隐写术 简单zip隐写(秘密藏在了哪里)

原创

幸运之河 于 2021-04-10 15:50:11 发布 1058 收藏 9

分类专栏： 隐写术 文章标签： 隐写术 zip

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/xinyue9966/article/details/115576047

版权

隐写术 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

前言

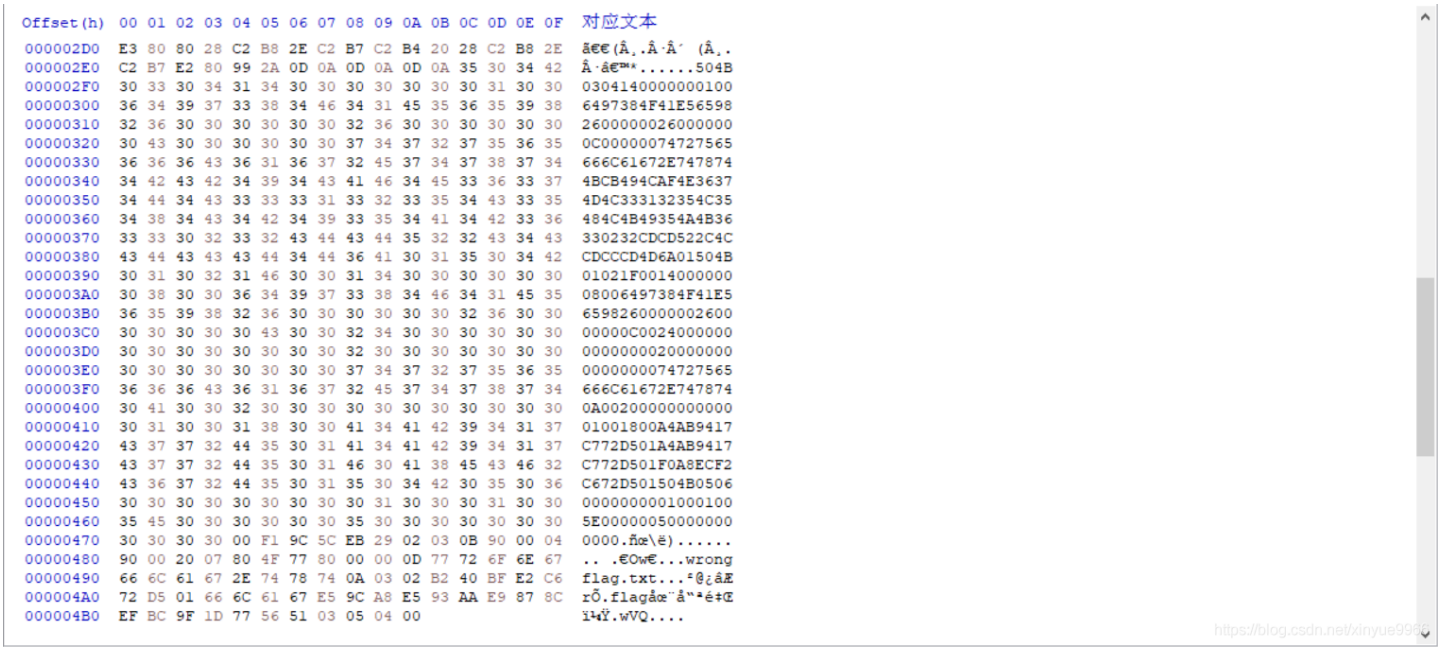
原文件:

链接：https://pan.baidu.com/s/1tZxxO1lHM1sRCz7hq_tySQ

提取码：j7k3

前天一个朋友深夜找我破解一个隐写术的题目，看了一遍复现步骤很简单，是一个关于zip破解的问题，先看下使用软件，WinRAR，HxD，备全即可，从WinRAR看到16进制数

使用HxD进行打开查看，zip格式可以更改文件加密显示，在HxD中更改文件后缀格式为.zip



发现了显示位数，那前面的代表数分别是什么意思呢，需要去看下zip文件构成

```
<strong>一个 ZIP 文件由三个部分组成：</strong>

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
<strong>
压缩源文件数据区：</strong>
50 4B 03 04：这是头文件标记（0x04034b50）
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
5A 7E：最后修改文件时间
F7 46：最后修改文件日期
16 B5 80 14：CRC-32校验（1480B516）
19 00 00 00：压缩后尺寸（25）
17 00 00 00：未压缩尺寸（23）
07 00：文件名长度
00 00：扩展记录长度
6B65792E7478740BCECC750E71ABCE48CDC9C95728CECC2DC849AD284DAD0500<br>
<strong>压缩源文件目录区：</strong>
50 4B 01 02：目录中文件文件头标记(0x02014b50)
3F 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）
08 00：压缩方式
5A 7E：最后修改文件时间
F7 46：最后修改文件日期
16 B5 80 14：CRC-32校验（1480B516）
19 00 00 00：压缩后尺寸（25）
17 00 00 00：未压缩尺寸（23）
07 00：文件名长度
24 00：扩展字段长度
00 00：文件注释长度
00 00：磁盘开始号
00 00：内部文件属性
20 00 00 00：外部文件属性
00 00 00 00：局部头部偏移量
6B65792E7478740A002000000000000010018006558F04A1CC5D001BDEBDD3B1CC5D001BDEBDD3B1CC5D001<br><strong>
压缩源文件目录结束标志：</strong>
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
```

全局方式位标记如果第二位是偶数，那么就不加密，反之，如果是奇数的话，就是加密的

复现

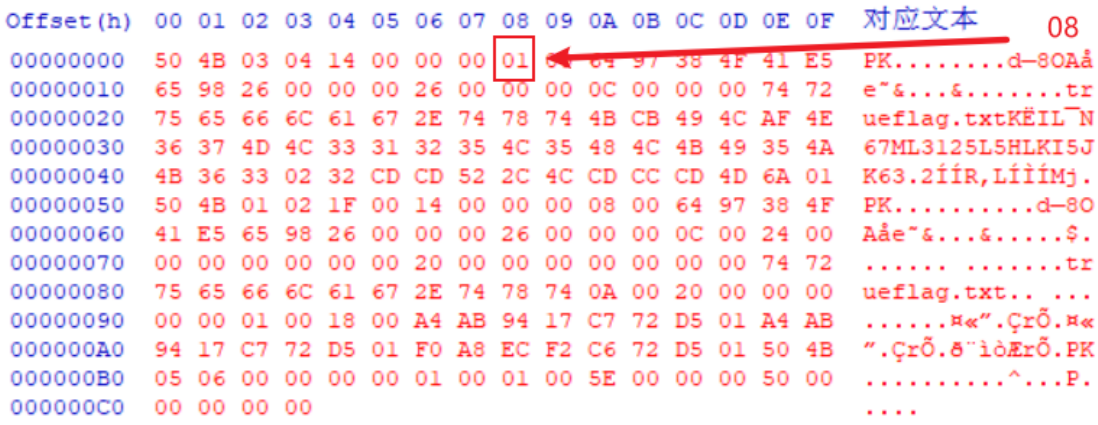
我们把16进制数复制到源文件左边，更改替换

flag.zip

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	对应文本
00000000	50	4B	03	04	14	00	00	00	01	00	64	97	38	4F	41	E5	PK.....d—8OAå
00000010	65	98	26	00	00	00	26	00	00	00	0C	00	00	00	74	72	e˜&...&.....tr
00000020	75	65	66	6C	61	67	2E	74	78	74	4B	CB	49	4C	AF	4E	ueflag.txtKËIL¯N
00000030	36	37	4D	4C	33	31	32	35	4C	35	48	4C	4B	49	35	4A	67ML3125L5HLKI5J
00000040	4B	36	33	02	32	CD	CD	52	2C	4C	CD	CC	CD	4D	6A	01	K63.2ÍÍR,LÍÌÍMj.
00000050	50	4B	01	02	1F	00	14	00	00	00	08	00	64	97	38	4F	PK.....d—8O
00000060	41	E5	65	98	26	00	00	00	26	00	00	00	0C	00	24	00	Aåe˜&...&.....$.
00000070	00	00	00	00	00	00	20	00	00	00	00	00	00	00	74	72	....tr
00000080	75	65	66	6C	61	67	2E	74	78	74	0A	00	20	00	00	00	ueflag.txt.. ...
00000090	00	00	01	00	18	00	A4	AB	94	17	C7	72	D5	01	A4	AB	.....¤«”.ÇrÕ.¤«
000000A0	94	17	C7	72	D5	01	F0	A8	EC	F2	C6	72	D5	01	50	4B	”.ÇrÕ.ð¨ìòÆrÕ.PK
000000B0	05	06	00	00	00	00	01	00	01	00	5E	00	00	00	50	00	.....^...P.
000000C0	00	00	00	00													....

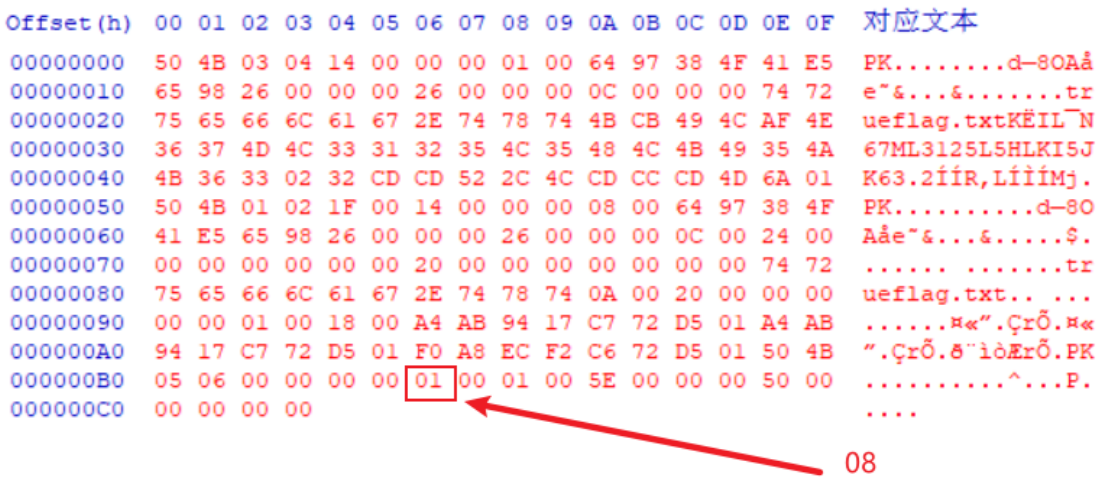
https://blog.csdn.net/xinyue9966

看到压缩源文件数据区开始50 4B 03 04是头文件标记，14 00是解压文件所需 pkware 版本，00 00是扩展记录长度，01 00是全局方式位标记（有无标记），01是加密标记，确认第一位改成任意偶数即可



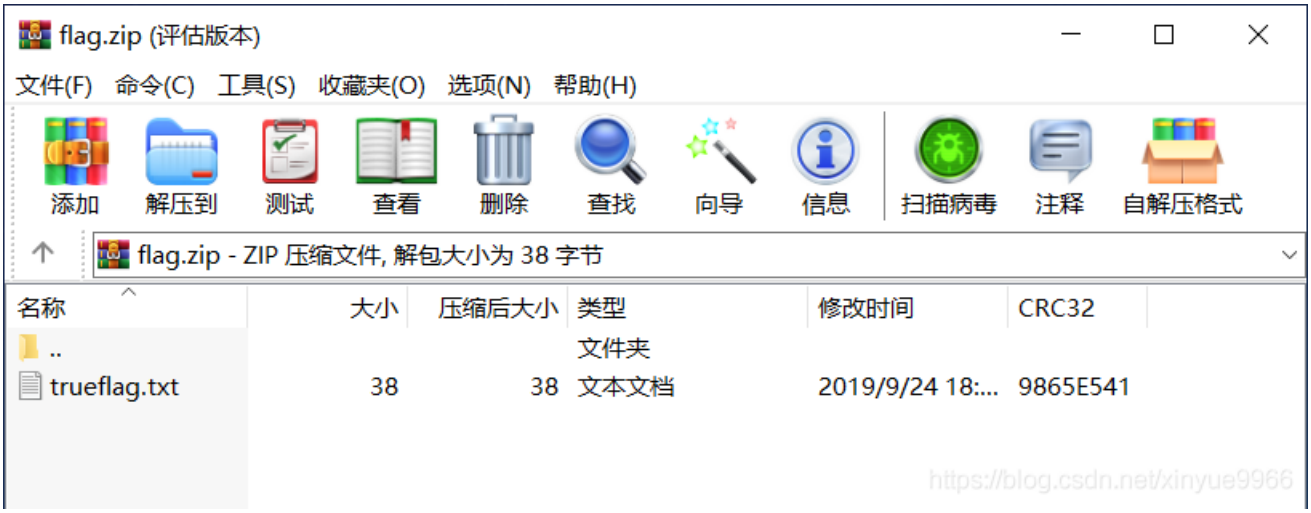
https://blog.csdn.net/xinyue9966

继续查看压缩源文件目录结束标志尾部，50 4B 05 06是目录结束标记，第一个00 00是当前磁盘编号，第二个00 00是目录区开始磁盘编号，01 00是同样为加密位修改成和全局方式标记位相同偶数即可



https://blog.csdn.net/xinyue9966

保存HxD支持Ctrl+s，完成后再次使用WinRAR打开保存后的flag.zip即可查看到true flag



https://blog.csdn.net/xinyue9966

同样此题支持一些java编写的脚本工具，去直接获得内在文件

后记

zip解密往往伴随着十六进制再次转换格式,可能得到的文件里面内嵌16进制转换为jpg、png等图片格式的代码，需要拼接或者转换，可以参考下一个老哥的解密png过程

> zip隐写术

喜欢的话不要吝啬一个点赞哦！