2021“春秋杯“新年欢乐赛wp（部分）

原创

时间大幻剧 于 2021-02-01 01:52:54 发布 2126 收藏 1

分类专栏： CTF 文章标签： 信息安全

本文链接：https://blog.csdn.net/qq_43349910/article/details/113488795

文章目录

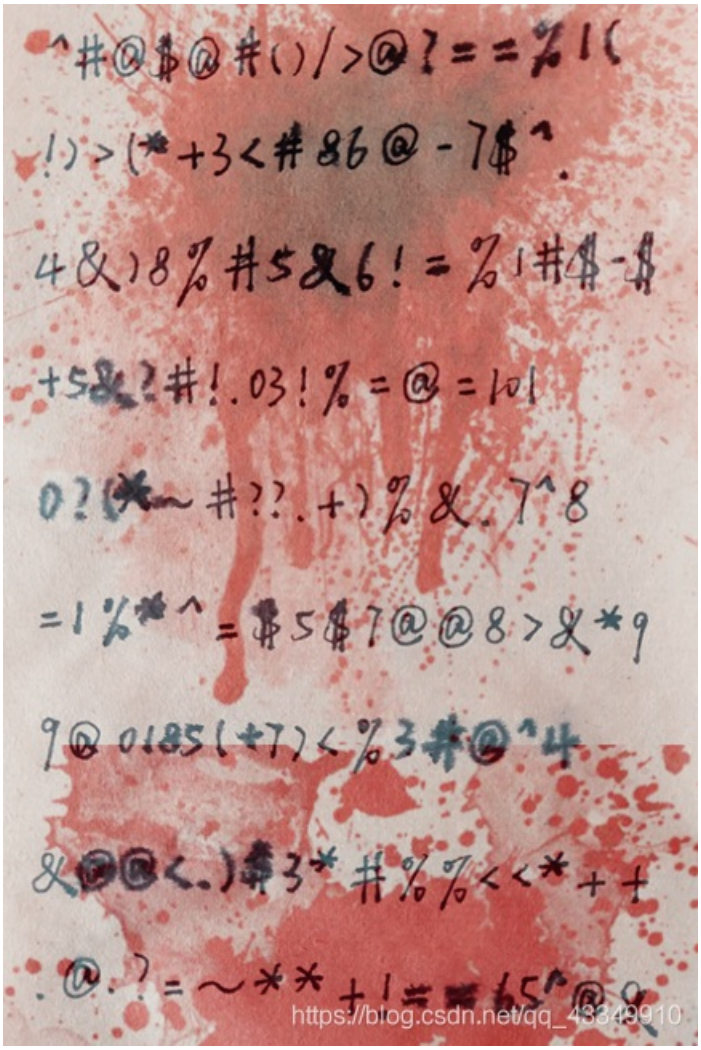
1 签到

操作内容：

手写一个FUN放在摄像头前，即可出flag

5 十二宫的挑衅

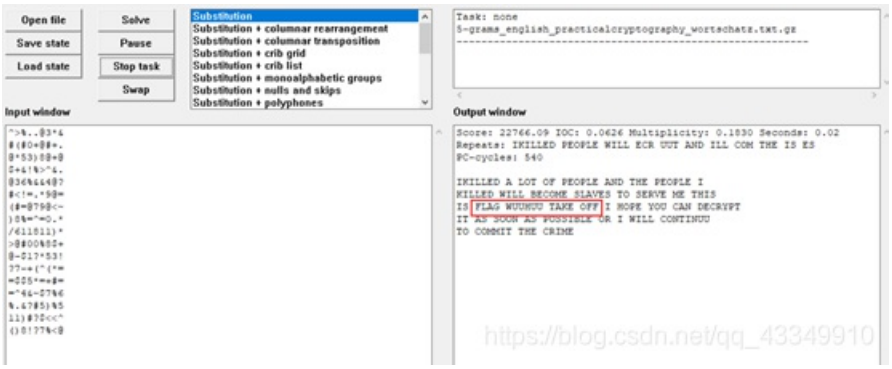
操作内容：
首先拿到一张图片，查找了一下十二宫的资料，看看是否相关，下载了AZ，并且按照真实的十二宫的解密方法解密。



将图片中的密文延对角线重组

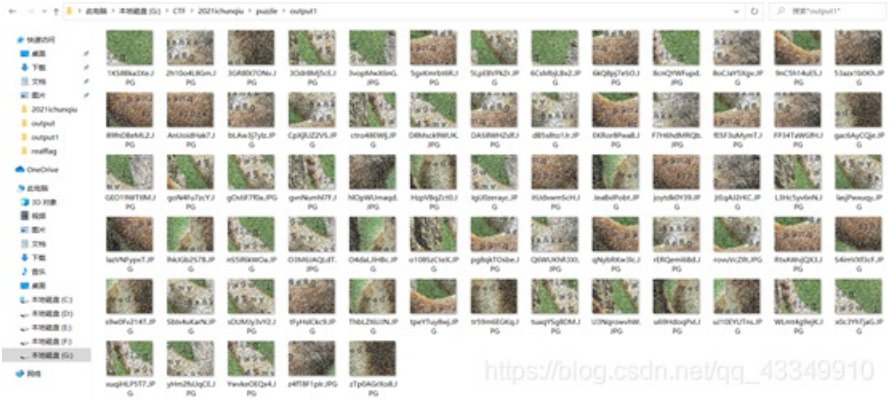
```
^>%..@3*&
#(#0+@#+.
@*53)8@+@
$+&!%>^&.
@36%&&4@?
#<!=.*9@=
(#=@79@<~
)8%=^=0.*
/611811)*
>@#00%8$+
@-$1?*53!
?7-+(^(*=
=$$5*=+#=
=^4&~$7%6
%.&?#5)%5
11)#?$<<^
()8!?7%<@
```

将重组后的密文放入AZ解密立刻得到flag



6 puzzle

操作内容：
这题看了图片碎片只有1000多张，而且查看了几个图片很快就发现了图片碎片里面flag的踪迹于是开始筛选。



由于c142在黑处，第一遍找的时候没找到，就拿了个三血。

7 2019-nCoV

操作内容：
首先下载下来一个COV和hint压缩包，COV里面的是一个wav和mp3音频，还有一个内容加密的压缩包，hint里面是base32加密的。
解码后得到三个网站和一句话，三个网站和一句话是用来解mp3隐写的密码。

NB2HI4B2F4XXO53XFZWWK4TSPFRGS3ZOMNXW2LTDNYXWE3DPM4XVGQKSKM'

http://www.merrybio.com.cn/blog/SARS-CoV-2-genomic-analysis.html
https://www.ncbi.nlm.nih.gov/orffinder/
http://www.merrybio.com.cn/blog/coronavirus-introduction.html

Please notice The largest structural protein
the password is the md5(it's gene sequence) and do not let the '\n' in md5()

请注意最大的结构蛋白

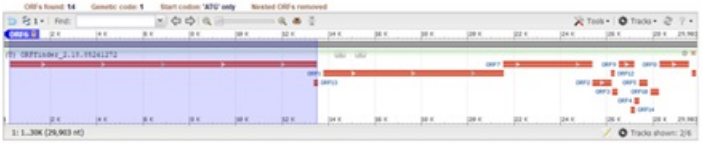
密码是md5（它的基因序列），不要在md5（）中使用'\n')

由第三个网站知S为最大的结构蛋白

- 刺突蛋白（Spike Protein，S）是病毒最大的结构蛋白，一般包含一些膜融合功能元件、受体结合区以及主要抗原结合位点，在识别/结合宿主细胞表面受体，以及介导病毒包膜与细胞膜融合的过程中起关键性作用。

再通过第一个网站找到病毒代号和对应序列号，用第二个网站搜索对应的基因序列。

利用NCBI上的ORF finder工具对该病毒 MN908947 进行基因组注释分析。



新型冠状病毒为线性单链RNA（ssRNA）病毒，全基因组序列全长29903 bp，共包含14个主要的开放阅读框（Open Reading Frame，ORF）。
其中：

- 1-265个核苷酸为5' UTR区域；
- 266-13483为“ORF1a”基因，13768-21555为“ORF1b”基因；ORF1a与ORF1b是两个大的重叠ORF（ORF1ab）；
- ORF1ab和ORF1b基因分别编码两个多聚蛋白pp1ab和pp1a，多聚蛋白pp1ab和pp1a经剪切，可产生15种nsps，即nsp1-nsp10，nsp12-nsp16。
- 21536-25384为“S”基因，可编码产生结构蛋白：病毒表面糖蛋白S；

使用python idle进行md5加密

```
>>> import hashlib
>>> md5 = hashlib.md5()
>>> md5.update()
Traceback (most recent call last):
  File "<pyshell#2>", line 1, in <module>
    md5.update()
TypeError: update() takes exactly one argument (0 given)
>>> md5.update('MFLLTTKRTMFVFLVLLPLVSSQCVNLTTRTQLPPAYTNSFTRGVYYPDKVFRSSVLHSTQDLF
LPFFSNVTWFHAIHVSGTNGTKRFDNPVLPFNDGVYFASTEKSNIIRGWIFGTTLDSKTQSLLIVNNATNVVIKVCEFQF
CNDPFLGVYYHKNNKSWMESEFRVYSSANNCTFEYVSQPFLMDLEGKQGNFKNLREFVFKNIDGYFKIYSKHTPINLVRD
LPQGFSALEPLVDLPIGINITRFQTLLALHRSYLTPGDSSSGWTAGAAAYYVGYLQPRTFLLKYNENGTITDAVDCALDP
LSETKCTLKSFTVEKGIYQTSNFRVQPTESIVRFPNITNLCPFGEVFNATRFASVYAWNRKRISNCVADYSVLYNSASFS
TFKCYGVSPTKLNDLCFTNVYADSFVIRGDEVRQIAPGQTGKIADYNYKLPDDFTGCVIAWNSNNLDSKVGGNYNYLYRL
FRKSNLKPFERDISTEIYQAGSTPCNGVEGFNCYFPLQSYGFQPTNGVGYQPYRVVVLSFELLHAPATVCGPKKSTNLVK
NKCVNFNFNGLTGTGVLTESNKKFLPFQQFGRDIADTTDAVRDPQTLEILDITPCSFGGVSVITPGTNTSNQVAVLYQDV
NCTEVPVAIHADQLTPTWRVYSTGSNVFQTRAGCLIGAEHVNNSYECDIPIGAGICASYQTQTNSPRRARSVASQSIIAY
TMSLGAENSVAYSNNSIAIPTNFTISVTTEILPVSMTKTSVDCTMYICGDSTECSNLLLQYGSFCTQLNRALTGIAVEQD
KNTQEVFAQVKQIYKTPPIKDFGGFNFSQILPDPSKPSKRSFIEDLLFNKVTLADAGFIKQYGDCLGDIAARDLICAQKF
NGLTVLPPLLTDEMIAQYTSALLAGTITSGWTFGAGAALQIPFAMQMAYRFNGIGVTQNVLYENQKLIANQFNSAIGKIQ
DSLSSTASALGKLQDVVNQNAQALNTLVKQLSSNFGAISSVLNDILSRLDKVEAEVQIDRLITGRLQSLQTYVTQQLIRA
AEIRASANLAATKMSECVLGQSKRVDFCGKGYHLMSFPQSAPHGVVFLHVTYVPAQEKNFTTAPAICHDGKAHFPREGVF
VSNGTHWFVTQRNFYEPQIITTDNTFVSGNCDVVIGIVNNTVYDPLQPELDSFKEELDKYFKNHTSPDVDLGDISGINAS
VVNIQKEIDRLNEVAKNLNESLIDLQELGKYEQYIKWPWYIWLGFIAGLIAIVMVTIMLCCMTSCCSCLKGCCSCGSCCK
FDEDDSEPVLKGVKLHYT'.encode('utf-8'))
>>> md5.hexdigest()
'98eb1b1760bcc837934c8695a1cee923'
>>>
```


再用mp3 stego进行解密

```
G:\CTFtools\MP3Stego_1_1_19\MP3Stego_1_1_19\MP3Stego>Decode.exe -X -P 98eb1b1760bcc837934c8695a1cee923 cov.mp3
MP3StegoEncoder 1.1.19
See README file for copyright info
Input file = 'cov.mp3'  output file = 'cov.mp3.pcm'
Will attempt to extract hidden information. Output: cov.mp3.txt
the bit stream file cov.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=3, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=single-ch, sblim=32, jsbd=32, ch=1
[Frame  791]Avg slots/frame = 417.434; b/smp = 2.90; br = 127.839 kbps
Decoding of "cov.mp3" is finished
The decoded PCM output file name is "cov.mp3.pcm"
```

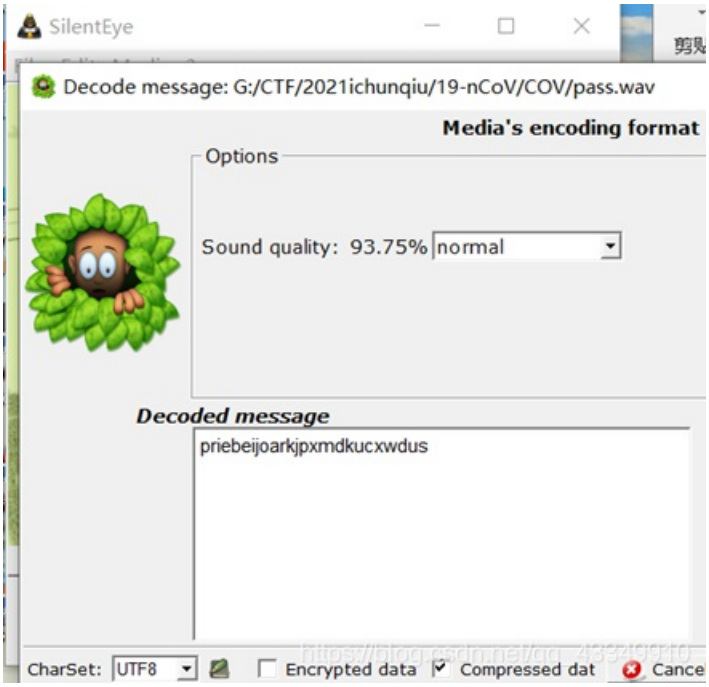
得到压缩包的密码。

cov.mp3.txt - 记事本

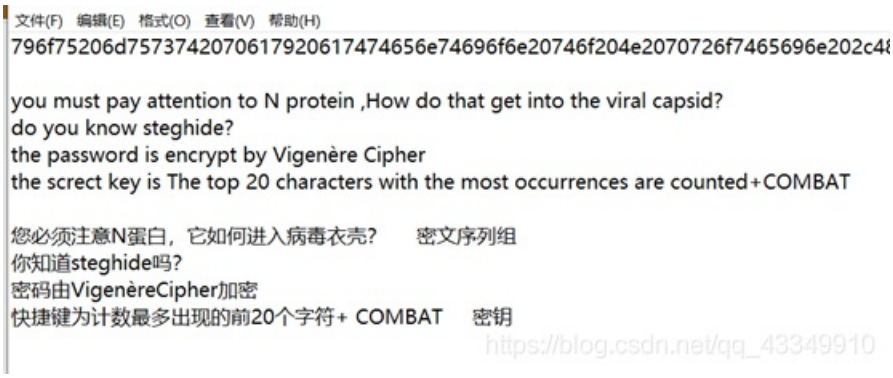
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

2019-nCoV

SilentEye解出一些东西。



用之前的密码解密压缩包，得到一个Hint2和jpg，hint2十六进制转字符串得到



由Hint2知道jpg是steghide隐写，他的密码由维吉尼亚密码加密，密钥就是第一句话的NME蛋白序列计数由高到低排的二十位字符+COMBAT。
用网上找的脚本跑出来，由于有几位是相同的，所以要换位置尝试，最后得到密钥是LGASTRIQKNDPFEVYMWHCCOMBAT。

```
-*- coding:utf-8 -*-
# Author: MoChu7
alphabet = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890!@#$%^&*()\_+-/={}[]    "#所有正常打印字符
# strings = open('./text.txt').read()#读取需要统计频数的文本
strings =   "MSDNGPQNQRNAPRITFGGPSDSTGSNQNGERSGARSKQRRPQGLPNNTASWFTALTQHGKEDLKFPRGQGVPINTNSSPDDQIGYYRRATRRIRGGDG
KMKDLSPRWYFYYLGTGPEAGLPYGANKDGIIWVATEGALNTPKDHIGTRNPANNAAIVLQLPQGTTLPKGFYAEGSRGGSQASSRSSSRSRNSSRNSTPGSSRGTSPARMA
GNGGDAALALLLLDRLNQLESKMSGKGQQQQGQTVTKKSAAEASKKPRQKRTATKAYNVTQAFGRRGPEQTQGNFGDQELIRQGTDYKHWPQIAQFAPSASAFFGMSRIGME
VTPSGTWLTYTGAIKLDDKDPNFKDQVILLNKHIDAYKTFPPTEPKKDKKKKADETQALPQRQKKQQTVTLLPAADLDDFSKQLQQSMSSADSTQAMADSNGTITVEELKKL
LEQWNLVIGFLFLTWICLLQFAYANRNRFLYIIKLIFLWLLWPVTLACFVLAAVYRINWITGGIAIAMACLVGLMWLSYFIASFRLFARTRSMWSFNPETNILLNVPLHGTI
LTRPLLESELVIGAVILRGHLRIAGHHLGRCDIKDLPKEITVATSRTLSYYKLGASQRVAGDSGFAAYSRYRIGNYKLNTDHSSSSDNIALLVQMFHLVDFQVTIAEILLII
MRTFKVSIWNLDYIINLIIKNLSKSLTENKYSQLDEEQPMEID"
# strings =   "MFHLVDFQVTIAEILLIIMRTFKVSIWNLDYIINLIIKNLSKSLTENKYSQLDEEQPMEID"

result = {}
for i in alphabet:
    counts =   strings.count(i)
    i =   '{0}'.format(i)
    result[i] = counts

res = sorted(result.items(), key=lambda item: item[1],   reverse=True)
num = 0
for data in res:
    num += 1
    print('频数第{0}: {1}'.format(num, data))

print('\n---------------以下是频数从多到少的字符，按照从前到后排序---------------')
for i in res:
    flag =   str(i[0])
      print(flag[0], end="")
```

维吉尼亚解密得到eliminatenovelcoronavirts，steghide解密得到flag

```
root@kali:~/Desktop# steghide extract -sf CoV-1.jpg
Enter passphrase:
wrote extracted data to "flag.txt".
root@kali:~/Desktop#
```