




BUU杂项

原创

暮w光  于 2021-10-31 02:01:25 发布  86  收藏

分类专栏: [# 杂项](#) 文章标签: [安全](#)

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/qi_SJQ_/article/details/121059404

版权



[杂项 专栏收录该内容](#)

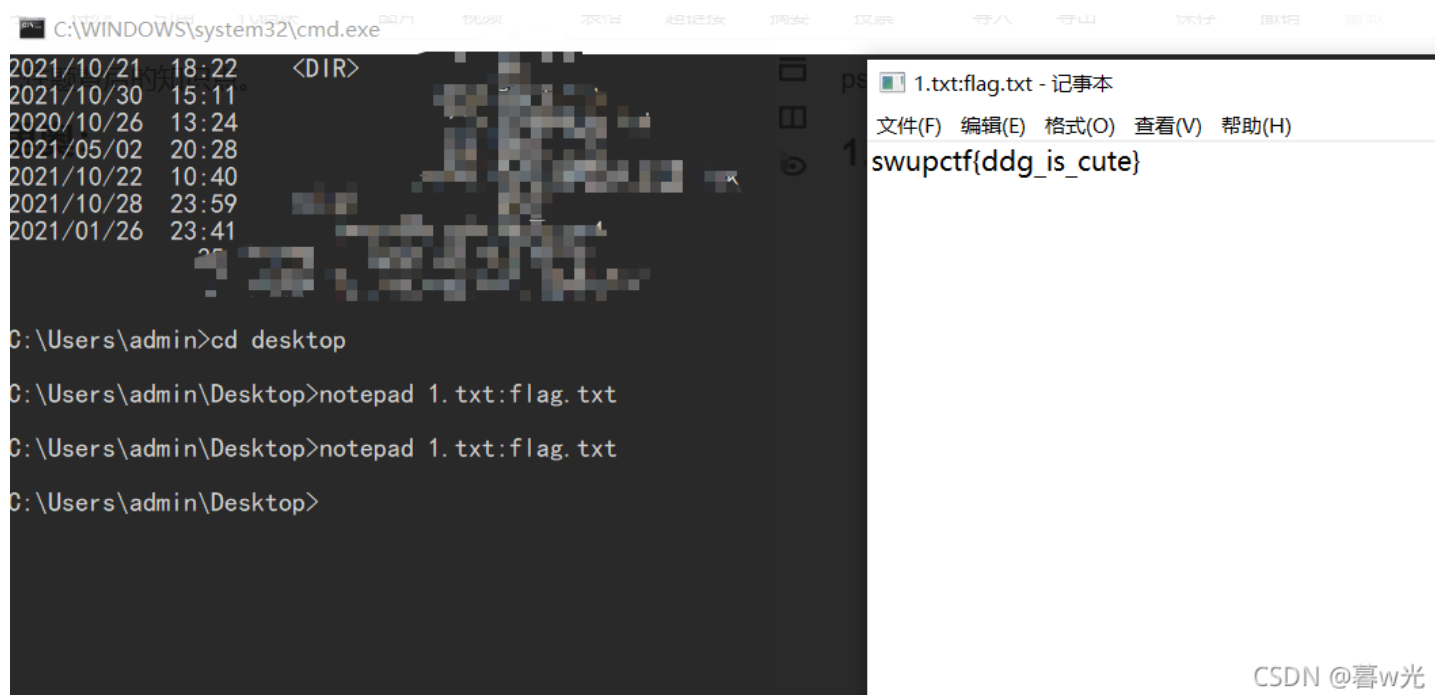
8 篇文章 0 订阅

订阅专栏

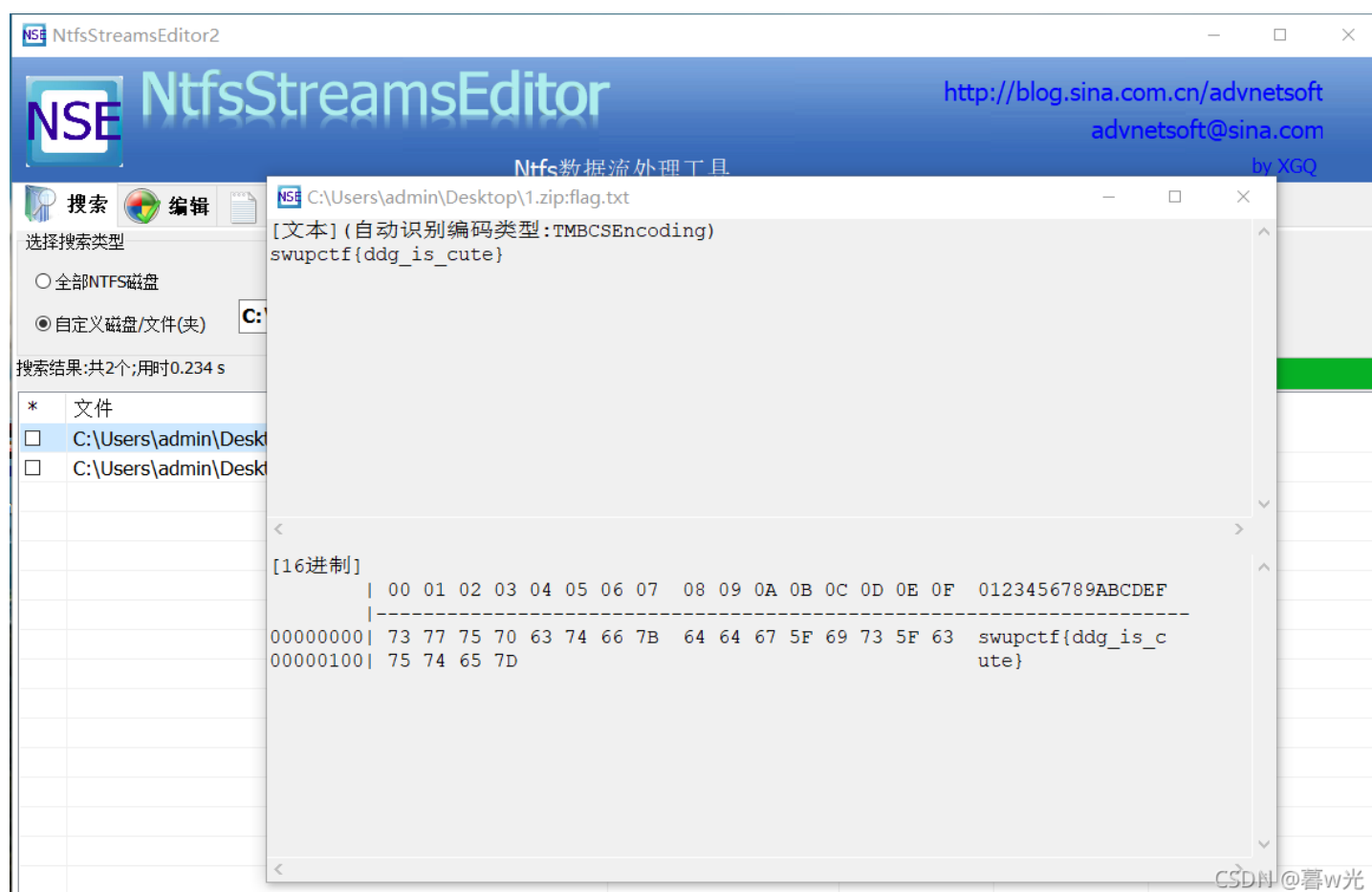
前言: 重点不在解题/写writeup而在于吸收/记住题背后的知识点。

1.[SWPU2019]我有一只马里奥:

NTFS流隐藏文件，(1) 直接cmd中解密 (2) 工具：



CSDN @暮w光

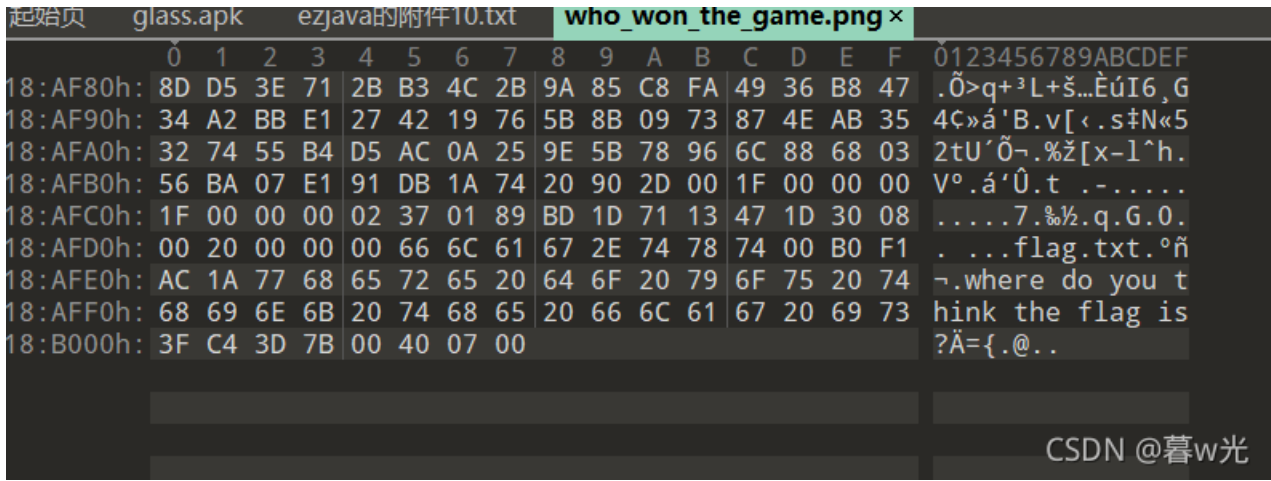


CSDN @暮w光

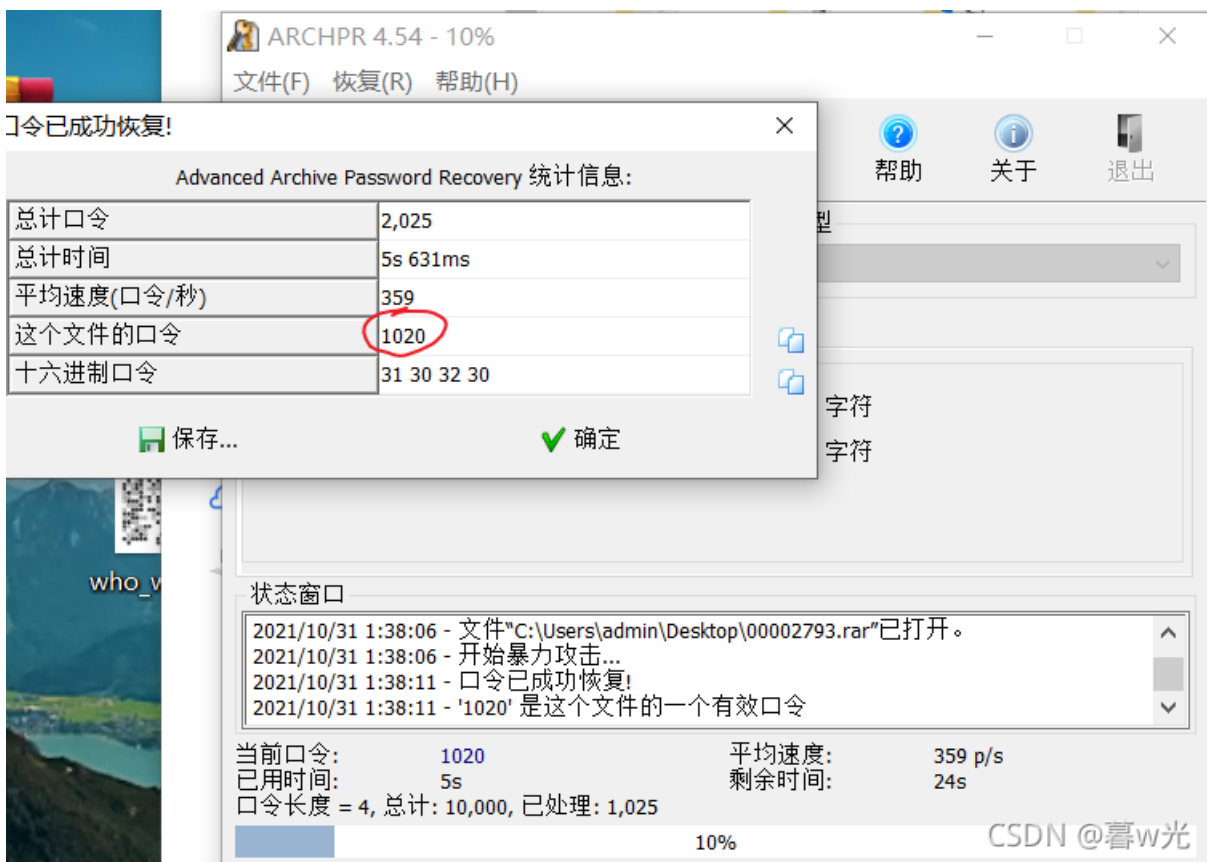
知识点：NTFS流隐写 (https://www.cnblogs.com/Chesky/p/ALTERNATE_DATA_STREAMS.html)
(https://blog.csdn.net/qq_45836474/article/details/111074356)

2.BUU [谁赢了比赛?]:

刚看照片以为是将黑棋白棋当成0,1来画二维码呢，吓我一跳，那个可不擅长，结果放010里发现想多了：

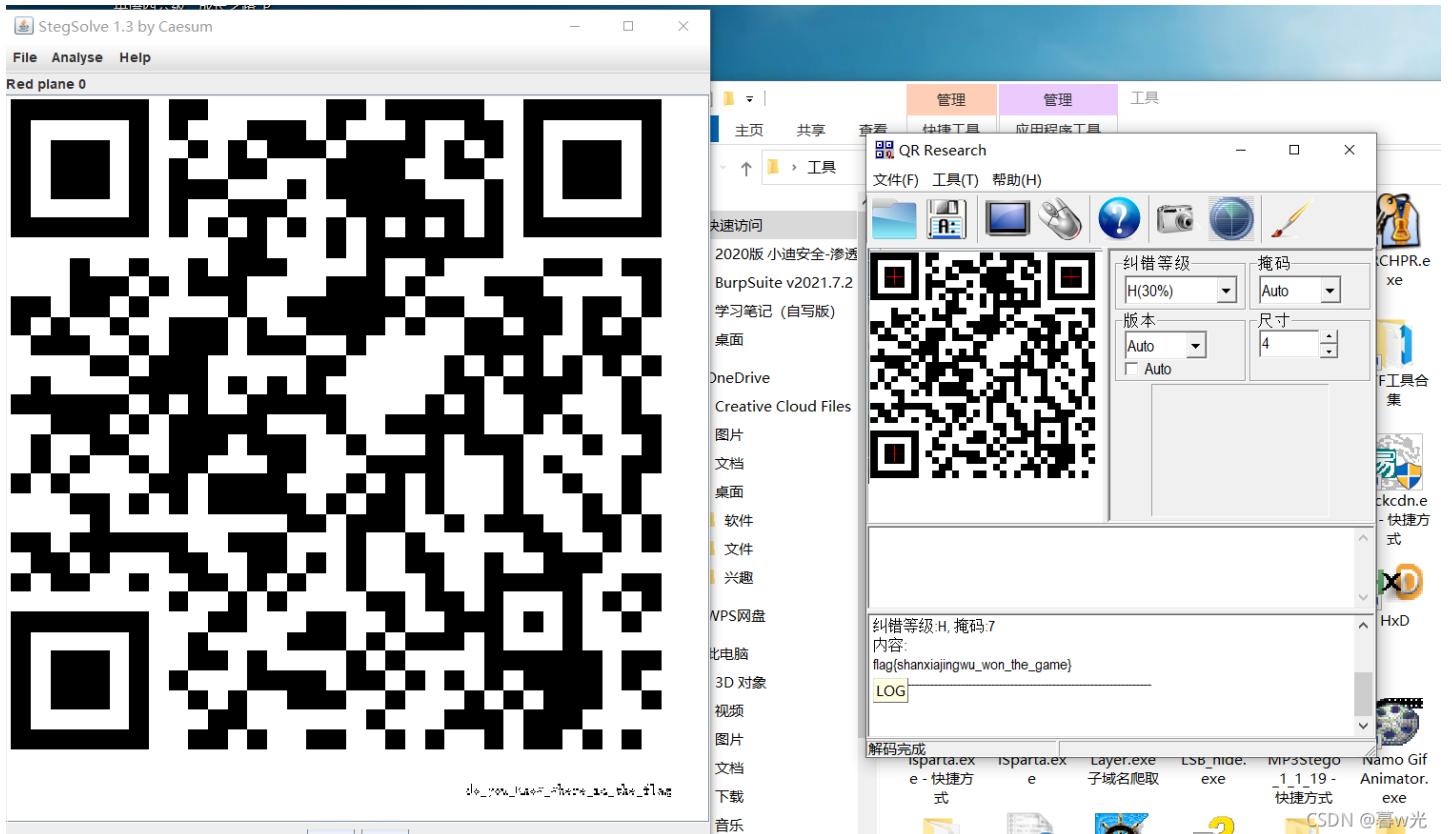


老套路：foremost分离出压缩文件，先弱口令爆破一次密码，成功爆破：



之后分离出gif文件，好家伙，360帧。

逐个查看，可以在stegsolve的analyse的frame browser 逐帧查看并保存，到310帧时可以看到右下角有一行字符，将文件再次保存下来再丢入stegsolve中调整通道翻可以显示出二维码。（还好不太难，不用修改r/g/b值）：



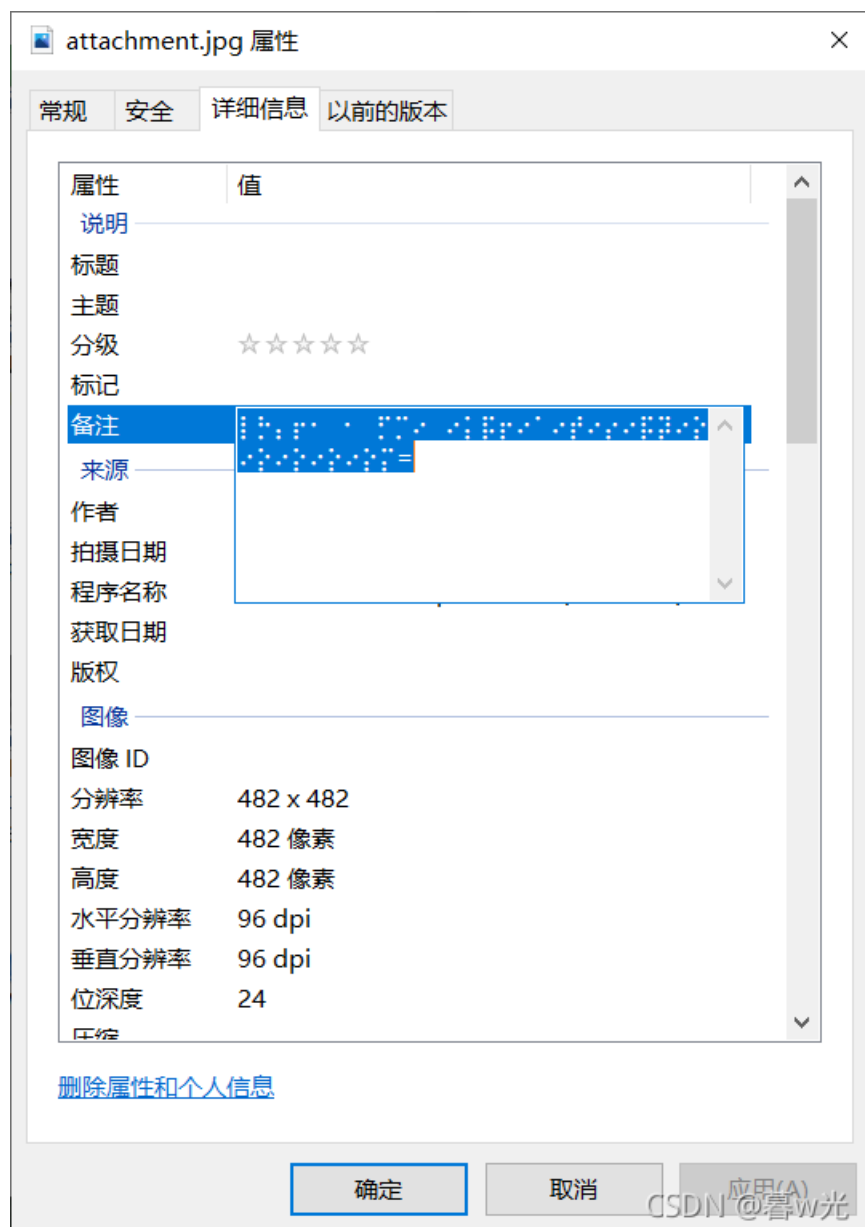
知识点：使用stegsolve。

3.[WUSTCTF2020]find_me

已我的经验拿到杂项图片题一般这个思路：

1. 右键看属性有无提示。
2. binwalk分析文件是否隐写入其他文件有则foremost分离。
3. 用winhex或010editor打开文件分析可能修改文件格式或者查找隐藏在其中的加密信息。
4. stegsolve查看lsb信道或其他信息。
5. 宽或高做修改，脚本/源码查看。
6. 其他奇葩的图片隐写方式，什么f5，根据函数坐标画个二维码等等。
7. 万能的百度大法。

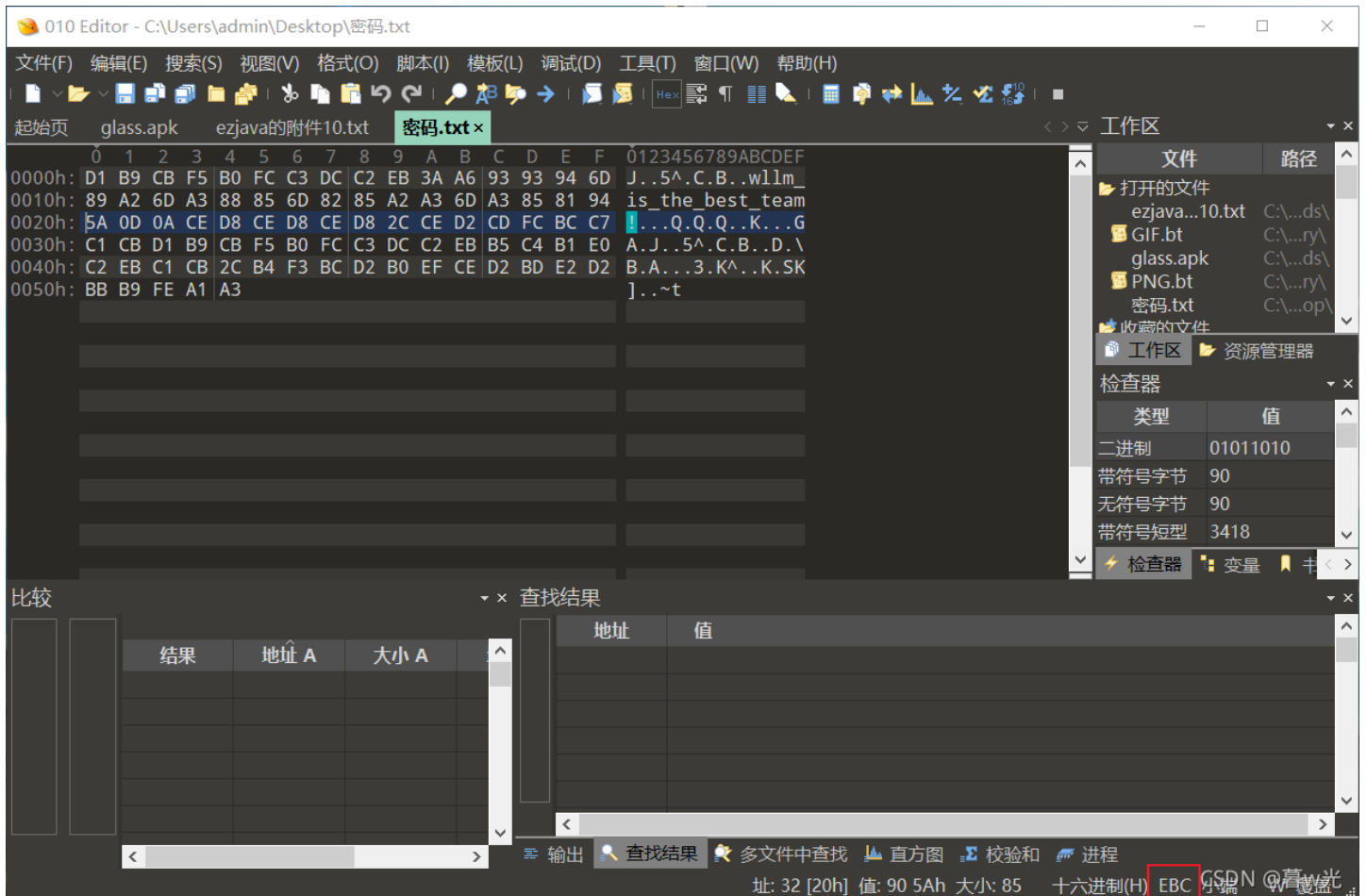
这个题就是右键属性可以看到提示，百度一下，知道是盲文，



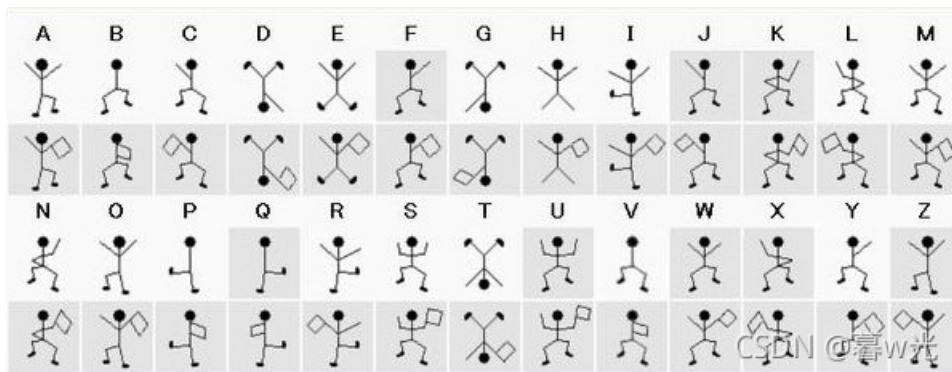
盲文在线加解密: <https://www.qqxiuzi.cn/bianma/wenbenjiami.php?s=mangwen>

4.[SWPU2019]伟大的侦探:

可以在010里修改编码，右下角改为ebc编码：



之后解压出小人，想到那张福尔摩斯跳舞的小人解密图：



```
flag{loveholmesandwllm}
```

知识：010里的编码修改功能，感觉比notepad++强；福尔摩斯跳舞的小人加密。

5. [MRCTF2020]你能看懂音符吗

首先打不开rar文件，文件损坏，010打开发现文件头正好换位了，正确rar文件头：52617221。

52	61	72	21	1A	07	01	00	94	E6	41	F6	0B	01	05	07	Ra	!	...	"	æ	A	ö	...											
00	06	01	01	95	CE	80	00	F4	00	98	0D	38	02	03	0B	...	•	î	€	.	ô	.	~	.	8	...								
C8	CD	00	04	86	DA	00	20	BF	3A	FE	97	80	03	00	1A	È	Í	.	†	Ú	.	¿	:	p	-	€	...							
E4	BD	A0	E8	83	BD	E7	9C	8B	E6	87	82	E9	9F	B3	E7	ä	½	è	f	½	ç	œ	<	æ	‡	,	é	ÿ	³	ç				
AC	A6	E5	90	97	2E	64	6F	63	78	0A	03	02	DF	F6	91	-	!	ä	.	-	ß	ö	'
8B	31	E9	D5	01	CC	74	C4	26	50	66	34	54	23	55	4E	<	1	ü	ö	!	+	Ä	&	P	f	4	T	#	1	0				

然后解压，

←
←
←

b#j || f j bbj b || || bbj || j j || j j || j j bbj || j j || j j bbb || f f || || || j j || j j || j j bbbbb
 § || j j bbj bbb || j b || f § bb# || j j f || j j || f || j j || j j || j j § =←

这都让你发现了，可是你能看懂吗？←

在线解密网站：[音符解密](#)