HGAME-WEEK2-WP

小霸哥xiaobug

misc DNS

描述

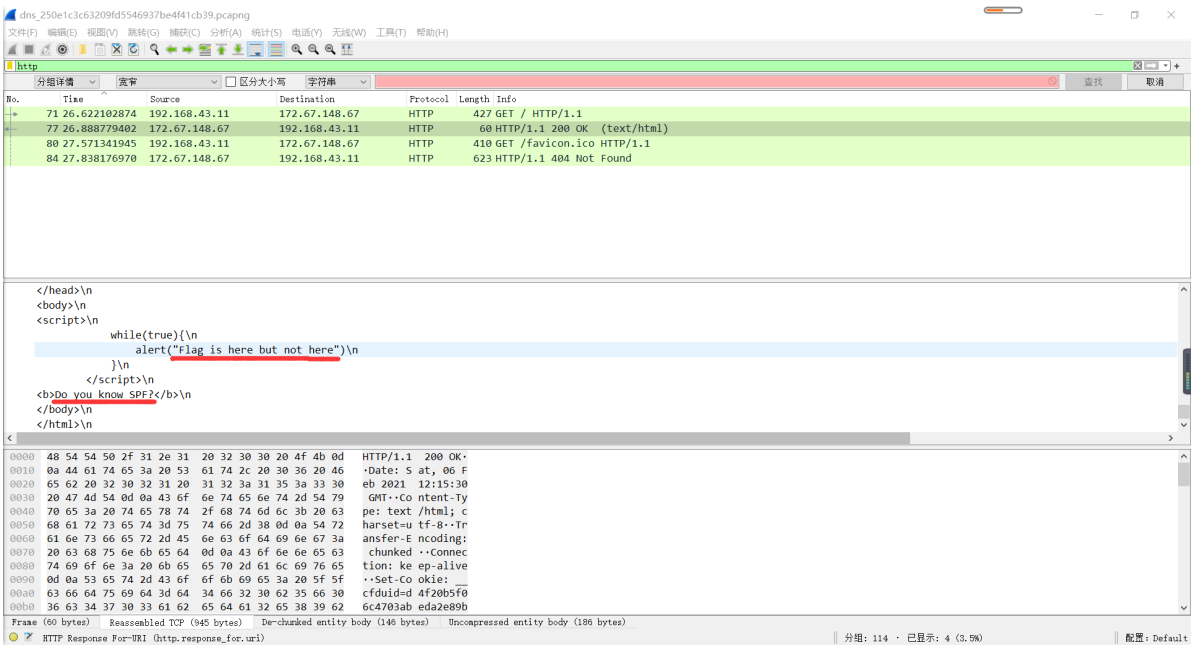
A significant invention.

题目地址

https://1.oss.hgame2021.vidar.club/dns_250e1c3c63209fd5546937be4f41cb39.pcapng

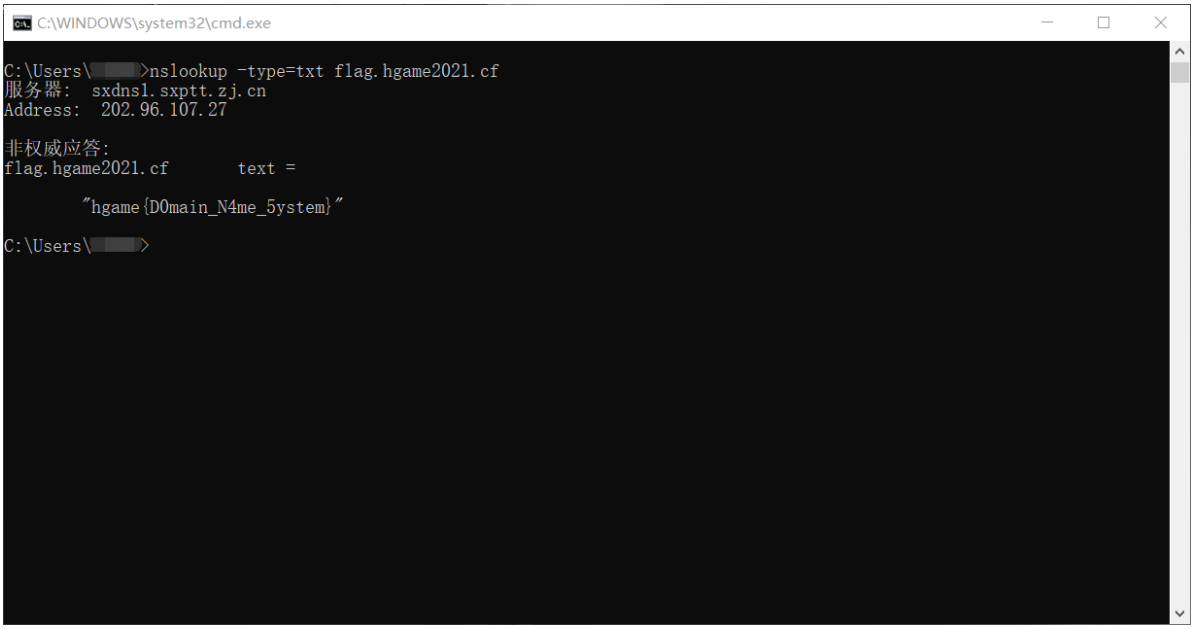
wp

首先，发现后缀是pcapng，就用wireshark打开，过滤显示DNS，啥也没看出来，再过滤显示http，发现新大陆：



又被嘲讽了，我确实不懂SPF，但好在也拿到了hint，百度搜索未果（忍不住爆粗口），bing搜出来了

Windows下进入DOS模式后用以下命令：`nslookup -type=txt 域名`



拿到flag：

> hgame{D0main_N4me_5ystem}

misc Tools

描述

工欲善其事，必先利其器。

题目地址

https://1.oss.hgame2021.vidar.club/tools_21d9ccfca5a4321d6256038d3e885b6d.zip

wp

ps：先感谢用心的出题人，这哪里是题啊，简直就是一份教程嘛，可以从中得到很大收获

打开下载的zip文件，发现F5.7z和Matryoshka.jpg，俄罗斯套娃吗？看样子是大工程

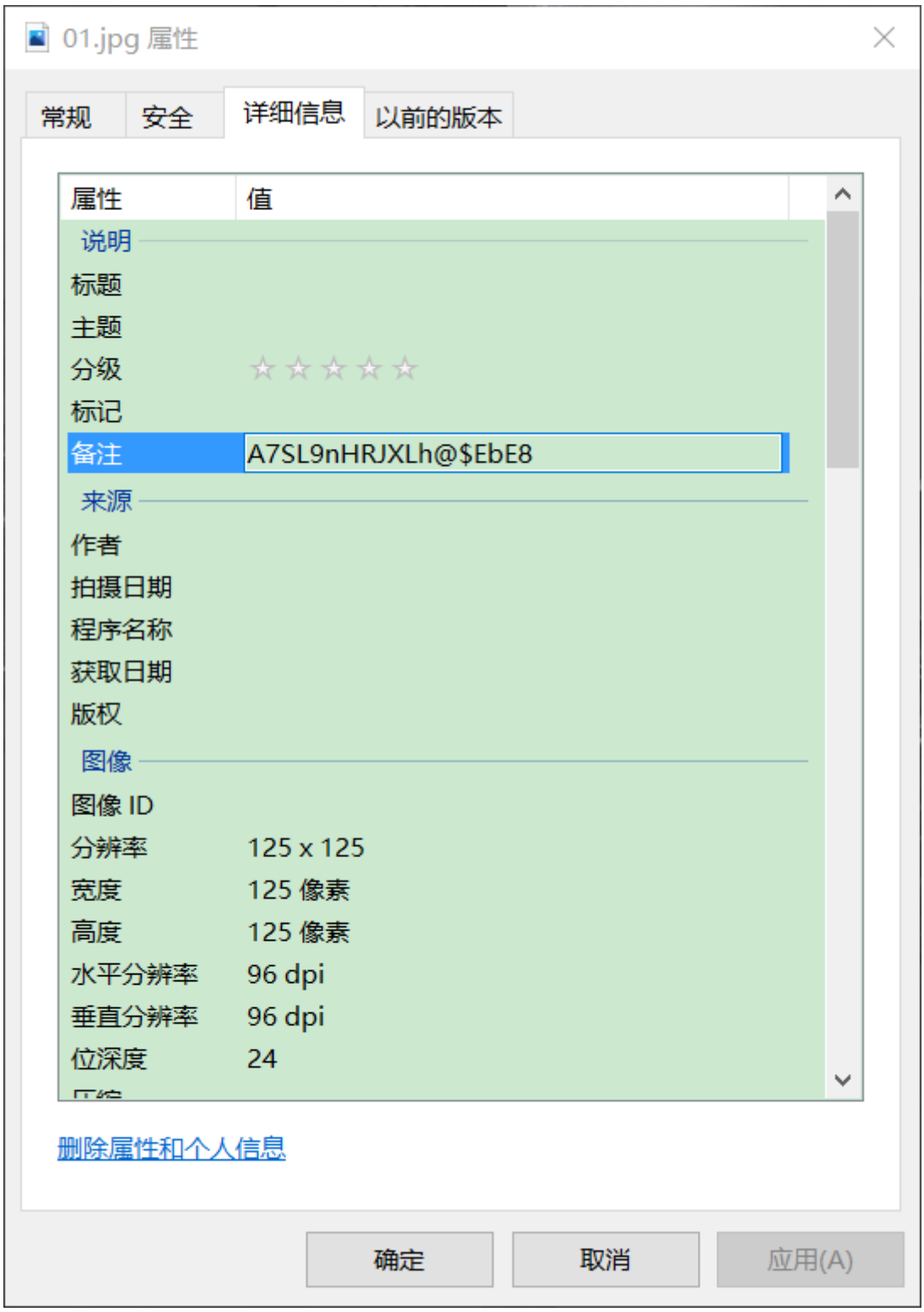
看文件名想到F5-steganography，下载了F5-steganography-master，再查看Matryoshka.jpg的详细信息

从备注得知密码，然后反隐写

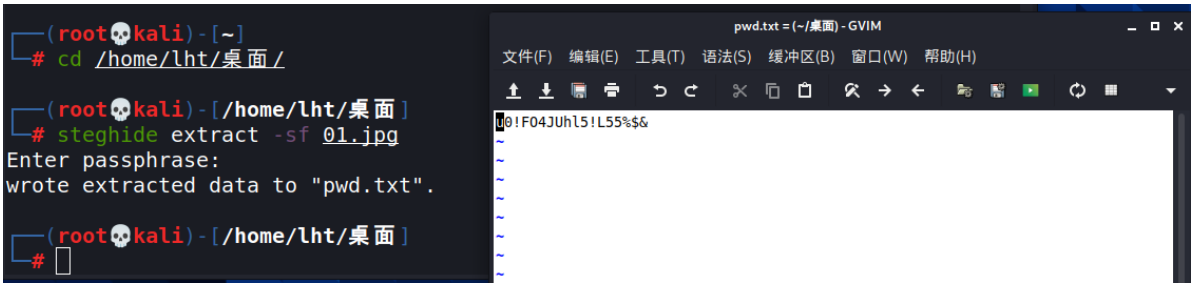
```
C:\                                    \F5-steganography-master>java Extract C:\Users\19269\Desktop\ctf\工具\F5-steganography-master\Matryoshka.jpg -p !LyJJ9bi"&"M7E72*JyD
Huffman decoding starts
Permutation starts
577536 indices shuffled
Extraction starts
Length of embedded file: 18 bytes
(1, 127, 7) code used
```

ps：输入&时要小心，需要加引号，不信可以试试

打开F5.7z，发现Steghide.7z和01.jpg，显然又是hint，查看备注，得到反隐写时用的密码



再进行反隐写

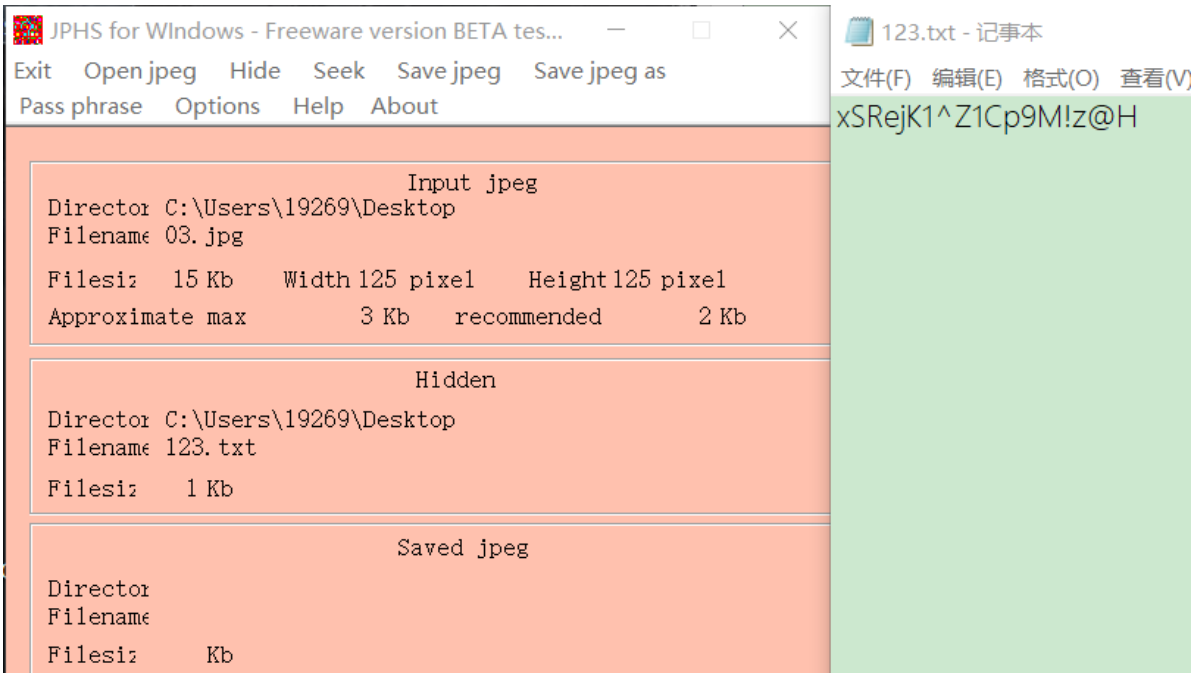


拿到Steghide.7z的密码，打开后得到Outguess.7z和02.jpg

操作与上面步骤相似，为节省篇幅，图片备注信息的截图就不再放了，下面是outguess反隐写的截图

得到Outguess.7z的密码，打开后得到JPHS.7z和03.jpg

同样的得到hint：JPHS，然后就知道怎么做了



得到 JPHS.7z的密码，打开得到最后一个04.jpg

最后一步把四张图都拼到一起，形成完整的二维码

得到flag：

> hgame{Taowa_is_N0T_g00d_but_T001s_is_Useful}

misc Hallucigenia

描述

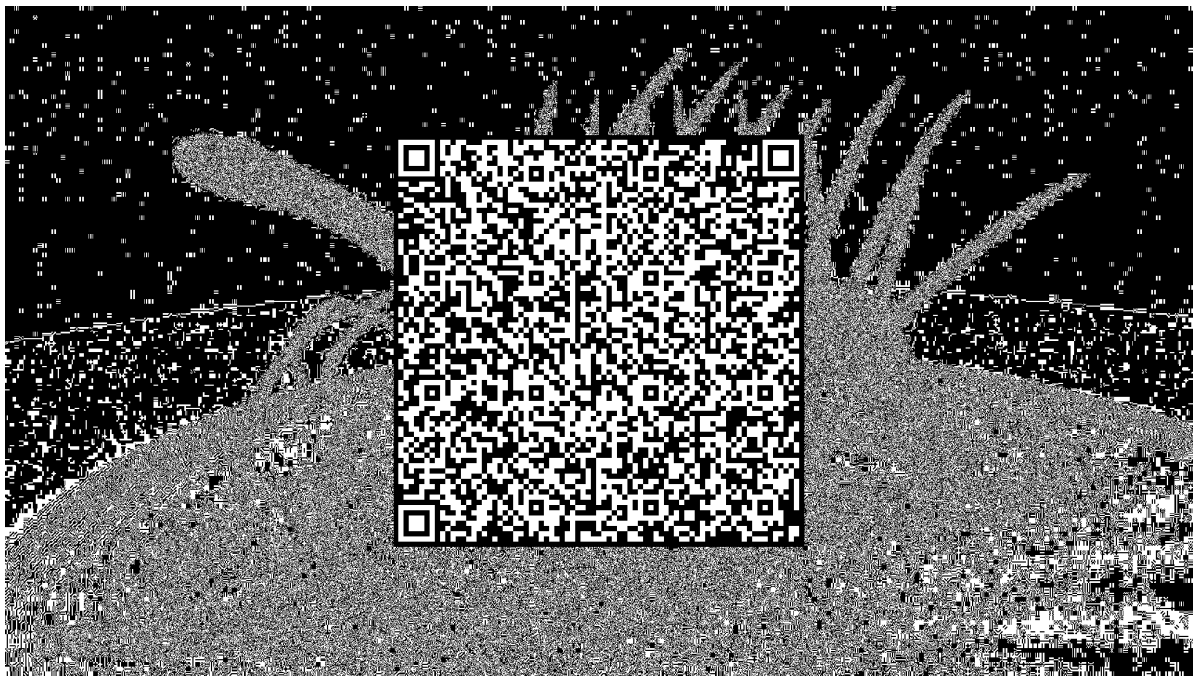
“我们不仅弄错了他的上下，还颠倒了它的左右。”

题目地址

https://1.oss.hgame2021.vidar.club/Hallucigenia_6aa99427e137e9e3563d83f5d639cc74.png

wp

先下载图片，利用`stegsolve.jar`打开，一直点向右或者向左的箭头，总能发现下图：



显然是扫描二维码，得到：

```
gmBCrkRORUkAAAAA+jrgsWajaq0BeC3IQhCEIQhCKZw1MxTzSlNKnmJpivW9IHVPrTjvkkuI3sP7bWAEdIHWCbDsGsRkZ9IUJC9AhfZFbpqrmZBtI+ZvptWC/KCPrLOgFeRPOcI2Wyqjndf UWlNj+dgWpe1qSTEcdurXzMRAc5EihsEflmIN8RzuguWq61JWRQpSI51/KHHT/6/ztPZJ33SSKbieTa1C5koONbLcf9aYmsVh7RW6p3SpASnUSb3JuSvpUBKxscbyBjiOpOTq8jcdRsx5/IndXw3VgJV6iO1+6jl4gjVpWouViO6ih9ZmybSPkhaqyNUxVXpV5cYU+Xx5sQTfKystDLipmqaMhxIcgvplLqF/LWZzIS5PvwbqOvrSlNHVEYchCEIQISICSZJijwu5OrRQHDyUpaF0y///p6FEDCCDFsuW7YFoVEFESTOBAACLgLOrAAAAAggUAAAAtAAAAFJESEkNAAAAChoKDUdOUIk=
```

然后用base64解密，因为该字符串解密后有不可见字符的存在，所以部分解密工具会出现解密错误的可能，这时候就吃了没经验的亏，~~干了一些富有想象力的事情~~，走了一些弯路，好在最后找到了不会报错的工具（能勉强显示不可见字符）

gmBCrkRORUkAAAAA+jrgsWajaq0BeC3IQhCEIQhCKZw1MxTzSlNKnmJpivW9IHVPrTjvkkuI3sP7bWAEdIHWCbDsGsRkZ9IUJC9AhfZFbpqrmZBtI+ZvptWC/KCPrLOgFeRPOcI2Wyqjndf UWlNj+dgWpe1qSTEcdurXzMRAc5EihsEflmIN8RzuguWq61JWRQpSI51/KHHT/6/ztPZJ33SSKbieTa1C5koONbLcf9aYmsVh7RW6p3SpASnUSb3JuSvpUBKxscbyBjiOpOTq8jcdRsx5/IndXw3VgJV6iO1+6jl4gjVpWouViO6ih9ZmybSPkhaqyNUxVXpV5cYU+Xx5sQTfKystDLipmqaMhxIcgvplLqF/LWZzIS5PvwbqOvrSlNHVEYchCEIQISICSZJijwu5OrRQHDyUpaF0y///p6FEDCCDFsuW7YFoVEFESTOBAACLgLOrAAAAAggUAAAAtAAAAFJESEkNAAAAChoKDUdOUIk=

清空 加密 解密 ☐ 解密结果以16进制显示

R# (qxI')MB拓5S행t□)ㅠㅂ+鐒U□8順7□Fع
Ż z🔲9x5iZ□ɴ□ülUzU嗝|y□ㅋ-□□e. -fs!.O□깰Ђs□!□B□!"□Ib□ŢQP□<t.D □.큨TADI=□□□□□□□□□□□□□□□□RDHI
□□□
□

GNP

复制

上图中出现了一些很明显的png图片的标志，不过很明显都倒过来了，接着勾选`解密结果以16进制显示`

```
gmBCrkRORUkAAAAA+jrgsWajaq0BeC3IQhCEIQhCKZwlMxTzSlNKnmJpivW9IHVPrTjvkkuI3sP7bWAEdIHWCbDsGsRkZ9IUJC9AhfZFbpqrmZBtI+ZvptWC/KCPrL0gFeRPOcI2Wvqjndf UWlNj+dgWpelqSTEcdurXzMRAc5EihsEflmIN8RzuguWq6lJWRQpSI51/KHHT/6/ztPZJ33SSKbieTalC5koONbLcf9aYmsVh7RW6p3SpASnUSb3JuSvpUBKxscbyBjiOpOTq8jcdRsx5/IndXw3VgJV6iO1+6jl4gjVpWouViO6ih9ZmybSPkhaqvNUxVXpV5cYU+Xx5sQTfKystDLipmqaMhxIcgvp1LqF/LWZzIS5PvwbqOvrSlNHVEYchCEIQISICSZJijwu50rRQHDyUpaF0y///p6FEDCCDFsuW7YFoVEFEST0BAACLgLOrAAAAAggUAAAAtAAAAFJESEkNAAAAChoKDUdOUIk=
```

清空 加密 解密 ☑ 解密结果以16进制显示

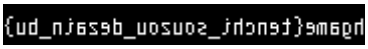
```
\x66 \xa3 \x6a \xad \x01 \x78 \x2d \xc8
\x42 \x10 \x84 \x21 \x08 \x42 \x29 \x9c
\x35 \x33 \x14 \xf3 \x4a \x53 \x4a \x9e
\x62 \x69 \x8a \xf5 \xbd \x20 \x75 \x4f
\xad \x38 \xef \x92 \x4b \x88 \xde \xc3
\xfb \x6d \x60 \x04 \x74 \x81 \xd6 \x09
```

复制

将上面的十六进制数据倒序记录在notepad++

Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
00000000	89	50	4e	47	0d	0a	1a	0a	00	00	00	0d	49	48	44	52	塒NG........IHDR
00000010	00	00	00	b4	00	00	00	14	08	02	00	00	00	ab	b3	80	...?........ €
00000020	8b	00	00	01	3d	49	44	41	54	68	81	ed	96	cb	16	83	?..=IDATh.頃??□□
00000030	20	0c	44	a1	a7	ff	ff	cb	74	a1	a5	94	3c	1c	50	b4	.D¨ 蔚¯?.P?
00000040	d2	b9	0b	8f	62	92	49	02	22	21	10	42	08	21	87	11	夜..b扦."!.B.!?
00000050	d5	d1	94	d2	fa	3a	ea	06	bf	4f	2e	21	73	66	2d	7f	昭斟??縊.!sf-.
00000060	a1	2e	65	fa	82	1c	12	87	8c	a6	9a	a9	b8	0c	2d	2b	?e鶤..噷 └.-+
00000070	2b	df	04	b1	79	7c	f9	14	c6	e5	55	7a	55	31	d5	c8	+?眹|?棋UzU1杖
00000080	aa	16	92	8f	b4	c9	66	d6	87	a2	ee	88	95	8b	5a	69	??瓷f謬㈩垥媄i□
00000090	35	82	78	39	ea	7e	ed	88	7a	95	80	d5	0d	5f	dd	89	5脩9陋師z睃?_輾
000000a0	fc	79	cc	46	1d	37	f2	ea	e4	a4	8e	38	06	f2	c6	b1	竜蘁.7蜿浹?.蚱?
000000b0	b1	12	50	e9	2b	b9	c9	bd	49	d4	29	01	a9	74	a7	ba	?P?股絀?. ?Ⅲ□
000000c0	15	ed	61	c5	9a	98	d6	7f	dc	b2	35	0e	4a	e6	42	ad	.韆艡.?懿5.J鋿?
000000d0	4d	9e	b8	29	92	74	df	49	f6	b4	f3	af	ff	d3	71	28	M灨)抉遼龂蟑 觯(
000000e0	7f	9d	23	52	0a	45	56	52	eb	aa	e5	82	ee	1c	f1	0d	..#R.EVR鵌鎥??□□
000000f0	62	96	1f	c1	86	22	91	73	40	c4	cc	d7	ea	76	1c	31	b?獿"甦@奶钻v.1□
00000100	49	6a	ed	a5	16	d8	f9	63	53	5a	d4	d7	9d	a3	2a	5b	Ij恁.仜cSZ宰.?[□
00000110	36	c2	39	4f	e4	15	20	bd	ac	8f	a0	fc	82	d5	a6	6f	6?O? 浆..鼇咋o□□
00000120	e6	23	6d	90	99	ab	9a	6e	45	f6	85	40	2f	24	14	d2	?m.樻齒E鱷@/$.?
00000130	67	64	c4	1a	ec	b0	09	d6	81	74	04	60	6d	fb	c3	de	gd?彀.?t.`m ?
00000140	88	4b	92	ef	38	ad	4f	75	20	bd	f5	8a	69	62	9e	4a	圛掞8璒u 锦姥b澱
00000150	53	4a	f3	14	33	35	9c	29	42	08	21	84	10	42	c8	2d	SJ?35?B.!?B?□□□□
00000160	78	01	ad	6a	a3	66	b1	e0	3a	fa	00	00	00	00	49	45	x.瑽 编:?...IE□
00000170	4e	44	ae	42	60	82											ND頭`?□

保存为png格式的图片，得到被水平翻转过的flag



进行水平翻转操作

好在这次没有肉眼识别flag的坑，得到flag：

> hgame{tenchi_souzou_dezain_bu}

misc Telegraph：1601 6639 3459 3134 0892

描述

他曾经最喜欢的曲师写的曲子，让人犹如漫步在星空之下，可如今他听见只觉得反胃。
由于文件名过长，单独给出附件的md5: E5C3EE3F441B860B07A3ADCD98BFFC00
请将flag以hgame{your_flag_here}形式提交，flag为全大写。

题目地址

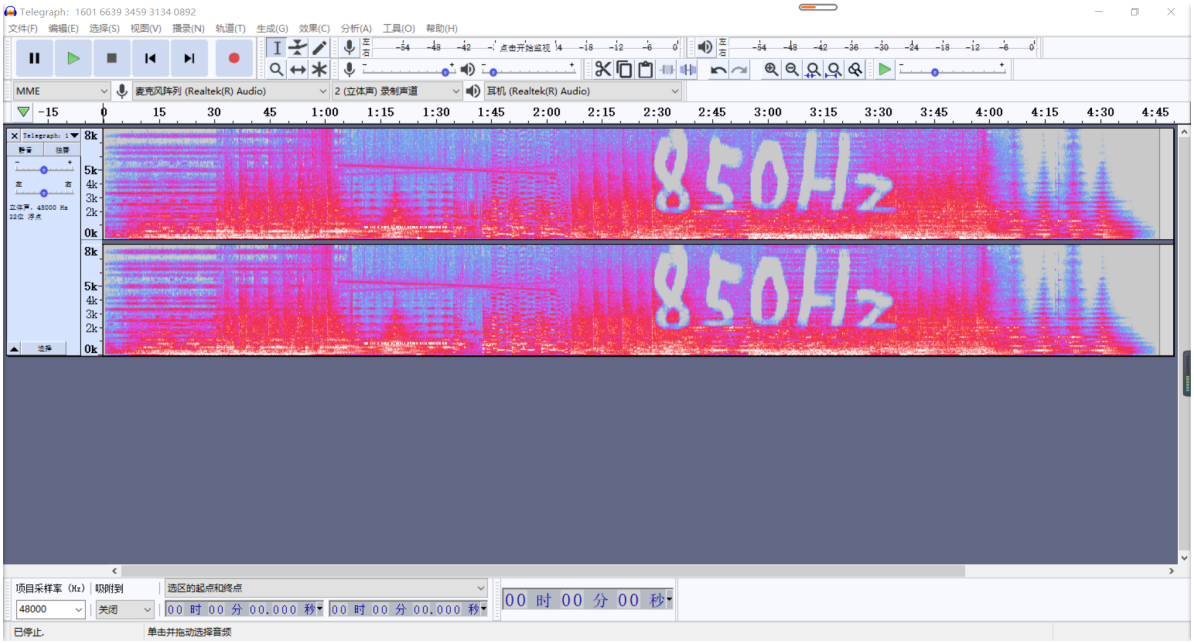
https://1.oss.hgame2021.vidar.club/Telegraph%EF%BC%9A1601%206639%203459%203134%200892.mp3

wp

作为没学过英语的孩子，首先得翻译一下`Telegraph`，得知后面跟的是电报码，用在线工具解密，发现是`带通滤波器`

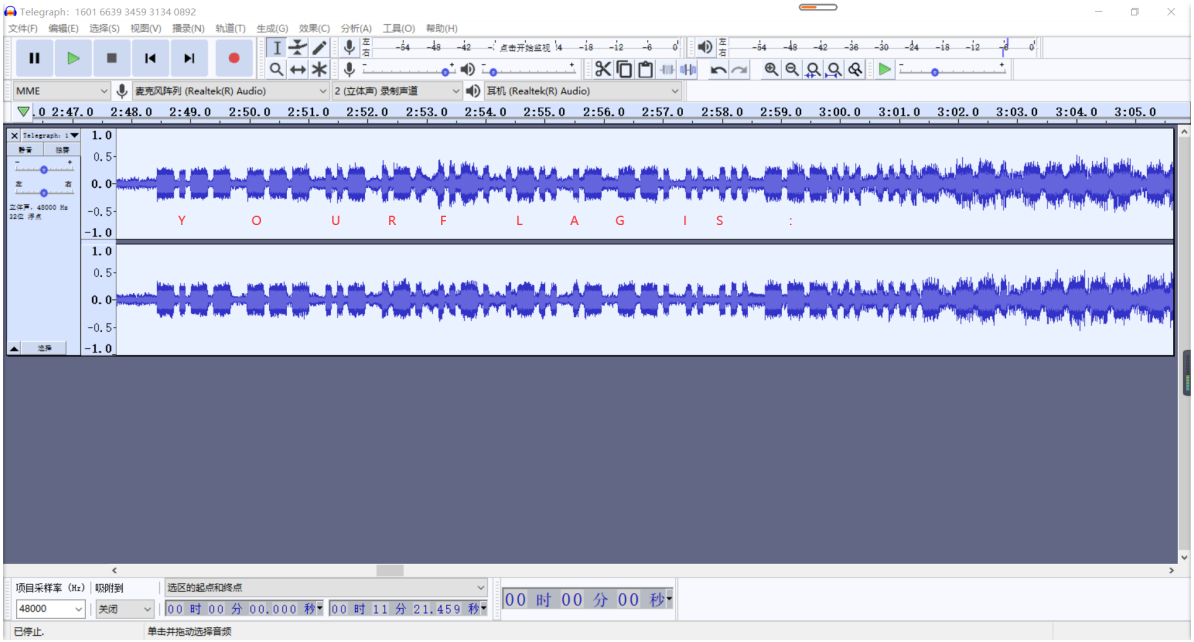
查了半天，也不知道这个与misc题目的联系

只好先下载MP3文件，用audacity打开，调成`频谱图`，得到：



再点击`效果`，我把`低通滤波器`和`高通滤波器`都改为`850Hz`试了试，啥也没看出来（解这道题我觉得完全可以不用到`带通滤波器`，乖乖等官方的题解了）

不死心的我，再换回`波形图`，然后将速率调为0.6，再将波形图放大到适当的大小，得到：



利用摩尔斯电码：

电码定义-字母

字符	电码符号	字符	电码符号	字符	电码符号
A	. −	B	− . . .	C	− . − .
D	− . .	E	.	F	. . − .
G	− − .	H	. . . .	I	. .
J	. − − −	K	− . −	L	. − . .
M	− −	N	− .	O	− − −
P	. − − .	Q	− − . −	R	. − .
S	. . .	T	−	U	. . −
V	. . . −	W	. − −	X	− . . −
Y	− . − −	Z	− − . .		

电码定义-数字

字符	电码符号	字符	电码符号	字符	电码符号
1	. − − − −	2	. . − − −	3	. . . − −
4	. . . . −	5	. . . . .	6	− . . . .
7	− − . . .	8	− − − . .	9	− − − − .
0	− − − − −				

> **电码定义-标点符号**
>
> | 字符 | 电码符号 | 字符 | 电码符号 | 字符 | 电码符号 |
> | --- | --- | --- | --- | --- | --- |
> | . | . – . – . – | : | – – – . . . | , | – – . . – – |
> | ; | – . – . – . | ? | . . – – . . | = | – . . . – |
> | ' | . – – – – . | / | – . . – . | ! | – . – . – – |
> | – | – . . . . – | _ | . . – – . – | " | . – . . – . |
> | (| – . – – . |) | – . – – . – | $ | . . . – . . – |
> | & | . . . . | @ | . – – . – . | | |

由此可得出flag：

> hgame{4G00DS0NGBUTN0T4G00DMAN039310KI}

web LazyDogR4U

描述

懒狗R4u把Flag藏起来了，但由于他是懒狗，所以flag藏的很不安全。

题目地址

http://c805224b7e.lazy.r4u.top

wp

在地址后面加了`/www.zip`，下载得到zip文件，发现里面有`flag.php`，打开得到：

```
<?php
session_start();

require_once 'lazy.php';


if(!isset($_SESSION['username'])){
    die('您配吗？');
}
?>


<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>Document</title>
    <link rel="stylesheet" href="static/style.css">
</head>

<body>
<form class="box" action="" method="post">
    <?php

    if($_SESSION['username'] === 'admin'){
        echo "<h3 style='color: white'>admin将于今日获取自己忠实的flag</h3>";
        echo "<h3 style='color: white'>$flag</h3>";
    }else{
        if($submit == "getflag"){
            echo "<h3 style='color: white'>{$_SESSION['username']}接近了问题的终点</h3>";
        }else{
            echo "<h3 style='color: white'>篡位者占领了神圣的页面</h3>";
        }
    }
        ?>
    <input type="submit" name="submit" value="getflag">
</form>
</body>

</html>
```

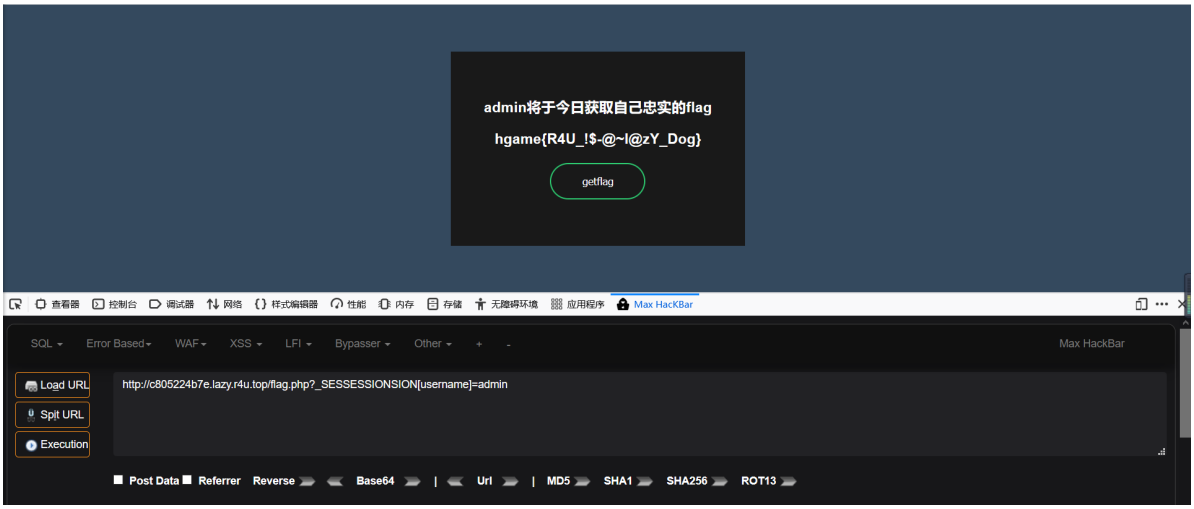
然后将地址后缀改成`/flag.php`，不出所料，页面显示：

> 您配吗?

看样子路没走错，根据flag.php的内容走就好了，这里也没什么奇奇怪怪的函数

然后打开`Hackbar`，先Laod URL，再跟上`?_SESSION[username]=admin`，再Execution，但是不好使

看到hint里的`变量覆盖`，那么如下：



得到flag：

> hgame{R4U_!$-@~l@zY_Dog}

crypto WhitegiveRSA

描述

N = 882564595536224140639625987659416029426239230804614613279163
e = 65537
c = 747831491353896780365654517748216624798517769637260742155527

题目地址

https://www.baidu.com

wp

因为bugku有rsa的题，所以就对着题解做（脚本也全出自下方链接）

https://blog.csdn.net/weixin_43211186/article/details/102997250

先用在线工具分解出两个质数p，q

Search | Sequences | Report results | Factor tables | Status | Downloads | Login

882564595536224140639625987659416029426239230804614613279163 Factorize!

Result:

status (?)	digits	number
FF	60 (show)	8825645955...63<60> = 857504083339712752489993810777<30> · 10292249479429980750803486472 19<31>

More information

ECM

利用下面代码解出m（python37）

```
import binascii
import sys
sys.setrecursionlimit(1000000)
def ByteToHex(bins):
    return ''.join(["%02X" % x for x in bins]).strip()
def n2s(num):
```

```
    t = hex(num)[2:-1]  # python
    if len(t) % 2 == 1:
        t = '0' + t
    #print(t)
    return(binascii.a2b_hex(t).decode('latin1'))
def egcd(a, b):
    if a == 0:
        return (b, 0, 1)
    else:
        g, y, x = egcd(b % a, a)
        return (g, x - (b // a) * y, y)
def modinv(a, m):
    g, x, y = egcd(a, m)
    if g != 1:
        print('modular inverse does not exist')
        return 'null'
    else:
        return x % m
c = 747831491353896780365654517748216624798517769637260742155527
p = 85750408333971275248999381077 7
q = 10292249479429980750803486472 19
e = 65537
n = p * q
d = modinv(e, (p - 1) * (q - 1))
m = pow(c, d, n)
print(m)
```

再用下面代码（python27）

```
import binascii


def n2s(num):
    t = hex(num)[2:-1]  # python
    if len(t) % 2 == 1:
        t = '0' + t
    # print(t)
    return binascii.a2b_hex(t).decode('latin1')

print(n2s(25599744719368613322506956018967498313805867172277298220 77))
```

得到flag：

> hgame{w0w~yOU_kNoW+R5@!}