

# Writeup-2020安洵杯-Misc题：开始抑郁

原创

Y5ncKO 于 2020-09-08 01:14:48 发布 90 收藏 1

文章标签：[python](#) [信息安全](#) [软件测试](#) [ffmpeg](#) [bug](#)

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/qq\\_41596969/article/details/110377794](https://blog.csdn.net/qq_41596969/article/details/110377794)

版权

不说了，到点了，我tm直接开始抑郁！

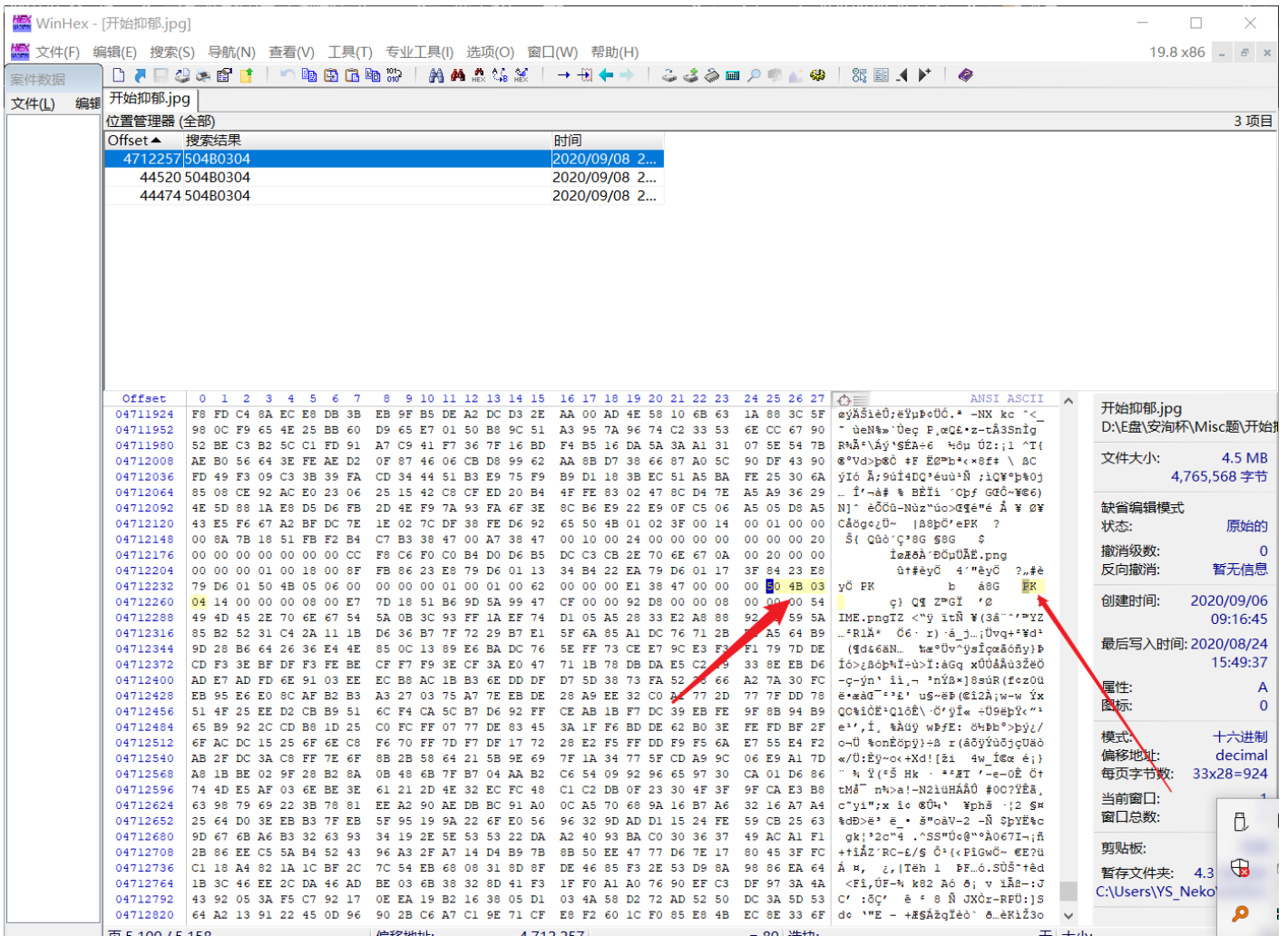
题目描述：开始抑郁

附件下载

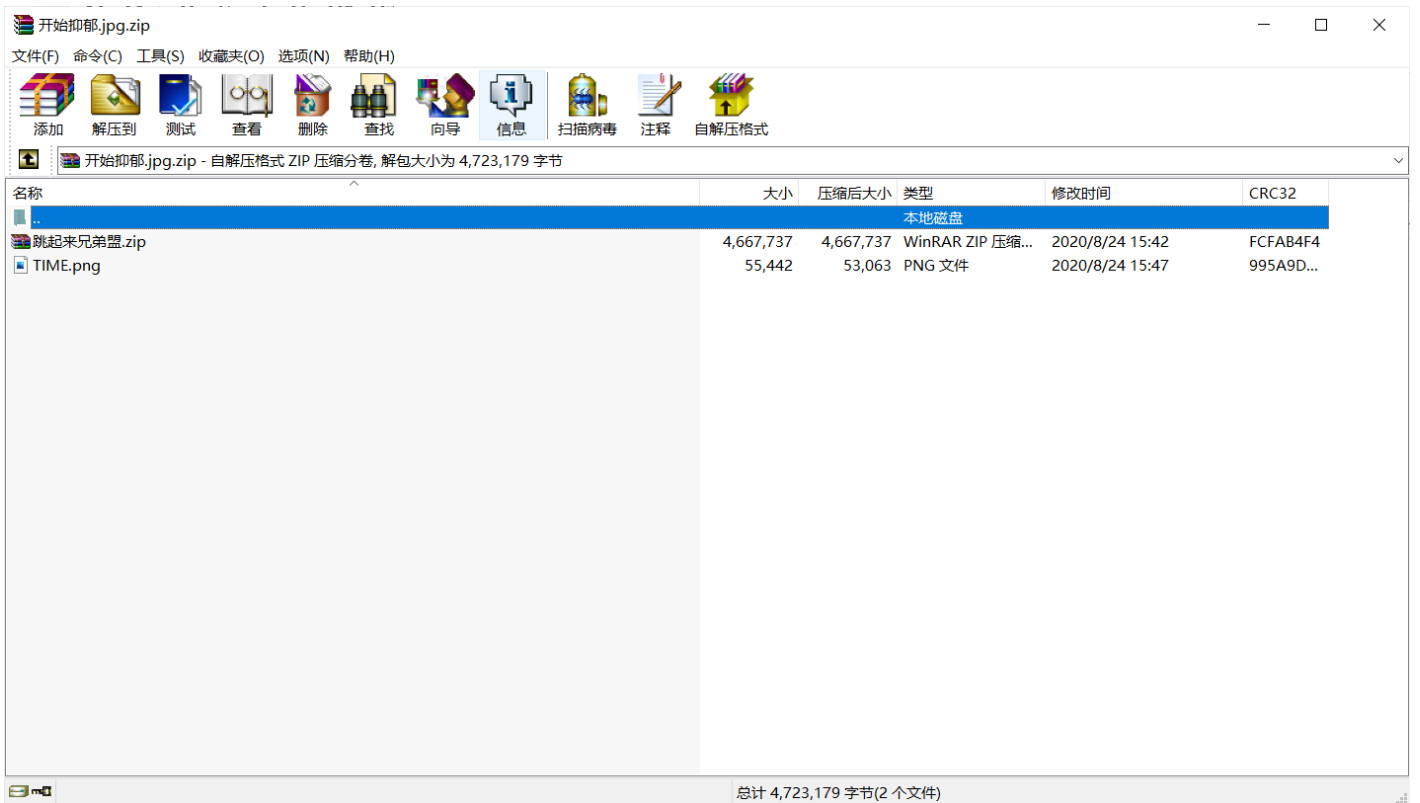
打开压缩包发现一张图片，解压出来，直接查看没有发现异常



观察图片大小发现过大，4.5M，推测为混合了其他文件



发现zip文件头，直接将格式改为zip解压得到两个文件



首先打开压缩包，发现是加密的，打开图片TIME.png，发现无法正常打开，推测需要修复，Winhex打开

WinHex - [TIME.png]

文件(F) 编辑(E) 搜索(S) 导航(N) 查看(V) 工具(T) 专业工具(I) 选项(O) 窗口(W) 帮助(H)

19.8 x 86

文件(L) 编辑

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27				
00000000	00	00	00	00	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	00	00	02	C4	00	00	02	C4	08	06	00	00				
00000008	00	0F	55	26	83	00	00	20	00	49	44	41	54	78	5E	EC	BD	E1	7A	DC	56	CE	74	9B	DC	FF	45	E7				
00000016	3C	72	26	E1	59	26	6E	B2	BD	D6	2C	63	53	12	FC	D7	DC	04	50	28	14	8A	54	AB	F5	E7	5F	7F				
00000024	FD	F5	D7	1F	6F	11	58	04	04	16	81	45	60	11	58	04	16	81	45	60	11	F8	A6	08	FC	B9	86	F8				
00000032	9B	76	7E	CB	5E	04	16	81	45	60	11	58	04	16	81	45	60	11	F8	A6	08	1A	E2	25	C2	22	B0	08				
00000040	2C	02	8B	C0	22	B0	08	2C	02	8B	C0	B7	46	60	0D	F1	B7	E6	FF	16	BF	08	2C	02	8B	C0	22	B0	08			
00000048	08	2C	02	8B	C0	22	B0	08	2C	02	8B	C0	B7	46	60	0D	F1	B7	E6	FF	16	BF	08	2C	02	8B	C0	22	B0	08		
00000056	43	FC	AD	DB	BF	C5	21	02	8B	C0	22	B0	08	2C	02	8B	C0	22	B0	08	2C	02	8B	C0	22	B0	08	2C	02	8B	C0	
00000064	A1	73	F5	85	19	57	B5	95	2F	D8	98	C2	C5	E4	56	35	EC	AE	46	8A	71	95	D3	BB	FB	18	BC	4A	1A	E2	3F	
00000072	5E	BC	CB	8F	FC	FF	54	5E	13	71	4A	2E	99	1E	13	DC	DF	5D	6B	6A	79	77	CF	57	FF	5F	F6	E5	05	05	05	
00000080	A9	F7	BA	C2	E5	33	62	6C	1A	B9	3A	63	38	5E	F6	F8	8E	AF	74	F7	99	5A	0C	96	26	CE	04	66	05	05	05	
00000088	13	31	8C	BE	9E	1E	3F	75	E1	9B	FA	EF	F8	B2	86	18	22	4A	45	01	DE	FE	FF	2E	37	43	6E	63	05	05	05	
00000096	FD	FB	9C	5A	4B	53	B8	7C	C6	49	42	FB	32	25	A4	13	71	4A	2E	9D	9C	89	8F	1E	9A	5A	68	EF	05	05	05	
00000104	8D	97	79	4B	46	3F	97	76	7A	91	98	B9	30	AC	28	FB	FF	D4	7B	95	7C	39	8D	B1	A9	E5	33	3E	05	05	05	
00000112	D8	53	D8	2F	E8	95	9E	BD	72	2E	68	FF	4B	5C	0C	F7	EF	CE	50	5C	28	27	EA	7C	CD	FD	D6	10	05	05	05	
00000120	AF	21	46	BC	31	E2	73	7A	30	8C	08	D0	E1	47	20	FE	0F	17	4F	E5	35	11	A7	E4	92	E9	F1	FF	05	05	05	
00000128	D0	86	9F	8E	9A	5A	4C	FC	B2	2F	4F	BD	17	35	11	1F	D7	97	FD	2F	71	31	B5	AC	21	66	93	51	05	05	05	
00000136	CF	E2	98	FA	CB	1E	97	F7	BE	BF	9A	E2	72	7A	EF	BF	AF	E8	E7	2B	52	43	7C	BA	99	F5	60	90	05	05	05	
00000144	31	9B	AA	BF	24	26	7D	13	77	47	82	89	FA	A7	86	EC	B3	E1	62	9E	EC	4D	2F	29	F7	E4	DE	36	05	05	05	
00000152	9B	F8	46	E4	E8	19	C3	B1	5B	21	85	0F	DD	75	FC	B2	FE	72	2E	68	5E	06	E3	AF	C4	31	8A	D7	05	05	05	
00000160	DD	83	C2	69	9E	99	5A	CA	9C	8D	57	28	93	9B	FA	CB	33	A5	8E	1B	4D	98	F0	0A	66	27	AE	21	05	05	05	
00000168	16	2C	33	64	12	61	2E	8F	D0	9F	5F	69	F8	D8	28	19	EC	CD	90	97	6F	76	4C	CE	F4	01	CE	98	05	05	05	
00000176	05	CA	BD	35	C4	FC	F3	D8	86	E3	E5	82	99	D2	08	CA	F1	35	C4	14	B1	EB	37	E7	A7	39	C6	2B	05	05	05	
00000184	B9	FF	26	17	AA	BD	53	1C	2F	E7	D2	60	46	77	92	99	31	B3	2B	4F	E3	A2	F6	D8	5F	17	59	9B	05	05	05	
00000192	9B	95	CD	A4	4D	BE	7B	52	36	79	9D	AE	9F	C6	FF	4A	C3	6F	84	DC	F4	D8	0C	39	15	65	93	97	05	05	05	
00000200	39	63	30	A3	F5	1B	21	35	86	DC	D4	4F	CF	94	78	DD	3D	10	50	8C	A7	F0	9A	D2	08	DA	97	EF	05	05	05	
00000208	CE	31	8A	D7	DD	DE	AB	39	6E	72	A3	67	CA	9C	A7	38	7E	DA	F8	51	AF	64	66	CC	ED	D8	69	5C	05	05	05	
00000216	A8	87	FA	A1	E3	6B	88	5F	D3	C9	80	49	87	FF	EE	7A	1A	FF	2B	0D	BF	11	45	83	BD	19	F2	35	05	05	05	
00000224	C4	6C	5E	A6	0C	1E	ED	BF	E1	D8	D4	22	99	E0	D8	94	5E	D0	BE	18	8C	BF	12	C7	28	5E	6B	88	05	05	05	
00000232	DD	1B	F2	AF	A4	FD	6B	88	D9	E4	DA	8F	4C	08	95	A1	86	54	84	B8	3D	42	E3	4F	2D	B8	89	A7	05	05	05	
00000240	3E	63	56	0C	FE	5F	49	14	0D	66	84	FE	EF	6E	56	4C	FD	14	E3	29	73	37	A5	17	74	2E	0D	C6	05	05	05	
00000248	53	98	D1	5A	CC	4C	D2	18	6B	88	D7	10	AF	21	5E	43	FD	12	81	D2	AC	51	43	6A	84	6C	DF	10	05	05	05	
00000256	33	22	D7	18	3F	D5	AC	98	3A	CD	F2	A5	F5	7F	B3	62	EA	A7	18	4F	99	BB	35	C4	66	CA	D8	05	05	05	05	
00000264	19	33	93	C2	C2	DF	57	3F	95	63	A6	16	83	99	A9	DF	9C	B9	AA	A7	F4	1D	06	B3	35	C4	CC	47	05	05	05	05
00000272	EC	1B	62	C1	B2	35	C4	AF	41	9B	18	7E	23	8A	A2	C5	BB	48	FE	7A	FD	27	2C	0D	F7	4D	CF	26	05	05	05	05
00000280	B8	44	97	85	35	A4	14	B3	D3	78	AD	21	36	8A	C1	CE	98	1E	B3	08	6B	88	ED	03	C1	1A	E2	C6	05	05	05	05
00000288	44	1A	1D	31	1C	37	67	A8	26	7F	C4	49	3F	43	5C	0A	80	21	6C	B9	60	69	2D	E6	ED	91	69	B2	05	05	05	05
00000296	79	4A	A5	C4	30	24	2F	CF	7C	77	2C	4B	13	37	C5	31	93	33	9D	71	33	DF	74	8E	4B	BC	EE	96	05	05	05	05
00000304	F5	5D	9C	89	79	9D	8A	5F	E2	49	F9	62	CC	D2	67	E4	D8	C4	4E	28	FB	F9	C3	78	5C	7C	4D	61	05	05	05	05
00000312	1D	87	DE	AF	E4	18	8D	6D	66	D2	70	DC	E4	55	E2	52	F6	D2	78	85	B1	37	C4	13	85	1A	E3	65	05	05	05	05
00000320	08	40	6B	31	8D	31	79	4D	88	9F	C1	B8	3C	F3	DD	B1	34	E6	B2	E4	92	E1	98	C9	99	9A	EC	67	05	05	05	05
00000328	34	2B	65	CE	14	AF	27	18	F2	92	97	65	FD	F4	A1	C3	9A	95	B2	7E	7A	2F	A3	A3	86	AF	34	AF	05	05	05	05
00000336	35	C4	1C	B1	72	BF	F2	EE	E8	63	39	66	5E	69	6E	35	C7	F7	0D	F1	45	07	D6	10	BF	06	C6	90	05	05	05	05
00000344	9C	9E	31	24	A7	83	74	77	BD	89	4F	6B	34	66	85	72	B2	C4	C4	E4	FB	6E	F1	51	CC	CC	B2	FE	05	05	05	05

ANSI ASCII

IHDR ã ã  
 Uzf IDÅ"i'házUvItUyEç  
 <rxIúgn\*H0\_ uáU P ( ŠTæç\_

TIME.png  
 D:\盘\安海杯\Misc\趣\开始

文件大小: 54.1 KB  
 55,442 字节

缺省编辑模式: 原始的  
 状态: 原始的  
 撤销级数: 0  
 反向撤销: 暂无信息

创建时间: 2020/09/08  
 20:42:33  
 最后写入时间: 2020/08/24  
 15:47:13

属性: A  
 图标: 0

模式: 十六进制  
 偏移地址: decimal  
 每页字节数: 51x28=1428

当前窗口: 1  
 窗口总数: 1

剪贴板: 可用

暂存文件夹: 4.3 GB 空余  
 C:\Users\YS\_Neko\winhex

页 1 / 39 偏移地址: 0 = 0 选项: 无 大小:

发现IHDR数据块和空缺的文件头，修复文件头保存后成功打开PS: IHDR为png特有的数据块



现在: 1599576976

控制: ■ 停止

时间戳

1599576768

秒(s)



转换 >>

北京时间

时间

202008241528

北京时间

转换 >>

1598254080

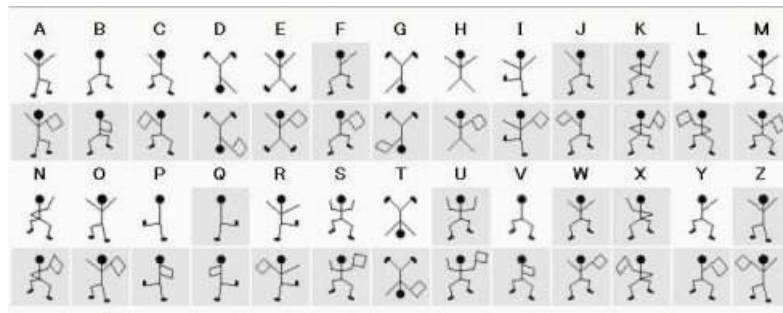
秒(s)



利用时间戳成功解压压缩包得到一张图片



经查找这是出自福尔摩斯探案集中的跳舞的人密码，密码对应为



解密为: WATCHTHEVIDEO(观看这个视频)

然后查看图片信息发现图片大小明显过大, 4.45M, 放进Winhex打开再次发现zip文件头



WinHex - [跳起来兄弟盟.png]

文件(F) 编辑(E) 搜索(S) 导航(N) 查看(V) 工具(T) 专业工具(I) 选项(O) 窗口(W) 帮助(H) 19.8 x86

案件数据 跳起来兄弟盟.png

位置管理器 (全部) 9 项目

Offset	搜索结果	时间
4140583	504B0304	2020/09/08 2...
3516937	504B0304	2020/09/08 2...
3143888	504B0304	2020/09/08 2...
2538333	504B0304	2020/09/08 2...
2056057	504B0304	2020/09/08 2...
1293113	504B0304	2020/09/08 2...
34380	504B0304	2020/09/08 2...
34340	504B0304	2020/09/08 2...
34305	504B0304	2020/09/08 2...

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
02538004	9B	CB	BF	FE	F2	E5	AF	BE	7A	FD	AB	AF	DE	7C	F6	ED	F9	E7	4F	2F	BE	7D	79	F3	FA	26	BF	58
02538005	37	57	BB	EE	7C	53	5F	6D	9B	4D	31	EE	6A	67	DF	79	DB	CE	DB	77	FE	B6	71	73	91	93	CC	72
02538006	D3	CE	8A	CA	31	AD	BC	A3	A7	97	F5	37	6F	F2	42	BD	65	51	3F	EA	A9	D0	26	2F	6B	B1	1A	2C
02538008	17	7B	51	D3	E5	10	34	DD	20	AB	28	0A	71	82	BC	6E	BF	CB	AF	EA	7E	9B	A6	EE	72	16	A5	81
02538116	1D	DA	43	E2	39	38	D5	6A	9A	41	C8	3E	7C	F7	C9	C3	B3	13	73	43	95	0F	A9	05	25	2A	2C	4D
02538144	F3	59	AD	C3	24	1E	75	DB	90	C9	13	39	C1	53	D3	37	66	7B	81	A0	D6	4C	5B	23	3C	A7	B3	99
02538172	96	F3	0A	E3	74	32	85	27	47	41	04	30	05	AE	87	79	BC	79	F9	72	7B	B7	56	87	0F	F1	17	9B
02538200	04	25	48	24	7C	77	E8	D4	EB	5F	E6	95	E3	86	30	E3	6F	9F	BE	1E	86	28	4D	57	44	B7	C9	74
02538228	B1	5C	AE	72	63	B8	5A	19	2D	00	24	9B	28	E9	9F	3E	FF	94	B7	E5	54	1E	19	9C	A5	3B	85	51
02538256	0F	B1	18	C3	C6	09	A5	78	04	20	D2	F8	D6	8F	0E	EE	06	FA	19	B8	53	6A	CA	1E	F3	92	39	08
02538284	26	8C	A9	BC	15	99	79	A9	53	CB	70	32	93	A2	F8	FC	86	1B	9A	43	D8	10	E3	96	1B	5B	E3	FF
02538312	0F	47	D8	FD	38	08	F1	EE	88	00	00	00	00	49	45	4E	44	AE	42	60	82	4B	03	04	0A	00	00	00
02538340	00	00	00	5C	95	0D	51	33	4D	E1	66	46	3D	09	00	46	3D	09	00	0F	00	00	00	66	6C	61	67	2F
02538368	66	6C	61	67	2F	34	2E	70	6E	67	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	44	49	44	52	00	00
02538396	02	52	00	00	01	BA	08	02	00	00	00	4C	42	3F	56	00	00	00	04	67	41	4D	44	00	00	B1	8F	0B
02538424	FC	61	05	00	00	00	09	70	48	59	73	00	00	0E	C3	00	00	0E	C3	01	C7	6F	A8	64	00	00	FF	B2
02538452	49	44	41	54	78	5E	EC	FD	05	60	1C	57	96	F6	0F	B7	A4	66	A8	2E	68	94	1A	A5	6E	31	4B	96
02538480	6D	99	99	99	99	99	99	99	E2	80	ED	24	76	E2	C4	8E	1D	87	C1	21	C7	6E	18	C2	CC	99	70	26
02538508	C9	60	32	F8	0E	EE	CE	CE	CC	EE	FA	7B	6E	1D	E9	AA	54	2D	39	76	32	33	7B	7E	F8	7F	3D	BF
02538536	A9	DC	3A	75	2E	D4	AD	D2	79	FA	54	57	55	1B	6C	16	87	D5	6C	D7	E1	76	49	82	53	B4	5B	9D
02538564	B4	0A	1F	87	5D	70	39	DD	56	AB	DD	62	B5	11	36	BB	DD	EE	70	3A	5C	2E	A7	48	70	09	6E	2C
02538592	61	21	60	C7	AA	DB	2D	0A	B0	38	5C	64	75	D8	9D	28	63	69	B3	D7	B0	8A	A5	D5	6C	B5	98	2C
02538620	00	85	06	23	5B	B4	00	75	07	D0	32	15	CC	16	AB	09	D5	CD	18	0C	06	D9	80	CD	E2	52	71	DA
02538648	ED	2E	78	C2	8F	7A	21	CC	26	0B	5A	E1	E3	47	0B	1C	6E	A4	C6	A9	23	C0	37	A1	60	34	99	01
02538676	0A	E4	A0	F5	6F	18	15	1A	B7	58	AD	30	AA	7B	C1	EA	5A	6C	18	1D	4D	2A	A8	C3	C3	C0	30	A5
02538704	B2	CD	2C	D9	2D	32	B0	59	25	93	C9	61	32	DB	5A	C3	6C	71	58	AC	4E	0D	2E	B3	D9	65	32	B9
02538732	8C	66	A7	D1	EC	00	26	8B	D3	6C	75	9A	6D	28	5B	4D	D8	45	9B	CD	C2	8E	15	8E	98	C5	6C	37
02538760	9B	B0	67	6C	5A	9B	0D	95	03	0B	46	48	3B	88	55	DA	41	43	46	26	96	64	C1	12	C5	2C	A3	09
02538788	B4	B8	E3	38	F4	64	D1	DA	79	9B	AD	81	AD	68	56	37	99	00	CD	A1	41	0E	9B	52	9B	C3	25	48
02538816	4E	97	E8	70	BA	09	BB	5D	30	5B	EC	46	13	86	6A	CD	CA	B2	64	66	9A	0C	19	46	0E	56	F9	68
02538844	01	7A	D1	42	A3	E2	DD	01	8B	15	7B	CD	C0	54	53	83	04	B5	4F	68	8E	05	79	B2	76	F8	0E	A2
02538872	20	B8	23	6E	31	26	4A	71	8F	47	48	51	72	D3	C1	26	20	C9	09	94	E1	73	09	C8	4D	EB	C9	1B
02538900	D1	00	63	52	51	52	84	D7	5B	40	48	72	32	1D	8F	27	3F	1D	5E	97	A3	73	20	74	3E	E4	28	16

页 2,748 / 5,052 偏移地址: 2,538,333 = 80 选择: 无 大小: 无

跳起来兄弟盟.png

D:\E盘\安海杯\Misc\跳起来兄弟盟.png

文件大小: 4.5 MB  
4,667,559 字节

状态: 原始的

撤销级数: 0

反向撤销: 暂无信息

创建时间: 2020/09/08 22:59:27

最后写入时间: 2020/08/24 15:28:18

属性: A

图标: 0

模式: 十六进制

偏移地址: decimal

每页字节数: 33x28=924

当前窗口: 2

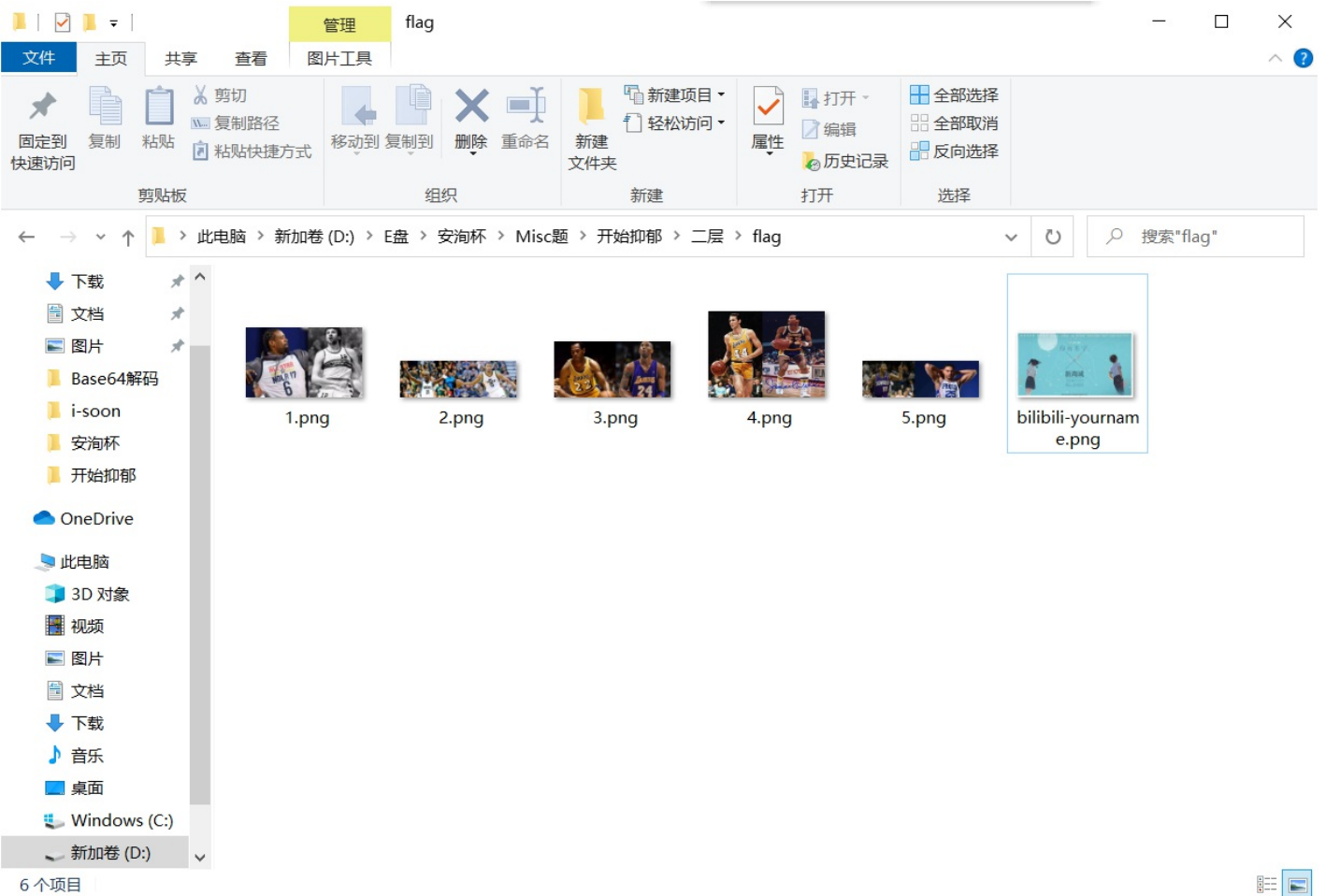
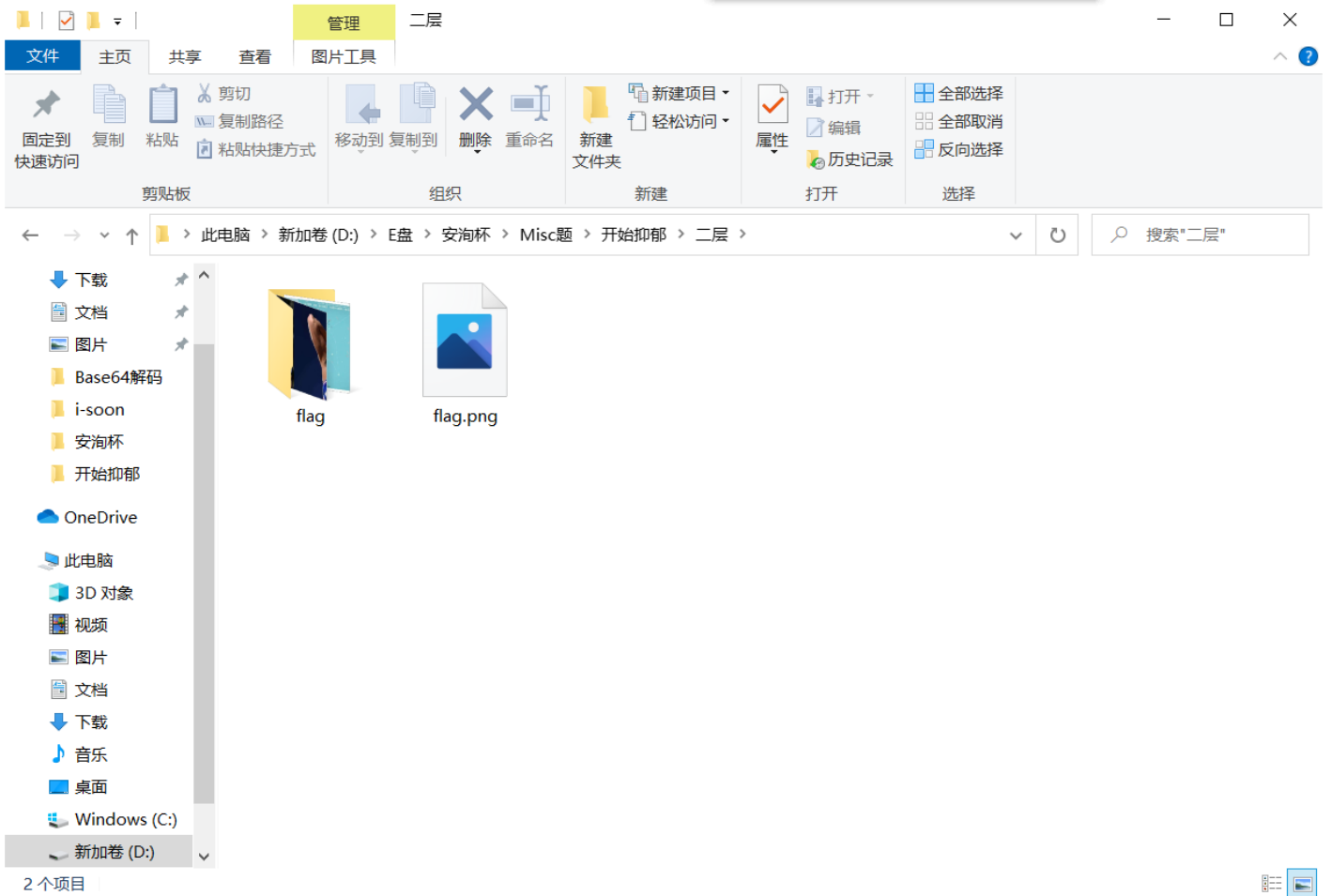
窗口总数: 1

剪贴板: 可用

暂存文件夹: 5.9 GB 空余

C:\Users\YS\_Neko\winhex

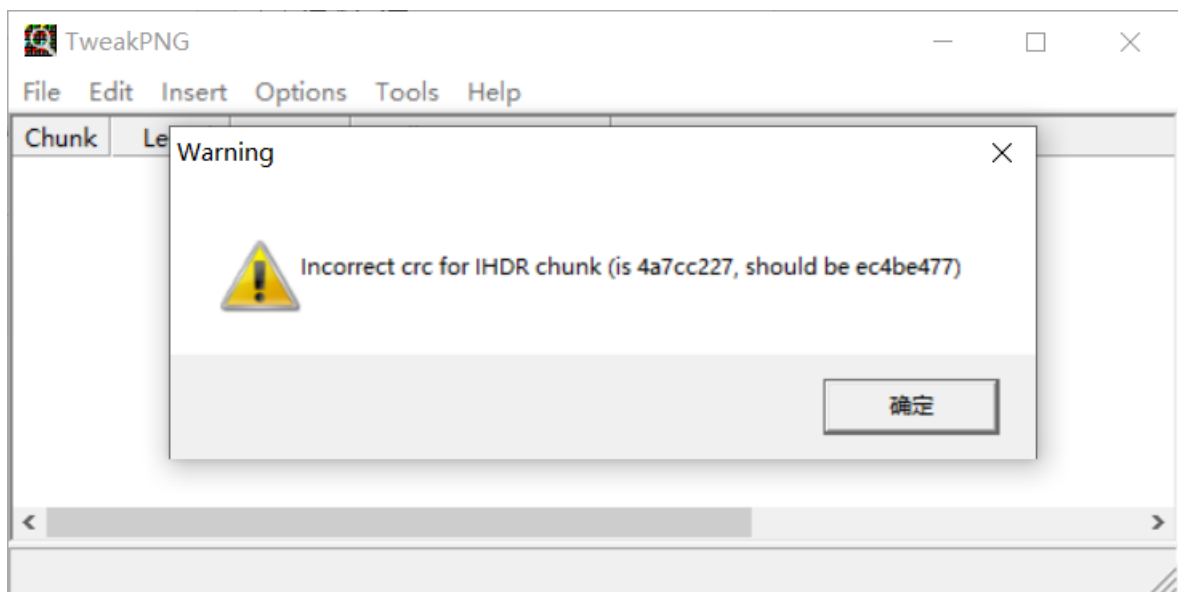
修改后缀为zip后打开得到几张图片



其中flag.png无法打开，Winhex打开发现又是缺少文件头，补充后打开得到一个表情包

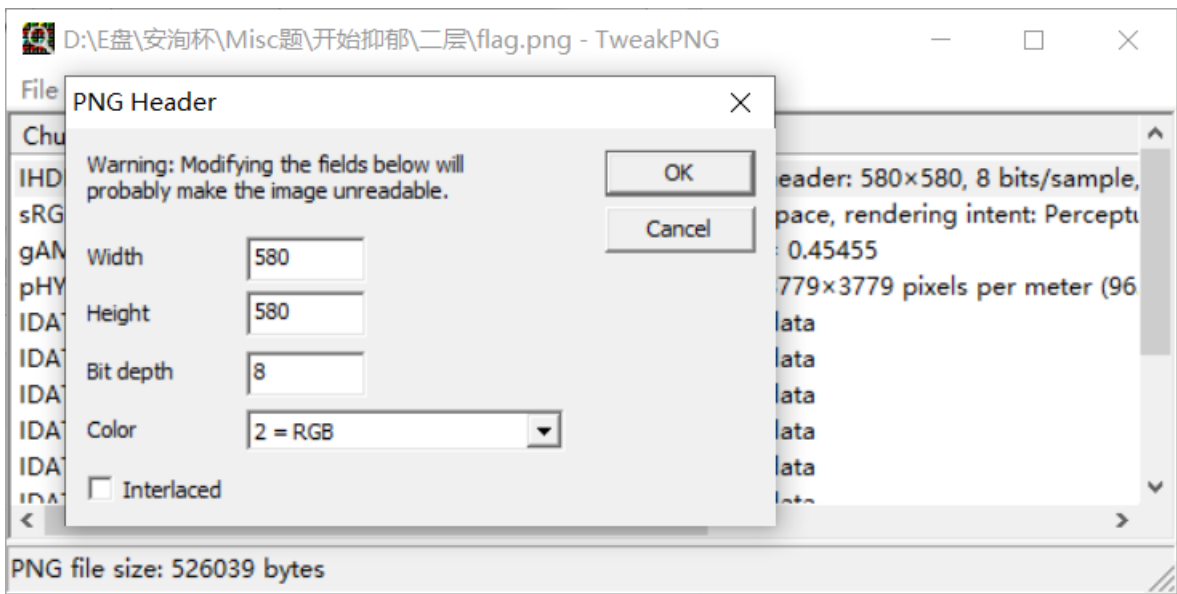


观察图片发现少了一截，用TweakPNG校验发现数据块异常



双击IHDR块修改图片宽高得到flag格式





flag格式: {1234-1234-ABCDEFGHI-ABCDEFGHIJK-1234}

得到格式后通过flag文件夹里的几张图片分别获取每段flag

flag文件夹里有六张图片，前五张图片球星的编号分别对应Bilibili中电影《你的名字》的五个时间片段，分别为

6分12秒/21分05秒/22分24秒/44分52秒/93分25秒



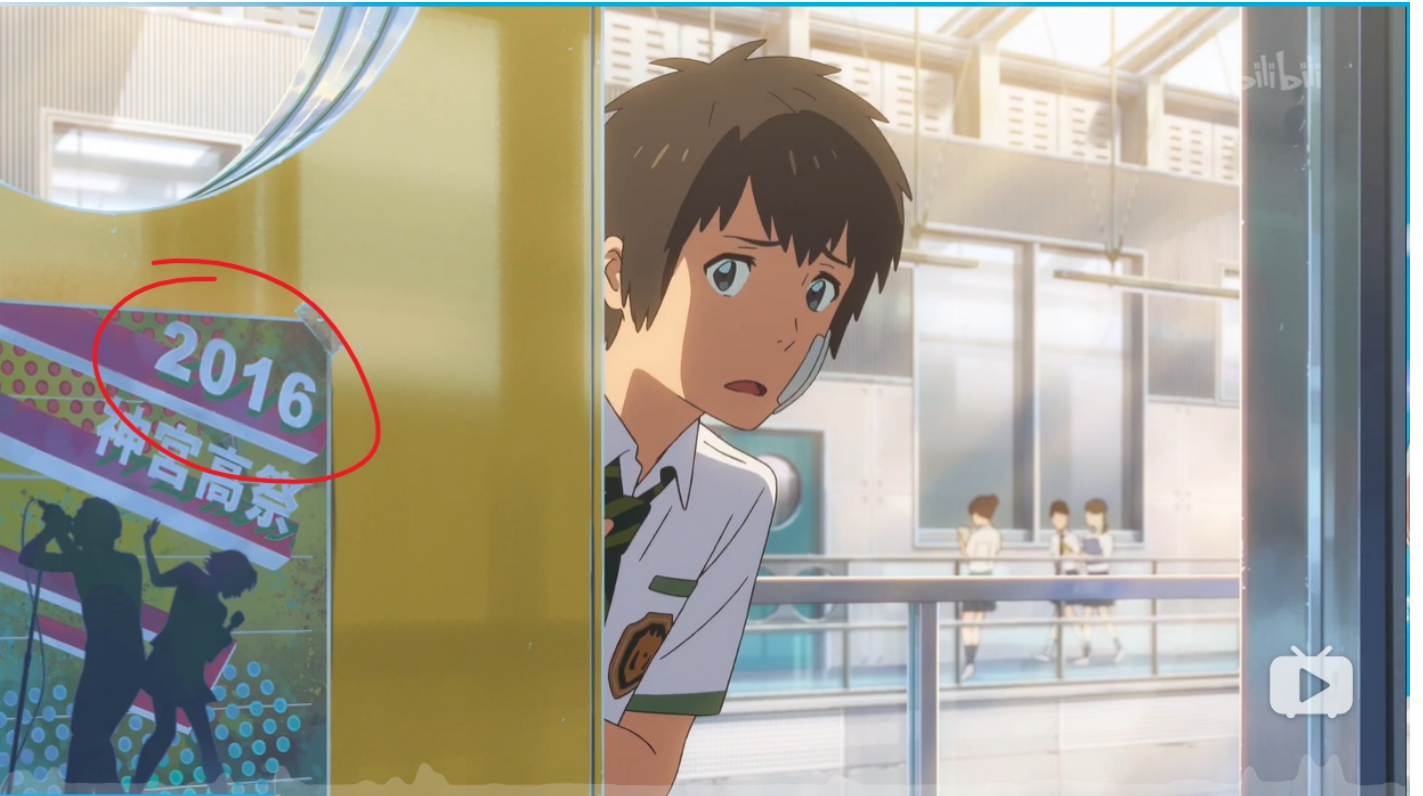
193 人正在看, 16110 条弹幕



发个友善的弹幕见证当下

弹幕礼仪 >

发送



193 人正在看, 16113 条弹幕

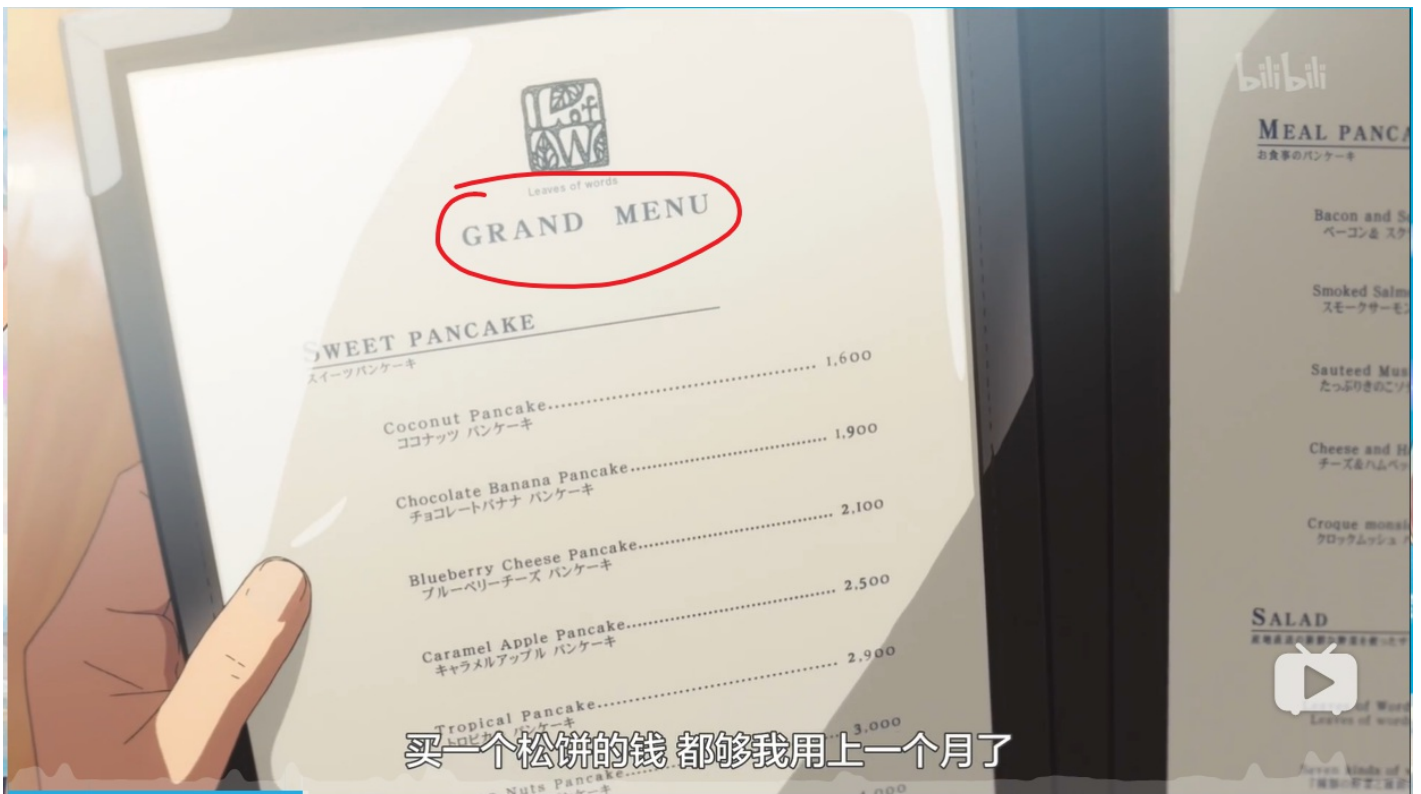


发个友善的弹幕见证当下

弹幕礼仪 >

发送





202 人正在看, 16113 条弹幕



发个友善的弹幕见证当下

弹幕礼仪 >

发送



202 人正在看, 16113 条弹幕



发个友善的弹幕见证当下

弹幕礼仪 >

发送



将五个线索填入flag格式并大写，得到最终flag:

```
flag{1200-2016-GRANDMENU-RCHITECTURE-1335}
```