Week1

MISC:

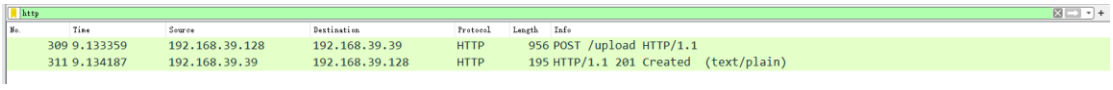
1、Sign In

直接 Base64 解码：

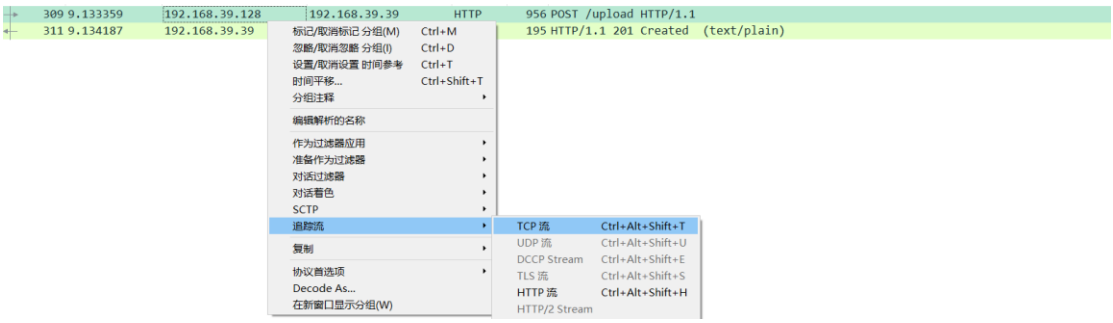
Flag：hgame{Welcome_To_HGAME2023!}

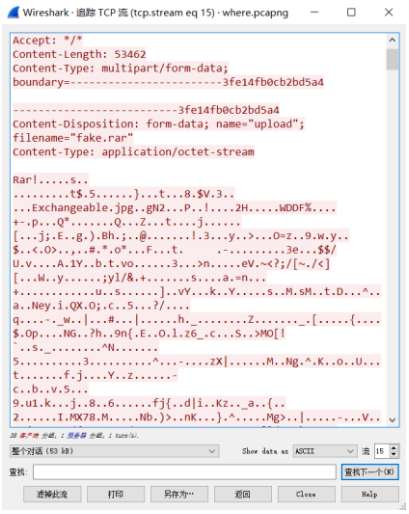
2、Where am I

下载附件，得到 where.pcapng 文件
用 Wireshark 软件分析
根据题目提示，在神秘地方拍照上传，那么上传图片是用到 http 协议，过滤出 http 协议的信息：

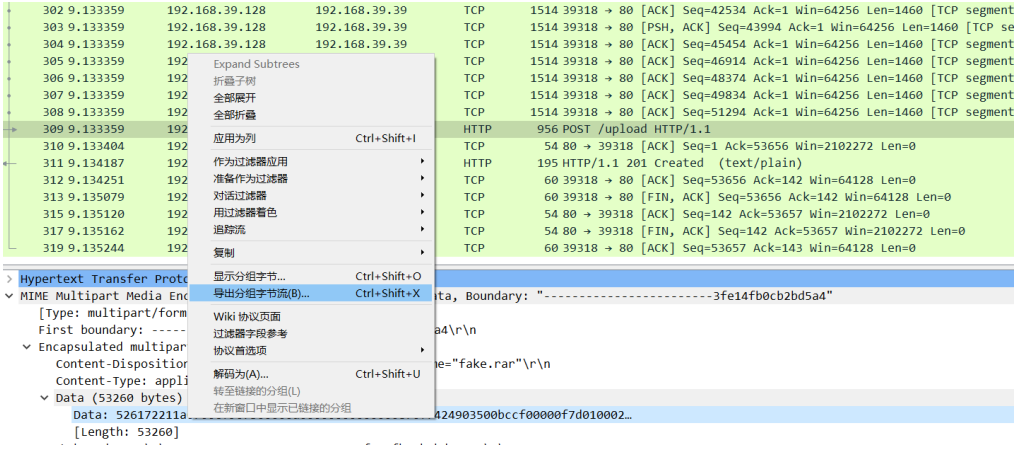


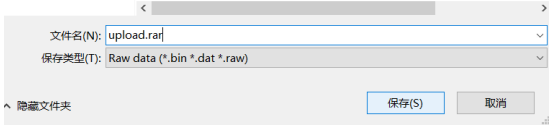
然后 TCP 流追踪：



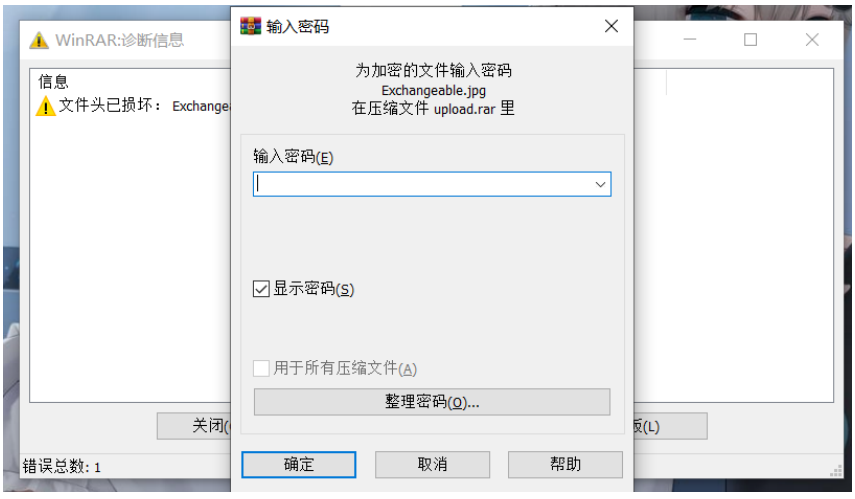


就可以发现，上传了一个文件名是 upload 的 rar 格式文件。将文件数据导出保存为 rar 后缀的文件：

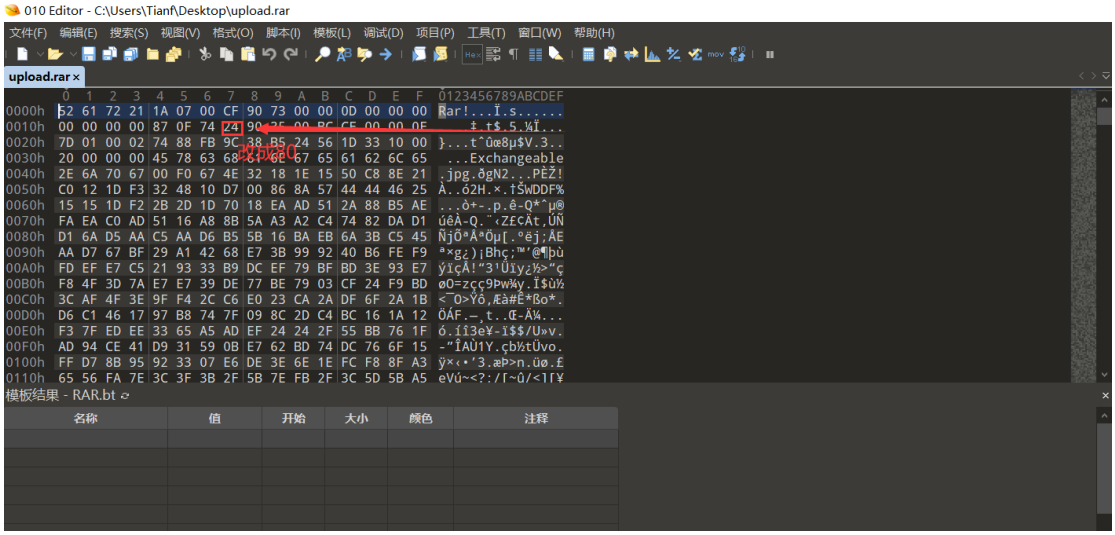




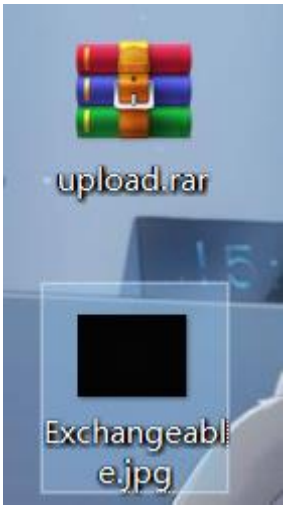
直接解压：



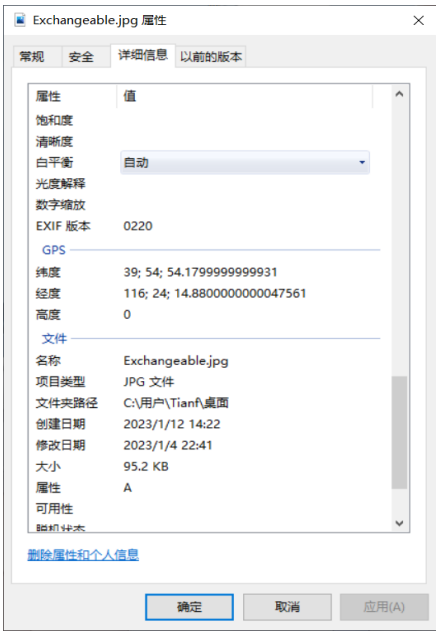
显示文件头损坏，还要输入密码。考虑伪加密，用 010 编辑器查看：



再解压，就可以得到一张 jpg 图片：



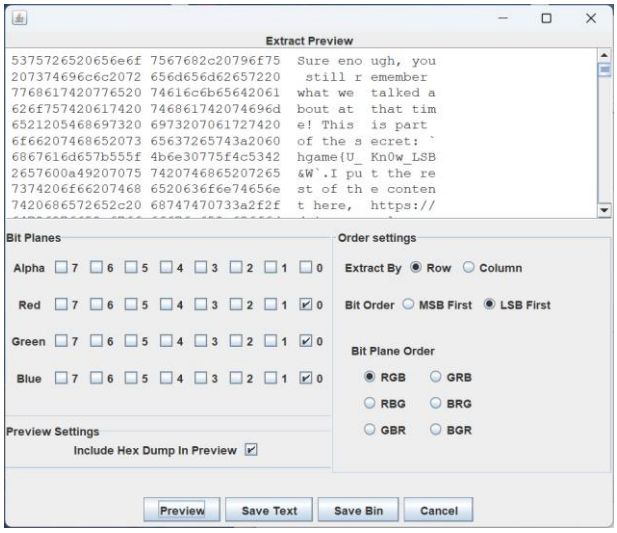
查看其属性，就找到了经纬度，就知道其 flag：hgame{116_24_1488_E_39_54_5417_N}



3、神秘的海报

下载附件拿到一张 png 图片，用 stegsolve 分析发现，一部分 flag 和另外一部分的提示：

```
Sure eno ugh, you
 still r emember
what we  talked a
bout at  that tim
e! This  is part
of the s ecret: `
hgame{U_ Kn0w_LSB
&W`.I pu t the re
st of th e conten
t here,  https://
drive.go ogle.com
/file/d/ 13kBos3I
xlfwkf3e 0z0kJTEq
Bxm7RUk- G/view?u
sp=shari ng, if y
ou direc tly acce
ss the g oogle dr
ive clou d disk d
ownload  in China
, it wil l be ver
y slow,  you can
try to u se Scien
tific In ternet a
ccess so lves the
 problem  of slow
 or inac cessible
 access  to exter
nal netw ork reso
urces. T his is m
y favori te music
, there  is anoth
er part  of the s
ecret in  the mus
ic, I us e Steghi
de to en crypt, t
he passw ord is a
lso the  6-digit
password  we agre
ed at th e time,
even if  someone
else fin ds out h
ere, it  should n
ot be so  easy to
 crack (  ( hope s
o.....  ........
........ ........
```

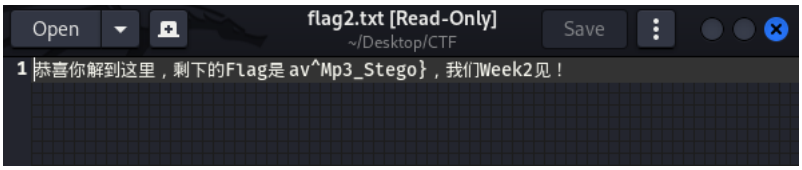


下载另外一部分音频，用 Audacity 并没有得到有用信息，kail 的 steghide 命令下发现有一个加密文件：

```
┌──(root㉿kali)-[/home/forever2/Desktop/CTF]
└─# steghide info Bossanova.wav
"Bossanova.wav":
  format: wave audio, PCM encoding
  capacity: 1009.3 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
steghide: could not extract any data with that passphrase!
```

直接暴力爆破密码,不过直接测试弱密码 123456 就成功了，得到一个 flag2.txt 文件，里面就有另外一部分的 flag：hgame{U_Kn0w_LSB&Wav^Mp3_Stego}

```
┌──(root㉿kali)-[/home/forever2/Desktop/CTF]
└─# steghide extract -sf Bossanova.wav
Enter passphrase:
wrote extracted data to "flag2.txt".

┌──(root㉿kali)-[/home/forever2/Desktop/CTF]
└─#
```



4、e99p1ant_wan

下载附件，得到一张图片，题目提示 crc 校验码不合适，直接脚本爆破：

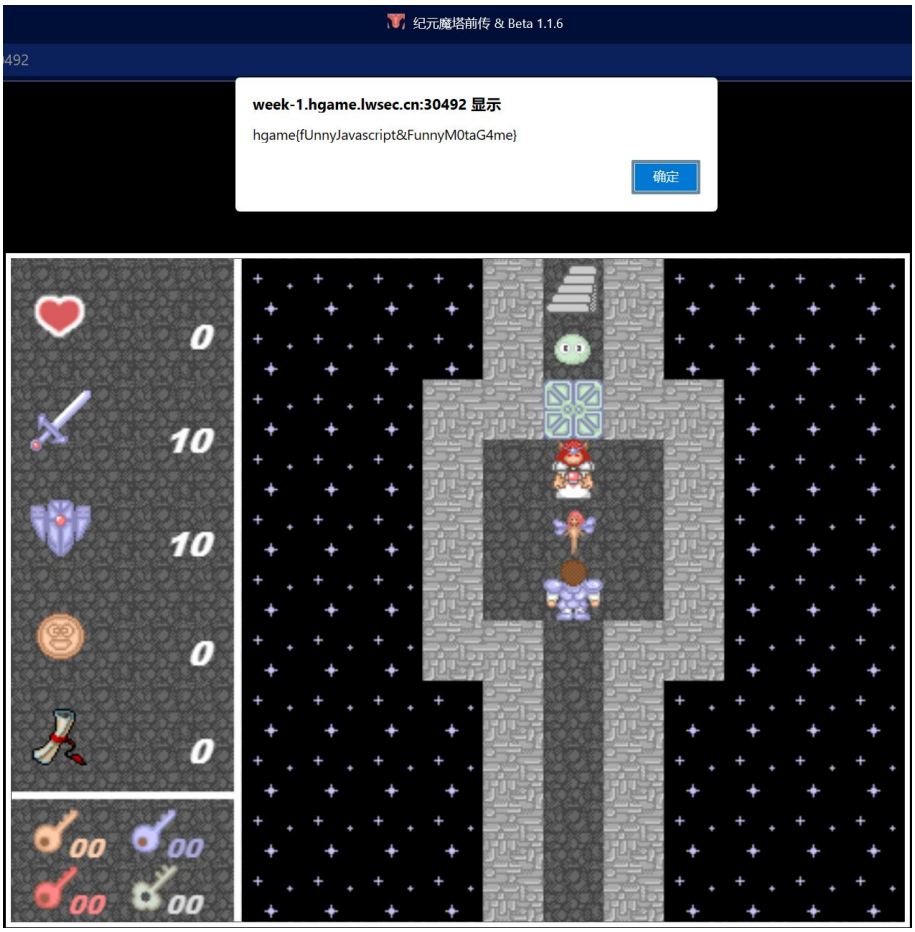
```
D:\python\python.exe                                    99p1ant_want_girlfriend\blast _crc.py"
图片中crc校验值是：2824366917
Width:512, Height:706
hex: 0x200 0x2c2

Process finished with exit code 0
```

将得到的高度值在 010 编辑器中修改，就得到了图片，最下面一行显示出 Flag:hgame{e99p1ant_want_a_girlfriend_qa_524306184}

Web:

1、Classic Childhood Game

打开链接，F12 分析源代码，在 Events.js 事件集合中发现在事件编号，41,42 时通关，并且会弹出一个信息框，直接吧 Switch 的值改成 41，触发一次事件，就直接得到 flag：hgame{fUnnyJavascript&FunnyM0taG4me}


纪元魔塔前传 & Beta 1.1.6
492
week-1.hgame.lwsec.cn:30492 显示
hgame{fUnnyJavascript&FunnyM0taG4me}
确定
0
10
10
0
0
00
00
00
00