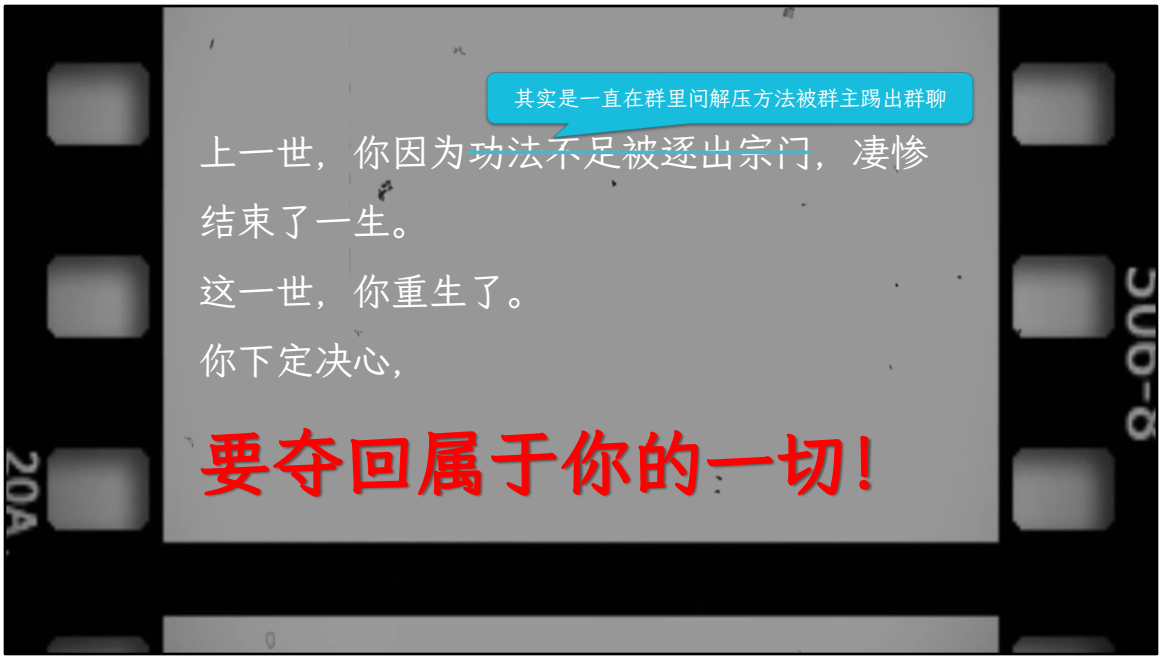


欢迎来到天璇战队招新宣讲，我是Misc方向的主讲人：圆周率
经常找旮旯给木资源的同学可能会知道，为了防止资源被和谐，人们想出了很多方法。这些方法很大一部分都和我们CTF的Misc方向是一致的。今天，就让我们从“找资源”这个角度切入，学习其中的Misc知识！


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


π
PiYuanZhouLv
Pi圆周率
DUBHE
MERAK
NewStar
GAME
2025



???

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）▣

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



你

你……你是谁？！ ▣

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



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）▣

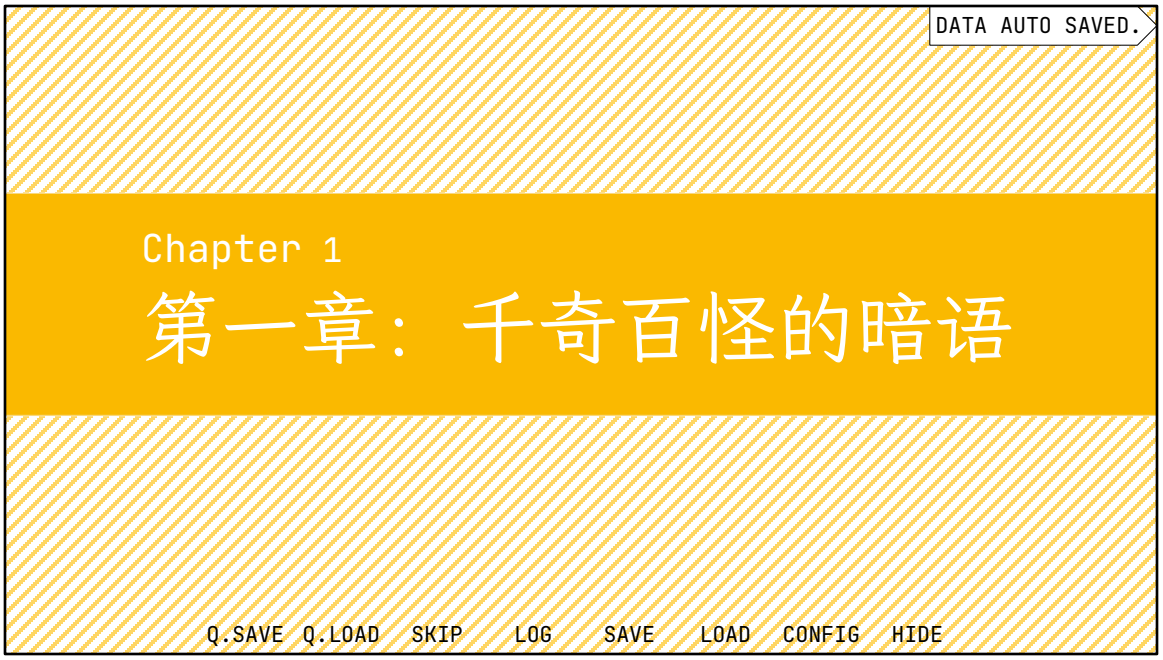
Q.SAVE Q.LOAD SKIP LOG SAVE LOAD CONFIG HIDE



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！

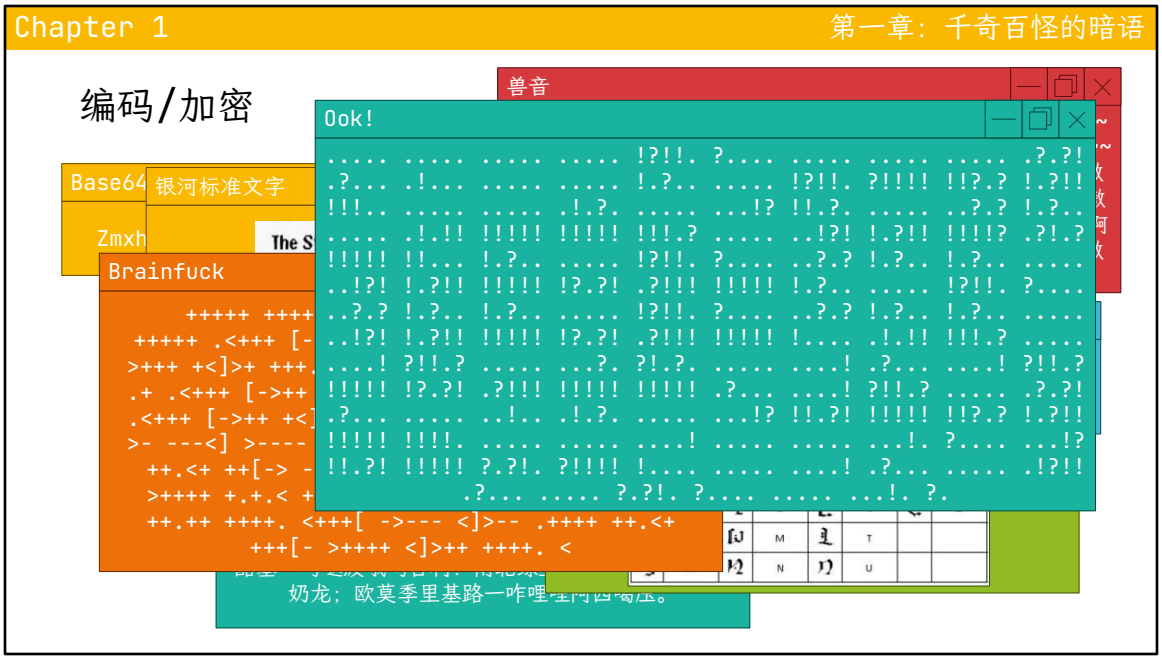
Q.SAVE Q.LOAD SKIP LOG SAVE LOAD CONFIG HIDE



那么，我们进入第一章：千奇百怪的暗语



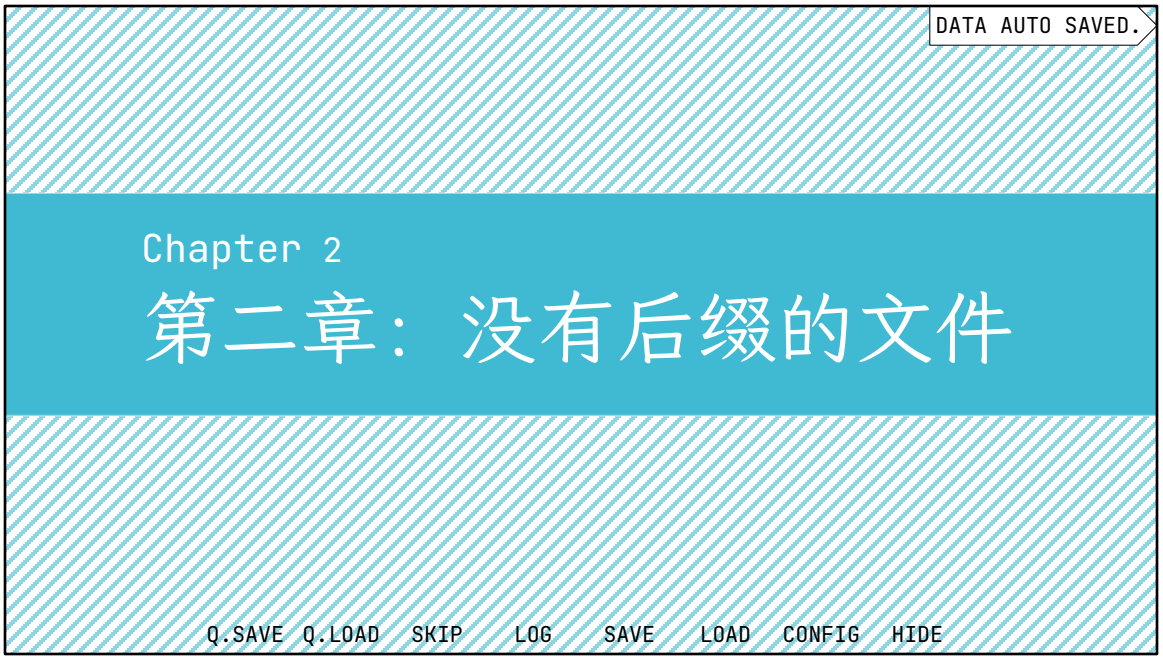
你凭借着信息搜集技能，很快在互联网的角落找到了大量的资源链接，但接下来你就犯了难，因为所有的链接是【点】这样的、【点】这样的、还有【点】这样的……【点】“这都是些什么玩意儿啊！”咳咳，不要着急【点，然后继续念】，这就是我们Misc常见的“编码/加密”【等待动画结束】



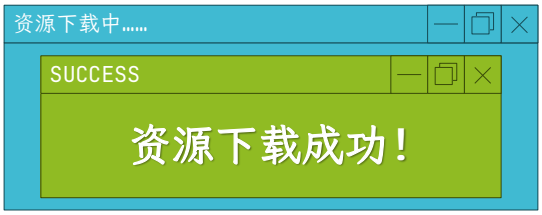
所谓编码，就是“把信息从一种形式或格式转换为另一种形式”。但我们有时候会遇到一些简单的可以填写密钥的自定义加密，由于在Misc中与编码类似，所以我把他们放到了一起。

CTF中常见的编码有：【点】Base64、【点】十六进制编码，常见的加密比如【点】ROT13；在旮旯给木资源链接加密中常见、偶尔也会出现在Misc当中的编码，比如【点】哈基米、【点】兽音、【点】与佛论禅；此外，我们还有可能会遇到人造文字，由于与编码类似，也归到这一类，比如【点】银河标准文字（MC的附魔台就是这种文字），甚至说【点】原神里的文字；另外还有esolang，这是对一些古怪语言的统称，也有编码的特性，例如【点】Brainfuck、【点】Ook!……Misc中的编码种类繁多，千奇百怪，但是大部分都有特点，见过了就不容易忘。

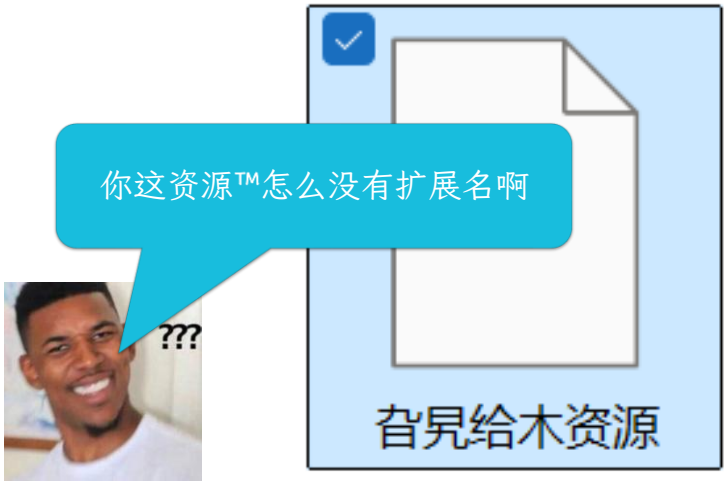
讲了这么多，下面就来看一个例子演示一下（演示时可以简单插入一下新/旧与佛论禅的事）。



解开了千奇百怪的密语后，你获得了资源的网盘网址，开始下载【点】



【将要出现弹窗时】但当下载完成后……看到的却是



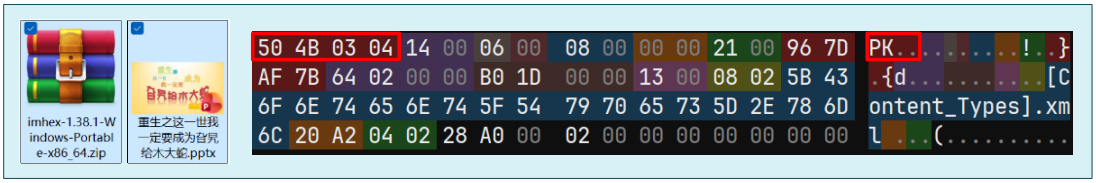
你这资源™怎么没有扩展名啊!
不过不要紧，没有扩展名，我们仍然可以根据文件内容推断出文件类型：

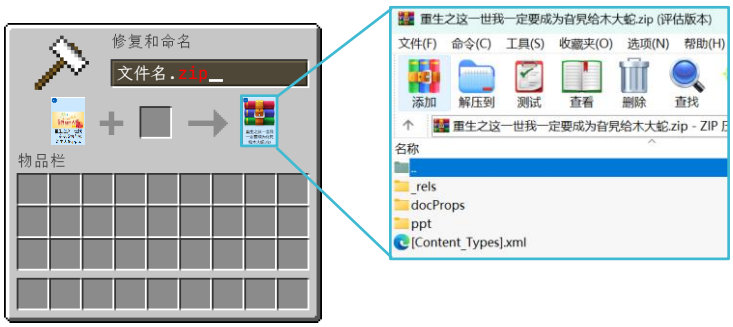


如果你用【点】记事本打开，或者，更专业地，使用【点】十六进制编辑器打开，你就会在大量的不可见字符中找到少量的可见字符，其中，【点】注意这个“PK”，确切说，是“PK”和后面不可见的“0304”。这是ZIP的特征。由于这种特征通常出现在文件开头起标识文件类型的作用，称为【点】“文件头”。
不止ZIP，其他很多文件类型都有对应的文件头：



比如PNG，在开头是"\x89PNG"；
7z，在开头是"7z\xBC\xAF\x27\x1C"；
exe也有明显的标识，虽然exe实际上的文件头是第一行的“MZ”和图片最后一行的“PE”，但是“This program cannot be run in DOS mode.”这个更为明显，也更常用……

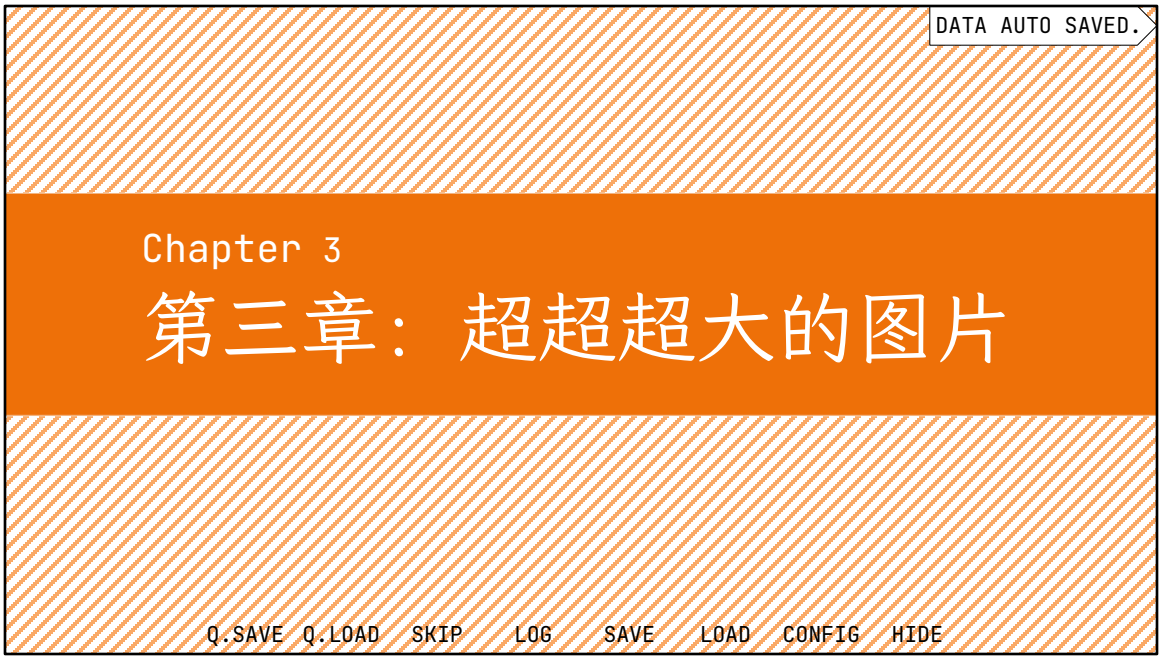




通过文件头，我们还可以看见一些文件的本质，比如pptx的开头同样有PK\x03\x04的文件头，说明pptx的实质就是ZIP文件；用铁砧（？）把pptx的扩展名改成zip，就可以用压缩软件打开，里面可以看到PPT内嵌入的媒体。不止pptx，还有很多文件类型的实质其实都是ZIP文件，大家可以多留意一下。既然这么多文件头，有没有什么好方法来分析文件类型呢？有的有的：



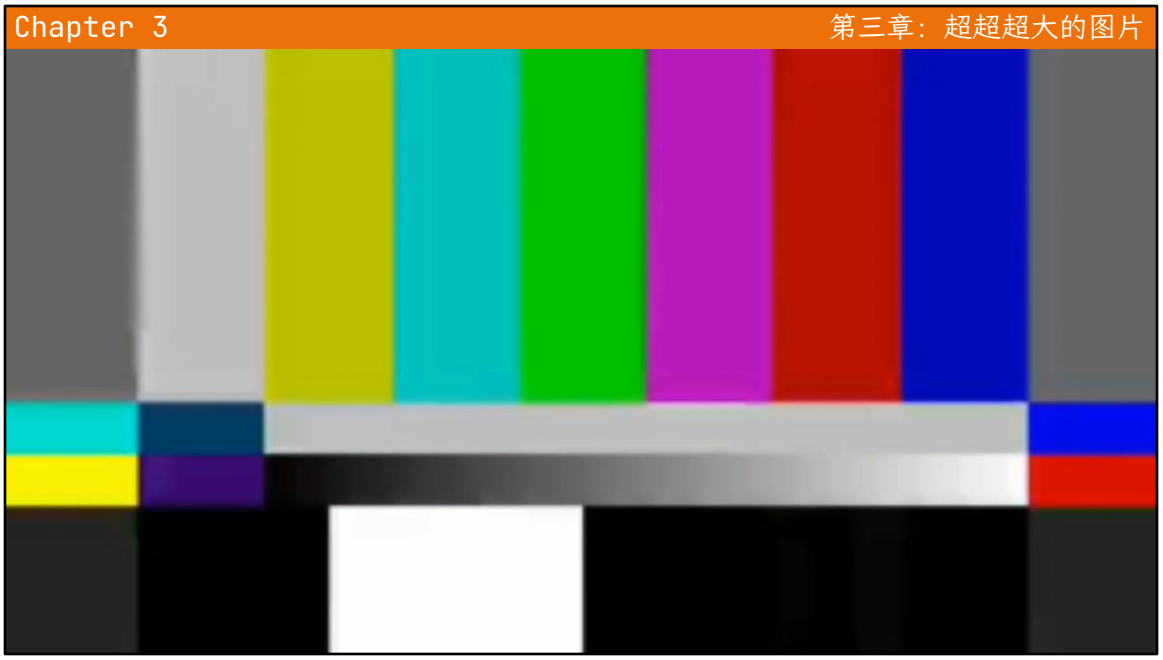
Linux操作系统下有一个“file”指令就是通过文件头来分析文件类型的。如PPT所示，file指令在扩展名缺失的情况下成功识别出了这三个文件对应的文件类型，还给出了一些额外的信息。



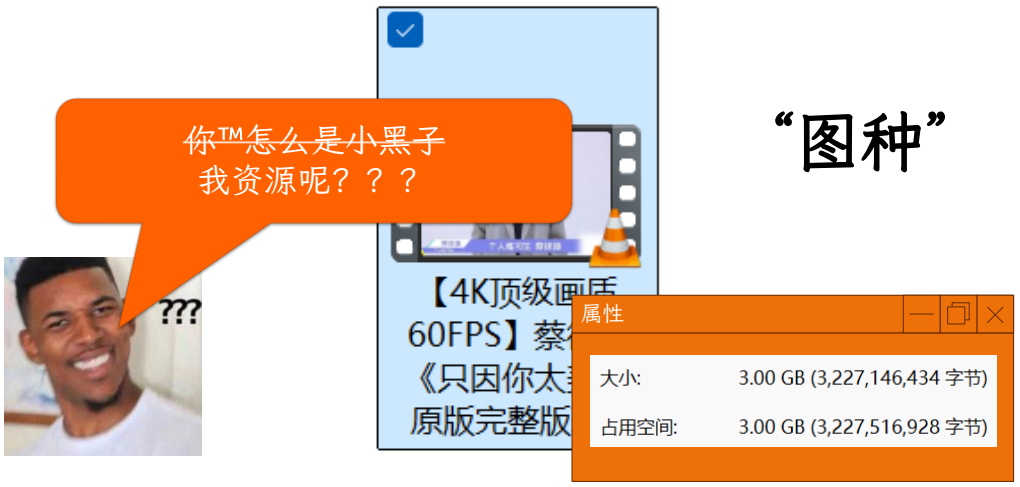
在文件头的帮助下，你恢复了文件的扩展名，开始解压……



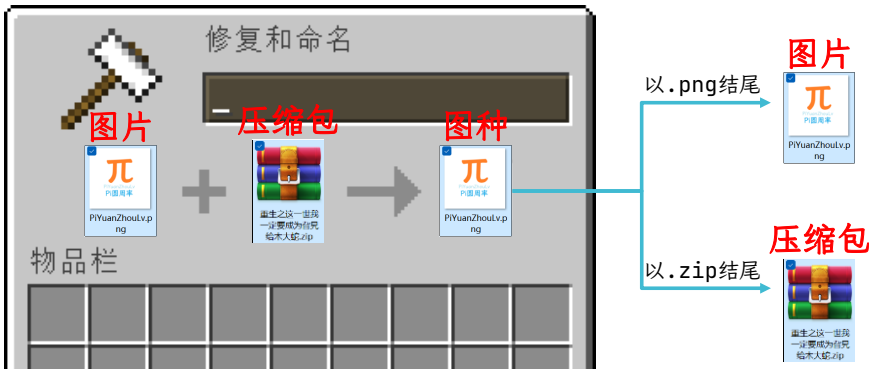
【将要弹窗时】不过当解压完成后，你看到的却是……



【哔——】



欸不是。我资源呢？？？就当你觉得被骗的时候，你敏锐地发现：这再怎么4K再怎么60FPS再怎么顶级画质，【点】你这视频也不可能3个G吧。这就是传说中的【点】“图种“技术



图种，简单来说，就是把【点】一张图片和【点】一个压缩包【点】合并到一块，得到的文件【点】在png扩展名下就是图片，【点】在zip扩展名下就是压缩包。

得益于文件头，我们可以恢复扩展名，同样得益于文件头，我们有了图种技术。还记得文件头之所以叫”文件头“是因为其一般在文件开头，对吧。所以文件头就可以作为文件开始的标识，这就允许了文件在文件头之前可以有一些其他数据。同样的文件，图片查看器就会读取图像的部分，压缩软件就会读取压缩文件部分，二者互不干扰。

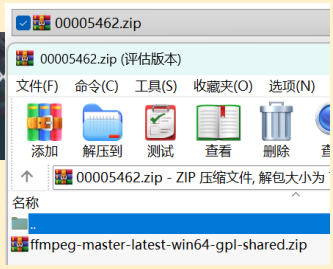
探测：binwalk

```
└─$ binwalk test.mp4

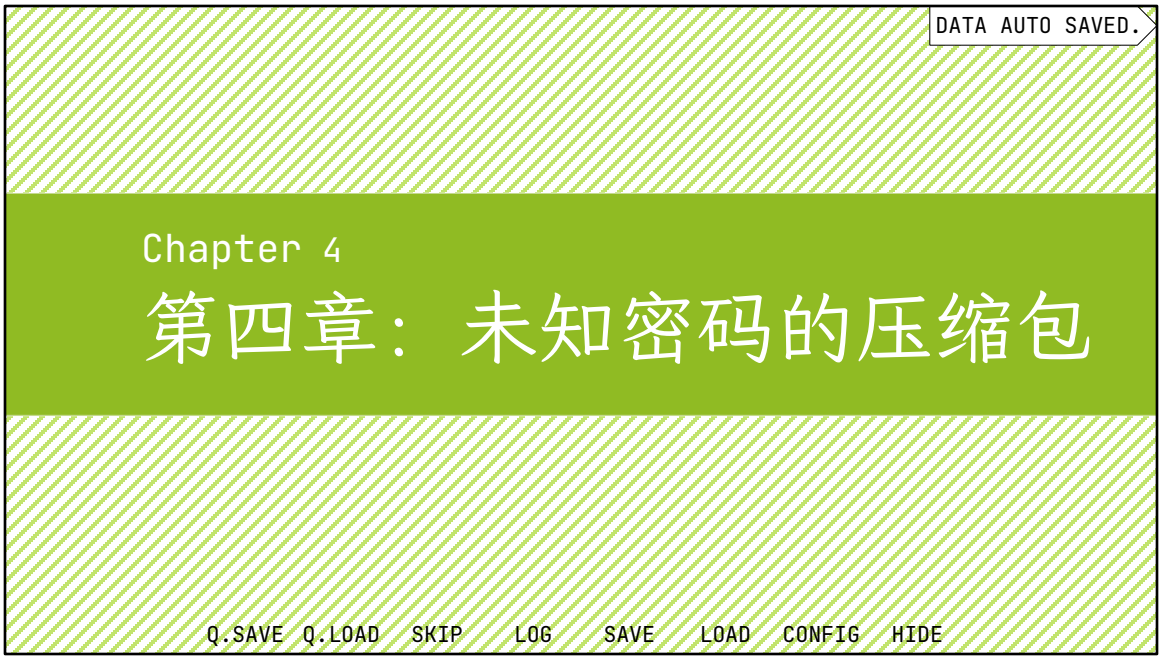
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
106           0x6A            Copyright string: "Copyright 2019-2021 (c) Bilibili Inc"
1849953       0x1C3A61        JBOOT STAG header, image id: 4, timestamp 0xD8B1E34F, image size: 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
```



在Misc题中，我们常用Linux下的”binwalk“指令检测这类文件，用”foremost“指令分离提取各部分文件。当然，从使用的角度来讲，其实改一个扩展名就可以啦。



从视频里提取了压缩包，最后只要解压就可以玩旮旯给木了……吗？


输入密码
为加密的压缩文件输入密码
奋晃给木.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

Chapter 4 第四章：未知密码的压缩包



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

Chapter 4 第四章：未知密码的压缩包



你

.....▣

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

Chapter 4 第四章：未知密码的压缩包



圆周率

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

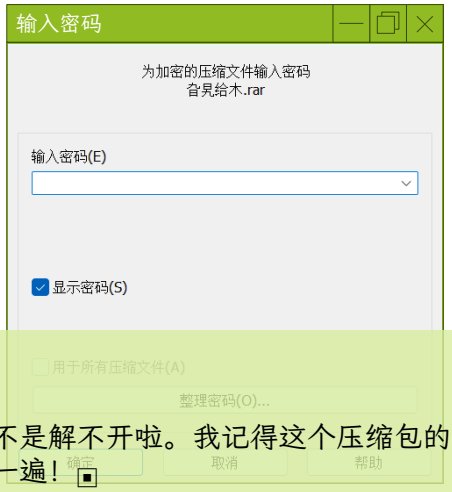
Chapter 4 第四章：未知密码的压缩包



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
奋晃给木.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

由于密码仅由4个大写字母构成，密钥空间较小，可以直接枚举爆破。在这里，我们需要用到两个软件：【点】John the Ripper和【点】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





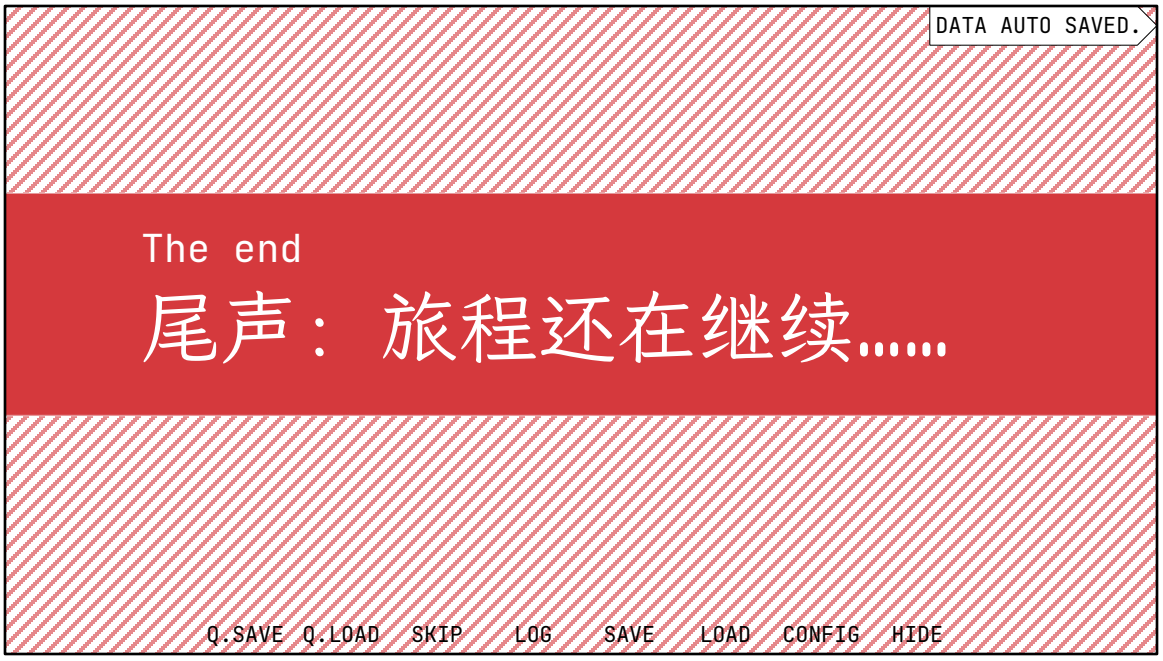
读完文本后就进行演示

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





也是读完文本后就进行演示



好了，我们的Misc之旅就要先告一段落了

The end 尾声：旅程还在继续……

读一下字幕



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~

自由提问时间!