

Misc 所见即为假

首先这个压缩文件有密码，我们考虑一下伪加密（百度出来伪加密猜测一波）

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	50	4B	03	04	14	00	00	00	08	00	07	76	F2	48	B7	EF	PK vòH·i
00000010	DC	83	03	00	00	00	01	00	00	00	05	00	00	00	31	2E	Üf 1.
00000020	74	78	74	33	04	00	50	4B	01	02	1F	00	14	00	09	00	txt3 PK
00000030	08	00	07	76	F2	48	B7	EF	DC	83	03	00	00	00	01	00	vòH·iÜf
00000040	00	00	05	00	24	00	00	00	00	00	00	00	20	00	00	00	\$
00000050	00	00	00	00	31	2E	74	78	74	0A	00	20	00	00	00	00	1.txt
00000060	00	01	00	18	00	B9	BB	82	5B	C0	E0	D1	01	22	A1	7C	'», [ÀàÑ "i
00000070	5B	C0	E0	D1	01	B3	10	74	58	C0	E0	D1	01	50	4B	05	[ÀàÑ ' tXÀàÑ PK
00000080	06	00	00	00	00	01	00	01	00	57	00	00	00	26	00	00	W &
00000090	00	00	00														

这是网图因为做的时候根本就没有保存截图

大致内容就是

假加密

压缩源文件数据区的全局加密应当为 00 00

且压缩源文件目录区的全局方式位标记应当为 09 00

真加密

压缩源文件数据区的全局加密应当为 09 00

且压缩源文件目录区的全局方式位标记应当为 09 00

所以基本上将压缩文件在 winhex 中打开之后直接拉到底找 0900 改为 0000 即可

此时取出图片，百度图片隐写，结合给出的提示 F5，应该是用到 F5-steganography

安装 F5-steganography

```
PS C:\Users\轩辕孟瑶\Desktop\F5-steganography-master> java Extract FLAG_IN_PICTURE.jpg -p N11D7CQon6dBsFLr
Huffman decoding starts
Permutation starts
10911744 indices shuffled
Extraction starts
Length of embedded file: 3283097 bytes
(1, 33554431, -7) code used
Incomplete file: only 0 of 3283097 bytes extracted
PS C:\Users\轩辕孟瑶\Desktop\F5-steganography-master>
```

分离出 output.txt 里面有一大串 16 进制字符串

尝试网络在线十六进制翻译失败了，得到学长提醒，将该字符串输入 winhex 得到 flag

应该是 rar 文件

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
000000	52	61	72	21	1A	07	01	00	33	92	B5	E5	0A	01	05	06	Rar! 3'pã
000010	00	05	01	01	80	80	00	B9	52	7A	EA	24	02	03	0B	A7	€€ 'Rzê\$ \$
000020	00	04	A7	00	20	CB	5B	DC	20	80	00	00	08	66	6C	61	\$ È[Ü€ fla
000030	67	2E	74	78	74	0A	03	02	9A	9D	6C	65	DF	CE	D5	01	g.txt š leßîö
000040	68	67	61	6D	65	7B	34	30	38	37	5E	7A	23	6D	73	77	hgame{4087^z#msw
000050	33	34	45	52	74	6E	46	55	79	71	70	4B	55	6B	32	64	34ERtnFUyqpKUk2d
000060	6D	4C	50	57	36	30	7D	1D	77	56	51	03	05	04	00	00	mLPW60} wVQ
000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Misc 地球上最后的夜晚

首先把 pdf 从头翻到尾也不知道讲了个什么

百度 pdf 与 CTF 的关系，得到 misc 中文档隐写的相关内容

用到工具 weStego，使用 decode 功能将密码分离

No password.pdf.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

Zip Password: OmR#O12#b3b%s*IW

然后得到一篇文章，看了一遍什么都没有。

猜测应该是 xml，于是按照网上的指引将其改为 zip，一个个翻，翻到了 flag

secret.xml

```
C: > Users > 轩辕孟瑶 > AppData > Local > Temp > Temp1_Last Evenings on Earth.zip > word > s
1  <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2  <flag>hgame{mkLbn8hP2g!p9ezPHqHuBu66SeDA13u1}</flag>
```