend		344 B	2017/05/22 20:4...	2017/05/22 20:4...	2017/05/22 20:4...	SH	1,397,438
(Root directory)		4.1 KB	2017/05/22 20:4...	2017/05/22 20:4...	2017/05/22 20:4...	SH	2,122,000
$AttrDef		2.5 KB	2017/05/22 20:4...	2017/05/22 20:4...	2017/05/22 20:4...	SH	2,121,216
$BadClus		0 B	2017/05/22 20:4...	2017/05/22 20:4...	2017/05/22 20:4...	SH	1,397,432
$Bitmap		64.0 KB	2017/05/22 20:4...	2017/05/22 20:4...	2017/05/22 20:4...	SH	24
$Boot		8.0 KB	2017/05/22 20:4...	2017/05/22 20:4...	2017/05/22 20:4...	SH	0
$LogFile		12.3 MB	2017/05/22 20:4...	2017/05/22 20:4...	2017/05/22 20:4...	SH	2,096,120
$MFT		32.0 KB	2017/05/22 20:4...	2017/05/22 20:4...	2017/05/22 20:4...	SH	1,397,416
$MFTMirr		4.0 KB	2017/05/22 20:4...	2017/05/22 20:4...	2017/05/22 20:4...	SH	16
$Secure		0 B	2017/05/22 20:4...	2017/05/22 20:4...	2017/05/22 20:4...	SH	
$UpCase		128 KB	2017/05/22 20:4...	2017/05/22 20:4...	2017/05/22 20:4...	SH	2,121,744
$Volume		0 B	2017/05/22 20:4...	2017/05/22 20:4...	2017/05/22 20:4...	SH	1,397,422
misc.mp4	mp4	13.1 MB	2017/05/22 20:4...	2017/05/22 20:4...	2017/05/22 20:4...	A	2,122,008
Free space (net)		2.0 GB					
Idle space		?					
Misc non-resident attributes		4.0 KB					2,121,208
Volume slack		4.0 KB					4,192,248

打开可以看到这些内容，带$的都是系统文件，肯定先看misc.mp4
保存出来，打开看看





经典动漫recreator的ED。来到了隐写的部分

此时一般思路是使用binwalk之类的看看有没有附加的东西，或者直接拿16进制编辑器看看，我选择了后者，因为前面都是视屏内容，我们从后往前看。

```
00D0C5F0  00 83 80 00 00 03 00 00  03 00 00 03 00 00 03 00  ƒ€
00D0C600  33 34 34 31 33 34 34 31  33 34 33 38 33 34 33 35  3441344134383435
00D0C610  33 35 33 35 33 35 33 32  33 35 33 33 33 34 34 35  3535353235333445
00D0C620  33 34 34 32 33 35 34 31  33 34 34 31 33 35 33 35  3442354134413535
00D0C630  33 33 33 34 33 35 33 33  33 33 33 32 33 34 34 36  3334353333323446
00D0C640  33 34 34 31 33 34 34 35  33 34 33 33 33 35 33 35  3441344534333535
00D0C650  33 33 33 32 33 35 33 36  33 34 33 33 33 35 33 34  3332353634333534
00D0C660  33 34 34 31 33 35 34 31  33 34 33 34 33 35 33 35  3441354134343535
00D0C670  33 35 33 35 33 35 33 34  33 34 33 33 33 34 33 36  3535353434333436
00D0C680  33 34 34 32 33 33 33 35  33 34 34 33 33 34 33 36  3442333534433436
00D0C690  33 34 33 37 33 35 33 36  33 34 33 33 33 34 34 33  3437353634333443
00D0C6A0  33 34 34 32 33 35 34 31  33 34 33 34 33 34 33 35  3442354134343435
00D0C6B0  33 34 34 34 33 35 33 36  33 34 34 32 33 35 33 34  3444353634423534
00D0C6C0  33 34 33 39 33 34 34 35  33 34 34 33 33 35 33 35  3439344534433535
00D0C6D0  33 35 33 35 33 35 33 36  33 35 33 33 33 34 34 32  3535353635333442
00D0C6E0  33 34 33 39 33 35 34 31  33 34 33 34 33 35 33 36  3439354134343536
00D0C6F0  33 34 33 35 33 35 33 35  33 33 33 32 33 35 33 31  3435353533323531
00D0C700  33 34 33 39 33 33 33 35  33 34 34 33 33 34 33 35  3439333534433435
00D0C710  33 34 34 34 33 35 33 36  33 34 34 32 33 34 34 35  3444353634423445
00D0C720  33 34 34 32 33 35 33 36  33 34 33 36 33 34 33 36  3442353634363436
00D0C730  33 34 34 32 33 35 33 33  33 34 34 32 33 34 34 36  3442353334423446
00D0C740  33 34 34 31 33 34 34 35  33 34 33 33 33 35 33 36  3441344534333536
00D0C750  33 34 34 36 33 35 33 35  33 33 33 32 33 35 33 34  3446353533323534
00D0C760  33 34 34 32 33 33 33 35  33 34 33 36 33 35 33 36  3442333534363536
00D0C770  33 34 33 35 33 35 33 32  33 35 33 33 33 35 33 37  3435353235333537
00D0C780  33 34 33 39 33 35 33 36  33 34 34 31 33 35 33 34  3439353634413534
00D0C790  33 34 33 35 33 35 33 36  33 33 33 32 33 34 34 32  3435353633323442
00D0C7A0  33 34 34 31 33 35 34 31  33 34 33 36 33 34 33 35  3441354134363435
00D0C7B0  33 34 34 32 33 35 33 32  33 34 34 32 33 35 33 33  3442353234423533
00D0C7C0  33 34 34 31 33 34 34 31  33 34 34 32 33 35 33 35  3441344134423535
00D0C7D0  33 35 33 39 33 35 33 32  33 35 33 33 33 34 33 38  3539353235333438
00D0C7E0  33 34 33 39 33 35 33 35  33 35 34 31 33 34 33 36  3439353535413436
00D0C7F0  33 34 33 37 33 35 33 33  33 33 33 32 33 35 33 37  3437353333323537
00D0C800  33 34 34 31 33 35 33 32  33 34 33 34 33 34 33 35  3441353234343435
00D0C810  33 35 33 39 33 35 33 32  33 34 34 32 33 35 33 34  3539353234423534
```

在某个位置发现了很奇怪的东西，全整下来，一顿操作，得到flag

具体步骤是

hex解码

hex解码

base32解码

base32解码

base32解码

base64解码

base64解码

hex解码

base32解码

base64解码

base64解码

```
#! python2
import base64
a="3441344134383435353535323533344534423541344135353343533333234463441344534333535333235363433353434413541343435
```

```
53535353534343334363442333534433436343735363433344334423541343434353444353634423534343934453443335353535353635333
44234393541343435363435353533323531343933353443343534443536344234453442353634363436344235333442344634413445343333
53634463535333235343442333534363536343535323533353734393536344135343435353633323442344135413436343534423532342333
53334413441344235353539353235333438343935353541343634373533333235373441353234343435353935323442353434413535354133
43534393533354135363439353634433436344235353523533344233353436343533343533343335363442333534413436343735343433333
44434413441343434363442353434423533344134453442353534463533353333444344235363441353634463535333234443441353234323
43535333536353334453442344435413436353135333533344634393541343335363442353535323533344135323434353535353534353333
43734413536344135353537353633323442344234413433343534423553332353634413445344234353537353435333437344235413442333
53634353531333234383441344534433435533353634333436344235413436353533363533333234442343935413433353533323536343333
44334423536343634353334353234333436344133353443343634373537353334433443344134343436344435343442352343735363444333
43535353533344135333442353634443536343535333332444343933335343535363535363533353434423444354134363437353335333333
53734393536343335353437353635333442344234453436353535353333433343634373441343735363437353635333442344235413436373
43534393532344235383441344534393435353335333533343634393541343735363439353333323534344134453438343534443536344233
53434423541344135353539353334413536344135363443343535373536344135333443343234363435353535343433343634393335344333
43534373536343334433443344134343436344435343332353534393445343235353539353235333434344235323437353634443535333323
53534413436344534353439353634423436344135353541343634463533353334373439333534423535344635363441353334413532343633
43635353532353334363441344534413534343535343332344234413541343334363442353633323534344234453437343535333535635333
43834423541343535353332344435333438344134413445343535353523442353834423335343235363439353333323332343944534333333
53635333535354135333441344534363436343535313332353543935363442353634373536343334423441354134343436344435343442333
53534393445343435353537353234413533343935363434353634423531333234443441353234363435343535363533353034423541344533
43634443532333234423441353234333534343935363442353434413445343535363535353334333537344134453442343534373534434233
44134373536343734353442353334423533344234453436343535373537353334333442353634343536343735353533353734413445344233
43535393536353335343442353634413536343735333541353634393541344334353442353635323533343933353435353634443534343333
43734393333534423436343735343433344433442354134373536344435353442353234373441344335353573534353334453442353533323
43634423535333234413441344534453435343735363533344534423445344135363435353335323553437344134423536344635535533333
43434393532343635363444353335333536343735413442343535373536333234423441354134363535344235363332353734423445345373
43535393531353334373442354134333536343335353332343834413435333235353332353634423541344235323432353535313533344233
53634433441344235353332353533323442344234453434353535353534343335363442344534433536343735333433344334433443441343433
43634423445343335353439344534413535353535343533344434393541343735363444353335333536344134453439353635353532353333
53034423444354134363446353335334446344135363434343534373536353335343439353234373435344435333433353634393536344233
43534373532353334383441344134373435344235363442353734423445343634353539353335333437344235413437353634373533333233
53434413445343834353535353634423538344233353441355353439353333323533343934413442353434393536344135333442354134363
43635353533353334363443343634413435353735343533344334423441343434363442353433323534344134443541343535393535235333
44434393535354134363444353533323435344134413438343534443532343334433442344534413553544635333533344534433441343333
43534463536333234343441353234363535353535343433353634413536344134353537353635333443344135413435343534423536333233
53734413445344534353537353535333438344235413437353634333444353335373441344134343435344435323442353234423439354133
43535393532333234463439344134433435333235353532353334393445343634353334353234333537344133353443343535373536344233
44334413541343434353444353434423534343734413442353535333534344135333439353634433536344435353332344534413436343633
43535373536344234433441354134413536344635333332344634393532344235363437353635333533442353634353536353535323442333
53734413335344134353437353535333442344134353541343634423536344235333442344534373435353535363533343434393541341333
53634374344435333538344134411344334353442353234423434344235413436343634373533333234423439354134433435343735363332
44334393536343635353332344535333535343734413439343535333534034393344"
b=a.decode('hex')
# print b
c=b.decode('hex')
# print c
d=base64.b32decode(c)
# print d
e=base64.b32decode(d)
# print(e)
f=base64.b32decode(e)
# print(f)
g=base64.b64decode(f)
# print(g)
h=base64.b64decode(g)
# print(h)
i=h.decode('hex')
# print(i)
j=base64.b32decode(i)
```

```
# print(j)
k=base64.b64decode(j)
# print(k)
l=base64.b64decode(k)
print(l)
```

后记

python2的hex转换还是比python3来的好，为什么python2不给耍了呢？？？