ZIP文件格式组成

转载

online_kns 于 2016-07-19 20:24:04 发布 5602 收藏 7
文章标签： ZIP 文件组成

今天在实验吧看了一道隐写题 ：

http://www.shiyanbar.com/ctf/716

把图片下载来，就使用binwalk～～发现有一个压缩文件zip格式的提取出来，加密了然后用aarp进行解密。。。没任何结果。。

没有头绪

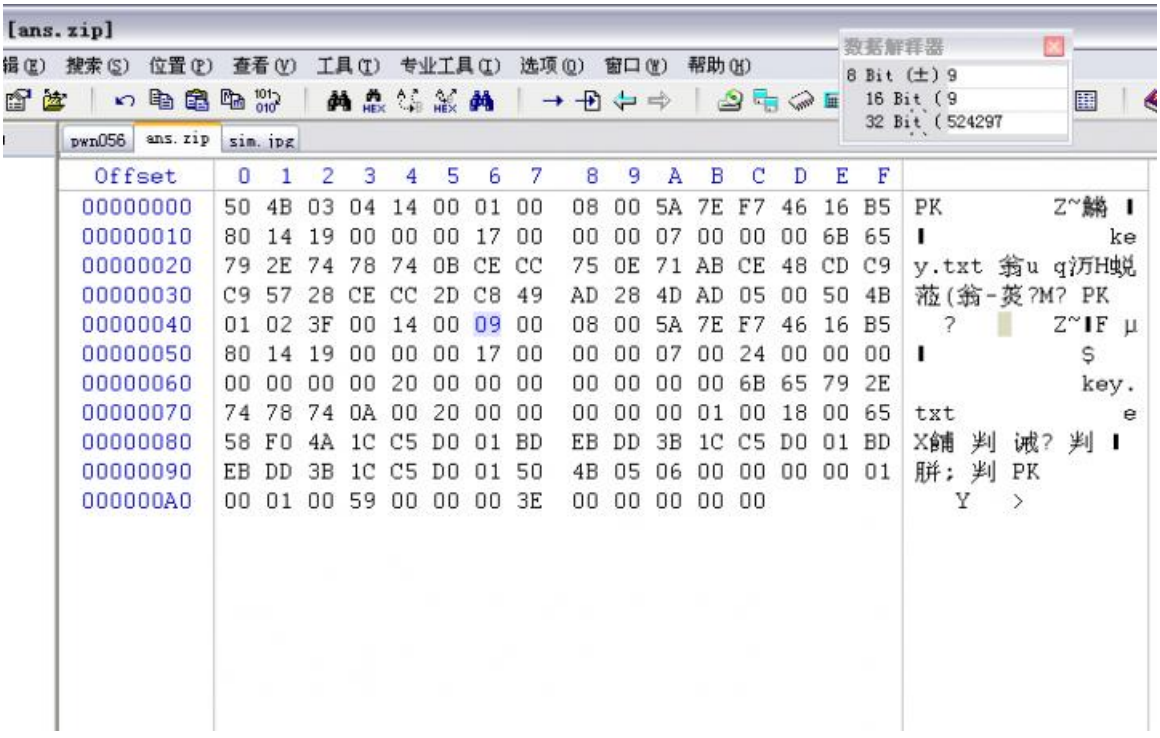
没有头绪

。。

看属性 winhex..无果

只能看writeup了

打开之后有密码，载入winhex看看，发现伪加密



把09改为00

就可以打开了

接下来分析下这个zip的文件16进制格式

压缩源文件数据区

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

压缩源文件目录区

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

6B65792E7478740A00200000000000001001800655 8F04A1CC5D001BDEBDD3B1CC5D001BDEBDD3B1CC5D001

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