




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

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/m0_57379855/article/details/124109242

版权



[Ctf 专栏收录该内容](#)

5 篇文章 0 订阅

订阅专栏

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

easyCAP.pcap [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 0

No.	Time	Source	Length	Destination	Protocol	Info
1	0.000000	172.31.98.1	74	192.155.81.	TCP	46046→7890
2	0.029197	192.155.81.	74	172.31.98.1	TCP	7890→46046
3	0.029275	172.31.98.1	66	192.155.81.	TCP	46046→7890

Follow TCP Stream (tcp.stream eq 0)

Stream Content

FLAG: 385b87afc8671dee07550290d16a8071

CSDN @half~

大流量分析（一）

统计 Statistics

Statistics—ipStatistics—ipaddresses

IP Addresses with filter:

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
IP Addresses	715015				0.7343	100%	10.7600	956.520
183.129.152.140	412703				0.4238	57.72%	4.1800	71.910
172.16.61.200	248659				0.2554	34.78%	10.5300	890.415
172.16.61.199	214311				0.2201	29.97%	4.1100	71.910
172.16.103.1	182690				0.1876	25.55%	10.5300	890.415
172.16.61.206	166370				0.1709	23.27%	2.3300	404.847
172.16.101.89	63546				0.0653	8.89%	6.5400	571.940
172.16.60.199	39616				0.0407	5.54%	0.2200	210.963
172.16.60.197	20183				0.0207	2.82%	1.9500	0.396
172.16.60.200	16157				0.0166	2.26%	1.0600	84.152
172.16.1.35	6540				0.0067	0.91%	0.3600	256.265
23.251.54.39	6168				0.0063	0.86%	0.0900	385.294
118.166.88.232	4033				0.0041	0.56%	0.0900	488.727
200.201.213.203	3742				0.0038	0.52%	0.1000	297.533

Copy Save

大流量分析（二）

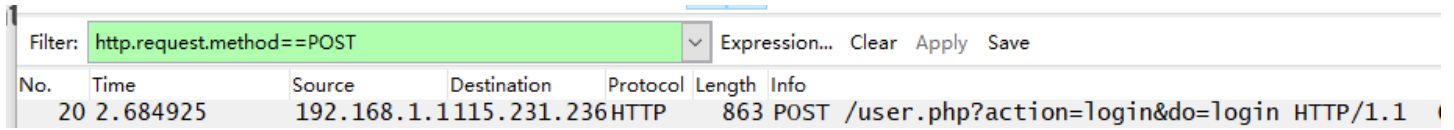
smtp

Filter: smtp

No.	Time	Source	Length	Destination	Protocol	Info
48888	68.950253	172.16.60.2	71	65.54.190.1	SMTP	S: 220 ESMTTP READY
49495	69.243333	65.54.190.1	86	172.16.60.2	SMTP	C: EHLO BAY004-OMC1S5.hotmail.com
49498	69.247468	172.16.60.2	201	65.54.190.1	SMTP	S: 250 mail.t3sec.cc Hello BAY004-
49984	69.569108	65.54.190.1	81	172.16.60.2	SMTP	C: MAIL FROM:<xsser@live.cn>
51101	70.197453	172.16.60.2	86	65.54.190.1	SMTP	S: 250 <xsser@live.cn>, Sender ok

wireshark

http.request.method==POST

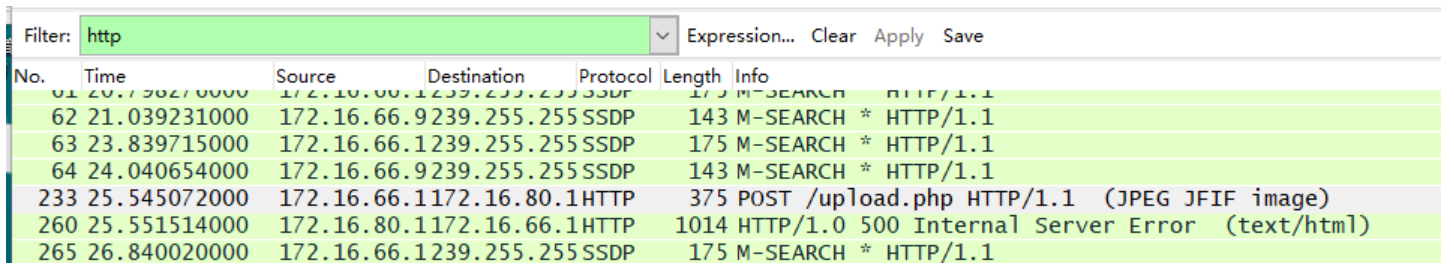


No.	Time	Source	Destination	Protocol	Length	Info
20	2.684925	192.168.1.1115	231.236	HTTP	863	POST /user.php?action=login&do=login HTTP/1.1

- HTML Form URL Encoded: application/x-www-form-urlencoded
 - Form item: "email" = "flag"
 - Key: email
 - Value: flag
 - Form item: "password" = "ffb7567a1d4f4abdfdb54e022f8facd"
 - Key: password
 - Value: ffb7567a1d4f4abdfdb54e022f8facd

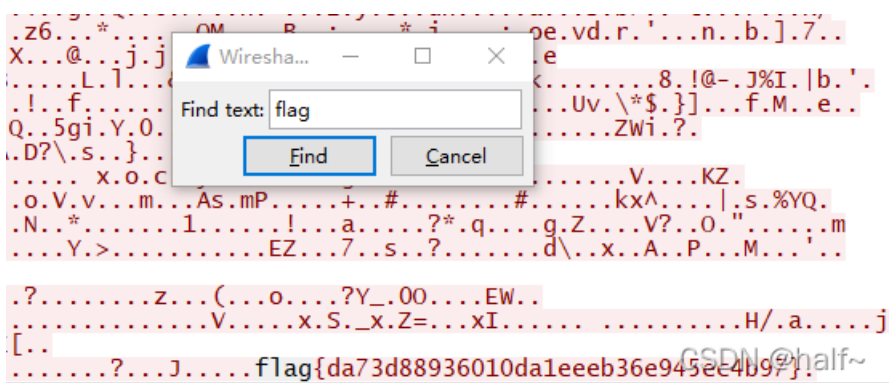
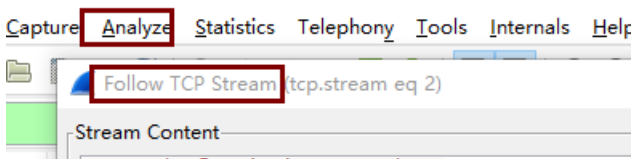
被嗅探的流量

http



No.	Time	Source	Destination	Protocol	Length	Info
61	20.798270000	172.16.66.1	239.255.255.255	SSDP	175	M-SEARCH * HTTP/1.1
62	21.039231000	172.16.66.9	239.255.255.255	SSDP	143	M-SEARCH * HTTP/1.1
63	23.839715000	172.16.66.1	239.255.255.255	SSDP	175	M-SEARCH * HTTP/1.1
64	24.040654000	172.16.66.9	239.255.255.255	SSDP	143	M-SEARCH * HTTP/1.1
233	25.545072000	172.16.66.1	172.16.80.1	HTTP	375	POST /upload.php HTTP/1.1 (JPEG JFIF image)
260	25.551514000	172.16.80.1	172.16.66.1	HTTP	1014	HTTP/1.0 500 Internal Server Error (text/html)
265	26.840020000	172.16.66.1	239.255.255.255	SSDP	175	M-SEARCH * HTTP/1.1

tcp追踪流



数据包中的线索

42	10.091579000	172.16.80.11	172.16.66.1	HTTP	444	HTTP/1.1	200	OK	(text/html)
43	10.091633000	172.16.66.1	172.16.80.1	TCP	54	1883+80	[ACK]	Seq=386	Ack=86531
44	10.091633000								
45	10.091633000								

Follow TCP Stream (tcp.stream eq 7)

Stream Content

```

00 0010 ae0h/IY/VaP8hvT/ABP8QX0fIyaxfP8A9tnqvH431iL511K+j/7bvWTRR7SH8hX1emdRp/xk8T6Z
08 0100 s8vw7793/A/7yuk0b9qjxNYbI7p7S+j/AL7p5c1eZ02T91HvrT3DGphKH24Hu2hftd20P/H5pdwn
10 0000 994X8yussP2oPDN8PmuJrX/rtDXy6JU8tH8z5JPuU+SV4o6w9mctbKaMvfr9h6f8wtB1PZ5Wq2P/
18 1011 AA0etqPwB0W3877RDs/v76+GZNUHij87f8m/Zvq/Hfva/Iskif79X9XOH+x4S+CZ9CFj9pu380
20 0100 yPZ6P5d9c/xzf8s468Z8wffDW/FsDw3mpTyQyffhT93HXOP1oTrv06Z6uFy2jSgNrKfAHjKz8UfE
28 0101 jxzYwCR/8S09tbW62f6uS5+y73/9krnf2gP2kbb4S3Fnomlwya14w1z9zpdns8uPzv77u/yVv7P
30 0000 H7LXi34VeDNSS9e8cfZ7nXL2bVNRfSrXZcSTP9/fcvvf/v2lmsIvq3PU/7cPNx20nLEwhQhz8nx
38 0111 HqnxI+L3h74QWDza5qUcFzJ/x62EP7y7vH/uQwp871hfs83PibxPqniHxt4i0268M3GubLX59Nd/
40 0010 9Is9Pg+553+28nz1jfsv/CvR9B/trxbZwz3T+INRd90v7+f7Vfx2qJst98/zp5km991euUVvYwXJ
48 0101 A1wtCtiuwT/8ALH9s3P/Pzcf9/Ho/tm5/5+bj/v49V6K4fZwPW+r0yf+2rv/n8uv+/9EmqTS/xy
50 0111 f991BRR70A/q90BJ9vc/f/eUyT97JSUUEzGX7MK5XxLa/wBteLiBx+DZXVvG654fvP7w+22Dx+Z5
58 0110 deFn2F9pRh70PN7/AL59Fw1UpOMTKU5ck+SXJ/iN+332v1+V8n1/x1v6h43k8w+EH0HXmnuTP3ea
kip/AKRbt/f3155Ha+IZf+W0cf8A3xwRpdRfr8AH1cxyf7CJSp4r6yvYpS5DnxeTFv6n1pYiHP
H+U6X4SfDbRvGvxwhT5tUurzRdJiR86g/wC8mc/ci/3P/iK9B/al+AuJ6RpuueNLPvr+zuJ0Ujmt
4X/dz07JHXjml2D2sczt9+4nd6v3ms6lLb21t9pnkto7pJ3R3/ufPXL/AGFD6pKHJ70gr5hiZ5jS
rRre7D3f8X83/gR798BfBen/AL0vwYuNW1iJkv7iEXV8+z95/sQp/n7710c/xwm8PwXVxrXh/VNM
WOFJrYnZN9q3vsSH5P8AltV2fJXz94o+MPibxTps1jdX0clv8Lx74/40ff/AOyVm+NvjB4k1zTp
JtW1aNIrR4blERP3cDo+9K6o0atKn7DDfZPm62Bjiq08Tjp+9Kb5r83923KfQmvfthW/guG7/tzT
W0y+tLX+0LW2e5R/tn+wzm7j769i/Z7+M998JfBmgeArLwF4gm1WbS5NdjE1zbl9tM03mXM0vz/u
S88zH5+7143+yj+wlrHxx8GyeN/F17DaS69HB/ZcTjz2Sy89Hmfmf/bng3oif8s/Mevr7UvgVeS+P
ff3iC11WC3u9a0KDRNMYw/8AIPKGZmdv7+WdP++K/UeE8lzXDw9v8HP/AIf73/2v3n4/xZmWRzqe
wjyz5d/i5fs7a/3pc3+HTodN8E/ivbfgL4XaP4mt7Wayh1iHzlhm4ePBK4P/AHrVj4SfDyH4Vfd
PQ/DsMnmR6NZRWiv/f2IFz+OKK+/p/2lyLn3tr6n5djPq7rz9gvcu+X0vp+B/9k=
0
  
```

CSDN @half~

base64转图片

```

n+06X43iDDBRvGvxwhT5tUurzRdJiR86g/wC8mc/ci/3P/iK9B/al+AuJ6RpuueNLPvr+zuJ0Ujmt
4X/dz07JHXjml2D2sczt9+4nd6v3ms6lLb21t9pnkto7pJ3R3/ufPXL/AGFD6pKHJ70gr5hiZ5jS
rRre7D3f8X83/gR798BfBen/AL0vwYuNW1iJkv7iEXV8+z95/sQp/n7710c/xwm8PwXVxrXh/VNM
WOFJrYnZN9q3vsSH5P8AltV2fJXz94o+MPibxTps1jdX0clv8Lx74/40ff/AOyVm+NvjB4k1zTp
JtW1aNIrR4blERP3cDo+9K6o0atKn7DDfZPm62Bjiq08Tjp+9Kb5r83923KfQmvfthW/guG7/tzT
W0y+tLX+0LW2e5R/tn+wzm7j769i/Z7+M998JfBmgeArLwF4gm1WbS5NdjE1zbl9tM03mXM0vz/u
S88zH5+7143+yj+wlrHxx8GyeN/F17DaS69HB/ZcTjz2Sy89Hmfmf/bng3oif8s/Mevr7UvgVeS+P
ff3iC11WC3u9a0KDRNMYw/8AIPKGZmdv7+WdP++K/UeE8lzXDw9v8HP/AIf73/2v3n4/xZmWRzqe
wjyz5d/i5fs7a/3pc3+HTodN8E/ivbfgL4XaP4mt7Wayh1iHzlhm4ePBK4P/AHrVj4SfDyH4Vfd
PQ/DsMnmR6NZRWiv/f2IFz+OKK+/p/2lyLn3tr6n5djPq7rz9gvcu+X0vp+B/9k=
  
```

编码源格式: 文本 Hex 解码结果: 自动检测 中文编码: UTF-8 编码 解码

该内容已经被插件识别为二进制数据。
 但未提供可供阅读的文本信息，且数据量较大，故不在此处显示hex内容。
 如需查看hex内容，请关闭自动模式!

插件【Jpeg】Jpeg Image(JFIF)
 另存为: jpg文件
 附加信息: CSDN @half~

荷兰宽带数据泄露

```
RouterPassView - C:\Users\zxh\Desktop\CTF\荷兰宽带数据泄露
File Edit View Options Help
<X_TP_IFName val=eth1 />
</WANIPConnection>
<WANIPConnection nextInstance=3 />
<WANPPPConnection instance=1 >
  <Enable val=1 />
  <DefaultGateway val=10.177.144.1 />
  <Name val=pppoe_eth1_d />
  <Uptime val=671521 />
  <Username val=053700357621 />
  <Password val=210265 />
<X_TP_IFName val=ppp0 />
<X_TP_L2IfName val=eth1 />
```

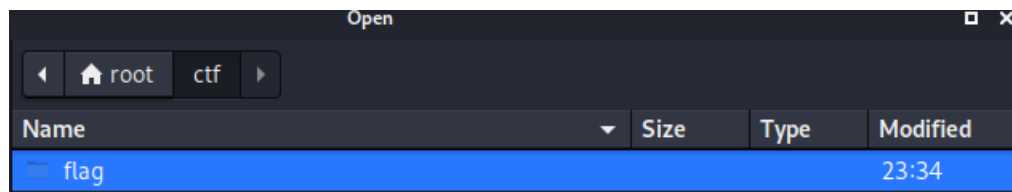
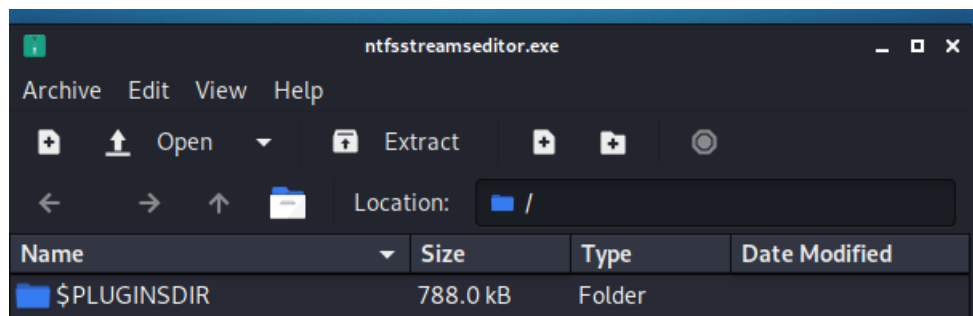
[ACTF新生赛2020]NTFS数据流

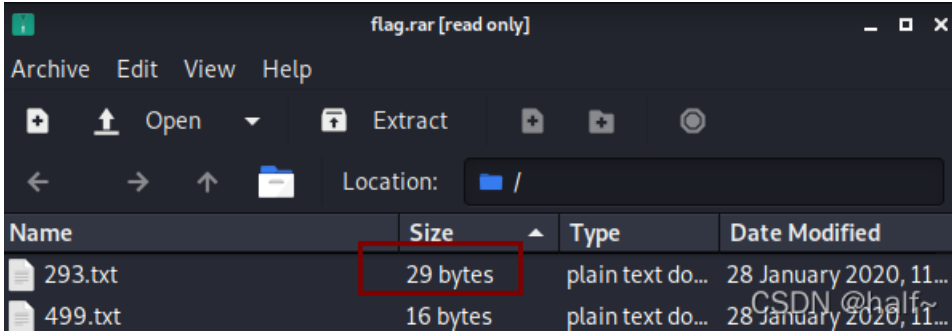
NTFS数据流

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

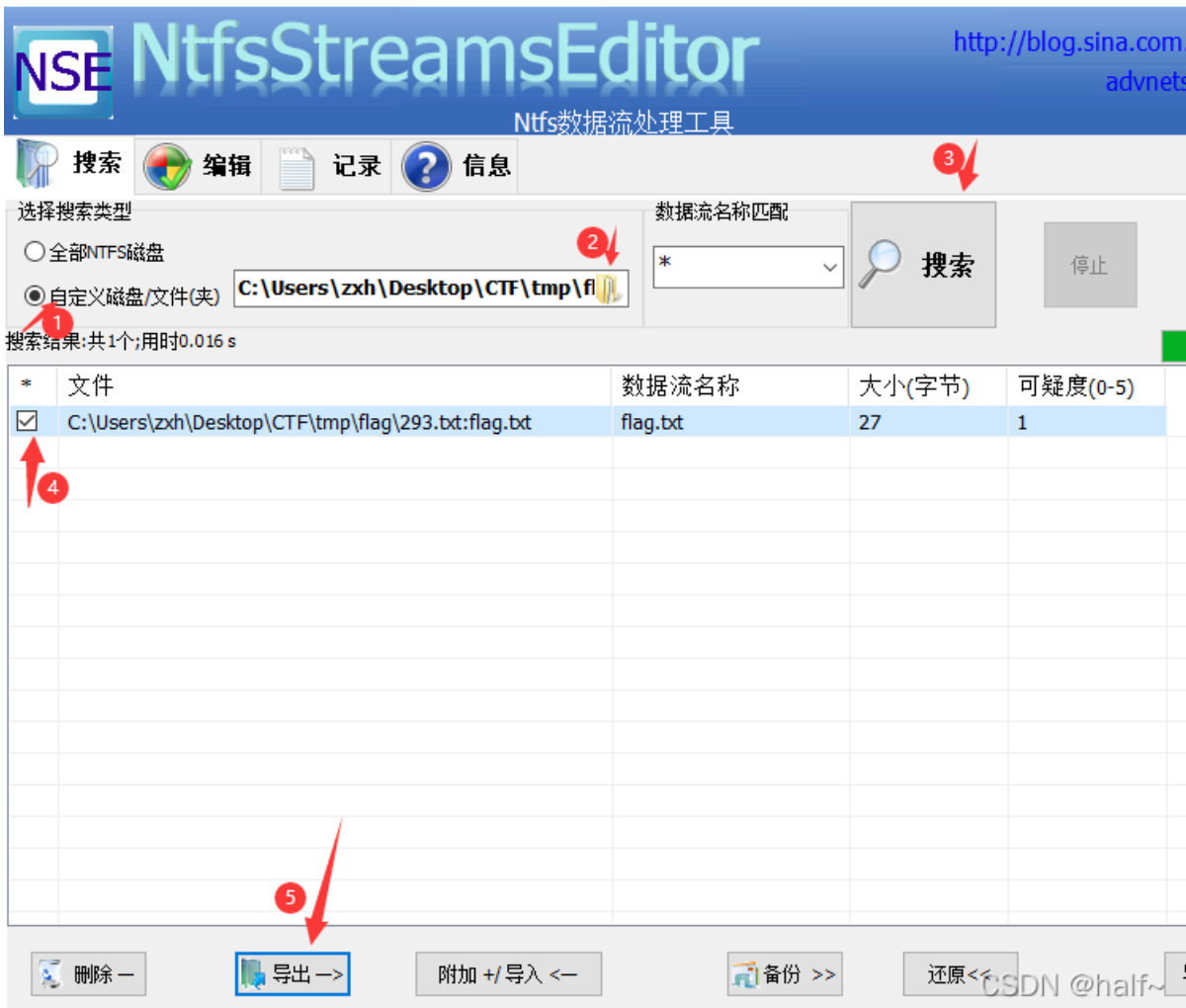




293.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

flag就在这里哦，找找看吧ADS:)



C:\Users\zxh\Desktop\CTF\tmp\flag\293.txt!flag.txt -

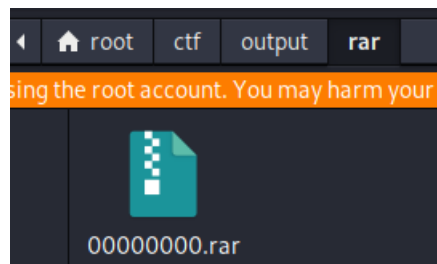
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

ACTF{AAAds_ntfs_ffunn?}

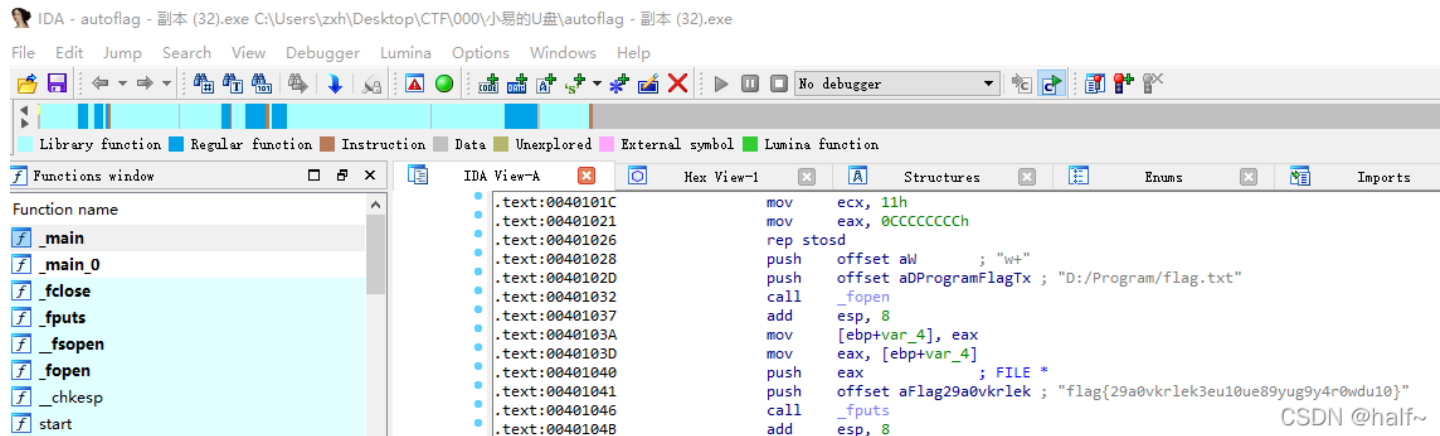
小易的U盘

foremost

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



IDA



[RCTF2019]disk

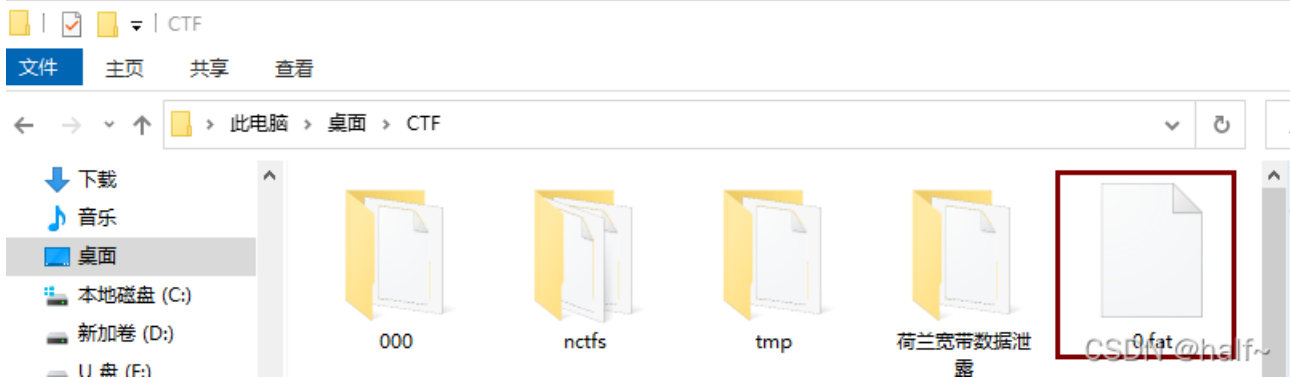
strings

```
(root@kali)~[~/ctf]
# strings encrypt.vmdk|grep ctf
ure_quick_form4t_volumerctf{unseCure_quick_form4t_volumerctf{unseCure_quick_f
orm4t_volumerctf{unseCure_quick_form4t_volumerctf{unseCure_quick_form4t_vo1um
erctf{unseCure_quick_form4t_volumerctf{unseCure_quick_form4t_volumerctf{unseC
```

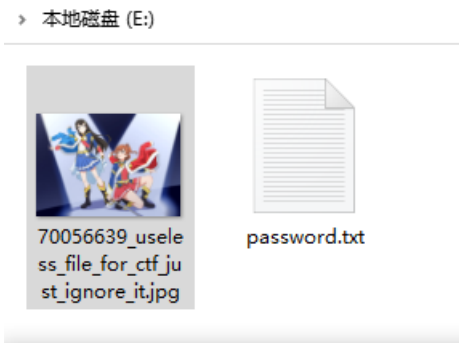
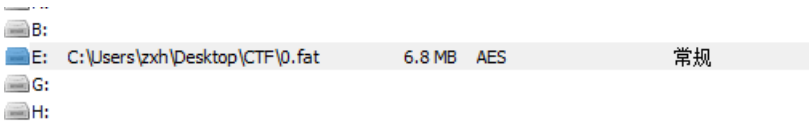
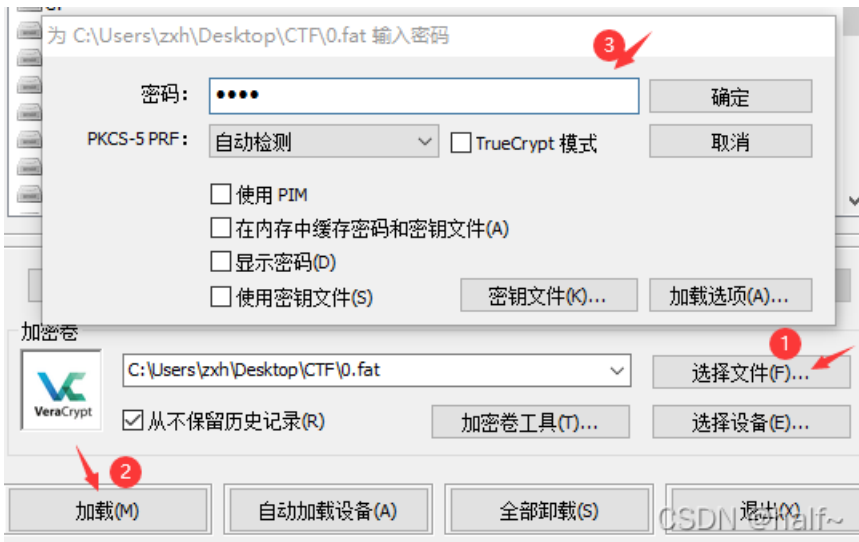
得到一些

ctf{unseCure_quick_form4t_vo1ume

7-ZIP解压vmdk



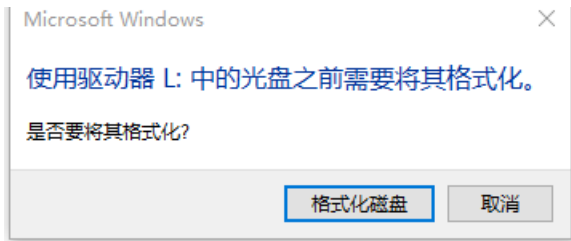
VeraCrypt挂载



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



Winhex->工具->打开磁盘

打开L盘

驱动器 L:															ANSI ASCII
2	3	4	5	6	7	8	9	10	11	12	13	14	15		
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_inner	
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_inner_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_inner_v0lume}	
E	64	5F	63	6F	72	72	75	70	74	65	64	5F	31	_and_corrupted_l	
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_inner	
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_inner_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_inner_v0lume}	
E	64	5F	63	6F	72	72	75	70	74	65	64	5F	31	_and_corrupted_l	
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_inner	
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_inner_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_inner_v0lume}	
E	64	5F	63	6F	72	72	75	70	74	65	64	5F	31	_and_corrupted_l	

得到第二部分

_and_corrupted_1nner_v0lume}