# bugku CTF misc 解题报告 一 （1-5）

原创

Vayn3 于 2021-02-09 17:18:50 发布 152 收藏

文章标签： 信息安全



本文链接：https://blog.csdn.net/qq_51090016/article/details/113760593



## bugku CTF misc解题报告



## 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：

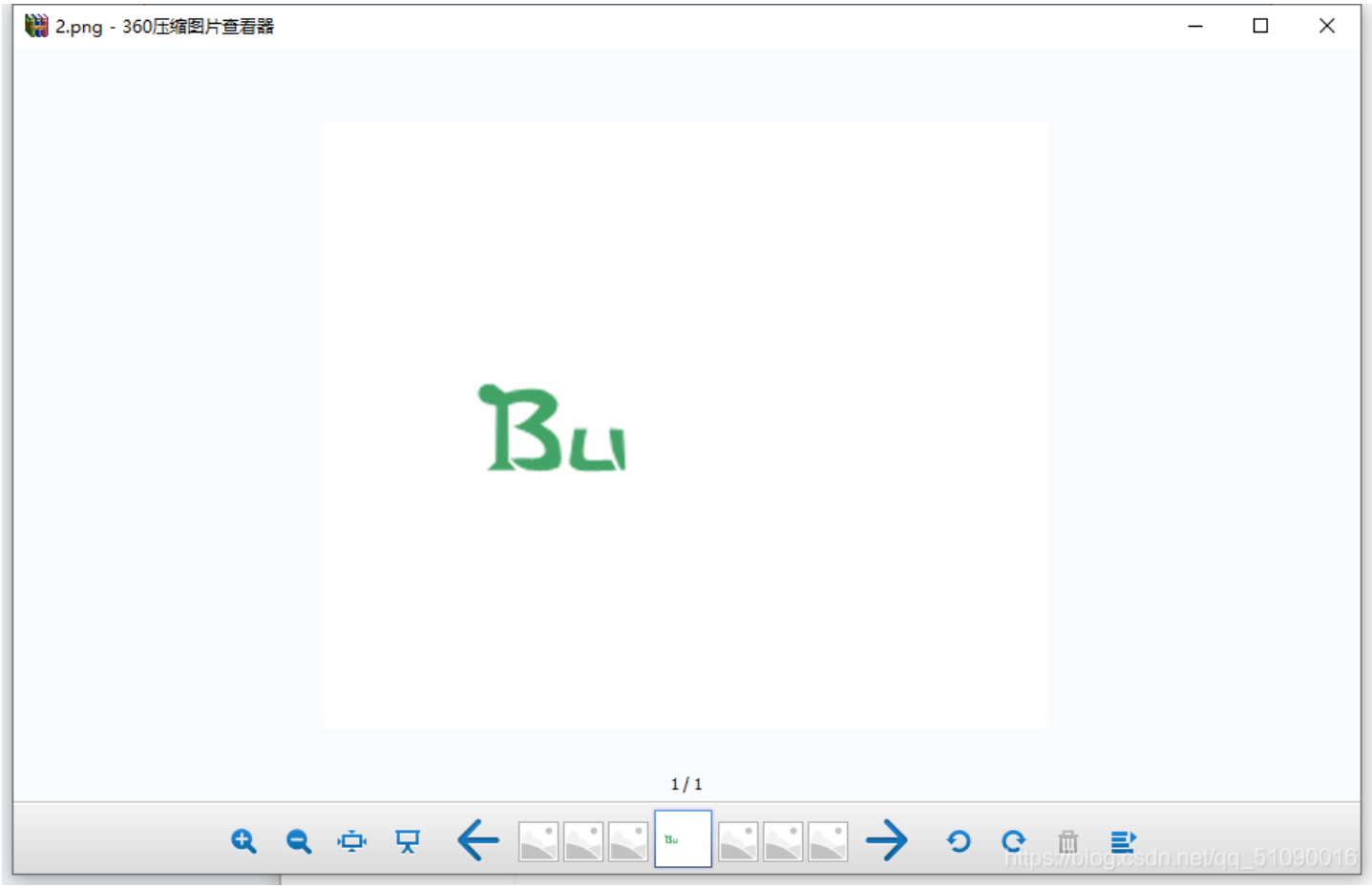
TUVWXYZcdefghijstuvwxyzƒ„…†‡ˆ‰Š‘ “” •—˜™š¢£¤¥¦§¨©ª²³
□□□□□□□□w□□□□□□!1□□AQ□aq□"2□□□B ‘¡±Á #3Rð□brÑ □$4á%ñ□□□□&'()*56789:CDEFGHIJSTUVWXYZcdefghijst
üOÐ¼.×vmp&ÕádŒÛ”
F9è:×®hZ®·¤ZjZ|žeµÌbD=□Ïf□˜r□ìA□« ‘ñÿ, 4ëï□ê¯§i□ g…¾Ök□j, ù9%□c□`ê’ □•l□à°>□û=x°ÏÃZêÃ}¨Ý□□þ7†□CbÝ'□” 3
□¬ÅûCx□ï¼¡¿¼Ž×ÊW7me6ÈÜ “û¶□w□Æ9©ÉçŽ}7DÖtýrÅot‹¸î˜íÞ‡î ‘ØƒÈ<Ž□□5ä □¾□é’ x"çSÑm□ÞóL□¥□ b%º€gÍ□Çï¾
Úk7□7¡:□îb□FÛsÝ¥” d÷ˆ□Ô□ôÍ|Oñ3ÃÃÂ~3ñ†Žb i3®µ§E€□VÝæ(ÈÂ®Ï9lõŽ?j÷o‰ □›Ã—_fÐ¬¯É°Kß5äcòÉ□¤*©à|
w6□ñ¯X½V ú~µr □□™|ù/"@:□ÒDêOûJ=+sö|ø†|!yý™¯□ “H½ŒÈ¤:□ □pÝ–#²• ä□¨□@□□ñž)n~*kšî□2› öÜÛÎ□□ÊG□’ m□
y¯□ñV□dß´4v×?ºMfûQ± ‘×, V].Ü□?ß□¿□úUœçÕ□Vv, ÷Ï£Ÿÿk B"Ô□0· ¬□KŽ□” ŽªHÈèpF@9□£@□□Q@□□Q@□□Q@□□
Ëìâ F¶†pÇi ™Ñ□»□□M/$□’ ¼×ÎZæƒs£K□úåÅ€½¸w□ZFñ–ƒ □™□€¬9R£□□âÄTœ[¶ÇÓdØL=x%R×w(ØµÅÕ™¹: “□d‰,'€!Ýä
÷4ÿ†ûÍo□¶Í7‰£K)b†÷Ì□€÷) x™$□ª[$|ÞY%□p:c “W h'ð*hÖ6:□©oqâ=5Ùæ6±□³]¬ÜÄ□Ê□»²¼œ*°,O^□ãHifqb□!ëå¨É□
³□Úì‹□□ÎpÌÇï□½ø□□□h·¾%ø©£k□YÜG¥éòX\ÝµÝ©€OçÜÁlG” ä°«*Hv· !□±?BxWÃ□7…t÷±ðîŸ …£¸ ‘¢‹8g□©»žåQr{ ’ ”’
#eRçÙr}»×±ø¯À^□ñAi5M=~ÔÛOÚ`&)N9]Ä}ð□ 6@ô¯□ñŸïÏg©Eæh¾ »ûH□•Ô’ 9□’ Xÿ¬DV^X’ Hbh□Õü□ñ□Cñ¥®û□-
|R9‰C)ëŒc•*JÐ□Ò´SQ•Ô2□Ê@ ŽsN □Š( □Š( □¦□&ŠHåEx□J²0È`x Žå¼ëâ?‡tï□ø□_Ôü+¡éVZ¼V¯²æ□T‰ÑO□Á” □□]Ç9ê□
‡ò□‡_□|C¯ÙéÚ□^eM*Öï24@fhâÇËÁèÌOô□'œ□ôwƒ>□øsÂ□□F³ ‘gP3,Ó¼…›□/, v«□ ’•□, GN+ÏX+ÏšGØTâw□3¥lê×Üp-ð&
Ɔñes¬¢£†Eš□•□(ê□O¨¨5ƒãó¬□□ë□Ã0Å>®-ÛÈŠGd□{€ÊC□+□¤□†Ç5¡ÊtTW, |□øÝ/‹µ&ð÷ŠâKMc¥
Úclå›È—ƒå□òHv¯□sŽ □¶Eoª|□â3ÅÚ2ê□L□€Þ\ÐJ6Ëo êŽ½U‡ëÔd□Ïø‹à{□□é ‘Ç4’ Yj–□æØj0q-¬ž ŽJ’ □W#8□, □□Mg«j□
□žx¯” > øRÿâ□Žµ□W_»ae¢7Ê□n□æGw`€, ¤□29'?1L†□Š÷ïÚ□[þÂøEâ)Ãª Ëq³@O-æ□Œ□¸RÍÇ`Mr?²6žÚofx_Rø…ã□øY^2HÓ
Œ□4□0□C€NO''9Ârö¿□|sà+˜ô¯□hRk)·0É:=□Û□sóeJ¾ÞFUp ¼{ú_í□
-ÇèüGœý=+Ð(¢€ àþ2x□ßÇ> ¼´□7öµ¼RIa4d+¬…H)’ @Úãã`N□>À×yE|Çû4|@}3T □x…^Í.□›□>åÅÀ8–□›£□ÜqÙÃ□’ Ã?N
3›Ô`»þ~Â½;àæ” tyI¡2ƒõ n □Å½ÍcþÍ□—ß ôÉ´ù&xnÉ□’ SŸ.P□%□ÑL^ì□ûU¥ñÒhm|□÷w<Åownì2GÊd Ü, 1ò³~□®[öN2'€µ»
ıŸ□¼:þ)ðV§¥Û?—|ñù¶’ □□ “¡ß□Ïa¸}‰¯&øOiú›‹áÙ"™âû□’ é—0ÏÄ¢ÖVWVn□L2¸Œœ˜ö8ú□Š( □Š( □Š( □Š( □Š(ïy§Çµ†
•`»mláXcÏRê)ÏR{ “@□TQE□â?□t□ðÿ‰.¯4í"□Ë=eþÓ·1G²é□E–7g*□SBòä□H&GPXá½°¸□‰›□Ôu{Y¤Ñ"³ºK¤òµ
!□~Y□Šä("0□□©|)â□□ÅZj^èWÑ\ÆÊ□£□□EžÎ½Tý~£#šÜ¢Š(¢Š(¢ŠäuÏ‰› Ñ□&£â]-
ıKI,¬□Pz’ x□¼§â □□Ÿ¤Ãs ¥Þ□ åš+{}Ë□Ú” œ□WF"E„çîª³°ÎUTaþs°ø…ãÿ‰ž , +iœl¼□¡±…
₂□□OÞ:Žë□g%$ÏÐ•OJ°·Òôû{+□ÄvÐ D\ “Ç©'' sÔžIäÔÊ(¢Š(¢ŠÎ×4m7^ÓeÓµ«□{û)~ü3Æ□sëÏCèG"¼_[ø□Ú~¬š¿ÃÏ□]é□Ñ1
yÚq□}+\ßŒ.î4©´□V9œYCt¶÷±gåh¦"0øõI□mžË¿Ö€›HÔ?h□□H‡û3SÖÛ□/Ú^Æ\õçå³^ÿþº£
□Xuï@□□j›□Ôu¡4¾#¼ø□â□"VÙ#éÍojì□□³Ï)Ú‡ÔÆ□ÏAŠf…à¹¯±□‡¼□s q□1½Î¶·ðgž□Á□Ä§§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□˜!Ð□8A@□·£iV□&Ÿ□† ‘g
’~@Ò&qó□Ô-};E□QE□WžÚx:-□âÃëúT ¾¯□¥ç•□å3□˜—þíîªCr□W□d□Š(□Ð¨¢Š(¢Š(¢Šÿkey{you are right}ÙÙ



这样就比较简单了。

## 2.隐写

是一个压缩文件，打开得到：




为什么解压打开就是这样的？？难不成这题目和像素有关吗？

看了大佬的wp才知道还真和像素有关，这是一种改变图片宽高的方法，具体如下：

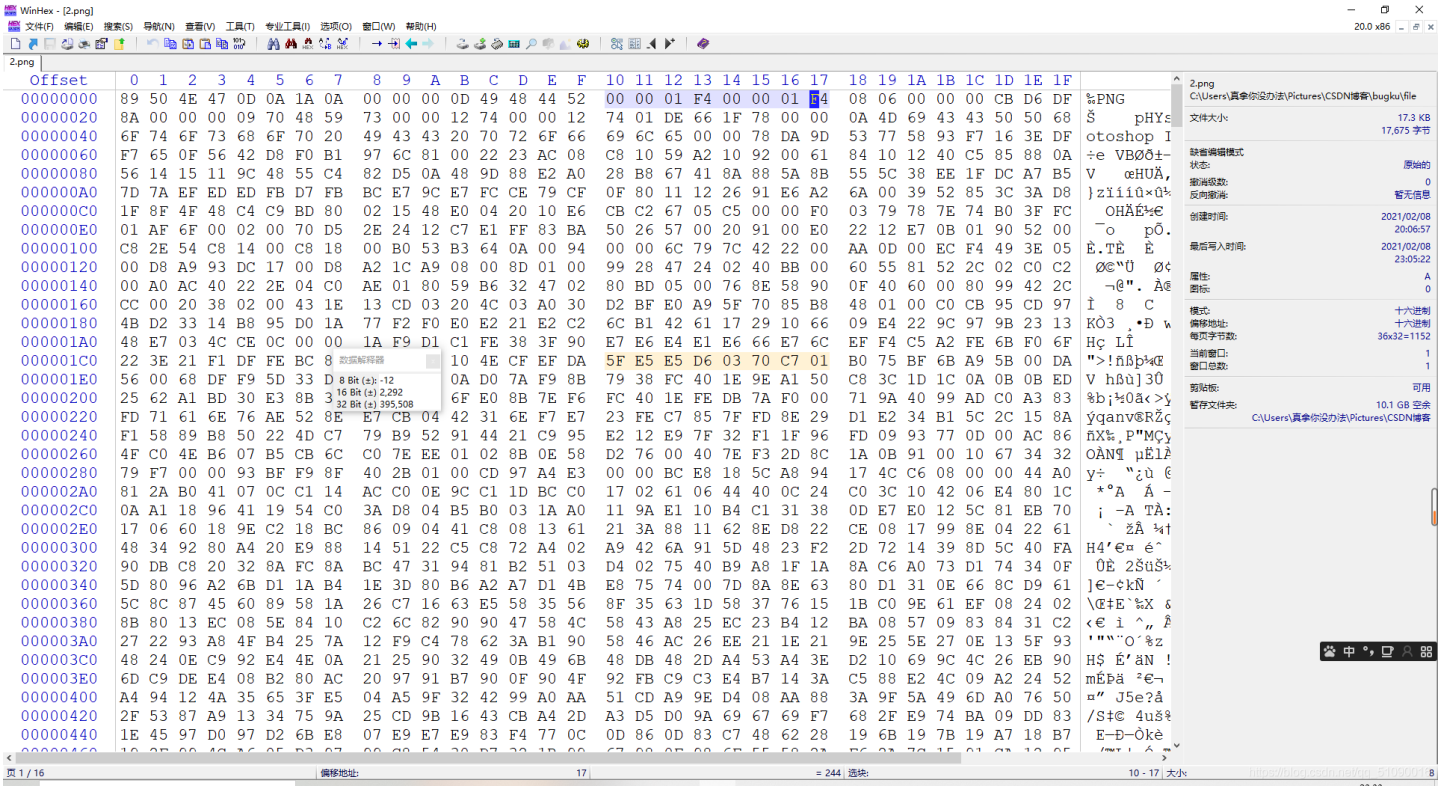
**图片隐写之修改宽高**

**1.图片长宽有问题 未显示完全 需修改后可查看**

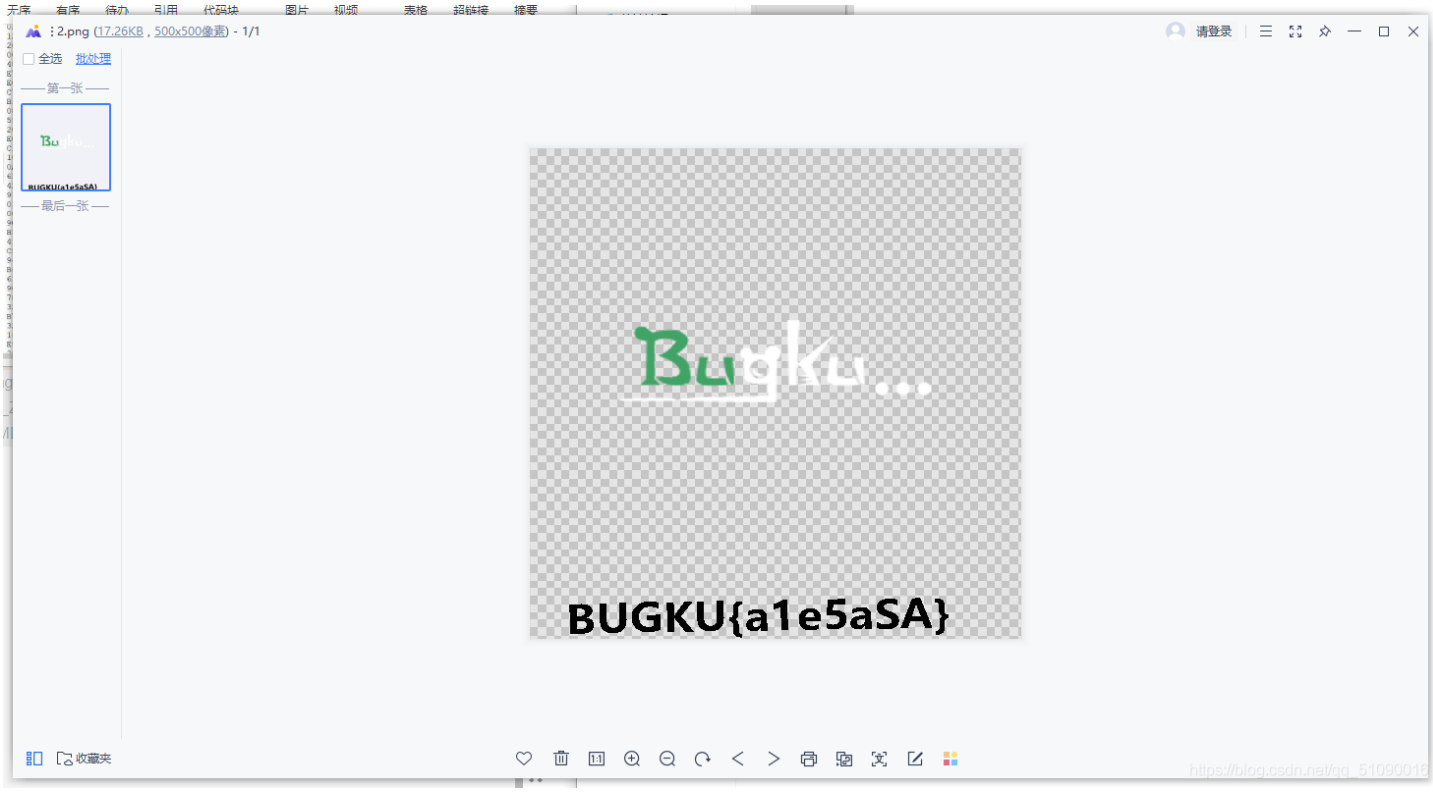
**2.原图片像素500*420 420的十六进制是01a4,拖进winhex,500的十六进制是01f4，修改**

**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：

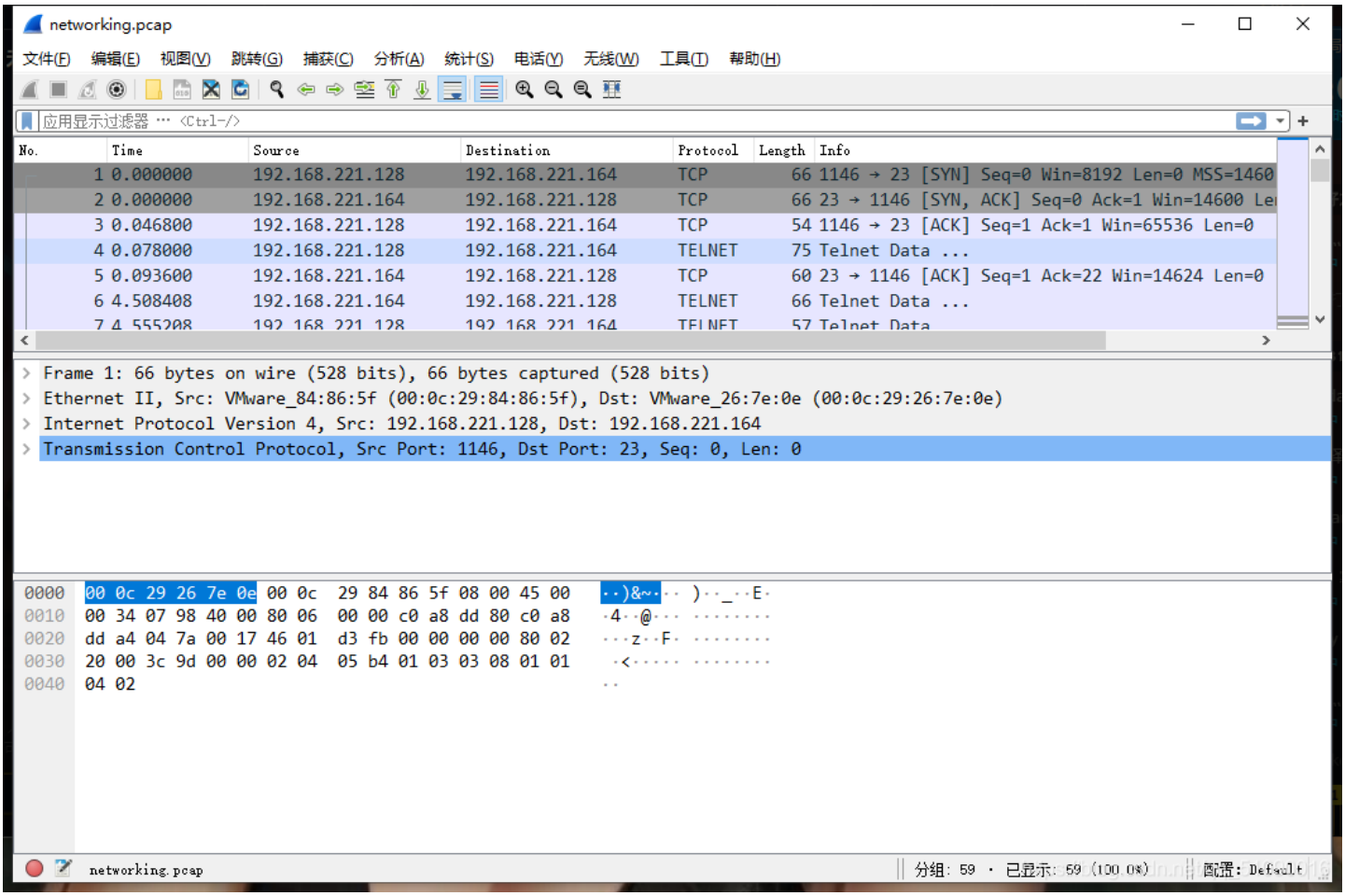


这样隐藏的信息就出来了

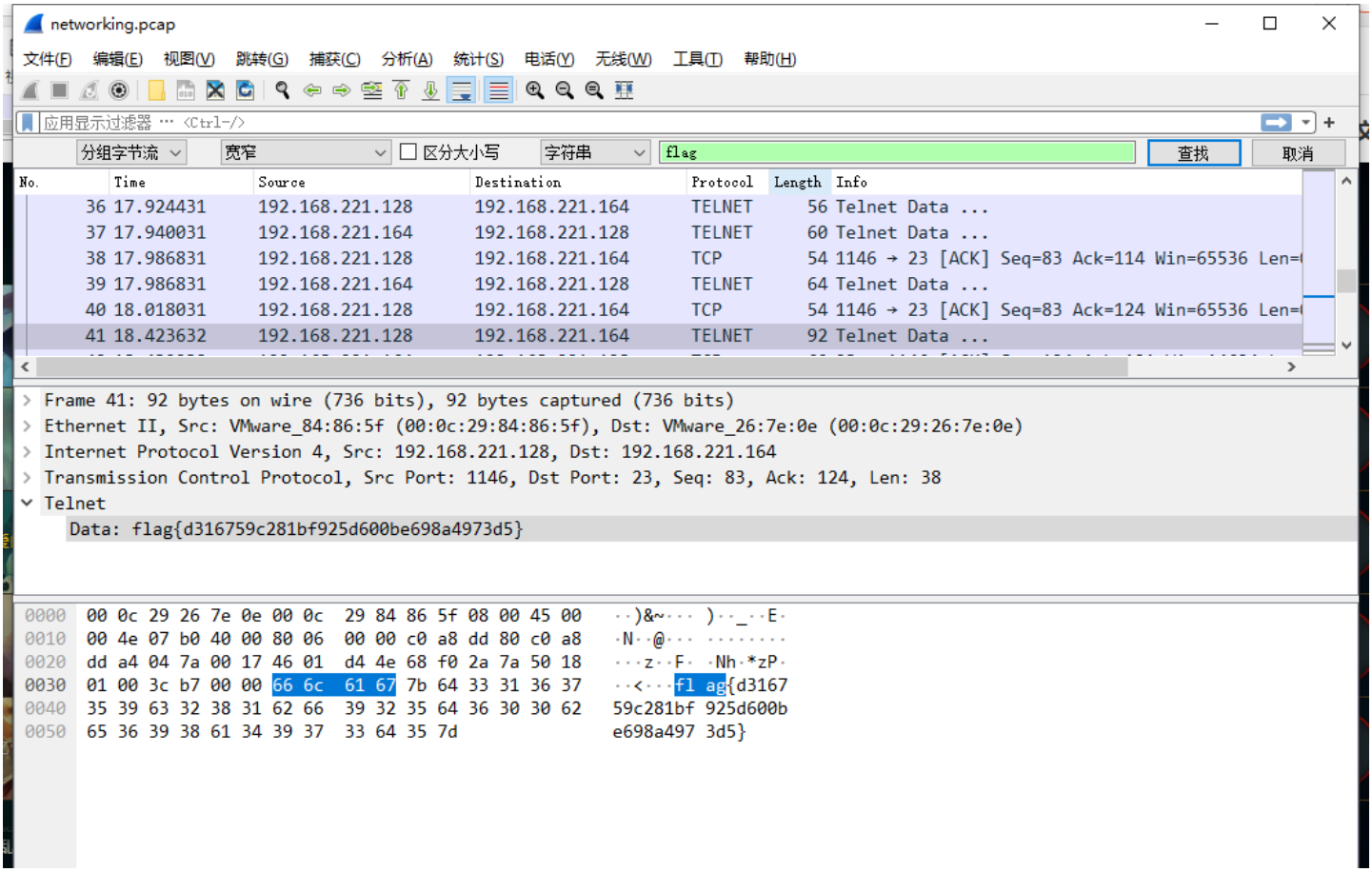



## 3 talent

打开文件：



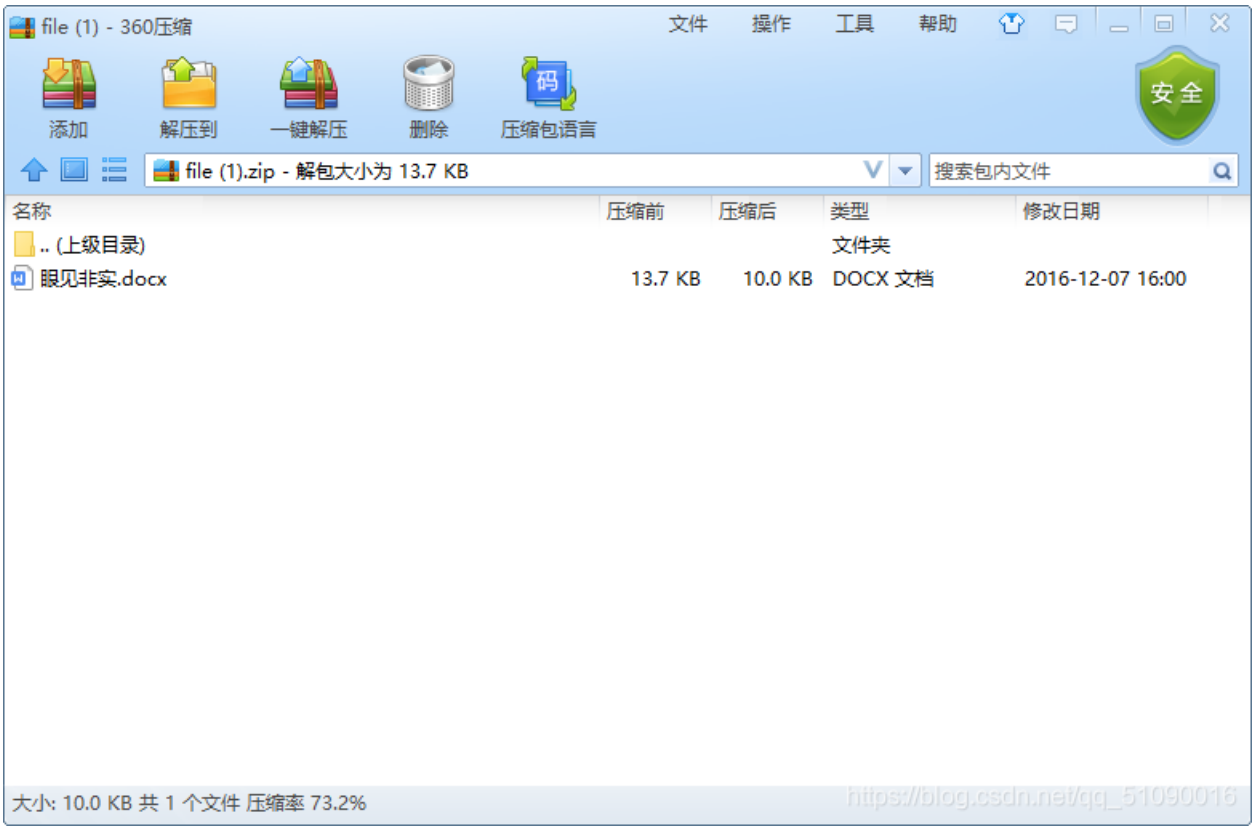

怎么自动用wireshark打开了。。既然打开了，那就ctrl f 搜索一下flag吧：



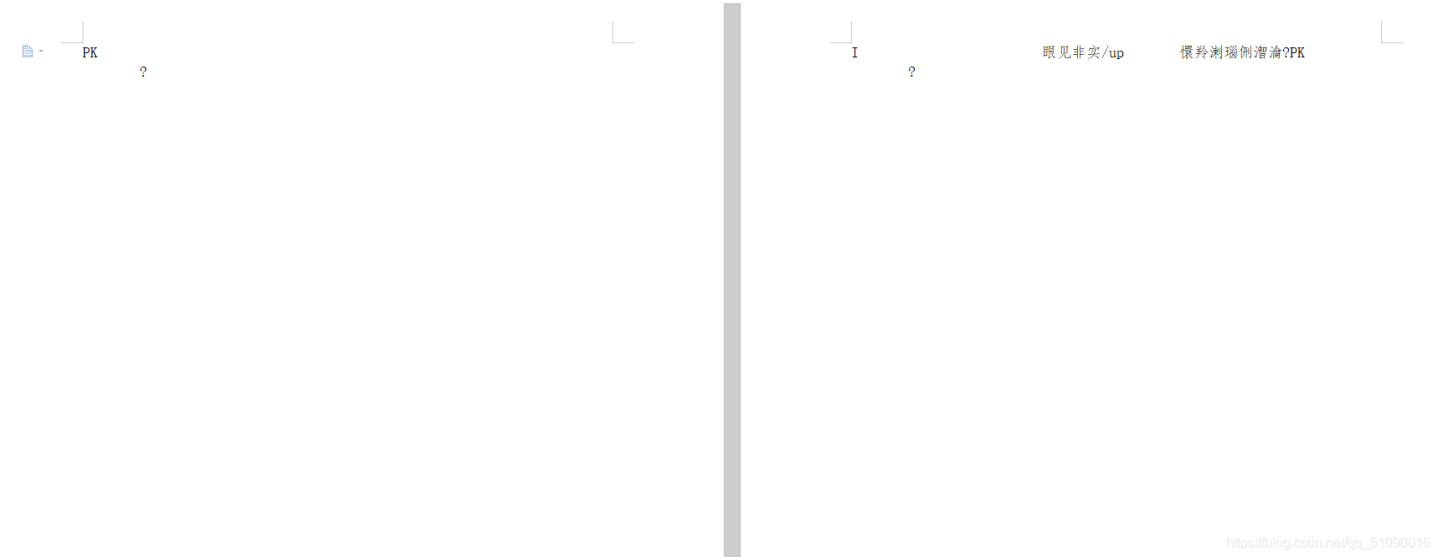

就这么出来了？？？终于有一道题我能自己做出来了。。。

## 4.眼见非实

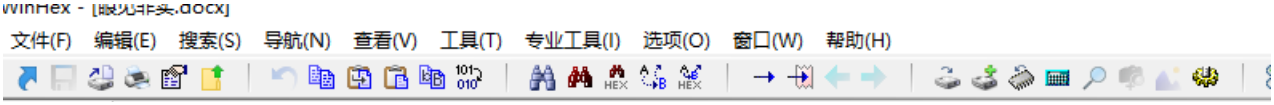
下载文件打开，是一个压缩包：




再打开里面的docx：




一堆奇怪的东西，用winhex看看文件头：

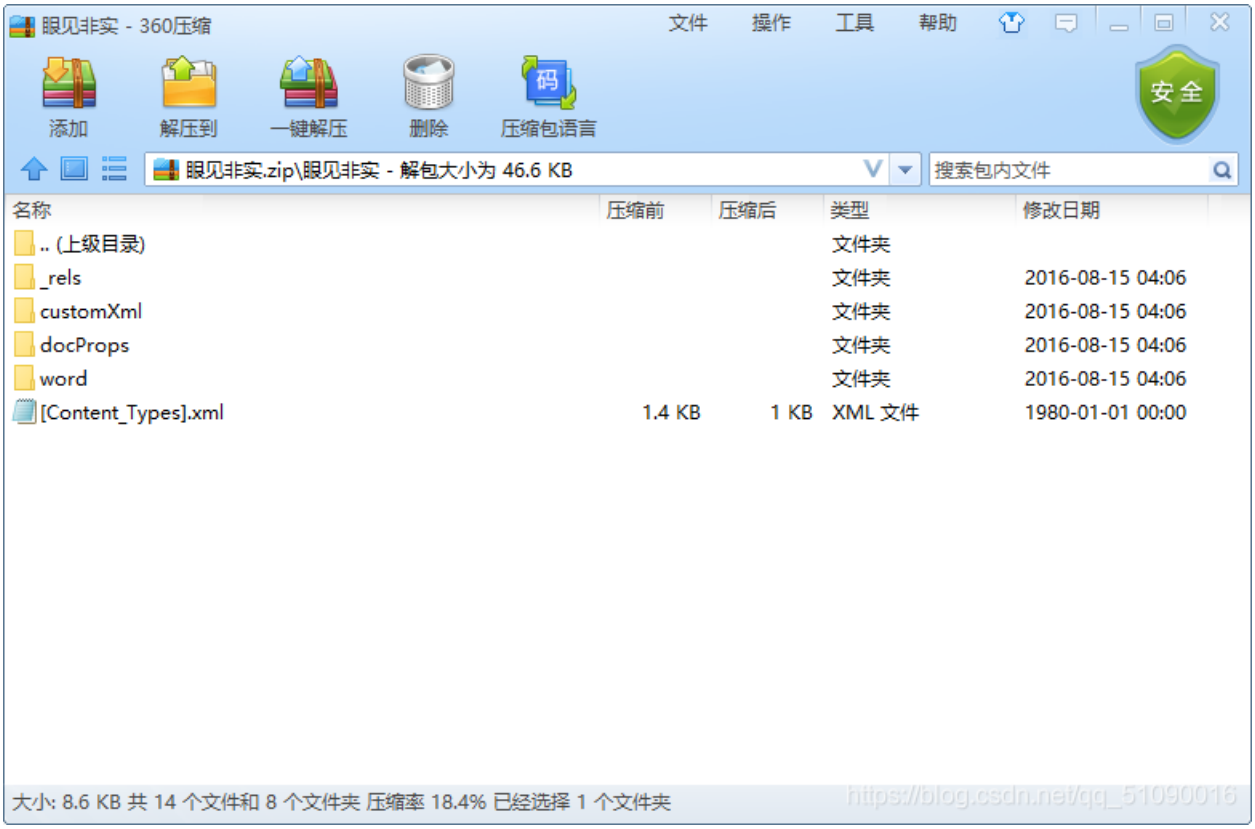


非实.docx

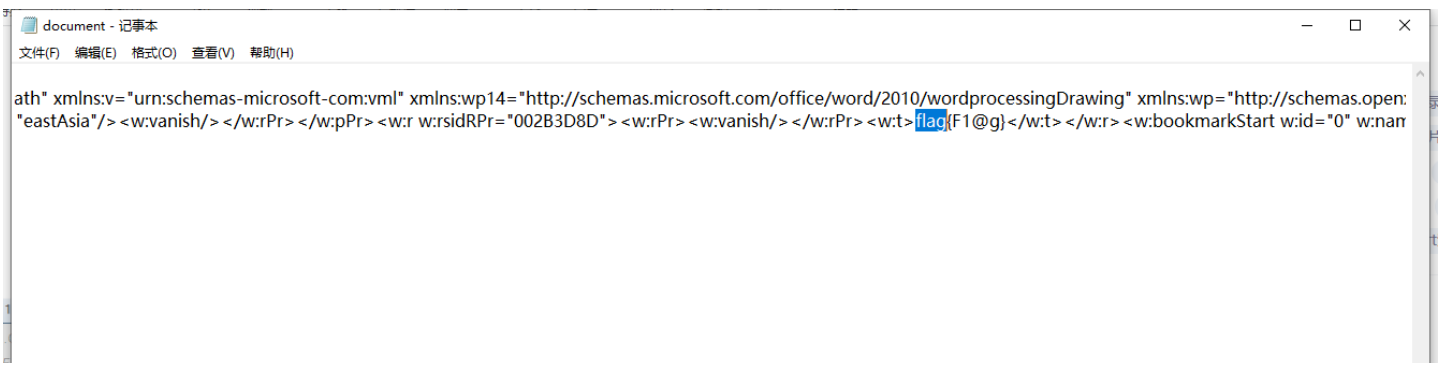
| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00000000 | 50 | 4B | 03 | 04 | 0A | 00 | 00 | 00 | 00 | 00 | E2 | 20 | 0F | 49 | 00 | 00 | 0 |
| 00000020 | BC | FB | B7 | C7 | CA | B5 | 2F | 75 | 70 | 12 | 00 | 01 | 19 | 91 | A4 | C1 | E |
| 00000040 | 04 | 0A | 00 | 00 | 00 | 00 | 00 | C1 | 20 | 0F | 49 | 00 | 00 | 00 | 00 | 00 | 0 |
| 00000060 | C7 | CA | B5 | 2F | 63 | 75 | 73 | 74 | 6F | 6D | 58 | 6D | 6C | 2F | 75 | 70 | 1 |
| 00000080 | E5 | AE | 9E | 2F | 63 | 75 | 73 | 74 | 6F | 6D | 58 | 6D | 6C | 2F | 50 | 4B | 0 |
| 000000A0 | 9D | 00 | 00 | 00 | FE | 00 | 00 | 00 | 1C | 00 | 29 | 00 | D1 | DB | BC | FB | B |
| 000000C0 | 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 | A0 | AB | 6E | 92 | 38 | 9A | 40 | 7 |
| 00000120 | D6 | 3C | 6C | 51 | 41 | 22 | 1C | 2C | 28 | 84 | 89 | E3 | 61 | A1 | A5 | EF | F |
| 00000140 | E3 | A1 | D8 | 93 | A5 | 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 | B1 | BF | A4 | BA | 86 | FD | 1E | EE | AE | 97 | 0F | 50 | 4B | 0 |
| 000001A0 | DB | 00 | 00 | 00 | 55 | 01 | 00 | 00 | 21 | 00 | 2E | 00 | D1 | DB | BC | FB | B |
| 000001C0 | 74 | 65 | 6D | 50 | 72 | 6F | 70 | 7 | | | | | 6D | 6C | 75 | 70 | 2A | 0 |

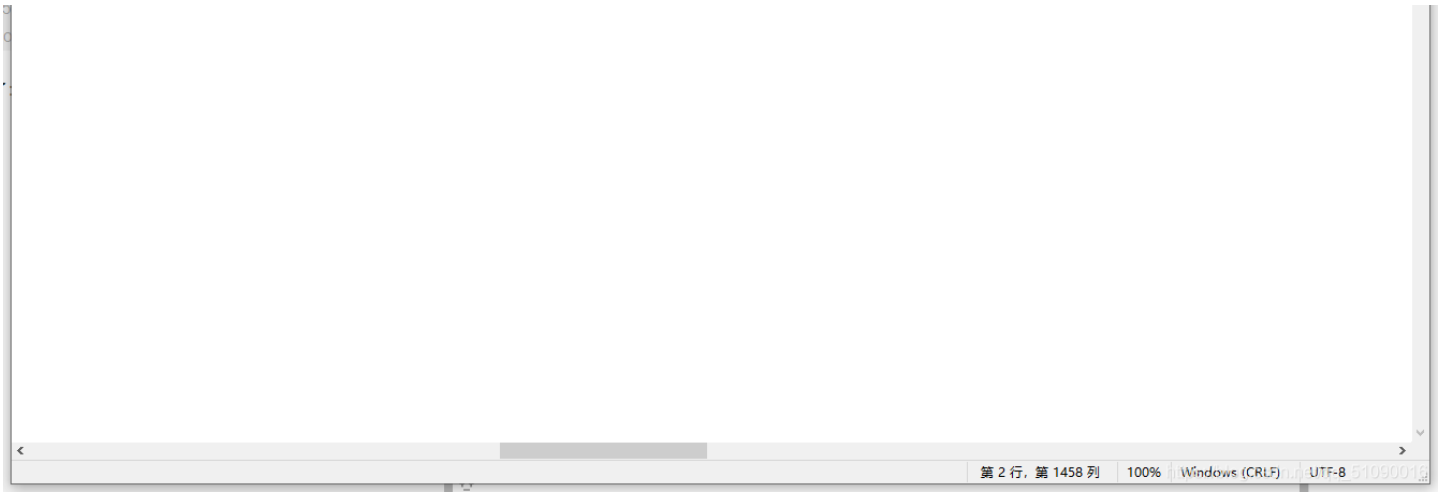
数据解释器

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：



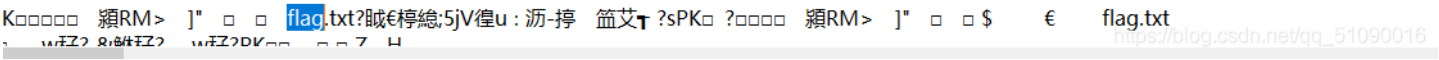



## 5.啊哒

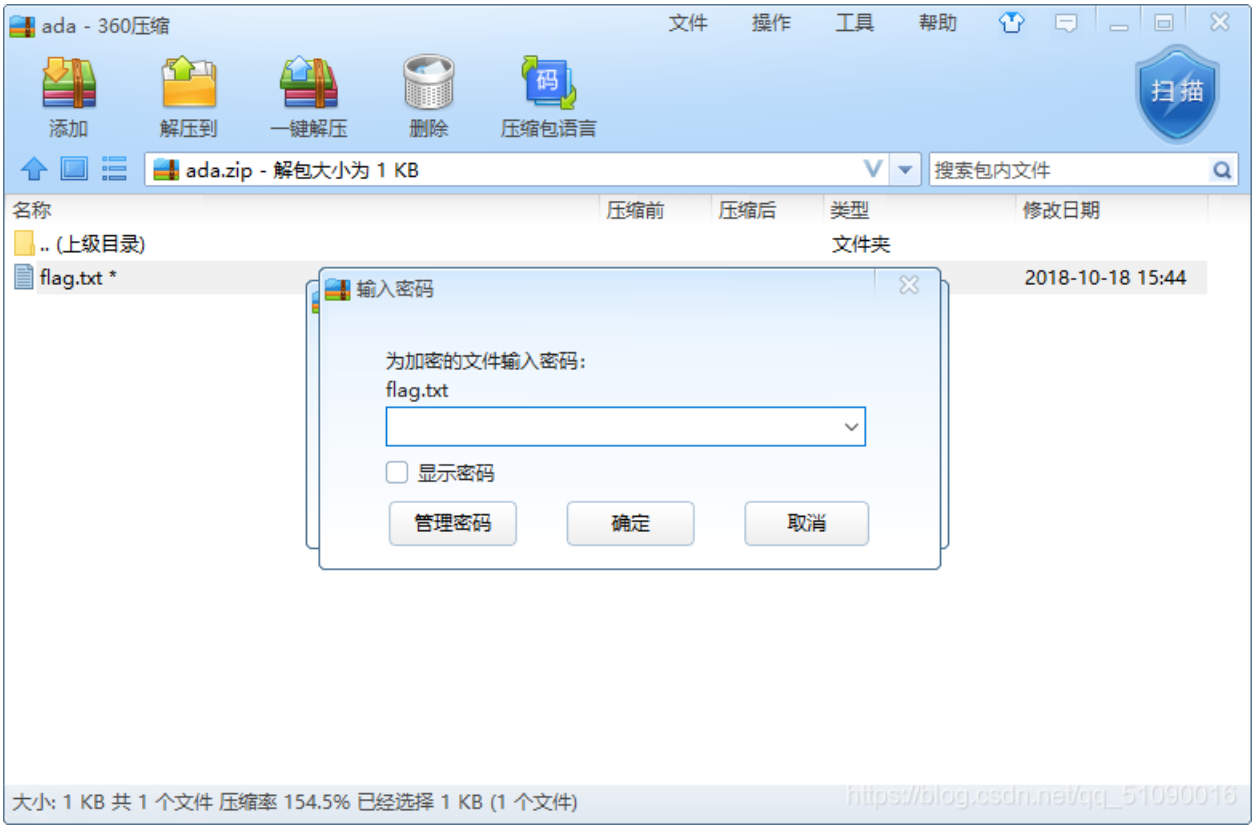
描述: 有趣的表情包 来源：第七届山东省大学生网络安全技能大赛

下载压缩包打开，是一张图片：

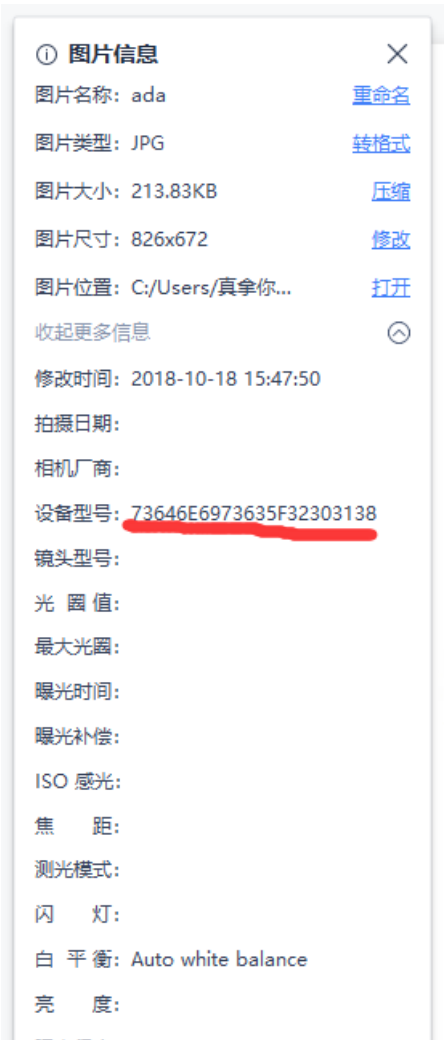

用记事本打开看看，搜索一下flag：



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：

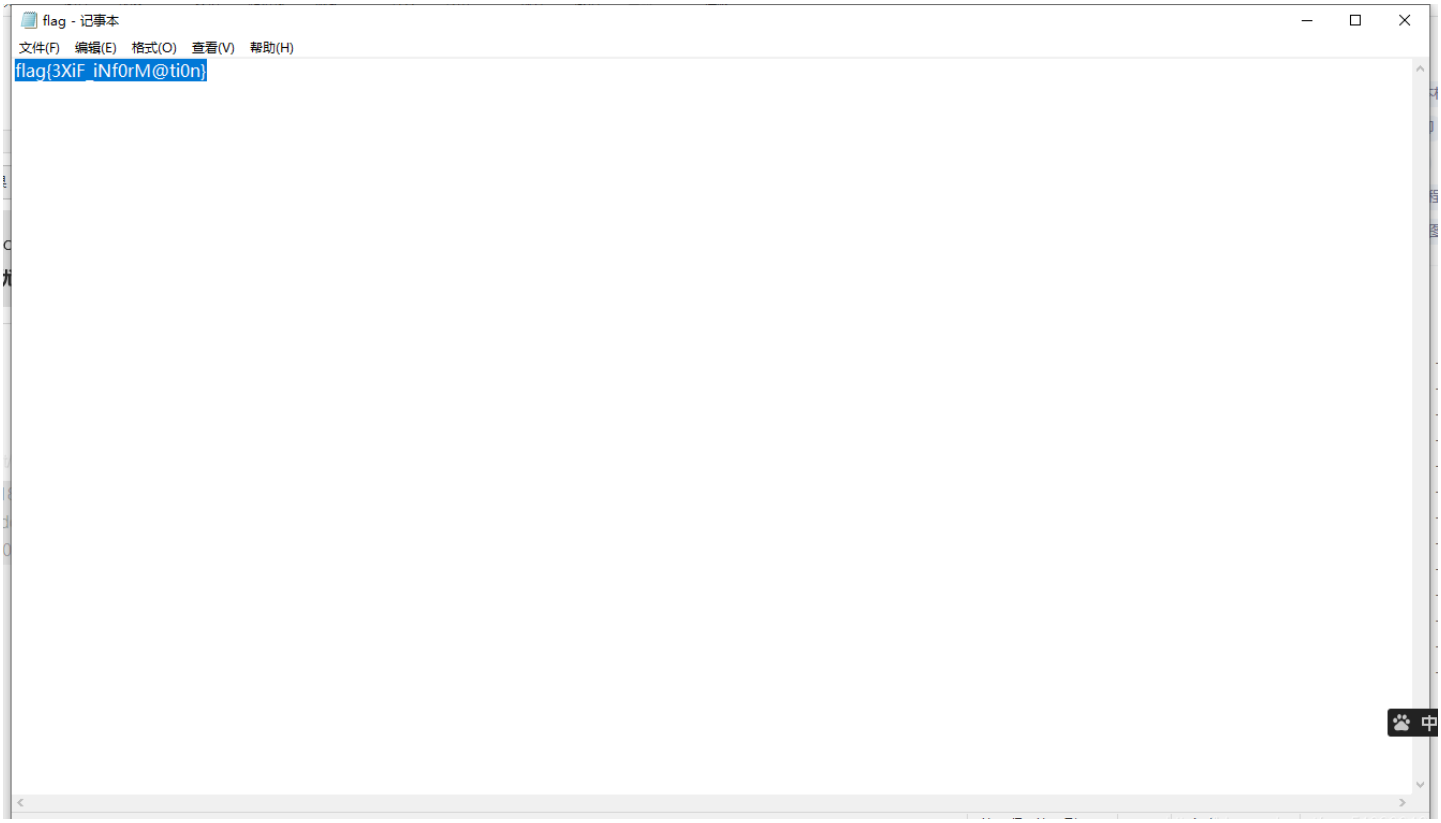



成功了，然后怎么获得密码又没思路了。。只好到此为止百度一下大佬。




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：


输密码解压就行了




## 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