

BUUCTF 面具下的flag

原创

仲璧 于 2022-01-26 13:51:03 发布 2111 收藏 1

分类专栏: [CTF](#) 文章标签: [debian](#) [运维](#)

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/m0_49025459/article/details/122699856

版权



[CTF 专栏收录该内容](#)

47 篇文章 1 订阅

订阅专栏

题目

题目 解题快手榜

面具下的flag

1

注意: 得到的 flag 请包上 flag{} 提交

[2c1606ee-4...](#)

Flag

提交

CSDN @ 壬二舟

解压压缩包获得图片



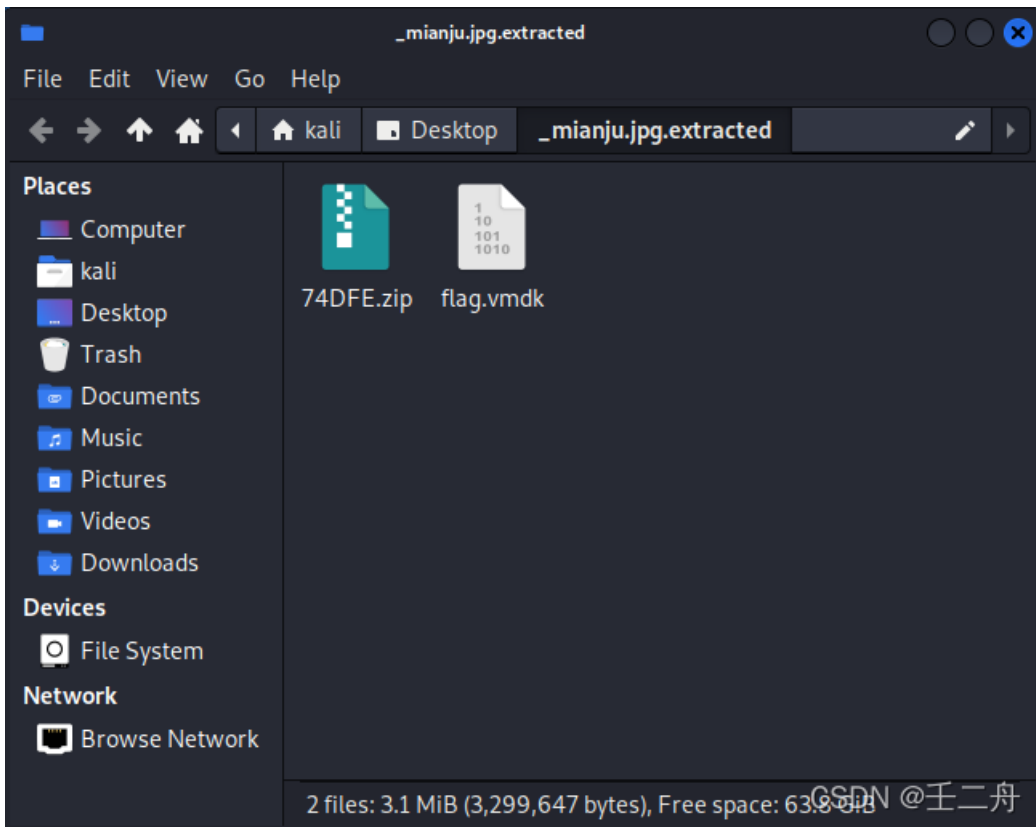
用kali命令binwalk打开图片

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
└─$ binwalk mianju.jpg

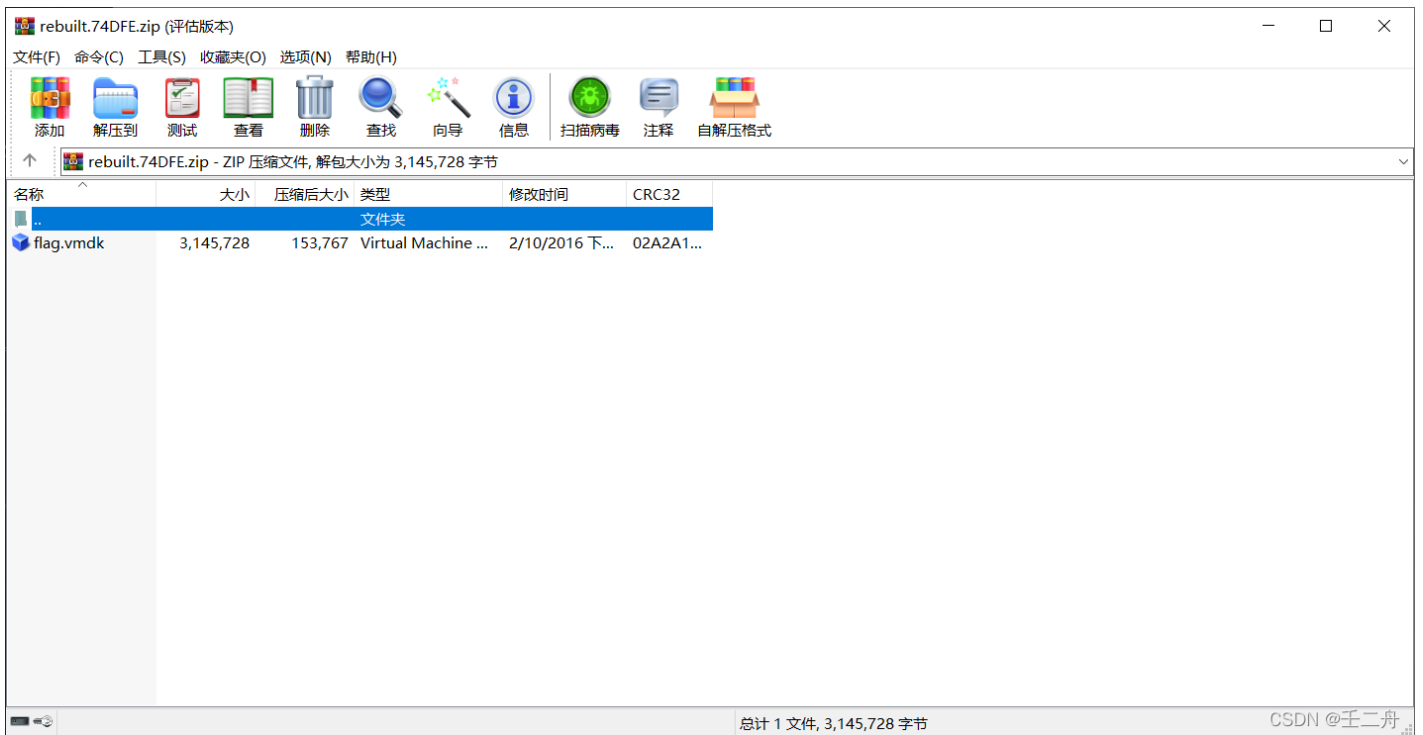
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          JPEG image data, EXIF standard
12          0xC          TIFF image data, little-endian offset of first
image directory: 8
478718      0x74DFE      Zip archive data, at least v2.0 to extract, com
pressed size: 153767, uncompressed size: 3145728, name: flag.vmdk
632615      0x9A727      End of Zip archive, footer length: 22

(kali@kali)-[~/Desktop]
└─$
```

发现里面有zip文件，使用binwalk -e 文件名 命令打开



分离出一个压缩包文件，发现这是一个伪加密，我们使用WinRAR自带的修复文件



取出flag.vmdk文件，然后在kali里使用7z解压flag.vmdk

```
kali@kali: ~/Desktop
File Actions Edit View Help
led correctly
478718      0x74DFE      Zip archive data, at least v2.0 to extract, com
pressed size: 153767, uncompressed size: 3145728, name: flag.vmdk
632615      0x9A727      End of Zip archive, footer length: 22

(kali@kali)-[~/Desktop]
└─$ 7z x flag.vmdk -o./

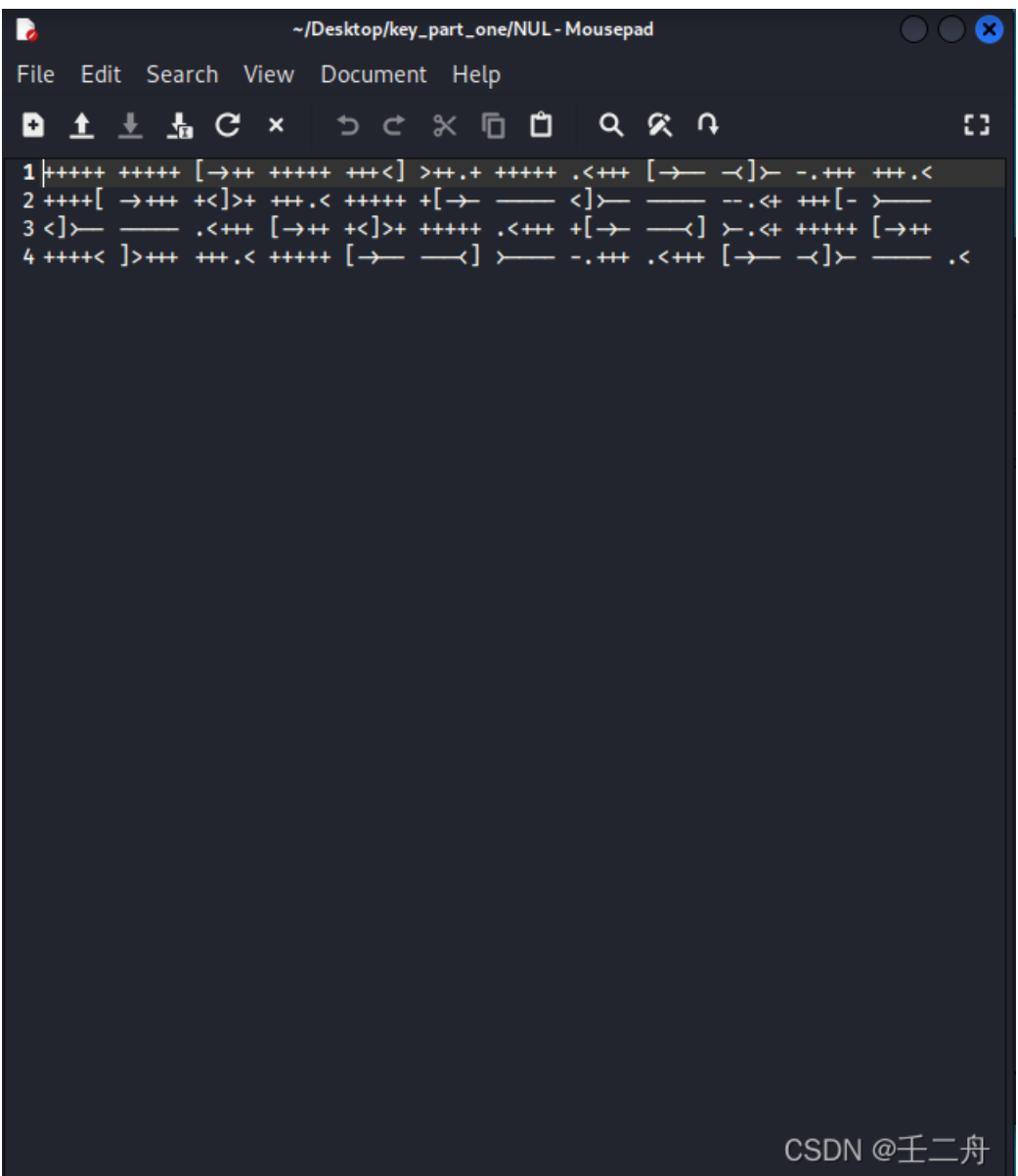
7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs
Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz (906EA),ASM,AES-NI)

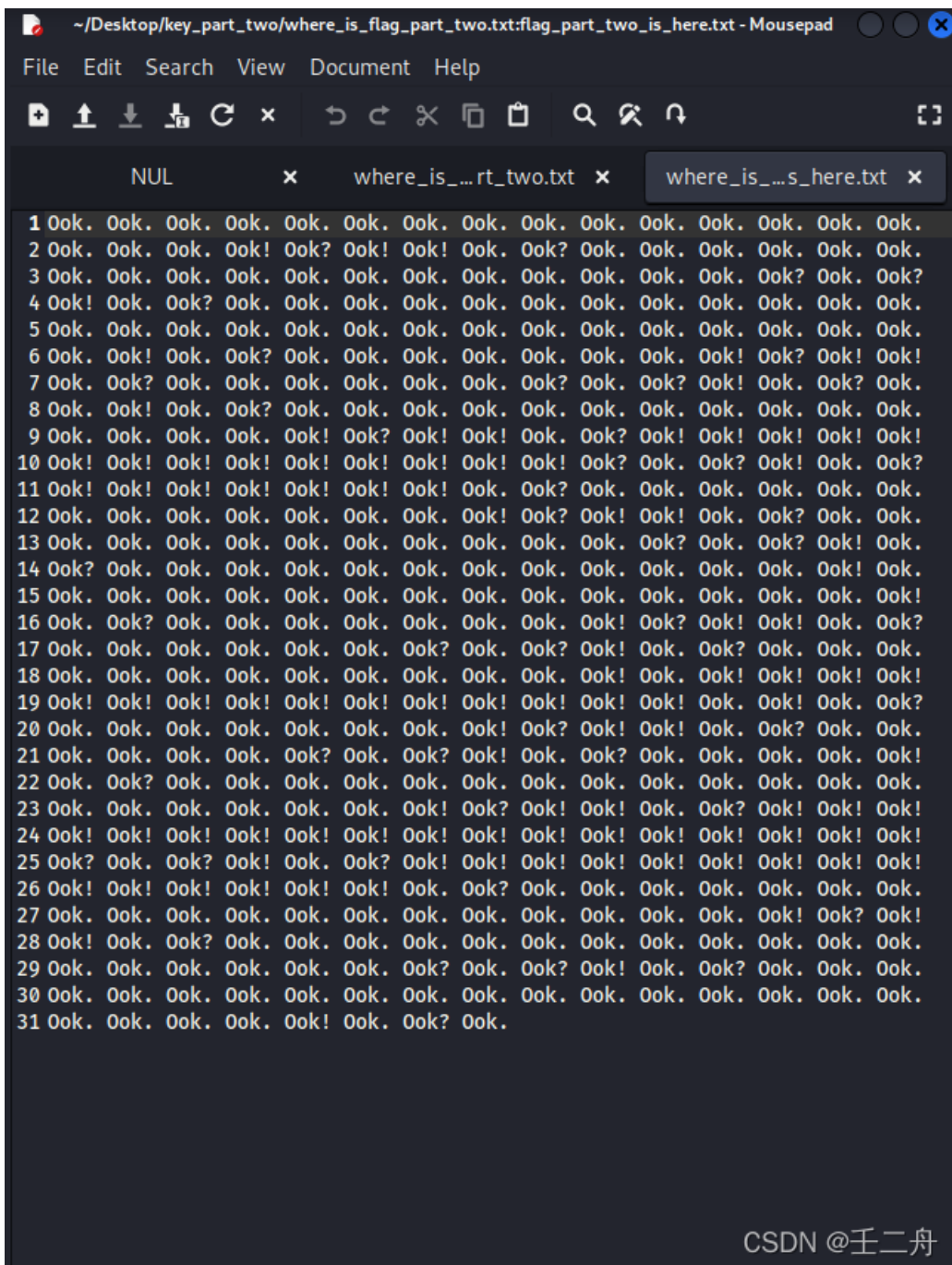
Scanning the drive for archives:
1 file, 3145728 bytes (3072 KiB)

Extracting archive: flag.vmdk
--
Path = flag.vmdk
Type = VMDK
Physical Size = 3145728
Method = "monolithicSparse"
Cluster Size = 65536
Headers Size = 65536
ID = 1da959fe
Name = flag.vmdk
Comment = # Disk DescriptorFile
```

CSDN @壬二舟

在解压的文件中寻找发现只有两个文本文档有用





CSDN @壬二舟

使用在线解密工具 [Brainfuck/0ok! Obfuscation/Encoding \[splitbrain.org\]](https://www.splitbrain.org/services/ook)

<https://www.splitbrain.org/services/ook>

最后分别得到两个字符串，拼接在一起就是flag

```
f1ag{N7F5_AD5_i5_funny!}
```