2.BJDCTF(2020第二届)——Misc杂项题

原创

qwsn 于 2020-04-02 18:59:18 发布 2294 收藏 7

分类专栏： # 1.BJDCTF 2nd 文章标签： 2.BJDCTF—Misc 解压300次套娃题目 outguess隐写 视频PS/Pr分帧 新佛曰解码

qwsn

1.BJDCTF 2nd 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

2.BJDCTF(2020第二届)——Misc杂项题

0x01.题目统计

题目统计

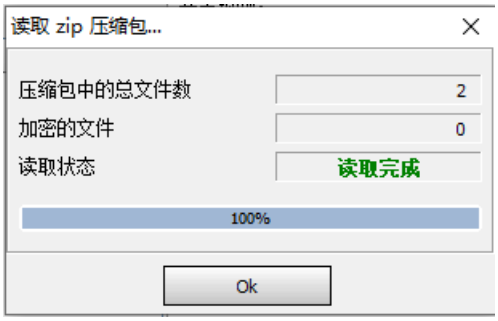
方向	数量	分值	比重
Web	10	2600	24%
Pwn/Game	11	3000	28%
Misc	8	1550	14%
Blockchain	2	900	8%
Programming	1	800	7%
Crypto	8	1160	11%
Reverse	3	850	8%
总计	43	10860	100%

0x02.Misc复现

第一题：[BJDCTF 2nd]最简单的misc-y1ng

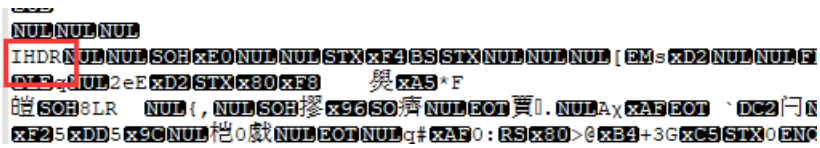
（1）题目

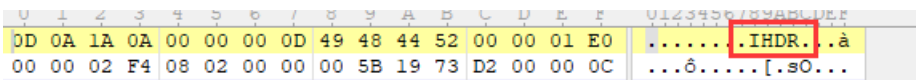
（2）解压附件得到的压缩包，发现需要密码，我们使用Ziperello暴力破解zip压缩包软件，读取压缩包，发现没有加密的文件；（猜测是伪加密）



（3）伪加密解密即可：java -jar ZipCenOp.jar r xxx.zip 解密

（4）解密得到一个secret文件，记事本或者010edit打开后经过搜索，
发现一：头部是：IHDR（这个是PNG图片的标志）
发现二：一串特殊的语句，应该是说经过了PS，经过整理后，发现两个特殊字符串





```
58 69 43 43 50 44 69 73 70 6C 61 79 00 00 48 89  XiCCPDisplay..H‰
95 57 77 54 53 F7 FB 7E EE C8 64 43 44 40 90 00  •WwTS÷û~îÈdCD@..
32 04 51 04 41 10 19 21 4C 41 41 36 B8 08 49 80  2.Q.A..!LAA6¸.I€
30 42 BC 24 A8 B8 D1 A2 A2 75 8B 28 8E 3A AA A2  0B¼$¨¸Ñ¢¢u‹(Ž:ª¢
16 AD 56 40 EA 40 D4 E2 2A EE 55 C7 17 07 8E 4A  .-V@ê@Ôâ*îUÇ..ŽJ
2D D6 2D 2A BF 3F 12 A8 B5 DF F3 FB 9D DF 7B CE  -Ö-*¿?.¨µßóû.ß{Î
BD F7 3D CF FB BC CF 3B EE 3D 39 F9 00 46 EB 24  ½÷=Ïû¼Ï;î=9ù.Fë$
2A 55 3E 69 0C 14 28 D5 4C 7C 44 88 30 35 2D 5D  *U>i..(ÕL|Dˆ05-]
C8 79 08 12 6C E8 61 10 B8 12 69 91 4A 14 17 17  Èy..lèa.¸.i'J...
```

```
<?xpacket begin="ï»¿" id="W5M0MpCehiHzreSzNTczkc9d"?>
    <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c145 79.163499, 2018/
        <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
            <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:
                <rdf:Seq>
                    <rdf:li stEvt:action="created" stEvt:instanceID="xmp.iid:4fceb197-7ec
                    <rdf:li stEvt:action="saved" stEvt:instanceID="xmp.iid:d4e03a4a-dc77-
                </rdf:Seq>

                    </xmpMM:History>

                <photoshop:TextLayers>
                    <rdf:Bag>
                        <rdf:li photoshop:LayerName="424A447B79316E677A7569736875616 97D"
                        <rdf:li photoshop:LayerName="@é¢-å¥‡Lâ€™Amore" photoshop:LayerTex
                    </rdf:Bag>
                </photoshop:TextLayers>
            </rdf:Description>
        </rdf:RDF>
    </x:xmpmeta>
<?xpacket end="r"?>
```


（5）先解决线索一：010edit打开文件，Ctrl+Shift+I，添加4字节的十六进制位，给PNG加文件头89 50 4e 47

```
89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52  %PNG........IHDR
```

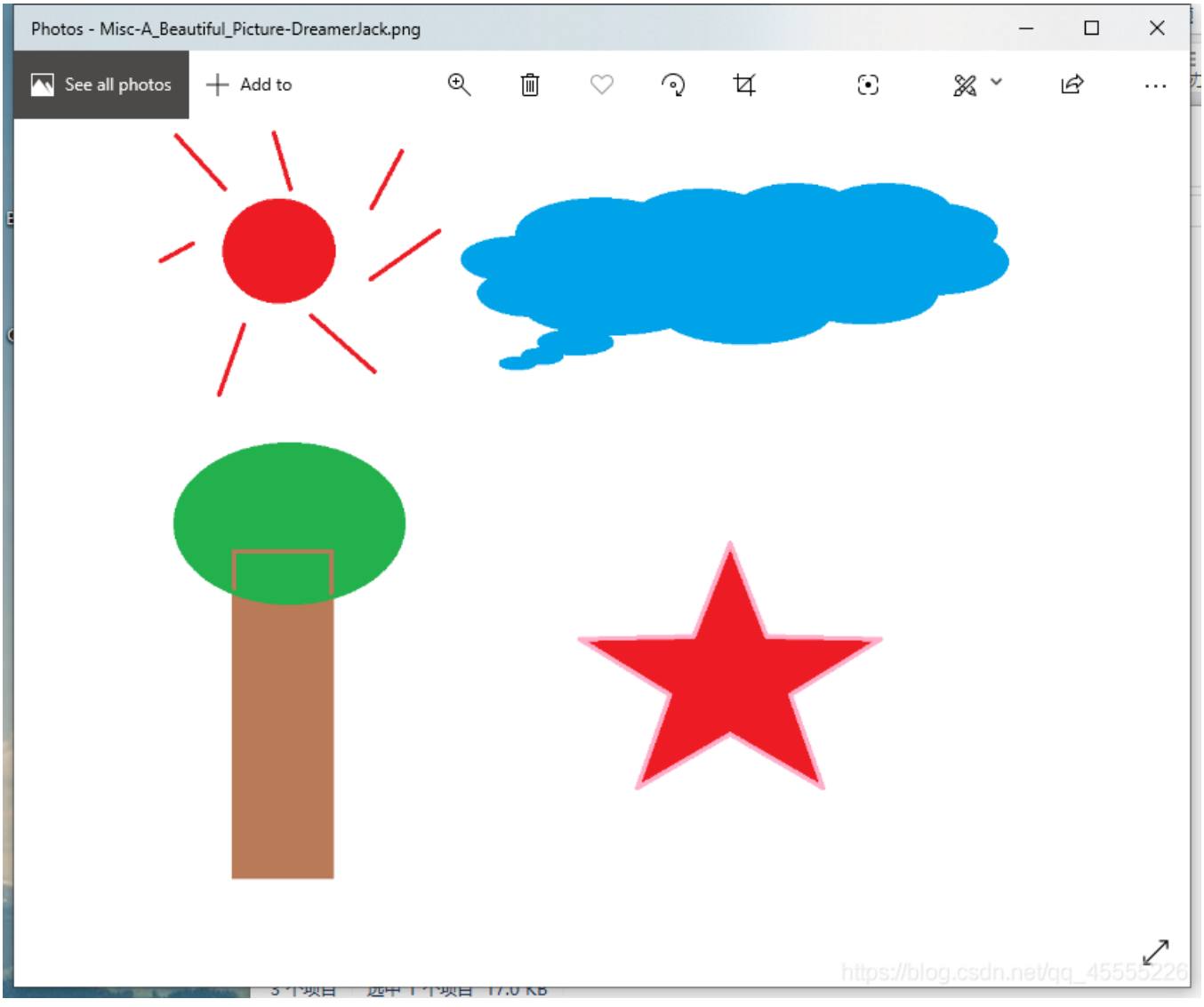
（6）保存修改，后缀直接改成png，打开图片得到十六进制字符串（与之前的发现而对应了），解码即可

（7）flag：BJD{y1ngzuishuai}

第二题：[BJDCTF 2nd]A_Beautiful_Picture

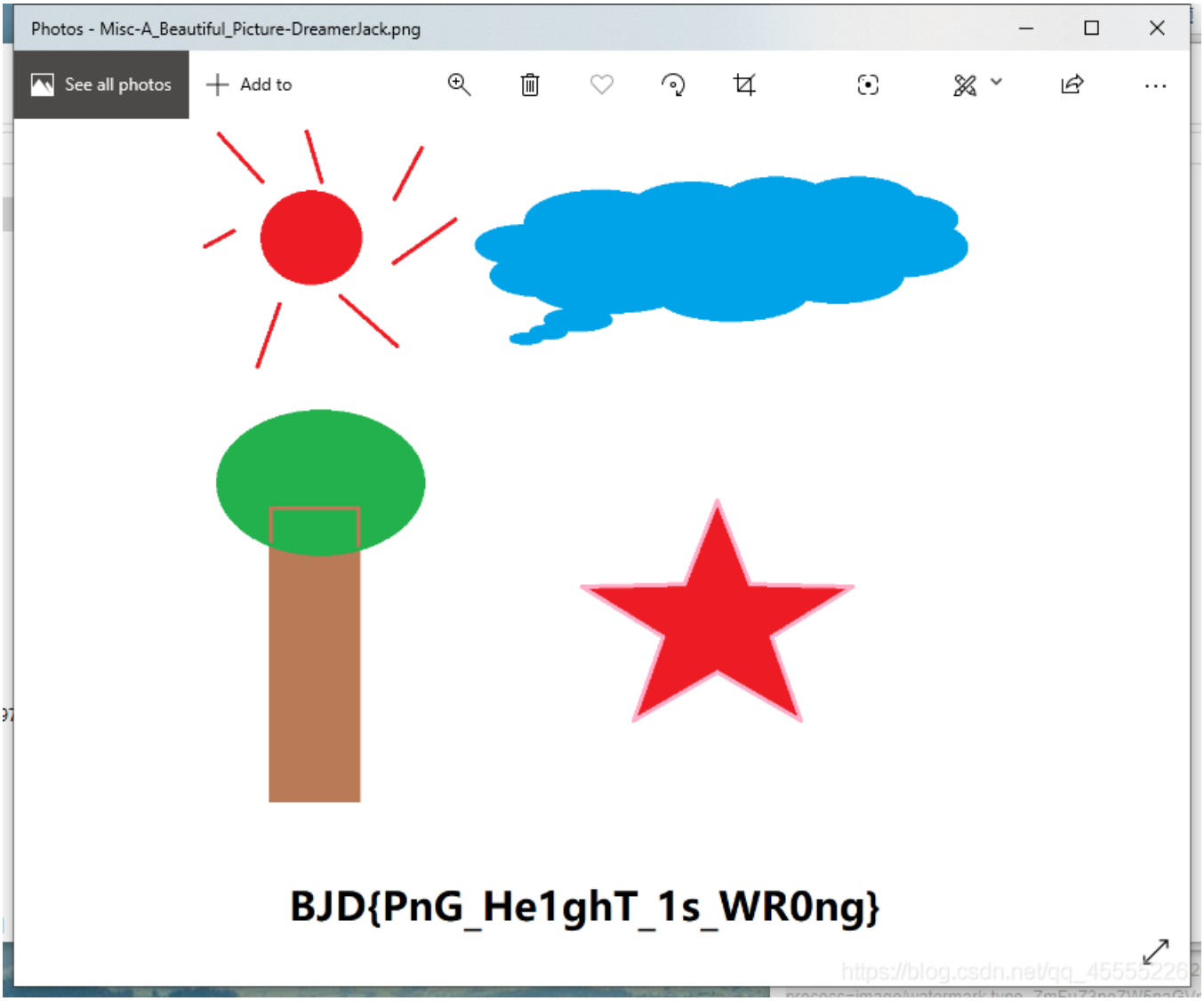
（1）题目

（2）打开图片，没有任何发现



（3）右键属性，发现（高度x宽度=1000 x 900 = 03e8 x 0384 ）

（4）尝试使用010edit修改宽度为高度，0384–>03e8，得到flag

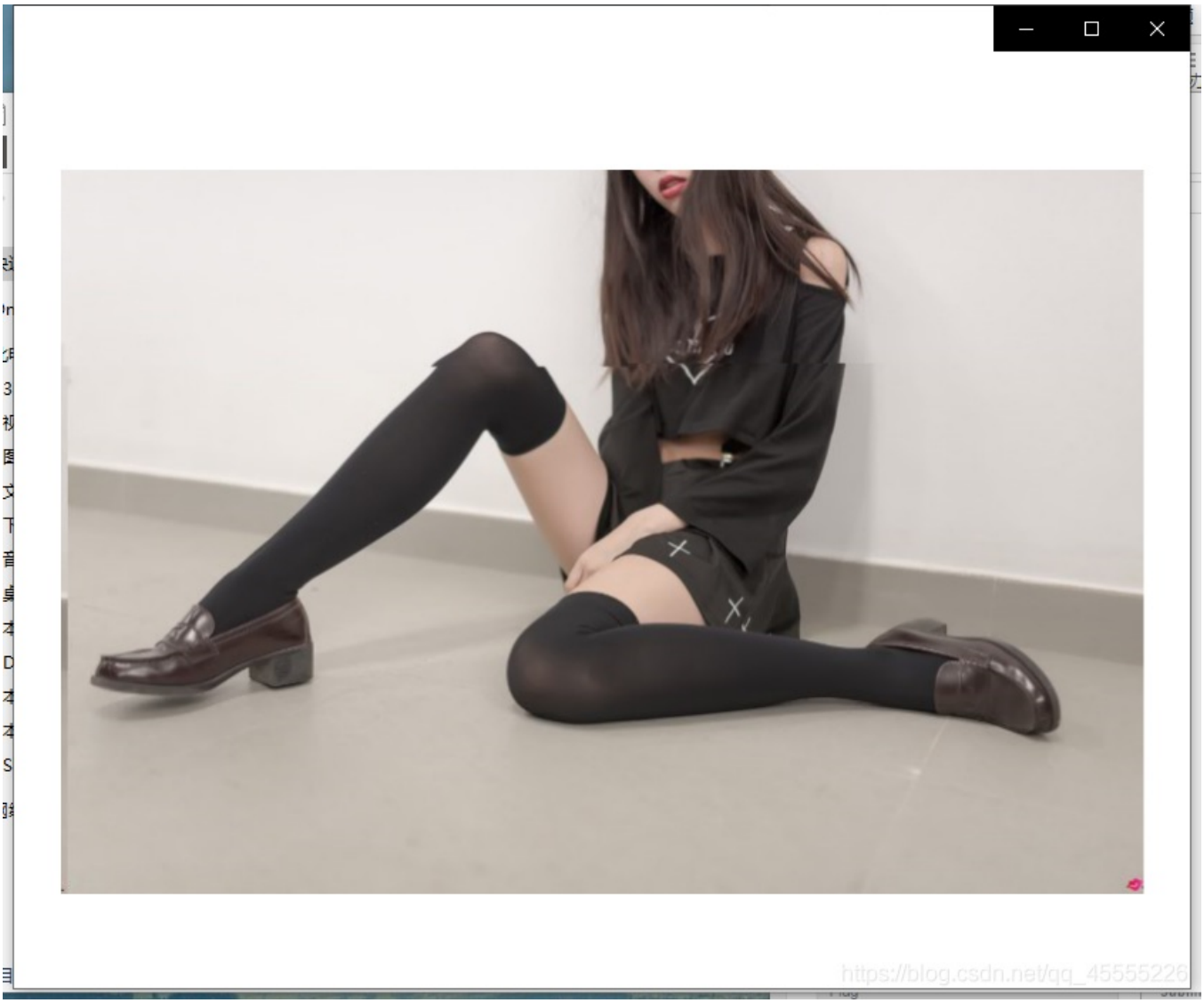


（5）flag：BJD{PnG_He1ghT_1s_WR0ng}

第三题：[BJDCTF 2nd]小姐姐-y1ng

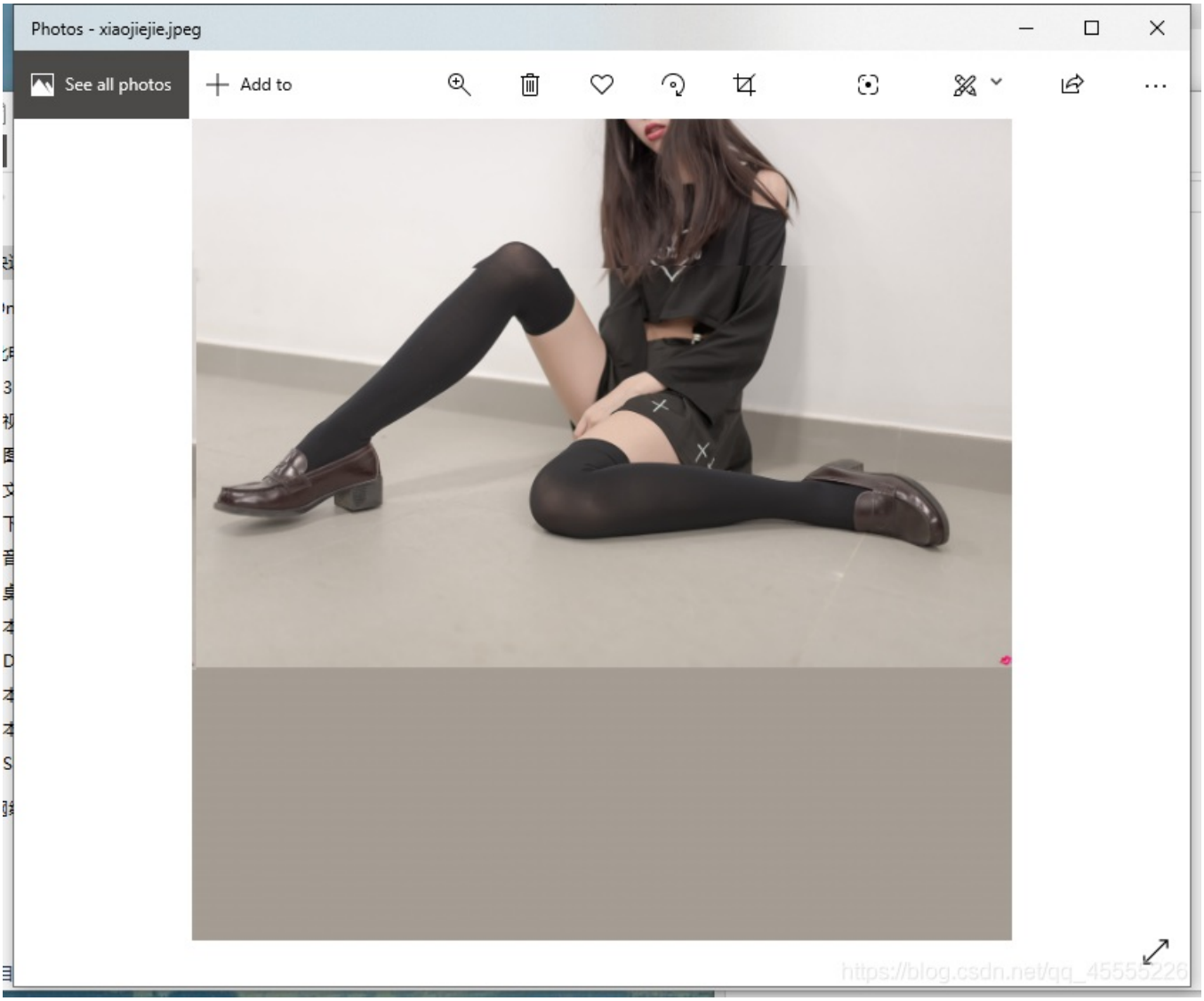
（1）题目：

（2）解压后得到一张，小姐姐的图片



（3）开始图片隐写的套路

第一步：双击打开结合右键属性详细信息，发现宽高好像有问题，010edit修改宽高后，无任何信息



第二步：记事本打开，搜索BJD，查看头部信息，拉到最后面，无任何信息

第三步：010edit打开，搜索text：BJD即可

```
3B 7A 56 86 0C E9 42 4A 44 7B 68 61 6F 6B 61 6E  ;zV†.éBJD{haokan
6D 61 5F 78 6A 6A 7D 7C 2F 7C EA 4C 6E 77 2F 03  ma_xjj}|/|êLnw/.
```

（4）flag：BJD{haokanma_xjj}

第四题：[BJDCTF 2nd]EasyBaBa

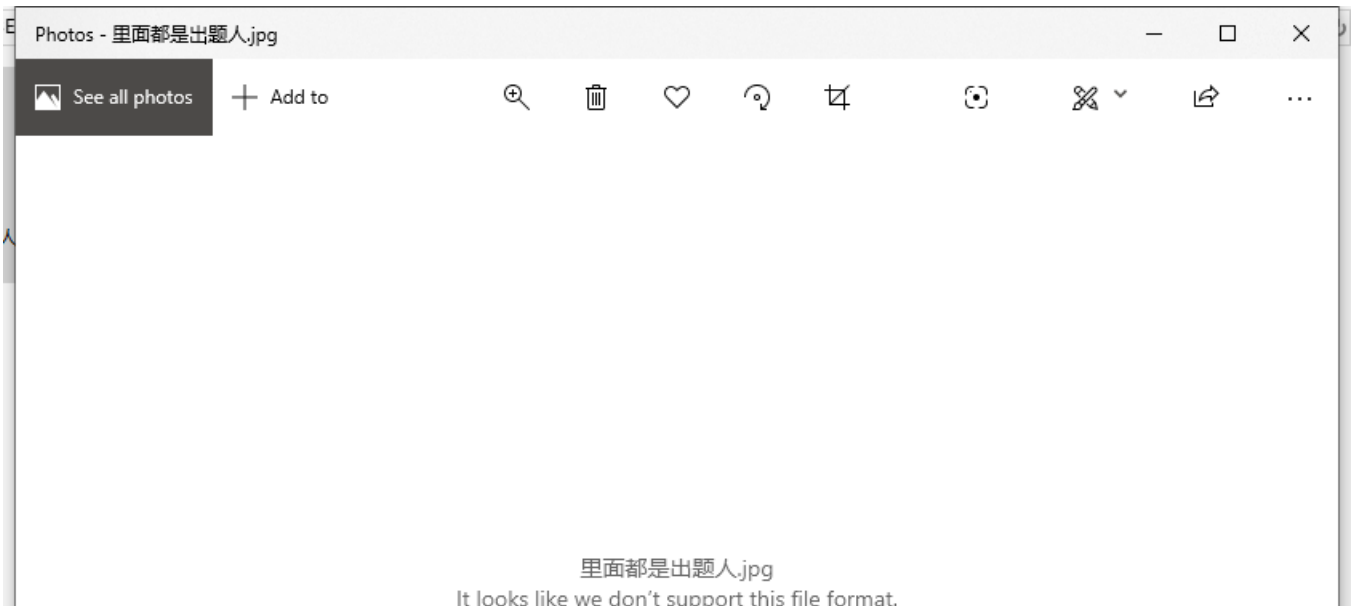
（1）题目：

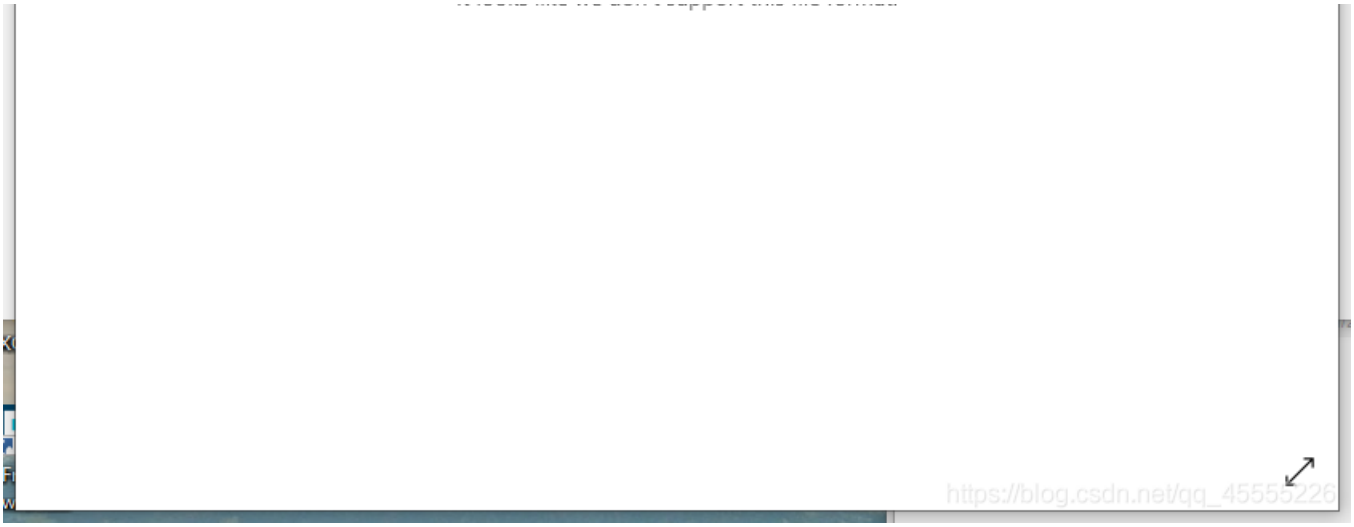
（2）下载附件的时候，发现图片大小是19.9MB，很明显有东西，猜测是压缩包

（3）010edit打开图片，分割出来zip压缩包

搜索：ffd8ff和ffd9
搜索：504b 0304和504b 0506
发现图片尾部之后，刚刚好是压缩包的头部

（4）解压后，得到一个好像是坏了的jpg图片





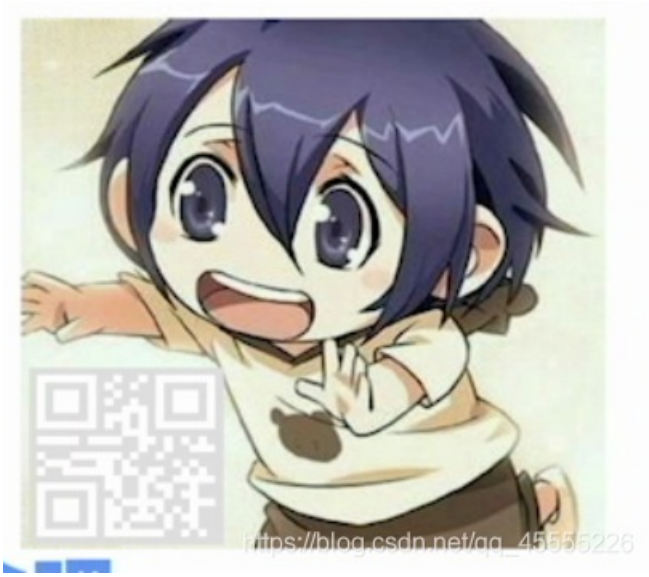
（5）记事本，010打开后，发现文件头部是RIFF AVI，很明显是avi格式的视频，直接修改后缀为avi即可

（6）打开视频，一直在叫爸爸（第4秒的时候，开始闪出图片）

第一步：从视频里面分割出图片

方法一：使用某讯视频，或者某奇艺视频打开该视频，放慢速度，截图可以得到四张二维码（不过第四张图片需要PS）


你tooyoung



方法二：或者使用PS直接分帧，或者Pr分帧

第二步：对图片四进行PS，修改颜色得到

第三步：使用CQR依次扫描二维码，得到一串十六进制字符串：6167696E5F6C 6F76655F59 424A447B696D 316E677D

第四步：十六进制转字符串得到：agin_love_YBJD{im1ng}

第五步：修改顺序得到：BJD{imagin_love_Y1ng}

（7）flag：BJD{imagin_love_Y1ng}

第五题：[BJDCTF 2nd]Real_EasyBaBa

（1）题目：

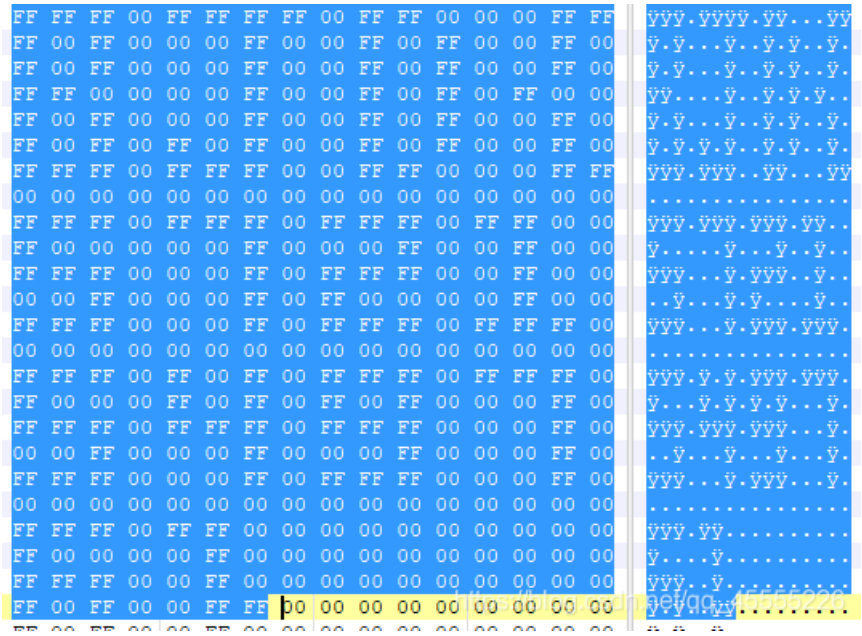
（2）附件，又是一张图片；

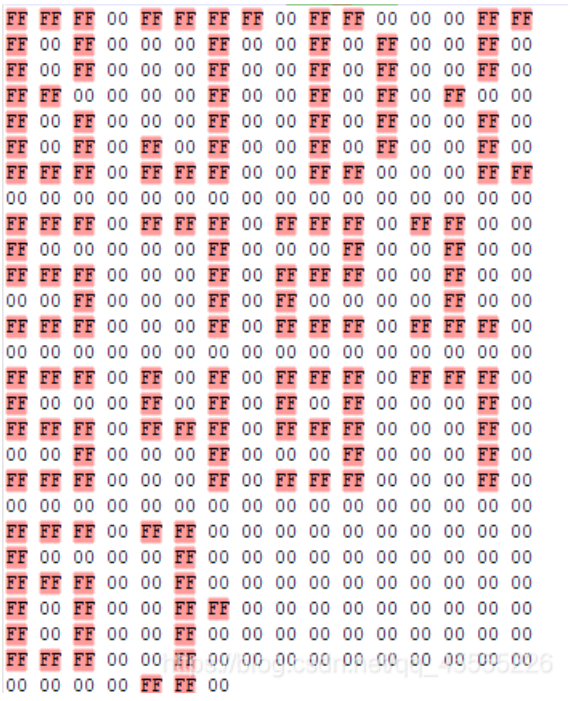
第一步：打开图片，右键属性，无可用信息

第二步：记事本打开，看头部，尾部，搜索关键字BJD，无可用信息

第三步：010edit打开，看头部，尾部，搜索关键字：504b 0304，377a，8950 4e47，BJD，无可用信息

第四步：发现了一些特殊的区域，把该区域的16进制给保存下来，使用notepad++打开，把FF标记即可





（3）flag：BJD{572154976}

第六题：[BJDCTF 2nd]圣火昭昭-y1ng

（1）题目：

（2）提示1：flag靠”猜“，推测是outguess隐写题目

（3）提示2：key值，需要我们自己搞出来，去掉com

（4）解压附件压缩包，得到一张图片；

第一步：双击打开，右键属性详细信息发现了，新佛曰密码，解码即可
新佛曰：諸壽隸僧壽降吽壽諸壽陀壽摩隸僧鉢薩願心壽咤壽囉寂壽闍諸壽哆壽慧壽聞壽色吽愍壽所壽蜜如

第二步：进入新佛曰网址**（http://hi.pcmoe.net/buddha.html）**，解码得到key：gemlovecom，去掉com，就是gemlove

（5）在kali，里面使用outguess命令：`outgess -k gemlove -r sheng_huo_zhao_zhao.jpg -d hided.txt`

得到flag：

```
root@qium0:~/Public/0x06.BUUCTF/3# cat hided.txt
BJD{wdnmd_misc_1s_so_Fuck1ng_e@sy}
```

（6）flag：BJD{wdnmd_misc_1s_so_Fuck1ng_e@sy}

第七题：[BJDCTF 2nd]TARGZ-y1ng

（1）题目：

（2）提示1：tar -zxvf没有用

（3）提示2：解压密码不需要爆破，猜测是伪加密，或者是题目名字，或者是文件名字（亲测是文件名字）

（4）这个压缩包实际上是，zip文件。（经过kali的file命令识别，或者是文件头504b 0304都能看出这只是一个普通的zip格式的压缩包）（不过这题是个套娃，需要解压300次，每次的密码都是自己的文件名字）

方法一：手动解压300次

方法二：python脚本跑

注意：虽然会报错，但是目录下还是产生了flag文件，cat一下即可

注意：百度来的脚本

```
import zipfile

name = 'hW1ES89jF'
while True:
    fz = zipfile.ZipFile(name + '.tar.gz', 'r')
    fz.extractall(pwd=bytes(name, 'utf-8'))
    name = fz.filelist[0].filename[0:9]
    fz.close()
```

（5）FLAG：BJD{wow_you_can_rea11y_dance}

第八题：[BJDCTF 2nd]Imagin - 开场曲

（1）题目：

（2）分析附件mp4，打开视频后，发现一个网址：**https://aidn.jp/mikutap**

（3）发现该网站，支持点击不同的格子，发出不同的声音

（4）猜测是：根据附件的声音，推测是其音节对应的字符（咋也没有对应表，也听不懂，也不知道官方的WP，怎么能那么简单就听出来了，真是秀，呵呵）

百度的一个音节表，不对呀吖，主要是。。。。

mikutap-发音对应表

Sophie_2333 2019-03-16 19:21:11

0	1	2	3	4
1	my	pu	to	ka
2	te	no e	so	wei~
3	ka	ra	ra/	me
4	ra	ye	te~	ra~
5	re	pi	za	wa
6	sa	hi	na	sa
7	ya	hi	te	pa
8	o	a	tsu	de

（5）flag：BJD{MIKUTAP3313313}

0x03.总结

- 伪加密
- PNG文件标志：IHDR
- PNG文件头：8950 4e47
- 修改宽高
- 直接搜索关键字BJD
- AVI文件标志：（标志RIEF：52 49 46 46，AVI：41 56 49）
- PS/Pr对视频分帧，修改图片色度
- 考验视力，FF 00
- 猜 outguess隐写
- 套娃题，300次解压
- 音节对应字符