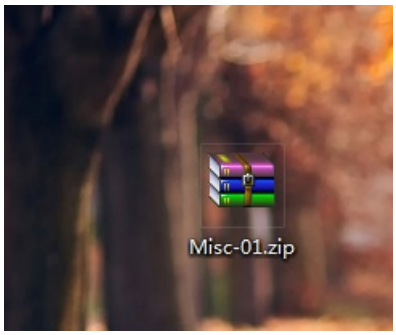
ISCC2019-MISC-最危险的地方就是最安全的地方

原创

菜鸟之小菜 于 2019-06-03 20:09:10 发布 639 收藏
分类专栏： Writeup 安全 文章标签： ISCC MISC Writeup

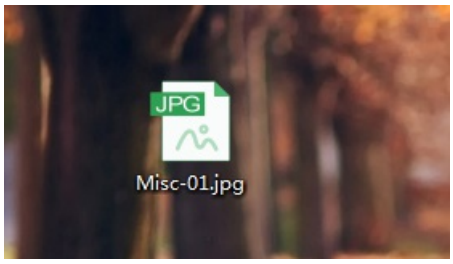
0x00

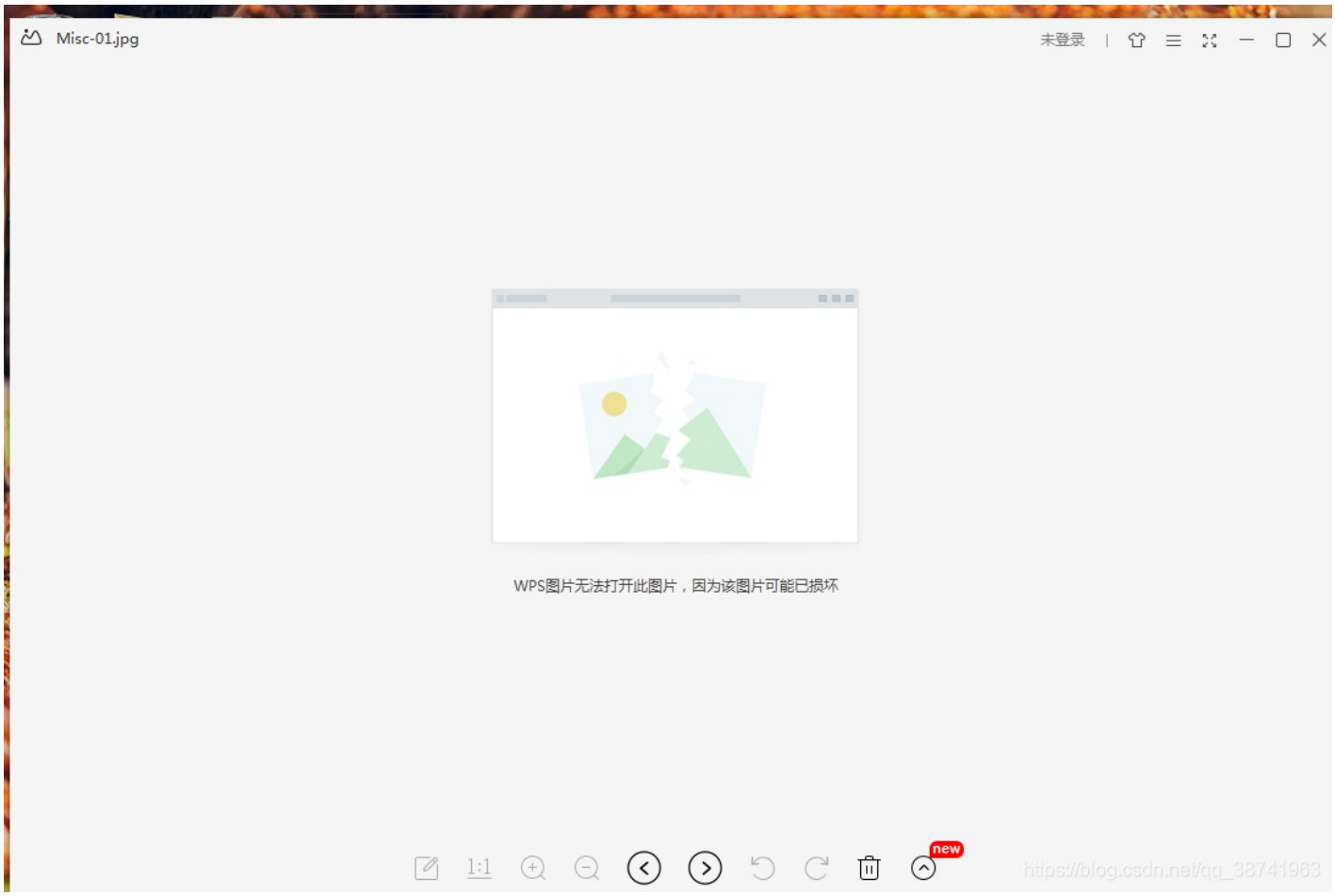
下载附件是一个压缩包：



0x01

解压压缩包是一张损坏的图片





那么就notepad++打开看一下有没有什么明显的隐写？

打开之后在最后几行明显看到了隐写的二维码，如下：

```
NUL NUL NUL NUL NUL NUL SOH NUL CAN NUL BS DLE 意 EOT 驮 SOH  a?□
驮 SOH  a?□
驮 SOH PK SOH STX US NUL DC4 NUL NUL NUL BS NUL " YN?)-ETX NUL NUL H ETX NUL NUL
NUL $ NUL NUL NUL NUL NUL NUL NUL  NUL NUL NUL 啡 NUL NUL QRcode/46.png
NUL NUL NUL NUL NUL NUL SOH NUL CAN NUL # ESC 摈 EOT 驮 SOH 仉a?□
驮 SOH 墩a?□
驮 SOH PK SOH STX US NUL DC4 NUL NUL NUL BS NUL " YN默g  ETX NUL NUL D ETX NUL NUL
NUL $ NUL NUL NUL NUL NUL NUL NUL  NUL NUL NUL b? NUL QRcode/47.png
NUL NUL NUL NUL NUL NUL SOH NUL CAN NUL h& 柜 EOT 驮 SOH 褚a?□
驮 SOH 褚a?□
驮 SOH PK SOH STX US NUL DC4 NUL NUL NUL BS NUL " YNm 娄 舅 ETX NUL NUL < ETX NUL NUL
NUL $ NUL NUL NUL NUL NUL NUL NUL  NUL NUL NUL 鏡 NUL NUL QRcode/48.png
NUL NUL NUL NUL NUL NUL SOH NUL CAN NUL U  ?驮 SOH x NUL b?□
驮 SOH x NUL b?□
驮 SOH PK SOH STX US NUL DC4 NUL NUL NUL BS NUL " YN FS '远 I ETX NUL NUL D ETX NUL NUL
NUL $ NUL NUL NUL NUL NUL NUL NUL  NUL NUL NUL B? NUL QRcode/49.png
NUL NUL NUL NUL NUL NUL SOH NUL CAN NUL q  洧 EOT 驮 SOH GMb?□
驮 SOH X&b?□
驮 SOH PK SOH STX US NUL DC4 NUL NUL NUL BS NUL " YN  阁 f ETX NUL NUL a ETX NUL NUL FF NUL $ NUL NUL NUL NUL NUL NUL NUL  NUL NUL NUL 秸 NUL NUL QRcode/5.png
NUL NUL NUL NUL NUL NUL SOH NUL CAN NUL s1"?驮 SOH 郭c?□
驮 SOH 郭c?□
驮 SOH PK SOH STX US NUL DC4 NUL NUL NUL BS NUL @ 鹋 Nic 元 鏕 NUL NUL $ z NUL NUL
NUL $ NUL NUL NUL NUL NUL NUL NUL  NUL NUL NUL F? NUL QRcode/50.jpg
NUL NUL NUL NUL NUL NUL SOH NUL CAN NUL SUB 昏 -e  SOH SUB 昏 -e  SOH 栃 3 鄙  SOH PK SOH STX US NUL DC4 NUL NUL NUL BS NUL " YN:WS昨 ETX NUL NUL F ETX NUL NU
NUL NUL NUL NUL NUL NUL SOH NUL CAN NUL 呵 $?驮 SOH ?d?□
驮 SOH ?d?□
驮 SOH PK SOH STX US NUL DC4 NUL NUL NUL BS NUL " YN 鍵 踩 c ETX NUL NUL ^ ETX NUL NUL FF NUL $ NUL NUL NUL NUL NUL NUL NUL  NUL NUL NUL 顽 NUL NUL QRcode/7.png
NUL NUL NUL NUL NUL NUL SOH NUL CAN NUL ■ '?驮 SOH 玲 d?□
驮 SOH 麓 d?□
驮 SOH PK SOH STX US NUL DC4 NUL NUL NUL BS NUL " YNT 逍  ETX NUL NUL P ETX NUL NUL FF NUL $ NUL NUL NUL NUL NUL NUL NUL  NUL NUL NUL Z? NUL QRcode/8.png
NUL NUL NUL NUL NUL NUL SOH NUL CAN NUL V1 ?? SOH 睨 d?□
驮 SOH 睨 d?□
驮 SOH PK SOH STX US NUL DC4 NUL NUL NUL BS NUL " YN 惚 杜 x ETX NUL NUL s ETX NUL NUL FF NUL $ NUL NUL NUL NUL NUL NUL NUL  NUL NUL NUL 兇 NUL NUL QRcode/9.png
NUL NUL NUL NUL NUL NUL SOH NUL CAN NUL 胂,?驮 SOH 蓓 d?□
驮 SOH 蓓 d?□
驮 SOH PK ENQ ACK NUL NUL NUL NUL 3 NUL 3 NUL ? NUL NUL { ? NUL NUL NUL
```

0x02

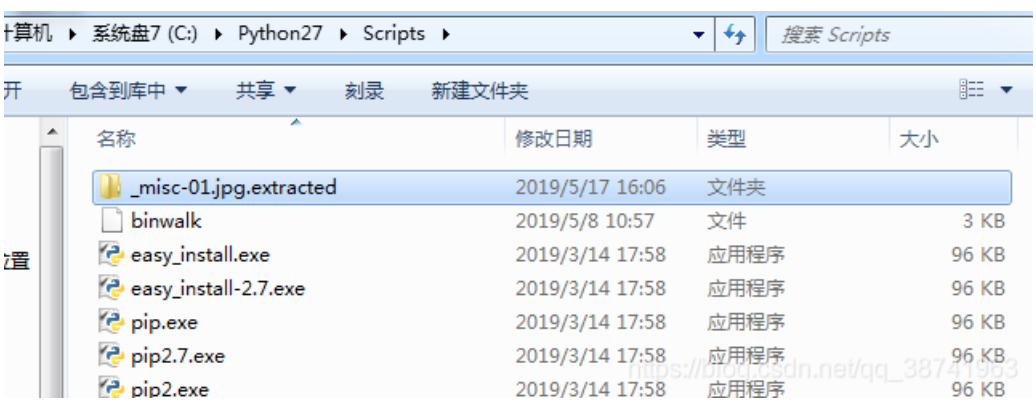
<1>binwalk查看文件如下：（打马赛克的地方是电脑的用户名，我是把图片放在桌面查看的）

```
C:\Python27\Scripts>python binwalk "/users/[redacted]/desktop/misc-01.jpg"

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------

18527         0x485F          Zip archive data, at least v1.0 to extract, name:
QRcode/
18564         0x4884          Zip archive data, at least v2.0 to extract, com
ssed size: 838, uncompressed size: 833, name: QRcode/1.png
19444         0x4BF4          Zip archive data, at least v2.0 to extract, compre
ssed size: 878, uncompressed size: 873, name: QRcode/10.png
20365         0x4F8D          Zip archive data, at least v2.0 to extract, compre
ssed size: 816, uncompressed size: 811, name: QRcode/11.png
21224         0x52E8          Zip archive data, at least v2.0 to extract, compre
ssed size: 839, uncompressed size: 834, name: QRcode/12.png
22106         0x565A          Zip archive data, at least v2.0 to extract, compre
ssed size: 799, uncompressed size: 794, name: QRcode/13.png
22948         0x59A4          Zip archive data, at least v2.0 to extract, compre
ssed size: 863, uncompressed size: 858, name: QRcode/14.png
23854         0x5D2E          Zip archive data, at least v2.0 to extract, compre
ssed size: 819, uncompressed size: 814, name: QRcode/15.png
```


<2>分离出隐写的图片

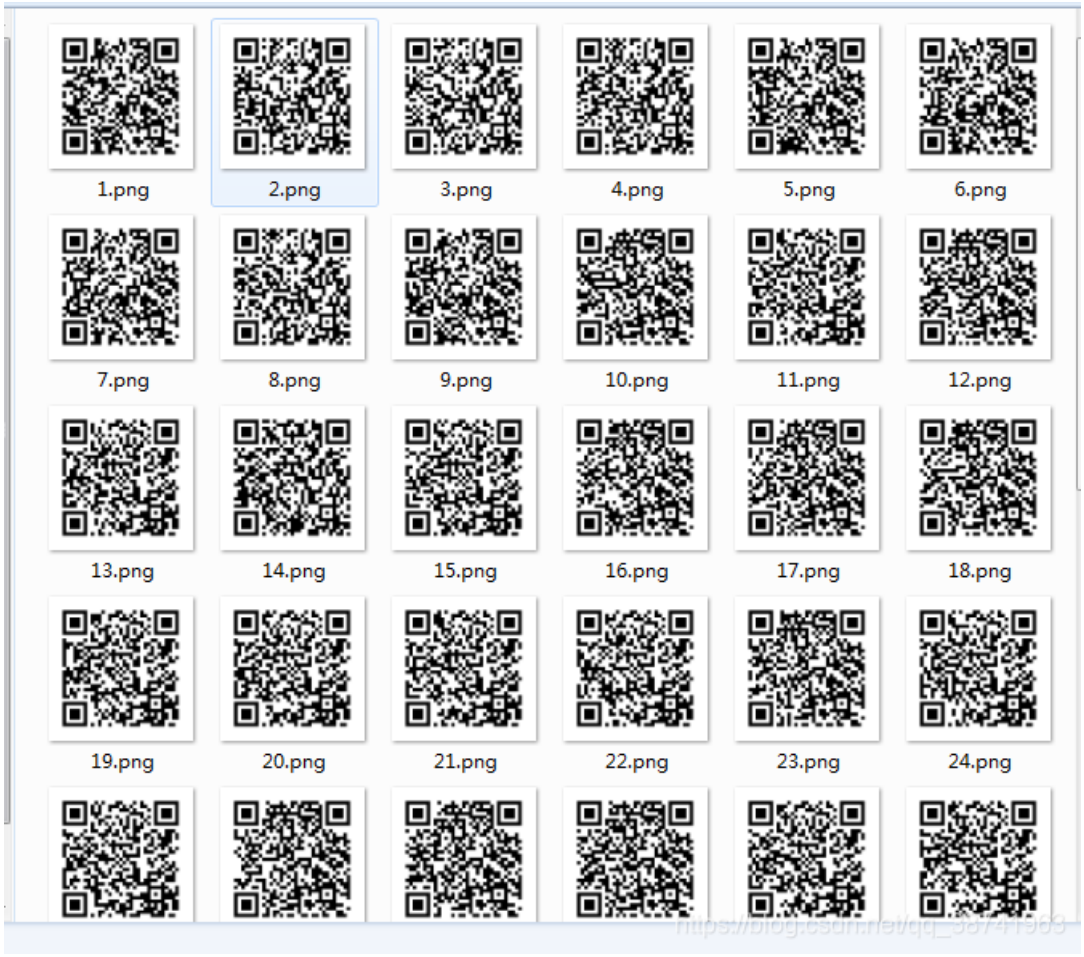
```
管理员: C:\Windows\system32\cmd.exe
C:\Python27\Scripts>python binwalk -e "/users/[redacted]/desktop/misc-01.jpg"

WARNING: The Python LZMA module could not be found. It is *strongly* recommended
 that you install this module for binwalk to provide proper LZMA identification
and extraction results.

WARNING: The Python LZMA module could not be found. It is *strongly* recommended
 that you install this module for binwalk to provide proper LZMA identification
and extraction results.

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------


WARNING: Extractor.execute failed to run external extractor 'unzip '%e'': [Error
 2] , 'unzip '%e'' might not be installed correctly
18527         0x485F          Zip archive data, at least v1.0 to extract, name:
QRcode/
18564         0x4884          Zip archive data, at least v2.0 to extract, compre
ssed size: 838, uncompressed size: 833, name: QRcode/1.png
19444         0x4BF4          Zip archive data, at least v2.0 to extract, compre
ssed size: 878, uncompressed size: 873, name: QRcode/10.png
20365         0x4F8D          Zip archive data, at least v2.0 to extract, compre
```


<3>在python安装目录的scripts目录下找到分离出的二维码图片：

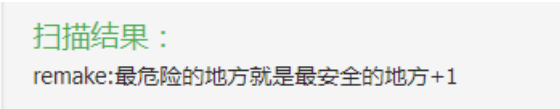


<4>选中文件夹，剪贴到桌面（方便一会对二维码的识别），打开草料二维码识别站点（https://cli.im/deqr）

<5>打开分离出的二维码图片一共有50张：



<6>上传第1张图片，识别结果如下：



第2张识别结果如下：

扫描结果：
remake:最危险的地方就是最安全的地方+2

第3张识别结果如下：

扫描结果：
remake:最危险的地方就是最安全的地方+3

<7>貌似有规律，如果一直这样识别，那需要很长时间了，所以从最后一张试试看，会不会有惊喜？（果然有惊喜）

扫描结果：
remake:最危险的地方就是最安全的地方+10086

<8>又仔细看看，才发现第50张是jpg格式，其它都是Png格式？所以notepad++打开看看，没发现什么明显的线索，所以就winhex试试看？

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	60	ÿØÿà JFIF `
00000010	00	60	00	00	FF	E1	10	84	45	78	69	66	00	00	4D	4D	` ÿá „Exif MM
00000020	00	2A	00	00	00	08	00	03	87	69	00	04	00	00	00	01	* ‡i
00000030	00	00	08	3E	9C	9C	00	01	00	00	00	2A	00	00	08	0C	>œœ *
00000040	EA	1C	00	07	00	00	07	DA	00	00	00	32	00	00	00	00	ê Ú 2
00000050	1C	EA	00	00	00	08	00	00	00	00	00	00	00	00	00	00	ê
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

<9>发现好多0，向下拉拉，发现惊喜，如下：

<10> f l a g { 1 5 c C 9 0 1 2 } 拿去提交发现不对，各种尝试之后发现flag是这样的 15cC9012 （这也算是个小坑吧）

0x03

这道题100分，基本上没有什么难度，几分钟的时间就被人秒了