[MISC 3](#_Toc24100)

[一.隐写 3](#_Toc27609)

[1.Stegsolve 3](#_Toc17262)

[2.010Editor 5](#_Toc14782)

[（一）文件头 5](#_Toc8726)

[（二）搜索 6](#_Toc32746)

[（三）规律字符串 7](#_Toc30663)

[（四）长宽 7](#_Toc6737)

[（五）插入字节 8](#_Toc6588)

[（六）RAR的CRC错误 8](#_Toc5652)

[（七）导入16进制文件 8](#_Toc25141)

[（八）异或隐写 9](#_Toc26502)

[（九）伪加密 10](#_Toc21224)

[3.Python脚本 10](#_Toc13679)

[（一）图片像素点变字符 10](#_Toc7104)

[（二）将base64字符串或文件代表的文件输出出来 11](#_Toc2893)

[（三）文件批量改名 12](#_Toc12438)

[（四）CRC批量爆破 12](#_Toc4765)

[（五）解压缩套娃文件 12](#_Toc11733)

[（六）RGB生成二维码 13](#_Toc13173)

[（七）对文件做数学运算并生成新文件 14](#_Toc2858)

[（八）TTL隐写 14](#_Toc16125)

[4.RoutePassView 15](#_Toc21668)

[5.Audacity 16](#_Toc6781)

[（一）摩斯电码 16](#_Toc9720)

[（二）二进制数 16](#_Toc22561)

[6.Steghide 17](#_Toc16582)

[7.F5-steganography 17](#_Toc21159)

[8.Foremost 17](#_Toc7689)

[9.Binwalk 17](#_Toc19331)

[10.Gunplot 18](#_Toc7203)

[11.Outguess 18](#_Toc18253)

[12.NTFS流 19](#_Toc13852)

[13.Sublime 20](#_Toc627)

[14.LSB隐写 20](#_Toc22035)

[15.Exiftool多文件内容查找 21](#_Toc26744)

[16.USB隐写 21](#_Toc9196)

[17.DOC隐写 21](#_Toc2644)

[（一）隐藏内容 22](#_Toc31427)

[（二）修复 22](#_Toc13487)

[18.Excel隐写 22](#_Toc17073)

[19.SonicVisualiser 24](#_Toc3336)

[20.SlientEye 24](#_Toc6619)

[21.Montage 25](#_Toc5389)

[21.Gaps 25](#_Toc20201)

[21.TXT去除重复行 26](#_Toc11689)

[22.时间隐写 26](#_Toc93)

[二.流量 28](#_Toc16279)

[1.length排序 28](#_Toc3928)

[2.搜索内容 28](#_Toc7546)

[3.ftp协议 28](#_Toc18896)

[4.HTTP流导出文件 29](#_Toc5068)

[5.搜索流 29](#_Toc3918)

[6.SSL秘钥 29](#_Toc32029)

[7.Voip通话 30](#_Toc3231)

[8.内容导出 31](#_Toc9597)

[三.爆破 32](#_Toc20008)

[1.ARCHPR 32](#_Toc24070)

[四.各种稀有文件格式 34](#_Toc9660)

[1.文件没有后缀名 34](#_Toc27102)

[2.VMDK文件 34](#_Toc2073)

[3.DOC文件源文件夹 35](#_Toc30767)

[4.Issas.dmp 35](#_Toc26504)

[5.Bpg文件 36](#_Toc15070)

# MISC

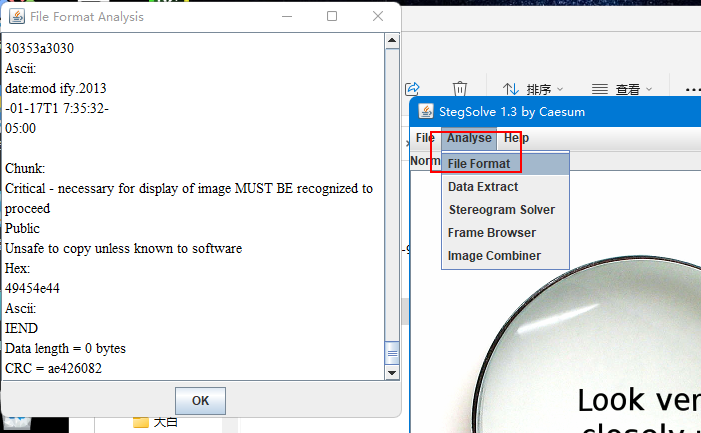
## 一.隐写

常见的几种解决工具：

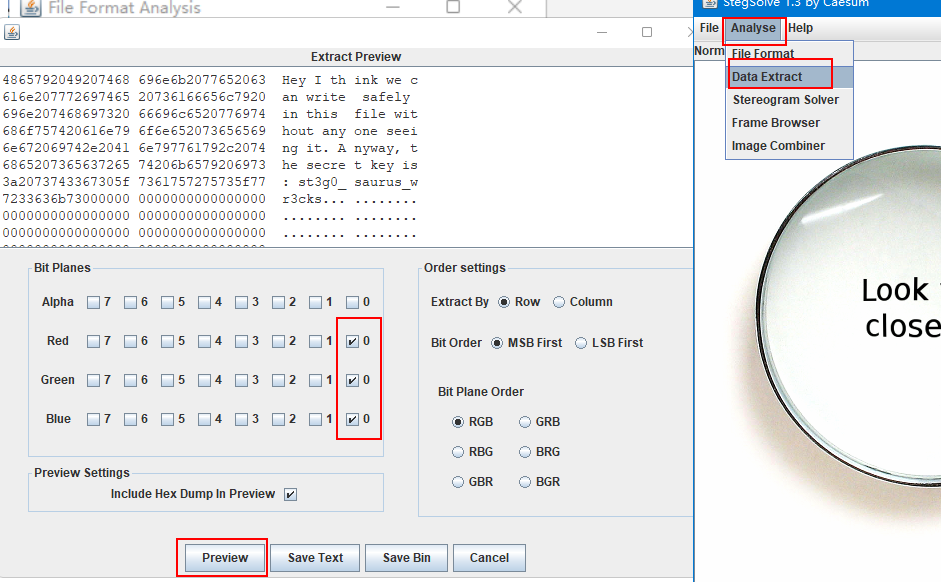
1.Stegsolve：

打开方式：java -jar jar的路径

（一）查看File Format里是否存在flag或者一些有用的字符串

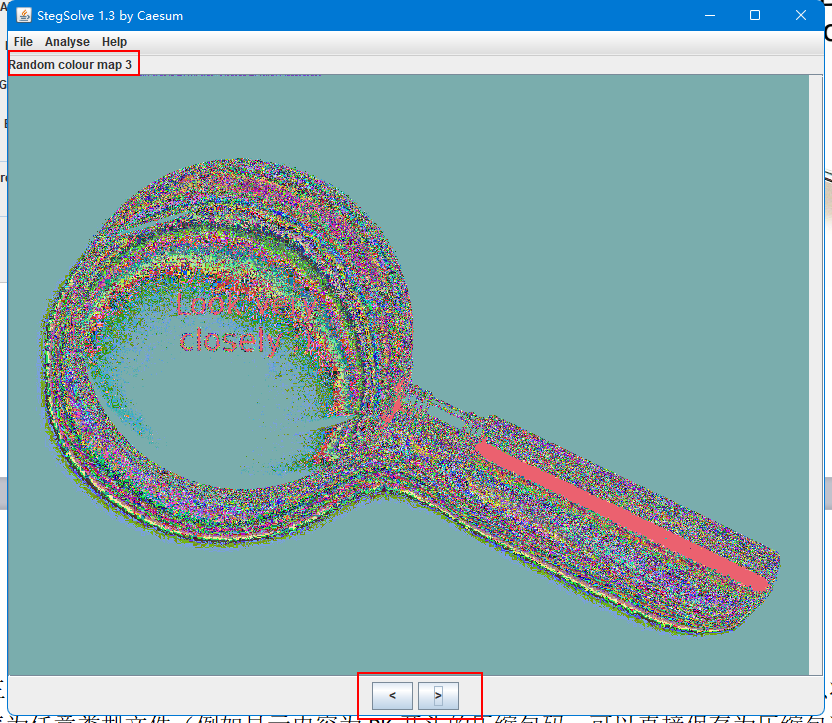


（二）查看Data Extract里是否存在flag或者一些有用的字符串，点击Save Bin可以将内容保存为任意类型文件（例如显示内容为PK开头的压缩包码，可以直接保存为压缩包）

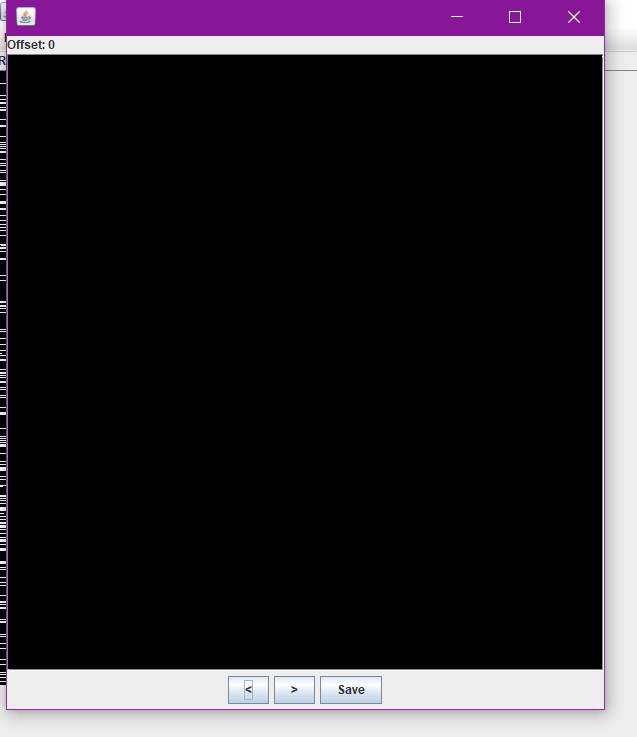


如果存在隐藏文件，可以点击SaveBin保存为指定格式文件

（三）主页点击下方左右按钮可以查看是否存在隐藏文件



1. 如果是gif，查看Frame Browser里是否存在有用的图片



2.010Editor：

打开文件查看16进制与文本信息

#### （一）文件头

里面是否存在请求头信息（隐藏文件），删除无用部分保存文请求头类型的文件并输出，一些常见的请求头如下

JPEG (jpg)，文件头：FFD8FFE0或FFD8FFE1或FFD8FFE8文件尾：FF D9

GIF ([gif](https://baike.baidu.com/item/gif/217778?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E6%96%87%E4%BB%B6%E5%A4%B4/_blank))，文件头：47494638PNG文件尾：00 3B

PNG，文件头：89504E47文件尾：AE 42 60 82

TIFF (tif)，文件头：49492A00

Windows Bitmap (bmp)，文件头：424DC001

CAD ([dwg](https://baike.baidu.com/item/dwg/5953048?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E6%96%87%E4%BB%B6%E5%A4%B4/_blank))，文件头：41433130

Adobe Photoshop (psd)，文件头：38425053

Rich Text Format ([rtf](https://baike.baidu.com/item/rtf/13211185?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E6%96%87%E4%BB%B6%E5%A4%B4/_blank))，文件头：7B5C727466

XML (xml)，文件头：3C3F786D6C

HTML (html)，文件头：68746D6C3E

Email [thorough only] (eml)，文件头：44656C69766572792D646174653A

Outlook Express (dbx)，文件头：CFAD12FEC5FD746F

Outlook (pst)，文件头：2142444E

MS Word/Excel (xls.or.doc)，文件头：D0CF11E0

MS Access ([mdb](https://baike.baidu.com/item/mdb/9688610?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E6%96%87%E4%BB%B6%E5%A4%B4/_blank))，文件头：5374616E64617264204A

WordPerfect (wpd)，文件头：FF575043

Adobe Acrobat ([pdf](https://baike.baidu.com/item/pdf/317608?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E6%96%87%E4%BB%B6%E5%A4%B4/_blank))，文件头：255044462D312E

Quicken (qdf)，文件头：AC9EBD8F

Windows Password (pwl)，文件头：E3828596

ZIP Archive ([zip](https://baike.baidu.com/item/zip/15417954?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E6%96%87%E4%BB%B6%E5%A4%B4/_blank))，文件头：504B0304文件尾：50 4B

RAR Archive ([rar](https://baike.baidu.com/item/rar/2502036?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E6%96%87%E4%BB%B6%E5%A4%B4/_blank))，文件头：52617221

Wave ([wav](https://baike.baidu.com/item/wav/218914?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E6%96%87%E4%BB%B6%E5%A4%B4/_blank))，文件头：57415645

AVI ([avi](https://baike.baidu.com/item/avi/213655?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E6%96%87%E4%BB%B6%E5%A4%B4/_blank))，文件头：41564920

Real Audio (ram)，文件头：2E7261FD

Real Media (rm)，文件头：2E524D46

MPEG ([mpg](https://baike.baidu.com/item/mpg/213809?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E6%96%87%E4%BB%B6%E5%A4%B4/_blank))，文件头：000001BA

MPEG (mpg)，文件头：000001B3

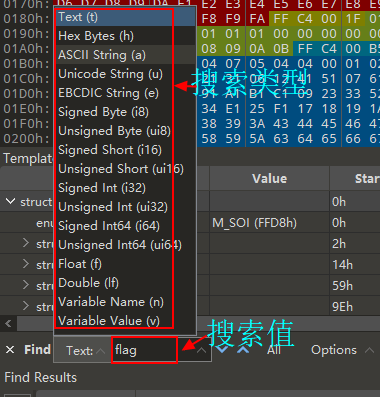
Quicktime (mov)，文件头：6D6F6F76

Windows Media ([asf](https://baike.baidu.com/item/asf/3918?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E6%96%87%E4%BB%B6%E5%A4%B4/_blank))，文件头：3026B2758E66CF11

MIDI (mid)，文件头：4D546864

#### （二）搜索

直接搜索某些字段值，或者某些编码（例如乱码可以尝试EBCDIC格式显示）



#### （三）规律字符串

一些规律的字符串很可能藏有信息，直接拖进CyberChef尝试。此外还有几种情况：

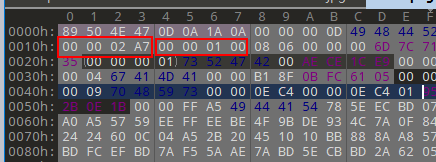
只含0和1的->8位一组转为ASCII

data:image开头：程序或在线网站解析

16进制代码包含A-F的规则字符串

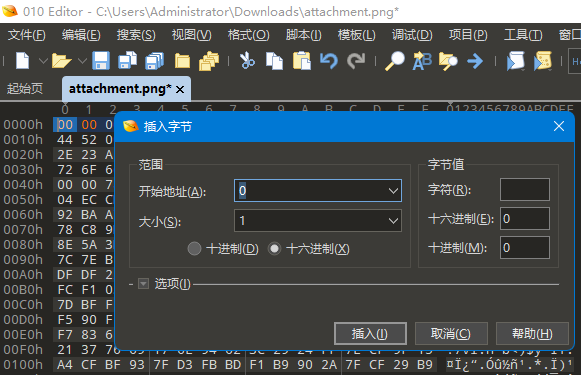
#### （四）长宽

图片可以修改长度和宽度，长和宽分别由每8位hex决定，值越大长宽也越大：



#### （五）插入字节

点击编辑->插入/覆盖->插入字节，开始地址设置成0，大小为1就插入了一个00字节



#### （六）RAR的CRC错误

rar有可能隐藏png，且png的图片压缩的文件头有问题，文件块的HEAD\_TYPE应该是0x74而不是0x7A。

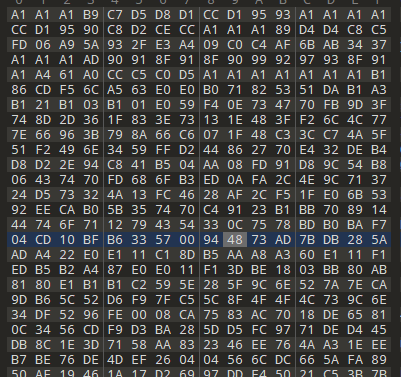


#### （七）导入16进制文件

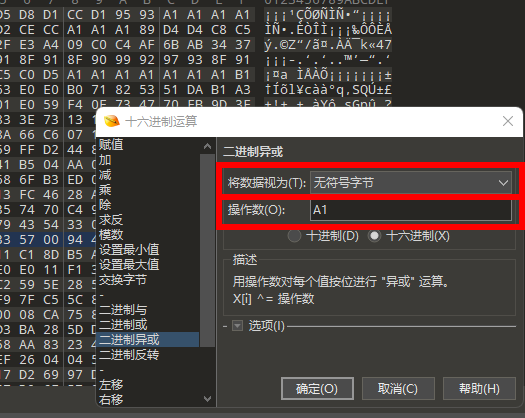
File->Import Hex...选择16进制文件，或者左侧全选使用Ctrl+Shift+V粘贴

#### （八）异或隐写

类似16进制文本存在大量相同字符(下面是A1)

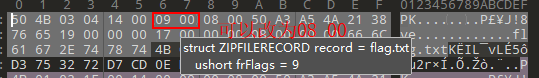


工具->十六进制运算->二进制异或，选择无符号字节，输入操作数(相同字节)，点击确定后保存为文件即可



#### （九）伪加密

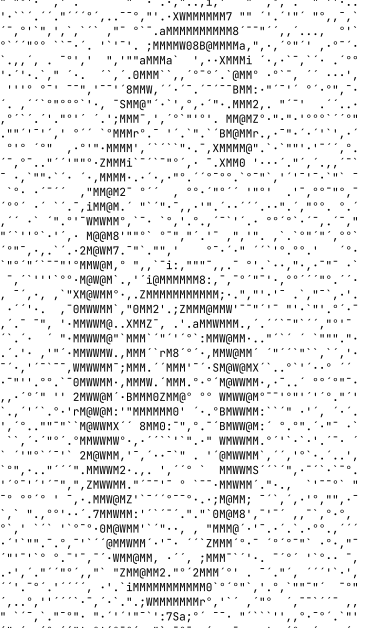
打开文件可能藏有信息。另外有可能是伪加密，打开压缩包找到头部其中四位的0? 00，如果?是奇数加密，偶数不加密，可以改为偶数尝试是否能解压



3.Python脚本：

#### （一）图片像素点变字符

将图片的像素点转换为字符，将字符组合成像素矩阵图像，字符串按一定宽度排列



#### （二）将base64字符串或文件代表的文件输出出来

注意里面输出的格式根据实际修改

字符串读取输出



文件读取输出



#### （三）文件批量改名

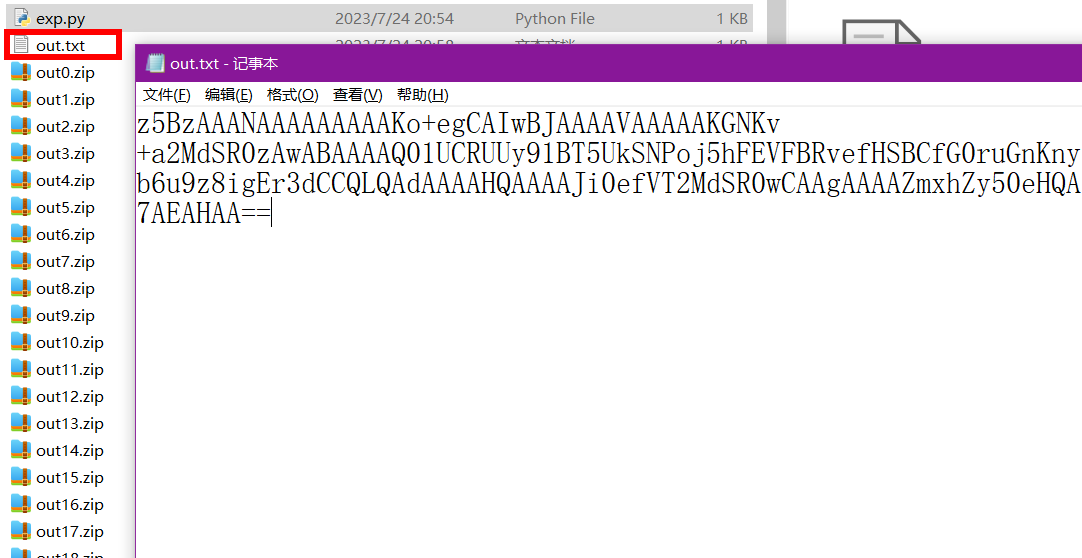
exp改的是后缀名，exp2改的是文件名



#### （四）CRC批量爆破

如果一堆特别小的压缩包可以使用CRC批量爆破脚本，注意脚本里文件名跟实际修改，运行后生成一个out.txt得到所有压缩包内容的拼接

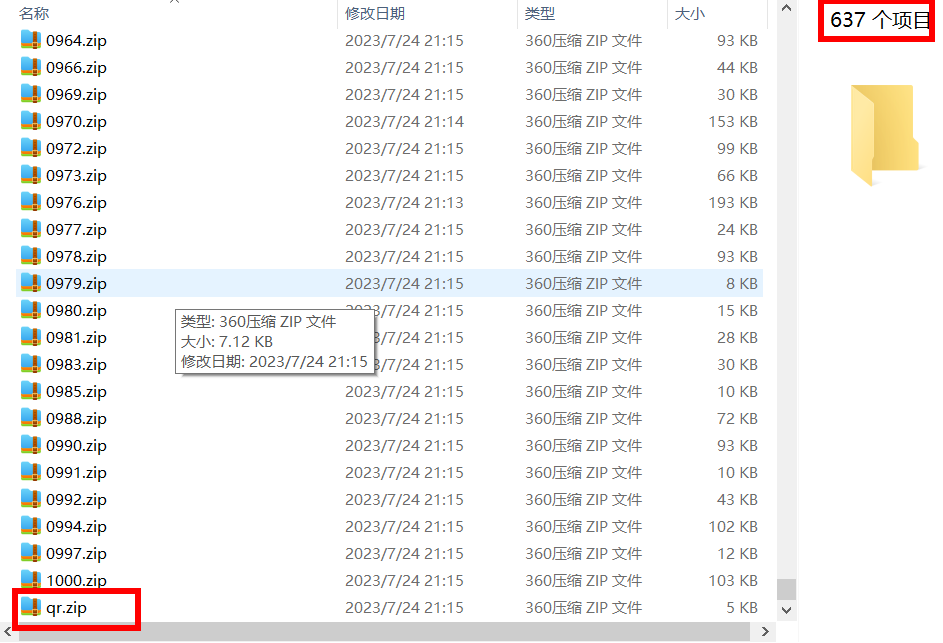




#### （五）解压缩套娃文件

注意更改读取压缩包文件名即可

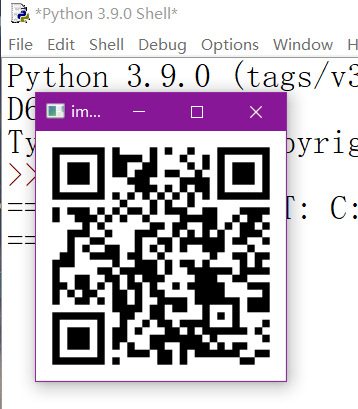




#### （六）RGB生成二维码

注意根据需求文件修改文件名





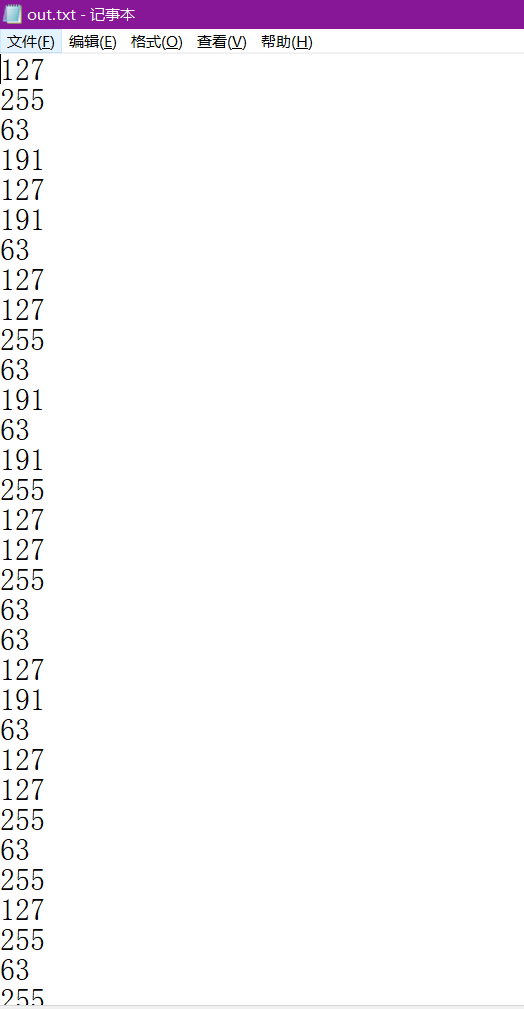
#### （七）对文件做数学运算并生成新文件

下面的运算过程和文件名根据需求改



#### （八）TTL隐写

给定文件格式：

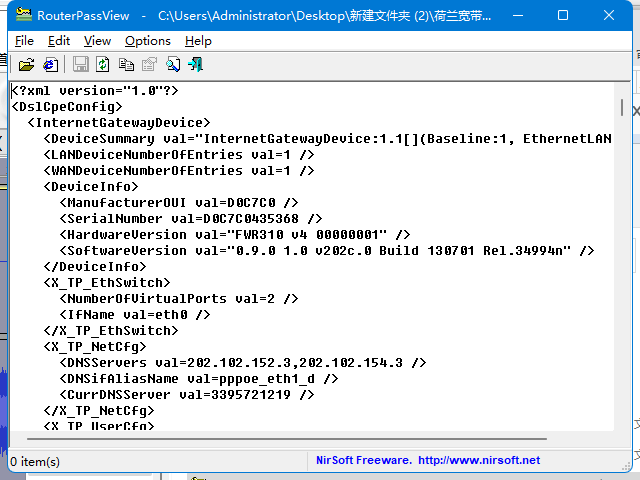


注意根据需求文件修改文件名



4.RoutePassView：

这个工具专门用来打开bin文件可以查看到文件信息进行搜索

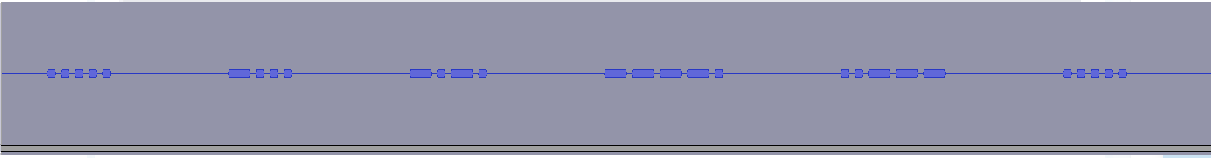


5.Audacity：

音乐文件可以用这个工具打开查看频谱图，图中可能藏有信息

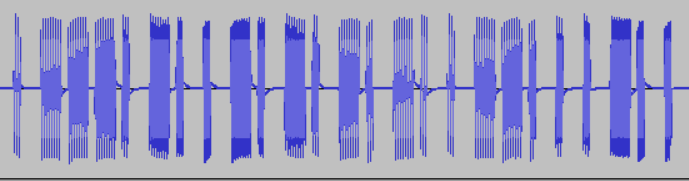
#### （一）摩斯电码

短的对应.，长的对应-



#### （二）二进制数

短的对应0，长的对应1。或者相反

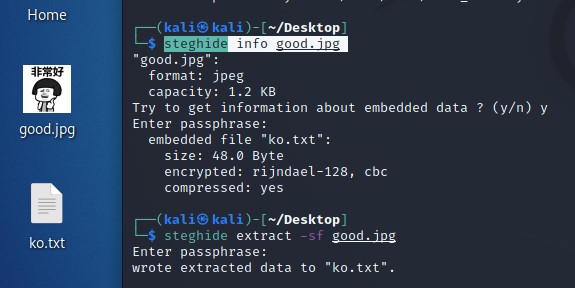


6.Steghide：

Kali下使用：文件放在桌面就行，先使用指令steghide info 文件名

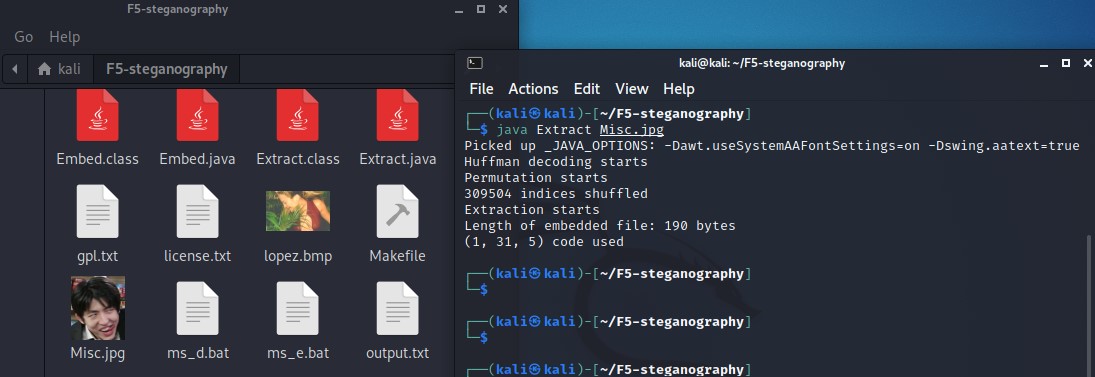
在使用指令steghide extract -sf 文件名即可获得其中隐藏的文件

Enter passphrase:直接回车就行



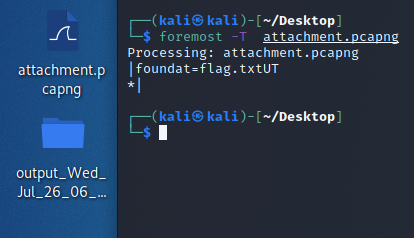
7.F5-steganography：

Kali下使用：文件放在F5-steganography文件夹中：使用指令java Extract 文件名即可获取隐藏文件



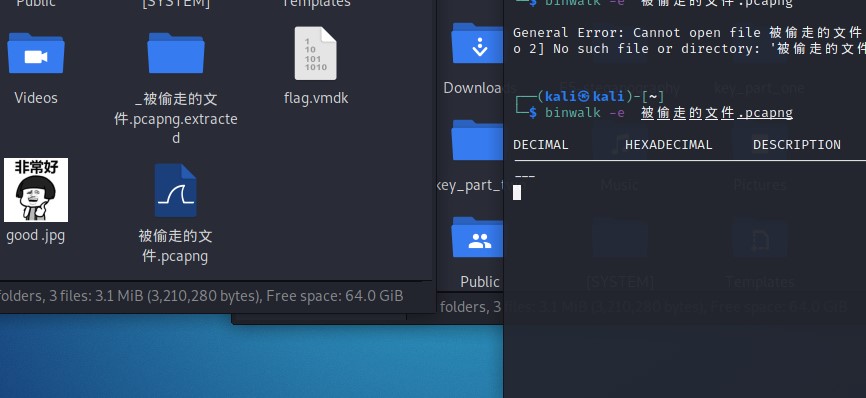
8.Foremost：

Kali下使用：文件放在桌面就行，使用指令foremost -T 文件名即可获取隐藏文件信息



9.Binwalk:

Kali下使用：文件放在桌面Home文件夹下，使用指令binwalk -e 文件名即可获取隐藏文件并保存到Home文件夹下



10.Gunplot:

根据点的坐标组合生成图片，需要在安装exe文件家中放入坐标点集合的txt文件，然后运行gnuplot.exe，输入plot “文件名”即可输出生成的文件(文件路径即名称不能问中文!)

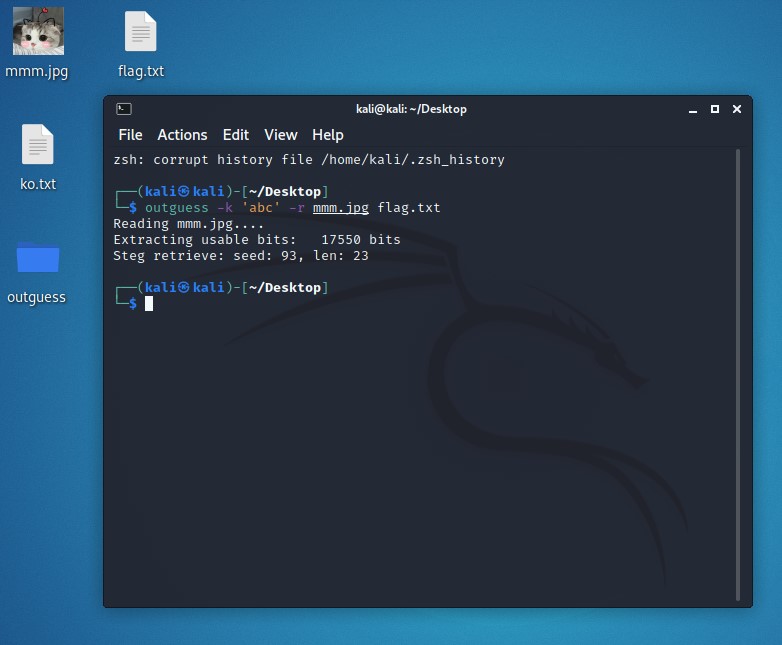


11.Outguess:

下载后放到kali中，进入根文件夹运行：sudo ./configure && make && sudo make install安装配置文件



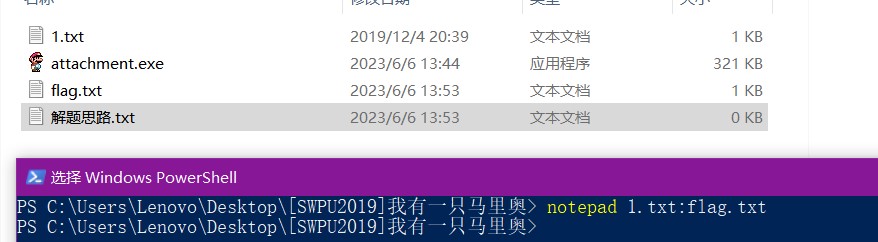
运行outguess -k ‘key值’ -r 隐写文件名 破解出来文件名，可以将文件的隐写内容输出到破解出来文件中



12.NTFS流:

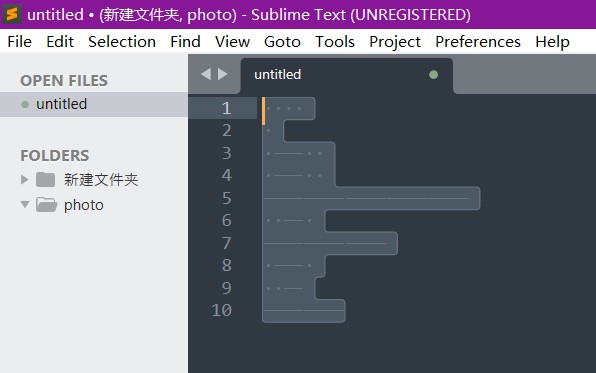
运行notepad文件名:输出文件名

即可将隐藏数据写到输出文件中



13.Sublime:

用来查看一些不可见字符，粘贴进来后全部选中可以看到隐藏信息

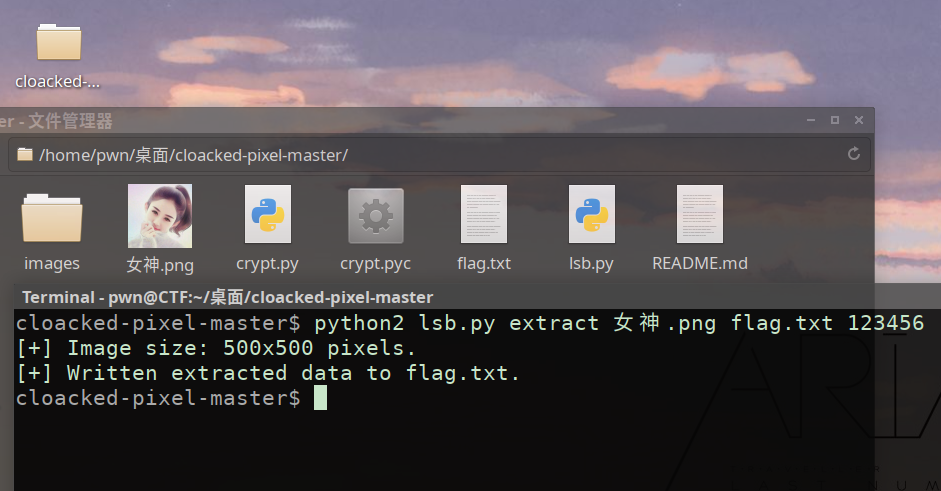


14.LSB隐写:

图片文件放在Xubuntu中的cloacked-pixel-master中，在这个文件夹打开cmd输入：

python2 lsb.py extract 图片名 输出文件名 密码

即可得到输出文件并查看信息



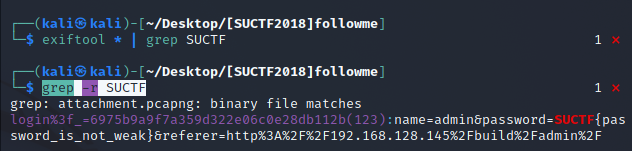
15.Exiftool多文件内容查找:

在文件夹中打开命令行输入：

exiftool \* | grep 查找的字符串



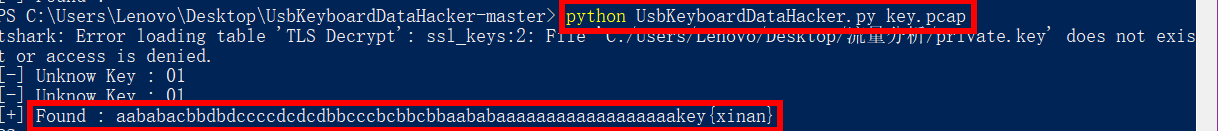
如果没有就grep -r 查找的字符串



16.USB隐写:

将流量包放到UsbKeyboardDataHacker文件夹中，文件夹中打开命令行输入：

python UsbKeyboardDataHacker.py 流量包名



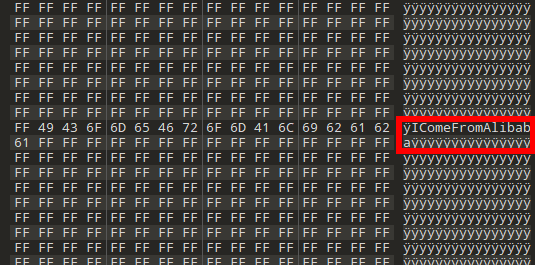
17.DOC隐写:

#### （一）隐藏内容

全选变色

#### （二）修复

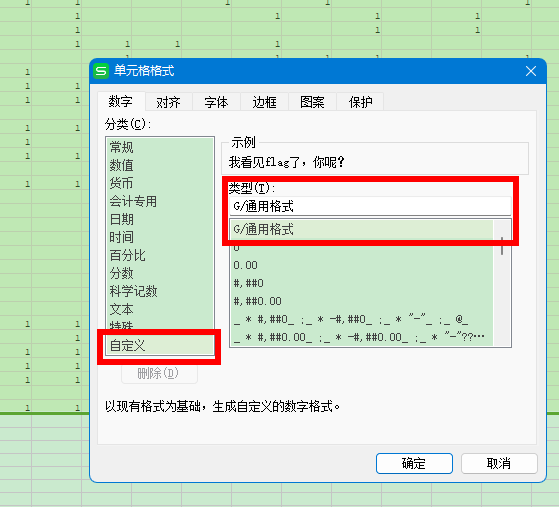
类似：



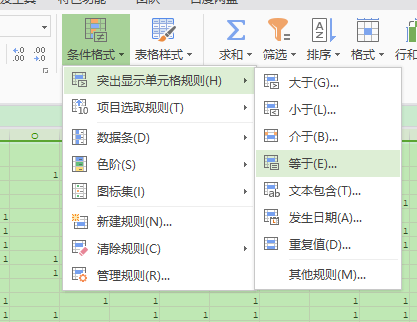
将这里改为相同的16进制FF即可

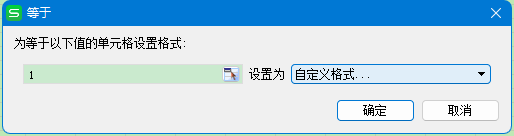
18.Excel隐写

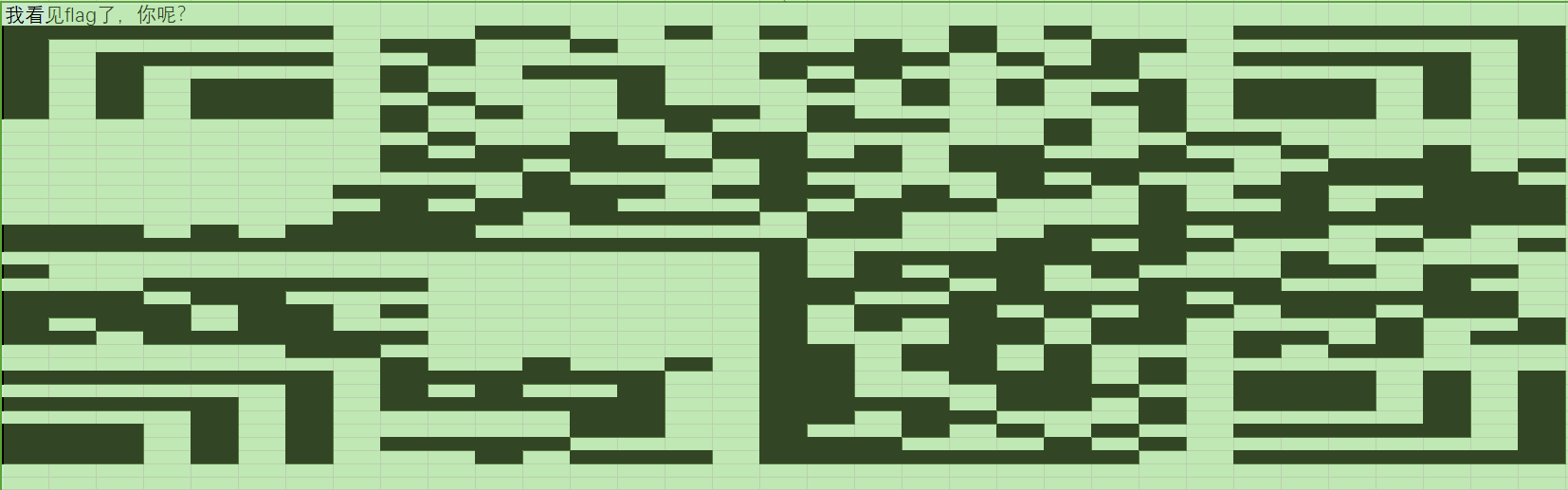
全选设置单元格格式为自定义->G/通用格式



条件格式->突出显示单元格规则->等于->输入值和颜色，突出显示转换为图案

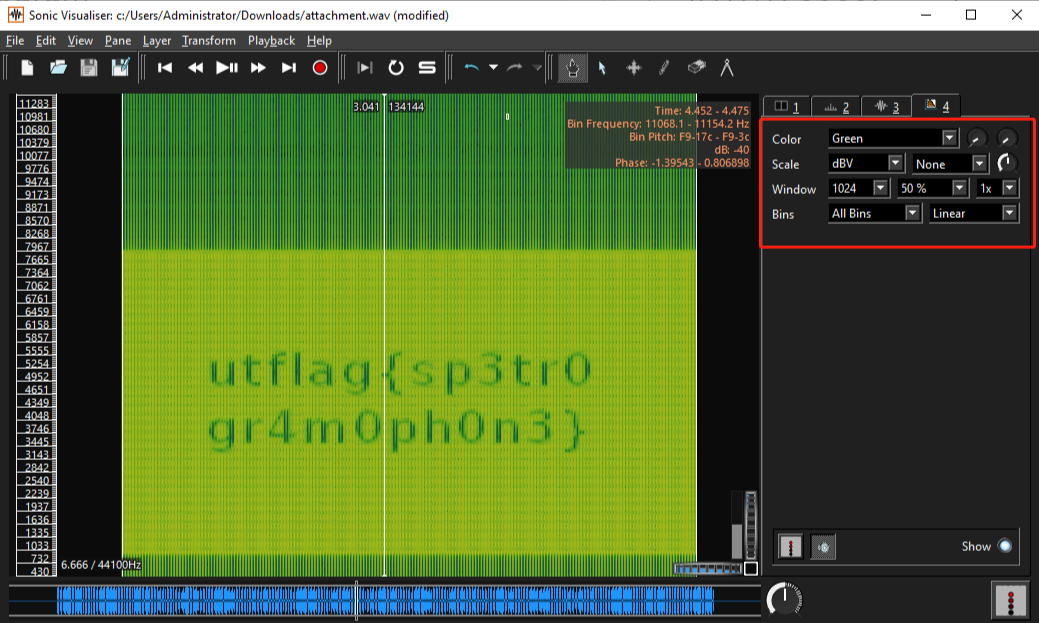






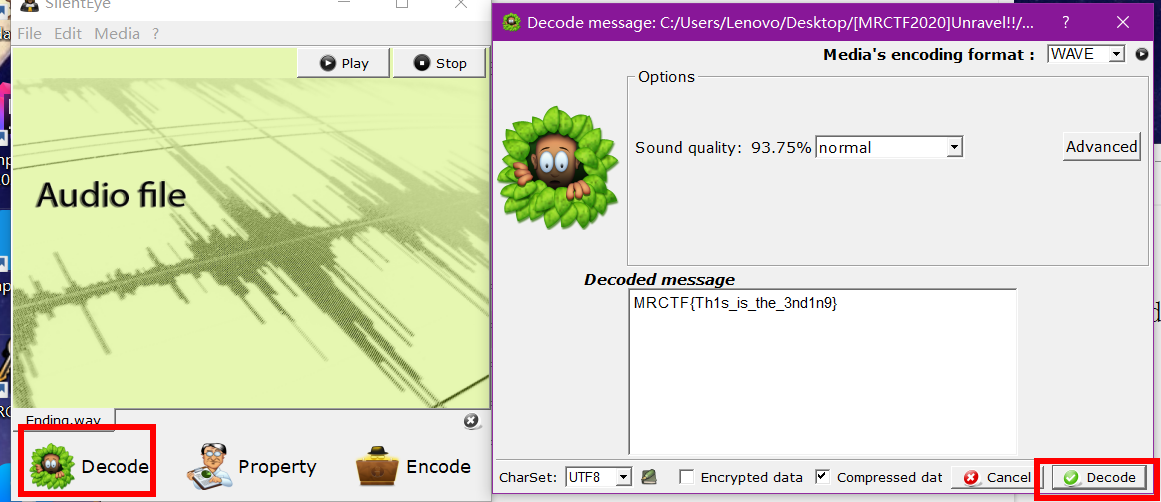
19.SonicVisualiser

打开音频文件，Layer->Add Peak Frequency Spectrogram或者Shift+K，做如下调整可以看到隐藏信息



20.SlientEye

打开音频软件，点击Decode->Decode可以解密隐写内容



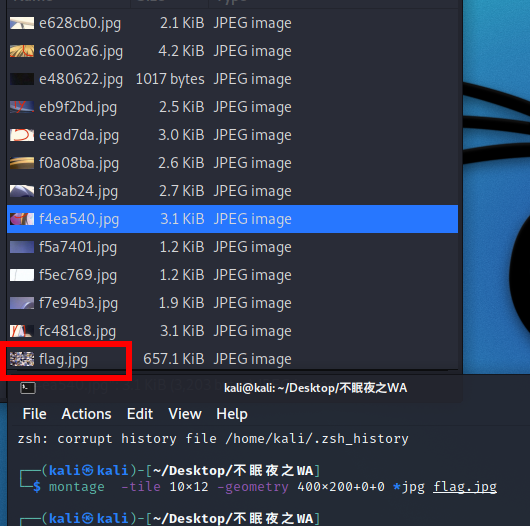
21.Montage

合成多个图片为一张图，在拼图文件夹cmd运行montage -tile 长x宽 -geometry 400x200+0+0 \*图片格式 输出文件名

-geometry +0+0的用处是让图片之间没有间隙

tile后是从左往右张数x从上往下张数（宽的图片数x长的图片数）

\*.jpg指目标为目录下所有的jpg格式图片



21.Gaps

将一张图片正常拼图，图片放在gaps/bin文件夹，打开cmd运行：python gaps --image=图片名 --generations=40 --population=120 --size=宽度像素值

–image 指向拼图的路径

–size 拼图块的像素尺寸

–generations 遗传算法的代的数量

–population 个体数量

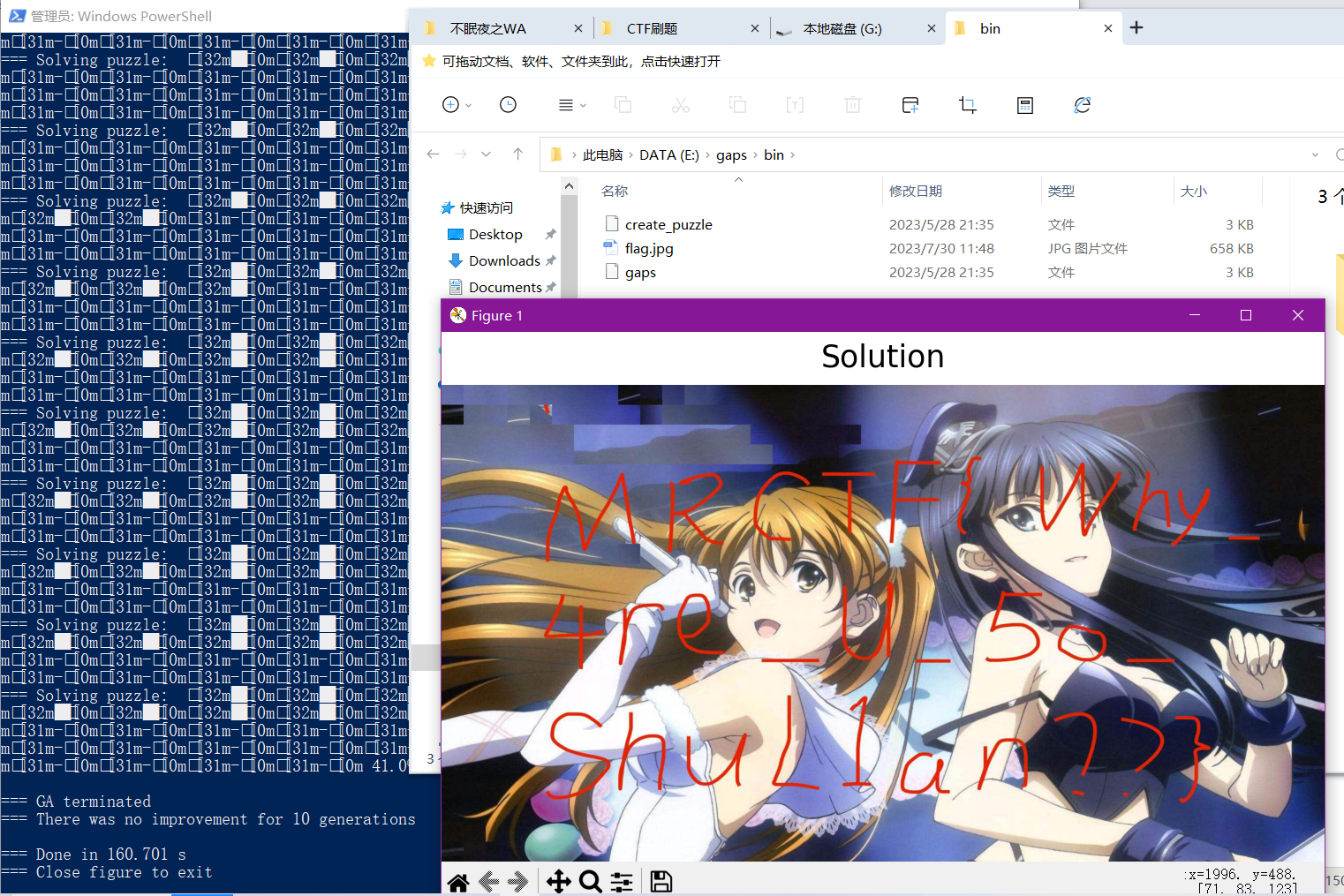
–verbose 每一代训练结束后展示最佳结果

–save 将拼图还原为图像

“–size”这个参数是最关键的，程序会根据这个选项设置的参数来判断piece的数量，值为宽度的像素值





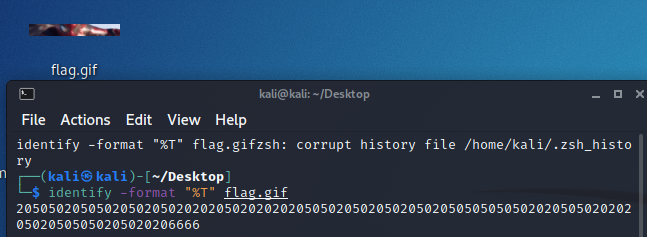


21.TXT去除重复行

用notepad打开，全选后编辑->行操作->删除重复行

22.时间隐写

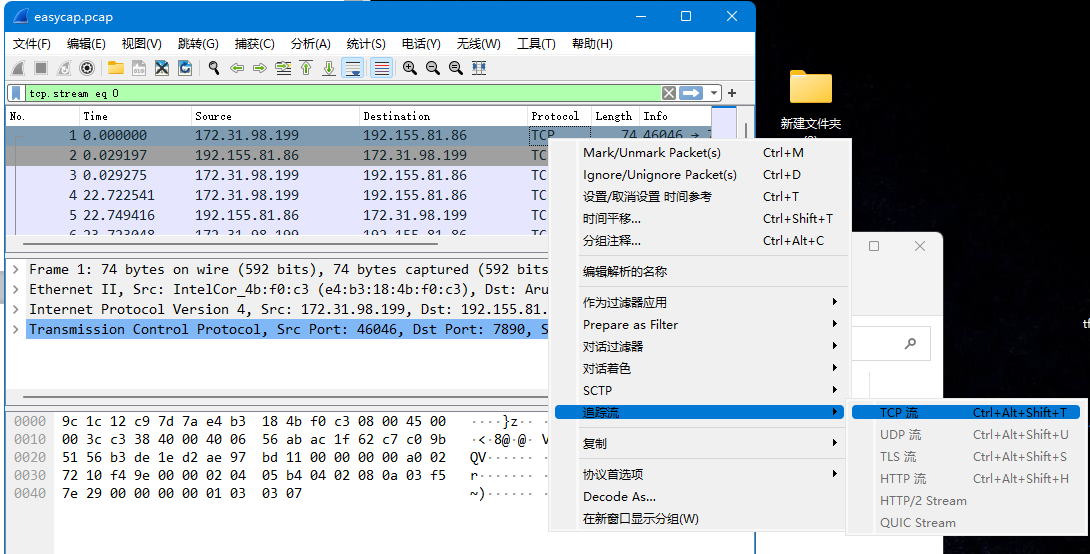
cmd输入：identify -format "%T" 动图文件名



## 二.流量

1.length排序

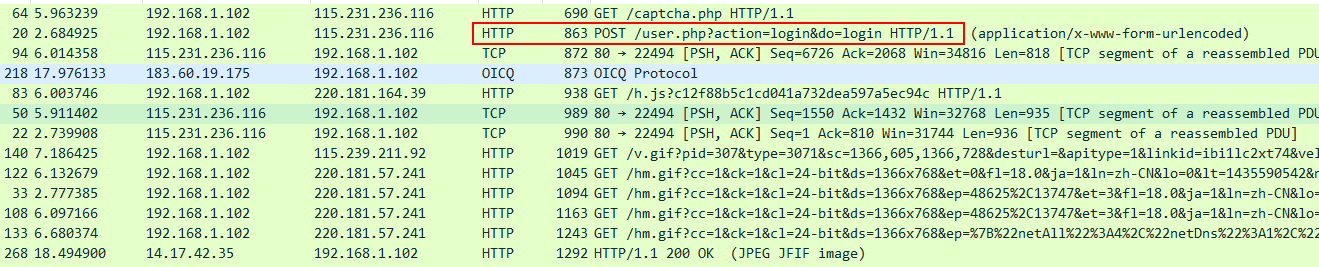
一般有数据的length会比较大，追踪TCP流:



2.搜索内容

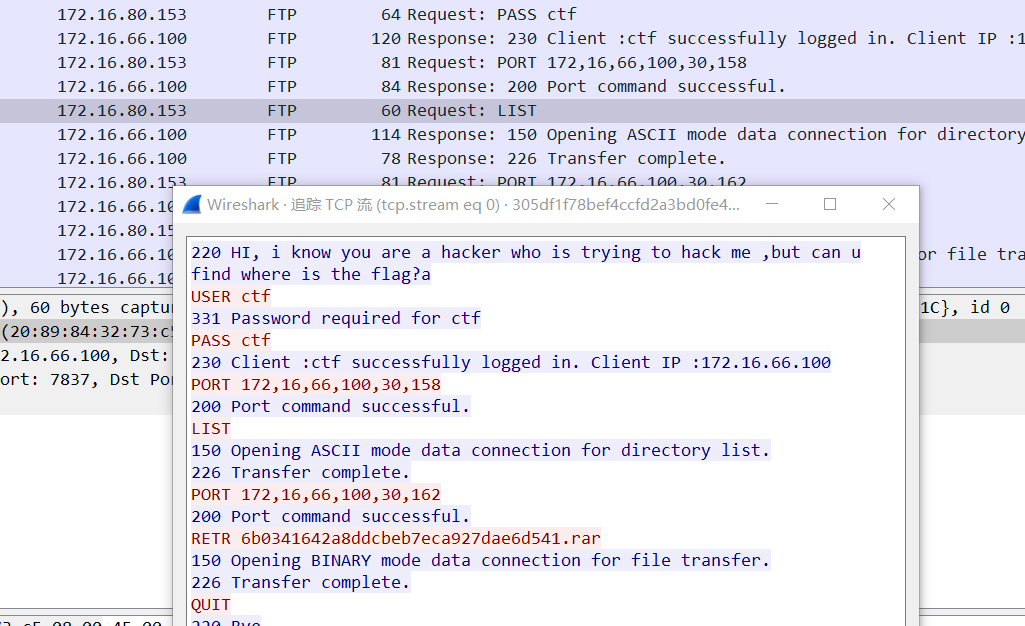
tcp contains "搜索字符串"

搜索flag字段，或者查找一些有用的内容。在过滤流时，一些网页登录信息等要尤其注意，很可能藏有数据



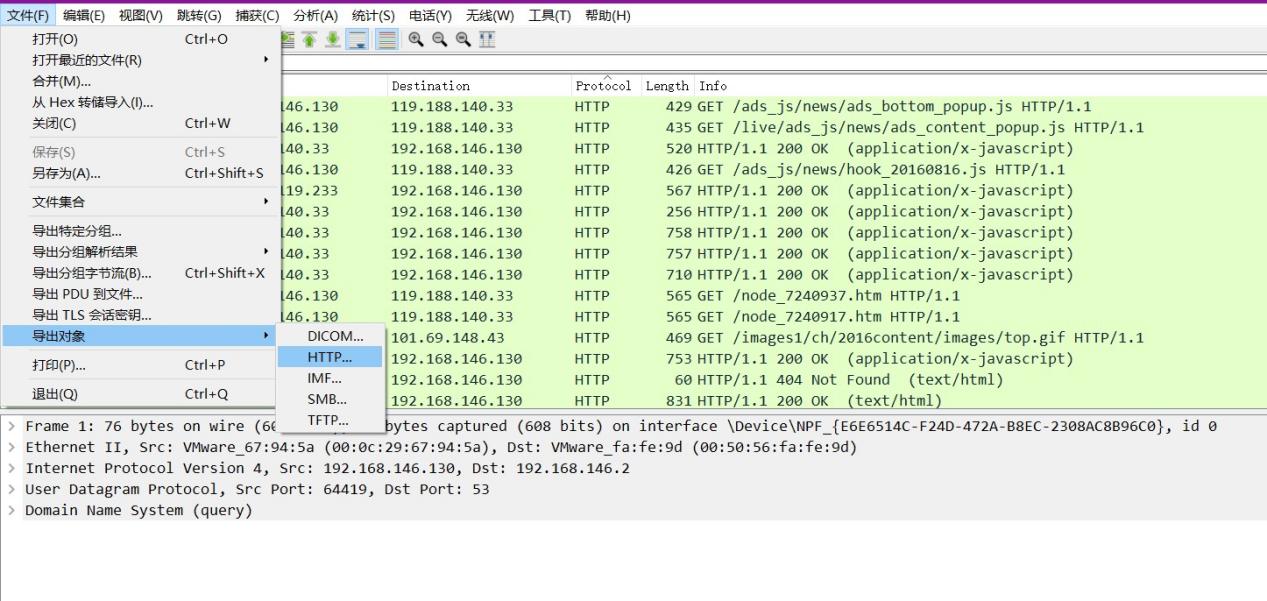
3.ftp协议

注意ftp协议，可能会有信息



4.HTTP流导出文件

当遇到HTTP流时，可以通过文件->导出对象->HTTP...选项，选择导出文件夹，提取所有HHTP流包含文件到当前文件夹中

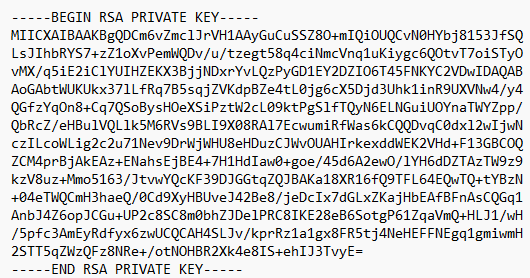


5.搜索流

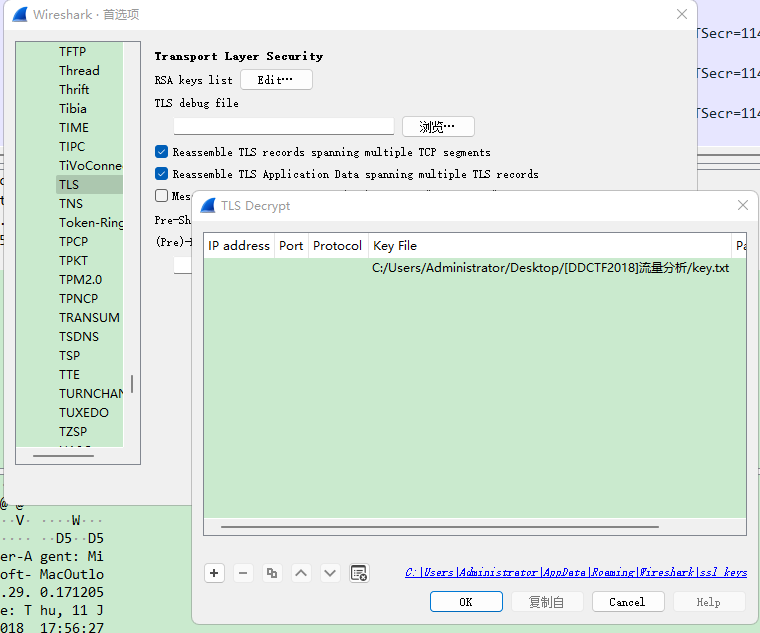
追踪tcp流：tcp.stream eq 114

6.SSL秘钥

类似这种格式：



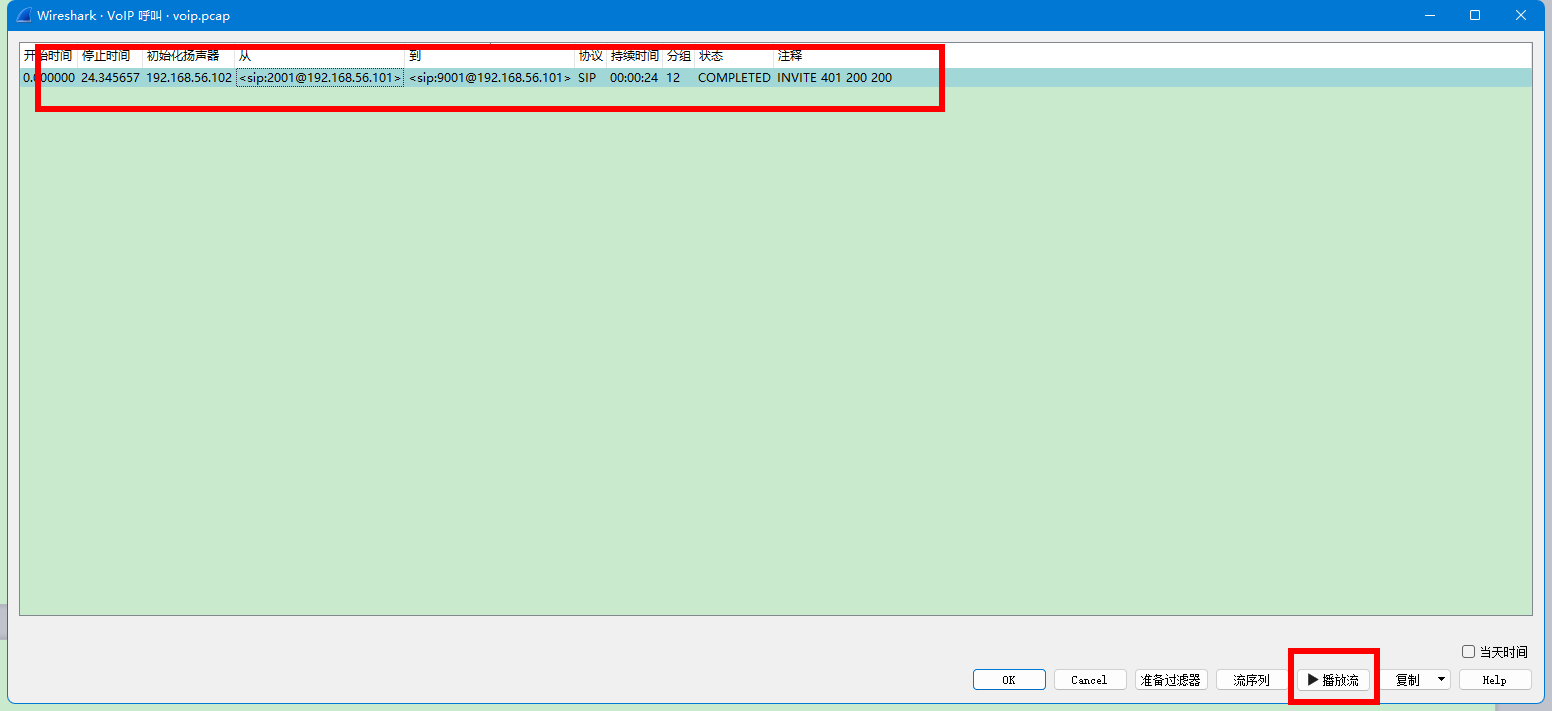
编辑->首选项->Protocols->TLS->Edit...->选择对应key文件保存，关闭后重新打开才会生效

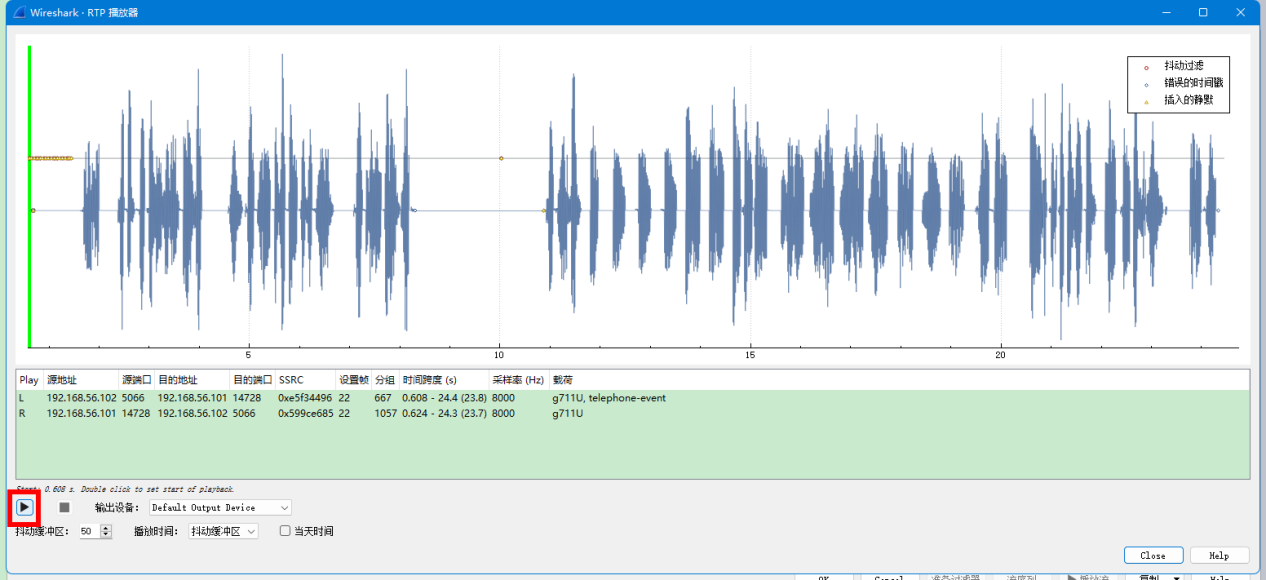


7.Voip通话

使用sonic-visualiser-4.5.2-win64打开音频文件，电话->voip通话->选中音频->播放流->点击播放按钮

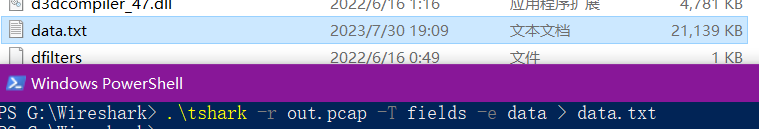






8.内容导出

将流量包放到G:\Wireshark文件夹下，输入：.\tshark -r 流量包名 -T fields -e data > 导出文件名

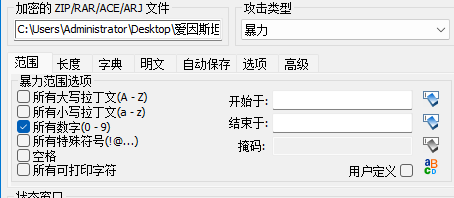


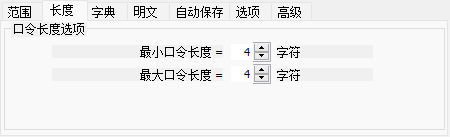
## **三.爆破**

常见的几种解决工具：

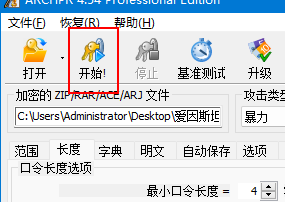
1.ARCHPR

文件直接拖进窗口就行，下面时一些常用可选配置：





点击开始进行爆破：



1. 注意有的文件压缩包打开时能看到，但是解压后就会自动消失
2. 掩码爆破

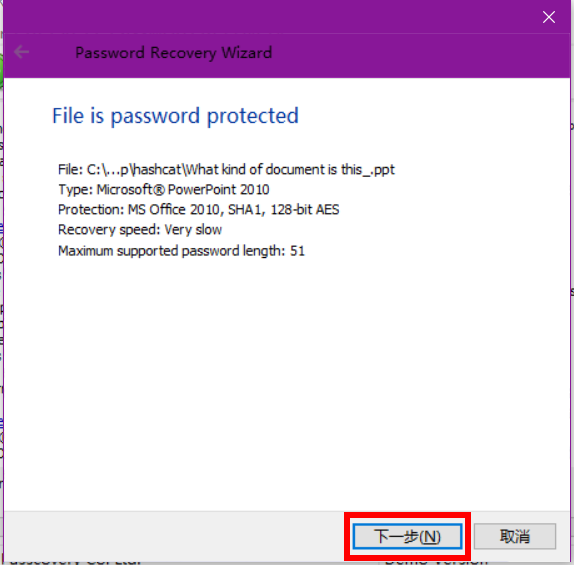
时间戳格式

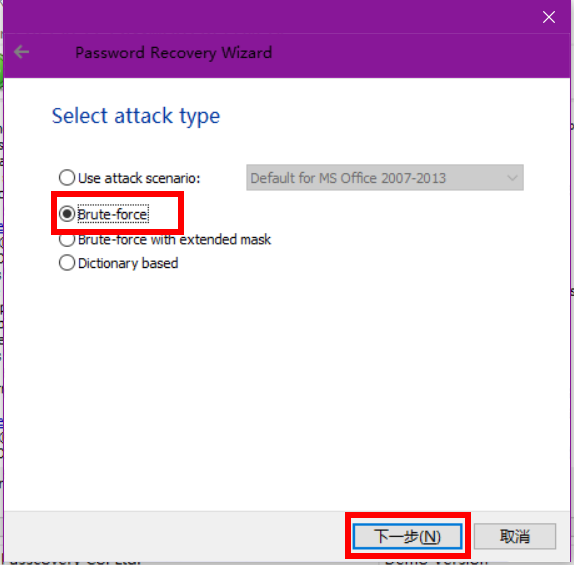


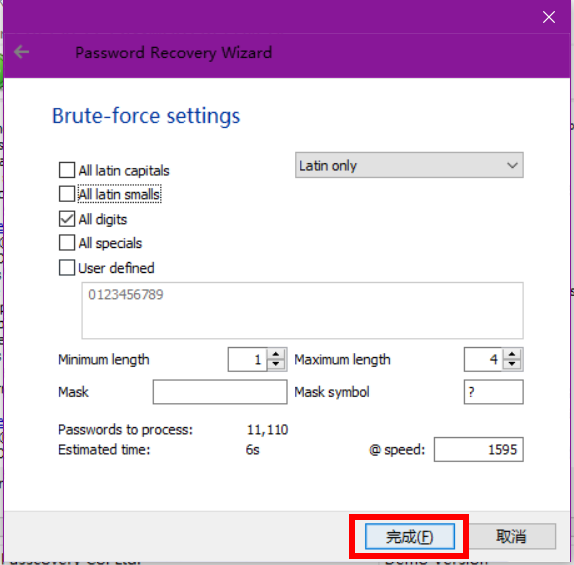


2.Accent EXCEL Password Recovery

打开加密文件后点击下一步，之后选择burp-force->下一步，之后根据需求选择后点击完成开始爆破



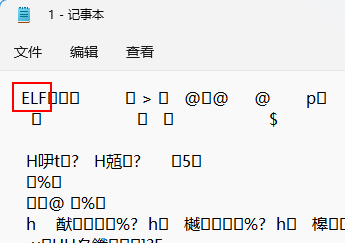


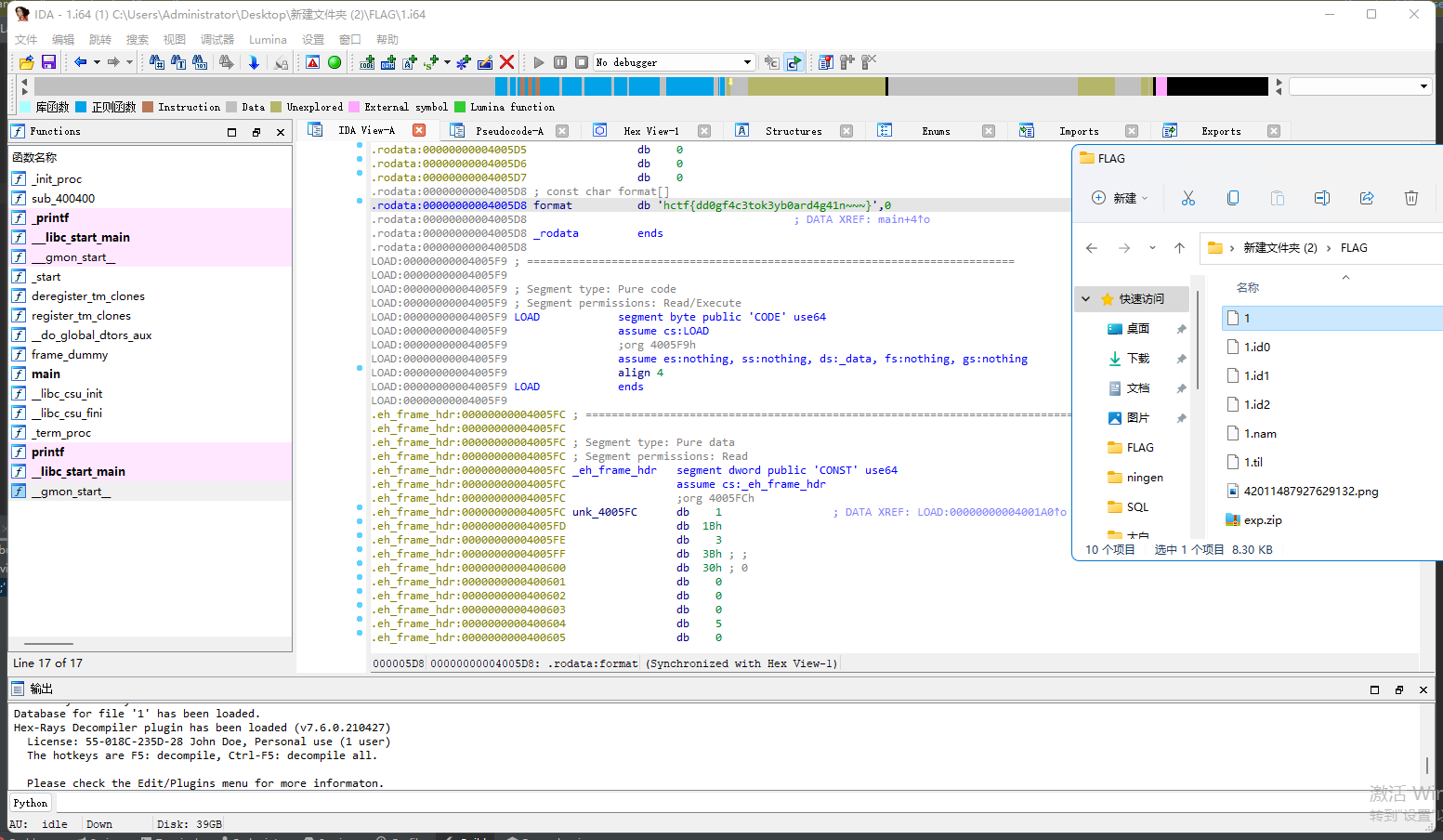


## **四.各种稀有文件格式**

1.文件没有后缀名

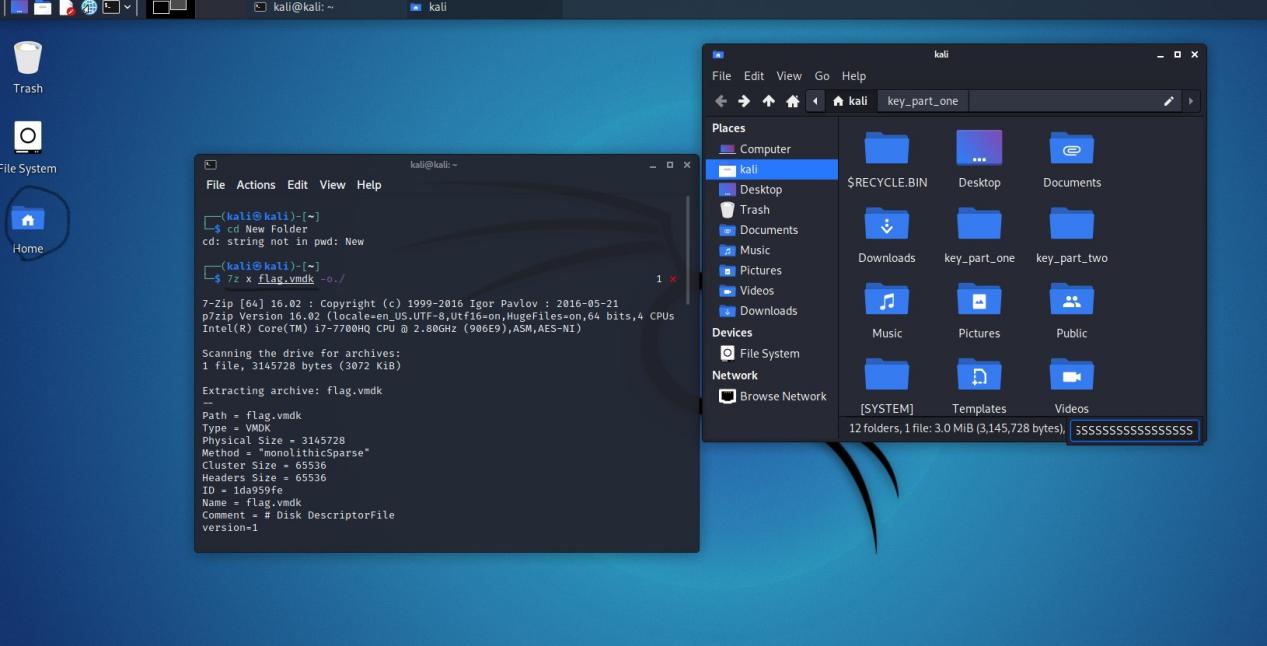
文件打不开的话，右键用记事本打开，如果头部是ELF，那么使用IDA打开即可





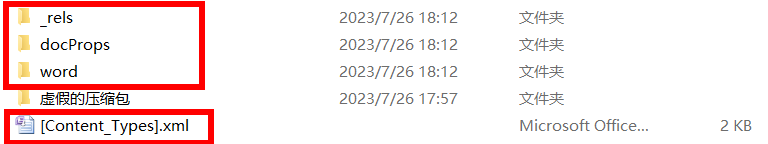
2.VMDK文件

这是虚拟机的压缩文件，只能用Linux查看，如果Windows解压可能会缺少文件，将文件放到桌面根目录下即可，Linux解压指令：7z x 文件名 -o./



3.DOC文件源文件夹

如果压缩包解压出这样的结构，直接将压缩包改名为doc



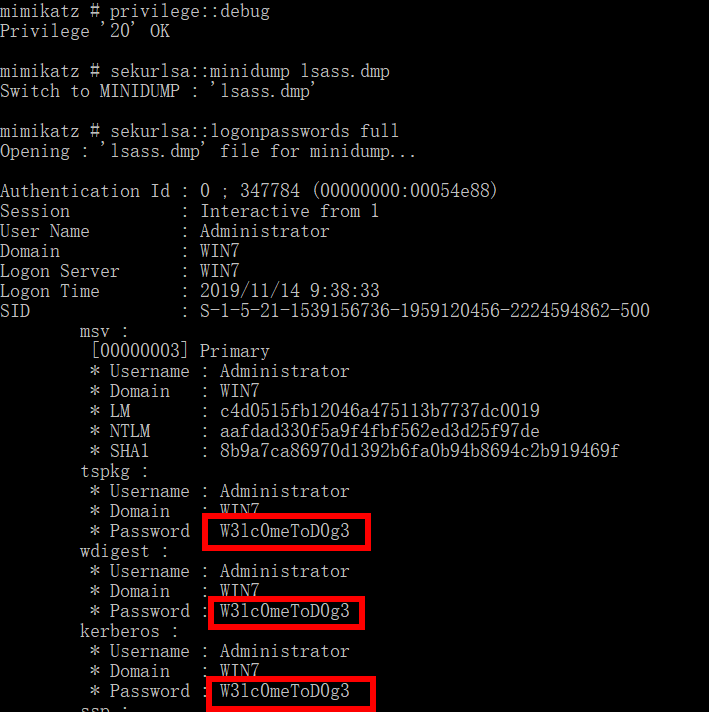
4.Issas.dmp

如果遇到lsass.dmp文件，lsass是windows系统的一个进程，用于本地安全和登陆策略。mimikatz可以从 lsass.exe 里获取windows处于active状态账号明文密码。本题的lsass.dmp就是内存运行的镜像，也可以提取到账户密码。将lsass.dmp放到x64文件夹下，也就是mimikatz.exe同级目录中，**管理员**启动mimikatz.exe，分别执行以下指令得到用户信息：

//提升权限 privilege::debug

//载入dmp文件 sekurlsa::minidump lsass.dmp

//读取登陆密码 sekurlsa::logonpasswords full



5.Bpg文件

bpg格式图片拖到bpgview.exe中查看结果



