




# GKCTF X DASCTF应急挑战杯Misc-Writeup

原创

末初  于 2021-07-01 20:23:37 发布  823  收藏 3

分类专栏: [CTF\\_MISC\\_Writeup](#)

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/118365556>

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

[签到](#)

[你知道apng吗](#)

[FireFox Forensics](#)

[excel 骚操作](#)

[0.03](#)

---

## Misc

[签到](#)

# 签到

## 200

师傅们玩的开心~ (flag由flag头包裹)

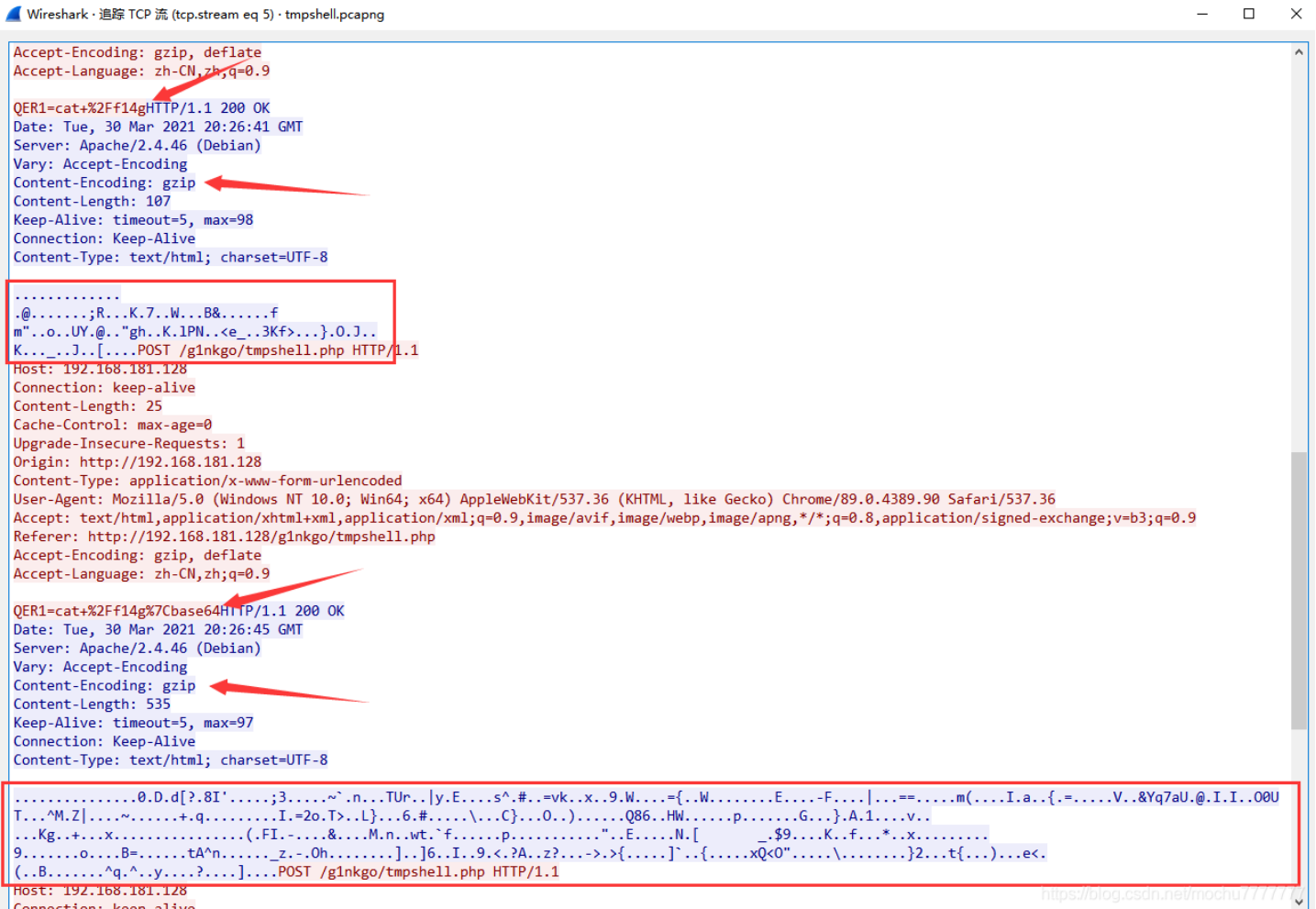
tmpshell.pc...

Flag

Submit

<https://blog.csdn.net/mochu7777777>

tcp.stream eq 5 发现 cat /f14g 操作



尝试直接 foremost 分离无果，只能切换为显示Hex数据，然后手动复制出Hex数据，转存为gzip

gzip的文件开头Hex为: 1f 8b



第一部分:

Q0NDQ0MhIQ==

解码后得到:

CCCCC!!

第二部分:

Y2MpKVvliKDpmaRdIFvliKDpmaRdIDAwbW1lZV9fR0dra0NDNDRGRl9fbW0xMXNzaWlDQ0NDQ0ND
MCAYMDowMT0xMw0KW+Wbnui9p10gW+Wbnui9p10gW+Wbnui9p10gZmZsbGFhZ2d7e319V1d1ZWxs
LS0tLS0tLS0tLS0NCueq1+WPoZoqbMv3IDUyIC0gTm90ZXBhZCsrDQrm17bp17Q6MjAyMS0wMy0z
MDE6MTMNC1vlm57ovaZdIA0KLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0t
LS0tLS0tDQrnqpf1j6M6Km51dyA1MiAtIE5vdGVvYWQrKw0K5pe26Ze00jIwMjEtMDMtMzAgMjA6
IyMjIyMjIyMjIyMNCi0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0t
MjEtMDMtMzAgMjA6MDE6MDggICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
DQoNCiMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIw0KIyAgICAgICAgIDlw==

解码后得到:

cc))[删除] [删除] 00mme\_ \_GGkkCC44FF\_\_mm11ssiCCCCCCCC 20:01:13
[回车] [回车] [回车] ff11aagg{{}}WWeell-----
窗口:\*new 52 - Notepad++
时间:2021-03-30 20:01:13
[回车]
-----
窗口:\*new 52 - Notepad++
时间:2021-03-30 20:01:08 #
#####
#####
# 20

第三部分:

Y2MpKVvliKDpmaRdIFvliKDpmaRdIDAwbW1lZV9fR0dra0NDNDRGRl9fbW0xMXNzaWlDQ0NDQ0ND
MCAYMDowMT0xMw0KW+Wbnui9p10gW+Wbnui9p10gW+Wbnui9p10gZmZsbGFhZ2d7e319V1d1ZWxs
LS0tLS0tLS0tLS0NCueq1+WPoZoqbMv3IDUyIC0gTm90ZXBhZCsrDQrm17bp17Q6MjAyMS0wMy0z
MDE6MTMNC1vlm57ovaZdIA0KLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0t
LS0tLS0tDQrnqpf1j6M6Km51dyA1MiAtIE5vdGVvYWQrKw0K5pe26Ze00jIwMjEtMDMtMzAgMjA6
IyMjIyMjIyMjIyMNCi0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0t
MjEtMDMtMzAgMjA6MDE6MDggICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
DQoNCiMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIw0KIyAgICAgICAgIDlw==

解码后得到:

cc))[删除] [删除] 00mme\_ \_GGkkCC44FF\_\_mm11ssiCCCCCCCC 20:01:13
[回车] [回车] [回车] ff11aagg{{}}WWeell-----
窗口:\*new 52 - Notepad++
时间:2021-03-30 20:01:13
[回车]
-----
窗口:\*new 52 - Notepad++
时间:2021-03-30 20:01:08 #
#####
#####
# 20

这里感觉有坑点, flag靠猜测

flag{We1c0me\_GkC4F\_m1siCCCCC!}

你知道png吗

# 你知道apng吗

## 200

(flag由flag头包裹)

 girl.apng


Flag

Submit

<https://blog.csdn.net/mochu7777777>

## APNG [编辑]

维基百科，自由的百科全书

 此条目需要扩展。 (2019年5月16日)  
请协助改善这篇条目，更进一步的信息可能会在讨论页或扩充请求中找到。请在扩展条目后将此模板移除。

**动态可移植网络图形**（英语：Animated Portable Network Graphics，缩写**APNG**）是一种继承自**便携式网络图形**（PNG）的文件格式，他允许像GIF格式一样播放动态图片，并且拥有GIF不支持的24位图像和8位透明性。它还保留了与非动画PNG文件的向后兼容性。

APNG文件的第一帧存储为普通PNG流，因此大多数标准PNG解码器都能够显示APNG文件的第一帧。帧速度数据和额外的动画帧存储在额外的数据块中（如原始的PNG规范所规定）。APNG的竞争对手是由PNG团队创建的位图动画的全面格式——多图像网络图形（MNG）。与其相比，APNG的优势是更小的存储大小以及对旧的PNG完全兼容。

通过对比GIF、APNG和WebP，可以看出APNG在质量相同的时候有着更小的体积<sup>[1]</sup>。

**目录** [隐藏]

- 历史
- 软件支持
- 参见
- 外部链接

## 历史 [编辑]

2004年，APNG由Mozilla公司的Stuart Parmenter和Vladimir Vukićević所创立，希望Mozilla社区将其用于**图形界面**及**XUL**，也期望广泛用于网页，但提案未能通过。

2006年，Google Summer of Code活动中，加拿大圣力嘉学院的学生为libpng程序库加入APNG支持。

此后开发者继续向Mozilla社区推荐APNG，但一直没有什么进展。

2007年3月23日，Mozilla Firefox 3.0在开发测试中支持APNG。<sup>[2]</sup>

2007年4月20日，PNG组织投票以10:8否决APNG进入官方标准。PNG组织决心继续推广MNG，不过其权力有限，许多常见软件继续支持了APNG。

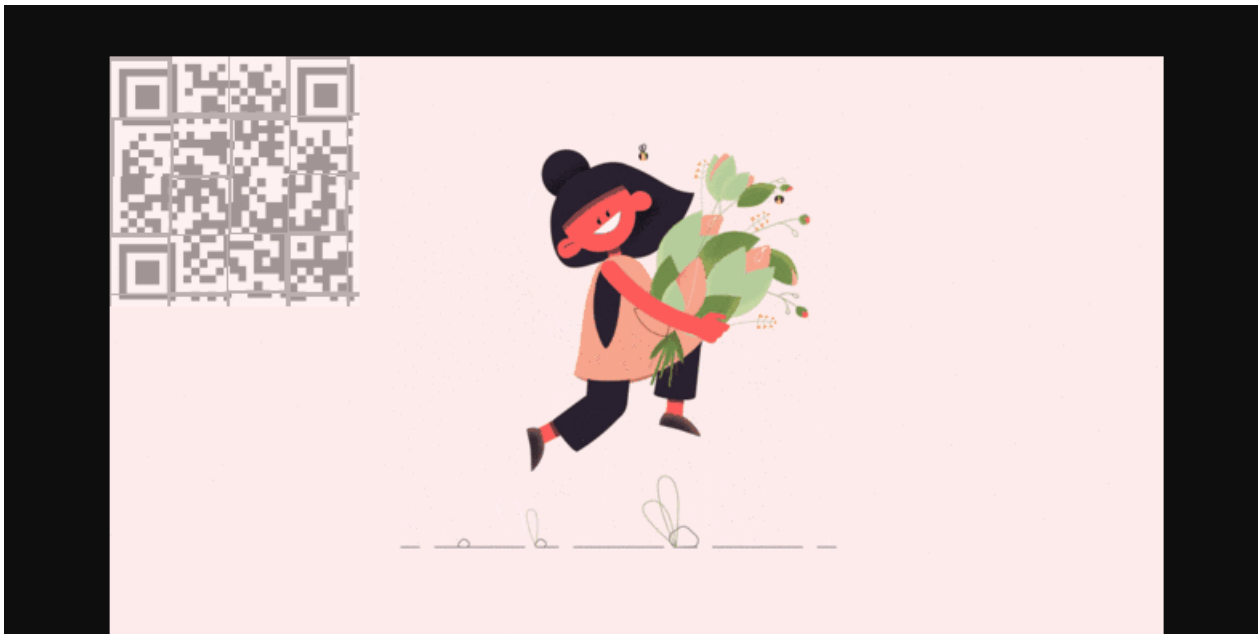
### 动态PNG

	
<b>扩展名</b>	.png、.apng
<b>初始版本</b>	2008年8月4日
<b>格式类型</b>	动画位图PNG
<b>延伸自</b>	PNG
<b>自由格式</b>	是



<https://blog.csdn.net/mochu7777777>

改为png只能显示第一帧，wiki上说Firefox支持apng，尝试直接拖入Firefox发现可以显示（我用Chrome也行）



我用 ScreenToGif 直接截成Gif，然后放入 Stegsolve 一帧一帧看



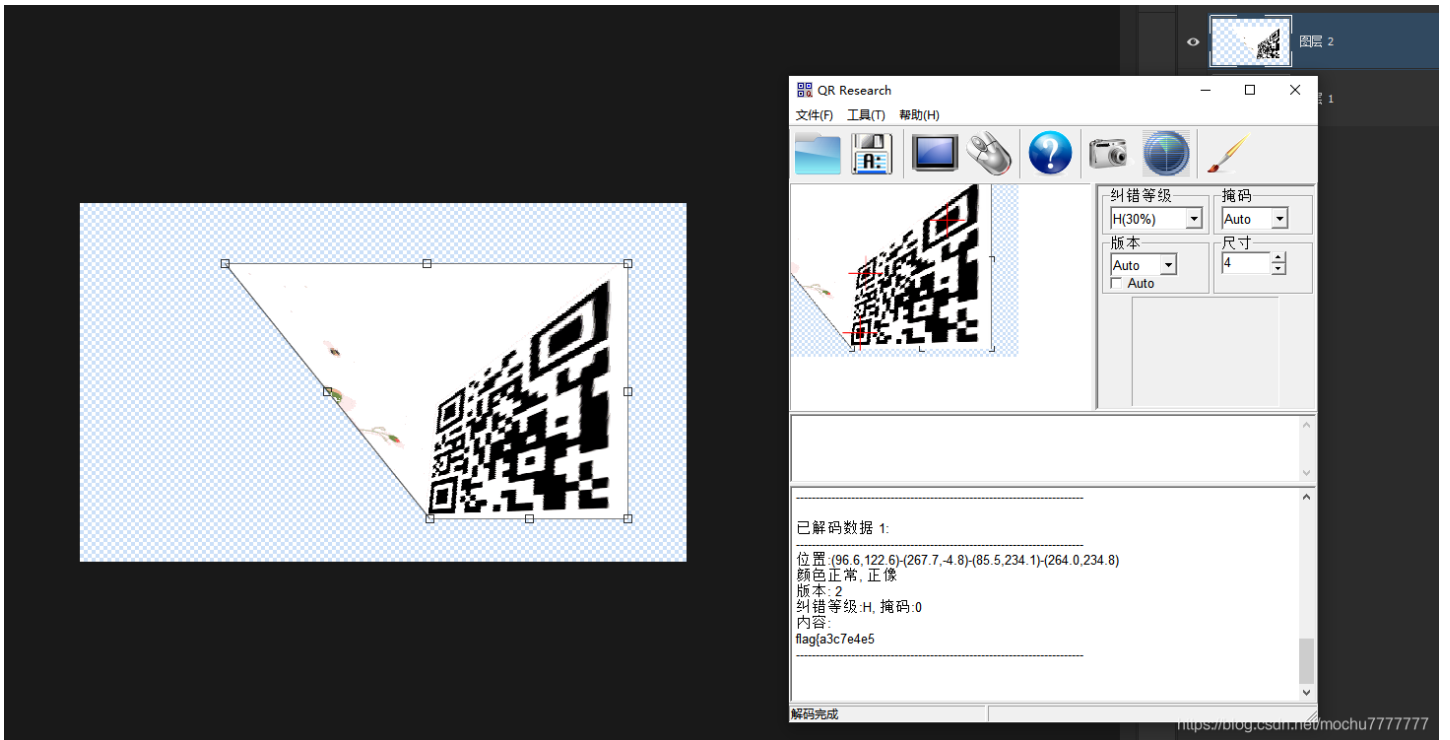
-0327-288a235370ea}



-ad20

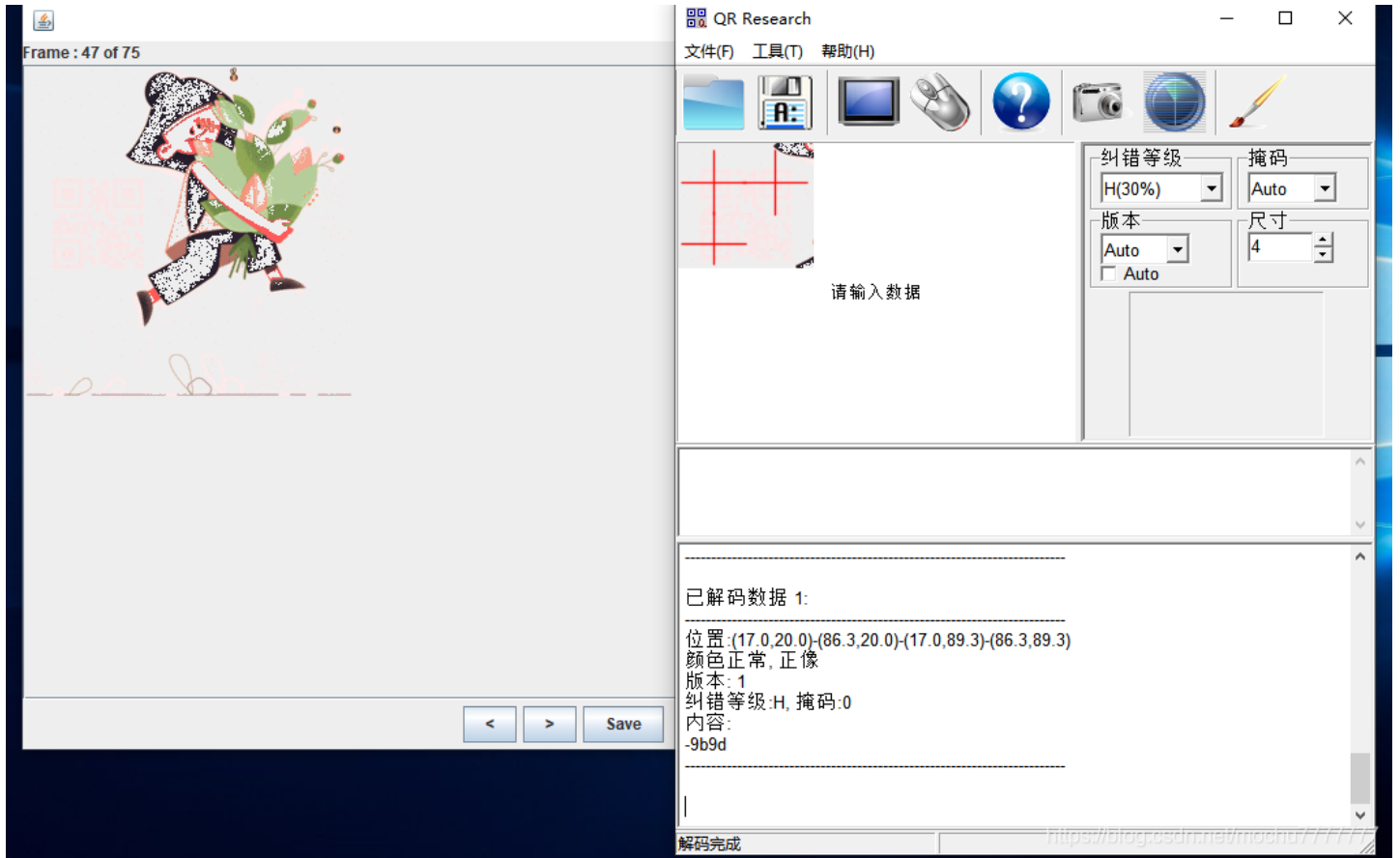


这张导出来，用 PS 打开，拉一下就行



flag{a3c7e4e5}

还有一张隐藏的比较深



-9b9d

最终flag为

flag{a3c7e4e5-9b9d-ad20-0327-288a235370ea}

另外也可以使用 [APNG Disassembler](#) 来分离出 apng 图片的每一帧

APNG Disassembler: <http://pngdis.sourceforge.net>

## FireFox Forensics

Challenge Top 3 Solves X

# FireFox Forensics

200

取证大佬说这是一份登录凭证文件

Firefox\_For...

Flag

Submit

<https://blog.csdn.net/mochu7777777>



从文件内容上看应该是 **Firefox** 的网页登录密码保存加密文件，给了key

此电脑 > 下载 > FireFox\_Forensics

名称	修改日期	类型	大小
key4.db	2021/5/8 18:39	Data Base File	288 KB
logins.json	2021/5/8 18:53	JSON Source File	1 KB

Google找一下有没有工具

The screenshot shows a Google search result for "Decrypto Mozilla Password Github". The search bar contains the text "Decrypto Mozilla Password Github". Below the search bar, there are navigation options: "All", "Videos", "Images", "News", "Maps", and "More". The search results show "About 1,76,000 results (0.52 seconds)". The first result is titled "Including results for **Decrypt** Mozilla Password Github" and includes a snippet: "About. **Firefox Decrypt** is a tool to extract **passwords** from profiles of **Mozilla** (Fire/Water)fox™, **Thunderbird**®, SeaMonkey® and derivates. It can be used to recover **passwords** from a profile protected by a Master **Password** as long as the latter is known." Below this is a link to "unode/firefox\_decrypt: Firefox Decrypt is a tool to ... - GitHub". A second result is highlighted with a red box and titled "firepwd.py, an open source tool to decrypt Mozilla ... - GitHub", with a snippet: "18-Apr-2020 — This educational tool was written to illustrate how **Mozilla passwords** (**Firefox**, **Thunderbird**) are protected using contents of files key4.db (or ...". A third result is titled "firefox-decrypt · GitHub Topics · GitHub" and includes a snippet: "05-Sep-2020 — **Firefox Decrypt** is a tool to extract **passwords** from **Mozilla** (**Firefox**™, **Waterfox**™, **Thunderbird**®, **SeaMonkey**®) profiles. python **firefox** ...". A fourth result is titled "firefox\_decrypt/firefox\_decrypt.py at master · unode ... - GitHub" and includes a snippet: "**Firefox Decrypt** is a tool to extract **passwords** from **Mozilla** (**Firefox**™, **Waterfox**™, **Thunderbird**®, **SeaMonkey**®) profiles - unode/firefox\_decrypt." At the bottom right of the search results, there is a URL: "https://blog.csdn.net/mochu7777777".

<https://github.com/lclevy/firepwd>

```

PS D:\Tools\Misc\firepwd-master> python .\firepwd.py -d C:\Users\Administrator\Downloads\FireFox_Forensics
globalSalt: b'1e26e84b2f01da28d865e7258f9003d16b9c43f2'
SEQUENCE {
  SEQUENCE {
    OBJECTIDENTIFIER 1.2.840.113549.1.5.13 pkcs5 pbes2
    SEQUENCE {
      SEQUENCE {
        OBJECTIDENTIFIER 1.2.840.113549.1.5.12 pkcs5 PBKDF2
        SEQUENCE {
          OCTETSTRING b'66a735e17767b37d83d464126b36d4269243f9e0c99405ccd68f442798f83129'
          INTEGER b'01'
          INTEGER b'20'
          SEQUENCE {
            OBJECTIDENTIFIER 1.2.840.113549.2.9 hmacWithSHA256
          }
        }
      }
    }
  }
  SEQUENCE {
    OBJECTIDENTIFIER 2.16.840.1.101.3.4.1.42 aes256-CBC
    OCTETSTRING b'24eb241594de7ab37ec379d9ba06'
  }
}
OCTETSTRING b'946322a2b2978db6601e449e1bdf7c4d'
}
clearText b'70617373776f72642d636865636b0202'
password check? True
SEQUENCE {
  SEQUENCE {
    OBJECTIDENTIFIER 1.2.840.113549.1.5.13 pkcs5 pbes2
    SEQUENCE {
      SEQUENCE {
        OBJECTIDENTIFIER 1.2.840.113549.1.5.12 pkcs5 PBKDF2
        SEQUENCE {
          OCTETSTRING b'56722302469f529a29dc73f28d6af3ed0ee483cceff05772e96e2313336816fd'
          INTEGER b'01'
          INTEGER b'20'
          SEQUENCE {
            OBJECTIDENTIFIER 1.2.840.113549.2.9 hmacWithSHA256
          }
        }
      }
    }
  }
  SEQUENCE {
    OBJECTIDENTIFIER 2.16.840.1.101.3.4.1.42 aes256-CBC
    OCTETSTRING b'ef6a4df3e5fd7608c97df9e22092'
  }
}
OCTETSTRING b'51b24cd6a2672c312255d7f2dddeb67336fd56973b4302bb2eacf2270c251d41'
}
clearText b'673dec57458fb95bd50bdc9198541038970e5b3d518973a408080808080808'
decrypting login/password pairs
https://ctf.g1nkg0.com:b'admin',b'GKCTF{9cf21dda-34be-4f6c-a629-9c4647981ad7}'
PS D:\Tools\Misc\firepwd-master>

```

```
GKCTF{9cf21dda-34be-4f6c-a629-9c4647981ad7}
```

excel 骚操作







在线的汉信码站用不了了：<http://www.efittech.com/hxdec.html>

但是在网上看到有一个叫 **中国物品编码中心** 的APP可以扫描识别

### 中国物品编码中心研发的“汉信码”手机识读软件上线啦！

发布时间：2013-10-16 | 信息来源：中国自动识别网 | 文章作者： | 点击数：3083

中国物品编码中心研发的“汉信码”手机识读软件上线啦！

目前支持以下功能：

- 1.快速的汉信码识读，包括多种信息格式（文本、网址、名片等）；
- 2.扫描二维码名片添加到本地通讯录；
- 3.扫描汉信码上网服务；
- 4.扫描结果通过邮箱和好友一起分享；
- 5.扫描历史的保存。

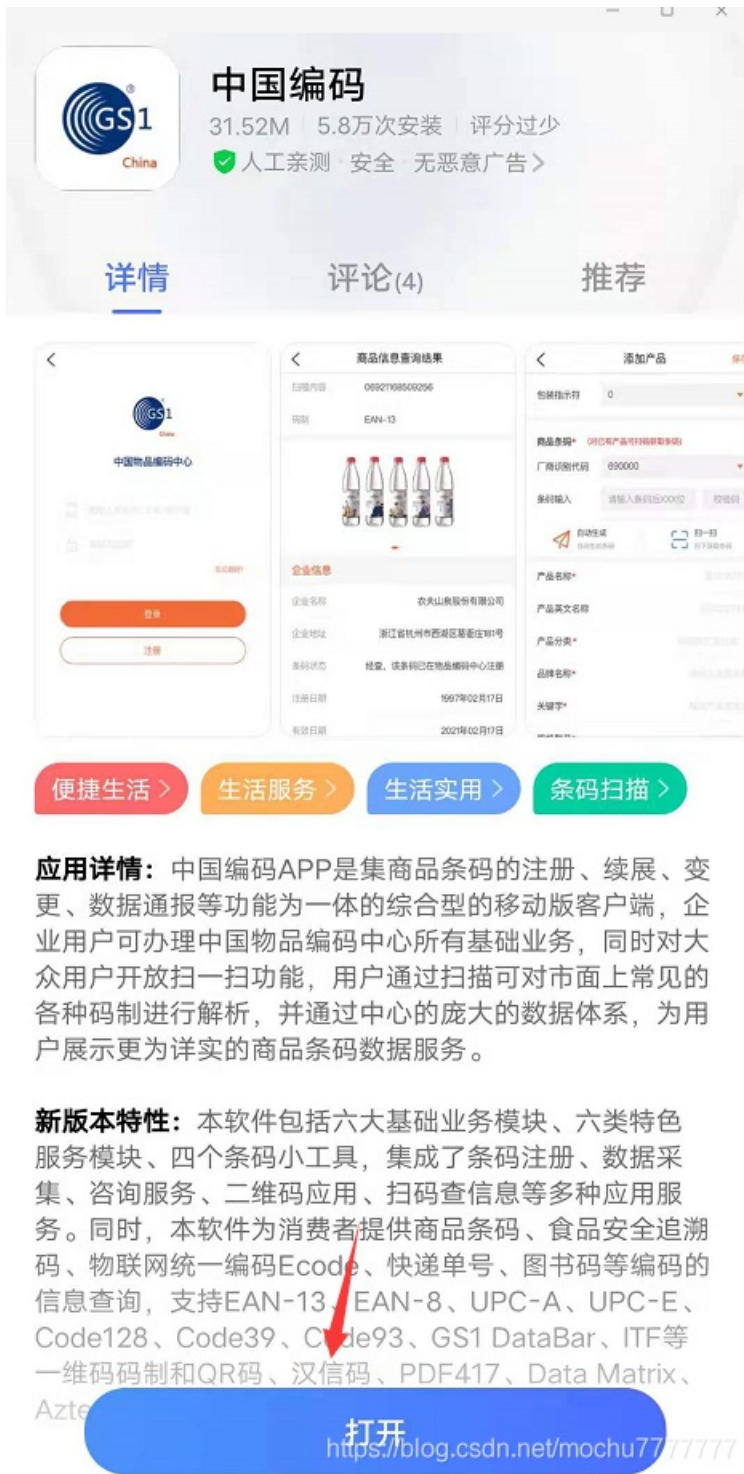
“汉信码”手机识读软件分为iOS版和Android版，分别适用于苹果公司iPhone4、4S、5等系列手机（以及iPad系列和iPod Touch 4、iPod Touch 5）以及三星、HTC等公司的Android系列手机。

iPhone安装：对于iPhone手机，请各位登录苹果商店（APP Store），搜索“汉信二维码”（注意是汉信二维码，不是汉信码），在搜索结果排名第一的就是该软件，或者用苹果设备访问以下网址：<https://itunes.apple.com/us/app/han-xin-er-wei-ma/id665768613?mt=8>

点击下载即可下载安装。

三星、HTC等Android系统手机安装：

对于三星、HTC等手机用户，请各位访问安智市场（[http://www.anzhi.com/soft\\_969237.html#](http://www.anzhi.com/soft_969237.html#)，这个链接可以下载），或者安卓市场（<http://apk.hiapk.com/html/2013/07/1662908.html?module=256&info=SWzhTwf4>，这个链接可以下载）；或在安智、安卓市场搜索“汉信码”，排名第一的就是该软件，用手机访问时，点击下载即可下载安装，用电脑等设备访问时，可以下载到电脑上，用豌豆荚、91助手等手机软件工具帮助安装，也可以用腾讯手机管家一键安装。



**应用详情:** 中国编码APP是集商品条码的注册、续展、变更、数据通报等功能为一体的综合型的移动版客户端，企业用户可办理中国物品编码中心所有基础业务，同时对大众用户开放扫一扫功能，用户通过扫描可对市面上常见的各种码制进行解析，并通过中心的庞大的数据体系，为用户展示更为详实的商品条码数据服务。

**新版本特性:** 本软件包括六大基础业务模块、六类特色服务模块、四个条码小工具，集成了条码注册、数据采集、咨询服务、二维码应用、扫码查信息等多种应用服务。同时，本软件为消费者提供商品条码、食品安全追溯码、物联网统一编码Ecode、快递单号、图书码等编码的信息查询，支持EAN-13、EAN-8、UPC-A、UPC-E、Code128、Code39、Code93、GS1 DataBar、ITF等一维码码制和QR码、汉信码、PDF417、Data Matrix、Aztec

打开 <https://blog.csdn.net/mochu7777777>



汉信码是由中国物品编码中心研制开发，是我国第一个制定了国家标准的自主知识产权的二维码，具

有知识产权免费、汉字编码能力强、抗污损、抗畸变、信息容量大等特点。2007年8月23日，国家标准化管理委员会发布了GB/T 21049《汉信码》国家标准。和其他二维码相比，汉信码更适合汉字信息的表示，其支持GB 18030中规定的160万个汉字信息字符，具有高度的汉字表达能力和汉字压缩效率；具有很强的纠错能力、抗污损和畸变能力，支持加密技术。

<https://blog.csdn.net/mochu7777777>

flag{9ee0cb62-f443-4a72-e9a3-43c0b910757e}

### 0.03

Challenge Top 3 Solves ×

0.03  
975

我的真心值三分吗



链接: [https://pan.baidu.com/s/1OXIYfEr0s\\_zd\\_ZXdz48XKg](https://pan.baidu.com/s/1OXIYfEr0s_zd_ZXdz48XKg) 密码: bian

<https://gkctf20201-1251267611.file.myqcloud.com/0.03.rar>

View Hint

Flag

<https://blog.csdn.net/mochu7777777>

 flag_in_the_disk.zip	2021/6/11 9:58	ZIP 压缩文件	358,400 KB
 secret.txt	2021/6/22 10:20	TXT 文件	1 KB

C:\Users\Administrator\Downloads\0.03\secret.txt - Sublime Text (UNREGISTERED)

File Edit Selection Find View Goto Tools Project Preferences Help

```
secret.txt  x  whatyoumaywant.txt  x
1 do you believe that you get?
2
3 311223313313112122312312313311
4
```

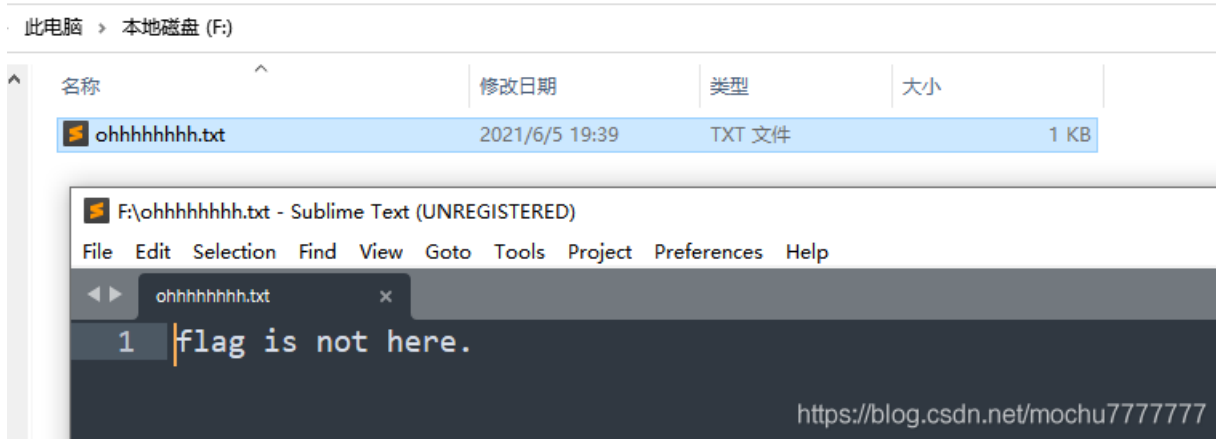
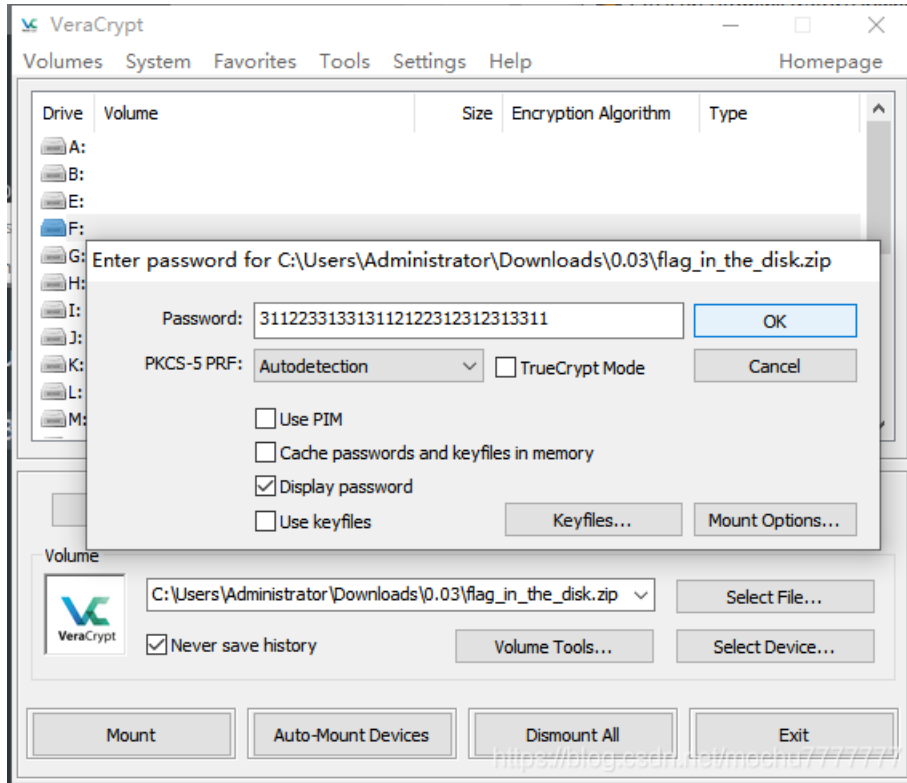
<https://blog.csdn.net/mochu7777777>



flag\_in\_the\_disk.zip 并非 zip 文件，也没识别出来是什么

```
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/0.03# ls
flag_in_the_disk.zip secret.txt
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/0.03# file flag_in_the_disk.zip
flag_in_the_disk.zip: data
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/0.03#
```

但是看大小猜测可能为 **虚拟系统文件**，可能需要挂载，经过多次尝试发现当密码为：**311223313313112122312312313311** 时 VeraCrypt 可以挂载。



VeraCrypt 对于同一个文件可以用不同密码挂载，得到不同内容。需要找到真的密码，secret.txt 中的信息都试了不行，当看到 0.03.rar 是RAR的压缩包时猜测可能存在 **NTFS文件流隐写**。

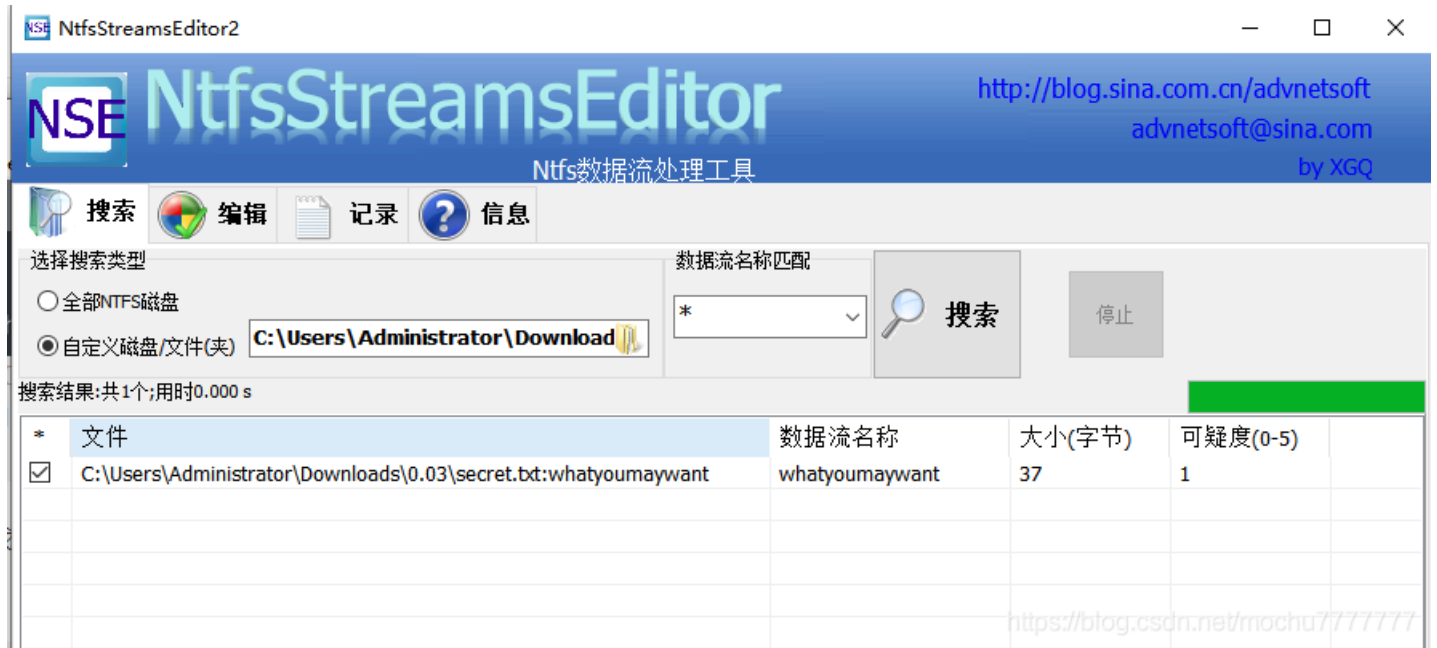




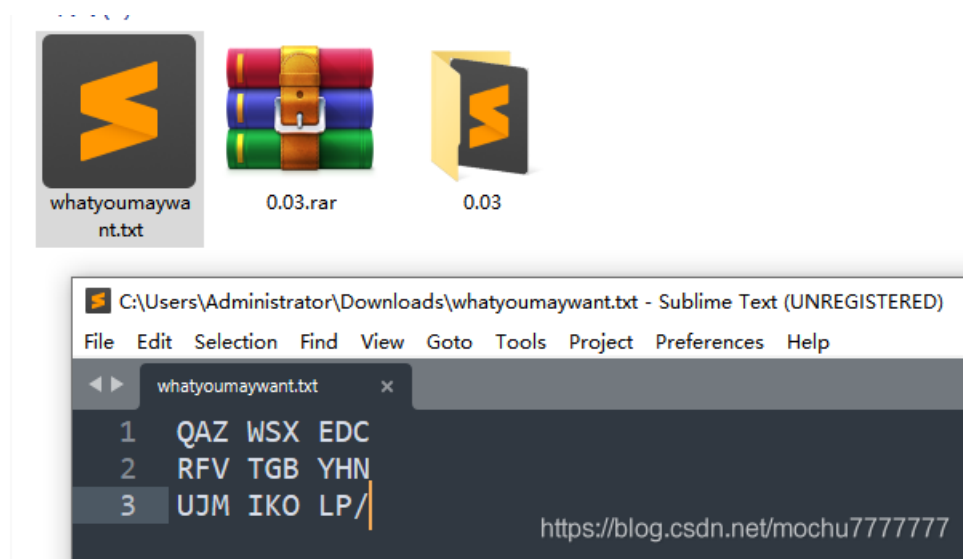
0.03.rar

0.03

扫描一下发现确实存在NTFS文件流隐写



<https://blog.csdn.net/mochu777777>



<https://blog.csdn.net/mochu777777>

```

0 1 2 3 (x)

1 QAZ WSX EDC

2 RFV TGB YHN

3 UJM IKO LP/

(y)

```

看着有点像 敲击码，联合 secret.txt 中的那串数字确实类似敲击码中的坐标，但是如果只有 x,y，那只能定位到三个一组的字符串，经过尝试发现这样得到字符串并不是正确的密码。所以怀疑是 x,y,z 三位一组的坐标，一组坐标定位一个字符串。最后一位数字定位 x,y 坐标得到的三个字符串中的前后顺序。密码的真实坐标如下：

311 223 313 313 112 122 312 312 313 311  
E B C C A F D D C E

得到密码: EBCCAFDDCE

此电脑 > 本地磁盘 (F:)

名称	修改日期	类型	大小
flag.txt	2021/6/11 9:35	TXT 文件	1 KB

F:\flag.txt - Sublime Text (UNREGISTERED)

File Edit Selection Find View Goto Tools Project Preferences Help

flag.txt

1 flag{85ec0e23-ebbe-4fa7-9c8c-e8b743d0d85c}  
<https://blog.csdn.net/mochu777777>

flag{85ec0e23-ebbe-4fa7-9c8c-e8b743d0d85c}