BUUCTF笔记之Misc系列部分WriteUp（一）

原创

KogRow 于 2021-05-24 19:27:22 发布 504 收藏
分类专栏： CTF 杂项 文章标签： 杂项 CTF

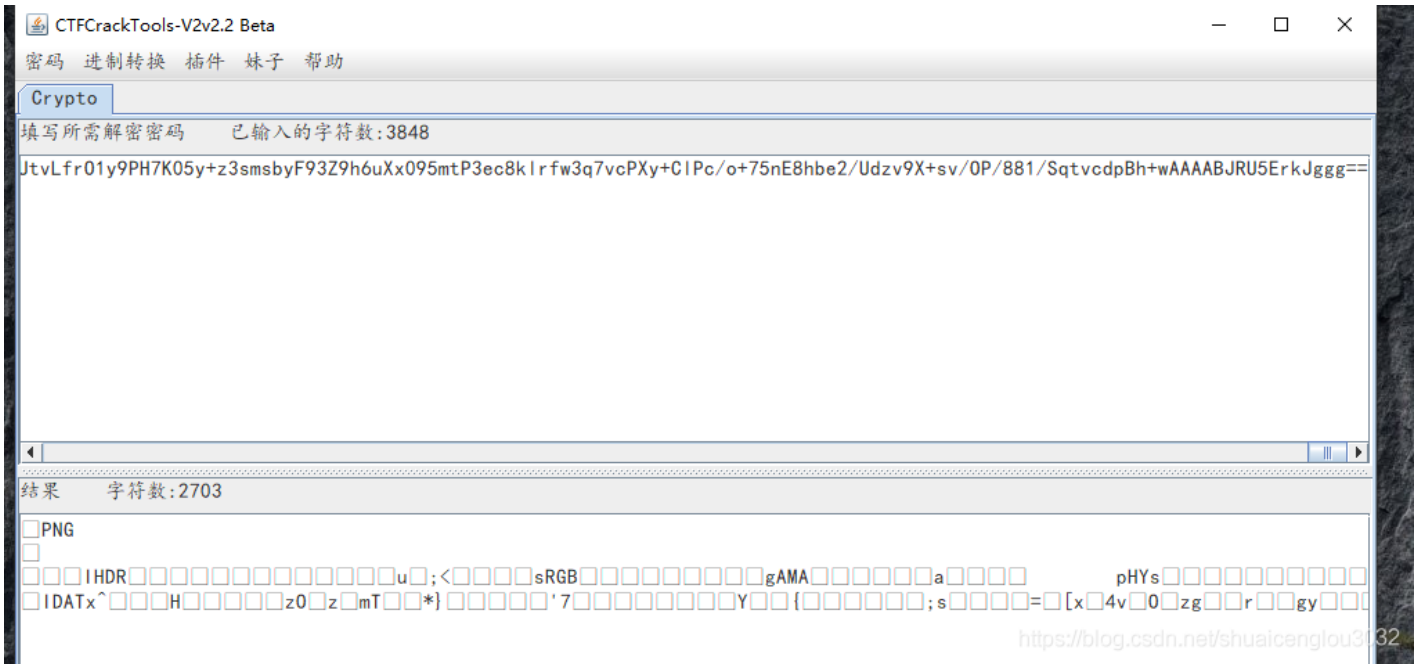
话说misc系列可以说是调剂放松了，web和crypto做吐了，就来做点简单的misc放松一下。

1.N种方法解决

乍一看以为真是个exe，我还拖进IDA看了一波，结果还是吃了没见识的亏，后来IDA无果，拖进winhex看发现是一个图片文件。。。

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	64	61	74	61	3A	69	6D	61	67	65	2F	6A	70	67	3B	62	data:image/jpg;b
00000010	61	73	65	36	34	2C	69	56	42	4F	52	77	30	4B	47	67	ase64,iVBORw0KGg
00000020	6F	41	41	41	41	4E	53	55	68	45	55	67	41	41	41	49	oAAAANSUhEUgAAAI
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	19hwPCDcrMJ9m7/7
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	Hbf9rXO3P4lLvYPc
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

重命名为jpg打开无果，发现文件头后面有个base64，看看文件末尾有等于号，那把中间这一大坨拿出来解码试试：



解码出来提示是png了，那把它解码之后的数据转成图片：

扫码得到flag。

2.大白

根据提示和大佬的wp得知是修改了文件的高度，因此还原文件高度就行。

这里把1图片用winhex打开：

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
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	01	00	08	06	00	00	00	6D	7C	71	S m|q
00000020	35	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	5 sRGB ®Î é
00000030	00	04	67	41	4D	41	00	00	B1	8F	0B	FC	61	05	00	00	gAMA ± üa
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	+ ÿ¥IDATx^ì½
00000060	A0	A5	57	59	EE	FF	EE	BE	4F	9B	DE	93	4C	7A	0F	84	¥WYîÿî¾O›Þ“Lz „
00000070	24	24	60	0C	04	A5	2B	20	45	10	10	BB	88	8A	A8	57	$$` ¥+ E »ˆŠ¨W
00000080	BD	FC	EF	BD	7A	F5	5A	AE	7A	BD	5E	CB	BD	2A	62	05	½üï½zõZ®z½^Ë½*b
00000090	04	69	52	04	E9	01	42	48	48	42	7A	EF	7D	52	A6	CF	iR é BHHBzï}R¦Ï

这里放一下PNG的文件头格式：

PNG图像格式文件由文件署名和数据块(chunk)组成,8字节的文件头标记该文件属于PNG:89 50 4E 47 0D 0A 1A 0A

文件署名之后就是文件头数据块，格式如下：

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，组成结构如下：

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84：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)

根据这个我们查看题目给的图片的IHDR：

00 00 02 A7 00 00 01 00就是图像的宽度和高度。

这里把高度修改成和宽度一样看看：

00 00 02 A7 00 00 02 A7 成功拿到flag

3.你竟然赶我走

这题很简单，一般的图片可以有以下套路：

1.先上winhex，搜索一下flag，看看十六进制数据有没有什么异常或者提示。

2.然后stego看一波。

3.要是没有，binwalk分析一波。

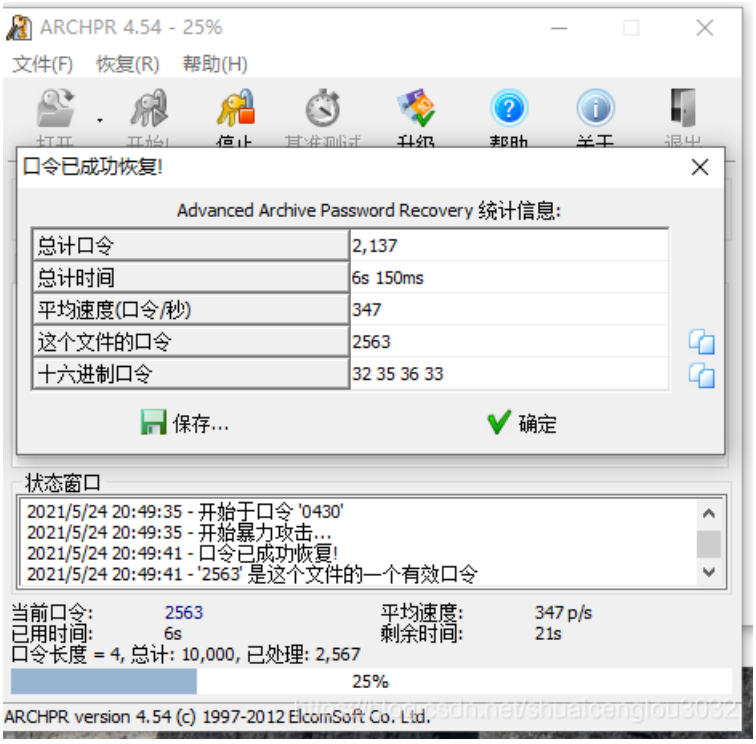
如果是二维码类型的图片可能还需要考虑二维码修复等等，一般就先上这三件套。

这题也一样，winhex打开，search--->find text直接拿到flag:

```
40 05 14 51 40 05 14 51  40 1F FF D9 2D 2D 2D A1  @  Q@  Q@ ÿÙ---¡
B7 66 6C 61 67 20 49 53  20 66 6C 61 67 7B 73 74  ·flag IS flag{st
65 67 6F 5F 69 73 5F 73  30 5F 62 6F 72 31 69 6E  ego_is_s0_bor1in
67 7D                                             g}
```

4.基础破解

根据提示这个压缩包是4位数字密码加密。爆破得到解压密码2563：



打开得到字符串ZmxhZ3s3MDM1NDMwMGE1MTAwYmE3ODA2ODgwNTY2MWI5M2E1Y30=

base64解码得到flag{70354300a5100ba78068805661b93a5c}

5.乌镇峰会种图

这题同上面的《你竟然赶我走》

最后flag:

```
06 5C 1E 8A 38 15 16 C5  DD D3 1F 4A D1 20 1F 9F  \ 8 ÅÝÓ JÑ
7A 29 DE 5A FB D1 4F 51  1F FF D9 0D 0A 66 6C 61  z)ÞZûÑOQ ÿÙ fla
67 7B 39 37 33 31 34 65  37 38 36 34 61 38 66 36  g{97314e7864a8f6
32 36 32 37 62 32 36 66  33 66 39 39 38 63 33 37  2627b26f3f998c37
66 31 7D                                          f1}
```

6.LSB

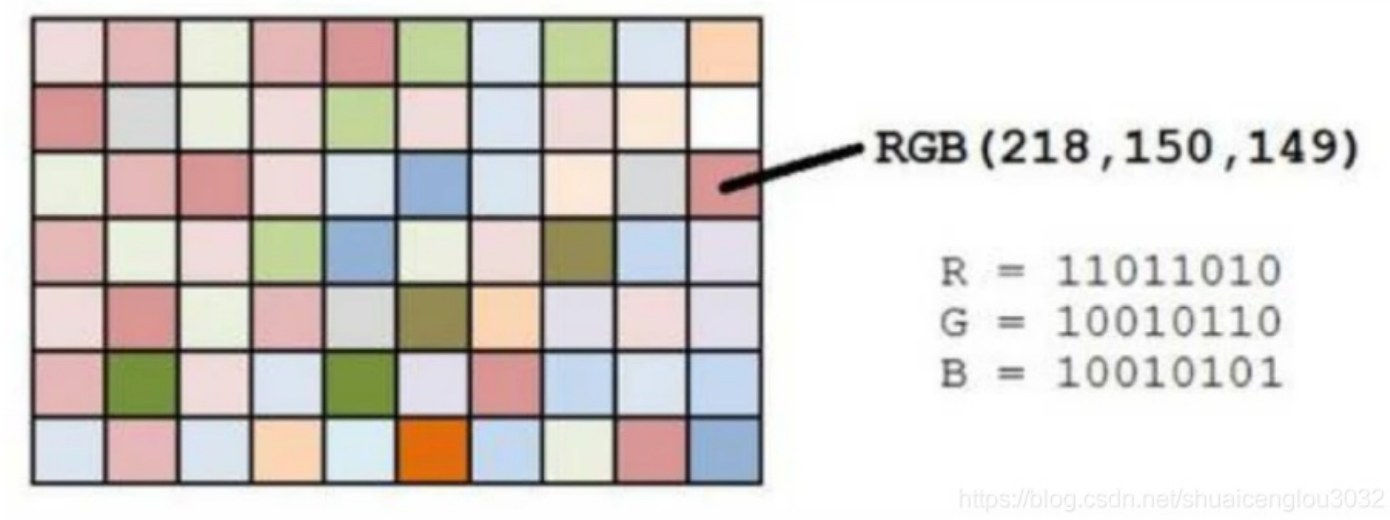
题目给的提示很明确，LSB隐写。

然后这里记录一下怎么解LSB隐写的题

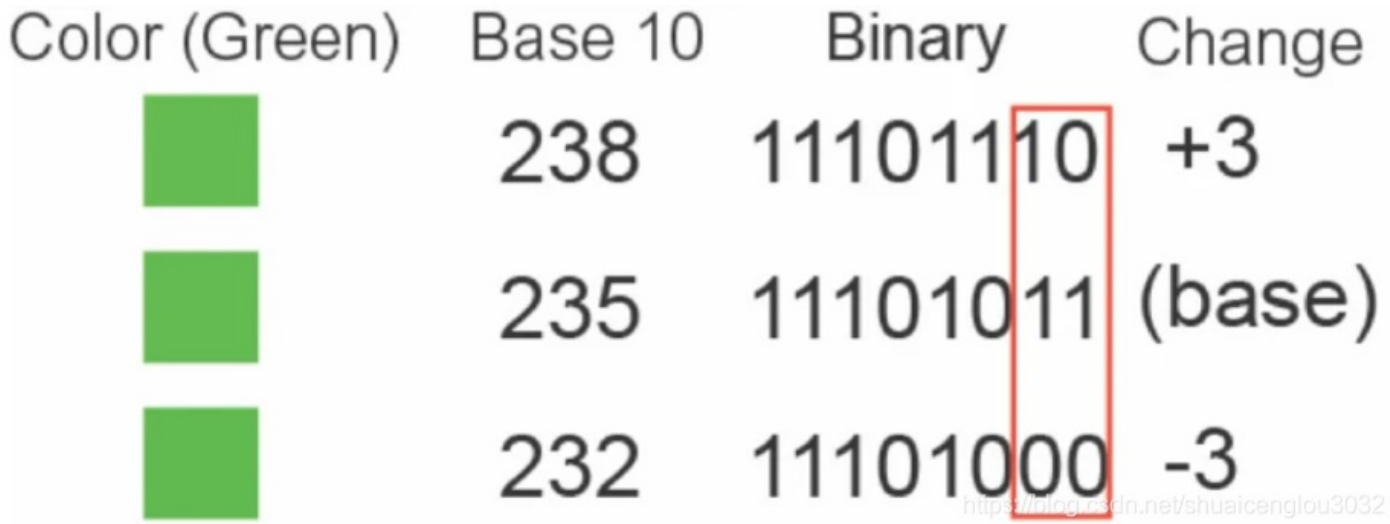
以下文字来自Lsb图片隐写

LSB全称为 least significant bit，是最低有效位的意思。Lsb图片隐写是基于lsb算法的一种图片隐写术

只有在无损压缩或者无压缩的图片（BMP）上实现lsb隐写。如果图像是jpg图片的话，就没法使用lsb隐写了，原因是jpg图片对像数进行了有损压缩，我们修改的信息就可能会在压缩的过程中被破坏。而png图片虽然也有压缩，但却是无损压缩，这样我们修改的信息也就能得到正确的表达，不至于丢失。BMP的图片也是一样，是没有经过压缩的。BMP图片一般是特别的大的，因为BMP把所有的像数都按原样储存，没有进行压缩。png图片中的图像像数一般是由RGB三原色（红绿蓝）组成，每一种颜色占用8位，取值范围为0x00~0xFF，即有256种颜色，一共包含了256的3次方的颜色，即16777216种颜色。而人类的眼睛可以区分约1000万种不同的颜色，这就意味着人类的眼睛无法区分余下的颜色大约有677万种。

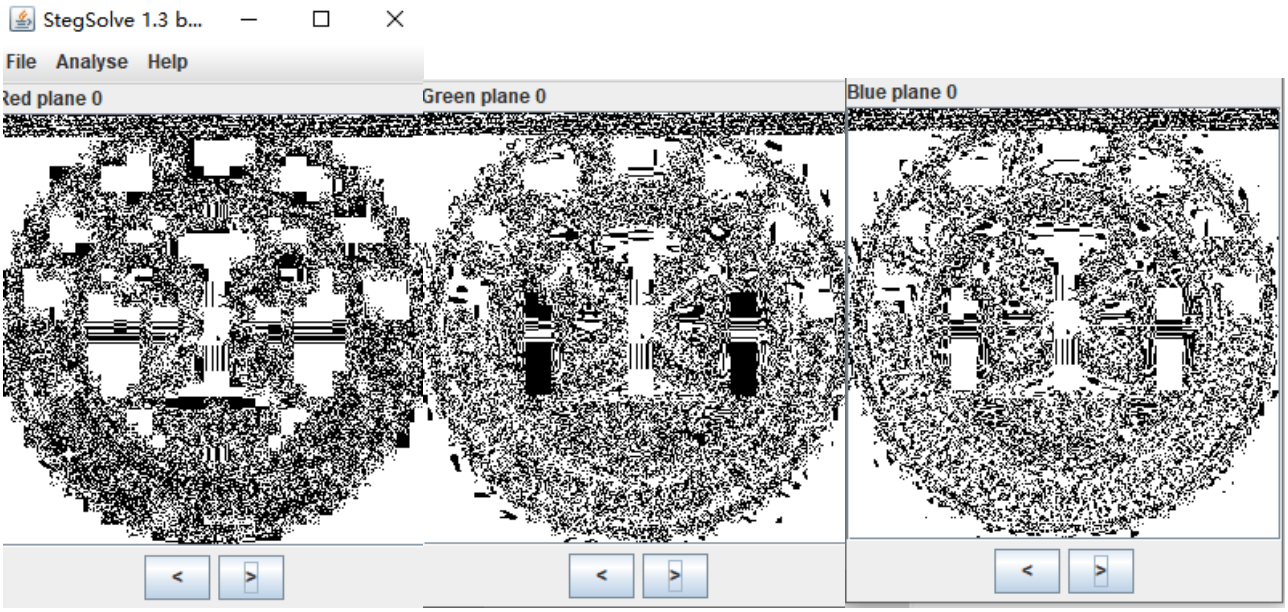


LSB隐写就是修改RGB颜色分量的最低二进制位也就是最低有效位（LSB），而人类的眼睛不会注意到这前后的变化，每个像素可以携带3比特的信息，为什么是3比特，一个像素有RGB三个分量，每个分量能表示1个比特的信息，那就是3比特。

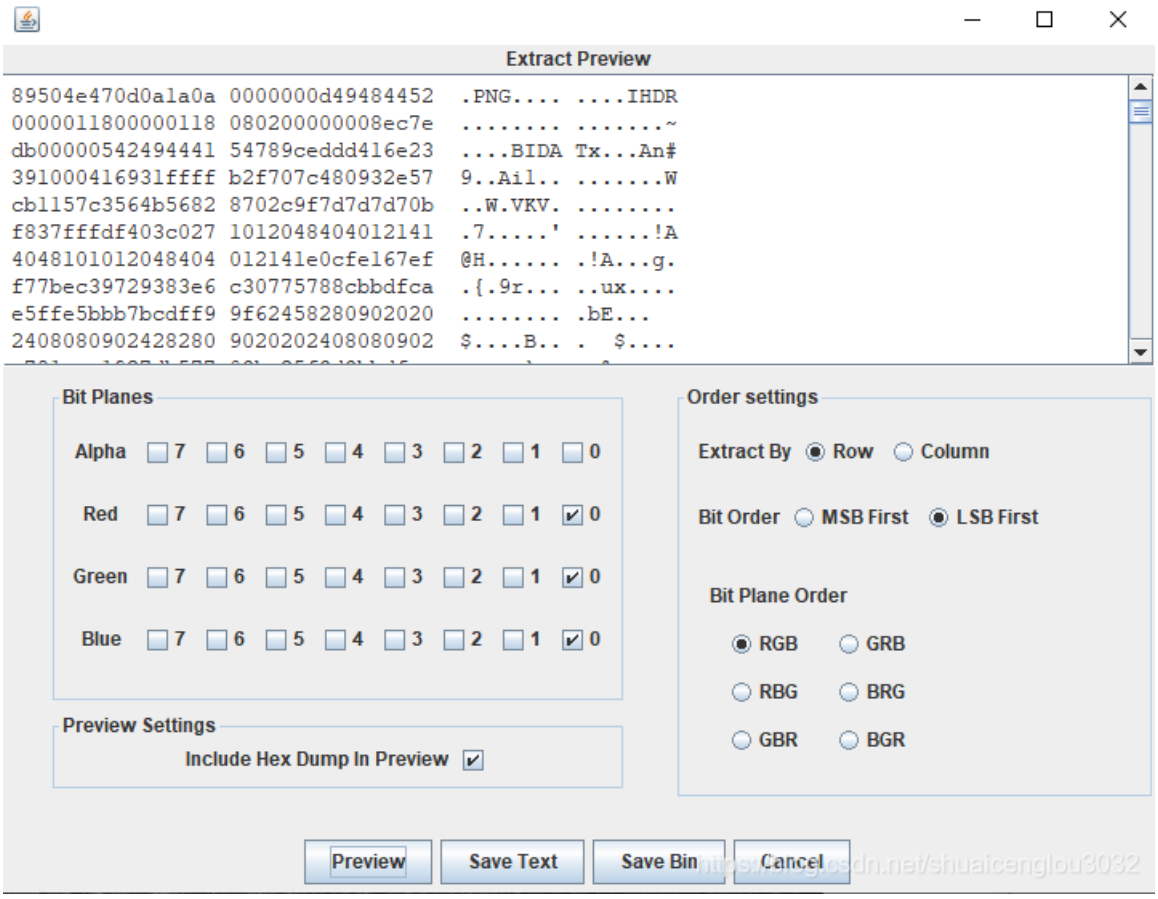


上图我们可以看到，十进制的235表示的是绿色，我们修改了在二进制中的最低位，但是颜色看起来依旧没有变化。我们就可以修改最低位中的信息，实现信息的隐写。修改最低有效位的信息的算法就叫做lsb加密算法，提取最低有效位信息的算法叫做lsb解密算法。

直接上stego:



RGB三个颜色的0通道上都有一条横线，所以选中看看：

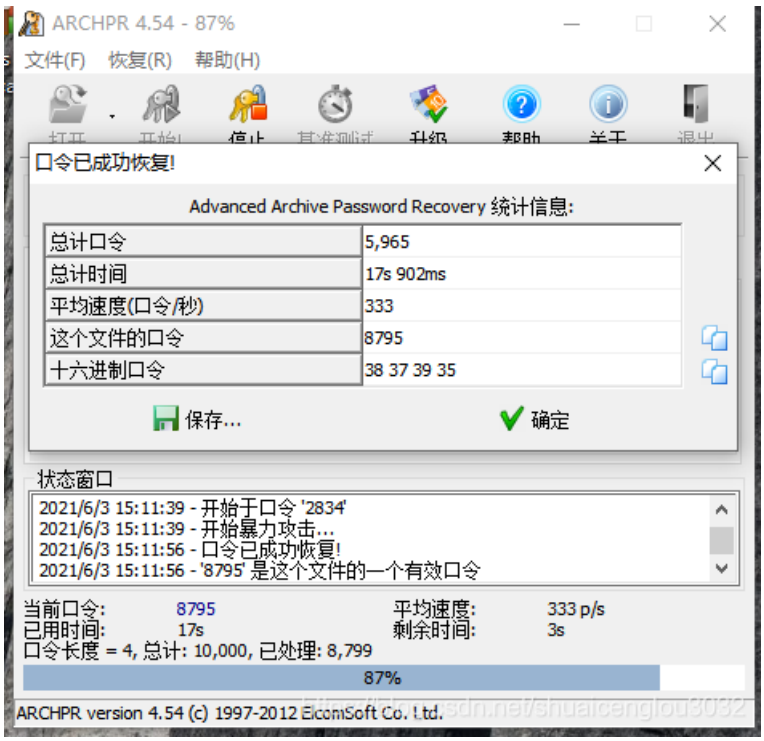


发现是把图片隐写进了图片。save bin之后得到一张二维码：

扫码得到flag：

7.rar

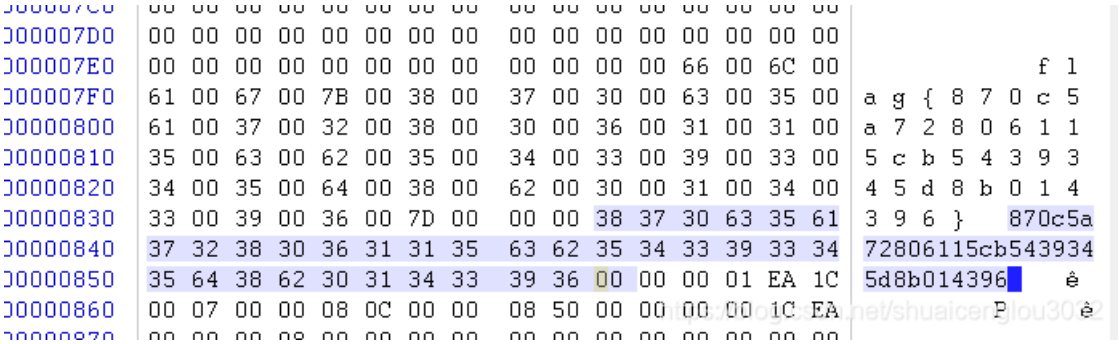
一样的，爆破得到口令8795：



解压就得到flag。

8.文件中的秘密

winhex打开，得到flag：



00007D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00007E0	00	00	00	00	00	00	00	00	00	00	00	00	66	00	6C	00	f l
00007F0	61	00	67	00	7B	00	38	00	37	00	30	00	63	00	35	00	a g { 8 7 0 c 5
00000800	61	00	37	00	32	00	38	00	30	00	36	00	31	00	31	00	a 7 2 8 0 6 1 1
00000810	35	00	63	00	62	00	35	00	34	00	33	00	39	00	33	00	5 c b 5 4 3 9 3
00000820	34	00	35	00	64	00	38	00	62	00	30	00	31	00	34	00	4 5 d 8 b 0 1 4
00000830	33	00	39	00	36	00	7D	00	00	00	38	37	30	63	35	61	3 9 6 } 870c5a
00000840	37	32	38	30	36	31	31	35	63	62	35	34	33	39	33	34	72806115cb543934
00000850	35	64	38	62	30	31	34	33	39	36	00	00	00	01	EA	1C	5d8b014396 ê
00000860	00	07	00	00	08	0C	00	00	08	50	00	00	00	00	1C	EA	P ê

9.zip伪加密

这些都是很基础的题，很适合入门，现在CTF赛事基本不会有这种简单题了。

```
java -jar ZipCenOp.jar r 1.zip
```

如此操作之后可以直接打开压缩包得到flag{Adm1N-B2G-kU-SZIP}

另外还有一种办法，将该压缩包用winhex打开，修改加密标志位：

ZIP文件的文件头如下：

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	50	4B	03	04	14	00	09	00	08	00	50	A3	A5	4A	21	38
00000010	76	65	19	00	00	00	17	00	00	00	08	00	00	00	66	6C
00000020	61	67	2E	74	78	74	4B	CB	49	4C	AF	76	4C	C9	35	F4

这里的504B0304是ZIP的头文件标记。

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	50	4B	03	04	14	00	09	00	08	00	50	A3	A5	4A	21	38
00000010	76	65	19	00	00	00	17	00	00	00	08	00	00	00	66	6C
00000020	61	67	2E	74	78	74	4B	CB	49	4C	AF	76	4C	C9	35	F4
00000030	D3	75	32	72	D7	CD	0E	D5	0D	8E	F2	0C	A8	05	00	50
00000040	4B	01	02	1F	00	14	00	09	00	08	00	50	A3	A5	4A	21

1400是解压文件所需pkware版本。

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	50	4B	03	04	14	00	09	00	08	00	50	A3	A5	4A	21	38
00000010	76	65	19	00	00	00	17	00	00	00	08	00	00	00	66	6C
00000020	61	67	2E	74	78	74	4B	CB	49	4C	AF	76	4C	C9	35	F4
00000030	D3	75	32	72	D7	CD	0E	D5	0D	8E	F2	0C	A8	05	00	50
00000040	4B	01	02	1F	00	14	00	09	00	08	00	50	A3	A5	4A	21

0900是全局方式位标记。

上面是ZIP的源文件数据区

下面是ZIP源文件目录区，这个目录区一般紧接着上面的数据区：

```
00000030  D3 75 32 72 D7 CD 0E D5  0D 8E F2 0C A8 05 00 50
00000040  4B 01 02 1F 00 14 00 09  00 08 00 50 A3 A5 4A 21
00000050  38 76 65 19 00 00 00 17  00 00 00 08 00 24 00 00
```

504B0102，是目录中的头文件标记。

后面的1F00是压缩文件使用的pkware版本。

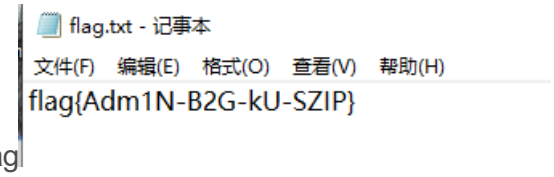
再往后的1400是解压文件所需 pkware 版本。

再往后的0900是全局方式位标记（有无加密，伪加密的关键）。

修改其压缩源文件目录区的全布局方式标记比特值之后即可对文件加密或解密

09改为00即可解密。

00改为09即可加密。



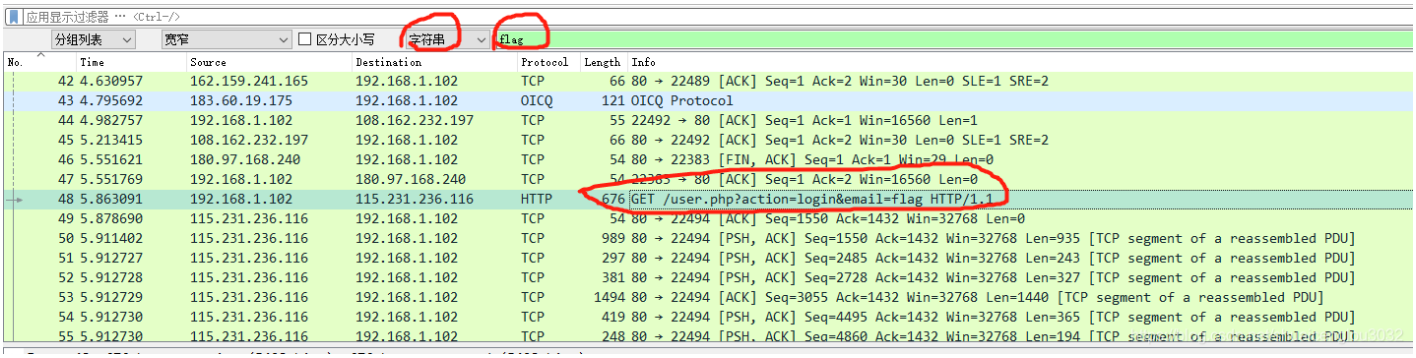
改完就能解压得到flag

10.wireshark

题目给了提示：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)

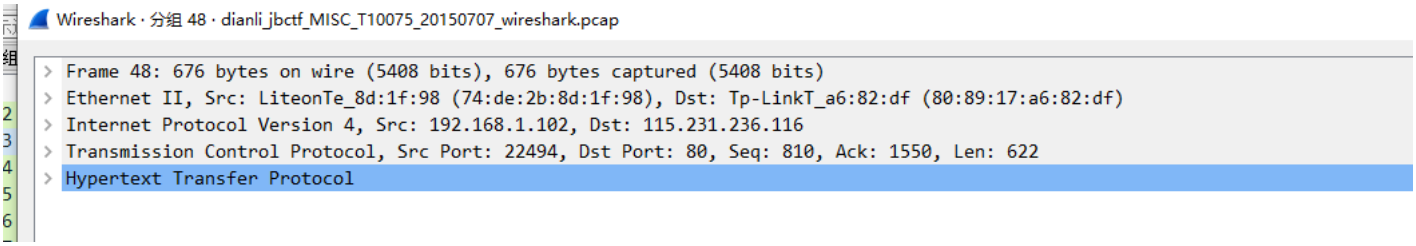
这题是流量分析。恶补一波流量分析知识。

这里用wireshark打开下载的附件，先习惯性搜索一波flag：



记得要搜索字符串，不然会一无所获。

双击这个GET请求看看：



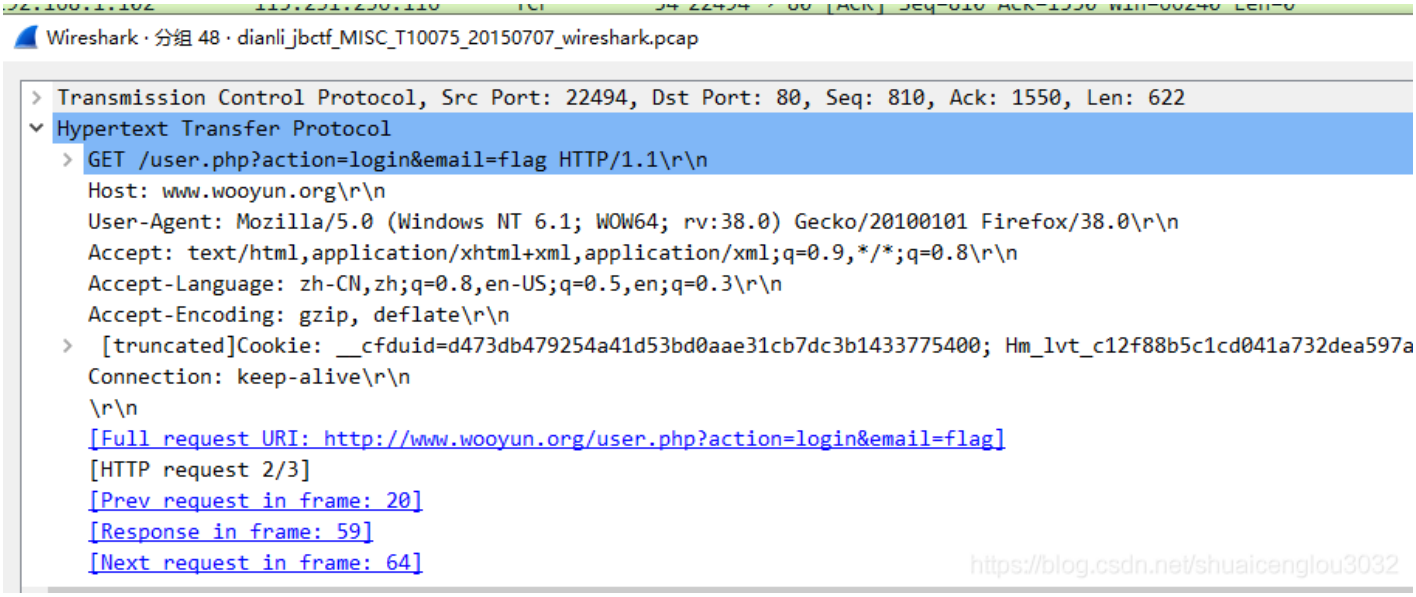
解释一下这里，蓝色这条意思是超文本传输协议，也就是http。

往上一条是传输控制协议，也就是TCP

再往上是网际协议，版本4，也就是IPv4

再往上是数据链路层的MAC。

再往上是Frame，目测是物理层，wireshark把一个包按分层的形式展现出来。先看看HTTP里面有些什么：



没有什么有用的东西，我们直接点追踪流：

```
POST /user.php?action=login&do=login HTTP/1.1
Host: www.wooyun.org
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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=14348
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
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Server: yunjiasu-nginx
CF-RAY: 1fe28d0a63e91c3b-JXG
Content-Encoding: gzip

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-tran
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<meta http-equiv="refresh" content="3; url=/user.php?action=login&email=flag"/>
<title> WooYun.org | ............................... </title>
<meta name="author" content="80sec"/>
<meta name="copyright" content="http://www.wooyun.org/"/>
<meta name="keywords" content=",wooyun,.....,web.....,.....,.....,.....,.....
<meta name="description" content="WooYun.....,
<link href="/css/style.css" rel="stylesheet" type="text/css"/>
```

```
<script src="/js/jquery-1.4.2.min.js" type="text/javascript"></script>
<script type="text/javascript">

$(function(){

 $(".listTable tbody tr").hover(function(){

  $(this).css("background","#EBEBEB");

 },function(){

  $(this).css("background","none");

 });

});

</script>
</head>

<body>

 <div class="banner">
  <h1>WooYun.org</h1>
 </div>

 <div class="nav">
  <ul>
   <li><a href="/index.php">......</a></li>
   <li><a href="/corps/">.....</a></li>
   <li><a href="/whitehats/">.....</a></li>
   <li><a href="/bugs/">.....</a></li>
   <li><a href="/bug/submit">.....</a></li>
   <li><a href="/help">......</a></li>
   <li><a href="/about">......</a></li>
  </ul>
  <p><a href="#"><img src="/images/search.jpg" alt="......" title="....."/></a><input type="text"/></p>
 </div>

 <div class="content" style="height:300px">
  <div class="success">
   <p>.............................</p>
   <p><a href="/user.php?action=login&email=flag">.....................................</a></p>
  </div>
 </div>

 <div class="copyright">
  Copyright &copy; 2010 <a href="#">www.wooyun.org</a> All Rights Reserved.
 </div>

</body>
</HTML>
GET /user.php?action=login&email=flag HTTP/1.1
Host: www.wooyun.org
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: __cfduid=d473db479254a41d53bd0aae31cb7dc3b1433775400; Hm_lvt_c12f88b5c1cd041a732dea597a5ec94c=14348
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Date: Mon, 29 Jun 2015 15:09:13 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Server: yunjiasu-nginx
CF-RAY: 1fe28d1e456a1c3b-JXG
Content-Encoding: gzip

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-tran
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<meta http-equiv="x-ua-compatible" content="ie=7"/>
<title> WooYun.org | ..... </title>
<meta name="author" content="80sec"/>
<meta name="copyright" content="http://www.wooyun.org/"/>
<meta name="keywords" content=",wooyun,.....,web.....,.....,.....,.....,.....
<meta name="description" content="WooYun.....,
<link rel="icon" href="/favicon.ico" sizes="32x32" />
<link href="/css/style.css?v=201501291909" rel="stylesheet" type="text/css"/>
<script src="/js/jquery-1.4.2.min.js" type="text/javascript"></script>
</head>

<body>

<style>
#myBugListTab { position:relative; display:inline; border:none }
#myBugList { position:absolute; display:none; margin-left:309px; * margin-left:-60px; * margin-top:18px ; b
#myBugList li { text-align:left }
</style>
<script type="text/javascript">
$(document).ready(function(){

 if ( $("#__cz_push_d_object_box__") ) {
  $("script[src^='http://cip4.czpush.com/']").attr("src"," ").remove();
  $("#__cz_push_d_object_box__").empty().remove();
  $("a[id^='__czUnion_a']").attr("href","#").remove();
 }

 if ( $("#ooDiv") ) {
  $("#ooDiv").empty().parent("div").remove();
 }

 $("#myBugListTab").toggle(
  function(){
   $("#myBugList").css("display","block");
  },
  function(){
   $("#myBugList").css("display","none");
  }
 );

 if ( $(window).scrollTop() > 120 ) {
  $("#back-to-top").fadeIn(300);
```

```
 } else {
  $("#back-to-top").fadeOut(300);
 }

 $(window).scroll(function(){
  if ( $(window).scrollTop() > 120 ) {
   $("#back-to-top").fadeIn(300);
  } else {
   $("#back-to-top").fadeOut(300);
  }
 });

 $("#back-to-top a").click(function() {
  $('body,html').animate({scrollTop:0},300);
  return false;
 });

 $("#go-to-comment a").click(function() {
  var t = $("#replys").offset().top - 52;
  $('body,html').animate({scrollTop:t},300);
  return false;
 });

});

function gofeedback(){
 var bugid=$("#fbid").val();
 if(bugid){
  var url="/feedback.php?bugid="+bugid;
 }else{
  var url="/feedback.php"
 }
 window.open(url);
}
</script>

 <div class="go-to-wrapper">
  <ul class="go-to">
      <li id="go-to-comment" title="............."><a href="#">.............</a></li>
      <li id="go-to-feedback" title="............."><a href="javascript:void(0)" onclick="gofeedback()">....
      <li id="back-to-top" title="............."><a href="#">.............</a></li>
  </ul>
 </div>
 <div class="banner">
  <div class="logo">
  <h1>WooYun.org</h1>
  <div class="weibo"><iframe width="136" height="24" frameborder="0" allowtransparency="true" marginwidth="
  </div>
  <div class="wxewm">
   <a class="ewmthumb" href="javascript:void(0)"><span><img src="/images/ewm.jpg"width="220" border="0"></s
  </div>
  </div>

    <div class="login">
     <a href="/user.php?action=login">......</a> | <a href="/user.php?action=register" class="reg">......</
    </div>
    </div>

 <div class="nav" id="nav_sc">
  <ul>
```

```
   <li><a href="/index.php">......</a></li>
   <li><a href="/corps/">.....</a></li>
   <li><a href="/whitehats/">.....</a></li>
   <li><a href="/top/">.....</a></li>
            <li><a href="/teams/">.....</a></li>
            <li><a href="/bugs/">.....</a></li>
   <li class="new"><a href="/bug/submit">.....</a></li>
   <!--li><a href="/corp_actions">.....</a></li-->
   <!--<li><a href="/security_center.php#nav_sc">.....</a></li>-->
   <li><a href="http://summit.wooyun.org" target="_blank" style="color:rgb(246,172,110);font-size:14px;font
   <!--li><a href="/job/">.....</a></li-->
   <li><a href="http://job.wooyun.org" target="_blank">.....</a></li>
      <li><a href="http://drops.wooyun.org" target="_blank">.....</a></li>
   <li><a href="/notice/">.....</a></li>
  </ul>
        <form action="/searchbug.php" method="post" id="searchbox">
            <input type="text" name="q" id="search_input" />
            <input type="submit" value="....." id="search_button" />
        </form>
 </div>

 <div class="bread">
  <div style="float:left">.....<a href="/index.php">WooYun</a> >> <a href="#">.....</a></d
  </div>

<form action="user.php?action=login&do=login" method="POST">
 <div class="content">

  <table class="formTable">
   <tbody>
    <tr>
     <th width="100">E-mail...</th>
     <td><input type="text" name="email" value="flag" style="width:150px" /></td>
    </tr>
    <tr>
     <th>.....</th>
     <td><input type="password" name="password" style="width:150px" />    <a href="/use
    </tr>
    <tr>
    <tr>
     <th>.....</th>
     <td><input type="text" name="captcha" style="width:80px" /> <img onclick="this.src='/captcha.php?
    </tr>
    <tr>
     <th> </th>
     <td><input type="submit" value="....."/></td>
     <td><input type="hidden" value="123456"/></td>
    </tr>
   </tbody>
  </table>

 </div>
</form>

 <div id="footer">
       <span class="copyright fleft">
      Copyright &copy; 2010 - 2015 <a href="#">wooyun.org</a>, All Rights Reserved
      <a href="http://www.miibeian.gov.cn/">...ICP...12001400...-1</a>
      <!--a href="http://sae.sina.com.cn" target="_blank"><img src="/images/sae_bottom_logo.png" title="Pow
```

```
     </span>
        <span class="other fright">
            <a href="/impression">............</a>
            .. <a href="/lawer">............</a>
            .. <a href="/contactus">............</a>
            .. <a href="/help">......</a>
            .. <a href="/about">......</a>
        </span>
    </div>
 <script type="text/javascript">
 var _bdhmProtocol = (("https:" == document.location.protocol) ? " https://" : " http://");
 document.write(unescape("%3Cscript src='" + _bdhmProtocol + "hm.baidu.com/h.js%3Fc12f88b5c1cd041a732dea597
 </script>
    <script type="text/javascript" id="bdshare_js" data="type=button" ></script>
    <script type="text/javascript" id="bdshell_js"></script>
    <script type="text/javascript">
        document.getElementById("bdshell_js").src = "http://bdimg.share.baidu.com/static/js/shell_v2.js?cdn

        if (top.location !== self.location) top.location=self.location;
    </script>
</body>
</html>GET /captcha.php HTTP/1.1
Host: www.wooyun.org
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
Accept: image/png,image/*;q=0.8,*/*;q=0.5
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&email=flag
Cookie: __cfduid=d473db479254a41d53bd0aae31cb7dc3b1433775400; Hm_lvt_c12f88b5c1cd041a732dea597a5ec94c=14348
Connection: keep-alive

HTTP/1.1 200 OK
Date: Mon, 29 Jun 2015 15:09:13 GMT
Content-Type: image/png
Transfer-Encoding: chunked
Connection: keep-alive
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: private, no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0, max-age=0
Pragma: no-cache
Server: yunjiasu-nginx
CF-RAY: 1fe28d1ee5761c3b-JXG

.PNG
.
...
IHDR...A..........$K...+IDATH.eWKk.M..{_..I.....n.5...!..RAA]...(*.. .."7.J\.d&3.{].....k.}..=US]........=
..A..}]..sJ).... .(..9!....{~...+W.t]..o....t6..c....fm..c....
.*...s..C)]....]+..{O)..|..L&.!D.e[[[...R..4M....v.u]..m.uUUM..0...e.9..+..J....BH.u....1..!...i.8.Rz.9....
...%I.....q[k.0d.!>....9'...Z)..A..J)!.....|...A.y.....[].!.<.. h..,.......(B48)....!........L..9.......T..
.9h9....QBkm.......z.......q|qq1..AnB.../....7o..dY...GB........M..]....Xi.&.....QJeY..q.$..&MS.X].UU1...4M
.])eY.PgL*JiY..9J)C....sBH..q.3..........u].&<.....16.a.\...h0..s..
..P.q. ....Z.q$.X...BP..=.'Ib...3.W..r.. ..0..sa..}.....j.Q.|...N..}........>x..h......<T.#.....=D31..1@c..
8.......`......8...Z.%.
.l.kY..t.E..M.0$
.E&.:...1..R..k.....4...r....%...D.M.,..A.Qr..........{.W..SJ....hP3J..E...X...Sp&._....... ..{.wwwQ..,W...
~.-..(.`......H...N.Q0.Z.$I.+...V...@.g.]..6..S..D.....IEND.B`.
```

这里已经可以看见password了，就在第一个请求包里：

```
POST /user.php?action=login&do=login HTTP/1.1
Host: www.wooyun.org
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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=14348
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

email=flag&password=ffb7567a1d4f4abdffdb54e022f8facd&captcha=BYUG
```

包上flag{}就可以。

11.qr

扫码得到flag.

12.ningen

人类的科学日益发展，对自然的研究依然无法满足，传闻日本科学家秋明重组了基因序列，造出了名为ningen的超自然生物。某天特工小明偶然截获了日本与俄罗斯的秘密通信，文件就是一张ningen的特写，小明通过社工，知道了秋明特别讨厌中国的六位银行密码，喜欢四位数。你能找出黑暗科学家秋明的秘密么？

下载下来是一张图：

binwalk分析一波。

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0×0             JPEG image data, JFIF standard 1.01
38689         0×9721          Zip archive data, encrypted at least v2.0 to extract,
size: 50, uncompressed size: 38, name: ningen.txt
38871         0×97D7          End of Zip archive, footer length: 22
```

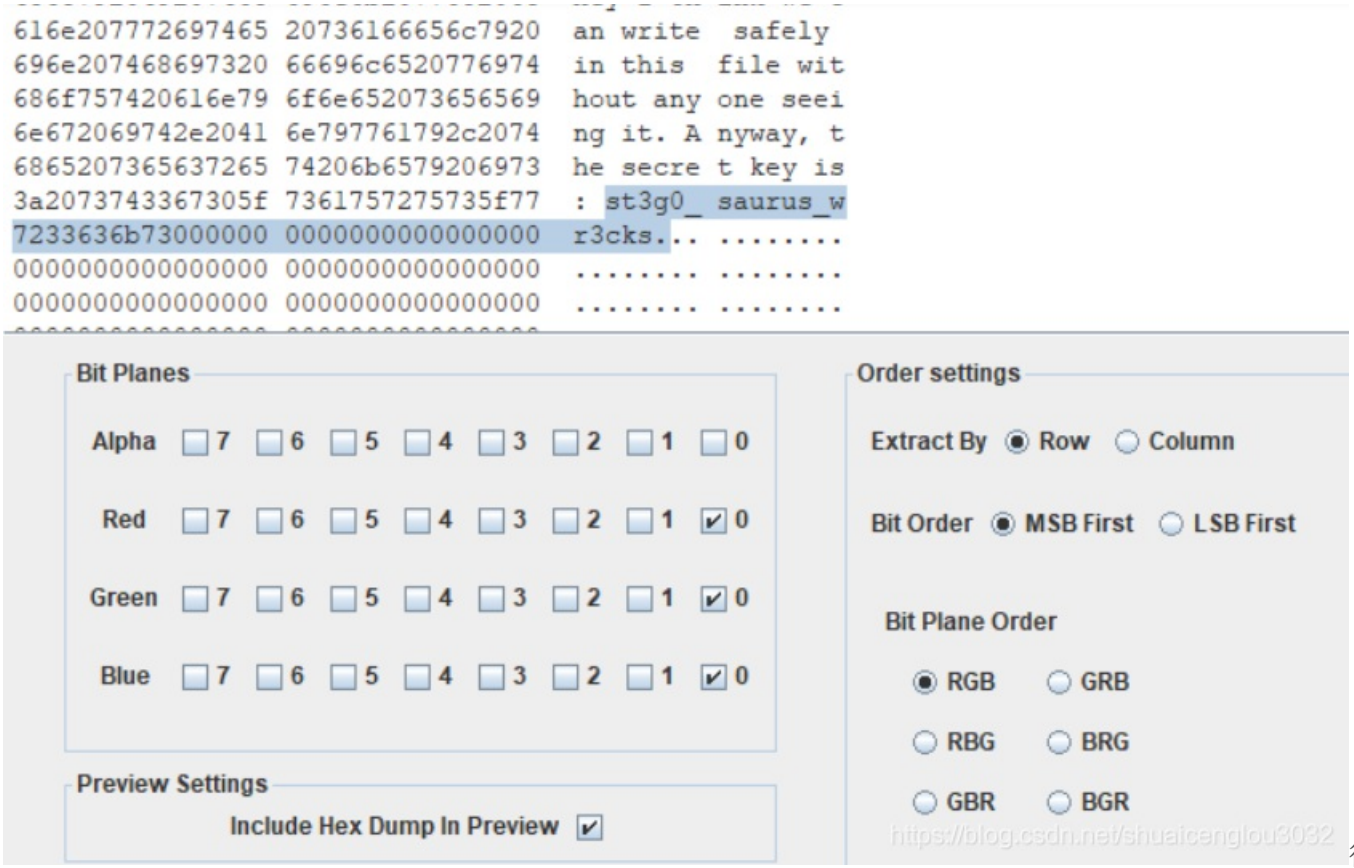
发现一个zip包，用foremost把它分离出来，爆破zip密码得到8368：

解压得到flag{b025fc9ca797a67d2103bfbc407a6d5f}

13.镜子里面的世界

下载下来文件名是steg.png。直接上steg

查看RGB的0通道发现有问题：



得到flag。

14.[NPUCTF2020]签到

这题就是纯粹难为人了，西北工业大学信息安全协会脑洞大开啊。

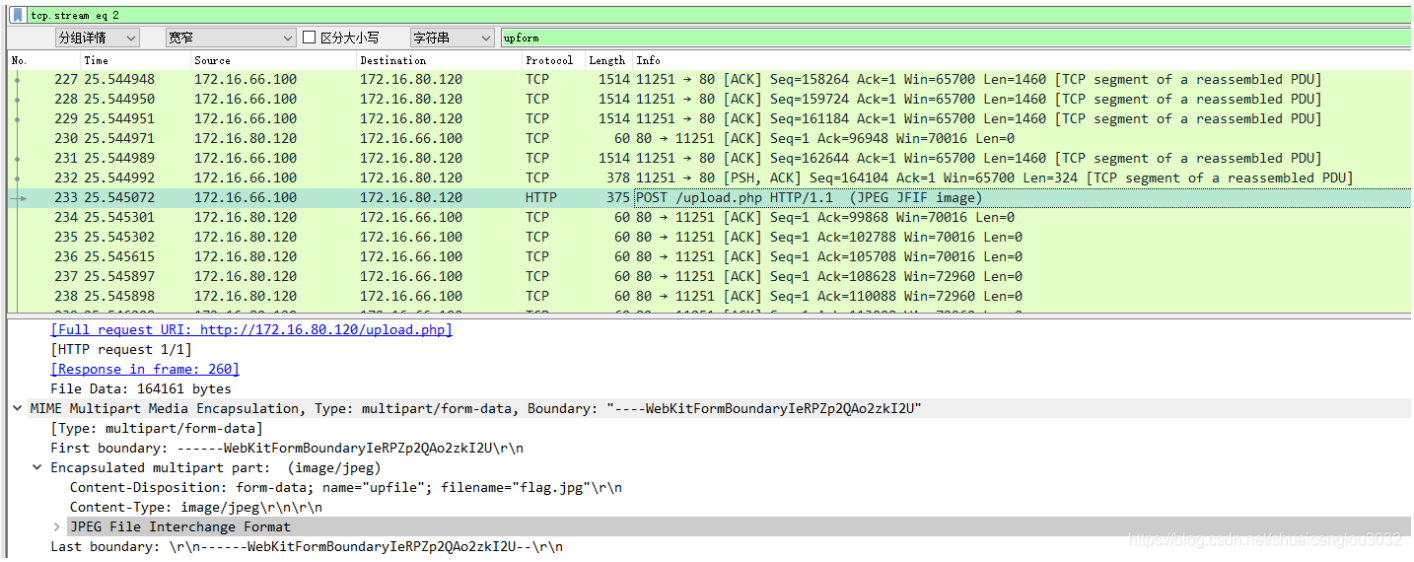
这题要用minecraft1.15.2（中文名我的世界，一个沙盒游戏）打开。打开之后根据闪烁时间长短转换为0和1，常亮为1，短亮为0.

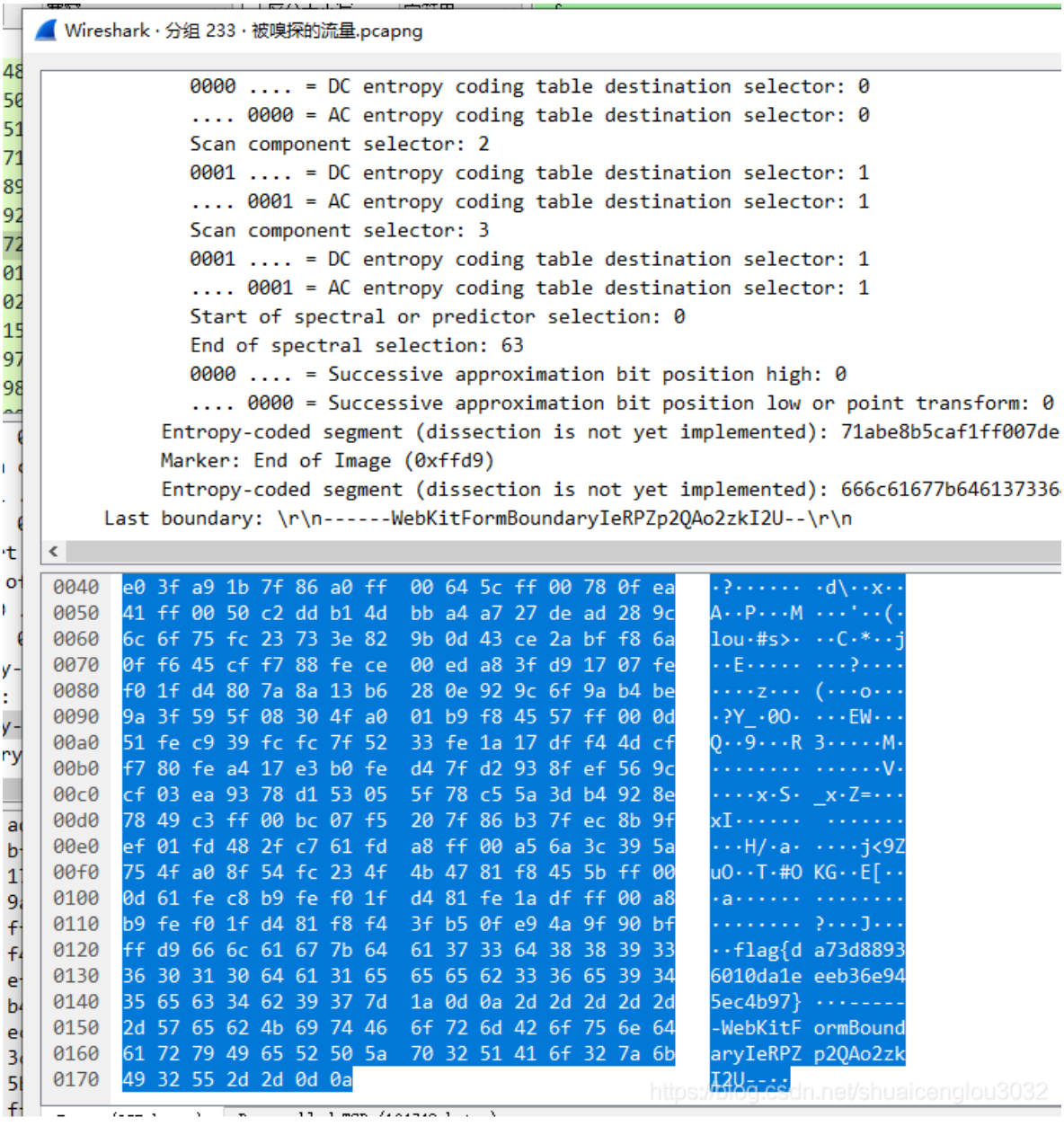
得到一串二进制。二进制序列八位为一组转ascii得到字符串：9a9.

9a9转成32位大写md5就是flag.

flag{8F108D05D23041B5866F9CB2FF109661}

15.被嗅探的流量


tcp.stream eq 2
分组详情
宽窄
区分大小写
字符串
upform
No. Time Source Destination Protocol Length Info
227 25.544948 172.16.66.100 172.16.80.120 TCP 1514 11251 → 80 [ACK] Seq=158264 Ack=1 Win=65700 Len=1460 [TCP segment of a reassembled PDU]
228 25.544950 172.16.66.100 172.16.80.120 TCP 1514 11251 → 80 [ACK] Seq=159724 Ack=1 Win=65700 Len=1460 [TCP segment of a reassembled PDU]
229 25.544951 172.16.66.100 172.16.80.120 TCP 1514 11251 → 80 [ACK] Seq=161184 Ack=1 Win=65700 Len=1460 [TCP segment of a reassembled PDU]
230 25.544971 172.16.80.120 172.16.66.100 TCP 60 80 → 11251 [ACK] Seq=1 Ack=96948 Win=70016 Len=0
231 25.544989 172.16.66.100 172.16.80.120 TCP 1514 11251 → 80 [ACK] Seq=162644 Ack=1 Win=65700 Len=1460 [TCP segment of a reassembled PDU]
232 25.544992 172.16.66.100 172.16.80.120 TCP 378 11251 → 80 [PSH, ACK] Seq=164104 Ack=1 Win=65700 Len=324 [TCP segment of a reassembled PDU]
233 25.545072 172.16.66.100 172.16.80.120 HTTP 375 POST /upload.php HTTP/1.1 (JPEG JFIF image)
234 25.545301 172.16.80.120 172.16.66.100 TCP 60 80 → 11251 [ACK] Seq=1 Ack=99868 Win=70016 Len=0
235 25.545302 172.16.80.120 172.16.66.100 TCP 60 80 → 11251 [ACK] Seq=1 Ack=102788 Win=70016 Len=0
236 25.545615 172.16.80.120 172.16.66.100 TCP 60 80 → 11251 [ACK] Seq=1 Ack=105708 Win=70016 Len=0
237 25.545897 172.16.80.120 172.16.66.100 TCP 60 80 → 11251 [ACK] Seq=1 Ack=108628 Win=72960 Len=0
238 25.545898 172.16.80.120 172.16.66.100 TCP 60 80 → 11251 [ACK] Seq=1 Ack=110088 Win=72960 Len=0
[Full request URI: http://172.16.80.120/upload.php]
[HTTP request 1/1]
[Response in frame: 260]
File Data: 164161 bytes
MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "----WebKitFormBoundaryIeRPZp2QAo2zkI2U"
[Type: multipart/form-data]
First boundary: ------WebKitFormBoundaryIeRPZp2QAo2zkI2U\r\n
Encapsulated multipart part: (image/jpeg)
Content-Disposition: form-data; name="upfile"; filename="flag.jpg"\r\n
Content-Type: image/jpeg\r\n\r\n
JPEG File Interchange Format
Last boundary: \r\n------WebKitFormBoundaryIeRPZp2QAo2zkI2U--\r\n


Wireshark · 分组 233 · 被嗅探的流量.pcapng
0000 .... = DC entropy coding table destination selector: 0
.... 0000 = AC entropy coding table destination selector: 0
Scan component selector: 2
0001 .... = DC entropy coding table destination selector: 1
.... 0001 = AC entropy coding table destination selector: 1
Scan component selector: 3
0001 .... = DC entropy coding table destination selector: 1
.... 0001 = AC entropy coding table destination selector: 1
Start of spectral or predictor selection: 0
End of spectral selection: 63
0000 .... = Successive approximation bit position high: 0
.... 0000 = Successive approximation bit position low or point transform: 0
Entropy-coded segment (dissection is not yet implemented): 71abe8b5caf1ff007de
Marker: End of Image (0xffd9)
Entropy-coded segment (dissection is not yet implemented): 666c61677b646137336
Last boundary: \r\n------WebKitFormBoundaryIeRPZp2QAo2zkI2U--\r\n
0040 e0 3f a9 1b 7f 86 a0 ff 00 64 5c ff 00 78 0f ea
0050 41 ff 00 50 c2 dd b1 4d bb a4 a7 27 de ad 28 9c
0060 6c 6f 75 fc 23 73 3e 82 9b 0d 43 ce 2a bf f8 6a
0070 0f f6 45 cf f7 88 fe ce 00 ed a8 3f d9 17 07 fe
0080 f0 1f d4 80 7a 8a 13 b6 28 0e 92 9c 6f 9a b4 be
0090 9a 3f 59 5f 08 30 4f a0 01 b9 f8 45 57 ff 00 0d
00a0 51 fe c9 39 fc fc 7f 52 33 fe 1a 17 df f4 4d cf
00b0 f7 80 fe a4 17 e3 b0 fe d4 7f d2 93 8f ef 56 9c
00c0 cf 03 ea 93 78 d1 53 05 5f 78 c5 5a 3d b4 92 8e
00d0 78 49 c3 ff 00 bc 07 f5 20 7f 86 b3 7f ec 8b 9f
00e0 ef 01 fd 48 2f c7 61 fd a8 ff 00 a5 6a 3c 39 5a
00f0 75 4f a0 8f 54 fc 23 4f 4b 47 81 f8 45 5b ff 00
0100 0d 61 fe c8 b9 fe f0 1f d4 81 fe 1a df ff 00 a8
0110 b9 fe f0 1f d4 81 f8 f4 3f b5 0f e9 4a 9f 90 bf
0120 ff d9 66 6c 61 67 7b 64 61 37 33 64 38 38 39 33
0130 36 30 31 30 64 61 31 65 65 65 62 33 36 65 39 34
0140 35 65 63 34 62 39 37 7d 1a 0d 0a 2d 2d 2d 2d 2d
0150 2d 57 65 62 4b 69 74 46 6f 72 6d 42 6f 75 6e 64
0160 61 72 79 49 65 52 50 5a 70 32 51 41 6f 32 7a 6b
0170 49 32 55 2d 2d 0d 0a

16.小明的保险箱

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0×0             JPEG image data, JFIF standard 1.01
30            0×1E            TIFF image data, big-endian, offset of first
79903         0×1381F         RAR archive data, version 4.x, first volume t
```

发现一个rar。

爆破得到密码7869：

解压得到flag。