

【CTF/MISC】图片隐写题（binwalk/foremost/010editor配合使用）

原创

[mengmeng0510](#) 于 2021-10-24 14:20:52 发布 1376 收藏 11

分类专栏: [CTF](#) 文章标签: [CTF binwalk 010editor](#)

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/mengmeng0510/article/details/120933296>

版权



[CTF 专栏收录该内容](#)

7 篇文章 2 订阅

订阅专栏

图片隐写

题目

解题思路

binwalk工具查看是否有隐藏文件

foremost工具分离文件

010editor查看二进制数据, 寻找解压密码

解题心得

题目连接

题目

题目是一张图片：



CSDN @mengmeng0510

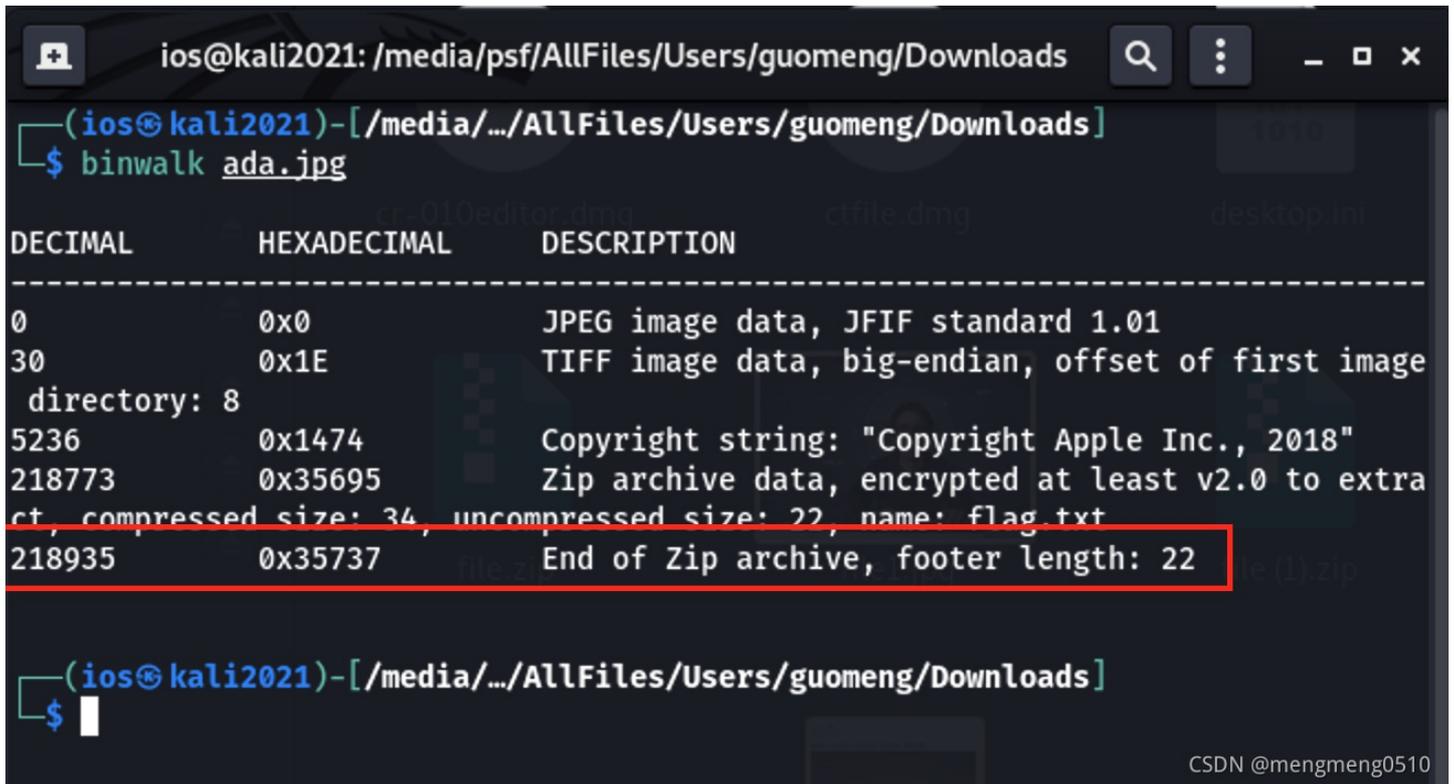
寻找题目中隐藏的flag。

解题思路

一般来说我碰到图片隐写这种题，都会用到010editor和binwalk这两个工具，来看看图片中有没有什么隐藏的信息。

[binwalk](#)工具查看是否有隐藏文件

首先我用binwalk工具查看一下图片中有没有隐藏其他的文件：



```
(ios@kali2021)-[~/media/.../AllFiles/Users/guomeng/Downloads]
└─$ binwalk ada.jpg
```

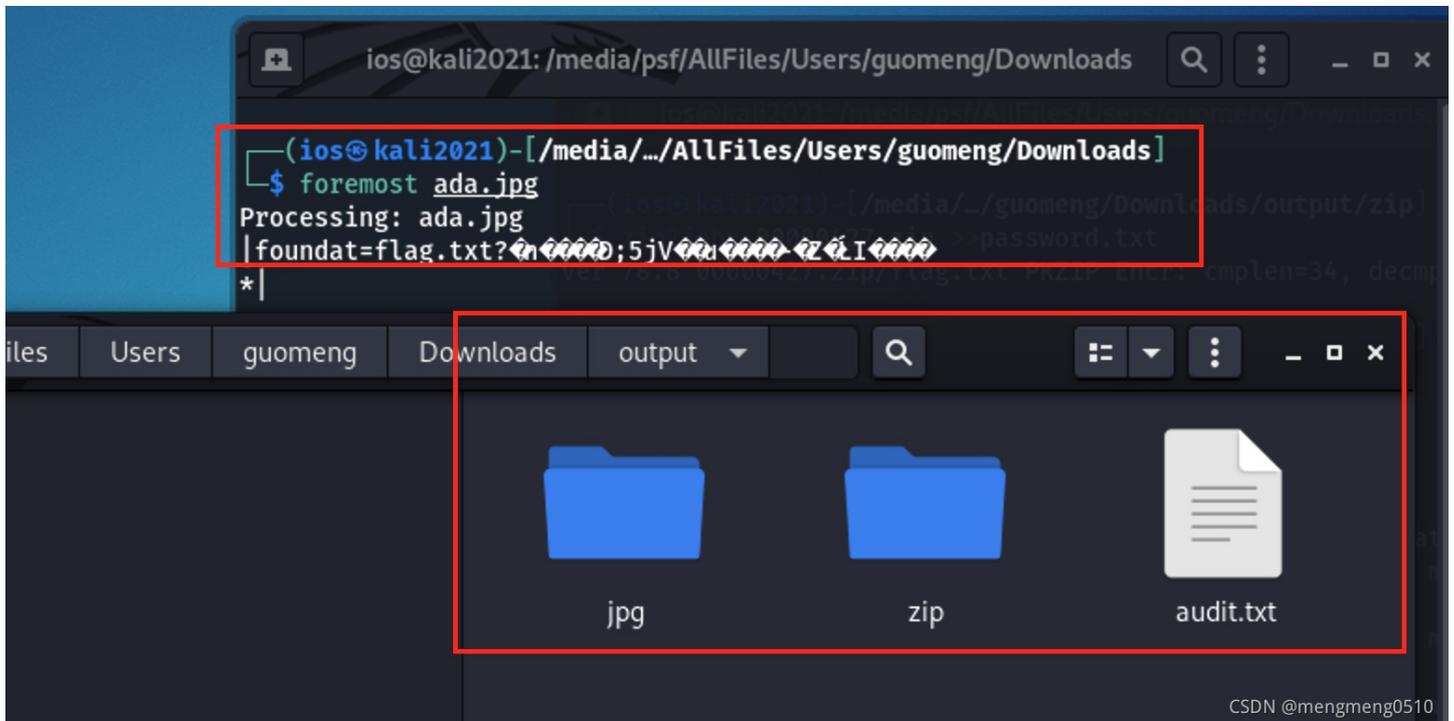
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
30	0x1E	TIFF image data, big-endian, offset of first image directory: 8
5236	0x1474	Copyright string: "Copyright Apple Inc., 2018"
218773	0x35695	Zip archive data, encrypted at least v2.0 to extract, compressed size: 34, uncompressed size: 22, name: flag.txt
218935	0x35737	End of Zip archive, footer length: 22

```
(ios@kali2021)-[~/media/.../AllFiles/Users/guomeng/Downloads]
└─$
```

CSDN @mengmeng0510

在里面我们发现藏有zip文件。

foremost工具分离文件



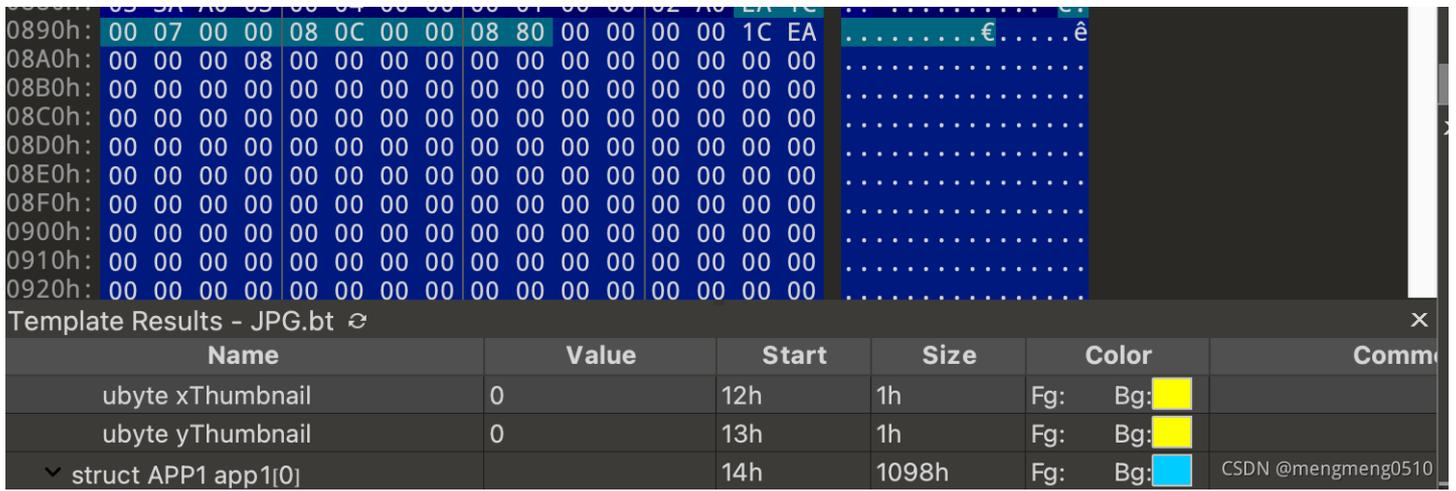
```
(ios@kali2021)-[~/media/.../AllFiles/Users/guomeng/Downloads]
└─$ foremost ada.jpg
Processing: ada.jpg
|foundat=flag.txt?;5jV;I
```

Files: Users | guomeng | Downloads | output

- jpg
- zip
- audit.txt

CSDN @mengmeng0510

foremost分离得到的文件存放在output文件夹下，我们可以看到有两个文件夹jpg和zip。jpg文件夹下就是存放着剥离后的照片。我们打开zip文件夹，发现里面有个压缩包，压缩包里面有个flag.txt文件。而这个flag.txt文件应该就藏着我们要找的flag信息了。但是此时我们发现解压文件需要密码：

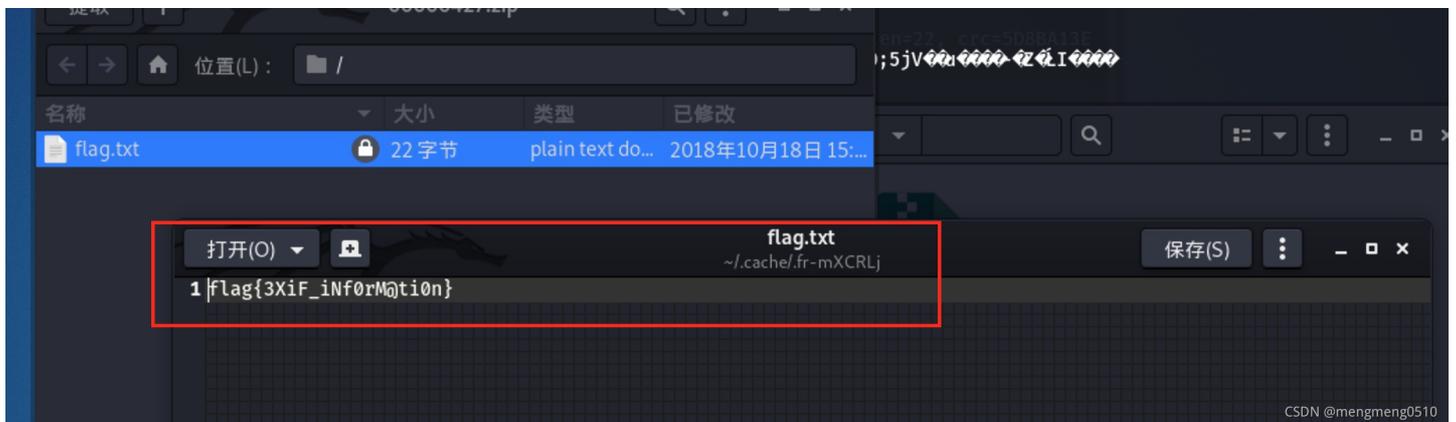


我们在一堆00字节的中间发现了一串编码，我们发现这串编码只包含0~9的数字和大写字母ABCDEF，因此我们可以怀疑这串编码为base16编码，我们通过在线解码工具进行解码：

Base16编码解码



sdnisc_2018应该就是我们要找的解压密码：



解题心得

解题过程中要有思路，要有耐心，熟练掌握各种工具的使用，就一定能找到flag。

题目连接

<https://ctf.bugku.com/challenges/detail/id/6.html?page=3>