东华杯-Misc250-面具-writeup（zip伪加密）

原创

n4nch3ng 于 2016-11-19 14:56:41 发布 2064 收藏

分类专栏： misc 文章标签： zip伪加密 ctf

本文链接：https://blog.csdn.net/fuzz_nancheng/article/details/53230389

版权

misc 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

三步：提取-分析-解密

第一步：提取

压缩包加密有一种伪加密的方法，首先我们需要先了解一下zip文件的格式信息。

一个 ZIP 文件由三个部分组成：

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

其中：

压缩源文件目录区：

50 4B 01 02：目录中文件文件头标记(0x02014b50)

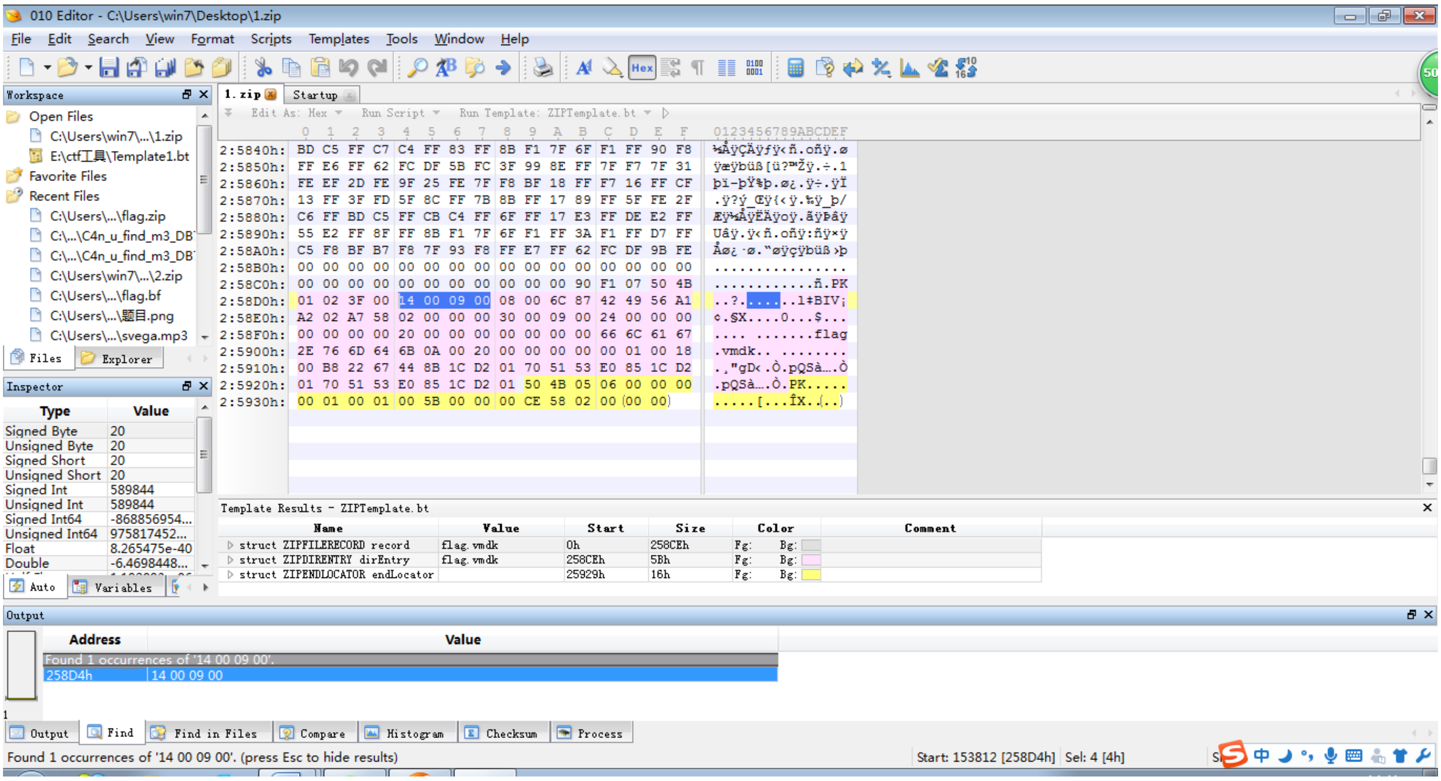
3F 00：压缩使用的 pkware 版本

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

我们用010editor打开压缩包，搜索14 00 09 00，发现果然存在



Type	Value
Signed Byte	20
Unsigned Byte	20
Signed Short	20
Unsigned Short	20
Signed Int	589844
Unsigned Int	589844
Signed Int64	-868856954...
Unsigned Int64	975817452...
Float	8.265475e-40
Double	-6.4698448...

```
           0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
2:5840h:  BD C5 FF C7 C4 FF 83 FF 8B F1 7F 6F F1 FF 90 F8   ½ÅÿÇÄÿƒÿ‹ñ.oñÿ.ø
2:5850h:  FF E6 FF 62 FC DF 5B FC 3F 99 8E FF 7F F7 7F 31   ÿæÿbüß[ü?™Žÿ.÷.1
2:5860h:  FE EF 2D FE 9F 25 FE 7F F8 BF 18 FF F7 16 FF CF   þï-þŸ%þ.ø¿.ÿ÷.ÿÏ
2:5870h:  13 FF 3F FD 5F 8C FF 7B 8B FF 17 89 FF 5F FE 2F   .ÿ?ý_Œÿ{‹ÿ.‰ÿ_þ/
2:5880h:  C6 FF BD C5 FF CB C4 FF 6F FF 17 E3 FF DE E2 FF   Æÿ½ÅÿËÄÿoÿ.ãÿÞâÿ
2:5890h:  55 E2 FF 8F FF 8B F1 7F 6F F1 FF 3A F1 FF D7 FF   Uâÿ.ÿ‹ñ.oñÿ:ñÿ×ÿ
2:58A0h:  C5 F8 BF B7 F8 7F 93 F8 FF E7 FF 62 FC DF 9B FE   Åø¿·ø.“øÿçÿbüß›þ
2:58B0h:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2:58C0h:  00 00 00 00 00 00 00 00 00 00 00 90 F1 07 50 4B   ............ñ.PK
2:58D0h:  01 02 3F 00 14 00 09 00 08 00 6C 87 42 49 56 A1   ..?.......l‡BIV¡
2:58E0h:  A2 02 A7 58 02 00 00 00 30 00 09 00 24 00 00 00   ¢.§X....0...$...
2:58F0h:  00 00 00 00 20 00 00 00 00 00 00 00 66 6C 61 67   .... .......flag
2:5900h:  2E 76 6D 64 6B 0A 00 20 00 00 00 00 00 01 00 18   .vmdk.. ........
2:5910h:  00 B8 22 67 44 8B 1C D2 01 70 51 53 E0 85 1C D2   .¸"gD‹.Ò.pQSà….Ò
2:5920h:  01 70 51 53 E0 85 1C D2 01 50 4B 05 06 00 00 00   .pQSà….Ò.PK.....
2:5930h:  00 01 00 01 00 5B 00 00 00 CE 58 02 00 00 00      .....[...ÎX....
```

Template Results - ZIPTemplate.bt

Name	Value	Start	Size	Color	Comment
struct ZIPFILERECORD record	flag.vmdk	0h	258CEh	Fg: Bg:	
struct ZIPDIRENTRY dirEntry	flag.vmdk	258CEh	5Bh	Fg: Bg:	
struct ZIPENDLOCATOR endLocator		25929h	16h	Fg: Bg:	

Address	Value
Found 1 occurrences of '14 00 09 00'.	
258D4h	14 00 09 00

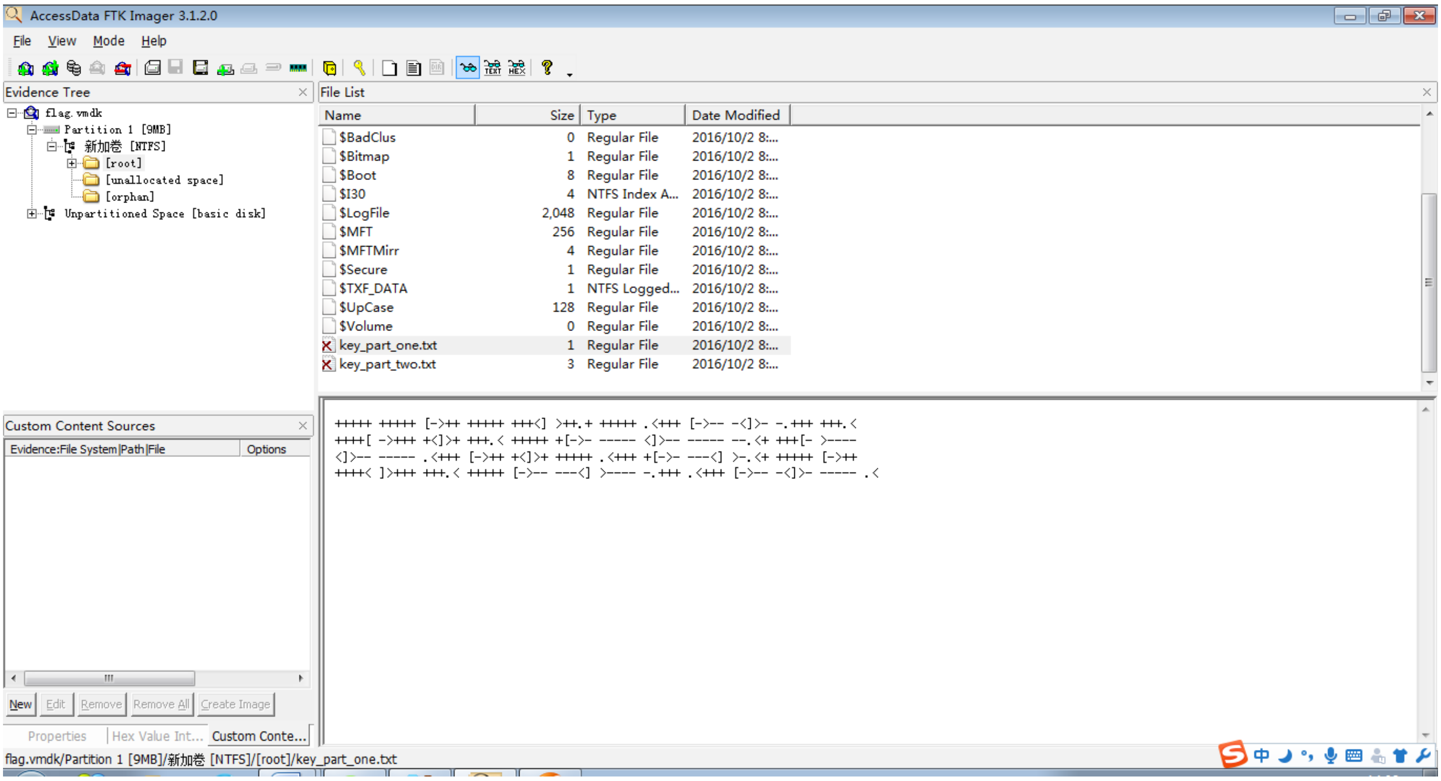
Found 1 occurrences of '14 00 09 00'. (press Esc to hide results)

Start: 153812 [258D4h] Sel: 4 [4h]

将14 00 09 00修改为14 00 00 00后打开，可以提取出flag.vmdk

第二步：分析

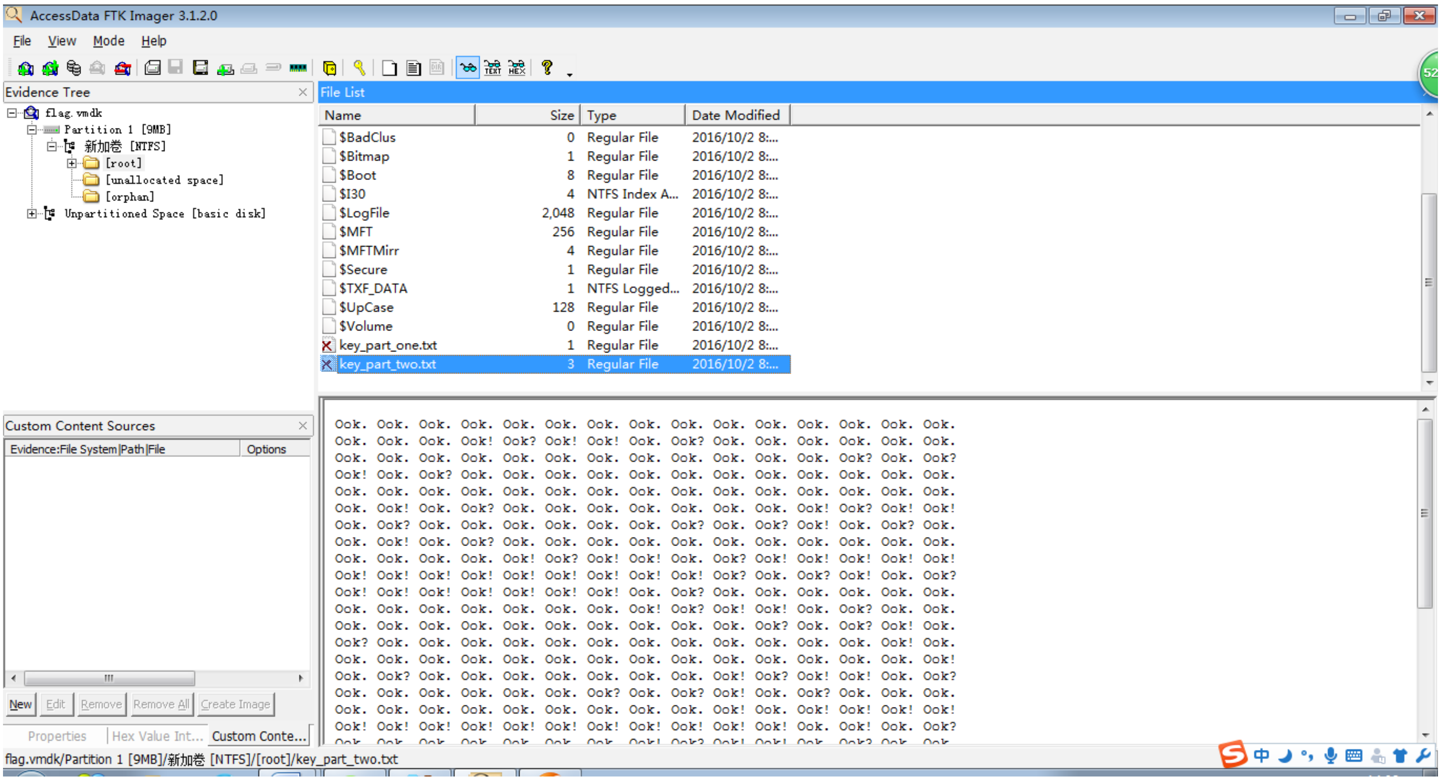
很明显，这是一个磁盘取证分析环节，先下载安装好磁盘取证工具AccessData FTK Imager（http://download.csdn.net/download/streetmilk/5238752），或者其他工具也行。直接打开，可以发现两个文件：



Name	Size	Type	Date Modified
$BadClus	0	Regular File	2016/10/2 8:...
$Bitmap	1	Regular File	2016/10/2 8:...
$Boot	8	Regular File	2016/10/2 8:...
$I30	4	NTFS Index A...	2016/10/2 8:...
$LogFile	2,048	Regular File	2016/10/2 8:...
$MFT	256	Regular File	2016/10/2 8:...
$MFTMirr	4	Regular File	2016/10/2 8:...
$Secure	1	Regular File	2016/10/2 8:...
$TXF_DATA	1	NTFS Logged...	2016/10/2 8:...
$UpCase	128	Regular File	2016/10/2 8:...
$Volume	0	Regular File	2016/10/2 8:...
key_part_one.txt	1	Regular File	2016/10/2 8:...
key_part_two.txt	3	Regular File	2016/10/2 8:...

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

flag.vmdk/Partition 1 [9MB]/新加卷 [NTFS]/[root]/key_part_one.txt



Name	Size	Type	Date Modified
$BadClus	0	Regular File	2016/10/2 8:...
$Bitmap	1	Regular File	2016/10/2 8:...
$Boot	8	Regular File	2016/10/2 8:...
$I30	4	NTFS Index A...	2016/10/2 8:...
$LogFile	2,048	Regular File	2016/10/2 8:...
$MFT	256	Regular File	2016/10/2 8:...
$MFTMirr	4	Regular File	2016/10/2 8:...
$Secure	1	Regular File	2016/10/2 8:...
$TXF_DATA	1	NTFS Logged...	2016/10/2 8:...
$UpCase	128	Regular File	2016/10/2 8:...
$Volume	0	Regular File	2016/10/2 8:...
key_part_one.txt	1	Regular File	2016/10/2 8:...
key_part_two.txt	3	Regular File	2016/10/2 8:...

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

flag.vmdk/Partition 1 [9MB]/新加卷 [NTFS]/[root]/key_part_two.txt

第三步：解密

可以看到两个文件里面的内容为brainfuck跟Ook编码，直接在线解密即可得到结果

https://www.splitbrain.org/services/o