[ACTF新生赛2020]剑龙

原创

cuihua2021 于 2022-03-31 21:08:45 发布 384 收藏

分类专栏： BUU-Misc 文章标签： 其他

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/WYHPROGRAME/article/details/123883510

版权

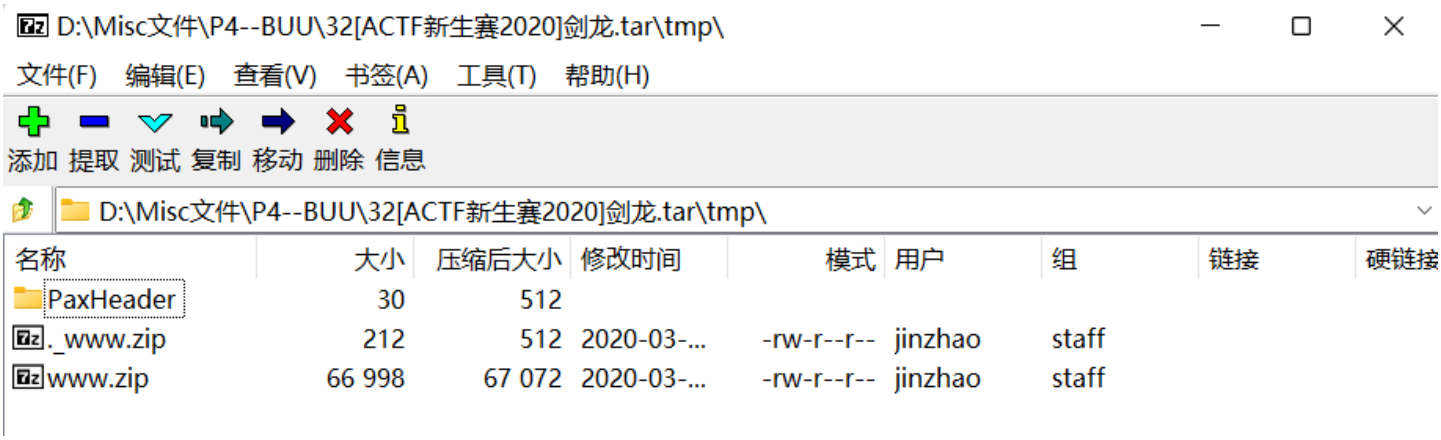
BUU-Misc 专栏收录该内容

9 篇文章 0 订阅

订阅专栏

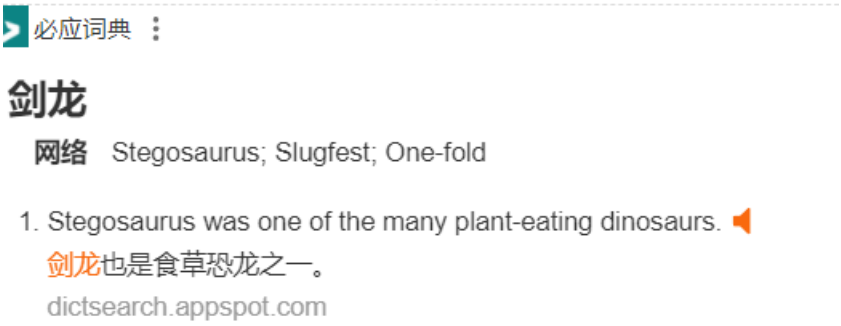
32.[ACTF新生赛2020]剑龙

1.题目概述



2.解题过程

直接解压www.zip，出了一个o_o文件，O_O是pyc文件，题目名称叫剑龙



pyc文件

借一段话，转自

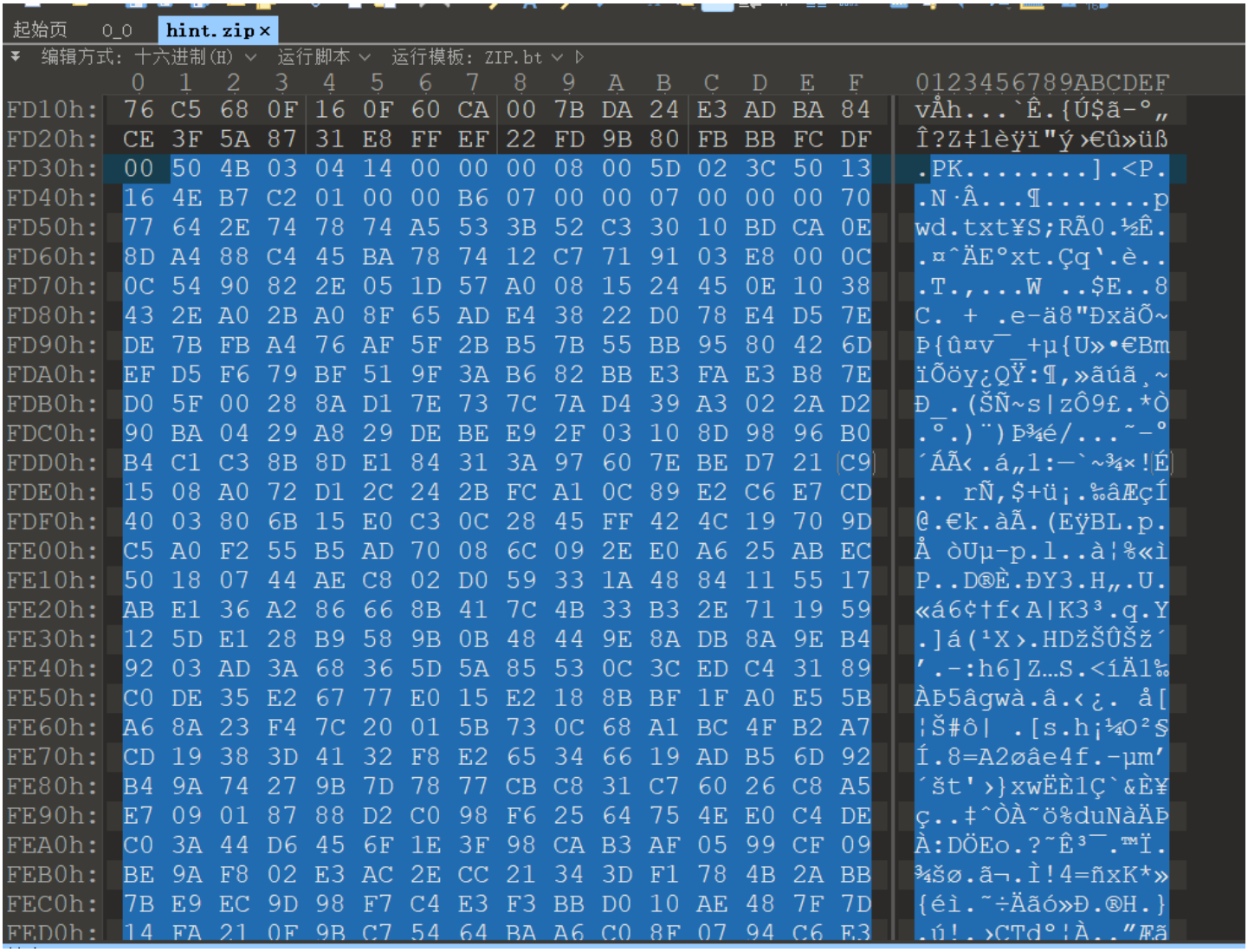
一文让你完全弄懂Stegosaurus - Angel_Kitty - 博客园 (cnblogs.com)

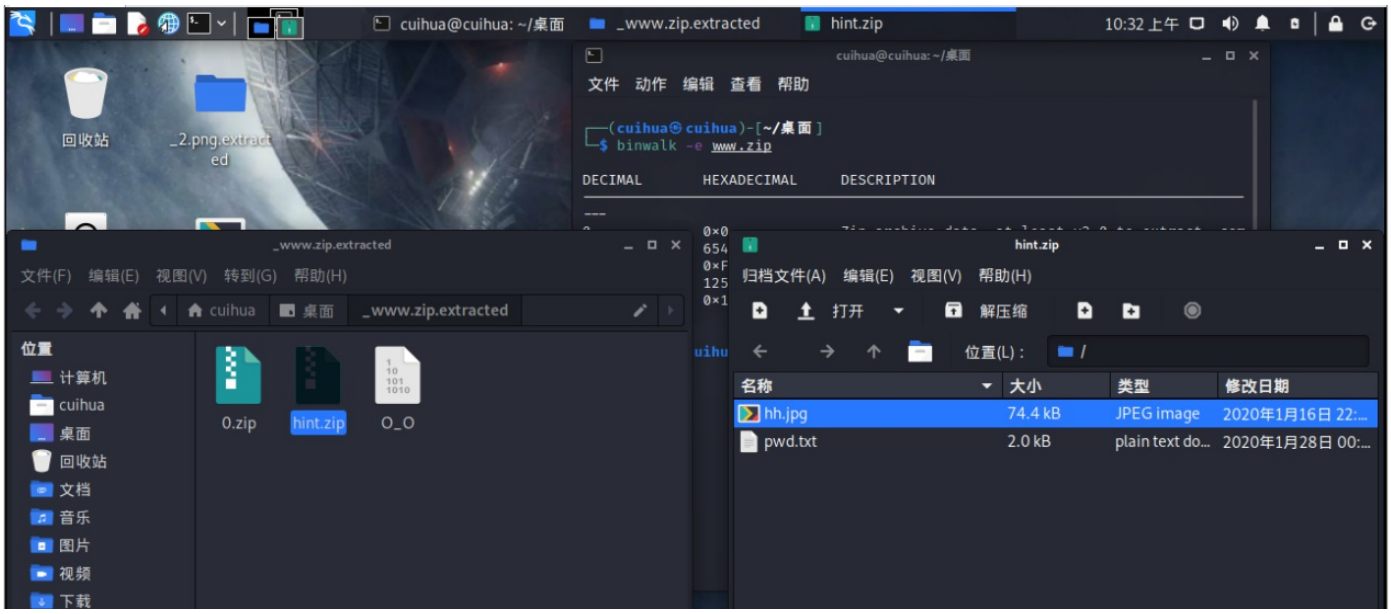
简单来说， pyc 文件就是 Python 的字节码文件，是个二进制文件。我们都知道 Python 是一种全平台的解释性语言，全平台其实就是 Python 文件在经过解释器解释之后(或者称为编译)生成的 pyc 文件可以在多个平台下运行，这样同样也可以隐藏源代码。其实， Python 是完全面向对象的语言， Python 文件在经过解释器解释后生成字节码对象 PyCodeObject， pyc 文件可以理解为是 PyCodeObject 对象的持久化保存方式。而 pyc 文件只有在文件被当成模块导入时才会生成。也就是说， Python 解释器认为，只有 import 进行的模块才需要被重用。 生成 pyc 文件的好处显而易见，当我们多次运行程序时，不需要重新对该模块进行重新的解释。主文件一般只需要加载一次，不会被其他模块导入，所以一般主文件不会生成 pyc 文件。

pyc文件破解需要密码，先放在这里，去寻找密码

www.zip解压后是一个hint.zip，010查看发现藏着其他压缩包，

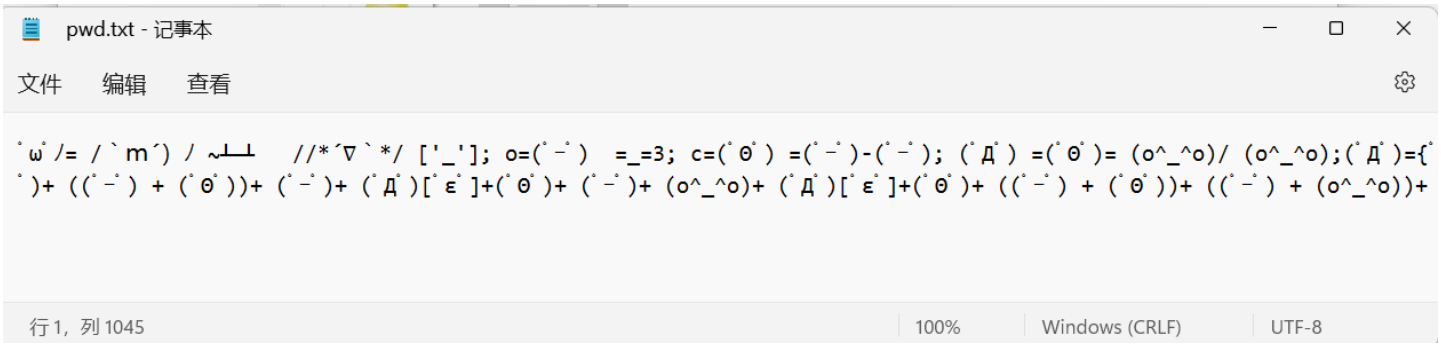
biwalk分离


起始页
0_0
hint.zip
编辑方式：十六进制(H)
运行脚本
运行模板：ZIP.bt
0 1 2 3 4 5 6 7 8 9 A B C D E F
0123456789ABCDEF
FD10h: 76 C5 68 0F 16 0F 60 CA 00 7B DA 24 E3 AD BA 84
FD20h: CE 3F 5A 87 31 E8 FF EF 22 FD 9B 80 FB BB FC DF
FD30h: 00 50 4B 03 04 14 00 00 00 08 00 5D 02 3C 50 13
FD40h: 16 4E B7 C2 01 00 00 B6 07 00 00 07 00 00 00 70
FD50h: 77 64 2E 74 78 74 A5 53 3B 52 C3 30 10 BD CA 0E
FD60h: 8D A4 88 C4 45 BA 78 74 12 C7 71 91 03 E8 00 0C
FD70h: 0C 54 90 82 2E 05 1D 57 A0 08 15 24 45 0E 10 38
FD80h: 43 2E A0 2B A0 8F 65 AD E4 38 22 D0 78 E4 D5 7E
FD90h: DE 7B FB A4 76 AF 5F 2B B5 7B 55 BB 95 80 42 6D
FDA0h: EF D5 F6 79 BF 51 9F 3A B6 82 BB E3 FA E3 B8 7E
FDB0h: D0 5F 00 28 8A D1 7E 73 7C 7A D4 39 A3 02 2A D2
FDC0h: 90 BA 04 29 A8 29 DE BE E9 2F 03 10 8D 98 96 B0
FDD0h: B4 C1 C3 8B 8D E1 84 31 3A 97 60 7E BE D7 21 C9
FDE0h: 15 08 A0 72 D1 2C 24 2B FC A1 0C 89 E2 C6 E7 CD
FDF0h: 40 03 80 6B 15 E0 C3 0C 28 45 FF 42 4C 19 70 9D
FE00h: C5 A0 F2 55 B5 AD 70 08 6C 09 2E E0 A6 25 AB EC
FE10h: 50 18 07 44 AE C8 02 D0 59 33 1A 48 84 11 55 17
FE20h: AB E1 36 A2 86 66 8B 41 7C 4B 33 B3 2E 71 19 59
FE30h: 12 5D E1 28 B9 58 9B 0B 48 44 9E 8A DB 8A 9E B4
FE40h: 92 03 AD 3A 68 36 5D 5A 85 53 0C 3C ED C4 31 89
FE50h: C0 DE 35 E2 67 77 E0 15 E2 18 8B BF 1F A0 E5 5B
FE60h: A6 8A 23 F4 7C 20 01 5B 73 0C 68 A1 BC 4F B2 A7
FE70h: CD 19 38 3D 41 32 F8 E2 65 34 66 19 AD B5 6D 92
FE80h: B4 9A 74 27 9B 7D 78 77 CB C8 31 C7 60 26 C8 A5
FE90h: E7 09 01 87 88 D2 C0 98 F6 25 64 75 4E E0 C4 DE
FEA0h: C0 3A 44 D6 45 6F 1E 3F 98 CA B3 AF 05 99 CF 09
FEB0h: BE 9A F8 02 E3 AC 2E CC 21 34 3D F1 78 4B 2A BB
FEC0h: 7B E9 EC 9D 98 F7 C4 E3 F3 BB D0 10 AE 48 7F 7D
FED0h: 14 FA 21 0F 9B C7 54 64 BA A6 C0 8F 07 94 C6 E3


cuihua@cuihua: ~/桌面
_www.zip.extracted
hint.zip
10:32 上午
回收站
_2.png.extracted
文件 动作 编辑 查看 帮助
(cuihua㉿cuihua)-[~/桌面]
$ binwalk -e www.zip
DECIMAL HEXADECIMAL DESCRIPTION
_www.zip.extracted
文件(F) 编辑(E) 视图(V) 转到(G) 帮助(H)
cuihua 桌面 _www.zip.extracted
位置
计算机
cuihua
桌面
回收站
文档
音乐
图片
视频
下载
0.zip
hint.zip
O_O
hint.zip
归档文件(A) 编辑(E) 视图(V) 帮助(H)
打开
解压缩
位置(L): /
名称 大小 类型 修改日期
hh.jpg 74.4 kB JPEG image 2020年1月16日 22:...
pwd.txt 2.0 kB plain text do... 2020年1月28日 00:...

打开图片

打开pwd.txt



AAencode编码

CTF在线工具-在线AAencode编码|AA编码|AAencode解码|AAencode编码原理|AAencode编码算法 (hiencode.com)

AAencode

AAencode

```
ﾟωﾟﾉ= / ｀m´）ﾉ ~┻━┻   //*´∇｀*/ ['_']; o=(ﾟｰﾟ)  =_=3; c=(ﾟΘﾟ) =(ﾟｰﾟ)-(ﾟｰﾟ); (ﾟДﾟ) =(ﾟΘﾟ)= (o^_^o)/ (o^_^o);(ﾟДﾟ)={ﾟΘﾟ: '_' ,ﾟωﾟﾉ : ((ﾟωﾟﾉ==3) +'_') [ﾟΘﾟ] ,ﾟｰﾟﾉ :(ﾟωﾟﾉ+ '_')[o^_^o -(ﾟΘﾟ)] ,ﾟДﾟﾉ:((ﾟｰﾟ==3) +'_')[ﾟｰﾟ] }; (ﾟДﾟ) [ﾟΘﾟ] =((ﾟωﾟﾉ==3) +'_') [c^_^o];(ﾟДﾟ) ['c'] = ((ﾟДﾟ)+'_') [ (ﾟｰﾟ)+(ﾟｰﾟ)-(ﾟΘﾟ) ];(ﾟДﾟ) ['o'] = ((ﾟДﾟ)+'_') [ﾟΘﾟ];(ﾟoﾟ)=(ﾟДﾟ) ['c']+(ﾟДﾟ) ['o']+(ﾟωﾟﾉ +'_')[ﾟΘﾟ]+ ((ﾟωﾟﾉ==3) +'_') [ﾟｰﾟ] + ((ﾟДﾟ) +'_') [(ﾟｰﾟ)+(ﾟｰﾟ)]+ ((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+((ﾟｰﾟ==3) +'_') [(ﾟｰﾟ) - (ﾟΘﾟ)]+(ﾟДﾟ) ['c']+((ﾟДﾟ)+'_') [(ﾟｰﾟ)+(ﾟｰﾟ)]+ (ﾟДﾟ) ['o']+((ﾟｰﾟ==3) +'_') [ﾟΘﾟ];(ﾟДﾟ) ['_'] =(o^_^o) [ﾟoﾟ] [ﾟoﾟ];(ﾟεﾟ)=((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+ (ﾟДﾟ) .ﾟДﾟﾉ+((ﾟДﾟ)+'_') [(ﾟｰﾟ) + (ﾟｰﾟ)]+((ﾟｰﾟ==3) +'_') [o^_^o -ﾟΘﾟ]+((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+ (ﾟωﾟﾉ +'_') [ﾟΘﾟ]; (ﾟｰﾟ)+=(ﾟΘﾟ); (ﾟДﾟ)[ﾟεﾟ]='\\'; (ﾟДﾟ).ﾟΘﾟﾉ=(ﾟДﾟ+ ﾟｰﾟ)[o^_^o -(ﾟΘﾟ)];(oﾟｰﾟo)=(ﾟωﾟﾉ +'_')[c^_^o];(ﾟДﾟ) [ﾟoﾟ]='\"';(ﾟДﾟ) ['_'] ( ﾟДﾟ) ['_'] (ﾟεﾟ+(ﾟДﾟ) [ﾟoﾟ]+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ ((ﾟｰﾟ) + (o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (o^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ ((ﾟｰﾟ) + (o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+((o^_^o) +(o^_^o))+ (o^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟｰﾟ)+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟoﾟ]) (ﾟΘﾟ)) ('_');
```

加 密　　解 密

welcom3!

```
welcom3!
```

再看看图片，

不是LSB隐写，有密码，可能是steghide隐写

steghide隐写

隐写工具Steghide - 简书 (jianshu.com)

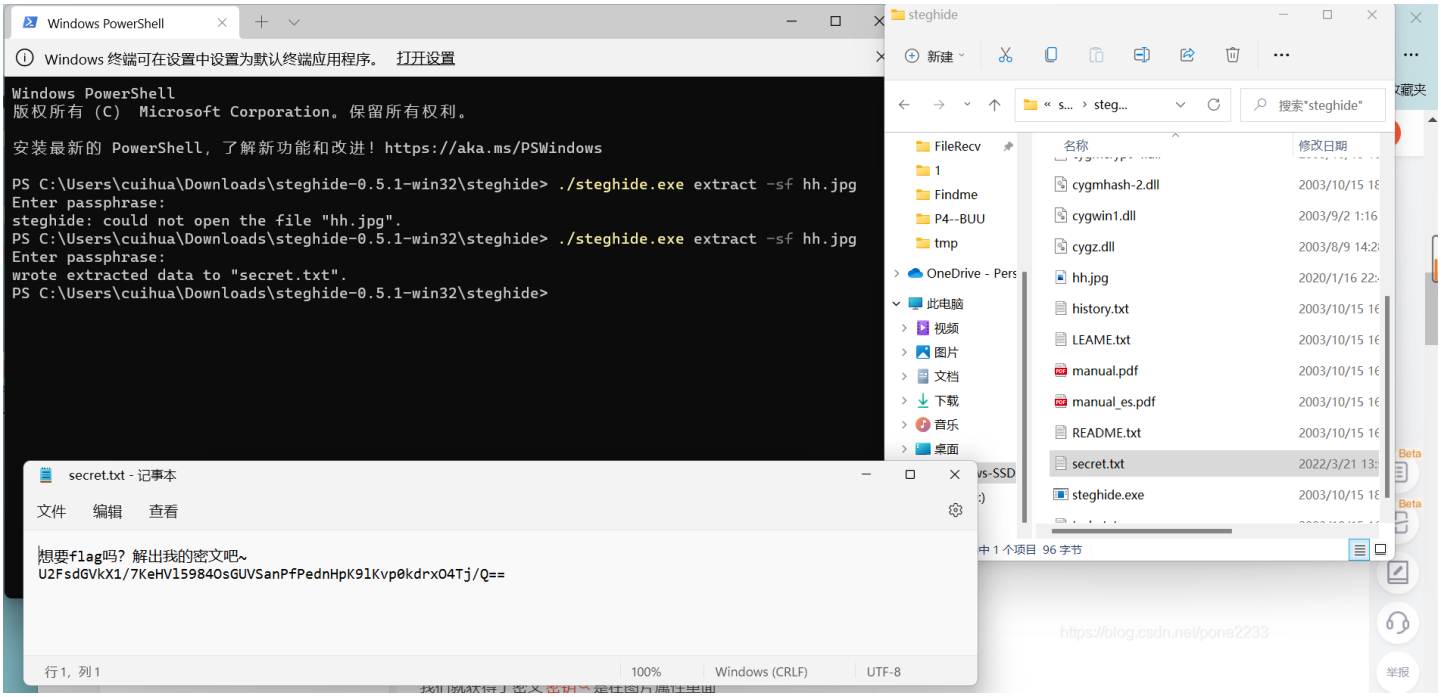
Steghide是一个可以将文件隐藏到图片或音频中的工具

下载地址：

Find out more about steghide | SourceForge.net

命令

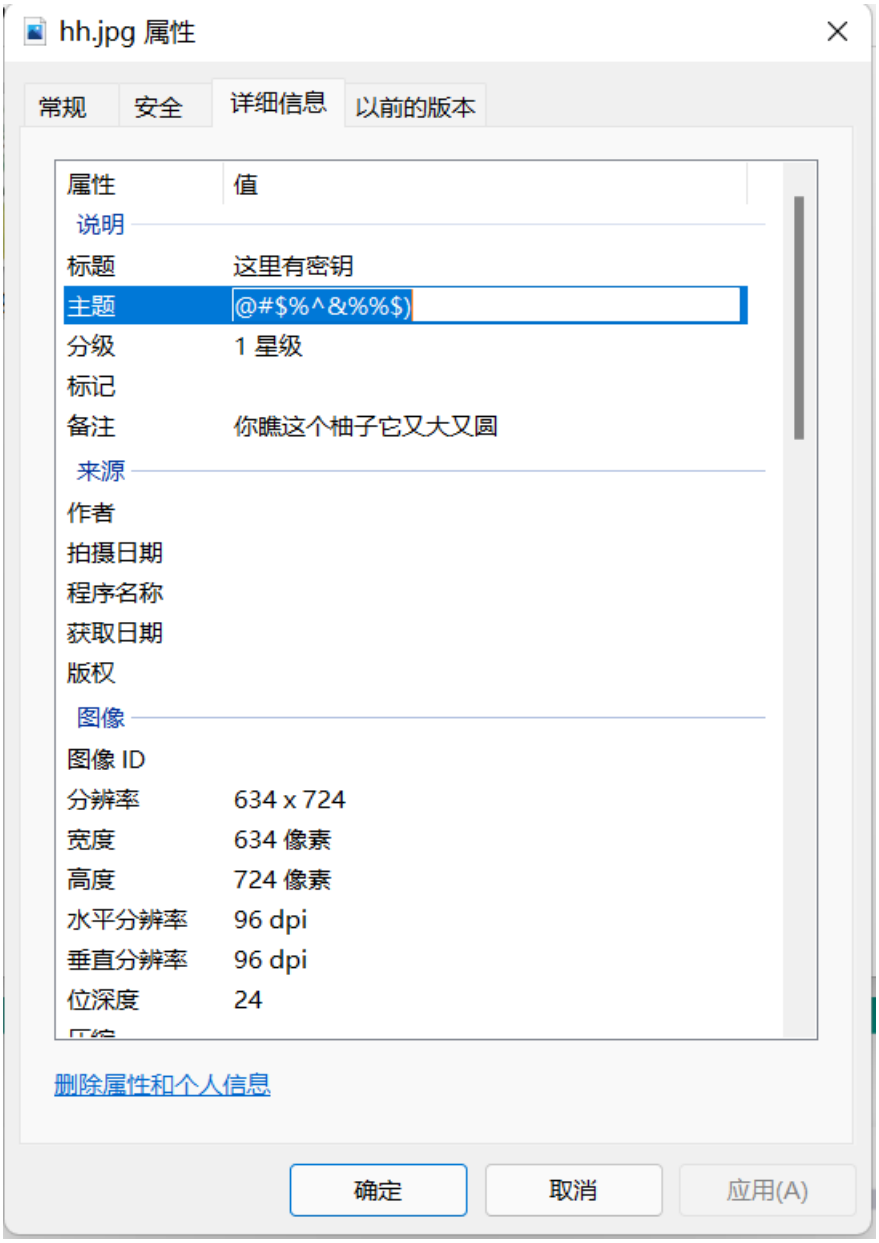
```
./steghide.exe extract -sf hh.jpg
```




```
想要flag吗？解出我的密文吧~
U2FsdGVkX1/7KeHVl5984OsGUVSanPfPednHpK9lKvp0kdrxO4Tj/Q==
```

再找密码

查看属性




```
@#$%^&%%$)
```

解密网址

在线DES加密 | DES解密- 在线工具 (sojson.com)

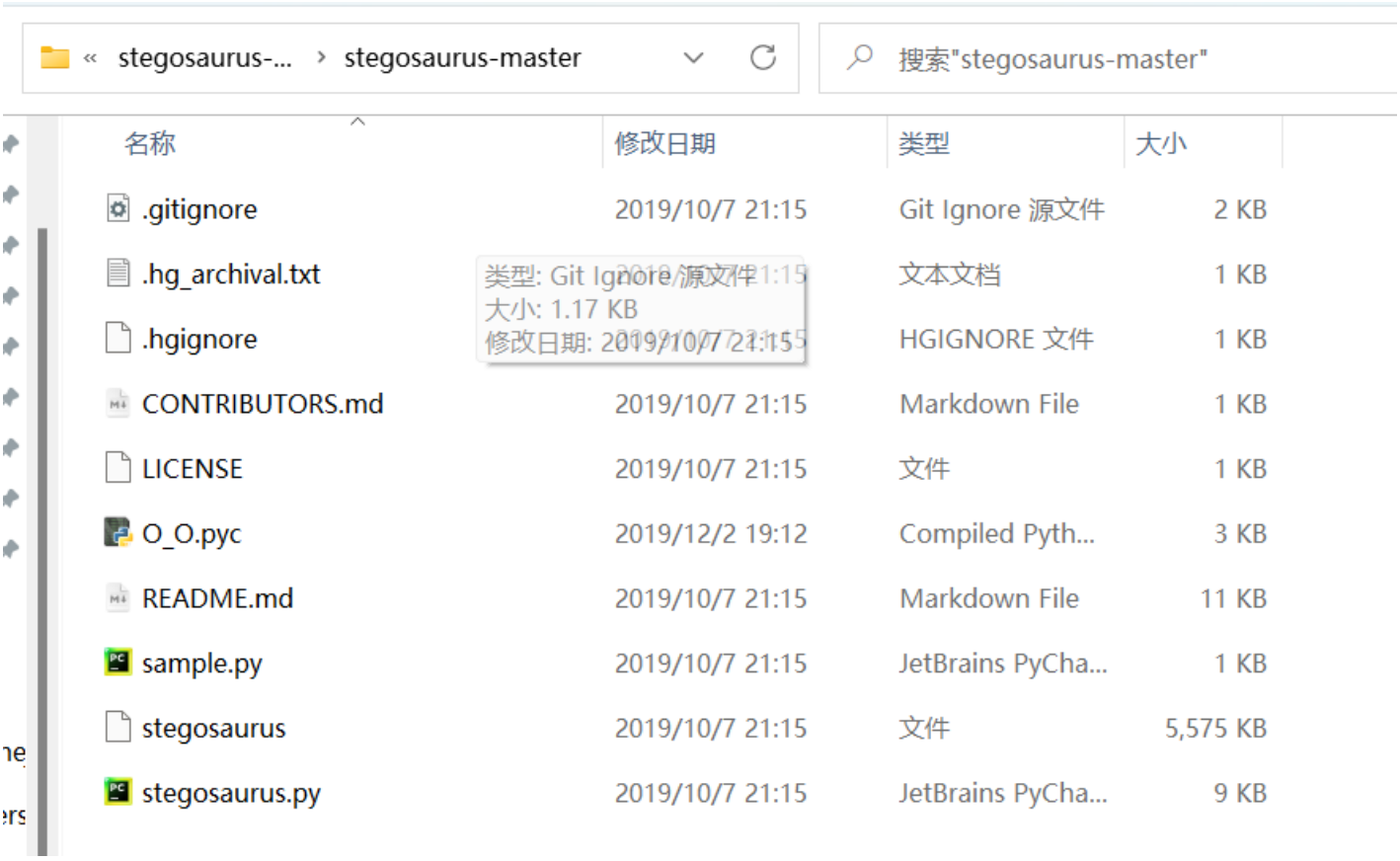
DES 介绍

stegosaurus加密

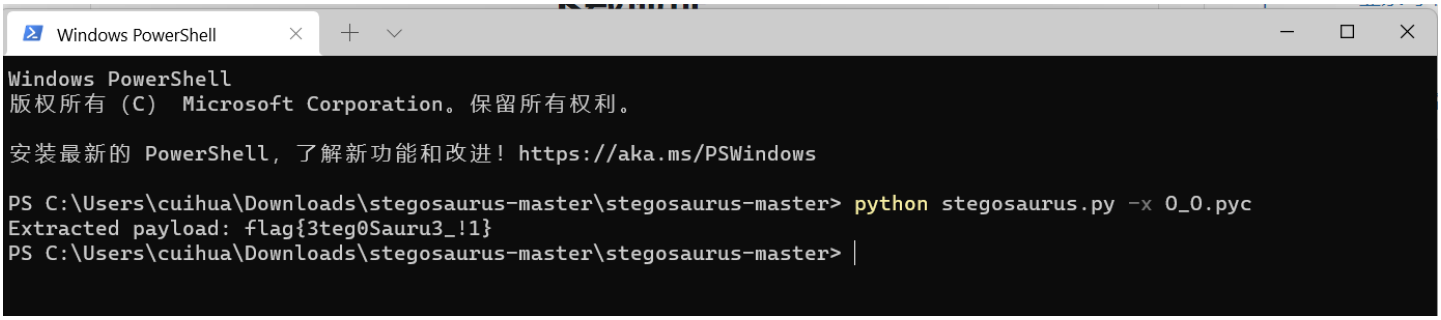
回到前面那个O_O.pyc的文件，使用工具stegosaurus

下载地址

AngelKitty/stegosaurus: A steganography tool for embedding payloads within Python bytecode. (github.com)




```
python stegosaurus.py -x O_O.pyc
```



python版本为3.7.9

3.flag

flag{3teg0Sauru3_!1}

创作打卡挑战赛
赢取流量/现金/CSDN周边激励大奖