




# 西湖论剑2021中国杭州网络安全技能大赛部分Writeup

原创

末初  于 2021-11-21 12:38:48 发布  8564  收藏 22

分类专栏: [CTF\\_MISC\\_Writeup](#) 文章标签: [2021西湖论剑](#)

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/mochu7777777/article/details/121444273>

版权



[CTF\\_MISC\\_Writeup](#) 专栏收录该内容

246 篇文章 46 订阅

订阅专栏

## 文章目录

### MISC

[真签到](#)

[YUSA的小秘密](#)

[Yusa的秘密](#)

### WEB

[灏妹的web](#)

MISC题目附件请自取

链接: [https://pan.baidu.com/s/1Hm1VQbeLPnxYLab\\_X1N2-A](https://pan.baidu.com/s/1Hm1VQbeLPnxYLab_X1N2-A)

提取码: obzz

## 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** 财贾夺Flag队

相关附件: [下载附件](#) [下载](#)

CSDN @末初

4\*



暗号对上, DASCTF{welc0m3\_t0\_9C51s\_2021} ~

温馨提醒, 本次比赛 flag 格式一般为 DASCTF{}/flag{}, 在界面上提交时只需要提交括号内的内容, 比如这个题你就只需要提交 welc0m3\_t0\_9C51s\_2021 作为 flag 即可!

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](#)

CSDN @末初

使用Stegsolve打开调整通道可以发现藏有flag; 但是被干扰倒是无法看清  
搜索引擎查阅资料发现题目这里指的是一种叫 **YCrCb** 颜色编码模型



jackwang 院士 2006-12-22 22:43:00 评分

2楼

问 另外请问:  
支持ITU601的**YCbCr4:2:2**格式与普通的**YCbCr4:2:2**格式有什么区别?

小弟刚刚涉及这些概念, 请大侠指点!

答 1: 详细介绍一下**YUV** (也称YCrCb) 是被欧洲电视系统所采用的一种颜色编码方法 (属于PAL制式)。**YUV**主要用于优化彩色视频信号的传输, 使其向后兼容老式黑白电视。与RGB视频信号传输相比, 它最大的优点在于只占用极少的带宽, 而RGB要求三个独立的视频信号同时传输。

在**YUV**中, "Y" 代表亮度 (Luminance或Luma), 也就是灰阶值; 而 "U" 和 "V" 表示的则是色度 (Chrominance或Chroma), 作用是描述影像色彩及饱和度, 用于指定像素的颜色。"亮度" 是通过RGB输入信号来创建的, 方法是将RGB信号的特定部分叠加到一起。"色度" 则定义了颜色的两个方面——色调与饱和度, 分别用Cr和Cb来表示。其中, Cr反映了RGB输入信号红色部分与RGB信号亮度值之间的差异, 而Cb反映的是RGB输入信号蓝色部分与RGB信号亮度值之间的差异, 此即所谓的色差信号, 也就是我们常说的分量信号 (Y、R-Y、B-Y)。

在专业领域了, "Y CB CR" 表示数字色差信号而不是模拟色差信号。色差信号Y,R-Y,B-Y信号一般通称为Y, Cr,Cb; 习惯上Y,Cr,Cb为数字(PCM)的色差信号, 模拟的色差信号则称Y,Pr,Pb, 所以我们常在DVD Player的内部看到Y,Cr,Cb而在DVD Player的外部看到色差输出标示为Y,Pr,Pb或**YUV**; **YUV**则是在欧洲电视系统PAL中的色差信号的通称, 包含数字及模拟的色差信号都称**YUV**, 所以当您看到**YUV**时您就要联想到它是PAL系统中的Y,R-Y,B-Y信号, 它可能是数字 (PCM) 的**YUV**, 也可能是模拟的**YUV**。答 2: 也就是说模拟和数字的区别了习惯上有所区别: "习惯上Y,Cr,Cb为数字(PCM)的色差信号, 模拟的色差信号则称Y,Pr,Pb, 所以我们常在DVD Player的内部看到Y,Cr,Cb而在DVD Player的外部看到色差输出标示为Y,Pr,Pb或**YUV**;"

实际上可能一样:

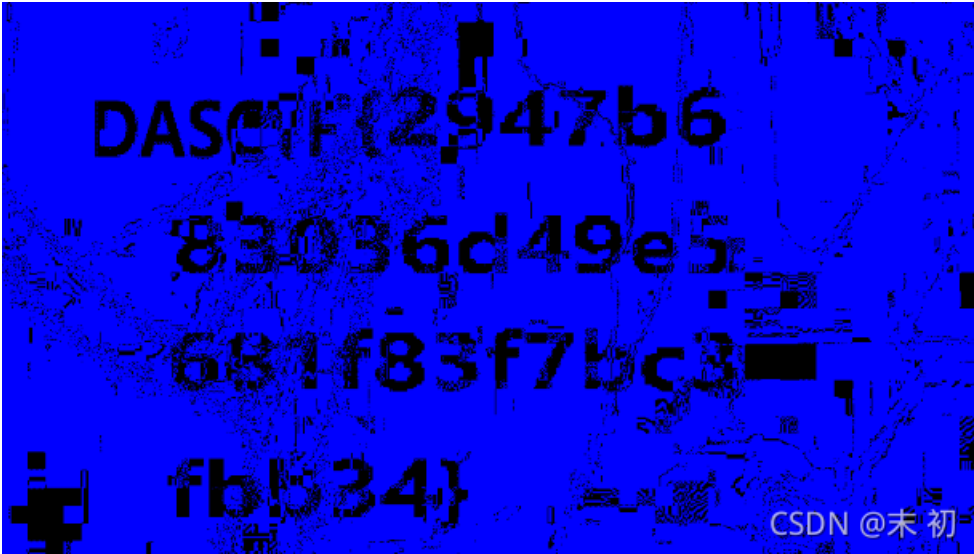
"**YUV**则是在欧洲电视系统PAL中的色差信号的通称, 包含数字及模拟的色差信号都称**YUV**, 所以当您看到**YUV**时您就要联想到它是PAL系统中的Y,R-Y,B-Y信号, 它可能是数字 (PCM) 的**YUV**, 也可能是模拟的**YUV**。"

谢谢雷风! 祝您新春快乐! 答 3: **YUV** 和 Y,Cr,Cb对于数字电路而言:**YUV** 和 Y,Cr,Cb只是相差128,**YUV**没有负值,Y,Cr,Cb最高位为符号位,U = Cr + 128;V = Cb + 128. 参见iru bt656 or ccir 656

CSDN @末初

```
from cv2 import *
img = cv2.imread('yusa.png')
cv_color = cv2.cvtColor(img, cv2.COLOR_BGR2YCrCb)
cv2.imwrite('flag.png', cv_color)
```

将得到图片再次使用Stegsolve打开调整通道



```
DASCTF{2947b683036d49e5681f83f7bc3fbb34}
```

## Yusa的秘密

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%20a%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

CSDN @末初

```
volatility -f Yusa-PC.raw --profile=Win7SP1x64 psxview
```

```

root@kali /home/mochu7/Desktop % volatility -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  vmttoolsd.exe     1520 True    True    True     True    True   True     True
0x000000003e6ca750  cmd.exe            2536 True    True    True     True    True   True     False
0x000000003e0804b0  vmttoolsd.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
0x000000003e277b30  sppsvc.exe         1736 True    True    True     True    True   True     True
0x000000003f2cb260  wmpnetwk.exe       2792 True    True    True     True    True   True     True
0x000000003e903a10  lsm.exe            512  True    True    True     True    True   True     False
0x000000003e61ab30  vmacthlp.exe       680  True    True    True     True    True   True     False
0x000000003f70a920  wab.exe            2448 True    True    True     True    True   True     False
0x000000003e68b460  StickyNot.exe      2228 True    True    True     True    True   True     False
0x000000003e557b30  VGAuthService.    1468 True    True    True     True    True   True     True
0x000000003e312520  msdtc.exe          308  True    True    True     True    True   True     True
0x000000003e9fe9f0  svchost.exe        620  True    True    True     True    True   True     False
0x000000003e2b3560  WmiPrvSE.exe       1908 True    True    True     True    True   True     True
0x000000003e7deb30  explorer.exe       2276 True    True    True     True    True   True     False
0x000000003e8d2b30  taskhost.exe       2160 True    True    True     True    True   True     False
0x000000003e8dfb30  wininit.exe        388  True    True    True     True    True   True     True
0x000000003e79a6e0  svchost.exe        984  True    True    True     True    True   True     True
0x000000003e904b30  lsass.exe          504  True    True    True     True    True   True     False
0x000000003f4cdb30  smss.exe           244  True    True    True     True    False  False   False
0x000000003eb50340  csrss.exe          336  True    True    True     True    False  True    True
0x000000003e8e15d0  csrss.exe          396  True    True    True     True    False  True    False
0x000000003ff7cae0  System             4    True    True    True     True    False  False   False
0x000000003fa41060  dllhost.exe        1000 True    True    True     False   False  True    False
0x000000003f1c07d0  wab.exe            3020 False   True    False    False   False  False   False

```

2021-10-28 06:10:16 UTC+0000  
CSDN @未初

分析可疑进程

- **wab.exe** : 是Windows操作系统自带的程序，用于储存地址簿、联系人和Email地址。用以支持类似Outlook之类的程序。
- **StickyNot.exe** : Windows便签程序

首先还是先来看一下五个彩蛋吧(虽然没啥用)





```
>>> from base64 import *from base64 import *
>>> b64decode('eXVzYelWnkOWnkOacieWlveWkmulvewkmueahOWwj+Woh+Wmu++8j0a4o+eUtw==').decode('utf-8')
'yusa姐姐有好多好多的小娇妻，渣男'
```

egg5

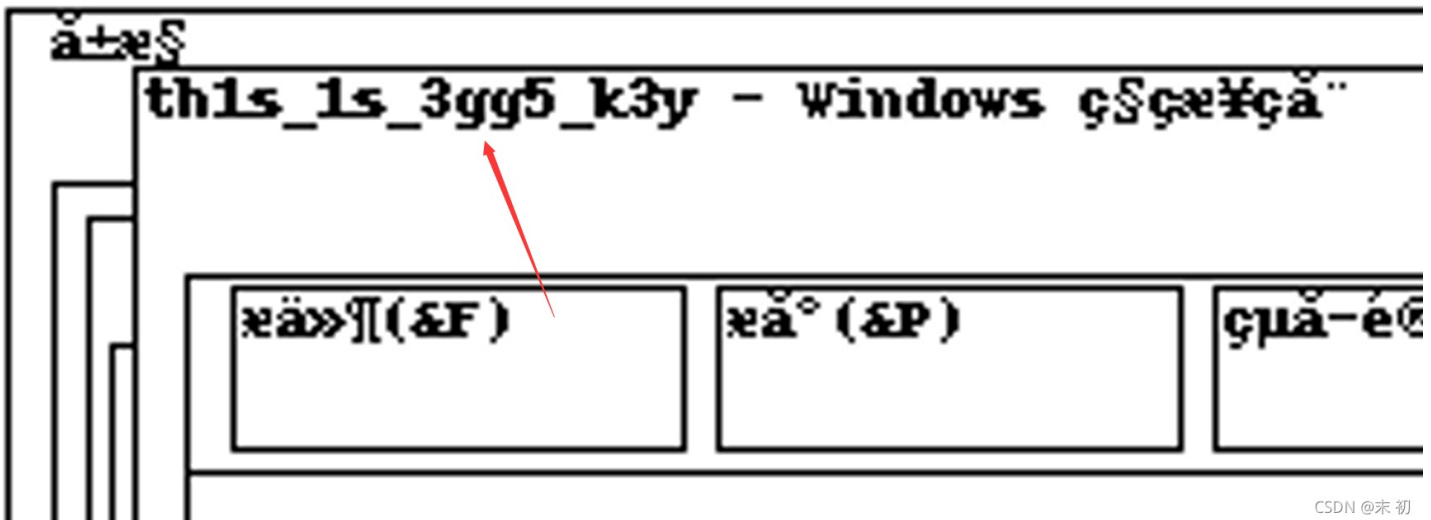
```
File Edit View Bookmarks Settings Help
root@kali /home/mochu7/Desktop % volatility -f Yusa-PC.raw --profile=Win7SP1x64 filescan | grep 'egg5'
Volatility Foundation Volatility Framework 2.6
0x000000003f2ae290 1 0 R--r-- \Device\HarddiskVolume2\Users\Yusa\Desktop\Sakura文件\Sakura-egg5
root@kali /home/mochu7/Desktop % volatility -f Yusa-PC.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000003f2ae290 -D ./
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x3f2ae290 None \Device\HarddiskVolume2\Users\Yusa\Desktop\Sakura文件\Sakura-egg5
root@kali /home/mochu7/Desktop % ls
egg5.zip file.None.0xfffffa8003d02010.dat Yusa-PC.raw
root@kali /home/mochu7/Desktop % file file.None.0xfffffa8003d02010.dat
file.None.0xfffffa8003d02010.dat: Zip archive data, at least v2.0 to extract
root@kali /home/mochu7/Desktop %
```

CSDN @末初

egg5.zip 有密码，密码在截屏中

```
root@kali /home/mochu7/Desktop % volatility -f Yusa-PC.raw --profile=Win7SP1x64 screenshot -D ./
Volatility Foundation Volatility Framework 2.6
Wrote ./session_0.msswindowstation.mssrestricteddesk.png
Wrote ./session_0.Service-0x0-3e4$.Default.png
Wrote ./session_0.Service-0x0-3e5$.Default.png
Wrote ./session_0.WinSta0.Default.png
Wrote ./session_0.WinSta0.Disconnect.png
Wrote ./session_0.WinSta0.Winlogon.png
Wrote ./session_0.Service-0x0-3e7$.Default.png
Wrote ./session_1.WinSta0.Default.png
Wrote ./session_1.WinSta0.Disconnect.png
Wrote ./session_1.WinSta0.Winlogon.png
root@kali /home/mochu7/Desktop % ls
egg5.zip 'session_0.Service-0x0-3e4$.Default.png' session_0.WinSta0.Default.png session_1.WinSta0.Default.png Yusa-PC.raw
file.None.0xfffffa8003d02010.dat 'session_0.Service-0x0-3e5$.Default.png' session_0.WinSta0.Disconnect.png session_1.WinSta0.Disconnect.png
'session_0.msswindowstation.mssrestricteddesk.png' 'session_0.Service-0x0-3e7$.Default.png' session_0.WinSta0.Winlogon.png session_1.WinSta0.Winlogon.png
root@kali /home/mochu7/Desktop %
```

CSDN @末初



CSDN @末初

this\_1s\_3gg5\_k3y

```
egg5.txt
1 yusa姐姐希望西湖论剑的flag格式为yusameinv{.*?}, 我就不^_^|
```

彩蛋看完了，开始做题

```
volatility -f Yusa-PC.raw --profile=Win7SP1x64 filescan | grep -E '.zip$|.rar$|.7z$'
```



```
File Edit View Bookmarks Settings Help
root@kali /home/mochu7/Desktop % volatility -f Yusa-PC.raw --profile=Win7SP1x64 filescan | grep -E '.zip$|.rar$|.7z$'
Volatility Foundation Volatility Framework 2.6
0x000000003f3356f0 1 0 R--rw- \Device\HarddiskVolume2\PROGRA~1\MSBuild\MICROS~1\WINDOW~1\key.zip
root@kali /home/mochu7/Desktop % volatility -f Yusa-PC.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000003f3356f0 -D ./
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x3f3356f0 None \Device\HarddiskVolume2\PROGRA~1\MSBuild\MICROS~1\WINDOW~1\key.zip
root@kali /home/mochu7/Desktop % ls
file.None.0xfffffa800284bd00.dat Yusa-PC.raw
root@kali /home/mochu7/Desktop % file file.None.0xfffffa800284bd00.dat
file.None.0xfffffa800284bd00.dat: Zip archive data, at least v2.0 to extract
root@kali /home/mochu7/Desktop % mv file.None.0xfffffa800284bd00.dat key.zip
root@kali /home/mochu7/Desktop % ls
key.zip Yusa-PC.raw
root@kali /home/mochu7/Desktop %
```

CSDN @末初

key.zip 需要密码；继续分析

调用过 StickyNot.exe，尝试寻找 snt 文件

## 什么是SNT文件？

由Sticky Notes创建的文件，Sticky Notes是Windows Vista和Windows 7附带的桌面笔记程序；保存漂浮在桌面上的一个或多个便签；将每个笔记的文本，字体，颜色和位置存储在桌面上；允许即使用户注销Windows并再次登录也可以保存打开的便签。

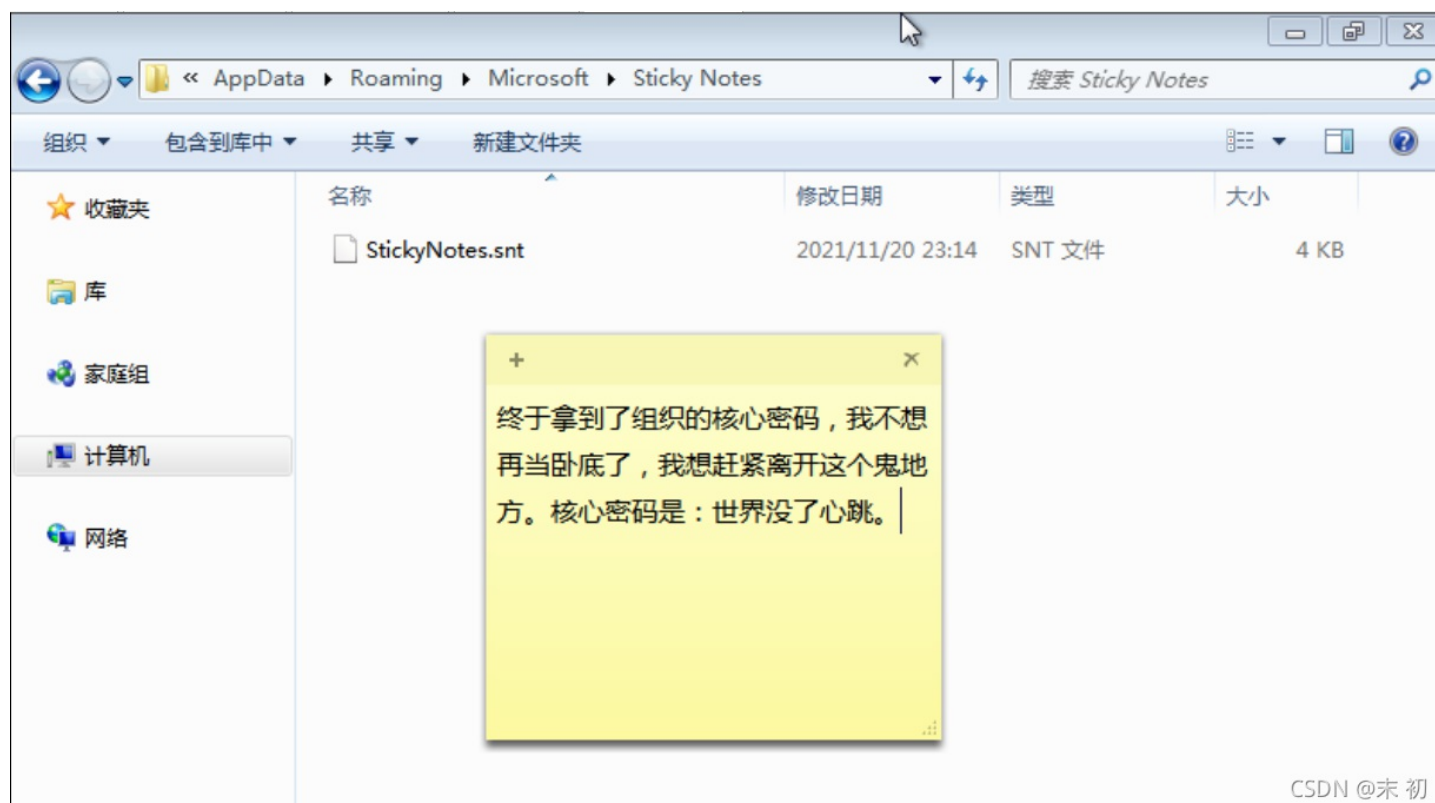
```
root@kali /home/mochu7/Desktop % volatility -f Yusa-PC.raw --profile=Win7SP1x64 filescan | grep -E '.snt$'
Volatility Foundation Volatility Framework 2.6
0x000000003fb306e0 16 1 RW-r-- \Device\HarddiskVolume2\Users\Yusa\AppData\Roaming\Microsoft\Sticky Notes\StickyNotes.snt
root@kali /home/mochu7/Desktop % volatility -f Yusa-PC.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000003fb306e0 -D ./
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x3fb306e0 None \Device\HarddiskVolume2\Users\Yusa\AppData\Roaming\Microsoft\Sticky Notes\StickyNotes.snt
root@kali /home/mochu7/Desktop % ls
file.None.0xfffffa8003e70590.dat key.zip Yusa-PC.raw
root@kali /home/mochu7/Desktop % file file.None.0xfffffa8003e70590.dat
file.None.0xfffffa8003e70590.dat: Composite Document File V2 Document, Cannot read section info
root@kali /home/mochu7/Desktop %
```

导出文件，使用win7的便签去加载这个文件

PS: 经测试，Win10也可以这样加载

位置: C:\Users\xxx\AppData\Roaming\Microsoft\Sticky Notes\StickyNotes.snt

PS: 可能找不到这个 **Sticky Notes** 文件夹，可以开启一个临时便签之后即可发现有这个文件夹



CSDN @末初

然后使用我们导出的 **StickyNotes.snt** 替换这里临时生成 **StickyNotes.snt** 即可；然后再次打开便签即可发现线索

**key.zip** 密码：**世界没了心跳**

得到 **exp.py**

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

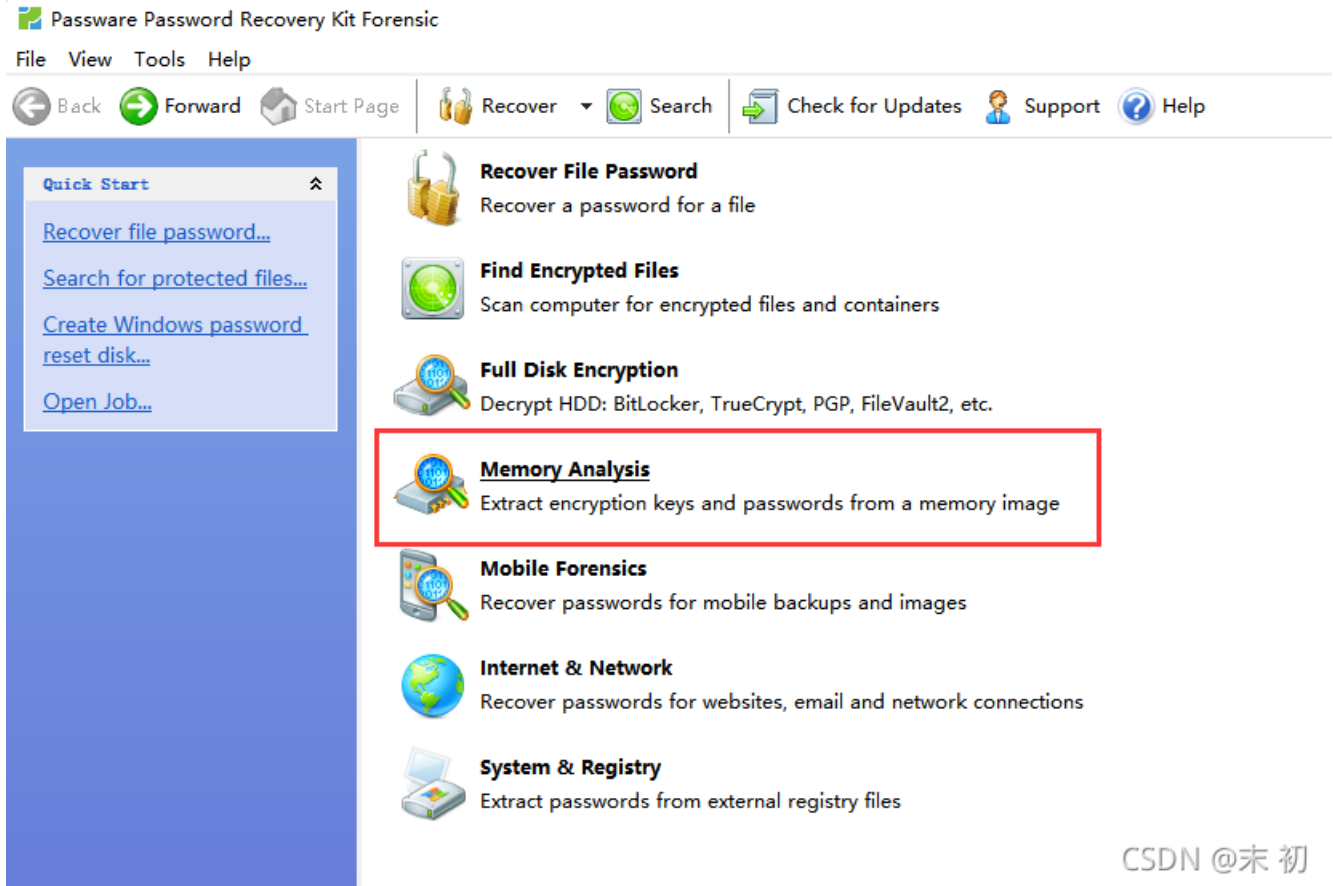
a, b = pic.size
list1 = []
for y in range(b):
    for x in range(a):
        pixel = pic.getpixel((x, y))
        list1.extend([pixel[1], pixel[0], pixel[2], pixel[2], pixel[1], pixel[0]])

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()
```

需要得出的是 **flag** 文件，**Who\_am\_I.zip** 有密码；whoami在这里指的应该是Yusa；

```
File Edit View Bookmarks Settings Help
root@kali /home/mochu7/Desktop % volatility -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:::
root@kali /home/mochu7/Desktop %
```

尝试破解Yusa账户的密码，使用 [Passware Kit 13](#)



Passware Password Recovery Kit Forensic

File View Tools Help

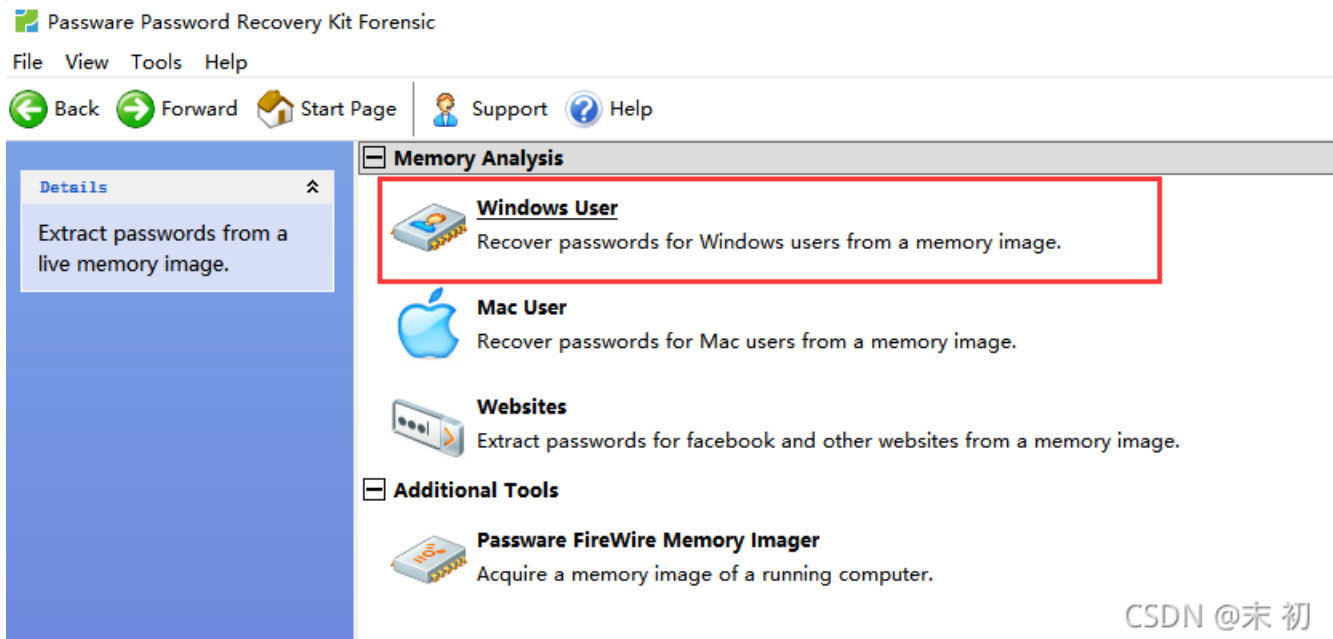
Back Forward Start Page Recover Search Check for Updates Support Help

**Quick Start**

- [Recover file password...](#)
- [Search for protected files...](#)
- [Create Windows password reset disk...](#)
- [Open Job...](#)

- Recover File Password**  
Recover a password for a file
- Find Encrypted Files**  
Scan computer for encrypted files and containers
- Full Disk Encryption**  
Decrypt HDD: BitLocker, TrueCrypt, PGP, FileVault2, etc.
- Memory Analysis**  
Extract encryption keys and passwords from a memory image
- Mobile Forensics**  
Recover passwords for mobile backups and images
- Internet & Network**  
Recover passwords for websites, email and network connections
- System & Registry**  
Extract passwords from external registry files

CSDN @末初



Passware Password Recovery Kit Forensic

File View Tools Help

Back Forward Start Page Support Help

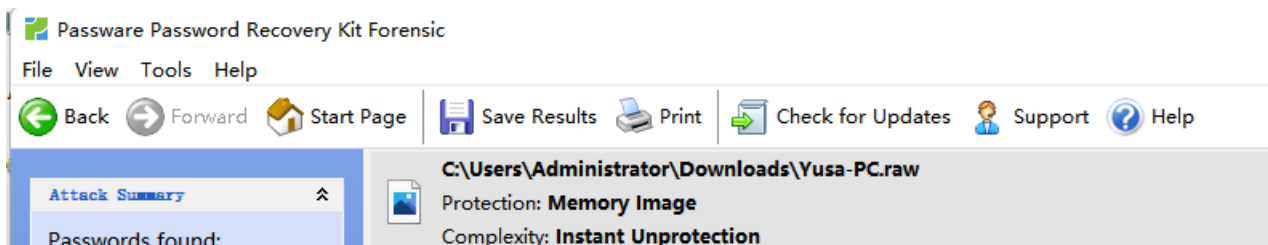
**Memory Analysis**

- Windows User**  
Recover passwords for Windows users from a memory image.
- Mac User**  
Recover passwords for Mac users from a memory image.
- Websites**  
Extract passwords for facebook and other websites from a memory image.
- Additional Tools**
  - Passware FireWire Memory Imager**  
Acquire a memory image of a running computer.

**Details**

Extract passwords from a live memory image.

CSDN @末初



Passware Password Recovery Kit Forensic

File View Tools Help

Back Forward Start Page Save Results Print Check for Updates Support Help

**Attack Summary**

Passwords found:

C:\Users\Administrator\Downloads\Yusa-PC.raw

Protection: **Memory Image**

Complexity: **Instant Unprotection**

# 1 password

Total time elapsed:

**25 sec.**

Estimated completion time:

**[completed]**

**Memory image file:** Yusa-PC.raw  
**Folder:** C:\Users\Administrator\Downloads\  
**Protection:** Memory Image - 1 Password(s)  
**Complexity:** Instant Unprotection

YUSA-PC\Yusa password: [YusaYusa520] (no brackets) <Copy>

CSDN @末初

得到密码: YusaYusa520

解压得到 Who\_am\_I

Who\_am\_I 有了, 就差 key.bmp 文件就可以得到 flag 文件了

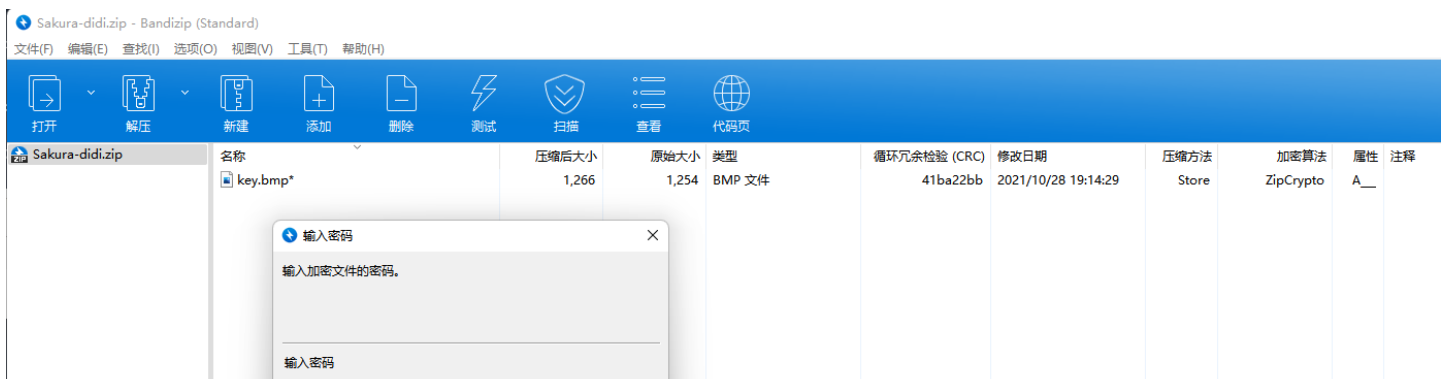
```
File Edit View Bookmarks Settings Help
root@kali /home/mochu7/Desktop % volatility -f Yusa-PC.raw --profile=Win7SP1x64 filescan | grep "Sakura"
Volatility Foundation Volatility Framework 2.6
0x000000003e58ada0 1 0 R--r-- \Device\HarddiskVolume2\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\Sakura-didi
0x000000003e78c6a0 1 0 R--r-- \Device\HarddiskVolume2\Users\Yusa\Desktop\Sakura文件\Sakura-公告
0x000000003f2ae290 1 0 R--r-- \Device\HarddiskVolume2\Users\Yusa\Desktop\Sakura文件\Sakura-egg5
0x000000003f959980 1 0 R--r-- \Device\HarddiskVolume2\Users\Yusa\Desktop\Sakura文件\Sakura-备忘录
0x000000003faa3a20 2 0 RW-rw- \Device\HarddiskVolume2\Users\Yusa\AppData\Roaming\Microsoft\Windows\Recent\Sakura文件.lnk
0x000000003fab220 1 0 R--r-- \Device\HarddiskVolume2\Users\Yusa\Desktop\Sakura文件\Sakura-logo
root@kali /home/mochu7/Desktop %
```

```
root@kali /home/mochu7/Desktop % ls
key.zip Yusa-PC.raw
root@kali /home/mochu7/Desktop % volatility -f Yusa-PC.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000003e58ada0 -D ./
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x3e58ada0 None \Device\HarddiskVolume2\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\Sakura-didi
root@kali /home/mochu7/Desktop % ls
file.None.0xfffffa8003bd2ba0.dat key.zip Yusa-PC.raw
root@kali /home/mochu7/Desktop % file file.None.0xfffffa8003bd2ba0.dat
file.None.0xfffffa8003bd2ba0.dat: Zip archive data, at least v2.0 to extract
root@kali /home/mochu7/Desktop % mv file.None.0xfffffa8003bd2ba0.dat Sakura-didi.zip
root@kali /home/mochu7/Desktop % ls
key.zip Sakura-didi.zip Yusa-PC.raw
root@kali /home/mochu7/Desktop %
```

CSDN @末初

```
root@kali /home/mochu7/Desktop % ls
key.zip Yusa-PC.raw
root@kali /home/mochu7/Desktop % volatility -f Yusa-PC.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000003e58ada0 -D ./
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x3e58ada0 None \Device\HarddiskVolume2\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\Sakura-didi
root@kali /home/mochu7/Desktop % ls
file.None.0xfffffa8003bd2ba0.dat key.zip Yusa-PC.raw
root@kali /home/mochu7/Desktop % file file.None.0xfffffa8003bd2ba0.dat
file.None.0xfffffa8003bd2ba0.dat: Zip archive data, at least v2.0 to extract
root@kali /home/mochu7/Desktop % mv file.None.0xfffffa8003bd2ba0.dat Sakura-didi.zip
root@kali /home/mochu7/Desktop % ls
key.zip Sakura-didi.zip Yusa-PC.raw
root@kali /home/mochu7/Desktop %
```

CSDN @末初





得到 `Sakura-didi.zip`，但是还是有密码；继续分析，还有一个线索没有利用到就是 `wab.exe` 联系人文件后缀名为 `.contact`

## 什么是一 .CONTACT 文件?

附加了文件名为 `.contact` 被扩展也称为 Windows 联系人文件，并且这些文件通常被分类为数据文件。联系人文件所使用的，是由微软，还开发了 CONTACT 文件格式开发的 Windows 联系人应用程序。微软 Windows 联系人软件被列为被内置到基于 Microsoft Windows 的系统，尤其是微软的 Windows 7 和 Windows Vista 中的联系人管理应用程序。这些联系的文件的内容包括：通过与 Microsoft Windows 联系人软件包括在文件中的接触的用户输入的信息。这些细节在保存用户名为 `.contact` 的文件包括姓名，地址，电子邮件地址和电话号码之间的有关关联到联系人列表条目的个人或组织其他信息的。这些接触文件还可能包含的个人或机构的标志图像或照片。基于 Microsoft Windows 的系统的用户可以安装微软的 Windows Live Mail 软件和微软的 Windows Mail 程序来实施这些接触文件的支持，并且还集成了电子邮件管理功能集成到他们的系统。用于这些图标名为 `.contact` 文件相关联并通过相应的联系的文件创建者存储的照片或数字图像

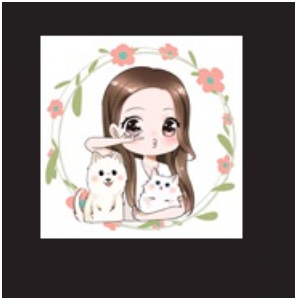
CSDN @末初

```
root@kali /home/mochu7/Desktop % ls
key.zip Sakura-didi.zip Yusa-PC.raw
root@kali /home/mochu7/Desktop % volatility -f Yusa-PC.raw --profile=Win7SP1x64 filescan | grep "contact"
Volatility Foundation Volatility Framework 2.6
0x000000003e748f20 1 0 R--r-d \Device\HarddiskVolume2\Users\Yusa\Contacts\Yusa.contact
0x000000003fa09070 1 0 R--r-d \Device\HarddiskVolume2\Users\Yusa\Contacts\Mystery Man.contact
root@kali /home/mochu7/Desktop %
```

`Yusa.contact`，将这些base64利用在线站解码：<https://the-x.cn/zh-cn/base64/>

```
C:\Users\Administrator\Downloads\Yusa.contact - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
Yusa.contact
1 <?xml version="1.0" encoding="UTF-8"?>
2 <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">
3   <c:Notes c:Version="1" c:ModificationDate="2021-10-28T10:55:46Z">一位经常忘事，所以会把重要的事情记录在便笺里的漂亮女孩</c:Notes><c:CreationDate>
2021-10-28T03:30:27Z</c:CreationDate><c:Extended xsi:nil="true"/>
4   <c:ContactIDCollection><c:ContactID c:ElementID="e2fb3eaa-f73d-4b85-8910-c410d1b64e4b"><c:Value>b2528d19-9d57-4470-9121-790ebe4f1ea3</c:Value></c:
ContactID></c:ContactIDCollection><c:NameCollection><c:Name c:ElementID="65c2cde-46b1-4a8d-a633-4bd47c6e7739"><c>Title c:Version="1" c:
ModificationDate="2021-10-28T05:43:58Z">吃饭</c>Title><c:GivenName c:Version="1" c:ModificationDate="2021-10-28T03:30:27Z">Yusa</c:GivenName><c:
FormattedName>Yusa</c:FormattedName></c:Name></c:NameCollection><c:PhotoCollection c:Version="1" c:ModificationDate="2021-10-28T03:30:27Z"><c:Photo
:ElementID="87a5e417-9be2-4199-a81f-bd57848f125d" c:Version="1" c:ModificationDate="2021-10-28T03:30:27Z"><c:Value c:ContentType="image/bmp" c:
Version="12" c:ModificationDate="2021-10-28T10:55:46Z">Qk1YFAAAAAAAAAFAAAAAoAAAAfGAAAH4AAAAABABAAAwAAAAH8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAPgA
5 AOAHAaAFAAAAAAAAAAAAAAAAAAAAAD//
6 //
7 //
8 //
9 //
10 //
11 //
12 //
13 //
14 //
15 //
16 //
17 //
18 //
19 //
20 //
21 //
22 //
23 //
24 //
25 //
26 //
27 //
28 //
29 //xv/dPUz9db1//f/533ffdc71zv0+c75xrfG+f63vne+ed4a31vn
30 FOf55jbm2u7//
31 //
32 //
33 ////3//7/1P1M/0T/ZX1//nvdc7xrf+d7Y1tne
```

得到一张bmp文件，但是这并不是我们想要的 `key.bmp`



## MysteryMan.contact

```

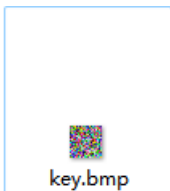
C:\Users\Administrator\Downloads\MysteryMan.contact - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
Yusa.contact MysteryMan.contact
1 <?xml version="1.0" encoding="UTF-8"?>
2 <c:contact c:Version="1" xmlns:c="http://schemas.microsoft.com/Contact" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:MSP2P="
http://schemas.microsoft.com/Contact/Extended/MSP2P">
3   <c:Notes c:Version="2" c:ModificationDate="2021-10-28T11:47:56Z">[F2XGYPXSGOP04E465YPZMITLSYRGXGWS70J0EL4202LZFYQDSLKXEX056LCVB566IZ2FPW7S37K7HQK46
LLUM42EJB354RTSL3IHFR6VONHEJ454ITZNEVHTJPNXJS620HAECGZGCWWRVOBUXMNMKGJTTKTDZME2TKU3PGVMMS5ZVGUVYKYJSKY2TON3ZJU2VSK3WGVGHK3BVGJW6NLBGZCDK33NKQ2WE6K8G
U3XKRJV652UQNJXOVNDKTB5M42TK4KFGVRGK3BVLFLTGNBUINBTKYTFNQ2VSVZTGVNEOOJVLJBU4NKMKGZSDKNCXNY2UY4KHGVBHSZZV652WMNSLMVCTKWJLI2DIQ2DMEZFMNJXG54WCT2EJF3VSV
2NGVGM2SJVLIJVFKNCKRIXSWLNJJUVS6SJGNMTERLZJ5KFM3KNK5HG2TSEM46Q===</c:Notes><c:CreationDate>2021-10-28T05:56:31Z</c:CreationDate><c:Extended xsi:nil=
"true"/>
4   <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:NameCollection><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 c:Version="1" c:ModificationDate="2021-10-28T06:06:09Z">C:\Users\Yusa\Desktop\QQ图片20211028140534.jpg</
c:Url></c:LabelCollection><c:Label>UserFile</c:Label></c:LabelCollection></c:Photo></c:PhotoCollection><c:PositionCollection c:Version="1" c:
ModificationDate="2021-10-28T06:21:33Z"><c:Position c:ElementID="2764bbad-0421-4e95-9e67-96338457cd41" c:Version="1" c:ModificationDate="
2021-10-28T06:21:33Z"><c:JobTitle c:Version="1" c:ModificationDate="2021-10-28T06:22:34Z">中层领导</c:JobTitle><c:Department c:Version="2" c:
ModificationDate="2021-10-28T06:22:34Z">Sakura组织</c:Department><c:LabelCollection><c:Label c:Version="1" c:ModificationDate="2021-10-28T06:21:33Z">
Business</c:Label></c:LabelCollection></c:Position></c:PositionCollection></c:contact>
CSDN @未初

```

## base32->base64

这是你会用到的key，可以用它打开组织给你的工具。工具命名依照了传统规则。key: 820ac92b9f58142bbbc27ca295f1c4f48

使用这个key解压 `Sakura-didi.zip`



解密脚本其实参考上面的 `exp.py` 即可，`key.bmp` 不变，将 `flag` 作为输出，`who_am_I` 作为输出即可，换一下位置



```

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

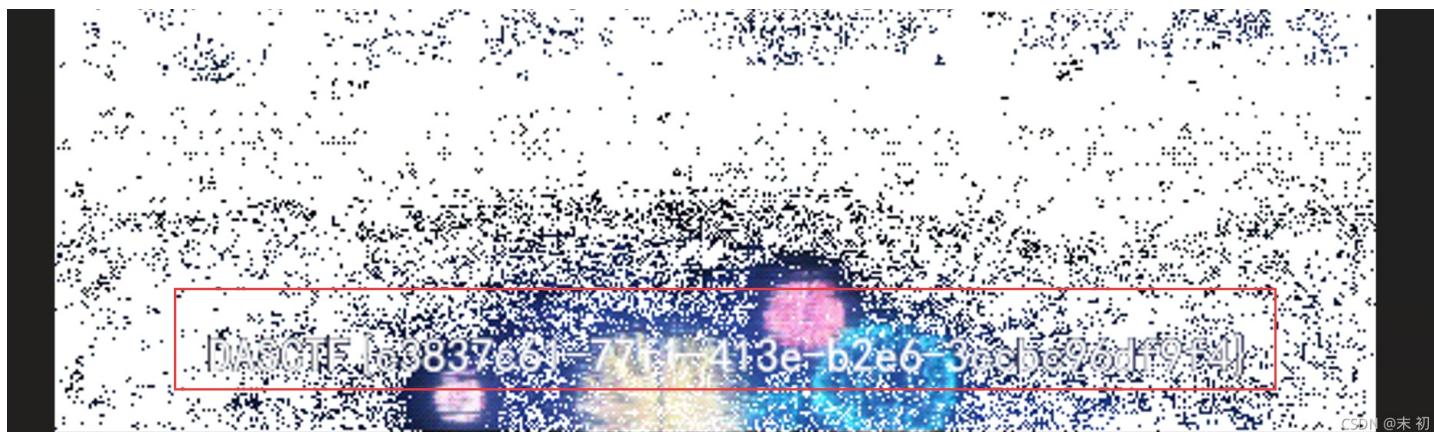
data = fp.read()

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

fp.close()
fs.close()

```

得到的 `flag` 是 `gif` 文件，使用 `stegsolve` 查看每一帧，第10帧能勉强看到flag



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

## WEB

### 灏妹的web

### 赛题详情

题目名称: 诱人的web

题目内容: 诱人上次拿向晚的生日加密压缩文件被我发现好康了的之后, 就马上痛定思痛, 开始用更加高技术的方式当好安恒第一顶碗人了, 他准备给向晚弄个小作文展示网, 不过在开发中似乎又被我发现了一些好康的。

题目分数: 100

当前答出前三名:

第一名 北门波波鱼

第二名 南门辣子鸡

第三名 volcano-中北

相关附件: 靶机附件 [下载](#)

CSDN @末初

### 目录扫描

```
python3 dirsearch.py -u "http://b1c34857-a729-4b00-a22a-98323505597c.haomeidehelloworld-ctf.dasctf.com:2333/" -i 200 | grep -v "0B"
```

扫描过程中发现多次 `/.idea/dataSources.xml` 这个路径, 扫出来的完整路径访问都是404

```
[09:44:56] Starting:
[09:44:57] 200 - 8KB - /.DS_Store
[09:45:46] Starting: .;/
[09:46:07] 200 - 221B - /././index.php/login/ (Added to queue)
[09:46:17] Starting: .admin/
[09:46:42] 200 - 221B - /.admin/index.php
[09:46:42] 200 - 221B - /.admin/index.php/login/ (Added to queue)
[09:46:55] Starting: .ansible/
[09:47:25] Starting: .aspnet/DataProtection-Keys/
[09:47:53] Starting: .apt_generated/
[09:47:57] 200 - 3KB - /.apt_generated/.idea/workspace.xml
[09:48:29] Starting: .axoCover/
[09:49:03] Starting: .aws/
[09:49:26] 200 - 221B - /.aws/index.php/login/ (Added to queue)
[09:49:42] Starting: .build/
[09:50:17] Starting: .buildpath/
[09:50:54] Starting: .bundle/
[09:51:34] Starting: .bzip/
[09:52:15] Starting: .c9revisions/
[09:52:18] 200 - 468B - /.c9revisions/.idea/dataSources.local.xml
[09:52:18] 200 - 505B - /.c9revisions/.idea/dataSources.xml
[09:52:18] 200 - 313B - /.c9revisions/.idea/encodings.xml
[09:52:18] 200 - 174B - /.c9revisions/.idea/misc.xml
[09:52:18] 200 - 272B - /.c9revisions/.idea/modules.xml
[09:52:41] 200 - 221B - /.c9revisions/index.php/login/ (Added to queue)
[09:53:07] Starting: .c9/
[09:54:02] Starting: .cache/
[09:54:48] Starting: .cabal-sandbox/
[09:55:30] Starting: .capistrano/
[09:56:20] Starting: .capistrano/metrics/
[09:57:06] Starting: .cfg/
[09:57:10] 200 - 468B - /.cfg/.idea/dataSources.local.xml
[09:57:10] 200 - 505B - /.cfg/.idea/dataSources.xml
[09:57:50] Starting: .circleci/
[09:58:31] Starting: .clcbio/
[09:59:03] Starting: .components/
```

CSDN @末初

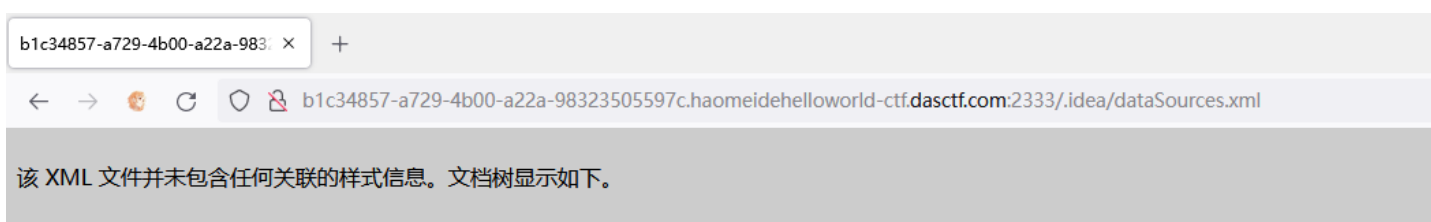
```
[10:13:06] Starting: .git-rewrite/
[10:13:48] Starting: .git/
[10:14:10] 200 - 221B - /.git/index.php
```



```
[10:14:10] 200 - 221B - /.git/index.php/login/ (Added to queue)
[10:14:23] Starting: .git/info/
[10:14:56] Starting: .git/logs/
[10:15:30] Starting: .git/branches/
[10:15:32] 200 - 468B - /.git/branches/.idea/dataSources.local.xml
[10:15:32] 200 - 505B - /.git/branches/.idea/dataSources.xml
[10:15:32] 200 - 313B - /.git/branches/.idea/encodings.xml
[10:15:32] 200 - 174B - /.git/branches/.idea/misc.xml
[10:15:32] 200 - 272B - /.git/branches/.idea/modules.xml
[10:16:06] Starting: .git/hooks/
[10:16:38] Starting: .git/refs/
[10:17:10] Starting: .git/objects/
[10:17:12] 200 - 468B - /.git/objects/.idea/dataSources.local.xml
[10:17:12] 200 - 174B - /.git/objects/.idea/misc.xml
[10:17:12] 200 - 505B - /.git/objects/.idea/dataSources.xml
[10:17:12] 200 - 272B - /.git/objects/.idea/modules.xml
[10:17:12] 200 - 313B - /.git/objects/.idea/encodings.xml
[10:17:42] Starting: .git2/
[10:18:03] 200 - 221B - /.git2/index.php
[10:18:03] 200 - 221B - /.git2/index.php/login/ (Added to queue)
[10:18:15] Starting: .github/
[10:18:17] 200 - 174B - /.github/.idea/misc.xml
[10:18:17] 200 - 272B - /.github/.idea/modules.xml
[10:18:17] 200 - 3KB - /.github/.idea/workspace.xml
[10:18:46] Starting: .gitignore/
[10:18:48] 200 - 3KB - /.gitignore/.idea/workspace.xml
[10:19:18] Starting: .gnome/
[10:19:21] 200 - 505B - /.gnome/.idea/dataSources.xml
[10:19:21] 200 - 468B - /.gnome/.idea/dataSources.local.xml
[10:19:21] 200 - 313B - /.gnome/.idea/encodings.xml
[10:19:21] 200 - 174B - /.gnome/.idea/misc.xml
[10:19:21] 200 - 272B - /.gnome/.idea/modules.xml
[10:19:51] Starting: .gnupg/
[10:19:53] 200 - 313B - /.gnupg/.idea/encodings.xml
[10:19:53] 200 - 174B - /.gnupg/.idea/misc.xml
[10:19:53] 200 - 272B - /.gnupg/.idea/modules.xml
[10:19:53] 200 - 3KB - /.gnupg/.idea/workspace.xml
[10:21:14] Starting: .gphoto/
```

CSDN @末初

尝试直接访问 `/.idea/dataSources.xml`



```
-<project version="4">
- <component name="DataSourceManagerImpl" format="xml" multifile-model="true">
- <data-source source="LOCAL" name="flag@localhost" uuid="9e687dff-ebb7-45db-b542-b1b5d7c402cd">
  <driver-ref>mysql.8</driver-ref>
  <synchronize>true</synchronize>
  <jdbc-driver>com.mysql.cj.jdbc.Driver</jdbc-driver>
- <jdbc-url>
  jdbc:mysql://DASCTF{e4bd12e6325597a2efa71744f2618f15}:3306
  </jdbc-url>
</data-source>
</component>
</project>
```

CSDN @末初