【攻防世界】十、SimpleRAR

原创

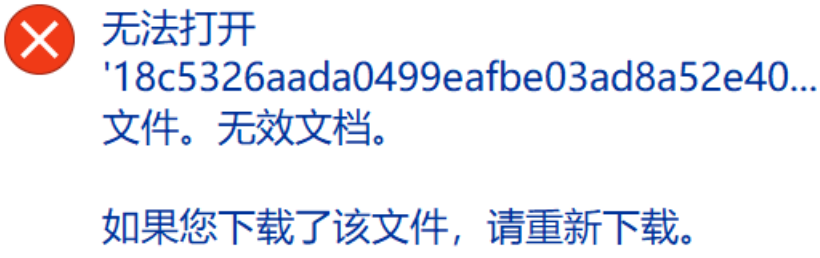
我是大肥鼠 于 2021-10-22 14:29:34 发布 91 收藏

分类专栏： # 攻防世界MISC 文章标签： 安全 rar 二维码

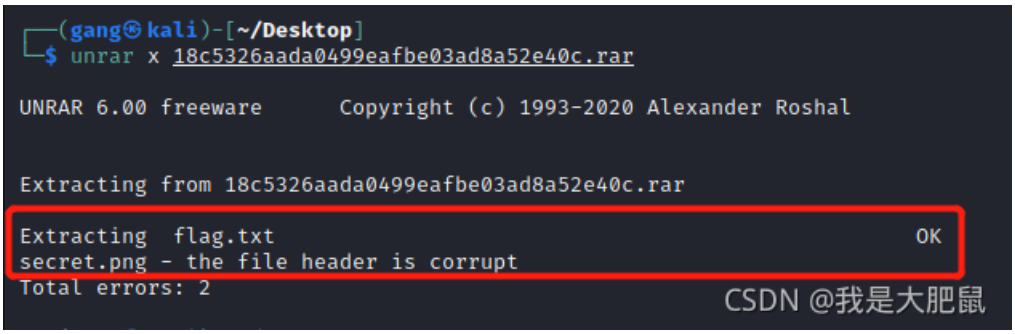
只能看不能摸哟！

步骤

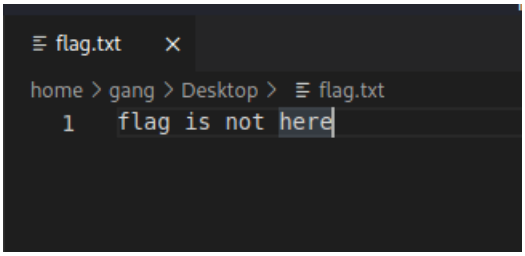
下载所给附件，发现是一个rar压缩文件，解压之后应该可以发现里面有一个flag.txt文件，还有一个secret.png提示文件头损坏没解压出来，我第一次使用winzip直接提示我无效文档？？？



然后我不信邪又用kali里的命令进行解压缩，成功解压出来flag.txt文件，并提示我secret.png文件头损坏



打开flag.txt文件进行查看，发现是一个烟雾弹



再次吐槽一下winzip真是lj，选对工具真的是非常非常重要！

那么线索只能是在secret.png文件里了，根据题目描述搞错了一块，说明压缩包有问题，我们使用winhex打开压缩文件

18c5326aada0499eafbe03ad...

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	52	61	72	21	1A	07	00	CF	90	73	00	00	0D	00	00	00	Rar! Ï s
00000016	00	00	00	00	D5	56	74	20	90	2D	00	10	00	00	00	10	ÕVt -
00000032	00	00	00	02	C7	88	67	36	6D	BB	4E	4B	1D	30	08	00	Çˆg6m»NK 0
00000048	20	00	00	00	66	6C	61	67	2E	74	78	74	00	B0	57	00	flag.txt °W
00000064	43	66	6C	61	67	20	69	73	20	6E	6F	74	20	68	65	72	Cflag is not her
00000080	65	A8	3C	7A	20	90	2F	00	3A	15	00	00	42	16	00	00	e¨<z / : B
00000096	02	BC	E9	8C	2F	6E	84	4F	4B	1D	33	0A	00	20	00	00	¼éŒ/n„OK 3
00000112	00	73	65	63	72	65	74	2E	70	6E	67	00	F0	40	AB	18	secret.png ð@«
00000128	11	C1	11	55	08	D1	55	80	0D	99	C4	90	87	93	22	19	Á U ÑU€ ™Ä ‡""
00000144	4C	58	DA	18	B1	A4	58	16	33	83	08	F4	3A	18	42	0B	LXÚ ±¤X 3ƒ ô: B
00000160	04	05	85	96	21	AB	1A	43	08	66	EC	61	0F	A0	10	21	…–!« C fìa !
00000176	AB	3D	02	80	B0	10	90	C5	8D	A1	1E	84	42	B0	43	29	«= €° Å ¡ „B°C)
00000192	08	10	DA	0F	23	99	CC	F3	9D	C4	85	86	67	73	39	DE	Ú #™Ìó Ä…†gs9Þ
00000208	47	63	91	DE	C4	77	ED	A8	DC	46	F4	C5	54	CD	55	6A	Gc'ÞÄwí¨ÜFôÅTÍUj
00000224	AA	A3	5F	CD	6E	77	3B	8D	EF	7A	99	A9	A9	8F	D5	3F	ª£_Ínw; ïz™©© Õ?
00000240	0A	AA	F9	55	7F	02	9E	A2	9C	86	88	CC	59	CC	FF	0C	ªùU ž¢œ†ˆÌYÌÿ
00000256	57	34	7B	8B	8F	F9	C0	F7	E6	30	E3	25	60	55	58	00	W4{‹ ùÀ÷æ0ã%`UX
00000272	9A	CC	E6	CD	CB	FD	19	24	43	83	30	46	D6	97	30	0C	šÌæÍËý $Cƒ0FÖ–0
00000288	ED	2D	4D	8D	E8	E6	3F	1A	FB	23	10	0D	8D	1F	A8	5F	í-M èæ? û# ¨_
00000304	41	55	3D	55	70	4C	69	6B	6C	50	78	71	69	5B	78	56	AU=UpLiklPxqi[xV
00000320	5C	08	F0	DA	11	11	A0	C5	25	20	02	30	80	62	03	38	\ ðÚ Å% 0€b 8
00000336	06	FB	D5	98	07	E8	6E	6F	72	FD	6F	DD	EC	CD	01	F9	ûÕ˜ ènoryoÝìÍ ù
00000352	02	07	CB	9F	F7	DE	3C	E4	0F	F8	4E	DC	DB	7E	D0	95	Ë Ÿ÷Þ<ä øNÜÛ~Ð•
00000368	F9	C0	1F	B9	94	C0	FC	84	00	41	3B	40	02	10	F4	F8	ùÀ ¹”Àü„ A;@ ôø
00000384	F8	00	20	47	67	DD	B4	1F	F8	4F	8E	80	1F	FE	BC	FC	ø GgÝ´ øOŽ€ þ¼ü
00000400	F0	F7	97	E0	40	7E	C4	0F	EC	60	CF	D0	80	7F	38	31	ð÷—à@~Ä ì`ÏÐ€ 81
00000416	E5	28	E2	D1	E0	06	B4	9A	9D	FC	93	E5	D3	FA	1A	DC	å(âÑà ´š ü“åÓú Ü
00000432	DC	DC	01	9F	1F	3B	7F	EC	76	EC	80	77	C8	BB	51	F1	ÜÜ Ÿ ; ìvì€wÈ»Qñ

因为只有两个文件，here结束之后的位置应该就是sercet.png文件的开始部分，然后了解了一下rar的组成：

每个数据块的结构：

```
HEAD_CRC：校验码，2字节
HEAD_TYPE：块的类型，1字节，也可理解为块的头部类型，不同的块对应不同的块头部
HEAD_FLAG：块标记，2字节
最后两个字节表示块的大小
```

声明的块类型：

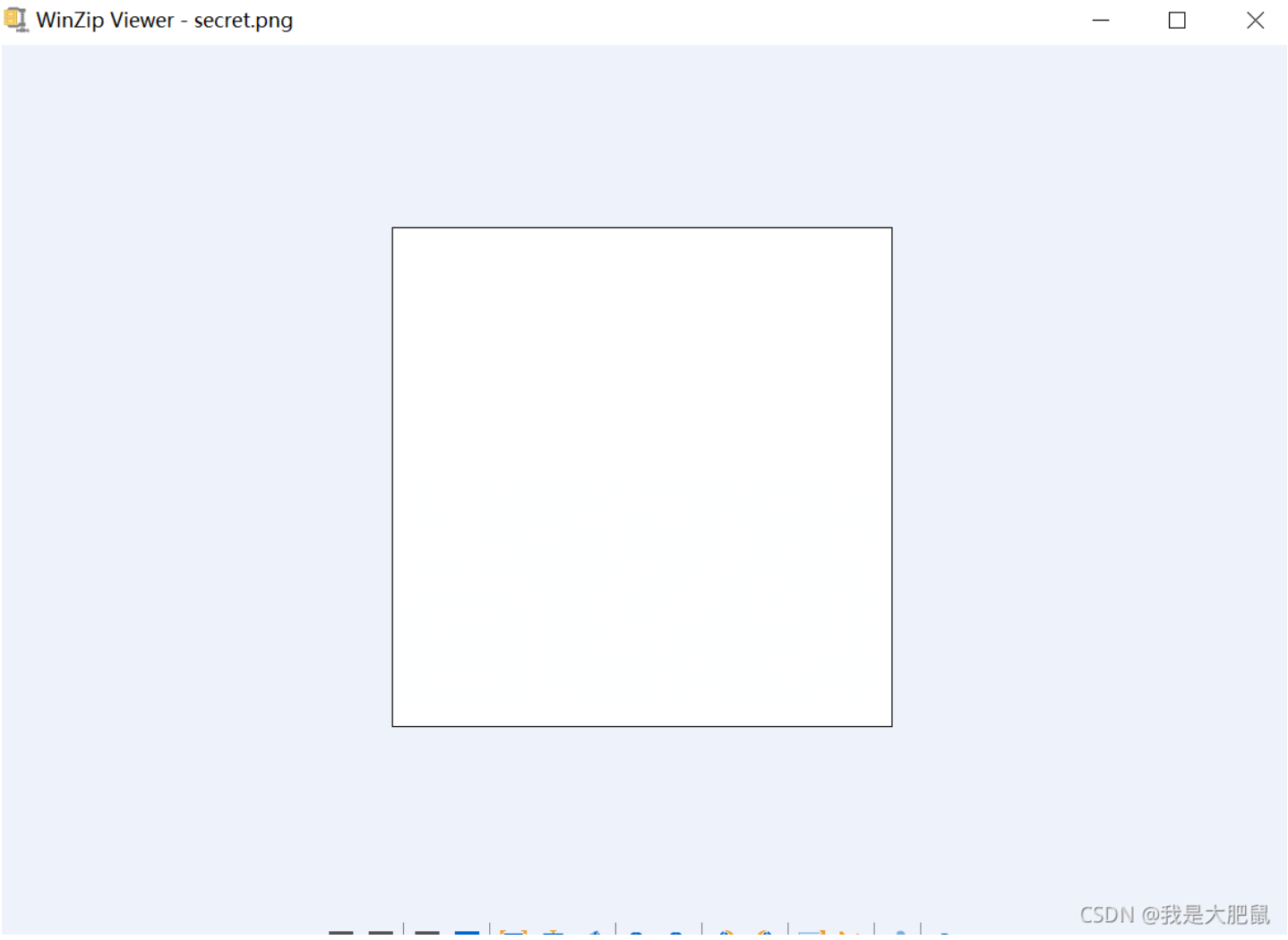
```
HEAD_TYPE=0x72：标记块
HEAD_TYPE=0x73：归档头部块（压缩文件头）
 HEAD_TYPE=0x74：文件块（文件头）
HEAD_TYPE=0x75：老风格的注释块
HEAD_TYPE=0x76：老风格的用户身份信息块
HEAD_TYPE=0x77：老风格的子块
 HEAD_TYPE=0x78：老风格的恢复记录块
HEAD_TYPE=0x79：老风格的用户身份信息块
 HEAD_TYPE=0x7a：子块
 HEAD_TYPE=0x7b：结束块
```

由于我们这里的是文件块而不是子块，所以将7A改为74，另存为文件

18c5326aada0499eafbe03ad...

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	52	61	72	21	1A	07	00	CF	90	73	00	00	0D	00	00	00	Rar! Ï s
00000016	00	00	00	00	D5	56	74	20	90	2D	00	10	00	00	00	10	ÕVt -
00000032	00	00	00	02	C7	88	67	36	6D	BB	4E	4B	1D	30	08	00	Çˆg6m»NK 0
00000048	20	00	00	00	66	6C	61	67	2E	74	78	74	00	B0	57	00	flag.txt °W
00000064	43	66	6C	61	67	20	69	73	20	6E	6F	74	20	68	65	72	Cflag is not her
00000080	65	A8	3C	74	20	90	2F	00	3A	15	00	00	42	16	00	00	e¨<t / : B
00000096	02	BC	E9	8C	2F	6E	84	4F	4B	1D	33	0A	00	20	00	00	¼éŒ/n„OK 3
00000112	00	73	65	63	72	65	74	2E	70	6E	67	00	F0	40	AB	18	secret.png ð@«
00000128	11	C1	11	55	08	D1	55	80	0D	99	C4	90	87	93	22	19	Á U ÑU€ ™Ä ‡""
00000144	4C	58	DA	18	B1	A4	58	16	33	83	08	F4	3A	18	42	0B	LXÚ ±¤X 3ƒ ô: B
00000160	04	05	85	96	21	AB	1A	43	08	66	EC	61	0F	A0	10	21	…–!« C fìa !
00000176	AB	3D	02	80	B0	10	90	C5	8D	A1	1E	84	42	B0	43	29	«= €° Å ¡ „B°C)
00000192	08	10	DA	0F	23	99	CC	F3	9D	C4	85	86	67	73	39	DE	Ú #™Ìó Ä…†gs9Þ
00000208	47	63	91	DE	C4	77	ED	A8	DC	46	F4	C5	54	CD	55	6A	Gc'ÞÄwí¨ÜFôÅTÍUj
00000224	AA	A3	5F	CD	6E	77	3B	8D	EF	7A	99	A9	A9	8F	D5	3F	ª£_Ínw; ïz™©© Õ?
00000240	0A	AA	F9	55	7F	02	9E	A2	9C	86	88	CC	59	CC	FF	0C	ªùU ž¢œ†ˆÌYÌÿ
00000256	57	34	7B	8B	8F	F9	C0	F7	E6	30	E3	25	60	55	58	00	W4{‹ ùÀ÷æ0ã%`UX
00000272	9A	CC	E6	CD	CB	FD	19	24	43	83	30	46	D6	97	30	0C	šÌæÍËý $Cƒ0FÖ—0
00000288	ED	2D	4D	8D	E8	E6	3F	1A	FB	23	10	0D	8D	1F	A8	5F	í-M èæ? û# ¨_

解压之后可以看到一张图片，打开发现是白色的图

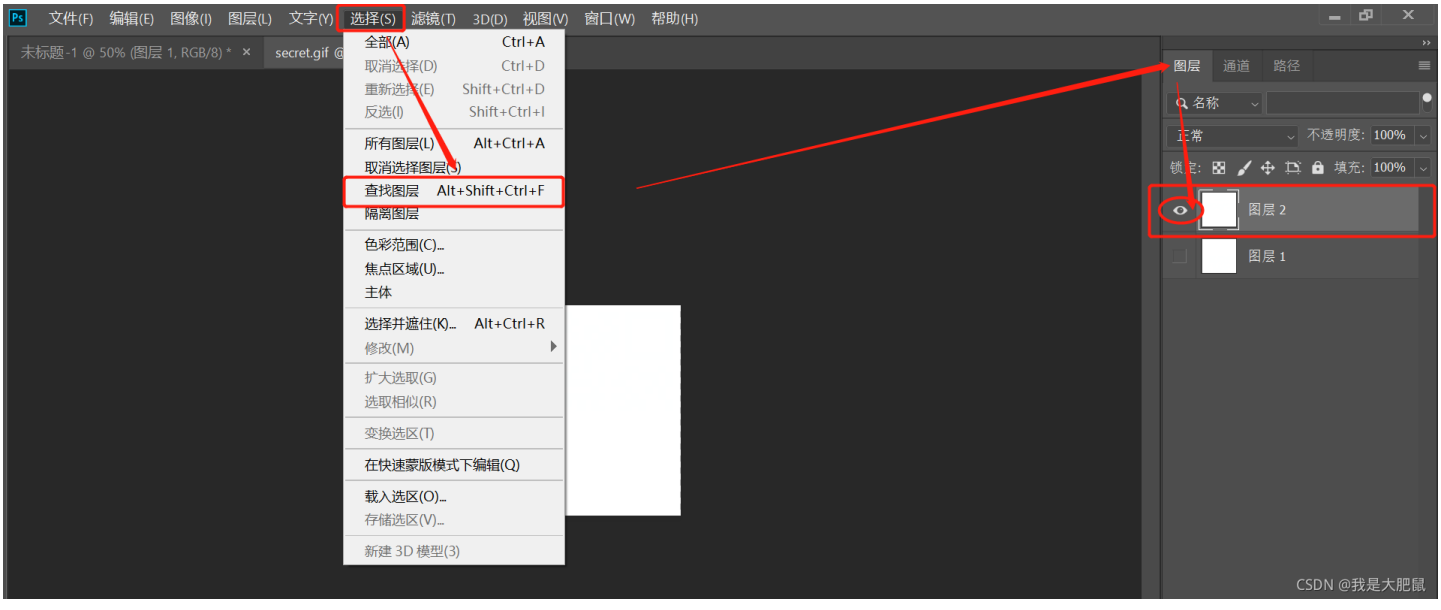


老规矩，用winhex打开secret.png图片，发现它实际上是一个gif文件，怎么看出来的可以看一下这位师傅的文章

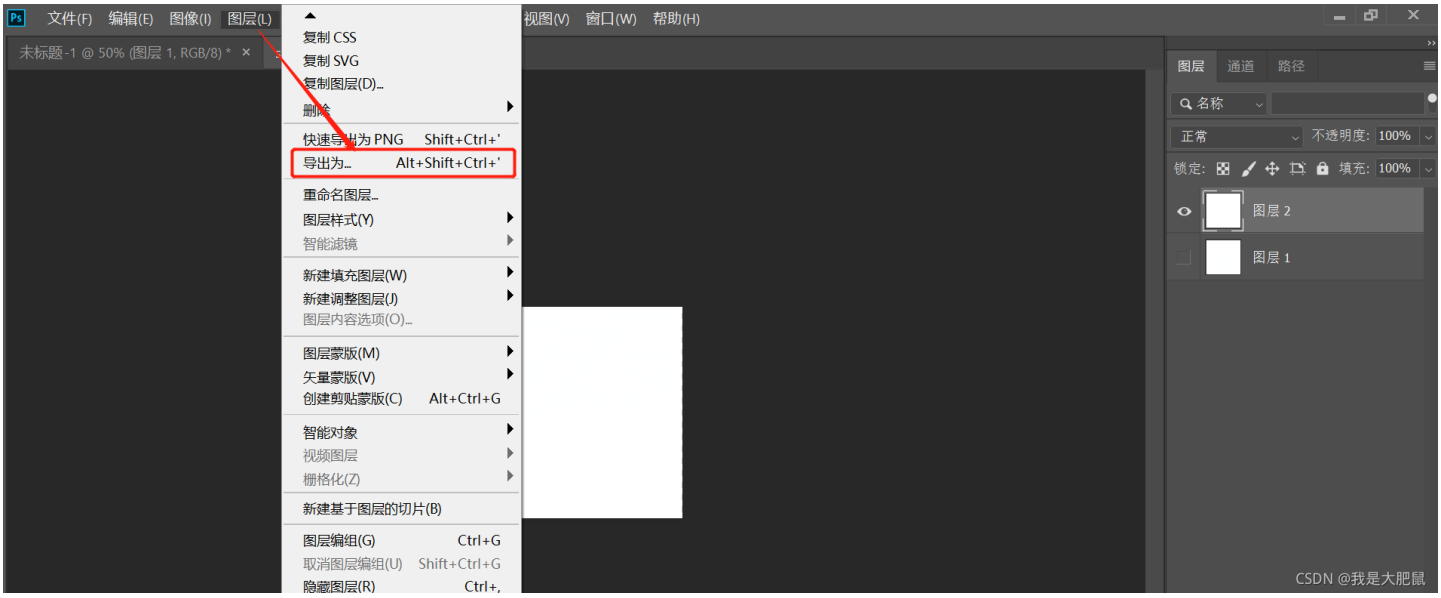
将后缀修改为gif，之后用stegsolve.jar打开，发现了半个二维码

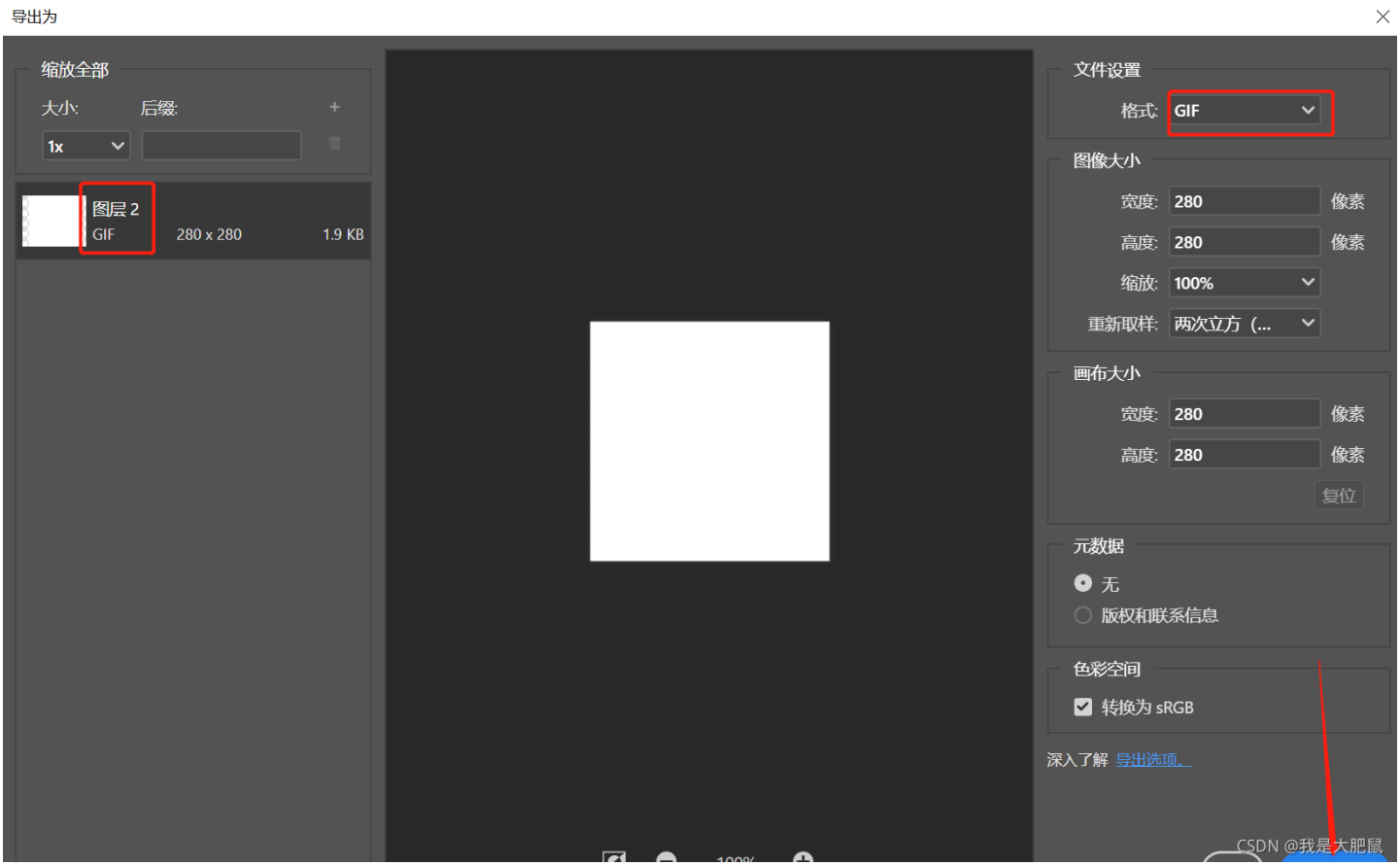
题目描述中又提示双图层，唉，被迫下载了ps

打开文件secret.gif，查看图层，发现有两个图层，选中第2个图层

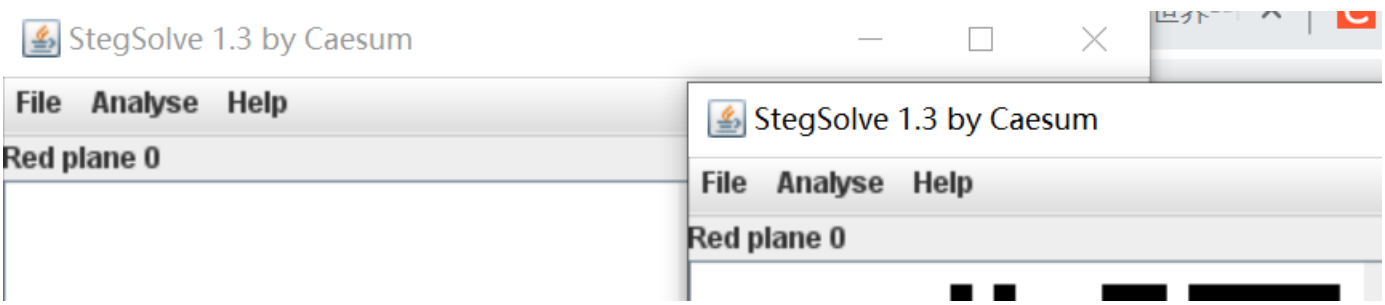


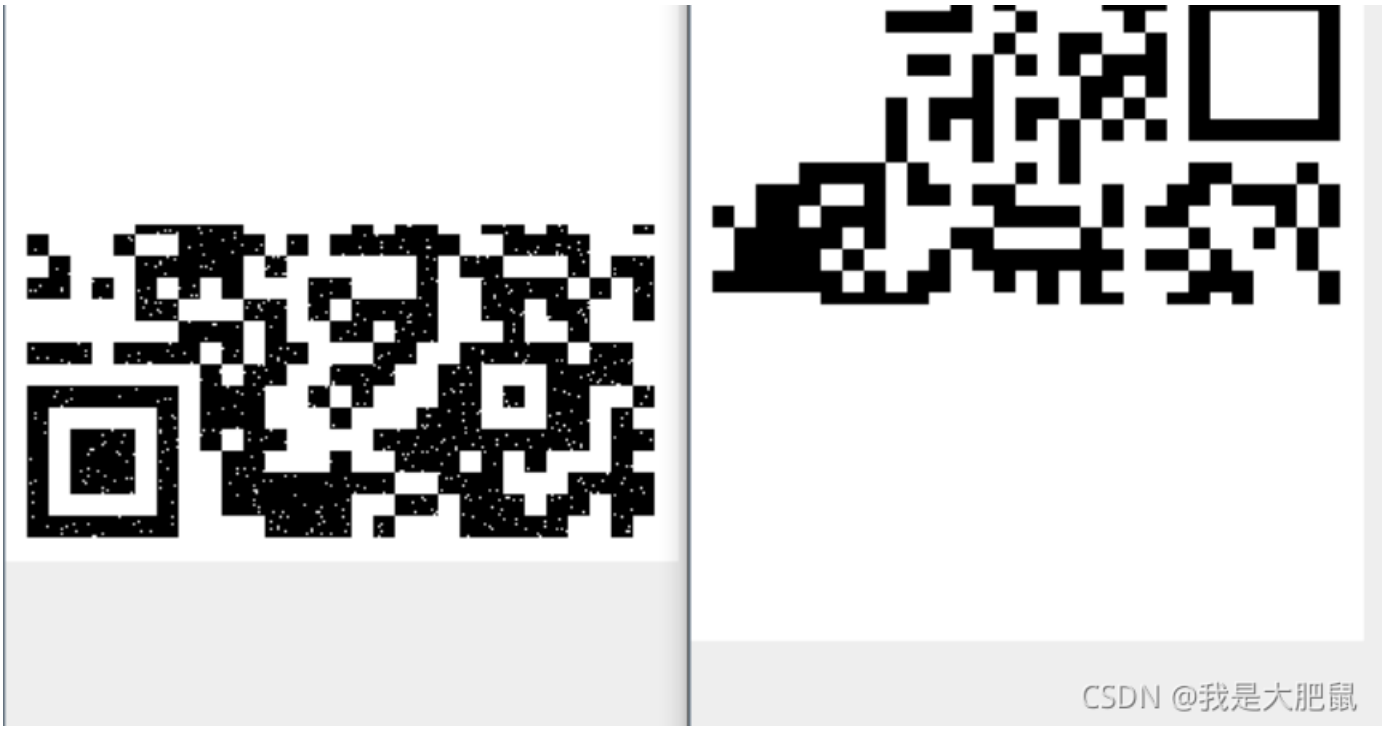
另存为secret1.gif文件





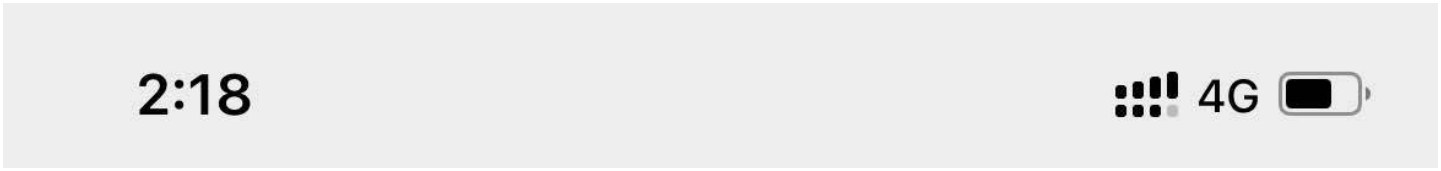
之后使用stegsolve分别打开两个gif图片：





发现了两张半个二维码，然后将两张图片拼接起来，添加缺失的定角符：

扫描二维码得出flag



扫描结果

flag{yanji4n_bu_we1shi}

吐槽一下，ps是真的难用啊…

总结

rar压缩文件的了解
各种图片头文件格式的了解
工具的选择与使用
二维码的了解