Chive WriteUp

原创

WustHandy 于 2020-04-20 13:12:43 发布 952 收藏 2

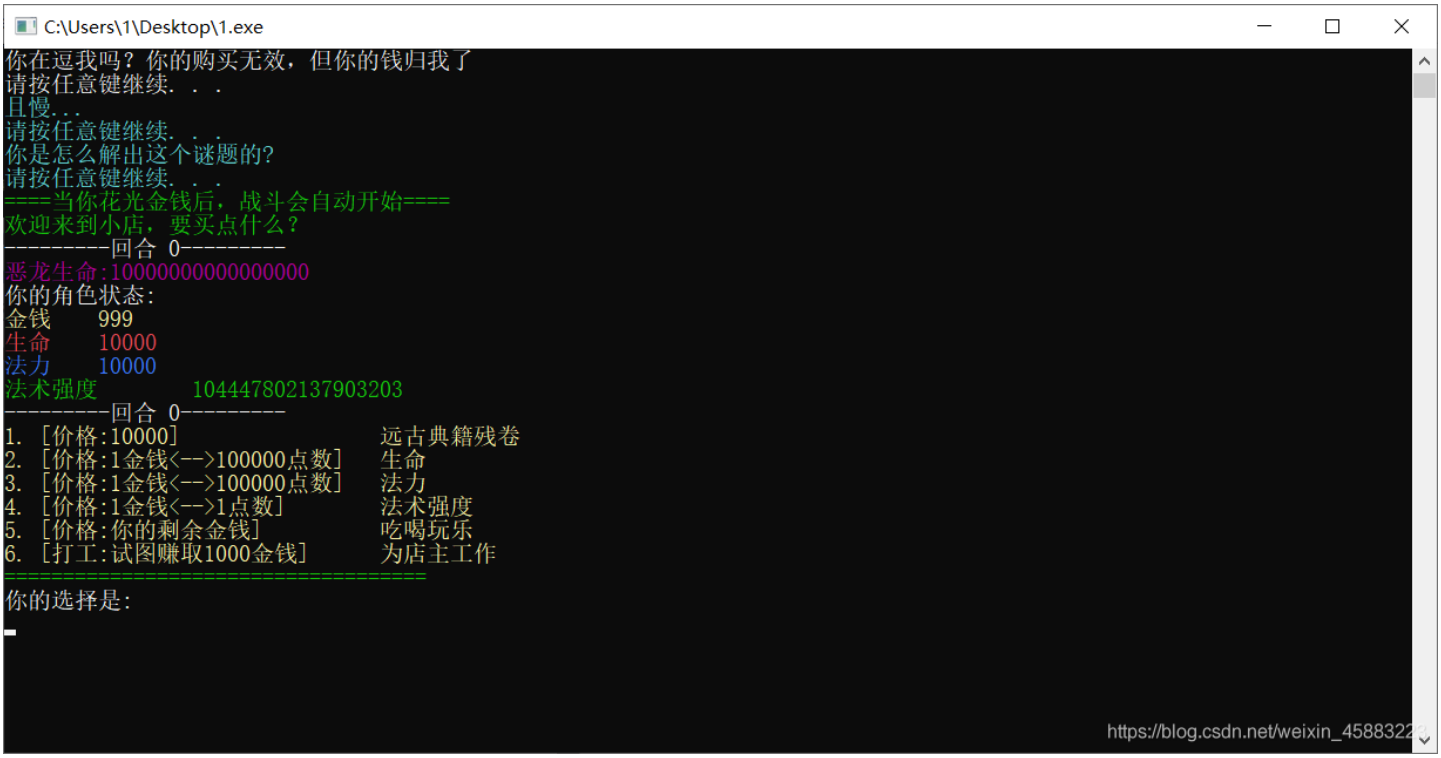
分类专栏： WriteUp 文章标签： 信息安全

Chive WriteUp

签到

小游戏

先打工赚钱买“远古典籍残卷”得到提示，然后买法术强度时输入-1，法强会变很大，再打工买生命值打败恶龙拿到flag。



magicCube

按F12在调试器里搜索flag{。

re

doyouknowida

拖到ida里第一个页面就显示了flag

web

index.?

url最后加/index.php后按F12，flag在注释里。

勇者斗恶龙

F12改一下打史莱姆的maxlength，练级到刚好比可以挑战恶龙的10000战斗力多一点点（等级100），挑战恶龙，领取flag。

勇者谎称斗恶龙

提示是这个

只要取得打败恶龙的证据就可以了

查看源代码

```
//挑战恶龙
function boss()
{
    var aexp = 0;
    var num = 1;
    var enemy = elong;
    if(power>=enemy)
    {
        aexp = 1;
        hexp += aexp;
        document.getElementById("reflection").innerHTML="战斗成功,获得经验值"+aexp+"!";
        levelup();
        document.getElementById("solve").value=0;
    }
    else
    {
        document.getElementById("reflection").innerHTML="你被打败了，对方的战斗力为"+enemy+",经验值损失一半！";
        hexp /= 2;
        hexp = Math.floor(hexp);
        levelup();
    }
}
```


在控制台输入if(power>=enemy)后的语句就可以领取flag。

catchME

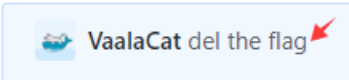
打开发现博客的内容和首页存在301跳转，用BP抓第一个页面的包，send to repeater，send看response。

magicpassword

万能密码

GITHUB

在GitHub搜索作者名字，找到最新的一篇博客，点这个。

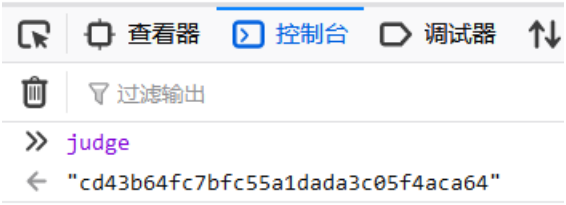


一百万猜数

查看源代码，guess是自己输入的数

```
function check()
{
    var guess = document.getElementById("guess").value;
    fff = guess;
    times += 1;
    if(finish == 1)
        return;
    if(times == 2)
        return;
    if(md5(md5(guess)) == judge)
        {
            finish = 1;
            solve = 1;
            flag();
        }
    if(times == 1 && finish != 1)
        {
            document.getElementById("respond").innerHTML="很遗憾你没有猜对，答案是"+num;
            finish = 1;
        }
}
```


控制台可以查看judge的值，md5解码即可。



生日快乐

选第二个卡片和2000年，随便输月日，用BP抓包，在intruder里爆破一下月日即可。

ezheader

用BP抓包，按照提示要求，先加上127.0.0.1，发现BAN了XFF头，就用Client-IP，再按提示改User-Agent和Referer。

magicMD5

用dirsearch扫描目录发现有/index.php.bak，在url最后加上得到这个，开始代码审计。

```php
<?php
    echo "do you know how i backup my file<br><br>";
    $a1=$_GET['a1'];
    $a2=$_GET['a2'];
    $b1=$_GET['b1'];
    $b2=$_GET['b2'];
    $c1=$_POST['c1'];
    $c2=$_POST['c2'];
    $d1=$_POST['d1'];
    $d2=$_POST['d2'];
    if(is_numeric($a1)&&(!is_numeric($a2))&&intval($a1)==intval($a2)){
        echo 'level 1 pass<br>';
    }else{
        die('get out');
    }

    if($b1!=$b2&&md5($b1)==md5($b2)){
        echo 'level 2 pass<br>';
    }else{
        die('get out');
    }

    if($c1!==$c2&&md5($c1)===md5($c2)){
        echo 'level 3 pass<br>';
    }else{
        die('get out');
    }

    if((string)$d1!==(string)$d2&&md5($d1)===md5($d2)){
        echo 'level 3 pass<br>';
    }else{
        die('get out');
    }

    $flag = 'flag_here';
    echo "<!-- ".$flag." -->";
?>
```

利用php的md5漏洞构造如下：

```
http://vps.vaala.cat:28013/?a1=1&a2[]=1&b1=s878926199a&b2=s155964671a
```

Post data

```
c1[]=1&c2[]=2&d1=%4d%c9%68%ff%0e%e3%5c%20%95%72%d4%77%7b%72%15%87%d3%6f%a7%b2%1b%dc%56%b7%4a%3d%c0%78%3e%7b%95%18%af%bf%a2%00%a8%28%4b%f3%6e%8e%4b%55%b3%5f%42%75%93%d8%49%67%6d%a0%d1%55%5d%83%60%fb%5f%07%fe%a2&d2=%4d%c9%68%ff%0e%e3%5c%20%95%72%d4%77%7b%72%15%87%d3%6f%a7%b2%1b%dc%56%b7%4a%3d%c0%78%3e%7b%95%18%af%bf%a2%02%a8%28%4b%f3%6e%8e%4b%55%b3%5f%42%75%93%d8%49%67%6d%a0%d1%d5%5d%83%60%fb%5f%07%fe%a2
```

正则公主的秘密日记

F12在注释里发现了正则表达式

```
/^I?\sa+m*\sp{4}r{2,}i{1,2}(nc)*\w\s[of]?\s[a-z]{5}$/
```

构造如下（有多种）

I amm pppprrincnce f aaaaa

贷款

url里发现了
data=5d4aace023dc088767b4e08c79415dcd80432911e07b111f6a05fd7c904c1bc9
md5加密后应是32位，而这是64位，从中间分成两端分别md5解码再base64解码，得到了10和0，分别对应持有金钱和所欠款额的值，把一个大于100的数base64加密再md5加密填入url即可去商店买flag。

crypto

你以为这是普通的栅栏？

W型栅栏密码

ez_RSA

根据e,p,q写py解d

```
import gmpy2

e = 17
p = 8169558889361
q = 1513871

d = gmpy2.invert(e, (p-1)*(q-1))
print(d)
```

use_the_keyboard

先base64解码再在键盘上看每四个字符圈起来的中间的字符

皇帝的flag

把txt拖进winhex里

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
E5	87	BA	E9	A2	98	E4	BA	BA	E5	B1	85	E7	84	B6	E7	å‡°é¢˜ä°°å±…ç„¶ç
9B	B4	E6	8E	A5	E7	BB	99	E4	BD	A0	66	6C	61	67	E4	›´æŽ¥ç»™ä½ flagä
BA	86	EF	BC	9A	66	6C	61	67	7B	E2	80	8D	E2	80	8D	°†ï¼šflag{â€ â€
E2	80	8C	E2	80	8C	E2	80	8B	E2	80	8C	E2	80	8B	E2	â€Œâ€Œâ€‹â€Œâ€‹â
80	8C	E2	80	8D	E2	80	8C	E2	80	8B	E2	80	8D	E2	80	€Œâ€ â€Œâ€‹â€ â€
8D	E2	80	8D	E2	80	8B	E2	80	8C	E2	80	8D	E2	80	8D	â€ â€‹â€Œâ€ â€
E2	80	8B	E2	80	8C	E2	80	8C	E2	80	8B	E2	80	8D	E2	â€‹â€Œâ€Œâ€‹â€ â
80	8C	E2	80	8C	E2	80	8B	E2	80	8D	E2	80	8B	E2	80	€Œâ€Œâ€‹â€ â€‹â€
8C	E2	80	8C	E2	80	8C	E2	80	8C	E2	80	8B	E2	80	8D	Œâ€Œâ€Œâ€Œâ€‹â€
E2	80	8D	E2	80	8B	E2	80	8D	E2	80	8D	E2	80	8D	E2	â€ â€‹â€ â€ â€ â
80	8B	E2	80	8C	E2	80	8D	E2	80	8C	E2	80	8B	E2	80	€‹â€Œâ€ â€Œâ€‹â€
8C	E2	80	8C	E2	80	8C	E2	80	8B	E2	80	8C	7D	EF	BC	Œâ€Œâ€Œâ€Œâ€‹â€Œ}ï¼
8C	E4	BD	A0	E7	9C	8B	E5	88	B0	66	6C	61	67	E4	BA	Œä½ çœ‹å^°flagä°
86	E5	90	97	EF	BC	9F										†å¯—ï¼Ÿ

根据utf-8的无宽度字符转换为摩斯电码再解码

U+200B		\xe2\x80\x8b	ZERO WIDTH SPACE
U+200C		\xe2\x80\x8c	ZERO WIDTH NON-JOINER
U+200D		\xe2\x80\x8d	ZERO WIDTH JOINER

misc

菩提本无树，明镜亦非台

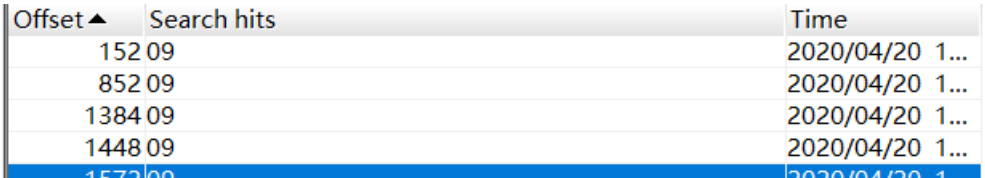
与佛论禅发现不对，全选后字体颜色改为红色发现下面还有一段，把下面的与佛论禅。

害怕黑暗吗

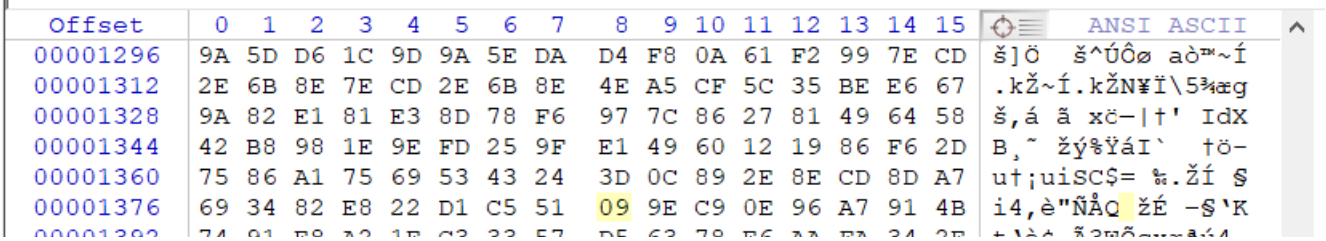
用stegsolve打开图片，按左右方向键

give_you_flag

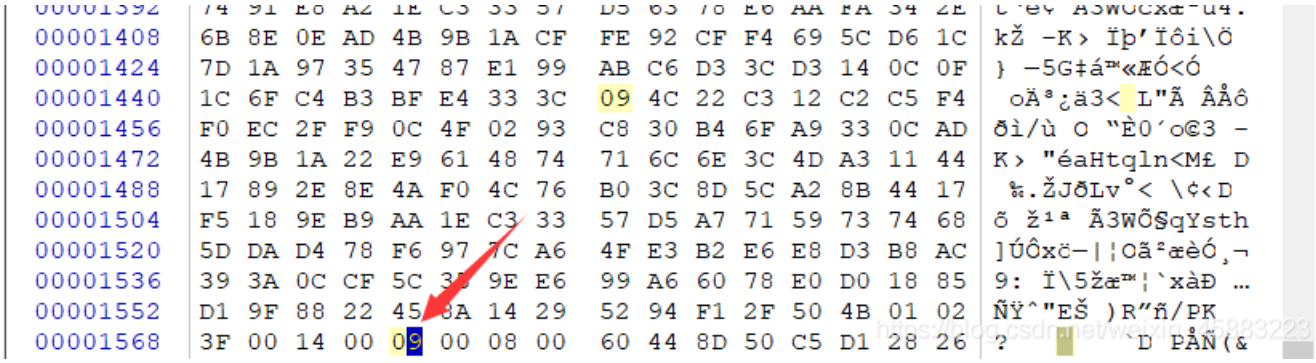
需要密码，把zip压缩包放进winhex，发现是伪加密



Offset ▲	Search hits	Time
152	09	2020/04/20 1...
852	09	2020/04/20 1...
1384	09	2020/04/20 1...
1448	09	2020/04/20 1...
1572	09	2020/04/20 1...

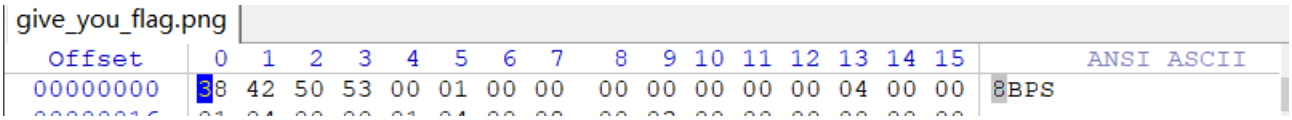


Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00001296	9A	5D	D6	1C	9D	9A	5E	DA	D4	F8	0A	61	F2	99	7E	CD	š]Ö š^ÚÔø aò™~Í
00001312	2E	6B	8E	7E	CD	2E	6B	8E	4E	A5	CF	5C	35	BE	E6	67	.kŽ~Í.kŽN¥Ï\5¾æg
00001328	9A	82	E1	81	E3	8D	78	F6	97	7C	86	27	81	49	64	58	š,á ã xö–|†' IdX
00001344	42	B8	98	1E	9E	FD	25	9F	E1	49	60	12	19	86	F6	2D	B¸˜ žý%ŸáI` †ö-
00001360	75	86	A1	75	69	53	43	24	3D	0C	89	2E	8E	CD	8D	A7	u†¡uiSC$= ‰.ŽÍ §
00001376	69	34	82	E8	22	D1	C5	51	09	9E	C9	0E	96	A7	91	4B	i4,è"ÑÅQ žÉ –§'K



00001392	74	91	E8	A2	1E	C3	33	57	D5	63	78	E6	AA	FA	34	2E
00001408	6B	8E	0E	AD	4B	9B	1A	CF	FE	92	CF	F4	69	5C	D6	1C
00001424	7D	1A	97	35	47	87	E1	99	AB	C6	D3	3C	D3	14	0C	0F
00001440	1C	6F	C4	B3	BF	E4	33	3C	09	4C	22	C3	12	C2	C5	F4
00001456	F0	EC	2F	F9	0C	4F	02	93	C8	30	B4	6F	A9	33	0C	AD
00001472	4B	9B	1A	22	E9	61	48	74	71	6C	6E	3C	4D	A3	11	44
00001488	17	89	2E	8E	4A	F0	4C	76	B0	3C	8D	5C	A2	8B	44	17
00001504	F5	18	9E	B9	AA	1E	C3	33	57	D5	A7	71	59	73	74	68
00001520	5D	DA	D4	78	F6	97	7C	A6	4F	E3	B2	E6	E8	D3	B8	AC
00001536	39	3A	0C	CF	5C	3D	9E	E6	99	A6	60	78	E0	D0	18	85
00001552	D1	9F	88	22	45	8A	14	29	52	94	F1	2F	50	4B	01	02
00001568	3F	00	14	00	09	00	08	00	60	44	8D	50	C5	D1	28	26

把这个9改成0保存就可打开里面的png图片，发现不是png格式，放进winhex查看发现文件头是8BPS，应该是.psd文件

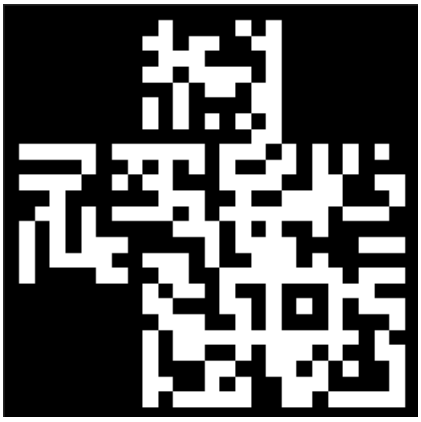


give_you_flag.png

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	38	42	50	53	00	01	00	00	00	00	00	00	00	04	00	00	8BPS

改成.psd后

放进PS



Ctrl+i反色后导出，用画图软件补齐三个角扫描二维码。

搏击第五空间

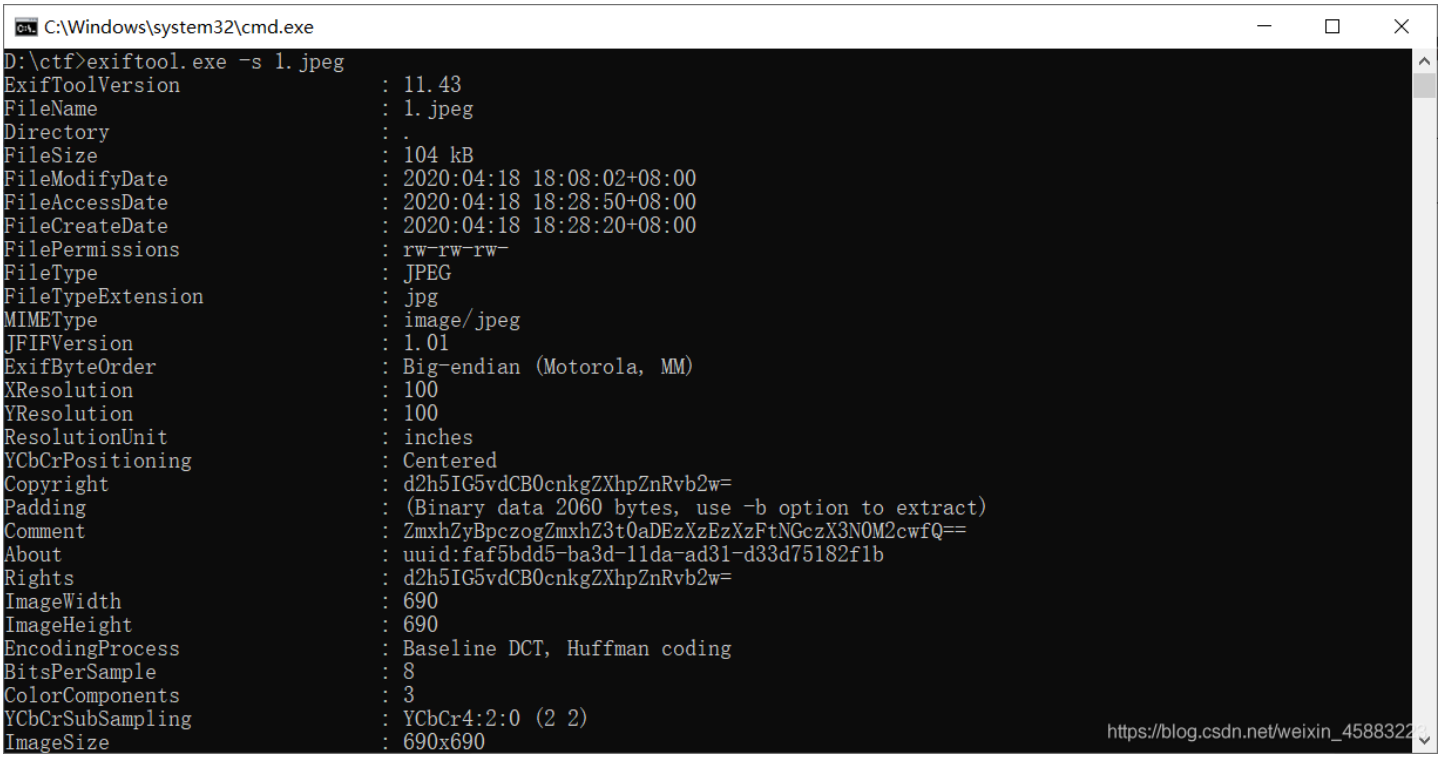
属性的详细信息的版权是base64，解码

d2h5IG5vdCB0cnkgZXhpZnRvb2w=

编码 base64

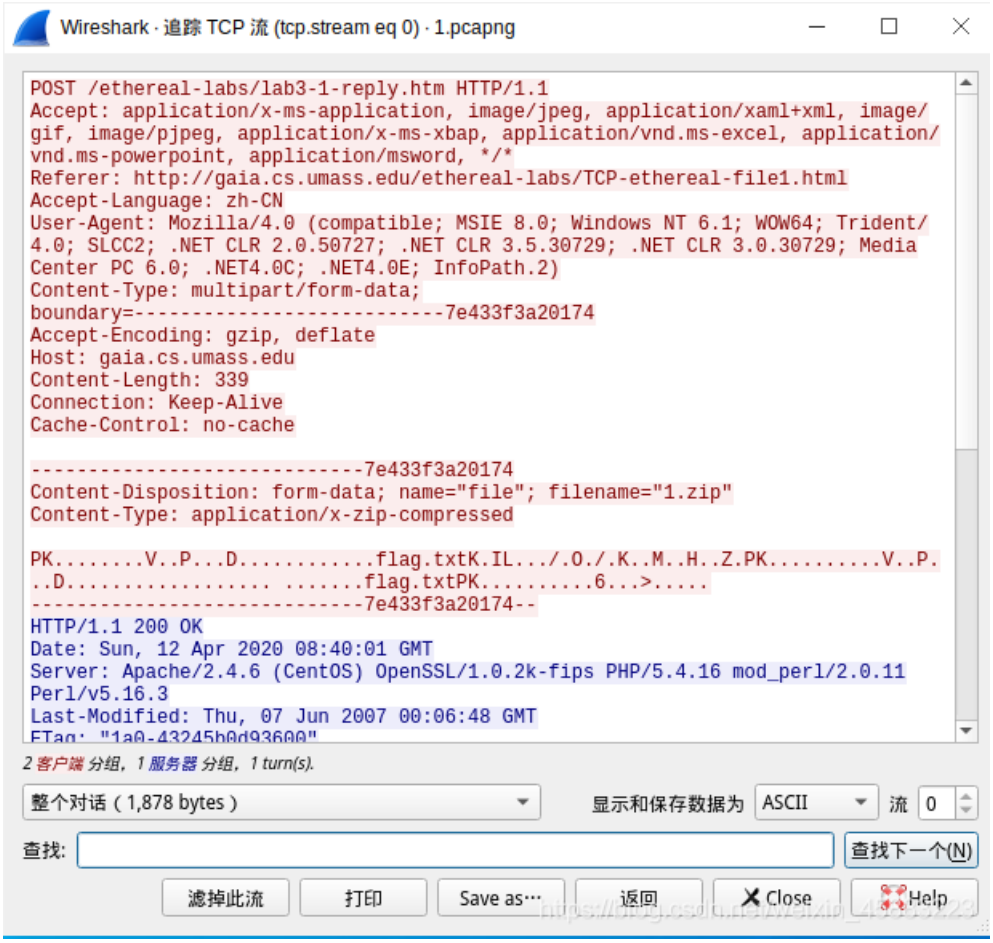
why not try exiftool

下载exiftool，把Comment后的base64解码



简单流量分析

用kali的wireshark打开.pcapng文件，右键-追踪流-TCP流



把“显示和保存数据为”改为原始数据，导出，再把导出文件用foremost分离出，在output里有压缩包，里面有flag.txt

君は薔薇より美しい

图片用winhex打开，改一下宽高

B站搜索BV号，下载视频，用ffmpeg分离出一个个图片，把黑白小方格转为二进制再转为字符串。