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

原创

七堇墨年 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

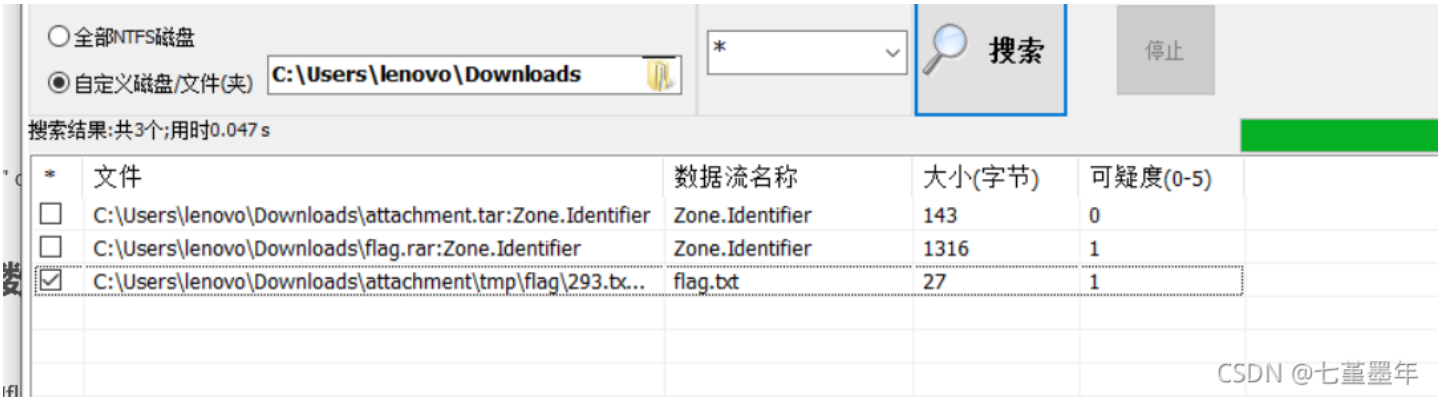
3.[SUCTF2018]single dog

4.john-in-the-middle

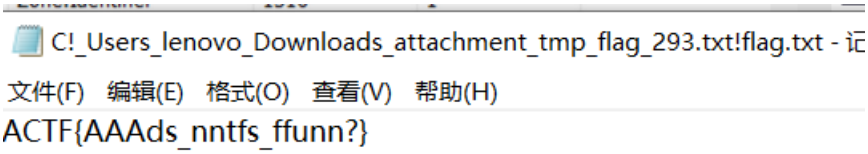
1.[ACTF新生赛2020]NTFS数据流

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



导出发现flag：ACTF{AAAds_nntfs_ffunn?}

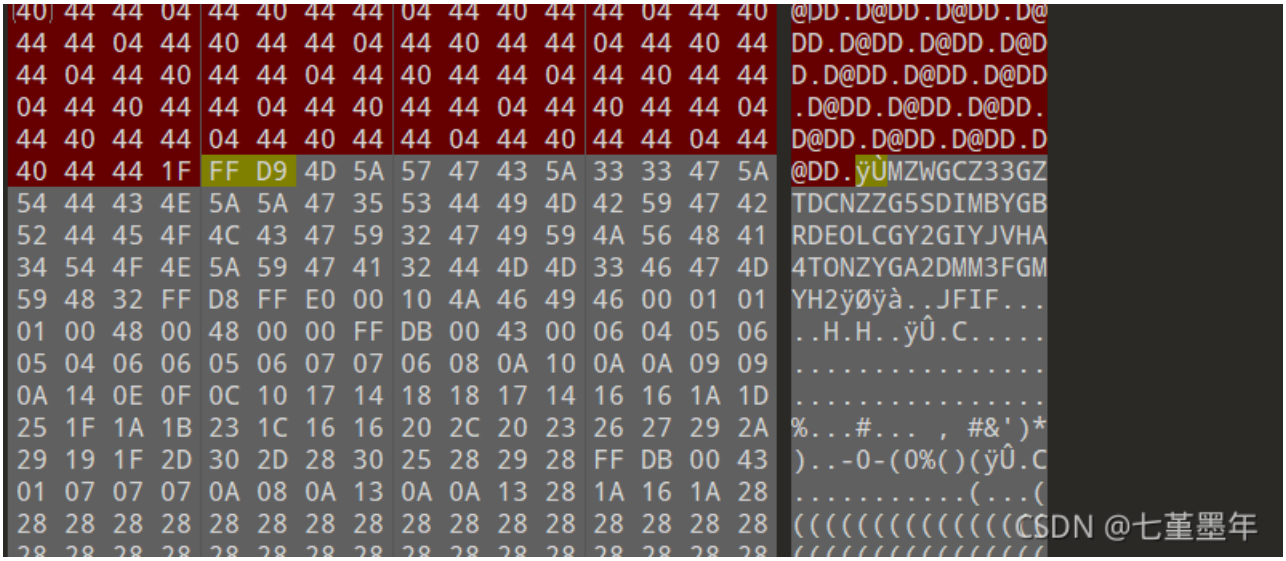


CSDN @七堇墨年

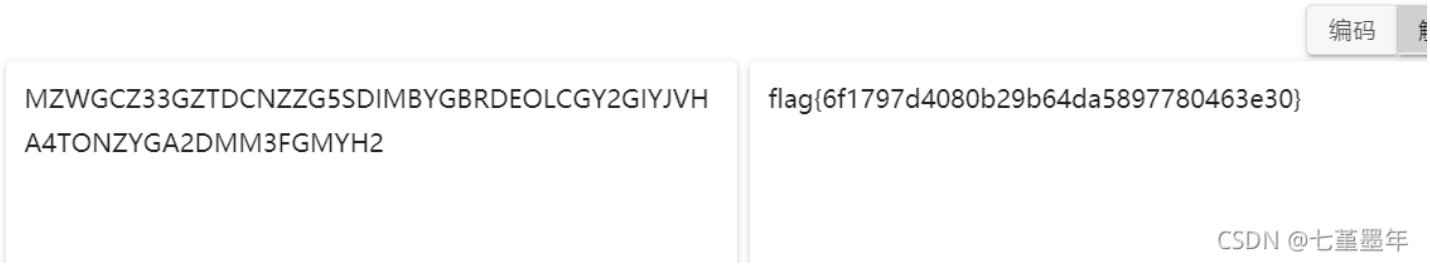
flag{AAAds_nntfs_ffunn?}

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：
MZWGCZ33GZTDCNZZG5SDIMBYGBRDEOLCGY2GIYJVHA4TONZYGA2DMM3FGMYH2



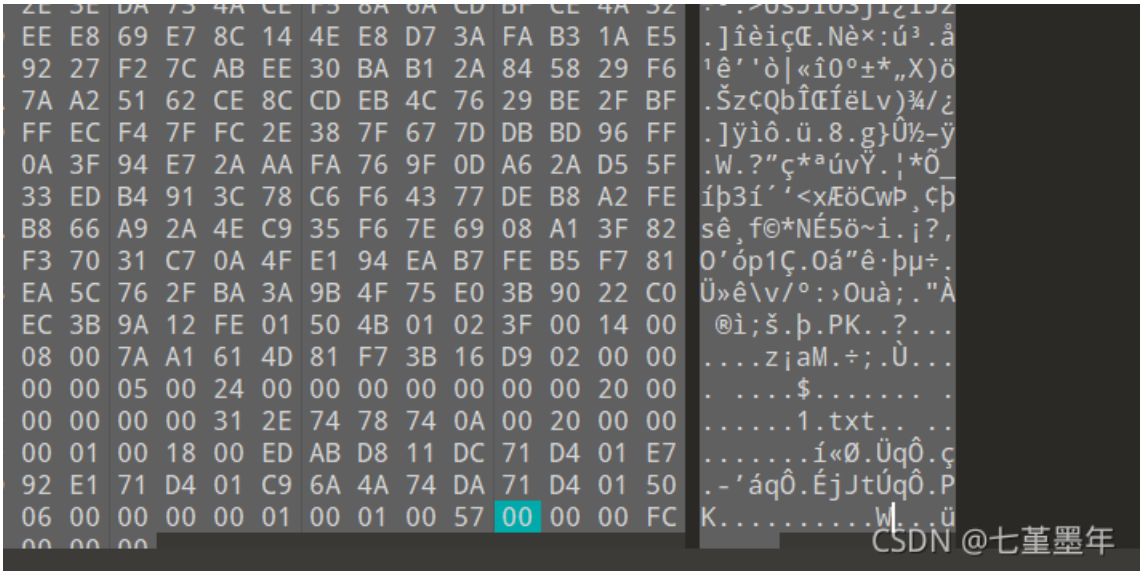
base32解码



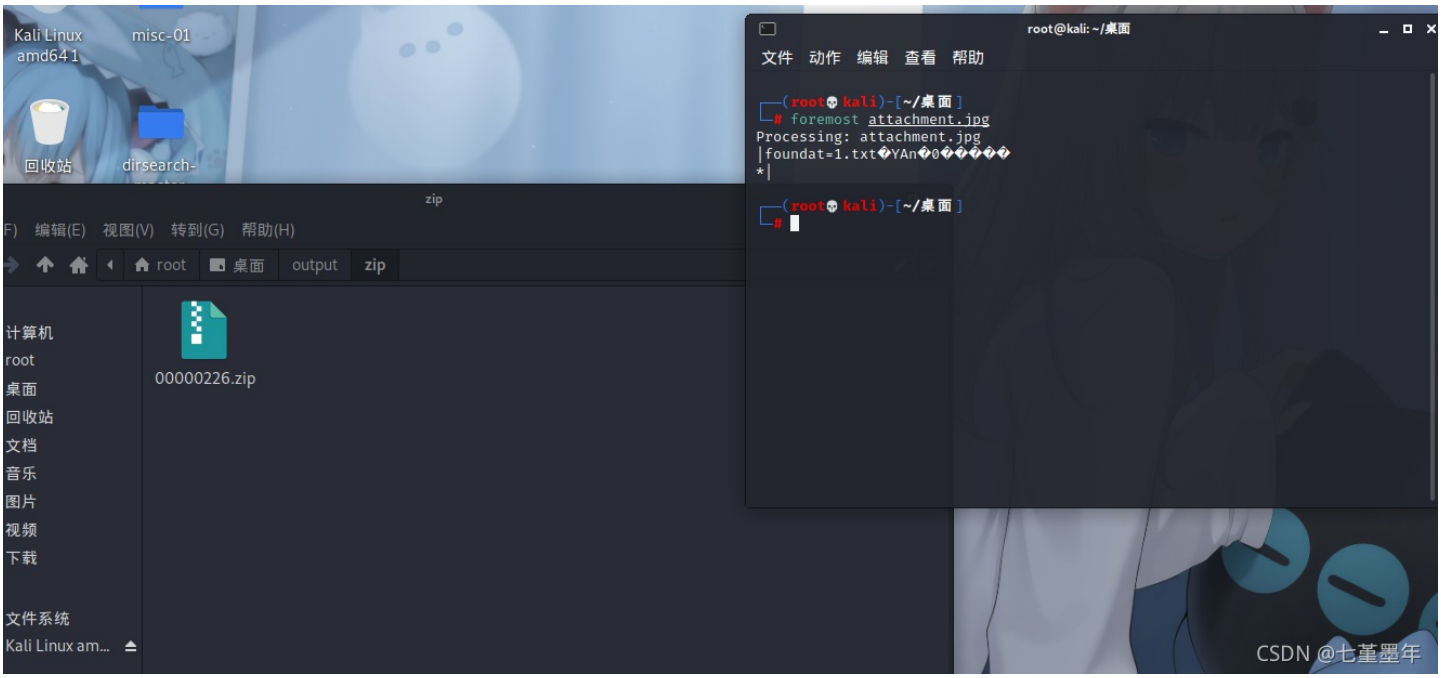
flag{6f1797d4080b29b64da5897780463e30}

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
解题步骤：010打开图片，发现.PK与1.txt

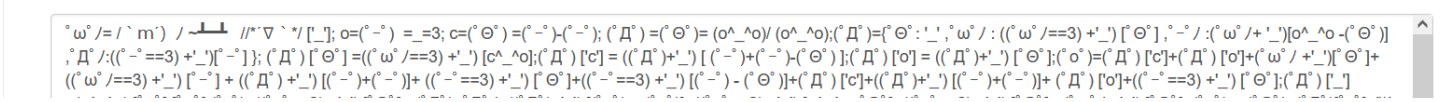


foremost分离文件



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）



解密结果为：

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

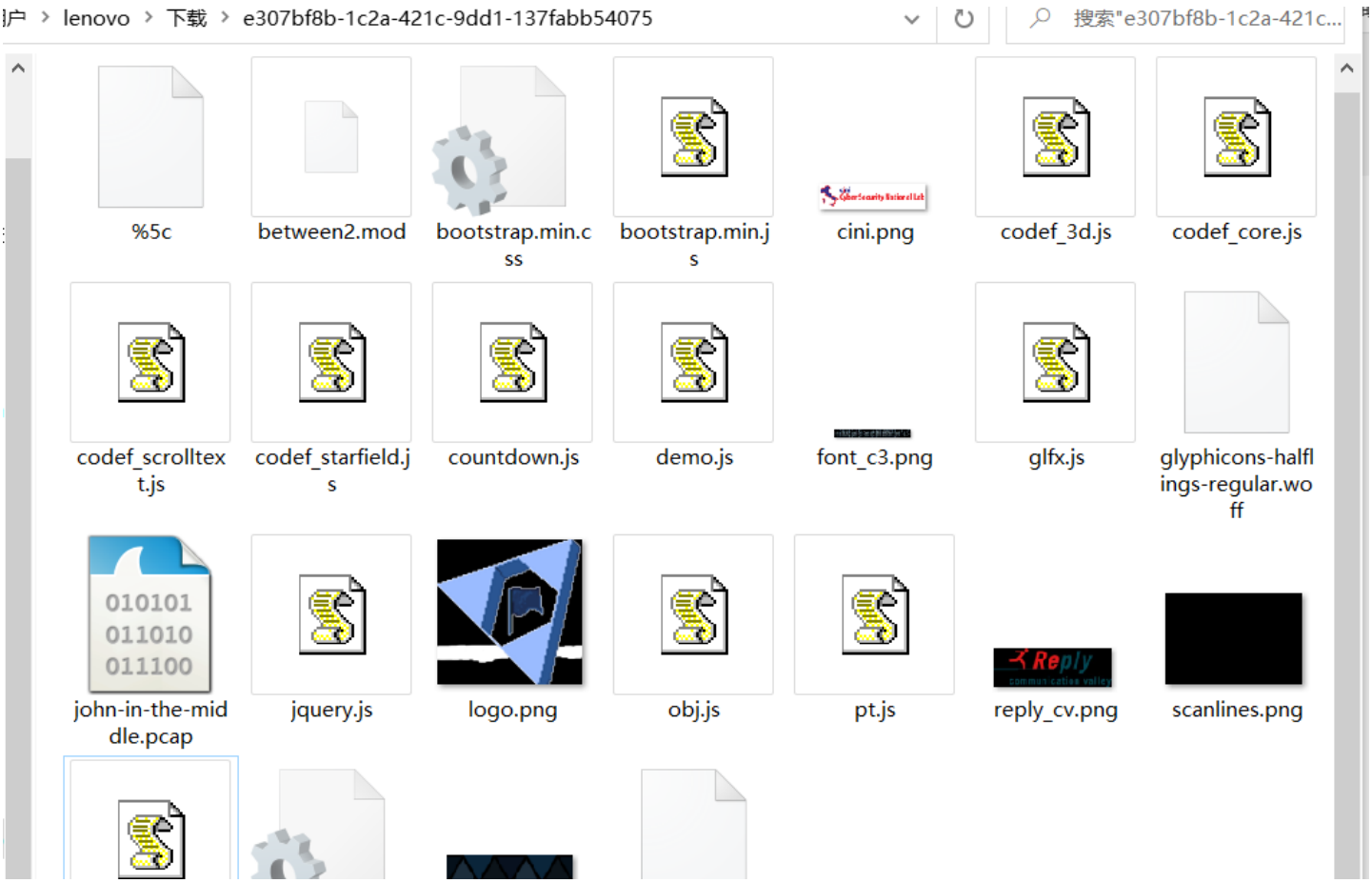
得到flag：SUCTF{happy double eleven}

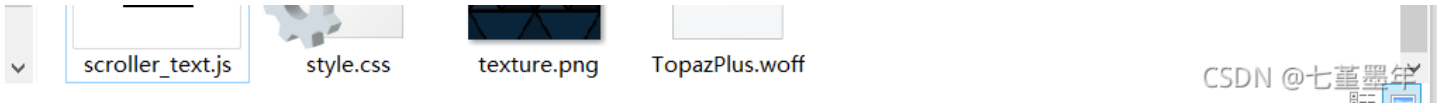
flag{happy double eleven}

4.john-in-the-middle

题目描述：注意：得到的 flag 请包上 flag{} 提交

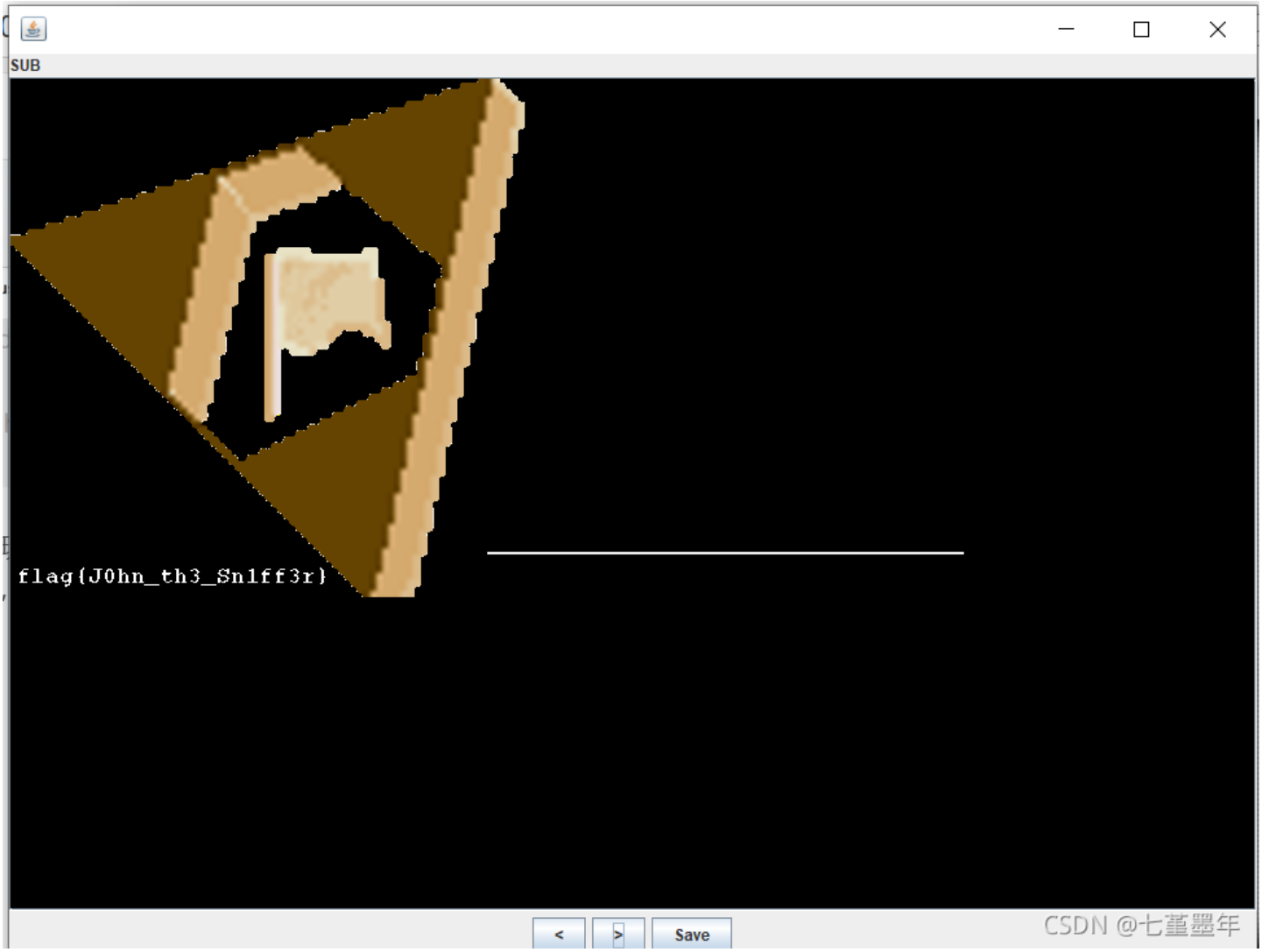
解题步骤：Wireshark打开，导出HTTP数据包，结果如下：





CSDN @七堇墨年

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



CSDN @七堇墨年

flag{J0hn_th3_Sn1ff3r}