# 攻防世界-CTF小白-MISC(新手)

# 原创

王耶 ● 于 2020-05-09 21:53:09 发布 ● 3096 ◆ 收藏 28
分类专栏: CTF 文章标签: 信息安全
版权声明:本文为博主原创文章,遵循 CC 4.0 BY-SA 版权协议,转载请附上原文出处链接和本声明。
本文链接: https://blog.csdn.net/weixin\_43550772/article/details/106028357
版权

# C

CTF 专栏收录该内容

5 篇文章 1 订阅 订阅专栏 我会一题一题的做,因为也是新手所以我会尽可能的写的清楚明白

后面所需要的工具我会慢慢发出来,也可以私信我

# MISC新手区

# 1、this\_is\_flag

题目描述: Most flags are in the form flag{xxx}, for example:flag{th1s\_!s\_a\_d4m0\_4la9} 答案很明显告诉你了前面写着flag的格式 flag{} 后面告诉你了flag 很明显

flag{th1s\_!s\_a\_d4m0\_4la9}

# $2_{\gamma}$ pdf

题目描述:菜猫给了菜狗一张图,说图下面什么都没有



打开是一张这样是pdf图片,题目说图下面什么都没有,那可以想想flag可能在图片下面 我发现了两种做法,第一种是pdf转换成word,还有一一个就是,pdf图片点一点,发现中间鼠标图标会变成 I



大概这个位置,直接全选复制粘贴出来就是flag了

flag{security\_through\_obscurity}

3、give\_you\_flag

题目描述:菜狗找到了文件中的彩蛋很开心,给菜猫发了个表情包 附件保存打开后是一个GIF,发现有一帧弹出了二维码 用动图分离工具分解后得到如果没有工具需要下载一个喔



打开后发现缺少定位符,要手动补上去,我是用随便二维码定位符截取下来然后PS上去



那三个就是我P上去的然后手机微信二维码扫一下就有了

 $\times$ 扫描结果

# $flag\{e7d478cf6b915f50ab1277f78502a2c5\}$

https://blog.csdn.net/weixin\_43550772

flag{e7d478cf6b915f50ab1277f78502a2c5}

# 4、坚持60s

题目描述: 菜狗发现最近菜猫不爱理他,反而迷上了菜鸡 打开后是一个小游戏,要撑过60s,然后太难了,我办不到



# 然后我使用jd-gui打开发现flag,但是,是base64位,所以解码一下就好啦

🍵 Java Decompiler - PlaneGameFrame.class							— [	⊐ ×	<
File Edit Navigate Search Help									
🚖   😂 🖋   🗢 🔿									
9dc125bf1b84478cb14813d9bed6470c.jar $\times$									Ŧ
E META-INF	MANIFEST.M	F MyFrame.class	Bullet.class	Explode.class	GameObject.class	Plane.class	PlaneGameFrame.class	×	Ţ
MANIFEST.MF	1								-
n.bjsxt	51	printInfo(g, "兄	弟就死了的嘛	", 50, 150, 20	0);				
i plane	52	int period - (int	t)//this and	Time getTime()	this startTime	actTime())	( 10001) -		
⊞ 🗾 Bullet	54	printInfo(g, "你	的持久度才",	+ period + "秒	", 50, 150, 250);	.getiime())	/ 10005);		
Explode									
GameObject	56	switch (period /	10) {						
	58	printInfo(g, "	真.头顶一片青	青草原", 50,	150, 300);				密
	59	break;							5
	61	case 1:	这在市场地展	松梯井2 " 50	150 2001 -				
	62	break;		124 <b>2</b> m : , 30,	130, 300),				
		case 2:							
	64	printInfo(g, "	如果梦想有颜:	<b>色,</b> 那一定是原	谅色", 40, 30, 30	0);			
	0.5	case 3:							
	67	printInfo(g, "	哟,炊事班长	讶兄弟", 50, 1	50, 300);				
	68	break;							-
	70	printInfo(g, ")	加油你就是下	一个老王", 50,	150, 300);				
	71	break;							
	73	case 5:	加星塔过一分	钟我曾不是很没	雨子" 40 30 30	0) •			
	74	break;	xex	an ski eshi venkibe		~,,			
	76	case 6:							
	70	printinio(g, ": break:	flag{RGFqaURI	nbGlfSmlud2FuQ	2npamk=}", 50, 15	0, 300);			
		}							
	, I.I.,								
	publ	lic void printInfo	o(java.awt.G	raphics g, Str	ing str, int size	, int x, int	t у)		
	90 <sup>1</sup> Co	olor c = g.getColo	or();						
	91 a	setColor(Colbr.R	ED):						



#### base64解密网站

flag{DajiDali\_JinwanChiji}

## 5、gif

题目描述: 菜狗截获了一张菜鸡发给菜猫的动态图, 却发现另有玄机

附件下载解压后有两个文件夹

gif	143.30 KB	46.13 KE	
MACOSX	1 KB	1 KE	

有个gif的文件夹打开后发现里面有104张的黑白照片,这时候就考验计算机的基本功啦,我是联想到了二进制



这些是我得到的二进制数,运用python运行



#### 得到结果

flag{FuN\_giF}

6、掀桌子

题目描述: 菜狗截获了一份报文如下

c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e8eaf9 eaf3e2e4e6f2, 生气地掀翻了桌子(╯°□°) ╯ ⌒ ┶━━┶

啥也不说,上脚本

```
string = "c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e8
eaf9eaf3e2e4e6f2"
flag = ''
for i in range(0,len(string), 2):
    s = "0x" + string[i] + string[i+1]
    flag += chr(int(s, 16) - 128)
print(flag
```

flag{hjzcydjzbjdcjkzkcugisdchjyjsbdfr}

是用PYthon

可能有别的更快的方法,但是我觉得写代码还是要会的 这一题我是参考https://adworld.xctf.org.cn/task/writeup?type=misc&id=5105&number=1&grade=0&page=1这个链接的

## 7、如来十三掌

#### 题目描述: 菜狗为了打败菜猫, 学了一套如来十三掌。 附件下载后打开是

夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀 諳怖奢智侄諸若奢數苔奢集遠俱老竟寫明奢搭梵等盧皤豆蒙密離怯婆皤礙他哆提哆 多缽以南哆心曰姪罰蒙呐神。舍切真怯勝呐得俱沙罰娑是怯遠得呐數罰輸哆遠薩得 槃漫夢盧皤亦醯呐娑皤瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇 輸奢恐豆侄得罰提哆伽諳沙楞缽三死怯摩大蘇者數一遮↩

#### 在与佛论禅上解密

MzkuM3gvMUAwnzuvn3cgozM	lMTuvqzAenJchMUAeqzWenzE	mLJW9	
听佛说宇宙的真谛	参悟佛所言的真意		普度众生
	心不动,	万物皆不动	
佛曰: 夜哆悉諳多苦奢陀着 著集臺俱老貴寫明著若梵等 娑是怯遠得呐數罰輸哆遠頗 輸奢恐豆侄得罰提哆伽諳沙	諦冥神哆盧穆皤三侄三即尉 盧皤豆蒙密離性婆皤礙他吃 得槃漫夢盧皤亦醯呐娑皤 時 時 時 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	儲證即冥迦冥隸數顛耶迦奢若吉怯吃諳怖奢待 發提哆多砵以南哆心曰姪罰蒙呐神。舍切真怕 歸儲音尼摩罰薩冥大倒參夢侄阿心罰等奢大度	譻侄諸若奢數菩 去勝呐得俱沙罰 寛地冥殿皤沙蘇
		https://blog.csdn.net/weixir	_43550772

这里很dog你要加佛曰...才能参悟佛所言的真意 解密后是

MzkuM3gvMUAwnzuvn3cgozMIMTuvqzAenJchMUAeqzWenzEmLJW9

因为比较像base64所以base64解密,发现不对,怀疑可能是被置换了,用rot-13解码得 rot-13解码计算器

ZmxhZ3tiZHN jamhia 3 ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

base64解密得到flag base64加密解密

flag{bdscjhbkzmnfrdhbvckijndskvbkjdsab}

```
ps一条 ROT-13(回转13位,rotateby13places,有时中间加了个减号称作ROT-13)是一种简易的置换暗码。所以会考虑是 ROT-13
```

#### 8、stegano

#### 附件打开啥也不是,就全部复制下来到notepad++里面看看发现顶上有一串

盲猜摩斯密码把"A"替换为".","B"替换为"-",摩斯解密得到flag:

#### 附上解密在线网站摩斯密码解密

flag{1nv151bl3m3554g3}

#### 9、SimpleRAR

题目描述: 菜狗最近学会了拼图,这是他刚拼好的,可是却搞错了一块(ps:双图层) 下载压缩包后解压发现有两个文件,但是有一个提示文件头损坏(不建议用好压,因为不会报错,当然别的电脑会不会我就不清 楚啦)



问题就出在这几个地方,首先看文件头是正常的符合rar52-21,可以判断not here后面就是想要的文件了百度看了一下

#### 要的是文件块而不是子块,所以修改7A为74

	) 📑 🗔 🕹 8	۱	' 🕤		5	<b>b</b> (	30	3 68	101- 010	l d	4 <i>#</i>	HEX	≜. ₽B	<b>₩</b> HE×	-	→ -{	N 🔶	• 🔶 😂 🍣 📾 🔎 •	ļ
1	8c5326aada049	9eafb	e03a	ad															
	👫 18c5326aada	0499	eafb	e03a	d8a5	2e40	)c.rar												
	Offset	0	1	2	3	4	- 5	6	- 7	8	- 9	A	В	C	D	Е	F	^	
	00000000	52	61	72	21	1A	07	00	CF	90	73	00	00	OD	00	00	00	Rar! Ïs	
	00000010	00	00	00	00	D5	56	74	20	90	2D	00	10	00	00	00	10	ÕVt -	
	00000020	00	00	00	02	C7	88	67	36	6D	BB	4E	4B	1D	30	08	00	Ç∎g6m≫NK O	
	00000030	20	00	00	00	66	6C	61	67	2E	74	78	74	00	ΒO	57	00	flag.txt °W	
	00000040	43	66	6C	61	67	20	69	73	20	6E	6F	74	20	68	65	72	Cflag is not her	
	00000050	65	Α8	3C	7A	20	90	2F	00	ЗA	15	00	00	42	16	00	00	e <sup>∵</sup> ≺z ∕; B	
	00000060	02	BC	Ε9	8C	2F	6E	84	4F	4B	1D	33	ΟA	00	20	00	00	¼é∣∕n∣OK 3	
	00000070	00	73	65	63	72	65	74	2E	70	6E	67	00	FΟ	40	AB	18	secret.png ð@«	
	00000080	11	C1	11	55	08	D1	55	80	OD	99	C4	90	87	93	22	19	n ásu ñuin 183559772	
		·			· -	- ·			• -				— ·		· -	· -			

🔛 18c5326aada	0499	eafbe	e03a	d8a5	2e40	c.rar											
Offset	0	1	2	3	4	- 5	6	- 7	8	- 9	A	В	C	D	Е	F	
00000000	52	61	72	21	1A	07	00	CF	90	73	00	00	OD	00	00	00	Rar! Ï s
00000010	00	00	00	00	D5	56	74	20	90	2D	00	10	00	00	00	10	ÕVt -
00000020	00	00	00	02	С7	88	67	36	6D	BB	4E	4B	1D	30	08	00	Ç∎g6m≫NK O
00000030	20	00	00	00	66	6C	61	67	2E	74	78	74	00	BO	57	00	flag.txt °W
00000040	43	66	6C	61	67	20	69	73	20	6E	6F	74	20	68	65	72	Cflag is not her
00000050	65	Α8	ЗC	74	20	90	2F	00	ЗA	15	00	00	42	16	00	00	eï≺t ∕: B
00000060	02	BC	Ε9	8C	2F	6E	84	4F	4B	1D	33	ΟA	00	20	00	00	¼é∎∕n∎OK 3

#### 保存后退出解压,这个文件就出现了



解压出来后是空白的图片

https://blog.csdn.net/weixin\_43550772

#### 再用winhex打开查看发现是GIF文件,头为474946

导航	(N)	查看	(V)	I.	具(	T)	€业	Τ具	(I) j	先项((	<b>)</b> i	窗口
		3		٩	3	1	1 🔄		5	BB (	Ð (	<u>3</u> (
	sec	ret.p	ng									
	HEX	secr	ret.p	ng								
		Of	fse	t		0	1	2	3	- 4	- 5	1
	(	000	000	00		47	49	46	38	39	61	1
	(	000	000	10	Τ	FF	FF	FF	FF	FF	FF	01
	(	000	000	20		44	61	74	61	58	4D	51

修改后缀为.gif打开发现还是空白,那既然是gif就给他图层分离试试,把每一帧都分离出来

1	- □ ×
	✓ ひ 搜索"1" ク
	🕅 GifSplitter —
	输入 Gibli回文件: C:\Users\12437\Desktop\secret.gif
IMG00000.bmp IMG00001.bmp	Gif 信息: 280 × 280 (像素) , 2帧 状态: 就绪
	输出 图像输出目录: C:\Users\12437\Desktop\1\
	□ 以文件名自动创建输出文件夹 □ 对透明的Gii采用单色背景
	开始分离     关于     退出

我是使用这个软件分离出来,然后分别用steglove分析,打开软件后open两张图片然后一直>得到两个残缺的二维码图片然后合在一起





将两幅二维码拼接到一起并补全定位点,扫描二维码得到flag可用QR Research V1.0 ,也可以直接PS然后扫一下就出flag了



flag{yanji4n\_bu\_we1shi}

10、base64stego

首先下载附件,得到一个压缩包,发现有密码。 先去kali binwalk命令暴力破解发现破解不在这里插入图片描述了 这个时候就用winhex打开。 压缩源文件数据区 50 4B 03 04:这是头文件标记 14 03:解压文件所需 pkware 版本 00 00:全局方式位标记(判断有无加密的重要标志)

a2eb7ceaf5ab	549f7	acb3	3de2	2e7e	ed74	a.zip															
Offset	0	1	2	3	4	5	6	- 7	8	- 9	A	В	C	D	E	F					^
00000000	50	4B	03	04	14	03	00	00	08	00	68	BF	9B	48	FΕ	32	ΡK		hċ∎H	þ2	
00000010	7D	4B	Ε9	OD	00	00	B5	1B	00	00	09	00	00	00	73	74	}Ké	Д		st	
00000020	65	67	6F	2E	74	78	74	7D	59	C9	76	E2	48	10	BC	EΒ	ego.	txt	}YÉvâH	14ë	
00000030	57	E6	22	24	33	CF	1C	38	8C	68	83	C4	18	7A	00	AЗ	Wæ"≎	\$3Ï (	3∎h∎Ä z	£	
00000040	ED	Α6	C5	OF	01	12	30	OD	08	C4	D7	4F	44	56	09	68	í¦Å	0	Ä×ODV	h	

压缩源文件目录区:

50 4B 01 02: 目录中文件文件头标记,,, 3F 03: 压缩使用的 pkware 版本

14 03: 解压文件所需 pkware 版本

00 00: 全局方式位标记(有无加密的重要标志,这个更改这里进行伪加密,改为09 00打开就会提示有密码了) 然后就是识别真假加密

1.无加密

压缩源文件数据区的全局加密应当为00 00

且压缩源文件目录区的全局方式位标记应当为0000

2.假加密

压缩源文件数据区的全局加密应当为00 00

且压缩源文件目录区的全局方式位标记应当为0900

3.真加密

压缩源文件数据区的全局加密应当为0900

且压缩源文件目录区的全局方式位标记应当为0900

然后这题全局为00 00 但是在结尾发现是09 00,所以为假加密,把09 00 改成00 00就能解压打开文件了。

00000E10	50	4B	01	02	ЗF	03	14	03	09	00	08	00
00000E20	FΕ	32	7D	4B	Ε9	OD	00	00	B5	1B	00	00
00000E30	00	00	00	00	00	00	20	80	ED	81	00	00
00000E40	65	67	6F	2E	74	78	74	0A	00	20	00	00

00000E10	50	4B	01	02	ЗF	03	14	03	00	00	08	00	68	BF	9B	48
00000E20	FΕ	32	7D	4B	Ε9	OD	00	00	B5	1B	00	00	09	00	24	00
00000E30	00	00	00	00	00	00	20	80	ED	81	00	00	00	00	73	74
00000840	25	<u>~ ¬</u>	6 P.	<u> </u>	A	20	т A	0.2	00	20	00	~~	00	~~	~~	. e e 1

```
def get base64 diff value(s1, s2):
    base64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
   res = 0
        if s1[i] != s2[i]:
            return abs(base64chars.index(s1[i]) - base64chars.index(s2[i]))
    return res
def solve_stego():
        file_lines = f.readlines()
        bin str = ''
        for line in file_lines:
            steg_line = line.replace('\n', '')
            norm_line = line.replace('\n', '').decode('base64').encode('base64').replace('\n', '')
            diff = get_base64_diff_value(steg_line, norm_line)
            print diff
            pads_num = steg_line.count('=')
            if diff:
                bin_str += bin(diff)[2:].zfill(pads_num * 2)
                bin str += '0' * pads num * 2
            print goflag(bin_str)
def goflag(bin_str):
    for i in xrange(0, len(bin_str), 8):
        res_str += chr(int(bin_str[i:i + 8], 2))
    return res_str
if _____name___ == '____main__':
   solve stego()
```

我个人代码比较麻烦,所以去网上找了一份看上去容易点的运行后就得到FLAG啦

flag{Base\_sixty\_four\_point\_five}

### 11、ext3

题目描述:今天是菜狗的生日,他收到了一个linux系统光盘

既然说是linux 那就拖到linxu看看

查看flag发现估计就是这个了,记住这个目录,然后查看发现是让你恢复文件,那就

root@kali:~/Desktop# file f1fc23f5c743425d9e0073887c846d23
f1fc23f5c743425d9e0073887c846d23: Linux rev 1.0 ext3 filesystem data, UUID=cf6d7bff-c377-403f-84ae-956c
e3c99aaa



#### 然后进入到刚才看到的那个文件夹中发现一串base64, base64解密



#### 解码得到flag

明文:		BASE64:						
flag{sajbcibzskjjcnbhsbvcjbjszcszbkzj}	BASE64编码 > <base64解码< td=""><td>ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=</td></base64解码<>	ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=						
flag{sajbcibzskjjcnbhsbvcjbjszcszbkzj}								

# 12、功夫再高也怕菜刀

题目描述: 菜狗决定用菜刀和菜鸡决一死战

附件下载后我就直接丢进kali查看有没有别的东西

rootākali	:~/Desktop# binwalk a	acfff53ce3fa4e2bbe8654284dfc18e1.pcapng
DECIMAL	HEXADECIMAL	DESCRIPTION
663085	0×A1E2D	xz compressed data
664045	0×A21ED	xz compressed data
812025	0×C63F9	xz compressed data
814001	0×C6BB1	xz compressed data
1238637	0×12E66D	xz compressed data
1240937	0×12EF69	xz compressed data
1391563	0×153BCB	xz compressed data
1393067	0×1541AB	xz compressed data
1406647	0×1576B7	xz compressed data
1412887	0×158F17	xz compressed data
1422689	0×15B561	Zip archive data, encrypted at least v2.0 to
extract,	compressed size: 52,	uncompressed

#### 貌似还蛮多的,然后分解后



发现有个zip解压发现要密码

用wireshark去看看这个包

	🖊 a	cfff53ce3fa	4e2bbe86542	284dfc18e1.p	capng											
ſ	文件(	(E) 编辑(E	)视图(V)	跳转( <u>G</u> ) 捕獲	英( <u>C</u> ) 分析( <u>A</u> ) 纷	\;) 电话(Y) 矛	5线(W) 工具(T)	帮助( <u>H</u> )								
1:	4		- 🖪 🔀	ج 🔉 🔁	⇒ 🕾 🗿 🛓 🗖		壅							4	k	
3	一应	用显示过滤	器 … 💴	5 1			2		3							表达式…
		分组字节	流 〜 寛	窄	~ 🗆 区分大	小写 字符串	∨ flag. txt								查找	取消
ľ	No.	Tin	ie	Source		Destination	Protoco	l Length	Info							
		1141 49	.896906030	192.168	.25.128	219.216.128.2	25 TCP	54	58432 → 80 [ACH	] Seq=145	Ack=175261 Win=65	5535 Len=0				
		1142 49	.897175062	219.216	.128.25	192.168.25.12	28 TCP	1434	80 → 58432 [PSH	I, ACK] Sec	q=175261 Ack=145 V	√in=64240 Len=	1380 [TCP seg	gment of a reas	ssembled P	DU]
		1143 49	.897215668	192.168	.25.128	219.216.128.2	25 TCP	54	58432 → 80 [ACH	[] Seq=145	Ack=176641 Win=65	535 Len=0				
94	+	1144 50	.098716397	192.168	.43.83	192.168.25.12	28 HTTP	300	HTTP/1.1 200 OF	(text/h	tml)					
1		1145 50	.098792302	192.168	.25.128	192.168.43.83	3 TCP	54	47856 → 80 [ACH	[] Seq=2052	239 Ack=247 Win=30	0016 Len=0				
L		1146 50	.134447510	192.168	.25.128	192.168.43.83	3 TCP	290	47856 → 80 [PSH	I, ACK] See	q=205239 Ack=247 V	Vin=30016 Len=	236 [TCP segm	ent of a reass	sembled PD	U]
ł.		1147 50	.138633287	192.168	.43.83	192.168.25.12	28 TCP	60	80 → 47856 [ACH	[] Seq=247	Ack=205475 Win=64	1240 Len=0				
	->	1148 50	.138903657	192.168	.25.128	192.168.43.83	B HTTP	777	POST /upload/1.	php HTTP/:	1.1 (application,	/x-www-form-ur	lencoded)			
		1149 50	.140816842	192.168	.43.83	192.168.25.12	28 TCP	60	80 → 47856 [ACH	[] Seq=247	Ack=206198 Win=64	1240 Len=0				
1	<u>+</u>	1150 50	.14/5/6455	192.168	.43.83	192.168.25.12	28 HTTP	515	HTTP/1.1 200 OF	. (text/h	tml)					
Г	> Tr	ransmiss	ion Contro	ol Protoco	1, Src Port:	80, Dst Port:	47856, Seq: 2	47, Ack:	206198, Len: 4	51						
I.	> Hy	ypertext	Transfer	Protocol												
I.	∽ Li	ine-base	d text dat	a: text/h	tml (7 lines)											
I.		-> ./\†	t2017-12-0	8 11:42:11	1\t0\t0777\n											
I.		/\t20	317-12-08	11:39:10\1	t4096\t0777\n											
I.		1.php\	t201/-12-0	8 11:33:10	5\t33\t0666\n											
I.		6666.jp	og\t2017-1.	2-08 11:44	2:11\t102226\	t0666\n () -										
Ŀ		Tiag. C	KL\L2017-1	2-00 11:5:	5:29\L17\L000	n/ o										
L	0146	0 30 09	30 37 37	37 0a 2e	2e 2f 09 32	30 31 37 2d	0.0777/.2	017-								
L	0150	0 31 32	2d 30 38	20 31 31	3a 33 39 3a	31 30 09 34	12-08 11 :39:	10.4								
ų.	0150	0 30 39	27 24 21	3/ 3/ 3/	0a 31 2e 70	08 70 09 32	096.0/// ·1.p	np•2								
L	0180	0 30 31 0 31 36	09 33 33	09 30 36	36 36 0a 36	36 36 36 2e	16.33.06 66.6	666								
L	019	0 6a 70	67 09 32	30 31 37	2d 31 32 2d	30 38 20 31	ipg·2017 -12-	08 1								
L	01a(	0 31 3a	34 32 3a	31 31 09	31 30 32 32	32 36 09 30	1:42:11 1022	26.0	-							
L	01b(	0 36 36	36 0a 66	6c 61 67	2e 74 78 74	09 32 30 31	666.flag .txt	·201								
L	01c6	0 37 2d	31 32 2d	30 38 20	31 31 3a 33	35 3a 32 39	7-12-08 11:3	5:29 -								
	01d6	0 09 31	37 09 30	36 36 36	0a 68 65 6c	6c 6f 2e 7a	•17•0666 •hel	lo.z								
T	01e6	0 69 70	09 32 30	31 3/ 2d	31 32 2d 30	38 20 30 39	1p·201/- 12-0	8 09								
T	0200	0 38 33 0 7c 3c	24	20 09 32	52 34 09 30	50 36 36 Øa	:52:36-2 24-0	000.								
	0200	, , <u>, , , , , , , , , , , , , , , , , </u>	20				1.									
ľ	0 '	🎽 Text i	tem (text), 3	4 字节								分组: 2	139 ・ 已显示 213	395(100.0%)dm.nei/	weixin 48	配置: Defa
L	-	**							100000000000000000000000000000000000000			1 75-1				

这就是我所发现的,一个个找呗

🚄 ac	fff53ce3fa4e2bbe865428	84dfc18e1.pcapng							
文件(E	) 编辑(E) 视图(V) 🖁	特(G) 捕获(C) 分析(A)	统计( <u>S</u> )	电话(Y)	无线( <u>W</u> )	工具( <u>T</u> )	帮助( <u>H</u> )		
	1 🖉 💿 📙 🔚 🔀 🕻	👌 ९ 🗢 🔿 🗟 🕢 👲		⊕ ⊖	Q. 🎹				
,应用									
	→ 分组字节流 ~	Ê V 🗆 🖂	<del>}</del> 大小写	字符段	₿ ~	flag. txt			
No.	Time	Source	Dest	ination		Protoco	l Length	Info	
	1141 49.896906030	192.168.25.128	219	.216.12	8.25	TCP	54	58432 → 80 [ACK]	Seq=145 Ack=175261 W
	1142 49.897175062	219.216.128.25	192	.168.25	.128	TCP	1434	80 → 58432 [PSH,	ACK] Seq=175261 Ack=
	1143 49.897215668	192.168.25.128	219	.216.12	8.25	TCP	54	58432 → 80 [ACK]	Seq=145 Ack=176641 W
+ :	1144 50.098716397	192.168.43.83	192	.168.25	.128	HTTP	300	HTTP/1.1 200 OK	(text/html)
	1145 50.098792302	192.168.25.128	192	.168.43	.83	TCP	54	47856 → 80 [ACK]	Seq=205239 Ack=247 W
	1146 50.134447510	192.168.25.128	192	.168.43	.83	TCP	290	47856 → 80 [PSH,	ACK] Seq=205239 Ack=
	1147 50.138633287	192.168.43.83	192	.168.25	.128	TCP	60	80 → 47856 [ACK]	Seq=247 Ack=205475 W
<b>•</b>	1148 50.138903657	192.168.25.128	192	.168.43	.83	HTTP	777	POST /upload/1.p	hp HTTP/1.1 (applica
	1149 50.140816842	192.168.43.83	192	.168.25	.128	TCP	60	80 → 47856 [ACK]	Seq=247 Ack=206198 W
+ :	1150 50.147576455		192	.168.25	.128	HTTP	515	HTTP/1.1 200 OK	(text/html)
> Tr	ansmission Contr		0.	Dst Por	t: 47856	, Seg: 2	47, Ack:	206198, Len: 46	1
> Hy	pertext Transfer	必略/蚁洞恐略 万祖(!)				· ·			
Y Li	ne-based text da	设置/取消设置 时间参考							
	-> ./\t2017-12-0	时间平移							
	/\t2017-12-08	分组注释							
	1.php\t2017-12-€	编辑解析的名称							
	6666.jpg\t2017-1		2666	5\n					
	flag.txt\t2017-1	作为过滤器应用	▶ \n						
0000	00 50 56 21 b8	准备过滤器	10.0	0 15 00	- DV/1 -	D V	E.		
0000	00 50 50 21 08 01 f5 52 fd 00	对话过滤器	<ul> <li>Ib 5</li> </ul>	3 c0 a8	···R··	···· •··-	+5		
0020	19 80 00 50 ba	对话着色	<ul> <li>3 6</li> </ul>	0 50 18	p.	·w· 5·o	1. P.		
0030	fa f0 ff 43 00	SCTP	▶ !e 3	1 20 32	· · · C ·	·HT TP/1	1.1 2		
0040	30 30 20 4f 4b	追踪流	• 0 4	6 72 69	00 OK	···D ate:	Fri		
0050	2c 20 30 38 20		-72	0 31 31	, 08	Dec 201	17 11		
0060	3a 34 32 3a 31	复制	3 6	5 72 76	:42:1	1 G MT	Serv		
0070	05 /2 38 20 41	协议首选项	• a 3	4 Ze 32	er:A	pac he/2	4.4.Z		
0000	36 2e 32 35 0d	解码为(A)	12 6	5 64 2d	6 25.	·X- Powe	red-		
0050	50 20 52 55 Ou	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	2 0	5 0 <del>4</del> 20	0.25	A TOWE			

00a0	42	79	3a	20	50		在新	新窗口	显示	分组	(W)		12	35	0d	0a	By: PHP/ 5.6.25
00b0	43	6f	6e	74	65 <sup>1</sup>	ъe	74	zu	40	00	oe	07	-74	68	3a	20	Content- Length:
00c0	32	32	31	0d	0a	4b	65	65	70	2d	41	6c	69	76	65	3a	221 · · Kee p-Alive:
00d0	20	74	69	6d	65	6f	75	74	3d	35	2c	20	6d	61	78	3d	timeout =5, max=

在这里右键选择追踪TCP流,查看flag的时候应该有看出这个的不一样有个jpg

DOST /upload/1 pk	B HTTD/1 1					
lson_Agont: lova	1 8 0 151					
Host: 192 168 /3	83					
Accent: text/html	image/gif	image/i	neg *• (	1= 2 */*· (	n= 2	
Connection: keen-	alive	, image/j	P-8) ) ·	,, / , ·	1 • 4	
Content-type: apr	lication/x-	www-form-	urlencode	d		
Content-Length: 2	04999					
22-00V21						
aa-weva⊥. (base6/ decode(\$	POSTIaction	1))·&acti	on=061ua\	/977X00TmRn/	-3ReVX1+7X	lvb31zT
iwiMCInO08z7XRfd0	1+7V9saW1nd		VAX21h721	HX3E1b3R1c1	19vdW50aW1	1KDAp02
/iaG8oTi0%28fCTnC	)zek7i1iVXN1	NiRf7GVib	2R1KCRFUE	GTVEsiaiFi)	XSk71GM91E	90T1NUW
/J6MiJdOvRiPXN0cl	9v7XBcYWN1K	CleciIsTi	TelGMnOve	PXN0c19v7		chilsIi
[c]GMpOvRidWV9Ti]	77m9vKCRpPT	A716k8c3R	vbGVuKCR+	ikTekaSe9Mil	kkVnVml i11	cmvk7WN
/7GUoTillil nN1YnN0	loigkYvwkaSw	vKSk77WNo	hvh07ndva	XR1KG7ycGV		iks1G11
7ik%2FTiFiOiTwTik	702ViaG8oIn	W8LSTn02R	n7SonOw%		acd2EtcDY0	XHd3d1v
LCGXVYWRcNiY2Ni5c	1 < G < 3D	EDSEEF000	104446494	6000101010	2780078000	0EEDB00
1300010101010101010	1010101010101	010101010	10101010101	0101010101010	210101010101	0101010
10	0101010101010	1010101010	0101010101	1010101010101	101FEDB004	301010101
310101010101010101010	10101010101010	01010101010	10101010101	0101010101010	210101010101	01010101
10101010101010101010101	0101010101010	1010101010	0101010101	101010101010101	2110801390	1F20301
2200021101031101	FC4001F0000	010501010	10101010	000000000000000000000000000000000000000	000010203	0405060
708090A0BFFC400B5	10000201030	302040305	050404000	0017001020	3000411051	2213141
0613516107227114	28191A10823	42B1C1155	2D1F0243	627282090A	161718191A	2526272
8292A343536373839	3A434445464	748494A53	5455 <mark>5657</mark> 5	8595A63646	5666768696	A737475
767778797A8384858	68788898A92	939495969	798999AA2	A3A4A5A6A7	A8A9AAB2B3	B4B5B6B
7B8B9BAC2C3C4C5C6	C7C8C9CAD2D	3D4D5D6D7	D8D9DAE1E	2E3E4E5E6E7	7E8E9EAF1F	2F3F4F5
F6F7F8F9FAFFC4001	F0100030101	010101010	101010000	00000000001	0203040506	0708090
A0BFFC400B5110002	201020404030	407050404	000102770	00102031104	4052131061	2415107
51711322328108144	291A1B1C109	233352F01	56272D104	162434E125	F11718191A	2627282
92A35363738393A43	44454647484	94A535455	565758595	A6364656667	768696A737	4757677
78797A82838485868	788898A9293	949596979	8999AA2A3	A4A5A6A7A8	49AAB2B3B4	B5B6B7B
BB9BAC2C3C4C5C6C7	C8C9CAD2D3D	4D5D6D7D8	D9DAE2E3E	4E5E6E7E8E9	9EAF2F3F4F	5F6F7F8
F9FAFFDA000C03010	00211031100	3F00FC188	23DB907E6	2481211D649	93F86143D9	14E012B
CF5E30056C4310192	E7D0CC40EFF	C30478E3B	0DFF00FD8	F352DA3DBB	0AF0769F2C	1FF0096
102060000220660001	10071002200	651070040	ED0201071	000000000000000000000000000000000000000	0010005006	2017055
始884.53 客户端 分组,2	服务器 分组, 3 tur	n(s).点击选择。				
暨个对话(206 kB)			$\sim$	显示和保存数排	屠为 ASCII	~ 流 7
时北:						查找下——个

4	_ Wireshark ·追踪 TCP 流 (tcp.stream eq 7) · acfff53ce3fa4e2bbe8654284dfc18e1 — □	×	
	8DE841C633D90567C843799E63908306E1D78C95EE0055650E4EDD0181D31CE09CDE1E76C	~	
	3EEBACDFF00A10ACDFF0097783FEBFDFF00F65AEDA6B48F5BD9EBE6A0FE7F1EADEFEF759B		
	6B96A371BABBDD2EDF69EAB7B7C1A745EE696824EACEBBE40F2E12487E72E3836303C525B		ų,
	F911631B65B886796190039314AF1B0C33815E56EC7F74DE5E71938B4B53CE31FC53CA08E		ľ
	4E09DDD8BE04D27FAA97FEC27FD64AA97BFF002FDFF5F917FECD5DD4A0AEDD97335772B6A		
	F953B27FF0080E9D9C9B56B47979E527CA936DA8D9455F45774AF65AA4AF2D5755149B779		
	B9549189DA41F2C843E483D2D2D8925E67FF00A6D367823E63D41F996B3252C4A6C014E18		
	DB8603F7518CF9B792F6F30F3B4B1C82011C0506FDE74BEFAC1FCAB3EE7ADFF00FD7083F9		
	C75D0FDD83B74D7D6DCDE565FC3EDBB5FC91B73D2F7A4BCF937D6DCFEC97CECAADB5DD295		
	FE393322E24C6C1183925BECCAC4F5E7CDBC9BD48DADB41C018E32139C694801447F38DCD		
	E486FF0096F3747B997B08D3076EEF61D9C56A5DFDFB8FFB0745FF00B4EB1E6EABFF0060E		
	7FE42BCCAD75A76F2B6B74AE97CB4E8BDD4EE9352F630E95A3E76FC545FFEDDD2DBCDAB39		
	2E4CD99B0A31FBD05FE4CF2D79723EF48D93930C648EBC608CE0935893BE7713990799838		
	39FB4DD374553FF003CA33D80E79EEC00D49BEF41FF005E32FF0027ACA3D6D3FEB85CFF00		
	296BC6ACF5F9A5F7FB3FFE4FE6959FC53E6F770E96AFB5FCB6E67D366DC3A689B6D2D236C		
	8BA9000DB89705BF798CE679C1F96043FF3CE3EA5BA7191FC158B70E4F98643BB0409D971		
	F3B7FCB2B58F03855C7CDB41039FEEA83A72FDFB3FF7DFFF0066AC83D2D3FEBEA4FF00D0C		

T.	578F8896CBBC53FBD53767DFF0089D775CDFCEEDEE192BFA36BE69DAFE5F0E96DBDDB690
L	465CEF8326FE08C7DA197A20E365B47D831C00DE9DF201CE3DCB677866DADB71291FF2C61
L	E8B02FABBF1B8638DD83CEEAD297FD5A7FD7F37F4AC8B8E92FF00D7E8FE46BC5AD276BFCF
L	EFF7B57F87CE4FAAB7BD865771E9ADBD2D251FD36DBE156693E6C9BA90E580C21D9866FF0
L	09F780F1B467A4926E00FF176E0B3118731C7CD8D876128A738B780F2646FFA6B2678C1E4
	9E30480356EFEEDCFF00D7D27E37ACAD47A5FF00FBF07F235E3577A7AB7F85FF001F7775B
ξ.	377568452E680DA88278C9C75E5E651D86D39EEE56E8526E0EE1CB30D9E28018C00E3E751
1	F57B8931EF002D1B191E99E32319C999F681B7A90C6156C60609DD73276E31F2E7B8183F2
L	E37EE7EEDCEED7383E9C758E77D65EE00AE78EE00E408EBC6C4DD44DE4E5E4EDBD97BBA2E
L	9A7F2A3F830FB45F89F7DD41FBD5FC7AF7F7BAC9B59F658327293B9CF2F1BFF7FB5FF02FB
L	F8D15763FF571FF00B8BFFA08A2B86DFF1FFC05797F93FBFFFF9F65DA5FF81BFF002F5FF9
L	6BEED9HTTP/1.1 200 OK
	Date: Eri, 08 Dec 2017 11:42:07 GMT
L	Server: Apache/2,4,23 (Win64) PHP/5,6,25
L	X-Powered-By: PHP/5.6.25
L	Content-Length: 7
L	Keep-Alive: timeout=5, max=100
L	Connection: Keen-Alive
L	Content-Type: text/html: charset=UTE-8
L	分超 1144. 53 客户增 分组, 2 服务器 分组, 3 turn(s).点击选择。
	整个对话 (206 kB) - 显示和保存数据为 ASCII - 流 7 🗧
4	查找: 查找下一个())
	滤掉此流 打印 Save as <sup></sup> 返回 Close Help
L	

#### 科普一下头文件JPEG的头文件开头是 FFD8FF然后直接拉到最后到FFD9

全部复制出来我是先放到txt里整理然后就要使用WINHEX啦 先winhex新建一个空的,然后把整理的十六进制复制进去以hex形式用winhex打开

🚟 WinHex				– 🗆 ×
文件(F) 编辑(E) 搜索(S) 导航(N) 查看(V) 工	具(T) 专业工具(I) 选项(O) 窗口(W) 幕	等助( <u>H</u> )		18.5 SR-3 x64
案件数据	💌 🛍 🛅 👘 🕋 🐂	🎮 🛤 🚓 🎲 ¥€   → +₩ 🔶	• 🔶 😂 🍣 🚞 🔎 🌗	🖗 🖌 🕨
文件(L) 编辑(D) 未命名				
# <u>**</u> 未命名				
Offset	0 1 2 3 4 5 6 7	89ABCDEF	^	未命名
0000000	FF D8 FF E0 00 10 4A 46	49 46 00 01 01 01 00 78	ÿØÿà JFIF x	未命名
00000010	00 78 00 00 FF DB 00 43	00 01 01 01 01 01 01 01 01	x ÿUC	<b>立供士</b> 小、 110 KB
0000020	01 01 01 01 01 01 01 01 01	01 01 01 01 01 01 01 01 01		文件入小: 110 KB 112 466 字节
00000030				112,400 9-13
0000040				缺省编辑模式
00000050		U1 FF DB UU 43 U1 U1 U1	yu c	状态: 修改
0000060				撤消级别: 1
00000070				反向撤消: 正在粘贴数据
0000080				创建时间: 2020/09/08
00000030		01 01 01 01 01 01 01 17 00	0 A "	15:36:45
00000000				最后写入时间· 2020/09/08
00000000			ул	15:36:45
0000000	00 00 00 00 00 00 00 01		52Å 11	■性・ Δ
00000050	05 04 04 00 00 01 7D 01		3 1	图标: 0
00000050	31 41 06 13 51 61 07 22	71 14 32 81 91 A1 08 23	1A 0a "m 2 1i #	
00000100	42 B1 C1 15 52 D1 F0 24	33 62 72 82 09 0A 16 17	B+Á RÑáS3br	模式: 十六进制
00000110	18 19 1A 25 26 27 28 29	2A 34 35 36 37 38 39 3A	%&'()*456789:	子付男 数据解释器
00000120	43 44 45 46 47 48 49 4A	53 54 55 56 57 58 59 5A	CDEFGHIJSTUVWXYZ	每页配 8 Bit (+): 1 0
00000130	63 64 65 66 67 68 69 6A	73 74 75 76 77 78 79 7A	cdefghijstuvwxyz	16 Bit (±) 257
00000140	83 84 85 86 87 88 89 8A	92 93 94 95 96 97 98 99	minimi	□=前間 32 Bit (±) 16,843,009 1 窗口 5:ev:
00000150	9A A2 A3 A4 A5 A6 A7 A8	A9 AA B2 B3 B4 B5 B6 B7	¢£¤¥¦S"©ª²³′μ¶∙	
00000160	B8 B9 BA C2 C3 C4 C5 C6	C7 C8 C9 CA D2 D3 D4 D5	,¹ºÂÃĂÅÆÇÈÉÊÒÓÔÕ	剪贴板: 可用
00000170	D6 D7 D8 D9 DA E1 E2 E3	E4 E5 E6 E7 E8 E9 EA F1	0×0ÙÚáâãäåæçèéêñ	临时文件夹: 24.5 GB 空余
00000180	F2 F3 F4 F5 F6 F7 F8 F9	FA FF C4 00 1F 01 00 03	òóôõö÷øùúÿÄ	ers\12437\AppData\Local\Temp
00000190	01 01 01 01 01 01 01 01 01	01 00 00 00 00 00 00 01		
000001A0	02 03 04 05 06 07 08 09	OA OB FF C4 00 B5 11 00	ÿÄ μ	
000001B0	02 01 02 04 04 03 04 07	05 04 04 00 01 02 77 00	W	
000001C0	01 02 03 11 04 05 21 31	06 12 41 51 07 61 71 13	!1 AQ aq	
000001D0	22 32 81 08 14 42 91 A1	B1 C1 09 23 33 52 F0 15	"2 B1i±Á #3Rð 🗸	
页面 1 / 235	偏移量:	2C = 1 ž	缺: 0-1	8F51 大小: 18F52

然后保存修改后缀为jpg打开





#### 说这个就是密码,然后拿去zip输入打开得到flag

e					flag.txt
	文件(F)	编辑(E)	搜索(S)	选项(O)	帮助(H)
archiv	flag{3	OpWdJ-	JP6FzK	- koCMA	K-VkfWBq-75Un2z}

flag{3OpWdJ-JP6FzK-koCMAK-VkfWBq-75Un2z}