

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[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



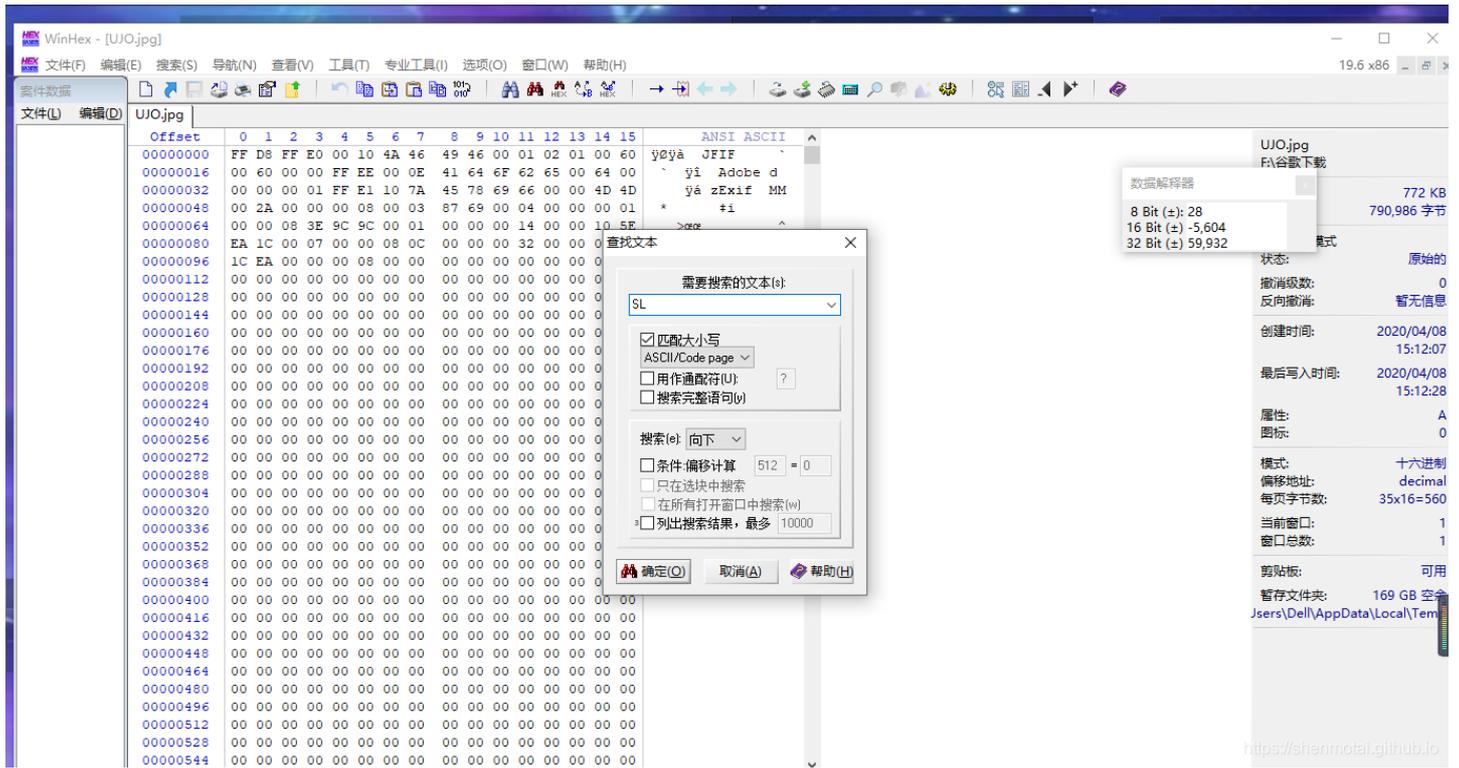
没错上面是错误的示范, 我居然憨憨的不知道看详细信息, 我太菜了, hhh。

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 'jörE ÜëBñi0-
00551792	66	F6	E3	40	09	A7	48	19	56	D6	82	72	6F	05	DD	BE	fðã@ \$H VÖ,ro Ý%
00551808	8C	11	A3	E9	07	73	DB	3F	10	A4	C6	7C	69	95	A2	B9	Œ éé sŰ? mÆ i·c³
00551824	F9	B8	BB	CF	49	EC	D5	5B	C9	A7	7B	69	05	BB	D3	84	ù,»IiìŒ[ÉS(i »Ó,,
00551840	50	A8	73	64	56	BB	A0	1D	37	FE	69	19	68	2F	B6	B9	F"sdV» 7pi h/Œ¹
00551856	86	70	6D	5C	E4	98	38	B6	B3	03	28	19	17	51	C8	77	tpm\ä"8Œ³ (QÈw
00551872	67	AA	50	3E	9A	29	AE	6A	07	BA	8E	96	E2	55	10	B6	g²P>š)@j oŽ-ãU Œ
00551888	5E	C4	16	D5	A0	EB	A1	AC	BB	CF	A0	34	58	AB	6F	FD	^Ä Œ ë;»I 4X«oy
00551904	88	62	CF	03	4F	7C	AB	5C	B6	B0	B1	75	D9	83	A1	D8	^bI Œ «\Œ°±uŒf;Œ
00551920	F9	FF	00	EF	7F	48	E1	01	B6	E5	82	0D	33	5C	FF	00	ùÿ i Há Œã, 3\ÿ
00551936	F9	63	07	BE	60	1D	FC	F7	2E	0B	B4	39	1E	B0	1A	AE	ùc %` ù±. '9 ° @
00551952	CC	87	DE	26	1A	CD	5D	9A	F1	55	53	4C	7B	69	61	6D	I±B& I]šñUSL(iam
00551968	66	6C	61	67	7D	B3	53	23	AE	4C	5D	15	28	46	76	76	flag]°S#ŒL] (Fvv
00551984	4E	4F	11	6F	04	65	CB	F1	B5	2D	1A	D0	F1	74	4F	01	NO o eÈñp- ðñtO
00552000	91	2E	5C	11	A3	FC	80	DC	AE	DA	7F	62	1D	1B	F2	DC	'\. ðüëÜšÜ b òÜ
00552016	B9	70	78	61	CA	5D	F8	0D	23	AD	23	18	22	B6	3A	DA	'pxaÈ]ø #-# "Œ:Ú
00552032	A3	5C	11	C9	01	FA	35	E7	7C	E5	3A	EF	B4	16	B6	46	É\ É ú5ç ã:i' ŒF
00552048	FD	AC	22	F0	BA	53	49	3C	05	CA	52	46	B8	32	63	15	ý-"š°SI< ÈRF,2c
00552064	00	BA	05	86	6F	34	AD	19	0B	34	EB	02	80	71	D2	52	° to4- 4ë €qŒR
00552080	68	31	C1	0B	11	11	D1	1C	27	A9	29	C5	DB	B6	52	CF	h1Á Ñ '(e)ÄŒŒRÍ
00552096	73	3D	61	89	61	20	0A	85	46	0D	B1	DC	D5	98	C9	DE	s=a&a ...F ±üŒ-ÉÈ
00552112	1F	47	56	C9	60	5B	08	7E	C2	D5	66	20	41	CB	19	1B	GVÉ`[~ÄŒf AE
00552128	B4	AA	86	12	5B	62	52	52	91	12	20	32	CE	67	84	0F	'±t [bRR' 2Ïg,,
00552144	99	5A	9A	A2	30	85	78	06	9B	69	F9	5B	51	24	4A	9A	"Zšc0...x >iù[QšJš
00552160	92	D0	AF	22	02	43	12	2A	E5	06	AD	36	8D	03	76	1C	'E" C *ã -6 v
00552176	F8	23	24	B0	13	8A	16	D4	D3	88	C6	52	2C	55	D7	6B	ø#š° Š ŒŒ-ÆR,U×k
00552192	67	35	80	D4	B9	C9	83	4C	B1	80	D9	81	28	AB	0B	7F	gšÈŒ-ÉfL±ëÜ («
00552208	66	E7	2B	0B	95	DC	75	C3	F0	B8	2F	A7	8C	95	22	DB	fç± ·ÜüÄš./šŒ·"Ü
00552224	17	17	B0	26	4A	84	81	9C	2B	15	B3	D0	C7	51	88	80	°&J,, α± 'ĐÇQ°È
00552240	89	76	B0	B6	A8	01	99	52	A6	48	1D	FE	20	1B	30	8E	%v°Œ" "R;H p ŒŽ
00552256	F0	28	E6	E0	DE	A4	B2	81	BD	67	55	62	22	89	08	13	š(æàš#æ %gÜb"%
00552272	71	93	6A	15	F6	B3	03	E4	29	42	BA	89	B5	C5	23	0B	q"j š' ä)B°%µÄ#
00552288	C9	B7	4A	C5	00	B9	18	B1	1B	70	A6	CA	1B	06	5D	8B	É·JÄ ' ± p È]<
00552304	52	6A	F5	0E	EB	35	73	41	67	50	D6	1D	4E	67	53	37	Rjž šš5sAgPŒ NgS7
00552320	09	04	4C	6C	A0	12	53	6A	9A	DA	C4	32	CB	82	43	45	L1 SjšÜÄ2È,CE

修改png图片的高



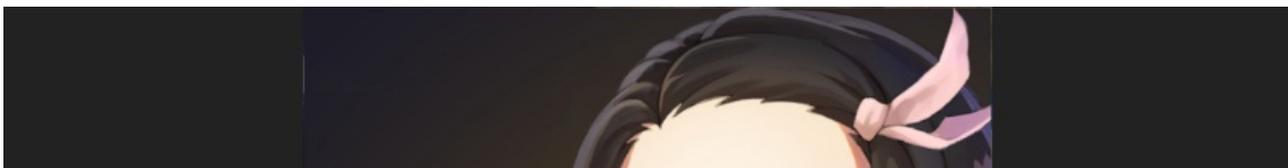
<https://shenmotai.github.io>

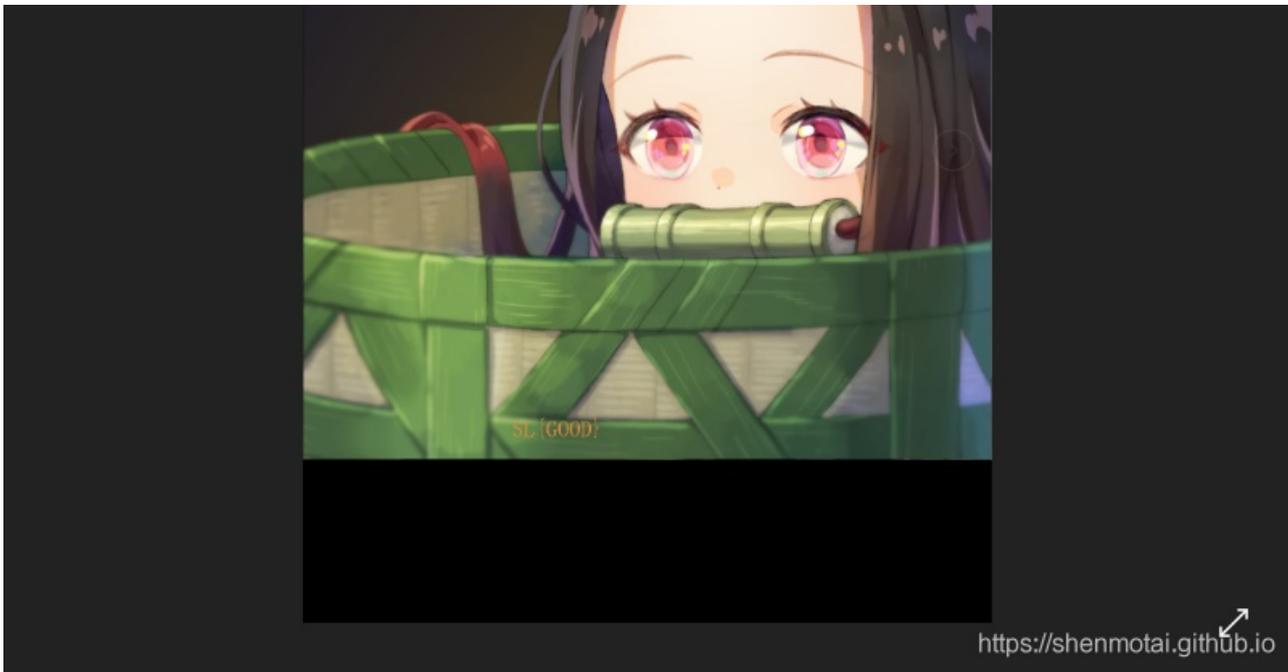
可爱的小姐姐，哈哈

将图片拖进winhex，将黄色标记的值修改的大一点，改成5，保存

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%FNG IHDR
00000010	00	00	04	5F	00	00	03	00	08	02	00	00	00	BE	0C	A5	- IDATx i4uv\$
00000020	9B	00	00	20	00	49	44	41	54	78	01	EC	BD	F9	76	24	> -gOI:-'EGEY--@
00000030	39	96	E6	47	D2	49	3A	F7	88	C8	8C	CA	A5	96	AC	AE	9-@IQKz =+p> K@Q
00000040	E9	6D	BA	CE	51	4B	7A	04	3D	87	FE	D7	13	4B	EA	51	em@IQKz =+p> K@Q
00000050	1F	A9	A7	6B	E6	74	F7	F4	92	99	91	8C	E0	E6	4E	27	@\$kac-@'*(@aN'
00000060	F5	FB	BE	0B	0C	60	E6	66	BE	D1	C9	88	AC	0A	04	C3	00% à#f%NÉ'- Á
00000070	1C	CB	C5	DD	70	01	C3	35	C0	60	BB	BF	FB	CB	FF	65	EÁYp ÁSA'»i0EYe
00000080	72	F3	61	77	67	E7	71	67	6F	77	F7	71	67	47	FF	1F	r0awgqggow+qgGy
00000090	1F	77	C8	D9	DD	25	93	C0	EF	CE	83	23	7B	94	50	FE	wEÜY%ÁiIf#('Fp
000000A0	B8	BB	BB	BB	07	0C	B0	06	20	B2	B3	FB	20	B0	54	8D	,»»» ° '»ú 'I
000000B0	9F	C7	87	47	32	F9	EF	38	B8	85	34	63	16	B2	08	BB	YÇ+G2úis...4c « »
000000C0	7B	A2	0C	74	02	DE	11	09	8A	12	AE	14	13	0C	D9	C0	{e t b š @ ÚÀ
000000D0	40	77	06	A7	C4	A9	18	41	D5	15	7B	DC	73	2D	45	55	@w šÁe Áó {Üs-EU
000000E0	DB	E1	11	C6	61	56	6C	C0	75	FE	51	11	55	CC	B0	EB	Üá zaVlÁupQ UI*é
000000F0	AA	00	FE	2D	7E	D4	23	03	29	85	08	04	81	9F	5F	31	* p--0#)... Ÿ_l
00000100	FB	10	EC	25	79	61	D7	15	04	9F	6A	BA	2A	0C	22	12	ú i!yax 'Yjox "
00000110	1C	A1	A2	02	21	80	AC	53	03	0B	7F	AA	E7	5F	25	F5	;c !e-S *g_š0
00000120	3F	32	A5	12	97	46	96	B2	89	B9	69	02	65	82	55	81	?Zy -F-'h'i e,U
00000130	9B	4D	FC	AB	85	AC	1B	83	BA	48	17	4A	84	25	F0	39	»Mú«... f°H J,«09
00000140	37	A4	8F	1C	C5	73	91	C0	84	05	F9	A5	67	6B	29	C8	7h Áš'á, úWqk)È
00000150	45	89	8B	03	C6	80	D6	53	60	57	5A	EA	52	55	FF	98	Eh< #E0S'WZÉRUY"
00000160	6A	55	4D	45	51	92	2A	B8	2C	B5	4B	AA	28	FE	C1	23	jUMEQ'*, ,pK+ (pÁ#
00000170	DD	AB	F5	64	39	61	12	66	C2	6D	12	6A	11	87	01	29	Y«0d9a fÁM j +)
00000180	BA	04	49	20	A0	90	C6	59	C2	19	38	24	90	B0	1A	8B	° I FYÁ 8š « <
00000190	B2	6D	0C	FA	55	0D	03	A3	59	5A	8B	66	23	2F	D3	A1	"m úU EYZ<f#;/C;
000001A0	40	ED	A7	AA	64	11	75	A3	64	3C	A5	7A	8A	04	22	55	{šs'd uEd<Yzš "U
000001B0	20	23	EC	29	78	17	7E	5B	93	70	25	EC	2E	29	15	89	#i)x ~["pÁi.) %
000001C0	10	28	26	E4	CC	40	17	D4	55	68	06	C5	40	80	19	36	(šáí@ CÜh Á@e 6
000001D0	C3	54	95	82	7C	A9	96	11	2A	5B	95	93	51	A5	DA	59	ÁI*, e- *["QVÜY
000001E0	23	A1	4C	00	DC	D3	05	29	66	32	21	A5	D4	E1	A4	20	#;L ÜC)f2!Y0Áh
000001F0	28	3D	00	2D	38	31	2D	48	23	C1	D0	53	0F	54	16	41	(= -01-H#ÁDS T A
00000200	6C	2A	16	78	04	23	D2	1A	09	52	0D	D5	04	55	EE	C9	1* x #0 R C ÜE!
00000210	BB	0F	6E	FB	A8	5C	EA	9B	05	63	C6	1C	D0	29	C5	80	» nú`è) c# È)ÁE
00000220	09	71	70	EA	1E	68	8C	0F	2A	37	97	66	12	32	F1	4F	qpè hÑ *7-f 2Á0

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

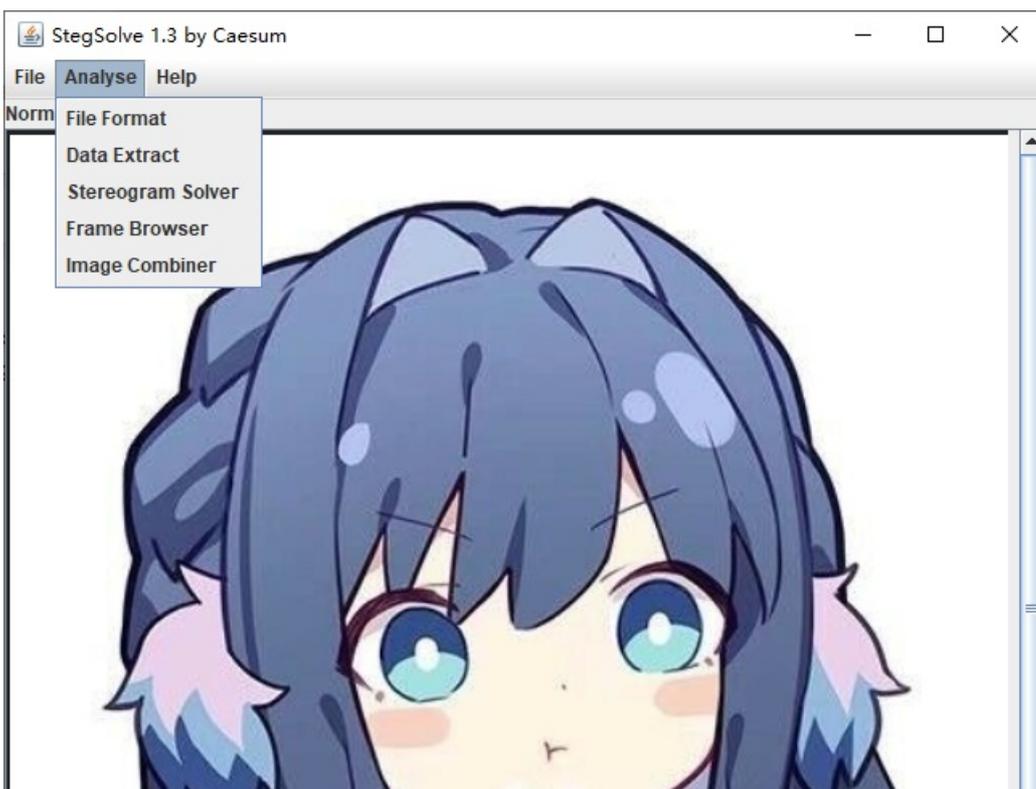
RAR Archive (rar), 文件头: 52617221

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

Stereogram Solve:立体试图 可以左右控制偏移

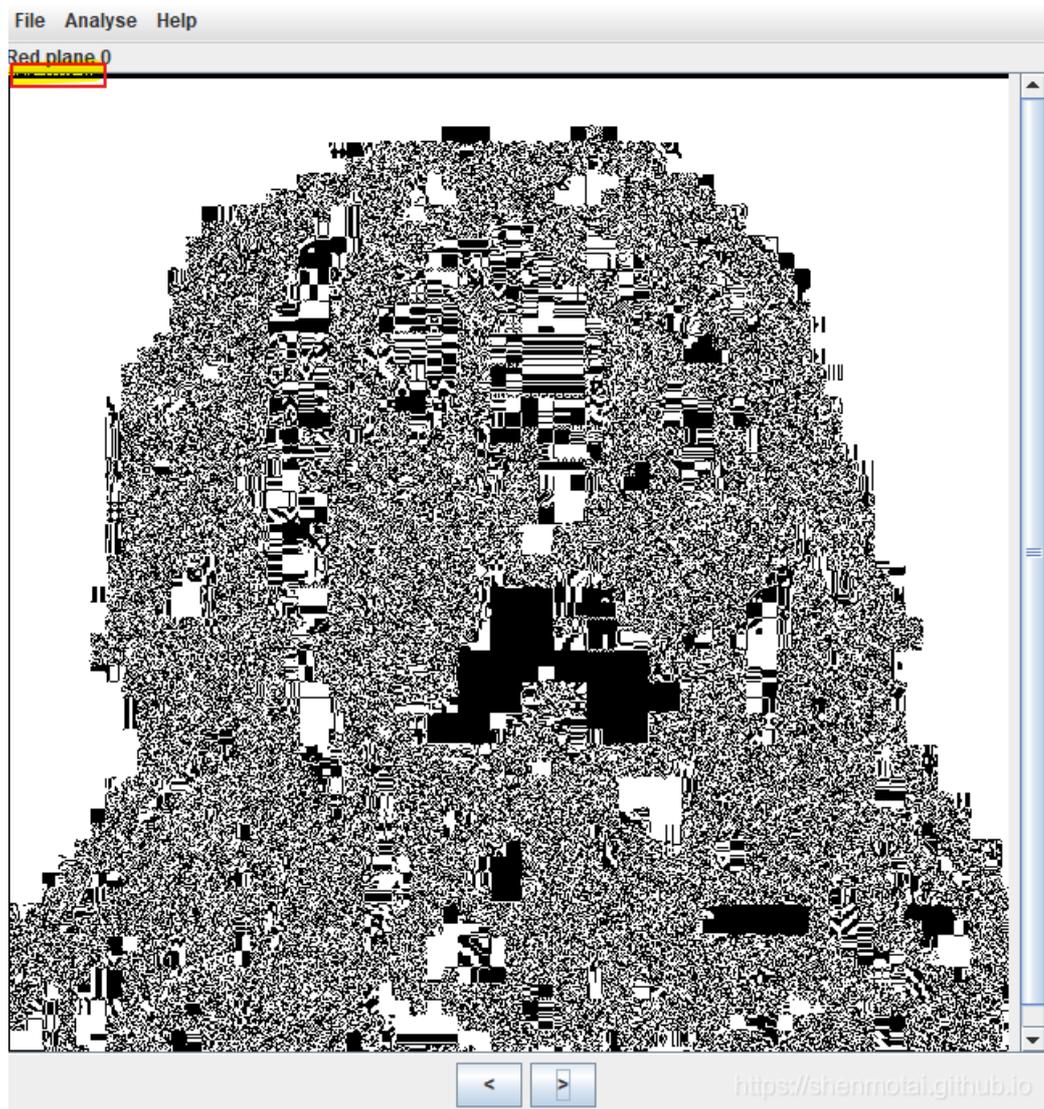
Frame Browser:帧浏览器，主要是对GIF之类的动图进行分解，动图变成一张张图片，便于查看

Image Combiner:拼图，图片拼接

这一题简单如图

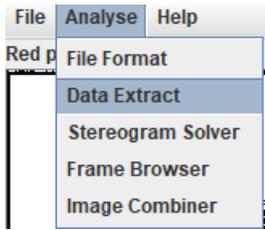


直接按下面的按钮切换

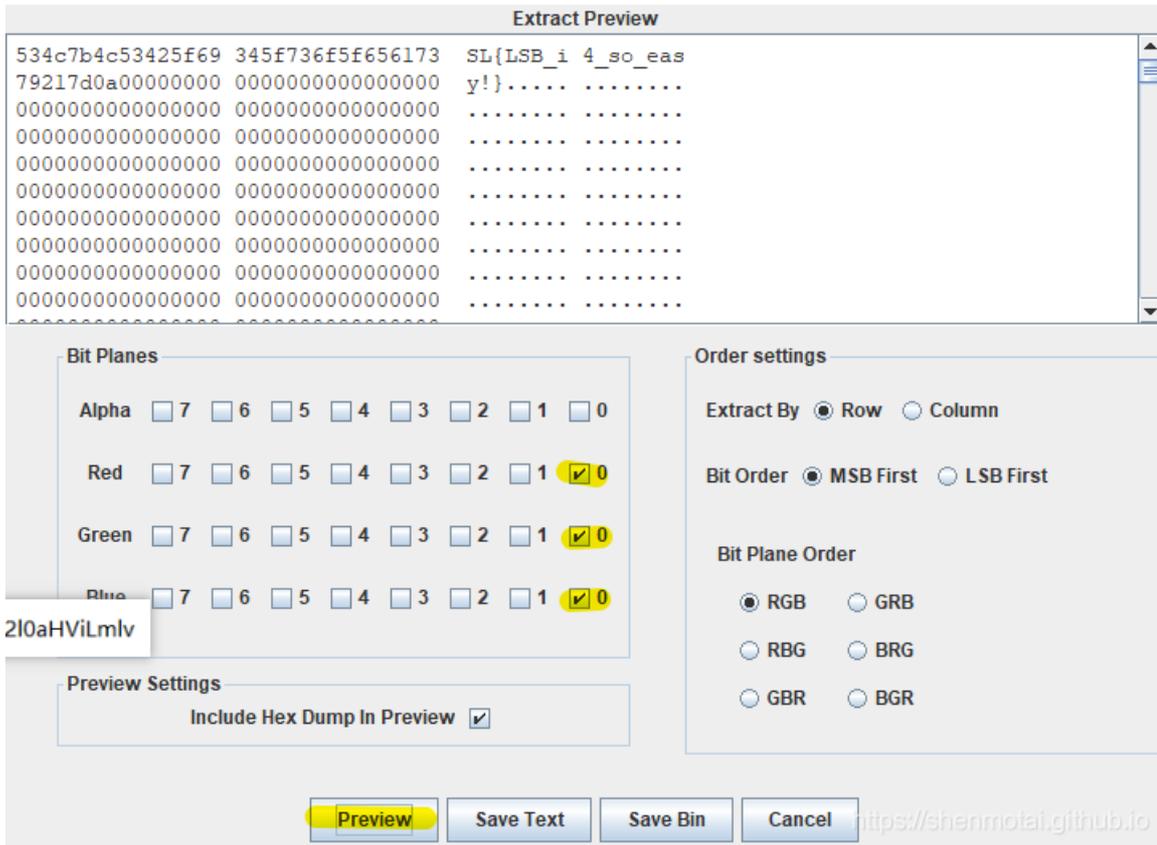


然后会发现左上角隐藏着什么东西，多往后切还会出现几张类似现象

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

```
shenmotai@kali1: ~/桌面/LSB/gaps
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)
#
# deb cdrom:[Kali GNU/Linux 2020.1b _Kali-last-snapshot_ - Official amd64
4 DVD Binary-1 with firmware 20200316-17:52]/ kali-rolling contrib main
non-free

#deb cdrom:[Kali GNU/Linux 2020.1b _Kali-last-snapshot_ - Official amd64
DVD Binary-1 with firmware 20200316-17:52]/ kali-rolling contrib main n
on-free

# This system was installed using small removable media
# (e.g. netinst, live or single CD). The matching "deb cdrom"
# entries were disabled at the end of the installation process.
# For information about how to configure apt package sources,
# see the sources.list(5) manual.
deb http://mirrors.ustc.edu.cn/kali kali-rolling main non-freecontrib
deb-src http://mirrors.aliyun.com/kali kali-rolling main non-free contri
~
https://shenmotai.github.io
```

第九条修改结果如下:

```
/home/shenmotai/桌面/LSB/gaps/requirements.txt - Mousepad
文件(F) 编辑(E) 搜索(S) 视图(V) 文档(D) 帮助(H)
ppencv-python=4.2.0.34
matplotlib=3.0.3
pytest=3.2.1
pillow=6.2.0
~
https://shenmotai.github.io
```

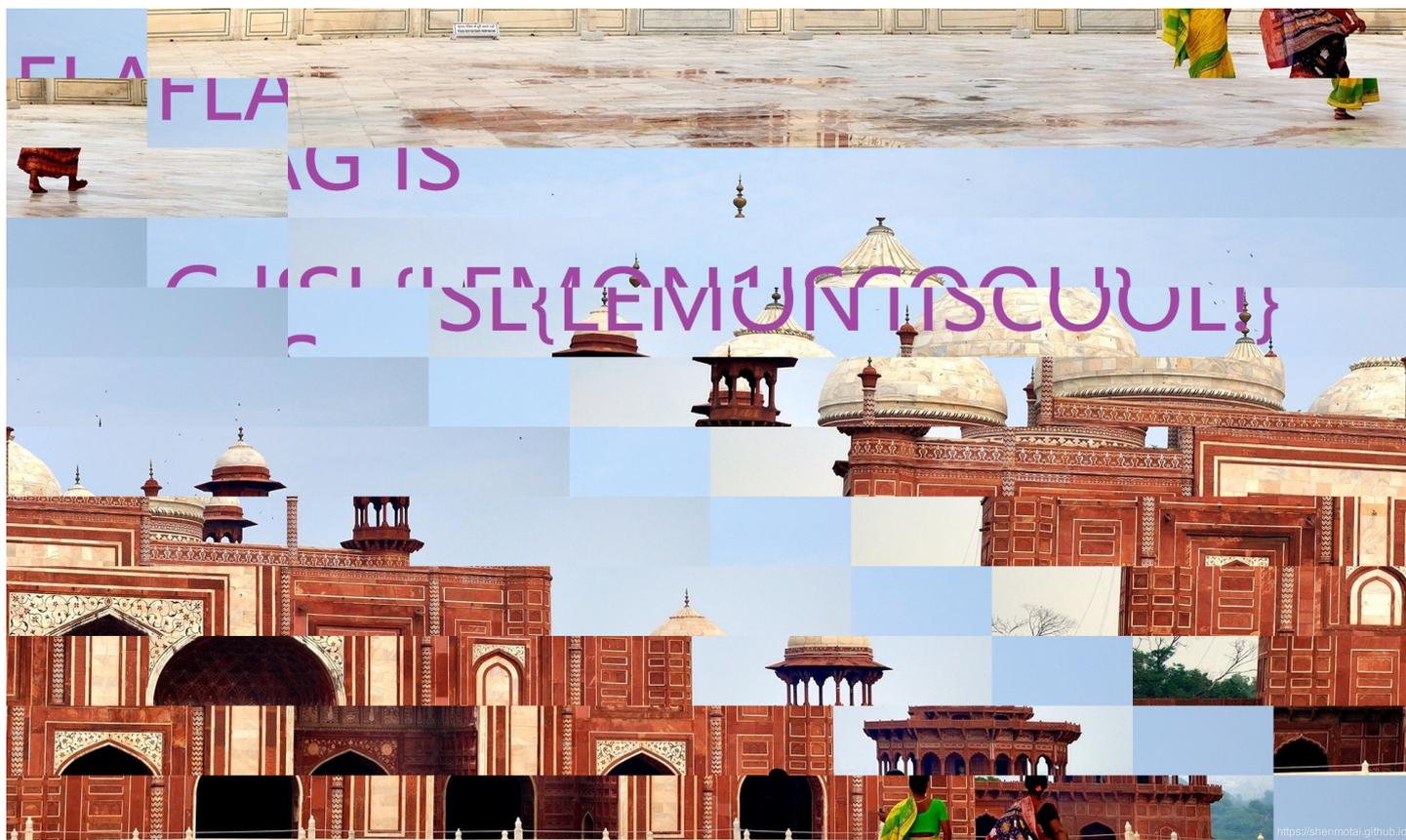
第七条配置文件内容如下:

```
shenmotai@kali1: ~/桌面/LSB/gaps
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)
[global]
index-url = http://mirrors.aliyun.com/pypi/simple/
[install]
trusted-host=mirrors.aliyun.com
~
~
~
~
shenmotai
~
```

在文件夹里打开黑窗口输入:

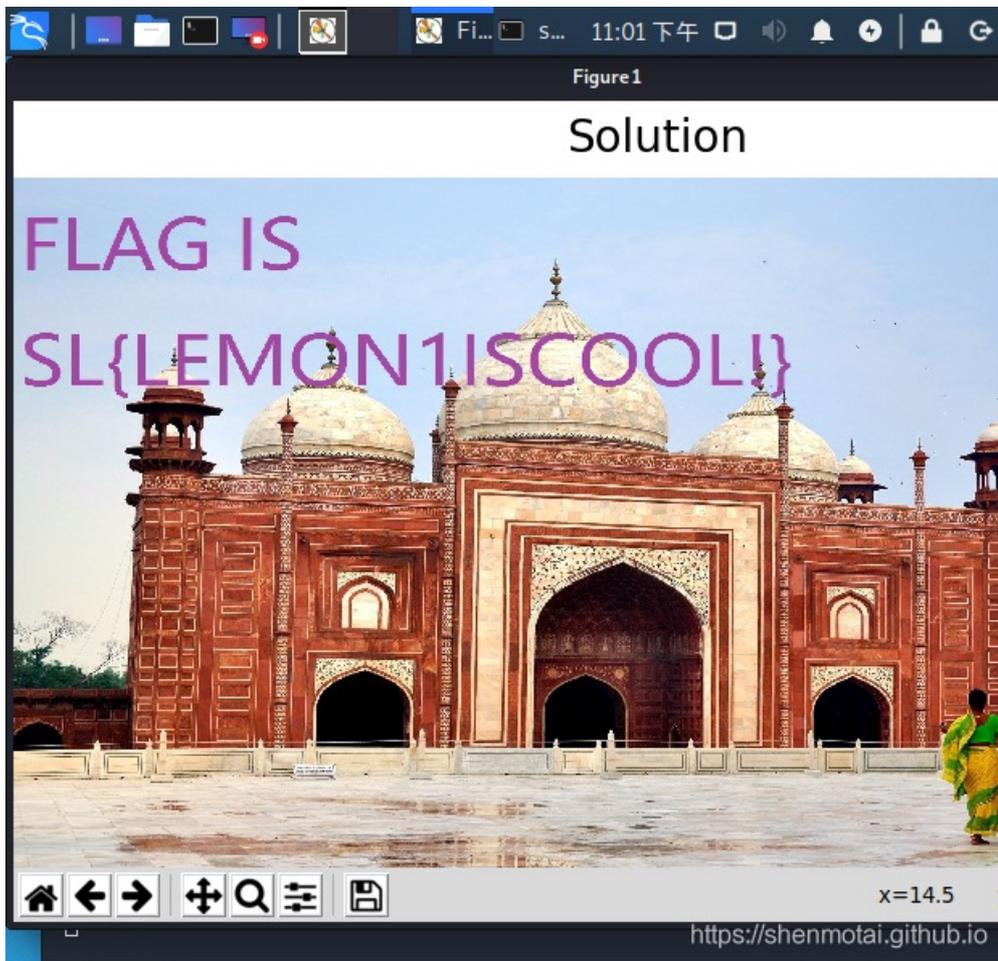
```
montage *jpg -tile 10x12 -geometry 200x100+0+0 out.jpg
```

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

