Misc之数据分析篇BUU

原创

half~ 已于 2022-04-13 20:34:33 修改 1666 收藏

分类专栏： Ctf 文章标签： 安全

于 2022-04-12 14:48:21 首次发布

Misc之数据分析篇BUU

easycap

follow tcp stream

大流量分析（一）

统计Statistics

大流量分析（二）

smtp

wireshark

http.request.method==POST

被嗅探的流量

http

tcp追踪流

数据包中的线索

base64转图片

荷兰宽带数据泄露

[ACTF新生赛2020]NTFS数据流

磁盘取证

小易的U盘

foremost

IDA

[RCTF2019]disk

strings

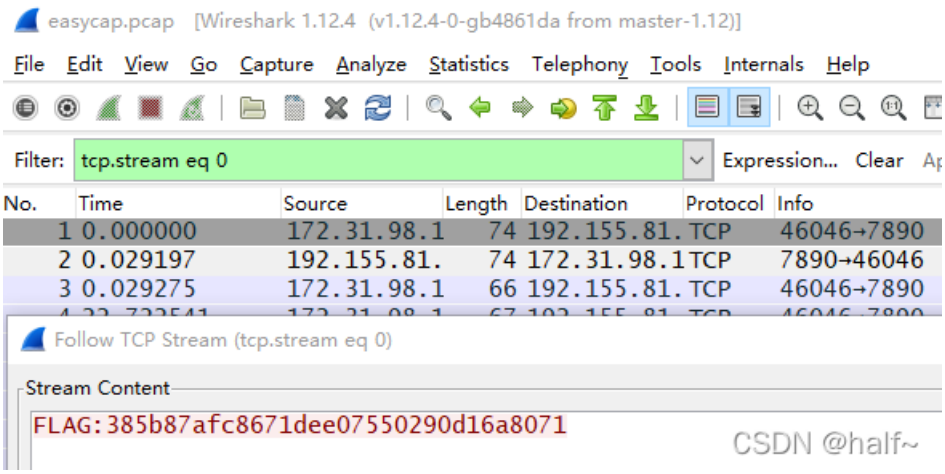
7-ZIP解压vmdk

VeraCrypt挂载

winhex

easycap

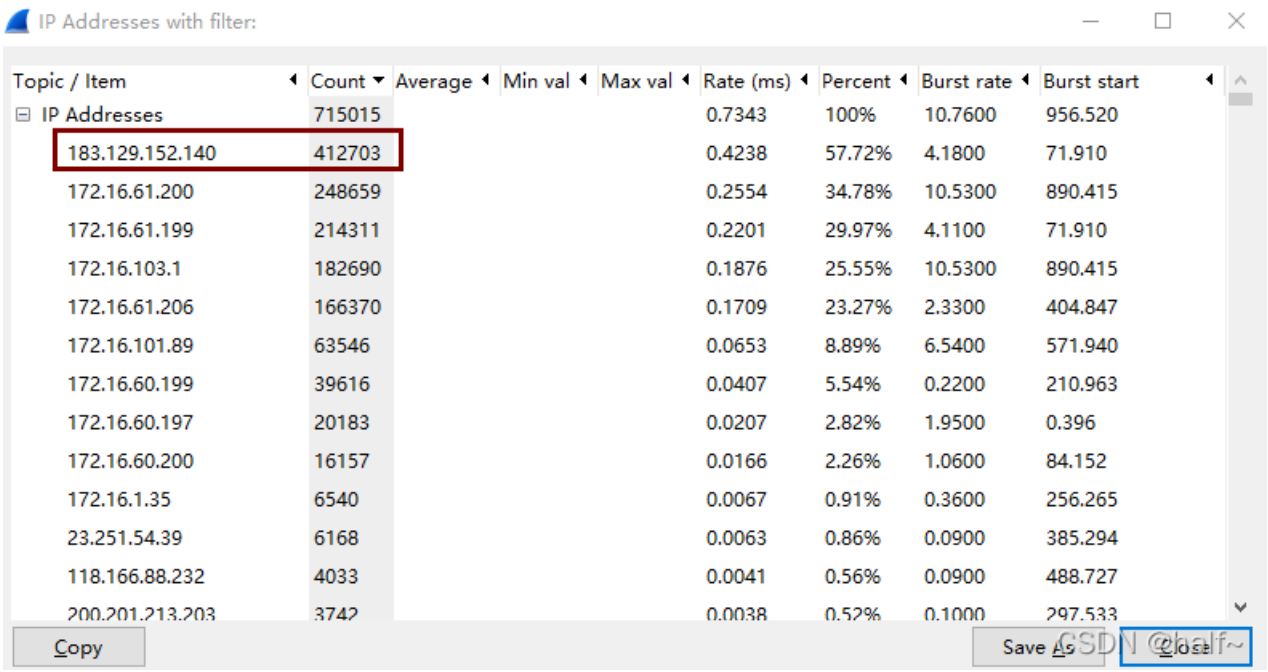
follow tcp stream



大流量分析（一）

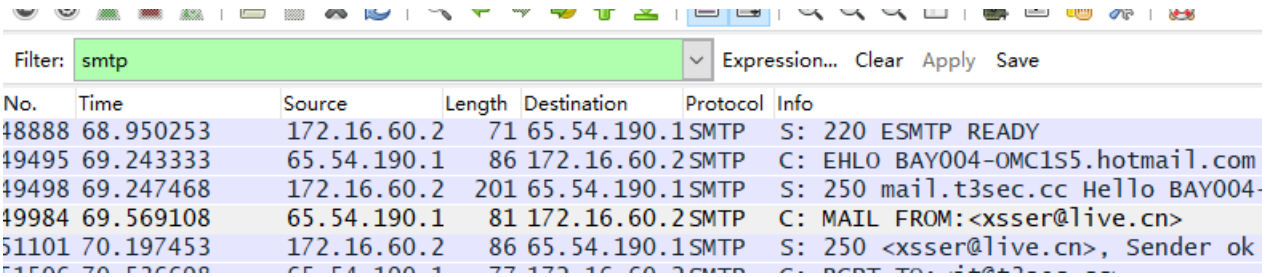
统计Statistics

Statistics–ipStatistics–ipaddresses



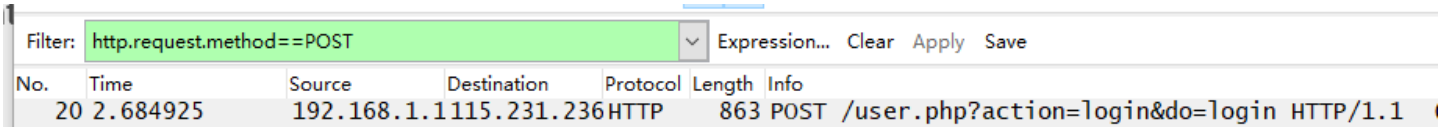
大流量分析（二）

smtp



wireshark

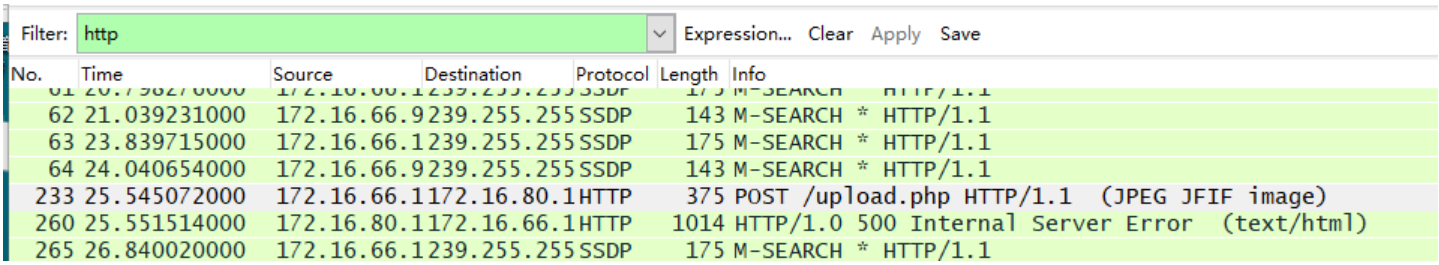
http.request.method==POST



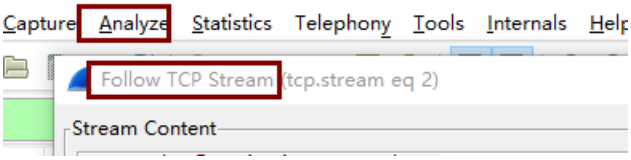

```
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "email" = "flag"
     Key: email
     Value: flag
  Form item: "password" = "ffb7567a1d4f4abdffdb54e022f8facd"
     Key: password
     Value: ffb7567a1d4f4abdffdb54e022f8facd
```

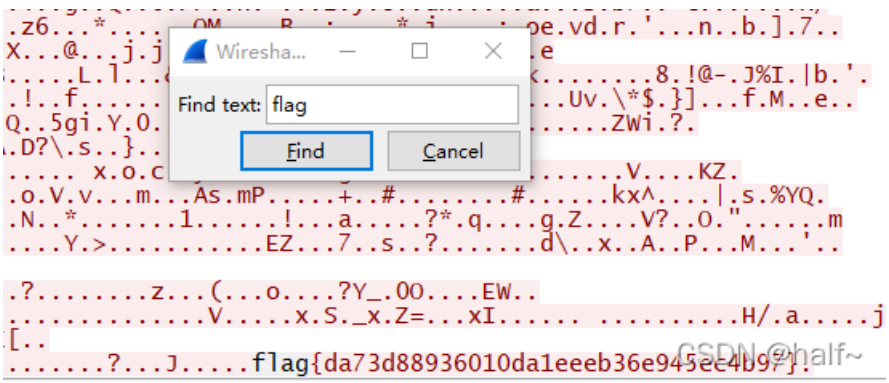
被嗅探的流量

http



tcp追踪流

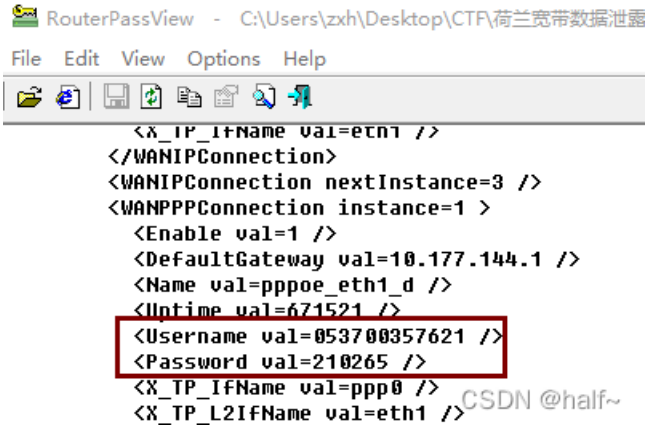




数据包中的线索

base64转图片

荷兰宽带数据泄露

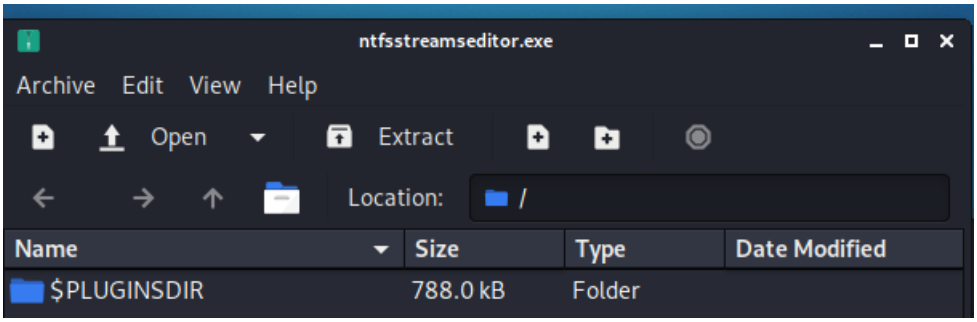


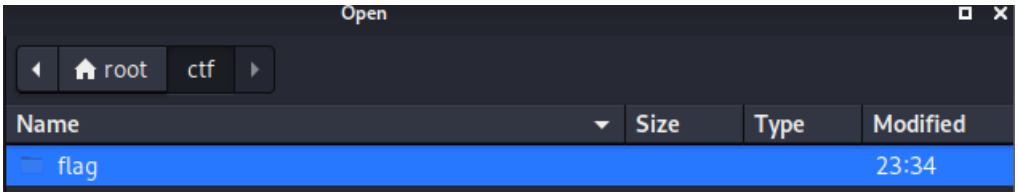
[ACTF新生赛2020]NTFS数据流

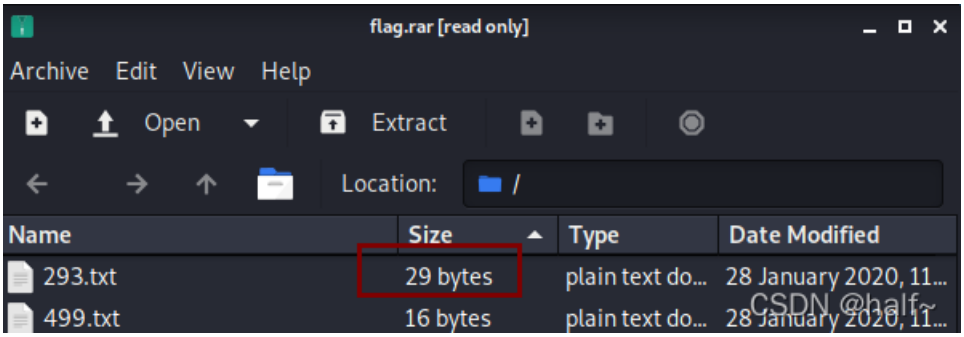
NTFS数据流
是NTFS磁盘格式的一个特性，在NTFS文件系统下，每个文件都可以存在多个数据流。

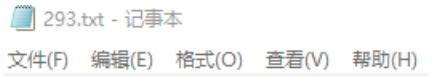
磁盘取证

ntfsstreamseditor

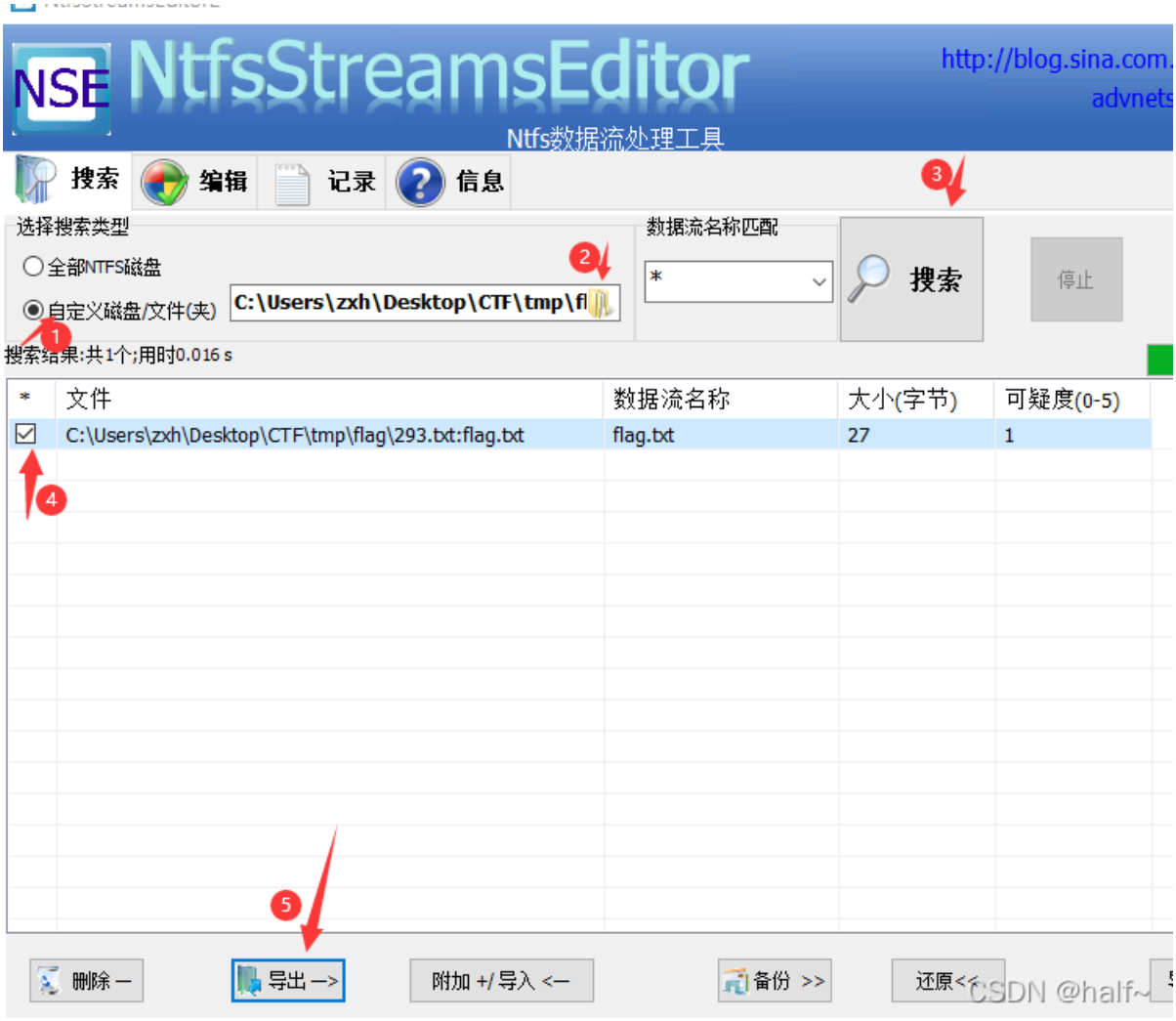








flag就在这里哦，找找看吧ADS:)

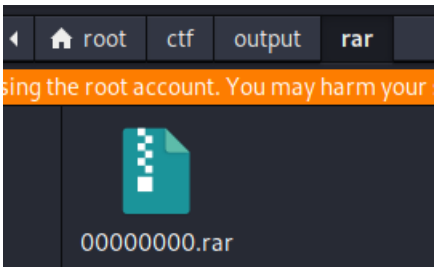


ACTF{AAAds_nntfs_ffunn?}

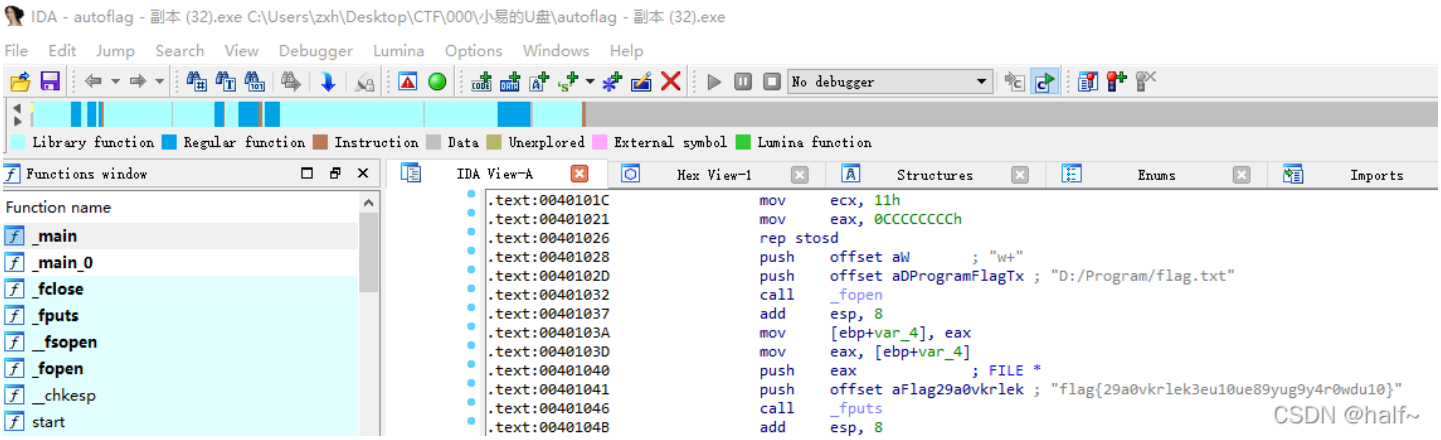
小易的U盘

foremost

```
┌──(root💀kali)-[~/ctf]
└─# apt-get install foremost
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
```



IDA



[RCTF2019]disk

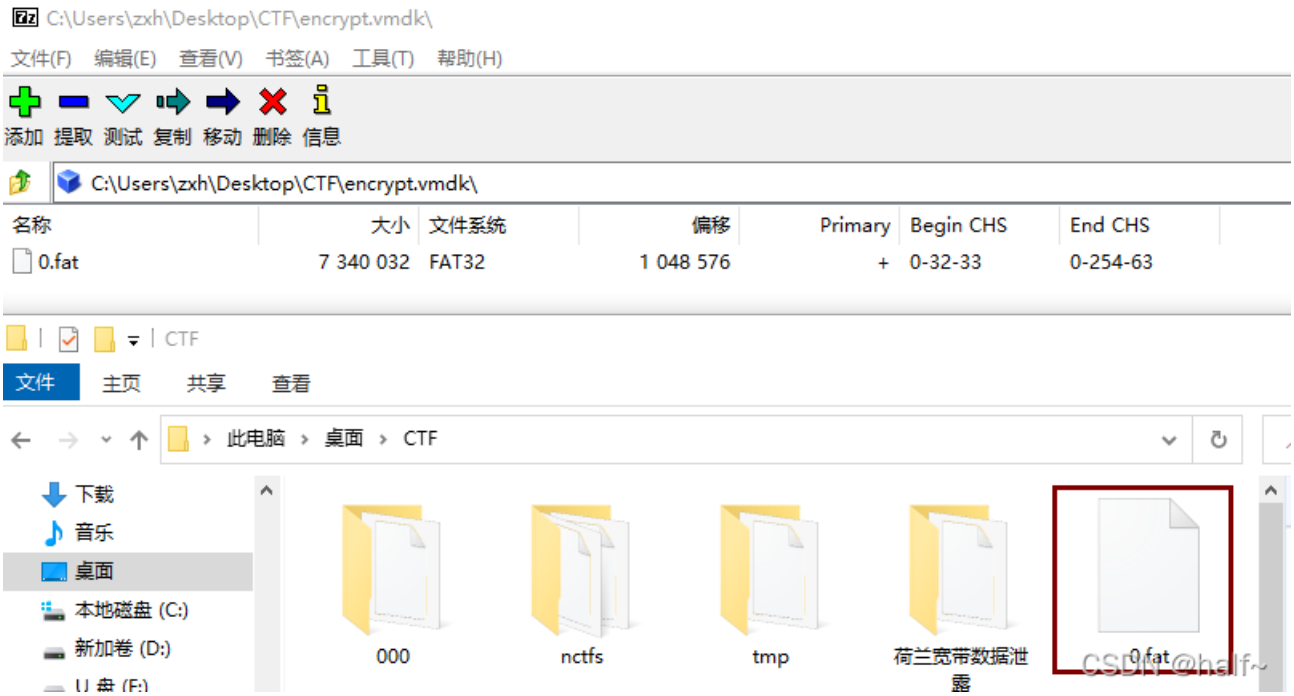
strings

```
┌──(root💀kali)-[~/ctf]
└─# strings encrypt.vmdk|grep ctf
ure_quick_form4t_vo1umerctf{unseCure_quick_form4t_vo1umerctf{unseCure_quick_f
orm4t_vo1umerctf{unseCure_quick_form4t_vo1umerctf{unseCure_quick_form4t_vo1um
erctf{unseCure_quick_form4t_vo1umerctf{unseCure_quick_form4t_vo1umerctf{unseC
```

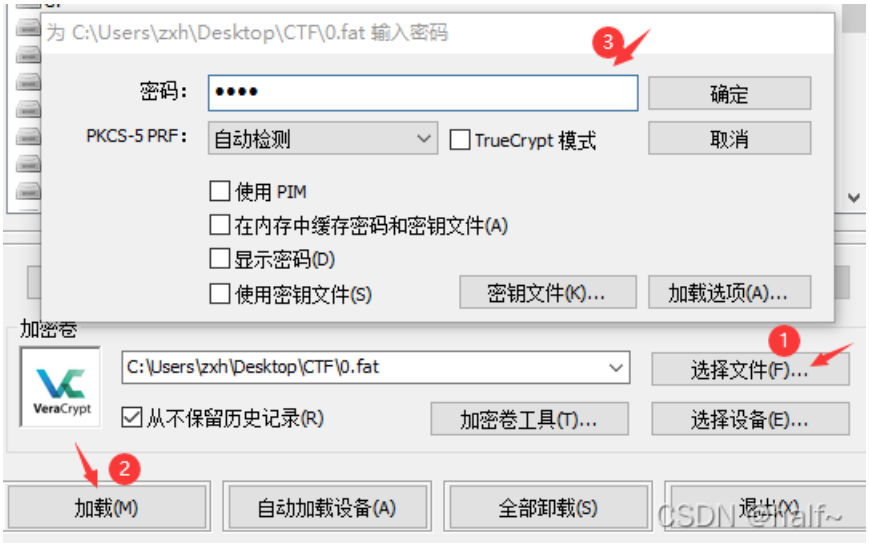
得到一些

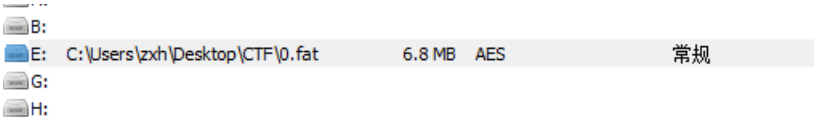
rctf{unseCure_quick_form4t_vo1ume

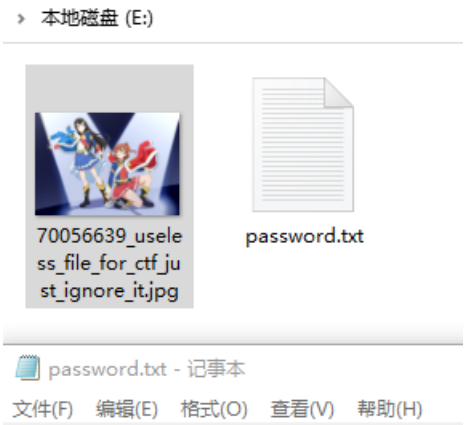
7-ZIP解压vmdk



VeraCrypt挂载





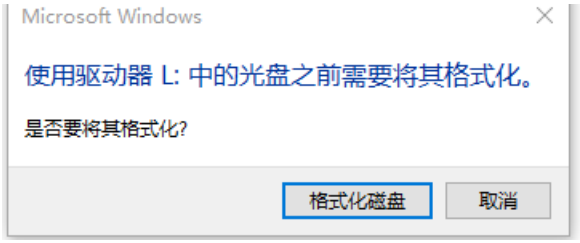


Password 2: RCTF2019

You're late... So sad

出现了一个新密码，不同的密码可以进入不同的文件系统

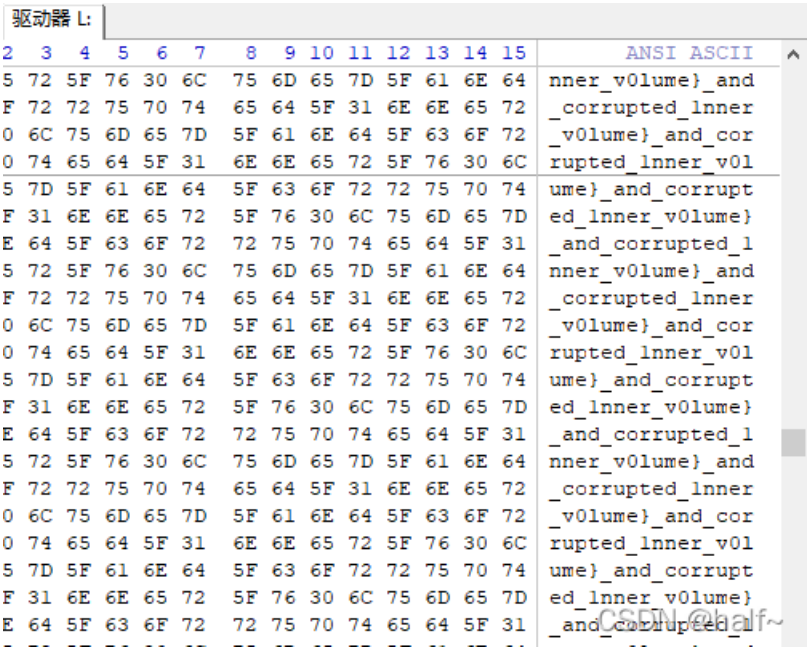
winhex



使用驱动器 L: 中的光盘之前需要将其格式化。

是否要将其格式化?

Winhex->工具->打开磁盘
打开L盘



```
2  3  4  5  6  7   8  9 10 11 12 13 14 15        ANSI ASCII
5 72 5F 76 30 6C  75 6D 65 7D 5F 61 6E 64   nner_v0lume}_and
F 72 72 75 70 74  65 64 5F 31 6E 6E 65 72   _corrupted_1nner
0 6C 75 6D 65 7D  5F 61 6E 64 5F 63 6F 72   _v0lume}_and_cor
0 74 65 64 5F 31  6E 6E 65 72 5F 76 30 6C   rupted_1nner_v0l
5 7D 5F 61 6E 64  5F 63 6F 72 72 75 70 74   ume}_and_corrupt
F 31 6E 6E 65 72  5F 76 30 6C 75 6D 65 7D   ed_1nner_v0lume}
E 64 5F 63 6F 72  72 75 70 74 65 64 5F 31   _and_corrupted_1
5 72 5F 76 30 6C  75 6D 65 7D 5F 61 6E 64   nner_v0lume}_and
F 72 72 75 70 74  65 64 5F 31 6E 6E 65 72   _corrupted_1nner
0 6C 75 6D 65 7D  5F 61 6E 64 5F 63 6F 72   _v0lume}_and_cor
0 74 65 64 5F 31  6E 6E 65 72 5F 76 30 6C   rupted_1nner_v0l
5 7D 5F 61 6E 64  5F 63 6F 72 72 75 70 74   ume}_and_corrupt
F 31 6E 6E 65 72  5F 76 30 6C 75 6D 65 7D   ed_1nner_v0lume}
E 64 5F 63 6F 72  72 75 70 74 65 64 5F 31   _and_corrupted_1
5 72 5F 76 30 6C  75 6D 65 7D 5F 61 6E 64   nner_v0lume}_and
F 72 72 75 70 74  65 64 5F 31 6E 6E 65 72   _corrupted_1nner
0 6C 75 6D 65 7D  5F 61 6E 64 5F 63 6F 72   _v0lume}_and_cor
0 74 65 64 5F 31  6E 6E 65 72 5F 76 30 6C   rupted_1nner_v0l
5 7D 5F 61 6E 64  5F 63 6F 72 72 75 70 74   ume}_and_corrupt
F 31 6E 6E 65 72  5F 76 30 6C 75 6D 65 7D   ed_1nner_v0lume}
E 64 5F 63 6F 72  72 75 70 74 65 64 5F 31   _and_corrupted_1
```

得到第二部分
_and_corrupted_1nner_v0lume}