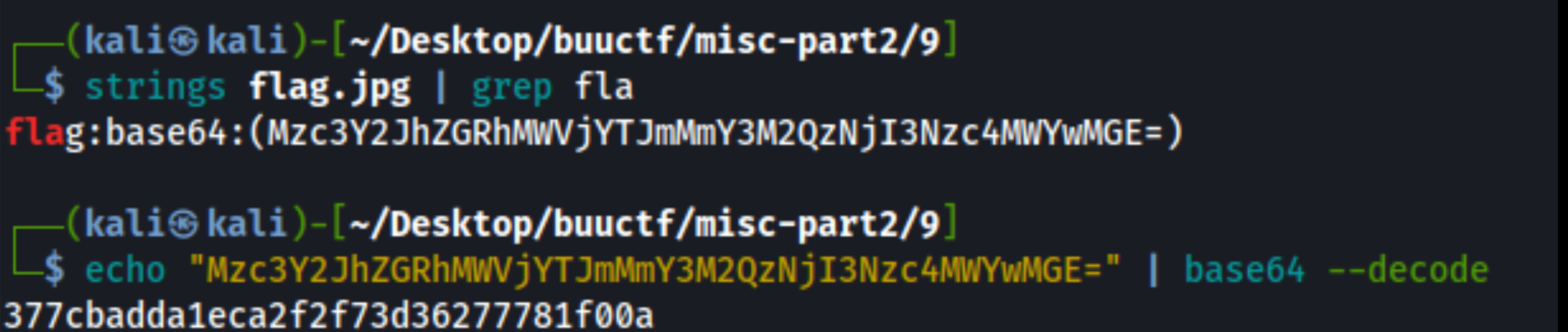
第一周周报

题目：

答案：flag{377cbadda1eca2f2f73d36277781f00a}

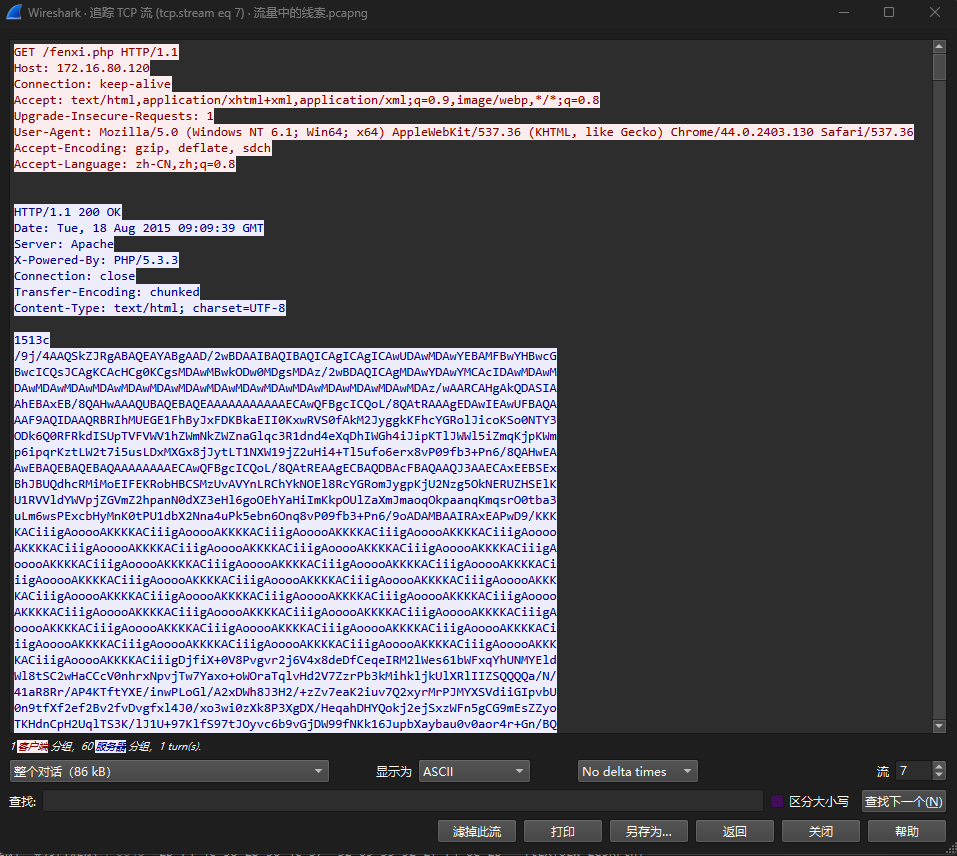
解题过程：属于图片隐写，下载题目文件，把图片放到kali中直接strings打印字符串就能得到答案的base64格式，解码后就是答案。



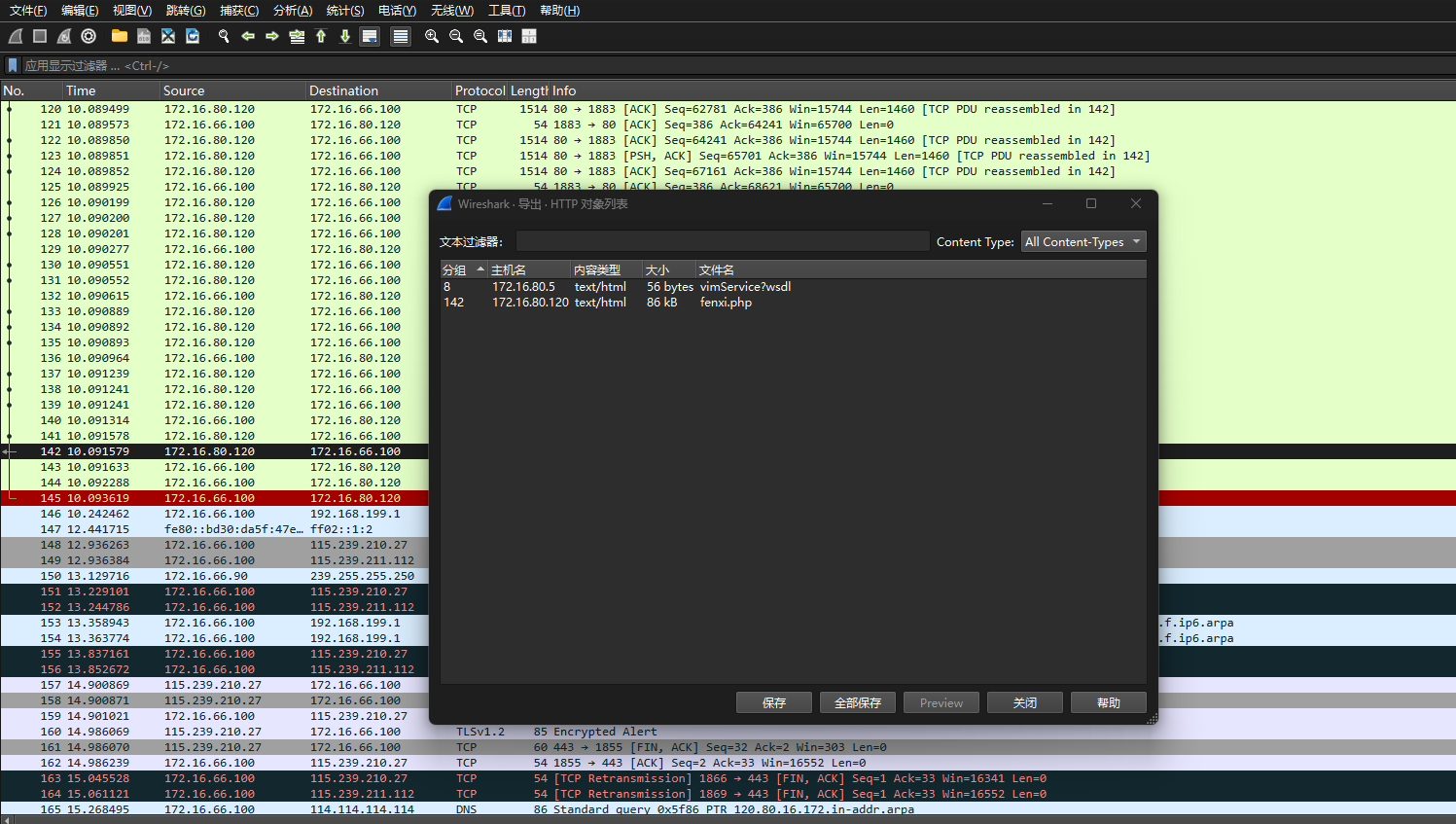
题目：

答案：flag{209acebf6324a09671abc31c869de72c}

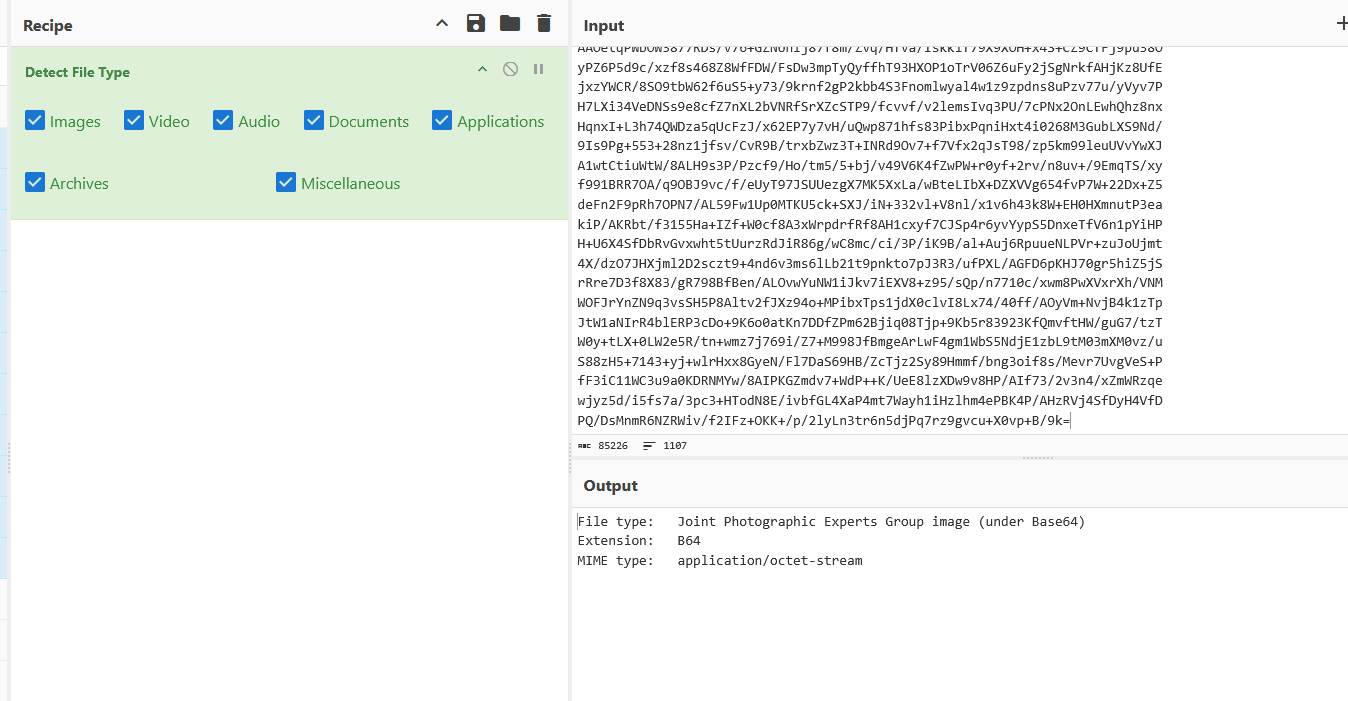
解题过程：（不太会，难题）日志分析，先下载题目文件，是个pcap，用wireshark打开，题目中提到是“数据包，但分析不出内容”，那首先找到目标数据包。打开流量日志后，右键选择追踪TCP流，很快就能浏览到一个可疑数据包流量，其请求了一个“fenxi.php”的文件，并且成功返回数据。



这里的数据非常像base64编码后的格式，所以我们的大致方向就是把这段编码提取出来然后base64解码试试。选择“文件”-“导出对象”-“HTTP”，就可以看到所有HTTP请求数据包的文件，我们把“fenxi.php”文件下载下来。



把文件中的内容导入在线CyberChef（新学的一个软件），导入后自动识别出了类型，是被base64编码后的jpg文件。

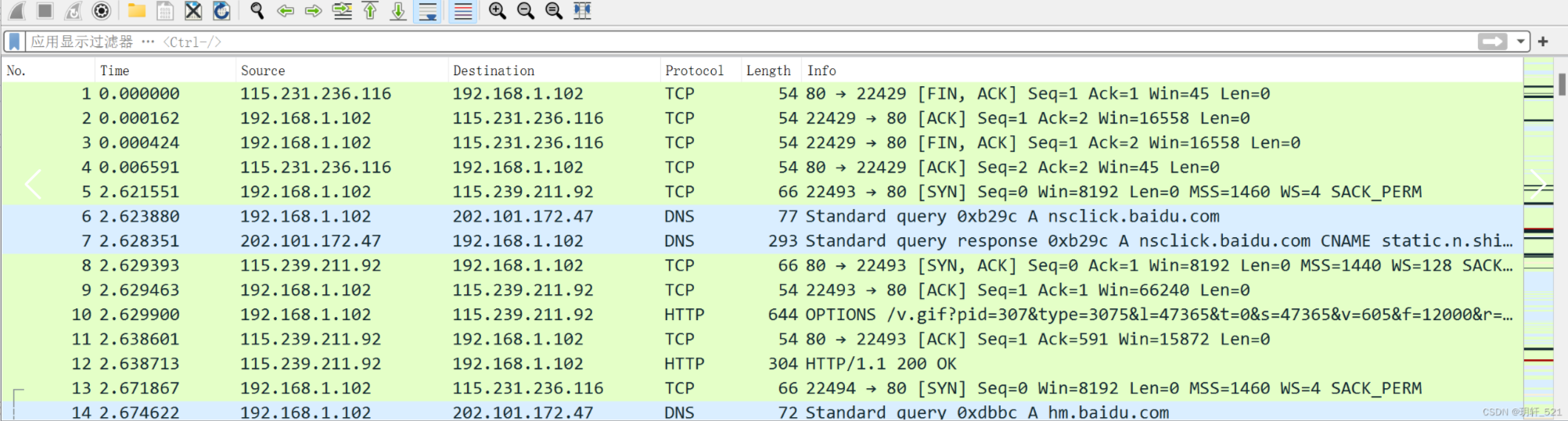
再base64解码，保存解码后的文件。该图像上就有我们要的答案了。这里base64解码后，CyberChef会提供在线渲染功能

题目：

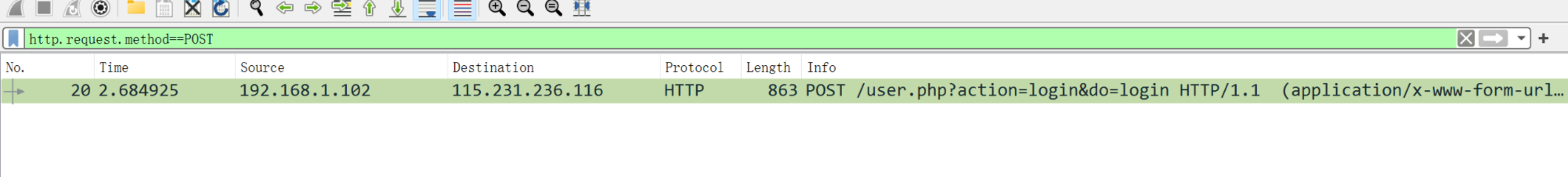
答案：flag{ffb7567a1d4f4abdffdb54e022f8facd}

解题过程：

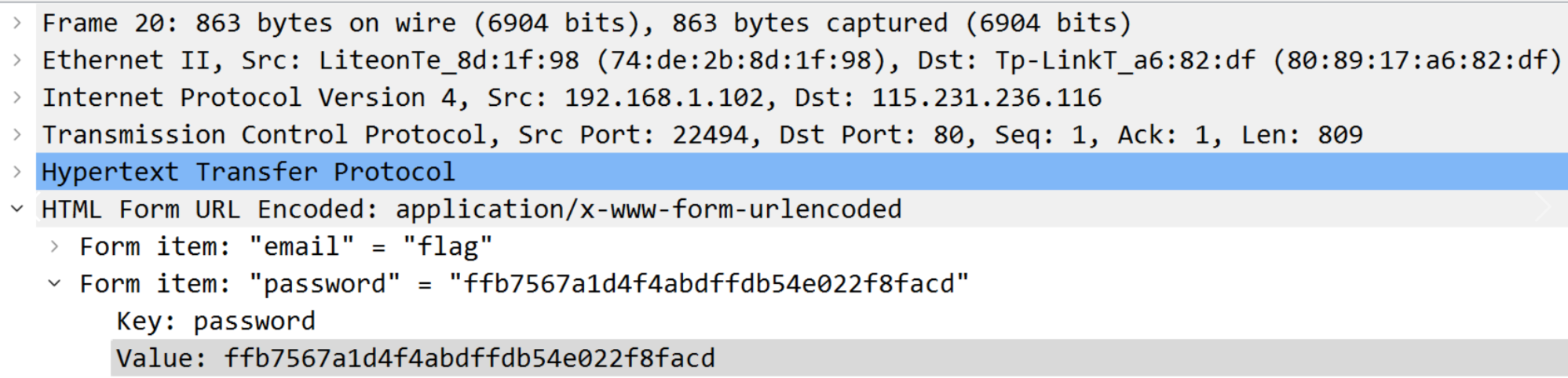
下载附件，解压后得到一个.pcap文件。双击文件，在wireshark打开。



分析题目，需要找到管理员登陆网站的流量，并从中找到登录密码。使用“http.request.method==POST”语句过滤流量包，得到一条登录流量。



分析这条流量，在[数据包](https://so.csdn.net/so/search?q=%E6%95%B0%E6%8D%AE%E5%8C%85&spm=1001.2101.3001.7020" \t "https://blog.csdn.net/YueXuan_521/article/details/_blank)详细信息中找到登陆密码“password”，得到flag。

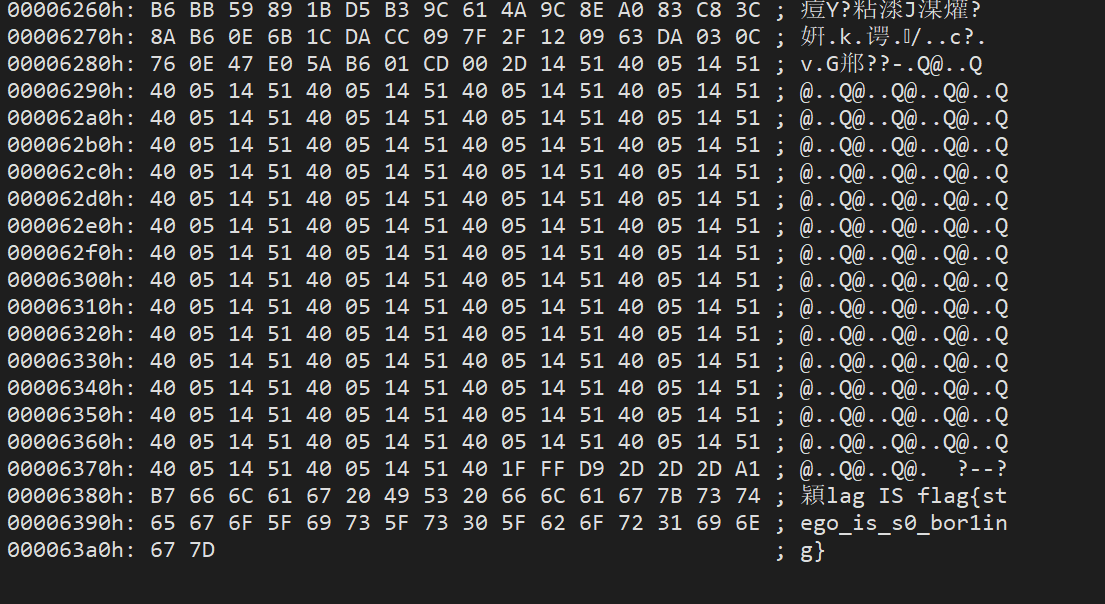


题目：

答案：flag{stego\_is\_s0\_bor1ing}

解题过程：首先下载文件，打开是一张图片

把图片放入UE找到最后flag



知识点：

工具：wireshark、CyberChef，UE

Wireshark是一款功能强大的开源网络抓包工具，广泛用于网络问题排查、协议分析和攻击溯源。

#选择菜单栏上Capture（捕获） -> Option（选项），勾选WLAN网卡（这里需要根据各自电脑网卡使用情况选择，简单的办法可以看使用的IP对应的网卡）。点击Start，启动抓包。

#[wireshark](https://so.csdn.net/so/search?q=wireshark&spm=1001.2101.3001.7020" \t "https://blog.csdn.net/wanqianshao/article/details/_blank)启动后，wireshark处于抓包状态中。

1、执行需要抓包的操作，如ping http://www.baidu.com。

2、操作完成后相关数据包就抓取到了。为避免其他无用的数据包影响分析，可以通过在过滤栏设置过滤条件进行数据包列表过滤，获取结果如下。说明：ip.addr 10.5.86.148 == and icmp 表示只显示ICPM协议且源主机IP或者目主机IP为10.5.86.148的数据包。

3、wireshark抓包完成。

UE：和010editor有异曲同工之妙，目前我只学会一点，就不详细说了