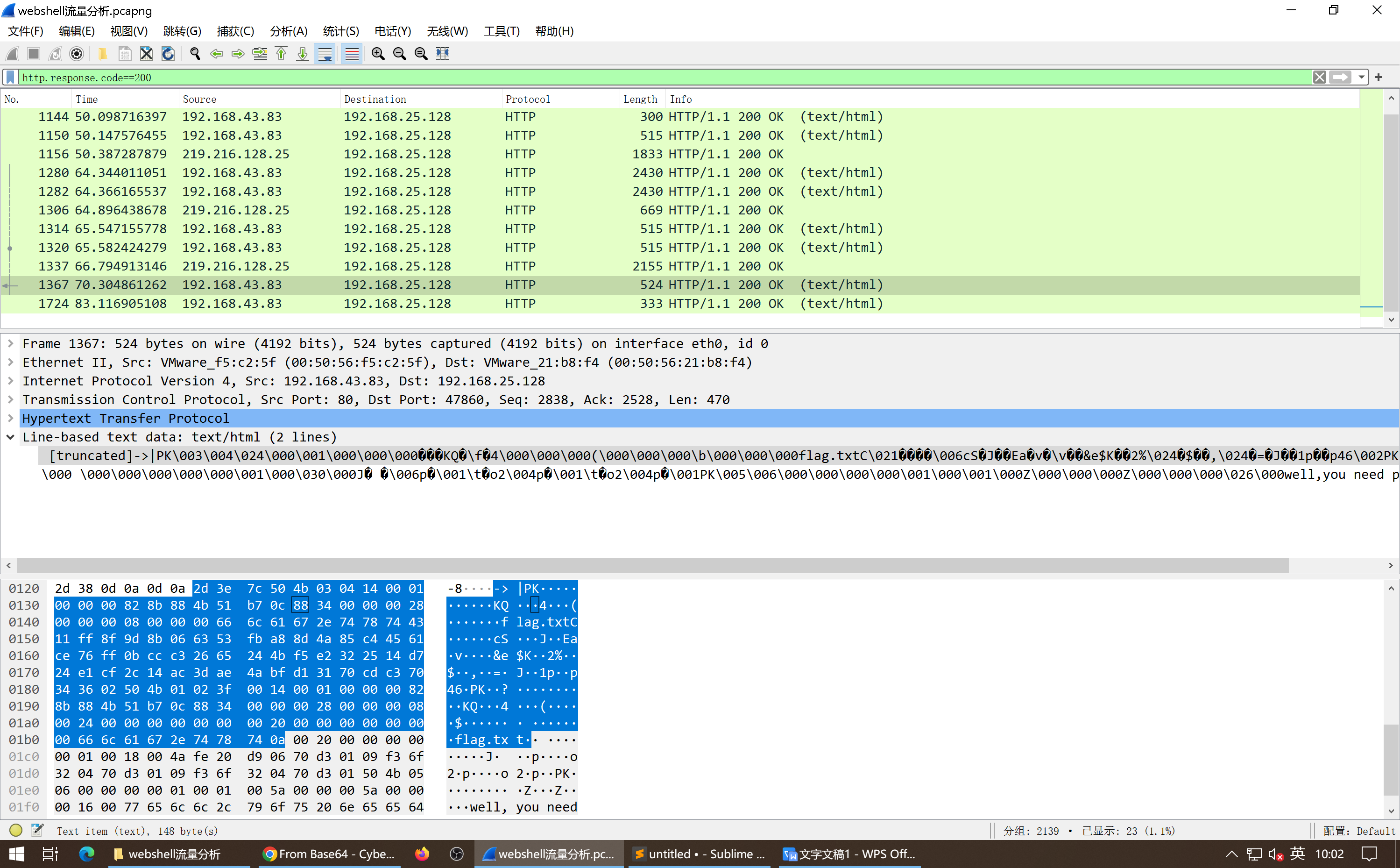
webshell流量分析

http.response.code==200

发现下载过一个zip包，追踪http流就能看到实际上返回的包在文件前后分别加了分隔符，删除分隔符提取zip，是加密的flag。

翻看与webshell的对话记录，发现网站目录下有个flag.txt，推测是通过向webshell发送命令加密压缩后回传的，密码就在向webshell发送的命令中



http.request.method==POST

翻了一遍并不是上面推测的，但是看到上传了一个图片，导出来之后发现是密码。

