2020

文档音频类隐写

chendong1@venustech.com.cn
启明星辰网络空间安全学院-培训教学部
陈栋

© 启明星辰1996-2018 版权所有

目录/Contents

© 启明星辰1996-2018 版权所有

01 文本文档隐写

启明星辰
网络空间安全学院

- word隐写
- PDF隐写
- 压缩包

© 启明星辰1996-2018 版权所有

Word隐写

- 随着Office软件的广泛使用，word文本文档也越来越多当做隐写的载体，基于word的隐写主要分为以下三种：

- 字体颜色
- 文字隐藏
- 文件本质

© 启明星辰1996-2018 版权所有

Word隐写

- 字体颜色
- 通过将要隐藏的文字字体颜色调成和背景色一致，达到信息隐藏的目的：

文本文档隐写

怒发冲冠，
凭栏处、潇潇雨歇。
抬望眼、仰天长啸，壮怀激烈。
三十功名尘与土，八千里路云和月。
莫等闲、白了少年头，空悲切

文本文档隐写

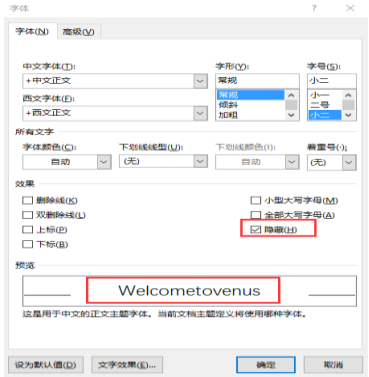
FLAG
怒发冲冠，
凭栏处、潇潇雨歇。
抬望眼、仰天长啸，壮怀激烈。
三十功名尘与土，八千里路云和月。
莫等闲、白了少年头，空悲切

© 启明星辰1996-2018 版权所有

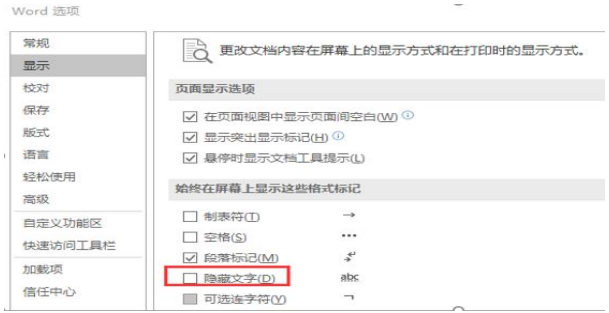
Word隐写

- 文字隐藏
- Word文字隐藏

1.选中文字，点击字体，隐藏
就能达到文字隐写的效果



2.文件-选项-显示-隐藏文字
就能看到隐藏字体



文本文档隐写

怒发冲冠，
凭栏处、潇潇雨歇。
抬望眼、仰天长啸，壮怀激烈。
三十功名尘与土，八千里路云和月。
莫等闲、白了少年头，空悲切
Welcometovenus

© 启明星辰1996-2018 版权所有

Word隐写

- 文件本质
- Word文件docx格式本质上是一个ZIP文件，主要内容是保存为XML格式的标记文件，所以才能排版好看。但文件并非直接保存于磁盘，就意味着可以解压缩，看到一部分隐写的内容。

© 启明星辰1996-2018 版权所有

01 文本文档隐写

启明星辰
网络空间安全学院

- word隐写
- PDF隐写
- 压缩包

© 启明星辰1996-2018 版权所有

PDF隐写

- 基于PDF隐写的工具不多，最常见的就是wbStego4open，
- 可以把文件隐藏到 BMP、TXT、HTM 和 PDF 文件中，且不会被看出破绽。还可以用它来创建版权标识文件并嵌入到文件中将其隐藏。

- PDF隐写原理：这个程序利用 PDF 文件头添加额外信息，这个区域的信息会被 Adobe Acrobat Reader阅读器忽略，所以不会读出来。

© 启明星辰1996-2018 版权所有

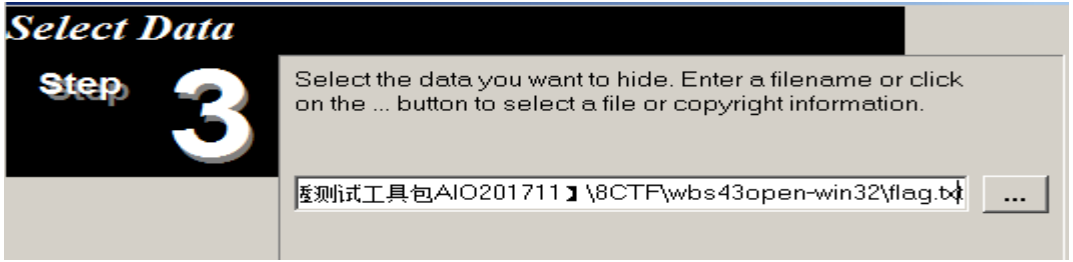
PDF隐写

- PDF隐写文本信息过程：
- wbStego4open 会把插入数据中的每一个 ASCII 码转换为二进制形式，然后把每一个二进制数字再替换为十六进制的 20或者 09，20代表0，09 代表 1。最后，这些转换后的十六进制数据被嵌入到 PDF 文件中。查看用 wbStego4open 修改后的文件内容，会发现文件中已混入了很多由 20 和 09 组成的 8 位字节。把这些 8 位字节取出来后，再提取其最低有效位，组合后即可获得其所代表的 ASCII码的二进制形式，然后再把二进制码转换成 ASCII 码就能得到原始消息了。

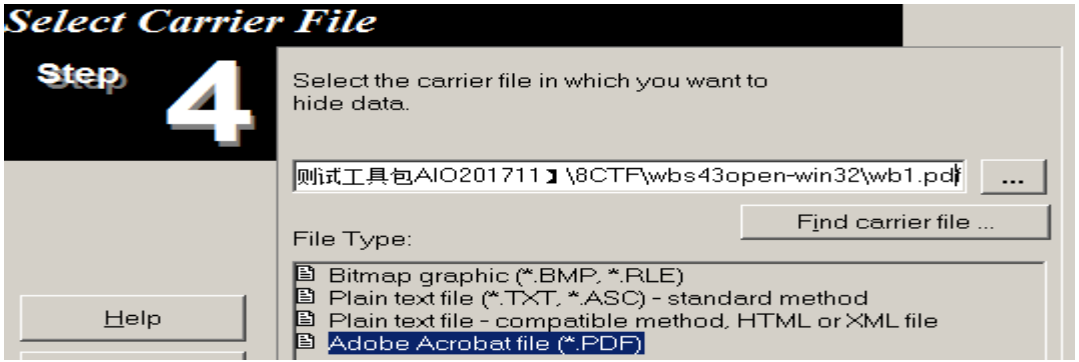
© 启明星辰1996-2018 版权所有

Wbstego4open的简单使用

- 选择需要隐写的文档



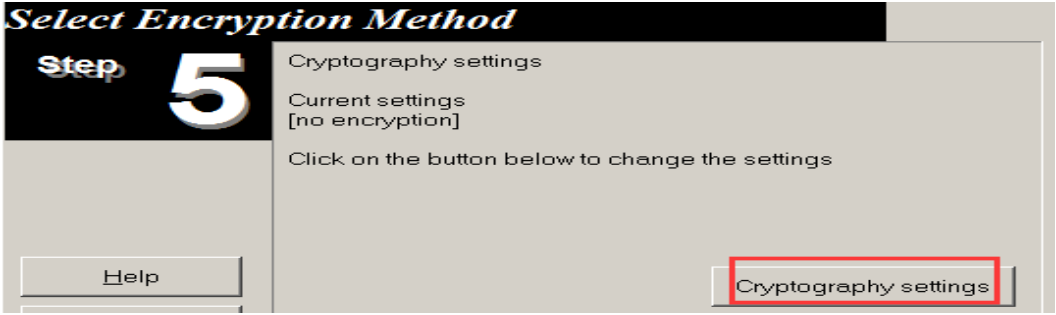
- 选择被加密的载体文档



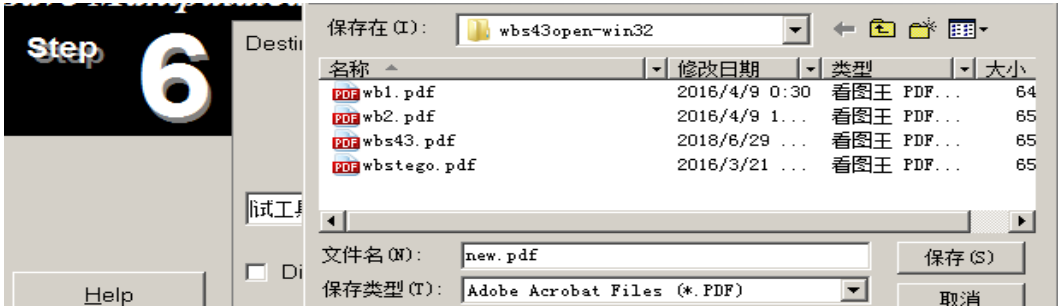
© 启明星辰1996-2018 版权所有

Wbstego4open的简单使用

- 是否使用密码加密



- 生成的加密后的文件名



解密步骤也是相似

© 启明星辰1996-2018 版权所有

01 文本文档隐写

启明星辰
网络空间安全学院

- word隐写
- PDF隐写
- 压缩包

© 启明星辰1996-2018 版权所有

压缩包

- CTF中对于压缩包考察知识点主要分为以下几种：
  - 伪加密
  - 暴力破解
  - 字典攻击
  - 掩码攻击
  - 明文攻击
  - CRC碰撞

© 启明星辰1996-2018 版权所有

ZIP伪加密

- 原理：
  - 与zip的文件格式有关，zip中有一位是标记文件是否加密的，如果更改一个未加密zip包的加密标记位，那么在打开压缩包时就会提示该文件是加密的。
- 格式：
  - 压缩源文件数据区+压缩源文件目录区+压缩源文件目录结束标志

© 启明星辰1996-2018 版权所有

ZIP伪加密

- 压缩源文件数据区：
  50 4B 03 04：这是头文件标记
  14 00：解压文件所需 pkware 版本
  00 00：全局方式位标记（有无加密）
  08 00：压缩方式
  07 76：最后修改文件时间
  F2 48：最后修改文件日期

© 启明星辰1996-2018 版权所有

ZIP伪加密

- 压缩源文件目录区：
  50 4B 01 02：目录中文件文件头标记(0x02014b50)
  1F 00：压缩使用的 pkware 版本
  14 00：解压文件所需 pkware 版本
  00 00：全局方式位标记（有无加密，这个更改这里进行伪加密，改为09 00打开就会提示有密码了,奇数加密，偶数未加密）
  08 00：压缩方式
  07 76：最后修改文件时间
  F2 48：最后修改文件日期

© 启明星辰1996-2018 版权所有

ZIP伪加密

- 压缩源文件目录结束标志：
  50 4B 05 06：目录结束标记
  00 00：当前磁盘编号
  00 00：目录区开始磁盘编号
  01 00：本磁盘上纪录总数
  01 00：目录区中纪录总数
  59 00 00 00：目录区尺寸大小
  3E 00 00 00：目录区对第一张磁盘的偏移量
  00 00：ZIP 文件注释长度

© 启明星辰1996-2018 版权所有

ZIP伪加密

- 解伪加密的三种方法01：
  - 修改标志位

flag.zip

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	50	4B	03	04	14	00	00	00	08	00	13	86	3B	4D	F2	1B	PK †;Mò
00000010	0F	4A	0E	00	00	00	0C	00	00	00	08	00	00	00	66	6C	J fl
00000020	61	67	2E	74	78	74	4B	CB	49	4C	AF	36	34	32	36	31	ag.txtKËIL¯64261
00000030	35	AB	05	00	50	4B	01	02	1F	00	14	00	09	00	08	00	5« PK
00000040	13	86	3B	4D	F2	1B	0F	4A	0E	00	00	00	0C	00	00	00	†;Mò J
00000050	08	00	24	00	00	00	00	00	00	00	20	00	00	00	00	00	$
00000060	00	00	66	6C	61	67	2E	74	78	74	0A	00	20	00	00	00	flag.txt
00000070	00	00	01	00	18	00	CE	2C	D9	E2	3E	56	D4	01	8E	AC	Î,Ùâ>VÔ Ž¬
00000080	5F	DD	3E	56	D4	01	8E	AC	5F	DD	3E	56	D4	01	50	4B	_Ý>VÔ Ž¬_Ý>VÔ PK
00000090	05	06	00	00	00	00	01	00	01	00	5A	00	00	00	34	00	Z 4
000000A0	00	00	00	00													

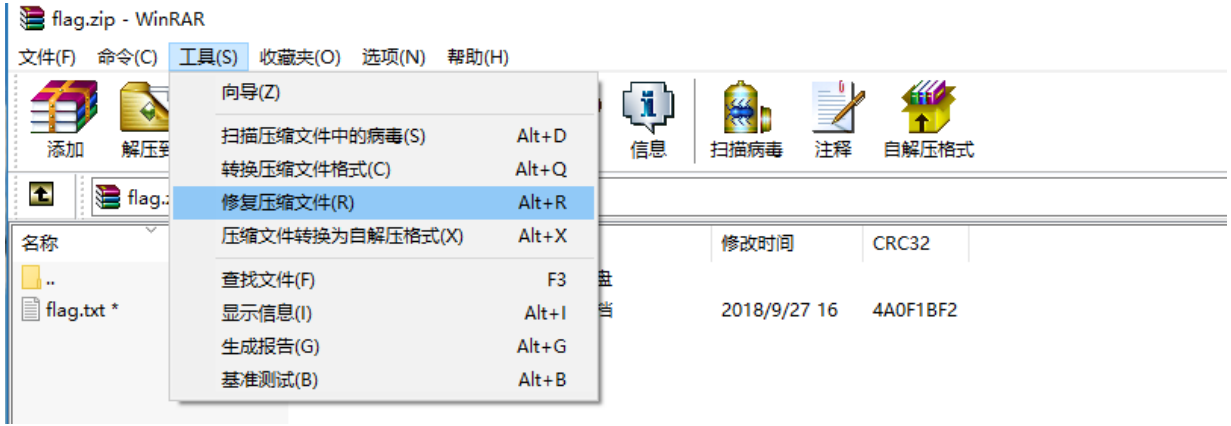
flag.zip

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	50	4B	03	04	14	00	00	00	08	00	13	86	3B	4D	F2	1B	PK †;Mò
00000010	0F	4A	0E	00	00	00	0C	00	00	00	08	00	00	00	66	6C	J fl
00000020	61	67	2E	74	78	74	4B	CB	49	4C	AF	36	34	32	36	31	ag.txtKËIL¯64261
00000030	35	AB	05	00	50	4B	01	02	1F	00	14	00	00	00	08	00	5« PK
00000040	13	86	3B	4D	F2	1B	0F	4A	0E	00	00	00	0C	00	00	00	†;Mò J
00000050	08	00	24	00	00	00	00	00	00	00	20	00	00	00	00	00	$
00000060	00	00	66	6C	61	67	2E	74	78	74	0A	00	20	00	00	00	flag.txt
00000070	00	00	01	00	18	00	CE	2C	D9	E2	3E	56	D4	01	8E	AC	Î,Ùâ>VÔ Ž¬
00000080	5F	DD	3E	56	D4	01	8E	AC	5F	DD	3E	56	D4	01	50	4B	_Ý>VÔ Ž¬_Ý>VÔ PK
00000090	05	06	00	00	00	00	01	00	01	00	5A	00	00	00	34	00	Z 4
000000A0	00	00	00	00													

© 启明星辰1996-2018 版权所有

ZIP伪加密

- 解伪加密的三种方法02：
  - WinRAR修复功能
  - 360解压/Mac OS和部分Linux系统（如Kali）直接解压



© 启明星辰1996-2018 版权所有

ZIP伪加密

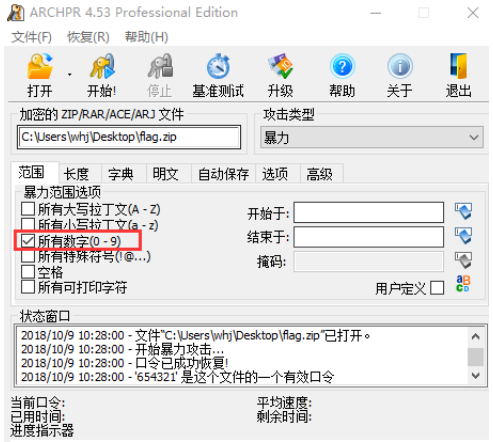
- 解伪加密的三种方法03：
  - 使用ZipCenOp.jar（需java环境）(推荐使用)

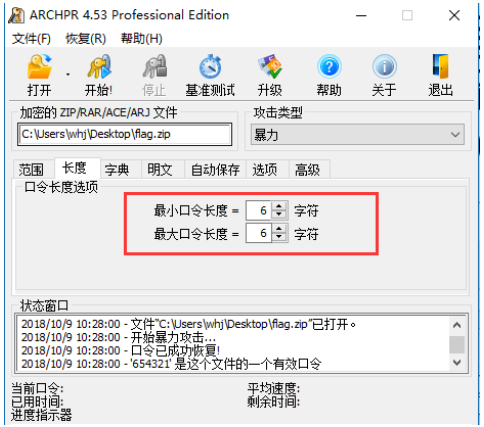
```
D:\【渗透测试工具包AIO201711】\8CTF>java -jar ZipCenOp.jar r C:\Users\whj\Desktop\flag.zip
success 1 flag(s) found
D:\【渗透测试工具包AIO201711】\8CTF>
```

© 启明星辰1996-2018 版权所有

暴力破解

- 爆破：顾名思义，逐个尝试选定集合中可以组成的所有密码，直到遇到正确密码（爆破的成功率取决于密码的复杂程度）
  - 根据题目的提示确定暴力破解的范围以及密码长度进行爆破

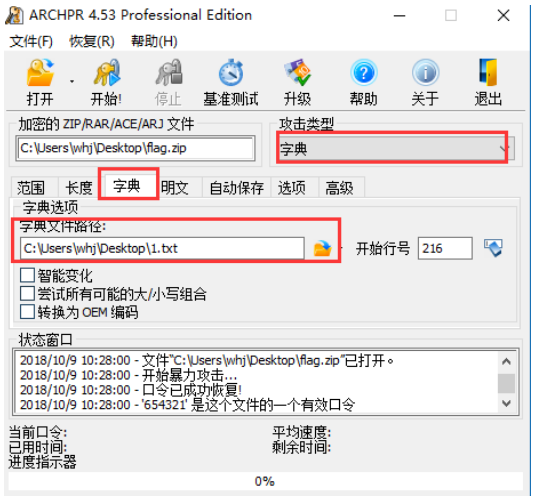




© 启明星辰1996-2018 版权所有

字典攻击

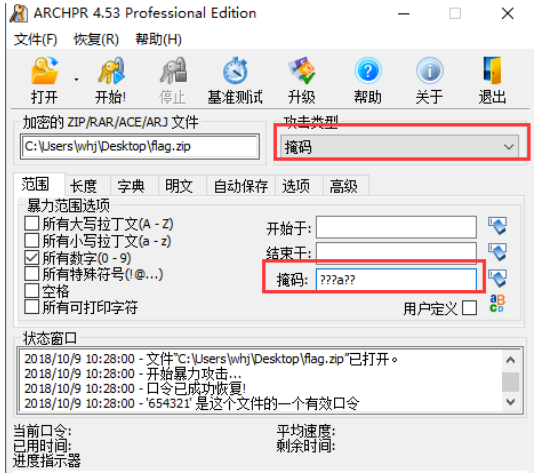
- 字典：就是常用密码的字符集，因为字典中存储了常用的密码，因此就避免了爆破时把时间浪费在脸滚键盘类的密码上，效率比爆破稍高。（成功率取决于字典的强大与否）
  - 需要一个足够强大的密码字典



© 启明星辰1996-2018 版权所有

掩码攻击

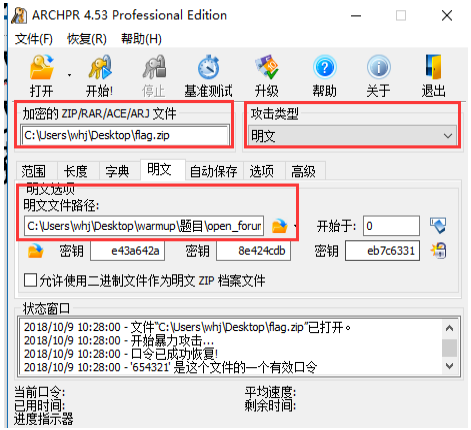
- 掩码：如果已知密码的某几位，如已知6位密码的第3位是a，那么可以构造 ??a??? 进行掩码攻击，掩码攻击的原理相当于构造了第3位为a的字典，因此掩码攻击的效率也比爆破高出不少
  - 确定密文长度与其中的某些加密字符



© 启明星辰1996-2018 版权所有

明文攻击

- 明文攻击：一种较为高效的攻击手段，利用已知的明文文件（文件大小要大于12Byte）来进行明文攻击获取未知的加密文档中的文件。因为同一个压缩包中的文件是利用同一个秘钥来进行加密的，利用明文攻击来找出秘钥，利用秘钥解密其它加密文件
  - 加密的文档和加密文档中的一个明文文件



© 启明星辰1996-2018 版权所有

目录/Contents

© 启明星辰1996-2018 版权所有

02 音频文件隐写

启明星辰
网络空间安全学院

- Wav音频隐写
- Mp3音频隐写
- 音频LSB隐写

© 启明星辰1996-2018 版权所有

wav隐写

- WAVE是录音时用的标准的windows文件格式，文件的扩展名为“WAV”，数据本身的格式为PCM或压缩型，属于无损音乐格式的一种。

- 音频分析软件
  - Adobe audition:一个专业音频编辑和混合环境，可提供先进的音频混合、编辑、控制和效果处理功能。

© 启明星辰1996-2018 版权所有

wav隐写

- 01.音频转换隐写
- 看一道隐写题wav01题目描述：用眼睛去倾听。
- 思考：明明是音频文件为什么要我们用眼睛去倾听
- 打开音频，是一段没有什么信息的声音。用AU打开，看到的波形图也看不出什么信息。

© 启明星辰1996-2018 版权所有

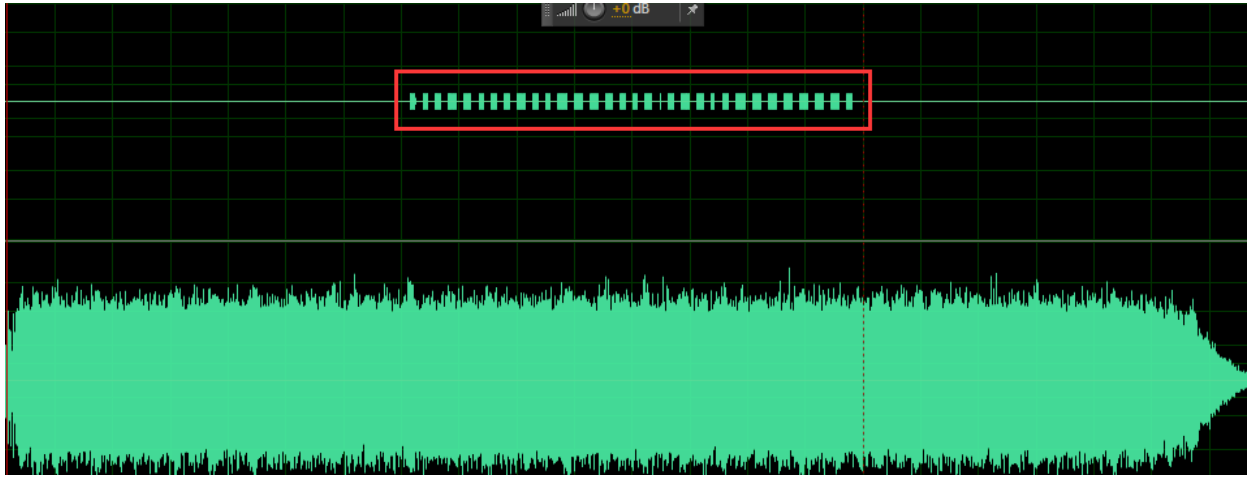
wav隐写

- 将波形图切换为频谱图直接得到隐秘信息

© 启明星辰1996-2018 版权所有

wav隐写

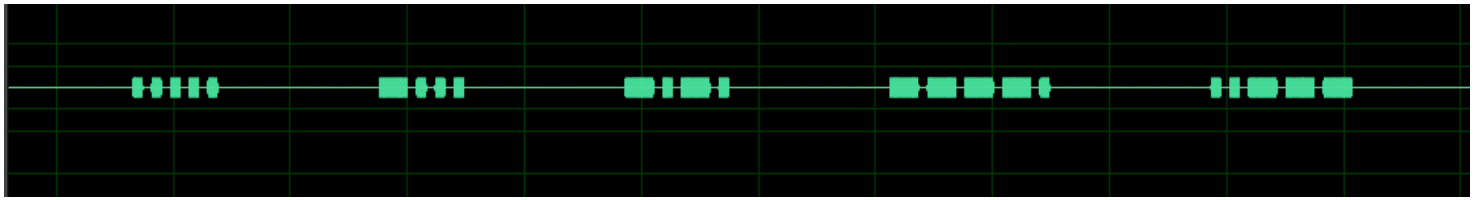
- 02. wav隐写摩斯电码
- 稍微难一点的题目通常会配合编码来使用，最常见的就是摩斯电码了。
- 看下面一道题：HelloKittyKitty.wav，载入AU，看到波形图



© 启明星辰1996-2018 版权所有

wav隐写

- 放大仔细看看，很明显是摩斯电码符号。

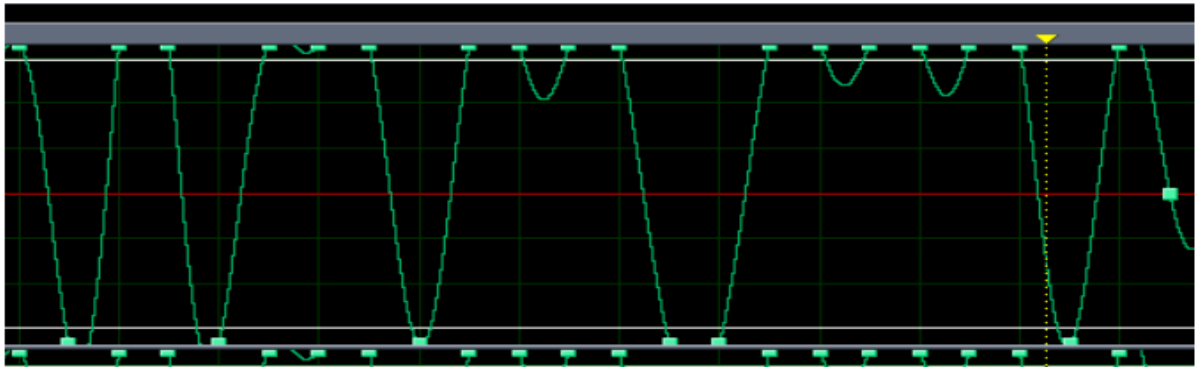


对照摩斯电码表就能得到flag，也不算是难题。

© 启明星辰1996-2018 版权所有

wav隐写

- 03.wav隐写二进制数据，不易察觉的题。
- 一般这类音频隐写题，主要观察题目的波形图，高电平代表1，低电平代表0，然后得到一串二进制字符串，再对得到的字符串进行具体的分析。



© 启明星辰1996-2018 版权所有

02 音频文件隐写

启明星辰
网络空间安全学院

- Wav音频隐写
- Mp3音频隐写
- 音频LSB隐写

© 启明星辰1996-2018 版权所有

Mp3音频隐写

- 在CTF中常见的mp3隐写一般由wav音频文件配合txt文本等文件来隐写组成新的音频文件mp3。

- 可以用mp3stego工具来解。这个工具是个命令行工具，能够把txt等文本文档隐写在wav格式的音频中，形成新的mp3音频文件。

© 启明星辰1996-2018 版权所有

Mp3stego的简单使用

- Encode

```
C:\Users\Administrator\Desktop\新建文件夹\MP3Stego_GUI>Encode.exe -E 1.txt -P 123456
 22.wav 22.mp3
MP3StegoEncoder 1.1.15
See README file for copyright info
Microsoft RIFF, WAVE audio, PCM, stereo 44100Hz 16bit, Length:  0: 4:33
MPEG-I layer III, stereo  Psychoacoustic Model: AT&T
Bitrate=128 kbps  De-emphasis: none  CRC: off
Encoding "22.wav" to "22.mp3"
Hiding "1.txt"
[Frame  10471 of  10471] (100.00%) Finished in  0: 0:52
```

- Decode

```
C:\Users\Administrator\Desktop\新建文件夹\MP3Stego_GUI>Decode.exe -X -P 123456 22.mp
3
MP3StegoEncoder 1.1.15
See README file for copyright info
Input file = '22.mp3'  output file = '22.mp3.pcm'
Will attempt to extract hidden information. Output: 22.mp3.txt
the bit stream file 22.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 10471]Avg slots/frame = 417.919; b/smp = 2.90; br = 127.988 kbps
Decoding of "22.mp3" is finished
The decoded PCM output file name is "22.mp3.pcm"
```

© 启明星辰1996-2018 版权所有

02 音频文件隐写

启明星辰
网络空间安全学院

- Wav音频隐写
- Mp3音频隐写
- 音频LSB隐写

© 启明星辰1996-2018 版权所有

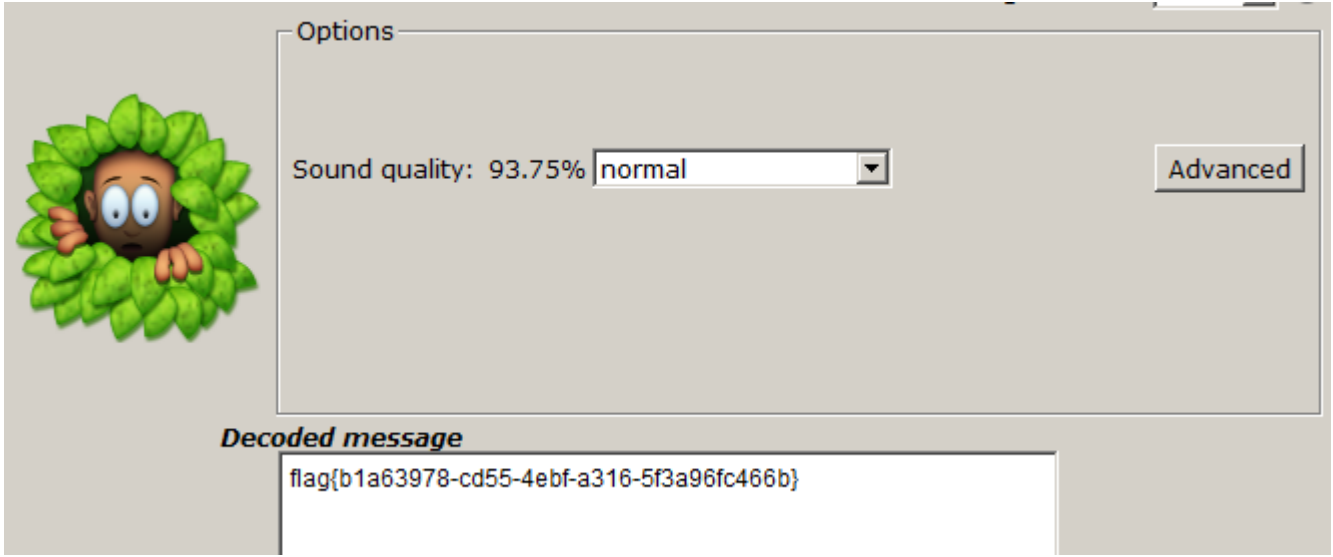
音频LSB隐写

- 对于音频文件来说，也有LSB隐写，不过音频文件的LSB隐写不像图片一样用神器打开就能发觉。所以对于音频文件隐写，如果不给提示很难有思路。主要考察工具Slienteye的使用。
- **SilentEye**是一款简单易用的信息隐藏工具，可帮助用户将隐秘信息隐藏到图片或者音频当中，通过它，用户可轻松地将不想让其他人知道的信息隐藏载体当中，且还可在文件中设置隐藏密码。

© 启明星辰1996-2018 版权所有

SilentEye的简单使用

- 图形化界面，如无需密码直接decode



© 启明星辰1996-2018 版权所有

目录/Contents

© 启明星辰1996-2018 版权所有

03 其他文件隐写

启明星辰
网络空间安全学院

- 视频文件隐写
- 磁盘文件隐写
- 字节码文件隐写

© 启明星辰1996-2018 版权所有

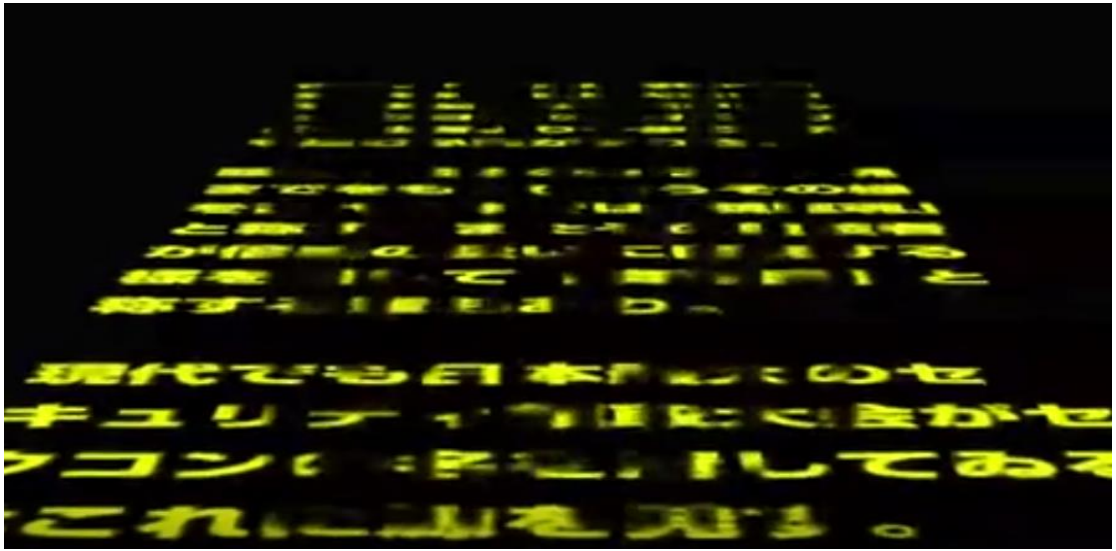
其他文件隐写

- 在CTF中除了前面介绍的图片、文本、音频文件，还有一些考察频率较低的特殊文件，一般有：
  - 视频文件（mp4等）
  - 磁盘文件隐写（vmdk等）
  - 字节码文件（pyc等）

© 启明星辰1996-2018 版权所有

MP4隐写

- CTF中关于MP4文件的隐写多数是将视频分帧考察。
  - 如题，给出一个war.mp4文件，播放视频，隐约看到一张二维码图如下：（只有当黄色字体扫过的时候才会出现）



© 启明星辰1996-2018 版权所有

MP4隐写

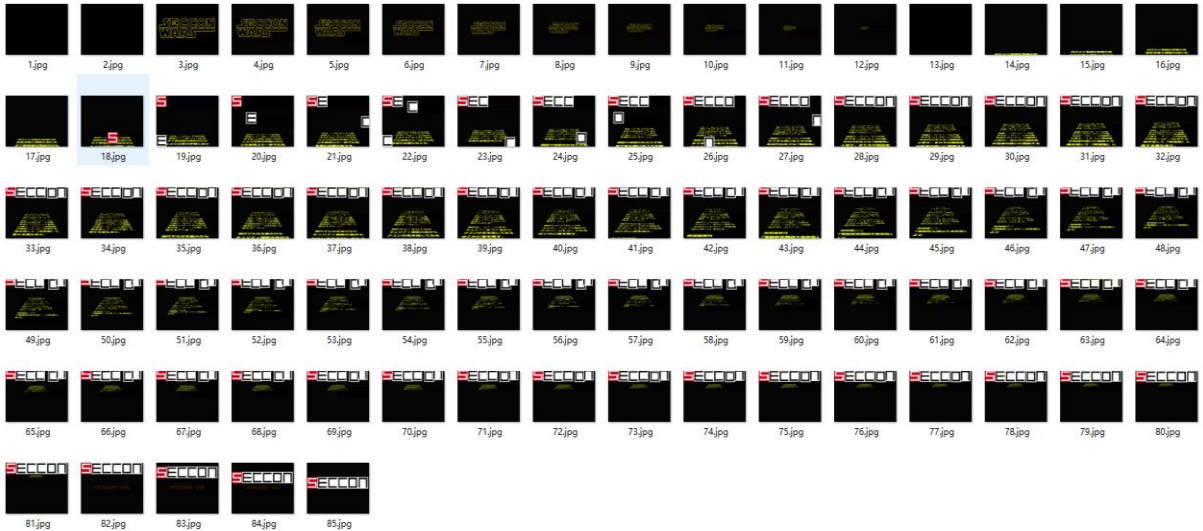
- 可以看出这张二维码图已经嵌入黑色背景，只有当黄色字体扫过的时候才会出现，需要使用ffmpeg工具将视频分帧。
  - 命令：ffmpeg -i wars.mp4 -r 1 -f image2 %d.jpg

```
D:\software\ffmpeg\ffmpeg-20181224-cdbf884-win64-static\bin>ffmpeg -i WARS.mp4 -r  1  -f image2 %d.jpg
ffmpeg version N-92795-gcdbf8847ea Copyright (c) 2000-2018 the FFmpeg developers
  built with gcc 8.2.1 (GCC) 20181201
  configuration: --enable-gpl --enable-version3 --enable-sdl2 --enable-fontconfig --enable-gnutls --enable-iconv --enable-li
s --enable-libbluray --enable-libfreetype --enable-libmp3lame --enable-libopencore-amrnb --enable-libopencore-amrwb --enable
bopenjpeg --enable-libopus --enable-libshine --enable-libsnappy --enable-libsoxr --enable-libtheora --enable-libtwolame --en
e-libvpx --enable-libwavpack --enable-libwebp --enable-libx264 --enable-libx265 --enable-libxml2 --enable-libzimg --enable-l
 --enable-zlib --enable-gmp --enable-libvidstab --enable-libvorbis --enable-libvo-amrwbenc --enable-libmysofa --enable-libsp
 --enable-libxvid --enable-libaom --enable-libmfx --enable-amf --enable-ffnvcodec --enable-cuvid --enable-d3d11va --enable-n
c --enable-nvdec --enable-dxva2 --enable-avisynth --enable-libopenmpt
  libavutil      56. 25.100 / 56. 25.100
  libavcodec     58. 42.104 / 58. 42.104
  libavformat    58. 25.100 / 58. 25.100
  libavdevice    58.  6.101 / 58.  6.101
  libavfilter     7. 46.101 /  7. 46.101
  libswscale      5.  4.100 /  5.  4.100
  libswresample   3.  4.100 /  3.  4.100
  libpostproc    55.  4.100 / 55.  4.100
Input #0, mov,mp4,m4a,3gp,3g2,mj2, from 'WARS.mp4':
  Metadata:
```

© 启明星辰1996-2018 版权所有

MP4隐写

- 得到每帧图像如下：



© 启明星辰1996-2018 版权所有

MP4隐写

- 现在需要做的就是将所有图片进行进行重叠，可以利用imagemagic中的convert工具实现
  - 命令：convert [image.jpg] -background none -compose lighten -flatten output.jpg
  - 注意：这里的image.jpg需要输入全部的图片名，太过繁琐，可以借助python脚本

© 启明星辰1996-2018 版权所有

MP4隐写

- Python脚本如下：
  - from glob import glob
  - import os
  - path = "*.jpg"
  - file = " ".join(glob(path))
  - command = "convert {} -background none -compose lighten -flatten output.jpg".format(file)
  - print(command)
  - os.system(command)

  - 注意：注意删除其他黄色图片的影响

© 启明星辰1996-2018 版权所有

MP4隐写

- 得到二维码，扫描得到flag

© 启明星辰1996-2018 版权所有

03 其他文件隐写

启明星辰
网络空间安全学院

- 视频文件隐写
- 磁盘文件隐写
- 字节码文件隐写

© 启明星辰1996-2018 版权所有

磁盘文件隐写

- 磁盘文件一般情况下考察取证，数据恢复，也会配合隐写来出题，常见磁盘文件类型如下：
  - vmdk
  - vhd
  - img
  - raw
  - ...

© 启明星辰1996-2018 版权所有

vmdk隐写

- 如题解压得到一个没有后缀的文件
  - file命令分析一下

  - 发现是vm的虚拟硬盘文件

© 启明星辰1996-2018 版权所有

vmdk隐写

- 使用disk genius打开，看到一个MP4文件

© 启明星辰1996-2018 版权所有

vmdk隐写

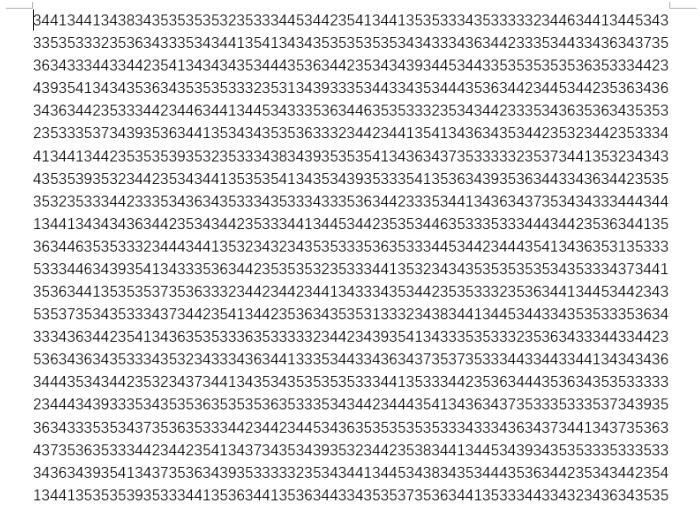
- Binwalk 分析，发现zip结构，foremost提取文件

```
root@kali2017-64:~/桌面# binwalk  misc.mp4

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
13686979      0xD0D8C3        Zip archive data, at least v2.0 to extract, compressed size: 346, uncompressed size: 1312, name: [Content_Types].xml
13687894      0xD0DC56        Zip archive data, at least v2.0 to extract, compressed size: 239, uncompressed size: 590, name: _rels/.rels
13688694      0xD0DF76        Zip archive data, at least v2.0 to extract, compressed size: 244, uncompressed size: 817, name: word/_rels/document.xml.rels
13689260      0xD0E1AC        Zip archive data, at least v2.0 to extract, compressed size: 1866, uncompressed size: 7329, name: word/document.xml
13691173      0xD0E925        Zip archive data, at least v2.0 to extract, compressed size: 1761, uncompressed size: 8398, name: word/theme/theme1.xml
13692985      0xD0F039        Zip archive data, at least v2.0 to extract, compressed size: 1132, uncompressed size: 2949, name: word/settings.xml
13694164      0xD0F4D4        Zip archive data, at least v2.0 to extract, compressed size: 488, uncompressed size: 1365, name: word/fontTable.xml
13694700      0xD0F6EC        Zip archive data, at least v2.0 to extract, compressed size: 280, uncompressed size: 576, name: word/webSettings.xml
13695030      0xD0F836        Zip archive data, at least v2.0 to extract, compressed size: 377, uncompressed size: 713, name: docProps/app.xml
13695717      0xD0FAE5        Zip archive data, at least v2.0 to extract, compressed size: 375, uncompressed size: 739, name: docProps/core.xml
13696403      0xD0FD93        Zip archive data, at least v2.0 to extract, compressed size: 2880, uncompressed size: 28941, name: word/styles.xml
13700033      0xD10BC1        End of Zip archive

root@kali2017-64:~/桌面# foremost misc.mp4
Processing: misc.mp4
|foundat=_rels/.rels ▯▯▯▯
foundat=word/_rels/document.xml.rels ▯▯▯▯
*|
```

© 启明星辰1996-2018 版权所有

vmdk隐写

- 得到word,打开看到一串字符编码


3441344134383435353532353334453442354134413535333435333332344634413445343
335353332353634333534344135413434353535353534343334363442333534433436343735
363433344334423541343434353444353634423534343934453443353535353536353334423
439354134343536343535353332353134393335344334353444353634423445344235363436
343634423533344234463441344534333536344635353332353434423335343635363435353
235333537343935363441353434353536333234423441354134363435344235323442353334
413441344235353539353235333438343935353541343634373533333235373441353234343
435353935323442353434413535354134353439353335413536343935363443343634423535
353235333442333534363435333435333435363442333534413436343753434333444344
134413434343634423534344235333441344534423535344635333533344434423536344135
363446353533323444344135323432343535333536353334453442344435413436353135333
533344634393541343335363442353535323533344135323434353535353534353334373441
353634413535353735363332344234423441343334353442353533235363441344534423343
535373534353334373442354134423536343535313332343834413445344334353533536343
333436344235413436353533363533333234423439354134333535333235363433344334423
536343634353334353234333436344133353443343634373537353334433443344134343436
344435343442353234373441343534353535353334413533344235363444353634353533333
234443439333534353536353535363533353434423444354134363437353353333537343935
363433335353437353635333442344234454343635353535353333433343634373441343735363
437353635333442344235413437343534393532344235383441344534393435353335333533
343634393541343735363439353333323534344134453483435344435363442353434423543
134413535353935353344135363441353634433435353735363441353334433432343634353 5

然后按照以下路径decode，即可得到flag

hex

hex

base32

base32

base32

base64

base64

hex

base32

base64

base64

- 那就应该是字符编码的转换了，最后按照上面的解码顺序得到flag

© 启明星辰1996-2018 版权所有

03 其他文件隐写

启明星辰
网络空间安全学院

- 视频文件隐写
- 磁盘文件隐写
- 字节码文件隐写

© 启明星辰1996-2018 版权所有

pyc文件隐写

- pyc文件是由py文件经过编译后生成的字节码文件，所以py文件变成pyc文件后，加载的速度会提高。并且在做软件开发过程中，不可能直接发布py源码，所以需要编译成pyc文件，这样一定程度上有利于源码保护。python中内置的类库py_compile 模块就可以用来实现把py文件编译为pyc文件。用法如下：

```
C:\Users\whj\Desktop>
C:\Users\whj\Desktop>python
Python 2.7.14 (v2.7.14:84471935ed, Sep 16 2017, 20:19:30) [MSC v.1500 32 bit (Intel)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import py_compile
>>> py_compile.compile(r'C:\Users\whj\Desktop\1.py')
>>>
```

© 启明星辰1996-2018 版权所有

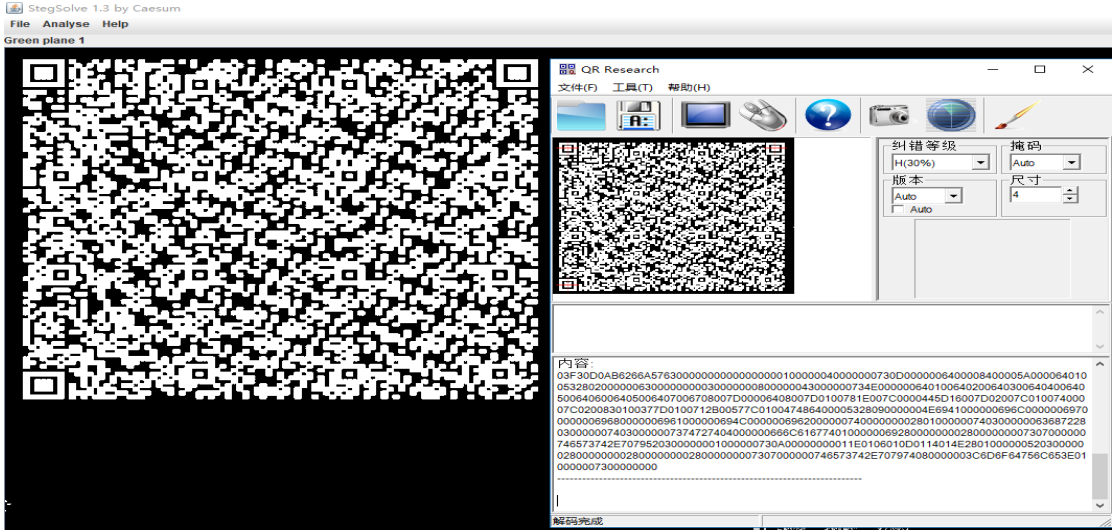
pyc文件隐写

- pyc文件也是可以反编译的，python源码中的opcode，可以根据pyc文件反编译出py文件源码。
  - 如题，得到一张png图片如下：

© 启明星辰1996-2018 版权所有

pyc文件隐写

- 根据图片类型为png，我们可以缩小解题范围，使用stegsolve检测LSB隐写，在蓝色通道1，发现一张二维码，CQR扫描得到字符03F，pyc文件头



© 启明星辰1996-2018 版权所有

pyc文件隐写

- 使用notepad++等工具进行hex转ascii得到pyc文件，然后反编译，得到flag

请选择pyc文件进行解密。支持所有Python版本

选择文件 未选择任何文件

```
#!/usr/bin/env python
# encoding: utf-8
# 如果觉得不错，可以推荐给你的朋友！http://tool.lu/pyc

def flag():
    str = [
        65,
        108,
        112,
        104,
        97,
        76,
        97,
        98]
    flag = ''
    for i in str:
        flag += chr(i)

    print flag
```

© 启明星辰1996-2018 版权所有

感谢观看

启明星辰
网络空间安全学院

© 启明星辰1996-2018 版权所有