




实验吧-隐写--易--小苹果

原创

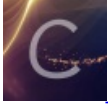
大千SS  于 2018-11-21 22:23:03 发布  155  收藏

分类专栏: [实验吧隐写](#) 文章标签: [隐写术](#)

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/zz_Caleb/article/details/83243348

版权



[实验吧隐写](#) 专栏收录该内容

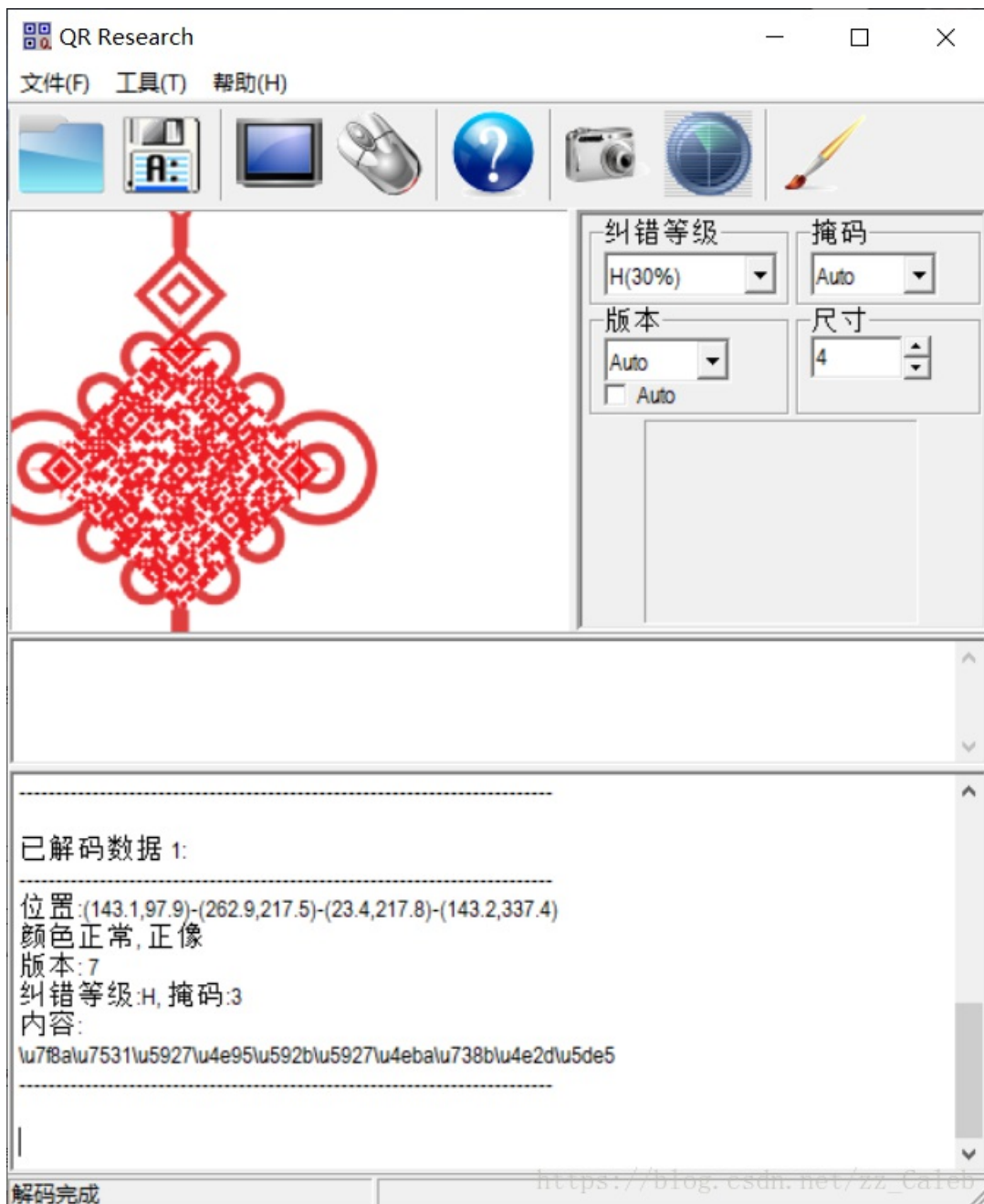
9 篇文章 0 订阅

订阅专栏

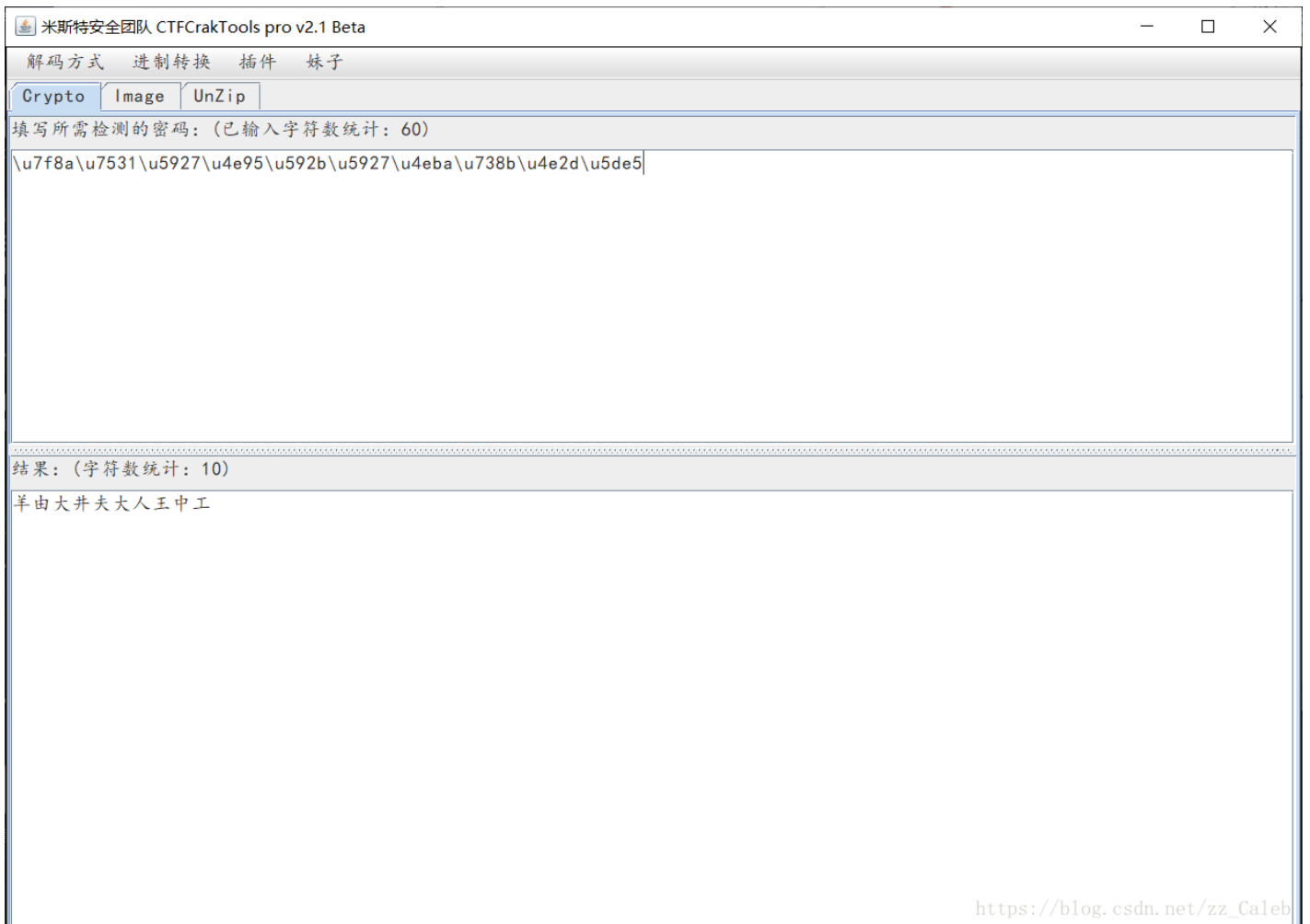
题目链接: <http://www.shiyanbar.com/ctf/1928>

1、首先下载图片保存到桌面（随便存，个人感觉桌面比较方便）

然后打开打开图片是一个二维码，用QR_Research扫描一下



发现下面是Unicode码，拿来解码一下



发现是一个当铺密码：解码之后是9158753624

到这里发现好像没什么用，进行不下去了，这时候试试咱们的kali，看看图片能不能分解

2、我直接用Xshell了，大家没有Xshell的可以直接进入虚拟机打开kali弄（感觉命令行界面比较爽）

Xshell用rz命令将文件传输到kali，然后看看能不能分解：binwalk apple.png，会发现图片是由几部分组成的，

然后用foremost apple.png将其分解，ls一下会发现多出来个output文件夹，这就是分解后的文件夹了，cd进入output，ls一下，发现有个rar文件，cd进入rar文件，ls发现有个压缩文件，将其上传到Windows上（Xshell用sz命令，虚拟机直接拖到桌面就行）。

```

root@Caleb:~# rz
root@Caleb:~# binwalk apple.png
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         PNG image, 400 x 400, 8-bit/color RGBA, no
41          0x29         Zlib compressed data, compressed
52876       0xCE8C      RAR archive data, first volume type: MAIN

root@Caleb:~# foremost apple.png
Processing: apple.png
[*]
root@Caleb:~# ls
'2018-08-21 15:08:45'  a      j      s      模板  图片  下载
'2018-08-21 15:08:50'  apple.png  output  公共  视频  文档  音乐
root@Caleb:~# cd output/
root@Caleb:~/output# ls
audit.txt  png  rar
root@Caleb:~/output# cat rar
cat: rar: 是一个目录
root@Caleb:~/output# cd rar
root@Caleb:~/output/rar# ls
00000103.rar
root@Caleb:~/output/rar# sz 00000103.rar
root@Caleb:~/output/rar#

```

https://blog.csdn.net/zz_Caleb

打开文件，发现是个MP3文件，打开听不出什么内容，只有火遍大江南北的小苹果歌谣啊。现在要用到MP3的隐写工具了，不过要先将MP3文件拖到文件夹里。

Decoder	2018/10/21 17:07	文件夹	
Encoder	2018/10/21 17:07	文件夹	
tables	2018/10/21 17:07	文件夹	
apple.mp3	2016/7/26 20:56	MP3文件	496 KB
Decode.exe	2006/6/13 7:38	应用程序	228 KB
Encode.exe	2006/6/13 7:39	应用程序	340 KB
hidden_text.txt	2000/11/30 12:13	文本文档	1 KB
MP3Stego.sln	2006/6/13 7:24	SLN 文件	3 KB
README.txt	2015/12/12 12:25	文本文档	6 KB

此时上面解出来的数字派上用场了，解码MP3文件时要用到。

在这里打开命令行用Decode.exe命令：Decode.exe -X apple.mp3 -P 9158753624

Decoder	2018/10/21 17:07	文件夹	
Encoder	2018/10/21 17:07	文件夹	
tables	2018/10/21 17:07	文件夹	
apple.mp3	2016/7/26 20:56	MP3文件	496 KB
apple.mp3.pcm	2018/10/21 18:08	PCM 文件	5,463 KB
apple.mp3.txt	2018/10/21 18:08	文本文档	1 KB
Decode.exe	2006/6/13 7:38	应用程序	228 KB
Encode.exe	2006/6/13 7:39	应用程序	340 KB
hidden_text.txt	2000/11/30 12:13	文本文档	1 KB
MP3Stego.sln	2006/6/13 7:24	SLN 文件	3 KB
README.txt	2015/12/12 12:25	文本文档	6 KB

```

管理员: C:\WINDOWS\System32\cmd.exe

F:\自理CTFtools\隐写\音频隐写\MP3Stego_1_1_18\MP3Stego>Decode.exe -X apple.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = 'apple.mp3' output file = 'apple.mp3.pcm'
Will attempt to extract hidden information. Output: apple.mp3.txt
the bit stream file apple.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=stereo, sblim=32, jsbd=32, ch=2
[Frame 1213]Avg slots/frame = 417.617; b/smp = 2.90; br = 127.895 kbps
Decoding of "apple.mp3" is finished
The decoded PCM output file name is "apple.mp3.pcm"

F:\自理CTFtools\隐写\音频隐写\MP3Stego_1_1_18\MP3Stego>

```

https://blog.csdn.net/zz_Caleb

发现这里多了几个文件，打开TXT文件发现：Q1RGe3hpYW9fcGluZ19ndW99

这是一个base64的码，用hackbar解码一下

Encryption ▾ Encoding ▾ Other ▾

Load URL

Split URL

Execute

CTF{xiao_ping_guo}

Post data Referrer User Agent Cookies

https://blog.csdn.net/zz_Caleb

这就是我们的结果了。

本人菜鸡，若有问题欢迎提出。