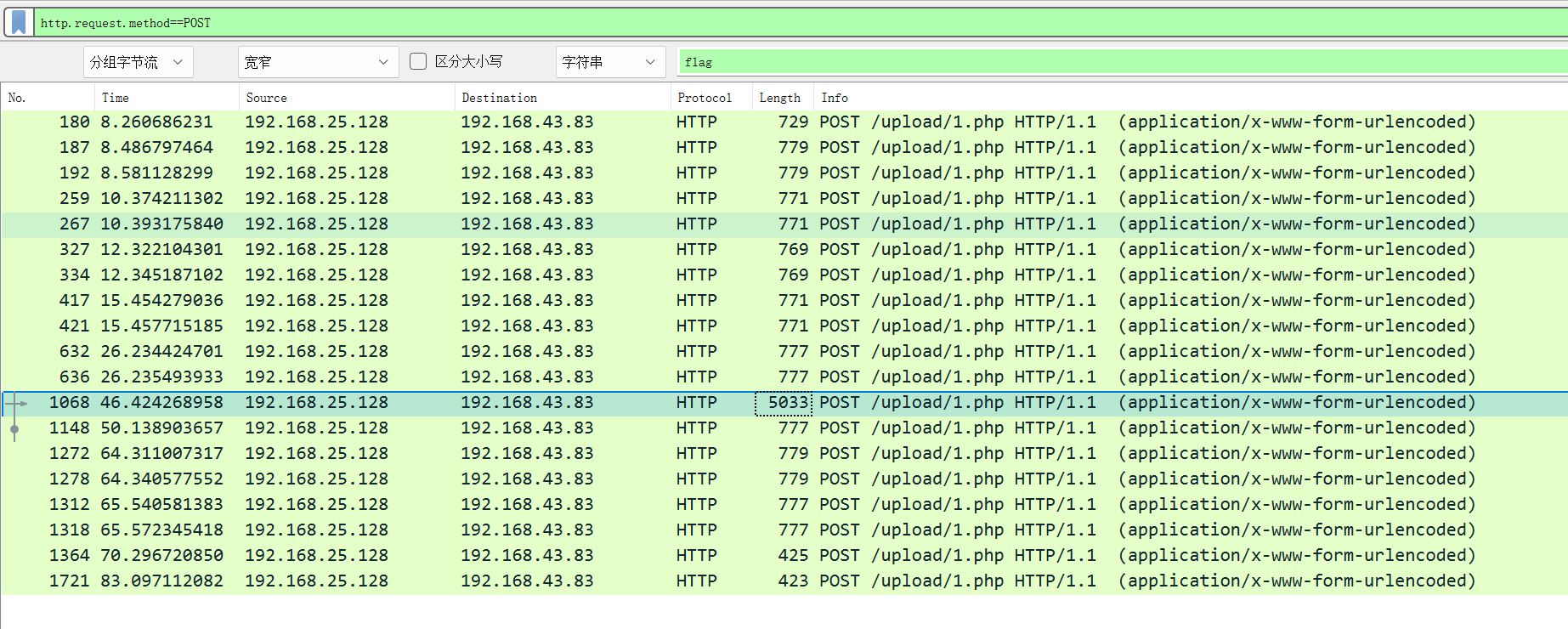
**Misc1**

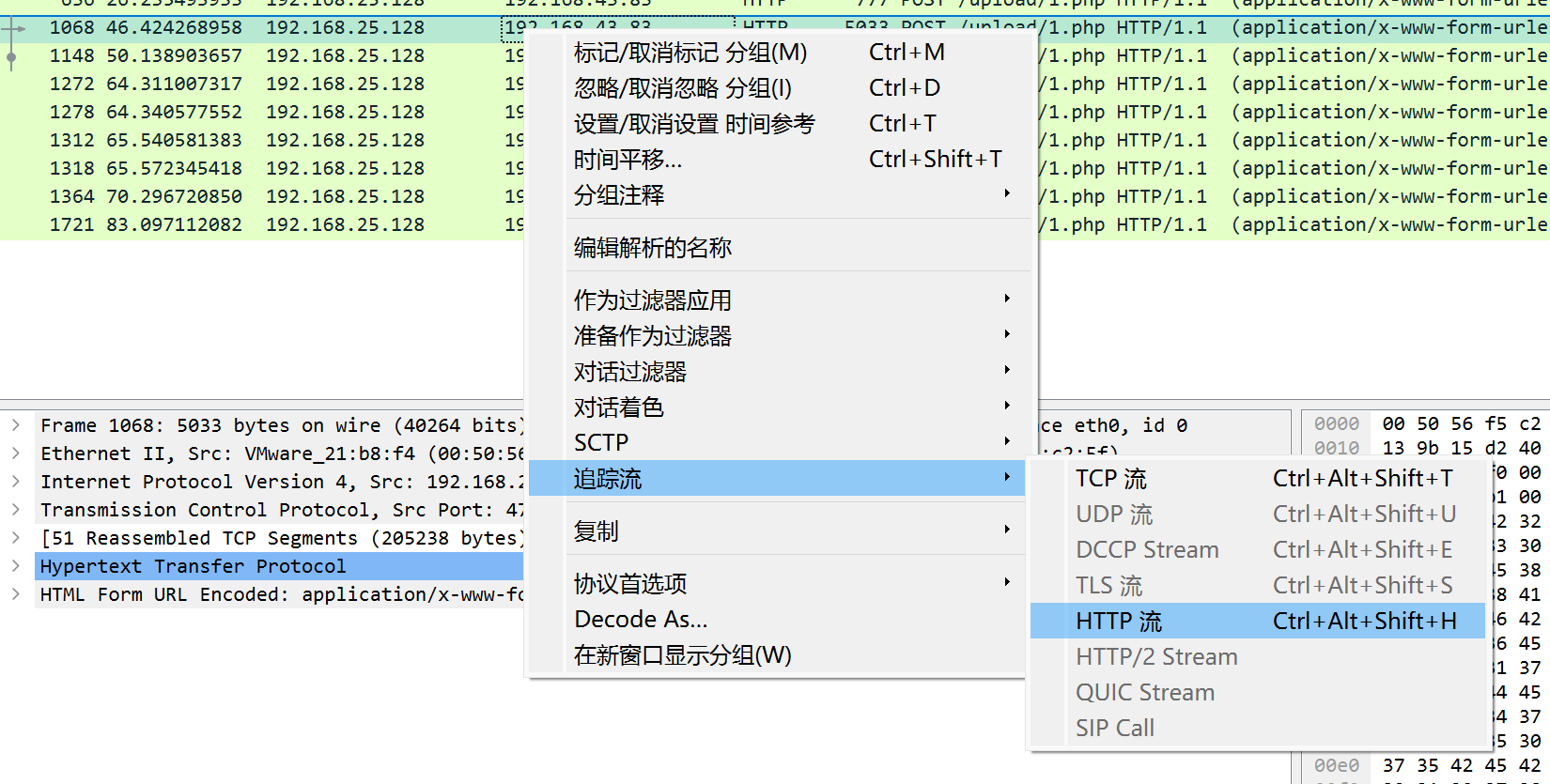
**学会解密123**

流量分析，你能找到flag吗 注意：得到的 flag 请包上 flag{} 提交

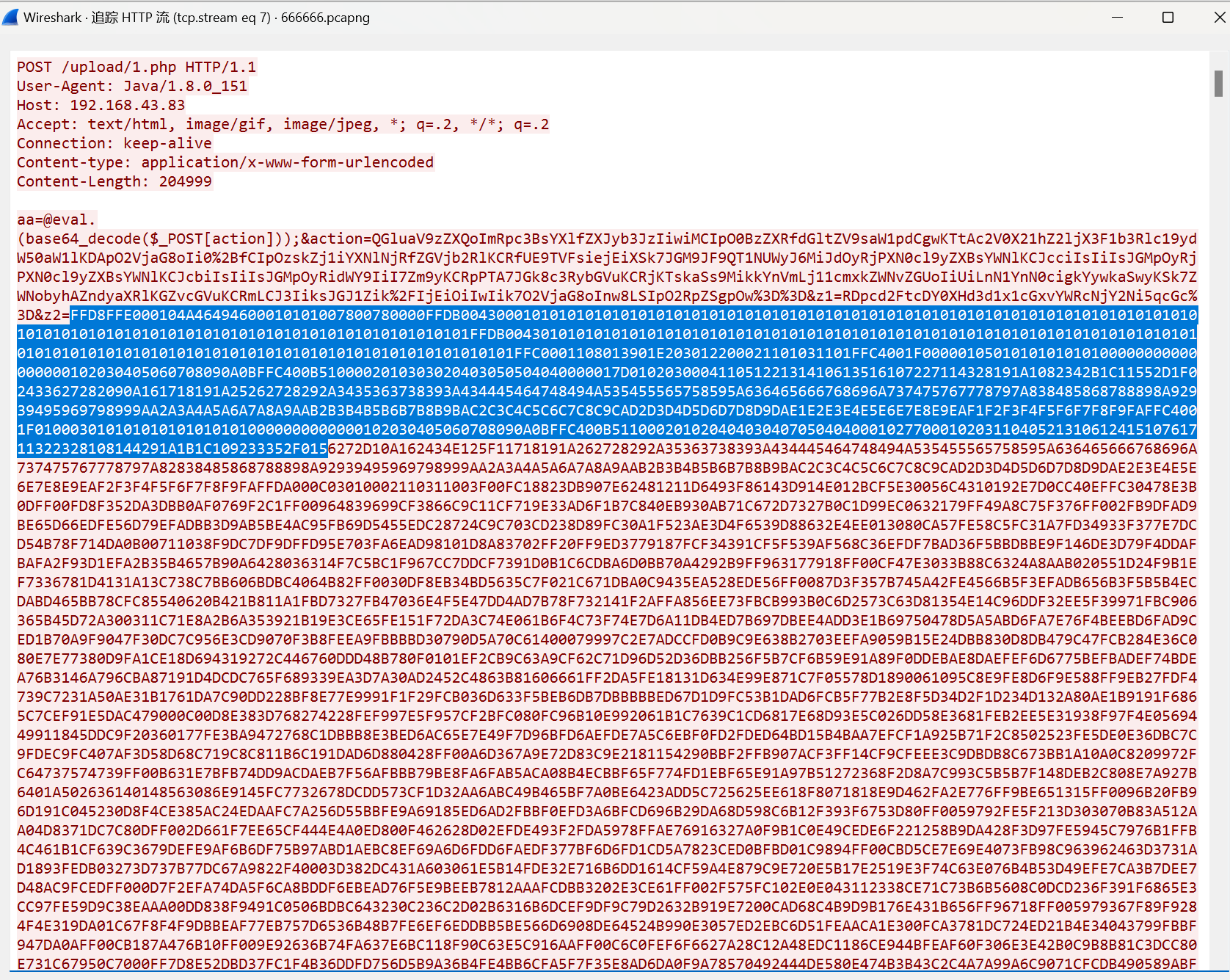
Wp:打开pcapng文件，http.request.method==POST，找post包，找到最大的一个包

****

**右击追踪流**

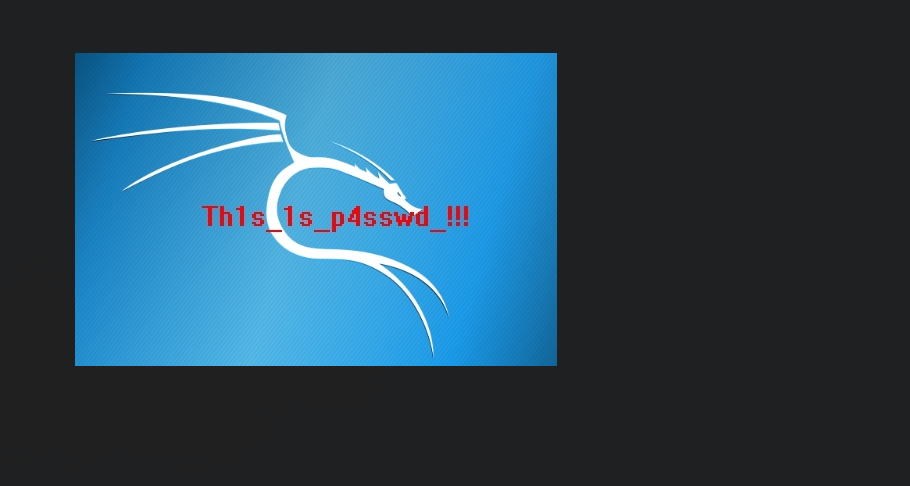
****

**发现可以的地方FF D8开头 FF D9 结尾，是jpg文件的二进制开头结尾，使用WinHex复制内容，保存，发现是一张图片。**

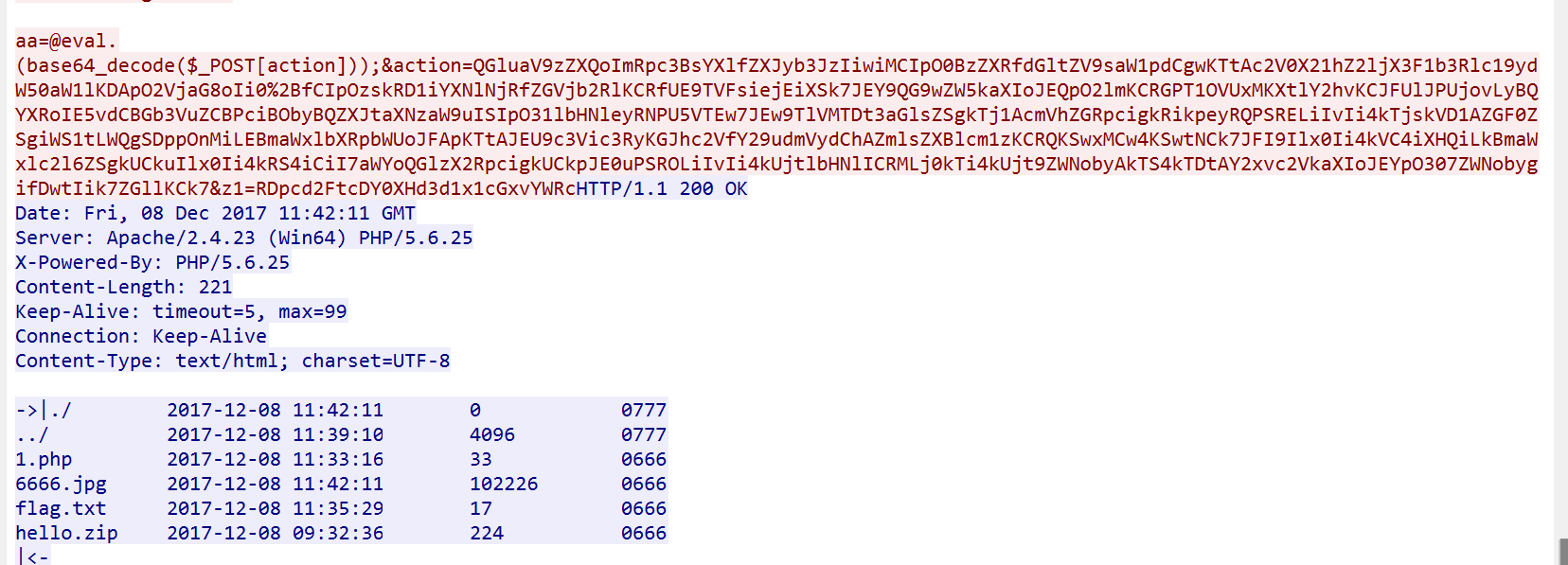
****

**根据图片内容这是一个密码。**

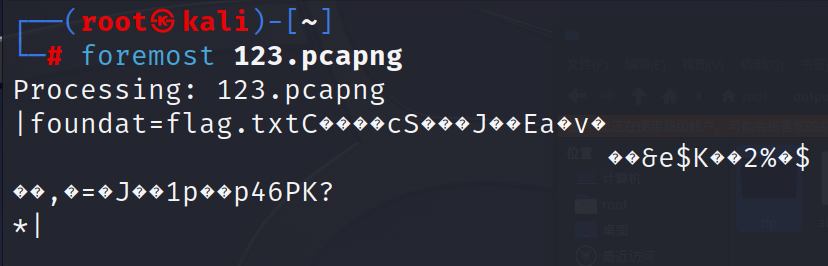
**Th1s\_1s\_p4sswd\_!!!**

****

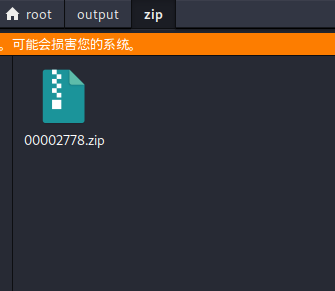
**我们回去再看一下pcapng文件，发现里面还有zip文件**

****

**利用foremost分离尝试分离123.pcapng文件**

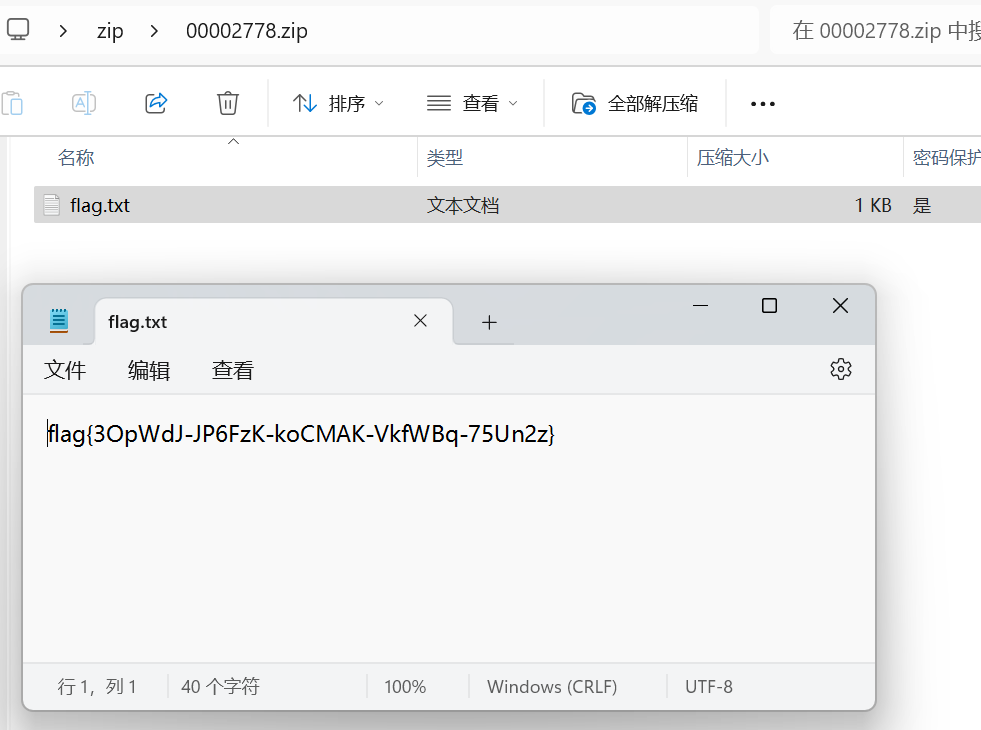
****

**存在zip文件**

****

**Zip文件是加密的状态，使用刚刚图片中的密码解密，解密成功，得到flag。**

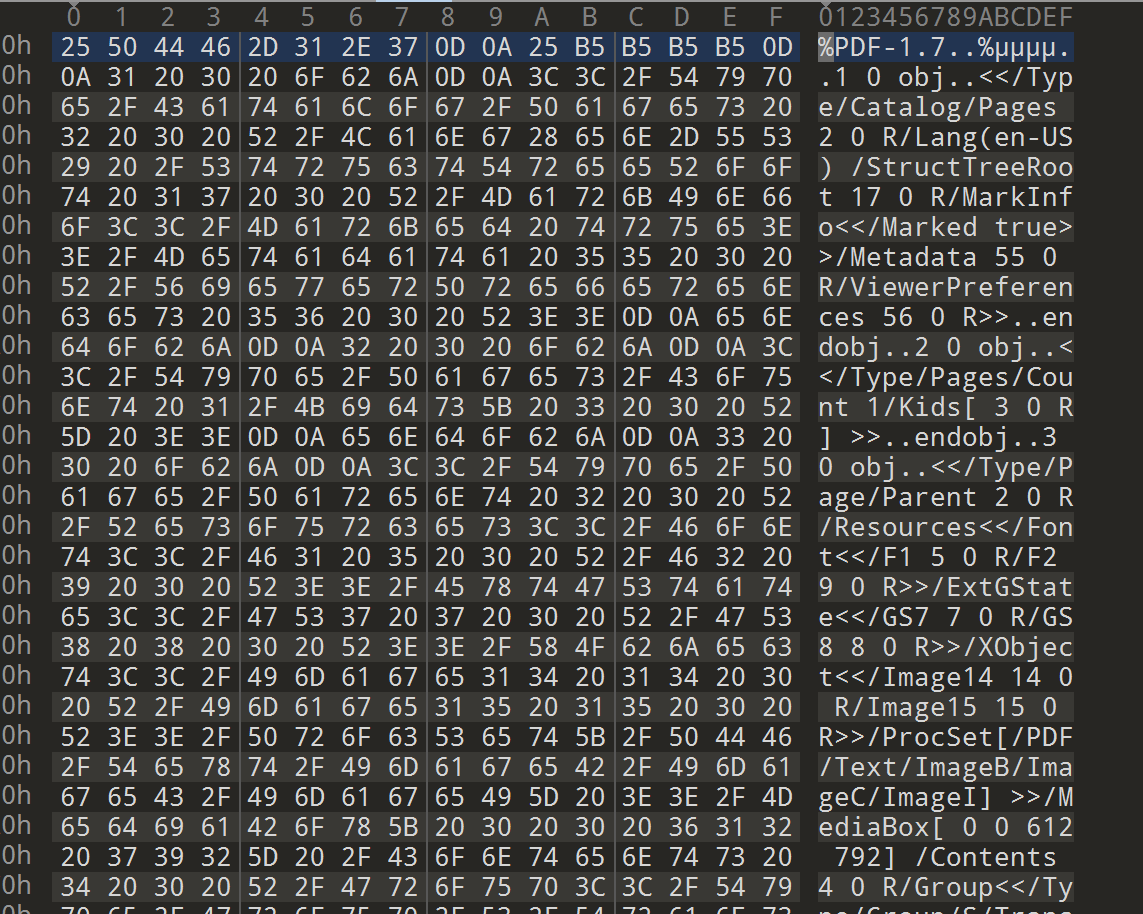
**flag{3OpWdJ-JP6FzK-koCMAK-VkfWBq-75Un2z}**

****

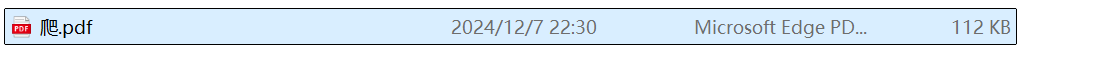
**Misc2**

**欢迎参加比赛，base庆祝！！！**

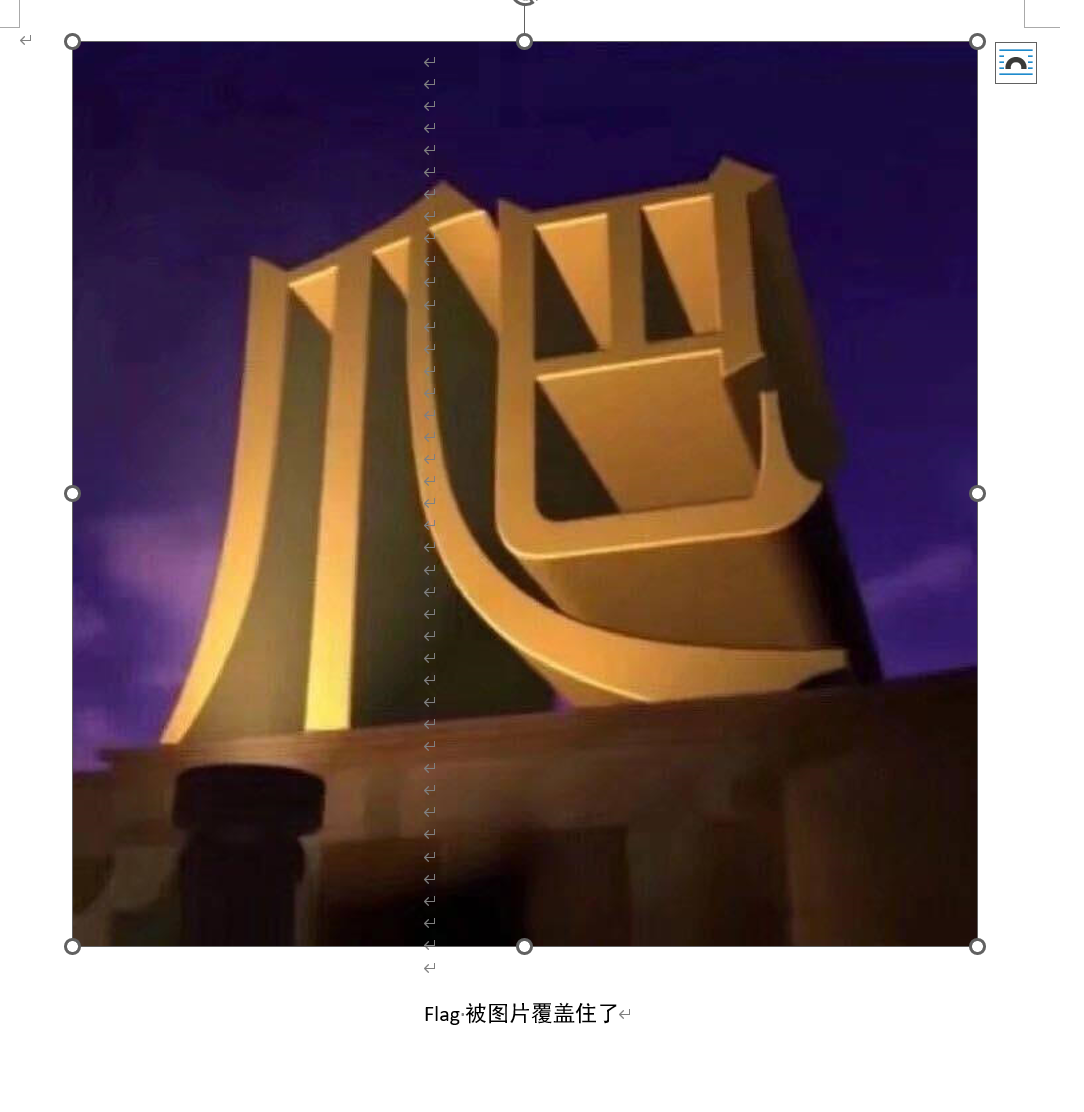
**下载文件，拖入010**

****

**发现是pdf，我们修改文件后缀，改为pdf**

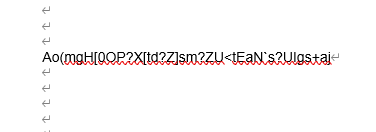
****

**转成文档**

****

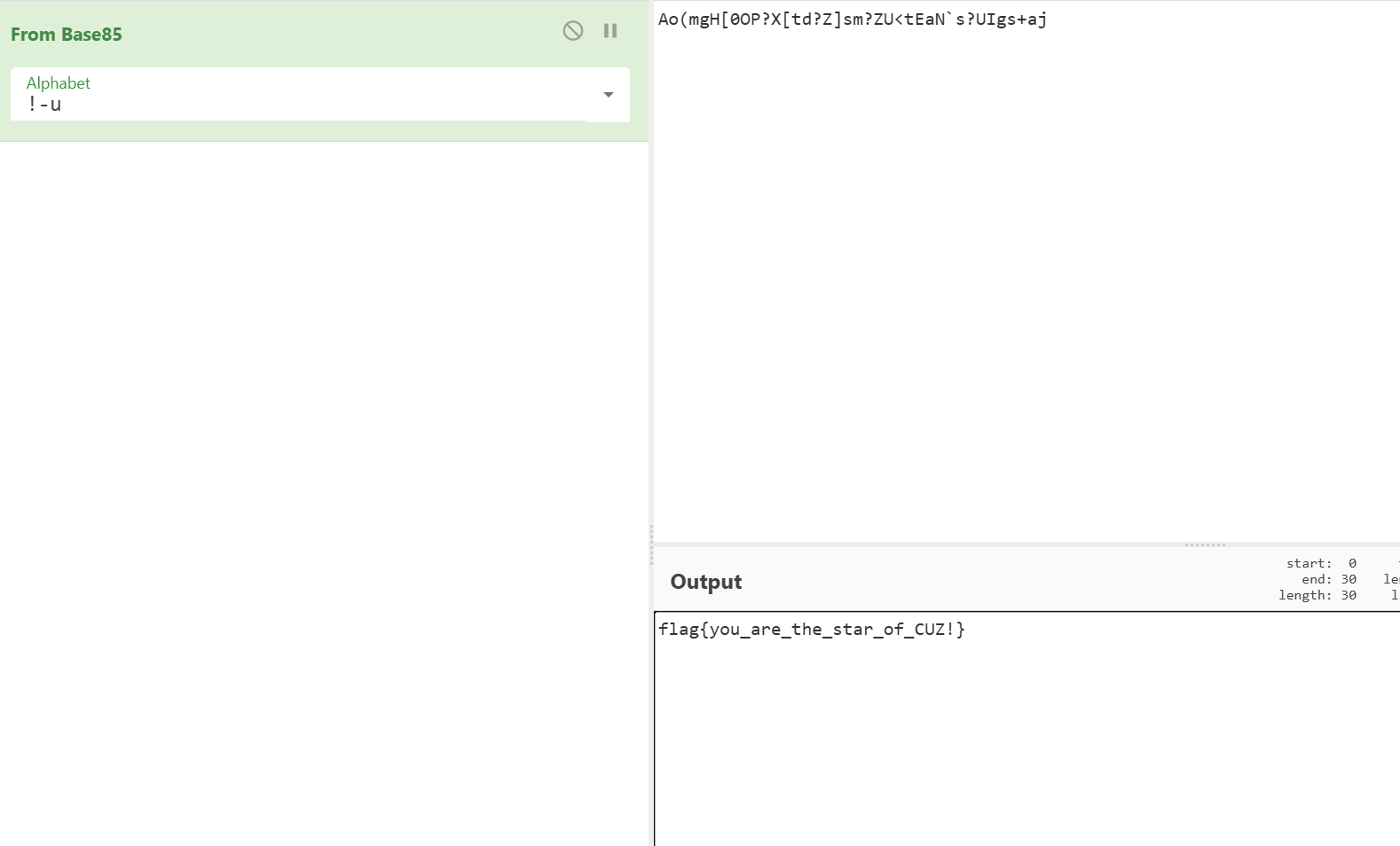
**直接删掉图片，我们获得了下面这个东西**

Ao(mgH[0OP?X[td?Z]sm?ZU<tEaN`s?UIgs+aj

****

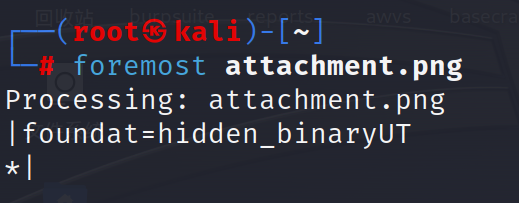
**CyberChef解密，Base85**

**flag{you\_are\_the\_star\_of\_CUZ!}**

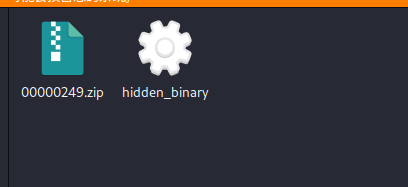
****

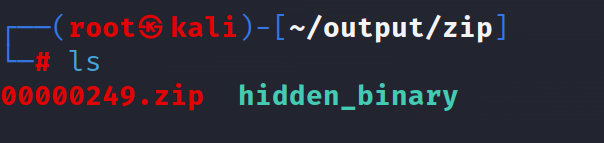
**Misc3**

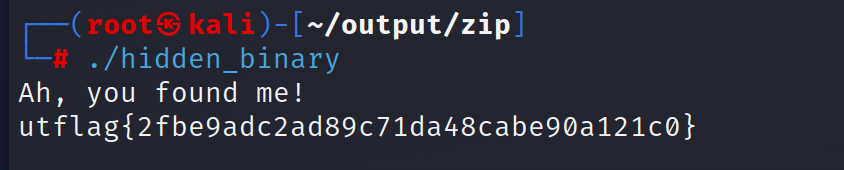
**真的很简单**

****

**解压缩zip**

****

****

****

**得到flag**

**utflag{2fbe9adc2ad89c71da48cabe90a121c0}**