

# 2021春秋杯

原创

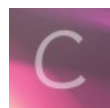
Ank1e 于 2021-12-08 10:49:35 发布 2276 收藏

分类专栏: [CTF Writeup](#) 文章标签: [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/qq\\_41636200/article/details/121786137](https://blog.csdn.net/qq_41636200/article/details/121786137)

版权



[CTF Writeup](#) 专栏收录该内容

11 篇文章 0 订阅

订阅专栏

## 2021春秋杯

### 战队信息

战队名称: 我发现这里有一个flag耶

战队排名: 31

### 解题情况

排名	队伍名称	总分	Misc					Cryp to	PWN			Reverse		Web	
			CT	se	he	Ma	问卷	Vi	su	Th	PW	Ba	Sn	ea	un
30	我**蚊	534			190		50	50							244
31	我发现这里有一个flag耶	530		380	50		50	50							
77	我**气	170			70		50	50							
135	我**斌	100					50	50							
190	我**歉	100					50	50							
203	b**我	100					50	50							
312	柒**我	100					50	50							
511	我**结	50					50								

### 解题过程

#### Crypto

## Input

Cipher Text:

```
cvnvwk lqae bw wzgy czrxlm gnaoiaafy. am ara xaufwiu qf
fwg mlfcckmnv tru aajtwxr pmed afw rfe zms ehvv bzmn lpiebq
yeeuiaa. zq hsl qrvq keskw fn jqswtvtp wjpwkmvuuq afw lzoz
feuarzksx lwoic qf unxhvdiluof litcjutq. amj usun jxwvijoh
vbvvlkluofl mekdgdw iieimldalbse bwetagk, imnqrkx ieoazewkmeo,
tunskc jmugramc, tzqbtgzvrzxk afw wf wf. fhw miru zms ohr
kpw fhakh gzale ag xym kqcggh eiluoftp zvvgelkmrt Aztwkrvb
kqcmkmg lqczgscwyf scbpca uamhxxzbaan, lai zvxaretzxf
eeunvzbq fratxytgz tjtmeqfs csft, rvv fhw litwfp pjbdv qf
fhw "zrvv'az cmi" grvaseexrk whorsmmfv azd etmebwzafvi
```

Cipher Variant:

Classical Vigenere

Language:

German

Key Length:

3-30

(e.g. 8 or a range e.g. 6-10)

Break Cipher

Clear Cipher Text

## Result

Clear text [\[hide\]](#)

Clear text using key "asterism":

```
nas many years of research experience and high technical level in
information security. his main research directions include
penetration testing, reverse engineering, binary security,
cryptography and so on. the team has won the third prize in the
second national industrial Internet security technology skills
competition, the information security triathlon training camp, and
the second prize in the "guan'an cup" management operation and
maintenance competition of isg network security skills
competition.cdusec welcome you, take your flag:53d613fc-6c5c-4dd6-
b3ce-8bc867c6f648
```

Details [\[show\]](#)

Key length statistics [\[show\]](#)

Histogram [\[show\]](#)

## MISC

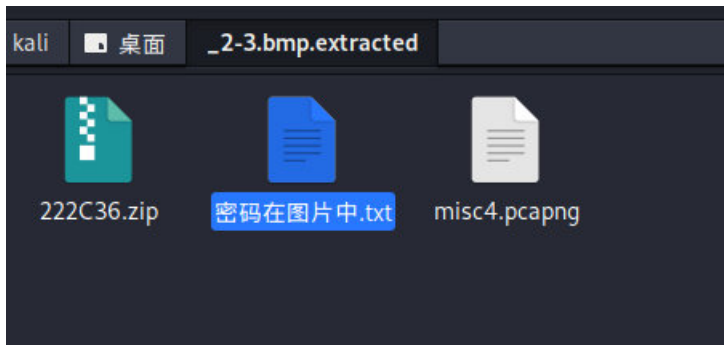
### helloworld

打开是个bmp图片，但是题目名字叫shark。直接用binwalk查看一下，发现压缩包。

```
(kali@kali)-[~/桌面/zsteg-master]
└─$ binwalk 2-3.bmp
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PC bitmap, Windows 3.x format,, 1152 x 648 x 24
2239542	0x222C36	Zip archive data, encrypted at least v2.0 to extract, compressed size: 599403, uncompressed size: 763412, name: misc4.pcapng
2839359	0x2B533F	End of Zip archive, footer length: 22

分离处理，压缩包有密码，显示密码在图片里。

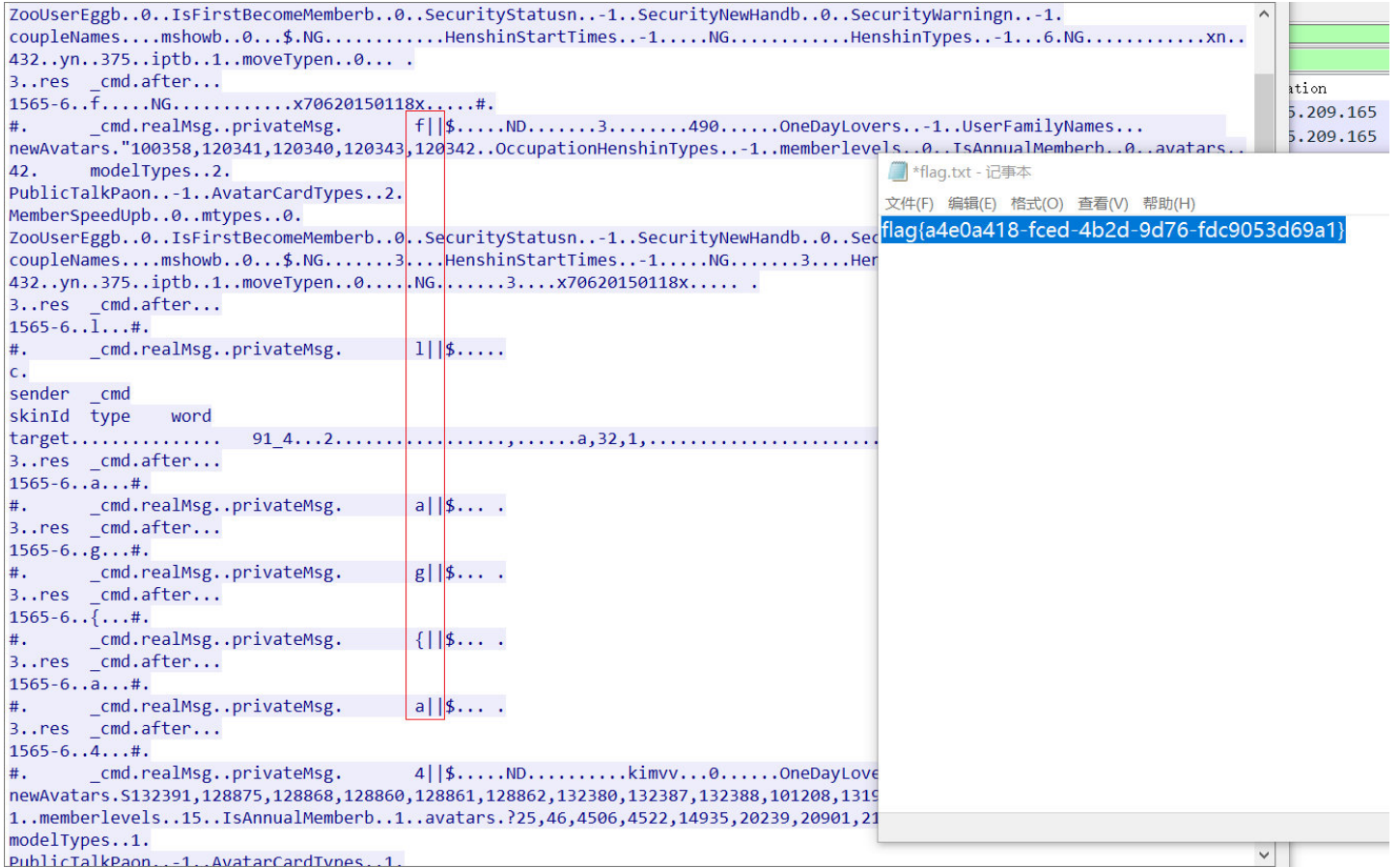


使用zsteg查看。找到密码。

```
文件 动作 编辑 查看 帮助
... /|
000000d0: 68 ea c7 84 48 ee a8 29 3e ed cd d3 2c 22 01 27 |h...H..>...
, ". '|
000000e0: fa bd e1 66 61 8b 26 e2 c8 69 be 13 80 51 60 42 |...fa.8..i..
.Q`B|
000000f0: 1a 92 c7 b1 06 fd e1 3e 6a e2 ad bb b0 49 48 a5 |.....>j...
.IH.|
imagedata .. text: ":ff:::::::::ff:"
b1,r,msb,xy .. file: Big-endian UTF-16 Unicode text, with very long lines, with no line terminators
b8,rgb,msb,xy .. file: RDI Acoustic Doppler Current Profiler (ADCP)
b1,r,lsb,yx .. text: "password:@91902AF23C#276C2FC7EAC615739CC7C0"
b4,rgb,msb,yx .. text: ["w" repeated 12 times]
b8,rgb,msb,yx .. file: RDI Acoustic Doppler Current Profiler (ADCP)
b2,rgb,lsb,yx,prime .. file: MPEG ADTS, layer III, v1, 160 kbps, 32 kHz, 2x Monoaural
b3,r,lsb,yx,prime .. file: very old 16-bit-int big-endian archive
b5,r,lsb,yx,prime .. file: MPEG ADTS, layer II, v1, 384 kbps, JntStereo
b8,r,msb,yx,prime .. file: ddis/ddif
b1,r,msb,Yx .. text: "0C7CC937516CAE7CF2C672#C32FA20919@drowssap"
b2,r,msb,Yx .. text: "_w_w_}_uWuwu"
b1,r,lsb,Yx,prime .. file: AIX core file fulldump
b4,rgb,msb,Yx,prime .. text: ["w" repeated 10 times]

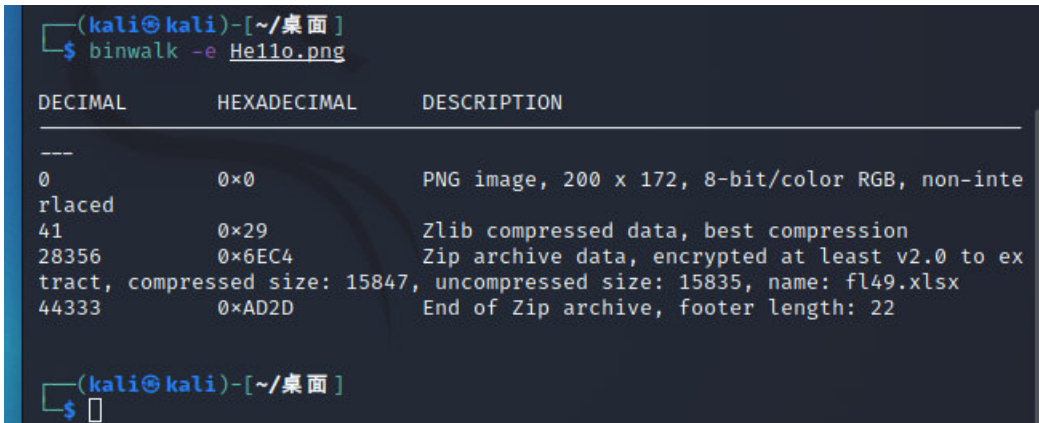
(kali@kali)-[~/桌面/zsteg-master]
└─$
```

解压得到一个流量包。查看流量包，在发包里面找到flag。



## secret\_chart

下载是个图片，查看末尾有个excel文件，直接binwalk分离一下，得到一个有密码的压缩包。



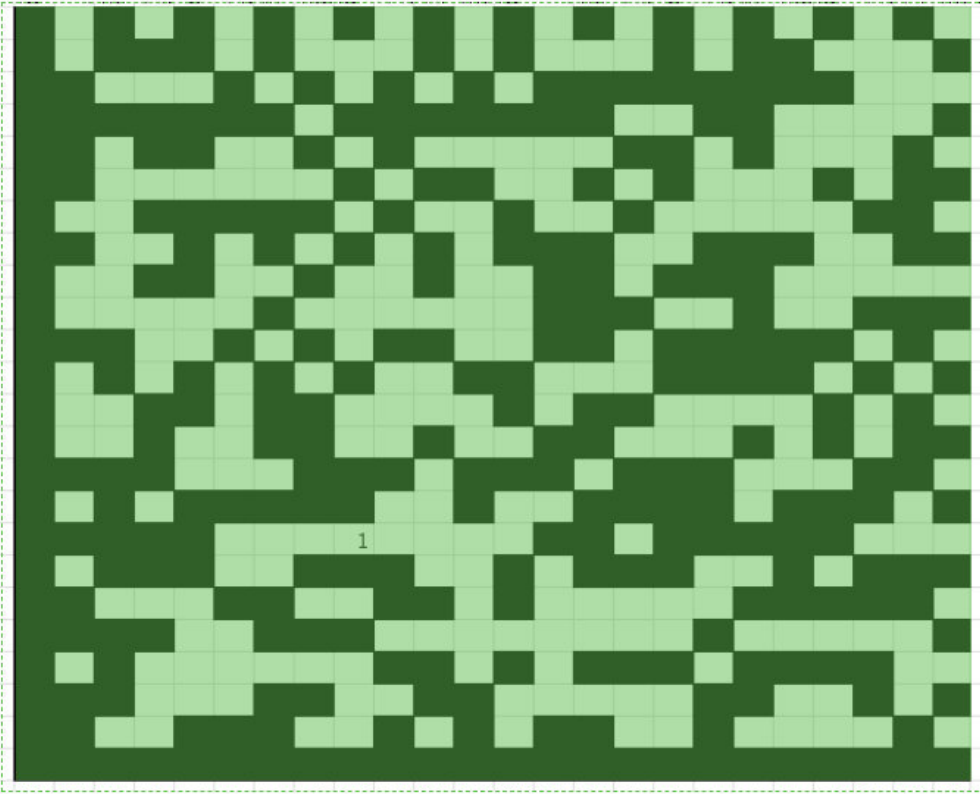
没有提示，爆破一下，得到密码。

解压是个excel。有6个月的表现。这里汇总到一个里面，然后看到有点像二维码，把所有的1填充成黑色。得到一个二维码

用这个网站: [Online Barcode Scanner](#) | [Barcode Reader SDK](#) | [Dynamsoft](#) 扫描得到一串字符

from camera

from local



Cost 93 ms.  
Found 1 barcode(s) in this file.  
▶ **DATAMATRIX** zfu{B3s1o9in1Nw0hal  
UnofuNc0HM1}

This demo is built with Dynamsoft  
Barcode Reader SDK.  
[Get Free Trial >](#)

凯撒恢复得到flag。



## 问卷调查

签退题。填问卷得到flag。