[CTF]Bugku Misc Writeup

原创

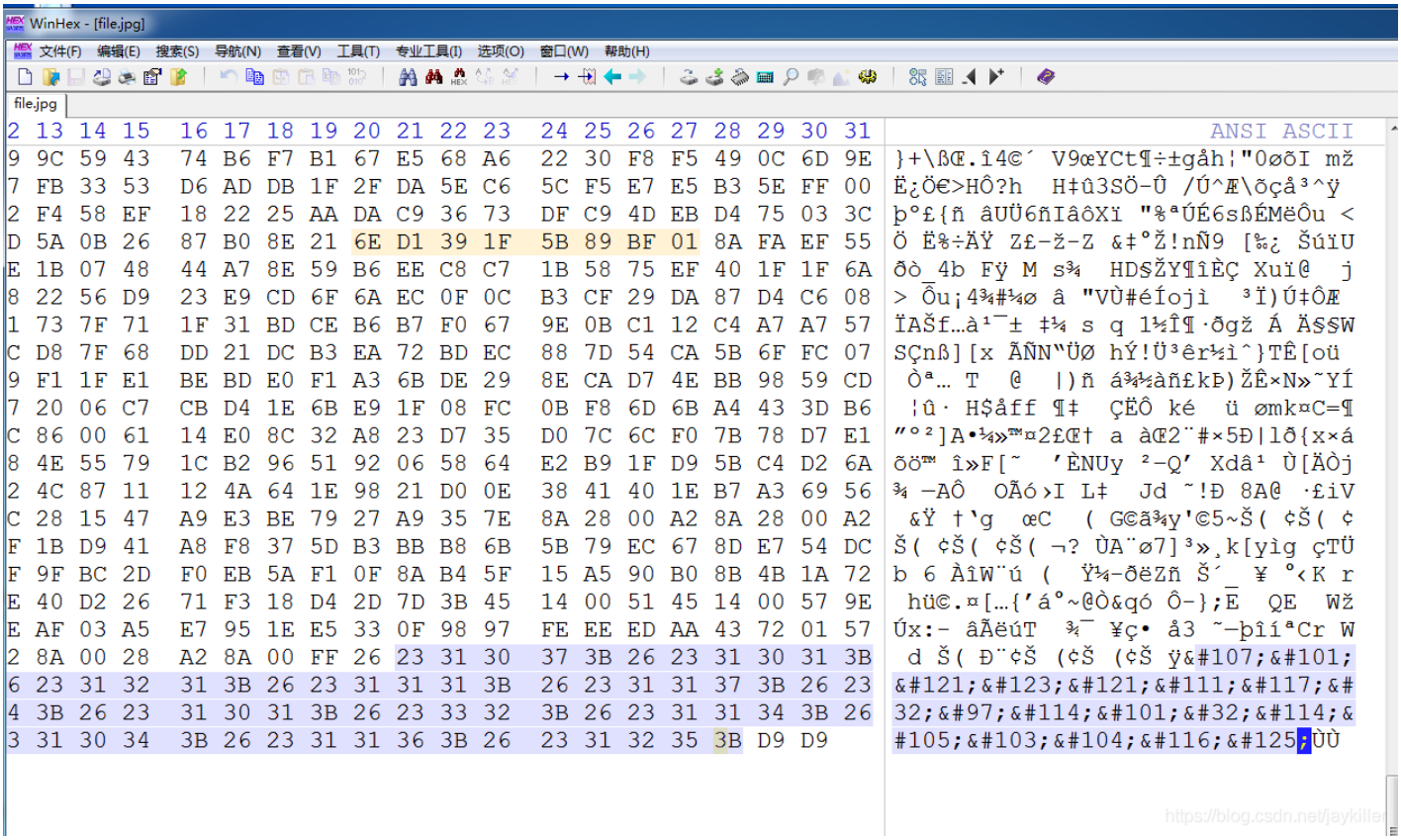
m3gaf0rce 于 2020-12-14 23:21:13 发布 137 收藏
分类专栏： CTF

题目：https://ctf.bugku.com/challenges/index.html

1.签到（略）。

2.这是一张单纯的图片。

下载图片后放入WinHex查看，拉到最后，发现有异样。

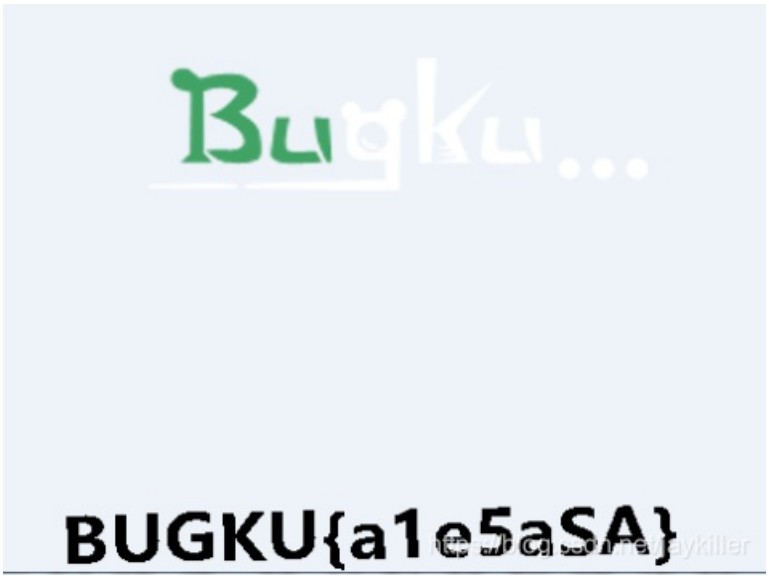


ascii码在线转换器：http://www.ab126.com/goju/1711.html

将这串数字 107 101 121 123 121 111 117 32 97 114 101 32 114 105 103 104 116 125 ascii码转字符后得到flag。（32对应的空格也要正确输入）

3. 隐写。

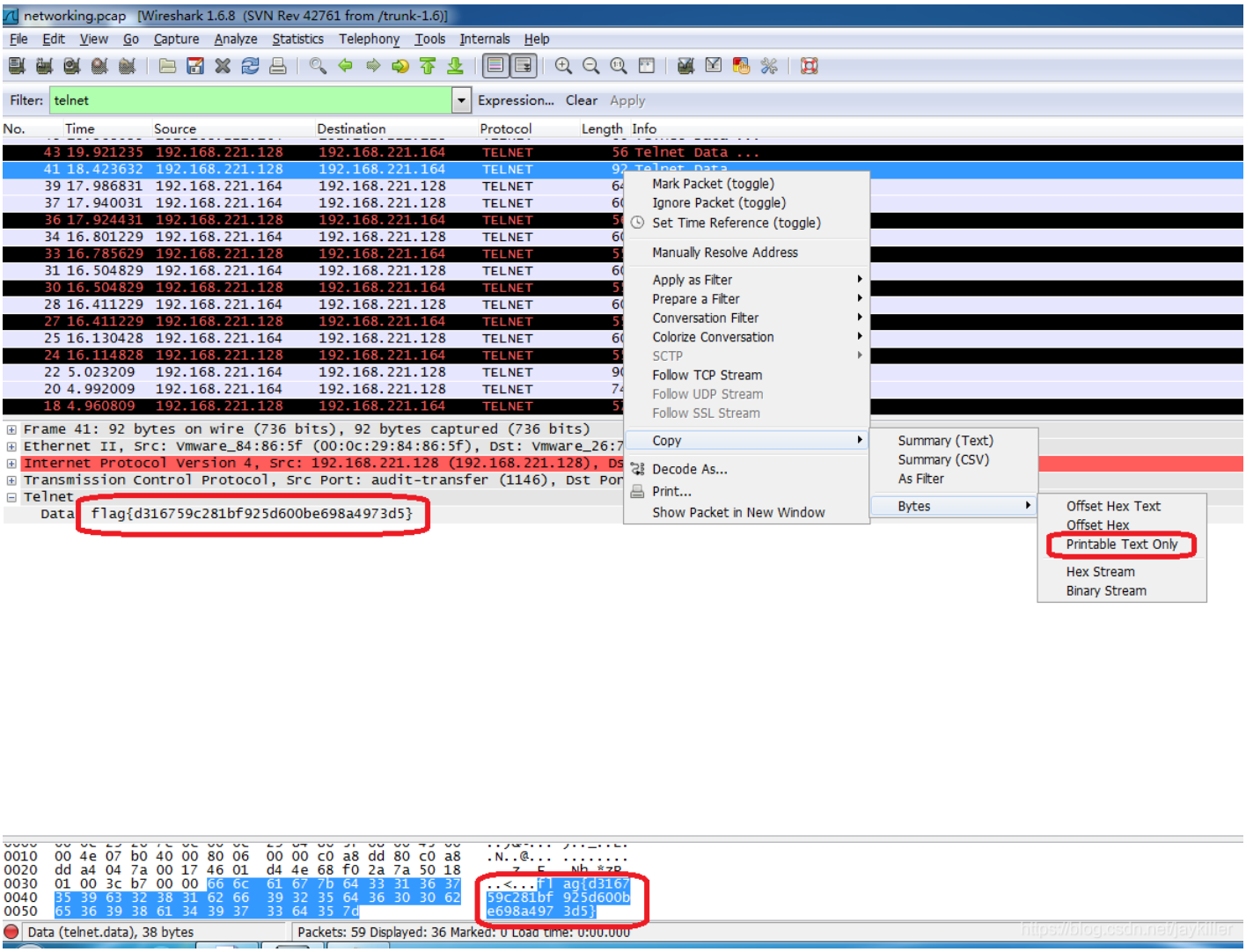
老题目，应该是高度被改了。根据CRC32求出原高度。修改原图高度后得flag。



4. telnet

pcap文件，直接放进wireshark中分析。根据题目提示，在过滤一栏中过滤条件为telnet。

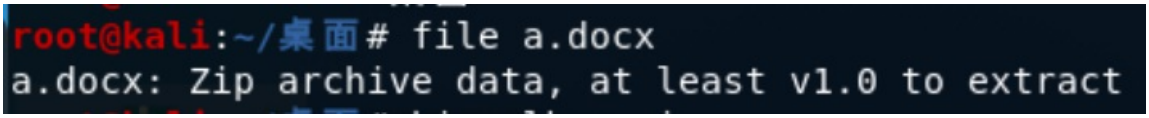
直接翻几个报文就看到了flag。



5. 眼见非实

附件解压打开，一个docx文件，file 眼见非实.docx这个文件，显示为.zip文件，扩展名改成.zip后解压。

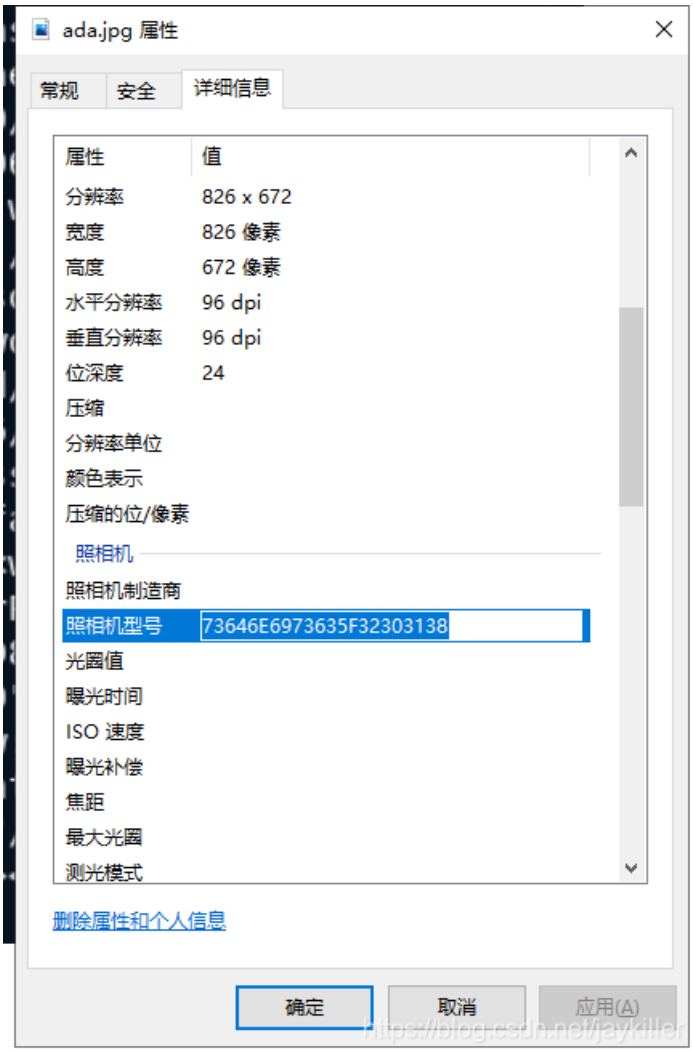
解压后全量搜索flag即可。



6. 啊哒

解压开一张图片，直接binwalk -e ada.jpg，分解出来一个压缩包，加密的，里面是flag.txt，需要知道解压密码。

archpr用不了，只能想其他办法。看图片属性，发现照相机型号后面有一串数字，先用这个数字试一试，失败。



ascii码在线转换器：http://www.ab126.com/goju/1711.html

上面的就是zip包密码，出flag。

7. 又一张图片，还单纯吗

直接Kali中用foremost分离即可，注意本题应该是出题者手误，是falg而不是flag。

falg{NSCTF_e6532a34928a3d1dadd0b049d5a3cc57}

8. 猜

一般这种题不太会在现在的ctf里面出现了，按道理应该是去识图网站识个图，但我在百度识图一下子就直接出答案了……

9. 宽带信息泄露

利用RouterPassView软件打开conf.bin文件，在里面搜索username。

```
<Uptime val=671521 />
<Username val=053700357621 />
<Password val=210265 />
```

10. 想蹭网先解开密码

flag格式：flag{你破解的WiFi密码} tips：密码为手机号，为了不为难你，大佬特地让我悄悄地把前七位告诉你1391040** Goodluck!! 作者@NewBee

aircrack-ng wifi.cap -w pass.txt

pass.txt是自己写的从13910400000-13910409999的密码字典。

```
[00:00:00] 9272/9999 keys tested (9329.54 k/s)

Time left: 0 seconds                                      92.73%

                    KEY FOUND! [ 13910407686 ]

Master Key     : 28 B6 77 93 8F 1B 3C 04 DF 17 C7 C8 02 B4 C3 03
                 28 09 4B 0E C0 16 B4 A0 98 B8 A6 87 C5 96 22 F1

Transient Key  : 42 5A E3 6D 00 27 34 DA 18 63 FF 1F D4 F8 01 FB
                 52 2C 3A C3 58 4F F5 3A C3 1A 2B 29 E0 4B FE EA
                 0D D2 04 9D 6C 95 2F C2 21 F5 E5 2A 62 B0 5D F3
                 77 11 6D 1A 98 91 7A DA 17 46 5B 01 0E 7F B6 DB

EAPOL HMAC     : 12 84 22 03 51 DE 51 9C A6 29 A1 6C D0 86 49 A2
```


11. 闪的好快

GIF分离：https://tu.sioe.cn/gj/fenjie/

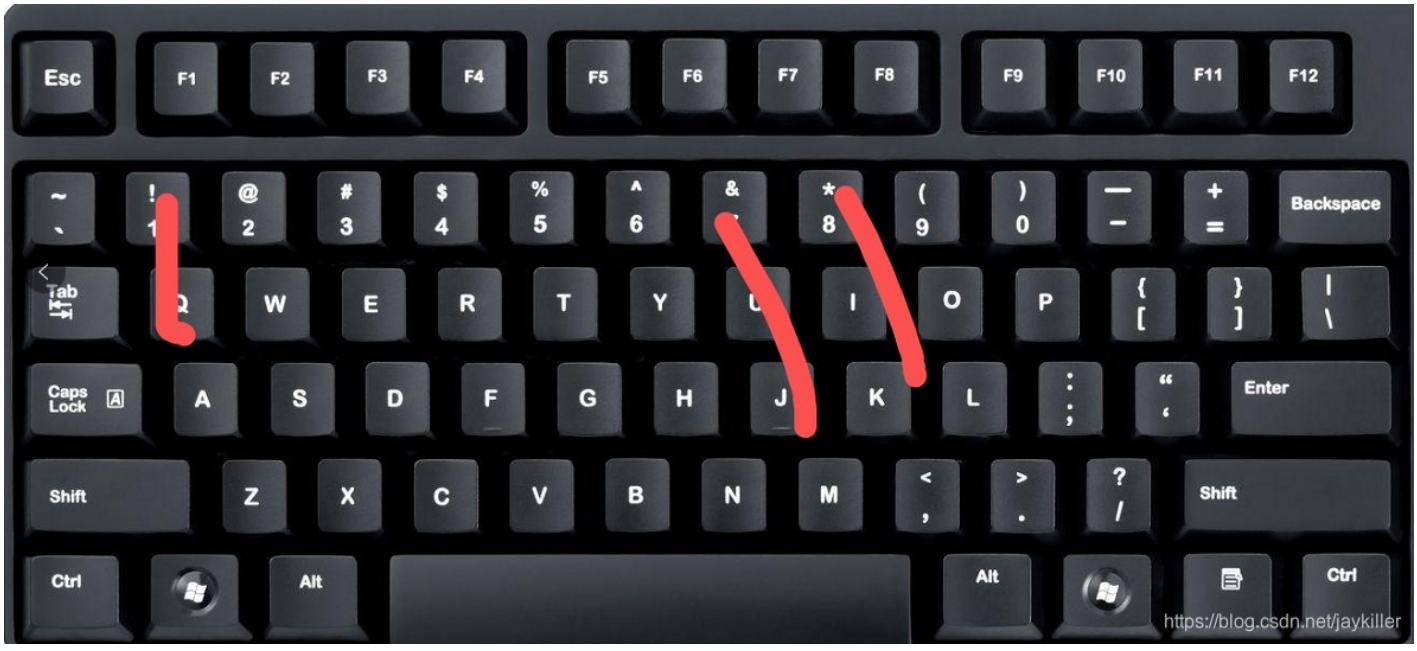
12. 隐写2

binwalk分离，分离后有个加密的rar包，有个提示图片。

告诉你们一个秘密，密码是3个数哦。

查理曼：
查理曼，法兰克王国国王，征服了西欧与中欧大部分土地，具有了至高无上的权威，下令全国人民信仰基督教，查理重振了西罗马帝国。
雅典娜：
女神帕拉斯·雅典娜，是希腊神话中的女战神也是智慧女神，雅典是以她命名的。
兰斯洛特，
英格兰传说中的人物，是亚瑟王圆桌骑士团中的一员。看上去就是一个清秀年轻的帅小伙儿，由于传说中他是一名出色的箭手，因此梅花J手持箭支。兰斯洛特与王后的恋爱导致了他与亚瑟王之间的战争。
Hint:
其实斗地主挺好玩的。

想到对应的是K Q J，键盘对应数字，8 1 7。



排列组合6种可能，最后尝试出871是这个rar的密码。解压后再次获得一个图片。

WinHex打开，拉到最后，出现flag。

56	39	45	0B	31	E1	82	B4	41	15	01	39	96	A9	4E	EE	%7ç	„Cj • 1R V9E 1á,´A 9–©Nî
3D	83	5B	B7	59	77	71	EC	96	D0	6D	6D	34	53	DC	D1	·•¢Ñ ó^(ë¿ ¯h¡S =ƒ[·Ywqì–Ðmm4SÜÑ
10	D6	0E	46	0D	C1	4A	0E	11	A1	54	D8	0D	EE	5D	FB	‘K˜£C")TMb "¢ Ö F ÁJ ¡TØ î]û
DE	38	C7	6C	F1	F7	A6	B5	2A	C8	A1	64	5A	6E	C3	20	L¦i´ä´ Þ ÛÏz^j–„Þ8Çlñ÷¦µ*È¡dZnÃ
20	F6	8E	B9	7F	AC	34	1B	BF	4D	EC	0A	02	7A	2A	F9	ö `^ f±’€ÉwA_# öŽ¹ ¬4 ¿Mì z*ù
44	0A	53	AC	45	FD	B7	F5	81	8C	12	7D	9E	B2	6A	0B	òa*Jch p Þ *v D S¬Eý·õ Œ }ž²j
17	83	C9	F3	AE	30	93	B4	EE	DA	19	9B	11	81	E9	F8	ÍäÀd„³Ãíøú)¾_çfí ƒÉó®0"´îÚ › éø
DE	9C	B0	18	6B	EC	9C	73	5C	FE	90	B8	C5	44	74	D9	¿ïxA [¤çãŸ9* ›Þœ° kìœs\þ ¸ÅDtÙ
E7	34	32	50	02	78	C2	17	D3	5F	8F	FC	C4	96	0D	BB	àÿ >™ -CÏY z Âq;ç42P xÂ Ó_ üÄ– »
07	83	29	DE	FF	00	01	F3	9B	2E	5A	88	01	83	F3	C7	Cƒ w ×iv!¹_|^Àà ƒ)Þÿ ó›.Z^ ƒóÇ
1C	F7	B1	FC	E1	CE	D8	4A	32	BB	C4	84	00	96	9F	BC	ëé¶Ñ ¥Â£, ¯œ#¥V ÷±üáÎØJ2»Ä„ –Ÿ¼
FE	36	06	F5	EF	70	05	C5	A7	93	81	BA	E7	57	D4	E7	Ý·a˜yfØÚ ›;9Å,Q þ6 õïp Å§" °çWÔç
9E	C2	AF	59	1B	9E	6F	1A	DD	6B	B5	E7	58	F8	34	1E	& œ% q ûá ÀoD• WžÂ¯Y žo ÝkµçXø4
F1	F2	89	C2	0B	C0	9C	0A	C7	BE	BF	78	68	50	25	31	ëÈX ;{ `#, à Mœñò‰Â Àœ Ç¾¿xhP%1
95	4D	9A	5C	01	54	DA	3A	F1	8E	2D	1E	6A	56	E1	B1	ƒÇC¿85 Ó˜-Mïïƒ•Mš\ TÚ:ñŽ- jVá±
D6	32	7B	25	E4	F1	53	17	8C	80	50	37	D7	1D	BF	9C	vƒ¾ …Ýõ/qÙøíøÖ2{%äñS Œ€P7× ¿œ
CB	15	9F	6F	6C	A0	86	25	6E	12	70	EB	BC	69	6B	41	.°)¬¦±-8 £bÏŒimË Ÿol †%n që¼ikA
54	42	31	49	45	46	79	5A	53	42	68	49	47	68	41	59	#ägÔÿÙ f1@g{eTB1IEFyZSBhIGhAY
1A																2tlciE=}

兴高采烈地去提交，结果发现不对，卧槽了。原来是flag中的内容还需要做一次base64解码。

```
root@kali:~# echo eTB1IEFyZSBhIGhAY2tlciE=|base64 -d
y0u Are a h@cker!root@kali:~#
```