



2021“西湖论剑”网络安全大赛Writeup

原创

Le1a  于 2021-11-21 13:46:30 发布  7242  收藏 6

分类专栏: [CTF](#) 文章标签: [安全](#) [网络安全](#)

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/weixin_52091458/article/details/121452876

版权



[CTF 专栏收录该内容](#)

12 篇文章 3 订阅

订阅专栏

2021"西湖论剑"网络安全大赛Writeup

我只写了自己做的部分, 完整WP请访问: <https://www.yuque.com/docs/share/4c901b3e-a9c4-4e67-9d1c-3030108ca4a0?#>

密码: slhq

Web

详见fmyyy师傅: <https://blog.csdn.net/fmyyy1/article/details/121451279?spm=1001.2014.3001.5501>

Misc

真·签到

赛题详情

题目名称: 真·签到

题目内容: 扫码进入西湖论剑网络安全大赛微信公众号, 发送语音说出“西湖论剑2021, 我来了。”即可获得本题 flag:)

题目分数: 100

当前答出前3名:

第一名 DebuGGer

第二名 ReT0

第三名 财贸夺Flag队

相关附件:

[下载附件](#) [下载](#)

扫码关注公众号, 发送语音即可



flag:

```
DASCTF{welc0m3_t0_9C51s_2021}
```

YUSA的小秘密

赛题详情

题目名称: YUSA的小秘密

题目内容: LSB, 但又不是LSB, 众所周知不止RGB。yusa, 我的yusa, 嘿嘿

题目分数: 100

当前答出前3名: **第一名 H4F** **第二名 南门辣子鸡** **第三名 0x401**

相关附件: "YUSA的小秘密"的题目附件 [下载](#)

这题跟去年的ByteCTF的 [Hardcore Watermark 01](#) 几乎一模一样, 官方wp链接:

<https://bytectf.feishu.cn/docs/doccnqzpGCWH1hkDf5ljGdjOJYg#>

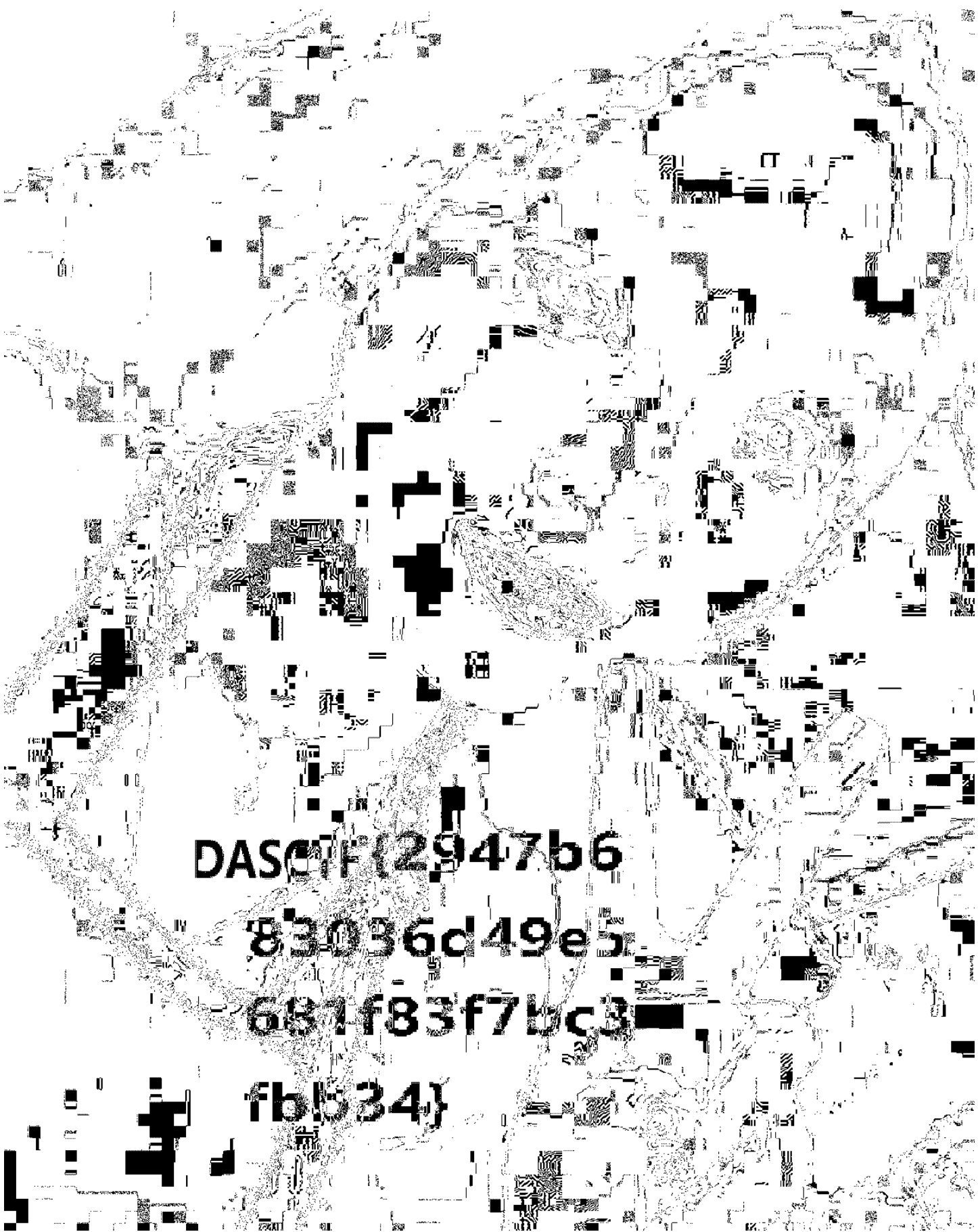
这题采用的不是RGB通道的LSB隐写, 而是采用的YCrCb通道。通过 `cv2.cvtColor(img, cv2.COLOR_BGR2YCrCb)` 对 `img` 图片数据进行色彩空间转换, 即可得到三个通道的数据, 然后对三个通道的数据分别根据奇偶做二值化处理并保存为图片

```
cv.imwrite('a.png', (a % 2) * 255) #对三个通道中的数据分别根据奇偶做二值化处理, 并分别保存为图片
cv.imwrite('b.png', (b % 2) * 255)
cv.imwrite('c.png', (c % 2) * 255)
```

所以完整脚本如下:

```
from cv2 import *
import cv2 as cv
img=cv2.imread('C:\\Users\\XXX\\Desktop\\yusa\\yusa.png')
src_value=cv2.cvtColor(img, cv2.COLOR_BGR2YCrCb)
a, b, c = cv.split(src_value) #使用cv.split分离通道
cv.imwrite('a.png', (a % 2) * 255) #对三个通道中的数据分别根据奇偶做二值化处理, 并分别保存为图片
cv.imwrite('b.png', (b % 2) * 255)
cv.imwrite('c.png', (c % 2) * 255)
```

运行后会得到三个通道的图片, 在其中 `a.png` 即可清晰看到flag



**DASCTF{2947b6
83036d49e5
681f83f7bc3
fbb34}**

flag:

DASCTF{2947b683036d49e5681f83f7bc3fbb34}

赛题详情

题目名称: Yusa的秘密

题目内容: Sakura组织即将进攻地球, 此时你意外得到了该组织内某个成员的电脑文件, 你能从中发现本次阴谋所用的关键道具吗。(注: 题目中包含了五个彩蛋, 且彩蛋对解题本身没有任何影响, 快去发现吧!) <https://gcsis-2021-misc-atta-1251267611.file.myqcloud.com/3iuryh387ryh34eiud/Yusa%E7%9A%84%E7%A7%98%E5%AF%86.zip>

题目分数: 200

当前答出前3名:

第一名 香香嘴炒饭

第二名 n03tAck

第三名 EDI

下载附件, 发现这是一个内存取证的题目, 先用命令获取一下内存镜像的进程

```
vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 psxview
```

```
C:\Windows\System32\cmd.exe
Microsoft Windows [版本 10.0.22000.318]
(c) Microsoft Corporation. 保留所有权利。

C:\Users\Yijiale\Desktop\取证>vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 psxview
Volatility Foundation Volatility Framework 2.6
Offset(P)      Name                PID  pslist  psscan  thrdproc  pspcid  csrss  session  deskthrd  ExitTime
-----
0x000000003f242b30  conhost.exe         1356 True    True    True     True    True    True     False
0x000000003e464b30  svchost.exe         1272 True    True    True     True    True    True     True
0x000000003e91d920  conhost.exe         1344 True    True    True     True    True    True     False
0x000000003e2af890  svchost.exe         1836 True    True    True     True    True    True     True
0x000000003f949060  audiodg.exe         2744 True    True    True     True    True    True     True
0x000000003e449470  taskhost.exe        1244 True    True    True     True    True    True     False
0x000000003fa2e590  dllhost.exe         1168 True    True    True     True    True    True     False
0x000000003e646b30  svchost.exe         712  True    True    True     True    True    True     True
0x000000003e6a4b30  svchost.exe         856  True    True    True     True    True    True     True
0x000000003e7703a0  svchost.exe         348  True    True    True     True    True    True     True
0x000000003e516630  svchost.exe         1408 True    True    True     True    True    True     True
0x000000003e9008f0  winlogon.exe        432  True    True    True     True    True    True     True
0x000000003e455810  dwm.exe             2260 True    True    True     True    True    True     False
0x000000003e122890  SearchIndexer.     2552 True    True    True     True    True    True     True
0x000000003e434910  spoolsv.exe         1212 True    True    True     True    True    True     True
0x000000003e6b5830  svchost.exe         884  True    True    True     True    True    True     True
0x000000003e6763e0  svchost.exe         772  True    True    True     True    True    True     False
0x000000003fab2b30  DumpIt.exe          820  True    True    True     True    True    True     False
0x000000003e58f060  vmtoolsd.exe        1520 True    True    True     True    True    True     True
0x000000003e6ca750  cmd.exe             2536 True    True    True     True    True    True     False
0x000000003e0804b0  vmtoolsd.exe        2380 True    True    True     True    True    True     False
0x000000003fb54b30  svchost.exe         1232 True    True    True     True    True    True     False
0x000000003e96e1d0  services.exe        488  True    True    True     True    True    True     False
```

这些进程都分析了一下, 发现有StikyNot.exe进程, 这是windows的便签程序, 可以尝试寻找snt文件来查看便签的内容。这里就直接来用filescan查找文件, 用windows的findstr命令筛选一下, 先查看压缩包

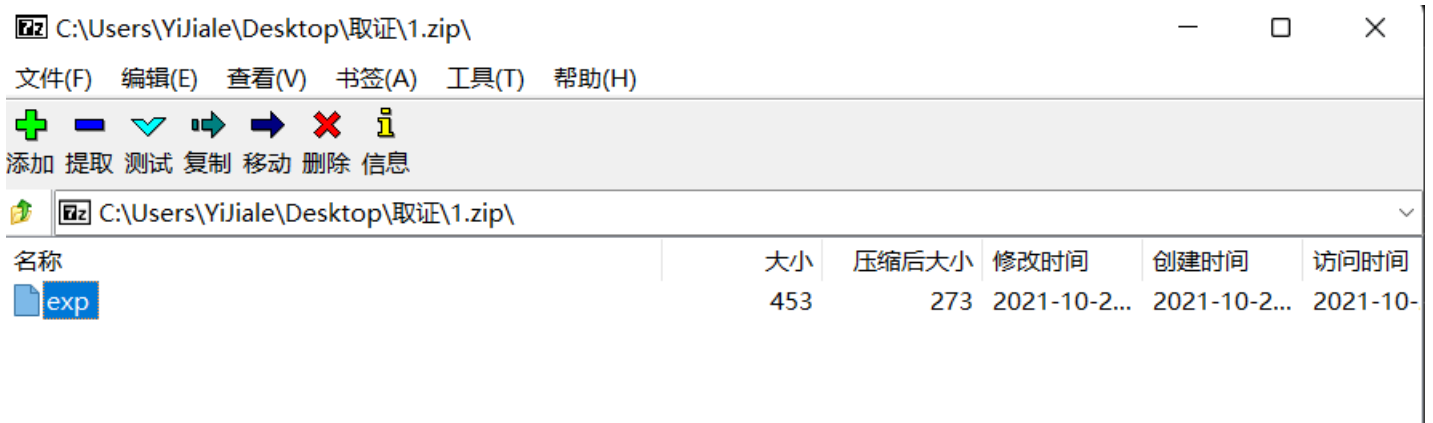
```
vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 filescan | findstr /r 'zip'
```

```
C:\Users\YiJiale\Desktop\取证>vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 filescan | findstr /r "zip"
Volatility Foundation Volatility Framework 2.6
0x000000003e444a60 15 0 R--r-d \Device\HarddiskVolume2\Windows\System32\zipfldr.dll
0x000000003ee522e0 16 0 R--r-d \Device\HarddiskVolume2\Program Files\VMware\VMware Tools\zip.exe
0x000000003f2f49e0 15 0 R--r-- \Device\HarddiskVolume2\Program Files\VMware\VMware Tools\zip.exe
0x000000003f3356f0 1 0 R--rw- \Device\HarddiskVolume2\PROGRA~1\MSBuild\MICROS~1\WINDOW~1\key.zip
C:\Users\YiJiale\Desktop\取证>
```

有一个 `key.zip`。直接使用命令dump下来，重命名为1.zip

```
vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000003f3356f0 -D C:\Users\XXX\Desktop\取证
```

里面是一个exp文件，但是压缩包加密了，需要寻找密码



刚刚查找进程提到过便签的进程，这里来尝试查找一下snt文件

```
vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 filescan | findstr /r "snt"
```

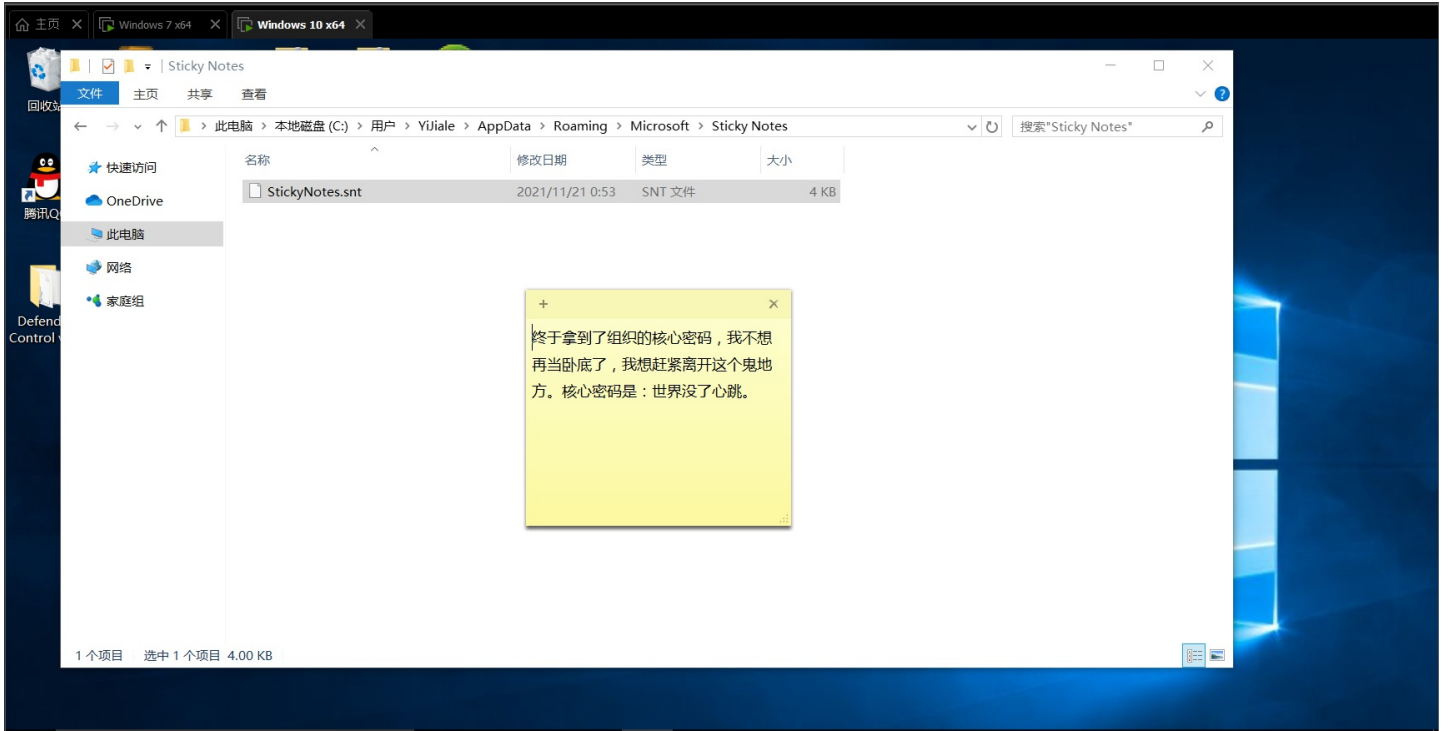
```
C:\Users\YiJiale\Desktop\取证>vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 filescan | findstr /r "snt"
Volatility Foundation Volatility Framework 2.6
0x000000003e2d29d0 16 0 R--r-d \Device\HarddiskVolume2\Windows\System32\zh-CN\sntsearch.dll.mui
0x000000003e9033d0 2 0 R--r-d \Device\HarddiskVolume2\Windows\System32\sysntfy.dll
0x000000003fb306e0 16 1 RW-r-- \Device\HarddiskVolume2\Users\Yusa\AppData\Roaming\Microsoft\Sticky Notes\Sticky
Notes.snt
C:\Users\YiJiale\Desktop\取证>
```

发现了便签文件，我们将他dump下来查看

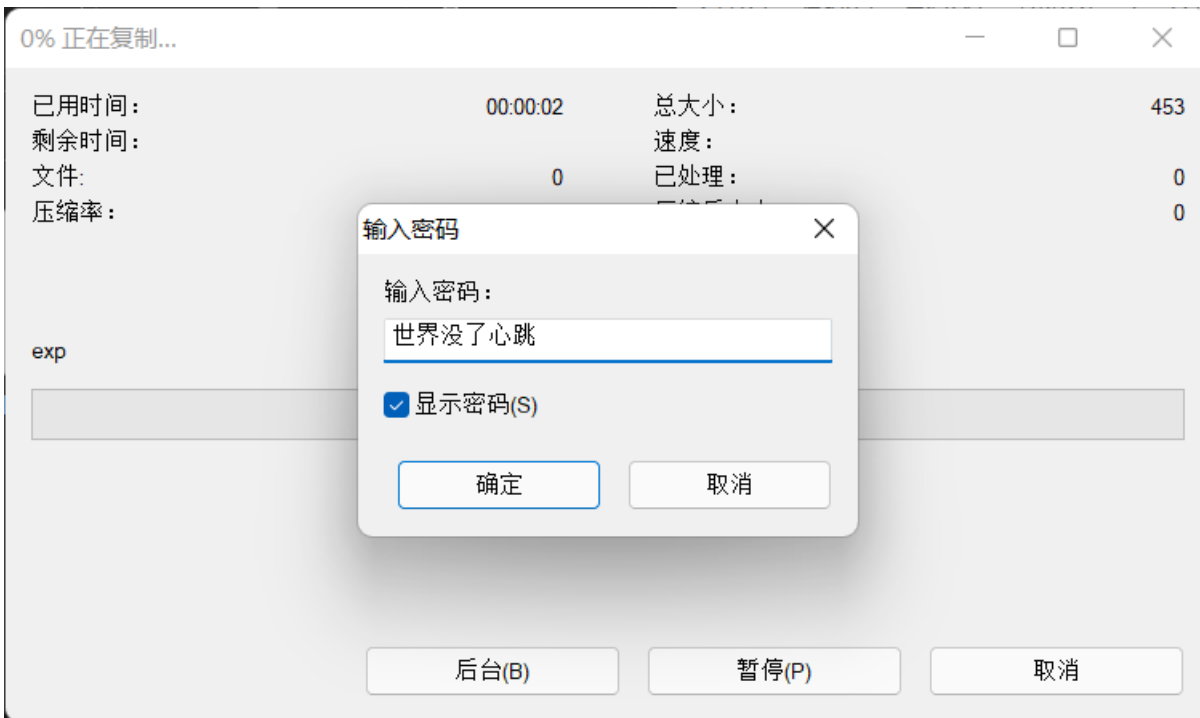
```
vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000003fb306e0 -D C:\Users\XXX\Desktop\取证
```

将其重命名为 `StickyNotes.snt`，用记事本打开是看不到上面东西的，既然数win7的便签，我们就将其传入win7虚拟机尝试打开(这里因为VMware tools始终无法装上，便采用QQ传输文件)，后来发现 家庭普通版的Win7居然没有便签这个程序，我是Win11，没有便签程序，于是我尝试下Win10虚拟机

将snt文件放入C:\Users\XXX\AppData\Roaming\Microsoft\Sticky Notes\路径下，然后打开便签程序，便可以得到



得到了一个密码：**世界没了心跳**



用这个密码成功打开刚刚的exp的压缩包，得到exp文件

```

from PIL import Image
import struct
pic = Image.open('key.bmp')
fp = open('flag', 'rb')
fs = open('Who_am_I', 'wb')

a, b = pic.size
list1 = []
for y in range(b):
    for x in range(a):
        pixel = pic.getpixel((x, y))
        list1.extend([pixel[1], pixel[0], pixel[2], pixel[2], pixel[1], pixel[0]])

data = fp.read()
for i in range(0, len(data)):
    fs.write(struct.pack('B', data[i] ^ list1[i % a*b*6]))
fp.close()
fs.close()

```

通过分析exp可以发现，目前还缺少两个文件便可以得到flag文件，分别是Who_am_I和key.bmp文件

这里Who_am_I，既然是Yusa的秘密，那用户应该就是Yusa了，使用命令来获取一下用户名的hash密码

```
vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 hashdump
```

```

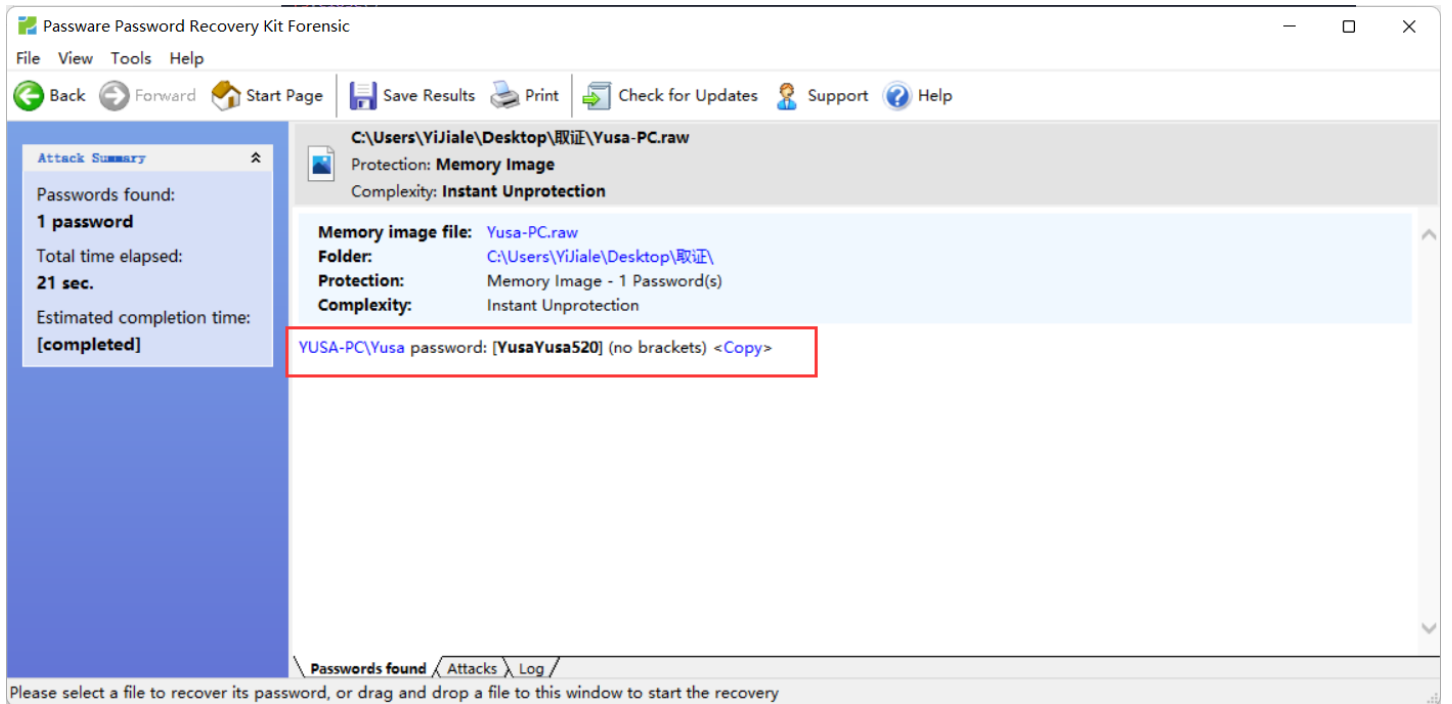
C:\Users\YiJiale\Desktop\取证>vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:84f851a4a47f1a1c9408b7e1ab7b469e:::
Yusa:1003:aad3b435b51404eeaad3b435b51404ee:74869621853fe4de089dc07679c2475b:::

C:\Users\YiJiale\Desktop\取证>_

```

使用 **Passware Kit 13** 来破解Yusa用户的密码

打开软件，点击 **Memory Analysis** 功能，再选择 **Windows User** 功能

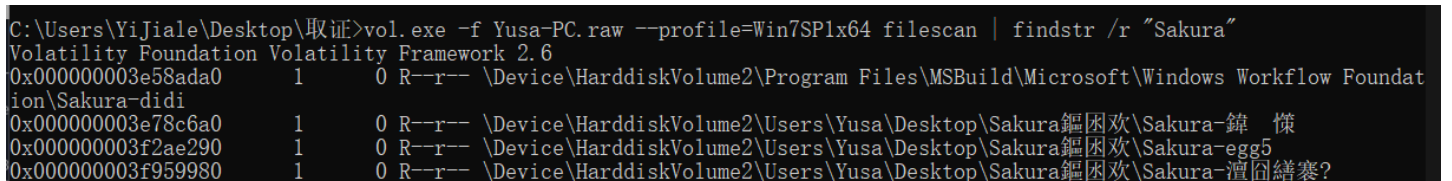


发现得到了密码为: **YusaYusa520**

成功打开了Who_am_I的压缩包得到了Who_am_I文件，题目描述中出现了Sakura组织，所以这里也查找一下相关文件

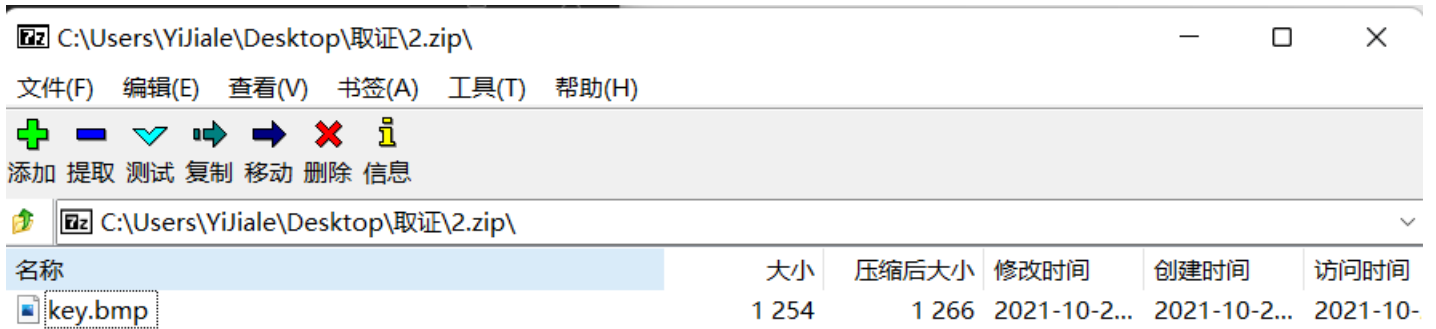


```
vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 filescan | findstr /r "Sakura"
```



这里得到的部分结果含有中文，在Windows里就乱码了，不过不影响，我们dmpup一下第一个文件 **Sakura-didi**，并且重命名为 2.zip

```
vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 dumpfiles -Q 0x00000003e58ada0 -D C:\Users\XXX\Desktop\取证
```



打开压缩包，里面确实是key.bmp文件，但是还是需要密码，接下来就只需要去找密码了

联想到一开始分析进程的时候，除了便签程序，还有一个平时很少遇到过的 `wab.exe`，这是通讯录的程序，我们试着找一下其中的联系人，联系人contact文件，用filescan搜索一下

```
vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 filescan | findstr /r "contact"
```

一共得到了两个联系人的文件，分别是Yusa.contact和Mystery Man.contact

```
C:\Users\YiJiale\Desktop\取证>vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 filescan | findstr /r "contact"
Volatility Foundation Volatility Framework 2.6
0x00000003e748f20      1      0 R--r-d \Device\HarddiskVolume2\Users\Yusa\Contacts\Yusa.contact
0x00000003fa09070      1      0 R--r-d \Device\HarddiskVolume2\Users\Yusa\Contacts\Mystery Man.contact
```

我们分别dump下来分析一下

```
vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 dumpfiles -Q 0x00000003e748f20 -D C:\Users\XXX\Desktop\取证
vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 dumpfiles -Q 0x00000003fa09070 -D C:\Users\XXX\Desktop\取证
```



```
file.None.0xfffffa8003b86010.dat - 记事本
文件(F) 编辑(E) 格式(O) 视图(V) 帮助(H)
<?xml version="1.0" encoding="UTF-8"?>
<c:contact c:Version="1" xmlns:c="http://schemas.microsoft.com/Contact"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:MSP2P="http://schemas.microsoft.com/Contact/Extended/MSP2P">
  <c:Notes c:Version="2" c:ModificationDate="2021-10-
28T11:47:56Z">LF2XGYPPXSGOPO4E465YPZMITLSYRGXGWS7OJOEL42O2
LZFYQDSLRLKXEXO56LCVB566IZ2FPW7S37K7HQK46LLUM42EJB354RTSL3I
HFR6VONHEJ4S4ITZNEVHTJPNXJS62OHAECGZGCWWRVOBUXMNKMGJTT
KTDZME2TKU3PGVMWS5ZVGVYUKYJSKY2TON3ZJU2VSK3WGVGHK3BVG
VJW6NLBGZCDK33NKQ2WE6KBGU3XKRJVG52UQNJXOVNDKTBSM42TK4
KFGVRGK3BVLFLTGNBUINBTKYTFNQ2VSVZTGVNEOOJVLJBU4NKMGSZDK
NCXNY2UY4KHGVGHSZZVG52WMNSLMVCTKWJLI2DIQ2DMEZFMNJXG5
4WCT2EJF3VSV2NGVGW2SJVLVFKNCNKRIXSWLNJJUVS6SJGNMTERLZJ5
KFM3KNK5HG2TSEM46Q====</c:Notes> <c:CreationDate>2021-10-
28T05:56:31Z</c:CreationDate> <c:Extended xsi:nil="true"/>
  <c:ContactIDCollection> <c:ContactID c:ElementID="c81482a1-
44bc-43bf-bfc0-159ab6a43962"> <c:Value>176e8955-bc8e-488a-9cb2-
b4fbffa547b3</c:Value> </c:ContactID> </c:ContactIDCollection> <c:Name
Collection> <c:Name c:ElementID="86ef8fab-e13d-4b52-9cf5-
ec0601898181"> <c:Title>保持神秘</c:Title> <c:FormattedName>Mystery
Man</c:FormattedName> <c:GivenName>Mystery
Man</c:GivenName> </c:Name> </c:NameCollection> <c:PhotoCollection>
<c:Photo c:ElementID="fdfaef8f-b334-4c80-813c-83d391488eb4"> <c:Url
```

行 1, 列 1

100%

Windows (CRLF)

UTF-8

需要解密的文本 ↓ 密钥(key): 字数统计 一键解密 粘贴剪切板 清空内容

LF2XGYPPXSGOP04E465YPZMITLSYRGXGWS70JOEL4202LZFYQDSLKXEX056LCVB566IZ7FPW7S37K7HQK46LLUM42EJB354RTSL3IHFR6VONHE
J4S4ITZNEVHTJPNXJS620HAECGZGCWWRVOBUXMNKMGJTTKTDZME2TKU3PGVMWS5ZVGVYUKYJSKY2TON3ZJU2VSK3WGVGHK3BVG VJW6NLBGZCDK3
3NKQ2WE6KBGU3XKRJVG52UQNJOVNDKTBSM42TK4KFGVRGK3BVLFLTGNBUINBTKYTFNQ2VSVZTGVNE00JVLJBU4NKMGSZDKNCXNY2UY4KHGVGHS
ZZVG52WMNSLMVCTKWLJLI2DIQ2DMEZFMNJXG54WCT2EJF3VSV2NGVGW2SJVJVFKNCKRIXSWLNJJUVS6SJGNMTERLZJ5KFM3KNK5HG2TSEM46Q
=====

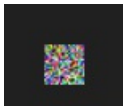
解密结果 ↓ 复制内容 ↑ 解密结果转至文本框 ↑

一键解密: | 结果
base64解码:
base32解码: Yusa, 组织刚刚派下来一个任务, 请快点完成, 你只有三天时间。6L+Z5piv5L2g5Lya55So5Yiw55qEa2V577yM5Y+v5
Lul55So5a6D5omI5byA57uE57uH57uZ5L2g55qE5be15YW344CC5be15YW35ZG95ZCN5L6d54Wn5LqG5Lyg57uf6KeE5YiZ44CCa2V577ya0DIw
YWM5MmI5Zju4MTQyYmJiYzI3Y2EyOTVnMWNmNDg=
base16解码: __

发现是base32编码, 后面还有一段base, 接着解密



得到了key: `820ac92b9f58142bbbc27ca295f1cf48`, 这应该就是key.bmp的密码了



成功得到了, 接着把文件都跟刚刚的exp放同一个目录下尝试运行

```
文件(F) 编辑(E) 视图(V) 导航(N) 代码(C) 重构(R) 运行(U) 工具(T) VCS(S) 窗口(W) 帮助(H) 取证 - exp.py
取证 \ exp.py
项目
  取证 C:\Users\Yijiale\Desktop\取证
    1.zip
    2.zip
    exp.py
    file.None.0xfffffa8003b86010.dat
    file.None.0xfffffa8002842f10.dat
    flag
    key.bmp
    StickyNotes.snt
    vol.exe
    Who_am_I
    Yusa-PC.raw
  外部库
  草稿文件和控制台

exp.py x flag x
1 from PIL import Image
2 import struct
3 pic = Image.open('key.bmp')
4 fp = open('Flag', 'rb')
5 fs = open('Who_am_I', 'wb')
6
7 a, b = pic.size
8 list1 = []
9 for y in range(b):
10     for x in range(a):
11         pixel = pic.getpixel((x, y))
12         list1.extend([pixel[1], pixel[0], pixel[2], pixel[2], pixel[1], pixel[0]])
13
14 data = fp.read()
15 for i in range(0, len(data)):
16     fs.write(struct.pack('B', data[i] ^ list1[i % a*b*6]))
17 fp.close()
18 fs.close()
19

运行: exp x
D:\Cc\Python\python.exe C:/Users/Yijiale/Desktop/取证/exp.py
进程已结束, 退出代码为 0
```

运行完成后, 并没有看到flag, 后来发现, flag跟Who_am_I文件需要在exp中互换一下位置

因为刚刚运行了一下导致Who_am_I为空了, 所以这里重新导入Who_am_I文件, 运行一下, 得到了一张gif图, 我们改一下后缀, 发现是在放烟花



逐一分帧查看后得到了flag



flag:

```
DASCTF{c3837c61-77f1-413e-b2e6-3ccbc96df9f4}
```

Cry部分

密码人集合

赛题详情

题目名称: 密码人集合

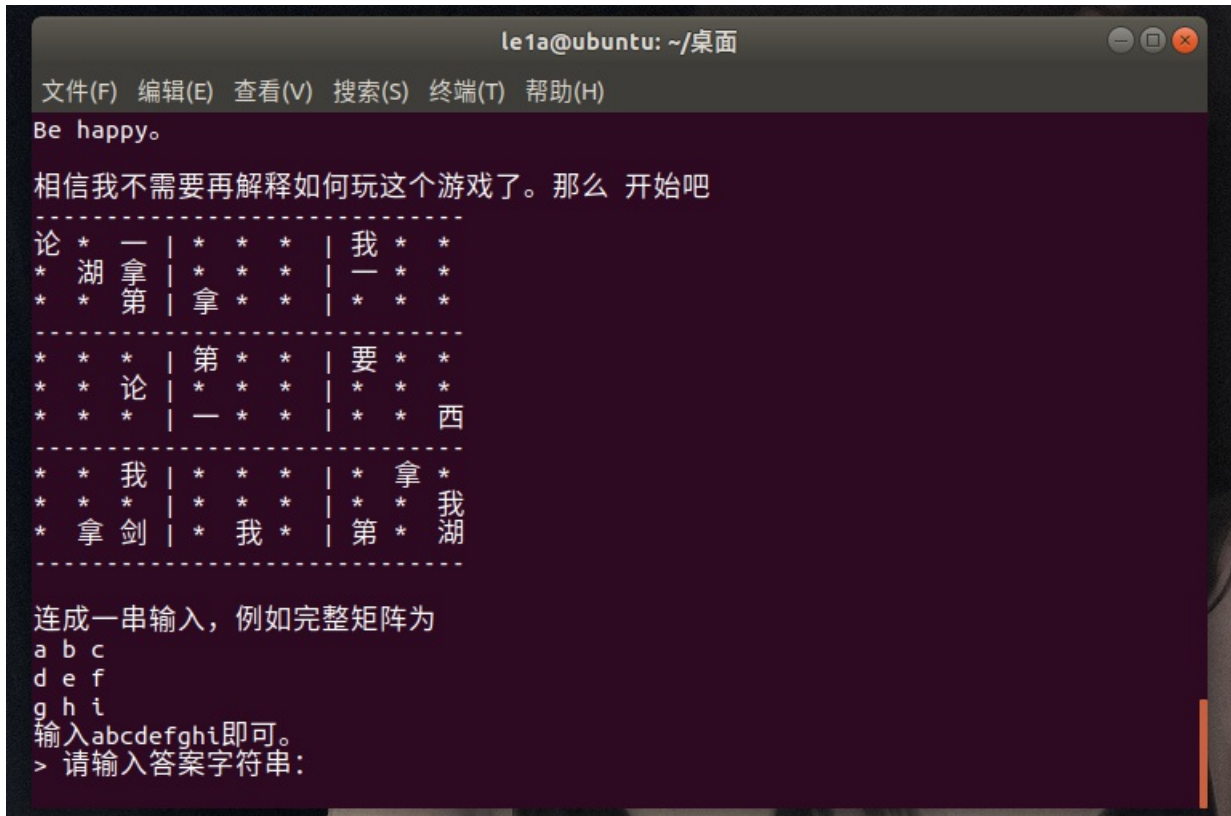
题目内容: A gift for u. enjoy it. XD

题目分数: 100

当前答出前3名: 第一名 V&N 第二名 Nu1L 第三名 坏女人万岁

相关附件: [靶机附件](#) [下载](#)

直接nc上去，得到一副矩阵，上面有 [我要拿西湖论剑第一](#) 的字样，看起来很像数独游戏



把 我要拿西湖论剑第一 转化为 1-9 的数字，找一个在线网站填上去

在线网址: <https://shudu.gwalker.cn/>

数独求解器

6	2	9	4	5	7	1	8	3
1	5	3	2	6	8	9	4	7
4	7	8	3	9	1	5	2	6
3	1	5	8	4	6	2	7	9
9	4	6	1	7	2	3	5	8
7	8	2	9	3	5	6	1	4
5	6	1	7	8	9	4	3	2
8	9	4	5	2	3	7	6	1
2	3	7	6	1	4	8	9	5

清空

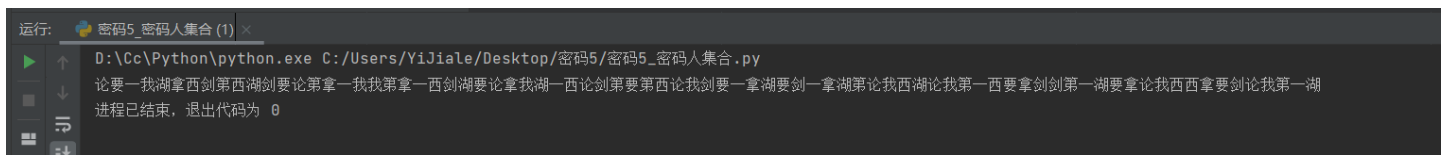
返回

得到结果后，按照先读小方格再读大方格的顺序依次写出来，得到

629153478457268391183947526315946782846172935279358614561894237789523614432761895

然后再把这些数字按照刚刚的转换顺序，再转回汉字，写个小脚本

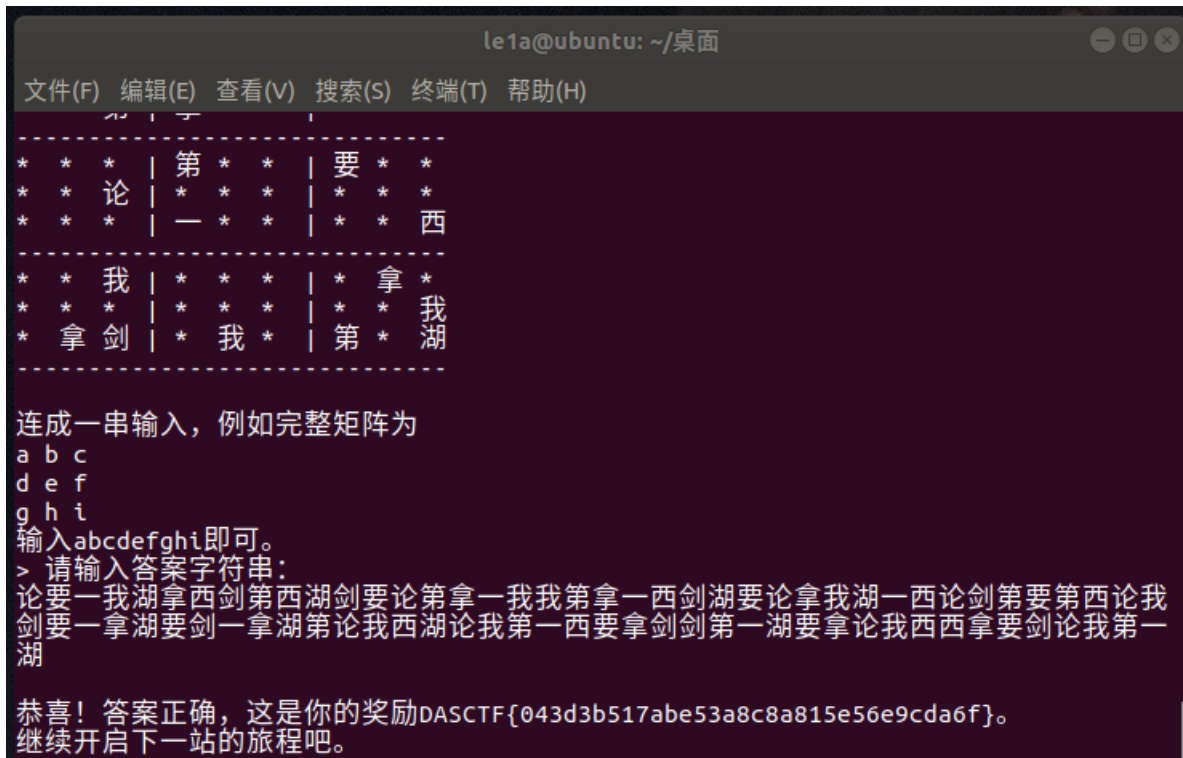
```
num=[6,2,9,1,5,3,4,7,8,4,5,7,2,6,8,3,9,1,1,8,3,9,4,7,5,2,6,3,1,5,9,4,6,7,8,2,8,4,6,1,7,2,9,3,5,2,7,9,3,5,8,6,1,4,5,6,1,8,9,4,2,3,7,7,8,9,5,2,3,6,1,4,4,3,2,7,6,1,8,9,5]
for i in num:
    if i == 1:print('我',end='')
    if i == 2:print('要',end='')
    if i == 3:print('拿',end='')
    if i == 4:print('西',end='')
    if i == 5:print('湖',end='')
    if i == 6:print('论',end='')
    if i == 7:print('剑',end='')
    if i == 8:print('第',end='')
    if i == 9:print('-',end='')
```



运行得到:

论要一我湖拿西剑第西湖剑要论第拿一我我第拿一西剑湖要论拿我湖一西论剑第要第西论我剑要一拿湖要剑一拿湖第论我西湖论我第一西要拿剑剑第一湖要拿论我西西拿要剑论我第一湖

把这个粘贴回虚拟机里，Enter一下，即可得到flag



flag:

DASCTF{043d3b517abe53a8c8a815e56e9cda6f}