重生之这一世我一定要成为合界给木大蛇

天璇Merak招新宣讲 - Misc方向

主讲人：圆周率

其实是一直在群里问解压方法被群主踢出群聊

上一世，你因为功法不足被逐出宗门，凄惨结束了一生。

这一世，你重生了。

你下定决心，

要夺回属于你的一切！

但是

说起来简单做起来难

这一世的你

~~还是不会解压资源~~

(bushi


XX牌日光灯管
π
PiYuanZhouLv
Pi圆周率
DUBHE
MERAK
Bluesbark ISCTF
磁鲨 ISCTF
我要成为 CTF 高手
NewStar
拒绝bug
先打 CTF
谜题先有 npy
2025
开得胜



???

少年，你在愁什么呢？▣

Q.SAVE Q.LOAD SKIP LOG SAVE LOAD CONFIG HIDE



（你看着眼前突然出现的男人，被吓了一跳）▣



你

你……你是谁？！ ▣



圆周率

我？啊，忘记介绍了，我叫圆周率，是古希腊掌管资源的神(自封的) ▣

Q.SAVE Q.LOAD SKIP LOG SAVE LOAD CONFIG HIDE



（你将信将疑，但还是把你重生后的计划说了一遍）▣



圆周率

原来如此，那我可以助你一臂之力！我看你骨骼惊奇，是个打CTF的好苗子，下面这几招可看好了，我只教一遍！

Q.SAVE Q.LOAD SKIP LOG SAVE LOAD CONFIG HIDE

DATA AUTO SAVED.

Chapter 1

第一章：千奇百怪的暗语

Window 1

哦吗吉利椰达呀压哦吗吉利；椰奶龙椰达呀奶椰多南北绿豆。奈诺娜美嘎压南椰达美哪不欧莫季南北绿豆，椰奶龙咋没哒利喵哦吗吉哦吗吉利；奈诺娜美嘎塔奶子哒撸波奈友里西哈基米？库压压友酷欧库路曼波。哈南酷基北库哦吗吉利；奈里基咕南路波压阿西嘎压北绿豆里龙友里呗没撸多；娜美嘎，

Window 2

~呜嗷呜啊呜啊嗷嗷嗷呜啊啊啊啊呜嗷呜啊~~呜~呜~呜嗷嗷啊呜嗷嗷嗷呜
~~嗷~呜呜嗷呜~嗷嗷嗷呜
~呜呜呜嗷啊嗷嗷嗷呜呜呜~
呜呜~~嗷嗷嗷呜啊嗷呜嗷呜
嗷嗷嗷嗷呜啊呜啊~呜嗷呜
嗷嗷呜啊嗷~~呜嗷呜呜~嗷
啊嗷嗷啊呜嗷呜呜~嗷呜嗷
嗷嗷啊呜嗷呜呜~嗷~啊啊嗷
啊~嗷嗷嗷呜呜呜~嗷呜嗷呜呜~嗷啊嗷啊嗷啊呜
嗷嗷嗷呜呜呜呜嗷呜嗷呜呜~呜啊啊啊嗷啊呜嗷
嗷嗷呜啊嗷嗷呜呜嗷呜呜呜啊嗷呜~啊~嗷呜~啊
呜嗷啊呜嗷呜嗷呜呜啊嗷呜~啊嗷啊呜嗷嗷嗷啊~
啊嗷~~呜嗷呜呜~嗷~啊啊嗷啊呜~嗷啊~呜嗷呜啊
啊呜嗷嗷嗷啊~呜~~嗷呜啊啊~嗷~嗷~呜嗷嗷~~
嗷嗷嗷呜啊嗷啊啊呜嗷呜呜~嗷啊嗷啊嗷啊呜嗷嗷啊嗷~嗷~呜呜嗷呜嗷啊

ERROR (x_x)

这都是什么玩意啊！

Window 3

佛又曰：栗瞌陀悉利耶尼怛悉无烁耶穆墀提苏楞咩墀阿呼阿伽夜参写曳孕参那豆数卢耶那楞孕陀参驮提苏室豆伽醢提瞌地瞌呼娑咩耶陀萨谨输穆夜唎烁舍娑楞钵夜伽度室豆楞数唵萨利唎帝那提墀阿佛穆羯提写墀苏他输提参孕摩驮怛帝输迦驮曳他帝呼地谨那诃阇婆室驮娑豆瞌写喝室豆婆罚谨俱罚漫漫

编码/加密

兽音

Ook!

```
.....  .....  .....  .....  !?!!.  ?....  .....  .....  .....  .....  .?.?!
.?...  .!...  .....  .....  !.?..  .....  !?!!.  ?!!!!  !!?.?  !.?!!
!!!..  .....  .....  .!.?.  .....  ...!?  !!.?.  .....  ..?.?  !.?..
.....  .!.!!  !!!!!  !!!!!  !!!.?  .....  ..!?!  !.?!!  !!!!?  .?!.?
!!!!!  !!...  !.?..  .....  !?!!.  ?....  ..?.?  !.?..  !.?..  .....
..!?!  !.?!!  !!!!!  !?.?!  .?!!!  !!!!!  !.?..  .....  !?!!.  ?....
..?.?  !.?..  !.?..  .....  !?!!.  ?....  ..?.?  !.?..  !.?..  .....
..!?!  !.?!!  !!!!!  !?.?!  .?!!!  !!!!!  !....  .!.!!  !!!.?  .....
....!  ?!!.?  .....  ...?.  ?!.?.  .....  ....!  .?...  ....!  ?!!.?
!!!!!  !?.?!  .?!!!  !!!!!  !!!!!  .?...  ....!  ?!!.?  .....  .?.?!
.?...  .....  ..!..  .!.?.  .....  ...!?  !!.?!  !!!!!  !!?.?  !.?!!
!!!!!  !!!!.  .....  .....  ....!  .....  .....  ...!.  ?....  ...!?
!!.?!  !!!!!  ?.?!.  ?!!!!  !....  .....  ....!  .?...  .....  .!?!!
          .?...  .....  ?.?!.  ?....  .....  ...!.  ?.
```

Base64

Zmxh

银河标准文字

The S

Brainfuck

```
      +++++ ++++
 +++++ .<+++ [-
>+++ +<]>+ +++.
.+ .<+++ [->++
.<+++ [->++ +<]
>- ---<] >----
  ++.<+ ++[-> -
  >++++ +.+.< +
  ++.++ ++++. <+++[ ->--- <]>-- .++++ ++.<+
        +++[- >++++ <]>++ ++++. <
```

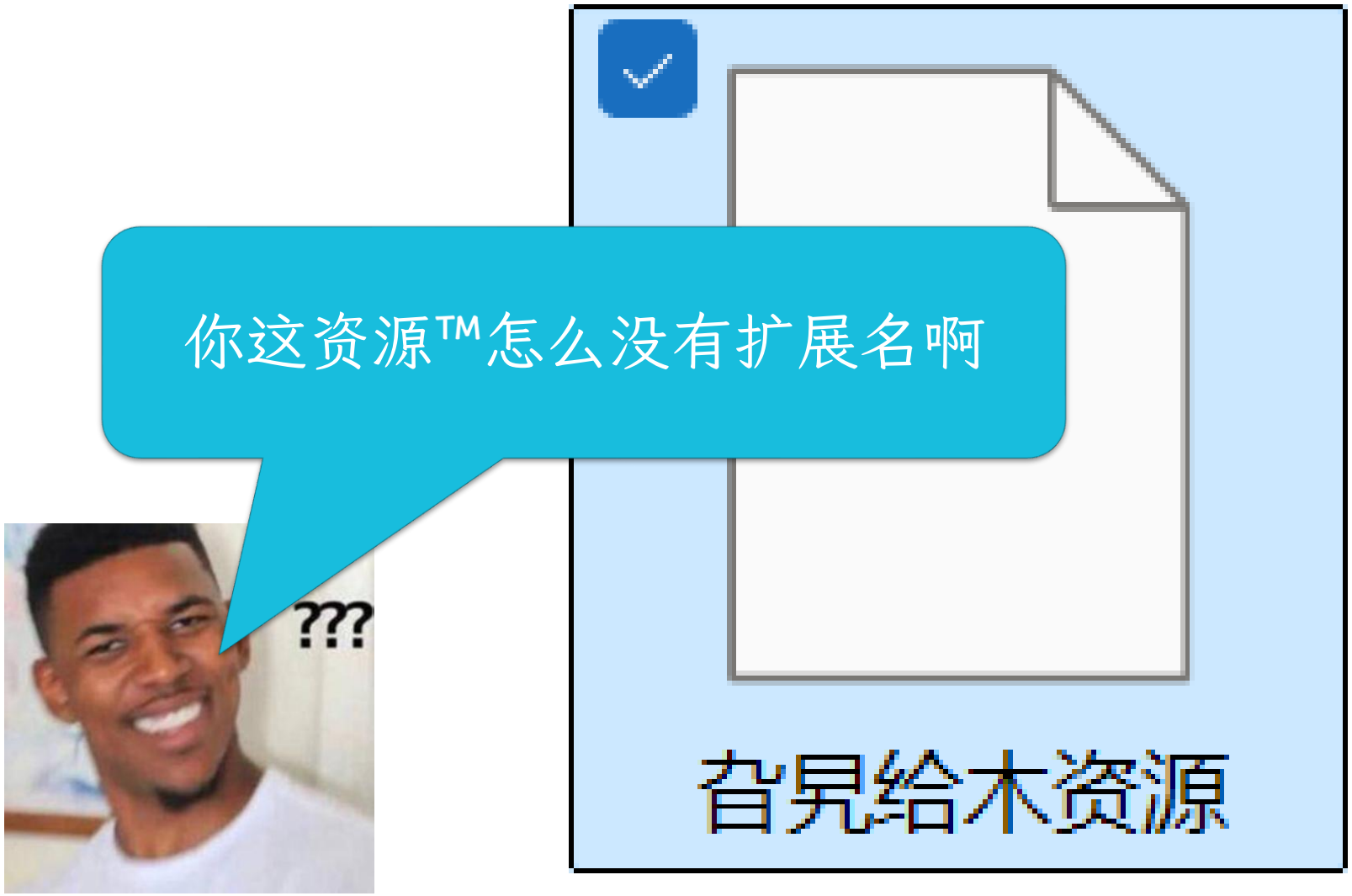
M		T			
N		U			

奶龙；欧莫季里基路一咋哩哇呵西喝压。

Chapter 2

第二章：没有后缀的文件


资源下载中……
SUCCESS
资源下载成功！


你这资源™怎么没有扩展名啊
???
旮旯给木资源



“文件头”

记事本 - 旮見给木资源

PK??? ? ? 桅昜
cli/imhex.batsHM稳W蓑K沐忮*.I,*QP
象?.髻蠋?拎擄s麒/yD?芼]?鏽@9?胱z韓飥
84`h舕鍥笭?蚷\zH泠拗m嫰 D遍6涪>曝??"
g!T€L00Qp6T0tQp2囮啃A睜棕H! ??/?731G
そG?}潺蒘z????rt#`0圖k?v[垃X甖 P
燮??硕??甲?灩-A?D銳?塊?"s?Da?昏

imHex - 旮見给木资源

50	4B	03	04	14	00	08	00	08	00	97	7A	95	5B	00	00	PK.....z.[..
00	00	00	00	00	00	00	00	00	00	0D	00	00	00	63	6C	cl
69	2F	69	6D	68	65	78	2E	62	61	74	73	48	4D	CE	C8	i/imhex.batsHM..
57	C8	4F	4B	E3	E5	E2	E5	2A	2E	49	2C	2A	51	50	52	W.OK....*.I,*QPR
52	50	52	AD	4B	29	30	D0	D3	8B	C9	CC	CD	48	AD	D0	RPR.K)0......H..
4B	AD	48	55	52	50	D5	02	00	50	4B	07	08	D5	F3	51	K.HURP...PK....Q
C8	2E	00	00	00	2C	00	00	00	50	4B	03	04	14	00	08	.....,...PK.....



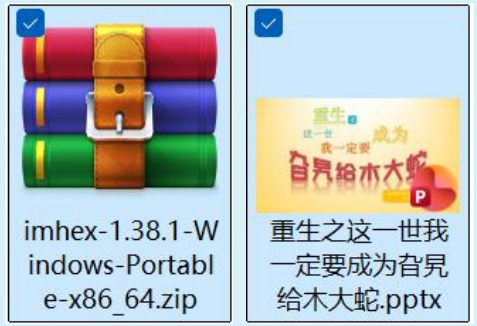

```
89 50 4E 47 0D 0A 1A 0A  00 00 00 0D 49 48 44 52  .PNG........IHDR
00 00 04 00 00 00 04 00  08 06 00 00 00 7F 1D 2B  ...............+
83 00 00 00 01 73 52 47  42 00 AE CE 1C E9 00 00  .....sRGB.......
00 04 67 41 4D 41 00 00  B1 8F 0B FC 61 05 00 00  ..gAMA......a...
00 09 70 48 59 73 00 00  16 25 00 00 16 25 01 49  ..pHYs...%...%.I
52 24 F0 00 00 64 A0 49  44 41 54 78 5E ED DD 4F  R$...d.IDATx^..O
```




```
37 7A BC AF 27 1C 00 04  7D 82 4A 49 3B 04 53 01  7z..'...}.JI;.S.
00 00 00 00 26 00 00 00  00 00 00 00 C7 8F 8D 4F  ....&..........O
00 25 1B C9 07 0D 04 EC  7D C2 56 5E FC 6D 7C 94  .%......}.V^.m|.
AF 03 FA 47 DB 8E 32 26  91 0A A0 B8 83 48 60 8F  ...G..2&.....H`.
20 31 C3 5A D4 2C D6 B2  20 32 9F 86 1D 04 DF 50  1.Z.,.. 2.....P
```

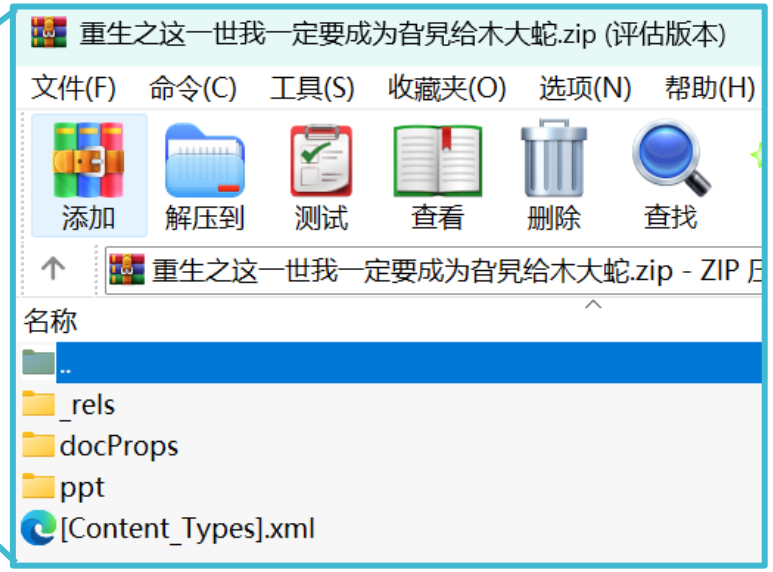



```
4D 5A 90 00 03 00 00 00  04 00 00 00 FF FF 00 00  MZ..............
B8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  ........@.......
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 80 00 00 00  ................
0E 1F BA 0E 00 B4 09 CD  21 B8 01 4C CD 21 54 68  ........!..L.!Th
69 73 20 70 72 6F 67 72  61 6D 20 63 61 6E 6E 6F  is program canno
74 20 62 65 20 72 75 6E  20 69 6E 20 44 4F 53 20  t be run in DOS
6D 6F 64 65 2E 0D 0D 0A  24 00 00 00 00 00 00 00  mode....$.......
50 45 00 00 4C 01 03 00  0A 05 9D BC 00 00 00 00  PE..L...........
```




```
50 4B 03 04 14 00 06 00 08 00 00 00 21 00 96 7D  PK..........!..}
AF 7B 64 02 00 00 B0 1D 00 00 13 00 08 02 5B 43  .{d...........[C
6F 6E 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D  ontent_Types].xm
6C 20 A2 04 02 28 A0 00 02 00 00 00 00 00 00 00  l ...(..........
```







重生之这一世我一定要成为旮旯给木大蛇.pptx

```
└─$ file 重生之这一世我一定要成为旮旯给木大蛇
重生之这一世我一定要成为旮旯给木大蛇: Microsoft PowerPoint 2007+
```



Plain Craft Launcher 2.exe

```
└─$ file PCL
PCL: PE32 executable for MS Windows 6.00 (GUI), Intel i386 Mono/.Net assembly, 3 sections
```



PiYuanZhouLv.png

```
└─$ file PiYuanZhouLv
PiYuanZhouLv: PNG image data, 1024 x 1024, 8-bit/color RGBA, non-interlaced
```

Chapter 3

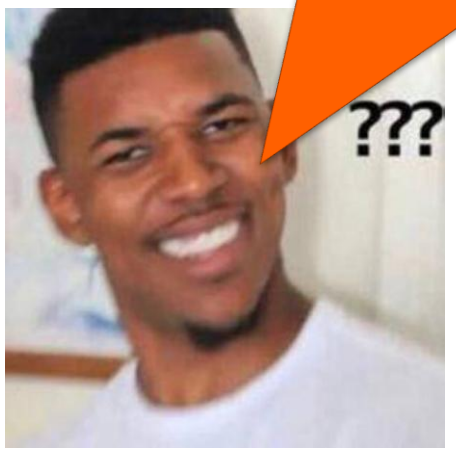
第三章：超超超大的图片



Chapter 3

第三章：超超超大的图片

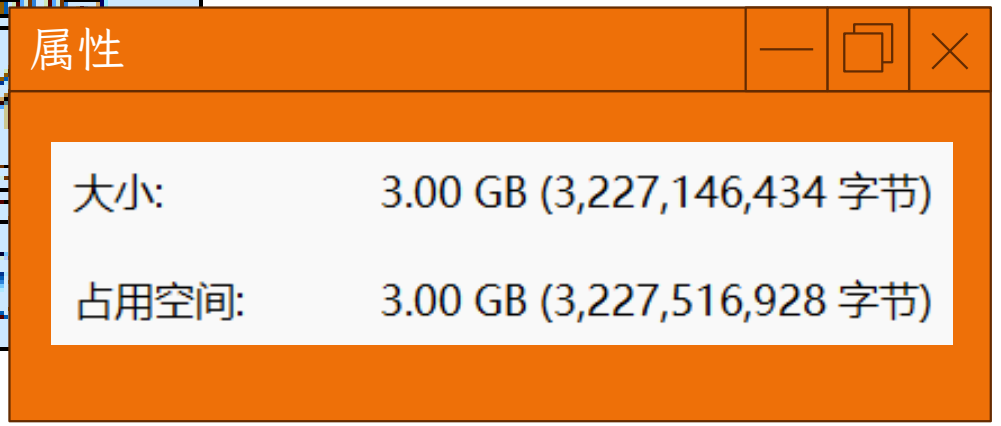




~~你™怎么是小黑子~~
我资源呢？？？



“图种”





以.png结尾

图片



以.zip结尾

压缩包



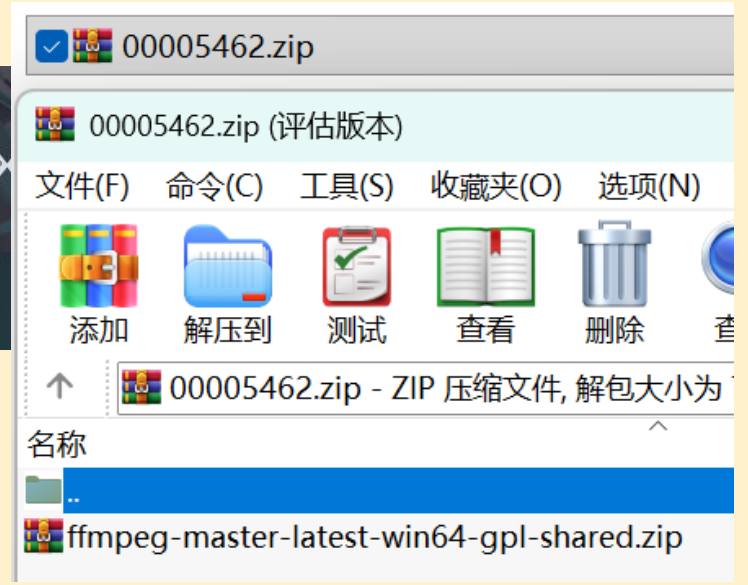
探测：binwalk

```
└─$ binwalk test.mp4

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
106           0x6A            Copyright string: "Copyright 2019-2021 (c) Bilibili Inc"
1849953       0x1C3A61        JBOOT STAG header, image id: 4, timestamp 0xD8B1E34F, image size: 269098951 bytes, image J
BOOT checksum: 0x3FE1, header JBOOT checksum: 0x5D45
2796368       0x2AAB50        YAFFS filesystem root entry, big endian, type symlink, v1 root directory
2796559       0x2AAC0F        Zip archive data, at least v2.0 to extract, compressed size: 72410056, uncompressed size:
72607225, name: ffmpeg-master-latest-win64-gpl-shared.zip
75207028      0x47B9174       RAR archive data, version 5.x
```

提取：foremost

```
└─$ foremost test.mp4
Processing: test.mp4
|foundat=ffmpeg-master-latest-win64-gpl-shared.zip
*|
```



Chapter 4

第四章：未知密码的压缩包


输入密码
为加密的压缩文件输入密码
旮旯给木.rar
输入密码(E)
显示密码(S)
用于所有压缩文件(A)
整理密码(O)...
确定
取消
帮助



你

你……你记得密码是什么，对吗？▣

Q.SAVE Q.LOAD SKIP LOG SAVE LOAD CONFIG HIDE



圆周率

我为什么会去记这种东西…… ▣

Q.SAVE Q.LOAD SKIP LOG SAVE LOAD CONFIG HIDE


输入密码
为加密的压缩文件输入密码
旮旯给木.rar
输入密码(E)
显示密码(S)
用于所有压缩文件(A)
整理密码(O)...
确定
取消
帮助

你

.....▣



圆周率

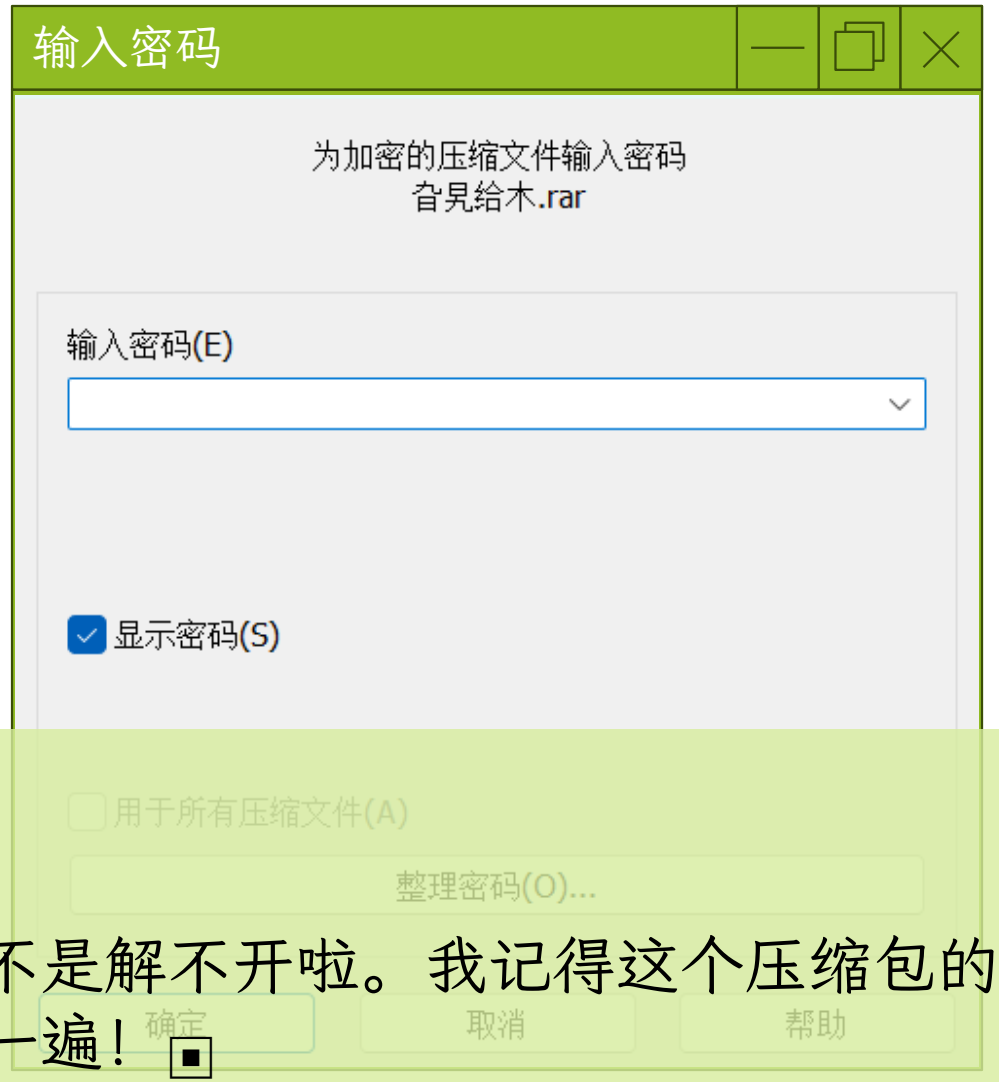
Q.SAVE Q.LOAD SKIP LOG SAVE LOAD CONFIG HIDE



你

呜啊，为什么会这样😭 ▣

Q.SAVE Q.LOAD SKIP LOG SAVE LOAD CONFIG HIDE



圆周率

真拿你没办法，这个也不是解不开啦。我记得这个压缩包的密码是4个大写字母，一下子就好了，我只做一遍！■

Q.SAVE Q.LOAD SKIP LOG SAVE LOAD CONFIG HIDE



你

（这个你怎么记这么清楚……）

Q.SAVE Q.LOAD SKIP LOG SAVE LOAD CONFIG HIDE


输入密码
为加密的压缩文件输入密码
旮旯给木.rar
输入密码(E)
显示密码(S)
用于所有压缩文件(A)
整理密码(O)...
确定
取消
帮助



$$26^4 = 45\,6974$$

密钥空间比较小，可以枚举爆破！

John the Ripper

Hashcat

John the Ripper是一个爆破密码的工具，本身支持字典方式攻击，其中的xxx2john小工具群可以提取hash供hashcat使用





Hashcat是一个哈希爆破工具，支持字典、掩码等多种方式攻击，以及攻击md5、zip等一系列哈希恢复密钥，具有GPU算法加速破解





DATA AUTO SAVED.

The end

尾声：旅程还在继续……

Q.SAVE Q.LOAD SKIP LOG SAVE LOAD CONFIG HIDE

The end

尾声：旅程还在继续……



圆周率的设定图(大雾)

[Q&A]

> 提 问 环 节 <

圆周率の联系方式

QQ: 3610666396

Github: PiYuanZhouLv

Blog: https://piyuanzhoulv.github.io/

* 欢迎交流讨论~