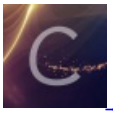
2021春秋杯网络安全联赛—秋季赛 勇者山峰wp（部分)

原创

依然脚踩众神 于 2021-11-30 10:43:23 发布 3729 收藏
分类专栏： 网络安全 CTF 文章标签： web安全 安全


网络安全 同时被 2 个专栏收录
1 篇文章 0 订阅
订阅专栏


CTF
1 篇文章 0 订阅
订阅专栏

汪汪队立大功 战队WRITEUP

- 战队信息

战队名称：汪汪队立大功

战队排名：11

- 解题情况

请粘贴战队排名截图和答题情况截图：

示例的操作流程：

“详细数据”→“解题总榜”→“找到您所在队伍”→“截图”

（提交的时候请把下图替换为您队伍解题总榜上的排名截图）

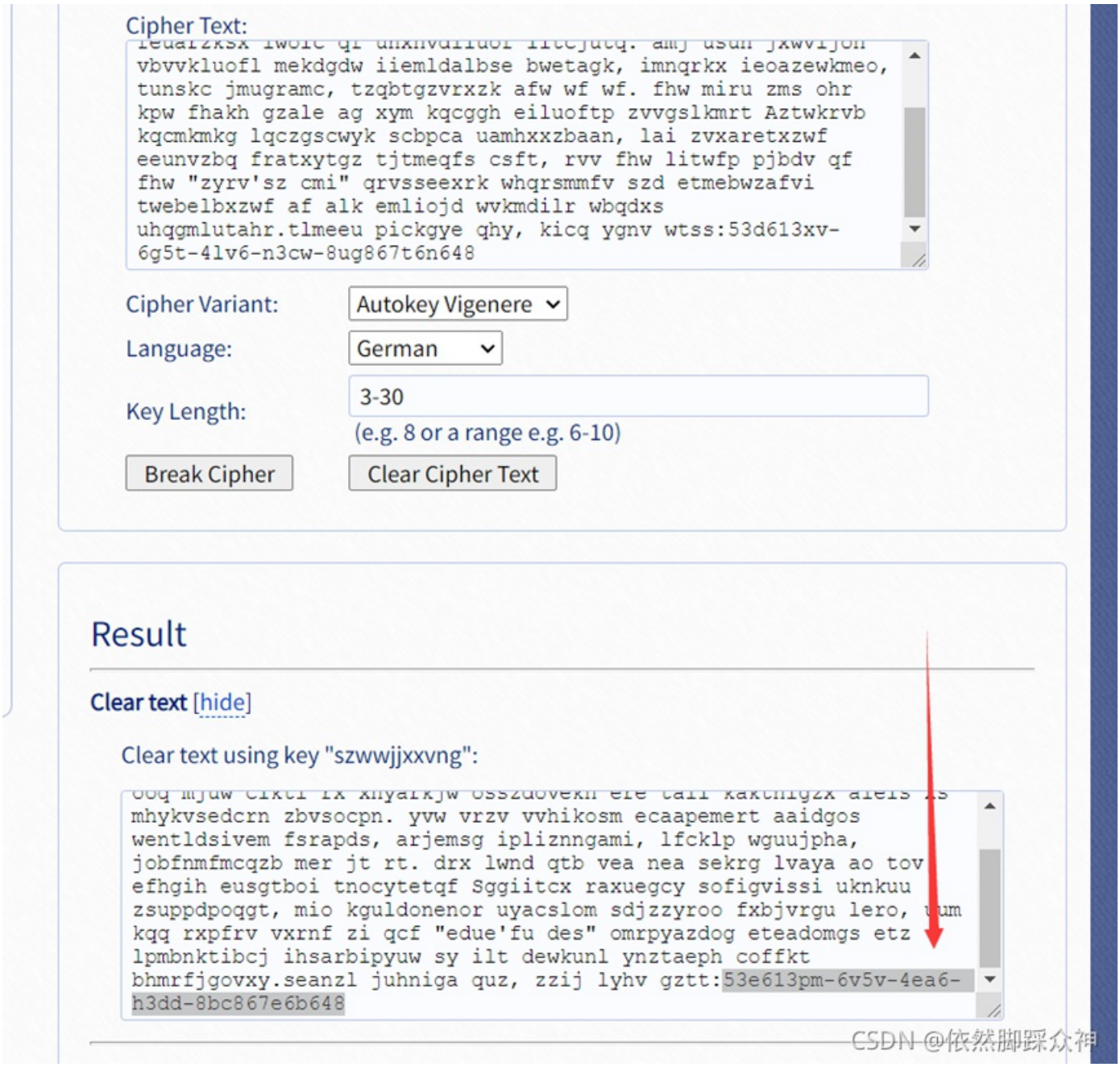
- 解题过程

1 Vigenere

（题目序号 请参考解题总榜上面的序号）

操作内容：

维吉尼亚解密网站https://www.guballa.de/vigenere-solver

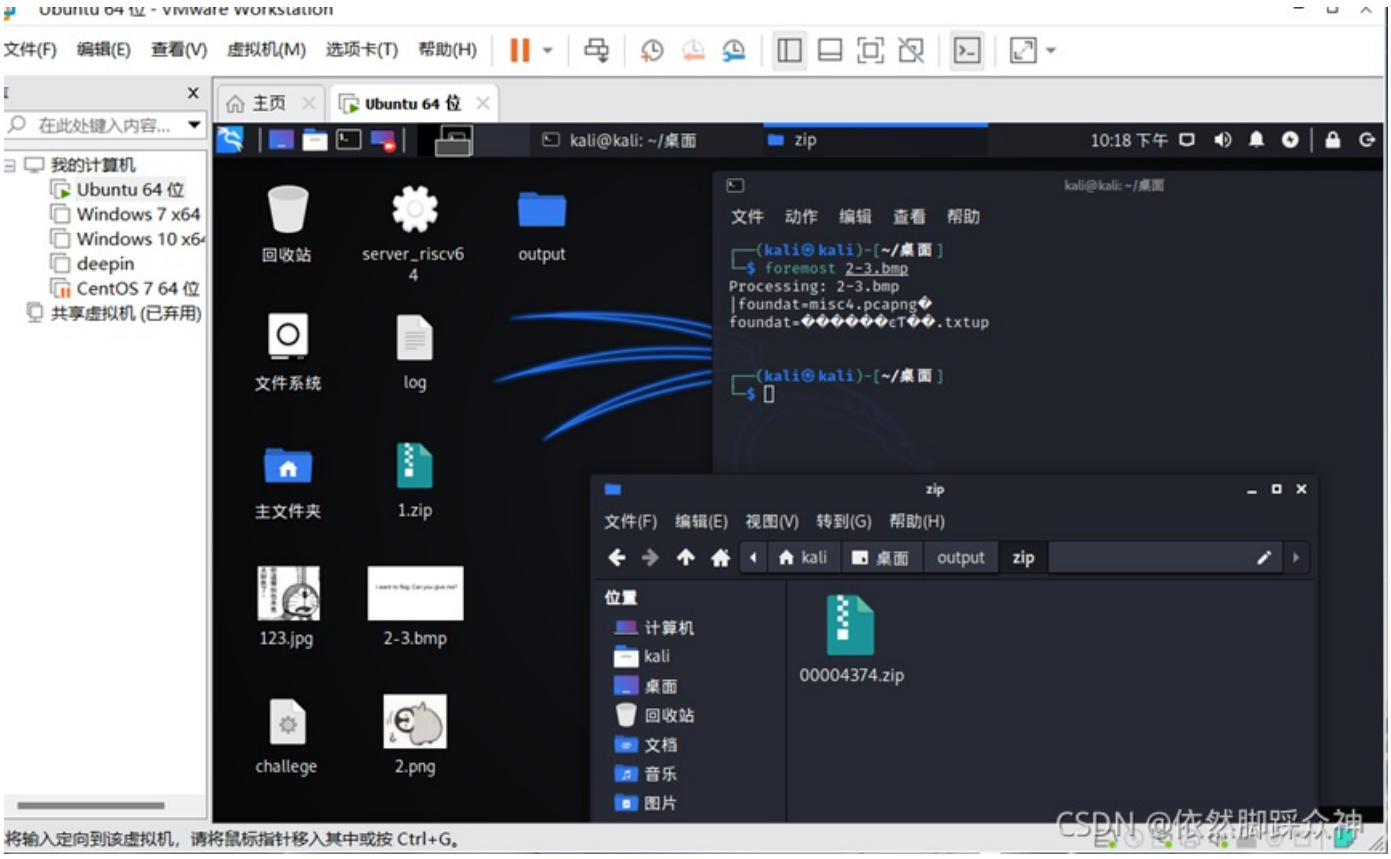


2 helloshark

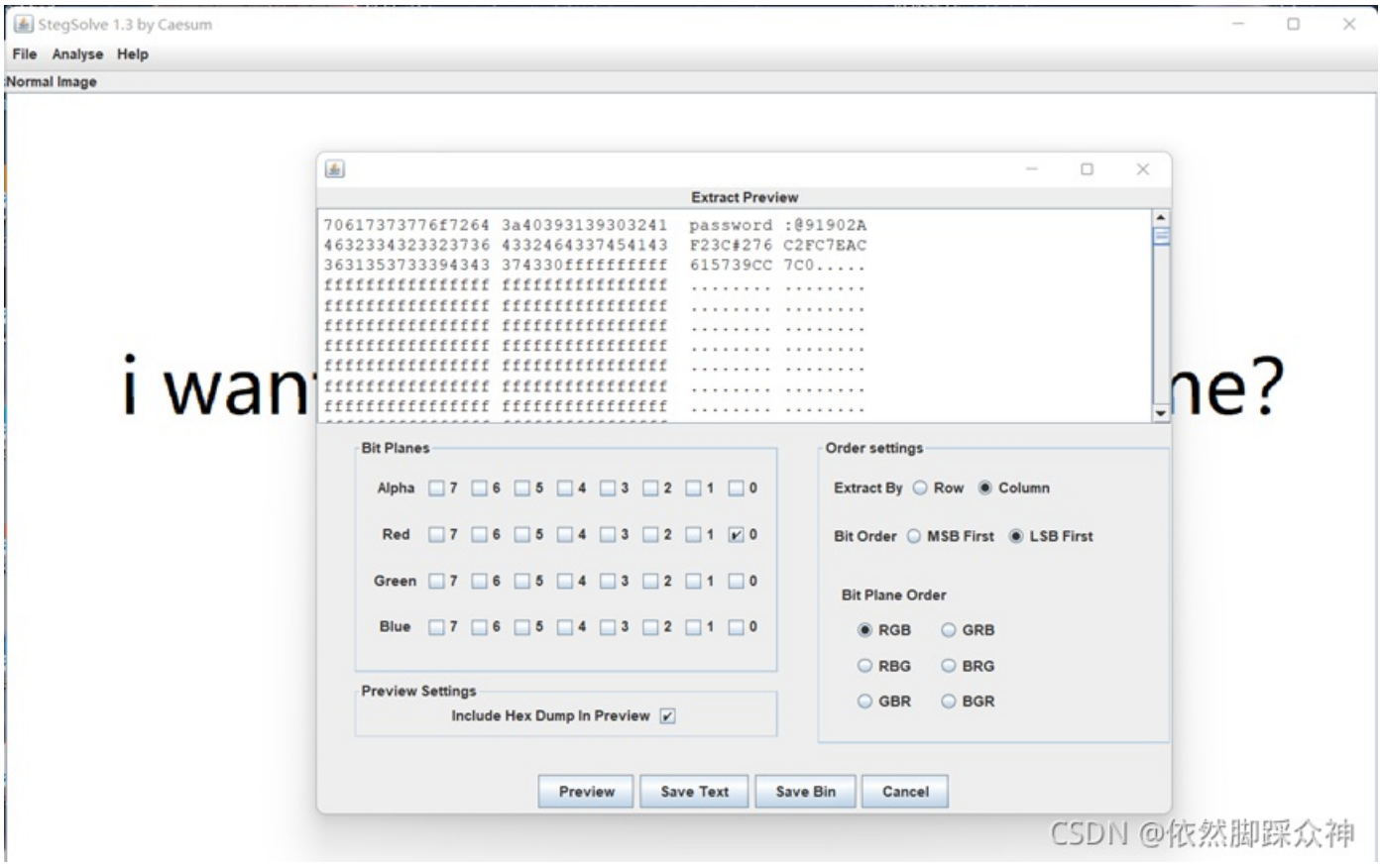
（题目序号 请参考解题总榜上面的序号）

操作内容：

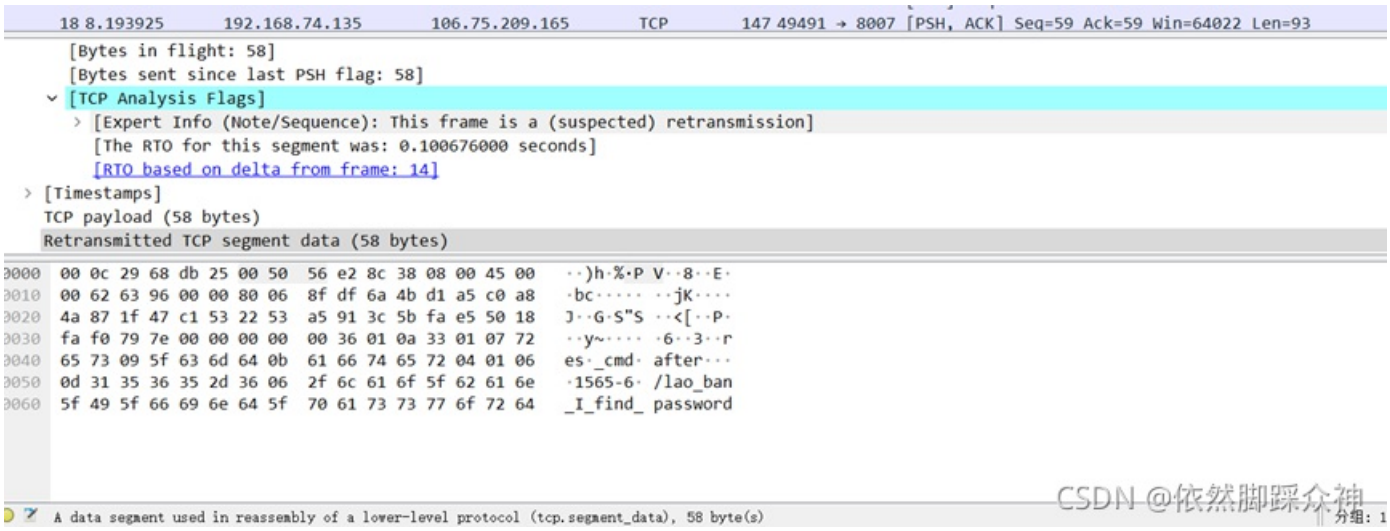
首先使用kali的foremost分离文件



然后发现此压缩包有密码，又根据压缩包里给出的提示推出图片隐写，接着我使用了stegSolve发现是lsb隐写



使用上面给出的password进行压缩包解密，得到流量分析文件，然后使用小鲨鱼流量分析软件



发现了这个，接下来追踪tcp流

```
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...
1565-6..a...C..o_.'^_..._..e/ri.>te",g
d^.t.Y.c.9.............l.=elk_.m.8.     .#|$n...#.
#.      _cmd.realMsg..privateMsg.       a||$... ..,..'........*.56..6
'..tT..... .
3..res  _cmd.after...
1565-6..4...C..=..'........7oriK~teplg
6..tR..cIy.............l\}el9..mNx.             c|$<...#.
#.      _cmd.realMsg..privateMsg.       4||$.....ND.........kimvv...0.....OneDayLovers..-1..UserFamilyName
newAvatars.S132391,128875,128868,128860,128861,128862,132380,132387,132388,101208,131941,131940..OccupationH
1..memberlevels..15..IsAnnualMemberb..1..avatars.?25,46,4506,4522,14935,20239,20901,21838,21945,22582,22932,
modelTypes..1.
PublicTalkPaon..-1..AvatarCardTypes..1.
```


靠眼力意外看见竖着写着个flag，将接下来竖着相同的字符输入了一遍，发现flag正确

flag值：

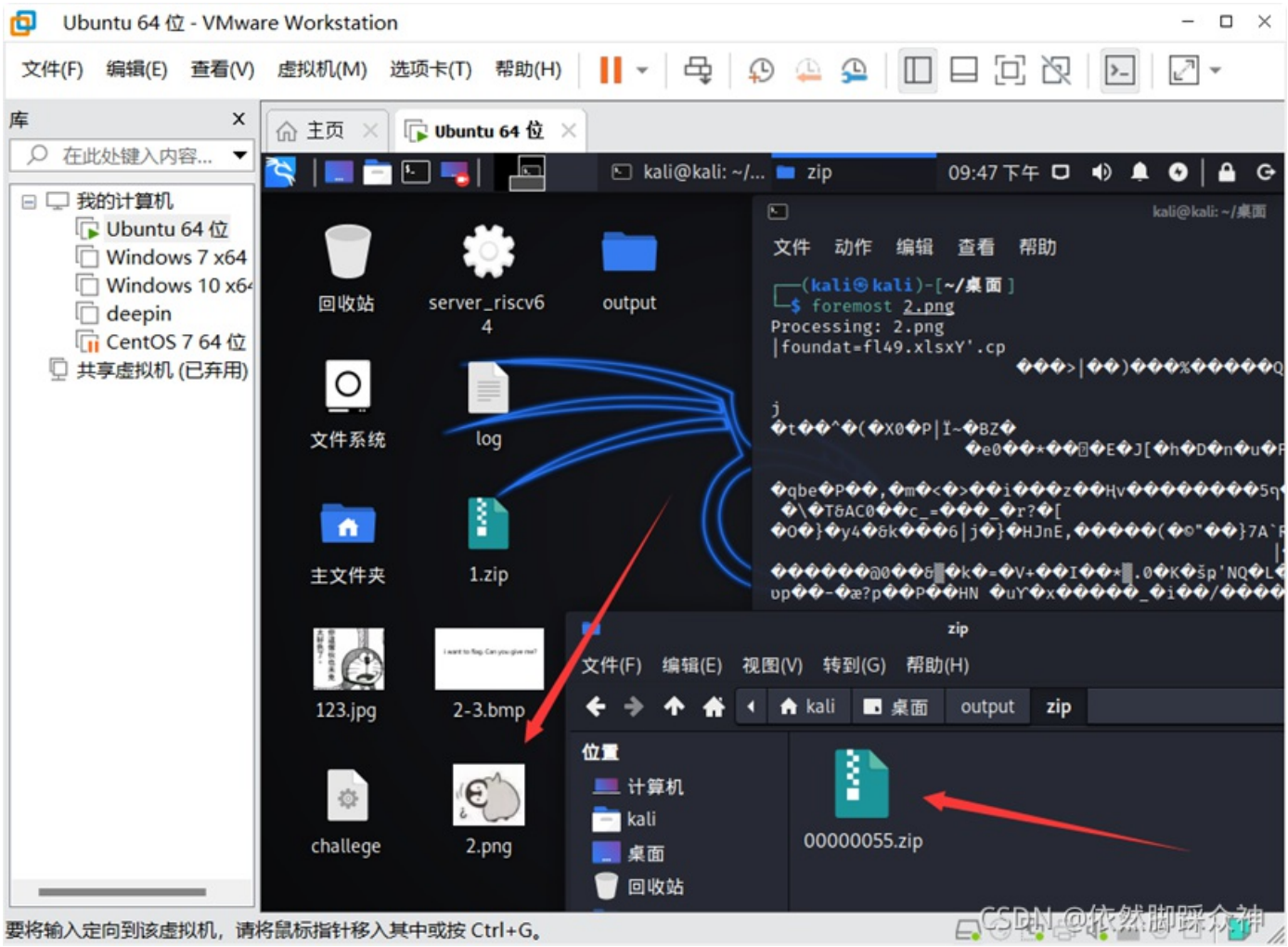
flag{a4e0a418-fced-4b2d-9d76-fdc9053d69a1}

3 secret_chart

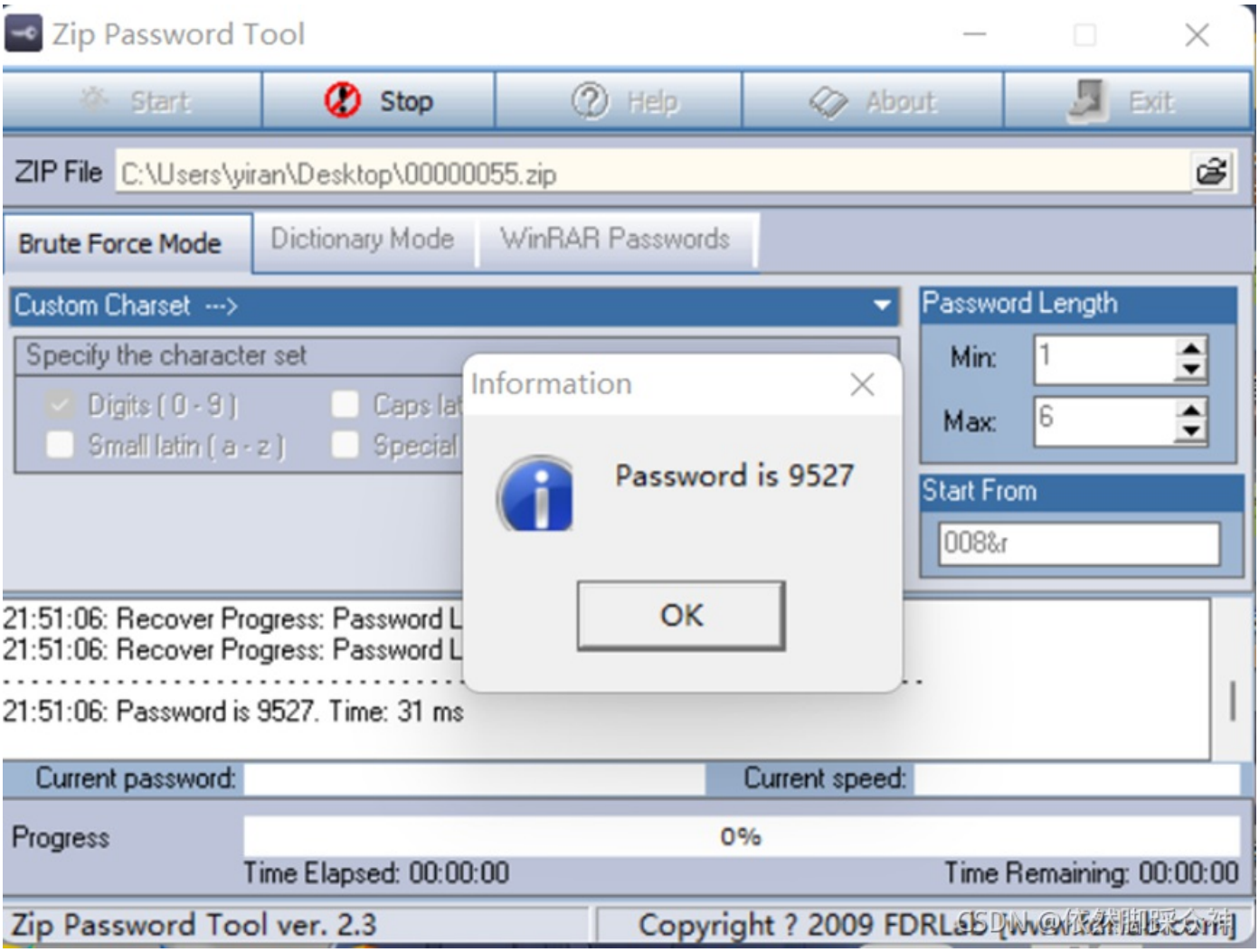
（题目序号 请参考解题总榜上面的序号）

操作内容：

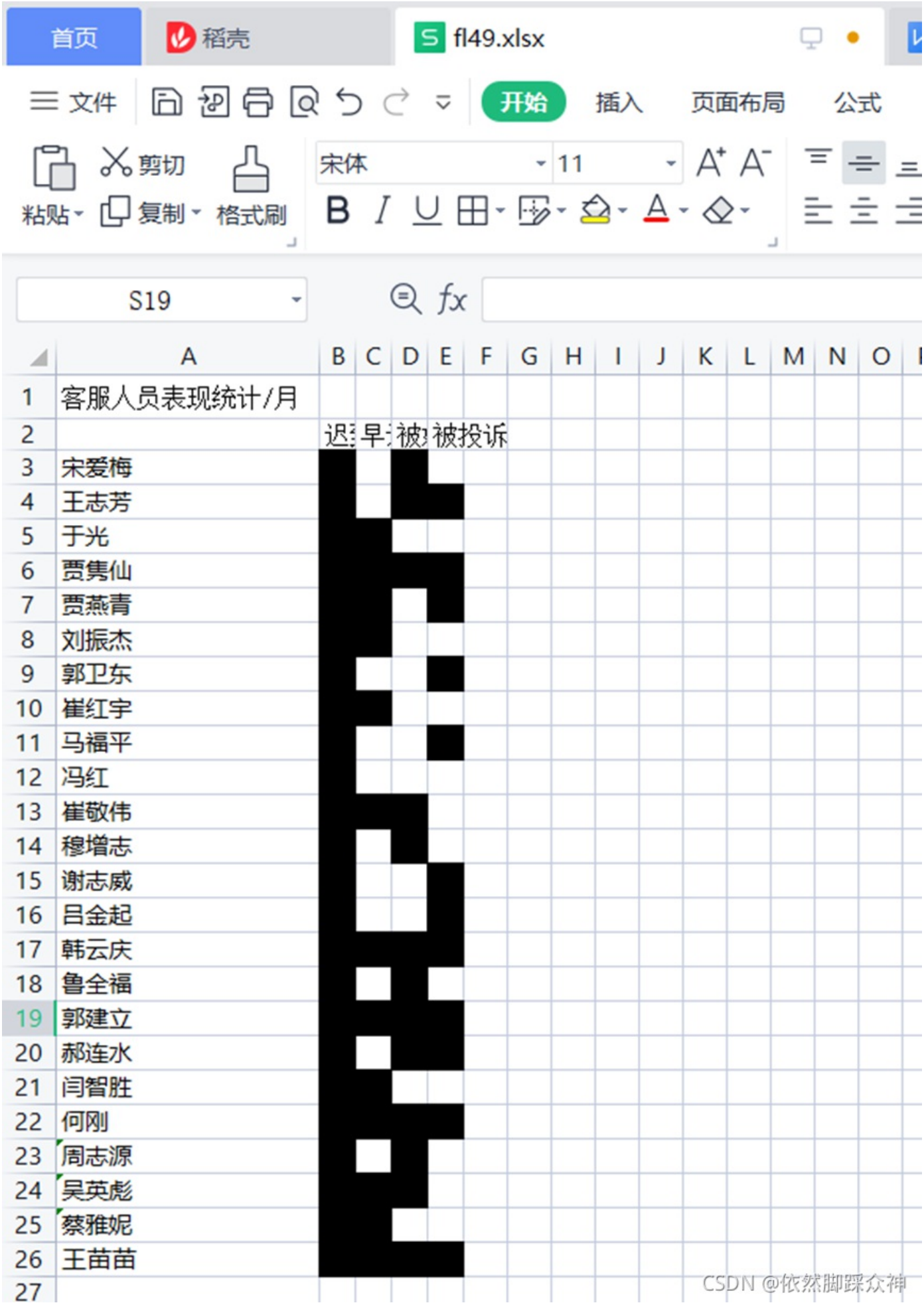
先将文件解压，用kali带的foremost分离出压缩包文件



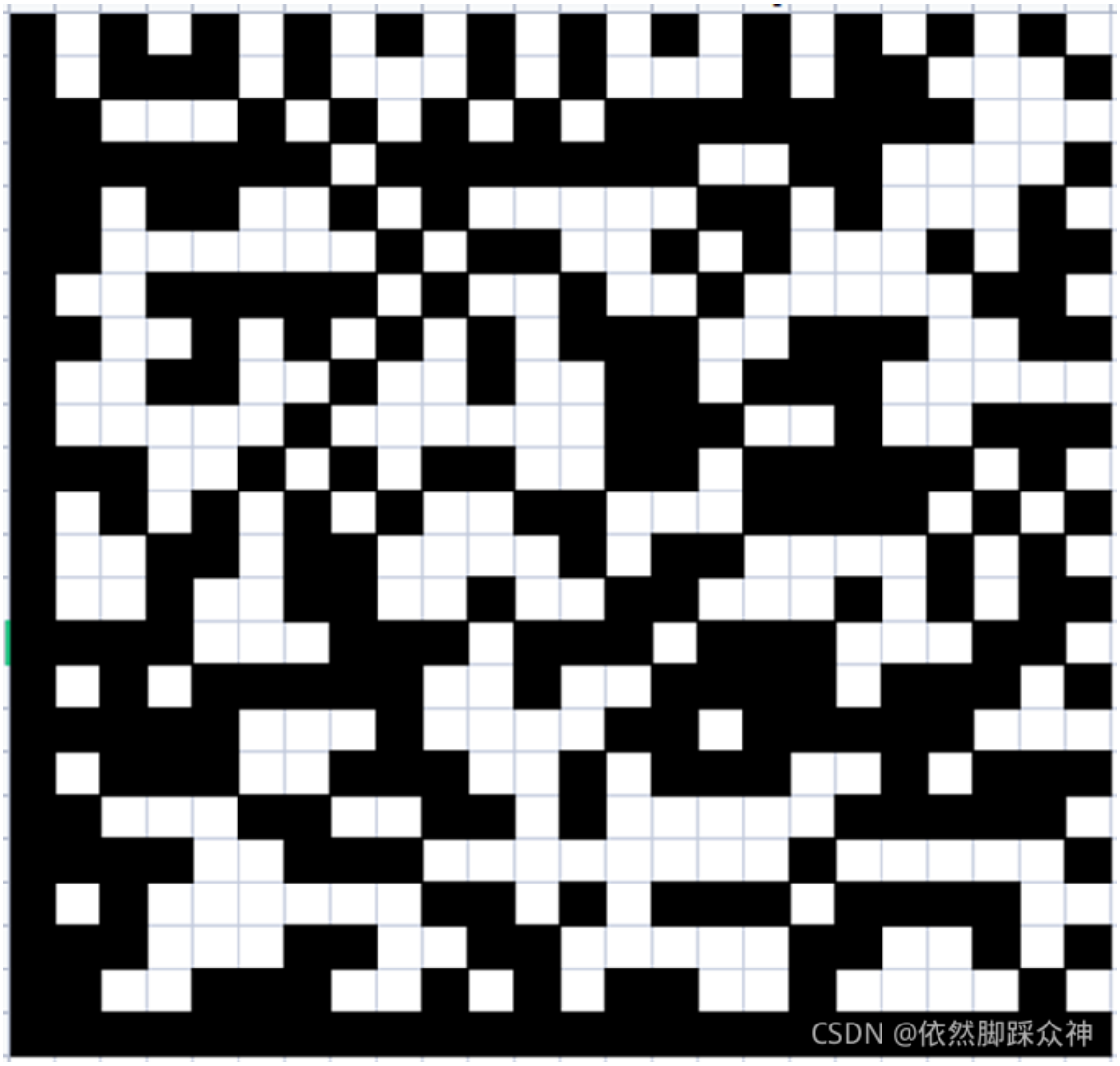
打开后发现文件有加密



用软件暴力破解之后发现密码意外的爆出来了，打开文件夹得到了一个文档文件，分析一波之后，此文档有规律，我将1全部转为黑色



发现它很像二维码，于是我将5-10月份的全部拼在了一起



用苹果自带的扫码器扫描之后，得到了zfua{B3s1o9in1Nw0halUnofuNc0HM1}

提交之后发现不对，想起来前缀应该是flag，第一想到是凯撒，于是将此去凯撒解密，一直偏移到20，发现前缀变成了flag

flag值：

flag{H3y1u9ot1Tc0ngrAtulaTi0NS1}