2021年春秋杯网络安全联赛秋季赛 勇者山峰 misc部分wp

原创

@Demo 于 2021-11-28 00:41:12 发布 445 收藏 1

分类专栏： 笔记

本文链接：https://blog.csdn.net/qq_47886905/article/details/121584147

版权

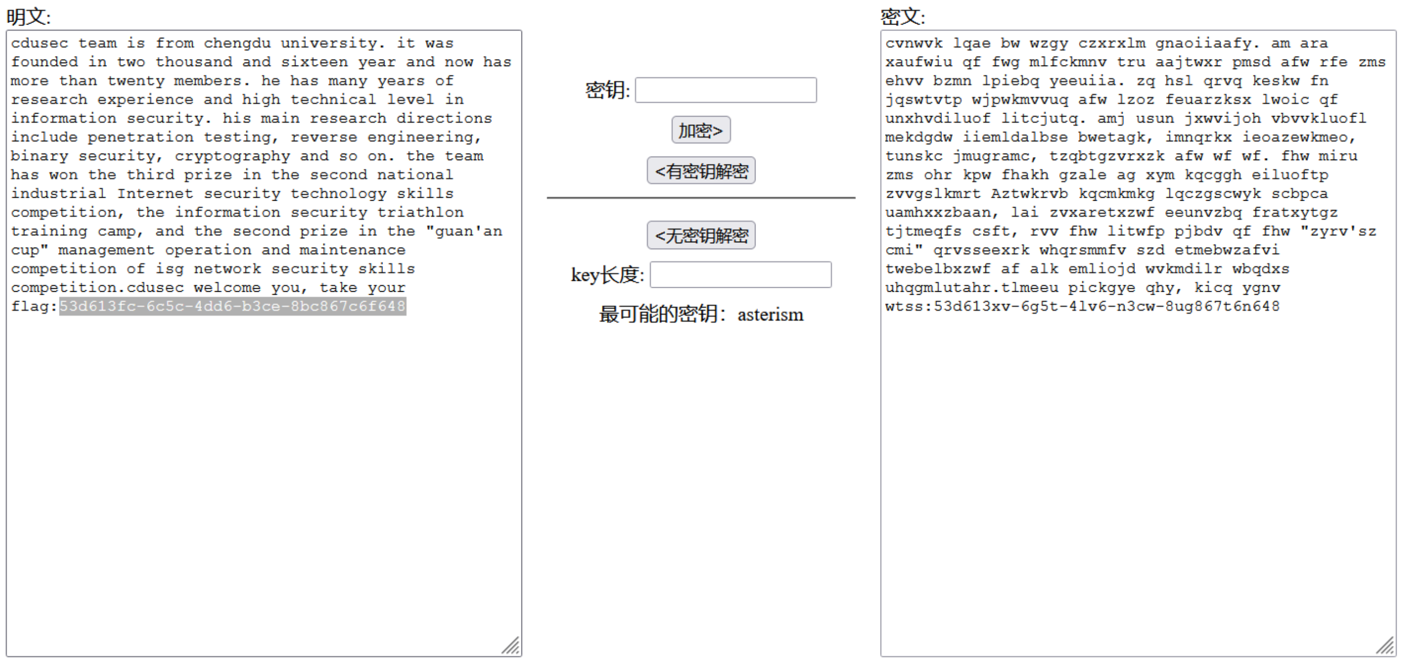
笔记 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

Crypto

https://atomcated.github.io/Vigenere/ 无秘钥解密即可



```
cdusec team is from chengdu university. it was
founded in two thousand and sixteen year and now has
more than twenty members. he has 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
```

最可能的密钥：asterism

```
cvnwvk lqae bw wzgy czxrxlm gnaoiiaafy. am ara
xaufwiu qf fwg mlfckmnv tru aajtwxr pmsd afw rfe zms
ehvv bzmn lpiebq yeeuiia. zq hsl qrvq keskw fn
jqswtvtp wjpwkmvvuq afw lzoz feuarzksx lwoic qf
unxhvdiluof litcjutq. amj usun jxwvijoh vbvvkluofl
mekdgdw iiemldalbse bwetagk, imnqrkx ieoazewkmeo,
tunskc jmugramc, tzqbtgzvrxzk afw wf wf. fhw miru
zms ohr kpw fhakh gzale ag xym kqcggh eiluoftp
zvvgslkmrt Aztwkrvb kqcmkmkg lqczgscwyk scbpca
uamhxxzbaan, lai zvxaretxzwf eeunvzbq fratxytgz
tjtmeqfs csft, rvv fhw litwfp pjbdv qf fhw "zyrv'sz
cmi" qrvsseexrk whqrsmmfv szd etmebwzafvi
twebelbxzwf af alk emliojd wvkmdilr wbqdxs
uhqgmlutahr.tlmeeu pickgye qhy, kicq ygnv
wtss:53d613xv-6g5t-4lv6-n3cw-8ug867t6n648
```

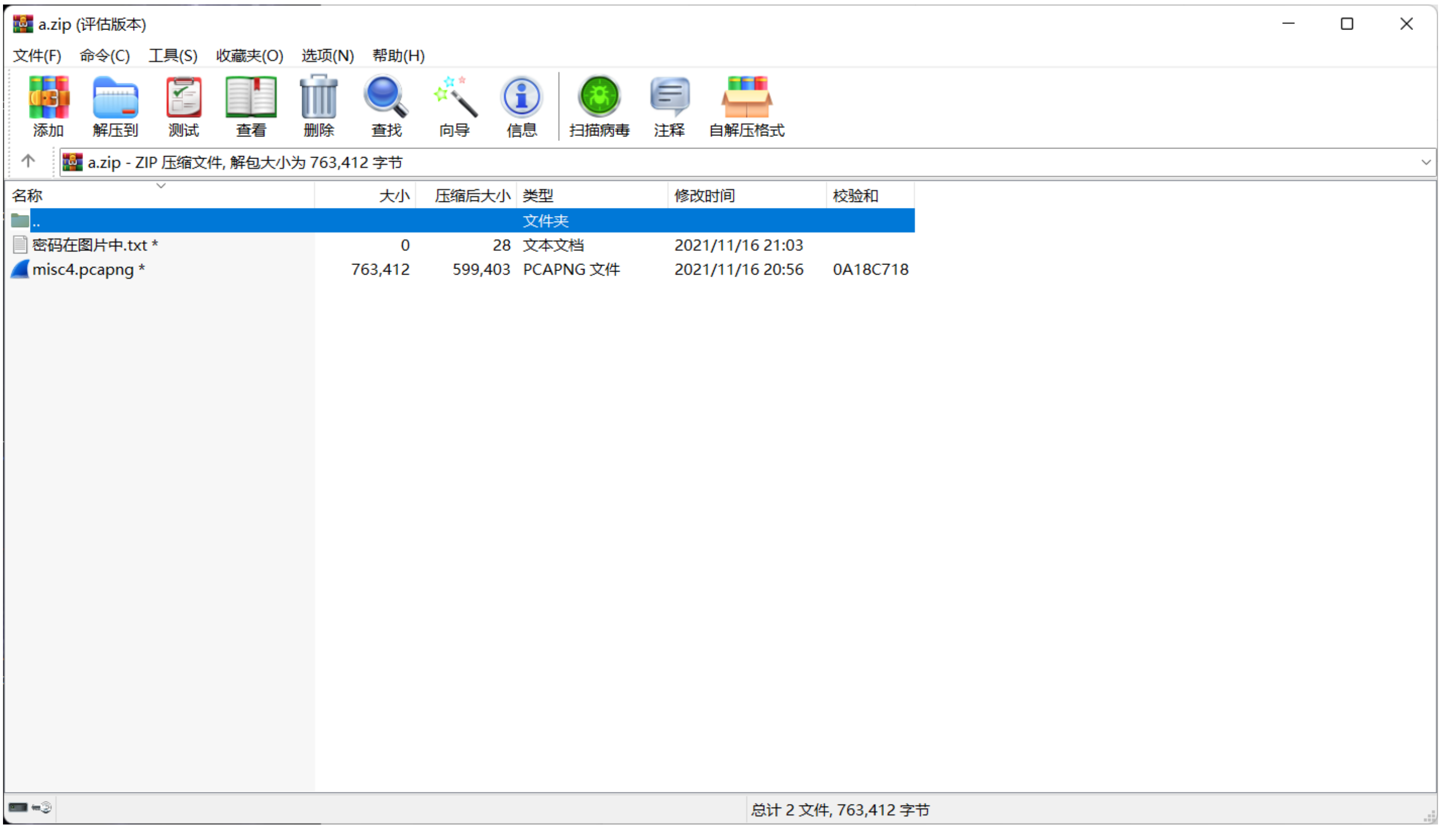
MISC

问卷

```
flag{让我们一起带给世界安全感}
```

helloshark

bmp图片尾藏了一个压缩包，存在一个密码在图片中.txt

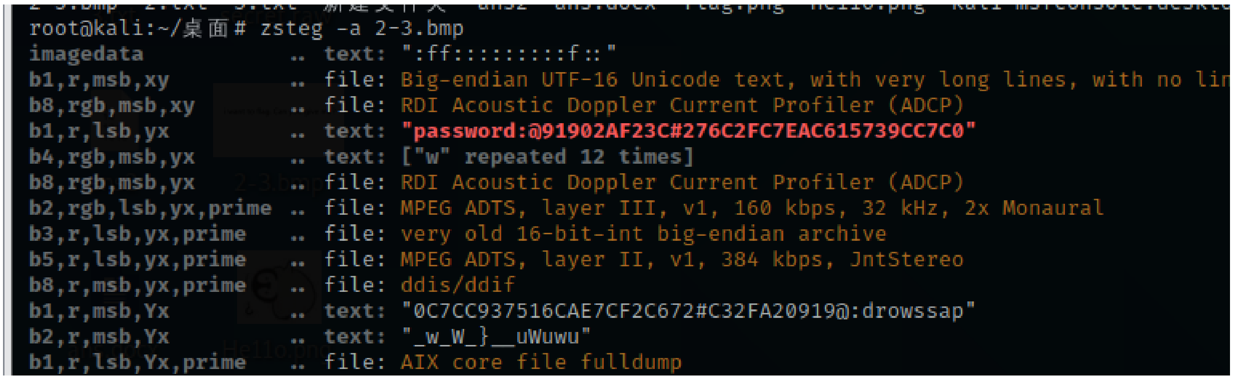


a.zip - ZIP 压缩文件, 解包大小为 763,412 字节

名称	大小	压缩后大小	类型	修改时间	校验和
..			文件夹		
密码在图片中.txt *	0	28	文本文档	2021/11/16 21:03	
misc4.pcapng *	763,412	599,403	PCAPNG 文件	2021/11/16 20:56	0A18C718

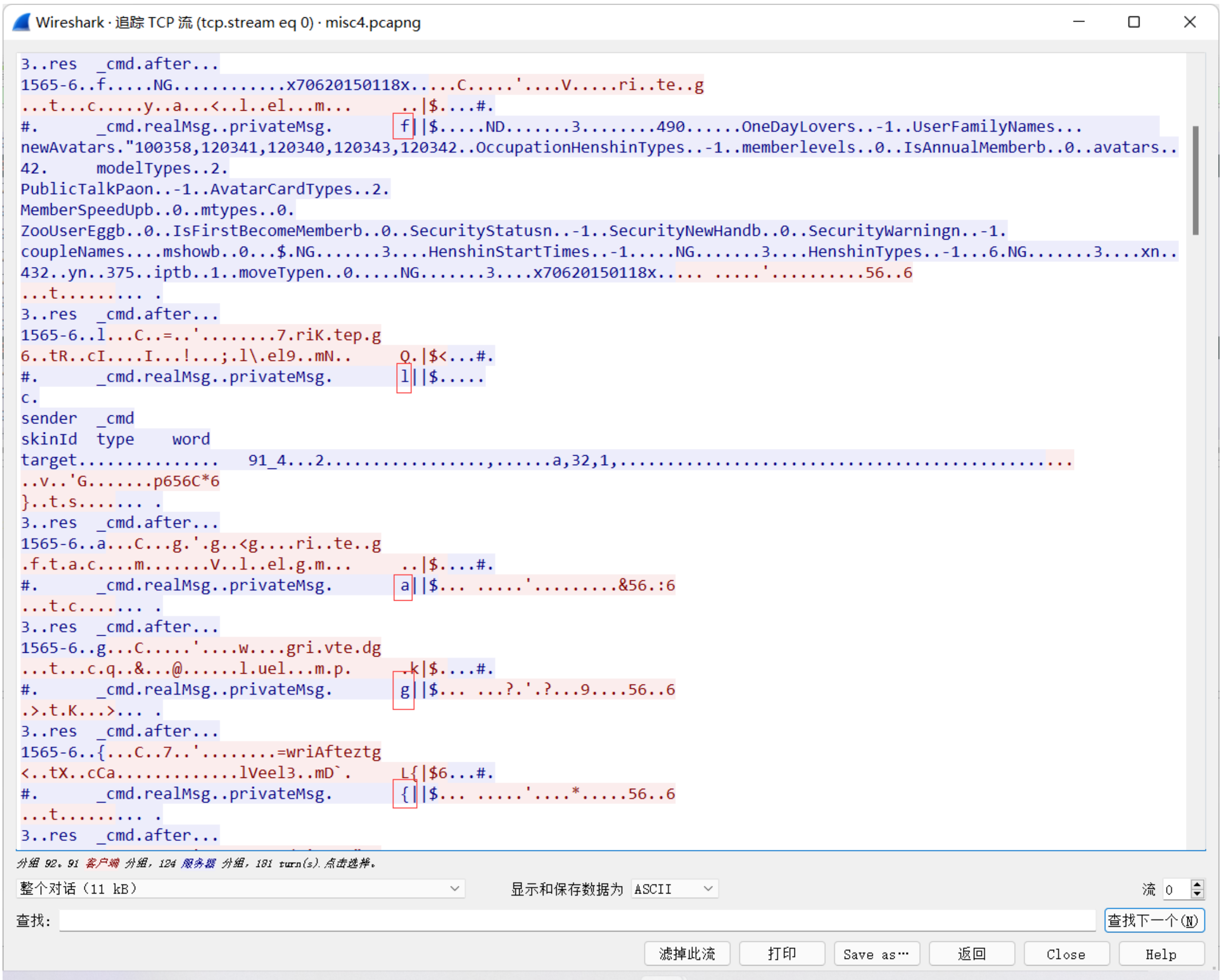
总计 2 文件, 763,412 字节

```
zsteg -a  2-3.bmp
```



```
root@kali:~/桌面# zsteg -a 2-3.bmp
imagedata           .. text: ":ff:::::::::f::"
b1,r,msb,xy         .. file: Big-endian UTF-16 Unicode text, with very long lines, with no lin
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 Monaural
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
```

解密得到pcapng追踪tcp流发现flag（蓝色||$前的字符）



```
3..res  _cmd.after...
1565-6..f.....NG............x70620150118x.....C.....'....V.....ri..te..g
...t...c.....y..a...<..l..el...m...      ..|$....#.
#.      _cmd.realMsg..privateMsg.       f||$.....ND.......3........490......OneDayLovers..-1..UserFamilyNames...
newAvatars."100358,120341,120340,120343,120342..OccupationHenshinTypes..-1..memberlevels..0..IsAnnualMemberb..0..avatars..
42.     modelTypes..2.
PublicTalkPaon..-1..AvatarCardTypes..2.
MemberSpeedUpb..0..mtypes..0.
ZooUserEggb..0..IsFirstBecomeMemberb..0..SecurityStatusn..-1..SecurityNewHandb..0..SecurityWarningn..-1.
coupleNames....mshowb..0...$.NG.......3....HenshinStartTimes..-1.....NG.......3....HenshinTypes..-1...6.NG.......3....xn..
432..yn..375..iptb..1..moveTypen..0.....NG.......3....x70620150118x..... .....'..........56..6
...t......... .
3..res  _cmd.after...
1565-6..l...C..=..'........7.riK.tep.g
6..tR..cI....I...!...;.l\.el9..mN..      Q.|$<...#.
#.      _cmd.realMsg..privateMsg.       l||$.....
c.
sender  _cmd
skinId  type    word
target...............   91_4...2................,......a,32,1,.............................................
..v..'G.......p656C*6
}..t.s....... .
3..res  _cmd.after...
1565-6..a...C...g.'.g..<g....ri..te..g
.f.t.a.c....m.......V..l..el.g.m...      ..|$....#.
#.      _cmd.realMsg..privateMsg.       a||$... .....'.........&56.:6
...t.c....... .
3..res  _cmd.after...
1565-6..g...C.....'....w....gri.vte.dg
...t...c.q..&...@......l.uel...m.p.      .k|$....#.
#.      _cmd.realMsg..privateMsg.       g||$... ...?.'.?...9....56..6
.>.t.K...>... .
3..res  _cmd.after...
1565-6..{...C..7..'........=wriAfteztg
<..tX..cCa.............lVeel3..mD`.      L{|$6...#.
#.      _cmd.realMsg..privateMsg.       {||$... .....'....*.....56..6
...t......... .
3..res  _cmd.after...
```

分组 92。91 客户端 分组，124 服务器 分组，181 turn(s).点击选择。

整个对话（11 kB）

显示和保存数据为 ASCII

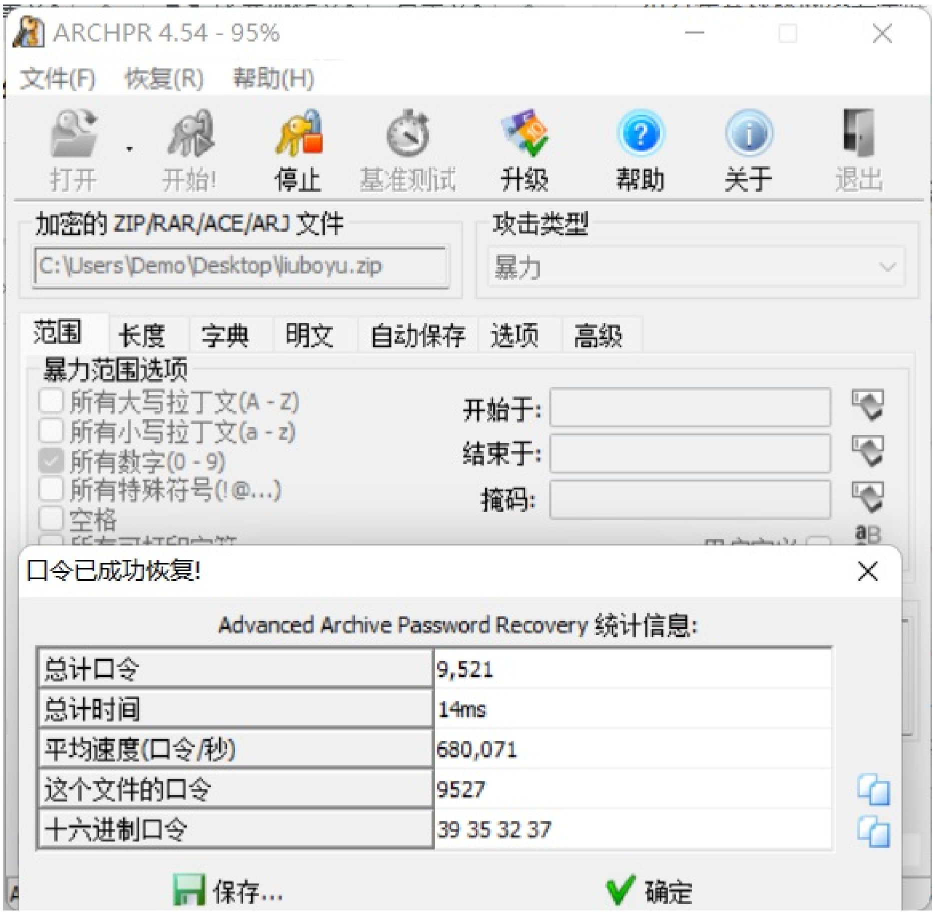
流 0

查找：

```
flag{a4e0a418-fced-4b2d-9d76-fdc9053d69a1}
```

secret_chart

png藏了一个压缩包，但是加密，爆破



加密的 ZIP/RAR/ACE/ARJ 文件: C:\Users\Demo\Desktop\liuboyu.zip

攻击类型: 暴力

暴力范围选项

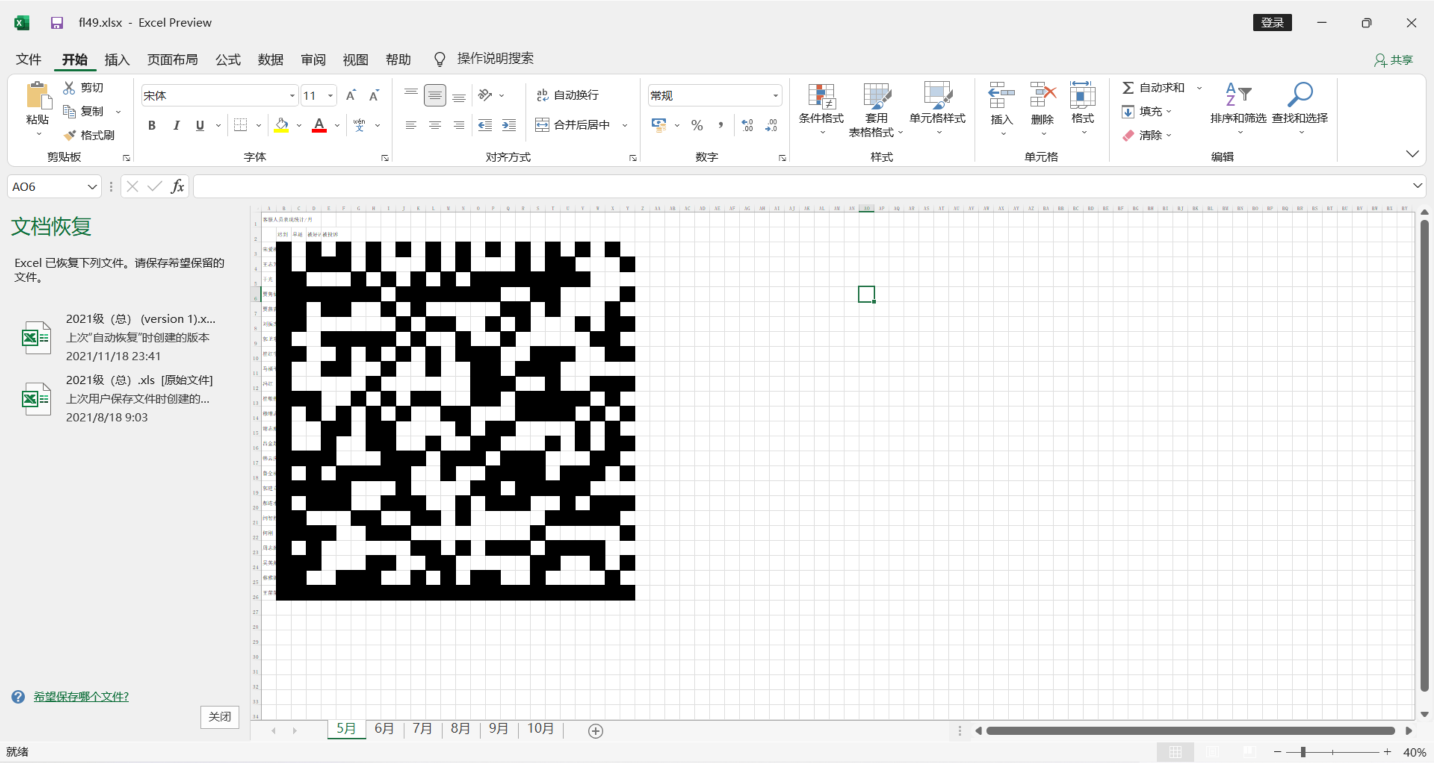
□ 所有大写拉丁文(A - Z)
□ 所有小写拉丁文(a - z)
☑ 所有数字(0 - 9)
□ 所有特殊符号(!@...)
□ 空格

口令已成功恢复!

Advanced Archive Password Recovery 统计信息:

总计口令	9,521
总计时间	14ms
平均速度(口令/秒)	680,071
这个文件的口令	9527
十六进制口令	39 35 32 37

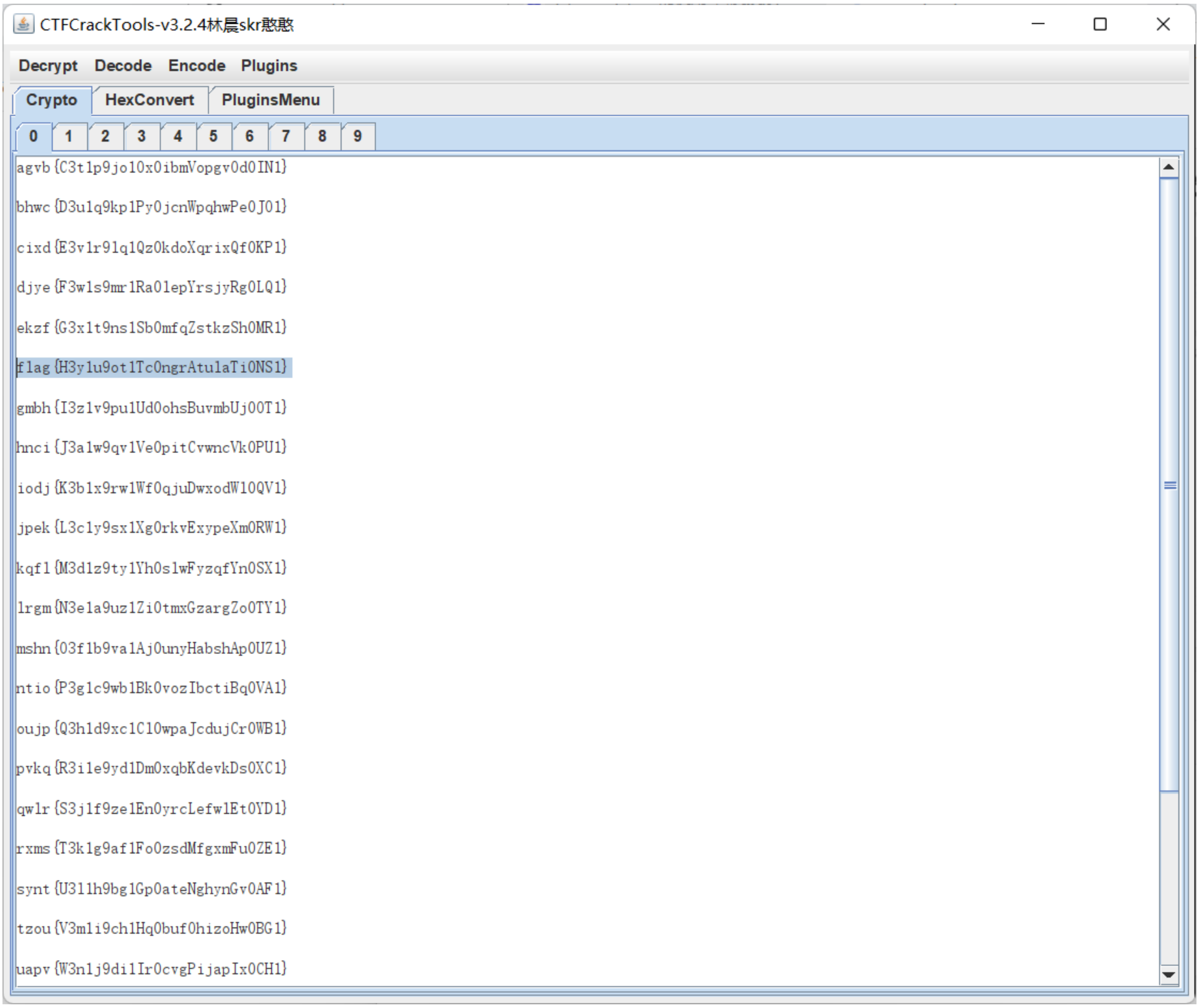
解密得到excel一共6个月，每一个月里有4列数据，合起来是24列，每个月都是24行联想到24-24二维码，恢复一下



DataMatrix二维码，http://boy.co.ua/decode.php
扫码得到

```
zfua{B3s1o9in1Nw0halUnofuNc0HM1}
```

凯撒一下


CTFCrackTools-v3.2.4林晨skr憨憨
Decrypt Decode Encode Plugins
Crypto HexConvert PluginsMenu
0 1 2 3 4 5 6 7 8 9

```
agvb{C3t1p9jo10x0ibmVopgv0d0IN1}

bhwc{D3u1q9kp1Py0jcnWpqhwPe0J01}

cixd{E3v1r91q1Qz0kdoXqrixQf0KP1}

djye{F3w1s9mr1Ra0lepYrsjyRg0LQ1}

ekzf{G3x1t9ns1Sb0mfqZstkzSh0MR1}

flag{H3y1u9ot1Tc0ngrAtulaTi0NS1}

gmbh{I3z1v9pu1Ud0ohsBuvmbUj00T1}

hnci{J3a1w9qv1Ve0pitCvwncVk0PU1}

iodj{K3b1x9rw1Wf0qjuDwxodW10QV1}

jpek{L3c1y9sx1Xg0rkvExypeXm0RW1}

kqf1{M3d1z9ty1Yh0s1wFyzqfYn0SX1}

1rgm{N3e1a9uz1Zi0tmxGzargZo0TY1}

mshn{03f1b9va1Aj0unyHabshAp0UZ1}

ntio{P3g1c9wb1Bk0vozIbctiBq0VA1}

oujp{Q3h1d9xc1C10wpaJcdujCr0WB1}

pvkq{R3i1e9yd1Dm0xqbKdevkDs0XC1}

qwlr{S3j1f9ze1En0yrcLefwlEt0YD1}

rxms{T3k1g9af1Fo0zsdMfgxmFu0ZE1}

synt{U311h9bg1Gp0ateNghynGv0AF1}

tzou{V3m1i9ch1Hq0buf0hizoHw0BG1}

uapv{W3n1j9di1Ir0cvgPijapIx0CH1}
```

```
flag{H3y1u9ot1Tc0ngrAtulaTi0NS1}
```