miscmisc 攻防世界

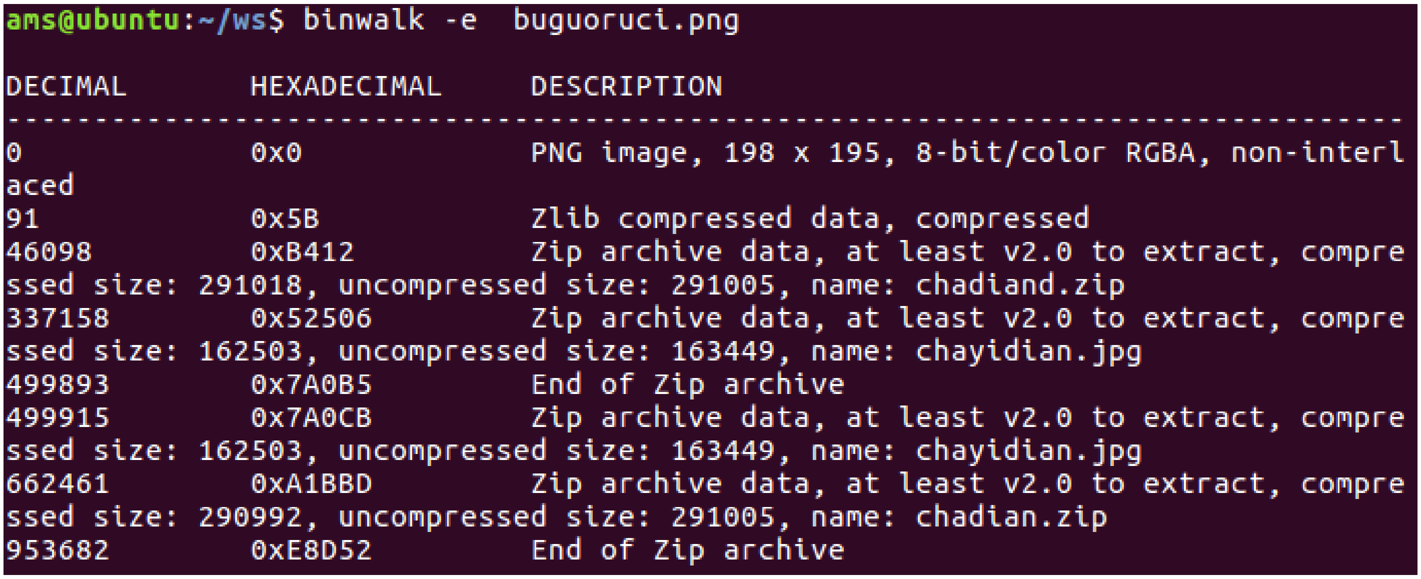
🐫 3分

题目描述

题目是一张图片

解题

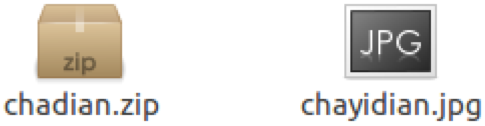
`binwalk`分离png文件



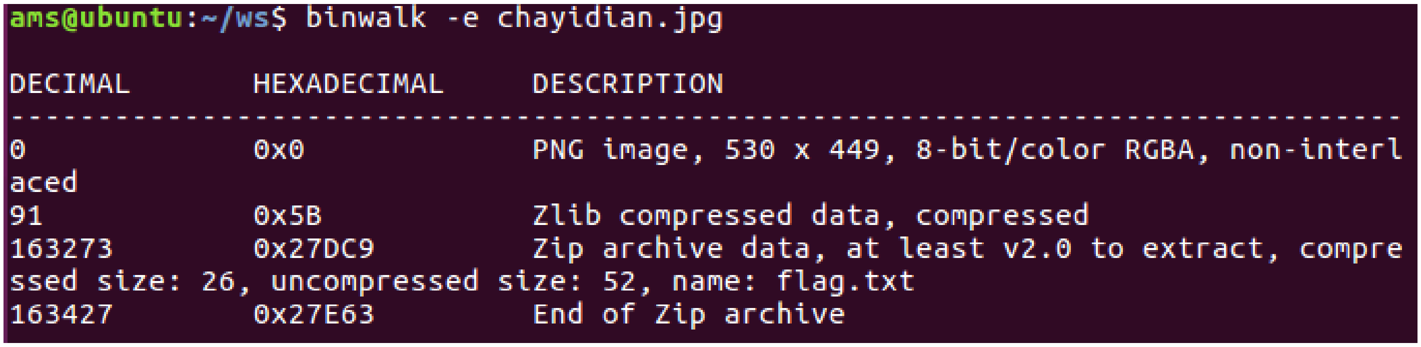
```
ams@ubuntu:~/ws$ binwalk -e  buguoruci.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 198 x 195, 8-bit/color RGBA, non-interl
aced
91            0x5B            Zlib compressed data, compressed
46098         0xB412          Zip archive data, at least v2.0 to extract, compre
ssed size: 291018, uncompressed size: 291005, name: chadiand.zip
337158        0x52506         Zip archive data, at least v2.0 to extract, compre
ssed size: 162503, uncompressed size: 163449, name: chayidian.jpg
499893        0x7A0B5         End of Zip archive
499915        0x7A0CB         Zip archive data, at least v2.0 to extract, compre
ssed size: 162503, uncompressed size: 163449, name: chayidian.jpg
662461        0xA1BBD         Zip archive data, at least v2.0 to extract, compre
ssed size: 290992, uncompressed size: 291005, name: chadian.zip
953682        0xE8D52         End of Zip archive
```

得到如下文件



压缩包需要密码，继续分离jpg文件

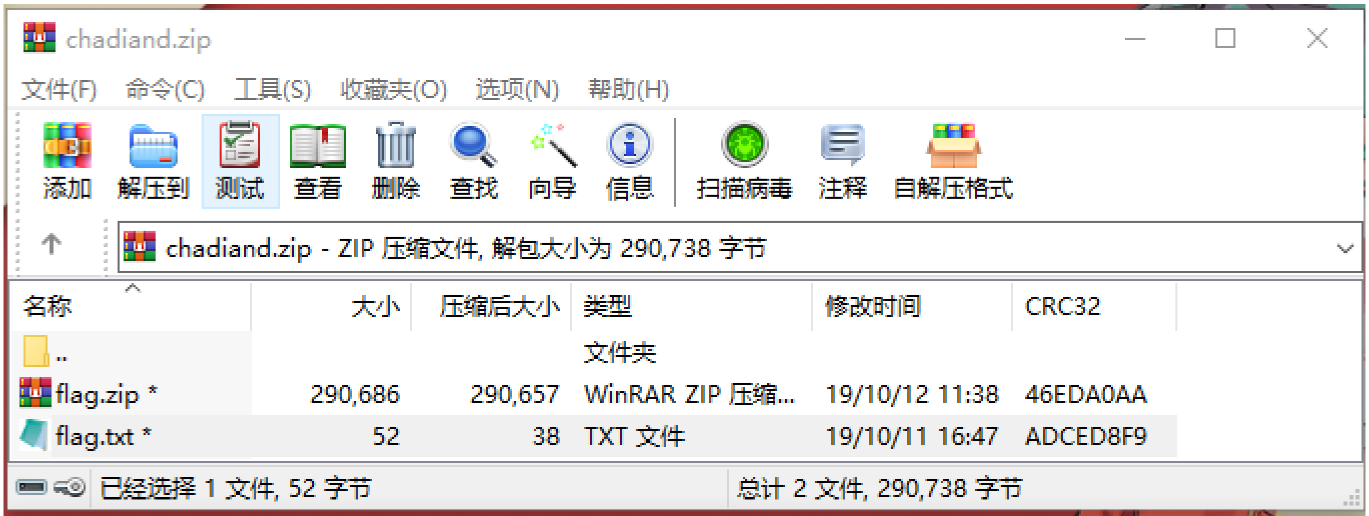


```
ams@ubuntu:~/ws$ binwalk -e chayidian.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 530 x 449, 8-bit/color RGBA, non-interl
aced
91            0x5B            Zlib compressed data, compressed
163273        0x27DC9         Zip archive data, at least v2.0 to extract, compre
ssed size: 26, uncompressed size: 52, name: flag.txt
163427        0x27E63         End of Zip archive
```

得到如下文件

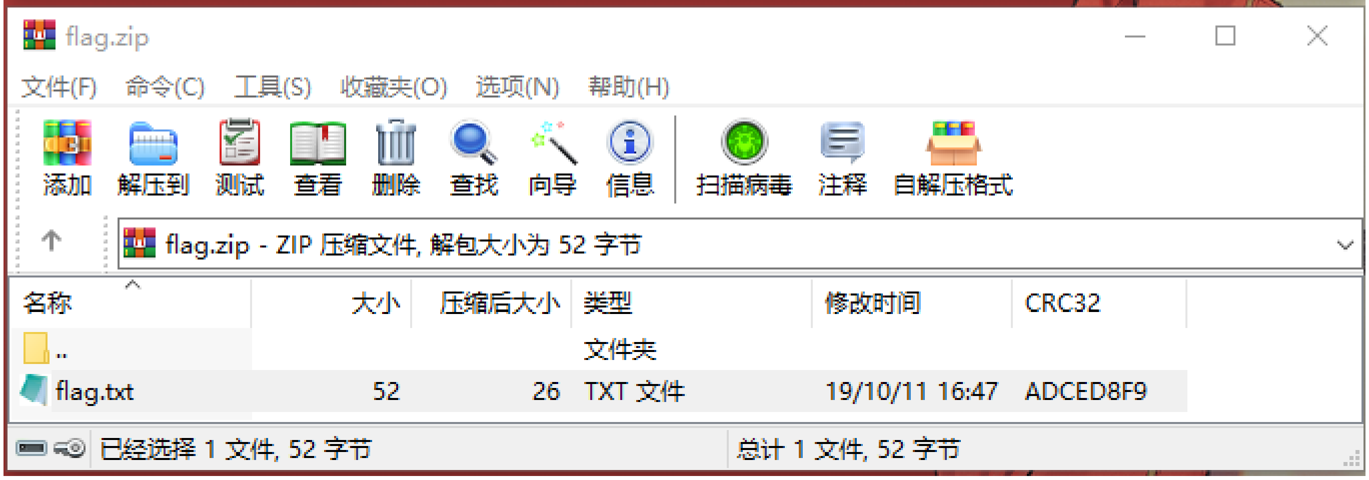
将`flag.txt`压缩后，发现与`chadian.zip`中`flag.txt`的CRC32一致，所以可以用明文攻击压缩包，来获得密码。


chadiand.zip
文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)
添加 解压到 测试 查看 删除 查找 向导 信息 扫描病毒 注释 自解压格式

chadiand.zip - ZIP 压缩文件, 解包大小为 290,738 字节

名称	大小	压缩后大小	类型	修改时间	CRC32
..			文件夹		
flag.zip *	290,686	290,657	WinRAR ZIP 压缩...	19/10/12 11:38	46EDA0AA
flag.txt *	52	38	TXT 文件	19/10/11 16:47	ADCED8F9

已经选择 1 文件, 52 字节　　总计 2 文件, 290,738 字节

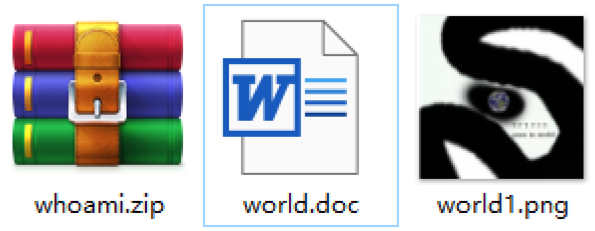

flag.zip
文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)
添加 解压到 测试 查看 删除 查找 向导 信息 扫描病毒 注释 自解压格式

flag.zip - ZIP 压缩文件, 解包大小为 52 字节

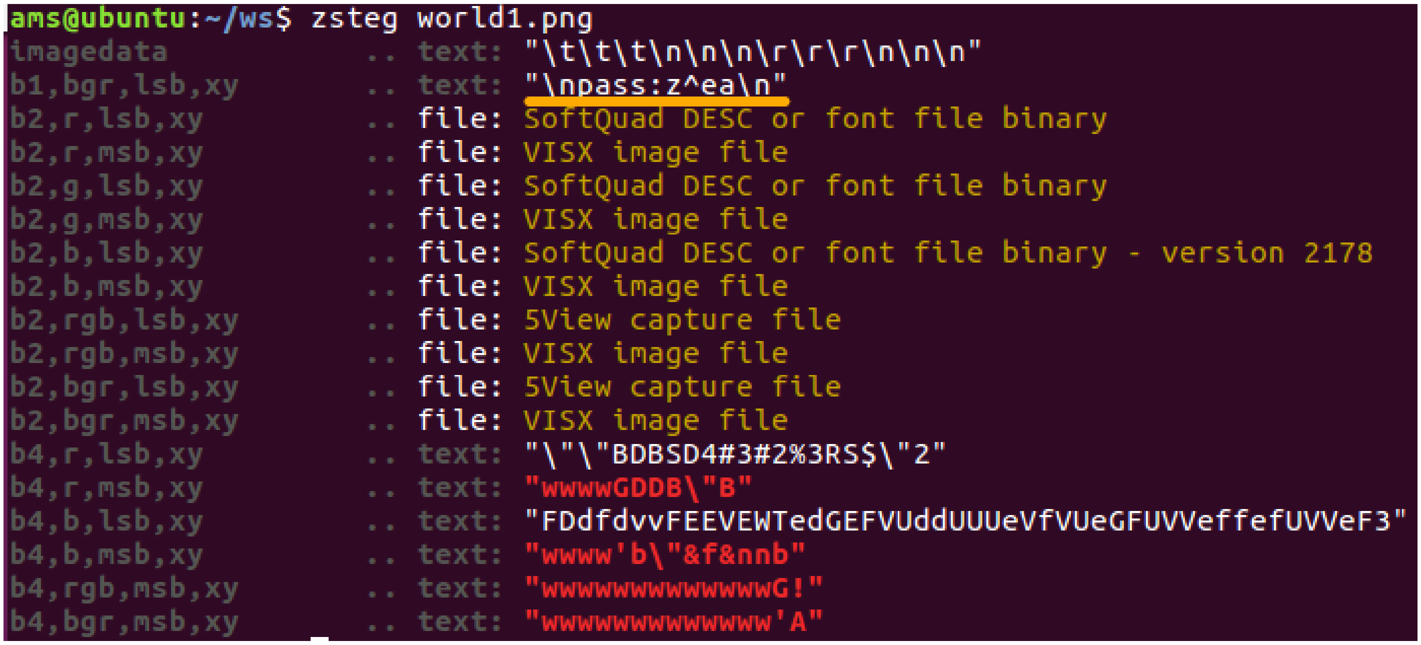
名称	大小	压缩后大小	类型	修改时间	CRC32
..			文件夹		
flag.txt	52	26	TXT 文件	19/10/11 16:47	ADCED8F9

已经选择 1 文件, 52 字节　　总计 1 文件, 52 字节

攻击得到密码 `z$^58a4w`，解压后得到如下文件，解压需要密码：

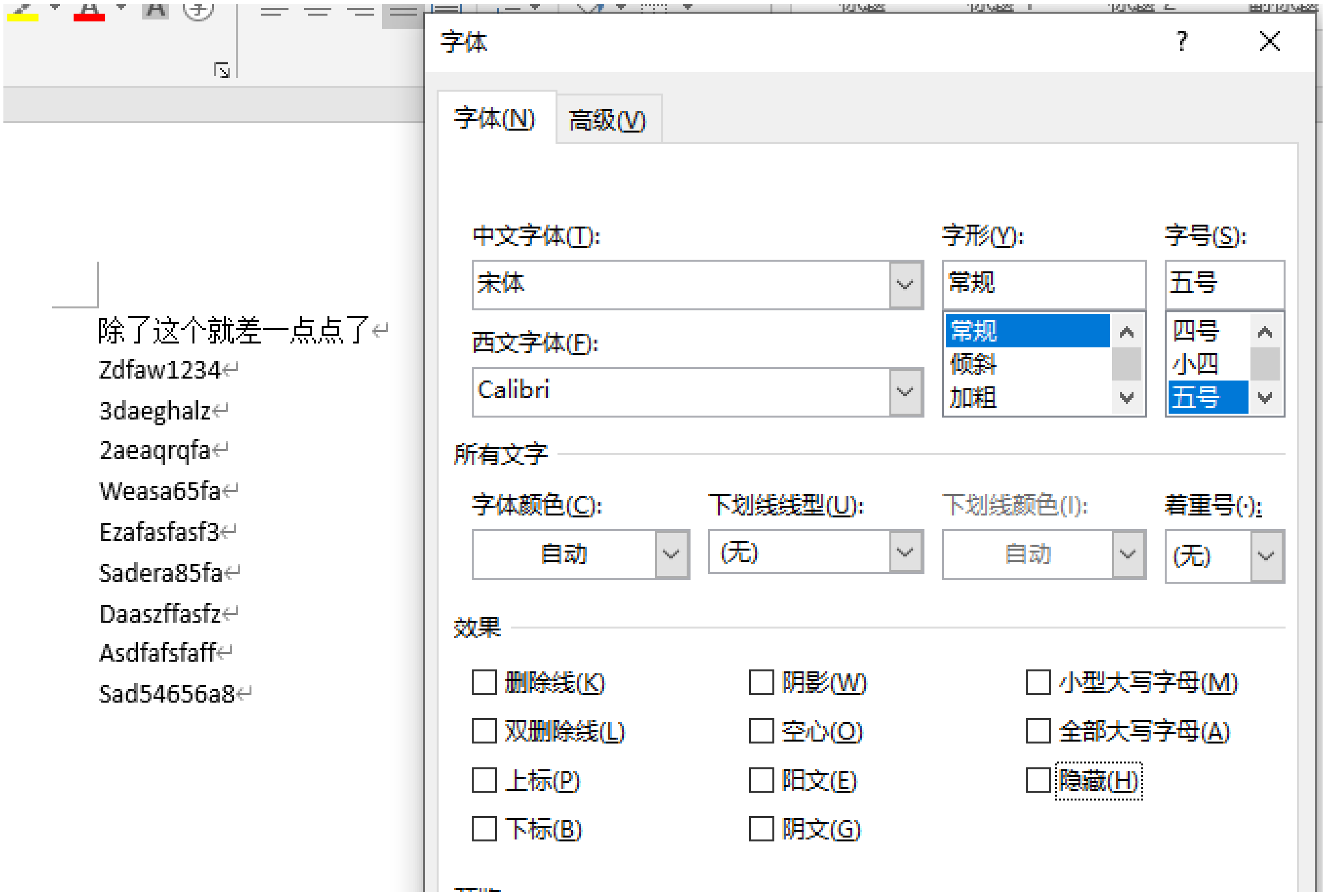


查看图片中的隐写字符串



```
ams@ubuntu:~/ws$ zsteg world1.png
imagedata           .. text: "\t\t\t\n\n\n\r\r\r\n\n\n"
b1,bgr,lsb,xy       .. text: "\npass:z^ea\n"
b2,r,lsb,xy         .. file: SoftQuad DESC or font file binary
b2,r,msb,xy         .. file: VISX image file
b2,g,lsb,xy         .. file: SoftQuad DESC or font file binary
b2,g,msb,xy         .. file: VISX image file
b2,b,lsb,xy         .. file: SoftQuad DESC or font file binary - version 2178
b2,b,msb,xy         .. file: VISX image file
b2,rgb,lsb,xy       .. file: 5View capture file
b2,rgb,msb,xy       .. file: VISX image file
b2,bgr,lsb,xy       .. file: 5View capture file
b2,bgr,msb,xy       .. file: VISX image file
b4,r,lsb,xy         .. text: "\"\"BDBSD4#3#2%3RS$\"2"
b4,r,msb,xy         .. text: "wwwwGDDB\"B"
b4,b,lsb,xy         .. text: "FDdfdvvFEEVEWTedGEFVUddUUUeVfVUeGFUVVeffefUVVeF3"
b4,b,msb,xy         .. text: "wwww'b\"&f&nnb"
b4,rgb,msb,xy       .. text: "wwwwwwwwwwwwwwG!"
b4,bgr,msb,xy       .. text: "wwwwwwwwwwwwww'A"
```

根据图片提示`pass in word`，打开doc，取消隐藏。



除了这个就差一点点了
Zdfaw1234
3daeghalz
2aeaqrqfa
Weasa65fa
Ezafasfasf3
Sadera85fa
Daaszffasfz
Asdfafsfaff
Sad54656a8

字体

字体(N) 高级(V)

中文字体(T): 宋体
西文字体(F): Calibri
字形(Y): 常规
字号(S): 五号

所有文字
字体颜色(C): 自动
下划线线型(U): (无)
下划线颜色(I): 自动
着重号(·): (无)

效果
□ 删除线(K)　□ 阴影(W)　□ 小型大写字母(M)
□ 双删除线(L)　□ 空心(O)　□ 全部大写字母(A)
□ 上标(P)　□ 阳文(E)　□ 隐藏(H)
□ 下标(B)　□ 阴文(G)

解压密码为`z^ea4zaa3azf8`

解压`whoami.zip`即可得到flag