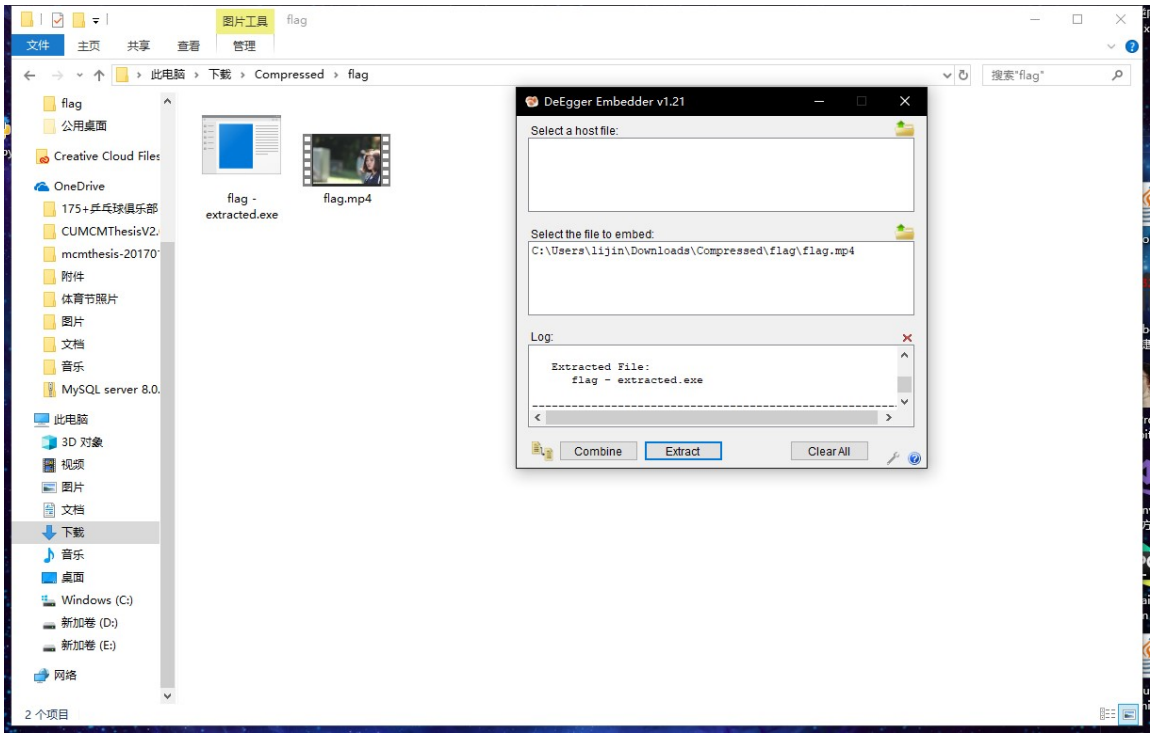
HGAME WRITEUP WEEK2——FzWjScJ

MISC

0x01 时至今日，你仍然是我的光芒

题目是一个zip文件，解压出来是一个mp4文件，据hint下载了一个DeEgger Embedder，打开解析出一个exe虽然不知道是什么，但是丢到winhex里看了一下!



发现有一个JFIF文件头，就把后缀换成jpg，得到一个似曾相识的照片233

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII	UTF-8
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01	ÿØÿà JFIF	□ □□JFIF□□□□□□
00000010	00	01	00	00	FF	DB	00	43	00	08	06	06	07	06	05	08	ÿÛ C	□□□□□ □□□□□□□□
00000020	07	07	07	09	09	08	0A	0C	14	0D	0C	0B	0B	0C	19	12		□□□ □ □□ □□□□□□
00000030	13	0F	14	1D	1A	1F	1E	1D	1A	1C	1C	20	24	2E	27	20	$.'	□□□ □ □ $.'
00000040	22	2C	23	1C	1C	28	37	29	2C	30	31	34	34	34	1F	27	",# (7),01444 '	",# (7),01444 '
00000050	39	3D	38	32	3C	2E	33	34	32	FF	DB	00	43	01	09	09	9=82<.342ÿÛ C	9=82<.342□ □
00000060	09	0C	0B	0C	18	0D	0D	18	32	21	1C	21	32	32	32	32	2! !2222	□□□□ □2! !2222
00000070	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	2222222222222222	2222222222222222
00000080	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	2222222222222222	2222222222222222
00000090	32	32	32	32	32	32	32	32	32	32	32	32	32	32	FF	C0	2222222222222ÿÀ	22222222222222□
000000A0	00	11	08	02	5F	04	38	03	01	22	00	02	11	01	03	11	_ 8 "	□□_□8□□"□□□□□□
000000B0	01	FF	C4	00	1F	00	00	01	05	01	01	01	01	01	01	00	ÿÄ	□□ □□□□□□□□□□
000000C0	00	00	00	00	00	00	00	01	02	03	04	05	06	07	08	09		□□□□□□□
000000D0	0A	0B	FF	C4	00	B5	10	00	02	01	03	03	02	04	03	05	ÿÄ µ	□□ □□□□□□□□□□
000000E0	05	04	04	00	00	01	7D	01	02	03	00	04	11	05	12	21	} !	□□□□□□}□□□□□□□□!
000000F0	31	41	06	13	51	61	07	22	71	14	32	81	91	A1	08	23	1A Qa "q 2 ‘¡ #	1A□□Qa□"q□2□ #
00000100	42	B1	C1	15	52	D1	F0	24	33	62	72	82	09	0A	16	17	B±Á RÑð$3br,	B□ □ br□ □
00000110	18	19	1A	25	26	27	28	29	2A	34	35	36	37	38	39	3A	%&'()*456789:	□□□%&'()*456789:
00000120	43	44	45	46	47	48	49	4A	53	54	55	56	57	58	59	5A	CDEFGHIJSTUVWXYZ	CDEFGHIJSTUVWXYZ
00000130	63	64	65	66	67	68	69	6A	73	74	75	76	77	78	79	7A	cdefghijstuvwxyz	cdefghijstuvwxyz
00000140	83	84	85	86	87	88	89	8A	92	93	94	95	96	97	98	99	ƒ„…†‡ˆ‰Š‘’“”•–—˜™	□ □ □ □
00000150	9A	A2	A3	A4	A5	A6	A7	A8	A9	AA	B2	B3	B4	B5	B6	B7	š¢£¤¥¦§¨©ª²³´µ¶·	□ □ □ □
00000160	B8	B9	BA	C2	C3	C4	C5	C6	C7	C8	C9	CA	D2	D3	D4	D5	¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕ	□ □ □ □
00000170	D6	D7	D8	D9	DA	E1	E2	E3	E4	E5	E6	E7	E8	E9	EA	F1	Ö×ØÙÚáâãäåæçèéêñ	□ □ □ □
00000180	F2	F3	F4	F5	F6	F7	F8	F9	FA	FF	C4	00	1F	01	00	03	òóôõö÷øùúÿÄ	□ □ □ □□□
00000190	01	01	01	01	01	01	01	01	01	00	00	00	00	00	00	01		
000001A0	02	03	04	05	06	07	08	09	0A	0B	FF	C4	00	B5	11	00	ÿÄ µ	□□□□□□□ □□ □□
000001B0	02	01	02	04	04	03	04	07	05	04	04	00	01	02	77	00	w	□□□□□□□□□□□□□□□w□
000001C0	01	02	03	11	04	05	21	31	06	12	41	51	07	61	71	13	!1 AQ aq	□□□□□□!1□□AQ□aq□
000001D0	22	32	81	08	14	42	91	A1	B1	C1	09	23	33	52	F0	15	"2 B‘¡±Á #3Rð	"2□ □ #3R□
000001E0	62	72	D1	0A	16	24	34	E1	25	F1	17	18	19	1A	26	27	brÑ $4á%ñ &'	□ 4□ □□□&'
000001F0	28	29	2A	35	36	37	38	39	3A	43	44	45	46	47	48	49	()*56789:CDEFGHI	()*56789:CDEFGHI
00000200	4A	53	54	55	56	57	58	59	5A	63	64	65	66	67	68	69	JSTUVWXYZcdefghi	JSTUVWXYZcdefghi
00000210	6A	73	74	75	76	77	78	79	7A	82	83	84	85	86	87	88	jstuvwxyz,ƒ„…†‡ˆ	jstuvwxyz□ □
00000220	89	8A	92	93	94	95	96	97	98	99	9A	A2	A3	A4	A5	A6	‰Š‘’“”•–—˜™š¢£¤¥¦	□ □ □ □
00000230	A7	A8	A9	AA	B2	B3	B4	B5	B6	B7	B8	B9	BA	C2	C3	C4	§¨©ª²³´µ¶·¸¹ºÂÃÄ	□ □ □ □
00000240	C5	C6	C7	C8	C9	CA	D2	D3	D4	D5	D6	D7	D8	D9	DA	E2	ÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚâ	□ □ □ □
00000250	E3	E4	E5	E6	E7	E8	E9	EA	F2	F3	F4	F5	F6	F7	F8	F9	ãäåæçèéêòóôõö÷øù	□ □ □ □
00000260	FA	FF	DA	00	0C	03	01	00	02	11	03	11	00	3F	00	E8	úÿÚ ? è	□ □□□□□□□□?□□
00000270	34	B3	8D	26	CF	FE	B8	27	F2	AB	A1	87	AD	64	69	B3	4³ &Ïþ¸'ò«¡‡-di³	&□ □ □
00000280	E3	4B	B3	FF	00	AE	09	FC	85	5A	13	73	5F	35	28	5E	ãK³ÿ ® ü…Z s_5(^	□ □□ Z□s_5(^
00000290	6C	F5	63	F0	A2	F6	FE	29	3C	CA	AB	E7	7B	D3	3C	FA	lõcð¢öþ)<Ê«ç{Ó<ú	l□ □ ƀ □ □
000002A0	7E	CC	65	DD	FC	D3	83	64	D5	35	94	13	52	89	40	A9	~ÌeÝüÓƒdÕ5” R‰@©	□ d□ R□
000002B0	70	02	D0	34	B9	A8	16	5E	29	DE	65	4B	80	58	79	35	p Ð4¹¨ ^)ÞeK€Xy5	□□ □^)□ Xy5
000002C0	13	35	0C	D5	0C	8F	F2	D0	A2	21	C5	B1	4D	DF	50	97	5 Õ òÐ¢!Å±MßP—	□5□□ T !ű M□
000002D0	A4	DD	57	CA	2B	93	03	CD	3F	3C	55	70	DC	D4	A3	A5	¤ÝWÊ+“ Í?<UpÜÔ£¥	□ □ <Up□
000002E0	0D	0A	E3	B7	51	9A	67	7A	4A	2C	31	5C	F1	55	24	35	ã·QšgzJ,1\ñU$5	□ gzJ,1\□
000002F0	65	BA	55	59	7A	D5	C5	0C	88	3F	35	34	6D	55	8F	DF	eºUYzÕÅ ˆ?54mU ß	e□ □ ?54mU□
00000300	15	3A	03	5A	CA	20	8B	E8	D5	61	5E	A9	46	6A	C0	6E	: ZÊ ‹èÕa^©FjÀn	□Z□ □ Fj□
00000310	2B	9A	51	19	29	90	03	47	98	3D	6A	AB	39	C9	A8	CC	+šQ) G˜=j«9É¨Ì	Q□)□ =j□ ˙
00000320	8D	9E	94	D5	3B	81	7C	48	29	C1	C1	1D	6A	9A	2C	8F	ž”Õ; |H)ÁÁ jš,	□ □ □ □
00000330	D0	1A	9B	CB	91	7B	66	87	4D	0D	45	92	EF	1E	B4	FD	Ð ›Ë‘{f‡M E’ï ´ý	□□ f□ □ □
00000340	FC	75	AA	8C	C4	1E	69	CA	E7	18	A3	90	69	16	0B	D2	üuªŒÄ iÊç £ i Ò	□ □ □ □

之后便用上了hint2，outguess，看了看官方文档，大概使用方法是

```
outguess -r 【解密图片】 -k 【密码】 -t 【输出文件名称】
```

在这之后我便弯弯曲曲走了两个方法……

way1：

> Python来写脚本爆破，脚本是写出来了，但是因为python读写本地文件太慢，差不多三四行outguess命令才进行一次读写，所以就没了附上那个无法跑出来的exp.py（但是一开始我觉得气不过，就用python命令行手动爆破了一遍，强行减慢命令执行时间，也手动爆破出来了
>
> 密码：securitypassword，flag：hgame{Whataya_Want_From_Me}

```
#!/usr/bin/env python
# coding=utf-8

import os
with open("flag.txt","r") as f1:
        with open("password.txt","r") as f2:
            with open("useful.txt",w) as f3:
                passwords = f2.readlines()
                for password in passwords:
                    password = password.strip("\n").strip("\r")
                    print password
                    os.popen("outguess -r flag.jpg -t flag.txt -k "+ bytes(password[0]))
                    $a.read()
                    print f1.readline()
                    if f1.readline(5) == 'hgame':
                        print "Find!"
                       print f1.readline()
                        f1.close()
                        f2.close()
                        break
                    else:
                        continue
                print "No useful Password!"
                f1.close()
                f2.close()
```

way2：

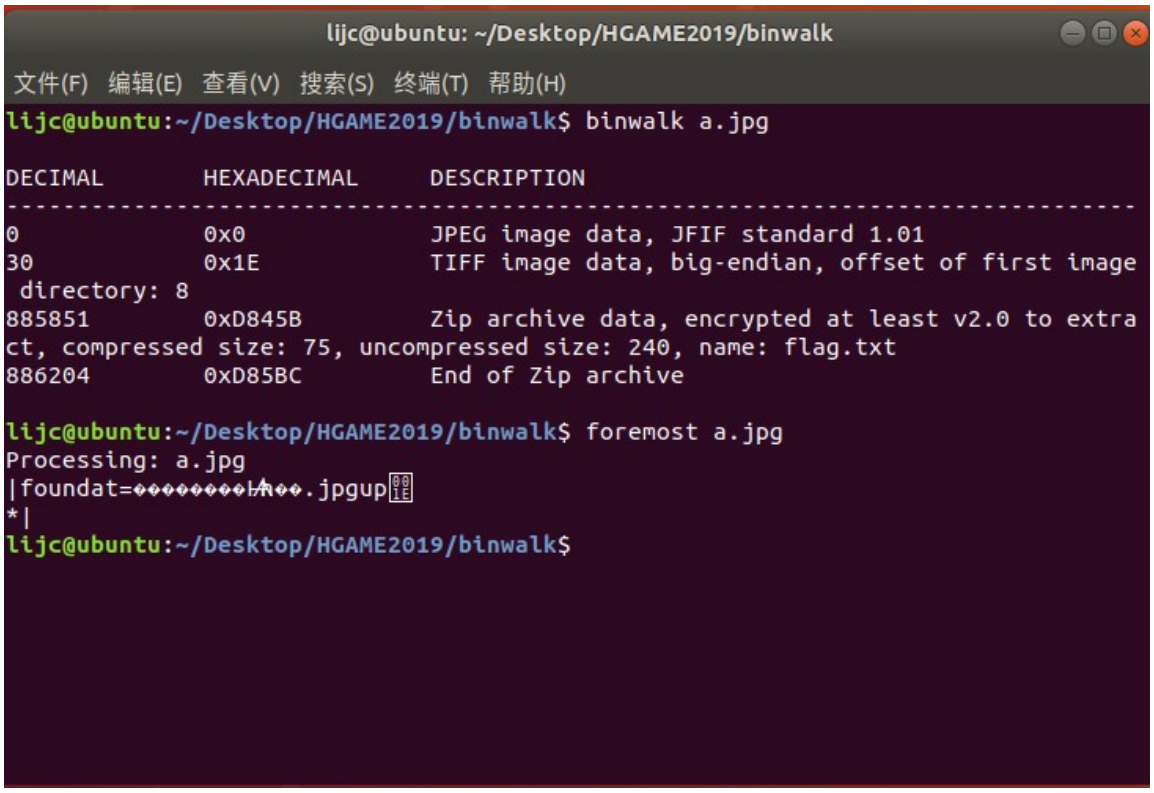
> 在问过出题人后又得到了一种新的脚本书写方法，用shell写脚本，在稍短的自学shell语法后写出了此题的shell脚本

```
#!/bin/bash
  echo "Begin"
  echo"********************************"
  for password in `cat $1`;
  do
      outguess -r flag.jpg -k $password -t flag.txt
      grep "hgame" flag.txt > /dev/null
      if [[ $? -eq 0 ]];
     then
        echo "********************************"
```

```
        echo "password is:$password"
        echo ""
        echo "Flag is:`cat flag.txt`"
        echo "**********************************"
        exit
        fi
    done
```

0x02至少像那雪一样

打开题目，~~一份色图~~,binwlak+foremost



然后用WinRAR查看出来的zip文件，发现有flag.txt以及原来那张图，这里推测应该是明文攻击zip文件，这里打开Advanced Archive Password Recovery进行明文攻击，打开flag.txt但是又是啥都没有……丢进Winhex里看

flag.txt

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	09	20	20	09	20	09	09	09	09	20	20	09	09	20	20	20
00000010	09	20	20	09	09	09	09	20	09	20	20	09	20	20	09	20
00000020	09	20	20	09	09	20	09	20	09	20	20	20	20	09	20	20
00000030	09	20	09	09	09	09	09	20	09	20	20	20	09	20	09	09
00000040	09	20	09	20	20	20	20	20	09	20	09	09	20	20	09	09
00000050	09	20	20	09	09	20	09	20	09	20	20	09	09	09	09	20
00000060	09	09	20	20	09	20	09	20	09	20	20	20	09	20	09	09
00000070	09	20	09	20	20	20	20	20	09	20	09	09	20	20	09	09
00000080	09	09	20	20	09	09	09	20	09	20	20	09	20	09	20	20
00000090	09	20	20	09	09	20	09	20	09	20	09	20	20	20	20	20
000000A0	09	20	20	20	09	20	09	09	09	20	09	09	20	09	09	09
000000B0	09	20	20	09	09	09	09	20	09	20	20	20	09	20	09	09
000000C0	09	20	09	20	20	20	20	20	09	20	20	20	09	09	20	20
000000D0	09	20	20	09	20	20	20	09	09	09	20	20	09	09	09	09
000000E0	09	20	20	20	09	20	20	20	09	20	20	20	20	20	09	20

一开始疯狂百度，Google09，20加密，到最后貌似发现了一个什么规律，尝试把09替代成0，20替代成1，得到一串二进制数字

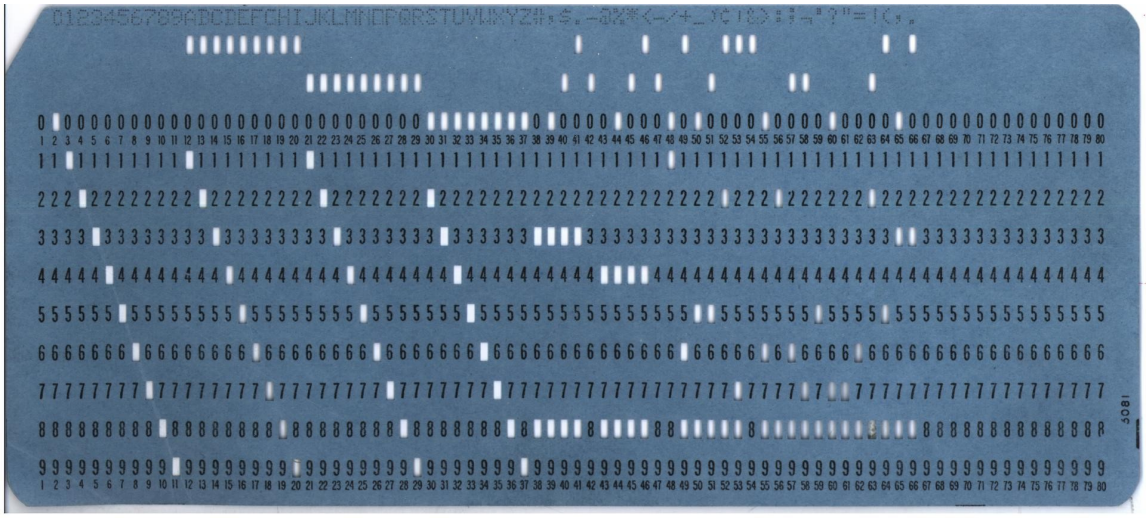
```
01101000011001110110000101101101011001010111101101000001011101000101111101001100011001010
```

之后转成16进制代码，得到`6867616D657B41745F4C656135745F4C316B655F744861745F736E30777D`在转成str字符串，得到flag：

`hgame{At_Lea5t_L1ke_tHat_sn0w}`

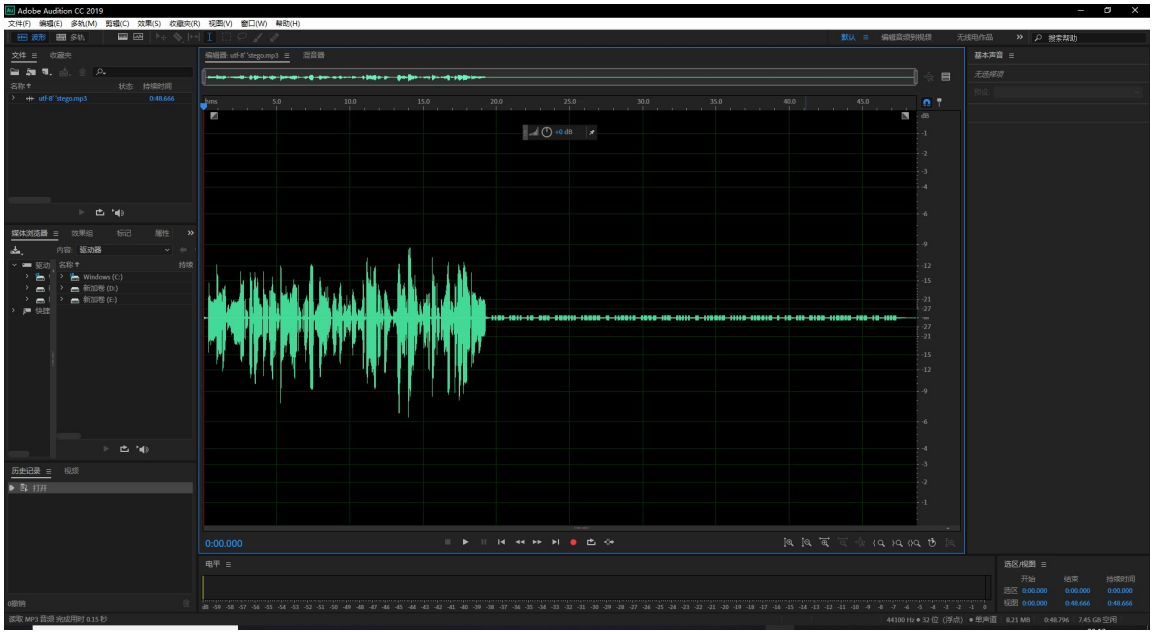
0x03旧时记忆

一道migo的脑洞题emmm，疯狂google搜图搜不到，在更新hint后得知是IBM打孔卡，对照着标准图一个个解得到flag:`hgame{0LD_DAY5%M3MORY}`



0x04听听音乐？

打卡题目是一段mp3文件，丢在Au里看看波纹~~（最后的波纹子）~~图，看长短应该是摩尔斯电码



记录下来

为:`..-./.-../.-/--./---.../.----/-/....-/.---/..-/...../-/....-/....-/..--.-/./.-/.../-.--/..--.-/.--/.-/...-`

翻译之后为:`hgame{1T_JU5T_4_EASY_WAV}`