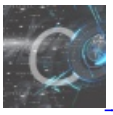
MISC隐写——图片

原创

沉迷二进制 于 2020-04-14 18:50:00 发布 772 收藏 7

分类专栏： 图片隐写

本文链接：https://blog.csdn.net/weixin_46148324/article/details/105388209



图片隐写 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

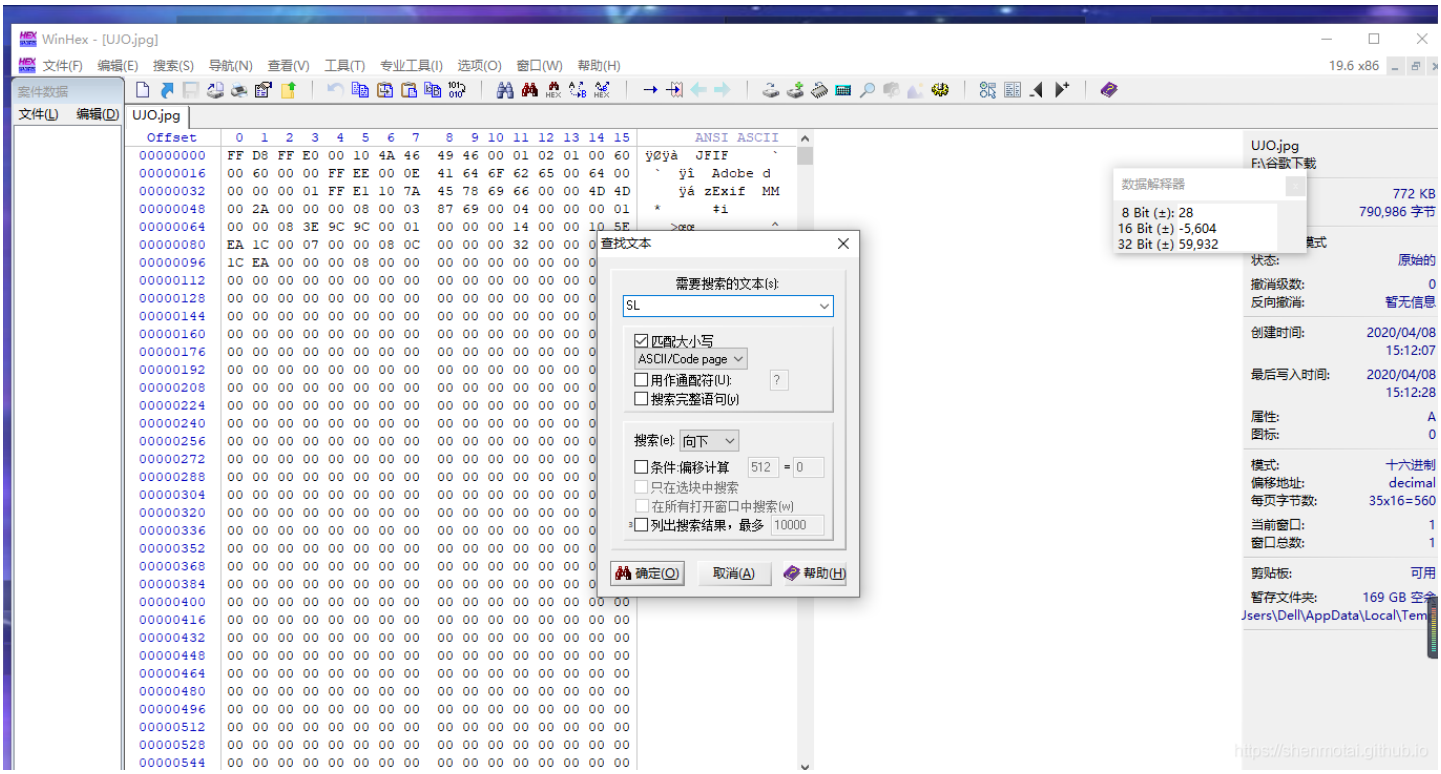
1、图片属性

没错上面是错误的示范，我居然憨憨的不知道看详细信息，我太菜了，hhh。

下面是正确的图片属性查看

2、flag隐藏在字节中，我们可以通过搜索关键字来找到

将文件拖到winhex中，用搜索文本flag开头**SL**



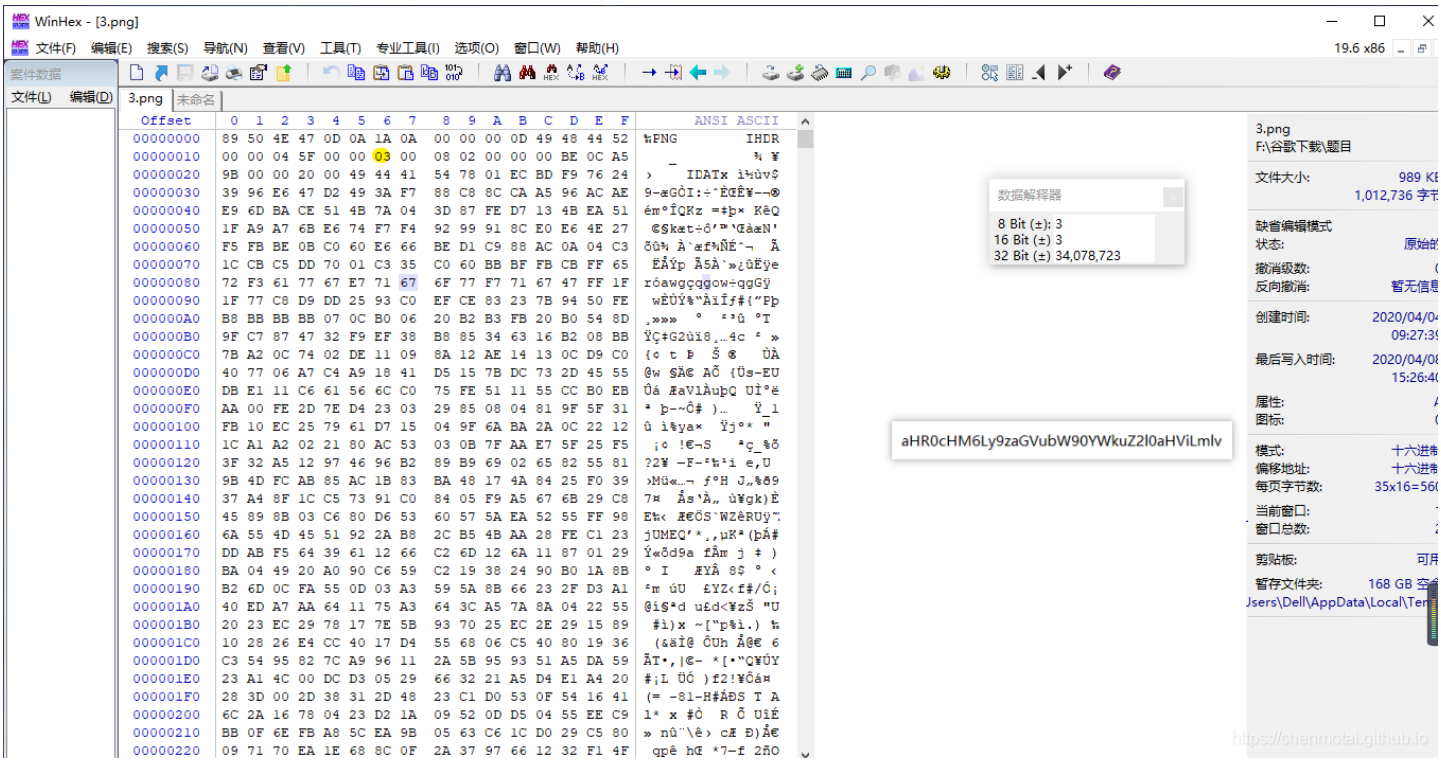
找到了（从开始向下搜索了好几次找到了）：

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00551776	64	C4	0E	B4	6A	F5	72	CB	81	D9	EB	DF	4E	EC	30	AD	dÄ ´jõrË ÙëßNì0-
00551792	66	F6	E3	40	09	A7	48	19	56	D6	82	72	6F	05	DD	BE	föã@ §H VÖ‚ro Ý¾
00551808	8C	11	A3	E9	07	73	DB	3F	10	A4	C6	7C	69	95	A2	B9	Œ £é sÛ? ¤Æ|i•¢¹
00551824	F9	B8	BB	CF	49	EC	D5	5B	C9	A7	7B	69	05	BB	D3	84	ù¸»ÏIìÕ[É§{i »Ó„
00551840	50	A8	73	64	56	BB	A0	1D	37	FE	69	19	68	2F	B6	B9	P¨sdV» 7þi h/¶¹
00551856	86	70	6D	5C	E4	98	38	B6	B3	03	28	19	17	51	C8	77	†pm\ä˜8¶³ (QÈw
00551872	67	AA	50	3E	9A	29	AE	6A	07	BA	8E	96	E2	55	10	B6	gªP>š)®j °Ž–âU ¶
00551888	5E	C4	16	D5	A0	EB	A1	AC	BB	CF	A0	34	58	AB	6F	FD	^Ä Õ ë¡¬»Ï 4X«oý
00551904	88	62	CF	03	4F	7C	AB	5C	B6	B0	B1	75	D9	83	A1	D8	ˆbÏ O|«\¶°±uÙƒ¡Ø
00551920	F9	FF	00	EF	7F	48	E1	01	B6	E5	82	0D	33	5C	FF	00	ùÿ ï Há ¶å‚ 3\ÿ
00551936	F9	63	07	BE	60	1D	FC	F7	2E	0B	B4	39	1E	B0	1A	AE	ùc ¾` ü÷. ´9 ° ®
00551952	CC	87	DE	26	1A	CD	5D	9A	F1	55	53	4C	7B	69	61	6D	Ì‡Þ& Í]šñUSL{iam
00551968	66	6C	61	67	7D	B3	53	23	AE	4C	5D	15	28	46	76	76	flag}³S#®L] (Fvv
00551984	4E	4F	11	6F	04	65	CB	F1	B5	2D	1A	D0	F1	74	4F	01	NO o eËñµ- ÐñtO
00552000	91	2E	5C	11	A3	FC	80	DC	AE	DA	7F	62	1D	1B	F2	DC	'.\ £ü€Ü®Ú b òÜ
00552016	B9	70	78	61	CA	5D	F8	0D	23	AD	23	18	22	B6	3A	DA	¹pxaÊ]ø #-# "¶:Ú
00552032	A3	5C	11	C9	01	FA	35	E7	7C	E5	3A	EF	B4	16	B6	46	£\ É ú5ç|å:ï´ ¶F
00552048	FD	AC	22	F0	BA	53	49	3C	05	CA	52	46	B8	32	63	15	ý¬"ðºSI< ÊRF¸2c
00552064	00	BA	05	86	6F	34	AD	19	0B	34	EB	02	80	71	D2	52	º †o4- 4ë €qÒR
00552080	68	31	C1	0B	11	11	D1	1C	27	A9	29	C5	DB	B6	52	CF	h1Á Ñ '©)ÅÛ¶RÏ
00552096	73	3D	61	89	61	20	0A	85	46	0D	B1	DC	D5	98	C9	DE	s=a‰a …F ±ÜÕ˜ÉÞ
00552112	1F	47	56	C9	60	5B	08	7E	C2	D5	66	20	41	CB	19	1B	GVÉ`[~ÂÕf AË
00552128	B4	AA	86	12	5B	62	52	52	91	12	20	32	CE	67	84	0F	´ª† [bRR‘ 2Îg„
00552144	99	5A	9A	A2	30	85	78	06	9B	69	F9	5B	51	24	4A	9A	™Zš¢0…x ›iù[Q$Jš
00552160	92	D0	AF	22	02	43	12	2A	E5	06	AD	36	8D	03	76	1C	’Ð¯" C *å -6 v
00552176	F8	23	24	B0	13	8A	16	D4	D3	88	C6	52	2C	55	D7	6B	ø#$° Š ÔÓˆÆR,U×k
00552192	67	35	80	D4	B9	C9	83	4C	B1	80	D9	81	28	AB	0B	7F	g5€Ô¹ÉƒL±€Ù («
00552208	66	E7	2B	0B	95	DC	75	C3	F0	B8	2F	A7	8C	95	22	DB	fç+ •ÜuÃð¸/§Œ•"Û
00552224	17	17	B0	26	4A	84	81	9C	2B	15	B3	D0	C7	51	88	80	°&J„ œ+ ³ÐÇQˆ€
00552240	89	76	B0	B6	A8	01	99	52	A6	48	1D	FE	20	1B	30	8E	‰v°¶¨ ™R¦H þ 0Ž
00552256	F0	28	E6	E0	DE	A4	B2	81	BD	67	55	62	22	89	08	13	ð(æàÞ¤² ½gUb"‰
00552272	71	93	6A	15	F6	B3	03	E4	29	42	BA	89	B5	C5	23	0B	q"j ö³ ä)Bº‰µÅ#
00552288	C9	B7	4A	C5	00	B9	18	B1	1B	70	A6	CA	1B	06	5D	8B	É·JÅ ¹ ± p¦Ê]‹
00552304	52	6A	F5	0E	EB	35	73	41	67	50	D6	1D	4E	67	53	37	Rjõ ë5sAgPÖ NgS7
00552320	09	04	4C	6C	A0	12	53	6A	9A	DA	C4	32	CB	82	43	45	Ll SjšÚÄ2Ë‚CE

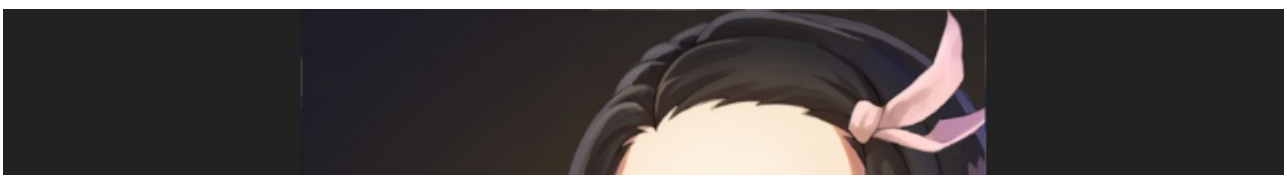
修改png图片的高

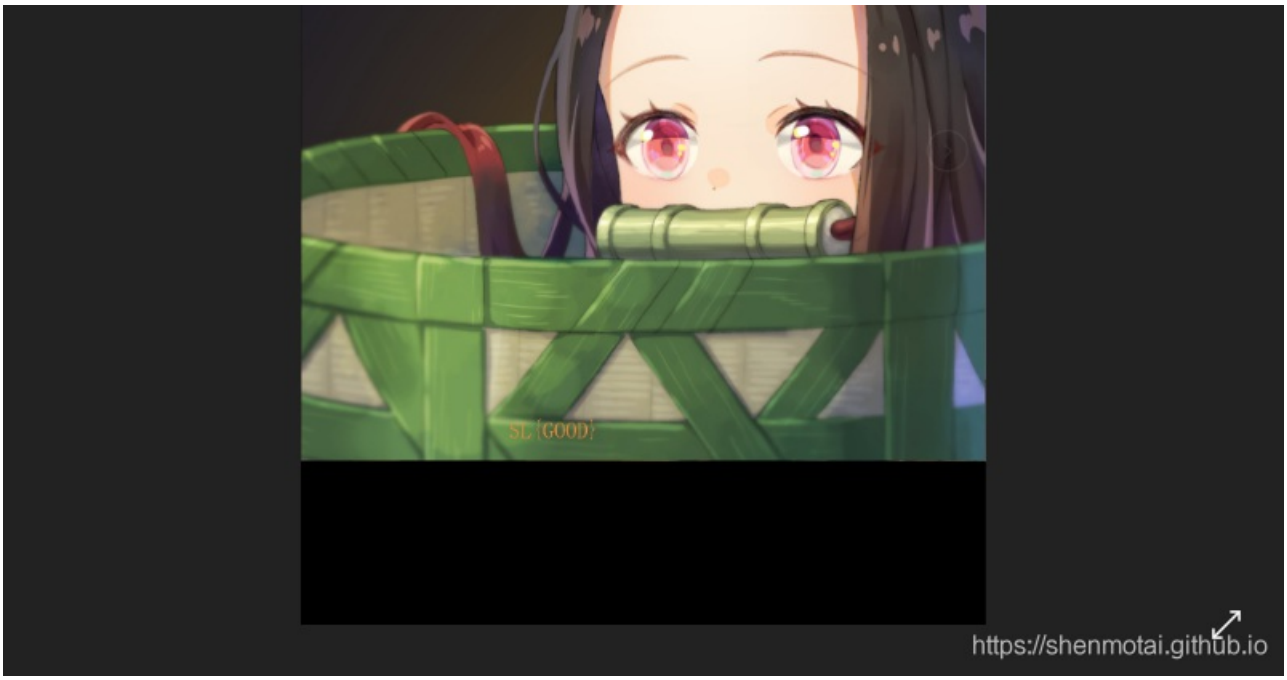
可爱的小姐姐，哈哈哈

将图片拖进winhex，将黄色标记的值修改的大一点，改成**5**，保存



得到flag：



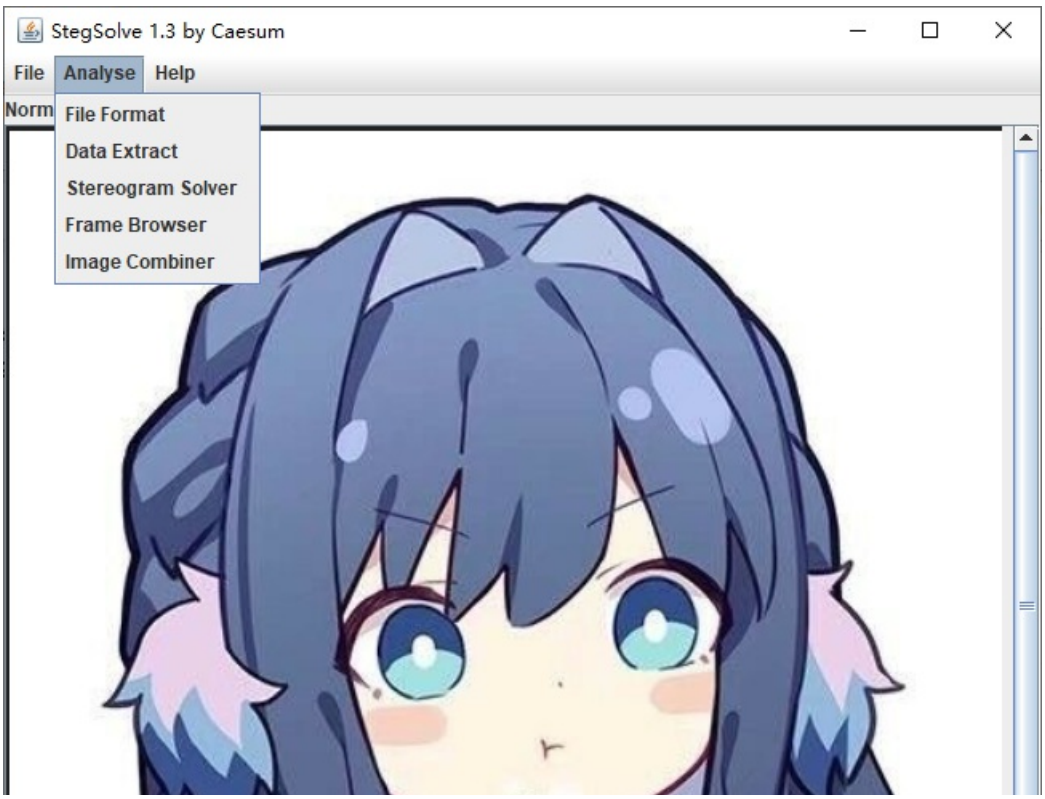


识别常见的文件开头和结尾，并进行添加剪切或保存

JPEG (jpg)， 文件头：FFD8FF 文件尾：FF D9
PNG (png)， 文件头：89504E47 文件尾：AE 42 60 82
GIF (gif)， 文件头：47494638 文件尾：00 3B
ZIP Archive (zip)， 文件头：504B0304 文件尾：50 4B
RAR Archive (rar)， 文件头：52617221
可以在winhex中进行操作，多练些题就能熟练掌握：

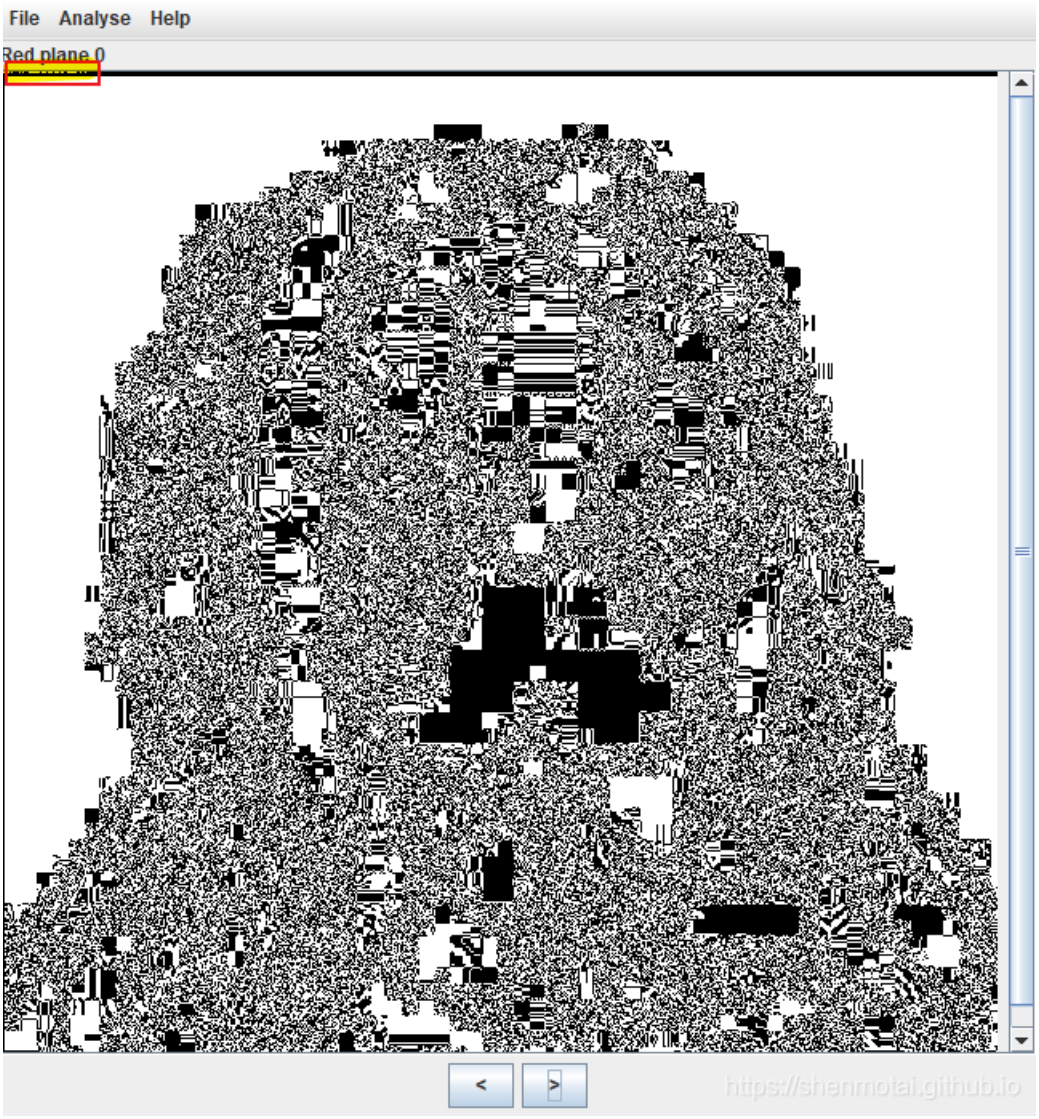
LSB隐写

需要用到工具**Stegsolve.jar**
用Stegsolve.jar打开图片



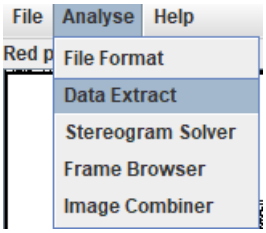
File Format:文件格式，这个主要是查看图片的具体信息
Data Extract:数据抽取，图片中隐藏数据的抽取
Steregram Solve:立体试图 可以左右控制偏移
Frame Browser:帧浏览器，主要是对GIF之类的动图进行分解，动图变成一张张图片，便于查看
Image Combiner:拼图，图片拼接
这一题简单如图

直接按下面的按钮切换

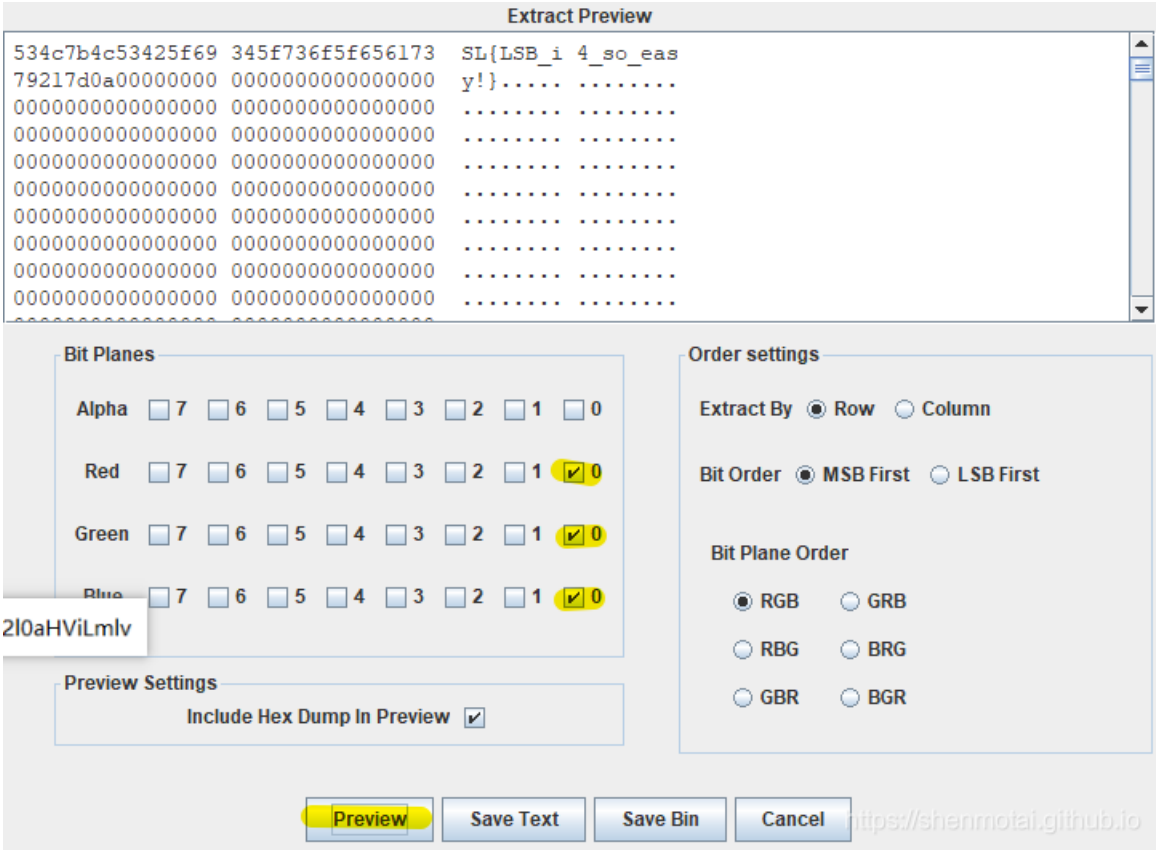


然后会发现左上角隐藏着什么东西，多往后切还会出现几张类似现象

然后进行如下操作：



将出现上述现象的图片勾选上得出隐藏信息



使用outguess工具

我是在我的kali虚拟机中下载的，下载kali具体步骤可以看我兄弟博客：https://blog.csdn.net/qq_45836474/article/details/104977042

输入如下代码下载：

```
1、sudo git clone https://github.com/crorvick/outguess #下载安装包到当前目录
2、sudo ./configure && sudo make && sudo make install #在当前目录下安装
```

使用方法详见大佬博客：https://blog.csdn.net/xuqi7/article/details/63362839/

内容如下：

加密：

outguess -k “my secret key” -d flag.txt demo.jpg out.jpg

加密之后，demo.jpg会覆盖out.jpg,

flag.txt中的内容是要隐藏的东西

解密：

outguess -k “my secret key” -r out.jpg hidden.txt

解密之后，解密内容放在hidden.txt中

F5-steganography工具的使用

kali中输入下载

```
sudo git clone https://github.com/matthewgao/F5-steganography
```

使用：

```
java Extract 图片的绝对路径/123.jpg -p 密码
```

然后打开output.txt文件查看flag

拼图

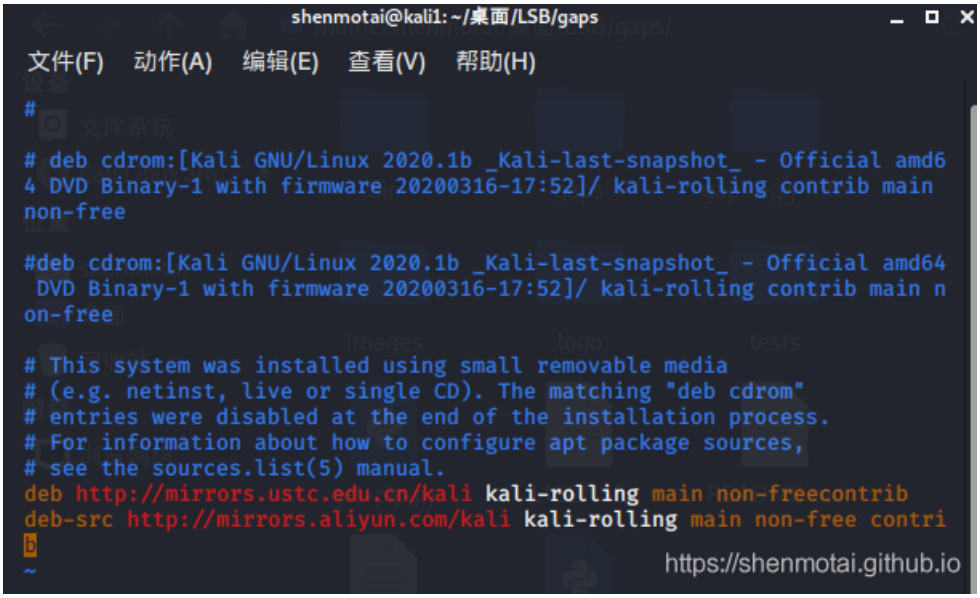
ImageMagick工具和gaps工具联合使用

重新建的虚拟机开始到入狱

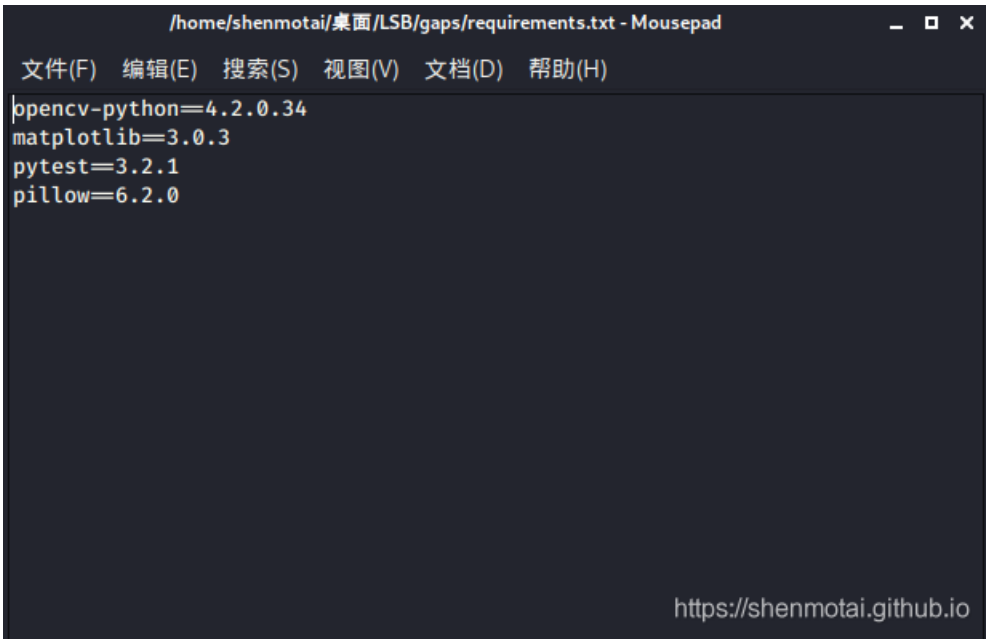
下载：

```
#先下载gaps保证不出意外
1、sudo vi /etc/apt/sources.list #添加阿里源
2、sudo apt-get update
3、sudo git clone https://github.com/nemanja-m/gaps.git #下载gaps
4、cd gaps #进入gaps文件夹
5、sudo wget https://bootstrap.pypa.io/get-pip.py #下载pip
6、sudo python3 get-pip.py #可能会因为网速下载失败，重启一下
7、sudo vi /etc/pip.conf #配置pip.conf文件
8、sudo pip install opencv-python==4.2.0.34 #更新opencv-python
9、sudo vi ./requirements.txt #修改requirements.txt文本文件
10、sudo pip install -r requirements.txt
11、sudo apt install python3-tk
12、sudo pip install -e . #结束后gaps就能用了
sudo apt-get install imagemagick #下载imagemagick
```

第一条修改如下



第九条修改结果如下：



第七条配置文件内容如下：

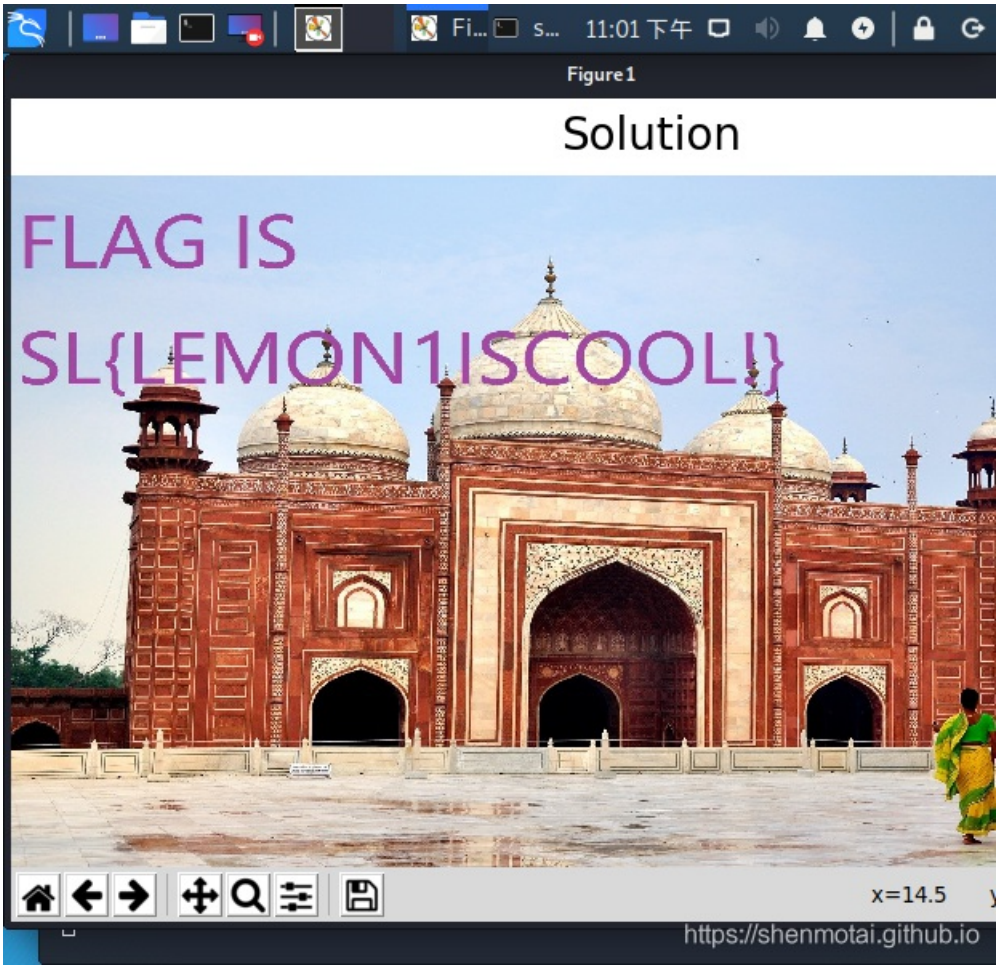
在文件夹里打开黑窗口输入：

```
montage *jpg -tile 10x12 -geometry 200x100+0+0 out.jpg
```

得到一张拼接后的图片：

使用gaps命令：

```
gaps --image=out.jpg --generations=40 --population=120 --size=100
```



使用steghide工具

下载

```
sudo apt-get install steghide
```

大佬博客：http://www.safe6.cn/article/102
查看图片中嵌入的文件信息

```
steghide info 1.jpg
```

提取图片中隐藏内容(有密码)

```
steghide extract -sf 1.jpg -p 密码
```

将1.txt文件隐藏到a.jpg中

```
steghide embed -cf a.jpg -ef 1.txt -p 密码
```

使用binwalk文件分离

kali自带，不用下载。
参考大佬博客：https://www.cnblogs.com/jiaxinguoguo/p/7351202.html

```
sudo binwalk cat.jpg
```

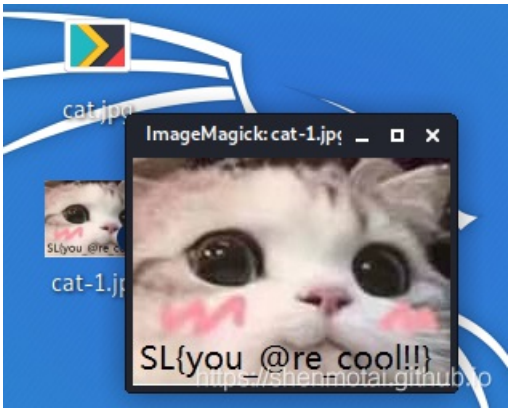
```
shenmotai@kali1:~/桌面$ sudo binwalk cat.jpg
[sudo] shenmotai 的密码：

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
5321          0x14C9          JPEG image data, JFIF standard 1.01
5351          0x14E7          TIFF image data, big-endian, offset of fi
st image directory: 8
```

很容易看出在5321和5351处有jpg图片，接下来取出他。

使用dd命令：

```
sudo dd if=cat.jpg of=cat-1.jpg skip=5321 bs=1
sudo dd if=cat.jpg of=cat-1.jpg skip=5521 bs=1
```

第一张



第二张（看来学长对ImageMagic执念很深啊，哈哈哈哈）

使用foremost工具分离

下载：

```
sudo apt-get install foremost
```

使用：

```
foremost cat.jpg
```

不知道为什么文件夹里没东西。。。可能是我脸黑吧。
还有几个工具有时间连上，偷懒+1