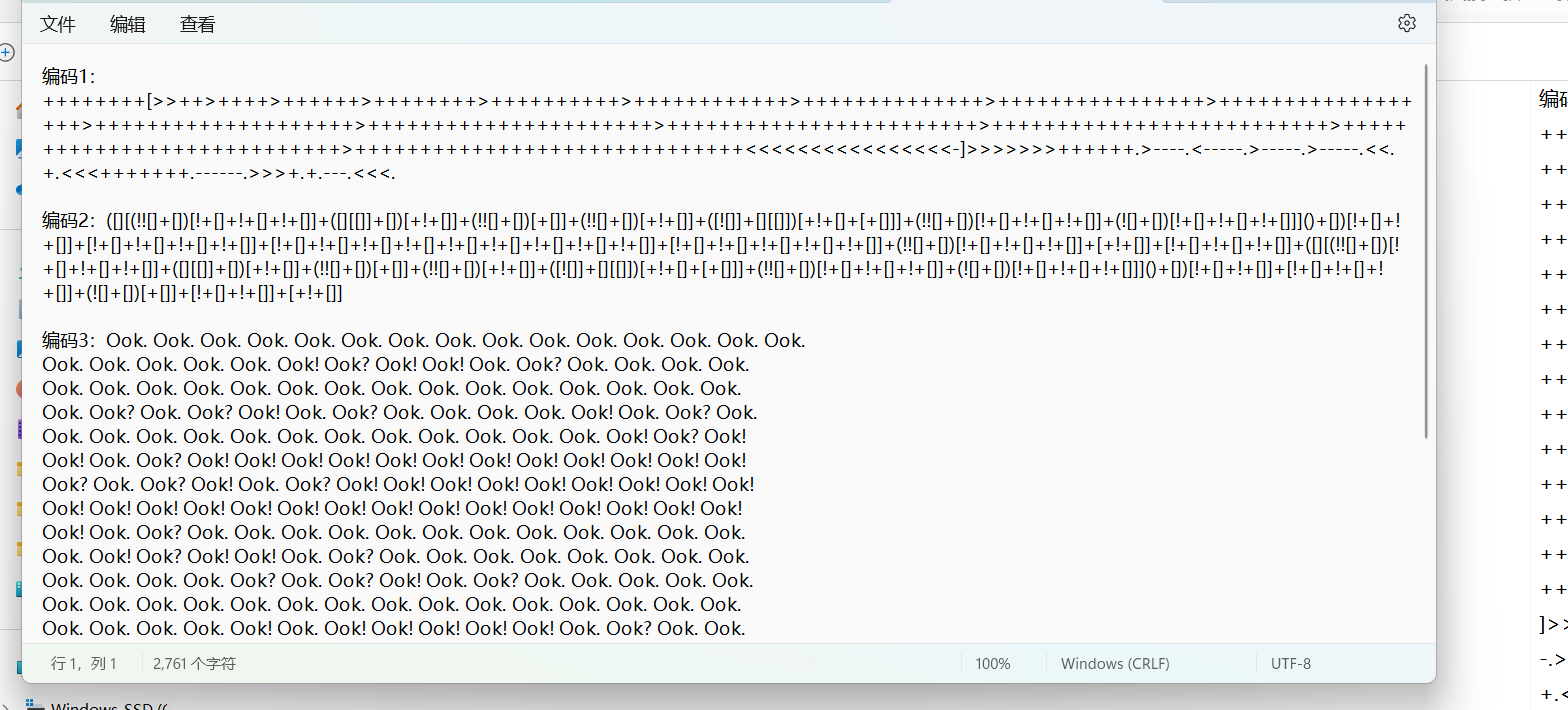
Misc

常见三种编码

Brainfuck

Jsfuck

Ook!



Brainfuck编码

语言只有八种符号，所有的操作都由这八种符号 \*\*(> < + - . , [ ])\*\* 的组合来完成

jsfuck编码

少量字符包括："!"、"+"、"("、")"、"["、"]"、"{"、"}"。只用这些字符就能完成对任意字符串的编码。

Ook! 编码

由Ook ! . ? 组成

网上解码网站很多

比如

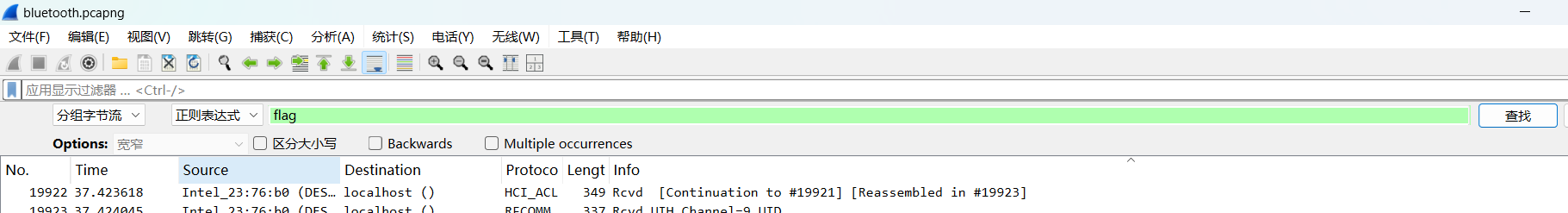
<http://www.hiencode.com/jsfuck.html>

<https://www.splitbrain.org/services/ook>

流量分析

1. flag明文

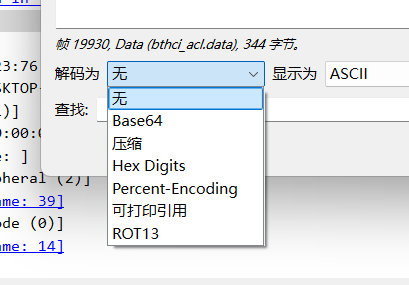
搜一下flag字符串



然后查看文本得到flag

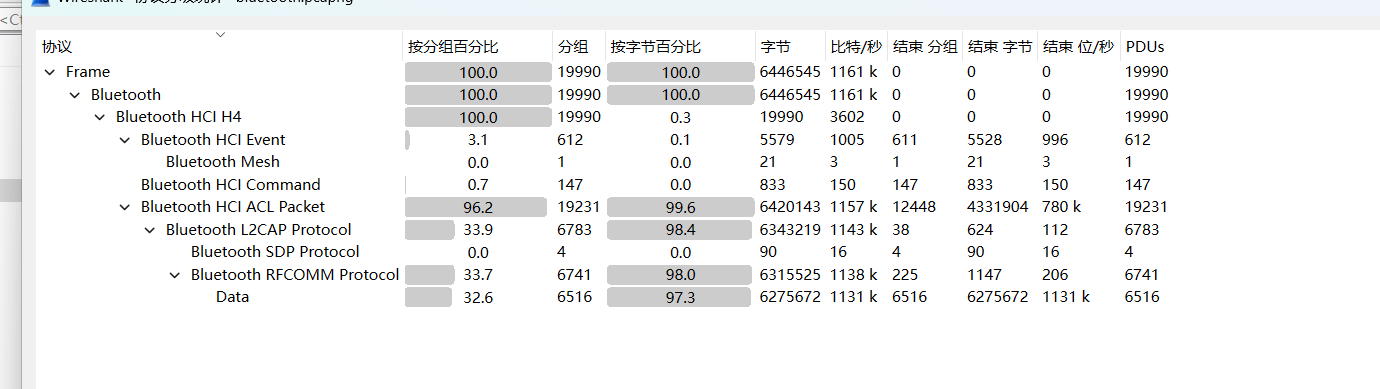
1. flag编码

显示分组字节后可以选择编码类型



1. 协议分析

整体浏览整个流量包协议，看看大多数是什么协议，再进行过滤



比如说http协议多，可以重点关注，过滤http流

4. 4.HTTP包

<1统计HTTP请求，看看是否有可疑文件，如果有例如php包，过滤HTTP找到php的发送包，然后追踪tcp流

<2导出HTTP对象，看看是否能输出什么信息，或者有什么数字和字符是能串成一串或者对大小排序

<3搜索得到的包里面的信息加入xinxi.php，可以先过滤http，再搜索xinxi字符串

<4过滤HTTP流，发现数据长度特别大异常的追踪它

http模式过滤

http.requst.method==”GET/POST”