

# BUUCTF-MISC-[ACTF新生赛2020]NTFS数据流~john-in-the-middle

原创

七董墨年 于 2021-12-25 16:58:43 发布 1306 收藏 1

文章标签: 安全

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/justruofeng/article/details/121360751>

版权

## 文章目录

- 1.[ACTF新生赛2020]NTFS数据流
- 2.我吃三明治
- 3.[SUCTF2018]single dog
- 4.john-in-the-middle

---

## 1.[ACTF新生赛2020]NTFS数据流

题目描述：得到的 flag 请包上 flag{} 提交

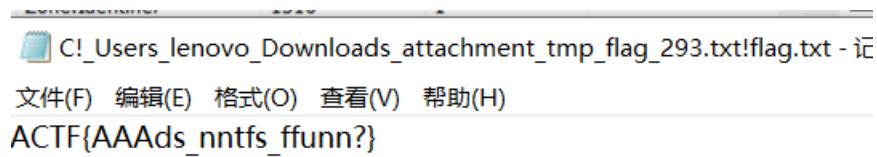
解题步骤：下载附件，解压tmp文件夹中的flag.rar，题目提示NTFS数据流，NtfsStreamsEditor扫下发现293.txt:flag.txt

The screenshot shows the NtfsStreamsEditor interface. The search bar at the top contains the text '293.txt'. Below the search bar is a table with four columns: '文件' (File), '数据流名称' (Stream Name), '大小(字节)' (Size), and '可疑度(0-5)' (Suspiciousness). There are three entries in the table:

文件	数据流名称	大小(字节)	可疑度(0-5)
C:\Users\lenovo\Downloads\attachment.tar:Zone.Identifier	Zone.Identifier	143	0
C:\Users\lenovo\Downloads\flag.rar:Zone.Identifier	Zone.Identifier	1316	1
<input checked="" type="checkbox"/> C:\Users\lenovo\Downloads\attachment\tmp\flag\293.tx...	flag.txt	27	1

At the bottom right of the interface, there is a watermark: 'CSDN @七堇墨年'.

导出发现flag: ACTF{AAAds\_nntfs\_ffunn?}



CSDN @七堇墨年

flag{AAAds\_nntfs\_ffunn?}

## 2.我吃三明治

题目描述：得到的 flag 请包上 flag{} 提交。

解题步骤：010 打开 flag.jpg，在中间发现 FF D9，应该是图片拼接，并发现拼接处有一串 base 编码：

MZWGCZ33GZTDCNZZG5SDIMBYGBRDEOLCGY2GIJVHA4TONZYGA2DMM3FGMYH2

## base32解码

MZWGCZ33GZTDCNZZG5SDIMBYGBRDEOLCGY2GIYJH  
A4TONZYGA2DMM3FGMYH2

flag{6f1797d4080b29b64da5897780463e30}

编研

CSDN @七堇墨年

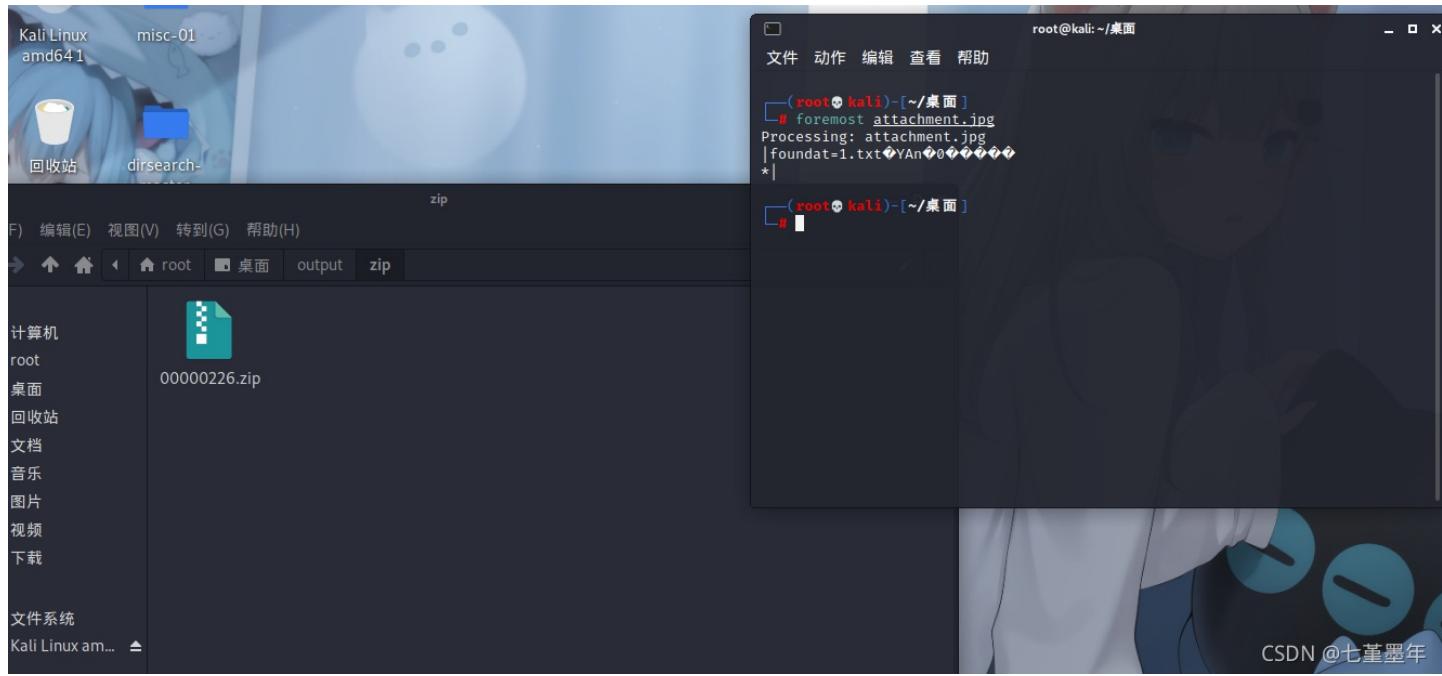
flag{6f1797d4080b29b64da5897780463e30}

### 3.[SUCTF2018]single dog

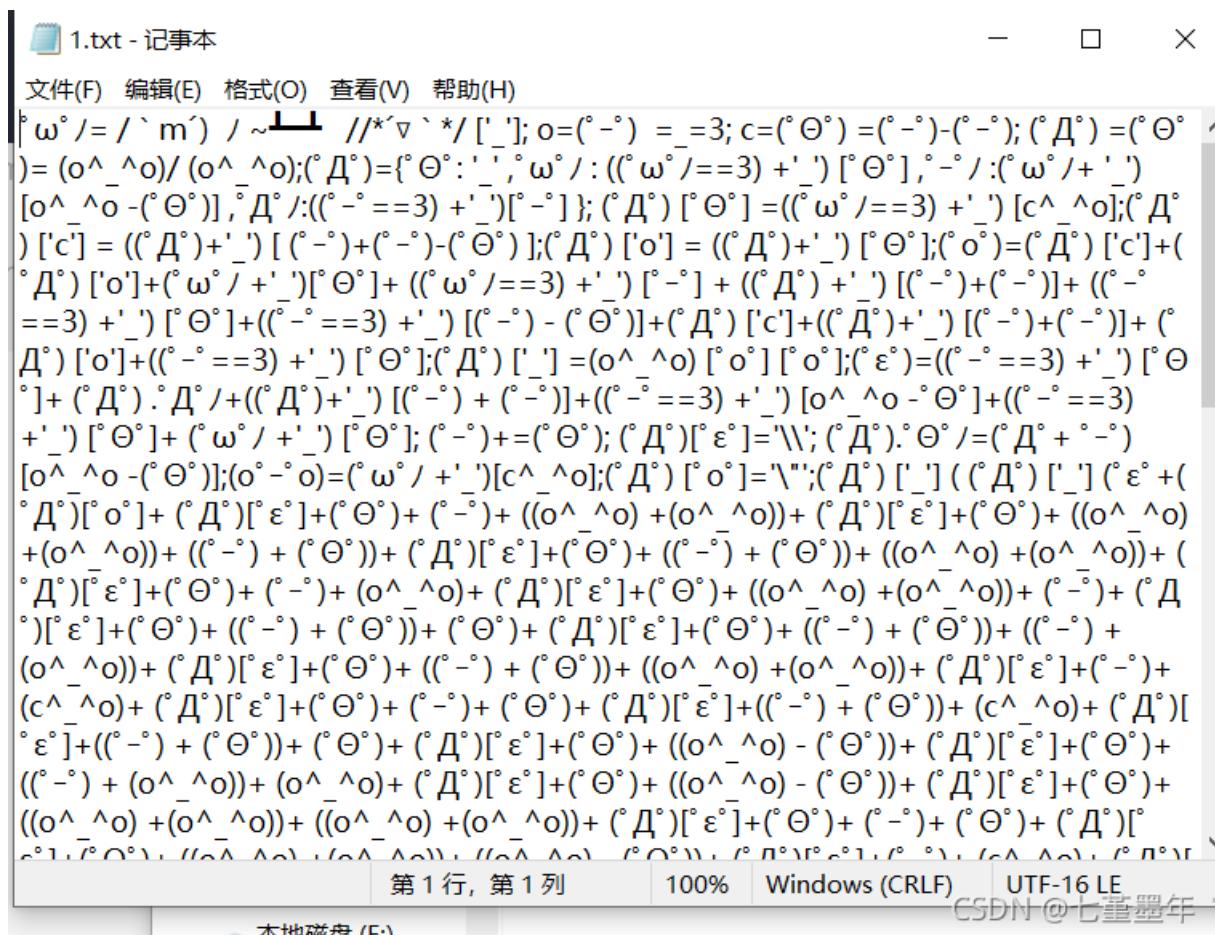
题目描述：得到的 flag 请包上 flag{} 提交。来源：[https://github.com/hebtuerror404/CTF\\_competition\\_warehouse\\_2018](https://github.com/hebtuerror404/CTF_competition_warehouse_2018)

解题步骤：010打开图片，发现.PK与1.txt

**foremost**分离文件



解压压缩包，发现1.txt，打开发现颜文字加密



颜文字解密（网址：<http://www.atoolbox.net/Tool.php?Id=703>）

## AAEncode加密/解密

加密

解密

```
function a()
{
var a="SUCTF{happy double eleven}";
alert("双十一快乐");
}
a();
```

CSDN @七堇墨年

解密结果为：

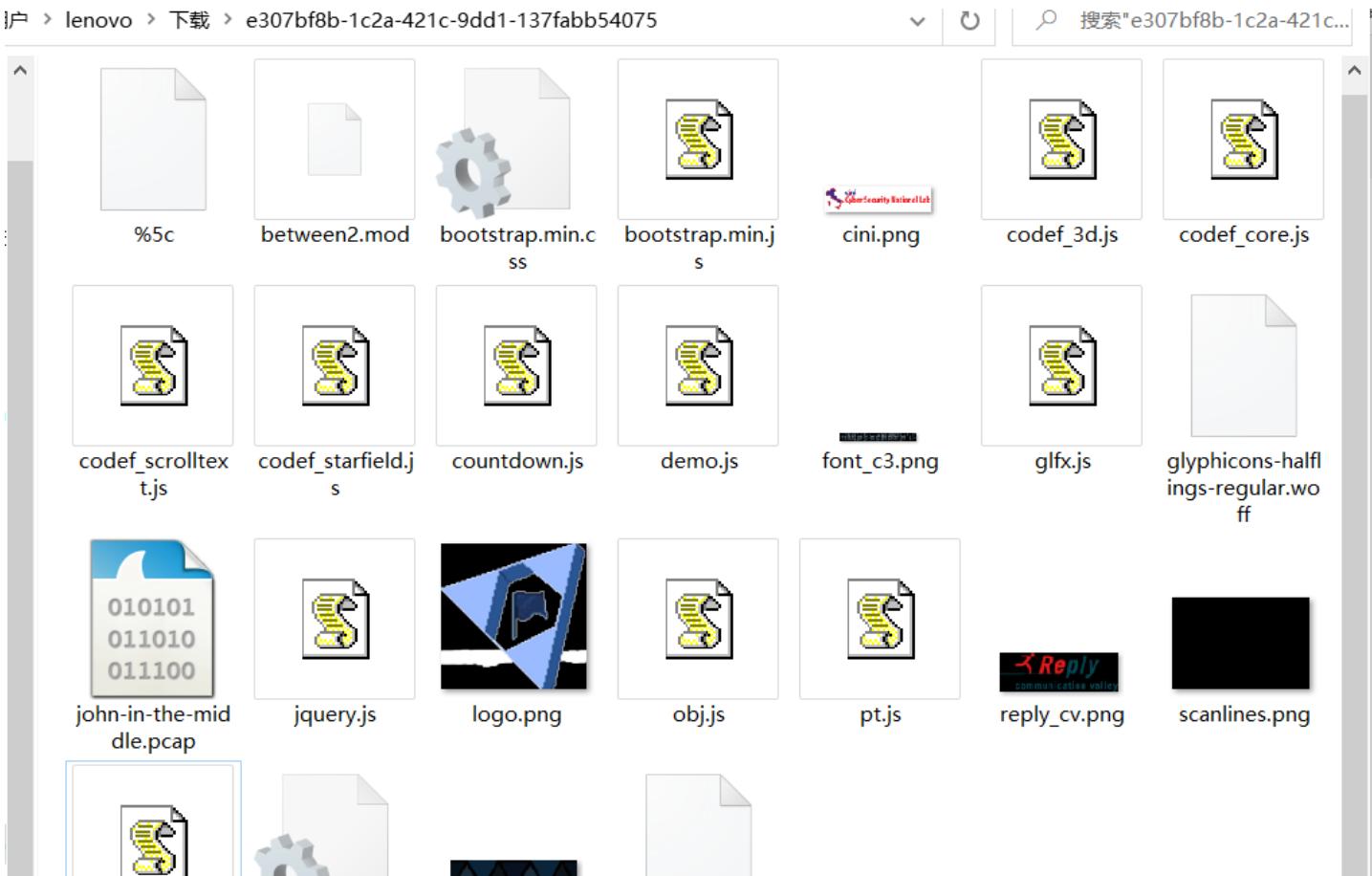
```
function a()  
{  
var a="SUCTF{happy double eleven}";  
alert("双十一快乐");  
}  
a();
```

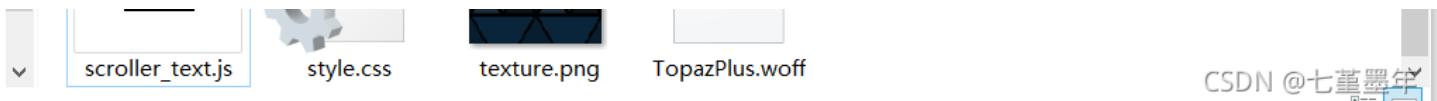
得到flag: SUCTF{happy double eleven}  
flag{happy double eleven}

## 4. john-in-the-middle

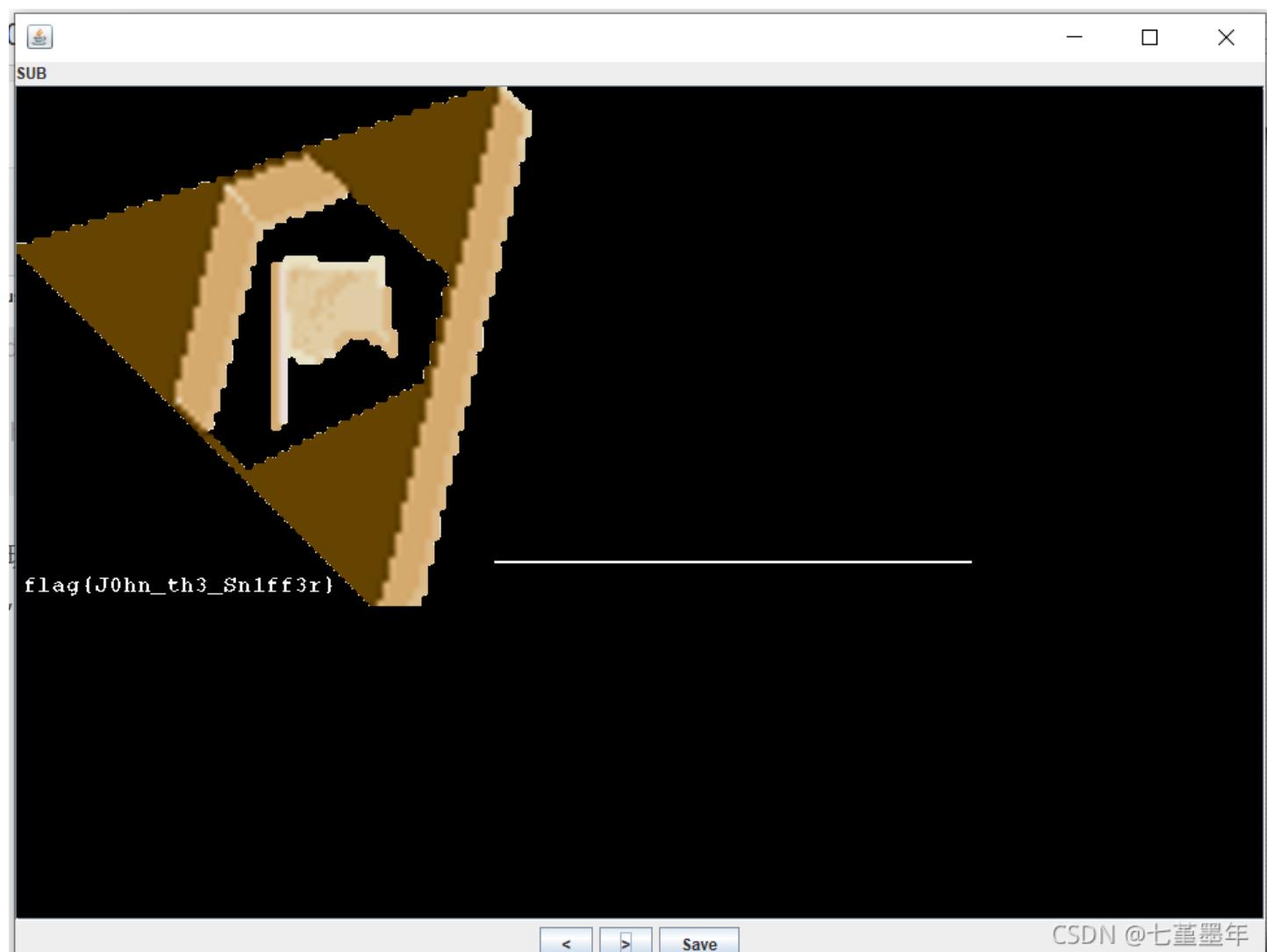
题目描述：注意：得到的 flag 请包上 flag{} 提交

解题步骤：Wireshark打开，导出HTTP数据包，结果如下：





StegSolve打开scanlines.png发现在很多图层都会发现一条线，然后logo.png图片缺了一条线，将两张图片使用stegslove进行Image Combiner进行叠加，调整通道发现flag



flag{J0hn\_th3\_Sn1ff3r}