# bugku CTF misc 解题报告一(1-5)

 「京创
 「于 2021-02-09 17:18:50 发布
 ①
 152 
 论 收藏
 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/qq\_51090016/article/details/113760593
 版权

### bugku CTF misc解题报告

1.这是一张单纯的图片
 2.隐写
 3 talent
 4.眼见非实
 5.啊哒
 总结:

1.这是一张单纯的图片



题目都这样说了,这图片肯定不单纯,打开看看:

怎样做更简单?我想了想,用winhex有点麻烦,直接改后缀名试试,改成txt或者html下载打开:

# TUVWXYZcdefghijstuvwxyzf,,...⁺ŧˆ‰Š′ "" •—~™š¢£¤¥¦§"©ª₂₃

□□□□□□□□□□□□□□□□□□□□□1□□AQ□aq□"2□□□B 'i±Á #3Rð□brÑ □\$4á%ñ□□□□&'()\*56789:CDEFGHIJSTUVWXYZcdefghijs üOм.×vmp&ÕádŒÛ″

F9è:×®hZ®<sup>·</sup>¤ZjZ|žeµÌbD=□Ïf□<sup>°</sup>r□ìA□« 'ñÿ, 4ëï□ê<sup>¬</sup>§i□ g...¾Õk□j, ù9%□c□`ê' □•l□à°>□û=xºÏÃZêÃ}''Ý□□þ7†□CbÝ'□" 3 ]ûCx□F¿¼Ž×ÊW7me6ÈÜ "û¶□w□Æ9©ÉçŽ}7DÖtýrÅot<ĵĩíÞ†î 'ØfÈ<Ž□□5ä □¾□é' x"çSÑm□ÞóL□¥□ b%°€gÍ□Çï¾ Úk7□7;:□îb□FÛsÝ¥" d÷<sup>°</sup>□Ô□ôÍ|Oñ3ÃÃÂ~3ñ†Žb i3®µ§E€□VÝæ(È®Ï9IõŽ?j÷o‰ □>× fЬ<sup>°</sup>ɰKß5äcòÉ□¤\*©à]

<sup>3</sup>□Úì<□□ÎpÌÇĩ□½ø□□□h·¾%ø©£k□YÜG¥éòX\ݵÝ©€OçÜÁlG″ä°≪\*Hv·!□±?BxWÃ□7...t÷±ðîŸ ...£, '¢<8g□©»žåQr{ ' ''' #eRçÙr}»×±ø¯À^□ñAi5M=~ÔÛOÚ`&)N9]Ä}ð□ 6@ô¯□ñŸiÏg©Eæh¾ »ûH□•Ô' 9□' Xÿ¬DV^X' Hbh□Õü□ñ□Cñ¥®û□-IR9‰C)ëŒc•\*JĐ□Ò´SQ•Ô2□Ê@ ŽsN □Š( □Š( □¦□&ŠHåEx□J²0È`x Žâ¼ëâ?ŧtï□ø□\_Ôü+¡éVZ¼V<sup>-</sup>2æ□T‰ÑO□Á″ □□]Ç9ê□ Iŧò□‡\_□|C¯ÙéÚ□^eM\*Öï24@fhâÇËÁèÌOô□'œ□ôwf>□øsÂ□□F³ 'gP3,Ó¼...>□/, v«□ '•□, GN+ÏX+ÏšGØTâw□3¥lê×Üp-ð& Dñes¬¢£†Eš□•□(ê□O``5fãó¬□□ë□Ã0Å>®-ÛÈŠGd□{€ÊC□+□¤□†Ç5;ÊtTW, |□øÝ/<µ&ð÷ŠâKMc¥

Úclå>È—ƒå□òHv¯□sŽ □¶Eoª|□â3ÅÚ2ê□L□€Þ\ÐJ6Ëo ꎽUŧëÔd□Ïø‹à{□□é 'Ç4' Yj–□æØj0q-¬ž ŽJ' □W#8□, □□Mg«j□ □žx¯″ > øRÿâ□޵□W\_»ae¢7Ê□n□æGw`€, ¤□29'?1L⁺□Š÷ïÚ□[þÂøEâ)êËq³@O-æ□Œ□,RÍÇ`Mr?²6žÚoƒ□x\_Rø...ã□øY^2HĆ Œ□4□0□C€NO''9Årö¿□|sà+~ô¯□hRk)·0É:=□Û□sóeJ¾ÞFUp ¼{ú\_í□

-KI,¬□Pz' x□¼§â □□Ÿ¤Ãs ¥Þ□ åš+{}Ë□Ú″ œ□WF"E,,c°ÎÙTaþs°ø...ãÿ‰ž,+iœl¼□;±...

ż□□OÞ:Žë□g%\$ÏЕOJ°·Òôû{+□ÄvÐ̈D\ "Ç©'' sÔžläṌÊ(¢Š(¢Šĺ×4m7^́ÓeÓµ«□{û)~ü3́Æ□sëľCèG"¼\_[ø□Ú~¬š¿ÃĬ□]é□Ñ1: yÚq□}+\βŒ.î4©´□V9œYCt¶÷±gåh¦"0øõI□mžË¿Ö€>HÔ?h□□Hŧû3SÖÛ□/Ú^Æ\õçå³^ÿþ°£

ĴXuï@□□j>□Ôu¡4¾#¼ø□â□"VÙ#éĺojì□□³Ï)Ú‡ÔÆ□ÏAŠf...๯±□‡¼□s q□1½î¶·ðgž□Á□ħ§WSÇnß][x□ÃÑN ″ÜØ hÝ! 2£Œ†a□àŒ2"#×5Ð|lð{x×áõö™□î»F[~'ÈNUy□²–Q'□Xdâ¹□Ù[ÄÒj¾□—AÔ□□OÃó›I□L‡□□Jd□~!Đ□8A@□·£iV□&Ÿ□† ′g⊨ '~@Ò&qó□Ô-};E□QE□WžÚx:-□âÃëúT ¾¯□¥ç•□å3□~—þîíªCr□W□d□Š(□Ш¢Š(¢Šý<mark>kev{vou</mark> are right}ÙÙ

https://blog.csdn.net/qq\_51090016

这样就比较简单了。



为什么解压打开就是这样的??难不成这题目和像素有关吗?



https://blog.csdn.net/qq\_51090016

#### 图片隐写之修改宽高

1.图片长宽有问题 未显示完全 需修改后可查看

2.原图片像素500\*420 420的十六进制是01a4,拖进winhex,500的十六进制是01f4,修改

3.得到原图片

也就是说,我们可以用winhex打开,然后把a4改成f4就行了,像下面这样:

WinHex - [2.png]		<b>r</b> Ska p		- @ ×
214(F) 3648(E) 38		890(H) • • · · · · · · · · · · · · · · · · · ·	8	20.0 X80 _ 8 ×
2.png			4	
Offset	0 1 2 3 4 5 6 7 8 9	ABCDEF10111	2 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F	^ 2 ppg
00000000	89 50 4E 47 0D 0A 1A 0A 00 00	00 0D 49 48 44 52 00 00 0	F4 00 00 01 4 08 06 00 00 00 CB D6 DF	SPNG C:\Users\真命你没办法\Pictures\CSDN博客\bugku\file
00000020	8A 00 00 00 09 70 48 59 73 00	00 12 74 00 00 12 74 01 D	66 1F 78 00 00 0A 4D 69 43 43 50 50 68	Š pHYs 文件大小: 17.3 KB
00000040	6F 74 6F 73 68 6F 70 20 49 43	43 20 70 72 6F 66 69 6C 6	00 00 78 DA 9D 53 77 58 93 F7 16 3E DF	otoshop I 17,675 字节
00000060	F7 65 0F 56 42 D8 F0 B1 97 60	81 00 22 23 AC 08 C8 10 5	A2 10 92 00 61 84 10 12 40 C5 85 88 0A	÷e VBØð±- 缺省编辑模式
00000080	56 14 15 11 9C 48 55 C4 82 D5	0A 48 9D 88 E2 A0 28 B8 6	41 8A 88 5A 8B 55 5C 38 EE 1F DC A7 B5	V ceHUÄ, mainersan
000000A0	7D 7A EF ED ED FB D7 FB BC E	9C E7 FC CE 79 CF 0F 80 1	. 12 26 91 E6 A2 6A 00 39 52 85 3C 3A D8	}Zïííû×û <sup>1</sup> 、反向撤消: 暂无信息
000000000	1F 8F 4F 48 C4 C9 BD 80 02 15	48 E0 04 20 10 E6 CB C2 6	05 C5 00 00 F0 03 79 78 7E 74 B0 3F FC	OHÄÉ <sup>1</sup> 2€ 創建时间: 2021/02/08
000000E0	01 AF 6F 00 02 00 70 D5 2E 24	12 C7 E1 FF 83 BA 50 26 5	00 20 91 00 E0 22 12 E7 0B 01 90 52 00	o pÕ. 20:06:57
00000100	C8 2E 54 C8 14 00 C8 18 00 B0	53 B3 64 0A 00 94 00 00 60	C 79 7C 42 22 00 AA 0D 00 EC F4 49 3E 05	È.TÈ È 最后写入时间: 2021/02/08
00000120	00 D8 A9 93 DC 17 00 D8 A2 10	A9 08 00 8D 01 00 99 28 4	24 02 40 BB 00 60 55 81 52 2C 02 C0 C2	ØC"Ü Ø¢
00000140	00 A0 AC 40 22 2E 04 C0 AE 01	80 59 B6 32 47 02 80 BD 0	00 76 8E 58 90 0F 40 60 00 80 99 42 2C	
00000160	CC 00 20 38 02 00 43 1E 13 CI	03 20 4C 03 A0 30 D2 BF E	A9 5F 70 85 B8 48 01 00 C0 CB 95 CD 97	Ì 8 C 模式: +大进制
00000180	4B D2 33 14 B8 95 D0 1A 77 F2	F0 E0 E2 21 E2 C2 6C B1 4	2 61 17 29 10 66 09 E4 22 9C 97 9B 23 13	KÒ3 ,•Đ w 偏移地址: 十六进制
000001A0	48 E7 03 4C CE 0C 00 00 1A F9	D1 C1 FE 38 3F 90 E7 E6 E	E1 E6 66 E7 6C EF F4 C5 A2 FE 6B F0 6F	HÇ LÎ 電贝字句数: 36x32=1152
000001C0	22 3E 21 F1 DF FE BC 8 数据解释器	10 4E CF EF DA 5F E5 E	D6 03 70 C7 01 B0 75 BF 6B A9 5B 00 DA	">! ñßþ¼Œ 2000 1
000001E0	56 00 68 DF F9 5D 33 D 8 Bit (±): -12	0A D0 7A F9 8B 79 38 F0	2 40 1E 9E A1 50 C8 3C 1D 1C 0A 0B 0B ED	V hßù]30
00000200	25 62 A1 BD 30 E3 8B 3 16 Bit (±) 2,292 32 Bit (±) 395,50	6F E0 8B 7E F6 FC 40 1	C FE DB 7A FO 00 71 9A 40 99 AD CO A3 83	%b;½0ã<>ý 暫存文件来: 10.1 GB 空余
00000220	FD 71 61 6E 76 AE 52 8E E7 CH	04 42 31 6E F7 E7 23 FE C	' 85 7F FD 8E 29 D1 E2 34 B1 5C 2C 15 8A	ýqanv®RŽç C:\Users\真争你没办法\Pictures\CSDN博客
00000240	F1 58 89 B8 50 22 4D C7 79 B9	52 91 44 21 C9 95 E2 12 E	7F 32 F1 1F 96 FD 09 93 77 0D 00 AC 86	ñX‱,P"MÇy
00000260	4F C0 4E B6 07 B5 CB 6C C0 7E	EE 01 02 8B 0E 58 D2 76 0	0 40 7E F3 2D 8C 1A 0B 91 00 10 67 34 32	OÀN¶ µËlÀ
00000280	79 F7 00 00 93 BF F9 8F 40 2F	01 00 CD 97 A4 E3 00 00 B	: E8 18 5C A8 94 17 4C C6 08 00 00 44 A0	y÷ ";ù €
000002A0	81 2A B0 41 07 0C C1 14 AC C0	0E 9C C1 1D BC C0 17 02 6	. 06 44 40 0C 24 CO 3C 10 42 06 E4 80 1C	*°A Á -
000002C0	OA A1 18 96 41 19 54 CO 3A D8	04 B5 B0 03 1A A0 11 9A E	. 10 B4 C1 31 38 OD E7 E0 12 5C 81 EB 70	; -A TÀ:
000002E0	17 06 60 18 9E C2 18 BC 86 09	04 41 C8 08 13 61 21 3A 8	11 62 8E D8 22 CE 08 17 99 8E 04 22 61	`žÂ ¼†
00000300	48 34 92 80 A4 20 E9 88 14 51	22 C5 C8 72 A4 02 A9 42 6	A 91 5D 48 23 F2 2D 72 14 39 8D 5C 40 FA	H4'€¤ é^
00000320	90 DB C8 20 32 8A FC 8A BC 47	31 94 81 B2 51 03 D4 02 7	6 40 B9 A8 1F 1A 8A C6 A0 73 D1 74 34 0F	ÛÊ 2ŠüŠ%
00000340	5D 80 96 A2 6B D1 1A B4 1E 3I	80 B6 A2 A7 D1 4B E8 75 7	00 7D 8A 8E 63 80 D1 31 0E 66 8C D9 61	]€-¢kÑ ´
00000360	5C 8C 87 45 60 89 58 1A 26 C	16 63 E5 58 35 56 8F 35 6	1D 58 37 76 15 1B CO 9E 61 EF 08 24 02	\@‡E`%X 6
00000380	8B 80 13 EC 08 5E 84 10 C2 60	82 90 90 47 58 4C 58 43 A	25 EC 23 B4 12 BA 08 57 09 83 84 31 C2	<€ ì ^" Â
000003A0	27 22 93 A8 4F B4 25 7A 12 F9	C4 78 62 3A B1 90 58 46 A	26 EE 21 1E 21 9E 25 5E 27 0E 13 5F 93	'"```O´%z
000003C0	48 24 0E C9 92 E4 4E 0A 21 25	90 32 49 0B 49 6B 48 DB 4	2D A4 53 A4 3E D2 10 69 9C 4C 26 EB 90	H\$ É'AN !
000003E0	6D C9 DE E4 08 B2 80 AC 20 97	91 B7 90 OF 90 4F 92 FB C	C3 E4 B7 14 3A C5 88 E2 4C 09 A2 24 52	mÉÞä ²€¬
00000400	A4 94 12 4A 35 65 3F E5 04 A5	9F 32 42 99 A0 AA 51 CD A	9 9E D4 08 AA 88 3A 9F 5A 49 6D AO 76 50	¤″ J5e?å
00000420	2F 53 87 A9 13 34 75 9A 25 CI	9B 16 43 CB A4 2D A3 D5 D	9A 69 67 69 F7 68 2F E9 74 BA 09 DD 83	/S‡© 4ušt
00000440	1E 45 97 D0 97 D2 6B E8 07 E9	E7 E9 83 F4 77 OC OD 86 01	83 C7 48 62 28 19 6B 19 7B 19 A7 18 B7	E-Ð-Òkè
< 00000460	10 0F 00 40 XC 0F F2 07 00 00		1 00 CP FF F0 28 PC 28 70 1F 01 08 10 0F	
页1/16	偏移地址:	17	= 244 选块:	10 - 17 大小: https://blog.csdn.nei/qq_5109001/8

#### 这样隐藏的信息就出来了



### 3 talent

```
打开文件:
```

е П.

🚄 net	working.pcap							×
文件(E)	编辑(E) 视图(V)	跳转(G) 捕获(C) 分析(A) 系	钻计( <u>S</u> ) 电话(Y) 无线( <u>W</u> )	工具(T) 帮!	助( <u>H</u> )			
	🖉 💿 📘 🛅 🗙	🖸 🍳 🗢 🔿 🕾 🕢 🛃	. 📃 🔍 🔍 🔍 🖽					
[] 应用:	显示过滤器 ··· ‹Ctrl-,	<i>/</i> >						+
No.	Time	Source	Destination	Protocol	Length Info			^
	1 0.000000	192.168.221.128	192.168.221.164	TCP	66 1146 → 23 [SYN] Seq=0 Win=8192	Len=0 MSS	=1460	
	2 0.000000	192.168.221.164	192.168.221.128	TCP	66 23 → 1146 [SYN, ACK] Seq=0 Ack	=1 Win=146	00 Lei	
	3 0.046800	192.168.221.128	192.168.221.164	TCP	54 1146 → 23 [ACK] Seq=1 Ack=1 Wi	n=65536 Le	:n=0	
	4 0.078000	192.168.221.128	192.168.221.164	TELNET	75 Telnet Data			
	5 0.093600	192.168.221.164	192.168.221.128	TCP	60 23 → 1146 [ACK] Seq=1 Ack=22 W	in=14624 L	.en=0	
	6 4.508408	192.168.221.164	192.168.221.128	TELNET	66 Telnet Data			
<	7 4 555208	192 168 221 128	192 168 221 164	TELNET	57 Telnet Data		>	, i
> Eth > Int > Tra	ernet II, Src: ernet Protocol nsmission Contro	VMware_84:86:5f (00:0c; Version 4, Src: 192.168 ol Protocol, Src Port:	29:84:86:5f), Dst: V 3.221.128, Dst: 192.1 1146, Dst Port: 23,	Mware_26: .68.221.16 Seq: 0, L	7e:0e (00:0c:29:26:7e:0e) 64 .en: 0			
0000	00 0c 29 26 /e	0e 00 0c 29 84 86 5t	08 00 45 00 ···)&~·	)	·E·			
0020	dd a4 04 7a 00	17 46 01 d3 fb 00 00	00 00 80 02 ···z··	F				
0030	20 00 3c 9d 00	00 02 04 05 b4 01 03	03 08 01 01					
0040	04 02							
0 🗹	networking. pcap				分组: 59 · 已显示: 59 (100.	0%)	置: Defa	<b>a</b> t016

怎么自动用wireshark打开了。。既然打开了,那就ctrl f 搜索一下flag吧:

<b>_</b> r	etworki	ing.p	сар																										_		×	(
文件	E) 编辑	輯(E)	视图	∃(V)	B	( <u>转(G</u>	i)	捕获(	<u>(C)</u>	分析	f( <u>A</u> )	统	i <del>tt (S</del>	) F	电话()	D i	无线( <u>W</u>	DI	具( <u>T</u> )	帮助	)( <u>H</u> )											
		۲	010				٩ «	÷ 4	> 🖻	<u> </u>	4				Ð, E		1															
	用显示过	が思る	\$ <	Ctrl	-/>										_															-	- +	
	分组	字节》	売 ∨		宽窄	2				~ [		分大	小写		字行	符串	~	fla	g										查找	取	消	
No.		Time				Sou	irce						Des	tina	ition				Protoc	;0l	Lengt	h I	Info									^
	36	17.9	92443	31		192	2.1	.68.2	221	.128	3		192	2.1	5 <mark>8.</mark> 2	21.	164		TELNF	ET	5	56 -	Telnet	: Dat	a							
	37	17.9	94003	31		192	2.1	.68.2	221	.164	4		192	2.1	<b>58.2</b>	21.	128		TELNE	ET	6	50 -	Telnet	: Dat	a							
	38	17.9	98683	31		193	2.1	.68.3	221	.128	3		193	2.10	6 <mark>8.</mark> 2	21.	164		ТСР		5	54 :	1146 -	• 23	[ACK]	Seq=8	3 Ack	=114	Win=65536	Len=	(	
	39	17.9	98683	31		193	2.1	68.3	221	.164	4		193	2.1	68.2	21.	128		TELNE	ET	6	64 -	Telnet	: Dat	a							
	40	18.0	0180	31		193	2.1	68.3	221	.128	8		192	2.1	68.2	21.	164		тср		5	54 :	1146 -	• 23	[ACK]	Seq=8	3 Ack	=124	Win=65536	Len=		
	41	18.4	42363	32		193	2.1	68.3	221	.128	8		192	2.1	68.2	21.	164		TELNE	ET	9	92 -	Telnet	: Dat	a							
<											-																			>		
S F	name (	11 :	92 h	vte	< 0	w w	ire	. (7	36	hit	5).	92	hv	+05	car	atur	ed (	736 ł	aits)			_										
ŚF	therne	+ T	TS	nc:	VM	war	0 8	84.8	6.5	f ((	273 99.1	ar:	29.	84.	86.0	Sf)	Dst	• VM	ane	26.7	70.00	- (	99.9c	. 29 . 2	06.7e	90)						
S T	terne	+ P	roto	col	Ve	nsi	e_c	4.0	Snc	. 10	92	168	22	1 1	28	Dst	F. 19	2 168	× 221	164	1	- (	00.00	. 2	.0.70.	00)						
S T	oonsmi	esi	on C	ont	nol	Pr	on	-, - col	5, 5	. 1 nc	Por	+•	114	6	Dst	Por	at · 2	3 50	a. 8	3 4	+ Vekt	12	A Ler	35	2							
vт	alnet		on c	Unic	102		000	1001	, -		0.		11-	,	552	10.		,	.q. c.	J,	ACK.		4,	1. 5.								
	Data	: f]	lag{c	1316	575	9628	81b	f925	5d66	10be	-698	3a49	9730	15}																		
		•					/	1						5																		
5																																
000	a <b>00</b>	θc	29.2	67	10 B	1e 0	10 (	Ar	29	84	86	5f	98	99	45 (	20	)	<u>گ</u> ~		F												
001	a 00	4e	07 b	04	00	10 8	10 6	86	00	00	c0	a8 -	dd	80	c0 i	a8	- N -	-@		<del>.</del>												ļ
002	bb 6	a4	04 7	a 0	0 1	7 4	16 (	ð1	d4	4e	68	fØ	2a	7a	50 1	18		z··F	· ·Nh	-*zF	ο.											
003	01	00	3c b	70	0 0	00 6	6 (	6c	61	67	7b	64	33	31	36 3	37	<	• • • <b>f</b>	L ag{	d316	57											
004	35	39	63 3	23	8 3	1 6	2 (	66	39	32	35	64	36	30	30 F	<u>52</u>	59c	281bf	F 925	d600	Эb											
005	ð 65	36	39 3	86	1 3	34 3	<b>9</b> 3	37	33	64	35	7d					e69	8a497	/ 3d5	}												-
																																- 1

就这么出来了???终于有一道题我能自己做出来了。。。

### 4.眼见非实

下载文件打开,是一个压缩包:

With With With With With With With With	📑 file (1) - 36	0压缩				文件	操作	工具 帮助	🍄 🗢 🗕	
添加 解圧到 -键解压 删除 压缩包清言          ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●					码				[	安全
●       ●	添加	解压到	一键解压	删除	压缩包语言					
医缩前         压缩前         压缩前         医细目         文件夹           ① 銀见非实.docx         13.7 KB         10.0 KB         DOCX 文档         2016-12-07 16:00	<b>☆</b> 🔲 🗄	📑 file (1).zi	p - 解包大小り	5 13.7 KB				V ▼ 搜	素包内文件	Q
■ (上级目录) 文件夹 ① 眼见非实.docx 13.7 KB 10.0 KB DOCX 文档 2016-12-07 16:00 大小: 10.0 KB 共 1 个文件 压缩率 73.2%	名称					压缩前	压缩后	类型	修改日期	
■ 眼见非实.docx 13.7 KB 10.0 KB DOCX 文档 2016-12-07 16:00 大小: 10.0 KB 共 1 个文件 压缩率 73.2% Ntips://blog.cscin.net/og_51/090018	📙 (上级目录	)						文件夹		
大小: 10.0 KB 共 1 个文件 压缩率 73.2%	🖲 眼见非实.do	ocx				13.7 KB	10.0 KB	DOCX 文档	2016-12-07	16:00
大小: 10.0 KB 共 1 个文件 压缩率 73.2%										
大小: 10.0 KB 共 1 个文件 压缩率 73.2%										
大小: 10.0 KB 共 1 个文件 压缩率 73.2%										
大小: 10.0 KB 共 1 个文件 压缩率 73.2%										
大小: 10.0 KB 共 1 个文件 压缩率 73.2%										
大小: 10.0 KB 共 1 个文件 压缩率 73.2%										
大小: 10.0 KB 共 1 个文件 压缩率 73.2%										
大小: 10.0 KB 共 1 个文件 压缩率 73.2%										
大小: 10.0 KB 共 1 个文件 压缩率 73.2% https://blog.csdn.net/gg_51090016										
大小: 10.0 KB 共 1 个文件 压缩率 73.2% https://blog.csdn.nai/qc_51090016										
大小: 10.0 KB 共 1 个文件 圧缩率 73.2% https://blog.csdn.nei/gq_51090016										
大小: 10.0 KB 共 1 个文件 压缩率 73.2% https://blog.csdn.nei/qc_51090016										
大小: 10.0 KB 共 1 个文件 压缩率 73.2% https://bloglesdn.nei/gq_51090016										
	大小: 10.0 KB	共 1 个文件 压	缩率 73.2%					https://blog	g.csdn.nət/qq_5	1090016

### 再打开里面的docx:

▶PK	I ?	眼见非实/up	懷美刘瑙例潛淪?PK
一堆奇怪的东西,用winhex看看文件头:			

建定.docx																	
Offset	0	1	2	3	4	5	6	7	8	9	Α	В	С	D	E	F	1
00000000	50	4B	03	04	0A	00	00	00	00	00	E2	20	0 F	49	00	00	0
00000020	BC	FB	В7	С7	CA	В5	2F	75	70	12	00	01	19	91	A4	C1	E
00000040	04	0A	00	00	00	00	00	C1	20	0 F	49	00	00	00	00	00	0
00000060	C7	CA	В5	2F	63	75	73	74	6F	6D	58	6D	6C	2F	75	70	1
08000000	E5	AE	9E	2F	63	75	73	74	6F	6D	58	6D	6C	2F	50	4B	0
0A000000	9D	00	00	00	FE	00	00	00	1C	00	29	00	D1	DB	BC	FB	В
00000000	74	65	6D	31	2E	78	6D	6C	75	70	25	00	01	9C	87	34	1
000000E0	73	74	6F	6D	58	6D	6C	2F	69	74	65	6D	31	2E	78	6D	6
00000100	91	2E	5C	88	0A	42	DD	D6	42	<b>A</b> 0	AB	6E	92	38	9A	40	7
00000120	D6	3C	6C	51	41	22	1C	2C	28	84	89	E3	61	A1	Α5	EF	F
00000140	E3	Α1	D8	93	Α5	E4	84	0F	E1	32	CE	96	92	17	C4	94	6
00000160	06	27	52	11	56	F0	79	9B	43	74	02	F3	19	17	16	CE	F
00000180	AB	3E	BE	Β1	BF	Α4	ΒA	86	FD	1E	EE	AE	97	0 F	50	4B	0
000001A0	DB	00	00	00	55	01	00	00	21	00	2E	00	D1	DB	BC	FB	В
000001C0	74	65	бD	50	72	6F	70	7数	据解释器		× 1	6D	60	75	70	2A	0

发现文件头为50 4B 03 04说明是一个压缩文件,后缀改成zip再解压缩:



#### 只好每个都看看,终于在document.xml里找到了:

7		-		×
i	文(年(F) 編編(E) 確式(C) 童音(V) 審測(F) ath" xmlns:v="urn:schemas-microsoft-com:vml" xmlns:wp14="http://schemas.microsoft.com/office/word/2010/wordprocessingDrawing" xmlns:wp="http://s "eastAsia"/> <w:vanish></w:vanish> <td>schen v:id="</td> <td>nas.op 0" w:n</td> <td>en: an</td>	schen v:id="	nas.op 0" w:n	en: an

0	
<	>
	第 2 行, 第 1458 列 100% Windows (CRLF) UTF-8_51090016

### 5.啊哒

描述: 有趣的表情包来源: 第七届山东省大学生网络安全技能大赛

下载压缩包打开,是一张图片:



用记事本打开看看,搜索一下flag:

有一个txt文件,按照我之前做题的经验,我可以把这个文件后缀改成zip然后用360压缩打开,应该就可以分离出文件:

<table-of-contents> ada - 360</table-of-contents>	缩				文件	\$ 操作	工具	帮助	<b>1</b>	_ 0	×
添加	<b>新</b> 定到	一键解压	副除	四月						扫描	
♠ 🔲 🗄 (	📕 ada.zip	- 解包大小为 1	1 KB				V	▼ 搜索	包内文件		Q
名称 (上级目录)					压缩前	压缩后	类型 文件夹		修改日期	1	
flag.txt *			入密码 为加密的文 flag.txt □ 显示密码 管理密码	件输入密码: 吗	确定	Ęχ	✓		2018-10	)-18 15:44	
大小: 1 KB 共 1	个文件 压缩	率 154.5% 已经	经选择 1 KB	(1 个文件)			https	:://blog.	csdn.net/q	q_510900	016

成功了,然后怎么获得密码又没思路了。。只好到此为止百度一下大佬。

① 图片信息	×
图片名称: ada	重命名
图片类型: JPG	转格式
图片大小: 213.83KB	压缩
图片尺寸: 826x672	<u>修改</u>
图片位置: C:/Users/真拿你	打开
收起更多信息	$\odot$
修改时间: 2018-10-18 15:47:50	
拍摄日期:	
相机厂商:	
设备型号: 73646E6973635F3230	3138
镜头型号:	_
光 圈值:	
最大光圈:	
曝光时间:	
曝光补偿:	
ISO 感光:	
焦 距:	
测光模式:	
闪 灯:	
白 平衡: Auto white balance	
亮 度:	

묘	14	得	Ż	
150	26	Ξ±/	7,	•
	~ •		-	

原来另一个关键点在图片属性里,查看图片属性会发现下面有一串16进制编码: 把这个16进制编码转字符,就是解压的密码了:

16进	制到文本字符串
加密	或解密字符串长度不可以超过10M
1	73646E6973635F32303138
16进	制转字符 字符转16进制 测试用例 清空结果 复制结果
	<ul> <li>Microsoft 微软官方商城</li> <li>24期免息, 免运费</li> <li>Surface Pro X</li> <li>网络优先,轻薄便携</li> </ul>
1	sdnisc_2018

### 输密码解压就行了

-						 	 									_
	🥘 flag ·	- 记事本												-	×	
	文件(F)	编辑(E) 相	格式(O) 查看()	/) 帮助	)(H)											
	flag(3X	iF iNf0r	M@ti0n}													$\sim$
	nagion		meetionij													-
																P
-																
c																100
j																
0																0.03
π																
																•
1																
1																
1																
0																1
1																·
0																
0																
																. eb
1																$\mathbf{v}$
	<														>	
- 10																

## 总结:

1.图片隐写先转换下格式看看:jpg可以换成html或者txt

2.图片隐写之修改宽高

.图片长宽有问题 未显示完全 需修改后可查看

原图片像素500\*420 420的十六进制是01a4,拖进winhex,500的十六进制是01f4,修改

3.文件按原本的格式打开不对时,可以用winhex打开看文件头看文件类型再打开

4.文件用winhex打开发现隐藏flag.txt文件时,可以改后缀名为zip,然后用360压缩打开,就可以分离出flag.txt

5.有些信息会隐藏在图片属性里